HITACHI
Inspire the Next

テレワーク向け標的型攻撃対策ソリューション ご説明資料

株式会社 日立ソリューションズ・クリエイト

HITACHI
Inspire the Next

Contents

1．標的型攻撃の被害

HITACHI
Inspire the Next

『情報セキュリティ10大脅威2020』では、組織向けの脅威として「標的型攻撃による機密情報の窃取」が１位に順位付けされています。

機密情報などが情報漏えいし、悪用されることよって企業の事業継続が困難になったり、膨大な対策費用が必要となります。

1位	標的型攻撃による機密情報の窃取	6位	予期せぬIT基盤の障害に伴う業務停止
2位	内部不正による情報漏えい	7位	不注意による情報漏えい（規則は遵守）
3位	ビジネスメール詐欺による金銭被害	8位	インターネット上のサービスからの個人情報の窃取
4位	サプライチェーンの弱点を悪用した攻撃	9位	IoT機器の不正利用
5位	ランサムウェアによる被害	10位	サービス妨害攻撃によるサービスの停止

出典：IPA 『情報セキュリティ −10大脅威2020-』から

被害事例

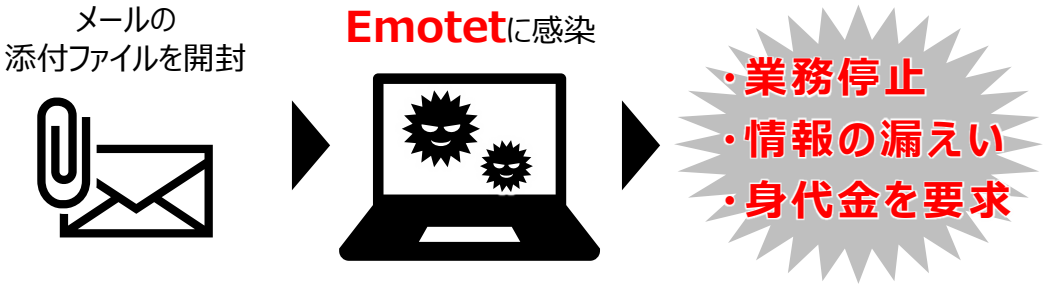
某製造業会社では、サイバー攻撃により国内外の工場で生産を一時停止する事態に陥りました。
同社のサーバーが外部から攻撃を受けたことで、社内ネットワークにウイルスが拡散され従業員のパソコンに感染。
メールシステムや業務システムに接続できない事態となり、原因の特定や対策ができずパソコンの利用を停止し、業務継続ができなくなりました。

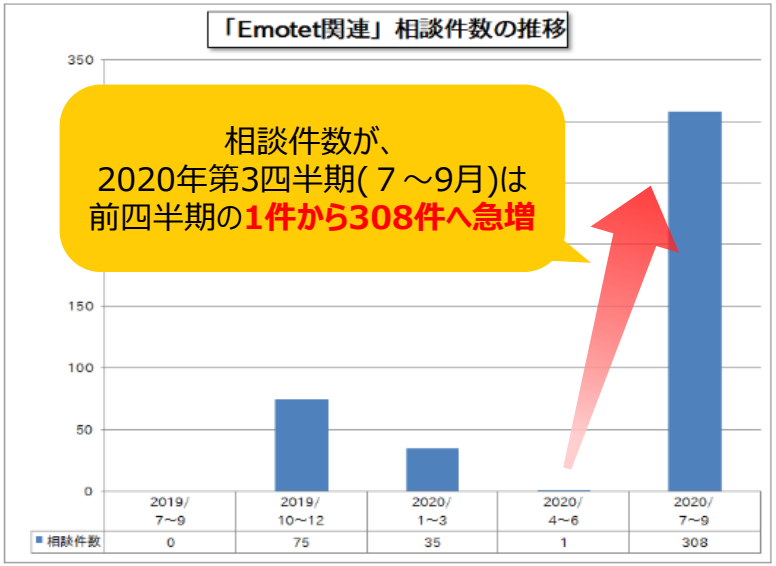
1．標的型攻撃の被害

HITACHI
Inspire the Next

Emotetの被害が多数発生しています。

近年、特定の組織内の情報を狙った標的型攻撃が増加傾向にあり、特に猛威を奮っているEmotetは、確認されている限りでは、そのほとんどが「なりすましメール」を介して感染するマルウェアの一種です。





引用:
https://www.ipa.go.jp/security/txt/2020/q3outline.html

攻撃者の手口は日々進化し、新たな脅威が生まれています

被害事例

取引先を装ったメールの添付ファイルを開いたことで、パソコン がEmotet に感染。感染に気付かず当該パソコンからさらに組織内外へウイルスメールが送信され、他の従業員が当該メールの添付ファイルを開いたことで感染源が広がり、業務停止、情報流出などに発展しました。

HITACHI
Inspire the Next

2.「今すぐ」、そして「これから」のシステム課題

2.「今すぐ」、そして「これから」のシステム課題

HITACHI
Inspire the Next

新型コロナウイルス感染症の完全終息が見えない中、今後、働き方についても
「新しい生活様式（ニューノーマル）」へ移行していきます。
生活様式が新しくなるということはシステムにも新しい課題が浮上します。
さまざまな企業が、下記のようなシステム課題に直面しています。

今すぐ

新型コロナウイルス感染症の拡大が懸念されている中、**テレワークができる環境**を早急に整えたい

テレワーク環境の早期立ち上げ

今すぐ～これから

急遽テレワークを導入したが、**社内だけで行っていた業務の運用レベルをテレワーク環境下でも確保したい**

テレワーク環境下での運用レベル維持

・テレワーク環境下で、**不正な作業をしていないかを確認**したい
・**未知のマルウェア**への対策をしたい

テレワーク環境下の不正監視/ウイルス対策

３．ソリューション内容

3-1 ソリューションが解決する課題

HITACHI
Inspire the Next

今すぐ

社内業務を在宅勤務で実施するため、
まずはテレワーク環境を導入

リモートアクセスツール　D Mobile

社内の自席パソコンを安全にリモートで操作することで、在宅勤務が可能になった

課題

- 自宅の端末は社内から物理的に切り離されているため、異なるポリシー設定や対策が必要
- 広域網を利用している場合、端末ごとに悪意あるトラフィックを抑止するエンドポイントセキュリティが重要

今すぐ~これから

左記課題を解決するため、マルウェアの不正な行為を監視・遮断するエンドポイントセキュリティの導入

エンドポイントセキュリティ　APPGUARD

✓悪意のある不正プログラムの実行を防止し、OSの中枢部を悪意のある行為から守る

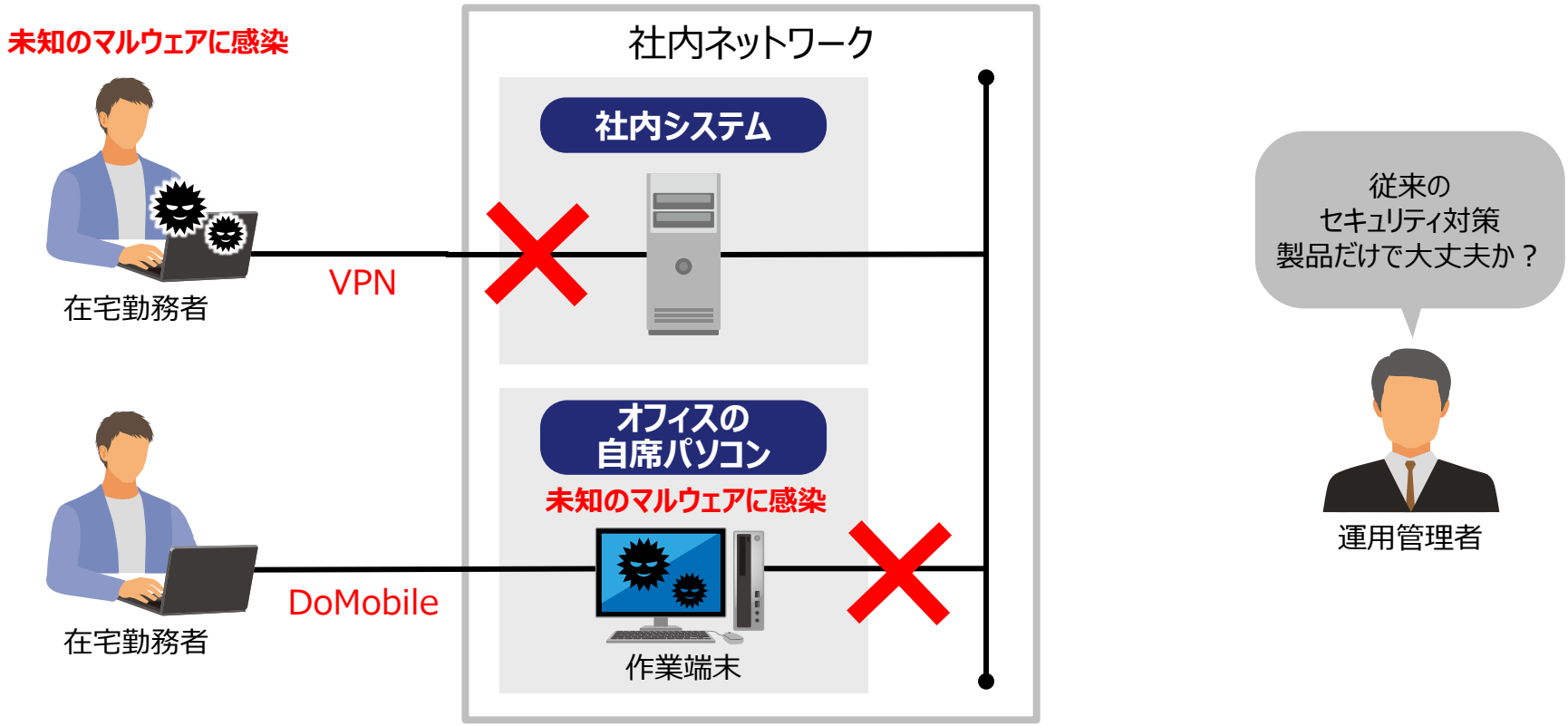
✓標的型メールなどでマルウェアに感染しても、システムを正常に動作・機能させ、不正な行為をプロセスレベルで未然に阻止

テレワーク環境下でも従来社内で行っていた標的型攻撃対策が可能になります!

3-2 ユースケース（今まで）

在宅勤務者は、社内ネットワークにリモートアクセスして業務に従事している。

作業端末が従来のウイルス対策製品では検知できない未知のマルウェアに感染した場合に、感染の拡がりを防ぐためにパソコンの電源やネットワークを断つと、代わりの端末や環境を準備するまで業務が停止してしまう。

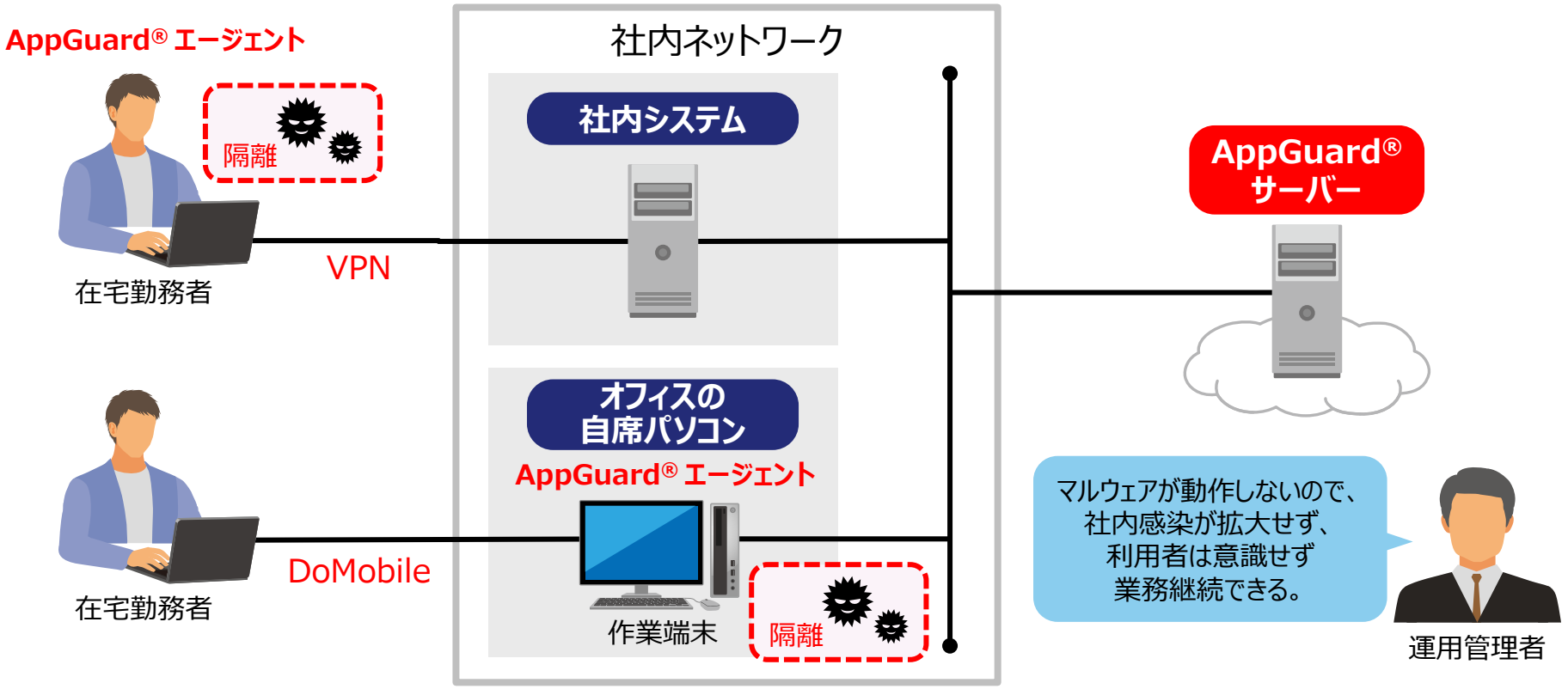


HITACHI
Inspire the Next

テレワーク向け標的型攻撃対策ソリューションを適用

作業者の端末に「AppGuard®エージェント」、
クラウド上のメーカー準備のAppGuard®サーバー」を利用

① 未知のマルウェアに感染した場合は隔離し、害を与える動作を無効化
② 従来の検知型対策製品で必要だった定義ファイルの更新が不要

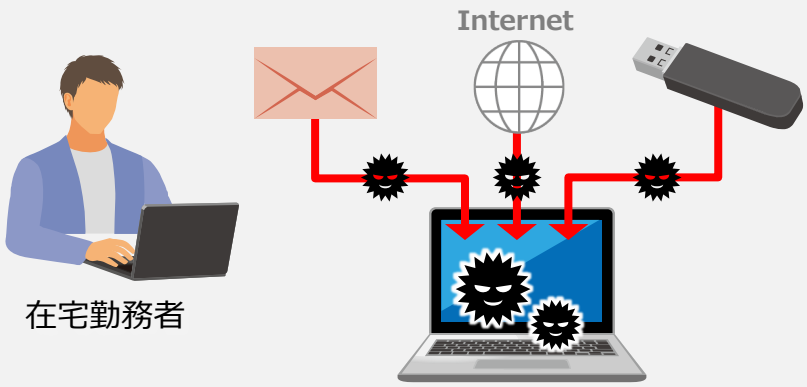


3-3 リモートワークで発生する問題事例①（未知のマルウェアに感染）

HITACHI
Inspire the Next

Before

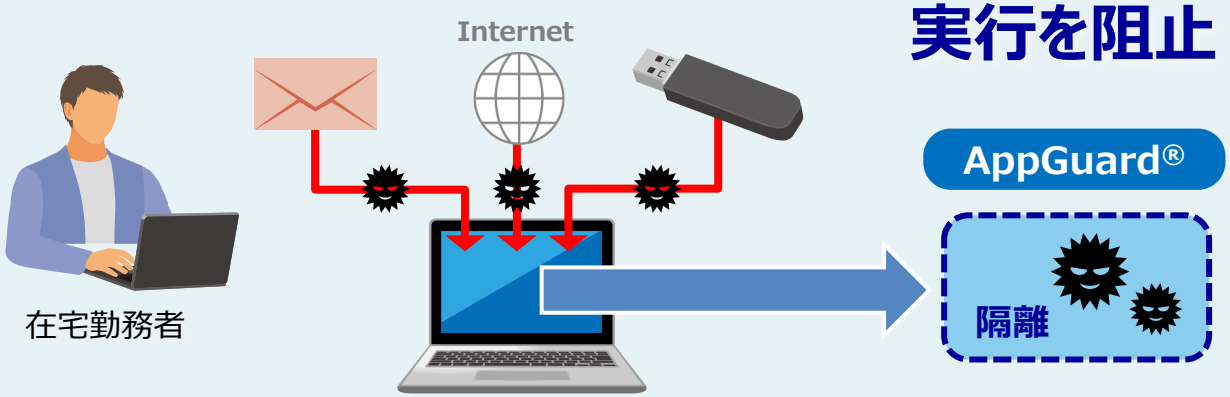
外部から**未知マルウェア**が侵入



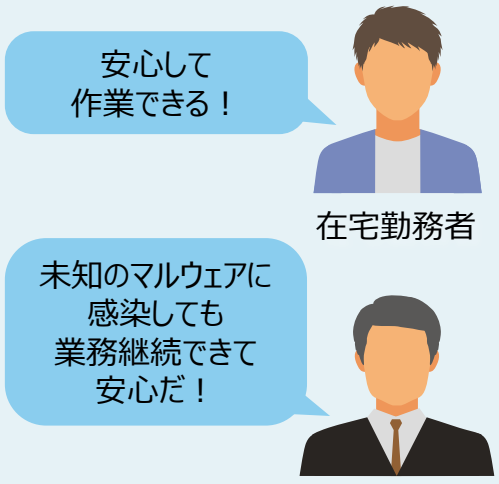
従来製品では**駆除できない**

After

外部から**未知マルウェア**が侵入



AppGuard®が
隔離し
実行を阻止



４．ソリューション構成

4-1 ソリューションの提供形態

HITACHI
Inspire the Next

「テレワーク向け標的型攻撃対策ソリューション」は、
2製品で構成しています。

DoMobile	リモートアクセスを実現する製品
AppGuard®	未知のマルウェアなどの最新の脅威であっても、システムに害を与える動作を未然に阻止する機能を提供する製品

(1)DoMobileはASPサービス版とオンプレミス版(CSE版)の2形態から選択が可能です。
(2) AppGuard®の提供形態はサブスクリプション版となります。(ライセンス形態は使用許諾、保守)

本ソリューションはリモートアクセス製品としてDoMobileの導入が必須ではありません。
既に別のリモートアクセス製品を導入されているお客さまにおいても、
「テレワーク向け標的型攻撃対策ソリューション」の適用が可能です。

HITACHI
Inspire the Next

テレワーク向け標的型攻撃対策ソリューションのサービスメニュー

サービス	概要	
導入支援サービス（DoMobileASP版）	トレーニング	AppGuard® Enterprise 運用管理者向けトレーニング ※別途、DoMobileASPサービス購入が必要
導入支援サービス（DoMobileCSE版）	トレーニング	AppGuard® Enterprise 運用管理者向けトレーニング
	環境構築	・DoMobileCSEサーバー　1台 ・DoMobileエージェント　1台
導入支援サービス	トレーニング	AppGuard® Enterprise 運用管理者向けトレーニング

※上記の他、管理対象や利用人数、導入形態に応じた「AppGuard®」「DoMobile」のライセンス購入が必要となります。

サービス	概要
サポートサービス（DoMobileASP版）	ソリューションサポート問い合わせ（2製品の一次切り分け含む） ※別途、DoMobileASP／AppGuard®サービス購入が必要
サポートサービス（DoMobileCSE版）	ソリューションサポート問い合わせ（2製品の一次切り分け含む） ※別途、DoMobileCSEサポート／AppGuard®サービス購入が必要
サポートサービス	ソリューションサポート問い合わせ　※別途、AppGuard®サービス購入が必要

4-3 動作環境

HITACHI
Inspire the Next

■システム全体構成

リモート端末 ⇔ DoMobile ※1 ※2 ⇔ 運用端末 ⇔ AppGuard®サーバー

■動作環境

リモート端末 ※1	パソコン	Microsoft Windows系のパソコン ブラウザにWindows Internet Explorer 9/10/11、Microsoft Edge、Google Chrome、Mozilla Firefoxのいずれかが必要
	タブレット	iPadOS/Android/Windows
	スマートフォン	iOS/Android
DoMobileサーバー ※1 ※2		Debian Linux 9 [amd64] サーバー
運用端末（自席端末）［AppGuard®エージェント］		WindowsXP SP3以降（2023年8月まで対応） Windows 7,Windows8および8.1,Windows10,
AppGuard®サーバー		クラウド(メーカー準備)

※1 リモートアクセスにDoMobileをご利用頂く場合の動作環境です。
※2 DoMobileサーバーは、DoMobile CSE版をご利用の場合のみ必要となります。

お問い合わせ

HITACHI
Inspire the Next

株式会社 日立ソリューションズ・クリエイト

Webでのお問い合わせ

www.hitachi-solutions-create.co.jp/contact/solution.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。

メールでのお問い合わせ

hsc-contact@mlc.hitachi-solutions.com

表示に関する注意事項

HITACHI
Inspire the Next

■他社商品名、商標などの引用に関する表示

- Linuxは，Linus Torvaldsの米国およびその他の国における登録商標あるいは商標です。
- Google Chromeは、Google LLCの商標または登録商標です。
- Microsoft Windows、Internet Explorer、Microsoft Edgeは、米国、その他の国における米国Microsoft Corp.の登録商標です。
- iOSはApple Inc.のOS名称です。IOSは米国その他の国におけるCiscoの商標または登録商標であり、ライセンス許諾を受けて使用されています。
- Androidは、Google LLC の商標です。
- Firefoxは、Mozilla Foundationの米国およびその他の国における商標または登録商標です。
- AppGuard®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。

■サービス・製品の仕様に対する表示

本資料に記載しているサービス・製品の仕様は、2025年4月現在のものです。

サービス・製品の改良などにより予告なく記載されている仕様が変更になることがあります。

■お問い合わせ情報について

お問い合わせ情報についてご相談・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（共同利用も含む）することがあります。
取り扱いには十分注意し、お客さまの許可なく他の目的に使用することはありません。