HITACHI
Inspire the Next

ランサムウェアの脅威は、進化する「秘文」で守る！

2016年、日本国内で検出されたランサムウェアは前年比約9.8倍*

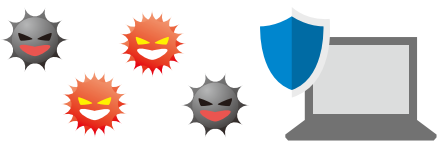
昨今、ランサムウェアの脅威が拡大しています。
その手口は巧妙化が進み、マルウェアの侵入を完全に防ぐことは困難です。
特にランサムウェアの多くはネットワークで急速に拡散する特性があり、
気づいた時にはエンドポイントでデータが破壊されていたという事例が少なくありません。
そのため企業にとってランサムウェアの対策は、喫緊の経営課題となっています。

＊ 情報セキュリティ10大脅威2017（組織編）/2017年5月IPA

ランサムウェア対策の課題

✓ 従来の対策では侵入を防げない

ランサムウェアは日々進化するため、侵入を完全に防ぐことは困難です。そのため、検知・防御に加え、万一侵入された場合に備え被害を最小限にする対策が重要です。



✓ 再発防止ができていない

ランサムウェアの侵入ルートは、メールの受信や、Webからのダウンロード、USBメモリからの感染など複数あります。再発防止を行うためには、侵入の原因を特定する必要があります。

秘文で実現するランサムウェア対策とは >>>

株式会社 日立ソリューションズ

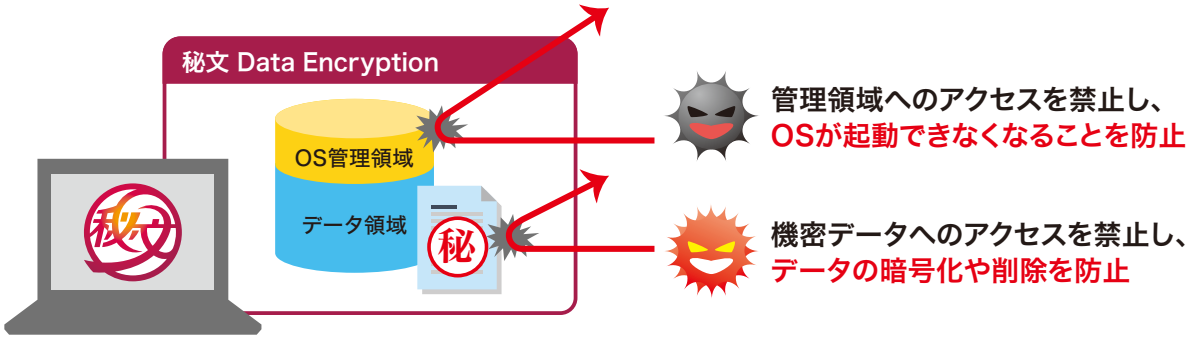
ランサムウェアが侵入した場合も 最後の砦として、秘文が重要情報を守ります。

HIBUN

Protect 1　ランサムウェアによるデータの破壊を防止

秘文 Data Encryption

強制暗号化や削除などでデータを破壊したり、OSを起動できなくするランサムウェアに対応。これにより、
万一ランサムウェアに感染した場合でもお客さまの機密データを守ります。



Protect 2　侵入の原因を特定し、再発防止を支援

秘文 Device Control
CylancePROTECT

ファイル操作や各種アプリケーション利用などのユーザー操作履歴を蓄積し、マルウェア検知情報と組み合わせて可視化。
これにより、ランサムウェア侵入の原因となったユーザー操作を特定するだけでなく、再発防止を支援します。

CylancePROTECTとは

マルウェア検知率99%以上*。AI（人工知能）ベースの独自の検出エンジンを搭載し、マルウェアを既知・未知問わず高精度に検知します。実行前検知機能によりランサムウェアに暗号化される前に検知および隔離を行います。

*2016年1月 ドイツに拠点をおくセキュリティ製品の性能検証・比較検証を行う第三者機関「AV-TEST」にて評価

CYLANCE

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/

S17S-01-01　2017.10