（報道発表資料）

2026 年 3 月 30 日

NTT ビジネスソリューションズ株式会社

セキュリティ監視・分析サービスの高度化とインシデントレスポンスサービスの提供開始

～平時から有事まで、日々のセキュリティ運用を伴走支援～

NTT ビジネスソリューションズ株式会社（本社：大阪市北区、代表取締役社長：木上 秀則、以下、NTT ビジネスソリューションズ）は、サイバーセキュリティに医療の考えを取り入れ「セキュリティのかかりつけ医」として、自治体や企業が抱える課題に寄り添い支援を行う「Cybersecurity Primary Care」※1の取り組みを実施してきました。※2

この取り組みをさらに進化させるため、平時におけるセキュリティ監視・分析サービスの更なる強化に加え、セキュリティベンダーと連携し、万が一セキュリティインシデントが発生した場合にも迅速かつ的確な対応を可能とする、インシデントレスポンスサービスを、2026 年 3 月 31 日（火）より提供開始します。これにより、日常的な運用からインシデント発生時の検知・初動対応、復旧支援、再発防止にいたるまでを一貫して支援する、伴走型のセキュリティ運用を実現します。

※1 「Cybersecurity Primary Care」の HP：https://www.nttbizsol.jp/service/cyber-security/

※2 地域社会のサイバーセキュリティ意識を高める「Cybersecurity Primary Care」の取り組み開始について（2025 年 5 月 14 日報道発表） https://www.ntt-west.co.jp/news/2505/250514a.html

1. 背景と目的

近年、サイバー攻撃は高度化・巧妙化し、インシデント発生時には業務停止や情報漏えいのみならず、企業の信用やブランド価値に重大な影響を及ぼし、サイバーセキュリティは事業継続を左右する重要な経営課題となっています。このような環境下において、脅威の兆候をいち早く捉え、被害拡大を防ぐための「平時からの継続的なセキュリティ監視・分析体制」の構築が不可欠ですが、すべてのリスクを未然に防ぐことは困難であり、インシデントの発生を想定した備えが求められています。

NTT ビジネスソリューションズは、「セキュリティのかかりつけ医」として、お客さまのサイバーセキュリティを継続的に支えられるよう、平時・有事の区分なく一貫して支援できる体制を整え、お客さまの企業価値と事業継続性を守る実効性の高いセキュリティ対策に貢献します。

2. 概要

今回のサービス高度化の内容および新たに提供を開始するサービスは、以下のとおりです。

（1）セキュリティ監視分析サービス（CPC SOC）の高度化

以下の内容を中心に機能強化を行い、高度な監視・分析に基づく的確な検知を行う SOC サービスを実現します。

① 複数ログを活用した相関分析による高精度な脅威検知

複数のログ情報を組み合わせた相関分析により、単一のアラートでは判断が難しい脅威の兆候も高精度に検知します。誤検知を抑えつつ、対応が必要な事象を的確に抽出します。

② 独自の SIEM 分析ルールやセキュリティアナリストによる高度な分析機能

独自の分析ルールやセキュリティアナリストによる高度な分析により、多様な手法のサイバー攻撃やインシデント発生を検知することができます。

③ お客さま専用ポータルサイトによる「視える」セキュリティ運用

検知状況や対応状況をポータルサイト上で可視化し、日々のセキュリティ運用状況を分かりやすく把握可能とすることで、効率的なセキュリティ運用を支援します。

（2）インシデントレスポンス（IR）サービスの提供

セキュリティインシデントが発生した際に、調査・対処・復旧までを一貫して支援することで、事業への影響を最小限に抑えることを目的としています。

前段のセキュリティ監視分析サービス等により、平時からお客さまのセキュリティ運用を支援している場合には、インシデント発生時にも初動対応をよりスムーズに進められることが期待されます。

① 初動対応／一次対処

お客さまからセキュリティインシデントの事象をヒアリングし、初期判断に必要な範囲で取得可能なログを用いて、被疑箇所の特定や被害拡大有無の推定を行い、インシデント概要を迅速に把握します。迅速な復旧に向けて対応方針などの助言を実施します。

② 調査・復旧

お客さまから提示いただいたログを基に分析・調査やサーバー/端末のフォレンジック[※3]を行います。システムの復旧に向けた対応方針などの助言を実施します。

③ 再発防止策の立案

調査結果を踏まえ、まず応急復旧後の運用を継続するために必要な暫定対処を整理・提示するとともに、根本的なリスク低減を図る恒久的な再発防止策をご提示します。

※3 フォレンジック：サイバーセキュリティ分野において、インシデント発生後に関連するログやデータを保全・分析し、事象の経緯や影響範囲、原因等を客観的に明らかにする調査手法。

３．提供開始日

2026 年　3 月 31 日（火）

４．提供エリア

西日本エリア（富山県、岐阜県、静岡県以西の 30 府県）

５．サービス提供価格

お客さまのご要望や構成内容により異なるため、営業担当者にお問い合わせください。

６．今後の展開

NTT ビジネスソリューションズは、今後も「セキュリティのかかりつけ医」として、お客さまのサイバーセキュリティ課題に伴走し、継続的な支援を通じてセキュリティ対策の成熟度向上に貢献していきます。

７．本件に関するお問い合わせ先

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　マネージドサービス部門　マネージドビジネス担当
E-mail：mc-soc_contact@west.ntt.co.jp

※ お問い合わせの際は、メールアドレスをお確かめのうえ、お間違いのないようお願いいたします。

※ ニュースリリースに記載している情報は、発表日時点のものです。変更になる場合がありますので、あらかじめご了承いただくとともに、ご注意をお願いいたします。