つなごう。驚きを。幸せを。
docomo Business

地域中核病院が取り組む情報漏洩対策 RINKを活用した多層防御で患者データを守る事例

課題　セキュリティ強化　業種　医療・介護

日本のある地域に複数の分院を持つ中核病院B病院。従業員数は医師や看護師、事務スタッフを含めて約1,000名にのぼり、1日に数百人の患者を受け入れる大規模医療機関です。
近年は電子カルテやオンライン予約システムなど、ITを活用した医療サービスが急速に普及し、診療情報や患者個人情報といった機密性の高いデータを大量に扱うようになりました。一方で、医療機関がサイバー攻撃の標的になりやすいというニュースが相次ぐ中、「万が一、情報漏洩が起きれば病院の信用が揺らぐ」といった不安が増大。セキュリティ強化を急務と考えたIT担当部門は、外部の専門ベンダーに相談し始めます。

しかし、B病院のIT部門は限られた人員と予算の中で、ネットワークを含むシステム全体を運用してきました。いくつものセキュリティ機器を個別に導入しても、それぞれの保守や運用を行うのは容易ではありません。そこで提案されたのが、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）が提供する統合ネットワークサービス「docomo business RINK®（以下、RINK）」でした。

RINKは、ネットワークとクラウド型セキュリティ機能を一体化して提供し、閉域網とインターネット接続、モバイルや固定回線など多彩なアクセス形態をワンストップで管理できるサービスです。

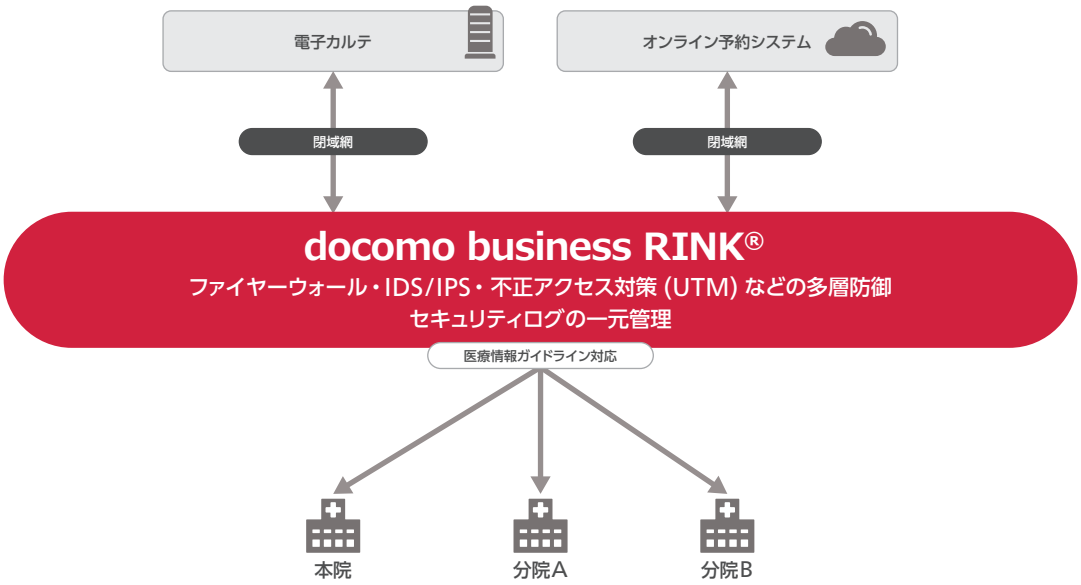
クローズド接続で電子カルテを安全に運用

電子カルテや医療システムは、インターネットから直接アクセスできる環境に置くと、サイバー攻撃のリスクが高まります。B病院ではRINKのクローズド接続（Flexible InterConnect や専用VPN）を利用し、電子カルテシステムを閉域環境で運用することにしました。これにより、院内で発生するトラフィックはインターネットと分離され、外部からの不正侵入や悪意ある通信を大幅に遮断。医療情報システムの安全管理に関する各種ガイドラインや法規制にも準拠しやすいネットワーク構成を実現できたのです。

©NTT DOCOMO BUSINESS, Inc. All Rights Reserved.

多層防御を実現するクラウド型セキュリティ

さらに、患者情報や診療データを扱う端末から外部クラウドサービスへアクセスする場合には、クラウド型のUTM（統合脅威管理）機能を備えた「Flexible Secure Gateway」を組み合わせることで多層防御を強化。ファイアウォール、IDS/IPS、不正アクセス対策など複数の防御層を設けることで、内部・外部を問わずさまざまな脅威を包括的にブロックし、情報漏洩リスクを大きく低減しました。セキュリティログはクラウド上で一元管理され、IT担当者はWebポータルを介して院内各所のアクセス状況や警告をまとめてチェックできます。



法令遵守とセキュリティ運用の両立

B病院にとって、医療情報システムに求められるのは常に高い信頼性と法令遵守です。例えば「医療情報システムの安全管理に関するガイドライン」では、システム間連携の際に厳格なアクセス制御やログ監査を実施するよう推奨されています。RINKなら、クラウド型セキュリティで発生するログをまとめて保管・監視できるうえ、アクセス権限や通信ルールの変更もWebポータルで即時に反映が可能です。したがって、院内のシステム変更やガイドラインの改訂にもスピーディに対応でき、セキュリティ面と運用面の両立を実現しました。

加えて、クラウド型のセキュリティサービスを利用することで、従来のように高価な専用機器を多台数導入する必要がなくなり、導入コストの圧縮にも成功。セキュリティ機器の保守やアップデート作業もNTTドコモビジネス側に任せられるため、院内IT担当者の負荷が大幅に軽減されました。

安心感の向上と運用負荷の軽減

RINK導入後は、患者の個人情報や診療データを扱う端末からの通信が多層防御でしっかり守られ、院内ネットワーク全体の可視化が進んだことで、万が一のトラブルにも迅速に対応できる体制が整いました。電子カルテシステムやオンライン予約を利用する医師や職員からは「システム応答が安定していて、セキュリティ対策に対する安心感が増した」と好評です。

院長や経営陣も、「情報漏洩がもたらす社会的ダメージは計り知れず、早期に手を打ててよかった」と評価。万全の対策とはいかないまでも、高度なセキュリティをクラウドサービスとして継続的に享受できる仕組みは、医療サービスの質を維持しながら運用コストを抑えるうえでも有効と考えられています。「医療機関として、セキュリティは後回しにできない課題」という認識が院内全体に浸透したことも、大きな成果といえます。

もし「電子カルテなどの重要システムを、インターネットと分離して安全に運用したい」「多層防御を導入したいが、IT担当者が少なくて難しい」という課題をお持ちでしたら、RINKの活用をぜひご検討ください。ネットワーク・セキュリティの両面を包括的にサポートし、医療機関の重要データを守りながら、運用負荷を軽減する具体的な方法が見つかるはずです。

本想定事例におけるポイント

POINT

● 閉域ネットワークで電子カルテシステムを保護

RINKのクローズド接続機能により、インターネットと切り離された環境で運用。外部からの不正侵入を大幅に抑制。

● 多層防御を可能にするクラウド型セキュリティ

ファイアウォール、IDS/IPS、不正アクセス対策など複数の防御レイヤーを統合し、患者情報や診療データを強固に保護。

● ログ管理・アクセス監査による法令遵守

セキュリティログをクラウドで一元管理し、必要に応じてガイドラインや監査要件にも柔軟に対応。電子カルテや患者データのやり取りを可視化し、コンプライアンスを強化。

● 導入・運用コストとIT担当者の負担を軽減

クラウド型セキュリティにより専用機器が不要になり、保守アップデートはNTTドコモビジネス側に委託。院内IT部門はコア業務に集中できる体制を整備。

docomo business RINK®

いつでも、どこからでも、安心・安全・簡単につながる新たなセキュリティ一体型のネットワークサービス

「クラウド型セキュリティ×ネットワーク」「オープン接続×クローズド接続」「モバイルアクセス×固定アクセス」の融合を実現し
企業が求める多様なネットワークと、複数のクラウド型セキュリティ機能を一体提供するサービス。
お申込みや設定変更もWebポータル上で簡単・迅速に完結できます。

サービス概要や料金プラン、導入にあたっての詳細ステップなど、お気軽にお問い合わせください。

お問い合わせはこちら >