つなごう。驚きを。幸せを。

2026 年 9 月 28 日

NTT ドコモビジネス株式会社

「docomo business RINK®」において、インシデント対応の迅速化を支援する「LAN セキュリティ」を提供開始

～NW 内の異常を可視化し、事業停止・情報漏えいリスクの低減を支援～

NTT ドコモビジネス株式会社(旧 NTT コミュニケーションズ株式会社、以下 NTT ドコモビジネス)は、多様なセキュリティ機能とネットワーク機能を統合した NaaS(Network as a Service)※1 である「docomo business RINK®」の新機能として「LAN セキュリティ(以下 本サービス)」を 2026 年 10 月 30 日より提供開始します。

1. 背景

近年、セキュリティ対策の制度などを背景に、企業にはログの適切な取得・保全、継続的な可視化、インシデント発生時の証跡確認が求められています。また、ランサムウェアやサプライチェーン攻撃などのサイバー攻撃は高度化し、外部からの侵入を防ぐ対策に加えて、侵入後の不審な挙動を早期に発見する対策の重要性が高まっています。攻撃者は、侵入後に社内ネットワーク内を探索し、重要な情報やシステムに到達しようとするため、その挙動を検知することが、侵害の進行を止め、被害の拡大を防止するために重要な対策となります。

一方で、企業の LAN 環境には PC やサーバーに加え、複合機や監視カメラなど多様な機器が接続されています。これらの機器は、エンドポイントセキュリティ製品を導入しづらい場合があり、企業内における“見えないリスク”となる可能性があります。

そこで、NTT ドコモビジネスはネットワーク機器やサーバーが標準的に備えている機能※2 を活用し、LAN 内で攻撃を受けている端末や不審な通信を特定できる「LAN セキュリティ機能」を NaaS に実装します。

2. 本サービスの概要と特長

「LAN セキュリティ」は、社内の通信を継続的に可視化・分析するネットワークに組み込まれたセキュリティサービスです。マルウェア感染端末や内部不正、情報漏えいの兆候、不審な通信などのリスクの可視化を支援します。

お客さまは既存のネットワーク環境を活用しながら、専用設備の追加導入や大規模な構築をすることなく社内 LAN の可視化を開始できます。これにより、巧妙化・高度化するサイバー攻撃への対策として、ログにもとづく状況把握、インシデント調査、被害拡大リスクの低減を支援します。

特長 1：ログの一元管理、インシデント調査の迅速化

本サービスでは、「docomo business RINK®」上でログ保管基盤を提供し、ネットワーク通信ログである NetFlow と、お客さまが指定するゲートウェイ機器やサーバーなどの Syslog を一元的に保管します。

平時からログを蓄積することで、インシデント発生時における証跡確保、初動調査や影響範囲の特定、社内報告・監査対応の迅速化を支援します。これにより、業界ガイドラインや SCS 評価制度※3 などで求められるログ管理・監視状況に関する説明責任の遂行にも貢献します。特に、エンドポイントに依存しない通信ログ（NetFlow）に加え、サーバーなどの Syslog をまとめて保管することで、インシデント発生後に機器ごとにログを探す手間や、必要なログが残っていないことによる調査遅延リスクを低減します。なお、Syslog の収集対象として、当社のクラウドサービスである「Smart Data Platform」上のサーバーにも対応します。これにより、お客さまは個別にログ保管環境を構築・運用する負担を抑えながら、インシデント対応の迅速化を図ることができます。

特長 2：相関分析※4 によるインシデントの予兆検知

ネットワーク、ゲートウェイ機器、サーバーログの相関分析を行うことで、インシデント発生時に「いつ」「どの端末が」「どこと通信し」「影響範囲がどこまで広がった可能性があるか」を可視化します。また、マルウェア感染や C&C 通信※5 の疑い、内部不正につながる通信、異常なデータ送信、不審な内部通信などの兆候を可視化します。調査や対処に要する時間の短縮を支援し、事業停止や情報漏えいなどの被害拡大リスクの低減を支援します。さらに、「WAN セキュリティ ふるまい検知」※6 と「LAN セキュリティ」による相関分析をすることで、社内外をまたぐ不審な挙動の早期発見を支援します。なお、本機能に関連する技術については、現在特許出願中です。

特長 3：個別の構築なく、簡単に利用開始

「docomo business RINK®」のネットワーク機能と組み合わせることで、重要拠点やリスクの高い機器から段階的に導入できます。個別にシステム構築することなく、ネットワーク機器やサーバーが標準的に備えている機能の活用と設定変更、ネットワークサービスとの組み合わせにより、簡単に対策を始められます。

特長 4：導入しやすい料金体系

必要な拠点数やログ容量から段階的に利用できる料金体系[月額 90,000 円(税込 99,000 円)～※7]により、セキュリティ対策に十分な予算や専門人材を確保しづらい企業でも導入しやすいサービスです。専用機器の追加導入や大規模な構築を抑え、社内ネットワークの可視化を低コストで開始できます。

3．提供開始日

2026 年 10 月 30 日

4．利用料金・お申し込み方法

お申し込み方法および各プランの詳細については、NTT ドコモビジネスグループ営業担当までお問い合わせください。

5．今後の展開

今後、対象ログを拡大するとともに、AI を活用して脅威検知および分析機能のさらなる高度化を図ります。AI が膨大なログデータを横断的に分析し、攻撃の可能性や影響度に応じて脅威を優先付けること

で、お客さまによる迅速な状況把握と初動対応を支援します。また、インシデント分析結果や対応内容をもとにレポートを自動生成し、セキュリティ運用業務の効率化に貢献します。これにより、高度化・巧妙化するサイバー攻撃に対する継続的なセキュリティ運用を支援します。

NTT ドコモビジネスは、AI 時代に最適な次世代 ICT プラットフォーム「AI-Centric ICT プラットフォーム®」※8 構想に基づき、docomo business RINK®をはじめとしたサービスを提供しており、今後もサービス拡張や高度化を見据えた基盤整備を進めていきます。また、本機能については、今後「docomo business SIGN®」への提供も予定しており、IoT 領域におけるセキュリティ運用の高度化にも貢献していきます。

6. NTT docomo Business Forum'26 出展情報

2026 年 10 月 8 日(木)、9 日(金)に開催する「NTT docomo Business Forum'26」にて、本サービスを紹介予定です。詳細は、公式 Web サイトの展示情報よりご確認ください。

公式 Web サイト：https://www.ntt.com/business/go-event.html

■展示名：AI 時代は、もっとつながる。セキュリティ・ネットワーク

■展示番号：IF-02

＊会場：ザ・プリンス パークタワー東京 B2 フロア

＊日時：2026 年 10 月 8 日(木)、9 日(金)　9:30～17:30

＊参加方法：完全招待制

＊参加費用：無料

「NTT コミュニケーションズ株式会社」は 2025 年 7 月 1 日に社名を「NTT ドコモビジネス株式会社」に変更しました。私たちは、企業と地域が持続的に成長できる自律・分散・協調型社会を支える「産業・地域 AX のプラットフォーマー」として、新たな価値を生み出し、豊かな社会の実現をめざします。

つなごう。驚きを。幸せを。
docomo Business

https://www.ntt.com/about-us/strategy.html

※1：NaaS とは、ネットワークや付随するセキュリティ機能などをクラウドサービスのように提供するもので、ユーザーはサブスクリプション型で利用できます。

※2：ネットワーク機器から出力される通信フローログである NetFlow v9 や、ゲートウェイ機器・サーバーなどから出力される Syslog などを指します。なお、利用可能なログ種別や取得範囲は、お客さま環境の機器仕様、設定状況およびご契約内容により異なります。

※3：SCS 評価制度とは、サプライチェーン強化に向けたセキュリティ対策評価制度のことです。

※4：相関分析とは、複数のログや通信情報を突き合わせ、単一のログでは判断しづらい不審な挙動や攻撃の兆候を把握する分析手法です。

※5：C&C 通信とは、Command and Control 通信の略であり、マルウェアに感染した端末などが、攻撃者の管理下にある外部サーバーと接続し、指令の受信や実行結果の送信を行う通信のことです。

※6：WAN セキュリティふるまい検知とは、docomo business RINK®においてネットワーク組み込み型で、普段と異なる挙動や兆候を検知してアラートを出す「ふるまい検知機能」のことです。

※7：LAN セキュリティへの接続やその他メニューが必要になる場合は、追加料金が発生します。

※8：AI-Centric ICT プラットフォーム®とは、企業が AI を活用して、生産性の抜本的改善、競争力強化やビジネスモデル変革を進める AI 時代に最適な次世代 ICT プラットフォームのことです。