サイバーセキュリティレポート

2025.05

NTT セキュリティ・ジャパン株式会社
プロフェッショナルサービス部　OSINT モニタリングチーム

目次

【1 ページサマリー】

当レポートでは 2025 年 5 月中に生じた様々な情報セキュリティに関する事件、事象、またそれらを取り巻く環境の変化の中から特に重要と考えられるトピック 3 点を選び、まとめたものである。各トピックの要旨は以下のとおりである。

第 1 章『中国製太陽光発電インバーターに埋め込まれた不審な通信機器』

- 5 月 14 日、ロイター通信は、アメリカのセキュリティ専門家が、中国製の太陽光発電用インバーターに不審な通信機器が組み込まれていることを発見したと報じた。
- これらの機器は、遠隔でインバーターのスイッチを切ったり設定を変更したりすることで、電力網が不安定になり、広範囲にわたる停電を引き起こす可能性があるなど、社会的なリスクとなる。
- 様々な産業の基盤となる電力インフラへのサイバー攻撃は経済だけでなく安全保障につながる重大な脅威である。信頼できる機器のみが調達される仕組みを整え、安全な重要インフラが構築されることが望まれる。

第 2 章『仮想通貨交換業者の内部不正により顧客情報が流出』

- 5 月 15 日、仮想通貨交換業者のコインベースは、複数のカスタマーサポート担当スタッフがハッカーグループに買収され、顧客情報が盗まれたと発表した。
- スタッフらを介して、ハッカーグループは 5 か月にわたり顧客情報にアクセスしていた。発覚後、コインベースは事件に関与したスタッフを解雇した。
- 本件は、社内関係者が外部のサイバー攻撃者と連携した不正事例であり、外部からの攻撃だけでなく内部不正への対策も講じる必要がある。

第 3 章『パスワード時代の終焉？ 進むパスキー導入拡大の動き』

- 「世界パスキーの日(World Passkey Day)」である 2025 年 5 月 1 日に、米 Microsoft 社は、従来のパスワードに代わる認証方式として、「パスワードレス認証」を既定のものとする方針を発表した。
- パスワード認証は、同じパスワードを使いまわすなどの問題により、セキュリティリスクを生む大きな要因となっている。
- パスキー認証はパスワード認証と比べて高いセキュリティを実現できる等のメリットが多いが、新たな認証方式となるため、導入にあたっては注意点を理解する必要がある。

1. 中国製太陽光発電インバーターに埋め込まれた不審な通信機器

1.1. 概要

5 月 14 日、ロイター通信は、アメリカの複数のセキュリティ専門家が、太陽光発電用の中国製インバーター（電流を変換する装置）に不審な通信機器が組み込まれていることを発見したと報じた。機器は外部との通信が可能であるが、メーカーはこれを公表していない。中国製インバーターは、太陽光パネルや風力タービンを電力網に接続するために世界中で使用されており、今回発見された通信機器の問題は国家安全保障に影響を及ぼすようなサイバー攻撃への懸念を高めている[1]。

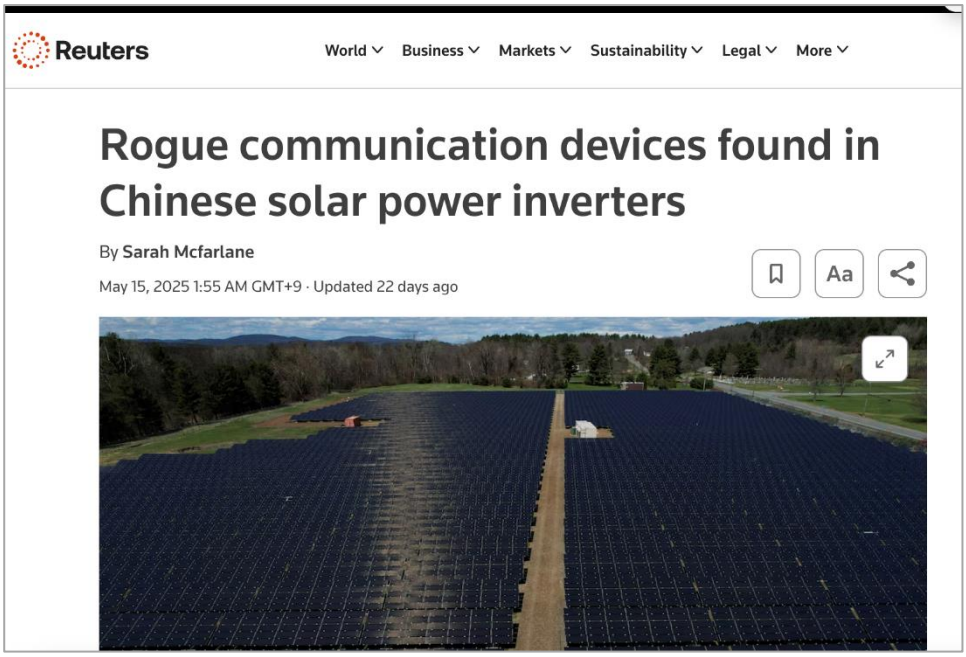


図 1 ロイター通信のニュース記事

1.2. 発見された「不審な通信機器」とその機能

米国の専門家が中国製機器のリスク評価過程で太陽光発電用インバーターを分解したことによって、インバーターの内部に不審な通信機器が存在することが明らかになった。このことは製品資料には含まれておらず、メーカーからも明確な説明はない（調査関係者らはメーカー名自体を明らかにしていない）が、これらの機器は外部ネットワークとの通信を行うことができる。

太陽光発電においてインバーターは太陽光パネルと電力網を接続し、発電量の最大化など電力の制御において重要な役割を担っている。インバーターに埋め込まれている不審な通信機器が悪用された場合、ネットワークを介して、外部との間で不正なリモートアクセスやデータ送信が行われる可能性がある。インバーターのスイッチを切ったり設定を変更したりすることができれば、電力網が不安定になり、広範囲にわたる停電を引き起こす等、社会的なリスクとなる。

例として、ウクライナでは 2015 年以降、ロシアによる電力制御システムを狙ったサイバー攻撃により、何度か大規模停電が

[1] 出典：Reuters『Rogue communication devices found in Chinese solar power inverters』
https://www.reuters.com/sustainability/climate-energy/ghost-machine-rogue-communication-devices-found-chinese-inverters-2025-05-14/

発生している[2]。

1.3. 米国政府の対応と国際的な影響

現時点で米国はこの問題を公式に確認してはいないが、同国のエネルギー省（DOE）や国土安全保障省（DHS）は、本件を国家安全保障上の脅威と位置づけ、調査と対応を進めている。今年 2 月には、2 名の上院議員が、国家安全保障上の懸念から、2027 年 10 月以降は DHS が一部の中国企業からバッテリーを購入することを禁止する法案を提出した。

連邦通信委員会（FCC）も、これらの機器が米国内の通信ネットワークに与える影響を精査しており、将来的には輸入禁止措置や認証制度の見直しも視野に入れている。欧州やアジア諸国でも同様の製品が使用されている可能性があり、国際的な波紋が広がっている。

1.4. まとめ

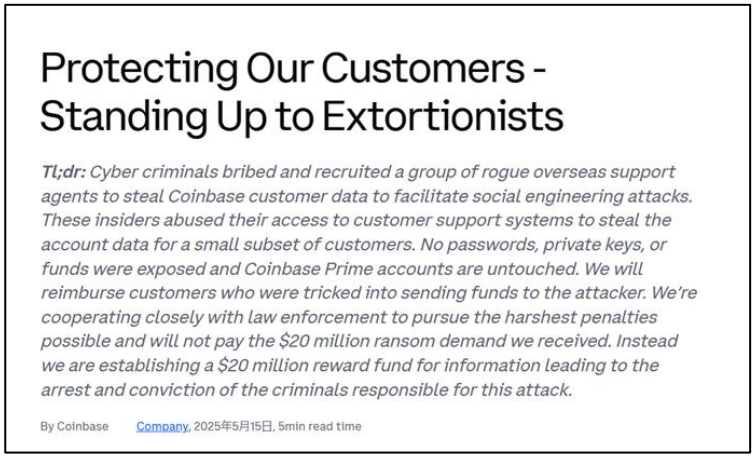
様々な産業の基盤となる電力インフラへのサイバー攻撃は経済だけなく安全保障につながる重大な脅威である。このような懸念を抱えなくてもよいように信頼できる機器のみが調達される仕組みを整え、安全な重要インフラが構築されることが望まれる。

[2] 出典：独立行政法人情報処理推進機構（IPA）『制御システムのセキュリティ ～サイバー攻撃の現状とリスク分析のすすめ～（ET&IoT Technology 2018 IPA ブースプレゼンテーション）』
https://www.ipa.go.jp/archive/files/000070062.pdf

2. 仮想通貨交換業者の内部不正により顧客情報が流出

2.1. 概要

5 月 15 日、米最大の暗号資産（仮想通貨）交換業者であるコインベース・グローバル社（以下、コインベース）は、ハッカーグループが同社の複数のカスタマーサポート担当スタッフを買収し、顧客情報を盗んだと発表した。さらに、同社の対応策として、ハッカーグループ逮捕に向けて懸賞金を出すことや、社内のセキュリティ対策の強化を進めていること等について述べた。


Protecting Our Customers - Standing Up to Extortionists

Tl;dr: Cyber criminals bribed and recruited a group of rogue overseas support agents to steal Coinbase customer data to facilitate social engineering attacks. These insiders abused their access to customer support systems to steal the account data for a small subset of customers. No passwords, private keys, or funds were exposed and Coinbase Prime accounts are untouched. We will reimburse customers who were tricked into sending funds to the attacker. We're cooperating closely with law enforcement to pursue the harshest penalties possible and will not pay the $20 million ransom demand we received. Instead we are establishing a $20 million reward fund for information leading to the arrest and conviction of the criminals responsible for this attack.

By Coinbase Company, 2025年5月15日, 5min read time

図 2 コインベースの声明[3]

2.2. 事件の経緯

コインベースは今年 1 月頃より、カスタマーサポートの一部のスタッフ（同社の従業員の他、外部の請負業者に所属する者を含む）による不審な行為を認識していた。具体的な例として、業務上不要な顧客データへアクセスしていたこと[4]や、私用の携帯電話を使用して業務用コンピューターの画面を撮影していたことが挙げられている[5]。

これらの行為の背後にはハッカーグループが存在していたと考えられている。グループはカスタマーサポートのスタッフらに賄賂を渡し、これと引き換えにスタッフを介して、顧客の氏名や住所、国籍、政府が発行した運転免許証等の身分証明書の画像、社会保障番号の下 4 桁、顧客の口座の残高情報等にアクセスできるようにしていたとみられる。この状態は約 5 か月間続いたとされるが、コインベースの最高セキュリティ責任者（CSO）であるフィリップ・マーティン氏はこれを否定。カスタマーサポートのスタッフがデータを犯罪グループと共有していたことが判明した時、すぐに当該スタッフのアクセス権を停止したと述べている[6]。

本件に関与したスタッフのうち、2 名はインドの請負業者「TaskUs」に所属していたが、これ以外にも、具体的な国名は明ら

[3] 出典：Coinbase『Protecting Our Customers – Standing Up to Extortionists』
https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists

[4] 出典：U.S. Securities and Exchange Commission『FORM 8-K Coinbase Global, Inc.』
https://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm

[5] 出典：Reuters『Coinbase breach linked to customer data leak in India, sources say』
https://www.reuters.com/sustainability/boards-policy-regulation/coinbase-breach-linked-customer-data-leak-india-sources-say-2025-06-02/

[6] 出典：Bloomberg『Coinbase Hack Rocks Company That Led Crypto Into Mainstream』
https://www.bloomberg.com/news/articles/2025-05-15/coinbase-says-bribed-workers-leaked-data-to-hacker-seeking-20-million-in-ransom

かにされていないものの、他国の業者の関与が確認されている[7]。

2.3. コインベースの対応

コインベースは、事件に関与した従業員らを特定すると、彼らをすぐに解雇した。また、TaskUs は同様の処分を関係者に対して下した他、「万全の注意を払うため」として、現地で請け負っていたコインベースの全業務を停止した。そしてこれにより、TaskUs の 226 人の従業員が多額の退職金と共に解雇されるに至った[8]。

5 月 11 日、コインベースは正体不明の人物から電子メールを受け取った。そこには、特定の顧客アカウントに関する情報およびカスタマーサービスやアカウント管理システム等に関する内部文書を入手したとの主張が記されていた[9]。差出人は前述のハッカーグループであると考えられる。メールでは更に、盗んだ顧客情報の削除と引き換えに 2,000 万ドル（約 29 億円）の身代金を要求していたが、同社は支払いを拒否した。そして同額を懸賞金として用意し、これをハッカーグループの逮捕に繋がる情報の提供に対して払う、と事件の公表時に述べた。

今後の内部不正への対策としては、米国内にサポート拠点を新設することや、スタッフ絡みの不正アクセスの監視・検知の拡充を進めることを表明している[10]。

同社は、被害を受けた顧客数はアクティブユーザーの 1%未満であり、パスワードや（暗号通貨の資金にアクセスするために必要な）秘密鍵等は流出していないと報告している。なお、攻撃者に騙されて資金を送ってしまった顧客に対しては補償するとしている。

被害総額に関して同社は、米国証券取引委員会（SEC）への提出書類の中で「本件に関連する修復費用と顧客への自主的な補償」として 1 億 8 千万ドルから 4 億ドルと言及している[11]。

2.4. まとめ

本件は、社内関係者による不正が、外部のサイバー攻撃者と連携して行われた事例である。外部からの攻撃だけでなく、内部不正への対策も講じる必要がある。

---

[7] 出典：Reuters『Coinbase breach linked to customer data leak in India, sources say』
https://www.reuters.com/sustainability/boards-policy-regulation/coinbase-breach-linked-customer-data-leak-india-sources-say-2025-06-02/

[8] 出典：THE TIMES OF INDIA『Coinbase breach: Two TaskUs India Staffers accessed customer data』
https://timesofindia.indiatimes.com/city/bengaluru/coinbase-breach-two-taskus-india-staffers-accessed-customer-data/articleshow/121630955.cms

[9] 出典：U.S. Securities and Exchange Commission『FORM 8-K Coinbase Global, Inc.』
https://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm

[10] 出典：Coinbase『Protecting Our Customers – Standing Up to Extortionists』
https://www.coinbase.com/blog/protecting-our-customers-standing-up-to-extortionists

[11] 出典：U.S. Securities and Exchange Commission『FORM 8-K Coinbase Global, Inc.』
https://www.sec.gov/Archives/edgar/data/1679788/000167978825000094/coin-20250514.htm

3. パスワード時代の終焉？ 進むパスキー導入拡大の動き

3.1. 概要

「世界パスキーの日(World Passkey Day)」である 2025 年 5 月 1 日に、米 Microsoft 社は、従来のパスワードに代わる認証方式として、「パスワードレス認証」を既定のものとする方針を発表した[12]。複数の企業がこの方針に賛同しており、今後、業界全体でパスワードレス認証の導入が加速するとみられる。

3.2.「世界パスキーの日」とは

「世界パスキーの日」は、5 月の第 1 木曜日に設けられた記念日であり、パスワードに代わる安全な認証技術であるパスキーの普及を促進することを目的としている。

この日は、元々「世界パスワードの日(World Password Day)」であり、パスワードの重要性を見直すことで、人々がより安全にアカウントを利用できるようにすることを目的に、2013 年に制定された記念日である[13]。これまで、強力なパスワードに必要な文字数、パスワード使いまわしの禁止、パスワード管理ツールの利用推奨など、様々なベストプラクティスが論じられるきっかけとなっていた。

一方、世界パスワードの日が制定されてから 10 年以上経過した今日でも、サイバー攻撃の初期侵入方法の中で、パスワードが悪用される割合は最多の 22%を占めており[14]、パスワードはセキュリティリスクを生む大きな要因となっている。そのため近年は、パスワードに代わる安全な認証方式について活発に議論されるようになっていた。パスキーの普及に賛同する複数の組織・企業は、今年から同日の呼称を「世界パスキーの日」と変更することで、パスキーがパスワードに代わるものであることをアピールする狙いがあるとみられる。

3.3. 従来の認証方式とパスキー

Microsoft や Google、Apple などの企業は「FIDO (Fast Identity Online) アライアンス」を立ち上げ、パスワードを使わない安全な認証の規格として、「FIDO 標準」の策定を進めてきた[15]。FIDO 標準に準拠した認証方式として、パスキーが考案されている[16]。

---

[12] 出典：Microsoft『Pushing passkeys forward: Microsoft's latest updates for simpler, safer sign-ins』
https://www.microsoft.com/en-us/security/blog/2025/05/01/pushing-passkeys-forward-microsofts-latest-updates-for-simpler-safer-sign-ins/

[13] 出典：Intel Community『Celebrating the 8th Annual World Password Day』
https://community.intel.com/t5/Blogs/Thought-Leadership/Big-Ideas/Celebrating-the-8th-Annual-World-Password-Day/post/1335057

[14] 出典：Verizon『2025 Data Breach Investigations Report』
https://www.verizon.com/business/resources/T487/reports/2025-dbir-data-breach-investigations-report.pdf

[15] 出典：FIDO Alliance『Alliance Overview』
https://fidoalliance.org/overview/

[16] 出典：FIDO Alliance『Passkeys』
https://fidoalliance.org/passkeys/

以下、従来の認証方式の問題点とパスキーのメリットについて整理する。

パスワード認証

IDとパスワードを入力する「パスワード認証」は、最も一般的な認証方式となっており、様々なシステムで利用されている。

パスワード認証のセキュリティ上の問題は、IDとパスワードが一致すれば、誰でもシステムにログインできることにある。そのため、不正ログインへの対策として、英数字や記号を組み合わせた複雑なパスワードをシステムごとに設定することが推奨されている。しかし、現実には複雑なパスワードを覚えることができないため、同じパスワードを使いまわしたり、推測されやすいパスワード(例:「123456」、「password」など)を使用したりするなど、ユーザー自身が弱点となっている。

攻撃者はこうした状況を悪用し、不正にIDとパスワードを入手するフィッシング攻撃、総当たりや推測等によるログイン試行などを積極的に行っている。不正に窃取したパスワードのやり取りも盛んに行われており、2024年4月からの1年間だけで新たに190億個のパスワードが公開されていることが明らかになっている[17]。

パスワード認証+ワンタイムパスワード方式の二要素認証

前述のようなパスワード認証の弱点から、二要素認証の導入が進んだ。パスワード認証に加え、ワンタイムパスワードの入力を求める二要素認証を利用することは、認証のセキュリティを強化する方法とみられてきた。

しかし、メールやSMSでワンタイムパスワードを送信する方法では、メッセージを傍受されるなどの恐れがある。特にSMSで送信する方式は、米サイバーセキュリティ・インフラセキュリティ庁などが利用中止を推奨している[18]。また、認証アプリなどでワンタイムパスワードを発行する場合でも、ユーザーがワンタイムパスワードを入力して送信する点を突いて、中間者攻撃、リアルタイムフィッシング、キーロガーによる読み取りなどの攻撃が行われることにより、認証を突破される恐れがある。

パスキー認証

パスキー認証では、公開鍵暗号方式の仕組みを利用し、サービス側に登録される公開鍵とユーザー自身の端末に保存される秘密鍵のペアで認証を行う。認証時の流れは図 3の通りとなっており、ID、パスワード、ワンタイムパスワードの文字列の入力を必要とせず、生体情報(指紋や顔の情報)などで認証を行う。

パスキーのメリットは、サービス提供側のサーバーではなく、ユーザー端末に認証情報が保存されることにより、サービスにアクセスできる端末が限定され、パスワードに比べて高いセキュリティを実現できることにある。また、パスキーはドメインごとに生成されるため、正規のサービスとはドメインが異なるフィッシングサイトなどでは認証が成立しないようになっている。

[17] 出典:Cybernews『19 billion leaked passwords reveal deepening crisis: lazy, reused, and stolen』 https://cybernews.com/security/password-leak-study-unveils-2025-trends-reused-and-lazy/

[18] 出典:CISA『Mobile Communications Best Practice Guidance』 https://www.cisa.gov/resources-tools/resources/mobile-communications-best-practice-guidance

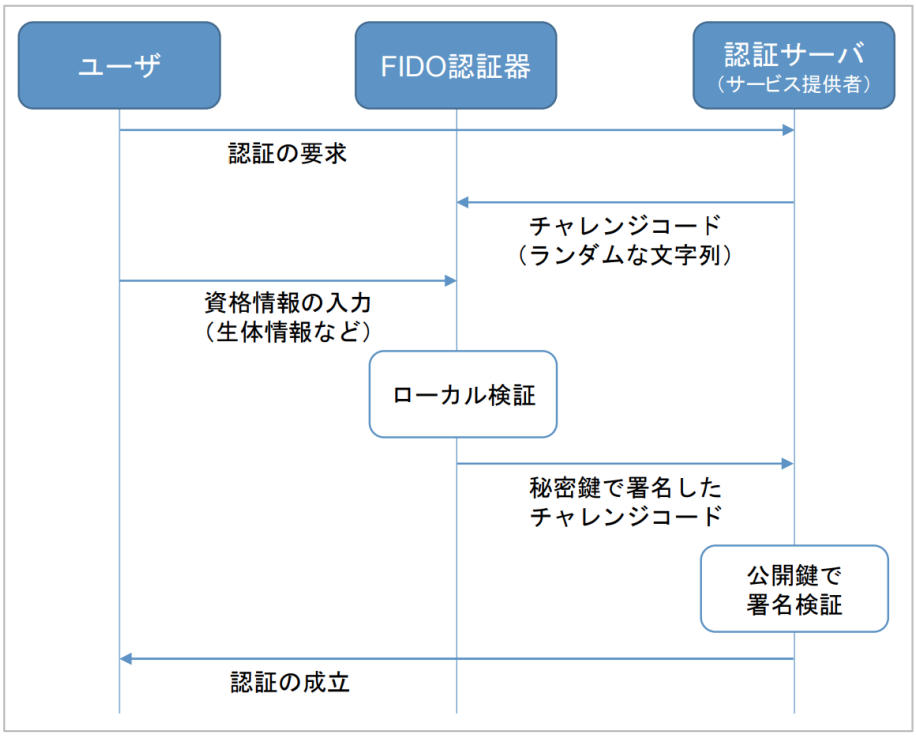


図 3 パスキーによる認証時の流れ[19]

ユーザー体験の面でもパスワード認証より優れており、パスワード認証と比べ、パスキー認証ではログインにかける時間が 8 倍早い。また、認証の成功率は、パスワード認証が 32%であるのに対し、パスキー認証は 3 倍の 98%となっている[20]。

メリットが多い一方、パスキーの導入にあたって注意すべき点もある。ユーザー端末に認証情報を保存するという仕様上、ユーザー端末を紛失してしまった場合、パスキーで認証したサービスにログインできなくなる恐れがある。ユーザー端末の買い替えや故障時にも同様の問題が起こるため、複数の端末でパスキーの同期を取るなどの対応が必要となる。紛失した端末が悪意のある人間の手に渡る可能性を考慮し、遠隔から端末を初期化する手段を用意しておくことも重要である。

また、端末に認証情報が保存されるため、共用端末で誤ってパスキーを設定してしまった場合、他人もログインできてしまう恐れがある。共用端末ではパスキーを利用しないなどのポリシー策定が必要となる。

3.4. パスキー宣言

パスキー導入拡大への取り組みとして、世界パスキーの日に FIDO Alliance は「パスキー宣言」[21]を発表した。この宣言は、年間を通して、パスキー導入拡大に向けた努力を求めるものである。宣言には法的拘束力はないものの、Microsoft を始め、日本からも NTT ドコモなど複数の企業が署名を行った。

---

[19] 出典：NTT ドコモ『FIDO アライアンスにおけるオンライン認証の標準化動向とドコモの貢献』
https://www.docomo.ne.jp/corporate/technology/rd/technical_journal/bn/vol28_1/005.html

[20] 出典：Microsoft『Pushing passkeys forward: Microsoft's latest updates for simpler, safer sign-ins』
https://www.microsoft.com/en-us/security/blog/2025/05/01/pushing-passkeys-forward-microsofts-latest-updates-for-simpler-safer-sign-ins/

[21] 出典：FIDO Alliance『The Passkey Pledge』
https://fidoalliance.org/passkeypledge/

同日、Microsoft は新規アカウントに対して、パスキーを標準の認証方式とすることを発表した。既存のユーザーに対してはアカウント設定からパスワードを削除できるようにし、早速パスキーの導入を推進する姿勢を示している。

3.5. まとめ

パスワード認証は、その利便性から IT 黎明期より利用されてきた。しかし、サイバー攻撃の高度化により、パスワード認証を利用することが大きなリスクとなってきている。パスワードに代わる認証方式として考案されたパスキーは、様々なサービスで利用が進んでいたが、主に個人利用に限ったものだった。今回、Microsoft 社がパスキーを標準の認証方式として採用すると表明したため、今後、企業で多く利用されている Windows PC でもパスキーの導入が急速に進むとみられる。

企業でのパスキー導入は、組織のセキュリティ強化や IT 管理者の負担軽減などに貢献すると思われる。一方で、新たな認証方式の導入となるため、その注意点を正しく理解し、最適な導入方法を検討する必要がある。

以上

免責事項

本記事の内容は、正確であることに最善を尽くしておりますが、内容を保証するものではなく、本記事の利用に起因して発生したいかなる損害、損失についても補償しませんのでご留意ください。記事内に誤植や内容の誤り、その他ご指摘等、お問い合わせ事項がある場合は、お手数ですが下記までご連絡ください。

お問い合わせ先：NTT セキュリティ・ジャパン株式会社

プロフェッショナルサービス部　OSINT モニタリングチーム
メールアドレス：nsj-co-osint-monitoring@security.ntt