HITACHI
Inspire the Next

News Release

2017年8月30日
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てもエンドポイントを守る「秘文」の最新版を提供開始

情報漏洩だけでなく情報破壊も防止する「秘文」に進化

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:柴原 節男／以下、日立ソリューションズ)は、ネットワーク対策とエンドポイント対策を組み合わせた多層防御が求められる中、侵入後、内部ネットワークへ急速に拡散するランサムウェアからエンドポイントを守る「秘文」シリーズの 2 製品の最新版を 8 月 31 日から提供開始します。

「秘文 Data Encryption」※1の最新版は、実行プログラム(EXE ファイル)に加え、プログラムが必要に応じてメモリに呼び出して利用する DLL(ダイナミックリンクライブラリ)ファイルも監視することで、正規のプログラム以外に機密データや OS のディスク管理領域へアクセスさせません。これにより、ランサムウェアが正規のプログラムを偽装し、強制暗号化や削除などのデータ破壊、PC の起動ロックなどを行おうとしても実行できず、お客様の機密データを守ることができます。

また、「秘文 Device Control」※2の最新版は、ユーザー操作履歴をログとして取得します。取得したログは、ログの統合管理やポリシー設定をする「秘文 Server」上で、エンドポイントに導入されたマルウェア対策製品による検知情報と組み合わせて可視化されます。これにより、お客様がランサムウェア侵入の契機となったメール受信や Web からのダウンロードなどのユーザー操作を特定し、再発防止策を迅速に立案することを支援します。今回は、AI を活用した次世代マルウェア対策製品「CylancePROTECT」との連携により、これを実現します。

「秘文」シリーズは、多くの実績がある暗号化、持出制御などの情報漏洩対策に加えて、データ破壊から情報を保護する対策および再侵入を防止する対策まで幅広く支援し、お客様のニーズに応じたセキュリティ対策を実現します。

※1:エンドポイントのデータ暗号化に加え、安全性が確認できるプログラムのみ、機密データへのアクセスを許可し、マルウェアから機密データを守ります
※2:デバイスの利用制限などにより、機密データの漏洩を阻止することに加え、マルウェアに感染した PC をネットワークから自動遮断します

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
Tel:03-5780-2111　ホームページ:http://www.hitachi-solutions.co.jp/

日立ソリューションズ

■背景

昨今、国内外で猛威を振るっているランサムウェアをはじめとするマルウェアは、今後さらに脅威が拡大することが予測されており、それらの対策は企業にとって喫緊の経営課題です。

攻撃の手口は複雑化・巧妙化しており、今や、ファイアウォールやウイルス対策ソフトを導入しても、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、気づいた時には数多くの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、侵入された場合の被害をいかに少なくするかが重要であり、また、侵入ルートを早期に特定し、二次被害や再侵入の防止に向けた対策が特に重要となっています。

■「秘文」最新版の主な特長

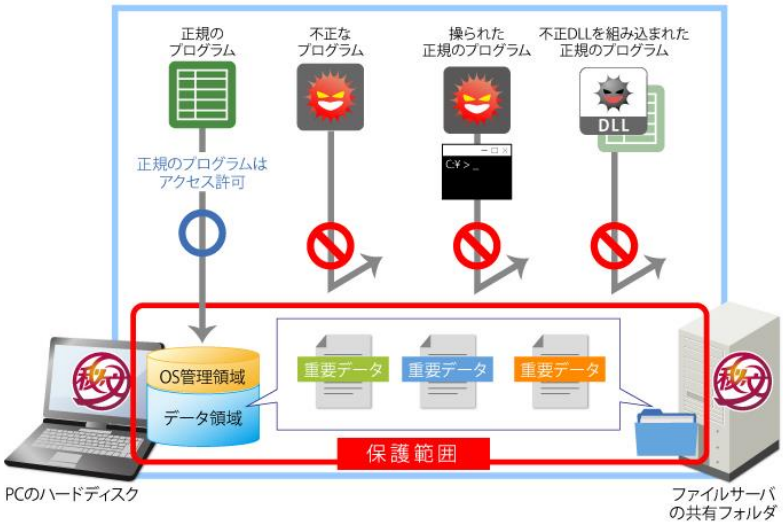
1. ランサムウェアによるデータ破壊を防止

正規のプログラム以外に機密データへアクセスさせない「秘文 Data Encryption」のマルウェア対策機能において、保護範囲を大幅に拡大することで、強制暗号化や削除などでデータを破壊する「暗号化型ランサムウェア」への対策を強化するとともに、PCを起動できなくする「端末ロック型ランサムウェア」※3にも対応し、最新のランサムウェア対策を実現します。

具体的には、従来から対応していた実行プログラム（EXEファイル）に加え、プログラムが必要に応じてメモリに呼び出して利用するDLL（ダイナミックリンクライブラリ）ファイルまで拡張しました。これにより、正規のプログラムを偽装して暗号化を実行するようなランサムウェアにも対応します。

また、従来のディスクドライブのデータ領域（ファイル／フォルダ）に加え、OSの管理領域まで保護する範囲を拡大することで、管理領域を不正に書き換える「端末ロック型ランサムウェア」にも対応します。

これにより、万一ランサムウェアに感染した場合でも、強制暗号化や削除などのデータ破壊から、お客様の機密データを保護します。



※3 ランサムウェアは、主に、感染端末自体を人質にする「端末ロック型ランサムウェア」と、データを人質にする「暗号化型ランサムウェア」に大別される。「端末ロック型ランサムウェア」は、OSのディスク管理領域を不正に書き換えて、PCが起動できないようにするもので、「暗号化型ランサムウェア」は、ファイルを暗号化して読めなくしたり、ファイルを消したりしてしまうなど、データを破壊するもの。

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
Tel:03-5780-2111 ホームページ:http://www.hitachi-solutions.co.jp/

日立ソリューションズ

2.「CylancePROTECT」と連携し、ランサムウェア侵入の契機となったユーザー操作を特定

「秘文 Device Control」の最新版では、従来の持ち出しログやデバイス接続ログに加え、今回、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ログとして取得できるようになりました。これらのログを収集・管理する「秘文 Server」上で、「CylancePROTECT」のマルウェア検知情報とユーザー操作履歴を組み合わせて可視化します。これにより、お客様がランサムウェア侵入の契機となったメール受信や Web からのダウンロードなどのユーザー操作を特定し、再発防止策を迅速に立案することを支援します。

■今後について

日立ソリューションズは、これまで、「秘文」とネットワークセキュリティ製品を連携し、マルウェア感染 PC の自動隔離による拡散防止を実現してきました。このたび、「秘文」の機能強化や、エンドポイントセキュリティ製品との連携により、ランサムウェアに感染した場合でも、お客様の被害抑止から再発防止の対応まで幅広く支援し、お客様のニーズに応じたセキュリティ対策を実現します。

今後も、ランサムウェアをはじめとするマルウェア対策を強化するため、「秘文」の技術革新によるデータ保護機能の強化や、先進的なアライアンス製品との連携に取り組むことで、お客様に一層の安全と安心を提供していきます。

■価格

製品名	価格(税別)	
秘文 Data Encryption※4	買取ライセンス 10,000円/クライアント	年間利用ライセンス 5,000円/クライアント
秘文 Device Control※4	買取ライセンス 10,000円/クライアント	年間利用ライセンス 5,000円/クライアント
CylancePROTECT※5(参考)	年間利用ライセンス 15,000円/クライアント(100クライアントの場合)	

※4 買取ライセンスに保守費、サーバーライセンスを含みません。年間利用ライセンスには保守費、サーバーライセンスを含みます。

※5 クライアント数など、各種条件や環境によって価格は変動します。

■提供開始時期:8 月 31 日

■「秘文」について（ http://www.hitachi-solutions.co.jp/hibun/sp/ ）

情報の漏洩を防ぐための「出さない」「見せない」という考え方と、万一、情報漏洩が起こった場合の漏洩拡大を抑止するための「放さない」という考え方に基づいた 3 つの製品で、高度化・複雑化する情報漏洩への対策を実現します。「秘文」シリーズは、これまでに 8,000 社、820 万ライセンス※6 の導入実績があり、ファイル暗号化ソフトウェアで国内シェア No.1※7 の製品です。

※6 2017 年 3 月末時点

※7 出典：「2016 ネットワークセキュリティビジネス調査総覧」株式会社富士キメラ総研（2015 年度金額ベース）
端末管理・セキュリティツール分野（持出制御ソフトウェア、暗号化ソフトウェア）にて国内シェア No.1

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
Tel:03-5780-2111 ホームページ:http://www.hitachi-solutions.co.jp/

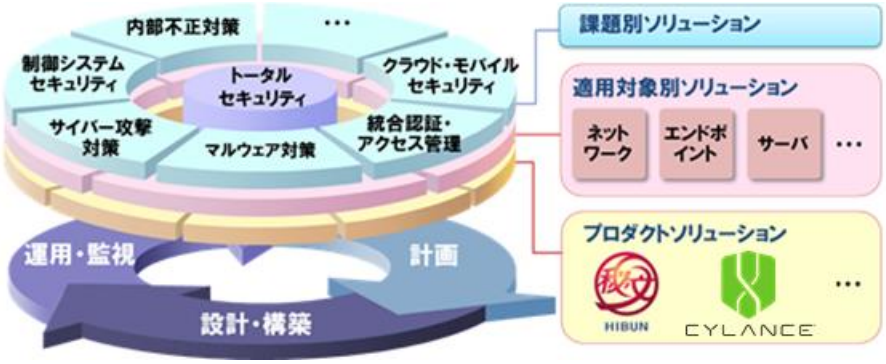
日立ソリューションズ

■CylancePROTECT について（ http://www.hitachi-solutions.co.jp/cylance/sp/）

正常なファイルやマルウェアファイルなどの数億個のファイルから抽出した約 700 万もの特徴を、AI 技術（機械学習）を利用した独自のアルゴリズムによって、未知のマルウェアが実行される前にエンドポイント上で高精度に検知・隔離する次世代マルウェア対策製品です。パターンファイルの定期更新が不要かつ管理システムをクラウド上で提供するため、システム管理者の運用負荷を軽減します。

■日立ソリューションズの「トータルセキュリティ」について（http://www.hitachi-solutions.co.jp/security/sp/）

日立ソリューションズは、企業のセキュリティライフサイクルを総合的に支援するため、自社やアライアンスの製品・サービスを「課題」「適用対象」「プロダクト」の 3 つの視点をもとに、システムのライフサイクルに必要なコンサルテーションと運用・監視のプロセスを強化した「トータルセキュリティ」として体系化しています。



■商品・サービスに関するお問い合わせ先

ホームページ：https://www.hitachi-solutions.co.jp/inquiry/　Tel：0120-571-488

■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:　竹谷、安藤
Tel：03-5479-5013　Fax：03-5780-6455　E-mail：koho@hitachi-solutions.com

日立ソリューションズ グループは、お客様の業務ライフサイクルにわたり、豊富なソリューションを全体最適の視点で組み合わせ、ワンストップで提供する「ハイブリッドインテグレーション」を実現します。

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
Tel:03-5780-2111　ホームページ:http://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。

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
Tel:03-5780-2111 ホームページ:http://www.hitachi-solutions.co.jp/

日立ソリューションズ