つなごう。驚きを。幸せを。
docomo Business

2026 年 7 月 31 日
NTT ドコモビジネス株式会社

「docomo business RINK® WAN セキュリティ」において サプライチェーン・企業グループ全体を守る「脅威情報共有」の提供開始

～サプライチェーンや企業グループ全体のセキュリティガバナンス強化に貢献～

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、「docomo business RINK® WAN セキュリティ※1」における脅威検知※2 を活用した新メニュー「脅威情報共有」(以下 本メニュー)の提供を 2026 年 7 月 31 日より開始します。本メニューにより、サプライチェーンや企業グループ全体における迅速な脅威把握と初動対応を実現し、事業継続性の確保に貢献します。

1. 背景

近年、サイバー攻撃が高度化・巧妙化し、サプライチェーンや企業グループでは委託先企業やグループ会社を起点として被害が発生・拡大する事案が増加しています。独立行政法人情報処理推進機構(IPA)が発表した「情報セキュリティ 10 大脅威 2026※3」によると、企業などの組織では「サプライチェーンや委託先を狙った攻撃」が 2 位として選出されており、サプライチェーンや企業グループ全体でのセキュリティ対策の強化が求められています。 一方で、人材不足やコスト負担の観点から、サプライチェーンや企業グループ全体に十分な監視体制や専門人材を確保することは難しく、セキュリティ対策強化への障壁となっています。そのため、サプライチェーンや企業グループ全体においては、委託元企業では委託先企業のセキュリティ対策状況を把握しづらく、委託先企業では複数の委託元企業から異なる対策を求められるなど、さまざまな課題が顕在化しています。

2. 本メニューの概要

「docomo business RINK® WAN セキュリティ」の脅威検知機能は、お客さまの通信全体をネットワーク上で監視し不正な通信を検知します。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 機器などにセキュリティ対策を施せるほか、すでにエンドポイントセキュリティを導入しているオフィスのパソコンなどに対しても多層防御として機能します。

本メニューは、サプライチェーンにおける委託先企業や企業グループにおけるグループ会社などに導入された「docomo business RINK® WAN セキュリティ」の脅威検知機能で検知した脅威情報を、あらかじめ設定した委託元企業や親会社などへ Web 管理ポータルおよびメールで通知する機能です(特許取得済)。本メニューの提供により、委託元企業や親会社は、委託先企業やグループ会社などで検知したセキュリティリスクを一元的に可視化し、継続的なセキュリティ管理を行うことができます。また、専門人材の不足する委託先企業やグループ子会社においてセキュリティの脅威が検知された場合でも、親

会社などのセキュリティ担当者が迅速に状況を把握し、対処を支援することが可能になります。これにより、各社で個別に高度な監視・運用体制を整備することが難しい場合でも、セキュリティ対策の負担を軽減しながら、サプライチェーンや企業グループ全体でセキュリティガバナンス強化とインシデントの早期発見・早期対応を実現します。

3. 本メニューの特長

(1)サプライチェーンや企業グループ全体での可視化と統制

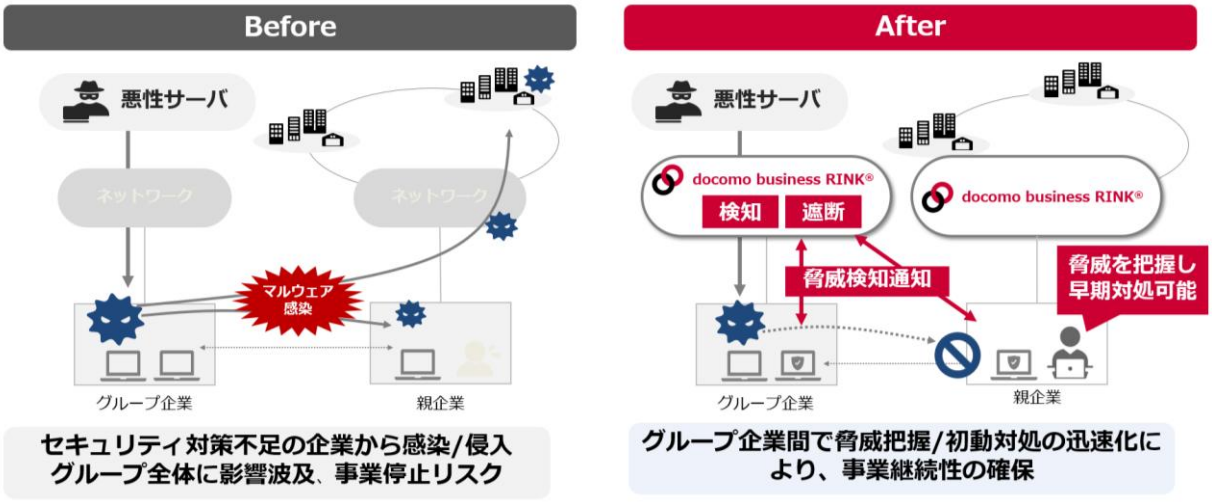
委託元企業や親会社が委託先企業やグループ会社のセキュリティ状況を一元的に把握し管理を行うことで、サプライチェーンや企業グループ全体のセキュリティガバナンス強化に貢献します。

(2)迅速な初動対応の実現

C&C サーバー※4やフィッシングサイトなど危険性の高いサイトとの不正通信が委託先企業やグループ会社で発生した際に委託元企業や親会社への速やかな情報共有と初動対応を実施することで、被害拡大の防止に寄与します。

(3)簡易導入と低コスト運用

月額 10,000 円(税込 11,000 円)からオンデマンドでお申し込み可能で、個別の設計や構築が不要なため、導入負荷やコストを抑えながら迅速に導入できます。



<本メニューのイメージ図>

4. 提供開始日

2026 年 7 月 31 日

5. ご利用料金・お申し込み方法

ご利用料金は、ご利用の拠点数に関わらず、脅威情報を提供するテナント※5と受領するテナントのペア毎に月額 10,000 円(税込 11,000 円)からご利用いただけます。(別紙 1)

ご利用料金とお申し込み方法の詳細は NTT ドコモビジネスグループ営業担当または Smart Data Platform ナレッジセンター※6までお問い合わせください。

6. 今後の展開

NTT ドコモビジネスは、本メニューの提供を通じて、企業間の安全な事業活動を支えるセキュリティ基盤の実現に貢献します。今後もセキュリティ機能のさらなる強化とともに、サプライチェーンや企業グループを含めたセキュリティリスクの可視化と迅速な対応を支援していきます。また、「docomo business RINK®」においては、アクセス回線種別の拡充やセキュリティ機能強化を継続するとともに、AI 技術を活用したネットワーク運用の自動化・自律化を推進し、さらに進化した NaaS(Network as a Service)※7 の提供をめざします。

これにより、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®」構想※8 の実現を推進し、企業の持続的な生産性向上、競争力強化、ビジネス成長に貢献していきます。

「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 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：WAN セキュリティとは、特許技術を活用した脅威を検知し、遮断する機能や通信ログの保管機能を備えた「docomo business RINK®」のセキュリティ機能のことです。

※2：脅威検知とは、ネットワーク上の不正通信を検知・通知する WAN セキュリティのメニューです。

※3：独立行政法人情報処理推進機構(IPA)「情報セキュリティ 10 大脅威 2026」
情報セキュリティ 10 大脅威 2026 | 情報セキュリティ | IPA 独立行政法人 情報処理推進機構

※4：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。

※5：テナントとは、Smart Data Platform において、docomo business RINK®を含むネットワークサービスなどのリソースを管理するグループのことです。

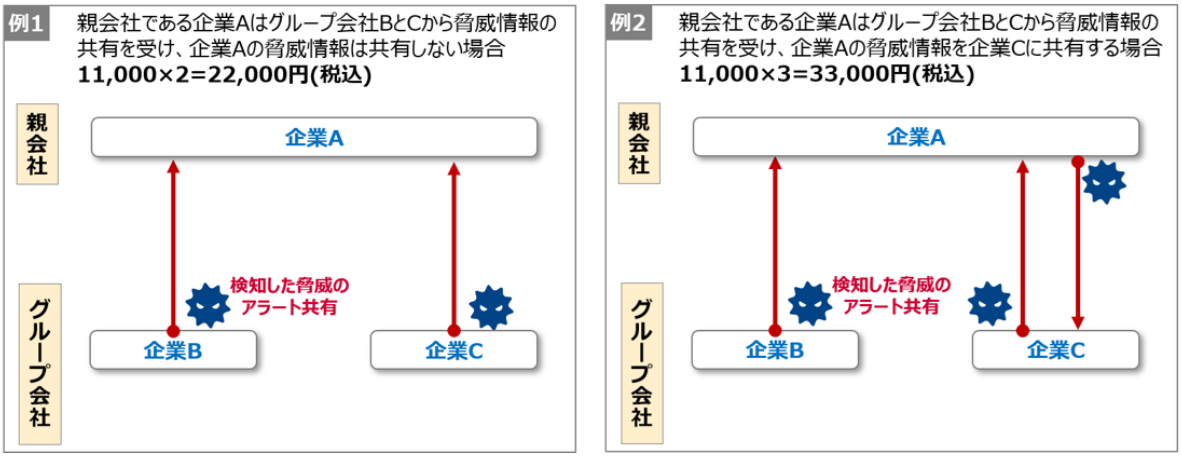
※6：SDPF ナレッジセンターとは、Smart Data Platform(SDPF)のサービス説明書などのドキュメントや、ご利用料金、稼働状況、お問い合わせ窓口などを紹介するサイトです。
Smart Data Platform Knowledge Center - Smart Data Platform

※7：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。

※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。

【別紙 1】

本メニューのご利用料金は、脅威情報の共有方向ごと(片方向ごと)に月額 10,000 円(税込 11,000 円)が発生します。ご利用になるテナント双方向で脅威情報を共有する場合は、2 件分のご利用料金が発生します。



<ご利用料金の例>