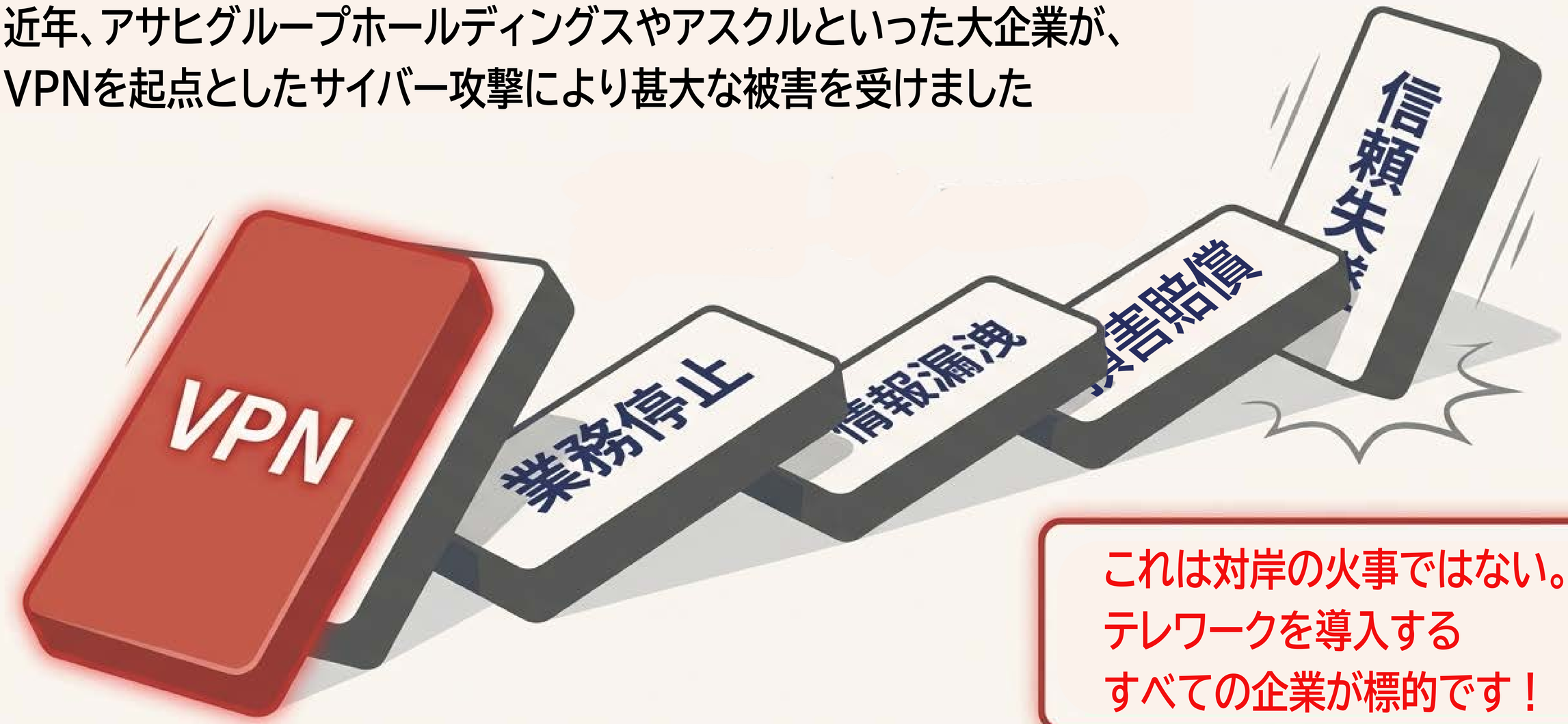
中小企業経営者のためのVPNサイバー攻撃対策ガイド

あなたの会社は「他人事」ではない。今、経営者が下すべき決断とは。

エフシーバンク
サイバーリスク対策の専門店

大手企業が陥った「VPN」という名の落とし穴

近年、アサヒグループホールディングスやアスクルといった大企業が、
VPNを起点としたサイバー攻撃により甚大な被害を受けました



これは対岸の火事ではない。
テレワークを導入する
すべての企業が標的です！

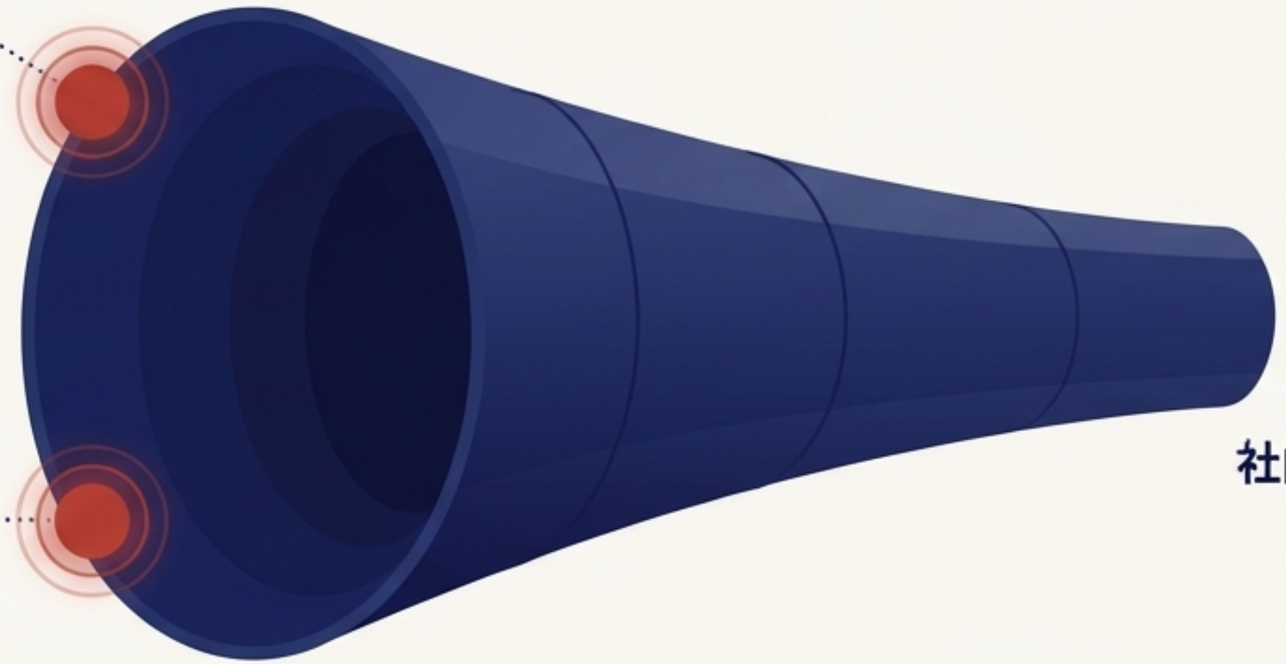
敵は「トンネルの入り口」を狙っている

① 脆弱性の悪用

古いソフトウェアに残された
「セキュリティの穴」からの侵入。

② 認証情報の悪用

流出したIDとパスワードで
「正規の社員」になりすます。



社内ネットワーク

経営判断として断行すべき「3つの防壁」

会社の情報資産を守るため、以下のIT投資・運用ルールを徹底することが急務です。
これは技術担当者任せにできない、経営マターです。

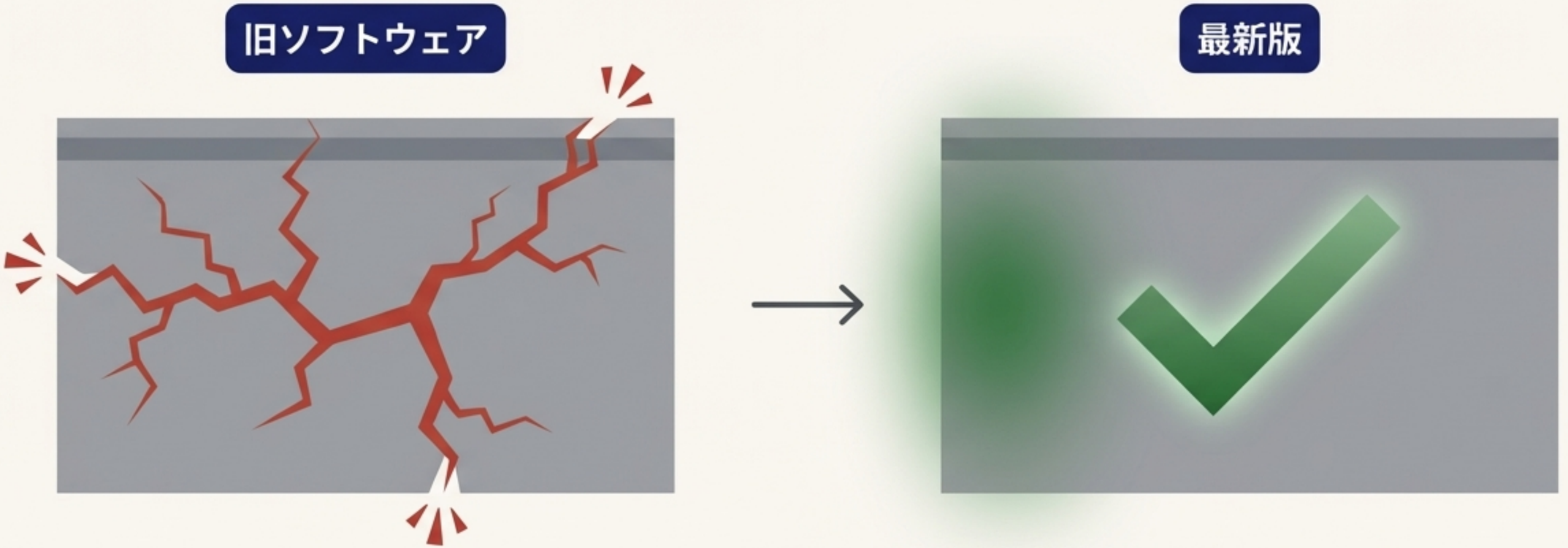
防壁①：アップデートの徹底

Action

VPN機器、PC、サーバーのソフトウェアを常に最新の状態に保つ。

Purpose

既知の「セキュリティの穴（脆弱性）」を完全に塞ぎ、攻撃者に侵入のきっかけを与えない。



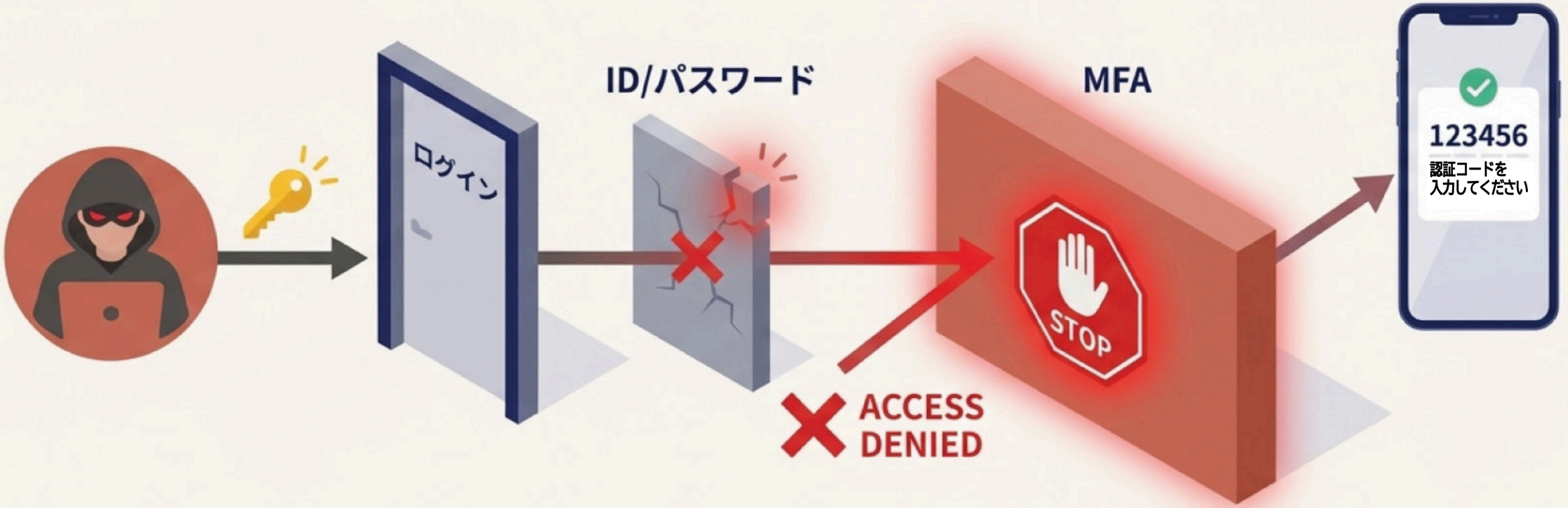
防壁②：多要素認証（MFA）の義務化

Action

IDとパスワードによるログインに加え、スマートフォンアプリやSMS等による追加認証を必須とする。

Purpose

万が一パスワードが漏洩しても、不正ログインを最終防衛ラインで阻止する。



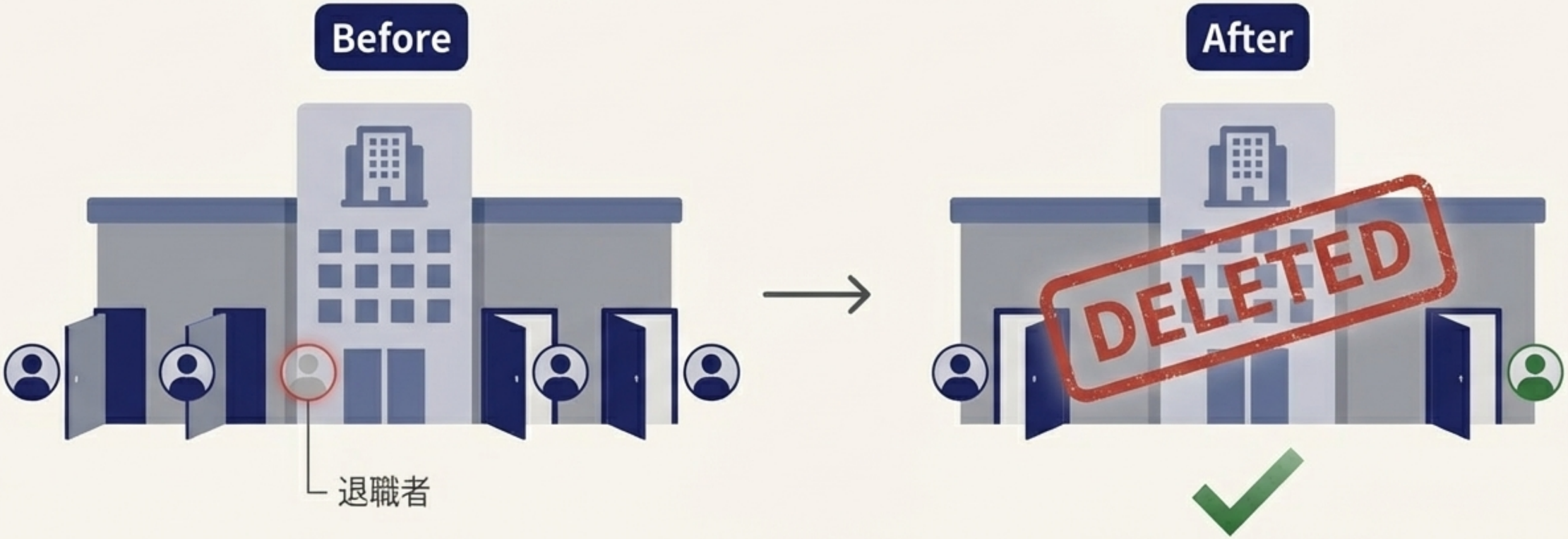
防壁③：権限の最小化と整理

Action

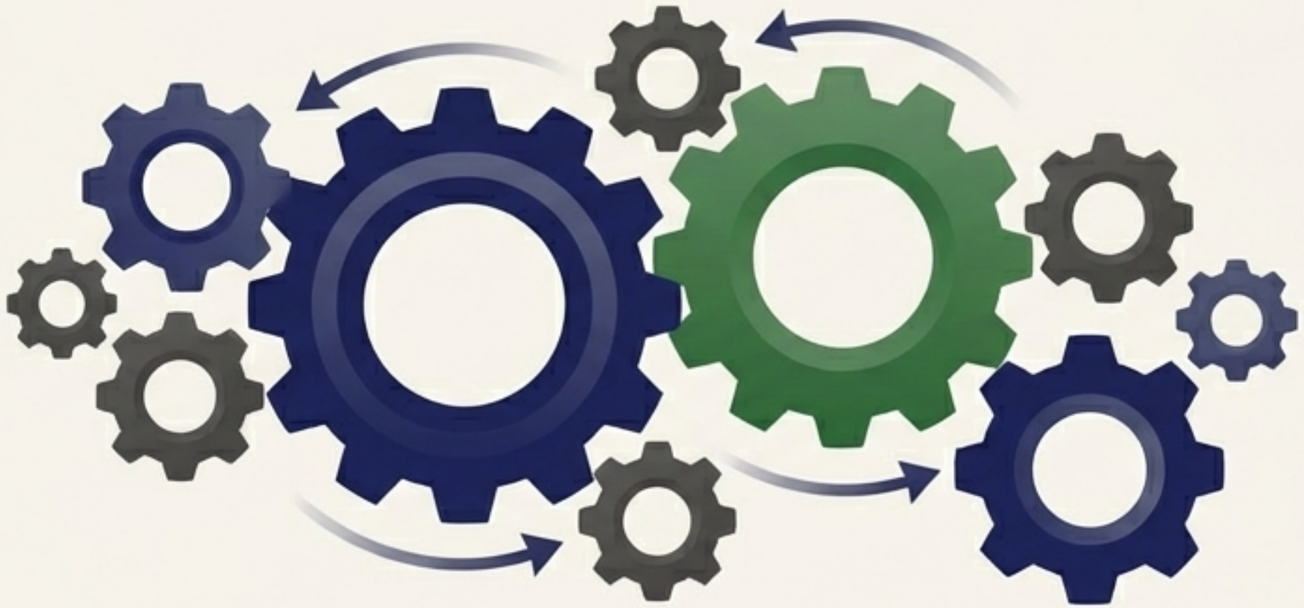
- **退職者アカウントの即時削除。**
- **社員のアクセス権を業務上最低限に絞る。**

Purpose

不要な「侵入口」を物理的に減らし、万が一侵入された際の被害範囲を限定する。



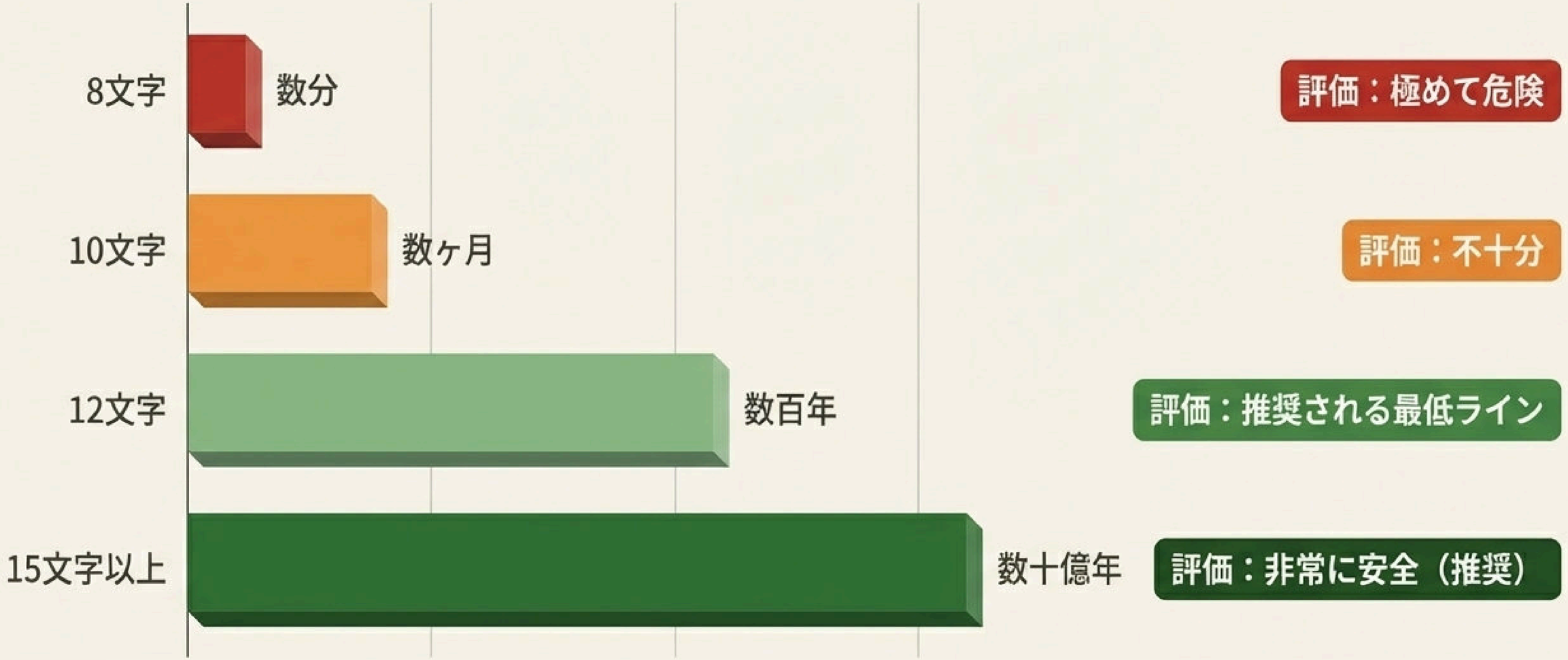
全社員で築く、会社の最終防衛ライン



最新の防御システムを導入しても、社員一人ひとりのセキュリティ意識が低ければ、
そこが弱点となります。
会社の安全は、全員の協力によって成り立ちます。

これから、全社員が明日から実践すべき「セキュリティ3ヶ条」を説明します。

パスワードの常識が変わる。「複雑さ」より「長さ」が重要。



※コンピュータによる総当たり攻撃での解析時間目安。ただしAIの発展によりどんどん短くなっています。

実践項目①：パスワードの「長文化」と「使い回し禁止」

Guideline 1

目指せ15文字以上

短く複雑なものより、覚えやすい単語を繋げた「パスフレーズ」を推奨します。

❌ 悪い例：`!P@ssw0rd!´

✔ 良い例：`blue-ocean-2026-coffee´（22文字）

人間には覚えやすく、コンピュータには解読が極めて困難です。

Guideline 2

公私混同は厳禁

SNSや個人のメール等で使っているパスワードを、
会社のシステムで使い回さないでください。

実践項目②：「身に覚えのない通知」は攻撃のサイン

- ログインしようとすると、あなたのスマートフォンに通知が届きます。
- あなたがログイン操作をしていない時に通知が届いた場合、それは第三者が不正ログインを試みている証拠です。

ためらわずに「拒否」を押し、すぐにシステム担当者へ報告してください。

実践項目③：「少しの違和感」を見逃さない

不審なメール

知り合いからのメールでも、添付ファイルやURLが不自然に感じたら、開かずにまず相談してください。

PCの異常

「動作が急に重くなった」「見慣れない画面が出る」といった小さな変化は、攻撃のサインかもしれません。迷わず報告してください。

あなたの「違和感」が、会社を救う最初のきっかけになります。

本日のまとめ：会社を守るための2つのアクションリスト

経営者が直ちに行うこと

- [ ] **アップデートの徹底**：VPN機器とPCを常に最新の状態に保つ。
- [ ] **多要素認証の義務化**：不正ログインを防ぐ最後の砦を導入する。
- [ ] **権限の整理**：退職者アカウントを削除し、アクセス権を最小化する。

全社員が明日から実践すること

- [ ] **パスワードの長文化**：15文字以上のパスフレーズを設定し、使い回さない。
- [ ] **不審なMFA通知への対応**：身に覚えのない通知は即**「拒否」**し、**報告**する。
- [ ] **「違和感」の報告**：不審なメールやPCの異常を放置しない。

セキュリティは一過性のイベントではなく、継続的な文化です。

全員が当事者意識を持つことで、はじめて会社は安全になります。
今日から、意識を変え、行動を変えましょう。

ご不明な点、不審な点があれば、すぐにシステム担当部署に相談してください。