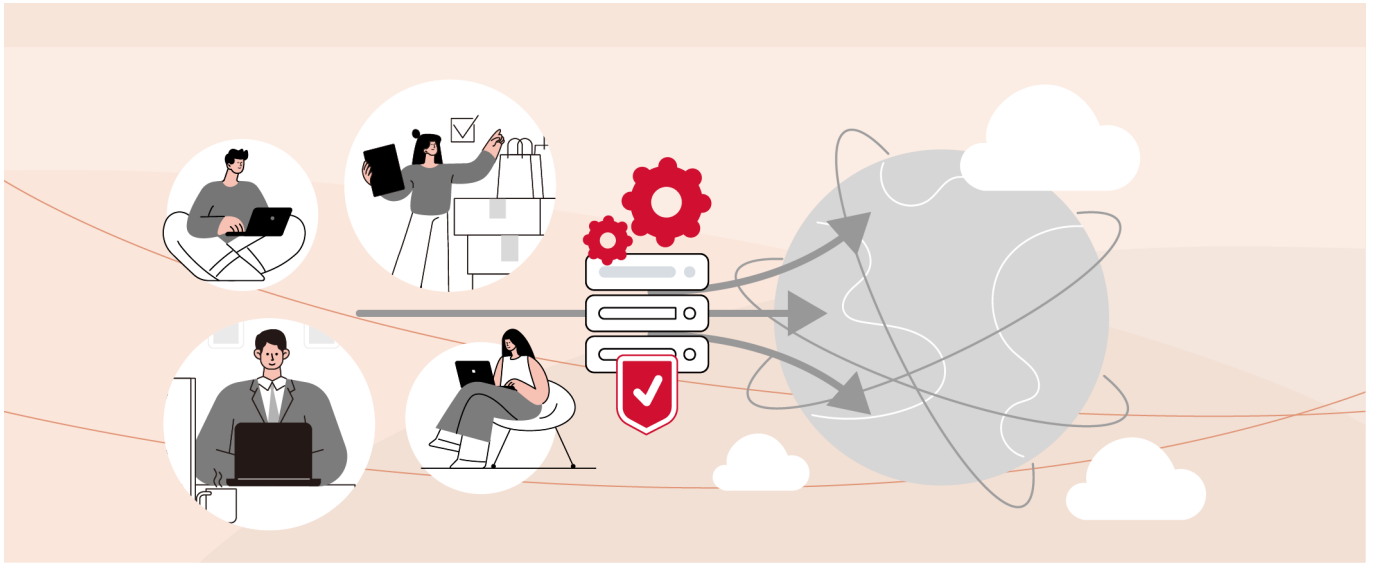




拠点ごとにばらつくインターネット利用環境を統制し、セキュリティと運用を両立

クラウドサービスやSaaSの利用が一般化した現在、企業ネットワークにおけるインターネット通信は年々増加しています。

一方で、拠点ごとに異なる構成でインターネット接続やセキュリティ対策を行っている場合、ポリシーの統一が難しく、運用負荷や管理コストが増大しやすい状況にあります。

ここでは、実在の企業をモデルにした想定事例を通じて、**インターネット利用を統制しながら、業務の柔軟性を損なわないネットワークの考え方**をご紹介します。

業 種 流通業

規 模 従業員 約600名

拠 点 本社+全国の営業拠点 約20拠点

IT体制 本社情シスが全拠点を集中管理

※本事例は実在の企業をモデルにした想定事例です。

課題

拠点ごとに異なるインターネット接続とセキュリティ対策

同社では、拠点ごとにインターネット回線やセキュリティ機器を導入しており、利用ルールや対策レベルにばらつきがありました。

その結果、拠点ごとにWebアクセス制御やログ取得の設定が異なりセキュリティポリシーの変更時には反映に時間がかかる、さらに機器管理や更新作業が拠点数ごとに発生し、運用負荷が高いといった課題が顕在化していました。

また、クラウドサービスや外部Webサイトの利用が増える中で、情報漏えいやマルウェア感染への不安も高まっていました。

拠点ごとにセキュリティもバラバラ



そこで同社は、インターネット接続とセキュリティ機能をネットワークに組み込んで提供されているdocomo business RINK®のインターネットゲートウェイを導入しました。

各拠点のインターネット通信を docomo business RINK®のインターネットゲートウェイ経由で集約・制御することで、Webアクセス制御やセキュリティポリシーを全拠点で統一することができ、通信口

グも一元的に取得。管理拠点側に専用のセキュリティ機器を設置せずに対策を実装することが可能となり、運用負荷を軽減することができました。

これにより、拠点数が増えても、設定変更や管理工数を最小限に抑えながら統制の取れたインターネット利用環境を実現しています。

導入後の姿

統制と利便性を両立したインターネット環境へ

docomo business RINK®のインターネットゲートウェイの導入後は、全拠点で同一のセキュリティポリシーを適用できるようになり、ガバナンスを強化しながらも、業務に必要なクラウドサービスやWeb利用を妨げない環境が整いました。

また、拠点ごとにセキュリティ機器を管理する必要がなくなったことで、運用負荷やコストも軽減。情シス部門は、日常的な保守作業から解放され、より戦略的なIT施策に注力できるようになりました。

同一セキュリティポリシーを運用

ガバナンス強化



セキュリティ機器の個別導入不要
拠点も同一運用

導入効果



- インターネット利用ルール・セキュリティポリシーの統一
- 通信ログの一元管理による可視化
- 拠点ごとの機器管理・更新作業の削減
- セキュリティレベルの平準化
- 運用負荷・コストの軽減



この事例からわかること

クラウド・SaaS 利用が前提となった現在、インターネット通信は「自由に使う」だけでなく、適切に統制・管理することが求められています。docomo business RINK®のインターネットゲートウェイのように、インターネット側（WAN 側）を接続する「出入り口」でインターネット利用を制御する仕組みは、セキュリティと利便性、運用効率を両立する有効な選択肢です。

docomo business RINK®に関するお問い合わせ

NTTドコモビジネス株式会社

NTTドコモビジネスコンタクトセンター（法人のお客さまからのお問い合わせ窓口）



0120-003300

受付時間 9:00～17:00

※携帯電話からもご利用になれます。土・日・祝日・年末年始は休業とさせていただきます。

サイト www.ntt.com/business/services/rink.html

●記載内容は2026年7月現在のものです。

●表記のサービス内容は予告なく変更することがありますので、お申し込み時にご確認ください。

●複数の商品・サービスを利用される場合には

お手元で計算された額と実際の請求書が異なる場合があります。

●フリーダイヤルのサービス名称とロゴマーク  はNTTドコモビジネスの登録商標です。

●記載されている会社名や製品名は、各社の商標または登録商標です。