NetIQ

# 多要素認証：
## プロセスを簡易化しながらリスクを排除する

フラッシュポイントペーパー

**多要素認証の導入決定を促進する条件：**

- **指令の要求**
- **情報漏洩**
- **テクノロジ / インフラストラクチャの更新**

### パスワードは亡きもの

ユーザ名とパスワードによるユーザ認証という古い考え方は、もはや機能していません。それはなぜでしょうか？それには多くの理由があります。ユーザはパスワードの扱いに不注意です。明らかに分かるものや、すべての状況で同じパスワードを使用し、書きとめてデスクに置いておくこともたびたびあります。しかし、すべてユーザが悪いわけではありません。

ユーザ名とパスワードがアクセスの唯一の条件であることから、ハッカーに対してクラッキングに慣れた認証モデルを提供しているわけです。知恵がはたらく犯罪者は、高度なアルゴリズムを作成して侵入方法を見つけようとします。いくつもの状況で同じパスワードを使用していると、セキュリティを侵害したハッカーは、さらにアクセス手段を広げることができます。あるユーザの Facebook パスワードを盗み出したハッカーが、企業インフラストラクチャ全体にアクセス可能になる状況を想像してみてください。

すなわち、ユーザ名とパスワードを使用したモデルでは、ユーザが知っている情報にもとづき認証処理全体が行われるのです。そして、その情報を手に入れることや、盗むことが可能です。

### 話題は多要素認証 (MFA) へ

その名前のとおり、MFA はアクセスの手段として複数の識別情報を組み合わせたものです。複数使うだけでは不十分です。最良の方法は、異なる**種類**の識別情報の組み合わせです。理想として MFA の組み合わせは、何か**知っていること** (PIN コードなど)、物理的に**所有しているもの** ( キーカードやトークンなど )、そしてユーザ**本人** ( 指紋、網膜スキャン、音声認識など ) の 3 つのうちの 2 つを使います。3 つのうち 2 つを要求することで、セキュリティ漏洩のリスクが大きく減ります。

一般的に、銀行が PIN コードと合わせて社会保障番号を尋ねる場合、これは 2 つの別々の識別情報であり ( 一方は銀行のもの、もう一方はそれ以外のもの )、MFA と考えることができます。しかし、これらはともに自分が**知っていること**なので、あまり洗練された方法とは言えません。

### 概念自体は新しいことではない

新しいのは、その導入方法です。MFA は、ほとんどの人が日常的に利用していることです。ATM では、物理的に**所有する**カードと自分が**知っている** PIN 番号を使います。空港キオスクでは、クレジットカード ( 持っているもの ) をかざして、目的地 (知っていること) を 3 桁で入力してチェックインの手続きをする必要があります。クレジットカードの決済に写真入り ID カードを示すのも ( 写真が「自分自身」を照明する )、多要素認証です。

MFA の重要性は明らかです。2 つの異なる形の認証を必要とするシステムは、侵害するためにその場にいる必要があるので、安全性が高まります。東ヨーロッパにいるハッカーがユーザ名とパスワードを盗み出すだけでは不十分で、あなたが**持っているもの**や**本人**の情報を入手する ( あるいはなりすます ) 必要があります。これは容易ではありません。

### MFA がトレンドとなる背景

オンライン取引のアカウントに単一要素の認証を使用することのリスクとコストを認識する組織が増えています。このトレンドは代償が高くつきますが、MFA で流れを変えることができます。電子決済を現金支払いと同じように素早く確実に行うことが可能になります。

**「Verizon の 2013 年のデータ侵害レポートでは、単一要素認証がセキュリティ漏洩の主な要因に指摘され、2012 年に発生したネットワーク侵入の 76 パーセントは脆弱な認証情報や盗難によるものとされています。」**

MFA が必要とされるもう 1 つの要因が、HIPAA などの新しい政府規制や指令の登場です。2013 年 3 月 26 日、米国の保健福祉省による規則が発効され、HIPAA のセキュリティ / プライバシー要件の適用が拡大されて、請負業者、ベンダー、サービスプロバイダなどの関係会社、医療事業者に代わってサービスを行う請求会社


## 最善のMFAは、少なくとも2つの要素への対応が必要:

- ユーザが知っていること
- ユーザが持っているもの
- ユーザ本人

や、医療データや患者データを統合するソリューションの提供者にまで対象が広がりました。これに従わないと多くの罰金が科せられることから、多くの組織は医療データ / 患者データへのアクセスを防止するために MFA を検討しています。

さらには、生体認証もかねてより多くの機器に組み込まれています。スマートフォンや PC の指紋スキャナを利用することで、多くの企業は当面のところ、MFA を導入することが可能になりました。意識せずに手間なく認証が行えます。

### それほど優れた MFA が必ずしも利用されない理由

たいていの技術進歩と同じく、変化への抵抗はさまざまです。多くの企業は、( 指紋スキャナなど ) MFA に必要な要素が手元にあることに気づいていません。ユーザエクスペリエンスを複雑にする、導入に関する懸念もあります。多くの場合、使いやすさは効率性につながるので、たとえセキュリティであっても、組織はワークフローを犠牲にするのをためらいます。最後に、最も重要なのが、MFA のメリットを十分に活かすには、バックエンドのアクセスシステムのセットアップと最適化が必要になることです。得られた情報を処理できず、システム全体で導入ができなければ、そのメリットは理想的とは言えません。

### MFA の考え方を変えるとき

新しいテクノロジが広がるときは、誰もその影響を十分考えずに失敗することがよくあります。MFA の場合、始める前に考えるべきことがいくつかあります。

- 認証が特別な機能であるとか、セキュリティシステムのある部分に組み込まれたものであると考えない。独自に詳細な認証ポリシーを考えて確立する必要があります。
- MFA を用いる場所をすべて調査する ( アクセスポリシーとして MFA を用いるのであれば、その使用を心がける )。できるところで複雑さを排除します。
  - **管理をしやすく**。社内のそれぞれ異なるシステムに異なる認証システムを使って管理することは、何としても避けたいところです。
  - **使いやすく**。使いにくいものは、抵抗を受けます。同時に、シングルサインオンソリューションの導入も十分検討してください。これによりユーザは、多くの異なるパスワードを覚えることや、システムごとに再認証をする必要がなくなります。

適切に導入すれば、MFA は実際にユーザの負担を軽減するはずです。つまり、スキャナに指をかざして PIN コードを入力する方が、ユーザ名とパスワードを覚えるよりも簡単です。

### MFA のベンダーに求めること

MFA の導入は、セキュリティと生産性への取り組みを支える上で不可欠であることから、会社の業務方針とうまく連携させる必要があります。

**1. 必要とする認証のタイプや適用方法について、選択肢と柔軟性のあるソリューションを考える。**

**2. 一種類の物理的認証方法に固執しない ( 選択したハードウェアに認証ポリシーが依存することのないようにする )。**

**3. 新しいテクノロジの登場とともに積極的に更新されるオープンなフレームワークを開発するベンダーを探す。**

**4. 最後に、使いやすいシステムを構築するベンダーを探す。**

選択する MFA ベンダーは、プラグインや容易な統合により、さまざまな用途に幅広く応えるベンダーでなければなりません。識別情報管理システムと密接に連携して取り組む必要があります。また、シングルサインオンなど、エンドユーザが簡単に使えるようにサポートしてくれるベンダーである必要があります。

オンライン認証にはセキュリティの脅威が拡大を続ける中で、組織には困難に挑戦することが求められます。それを怠った代償は高くつきます。

何をすべきか、**www.netiq.com** でご覧ください。

www.netiq.com

**NetIQ**
ノベル株式会社

〒107-6329
東京都港区赤坂5-3-1
赤坂Bizタワー29階
電話 0800-100-5575（フリーダイアル）

info@netiq.com
www.netiq.com/communities
www.netiq.com/ja-jp/

北米、ヨーロッパ、中東、アフリカ、
アジアパシフィック、および中南米の
弊社オフィスの一覧については、
**www.netiq.com/contacts**をご覧ください。

**www.netiq.com**