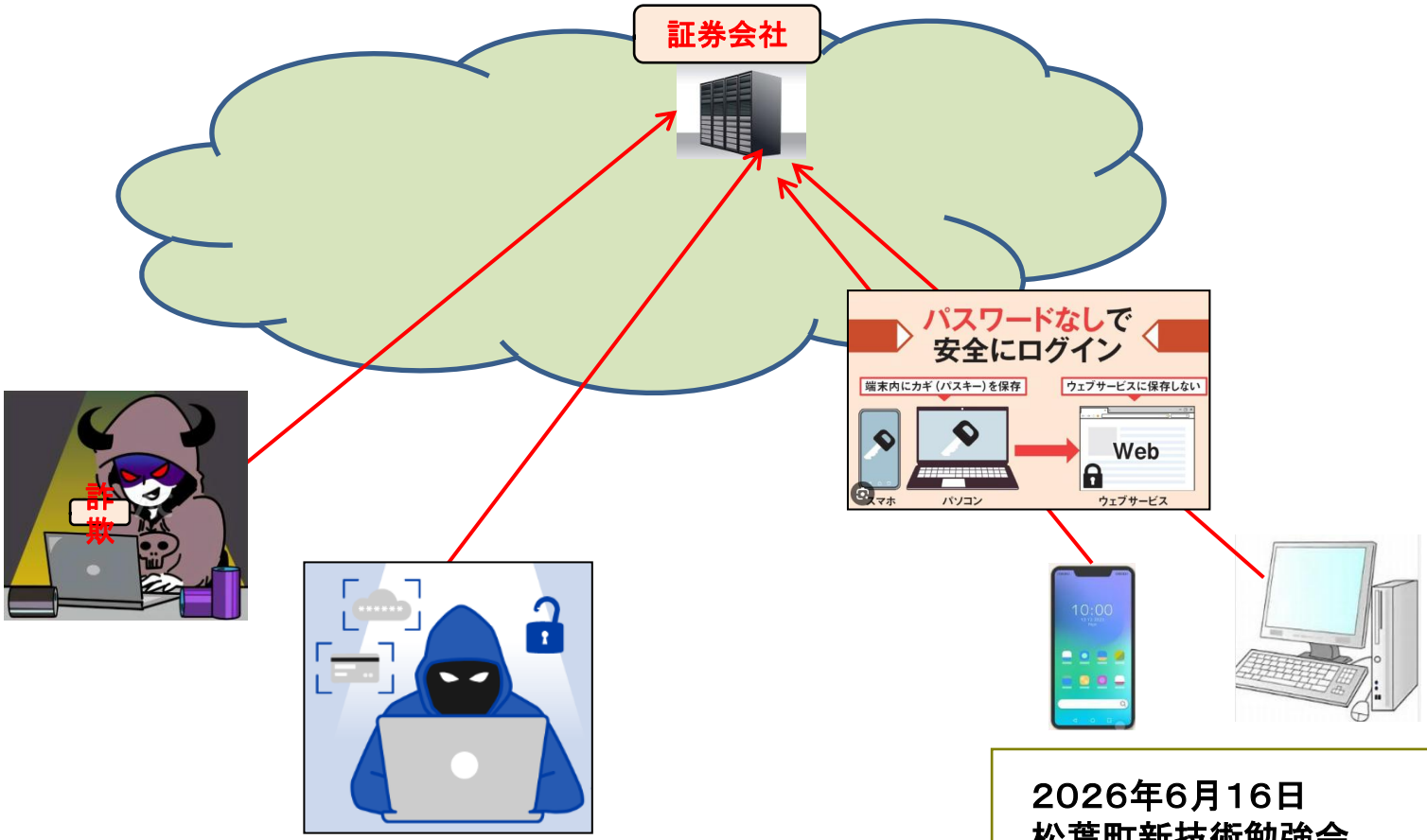
サイバー攻撃
（ネット被害・詐欺に遭わないためには！）



2026年6月16日
松葉町新技術勉強会
松葉町地域づくり委員会）中村年雄

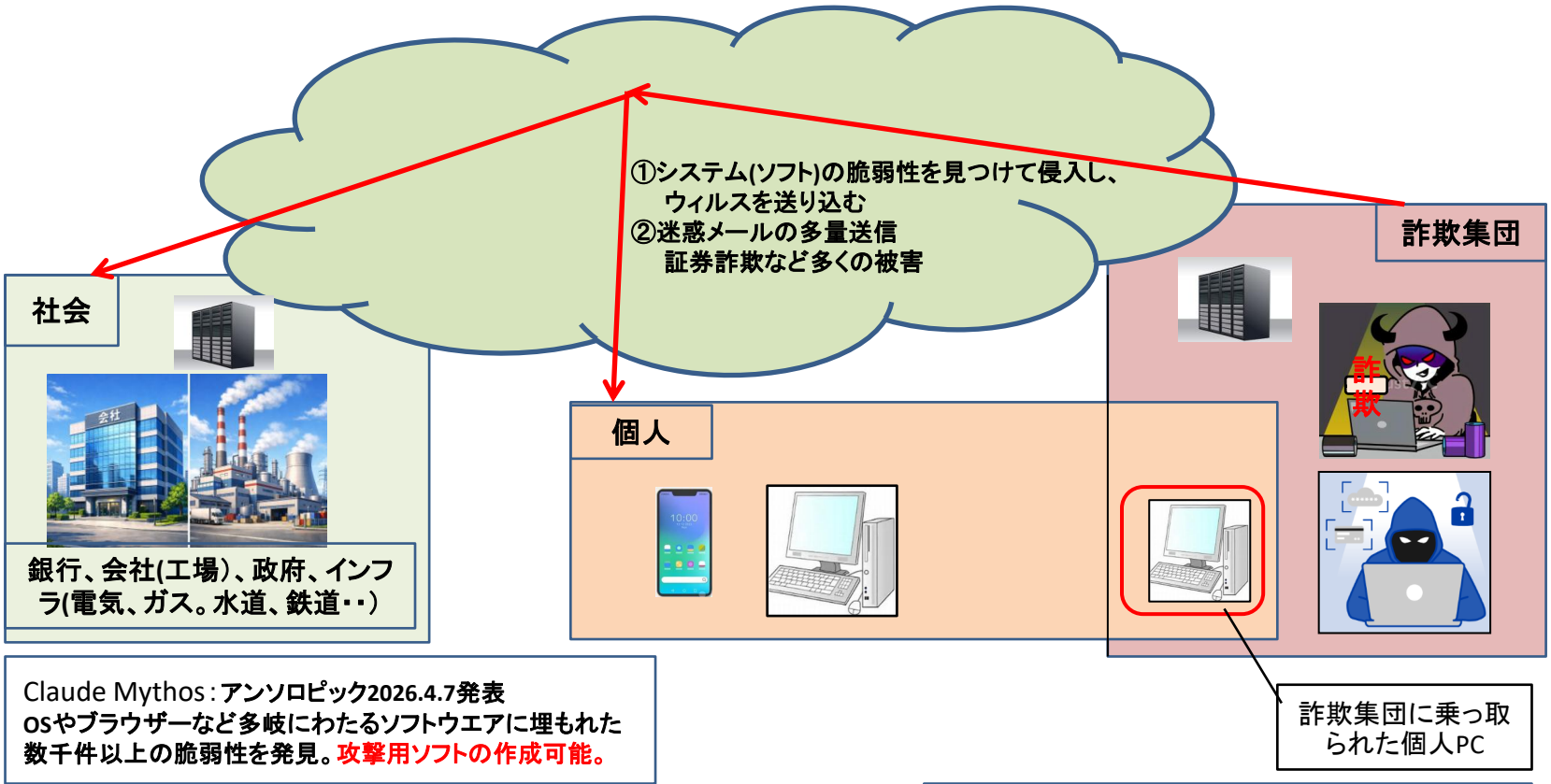
2025年 サイバー攻撃 被害状況（推定）

区分		攻撃の種類	被害件数（推定）	被害額（推定）	主な特徴
日本	個人	フィッシング詐欺	約250万件	約7,400億円+	偽メール・SMSによる金銭詐取が急増
		ランサムウェア感染	約25万件	約300億円	個人PC・スマホの暗号化被害
		偽サポート詐欺	約60万件	約200億円	「ウイルス感染」と偽り遠隔操作される
		ネットバンキング不正送金	4,677件	102億円	
		SNS投資詐欺・ロマンス詐欺	数十万件	1,827億円	
	企業	ランサムウェア攻撃	約2,800件	約2,200億円	中小企業中心に業務停止・情報漏洩
		情報漏洩（内部・外部）	約1,500件	約1,000億円	メール誤送信・クラウド設定ミス含む
		DDoS攻撃	約900件	約400億円	ECサイト・金融機関への集中攻撃
	政府・インフラ	標的型攻撃（APT）	約120件	約1,500億円	官公庁・電力・通信への侵入試行
		政府関連サイト改ざん	約80件	約数千億円	政治的メッセージ目的の攻撃
世界	個人	フィッシング詐欺	約3,000万件	約2兆円	SNS・暗号資産詐欺が拡大
		ランサムウェア感染	約800万件	約1.2兆円	個人スマホ・IoT機器への攻撃増加
	企業	ランサムウェア攻撃	約45,000件	約25兆円	医療・製造・金融が主な標的
		データ漏洩	約30,000件	約15兆円	クラウド・AI関連サービスの脆弱性悪用
	政府・インフラ	APT攻撃・国家レベル攻撃	約2,000件	約10兆円	電力網・通信・防衛関連への侵入

APT攻撃：特定の組織を長期間ねらい続ける高度で執拗なサイバー攻撃 。
単発の攻撃ではなく、数か月～数年かけて静かに侵入し、情報を盗み続ける 。

サイバー攻撃の世界

詐欺は「人をだます技術」であり、ウイルスは「パソコンに入り込む技術」



Claude Mythos：アンソロピック2026.4.7発表
OSやブラウザーなど多岐にわたるソフトウエアに埋もれた数千件以上の脆弱性を発見。攻撃用ソフトの作成可能。

攻撃ロボット(100万台ともいわれている。乗っ取られたPCも攻撃ロボットとして使われる。全IPを対象にしており家庭のPCも数十回/日攻撃されている。
ただ ネットにつながっているだけ で攻撃される。

核兵器より恐ろしいAI

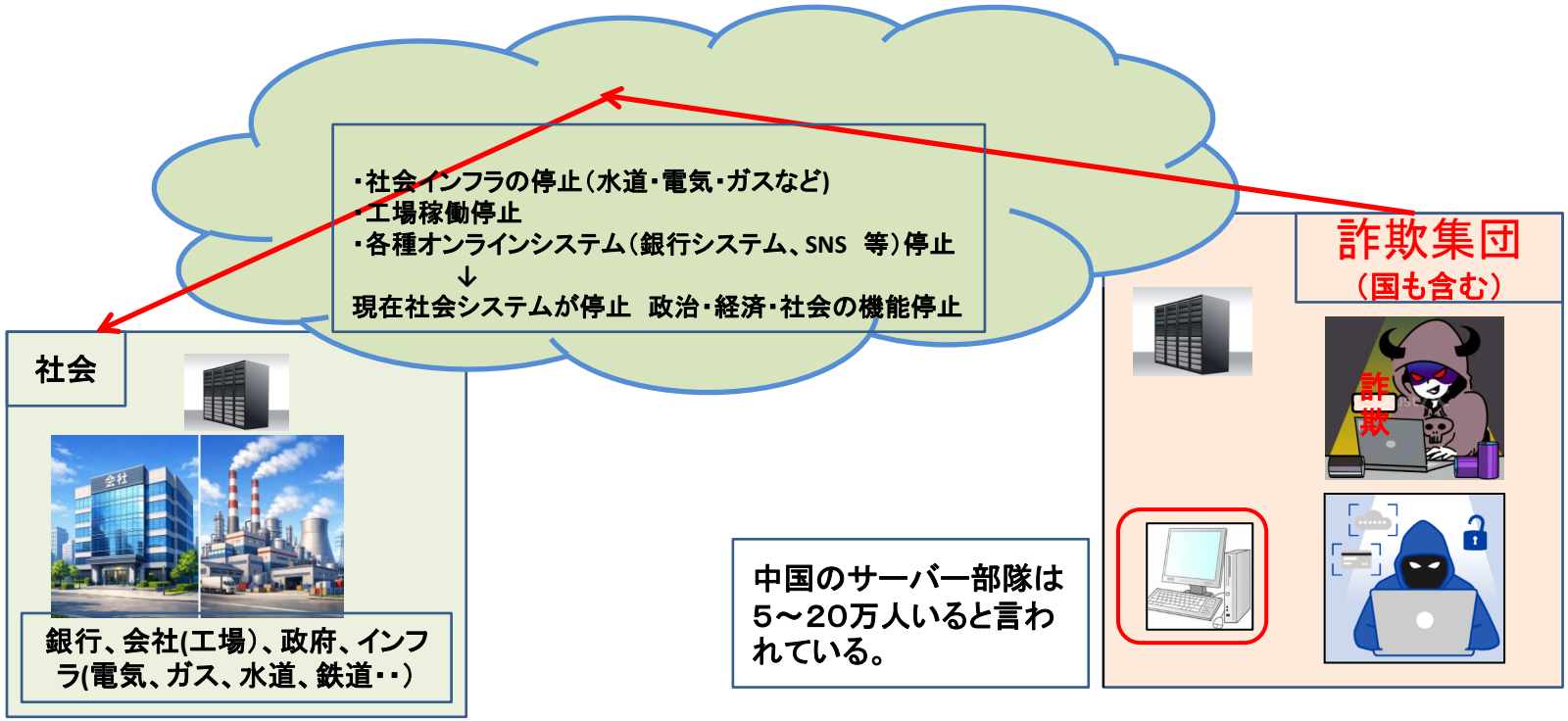
生成AIの進化は止まらない！！
1年後の世界：　対策を取らないと世界は大混乱？？

★中国はミトスと同様の性能の生成AIを１年以内に開発することができる。

★ミトスは約50社（米テック企業中止）で使用開始されている。その結果2026.5.22に1万件以上の脆弱性を発見した。
又オープンソース1000件以上をチェックして6200件の脆弱性を発見したと発表した。

発見された脆弱性は現在、人手で修正されており、とても人手不足で修正できる状態ではない。
生成AIが修正し、人間が承認する形へ

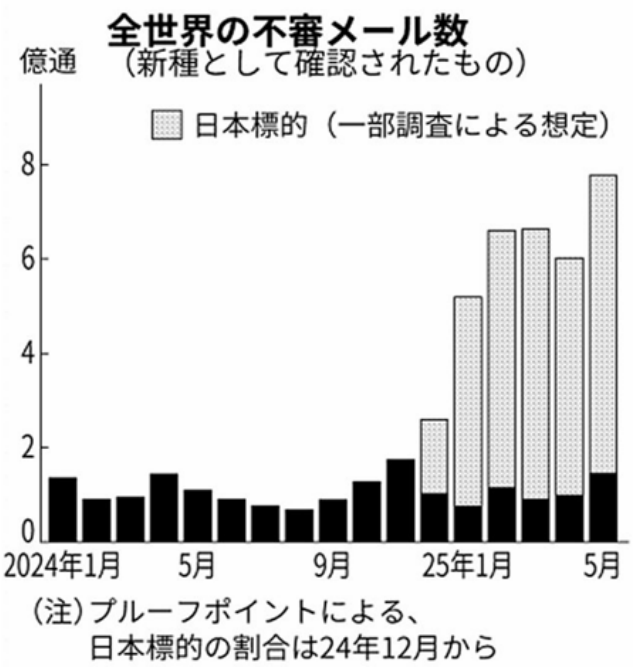
★OpenAIはClaude Mythosと同レベルの生成AIを開発したと2026．5に発表

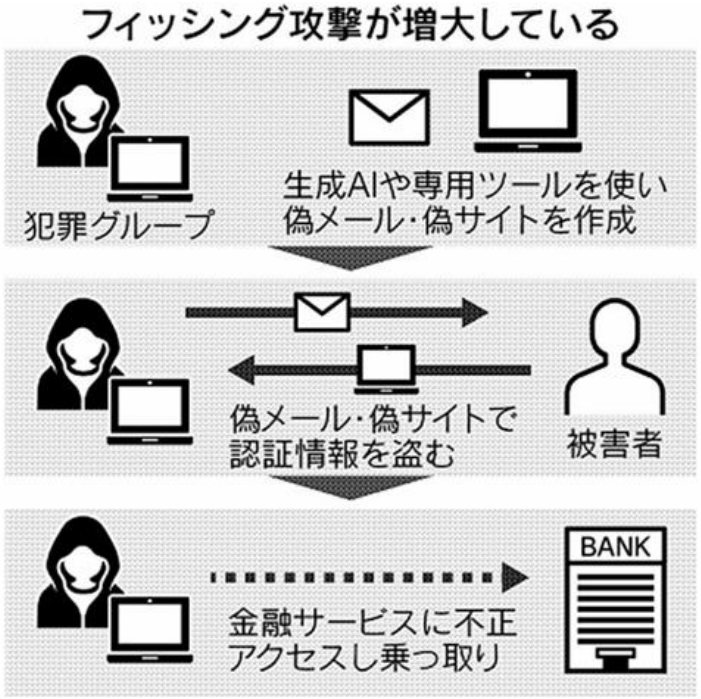


脆弱性とは

区分	主な脆弱性	具体例	何が起きる？	特徴
サーバー	ソフトの脆弱性	古いApache、PHP、WordPress、プラグイン	改ざん、乗っ取り、情報漏洩	公開サービスが多く攻撃されやすい
	設定ミス	パーミッション777、管理画面公開、DB公開	不正アクセス、データ盗難	人為的ミスが大きな原因
	パスワード弱い	admin/1234 など	ログイン突破、改ざん	総当たり攻撃の標的
	ネットワーク機器の脆弱性	古いルーター、VPN装置	内部侵入、全体乗っ取り	企業で多い
PC（Windows）	OSやアプリの古さ	Windows Update未適用、古いOffice	ウイルス感染、乗っ取り	更新を怠ると危険
	SMB共有の脆弱性	共有フォルダ、SMBv1	自動感染（WannaCry）	家庭内LANで広がる
	ブラウザの脆弱性	古いChrome/Edge	不正サイトで感染	PCの入口になりやすい
	操作ミス（人的脆弱性）	添付ファイルを開く、偽サイトに入力	情報盗難、感染	個人PCで最も多い
スマホ（Android）	OSアップデート停止	古いAndroid、格安機種	既知の脆弱性が残る	最大の弱点
	アプリの脆弱性	古いアプリ、不正アプリ	情報盗難、乗っ取り	アプリ経由の攻撃が多い
	権限の与えすぎ	カメラ・位置情報・連絡先を許可	情報抜き取り	Android特有の問題
	フィッシングSMS	宅配・銀行を装うSMS	偽アプリ・偽ログイン	スマホで最も多い
	公衆Wi-Fi	暗号化なし、偽Wi-Fi	通信盗聴	スマホ特有のリスク

参考





世界の不振メールの8割が日本に来ている。＝日本人はデジタルの知識がなくいいカモとみられている。特にシニア。

サイバー攻撃の種類

分類	攻撃名	どんな攻撃？	何が起きる？	個人/企業
侵入系	脆弱性攻撃	古いソフトの欠陥を突いて侵入	サーバー乗っ取り、改ざん	企業・個人PC
	パスワード総当たり（ブルートフォース）	ID/PW を機械的に試す	ログイン突破、改ざん	個人サイト・企業
	認証情報盗難	PC感染でパスワードが盗まれる	FTP・メール・SNS乗っ取り	個人・企業
詐欺系	フィッシング	偽サイトでID/PWを盗む	不正ログイン、金銭被害	個人（特にスマホ）
	スミッシング（SMS詐欺）	SMSで偽URLに誘導	不正アプリ・偽ログイン	個人
マルウェア系	ランサムウェア	データを暗号化し身代金要求	PC停止、業務停止	企業・個人
	トロイの木馬	正常に見えるが裏で悪さ	情報盗難、遠隔操作	個人・企業
	ボットネット化	PCが攻撃ロボット化	他サイト攻撃に利用される	個人PCが多い
Web攻撃	Web改ざん	サイトを書き換える	偽サイト化、信用失墜	個人サイト・企業
	DDoS攻撃	大量アクセスでサーバー停止	HP・サービスが落ちる	企業
	SQLインジェクション	入力欄からDBに不正命令	顧客情報流出	企業
ネットワーク系	中間者攻撃（Wi-Fi盗聴）	公衆Wi-Fiで通信を盗む	パスワード漏洩	個人（スマホ）
	ルーター攻撃	古いルーターの欠陥を突く	家庭内LANが乗っ取られる	個人
人間を狙う攻撃	なりすましメール（BEC）	社長・銀行を装う詐欺	振り込み被害	企業
	偽サポート詐欺	「ウイルス感染」と偽警告	遠隔操作・金銭被害	個人（シニア多い）

参考）　個人への影響を中心に考える

Windows10等サポート終了後にも使用続けると、どんな問題が起きる？

セキュリティの脆弱性	新しいウイルスやマルウェアに対する防御が弱くなり、個人情報が漏洩する可能性が高まります。
情報漏洩の危険	企業や個人のデータが不正アクセスされる可能性が高まり、重要な情報が流出するリスクがあります。
業務停止の可能性	企業や公的機関で使用されている場合、システムが攻撃を受けることで業務が停止する恐れがあります。
ソフトウェアの互換性問題	新しいアプリや周辺機器がWindows 10をサポートしなくなり、使えなくなる可能性があります。
オンラインバンキングやショッピングの危険性	セキュリティ更新がないため、ネット決済や個人情報入力時に不正アクセスされるリスクが増します。
パフォーマンスの低下	OSの最適化が行われなくなるため、動作が遅くなったり、不具合が増えることがあります。

ウィルスがパソコンに入り込み、ウイルスが何をするか？（代表例）

個人情報の漏洩	ウイルスは、パスワード、クレジットカード情報、住所などの個人データを盗み出すことがあります。サイバー犯罪者に悪用される危険性が高い。
PCの動作が遅くなる	バックグラウンドで不正なプログラムが動作し続けるため、PCの速度が大幅に低下することがある
勝手にファイルを削除・変更される	重要なデータやシステムファイルが改ざんされたり、削除されることで、PCが正常に動作しなくなる可能性がある。
迷惑な広告やポップアップが頻繁に表示される	ウイルスが広告を強制的に表示し、ユーザーの操作を妨げることがある。
別のウイルスをダウンロードさせられる	一度感染すると、新たな**マルウェア**を次々にダウンロードさせられ、より深刻な被害につながることがある。
PCが乗っ取られる（遠隔操作される）	悪意のある第三者がPCを乗っ取り、犯罪の踏み台として使用する可能性があります。
金銭的な被害	ランサムウェアのようなウイルスに感染すると、PCのデータが暗号化されて開けなくなり、解除するために金銭を要求されることも。

参考）マルウェアはどんな悪さをするのか？

マルウェアはどんな悪さをするのか？

マルウェアは、増殖するための仕組みや他のコンピュータに感染するための機能がある。

例えば、コンピュータ内のファイルに自動的に感染したり、ネットワークに接続している他のコンピュータのファイルに自動的に感染したりするなどの方法で自己増殖します。コンピュータに登録されている電子メールのアドレス帳や過去の電子メールの送受信の履歴を利用して、自動的にウイルス付きの電子メールを送信するものや、利用者がホームページを見るだけで感染するものも多く、世界中にマルウェアが蔓延する大きな原因となっています。マルウェアが実施できる主な活動は、以下の通りです。

No.	主な活動	内容
1	自己増殖	ウイルスの中には、インターネットやLANを使用して、他の多くのコンピュータに感染することを目的としているものがあります。
2	情報漏洩（じょうほうろうえい）	情報漏洩を引き起こすタイプのウイルスには、利用者がキーボードで入力した情報を記録するキーロガーや、コンピュータ内に記録されている情報を外部に送信するスパイウェアと呼ばれるものなどがあります。
3	バックドアの作成	感染したコンピュータの内部に潜伏するタイプのウイルスをトロイの木馬と呼びます。この中でも、コンピュータに外部から侵入しやすいように「バックドア」と呼ばれる裏口を作成するタイプのウイルスは、いつでも攻撃者から遠隔操作できてしまう可能性があるため極めて危険です。
4	コンピュータシステムの破壊	ウイルスによっては、コンピュータシステムを破壊してしまうものがあります。その動作はウイルスによって異なりますが、特定の拡張子を持つファイルを探し出して自動的に削除するものから、コンピュータの動作を停止してしまうものまでさまざまです。
5	遠隔操作	コンピュータを外部からの踏み台として遠隔操作するためのウイルスをボット（BOT）と呼びます。ボットに感染したコンピュータは、同様にボットに感染した他の多数のコンピュータとともにボットネットを形成し、その一員として動作するようになります。そして、インターネットを通じて、悪意のある攻撃者が、ボットに感染したコンピュータを遠隔操作し攻撃の踏み台として利用することがあります。
6	ランサムウェア	ランサムウェアとは、感染したPC上に保存しているファイル（PCからアクセス可能なネットワーク上のファイルも含みます。）を暗号化して使用ができない状態にするマルウェアです。攻撃者は、復旧させることと引き換えに身代金を要求するため、ランサム（身代金:ransom）ウェアと呼ばれています。 ただし、身代金を支払っても復旧されない可能性があることや、金銭を支払うことで犯罪者に利益供与を行ったと見なされてしまうこともあるため、支払いに応じることは推奨されません。 また、これまでは暗号化して身代金を要求するケースが多かったものの、攻撃者が「より手軽に」身代金を得るため、「暗号化」を行わず、盗み取ったデータの公開を対価に身代金を要求する「ノーウェアランサム」攻撃による被害も増加しています。

ウィルスの感染と被害

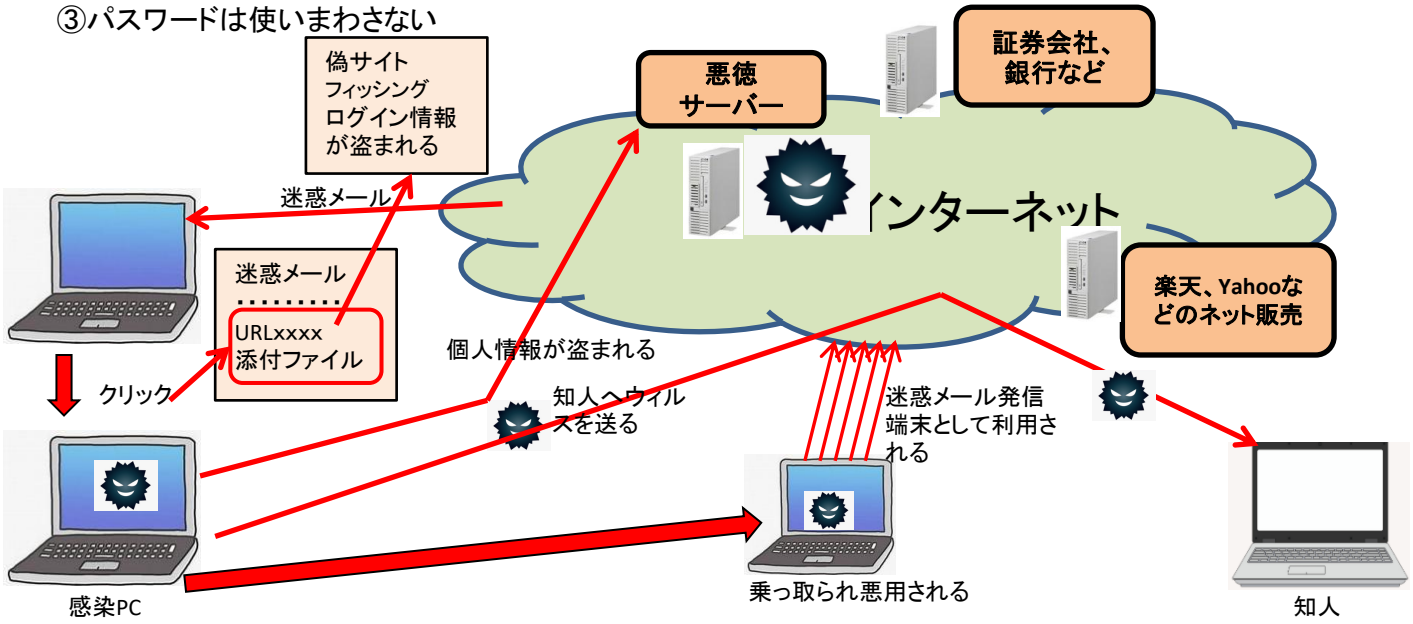
1.代表的なウィルスの感染と被害

1）迷惑メール（なりすましメール）に反応した。

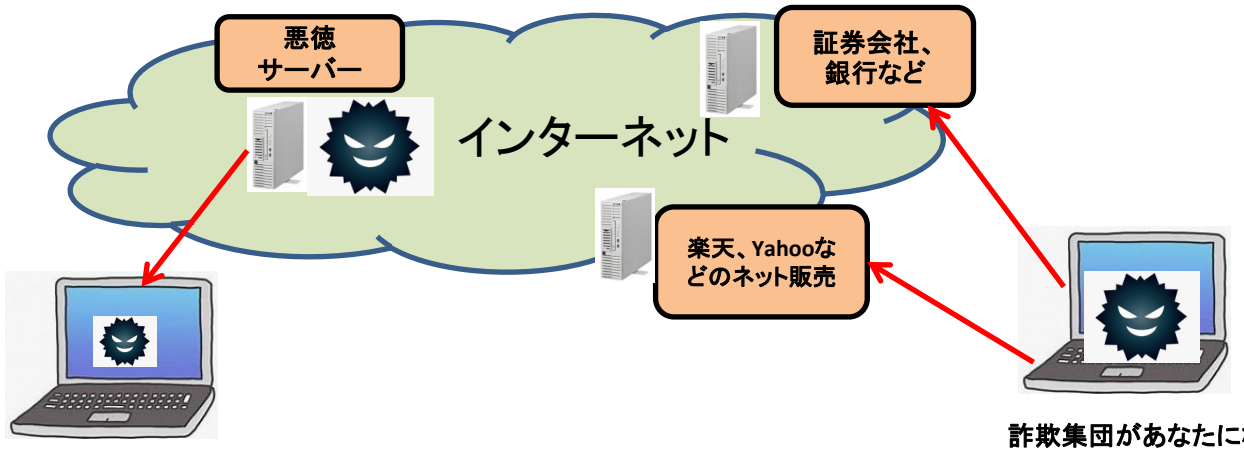
メールを開いただけでは通常ウィルスに感染しない。（キチンをサポートされているOSを使用している場合）
メール内にあるURLをクリックしたり、添付ファイルを開いたときに感染する。（最新のOSを使用していても感染する）
しかし、**サポートされていないOS（例：サポート終了後のWin10を使用している場合）は開いただけで感染する場合がある。**
参考）感染している人からのメールは注意。知人からのメールなので信用して添付ファイルを開くと知人がサポート切れのWin10を使用していた場合に知人が気が付かないでウィルスを添付してメールする場合がある。

2）インフォスティーラ （マルウェア）の感染
迷惑メール（＋感染している知人からのメール）から感染する。
悪徳サーバーからインフォスティーラに指示が出て、PC内にある個人情報が盗まれる。（各種ログイン情報等）

3）対策
①電子メールやSMSのリンクは開かない
②Webサイトのアクセスはブックマークから
③パスワードは使いまわさない



Windows１０サポート終了後に何もしない場合のリスク



詐欺集団があなたになりすまして、証券会社、銀行などにログインして取引を行ったり、ネットショッピングなどを行う

◇企業での影響

Windows11へのアップグレードは必須。行わないと最悪、倒産になる可能性あり。

・システムの停止：工場、電力、水道などがストップする。
・銀行など個人情報を扱っている企業からの漏れ、ブラックマーケットで売られる→信用が落ちる
・データにロックがかかり見れなくなる。身代金を請求される。企業活動が停止する

◇個人では具体的には；

・個人情報（クッキーなどから、各種ログイン情報（銀行、証券会社、ネットショッピングなどへのログイン情報）が漏れる。
→他人が勝手にログインし悪用して被害に遭う。
・データにロックがかかり見れなくなる。身代金を請求される。
他の人に迷惑をかける
・メールを通して相手にウィルスを送ってしまいます。
・PCが乗っ取られ、迷惑メール送るなど悪用される。

参考）最近話題になっている証券口座乗っ取り被害は2025.5j時点で1900件5,000億円以上の被害）

防衛策の基本

「自分が間違った操作をしない限り安全」は誤解

「ID・PWを自分から教える」「怪しい添付を開く」といった“**ユーザーのミス**”が原因の被害は多い。

ユーザーの操作ミスがなくても攻撃されるケースがある

攻撃者は“弱いPCを自動で探すロボット”を常に動かしている。

防衛策の基本中の基本

★サポートの終わったOS、アプリを使わない。（Windows10、Office2019はサポート切れです。）

★きちんとアップデートを行う。

サーバー攻撃に対する防衛策

防衛策	具体的に何をする？	防げる攻撃	企業	個人PC	個人スマホ
OS・ソフトを最新にする	Windows Update、Android/iOS更新、アプリ更新	脆弱性攻撃、改ざん、感染	○	○	○
多要素認証（2段階認証）	ログイン時にSMS/アプリ認証を追加	パスワード突破、不正ログイン	○	○	○
強力なパスワード	長く複雑なPW、使い回し禁止→パスキー	総当たり攻撃、乗っ取り	○	○	○
不要なサービス・ポートを閉じる	SSH/FTP/管理画面を外部公開しない	不正アクセス、侵入	○	ー	ー
WAF（Webアプリ防御）	SQLインジェクション・XSSを自動ブロック	Web攻撃全般	○	ー	ー
バックアップ	サイト・DB・PCデータを定期バックアップ	ランサムウェア、破壊	○	○	△
ログ監視	不審ログイン・アクセスを検知	侵入の早期発見	○	ー	ー
ウイルス対策（Defender等）	DefenderをON、スマホは標準保護でOK	マルウェア、トロイの木馬	○	○	△
フィッシング対策	怪しいメール・SMSのURLを開かない	偽ログイン、情報盗難	○	○	○
アプリの権限管理	カメラ・位置情報・連絡先を必要なアプリだけに	情報抜き取り、スパイアプリ	ー	ー	○
公衆Wi-Fiを避ける	暗号化なしWi-Fiを使わない	中間者攻撃、盗聴	ー	△	○
ルーター・VPNの更新	古いルーターを交換、最新ファーム更新	内部侵入、乗っ取り	○	○	ー
共有設定（SMB）を安全にする	SMBv1無効化、共有フォルダにPW設定	自動感染（WannaCry）	○	○	ー
不正アプリを入れない	Playストア以外のAPKを入れない	偽アプリ、乗っ取り	ー	ー	○

シニア向け

これから、シニア向けに分かり易く？説明します。

第1章：ネット詐欺とは？（導入）

1．シニアが遭いやすい詐欺トップ5

①フィッシング詐欺（偽メール・偽SMS） →銀行・宅配・マイナポータルを装う
②偽の警告画面（サポート詐欺） →「ウイルス感染！今すぐ電話！」
③偽ショッピングサイト →激安商品・在庫処分を装う
④投資詐欺（SNS・LINE） →「必ず儲かる」「有名人が推奨」
⑤アカウント乗っ取り →パスワード使い回しが原因

個人PCの主な感染ルート

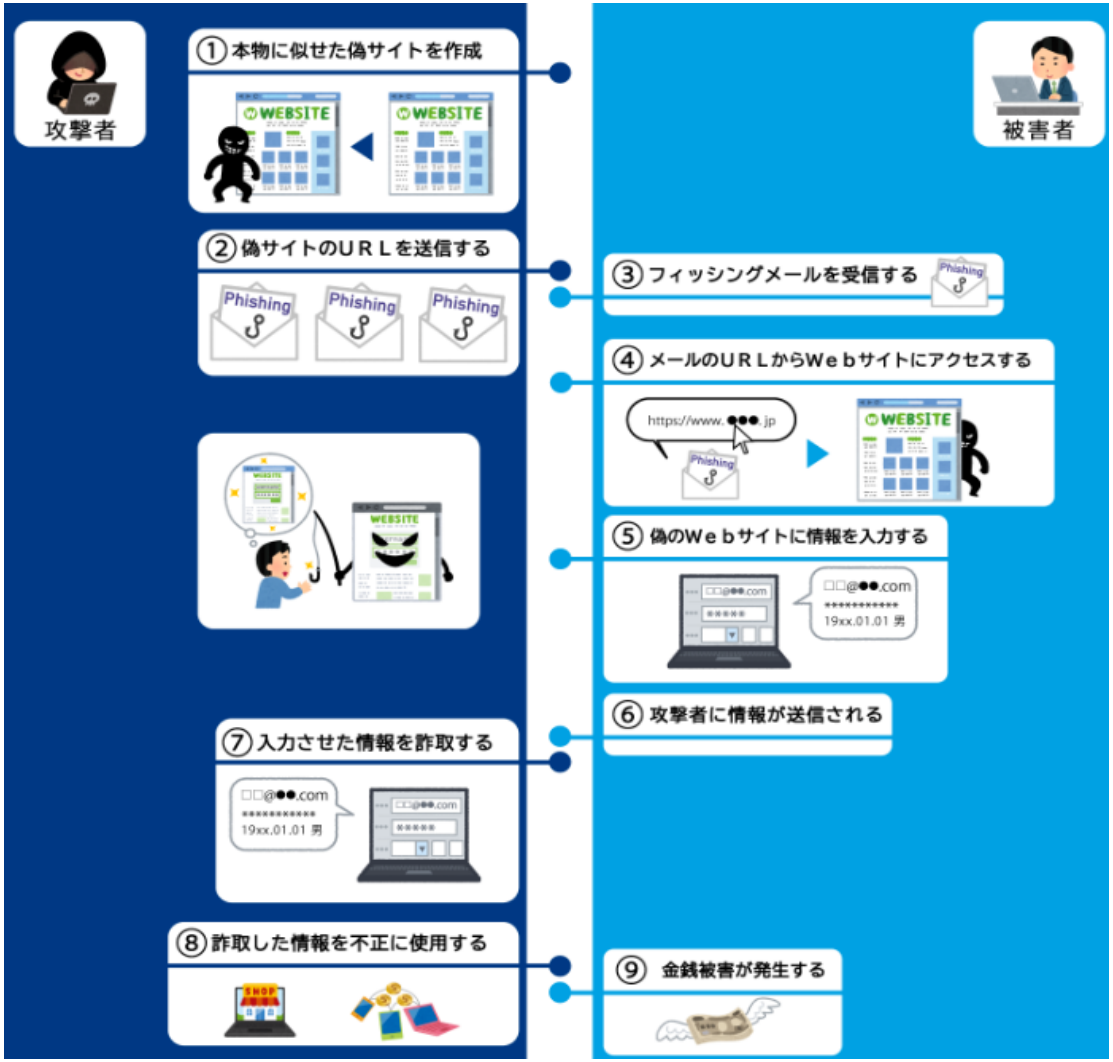
感染ルート	SMB関係？	説明
フィッシングメール	×	偽メールでID/PWを盗む
偽サイト（Amazon/銀行）	×	ログイン情報を盗む
悪意ある広告（マルバタイジング）	×	広告を表示しただけで感染することも
偽アプリ・偽ソフト	×	無料ソフトに見せかけたマルウェア
古いブラウザの脆弱性	×	Edge/Chromeが古いと危険
古いOfficeの脆弱性	×	Word/Excelの脆弱性を悪用
USBメモリ	×	持ち込み感染

2．詐欺に遭わないための“3つの鉄則”

鉄則1：メール・SMSのリンクは押さない →公式アプリやブックマークからアクセスする
鉄則2：電話番号を自分で調べてかけ直す →画面に出た番号は詐欺の可能性
鉄則3：パスワードを使い回さない →同じパスワードを使うと1つ漏れたら全部危険

具体例

①フィッシング詐欺（偽メール・偽SMS）→銀行・宅配・マイナポータルを装う



具体例

①フィッシング詐欺（偽メール・偽SMS）→銀行・宅配・マイナポータルを装う

具体例

マネックス証券より送信された安全なメールです

一時的な取引停止設定およびパスキー登録の確認

平素よりマネックス証券をご利用いただき、誠にありがとうございます。

当社では、不正アクセスからお客様の資産を守るため、**「一時的な取引停止」**および**「パスキー」**の登録を推奨しております。
2026年3月27日現在の設定状況を以下のボタンよりご確認ください。

パスキー登録・設定状況を確認する

※ログイン後、登録情報照会ページへ自動遷移します。

クリックしてはいけない！！

区分	対象となる主な商品・サービス
取引・閲覧ともに停止	出金、FX PLUS、マネックスゴールド、銘柄スカウター（外国株）、ジュニアNISA口座 等
取引のみ停止	国内株式、外国株式、債券、先物・オプション、投資信託（積立除く）等
制限の対象外	ログイン、入金、残高照会、投資情報、暗号資産CFD 等

※ 家計簿アプリ等への資産情報連携も停止設定後に中断されます。
※ 制限解除には、パスキー等の多要素認証が必要となります。

具体例

【みずほ証券】新しい口座安全対策の実施について
みずほ証券 [noreply@brzmnlpo.mail46.hbzjgt.com]
送信日時: 2026/05/18 (月) 14:00
宛先: nakamuratoshio@point.gmobb.jp

****
このメールアドレスは送信専用です。
返信によるお問い合わせはお受けしておりません。
****

お客様の大切な金融資産を守るため、以下の新しい口座安全対策を2026年1月15日(月)より実施いたします。

■ 新しい安全対策の概要:
- 強化されたログイン認証:ログイン時に追加の認証手続きを導入します。
- 不正アクセスの監視強化:異常なアクセス試行をリアルタイムで監視し、対応します。
- セキュリティ通知の送信:重要なセキュリティ関連の変更があった場合、即時に通知をお送りします。

■ お客様にお願いすること:
- 7月7日までに、みずほ証券ネット倶楽部にログインし、セキュリティ設定をご確認ください。

■ ログインはこちら:

https://www.matsui.co.jp/login/

クリックしてはいけない！！

ご不明な点がございましたら、お気軽にお問い合わせください:

==========
みずほ証券コールセンター
TEL:0120-324-390
営業時間:平日8:00～19:00、土曜日9:00～17:00(日祝休業)
==========

具体例

②偽の警告画面（サポート詐欺）→「ウイルス感染！今すぐ電話！」

大きな音が出るので驚く。いろいろ操作をしても消えない。

↓

電源を落とし、再起動する。通常の操作はできないので電源を強制的に落とす。
電源ボタンを５秒以上長押しする。

対策例（生成AIを活用）

実際に遭遇すると、それが迷惑メールなのか？実際のメールなのか判断できない。

対策案の１例　生成AIを活用し、判断してもらう。

Copilotにメールをアップし「添付のようなメールを受診しました。どのように対応したらよいですか？」と質問する。

回答；

結論：このメールは“Amazonを装ったフィッシングメール”の可能性が極めて高いので、リンクを絶対に開かず削除してください。

⚠ まず結論（最重要）

送信元アドレスが Amazon ではない → sq23.akanamujer.com は Amazon と無関係のドメイン

本文の日本語が不自然 →「お客様、ご注文の商品について」など、公式メールでは使わない表現

電話番号が Amazon公式ではない → Amazonの配送連絡は 050番号を使わない

“配達状況を確認する”ボタン → 偽サイトへ誘導する典型的な手口

□このメールが危険と判断できるポイント

差出人が Amazon公式ドメインではない Amazon公式は @amazon.co.jp のみ

リンク先が偽サイトの可能性 ログイン情報やクレジットカード情報を盗む目的が多い

「置き配の不備」など不安を煽る文面 → 典型的な誘導パターン

✔ いま取るべき対応（あなた向けに最適化）

リンクを絶対に押さない

添付・ボタンも開かない

メールは削除してOK

Amazonの注文状況は、必ず公式アプリ or 公式サイトから確認 → ブラウザで amazon.co.jp を直接開くのが安全

□念のため確認したいこと

以下のどれかを教えてください（1つでOK）：

このメールに 心当たりのある注文 はありますか？

「配達状況を確認する」ボタンを 押してしまったか？

Amazonにログイン情報を入力してしまったか？

状況に応じて、

パスワード変更、不正アクセスチェック、クレジットカード確認 など、必要な対処をすぐに案内します。

第2章：ウイルスはどう侵入する？

1．ウイルスの侵入経路（シニアが特に引っかかりやすい順）
①偽のメールの添付ファイル →「請求書」「領収書」「宅配便の不在通知」など
②偽のサイトに誘導されてダウンロードさせられる →「ウイルスに感染しています！」という警告画面
③古いOSや古いアプリの“穴（脆弱性）”を突かれる →Windows10のまま使うと特に危険
④USBメモリ経由 →他人のUSBを挿すのは危険

2．Windows10を使い続ける危険性
Windows10は 2025年10月にサポート終了
サポート終了＝ 泥棒に開けられる“鍵の壊れた家”に住み続けるのと同じ
新しいウイルスが出ても、Windows10はもう直してくれない
結果：
個人情報が盗まれる
ネットバンキングが乗っ取られる
PCが動かなくなる
詐欺サイトに勝手に誘導される

第3章：スマホで増えている詐欺

スマホ版：ネット詐欺に遭わないために。
スマホ特有の危険ポイント

1. SMS（ショートメール）詐欺が非常に多い
シニアが最も引っかかりやすいのが **SMSのリンク**
「宅配便の不在通知」
「料金未払い」
「アカウント停止」
「ETCカードの更新」
→ ほぼ100%詐欺。リンクは絶対に押さない。

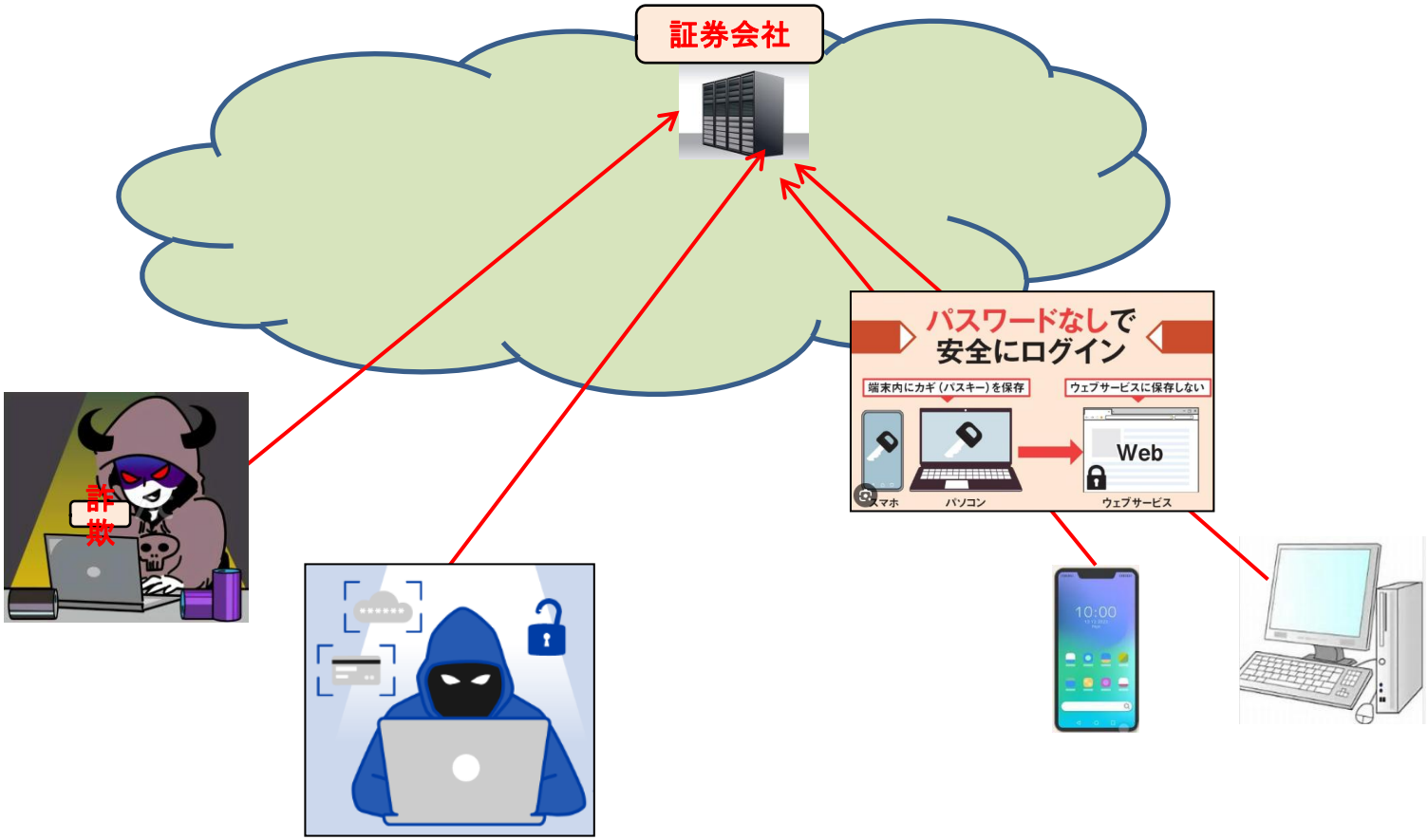
2. 偽の警告画面（スマホ版サポート詐欺）
「ウイルスに感染しました！」
「今すぐ電話してください！」
「スマホが破損しています！」
→ 触らず、閉じるだけでOK。絶対に電話しない。

3. 偽アプリ（特にAndroid）
本物そっくりの銀行アプリ
QRコード読み取りアプリに偽物が混ざる
無料ゲームにウイルスが仕込まれることも
→ Playストア以外からアプリを入れない。

4. LINE乗っ取り
「助けて」「プリペイドカード買って」
「写真送って」
「このURL見て」
→ パスワード使い回しが原因。

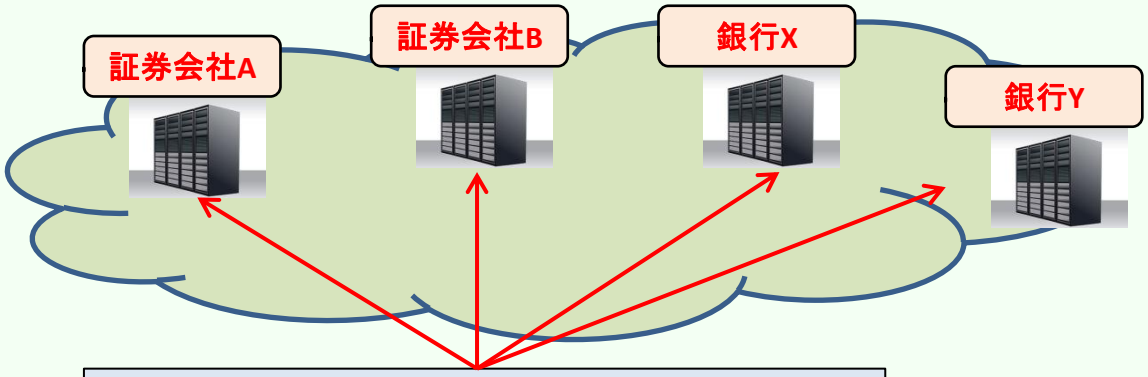
5. 公共Wi-Fiの危険
駅・カフェの無料Wi-Fi
偽のWi-Fiスポットに接続させる詐欺もある
→ 公共Wi-Fiではログインしない。

安全なパスキーとは

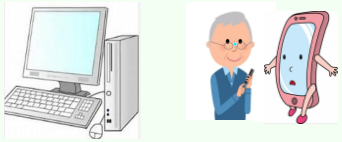

証券会社
詐欺
パスワードなしで
安全にログイン
端末内にカギ（パスキー）を保存
ウェブサービスに保存しない
Web
スマホ
パソコン
ウェブサービス
10:00

パスキーの強み

次世代の安全な仕組み。パスワードより100倍安全。



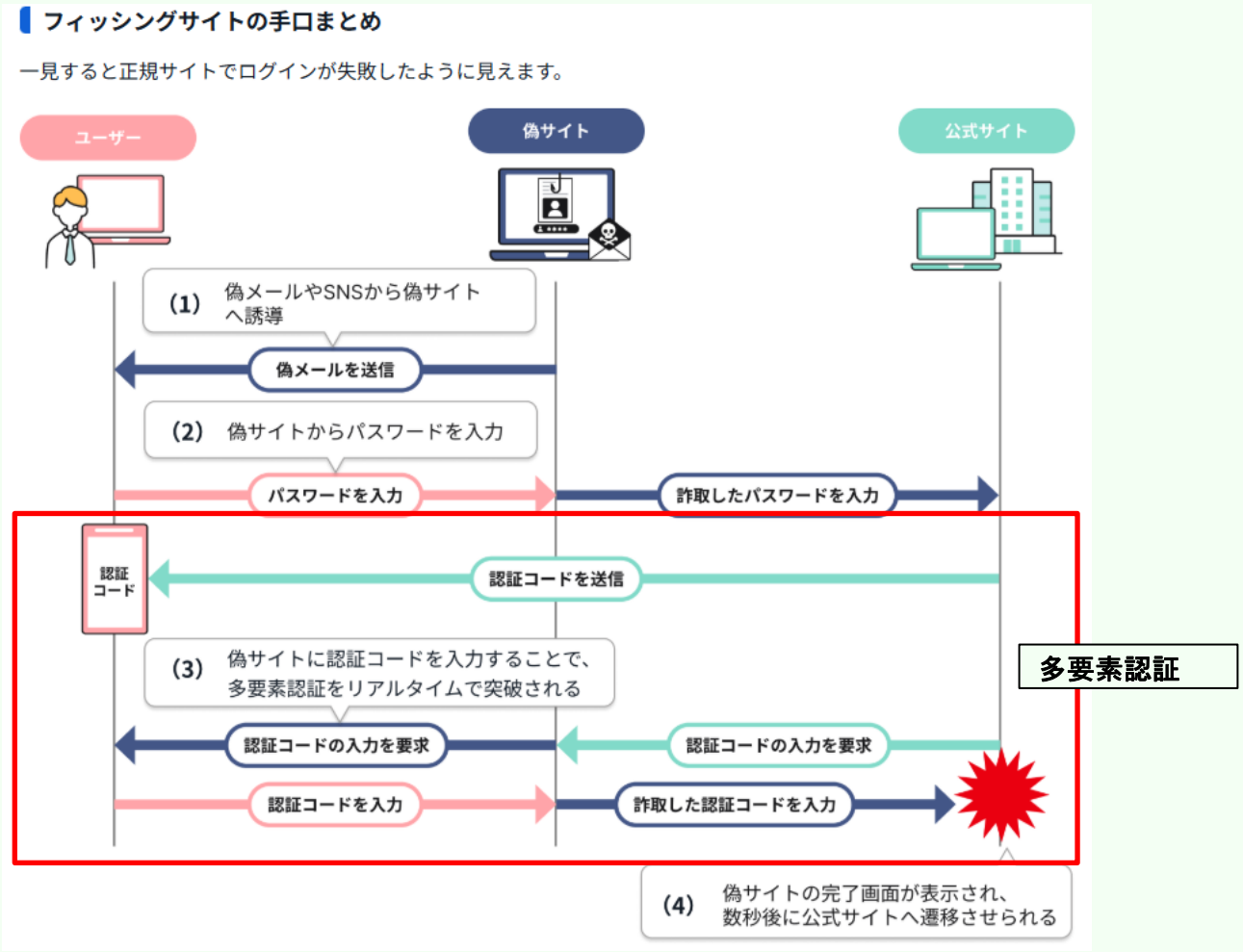
同じ操作（PIN、指紋認証、顔認証）でどこでもログインできる。
個別のログイン方法は必要ない！！



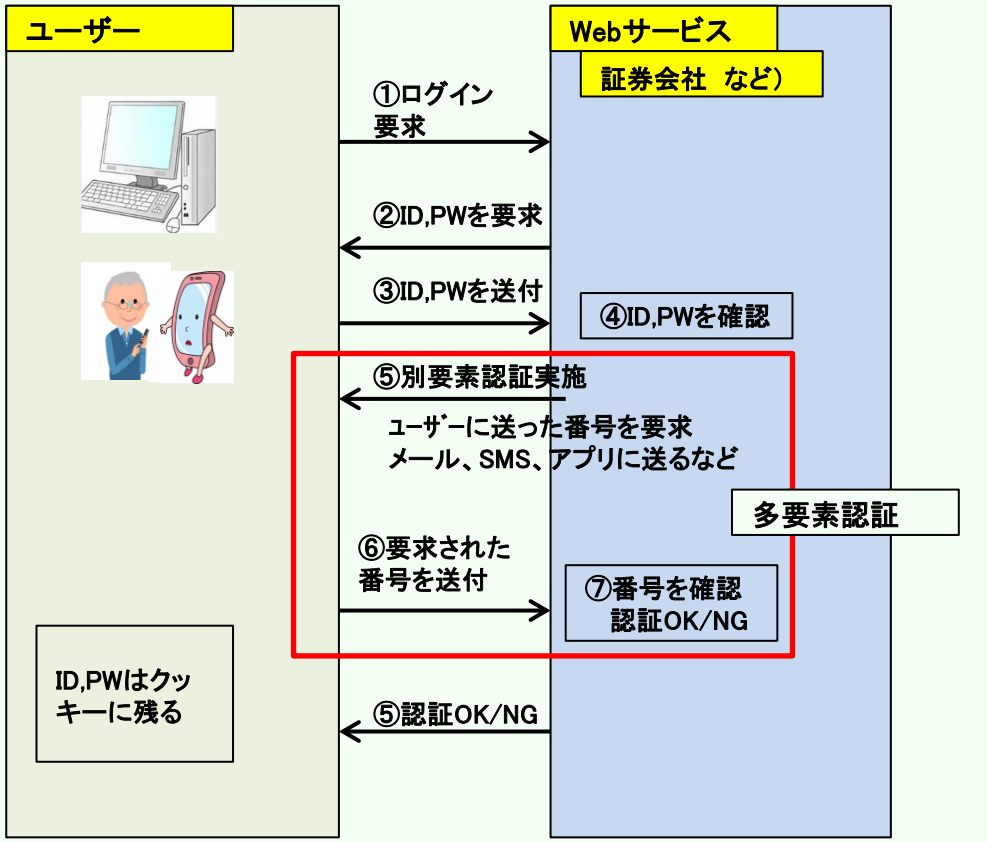
パスキーの強み

- フィッシングされない。→偽サイトは公開鍵が違うため認証できない
- パスワード漏洩が起きない→データ流出事件が起きても安全
- 入力が不要で速い➡ID,パスワードを覚える必要がない。
- PINや生体認証は端末ローカル（特定端末でしか認証できない）で安全
- 秘密鍵は端末外に出ない
- 端末紛失時の復旧手段が複数ある

フィッシングの流れ


フィッシングサイトの手口まとめ
一見すると正規サイトでログインが失敗したように見えます。
ユーザー
偽サイト
公式サイト
(1) 偽メールやSNSから偽サイトへ誘導
偽メールを送信
(2) 偽サイトからパスワードを入力
パスワードを入力
詐取したパスワードを入力
認証コード
認証コードを送信
(3) 偽サイトに認証コードを入力することで、多要素認証をリアルタイムで突破される
多要素認証
認証コードの入力を要求
認証コードの入力を要求
認証コードを入力
詐取した認証コードを入力
(4) 偽サイトの完了画面が表示され、数秒後に公式サイトへ遷移させられる

今までの認証方法

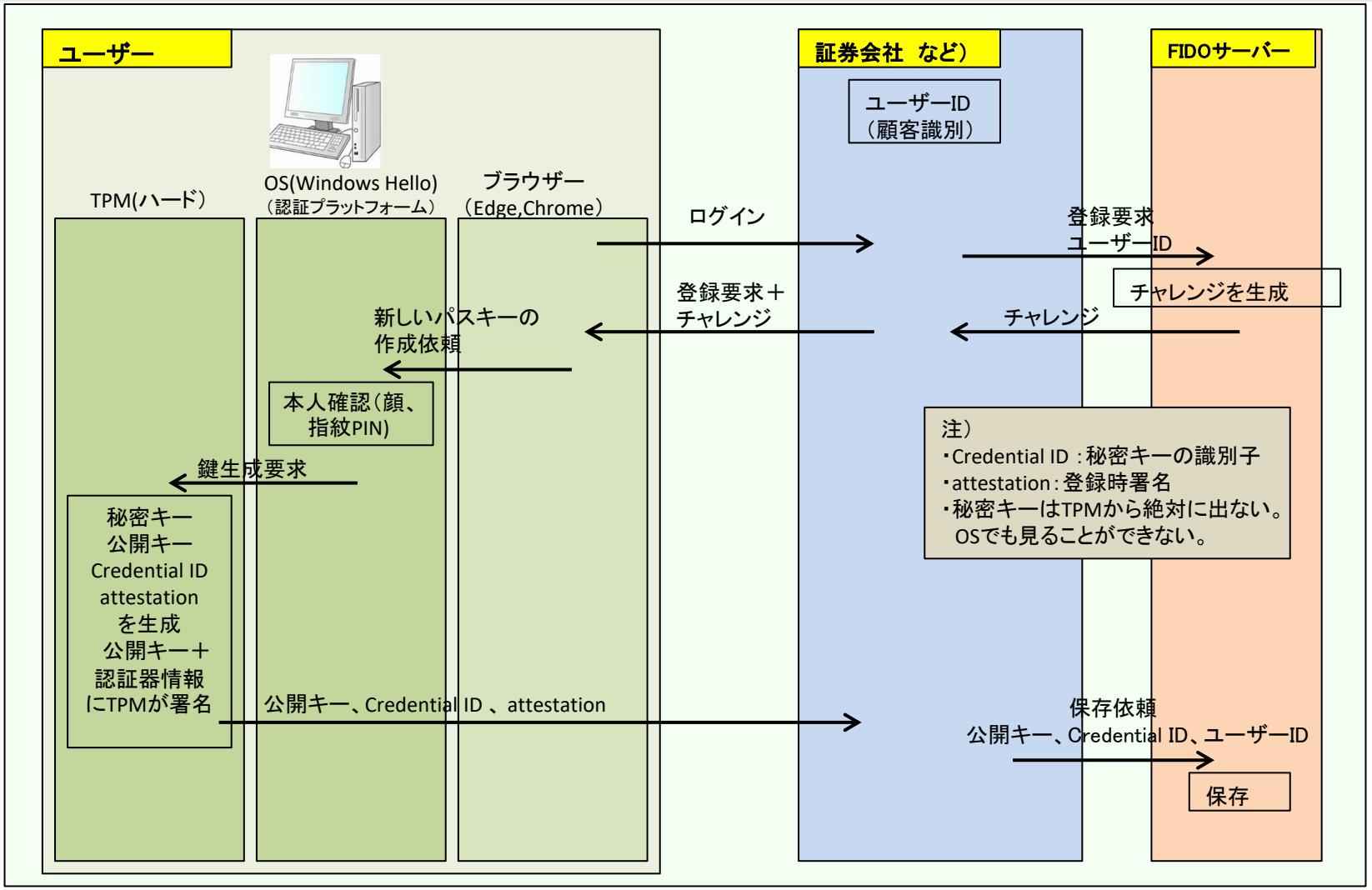


◇ID,PW認証
サービス毎のID,PWを覚えなくてはいけない。

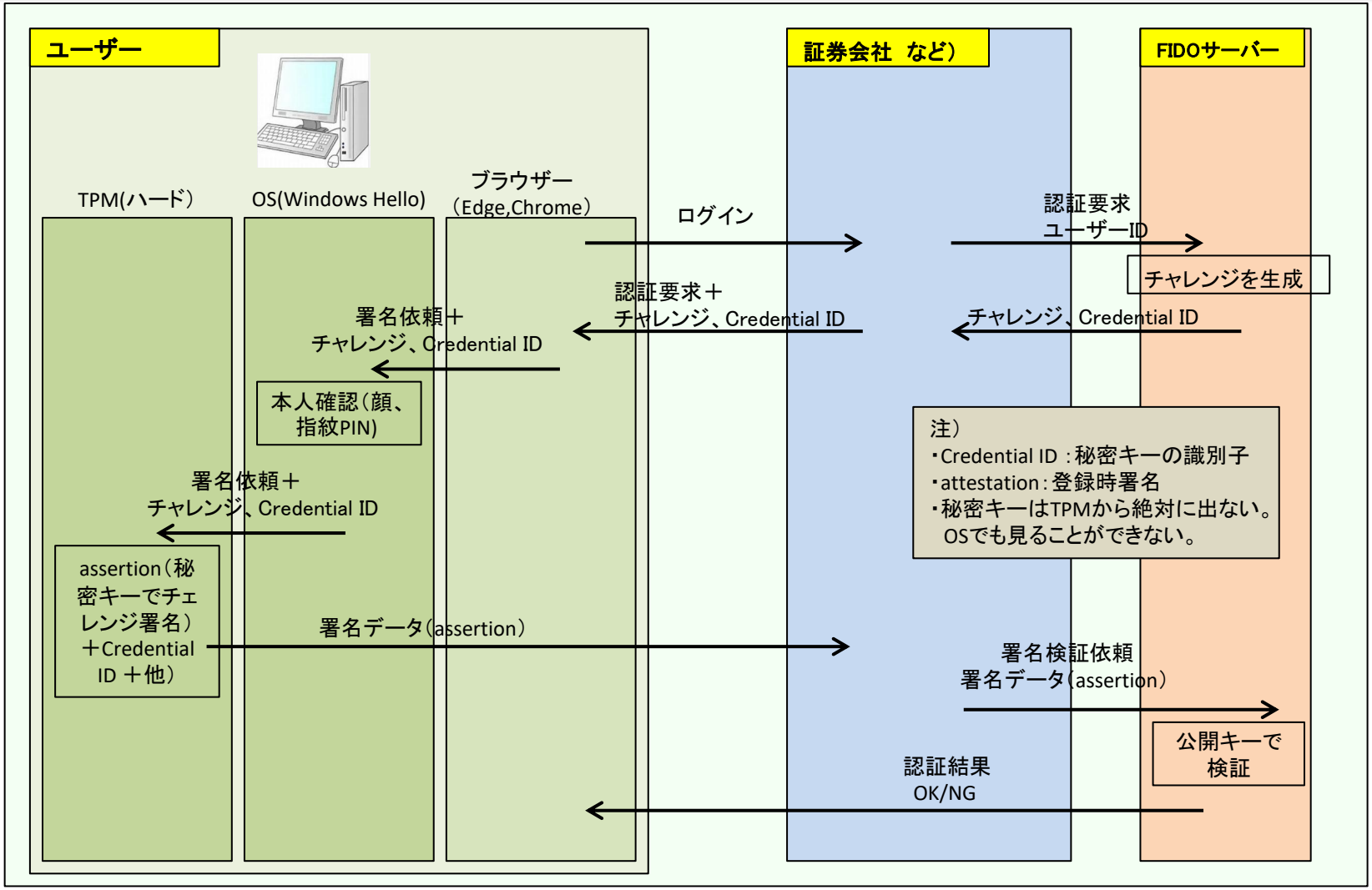
◇単要素認証（ID,PWだけで認証する）
詐欺に弱い！ID,PWが盗まれると終わり。偽メール、遠隔操作により乗っ取られる。

◇多要素認証（ID,PW＋α）
詐欺に強い！ID,PWを盗まれてもサービスが乗っ取られない。
しかし別途確認のためにスマホなどが必要で面倒である。

パスキーの流れ(登録時）PCの場合



パスキーの流れ(認証時）PCの場合



パスキー　スマホ（PCとの対応）

PC

TPM

Windows　Hello

スマホ

①iPhone:Secure Enclave
②Android：StrongBox
（またはTEE（TrustZone）

①iPhone：icloud　Kyechain
②Android：
Google Password Manager

ブラウザー

サービス（証券会社など）

FIDOサーバー

付加情報

・**FIDOサーバー**:FIDO（Fast IDentity Online）規格に準拠し、パスワードを使わずに安全な「パスキー認証」を実現するための認証サーバー

・パスキーはアカウントに紐づくのではなくデバイスに紐づく

・PCとスマホでは別々の認証方法が使える。
例：・PC：パスキー、・スマホ：ID，PW

・パスキーを登録しても今までのID＋PWでログインできる
サービス側（証券会社によって異なる。
パスキーを登録するとID,PWではログインできないサービスもある。

・**日本の証券会社の“実情”**はどうか？
現状の傾向をまとめると：
- パスキー導入＝ID＋PW無効化　海外大手サービスでは一般的
→日本では ほぼ無い
- **パスキーとID＋PWの併存→ ほぼ全社これ**
- ユーザーがパスワード無効化できる

・**チャレンジ**
数十バイトのランダムデータ。 同じものは1度しか使われない。

・**TPM**（Trusted Platform Module）：
PC の中にある“独立したセキュリティ専用ハードウェア”。
「小さな金庫」＋「暗号計算専用プロセッサ」

・**StrongBox**：高級スマホ
物理的に独立したセキュリティチップ

・**TEE（TrustZone）**中級、低級スマホ
物理的には独立していない。CPU内部のSecure World

- 高級機種 → StrongBox（＋TEE）
- 中級機種 → TEE（TrustZone）＋Keystore
- 低級機種 → ソフトウェアKeystore（TEEなし）

・**キーの保管場所**

PCの中（TPM）
秘密キー(サービスごと)
・SBI証券用秘密キー　A
・楽天証券用秘密キー　B
・XXXX用j秘密キー　C

証券会社
・A顧客用
PC用公開キー
スマホ用公開キー
・・・
・X顧客用公開キー

・ブラウザーにはメタデータを保存、同期の機能がある。メタデータとはサービスのドメイン（例：sbi.co.jp）、公開キー、Credential ID，どの方式（TPM/Secure Enclaveka） など

・**Credential ID**：秘密キーの識別子
・**attestation**：登録時署名（チャレンジも含まれる。） デバイスの信頼性（“鍵の出自”を保証）
・**assertion**:認証時署名（チャレンジも含まれる。） 本人の認証
・秘密キーはTPMから絶対に出ない。
OSでも見ることができない。

事前準備

PC

Windows Helloの“本人確認手段“の設定
・“設定”－“アカウント”－“サインオプション”
サインインする方法に“顔認証”“指紋認証”“PIN”から選び設定する。

スマホ

Android9以降のスマホはほぼ問題なく使える。

① 生体認証 or PIN を設定
設定 → セキュリティ → 画面ロック
- 指紋
- 顔
- PIN

のいずれかを設定
② Google パスワードマネージャーをオン
設定 → パスワードとアカウント → Google
「パスワードマネージャー」をオン
③ StrongBox または TEE が有効（自動）
これはユーザーが設定する必要はない。
スマホが対応していれば自動で使われる。

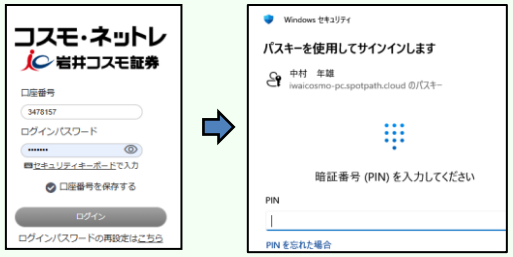
実例

岩井証券

①今までのID、PWでログインする。
②第二要素認証としてパスキーでログインする。

ログインに今までのID、PWが必要。
第二要素認証としてパスキーでログインできるので便利。ログインがPCだけでできる（メール、SMNなどを確認しないでもできる）は便利。

パスキーでないとログインできなくなる。



SBI証券

①パスキーでログイン
　注）ID,PWでもログインできる。
　ログイン画面にどちらかを選ぶようになっている。

今までのID,PWだけでログインできる。
パスキーを導入した意味がない！
フィッシング詐欺に弱い。

楽天証券

①IDのみを入力する。
②画面に出たQRコードをスマホで読み取りパスキーログインが完了。

パスキーを使うのに今までのIDが必要（PWは不要）
スマホが必須。使いづらい！

注）①パスキーの目的はID,PWが無くてもログインできること。
　②ID,PWを残す理由：「パスキーが使えない端末の人もいる」、「PC,スマホを紛失や故障した人が困る」 など
　Goole,Microsoft,Apple,多くの海外銀行　などはパスキーだけでログイン可能。当たり前

パスキー（付加情報（２））

★端末を紛失・故障したらどうするのか？ここが一番気になるところ。
実は、パスキーは “単一端末に閉じない仕組み” が用意されている。
A. 同じアカウントで同期されるパスキー（クラウド同期型）
Google、Apple、Microsoft のパスキーはアカウントに紐づいて複数端末に自動同期 されます。
例：
- iPhoneで作ったパスキー → iPad、Macにも自動でコピー
- Androidで作ったパスキー → 他のAndroid端末にも同期
- Windows Helloのパスキー → Microsoftアカウントでバックアップ

1台壊れても、他の端末でログイン可能

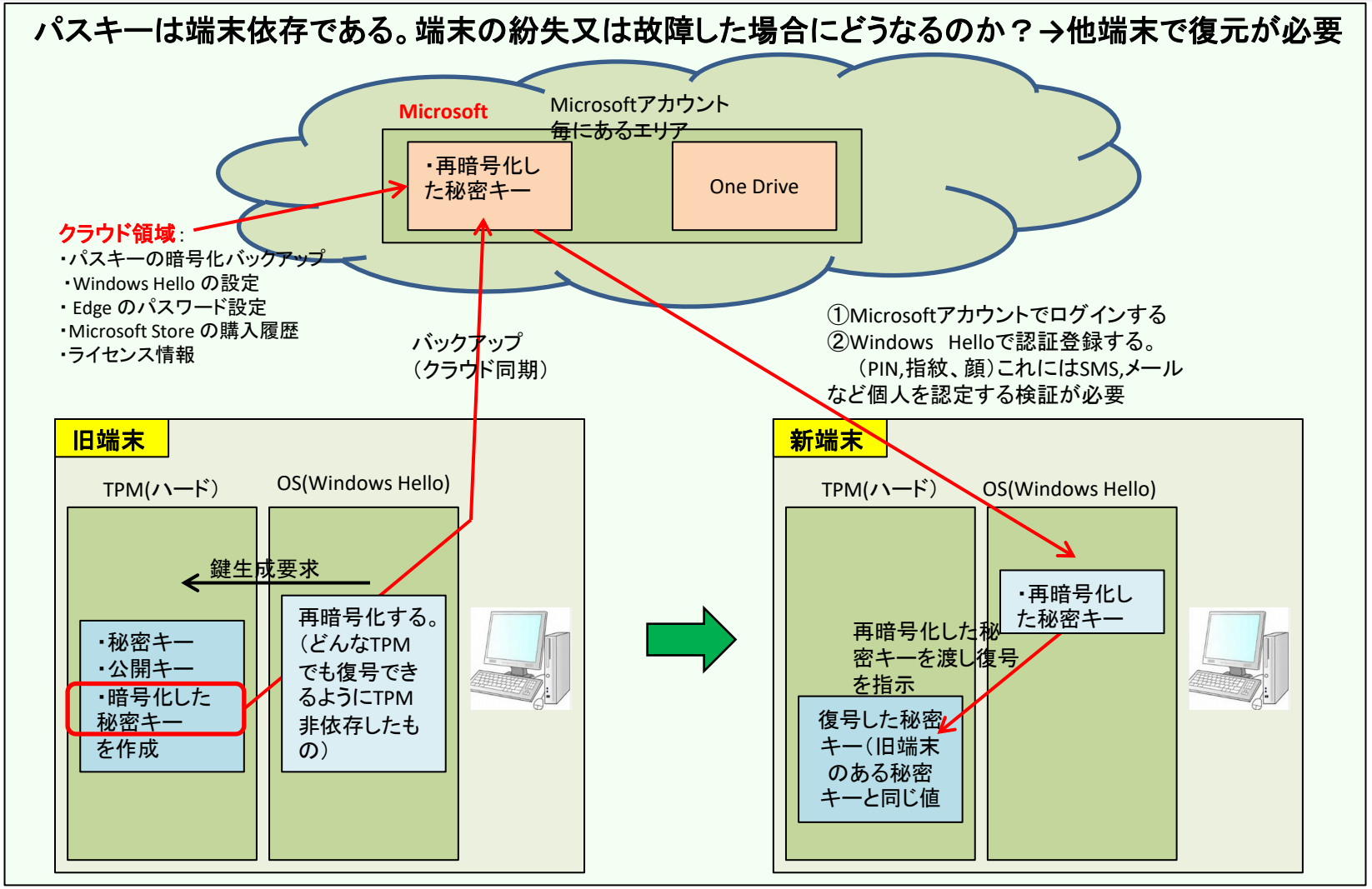
★ 日本の多くのサービスが「パスキー＋ID/PW併存」なのはなぜ？
理由はシンプルで、移行期間だからです。（→早い話が日本人はデジタル化に対応できない人がシニア中心に多いからです。）
- 日本のWebサービスはまだパスキー完全移行が進んでいない
- ユーザーの端末環境がバラバラ（古いAndroid、ガラホ、PCなど）
- パスキーだけにすると「ログインできない人」が大量に出る

そのため、現状は パスキーは“便利な追加手段” として提供されているだけで、
パスワード廃止はこれから という段階です。
海外（Google、Microsoft、Apple）はすでに
「パスキー優先・パスワードはほぼ使わない」方向に進んでいます。

★ Microsoft アカウントのクラウドとは何か？
これは「Microsoft アカウントの設定・秘密情報・暗号鍵などを安全に保存するためのクラウド基盤」のこと。
具体的には：
- Windows Hello の設定
- パスキーの暗号化バックアップ
- Edge のパスワード
- デバイスの暗号化キー（BitLocker 回復キーな）
- Microsoft Store の購入履歴
- ライセンス情報

パスキー（秘密キー）の復元流れ

パスキーは端末依存である。端末の紛失又は故障した場合にどうなるのか？→他端末で復元が必要



付録　Windows10パソコンの対応策