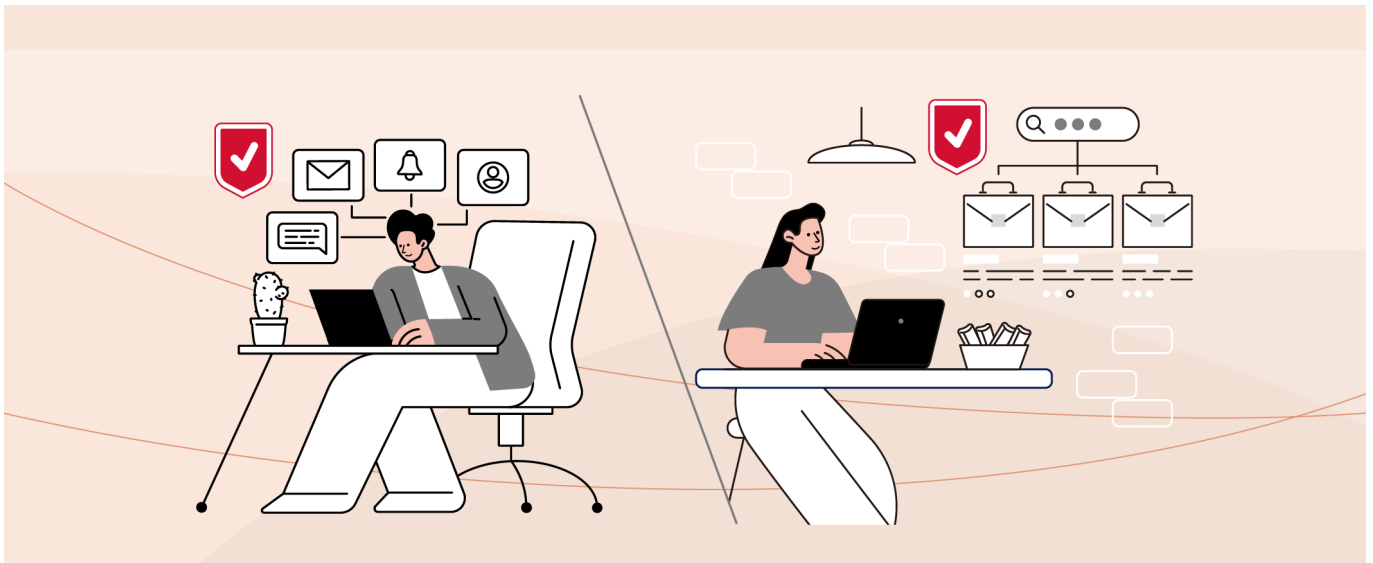




リモートワークを前提にした、安全で柔軟なアクセス環境へ

リモートワークやモバイルワークが定着した現在、社員が社外から業務システムやクラウドサービスへアクセスする機会は大幅に増えています。

一方で、従来の「社内ネットワークを前提としたアクセス設計」のままでは、セキュリティリスクの増大や、利用者・管理者双方の負荷が課題となりがちです。

ここでは、実在の企業をモデルにした想定事例を通じて、**リモートワークを前提にしたアクセス環境を、どのように整理・最適化できるのか**をご紹介します。

業 種 サービス業

規 模 従業員 約700名

勤務形態 リモートワークがメイン

IT体制 情シス部門が全社IT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

VPN前提のリモートアクセスが限界に

同社では、リモートワーク導入当初からVPNを利用した社内システムへのアクセス環境を整備していました。

しかし、利用者の増加や業務の多様化に伴い、VPN接続時の遅延や不安定さが社内ネットワークへの通信に集中。利用者サポートやアカウント管理の負荷増大といった問題が顕在化していました。

さらに、社外からのアクセスが増える中で、ID・認証管理や端末セキュリティをどう担保するかも大きな課題となっていました。

リモートアクセスの管理運営が煩雑に



解決

リモートワークを前提に設計されたアクセス環境へ

そこで同社は、リモートワークを前提に、アクセス制御とセキュリティを統合して提供する docomo business RINK® のリモートアクセスを採用しました。

業務システムやクラウドへのアクセスをユーザー単位で制御できるようにすることで、社内ネットワークへの不要な集中を回避し、利用場

所を問わずに安定したアクセス環境を確保、ID・認証・アクセス統制（ID管理・アクセス管理）を軸とした安全なセキュリティ基盤へ移行。従来の「社内に入るためのVPN」ではなく、**業務に必要なシステムへ安全にアクセスする**という考え方に切り替えました。

導入後の姿

安全性と利便性を両立したリモートアクセス

docomo business RINK® のリモートアクセスの導入により、リモートワーク時の通信品質は安定し、利用者からの問い合わせやトラブルも大幅に減少しました。

また、ID を起点にしたアクセス管理により、利用者の増減や役割変更にも柔軟に対応可能に。情シス部門は、日常的な VPN 管理や個別対応から解放され、運用負荷と管理コストの軽減を実現しました。

快適に各拠点など社内同等の環境にアクセス可能



安全・利便両立

安定品質

運用・稼働軽減

利用者の増減を柔軟に対応

導入効果



- リモートワーク時の通信安定性向上
- 社内ネットワークへの通信集中の解消
- ID・認証を軸としたアクセス統制
- 利用者サポート・運用負荷の削減
- セキュリティと利便性の両立



この事例からわかること

リモートワークが前提となった現在、「社内ネットワークにどう接続するか」ではなく、「**誰が、どの業務システムに、どう安全にアクセスするか**」という視点でアクセス環境を設計することが重要です。

docomo business RINK® のリモートアクセスは、働く場所に縛られない業務スタイルを支えながら、セキュリティと運用効率を両立するアクセス基盤を提供します。

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。