調 査 報 告 書

2024 年 2 月 19 日

社内調査委員会

第１　調査委員会の概要

１　調査委員会を設置するに至った経緯

西日本電信電話株式会社（以下「NTT 西日本」という。）の完全子会社である株式会社 NTT マーケティングアクト ProCX（以下「ProCX」という。）及び NTT ビジネスソリューションズ株式会社（以下「BS」という。）は、2023 年 7 月 13 日、BS 社屋に対して警察による捜索差押えが行われたことを契機として、ProCX がテレマーケティング業務に際して委託元から提供を受け、BS が管理するサーバに保管されていた顧客情報の不正な持ち出し（以下「本件不正持ち出し」という。）が行われていた可能性を覚知した。その後の検証の結果、BS の元派遣社員である X が、少なくとも 2013 年 7 月頃から 2023 年 2 月頃にかけて本件不正持ち出しを行っており、その流出範囲は少なくともユーザー数にして約 900 万件、委託元数において 59 件であることが明らかとなった。

他方、上記捜索差押えとは別に、ProCX は 2022 年 4 月、ProCX が受託しているテレマーケティング業務の委託元である A 社から、A 社が ProCX に対して提供した個人情報につき流出の疑いがあるとして、社内調査を依頼されていた。当該依頼に対しては、同月から同年 7 月にかけて ProCX 及び BS の担当者による調査（以下「本件過去調査」という。）が行われ、ProCX の担当者は A 社に対し、本件過去調査の結果 ProCX からの顧客情報の流出は確認されなかった旨を報告した。しかし、NTT 西日本、ProCX 及び BS が本件不正持ち出し発覚後に行った調査（以下「発覚後社内調査」という。）において、顧客情報流出の事実、及び、本件過去調査に際して ProCX が A 社に提出した回答の中に、事実とは異なる回答が複数含まれていたことが確認された。

NTT 西日本は、事態の重大性に鑑み、NTT 西日本グループの信頼回復のため、同社が主導して、警察と連携しつつ本件不正持ち出しに係る事実及び原因を解明するとともに、本件過去調査の真相を究明し、NTT 西日本グループ全体で再発防止を図るには、社内メンバーのみでの調査で十分でないと判断し、2023 年 11 月 16 日付けで、外部の専門家を含めた調査委員会（以下「当調査委員会」という。）を立ち上げることとした。

なお、X は、その後の 2024 年 1 月 31 日、不正競争防止法違反の容疑で岡山県警に逮捕されている。

２　調査委員会の目的及び調査事項

当調査委員会は、事実調査及び原因・課題分析を通じ、本件不正持ち出し及び本件過去調査に対する再発防止策の提言を行うとともに、NTT 西日本グループ全体における情報セキュリティ体制の改善策の提言を行うことを目的とする、NTT 西日本代表取締

役社長の諮問機関としての社内調査委員会である。

当調査委員会の調査（以下「本調査」という。）の対象となる事項は以下のとおりである。

① 本件不正持ち出し及び本件過去調査に関する事実の調査
② ①の原因分析
③ ①②を踏まえたNTT西日本グループ全体の課題の分析
④ 再発防止策の提言
⑤ その他、当調査委員会が必要と認めた事項

3 調査委員会の構成等

当調査委員会は、調査委員会本体の下に、その下部組織として、情報セキュリティタスクフォース（以下「情報セキュリティTF」という。）及び過去調査検証タスクフォース（以下「過去調査検証TF」という。）を設置した。

情報セキュリティTFは、NTT西日本の情報セキュリティ関連部署の責任者に外部専門家を加えたタスクフォースであり、主としてシステム面及び技術面から、本件不正持ち出しの事実解明、分析及び再発防止策の策定を担当するとともに、NTT西日本グループ全体の情報セキュリティ体制の点検、課題分析及び改善策の策定を担当した。

過去調査検証TFは、本件過去調査の検証を目的として、外部弁護士のみにより構成されたタスクフォースであり、外部の客観的な観点から、本件過去調査の事実経過の解明、不適切な態様の原因分析及び再発防止策の策定を主な役割としていた。

当調査委員会及び各タスクフォースの構成は、以下のとおりである。一部の委員がタスクフォースを兼務することで調査委員会本体と各タスクフォースの相互連携を図りつつ、過去調査検証TFについては外部弁護士のみにより構成することで調査の客観性を担保した。

⑴ 委員

委員長	国谷　史朗	弁護士
委員	畝本　毅	弁護士（元高松高等検察庁検事長）
委員	飯島　奈絵	弁護士　NTT西日本社外監査役
委員	猪俣　敦夫	大阪大学サイバーメディアセンター教授
委員	白波瀬　章	NTT西日本　技術革新部長（CISO）
委員	黒田　勝己	NTT西日本　経営企画部長
委員	梶原　全裕	NTT西日本　総務人事部長

⑵ 情報セキュリティ TF

メンバー	白波瀬　章	NTT 西日本　技術革新部長（CISO）
メンバー	黒田　勝己	NTT 西日本　経営企画部長
メンバー	小田　孝和	NTT 西日本　デジタル改革推進部長
メンバー	寺尾　和幸	NTT 西日本　情報セキュリティ推進部長
アドバイザリー	猪俣　敦夫	大阪大学サイバーメディアセンター教授

⑶ 過去調査検証 TF

メンバー	畝本　毅	弁護士（元高松高等検察庁検事長）
メンバー	中山　貴博	弁護士
メンバー	大多和　樹	弁護士
メンバー	石田　明子	弁護士

⑷ 補助者等

本調査に当たり、当調査委員会は、弁護士法人大江橋法律事務所に所属する中山貴博弁護士、大橋君平弁護士、大多和樹弁護士、石田明子弁護士、具嶋光弘弁護士、立村達哉弁護士、高見恭一弁護士、田中想音弁護士、及び、片山優弁護士[1]、並びに、NTT 西日本・情報セキュリティ推進部、同・技術革新部、同・総務人事部、同・財務法務部、及び、CSOC[2]を調査補助者又は調査事務局とした。

ただし、過去調査検証 TF は、上記各弁護士のみを調査補助者とした。

4　調査期間

当調査委員会による調査期間は、2023 年 11 月 16 日から 2024 年 2 月 19 日までである。

上記期間中、合計 7 回の調査委員会を開催した。

5　調査方法

当調査委員会が実施した調査の具体的な内容は、以下のとおりである。

⑴ 関係資料の分析及び検討

---

[1] 2023 年 12 月 15 日まで。

[2] 「Cyber Security Operation Center」の略称。CSOC は、株式会社 NTT フィールドテクノ内に設置された部署であり、NTT 西日本グループ内のサイバーセキュリティ戦略、サイバーセキュリティ対策、監視・分析業務などを担っている。

当調査委員会は、BS 及び ProCX を含む NTT 西日本グループにおける規程類、情報セキュリティに関する資料、本件不正持ち出し及び本件過去調査に関する資料等の関係資料について、必要と認める範囲で検証、分析した。

⑵　ヒアリング

当調査委員会は、本件不正持ち出しに関して NTT 西日本グループ役職員 27 名（22 回[3]）に対するヒアリングを実施し、また、本件過去調査に関して NTT 西日本グループ役職員を中心とする 14 名（25 回[4]）に対するヒアリングを実施した。

当調査委員会は、複数回にわたり X に対するヒアリングの実施を試みたが、X がこれに応じることはなく、強制的な調査権限ないし捜査権限のない当調査委員会においてヒアリングを実施することはできなかった。ただし、X は一度だけ電子メールによる照会に対して返信したことから、その限りで X への事実確認は実現した（後記第３参照）。

なお、本件過去調査に関するヒアリングにおいては、NTT 西日本グループ外にも調査を拡大する必要があると判断し、A 社役職員へのヒアリングを実施したほか、本件システム（後記第２・４にて定義する。）のベンダである B 社の担当者に対する書面照会を実施した。

⑶　デジタル・フォレンジック

当調査委員会では、X 及び本件調査担当者ら（後記第６・１にて定義する。）計 5 名の NTT 西日本グループ役職員のメールサーバ・社内チャットサーバ等のデータに対しデジタル・フォレンジックを行い保全した。その上で、メール及び社内チャット（elgana）についてキーワード検索等を行い、本調査に必要と判断される範囲でこれらの内容を検証した。

以上のほか、X に貸与され、X がその業務に使用していた保守端末（後記第３・３⑴参照）に対しては、CSOC その他の関係部署が各種ログの解析を実施した。

⑷　システム緊急点検

情報セキュリティ TF では、顧客情報の取扱いがある NTT 西日本グループ（NTT 西日本、BS 及び ProCX を含む）内の全システムから一定の条件で抽出したシステ

[3] 同時に複数名に対するヒアリングを実施した場合もある。
[4] うち、本件調査担当者ら（後記第６・１にて定義する。）に対しては、それぞれ、C 担当部長 5 回、D 担当課長 2 回、E 担当課長 5 回、F 担当課長 7 回のヒアリングを実施した。

ム（全 443 システム）を対象に、緊急のシステム点検を行った。この緊急点検の詳細は後記第 7 を参照されたい。

⑸　アンケート調査

当調査委員会は、本件不正持ち出し及び本件過去調査並びに発覚後社内調査等を踏まえ、NTT 西日本グループ全体においても、内部不正による情報漏洩に対する情報セキュリティ体制の実態や役職員の認識を把握する必要があると判断し、NTT 西日本グループの役職員に対するアンケート調査を実施した。

このアンケート調査は、個人情報の取扱いがある NTT 西日本グループ（NTT 西日本、BS 及び ProCX を含む）内の全システムから一定の条件で抽出したシステム（全 204 システム）を所管する部署の役職員を対象としている。このアンケート調査の詳細は後記第 8 を参照されたい。

⑹　NTT 西日本、ProCX 及び BS による発覚後社内調査結果等の引継ぎ

本件不正持ち出し発覚後、本件不正持ち出し及び本件過去調査の適切性の検証に関しては、NTT 西日本、BS 及び ProCX による調査が行われていた。当調査委員会は、本調査に当たり、NTT 西日本、BS 及び ProCX から当該調査で収集された資料及び調査結果等の引継ぎを受けた。

6　調査の前提及び限界等

本調査は強制的な調査権限ないし捜査権限に基づく調査ではなく、あくまでも関係者の任意の協力により行っているものである。NTT 西日本、BS 及び ProCX から開示を受けた資料及びヒアリング対象者の供述の真実性については、当調査委員会において慎重な検討・判断を行ったが、裏付け資料を十分に得られないものや記憶が曖昧な供述があること、X へのヒアリングが実施できなかったこと、警察により押収された証拠が存在すること等、一定の制約があることに留意されたい。

また、本調査における認定は、当調査委員会の要請にもかかわらず、NTT 西日本、BS 及び ProCX から開示されていない資料が存在しないことを前提としている。

本調査における認定は、上記のような前提・制約の中で行われたことであり、当調査委員会が収集した以外の資料・供述等が存在し、新たな事実が発覚した場合には、本調査報告書の内容が変更される可能性を否定するものではない。

また、本調査報告書は、調査対象に関する事実確認、原因分析及び再発防止策の提言のためにのみ用いられることが予定されており、これらの目的以外に用いられること

を予定していない。

第２　関係法人の概要

１　株式会社 NTT マーケティングアクト ProCX（ProCX）

ProCX は、大阪市にその本店が所在する、NTT 西日本の完全子会社である。ProCX の前身は、NTT 西日本のテレマーケティング業務を担当する会社として 2002 年 5 月に設立された株式会社エヌ･ティ･ティマーケティング アクト（以下「旧 NTT アクト」という。）であり、2022 年 4 月、ProCX に対する事業譲渡により旧 NTT アクトの事業が承継された。

主な事業内容は、コンタクトセンタビジネスを始めとした、BPO（ビジネス・プロセス・アウトソーシング）業務運営事業であり、日本全国 40 拠点にてコンタクトセンタを展開し、これらの拠点にて受託したコールセンタ業務及びテレマーケティング業務等を運営している。

本件不正持ち出しとの関係で問題となるテレマーケティング業務は、大きく、アウトバウンドテレマーケティング業務及びインバウンドテレマーケティング業務に分類される。アウトバウンドテレマーケティング業務は、顧客（委託元）から提供される顧客リストに記載されている個人又は法人に対し、所定の回数の架電を実施し、その通話内容及び勧奨結果等を記録し、当該記録を委託元に納品する業務である。これに対し、インバウンドテレマーケティング業務は、委託元に対する顧客からの問い合わせを受け付け、当該顧客の問い合わせ内容等を記録し、当該記録を委託元に納品する業務である。

２　NTT ビジネスソリューションズ株式会社（BS）

BS は、大阪市にその本店が所在する、NTT 西日本の完全子会社である。2002 年 5 月 1 日、NTT 西日本の営業系、設備系及び共通系の業務を担うアウトソーシング会社が各地域に設立され、その後の NTT 西日本グループ内での組織再編の結果、2013 年 10 月 1 日、BS が設立された。BS は 2021 年 7 月 1 日付けで旧 NTT アクト、株式会社 NTT フィールドテクノ（以下「NTT フィールドテクノ」という。）、株式会社エヌ・ティ・ティ ネオメイト（以下「エヌ・ティ・ティネオメイト」という。）及び株式会社エヌ・ティ・ティ・ビジネスアソシエ西日本社の一部事業を継承している。

主な事業内容は、ビジネスユーザーに対する情報通信システムの提案、構築及びサポート等業務であり、各種システムの開発、提供及び保守運用業務を行っている。

３　ProCX と BS の業務委託関係

前記１のとおり、ProCX は、コールセンタ業務やテレマーケティング業務を受託し

ているところ、当該業務の遂行のために、BS から提供を受けたコールセンタ業務用システム提供サービス（以下、このコールセンタ業務用システムを「本件システム」といい、このコールセンタ業務用システム提供サービスを「本件サービス」という。なお、本件システムは 2020 年に旧システムから新システムに更新されている。）を用いている。

すなわち、ProCX は、BS との間で締結された「AQStage IP コールセンタサービス利用契約」（現「ONE CONTACT Network サービス利用契約」）[5]に基づき、本件サービスを利用し、顧客（委託元）から受託したコールセンタ業務等を行っている。

ProCX のコンタクトセンタは、主にスーパーバイザー（以下「SV」という。）とオペレータにより構成されている。SV は、オペレータの統括を行う立場であり、ProCX の顧客（委託元）から預かった顧客（お客様）に関するデータ（以下「顧客データ」という。）を本件システム内のデータセンタにある「PDS サーバ」のデータベースにアップロードして格納したり、顧客データに紐づいたお客様との対応結果に係るレポートを出力したり、委託元にフィードバックしたりするなど、顧客データの管理や分析を行っている。一方、オペレータは、テレマーケティング業務を行うに当たり必要な顧客データを PDS サーバのデータベースから閲覧し、自動発信による架電又は受電を通じたお客様との対応結果を当該データベースに書き込むなどしている。

PDS サーバを搭載したコールセンタサービスは、2000 年頃に発表された 20 年以上の歴史を有するサービスであり、主としてアウトバンドテレマーケティング向けに利用されている。PDS とは「Predictive Dialing System」の略称であり、PDS サーバは、いわゆる自動予測発信機能を備えており、顧客データベースを元にオペレータの配置状況等に応じてシステムが自動的に発信し、顧客が応答した場合にのみオペレータに接続する。

BS は、本件サービスの提供主体として、当該サービスを安定的に提供するため、PDS サーバを含む本件システムの保守運用を行うとともに、ProCX による本件サービスの利用を専門的・技術的側面からサポートしている。

4　本件システムの構成

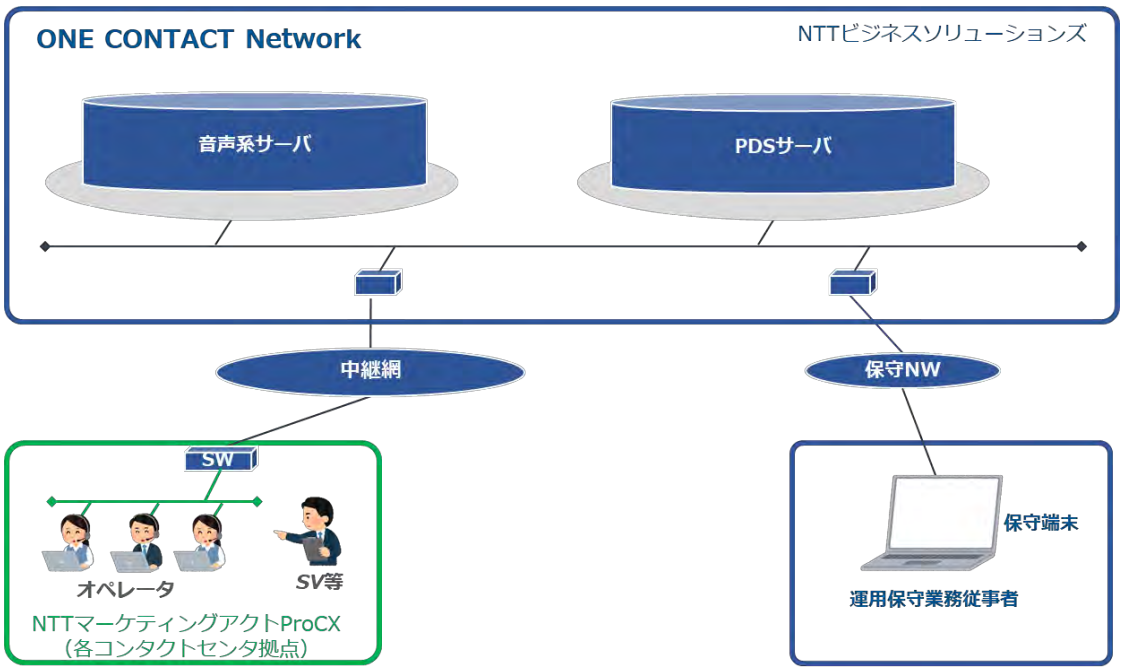
PDS サーバや音声系サーバを始めとした、本件システムの中枢となる機能は、「ONE CONTACT Network」というネットワーク（以下「本件ネットワーク」という。）上に存在する。各コンタクトセンタの SV やオペレータは、各コンタクトセンタから「中継網」を通じて本件ネットワークにアクセスし、保守運用を行う保守要員は、保守拠点か

[5] 2022 年 3 月 31 日付け「AQStage IP コールセンタサービス利用契約書の変更に関する覚書」に基づき、サービス名称が「AQStageIP コールセンタサービス」から「ONE CONTACT Network サービス」に変更され、これに伴い、ProCX・BS 間の契約名称も「ONE CONTACT Network サービス利用契約」に変更されている。

ら「保守網」を通じて本件ネットワークにアクセスする仕組みとなっている。

これらのシステムはいずれも閉域網[6]として構築されており、この仕組みを図示すると下図のとおりである。

【図　ONE CONTACT Network の構成】



6 外部からのアクセスが遮断され、許可された者のみがアクセス権限を有するネットワーク網をいう。

第３　本件不正持ち出し

１　概要

X は、BS において本件システムの運用保守業務等に従事していた。X は本件システムの運用保守業務従事者としての立場を悪用し、本件システムに特権的なアクセスが可能であったこと等に乗じて、少なくとも 2013 年 7 月頃から 2023 年 2 月頃にかけての約 10 年間にわたり、多数回、顧客情報を不正に外部に持ち出していた。

当該顧客情報は、アウトバウンドテレマーケティング業務の用に供するために ProCX が委託元である企業及び自治体から提供を受けた情報であり、電話番号のほか、電話番号に括り付けられた情報として、氏名・郵便番号・住所・性別・生年月日／年齢・顧客番号・配送方法・受注日時等の情報が含まれていた（ただし、委託元又は受託業務ごとに異なる。）。

本件不正持ち出しにより持ち出された顧客情報の少なくとも一部は、X によって、いわゆる名簿業者に売却されていたことが確認されている。X 自身も、電子メールでの質問に対し、詳細は明らかにしなかったものの、本件システムから顧客情報を外部に持ち出し、これを名簿業者に流出させたことを認めている[7]。

２　X の就業状況

X（昭和 35 年生まれ、男性）は BS の元派遣社員であり、同社が警察による捜索差押えを受けた 2023 年 7 月 13 日時点において、同社のバリューデザイン部（以下「VD 部」という。）内のグループ（以下「X 所属グループ」という。）に所属していた。

X は、2008 年 6 月、派遣元企業から BS の前身企業の一つであるエヌ・ティ・ティネオメイトに派遣され、それ以降、同氏の BS における最終勤務日である 2023 年 7 月 10 日に至るまで約 15 年間にわたり、PDS サーバに専門的な知見を有する有スキル者として本件システムの運用保守業務等に携わっていた。X は、BS 社屋に対して警察による捜索差押えが行われた後に音信不通となった。派遣元会社によれば、X は、一定期間連絡が取れなくなったことを適用事由とする自動退職規定の適用により、同月 25 日付けで派遣元会社を自動退職になったとのことである。

X は、X 所属グループにおいて、フロント SE 業務[8]（提案支援、仕様検討・構築支援等）を担当するチームに属しつつ、本件システムの運用保守業務のうち、主として ProCX 向け PDS サーバの運用保守及びサポート業務に従事していた。

---

[7] X が私用で用いていた電子メールアカウントを確認した上で、当該電子メールアカウントに対して質問事項を送信し、当該電子メールアカウントから、質問事項に対する返信を受けた。

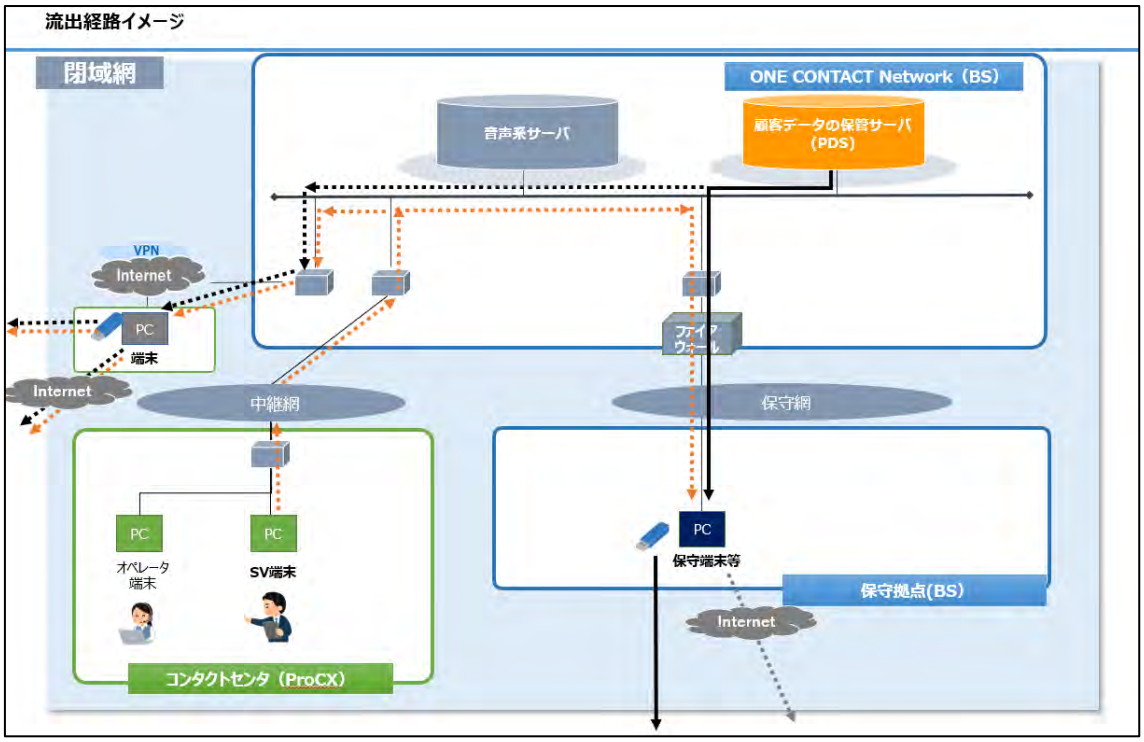
[8] システムのユーザーの目に直接触れる部分（操作メニュー・アイコン等）を扱うほか、提案支援、仕様検討・構築支援等を担当する SE を「フロント SE」という。

3　情報流出経路・不正持ち出しの方法

本件システムにおいて、ProCX がアウトバウンドテレマーケティング業務のために委託元から提供を受けた顧客データは、エヌ・ティ・ティ・スマートコネクト株式会社が運営するデータセンタ内において BS が管理する PDS サーバに格納されていた。BS の内部者が PDS サーバに格納された顧客データを外部に流出させる経路としては、①本件ネットワークへアクセスし、②PDS サーバ等から顧客データを取得の上、③顧客データを外部に持ち出すという経路を経ることが考えられる[9]。

BS 及び情報セキュリティ TF による調査の結果、X は、上記経路から、以下のとおり複数の方法を用いて、PDS サーバに格納されていた顧客データを不正に流出させていた可能性があることが判明した。

（想定流出経路の概念図）



⑴　本件ネットワークへのアクセス

前記第２・４のとおり、PDS サーバにアクセスするための本件ネットワークは閉域網として構築されており、本件ネットワークにアクセスするには「保守網」、「中継

[9] なお、本件ネットワークに対し外部から不正な通信があった形跡は確認されていない。

網」又は下記の在宅オプションのいずれかのルートを経ることになる。

X は本件システムの運用保守業務従事者として、同氏に貸与されていた保守端末から、「保守網」を通じて本件ネットワークにアクセスすることが可能であった[10]。X 自身も、本件不正持ち出しに当たり、この方法により本件ネットワークにアクセスしたことを認めている。

また、本件システムには、コールセンタのオペレータのリモートワークを想定して、オペレータが VPN を経由して本件ネットワークにアクセスできる機能があった（以下、このアクセス方式を「在宅オプション」という。）。BS の運用保守業務従事者である X が ProCX のコールセンタのオペレータ用の機能である在宅オプションを利用することは本来想定されていなかったが、ProCX のコールセンタ向けに在宅オプションの利用に必要なアカウント ID 及びパスワードを払い出す業務にも X が携わっていたことから、これらの ID 及びパスワードを知り得る立場にあった。X はこれらの情報を利用して在宅オプションを通じて本件ネットワークにアクセスすることも可能であり、実際、X が保守端末から、在宅オプションの利用に必要なアカウント ID 及びパスワードを使用して本件ネットワークにアクセスしていた形跡が確認されている。

上記のとおり、本件ネットワークには「中継網」を通じてアクセスするルートがあるが、「中継網」は ProCX の SV やオペレータのために設定されたネットワークであり、現在までのところ、X が当該ルートを用いて本件不正持ち出しを行った形跡は確認されていない。

したがって、X は、本件不正持ち出しに当たり、同氏に貸与されていた保守端末から、「保守網」又は在宅オプションのいずれかを使って本件ネットワークにアクセスしていたと推定される。

⑵　PDS サーバ等からの顧客データの取得

ア　システム管理者アカウントを用いた PDS サーバからのダウンロード

PDS サーバには、ProCX が設定する各テナント[11]に保存されている全ての顧客データを閲覧し、ダウンロードできるアカウントが存在し、X を含む BS の本件システムの運用保守従事者には全てのテナントにおける当該アカウント（以下、総称して「システム管理者アカウント」という。）の使用が許されていた。

PDS サーバのログ及び X に貸与されていた保守端末の解析結果等から、X は、

[10] 保守網には、BS のオフィスにおいては社内に設定されたネットワークを用い、オフィス外においては VPN を用いてアクセスする。

[11] テナントは、1 つの委託元団体に対し 1 つ設定される場合もあれば、委託元からの受託案件の内容に応じて受託案件ごと又はその他の区分ごとに細分化して設定される場合もある。

システム管理者アカウントを用いてPDSサーバから顧客データを保守端末又はこれに接続されたUSBメモリにダウンロードしていたことが判明した。

X自身も、保守端末からPDSサーバにアクセスし、システム管理者アカウントを用いて、PDSサーバからダウンロードした顧客データをUSBメモリに保存して外部に持ち出したことを認めている。

なお、本件システムでは、本件ネットワークへのアクセスルートとして保守網又は在宅オプションのいずれを用いる場合であっても、私有端末（PC等）を用いることは技術的に制限されていなかった。そのため、顧客データのダウンロードには上記保守端末だけではなく、Xの私有端末が用いられていた可能性もある[12]。

イ　その他の方法による顧客データ取得の可能性

Xにより不正に持ち出された顧客データには、システム管理者アカウントによるPDSサーバからのダウンロードログが確認できないものが存在する。

これらの顧客データにはコンタクトセンタのSVアカウントでダウンロードされたものが含まれているところ、PDSサーバのログの解析結果等からは、XがSVアカウントを用いてPDSサーバにアクセスしたことを示す証跡は発見されておらずその可能性は低い。そのため、Xは、前記アの方法のほかに、コンタクトセンタのSVが正当な業務として顧客データをダウンロードした際に、何らかの方法により当該顧客データを取得したと考えられるが、Xは具体的にどのような方法を用いたかを明らかにしていない。

そこで、情報セキュリティTFでは、以下のような複数の仮説を設定し、検証を行った。検証の結果、現時点では、このうち③（SVアカウントでダウンロードされ、SVが使用する端末（以下「SV端末」という。）に保存された顧客データに対し、共有設定を通じてアクセスし、これを取得した可能性）が有力視されている。

なお、警察の捜査に影響するおそれがあるため詳細な説明は控えるが、前記ア以外の方法による顧客データの取得方法の特定は、後記4記載の流出範囲に影響を与えるものではない。

① PDSサーバからの顧客データのインポート及びファイルをエクスポートしてダウンロードする時にシステム内で生成される一時保存ファイルを取得した可能性
② SVアカウントでダウンロードされ、各コンタクトセンタ内の共有サーバ

[12] 当調査委員会はXの私有PCを調査することができず、Xの私有PC又はこれに接続されたUSBメモリ等に顧客データがダウンロードされていた可能性を排除することができなかった。ただし、現状、Xの私有PCが顧客データの本件不正持ち出しに用いられたことを裏付ける証跡は見当たっていない。

（NAS サーバ等）に保存された顧客データにアクセスし、これを取得した可能性

③ SV アカウントでダウンロードされ、SV 端末に保存された顧客データに対し、共有設定によりアクセスし、これを取得した可能性

④ SV アカウントでダウンロードされ、SV 端末に保存された顧客データに対し、リモートデスクトップ接続によりアクセスした可能性

⑶ 取得した顧客データの外部への持ち出し方法

X に貸与されていた保守端末には、USB メモリ等の外部記録媒体へのデータの書き出しを不可能にする技術的な措置は講じられていなかった。X に貸与されていた保守端末の解析結果等によれば、X は PDS サーバ等から取得した顧客データを保守端末等に接続した私有 USB メモリに保存して外部に持ち出していた。X 自身もこの方法による持ち出しを認めている。

このほかに、当該保守端末の解析結果等から、X が、貸与された保守端末（ウェブメールへのアクセス制限措置は講じられていなかった。）からウェブメールのウェブページにアクセスしていた形跡が確認されている。そのため、X がウェブメールに添付してこれを保存ないし送信する方法で顧客データを外部に持ち出していた可能性もある。

なお、前記⑵アのとおり、本件システムでは、本件ネットワークへのアクセスルートとして保守網又は在宅オプションのいずれかを用いる場合であっても、私有端末（PC 等）を用いることは技術的に制限されていなかった。そのため、顧客データのダウンロードに X の私有端末が用いられていた場合には、X は何らの制約なく当該私有端末を経由して顧客データを外部に持ち出すことができたのであり、本件不正持ち出しにはこの方法が用いられた可能性もある。

なお、警察の捜査に影響する恐れがあるため詳細な説明は控えるが、保守端末に接続した USB メモリに書き出す方法以外による持ち出しの可能性は後記 4 記載の流出範囲に影響を与えるものではない。

⑷ 共犯の可能性について

X による本件不正持ち出しに共犯者が存在していた可能性は、可能性としては排除されない。

しかし、情報セキュリティ TF による PDS サーバのログ解析及び X に貸与された保守端末の解析等によっても、共犯者が存在したことを裏付ける証拠は見当たらなかった。また、X が使用していた業務用のメールアドレス及び社内チャットである

elgana のチャット履歴も調査したが、当該調査によっても、共犯者が存在したことを裏付ける証拠は見当たらなかった[13]。

4　持ち出された顧客情報の範囲

本件不正持ち出しにより X が持ち出した委託元の顧客情報は、アウトバウンドテレマーケティング業務の用に供するために ProCX が委託元から提供を受けた情報であり、電話番号のほか、電話番号に括り付けられた情報として、氏名・郵便番号・住所・性別・生年月日／年齢・顧客番号・配送方法・受注日時等の情報が含まれており、委託元 2 社については顧客 81 件のクレジットカード情報（番号、有効期限、支払方法、支払回数）が含まれていた（持ち出された情報の種類は、委託元又は受託業務ごとに異なる。）。

X が持ち出した顧客情報の分析から、本件持ち出しは、遅くとも 2013 年 7 月頃から 2023 年 2 月頃までの間、多数回にわたり行われていた。

ProCX 及び BS が 2023 年 10 月 17 日に公表した流出範囲は、委託元 59 団体、顧客数にして約 900 万件であったが、その後のさらなる調査により、委託元 69 団体、顧客数にして 928 万件の流出が確認されるに至った。

上記顧客数 928 万件のうち 117 万件は、委託元団体と紐づけることが困難な状況にある。

5　本件不正持ち出しの動機・正当化

X が本件不正持ち出しを行った動機については、X 本人の供述を得ることができず、これを解明するには至らなかった。しかし、X は不正に取得した顧客情報を名簿業者に売却していることからすれば、その動機には、名簿業者への売却による利益享受が含まれていたと認められる。

「動機」及び「機会」と並んで不正のトライアングルの一要素とされる「自己正当化」についても、X の供述を得ることができず、X の心理を解明するには至らなかったが、一つの可能性として、X が BS における自身に待遇について不満を抱いていた可能性が考えられる。すなわち、X が PDS サーバの有スキル者でありながら派遣社

[13] X の業務用の電子メールアカウントについて、電子メールの抽出が可能な 2016 年 11 月 16 日から X の最終出勤日である 2023 年 7 月 10 日までを対象期間として、X が送受信した電子メール 11 万 3405 件のうち、キーワード検索又は CSV ファイルの添付の有無等により絞り込みをかけた 6607 件のレビューを行った。X の私用のメールアドレスを宛先又は CC に含む電子メールも発見されたが、その大半は飲食店や宿泊施設の予約に関するものであり、本件不正持ち出しそのものに関連するメールは見当たらなかった。また、X の elgana のチャット履歴について、X が elgana を利用し始めた 2021 年 12 月 1 日から 2023 年 7 月 10 日までを対象期間とし、そのうち、キーワード検索によって絞り込みをかけた 356 件のメッセージをレビューしたが、いずれも業務上のやり取りと判断され、本件不正持ち出しに関連する履歴は見当たらなかった。

員という立場であったことを踏まえると、X が自身の賃金その他の待遇が PDS サーバの有スキル者としての貢献に釣り合ってないと考え、名簿業者への売却による利益享受はこのような不釣り合いを解消する行為であるなどと自己正当化していた可能性は否定できない。このような可能性はあくまでも可能性の一つであるはあるが、再発防止策を検討する際の一つの手掛かりになると考えられる。

第４　本件不正持ち出しを許した直接的な原因の分析

１　技術的な管理措置に係る重大な不備

後記第５・１のとおり、BS の情報セキュリティに係る管理措置には多数の不備が存在していたことが判明しているが、これらの中でも、下記の⑴から⑸の技術的な管理措置の不備が、X による本件不正持ち出しを許し、これを長年発見することができなかった直接的な原因を形成していると認められる。

⑴　PDS サーバからの顧客データのダウンロードを制御する措置の不存在

本件システムの運用保守業務においては、トラブル対応時のサポート等において PDS サーバにアクセスする必要が生じる場合があった。しかし、これらの業務において常に PDS サーバ内の顧客データを閲覧できるまでの必要性は乏しく、まして常に顧客データのダウンロードを可能にしておく必要性はなかった。

それにもかかわらず、X が使用することを許されていたシステム管理者アカウントには、ProCX が設定する各テナントに保存されているすべての顧客データをダウンロードする権限が設定されていた。そして、このダウンロード権限に対しては、事前承認を得ない限り顧客データのダウンロードはできないなどといった技術的な制限措置は講じられていなかった。

このほか、本件システムには、異常なダウンロードをシステム的に監視する振る舞い検知機能も、ダウンロードが実行されたことを然るべき監督者に通知する機能も存在していなかった。

このように、本件システムにおいては、システム管理者アカウントの使用者による PDS サーバからの顧客データのダウンロードを制御する措置は存在していなかった。

⑵　私有 USB メモリ等の外部記録媒体への書き出しを防止する措置の不存在

X が本件不正持ち出しに用いた保守端末（X に貸与されていたもの）には、使用を許可された指紋認証機能 USB メモリ以外の外部記録媒体へのデータの書き出しを物理的又は技術的に防止する措置は講じられておらず、保守端末から私有 USB メモリ等にデータを書き出すことが可能であった。

⑶　保守端末からのインターネット接続を制限する措置の不存在

X が本件不正持ち出しに用いた保守端末（X に貸与されていたもの）は、インター

ネット接続を技術的に制限する措置が講じられておらず、ウェブメールを用いて保守端末に保存した顧客データを自由に外部に送信することが可能であった。

⑷　ログ監視の不存在

本件システムのPDSサーバへのログインログ及び顧客データのインポート／エクスポート（ダウンロード[14]）ログは記録されていたが、これらのログを定期的に点検し、異常の有無をチェックする運用は行われておらず、これを実施する担当者も指定されていなかった。

加えて、システム管理者アカウントは、Xを含む本件システムの複数の運用保守従事者の間で共用されていたため、その使用者をログから一意に特定するというログ監視の前提的条件さえも欠く状況であった。

このほか、本件不正持ち出しに用いられたと考えられる経路に関して言えば、本件ネットワークへのアクセスルートである在宅オプションの接続ログ、外部記録媒体の接続ログ及び保守端末からインターネットへの接続ログについても、定期的に点検する運用は行われていなかった。

⑸　私有端末によるアクセスを制限する措置の不存在

本件システムでは、本件ネットワークへのアクセスルートとして保守網又は在宅オプションのいずれかを用いる場合であっても、私有端末（PC等）を用いることは技術的に制限されていなかった。前記第３・３⑵ア及び同⑶のとおり、本件不正持ち出しにXの私有端末が使用されていた可能性は否定できないことから、Xの私有端末が本件不正持ち出しに用いられていた場合には、私有端末によるアクセスが技術的に制限されていなかったことが、前記⑵及び⑶に代わり、本件不正持ち出しの直接的な原因の一つを構成することになる。

⑹　小括

前記⑴ないし⑸によれば、Xが顧客データの不正持ち出しを意図しさえすれば、これを容易に実行することが可能な状況が存在していた。このような状況は、内部不正による情報漏洩リスクに対し極めて脆弱であると言うほかなく、情報セキュリティに係るBSの技術的な管理措置には重大な不備があったと評価せざるを得ない。

このような技術的な管理措置の不備は、Xに本件不正持ち出しの機会を与えるものであり、結果としてXによる本件不正持ち出しを許し、これを長年発見すること

[14] ここでは「エクスポート」と「ダウンロード」は同義。以下、文脈に応じて使い分ける。

ができなかった直接的な原因を形成していると認められる。

2　内部者による情報漏洩リスクを高める業務運営体制

一般に特権的なアクセス権限には権限悪用リスクが内在するところ、以下に詳述するとおり、本件システムの運用保守業務の業務運営体制には当該リスクを高める状況が存在していた。このような状況が前記1で指摘した技術的な管理措置の不備と相まって、Xによる本件不正持ち出しを許し、これを長年発見することができなかった直接的な原因を形成していると認められる。

なお、当調査委員会の調査はXの最終勤務時期に重点を置いたものではあるが、2017年頃から業務上Xに接する機会のあったF担当課長へのヒアリングや2020年11月以降Xの上長を務めたE担当課長より以前のXの歴代上長等への簡易ヒアリング[15]によっても、本件不正持ち出しが確認されている2013年にまで遡った場合に上記状況と著しく異なる状況があったと考えるべき事情は見当らず、2013年からXの最終勤務時期に至るまで以下の状況が継続していたと見ることが妥当である。

⑴　Xの業務遂行状況

BS社屋に対して警察による捜索差押えが行われた2023年7月13日の直前期である同年6月末当時、XはBSのVD部内のX所属グループにおいて、E担当課長が統括するフロントSEチームに所属していた。

Xは、前記第３・２のとおり主としてProCX向けPDSサーバの運用保守及びサポート業務に従事していたが、フロントSEチーム自体は、ProCXとの関係では、同社の要望に応じた本件システムの提案、仕様検討、構築支援等のフロントSE業務を担当しており、本件システムの運用保守は担当していなかった。

フロントSEチームは、当時、Xを含め10名程度で構成され、ProCXへの委託元ごとに営業人員とフロントSE人員の各1名をペアとする担当分けが行われていたが、Xはフロント SEチームの本来の業務担当からすると異質なPDSサーバの運用保守及びサポート業務を担当していたことから、上記ペアの担当割当ても委託元の区別もなく、本件システムの提案、仕様検討、構築支援等を担当する同チーム内で特殊な立場にあった。

また、Xは、基本的に、E担当課長他フロントSEチームが主たる業務拠点としていた本社オフィスではなく、本件システムの運用保守全般を担当するバックSE[16]チームの主たる業務拠点であり、保守拠点として位置付けられていた拠点（以下、「本

[15] 正式なヒアリングとして実施したものではなく、簡易な形式で過去の状況を確認したものである。
[16] ユーザーの目に直接触れない部分（サーバ・データベース等）を扱うSEを「バックSE」という。

件保守拠点」という。）で業務をしていた。

このようなXの特殊な立場は、XがE担当課長の下に配属された2020年11月当初からのものであり、E担当課長によれば、このような状況は本件サービスがBSの前身企業の一つであるエヌ・ティ・ティネオメイトにより運営されていた頃から継続していたと思われるとのことである。

2008年頃より長年にわたりProCX向けPDSサーバの運用保守及びサポート業務に従事していたXは、フロントSEチーム及びバックSEチームのメンバーの中でPDSサーバに最も詳しく、PDSサーバのベンダであるB社の担当者と共同で社内向け研修講師を勤めるなど、傑出してPDSサーバに関する豊富な知見を有していた。そのため、X所属グループでは、PDSサーバに関わる作業のかなりの部分をXに依存しており、このような状況が長きにわたり固定化していた。

バックSEチームには、他にPDSサーバの有スキル者として、Xとは別の派遣社員1名がおり、同人もPDSサーバに関する保守又はサポート業務を行うことがあったが、同人とXが同一のトラブル対応又はサポート依頼に対して協働して対処することは通常なく、XによるPDSサーバに関連する作業はその大半が単独作業であった。

⑵　Xに対する業務監視が機能していなかった状況

ア　上長等による監督状況

前記⑴のとおり、Xとその直属の上長であるE担当課長は別の業務拠点で業務をしており、直属の上長がXの業務を直接監督できない状況にあった。また、XはPDSサーバに詳しい人物としてProCXの従業員から信頼を得ていた。そのため、XがE担当課長を通さずに、ProCXから直接かつ単独で対応依頼を受けることも珍しくなく、そのような場合はE担当課長に事後報告すらしないことも少なくなかった。E担当課長によれば、Xの業務状況については定期的なチームミーティング等で把握するように努め、また、Xに対し「個人事業主のような仕事の受け方はするな」という趣旨の指導はしていたが、大きな改善は見られず、半ばXの振る舞いを黙認していた面もあったとのことである。E担当課長は、このような状況を指して「Xは野放し状態。しかし、頼らざるを得なかったのが実態」と表現している。

また、E担当課長は、Xがその業務においてPDSサーバから顧客データをダウンロードする必要性について正確な認識を持っておらず、当調査委員会のヒアリングに際し「クライアントから『ダウンロードしてもエラーが出てしまう』といった問い合わせがあれば、テストのためにダウンロードすることはあったのではな

いかと思う。仮に X が顧客データをダウンロードしている現場を見ても、通常の業務と思うのではないかとも思う。」などと曖昧な理解を述べるにとどまった。

他方、X が主な勤務場所としていた本件保守拠点を業務拠点とするバック SE チームは F 担当課長が統括していたが、F 担当課長は直接の部下ではない X を監督する任になく、X とは、バック SE チームが行う業務について X の助力が必要になった場合に協働する形での関わりがあるにすぎなかった。なお、F 担当課長も、X がその業務において PDS サーバから顧客データをダウンロードする必要性について正確な認識を持っていなかった。

加えて、E 担当課長及び F 担当課長は、PDS サーバに最も詳しく ProCX の担当者の信頼も厚い X を信頼しきっており、X の業務に対して疑問を持つきっかけもなかった。

以上のほか、前記 1 ⑷のとおり、フロント SE チームにおいてもバック SE チームにおいても PDS サーバのログインログ及びエクスポートログの定期点検が実施されていなかったことを考え合わせれば、ProCX から提供を受けた顧客データの取扱いに関しては、上長等による X に対する監督はほとんど実効的に機能していなかったと評価せざるを得ない。

上記のように X がフロント SE チームとの関係でも、バック SE チームとの関係でも特殊な立場にあり、そのために、X に対する実質的な監督者が不在となっていた状況が生じた経緯は必ずしも明らかではないが、その背景には、X の PDS サーバに対する傑出した専門性ということのほかに、X が担当していた業務の内容がフロント SE チームとバック SE チームというチーム区分に当てはまらないものであったことも影響していると考えられる。すなわち、フロント SE チームとバック SE チームとの間には、本来は、フロント SE チームが顧客の要望を受けてその実現に必要な仕様や設定を定義し、バック SE チームがこれを受けて実装や改修を行うという役割分担が存在するところ、X は PDS サーバに関してはその両方の役割を遂行できるスキルを有し、現にその役割を担っていた。そのために、 X をフロント SE／バック SE というチーム区分の枠組みに当てはめることができず、その状況がこれまで続いてきたものと考えられる。

イ　同僚による相互牽制の状況

前記⑴のとおり、バック SE チームには、X の他に PDS サーバの有スキル者として、X とは別の派遣社員 1 名がいたが、同人と X が協働することは通常なく、X が PDS サーバに触れる作業については同僚による監視も機能していなかった。同人も当調査委員会のヒアリングに対し「同じオフィスにいれば、X が PDS サーバの作業をしていたことは分かるが、具体的に何をしていたかは知らなかった」と

述べている。

このように、X の PDS サーバに関する業務について同僚による相互牽制は機能していなかった。

⑶ 小括

以上のとおり、X 所属グループでは、PDS サーバに関する業務を X に依存しており、そのような状況が長期固定化されていたにもかかわらず、PDS サーバへの特権的なアクセス権限を持つ X に対する監督は実効的に機能していなかった。

このような状況は、一般にリスクが高いとされる特権的なアクセス権限を有する運用保守業務従事者による内部不正リスクをさらに高めるものであり、前記 1 で指摘した技術的な管理措置の不備と相まって、内部不正による情報漏洩リスクが極めて高い環境を作り出し、結果として、X に本件不正持ち出しの機会を与えたものと評価せざるを得ない。

第５　根本的な原因・背景の分析

本件不正持ち出しを許した直接的な原因の分析は前記第４のとおりであり、これらの原因がいずれもBSに帰することからしても、その一次的責任が本件システムを運用するBSにあることは論を待たない。もっとも、実効的な再発防止策を提言する観点からは、ProCX及び両社の親会社であるNTT西日本にまで視野を広げて、根本的な原因・背景分析を行うことが適切である。

そこで、当調査委員会は、以下のとおり、BS、ProCX及びNTT西日本の別に、根本的な原因・背景の分析を行った。

１　BSについての原因・背景分析

⑴　情報セキュリティに係る社内規律が遵守されていない状況

NTT西日本はNTT西日本グループの統一的な基準として「情報セキュリティマネジメント規程」及びその下位規程を策定し、BSはこれらを自社の規程として定めている（以下、これらの規程を総称して「NTT西日本グループ管理規程」という。）。

情報セキュリティに係る技術的な管理措置は、主として「情報セキュリティマネジメント規程」の一つである「情報セキュリティ規則ICT編」において定められている。また、「情報セキュリティマネジメント規程」の下位規程には「お客様情報[17]」の保護に焦点を当てた「お客様情報保護運用マニュアル」があり、当該マニュアルにも関連ルールが存在する。

前記第４・１で重大な不備があると指摘した技術的な管理措置については、以下のとおり、NTT西日本グループ管理規程が遵守されておらず、そのために、前記第４・１で指摘した重大な不備は長年是正されることなく放置されてきた。

ア　PDSサーバからの顧客データのダウンロードを制御する措置

（ア）アカウント管理

PDSサーバからの顧客データのダウンロードを制御するためには、その前提として、PDSサーバにアクセスできるアカウントを管理することが必須になる。

[17] お客様情報保護運用マニュアルにおいて、「お客様情報」とは、事業活動を行う過程で取得し、保有するお客様に関する情報を意味し、具体的には氏名、生年月日、住所、電話番号、その他記述等によりお客様を識別することができる者等を意味する。なお、「お客様」とは、個人及び法人その他団体であるかを問わず、当直接の顧客のほか、当該顧客の顧客を含み、また、現に顧客である者のほか、過去において顧客であった者及び今後顧客になり得る者を含む。

「情報セキュリティ規則 ICT 編」セキュリティ対策ルールは、この点について下表のとおりルールを定めている。

しかしながら、前記第４・１⑷のとおり、実際には、X が使用を許されていたシステム管理者アカウントは共用されており、アカウント管理の最低限の要請である「利用者アカウントを個人単位に付与すること」（3-12）という点すら遵守されていなかった[18]。

また、この共用されていたシステム管理者アカウントについては、その使用者が指定されていたわけではなく、本件システムの運用保守業務に携わる者がその必要に応じて使用している状況であった。加えて、システム管理者アカウントの ID とパスワードは、関係者であれば容易に知り得る単純な設定ルールに従って設定されており、これらが厳重に保秘されているとは言い難い状況であった。

このような杜撰な管理状況であったため、当然のことながら、管理手順及び管理者は定められておらず（3-1 及び 3-2）、アカウントの点検（3-3）も実施されていなかった。

番号	対策ルール
3-1	アカウントの不正取得や不正利用による侵害リスクを低減するため、アカウントの管理手順を定めること
3-2	アカウントの不正取得や不正利用による侵害リスクを低減するため、アカウント管理者を定めること
3-3	アカウントの不正利用による侵害リスクを低減するため、定期的にアカウントを点検すること
3-12	利用者アカウントの不正利用による侵害リスクや、被害発生時の分析を可能とするため、利用者アカウントを個人単位に付与すること

（イ）システム管理者アカウントの権限範囲

「情報セキュリティ規則 ICT 編」セキュリティ対策ルールは、システム管理者アカウントの権限範囲について下表のとおりルールを定めている[19]。

しかしながら、前記第４・１⑴のとおり、実際には、システム管理者アカウントの使用につき上長の承認を得る運用（10-5）は行われていなかった。

---

18 アカウントの共用に関しては、他の関連規程として、「情報セキュリティ規則一般業務編」が「共用のアカウントによるアクセスを禁止すること。機器仕様上の制約等によりやむを得ず共用アカウントを使用する場合は、当該アカウントを誰が利用したかを特定できるようにすること。」と定めている（同規則 3.1.1 h.）。

19 他の関連規程としては、「情報セキュリティ規則一般業務編」が「アカウント（利用者、管理者 ID 含め）の付与は、役割に応じた権限の付与状況を整理した上で、業務上の必要性を考慮し、必要最小限に絞り込むこと。」と定めている（同規則 3.1.1 e.）。

また、前記第４・１⑴のとおり、システム管理者アカウントには、その必要がないにもかかわらず、顧客データの無制限のダウンロード権限が付与されていた（3-5、3-9 及び 3-10 関係）。X 所属グループでは、このような権限設定が必要最小限であるのかという検討がされたこともなかった（3-10 関係）。

番号	対策ルール
10-5	保守運用行為による侵害リスクを低減するため、保守運用作業を管理すること ／システムの保守運用において、端末およびツールを使用する際は保守運用の責任者による承認を受けること。
3-5	アカウントの不正利用による侵害リスクを低減するため、アカウントに付与する権限を最小限とすること
3-9	特権アカウントの不正利用による侵害リスクを低減するため、特権アカウント所有者も通常業務においては利用者権限にてアクセスすること
3-10	特権アカウントの不正利用による侵害リスクを低減するため、特権の実行を制限すること ／システム利用者へ特権を付与する場合は、業務上必要な機能の実行だけを許可し、定期的な必要性の検証により、不要な特権の変更や削除を実施すること。

イ　私有 USB メモリ等の外部記録媒体への書き出しを防止する措置

お客様情報保護運用マニュアルは、①原則として、お客様情報の外部記録媒体へのデータのコピーを禁止しており、②業務上やむを得ず使用する場合は、使用する業務内容及び使用する媒体について、事前に情報管理責任者の承認を得るとともに、使用する外部記録媒体は、原則として、使用者及び使用可能端末を限定できる指紋認証機能付 USB メモリによらなければならないと定めている（第 2 編第 3 章第 1 節第 2 項）[20]。

また、「情報セキュリティ規則 ICT 編」セキュリティ対策ルールは、下表のとおり、端末に接続可能な機器を制限するルールを定めている。

しかしながら、前記第４・１⑷のとおり、実際には、X が本件不正持ち出しに用いた保守端末には、使用を許可された指紋認証機能 USB メモリ以外の外部記録媒体へのデータの書き出しを物理的又は技術的に防止する措置は講じられておらず、無断で保守端末から私有 USB メモリ等にデータを書き出すことが可能な状況であった。

[20] 他の関連規程としては、「情報セキュリティ規則一般業務編」が「USB メモリ等の小型可搬媒体は、業務上の必要性を許可された場合のみ、自社/自社グループ内で使用を許可されたものを使用すること。」と定めている（同規則 3.1.8 a.）。

番号	対策ルール
6-10A	情報漏洩リスクを低減するため、端末に接続可能な機器を制限すること
6-10B	リモートワークにおける情報漏洩リスクを低減するため、端末に接続可能な機器を制限すること

ウ　保守端末からのインターネット接続を制限する措置

「情報セキュリティ規則 ICT 編」セキュリティ対策ルールは、サイバー攻撃を念頭に置いたものではあるが、下表のとおりルールが定められている。

しかしながら、前記第４・１⑶のとおり、実際には、X が本件不正持ち出しに用いた保守端末は、インターネット接続を技術的に制限する措置が講じられておらず、ウェブメールを用いて保守端末に保存した顧客データを自由に外部に送信することが可能であった。

番号	対策ルール
2-7	サイバー攻撃による侵害リスクおよび侵害後の被害拡大リスクを低減するため、外部接続を限定すること ／システムの外部接続（インターネット、公衆網、自組織の管理外のネットワーク、など）は必要最小限とすること。

エ　ログ監視

「情報セキュリティ規則 ICT 編」セキュリティ対策ルールは、ログの監視について下表のとおりルールを定めている。

しかしながら、前記第４・１⑷のとおり、実際には、本件不正持ち出しの経路におけるログの定期的な点検は実施されていなかった。

番号	対策ルール
8-9A,B	インシデントの兆候や発生を検知し、インシデント対応を実施するため、ログを分析すること ／定期的（随時、週次、月次、など）にログを分析し、情報セキュリティインシデントの疑いがあるイベントの有無について確認すること。
10-4	保守運用行為による侵害リスクを低減するため、保守運用作業を管理すること ／システムの保守運用記録（アクセス記録、操作ログ、など）の取得内容を定め定期的に確認すること。
3-8	特権アカウントの不正利用による侵害リスクの低減や、被害発生時の分析を可能とするため、特権使用時のログへのアクセスを制限すること ／特権使用時のアクセスログおよび操作ログを取得し、当該特権使用者によるログへのアクセスを制限すること。
6-11A	情報漏洩リスクを低減あるいは情報漏洩を検知するため、端末への小型可搬媒体の接続について、定期的にログを確認すること
6-11B	リモートワークにおける情報漏洩リスクを低減あるいは情報漏洩を検知するため、端末への小型可搬媒体の接続について、定期的にログを確認すること

オ　小括

以上のとおり、BS では内部不正による情報漏洩を防止し得る管理措置を定めるルールは存在したが、X 所属グループではその多くが遵守されていなかった。

⑵　第 1 線（X 所属グループ含む VD 部）における情報セキュリティ体制の機能不全

前記⑴のとおり、いわゆる第 1 線の現場組織である X 所属グループにおいて内部不正による情報漏洩を防止し得る管理措置に係るルールの多くが遵守されておらず、そのような状況が長年是正されなかった。その原因としては、以下のような情報セキュリティ体制の機能不全があったと考えらえる。

ア　X 所属グループ

（ア）実質的な責任部署の不在

2023 年 7 月 13 日（BS 社屋に対して警察による捜索差押えが行われた日）の直前期である同年 6 月末当時、X 所属グループ内において ProCX 向けの本件システムの運用に関係する部署としては、フロント SE チーム（E 担当課長統括）、

本件システムの運用保守を担当するバック SE チーム（F 担当課長統括）、本件システムのサーバ等の構築を担当する基盤チーム（G 担当課長統括）が存在した。

しかしながら、いずれのチームの責任者も、本件システムの運用において情報セキュリティ上のルールの遵守を徹底させることを自ら又は自己のチームの具体的な業務範囲であるとは認識していなかった。

例えば、フロント SE チームを統括していた E 担当課長は、当調査委員会のヒアリングに対し、「PDS サーバのアカウント管理や保守端末からの USB メモリ等への書き出し制御などは基盤チームが指揮を取るべき事項であると認識していた」旨を述べ、バック SE チームを統括していた F 担当課長は、「本件システムの運用保守はバック SE チームの統括ではあるが、PDS サーバの作業ログのチェックが自身の業務範囲に含まれているという認識はなかった」旨を述べた。他方、基盤チームを統括していた G 担当課長は、「PDS が入っているサーバ全体は基盤チームで面倒を見ているが、PDS サーバの個別設定についてはバック SE チームが統括している」「情報セキュリティに関するリスクの特定や評価は、消去法で言えば私のチームで見るべきだったということになるかもしれないが、誰にもそのような役割が与えられていなかったのが実態」「保守端末のセキュリティについて言えば、運用を担うバック SE チームで見てほしいという意識がある」旨を述べた。

また、X 所属グループにはサービス企画を担当するチームも存在したが、同チームは本件システムの自主点検（後記(3)ア参照）を取りまとめる役割を担うにとどまっていた。

このように、X 所属グループ内には、本件システムの運用において情報セキュリティ上のルールの遵守を徹底させることを、責任を持って担う部署は実質的に存在していなかった。

（イ）内部不正による情報漏洩リスクに対する意識の希薄さ

X 所属グループでは、前記（ア）のフロント SE チーム、バック SE チームはもとより、グループ全体としても内部不正による情報漏洩リスクに対する意識は極めて低かった。

例えば、フロント SE チームを統括していた E 担当課長は、X 個人を念頭にしてではあるが、当調査委員会のヒアリングに対し、「X が顧客データを不正に持ち出すという想定は全くなかった。今でも全く信じられない。」旨を述べ、バック SE チームを統括していた F 担当課長は「本件システムは内部犯行を意識して運営されていなかった」「本件不正持ち出しが発覚するまで、内部犯行があ

るとは思ってもいなかった。運用保守業務従事者のアクセス権に関し、情報セキュリティ対策が必要という発想自体がなかった」旨述べている。

このような内部不正による情報漏洩リスクに対する認識の希薄さは、本件システムの運用状況にも現れている。前記第４・１⑴のとおり、PDS サーバのシステム管理者アカウントは、ProCX のコンタクトセンタの全顧客データをダウンロードできる特権的アカウントであるにもかかわらず、運用保守従事者の間で共用されていたが、そのこと自体が内部不正による情報漏洩リスクに対するリスク認識の希薄さを表している。そして、このようなアカウントの共有は、PDS サーバのみならず、通話録音や PBX といった本件システムを構成する他のサブシステムでも同様であり、これらの保守用アカウントも保守担当者の間で共用されていた。また、私有 USB メモリ等を端末に差し込んでデータを書き出せることは、フロント SE チーム、バック SE チームだけではなく、基盤チームでも同様の状況であった。

このような意識の低さが、本件システムの運用面において情報セキュリティ上のルールが遵守されてこなかったことの根底にある。

（ウ）業務上の便宜を優先させる意識

内部不正による情報漏洩リスクに対する意識の希薄さと表裏を成すものとして、X 所属グループでは、内部不正に対する情報セキュリティ対策よりも業務上の便宜を優先させる意識が強かった点を指摘することができる。

例えば、前記（イ）のとおり、本件システムでは、PDS サーバのシステム管理者アカウントのみならず、通話録音や PBX といった他のサブシステムのアカウントについても保守担当者の間で共用されていたが、その理由について基盤チームの G 担当課長は、当調査委員会のヒアリングに対し、「共用していた方が運用しやすく、今までそれでやっていた」旨を述べた。

もっとも、このような業務上の便宜を優先させる意識には、その背後に、そうせざるを得ない状況が存在していたことも窺われる。例えば、G 担当課長は、当調査委員会のヒアリングに対し、本件システムの実情として「自分たちで開発し、システムが止まったら自分たちで保守運用し、それに関し ProCX からの報告要請に対応する。そのような状況では、とにかくシステムを動かすことが最優先であった」旨を述べている。また、バック SE チームを統括していた F 担当課長も同様の認識を示しており、当調査委員会のヒアリングに対し、「本件システムは不具合等がよく起きるし、システムも作業もサービスの質もよくなかった。そもそも自力で手作りのサービスであり、それでなんとかなるうちはよかったが、近年は追いつかずトラブルが起きていた。とにかくトラブルを起こさない、なくさ

ないといけないということに毎日時間を費やしていた。」旨を述べている。加えて、当調査委員会のヒアリングに対し「部署内でミッションを与えられた人がいればよいと思うが、現状のミッションは事業計画で利益を上げること、そして業務を滞りなく進めることであるから、情報セキュリティは意識されないし、やっても評価もされない。ミッションがない中ではどこまでやるべきかの判断もできない。予算がつくかも分からない。」などと指摘する声もあった。これらの発言内容は偽らざる現場組織の実態を表していると言うべきであり、そのような状況が業務上の便宜を優先させる意識を正当化し、ひいては内部不正による情報漏洩リスクに対する感度を弱めていた面は否定できない。

（エ）歴史的経緯

前記（ウ）で指摘した、業務上の便宜を優先せざるを得ない状況については、本件サービスの立ち上げ時の状況及びそれ以降の歴史的経緯も関係していると考えられる。

コールセンタ業務用システム提供サービスである本件サービスは BS の前身企業において 2003 年にリリースされたが、NTT 西日本グループにおいてはコールセンタ業務用システムを内製し、これを自らで運用する実績に乏しく、そのようなサービスの立ち上げ自体に必ずしも習熟していなかった。そうした状況で、本件サービスにおける優先事項がコールセンタ業務用システムの本来的機能を滞りなく提供することに向けられ、内部不正による情報漏洩を防止する体制を充実させることは後回しにされてきた。このような歴史的経緯については当調査委員会によるヒアリングにおいて複数の者から指摘があった。例えば、「限られたリソース・期間内に各現場で作成していたため、構築時点における基盤の在り方、セキュリティに関する機能の埋め込みがそもそも担当者任せになってしまっていたのではないかと思う。」との指摘があった。また、「最低限の技術理解がないまま内製化していたことも問題点として指摘される。NTT 西日本グループではシステムを内製していないことが多く、情報セキュリティ面はベンダを頼りにしているところがある。そのような意識のまま自前でシステムを内製すると、情報セキュリティに対する意識が抜け落ちる」と指摘する声もあった。

このように見てくると、本件サービスはその立ち上げ時においてコールセンタ業務用システムの本来的機能を滞りなく提供することが最優先とされ、情報セキュリティの手当てについては現場任せになっていた一方、現場は現場で本来の担当業務に追われ、情報セキュリティを気にする余裕もなく、その結果、業務優先という名の下に情報セキュリティへの手当てがないがしろにされ、その

後大きな改善の契機がないまま今日に至った経緯があるように思われる。

このように、一定の歴史的経緯を背景に長年不備が是正されてこなかった組織においては、当該状況が望ましくないという認識があったとしても、強力なリーダーシップがなければ、これを改善することは通常困難である。その意味で、本件サービス立ち上げ時の状況及びそれ以降の歴史的経緯は、前記（ア）ないし（ウ）で指摘した事項の遠因として尾を引いている可能性は否定できないと思われる。

イ　VD 部全体（情報セキュリティに係るレポーティングライン）

BS では、NTT 西日本グループの統一的な規律に従って情報管理体制のレポーティングラインを定め、情報管理の統括者である「情報管理責任者」の下に「お客様情報適正利用監督者」を、さらにその下に「お客様情報適正利用推進者」等を置くレポーティングラインを設定している（下表参照）。VD 部においては、同部部長が情報管理責任者に、特定の部門長がお客様情報適正利用監督者に、各担当部長及び各担当課長がお客様情報適正利用推進者に、それぞれ指定されている。

しかしながら、このような VD 部内の情報セキュリティに係る管理体制のレポーティングラインが有効に機能していたとは言い難い。

一例を挙げれば、情報システムへのアクセス権限の設定は、お客様情報適正利用推進者である担当課長において行うものとされ、これについては服務指定簿による指定が行われなければならないとされていた。しかしながら、PDS サーバへのアクセス権については服務指定簿による指定は行われておらず、前記第４・１⑴のとおり、システム管理者アカウントが本件システムの運用保守業務従事者の間で事実上共用される状況が長年放置されていた。この服務指定簿の運用は、本来は、担当課長レベルで作成される月次の点検シート及び四半期ごとの点検シート（後記⑶イ参照）により、また、システムのアカウントが共有利用されていないことは四半期ごとの点検シートにより、それぞれチェックすることとされていたが、当調査委員会がこれらの点検シートをサンプルチェックしたところ、これらのチェック項目には斜線が引かれ、そもそもチェックの対象外とされていた（点検シートの問題点は後記⑶でも取り上げる。）。それにもかかわらず、点検シートの結果について報告を受けるべき特定の部門長及び VD 部部長はこうした状況について改善指示を行っていなかった。

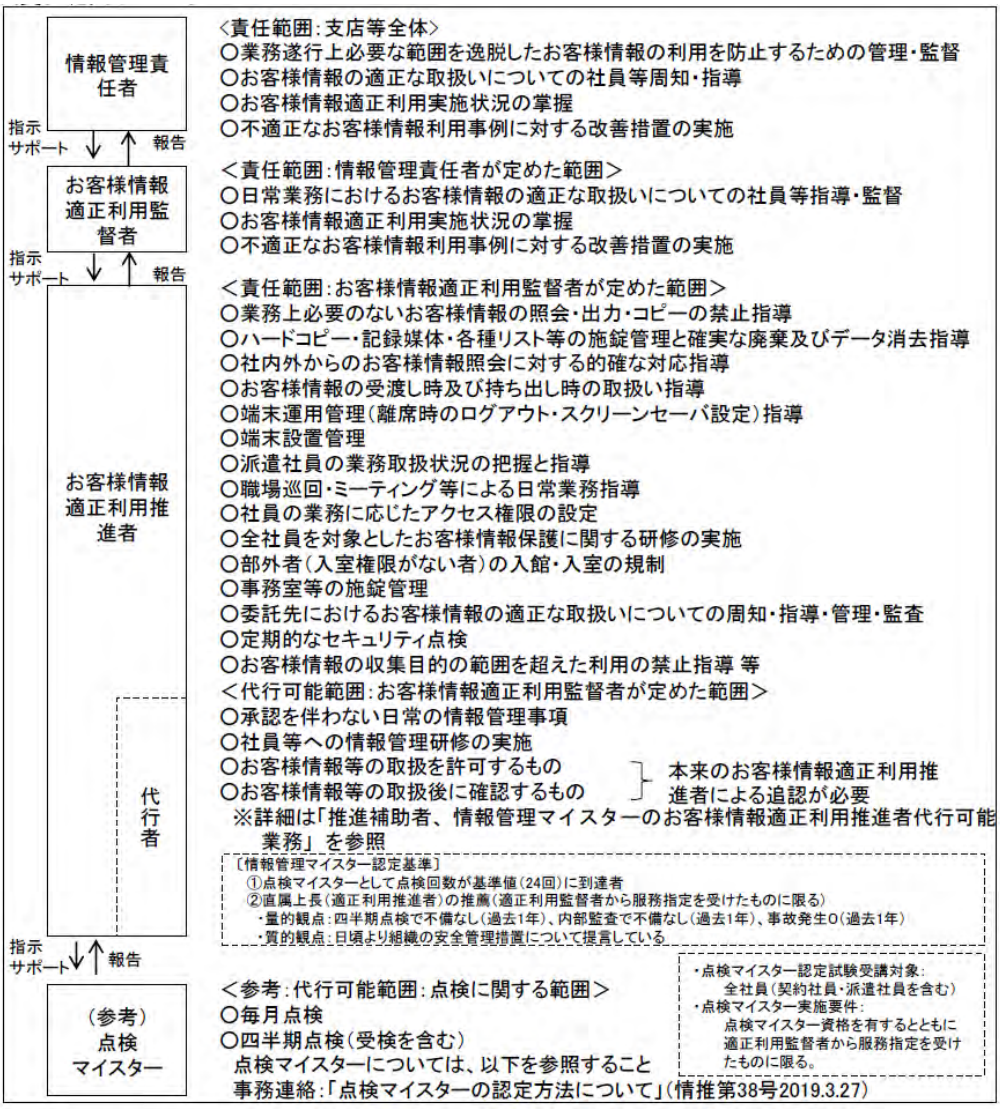
こうした状況について、VD 部の H 部長は、当調査委員会のヒアリングに対し、「誰がどの範囲の権限を特権 ID として保有するのかを誰が決めたのか分からないし、そもそも特権 ID という存在を認識できていなかった。現場管理者に近い人間でも、どこまで権限があるかを十分に認識した上で監督をできていなかったので

はないか。」と述べており、このような発言からもVD部全体としての管理体制が有効に機能していなかったことが分かる。

このような状況の背景には、X所属グループ等の現場組織が情報セキュリティ自主点検においてシステムの運用状況についての正確な情報をVD部部長に報告していなかったという事情も認められる（後記⑶ア参照）。しかし、少なくともアクセス権限の服務指定簿に関しては、システムの運用保守の部署においてそれがチェック項目の対象外であると報告されていること自体が常識的に考えてあり得ないことであるから、本来であれば、そのような報告を鵜呑みにすることなく、点検の正確性について確認すべきであったと言える。

また、情報セキュリティ自主点検にしても、VD部においては情報管理責任者であるVD部部長が点検結果を決裁するまでの過程で、X所属グループの自主的な点検で「○」とされた回答の正確性を検証したり、その根拠を確認したりする営みをしてこなかったのが実態であり（後記⑶イ）、本来であれば、こうした回答の正確性検証は、決裁者である情報管理責任者の責任においてVD部内で実施しておくべきものである。

このように、VD部内の情報セキュリティに係る管理体制（レポーティングライン）が有効に機能していたとは言い難い。情報管理責任者であるH部長においては、常に内部不正リスクを現実的なリスクとして捉え、必要な管理体制を整備しなければならなかったと言うべきである。



⑶　実態把握のための仕組みの機能不全

情報管理責任者である VD 部部長や BS の第 2 線と位置付けられるマーケティング戦略部事業推進部門が第 1 線の現場組織である X 所属グループにおける情報セキュリティ体制の運用上の不備を発見し、これを是正するためには、X 所属グループにおける情報セキュリティ体制の実態を正確に把握できなければならない。

BS では、このような実態把握のため、情報セキュリティ自主点検、毎月点検、4 半期点検等といった第 1 線の現場組織を点検者とする自主的な点検の仕組みを設けている。しかしながら、X 所属グループが本件システムについて行った自主点検の結果は本件システムの運用実態を正しく反映したものではなかった。

また、BS には、上記のような第 1 線の現場組織による自主点検の仕組み以外に、

情報セキュリティ体制の運用面での実態を把握できる仕組みは整備されていなかった。

ア　情報セキュリティ自主点検

（ア）概要

情報セキュリティ自主点検は、NTT 西日本の情報セキュリティ推進部が主導し、NTT 西日本グループ各社に指示して実施されるものであり、おおむね年に1度実施される。

情報セキュリティ自主点検はシステムごとに現場組織が行い、情報管理責任者が決裁をした上で、直接又はグループ会社の第 2 線となる情報セキュリティ担当部署を通じて、NTT 西日本の情報セキュリティ推進部に報告される。

X 所属グループでは、特定のチームが本件システムの点検結果を取りまとめていた。

（イ）不正確な点検結果

BS 及び情報セキュリティ TF では、過去に遡って、本件システムについての情報セキュリティ自主点検の結果を検証した。その結果、前記1⑴において情報セキュリティに係る規律が遵守されていないと指摘した多くの事項について、実施済み又は代替手段実施済みを意味する「○」がチェックされていたことが確認された。2021 年に実施された情報セキュリティ自主点検を例に挙げれば、以下の点検項目は実態に反していずれも「○」とされていた。

項目	チェック事項
アカウント管理及び システム管理者アカウントの権限範囲	✓　情報資産の利用に関し、利用資格の範囲の限定など適切なアクセス権限を設定した上で、個人を一意に特定する形で識別・認証を行うこと。 ✓　やむを得ず共有 ID 等を利用する際は、管理簿等を用いて、情報システム利用者を一意に特定する必要がある。
外部記録媒体への書き出し	✓　マルウェアの社内侵入や不正な情報持出しを防ぐために、会社が許可した可搬媒体以外のものをクライアント端末等に有線、無線を問わず接続させない対策（運用対処含む）を実施すること。

ログ監視	✓ インターネットに公開している情報システムについて、定期的にアクセスログを分析し、不正アクセスや、その試行を検出し、適切な対応をする必要がある。／インターネットに公開していない情報システムにおいても、重要な情報を扱うシステムについては、定期的にアクセスログ・認証ログ等を分析し、不正アクセスや情報窃取・改ざん等、その試行を検出し、適切な対応を行う必要がある。 ✓ 機密性の高い情報を扱うような重要な情報システムにおいては、情報システムの実務管理者及び運用担当者が行う操作の内容を記録しておき、定期的に操作内容の確認が行えるようにすること。

なお、情報セキュリティ自主点検では、併せて、対象となるシステムにおけるお客様情報の保有量の確認も行われているが、この点にも誤りがあり、お客様情報の保有量は「100～1 万未満」（レコード数）と正確でない数字が報告されていた。

（ウ）不正確な点検結果が報告されていた原因

前記（イ）のように不正確な点検結果が報告されていた原因には複合的な要素があったと認められる。

点検方法の実態として、X 所属グループで取りまとめを担当する特定のチームでは本件システムの運用実態を把握していないため、同チームは、適宜、分からない部分を基盤チームやバック SE チームに聞いてその結果を集約していた。このため、回答内容の正確性について相互チェックが働かず、むしろ、実質的な回答者が分散することで、回答根拠を確認しにくい状況が生まれていた。

また、それ以上に問題視すべき点として、なるべく「○」と回答する方向でのバイアスがあったことが指摘できる。この点について、X 所属グループで取りまとめに関与した者にヒアリングしたところ、各チームからの回答を集約する過程で、「×」回答については回答者にその理由を確認していたが、「○」回答についてはその根拠を確認することはなかったとのことである。点検の趣旨からすれば、むしろ、「○」との回答こそ根拠を含め確認すべきである。しかし、実際にはこれと逆の運用になっていたというのであり、このことは、なるべく「○」と回答する方向でのバイアスがあったことを示唆している。このヒアリング対象者は、そのような運用をしていた理由として、「○という回答が欲しいのだろ

うと感じていた」旨を述べたほか、「現場において×部分を改善するために時間を要したとしても、それが理由で業績が下がることは許されない。改善に人・金・時間をまわすと当然、業績に影響はあるが、全て現場の責任。」「仮に×とつけた場合に、○にすることのタスクが重すぎる。改善は全て現場でやってね、となるが、お金もつかないし、知識もない。」旨も述べた。基盤チームで回答に関与した者も、なるべく「○」と回答する方向でのバイアスがあったことを指摘しており、当調査委員会のヒアリングに対し「意識として、○にしないといけないという考えがあった。そのような風潮を感じたので、よくなかったとは思うが特に疑問を感じずにそれに倣っていた」旨述べた。このほかに、一部でも「○」という状況にあれば、その他の部分に「×」とすべきものが含まれていても「○」と回答していたパターンもあった模様である。

このように、なるべく「○」と回答する方向でのバイアスがあったことが回答結果を歪めていた面があることは否定できない。そして、このようなバイアスは、「×」とすることで面倒を引き受けることを避けたいという風潮があったことを示しているというだけではなく、X 所属グループにおいて情報セキュリティ体制を充実させることの優先順位が極めて低かったことを物語っている。

このほか、不正確な点検結果が報告されていた原因として、チェック項目の趣旨に対する誤解や、回答時に本件システムのどの部分を念頭に置くかという点について認識共有がなされていない状況（本件システムは、PDS サーバを含む複数のサブシステムから構成されており、どの部分を念頭に置くかによって回答が異なり得る）等を指摘する声もあった。

イ　毎月点検、四半期点検

BS では、お客様情報保護運用マニュアルに基づき、お客様情報を取り扱う情報システム端末設置部署等を対象として、お客様情報の日常レベルの管理状況を自主点検する仕組みとして、お客様情報適正利用推進者（担当部長、担当課長）を主体とする毎月点検及び四半期点検を実施している。

これらの点検はもともとお客様情報の日常レベルの管理状況の点検を主眼としており、システムの運用状況の確認を主目的とするものではないが、点検項目の一部にはシステムの運用に関する項目が存在している。例えば、前記１⑴の不備事項との関係では、毎月点検及び四半期点検には、①システムへのアクセス権について服務指定簿の存在を前提とした点検項目がある。また、②四半期点検にはログ監視に関連し得るものとして「お客様情報（他事業者情報を含む）の取り扱い端末について、業務目的と関係の無い操作が行われていないか確認」という点検項目がある。

当調査委員会が本件システムのフロント SE チーム及びバック SE の 2022 年以

降の毎月点検及び四半期点検の結果を確認したところ、これらすべての点検において全項目が「○」又は斜線となっており、前記１⑴の不備事項との関係では①の点検項目には前記⑵イのとおり斜線が引かれ、②の点検項目は「○」とされていた。

しかしながら、前記１⑴及び前記⑵イのとおり、①②の点検結果は少なくともPDS サーバの運用保守の実態として正確な回答ではない。

ウ　鵜呑みの連鎖

VD 部においては、情報管理責任者である VD 部部長が点検結果を決裁等するまでの過程で、現場組織が「○」と回答したことの正確性を検証したり、その根拠を確認したりする営みは事実上存在していなかった。また、第 2 線であるマーケティング戦略部事業推進部門においては、第 1 線である現業部門の情報管理責任者が決裁した結果を、明らかにおかしい点がない限り、基本的にそのまま受け入れていた。

加えて、BS には、前記ア及びイの自主点検以外に、運用面での情報セキュリティ体制の実態を把握する有効な手段が存在していなかった。

このようにして、第 1 線の現場組織である X 所属グループが取りまとめた不正確な点検結果についての鵜呑みの連鎖が生じ、これが本件システムの情報セキュリティ体制の運用面での実態の把握を難しくし、前記⑴の不備状況が長年是正されなかった原因の一部を形成していると認められる。

⑷　第 2 線の脆弱性

ア　マーケティング戦略部事業推進部門の第 2 線としての機能の不全

BS において、全社的な情報セキュリティ体制を所管していたのはマーケティング戦略部事業推進部門である。同部は BS 内のいわゆる第 2 線を担う管理部門として位置付けられることから、本来的には、第 1 線である現業部門が情報セキュリティについて遵守すべき事項を遵守しているかをモニタリングし、これを監督することで第 1 線に対する牽制機能を果たすとともに、第 1 線に対して必要な支援を提供することが期待されていると言える。

しかしながら、情報セキュリティに係る規律が遵守されていない状況（前記⑴）、第 1 線内における情報セキュリティ体制の機能不全（前記⑵）、情報セキュリティ体制の実態を把握する仕組みの機能不全（前記⑶）が見過ごされてきたこと等を踏まえると、マーケティング戦略部事業推進部門による第 1 線に対する牽制機能は機能不全に陥っていたと評価せざるを得ない。

イ　原因の考察

このような機能不全が生じた主要な原因としては、次の点を指摘できる。

（ア）第1線の現場組織の実態を独自にモニタリングする手段を持たないこと

前記⑶ウのとおり、BSでは、X所属グループ等の第1線の現場組織における内部不正に対する情報セキュリティ体制の運用面での実態を把握する手段を、現場組織が実施する自主的な点検結果に依存していた。その結果、現場組織が実施する自主的な点検結果及び現業部門における決裁結果を第2線において鵜呑みにせざるを得ない状況が発生していた。

このような状況では、業務優先に偏るおそれが常にある第1線に対して独立した立場から有効な牽制を行うという、第2線に期待される役割を果たすことができない。

（イ）組織設計上の問題

前記（ア）のように、マーケティング戦略部事業推進部門が第1線の実態を独自にモニタリングする手段を持たなかったのは、NTT西日本の情報セキュリティ推進部との役割分担を含む組織設計上の問題に由来すると考えられる。

マーケティング戦略部事業推進部門において情報セキュリティに関する業務を担当するのは、事業推進担当・情報システムグループ及び財務法務担当・業務品質グループであるが、両グループの実際の所掌分担を確認したところ、両グループとも、第1線に対して必要な牽制機能という役割を果たすための業務が具体化されておらず、その実務担当者の割当ても存在していなかった。

現業部門による自主点検との関係では、事業推進担当・情報システムグループはNTT西日本の情報セキュリティ推進部からの指示を受け、各部にこれを展開する役割を担い、年度によっては各部の点検結果を取りまとめ、NTT西日本・情報セキュリティ推進部に送付していた。他方、財務法務担当・業務品質グループはお客様情報の取扱いについての各部の自主点検（毎月点検、四半期点検等）を取りまとめ、NTT西日本の情報セキュリティ推進部に送付する役割を担っていた[21]。しかしながら、両グループとも、NTT西日本の情報セキュリティ推進部とBS内の各現業部門との間に入り、両者間の指示又は報告を中継する役割を担

[21] ただし、2023年度からは、取りまとめ方法がシステム化され、点検結果は情報管理責任者からNTT西日本・情報セキュリティ推進部に直接報告されるようになっている。

っているにとどまり、第 1 線による自主点検で問題なしと報告された結果の正確性を独自に検証することを自らの業務として行ってはいなかった。

このように、マーケティング戦略部事業推進部門は、実態として、第 1 線である現業部門が情報セキュリティ上のルールを遵守しているかをモニタリングし、第 1 線に対して必要な牽制機能を果たすという、本来第 2 線として担うことが期待される役割を果たしていなかった。

そして、実際問題としても、同部門の事業推進担当・情報システムグループ及び財務法務担当・業務品質グループとも、複数の業務を抱えながらそれぞれ 6 名程度の人員で稼働しており、現状の配置人員だけで上記のような役割を果たすことは事実上困難であった。

これは、マーケティング戦略部事業推進部門のみに帰されるべき問題ではなく、BS における組織設計上の問題である。

このような状況が生じた背景には、BS のマーケティング戦略部事業推進部門と NTT 西日本の情報セキュリティ推進部との間の役割分担について、両者の間に認識の相違があった可能性も窺われる。当調査委員会がヒアリングした BS のマーケティング戦略部事業推進部門の者からは「当部門は 2 線というよりも現場に近い 1 線の取りまとめ役というイメージでいる。NTT 西日本グループ全体の 2 線として位置付けられるのは NTT 西日本の情報セキュリティ推進部であり、当部門としては事実上この機能を担っていない。また、当部の現状の人員リソースでは 2 線として期待される機能を果たすことは難しい」旨の指摘があった。他方、当調査委員会がヒアリングした NTT 西日本の情報セキュリティ推進部の者は「同部では、BS を含む各社の情報管理責任者が情報セキュリティ自主点検を承諾していることまでしか確認していない」旨を述べた。このように、第 2 線としての役割をいずれが果たすべきかという点についての役割分担が明確でなく、両部の間に認識の相違があった可能性がある。

NTT 西日本の情報セキュリティ推進部との役割分担を含む組織設計上の問題を解決するためには、NTT 西日本と BS との間で第 2 線としての機能を担う部署を明確化する必要があるとともに、仮にこれを BS のマーケティング戦略部事業推進部門の役割分担とする場合には、そのために必要な人的リソースの割当てを併せて検討する必要がある。

⑸　内部不正による情報漏洩リスクに対する危機意識の弱さ

X 所属グループを含む VD 部全体として、内部不正による情報漏洩リスクに対する意識が希薄であったことは、前記⑵ア（イ）及び前記⑵イで指摘したとおりである。

第 2 線であるマーケティング戦略部事業推進部門においては、内部不正による情

報漏洩リスクに対する意識が希薄であるとまでは認められなかったが、同部門の者にヒアリングをしたところ、「同部門における情報セキュリティ上のリスクに対する関心は、内部不正ではなくサイバー攻撃への対処という面に焦点が向けられていた」とのことであり、「悪いことをしないのは当たり前という固定観念もあった」とのことである。内部不正による情報漏洩リスクも重大なセキュリティ上のリスクのひとつであることからすると、マーケティング戦略部事業推進部門の意識も、その求められる役割との対比では、やはり弱かったと言わざるを得ない。

⑹　情報セキュリティ上のリスクに対するリスクマネジメントプロセスの不存在

前記⑴ないし前記⑷は、主として、NTT 西日本グループ管理規程で定められた技術的な管理措置の不備並びに当該不備に係る第 1 線及び第 2 線の機能不全に焦点を当てていたが、これらは、より広い文脈で捉えれば、情報セキュリティ上のリスクに対するリスクマネジメントの問題であると言える。

しかしながら、第 1 線である X 所属グループを含む VD 部にも、第 2 線であるマーケティング戦略部事業推進部門にも情報セキュリティ上のリスクを特定、評価し、そのリスクのあり様に応じてリスク低減措置等の対応策を策定し、実行していくというリスクマネジメントプロセス自体が存在していなかった。

すなわち、X 所属グループについて本件システムのログの監視の点を取り上げれば、ログといっても本件システムには多数のログが存在するのであるから、その中から内部不正リスクのコントロールという目的に適合したログを的確に選定し、具体的なログ監視の手順を確立しなければならない。そのためにはまず、本件システムのどの部分でお客様情報等の重要情報を保持しているのか、当該情報の量及び重要性はどのようなものであるか、当該情報の想定流出経路はどこか、作業者の作業環境はどのようなものかといった複合的な視点から、内部不正のリスクを具体的に特定、評価する必要がある。その上で、当該リスクに対してシステム面でのリスク低減措置は講じられているのか、運用面で手当てが必要ならば、どのような方法で行えばそのリスクの大きさと業務効率性とのバランスを保つことができるかといったことを考慮しながら、具体的なリスク低減措置として、ログ監視の対象や手順等を策定する必要がある。そして、このようなリスクマネジメントのプロセスは一度きりではなく、状況の変化を取り込みながら、繰り返しその有効性の検証を重ねていく必要がある。しかしながら、X 所属グループ内では上記のようなリスクマネジメントプロセスの営みは行われていなかった。

第 2 線も同様である。BS の全社的な情報セキュリティ体制を確かなものにするためには、第 2 線と位置付けられるマーケティング戦略部事業推進部門において、NTT 西日本グループ管理規程で定められた規律を第 1 線に遵守させるだけではなく、BS

全体でどのような情報システムが存在し、それぞれどのような性質の情報を保持しているのかといった情報を前提に、情報セキュリティ上のリスクを構成する多様なリスク（サイバー攻撃のリスクや内部不正リスクはそのような多様なリスクのうちの一部である）の中から対処すべき優先順位の高いリスクを特定し、当該リスクを念頭においてそれに対処するための方針を策定した上、これを実行していくために必要となるリソースの配分を行う必要がある。しかしながら、BS の第 2 線であるマーケティング戦略部事業推進部門ではそのようなリスクマネジメントプロセスの営みは行われていなかった。

このような情報セキュリティ上のリスクマネジメントプロセスが確立できなければ、本件不正持ち出しとは別種のリスクが顕在化した場合に対処できない可能性が高い。したがって、本件不正持ち出しに応じた対応としては、単に不備が確認された事項を改善するだけではなく、より広く、リスクマネジメントの在り方が問われていることを理解する必要がある。

⑺　人員配置等の人事に関する問題

ア　情報セキュリティに知見を有する人材の不足

これまで指摘した BS の問題点を俯瞰すると、BS の全社的な問題として、情報セキュリティに知見を有する人材が不足している点が挙げられる。この点は、当調査委員会のヒアリングにおいても多数の者から指摘があった。

イ　特定の者への依存とその固定化

前記第４・２⑵のとおり、ProCX 向け PDS サーバの運用保守及びサポート業務は X 個人に依存する状況が長年固定化しており、このことが内部不正による情報漏洩リスクを高める大きな要因となっていた。

X は、もともと NTT 西日本グループにはない技術を利用したシステムを構築するに当たり、その知見を有するエンジニアとして派遣を受けることになった経緯がある。その後、X は PDS についての数少ない有スキル者として、BS 及びその前身企業において頼りにされ、ProCX の担当者からも信頼を得ていくようになった。一方、PDS は、緻密なカスタマイズが可能であるという特徴があり、その操作方法を熟知するには相応の時間を費やす必要があったが、コールセンタ業界において次々と新たな形態・種類のシステムが生み出されていく近年の状況において、BS 内部において新しく PDS の有スキル者を教育するという動きは見られなかった。その結果、PDS サーバに関する作業が X に集中し、その結果として PDS

に関する知見が同氏に集まるために、ますますPDSサーバに関する作業がXに集中し、固定化されていくという自己強化型のフィードバックループが発生していたと考えられる。

当調査委員会がヒアリングしたところ、上記のような状況はXのみではないとの指摘が複数見られた。例えば、「X所属グループは組織ではなく個人に頼る体制だった」であるとか、「X所属グループには、普段仕事をする上で、運用を整理したドキュメントに乏しく、そのため、古くからいる者に対し属人的に依存してしまっている面がある」、「VD部でも多くの派遣社員がいるが、正社員は定期的に異動がある一方、派遣社員は業務が固定されがちである。また、正社員では技術的に対応できないこともある。そうすると、派遣社員だけが詳しくなっていき、どんどん外せなくなっていく」などと指摘する声があった。

ウ　待遇への不満が存在していた可能性

前記第３・５のとおり、本件不正持ち出しには、持ち出した顧客情報を名簿業者に売却することで利益を得る目的が含まれており、Xが賃金その他の待遇について不満を抱いていた可能性は否定できない。Xの想定手取り額は年齢及び社員グレードをベースにした比較ではBSの正社員に比べて著しく乖離しているわけではなかったが、自らへの処遇がPDSの有スキル者としての貢献に対して釣り合わないと感じていた可能性はある。

後記第８の本アンケート調査においても、「契約社員・派遣社員に社員と同等かそれ以上の仕事内容・成果を求め、にもかかわらず処遇に格差があることが今回の件の遠因にあるように思います。」と指摘するものがあった。

これと同様の構図は、派遣社員のみならず、下請け又は業務委託先の従業員が事実上BS内の組織に組み込まれているケースでも顕在化し得る。

エ　派遣社員の監督状況

前記第４・２⑵のとおり、本件不正持ち出しに関しては、Xの業務の特殊性という面も相まって、上長等によるXに対する監督はほとんど実効的に機能していなかった。

この点、BSでは派遣社員の監督に関する規律[22]を定めており、これによれば「派遣労働者等がお客様情報を取り扱う場合は、従事の期間、その業務の難易度にかかわらず、常にグループリーダの管理監督下で業務に従事させる。」「社員が派遣労働者等の処理状況を見渡せる環境下で業務に従事させる。」「指揮命令者（課長等）自

[22] 「お客様情報保護運用マニュアル」

らが職場巡回し、所定の業務に従事しているか把握する。」「派遣労働者等への端末操作の指導に当たっては、真に業務に必要な範囲に限定した知識・操作方法の指導を行う。」等の対応が必要とされている。

X に対する監督状況はこれらの規律自体にも反するものであり、それ自体問題視されるべきである。

前記イのとおり、X 以外のケースでも特定の派遣社員への依存とその固定化が少なからず存在していることからすると、X 以外にも同様に派遣社員に対する実効的な監督ができていないケースが存在する可能性がある。

オ　情報セキュリティの重視に向けた動機付けが弱いこと

前記１⑵ア（ウ）のとおり、X 所属グループにおいて内部不正による情報漏洩リスクよりも業務上の便宜を優先させる意識が強くなっていたと認められるが、その背景には、前記１⑵ア（ウ）で指摘したとおり、情報セキュリティ体制に関する不備を指摘したり、その是正に取り組んだりしても、そのことが自己の人事上の評価に繋がらないという認識があったものと考えらえる。例えば、「ISMS 対応業務をしていた際に、情報セキュリティを踏まえた意見を言ったことがあるが、『それをすると開発が遅くなる』といった反応が返ってくる。新サービスを開発することは評価される一方で、情報セキュリティを強化する提案をしてもそれが自己の仕事の評価につながることがない」などという声もあった。

このような人事評価の在り方が、個々の従業員から情報セキュリティ体制の不備を是正していく意欲を削ぎ、情報セキュリティの重視に向けた動機付けを弱めていた可能性があることも問題点として認識されるべきである。

⑻　内部監査について

BS に対する内部監査は、BS 内の内部監査部門と NTT 西日本の内部監査部門である内部監査部が、監査対象となる部署を区分するなどして連携して実施している。VD 部に対する内部監査については、近年は主に NTT 西日本の内部監査部が担当していた。

同部は事前情報（例えば、リスク評価の資料として、お客様情報の取扱量、直近の不備事例の有無、業績傾向等を用いている）に基づきリスクベースでサンプルチェックの対象を決定しているところ、過去 10 年間は VD 部の X 所属グループはサンプルチェックの対象として選定されていなかった。

内部監査部門のリソースにも限界があることを踏まえれば、内部監査部門がリスクベースアプローチを採用すること自体は特段不合理ではなく、X 所属グループが

サンプルチェック対象から長年外れていたというだけで内部監査に落ち度があったとまでは言えない。

もっとも、NTT 西日本の内部監査部による監査は、管理簿に責任者のサインがあるかといった外形的なチェックにとどまっており、第 2 線による第 1 線に対する監督機能が有効に機能しているかを深堀りして監査するところまではできていなかった。このような深堀りした監査を実施していれば、BS における情報セキュリティ体制の運用面が各所で機能不全に陥っていたという実態を早期に把握できた可能性はあるから、この点は今後の課題として認識すべき事項であると言える。

なお、内部監査の対象決定におけるリスクベース判断の前提となる情報（例えば、お客様情報の取扱量）に誤りがある場合にはその判断を適切に行うことが困難になるが、NTT 西日本の内部監査部は、本件システムにおけるお客様情報の取扱量については第 1 線が第 2 線に報告した不正確な情報に基づき不正確な認識をしていた。第 2 線による第 1 線に対する監督機能の有効性を確認できていない状況においては、リスクベース判断の前提として第 1 線又は第 2 線から提供を受けた情報自体が正確でない可能性にも配意しておくべきであったと言え、この点も併せて課題として認識すべきである。

⑼　経営陣の責任

これまで指摘した問題点には、第 1 線、第 2 線及び第 3 線（内部監査部門）の在り方、人員リソース及び予算割当て、人事評価、NTT 西日本との役割分担など経営レベルでの解決を要する事項が多数含まれており、これらは BS の全社的問題である。したがって、本件不正持ち出しの発生を許し、警察による捜索を受けるまで 10 年間にわたりこれを発見することができなかったことは、現場組織である X 所属グループや同グループが属する VD 部のみの問題ではなく、究極的には、BS の経営陣にその責任が帰せられるべき問題である。

BS の経営陣がこれほどまでに自社の情報セキュリティ体制に綻びが生じていたことに対して、これまで何ら有効な改善措置を講じていなかったことは、現場組織から吸い上げられる報告が必ずしも正確ではなかったことを考慮してもなお致命的な怠慢であると言うほかない。

BS の主要な事業の一つであるコールセンタ業務用システム提供サービスは、そのシステム構成等の細部がどうであったとしても、何らかの形で大量の個人情報に接することになる。したがって、BS の経営陣としては、このような大量の個人情報を取り扱うシステムにおける内部不正その他の情報漏洩リスクを、日頃から、経営上の重大なリスク要因と位置づけ、下からの問題報告を待つまでもなく、主導性を発揮して、不備の発見と是正に向け陣頭指揮を執るべきであった。しかしながら、前記⑹の

とおり BS には情報セキュリティ上のリスクマネジメントのプロセス自体が存在すらしておらず、BS の経営陣自らがそうした状況の改善に向け主導性を持って取り組んだ事実もなかった。BS の経営陣にはリスクマネジメントに対する基本的な理解やこれを実際の経営に適用する能力が欠けていたとさえ言い得る。

X による本件不正持ち出しは BS における内部不正による情報漏洩リスクが顕在化したものであり、かかるリスクへの対処を怠ってきたという意味で、BS の経営陣の責任は殊に重い。

⑽　度重なる組織再編の影響

BS は、前記第２・２のとおり、度重なる組織再編を重ねて今日に至っている。このことが本件システムの情報セキュリティ面での運用実態の把握を難しくしている面があったとも考えられる。実際、当調査委員会のヒアリングに対し「組織が変わりすぎて、どうやって各システムができたのかといった事情を把握することが困難である」、「体制の見直しが多く、前任者が担当していた業務にどのような経緯があり、どのような注意点があるか等の運用の引継ぎが十分でない」などの指摘があった。

2　ProCX について

⑴　委託先管理に係る規律が遵守されていない状況

ア　規律が遵守されていない状況

ProCX は、NTT 西日本が NTT 西日本グループの統一的な基準として策定した「情報セキュリティマネジメント規程」を自社の規程として定めた上で、その下位規程を整備している。その一つに「個人情報・特定個人情報保護外部委託管理規程」がある。個人情報・特定個人情報保護外部委託管理規程は、個人情報を取扱う業務の全部又は一部の委託に関し、下表のような措置を講じなければならないとしている。

①　「個人情報業務委託会社調査表」（様式１）に基づく調査
②　業務委託契約には、次の事項を織り込むこと
(1)　責任の明確化に関する事項
(2)　個人情報の安全管理及び機密保持に関する事項
(3)　再委託に関する事項
(4)　個人情報の取扱い状況に関する委託元への報告の内容及び頻度

(5) 契約内容が遵守されていることを、定期的に、及び適宜に確認できる事項
(6) 契約内容が遵守されなかった場合の措置
(7) セキュリティ事件・事故が発生した場合の報告・連絡、委託先の責任に関する事項
(8) 契約終了後の措置
③ 委託先企業から「業務委託に伴う情報管理責任者等通知書」（様式５）の報告を受け、情報管理責任者等の責任体制について確認する
④ 電子媒体で個人情報リストを預ける場合、「個人情報・特定個人情報リスト原本受渡書」（様式６）により、リスト授受の記録を残さなければならない。
⑤実行責任者又は個人情報取扱者は、必要に応じて委託先の事務所への立入検査を実施し、委託先の個人情報・特定個人情報の管理状況を確認する。

しかしながら、ProCX は、上記事項のうち、契約条項の一部を除くすべての事項を遵守しておらず、個人情報の取扱いに関する限り、BS に対する委託先管理は実態として何もしていないに等しい状況であった。

イ　規律が遵守されていなかった原因

委託先管理に係る規律が遵守されていなかった原因は、直接的には、ProCX の担当者において、BS に対し個人情報の取扱いを委託しているとの認識がなかったことが挙げられるが、ProCX においては、そもそも規律はありながらも、委託先をどのように監督するかの実務フローが確立しておらず、また、個人情報の取扱いを委託している否かについて担当者の判断の当否をチェックしたり、審査したりする運用も存在していなかった。

このように、ProCX においては、個人情報の取扱いを委託するに当たっての規律が何ら実務的に実装されていなかった。このことが ProCX において BS に対する委託先管理が行われていなかった最大の原因であると考えられる。

⑵　顧客情報の漏洩に対する危機意識の乏しさ

前記⑴では、個人情報の取扱いに係る ProCX 内の規律との関係に焦点を当てたが、そのような規律の有無にかかわらず、ProCX はアウトバウンドテレマーケティング業務等を受託するに当たり、その委託元から大量の顧客情報の提供を受けているのであるから、本来、その取扱いには細心の注意が払われなければならなかった。

それにもかかわらず、前記⑴のような実態であったということは、ProCX 全体として、提供を受けた顧客情報が漏洩することにより、本件不正持ち出しのような深刻な事態が生じることへの危機意識が乏しかったと言わざるを得ない。

⑶　内部不正による情報漏洩リスクに対する情報セキュリティ体制の脆弱性

本件不正持ち出しとの関係における ProCX 側の主要な原因は前記⑴のとおりであるが、広く内部不正による情報漏洩に対する防止措置という観点では、後記第７・３のとおり、ProCX における緊急点検の結果、多数の不備事項が確認された。

そこで、当調査委員会は、ProCX において緊急点検の対応をした CX ソリューション部担当者及び ProCX における第 2 線と位置付けられる事業推進部総括担当との間で内部不正に対する情報セキュリティ体制についての認識共有のためのヒアリングを行った。その結果、BS と同様の問題として、①実態把握のための仕組みの機能不全、②第 2 線の脆弱性（担当者 1 名）、③内部不正による情報漏洩リスクに対する意識の希薄さ、④情報セキュリティ上のリスクに対するリスクマネジメントプロセスの不存在、⑤情報セキュリティに知見を有する人材の不足等があることを確認した。

⑷　ProCX と BS の関係性に由来する問題

ProCX と BS とは、2021 年の組織再編により、ProCX が BS からコールセンタ事業の営業部門を承継した経緯があり、もともと近い関係にあった。また、後記第６・４⑴のとおり、ProCX の代表取締役社長（以下「ProCX 社長」という。）及び同社の CX ソリューション部担当部長である C 担当部長は、いずれも BS の役職を兼務していた時期があった。

ProCX 社長はこのような関係性にある両社について「ProCX と BS の境目はぐちゃぐちゃ」と表現しており、現場レベルの感覚としては、委託元・委託先という明確な立場の相違がなかったものと考えられる。このような関係性が ProCX において委託先である BS に対する管理が疎かになった遠因を成している可能性は否定できない。

３　NTT 西日本について

⑴　内部不正リスクへの対応状況

情報セキュリティに関し、NTT 西日本グループ全体の第 2 線の機能を果たすのは NTT 西日本・情報セキュリティ推進部である。

同部では内部不正による情報漏洩リスクを情報セキュリティ上の主要なリスク要因として位置付けていた。しかしながら、当該リスクについて必ずしも具体的なリス

ク評価ができていたわけではなく、情報セキュリティ自主点検ではおおむね不備事項なしとの結果が報告されていたこともあり、内部不正による情報漏洩リスクは相対的にリスクが低いと受け止めていた。このような認識を前提に、NTT 西日本・情報セキュリティ推進部は、近年は、サイバー攻撃やマルウェア感染防止といったリスク要因を重視し、そのための対策の強化に注力しており、グループ各社への内部不正による情報漏洩に対する対策強化の指示やそのための支援は必ずしも重視していなかった。

⑵　情報セキュリティ自主点検の取扱い

情報セキュリティ自主点検は、NTT 西日本・情報セキュリティ推進部がグループ各社に指示して実施していた。しかしながら、同部では、特に不備事項の報告がなければ、基本的に、情報管理責任者の決裁を経ていることを確認するにとどまり、不備なしとされた事項についてその回答の正確性を独自に検証したり、その根拠を自ら確認したりする運用はしていなかった。

また、同部は、上記各社の自主的な点検結果以外に、グループ各社の内部不正による情報漏洩リスクに対する情報セキュリティ体制の実態を把握する有効な手段を持っていなかった。

その結果、NTT 西日本・情報セキュリティ推進部においてもグループ各社の第 1 線の現場組織の回答に対する鵜呑みの連鎖が発生していた。

⑶　グループ各社の第 2 線との役割分担

前記 1⑷イ（イ）でも指摘したとおり、BS その他のグループ各社にそれぞれ第 2 線の管理部門が存在する一方で、NTT 西日本グループ全体の第 2 線として NTT 西日本・情報セキュリティ推進部が存在するという二重構造の中で、グループ各社の第 2 線と NTT 西日本・情報セキュリティ推進部との間の役割分担に認識の相違が生じていた可能性がある。

後記 7 のとおり、グループ各社の緊急点検の結果、情報セキュリティ上の不備事項が多数確認されていることからすれば、この問題は、BS 及び ProCX だけではなく、NTT 西日本グループ全体における組織設計の問題であると位置付けられる。そして、BS 及び ProCX における第 2 線の人員の少なさに鑑みると、この問題の背景には、建前では第 1 線に対するグループ会社の第 2 線の実効的な監督が期待される一方で、実際にはそのために必要な人的リソースを配分できていないという状況が存在すると考えられる。

NTT 西日本グループ全体の人事施策は基本的には NTT 西日本が担っており、グ

ループ各社が独自の人事施策を行う余地は乏しいことから、このような状況をグループ各社が独自に解決することは困難である。他方で、NTT 西日本・情報セキュリティ推進部の人員構成にも余裕があるわけでもない。

したがって、この問題を解決するためには、併せて、NTT 西日本グループ全体として情報セキュリティに知見を持つ人的リソースの拡充及び配分の最適化を図っていく必要がある。

⑷　グループ全体での経営資源の配分の歪み

ア　人事施策全般について

前記⑶では、情報セキュリティに知見を持つ人的リソースの配分に言及したが、本アンケート調査（後記第８参照）においても、NTT 西日本グループ全体での人員の削減とこれによる人員の不足を派遣社員等の外部リソースで手当てしている状況について問題点を指摘する声が多数あり、例えば、「業務 DX が進んでいないのに、人員は減少し、定期的な異動があるなかで業務を維持するためには業務委託や派遣社員等の外部リソースに頼らざるを得ず、ほぼ丸投げ状態で社員が実務を把握できていない傾向にある」などと指摘する声があった。

こうした歪みは、第 1 の現場組織においてルールを遵守することを困難にさせるおそれがある。実際、前記第５・１⑵ア（ウ）及び（エ）のとおり、BS の X 所属グループにおいては、情報セキュリティ上のルールが遵守されていなかった背景として、本来所掌している業務に手一杯となり情報セキュリティにまで手が回らなかったという状況が確認されている。

NTT 西日本グループ全体の人事施策全般について踏み込んだ検討を行うことは当調査委員会の任務を超えるが、本件不正持ち出しの発覚を契機として、NTT 西日本グループ全体として抜本的な是正措置を講じるのであれば、上記問題提起も踏まえた見直しを行う必要があるとはいえるだろう。

イ　予算配分について

本件不正持ち出しに関する当調査委員会のヒアリングや本アンケート調査（後記第８参照）においては、予算上の制約により情報セキュリティ体制の抜本的な解決が図れないとの指摘も聞かれた。

NTT 西日本グループ全体の予算配分のあり方について踏み込んだ検討を行うことは当調査委員会の任務を超えるが、少なくとも、本件不正持ち出しの発覚を契機として、グループ各社に対して一定の対策を講じさせるのであれば、そのために必

要な予算措置が併せて講じられなければならないことは言うまでもない。

第６　本件過去調査の検証

１　本件過去調査の概要及びこれを調査対象とする必要性

⑴　本件過去調査の概要

ProCX は、2022 年 4 月 4 日、ProCX が提供するテレマーケティング業務の委託元の一つである A 社から、A 社が ProCX に提供した顧客情報が漏洩した疑いがあるとして調査を依頼された（以下「本件調査依頼」という。）。当該依頼を受けて、ProCX 及び BS の担当者 4 名（以下「本件調査担当者ら」という。）は、A 社からの質問や要望に都度対応する形で、2022 年 4 月から同年 7 月にかけて本件過去調査を実施した[23]。実際には、本件過去調査の時点で X による本件不正持ち出しが 9 年以上にわたって行われていたにもかかわらず、本件過去調査において、本件調査担当者らは、A 社に対して、内部からの顧客情報の流出は確認されなかった旨の報告を行った。

⑵　発覚後社内調査の経過及び本件過去調査を当調査委員会の調査対象とする必要性

NTT 西日本、ProCX 及び BS は、2023 年 7 月に本件不正持ち出しが発覚したことを踏まえて、本件過去調査に関する社内調査を行った。その結果、本件過去調査の過程で A 社に提出されたエクスポートログは本件調査担当者らの一部によって改変されたものであったこと、A 社に対する回答の中に事実とは異なる回答が複数含まれていたことを確認した。NTT 西日本、ProCX 及び BS は、本件調査担当者らが内部からの情報流出を認識しつつ積極的かつ意図的にこれを隠蔽しようとしたのではないかという問題意識を持ち、2023 年 7 月から同年 10 月にかけて、本件調査担当者らに対するヒアリングを中心とした発覚後社内調査を実施したが、各人の記憶が曖昧であったり、各人の供述内容に食い違いがみられたりする等したため、事態の完全な解明には至らなかった。

当調査委員会においても、本件過去調査において本件調査担当者らの一部がエクスポートログを改変していたこと及び事実と異なる回答をしていた点を非常に重大に受け止め、発覚後社内調査と同様、本件調査担当者らが内部からの情報流出を認識しつつ積極的かつ意図的にこれを隠蔽しようとしたのではないかという観点から、重ねて本件過去調査の検証を行うこととした。加えて、当調査委員会は、本件過去調

[23] なお、当調査委員会では、上記期間のほか、2023 年 6 月から 7 月にかけても、A 社から PDS サーバ等に関する質問が寄せられ、ProCX 及び BS が回答をした事実を確認している。しかし、当該期間におけるやり取りは、本件過去調査の約 1 年後かつ本件不正持ち出しについて警察による捜索差押えがなされる直前時期になされたものであるほか、本件過去調査に従事した者以外の従業員も回答に携わっており、本件過去調査とはその位置付けを異にすることから、当調査委員会による検証対象には含めないこととした。

査の経過及びその適切性について分析・評価することは、本件過去調査当時の ProCX 及び BS、ひいては NTT 西日本の個人情報漏洩事象に対する危機意識や対処能力を推し量るためにも重要であり、今後の再発防止策を検討する上でも必要であると判断したため、この点を当調査委員会の調査対象とすることとした。なお、発覚後社内調査で事態の完全な解明に至らなかった点を考慮し、客観的に本件過去調査を検証すべく、過去調査検証 TF は外部弁護士のみで構成した。

2　本件過去調査に対する総括

後記のとおり、本件過去調査には常識では考え難いほどの多数の問題点があり、あるがままを言えば、「調査」と表現することも憚られるほどの極めて杜撰な「作業」しか実施しておらず、X による本件不正持ち出しに全く気付くことのないまま事なかれ主義的な対応を繰り返したと評価せざるを得ない。かかる実態は、本件調査担当者ら自身の問題は当然として組織文化の問題が根強く影響していると言える。後記のとおり、本アンケート調査の結果においても、BS、ひいては NTT 西日本グループ全体において、「問題なし」との報告を上げることを是とする行動様式が組織文化として存在することが窺われており、本件過去調査はそのような組織文化が極めて色濃く表れた場面に他ならない。

本件過去調査を一見すると、本件調査担当者らが内部からの情報流出を知りつつ、これを積極的に隠蔽したのではないかと見られても致し方なく、当調査委員会もそのような可能性が十分に存在することを意識して慎重に調査を実施した。

しかし、本調査の結果、本件過去調査では、本件調査担当者らは本件不正持ち出しを発見することさえできておらず、また本件不正持ち出しの原因であった当時の情報セキュリティ管理体制の問題点について見直しを行うこともなく、結果として、X による本件不正持ち出しの継続を許していた実態が明らかとなった。つまり、本件過去調査において、本件調査担当者らは、内部からの情報流出を発見してこれを隠蔽するという次元よりも、個人情報漏洩事象に対する危機意識や対処能力という意味ではさらに低い次元、すなわち、内部からの情報流出を発見するにすら至らなかったものであり、隠蔽よりも問題があり、かつ、かかる問題は長年醸成されてきた組織文化とも関係する根深い問題と言わざるを得ない。

本件過去調査は、「調査」には似ても似つかない極めて杜撰な「作業」しか実施しておらず、事なかれ主義的な対応を繰り返すとともに、かかる対応を継続するために一部については虚偽の回答を繰り返していた。具体的には、本件調査担当者らは、エクスポートログについて十分な調査を実施せず、本件過去調査の初期段階で、短時間のうちに表面的にログの検討を行っただけで、内部からの情報流出はないと一方的に結論付けていた。そして、本件調査担当者らは、そのような誤った結論に基づき、事態の重大性

を認識することなく A 社からの本件調査依頼を軽視したこと等により、恣意的にログの開示範囲を限定していた。さらに、本件調査担当者らは、BS における情報セキュリティ管理体制の不足を隠蔽するため、A 社との取引を継続するため又は A 社からの更なる質問をかわすべく、故意に虚偽の回答を行うなどしていた。

本件過去調査に先立って、本件調査担当者らの一部の者は、A 社の顧客データの漏洩については警察による捜査が進められていることを通知されていた。つまり、捜査機関による強制捜査等を通じて事実が明らかになる可能性があることを認識していたにもかかわらず、杜撰な作業に終始し、事なかれ主義的な対応を繰り返し果てには虚偽回答にまで至ったことには唖然とするほかない。

このような前提がある中で、本件過去調査が極めて杜撰なものに終始した背景には、本件調査担当者らが A 社からの本件調査依頼を軽視するとともに、4 名という非常に限られた人員で本件過去調査を実施していたという実施体制等の問題があることから、以下では、まず本件過去調査に至る経緯及び本件過去調査の実施体制等について述べる。そして、本件調査担当者ら 4 名の中でも、本件過去調査における役割や本件過去調査に対する受け止め方や温度感等が異なるため、この点についても言及する。その後、本件過去調査に関する事実経過等、本調査において発見された本件過去調査における不適切回答及びその理由、本件過去調査の問題点に関する分析・評価について述べることとする。

3　本件過去調査に至る経緯

⑴　A 社における情報漏洩の発生認知及び社内調査の実施等

ア　A 社と ProCX の関係

A 社は、少なくとも 20 年以上もの長期にわたって、ProCX（その前身である旧 NTT アクト等も含む。）にテレマーケティング業務を委託しており、継続的に相当の受注量がある取引先である。このような背景もあり ProCX は、A 社に対する専属の営業窓口として岡山営業所（後に本社直轄の岡山拠点。以下両者を区別せずに「岡山支店」という。）を設けるなど、A 社を非常に重要な顧客と位置付けている。ProCX のコールセンタのオペレータが A 社商品の売上に大きく貢献していることから、A 社においても、ProCX は重要な取引先として認知されていた。

イ　A 社による情報漏洩の認知

A 社は、2022 年 1 月頃、自社の顧客から個人情報漏洩の疑いに関する問い合わ

せを受け、同年 3 月頃までに計 4 名の顧客から同様の問い合わせを受けた。A 社に当該問い合わせを行った顧客らは、いずれも貴金属業者から似通った内容の営業連絡を受けていたが、その際、当該貴金属業者の営業担当者は、顧客らが A 社を含めた複数社の健康食品を購入している方へ電話をしている旨の話をしたと伝えた。営業連絡を受けた A 社の顧客のうち 1 名が、当該貴金属業者の名称（以下「I 社」という。）を記憶していたことから、A 社の J 取締役と K 取締役は、2 回にわたり、東京所在の I 社のオフィスを訪問した（なお、2 回目には A 社顧問弁護士も同道した。）。その際、J 取締役及び K 取締役は、I 社が保有し営業に使用している顧客リストを確認したところ、A 社の顧客情報が何らかの形で漏洩し、I 社に渡っていることが判明した。なお、I 社は、いわゆる名簿業者から顧客情報を買い取ったものとみられるが、現在までに、A 社に対して販売元となる名簿業者の名称を明らかにしていない。

A 社は、自社の顧客情報が漏洩している事実を認知した後、A 社内部から情報が流出した可能性を念頭に、社内のシステム部門が中心となって社内における顧客情報の取扱いフローを確認するとともに、大量の顧客情報に触れ得る A 社担当者を対象としたログ調査を実施した。加えて、A 社はコールセンタ業務の一部を外部業者に委託していたことから、社外から顧客情報が流出した可能性も調査すべく、I 社にて確認をした顧客情報に該当する個人情報（以下「本件 A 社漏洩顧客情報」という。）を提供した外部業者を確認した。その結果、本件 A 社漏洩顧客情報は、コンタクトセンタの拠点は違えど、いずれも共通して ProCX に提供されたものであることが判明した。このことから、A 社は、情報の流出元は A 社内部であるか、ProCX のほぼ二択であると認識するに至り、同年 3 月以降、ProCX に対して、本件ネットワーク及び本件システムの構成等について質問をするようになった。

A 社は、このような状況を踏まえ、同年 3 月末頃、岡山県警本部生活安全部生活安全捜査課（以下「岡山県警」という。）に情報漏洩が生じている旨の被害相談を行うに至った。その際、A 社は、岡山県警から、ProCX 側が管理しているサーバや防犯カメラ映像等のデータを保全するよう指導された。

⑵　A 社から ProCX に対する本件調査依頼

ア　A 社による ProCX への面談要請及び当日の出席者

上記の事態を受け、J 取締役は、2022 年 3 月末頃、ProCX の CX ソリューション部担当部長として、日々A 社との契約交渉等を担っていた C 担当部長に対し、電話において、A 社本社で ProCX 社長との面談を希望する旨を伝えた。その際、J 取締役は、C 担当部長に対し、A 社において情報漏洩の発生を認知したこと等は

知らせず、面談の目的は当日に伝えるとしつつ、ProCX 社長の出席は必須であると伝えた。これに対し、C 担当部長は、ProCX 社長に加えて C 担当部長の出席を希望する旨を伝え、J 取締役はこれを了解した。

その後、同年 4 月 4 日、A 社本社において、A 社と ProCX の面談（以下「2022 年 4 月面談」という。）が実施された。2022 年 4 月面談には、A 社側からは A 社社長、J 取締役、K 取締役、個人情報保護の担当者及び A 社代理人弁護士が出席したが、A 社社長は挨拶のみで退室し、以後の顧客情報の漏洩に関する実質的な協議の場には参加しなかった。ProCX 側からは、ProCX 社長及び C 担当部長が出席した。D 担当課長は、普段 A 社の営業担当として A 社との打ち合わせに毎回出席していたが、2022 年 4 月面談の際は、岡山駅から A 社本社へ ProCX 社長と C 担当部長を自動車で送迎する役割を担ったものの、2022 年 4 月面談の場には同席せず、車内で待機していた[24]。

イ　2022 年 4 月面談におけるやり取り

（ア）A 社から ProCX に対する本件調査依頼

A 社は、2022 年 4 月面談の場において、ProCX 社長及び C 担当部長に対し、A 社の顧客情報が漏洩していること、J 取締役らが I 社を訪問した結果、A 社の顧客情報の漏洩が確認されたこと、本件 A 社漏洩顧客情報はコンタクトセンタの拠点は違えど、いずれも共通して ProCX に提供されていること、本件 A 社漏洩顧客情報が ProCX の各コンタクトセンタに委託された年月日、本件 A 社漏洩顧客情報の内容等に照らして流出元は A 社内部又は ProCX のいずれか一方である可能性が高いこと、このような面談は ProCX とのみ実施していること等を伝えた。その際、A 社は、ProCX 社長及び C 担当部長に対し、これらの情報の取扱いには留意されたいと伝えた。

さらに、A 社は、ProCX 社長及び C 担当部長に対し、顧客情報の漏洩について岡山県警に相談している旨を伝え、岡山県警からデータ保全の指導を受けているため ProCX 側が管理しているサーバや各コンタクトセンタに設置されている防犯カメラ映像等のデータ保全をするよう協力を要請した。そして、ProCX においても、内部から情報が流出していないか調査を実施するよう要請した。加えて、A 社でも、A 社内部からの情報漏洩の可能性について引き続き調査を実施するが、A 社では限られたメンバーのみが当該事象を把握しており、A 社の営業担

[24] 2022 年 4 月面談に D 担当課長が出席しなかった理由について、D 担当課長は、A 社が出席者を ProCX 社長と C 担当部長に限定したためと述べているが、一方の A 社は、ProCX 社長の出席は必須であるとしたものの、それ以上に出席者を指名又は限定したことはないと述べている。

当の従業員等には知らせていない旨を伝えた。なお、A 社は、2022 年 4 月面談の当時、本件システムの運用保守を担当しているのが ProCX ではなく BS であることは、ProCX から報告を受けていなかったため把握していなかった。

（イ）2022 年 4 月面談に関する ProCX 社長及び C 担当部長の認識

当調査委員会による 2022 年 4 月面談に関する事実認定は上記のとおりであるが、同面談におけるやり取りについて、ProCX 社長及び C 担当部長は、以下のとおり、複数の点について異なる認識を述べる。

第一に、ProCX 社長及び C 担当部長は、2022 年 4 月面談の際、A 社から、限られた人員でクローズドな調査を実施するよう要請を受けたと述べている一方、A 社の K 取締役は、A 社にメリットがないためそのような要請はしておらず、情報共有をある程度の範囲に留めるよう求めたにすぎないと述べている。この点について ProCX 側と A 社側で認識に相違があるが、K 取締役が述べるとおり、真相解明を望んでいた A 社が ProCX の調査体制や人員を限定する合理的理由はなく、2022 年 4 月面談の場で A 社が提供した情報の取扱いについて留意されたい旨の発言と、A 社内の調査は限られたメンバーが行っている旨の発言等を受けて、ProCX 社長及び C 担当部長が、ProCX においても、限られた人員でのクローズドな調査を実施するよう求められていると誤解した可能性が高い。

第二に、C 担当部長は、2022 年 4 月面談当時、顧客情報の流出元として、A 社内部又は ProCX のほぼ二択にまで絞られてはおらず、ProCX 以外の外部業者の可能性も残されていると認識していたと述べている。しかしながら、A 社の K 取締役は 2022 年 4 月面談時点では A 社内部又は ProCX のほぼ二択という説明をしたと述べ、また ProCX 社長も同様の受け止めをしたと述べている。さらに、前記のとおり、本件 A 社漏洩顧客情報は、コンタクトセンタの拠点は違えど、いずれも共通して ProCX に提供されたものであったという点を踏まえれば、C 担当部長によるこのような受け止めは客観的事実に反する。したがって、A 社は、2022 年 4 月面談当時、顧客情報の流出元として、A 社内部又は ProCX のほぼ二択にまで絞っており、これを前提としたやり取りがあったと認められる。

第三に、C 担当部長は、2022 年 4 月面談において、A 社から具体的かつ正式なデータ保全の依頼はなかったと述べるが、当時、A 社にとって、流出元の特定のための客観的資料の確保は急務であったとみられ、既に流出元が A 社又は ProCX のほぼ二択に絞られていた状況において保全の依頼を先送りする合理的な事情もない。また、ProCX 社長が、今後防犯カメラや各コンタクトセンタの入室記録を確認するので協力してほしいといったやり取りはあったと述べていることに照らせば、上記のとおり、2022 年 4 月面談の場において、A 社から

ProCX に対してデータ保全に関する協力要請があったものと評価できる。

4　本件過去調査の実施体制等

⑴　本件過去調査の関与者等

ア　限られた人員で調査を行う旨の方針決定

ProCX 社長と C 担当部長は、2022 年 4 月面談の帰路、D 担当課長が運転する自動車の車内において、同面談における A 社からの協力要請を踏まえ、ProCX からの情報流出の有無について調査を実施する旨の方針を固めた。ただし、この時点において、両名の問題意識は、ProCX の各コンタクトセンタに所属する SV 又はオペレータからの情報漏洩のみに向けられており、本件システムにアクセスすることができる BS の保守者からの情報漏洩の可能性には一切向けられていなかった。そして、ProCX 社長と C 担当部長は、前記のとおり、A 社から限られた人員で調査を実施することを求められたと理解していたことから、C 担当部長を含めた限られた人員で調査を実施することを確認した。

イ　本件過去調査の主な関与者

本件過去調査に関与した主な人物は、2022 年 4 月面談に出席した ProCX 社長及び C 担当部長に加え、C 担当部長の部下 3 名（D 担当課長、E 担当課長、F 担当課長）であった。これら 5 名の主な役職・経歴、関係性及び X との関係性は次のとおりである。

ProCX 社長は、2022 年 3 月末まで ProCX の代表取締役と BS の VD 部の役職を兼任していたが、2022 年 4 月 1 日以降は専ら ProCX 代表取締役の地位にあった。本件過去調査において、ProCX 社長が直接やり取りを行っていたのは、基本的に C 担当部長であり、後記のとおり、ProCX 社長が本件過去調査の一部の事項について報告を受けた際も、専ら C 担当部長が ProCX 社長への連絡を行っていた。また、ProCX 社長は、D 担当課長及び E 担当課長とは本件過去調査以前から面識があり、両名が本件過去調査を担当することを認識していた。他方、本件過去調査以前、F 担当課長とは面識がなく、F 担当課長が本件過去調査に関与していることを把握していなかった。また、ProCX 社長は、前記のとおり BS の VD 部の役職に就いていた時期があったものの、X との面識はなく、本件過去調査当時も X の存在を認識していなかった。

C 担当部長は、旧 NTT アクト時代を含め、長らく ProCX の CX ソリューショ

ン部の役職に就いていたが、本件過去調査の当時は、BS の VD 部の役職も兼任していた。C 担当部長は、本件過去調査当時、ProCX において D 担当課長の上長の立場にあったとともに、BS において E 担当課長及び F 担当課長の上長の立場にあった。ただし、本件過去調査当時、E 担当課長及び F 担当課長の直属の上長は後記の L 担当部長であり、その上に C 担当部長が位置していた。また、C 担当部長は、本件過去調査以前に業務で協働したことがあったため、X の存在は認知していた。

D 担当課長は、本件過去調査の当時、ProCX の CX ソリューション部に所属し、岡山支店を拠点としていた。本件過去調査当時、D 担当課長にとって C 担当部長は上長に当たり、本件過去調査以前にも業務上のやり取りを行うことがあったが、その頻度は高くなかった。また、D 担当課長が岡山支店を拠点としていたのに対し、C 担当部長は本社オフィスを主な拠点としていたため、主な業務拠点も異なっていた。また、D 担当課長は、E 担当課長と本件過去調査以前から業務上接点があったものの、やり取りをする機会は少なかった。他方、F 担当課長とは本件過去調査以前は面識がなかった。

E 担当課長は、旧 NTT アクトで勤務した後、本件過去調査の当時は BS の VD 部 X 所属グループに所属していた。C 担当部長とは、旧 NTT アクト在籍時代から上司・部下の関係にあり、前記のとおり、本件過去調査当時においても、BS の VD 部において同様の関係にあった。F 担当課長とは、旧 NTT アクトと BS の間で組織再編（この際、旧 NTT アクトの一部部署が BS に編入された。）が行われた以降から BS の同部署で勤務するようになり、E 担当課長が、X 所属グループのフロント SE[25]チームを統括し、ProCX 等といった BS の顧客と直接やり取りし、システムの販売・提案・支援を担っていたのに対し、F 担当課長はいわゆるバック SE チームの統括者として本件システムの運用保守を担っており、このように担当業務を分掌しつつ、必要に応じて連携しながら業務を行っていた。また、E 担当課長は本社オフィスを主な業務拠点としていたのに対し、F 担当課長は本件保守拠点を主な業務拠点としており、基本的に別拠点で業務を行っていた。X は、2020 年 11 月以降、E 担当課長が統括するフロント SE チームに所属し、本件過去調査当時も E 担当課長のグループに所属していた。すなわち、この間、E 担当課長は X の直属の上長の立場にあった（前記第４・２参照）。

F 担当課長は、本件過去調査当時、BS の VD 部 X 所属グループに所属しており、バック SE チームを統括していた。もっとも、F 担当課長自身は、日常的に PDS サーバの保守・運用業務に携わっていたわけではなかった。前記のとおり、

[25] システムエンジニア（System Engineer）。特に、システムのユーザーの目に直接触れる部分（操作メニュー・アイコン等）を扱う SE を「フロント SE」、ユーザーの目に直接触れない部分（サーバ・データベース等）を扱う SE を「バック SE」と呼ぶ。

C 担当部長は BS において F 担当課長の上長に当たるが、直接のやり取りを日常的に行っていたものではなく、業務拠点も基本的に別であった。業務内容としても、C 担当部長が ProCX における顧客向けの営業関係に比重を置いていたこともあり、F 担当課長が BS で担当する本件システム運用保守業務との関係では、管理者ミーティングやトラブル等が生じた場合を除き、日常的な業務報告を直接行う関係にはなかった。F 担当課長は、X 所属グループに所属しており、また同じく本件保守拠点を拠点としていたため、日常的に X と接触の機会があったが、X は E 担当課長のフロント SE チームに所属していたため、F 担当課長が X に直接指示を出すことは基本的になかった。ただし、X が特に PDS サーバの設定に詳しかったため、F 担当課長らバック SE のチームも ProCX 向けの対応やトラブル対応といった場面で X を頼ることが多かった（前記第４・２参照）。

ウ　D 担当課長、E 担当課長及び F 担当課長が本件過去調査に関与するに至った経緯等

C 担当部長は、2022 年 4 月面談を終え、A 社本社から岡山駅に向かう帰路において、ProCX のコンタクトセンタのうち、A 社の顧客データを取り扱っている豊橋、名古屋、福岡、熊本及び岡山の各拠点について緊急監査（以下「本件センタ緊急監査」という。）を実施することとし、A 社の営業担当であり、かつ日常の業務を通じて各センタとの繋がりがあった D 担当課長に本件センタ緊急監査を担当させることにした。C 担当部長は、2022 年 4 月面談の帰路において、D 担当課長に対して同面談の概要として、A 社の顧客情報が漏洩していること、A 社が警察に相談していること、ProCX からの流出の可能性について調査を実施すること等を伝え、本件センタ緊急監査を実施するよう伝えた。

また、C 担当部長は、各コンタクトセンタが本件システムを利用している以上、ProCX からの情報漏洩の有無を調査するに当たっては、本件システム関連の質問に対応できる者が関与する必要があると考えた。そこで、C 担当部長は、2022 年 4 月面談の帰路において、同面談の以前から A 社からの本件システム関連の問い合わせに対応し、システムエンジニアとして本件システムについて知識が豊富であると認識していた E 担当課長を調査メンバーに加えることを決め、帰路において ProCX 社長にその旨を伝えた。ProCX 社長も、C 担当部長と同様、E 担当課長をシステムエンジニアとして本件システムに関する知識が豊富な人物であると認識していたことから、これを承認した。なお、E 担当課長は、ProCX の従業員ではなく BS の従業員であったが、当時 C 担当部長が ProCX の役職と BS の役職を兼任していたことや、E 担当課長が旧 NTT アクトと BS の組織再編前は C 担当部長の直属の部下であり、ProCX 社長ともかつて同組織に所属していたこと等から、

ProCX 社長及び C 担当部長は、ProCX に対する本件調査依頼に BS の従業員である E 担当課長が対応することについて何らの違和感も抱いていなかった。そして、C 担当部長は、遅くとも 2022 年 4 月面談の翌日である同年 4 月 5 日までに、E 担当課長に対して A 社からの問い合わせに対応するよう指示しているが、D 担当課長とは異なり、この段階では、E 担当課長に対して A 社の顧客情報が漏洩していることを含め 2022 年 4 月面談の詳細を伝えていなかった。

F 担当課長は、ProCX 社長又は C 担当部長が調査メンバーとして選任したのではなく、エクスポートログに関する A 社からの質問を受けた E 担当課長が、自身のスキルに照らして対応可能な範疇を超えるため、この点についてより知識のあるバック SE である F 担当課長の助力を得る必要があると判断し、2022 年 4 月 18 日に協力を依頼した結果、本件過去調査に関与したものである。なお、この時点において、E 担当課長が A 社の顧客情報が漏洩していることを含め 2022 年 4 月面談の詳細について把握していなかったことから、当然 F 担当課長もこの点を認識していなかった。そして、F 担当課長が本件過去調査の回答作成に関与していることについて、C 担当部長は、2022 年 5 月 11 日の回答の時点では把握しておらず、同年 6 月 1 日回答の準備段階でその関与を知った。

エ　本件過去調査に対する ProCX 社長の認識

ProCX 社長は、後記の 2022 年 4 月 21 日回答の前後に、C 担当部長から、本件センタ緊急監査の結果、ProCX の各コンタクトセンタに特に問題は見当たらなかった旨の口頭報告を受けたが、2022 年 4 月 21 日回答の資料そのものの共有は求めず、回答資料の確認をしなかった。また、それ以降も A 社からの質問が続き、本件調査担当者らがこれに回答するなど 2022 年 7 月頃まで本件過去調査が継続していた事実について、本件調査担当者らが ProCX 社長に報告することはなく、ProCX 社長もこれらの事実を把握していなかった。すなわち、ProCX 社長は、2022 年 4 月下旬に ProCX の各コンタクトセンタに特に問題は見当たらなかったと A 社に回答したことをもって、本件過去調査は終結し、情報漏洩に関する懸念は解消されたものと認識していた。

C 担当部長は、4 月 21 日回答の後も、さらに A 社から質問が寄せられていたことをなぜ ProCX 社長に報告しなかったかという点について、A 社の質問内容の焦点が ProCX のコンタクトセンタから BS の保守担当者に移っていったところ、ProCX 社長は、当時既に BS の役職を離れていたため、ProCX 社長の所掌範囲外の事項と判断したためであると述べている。

オ　その他本件過去調査の存在を認識していた者

C 担当部長は、E 担当課長に本件過去調査を担当させることについて、E 担当課長の直属の上司である VD 部の L 担当部長に説明をするために、2022 年 5 月のゴールデンウィーク後、L 担当部長に対し、A 社の顧客情報の漏洩が発生していること、A 社から ProCX に対して流出の可能性について調査するよう依頼があったこと等を伝え、L 担当部長は E 担当課長が本件過去調査を担当することについて了解した。L 担当部長は、その後の具体的な調査や A 社に対する調査結果の回答の作成には携わっていないが、後記のとおり、本件過去調査において一部虚偽回答がなされたことは把握していた。

また、C 担当部長は、本件センタ緊急監査に先立ち、ProCX で A 社関連業務を担当しているエリアの一部の関係者に対し、本件センタ緊急監査の背景に A 社の顧客情報の漏洩があった旨を伝え、同監査に協力するよう依頼していた。また、C 担当部長は、福岡センタについては、同拠点に対する本件センタ緊急監査の前である 2022 年 4 月 6 日に同拠点を訪問し、関係者に A 社の顧客情報の漏洩があったこと等を説明していた[26]。これらの各関係者は、本件過去調査の存在は知っていたが、その後の具体的な調査や A 社に対する調査結果の回答作成には携わっていない。

⑵　各社におけるエスカレーションの欠如及び理由

ア　BS 内部でのエスカレーション

本件調査担当者らのうち、役職上、C 担当部長が最も上席に位置しているが、2022 年 4 月面談以降、2023 年 7 月に本件不正持ち出しが発覚するに至るまで、A 社から本件調査依頼があったことについて、C 担当部長より上席に位置する BS 上層部へのエスカレーションは一切行われていない。例えば、本件過去調査期間中、C 担当部長の上長として、VD 部 M 部門長や VD 部 N 担当部長がいたが、A 社から本件調査依頼があったことは両名にエスカレーションされていない。

その理由について、C 担当部長は、A 社から限られた人員でクローズドな調査を実施するよう要請を受けており、本件調査依頼の存在を知らせる範囲は限定した方がよいと判断したことに加え、M 部門長及び N 担当部長はいずれも A 社関連業務にほぼ携わっておらず、A 社とのコミュニケーションも頻繁ではなかったため、

[26] このように福岡センタを訪問した理由について、C 担当部長は、2022 年 4 月面談の際、本件 A 社漏洩顧客情報が福岡センタに委託されていたケースが多いことを把握し、福岡センタからの漏洩について特に問題意識を持っていたためであると述べている。

特に報告する必要はないと判断したためであると述べている。もっとも、C 担当部長は、本件過去調査の当時、ProCX 及び BS の役職を兼任していたものの、業務の比重は ProCX の業務に偏っていたことから、BS 内部でのエスカレーションの必要性について真摯に検討できていなかった可能性も指摘できる。

また、BS の従業員である E 担当課長、F 担当課長及び L 担当部長は、本件過去調査の当時、いずれも C 担当部長以上の役職者にエスカレーションされていないことを認識していたが、特にこの点について疑問を持つこともなく、何ら異議を述べることもなかった。

以上のとおり、BS 内部において、C 担当部長より上席の者は、誰一人として本件過去調査の存在を把握していなかった。

イ　ProCX 内部でのエスカレーション等

ProCX では、前記のとおり、ProCX 社長は A 社からの本件調査依頼について把握していた。しかし、ProCX では、「個人情報・特定個人情報保護基本規程」に基づき、事故が発生した際には事業推進部長が統括管理責任者を中心として対応に当たることが想定されているが、2022 年 4 月面談以降、2023 年 7 月に本件不正持ち出しが発覚するに至るまで、事業推進部長に対してこの点の情報共有はなされていない。

その理由について、ProCX 社長は、A 社から限られた人員でクローズドな調査を実施するよう要請を受けていたことに加え、統括管理責任者は名目的な役職であり、この点に対する信頼がなかったためであると述べている。また、C 担当部長は、ProCX の関係規程やマニュアルを確認したものの、文言上、今回の事象がエスカレーション対象になるか否かの判断がつかず、社内での報告よりも調査を進めることを優先したと述べている。

また、ProCX の従業員である D 担当課長については、ProCX の関係規程やマニュアルの存在こそ認識していたものの、特にこれらの内容を確認することはなかった。

ウ　NTT 西日本でのエスカレーション

2022 年 4 月面談以降､2023 年 7 月に本件不正持ち出しが発覚するに至るまで、A 社から本件調査依頼があったことについて、ProCX 又は BS から、NTT 西日本に対するエスカレーションは一切行われていない。

NTT 西日本へエスカレーションしなかった理由について、ProCX 社長は、2022 年 4 月面談の時点で、ProCX から個人情報が流出したことは明確に確認されてお

らずまだ疑いの段階であったこと、そして A 社から限られた人員でクローズドな調査を実施するよう求められていたためであると説明している。そして、情報漏洩のおそれを認知した際のエスカレーションルールの存在は特に認識していなかったと述べている。

5　本件過去調査の事実経過等

⑴　本件過去調査の概要

本件過去調査では、基本的に、A 社からの質問に対して本件調査担当者らが都度回答を準備し、これをメールで送付するという形式で進められていた。本件調査担当者らが提出した回答は、以下のとおり合計 7 件ある（いずれも 2022 年。以下、各回答を「4 月 15 日回答」等という。）。このうち、4 月 15 日回答から 4 月 21 日回答の時点では、主に ProCX のコンタクトセンタからの情報流出を想定した質問が A 社から寄せられていたため、回答もその点に焦点を当てた内容となっていた。

他方、5 月 11 日回答から 7 月 15 日回答の時点では、コンタクトセンタからの情報流出の可能性に加えて、システムの保守者からの情報流出を想定した質問が A 社から寄せられるようになっており、回答もこの点を踏まえた内容となっていた。

- 4 月 15 日回答
- 4 月 18 日回答
- 4 月 21 日回答
- 5 月 11 日回答
- 6 月 1 日回答
- 7 月 1 日回答
- 7 月 15 日回答

また、同年 7 月 1 日には、それまでの本件調査担当者らからの回答内容を踏まえて、A 社と本件調査担当者らによるウェブ会議（以下「本件ウェブ会議」という。）が実施されており、7 月 15 日回答は本件ウェブ会議における A 社からの質問事項に対する回答として位置付けられていた。

⑵　本件調査担当者らの役割分担及び情報の偏在

本件過去調査において、C 担当部長は、A 社からの質問に対する回答時期についておおよその目安を設定するとともに、D 担当課長、E 担当課長及び F 担当課長に対し、調査方針や方法の概要について方向性を示していた（ただし、C 担当部長は、5 月 11 日回答の時点で F 担当課長が本件過去調査に関与していたことを把握しておら

ず、本件システムの技術的な事項に関する調査方針等については、E 担当課長に伝えるなどしていた。)。その後、おおむね、D 担当課長が ProCX のコンタクトセンタに関係する事項の調査と回答案の作成を、E 担当課長及び F 担当課長が本件システムに関係する事項の調査を実施し、E 担当課長がシステム関係事項の回答案の作成を担当するという役割分担がなされていた。そして、C 担当部長は、A 社に提出する前に、回答内容の最終確認を行っていた。

前記のとおり、E 担当課長及び F 担当課長は、4 月 21 日回答の前後の時点では、A 社の顧客情報の情報漏洩が問題になっているという点を認識していなかったが、遅くとも 5 月 11 日回答を準備する段階ではこの点を認識していた。もっとも、C 担当部長は、E 担当課長及び F 担当課長に対し、本件過去調査の全期間を通じて、本件 A 社漏洩顧客情報はコンタクトセンタの拠点は違えど、いずれも共通して ProCX に提供されたものであったことや、本件 A 社漏洩顧客情報が ProCX の各コンタクトセンタに委託された年月日等といった 2022 年 4 月面談で A 社から示された情報を共有していない。C 担当部長は、その理由として、これらの情報は ProCX の各コンタクトセンタに関する情報であるため、システム面の調査を担当していた E 担当課長及び F 担当課長に共有する必要はないと判断したと述べている。また、C 担当部長だけでなく、D 担当課長も、E 担当課長及び F 担当課長に対し、本件過去調査の全期間を通じて、C 担当部長経由で把握していた 2022 年 4 月面談で A 社から示された情報を共有していない。F 担当課長は、同年 7 月 6 日、D 担当課長に対し、以下のメール（以下「7 月 6 日メール」という。）を送信しているが、D 担当課長は、これに対しても特に情報を把握していない旨回答していた。その理由について、D 担当課長は、C 担当部長を通じて自身が把握していた 2022 年 4 月面談で A 社から示された情報は、あくまでも断片的なものであり、これを F 担当課長らと共有しても解決に繋がらないと思っていたからであると述べている。

【F 担当課長→D 担当課長宛て（CC：E 担当課長）メール（2022 年 7 月 6 日 午後 5 時 20 分)】

「…また、A 社様側の調査で判明していることはないのか気になっております。D 担当課長[27]の方で以下のような内容をお聞きになっていないでしょうか？できれば教えていただきたいと思っています。

・外部に持ち出されたデータは全て回収して把握できているのか？

・当該データは、いつ（何年何月頃)、どのセンタへ渡したものか確認できているのか？#分かっていれば教えていただきたい。#2019/5～2022/6 と長い期間のご質問もあったので、どういうことかと。

・当該データの中にアクトが受け取っていないデータはなかったことが確認でき

[27] 元のメールでは、D 担当課長の苗字が記載されている。

ているのか？#調査されているということはアクト以外には正式に渡した相手はいないということかもしれませんが。

・当該データにどういう内容（項目）があったのか判明しているか？#分かっていればデータの項目を教えていただきたい。#アクトさんが受け取っているデータ項目と同じとか、逆に納品データの項目があるとか　#PDS にあるデータ項目しかなかった、となればかなり疑われていることになるので。

我々としても、何か手掛かりになるものがあった方が良いと思います。…」

⑶　本件調査担当者らによる各調査及び各回答内容

ア　4 月 15 日回答、4 月 18 日回答及び 4 月 21 日回答

（ア）4 月 15 日回答、4 月 18 日回答及び 4 月 21 日回答の位置付け等

4 月 21 日回答は、他の回答とは異なり一問一答形式になっていないが、これは 4 月 15 日回答及び 4 月 18 日回答において回答未了として積み残しになっていた部分を併せて回答したほか、本件センタ緊急監査等、本件調査担当者らの判断で実施した調査事項をまとめたことによる。後記のとおり、4 月 15 日回答、4 月 18 日回答及び 4 月 21 日回答には大きな問題点はないと認められるが、これらの回答を巡る経緯は、エクスポートされ改変されたログが提出される等した 5 月 11 日回答の当時の本件調査担当者らの認識等を理解する上で重要な意義を持つ。

（イ）4 月 15 日回答、4 月 18 日回答及び 4 月 21 日回答を巡る経緯

前記のとおり、A 社は、2022 年 4 月面談の以前から、ProCX に対して本件システム等について問い合わせをしており、C 担当部長、E 担当課長及び D 担当課長がその対応に当たっていた。C 担当部長は、2022 年 4 月面談後、E 担当課長に対し、①本件システムがネットワーク構造上外部からの侵入を一切遮断していることを示す根拠、②コンタクトセンタ内部からの接続・データエクスポートの可否及び可能であった場合の権限者と対象データ内容について極秘に調査するよう伝えた。E 担当課長は、PDS サーバのベンダである B 社の担当者に照会する等して、2022 年 4 月 5 日の時点で、②について、コンタクトセンタ内部からの接続について、証明書をインストールした特定端末かつ SV 以上の権限を持った ID でログインすることにより顧客データのインポート・エクスポートが可能となること、ログを追うことで、エクスポートした痕跡・ID 等の情報を特

定することが可能であることを初めて把握した。

他方、D 担当課長は、2022 年 4 月 12 日から同年 4 月 15 日にかけて、本件センタ緊急監査を実施し、各コンタクトセンタにおいて、A 社から配布される顧客データの受取の過程や、ProCX における業務終了後のデータ納品時におけるデータ削除の過程で特定 USB メモリの認証が正常に機能するか否か等を確認した。また、各コンタクトセンタの監視カメラの設置状況を確認した。

その後、2022 年 4 月 13 日、A 社の営業担当者から、C 担当部長に対し、メールで、別紙 6-1 記載の各質問と各管理簿の保管要請があった[28]。D 担当課長は、同年 4 月 15 日、これに対し、メールにて、同別紙記載の回答欄記載のとおり回答した[29]。同日、再び、A 社の営業担当者から、C 担当部長及び D 担当課長に対し、メールにて、別紙 6-2 記載の各質問と各管理簿の保管要請があった。D 担当課長は、同年 4 月 18 日、これに対し、メールにて、同別紙記載の回答欄記載のとおり回答した[30]。

E 担当課長は、4 月 18 日回答の前後において、F 担当課長に対し、A 社から本件システムにおける A 社の顧客データの出し入れに関するログに関する問い合わせが来ていることを電話で伝えた。そして、E 担当課長は、翌 4 月 19 日、F 担当課長に対し、4 月 18 日回答で回答を留保していたうちの二点、すなわち本件システムのログの保管期間の年数（質問 2）及び本件システムのログの永年保管の可否（質問 5）等について調査するようメールで依頼し、F 担当課長は B 社担当者に対してそれらの確認をメールで依頼した。B 社担当者は、F 担当課長に対し、翌 4 月 20 日、システムを新基盤に切り替えた 2016 年以降の顧客データのインポート・エクスポートのログは永年保管となっている旨メールで回答した。F 担当課長は、この時点で、今後エクスポートログの調査が必要になる事態を想定し、同日、B 社担当者に対して調査方法等について相談していた。B 社担当者は、同日、エクスポートログは、PDS の「アクセスログ」機能を利用すれば SV でも参照可能であること、期間、キャンペーン、ユーザーなどを指定して検索可能であることを説明した。これらの点は、F 担当課長から E 担当課長

[28] なお、A 社の営業担当者は、当該メールにおいて、当該質問は、A 社におけるアウトバウンドリストの取扱いに関する一連の流れについて見直しを進めている過程での各社への現状確認名目であると説明しており、本件調査依頼との関係性は明らかにしていなかった。

[29] なお、別紙 6-1 は、当事者間のメールでの質問及び回答のやり取りを表形式に整理したものである。

[30] 前脚注と同様、別紙 6-2 は、当事者間のメールでの質問及び回答のやり取りを表形式に整理したものである。4 月 18 日回答で回答を留保していた質問 6（利用者一覧）については、D 担当課長の部下が、2022 年 4 月 20 日に A 社営業担当者にメール送信している。D 担当課長の部下が送信した理由について、D 担当課長は、社外に添付ファイルを送信する際には、送信者の上席の承認手続が必要となるところ、部下が送信した場合には、D 担当課長自身が承認手続を行うことが可能となり簡便であったためと説明している。なお、当該部下は、A 社からの本件調査依頼の存在や本件過去調査の詳細について把握しておらず、実質的な関与もない。

に情報共有されていた[31]。

以上の調査結果等を踏まえ、E 担当課長及び D 担当課長は、これまでの調査結果を整理し、4 月 21 日回答（別紙 6-3）を作成した。E 担当課長は、4 月 21 日回答のうち、「■PDS サーバへのアクセスに関するセキュリティポリシーについて」（1 枚目）と「■操作ログ出力イメージ（サンプル）」（2 枚目）を担当し、D 担当課長は、「■リストデータの受け取り、納品に関する取扱いについて」（3 枚目）以降をそれぞれ担当している。4 月 18 日回答で回答を留保していた上記二点については、「■PDS サーバへのアクセスに関するセキュリティポリシーについて」（1 枚目）の④で回答がなされた。

4 月 21 日回答の際には、主に ProCX のコンタクトセンタにおける情報漏洩が念頭に置かれていたが、「■PDS サーバへのアクセスに関するセキュリティポリシーについて」（1 枚目）に補記として、「保守者はハードウェアのヘルスチェック・OS 再起動のみメンテナンス（月 1 回）を実施し、個別業務データへのアクセスは不可。」として、システム保守者の作業内容を念頭に置いた記述がある。

イ　5 月 11 日回答

A 社の J 取締役は、2022 年 4 月 28 日、C 担当部長に対し、別紙 6-4 記載の各質問をメールで送付し、本件調査担当者らは、同年 5 月 11 日、同別紙 6-4 記載のとおり回答した[32]。5 月 11 日回答の提出に先立ち、C 担当部長、D 担当課長及び E 担当課長は、回答資料に関する電話会議（以下「5 月 10 日電話会議」という。）を実施したが、F 担当課長は 5 月 10 日電話会議に出席していなかった。

5 月 11 日回答において、本件調査担当者らは、「ONE CONTACT Network の PDS サーバのデータにアクセスできるシステム管理者[33]の範囲（内部／外部、役職など）と人数、対象者氏名」の質問（質問 1）に対し、X、C 担当部長、E 担当課長及び X を含む体制について回答した。また、「前システム機器廃棄時のデータ取り扱い内容」に関する質問（質問 2 後段）に対し、「前システム（PDS サーバ等）については、NTT フィールドテクノのデータ消去サービスを行った上、産業廃棄処分（O 社）を実施しております。」と回答した。その上で、回答の別紙（以下「5 月 11 日回答別紙」という。）として、5 月 11 日回答別紙 1（2）「■PDS サーバへ

[31] なお、F 担当課長は、以上の 4 月 21 日回答までの間、E 担当課長からの問い合わせに対応して B 社担当者への照会等は行っていたものの、直接回答内容の作成には携わっておらず、A 社に提出する前に回答資料を確認することもしていない。

[32] 5 月 11 日回答以降の回答は、基本的に D 担当課長が A 社の J 取締役に回答資料を添付の上、メール送信する形で行われているが、その際の添付ファイル付外部メールの承認権限は D 担当課長の上長 3 名にあった。D 担当課長は、回答の送信の都度、当該承認権限者に連絡をとり、添付ファイルの中身を見ずに承認するよう依頼していた。

[33] A 社は、システム保守者を「システム管理者」として表記している。

アクセス可能な保守用端末の取り扱いについて」を添付し、5 月 11 日回答別紙 1（2）において、「…システム管理者＝保守者は、ハードウェアのヘルスチェック・OS 再起動のみメンテナンス（月 1 回）を実施しておりますが、メンテナンス時以外にも、各センタからの問合わせ（トラブル対応、画面修正依頼、疑似試験等があった場合のみ、弊社（〈本件保守拠点〉[34]）に設置している保守用端末より、PDS サーバ全 4 台へアクセスできる環境となっております。」、「②保守用端末の構成については、物理的に USB ポートのない端末で暗号化ソフトにて情報漏えい対策を実施、データ取出し不可」（下線について原文ママ）、「③保守用端末は、センタ端末同様証明書をインストールした特定端末及びテナント毎（拠点単位）にシステム管理者が利用する専用（ID/Password）により、必ず 2 名以上の体制にて、トラブル対応、模擬試験等の作業を実施するようにしております」（下線について原文ママ）、「各 PDS サーバのデータ出力ログを調査した結果、弊社テスト用のデータ出力のみであることを確認しております。」等と回答した。

さらに、5 月 11 日回答において、本件調査担当者らは、「ONE CONTACT Network 環境および前システム環境における、ネットワーク外へのデータ取り出し方法と、データ取り出しできるシステム管理者の範囲と人数、対象者の氏名」の質問（質問 3）に対し、「NO.2 関連、ONE CONTACT Network 環境及び前システム環境も、各センタからのアクセス経路においては、ネットワークの構造とテナント規制により、ネットワーク外への一括データ出力は不可となっております。但し、各センタからの問合せ（トラブル対応、画面修正、疑似試験等）があった場合のみ、弊社〈本件保守拠点〉[35]に設置している保守用端末〈※〉より、システム管理者（2 名以上:担当課長＋担当者）にて、テナント（拠点）に応じた専用 ID/パスワードにてログインし、キャンペーン構成・画面エラーチェック、動作試験等を実施することがありますが、データ出力したか否かの痕跡を調査した結果、5 月 11 日回答別紙 2 のとおり、当社テスト用キャンペーンの出力結果しかございませんでした。尚、システム管理者の範囲と人数、対象者は NO.1 に記載のとおり。〈※〉USB ポート無し、秘文ソフトウェアがインストールされた専用端末」と回答した。そして、回答の別紙として、5 月 11 日回答別紙 2「顧客データダウンロードログ」を添付し、2020 年 8 月から 2022 年 2 月までの間の全 255 行のログ（以下「本件提出ログ 1」という。）を 5 月 11 日回答とともに提出した。

なお、「ONE CONTACT Network と前システム（AQStage)の画面ハードコピー（弊社業務）を頂けますか。」との質問（質問 8）に関し、E 担当課長は、同年 5 月 9 日に、X に対応を依頼し、X が福岡拠点の A 社業務の画面キャプチャを入手した後、E 担当課長に送信している。

[34] 元の回答では、本件保守拠点の名称が記載されている。
[35] 同上。

ウ　6月1日回答

A社のJ取締役は、別紙6-5記載のとおり、2022年5月23日、C担当部長に対し、PDSサーバのデータにアクセスできるシステム管理者の体制を変更するよう依頼する（以下「本件体制変更依頼」という。）とともに、PDSサーバにおけるシステム管理ログ（顧客データダウンロード含む）の編集可否について質問した（以下「5月23日質問」という。）。また、A社のJ取締役は、同年5月25日[36]、C担当部長に対し、追加質問として、同別紙記載の各質問（質問1から質問9）をメールで送付した（以下「5月25日追加質問」という。）。本件調査担当者らは、5月23日質問と5月25日追加質問について、同年6月1日にまとめて回答した（同別紙）。なお、5月23日質問に対する回答は、5月11日回答に続く形で連番（質問9、質問10）が付されているが、5月25日追加質問に対する回答は、元々のA社が付していた質問番号（1ないし9）がそのまま維持されている。

6月1日回答において、本件調査担当者らは、本件体制変更依頼について、「4/28回答のNo.1記載の体制につきまして、システム保守者（システム管理者）4名について、以下のとおり体制見直しを図りました。」として、XとF担当課長を含むシステム保守者の現体制をE担当課長を含む新体制に変更した旨回答した。5月23日質問の「PDSサーバにおけるシステム管理者ログ（顧客データダウンロード含む）の編集可否」を問う質問に対しては、「PDSサーバへのアクセスログ・操作ログ等については、PDSサーバ本体へファイルとして自動で書出しされる仕組みとなっており、システム保守者は勿論、開発サイドでも編集することができない仕様となっております。」と回答した。

5月25日追加質問のうち、5月11日回答で「ONE CONTACT NetworkのPDSサーバのデータにアクセスできるシステム管理者の範囲（内部／外部、役職など）と人数、対象者氏名」の質問（5月25日追加質問1）で名前を列挙した者の所属先として、BSが含まれることを回答した。また、「データ削除（NTTフィールドテクノ社）や廃棄（O社）についての実施証明は取られていますでしょうか？」との質問に対して、「前回（4月28日No2.回答）”前システム（PDS）はデータ削除や産業廃棄処分を実施しております”とご回答させて頂きましたが、”データ削除や廃棄処分は未だ実施しておらず”、弊社情報伝達の不手際により誤ったご回答をしてしまい、申し訳ございません。」として5月11日回答の一部を訂正するとともに、「尚、”前システム（PDS）”のハードディスクは全てフォーマット化の上、デ

[36] 6月1日回答（別紙6-5）では、追加質問の日付が「5月24日」と記載されているが、A社のJ取締役がC担当部長に対してメールで追加質問を送付したのは、2022年5月25日である。

ータがないことを確認しており、弊社〈本件保守拠点〉[37]の鍵付き書庫に保管してあります。補足）データ削除（NTT フィールドテクノ）及び産業廃棄（O 社）に関する両社への申請手配は既に完了しておりますので、実施予定である 2022.7 月以降は実施証明書をご提出することは可能です。」と回答した。

5 月 25 日追加質問のうち、「保守端末からログインの実績については、実施記録とログの突合せにより誰がいつログインしたかの証明が可能な状態でしょうか？」との質問（5 月 25 日追加質問 3①）に対し、本件調査担当者らは、「保守端末においては、貴社以外のユーザ含めた緊急故障対応及び緊急設定依頼等を作業者が迅速且つ 早期復旧させる必要があることからも、実施記録簿はつけておりません。但し、作業については必ず管理者含む 2 名体制にてクロスチェックし実施するようにしております。」と回答した。

また、A 社は、5 月 25 日追加質問として、「別紙 2（※本件提出ログ 1 の意）のログについて、前システムのログは御座いますか？また、フィルターが掛けられていると思われるのでどのような内容でフィルターが掛かった状態でしょうか？」との質問をした（5 月 25 日追加質問 3②）が、本件調査担当者らは、「前システムログ（ONE CONTACT Network 移行前）は別紙 6 参照。／フィルターについては、新システム（ONE CONTACT Network）への移行分のみをサンプル抽出したこと、又、管理者用 ID（〈特定の文字列〉[38]を含む ID）のみに絞らせて頂きました。」と回答し、6 月 1 日回答別紙 6「顧客データダウンロードログ」を添付し、システム基盤切替以前 2016 年 2 月から 2020 年 7 月までの全 642 行のログ（以下「本件提出ログ 2」という。）を 6 月 1 日回答とともに提出した。

また、A 社は、5 月 25 日追加質問において、保守拠点である本件保守拠点での現地確認を希望する旨を要請したが、本件調査担当者らは、本件保守拠点には他社から委託を受けた機密情報等があることを理由に、BS の社屋等規程ルールに基づき当該要請を受け入れなかった。

6 月 1 日回答の後、A 社の J 取締役は、2022 年 6 月 3 日に C 担当部長に対し、「…あと、昨日 C 担当部長[39]にお問い合わせさせていただいた、旧システム廃棄（未廃棄）の件ですが、予定では 7 月の廃棄予定になっていますが、6 月中は保管されるということでよいでしょうか。この件、社内で確認中ですが、保全のご協力についてご相談させてください。」とのメールを送信した。また、2022 年 6 月 10 日には「…昨日お電話させていただいた 2 件につきまして、改めてメールさせていただきます。…②あと旧システム廃棄の件、保全のご協力をお願いしたこと。…」とのメールを送信し、同年 6 月 24 日にも同趣旨のメールを送信した。

[37] 元の回答では、本件保守拠点の名称が記載されている。
[38] 元の回答では、特定の文字列が記載されている。
[39] 元のメールでは、C 担当部長の苗字が記載されている。

エ　7月1日回答及び本件ウェブ会議の実施

A社のJ取締役は、C担当部長に対し、2022年6月24日、別紙6-6記載の各質問をメールで送付し、本件調査担当者らは、同年7月1日、同別紙記載のとおり回答した。

7月1日回答において、本件調査担当者らは、XとF担当課長を含むPDSサーバのデータにアクセスできるシステム管理者4名について、各担当者が現職であるかすでに離職しているかという質問（質問11後段）に対し、「上記システム管理者4名については、現在在籍しておりますが、本担当からは外れております。」と回答した。

また、本件調査担当者らは、「前システムのハードディスクをフォーマットされた日時の記載がありませんでしたが、いつ実施されたかをPDSサーバー毎に教えていただきたいです。」との質問に対し、「サーバ撤去日（2月21日）の1週間後に全サーバのハードディスクをフォーマット化しております。」と回答した。

そして、前記のとおり、同日には、A社と本件調査担当者らによる本件ウェブ会議が実施された。A社からは、J取締役及びK取締役のほか、システム関係者や営業担当者ら数名が出席し、本件調査担当者らは4名全員が出席した。C担当部長は、本件ウェブ会議に先立ち、J取締役に対し、「弊社メンバーはC担当部長、D担当課長、新旧のシステム管理者の4名を考えております」と伝えていた。本件ウェブ会議では、主に本件ネットワークのシステム関係の専門的事項に関するやり取りが行われ、本件調査担当者らのうち、この点について知識があったF担当課長が主に回答した。

オ　7月15日回答

本件ウェブ会議において、A社より別紙6-7記載の各質問が寄せられ、同別紙記載のとおり回答した。

6　本調査において発見された本件過去調査における不適切回答及びその理由・経緯

⑴　本件調査担当者らによる調査及び回答の問題点

以上のとおり、本件調査担当者らは、本件過去調査において、A社に対し、4月15日回答、4月18日回答、4月21日回答、5月11日回答、6月1日回答、7月1日回答及び7月15日回答の合計7件の回答を提出している。しかしながら、以上の回答の前提として行われた調査には多くの懈怠があり、回答自体にも、ログの改変、USB

ポートの設置状況と暗号化ソフトの導入状況に関する虚偽回答、本件体制変更依頼に対する虚偽回答、データ消去の状況に関する虚偽回答及び保守の作業体制に関する虚偽回答といった極めて重大な問題点が多数含まれている。

かかる対応が「調査」には似ても似つかない極めて杜撰な「作業」であり事なかれ主義的な対応を繰り返す極めて不適切なものであることは第６・２で述べたとおりである。本件調査担当者らは、杜撰なログ調査の結果、保守用アカウントからは、テスト環境によるキャンペーン出力結果しかない、すなわち顧客データが含まれていないテスト用キャンペーンに含まれるデータ（ダミーデータ）のエクスポートしか確認されなかったという自分たちの調査結果を最大かつ唯一の拠り所とし、本件調査担当者らが本件過去調査の重要性を理解せず本件調査依頼を非常に軽視していたという事情や、エクスポートログの内容や回答内容についての詳細な説明や A 社からの追加質問を回避したいという意図もあり、ログの開示範囲を限定していった。しかし、後記のとおり、本件調査担当者らが最大の拠り所としたログ調査の結果は、ログの誤読によって生まれたものであった。そうであるにもかかわらず、本件調査担当者らは、ログの誤読に気付かぬまま誤読に基づく調査結果に依拠して、以降、複数の場面で本件過去調査に誠実に対応せず、BS における情報セキュリティ管理体制の不足を隠蔽するため、A 社との取引を継続するため又は A 社からの更なる質問をかわすために、不都合な質問に対して虚偽の回答を繰り返した。

⑵　ログの改変及びこれに至る経緯（5 月 11 日回答・6 月 1 日回答）

ア　主なログの改変内容

本件過去調査において、本件調査担当者らは、BS の保守者によるエクスポートログを提出しているが、当該ログには、ダウンロード件数の削除、同一日に複数履歴がある場合のダウンロード履歴の大幅な削除及び IP アドレスの書き換え等といった問題点がある。以下、これらのログの改変に至る経緯について詳述する。

イ　ログの改変に至る経緯

5 月 11 日回答の対象となった「ONE CONTACT Network 環境および前システム環境における、ネットワーク外へのデータ取り出し方法と、データ取り出しできるシステム管理者の範囲と人数、対象者の氏名」の質問（質問 3）は、必ずしも直接的に顧客データのエクスポートログの提出を求めるものではない。しかし、C 担当部長は、本件過去調査の早い時期から、内部からの情報流出の有無を確認するためにはログの確認が直截であると考えており、その意識は E 担当課長にも共有さ

れていた。そして、C 担当部長及び E 担当課長は、前月の 2022 年 4 月の時点で A 社からログの保管期間等ログに関連する質問が複数寄せられていたところに「ネットワーク外へのデータ取り出し方法と、データ取り出しできるシステム管理者」に関する質問が寄せられたため、内部からの情報流出がないことを報告するには、システム管理者の顧客データダウンロードログを提出すべきであると考えるに至った。

F 担当課長は、2022 年 4 月 29 日、E 担当課長との社内チャットで、A 社からの上記質問 3 を含む質問 7 点（別紙 6-4）の内容を知らされた上で、当該質問事項に関連する問い合わせメールを B 社担当者宛てに送信するよう依頼されたことから、これに応じて、E 担当課長が作成した文面のとおり B 社担当者宛てに送信した。もっとも、F 担当課長は、当時の受け止め方として、A 社からの質問はシステムの保守者の作業内容をどのように管理しているかを問う趣旨であり、エクスポートログはあくまでも参考として添付することが求められているという認識が強かったと述べるとともに、まさか内部からの情報流出があるとは思っていなかったと述べている。

E 担当課長は、同年 5 月 2 日、上記質問事項への回答対応の一環として、F 担当課長に対して、「吉報になります。PDS 画面を触る行為とデータをエクスポートする行為については、同じ ID、PASSWORD になりますが、X[40]さんに聞いたところ、保守用の ID、PASSWORD を利用しているようです。なので、ログについてはこの保守用を調査すればと思いました」とチャットを送信し、「なるべく内々に動きたく、(※当調査委員会注：情報漏えいに関する調査を行っている旨の情報が) F 担当課長[41]止まりにて、上手く立ち回って頂けると幸いです私も X[42]への確認等は極力、ISMS 監査対応で、お仕切ろうと思ってます。」（原文ママ）と依頼した。

BS の保守運用担当者が利用していた保守用 ID は、テレマーケティングの委託元及び案件内容に応じて設定されるテナントごとに割り当てられているが、いずれも ID に特定の文字列の表記を含むものであるところ、F 担当課長は、同日（5 月 2 日）、E 担当課長からの連絡に基づき、B 社担当者に電話して、「ISMS 監査対応のために、PDS サーバ 4 台の A 社のテナントについて、全てのキャンペーンそれぞれのエクスポートログのうち、ユーザーID に特定の文字列を含むものを抽出して、一覧化してほしい」旨を要請した。

A 社の J 取締役は、同年 5 月 9 日、C 担当部長に対し、調査内容及び項目について尋ねる旨のショートメッセージを送信し、C 担当部長は、これを E 担当課長の私用携帯に転送した。E 担当課長は、同年 5 月 9 日午後 3 時 1 分、C 担当部長

[40] なお、社内チャット原文においては、X の苗字が記載されている。
[41] 社内チャット原文においては、F 担当課長の苗字が記載されている
[42] 同上。

に対し、「何となくですが、先方もかなり焦っているのでは、と感じました。キチンと回答すべく、部長とお話したとおりアクセスログを出して、何もないことを、証明できればと思っております。」とのショートメッセージを送信した。

B 社担当者は、ゴールデンウィーク明けの同月 9 日午後 10 時 53 分、F 担当課長に対して、前記の問い合わせ事項への回答及び前記の要請に対応する 2015 年 8 月以降のログ情報をいずれも含むエクセルファイルをメールで送信した。

当該ログ情報は、この時点で既にユーザー操作が記録されたログファイルそのものではなく、ログファイル中の情報を、前記エクセルファイル中の「顧客ダウンロード」と題する 1 つのシートのみに集約して転記した上で、テナント ID、IP アドレス、日時、ユーザーID、処理 ID 及びキャンペーン ID の 6 つの項目名を付して、テナント ID＞日時の順にソートをかけたものであった（以下「本件 B 社提供ログ」という。）。

【本件 B 社提供ログの冒頭（抜粋）】

F 担当課長は、同月 10 日、B 社担当者に電話で質問し、前記「処理 ID」欄の記載内容が「顧客データを CSV ファイルにエクスポートする処理をした」旨を意味することについて説明を受けるとともに、前記「キャンペーン ID」欄の記載内容に「当該エクスポート処理を行ったことと、これによって出力されたデータ件数」「キャンペーン ID」「レポート名」が含まれるという説明を受けた。F 担当課長は、本件 B 社提供ログを確認した際の心境として、社外に対して、このような内部の雑多な作業内容が示された資料を開示する必要が本当にあるのか疑問に思ったと述べている。

F 担当課長は、同日中に E 担当課長と電話で話をして、エクスポートログの記載内容について説明した。そして、F 担当課長は、本件 B 社提供ログには、保守用 ID を共有している ProCX のコンタクトセンタの SV 等によるエクスポートログ

も含まれていると考えられることから、システム管理者によるエクスポートのみを抽出する方法として、「レポート ID」欄に「ネオメイト」「NEO」「TEST」等が含まれるもののみを抽出すればよいと判断した[43]。その後、E 担当課長は、F 担当課長からの説明を受けて、5 月 11 日回答の質問 3 に対する回答に「PDS サーバの定期メンテナンス時において、システム管理者がデータを出力したか否かの痕跡を調査した結果、別紙 1（※のちに別紙 2 に訂正されている。）のとおり、当社テスト環境によるキャンペーン出力結果しかございませんでした。」と記載し、2022 年 5 月 10 日の午前 11 時 56 分頃、これを F 担当課長にメールで送信した。

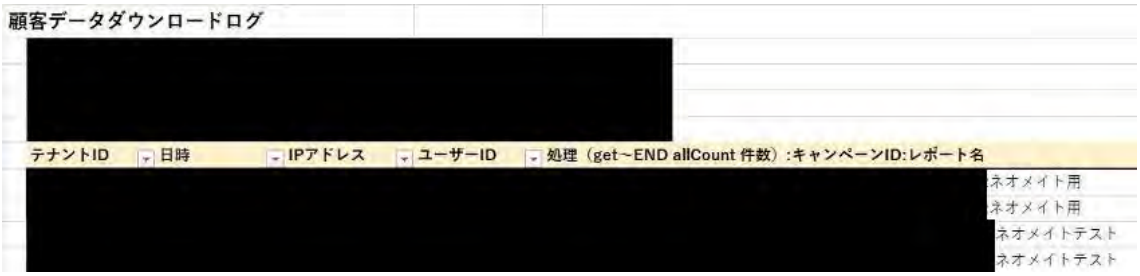
その後、F 担当課長は、前記「顧客ダウンロード」シートに次の 4 点の内容変更を加えて、これを「別紙 1_システム管理者ログ」と題するエクセルファイル内に格納した。F 担当課長は、2022 年 5 月 10 日午後 12 時 6 分頃、当該エクセルファイルを E 担当課長宛てにメールで送信するとともに、当該メール中で「システム管理者ログを添付します。G 列（※「処理（get～END allCount 件数）：キャンペーン ID：レポート名」欄の意）を見ていただくと「ネオメイト」や「TEST」等によるものだけです。顧客ダウンロードの方は結構な数です。」と説明した（ログの改変作業を以下「第一次改変」といい、第一次改変後のログを「第一次改変後ログ」という。）。

【第一次改変の内容】

- 「処理 ID」欄を全て削除する
- 「日時」欄と「IP アドレス」欄の順序を入れ替える
- 「キャンペーン ID」欄の名称を「処理（get～END allCount 件数）：キャンペーン ID：レポート名」に変更する
- 「レポート ID」に「ネオメイト」「NEO」「TEST」「B 社」が含まれるもののみを残して、それ以外のダウンロード履歴を全て削除する

【第一次改変後ログの冒頭（一部抜粋）】

[43] なお、F 担当課長がそのように判断した理由について、同担当課長は、E 担当課長が、X に対して、保守者によるテスト実施時に通常どのような名称を付するのか尋ねたところ、X が「TEST」等の名称を付けると回答したためであると述べるが、E 担当課長はそのような記憶はないと述べている。後記のとおり、E 担当課長は、ログの改変作業の過程である 2022 年 5 月 10 日午後 1 時 26 分頃、「先程の件の更問」として X にエクスポートログについて質問するメールを送信していることから、当該メールの以前に、E 担当課長及び X 間でエクスポートログないしエクスポートに関する何らかのやり取りがなされていた可能性はあるものの、F 担当課長も E 担当課長もエクスポート操作の実情を把握しておらず、「『TEST』という名称が付されるのは、通常、保守者によるテスト実施時のことだ」という判断が単なる推測であった可能性も十分にあるため、上記のようなやり取りの存在及びその内容を事実として認定できるまでには至っていない。



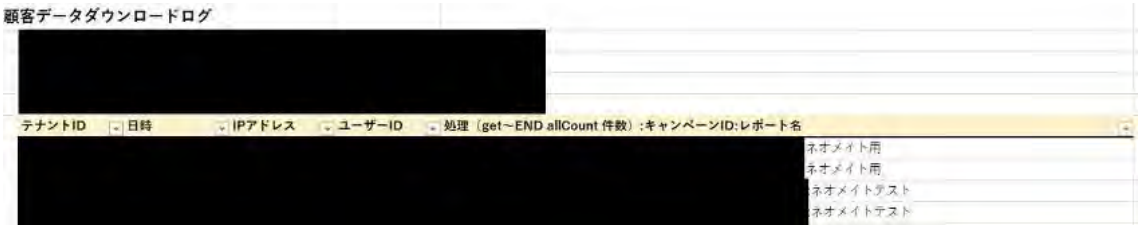
F 担当課長は、E 担当課長と電話で話をした後、A 社からの質問における「システム管理者」は BS の保守者であって B 社（ベンダ）は含まれないとの解釈に基づき、前記「システム管理者ログ」ファイルから、「レポート ID」に「B 社」が含まれるダウンロード履歴を全て削除して「別紙 1_システム管理者ログ_2」というファイル名に変更した上で、同日午後 1 時 34 分頃、これを E 担当課長宛てにメールで送信した（ログの改変作業を以下「第二次改変」といい、第二次改変後のログを「第二次改変後ログ」という。）。

【第二次改変の内容】

・ 「レポート ID」に「B 社」が含まれるダウンロード履歴を全て削除

【第二次改変後ログの冒頭（一部抜粋）】

※冒頭部分は、第一次改変後ログの冒頭と変化がないが、「レポート ID」に「B 社」が含まれるダウンロード履歴を全て削除したことによって、全体のボリュームが減少している。



他方、E 担当課長は、X に対し、同日午後 1 時 26 分頃、以下のメールを送信した。

「先程の件の更問となりますが、顧客データダウンロードのアクセスログとして・テナント ID・日時・IP アドレス・ユーザーID・処理（get～END allCount 件数）:キャンペーン ID:レポート名

↑

処理内に記載されてる件数が何を指すのか教えていただきたく。カラム数という認識でよいのかな？よろしくお願いします。」

X は、これに対し、同日午後 2 時 55 分頃、「顧客データダウンロードのアクセスログですが、〈B 社担当者〉[44]に問い合わせたところ、データの件数との事でした。」と返信した。F 担当課長は、E 担当課長と電話で話をした後、前記「システム管理者ログ」ファイルから、「(get～END allCount 件数)」との表示と、これに対応する数字（ダウンロード件数を指すもの）を全て削除して、「別紙 1_システム管理者ログ_3」にファイル名を変更した上で、同日午後 3 時 10 分頃、これを E 担当課長宛にメールで送信した（ログの改変作業を以下「第三次改変」といい、第三次改変後のログを「第三次改変後ログ」という。）。このようなダウンロード件数を削除した理由について、F 担当課長は、A 社の質問の趣旨はシステムの保守者の作業内容をどのように管理しているかという点にあると理解していたところ、システム管理者の操作内容が説明できるログを提出すれば足り、テスト環境での操作においてダウンロード件数の表示は不要と判断したと述べている。

【第三次改変の内容】

- 「(get～END allCount 件数)」との表示と、これに対応する数字（ダウンロード件数を指すもの）を全て削除

【第三次改変後ログの冒頭（一部抜粋）】

同日午後 4 時頃から、C 担当部長、E 担当課長及び D 担当課長が出席して 5 月 10 日電話会議が開催された。C 担当部長は、5 月 10 日電話会議の場あるいはその前に、エクスポートログには、保守者によるテストのダウンロード結果はあったが、顧客データの大量ダウンロードの痕跡はなかったとの報告を受けた。5 月 10 日電話会議の場あるいはその直後、C 担当部長及び E 担当課長の間で、現状のエクスポートログ（第三次改変後ログ）を全部 A 社に提出するか否かが話題に上った。その際、C 担当部長は、内部からの情報流出の形跡がないのであれば、特徴的なところだけ抜粋してエクスポートログを提出することでよいのではないかといった発言をした。

[44] 元のメールでは、B 社担当者の苗字が記載されている。

その後、F 担当課長は、E 担当課長と電話で話をした上で、前記「システム管理者ログ」ファイルについて、次の内容変更を加え、「別紙 2_システム管理者ログ」にファイル名を変更した上で、同日午後 8 時 41 分頃、これを「見直したログ」であるとして E 担当課長宛てにメールで送信した（ログの改変作業を以下「第四次改変」といい、第四次改変後のログを「第四次改変後ログ」という。）。

F 担当課長は、第四次改変において、同一日のダウンロード履歴のうち冒頭の 1 件のみを残して他のダウンロード履歴を全て削除した理由について、開示資料の量が多いためこれを減らす目的があったと述べており、前記の C 担当部長の発言が E 担当課長経由で F 担当課長に伝えられたとみられる。また、F 担当課長は、前記のとおり、元々A 社の質問の趣旨はシステムの保守者の作業内容をどのように管理しているかという点にあると理解していたところ、どのような形でログを残しているかということを示せれば足りると考えたとも述べている。他方、IP アドレスの改変については、5 月 11 日回答において本件保守拠点に保守用端末があるという回答案が既に作成されていたところ、当該回答との整合性を持たせるべく、他拠点（福岡）の保守用端末や過去使用していた保守用端末の IP アドレスを、現行の本件保守拠点の保守用端末の IP アドレスに敢えて書き換えている。なお、2020 年 8 月以降のダウンロード履歴のみを残して、それ以前のダウンロード履歴を全て削除した点については、新基盤切替後のログに限定する趣旨である。

【第四次改変の内容】

- 「日時」欄の記載上、同一日のダウンロード履歴につき、冒頭の 1 件のみを残して、他のダウンロード履歴を全て削除する
- 「IP アドレス」欄につき、その記載内容を全て本件保守拠点に所在する保守用端末の IP アドレス）となるよう変更する
- 「日時」欄の記載上、2020 年 8 月以降のダウンロード履歴のみを残して、それ以前のダウンロード履歴を全て削除する

【第四次改変後ログの冒頭（一部抜粋）】

第四次改変の後、E 担当課長は、同日午後 8 時 51 分、第四次改変後ログ等を含

む回答資料を以下の本文とともに C 担当部長及び D 担当課長にメール送信した。なお、メール本文には、エクスポートログに対する第四次改変の作業内容に関する記載はない。

「本日ご指摘頂きました点について、資料修正致しましたのでご報告いたします。
＜修正点＞
1．情報セキュリティにおける組織上のメンバーを追記
＃ISMS 管理責任者（本社・各エリア）を記載
＃B 社[45] ベンダ名は削除
2．保守端末の取扱いについて、資料化
＃どういうときに、PDS サーバへアクセスするか、
限られらた権限を持った実施者・ルール条件等を記載」

D 担当課長は、これに対し、翌 5 月 11 日午前 10 時 28 分、「＜E 担当課長へ[46]確認させてください＞・PDS 出力のログはテストデータのみを確認とありますが、別紙 2 は PDS から保守用端末への出力ログで、PDS から保守用端末への出力は可能、保守用端末は USB ポート無し、暗号化ソフトで情報取出しが不可という理解で合っていますでしょうか？」と返信した。E 担当課長は、これに対し、同日午前 10 時 34 分、「ご認識のとおりです。テナント毎（拠点）の専用 ID/Password を使用、切替利用することで出力は可能ですが、まず、ログ結果からは、ダウンロードした痕跡がなかったこと。加えて保守用端末は USB ポートなし、暗号化ソフトによる取出し不可となっております。」と返信した。

その後、D 担当課長は、同日午前 11 時 34 分、A 社の J 取締役に対し、第四次改変後ログ等を含む最終の回答資料をメール送信した[47]（すなわち、第四次改変後ログと、本件提出ログ 1 は同内容である。）。

その後、2022 年 5 月 25 日、本件提出ログ 1 について、「前システムのログは御座いますか？また、フィルターが掛けられていると思うのでどのような内容でフィルターが掛かった状態でしょうか？」との質問（6 月 1 日回答 3②）に対し、本件提出ログ 2 を提出するとともに、「フィルターについては、新システム（ONE CONTACT Network）への移行分のみサンプル抽出したこと、又、管理者用 ID（〈特定の文字列〉[48]を含む ID）のみに絞らせていただきました。」と回答し、第一次改変ないし第四次改変の作業内容の詳細を回答しなかった。本件提出ログ 2 についても、本件提出ログ 1（第四次改変後ログ）と同様の改変が施されているが、ログ

[45] 元のメールでは、B 社の名称が記載されている。
[46] 元のメールでは、E 担当課長の苗字が記載されている。
[47] なお、外部メールアドレスへの添付ファイルの承認手続に時間がかかり、A 社の J 取締役に添付ファイルの解凍パスワードを送信したのは、同日午後 12 時 33 分であった。
[48] 元の回答では、特定の文字列が記載されている。

の期間は、新基盤切替以前の 2016 年 2 月から 2020 年 7 月分までとなっている。

ウ　ログに対する本件調査担当者らの調査内容及び認識

（ア）総論－本件調査担当者らがログに対する分析・評価を誤ったこと

以上のようなログの改変内容（特に、ダウンロード件数の削除、同一日の履歴の一括化及び IP アドレスの変更等）に照らし、当調査委員会は、本件調査担当者らが内部からの情報流出を認識しつつこれを意図的に隠蔽したのではないかという観点から検証を実施した。

しかし、実態としては、以下に述べるとおり、むしろ本件過去調査において、本件調査担当者らは全く十分な調査を実施できておらず、F 担当課長が「キャンペーン ID」や「レポート名」の意味を取り違えてログに対する分析・評価を誤ったことにより、内部からの情報流出に気付くことすらできていなかった。すなわち、F 担当課長は、本件過去調査当時、エクスポートログ上の「キャンペーン ID」との項目中にみられた「ネオメイト」や「ネオメイトテスト用」等の記載は「レポート名」である旨の説明は受けたものの、その意味や詳細までは把握できていなかったため、「レポート名」が「出力条件 ID」（エクスポート時に当該エクスポート条件を指すものとして、エクスポート操作を行う者が任意に付することができる名称）を指すものだと理解することができず、「キャンペーン ID」に対応するものである「キャンペーン名」であって、保守担当者によるテスト用である旨が表示されたもの（テスト用のダミーデータが格納されたキャンペーンであることを示す名称）であると誤解した結果、BS の保守者によるダウンロードの形跡はあるが、これらは通常の保守作業の過程で生じるものであり、顧客データではないダミーデータがダウンロードされたものであるから内部からの情報流出はない、と極めて短時間のうちに結論付けていた。

（イ）本件調査担当者らがログに対する分析・評価を誤った過程

BS では、保守担当者が用いていた PDS サーバの ID は、複数名によって共用することができるよう、容易に推測できる ID・パスワードが設定されており、事実上、ProCX 社の各コンタクトセンタの SV が用いることも多くあった。そのため、本件 B 社提供ログにも、「納品データ用サプリサンプル」、「（氏名）コール検証」、「コンタクト件数」等といった、SV による操作であることを強く示唆する記載があるダウンロード履歴が多く含まれていた。前記のとおり、この記載は「出力条件 ID」として、エクスポート操作時に当該エクスポート条件を指

すものとして任意に付することができるものである。

本件過去調査においてログの分析を担当した F 担当課長は、エクスポートログから保守担当者によるダウンロード履歴を把握することを求められていたところ、本件 B 社提供ログにおいて、保守担当者によるエクスポートか否かを判別する手掛かりとなり得るのは、「レポート名」以外にはなかった。そして、保守担当者による操作であることを示唆する「レポート名」としては、「ネオメイト」や「TEST」を含むものがみられたため、これらはいずれも保守担当者がテスト用のキャンペーンから出力したレポートであることを示すものであって、保守担当者による出力は全て「テスト用キャンペーン」として格納されたダミーデータの出力だけであると、ごく短時間のうちに結論づけた[49]。

しかしながら、ここでいう「レポート名」は、当初「キャンペーン ID」という項目の中で、キャンペーン ID と並んで記載されていたものではあったものの、キャンペーン ID と結びつくキャンペーン名（テスト用のダミーデータが格納されたキャンペーンに付された名称）ではなく、出力条件 ID（エクスポート操作を行う者が、当該エクスポート条件に対応するものとして任意に付けられる名称）であって、エクスポート作業の対象が何であるかを保証する意味までは持たないものであった。すなわち、レポート名が「TEST」等の保守担当者によるテスト作業の存在をうかがわせる名称であるからといって、エクスポートされた対象となるデータがテスト用データであることを示すとは限らず、本来的には、エクスポートの対象となったキャンペーン名や当該キャンペーンに含まれる情報の内容を確認する必要があったが、F 担当課長は、本件過去調査においてこの点を確認していない。また、このエクスポートログには、「(get～END allCount 件数)」との表示において、非常に多数の情報の出力履歴が示されていることから、これが全てテスト用に実施された正当なエクスポートであったか否かを判断するためには、本来、保守者の作業記録と突合する必要があったが、F 担当課長がこの点を具体的に検討した形跡はなく、いずれもテスト環境によるダウンロードしかないと結論付けていた。

これは、F 担当課長がレポート名とキャンペーン名の違いを十分に認識していなかったために生じたものであると思われる。F 担当課長は、本件過去調査において、自ら PDS サーバを操作してエクスポートログを出力することをせず、これをベンダに委ねた上で、エクスポートログの項目の意味について、エクスポート操作を行う際の画面表示などを確認することもなく、各項目の意味について質問した際に、一言で要約した場合の意味内容というごく初歩的な理解にしかつながらない回答を得るに留まっている。しかし、F 担当課長は、日常的に PDS

[49] そのうち、「＊＊TEST」という出力条件 ID は、X のイニシャルと TEST を組み合わせたものと考えられる。実際の出力条件の記載では「＊＊」にアルファベット 2 文字が入る。

サーバの保守運用業務に携わっていたわけではなかったことに加えて、PDS サーバのウェブアプリケーションを実際に操作して、顧客データのエクスポートを実行した経験がなかった。それゆえ、本件過去調査の当時、F 担当課長が、レポート名が出力条件 ID を意味するものであり、これがキャンペーン名と異なるものを指すということを正しく理解していたとは考え難く、F 担当課長も理解を有していなかったと述べる。

また、F 担当課長が最初に目にしたエクスポートログである本件 B 社提供ログには、レポート名その他の情報を含む項目名として、一括して「キャンペーン ID」との記載があった。当該項目中の情報には、キャンペーン ID（各キャンペーンを特定するために付される英数字の組み合わせをいう。）が含まれていたため、レポート名がキャンペーン ID と関連づけられるものであることを印象づけるような記載があったことも、このような F 担当課長による誤解を招いた一因となった可能性がある。F 担当課長は、「キャンペーン ID」との項目に、「レポート名」が含まれることについてベンダの営業担当者から口頭で説明を受けて、自らも第一次改変においてその旨を項目名に記載しているが、前記のとおり、「キャンペーン ID」(から想起されるところのキャンペーン名)と「レポート名」の相違を明確に認識できるだけの前提知識を有していたとは考え難い。このように、F 担当課長は出力条件 ID の意味を正しく理解することを可能とするようなベンダとの共通認識を持っておらず、むしろ、出力条件 ID の意味を誤解することが十分に想定できる状況にあった中で、当初の本件 B 社提供ログに「キャンペーン ID」というキャンペーン名を想起させるような記載があったことで、本件 B 社提供ログ記載のレポート名を、キャンペーン名であると誤解した可能性が指摘できる。

加えて、PDS サーバの運用に当たって、保守者において PDS サーバが正しく動作するかをテストすべき場面があり得るところ、F 担当課長は、顧客データのダウンロードのテストをどの程度の頻度で行う必要が生じるかといった具体的な事情を全く把握していなかった。そうすると、F 担当課長が、「システム管理者ログ」として、「ネオメイト」や「TEST」を含む履歴のみを抽出する作業を行った際に、これが「保守担当者によるテスト行為」によるダウンロード履歴であり、ダミーデータのダウンロードを示すものだと誤解したことも十分に想定される。

また、エクスポートログについては、F 担当課長以外に E 担当課長も内容の検討をしているが、E 担当課長が F 担当課長以上の PDS サーバのエクスポートログの項目の意味を理解するだけの知識を有していたとは認められない。また、E 担当課長においても、前記第４・２（2）ア記載のとおり、X を含む BS の保守者が、PDS サーバの運用・保守の場面でテストを実施し、データを適切にエ

クスポートできるかを確認することはあるだろうと認識していたものの、具体的にどのような場面でダウンロードの必要が生じるかについては全く把握していなかった。このことからすると、E 担当課長が F 担当課長による上記誤解に気付くことはなかったと思われる[50]。

以下では、このような F 担当課長によるログに対する分析・評価の誤りが生じた背景事情について述べる。

（ウ）ログに対する分析・評価を誤った背景事情－分析を行うだけの前提情報や時間的余裕の不足等

そもそも、BS では、PDS サーバからの顧客データのエクスポートについて、定期的にログを取得することをしておらず、かつ、これと対照すべき BS 保守担当者の作業記録も残していなかった。そのため、本件調査担当者らは、PDS サーバのエクスポートログの取得方法及びエクスポートログにどのような情報が含まれているかを全く把握しておらず、また、X を含む BS の保守者が PDS サーバについて実施した作業の記録を参照することもできない状況にあった。

また、PDS サーバから顧客データをエクスポートする際には、PDS サーバのウェブアプリケーションから出力すべき顧客データを検索によって抽出し、任意の「出力条件 ID」（レポート名）を入力した上で、出力のためのボタンを押下するという操作を行うところ、エクスポートログに含まれるのは、これらの操作に対応したデータであるため、実際に PDS サーバから顧客データのエクスポートを実行した経験があれば、それ以上の情報がなくても、エクスポートログの「レポート名」が出力条件 ID を指すものであるとの判断に至り得たと考えられる。しかし、F 担当課長は、そもそも日常的に PDS サーバの保守運用業務に携わっていたわけではなく、BS 社内でも、PDS サーバのウェブアプリケーションを実際に操作して、顧客データのエクスポートを実行した経験に富む者は、ごくわずかにとどまっていた[51]。そのため、エクスポートログの内容を正確に理解するためには、BS の保守者又は B 社担当者に対してエクスポートログの記載内容の詳細を確認することが必須の状況であったが、そのような確認を行った形跡はない。すなわち、本件過去調査の当時、F 担当課長は、エンジニアとしてシステムの一定の知識・素養・経験があったものの、 PDS サーバの保守運用におけるエクスポートログの検証を行うに足りるだけの材料や情報を十分に有してい

[50] なお、本調査において、X が「TEST」等の出力条件 ID を付するにとどまらず、敢えて「テストとしてダウンロードを行っていた」旨の虚偽説明を本件調査担当者らに直接・間接に行ったことを具体的に示す証跡までは見当たっていない。

[51] 具体的には、X の他、PDS サーバの保守運用業務に関与していたバック SE3 名の合計 4 名に限られていた。

ない状況であった。そして、E 担当課長についてもこの点は同様であった。実際、本調査において、BS のバック SE として本件システムの保守運用に携わりつつも、PDS サーバウェブアプリケーションを使用した経験が限られている 2 名に対し、本件 B 社提供ログを提示したところ、出力条件 ID の記載はキャンペーン名であると誤解することもあり得ることが確認された[52]。

また、本件過去調査において、F 担当課長に与えられたログの分析時間が極めて短時間であったことも、このようなログの誤読を招いた一因であったことが指摘できる。つまり、上記のとおり、本件過去調査は有効な調査を行う前提を欠いていたにもかかわらず、本件調査担当者らは、この点について特段の考えを巡らせることなく、2022 年 4 月 28 日に A 社から質問を受領した後、ゴールデンウィーク明けすぐ（同年 5 月 11 日）の回答をめざしていた。暦日上は、日数があるように思えるが、営業日ベースでいうと、実際には質問を受領した時点で提出日まで数日程度しかなかった。とりわけ、エクスポートログについては、ゴールデンウィーク空けの 2022 年 5 月 9 日又は 10 日に B 社から入手し、その内容を踏まえた回答を同月 11 日に行うことが計画されており、実際に F 担当課長が本件 B 社提供ログを受領したのは同年 5 月 9 日の深夜 11 時頃であった。そのため、エクスポートログを取得してその内容を検討した F 担当課長は、そのような短期間で対応するために都合のよいようにログの内容を解釈するよう、無自覚のうちに動機づけられていたと見られても仕方のない状態にあったとさえいえる。

そして、本件過去調査において調査の方向性等を指示する立場にあった C 担当部長は、本件過去調査におけるログ確認の重要性を認識していた一方で、自身はエクスポートログの内容について分析できるだけのシステムの知識・素養・経験を欠いており、F 担当課長の分析を基にした E 担当課長らの報告を鵜呑みにしているだけで、特にエクスポートログの記載内容を確認することはなかった。そのような客観的な状況に照らせば、本件過去調査では、より適切な人員を調査に加えるか、少なくとも本件調査担当者らが有意義な調査を行えるだけの材料や情報を収集できるような体制を整え、さらにそれができるだけの時間的余裕を与えた上で、PDS サーバのエクスポートログに対する適切な検証を実施させるべきであった。しかし、本件過去調査において、C 担当部長をはじめとする本件調査担当者らが、このような問題について認識ないし検討した形跡は一切な

52 なお、本調査において、PDS サーバのウェブアプリケーションを多数回使用した経験のある BS の保守者（第４・２（1）で言及したバック SE チームの PDS サーバの有スキル者である派遣社員）に対し、エクスポートログのレポート名の意味を問うた際、同担当者も当初これをキャンペーン名であると誤解した。同担当者は、「レポート名」は、キャンペーン名とは異なり、エクスポート時に付される名称ではないかとの指摘を受けて、これが出力条件 ID を指すものと理解して認識を訂正したが、このような経過は、エクスポートログのレポート名の意味内容が有スキル者にとっても一読了解でないことを示唆している。

く、むしろ C 担当部長は、E 担当課長にはエクスポートログの分析を行うだけの能力があると信じ、5 月 11 日回答の時点で、E 担当課長がログの検討をした結果、内部からの情報流出の形跡がないというのであれば問題ないとさえ考えていた。

エ　ログの改変に対する評価

（ア）ログの改変に至った背景事情

以上のとおり、本件過去調査において、F 担当課長がログに対する分析・評価を誤ったものと認められるが、そこからさらにログの改変が行われた背景には、そうしたログの誤読によって内部からの情報流出がないという誤った結論があったことに加え、そもそも本件調査担当者らが本件過去調査の重要性を理解せず本件調査依頼を非常に軽視していたという事情や、エクスポートログの内容や回答内容についての詳細な説明や A 社からの追加質問を回避したいという意図もあったと考えられる。

例えば、前記のとおり、F 担当課長は、当調査委員会に対し、ログの改変を実施した理由について、当時の A 社の質問の趣旨はシステムの保守者の作業内容をどのように管理しているかという点にあると理解していたところ、システム管理者の操作内容が説明できるログを提出すれば足りると理解していたと述べる。顧客データの漏洩が問題となっている状況においてエクスポートログを分析する意義は、まさに不正の形跡がないか否かの検討の点にあるところ、当調査委員会としてこのような F 担当課長の認識を文字どおり受容することはできないが、まさか内部からの情報流出があるとは思っていなかったと F 担当課長が述べている点と合わせて考えれば、少なくとも、F 担当課長が、本件過去調査の当時、本件調査依頼の切実さや事の重大さを全く理解していなかったことは窺い知ることができる。そして、前記のとおり、5 月 11 日回答の当時、A 社と直接連絡をとっていたのは C 担当部長であり、その時点では C 担当部長は F 担当課長が本件過去調査に関与していたことを認識していなかったため、A 社の意向等が、C 担当部長と E 担当課長を経由して F 担当課長に伝えられていたことに照らせば、間に複数人を挟んだことによって、F 担当課長が緊迫感をもって事態の深刻さを捉えることができなかった可能性は否めない。

他方、C 担当部長及び E 担当課長は、エクスポートログを提出する意義は一定理解していたはずであり、A 社の窮状や事態の深刻さは感じていたはずであるが、E 担当課長は F 担当課長と相談しながらログの改変に関与し、C 担当部長も 5 月 10 日電話会議の場あるいはその直後に開示範囲を限定する方向での発

言をしている。この点については、内部からの情報流出の形跡がないという誤った分析結果が基にあるとはいえ、やはりエクスポートログの内容や回答内容についての詳細な説明や A 社からの追加質問を回避したいという意図があったと思われる。

したがって、本件調査担当者らによるログの改変については、内部からの情報流出の形跡がないという誤った分析結果を基に、総じて本件調査依頼を軽んじた結果行われたものということができる。

（イ）ログの改変の有害性

エクスポートログの第一次改変ないし第四次改変は、A 社にとって無害なものもあれば、A 社にとって結果有害であったものも含まれる。例えば、第一次改変における処理 ID の削除については、単純に処理 ID が「顧客データを CSV ファイルにエクスポートする処理をした」ということを意味する文字の羅列に過ぎず、むしろそのようなエクスポートしたもののログであることが前提になっていたことから、不要な情報であるとして削除しても害のない加工であるといえる。

他方、第三次改変におけるダウンロード件数の削除や第四次改変における同一日のダウンロード履歴の大幅な削除（ダウンロード回数を読み取れなくする改変）については、システム保守者による作業内容を不透明なものとする加工であって、顧客情報の流出元の特定が課題となっている A 社にとって有害なものであったというほかない。また、第四次改変における IP アドレスの変更に至っては、5 月 11 日回答において本件保守拠点に保守用端末があるという回答をするという方針ありきで、他拠点（福岡）の保守用端末や過去使用していた保守用端末の IP アドレスを、現行の本件保守拠点の保守用端末の IP アドレスにわざわざ書き換えていることから、当時の調査や回答の不十分さを隠蔽する目的があったことが明らかだとはいえ、この点を踏まえると、本件過去調査の不十分さを隠蔽するためにログの改変が行われたとみられてもやむを得ない側面があることも否定できない。

そして、6 月 1 日回答の質問 3②において、本件提出ログ 1 についてどのようなフィルターが掛けられているのかという質問に対し、第一次改変ないし第四次改変の作業内容を詳らかにせずその一端のみを回答し、本件提出ログ 2 についても同様の改変を施して A 社に提出した点については、きわめて不正確かつ不誠実なものであったというほかなく、ここでもやはりエクスポートログの内容や回答内容についての詳細な説明や A 社からの追加質問を回避したいという意図があったものと考えられる。

⑶　USB ポートの設置状況と暗号化ソフトの導入状況に関する虚偽回答（5 月 11 日回答）

ログの改変については、ログの誤読とそれに基づく誤った開示範囲の限定という面があったが、5 月 11 日回答のうち、質問 3 に対してなされた「〈※〉　USB ポート無し、秘文ソフトウェアがインストールされた専用端末」の回答と、これと同趣旨を述べる「②保守用端末の構成については、物理的に USB ポートのない端末で暗号化ソフトにて情報漏えい対策を実施、データ取出し不可」（下線について原文ママ）（5 月 11 日回答別紙 1（2））という回答（以下、総称して「本件 USB ポート等回答」という。）については、本件調査担当者らのうち、C 担当部長、E 担当課長及び F 担当課長は、真実に反することを知りながら、虚偽の回答をしたものである。そのような虚偽回答をするに至った経緯及び理由は、以下のとおりである。

E 担当課長は、保守用端末で USB ポートは使用できないであろうと考えていたことから、質問 3 について、「尚、メンテナンス用 PC は、専用端末となっており、ハードウェア的にもソフトウェア的にも USB は利用できない環境としております…」との回答案（以下「本件 USB ポート等回答案」という。）を作成した。その後、E 担当課長は、保守用端末には USB ポートがあり、またこれを使える状態であったことを知った。C 担当部長は、2022 年 5 月 10 日頃、E 担当課長よりエクスポートログに大量ダウンロードの形跡がなかったとの報告を受けるとともに、保守用端末に USB ポートがあり、直ちに閉鎖することは難しいとの報告を受けた。C 担当部長は、質問 3 でネットワーク外への取り出し方法について質問されている以上、USB ポートの有無について回答する必要がある（もし USB ポートの有無について回答しなければ A 社から追加質問がくる）と考えていたところ、USB ポートが使える状態になっていると回答すると、適切な措置を講ずるまでの間、A 社との取引が停止されてしまうのではないかという危惧を抱いた。そこで、C 担当部長は、エクスポートログに保守者からの情報漏洩を推認させるような大量ダウンロードの形跡がなかった、つまり保守者からの情報漏洩がなかったのであれば、USB ポートの有無について虚偽の回答をしても、大勢に影響はないと判断した。そこで、C 担当部長は、E 担当課長に対し、本件 USB ポート等回答案を維持するよう指示した。E 担当課長は、F 担当課長に対し、同日頃、上記のとおり USB ポートはないと虚偽の回答をする旨の方針を知らせた。

そして、暗号化ソフトについても、実際は保守用端末に導入されていなかったが、同年 5 月 10 日から 5 月 11 日までの間に、USB ポートに関する記述とともに、暗号化ソフトが導入されているとの虚偽の回答を行う旨の方針が決まった。

なお、D 担当課長は、本件 USB ポート等回答が虚偽であることは把握していなか

った。実際、D 担当課長は、同年 5 月 11 日午前 10 時 28 分、E 担当課長に対し、「＜E 担当課長へ[53]　確認させてください＞・PDS 出力のログはテストデータのみを確認とありますが、別紙 2 は PDS から保守用端末への出力ログで、PDS から保守用端末への出力は可能、保守用端末は USB ポート無し、暗号化ソフトで情報取出しが不可という理解で合っていますでしょうか？」と質問している[54]が、E 担当課長は、これに対し、同日午前 10 時 34 分、「ご認識のとおりです。テナント毎（拠点）の専用 ID/Password を使用、切替利用することで出力は可能ですが、まず、ログ結果からは、ダウンロードした痕跡がなかったこと。加えて保守用端末は USB ポートなし、暗号化ソフトによる取出し不可となっております。」と返信し、D 担当課長に対しても虚偽の説明をしている。なお、このような D 担当課長からの問い合わせを受けて、E 担当課長は、本件 USB ポート等回答案を、最終の本件 USB ポート等回答の表現（〈※〉　USB ポート無し、秘文ソフトウェアがインストールされた専用端末）に改めている。

以上のとおり、本件 USB ポート等回答については、C 担当部長が、ログの誤読を前提としたエクスポートログの調査結果に依拠しつつ、USB ポートの設置状況等について虚偽の回答を行うという方針を決定し、E 担当課長及び F 担当課長がこれを認識した上で行われたものである[55]。

⑷　作業体制に関する虚偽回答（5 月 11 日回答）

5 月 11 日回答のうち、質問 3 に対してなされた「但し、各センタからの問合せ（トラブル対応、画面修正、疑似試験等）があった場合のみ、弊社〈本件保守拠点〉[56]に設置している保守用端末〈※〉より、システム管理者（2 名以上:担当課長＋担当者）にて、テナント（拠点）に応じた専用 ID/パスワードにてログインし、キャンペーン構成・画面エラーチェック、動作試験等を実施することがあります…」（下線部は当調査委員会による）という回答（以下「本件作業体制回答」という。）については、真実に反するものである。

E 担当課長は、本件作業体制回答は F 担当課長に確認の上で作成したというが、F 担当課長は、作業体制の実態として、急を要するときやリモートで対応する際には 1

[53] 元のメールでは、E 担当課長の苗字が記載されている。
[54] このように D 担当課長が USB ポートに関する回答内容について確認した理由について、D 担当課長は、ProCX の各コンタクトセンタでは、物理的に USB ポートは存在するがソフトウェアで使用制限をかけているところ、保守者側では物理的に USB ポートがないのかを確認したかったと説明している。
[55] なお、E 担当課長は、5 月 11 日回答の提出後である 2022 年 5 月 24 日、L 担当部長に対し、本件体制変更依頼について連絡する際、本件 USB ポート等回答が記載された 5 月 11 日回答を添付ファイルとして送付しているが、L 担当部長が、当時ファイルを開封して 5 月 11 日回答を確認したことまでは認められない。
[56] 元の回答では、本件保守拠点の名称が記載されている。

名で対応する場合もあったが、基本的には 2 名で実施することとされているので虚偽とは考えていないと述べる。しかし、X は、各コンタクトセンタから直接依頼を受け、1 名で作業することが多かったとみられるところ、あらゆる保守作業を 2 名以上で実施しているかのような内容の本件作業体制回答は、過剰というにとどまらず、真実に反する虚偽の回答であったと認められる。なお、本件作業体制回答と同様の旨を述べる 6 月 1 日回答における質問 3①に対する回答についても、同じく虚偽の回答であると言い得る。

⑸　データ消去の状況に関する虚偽回答（5 月 11 日回答・6 月 1 日回答・7 月 1 日回答）

ア　5 月 11 日回答における問題点

5 月 11 日回答のうち、「前システム機器廃棄時のデータ取り扱い内容」に関する質問（質問 2 後段）に対し、「前システム（PDS サーバ等）については、NTT フィールドテクノ社のデータ消去サービスを行った上、産業廃棄処分（O 社）を実施しております。」と回答した部分についても、真実に反する虚偽の回答である。ただし、この点は、6 月 1 日回答の 2②「データ削除（NTT フィールドテクノ社）や廃棄（O 社）についての実施証明は取られていますでしょうか？」との質問に対して、「前回（4 月 28 日 No2.回答）”前システム（PDS）はデータ削除や産業廃棄処分を実施しております”とご回答させて頂きましたが、”データ削除や廃棄処分は未だ実施しておらず”、弊社情報伝達の不手際により誤ったご回答をしてしまい、申し訳ございません。」と回答したことにより、訂正されている。

しかし、E 担当課長は、2022 年 4 月 29 日の時点で、F 担当課長より「…旧基盤のサーバは撤去が終わったところで倉庫に保管中で、まだ廃棄前です。」と社内チャットで知らされており、5 月 11 日回答時点でまだ産業廃棄処分となっていないことを把握していた。そして、E 担当課長は、この点について虚偽回答をする方針を示唆したのは C 担当部長であると述べる。また、F 担当課長については、上記のとおり、5 月 11 日回答の発出以前からまだ廃棄処分となっていないことを把握していたことから、虚偽回答である旨の認識はあったとみられる。

イ　6 月 1 日回答・7 月 1 日回答における問題点

上記の 6 月 1 日回答の 2②「データ削除（NTT フィールドテクノ社）や廃棄（O 社）についての実施証明は取られていますでしょうか？」との質問に対して、本件調査担当者らは、その第三文以降で、「尚、”前システム（PDS）”のハードディスクは

全てフォーマット化の上、データがないことを確認しており、弊社〈本件保守拠点〉[57]の鍵付き書庫に保管してあります。補足）データ削除（NTT フィールドテクノ）及び 産業廃棄（O 社）に関する両社への申請手配は既に完了しておりますので、実施予定である 2022.7 月以降は実施証明書をご提出することは可能です。」と回答している。また、7 月 1 日回答では、「前システムのハードディスクをフォーマットされた日時の記載がありませんでしたが、いつ実施されたかを PDS サーバー毎に教えていただきたいです。 」との質問 15 に対し、「弊社の作業運用ルールにより、サーバ撤去日（2 月 21 日）の 1 週間後に全サーバのハードディスクをフォーマット化しております。」と回答していた。しかしながら、実際には、PDS サーバの旧システムのハードディスク 13 台（以下「本件ハードディスク」という。）のフォーマット化（社内でゼロで上書きをする方式を含む方法により初期化することをいう。）は、2022 年 6 月 2 日から同年 6 月 6 日にかけて実施されており、上記の回答は、その実施時期についていずれも虚偽を述べるものであった。

そもそも、本件ハードディスクは、2022 年 2 月 21 日に撤去されていたにもかかわらず、本件調査担当者らが 5 月 25 日追加質問の 2②「データ削除（NTT フィールドテクノ社）や廃棄（O 社）についての実施証明は取られていますでしょうか？」との質問を受領した同年 5 月 25 日の時点で、データ削除（外部業者に依頼するデータの完全削除のことをいう。）もフォーマット化もいずれも実施されていない状態、すなわち内部にデータが残ったままの状態であった。

E 担当課長及び F 担当課長は、3 か月以上も本件ハードディスクに大量の顧客情報が格納されたまま保管することは情報セキュリティ管理上問題であると考え、フォーマット化だけでも直ちに実施しておかなければ、 BS での本件ハードディスクの前記のような保管状況が十分なものであったか否かが問題になりうるため、その不十分さを隠す目的の下、フォーマット化を実施することとし、F 担当課長が部下にフォーマット作業を実施するよう指示をした。そして、6 月 1 日回答として、「尚、“全システム（PDS）”のハードディスクは全てフォーマット化の上、データがないことを確認しており、弊社〈本件保守拠点〉[58]の鍵付き書庫に保管してあります。」との回答をしたが、実際にフォーマット化が実行されたのは、2022 年 6 月 2 日から同年 6 月 6 日であり、当該回答時点ではフォーマット化はまだ完了していない状態であった。翻ってみれば、当時の回答内容として、本件ハードディスクのフォーマット化は実施できていなかったため、速やかに実施する予定である旨を回答する選択肢もありえたと考えられるが、前記の経過のとおり、そのような選択肢が実際には採用されなかったのは、E 担当課長と F 担当課長が、BS における情報セキュリティ管理体制の不十分さを取り繕うことを優先したことを意味している。また、この段でフォーマ

[57] 元の回答では、本件保守拠点の名称が記載されている。
[58] 同上。

ット化を行ったという行為に対する評価として、本件ハードディスクに大量の顧客データが格納されたまま引き続き保管することに情報セキュリティ管理上の懸念はあったと思われるものの、A 社が 2022 年 4 月面談の時点でデータ等の保全を C 担当部長等に依頼していたことに照らせば、その保全の依頼の趣旨に反する行為であったと評価できる（ただし、E 担当課長と F 担当課長は、そのような 2022 年 4 月面談における A 社からの保全要請を認識していなかった。）。実際、A 社の J 取締役は、本件ハードディスクの保全について、遅くとも 2022 年 6 月 3 日の時点で C 担当部長に保全の協力を求めることが可能か相談をしており、また、遅くとも同年 6 月 9 日には明確に保全するよう依頼しており、今日まで本件保守拠点の倉庫で保管される状況が続いている。このような A 社の保全に向けた動きが、フォーマット化が完了した 2022 年 6 月 6 日までに E 担当課長及び F 担当課長に明確に伝わっていたことは確認されていないが、客観的にみれば、A 社が保全の相談を開始した時点でフォーマット化が進行中であったということになる。

その後、2022 年 6 月 24 日に、A 社から「前システムのハードディスクをフォーマットされた日時の記載がありませんでしたが、いつ実施されたかを PDS サーバー毎に教えていただきたいです。」と問われたが、E 担当課長及び F 担当課長は、前回の質問を受けた直後に急遽フォーマット化をしたと回答すると、結局 BS における情報セキュリティ管理体制の不十分さが露になってしまうことから、再びこれを取り繕うためにフォーマット化の実施時期を偽り、上記のとおり「サーバ撤去日（2 月 21 日）の 1 週間後」という虚偽の回答を重ねた（以下、5 月 11 日回答、6 月 1 日回答及び 7 月 1 日回答におけるデータ消去等に関する一連の虚偽回答を「本件データ消去回答」という。）。

⑹　本件体制変更依頼に対する虚偽回答（6 月 1 日回答）

本件調査担当者らは、5 月 23 日質問の質問 9「ONE CONTACT Network の PDS サーバーのデータにアクセスできるシステム管理者の体制変更」（6 月 1 日回答）、7 月 1 日回答の質問 11 後段として本件システムのシステム管理者 4 名が「現職」又は「離職」の別を問う質問、7 月 15 日回答の質問 18 としてシステム管理者 4 名の在職期間について、それぞれ、真実は体制変更が実施されていないにもかかわらず、体制変更を実施したことあるいは実施したことを前提とする虚偽の回答（以下「本件体制変更回答」という。）をした。特に、6 月 1 日回答の時点では、本件調査担当者ら全員が、BS における人的リソースの制限から一両日中の保守者の体制変更が困難であることは認識していたにもかかわらず、虚偽の回答をした。

その理由と経緯について、C 担当部長は、A 社から状況を改善するまで取引を停止されるおそれがあったため、実際の状況を踏まえた回答をすることができなかった

ものの、元々体制を変更しなければならないという問題意識は持っていたため、全くの虚偽という意識はなかったと述べる。しかしながら、本件体制変更回答を受けたA社は、実際に体制変更が行われたと理解しており、実際の回答の文言も「…以下のとおり体制見直しを図りました」(6月1日のうち5月23日質問9に対する回答)、「…現在在籍しておりますが、本担当（※ONE CONTACT NetworkのPDSサーバーにアクセスできるシステム管理者の意）からは外れております。」（7月1日回答11後段）等として、既に体制変更が行われたことを示す内容となっていることから、上記C担当部長の弁解は不合理なものというほかない。

A社が体制変更を依頼した理由は、流出したA社の顧客データがProCXの複数のコンタクトセンタに委託されていたものであったが、本件調査担当者らによる2022年4月21日回答において、各コンタクトセンタからは他のセンタの情報にアクセスできない旨の回答があったところ、複数センタの情報が漏洩するとしたら保守者側しかあり得ないと思ったためであった。A社は、本件体制変更依頼の理由としてこの点もC担当部長に伝えていたが、本件調査担当者らにこの点が十分共有されることはなかった。

そして、6月1日回答において体制変更について虚偽の回答をすることについては、本件調査担当者らに加えて、L担当部長も把握していた。

⑺ 4月21日回答の〈補記〉について

4月21日回答において、「■PDSサーバへのアクセスに関するセキュリティポリシーについて」(1枚目）に補記として、「保守者はハードウェアのヘルスチェック・OS再起動のみメンテナンス（月1回）を実施し、個別業務データへのアクセスは不可。」（下線について原文ママ）として、システム保守者の作業内容を念頭に置いた記述という回答があるが、ここでの「個別業務データ」には、PDSサーバ内の各顧客情報も含むものと考えられるが、前記のとおり、保守者は、顧客データにアクセス可能であったため、客観的には真実に反する回答であったといえる。ただし、2022年5月11日の回答ではこの点を改める内容の回答がなされていることに加え、そもそも本件調査担当者らは、PDSサーバのエクスポートログの取得方法及びエクスポートログにどのような情報が含まれているかを全く把握しておらず、また、XがPDSサーバについて実施した作業の記録を参照することもできない状況にあったこと、また4月21日当時はProCXのコンタクトセンタからの情報漏洩を念頭に置いた質問と回答がなされていたといった当時の状況等を踏まえると、本件調査担当者らが、4月21日回答の時点でこの点に関して故意に虚偽回答をしたとまでは言い難く、十分に裏付け調査を行わずに回答したというのが実態ではないかと考えられる。

7　本件過去調査の問題点に関する分析・評価

⑴　BS における情報セキュリティ管理体制の欠如及びこれを取り繕おうとする動機

エクスポートログの誤読に係る経緯は前記のとおりであるが、これに限らず、本件 USB ポート等回答、本件体制変更回答、本件データ消去回答、本件作業体制回答のいずれについても、長年 BS において、運用保守業務従事者による情報漏洩を想定した情報セキュリティ管理体制が敷かれていなかったことが共通の背景としてあることが指摘できる。すなわち、ログの誤読は、そもそも BS で運用保守業務従事者の作業記録をつけていなかった等の情報セキュリティ管理体制の欠如がその一因となっているが、C 担当部長、E 担当課長又は F 担当課長は、それぞれ BS において、保守者による情報漏洩を想定した情報セキュリティ管理体制が十分に敷かれておらず、不足があったことを認識していた。そして、これを A 社向けに取り繕うために、本件 USB ポート等回答、本件体制変更回答、本件データ消去回答及び本件作業体制回答についてそれぞれ虚偽回答を行ったものと評価できる。特に、C 担当部長、E 担当課長又は F 担当課長は、それぞれ BS の役職者として、このような BS における長年の情報セキュリティ管理体制の不足を取り繕い、十分な管理体制が存在している旨の虚偽回答をする動機があったと認められ、特に C 担当部長についていえば、同氏が一部明確に認めるとおり、ProCX の営業責任者として、ProCX の重要な取引先である A 社との契約を維持するためにこの点を取り繕いたいという動機が明確であったと認められる。そして、そのような背景には、責任者が短期間で入れ替わる中で少数の有スキル者に PDS サーバの運用・保守を頼っているという大きな流れを、個々の役職員が改善することは困難だという意識も働いていたのではないかとみられる。

以上の分析に照らせば、本件過去調査の問題点を招来した最大の要因は、本件不正持ち出しそのものの原因と同様、BS における長年の情報セキュリティ管理体制の欠如にあり、これを取り繕おうとする動機が本件過去調査における各虚偽回答を招いたといえる。

⑵　調査体制における問題点

ア　司令塔的役割を果たす人物の不在

A 社は、2022 年 4 月面談において、ProCX のトップである ProCX 社長に直接調査を依頼したにもかかわらず、前記のとおり、ProCX 社長は、本件過去調査の各調査内容や各回答内容はもちろんのこと、4 月 21 日回答の後も 2022 年 7 月頃まで引き続き調査が継続していたことすら把握していなかった。本来経営者が持

つべき通常のリスクマネジメント感覚からすれば、2022 年 4 月面談のように、自社が当該情報を大量に取り扱っている重要顧客のエンドユーザー情報の漏洩が発生し、既に警察への被害相談もなされており、自社にも証拠保全の要請がなされたという事態に接すれば、たちまち事態の重大性と緊急性を理解し、事態に応じた調査体制の構築やメンバー間での情報共有を指示して然るべきである。また、部下から問題がなかった旨の報告を受けたとしても、顧客の不安を解消するために、顧客目線に立って、どのような調査を実施し、どのような回答をしたのかについて報告を求めるはずである。このように、本件過去調査では、上層部が顧客の抱える懸念や問題意識に真摯に向き合い、リーダーシップを発揮し、調査事項や調査方法について担当者間で意思の統一を図り、組織的かつ綿密な調査を実施することが強く期待されていたものであり、A 社が 2022 年 4 月面談に ProCX 社長の参加が必須であるとしたのも、そのようなリーダーシップに基づく調査がなされることを期待してのことであったと思われる。

しかし、ProCX 社長は、2022 年 4 月面談の後、ProCX、BS 及び NTT 西日本への適切なエスカレーションや情報共有を一切せず、A 社に限られた人員でのクローズドな調査を依頼されたという一点のみをもって、C 担当部長、E 担当課長及び D 担当課長といった限られた人員で調査体制を敷くことを了承した（そもそも A 社がそのような調査体制を限定する旨の依頼をしていないことは、前記のとおりである。）。また、自身が司令塔となって調査チームを組成するでも調査の方向性を定めるでもなく、結果的に 2022 年 4 月面談に同行していた C 担当部長に全ての調査及び回答を委ね、これらの詳細を確認することもなかった。

そして、ProCX 社長に代わって本件過去調査を主導した C 担当部長は、本件過去調査の当時、BS の VD 部の役職に就いていたものの、システム関係の知識に明るくなく、PDS サーバの特殊性等を踏まえつつシステム関係の調査について適切な方針を示すだけの技量もなかった一方で、BS の保守部隊の上長として情報セキュリティ管理体制について虚偽回答を容易にできる立場でもあった。そして、C 担当部長は、 ProCX の CX ソリューション部の担当部長として、A 社との関係では営業責任者の立場でもあり、結果、A 社との取引を維持するために、BS の情報セキュリティ管理体制について虚偽の回答を行った。

以上のとおり、本件過去調査では、ProCX 社長によるリーダーシップが全く見られず、適切かつ確実に司令塔的役割を果たす者がいなかったため、全体を見通した上での調査事項や調査方法の検討というものが一切行われておらず、その場しのぎの調査や回答に終始していた面が否めない。そして、この点は、本件調査担当者らの間で事態の深刻さや A 社の要望に対して統一的な認識が形成されなかった一因にもなっていたと考えられる。

イ　本件調査担当者ら内部における情報共有の不足

本件過去調査は、本件調査担当者ら 4 名という非常に限られた人員で実施されたが、その 4 名の中でも事態の深刻さに対する受け止めに濃淡がある。特にエクスポートログの分析に関して、F 担当課長が本件調査依頼の切実さや事の重大さを全く理解していなかったことは前記のとおりであるが、その原因の一つとして、本件調査担当者らのうち E 担当課長と F 担当課長は、2022 年 4 月面談で A 社から共有された情報の共有を十分に受けていなかったという点が指摘できる。

すなわち、前記のとおり、C 担当部長は、2022 年 4 月面談の時点で、本件 A 社漏洩顧客情報はコンタクトセンタの拠点は違えど、いずれも共通して ProCX に提供されたものであることや、本件 A 社漏洩顧客情報が ProCX の各コンタクトセンタに委託された年月日等を把握していたところ、これらの情報は、流出元の特定につながる重要な解決の糸口になり得た。そうであるにもかかわらず、C 担当部長は、それらの情報は ProCX の各コンタクトセンタに関する資料であるため、システム面の調査を担当していた E 担当課長及び F 担当課長に共有する必要はないと判断した。さらに、D 担当課長は、あくまでもそれらの情報は断片的なものであり、これを E 担当課長及び F 担当課長らと共有しても解決に繋がらないとの判断の下、最後までこれを共有しなかった。

これにより、本件過去調査は、A 社の意向を理解しているが技術のバックグラウンドがない者と、一定の前提情報等があれば検証を行えるだけのシステムのバックグラウンドはあるが A 社の意向を十分に理解していない者によって実施されていた。つまり、システム面の調査に携わっていた E 担当課長及び F 担当課長が、調査の糸口を与えられていなかったことで、本件調査依頼の深刻さについて早い段階で共通認識が醸成されず、十分な調査に繋がらなかった可能性がある。

ウ　各社におけるエスカレーションや情報共有の欠如

（ア）各規程に基づくエスカレーション等の必要性とその欠如による調査体制の不足

NTT 西日本、BS 及び ProCX におけるエスカレーション等に関する規程類の概要は、別紙 6-8 のとおりである。

前記のとおり、本件過去調査では、関係各所に対する適切なエスカレーションや情報共有が誰からもなされていないが、以下のとおり、適切なエスカレーション等を実施し、調査体制の充実を図るべきであった。

殊に、ProCX 社長及び C 担当部長は、2022 年 4 月面談の時点で、ProCX が

委託を受けた A 社の顧客情報が ProCX から流出している可能性があるとの説明を受けたことにより、ProCX から顧客情報の漏洩が生じているおそれがあることを認識した。2022 年 4 月面談の時点では、コールセンタからの漏洩に関する話題が主であり、ProCX 社長及び C 担当部長においても、BS からの漏洩に対する認識は乏しかったとみられるが、ProCX 社長は、2022 年 4 月面談の数日前である同年 3 月 31 日まで BS の役職を兼任しており ProCX によるテレマーケティング業務において BS のシステムを利用していることを認識していた以上、BS からの漏洩の可能性に思い至るべきであった。また、C 担当部長については、遅くとも同年 4 月 28 日に A 社の J 取締役から BS の保守者を念頭に置いた質問が寄せられた時点で、BS からの情報漏洩の可能性もあることを認識したと言うべきである。

ProCX 社長は ProCX の管理者、C 担当部長は ProCX 及び BS の管理者として、NTT 西日本が定めたリスクマネジメントマニュアルを遵守すべき立場にあり、A 社からの説明により、同マニュアルにおいて内部リスクと位置付けられている[59]個人情報の漏洩が生じたおそれが相当程度具体的に示されている以上、同マニュアルの定めに従い、当該問題の深刻化を可及的速やかに防止するために、NTT 西日本の情報セキュリティ推進部等に対するエスカレーションを実施すべきであった。

特に、BS では、①BS における情報漏えい初動対応マニュアルが情報漏洩事案発生時の対応を詳細に定め、情報漏洩事案発生の際の被害の最小化を図ろうとしていること並びに②BS 個人情報保護管理規則細則において一定の重大な個人情報の漏洩等のおそれが生じた場合に情報管理責任者から NTT 西日本・情報セキュリティ推進部及び本社関係部門に対する報告が必要と規定されている。この点に鑑みれば、BS の管理者としてこれらの規程の内容を認識・遵守すべき立場にあった C 担当部長はもちろん、同年 3 月 31 日まで BS の管理者の地位も兼任し、同マニュアルの内容を認識すべき立場にあり、その後も ProCX 代表取締役として ProCX の事業上の重大なリスクに対して最大限慎重に対応すべき立場にあった ProCX 社長においても、A 社からの説明により認知した個人情報漏洩のおそれが ProCX 及び BS の事業上、非常に重要なリスクであることを十分に理解し、リスクマネジメントマニュアルに基づくエスカレーションの実施が必要であることを認識すべきであった。

加えて、C 担当部長については、上記の BS 個人情報保護管理規則細則 12（1）の規定を踏まえ、情報管理責任者である自らの上長（VD 部部長）が同細則に基

[59] なお、NTT 西日本コンプライアンス・BRM 推進委員会は 2021 年 9 月頃までに、リスクマネジメントマニュアルにおいてお客様情報・会社情報等の漏洩を最重要リスクと位置付ける改定を決定していたところ（実際の改定は 2023 年 7 月に実施された）、ProCX 社長は同委員会の委員であり、当該改定を認識すべき立場にあった。

づく NTT 西日本関連部署への報告を実施できるよう、自らが認識した情報漏洩のおそれについて上長である部門長ないし部長にエスカレーションを行うべきであった。

そうすると、本件過去調査に際し、ProCX 社長及び C 担当部長は、A 社から伝えられた ProCX ないし BS における個人情報漏洩のおそれについて、NTT 西日本の情報セキュリティ推進部等の関連部署に対する事実関係の報告（エスカレーション）（C 担当部長については、加えて BS 上長への報告（エスカレーション））を適時に行うべきであった。

なお、ProCX では、前記のとおり、情報漏洩等のおそれが生じた時点における具体的な対応手順等を定めた規程はなく、また、ProCX の経営トップである ProCX 社長も事態を把握した状態において、C 担当部長が同規程に従ったエスカレーションをしなかったことが、直ちに ProCX の規程に違反するものでもないが、本件調査依頼をエスカレーションの対象としない規程はその見直しを図るべきである。

（イ）一般的な危機管理意識に基づくエスカレーションの必要性とその欠如

各規程に基づくエスカレーションの要件等は以上のとおりであるが、翻って考えるに、2022 年 4 月面談の時点で、ProCX に委託されていた A 社の顧客情報がどこかから漏洩していることは既に確定しており、漏洩元が A 社であるか ProCX であるかの二択という状況下において、これを単なる情報漏洩の「おそれ」として小さなリスクと評価することはあまりにも硬直的かつ形式的に過ぎる対応であると言わざるを得ない。NTT 西日本では、かつて、単発的な FAX の誤送信や書類の置き忘れといった情報漏洩事案についてもインシデント報告の対象としていたが、本件調査依頼は、そのような事案よりもさらに重大なインシデントとして捉えられるべき事象であり、一般的な危機管理の感覚からすれば、直ちに関係部署等へのエスカレーションや情報共有がなされるべき事案であった。

しかしながら、本件過去調査に関与又はその存在を知っていた者は、誰一人として、関係各所へのエスカレーションや情報共有をすることなく、またその必要性について思いを至らせることもほぼなかった。たとえ ProCX 社長や C 担当部長が述べるとおり、A 社から限られた人員でクローズドな調査を行うよう要請があったと両名が誤解した点を最大限有利に斟酌するとしても、社内でのエスカレーションの必要性を説明し、A 社の理解を得ようと努力すべきであるが、両名がこの点を検討した形跡すらもない。また、L 担当部長、E 担当課長、F 担当課長及び D 担当課長においては、全員がエスカレーションの必要性の検討すら

行っておらず、ただ上長である ProCX 社長や C 担当部長が設定した調査体制に疑問を持つこともなかった。このように、複数の人間が一様にエスカレーションの必要性に対する判断を誤ったという事態に鑑みると、単なる個々人の資質の問題にはとどまらず、ProCX 及び BS において、事象の深刻さを客観的に把握できないといった危機管理意識が欠如していると言わざるを得ない。

⑶　クライアントと対話をする姿勢の欠如

C 担当部長は、本件 USB ポート等回答及び本件体制変更依頼に対して虚偽の回答をした理由として、A 社との取引が停止となることを怖れたと述べるが、その時点で具体的な懸念があったわけではない。また、仮にそのような懸念があったとしても、「こういった理由で直ちに実現することは困難であるが、この程度のタイムスケジュールで改善に向けて対応する」などといった形で自社の見通しを示しつつ、現実的に可能な対応策について A 社と協議・対話すべきであったが、A 社と何らの協議・対話の場を持つことなく、安易に虚偽回答に走っている。

ProCX 社長と C 担当部長は、2022 年 4 月面談において、A 社から限られた人員でクローズドな調査を行うよう要請されたと述べるが、この点について両名に何らかの誤解があったことは前記のとおりである。しかし、A 社がそう要請したと理解した場合であっても、十分な調査を実施するためには十分な人員を確保する必要がある、あるいは適切なエスカレーションをする必要があるなどと述べ、A 社から了解をもらうという選択肢もあった。そのような対話の場を持てば、ProCX 社長及び C 担当部長による上記誤解も解けたであろうし、万が一、A 社が限られた人員でクローズドな調査を行うよう要請していた事実があったとしても、そこで必要かつ十分な調査体制について深く協議することが期待できた。

また、システム面の調査を担当していた E 担当課長や F 担当課長が、直接 A 社と対話をし、情報漏洩に関して A 社で判明している事項等について質問することができれば、本件調査担当者らの間の情報格差も解消されたであろうし、新たな調査の糸口が得られた可能性がある。しかし、本件過去調査において、本件ウェブ会議で A 社からのシステム面関連の質問についてやり取りがあったことを除き、E 担当課長及び F 担当課長が、A 社側と直接やり取りをした形跡はない。A 社と直接取引関係のない BS の従業員である両名が A 社と直接やり取りをすることは困難であったと推察されるが、E 担当課長や F 担当課長が抱いた疑問について A 社に確認する機会を設けようとしなかったことは、本件過去調査において本件持ち出しを発見できなかった一因となっていると考えられる。

⑷　内部からの情報流出の事実を認識しつつ積極的に隠蔽したとまでは認められな

いこと

ア　不特定の内部からの情報流出の事実を認識していなかったこと

以上のとおり、本件過去調査には常識では考え難いほどの多数の問題点があり、これらを客観的にみた場合、本件調査担当者らが内部からの情報流出の事実を認識しつつ、これを積極的に隠蔽したのではないかと見られて然るべきとも言える。しかし、上記のとおり、本件調査担当者らは、極めて杜撰なログの調査しか実施しておらず、その他の虚偽回答の時点においても、本件調査担当者らが内部からの情報流出の事実を認識していたものとは認められない。以下、本件調査担当者らによる隠蔽を否定する事情について述べる。

まず、本件不正持ち出しが発覚した後の本件調査担当者ら同士でのメール等のやり取りを含め、本件過去調査の当時に、本件調査担当者らが内部からの情報流出の事実を認識していたことを示すものは発見されておらず、むしろ、本件調査担当者ら内部において情報流出元の検討をしている形跡がある。例えば、E 担当課長は、2022 年 6 月 30 日午後 3 時 15 分、C 担当部長、D 担当課長及び F 担当課長に、以下のメールを送信しており、B 社からの情報流出の可能性について検討していた。仮に、既に内部からの情報流出を認識しつつこれを隠蔽している場合、他からの情報流出の可能性を検討する意義はない。

【E 担当課長→C 担当部長、D 担当課長及び F 担当課長宛てメール（2022 年 6 月 30 日午後 3 時 15 分)】

「…先程、お話させて頂いておりました、社内利用（113,116 等）の利用ケースについて VD 部〈担当部署〉[60]へ確認致しました。

結果、、、 セキュリティ対策の粒度は様々でしたが、悪意があれば、ベンダーはマスターデータ を抜くことは可能とのことでした。 防止策(例)として、テラターム等のリモート接続ツールを用い ”作業ログを保存する” 仕組みを用いているとの回答もありましたが、ログ改ざんすることも可能であり、 本ツールを使用したか否か判断できるものはなく、やはり”人”によるところでした。C 担当部長[61]のご指摘のとおり、これらは、当担当においても例外ではなく、同じですと 言えるのではと考えております。

因みに、参考までになりますが、B 社[62]とのルールは以下のように定めております。

[60] 元のメールでは、BS の VD 部の担当部署の名称が記載されている。
[61] 元のメールでは、C 担当部長の苗字が記載されている。
[62] 元のメールでは、B 社の名称が記載されている。

1. B 社[63]との保守契約書内に、機密情報の取扱いを記載（第三者へ開示を禁ずる）
2. B 社[64]にて利用されている USB は 1 台のみ。 利用者は持出管理簿へ用途を記載の上、当日管理者である〈B 社担当者名〉[65]へ返却。 デスク鍵付きにて USB を保管するルールとしております。…」

また、F 担当課長も、前述のとおり、本件過去調査の終盤である同年 7 月 6 日に、D 担当課長に対して 7 月 6 日メールを送信して、A 社側の調査で判明している事項の有無を問い合わせており、本件過去調査の参考となる情報を自ら得ようとしていたが、F 担当課長が内部からの情報流出の事実を把握していた場合に本件調査担当者ら内部でこのような行動を取るはずはない。

さらに、本件調査担当者らのうち、C 担当部長及び D 担当課長は、2022 年 4 月面談の時点で A 社が既に岡山県警に被害相談をしていることを把握しており、E 担当課長も遅くとも 5 月 11 日回答の時点ではこの点を認識していた。A 社は、ProCX にとって重要な取引先であって、今後も取引を継続していきたいと考えていたところであり、近い将来、捜査機関による強制捜査の結果全てが詳らかになる可能性がある状況下において、自己が刑法犯に問われるリスクを背負いながら、内部からの情報流出の事実を積極的に隠蔽し、虚偽の報告をする動機にも乏しい。

したがって、本件調査担当者らが、内部からの情報流出を認識しつつ、これを積極的に隠蔽していたとは認められない。

イ　X による本件不正持ち出しの事実を認識していなかったこと

さらに、本件調査担当者らが、特に X が本件不正持ち出しを行っていたことの認識がなかったことは、以下の複数の事実から裏付けられる。例えば、E 担当課長は、5 月 11 日回答の作成に向けて、本件調査依頼があったことは伏せた上で、X 自身に保守作業で使用する ID は何かを尋ねている。さらに、エクスポートログの第一次改変後には、X に「処理（get～END allCount 件数）:キャンペーン ID:レポート名」の「件数」の意味を尋ねているが、仮に X による本件不正持ち出しの疑いを持つに至っていた場合には、X による証拠隠滅や虚偽回答を防ぐために X 以外の保守者に問い合わせ、その内容の検証を先行することが自然かつ合理的であるし、X がまさに本件不正持ち出しの当事者であると知っていればまず取らない行動であるといえる。

加えて、たとえ本件調査担当者らが本件過去調査の当時に X による本件不正持ち出しを知りつつこれを隠蔽したとしても、本件調査担当者らが当該事実を把握

63 同上。
64 同上。
65 元のメールでは、B 社の担当者の苗字が記載されている。

しながら更なる情報流出までも容認するということは考え難い。そして、X による本件不正持ち出しを認識していた場合には、USB ポートが使用可能な状態であるなどといった基本的な情報セキュリティ上の不備をそのまま放置せず、少なくとも更なる情報流出を防ぐために何らかの措置や対策を講じるはずであるが、本件過去調査の後に本件調査担当者らがそのような措置や対策を講じた形跡はない。本件過去調査の後も X による本件不正持ち出しが従前と同様に継続していた事実は、本件調査担当者らが、本件過去調査において X による本件不正持ち出しを発見できていなかったことと符合する。

その他、本件不正持ち出しが発覚した後の本件調査担当者ら同士でのメール等のやり取りを含め、本件過去調査の当時、X が本件持ち出しを行っていたことを本件調査担当者らが認識していたことや、本件調査において X を庇ったり、X による犯行だとして積極的にこれを隠蔽しようとした形跡、及び本件調査担当者らが X と特段親しかった等の事情も見当たらない。

以上のことからすれば、本件調査担当者らが X による本件不正持ち出しを知りつつこれを庇ったり、積極的に隠蔽したりしたものと認定することはできない。

8　本件過去調査に対する評価

以上のとおり、本件過去調査は極めて杜撰なものであり、本件 USB ポート等回答、本件作業体制回答、本件データ消去回答及び本件体制変更回答については、A 社に対して虚偽の回答が行われていた。その背景には、本件不正持ち出しの原因と同様に、BS における情報セキュリティ管理体制の不足があり、ログの誤読もそのような日常的な管理の不足等によって招かれたものであると考えられるが、本件過去調査は、その後の複数の虚偽回答と相まって、本件調査担当者らが内部からの情報流出の事実を知りながら意図的に隠蔽したと捉えられても仕方ないほど粗末な内容に終始した。

X による本件不正持ち出しは、10 年以上にわたって行われてきたとみられるが、A 社による本件調査依頼は、ProCX 及び BS がこれを発見し、さらなる情報流出を防ぐ最大の機会であったと考えられる。そうであるにもかかわらず、杜撰な調査によってその好機を逃し、さらなる個人情報の流出を許した ProCX 及び BS の責任は非常に重大なものと言わざるを得ない。

第7　情報セキュリティTFによる緊急点検

1　概要

情報セキュリティTFは、BS及びProCXを含むNTT西日本グループ全体のシステム緊急点検・是正協議を行い、その結果を踏まえ、主としてシステム面及び技術面から、本件不正持ち出しの再発防止策の検証及び策定、並びに、NTT西日本グループ全体の情報セキュリティ体制の課題分析及び改善策の策定を行った。

なお、情報セキュリティTFの発足に先立ち、NTT西日本は、情報セキュリティ推進部主導の下、以下のとおり、本件不正持ち出しが発生した本件システムに対する点検及びNTT西日本グループのシステムの点検に着手していた。

① 2023年7月の本件不正持ち出し発覚以降、本件システムを対象とする点検
② 2023年9月5日以降、NTT西日本グループにおいてお客様情報を1万件以上保有するシステムに関する点検
③ 2023年10月18日以降、NTT西日本グループにおいてお客様情報を保有する全てのシステム（上記②のお客様情報を1万件以上保有するシステムを除く。）及び機密性の観点の重要度が「高」と分類されているシステム[66]に関する点検

その後、同年11月16日に発足した情報セキュリティTFは、これらの点検を引き継いだものである（以下、本件不正持ち出しが発覚して以降のNTT西日本グループにおけるシステム点検を「本緊急点検」という。）。そのため、情報セキュリティTFは、引継ぎ前の本緊急点検の実施内容の検証も行った。

2　BSにおける本件システムの緊急点検

⑴　情報セキュリティTF発足前の対応

ア　2023年7月の本件不正持ち出し発覚後の点検

NTT西日本の情報セキュリティ推進部は、本件不正持ち出しが発覚した後、本件システムの緊急点検を行うため、以下の44の点検項目（以下「点検44項目」という。）を設定した。

なお、点検44項目は、本件不正持ち出しを踏まえてNTT西日本の親会社であ

[66] NTT西日本の「情報セキュリティ規則ICT編」9頁記載の分類によるもので、「金銭や課金、お客様情報、他事業者情報、重要な内部情報などの機密情報を保有・流通し、情報漏えいによりお客様や社会、又は事業に重大な影響が及ぶ恐れがあるシステム」をいう。

る日本電信電話株式会社から発出された点検項目（26 項目）に、NTT 西日本の情報セキュリティに関する規程である「情報セキュリティ規則 ICT 編」所定の点検項目や親会社グループ内の近時の情報漏洩事案を踏まえ調査すべきと考えられる項目を加えたものである。

（点検 44 項目）

大項目	項番	小項目
持ち出し制御	1	（1 は業務上 USB メモリ利用がない場合の点検項目）会社が許可した USB メモリ等以外を利用させない対策が取られているか
	2	（2 から 6 は業務上 USB メモリ利用がある場合の点検項目）USB メモリ等を利用する場合は、会社支給の生体認証／暗号化等の対策が実施されたものを利用しているか
	3	会社が許可した USB メモリ等以外を利用させない対策が取られているか
	4	会社が許可した USB メモリ等を利用する場合、事前の承認を得て記録しているか
	5	端末への USB メモリ等の接続についてログを取得し定期的に確認しているか 又は第三者立会いによる操作内容の目視確認を実施しているか
	6	USB メモリ等を別用途で再利用もしくは廃棄する場合は情報の復元が不可能な方法でデータ消去しているか
端末管理	7	端末のアカウント共用がないか
	8	マルウェア対策ソフトを導入しているか
	9	端末及び USB メモリ等を施錠保管しているか
	10	端末及び USB メモリ等を社外に持ち出す場合、承認を含めた持出管理をしているか
	11	お客様情報／重要情報等を取り扱う場合、他の業務のネットワークとは別に、インターネットへの接続がない個別ネットワークを用意し、業務を実施しているか
	12	端末の不用なポートの閉塞・FW 設定の有効化をしているか、端末内フォルダの不要な共有設定をしていないか
端末制限	13	重要な情報を扱う場合、アクセス可能な端末を制限し、私有端末等からのアクセスを禁止しているか
	14	私有端末からシステムを利用させる場合は、私有端末に会社情報を保存させない対策を実施しているか
メール・クラウド等による漏洩防止	15	メール送信時の検閲機能、もしくは、定期的にメール送信履歴が確認できる機能を実装しているか
	16	お客様情報／重要情報等を取り扱う場合に、情報漏洩のリスクが高いサイト（ファイル共有サイト、クラウドストレージ、SNS 等）への接続を制限しているか
アカウント管理	17	アカウントの共用がないか（作業者を特定できるか）
	18	アカウントの管理手順を定め、作成・変更・削除時は管理手順に従っているか

大項目	項番	小項目
	19	アカウントへ付与する権限レベルを定め、必要最小限の権限付与としているか
	20	異動／退職者等不要アカウントが無いか定期点検しているか
	21	重要な情報を保有する場合、多要素認証としているか
作業管理	22	特権アカウントによる作業について、事前に承認・記録しているか
	23	特権アカウントによる作業ログ（お客様情報出力を含む）を取得しているか
	24	保守作業者の作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか
	25	特権を持つシステム利用者による作業について、ログの削除・改ざんをできない仕組みとなっているか
	26	ログの定期点検を実施しているか
委託先管理	27	業務委託先に対する要求事項としてセキュリティ対策を要求しているか
	28	システム構築・運用に関する業務委託範囲や内容に応じて自社のセキュリティ管理策の実装もしくは運用の実施を委託先に要求し、対応可能であるか確認しているか
	29	委託先のセキュリティ対策の遵守状況を定期的に点検しているか
	30	委託先の保守作業について作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか
共有ファイルサーバ利用	31	共有フォルダに重要な情報を保管している場合、アクセス制限及びパスワード設定をしているか
	32	アクセス制限について、異動／退職者等不要アカウントがないか定期点検しているか
	33	共有フォルダへの保存期間を定め、期間を過ぎたものは削除しているか
	34	重要情報を保存しているフォルダについてアクセスログを取得しているか また、不要なアクセスがないか確認しているか
システム保管場所	35	重要情報を保管しているシステムの設置場所について、アクセス制限がされ、入退室管理並びに監視及び盗難対策等がされているか
	36	システムの設置場所への入退室は、管理者によって管理され、特定の人員にのみ入室権限の付与がされているか
	37	アクセスが制限されていない場所に設置せざるを得ない場合は部外者によるシステムの利用・接続や盗難を防止する措置を講じているか
	38	設置場所への機器の持込み／持ち出し時は、承認権限者の許可を得て、監視や作業記録を保存しているか
	39	設置場所への入室権限について、定期的に見直しをし、不要な権限の削除を実施しているか
	40	入室に必要となる鍵については員数管理し、紛失時の対応をしているか パスワード認証の場合は定期的に変更を行っているか

大項目	項番	小項目
リモート接続	41	リモートで接続させる場合、ID／パスワード認証より強固な認証方式か
	42	VPN 接続アカウントの共用がないか（接続者を特定できるか）
	43	リモート接続時の利用端末・利用環境はオフィス端末と同様の各種対策が実施されているか
暗号化	44	顧客情報は参照権限を持たない人が参照できないよう、システム的に暗号化されているか

NTT 西日本の情報セキュリティ推進部は、BS に対し、上記点検項目に基づく本件システムの点検を依頼し、点検結果の検証を行った（点検結果取りまとめ日は 2023 年 8 月 3 日）。その結果、点検 44 項目のうち 30 項目に不備があり、大幅な改善が必要な状況であった（点検結果は別紙 7-1 参照）。

そこで、NTT 西日本の情報セキュリティ推進部は、BS と上記不備項目について対応を協議したところ、システム構成の把握、リスク個所の把握、それを踏まえた技術的な対策の設計・導入に、相応の時間を要することが想定されたため、随時 BS による対処を支援しつつ、一定期間経過後に再度状況を確認することとした。

イ　2023 年 10 月の点検

NTT 西日本の情報セキュリティ推進部は、2023 年 10 月、前記の不備項目への対処の進捗を確認するため、再度、BS に対し、本件システムの点検を依頼し、点検結果の検証を行った（点検結果取りまとめ日は 2023 年 10 月 23 日）。その結果、点検 44 項目のうち不備事項は 4 項目となり、おおむね改善されていることを確認した（点検結果は別紙 7-1 参照）。

本件不正持ち出しを許した直接的な原因となった、内部不正を想定した技術的な管理措置における重大な不備は、BS における本件システムに関するものであったところ（第４・１参照）、BS は、それらの不備を是正する対処として、以下の措置を講じた（詳細は第９・１⑴に記載する。）。

① PDS サーバからの顧客データのダウンロードを制御する措置（項番 23～25 関連）
② 私有 USB メモリ等の外部記録媒体への書き出しを防止する措置（項番 2～5 関連）
③ 保守端末からのインターネット接続を制限する措置（項番 16 関連）
④ ログによる監視等の措置（項番 23～26 関連）

⑤ 私有端末によるアクセスを制限する措置（項番 13、14 関連）
⑥ 在宅オプション、SV 端末に関する措置（項番 41 関連）

ウ　2023 年 10 月の点検以後の対応

前記イの点検以降、BS は、積み残しとなった 4 つの不備項目の改善を図る他、一部運用で対処している項目[67]については、追ってシステム的な本格対処を実施することとした。そこで、NTT 西日本の情報セキュリティ推進部は、その状況を注視することとした。

⑵　情報セキュリティ TF による対応

情報セキュリティ TF は、その立ち上げ後、前記⑴の点検項目の検証、積み残しの不備事項や運用で対処している項目の進捗の確認、BS において実施した対処の検証を行った。

ア　点検項目の検証

情報セキュリティ TF は、NTT 西日本の情報セキュリティ推進部が設定した点検 44 項目は、①重要な情報を外部に持ち出せるルートを無くし、やむを得ず必要な場合は持ち出せるルートを限定する観点、及び、②重要な情報に対し、取扱い状況をトレースし、チェックする仕組みを整える観点が適切に考慮されていることから、妥当なものであると判断した。

イ　積み残しの不備事項等の進捗の確認等

積み残しの不備事項や運用で対処している項目の進捗を確認するため、情報セキュリティ TF は、再度、BS に対し、本件システムの点検を依頼し、点検結果の検証を行った。

2024 年 1 月末日時点の BS における本件システムの点検結果は別紙 7-1 のとおりであり、点検 44 項目のうち不備事項は 2 項目となり、また、運用で対処していた項目についてもシステム的な対処が実施され[68]、又は、実施が決定される等、改

[67] 「運用で対処」したものとしては、例えば、項番 3（会社が許可した USB メモリ等以外を利用させない対策）の対処のうち、やむを得ずお客様情報等を外部記録媒体へ書き出すに当たり、管理監督者（作業者）による作業を別の管理監督者（監視者）が監視するという運用（第９・１⑴ア（イ）参照）等があった。
[68] セキュリティ対策（ログ管理、不正操作注意表示、端末機制限・制御）や IT 資産管理を行うソフトウェ

善されていることを確認した。

そのうち本件不正持ち出しを許した原因との関連性が高い 17 項目（以下「優先 17 項目」という。優先 17 項目を設定した経緯については、後記 4 参照。）に関する点検結果は以下のとおりである。

（2024 年 1 月末日時点　優先 17 項目に関する BS の点検結果）

大項目	項番	小項目	対処	
持ち出し制御	1	（1 は業務上 USB メモリ利用がない場合の点検項目）会社が許可した USB メモリ等以外を利用させない対策が取られているか	－	（該当なし）
	3	会社が許可した USB メモリ等以外を利用させない対策が取られているか	○	セキュリティ対策ソフトウェアにて制御
	4	会社が許可した USB メモリ等を利用する場合、事前の承認を得て記録しているか	○	会社が許可した USB メモリ等を利用する場合は承認を得て記録していた
	5	端末への USB メモリ等の接続についてログを取得し定期的に確認しているか 又は第三者立会いによる操作内容の目視確認を実施しているか	○	セキュリティ対策ソフトウェアにてログを取得し、USB メモリ等接続時はリアルタイムで接続アラームメールを発出
端末管理	11	お客様情報／重要情報等を取り扱う場合、他の業務のネットワークとは別に、インターネットへの接続がない個別ネットワークを用意し、業務を実施しているか	○	データセンタのインターネットアクセスを必要最小限に限定し、保守網からのインターネットアクセスを遮断
端末制限	13	重要な情報を扱う場合、アクセス可能な端末を制限し、私有端末等からのアクセスを禁止しているか	○	MAC アドレス制限で管理外端末の接続を遮断
アカウント管理	17	アカウントの共用がないか（作業者を特定できるか）	○	アカウントを個人化。個人化不可のシステムアカウントについても中継サーバサーバにより作業者特定可能
	18	アカウントの管理手順を定め、作成・変更・削除時は管理手順に従っているか	○	アカウントの申請・払出し手順を整備
	19	アカウントへ付与する権限レベルを定め、必要最小限の権限付与としているか	○	業務上必要な権限細分化と必要最小限の権限付与

アを導入し、例えば、前脚注の項番 3（会社が許可した USB メモリ等以外を利用させない対策）について言えば、BS が許可した USB メモリしか使えないよう、システム的な対処を行った。

大項目	項番	小項目	対処	
	20	異動／退職者等不要アカウントが無いか定期点検しているか	○	異動・退職時等のアカウント削除漏れがないかを四半期に一度確認
作業管理	22	特権アカウントによる作業について、事前に承認・記録しているか	○	原則、作業者はお客様情報にアクセスしない。委託元からの指示がある場合は事前承認の上実施
	23	特権アカウントによる作業ログ（お客様情報出力を含む）を取得しているか	○	中継サーバ経由でのみ作業が可能で、作業ログも取得
	24	保守作業者の作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか	○	中継サーバ経由でのみ作業が可能で、作業ログも取得
	25	特権を持つシステム利用者による作業について、ログの削除・改ざんをできない仕組みとなっているか	○	改ざんされないよう権限付与対応済。追加改善でSyslogサーバ構築し改ざんできない対策を追加予定（3月末）
	26	ログの定期点検を実施しているか	○	セキュリティ対策ソフトウェアにてログを取得し定期的な点検を実施
委託先管理	30	委託先の保守作業について作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか	○	委託先作業記録の運用開始。中継サーバでセキュリティ対策ソフトウェア操作映像を記録
共有ファイルサーバ利用	31	共有フォルダに重要な情報を保管している場合、アクセス制限及びパスワード設定をしているか	○	共有フォルダのアクセス権をディレクトリ・サービス・システムで管理し、組織ごとにフォルダを整理

ウ　情報セキュリティTFによる評価

情報セキュリティTFは、以上のBSの対処について、多要素認証等、未実施の項目（点検項目21及び44）はあるものの、既に実施済みの項目により情報漏洩防止の効果が期待できるものであり、BSにおける本件システムに対する現時点の対応として妥当なものであると判断した。

3　ProCXにおける本件システムの緊急点検

⑴　情報セキュリティ TF 発足前の対応

ア　2023 年 7 月の本件不正持ち出し発覚後の点検

NTT 西日本の情報セキュリティ推進部は、BS に続き、ProCX に対しても、点検 44 項目に基づく本件システムの点検を依頼し、点検結果の検証を行った（点検結果取りまとめ日は 2023 年 9 月 7 日[69]）。その結果、点検 44 項目中、7 項目に不備があった（点検結果は別紙 7-2 参照）。

そこで、NTT 西日本の情報セキュリティ推進部は、BS への対応と同様、随時 ProCX による対処を支援しつつ、一定期間経過後に再度状況を確認することとした。

イ　2023 年 10 月の点検

NTT 西日本の情報セキュリティ推進部は、2023 年 10 月、前記の不備項目への対処の進捗を確認するため、再度、ProCX に対し、本件システムの点検を依頼し、点検結果の検証を行った（点検結果取りまとめ日は 2023 年 10 月 23 日）。その結果、点検 44 項目のうち、6 項目に不備があり、引き続き改善が必要な状況であった（点検結果は別紙 7-2 参照）。なお、これは、NTT 西日本の情報セキュリティ推進部が、人員に限りがある中で、本件不正持ち出しを許した直接的な原因に対処するため BS の対応を優先したことや、前記アの点検後の対処期間が BS と比較して ProCX の方が短期間であったことが一因であると考えられる。

ウ　2023 年 10 月の点検以後の対応

前記イの点検結果を踏まえ、NTT 西日本の情報セキュリティ推進部は、引き続き、ProCX による対処の支援及び進捗確認を継続することとした。

⑵　情報セキュリティ TF による対応

ア　点検項目の検証

情報セキュリティ TF は、その立ち上げ後、前記 2⑵アと同様の理由から、ProCX における本件システムの緊急点検との関係でも、点検 44 項目が妥当なものである

[69] 同時点では、2 拠点を対象に実査を行い、点検結果を把握した。「イ　2023 年 10 月の点検」についても同様。

と判断した。

イ　積み残しの不備事項等の進捗の確認等

情報セキュリティ TF は、前記⑴の点検結果を踏まえ、人員を都度派遣し、不備項目の対処の進捗確認、対処完了時期の意識合わせを行う等、ProCX に対し、助言を行った。その際、情報セキュリティ TF は、優先 17 項目の不備事項につき、優先的な対応を求めた。

上記の対応を経て、情報セキュリティ TF は、再度、ProCX に対し、本件システムの点検を依頼し、点検結果の検証を行った。

2024 年 1 月末日時点[70]の ProCX の対応状況に関する点検結果は、別紙 7-2 のとおりであり、その結果、点検 44 項目のうち不備事項は 0（ただし、運用による対処が 14 項目）となった。

そのうち優先 17 項目に関する点検結果は以下のとおりである。

（2024 年 1 月末日時点　優先 17 項目に関する ProCX の点検結果）

大項目	項番	小項目	対処	
持ち出し制御	1	（1 は業務上 USB メモリ利用がない場合の点検項目）会社が許可した USB メモリ等以外を利用させない対策が取られているか	○	グループポリシーで禁止済
	3	会社が許可した USB メモリ等以外を利用させない対策が取られているか	△	・USB メモリ利用 PC を最小化済 ・USB メモリなし PC に USB メモリ遮断設定済 ・原則データブリッジを利用予定（2 月末）
	4	会社が許可した USB メモリ等を利用する場合、事前の承認を得て記録しているか	○	利用承認・記録を管理簿にて管理 作業は複数人実施
	5	端末への USB メモリ等の接続についてログを取得し定期的に確認しているか 又は第三者立会いによる操作内容の目視確認を実施しているか	△	セキュリティ対策ソフトウェア導入によるログ管理予定（3 月末）。それまでは No3、4 で対処

[70] 同時点では、本件事案を踏まえた本件システムの利用に関する ProCX の対策チームから回答を得た。

大項目	項番	小項目	対処	
端末管理	11	お客様情報／重要情報等を取り扱う場合、他の業務のネットワークとは別に、インターネットへの接続がない個別ネットワークを用意し、業務を実施しているか	○	インターネット接続はできない、専用網で業務実施
端末制限	13	重要な情報を扱う場合、アクセス可能な端末を制限し、私有端末等からのアクセスを禁止しているか	○	セキュリティ対策ソフトウェア導入による禁止 それまでは私物端末持込禁止及びチェックの運用を徹底済
アカウント管理	17	アカウントの共用がないか(作業者を特定できるか)	△	・JOB ごとの業務フローに沿った共用アカウントの最小限化・管理は実施済 ・本社統一ルール展開実施中（2 月末） ・ディレクトリ・サービス・システム導入による個人特定とログ取得・点検予定（3 月末）
	18	アカウントの管理手順を定め、作成・変更・削除時は管理手順に従っているか	△	
	19	アカウントへ付与する権限レベルを定め、必要最小限の権限付与としているか	△	
	20	異動／退職者等不要アカウントが無いか定期点検しているか	△	
作業管理	22	特権アカウントによる作業について、事前に承認・記録しているか	△	・JOB ごとの業務フローに沿った対応は実施済 ・本社統一ルール展開実施中（2 月末）
	23	特権アカウントによる作業ログ（お客様情報出力を含む）を取得しているか	△	No.22 の徹底
	24	保守作業者の作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか	－	（対象外）
	25	特権を持つシステム利用者による作業について、ログの削除・改ざんをできない仕組みとなっているか	○	DL ログの改ざん不可
	26	ログの定期点検を実施しているか	△	（No23 と同様）
委託先管理	30	委託先の保守作業について作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか	○	BS と覚書を締結。保守業務に関する作業ログを取得し、作業記録簿との対照による検証を実施

大項目	項番	小項目	対処	
共有ファイルサーバ利用	31	共有フォルダに重要な情報を保管している場合、アクセス制限及びパスワード設定をしているか	△	・JOB ごとに業務フローを定め対応 ・顧客データ保有のフォルダアクセス権最小化済 ・顧客データは原則利用後削除 ・本社管理手順による運用展開中（2 月末）

さらに、ProCX は、今後、システム的な対処も実施していく予定であるところ、情報セキュリティ TF は、この点に関するアドバイスや内容の確認も行った。

ウ　情報セキュリティ TF による評価

情報セキュリティ TF は、以上の ProCX の対処について、情報漏洩防止の効果が期待できるものであり、ProCX における本件システムに対する現時点の対応として妥当なものであると考えている。一方で、点検 44 項目のうち、14 項目は運用で対処しており、システム的な対処は、今後の対応事項であるところ、引き続き、取組が必要である。

4　その他のシステムにおける緊急点検

⑴　情報セキュリティ TF 発足前の対応

ア　点検対象システム

NTT 西日本の情報セキュリティ推進部は、NTT 西日本グループ内の各組織に対し、2023 年 9 月 5 日、お客様情報を 1 万件以上保有するシステムに関する点検を依頼し、さらに、同年 10 月 18 日、お客様情報を保有する全てのシステム（同年 9 月 5 日に点検着手済みのお客様情報を 1 万件以上保有するシステムを除く。）及び機密性の観点の重要度が「高」と分類されているシステムに関する点検を依頼した。その結果、前記 2 及び 3 による本件システム点検と併せて、点検対象のシステムの総数は 443 システムとなった。

イ　点検実施者

セキュリティ遵守状況は、システムの利用形態によって異なることが想定され

たため、各システムについて、①システムの利用者、②ヘルプデスク等の特権アカウントを用いるシステム利用者、③システム保守者を対象とし、それぞれに点検を依頼した（ただし、システムによっては、一人の者が上記①から③の複数の立場を兼ねている場合があるところ、その場合には、その者が、①から③の複数の立場から点検項目に回答した。）。

ウ　点検項目

点検項目は、本件システムに関する点検と同様、点検 44 項目を用いた。

エ　点検方法

NTT 西日本の情報セキュリティ推進部は、点検を実効的なものとするため、以下のプロセスで、各システムを主管する組織と、点検方法に関する協議・助言を行った。

① まず、システムを主管する各組織に、システムの構成を説明する帳票の提出を求めた。
② NTT 西日本の情報セキュリティ推進部の担当者は、上記帳票をもとに、点検対象のシステム構成を把握し、システムごとに、リスク分析を行って、各点検項目について、どのような方法で点検を行うか検討した。その際、判断基準に不整合が生じないよう、NTT 西日本の情報セキュリティ推進部の担当者間で情報共有を行った。
③ 上記の検討結果を踏まえ、NTT 西日本の情報セキュリティ推進部の担当者は、システムを主管する各組織に、点検方法について助言するとともに、進捗確認、対処完了時期の意識合わせを行った。
④ システムを主管する各組織による点検結果について、点検項目の基準を満たしている（〇）、満たしていない（×）を問うだけでなく、回答の根拠を具体的に確認した。

⑵　情報セキュリティ TF による対応

ア　点検の引継ぎ

情報セキュリティ TF は、その立ち上げ後、前記⑴のアないしエによる点検の継続が適切であると判断し、これを引き継いだ。

当初、情報セキュリティ TF は、2023 年 11 月 17 日を点検結果の報告期日に設

定し、12 月 8 日まで各組織における点検について情報セキュリティ TF においてチェックし、点検において不備が発見された場合は、12 月末日までに是正を完了することを予定していた。しかし、情報セキュリティ TF として、全 443 システムについて、システム構成の把握、リスク個所の把握、それを踏まえた技術的な対策の設計・導入の検討を行うには相応の時間を要したことに加え、各組織においても、人員不足やシステムに関する状況把握が不十分等の個別の事情があり、報告遅れ（情報セキュリティ TF からの質問への回答の遅れを含む。）、根拠不記載、判断基準の誤り等が多数発生した。そのため、情報セキュリティ TF は、上記期限を延長し、また、優先 17 項目を優先対応項目として対応を先行させるとともに（優先 17 項目の選定理由は別紙 7-3 参照）、点検 44 項目のその他の項目についても当委員会の調査期間中に可能な限り是正を図ることを求めた。

その結果、最終的には、点検対象の全 443 システムについて、各組織からの点検結果の報告、情報セキュリティ TF による検証を終え、①持ち出しルートを無くし又は限定する観点、及び、②重要情報の取扱い状況をトレースし、チェックする観点（上記２⑵ア参照）から、各システムの暫定対処（運用面での対処を含む。）を 2024 年 2 月 16 日までに完了するに至った。

イ　点検結果

各組織からの点検結果の当初の報告により、全ての点検項目に何らかの不備が確認され、特に、端末管理・制限（項番 11、13）、アカウント管理（項番 17～21）、作業管理（項番 22～26）、暗号化（項番 44）に関する不備事項が多く見られた。各点検項目の不備率は下表のとおりである。なお、下表は、本緊急点検における各システムの初期的な点検結果を取りまとめたものであるところ、前記のとおり、本緊急点検では、443 システムについて、並行して点検及び是正対応を行ったため、初期的な点検結果が得られた時期はシステムごとに異なる。

（各点検項目の不備率）※赤色が 20%以上、オレンジ色が 10%以上

確認項目			是正要システム種別（数字は不備システム数、%は不備率）					
			利用者		保守ヘルプデスク		保守SE	
持ち出し制御	1	（1 は業務上 USB メモリ利用がない場合の点検項目）USB メモリ等を利用できない対策が取られてい	24	5.4%	17	3.8%	43	9.7%

確認項目			是正要システム種別（数字は不備システム数、%は不備率）					
			利用者		保守ヘルプデスク		保守SE	
		るか						
	2	（2 から 6 は業務上 USB メモリ利用がある場合の点検項目）USB メモリ等を利用する場合は、会社支給の生体認証／暗号化等の対策が実施されたものを利用しているか	19	4.3%	8	1.8%	8	1.8%
	3	会社が許可した USB メモリ等以外を利用させない対策が取られているか	24	5.4%	15	3.4%	33	7.4%
	4	会社が許可した USB メモリ等を利用する場合、事前の承認を得て記録しているか	6	1.4%	8	1.8%	8	1.8%
	5	端末への USB メモリ等の接続について、ログを取得し定期的に確認しているか、又は第三者立会いによる操作内容の目視確認を実施しているか	21	4.7%	10	2.3%	17	3.8%
	6	USB メモリ等を別用途で再利用もしくは廃棄する場合は情報の復元が不可能な方法でデータ消去しているか	7	1.6%	8	1.8%	6	1.4%
端末管理	7	端末のアカウントの共用がないか	28	6.3%	16	3.6%	32	7.2%
	8	マルウェア対策ソフトを導入しているか	14	3.2%	10	2.3%	16	3.6%
	9	端末及び USB メモリ等を施錠保管しているか	14	3.2%	9	2.0%	15	3.4%
	10	端末及び USB メモリ等を社外に持ち出す場合、承認を含めた持ち出し管理をしているか	22	5.0%	4	0.9%	10	2.3%
	11	お客様情報／重要情報等を取り扱う場合、他の業務のネットワークとは別にインターネットへの接続がない個別ネットワークを用意し業務を実施しているか	126	28.4%	96	21.7%	90	20.3%
	12	端末の不要なポートの閉塞・FW 設定の有効化をしているか、端末内フォルダの不要な共有設定を行っていないか	26	5.9%	18	4.1%	27	6.1%

確認項目			是正要システム種別（数字は不備システム数、%は不備率）					
			利用者		保守ヘルプデスク		保守SE	
端末制限	13	重要な情報を扱う場合、アクセス可能な端末を制限し、私有端末等からのアクセスを禁止しているか	58	13.1%	44	9.9%	69	15.6%
	14	私有端末からシステムを利用させる場合は、私有端末に会社情報を保存させない対策を実施しているか	30	6.8%	20	4.5%	33	7.4%
メール・クラウド等による漏洩防止	15	メール送信時の検閲機能、もしくは、定期的にメール送信履歴が確認できる機能を実装しているか	27	6.1%	21	4.7%	23	5.2%
	16	お客様情報／重要情報等を取り扱う場合に、情報漏洩のリスクが高いサイト（ファイル共有サイト、クラウドストレージ、SNS 等）への接続を制限しているか	28	6.3%	16	3.6%	22	5.0%
アカウント管理	17	アカウントの共用がないか（作業者を特定できるか）	49	11.1%	31	7.0%	84	19.0%
	18	アカウントの管理手順を定め、作成・変更・削除時は管理手順に従っているか	59	13.3%	26	5.9%	75	16.9%
	19	アカウントへ付与する権限レベルを定め、必要最小限の権限付与としているか	23	5.2%	9	2.0%	22	5.0%
	20	異動／退職者等不要アカウントがないか定期的に点検しているか	39	8.8%	26	5.9%	51	11.5%
	21	重要な情報を保有する場合、多要素認証としているか	99	22.3%	62	14.0%	31	7.0%
作業管理	22	特権アカウントによる作業について、事前に承認・記録しているか	118	26.6%	52	11.7%	69	15.6%
	23	特権アカウントによる作業ログ（お客様情報出力を含む）を取得しているか	74	16.7%	6	1.4%	8	1.8%
	24	保守作業者の作業ログの取得又は第三者の立会いによる作業内容の確認が行われているか	2	0.5%	29	6.5%	41	9.3%
	25	特権を持つシステム利用者による作業について、ログの削除・改ざんをできない仕組みとなっているか	61	13.8%	59	13.3%	115	26.0%
	26	ログの定期点検を実施しているか	138	31.2%	84	19.0%	128	28.9%

確認項目			是正要システム種別（数字は不備システム数、%は不備率）					
			利用者		保守ヘルプデスク		保守SE	
委託先管理	27	業務委託先に対する要求事項としてセキュリティ対策を要求しているか	2	0.5%	2	0.5%	9	2.0%
	28	システム構築・運用に関する業務委託範囲や内容に応じて自社のセキュリティ管理策の実装もしくは運用の実施を委託先に要求し、対応可能であるかを確認しているか	7	1.6%	17	3.8%	12	2.7%
	29	委託先のセキュリティ対策の遵守状況を定期的に点検しているか	13	2.9%	42	9.5%	38	8.6%
	30	委託先の保守作業について作業ログの取得又は第三者の立会いによる作業内容の確認が行われているか	1	0.2%	15	3.4%	26	5.9%
共有ファイルサーバ利用	31	共有フォルダに重要な情報を保管している場合、アクセス制限及びパスワード設定をしているか	16	3.6%	20	4.5%	18	4.1%
	32	アクセス制限について、異動／退職者等不要アカウントがないか定期点検しているか	13	2.9%	5	1.1%	6	1.4%
	33	共有フォルダへの保存期間を定め、期間を過ぎたものは削除しているか	18	4.1%	23	5.2%	19	4.3%
	34	重要情報を保存しているフォルダについてアクセスログを取得しているか また不要なアクセスがないか確認しているか	23	5.2%	21	4.7%	22	5.0%
システム保管場所	35	重要情報を保管しているシステムの設置場所について、アクセス制限がされ、入退室管理並びに監視及び盗難対策等がされているか	2	0.5%	8	1.8%	13	2.9%
	36	システムの設置場所への入退室は管理者によって管理され、特定の人員にのみ入室権限の付与がされているか	1	0.2%	5	1.1%	9	2.0%
	37	アクセスが制限されていない場所に設置せざるを得ない場合、部外者によるシステムの利用、接続及び盗難を防止する措置を講じているか	1	0.2%	0	0.0%	0	0.0%

確認項目			是正要システム種別（数字は不備システム数、%は不備率）					
			利用者		保守ヘルプデスク		保守SE	
	38	設置場所への機器の持込み／持ち出し時は、承認権限者の許可を得て、監視や作業記録を保存しているか	7	1.6%	11	2.5%	21	4.7%
	39	設置場所への入室権限について定期的に見直しをし、不要な権限の削除を実施しているか	0	0.0%	3	0.7%	5	1.1%
	40	入室に必要となる鍵については員数管理し、紛失時の対応をしているか パスワード認証の場合は定期的に変更を行っているか	1	0.2%	7	1.6%	10	2.3%
リモート接続	41	リモートで接続させる場合、ID／パスワード認証より強固な認証方式か	13	2.9%	11	2.5%	13	2.9%
	42	VPN 接続アカウントの共用がないか（接続者を特定できるか）	4	0.9%	7	1.6%	10	2.3%
	43	リモート接続時の利用端末・利用環境はオフィス端末と同様の各種対策が実施されているか	4	0.9%	6	1.4%	11	2.5%
暗号化	44	顧客情報は参照権限を持たない人が参照できないよう、システム的に暗号化されているか	2	0.5%	8	1.8%	176	39.7%

ウ　是正対応の概要

前記の不備事項に関し、情報セキュリティ TF の助言の下、各システムを主管する組織において、是正対応を実施し、又は、行うことが予定されるに至った。点検 44 項目に関する主な是正対応（予定も含む。）は別紙 7-4 のとおりであり、不備率の高かった端末管理・制限、アカウント管理、作業管理、暗号化に関する主な是正対応（予定も含む。）は以下のとおりである。

（不備率の高い項目に関する主な是正対応）

確認項目			主な是正対応（運用対処及び対応予定のものを含む）
端末管理	11	お客様情報／重要情報等を取り扱う場合、他の業務のネットワークとは別にインターネットへの接続がない個別ネットワークを用意し業務を実施しているか	・安全とみなしたウェブサイトのリストであるホワイトリスト以外のアクセス先を制限する ※社内利用システムの通信網である OA 網から利用する SaaS 等システムについては OA 網の対策で保護されていると判断
端末制限	13	重要な情報を扱う場合、アクセス可能な端末を制限し、私有端末等からのアクセスを禁止しているか	・MAC アドレスフィルタにて管理外端末の接続を禁止する ・ディレクトリ・サービス・システムに登録された端末以外からのアクセスを禁止する ・各種ソフトウェアへのアクセスを登録されたデバイスに限定する ・セキュア FAT 以外からアクセスできないよう接続元 IP アドレスを限定する
アカウント管理	17	アカウントの共用がないか（作業者を特定できるか）	・システムのアカウントを個人アカウントに変更する ・システムの制約上、SE 業務を共用アカウントで実施する必要がある場合は、作業承認を得て管理簿に記録する。また承認のないログインがないかを定期ログ点検にて確認する
	18	アカウントの管理手順を定め、作成・変更・削除時は管理手順に従っているか	・アカウント管理手順を定める ・アカウント共用を解消できない場合は、共用アカウント利用管理簿を作成する
	20	異動／退職者等不要アカウントがないか定期点検しているか	・アカウント点検を運用に追加する ・委託先への払い出しアカウントについても毎月 1 回の棚卸を実施する
	21	重要な情報を保有する場合、多要素認証としているか	・ID／パスワードのみではなく、システムへのアクセス時に SMS によるワンタイムコード認証を追加 ・多要素認証導入までは毎月の定期点検にて重要情報を扱う操作ログの点検を実施
作業管理	22	特権アカウントによる作業について、事前に承認・記録しているか	・特権アカウントによる作業管理簿を整備。作業前に承認を得て、記録する ・管理者の口頭承認による運用から、システム上で承認を得るフローに変更する
	23	特権アカウントによる作業ロ	・お客様情報出力ログを取得する機能追加開発を実施する

確認項目			主な是正対応（運用対処及び対応予定のものを含む）
		グ（お客様情報出力を含む）を取得しているか	・ログ取得できない場合は、2 名以上の操作を義務付けることで不要な行為を防止する
	25	特権を持つシステム利用者による作業について、ログの削除・改ざんをできない仕組みとなっているか	・作業画面を録画する ・SE 作業は必ず 2 名以上で実施し、作業ログを取得する。作業完了後にログを提出し、サーバ SE がアクセスできない場所にログを保管
	26	ログの定期点検を実施しているか	・月次で、ログインログ／システムの操作ログと作業管理簿を突合し、承認されていないログイン／操作がないかを点検する
暗号化	44	顧客情報は参照権限を持たない人が参照できないよう、システム的に暗号化されているか	・本点検において暗号化有無を確認済 ・当該確認結果を踏まえ、今後具体的な内容・方法について整理の上、各システムにおいて実装を予定

エ　情報セキュリティ TF による評価

前記⑵のとおり、点検対象の全 443 システムの点検結果について、情報セキュリティ TF による検証を行い、各システムを主管する組織において、2024 年 2 月 16 日までに、各システムの暫定対処（運用面での対処を含む。）を完了した。これらの対応は、点検対象の全 443 システムにおける情報漏洩防止の効果が期待できるものであり、各システムを主管する組織における現時点の対応として妥当なものであると考えている。

一方で、全 443 システムについて、運用面での是正対応に留まっている項目も存在し、点検 44 項目の全ての不備を是正したわけではない。したがって、今後も、各システムを主管する組織における是正対応、NTT 西日本による監督、助言を継続することに加え、NTT 西日本グループ全体でのシステム的な対処による是正についても検討すべきである。

また、本緊急点検においては、点検 44 項目に関する不備に留まらない以下の問題点も判明した。

① 各システム主管組織において、システム構成や顧客情報の保管状況を十分に把握できていないことがある。そのため、システム全体の構成を基に情報漏洩リスクを把握することができていないことがある。

② 業務用システムを構築する際、社内ルール（「情報セキュリティ規則 ICT 編」）に従って、サイバー攻撃による侵害リスク及び侵害後の被害拡大リスクを低減する

ために外部接続を必要最小限にするには、業務ごとに他のネットワークから独立した個別システムを構築することになる。しかし、個別システムを構築する負担が大きく、本来実施すべきセキュリティ対策が疎かになってしまっていることがある。

③ 点検項目が多数であること、どの程度の対応が必要であるのか基準や具体例が明確でないこと、点検の対象となるお客様情報や機密情報といった重要情報を保有するシステムへの該当性を判断基準が明確でないこと等から、実効的な点検が困難である等、点検項目・点検方法に関する意見も提示された。また、これらの事情が、従前行われていた点検の形骸化を招いていたと推測される。

したがって、今後は、点検 44 項目に関する対処に加え、これらの問題点を解消するための取組も必要であると考える。

5　本緊急点検を踏まえた再発防止策等の策定

情報セキュリティ TF は、本緊急点検の結果を踏まえ、BS、ProCX 及び NTT 西日本グループ全体で取り組むべき、今後のシステム上の対処策を取りまとめた。その内容は、再発防止策等の提言の一部として、後記第９・１⑴、同２⑵、同３⑴及び⑵に記載する。また、情報セキュリティ TF は、調査委員会本体と相互連携を図り、本緊急点検の結果明らかになった、システム面及び技術面以外の問題点についても調査委員会本体に報告し、再発防止策の策定に関与した。

第８　NTT 西日本グループの役職員に対するアンケート調査

１　アンケートの目的

当調査委員会は、本件不正持ち出し及び本件過去調査並びにこれらを受けた調査等を踏まえ、NTT 西日本グループ全体でも、内部不正による情報漏洩に対する情報セキュリティ体制の実態や役職人の認識を把握する必要があると判断し、NTT 西日本グループの役職員に対するアンケート調査（以下「本アンケート調査」という。）を実施した。

２　アンケート調査の範囲及び方法

⑴　アンケート調査の範囲

当調査委員会は、NTT 西日本並びに ProCX 及び BS を含む NTT 西日本のグループ会社の役職員のうち、1 万件以上のお客様情報を保有する 204 システムの情報管理責任者、お客様情報適正利用監督者、お客様情報適正利用推進者及び各システムの点検実施者である役職員 288 名（以下、総称して「管理責任者等」という。）を対象としてアンケート調査を実施した。

また、管理責任者等に対する上記アンケート調査を補完するため、一部の質問については、上記 204 システムの主管組織の管理責任者等を除く全役職員 2609 名（以下、総称して「一般社員」という。）に対しても、アンケート調査を実施した。

管理責任者等については回答を必須とし 100%の回答率に至った。一般社員については任意回答としたものの、52%の回答率に至った。

⑵　アンケート調査の方法

当調査委員会は、2023 年 12 月 18 日付け「社内アンケートへのご協力のお願い」と題する案内文書[71]を回覧し、同月 19 日から 2024 年 1 月 19 日までの期間、Microsoft Forms のアンケートフォームから回答をすることを求める方法によるアンケート調

---

71 当調査委員会は、役員及び従業員から、忌憚のない意見を収集することを目的として、案内文書に次の内容を明記した。

当委員会は社内調査委員会という位置付けではありますが、上記アンケートプラットフォームは当職（当委員会委員長国谷史朗）が所属する法律事務所が構築・運用するものであり、貴社及び貴社グループ会社のいかなる役職員も、皆様のご回答内容を閲覧する権限を有していません。また、アンケートにより得られた情報・ご指摘等は、真因究明分析及び再発防止策の立案に資する限度で、かつ、個々の回答者が特定されない方法によってのみ、当委員会を構成する貴社の役職員に共有されます。皆様の個別の回答内容が、回答者を特定する態様で貴社の役職員に提供されることはありません。

査を実施した。

回答の基準時は、ProCX 及び BS によって本件不正持ち出しが公表された 2023 年 10 月 17 日時点と設定し、本件不正持ち出しが公表された後の認識等を問う一部の質問項目については回答時点と設定した。

3　本アンケート調査の結果及びその分析

本アンケート調査は、本件不正持ち出し、本件過去調査及び本緊急点検の結果等を踏まえ、次の質問構成にてアンケートを実施した。

- ○　役職員のリスク認識及び評価
- ○　日常管理
- ○　自主点検
- ○　目的外利用の監視
- ○　外部記録媒体の遮断措置
- ○　インシデント対応
- ○　システム管理者又は運用保守従業者を取り巻く状況
- ○　組織風土
- ○　本件不正持ち出しを踏まえた対応等

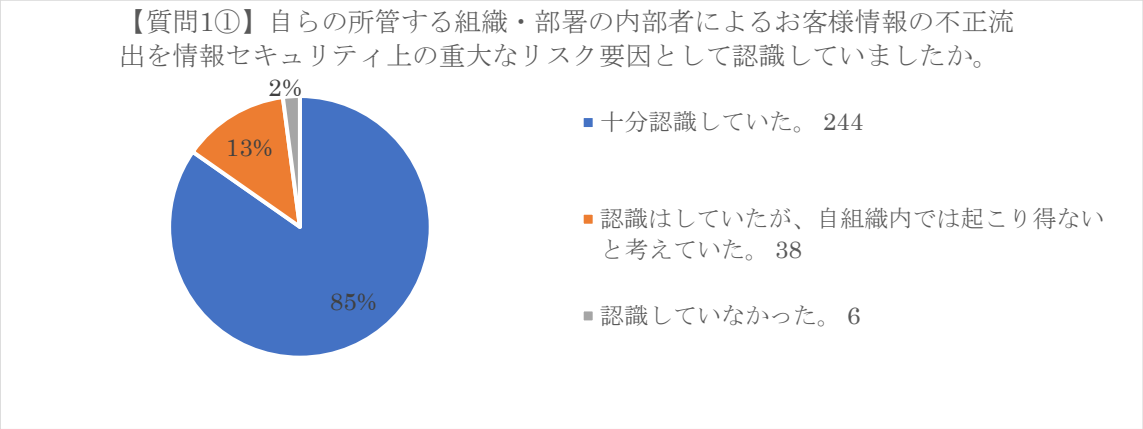
アンケートの結果は後記⑴から⑼のとおりである。本アンケート調査は、管理責任者等に対するアンケート調査を主とし、一般社員に対するアンケート調査は補完的なものとして位置付けている。したがって、後記⑴から⑼では特に断らない限り、管理責任者等に対するアンケートを取り上げている。

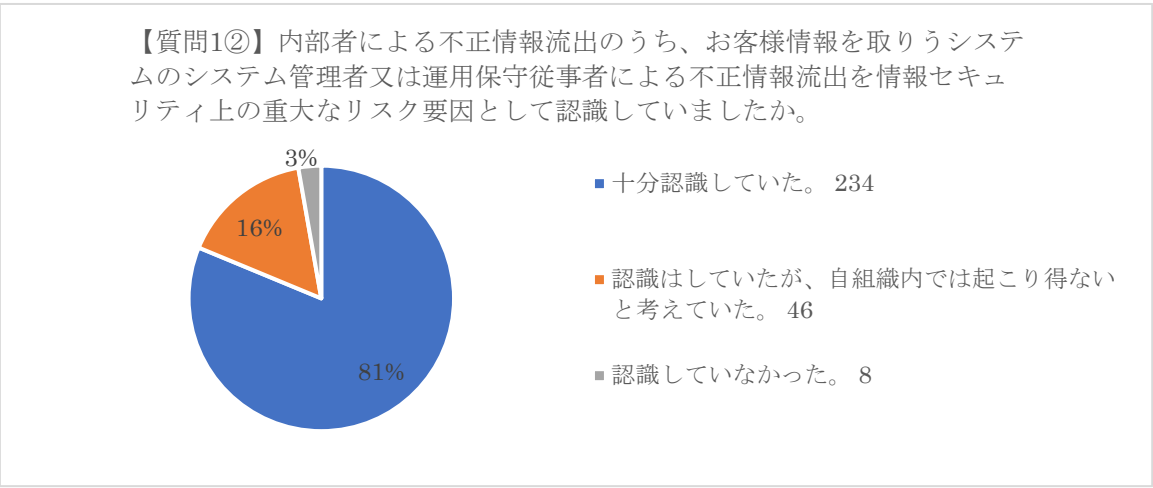
なお、一般社員に対するアンケートを含め、本文中に掲載しなかった質問事項及びこれに対する回答のうち、主だったものは別紙 8 に記載している。また、自由回答方式の質問事項に対する回答は、原文のまま掲載しているが、それのみをもって個人を識別できる情報が含まれる場合には、一定の加工処理をしている。

⑴　役職員のリスク認識及び評価

ア　役職員のお客様情報の不正流出に対する認識

（ア）アンケート結果





（イ）評価・考察

質問 1①及び②ともに、管理責任者等の 8 割以上が「十分認識していた。」と回答しており、これのみを見れば相応に評価できる結果と言える。

他方で、少なくない割合（質問 1①については 13%、質問 1②については 16%）の管理責任者等が、上記のようなリスクを「認識はしていたが、自組織内では起こり得ないと考えていた。」と回答している。本アンケート調査では、上記のようなリスクについて「認識はしていたが、自組織内では起こり得ないと考えていた。」と回答した者に対し、その理由をさらに確認している（質問 1③及び④）。その中でも多くの回答は、性善説に立ってそもそも疑いを持っていなかったという薄弱な根拠に依拠しているものであり（下表参照）、システムの仕様や物理的又は技術的な管理措置の存在といったより具体的な根拠を示す回答は 10%にも満たなかった。

このように、リスクとして認識しているにもかかわらず具体的な根拠無く情

報漏洩が起こらないと考えている管理責任者等が一定数存在することが判明した。BS においては、前記第５・１⑵ア（イ）、同イ及び⑸で指摘したとおり、本件不正持ち出しの原因・背景の一つとして、内部不正による情報漏洩リスクに対する意識の弱さがあったが、上記アンケート結果は NTT 西日本グループ全体でも同様の傾向が生じている可能性を示唆しており、性善説などに依拠するのではなく、情報キュリティに関する理解を深める活動を充実する必要がある。

【質問 1④】質問 1①の回答が「認識はしていたが、自組織内では起こり得ないと考えていた。」の場合、そのように考えていた理由をご回答ください。（性善説を理由とするもの）

- 内部者に不正流出を行おうとする者は存在していないと思っていた。
- 自組織の内部者がお客様情報を不正に持ち出す事案がこれまでなかったから。
- これまでも大きな事故もなかったことから、性善説によった考え方が浸透していた
- 運用フローが定まっており、悪意を持って情報流出させることは想像できなかった。
- 性悪説に基づいた対応を考えていなかったため

【質問 1④】質問 1②の回答が「認識はしていたが、自組織内では起こり得ないと考えていた。」の場合、そのように考えていた理由をご回答ください。（性善説を理由とするもの）

- NTT に属する一員として倫理的に不正流出につながる行為を実行することはないという思い込み
- システム管理に従事する社員についてはモラルが高い社員を配置しており、不正は出ないものと性善説に立っていたため
- マニュアルに基づき実施していれば大丈夫と言った性善説に立っていた！
- 内部者に不正流出を行おうとする者は存在していないと思っていた。
- 自組織のシステム管理者や運用保守従事者がお客様情報を不正に持ち出す事案がこれまでなかったから。

イ　リスク認識に関連する検証・評価及びリスク低減措置

（ア）アンケート結果

【質問1⑤】①内部者による不正情報流出リスク、②システム管理者又は運用保守従事者による不正情報流出リスクに対し、自らの所管する組織・部署の情報セキュリティ体制がどの程度脆弱であるか、また、そのような脆弱性に対して有効なリスク低減措置が実施されているかを、自ら又は部下に指示して検証・評価したことがありますか。

【質問1⑧】①内部者による不正情報流出リスク、②システム管理者又は運用保守従事者による不正情報流出リスク）に対し、自らの所管する組織・部署の情報セキュリティ体制がどの程度脆弱であるかを検証・評価するにあたり、その前提となる情報（システムの概要、取扱い情報の属性、リソース、インシデント情報等）が的確に自らに届いていると思いますか。

（イ）評価・考察

質問 1⑤のアンケートでは、半数にも及ぶ管理責任者等がリスクの特定、評価、リスク低減措置等の策定というリスクマネジメントプロセスを実施していないと回答している。このように回答した者の中には、質問 1①②で内部不正による情報漏洩リスクを認識していると回答した者が多数含まれていることからすれば、内部不正による情報漏洩リスクを意識しているとする者が具体的な対応を取っていない場合が存在することが明らかとなる。

また、質問 1⑤のアンケートでは、情報セキュリティ体制の脆弱性の検証・評価するに当たり、その前提となる情報が的確に届いているかという点につき「ど

ちらかというと、そう思わない」又は「そう思わない」との回答が 24%、「何が必要な情報かの判断がつかない。」との回答が 7%であった。このような回答を前提にすると、リスクマネジメントプロセスのスタート地点にすら立てていないケースが存在しうることになるため、管理責任者等にとって必要な情報が共有される仕組み作りが必要である。

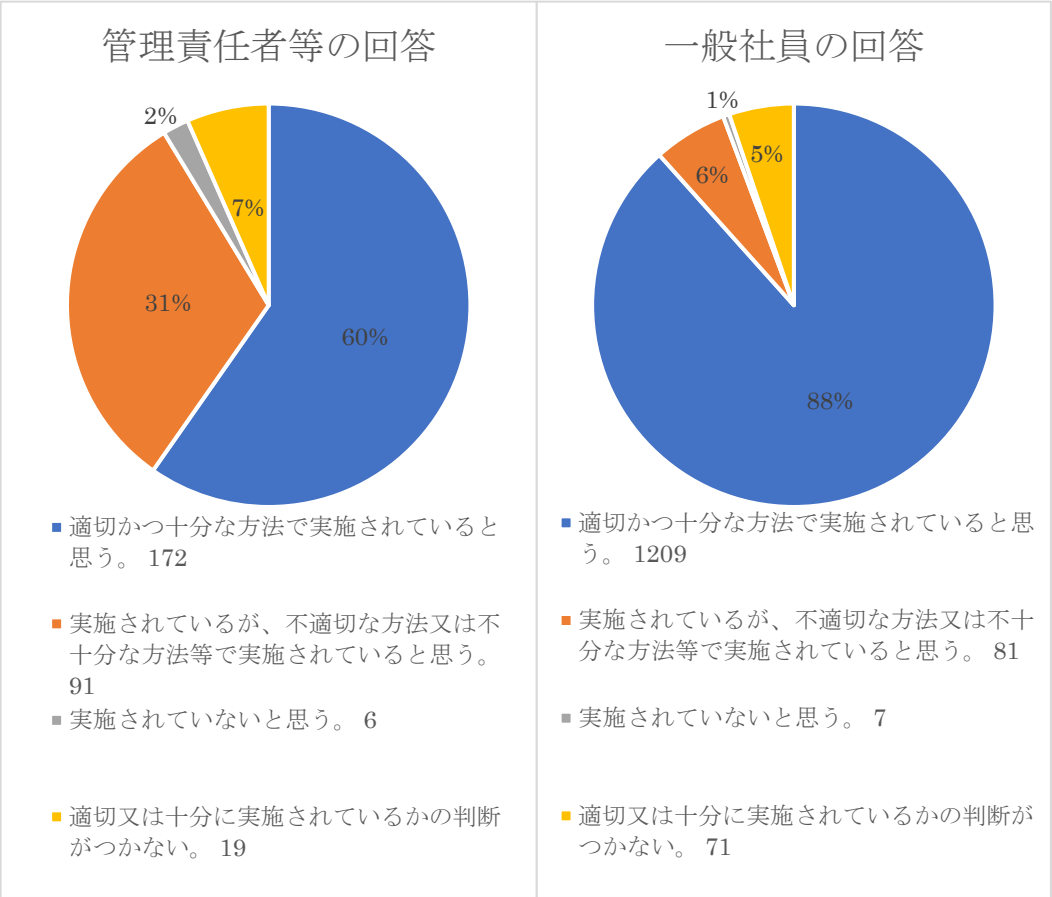
BS においては、前記第５・１⑹で指摘したとおり、本件不正持ち出しの原因・背景の一つとして、リスクマネジメントプロセスの不存在があったと考えられるが、上記アンケート結果は NTT 西日本グループ全体でも同様の状況が生じている可能性を示唆している。

なお、質問 1⑤の関連質問として、「質問 1⑤の検証・評価は、貴社内又は NTT 西日本グループ内においてどの部署が行うべきものと理解していましたか。」という点を確認した（質問 1⑥）。これに対する回答には、自社内の部署ではなく NTT 西日本の情報セキュリティ推進部及び CSOC 等が行うべきとする回答が相当数あった。このような回答は、BS について既に指摘したように（前記第５・１⑷イ（イ）参照）、NTT 西日本グループ全体の中のどの部署がグループ各社の情報セキュリティ体制を主導すべきかという組織設計上の課題があることを示唆しており、第 2 線としての機能を担う部署を明確化する必要性を裏付けている。

⑵　日常管理

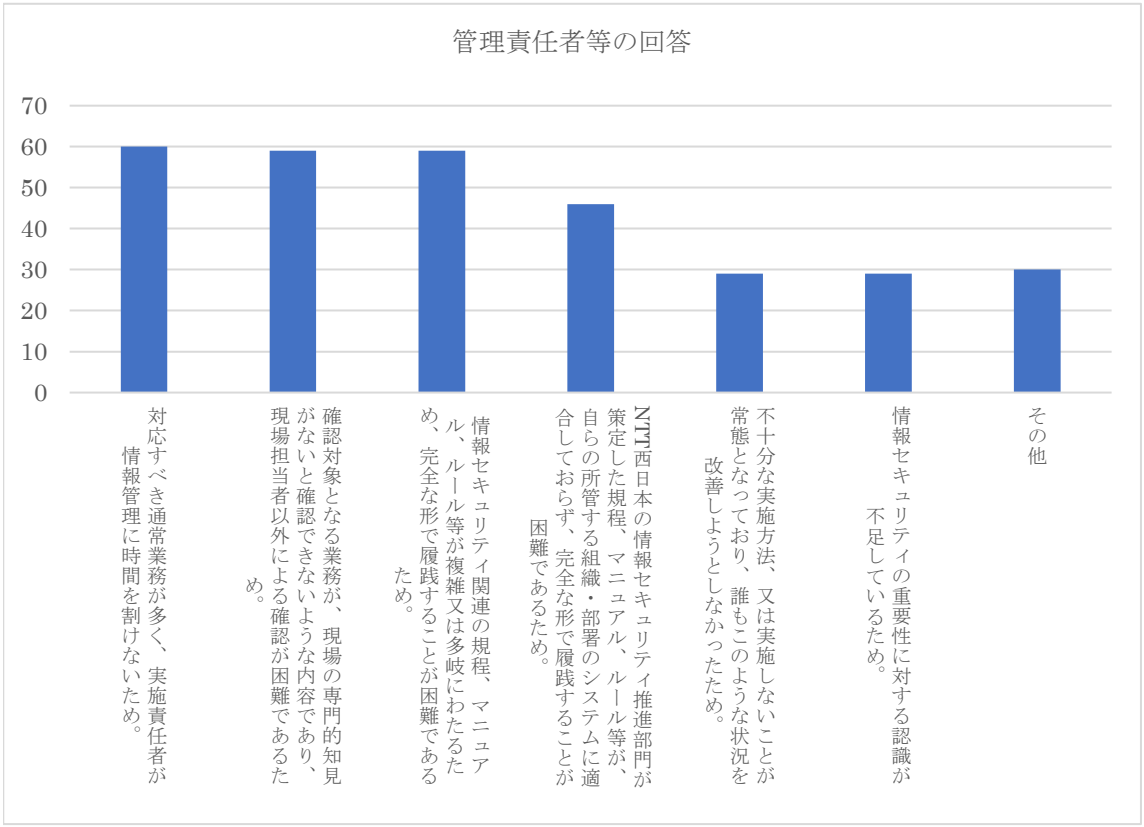
ア　アンケート結果

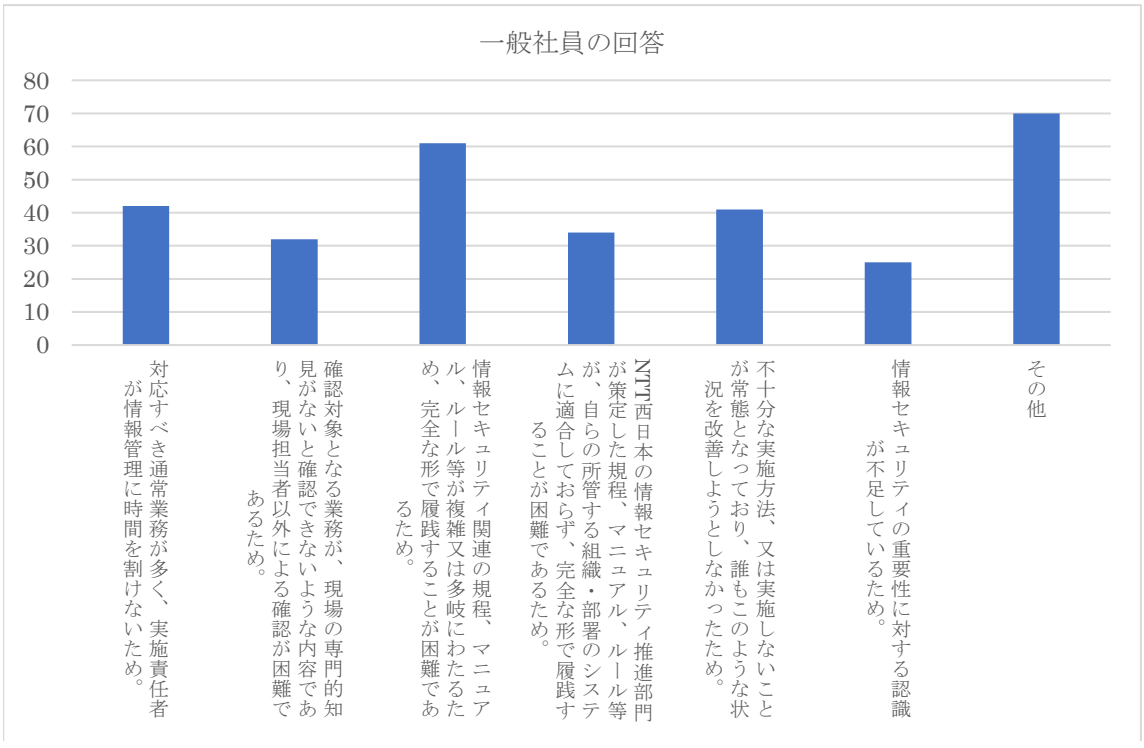
【質問 2①】自らが所属する部署における、お客様情報の日常管理（アクセス権限・パスワードの管理、私有の USB メモリその他の外部記憶媒体の利用禁止措置、端末設置場所の入退室管理、業務外利用の禁止措置等）は適切に実施されていると思うか。



【質問 2②】質問 2①で回答した状況の原因はどのようなところにありますか。（複数回答）

（質問 2①の回答が「適切かつ十分な方法で実施されている」以外の管理責任者 116 名及び一般社員 158 名が回答対象。）





イ　評価・考察

質問 2①のアンケートでは、お客様情報の日常管理につき、管理責任者等の 31%が「実施されているが、不適切な方法又は不十分な方法等で実施されていると思う。」と回答しており、NTT 西日本グループ全体でも、お客様情報の日常管理が不十分であるという認識を相当数が有していることが分かる。

質問 2②のアンケート結果によれば、不適切な方法又は不十分な方法等で実施されている原因については「対応すべき通常業務が多く、実施責任者が情報管理に時間を割けないため。」、「確認対象となる業務が、現場の専門的知見がないと確認できないような内容であり、現場担当者以外による確認が困難であるため。」及び「情報セキュリティ関連の規程、マニュアル、ルール等が複雑又は多岐にわたるため、完全な形で履践することが困難であるため。」を選択した割合が相対的に多い。管理責任者等のアンケート結果と一般社員のアンケート結果を対比すると、一般社員のアンケートでは「適切かつ十分な方法で実施されていると思う。」の割合が 88%であり、管理責任者等における 60%と比較して有意に多いことが大きな特徴である。現実には NTT 西日本グループ各社においても情報セキュリティ体制に不備が確認されていること（前記第 7 参照）を踏まえると、一般社員の「適切かつ十分な方法で実施されている」との認識は、実態を反映したものではなく、むしろ情報セキュリティに関する知見や遵守事項が一般社員にまでは十分に浸透していないことを示しているとも解釈し得る。

質問 2③の関連質問として、管理責任者等及び一般社員に対して、どのような点が不適切又は不十分であるか（質問 2④）を確認し、また、一般社員に対して、日常的な情報管理全般に対してどのような問題意識を持っているか（質問 2⑤）を確認している。その主な回答は下表のとおりである。このうち、質問 2⑤のアンケート結果には、アクセス権限・パスワードの管理の厳しさを問題点として挙げる意見も見受けられたが、これは一面では顧客の立場より業務遂行上の自らの利便性を重視することに繋がりかねないとも解釈し得る。

【質問 2④】「実施されているが、不適切な方法又は不十分な方法等で実施されていると思う。」または「実施されていないと思う。」の場合】どのような点についてそのように思いますか。不十分又は実施されていないと思う事項をご回答ください。

＜管理責任者等の回答＞

（実施されていないことを指摘するもの）

・ ルールが徹底できていない場面を目撃することがある。例えば 2 段階認証の設定が必須だが、していなかったというケース。

（ログの管理状況について指摘するもの）

・ アクセスログ等の確認について、十分に行なえていない部分があると思われる。（定期的なチェックが形骸化している面も含めて）
・ ログ等の取得、確認が実施されていなかった

＜一般社員の回答＞

（外部記憶媒体の管理状況について指摘するもの）

・ USB メモリは持っていないが使用可能ではある。
・ 私有の USB メモリは利用可能のため悪意をもって隠しもって入れば持ち出しが可能。ただし管理者の権限をもつ人による

（ログの管理状況について指摘するもの）

・ 改善中かと思うが、データの書き込み・郵送など記録を取っていないように思われる時があった。
・ 各種システムの利用ログやお客様端末へのリモートログインの履歴（いつ、誰が作業した等）が残っていない。また各システムを共用の ID で使用しているため、誰が操作したのか不明瞭。

【質問 2⑤】自らの所属する部署におけるお客様情報を取り扱うシステムの日常的な情報管理について、問題意識（気になっている点、おかしいと感じる点等）、お考え、要望、改善提案等がありましたら、ご記載ください。併せて、そのように考えるきっかけとなった具体的な場面やエピソード（いつ、どこで、誰が、何をしたか等）があれば、ご回答ください。

（現状について理解できていない旨指摘するもの）

- お客様情報に直接触れる機会がないためそれ以上はよくわからない。
- どのような対策を行っているかよく知らない

（情報セキュリティに関する研修・指導が必要である旨指摘するもの）

- 新しいサービスで新しいシステムを作成する際に、セキュリティ的に管理することや管理簿などの必要性について、アドバイスできるような環境があればよいと思う。
- 情報セキュリティに関する教育やトレーニングをこのようなアンケート形式でも良いので定期的に行うのはいかがか。時間のかかるものではなく、簡素なものでよいと思う。セキュリティ事故を起こさせないために意識に植え付けておくことが目的。

（マニュアルが不明確・難解である旨指摘するもの）

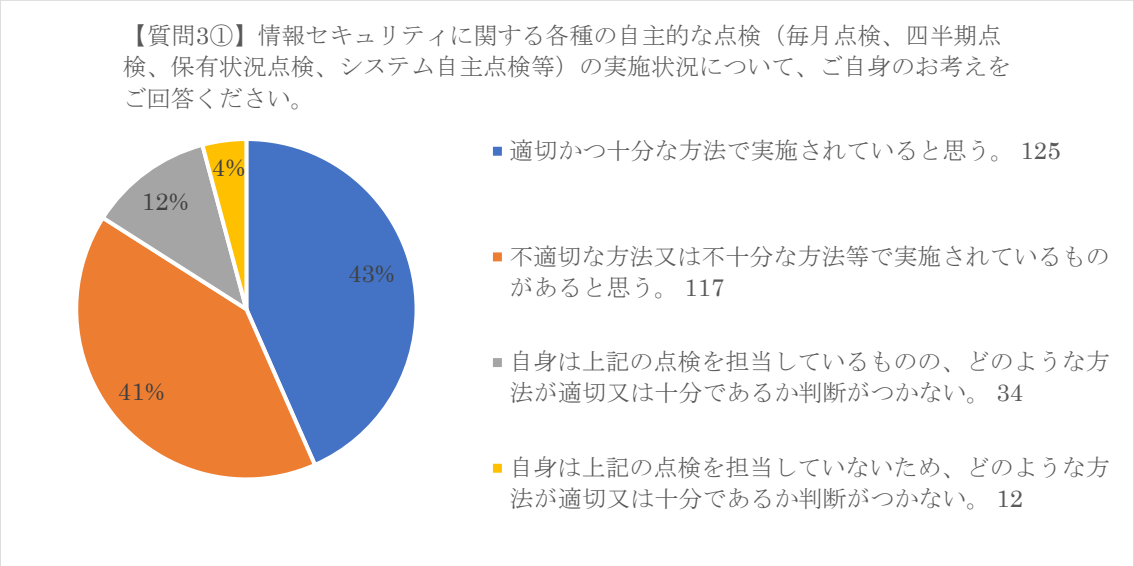
- それぞれの立場での取扱いに関するマニュアルの指示がすこし不明瞭に感じます。
-
- 諸々の規定が多ファイル、多ページあるため他の業務と並行してこれらをすべて読解するのは困難。ベストプラクティスの提示・AI チャットボットによるセキュリティに関する問合せの即回答を希望します。

（ルールに不備がある旨指摘するもの）

- お客様情報保護の観点ではよいことだと思うが、アクセス権限・パスワードの管理が厳しすぎると思われる。いざというときに柔軟な対応ができない。
- 業務で仕方ないと思いますが、閲覧権限などがざっくりと振り分けられている印象があります。

⑶　自主点検

ア　アンケート結果



イ　評価・考察

質問 3①のアンケートでは、自主点検の実施状況につき、管理責任者等の 41%が「不適切な方法又は不十分な方法等で実施されているものがあると思う。」と回答しており、NTT 西日本グループ全体においても、情報セキュリティの自主点検が機能不全に陥っている状況が見て取れる。

質問 3①の関連質問として、「不適切な方法又は不十分な方法等で実施されているものがあると思う。」と回答した理由・背景の具体的内容を確認している（質問 3③）。その主な回答は下表のとおりである。これによれば、そもそも自主点検が実施されていないケースもあり、BS で見られた自主点検の機能不全（前記第５・1（3）ア参照）よりも、深刻な状況が発生している部署が存在している可能性がある。このほかには、点検が形骸化していることを指摘する回答、点検者の能力に依存することを指摘する回答が多く見られた。このように見てくると、情報セキュリティ TF による本緊急点検の結果（前記第７参照）と同様、NTT 西日本グループの多くの子会社において、自主点検の仕組みが機能不全に陥っていると評価せざるを得ない。

また、質問 3①の関連質問として、管理責任者等に対し、「各種の自主的な点検（毎月、四半期点検、保有状況点検、システム自主点検等）のチェックポイントを確実に実践できていれば、想定される情報流出経路からの情報流出は有効に防止できると考えていましたか。」という点も確認している（質問 3⑥）。これに対して

は、管理責任者等の 65%が「いいえ」と回答しており、自主点検が適切に実施されたとしてもその有効性に疑問があることが示されており、自主点検の内容の改善、点検者における点検能力の涵養やリソースの配分といった点に対応することの必要性が見て取れる。

【質問 3③】質問 3①の回答が「不適切な方法又は不十分な方法等で実施されているものがあると思う」の場合、どのような点に問題があると思いますか。問題だとお考えの点検と当該点検の問題点をご回答ください。具体的な場面やエピソードがあれば、併せてご回答ください。

（点検が実施されていないことを指摘するもの）

- 年 1 回点検は実施しているものの、毎月、四半期の点検は実施できていない。
- 一部組織で現場での認識不足があり定期点検が実施できていないことがあった。

（点検の形骸化を指摘するもの）

- 点検シートの内容が形骸化されており、なぜその項目の確認が必要なのか説明を受けていない。
- 実態を個別確認せずに、前回報告内容を踏襲（コピー）して報告してるケースがある。
- マニュアル基づき実施をしているものの、しっかりと内容を熟知して点検を行っていないケースも想定されるため。
- 点検項目が過多。点検内容が所作・手段を問うものが多く曖昧であるため、回答者の拡大解釈により、勝手に代替手段を以て OK としてしまうケースが発生し得る。これが世代交代を繰り返すことにより、結果的に形骸化につながっているのではと想定。
- 点検等は前回、前年度踏襲するケースが散見され、前回点検結果の妥当性について踏み込んだ確認を実施していない
- 業務繁忙により点検が形骸化している

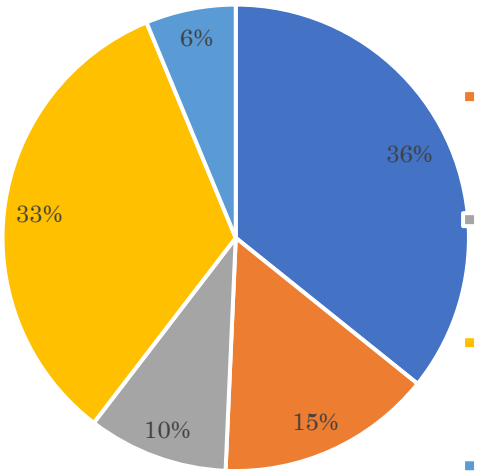
（点検者への依存及び点検者の知識不足を指摘するもの）

- 担当者への依存具合が大きいため、システム的な点検を導入するべきだと考えている。
- システムの具体的内容を把握しているのはシステム主管のみであり、システム主管のさじ加減で点検結果を記入する事が出来る。

⑷　目的外利用の監視

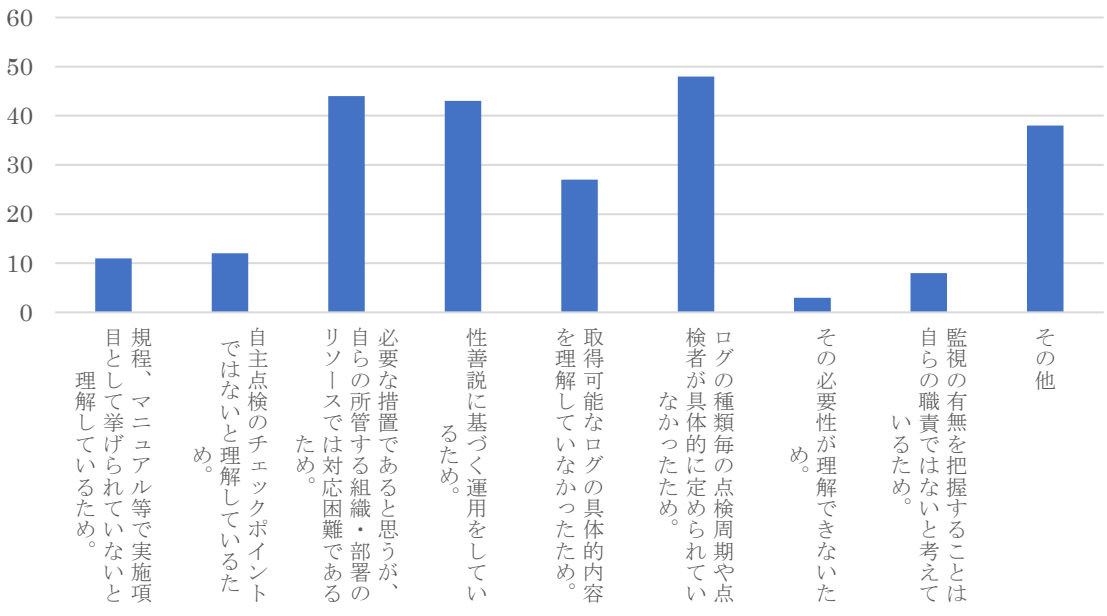
ア　アンケート結果

【質問4①】お客様情報を取り扱うシステムに対しアクセス権限を付与された者（システム管理者又は運用保守従事者を含む）が業務目的外で当該システムを利用していないかを監視する仕組みについて、ご回答ください。



- 該当するすべてのシステムについて、ログの種類毎の点検周期や点検者を具体的に定める等した上で、アクセス及びダウンロードログの定期的な監視をしている。 103
- 該当するすべてのシステムについて、ログの種類毎の点検周期や点検者を具体的に定められているが、実際には、アクセス及びダウンロードログの定期的な監視をしていない。 43
- 該当するすべてのシステムについて、アクセス及びダウンロードログの定期的な監視以外の方法で実効的な監視をしている。 28
- 全部又は一部のシステムについて、ログの種類毎の点検周期や点検者を具体的に定めていない等、実効的な監視の仕組みが存在しない。 96
- 監視しているか否か把握していない。 18

【質問4②】質問4①の状態が生じているのはなぜですか。当てはまる理由をご回答ください。（複数回答可能）
（質問4①において「全部又は一部のシステムについて実効的な監視の仕組みが存在しない。」又は「監視しているか否か把握していない。」と回答した役職員114名が対象。）



イ　評価・考察

質問 4①のアンケートでは、管理責任者等の 15%が「ログの種類毎の点検周期や点検者を具体的に定められているが、実際には、アクセス及びダウンロードログの定期的な監視をしていない」と回答し、33%が「全部又は一部のシステムについて実効的な監視の仕組みが存在しない」と回答しており、管理責任者等の約半数が、ログの監視が実施されていない又はそもそも監視の仕組みが存在しないとする。

BS においては、本件不正持ち出しを許した原因の 1 つとして、特権的アクセス権限を持っていた X による PDS サーバへのアクセス状況を監視していなかったことが挙げられる（前記第 4 の 2（2）参照)。質問 4①への回答は、かかる事象が本件不正持ち出しに特有のものではなく、NTT 西日本グループ全体においても同様の状況が相当数存在していることが示唆されている。

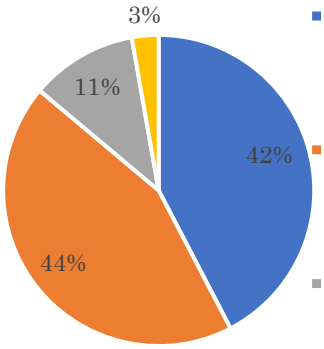
質問 4①の関連質問として回答の理由をさらに確認したところ（質問 4②。上記グラフ参照)、48 名が「ログの種類毎の点検周期や点検者が具体的に定められていなかったため。」と回答し、44 名が「必要な措置であると思うが、自らの所管する組織・部署のリソースでは対応困難であるため。」と回答しており、規程の不十分さやリソースに対する問題を提起している。なお、本項⑴でも言及した性善説についても 43 名が言及しているところ、かかる認識を速やかに改める必要があることは前述したとおりである。

以上に対して、管理責任者等の 10%程度が、アクセス及びダウンロードログの定期的な監視以外の方法で実効的な監視をしている旨の回答をしている。質問 4①の関連質問として、上記のような回答をした管理責任者等に対してどのような監視方法を実施しているのかをさらに確認したが（質問 4③)、これに対する回答としては、「作業管理簿の作成」、「管理者・現場監督者による職場巡回」及び「入退室の管理」といった方法を挙げるものが多かった。しかし、作業管理簿を作成するのみでは足りず、その真正を検証するためにはログの監視が必要となる。また、職場巡回などには限界があることを踏まえると、今後はログの定期点検や振る舞い検知といったシステム的な対応への移行が望まれる。

⑸　外部記録媒体の遮断措置

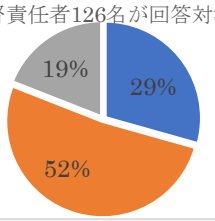
ア　アンケート結果

【質問5①】お客様情報の取扱いが可能な端末における外部記憶媒体（USBメモリ等）へのデータのコピー・書き出しの可否についてご回答ください。新たな調査は不要ですので、現時点でのご自身の認識でご回答ください。



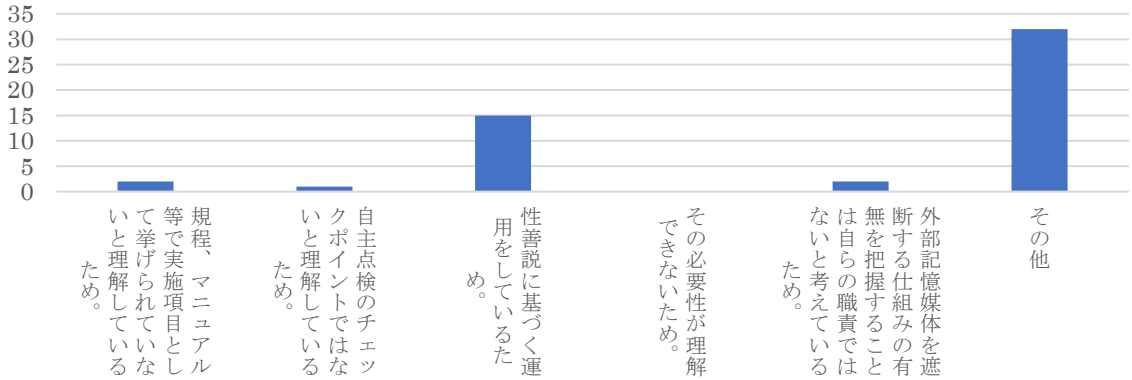
- 該当する全ての端末に対して、一切の外部記憶媒体へのデータのコピー・書き出しができないような措置を講じている。 122
- 該当する全ての端末に対して、許可された外部記憶媒体以外にはデータのコピー・書き出しができないような措置（物理的な措置として端末にUSBポートを設けない方法や、ソフトウェア制御によりコピー等を不可とする方法）を講じている。 126
- 全部又は一部の端末について外部記憶媒体を遮断する仕組みが存在しない。 32
- どのような仕組みが導入されているか把握していない。 8

【質問5②】許可された外部記憶媒体が悪用されていないかを検証する仕組みの有無をご回答ください。なお、質問5①の回答が「該当する全ての端末に対して、許可された外部記憶媒体以外にはデータのコピー・書き出しができないような措置（物理的な措置として端末にUSBポートを設けない方法や、ソフトウェア制御によりコピー等を不可とする方法）を講じている。」の監督責任者126名が回答対象。



- ログ監視をしている。 37
- ログ監視以外の方法で検証している。 65
- 検証する仕組みは存在しない。 24

【質問5③】質問5①の回答が「全部又は一部の端末について外部記憶媒体を遮断する仕組みが存在しない。」又は「どのような仕組みが導入されているか把握していない。」の場合、そのような状態が生じているのはなぜですか。（複数回答）



イ　評価・考察

（ア）外部記録媒体の遮断措置についての認識

質問 5①のアンケートでは、管理責任者等の 11%が「全部又は一部の端末について外部記憶媒体を遮断する仕組みが存在しない。」と回答している。USB メモリ等の外部記録媒体の制御は情報セキュリティの基本中の基本であり、11%もの管理責任者等がこのように回答していることからしても、NTT 西日本グループとしてこの点への対応を急ぎ進める必要があることを裏付けている。

加えて、質問 5①のアンケート結果からは、管理責任者等が自らの関与するシステムの状況について正確な知見を持っていないという状況も見て取れる。ProCX を例に挙げると、ProCX の管理責任者等の 75%は質問 5①に対し「該当する全ての端末に対して、一切の外部記憶媒体へのデータのコピー・書き出しができないような措置を講じている。」との回答を選択している。しかし、ProCX の本緊急点検の結果（前記第 7 の 3⑶イ）にあるとおり、実際には許可された USB メモリであれば使用可能な状況であり、一切の外部記録媒体を使用できないといった認識は誤っている。

これらを踏まえると、外部記録媒体を適切に遮断するための仕組み作りに加え、自らが使用している情報システムの理解を促進することが必要となる。

（イ）外部記録媒体が悪用されていないかを検証する仕組み

質問 5①の関連質問である質問 5②において、許可された外部記録媒体が悪用されていないかを検証する仕組みの有無についても確認しているが（質問 5①において「許可された外部記憶媒体以外にはデータのコピー・書き出しができないような措置を講じている」と回答した 126 名が回答対象）、これに対し、管理責任者等の約 20%が「検証する仕組みは存在しない。」と回答している。許可された外部記録媒体を悪用する可能性がある以上、許可の前提となった使用目的及び実際の作業内容を検証する必要があることは明らかであり、ログ等による検証を可能にすることが必要であることは言うまでもない。

また、質問 5①の関連質問として、「全部又は一部の端末について外部記憶媒体を遮断する仕組みが存在しない」又は「どのような仕組みが導入されているか把握していない」状態が生じている理由をさらに確認している（質問 5③）。これに対する回答は、「性善説に基づく運用をしているため。」との回答が多く、このほか「その他」における自由記述として「セキュリティルールが浸透しきっておらず、利便性が優先されるため」、「システムメンテナンス時の資材の持込や、

エビデンスの取得、トラブル対応等のログ抽出の際に必要であるため」といった利便性を理由とする回答が複数確認された。ここでも性善説に言及するものが多いことは由々しき事態と言わざるを得ないが、その他として記載されている事項についても、BS において、技術的な管理に係る措置が長年放置されてきた背景と共通するものであり、内部不正による情報漏洩に対する危機意識の低さの表れとも評価し得る。

⑹ インシデント対応

ア アンケート結果

【質問 6①】本セクションにて、管理責任者等及び一般社員に対して、お客様情報の漏洩又はその可能性を認識しながら、上長又は最終報告対象者に所定の報告、エスカレーションを行わなかったことがあるかとの質問に対しては、7 名の役職員（管理責任者等 3 名、一般社員 4 名）がエスカレーションを行わなかったことがあると回答した。

【質問 6②】取引先から、お客様情報の漏洩又はその可能性を指摘されながら、情報漏洩の事実又はその可能性を隠ぺいしたり、事実と異なる調査結果を報告したりするなど、当該取引先に対し、適切な報告をしなかったことはあるかとの質問に対しては、管理責任者等及び一般社員の全員が「いいえ」（つまり、情報漏洩の事実又はその可能性を隠蔽したり、事実と異なる調査結果を報告したという事象はない。）と回答した。

イ 評価・考察

本アンケート項目は、本件過去調査の実態解明を通じ、エスカレーションの懈怠や顧客に対する不適切な報告が行われていることが確認されたことから、NTT 西日本グループ全体でも同様の兆候がないかを検証する趣旨で設けられた。

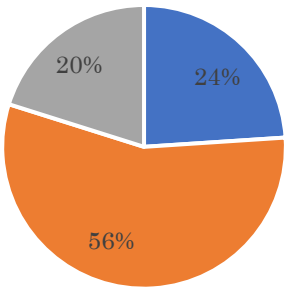
質問 6①のアンケートでは、一部の管理責任者等や一般社員がエスカレーションを行わなかったことがあると回答したが、個別に確認したところ、本質的に問題視すべき事案は検出されなかった[72]。

[72] 当調査委員会が、質問 6①においてエスカレーションを行わなかったことがあると回答した 7 名の役職員に対して、追加で個別的な確認を行ったところ、このうち、2 名が既にエスカレーション済みの事案のことを回答したこと、別の 2 名が（個別具体的なインシデントを離れて）上長に対して理論上考え得るリスクを報告しなかったという趣旨で上記回答を行ったこと、及びさらに別の 2 名が誤って上記回答をしたことが分かった。また、残る 1 名については、20 年以上前に、社外の顧客宛てのメールを送信する際に、送信先に別の顧客のメールアドレスを誤って含めて送信してしまった事案について、エスカレーションを行

⑺　システム管理者又は運用保守従業者を取り巻く状況

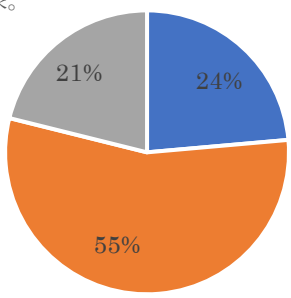
ア　アンケート結果

【質問7①】 自らの所管する組織・部署におけるお客様情報を取り扱うシステムについて、特定のシステム管理者又は運用保守従事者が長期間（3年超）にわたり同一の業務に従事し続ける状況の有無について把握していますか。



- そのような状況はない。 69
- そのような状況はある。 161
- そのような状況の有無を把握していない。 58

【質問7②】自らの所管する組織・部署におけるお客様情報を取り扱うシステムについて、特定のシステム管理者又は運用保守従事者が長期間（3年超）にわたり同一の業務に従事し続ける状況について、情報セキュリティ上の問題として捉えていますか。なお、質問7①において、特定のシステム管理者又は運用保守従事者が長期間にわたり同一の業務に従事し続ける状況があると回答した役職員161名が対象。



- 情報セキュリティ上の問題として捉え、特定のシステム管理者又は運用保守従事者による不正情報流出のリスクを念頭においた具体的なリスク低減措置を実施している。 38
- 情報セキュリティ上の問題として捉えているが、具体的な対策（リスク低減措置）を講じるまでには至っていない。 89
- 情報セキュリティ上の問題として捉えていない。 34

わなかったとのことであった（なお、当該メールには、顧客名簿などの重要な情報は含まれていなかったとのことであった。）。当該従業員がエスカレーションを行わなかった理由は、速やかに顧客に謝罪したところ、顧客からの理解を得ることができ、当該案件が解決したためであった。

イ　評価・考察

質問 7①のアンケートでは、管理責任者等の過半数が、「そのような状況はある。」すなわち、特定のシステム管理者が 3 年超にわたり同一の業務に従事し続ける状況があると回答している。

前記第５・１⑺イのとおり、情報システムに対して特権アカウントを持つ特定の者への依存とその固定化は、内部不正による情報漏洩リスクを高める要因であるが、上記のアンケート結果からは、NTT 西日本グループ全体において同種のリスク要因が一定数存在していることが明らかとなる。

次に、質問 7②のアンケートにおいて、このような固定化により生じるリスクに対して具体的なリスク低減措置を実施していると回答した管理責任者等は全体のわずか 24%にとどまった。そして、55%の管理責任者等は特定の従業員が長期間にわたり同一の業務に従事し続けることを情報セキュリティ上の問題として捉えているものの、具体的な対策を講じるまでには至っていないと回答し、21%の管理責任者等はそもそもリスクとして捉えてすらいないと回答する。

質問 7②関連質問として、問題意識を持ちつつも状況改善が困難と回答した者に対し、さらにその理由を確認した（質問 7③：下表参照）。ここでは、「システム保守に精通した社員の育成や人事異動が難しい。」、「システムの開発維持運用保守業務に関しては、ノウハウ定着までに多くの時間を要するため 3 年以上従事することが多々ある。」、「業務が属人化している面があり、人的リソースの短期入れ替えが発生すると業務運営が難しくなる可能性がある。」といったような回答が多く、長期間同一の業務に配置せざるを得ない状況が存在していることが見て取れる。このような人員リソースに関連する NTT 西日本グループ全体の問題として、経営陣のコミットメントの下で対応する必要がある（後記第９・１⑵ア参照）。

【質問 7③】質問 7②の回答が「情報セキュリティ上の問題として捉えているが、具体的な対策を講じるまでには至っていない。」の場合、情報セキュリティ上の問題意識を持ちつつも、状況改善が困難な事情があれば、当該事情をご回答ください。

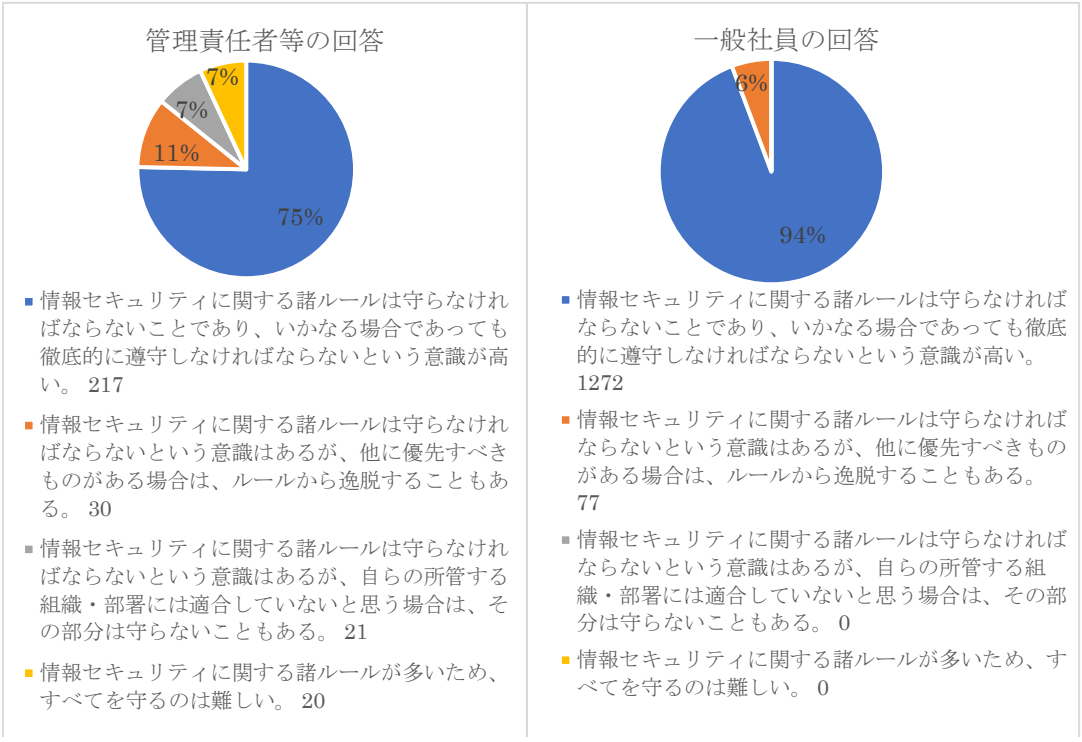
- システム保守に精通した社員の育成や人事異動が難しい
- システム管理従事者は高いスキルが必要であり、代わりの人材が不足している（育成出来ていない）
- システム管理者は専担者ではなく複数の総括的な業務を実施しており、現状は業務運営上全て３年で異動させるのは難しい状況
- システムの開発維持運用保守業務に関しては、ノウハウ定着までに多くの時間を要するため３年以上従事することが多々ある

⑻　組織風土

ア　組織・部署全体の情報セキュリティに対する意識

（ア）アンケート結果

【質問 8①】自らの所管する組織・部署全体の情報セキュリティに対する意識について、どのように思いますか。



（イ）評価・考察

管理責任者等の 11%、一般社員の 6%が、「情報セキュリティに関する諸ルールは守らなければならないという意識はあるが、他に優先すべきものがある場合は、ルールから逸脱することもある。」と回答した。

BS については、前記第５・１⑵ア（エ）で指摘したとおり、情報セキュリティ上のルールが遵守されていなかった背景として業務を優先せざるを得ない状況が存在していたが、NTT 西日本グループ各社の少なくともその一部には同様の状況が存在している可能性がある。

本アンケート調査では、上記回答に関連して、他に優先すべきものがあるルールから逸脱することもある」とはどのような場合かを確認している（質問 8②）。これに対する回答の代表例は下表のとおりである。

【質問 8②】質問 8①の回答が「情報セキュリティに関する諸ルールは守らなければならないという意識はあるが、他に優先すべきものがある場合は、ルールから逸脱することもある」の場合、ルールから逸脱せざるを得ないのはどのような場合ですか。具体的な場面やエピソードがあればご回答ください。

＜管理責任者等の回答＞

（顧客対応を理由とするもの）

- 現場におけるお客様要望にその場で応える必要がある場合
- お客様影響があるサービス・システムの故障
- システム不具合や故障対応においてログ抽出等の作業があり、外部記憶媒体に書き出す際に、管理簿への記載や電子承認を後回しにすることがある。（後日管理簿へは記載を実施）

（納期・業務の繁忙状況を理由とするもの）

- 業務運用上、セキュリティ確保にかける工数がない。納期が守れない。
- 費用も人員も足りない中で、スケジュール（納期）に追われているため
- 業務が忙しい時など、自らの確認を徹底せずに、点検者の報告内容を信じて承認したことがある。
- トラブル時のお客様情報の管理、その後の削除まで含めた運用管理で確認が取れてなかった点

＜一般社員の回答＞

（顧客対応を理由とするもの）

- 既存システムではお客様への最適なサービス提供ができない場合。特に現場でお客様とやり取りされる方々は多いように感じる
- 装置の故障やシステムの不具合が発生することにより、お客様の業務に影響が出ている場合。またはお客様より設定関連の緊急のオーダーが入り、納期に間に合わせなければならない場合。

（納期・業務の繁忙状況等を理由とするもの）

- 将来的に諸ルールに合わせて対応する予定があっても、期日切迫などにより対応が後回しになっていると短期間的にもルールから逸脱していたと判断しました。
- システムを開発するにあたり、スケジュール遵守が最優先となっている。

（適式な手続を行った場合にかかる手間・時間を理由とするもの）

- エスカレーション先がわからないほど高いのに、リスクはごく少ない場合。
- スピーディな対応が求めら、かつルールを多少逸脱しても問題が顕在化しないと想定される場合。

また、質問 8①において「情報セキュリティに関する諸ルールは守らなければならないという意識はあるが、自らの所管する組織・部署には適合していないと思う場合は、その部分は守らないこともある」と回答した者に対して、「適合していないと考える部分はどのような部分か」という点をさらに確認している（質問 8③）。その代表的な回答は下表のとおりである。このうち、NTT 西日本グループの統一的な基準が自組織に整合していないという趣旨の回答は、各組織において、どのようにして当該基準に適合させていくかが十分に議論・検討されていない状況を示唆するものとも評し得るため、グループ各社・各レベルにおいてリスクマネジメントプロセスの確立が求められる（後記第９・３⑶ウ参照）。

【質問 8③】質問 8①の回答が「情報セキュリティに関する諸ルールは守らなければならないという意識はあるが、自らの所管する組織・部署には適合していないと思う場合は、その部分は守らないこともある」の場合、情報セキュリティに関する諸ルールが自らの所管する組織・部署には適合していないと考える部分はどのような部分ですか。どのような部分がどのように適合していないか、具体的にご回答ください。

＜管理責任者等の回答＞

（ルールが個別のサービス・システムに適合していないことを理由とするもの）

・ 事業化業務に準じた内容のルールが規定されていることが一部ある点

（役職員のスキル・経験・意識等を理由とするもの）

・ 上記の設問の内容とズレるかもしれないが、セキュリティが重要と考える人と考えない人の差が激しい。セキュリティを遵守することが評価される会社ではないため、守らずに効果を最短で出そうと考える人間が必ずいる。

（ルールの複雑さを理由とするもの）

・ ルール運営や解釈に幅があり、ゼロイチで判定がむつかしく、現場での解釈幅が許容されていると思う。また、ルールが一律で、特にクライアント要請に柔軟に対応すべき部署やシステムでは、最大幅で運営せざるを得ない状況が存在するのでは。その幅が、組織的な責任で認知設定できていない。

＜一般社員の回答＞

（ルールが個別のサービス・システムに適合していないことを理由とするもの）

・ お客様情報を含むデータベース(WINKS)にはアクセスするが、自分の所属するチームではお客様情報を USB で持ち出す業務はない。したがって、同部署内の別チームには必要であってもこちらのチームでは適合していない(過剰)なルールがある。

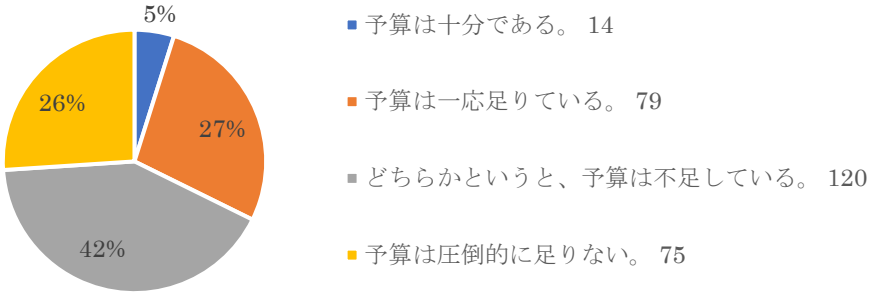
（役職員のスキル・経験・意識等を理由とするもの）

・ このケースはこう処理すれば問題ないというような情報が圧倒的に不足しており、そもそもルールがどうなっているかの正しい知識を持つものもいないと感じる。（上長に確認しても人によって回答が違う。）

イ　情報セキュリティの確保に必要な予算・人員数・役職員のスキル

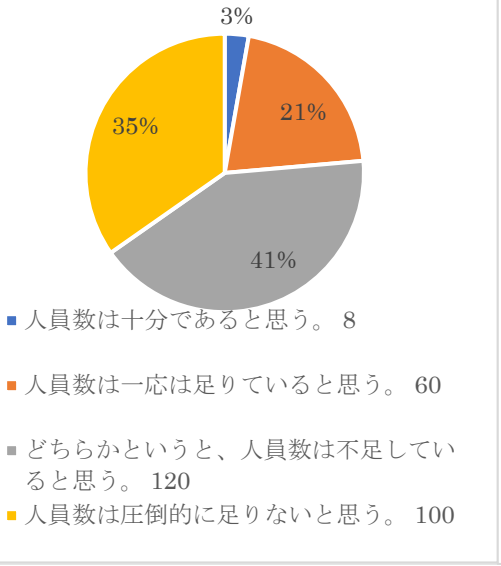
（ア）アンケート結果

【質問8④】自らの所管する組織・部署に関し、情報セキュリティ関連の諸ルールで要求される内容を実現するための予算が十分かどうか、ご自身のお考えをご回答ください。

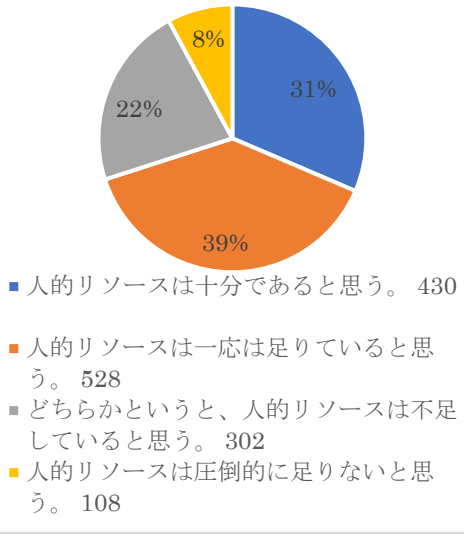


【質問 8⑤】自らの所管する組織・部署に関し、情報セキュリティ関連の諸ルールで要求される内容を実現するための人員数は十分だと思いますか。ご自身のお考えをご回答ください。

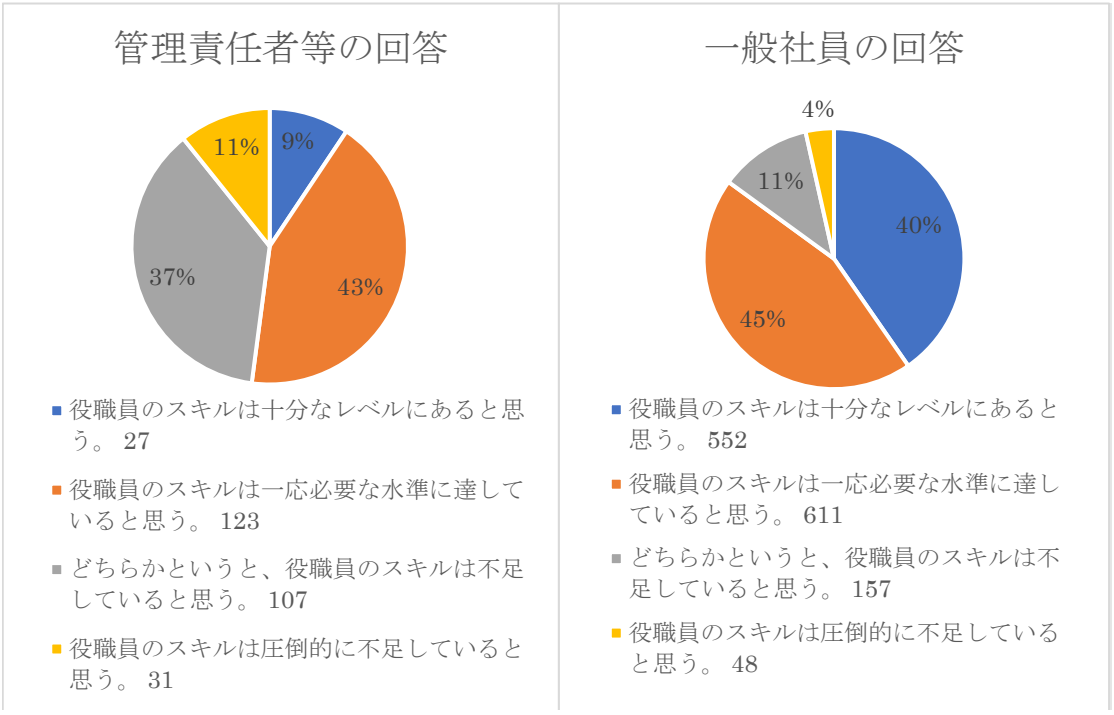
管理責任者等の回答



一般社員の回答



【質問 8⑥】自らの所管する組織・部署に関し、情報セキュリティ関連の諸ルールで要求される内容を実現するための役職員のスキルは十分だと思いますか。ご自身のお考えをご回答ください。



（イ）評価・考察

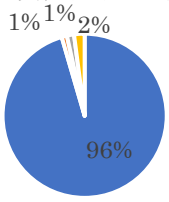
予算、人員数及びスキルに関するアンケート結果を比較すると、管理責任者等としては、情報セキュリティ関連の諸ルールで要求される内容を実現するためには、役職員のスキルよりも、予算及び人員数の確保が重要であると認識していることが示唆されており、予算割当てや人事施策の見直しが必要と思われる（後記第９・３⑸ア参照）。

ウ　上司との関係性

（ア）アンケート結果

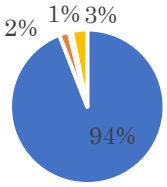
【質問 8⑦】自らの所属する部署において不祥事その他の重大な問題（情報セキュリティ上の問題に限られません。以下同様。）が生じた場合の上司との関係性について、どのように思いますか。

管理責任者等の回答



- 上司に対して、不祥事その他の重大な問題を報告できる関係性がある。 275
- 上司に対して、不祥事その他の重大な問題を報告しにくい雰囲気がある。 3
- 過去は、上司に対して、不祥事その他の重大な問題を報告できる雰囲気ではなかったが、現在、改善しつつある。 4
- いずれともいえない。 6

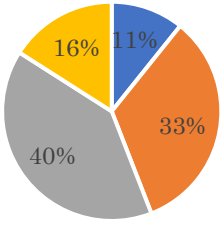
一般社員の回答



- 上司に対して、不祥事その他の重大な問題を報告できる関係性がある。 1287
- 上司に対して、不祥事その他の重大な問題を報告しにくい雰囲気がある。 28
- 過去は、上司に対して、不祥事その他の重大な問題を報告できる雰囲気ではなかったが、現在、改善しつつある。 9
- いずれともいえない。 44

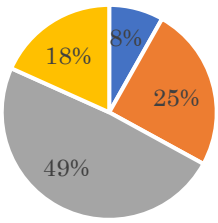
【質問 8⑩】自らの属する組織・部署において不祥事が発生した場合、不祥事が発生したこと自体が自身の人事評価に悪影響を及ぼすか否かという点について、ご自身のお考えをご回答ください。

管理責任者等の回答



- そのような傾向が強いと思う。 31
- どちらかというと、そのような傾向があると思う。 96
- どちらかというと、そのような傾向はないと思う。 115
- そのような傾向は全くないと思う。 46

一般社員の回答



- そのような傾向が強いと思う。 112
- どちらかというと、そのような傾向があると思う。 339
- どちらかというと、そのような傾向はないと思う。 667
- そのような傾向は全くないと思う。 250

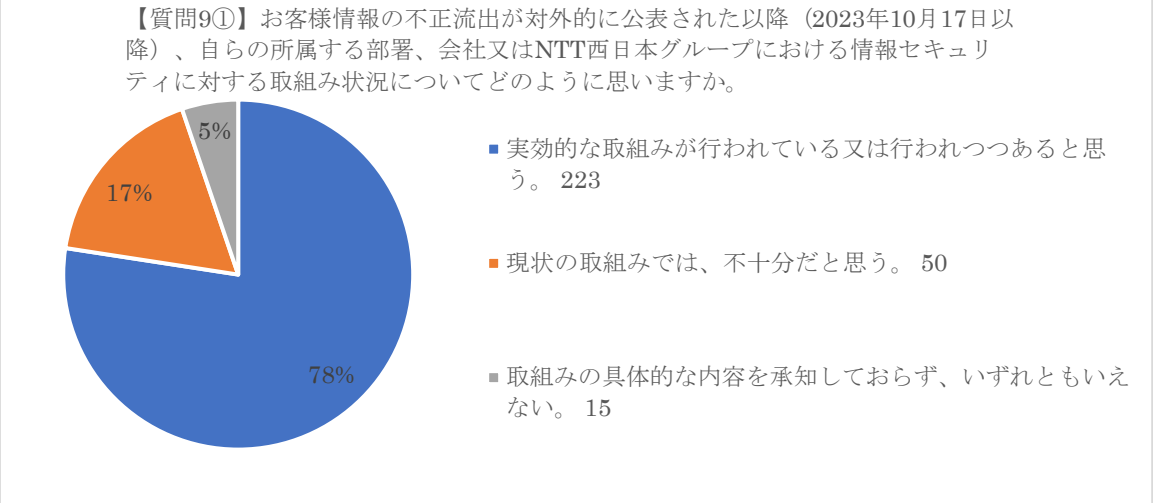
（イ）評価・考察

質問 8⑦のアンケートに対しては、管理責任者等の 96%及び一般社員の 94%が「上司に対して、不祥事その他の重大な問題を報告できる関係性がある。」と回答した。

このような回答結果は、一見、組織の風通しの良さを表しているようにも思われる。しかし、質問 8⑩のアンケートは不祥事が発生したこと自体が自身の人事評価に悪影響を及ぼすと思うかを質問するものであるが、この質問に対しては、管理責任者等のうち 44%が、一般社員のうち 33%の役職員が、「そのような傾向が強いと思う。」又は「どちらかというと、そのような傾向があると思う。」と回答している。このような回答は、自身の人事評価に悪影響を及ぼすことを回避するために報告を上げないという動機が形成されやすい状況があることを示唆しており、このような状況は実際に情報漏洩を含む不祥事が起きた際の迅速なエスカレーションの障害になり得るため、人事評価の在り方も含め配慮が必要であると考えられる。

⑼　本件不正持ち出しを受けて

ア　アンケート結果



イ　評価・考察

質問 9①のアンケートでは、管理責任者等の 17%が「現状の取組みでは、不十分だと思う。」旨の回答をした。本アンケート調査では、そのように考える理由についてさらに確認をしているが（質問 9③）、その代表的な回答は下表のとおりである。今後の取組の方向性に疑問を感じているというよりは、取組が形式的なものにとどまるのではないかとの不安や予算・人員・スキル等のリソースへの懸念など今後の取組の実現可能性への問題意識が多い。

【質問 9③】質問 9①の回答が「現状の取組みでは、不十分だと思う。」の場合、どのような点が不十分だと思いますか。ご意見をご記載ください。

（対応・チェックが形骸的であると指摘する回答）
- 本当にそこまで必要なのかという事項もある。すべてを金太郎あめ的に対応しようとしている気がする。
- 規程類、点検項目などが複雑化しており、不要そうな点検項目なども見受けられる。必要以上に点検項目を増やして形式的なチェックとなってしまうのであれば、重要な項目に絞って点検するなどの改善が必要と考えます。
- チェックを社員の稼働を膨大にかけて行っているが、本質的に実効性のある監査体制（通常業務の範囲で実施できる状態）にはまだ相当の時間がかかると思うため。

（予算・人員・スキル等のリソースが不足する旨指摘する回答）
- コスト削減をしすぎてチェック体制は十分でないと感じているため。
- ガーディアンや定期検査などチェック体制はあるが、サービス運用側の裁量が大きく、担当のスキル不足で正確な報告が行われないケースがありそうだと感じる。
- 情報セキュリティに対しどのように対処すれば良いかのスキルが足りない。
- 業務を行う人材の適正化、リソース設計の見直し、取得情報に基づく分析強化対策
- 性悪説での対処（ログ取得とチェック）に対応するシステム整備、チェック体制（人材）

（グループ内における情報共有の不足を指摘する回答）
- NTT 西日本　情報セキュリティ推進部（関連タスクフォース）よりヒアリングシートによる各種点検が実施されているが、点検上　不備となる項目に対して　システム導入による対応策を検討しているがその導入費用について　社内をサポートする（費用支援いただける）情報展開が無い点
- まだ末端まで具体的な情報がおりてきていない

また、本アンケート調査では、管理責任者等、一般社員の双方に、情報セキュリティという面で問題だと思うこと、気になっていることを確認している（質問 9③）。その代表的な回答は下表のとおりであるが、ルールと実務の乖離、チェック項目の形骸化とそれに伴う業務負担の増大等を挙げている回答が目立つ。NTT 西日本グループとしては、このような指摘を踏まえ、内外に、リソースの手当てを含め、実効性ある再発防止策及び課題への対処策を示していく必要がある。

【質問 9⑤】これまでご回答いただいた内容以外に、情報セキュリティという面で、自らの所属する部署、会社又は NTT 西日本グループの組織風土について、問題だと思うこと、気になっていること等があれば、ご回答ください。

＜管理責任者等の回答＞

（ルールと実務の乖離を指摘するもの）

・ 電話交換機の時代からセキュリティの考え方が全く変化していないセキュリティのルールと業務とが乖離しているために「例外対応」や「セキュリティの穴」が意図的に作られざるを得ない状態であることを認識し、業務の変化に応じてセキュリティルールの変更と制御、抑止するべきポイントを集約・明確にし、コストをかけて、システム的に抑止する仕組みを導入するべきである

（人的リソース・スキル・経験等に関するもの）

・ 人事異動などの機会にセキュリティのノウハウなどを引き継ぐのはかなり難度が高く、先にも述べたように時間の経過とともに低減していくスキルを補う方法を検討しない限り、有スキル者への依存が大きくなり今回のような事象につながるのではないかと判断する長期間の同業務へ従事させない体制とスキルの移転・向上のバランスを人事要員が少ない中でどのように図っていくかが課題となるように思われる

＜一般社員の回答＞

（形骸化したチェック項目やこれに伴う業務負担の増大などに関するもの）

・ セキュリティインシデントが起こる度に形式的なチェック項目が増えていくため、現場としては必要性は理解しつつ煩わしさは感じていると思う。また、過去業務遂行において負担になり形骸化しているものもあると思うし、そういったのは新しく入ってきた社員等は知らない事も多いので再発防止という観点でどれだけ意味を成しているかが分からない。社員のセキュリティ意識を高める事も大切だが、業務慣れからふと意識していない時にインシデントが発生しないような土台を作る方向性も大切だと考える。

（派遣社員等の管理等に関するもの）

・ 業務を外部に切り出してアウトソースすると、より自社で業務完結するよりも、強めのセキュリティ強度を構築しなければならないため、内製化かアウトソースかの投資判断にも影響してくると感じる。また、改めてエンゲージメントの向上が必要だと思った。

（人的リソース・スキル・経験等に関するもの）

・ 管理をするためには十分な人的リソースが必須であるものの、業務にリソースが圧迫されており、全組織で十分な管理をすることは現実的に不可能と考えている。

第９　再発防止策等の提言

これまで見たとおり、本件不正持ち出しを許し、これを長年見過ごしてきたことの一次的責任が本件システムを運用する BS にあることは論を待たないが、前記第５のとおり、ProCX には個人情報の取扱いに係る委託者としての管理上の問題があり、NTT 西日本には NTT 西日本グループを主導する親会社における子会社管理上の問題があると認められる。

そこで、以下では、BS、ProCX 及び NTT 西日本のそれぞれについて本件不正持ち出し及び本件過去調査の再発防止策を提言するとともに、これを契機とした NTT 西日本グループ全体の情報セキュリティ体制の改善に向けた提言を行う。

１　BS について

⑴　技術的な管理措置についての対処策

ア　技術的な管理措置について BS が実施した対処策

BS では、本件不正持ち出しが確認されたことを受け、NTT 西日本の情報セキュリティ推進部及び情報セキュリティ TF と連携しつつ、本件システムに関し、技術的な管理措置について対処策を実施した。前記第７・２⑵イのとおり、2024 年１月末日時点の BS における本件システムの点検結果は点検 44 項目のうち不備事項は２項目となった。情報セキュリティ TF は、これらの対処について、検証を行ったところ、情報漏洩防止の効果が期待できるものであり、後記⑵の追加対処策を要するものの、BS における本件システムに対する現時点の対応として妥当なものであると判断した。

このうち、本件不正持ち出しの直接的な原因に対して BS が実施した具体的な対処策は以下のとおりである。

（ア）PDS サーバからの顧客データのダウンロードを制御する措置

前記第４・１⑴のとおり、X が使用することを許されていたシステム管理者アカウントには、ProCX が設定する各テナントに保存されている全ての顧客データをダウンロードする権限が付与されており、事前承認を得ない限り顧客データのダウンロードを不可とするような技術的な制限措置は講じられていなかった。その上、前記第４・１⑷のとおり、システム管理者アカウントは、X を含む本件システムの複数の運用保守従事者の間で共用されていたことから、本件シ

ステムの複数の運用保守従事者であれば、上記権限を用いて顧客データを保守端末にダウンロードできる状態であった。

そこで、以下の段階的な措置により、最終的には、BS において PDS サーバからの顧客データのダウンロード権限を有するアカウントを保持しないものとし、業務上の必要性から、BS が PDS サーバから顧客データのダウンロードをする場合には、ProCX の承諾を得て、ProCX からシステム管理者アカウントの付与を受けるという方法に変更した。

まず、保守端末と PDS サーバを繋ぐ本件ネットワーク内に中継サーバを設置することで、アカウントに付与された顧客データのダウンロード権限の有無にかかわらず、保守端末に顧客データをダウンロードできないようにする対処策を講じた。具体的には、2023 年 8 月 5 日、PDS サーバに格納されている顧客データをダウンロードする場合には、必ず中継サーバを経由し、ダウンロード先が中継サーバになるよう設定し、保守端末からはリモートデスクトップ接続で、中継サーバにダウンロードされた顧客情報を閲覧することだけが可能となるよう対処を行った。

次に、システム管理者アカウントについては、共用アカウントの利用を停止した上で、業務上必要な最小限の範囲で、担当者に個人単位のアカウントを付与することとした。具体的には、同年 8 月 9 日、X 所属グループで本件システムの運用保守全般を担当するバック SE チームの担当課長及び同チームの担当者の 2 名にのみ、個人単位のシステム管理者アカウントを付与する運用に変更した。

その後、BS と ProCX が協議し、2024 年 1 月 26 日以降は、BS がシステム管理者アカウントを用いて行っていた業務（ProCX からの本件システムに関する問い合わせ対応のうち、顧客データ等 、ProCX が PDS サーバに格納するデータを取り扱う必要がある業務）は、ProCX において問合せ対応窓口を設け、ProCX が自ら行うこととした[73]（なお、これに伴い、システム管理者アカウント

[73] 当該業務以外の、本件システムに関する保守業務（機器故障の対応等）は、引き続き BS が行っているが、BS が現在の業務で用いているアカウントでは、ProCX が本件システムに格納する顧客データにアクセスすることはできず、業務上の必要性がある場合には本文の通り ProCX からその都度システム管理者アカウントの付与を受けるという方法に変更した。なお、PDS サーバの保守業務（機器故障の対応等）にあたっては、本件不正持ち出しが発覚する以前から現在に至るまで、BS から委託を受けた外部ベンダによる故障原因調査を行う場合がある。当該外部ベンダは、保守網を介し、自身が保持するアカウントを用いて、PDS サーバにアクセスするところ、このアカウントは、ProCX が PDS サーバに格納する顧客データにアクセスすることが可能である。しかし、本件不正持ち出しが発覚する以前から現在に至るまで、BS には当該アカウントの ID 及びパスワードは通知されていないため、BS が当該アカウントを使用して PDS サーバのデータにアクセスすることはできない。さらに本件不正持ち出し発覚以後は、当該外部ベンダの委託先管理措置として、当該外部ベンダが PDS サーバにアクセスする際には、ProCX の承認を得る運用を開始し、当該外部ベンダが PDS サーバにアクセス可能な時間を、システム上、その都度 BS が承認した範囲に限定した他、別紙 7-4 項番 27～30 の措置を取った。また、BS が保守業務を行うに当たり当該外部ベンダが取得した顧客データを取扱うことがあるが、その場合は ProCX の承認を得て、BS と ProCX とが締結した「お客様情報の取扱いに関する覚書」（後記 2⑴参照）に定める安全管理措置等を講じた上で対応する運用に変更した。

を設定する権限も ProCX に移させた。)。こうした業務変更により、BS 側でシステム管理者アカウントを用いる業務上の必要性が原則として生じないようにした上で、同年 2 月 2 日、上記 2 名に付与していたシステム管理者アカウントを削除し、BS ではシステム管理者アカウントを保持しないこととした。なお、例外的に、BS においてシステム管理者アカウントを利用する必要が生じた場合、BS は ProCX の承諾を得て、ProCX からシステム管理者アカウントの付与を受ける方法に変更した。

（イ）私有 USB メモリ等の外部記録媒体への書き出しを防止する措置

前記第４・１⑵のとおり、X が本件不正持ち出しに用いた保守端末（X に貸与されていたもの）には、使用を許可された指紋認証機能 USB メモリ以外の外部記録媒体へのデータの書き出しを物理的又は技術的に防止する措置は講じられておらず、保守端末から私有 USB メモリ等に自由にデータを書き出すことが可能であった。

そこで、2023 年 7 月 18 日、保守端末に保存された情報の外部記録媒体への書き出しが不可となるよう設定する対処策（外部記録媒体への書き込みアクセス権をシステム上、拒否する設定）を講じた。

なお、保守運用業務上、外部ベンダによる故障原因調査等を行う場合に、PDS サーバに格納されたデータ（顧客データに限らない。）を閉域網の端末から、外部記録媒体（USB メモリ等）を用いて、外部送信用端末へ移さなければならない場合がある。このように、やむを得ず PDS サーバに係るデータを外部記録媒体に書き出す必要があるときには、保守端末ではなく、管理監督者[74]のみが利用可能な専用端末（データ書き出し専用の端末であり、保守端末とは異なる。）のみでこれを実施できるようにした上で[75]追加的な管理措置を導入した。すなわち、専用端末への USB 接続時に、複数の管理監督者へ接続アラームメールが発出される措置を講じると共に、専用端末を用いたデータの書き出しは、保守運用業務従事者（申請者）が管理職である管理監督者（作業者）へ書き出し等を申請し、管理監督者（作業者）による作業を別の管理監督者（監視者）が監視するという運用とした。また、上記の手続により外部記録媒体に書き出したデータを取り扱

[74] この管理監督者とは、X 所属グループの担当課長 6 名を指す。

[75] PDS サーバに格納されたデータを専用端末にダウンロードするには、まず PDS サーバから中継サーバにデータのダウンロード行い、その後、中継サーバから専用端末にデータを移転することになる。PDS サーバから中継サーバへのデータのダウンロードは、システム管理者アカウント又は PDS サーバの保守業務を行う外部ベンダによって行われるが、中継サーバから専用端末にデータを移転する権限及び専用端末の利用権限を管理監督者の個人アカウント（一意に利用者を特定できるもの）にのみ付与することにより、管理監督者のみが中継サーバから専用端末へのデータ移転をできるものとし、かつ、どの管理監督者が専用端末へのダウンロードを行ったかが特定できるようにした。

う際には、管理監督者である作業者と監視者が 2 名のクロスチェック体制の下で外部送信用端末にデータを格納する等の必要な作業を実施することとした。かかるクロスチェックにより、管理監督者による不正を抑止すると共に、必要な作業を終えた後は外部記録媒体内のデータを即時に削除することとした。さらに、こうした作業を行うに当たっては、作業着手前に、作業内容と申請者・作業者・監視者の氏名を作業記録簿に記載するとともに、作業完了後に、関係者がデータの削除結果等を含めて作業記録する運用とし、事後的な検証を可能にした。

（ウ）保守端末からのインターネット接続を制限する措置

前記第４・１⑶のとおり、X が本件不正持ち出しに用いた保守端末（X に貸与されていたもの）は、インターネット接続を技術的に制限する措置が講じられておらず、ウェブメールを用いて保守端末に保存した顧客データを自由に外部に送信することが可能であった。

そこで、BS は、2023 年 10 月 16 日、データセンタのインターネットアクセスを必要最小限にし、保守端末からはインターネットアクセスができないようする措置を実施した。

さらに、業務上の必要性からインターネットアクセスができるサーバについても、2023 年 12 月 20 日、インターネット接続先をホワイトリストにて制限することとし、ウェブメールを用いることができないようにした。

（エ）ログによる監視等の措置

前記第４・１⑷のとおり、PDS サーバへのログインログ及び顧客データのインポート／ダウンロードログを定期的に点検し、異常の有無をチェックする運用は行われておらず、これを実施する担当者も指定されていなかった。加えて、システム管理者アカウントは、X を含む本件システムの複数の運用保守従事者の間で共用されていたため、その使用者をログから一意に特定することができない状況にあり、ログ監視の前提的条件さえも欠く状況であった。

そこで、前記（イ）のとおり、保守運用業務上、やむを得ずシステムログや設定データ等を外部記録媒体に書き出す必要があるときには、管理監督者のみが利用可能な専用端末のみで実施できるものとする等の対処策を講じたことに加えて、2023 年 10 月 16 日から、当該専用端末に内部不正監視システムを導入し、当該専用端末に外部記録媒体が接続された時点で、外部記録媒体が接続されたこと、及び、誰が端末操作を行っているか、承認された適正な外部記録媒体であるか、といった情報を複数の管理監督者に即座に通知し、複数の管理監督者によ

って不正利用でないことをリアルタイムに監視する仕組みを導入した。

また、2023 年 10 月からは、BS が週次でログチェックを行い、同年 11 月からは、BS から ProCX に対して、月次でログチェックの結果を報告している。加えて、主管組織以外の第三者による抜き打ち検証も実施することとした。

さらに、BS では、ディレクトリ・サービス・システム[76]を導入し、全ての端末に個人単位のアカウントでのログインを必要とするシステム上の変更を実施した。また、個人単位のアカウントについて、多要素認証を導入することを検討している。

（オ）私有端末によるアクセスを制限する措置

前記第４・１⑸のとおり、本件システムでは、本件ネットワークへのアクセスルートとして保守網又は在宅オプションのいずれを用いる場合であっても、私有端末（PC 等）を用いることは技術的に制限されていなかった[77]。

そこで、BS は、私有端末から保守網を用いて本件ネットワークにアクセスすることができないようにするため、MAC アドレス認証等の導入を通じ、未登録の端末を社内ネットワークに接続できないようにした[78]。また、BS は、ProCX のコールセンタ向けの在宅オプションを通じた本件ネットワークへのアクセスを停止し、私有端末（PC 等）から在宅オプションを用いて本件システムの情報にアクセスすることができないようにした。

（カ）在宅オプション、SV 端末に関する措置

前記第３・３⑴のとおり、X は、ProCX のコールセンタのオペレータ用に設置された在宅オプションの利用に必要なアカウント ID 及びパスワードを知り得る立場にあり、これらを利用して在宅オプションを通じて本件ネットワークにアクセスすることも可能であった。そこで、BS は、前記（オ）のとおり、ProCX のコールセンタ向けの在宅オプションを通じた本件ネットワークへのアクセスを停止した。なお、在宅オプションの廃止に伴い、ProCX は、画面の閲覧のみ可能でデータのダウンロードはできない方式のリモートアクセス環境を整備し

[76] アカウントやネットワーク資源（サーバ、共有フォルダ等）を一元管理できるもので、特定のシステムに対し、どのアカウントからのアクセスを認めるか等のアクセス権の制御も可能である。
[77] お客様情報保護運用マニュアルにおいて「お客様情報を取扱うシステム端末席上に私物（個人の携帯電話、個人の手帳など）を置いていない。」等の日常管理の確認事項が定められているに留まっていた。
[78] なお、保守網には、社内ネットワークの他、VPN を用いてアクセスすることも可能であるところ、私有端末から同 VPN を用いて保守網へアクセスすることも技術的には可能であるが、上記（ア）の対応を講じたため、PDS サーバから私有端末にデータをダウンロードすることはできない。

た。

また、前記第３・３⑵イのとおり、SV アカウントでダウンロードされ、SV 端末に保存された顧客データについて、X が、共有設定によりアクセスし、これを取得した可能性もあることから、BS の運用保守業務従事者が作業を行う中継サーバから ProCX の SV 端末にアクセスできないようにするために、同中継サーバのファイアウォール機能を用いたルーティング不可設定を実施することで、SV 端末へのアクセスを技術的に停止した。

イ　技術的な管理措置に関する追加的な対処策

BS では、本件システムに関し、点検 44 項目のうち積み残しとなった不備事項の 2 項目について、①個人単位のアカウントについて、2024 年 3 月末日までに、多要素認証を導入することを予定しており（項番 21）、また、②顧客情報保有サーバについて、同情報の参照権限を持たない者が参照できないよう、暗号化することを検討している（項番 44）。これらの対処策についても、情報漏洩を防止する上で有用な措置であることから、BS 及び NTT 西日本において、引き続き検討を進めるべきである。

また、前記ア（オ）については、MAC アドレスを詐称することにより、未登録の端末から社内ネットワークに接続することも技術的には可能であることを踏まえ、上記に加え、端末の認証によりアクセス制御を行う仕組み（802.1X 認証等）を導入する等、より厳密な制限を設定することも検討すべきである。

これらの追加的な対処策の検討を行う際は、後記３に述べる NTT 西日本グループ全体の対処策によって是正を図ることも考えられるところ、対処策に重複や齟齬が生じることのないよう、BS 及び NTT 西日本は引き続き連携して対処に取り組むことが必要である。

⑵　情報セキュリティ体制のガバナンス面の改善

前記第５（根本的な原因・背景の分析）及び前記第６（本件過去調査）において指摘したとおり、本件不正持ち出しの再発防止のためには、単に技術的な管理措置について対処策を実施するだけではなく、情報セキュリティ体制のガバナンス面についても改善策を講じる必要がある。

ア　経営陣のコミットメント

前記５・１⑼のとおり、BS の経営陣が、これほどまでに自社の情報セキュリテ

ィ体制に綻びが生じていたことに対して従前何ら有効な改善措置を講じていなかったことは、現場組織から吸い上げられる報告が必ずしも正確ではなかったことを考慮してもなお致命的な怠慢であると言うほかない。

BS の経営陣には、本件不正持ち出しを許した当事会社として、本件不正持ち出しの発生を極めて深刻に受け止め、情報漏洩リスクが経営上の重大なリスクになることを改めて認識した上で、情報セキュリティ体制の抜本的な立て直しに向けた陣頭指揮を執らなければならない。当然のことながら、BS の各部門に安易に対応を委ねることはあってはならず、NTT 西日本とも連携しつつ、情報セキュリティ体制の改善に向けて主導的な役割を果たすことが求められる。

さらに、情報漏洩を防止するための情報セキュリティへの取組を浸透させるためには、経営陣が率先して内外に情報セキュリティにコミットする姿勢やメッセージを示していくことが重要である。

イ　リスクマネジメントプロセスの確立

今回の事例では、X による本件不正持ち出しという形で情報漏洩リスクが顕在化したが、BS を取り巻く情報漏洩リスクはこれだけにとどまらない。また、本件不正持ち出しと同種の不正行為の発生を防止するための具体的な対処策は当然に講じられるべきであるが、そのことに安心して情報セキュリティ対策の他の面が疎かになることも許されない。

この点、前記第５・１⑹で指摘したように、BS では、X 所属グループを含む VD 部全体にも、第 2 線であるマーケティング戦略部事業推進部門にも、情報セキュリティ上のリスクを特定、評価し、その在り様に応じてリスク低減措置を策定し、実行していくというリスクマネジメントプロセス自体が存在していなかった。

顕在化したリスクのみに注目し、その対策のみ固執するのは本来のリスクマネジメントではない。将来にわたり有効な情報セキュリティ体制を確立するためには、経営陣、事業部、現場組織といった各レベルで、真の意味で有効なリスクマネジメントのプロセスを確立しなければならない。

このようなリスクマネジメントプロセスを確立するためには、実務的にこれを主導する第 2 線の役割が重要になることは言うまでもない。

なお、情報セキュリティ TF では、本調査の一環として、NTT 西日本グループの一部のシステムを対象に情報漏洩経路の視える化を行った。こうした取組は、リスクマネジメントの出発点となるリスクの特定の試みの一つであるが、今後は、タスクフォースによる一時的な措置としてではなく、リスクマネジメントに必須の手順として、然るべき部署において恒常的に実施される必要がある。

ウ　第 2 線の強化

第 2 線の管理部門には、前記イで指摘したリスクマネジメントのほか、第 1 線である現業部門が情報セキュリティについて遵守すべき事項を遵守しているかをモニタリングし、これを監督、支援する役割がある。

BS においてこの第 2 線の機能が極めて脆弱であったことは前記第５・１⑷で指摘したとおりである。したがって、第 2 線の機能を拡充させることは急務である。

この点、BS には BS 内の第 2 線としてマーケティング戦略部事業推進部門が存在する一方、NTT 西日本グループ全体の第 2 線として NTT 西日本・情報セキュリティ推進部が存在する。このほか、NTT 西日本グループ内では、サイバーセキュリティに関する事項については NTT 西日本・技術革新部サイバーセキュリティ戦略室や CSOC といった別の組織も重要な役割を果たしている。こうした多層的な第 2 線の組織構成において、BS の情報セキュリティ体制の改善に向け、どの組織にどのような役割を与えるかは、NTT 西日本グループ全体での経営上の判断であるが、そのような役割分担においてどの部署も BS を実質的にカバーしていないといった事態が生じることのないように留意しなければならない。

そして、このような役割分担を明確にした上で、第 2 線の機能を果たすべき部署に情報セキュリティに知見を有する人材を拡充するなどの対処策が求められる。

エ　第 1 線におけるルール遵守のための改善措置

X 所属グループについては、情報セキュリティに関する規律が遵守されていない状況のほか、システムの運用面での情報セキュリティに責任を持つ部署が実質的に存在していなかったこと、業務上の便宜が優先される状況の存在、事業立ち上げ時に情報セキュリティの手当てが十分に考慮されていなかったこと等、多数の問題点が存在している。また、VD 部全体の問題として、情報管理責任者を頂点とする、情報セキュリティ体制を管理するレポーティングラインも機能不全に陥っていた。

このうち、情報セキュリティに関する規律が遵守されていない状況そのものに対しては、前記⑴のとおり具体的な対処策が実施又は検討されている。

しかしながら、こうした対処策には引き続き現場組織の運用に委ねられる面があるため、第 1 線である X 所属グループにおいては、対処策が一時的なものとなり、形骸化することが無いよう注意が必要である。

X 所属グループには上記のような多数の問題があったことからすれば、情報セキュリティに関する規律を確実に履践していくことは必ずしも容易ではないが、確実な履践のためには、ルールを実務に実装していくこと、すなわち、実行責任者

を具体的に指定し、当該責任者が行うべき作業の手順・方法を確立することが重要である。

また、これと人事上の評価を結びつけることも有効であり、具体的には、実行責任者がその役割を果たした場合にはこれを人事上プラスに評価する一方、実行責任者がその役割を果さない場合には人事上マイナスに評価するといった処遇を行うことが考えられる。もっとも、このような人事評価を行う場合には、実行責任者がその職責を果たせていないことを取り繕う動機付けを与えないようにしなければならず、例えば、実行不可能である過大な役割を与えないこと、これまで見過ごされていた不備の発見についてはこれを奨励すること等に配慮が必要である。

また、第１線にも、取り扱うシステムの重要度に応じて、情報セキュリティに知見を有する人材を配置するなどの施策も考えられる。さらに、情報セキュリティに関する規律を遵守するためにツールの導入等が必要であれば、これに予算措置を講じる等の手当てを講じることも重要である。これらは、当然のことながら、現場のみで解決できる問題ではないため、経営レベルで取り組む必要がある。

オ　情報セキュリティ体制の実態把握のための仕組みの見直し

前記第５・１⑶のとおり、BS では、X 所属グループ等の現場組織における情報セキュリティ体制の運用実態を把握するための仕組みが機能不全に陥っていた。

現場組織における運用実態を把握することは、情報セキュリティ体制の不備を早期に発見するためにも、また、現場組織に情報セキュリティ上のルールを遵守させる動機付けを与えるためにも、必要不可欠であるから、このような機能不全は早急に解消しなければならない。

その方法としては、①情報セキュリティ自主点検等の既存の自主点検の仕組みを改善するほか、②新たな実態把握のための仕組みを導入することが考えらえる。

①については、例えば、これまでは担当課長クラスが点検した結果が十分に検証されることなく情報管理責任者にまで上がっていたという実態があったが、今後は、その途中過程で、現場に近い担当部長クラスが点検結果を検証するようにしたり、点検結果の妥当性を裏付ける証跡の提出を必須にしたりすることで、点検結果の正確性を担保していくことが考えられる。また、自主点検については点検項目の趣旨が分かりにくい等といった指摘もあることから、正確な点検ができるような実務的な工夫も必要である。

②については、第１線による自主点検とは別に、第２線が第１線の現場組織の実態を直接チェックする仕組みを導入することも考えられる。例えば、第２線において第１線の現場組織を実査して、ルールを遵守するための体制・手順が確立されているか、それらの体制・手順が実際に履践されていることを裏付ける証跡が

あるかといったことを直接チェックすること等が考えらえる。

カ　内部不正による情報漏洩リスクに対する危機意識の浸透及び教育

第５・１⑸で指摘したとおり、BS においては内部不正による情報漏洩リスクに対する意識の弱さが顕著に認められた。その背景には、性善説的な発想があるものと考えられるが、そのような発想に根拠はない。

内部不正による情報漏洩リスクに対する危機意識の弱さは、内部不正を企図する者に付け入る余地を与えるものであり、また、情報セキュリティ上のルールを履践する動機付けを弱くするものでもある。

したがって、研修や情報発信を通じて、全従業員に対して、改めて内部不正による情報漏洩リスクに対する危機意識の浸透を図るとともに、情報セキュリティ上のルールの遵守を強く求めていく必要がある。

キ　エスカレーションの徹底に向けた改善

前記第６・７⑶ウのとおり、本件過去調査では、X 所属グループが属する VD 部の情報管理責任者である VD 部部長にも、BS において情報セキュリティを所管するマーケティング戦略部事業推進部門にも、エスカレーション（状況報告等）は実施されていなかった。エスカレーションが適切に実施されていたならば、本件過去調査は適切に実施されていたはずである。

今後は、エスカレーションの必要性の浸透、手順の明確化、研修等を通じてエスカレーションの徹底を図っていく必要がある。

ク　内部監査部門の拡充及び地位の向上

前記第５・１⑷のとおり、BS の情報セキュリティ体制については、第 1 線の現業部門のみならず、これを監督、支援すべき第 2 線にも脆弱性が認められた。このように、第 1 線及び第 2 線のいずれも有効に機能しない場合に、そのような機能不全を発見し、その是正を促す役割を担う第 3 線の内部監査部門の重要性は改めて指摘するまでもない。

BS の内部監査部門（NTT 西日本・内部監査部門を含む）には、前記第５・１⑻のとおり課題が認められたことから、今後は、第 2 線による第 1 線に対する監督機能が有効に機能しているかという観点での深堀り監査を行うとともに、リスクベース判断の前提として第 1 線又は第 2 線から提供を受けた情報自体の正確性を独自に検証するなどして、内部監査部門の質の拡充を図っていく必要がある。

また、内部監査部門がいわゆる 3 線防衛において最後の砦の役割を果たすことに鑑みれば、将来自社の経営を担うべき人材を内部監査部門に配置するなど、内部監査部門の地位向上にも努める必要がある。

内部監査部門は、会社の多くの問題点を把握でき、経営・業務改善、新規ビジネスの端緒を得る部門としても重視すべきである。

⑶　経営上の課題（人事施策等）

ア　特定の者への依存とその固定化等への対処

前記第４・２⑵及び第５・１⑺イのとおり、ProCX 向け PDS サーバの運用保守及びサポート業務は X 個人に依存する状況が長年固定化しており、このことが内部不正による情報漏洩リスクを高める大きな要因となっていた。

このような状況には自己強化型のフィードバックループが作用するため、自然に解消することは困難である。そのため、重要情報に触れる者を一定の期間を超えて同一の業務に従事させることを禁じるルールを導入することも考えられる。こうしたルールを導入する場合には、必ずと言っていいほど、「その者しか業務が分からないので、異動させると業務が滞る」といった現場からの不満が生じるが、そのような事態を生じさせていること自体がマネジメントの失敗である。したがって、普段から、後任者を育てるなど、特定の者への依存を回避するための施策を長期的な視野を持って進める必要がある。

そして、こうした施策は現場レベルでは解決できない人員配置の問題でもあるため、現場で解決すべき問題であるとして現場任せにせず、経営レベルで取り組む必要がある。

他方、現場レベルでは、特定の者への依存とその固定化による業務のブラックボックス化を避けるため、上長等による監督を徹底する必要がある（前記第５・１⑺エ参照）。

なお、前記第４・２のとおり、X については、フロント SE チームにもバック SE チームにも事実上属さず、実質的な監督者を欠く状況となっていた。これは X の属人的な特殊性によるものであるから、X が BS の業務を離れたことによりこの問題自体は解消している。しかし、このような状況はスキルを有するが故に長年同一の業務に従事する者について生じやすい傾向があるから、実質的な監督者不在の状況がほかにもあるのであれば、そのような者に対する監督の強化を徹底する必要がある。

イ　派遣社員等の待遇、動機付け（モチベーション）への配慮

前記第５・１⑺ウのとおり、X が本件不正持ち出しに及んだ動機及び正当化根拠には自らの待遇への不満があった可能性がある。不正に至る動機及び正当化根拠を生じにくくすることは、内部不正による情報漏洩リスクを減じるために必要な視点である。

正社員以外の派遣社員等については、会社への忠誠心（ロイヤリティ）において正社員とは自ずと異なること、正社員とは質的に異なる不満を持ち得ること等に十分留意し、正社員以外の派遣社員等の待遇の見直し、その貢献を評価する顕彰制度なども検討すべきである。

正社員であるかどうかを問わず、同じ職場で働く者ができるだけ生き生きと仕事ができる環境の整備に留意すべきである。

２　ProCX について

ProCX における本件不正持ち出しの再発防止策としては、直接的には委託先の管理体制の改善が重要である。もっとも、本調査におけるヒアリングや本緊急点検の結果、技術的な管理措置の面及び情報セキュリティ体制のガバナンス面の双方において、改善すべき問題が確認されたことから、当調査委員会としては、これらを踏まえた改善策を講じていく必要があると考える。

⑴　委託先管理体制の見直し

前記第５・２⑴のとおり、ProCX では、個人データの取扱いを委託するに際しての情報セキュリティ上の規律を定めていたのにもかかわらず、それがほとんど遵守されていなかった。

その原因の中心を占めるのは、ProCX の担当者において、BS に対し個人データの取扱いを委託しているとの認識がなかったことであるが、これを個人のミスであると矮小化して捉えることは許されない。

前記第５・２⑴イで指摘したとおり、ProCX については、委託先をどのように監督するかの実務フローが確立していなかったこと、個人データの取扱いの委託に当たるか否かについての ProCX の担当者の判断の当否をチェックしたり、審査したりする運用が存在しなかったことが委託管理上の問題点として指摘できるのであり、これらは要するに、個人データの取扱いを委託するに当たっての規律が実務的に何ら実装されていなかったことを意味している。

したがって、委託先管理に当たっての実務プロセスを確立することは急務である。この点、ProCX は、2023 年 10 月 19 日、BS との間で「お客様情報の取扱いに関する覚書」を締結した。同覚書では、BS における個人情報の安全管理措置の状況を確認するための ProCX の立入り検査権限や報告要求権限等が定められている。ProCX は、同日、同覚書に基づき、BS に対し、適切な安全管理措置を遂行するためのシステム面・運用面の対処策（本件システムの運用保守従事者における個人データの取扱状況を確認する手段の整備、本件システムの運用保守従事者における個人データの取扱監査の実施、本件システムの運用保守に当たってのアクセス制御等技術的安全措置）を提示するよう求めており、現在、これに基づき両社間で必要な連携が行われている。

今後は、ProCX 内の規律及び上記覚書に基づき、BS に対する委託先管理措置を実務面において実装し、これを確実に実践することが求められる。

⑵　緊急点検により確認された技術的な管理措置に係る不備の是正

前記第７・３のとおり、緊急点検の結果、ProCX の情報セキュリティ体制にも多数の不備が確認された。前記第７・３⑵のとおり、2024 年１月末日時点で、点検 44 項目の不備事項は 0 となったが、運用により対処しているものが 14 項目残っていることから、これらの項目について、システム的な対処による是正が求められる。その際、後記３に述べる NTT 西日本グループ全体の対処策によって是正を図ることも考えられるところ、対処策に重複や齟齬が生じることのないよう、ProCX 及び NTT 西日本は引き続き連携して対処に取り組むことが必要である。

⑶　顧客情報の漏洩に対する危機意識の浸透及び教育

前記第５・２⑵で指摘したとおり、ProCX においては顧客情報の漏洩に対する危機意識の乏しさが認められた。

本件不正持ち出しを契機に、研修や情報発信を通じて、全従業員に対して、改めて顧客情報の漏洩に対する危機意識の浸透を図るとともに、委託先管理を含め情報セキュリティ上の規律の遵守を強く求めていく必要がある。

⑷　情報セキュリティ体制のガバナンス面の強化

前記第５・２⑶のとおり、ProCX の情報セキュリティ体制のガバナンス面については、BS と同様の問題として、①実態把握のための仕組みの機能不全、②第２線の脆弱性（担当者１名）、③内部不正による情報漏洩リスクに対する意識の希薄さ、④

情報セキュリティ上のリスクに対するリスクマネジメントプロセスの不存在、⑤情報セキュリティに知見を有する人材の不足等の問題点が確認されている。

これに対する対処策の方向性は、前記１⑶で指摘した BS における対処策の方向性と基本的には同様である。ProCX においても、BS と同様に、情報セキュリティ体制のガバナンス面を強化していくことが求められる。

⑸　エスカレーションの徹底に向けた改善

前記第６・４⑵のとおり、本件過去調査では、ProCX において情報セキュリティを所管する事業推進部・総括担当にも、NTT 西日本・情報セキュリティ推進部にも、エスカレーション（状況報告等）は実施されていなかった。前記１⑵キでも指摘したとおり、エスカレーションが適切に実施されていたならば、本件過去調査は適切に実施されていたはずである。

今後は、エスカレーションの必要性の浸透、手順の明確化、研修等を通じてエスカレーションの徹底を図っていく必要がある。

⑹　ProCX と BS の関係性の明確化

前記第５・２⑷のとおり、ProCX と BS は従来非常に近い関係の会社であり、現場レベルの感覚としては、委託元・委託先という明確な立場の相違がなかったものと考えられる。

このような曖昧な関係性は、委託先である BS に対する管理を疎かにさせる可能性があるため、今後は両社の役職を兼任させないなど、管理する側の委託元と管理される側の委託先という関係性が曖昧にならないような措置を講じる必要がある。

３　NTT 西日本

前記第４から前記第８で指摘したとおり、NTT 西日本グループ全体の情報セキュリティ体制にも数々の問題があることが確認された。そこで、当調査委員会は、NTT 西日本においても、NTT 西日本グループ全体の情報セキュリティ体制の改善が必要と考える。

⑴　グループ全体での情報セキュリティ体制上の技術的な管理措置に係る不備の是正

前記第７のとおり、本件不正持ち出しの発覚を契機に NTT 西日本グループの全システムのうち、お客様情報を保有する全システム、及び、機密性の観点の重要度が「高」

と分類されているシステムの合計 443 のシステムを対象に本緊急点検を実施したところ、BS と同種又は類似の情報セキュリティ上の不備が確認された。

全 443 システムについて、2024 年 2 月 16 日までに、暫定対処を完了し、これらの対処によって情報漏洩防止の効果が期待できるものの、運用面での是正対応に留まっている項目も存在し、点検 44 項目の全ての不備を是正したわけではない。今後も、NTT 西日本グループが一丸となって、早急に認識された不備を是正していく必要がある。併せて、改めて情報セキュリティに関するルールの周知・徹底を図る必要がある。

⑵　今後グループとして取り組むべきシステム上の対処策

情報セキュリティ TF は、本件不正持ち出しについての原因分析及び本緊急点検の結果等を踏まえ、以下のとおり、NTT 西日本グループ全体で取り組むべき今後のシステム上の対処策を取りまとめた。

ア　個々の課題に関する対処策

（ア）外部記録媒体（USB メモリ等）の使用に関する制限

本件不正持ち出しを許した直接的な原因として、BS において、利用を許可された指紋認証機能 USB メモリ以外の外部記録媒体へのデータの書き出しを物理的又は技術的に防止する措置が講じられていなかったことが挙げられる。

そこで、NTT 西日本グループとしても、BS が実施した対処策と同様（前記 1⑴参照）、利用することができる外部記録媒体を特定のものに限定し、利用に際する申請及び承認手続に加え、利用を許可されていない外部記録媒体を挿入した時には管理者へアラートが送信される等の仕組みを構築する必要がある。また、ディレクトリ・サービス・システムが導入されているシステムについては、ポリシー設定により外部記録媒体の接続を制御すべきである。

また、外部記録媒体の使用に関する制限の未実施についての根本的な対処策として、外部記録媒体を使用してデータを書き出す必要のない業務設計やシステムを構築することも検討すべきである。

（イ）私有端末（私有 PC 等）の使用に関する制限

情報の持ち出しを防止するためには、私有 PC 等の私有端末を利用した持ち出しの可能性を考慮した対策をとることも必要である。

そこで、社内 OA 等、既に対策が講じられているネットワーク以外の個別ネットワークにおいても、私有端末の社内への持込みを原則として禁止することに加え、未登録の端末を社内ネットワークに接続させないようにすることや、当該端末のログの定期的な確認等の運用管理を行うことも必要である。また、MAC アドレスを詐称することにより、MAC アドレスが未登録の状態で社内ネットワークに接続することも技術的には可能であることを踏まえ、上記に加え、端末の認証によりアクセス制御を行う仕組み（802.1X 認証等）を導入する等、より厳密な制限を導入することも検討すべきである。

（ウ）インターネットの使用に関する制限

情報の持ち出しを防止するためには、インターネット経由での持ち出しについても対策が必要である。そこで、インターネットを経由した接続先に関するホワイトリストを設定し、ウェブメールへのアクセスや社外クラウドサービスを利用できないようにすることにより、これらを用いた情報の持出しを防止するほか、クラウドサービスを利用したシステム構築が増加していることを踏まえ、利用者が用いる端末そのものにセキュリティ対策を講じることも検討すべきである（後記イ参照）。

（エ）アカウントの管理方法の改善

NTT 西日本グループでは、本緊急点検の対象としたお客様情報等を保有するシステムにおいて、システム管理者のアカウントが複数の使用者の間で共用されていることがあり、その使用者をログから一意に特定することができない状況にあった。内部不正が起こらないよう監視し、また、内部不正のおそれが生じた際に適切な調査を実施できるようにするためには、使用者をログから特定することができるような措置をとることが必要である。

個人特定可能なアカウントに変更するにあたっては、アカウントの認証及びアカウントに紐づく権限を適切に管理・認可するために、ディレクトリ・サービス・システム等の導入によるシステム的な対処が必要である。その際、アカウント管理の仕組みを個々のシステムごとに構築することには多大なコストが必要になる上、個々のシステムごとに仕組みを構築した場合、各システム間の連携、利用者の追加又は削除等の情報の管理、セキュリティレベルの維持等が困難となることから、NTT 西日本グループにおいて、全社的に統合したアカウント管理の仕組みを導入することを検討すべきである（後記イ参照）。

なお、ネットワーク機器の保守アカウントやサーバ内で実行されるプロセス

のアカウントについては、特定のアカウントを利用しなければならないものがあり、当該アカウントについては共有が避けられない。そのような場合には、業務上必要な範囲で、特定の管理者のみが当該アカウントの利用時に必要なパスワードを知り得るよう厳密な管理を実施すること、当該アカウントの利用時には必ず複数者での作業をするようにすること、当該アカウント利用管理簿への記録によってアカウント利用者を特定できるようにすること等の運用を実施することが必要である。また、特定のアカウントを共有することが必要なシステムについては、利用者を特定できるよう、利用者を特定可能なアカウントでログインできる中間サーバ等を配置することにより、そのアクセスログを記録できるようなシステムを構築することも考えられる。

（オ）情報管理・機器管理の明確化

情報の管理を適切に実施する前提として、顧客情報等の重要情報を明確に特定し、また、当該ファイルの保存先も明確に管理されているのかを明確に把握する必要がある。そこで、重要情報を含むファイルには、各種規程に従った機密度ラベルを貼付するとともに、その保存場所である IT 機器の管理方法についても見直しを行うべきである。また、不適切な持出しがなされた場合に備え、重要情報は暗号化するとともに、暗号を解除する際には管理者の承認を必要とする等の運用を整備することも必要とする等、情報管理・機器管理に関するワークフローを整備すべきである。

イ　社内ネットワーク設計に関する考え方の抜本的な見直し

前記アの個別の課題に関する対処策の検討と並行して、社内ネットワーク設計に関する考え方の抜本的な見直しも検討すべきである。

現在の「情報セキュリティ規則 ICT 編」別紙セキュリティ対策ルールに規定されているルールに従って、サイバー攻撃による侵害リスク及び侵害後の被害拡大リスクを低減するために外部接続を必要最小限にするには、業務ごとに他のネットワークから独立した個別システムを構築することが必要になり得る。しかし、当該ルールの存在により、十分な開発費用がないために必要なセキュリティが備わっていない個別システムが構築されているという側面があることが判明した。加えて、NTT 西日本グループ内に、特定の業務に利用する独立した個別システムが多く存在することで、NTT 西日本として、各システムの構成やリスクの所在を正確に把握した上で NTT 西日本グループ各社に適切なセキュリティ対策を助言・指示することが困難となり、また、情報セキュリティ自主点検の形骸化（後記⑶オ（ア）

参照。）を招く一因になったとも考えられる。さらに、昨今の SaaS（Software as a Service）[79]の充実に伴い、NTT 西日本グループにおいて今後新たに業務システムを構築する際には、全てを自社開発するのではなく、SaaS を有効活用する例が増加することが想定されるところ、その意味からも、他のネットワークから独立した個別システムを構築するという、いわゆる境界防御型のセキュリティ対策を維持することは必ずしも適切ではない。

これらの状況に対処するためには、独立した個別システムの構築が求められ得る上記ルールを見直す必要がある。その際には、現在の NTT 西グループにおけるシステム環境を踏まえ、実効的かつ実現可能性のあるルールを設けることが求められる。

この点、既に NTT 西日本内で運用している社内 OA 網は、SaaS の利用も念頭に置いて、アカウント管理、外部記録媒体の利用制限、ログ管理といった基本的なセキュリティ対策を具備していることから[80]、情報セキュリティ TF は、NTT 西日本以外の NTT 西日本グループ各社の業務ネットワーク（既存のものを含む。）についても、当該 OA 網に移行させ、当該 OA 網の機能を用いて、NTT 西日本グループ全体のセキュリティ対策を行うことが適切であると考えている。そのため、当調査委員会終了後の情報セキュリティ TF の後継組織において、引き続き、かかる対処策の具体化及び上記ルールの改訂に関する検討を行う予定である。

⑶ ガバナンス面の改善

ア グループ全体の情報セキュリティ体制の改善に向けた経営陣のコミットメント

これまで見てきたとおり、BS で確認された情報セキュリティ上の問題の多くは、NTT 西日本グループ全体にわたって存在している。

NTT 西日本の経営陣は、このような事態を危機意識を持って受け止め、NTT 西日本グループ全体の情報セキュリティ体制の改善に向け主導的な役割を果たさなければならない。

その一環として、NTT 西日本グループでは、従来は情報セキュリティ担当役員を最高位の参加メンバーとして開催されていた NTT 西日本グループの情報セキュリティ推進委員会の運営方法を改め、2024 年 2 月からは、NTT 西日本の社長及び

---

[79] クラウドサービスの一種で、利用者に、特定の業務系のアプリケーション、コミュニケーション等の機能、運用管理系の機能、開発系の機能、セキュリティ系の機能等がサービスとして提供されるもの。

[80] NTT 西日本の社内 OA 網においては、ディレクトリ・サービス・システムを用いたアカウント管理による個人毎の認証やデバイス制御が実現されている。また、自動でのファイル暗号化機能が実装されており、社外にファイルを持ち出す際には上長承認が伴う暗号解除処理を行う必要があり、その際にはログが保存される仕組みとなっている。

副社長を当該委員会のメンバーに加えた。NTT 西日本の経営陣には、このような委員会を通じて情報セキュリティ体制の現状を的確に把握し、それらを元に情報セキュリティ体制の改善を主導し、そのため意思決定を迅速に行うことが求められる。

また、今後、NTT 西日本グループ全体として前記⑵のようなシステム上の対処策に取り組んでいくためには相応の予算措置が必要であると考えられるが、情報セキュリティ対策のための予算措置についても、経営陣が主導して必要な意思決定を行わなければならない。

イ　内部不正による情報漏洩リスクに対する危機意識の周知・浸透

前記第８・３⑴アのとおり、本アンケート調査からは、NTT 西日本グループ全体でも、BS 及び ProCX と同様に、内部不正による情報漏洩リスクに対する脅威認識に甘い面があったことが示唆される。

したがって、NTT 西日本グループ全体でも研修や情報発信を通じて、改めて内部不正による情報漏洩リスクに対する危機意識の浸透を図っていく必要がある。

ウ　リスクマネジメントプロセスの確立

前記第８・３⑴イのとおり、本アンケート調査からは、NTT 西日本グループ全体でも、BS 及び ProCX と同様に、リスクマネジメントプロセスの確立の点に課題があることが示唆される。

また、前記第５・３⑴のとおり、NTT 西日本グループ全体の情報セキュリティ体制を統括する NTT 西日本グループ・情報セキュリティ推進部においても、内部不正による情報漏洩リスクについては必ずしも具体的なリスク評価ができていたわけではなかった。

前記１⑵イでも指摘したように、将来にわたり有効な情報セキュリティ体制を確立するためには、グループ各社の経営陣、事業部、現場組織といった各レベルで、リスクマネジメントのプロセスを確立していく必要がある。

エ　第２線の強化

前記第７のとおり、NTT 西日本グループ内の 443 のシステムを対象に実施された緊急点検において、BS と同種又は類似の情報セキュリティ上の不備が確認されたことを踏まえると、NTT 西日本グループ全体として第２線の機能が脆弱であったと言うほかない。

NTT 西日本・情報セキュリティ推進部としても、グループ各社の第 2 線には必ずしも十分な人員の割当てがなく、脆弱な面があるとの認識を有している。

したがって、NTT 西日本グループ全体として情報セキュリティに関する第 2 線の機能の底上げを図る必要がある。この点、前記１⑶ウでも指摘したように、NTT 西日本グループでは、グループ各社にそれぞれ第 2 線として情報セキュリティ担当が配置されている一方、西日本グループ全体の第 2 線として NTT 西日本・情報セキュリティ推進部が存在し、このほかにも NTT 西日本・技術革新部サイバーセキュリティ戦略室や CSOC といった別の組織も重要な役割を果たしている。こうした多層的な第 2 線の組織構成において、NTT 西日本グループ全体の情報セキュリティ体制の向上のために、人員や予算をどのように配分するかは、NTT 西日本グループ全体として特に重要な経営上の判断である。

オ　情報セキュリティ体制の実態把握のための仕組みの見直し

（ア）情報セキュリティ自主点検等の定期点検の見直し

前記第５・１⑶のとおり、BS では、情報セキュリティ自主点検が機能不全に陥っていた。

また、本緊急点検においては、NTT 西日本グループ各社においても、従前の情報セキュリティ自主点検の結果が必ずしも正確でないことが判明したケースが多数確認された。

さらに、前記第８・３⑶のとおり、本アンケート調査においても、相当数の回答者が自主点検は不適切又は不十分な方法で実施されているとの認識を示しており、その形骸化を指摘する回答も多数に上った。

したがって、情報セキュリティ自主点検等の定期点検の実施方法は見直していかなければならない。当調査委員会のヒアリングや本緊急点検等で確認された実施方法上の課題としては例えば以下の点がある（回答者側の問題点には、８・３⑶のアンケート結果を参照されたい）。

①　点検項目の量及び曖昧さ

NTT 西日本グループにおいては、本件不正持ち出しとは関係ないものも含め、多数の情報セキュリティルールが策定されている。

しかし、本緊急点検においては、これらのセキュリティルールに基づいて実施される定期点検の点検項目が多数に上ることが、点検者への負担を増大させ、定期点検の形骸化を招いている状況に加え、点検項目の中には解釈の余地

があるものも多く含まれていることにより、点検者の解釈によって不適切な点検結果が記載されている状況も見受けられた。

この点は、BS の点検担当者へのヒアリングでも同様の指摘があった（前記第５・１⑶ア（ウ）参照）。

そこで、実効的な点検を継続して実施するために、点検項目を可能な範囲で重要なものに限定するとともに、点検内容をより明確に規定することが必要である。

② 回答結果の検証

前記第５・１⑶ウで指摘したとおり、BS の情報セキュリティ自主点検においては、第１線の現場組織である X 所属グループが取りまとめた不正確な点検結果が特に検証されることなく、情報管理者である VD 部部長に報告され、さらに、第 2 線であるマーケティング戦略部・事業推進部門もその結果をそのまま受け取るという、鵜呑みの連鎖が生じていた。

そして、前記第５・３⑵で指摘したとおり、グループ各社からの点検結果の報告を受ける NTT 西日本・情報セキュリティ推進部においても、形式的な確認をするにとどまり、不備なしとされた事項についてその回答の正確性を独自に検証したり、その根拠を自ら確認したりする運用はしていなかった。

したがって、定期点検を実効的に実施するだけでなく、点検結果についても実効的にモニタリングする体制を構築することが必要といえる。また、かかる体制を構築するに当たっては、NTT 西日本の情報セキュリティ推進部その他の関連組織とグループ各社の情報セキュリティ担当のそれぞれが果たすべき役割を明確にすることも必要である。

（イ）その他の実態把握の手段の確保

前記１⑶オのとおり、BS については、情報セキュリティ体制の実態把握のための仕組みの見直し方法として、新たな実態把握のための仕組みを導入することを提言した。これと同様に、NTT 西日本グループ全体でも、第１線による自主点検とは別に、第 2 線が第 1 線の現場組織の実態を直接チェックする仕組みを導入することが考えられる。

カ システムライフサイクルにおけるガバナンス

前記第５・１⑵ア（エ）のとおり、本件システムについては、開発段階で内部不

正を想定した情報セキュリティ対策が後回しにされたという経緯が存在したが、企画・開発段階から、可能な限り運用ではなくシステムの機能として情報漏洩対策を図ることができるのならば、その方が望ましいと言える。そのためには、企画・開発段階から、システムが具備すべき情報セキュリティ機能を定め、これが開発されるシステムにおいて充足されているかを確認することが必要である。

この点、NTT 西日本グループにおいてはインターネットへの公開を前提としたシステムにおいては、サイバー攻撃への対策として、開発の意思決定時点でセキュリティ審査を受けることが IT ガバナンスの仕組みとして組み込まれているが、インターネットへの公開を前提としない閉域網に構築するシステムについては、必ずしもその仕組みがない。

そこで、今後は、閉域網に構築するシステムについても、開発の企画段階から情報セキュリティ対策としてのセキュリティ審査を必須とする仕組みを導入すべきと考えられる。

キ　エスカレーションの徹底に向けた改善

前記１⑵キ及び前記２⑸では、本件過去調査を踏まえ、BS 及び ProCX におけるエスカレーションの徹底の必要性を指摘したが、NTT 西日本としても、NTT 西日本グループ全体として、エスカレーションの必要性の浸透、手順の明確化、研修等を通じてエスカレーションの徹底を図っていく必要がある。具体的には、情報漏洩事案の発生が確定的に確認されない「情報漏洩のおそれ」の段階での初動対応が特に重要になるため、既存のエスカレーション関連規程において初動体制の確立手順を明記すること等が考えらえる。

また、初動時にはデータやログの迅速な保全、解析が必要となるため、NTT 西日本がグループ各社にこれらの技術支援を行うことができるよう、対応組織、連絡体制を整備することも重要である。

なお、エスカレーションが適切に行われるには、これを受ける立場の者がエスカレーション報告を真摯に受け止めなければならない。一般論として、実務においてはエスカレーションを要する事象であるか否かの判断が容易でないことも多いが、エスカレーションを受ける立場の者が日頃から判断に迷う事象の報告をないがしろにしたり、放置したりしていれば、そのような対応の積み重ねにより、報告者の側に「このレベルなら報告の必要なし」という意識が定着してしまうおそれがある。そのような意識が定着している組織においては、真にエスカレーションが必要な場合に適切なエスカレーションを期待することができない。エスカレーションが適切に行われるか否かはルールや手続もさることながら、このような日頃の実務の積み重ねに影響される面があるから、エスカレーションを受ける立場の者には、

ささいなものであっても、日頃からその報告を真摯に受け止める姿勢が求められる。

⑷　情報セキュリティに係るルールの見直し

本アンケート調査（第８参照）においては、情報セキュリティに関するルールの形骸化を指摘する声が非常に多かった。その理由としては、ルールの量・煩雑さ、ルールを運用するための作業負担の多さを指摘するものが多く、例えば、「改定された規程類のボリュームが多すぎて、咀嚼できず、実効性が低い。」、「チェックシートやルールなど多く、理解が追い付かない。」、「ルールを厳しくすることにばかり傾倒し、その結果業務が回らなくなると、ルールは形骸化してしまう」、「情報セキュリティを守るためのルールや運用が管理簿やチェックシート等、アナログな対策が多く、かなりの業務負担になっている。煩雑なルールや運用は形骸化するリスクもある。人間が介在する運用では必ずミスが発生することから、システムに投資する方がよいと考える。」などといった指摘があった。

上記指摘の一部でも言及されているように、現場組織に守れない負荷を課すようなルールは、形骸化するおそれがある。前記⑵イでも触れたとおり、今後の情報セキュリティ体制は、現場組織の運用に頼らず、システムによる対処にシフトしていくべきであるが、そのことを前提として、システムによる対処の進展に応じて、現場組織が遵守すべきルールも現場組織が対応可能な負荷レベルとなるように見直されるべきである。

⑸　経営上の課題（人事施策、経営資源の配分等）

ア　グループ全体での経営資源配分と人事政策の見直し

前記第５・３⑷のとおり、情報セキュリティ体制に関するNTT西日本グループ全体の問題として、人事施策及び収益配分の歪みを指摘する声があった。

本件不正持ち出しを契機として、NTT西日本グループ全体として抜本的な是正措置を講じるのであれば、上記問題提起も踏まえ、予算割当てや人事施策について抜本的な見直しをする余地がないかを検討していくことも必要であろう。

コンプライアンス上のルールに違反した売上や利益は法的に正当化し得るものではない。一旦コンプライアンス（ルール）違反が発生すれば、事業遂行に大きな悪影響が発生することを肝に銘じて、重点の置き所を再検討すべきであろう。ガバナンス、コンプライアンス、監査などの徹底は収益に直結するものではないと捉えられがちであるが、企業が健全に成長していくためには、足腰を鍛えながら着実に

進むことが必要である。

その意味でも経営の中枢を担うべき人材をこれらの部門に配置し、実効性を確保するとともに、そのような配置が中核的人材の育成の観点からも有用であるとの意識を持つことも必要ではないかと考えられる。

また、予算割当てについても、グループ各社に対し自社のリスク環境に応じた情報セキュリティ体制の構築を求めるのであれば、グループ各社が自律的に必要な対策を実施できるような予算割当ての在り方が検討されるべきである。

イ　特定の者への依存とその固定化等への対処

前記１⑶アのとおり、BS については特定の者への依存とその固定化等への対処の必要性を指摘したが、本アンケート調査（前記第８参照）の結果、NTT 西日本グループ全体においても、BS と同様、特定のシステム管理者又は運用保守従事者が長期間（3 年超）にわたり同一の業務に従事しているにもかかわらず、そのことに対しての危機意識が浸透しておらず、又は、具体的なリスク低減措置を講じるまでには至っていない状況が確認されている（前記第８・３⑺）。

そのため、BS について指摘したように（前記１⑶ア参照）、重要情報に触れる者を一定の期間を超えて同一の業務に従事させることを禁じるルールを導入するなどの措置を NTT 西日本グループ全体で検討する必要がある。

ウ　業務委託、派遣関係の契約と実務の再検討と見直し

ある程度の規模以上の企業グループにおける情報漏洩その他の不祥事は、業務委託、派遣社員の関係で発生してきているものが少なくない。NTT 西日本グループにおいても、業務の専門化、効率性などの要請から、多くの業務委託、派遣契約が事業に組み込まれているが、本件不正持ち出しに直接関連する点を含め、関連契約と契約に基づく実務を再検討し、見直す必要があると考える。今日、グローバルベースでサプライチェーンの全てにわたってガバナンスやコンプライアンスの観点から見直しをすることが必要となりつつあるが、グループの業務・運営における業務委託、派遣の利用についても同様に、自社のガバナンス、コンプライアンスを基準にしつつ、業務委託と派遣に特有の要素を考慮し、関係先のガバナンス、コンプライアンス面での見直しをすることが必要となる。業務委託先、派遣元への質問権の規定、監査権、報告の徴求、などについても検討すべきであろう。関係先のコンプライアンス体制や、コンプライアンス教育の実施状況の確認なども、より実質的な観点から再検討すべきであろう。

⑹　組織文化の変革

ア　無謬性への執着

本緊急点検等の結果、本件不正持ち出しが生じた BS のみならず、NTT 西日本グループ各社において、実際には情報セキュリティ上の不備があるにもかかわらず、情報セキュリティ自主点検等では不備なしと報告されていた事例が多数確認された。この点について、BS の自主点検に関与した者は「意識として、〇にしないといけないという考えがあった。」と述べていたが[81]、これほどまでに多くの不正確な報告が各所で行われていたことを踏まえると、NTT 西日本グループの組織文化として、無謬性への執着というものが根強く存在していると考えざるを得ない。

本件過去調査において A 社に対する報告にいくつもの虚偽の内容が含まれていたのも、情報セキュリティ体制の不備を取り繕おうとする動機（前記第６・７）によるものであり、情報セキュリティ自主点検と同様、無謬性への執着の現れと考えられる。

イ　自分事として捉えない行動様式と前例踏襲

BS で確認された問題事象を俯瞰すると、（ⅰ）X 所属グループのバック SE チームの責任者は、同チームと同じ業務拠点で業務を行っていた X が特権的なアカウントを使用していることを知りつつも、自己の部下でないという理由で X の業務内容について特段の注意を向けていなかったこと（前記第４・２⑵）、（ⅱ）X 所属グループ内の本件システムに関係するチーム間では、情報セキュリティ上のルールの遵守に責任を負うべきチームが不明確な状況下、どのチームもこれを引き受けない状況となっていたこと（前記第５・１⑵ア（ア））、（ⅲ）情報セキュリティ自主点検の結果は、現場組織から NTT 西日本・情報セキュリティ推進部に報告される過程で BS 内の様々な部署を経由するにもかかわらず、各部署は点検結果を鵜呑みにして中継するだけであったこと（前記第５・１⑶）等の事実があり、これらは、いずれも、自己の所管する業務に関連した情報セキュリティ上のリスク・問題点を（少なくとも抽象的には）理解しながらも、定められた自己の責任範囲でなければ自ら積極的に解決に当たろうとはしない行動様式として括り出すことができる。

このような行動様式は、本件過去調査において自社からの情報漏洩の疑いという危機状況に接しながら、調査担当者らの誰ひとりとして、情報漏洩の有無を確認

[81] 前記第５・１⑶ア（ウ）参照。

するための積極的な調査を提案せず、A 社からの質問対応に終始していたことにも表れていると考えらえる（前記第６参照）。

NTT 西日本グループ各社においても、情報セキュリティ上の不備が多数存在し、それが自主点検等で見過ごされてきた状況があることからすると（前記第７参照）、BS について指摘した行動様式、すなわち、定められた自己の責任範囲でなければ自ら積極的に解決に当たろうとはしない行動様式は、少なくとも NTT 西日本グループの一部の役職員にも見られる。

本件アンケート調査（前記第８参照）においても、「率先して自ら行う風土はない」、「自分事として受け止めている風だが、実際まだまだ他人事と受け止めている様な気がする。」などの指摘（回答）があった。

以上に加え、本件アンケート調査では、前例踏襲の風土があるとの指摘も多数あった。これも、前例を踏襲していれば自己の責任ではないという発想に根差すものであり、それを理由に自ら積極的に解決に当たろうとはしないという意味では同根であると言える。

ウ　現場任せの風潮

本アンケート調査（前記第８参照）では、各種の情報セキュリティ上のルールの遵守が現場任せになっているとの指摘が多数あった。例えば、「問題が起きるたびに新たなルールを制定し、再発防止をしてきているのは当然のことだと考えていますが、対策をコスト（稼働等）を無視してどんどん追加するため、実際にそのルールを守りつつ運営できるか？という観点や、稼働が増えることでのコストへの手当（人員増等）の議論をせず、気合と根性、起きたらその人（部署）の責任論にするのは、誰も得しないと考えてます。」、「対処可能な範囲のチェックや対策は山ほど挙げるが、その有効性、実効性が確認されることは少なく、軽微な事象が発生するたびに、ほとんど効果が無さそうなチェック項目やフローが増える。また、それを減らすことも考えない。」などの指摘があった。

前記⑷で触れたルールの形骸化が NTT 西日本グループの各所で見られることからすれば、NTT 西日本グループ全体として上記のような現場任せの風潮があり、それがルールの形骸化につながったと考えられる。

エ　顧客の立場に立つ目線の不足

本件過去調査では、「調査」と表現することも憚られるほどの極めて杜撰な「作業」しか実施されておらず、事なかれ主義的な対応が繰り返されていたばかりか、故意に虚偽の回答を行うなどの極めて悪質な行為が行われていた（前記第６参照）。

そこには、「BS における情報セキュリティ管理体制の不備を取り繕うため」「A 社との取引を継続するため」あるいは「A 社からの更なる質問をかわすため」といった内向きの論理があるのみであり、顧客である A 社の不安を解消し、同社の抱える懸念や問題意識に真摯に向き合うという視点が決定的に欠けていたと言わざるを得ない。

この点のみをもって、NTT 西日本グループ全体として顧客の立場に立つ目線が不足していたと結論付けることはやや拙速であるが、本件過去調査の調査担当者らの上記のような内向きの論理は前記アで指摘した「無謬性への執着」や前記イで指摘した「自分事として捉えない行動様式」などの現れであると言えることからすれば、同様の問題、すなわち、顧客の立場に立つという目線の不足という問題が、BS 及び ProCX のみならず、NTT 西日本グループ全体に内在している可能性は否定できない。したがって、NTT 西日本グループ全体の組織文化を見直すに当たっては、この点についても重要な課題として認識する必要がある。

オ　変革の必要性

NTT 西日本グループの組織文化についての更なる検証は当調査委員会への委嘱範囲を超えるが、本調査から垣間見える、前記のような組織文化、前記ア「無謬性への執着」、イ「自分事として捉えない行動様式と前例踏襲」、ウ「現場任せの風潮」、エ「顧客の立場に立つ目線の不足」に対しては、NTT 西日本グループをあげて早急に改善に向けた行動を起こさねばならない。さもないと、NTT 西日本グループの発展を阻害することとなろう。

組織文化に根ざす行動様式は、当該組織の歴史、人、取り巻く諸制度、関連法令等が複雑に作用して形成され、変革は容易ではなかろうが、トップが変革への強い意志を持って組織文化のあるべき姿を指し示せば成し得ないものではない。また、こうした組織文化の変革は、上記のようなトップの姿勢に役職員一人一人が応えていくことも不可欠である。組織を率いる各階層のリーダーが自ら率先垂範して組織を牽引していくこと、そして、社員一人一人も自己の所管する業務の問題点を理解し、単に社内規律を遵守するに留まらず真に顧客の立場に立って、定められた自己の責任範囲だけに止まることなく自ら積極的に解決に向けて行動を起こすことで、変革はさらに進んでいくものと考えられる。本件不正持ち出し及び本件過去調査をグループ会社における個別の不祥事として捉えるのではなく、本調査を機に、組織文化を見直す機会とすることが求められる。

以上

	質問	回答（2022年4月15日）
1	リスト受け取りから削除までの流れに関するフロー及び規定	フローは決まっています。大まかには以下となります。 1.USB保管場所（鍵付き書庫）の鍵を受領する、 2.USBを書庫から取出す、3.[redacted]へログイン、USBを接続、リストデータを移動する、4.USBを[redacted]取り外し、5.OneContact端末（取込み端末）へUSBを接続、リストデータを移動する、6.USBにデータが残っていないことを確認して、取り外し、7.USBを保管場所へ返却、施錠、8.鍵の返却 規定というのは、貴社と締結しております以下の契約、覚書で認識合いますでしょうか。 [redacted]
2	データ授受、作業工程ごとの管理簿	「データ授受管理簿・削除管理簿」で運用しています。
3	データ授受、作業工程ごとの担当者名と職位（どの職位の誰がこの工程を行うことになっているかがわかるもの）	管理簿の記入、確認はセンタ毎に若干変わる部分はありますが、管理簿にて確認ができます。 作業：クラーク、SVが実施
4	USB貸出しの管理簿	「電子記録媒体使用管理簿」で運用しています。
5	USB取り扱いの運用ルール（鍵付き書庫で保管し、利用する場合はMGに承認をもらい、管理簿に記載して持ち出し・・・など、持ち出しから返却までの流れ）	運用ルールはあります。 鍵付き書庫で保管し、「電子記録媒体使用管理簿」へ記入、データが残っていないことを確認、返却まで管理 情報管理推進者（JM、センタ長等）が鍵付き書庫の鍵を保管、管理
6	USBを含め、各工程のログとログの保管期間（ログは個人単位で追うことができるようになっているかも含めて教えていただきたいです。）ログが無い場合は、その理由も合わせてお聞かせください。（理由：ログを取得する仕組みがない、作業者が共通のID、PWを使用しているため個人の特定ができない・・など）	[redacted]ログから個人特定は出来かねます。 OneContact端末は業務センタ毎にアクセス権限設定をしており、自センタ業務のみアクセス可、他センタへは接続不可の設定となっております
その他	また、管理簿につきましても1カ月以内に廃棄の予定がございましたら、見直しが完了するまでの期間は保管をお願いできますでしょうか。 見直しが出来ましたら、改めてご連絡させていただきます。	承知しました。各管理簿ごとに2年、3年などの保管期限を定めて運用しておりますが、ご連絡いただくまで当面保管するようにいたします。

	質問（2022年4月15日）	回答（2022年4月18日）
1	①授受管理簿は個人が特定できる状態になっていますでしょうか？もしなっていないようでしたら、個人特定ができるようにお願いします。	授受管理簿は実施者の個人が特定できるようになっております。
2	OneContactのログ保管期間は何年でしょうか？	【確認中】確認後回答いたします。
3	OneContactのログと管理簿を合わせて確認することで、誰がいつ操作を行ったのか分かる状態になっているのでしょうか？	[redacted] 操作の個人特定は可能です。
4	OneContactのID、PWをセンター単位から個人単位に変更していただくことは可能でしょうか？	可能です。現時点で個人単位で運用しております。
5	管理簿、OneContactのログについて、システムの入れ替えなどを除き、原則永年保管へ変更をお願いいたします。永年保管が難しい場合、その理由をご教示ください。	【確認中】確認後回答いたします。
6	[redacted]を個人単位に変更を予定しています。そのため、使用される方の氏名、メールアドレスをご教示いただけますでしょうか。	利用者一覧をとりまとめ、別途送付いたします。

■ PDSサーバへのアクセスに関するセキュリティポリシーについて

別紙6-3

2022年4月21日
NTTマーケティングアクトProCX

ONE CONTACT Networkにおける[redacted]データセンタに設置している[redacted]**PDSサーバ" 全４台は自社資産**として取扱っております

① 全体構成としては、**"完全プライベートネットワーク（閉域網）"による、当社センタのみがアクセスできる環境となっております。**

② ハードウェア構成については、PDSサーバを４分割しているため**サーバ間を跨ぐアクセスは不可**となっており、各センタから格納されたデータに関しても、**NWの構造とテナント規制により、一括出力できない仕組みを採用しております（当該センタ以外からアクセス不可）**

例）福岡の場合、**証明書をインストールした特定端末、権限者[JM,SV,CL]**[redacted]により、**自センタのデータのみ出力可能**

又、データの格納につきましても、特定端末、[redacted]により所属するサーバへアクセスし、データアップロードを行います

③ 権限者[JM,SV,CL]に付与する[redacted]**個人毎に付与しております。**

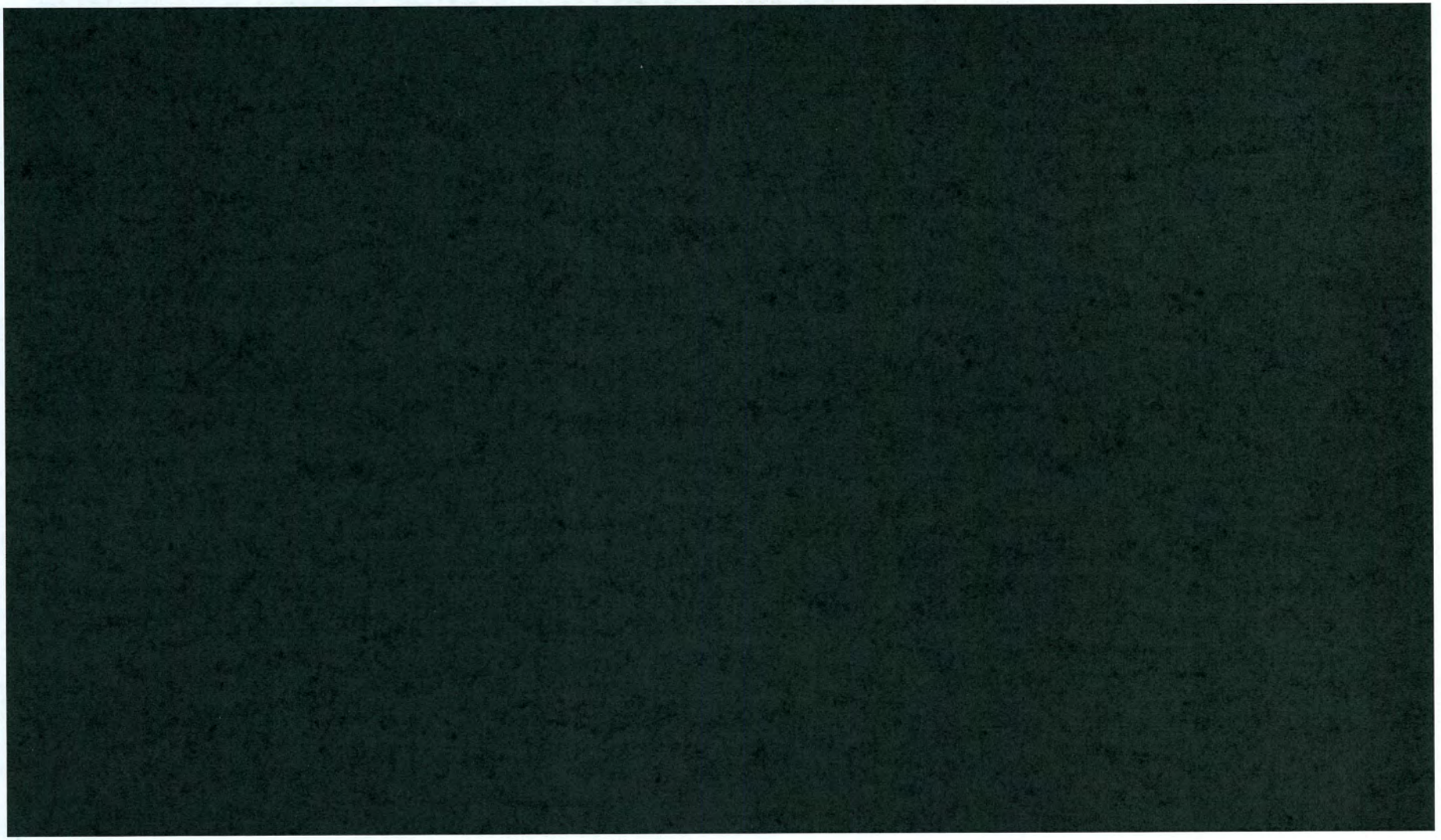
④ アクセス操作ログ（次項）を利用することにより、保存期間は永年対応が可能（但し、ディスク容量による。現時点十分な容量を確認）

＜補記＞ 保守者は**ハードウェアのヘルスチェック・OS再起動**のみメンテナンス（月1回）を実施し、個別業務データへのアクセスは不可。

[redacted]

■ 操作ログ出力イメージ（サンプル）

2022年4月21日
NTTマーケティングアクトProCX



■ リストデータの受け取り、納品に関する取扱いについて

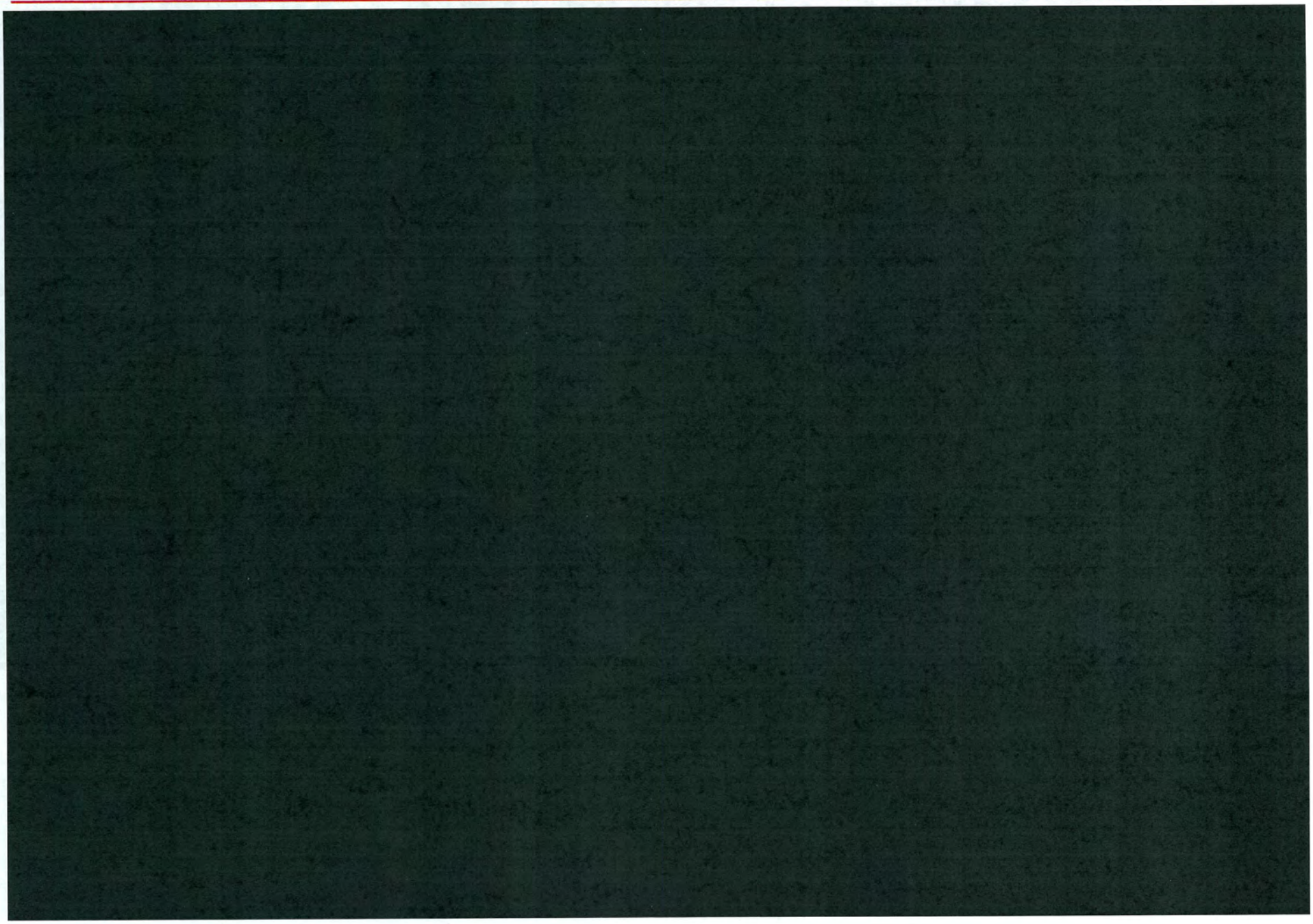
2022年4月21日
NTTマーケティングアクトProCX

- [redacted]様より配布された「リストデータ」の授受 に関しては、情報漏洩の対策(専用ブース、入退室管理)を実施した環境のもと運営しております。
- 特定USBメモリ(貴社貸与品、アクト備品)を利用し、①PC(貴社貸与品)から②PC(アクト端末)へとリストデータの移動し、ONE CONTACT Networkのサーバへ取込む。 また、業務終了後のアウト結果データ納品時は、②PCから特定USBメモリを使用し、①PCへ格納。
- 上記のデータ移動後は、使用した特定USBメモリ内、移動元②PC内、 ONE CONTACT Networkのサーバ内のデータ削除を実施、確認。

[redacted]

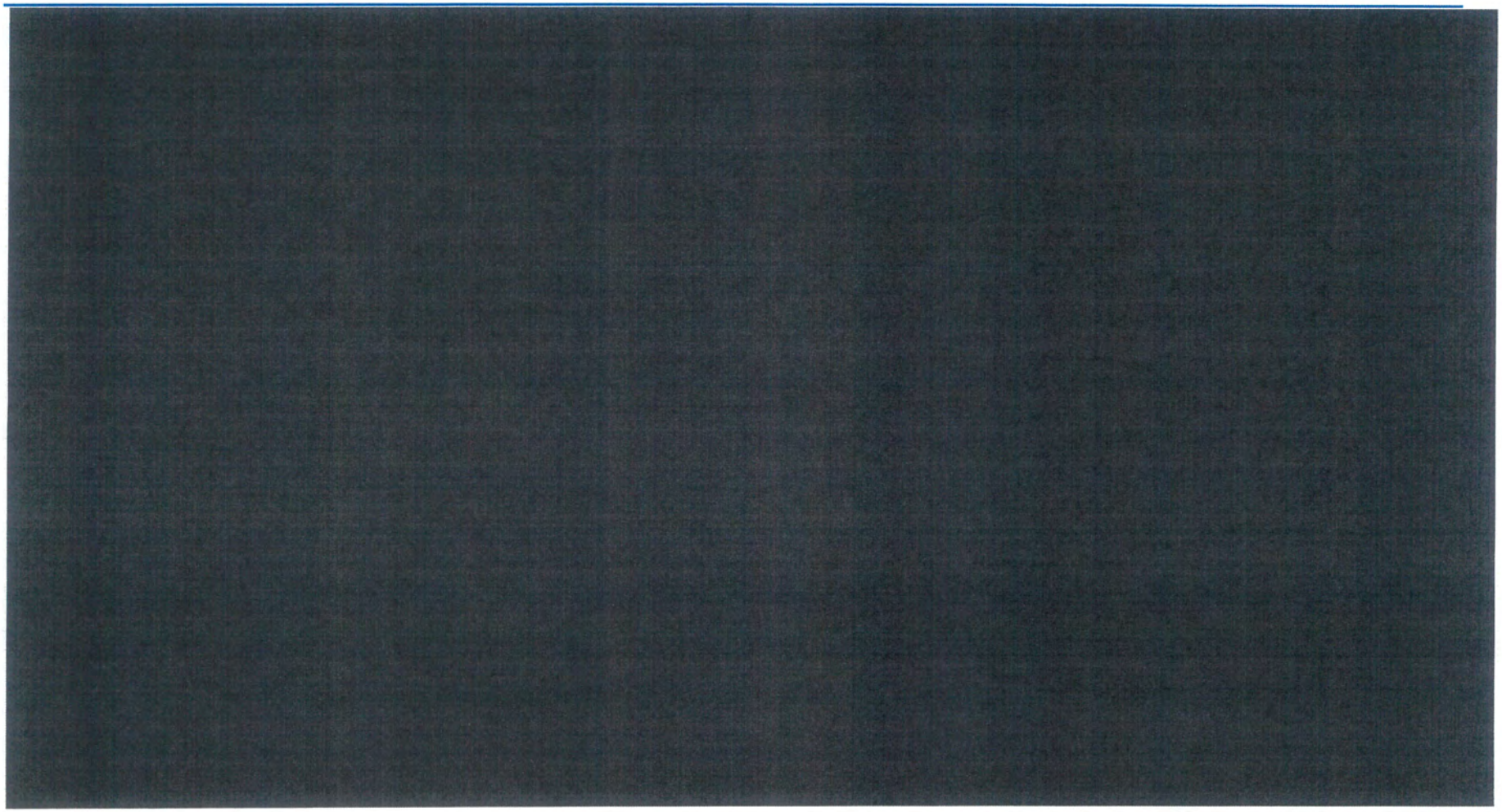
■ リストデータの受け取り、納品に関する監査結果

2022年4月21日
NTTマーケティングアクトProCX



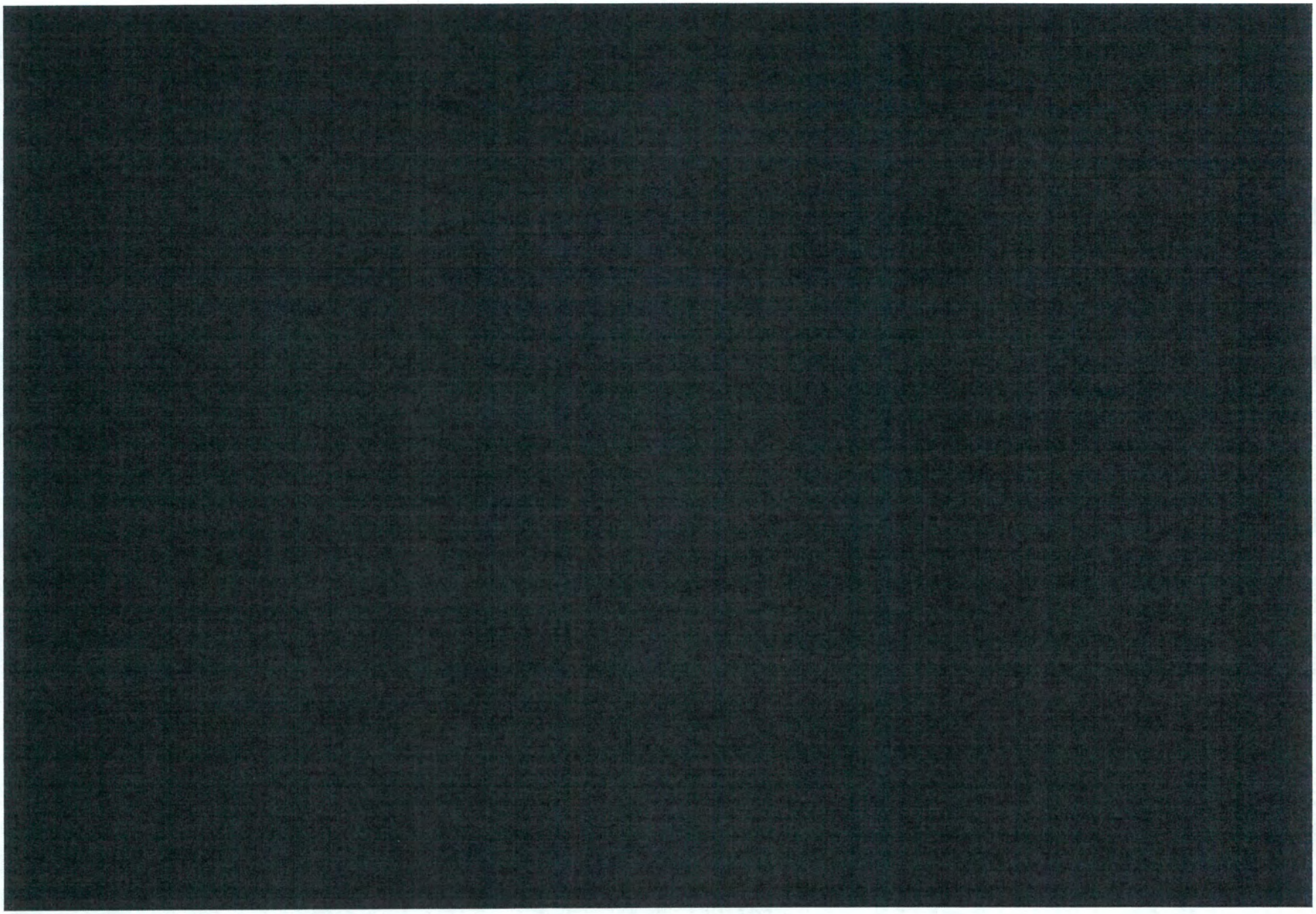
■センタフロア図及び監視カメラ設置状況について（1/5）

2022年4月21日
NTTマーケティングアクトProCX



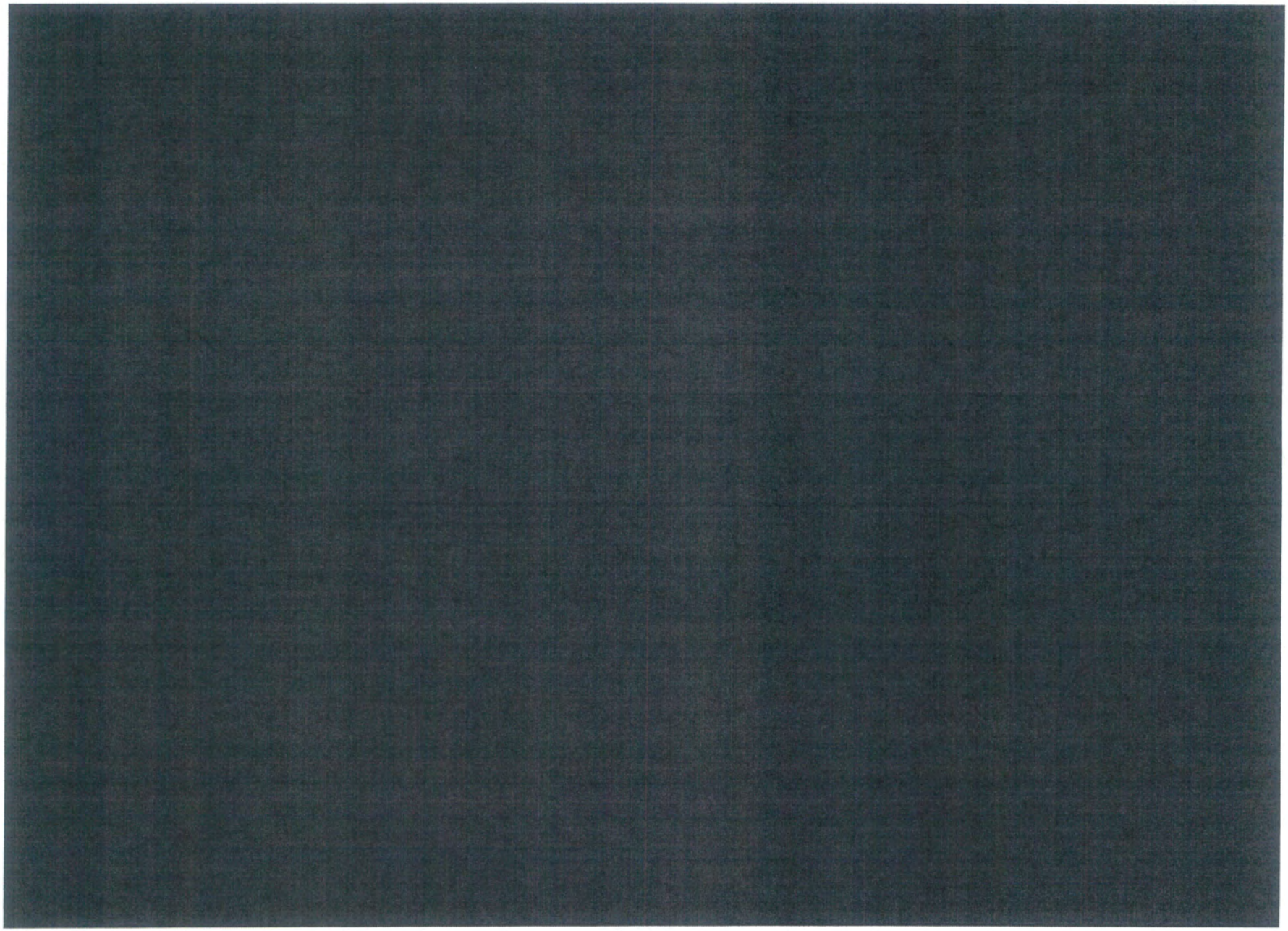
■センタフロア図及び監視カメラ設置状況について(2/5)

2022年4月21日
NTTマーケティングアクトProCX



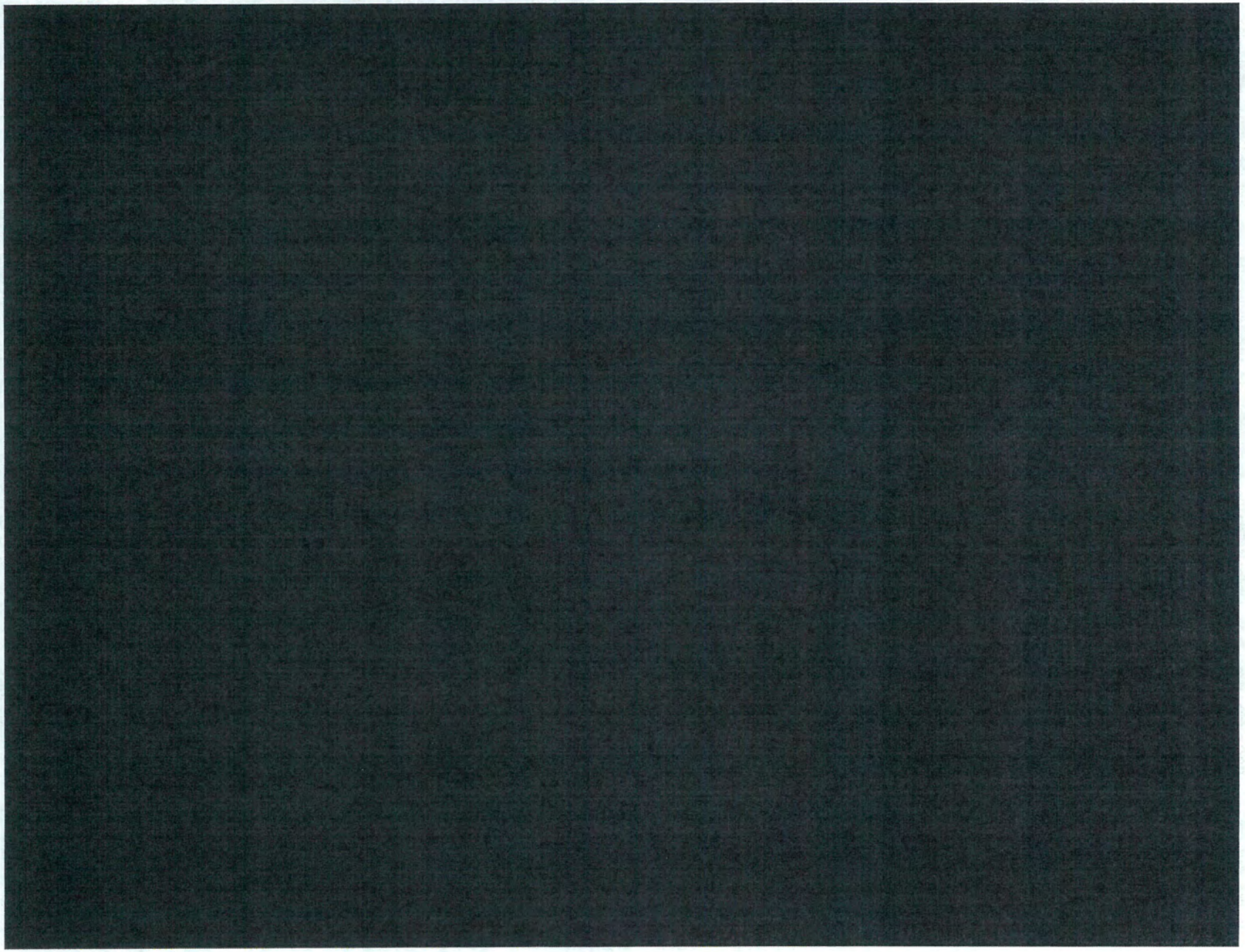
■センタフロア図及び監視カメラ設置状況について（3/5）

2022年4月21日
NTTマーケティングアクトProCX



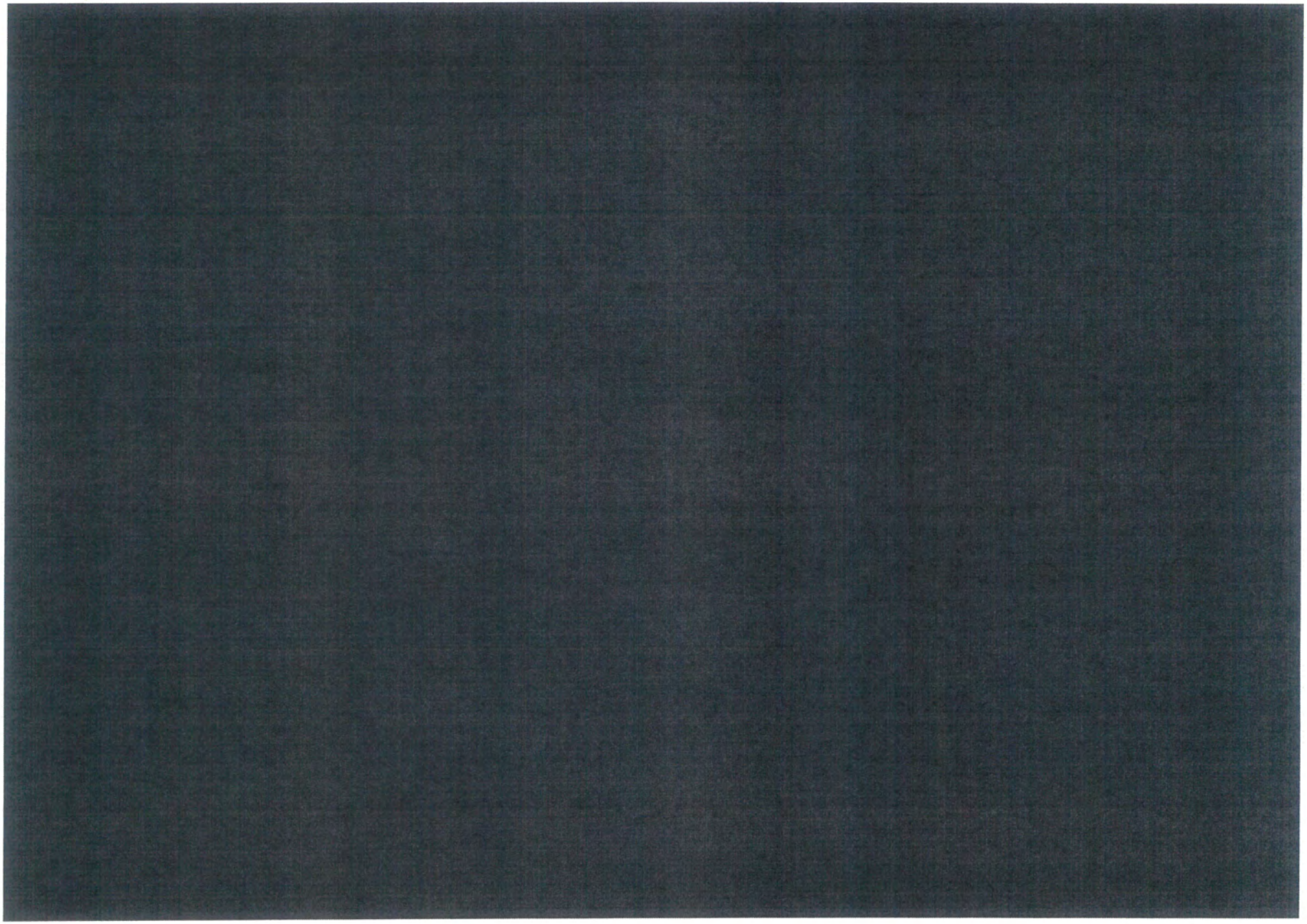
■センタフロア図及び監視カメラ設置状況について（4/5）

2022年4月21日
NTTマーケティングアクトProCX



■センタフロア図及び監視カメラ設置状況について（5/5）

2022年4月21日
NTTマーケティングアクトProCX



■ PDSサーバへのアクセスに関するご質問に関するご回答

別紙6-4　2022年5月11日　NTTマーケティングアクトProCX

■【質問表】

No.	日付	内容	回答	回答日	別紙
1	4月28日	ONE CONTACT NetworkのPDSサーバーのデータにアクセスできるシステム管理者の範囲（内部／外部、役職など）と人数、対象者氏名	■ISMS管理責任者5名 及び システム保守者4名となります。又、PDSサーバのデータにアクセスできる作業者はシステム管理者の4名。 [redacted]	5月11日	－
2	4月28日	前システムのセキュリティポリシー（20220421セキュリティ確認ご報告資料.pdfの１ページ目に相当する内容）と前システム機器廃棄時のデータの取り扱い内容	■前システム同様、ONE CONTACT Networkのセキュリティポリシーにつきましても、前回ご報告させて頂きました資料（20220421セキュリティ確認ご報告資料.pdfの１ページ目）と同じになりますが、システムメンテナンス等における保守用端末の取り扱いについては、別紙1(2)のとおり。 尚、前システム（PDSサーバ等）については、NTTフィールドテクノ社のデータ消去サービスを行った上、産業廃棄処分 [redacted] を実施しております。	5月11日	有（別紙1）
3	4月28日	ONE CONTACTNetwork環境および前システム環境における、ネットワーク外へのデータ取り出し方法と、データ取り出し出来るシステム管理者の範囲と人数、対象者の氏名	■NO.2関連、ONE CONTACT Network環境及び前システム環境も、各センタからのアクセス経路においては、ネットワークの構造とテナント規制により、ネットワーク外への一括データ出力は不可となっております。但し、各センタからの問合せ（トラブル対応、画面修正、疑似試験等）があった場合のみ、弊社([redacted])に設置している保守用端末〈※〉より、システム管理者（2名以上：担当課長＋担当者）にて、[redacted] キャンペーン構成・画面エラーチェック、動作試験等を実施することがありますが、データ出力したか否かの痕跡を調査した結果、別紙2のとおり、当社テスト用データの出力のみを確認しております。尚、システム管理者の範囲と人数、対象者はNO.1に記載のとおり。 〈※〉USBポート無し、暗号化ソフトがインストールされた専用端末	5月11日	有（別紙2）
4	4月28日	ネットワーク外へのデータ取り出し時の管理	■各センタにて特定USBメモリの使用、特定USBメモリの保管書庫の鍵管理、お客様情報の授受、削除管理を管理簿にて管理しています。作業実施者と確認者で確認する運営としています。 ① 特定USBメモリの使用管理 ・・・電子記録媒体使用管理簿 ② 特定USBメモリ保管書庫の鍵管理 ・・・鍵管理簿 ③ お客様情報の授受、削除管理 ・・・お客様データ授受・削除管理簿	5月11日	－
5	4月28日	パスワード管理ポリシー（必要な文字数、英文字・数字・記号などの条件）と更新頻度、更新実施者、取扱いルールについて	■システム管理上、パスワードの更新頻度は[redacted]	5月11日	－
6	4月28日	ONE CONTACT Networkへのシステム切り替えタイミングと、前システム（AQStage)からの移行時の切り替え手順（移行計画）書	■ONE CONTACT Networkへの切替日は以下のとおり各センタ単位で五月雨となっております。 第一回（岡山、福岡）　2020年 8月 1日 第二回（名古屋）　2020年12月11日 第三回（広島、高蔵寺）2021年 4月27日 第四回（熊本）　2021年 5月27日 第五回（豊橋）　2021年 7月30日 ＃切替手順書（福岡）は、別紙2のとおり	5月11日	有（別紙3）
7	4月28日	アウトバウンド業務終了後のデータ削除処理方法と実施ログの例（手動で削除の場合は、削除コマンドやＳＱＬ文、プログラム削除の場合は、処理仕様書やプログラムソースなど具体的な処理内容が分かるもの）	■アウトバウンド業務終了後のデータ削除については、システムに予め用意されているキャンペーンの削除機能にて実施いたします。 ＃キャンペーン削除のサンプル画面は別紙3のとおり	5月11日	有（別紙4）
8	4月28日	ONE CONTACT Networkと前システム（AQStage)の画面ハードコピー（弊社業務）を頂けますか。	前システム同様、ONE CONTACT NetworkもPDS画面そのものは同じものとなります。 ＃御社業務用のサンプル画面（福岡）は別紙4のとおり	5月11日	有（別紙5）

別紙1 ■ PDSサーバへのアクセスに関するセキュリティポリシーについて

2022年5月11日
NTTマーケティングアクトProCX

2022年4月21日ご提出資料

ONE CONTACT Networkにおける[redacted]データセンタに設置している[redacted]**PDSサーバ" 全４台は自社資産**として取扱っております

① 全体構成としては、**"完全プライベートネットワーク（閉域網）"による、当社センタのみがアクセスできる環境となっております。**

② ハードウェア構成については、PDSサーバを４分割しているため**サーバ間を跨ぐアクセスは不可**となっており、各センタから格納されたデータに関しても、**NWの構造とテナント規制により、一括出力できない仕組みを採用しております（当該センタ以外からアクセス不可）**

例）福岡の場合、**証明書をインストールした特定端末、権限者[JM,SV,CL]**[redacted]により、**自センタのデータのみ出力可能**

又、データの格納につきましても、特定端末[redacted]により所属するサーバへとアクセスし、データアップロードを行います

③ 権限者[JM,SV,CL] に付与する[redacted]**個人毎に付与しております。**

④ アクセス操作ログ（次項）を利用することにより、保存期間は永年対応が可能（但し、ディスク容量による。現時点十分な容量を確認）

＜補記＞ 保守者は**ハードウェアのヘルスチェック・OS再起動**のみメンテナンス（月1回）を実施し、個別業務データへのアクセスは不可。

[redacted]

別紙1(2) ■ PDSサーバへアクセス可能な保守用端末の取り扱いについて

2022年5月11日
NTTマーケティングアクトProCX

前項のとおり、システム管理者＝保守者は、ハードウェアのヘルスチェック・OS再起動のみメンテナンス（月1回）を実施しておりますが、メンテナンス時以外にも、**各センタから問合せ（トラブル対応、画面修正依頼・疑似試験等）があった場合のみ、弊社([redacted])に設置している保守用端末より、PDSサーバ全4台へアクセスできる環境となっております。**

① 全体構成としては、各センタ同様、**“完全プライベートNW（閉域網）”による、保守用端末のみがアクセスできる環境となっております**

② 保守用端末の構成については、**物理的にUSBポートのない端末で暗号化ソフトにて情報漏洩対策を実施、データ取出し不可**

③ 保守用端末は、センタ端末同様 **証明書をインストールした特定端末 及び テナント毎（拠点単位）に[redacted]により、必ず２名以上の体制にて、トラブル対応、模擬試験等の作業を実施するようにしております**

各PDSサーバのデータ出力ログを調査した結果、弊社テスト用のデータ出力のみであることを確認しております。

[redacted]

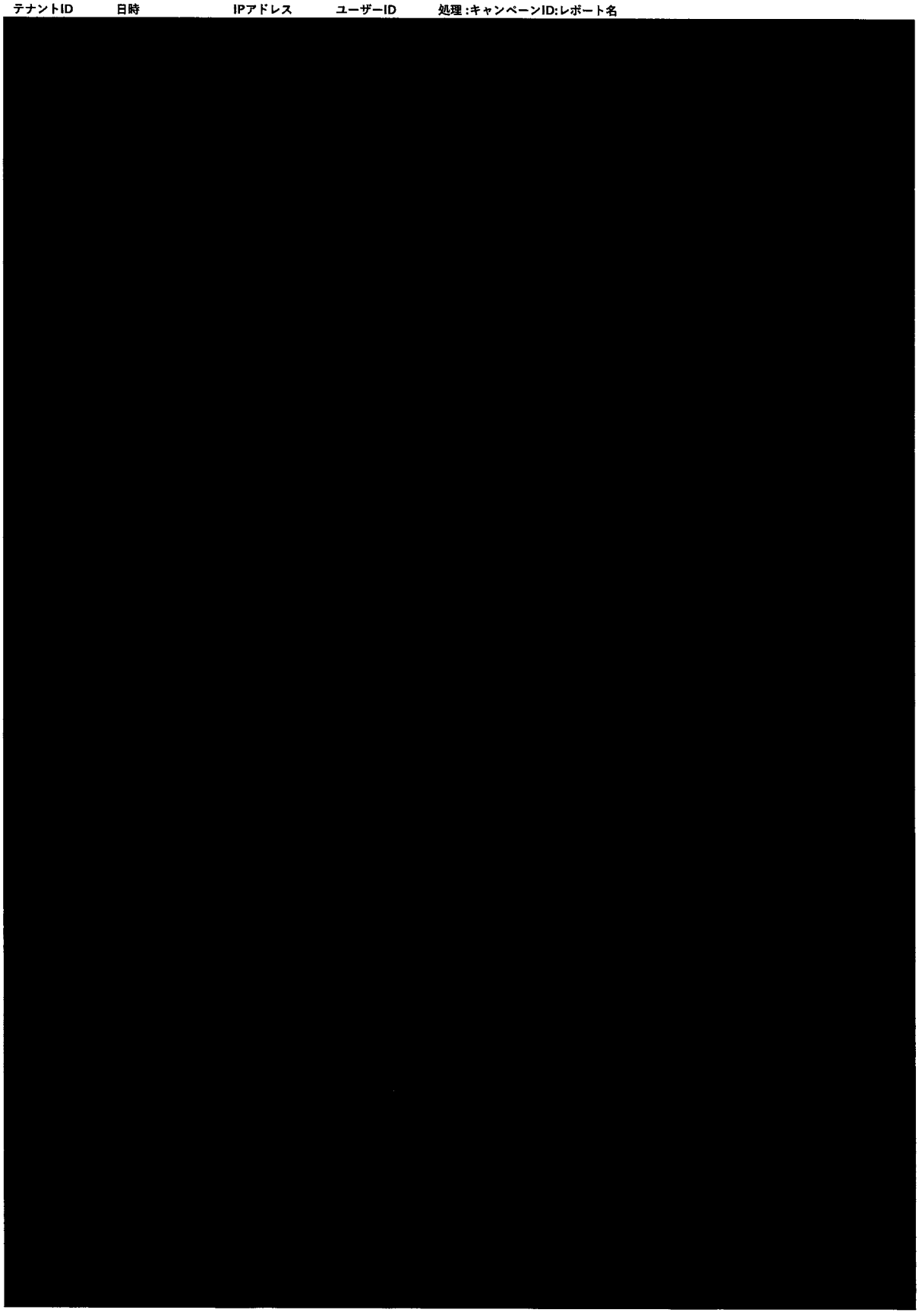
顧客データダウンロードログ

■期間：ONE CONTACT Network移行後（2020年8月11日） ～現在（2022年2月28日）

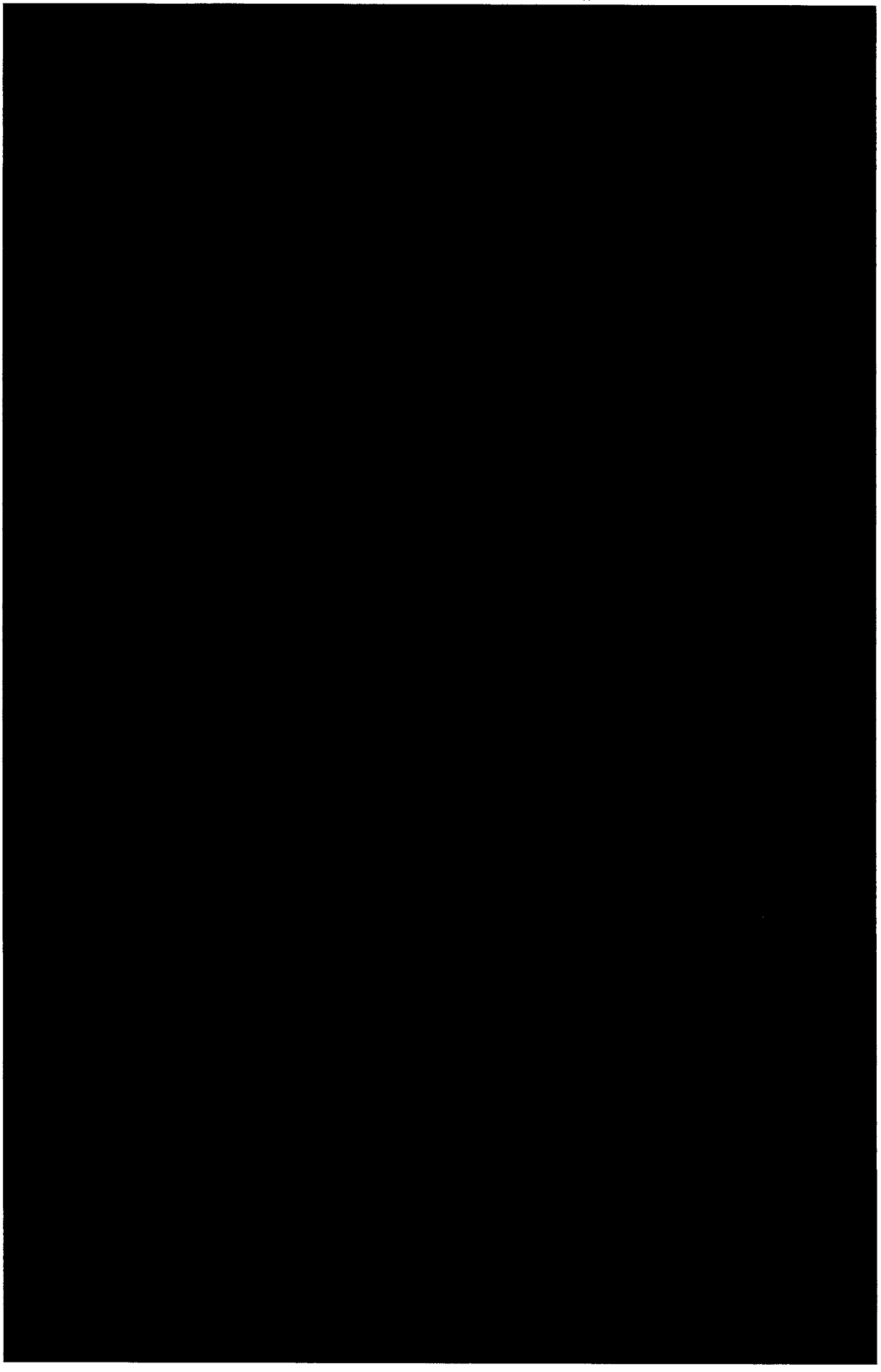
■テスト実施件数：255回

■調査結果：当社テスト用キャンペーンのダウンロードログのみ

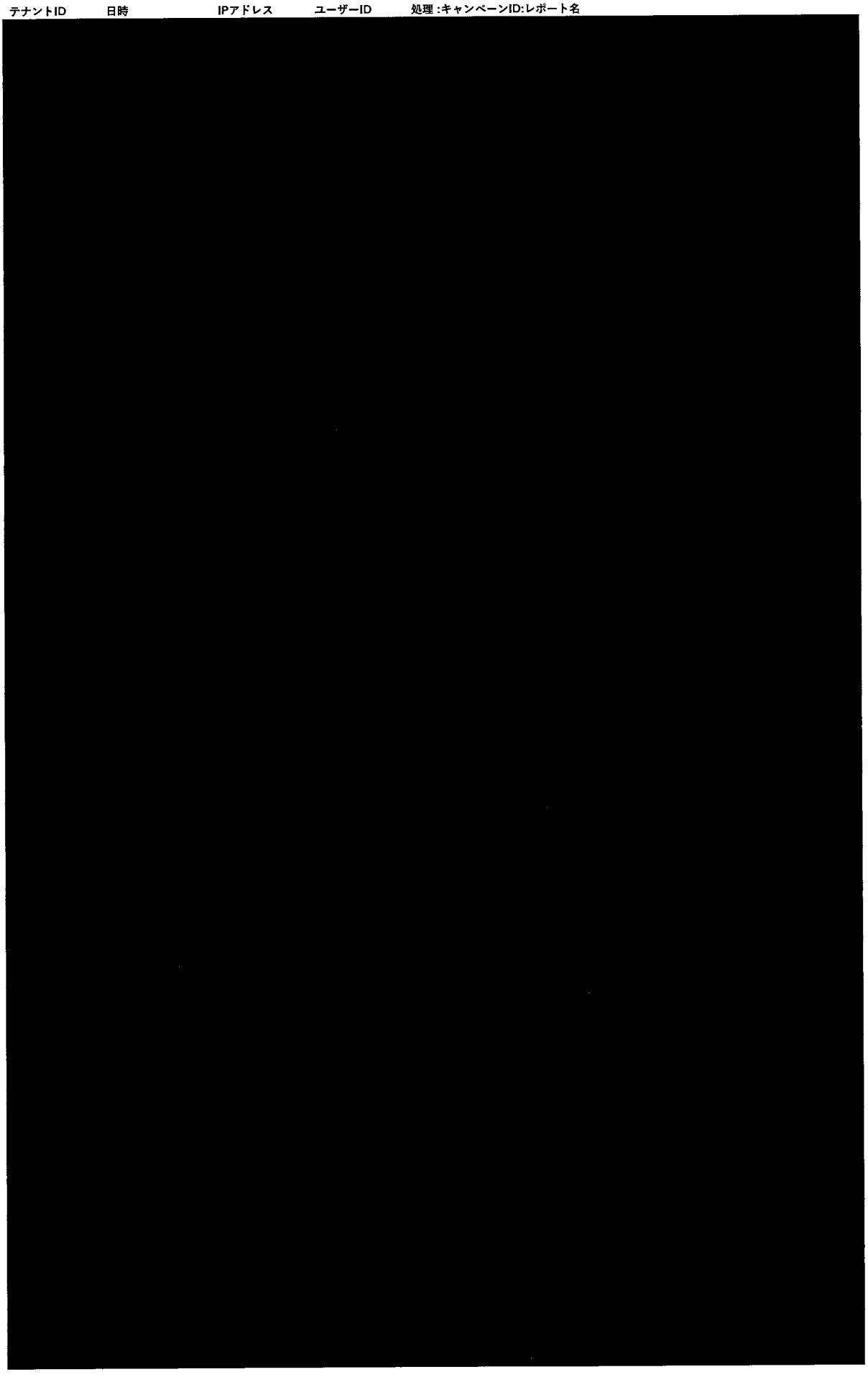
テナントID	日時	IPアドレス	ユーザーID	処理 :キャンペーンID:レポート名



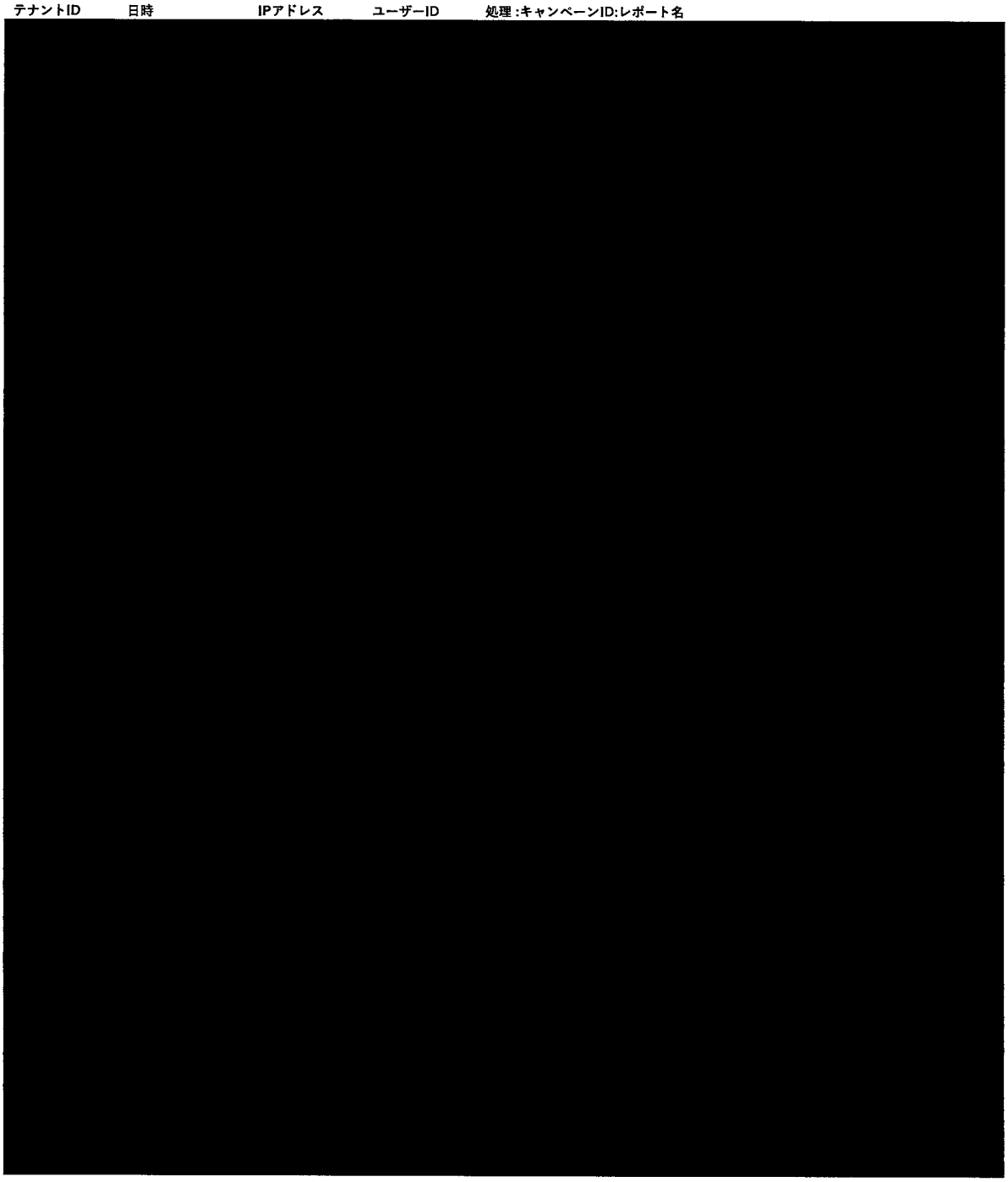
テナントID　日時　IPアドレス　ユーザーID　処理 :キャンペーンID:レポート名



テナントID　日時　IPアドレス　ユーザーID　処理 :キャンペーンID:レポート名



テナントID　日時　IPアドレス　ユーザーID　処理 :キャンペーンID:レポート名

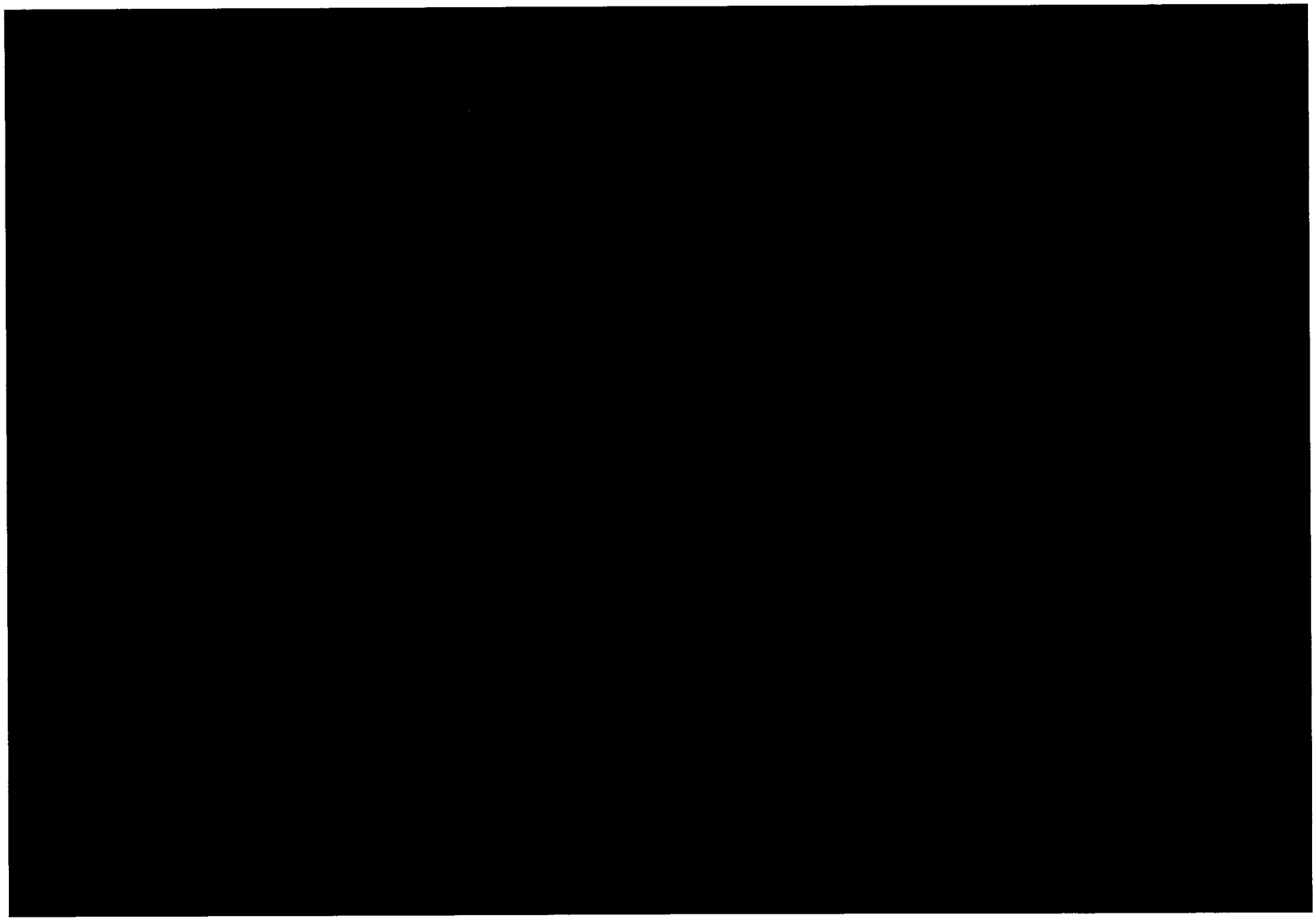


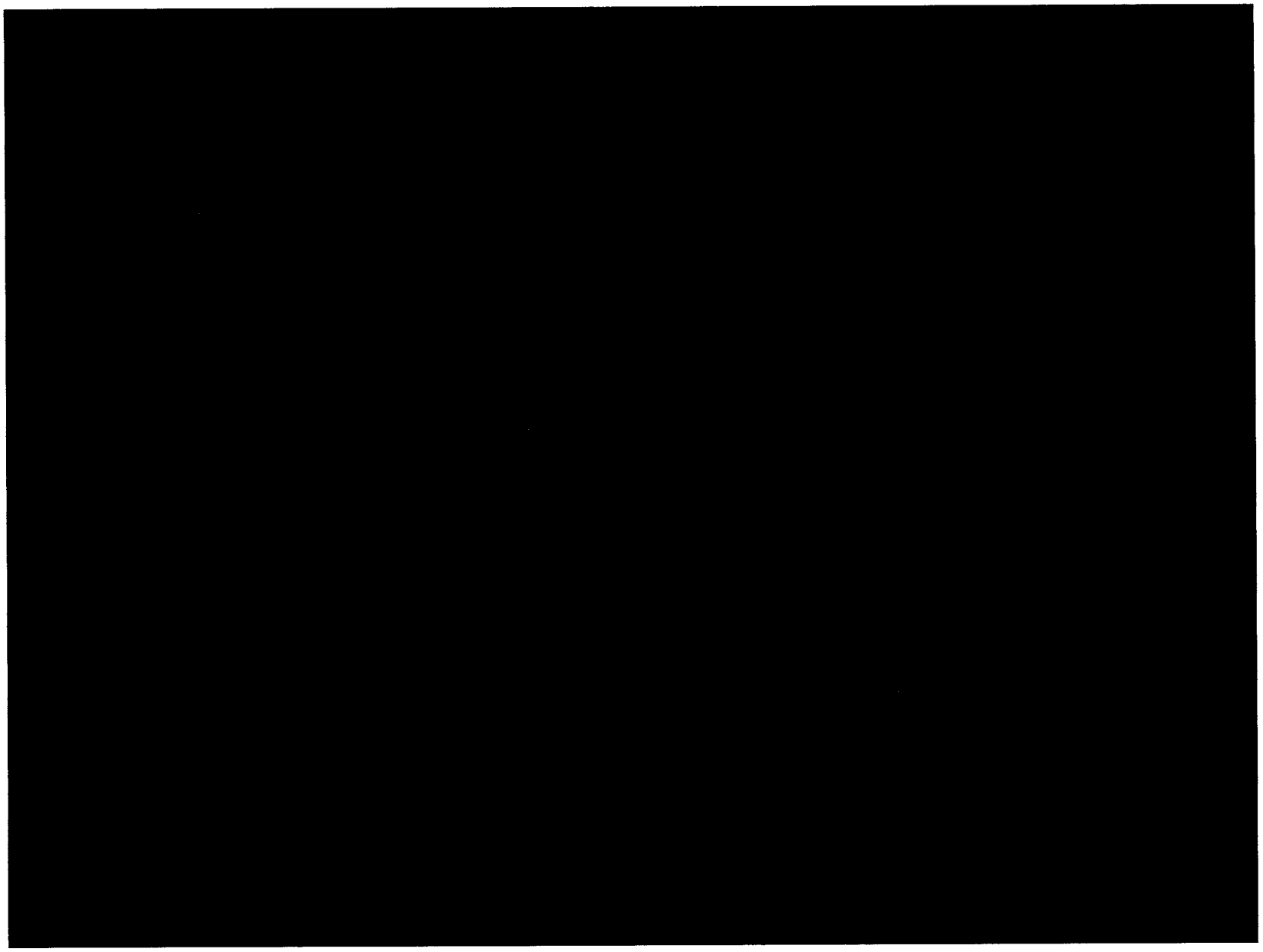
作業計画書

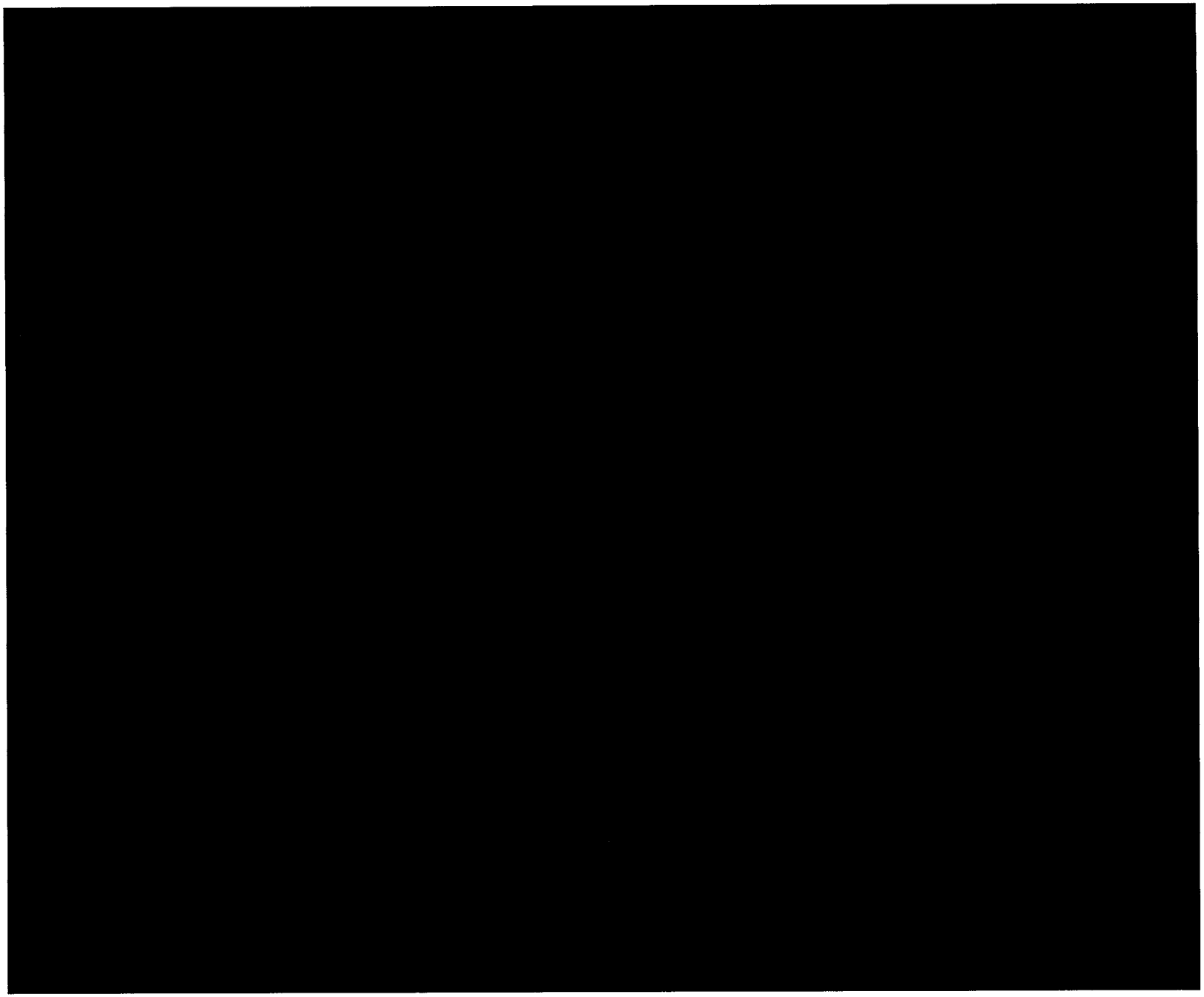
2020年7月28日 作成

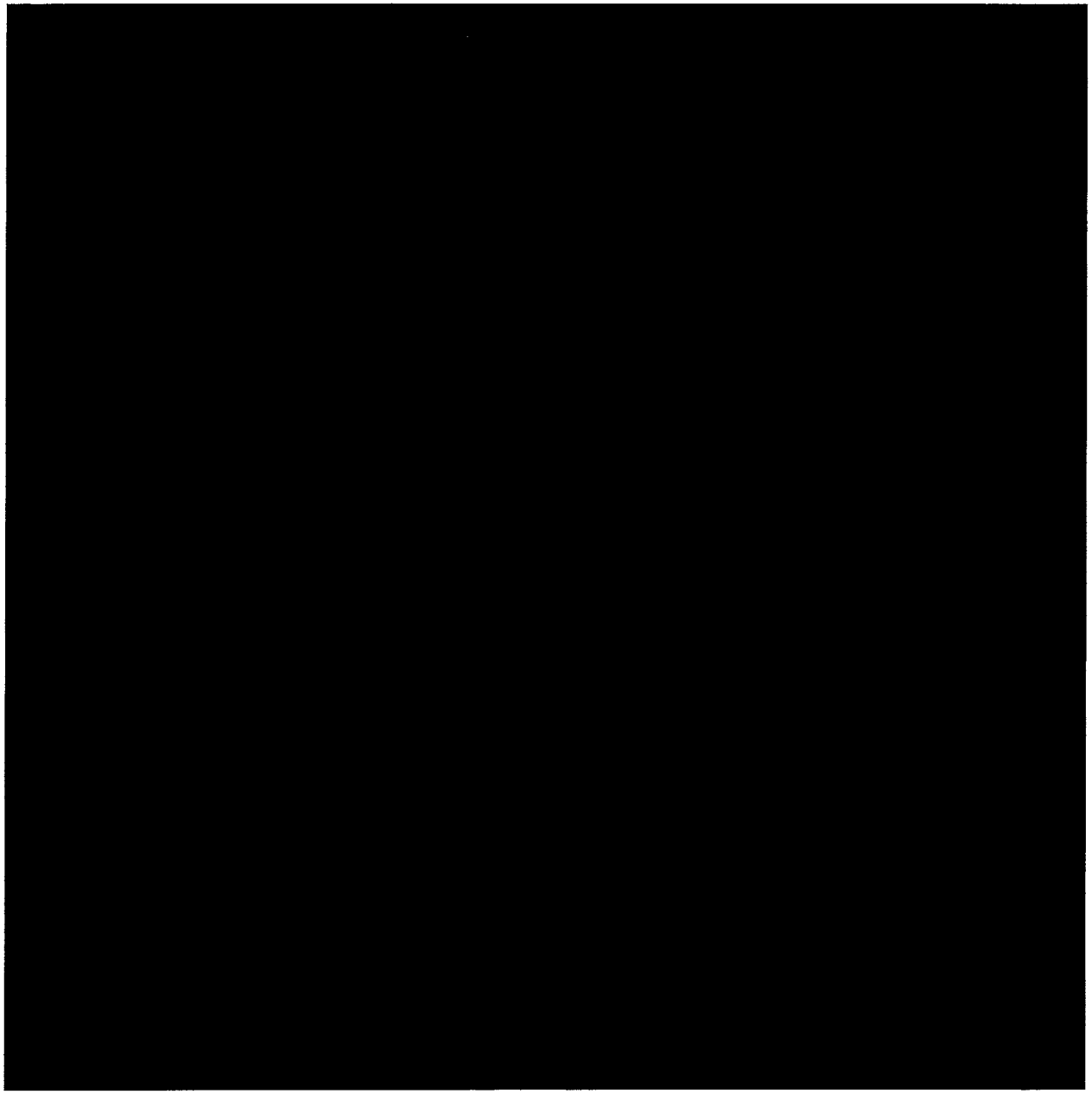
[redacted]

作成： 2020/7/13
更新： 2020/7/21









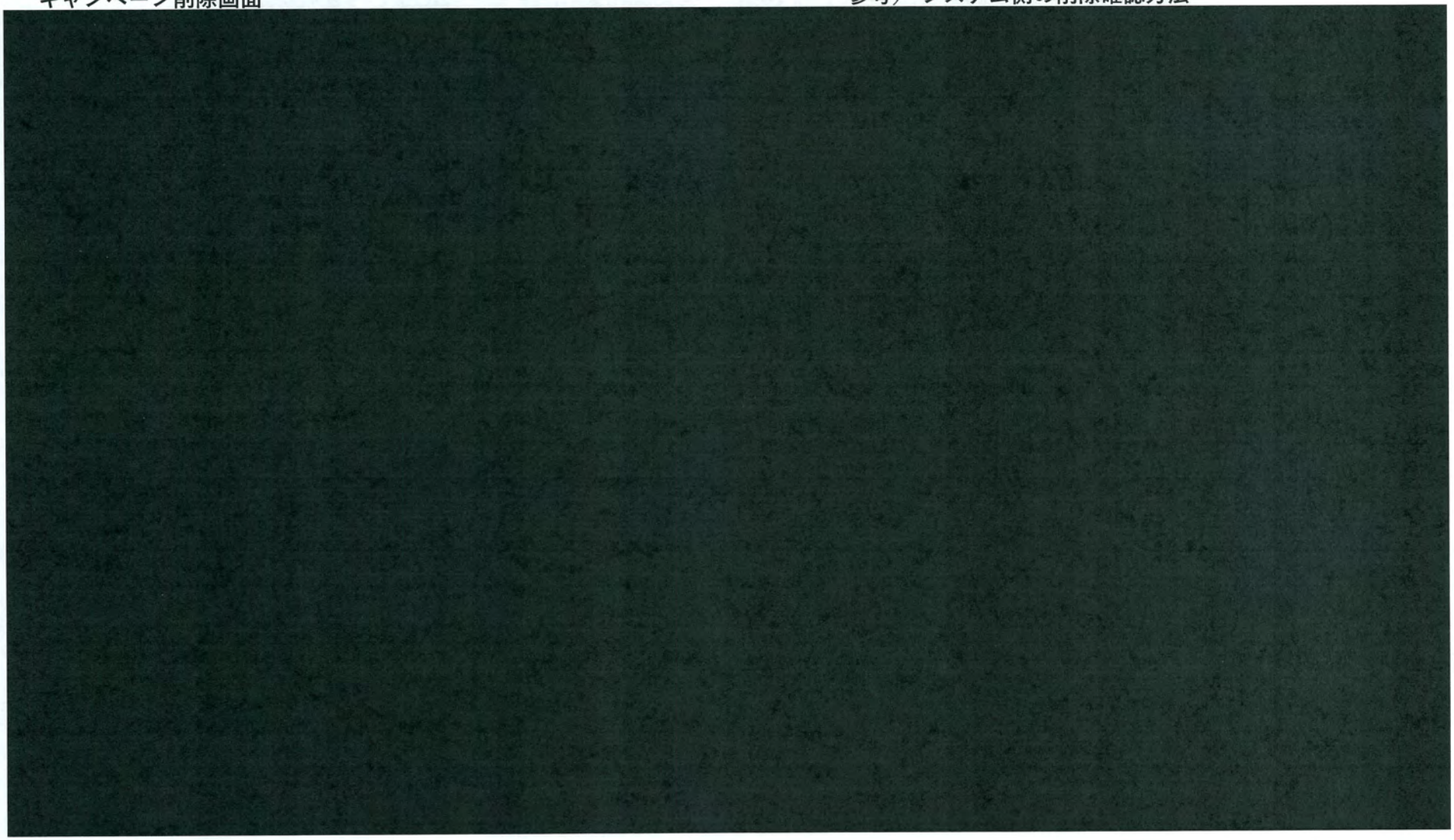
別紙4 ■ アウトバウンド業務終了後のデータ削除方法と実施ログの例

2022年5月11日
NTTマーケティングアクトProCX

✓ キャンペーン削除は、管理者権限のユーザーが[redacted]の「キャペーン構築」画面から実行できます。

✓ アウトバウンド業務終了後、当該業務のキャンペーンID【①】を選択し、削除【②】を実施します。

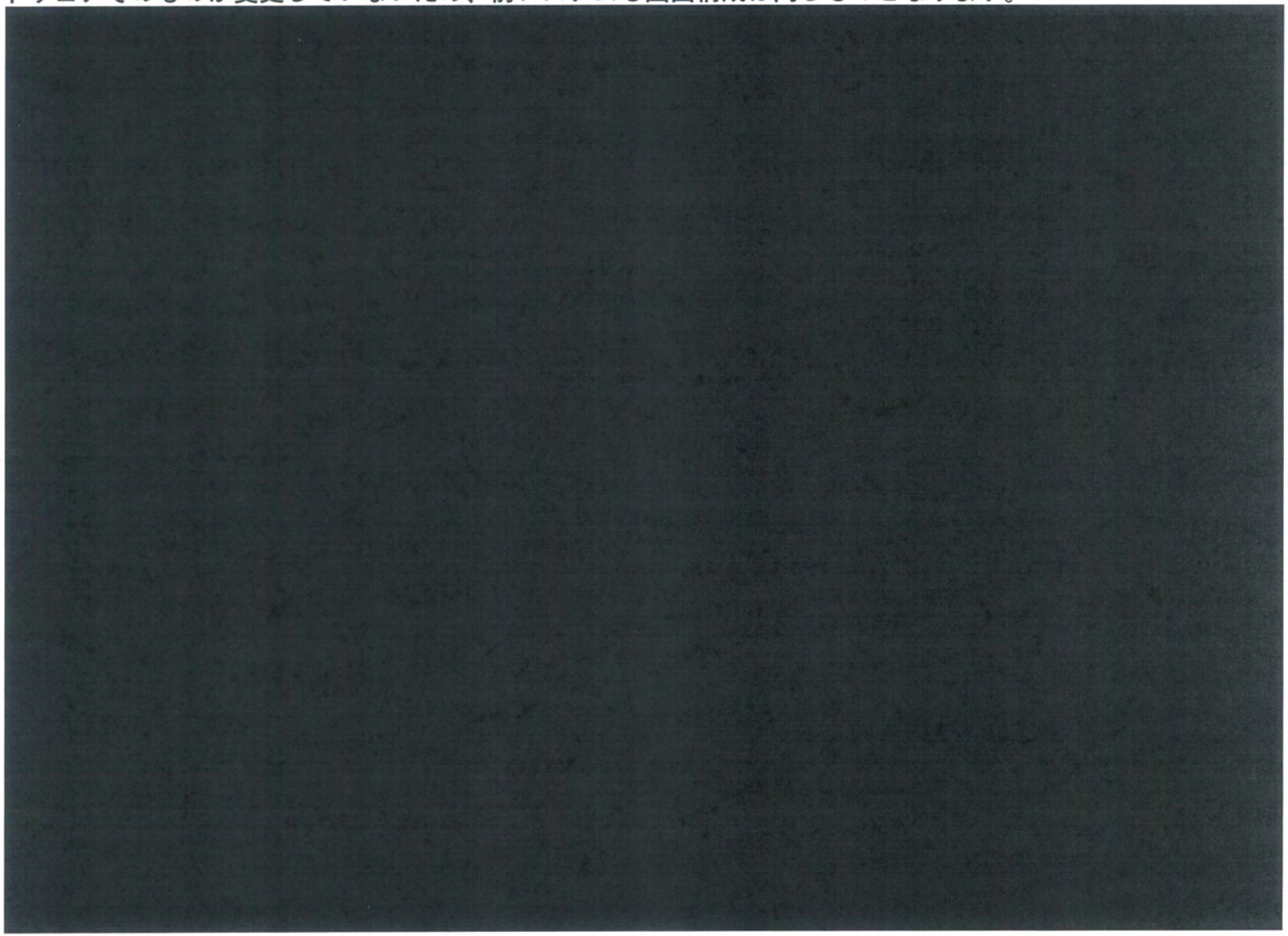
キャンペーン削除画面　　参考） システム側の削除確認方法



別紙5 ■ アウトバウンド業務画面のサンプルデータ

2022年5月11日
NTTマーケティングアクトProCX

✓ 以下、現在福岡センタにて利用中のサンプル画面（オペレータが受付・応対する画面）となります。
ソフトウェアそのものが変更していないため、前システムも画面構成は同じものとなります。



■ PDSサーバへのアクセスに関するご質問に関するご回答

別紙6-5　2022年6月1日
NTTマーケティングアクトProCX

No.	日付	内容	回答	回答日	別紙
1	4月28日	ONE CONTACT NetworkのPDSサーバーのデータにアクセスできるシステム管理者の範囲（内部／外部、役職など）と人数、対象者氏名	■ISMS管理責任者5名 及び システム保守者4名となります。又、PDSサーバのデータにアクセスできる作業者はシステム管理者の4名。 [redacted]	5月11日	－
2	4月28日	前システムのセキュリティポリシー（20220421セキュリティ確認ご報告資料.pdfの１ページ目に相当する内容）と前システム機器廃棄時のデータの取り扱い内容	■前システム同様、ONE CONTACT Networkのセキュリティポリシーにつきましても、前回ご報告させて頂きました資料（20220421セキュリティ確認ご報告資料.pdfの１ページ目）と同じになりますが、システムメンテナンス等における保守用端末の取り扱いについては、別紙1(2ページ)のとおり。 尚、前システム（PDSサーバ等）については、NTTフィールドテクノ社のデータ消去サービスを行った上、産業廃棄処分[redacted]を実施しております。	5月11日	有 （別紙1）
3	4月28日	ONE CONTACTNetwork環境および前システム環境における、ネットワーク外へのデータ取り出し方法と、データ取り出し出来るシステム管理者の範囲と人数、対象者の氏名	■NO.2関連、ONE CONTACT Network環境及び前システム環境も、各センタからのアクセス経路においては、ネットワークの構造とテナント規制により、ネットワーク外への一括データ出力は不可となっております。但し、各センタからの問合せ（トラブル対応、画面修正、疑似試験等）があった場合のみ、弊社[redacted]に設置している保守用端末〈※〉より、システム管理者（2名以上:担当課長＋担当者）にて、[redacted]キャンペーン構成・画面エラーチェック、動作試験等を実施することがありますが、データ出力したか否かの痕跡を調査した結果、別紙2のとおり、当社テスト用キャンペーンの出力結果しかございませんでした。尚、システム管理者の範囲と人数、対象者はNO.1に記載のとおり。 〈※〉USBポート無し、秘文ソフトウェアがインストールされた専用端末	5月11日	有 （別紙2）
4	4月28日	ネットワーク外へのデータ取り出し時の管理	■各センタにて特定USBメモリの使用、特定USBメモリの保管書庫の鍵管理、お客様情報の授受、削除管理を管理簿にて管理しています。作業実施者と確認者で確認する運営としています。 ① 特定USBメモリの使用管理　・・・電子記録媒体使用管理簿 ② 特定USBメモリ保管書庫の鍵管理　・・・鍵管理簿 ③ お客様情報の授受、削除管理　・・・お客様データ授受・削除管理簿	5月11日	－
5	4月28日	パスワード管理ポリシー（必要な文字数、英文字・数字・記号などの条件）と更新頻度、更新実施者、取扱いルールについて	■システム管理上、パスワードの更新頻度は[redacted]	5月11日	－
6	4月28日	ONE CONTACT Networkへのシステム切り替えタイミングと、前システム（AQStage)からの移行時の切り替え手順（移行計画）書	■ONE CONTACT Networkへの切替日は以下のとおり各センタ単位で五月雨となっております。 第一回（岡山、福岡）　2020年 8月 1日 第二回（名古屋）　2020年12月11日 第三回（広島、高槻寺）2021年 4月27日 第四回（熊本）　2021年 5月27日 第五回（豊橋）　2021年 7月30日 第六回（北九州）　2021年12月14日 ＃切替手順書（福岡）は、別3のとおり	5月11日	有 （別紙3）
7	4月28日	アウトバウンド業務終了後のデータ削除処理方法と実施ログの例（手動で削除の場合は、削除コマンドやＳＱＬ文、プログラム削除の場合は、処理仕様書やプログラムソースなど具体的な処理内容が分かるもの）	■アウトバウンド業務終了後のデータ削除については、システムに予め用意されているキャンペーンの削除機能にて実施いたします。 ＃キャンペーン削除のサンプル画面は別紙4のとおり	5月11日	有 （別紙4）
8	4月28日	ONE CONTACT Networkと前システム（AQStage)の画面ハードコピー（弊社業務）を頂けますか。	前システム同様、ONE CONTACT NetworkもPDS画面そのものは同じものとなります。 ＃御社業務用のサンプル画面（福岡）は別紙5のとおり	5月11日	有 （別紙5）

■ PDSサーバへのアクセスに関するご質問に関するご回答

2022年6月1日
NTTマーケティングアクトProCX

No.	日付	内容	回答	回答日	別紙
9	5月23日	ONE CONTACT NetworkのPDSサーバーのデータにアクセスできるシステム管理者の体制変更	■4/28回答のNo.1記載の体制につきまして、システム保守者（システム管理者）4名について、以下のとおり体制見直しを図りました。 （ISMS管理責任者/体制はそのまま継続） ・システム管理者 [redacted]	6月1日	－
10	5月23日	PDSサーバにおけるシステム管理ログ（顧客データダウンロード含む）の編集可否について	■PDSサーバへのアクセスログ・操作ログ等については、PDSサーバ本体へファイルとして自動で書出しされる仕組みとなっており、システム保守者は勿論、開発サイドでも編集することができない仕様となっております。	6月1日	－

■ PDSサーバへのアクセスに関するご質問に関するご回答

2022年6月1日
NTTマーケティングアクトProCX

No.	日付	内容	回答	回答日	別紙
1	5月24日	①お名前がある方の所属会社名を教えて下さい。	■NTTビジネスソリューションズ株式会社 バリューデザイン部 [redacted] より、以下6名となります。 [redacted] ■株式会社NTTマーケティングアクトProCX カスタマーソリューション事業推進部 [redacted] より、以下3名となります。 [redacted]	6月1日	–
		②ISMS管理責任者は、PDSサーバーのデータへのアクセスは可能でしょうか？（可能な場合、全拠点分か自拠点分のみかも合わせてお願いします）	■アクセス不可となります。 ■ISMS管理責任者等は、あくまでも情報マネジメントシステムにおける認証グループ全体の統括・統制する役割であり、システムへのログイン権限は持ち合わせておりません。	6月1日	–
2	5月24日	①前システムは現システムと全く同じ（"PDSサーバー"がエリア毎に分かれていた）構成でしょうか？	■同じ構成となります。エリア毎にサーバを物理的に４台分離した構成としております。（2022年4月21日ご提出資料のとおり【別紙1】）	6月1日	–
		②データ削除（NTTフィールドテクノ社）や廃棄[redacted]についての実施証明は取られていますでしょうか？	■前回（4月28日 No2.回答）"前システム（PDS）はデータ削除や産業廃棄処分を実施しております"とご回答させて頂きましたが、"データ削除や廃棄処分は未だ実施しておらず"、弊社情報伝達の不手際により誤ったご回答をしてしまい、申し訳ございません。 又、未実施の理由につきましては、他物品との兼ね合いもあり、固定資産（サーバ類等）の除却は弊社として2022年.7月実施するルールとしておりました。 尚、"前システム（PDS）"のハードディスクは全てフォーマット化の上、データがないことを確認しており、弊社[redacted]ビルの鍵付き書庫に保管してあります。 補足）データ削除（NTTフィールドテクノ）及び 産業廃棄[redacted]に関する両社への申請手配は既に完了しておりますので、実施予定である2022.7月以降は実施証明書をご提出することは可能です。	6月1日	–
		③システム切り替え（最終のみで結構です）、サーバー撤去、データ消去、サーバー廃棄がそれぞれ何月何日に実施されたか教えて下さい。	■サーバ撤去日につきましては、2月21日となります。 ■データ消去 及び サーバ廃棄に関しては、No.2-②の示すとおり、2022.7月実施予定。	6月1日	–
3	5月24日	①保守端末からログインの実績については、実施記録とログの突合せにより誰がいつログインしたかの証明が可能な状態でしょうか？	■保守端末においては、貴社以外のユーザ含めた緊急故障対応 及び 緊急設定依頼等を作業者が迅速 且つ 早期復旧させる必要があることからも、実施記録簿はつけておりません。 但し、作業については必ず管理者含む2名体制にてクロスチェックし実施するようにしております。	6月1日	–
		⇒現地希望確認（実施記録とログの突合せ確認）	■NTTビジネスソリューションズにて定めた社屋等規程ルール＜第6条＞により、高セキュリティエリアにおいては、貴社以外から頂いた様々な機密情報、設備等をお預かりしているエリアには、許可された者（契約業者、社員）だけが入室できるエリアとしている為、現地確認は見合わせて頂きたく、お願い申し上げます。 但し、こちらから開示できる資料、ログ出力情報等につきましてはご協力させていただきます。	6月1日	–
		②別紙２のログについて、前システムのログは御座いますか？また、フィルターが掛けられていると思われるのでどのような内容でフィルターが掛かった状態でしょうか？	■前システムログ（ONE CONTACT Network移行前）は別紙6参照。 ■フィルターについては、新システム（ONE CONTACT Network）への移行分のみをサンプル抽出したこと、又、管理者用ID [redacted]を含むID）のみに絞らせて頂きました。	6月1日	別紙6
		③同一PDSサーバー上の別の拠点のデータへのアクセス制限は、ID/Passの制御によるものでしょうか？	■ご認識のとおりです。[redacted]	6月1日	–
		④別のPDSサーバー上の別の拠点のデータへのアクセス制限は、ネットワーク設定によるものでしょうか？	■ご認識のとおりです。[redacted]	6月1日	–
4	5月24日	①ご回答に記載の①～③の管理簿の内容を証明するシステムのログは御座いますでしょうか？	■①～③の管理簿のうち、①USBメモリの使用管理、②USBメモリの保管倉庫の鍵管理におけるシステムログはございません。③ お客様情報の授受、削除管理『お客様データ授受・削除管理簿』に記載のデータインポート、データ削除を確認できるシステムログがございます。 尚、システムログ（データインポート、エクスポート）は永年保存、センタ端末にて確認できます。但し、システムログ（データ削除に関して）は1週間保存となりサーバ本体での確認となります。	6月1日	–
		⇒現地希望確認（実施記録とログの突合せ確認）	■No.3-①ご回答のとおり、[redacted]での現地確認は、見合わせて頂きたくお願い申し上げます。但し、こちらから開示できる資料、ログ出力情報等につきましてはご協力させていただきます。 又、③ お客様情報の授受、削除管理『お客様データ授受・削除管理簿』については、各センタで保存しているものをご提出することが可能です。	6月1日	–
		②このご回答にある"削除管理"とは、システムからのデータ削除のことでしょうか？またはシステム外に取り出したデータの削除の事でしょうか？	■システム画面上、PCローカルフォルダ、USBメモリ内のデータ削除を目視確認しています。	6月1日	–
		③システム外に取り出したデータを削除する際は、完全削除（"ごみ箱"から削除）することがルール化されていますでしょうか？	■はい、データ削除は貴社によるセキュリティ監査をの確認内容を踏まえまして、完全削除（ゴミ箱内の削除）をする運用ルールとしております。	6月1日	–

■ PDSサーバへのアクセスに関するご質問に関するご回答

2022年6月1日
NTTマーケティングアクトProCX

No.	日付	内容	回答	回答日	別紙
5	5月24日	①パスワードの文字数制限に"0～12文字以内"とありますが、パスワード無しも可でしょうか？	[redacted]	6月1日	－
		⇒現地希望確認（実施記録とログの突合せ確認）	■No.3-①ご回答のとおり、[redacted]での現地確認は、見合わせて頂きたくお願い申し上げます。 ■[redacted]センタ側での変更手順：[redacted]側にて出力したシステムログを突合し確認することは可能です。[redacted]	6月1日	－
6	5月24日	①データ移行作業に実施もしくは立ち会われた方は、手順書にお名前のあるお二方のみでしょうか？	■二名以外に作業責任者である[redacted]の立ち合いのもと実施しております。	6月1日	－
7	5月24日	①旧PDS1の手順書「3. テナントエクスポート」でエクスポートされたファイルはどのタイミングで新旧サーバーから削除されましたでしょうか？	■新サーバへ移行したエクスポートファイルについては、弊社の作業運用ルールにより、切替日1週間後に削除しております。 又、旧サーバのエクスポートファイル（原本）は、No.2-②ご回答のとおり、フォーマットしております。 補足）No.2-②ご回答のとおり、2022.7月にてデータ消去及びサーバ廃棄を行います。	6月1日	－
		②旧および新サーバー上で「テナントエクスポート」されたファイルの削除や操作の記録（ログ）は確認可能でしょうか？	■新サーバへ移行したエクスポートファイルの削除に関しては手順書(サンプル)になりますが、ご確認いただくことは可能です。 又、旧サーバに関しては、No.2-②ご回答のとおり、フォーマットのみ実施した形式となります。	6月1日	－
		⇒現地希望確認（実施記録とログの突合せ確認）	■No.3-①ご回答のとおり、[redacted]での現地確認は、見合わせて頂きたくお願い申し上げます。但し、手順書（タイムスタンプ有り）をご提出することは可能です。	6月1日	－
		③新PDS1の手順書「1. エクスポートファイルをコピー」のバックアップファイルの内容（バックアップのサイクル、対象、形式など）を教えて下さい。	■手動バックアップファイルにおける内容については以下のとおり a. サイクル：日次（夜間） b. 対象　：DBデータおよびログファイル c. 形式　：DBデータはダンプ出力し tar に圧縮 　　ログファイルは tar に圧縮 d. 保存期間：　DBは１週間。	6月1日	－
		⇒現地希望確認（実施記録とログの突合せ確認）	■No.3-①ご回答のとおり、[redacted]での現地確認は、見合わせて頂きたくお願い申し上げます。 ■実施記録については、2022年5月11日ご提出資料【別紙3】作業手順書シートにタイムスタンプを記載しておりますが、手動にてバックアップしたファイルは上記保存期間に示すとおり、1週間しか保存されていないため、突合することが困難な状況です。	6月1日	－
8	5月24日	①弊社データを取り込んだ時に作成されるデータについて下記の教えて下さい。 ⇒テーブルの命名規則、名前の付け方（自動or手動）、キャンペーンIDとテーブル名の関係、削除アプリのキャンペーンIDと削除対象テーブル判断の仕様	■テーブル命名規則 [redacted] ■キャンペーンIDとテーブル名の関係は[redacted] ■削除アプリは[redacted]削除を実行します。 ■削除対象テーブル判断の仕様 [redacted]	6月1日	－
		②実際の運用でデータ削除をした際の処理結果のログを確認させて下さい。	■実運用データの削除は、キャンペーン終了後でしか実行できないこと。又、前回ご提出させて頂きました【別紙4】アウトバウンド業務終了後のデータ削除方法と実施ログの例に記載しております、削除後のログ確認はシステム側にて開発ツールを用いて実行するため、キャンペーン終了後のタイミングに合わせ、削除ログを取得しご提出となります	6月1日	－
		⇒現地希望確認（実施記録とログの突合せ確認）	■No.4-①ご回答のとおり システムログに関しては、データ削除は1週間分のみご提出することは可能です。 又、お客様データ授受・削除管理簿については、各センタで保存しているものをご提出することが可能です。	6月1日	－
9	5月24日	①（別紙5 ■ アウトバウンド 業務画面のサンプルデータ）で実際の当社のデータが入った画面を確認させて下さい。 ⇒現地希望確認（実施記録とログの突合せ確認）	■業務画面につきましては、各センタにて業務実施移管内でご確認いただくことが可能です。	6月1日	－ －

顧客データダウンロードログ

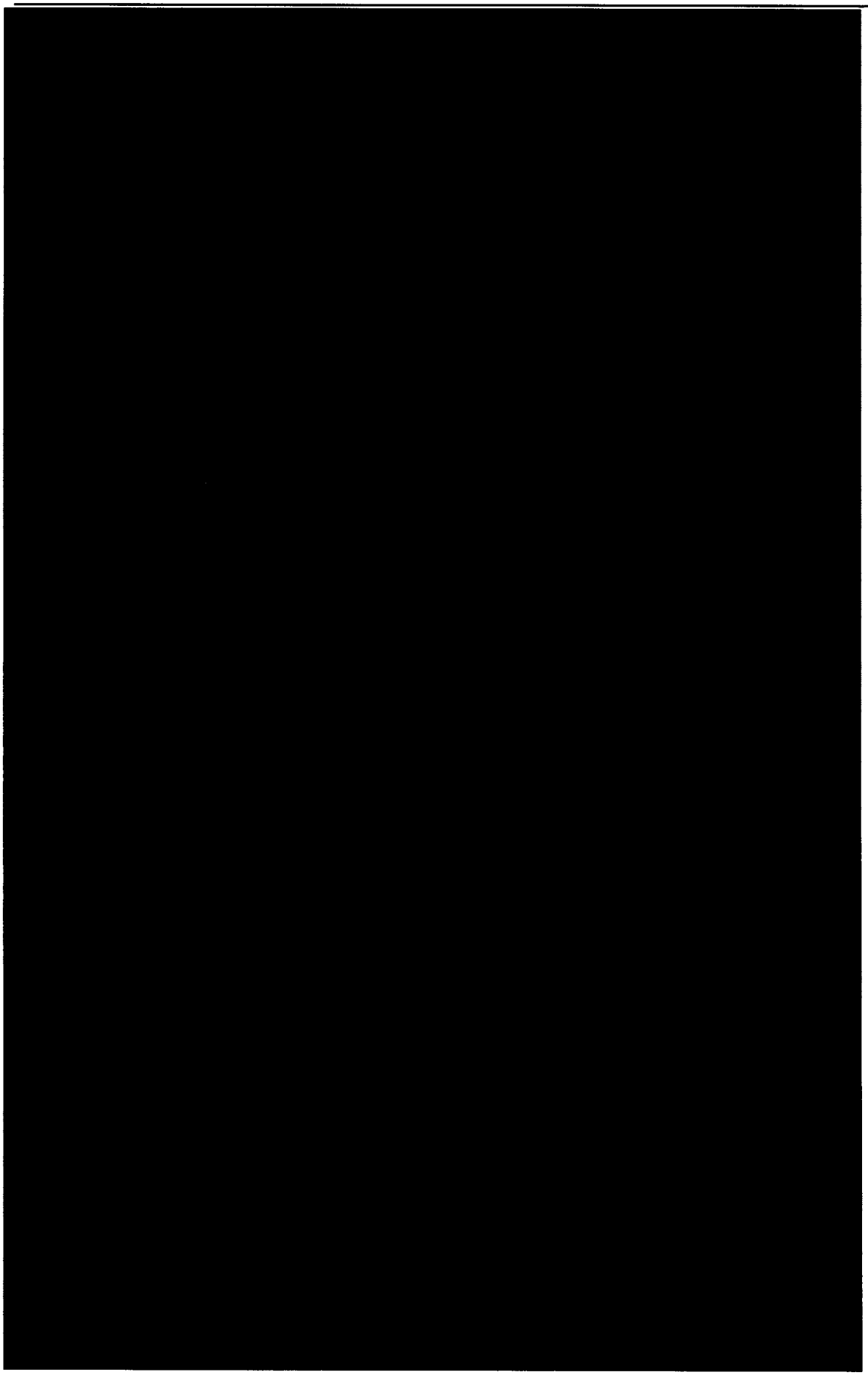
[redacted]

テナントID	日時	IPアドレス	ユーザーID	処理 :キャンペーンID:レポート名

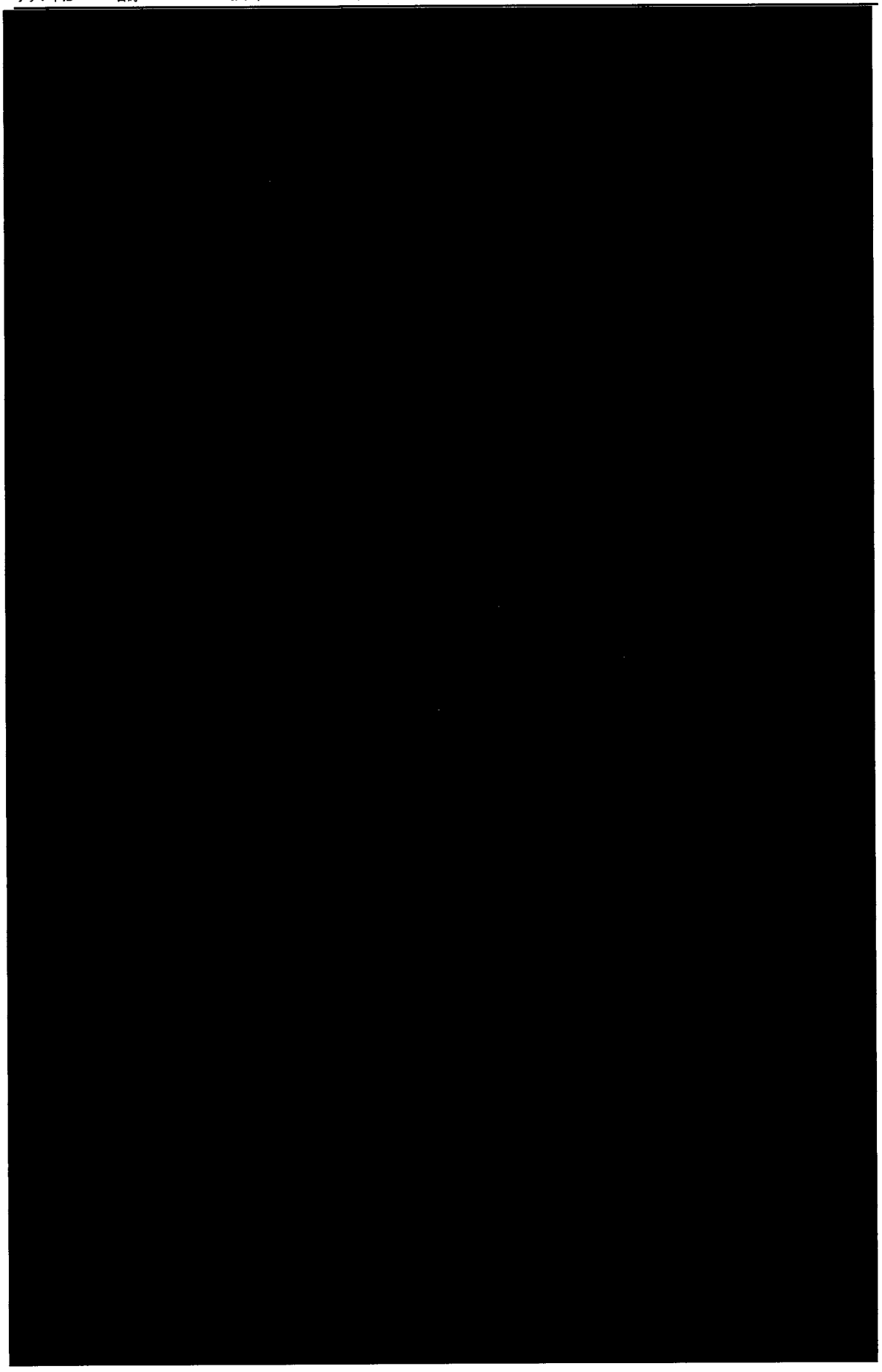
[redacted]

テナントID	日時	IPアドレス	ユーザーID	処理 :キャンペーンID:レポート名

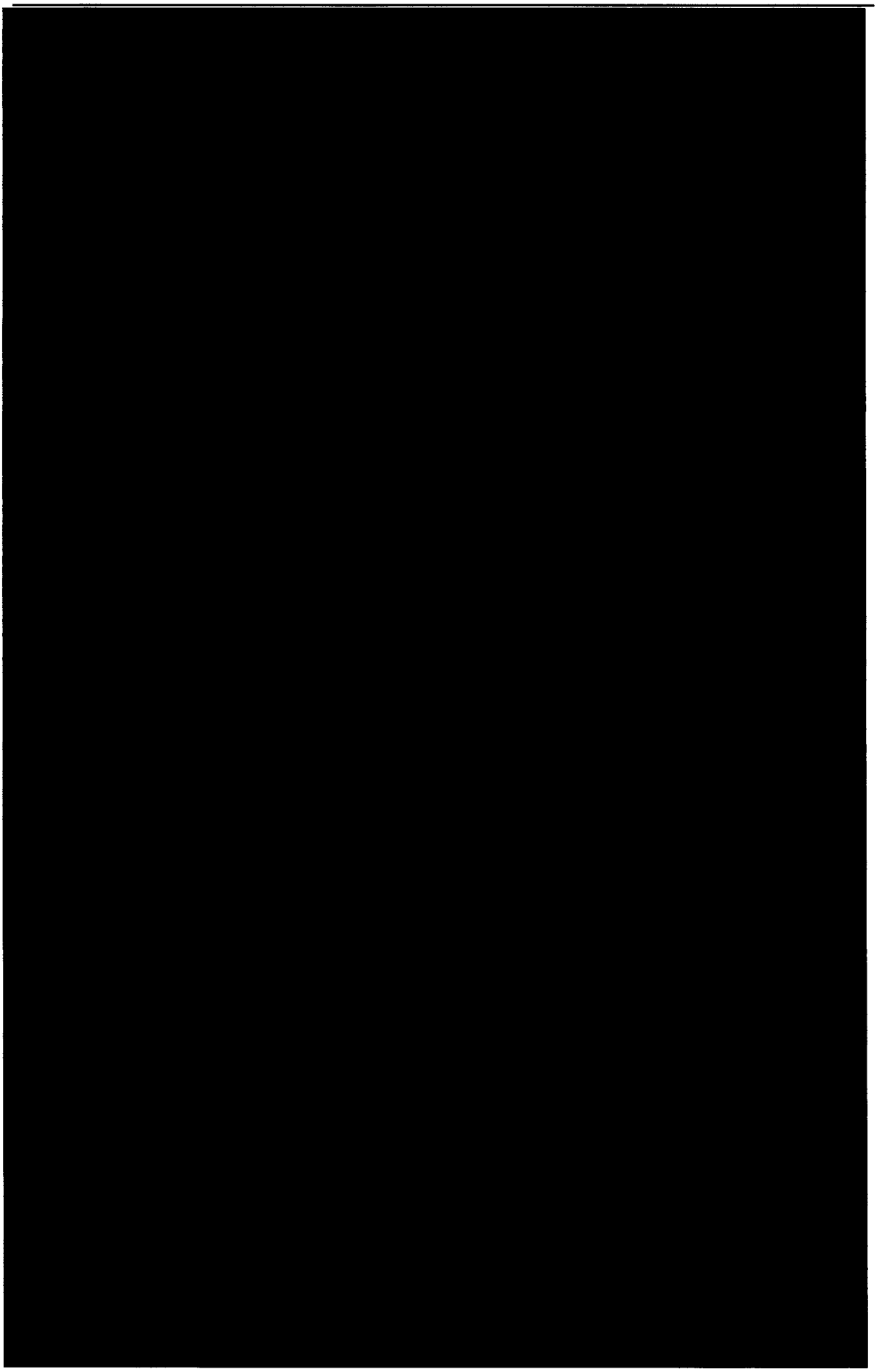
テナントID	日時	IPアドレス	ユーザーID	処理 :キャンペーンID:レポート名



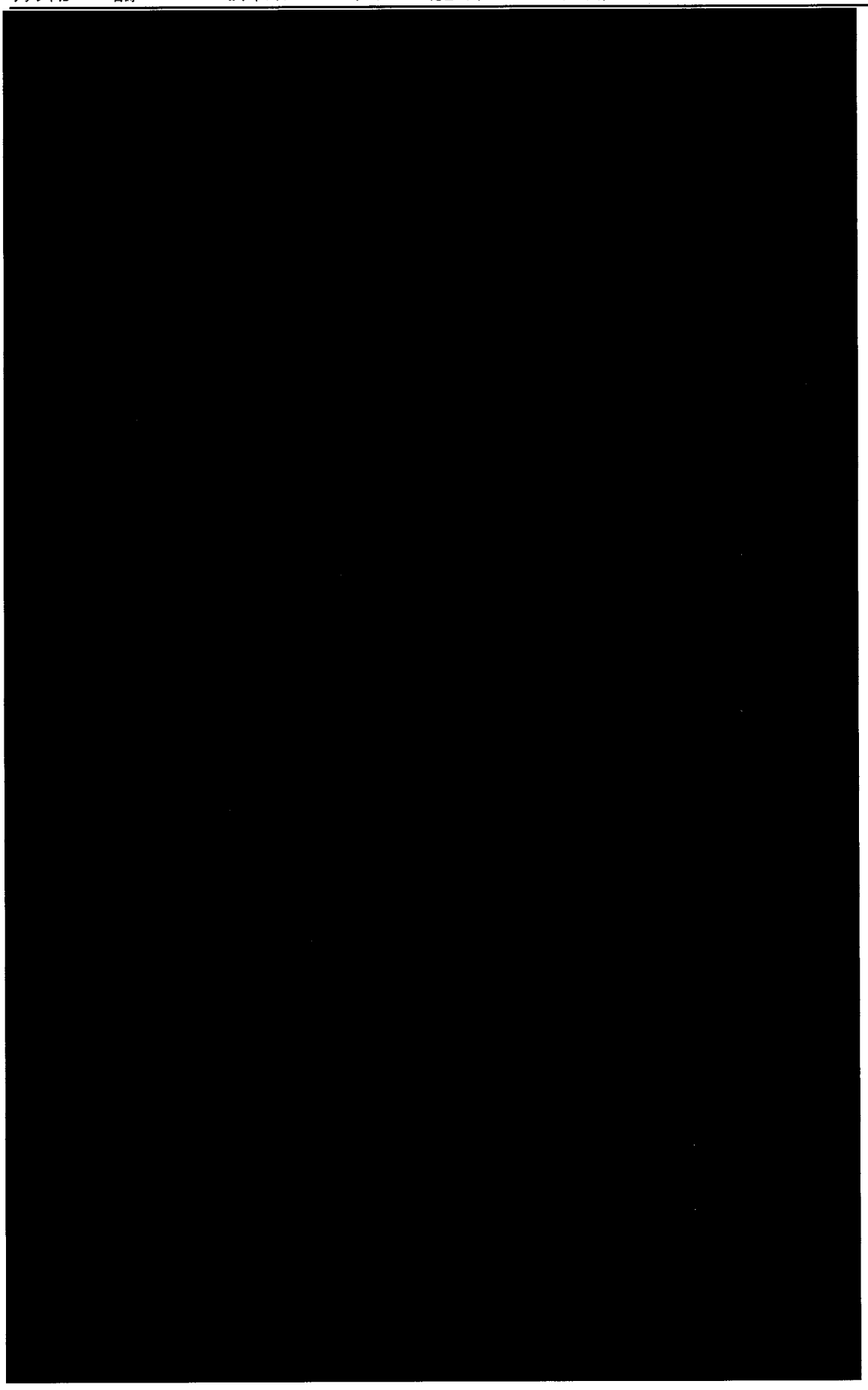
テナントID	日時	IPアドレス	ユーザーID	処理 :キャンペーンID:レポート名



テナントID	日時	IPアドレス	ユーザーID	処理:キャンペーンID:レポート名



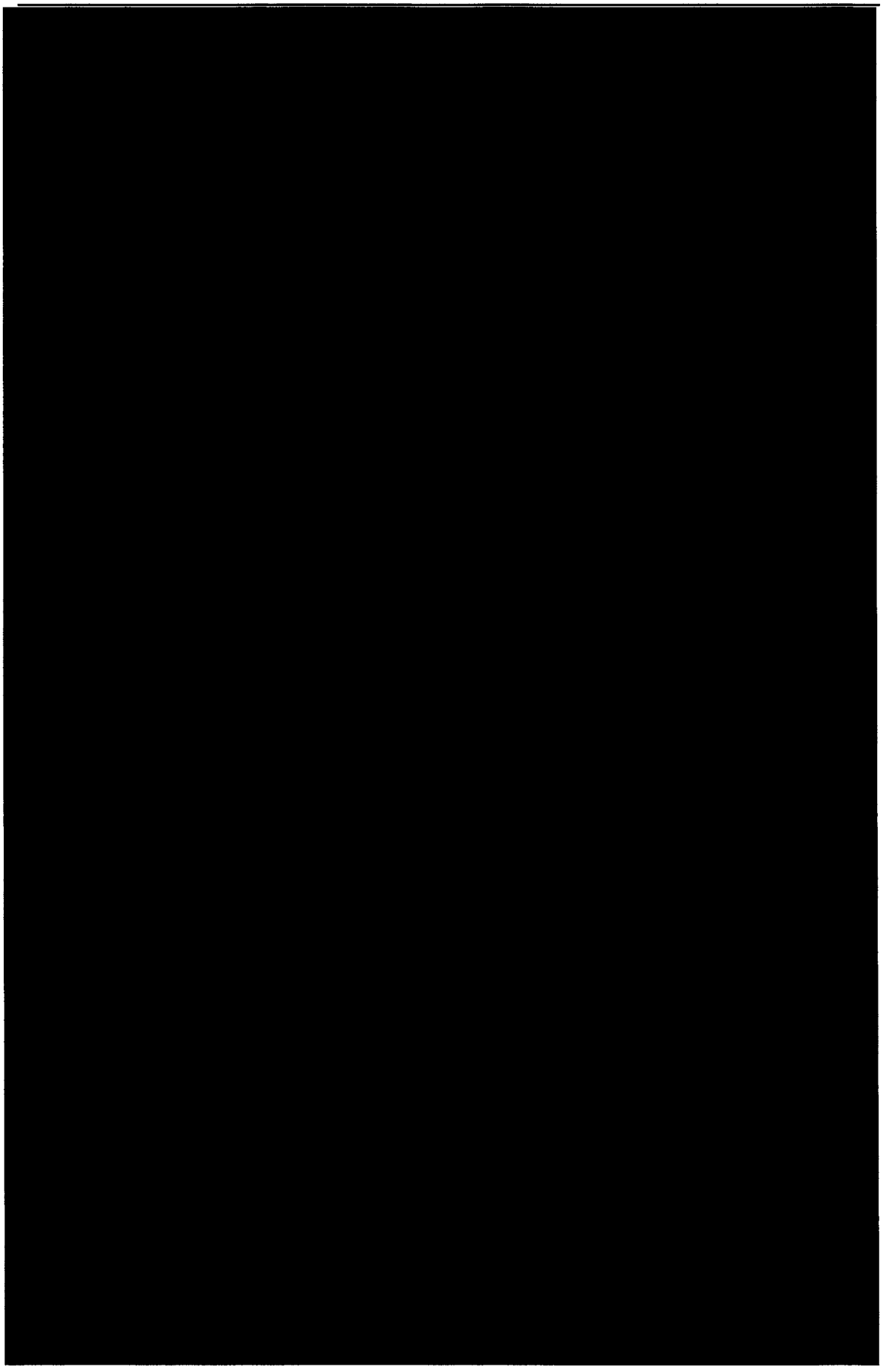
テナントID	日時	IPアドレス	ユーザーID	処理 :キャンペーンID:レポート名



テナントID	日時	IPアドレス	ユーザーID	処理 :キャンペーンID:レポート名
[redacted]				

テナントID	日時	IPアドレス	ユーザーID	処理 :キャンペーンID:レポート名
[redacted]				

テナントID	日時	IPアドレス	ユーザーID	処理 :キャンペーンID:レポート名



テナントID	日時	IPアドレス	ユーザーID	処理 :キャンペーンID:レポート名
[redacted]				

■ PDSサーバへのアクセスに関するご質問に関するご回答

別紙6-6　2022年7月1日　NTTマーケティングアクトProCX

No.	日付	内容	回答	回答日	別紙
11	6月24日	・ONE CONTACT NetworkのPDSサーバーのデータにアクセスできるシステム管理者は４名ということですが、前システムも含め2019/5～2022/6までの担当者の履歴を、担当されていた期間ごとに教えていただけますでしょうか。	該当期間におけるシステム管理者4名[redacted]）以外、他担当者はございません。（変更なし）	7月1日	－
		また各担当者が「現職」、「離職」なのかもお教えいただきたいです。	上記システム管理者4名については、現在在籍しておりますが、本担当からは外れております。		
12	6月24日	・前システムの切り替えは2020/8/1～2021/12/14までセンタ単位で段階的に実施⇒サーバー撤去は2022/2/21との回答を頂いておりますが、切替後～ サーバー撤去までの期間のアクセス履歴を確認させていただきたいです。	前回（6/1）No.2にてご回答させて頂きましたとおり、旧サーバのハードディスクは既にフォーマット化したため、ログは残っておりません。	7月1日	－
		自動で書き出しされるPDSサーバへのアクセスログ・操作ログ、OSのイベントログを PDSサーバーごとにいただけないでしょうか？			
13	6月24日	・システム切替時に前システムのバックアップファイルを移行されてましたが、ログに関しては現在でも残ってますでしょうか？	前回（6/1）No.7-③にてご回答させて頂きましたとおり、バックアップ保存期間は1週間となっておりますので、ログは残っておりません。	7月1日	－
		DB、ログともにtarで圧縮されているとのことですが、解凍方法についてお教えいただけますでしょうか？（パスワード、暗号化）	解凍方法については、圧縮コマンド同様、Linuxコマンド「tar」にて実施。尚、暗号化やパスワードの設定はしておりません。		
14	6月24日	・システム切替時の新旧サーバーからのエクスポートファイルの削除が証明できるものはありますでしょうか？	旧サーバに関しては、フォーマット化しているため、ファイル削除を証明できるものはございませんが、新サーバに関しては、該当ディレクトリーにファイルが存在していないことを確認しております。	7月1日	－
		また、移行後に旧サーバーのバックアップファイルの削除が証明できるものはありますでしょうか？PDSサーバーごとにお教えいただきたいです。	上記回答のとおり、旧サーバはフォーマット済みのため、ファイル削除を証明できるものはございません。		
15	6月24日	・前システムのハードディスクをフォーマットされた日時の記載がありませんでしたが、いつ実施されたかをPDSサーバー毎にお教えいただきたいです。	弊社の作業運用ルールにより、サーバ撤去日（2月21日）の1週間後に全サーバのハードディスクをフォーマット化しております。	7月1日	－
		またフォーマット前にバックアップを取得、保管されてないかと、フォーマット手順についてもお教えいただけないでしょうか？	復元する必要がないため、バックアップの取得も保管もしておりません。フォーマットは手順は以下のとおり ①[redacted] 起動 ②[redacted]を起動 ③論理ドライブを削除 ④0埋め方式を選択し消去		
16	6月24日	・前システムのサーバー撤去後から現在までは鍵付き書庫に保管されている、との回答をいただいておりますが、保管運用についてお教えいただきたいです。	各サーバ内に搭載されている全ハードディスクを取り外し・専用トレーに格納の上、鍵付き書庫にて保管しております。	7月1日	－
		誰でも鍵を開けて触れる状態にあったのか？鍵開けされた履歴が確認できるものはあるか？	鍵開けされた履歴を確認できるものはございませんが、上記のとおり、ハードディスクを取り外していること、又、ハードディスクは全てフォーマット化されていることもあり、復元することはできない状況としております。		
		撤去後はサーバーの電源を落としていると想定しておりますが、電源を入れられた形跡（システムログなど）が確認できますでしょうか？	物理的にハードディスクのみとなっているため、電源を投入できない形となっておりますので、システムログはございません。		
17	6月24日	・新サーバー移行後の弊社データの削除ログを確認させていただきたいです。No.4の移行対象データとその後にお渡ししたデータについて、各データごとに削除を実行した日時が分かる証跡をいただけないでしょうか？	前回（6/1）No.4-①にてご回答さえて頂きましたとおり、データ削除に関するシステムログの保存期間は1週間となっているため、ログは残っておりません。	7月1日	－

■ 2022年7月1日 お打合せ時に頂いた追加質問に関するご回答

別紙6-7　2022年7月15日 NTTマーケティングアクトProCX

No.	日付	内容	回答	回答日	別紙
18	7月1日	・該当期間におけるシステム管理者4名[redacted]）の方における、在職期間をそれぞれ教えて頂けますでしょうか？	システム管理者4名における在職期間は以下のとおりです。 [redacted]：2017年 7月 ～ 2022年6月末 ：2008年10月 ～ 2022年6月末 ：2008年12月 ～ 2022年6月末 ：2017年 4月 ～ 2022年6月末	7月15日	－
19	7月1日	・ハードディスクのフォーマット化に関しては、上記システム管理者4名以外に2名と伺いましたが、お名前と在職期間をそれぞれ教えて頂けますでしょうか？	フォーマット作業者2名の担当者名、在籍期間は以下のとおりです。 [redacted]：2019年 7月 ～ 現職 ：2017年11月 ～ 現職	7月15日	－
20	7月1日	・システム切替時のエクスポートファイルの削除について、作業手順書のようなものにて日付等を確認できるものがありますか？	本作業においては、切替後の後工程となるため、作業メンバー・日付等が確認できる作業手順書は残しておりません。 但し、本作業においては、社内にて作成したマニュアルを参照の上、実施しております。	7月15日	－
21	7月1日	・システムのDBにおけるOSは何になりますか？	[redacted]となります。	7月15日	－
22	7月1日	・ベンダはオンサイトにて支援頂いているとのことですが、何か証明できるものはありますでしょうか？	当社[redacted]ビルへの入退室管理簿より、ベンダの入室日を確認しております（別紙9） 但し、社内規程上、入退室管理簿における記載日については、保存期間の2年としております。	7月15日	別紙9
23	7月1日	・ONE CONTACT Networkにおける外部からの侵入経路について教えてください。例えば、FW等が設置されていると思いますが、アクセスログ等はありますでしょうか？	外部とは[redacted]社の接続サービスを利用しており、通信はVPN接続と内部から外部への必要通信しか許可していません。 又、FWでのアクセスログは取得しておらず、外部からの不正アクセス等は[redacted]社で監視していますが、セキュリティ対策の観点から公開しておりません。 尚、セキュリティ診断による社内審査を受けております。	7月15日	－
24	7月1日	・前回エクスポート頂いたログ、他撤去されたディスク等について、現地にて確認させて頂くことは可能でしょうか？	前回ご回答させて頂いておりますとおり、高セキュリティエリア・ルームへの入室については、当社の社屋等規定ルール及び他ユーザの機密情報が含まれておりますので、ご遠慮いただきたくお願いします。但し、[redacted]ビルの別室（会議室等）にて現物確認を行っていただく もしくは、ディスク等をご送付させて頂くことは可能です。	7月15日	－
25	7月1日	・データ削除ログは1週間とのことですが、直近センタにて削除されたものでも構いませんので、ログはありますでしょうか？	直近1週間分（2022年6月27日～7月3日）のキャンペーン削除ログをご提示します。	7月15日	別紙10

■ PDSサーバへのアクセスに関するご質問に関するご回答

7/1ご提出資料

2022年7月1日
NTTマーケティングアクトProCX

No.	日付	内容	回答	回答日	別紙
11	6月24日	・ONE CONTACT NetworkのPDSサーバーのデータにアクセスできるシステム管理者は４名ということですが、前システムも含め2019/5～2022/6までの担当者の履歴を、担当されていた期間ごとに教えていただけますでしょうか。	該当期間におけるシステム管理者4名[redacted]）以外、他担当者はございません。（変更なし）	7月1日	－
		また各担当者が「現職」、「離職」なのかもお教えいただきたいです。	上記システム管理者4名については、現在在籍しておりますが、本担当からは外れております。		
12	6月24日	・前システムの切り替えは2020/8/1～2021/12/14までセンタ単位で段階的に実施⇒サーバー撤去は2022/2/21との回答を頂いておりますが、切替後～ サーバー撤去までの期間のアクセス履歴を確認させていただきたいです。	前回（6/1）No.2にてご回答させて頂きましたとおり、旧サーバのハードディスクは既にフォーマット化したため、ログは残っておりません。	7月1日	－
		自動で書き出しされるPDSサーバへのアクセスログ・操作ログ、OSのイベントログを PDSサーバーごとにいただけないでしょうか？			
13	6月24日	・システム切替時に前システムのバックアップファイルを移行されてましたが、ログに関しては現在でも残ってますでしょうか？	前回（6/1）No.7-③にてご回答させて頂きましたとおり、バックアップ保存期間は1週間となっておりますので、ログは残っておりません。	7月1日	－
		DB、ログともにtarで圧縮されているとのことですが、解凍方法についてお教えいただけますでしょうか？（パスワード、暗号化）	解凍方法については、圧縮コマンド同様、Linuxコマンド「tar」にて実施。尚、暗号化やパスワードの設定はしておりません。		
14	6月24日	・システム切替時の新旧サーバーからのエクスポートファイルの削除が証明できるものはありますでしょうか？	旧サーバに関しては、フォーマット化しているため、ファイル削除を証明できるものはございませんが、新サーバに関しては、該当ディレクトリーにファイルが存在していないことを確認しております。	7月1日	－
		また、移行後に旧サーバーのバックアップファイルの削除が証明できるものはありますでしょうか？PDSサーバーごとにお教えいただきたいです。	上記回答のとおり、旧サーバはフォーマット済みのため、ファイル削除を証明できるものはございません。		
15	6月24日	・前システムのハードディスクをフォーマットされた日時の記載がありませんでしたが、いつ実施されたかをPDSサーバー毎にお教えいただきたいです。	弊社の作業運用ルールにより、サーバ撤去日（2月21日）の1週間後に全サーバのハードディスクをフォーマット化しております。	7月1日	－
		またフォーマット前にバックアップを取得、保管されてないかと、フォーマット手順についてもお教えいただけないでしょうか？	復元する必要がないため、バックアップの取得も保管もしておりません。フォーマットは手順は以下のとおり ①[redacted]起動 ②[redacted]を起動 ③論理ドライブを削除 ④0埋め方式を選択し消去		
16	6月24日	・前システムのサーバー撤去後から現在までは鍵付き書庫に保管されている、との回答をいただいておりますが、保管運用についてお教えいただきたいです。	各サーバ内に搭載されている全ハードディスクを取り外し・専用トレーに格納の上、鍵付き書庫にて保管しております。	7月1日	－
		誰でも鍵を開けて触れる状態にあったのか？鍵開けされた履歴が確認できるものはあるか？	鍵開けされた履歴を確認できるものはございませんが、上記のとおり、ハードディスクを取り外していること、又、ハードディスクは全てフォーマット化されていることもあり、復元することはできない状況としております。		
		撤去後はサーバーの電源を落としていると想定しておりますが、電源を入れられた形跡（システムログなど）が確認できますでしょうか？	物理的にハードディスクのみとなっているため、電源を投入できない形となっておりますので、システムログはございません。		
17	6月24日	・新サーバー移行後の弊社データの削除ログを確認させていただきたいです。No.4の移行対象データとその後にお渡ししたデータについて、各データごとに削除を実行した日時が分かる証跡をいただけないでしょうか？	前回（6/1）No.4-①にてご回答さえて頂きましたとおり、データ削除に関するシステムログの保存期間は1週間となっているため、ログは残っておりません。	7月1日	－

■ PDSサーバへのアクセスに関するご質問に関するご回答

6/1ご提出資料

2022年6月1日
NTTマーケティングアクトProCX

No.	日付	内容	回答	回答日	別紙
1	4月28日	ONE CONTACT NetworkのPDSサーバーのデータにアクセスできるシステム管理者の範囲（内部／外部、役職など）と人数、対象者氏名	■ISMS管理責任者5名 及び システム保守者4名となります。又、PDSサーバのデータにアクセスできる作業者はシステム管理者の4名。 [redacted]	5月11日	－
2	4月28日	前システムのセキュリティポリシー（20220421セキュリティ確認ご報告資料.pdfの１ページ目に相当する内容）と前システム機器廃棄時のデータの取り扱い内容	■前システム同様、ONE CONTACT Networkのセキュリティポリシーにつきましても、前回ご報告させて頂きました資料（20220421セキュリティ確認ご報告資料.pdfの１ページ目）と同じになりますが、システムメンテナンス等における保守用端末の取り扱いについては、別紙1(2ページ)のとおり。 尚、前システム（PDSサーバ等）については、NTTフィールドテクノ社のデータ消去サービスを行った上、産業廃棄処分[redacted]を実施しております。	5月11日	有 （別紙1）
3	4月28日	ONE CONTACTNetwork環境および前システム環境における、ネットワーク外へのデータ取り出し方法と、データ取り出し出来るシステム管理者の範囲と人数、対象者の氏名	■NO.2関連、ONE CONTACT Network環境及び前システム環境も、各センタからのアクセス経路においては、ネットワークの構造とテナント規制により、ネットワーク外への一括データ出力は不可となっております。但し、各センタからの問合せ（トラブル対応、画面修正、疑似試験等）があった場合のみ、弊社[redacted]に設置している保守用端末(※)より、システム管理者（2名以上:担当課長＋担当者）にて、[redacted]キャンペーン構成・画面エラーチェック、動作試験等を実施することがありますが、データ出力したか否かの痕跡を調査した結果、別紙2のとおり、当社テスト用キャンペーンの出力結果しかございませんでした。尚、システム管理者の範囲と人数、対象者はNO.1に記載のとおり。 (※) USBポート無し、秘文ソフトウェアがインストールされた専用端末	5月11日	有 （別紙2）
4	4月28日	ネットワーク外へのデータ取り出し時の管理	■各センタにて特定USBメモリの使用、特定USBメモリの保管書庫の鍵管理、お客様情報の授受、削除管理を管理簿にて管理しています。作業実施者と確認者で確認する運営としています。 ① 特定USBメモリの使用管理 ・・・電子記録媒体使用管理簿 ② 特定USBメモリ保管書庫の鍵管理 ・・・鍵管理簿 ③ お客様情報の授受、削除管理 ・・・お客様データ授受・削除管理簿	5月11日	－
5	4月28日	パスワード管理ポリシー（必要な文字数、英文字・数字・記号などの条件）と更新頻度、更新実施者、取扱いルールについて	■システム管理上、パスワードの更新頻度は[redacted]	5月11日	－
6	4月28日	ONE CONTACT Networkへのシステム切り替えタイミングと、前システム（AQStage)からの移行時の切り替え手順（移行計画）書	■ONE CONTACT Networkへの切替日は以下のとおり各センタ単位で五月雨となっております。 第一回（岡山、福岡） 2020年 8月 1日 第二回（名古屋） 2020年12月11日 第三回（広島、高蔵寺）2021年 4月27日 第四回（熊本） 2021年 5月27日 第五回（豊橋） 2021年 7月30日 第六回（北九州） 2021年12月14日 ＃切替手順書（福岡）は、別3のとおり	5月11日	有 （別紙3）
7	4月28日	アウトバウンド業務終了後のデータ削除処理方法と実施ログの例（手動で削除の場合は、削除コマンドやＳＱＬ文、プログラム削除の場合は、処理仕様書やプログラムソースなど具体的な処理内容が分かるもの）	■アウトバウンド業務終了後のデータ削除については、システムに予め用意されているキャンペーンの削除機能にて実施いたします。 ＃キャンペーン削除のサンプル画面は別紙4のとおり	5月11日	有 （別紙4）
8	4月28日	ONE CONTACT Networkと前システム（AQStage)の画面ハードコピー（弊社業務）を頂けますか。	前システム同様、ONE CONTACT NetworkもPDS画面そのものは同じものとなります。 ＃御社業務用のサンプル画面（福岡）は別紙5のとおり	5月11日	有 （別紙5）

■ PDSサーバへのアクセスに関するご質問に関するご回答

6/1ご提出資料

2022年6月1日
NTTマーケティングアクトProCX

No.	日付	内容	回答	回答日	別紙
9	5月23日	ONE CONTACT NetworkのPDSサーバーのデータにアクセスできるシステム管理者の体制変更	■4/28回答のNo.1記載の体制につきまして、システム保守者（システム管理者）4名について、以下のとおり体制見直しを図りました。 [redacted]	6月1日	－
10	5月23日	PDSサーバにおけるシステム管理ログ（顧客データダウンロード含む）の編集可否について	■PDSサーバへのアクセスログ・操作ログ等については、PDSサーバ本体へファイルとして自動で書出しされる仕組みとなっており、システム保守者は勿論、開発サイドでも編集することができない仕様となっております。	6月1日	－

■ PDSサーバへのアクセスに関するご質問に関するご回答

6/1ご提出資料

2022年6月1日
NTTマーケティングアクトProCX

No.	日付	内容	回答	回答日	別紙
1	5月24日	①お名前がある方の所属会社名を教えて下さい。	■NTTビジネスソリューションズ株式会社 バリューデザイン部 [redacted] より、以下6名となります。 [redacted] ■株式会社NTTマーケティングアクトProCX カスタマーソリューション事業推進部 [redacted] より、以下3名となります。 [redacted]	6月1日	－
		②ISMS管理責任者は、PDSサーバーのデータへのアクセスは可能でしょうか？（可能な場合、全拠点分か自拠点分のみかも合わせてお願いします）	■アクセス不可となります。 ■ISMS管理責任者等は、あくまでも情報マネジメントシステムにおける認証グループ全体の統括・統制する役割であり、システムへのログイン権限は持ち合わせておりません。	6月1日	－
2	5月24日	①前システムは現システムと全く同じ（"PDSサーバー"がエリア毎に分かれていた）構成でしょうか？	■同じ構成となります。エリア毎にサーバを物理的に４台分離した構成としております。（2022年4月21日ご提出資料のとおり【別紙1】）	6月1日	－
		②データ削除（NTTフィールドテクノ社）や廃棄[redacted]についての実施証明は取られていますでしょうか？	■前回（4月28日 No2.回答）"前システム（PDS）はデータ削除や産業廃棄処分を実施しております"とご回答させて頂きましたが、"データ削除や廃棄処分は未だ実施しておらず"、弊社情報伝達の不手際により誤ったご回答をしてしまい、申し訳ございません。 又、未実施の理由につきましては、他物品との兼ね合いもあり、固定資産（サーバ類等）の除却は弊社として2022年.7月実施するルールとしておりました。 尚、"前システム（PDS）"のハードディスクは全てフォーマット化の上、データがないことを確認しており、弊社[redacted]ビルの鍵付き書庫に保管してあります。 補足）データ削除（NTTフィールドテクノ）及び 産業廃棄[redacted]に関する両社への申請手配は既に完了しておりますので、実施予定である2022.7月以降は実施証明書をご提出することは可能です。	6月1日	－
		③システム切り替え（最終のみで結構です）、サーバー撤去、データ消去、サーバー廃棄がそれぞれ何月何日に実施されたか教えて下さい。	■サーバ撤去日につきましては、2月21日となります。 ■データ消去 及び サーバ廃棄に関しては、No.2-②の示すとおり、2022.7月実施予定。	6月1日	－
3	5月24日	①保守端末からログインの実績については、実施記録とログの突合せにより誰がいつログインしたかの証明が可能な状態でしょうか？	■保守端末においては、貴社以外のユーザ含めた緊急故障対応 及び 緊急設定依頼等を作業者が迅速 且つ 早期復旧させる必要があることからも、実施記録簿はつけておりません。 但し、作業については必ず管理者含む2名体制にてクロスチェックし実施するようにしております。	6月1日	－
		⇒現地希望確認（実施記録とログの突合せ確認）	■NTTビジネスソリューションズにて定めた社屋等規程ルール＜第6条＞により、高セキュリティエリアにおいては、貴社以外から頂いた様々な機密情報、設備等をお預かりしているエリアには、許可された者（契約業者、社員）だけが入室できるエリアとしている為、現地確認は見合わせて頂きたく、お願い申し上げます。 但し、こちらから開示できる資料、ログ出力情報等につきましてはご協力させていただきます。	6月1日	－
		②別紙２のログについて、前システムのログは御座いますか？また、フィルターが掛けられていると思われるのでどのような内容でフィルターが掛かった状態でしょうか？	■前システムログ（ONE CONTACT Network移行前）は別紙6参照。 ■フィルターについては、新システム（ONE CONTACT Network）への移行分のみをサンプル抽出したこと、又、管理者用ID [redacted]を含むID）のみに絞らせて頂きました。	6月1日	別紙6
		③同一PDSサーバー上の別の拠点のデータへのアクセス制限は、ID/Passの制御によるものでしょうか？	■ご認識のとおりです。[redacted]	6月1日	－
		④別のPDSサーバー上の別の拠点のデータへのアクセス制限は、ネットワーク設定によるものでしょうか？	■ご認識のとおりです。[redacted]	6月1日	－
4	5月24日	①ご回答に記載の①～③の管理簿の内容を証明するシステムのログは御座いますでしょうか？	■①～③の管理簿のうち、①USBメモリの使用管理、②USBメモリの保管倉庫の鍵管理におけるシステムログはございません。③ お客様情報の授受、削除管理『お客様データ授受・削除管理簿』に記載のデータインポート、データ削除を確認できるシステムログがございます。 尚、システムログ（データインポート、エクスポート）は永年保存、センタ端末にて確認できます。但し、システムログ（データ削除に関して）は1週間保存となりサーバ本体での確認となります。	6月1日	－
		⇒現地希望確認（実施記録とログの突合せ確認）	■No.3-①ご回答のとおり、[redacted]での現地確認は、見合わせて頂きたくお願い申し上げます。但し、こちらから開示できる資料、ログ出力情報等につきましてはご協力させていただきます。 又、③ お客様情報の授受、削除管理『お客様データ授受・削除管理簿』については、各センタで保存しているものをご提出することが可能です。	6月1日	－
		②このご回答にある"削除管理"とは、システムからのデータ削除のことでしょうか？またはシステム外に取り出したデータの削除の事でしょうか？	■システム画面上、PCローカルフォルダ、USBメモリ内のデータ削除を目視確認しています。	6月1日	－
		③システム外に取り出したデータを削除する際は、完全削除（"ごみ箱"から削除）することがルール化されていますでしょうか？	■はい、データ削除は貴社によるセキュリティ監査をの確認内容を踏まえまして、完全削除（ゴミ箱内の削除）をする運用ルールとしております。	6月1日	－

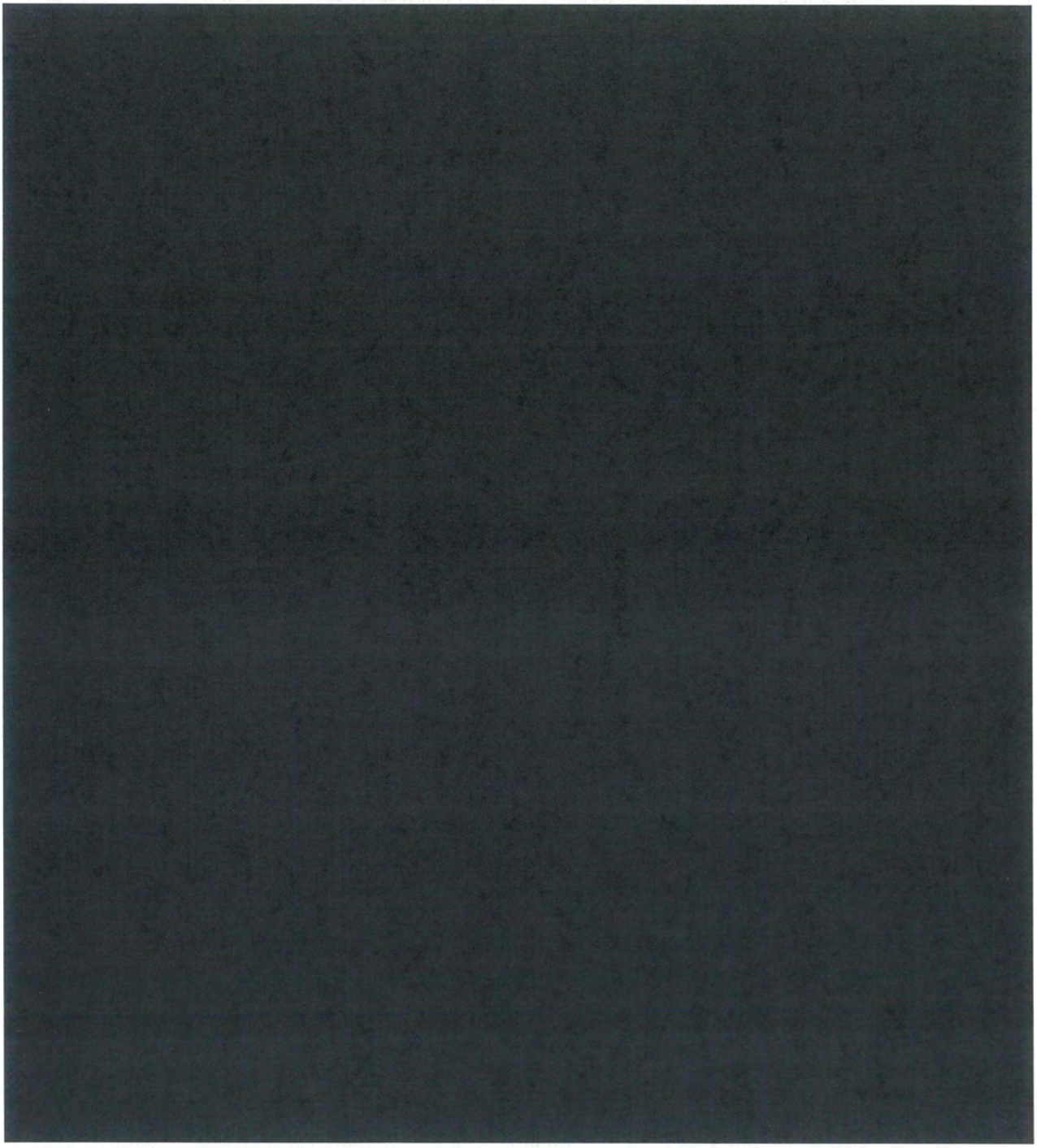
■ PDSサーバへのアクセスに関するご質問に関するご回答

6/1ご提出資料

2022年6月1日
NTTマーケティングアクトProCX

No.	日付	内容	回答	回答日	別紙
5	5月24日	①パスワードの文字数制限に"0～12文字以内"とありますが、パスワード無しも可でしょうか？	■無しも可能です。但し、運用ルールとして、必ずパスワードを常に設定するよう実施しております。	6月1日	－
		⇒現地希望確認（実施記録とログの突合せ確認）	■No.3-①ご回答のとおり、[redacted]での現地確認は、見合わせて頂きたくお願い申し上げます。 ■パスワード更新タイミングを見計らい、センタ側での変更手順と[redacted]側にて出力したシステムログを突合し確認することは可能です。但し、システムログ（パスワード変更に関しては）は1週間となっております。	6月1日	－
6	5月24日	①データ移行作業に実施もしくは立ち会われた方は、手順書にお名前のあるお二方のみでしょうか？	■二名以外に作業責任者である[redacted]の立ち合いのもと実施しております。	6月1日	－
7	5月24日	①旧PDS1の手順書「3. テナントエクスポート」でエクスポートされたファイルはどのタイミングで新旧サーバーから削除されましたでしょうか？	■新サーバへ移行したエクスポートファイルについては、弊社の作業運用ルールにより、切替日1週間後に削除しております。 又、旧サーバのエクスポートファイル（原本）は、No.2-②ご回答のとおり、フォーマットしております。 補足）No.2-②ご回答のとおり、2022.7月にてデータ消去及びサーバ廃棄を行います。	6月1日	－
		②旧および新サーバー上で「テナントエクスポート」されたファイルの削除や操作の記録（ログ）は確認可能でしょうか？	■新サーバへ移行したエクスポートファイルの削除に関しては手順書(サンプル)になりますが、ご確認いただくことは可能です。 又、旧サーバに関しては、No.2-②ご回答のとおり、フォーマットのみ実施した形式となります。	6月1日	－
		⇒現地希望確認（実施記録とログの突合せ確認）	■No.3-①ご回答のとおり、[redacted]での現地確認は、見合わせて頂きたくお願い申し上げます。但し、手順書（タイムスタンプ有り）をご提出することは可能です。	6月1日	－
		③新PDS1の手順書「1. エクスポートファイルをコピー」のバックアップファイルの内容（バックアップのサイクル、対象、形式など）を教えて下さい。	■手動バックアップファイルにおける内容については以下のとおり a. サイクル：日次（夜間） b. 対象　：DBデータおよびログファイル c. 形式　：DBデータはダンプ出力し tar に圧縮 　　ログファイルは tar に圧縮 d. 保存期間：　DBは1週間。	6月1日	－
		⇒現地希望確認（実施記録とログの突合せ確認）	■No.3-①ご回答のとおり、[redacted]での現地確認は、見合わせて頂きたくお願い申し上げます。 ■実施記録については、2022年5月11日ご提出資料【別紙3】作業手順書シートにタイムスタンプを記載しておりますが、手動にてバックアップしたファイルは上記保存期間に示すとおり、1週間しか保存されていないため、突合することが困難な状況です。	6月1日	－
8	5月24日	①弊社データを取り込んだ時に作成されるデータについて下記の教えて下さい。	■テーブル命名規則 [redacted]	6月1日	－
		⇒テーブルの命名規則、名前の付け方（自動or手動）、キャンペーンIDとテーブル名の関係、削除アプリのキャンペーンIDと削除対象テーブル判断の仕様	■キャンペーンIDとテーブル名の関係は[redacted] ■削除アプリは[redacted]検索して削除を実行します。 ■削除対象テーブル判断の仕様 [redacted]		
		②実際の運用でデータ削除をした際の処理結果のログを確認させて下さい。	■実運用データの削除は、キャンペーン終了後でしか実行できないこと。又、前回ご提出させて頂きました【別紙4】アウトバウンド業務終了後のデータ削除方法と実施ログの例に記載しております、削除後のログ確認はシステム側にて開発ツールを用いて実行するため、キャンペーン終了後のタイミングに合わせ、削除ログを取得しご提出となります	6月1日	－
		⇒現地希望確認（実施記録とログの突合せ確認）	■No.4-①ご回答のとおり システムログに関しては、データ削除は1週間分のみご提出することは可能です。 又、お客様データ授受・削除管理簿については、各センタで保存しているものをご提出することが可能です。	6月1日	－
9	5月24日	①（別紙5 ■ アウトバウンド 業務画面のサンプルデータ）で実際の当社のデータが入った画面を確認させて下さい。	■業務画面につきましては、各センタにて業務実施移管内でご確認いただくことが可能です。	6月1日	－
		⇒現地希望確認（実施記録とログの突合せ確認）			－

2022年6月27日～2022年7月3日の間に削除されたキャンペーン



ベンダ入室日付

日付	氏名	目的	入室時間	退室時間
2020/6/18	[redacted]			
2020/6/19				
2020/6/20				
2020/6/21				
2020/6/22				
2020/6/23				
2020/6/24				
2020/6/25				
2020/6/26				
2020/6/29				
2020/6/30				
2020/7/1				
2020/7/2				
2020/7/3				
2020/7/17				
2020/7/31				
2020/11/4				
2020/11/11				
2020/11/25				
2020/12/10				
2020/12/13				
2021/2/19				
2021/4/19				
2021/4/26				
2021/4/28				
2021/5/17				
2021/5/26				
2021/5/29				
2021/5/30				
2021/5/31				
2021/6/15				
2021/6/24				
2021/7/19				
2021/7/29				
2021/8/20				
2021/8/23				
2021/8/31				
2021/9/14				
2021/9/27				
2021/12/1				
2021/12/13				

NTT 西日本が定めるエスカレーションマニュアル

① NTT 西日本グループビジネスリスクマネジメントマニュアル

NTT 西日本は、「NTT 西日本グループビジネスリスクマネジメントマニュアル」(「リスクマネジメントマニュアル」) を制定しているところ、本件過去調査当時の同マニュアル (2021 年 7 月改定版) では、「情報セキュリティ事故 (お客様情報漏洩)」が企業内部リスクの一番目の事項に位置づけられ、ビジネスリスクマネジメントの徹底として「事前に特定したリスクは芽のうちに摘み取り、問題を深刻化・長期化させない。」「経営トップが『知らないまま』『その後の報告を受けないまま』に、問題を取り返しのつかない事態にさせない。」と規定されている。そして、リスクマネジメントマニュアルは、NTT 西日本グループ全社の全役職員を対象に、「リスク発生時の迅速な対応」等を適切に実施する観点から NTT 西日本グループ全組織との間で連絡体制を整備するとともに、緊急情報連絡の徹底を図っており、緊急情報連絡については、同マニュアルによって整備・確立された緊急情報連絡体制により、NTT 西日本に対するエスカレーションを迅速に実施すべき旨を定めている。ここでは、お客様情報・会社情報等の漏洩も緊急情報連絡により連絡されるべき事項として挙げられており、主管室部は情報セキュリティ推進部・技術革新部・相互接続推進部と定められている。

② 情報漏洩事案発生時における初動対応マニュアル

NTT 西日本情報セキュリティ推進部は、リスクマネジメントマニュアルを補足するものとして、「情報漏えい事案発生時における初動対応マニュアル (4 版)」(2022 年 4 月制定) (「情報漏えい初動対応マニュアル」) を定めており、BS は同マニュアルの対象組織に含まれている。

情報漏えい初動対応マニュアルは、対象組織における重要情報[1]の漏洩等の事案を適用範囲として、当該事案発生時の①初動対応の明確化、②連絡フローの整理を目的としている。

特に、①初動対応の明確化としては、第一に、事案検知の場面において、発生元組織の管理者が情報漏洩事案を検知した場合、想定される被害の規模や対応を上長へ報告すべきものとされており、具体的には、(1) 事案状況・被害状況の把握、(2) 事案対応が完了するまでの一連の対応等の記録・管理、(3) 総務人事部の規定するリスクマネジメントマニュアルに則った、NTT 西日本総務人事部総務・渉外担当、関連部及び、情報セキュリティ推進部等に対する緊急情報連絡票による報告 (初報) を行うべきものとされている。そして、第二に、事案検知後の初動対応として、(1) 事案管理体制の確立、(2) お客様等への対応、(3) 拡大防止のための対応策、(4) 詳細な情報集を行うべき

[1] 「お客様情報等、最も厳重な管理が必要な情報であり、漏えい等 (漏えい、滅失、毀損) により会社及び株主、取引先、社員等に深刻かつ重大な影響が想定される情報」と定義される。

旨が規定されている。

BS の関連規程

BS は、本件過去調査当時、「お客様情報及びお客様特定個人情報等保護管理規則」（2022 年 4 月 1 日制定）（「BS 個人情報保護管理規則」）及び「お客様情報及びお客様特定個人情報等保護管理規則細則」（「BS 個人情報保護管理規則細則」）（2022 年 4 月 1 日制定）を定めていたところ、これらの規程には、お客様情報の漏洩等に関し、次の規定が存在する。

【BS 個人情報保護管理規則】

（お客様情報の漏えい等が発生した場合の対応）

第 28 条

お客様情報の漏えい、滅失又はき損（以下これらを「漏えい等」という。）が発生した場合は、直ちに情報管理責任者及び細則に定める者に報告するとともに、二次被害の防止、類似事案の発生回避等の観点から、再発防止策を策定し、また、可能な限り、当該漏えい等に係る事実関係等を公表するなどの適切な対処を行わなければならない。

2　お客様情報の漏えいが発生した場合であって、個人の権利利益を害するおそれが大きいものとして個人情報保護委員会規則で定めるものが生じたときは、個人情報保護委員会規則及び細則で定めるところにより、当該事態が生じた旨及び一定の事項を個人情報保護委員会又は総務省その他の行政機関に報告するとともに、本人に通知しなければならない。

【BS 個人情報保護管理規則細則】

１２　漏えい等が発生した場合の対応【本則第 28 条関連】

(1) お客様情報の漏えい等が発生した場合、当該漏えい等に係る事実関係を行政機関等に直ちに報告することが法律上の義務となっていることから、情報管理責任者は情報セキュリティ推進部及び本社関係部門（当該漏えい、滅失又はき損が発生したお客様情報の本社主管部門及び総務部法務部門）に対して、その事実関係を直ちに報告しなければならない。

なお、法律上報告の義務を要する「個人の権利利益を害するおそれが大きいもの」として個人情報保護委員会規則で定められた事態とは、具体的には次のとおり。

- 要配慮個人情報が含まれる個人データの漏えい等が発生し、又は発生した恐れがある事態
- 不正に利用されることにより財産的被害が生じるおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態
- 不正の目的をもって行われたおそれがある個人データの漏えい等が発生し、又は発生したおそれがある事態

・　個人データに係る本人の数が千人を超える漏えい等が発生し、又は発生したおそれがある事態

これらの事態に該当する場合であっても、漏えい等が発生し、又は発生したおそれがある個人データについて、高度な暗号化等の秘匿化がされている場合等、個人の権利利益を保護するために必要な措置が講じられている場合については報告を要しない。

(2) お客様情報の漏えい等が発生した場合は、個人情報の保護に関する法律その他の法令に従い、本人が適切に対応できるようにするため、速やかに、当該漏えいに係る事実関係を本人に通知しなければならない。ただし、本人への通知が困難な場合であって、本人の権利利益を保護するため必要なこれに代わるべき措置をとるときは、この限りでない。

(3) 個人データの取扱いを委託している場合においては、委託先が委託元に(1)に規定する事態が発生したことを通知した時は、委託先は報告義務を免除される。

(4) お客様情報の漏えい等が発生した場合の公表については、広報室等と連携の上実施するものとする。

このように、BS 個人情報保護管理規則細則 12（1）においては、一定の重大な個人情報の漏洩等について、実際に事案が発生した場合に加え、そのおそれが認められた場合をも適用範囲として想定し、情報管理責任者から情報セキュリティ推進部及び本社関係部門（当該漏洩、滅失又はき損が発生したお客様情報の本社主管部門及び総務部法務部門）に対する報告を求めている。

なお、本件過去調査当時、C 担当部長の上長である VD 部長（H 部長）が情報管理責任者を務めていた。

ProCX の関連規程

本件過去調査当時、ProCX は、「個人情報・特定個人情報保護安全確保対策規程」（2022 年 4 月 1 日制定）を定め、「(同社が) 所有している個人情報・特定個人情報について、漏えい、滅失、き損などが生じること」を「事故」と定義し、事故が発生した場合の対応手順等を定めていた。他方で、ProCX における他の規程類も含め、情報漏洩等のおそれが生じた時点における具体的な対応手順等を定めた規定は ProCX に存在しなかった。

BSにおける本件システム点検結果

○：対処済、×：ルール不適合、△：運用対処済、－：対象外

別紙7-1

カテゴリ		点検項目	2023/8/3点検		2023/10/23点検		2024/1/31点検	
持ち出し制御	1	（1は業務上USBメモリ利用がない場合の点検項目）会社が許可したUSBメモリ等以外を利用させない対策が取られているか	－	（該当なし）	－	（該当なし）	－	（該当なし）
	2	（2から6は業務上USBメモリ利用がある場合の点検項目）USBメモリ等を利用する場合は、会社支給の生体認証／暗号化等の対策が実施されたものを利用しているか	×	運用ルールとしては私有USBメモリ利用は禁止。遵守されていなかった	○	持ち出し可能端末を限定。会社管理の指紋認証付きUSBメモリとデータブリッジ以外持ち出し不可。該当端末は管理者のみログイン可能	○	持ち出し可能端末を限定。会社管理の指紋認証付きUSBメモリとデータブリッジ以外持ち出し不可。該当端末は管理者のみログイン可能
	3	会社が許可したUSBメモリ等以外を利用させない対策が取られているか	×	私有USBメモリも利用可能な状態	○		○	セキュリティ対策ソフトウェアにて制御
	4	会社が許可したUSBメモリ等を利用する場合、事前の承認を得て記録しているか	○	会社が許可したものを利用する場合は承認を得て記録していた	○	会社が許可したものを利用する場合は承認を得て記録していた	○	会社が許可したものを利用する場合は承認を得て記録していた
	5	端末へのUSBメモリ等の接続についてログを取得し定期的に確認しているか 又は第三者立会いによる操作内容の目視確認を実施しているか	×	USBメモリの利用ログは取得できていなかった	○	セキュリティ対策ソフトウェアにてログ取得しUSBメモリ接続時はリアルタイムで接続アラームメール発出	○	セキュリティ対策ソフトウェアにてログ取得しUSBメモリ接続時はリアルタイムで接続アラームメール発出
	6	USBメモリ等を別用途で再利用もしくは廃棄する場合は情報の復元が不可能な方法でデータ消去しているか	○	指定データ消去サービス利用（実績なし）	○	指定データ消去サービス利用（実績なし）	○	指定データ消去サービス利用（実績なし）
端末管理	7	端末のアカウント共用がないか	×	端末へのログインアカウントを共用	○	ディレクトリ・サービス・システムを導入し個人特定可能化	○	ディレクトリ・サービス・システムを導入し個人特定可能化
	8	マルウェア対策ソフトを導入しているか	○	アンチウイルスソフトウェア	○	アンチウイルスソフトウェア	○	アンチウイルスソフトウェア
	9	端末及びUSBメモリ等を施錠保管しているか	○	会社が許可USBメモリは施錠管理・保管	○	会社が許可USBメモリは施錠管理・保管	○	会社が許可USBメモリを施錠管理・保管
	10	端末及びUSBメモリ等を社外に持ち出す場合、承認を含めた持出管理をしているか	×	リモート保守用端末の持ち出し管理簿はあるが厳格な運用ができていない USBメモリの社外持ち出しは無し	○	リモート保守用端末の持ち出し管理の厳格化	○	リモート保守用端末の持ち出し管理の厳格化
	11	お客様情報／重要情報等を取り扱う場合、他の業務のネットワークとは別に、インターネットへの接続がない個別ネットワークを用意し、業務を実施しているか	×	他の業務と別NWを用意しているが、一定のインターネット通信を保守端末からも利用可能だった	○	データセンタのインターネットアクセスを必要最小限に限定し、保守網からのインターネットアクセスを遮断	○	データセンタのインターネットアクセスを必要最小限に限定し、保守網からのインターネットアクセスを遮断
	12	端末の不用なポートの閉塞・FW設定の有効化をしているか、端末内フォルダの不要な共有設定をしていないか	○	不要なポート開放無し	○	不要なポート開放無し	○	不要なポート開放無し

カテゴリ		点検項目	2023/8/3点検		2023/10/23点検		2024/1/31点検	
端末制限	13	重要な情報を扱う場合、アクセス可能な端末を制限し、私有端末等からのアクセスを禁止しているか	×	私有端末を接続可能	〇	MACアドレス制限で管理外端末の接続を遮断	〇	MACアドレス制限で管理外端末の接続を遮断
	14	私有端末からシステムを利用させる場合は、私有端末に会社情報を保存させない対策を実施しているか	×	私有端末を接続した場合、私有端末に情報持ち出し可能	〇	中継端末の画面転送により、情報持ち出し不可	〇	中継端末の画面転送により、情報持ち出し不可
メールクラウドによる漏洩防止	15	メール送信時の検閲機能、もしくは、定期的にメール送信履歴が確認できる機能を実装しているか	×	メール利用なしだが、保守端末からWebメールが利用できる状態だった	×	（同左）	〇	一部サーバからWebメール利用できる状態であるが添付ファイル制限済かつアラート通知設定済（UTM導入によるWebメール規制12/20実施済）
	16	お客様情報／重要情報等を取り扱う場合に、情報漏洩のリスクが高いサイト（ファイル共有サイト、クラウドストレージ、SNS等）への接続を制限しているか	×	一定のインターネット通信を保守端末からも利用可能であった	〇	データセンタのインターネットアクセスを必要最小限に限定	〇	インターネットアクセスを最小限のサーバのみ限定済だが接続先のさらなる制限予定（UTM導入12/20実施済）

○：対処済、×：ルール不適合、△：運用対処済、－：対象外

カテゴリ	点検項目		2023/8/3点検		2023/10/23点検		2024/1/31点検	
アカウント管理	17	アカウントの共用がないか（作業者を特定できるか）	×	保守端末・システムアカウントが共用のため業者特定不可	○	アカウントを個人化。個人化不可のアカウントについても中継端末により作業者特定可	○	アカウントを個人化。個人化不可のアカウントについても中継サーバにより作業者特定可
	18	アカウントの管理手順を定め、作成・変更・削除時は管理手順に従っているか	×	手順整備なし。共有アカウントのID／パスワードを共有フォルダに平文保管	○	アカウントの申請・払出し手順を整備	○	アカウントの申請・払出し手順を整備
	19	アカウントへ付与する権限レベルを定め、必要最小限の権限付与としているか	×	共有アカウントかつ権限に応じた付与ができていない	○	業務上必要な権限細分化と必要最小限の権限付与	○	業務上必要な権限細分化と必要最小限の権限付与
	20	異動／退職者等不要アカウントが無いか定期点検しているか	×	共用アカウントであり、個人特定できず、定期的な点検・削除ができていない	○	異動・退職時等のアカウント削除漏れがないかを四半期に一度確認	○	異動・退職時等のアカウント削除漏れがないかを四半期に一度確認
	21	重要な情報を保有する場合、多要素認証としているか	×	多要素認証なし	×	中継サーバのログイン認証を多要素認証化（12月中目途）	×	多要素化調整中（3月末予定）
作業管理	22	特権アカウントによる作業について、事前に承認・記録しているか	×	サーバ保守は計画・承認していたが作業記録の厳格運用なし。ヘルプ業務で抽出時の承認なし	○	原則、作業者はお客様情報にアクセスしない。委託元からの指示がある場合は事前承認の上実施	○	原則、作業者はお客様情報にアクセスしない。委託元からの指示がある場合は事前承認の上実施
	23	特権アカウントによる作業ログ（お客様情報出力を含む）を取得しているか	×	ヘルプ業務で抽出ログ取得も、アカウント共用のため作業者特定困難	○	中継サーバ経由でのみ作業が可能で、作業ログも取得	○	中継サーバ経由でのみ作業が可能で、作業ログも取得
	24	保守作業者の作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか	×	サーバ保守は計画・承認していたが作業記録の厳格運用なし。	○	中継サーバ経由でのみ作業が可能で、作業ログも取得	○	中継サーバ経由でのみ作業が可能で、作業ログも取得
	25	特権を持つシステム利用者による作業について、ログの削除・改ざんをできない仕組みとなっているか	×	ヘルプ業務で抽出ログ取得も、アカウント共用のため作業者特定困難	○	中継サーバにおいてセキュリティ対策ソフトウェアによる操作映像を記録	○	改ざんされないよう権限付与対応済。追加改善でSyslogサーバ構築し改ざんできない対策を追加（3月末）
	26	ログの定期点検を実施しているか	×	できていなかった	○	セキュリティ対策ソフトウェアにてログ取得し定期的な点検を実施	○	セキュリティ対策ソフトウェアにてログ取得し定期的な点検を実施
委託先管理	27	業務委託先に対する要求事項としてセキュリティ対策を要求しているか	○	保守契約において要求	○	保守契約において要求	○	保守契約において要求
	28	システム構築・運用に関する業務委託範囲や内容に応じて自社のセキュリティ管理策の実装もしくは運用の実施を委託先に要求し、対応可能であるか確認しているか	×	一部の委託先でID個人化・USBメモリ制限等ができていなかった	○	お客様情報取扱いに関する運用ルールに従い、委託先チェックシートにて実施	○	お客様情報取扱いに関する運用ルールに従い、委託先チェックシートにて実施
	29	委託先のセキュリティ対策の遵守状況を定期的に点検しているか	×	一部の委託先の点検ができていない	×	事案公表後、委託先点検を実施	○	事案公表後、委託先点検を実施
	30	委託先の保守作業について作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか	×	お客様情報出力ログは取得も、アカウント共用のため作業者特定困難	○	委託先作業記録の運用開始。中継サーバでセキュリティ対策ソフトウェアにより操作映像を記録	○	委託先作業記録の運用開始。中継サーバでセキュリティ対策ソフトウェアにより操作映像を記録

○：対処済、×：ルール不適合、△：運用対処済、－：対象外

カテゴリ		点検項目	2023/8/3点検		2023/10/23点検		2024/1/31点検	
共有ファイルサーバ利用	31	共有フォルダに重要な情報を保管している場合、アクセス制限及びパスワード設定をしているか	×	アカウント共用のため、個人認証なし	○	共有フォルダのアクセス権をディレクトリ・サービス・システムで管理し、組織ごとにフォルダを整理	○	共有フォルダのアクセス権をディレクトリ・サービス・システムで管理し、組織ごとにフォルダを整理
	32	アクセス制限について、異動／退職者等不要アカウントがないか定期点検しているか	×	アカウント共用のため、点検の概念なし	○	メンバ変更都度、また四半期毎に確認	○	メンバ変更都度、また四半期毎に確認
	33	共有フォルダへの保存期間を定め、期間を過ぎたものは削除しているか	－	共有フォルダに保存期間設定が必要な情報なし	－	共有フォルダに保存期間設定が必要な情報なし	○	原則7年だが、保管期間の決めにくいものは定期的な棚卸で対応
	34	重要情報を保存しているフォルダについてアクセスログを取得しているか また、不要なアクセスがないか確認しているか	×	共有サーバへのアクセスログ取得なし	○	中継サーバ経由での作業ログを取得し管理簿と突合運用開始	○	中継サーバ経由での作業ログを取得し管理簿と突合運用開始
システム保管場所	35	重要情報を保管しているシステムの設置場所について、アクセス制限がされ、入退室管理並びに監視及び盗難対策等がされているか	○	一部DCに設置。保守拠点でも特定人員のみ入室可能で入室記録あり	○	一部DCに設置。保守拠点でも特定人員のみ入室可能で入室記録あり	△	現行でも一定対策はしているが、さらなる強化として保守拠点のセキュリティゾーン設置・入退室管理及び監視カメラによる常時監視予定、引き続き確認（3月末）
	36	システムの設置場所への入退室は、管理者によって管理され、特定の人員にのみ入室権限の付与がされているか	○	DCでは事前申請や厳格な入退出管理を実施。保守拠点でも特定人員のみICカードを払出し	○	DCでは事前申請や厳格な入退出管理を実施。保守拠点でも特定人員のみICカードを払出し	△	
	37	アクセスが制限されていない場所に設置せざるを得ない場合は部外者によるシステムの利用・接続や盗難を防止する措置を講じているか	－		－		－	
	38	設置場所への機器の持込み／持ち出し時は、承認権限者の許可を得て、監視や作業記録を保存しているか	×	私有端末やUSBの持込みは運用上禁止していたが、監視や管理が不十分	○	私有端末やUSBメモリの持込みは禁止。管理簿にて記録。仮に持込まれても接続不可	○	私有端末やUSBメモリの持込みは禁止。管理簿にて記録。仮に持込まれても接続不可
	39	設置場所への入室権限について、定期的に見直しをし、不要な権限の削除を実施しているか	○	実施中	○	実施中	○	実施中
	40	入室に必要となる鍵については員数管理し、紛失時の対応をしているか パスワード認証の場合は定期的に変更を行っているか	○	予備保管分も含めてICカードの定期的な棚卸を実施	○	予備保管分も含めてICカードの定期的な棚卸を実施	○	予備保管分も含めてICカードの定期的な棚卸を実施
リモート接続	41	リモートで接続させる場合、ID ／パスワード認証より強固な認証方式か	○	ID／パスワード + 事前情報共有鍵（ID／パスワードより強固）	○	ID／パスワード + 事前情報共有鍵（ID／パスワードより強固）	○	さらなる強化として、多要素認証導入予定（3月末）。（No.21と同旨）
	42	VPN接続アカウントの共用がないか（接続者を特定できるか）	×	VPNアカウント共用のため特定困難	○	VPNアカウントは共用だが、中継サーバで作業者特定可	○	さらなる強化として、多要素認証にあわせVPNアカウント個人化（3月末）。（No.21と同旨）
	43	リモート接続時の利用端末・利用環境はオフィス端末と同様の各種対策が実施されているか	×	私有端末を接続し情報持ち出し可能	○	中継サーバ経由で情報持ち出し不可	○	中継サーバ経由で情報持ち出し不可
データ暗号化	44	顧客情報は参照権限を持たない人が参照できないよう、システム的に暗号化されているか	×	ベンダ協議要	×	持ち出し制限かつ暗号化対応USB利用	×	さらなる改善として、顧客情報保有サーバは暗号化対応を検討中

ProCXにおける本件システム点検結果

○：対処済、×：ルール不適合、△：運用対処済、－：対象外

別紙7-2

注：2023/9/7及び2023/10/23は、2拠点（●・●）の回答をとりまとめたもの
2024/1/31は、本件システムの利用に関し、ProCXの対策チームの回答をとりまとめたもの

カテゴリ		点検項目	2023/9/7点検		2023/10/23点検		2024/1/31点検	
持ち出し制御	1	（1は業務上USBメモリ利用がない場合の点検項目）会社が許可したUSBメモリ等以外を利用させない対策が取られているか	－	（対象外）	－	（対象外）	○	ポリシー設定でシステム上禁止済
	2	（2から6は業務上USBメモリ利用がある場合の点検項目）USBメモリ等を利用する場合は、会社支給の生体認証／暗号化等の対策が実施されたものを利用しているか	○	指定USBメモリ／データブリッジ利用	○	指定USBメモリ／データブリッジ利用	○	原則データブリッジ利用 USB利用時は指定USB利用
	3	会社が許可したUSBメモリ等以外を利用させない対策が取られているか	○	接続禁止制御実施	○	接続禁止制御実施	△	・USBメモリ利用PCを最小化済 ・USBメモリ利用なしPCへUSBメモリ遮断設定済 ・原則データブリッジ利用（2月末）
	4	会社が許可したUSBメモリ等を利用する場合、事前の承認を得て記録しているか	○	利用承認・記録を管理簿管理	○	利用承認・記録を管理簿管理	○	利用承認・記録を管理簿にて管理 作業は複数人実施
	5	端末へのUSBメモリ等の接続についてログを取得し定期的に確認しているか 又は第三者立会いによる操作内容の目視確認を実施しているか	×	USBメモリ利用ログは取得なし（●）	×	USBメモリ利用ログは取得なし（●）	△	セキュリティ対策ソフトウェア導入によるログ管理（3月末）。それまではNo.3、4で対処
	6	USBメモリ等を別用途で再利用もしくは廃棄する場合は情報の復元が不可能な方法でデータ消去しているか	－	（実績なし対象外）	－	（実績なし対象外）	○	今後、余剰USBメモリを回収し専門業者で廃棄予定（2月末）。
端末管理	7	端末のアカウント共用がないか	×	SV端末は未確認 一般オペレータは端末アカウント共用	×	SV端末は未確認 一般オペレータは端末アカウント共用	△	・JOB毎業務フローに沿って利用者・SV端末の共用アカウント使用者管理は実施済 ・統一的な共用アカウント運用・毎月点検ルール徹底中（2月末）
	8	マルウェア対策ソフトを導入しているか	○	マルウェア対策ソフト導入済み	○	マルウェア対策ソフト導入済み	○	ONE CONTACT Network（OCN）端末は導入済
	9	端末及びUSBメモリ等を施錠保管しているか	○	施錠管理	○	施錠管理	○	端末ワイヤーロック、USBメモリ施錠管理済
	10	端末及びUSBメモリ等を社外に持ち出す場合、承認を含めた持出管理をしているか	－	（持ち出し業務なし対象外）	－	（持ち出し業務なし対象外）	○	可搬媒体の施錠管理および承認管理
	11	お客様情報／重要情報等を取り扱う場合、他の業務のネットワークとは別に、インターネットへの接続がない個別ネットワークを用意し、業務を実施しているか	○	インターネット接続はできない、専用網で業務実施	○	インターネット接続はできない、専用網で業務実施	○	インターネット接続はできない、専用網で業務実施
	12	端末の不用なポートの閉塞・FW設定の有効化をしているか、端末内フォルダの不要な共有設定をしていないか	×	端末のtelnet（※1）有効化・FW無効化（※2）・RDP有効化	×	（10/17BSより設定マニュアル提供）	○	OCN端末はFW機能・ポート閉塞実施済

○：対処済、×：ルール不適合、△：運用対処済、－：対象外

カテゴリ		点検項目	2023/9/7点検		2023/10/23点検		2024/1/31点検	
端末制限	13	重要な情報を扱う場合、アクセス可能な端末を制限し、私有端末等からのアクセスを禁止しているか	×	・端末の制限制御なし 運用上は私有端末持込不可徹底 （クリアバッグ必須）	×	・端末の制限制御なし 運用上は私有端末持込不可徹底 （クリアバッグ必須）	○	セキュリティ対策ソフトウェア導入 による禁止済 それまでは私物端末持込禁止と チェックの運用を徹底済
	14	私有端末からシステムを利用させる場合は、私有端末に会社情報を保存させない対策を実施しているか	－	（私有端末利用無し対象外）	－	（私有端末利用無し対象外）	－	私有端末の業務利用なし 加えて、私物端末からの接続遮断予定（3月末）
メールクラウドによる漏洩防止	15	メール送信時の検閲機能、もしくは、定期的にメール送信履歴が確認できる機能を実装しているか	－	（メール利用不可対象外）	－	（メール利用不可対象外）	－	（メール利用不可対象外）
	16	お客様情報／重要情報等を取り扱う場合に、情報漏洩のリスクが高いサイト（ファイル共有サイト、クラウドストレージ、SNS等）への接続を制限しているか	－	（インターネット接続不可対処外）	－	（インターネット接続不可対処外）	－	（インターネット接続不可対処外）

○：対処済、×：ルール不適合、△：運用対処済、－：対象外

カテゴリ	点検項目		2023/9/7点検		2023/10/23点検		2024/1/31点検	
アカウント管理	17	アカウントの共用がないか（作業者を特定できるか）	×	オペレータ／SV端末のAdminアカウント（※3）とパスワードが同一の為、特定不可	○	暫定としてSV端末のAdminアカウント（※3）のパスワード変更済。オペレータ端末は共用（DL・持ち出しは不可）	△	・JOBごとの業務フローに沿った共有アカウントの最小限化・管理は実施済 ・本社統一ルール展開実施中（2月末） ・ディレクトリ・サービス・システム導入による個人特定とログ取得・点検予定（3月末）
	18	アカウントの管理手順を定め、作成・変更・削除時は管理手順に従っているか	○	アカウント申請ルールあり、管理簿あり	○	アカウント申請ルールあり、管理簿あり	△	
	19	アカウントへ付与する権限レベルを定め、必要最小限の権限付与としているか	○	システムのログインアカウントは個人単位に払出し	○	システムのログインアカウントは個人単位に払出し	△	
	20	異動／退職者等不要アカウントが無いか定期点検しているか	○	異動・退職時のアカウント削除実施	○	異動・退職時のアカウント削除実施	△	
	21	重要な情報を保有する場合、多要素認証としているか	×	ID/パスワードのみ	×	（保守側の多要素認証を優先し、センタ対応を検討）	○	リモートは多要素認証済（本件システム利用端末は別管理）
作業管理	22	特権アカウントによる作業について、事前に承認・記録しているか	○	顧客リストデータDLはデータブリッジ／USBメモリ持ち出しとあわせ管理簿で管理	○	顧客リストデータDLはデータブリッジ／USBメモリ持出とあわせ管理簿で管理	△	・JOBごとの業務フローに沿った対応は実施済 ・本社統一ルール展開実施中（2月末）
	23	特権アカウントによる作業ログ（お客様情報出力を含む）を取得しているか	○	作業ログ取得、持ち出し管理簿管理	○	作業ログ取得、持ち出し管理簿管理	△	・No.22の徹底
	24	保守作業者の作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか	－	（対象外）	－	（対象外）	－	（対象外）
	25	特権を持つシステム利用者による作業について、ログの削除・改ざんをできない仕組みとなっているか	○	DLログの改ざん不可	○	DLログの改ざん不可	○	DLログの改ざん不可
	26	ログの定期点検を実施しているか	×	定期点検実施なし	×	検討中	△	（No.23と同様）
委託先管理	27	業務委託先に対する要求事項としてセキュリティ対策を要求しているか	－	（委託に関する整理を検討）	－	（委託に関する整理を検討）	○	BSと覚書締結済
	28	システム構築・運用に関する業務委託範囲や内容に応じて自社のセキュリティ管理策の実装もしくは運用の実施を委託先に要求し、対応可能であるか確認しているか	－	（対象外）	－	（対象外）	－	（対象外）
	29	委託先のセキュリティ対策の遵守状況を定期的に点検しているか	－	（委託に関する整理を検討）	－	（委託に関する整理を検討）	－	BSとの覚書に従い、委託先の保守作業に関する全管理措置の状況確認を実施
	30	委託先の保守作業について作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか	－	（業務委託でないため対象外）	－	（業務委託でないため対象外）	○	BSとの覚書に従い、委託先の保守作業に関する作業ログを取得し、作業記録簿との対照による検証を実施。

○：対処済、×：ルール不適合、△：運用対処済、－：対象外

カテゴリ	点検項目		2023/9/7点検		2023/10/23点検		2024/1/31点検	
共有ファイルサーバ利用	31	共有フォルダに重要な情報を保管している場合、アクセス制限及びパスワード設定をしているか	－	（共有サーバなし対象外）	－	（共有サーバなし対象外）	△	・JOBごとに業務フローを定め対応 ・顧客データ保有のフォルダアクセス権最小化済 ・顧客データは原則利用後削除 ・本社管理手順による運用展開中（2月末）
	32	アクセス制限について、異動／退職者等不要アカウントがないか定期点検しているか	－		－		△	
	33	共有フォルダへの保存期間を定め、期間を過ぎたものは削除しているか	－		－		△	
	34	重要情報を保存しているフォルダについてアクセスログを取得しているか また、不要なアクセスがないか確認しているか	－		－		△	セキュリティ対策ソフトウェア取得ログ踏まえ検討(3月末）（それまで優先17項目徹底）
システム保管場所	35	重要情報を保管しているシステムの設置場所について、アクセス制限がされ、入退室管理並びに監視及び盗難対策等がされているか	－	（BS所掌のため対象外、居室の対応は実施）	－	（BS所掌のため対象外、居室の対応は実施）	－	（BS所掌のため対象外、居室の対応は実施）
	36	システムの設置場所への入退室は、管理者によって管理され、特定の人員にのみ入室権限の付与がされているか	－		－		－	
	37	アクセスが制限されていない場所に設置せざるを得ない場合は部外者によるシステムの利用・接続や盗難を防止する措置を講じているか	－		－		－	
	38	設置場所への機器の持込み／持ち出し時は、承認権限者の許可を得て、監視や作業記録を保存しているか	－		－		－	
	39	設置場所への入室権限について、定期的に見直しをし、不要な権限の削除を実施しているか	－		－		－	
	40	入室に必要となる鍵については員数管理し、紛失時の対応をしているか パスワード認証の場合は定期的に変更を行っているか	－		－		－	
リモート接続	41	リモートで接続させる場合、ID ／パスワード認証より強固な認証方式か	－	2拠点ではリモート接続なし対象外だが、既存リモート接続環境は、VPN認証アカウントが共用で私物端末接続可	－	2拠点ではリモート接続なし対象外だが、既存リモート接続環境の利用を停止。セキュリティ要件を満たす「在宅PF」に切替	○	「在宅PF」を利用する ※MACアドレス・端末証明書認証
	42	VPN接続アカウントの共用がないか（接続者を特定できるか）	－		－		○	在宅PFの利用アカウントは共用せず個人単位に払い出す
	43	リモート接続時の利用端末・利用環境はオフィス端末と同様の各種対策が実施されているか	－		－		○	「在宅PF」はシンクラ方式
データ暗号化	44	顧客情報は参照権限を持たない人が参照できないよう、システム的に暗号化されているか	－	（BS所掌のため対象外）	－	（BS所掌のため対象外）	－	（本件システムはBS所掌のため対象外）

※1：telnet: 遠隔でPCにログインし任意のコマンドを発行することで各種操作ができる機能（通常は無効化）
※2：Firewall:悪意のある攻撃・通信から端末を守る機能（通常は有効化）
※3：Adminアカウント：端末に対しあらゆる設定変更が可能なアカウント、SV端末：お客様情報をダウンロードできるSV（スーパーバイザー）利用端末

優先17項目の考え方

➢ 点検44項目のうち、特に事案に直結する項目を優先17項目と設定

情報を持ち出せない・持ち出せるなら限定する			優先１７項目
持ち出し制御	1, 3	会社許可USBメモリ等以外を利用させない対策をしているか	
	2	USBメモリ等を利用する場合は、会社支給の生体認証/暗号化等の対策をしているか	
	4	会社が許USBメモリ等を利用時、事前の承認を得て記録しているか	
	5	端末へのUSBメモリ等の接続についてログ取得・定期的確認（リアルタイムに検知する仕組み有無）。または第三者立会による操作内容の目視確認	
	6	USBメモリ等を別用途で再利用もしくは廃棄する場合は情報の復元が不可能な方法でデータ消去	
端末管理	7	端末のアカウント共用がないか	
	8	マルウェア対策ソフトを導入しているか	
	9	端末およびUSBメモリ等を施錠保管しているか	
	10	端末およびUSBメモリ等を社外に持ち出す場合、承認を含めた持出管理をしているか	
	11	重要情報等を取り扱う場合、インターネットへの接続が無い個別NW用意し、業務を実施しているか	
	12	端末の不要なポートの閉塞・FW設定の有効化しているか、端末内フォルダの不要な共有設定をしていないか	
端末制限	13	重要な情報を扱う場合、アクセス可能な端末を制限し、私有端末等からのアクセスを禁止しているか	
	14	私有端末からシステムを利用させる場合、私有端末に会社情報を保存させない対策をしているか	
メール・クラウド等による漏洩防止	15	メール送信時の検閲機能、もしくは定期的にメール送信履歴が確認できる機能を実装しているか	
	16	重要情報等を取り扱う場合、情報漏えいのリスクが高いサイト（クラウドストレージ等）へ接続制限しているか	
トレース検知する・検知した情報をチェックする			
アカウント管理	17	アカウントの共用が無いか（作業者を特定できるか）	
	18	アカウントの管理手順を定め、作成・変更・削除時は管理手順に従っているか	
	19	アカウントへ付与する権限レベルを定め、必要最小限の権限付与としているか	
	20	異動／退職者等不要アカウントが無いか定期点検しているか	
	21	重要な情報を保有する場合、多要素認証としているか	
作業管理	22	特権アカウントによる作業について、事前に承認・記録しているか	
	23	特権アカウントによる作業ログ（お客様情報出力を含む）を取得しているか	
	24	保守作業者の作業ログの取得、または第三者の立会による作業内容の確認が行われているか	
	25	特権を持つシステム利用者による作業について、ログの削除・改ざんをできない仕組みとなっているか	
	26	ログの定期点検を実施しているか	
委託先管理	27	業務委託先に対する要求事項としてセキュリティ対策を要求しているか	
	28	システム構築・運用に関する業務委託範囲や内容に応じ自社セキュリティ管理策の実装もしくは運用実施を委託先に要求し、対応可否を確認しているか	
	29	委託先のセキュリティ対策の遵守状況を定期的に点検しているか	
	30	委託先の保守作業について作業ログの取得、または第三者の立会による作業内容の確認が行われているか	
共有サーバ利用	31	共有フォルダに重要な情報を保管している場合、アクセス制限およびパスワード設定をしているか	
	32	アクセス制限について、異動／退職者等不要アカウントが無いか定期点検しているか	
	33	共有フォルダへの保存期間を定め、期間を過ぎたものは削除しているか	
	34	重要情報を保存しているフォルダについてアクセスログを取得しているか　また不要なアクセスが無いか確認しているか	
システム保管場所	35	重要情報を保管しているシステムの設置場所について、アクセス制限がされ、入退室化に並びに監視および、盗難対策等がされているか	
	36	システムの設置場所への入退室は、管理者によって管理され、特定の人員にのみ入室権限の付与がされているか	
	37	アクセスが制限されていない場所に設置せざるを得ない場合は部外者によるシステムの利用・接続や盗難を防止する措置を実施しているか	
	38	設置場所への機器の持込み／持出し時は、承認権限者の許可を得て、監視や作業記録を保存しているか	
	39	設置場所への入室権限にるいて、定期的に見直しをし、不要な権限の削除を実施しているか	
	40	入室に必要となる鍵については員数管理し、紛失時の対応をしているか。パスワード認証の場合は定期的に変更を行っているか	
リモート接続	41	リモートで接続させる場合、ID/PW認証より強固な認証方式か	
	42	VPN接続アカウントの共用が無いか（接続者を特定できるか）	
	43	リモート接続時の利用端末・利用環境はオフィス端末と同様の各種対策が取られているか	
暗号化	44	顧客情報は参照権限を持たない人が参照できないよう、システム的に暗号化されているか	

事案の原因（公表①～④＋⑤⑥）

- ①保守作業端末にダウンロードが可能になっていた
- ②保守作業端末に外部記録媒体を接続し、データを持ち出すことが可能になっていた
- ③セキュリティリスクが大きいと想定される振る舞いをタイムリーには検知できていなかった
- ④各種ログ等の定期的なチェックが十分でなかった
- ⑤個人を特定できる仕組みがなかった
- ⑥許可していない端末の接続を禁止できていなかった

点検 44 項目に関する主な是正対応（予定を含む。）

カテゴリ		点検項目	主な是正対応（運用対処及び対応予定のものを含む）
持ち出し制御	1	（1 は業務上 USB メモリ利用がない場合の点検項目） USB メモリ等を利用できない対策が取られているか	・エージェントソフトウェア導入により禁止する ・ディレクトリ・サービス・システムで利用可能端末、アカウント、USB メモリ等の接続を制御する ・USB 用ポートブロックにて物理的に USB ポートを塞ぐ ・利用可能な USB メモリは会社支給の指紋認証付き USB メモリのみとし、USB メモリ利用者は施錠管理者に限定する ・USB メモリではなくデータブリッジを利用することで媒体の社外持ち出しリスクをなくす
	2	（2 から 6 は業務上 USB メモリ利用がある場合の点検項目）USB メモリ等を利用する場合は、会社支給の生体認証／暗号化等の対策が実施されたものを利用しているか	
	3	<USB メモリ等の外部記録媒体を利用する業務がある場合> 会社が許可したUSBメモリ等以外を利用させない対策が取られているか	
	4	会社が許可したUSBメモリ等を利用する場合、事前の承認を得て記録しているか	・USB メモリ利用の都度管理者の承認を得て、外部記録媒体利用管理簿で管理する。返却時は USB メモリ格納情報が削除されていることを管理者が確認後に管理簿に記録
	5	端末へのUSBメモリ等の接続についてログを取得し定期的に確認しているか 又は第三者立会いによる操作内容の目視確認を実施しているか	・ログ取得の実現までの間は、複数人で作業を実施するルールとし、外部記録媒体利用管理簿に立会者名も記載する
	6	USB メモリ等を別用途で再利用もしくは廃棄する場合は情報の復元が不可能な方法でデータ消去しているか	・別用途で再利用する際はフォーマットする（クイックフォーマットは不可） ・廃棄の際は破砕業者に依頼し写真等証跡を確認する

カテゴリ	点検項目		主な是正対応（運用対処及び対応予定のものを含む）
端末管理	7	端末のアカウント共用がないか	・共用アカウントを廃止し個人別にアカウントを払い出す
	8	マルウェア対策ソフトを導入しているか	・アンチウイルスソフトウェア、セキュリティ対策ソフトウェアを利用する
	9	端末及び USB メモリ等を施錠保管しているか	・持ち出し PC や USB メモリは鍵付き書庫で保管し、書庫の鍵は管理者が管理する
	10	端末及びUSBメモリ等を社外に持ち出す場合、承認を含めた持出管理をしているか	・社外への持ち出し時は、事前に社外持ち出し管理簿に記載し、都度管理者の事前承認を得る
	11	お客様情報／重要情報等を取り扱う場合、他の業務のネットワークとは別に、インターネットへの接続がない個別ネットワークを用意し、業務を実施しているか	・安全とみなしたウェブサイトのリストであるホワイトリスト以外のアクセス先を制限する ※社内利用システムの通信網である OA 網から利用する SaaS 等システムについては OA 網の対策で保護されていると判断
	12	端末の不用なポートの閉塞・FW 設定の有効化しているか、端末内フォルダの不要な共有設定をしていないか	・ファイアウォールを有効とし、初期状態から不要な通信の許可をしない ・端末内フォルダの共有設定をしない ・承認なく勝手にアプリをインストールしない
端末制限	13	重要な情報を扱う場合、アクセス可能な端末を制限し、私有端末等からのアクセスを禁止しているか	・MAC アドレスフィルタにて管理外端末の接続を禁止する ・ディレクトリ・サービス・システムに登録された端末以外からのアクセスを禁止する ・各種ソフトウェアへのアクセスを登録されたデバイスに限定する ・セキュア FAT 以外からアクセスできないよう接続元 IP アドレスを限定する

カテゴリ		点検項目	主な是正対応（運用対処及び対応予定のものを含む）
	14	私有端末からシステムを利用させる場合は、私有端末に会社情報を保存させない対策を実施しているか	・私有端末からのリモートデスクトップ接続を認める場合、画面転送方式とし私有端末へのデータ持ち出しは不可とする
メール・クラウド等による漏洩防止	15	メール送信時の検閲機能、もしくは、定期的にメール送信履歴が確認できる機能を実装しているか	・社内 OA 端末を利用する場合は会社のメールを利用し添付ファイル送信時は上長承認を得る
	16	お客様情報／重要情報等を取り扱う場合に、情報漏洩のリスクが高いサイト（ファイル共有サイト、クラウドストレージ、SNS 等）への接続を制限しているか	・フィルタリングソフトを導入し、高リスクサイトや業務に不要なサイトへのアクセス制限設定を実施
アカウント管理	17	アカウントの共用がないか（作業者を特定できるか）	・システムのアカウントを個人アカウントに変更する ・システムの制約上、SE 業務を共用アカウントで実施する必要がある場合は、作業承認を得て管理簿に記録する。また、承認のないログインがないかを定期ログ点検にて確認する
	18	アカウントの管理手順を定め、作成・変更・削除時は管理手順に従っているか	・アカウント管理手順を定める ・アカウント共用を解消できない場合は、共用アカウント利用管理簿を作成する
	19	アカウントへ付与する権限レベルを定め、必要最小限の権限付与としているか	・権限付与を見直し、権限パターンを細分化する
	20	異動／退職者等不要アカウントがないか定期点検しているか	・アカウント点検を運用に追加する ・委託先への払出しアカウントについても毎月 1 回の棚卸を実施する
	21	重要な情報を保有する場合、多要素認証としているか	・ID／パスワードのみではなく、システムへのアクセス時に SMS によるワンタイムコード認証を追加 ・多要素認証導入までは毎月の定期点検にて重要情報を扱う操作ログの点検を実施

カテゴリ		点検項目	主な是正対応（運用対処及び対応予定のものを含む）
作業管理	22	特権アカウントによる作業について、事前に承認・記録しているか	・特権アカウントによる作業管理簿を整備。作業前に承認を得て、記録する ・管理者の口頭承認による運用から、システム上で承認を得るフローに変更する
	23	特権アカウントによる作業ログ（お客様情報出力を含む）を取得しているか	・お客様情報出力ログを取得する機能追加開発を実施する ・ログ取得できない場合は、2 名以上の操作を義務付けることで不要な行為を防止する
	24	保守作業者の作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか	・作業画面を録画する ・SE 作業は必ず 2 名以上で実施し、作業ログを取得する。作業完了後にログを提出し、サーバ SE がアクセスできない場所にログを保管
	25	特権を持つシステム利用者による作業について、ログの削除・改ざんをできない仕組みとなっているか	
	26	ログの定期点検を実施しているか	・月次で、ログインログ／システムの操作ログと作業管理簿を突合し、承認されていないログイン／操作がないかを点検する
委託先管理	27	業務委託先に対する要求事項としてセキュリティ対策を要求しているか	・委託先とお客様情報保護に関する覚書を締結し、具体的なセキュリティ対策について合意する
	28	システム構築・運用に関する業務委託範囲や内容に応じて自社のセキュリティ管理策の実装もしくは運用の実施を委託先に要求し、対応可能であるか確認しているか	
	29	委託先のセキュリティ対策の遵守状況を定期的に点検しているか	・NTT 西日本標準の「情報管理状況チェックシート」により月次点検を実施する
	30	委託先の保守作業について作業ログの取得、又は第三者の立会いによる作業内容の確認が行われているか	・これまで作業ログの提出は求めていなかったが今後は提出を求める ・操作ログ管理ツールを導入し、委託先の操作を管理可能とする

カテゴリ		点検項目	主な是正対応（運用対処及び対応予定のものを含む）
共有サーバ利用	31	共有フォルダに重要な情報を保管している場合、アクセス制限及びパスワード設定をしているか	・ファイルサーバにはセキュリティグループを設定しアクセス制限をかけているが、お客様情報を含むファイルには、今後はパスワードも設定する
	32	アクセス制限について、異動／退職者等不要アカウントがないか定期点検しているか	・異動／退職等のタイミングで都度アカウント削除を実施する。加えて、四半期に一度、アカウントの棚卸を実施する
	33	共有フォルダへの保存期間を定め、期間を過ぎたものは削除しているか	・保管期間を定め、期間後は削除する ・不要ファイル削除の運用ルールを定め、毎年棚卸を実施する
	34	重要情報を保存しているフォルダについてアクセスログを取得しているか また、不要なアクセスがないか確認しているか	・サーバオペレーティングシステムのイベントログ収集を設定する
システム保管場所	35	重要情報を保管しているシステムの設置場所について、アクセス制限がされ、入退室管理並びに監視及び、盗難対策等がされているか	・入室の際は管理者による事前登録と受付での本人確認の後、入室用カードが貸し出されるデータセンタに設置する
	36	システムの設置場所への入退室は、管理者によって管理され、特定の人員にのみ入室権限の付与がされているか	・社員カードで入退室管理を行い、権限のない社員は入室不可な部屋に設置する
	37	アクセスが制限されていない場所に設置せざるを得ない場合は部外者によるシステムの利用・接続や盗難を防止する措置を講じているか	・アクセスが制限されていない場所への設置はしない ・サーバを施錠したケージで囲い、管理は開錠可能なボックスに鍵を保管する
	38	設置場所への機器の持込み／持ち出し時は、承認権限者の許可を得て、監視や作業記録を保存しているか	・持込みを禁止し、サーバ室内は監視カメラで行動監視を行う ・持込み時は入室申請時に持込みの許可を得て記録する

カテゴリ		点検項目	主な是正対応（運用対処及び対応予定のものを含む）
	39	設置場所への入室権限について、定期的に見直しをし、不要な権限の削除を実施しているか	・メンバー変更があった際には入室権限者の登録・削除を実施する。また四半期に一度、権限者の棚卸を実施する
	40	入室に必要となる鍵については員数管理し、紛失時の対応をしているか パスワード認証の場合は定期的に変更を行っているか	・入室カードの棚卸を定期的に実施し、紛失があった場合は直ちに失効処理を実施する ・パスワードは四半期に一度変更する
リモート接続	41	リモートで接続させる場合、ID／パスワード認証より強固な認証方式か	・ID／パスワードに加え、認証アプリによる多要素認証を行う ・ID／パスワードに加え、事前配布鍵による認証を行う
	42	VPN 接続アカウントの共用がないか（接続者を特定できるか）	・VPN 接続アカウントは個人単位で払い出す
	43	リモート接続時の利用端末・利用環境はオフィス端末と同様の各種対策が取られているか	・システムへのアクセスは踏み台サーバへのリモートデスクトップ接続による画面転送方式に限定することでセキュリティを担保
暗号化	44	顧客情報は参照権限を持たない人が参照できないよう、システム的に暗号化されているか	・本点検において暗号化有無を確認済 ・当該確認結果を踏まえ、今後具体的な内容・方法について整理の上、各システムにおいて実装を予定

アンケート回答結果（主なもの）

【質問 1③】「自らの所管する組織・部署の内部者によるお客様情報の不正流出を情報セキュリティ上の重大なリスク要因として認識していましたか。」との質問（質問 1①）に対して、「認識はしていたが、自組織内では起こり得ないと考えていた。」と回答した理由をご回答ください。

【結果】

（性善説を理由とするもの）

- 内部者に不正流出を行おうとする者は存在していないと思っていた。
- 自組織の内部者がお客様情報を不正に持ち出す事案がこれまでなかったから。
- これまでも大きな事故もなかったことから、性善説によった考え方が浸透していた
- 運用フローが定まっており、悪意を持って情報流出させることは想像できなかった。
- 性悪説に基づいた対応を考えていなかったため
- ある程度のシステム的な対処はするが、古いシステムであるということもあり対応できる策に制限があり、性善説で業務運営していた。
- 自組織の中に不正流出させるような社員、仕組みはないだろう、と無意識で思い込んでいた

（十分な研修が行われていたことを理由とするもの）

- 情報セキュリティの各種研修、啓蒙活動を実施してること等から、自組織への発生は疑っていなかった
- 日頃より情報漏洩に対する啓蒙活動を実施しており、性善説よりお客様情報を盗むことがないと考えていたため
- 電気通信設備に係るシステム群を取り扱う社員については、教育が行き届いており、全般にロイヤリティも高く、不正が発生しにくいと考えていたから
- セキュリティインシデント等、定期的な研修を実施しており、十分に理解していると思っていたため。
- 各種研修、日常の指導から管理は徹底されており、不正を働くことはないと考えていた
- 情報セキュリティについて、度重ねて実施される研修等や定期的に提供される啓発情報にてチームメンバー全員に充分にいきわたっていると思っているからです。

（物理的な措置を理由とするもの）

- そもそも社外へメール添付もできないし、USB も使えない。携帯電話も持ち込み不可であるから
- USB メモリは使用の実績がなく、社外メールは自らもしくは管理者が承認しているため。
- アクセスできるロケーションは限定されており、管理もルール順守されていると考えていた。

【質問 1④】「内部者による不正情報流出のうち、お客様情報を取り扱うシステムのシステム管理者又は運用保守従事者による不正情報流出を情報セキュリティ上の重大なリスク要因として認識していましたか。」との質問（質問 1②）に対し、「認識はしていたが、自組織内では起こり得ないと考えていた。」と回答した理由をご回答ください。

【結果】

（性善説を理由とするもの）

- NTT に属する一員として倫理的に不正流出につながる行為を実行することはないという思い込み
- システム管理に従事する社員についてはモラルが高い社員を配置しており、不正は出ないものと性善説に立っていたため
- マニュアルに基づき実施していれば大丈夫と言った性善説に立っていた！
- 内部者に不正流出を行おうとする者は存在していないと思っていた。
- 自組織のシステム管理者や運用保守従事者がお客様情報を不正に持ち出す事案がこれまでなかったから。
- 性善説に立っていた
- 自社の信用失墜につながるので、悪意を持って情報を流出させることは想像できなかった。

（十分な研修が行われていたことを理由とするもの）

- 研修等を通じてお客様情報の取り扱いについては意識が浸透していると認識していたため
- 情報セキュリティに関する研修を定期的に実施しており、対応はできていると考えていた（上記と同じく性悪説に基づいた対応はできていなかった）ため。
- 各種研修、日常の指導から管理は徹底されており、不正を働くことはないと考えていた
- 重大なリスク要因として認識はしていたが、コンプライアンスに関する社員研修も定期的に実施しており、社員のマインドも高まっていると認識していた
- 情報セキュリティ研修等、きめ細かく実施しているため

（物理的な措置を理由とするもの）

- さまざまな技術的対策が講じられており、情報の持ち出しが容易ではないため。
- USB 等媒体接続ができないこと、メール送信はすべて承認を要することなどから、そもそも不正情報流出をできる術がない

【質問 1⑦】「①内部者による不正情報流出リスク、②システム管理者又は運用保守従事者による不正情報流出リスクに対し、自らの所管する組織・部署の情報セキュリティ体制がどの程度脆弱であるか、また、そのような脆弱性に対して有効なリスク低減措置が実施されているかを、自ら又は部下に指示して検証・評価したことがありますか。」（質問 1⑤）との質問に対して「はい」と回答した場合、具体的な検証・評価方法をご回答ください。

【結果】

（自主点検等に基づく方法）

- ヒヤリングシートを活用しグループミーティングで項目単位に音読し検証
- 情セキ部が実施する、セキュリティチェックシートに従い検証、評価している
- チェックシートに基づいたヒアリング
- 年一回のセキュリティ自主点検を契機とし、各点検項目の要件を満たしているかの確認を、作業委託者を含めたシステム保守者と議論することで自ら行った。

（ISMS に基づく方法）

- ISMS の運用により定期的に情報セキュリティに関する確認を実施
- ISMS の取組みにおいて評価、検証している

（CSOC の指摘に基づく方法）

- CSOC からの指摘に基づいたセキュリティホールへの対応指示
- 情報セキュリティ事案発生の際はその事例を元に、また本社組織（CSOC 等）からの指示なども含めて都度システム担当に確認の指示を行っていた。
- csoc の指摘事項をベースに検証などを実施

（アカウントの管理による方法）

- システムアカウントの棚卸により、不要なユーザが登録されていないか、不要な権限が付与されていないかの確認を実施している。
- 転入出時におけるアカウント管理の徹底
- アクセス権限一覧を提出させ、適切な更新ができているか確認等

（その他の方法）

- 入退室ログと実態との突合チェック
- 不正操作がないか等、定期的にログ確認を実施
- 本社から送付の点検シートによる再検証を実施

【質問 1⑨】「①内部者による不正情報流出リスク、②システム管理者又は運用保守従事者による不正情報流出リスク）に対し、自らの所管する組織・部署の情報セキュリティ体制がどの程度脆弱であるかを検証・評価するにあたり、その前提となる情報が的確に自らに届いていると思いますか」（質問 1⑧）との質問に対して、「どちらかというと、そう思わない。」又は「そう思わない。」と回答した場合、そのような状態が生じている原因・背景として、お考えのことをご回答ください。そのように考えるに至った具体的なエピソード（いつ、どこで、誰が、何をしたか等）があれば、併せて、ご回答ください。

【結果】

（チェックシートの問題点を指摘するもの）

- チェックシートだけでは、システムに関する情報がすべて報告しきれていないと思う。
- セキュリティチェックシートや委託先チェックシートの内容が形骸化されており、なぜそのチェックシートの項目の確認が必要なのか説明を受けていない。
- 管理簿・点検マニュアルが現場の実運用をしっかり踏まえた上での内容としては不十分であり、かつ複雑で意図が解りづらく、非常に使いづらいと考える。何を目的にしているか、明確に理解でき、シンプルで日々運用しやすい内容に根本から見直すべきである。

（役職員の知識不足等を指摘するもの）

- 対象のシステムが多すぎることと、その他業務量が多すぎるため社員本人の意識がついてきていない
- 管理する側が、システム仕様を十分に理解していないため、チェックシートや報告物の正当性を十分に評価することができない。担当者の報告内容を信用するしかない。特に担当者がそれで良いと思い込んでいた場合、それを指摘、是正することが不可能に近い。
- 自主点検のチェックシート項目それぞれの意味をチェックを関係するメンバー全員が理解できていると思えない。事例が発生するごとに、チェック項目が雪だるま式に増加した結果、分かりにくいマニュアルと膨大なチェック項目となり、チェックする優先順位がなく、確認行為が形骸化してしまっているのではないか。

（検証・評価の役割分担・運用に問題があることを指摘するもの）

- 毎月点検等の実施報告等の依頼は届いているが、自組織にあった点検の正しいやり方を自組織以外から指導されることがないため、自組織で実施している方法が間違っているのか明確に確認を取らないまま運用してしまっている。
- 複数のシステムを管理しそれ以外の業務も掛け持ちしているので、問題が起こるまでは報告は届かないと思われます。
- 着任前から維持管理しているシステムであり、担当者からの報告を元に判断しており、自ら検証・評価はできていない。
- システム主管と利用部門の責任がハッキリしていない。検証・評価は定期的かつ自主的に実施するものかなか？一定の指示に基づいて実施するものなか、そのあたりは社内的に明確になっているのでしょうか？

【質問 2③】「自らが所属する部署における、お客様情報の日常管理は適切に実施されていると思いますか。」（質問 2①）との質問に対して、「適切かつ十分な方法で実施されている」と回答した場合、そう考える理由をご回答ください。

【結果】

（ルールに則った運用がされていることを理由とするもの）

- 情報セキュリティ指針などのルールに則り実施されているため
- 毎年の情報セキュリティ研修で注意喚起される内容は、理解し実践している。
- ＮＴＴ西日本のセキュリティ指針に従った運用を行っている。
- ルールに則った方法で管理を実施しているため
- USB の扱いについては、マニュアルのルールに沿って実施して頂いています。
- マニュアルに基づき実施しているため
- 情報セキュリティマネジメント規程に則して運用を実施しているため
- 情報セキュリティの指針に基づく各種管理ルールを遵守しているため。
- 規則に基づく運用をしている

（物理的な措置を理由とするもの）

- アクセス権、パスワードの管理を実施しているから。また USB メモリの利用は不可としている。
- アクセス権限は服務指定簿を作成、各システム担当に服務指定簿を送付てアクセス権限を取得。USB メモリは指紋認証端末限定（使用者限定）を服務指定簿作成、課長承認時のみ使用可能。端末使用は、事務所内のみ使用可能、事務所への入室は入館・入室許可申請を行い許可後、システム登録した社員のみが社員証・パートナーカードを使用して入室可能
- 抽出端末が限定されており、USB 接続等についても、運用ではなくシステムで管理されているため。
- アクセス権限管理、USB メモリの利用都度：管理簿に記述、管理者のサイン（私の担当内で実施）。端末設置場所の入退室管理（総括担当で管理）：社員カードで管理。私の担当では十分に行えているが、その他のところは評価しがたい
- ソフトで USB 制御していること。また、入退室は社員のみ可能であり、指紋認証 USB のみ使用可能であること。
- USB は利用禁止にしているため、外部に持ち出せない。
- USB 持ち出し等、テクニカル的に実行不可な環境となっているため。
- そもそも、USB は利用できない。権限も適切に付与している。しなかったことに対するリスクを把握して業務を実施している（これが重要だと思います）
- アクセス権限、パスワードの管理、入退室管理は、個人単位で厳格に管理されている。USB メモリは使用できないシステム仕様になっている。
- 会社指定の USB 以外利用できない様に制限されている。端末設置場所については、入退室管理ができる社員証または生体認証を利用
- USB 利用禁止等、適切に実施されている

【質問 2④】「自らが所属する部署における、お客様情報の日常管理は適切に実施されていると思いますか。」（質問 2①）との質問に対して、「実施されているが、不適切な方法又は不十分な方法等で実施されていると思う。」または「実施されていないと思う。」と回答した場合、どのような点についてそのように思いますか。不十分又は実施されていないと思う事項をご回答ください。また、具体的な場面やエピソード（いつ、どこで、誰が、何をしたか等）があれば、併せてご回答ください。
（※管理責任者等と一般社員の両方が対象）

【結果】

＜管理責任者等の回答＞

（実施されていないことを指摘するもの）

- ルールが徹底できていない場面を目撃することがある。例えば 2 段階認証の設定が必須だが、していなかったというケース。
- 日常管理を実施しない、もしくは不適切に実施している社員が多い。性善説に立った日常管理が行われているため、不正を行う社員の発見および制限を行う事が出来ない。

（ログの管理状況について指摘するもの）

- アクセス者の絞り込みは掛けているものの（情シス担当者のみ）データを持ち出された実績を追いかける方法しかなく、対策が事後対応のものとなってしまっている。
- アクセスログ等の確認について、十分に行なえていない部分があると思われる。（定期的なチェックが形骸化している面も含めて）
- アクセス権限の管理、ログ監視が十分でない点がある。
- ログ等の取得、確認が実施されていなかった
- ログの確認がとれる環境が整っていない点
- 業務外利用の禁止措置について、システム利用ログ確認の定期実施がなされていないから

（ルールの形骸化を指摘するもの）

- 多岐にわたるシステムが過去から現在に至るまで運用されているが、部署全体で見れば、ルールが形骸化されており、特に年数が経っている今回の事案を発生させたシステムなどは、新たに発生する脅威への対処が適切に講じられていないため（今のガーディアンチェックでは通らない）
- 適切な管理、運用方法になっているものの形骸化している部分が見受けられる

（役職員の知識・経験不足を指摘するもの）

- 運用上のルールは決められているが、それを守るかどうかは作業者の良心にゆだねられている面がある。また、ルールが規定されているマニュアルも、例えば、お客様情報とは何かが、明確に記載がなく、読み手によって判断が異なる恐れがあると感じる。
- 今回の事案を受けて、改善した結果は、今は適切に実施できている。これまでは、不十分なところがあった点については、知識・理解不足（システムの対する知識・理解不足）、及びチェックの煩雑性が要因だと思う。管理表が紙・サインで行われていたり、エクセル管理されていたりと、チェック自体のフィージビリティが低いのも要因ではないか。

＜一般社員の回答＞

（外部記憶媒体の管理状況について指摘するもの）

- USB メモリは持っていないが使用可能ではある。
- 私有の USB メモリは利用可能のため悪意をもって隠しもって入れば持ち出しが可能。ただし管理者の権限をもつ人による
- 指紋付き USB（及びデータ移動用端末）の利用管理簿：承認者不在・リモートワークの機会が多く手書きの管理において承認者のサイン（事前と事後）取得時メール等で承認の証跡を残すとあるが運用上煩雑である（全体で月１００～４０件)、ため実際には行われず、担当間ダブルチェックを行っている（事後のサインは取得）
- 私有の USB メモリの使用が可能だった

（ログの管理状況について指摘するもの）

- 改善中かと思うが、データの書き込み・郵送など記録を取っていないように思われる時があった。
- 各種システムの利用ログやお客様端末へのリモートログインの履歴（いつ、誰が作業した等）が残っていない。また各システムを共用の ID で使用しているため、誰が操作したのか不明瞭。
- 内部調査で、外部媒体の使用管理に問題があり現在は是正したが、ログの取得等ソフトウェアの仕様に関わる部分は、是正の目途が立っていない。

（アクセス権限の管理状況について指摘するもの）

- 退職者、異動者のアカウント削除が依頼から実施までリードタイムが長い（数週間）
- アクセス権限・パスワードの管理：昔から不要なユーザーに完全アクセス権限が付与されており、やろうと思えば中身を見たり、修正したりすることは現状でも可能。また定期的なパスワード変更機能やパスワードの規則(英数字と記号を含ませる等)の機能はそもそも実装されていない。
- アクセス権が適切に設定されていない。該当システムでは無駄に完全アクセス権（フルアクセス）が設定されていた。
- 保守端末へのログインが同一アカウントで行われている

（ルールの形骸化を指摘するもの）

- クラウドサービスの ID 払い出しやアクセス権限の設定において、管理者の意思決定プロセスがない。慣例的な作業手順の申し送りはあるが、ルールや作業手順は明確でなく、どんなリスクがあるのか管理者は把握できていない。
- 業務は営業担当のバックヤードとして勤しんでいますが、調査依頼を依頼される場合は依頼方法や問い合わせに対し回答など明確なルールが設定されていないため、個々人で運用の仕方が異なっていると感じています。
- 形骸化、陳腐化している。情報システムや情報セキュリティは日進月歩であり、業務環境も変化しているにもかかわらず、社内規定が基本的には昔からのままであるため運用等に無理が生じているように思う。
- ルール上、禁止項目とされているが、システム的に完全にロックされている状態ではない為、抜け道はあると思うため。

【質問 2⑤】自らの所属する部署におけるお客様情報を取り扱うシステムの日常的な情報管理について、質問 2①等でお答えいただいた以外に、問題意識（気になっている点、おかしいと感じる点等）、お考え、要望、改善提案等がありましたら、ご記載ください。併せて、そのように考えるきっかけとなった具体的な場面やエピソード（いつ、どこで、誰が、何をしたか等）があれば、ご回答ください。（※一般社員のみが対象）

【結果】

（現状について理解できていない旨指摘するもの）

- お客様情報に直接触れる機会がないためそれ以上はよくわからない。
- どのような対策を行っているかよく知らない

（情報セキュリティに関する研修・指導が必要である旨指摘するもの）

- 新しいサービスで新しいシステムを作成する際に、セキュリティ的に管理することや管理簿などの必要性について、アドバイスできるような環境があればよいと思う。
- 情報セキュリティに関する教育やトレーニングをこのようなアンケート形式でも良いので定期的に行うのはいかがか。時間のかかるものではなく、簡素なものでよいと思う。セキュリティ事故を起こさせないために意識に植え付けておくことが目的。
- 適切なルールの周知徹底が圧倒的に不足。情報セキュリティのルール・制度を持つ主管から、利用部門のミクロな単位に、「制度・ルール・運用」面での正しい理解を促進する営みが必要。「メールや動画をみておいて、勉強して、ルール守ってください」では、正しい運用が理解できないし、利用者の知識レベルも統一しないと思います

（マニュアルが不明確・難解である旨指摘するもの）

- それぞれの立場での取扱いに関するマニュアルの指示がすこし不明瞭に感じます。
- 諸々の規定が多ファイル、多ページあるため他の業務と並行してこれらをすべて読解するのは困難。ベストプラクティスの提示・AI チャットボットによるセキュリティに関する問合せの即回答を希望します。

（アクセス権限に不備がある旨指摘するもの）

- お客様情報保護の観点ではよいことだと思うが、アクセス権限・パスワードの管理が厳しすぎると思われる。いざというときに柔軟な対応ができない。
- 派遣社員がシステムから情報を抽出できることが問題かと思いますが、現時点では業務上必要で、派遣社員の情報抽出の権限をなくすには人材が必要。
- 業務で仕方ないと思いますが、閲覧権限などがざっくりと振り分けられている印象があります。

（人的リソースが不足している旨指摘するもの）

- 右肩上がりの事業計画に対し、管理者・社員一丸となった懸命の努力により達成してきた。その一方、経年的な重要課題となっているリソース不足について、上位に対し毎年相談してきたが、解消に至っていないのが実態（組織再編の影響等から、むしろ減員傾向が継続）。

【質問 3②】「情報セキュリティに関する各種の自主的な点検（毎月点検、四半期点検、保有状況点検、システム自主点検等）の実施状況について、ご自身のお考えをご回答ください。」との質問（質問 3①）に対して、「適切かつ十分な方法で実施されていると思う。」と回答した場合、各種点検の正確性・信頼性が十分に担保されていると考える理由をご回答ください。

【結果】

（ルールに則った運用をしていることを理由とするもの）

- お客様情報保護運用マニュアルに則り、実践している。
- 情報セキュリティ指針に従った運用とチェックと上部組織への報告を行っている。
- ルールに基づき、クロス点検も含めた各種点検（毎月、四半期点検 etc）を実行しているから。
- ルールに基づいて適切に処理しているため
- 運用マニュアルに沿って、適正且つ確実に点検を実施しているため
- ルールに沿って点検を実施している。
- 実施要領やルールに基づき管理対象物の現認や服務指定管理簿等の確認を欠かさず実施しているため。
- 点検フローに則って実施されている。
- マニュアルに則って実施しているため
- マニュアルに従い、手順通りに実施しているため
- ルールに遵守した運用を実施しているから
- 運用ルールに準じて実施していることから

（複数名の目で確認を行っていることを理由とするもの）

- 複数の社員がチェックしそれを上長がチェックし、更にはタスク間のクロスチェックを実施しているため
- 毎月、ミーティングで周知して実施しているから。
- 数名で実施し、自分自身も最終確認しており、気になる点はきちんと質問等のより解消しているから
- 各種点検は私だけでなく、点検マイスターとのダブルチェックで期限通りに実施している
- 担当者と管理者、その上位管理者による複数目線によるチェックがおこなわれているため
- 複数名による点検、クロスチェック等、目を変えた点検を毎回実施している。
- 複数のメンバーで厳格に運用している。
- 複数の管理者および関係者で情報管理体制をチェックしている為。
- 実施者のみのチェックだけでなく、お客様情報適正利用推進者によるチェック等、クロスチェック体制があるため。

【質問 3③】「情報セキュリティに関する各種の自主的な点検（毎月点検、四半期点検、保有状況点検、システム自主点検等）の実施状況について、ご自身のお考えをご回答ください。」との質問（質問 3①）に対して、「不適切な方法又は不十分な方法等で実施されているものがあると思う」と回答した場合、どのような点に問題があると思いますか。問題だとお考えの点検と当該点検の問題点をご回答ください。具体的な場面やエピソードがあれば、併せてご回答ください。

【結果】

（点検が実施されていないことを指摘するもの）

- 年１回点検は実施しているものの、毎月、四半期の点検は実施できていない。
- 一部組織で現場での認識不足があり定期点検が実施できていないことがあった。

（点検の形骸化を指摘するもの）

- 点検シートの内容が形骸化されており、なぜその項目の確認が必要なのか説明を受けていない。
- PMS,ISMS のルールに則り、チェックを実施しているが、システムの抱える真のリスクまでチェック出来ていないと思われるため。
- 実態を個別確認せずに、前回報告内容を踏襲（コピー）して報告してるケースがある。
- マニュアル基づき実施をしているものの、しっかりと内容を熟知して点検を行っていないケースも想定されるため。
- 点検項目が過多。点検内容が所作・手段を問うものが多く曖昧であるため、回答者の拡大解釈により、勝手に代替手段を以て OK としてしまうケースが発生し得る。これが世代交代を繰り返すことにより、結果的に形骸化につながっているのではと想定。
- 点検等は前回、前年度踏襲するケースが散見され、前回点検結果の妥当性について踏み込んだ確認を実施していない
- 業務繁忙により点検が形骸化している

（点検者への依存及び点検者の知識不足を指摘するもの）

- 担当者への依存具合が大きいため、システム的な点検を導入するべきだと考えている。
- システムの具体的内容を把握しているのはシステム主管のみであり、システム主管のさじ加減で点検結果を記入する事が出来る。
- 点検項目があいまいで、点検者のスキルに依存していると思う。
- 点検が多いため、頻度が高いほど形骸化してしまう。点検項目の解釈幅が広いケースがあり、対応者の技術水準に依存してしまう。

（点検のためのリソース不足を指摘するもの）

- 全部ではなく一部と思うが、忙しさやリソース不足を理由にちゃんと確認しないままで「OK」と出している事例があるのではないかと想定。
- 点検者の認識（スキル）に依存されている。
- 人により認識や稼働が違うため、実施の濃淡があると考えるため

【質問 3④】「情報セキュリティに関する各種の自主的な点検（毎月点検、四半期点検、保有状況点検、システム自主点検等）の実施状況について、ご自身のお考えをご回答ください。」との質問（質問 3①）に対して、「適切かつ十分な方法で実施されていると思う。」以外の場合、そのような状態が生じている原因・背景として、お考えのことをご回答ください。

【結果】

（点検の形骸化を指摘するもの）

- 過去のチェック内容を流用する等の形骸化
- 前の質問と同様であるが、定期点検についてはどうしても形骸化する懸念があり、我々の業務運営においてもグループ他社、他部署で発生した情報セキュリティ事故を我が事化した点検項目を追加する等、随時形骸化防止に努めているところではあるが、どこまで徹底すれば良いのかという基準が無く万全であるとは言い切れないため。
- お客様情報管理においては、性善説たった対策と認識しており、形骸化も考えられる
- 日々の業務に追われ、点検項目が煩雑であることもあり、点検行為自体が形骸化している。人事異動の度に従事者が代わり、十分な引継ぎ等が行われていない。点検項目の意味がわかりづらいものがある

（業務の繁忙・人的リソースの不足について指摘するもの）

- 時間やリソース、スキル、重要性の認識、インセンティブなど、多くの問題が複雑に関係した結果であると思う。
- 業務が多忙であり、実施している余裕がない。
- 対応業務が多く、手が回らない。
- 慢性的な社員不足や委託費の削減要求による稼働逼迫により、業務サイドへのサービス提供へ稼働を優先する必要があるため、点検業務等が後手に回りがち
- 忙しさやリソース不足、業務量の著しい増に対して人は増えない（増やせない）ため→人事の枠の問題、収支の問題（費用を抑える）

（点検者の知識・経験不足について指摘するもの）

- 自身のスキル未熟、課題認識、問題意識の希薄性
- 知識・ノウハウの不足のためシステム化が不十分
- システムスキルを持った人材不足、ノウハウを持った管理要員不足など人的な要因が大きいと判断する。各システムの開発時の担当者が人事異動等でいなくなると後任者の知識・管理レベルは低減していく

（点検項目の不備について指摘するもの）

- 点検の管理簿自体を見直す必要がある。誰が点検しても、目的や意図、点検するポイントが直ぐに理解でき、同じレベルで適切に対応できる内容に見直して頂きたい。（社外のノウハウを導入する必要があるかもしれません。）

【質問 3⑤】自らの所属する部署におけるお客様情報を取り扱うシステムの各種自主的な点検について、上記でお答えいただいた以外に、問題意識（気になっている点、おかしいと感じる点等）、お考え、要望、改善提案等がありましたら、ご記載ください。併せて、そのように考えるきっかけとなった具体的な場面やエピソード（いつ、どこで、誰が、何をしたか等）があれば、ご回答ください。

【結果】

（管理方法の改善が必要であると指摘するもの）

- 各システムの権限棚卸についてもう少し自動化してほしい。過去組織にいたメンバーの名簿と棚卸リストを手作業で照らし合わせるなどチェック者の稼働負担が多く見逃す可能性も高い。
- アナログ的なチェックが膨大になってきており、形骸化しやすいのではないかと思っており、業務プロセス見直しやチェック稼働の低減化などをセットで検討している。

（管理体制の改善が必要であると指摘するもの）

- 日常の点検においては不備が無いことを前提としているが、不備を見付けること、不備を解消することを前提とした意識改革が必要と考える。また不備が見つかった際に本社の対応スタンスは、現場での対応、報告を逐次求めるようなスタンスでは無く、特設チームが現場に入り込んで現場をサポートする等、実効性のある仕組みづくりが必要と考える。
- 社内に専門的な知識を保有する人材が十分いるわけではないため、具体的な課題抽出・改善策の実施にあたり、今以上にN西本社等からの支援体制の充実があることが望ましい。
- 情報セキュリティは守るだけではないので、システムや業務運用を俯瞰的にみて情報セキュリティリスクがどこにあるのかを洗い出し、そのリスク管理（許容するのか、軽減するのか、保有するのか）を議論する仕組みを作る

（役職員の知識・経験不足を指摘するもの）

- 社員の長期配置ができず、スキル・ノウハウが蓄積できない。そのため、人材派遣社員等に頼らざるを得ないことにより、適正な管理ができず、不正に気づけず、見逃してしまう
- セキュリティに関する知識および意識が低くても、システム主管の役割を与えられて従事している社員が多い。

（点検シートの見直しの必要を指摘するもの）

- 点検シートの定期的な見直しと更新により形骸化を防ぐとともに、実際の脅威等を取り入れた抽象的でない具体的な項目を追加することで、実践的で効果的な点検が可能になると考えている。
- 似たような点検が毎年実施されている。そんな中で点検に対する稼働を十分に確保できておらず、重要性の相互理解が進んでいないように見える。シンプル化し、誰が見てもわかりやすい方法で自主点検を進められるようにやり方の見直しをしていただきたい。各種点検（毎月点検、四半期点検、保有状況点検、システム自主点検等）のフォーマット統一化等。

【質問 3⑦】「各種の自主的な点検（毎月、四半期点検、保有状況点検、システム自主点検等システム自主点検等）のチェックポイントを確実に実践できていれば、想定される情報流出経路からの情報流出は有効に防止できると考えていましたか。」との質問（質問 3⑥）に対して、「いいえ」と回答した場合、想定される情報流出経路に照らして自主点検のチェックポイントだけでは十分でないと考えた理由と、追加すべきチェックポイントをご回答ください。

【結果】

（追加の物理的な対策が必要であると指摘するもの）

- 悪意ある人間の恣意的な情報流出を止めるのは、システム構成の見直し等の物理的な対策が一番効果的であると考えられるため。
- 自主点検は自己申告ベース（システム保守に携わるものが点検）のため、性善説が前提のため。システムよる確認（ログ等）や（システムに強い）第 3 者によるチェックが必要

（チェック方法の改善が必要であると指摘するもの）

- チェックシートポイントが実態と合ってなかったり、ポイントの内容を十分理解した上でチェックできていないことがある。チェックポイントに関する説明、資料が不十分である。
- チェックポイントがあいまいさを残しており、点検者の判断で正常か否かを判断してしまっているのではないか。
- 自主点検のチェックシートの質問内容を確認した際、点検実施者によってさまざまな解釈が可能ではないか、と感じたため

（その他の手段によるべきとするもの）

- システム的な自動チェック（AI を活用したインシデントチェック、アラーム発出などのテクノロジーの導入）の導入をしたとしても、人が介在する以上、完全に防止する方法はないと考えているため、最後の抑止力として、損害賠償を明記した誓約書へのサインや、同一業務へ同一人物を長期的に配置しない（人員増強が前提）などのルール化が必要だと思う。
- AI によるシステム内の振る舞い検知などを導入することで、チェックの即時性を高めることは可能と考えるが、人と業務が常在する限り未然に防止できる方法はないと考える。他では雇用契約書における損害賠償責任の明記、誓約書へのサインなど内部者等の心理的な抑止について工夫の余地があると考える。

【質問 7③】「自らの所管する組織・部署におけるお客様情報を取り扱うシステムについて、特定のシステム管理者又は運用保守従事者が長期間（3 年超）にわたり同一の業務に従事し続ける状況を情報セキュリティ上の問題として捉えていますか。」との質問（質問 7②）に対して、「情報セキュリティ上の問題として捉えているが、具体的な対策を講じるまでには至っていない。」と回答した場合、情報セキュリティ上の問題意識を持ちつつも、状況改善が困難な事情があれば、当該事情をご回答ください。

【結果】

（回答全般として役職員の人員又はスキルの不足を指摘するもの）

- 運用保守従事者を内製稼働で配置しており、後進の育成・スキルの継承ができておらず長期間の配置となっている
- 長期に同一人物による対応と、必要なスキル保有、一定のセキュリティが担保されている社内 OA 端末からのアクセスの観点から、現状の運用となっている認識
- システム管理従事者は高いスキルが必要であり、代わりの人材が不足している（育成出来ていない）
- システムの仕様を把握している SE スキルの移管に膨大な稼働と時間を費やすため
- システム管理者は専担者ではなく複数の総括的な業務を実施しており、現状は業務運営上全て 3 年で異動させるのは難しい状況
- システム管理者（開発、維持管理）として、専門的な知識を有する人材育成（リソース）が出来無い。
- システムの開発維持運用保守業務に関しては、ノウハウ定着までに多くの時間を要するため３年以上従事することが多々ある
- 当該分野にも十分なリソースが配分されるよう、人材リソース戦略を立てることが必要。
- 人材が不足しており、結果的に長期配置せざるを得ない状況
- 情報セキュリティに関する知識およびスキルを有する社員が少なく、従事する業務を定期的に変更する体制を有していない。情報セキュリティに関する対処や体制構築の必要性を理解せず、外注やクラウドを使用して低セキュアなビジネスを立ち上げる事に対して危険性を感じない、社員および管理職が多い。
- システム管理者を育成するのに時間を要するので、短期間で容易に変更できない
- 唯一無二の専門スキル者として重宝し続けなければならない個々の事情となっている。打開に向けてはスキル移管含めた後任候補との重複配置や、スキルレベルそのものを理解できる人材育成が合わせて必用。
- 特定のスキル者しか出来ない部分もあり、技術スキル・ノウハウ的に他の社員では厳しいところもある。また該当社員も実業務を持っており、サーバ保守や、端末保守・設置を業務としている専門家ではないため、技術スキル面、体制面、環境面と色々と難しい事があると想定している。
- システムに携わる中核社員は無期社員で、配置転換に限りがある。キャリアアップスキームもない。人手不足は人材派遣補充しかなく、従事させてしまっている。新たな人事制度で無期社員の流動性を高められるのは期待できるが、属人化した業務を平準化させられるかは課題。

【質問 7④】「自らの所管する組織・部署におけるお客様情報を取り扱うシステムについて、特定のシステム管理者又は運用保守従事者が長期間（3 年超）にわたり同一の業務に従事し続ける状況を情報セキュリティ上の問題として捉えていますか。」との質問（質問 7②）に対して、「情報セキュリティ上の問題として捉え、具体的な対策を講じている。」と回答した場合、どのような対策を講じているか、具体的にご回答ください（ログ監視の多重化、アクセス権限の限定化、権限者の分散化、定期的な配置転換等）。

【結果】

（ログ監視）

- ログ監視の複数人での実施
- システム保守者はノウハウもあり 3 年以上の期間保守者として対応しているものもいるが、システムを利用する際、A 区画での作業やデータダウンロードする場合は 2 人以上での監視、及び定期的なログ監視をしている。
- アクセスログについては毎週月曜にログレポートを受領し、長期間従事ユーザーの操作ログを確認

（アクセス権限の限定化）

- アクセス権限の限定化、及び管理者による作業管理簿のクロスチェックを実施
- システムへのアクセス権限は最低限なものに限定している。作業時は 2 人以上の作業者が相互に確認して実施する
- 必要な権限のみ付与する。複数人が見ている中で本番環境を触る
- アクセス権限の限定化や複数人での作業実施等。

（権限者の分散化）

- 業務に従事するものに対して、必要最小限の範囲でユーザー情報へのアクセス権(参照・更新・削除)を与え、エクスポート権限についても必要最小限の範囲で制限を行っている。また、「業務委託に伴う情報管理責任者通知書」でお客さま情報使用者と申請しているメンバーのみにアクセス権を絞っており、1 年に 1 回、アクセス権限の棚卸しを実施している。アクセスログについては毎週月曜にログレポートを受領し、長期間従事ユーザーの操作ログを確認している。

（定期的な配置転換）

- 長期配置者の計画的な人事異動の実施
- 定期的な担務内容の変更、定期的な勉強会によるセキュリティ意識の醸成深化
- アクセス権限の限定化、権限者の分散（複数名での実施）、定期的な担当替えなど

（物理的な措置）

- 外部媒体の利用を許可していない運用であること、保守に関するアクセス権限付与者を少人数に限定していること、セキュリティ自主点検や監査等を通じ定期的なチェックを行うことによりリスク低減を図っている。
- 業務委託メンバーは、入れ替わりが発生する。業務委託先の責任者は 3 年以上の配置となっているが、ログの監視や物理的に USB が利用できないようにする、情報セキュリティに啓発を行う等により、情報漏洩が発生しないようにしている。

【質問 8②】「自らの所管する組織・部署全体の情報セキュリティに対する意識について、どのように思いますか。」との質問（質問 8①）に対して、「情報セキュリティに関する諸ルールは守らなければならないという意識はあるが、他に優先すべきものがある場合は、ルールから逸脱することもある」と回答した場合、ルールから逸脱せざるを得ないのはどのような場合ですか。具体的な場面やエピソードがあればご回答ください。
（※管理責任者等と一般社員の両方が対象）

【結果】

＜管理責任者等の回答＞

（顧客対応を理由とするもの）

- 現場におけるお客様要望にその場で応える必要がある場合において、現場の判断で、ルールから逸れた対応を行っている可能性（リスク）を感じている。
- クライアント（外部企業・自治体）の判断により構築費用の削減を求められた場合。
- お客様影響が発生する場合
- お客様影響があるサービス・システムの故障
- トラブル対応時のお客様情報の扱い
- お客様へサービス提供している中で、迷惑をかけれないという意識があり、セキュリティ面が疎かになってしまっていたというのは多分にあったかと思います。

（納期・業務の繁忙状況等を理由とするもの）

- 重大故障などの場合にシステムへのアクセス許可などが後回し（記録が残っていない）になることがある。また、連日作業が続く場合に、作業記録等を残すことを失念していることがある。
- 業務運用上、セキュリティ確保にかける工数がない。納期が守れない。
- 費用も人員も足りない中で、スケジュール（納期）に追われているため
- 業務が忙しい時など、自らの確認を徹底せずに、点検者の報告内容を信じて承認したことがある。
- トラブル対応時にシステム情報を確認するためゾーン４へ入る際、撮影機能付き携帯電話を持ち込み、それでトラブルアクション会議へ参加するケースがある。
- 費用も人員も足りない中で、スケジュール（納期）に追われているため
- 業務が忙しい時など、自らの確認を徹底せずに、点検者の報告内容を信じて承認したことがある。
- 主に障害回復対応時などで個別情報がやり取りされていることはあると感じる。（逸脱していないかもしれないが）
- 運用ルールは守っているが、管理簿記載ではなく口頭連絡で作業を進める場合がある。
- トラブル時のお客様情報の管理、その後の削除まで含めた運用管理で確認が取れてなかった点

＜一般社員の回答＞

（顧客対応を理由とするもの）

- 既存システムではお客様への最適なサービス提供ができない場合。特に現場でお客様とやり取りされる方々は多いように感じる
- 装置の故障やシステムの不具合が発生することにより、お客様の業務に影響が出ている場合。またはお客様より設定関連の緊急のオーダーが入り、納期に間に合わせなければならない場合。
- お客様要望や稼働時間の削減
- システム不具合発生時に早急に問題を解決しなければならない場合に、動作ログ取得の為、保守端末に接続するが、この時に保守端末の作業内容を記入してからの調査等を行っていると、ユーザーに対しての影響が大きくなってしまう。

（納期・業務の繁忙状況等を理由とするもの）

- 将来的に諸ルールに合わせて対応する予定があっても、期日切迫などにより対応が後回しになっていると短期間的にもルールから逸脱していたと判断しました。
- システムを開発するにあたり、スケジュール遵守が最優先となっている。
- 工数見積、要件定義、設計といった上流工程において、セキュリティ対応が組み込まれていないことが多いと感じる。
- スケジュールの都合により業務スピードを優先してしまう時。例えば、お客様環境での作業で複数名による立会と確認が必要と定めているところを、単独で作業を進めてしまう場合。
- スケジュール重視で、セキュリティ対策は優先順位が下がる。順位が下がるのはセキュリティ対策の全てではないが、ルール決め等後回しになりがちなものが、そのままスケジュール重視で進んでしまい、万全な状態になかなか持っていくことができない。
- 対応期日等の求められるスピード感に対して、情報セキュリティ上の事務手続きが多すぎる
- 業務が忙しすぎる時は、お客様情報受け渡し管理簿のやりとりが遅くなったりする。
- 繁忙で対応が追い付かない
- 急ぎ上長承認を得る必要があるが、上長が不在な場合等
- 時間切迫など、確認する時間がない場合など
- 緊急性をようするシステム復旧対応等

（適式な手続を行った場合にかかる手間・時間を理由とするもの）

- エスカレーション先がわからないほど高いのに、リスクはごく少ない場合。
- スピーディな対応が求めら、かつルールを多少逸脱しても問題が顕在化しないと想定される場合。
- 意図的な逸脱ではなく、ルール全ての把握・網羅、また前述のリソース問題等から、そこに目も手も回らなかったのが実態。
- お客様情報の受け渡し管理簿など、遵守した場合の稼働、手間が現実的ではない場合

【質問 8③】「自らの所管する組織・部署全体の情報セキュリティに対する意識について、どのように思いますか。」との質問（質問 8①）に対して、「情報セキュリティに関する諸ルールは守らなければならないという意識はあるが、自らの所管する組織・部署には適合していないと思う場合は、その部分は守らないこともある」と回答した場合、情報セキュリティに関する諸ルールが自らの所管する組織・部署には適合していないと考える部分はどのような部分ですか。どのような部分がどのように適合していないか、具体的にご回答ください。
（※管理責任者等と一般社員の両方が対象）

【結果】

＜管理責任者等の回答＞

（ルールが個別のサービス・システムに適合していないことを理由とするもの）

- NTT 西日本の情報セキュリティ推進部門が策定した規程、マニュアル、ルール等は、商用サービスを展開する NTT ソルマーレには適合しておらず、同等レベルでの運用は困難である。
- 事業化業務に準じた内容のルールが規定されていることが一部ある点
- NTT 西日本が現在策定・運用している規程、マニュアル、ルール等は、単一の古いモノリシックアーキテクチャを想定してつくられており、時代遅れのルールや制度になっていると考えている。
- 取り扱う情報のレベルが高いのに、セキュリティ意識の低い社内ルールがビジネスの立ち上げ時から持続している。

（役職員のスキル・経験・意識等を理由とするもの）

- 設問の内容とズレるかもしれないが、セキュリティが重要と考える人と考えない人の差が激しい。セキュリティを遵守することが評価される会社ではないため、守らずに効果を最短で出そうと考える人間が必ずいる。
- 情報システムは一つの部署で完結するものばかりではなく、多くの部署が複合的に関与しながら実現している。自部門で管理可能なものは統制できるが、それ以外は統制できないケースもある。具体的には、情報システムやサービスの開発主管はバリューデザイン部であっても、保守や受付の主管はカスタマーサクセス部であったり、販売側に一部情報を渡す場合はエンタープライズビジネス営業部やスマートビジネス営業推進部に権限を付与することもある。現場の設置工事業務はフィールドテクノ社などが実施している。これらの組織が再編によって後継組織に引き継がれていくと、全体像を把握している人が少なくなり、形骸化が起こる。
- 情報システムは一つの部署で完結するものばかりではなく、多くの部署が複合的に関与しながら実現している。自部門で管理可能なものは統制できるが、それ以外は統制できないケースもある。具体的には、情報システムやサービスの開発主管はバリューデザイン部であっても、保守や受付の主管はカスタマーサクセス部であったり、販売側に一部情報を渡す場合はエンタープライズビジネス営業部やスマートビジネス営業推進部に権限を付与することもある。現場の設置工事業務はフィールドテクノ社などが実施している。
- これらの組織が再編によって後継組織に引き継がれていくと、全体像を把握している人が少なくなり、形骸化が起こる。

（ルールの複雑さを理由とするもの）

・ ルール運営や解釈に幅があり、ゼロイチで判定がむつかしく、現場での解釈幅が許容されいると思う。また、ルールが一律で、特にクライアント要請に柔軟に対応すべき部署やシステムでは、最大幅で運営せざるを得ない状況が存在するのでは。その幅が、組織的な責任で認知設定できていない。

＜一般社員の回答＞

（ルールが個別のサービス・システムに適合していないことを理由とするもの）

・ お客様情報を含むデータベース(WINKS)にはアクセスするが、自分の所属するチームではお客様情報を USB で持ち出す業務はない。したがって、同部署内の別チームには必要であってもこちらのチームでは適合していない(過剰)なルールがある。
・ 受託業務でお客様と共に利用するシステムなので、お客様環境や事情によっては十分な制限がかけられない場合がある
・ 委託先に対する立入検査等について、相手は独立した会社であり、その会社の事務所に入って取扱い状況（ファイルサーバや書庫など）を目視チェックするようなことは現実的なのか疑問に思う。現場にとっては非常に負担となるため努力目標であれば規定から削除してほしい。
・ お客様情報保護運用マニュアルについては　USB利用や入退室管理簿など様式などは利用しているが、利用対象から ProCX は外れており、様式も少し合わない箇所は省いたり工夫しながら利用しています。パスワード・スクリーンセーバーについもコールセンタ業務で色々な方が利用し、コールがいつ入ってい来るか不明でスクリーンセーバーを外す作業をしていると受付するのに時間が掛かる。

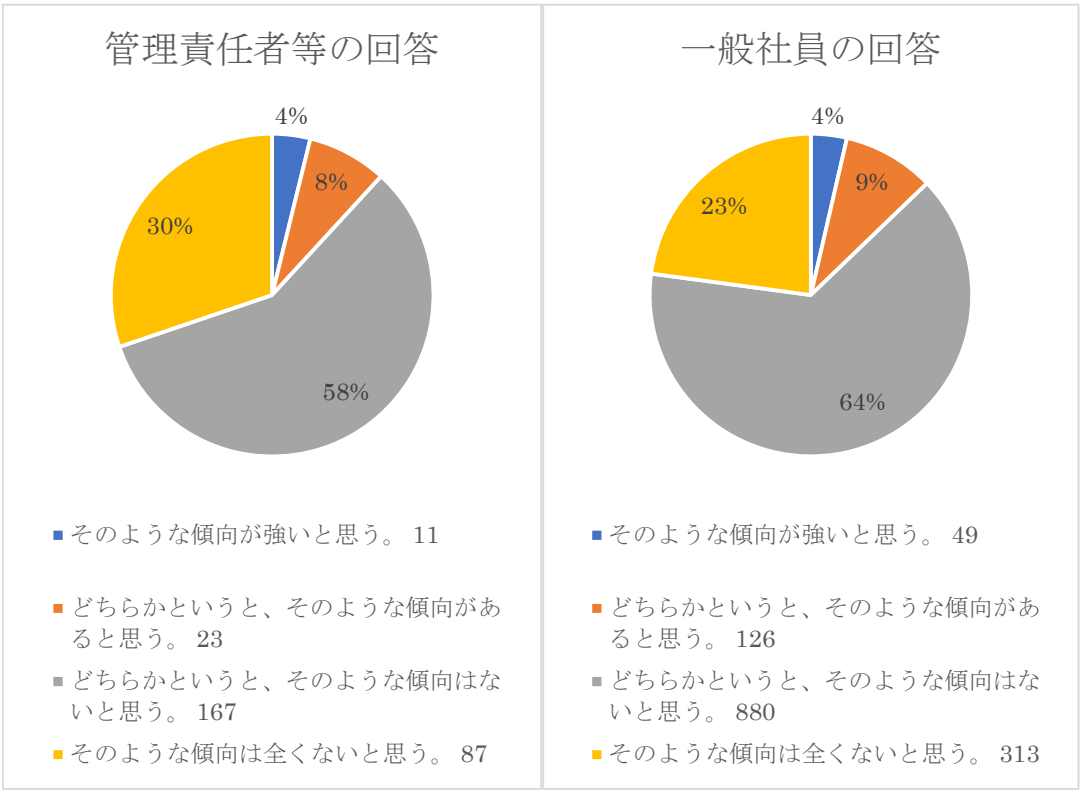
（役職員のスキル・経験・意識等を理由とするもの）

・ このケースはこう処理すれば問題ないというような情報が圧倒的に不足しており、そもそもルールがどうなっているかの正しい知識を持つものもいないと感じる。（上長に確認しても人によって回答が違う。）

（ルールの複雑さを理由とするもの）

・ 守らないという意識はないが、紙を前提とした定義や解釈が複数できる内容もあり、結果として守れていない場合があると考えている。
・ 守らないというのは言い過ぎだが、徹底的に遵守というのも違うと思ったため選択した。マニュアルの文言通りだと厳しく読むと順守するのは無理なルールが多い。セキュリティと業務効率は相反するため、業務に応じてマニュアルを作るべきであり、業務共通のマニュアルとしては今のマニュアルは細かいところまで指定しすぎており、業務と矛盾を生んでいる。

【質問 8⑧】自らの属する組織・部署において不祥事が発生した場合、その真因分析や再発防止に向けた対応よりも、誰の責任かという個人の責任問題が重視される傾向があるかという点について、ご自身のお考えをご回答ください。
（※管理責任者等と一般社員の両方が対象）



【質問 8⑨】「自らの属する組織・部署において不祥事が発生した場合、その真因分析や再発防止に向けた対応よりも、誰の責任かという個人の責任問題が重視される傾向があるかという点について、ご自身のお考えをご回答ください。」との質問（質問 8⑧）に対して、「そのような傾向が強いと思う。」又は「どちらかというと、そのような傾向があると思う。」と回答した場合、そのように考えるに至った具体的なエピソード（いつ、どこで、誰が、何をしたか等）があれば、ご回答ください。
（※管理責任者等と一般社員の両方が対象）

【結果】

＜管理責任者等の回答＞

（個人の責任が問われることを指摘するもの）

- ミスや失敗をした場合は、からなず、「誰が」を確認するから
- 上司は、全ての業務において、現場実態（業務量）を正確に理解しようとせずに、担当ができていないことの管理責任を各課長に問うシーンが多い。そもそも上司も所掌領域が広すぎて余裕がない状態となっている。
- セキュリティ事案ではないが日常的に発生する様々な事象について誰の責任なのかが最初に議論されることが多い
- 情報漏洩事案は”属人”の行為が原因となるケースが圧倒的に多く、再発防止等を講じるに際しては個人の責任問題に結果的に帰結する場合が圧倒的に多いと考えるため。

（責任を押し付け合う傾向にあることを指摘するもの）

- 情報セキュリティだけでなく役割の考え方が完全に縦割りであり、あるべき論で業務を押し付けあう傾向があるため。例：毎年の ISMS 監査におけるシステム面について弊担当に全て対応を求めるなど、仕組み体制を理解しようという気概が感じられない。
- お客様対応を日々実施しているセンタ等において、誤請求事案等生じた際、本来ならシステムで制御するべきものが予算不足のために機能具備できず、「手動や目視での運用」で投入するケースが多々ある。人による作業のためミスを０％にすることは至難であるが、情報セキュリティ委員会等において当該オペレータの上長のマネジメント不足ということで個人が処分対象となるケースがああった。手運用せざるを得ない場合において、日々お客様情報と向き合っている社員はリスクと隣合わせのため、処分方法や責任の在り方について、検討いただきたい

＜一般社員の回答＞

（個人の責任が問われることを指摘するもの）

- 不祥事の事案はないが、PJ 遂行において犯人捜しが行われる場面があった。
- 不祥事ではないが、システムトラブルが発生した場合を想定して保守的な姿勢となっているなと感じる（一方、トラブルが多発すると対応稼働がかなりひっ迫するため仕方ないとは思う）

- 「いつのどれ」というよりも、噂好きの社員さんたちが犯人捜しをひそひそする場面が多い。
- 幸い自分が所属しているチームではそのような経験はないですが、他チームの方から、真因分析の名のもと報告書類作成や対面面談などに多大に時間を取られているという話を聞いたことがある。
- 人為的ミスが発生した際だれが対応したのか社員が問い詰めることがあった
- 普段の仕事での些細な人為的ミス等も、解決策よりも誰が？どこが？と問い詰めるシーンをよく目にする
- 不具合トラブル時に原因究明を行う中で個人にたどり着くため
- 情報セキュリティ上の問題が起こった時　役職者が朝礼で　名指しで事象を話した。業務の状況や仕様を理解せず説明したため　●●さんの責任で…という印象を強く受けた。
- 具体的な事象はあげれないが、真因の掘り起こしをする過程で誰が・何故そうなったのかを詰められる雰囲気は強い

（責任を押し付け合う傾向にあることを指摘するもの）

- 経験があるわけではないが、組織の縦割り間が強すぎると感じた時があった。
- アプリで致命的な脆弱性が見つかった場合に、開発者個人に責めがいくことがあった。（開発者が、本来の開発プロセスを逸脱していた、という原因もあるが…）
- ２～３年前に WING 端末アカウント（ＩＤ）の共同利用が不正だということを指摘すると、業務が滞ることを前上司に責任転嫁されそうになった。

【質問 8⑪】

「自らの属する組織・部署において不祥事が発生した場合、不祥事が発生したこと自体が自身の人事評価に悪影響を及ぼすか否かという点について、ご自身のお考えをご回答ください。」との質問（質問 8⑩）に対して、「そのような傾向が強いと思う。」又は「どちらかというと、そのような傾向があると思う。」と回答した場合、そのように考えるに至った具体的なエピソード（いつ、どこで、誰が、何をしたか等）があれば、ご回答ください。

（※管理責任者等と一般社員の両方が対象）

【結果】

＜管理責任者等の回答＞

- 月次の全社員向けミーティングにおいて、各種事案に関しては、起こしてしまった事より、どのように素早く対処するのかが重要であり、意図的ではなく不祥事となった場合などは特に、エスカレーションをしっかり行い、会社としての対処を一緒に進めていくというメッセージを、社長や情報セキュリティ担当者から発信している。ただ、採用形態がスペシャリスト（年棒制）である社員が多いため、自らのミスで事案可し、本来の成果が出せなかった場合、人事評価に影響を及ぼすと社員が感じていると思う。
- 業績評価において、インシデントを起こした社員の評価の相対評価を下げるケースを経験したことがある
- 不祥事が、誣告であったとしても、そのような事が話題になること自体がマネジメントの問題であるとのことで注意を受け、賞与の評価も低かった。
- メール誤送信案件があった際、派遣社員がやめることになったため。

＜一般社員の回答＞

- オープンに懲罰等の公表がなく、どう影響しているのかが不透明だと感じる。噂等で●●さんは XX で訓告受けているから、、とかが独り歩きし、その対象者が少し不憫な状況になると、そのせいで。といった雰囲気が出る時がある。
- 不祥事があれば各個人の責任が問われるのは当然のことと思います。
- 過去の事案で処分された実績について周知されているため
- 研修のなかでもそううたっている
- 不祥事があった部署の上長はいつも異動させられているから。
- 5 年前くらいにパワハラ関連で直属ではない上司が一時的に停職していたため。
- 「いつのどれ」というよりも、噂好きの社員さんたちが犯人捜しをひそひそする場面が多い。その「噂」が「印象」となって評価に悪影響がでるのではないかと不安である。
- インシデント報告した同僚から明らかに賞与が減ったという話を聞いたことがある
- 申込書紛失の情報漏洩案件が発生した際に人事処分も検討されていたから
- 自分自身の経験による、10 年以上前に情報漏洩（故意ではなく過失）の当事者となったが、人事的な影響は非常に大きかった。一度の失敗が、人事として致命的な影響を与えた

- 日常的に上司から、他の社員の悪口や問題点・評価への影響などを聞かされる機会があり、もし今の上司のままで不祥事が発生したとしたら聞いていた通りになるんだろうなと感じた。
- 以前の部署で、部下（不祥事した人）、上司ともに処分されていたため。
- 入社してからの人事評定は記録され続けるため、影響するんじゃないですかね？（人事に影響しないのであればわざわざ記録する必要はないわけで）
- 過去に昇級が見送られたことがあった
- 業務でミスしたという結果だけで評価が下がったことがある
- 情報漏洩とは違うが、停車中に追突されたのに、それを理由に評価が下がった。
- 不祥事や人為ミスがないことをタレマネの目標に入れているため、それが満たされなかったなって、人事評価が下がってしまうような状況がある。
- 10 数年前、お客様情報を紛失した事例が周知された際に、当時の上長（課長）が「紛失した人とその上司は D 評価（当時の最低評価）だな」と言っていた。

【質問 9②】「お客様情報の不正流出が対外的に公表された以降（令和 5 年 10 月 17 日以降）、自らの所属する部署、会社又は NTT 西日本グループにおける情報セキュリティに対する取組み状況についてどのように思いますか。」との質問（質問 9①）に対して、「実効的な取組みが行われている又は行われつつあると思う。」と回答した場合、どのような点が実効的だと感じていますか。ご意見をご記載ください。

【結果】

（全社的な点検・体制構築等を理由とするもの）

- 情セキ部が先頭に立って、すべての社内システムについて水平展開調査を迅速に実施した点。
- タスクフォース体制（本社）で対処する等、迅速に責任感のある体制構築がされている。
- 当社本社からＮＴＴ西日本本社の情報セキュリティ部門へ当該システムにおけるセキュリティ関連対応が適切であるかどうか監督してもらい、必要な措置を行う動きをしている。
- 会社として緊急調査を行うなどの取り組みが行われ、自身も自担当の調査を行った
- 「お客様情報所有システムの緊急調査」を受けて、社内での責任範囲（OPS 部/自部）の明確化と対処内容、対処期日を設けた対応などを担当者と対話するきっかけができた
- 緊急点検によりベンダへも確認している事
- 緊急点検に対する更といのレベルが、普段より深い。本気度を感じる
- 緊急点検を行い、暫定対策を策定し実行しているから
- 全社をあげてシステム対応等を行っているため

（USB の利用制限に関する対応を理由とするもの）

- USB の利用を廃止することが可能か検討している。あるいは、有効なログのチェックが可能か、検討している。
- USB 利用をやめてデータブリッジ化、ふるまい検知の導入等
- USB 利用に関するセキュリティの強化。少なくとも大量のデータを外部に簡単に持ち出せるような操作は、きびしく対策すべきだと思う。

【質問 9③】「お客様情報の不正流出が対外的に公表された以降（令和 5 年 10 月 17 日以降）、自らの所属する部署、会社又は NTT 西日本グループにおける情報セキュリティに対する取組み状況についてどのように思いますか。」との質問（質問 9①）に対して、「現状の取組みでは、不十分だと思う。」と回答した場合、どのような点が不十分だと思いますか。ご意見をご記載ください。

【結果】

（対応・チェックが形骸的であると指摘する回答）

- 本当にそこまで必要なのかという事項もある。すべてを金太郎あめ的に対応しようとしている気がする。
- 規程類、点検項目などが複雑化しており、不要そうな点検項目なども見受けられる。必要以上に点検項目を増やして形式的なチェックとなってしまうのであれば、重要な項目に絞って点検するなどの改善が必要と考えます。
- 総務省等外部向けに「対策を行っている」と公表するためだけのチェックなり対応であり、根本的に問題を解決しようとする対応が何もない。「定期チェックを実施するように改善した」という報告をする点検/ヒアリングに何の意味があるのか
- チェックを社員の稼働を膨大にかけて行っているが、本質的に実効性のある監査体制（通常業務の範囲で実施できる状態）にはまだ相当の時間がかかると思うため。

（予算・人員・スキル等のリソースが不足する旨指摘する回答）

- コスト削減をしすぎてチェック体制は十分でないと感じているため。
- ガーディアンや定期検査などチェック体制はあるが、サービス運用側の裁量が大きく、担当のスキル不足で正確な報告が行われないケースがありそうだと感じる。
- 情報セキュリティに対しどのように対処すれば良いかのスキルが足りない。
- 業務を行う人材の適正化、リソース設計の見直し、取得情報に基づく分析強化対策
- 性悪説での対処（ログ取得とチェック）に対応するシステム整備、チェック体制（人材）
- 幹部からの発信、情セキ部からの点検により対策機会が得られた点はよかったが、取り組み内容、予算措置、実行までの期間など実態として困難な部分が多く、対応が各システム主管に依存しているところがあると感じるため。

（グループ内における情報共有の不足を指摘する回答）

- NTT 西日本　情報セキュリティ推進部（関連タスクフォース）よりヒアリングシートによる各種点検が実施されているが、点検上　不備となる項目に対して　システム導入による対応策を検討しているがその導入費用について　社内をサポートする（費用支援いただける）情報展開が無い点
- まだ末端まで具体的な情報がおりてきていない
- 取り組み自体は行われているが、サポートが不十分であると感じているため。会社としての言葉はあるが、具体的なサポートが不足している。
- 情セキからの具体的な指示はないと思っている

【質問 9④】お客様情報の不正流出が対外的に公表されたことを受け、ご自身の情報セキュリティに対する認識や問題意識に何か変化はありましたか。もしあれば、どのように変化したかをご回答ください。
（※管理責任者等と一般社員の両方が対象）

【結果】

＜管理責任者等の回答＞

（具体的な改善措置が取られた旨回答するもの）

- 社員の長期配置の廃止（社員交流（人事異動）の推進）
- 会社として緊急調査を行うなどの取り組みが行われ、自身も自担当の調査を行った
- システム運用管理対策の具体的な検討の動きが始まった

（意識の改善がなされた旨回答するもの）

- 今一度、気を引き締めて、チェック体制を強化する必要があると感じた。
- 社会的な影響が非常に大きいと受け止めており、より一層の社員への声掛けを行うよう心掛けた。本当にセキュリティ対策がしっかり機能していることを様々なシステムのログを自身で確認することで実行可能性を見極める行動を起こした
- 担当するシステムのセキュリティに関する問題意識が高まった。
- リスクの積み重ねが大きな事象に発展すると認識し、リスクへの感度を高める必要性を感じた。
- これまでは、性善説に立った対策を講じてきたと認識しており、またログチェックなどのノウハウが十分でないことを改めて認識した
- 社員任せ、ベンダ任せとならいように保有システムのセキュリティ対策を自ら責任をもって確認しなければならないという意識を強くした。
- このような問題を決して今後起こさないために、言うべきことは言おう、NTT 西日本の文化を根こそぎ変えて行かねばと考えるに至っています。

（変化がない旨回答するもの）

- これまでの最低限のことは実施しているつもりであり、改めての認識はない。
- 変化はない。今まで通りしっかり取り組んでいく。
- お客様情報を守る事へ取り組みの重要さは、従前より理解しているし、課題のある管理簿やマニュアルだけに頼らず、自分なりの手法も推進してきているので、発生した事を残念に感じた以外は、何も変わらない。

＜一般社員の回答＞

（具体的な改善措置が取られた旨回答するもの）

- USB メモリの使用停止措置を行うために運用方法変更等の検討を進めている。
- 他人ごとではないと思いました。日ごろからセキュリティに対する意識はありましたが、情報システムグループ内でも改めて社内システムに抜け漏れがないか、キッティング作業の手順書見直し等も実施しました。
- 個人やお客様が特定できる情報が記載されている紙類や伝票は SS-BOX へ破棄しています。
- ファルダ内で共有していたお客様情報の削除を行った

（意識の改善がなされた旨回答するもの）

- お客様情報セキュリティの意識が低いと、社内システムの存在意味自体が危うくなることを認識した。これからは一社員として問題を発見するときすぐに上長と相談し、システムのセキュリティ設計について強化するよう呼びかけ続ける。
- 今までは他人事かのように感じていたが、今回の事件を受け再認識すべきと感じた。
- セキュリティ実装や認証・認可フローにおけるロギング、堅牢な設計などについてのスキル不足を解消するための継続的な取り組みについて、もっとしっかりしないとという危機感が強まりました。
- どこに流出の危険性が潜んでいるがわからないので、緊張感をもって業務にあたる必要があると再認識しました。
- 過去の慣習から引き継いで今も実施している業務に問題がないのかを強く意識するようになった。
- お客様情報管理の重要性を再認識するとともに、形骸化させないために何ができるのかを常に考え続けることが大切であると感じた。
- 自部署でも起こりうる事件だと思い、USB の使用について改めて慎重さが必要だと話し合いをした。
- お客様情報の不正流出が対外的に公表されたことを受け、社内でそのような事が今後起きないようにすることが使命であると考える。
- 顧客情報を扱うシステムは使わないといって、油断してた気持ちが引き締まった。メール等より一層注意を払わねばと思った。

（変化がない旨回答するもの）

- 特に変化はない。やろうと思ったことがない。
- 変化はなかった。今まで通りセキュリティを常に意識していきたい。
- 変化はない、普段からお客様情報漏洩はあってはならないことだと認識しておりお客様あっての商売である以上、順守するのは当然のこと。

【質問 9⑤】これまでご回答いただいた内容以外に、情報セキュリティという面で、自らの所属する部署、会社又は NTT 西日本グループの組織風土について、問題だと思うこと、気になっていること等があれば、ご回答ください。
（※管理責任者等と一般社員の両方が対象）

【結果】

＜管理責任者等の回答＞

（ルールと実務の乖離を指摘するもの）

- 電話交換機の時代からセキュリティの考え方が全く変化していないセキュリティのルールと業務とが乖離しているために「例外対応」や「セキュリティの穴」が意図的に作られざるを得ない状態であることを認識し、業務の変化に応じてセキュリティルールの変更と制御、抑止するべきポイントを集約・明確にし、コストをかけて、システム的に抑止する仕組みを導入するべきである
- 私たちのセンタのようにお客様情報を日々扱うセンタにはセンタに合わせて管理・監督方法があると思う。企画部門等と同じマニュアルで、同じ管理簿。指導する情報セキュリティ部門では現場（センタの実態）がわかってないと思う。部署ごとにルールを決めることは効率的ではないかもしれない。費用対効果も理解する。が、AI の時代、お金をかけなければいけないところはある。ビル改修より、システム改修し、投入エラーやエラーチェックの自動化等人に頼らない、人が起こせないような措置を取ってほしい。
- 規定類を定める、ルールを作ることだけではなく、具体的な対処策を技術的側面から支援し、確実に実行されているかを判断するところまでチェックする体制が必要だと思います。いくら規定類やルールを定めても、それをどう解釈してどう報告するかを主管部任せにすると、認識が甘いところでインシデントが起こってしまいます。一元的にチェックする組織と、主管部責任者の両方で、確実にチェックしていくことが必要だと思います。
- 改定された規程類のボリュームが多すぎて、咀嚼できず、実効性が低い。リソース不足を感じており、専門（専担）人材の配置やグループ全体で集約してコントールする、としてほしい。
- 一律の点検では形骸化するリスクがあるため、点検簿の管理等、運用面でカバーするのではなく、システム面の整備により、未然に故意の事案を防ぐとともに、過失による事案発生リスクから社員を守る環境構築が必要と考える

（人的リソース・スキル・経験等に関するもの）

- 人事異動などの機会にセキュリティのノウハウなどを引き継ぐのはかなり難度が高く、先にも述べたように時間の経過とともに低減していくスキルを補う方法を検討しない限り、有スキル者への依存が大きくなり今回のような事象につながるのではないかと判断する長期間の同業務へ従事させない体制とスキルの移転・向上のバランスを人事要員が少ない中でどのように図っていくかが課題となるように思われる
- セキュリティの重要性は伝わっていると思うが、インフラや運用担当任せになっており、知識不足の人が多いように思う
- 以前の項目に散りばめていますが、人材とコストの不足・一線二線の相互理解・電気通信事業とそれ以外の区分けは大きな課題だと思います

＜一般社員の回答＞

（形骸化したチェック項目やこれに伴う業務負担の増大などに関するもの）

- チェックシートやルールなど多く、理解が追い付かない。情報の在りかを探すことに時間と労力を要する。社員の異動時に十分引き継がれているかどうか。
- 事案が生じるとチェック等が多くなり直後は機能しても月日が経つと意識も薄れ、チェック等の形骸化がどうしても進んでしまいがちだと感じる。お客様情報は物理的に持ち出せないようにするなど人の善意に頼らない運用に見直すしか漏洩ゼロにする方法はないのではないでしょうか
- 細かなセキュリティルールが定められ、それを統括する組織も存在していますが、それを実行する現場には、わかってはいるがそれをやっている稼働がない、セキュリティルールを理解し、実際のシステム構成に落とし込み、運用できるスキルを持っている人物がいないという問題があり、絵に描いた餅になってしまっている現実があるかと思います。

（派遣社員等の管理に関するもの）

- 業務を外部に切り出してアウトソースすると、より自社で業務完結するよりも、強めのセキュリティ強度を構築しなければならないため、内製化かアウトソースかの投資判断にも影響してくると感じる。また、改めてエンゲージメントの向上が必要だと思った。
- セキュリティー面というわけではないが、組織風土として派遣社員や契約社員の方にも社員と同じような仕事を割り振りしている部署が多いように感じる。給料が高い社員は働かず、派遣や契約社員に大変なことをまかせすぎていることに不満を持っている人も多い。このような不満からエンゲージメントが低下し、セキュリティーを守るという意識が低下したのではないかと感じる。個人の資質にも問題がある場合があるが、働いている人を大切にする意識を会社が向上させる必要があると感じる。
- やはり正社員の減少が気になります。パートナー社員の方に１０年前であれば正社員がしていた様々な業務をしていただいてる現状ですが、細部にまで目が届かなくなってる部署もあるのかなと思いました。（社員、パートナ社員含め各個人のモラルに依存？仕組みとして防げるのがよい）

（人的リソース・スキル・経験等に関するもの）

- 管理をするためには十分な人的リソースが必須であるものの、業務にリソースが圧迫されており、全組織で十分な管理をすることは現実的に不可能と考えている。
- NTT 西日本グループの社員は、ジェネラリスト志向が強く技術的なスキルを延ばすことを怠ってきた人が多いように思う。そのため、情報セキュリティの仕組みを検討・構築する際に、一部の優れた技術的スキルを持った社員だけで対応することになり、多くの社員はその内容を理解できず、適切な情報セキュリティ対策を打てているか判断できない（今回の情報流出の対応でも、技術的な部分については、ほとんどの管理者は作業担当者の説明を受け身で聞いて、どこの場でもよく聞くふんわりとした質問をするだけ）。通信の生業にする企業であるため、そこに関わる最低限のスキルを全社員が身に着け、管理者は本当の意味で自社の情報セキュリティ対策に責任を持てるようにするべきだと思う。