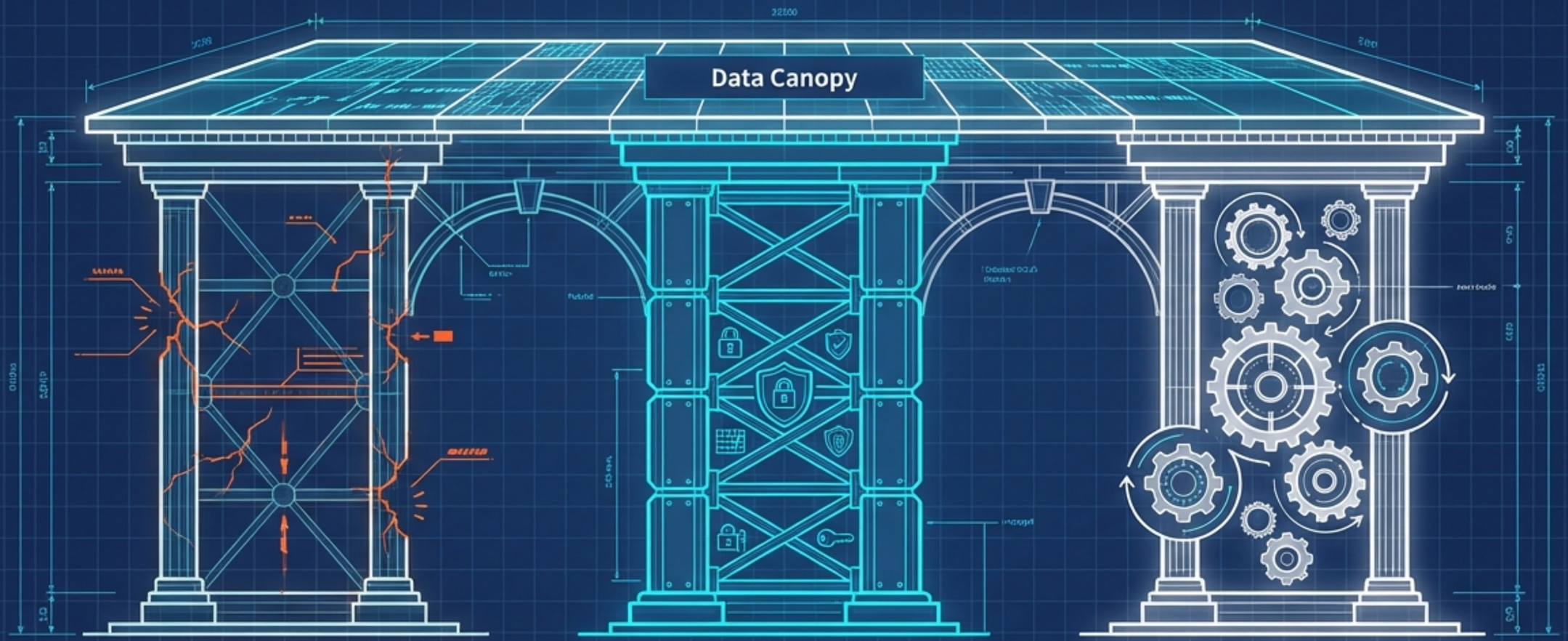
情報セキュリティの全体像

脅威の解剖から防御・管理のアーキテクチャまで

情報セキュリティの3本柱



脅威（インベーダー）

コンピュータウイルスと不正アクセスの実態と被害効果

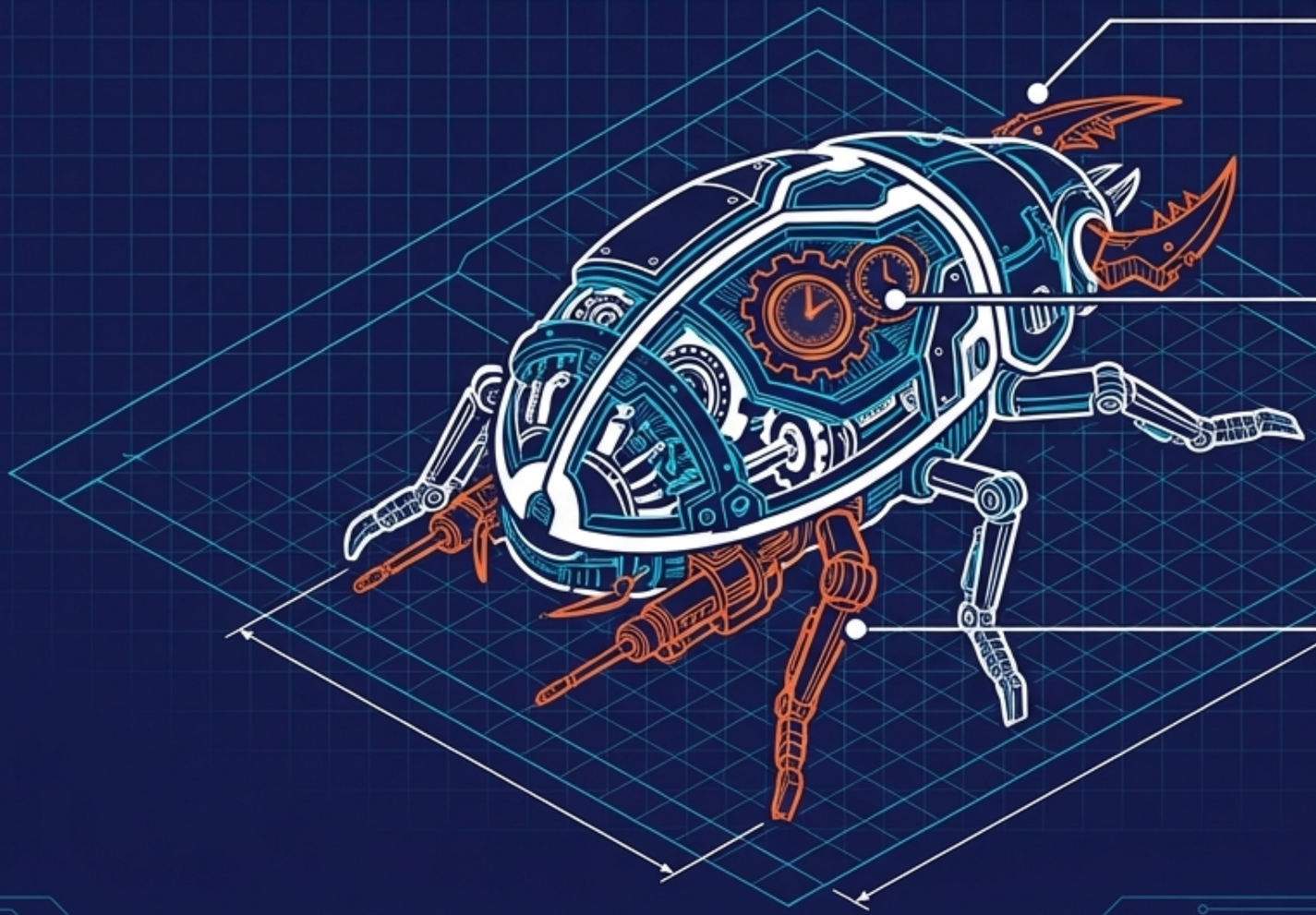
防御（要塞）

パスワード、ファイアウォール、暗号化、電子署名による技術的保護

管理（ガバナンス）

CIAを維持し、リスクを統制するマネジメントとPDCAサイクル

経済産業省告示によるコンピュータウイルスの定義（3つの機能のうち1つ以上を有するもの）



1 **自己伝染機能**

他のプログラムやシステムに自らをコピーし伝染する。

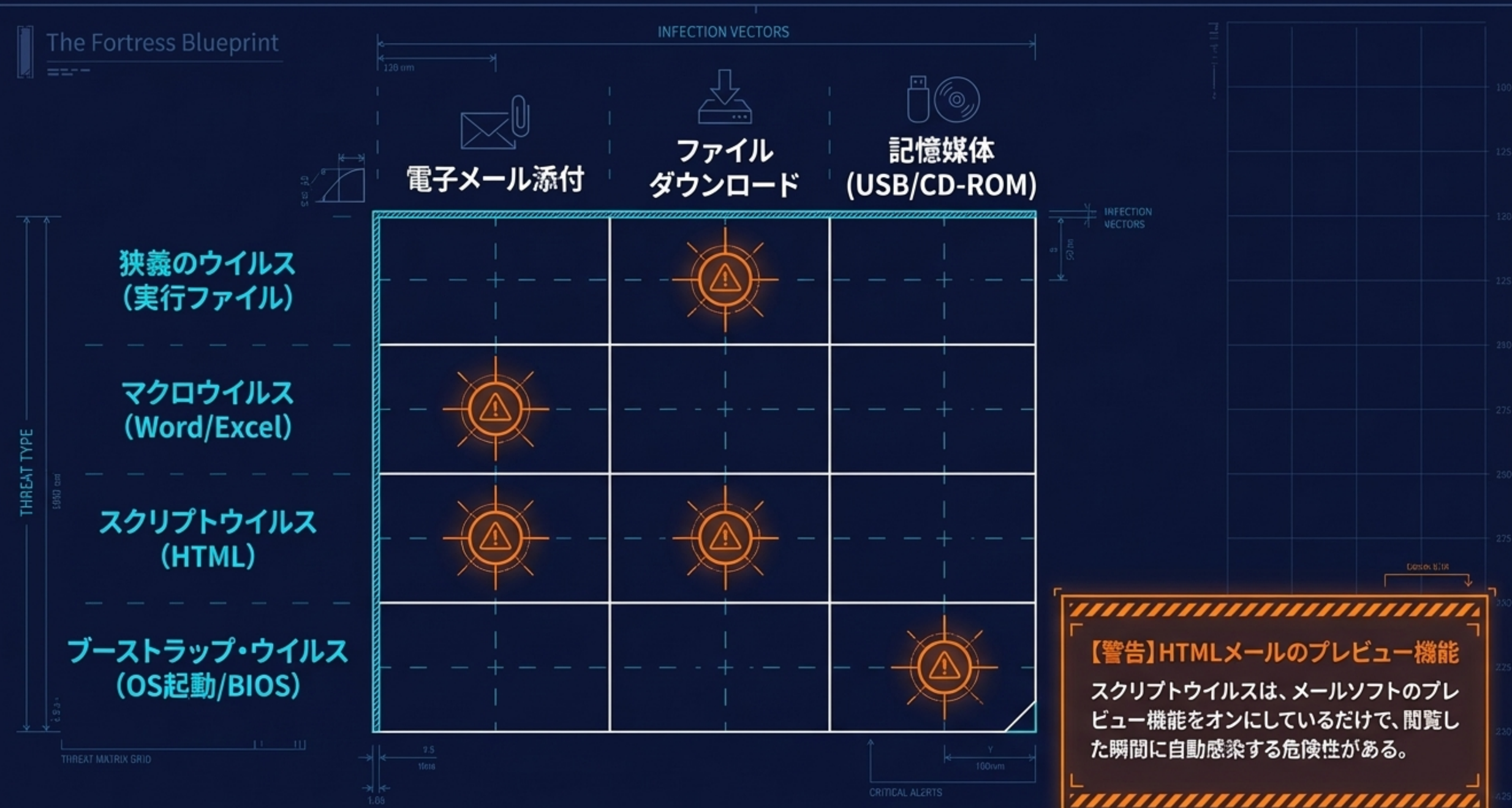
2 **潜伏機能**

特定時刻、一定時間、処理回数などの条件を満たすまで症状を隠す。

1 **発病機能**

ファイルの破壊や、設計者の意図しない異常動作を引き起こす。

The Fortress Blueprint



【警告】HTMLメールのプレビュー機能

スクリプトウイルスは、メールソフトのプレビュー機能をオンにしているだけで、閲覧した瞬間に自動感染する危険性がある。

ウイルス発見時の緊急対応フロー

発見者（利用者）

ネットワークから切り離す
（独断での解決は厳禁）

速やかにシステム管理者に
電話し、指示を仰ぐ

システム管理者

影響範囲の調査（伝染の有無）

関係者全員への対処指示

対象PCからのウイルス除去

IPA（情報処理推進機構）への
ウイルス感染届出

連鎖的被害の発生メカニズム

不正アクセス禁止法に基づく
「なりすまし」や
「許可外アクセス」

データの漏洩・改ざん

個人情報保護法違反に直結。
顧客や取引先への甚大な損害。

ウイルスの伝播

社内サーバーを介して外部へ
ウイルスを拡散する加害者へ転落。

DoS攻撃の踏み台

トロイの木馬やボットを仕掛けられ、
第三者のシステムを麻痺させる
大量データ送信の「踏み台」にされる。

IMPACT SEVERITY

THREAT AMPLIFICATION

第一の防壁：アクセス制御と本人認証

パスワードの脆弱性と適切な管理

【不適切】

辞書にある単語、短い文字列、
名前や生年月日。

【適切】

無意味な文字列、8文字以上、
英数字・特殊記号の混在。
定期的な変更と「記憶させない」運用。

強固な部分対策

バイオメトリクス認証

指紋、手形、網膜など、
身体の一部を用いた厳重な
本人認証。

ワンタイムパスワード

アクセスのたびに毎回変更
される使い捨ての仕組み。

コールバック

外部接続時、サーバーから登録済みの電話番号へかけ直すこと
で、場所のなりすましを防止。

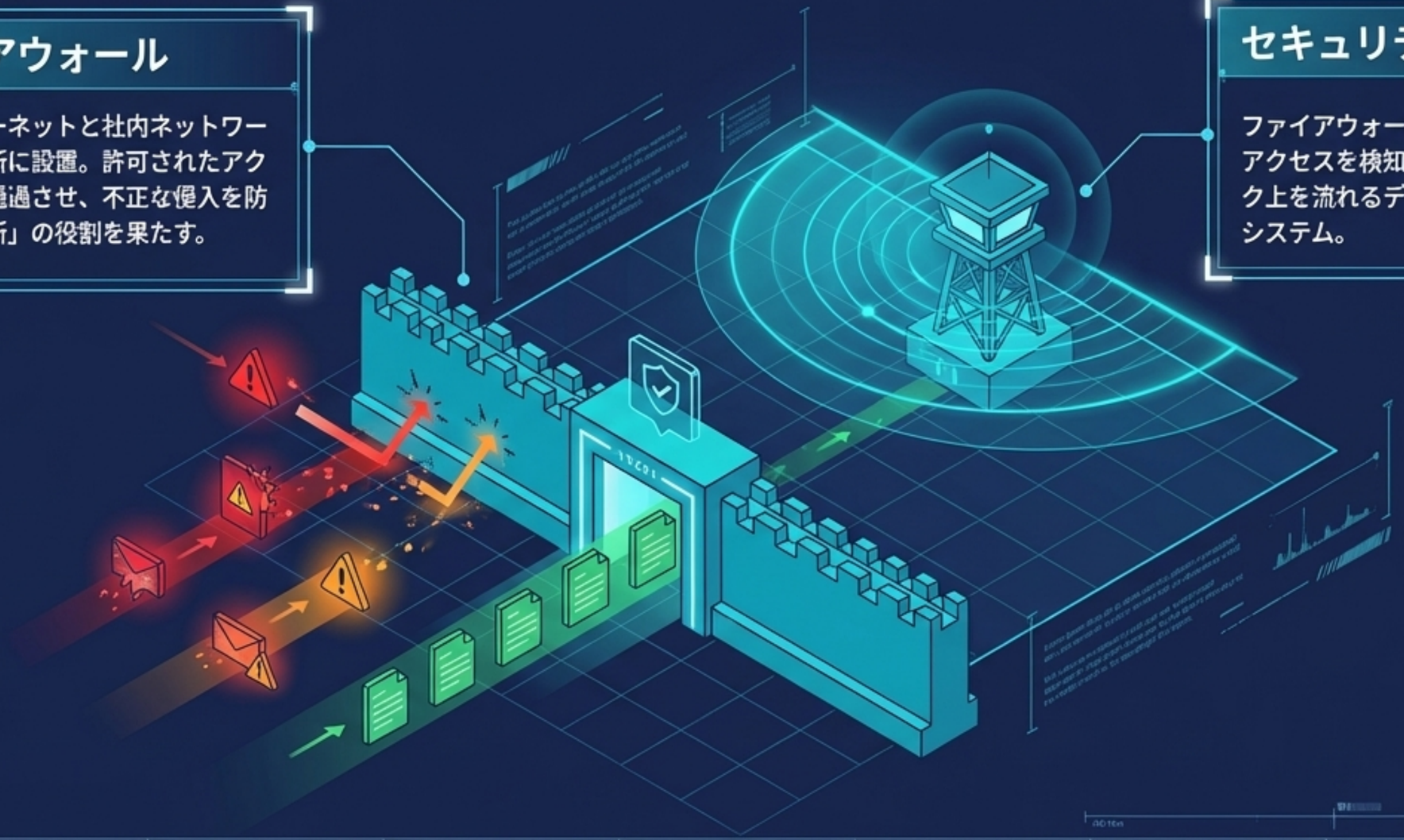
ネットワーク防衛網：境界の関所と内部の監視

ファイアウォール

外部インターネットと社内ネットワークの接続箇所に設置。許可されたアクセスのみを通過させ、不正な侵入を防止する「関所」の役割を果たす。

セキュリティ監視

ファイアウォールを潜り抜けてきたアクセスを検知するため、ネットワーク上を流れるデータを常時監視するシステム。

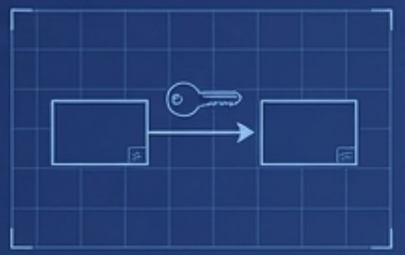


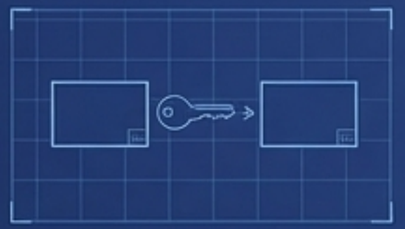
暗号方式の比較マトリクス

秘密鍵暗号方式 (共通鍵 - DES)

処理速度

鍵管理の容易さ



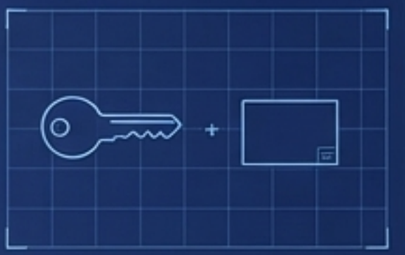


- 仕組み：暗号化と復号に「同じ鍵」を使う。
- 長所：処理速度が速い。
- 短所：鍵を相手に安全に渡すのが困難（盗聴リスク）。相手が増えると鍵の管理が破綻する。

公開鍵暗号方式 (RSA)

処理速度

鍵管理の容易さ



- 仕組み：暗号化には「公開鍵」、復号には「秘密鍵」を使う。
- 長所：暗号化鍵を公開できるため、不特定多数との通信でも鍵管理が容易で安全。
- 短所：計算が複雑で処理に時間がかかる。

公開鍵による安全な配送

送信者Aは受信者Bの「公開鍵」で暗号化する。このデータは、Bが持つ「秘密鍵」でしか復号できない。

セション鍵暗号方式：

ハイブリッドの最適解

公開鍵の「遅さ」を克服する実際の標準方式。通信のたびに使い捨ての共通鍵（セション鍵）を作成し、それを公開鍵で暗号化して相手に送付。実際の長文データは高速な共通鍵で暗号化する。

なりすましと否認を防ぐ「電子の印鑑」

実社会の証明

デジタル世界の証明

電子署名（実印の押印）：送信者Aの「秘密鍵」で認証番号を暗号化。Aしか使えない鍵であるため、本人証明となる。

認証（印鑑証明）：認証局（CA）が受信者Bに対して証明書を発行。公開鍵で復号できたという事実と共に、実印の正当性を担保する。

⚠ 【電子署名法】実社会の実印と同等の法的効力を持つことが定められている。

セキュリティマネジメントの基礎：情報セキュリティの3要件（CIA）

機密性 - Confidentiality

許可された者だけが情報にアクセスできること。

❗ (※パスワード、暗号化がここに寄与)

完全性 - Integrity

情報や処理方法が正確で、改ざんや破壊から保護されていること。

❗ (※電子署名がここに寄与)

可用性 - Availability

許可された利用者が、必要な時に確実に情報へアクセスできること。

❗ (※ファイアウォール、DDoS対策がここに寄与)

リスクマネジメントの構造：脅威と脆弱性の算定

リスクの大きさ = 発生確率 × 被害の額

インシデントとリスクの構造

脅威 (Threat)
災害、故障、故意の攻撃など。排除することは極めて困難。

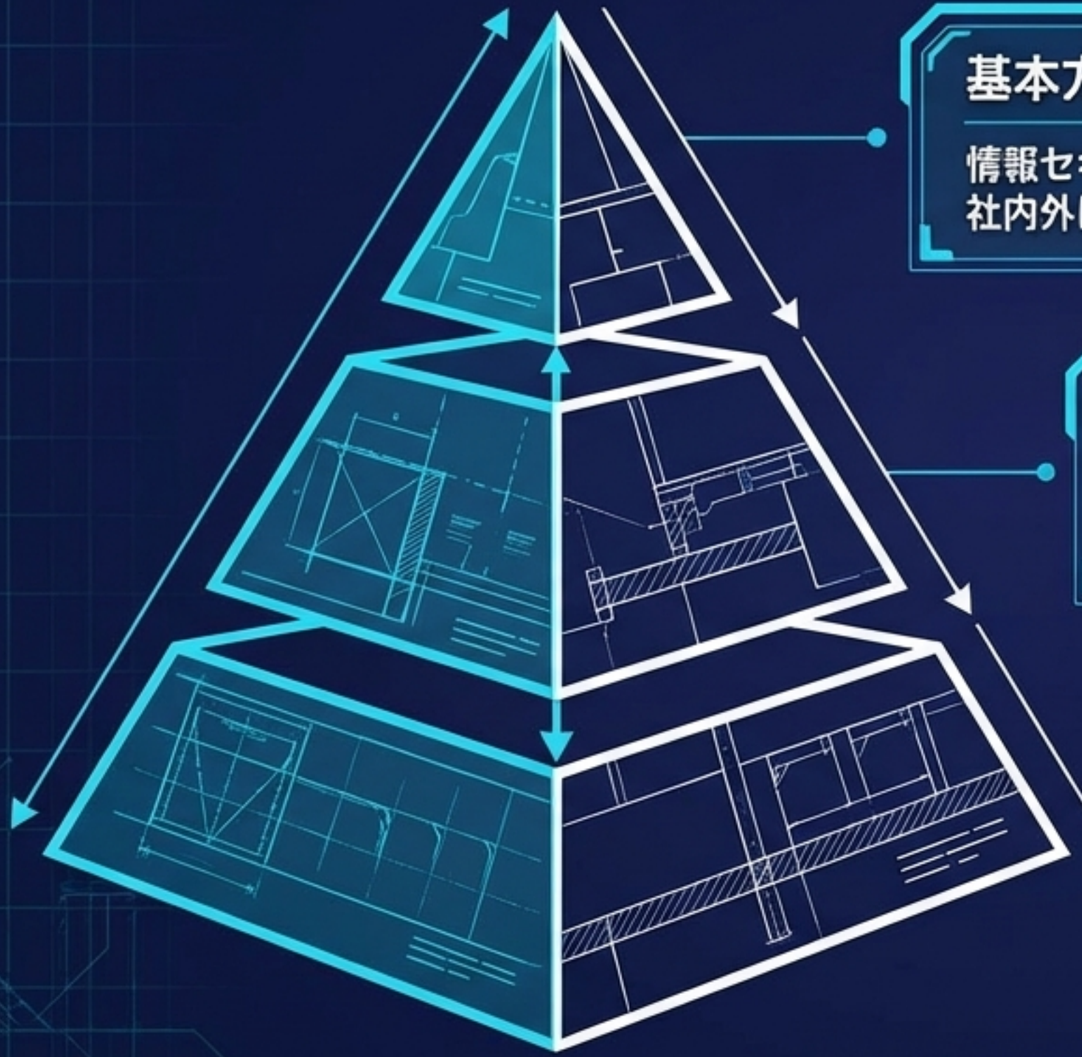
脆弱性 (Vulnerability)
システムにおけるCIAの欠如。

対策の本質
脅威そのものは消せない。したがって、システムの「脆弱性」を減らすことで、リスクの大きさをコントロールする。

個人情報保護法のリスク

過去6ヶ月以内で5000人を超える個人データを扱う事業者は「個人情報取扱事業者」として厳格な保護義務を負う（漏洩時の被害額が甚大化するため）。

セキュリティポリシーの階層構造



基本方針（狭義のポリシー）- 経営者

情報セキュリティに対する目標と、企業が取るべき行動を社内外に宣言するトップの意志。

対策基準（ガイドライン）- 各部門長

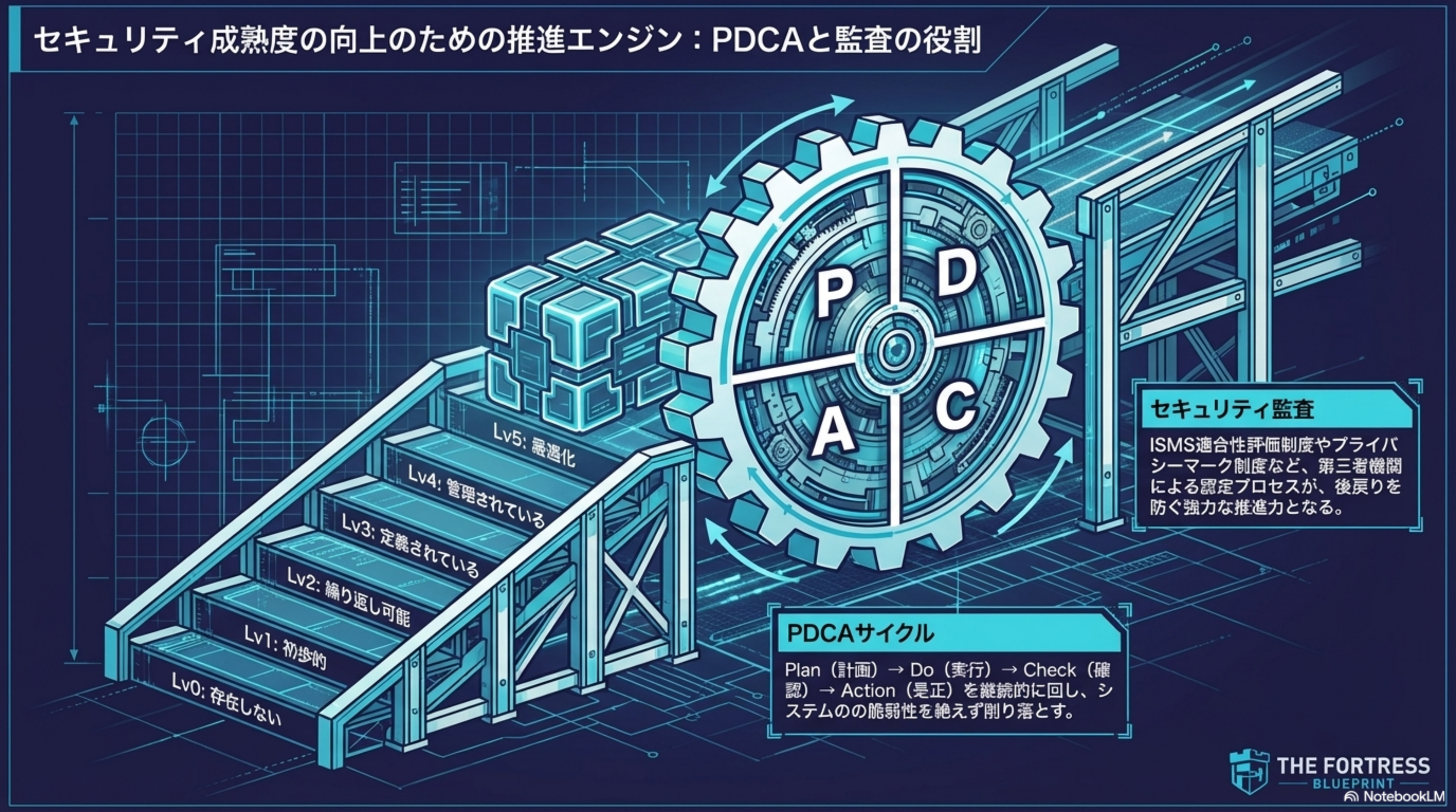
リスクと重要性を比較し、遵守すべき活動基準を明文化。「パスワードを秘守しなければならない」などの規定。

実施基準（マニュアル）- 現場担当者

現場の実施手順。「パスワードは8文字以上で、特殊文字を2文字以上入れること」など、極めて具体的なルール設定。

THE FORTRESS BLUEPRINT

セキュリティ成熟度の向上のための推進エンジン：PDCAと監査の役割



セキュリティ監査

ISMS適合性評価制度やプライバシーマーク制度など、第三者機関による認定プロセスが、後戻りを防ぐ強力な推進力となる。

PDCAサイクル

Plan（計画）→ Do（実行）→ Check（確認）→ Action（是正）を継続的に回し、システムのの脆弱性を絶えず削り落とす。

THE FORTRESS BLUEPRINT