HITACHI

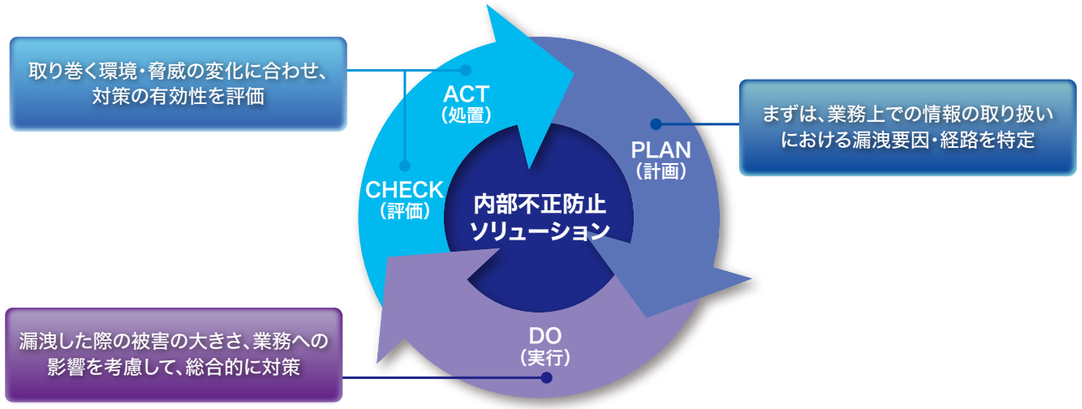
不正につながる“機会”をなくす

内部不正防止ソリューション

株式会社 日立ソリューションズ

日立ソリューションズの「内部不正防止ソリューション」は、現状のセキュリティ対策の不足部分を明確にし、認証強化や持ち出し制御などのソリューションを組み合わせることで「不正行為につながる機会」の排除を支援します。

昨今、企業や組織の内部関係者の不正行為による情報漏洩事件が多数発生しています。情報漏洩は、損害賠償金の支払いといったコスト面だけでなく、社会的な信頼失墜など、企業に与える影響は計り知れません。そのため、情報資産にアクセスする際の認証強化や外部デバイスなどへの持ち出し制御、ユーザーの利用状況を監査する仕組みなど、内部不正対策の重要性が増しています。「内部不正防止ソリューション」は内部不正対策において欠かせないクラウドやエンドポイント、サーバーへの対策を中心に、コンサルティングから対策の導入、運用、保守までをワンストップで提供。必要となるセキュリティ対策のPDCAサイクルを支援します。



内部不正防止ソリューション 特長

1. 「現状分析サービス」により必要な対策を明確化

独立行政法人 情報処理推進機構（IPA）が公開する「組織における内部不正防止ガイドライン」に基づいたヒアリング項目を設定し、経験豊富なコンサルタントが調査を行い、対策の不足点を洗い出します。

2. お客さまの環境に適したソリューションを提供

明確になったセキュリティ対策の不足部分に対し、日立ソリューションズが提供する豊富なソリューションを組み合わせ、お客さまの業務環境に適したセキュリティ対策を提供します。

3. 高度な知識や技術を有するセキュリティの専門家が対応

業種問わずさまざまな企業への豊富な導入実績から培ったノウハウを生かし、具体的な対策の導入から運用・保守までセキュリティの専門家が支援します。

不正をさせないためには「機会」をなくすこと

内部不正による情報漏洩事件の背景に労働・雇用環境の変化が・・・。

近年、顧客情報の大量漏洩事件など、内部不正による情報漏洩事故が相次いで発生しており、セキュリティ対策の見直しの必要性が高まっています。

従来の労働環境		これからの労働環境		
正社員中心	長期的雇用が中心	アウトソース	短期的雇用の増加	管理の目が届かない！
モノカルチャー	人も情報も社内のみ	ダイバーシティ	人と情報が社外へ	

技術的対策によって、不正行為の「機会」を無くすことから内部不正対策を始めてみませんか？

何から実施してよいかわからない / 現状を把握したい

■コンサルティングの概要

豊富な実績のあるコンサルタントの現地調査により、お客さまの情報セキュリティをはじめとするITガバナンス強化のための要件整理、対応方針策定を支援します。

情報セキュリティアセスメント	IPA「組織における内部不正防止ガイドライン」にもとづいたヒアリング項目を設定し、お客さまの事情に合わせた分析評価を実施します。
セキュリティポリシー／ガイドライン策定コンサルティング	基本方針策定から運用に至るまで、情報セキュリティポリシーに関わる作業を総合的に支援します。
CSIRT構築コンサルティング	インシデント発生時の早期対応を実現する、組織にフィットしたCSIRTの構築および運用を支援します。
情報セキュリティ監査サービス	お客さまの情報セキュリティポリシーの遵守状況を監査し、対応策について適切な助言を行います。

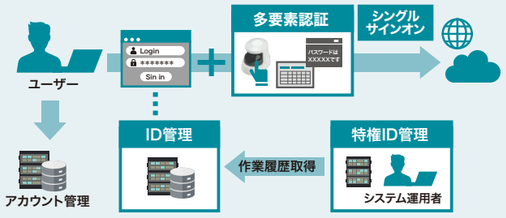
具体的な対策を実施したい

技術的対策を実施しているつもりでも、見落としは意外とあるものです。以下の4つのポイントから、内部不正が“できない仕組み”を構築しましょう。

認証強化・ID管理（特権IDを含む）

認証強化・ID管理により、なりすましやIDの削除漏れを防止。
また、特権ID管理の仕組みを導入することで不正な作業を抑止。

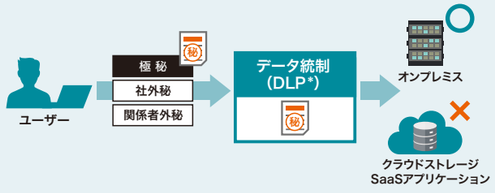
- ☑ 正規の利用者のみサーバーアクセスを許可
- ☑ 作業履歴を取得し不正アクセスを抑止



データ統制

データの機密度に応じた情報の保護・データの持ち出し制御を行うことにより、情報漏洩対策を実現。

- ☑ ポリシーにもとづいたデータのアップロード制御
- ☑ 持ち出しデータの編集・複製・印刷可否などを管理

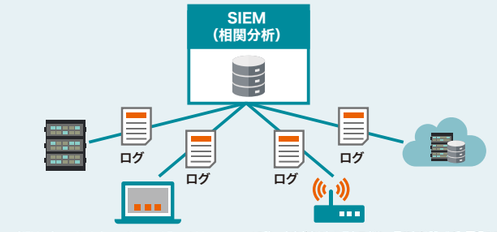


＊DLP：Data Loss Prevention

監視・監査

PCやサーバー、ネットワーク機器などのログをSIEM*基盤に集約し、相関分析をすることにより不審な操作をリアルタイムに検知。

- ☑ PC操作やサーバーアクセスの記録、不正アクセスを監視
- ☑ ログ管理／相関分析により問題を早期発見、情報漏洩を抑止

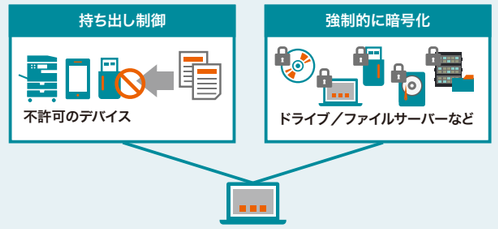


SIEM：Security Information and Event Managementの略。さまざまなシステムログを一元的に検索・分析・可視化する。

エンドポイント管理（持ち出し制御）

私物USBなどの不許可デバイスの使用を禁止し、社内情報の持ち出しを制御。
また、ドライブやファイルサーバーなどは強制的に暗号化し、データを保護。

- ☑ 不許可デバイスの接続を防止
- ☑ ドライブやファイルサーバーなどは強制的に暗号化



■「内部不正防止ソリューション」 ソリューション一覧

コンサルティング		セキュリティコンサルティング	全社セキュリティ強化 （リスク分析、情報セキュリティポリシー策定、情報セキュリティ監査サービスなど）
認証強化・ID管理・特権ID管理	認証強化（生体認証）	静紋	指静脈認証を用いた確実な本人確認により不正利用、なりすましを防止
		AUthentiGate	指静脈認証、顔認証、IC カードを用いた確実な本人認証により不正利用、なりすましを防止
		Biometric Signature Sign-in Service	生体情報をどこにも保管しない生体認証を提供することで漏洩防止、なりすましを防止
	認証強化（OPT）	Entrust IdentityGuard	乱数表やワンタイムパスワードなどを用いた二要素認証で不正アクセス、なりすましを防止
	統合ID管理	Okta	SSO（シングルサインオン）、ID管理、多要素認証などの機能をクラウド上で実現
		Microsoft Entra ID	ID管理に加え、多要素認証や条件付きアクセス・シングルサインオンといった機能を用いて、第三者による不正アクセスや情報窃取を防止
	特権ID管理	SecureCube Access Check	安全性の高いゲートウェイ型のソリューション、特権アクセスを強力に制御
		ESS AdminONE	オンプレミスやクラウドなど多種多様なシステムの特権IDを一元的に管理
データ統制	DLP	Microsoft Purview	データの分類化、情報保護・データの持ち出し制御を実現
		Netskope（DLP機能）	データ持ち出しなどの不正な利用の検知や制御を実現
監視・監査	SIEM	Splunk	各機器のログを検索、相関分析を行いリアルタイムに可視化
	管理者操作ログ	ESS REC	クライアントPCやサーバーの操作を監視、ログ取得（動画／ テキスト）
	ユーザー操作ログ	Proofpoint ITM （Insider Threat Management） （旧称：ObserveIT）	クライアントPCやサーバーにおける従業員の操作ログを取得
		SKYSEA Client View	ユーザー操作を録画、内部不正リスクを可視化することで、情報漏洩を防止
		Ivanti	クライアントPCやサーバーにおける従業員の操作ログを取得
		Splunk	ログ収集と相関分析による内部不正の可視化
	クラウドストレージ監視	Netskope（CASB機能）	SaaSにアップロードされているファイルに機密情報が含まれていないかを可視化
エンドポイント管理（持ち出し制御など）	エンドポイント管理（持ち出し制御など）	秘文シリーズ	リムーバブルデバイスやスマートデバイスへのファイルコピー、印刷、メール送信を制御
			接続ネットワーク制御、アクセスポイント制御
			Webサイトへの不正な書き込み、ファイルのアップロードを防止
		SKYSEA Client View	情報漏洩リスクとなりやすい外部記録媒体に対する制御、デバイスの管理
		Ivanti	未許可の外部記録媒体へのデータ持ち出し制御、デバイスの管理
	メール	proofpoint	社外メールの添付ファイル送信／誤送信防止、メールのウイルス対策、スパム対策
	ネットワーク制御	Aruba ClearPass	接続ネットワーク制御、アクセスポイント制御

※秘文、静紋、AUthentiGateは、株式会社日立ソリューションズの登録商標です。※Oktaは、Okta, Inc. の米国およびその他の国における商標または登録商標です。※SecureCube Access Checkは、株式会社野村総合研究所の登録商標です。 ※Microsoft（Microsoft Entra、Microsoft Purview）は、マイクロソフトのグループ企業の、米国およびその他の国における商標または登録商標です。※Netskopeは、Netskope, Inc.の米国およびその他の国における商標または登録商標です。※proofpointは、Proofpoint, Inc.の米国およびその他の国における商標または登録商標です。※SKYSEA、SKYSEA Client Viewは、Ｓｋｙ株式会社の登録商標です。※Ivantiは、IVANTI, INC.の米国およびその他の国における商標または登録商標です。※ESS RECは、エンカレッジ・テクノロジ株式会社の登録商標です。 ※Splunkは、Splunk Inc.の米国およびその他の国における商標または登録商標です。 ※Entrustは、Entrust,Inc.の米国およびその他の国における商標または登録商標です。※Aruba、ClearPassは、Hewlett Packard Enterprise社の米国およびその他の国における商標または登録商標です。 ※その他、本カタログ中の会社名、商品名は各社の商標、または登録商標です。※本文中および図中では、TMマーク、®マークは表記しておりません。 ※製品の仕様は、改良のため、予告なく変更する場合があります。 ※本製品を輸出される場合には、外国為替及び外国貿易法ならびに米国の輸出管理関連法規などの規制をご確認の上、必要な手続きをお取りください。なお、ご不明な場合は、当社担当営業にお問い合わせください。 ※本カタログ中の情報は、カタログ作成時点のものです。※本カタログの一部は、生成AIにより生成されたコンテンツを使用しています。

株式会社 日立ソリューションズ

www.hitachi-solutions.co.jp

本カタログ掲載商品・サービスの詳細情報

www.hitachi-solutions.co.jp/security/sp/solution/task/fraud_prevention.html

S14S-03-04 | 2025.09