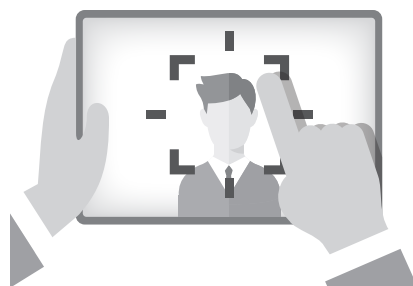


パスワードレスの時代が到来!?

「パスキー」を ビジネス利用する際の 留意点

パスワードレス認証の「パスキー」の導入が企業でも進んでいます。パスキーは、従業員個人の指紋や顔などの生体認証を利用するため、情報セキュリティやプライバシーの観点で留意が必要です。中小企業が導入する際の留意点を解説します。



弁護士法人みお総合法律事務所

弁護士

倉田 壮介

弁護士

石田 優一

パスキーとは どのような技術なのか

最近、ビジネスやプライベートにおいて、「パスキー」という用語を耳にする機会が増えました。パスキーは、Webサービスなどにログインする際に、パスワードの入力を不要にする技術です。2

023年は「パスキー元年」とも呼ばれ、今後、パスキーの利用頻度が、ビジネスの場において急速に増加することが予想されます。

パスキーを活用する際に、その仕組みを正確に理解する必要はありませんが、参考までにパスキーの技術の概要について、**図表1**の例を使って解説していきます。

図表1の「おてがる発注」は、

図表1 クラウドサービスにログインする際のパスキー利用の例

発注管理クラウドサービス「おてがる発注」では、パスキーによる認証ができます。具体的な利用方法は、次のとおりです。

- ① 利用者は、自分のスマートフォンに、当該クラウドサービスに対応したパスキー認証用の専用アプリを、あらかじめインストールしておく。
- ② 利用者は、利用登録の際に、パスキー認証用の専用アプリを起動して、スマートフォン上で指紋、顔、パスコード(PIN)などを用いて本人認証を行なう。パスワードを設定する必要はない。
- ③ 次回ログイン時は、スマートフォンで専用アプリを起動し、スマートフォン上で指紋、顔、パスコード(PIN)などを利用して本人認証をすれば自動的にログインされ、パスワードを覚えておく必要はない。

※「おてがる発注」は、現実に存在するサービスではありません。

パスキー認証によって、パスワードを設定しなくてもログインができます。

このパスキー認証には、非営利団体FIDOアライアンスがグローバルで標準化と普及を進めている「FIDO」(ファイド)とい

う新しい認証技術が使われています(図表2)。

(1) 利用登録時

パスキー認証に対応したサービスは、FIDOサーバという認証用のサーバと連携しています。

FIDOサーバは、利用者のデバイスに、「チャレンジコード」という1回限りのコードを送信します。デバイス側では、受け取ったチャレンジコードをハッシュ関数に入れて、ハッシュ化という処理を行ないます。

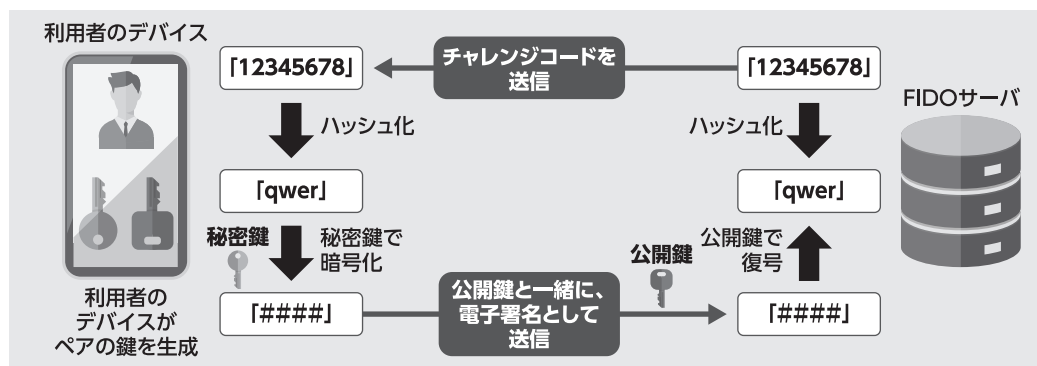
ハッシュ関数は、ある文字列を入れると(元の文字列を推測できない)特定の文字列を返す特徴があります。ハッシュ関数に入れて出てきた答えをハッシュ値といいます。

その後、ハッシュ値を暗号化するために、生体情報などで本人認証を行ない、秘密鍵と公開鍵という、ペアの鍵をデバイス側で用意します。

秘密鍵と公開鍵は別の鍵ですが、「秘密鍵で暗号化したものは公開鍵でしか復号できない」、そして、「公開鍵から秘密鍵を推測できない」という、不思議な特徴があります。

デバイス側では、ハッシュ値を

図表2 パスキーの利用登録時・ログイン時におけるイメージ



秘密鍵で暗号化して、公開鍵と一緒にFIDOサーバに送信します。FIDOサーバは、このハッシュ値を公開鍵で復号し、自分で計算したハッシュ値と一致するか

を検証します。

もし一致すれば、その公開鍵を、正規のものとして登録します。デバイスには、秘密鍵が、外部に漏れない形で大切に保存されます。

(2) ログイン時

ログイン時も、流れは利用登録時とおおむね同じです。

デバイス側は、デバイスの利用者が本人であることを生体認証などで確認したうえで、利用登録時に使用したのと同じ秘密鍵で、ログイン時に改めてFIDOサーバから送られてきたチャレンジコードをハッシュ化して得られたハッシュ値を暗号化し、FIDOサーバに送信します。

FIDOサーバは、利用登録時に登録した公開鍵で暗号化されたハッシュ値を復号し、自分で計算したハッシュ値と一致するかどうかを検証します。

仮に、送信されてきたものが、利用登録時に使用されていた秘密鍵で暗号化されていなければ（第三者のなりすましであれば）、2つのハッシュ値は一致しません。このような方法で、パスキー認証においては、パスワードを使うことなく、第三者によるなりすまし

しを防止することができます。

(3) 秘密鍵をクラウド上で同期させる技術

ここまで説明したパスキー認証の仕組みには、大きな欠点があります。それは、秘密鍵が保存されたデバイスが故障すると、パスキー認証ができなくなってしまうことです。

この問題を防ぐために、最近では、クラウド上に秘密鍵を同期させて、複数のデバイスでパスキー認証ができるようにする技術が普及しています。

パスキー導入時における課題は？

(1) 個人情報保護法上の問題は？

会社の業務でパスキーを利用する場合、生体認証のためにデバイスに指紋や顔などの生体情報が保存されることが、会社による個人情報の取得に該当する可能性が考えられます。

もともと、仮に取得に該当するとしても、取得の状況からみて生体情報の利用目的は明らかです。で、利用目的の通知・公表義務（個人情報保護法21条1項）は生じないと思われます（同条4項4

号）。

また、生体情報はデバイス上で管理され、データベース化されませんので、「個人データ」に関する個人情報保護法のルールも適用されないものと思われます。

以上の理由から、個人情報保護法上の問題は特にないでしょう。

(2) プライバシーへの配慮

生体情報はデバイス上で管理され、会社が生体情報をパスキー認証以外の目的で利用することはできませんので、プライバシーの観点でも問題はないように思われます。ただ、導入に際して、従業員から「本当に生体情報が不正に使われる心配はないのか？」という意見が出ることは十分に想定されます。

先ほど、パスキー認証の技術について概略的な説明を行ないましたが、実際の技術はさらに複雑で、専門家でもない完全にその仕組みを理解することは困難です。そのため、パスキー認証の導入時には、一定数の従業員から反発を受けるおそれがあります。

このような問題を防ぐためには、従業員の不満をできる限り生じさせないための努力が求められます。

この点について参考になるのが、個人情報保護委員会が公表する「『個人情報保護の保護に関する法律』についてのガイドライン」に関するQ&A」のQ2-2です。

ここには、雇用する従業員の個人情報を取り扱う場合、従業員との争いを避けるために、「あらかじめ労働組合等に通知し、必要に応じて協議を行なうことも望ましい」と示されています。パスキーを導入する際には、労働組合や労働者代表からの意見聴取の機会を持って、従業員の不安をできる限り解消するよう努めましょう。

たとえ経営層がパスキー導入に積極的であっても、実際にパスキーを利用する従業員の多くが不満を持つてしまえば、うまく普及させることができません。労働組合や労働者代表からの意見聴取のほか、全体説明会の開催、アンケートの実施など、会社全体でパスキー導入に前向きになれるような取り組みが必要です。

(3) その他の課題

生体認証については、精度の問題（うまく認証できない問題）もあります。たとえば、指紋認証であれば、冬場の手荒れや指先のけがなどが原因で認証に失敗するこ

とがあります。

また、顔認証も、マスクを着けているとうまく認証ができないなど、同様の問題があります。

情報セキュリティという点、漏えいや改ざんの問題に目が行きがちですが、必要なときに必要な情報にアクセスできる「可用性」の観点も無視できません。

たとえば、重要な取引で顧客を訪問した担当者が、生体認証に失敗してシステムにログインできなかったら、顧客との法的トラブルにつながるおそれもあります。

このような問題を防ぐためには、生体認証以外の方法によるログインの道も、選択肢として残さざるを得ません。

たとえば、生体認証に失敗する場合に、パスコード（PIN）の入力によるログインを可能にすることなどが考えられます。

もっとも、この場合は、パスコード（PIN）の管理方法について、社内ルールを定めておく必要があります。

情報セキュリティ上の留意点

ここからは、パスキー導入後に

おける情報セキュリティの観点に絞って、深掘りしていきます。

(1) デバイス紛失により生じる問題

パスキーは、スマートフォンなどの秘密鍵が保存されるデバイスが安全に管理されることが前提になった仕組みです。万が一、スマートフォンなどのデバイスを紛失すれば、情報漏えいのリスクが生じます。とくに、パスコード（PIN）など、生体認証以外の方法を許容する場合は、要注意です。

少なくとも、パスコード（PIN）については、推測されにくいものを使用するようにルールを定めておく必要があります。

生体認証を原則としながら、生体認証に失敗した場合に備えてパスコード（PIN）によるログインの道を残す場合、（普段使用しない）パスコード（PIN）を忘れないように、メモを残したくなります。しかし、スマートフォンと、パスコード（PIN）をメモした紙を入れた鞆をどこかに置き忘れてしまえば、取り返しがつかないことになります。

どれほど技術が向上しても、その技術を使う人の意識が低ければ、情報漏えいは起きてしまいます。世の中の情報漏えい事故の多

くが「人のうっかり」によって起きていることを、パスキー導入時にも意識する必要があります。

(2) パスコード（PIN）を覗き見られる問題

パスコード（PIN）については、使用中に周囲の人から覗き見られるリスクがあります。

たとえば、商談先でスマートフォンを机の上に置いていたところ、覗き見られたパスコード（PIN）で不正ログインされてしまうような状況も考えられます。

このように、重要な情報を、情報通信技術を用いることなく盗み出す手法を、ソーシャルエンジニアリング攻撃といいます。

(3) 複数のデバイスでパスキー認証を利用する場合における問題

スマートフォン、タブレットなど、複数のデバイスでパスキー認証を利用する場合、普段使用していないデバイスを紛失したにもかかわらず、長期間そのことに気づかず、情報漏えいのリスクを高めてしまうおそれがあります。

このような問題を防ぐためには、パスキー認証を利用するすべてのデバイスについて、適切な管理を行なうようにルール化する必要があります。

複数のデバイスでパスワード認証を利用する場合、従業員間でのデバイスの共用も考えられます。とくに、パスワード（PIN）でのログインを許可する場合、「タブレットにパスワード（PIN）を書いた付箋を貼り付けて、部課内

で共用する」といった危険な状況も起きやすくなります。デバイスを共用すると、従業員ごとに適切なアクセス権限を設定することができなくなるので、デバイスの共用は、厳格に禁止しておく必要があります。

情報セキュリティ規程 整備のポイント

ここまでの説明を踏まえて、情報セキュリティ規程をどのように整備すべきか、条項例を適宜示しながら説明します。

(1) パスキー認証の初期設定時に おける手順

パスキー認証の初期設定（利用登録）は、個々の従業員に委ねる必要がありますので、手順をマニュアル化して、必ずその手順どおりに設定を進めるようにルール化しなければなりません。

たとえば、**図表3**のような条項を定めることが考えられます。

(2) パスコード（PIN）による 認証を許可する場合

パスワード（PIN）による認証を許可する場合についても、ルールが必要です。

たとえば、**図表4**のような条項を定めることが考えられます。

(3) その他のルール

その他、パスキー認証を使用するデバイスについて、共用を禁止する旨を定める必要があります。

また、パスキー認証に使用するソフトウェアに脆弱性があれば、

秘密鍵が漏えいするリスクが高まります。インストールするソフトウェアを常に最新のものに保つべきことも、ルール化しておくことが望ましいでしょう。

就業規則の 整備について

情報セキュリティ規程を実効的なものにするためには、違反した従業員に対して、懲戒処分をしたり、情報漏えい時の損害賠償責任を追及したりすることができるようしておく必要があります。

そのためには、就業規則に、たとえば**図表5**のような規定を設けなければなりません。

就業規則と情報セキュリティ規程との関係性が不明瞭な場合、情報セキュリティ規程に違反した従業員を処分することができないおそれがありますので、十分に注意が必要です。

パスキーのビジネス利用においては課題もありますが、基本的には、従来のパスワード認証よりも安全性が高く、利便性も高い認証方法です。規模を問わず、多数の企業においてパスキーの導入が加速していくことを期待します。▲

図表3 サービス利用登録時に関するルールの例

- 従業員は、発注管理クラウドサービス「おてがる発注」を業務上使用する際は、システム管理部が通知する手順書に従って、利用登録を完了させなければならない。
- システム管理部は、発注管理クラウドサービス「おてがる発注」の利用登録について手順書を通知する際（通知した手順書の内容を改訂することを含む。）には、あらかじめ、その案を情報セキュリティ委員会に上程し、承認を得なければならない。

図表4 パスコードに関するルールの例

- パスコード（PIN）は、少なくとも●文字以上とし、生年月日その他推測されやすいものを使用してはならない。
- パスコード（PIN）は、書面への記入その他の方法で記録してはならない。
- パスコード（PIN）をデバイスに入力する際には、周囲の状況を踏まえて、覗き見その他の理由によって第三者に知られることのないように留意しなければならない。

図表5 情報セキュリティに関する規定例

第〇条（情報セキュリティマネジメント）

従業員は、当社において別途制定する「情報セキュリティ規程」を遵守し、業務上取り扱う一切の情報について、機密性、完全性および可用性を確保するために必要な対策を適切に講じなければならない。