つなごう。驚きを。幸せを。

2025 年 9 月 26 日

NTT ドコモビジネス株式会社

「docomo business RINK®」において、ネットワーク組み込み型セキュリティ機能「WAN セキュリティ」を提供開始

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※1「docomo business RINK®」の新機能として「WAN セキュリティ」を 2025 年 9 月 30 日より提供開始します。「WAN セキュリティ」は、特許技術を活用した脅威検知・遮断機能や通信ログの保管機能を備えた新たなセキュリティ機能です。お客さまが個別にセキュリティ製品を導入しなくても、「docomo business RINK®」に組み込まれた「WAN セキュリティ」がお客さまの通信全体を監視し、オフィスのパソコンに加えエンドポイントセキュリティの導入が難しい OA 機器や工場 LAN 内の IoT 機器などに対する不正な通信を検知します。「docomo business RINK®」は、巧妙化するサイバー攻撃やインシデントに迅速に対処できる機能を追加し、企業の ICT 基盤強化と健全な事業成長を支援します。

1. 背景

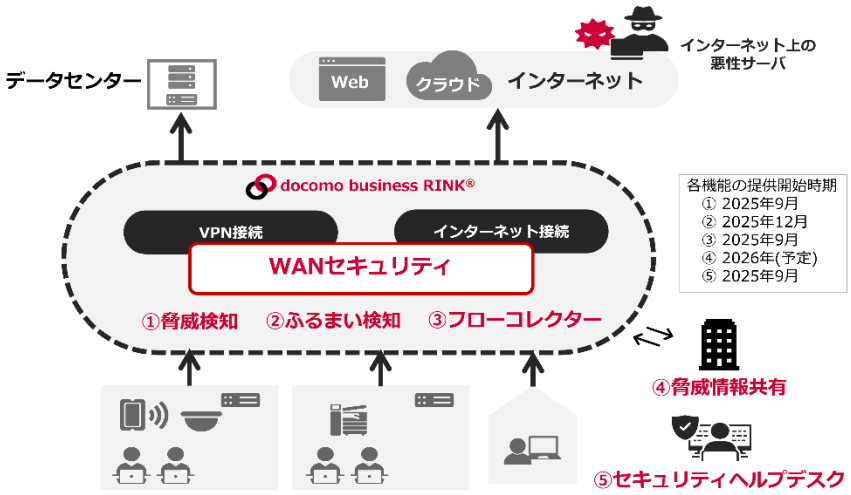
近年、サイバー攻撃の手法が巧妙化し、企業のシステム、パソコンやプリンター、監視カメラなどのあらゆる機器が攻撃対象になっています。さらに、AI エージェント※2 などの登場により、AI がさまざまな機器と通信する時代が到来すると、新たなセキュリティリスクが一層拡大すると見込まれます。一方で、企業の IT インフラはクラウド利用の進展や多様な働き方の広がりにより分散化が進み、従来の境界型防御※3 では十分なセキュリティ対策ができない状況となっています。また、2025 年 5 月に制定された能動的サイバー防御法では、インシデントを早期に発見し、国と企業が連携して対応する体制の強化が定められました。サイバー攻撃は 1 社の被害でもサプライチェーン全体に影響が波及する可能性があるため、企業は自社だけでなく、取引先やグループ企業を含めたサプライチェーン全体のセキュリティガバナンスの整備が求められています。

2.「docomo business RINK®」の概要と「WAN セキュリティ」の特長

「docomo business RINK®」は今回追加の「WAN セキュリティ」をはじめとするさまざまなセキュリティ機能が統合された NaaS として、「モバイル/固定融合ネットワーク」や「オープン※4/クローズド※5 融合ネットワーク」など企業のニーズに応じて多様な使い方ができるネットワークを簡単・スピーディーに提供するサービスです。

<「docomo business RINK®」のサービス全体像>

今回、2025 月 9 月に提供開始する新機能の「WAN セキュリティ」では、脅威インテリジェンス※6 を活用した脅威検知・遮断機能(特許取得済み)や、インシデント発生時の早期解決につながる通信ログの保管機能(フローコレクター)をネットワークに組み込み、as a Service として提供します。合わせて、脅威検知発生後の対処をサポートするセキュリティヘルプデスクを提供します。また、今後の提供予定として、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」や、グループ会社やサプライチェーンを構成する企業間で脅威検知情報を共有する「脅威情報共有機能」を追加します。これにより、企業やサプライチェーン全体におけるセキュリティインシデント発生時の対応の迅速性、サイバー攻撃への対応力の向上を図り、経済的損害やレピュテーションリスクを抑制します。またいずれの機能もネットワーク組み込み型として提供するため、低コストで簡単・手軽にセキュリティレベルの向上が図れます。



＜WAN セキュリティの概要＞

「WAN セキュリティ」の主な特長は、以下の通りです。詳細は別紙をご確認ください。

（1） インターネット通信の監視・検知・遮断まで一元管理と多層防御

脅威インテリジェンスを用いた脅威検知機能により、インターネット通信を監視し、C&C サーバー※7やフィッシングサイトなど危険性の高いサイトとの通信を検知します。さらに検知した通信をお客さまにて遮断することも可能です。脅威検知機能により、お客さまは、不正な通信の発生を網羅的にいち早く発見、遮断することができ、自社内や関連企業でのマルウェア感染拡大などのサイバー攻撃被害拡大を防止できます。また、提供中のインターネットゲートウェイ、リモートアクセス、認証情報管理などのクラウド型セキュリティ機能と組み合わせることで、より一層の多層防御も可能にします。

（2） インシデント発生時の原因調査の効率化

フローコレクター機能※8により、お客さまは通信ログを最大 1 年間保持できます。万が一、サイバー攻撃を受けてしまった場合、端末や通信機器などのさまざまな機器のログを分析し原因や影響範囲の調査を行う必要がありますが、フローコレクター機能により収集した通信ログを活用することで、網羅性のある調査が可能となり、調査や対処に要する時間の短縮が期待できます。

（3） ネットワーク組み込み型により簡単でスピーディーなセキュリティの導入が可能

お客さまは Web の管理ポータルから「WAN セキュリティ」を選択するだけで導入が可能です。手続きは、NaaS の特長を活かした Web 完結型であり、物理的な工事も不要なため、使いたい時にすぐご利用いただけます。お客さまは、対象拠点のセキュリティ重要性の変化やサイバー攻撃の激化などの社会情勢に応じて、「WAN セキュリティ」の 5 つの機能（別紙参照）を追加していくことで、自社や関連企業のセキュリティ対策をスピーディーに強化していくことが可能です。

（4） リーズナブルな価格設定

「WAN セキュリティ」は、別途初期費 0 円、1 拠点あたり月額 2,600 円(税込 2,860 円)※9からご利用いただけます。個別にセキュリティ製品を導入するよりもリーズナブルにセキュリティ対策が可能です。オフィスや工場などの拠点内には、エンドポイントセキュリティが導入できない OA 機器、IoT、OT 機器も多く存在し、個別のセキュリティ対策は導入費用の増加が考えられます。お客さまは、「WAN セキュリティ」により、リーズナブルに拠点全体の不正な通信の検知・遮断や通信ログ保管を導入でき、コストを抑えながら万が一のサイバー攻撃被害拡大防止を推進できます。

3. お申し込み方法・ご利用料金

ビジネスポータル※10からお申し込みが可能です。お申し込み方法の詳細、およびご利用料金については SDPF ナレッジセンター※11 または 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。

4. 今後の展開

今後も「docomo business RINK®」は、さらなるセキュリティ機能やモバイルなどのアクセス回線種別、AI を活用した機能の拡張を図ります。また、企業が AI エージェントなどを活用して、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(AI-Centric ICT プラットフォーム)構想※12の実現に向けて取り組んでいきます。NTT ドコモビジネスは、環境変化や事業変化にもいち早く対応できる即時性と、安全にデータを流通できる基盤を提供し、企業の持続的な生産性向上、競争力強化、ビジネスの発展に貢献します。

5. 出展情報

NTT ドコモビジネスが 2025 年 10 月 9 日(木)～10 日(金)に開催する「docomo Business Forum'25」にて、本サービスを紹介予定です。詳細は、以下出展概要をご確認ください。

docomo Business Forum'25 出展概要

■展示会名称：docomo Business Forum'25
■展示会期間：2025 年 10 月 9 日(木)～10 日(金) 9:30-17:30
■特設サイト：https://www.ntt.com/business/go-event.html?ir=nr
■展示会場所：ザ・プリンスパークタワー東京 B2
■展示名：セキュリティ統合型 NaaS「docomo business RINK®」

「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型社会を支える「産業・地域 DX 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/nttdocomobusiness.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：AI エージェントとは、ユーザーの質問から目的を理解し、自律的に目的達成に向けタスクを分解し、実行する AI システムのことです。

※3：境界型防御とは、企業ネットワークの内と外の間に「境界」を設け、ファイアウォールや VPN などのセキュリティ対策を施して、外部からの不正なアクセスや攻撃を防ぐセキュリティモデルです。

※4：オープンネットワークとは、インターネットの別呼称です。

※5：クローズドネットワークとは、特定の権限を持った利用者だけがアクセスできるネットワークです。

※6：脅威インテリジェンスとは、サイバー攻撃に関する情報を収集・分析し、悪性通信を行う可能性の高い通信相手の IP アドレスや DNS ドメイン名などの情報を整えたデータベースのことです。

※7：C&C サーバーとは、コマンド&コントロールサーバーの略であり、外部から侵入して乗っ取ったコンピューターを多数利用したサイバー攻撃において、コンピューター群に指令を送って制御するサーバーやコンピューターのことです。

※8：フローコレクター機能とは、「docomo business RINK®」における通信ログを保存する機能です。

※9：ワイヤレスアクセスで脅威検知(検知履歴 3 カ月保管プラン)をご利用いただいた場合の料金、1 分毎 0.090278 円の月額上限値です。金額は 2025 年 9 月 26 日時点の予定であり、今後変更の可能性があります。

※10：ビジネスポータルとは、NTT ドコモビジネスでご契約中の複数サービスをお客さまご自身で一元管理・運用できる無料のポータルサービスです。

※11：Smart Data Platform Knowledge Center - Smart Data Platform

※12：次世代 ICT プラットフォーム(AI-Centric ICT プラットフォーム)構想とは、NTT ドコモビジネス、ゲットワークス、NTTPC が発表した、「分散」「柔軟」「安全」「リーズナブル」といった今後の企業ニーズに合致した AI 時代に最適な次世代 ICT プラットフォーム構想です。
ニュース 2025 年 6 月 10 日:NTT Com、ゲットワークス、NTTPC が戦略的業務提携を締結

＜別紙＞

「WAN セキュリティ」の機能詳細は以下の通りです。

(1)脅威検知(特許技術活用)

脅威インテリジェンスを活用し、「docomo business RINK®」の通信ログをもとに、「docomo business RINK®」のネットワーク内で不正通信を検知します。検知した不正通信は、お客さまにて Web の管理ポータル上で確認することができ、該当通信を選択して遮断することが可能です。【2025 年 9 月提供開始】

(2)ふるまい検知(特許技術出願中)

「docomo business RINK®」の通信ログより、普段と異なる挙動や兆候の通信を検知します。これにより、未知の脅威、内部不正、設定ミスなどに気づき、インシデント発生前の対策や気づきからの早期対処につなげることが可能です。【2025 年 12 月提供開始予定（2025 年 9 月試行版提供開始）】

(3)フローコレクター

「docomo business RINK®」における通信ログを長期間保存できます。インシデントが発生した際、通信ログのデータをダウンロードし、お客さまの分析基盤にて脅威分析やインシデントの調査プロセスに活用いただくことが可能です。【2025 年 9 月提供開始】

(4)脅威情報共有

お客さまのグループ会社内にて、子会社の脅威検知情報を親会社に共有することが可能です。これにより、親会社は関係する会社の状況を一元的に把握可能で、グループ会社全体でのセキュリティガバナンスを向上させることが可能です。【2026 年提供開始予定】

(5)セキュリティヘルプデスク

脅威検知時のアラートに対する初動対応や原因調査の支援、およびそれらを踏まえた今後のさらなるセキュリティ対策の提案を行います。WAN セキュリティを通じ、お客さまのセキュリティ対策を伴走型でサポートします。【2025 年 9 月提供開始】