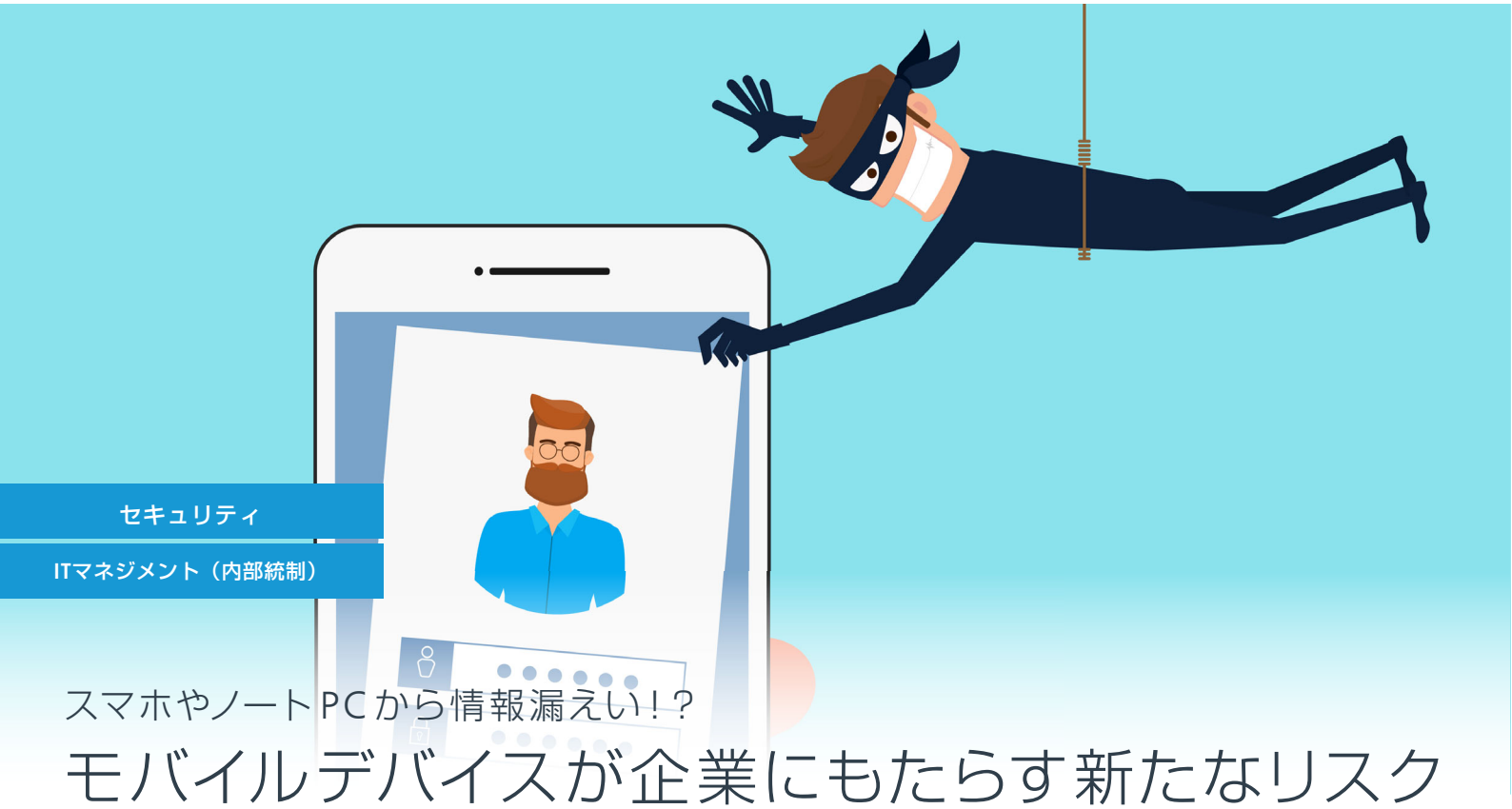

セキュリティ

ITマネジメント（内部統制）

スマホやノートPCから情報漏えい！？

モバイルデバイスが企業にもたらす新たなリスク

ICT技術やデバイスの進化により、個人保有のスマホやタブレット、ノートPCなどを業務使用するBYOD (Bring your own device)が拡大しています。一方、セキュリティ面のリスクが増大していることも忘れてはなりません。「従業員のノートPCが出先でマルウェアに感染」「業務データをコピーしたスマホを紛失」など、モバイルデバイス活用によるセキュリティリスクと、情報漏えいを防ぐしくみについて解説します。

フリーWi-Fiによるマルウェア感染、業務データのローカル保存

ノートPCやタブレット、スマートフォン、IoT機器など、デバイスの高性能化・多様化が急速に進んでいます。出先でも業務を行えるようになるなど、業務は大幅に効率化され、在宅勤務など働き方改革の促進にも寄与しています。

一方で、セキュリティ面のリスクも増大しています。例えばノートPCなどによる社外でのインターネット接続にカフェなどで提供されているフリー Wi-Fiを利用しているケースです。これらは通信が暗号化されておらず、第三者から盗聴される危険があります。サイバー攻撃者の手によってフリー Wi-Fiが設置されることもあり、利用することでマルウェア感染の可能性もあります。社外でマルウェアに感染した場合、会社へ戻ってデバイスを社内ネットワークに接続した結果、マルウェアが全社へ広がってしまうことすらあります。

デバイスの盗難や紛失によるデータ流出も考慮すべき点です。社内の業務データをコピーしたデバイスが出先で盗難や紛失に遭うことによって、大規模な機密情報の漏えいにつながることもあります。第三者が容易にログインできない認証システムはもちろん、ローカルに業務データを残しておかないなど運用面での対策も必要です。

社内の業務においても、さまざまなリスクが生まれています。例えば、部門単位で安価なWi-Fiアクセスポイントや、リモートアクセスが可能な外付ハードディスクを導入している場合、外部から不正アクセスを許して情報漏えいが発生するリスクがあります。ある企業では、スマートフォンを充電しようとPCのUSBポートに接続したことで機密情報が漏えいした例もあります。この企業はPCへのデバイス制御を行っていたのですが、スマートフォンの充電モードについては対象外だったのです。

エンドポイント、ゲートウェイ、監視による「多層防御」が主流

このようなことから、モバイルデバイスやIoT機器におけるセキュリティ対策には、マルウェアなど対する備えのみならず、ネットワーク監視や情報資産管理などで社内の状況も可視化するなど、さまざまなセキュリティ対策を組み合わせた「多層的な防御」が必要となります。

多層防御のポイントは主に3つあります。1つめは、モバイルデバイスによる出先でのアクセスや在宅勤務に対する「エンドポイント対策」。2つめは、ネットワークでの不正通信をファイアウォールやUTM（統合脅威管理）などで守る「ゲートウェイ対策」。最後に、セキュリティ専門家による「情報システムの監視」です。

しかし、これらを実行するにはセキュリティについての高度なスキルや専門知識が必要になるため、社内に人材を抱えるのは難しいのが多くの企業の実情です。そのため、これらを複合したセキュリティ対策を「クラウド上」で提供するサービスが増えています。

モバイルデバイスに対応しやすい「クラウド型」セキュリティ対策

NTT Comが提供する「マイセキュア ビジネス」は、多層的なセキュリティ対策を「フルクラウド型」で提供するサービスです。モバイルデバイスなどのエンドポイントにおけるマルウェア対策は高い検出率を誇り、ランサムウェアにも対応。未知の脅威に関しては危険か安全か判定が難しいため、ローカル端末の中に隔離された仮想環境（サンドボックス）を用意し、その中で振る舞い検知をするほか、振る舞いでも判定がつかない場合は継続監視を行います。Webブラウザからアクセスできる管理画面で、社内の全端末を集中管理することも可能です。

パスワードや端末による認証をユーザーごとに設定できる「Arcstar Universal One クラウドWi-Fi」というクラウド型認証基盤の提供サービスもあります。アクセスポイントなどWi-Fi環境に必要な機器一式のレンタルサービスもあるので、「エンドポイントでのセキュアなWi-Fiネットワーク構築を急ぎたい」という場合の選択肢となるでしょう。

“全部お任せ”のマネージドセキュリティサービスも

ICT部門のリソースに限りがあり「セキュリティ担当の確保が難しい」という企業は少なくありません。そういった場合、リスクマネージメント業務をアウトソースする選択肢もあります。NTT Comグループが提供する総合リスクマネジメントサービス「WideAngle」では、エンドポイントとネットワークでのセキュリティ対策に加えて、社内に設置したセキュリティ機器の運用監視／ログ監視をサービス側で行い、インシデント発生時の対応を支援するマネージドセキュリティサービス（MSS）を提供しています。

AI（人工知能）を搭載したSIEM（セキュリティ情報イベント管理）エンジンと、世界16カ国、1,500名以上のセキュリティ専門家によるセキュリティオペレーションセンター（SOC）のリスクアナリストが、ユーザーのICT環境を24時間365日監視します。リスクマネージメント業務のアウトソースによって社内のICT部門は、ビジネス戦略に関わるICT活用計画など、生産性の高い作業へリソースを振り向けることが可能になります。

これら多層防御に必要なセキュリティ対策は、企業ごとのポリシーや設備の状況、投資への考え方によって異なります。セキュリティ対策に高度な専門性が求められる時代、自社に必要なサービスやソリューションの見極めは、知見やノウハウを持つベンダーから情報を収集することが第一歩となるでしょう。

関連サービス

マイセキュア ビジネス	クラウドにある最新のセキュリティテクノロジーを最小の管理コストで実現します。 先進の「ファイル形式&行動認証テクノロジー」を、クラウドコンピューティングのパワーと組み合わせることで、既知の脅威をブロックし、ゼロデイ攻撃を防止します。
Arcstar Universal One クラウドWi-Fi	アクセスポイントのレンタルから認証基盤まで、セキュアなWi-Fi環境に必要なすべてをNTTコミュニケーションズが一元的に提供します。 さらにアクセスポイント設置やLAN配線工事などを行い、ネットワークと合わせて24時間365日保守対応するプランも提供することで、お客さまの負担を軽減し最適なWi-Fi環境の構築を実現します。
WideAngle マネージドセキュリティサービス	人工知能搭載のSIEMエンジンとセキュリティオペレーションセンター(SOC)のリスクアナリストが、ICT環境を24時間365日サポート。高度なセキュリティ監視により、実在するリスクと潜在リスクを可視化します。 また、「NWセキュリティ」をはじめとするセキュリティ対策パックメニューや、「リアルタイムマルウェア検知」などの機能をご用意、様々なご要望に応じて総合的なセキュリティソリューションを提供します。