デジタル時代の要塞を築く：セキュリティとプライバシーの設計図

抽象的な原則から具体的な防御策まで、私たちのデジタル世界を守るための知識の探求。

なぜ今、デジタルセキュリティを学ぶのか？

学習到達目標

1. デジタルセキュリティの基本原則（暗号化、アクセス制御等）を理解し説明できる。
2. プライバシーの重要性を認識し、その保護手法（インフォームドコンセント、匿名化等）を説明できる。
3. デジタルセキュリティとプライバシーの関連性を理解し説明できる。

キータームの定義

デジタルセキュリティ：コンピュータシステム、ネットワーク、データを保護し、機密性、完全性、可用性を確保する取り組み。

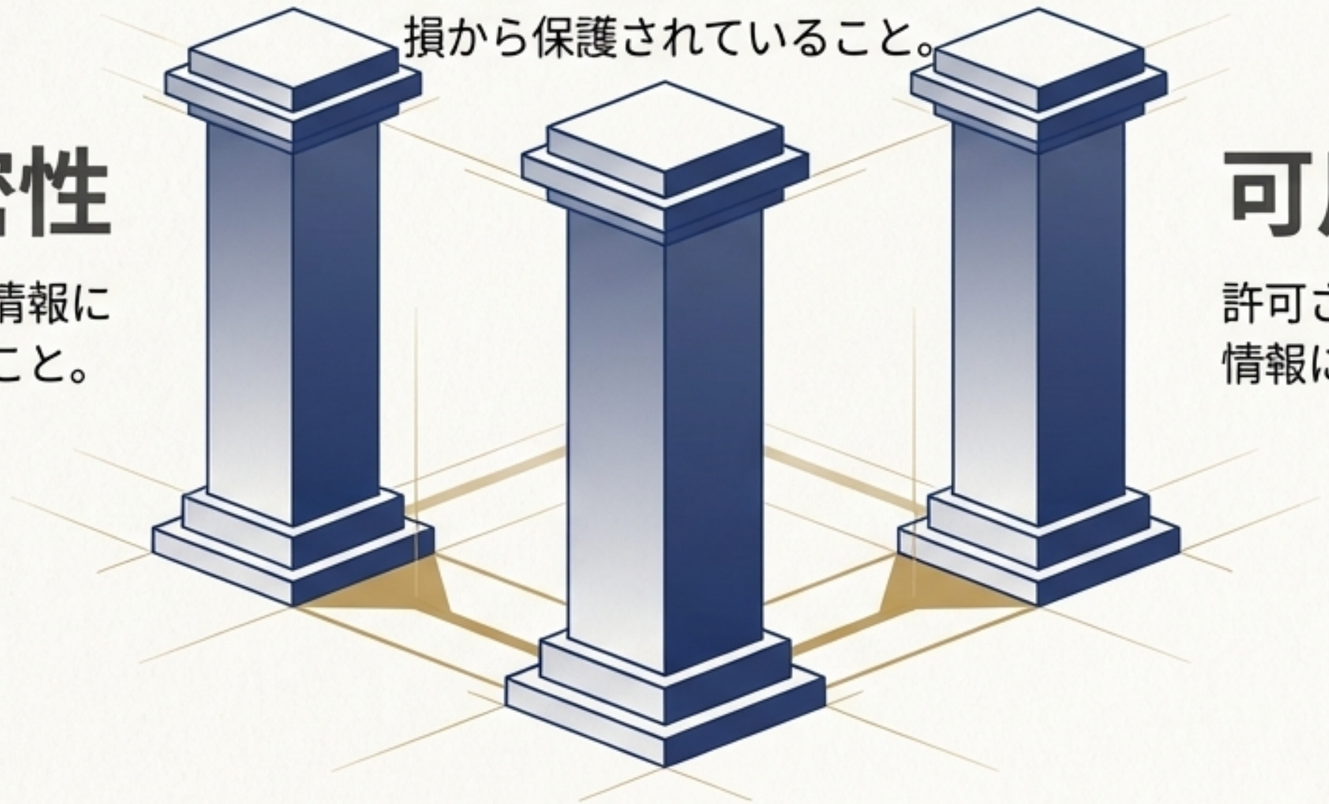
サイバーセキュリティ：データ漏洩や不正な活動からの防御に重点を置いた概念（サイバーセキュリティ基本法第２条による定義）。

情報セキュリティ：サイバー空間と現実空間の両方を含む、より広範な概念。情報の機密性、完全性、可用性を維持すること。

要塞の礎：情報セキュリティの3つの柱

完全性

情報が正確であり、改ざんや破損から保護されていること。



機密性

許可された者だけが情報にアクセスできること。

可用性

許可された者が、必要な時に情報にアクセスできること。

第一の柱「機密性」：許可なき者の侵入を許さない

認可されていない者（人、システム、アプリ）に情報を使用させないこと。
許可された者だけが、許可された方法で情報にアクセスできる状態を確保する。

実現する仕組み

認証（Authentication）：システムにアクセスするユーザーやデバイスの身元を確認するプロセス。

アクセス制御 (Access Control)：認証されたユーザーに対し、許可された範囲内でででのみアクセスを許す仕組み。

具体例

学校のネットワークやサーバーにアクセスできる人間を限定する。
教師用端末には教員以外がログインできないようにする。

要塞の門：本人認証の3つの鍵

物理認証

具体例: 物理鍵、印鑑、ICカード

メリット: 簡便で安全

デメリット: 貸し借り・紛失・盗難・複製の恐れ、管理が煩雑

知識認証

具体例: パスワード、暗証番号

メリット: 導入が容易、無くさない

デメリット: 推定やクラッキングの可能性、本人が忘れる

生体認証

具体例: 指紋、声紋、虹彩、静脈、顔、歩容

メリット: 本人以外を認証する可能性が極めて低い

デメリット: 導入コストが高い、体調の変化で誤認の恐れ

補足：知識認証の弱点を補う「多要素認証」の重要性を強調。

第二の柱「完全性」：情報が改ざんされていないことの保証

情報が正確であり、意図しない書き換え（改ざん）や破損から保護されている状態を維持すること。

主要技術：デジタル署名

公開鍵暗号方式を使用し、電子文書やデータの真正性と整合性を保証する技術。

3つの役割

1. 真正性の確認

文書が特定の送信者から送られたことを確認。

2. 整合性の保証

送信後に改ざんされていないことを保証。

3. 否認防止

送信者が「送っていない」と否認することを防ぐ。

第三の柱「可用性」：必要な時にいつでも情報を使える状態

許可された利用者が、必要な時に情報にアクセスできることを確実にすること。情報が使えなければ意味がない。

可用性を損なう要因

システムの故障、停電、災害、ランサムウェア(Ransomware)によるファイルの暗号化など。

> ランサムウェアの定義：感染したPCをロックしたりファイルを暗号化したりして使用不能にし、元に戻すことと引き換えに「身代金」を要求する不正プログラム。

担保する方策

システムの多重化・クラウド化

定期的なバックアップの作成と別場所での保管

我々の情報資産を脅かすものは何か？

自然災害

地震、水害、火災、停電など。発生頻度は低いが影響は甚大。

機器の障害

ハードウェアやネットワークの故障。

人間の故意

ウイルス、不正アクセス、盗難。

人間の過失

誤操作、紛失、誤配送。
情報漏洩のトラブルでは、これが大多数を占める。

「リスクを完全に無くすことは困難。
故に、インシデント発生時の対応を事前に検討しておくことが重要となる。」

リスクの解剖学：脅威は脆弱性を突いて資産を狙う

リスク (Risk) ＝ 情報資産 (Info Assets) × 脅威 (Threats) × 脆弱性 (Vulnerabilities)

情報資産 (Information Assets)

組織にとって価値のある情報やシステム。

区分	例
情報	データベースやデータファイル、契約書・同意書、システム関連文書、調査情報、利用者マニュアル、訓練資料、運用手順・サポート手順書、事業継続計画、代替手段の取り決めめ、取り決め、監査証跡、保存情報
ソフトウェア	業務用ソフト、システムソフト、開発用ツール、ユーティリティソフト
物理的資産	コンピュータ装置、通信装置、取り外し可能な媒体、その他の装置
サービス	計算処理サービス、通信サービス、一般ユーティリティ（例えば、暖房、照明、電源、空調）
その他	人、保有する資格・経験、無形資産（例えば、組織の評判・イメージ）

脅威 (Threats)

資産に損害をもたらす事象の潜在的原因。

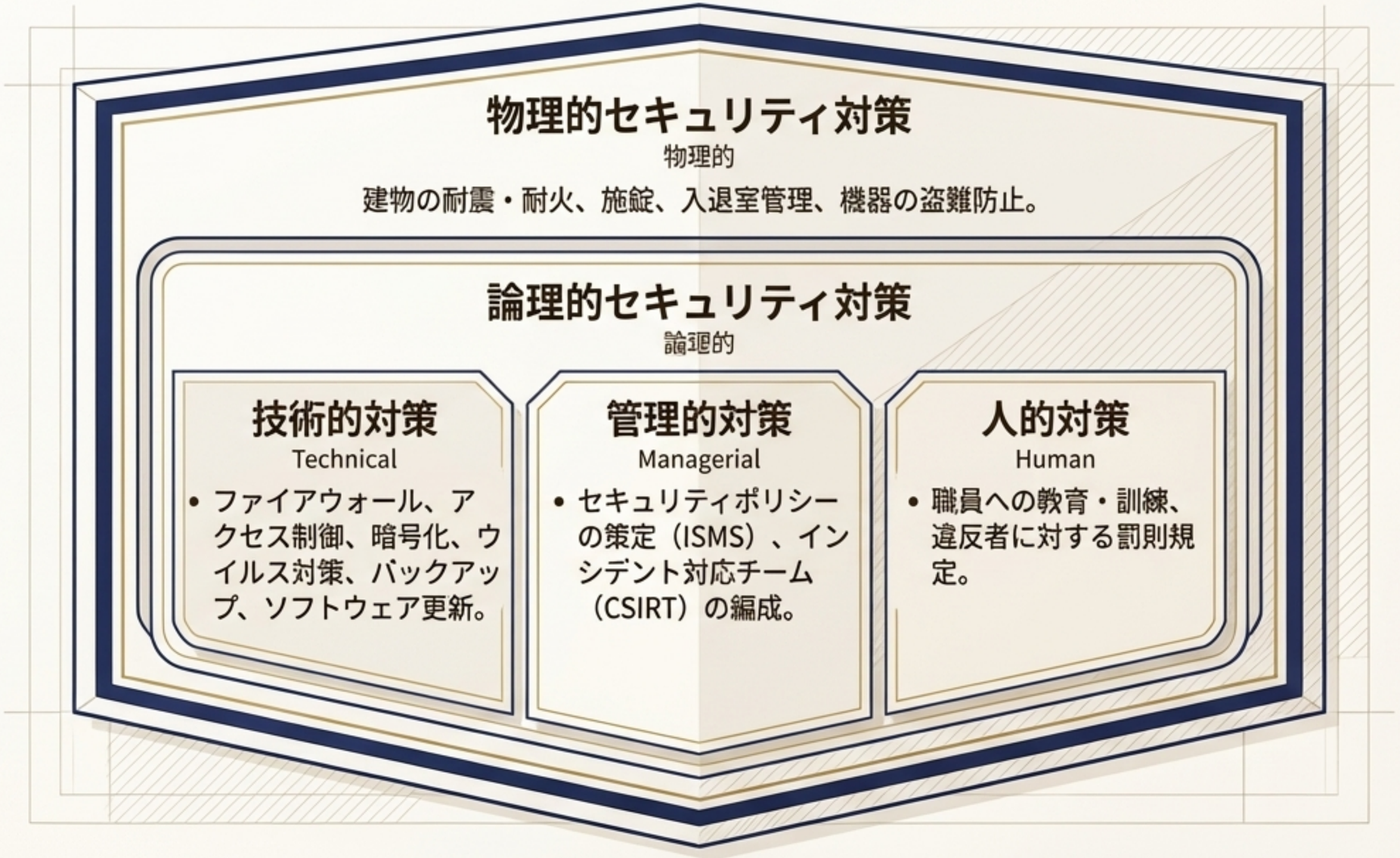
大区分	区分	例
人為的脅威	意図的脅威	コンピュータウィルス、不正侵入、改ざん、盗難 など
	偶発的脅威	人為的ミス、誤動作、故障 など
環境的脅威	－	地震、停電、火災、洪水、静電気 など

脆弱性 (Vulnerabilities)

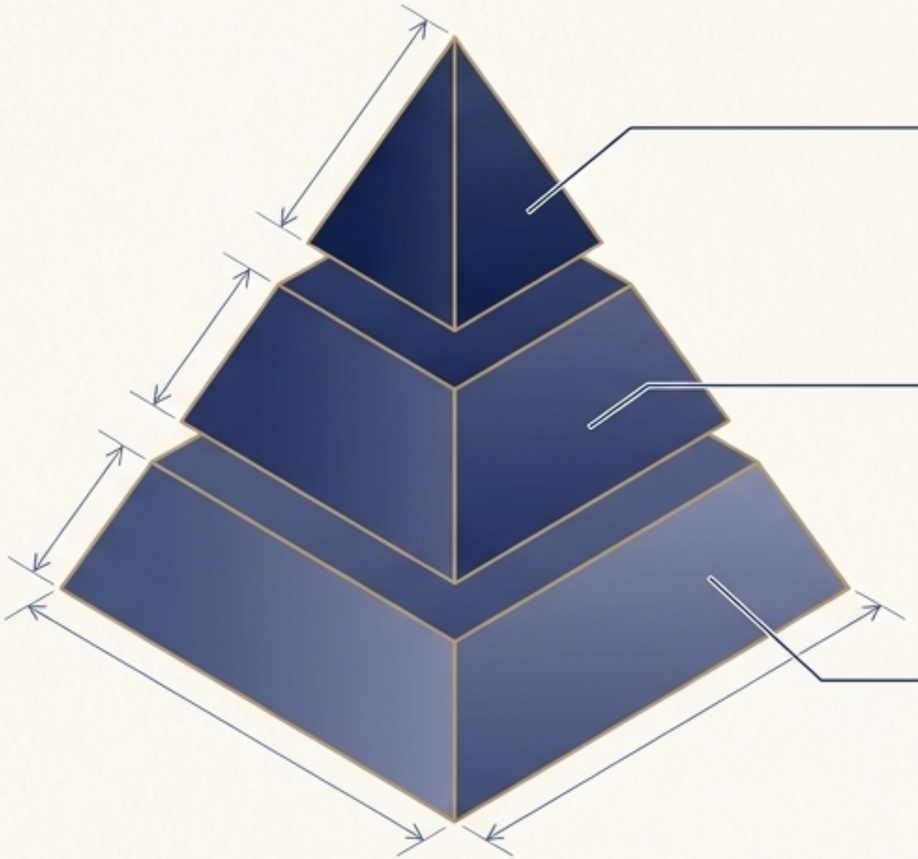
脅威の発生を誘引する原因。

分類	脆弱性の例	関連する脅威
環境、設備	自由に出入りできる事務所	盗難、不正アクセス
ソフトウェア	アクセス制限のないパソコン	不正アクセス、なりすまし、改ざん
ハードウェア	老朽化したファイルサーバ	故障（データ破壊）
人	不注意	盗難、置き忘れ、情報漏えい

要塞の防衛戦略：4つのセキュリティ対策



城塞の掟：情報セキュリティポリシーの構造



基本方針
(Basic Policy)

組織の情報セキュリティに対する基本方針・宣言。

対策基準
(Countermeasure Standards)

基本方針を実現するための具体的な規則。

実施手順・運用規則
(Implementation Procedures)

対象者や用途に応じた必要な手続きを明確にした手順。

文部科学省が学校設置者に対し「教育情報セキュリティポリシー」の策定を求めていることに言及。

第三部：要塞が守るべき宝——プライバシーという権利

強固なセキュリティ対策は、それ自体が目的ではない。それは、私たちの最も重要なデジタル資産である「プライバシー」を守るための不可欠な手段である。

プライバシーと個人情報の定義

プライバシーとは？

概念：個人が自分に関する情報をコントロールする権利。他者から干渉・侵害を受けない権利。

憲法上の根拠：日本国憲法第13条（個人の尊重、幸福追求権）が根拠とされる。

個人情報とは？ [個人情報保護法 第2条]

定義：生存する個人に関する情報で、氏名、生年月日などにより特定の個人を識別できるもの。
最近の情報 OKに拡張：

- **個人識別符号**：マイナンバー、運転免許番号、顔・指紋認識データ等。
- **要配慮個人情報**：人種、信条、病歴、犯罪の経歴等。取得には本人同意が必須。

インフォームドコンセント（Informed Consent）：本人に情報の収集・利用目的を十分に提供し、その同意を得ることで自己情報コントロール権を保護する手法。

セキュリティはプライバシーの礎である

セキュリティが確保されていなければ、不正アクセス等のリスクが高まり、個人情報やプライバシーが侵害される。
十分なセキュリティ対策の実施が、プライバシー保護を強化する。

現代における重要性

IoT時代では、あらゆる機器がオンラインに繋がり、意識しないうちに行動履歴や位置情報が収集・蓄積されている。
金融情報や診療情報など、価値の高い情報がオンラインで扱われる今、これらを狙うサイバー攻撃も増加している。

デジタルセキュリティの原則を理解し実践することは、技術的な課題であるだけでなく、デジタル社会における個人の尊厳と権利を守るための倫理的な責務である。