

テレワーク向け
標的型攻撃対策ソリューション

ゼロデイ攻撃対策

マルウェア被害の拡大防止

働く場所やテレワーク端末の多様化が進む中、世界中でテレワーク中の社員を狙った標的型攻撃が増加しています。本ソリューションは、OSプロテクト型で不正な行為を監視・遮断し、Emotetや未知の脅威に対応します。

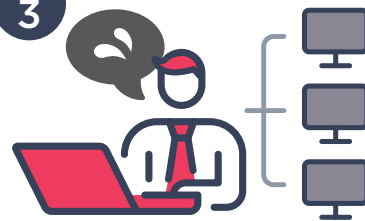
テレワーク端末のリスク

リスク
1

ゼロデイ攻撃の被害

リスク
2

マルウェア攻撃の被害

リスク
3定義ファイル配信などの
管理が煩雑対策
1対策
2OSに対して害のある行為をさせない
「OSプロテクト型」で端末を守る

リモートアクセス機能

テレワーク向け
標的型攻撃対策
ソリューション

標的型攻撃対策機能

対策
3定義ファイルベースではないため
定期的な定義ファイルの更新が不要

インシデント発生時の対応費用	コスト削減
保守・運用費用	保守・運用費用
EDR*・サンドボックスなどEPライセンス費用	ライセンス費用
アンチウイルスソフトライセンス費用	
従来型対策製品	本ソリューション

*EDR:Endpoint Detection and Response

既存のネットワーク環境はそのまま、セキュアにリモートアクセスを実現
※ 既設のテレワーク環境を活用して、「標的型攻撃対策機能」のみご利用いただくことも可能です。

当社は豊富な導入実績とノウハウを基に、効果的な対策をご提案します

ぜい弱性の脅威から完全に逃げ切ることはできません。
たとえマルウェアに感染しても害のある行為を未然に防ぐことで、
情報資産を守ります。

ゼロデイ攻撃など未知の脅威対策

ファイルレスマルウェア攻撃対策

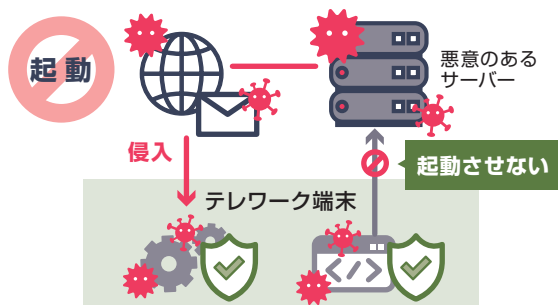
端末上での定期スキャンが不要で軽快な動作

OSプロテクト型のため定義ファイルの配信不要

テレワーク向け標的型攻撃対策ソリューションの活用方法

未知の脅威に対応

- マルウェアの検知ではなく、システムに害を与える動作を未然に防止
- 未知、ゼロデイ、ファイルレスのマルウェアなどの不正プログラムから、OSの中枢部を保護



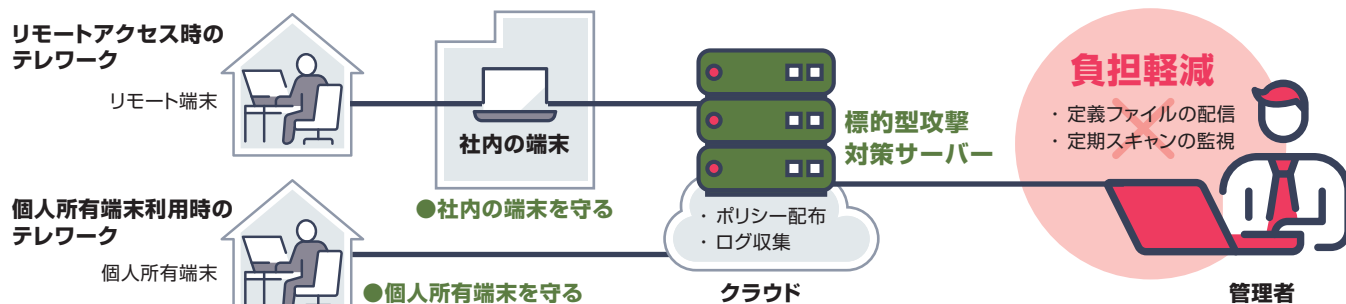
破られたことのない強固な防御

- 米国政府機関でも採用され、過去20年以上防御を破られたことがないAppGuard®を活用
- 「政府機関等の対策基準策定のためのガイドライン」に準拠



セキュアなリモート接続

- 社内の端末の画面だけをリモート端末に表示
- リモート端末がウイルスに感染しても、社内の端末へは持ち込ませない



定義ファイル更新等の負担軽減

- 定期的な定義ファイル更新が不要
- 従来の検知型対策製品から置き換えた場合、保守・運用費用の削減が可能

・ AppGuard® の製造元は株式会社Blue Planet-worksです。
・ AppGuard®、AppGuard® のロゴは米国法人 AppGuard, Inc.、または株式会社Blue Planet-works及びその関連会社の、米国、日本またはその他の国における登録商標、または、商標です。

商品・サービスに関するお問い合わせ・ご相談受付

Webによる受付

www.hitachi-solutions-create.co.jp/inq.html

お問い合わせページより、商品・サービスをお選びください。

メールによる受付

hsc-contact@mlc.hitachi-solutions.com

*ご相談・ご依頼いただいた内容は回答などのため、当社の関連会社（日立ソリューションズグループ会社）および株式会社日立製作所に提供（共同利用含む）することがあります。
取り扱いには十分注意し、お客様の許可なく他の目的に使用することはありません。

HSC202101

*商品仕様は、改良のため予告なく変更する場合がございます。最新情報は、当社Webページをご確認ください。
*本カタログに記載されている会社名、商品名は各社の商標または登録商標です。
*本カタログの内容は、2021年1月現在のものです。

株式会社 日立ソリューションズ・クリエイト
www.hitachi-solutions-create.co.jp/