■ 機能一覧

分類	機能	メニュー	概要
ポスチャマネジメント	可視化	ポスチャマネジメント ダッシュボード	管理しているPCのセキュリティ設定・アンチウイルスソフト・ファイアウォール設定・ソフトウェア脆弱性・暗号化の状態をチェックした結果や、リスクへの対策状況を一目で確認できます。
	分析・評価	セキュリティ設定*1	OSのセキュリティ設定*2に不備がないかをセキュリティガイドラインの推奨事項に沿って定期的に自動診断します。
		アンチウイルスソフト*1	アンチウイルスソフトの導入、ふるまい検知やリアルタイムスキャンが有効に設定されているかなどを診断します。
		ファイアウォール設定*1	Windows Defender ファイアウォールで、不要なインバウンド通信をブロックしているか診断することができます。
		ソフトウェア脆弱性*3	OSやアプリケーションの脆弱性診断を自動で行い、見つかった脆弱性に対してCVSS V3*4をベースに深刻度を評価します。
		暗号化の状態確認	PCを秘文またはBitLockerで暗号化しているか、または暗号化していないかの状態を確認します。
		利用シーンに応じた管理項目の切り替え*1	PCが接続しているネットワークから利用シーンを判断し、利用シーンに応じた診断項目でポスチャマネジメントを行います。
		アプリケーション管理	OSのセキュリティパッチや、インストールされているアプリケーションのバージョンが最新かどうかをチェックします。
	対策	自動是正*1	分析・評価におけるセキュリティ設定*5・アンチウイルスソフト・ファイアウォール設定の結果に不備があった場合には、自動で是正します。管理者やユーザーの手を煩わせることなく対策できます。
		警告通知設定（メール）	分析・評価の結果、アラートの件数が指定した閾値を超えた場合には、管理者へメールで通知します。
内部不正・盗難紛失対策	禁止ソフトウェア起動制御		リスクのあるソフトウェアの起動を制御し、内部不正などによる情報漏洩を未然に防ぎます。
	デバイス制御		スマートフォン、USBメモリー、CD・DVDなど、さまざまなデバイスの利用を禁止することで、不正コピーによる情報漏洩を防止します。
	ネットワーク制御	アクセスポイント制御	管理者が許可するアクセスポイントを指定できます。スマートフォンのテザリング機能などによる未許可アクセスポイントへの接続を制御することで、不正なネットワーク経由での情報漏洩を防止します。
		VPN利用強制	在宅勤務などのテレワーク環境では、VPN利用を強制し、必ず社内ネットワーク経由で接続させるので、安全なテレワーク環境を実現できます。
	操作ログ取得		エクスプローラーを使用したファイル操作や持ち出し、アプリケーション操作などの履歴をユーザー操作ログとして取得します。定期監査や有事の際の調査に活用できます。
	BitLocker管理		Windosws10端末のディスク暗号化状況やBitLockerの回復パスワードをコンソールから一括管理できます。また紛失時の対策として、遠隔操作で暗号化の実行やBitLockerのパスワードを変更することも可能です。
	メディア・ファイル暗号化★		ファイルやPCのハードディスク、USBメモリーなどのメディアなどを暗号化することができます。万が一、不正に持ち出されたり紛失した場合も、情報漏洩を防ぎます。
	共有フォルダの暗号化★		ファイルサーバー上のファイルをフォルダ単位で暗号化できます。サーバーのメンテナンス担当者などアクセス権がある場合でも、直接ファイルを参照はできないため、内部不正対策としても有効です。
IT資産管理	ハードウェア・ソフトウェア管理		社内および社外にあるPCのハードウェア・ソフトウェアの情報を自動で収集し、管理できます。
	ライセンス管理		収集したソフトウェア情報から、ライセンスの状態を把握することで、ライセンス違反や超過購入を防ぎます。
	グループ企業管理（関連顧客管理）		グループ企業のセキュリティレベルを総合診断しダッシュボードで確認できるので、問題のある端末の台数などを一目で把握できます。
	リモートコントロール		社内LANに接続しているPCに対してリモート操作が可能です。
	インターネットリモートコントロール★		インターネットを経由して、出張先や自宅など遠隔地にあるPCに対してリモート操作が可能です。
	ソフトウェアリモートインストール*6		業務に必要なファイルやソフトウェアを、社内ネットワーク・インターネットを経由して、配布できます。
	メッセージ通知		PCに対して任意のメッセージを通知できます
	Windows 10管理・運用支援		更新モデルの指定（SACT・SACなど）、アップデート適用延長日数の指定、高速スタートアップの有効・無効の設定が可能です。
スマートデバイス管理★	運用・制御	各種脆弱性診断レポート	AndroidやiOSの脆弱性診断を実施し、診断結果をコンソール上で確認できます。
		アプリケーション配布（アプリケーションポータル配布）	業務に必要なアプリケーションを管理者側から配布や削除を行うことができます。社内で利用を許可しているアプリケーションをダウンロードできるポータルを作成し、まとめて管理することも可能です。
		Root化・Jailbreak検知	脆弱性を突かれやすいRoot化・Jailbreakを行っている端末を検知し、管理者にメールで通知します。
		Bluetooth・Wi-Fi接続先制御	Wi-FiやBluetooth通信の無効化、といったスマートデバイス上での情報漏洩になりうる通信接続を制御します。
	紛失対策	位置情報の取得	GPSで位置情報を取得し現在地を確認することで、紛失したスマートデバイスの発見や、社員の行動管理に役立ちます。
		リモートロック・ワイプ	Android*7・iOS端末の盗難や紛失などの緊急時にリモートロック・ワイプといった操作を遠隔で実行できます。
その他	ファイル保護★		安全性が確認できるプログラムにのみ、機密データやOS管理領域（Master Boot Recordなど）へのアクセスを許可します。これにより万が一マルウェアに感染しても、マルウェアから機密情報を守ります。
	勤怠管理*8		従業員の勤務時間を把握し、時間外労働の超過を抑止することができます。

＊1 Windows10 OSのみサポートしています。 ＊2 グループポリシー、アカウントポリシー、ローカルポリシー、監査ポリシー、Windows機能、Windowsファイアウォール ＊3 Windows10 64ビットOSのみサポートしています。
＊4 Common Vulnerability Scoring System（共通脆弱性評価システム） ＊5 一部自動是正に対応していない設定があります。 ＊6 インターネット経由での配布を希望される場合は、お問い合わせください。
＊7 Android 7以降では、リモートロック機能には対応しておりません。 ＊8 勤怠システムとの連携が必要です。 ★ オプションを購入いただくことで利用可能な機能です。

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/hibun/sp/

S20S-01-01 | 2021.12

HIBUN

HITACHI
Inspire the Next

エンドポイントはゼロトラストで守る時代
対症療法から自律的コントロールによる予防へ

秘文 統合エンドポイント管理サービス

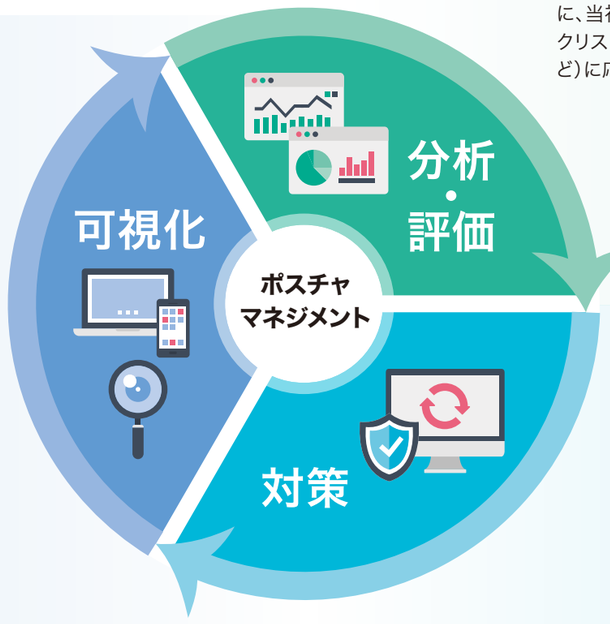
株式会社 日立ソリューションズ

ゼロトラストセキュリティを実現するために、エンドポイントのセキュリティを自動で維持する仕組みを提供

クラウドシフトやテレワークの導入が進むビジネス環境において
あらゆるデータにアクセスするエンドポイントのセキュリティを常に信頼される状態に維持しておくことは、
ゼロトラストセキュリティにおいて重要な要素の1つです。

秘文は **可視化** **分析・評価** **対策** の3つのステップでエンドポイントのセキュリティを
自律的にコントロールする**ポスチャマネジメント**を提供します。

セキュリティ運用業務を秘文が支援することで、
運用負荷を軽減するだけではなくセキュリティを高めることも可能です

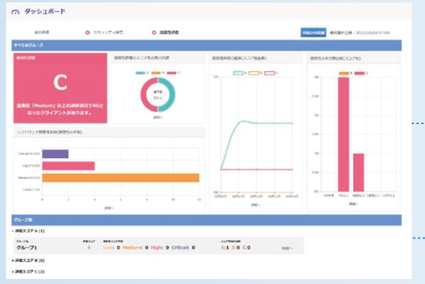


Step 1 組織全体のセキュリティ状態を可視化

インベントリ情報の管理はもちろん、Windows OSのセキュリティ設定や、ソフトウェアの脆弱性、リスクへの対策状態を可視化

PCのセキュリティ状態をダッシュボードに一覧表示

インベントリ情報の管理はもちろん、Windows OSのセキュリティ設定やソフトウェアの脆弱性、リスクへの対策状態を可視化することが可能。テレワークなどで管理者の目が届かないところにあるエンドポイントのセキュリティ管理や対策が容易。



長期間未対策のPCをすぐに確認可能

PCのセキュリティの評価をグループごとに確認できるため、評価が低いグループに絞った対処の検討が可能

リスクを検知した機器の診断結果を確認
- Windows OSのセキュリティ設定
- アンチウイルスソフト設定
- ファイアウォール設定
- ソフトウェア脆弱性
- 暗号化の状態

Step 2 セキュリティリスクの分析・評価

Windows OSのセキュリティ設定やソフトウェア脆弱性を毎日自動で診断

PCの利用状況に合わせたチェック項目で診断

セキュリティのガイドラインによる推奨事項*1（200項目以上）をベースに、当社のセキュリティの専門家の知見を取り込んだセキュリティチェックリストを使用して診断を実施。PCの利用シーン（社内やテレワークなど）に応じて診断項目を自動で切り替え可能。

ソフトウェアの脆弱性を診断し、深刻度を自動で評価

Windows OSやアプリケーションについて既知の脆弱性が存在するかどうかを自動で診断。見つかった脆弱性に対して、CVSS V3*2をベースに深刻度を評価。

*1 Defense Information Systems Agency（DISA）が作成したSecurity Technical Implementation Guides（STIGs）を採用
*2 CVSS：Common Vulnerability Scoring System（共通脆弱性評価システム）

Step 3 セキュリティリスクに応じた対策

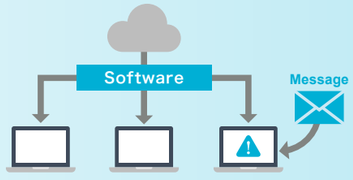
リスクが見つかった場合には、自動で是正を実施したり、対策を支援する機能を提供することで、管理者の負荷を軽減

OSのセキュリティ設定の不備を自動是正

Windowsの各種ポリシーやファイアウォール、Windows Defenderの設定に不備があった場合には、自動で是正。管理者やユーザーの手を煩わせずにセキュリティを維持することが可能。

ソフトウェア配布やメッセージ通知により、対策を支援

ソフトウェアの脆弱性を発見した場合、社内ネットワーク経由でセキュリティパッチを配布可能。また脆弱なパスワードの利用などユーザー側で設定変更が必要な場合は、メッセージで是正を要求。

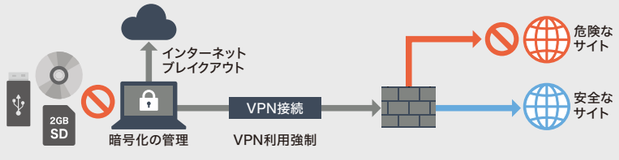


その他の特長

エンドポイントの管理
・
セキュリティ対策を
1つのサービスで提供

内部不正・盗難紛失対策

禁止ソフトウェアの起動制御やBitLocker管理、デバイス制御により内部不正や盗難紛失による情報漏洩を防止します。また社外でのインターネットブレイクアウトにより在宅勤務などのテレワーク環境では、お客様が指定した信頼できる特定クラウドサービスへの通信のみ、VPNを経由せず直接接続させることができます。これにより、快適で安全なテレワーク環境を実現します。



IT資産管理

*3 インターネット経由でのリモート操作はオプションです。

出張先や自宅など、社内ネットワークに接続されていないPCを含め、一元管理します。遠隔地にあるPCをリモートで操作することも可能*3で、社内LANにアクセスできないPCの運用管理も支援します。

スマートデバイス管理

スマートデバイスをPCと同一コンソールで一元管理でき、管理者側からアプリケーションの配布や削除が可能です。また盗難・紛失時の対策として、GPSによるスマートデバイスの位置情報の取得や、リモートロック・ワイプが可能です。