勝見 勉氏　宮川晃一氏

日本ネットワークセキュリティ協会

左が勝見氏、右が宮川氏。

いつでもどこからでも社内システムにアクセスできる環境が整備されつつある中で、企業のデータやシステムはどう守っていけばいいのか。日本ネットワークセキュリティ協会のセキュリティ市場調査ワーキンググループでリーダーを務める勝見 勉氏と、アイデンティティ管理ワーキンググループでリーダーを務める宮川晃一氏に、認証やアクセス管理の側面から話を伺った。

ID管理製品は伸び続ける

端末のログオン認証に依存しないセキュリティ環境の構築が重要

――マルチデバイス環境では、認証やアクセス管理における課題に変化が生じてきているようですね。

勝見氏（以下、敬称略）●モバイル環境が変わって、社外から社内システムにログオンする従業員の認証をどのようにするかが問題となっています。BYODに関連して端末認証の要素も重要度が増してきました。

宮川氏（以下、敬称略）●社外で端末を使用する際に、IDとパスワードだけでいいのかという問題が出てきますね。スマートデバイスでWebアプリケーションなどのIDやパスワードを記憶させておくと、端末が誰かに拾われた場合、端末ロックが解除されてしまえばWebアプリケーションが使われてしまいます。端末自体のログオン認証に依存してしまうと非常に危険なのです。そこで必要になるのが多要素認証です。例えば、ワンタイムパスワードやコールバック認証、二段階認証などですね。また、スマートデバイスは電子証明書も有効です。

勝見●電子証明書もどのように保持するかで効果が変わってきますね。スマートデバイス内にインストールされていて、自動でアプリケーションが手続きする仕組みだと、端末自体のログオン認証にセキュリティが左右されてしまいます。電子認証をする際に、再度IDとパスワードを入力する仕組みを用意したりすれば、端末自体のログオン認証に左右されずにすみます。

宮川●IT環境としては、クラウドサービスの採用も広がっています。クラウドサービスを利用する際には、スマートデバイスからクラウドサービスに直接アクセスするので、企業を通過しなくなります。この部分では、認証連携を利用する必要があります。まずは社内の認証基盤にアクセスして、その後クラウドサービスにアクセスさせる仕組みですね。

勝見●クラウドサービスベンダーも認証の仕組みを提供していますね。問題は認証のための情報をどう保持するかにあります。やはり、認証基盤はクラウド側に置くのではなく、企業側に置いて、社内システム経由でアクセスさせる方が、適

切なアクセスコントロールが可能です。

どのサービスを選択するかはどのレベルのリスクをとるかによる

――認証の強度と利便性の問題についてはどうでしょうか。

宮川●認証については、簡単にすればセキュリティのレベルが落ちてしまうので、ある程度の手間は許容しなければならないでしょう。社外からのアクセスだけに多要素認証を利用したいとか、アクセス先の状況によって認証のレベルを変えたいというニーズも高いですね。認証のライセンスは社外からアクセスする人員分だけでいいというシビアな要求もあります。認証システムは、どうしても人数分のコストになるため、コスト負担は重くなりがちです。

※認証連携で ID やパスワードなどのユーザー情報を管理する。ユーザーは IdP に ID やパスワードなどを入力して認証を受ける。

また、最近は社内システムのクラウド化を進める過程で、認証システムもクラウド化したいというニーズがあります。せっかく社内からサーバーをなくそうとしているのに、認証するためにまた社内にサーバーを置くのは矛盾するからです。

勝見●クラウドサービスとシングルサインオンを連携させると非常に便利になりますが、IdP（Identity Provider）※における個人の認証部分は結局残るため、IDとパスワードなのか、二要素認証なのか電子証明書なのかといった、本人や端末をどう判別するかという問題は残りますね。

――認証やアクセス管理はどこから始めるべきなのでしょうか。

宮川●例えば、メールやグループウェアなどの利用であれば、簡単な仕組みで大丈夫でしょう。メールサーバーから添付ファイルをダウンロードできないような仕組みでも情報漏洩は防げます。

勝見●本人確認のレイヤーとアクセスコントロールのレイヤーがありますが、本人確認のレイヤーはどこまで行っても同じなのですね。ID とそれに対応するパスワードなどをどう組み合わせるか。強度を高めれば使い勝手が悪くなり、コストは高くなります。何を選択するのかは、どのレベルのリスクをとるのかによります。コストを抑えるのならば、ID と固定パスワードですね。その場合は、パスワードの管理を徹底しなければなりません。

宮川●最終的には、守りたいものは何か

日本ネットワークセキュリティ協会では、アイデンティティ管理の意義からクラウド環境における ID 管理の運用までを詳述した書籍も執筆している。

というセキュリティの根本に行き着きます。

勝見●アクセスの管理レベルを情報資産の重要度のレベルに応じていくつか分けて、何段階かの強度のものを使い分けることになります。強度が必要なシステムやデータに対してはアクセスする人数が減ってくるので、多少コストがかかる認証手段を使っても、それほどコストには影響がでないでしょう。段階的なセキュリティ対策を施す手間はかかりますが、トータルのコストは抑えられます。

マイナンバーが認証基盤になる可能性も

――認証連携も進んできました。

宮川●認証連携の仕様の一つであるSAMLはかなりメジャーになってきているので、実装しているサービスは多いですね。企業向けのサービスではSAMLがよく使われています。マイクロソフトのADFS（Active Directoryフェデレーションサービス）もSAML準拠ですから。コンシューマー向けサービスのシングルサインオンに使われるケースが多いのはOpenIDですね。ただし、接続を容易にしたOpenID Connectという仕様が策定されており、企業で使って欲しいという動きを見せています。使い勝手のいい方を企業が選択していけばいいのではないでしょうか。

グローバル企業では、海外拠点とのシングルサインオンが課題です。以前は認証基盤を統合しようという話が多かったのですが、現在は認証連携の仕組みを構築すれば、グローバルでのシングルサインオンができるようになりました。グローバル企業ではそうした動きが活発化しています。認証基盤を統合するよりも、圧倒的にコストが安くなりますから。

勝見●グローバルで社内システムを統一させる動きも出てきています。セキュリティレベルを合わせるためにも認証連携が欠かせなくなるでしょう。また、認証基盤をクラウドに置けるのかどうかという問題もあります。アイデンティティ管理には組織情報や権限情報が入っているので、抜かれると困ってしまいますね。ただし、基幹システムまでもクラウド化するのであれば、認証基盤だけオンプレミスにするのはどうかという議論も出るでしょう。

――今後の市場動向における注目ポイントを教えてください。

勝見●ログオンとアクセスコントロールは従来から基本的なシステムには実装されていたので成熟しています。一方で、認証基盤を運用するためのアイデンティティ管理製品は伸び続けるでしょう。認証そのものについては、認証と管理の手間、そして信頼性の観点から判断すると、ワンタイムパスワードと生体認証がさらに利用されていくのではないでしょうか。

ワンタイムパスワードはハードウェアトークンやオンデマンドトークンまで様々ありますが、すべての利用率が上がるでしょう。生体認証は精度の向上とコストの低下が予測されます。今よりも持ち運びがしやすくなり、ユーザー側の負担は軽くなるでしょう。生体認証はなりすましがしにくいので、信頼性も高いですね。

それと、社会保障に関する共通番号「マイナンバー」は政府が保証するIDとなるため、簡略な認証基盤になる可能性もあります。