プライバシープロテクション

プライバシーを尊重しながらセキュリティシステムを構築する方法

フィジカルセキュリティの導入はプライバシーをあきらめることではありません。プライバシーを保護するための総合的で段階的なアプローチを進めることで、個人の権利を守りつつ、データをより適切にコントロールすることができます。

プライバシーやデータ漏洩に関する統計

11秒ごとに
新たな企業へのランサムウェア攻撃が発生
（出典：Cybersecurity Ventures）

315日
悪意のある攻撃や犯罪的な攻撃による平均的なデータ漏洩ライフサイクル
（出典：IBM）

$150
お客様個人を特定できる情報（PII）が漏洩したときのレコード当たりの損失額（約17,200円）
（出典：Cybersecurity Capita）

€1,059,520,456
GDPRに基づいて徴収された罰金の総額（約1,370億円）
（出典：Privacy Affairs）

データを安全に保つための5つのステップ

Step 1

目的を明確にして、最適な人材を雇用

- データ保護の戦略をリードできるデータ保護最高責任者（DPO）を採用し当局の規制の遵守に取り組む
- データの収集方法、保存場所、保存期間、アクセス権の設定などを詳細に検討する
- 収集されている各種データを分類（リスク度合の高、中、低）して整理する
- データにアクセスする必要があると判断される組織外のユーザーを特定する
- データ処理プロセスが一般の権利に及ぼすリスクレベルを評価する

75%
の顧客が企業のプライバシー対応と信頼性を強く関連付けて考えています。
（出典：Salesforce）

107カ国
には、データとプライバシーの保護を定めた規制が在ります。
（出典：UN）

Step 2

データ保護戦略の策定

- データ処理作業の潜在的な改善点を明確にするためにギャップ分析を実施
- 既存システムを精査して、リソースを浪費することなくプライバシーに効果的に対処可能かを判断
- 新しい取り組みを導入し、すべてのプライバシーポリシーやその取り扱いに関してドキュメント化を実施
- サイバーセキュリティおよび最善のプライバシー管理方法について社員を教育
- データ保護とプライバシー保護への取り組みについて情報を一般に公開してさらに透明性を高める

52%
のインシデントは悪意のある者が関与した攻撃であり、25%がシステムの不具合、23%が人的エラーによるものです。（出典：IBM）

75%
のCEOは2024年までにサイバーフィジカルセキュリティシステム攻撃に対して個人的に責任を負うこととなります。
（出典：Gartner）

Step 3

最適なシステムとベンターの選択

- ベンダーが提供可能なプライバシーとデータ保護を推進するためのツールを探す
- ベンダーが取得している各種認証や自社がプライバシー関連法を遵守するためにどのような対策を実施しているかについて確認する
- 各ベンダーの自社のデータポリシーとその実施に関する透明性のレベルを評価する
- プライバシー機能がデフォルトで有効となっている「プライバシー・バイ・デザイン」アプローチで構築されたソリューションの導入またはアップグレードを行う
- 異なる地域においてもプロセスとポリシーを標準化できるソリューションの検討

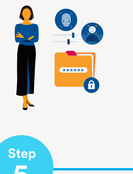
59%のみ
の企業がGDPR要件に全て対応済みと報告しています。
（出典：Cisco）

75%
の公安テクノロジーが、データの透明性を求める声に応えてポリシーベースの規制や倫理的な仕様詳細を策定しています。（出典：IDC）

Step 4

システムセットアップ時にプライバシーを考慮

- フィジカルなセキュリティシステムから収集された個人情報の保護のために多階層の防御手段を有効化する
- アクセス可能なユーザーと権限を定義し、アプリケーションにログインできるユーザーを表示のみまたは操作権限がある者に区別して制限する
- ビデオ映像上の個人を特定可能な情報にぼかし処理するなど、映像の匿名化処理のためのアドオンプライバシー機能を導入する
- データ保存ポリシーを自動化し、要求された通りに確実にデータの削除を行う
- デジタル証拠管理システムに投資し、調査のため、一般から情報を要求されたときに安全に共有できる環境を整備する



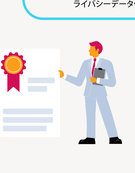
56%
の企業は必要に応じて各国の規制基準に合わせて調整可能な、データ保護およびプライバシー方針に関するグローバルな戦略を導入しています。
（出典：IAPP）

漏洩コストは
95%以上増加
セキュリティの自動化を導入していない企業は、完全な自動化を導入している企業と比べて漏洩コストが95%も高くなります。（出典：IBM）

Step 5

プライバシーを取り扱うときは細心の注意をはらい効率的に

- 最新のプライバシー保護に関する法令に追随し、必要に応じてポリシーやプロセスを改善する
- セキュリティ強化ツールを活用してサイバーセキュリティへの対応が適切であるか絶えずモニターし、ファームウェアやソフトウェアのアップデートが最新であるかをチェックする
- ユーザーアクティビティログをチェックして、誰が、何のデータに、どのシステムやファイルにアクセスしたかをいつでも把握する
- 死活監視システムを使用して、デバイスがオフラインになったりシステムの脆弱性が検出されたり時に自動的に通知を受信するようにする
- ハイブリッドクラウドの導入により、最新のサイバーセキュリティやプライバシーデータ保護手段へのアクセスの効率化を検討する



84%
の顧客はセキュリティ管理を強化している企業により好印象を持ちます。
（出典：Salesforce）

97%
の企業はプライバシー保護への投資が、競争上の優位性や投資家のアピールなどにおいて有利であることを認識しています。
（出典：Cisco）

信頼できるベンダーと業務にあたる

サイバー脅威とプライバシー規制が進む中で、企業はその動向を注視し続ける必要があります。プライバシーとサイバーセキュリティを重視して構築されたセキュリティソリューションへの投資は、プライバシーとデータ保護対策を実現し、コンプライアンスを維持するためのツールとなります。

プライバシーとサイバーセキュリティに関する弊社のアプローチやプライバシーデータを安全を保護する方法については、Genetec Trust Center をご覧ください。

genetec.com/ja/trust

Genetec