



資料 1 - 2
※一部非公開※

警察庁の取組について

警 察 庁

令和8年9月7日
レジデンシャルプロキシ対策アライアンス
(第1回)

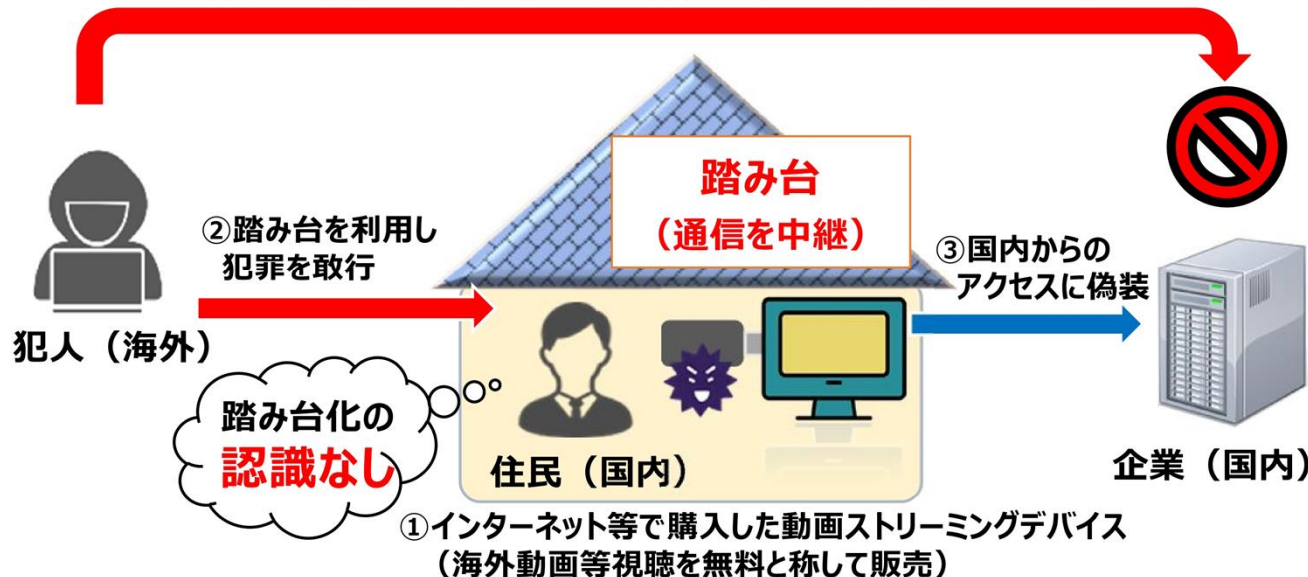
レジデンシャルプロキシの実態 ①

■ サマリー

- 家庭用IoT機器等がレジデンシャルプロキシ化してサイバー攻撃等の踏み台として悪用される事案が多数発生。
- 攻撃者は、当該機器等を経由し接続元を一般家庭と偽ることで攻撃先企業等のセキュリティ対策を回避するほか、攻撃者に対する捜査を困難なものにしている。
- 令和6年中のインターネットバンキング不正送金事犯においてレジデンシャルプロキシが高い割合で悪用されているほか、その他の犯罪種別でも悪用されている実態がみられる。
- レジデンシャルプロキシの種類には、プロキシ化ソフトウェアのインストール等に伴うもの（収益アプリ等）、機器自体に仕込まれたマルウェアによるもの（動画ストリーミングデバイス）が存在。
- プロキシ化ソフトウェアのインストール等に伴うものでは、収益アプリとVPNアプリが目立つ。
- 機器自体に仕込まれたマルウェアによるものでは、動画ストリーミングデバイスが大半を占める。
- 犯罪インフラとしての汎用性が高く、今後もサイバー攻撃等での悪用が懸念されており、早急な対策が必要。

「インターネットバンキング不正送金事犯に悪用されたイメージ」

踏み台を利用せず犯罪を敢行すると、海外からのアクセスはブロックされる



インターネットバンキング不正送金事案におけるレジデンシャルプロキシ悪用割合（令和6年）

44%
被害件数の割合

全体被害件数4,369件のうち
少なくとも1,918件

33%
被害額の割合

全体被害額約86.9億円のうち
少なくとも約28.9億円

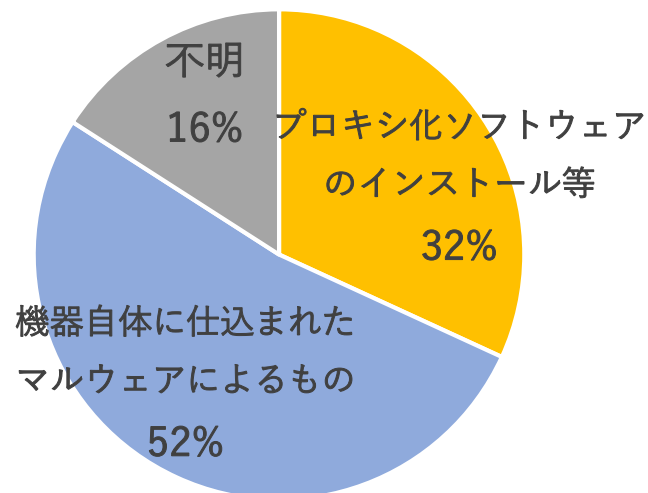
【構成員等限り】

レジデンシャルプロキシの実態 ③

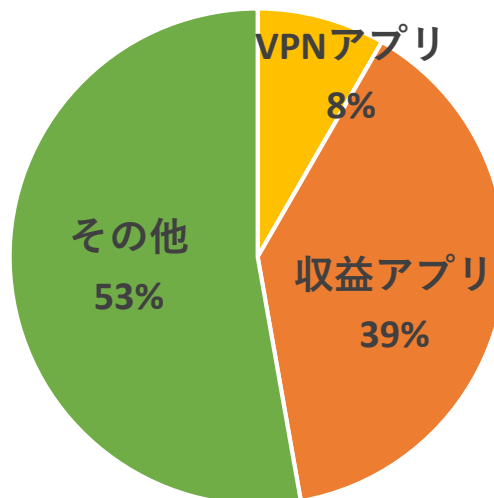
■ レジデンシャルプロキシの悪用実態

- 令和7年度中のサイバー犯罪等におけるレジデンシャルプロキシの実態（警察庁が報告を受けたもの）は、
- ・ 「機器自体に仕込まれたマルウェアによるもの」が約5割、「プロキシ化ソフトウェアのインストール等に伴うもの」が約3割
 - ・ 「プロキシ化ソフトウェアのインストール等に伴うもの」では、VPNアプリと収益アプリで約半数を占める
 - ・ 「機器自体に仕込まれたマルウェアによるもの」では、動画ストリーミングデバイスが約9割
 - ・ 入手元については、オンラインショップ、海外で購入、知人から譲受け（機器設置者から聴取した結果）等であった。

① レジデンシャルプロキシの種類

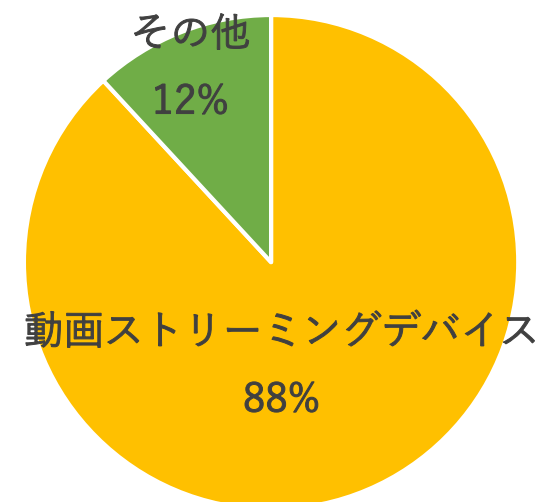


② プロキシ化ソフトウェアのインストール等に伴うもの



※ その他には音楽アプリ、壁紙設定アプリ等が含まれる。

③ 機器自体に仕込まれたマルウェアによるもの

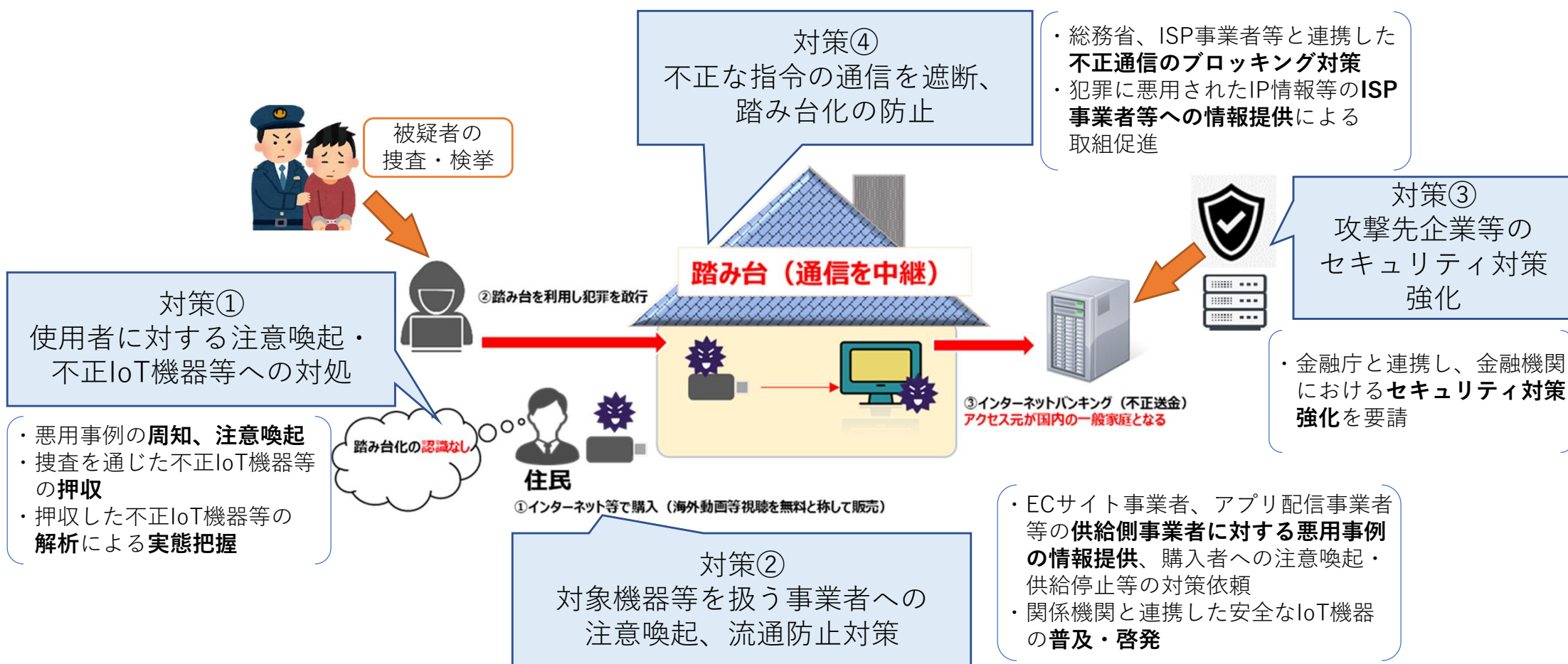


※ その他にはデジタルフォトフレーム等が含まれる。

警察におけるレジデンシャルプロキシ対策・全体像

警察におけるレジデンシャルプロキシ対策の全体像

- 警察では、被疑者の捜査・検挙に加え、レジデンシャルプロキシを悪用する各種サイバー事案の未然防止のため、家庭用IoT機器利用者に対する注意喚起等（対策①）、対象機器等を扱う事業者への注意喚起等（対策②）、攻撃のターゲットとなる企業等へのセキュリティ対策強化の要請（対策③）、不正な指令の通信の遮断措置（対策④）等の対策を関係機関等と連携して展開。



警察におけるレジデンシャルプロキシ対策 ①

■ 対策① 使用者に対する注意喚起・広報啓発活動

- 「サイバー警察局便り」や「サイバー空間をめぐる脅威の情勢等について」を活用し、レジデンシャルプロキシに関する注意喚起を実施。
- 本アライアンスの設置を受けて、本アライアンス構成機関の連名での注意喚起も実施。
- 捜査の過程で悪用された家庭用IoT機器等の使用者が特定できた場合、使用者に対する指導・注意喚起も実施。

サイバー警察局便り
Cyber Police Agency Letter R6 Vol.17

あなたの家のIoT機器が悪用されている！

インターネットバンキング不正送金事案などで「踏み台」に！

一般家庭A (IPアドレス: 110.10.10.110) 不正送金

踏み台を利用し犯罪を敢行

踏み台化の認識なし

踏み台 (通信を中継)

「踏み台」化したパソコンなどの家庭用インターネット通信機器

警察へ被害申告

どんな悪用事例がある？

- ◆ 警察ではマルウェアに感染した家庭用パソコンやIoT機器が悪用されプロキシサービスを通して犯罪の踏み台となる事例を確認しています。
- 事例1 海外で放送されているTV番組やインターネット配信の動画を視聴するためのIoT機器がマルウェアに感染しており、不正送金の踏み台に悪用されていた。
- 事例2 「余っているネット帯域を他者に共有して利益が得られる」という、いわゆる収益アプリをインストールし、他者へ自身のネット帯域の貸し出しに同意したところ、不正送金の踏み台に悪用されていた。

自宅のIoT機器を悪用されないために…

- ・ 安価な製品の利用はマルウェアに感染するリスクがあります。最低限のセキュリティ基準を満たしたIoT製品にラベルを付与するJC-STAR制度が本年3月から始まります。安心できるラベル付きのIoT製品を購入し、利用しましょう。
- ・ フリーソフトやアプリのインストールはマルウェア感染や、悪用されるリスクがあります。制作元をよく確認し、不審なソフトやアプリのインストールは避けましょう。
- ・ その他、使用している機器のウイルスチェックや使用しない機器のネットワークからの切断など、基本的な対策を徹底しましょう。

もしかして悪用されている…？→不安があれば警察にご相談を！！
最寄りの警察又はサイバー犯罪相談窓口 → <https://www.npa.go.jp/bureau/cyber/soudan.html>

警察庁 経済産業省

「サイバー警察局便り」
(令和7年3月)

サイバー警察局便り
Cyber Police Agency Letter 2026 Vol.9 (R8.8)

家庭にある機器が悪用されています

一般家庭で使用されている動画視聴用の端末 (ストリーミングデバイス) やデジタルフォトフレームなどがサイバー攻撃の踏み台として悪用されています。このような踏み台となる機器は「レジデンシャルプロキシ」と呼ばれます。

※ 一般家庭向けのネット回線に接続された機器が第三者の通信を中継する仕組みのこと。

「インターネットバンキング不正送金事案に悪用されたイメージ」

踏み台を利用せず犯罪を敢行すると、海外からのアクセスはブロックされる

「不正送金の手口内訳」

踏み台 (通信を中継)

踏み台化の認識なし

住民 (国内)

企業 (国内)

海外からのサイバー攻撃が、国内の個人宅からのアクセスに偽装されるため、住民の方に捜査へ御協力いただく場合があります。

あなたの家庭ではいくつ当てはまりますか？

- ☐ 提供元不明のソフトウェア、アプリ、無料VPNを利用している
- ☐ 「収益が得られます」と宣伝するサービスやアプリを利用している
- ☐ 無料で動画が見られるストリーミングデバイスを使用している
- ☐ 購入してから一度も更新を行っていない古いIoT機器を使用している

※ インターネットに繋がる機器のこと。

みんなで悪用を防ぐために必ずチェック

警察庁、総務省、NICTではウェブサイトにおいて、「家庭用IoT機器を悪用するレジデンシャルプロキシの現状」を公開しました。

<https://www.npa.go.jp/bureau/cyber/koho/news/residentialproxy.html>

警察庁 総務省 NICT ICT-JSAC JC3

「サイバー警察局便り」
(令和8年8月)

令和7年におけるサイバー空間をめぐる脅威の情勢等について

不正なソフトウェアが仕込まれた機器が流通しているものもあり、当該機器をインターネットに接続することにより、使用者の気付かないうちにマルウェアをインストールしてプロキシとして動作するものがある。これらの機器が踏み台となり、攻撃者の通信を中継した場合、通信先のサーバのログには、攻撃者のIPアドレスではなく、踏み台となった機器のIPアドレスが記録される。海外の攻撃者であっても、国内の機器を踏み台とすることにより、海外からのアクセスを制限したサーバにアクセスすることも可能となるなど、セキュリティ対策上の重大な脅威となっているとともに、サイバー犯罪捜査においても深刻な障害となっている。

【図表30: IoT機器が踏み台となる攻撃のイメージ】

令和8年3月 警察庁サイバー警察局

踏み台 (通信を中継)

インターネットバンキング (不正送金) アクセスが踏み台のIPアドレスで記録される

住民

インターネット等で購入した動画ストリーミングデバイス (海外動画視聴を無料と称して販売)

例えば、令和6年中に発生したインターネットバンキングに係る不正送金事案 (被害件数4,369件、被害額約86.9億円) において、犯行時にレジデンシャルプロキシが用いられたのは少なくとも1,918件、被害額は約28.9億円に及び、被害件数全体の約44%、被害額では約33%を占める。また、令和7年中においても、引き続き犯行時にレジデンシャルプロキシが用いられた事案を多数認知しており、依然としてセキュリティ対策上の脅威となっている。

【図表31: インターネットバンキング不正送金被害件数の内訳】

項目	件数	割合
レジデンシャルプロキシ	1,918件	(44%)
その他	2,451件	(56%)

35

「サイバー空間をめぐる脅威の情勢等について」
(令和8年3月)

警察におけるレジデンシャルプロキシ対策 ②

■ 対策② 対象機器等を扱う事業者への注意喚起、流通防止対策

- 昨年、警察が認知した証券口座への不正アクセス・不正送金事案において、不正アクセス元のIPアドレスが割り当てられていた回線契約者を特定し、回線契約者宅へ訪問して捜査を実施。
- 回線契約者は、証券口座への不正アクセス行為への関与を否定。
- 回線契約者は、小型動画ストリーミングデバイスに、音楽視聴アプリをインストールして利用しており、当該アプリがレジデンシャルプロキシとして稼働していたものと判明。



小型動画ストリーミングデバイスに
音楽視聴アプリをインストール

音楽視聴アプリを解析したところ、

- プロキシ機能が組み込まれていること
- アプリ起動時にプロキシ機能の制御情報をインターネット上からダウンロードしていること
- ダウンロードした制御情報に基づいてプロキシが動作することが判明している。

【警察によるアプリ配信ストアへの要請】

- 当該音楽視聴アプリの配信を行っていたアプリ配信ストアを運営する事業者に対し、当該アプリが不正アクセスに悪用されている実態について情報提供を行い、被害拡大防止のための対応を要請。

⇒ **警察からの要請を受けて、アプリ配信ストアでの当該アプリの配信が停止された。**

警察におけるレジデンシャルプロキシ対策 ③

■ 対策③ 攻撃先企業等のセキュリティ対策の強化

- 令和7年4月、犯罪対策閣僚会議において「国民を詐欺から守るための総合対策2.0」を決定。本対策に基づく各種対策を関係機関等と連携して推進。
- 令和7年7月、金融庁と連名で、金融関係協会に対して、顧客口座・アカウントにおける不正アクセス対策の強化等について要請を実施。
- DMARCやパスキーの導入・利用の推奨について、広く広報啓発を実施。

① メールのなりすまし防止技術(DMARC)の普及促進

Domain-based Message Authentication Reporting and Conformance

・利用者に送信されたメールが、正規の送信元（証券会社）からのメールであるかどうかを検証する仕組み

・証券会社のメールアドレスを騙ったメールが利用者に届かないよう、証券会社において、利用者に受信させない/迷惑メールフォルダに入れる、といった設定を行うことが可能

② フィッシングサイトの閉鎖活動

・証券会社のフィッシングサイトを、利用者が閲覧できないようにするため、インターネット事業者に対して、フィッシングサイトの閉鎖（削除）を要請するもの

③ パスキーの導入促進

・証券会社のアプリ等において、簡単に安全な認証方式である「パスキー」を利用できるようにするもの

・端末（スマホ）そのものが認証に必要な鍵となり、端末のロック解除と同様の本人認証により、アプリへのログインを可能とする

・ネット上に、パスワードを送信しないため、パスワードが窃取されない

金融関係協会への要請内容（一部）
（令和7年7月）

金融犯罪者はなりすましが得意だから

従来のパスワード対策では危険です!!

フィッシングに耐性のある多要素認証が効く!

パスワードを入力する必要がある、安全性の高い仕組みでなりすましを防ぐ!

パスキーによる認証
パスワードの代わりに生体認証（指紋認証や顔認証）、PINコードなどを使ってログインする。より安全で簡単な次世代認証方式です。パスワードを覚える手間もなくセキュリティと利便性を両立できます。

PKI（公開鍵基盤）による認証
公開鍵と秘密鍵のキーペアからなる技術で、信頼できる第三者（認証局）を通じて、本人であることを電子的に証明する仕組みです。マイナンバーカードを認証に利用することもできます。

もしもフィッシングサイトに誘導されても、パスキー・PKI認証があなたを守る!

メール・SMSのURLリンクは危険!!

偽物サイトは見た目で違いはわからないから。

いつものサイトはいつもの方法で入る「正規アクセス」が効く!

ブックマークやアプリなどを使った正しいログインならフィッシング被害に遭わない!

公式サイトをブックマーク
ウェブブラウザでよく見るページを登録しておいて、すぐ開けるようにする機能のことです。検索エンジンで正規サイトにアクセスしたらブックマークを心がけましょう。

公式アプリ
正規のアプリストアで配布されているアプリは開発元が明記されていて信頼できるものです。アプリをインストールする際は正規のアプリストアからインストールしましょう。

そのために! 金融機関名のメールであっても偽物の場合があります! 送信アドレスやリンクを注意して確認! ブックマークした公式サイトや公式アプリからアクセス!

大切な資産は、奪わせない。

金融庁 警察庁

金融庁等との連名による広報啓発
（令和8年4月）

サイバー警察局便り
Cyber Police Agency Letter 2026 Vol.12 (R8.9)

パスワードだけの認証はもう限界です。
自社サービスにパスキーを導入し、安全で快適なログインを実現しましょう!

手紙のやり取りにたとえるパスキーの仕組み

① 印鑑作成（鍵ペア作成）
利用者が印鑑を作成し、金庫に保管。
印鑑をサービス事業者へ提出。
（印鑑＝秘密鍵、印影＝公開鍵、金庫＝スマホ）

② 手紙の送付（認証要求）
サービス事業者がランダムな文字列の手紙を送付。
（チャレンジ送信）

③ 手紙に押印（本人確認・電子署名）
利用者が顔認証や指紋認証を行い、金庫から印鑑を取り出して押印。

④ 印鑑の照合（署名検証）
サービス事業者が登録済の印影と一致するか、手紙の内容が一致するかを確認。

パスキー導入の主なメリット

漏えいリスク低減
秘密鍵は端末の安全な領域に保存されるため、漏えい被害を抑制

ブランド・信頼の維持
偽サイトでは認証できないため、自社ブランドの信頼を高め、企業イメージを守る

利用者満足度の向上
パスワード入力不要、顔認証・指紋認証ですぐログイン

パスワードから、パスキーへ。
パスワード漏えいやフィッシングのリスクから利用者を守るために、より安全な認証方式として、パスキーの導入を検討ください。

警察庁
National Police Agency

「サイバー警察局便り」
（令和8年9月）

【構成員等限り】