Wisecurecech
ワイセキュア株式会社

データ保護と暗号化

現在、多くの企業がランサムウェア攻撃を受けています。億単位の被害と顧客の信頼損失を経験した事例もあります。
システムが侵入されても、暗号化されたデータは読み取れません。内容漏洩のリスクを大幅に下げるため、重要なデータには「暗号化」が必須です。

攻撃後の対策は遅すぎる現実

241日

攻撃を受けた企業が侵入事件の全容を理解することまでかかる平均時間。（IBM の 2023 年のレポートによる）

98%

第三者のサプライチェーンに依存する企業中、少なくとも 1 回のデータ漏洩を経験している企業数
（SecurityScorecard の 2024 のレポートによる）

82%

複数の環境に保存されたデータと関係した侵害の割合
（IBM の 2023 年のレポートによる）

研究によると、悪意のある侵入を発見されるまでには長い期間がかかることが多いです。
その間、攻撃者は最も価値の高いデータを標的にし、盗み取る可能性があります。

データが流出しても、内容を漏洩させないための対策として「暗号化」 が有効です。

「暗号化」とは、データ漏洩防止の保護において最も効果的な手段です。

暗号化するメリット
- データを盗まれても、内容を読み取ることができない
- ランサムウェア攻撃のリスクを低減する
- コンプライアンス遵守と責任リスク管理の強化

万が一、システムが攻撃を受けた場合でも、暗号化が適切に行われていることを証明できれば、法律上の責任リスクを大幅に軽減することが可能です。

大切なものは必ず金庫の中に保管するように、
検知や身元認証だけでは機密データの保護には不十分です。
最も重要なデジタル資産は、「暗号化技術」によって守るべきです。

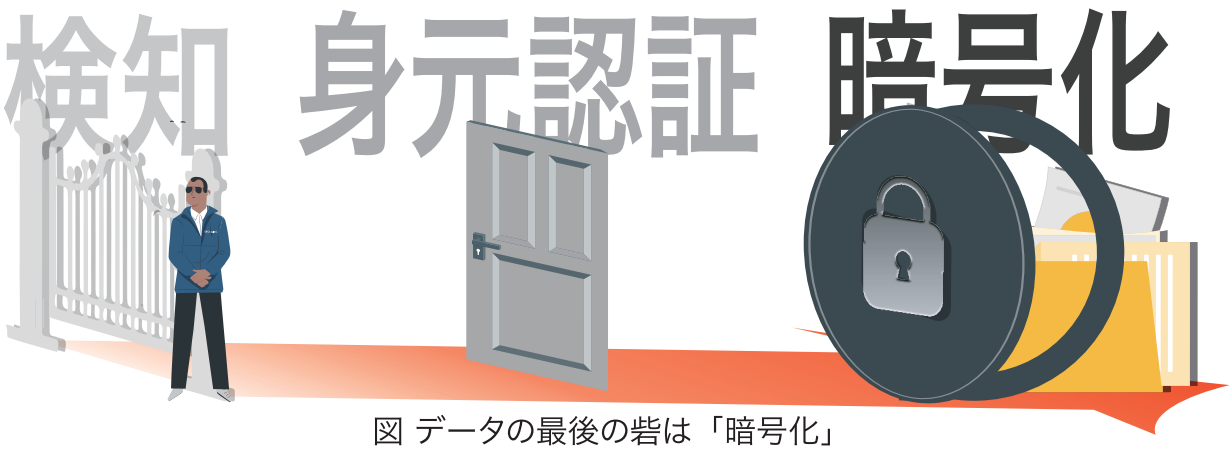

図 データの最後の砦は「暗号化」

暗号化における課題：貴社の暗号化は本当に安全ですか？

暗号化の安全性を確保するためには、暗号アルゴリズムの強度だけではなく、暗号鍵の品質、ライフサイクル管理、そして鍵の保護方法もしっかりと考慮する必要があります。
特に、多くのクラウドサービスでは、システム全体が一つの暗号鍵で守られていることが一般的です。この鍵が漏洩した場合、暗号化の効果が失われ、暗号化されていることに安心してしまい、データの漏洩に気づかない危険性もあります。

WiSECUREは信頼できる暗号化ソリューションを提供

Google Workspace

1. Google Workspace CSE（Client-Side Encryption）
組織内のコミュニケーションやデータ共有を暗号化することで、セキュリティを強化しながら、業務効率を損なうことなく安全に保ちます。スマートな暗号化セキュリティ対策として、ビジネスにおける情報保護を確実にサポートします。

Data Isolation

2. 企業向けデータ隔離戦略
システムには最低限の変更を加えるだけで、データをエンドポイントから隔離し、漏えいや不正アクセスを未然に防ぎます。企業や組織の重要な情報を確実に保護します。

3. PGP 暗号化を搭載したハードウェア USB—PPAP 代替案
企業版と個人版があり、複雑な操作は不要。PC 内の重要なファイルを誰でも手軽に暗号化でき、高いセキュリティを保ちながら日常の業務にストレスなく導入できるセキュアなファイル交換ツールです。

ワイセキュア株式会社　WiSECURE Inc.
埼玉県川口市金山町12-1 サウスゲートタワー川口2階 Mio川口
048-400-3057　https://wisecure-tech.jp
お問合せ担当者：Rose Lin　rose@wisecure-tech.jp

Wisecuretech
ワイセキュア株式会社