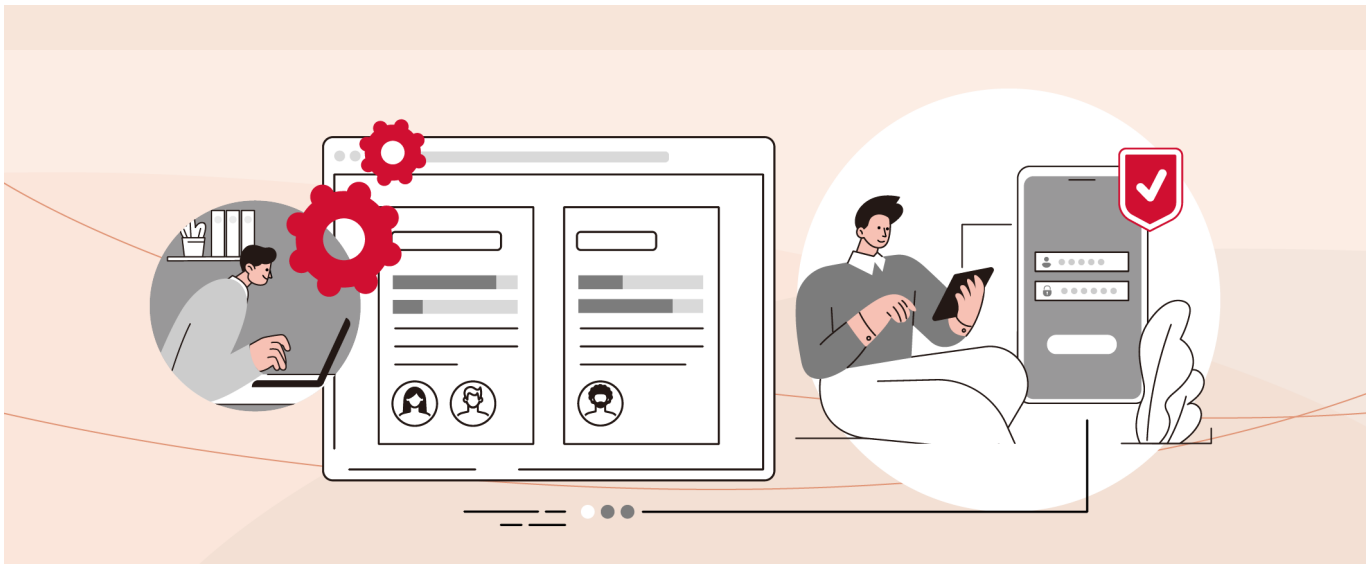
つなごう。驚きを。幸せを。
docomo Business



SaaS・クラウド利用時の不正アクセスリスクを“入口”で防止し、認証管理をシンプルに

クラウドサービスやSaaSの利用が広がる中で、IDとパスワードを起点とした不正アクセスや情報漏えいは、多くの企業にとって現実的なリスクとなっています。
特に、サービスごとにID管理や認証方式が分かれている場合、利用者・管理者ともに負荷が高まり、セキュリティ対策が形骸化してしまうケースも少なくありません。

ここでは、実在の企業をモデルにした想定事例を通じて、**不正アクセスを境界で防止し、認証管理を効率化する考え方**をご紹介します。

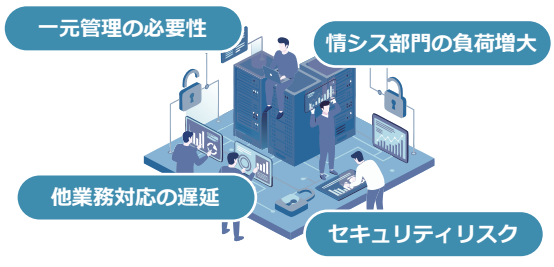
業　種	ITサービス業
規　模	従業員 約400名
利用環境	複数のクラウドサービス・SaaSを業務で利用
IT体制	情シス部門がID管理・セキュリティを担当

※本事例は実在の企業をモデルにした想定事例です。

課題　ID管理の分散が招くセキュリティリスクと運用負荷

同社では、SaaSやクラウドサービスごとにID・パスワードを管理しており、利用者の増減や異動のたびに、個別にアカウント管理を行っていました。
その結果、**パスワードの使いまわしによる不正アクセスのリスク、退職者・異動者のアカウント削除漏れ、問い合わせ対応や設定変更に追われるなど課題が顕在化**。
セキュリティ対策を強化したい一方で、運用が複雑になることへの懸念も大きくなっていました。

退職者・異動者の ID 管理による情シス部門の課題



解決　IDaaSによる認証の一元化と境界対策

そこで同社は、**ID・認証をクラウドで一元管理するdocomo business RINK® のIDaaS**を導入し、認証の仕組みを整理しました。
業務システムやSaaSへのアクセスをIDaaSを介して制御することで、多要素認証によるセキュリティ強化や、ユーザーのID・パスワードの一元管理によって管理者の運用業務の大幅削減を実現。
不正アクセスを「侵入後に検知する」のではなく、**そもそも境界で防止する**という考え方へ切り替えました。

導入後の姿　安全性と運用効率を両立した認証環境

IDaaSの導入により、利用者は複数のサービスを意識することなく、シンプルな認証で業務を行えるようになりました。
一方、情シス部門では、ID管理や認証設定を一元的に行えるようになり、運用負荷と管理コストを大幅に削減。
セキュリティレベルを引き上げながらも、業務の利便性を損なわない認証環境が整いました。

業務アプリのセキュリティと利便性を向上

導入が簡単

統一されたIDとパスワードポリシー

不正アクセスを防止

セキュリティレベルを向上

導入効果

- 不正アクセスリスクの低減
- 多要素認証によるセキュリティ強化
- ID・認証管理の一元化
- アカウント管理工数・問い合わせ対応の削減
- 利便性とガバナンスの両立

この事例からわかること

クラウドサービスや SaaS の利用が広がり**セキュリティリスクを“境界”で防止し、認証管理をシンプル**に。
docomo business RINK® の IDaaS を活用した認証の一元化は、不正アクセス対策と運用効率を同時に高める、現実的で効果の高いアプローチです。

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