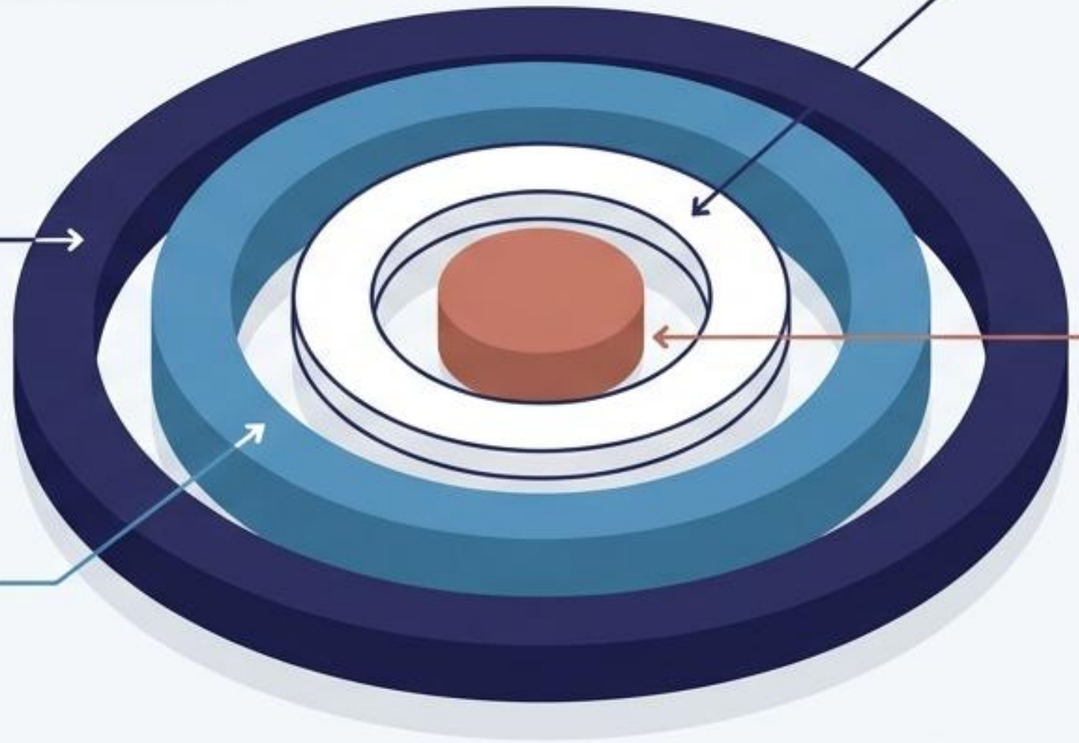
デジタル防衛ダッシュボード

個人の習慣から組織の安全を築くプレイブック

サイバー脅威から身を守るための
「4つの防衛層」と実践的アクション

サイバーセキュリティ空間の「4つの防衛層」

インターネット上の脅威に対する「モグラたたき」をやめましょう。自分自身のデジタル端末と組織のネットワークを守るためには、体系立てられた「要塞」を築く必要があります。



Layer 1 (外壁):
OS・ソフトウェアの更新

Layer 2 (関所):
パスワードと多要素認証

Layer 3 (衛兵):
フィッシング対策とアプリ管理

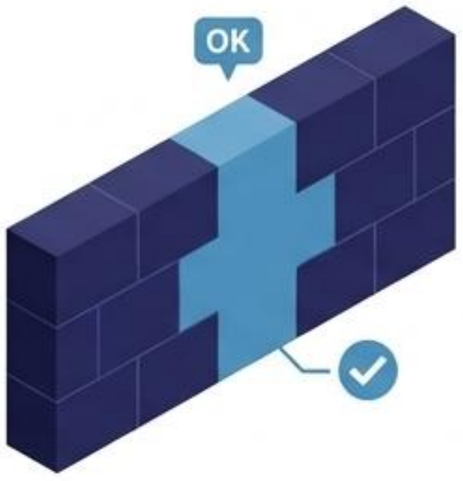
Layer 4 (金庫):
物理ロック・バックアップ・報告

防衛層 1：外壁の修復（アップデート）

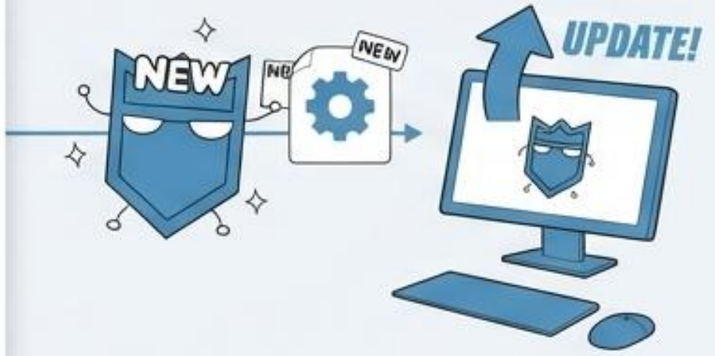
アップデート前（BEFORE）

脆弱性（穴）が開いたままの状態

アップデート後（AFTER）



穴が修復され、防御が強化された状態



更新すべき最重要ターゲット:

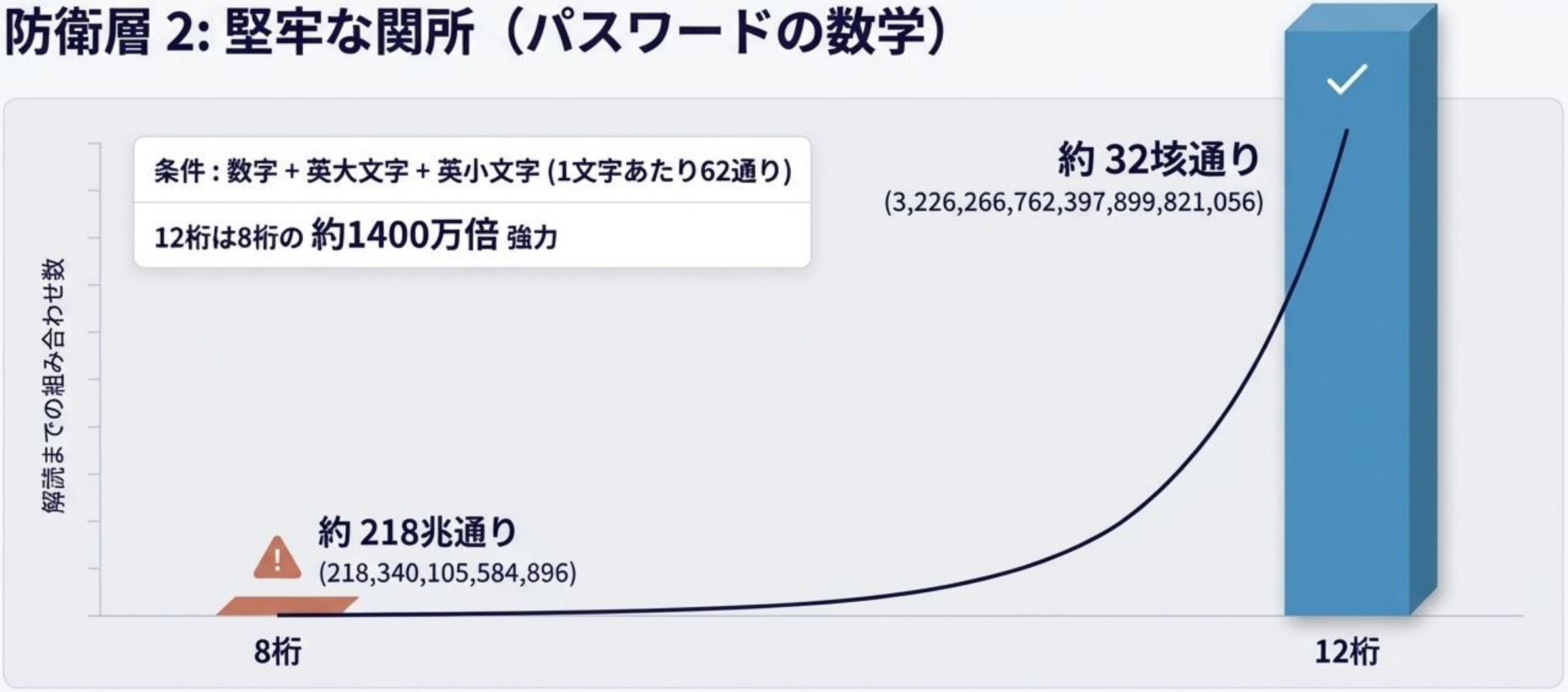
- 1. OS (Windows, macOS, iOS, Android)
- 2. ウェブブラウザ (Chrome, Edge, Safari) とプラグイン
- 3. 標的にされやすいソフト (Adobe Reader, Java)
- 4. ネットワーク機器 (ルータ、IoT家電、監視カメラのファームウェア)

重要ポイント:

脆弱性は「見つかっていないだけ」の穴。アップデートの終了した古いOSやソフトの利用は、壁に穴を開けたまま放置するのと同じです。

Editorial Dashboard

防衛層 2: 堅牢な関所（パスワードの数学）



総当たり攻撃（ブルートフォース）を防ぐ唯一の方法は、「突破に非現実的な時間がかかる状態」を作ること。
文字数を増やすだけで、防御力は指数関数的に跳ね上がります。

使い回しのドミノ倒し（リスト型攻撃）

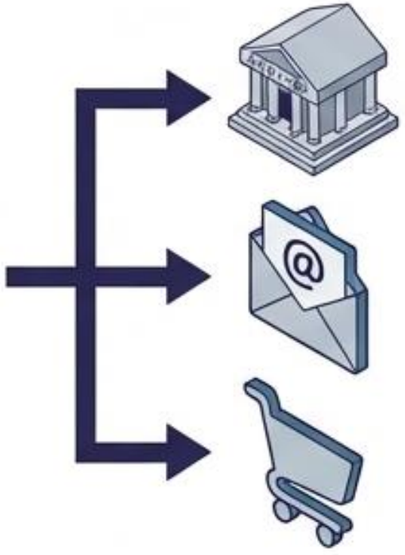
1. 最初の情報漏洩

情報管理の甘いサイトから、IDとパスワードのペアが流出。

2. 同じ鍵の試行

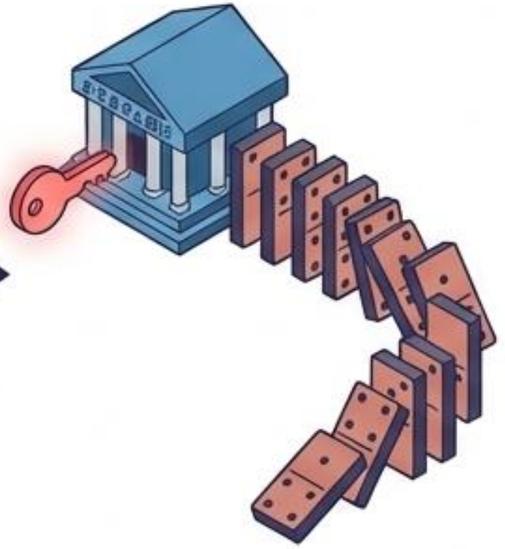
攻撃者は、手に入れた認証情報（鍵）を他のサービスで試行。

3. 複数ターゲット



銀行、メール、ショッピングなど、生活に直結する重要サービスが標的。

4. ドミノ倒し



1つが突破されると、使い回している全てのサービスが次々と乗っ取られる。

12桁の複雑なパスワードを作成しても、複数のサービスで使い回していれば意味がありません。1箇所から漏洩すれば、すべてのアカウントが一網打尽にされます。

「基本のパスワード＋末尾に数字/サービス名」のような単純な法則性もすぐに見破られます。独立したパスワード管理アプリか、物理ノートでの管理を徹底してください。

多要素認証（MFA）という最後の砦

認証スペクトラム

パスワードは、マルウェア感染や通信経路、サービス側のサーバ侵害など、自分に落ち度がなくても漏洩する可能性があります。

【プッシュ通知の罠】

攻撃者がログインを試行した際に届く、見知らぬ二要素認証の承認通知を絶対に許可してはいけません。

防衛層 3: 衛兵の眼（フィッシング詐欺の解剖）

心理的盲点を突く「焦燥感」の煽り

攻撃者は、利用者に焦りを感じさせ、冷静な判断を奪うために、時間制限や緊急性を装う言葉を使用します。

正規サイトを偽装した不審なURLドメイン

「.gq」などの見慣れないドメインや、正規の「.co.jp」に似せた文字列が含まれており、アクセス先が正規の銀行ではないことを示唆しています。

宅配業者は通常、SMSで不在通知を送りません

多くの正規サービスや宅配業者は、不在通知をSMSではなく、公式アプリや電子メール、あるいは紙の不在票で通知します。SMSでの連絡は疑うべき兆候です。

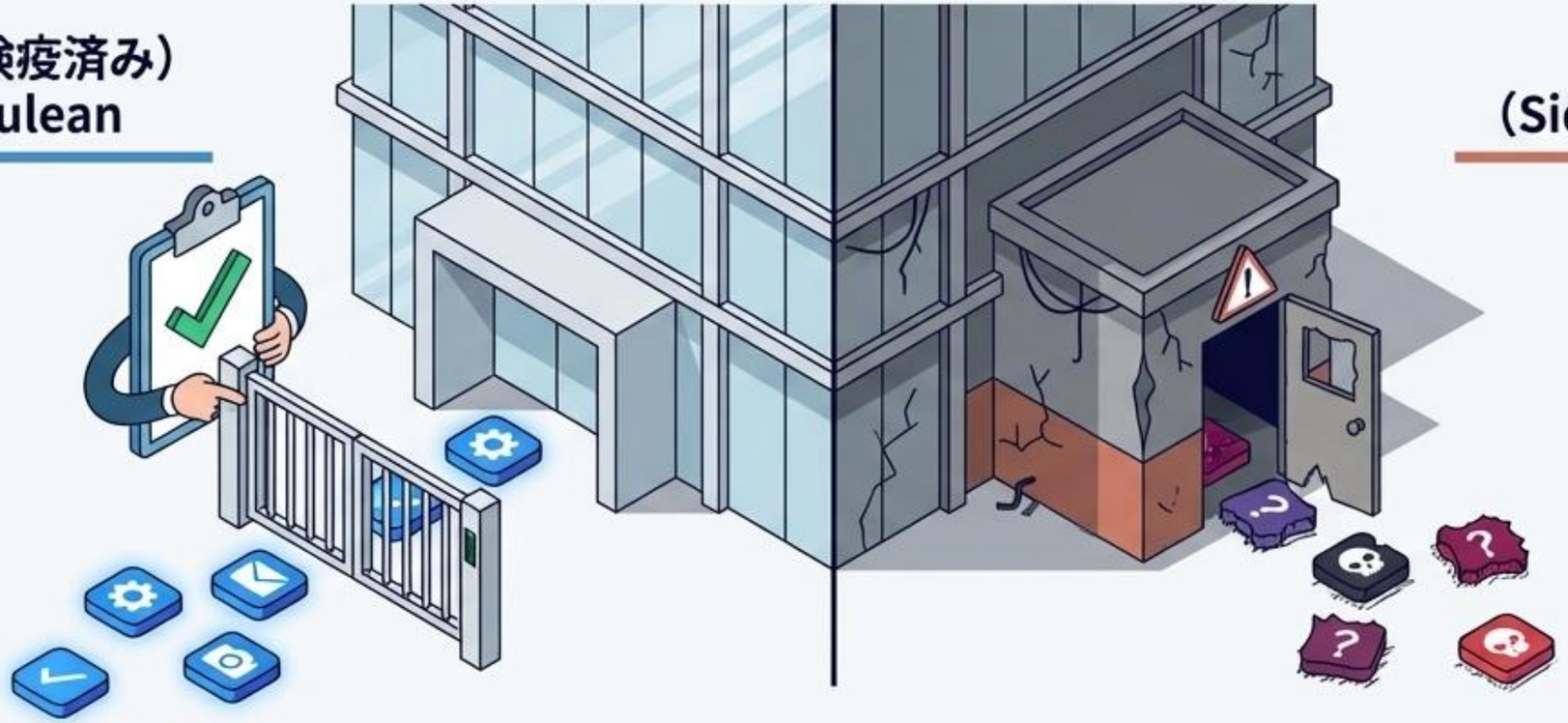
攻撃者は災害時や緊急時など、人間の警戒心が弱くなる瞬間を狙います。
「見るだけで完結しない情報（リンクやファイル）」はすべて疑うのが基本です。

公式ストアと「勝手口」のリスク

スマホのセキュリティは、メーカーが想定する
利用方法を守ることが大前提です。

公式ストア（検疫済み）
Matte Cerulean

勝手口
（Sideloading / 脱獄）



- 公式ストアのアプリは､配信前にセキュリティ審査 (検疫) を通過しています。
- 「root化」や「JailBreak (脱獄)」などの改造は、セキュリティレベルを著しく下げる危険行為です。
- 「不明なアプリのインストール」　設定は、常にオフを維持してください。

アプリ権限のX線検査（最小権限の原則）

初回起動時に求められる**「権限（アクセス許可）」の同意画面を読み飛ばしてはいけません。**
単なる電卓や壁紙アプリが、なぜカメラや住所録へのアクセスを求めるのでしょうか？
不必要な権限を求めるアプリは、**背後で情報を抜き取るスパイアプリの可能性**があります。
インストールを中止してください。

防衛層 4: 物理金庫（画面ロックと通知の死角）

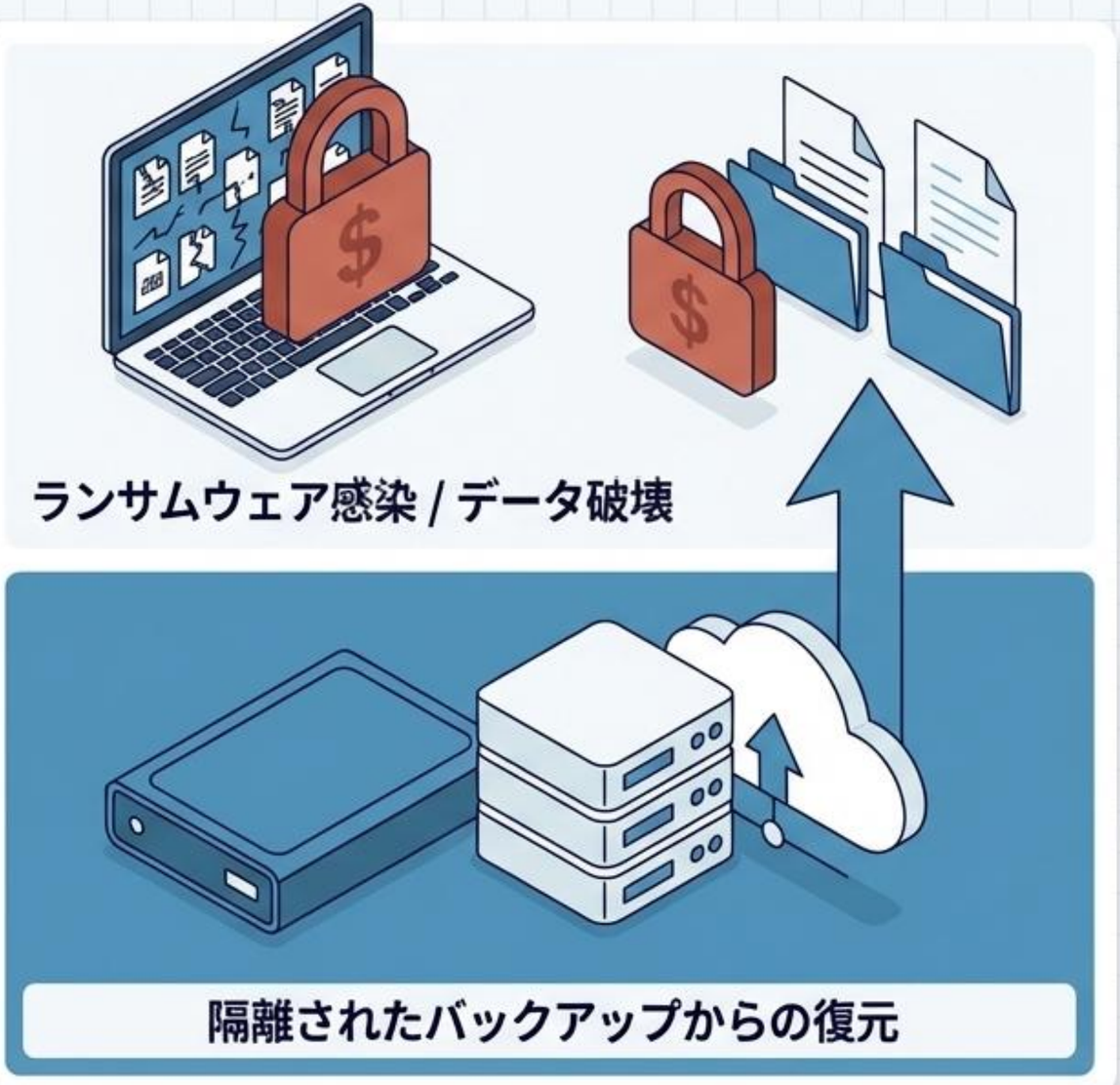
端末は「全情報が詰まった持ち歩く金庫」です。

端末は「全情報が詰まった持ち歩く金庫」です。離席時の置きっ放しや、他人に安易に貸し出す行為は厳禁です。生体認証やPINコードで必ずロックをかけましょう。

⚠ 【通知画面の罠】

ロックをかけていても、画面にメール本文や多要素認証のコードが表示される設定では、覗き見（ショルダーハッキング）だけで認証を突破される危険があります。

究極の復元力（バックアップ体制）



ランサムウェア（身代金要求型マルウェア）や天災によって重要データが破壊された場合、唯一確実な対抗手段は、安全な場所に隔離されたバックアップです。

OSやシステムの復旧と、データの復元は分けて考え、定期的に「正常な状態」を複製・保管しておくことが事業継続（BCP）の鍵となります。

個人の防衛から、組織の盾へ

サイバー攻撃の被害を最小限に抑えるためには、「隠さない」「1人で悩まない」、ことが鉄則です。
不審なメールを開いてしまった、端末を紛失したなどの問題を発見した際は、直ちに組織のルールに従って報告してください。

インシデント対応連絡網

個人情報保護管理者：＿＿＿＿＿＿＿＿

各部門責任者：＿＿＿＿＿＿＿＿

現場従業者が守るべきこと：＿＿＿＿＿＿

問題を発見した際の第一報告先：＿＿＿＿＿

各自の部署の連絡先を上記ダッシュボードに記入し、常に確認できる状態にしてください。

デジタル防衛ダッシュボード・チェックリスト

外壁

OS/ソフトのアップデート

関所

長く複雑なパスワード・使い回し禁止・多要素認証

衛兵

偽メールへの警戒・公式ストアの利用・権限の確認

金庫

画面ロックの徹底・バックアップ・迅速な報告と相談

サイバー空間は、誰もが参加する社会インフラです。システムに「攻撃できる穴」を作らない一人ひとりの行動が、社会全体のネットワークを安全に保ちます。
今日からこのダッシュボードの習慣を実践しましょう。

出典：内閣サイバーセキュリティセンター(NISC)「サイバーセキュリティ対策9か条」

202603