

2021年3月17日

株式会社日立ソリューションズ

「秘文」が、境界防御モデルからゼロトラストモデルへの移行を支援する ポスチャマネジメントサービスへ拡張 「秘文 統合エンドポイント管理サービス」を提供し、第一弾としてセキュリティリスクを可視化

株式会社日立ソリューションズ(本社:東京都品川区、取締役社長:星野 達朗/以下、日立ソリューションズ)は、エンドポイントの情報漏洩防止を支援する「秘文」のサービスをセキュリティインシデントへの対応力を高めるポスチャマネジメントサービスへと拡張するため、新たに「秘文 統合エンドポイント管理サービス」を3月31日に提供開始します。

秘文のポスチャマネジメントサービスは、企業で使用するあらゆるデバイスの状況を常に把握し、セキュリティの課題に対してリアルタイムに対処することで、セキュリティ侵害を未然に防止し、エンドポイントの自律的な管理を実現し、ゼロトラストモデルへの移行を支援します。

秘文のポスチャマネジメントのサイクルは、「可視化」「分析・評価」「対策」の3つのステップで構成されています。「秘文 統合エンドポイント管理サービス」の今回提供する機能は、オフィスワークとテレワークのセキュリティリスクを「可視化」するものです。

今後、段階的に「分析・評価」「対策」の機能も提供していきます。さらに、サイクルを自動処理し、利用者の危険な操作や振る舞いなどを分析することで、評価の精度を高めます。

日立ソリューションズは秘文新サービスを通じて、社員が場所や時間にとらわれず安心して企業活動に専念できる環境維持を支援するとともに、システム管理者の運用負荷を軽減します。

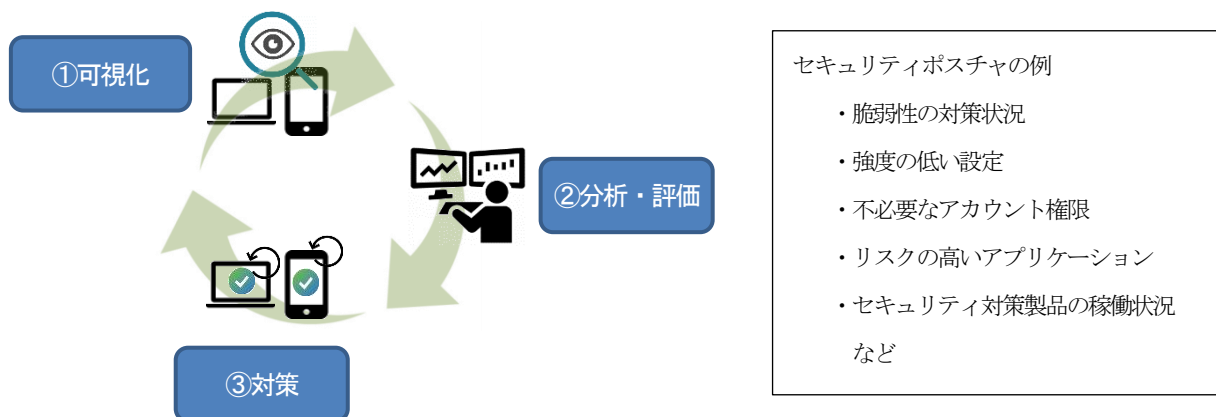


図 1: 秘文のポスチャマネジメントのサイクル

■ 背景

新常態(ニューノーマル)においては、企業におけるテレワークの導入やクラウドシフトが加速し、業務情報が外部サービスに保管されるなど、セキュリティリスクが増しており、境界防御モデルではセキュリティ維持が困難になっています。このような状況の中で、セキュリティインシデントへの対応力を高めるためには、一つひとつセキュリティリスクに対する対策を積み上げるだけでは十分ではありません。

また、米国国立標準技術研究所(NIST)が公開するゼロトラストアーキテクチャ(NIST.SP.800-207)では、基本原則としてセキュリティにおけるポスチャ改善の重要性が定義されています。さまざまなセキュリティ対策を統合的に管理するポスチャマネジメントは、ゼロトラストモデルへの移行を進める企業にとって必要な考え方となります。

そこで、日立ソリューションズは、金融、公共から産業まで幅広く導入してきたエンドポイントの情報漏洩防止を支援する「秘文」を、ポスチャマネジメントサービスに拡張することにしました。さまざまなセキュリティ対策を統合的に管理するとともに、企業のリソースであるハードウェア、ソフトウェア、ポリシー、人のふるまいなどをリアルタイムに評価し、改善点を自律的に見直していくことで、エンドポイントの情報セキュリティガバナンスを再徹底するものです。

表：ゼロトラストアーキテクチャの基本原則（NIST.SP.800-207 より）

	基本原則
1	すべてのデータソースとコンピューティングサービスはリソースと見なす
2	ネットワークの場所に関係なく、全ての通信を保護する
3	企業リソースへのアクセスは、個別のセッション単位で付与する
4	リソースへのアクセスは、動的ポリシーによって決定する
5	企業は、全ての資産の整合性とセキュリティポスチャを監視し、測定する
6	全てのリソースの認証と認可は動的に行われ、アクセスが許可される前に厳格に実施する
7	企業は、資産、ネットワーク、通信の状態について可能な限り多くの情報を収集し、セキュリティポスチャの改善に利用する

■ 「秘文 統合エンドポイント管理サービス」の新機能(可視化)の特長

1. テレワーク環境でのセキュリティリスクをリアルタイムに可視化

時間や場所にとらわれず、PC やスマートデバイスなどを活用し、多様な働き方を支援するため、さまざまなシーンでエンドポイントのセキュリティリスクをリアルタイムに可視化します。

セキュリティリスクを検出したエンドポイントに対する利用制御やポリシー変更によって自動的に、セキュアな設定に変更することで、システム管理者の負担なく、セキュリティインシデントの発生を未然に防ぐことができます。

2. セキュリティ対策強化と運用コスト削減の両立

クラウドサービスとして提供するため、初期導入コストを抑え、迅速に導入することができます。これまで提供してきた強固なセキュリティ対策に加えて、IT 資産管理、スマートデバイス管理などの管理機能を統合的に 1 つのサービスで対応できるため、システム管理者の運用負荷を軽減します。

■ **販売開始日** 2021年3月31日

■ 「秘文 統合エンドポイント管理サービス」の提供価格(税別)

標準価格

サブスクリプション型 1台当たり 7,800円/年 (500台の場合)

スタートダッシュキャンペーン価格(2022年3月31日まで)

サブスクリプション型 1台当たり 4,000円/年 (500台の場合)

■ スタートダッシュキャンペーンのお知らせ

2021年3月17日～2022年3月31日の期間、導入費用をディスカウントするキャンペーンを実施します。「秘文 統合エンドポイント管理サービス」の導入から運用開始までのサポートも提供します。詳細につきましては、販売代理店または弊社営業までお問い合わせください。

■ 「秘文」の新サービス体系について

「秘文」シリーズでは、20年間以上、他社に先駆け、エンドポイントから情報漏洩を防止するソリューションを提供してきました。これまでに、累計8500社、910万ライセンスの導入実績があり、2004年度から16年連続シェアNo.1^{*1}です。

これまで「秘文」シリーズは、デバイスの利用制限や接続先ネットワークの制御を行い、データを持ち出させない「秘文 Device Control」、データを暗号化し、漏洩してもデータの中身を見せない「秘文 Data Encryption」、ファイルの失効(閲覧停止)で、相手先に渡した情報の不正利用や流出・拡散を防止する「秘文 Data Protection」の3製品と、サービスモデルで管理者の運用負荷を軽減する「秘文 Endpoint Protection Service」で構成されていました。

このたび、「秘文 Endpoint Protection Service」を、「秘文 統合エンドポイント管理サービス」に再編し、エンドポイントにおけるポスチャマネジメントを実現するサービスを提供していきます。

*1:株式会社 富士キメラ総研「2005～2020ネットワークセキュリティビジネス調査総覧」<ファイル暗号化・持出制御ツール・金額ベース>より

URL : <https://www.hitachi-solutions.co.jp/hibun/sp/product/eps/>

◎株式会社 日立ソリューションズ

本社 〒140-0002 東京都品川区東品川四丁目12番7号
ホームページ: <https://www.hitachi-solutions.co.jp>

日立ソリューションズ

■ 日立ソリューションズが提供するゼロトラストセキュリティソリューションについて

ゼロトラストセキュリティとは、「社内は安全である」という前提で境界を守る「境界防御モデル」でのセキュリティ対策ではなく、「すべて信頼できない（ゼロトラスト）ことを前提として、すべてのデータ・コンピュータリソースが保護され、すべてのトラフィックやログの可視化・監視を行う」、性悪説に基づいたセキュリティアプローチです。

日立ソリューションズでは、境界防御モデルからゼロトラストモデルへ移行するためのベストプラクティスとして、以下のような段階的な移行シナリオを描き、ソリューションを提供していきます。

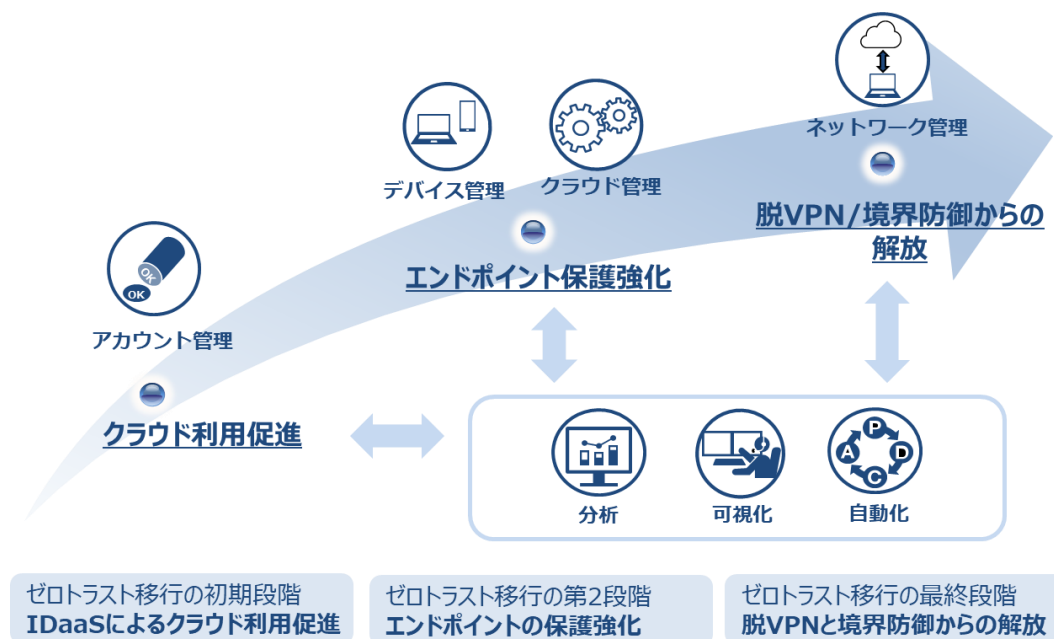


図2：ゼロトラストモデルへの移行シナリオ

URL : <https://www.hitachi-solutions.co.jp/security/sp/solution/task/zerotrust.html>

■ 商品・サービスに関するお問い合わせ先

URL: <https://www.hitachi-solutions.co.jp/inquiry/>

■ 報道機関からのお問い合わせ先

担当部署: 経営企画本部 広報・宣伝部

担当者: 多田、安藤

E-mail: koho@hitachi-solutions.com

※ 秘文は、株式会社日立ソリューションズの登録商標です。

※ その他記載の会社名、製品名は、それぞれの会社の商標もしくは登録商標です。

◎ 株式会社 日立ソリューションズ

本社 〒140-0002 東京都品川区東品川四丁目12番7号
ホームページ: <https://www.hitachi-solutions.co.jp>

日立ソリューションズ

このニュースリリース記載の情報(製品価格、製品仕様、サービスの内容、発売日、お問い合わせ先、URL等)は、発表日現在の情報です。予告なしに変更され、検索日と情報が異なる可能性もありますので、あらかじめご了承ください。
