URL https://journal.ntt.co.jp/article/37030
DOI https://doi.org/10.60249/25113102

# docomo business RINK® セキュリティ機能のさらなる強化

本稿では，お客さまのICT環境をas a Serviceで実現する，セキュリティ・ネットワーク一体型サービスである“docomo business RINK®”と，2025年9月より新たに加わったWAN（Wide Area Network）組み込み型セキュリティ「WANセキュリティ」についての機能概要や特長，構成技術，ユースケース，ロードマップ等について紹介します．

## docomo business RINK® とは

### ■docomo business RINK® の概要

docomo business RINK®（RINKはResilient Integrated NetworKから命名）はセキュリティ・ネットワーク一体型サービスです（**図1**）．NTTドコモビジネスは，旧社名NTTコミュニケーションズ時代より，ネットワークサービスであるOCN（Open Computer Network）やUNO（Arcstar Universal One），またセキュリティサービスであるFSG（Flexible Secure Gateway）やFRA（Flexible Remote Access）など，お客さまのICT環境を構築するさまざまなサービスを提供しています．

そしてdocomo business RINK®は，これらサービスの機能や培ってきた知見を結集させ，「as a Service*1化」「セキュリティ一体化」というキーワードの下，お客さまに求められるネットワークを再定義し，お客さまのICT環境を必要十分・迅速・明瞭・簡潔に提供することで，自由に，柔軟にビジネスの発展へご活用いただけることをめざして誕生したサービスです．

### ■docomo business RINK® の背景

昨今，ビジネスにおけるインフラとしてのネットワークは，求められるあり様が大きく異なってきています．これまでは，接続したい対象が明確に定まっており，それらを間違いなく接続することが求められてきました．そのため従来のネットワークは，確かで，堅いことが基本的で，その中に属する「誰かと誰か」・「誰かと何か」をつなぐため，「内部」を明確に定義し，「外部」を除外することが求められてきました．変更・拡張が行われる際も，十分な吟味が行われたうえで，時間をかけて実施されることが主だったため，そのスタイルが受け入れられてきました．

しかし現在では，いわゆるインターネットの利活用が日々進化していて利用するリソースをクラウド等の「外部」に依存するメリットがデメリットを上回り，利用するユーザもリモートワーク等の「外部」から接続することが一般的となりました．それに伴い，ネットワークに対する要件も，変化の激しい市場環境において必要なリソースやユーザを迅速に取り込める，流動的な形式が好まれる

*1 as a Service：IT業界で広く使われる概念で，サービスとして提供される形態．


図1　docomo business RINK® の概要

ようになりました．注意いただきたいことは，これはあくまでネットワークの要件であり，後述するセキュリティにおける要件とは別軸であり，「ネットワークそのものが柔軟である」ということが肝要となります．

では，セキュリティについてはどうなのか，ということについてですが，これまでのセキュリティの思想を過去のものとしたのは，「ゼロトラスト*2」の登場です．ゼロトラストとは，文字どおり「何ものも信じない」ということであり，前述した「内部」「外部」という区別がない概念です．そもそも専用線が引かれてネットワークがつくられていた時代はさておき，現代の企業ネットワークは基本的に，外部であるインターネットとの接点を持ちます．また，生成AI（人工知能）の隆盛でさらに加速されることが予想されますが，攻撃者の手法も巧みになり続けていきます．そのような環境で，「外部から内部への攻撃が成功している」あるいは「内部にすでに攻撃者がいる」という状況は想定しなければならないものであり，危険な外部と安全な内部という境界線のある前提を置くことはもはや許されず，あらゆる接続を疑ってかかることが重要である，との考え方です．

ここまでの内容をまとめると，ネットワークの要件としても，セキュリティの要件としても，接続する対象が不動・あるいはゆるやかな変動しかない，という思考はビジネスの維持や発展を妨げるものであり，時々刻々と柔軟に付き従えることが重要である，ということです．

### ■docomo business RINK®の目的

前述のとおり，docomo business RINK®は「as a Service化」と「セキュリティ一体化」を行ったサービスです．

まず「as a Service化」については，「ネットワークそのものが柔軟である」ということを実現するための手法です．SaaS*3/IaaS*4/PaaS*5など，昨今ではさまざまな商品がサービス化していますが，これはユーザニーズの変化に柔軟な対応を果たすために生まれてきました．ユーザとしても，今この瞬間に必要な商品を享受でき，提供者としても適宜商品にアップデートをかけていくことのできるこの形態は，現代のスピード感に追従するうえでのベストな選択肢の1つとなり，その概念をこれまで堅くあり続けたネットワークという領分で取り入れることが目的となります．

次に「セキュリティ一体化」ですが，ここでいうセキュリティとは，主に防御ではなく可視化に属する類のもので，例えるとすれば自動車におけるオービスのようなイメージとなります．検問のように都度ネットワークにおける流通を止めて確認するのではなく，自由に通行させながらも，その挙動をとらえ続ける機能をネットワーク内に組み込む，ということです．これにより，as a Service化したことにより得たネットワークの柔軟性を妨げることなく，セキュリティ要件であるゼロトラストの概念に対応していくことができます．この機能が本稿の主題となる「WANセキュリティ」であり，以降で詳細について触れていきます．

### ■docomo business RINK®という提案

これまで述べてきたとおり，docomo business RINK®とは昨今の情勢を踏まえてつくられた新たなネットワークサービスであり，お客さまのビジネスの発展にいかに寄与するかという点に主眼を置いています．docomo business RINK®にはさまざまな機能が具備されていますが，大きく「コア機能」と「拡張機能」に分類しています．ゼロトラストの根本を備えた柔軟なネットワークをコア機能とし，必要に応じて必要なセキュリティを拡張機能として追加いただく，という構図となります．

具体的には，有線・無線などのアクセス形態を利用でき，企業内リソース・インターネットいずれにもアクセスでき，それらをオンデマンド*6で変更できます。さらに特に攻撃の舞台となるインターネットアクセスにおいて流れる通信を監視・保管することで攻撃の早期検知や対応ができるネットワークにさらに，インターネットアクセスのための防御セキュリティも追加したい，などの要望にもおこたえできるサービスです．本稿ではdocomo business RINK®のWANセキュリティ以外の詳細については割愛しますが，ご興味があれば弊社までお問い合わせください．

## docomo business RINK® WANセキュリティとは

### ■WANセキュリティの概要

WANセキュリティは「インターネットアクセスにおいて流れる通信を監視・保管することで攻撃の早期検知や対応」をWAN単体で実現する可視化機能です（**図2**）．ゼロトラストの概念に基づくと，「攻撃されない」「攻撃されても防げている」との前提を置くことは許されず，「すでに攻撃が成功していて，いつ被害が発生してもおかしくない」というところまで常に疑わなければなりません．これまでは，攻撃を成功させないよう事前に防御することに重きが置かれ，攻撃が成功した事後の対応についてはおざなりになりがちでしたが，完全な防御が現実的ではない以上，むしろ事後の対応ができていることをベースとすることが，これからのセキュリティ対策として重視すべきポイントとなります．

WANセキュリティでは，①脅威検知・遮断，②フローコレクター，③セキュリティヘルプデスクという機能を提供します．docomo business RINK®を利用している拠点とインターネットとの間で行われる通信について，その通信品質に影響を与えない

---

*2 ゼロトラスト：従来の「社内＝安全，社外＝危険」という境界型モデルから脱却し，IDとコンテキストに基づく動的なアクセス制御を行う考え方．
*3 SaaS：ソフトウェアをインターネット経由で提供するサービス形態．
*4 IaaS：仮想化されたITインフラ（サーバ，ストレージ，ネットワークなど）をインターネット経由で提供するクラウドサービス．
*5 PaaS：アプリケーション開発や運用に必要なプラットフォームをクラウドで提供するサービス形態．
*6 オンデマンド：必要なときに，必要な分だけ提供されるサービスや仕組み．

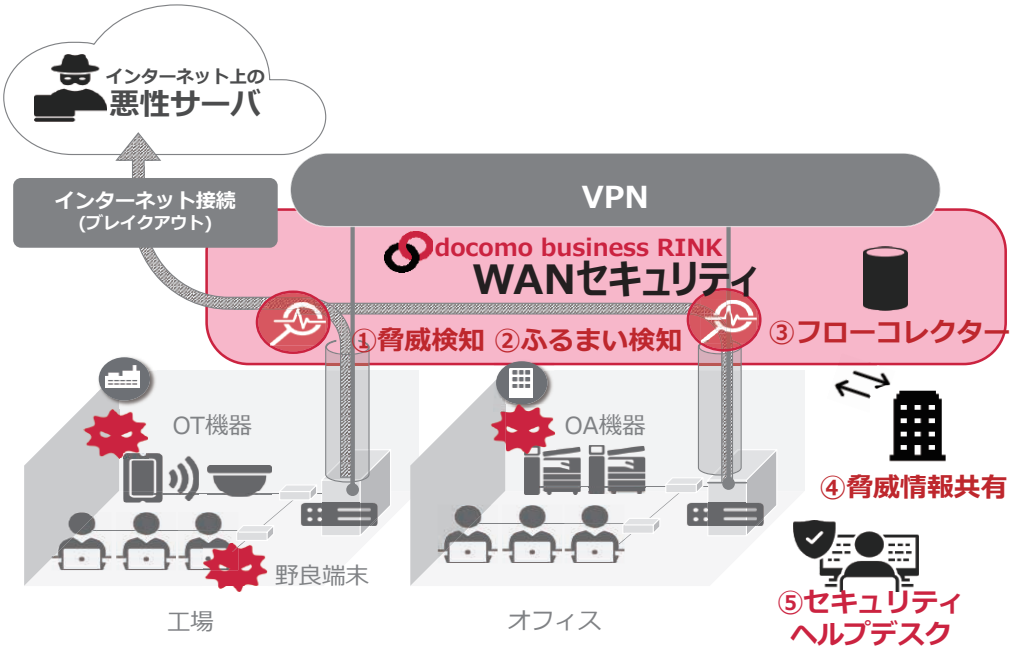


図2　WANセキュリティの概要

かたちで①危険な宛先と通信していないか確認し，危険な宛先との通信を検知した場合は必要に応じて遮断ができ，②通信ログを保管しておくことで，インシデントが発生してしまった際には遡ってインシデントの影響範囲の確認に活用することができ，③セキュリティの専門家へ検知した脅威の内容やその後の対応について相談することが可能となっています．これらを活用することで，「攻撃された際の備えが常にできている」状態でネットワークを柔軟に展開し，ビジネスを自由に発展することができます．

**■WANセキュリティの特長**

可視化を実現するサービスは多数ありますが，その中でWANセキュリティはWANに組み込まれているために「利用が容易」なことと「エンドの特性を問わない」ことが最大の特長です．

利用の容易さについては，WANセキュリティはオンデマンドでポータルから項目を選択いただくことだけで完結します．設備はすべてサービス側に組み込まれており，オーダはオンラインで完了するため，お客さまによる作業は一切必要ありません．他の手法は一般的に，ネットワークのいたるところに可視化のための機器を配備する，あるいはネットワーク構成を変更して可視化のための機器を一度経由するように集約させる，といった手間が発生するため導入のハードルが非常に高く，その後のあらゆる変更の際にその制約を念頭に入れなければなりません．

エンドの特性を問わない点についてですが，これはWANとエンドというポイントの違いに由来します．エンドポイントセキュリティは，ゼロトラストの概念からも重要な対策検討個所ですが，そもそもの導入ハードルが高い場合があります．例えばOA機器やIoT（Internet of Things），あるいは特定のOSなど，デバイスの特性としてエンドポイントセキュリティが対応していないケースや，不定期に利用するユーザが多いケースなどが挙げられます．攻撃者は対策が不十分な個所をねらってくるため，弱い部分をつかれて被害にあってしまう，という事例も多く，その点WANセキュリティは，エンドの特性を問わずWANを流れる通信でありさえすれば対象とできます．

**■WANセキュリティの機能**

⑴　脅威検知・遮断

脅威検知・遮断は，C&Cサーバ*7などの危険な対象と通信していないかを検知し，必要に応じてその対象との通信を遮断することができる機能です．検知は弊社脅威インテリジェンス*8との照合によって行われ，検知された際にはオンラインでポータルから該当の通信を確認できます．ポータル上では，検知された通信のリスクレベル（Critical/high等）や脅威タイプ（C&C/フィッシング等）も表示されます．それらの情報を踏まえ遮断が必要だと判断した場合は，数度クリックするだけで対象との通信をルータ単位で簡単に遮断できます．遮断後は，対象と何度通信を試みたかの回数も表示されるため，攻撃の継続状況等も逐次把握できるようになります．

*7　C＆Cサーバ：マルウェアやボットネットが外部から指令を受け取るために使用するサーバで，サイバー攻撃において，感染した端末（ボット）を遠隔操作するための「司令塔」の役割を果たします．
*8　脅威インテリジェンス：サイバー脅威に関する情報を収集・分析し，攻撃の予防・検知・対応に活用するための情報．

⑵　フローコレクター

フローコレクターは，通信ログを保管・ダウンロードして確認することができる機能です．通信ログの保管については，ACD（Active Cyber Defense：能動的サイバー防御）法が2025年５月に成立するなど現在重要視されている一方で，ログを取得・保管するにはそれを踏まえた環境構築が必要なため，導入に対する一定のハードルがありました．しかしフローコレクターでは，お客さまに個別でシステム構築していただくことは特になく，インターネットアクセスの通信ログが自動で保管されていきます．そして，もしインシデントが発生し調査が必要になった場合は，ダウンロードして確認いただけます．

⑶　セキュリティヘルプデスク

セキュリティヘルプデスクは，docomo business RINK®全般で提供しているヘルプデスクと異なり，WANセキュリティに起因する内容に対応した問合せ窓口となります．脅威を検知した際の対応についての相談を受けるほか，検知状況を踏まえた今後の改善も提案でき，WANセキュリティで把握した現状をフルで活用し，短・中・長期的なお客さまの環境構築をサポートします．

**■WANセキュリティの構成技術**

WANセキュリティでは，キャリアのバックボーン（お客さまのトラフィックが集約される個所）に，通信データを収集する装置および脅威インテリジェンスと照合する装置を設置し，ほぼリアルタイムでお客さまの通信から悪性な通信を検知する仕組みを構築しています．

検知された悪性通信に関する情報は，お客さまがポータル上で閲覧可能であり，さらにポータルからサービスルーターへ指示を出すことで，通信の遮断も可能です．

この脅威検知から遮断に至る一連の技術については，ビジネスモデル特許を取得することで差別化を図り，弊社の独自性を打ち出しています．また，キャリアのネットワーク上に各種装置を設置することで，お客さま個々のネットワークへの設定追加や端末へのソフトウェアインストールを必要とせず，NaaS（Network as a Service）としてご利用いただける仕組みとなっています．

なお，脅威検知に用いるインテリジェンスは，セキュリティベンダーのデータ，OSINT（オープンソースインテリジェンス），および弊社独自に調達したデータを組み合わせており，幅広い脅威通信の検知を可能にする構成となっています．

**■WANセキュリティの展望**

WANセキュリティの将来ロードマップとして，「ふるまい検知」（2025年12月提供開始予定）と「脅威情報共有」（2026年提供開始予定）の２つの機能をリリースする予定です．

ふるまい検知は，端的にいえば未知の脅威への対策の１つです．前述の脅威検知・遮断は，他の事例やセキュリティ機関の調査によって危険と分かっている宛先のリストと照合し，危険な通信が行われていないかを確かめる機能であり，既知の脅威への対策ですが，ふるまい検知は，通信の挙動が普段と異なっていないか監視し，危険な状態に陥っていないかを検知できる機能となります．例えば普段と違う時間であるとか，国であるとか，量であるとか，そういった通信の異常さを報告してくれます．セキュリティ攻撃は高度化の一途を辿っており，新種の攻撃がなされることも少なくなく，既知の脅威に対策できることは当然のこととして，未知の脅威にも対策できるようにしておくことを推奨します．

脅威情報共有は，主にグループ・サプライチェーンの親会社に対し，その子会社が検知した脅威情報を共有することで，セキュリティポリシーの統一やガバナンスの向上を促進する環境を実現するために実装される機能です．攻撃者が脆弱な個所をねらってくることはすでに述べていますが，それは一企業に閉じた話ではありません．企業と企業が当たり前につながってビジネスを行っている現在では，セキュリティ対策が十分にできていない子会社がねらわれ，そこから親会社まで蔓延してしまうケースが少なからず出てきています．しかし，人的・金銭的・時間的コストの課題から，特に規模の大きくない企業では大企業相当の防御環境を直ちに整えることは厳しい状況が予想されます．そこでWANセキュリティの検知機能とともに脅威情報共有を利用いただくことで，まずは危険を検知すること，そしてそれを親会社・子会社間で共有する能力を獲得し，これからの対策ロードマップを策定するためのソースとして活用いただくことができます．

今回は主にインターネット向け通信の観点で記載しましたが，中期的な展望としてはdocomo business RINK®網内のすべての通信への対応を視野に入れています．現在は，インターネット接続やデータセンタ等ギャランティ回線拠点向けの通信について対応していますが，今後，すべての拠点に対するラテラルムーブメントや社内の悪意のあるユーザの通信にも対応できることが望ましく，ベストエフォート拠点間の通信への対応も検討予定です．さらにAIによる運用管理，インシデント管理などの効率化とUI（User Interface）/UX（User Experience）改善を追求し続け，「お客さまのあまねく通信を監視・保管できるWANセキュリティ，その環境を前提とした自律型セキュアNaaS[*9]（Network as a Service）docomo business RINK®」へ昇華させていきます．これからのビジネスをつくる，これからのICT環境を検討される読者の皆様に，是非とも弊社サービスを活用いただければ幸いです．

**◆問い合わせ先**

NTTドコモビジネス
プラットフォームサービス本部
クラウド&ネットワークサービス部　販売推進部門

*9　自律型セキュアNaaS（Network as a Service）：最新セキュリティ技術を組み込んだクラウドベースで提供されるネットワークサービスに，AIや自動化技術を組み合わせて，ネットワークの構成・運用・セキュリティ管理を自動化・最適化する次世代型のサービス．