セキュリティ

ICTシステム環境の最適化

元従業員からの情報漏えいも!?

# IDの一元管理と多要素認証で情報を守る!

「テレワーク」を働き方改革の一環として導入する企業が増えつつあります。しかしセキュリティの観点からすると、テレワークなどによるリモート環境から社内サーバーへのアクセスが増加する場合は、アクセス権限などの管理強化を行うべきでしょう。もし管理が行き届いていなければ、退職者や転職者などの元従業員にリモート環境から社内サーバーへ不正アクセスされて情報漏えいというケースが考えられます。そういったセキュリティリスクを生まないために、企業の情報管理者は各従業員のIDを、退職や転職、あるいは部署や職位などの異動などによるアクセス権限の変更を、厳密に管理することが重要です。ここでは、クラウド利用にも対応するSSO(シングルサインオン)「ID Federation」と「Arcstar Universal One」のオプションサービス「クラウドWi-Fi」を通じて、テレワークにおけるセキュリティ管理について解説します。

## IDの放置が情報漏えい事故につながる

従業員のID管理にActive Directoryを利用している企業は少なくありません。そのメリットとしては、従業員をPCやデバイスとひも付ける設定を均一化できるほか、従業員ごとのアクセス権限なども管理できるので、管理者の手間を大幅に減らすことが挙げられます。一方で、異動や入退社など、従業員に動きがあったときには遅滞なく登録内容の変更・新規登録を行う必要があります。このときIDを古い状態のままにしておくと、元従業員といった外部の第三者から不正にアクセスされる可能性があり、情報漏えいなどの被害につながってしまいます。

退職・転職をする従業員の情報で削除が必要なものは、Active Directoryだけではありません。最近では、業務においてさまざまなクラウドサービスも利用するケースが増えており、これらのアカウントも削除する必要があります。もし第三者がアクセスできてしまうと、顧客のデータや進行中のプロジェクトの状況など、重要な情報を持ち出されてしまう危険性も考えられます。

同様に社内にWi-Fiを導入している場合は、そのアクセス管理にも注意が必要です。一般的に、Wi-Fiへの接続はアクセスポイント側のID(SSID)とパスワードを使ってアクセスしますが、ユーザー認証を実施していない場合、電波の届く範囲なら第三者でもログインを試みることができます。IDとパスワードが第三者に知られてしまった場合、簡単に社内サーバーにアクセスできてしまうのです。

## 従業員のID管理に最適な「ID Federation」

このように、情報漏えい対策において従業員のID管理は極めて重要です。そこで効果的な対策を導入する必要が出てくるのです。その対策としてNTT Comが提供する「ID Federation」は、クラウドサービスを含む複数のIDを統合して管理できます。特にSSO（シングルサインオン）に対応しているという点は、管理者とユーザーの双方にメリットをもたらします。

Active DirectoryとSSO連携ができるので、管理者はユーザーのアプリ利用状況を管理者ポータルやログ情報から一元的に閲覧・管理することができます。部員や社員、パートナーなどといったユーザー属性に応じて、利用できるアプリを管理者が一括制御することも可能です。

ユーザーは認証が一元化されるので、1つのパスワードですべてのサービスにログインできるようになります。

さらに多要素認証にも対応しているので、ID・パスワードに加えて、登録されたIPアドレスからのみアクセスできる「IPアドレス制御」機能や、本人性を担保する「指紋認証」などの認証メニューを追加することで、認証強度を高めることができます。

「ID Federation」のSSOは、特にクラウドサービスとの連携機能が充実しています。「Office 365」や「G Suite」、「Box」、「Salesforce」などの主要なSaaSはもちろん、1,700を超える種類のSaaSへのシングルサインオンを実現します。また、ユーザーが自社で構築した業務アプリケーションと接続できるソリューションも用意されています。

「ID Federation」の認証機能の一部には、IDアクセス管理ソリューションの先駆者であるPing Identity社の技術を採用しています。またユーザーの要望に合わせ、Ping Identity社のサービスを用いたソリューションを利用することも可能です。クラウド型／オンプレミス型の認証ソリューションが用意されており、ID数や接続アプリ数の変動に応じた料金体系なので、ユーザーのROI（投資利益率）にも貢献するサービスといえるでしょう。

## セキュアで柔軟なWi-Fi環境を実現する「クラウドWi-Fi」

クラウド型の認証ソリューションとしては、NTT Comが提供するキャリア品質で国内外のシームレス化を実現した、高品質・高信頼のネットワークサービス「Arcstar Universal One」のオプションサービス「クラウドWi-Fi」が有効です。クラウドWi-Fiは、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環境に必要なものすべてをNTT Comが一元的に提供するサービスです。

このサービスでは、機器の提供だけでなく、煩雑なネットワーク設定から高度な知識を求められるWi-Fi環境の設計、さらにLAN配線やWi-Fiアクセスポイントの設置工事（壁面など）までNTT Comがワンストップに対応するというのが特長となっています。

クラウド型の認証基盤を利用することで、パスワードや端末による認証をユーザー単位に設定できます。これによりID／パスワードの使い回しを防止できるので、セキュアなWi-Fi環境が実現できるのです。また、従業員が他の事業所に出張をした場合でも、本サービスを導入しているロケーションであれば、社内環境やインターネットへ容易にアクセスすることが可能になります。認証設定はポータル上でオンデマンドに変更できるため、従業員の異動や退職などへの対応も迅速かつ柔軟に行えるしくみです。これにより第三者からの不正アクセスの防止や、異動によるID変更にも素早く対応することが可能になります。

また問い合わせやサポート、料金精算の窓口も一元化されているので、管理者の負担が軽減されます。料金については、設計・工事費用を含めた初期費用・月額料金が設定されているので、導入コストも簡単に算定することが可能です。なお、10IDまで無料で利用できるため、小規模オフィスやブランチオフィスなどに導入しやすくなっている点も特長です。

こうしたサービスを活用すれば、従業員や関係者のIDの状況を常に最新に保ち、システムやネットワークへの不正なアクセスを防ぐことができるようになるでしょう。

## 関連サービス

| | |
|---|---|
| **ID Federation** | Office 365・G Suite・Boxなどの1,700以上のSaaSアプリをはじめ、お客さまのオンプレミスアプリやActive Directoryとも連携し、シングルサインオン・アクセスセキュリティ強化を実現する認証サービスです。 |
| **Arcstar Universal One クラウドWi-Fi** | Arcstar Universal Oneでは、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。 |
| **テレワーク・スタートパック** | 設定不要ですぐにセキュアなテレワークを始められる「テレワーク・スタートパック」。テレワークに必要なノートパソコン、モバイル通信、およびセキュリティサービスをパッケージ化。事前の設定も完了した状態でお届けします。 |