セキュリティ

ITマネジメント（内部統制）

ITの進化が招く新たなリスク

# リモートワーク／IoT時代の「シャドーIT」対策とは

IT技術やインターネット、クラウドサービスの進化により、今では個人用デバイスでも業務を行うことが可能になりました。こうした状況は、働き方改革の主要な施策であるリモートワークを後押ししますが、同時に企業が把握していないデバイスで業務が行われる「シャドーIT」が発生するリスクも含んでいます。このリスクは、部署単位で導入されているルータや外付けHDDなどのIoT機器にも存在するのです。ここでは、リモートワーク／IoT時代にシャドーITへどのように取り組めばよいかについてご紹介します。

## 個人用デバイスを業務に利用する際のリスク

近年、スマートフォンやタブレットといった個人用デバイスの高性能化、高機能化が進んでいます。また、インターネットが高速化した上に、公衆無線LANサービス（Wi-Fi）の普及で、時と場所を選ばず利用できるようになりました。さらには、クラウドサービスの多様化により、クラウド経由で業務を行うことも可能になっています。結果、社外でも個人用デバイスを使って業務が進められるようになったのです。

このような個人用デバイスを業務に使用することを、BYOD（Bring Your Own Device）と呼びます。従業員が常に持ち歩いているデバイスで業務を行うことができれば、出先での対応が可能になりますし、日報の提出や経費の精算などといった業務のために会社へ戻る必要もなくなります。これは移動時間を削減し業務効率を向上させますし、残業時間の短縮にもつながります。そのため「働き方改革」の主要な施策とされるリモートワークを推進する上でも個人用デバイスは役立つでしょう。

一方で個人用デバイスを業務に使用すれば、仕事上の機密情報やアドレス帳に顧客情報、各サービスへのログイン情報なども格納していることがあります。そのため、紛失や盗難に遭った際には、所有者の情報が漏えいするだけでなく、業務上のメールやファイルを閲覧され、社内サーバーやクラウドサービスなどにアクセスされて、機密情報も漏えいしてしまう可能性もあります。

特に注意したいのは、BYODが許可されていないにも関わらず、従業員が勝手に個人用デバイスを業務で使っており、企業がその存在を認識していないケースです。これを「シャドーIT」と呼んでいます。

## 社内にも存在する「シャドー IT」の IoT 機器

シャドー ITと見なされるのは、個人用デバイスだけではありません。企業においても、外付けハードディスクドライブ(HDD)やWi-Fiアクセスポイントなどの機器を、報告書を上げずに部署単位で導入していませんか。これらもシステム部門などの管理者が存在を把握できていない上に、インターネットに接続する機能を持つので、シャドー ITと見なすのです。

近年はさまざまな機器のIoT化が進みました。例えば、HDDなら出先からアクセス可能な製品が増えています。それは同時にインターネットを通じて第三者からアクセスされてしまう可能性もあるのです。また、部署内でしか使わないからと、Wi-Fiに暗号化やパスワードを設定していなかった場合は、無線の届く範囲にいる第三者がネットワークへアクセスしてくるリスクがあります。こうした状態を放置しておくと、不正アクセスやマルウェア感染、情報漏えいなどにつながるおそれがあります。

BYODや部署が報告していないなどのシャドー IT以外でも、不正アクセスのリスクが認識されていない機器が社内に存在していることもあるのです。例えば、会議室などにブルーレイレコーダーを設置していないでしょうか。それらには、外出先から録画予約や、録画した番組をスマートフォンなどの端末で視聴するなどの機能を搭載しているものがあります。つまり、インターネット環境に接続できるIoT機器なのです。それらのIDとパスワードが初期状態のままだと、メーカーによっては製品共通のものになっているかもしれません。そのようなIoT機器は外部から不正アクセスされる可能性があります。

実際、こうしたIoT家電や監視カメラがインターネットから侵入を受け、「Mirai」などのマルウェアに感染するケースが世界中で発生しています。感染した機器はサイバー攻撃者の指令により、DDoS攻撃などを行ったりします。つまり、知らないうちにサイバー攻撃へ加担することになってしまうのです。

## ネットワークへのアクセスの把握と監視を

シャドーITへの対策としては、社内のネットワークに接続されるデバイスを把握することが重要ですが、その際に効果的なのがIT資産管理ツールです。こうしたツールでは、登録されていないデバイスがネットワークへアクセスしようとしたとき、管理者が許可／不許可を判断することになりますが、誰がどんなデバイスでアクセスしようとしたのかを確認することで、シャドー ITの存在を明らかにできます。

IT資産管理ツールを導入すれば、許可されたデバイスのみネットワークに接続可能になるため、BYOD管理につながります。同時にスマートフォンやスマートデバイスなどのデバイスにもIT資産管理ツールをインストールすることで、内部を業務用エリアと個人用エリアに分け、業務用エリアでは必要最小限のアプリのみ動作可能にするということも可能です。また、MDM(モバイルデバイス管理)を導入すれば、デバイスが紛失や盗難に遭った際、遠隔でロックや初期化を行えるので、万が一への対策になります。

ツールによる対策と同時に、部署単位で導入されるIoT機器に対しては、事前に必ずシステム部門の許可を得るか報告を行うよう制度を整備しましょう。また、ハードディスクやレコーダーなどの機器を設置する際には直接インターネットへ接続せず、ルータやスイッチを介して接続すれば、不正アクセスが難しくなります。

## 関連サービス

| | |
|---|---|
| **WideAngle<br>マネージドセキュリティサービス<br>NWセキュリティ** | ファイアウォールやIPS/IDS、アンチウイルスなど、ご要望の高いネットワークセキュリティやコンテンツセキュリティを一括してアウトソーシングできるパックメニューです。<br>セキュリティ運用基盤(SIEM)とリスク分析官による相関分析で、ファイアウォールなど機能単体での運用では気がつかない未知の脅威をあぶりだします。 |
| **マイセキュア ビジネス** | 標的型ウイルスなどの新たな脅威からPC、スマホなどを守る超高速・超軽量の次世代型エンドポイントセキュリティサービス。Webベースの管理コンソールひとつで、すべてのエンドポイント端末の集中管理が可能なため、働き方改革のセキュリティ対策を強化できます。 |
| **Box over VPN** | 社内・取引先とのファイル共有や、Salesforceなどの業務アプリケーションとのシームレス連携を可能にする“コンテンツ・マネジメント・プラットフォーム”です。<br>ファイルの保管時にAES256bitでファイルを暗号化。ISO27001と27018という世界標準の情報セキュリティマネジメントシステムに準拠しています。 |
| **Global Management One** | ICT環境の監視、運用並びに最適化業務をワンストップで行うリモート・インフラストラクチャ・マネジメントサービスです。ITILのベストプラクティスにもとづき、高度な運用プラットフォームや幅広いスキルを持ったサービスマネージャーとサービスデスクによって、お客さまのICT環境の個別のニーズに即したサービスを提供し、ITシステムの投資対効果の向上に貢献します。 |