セキュリティにリソースをさけない企業も鉄壁に守るサービスでテレワーク環境を万全に
-HP Proactive Securityのご紹介-

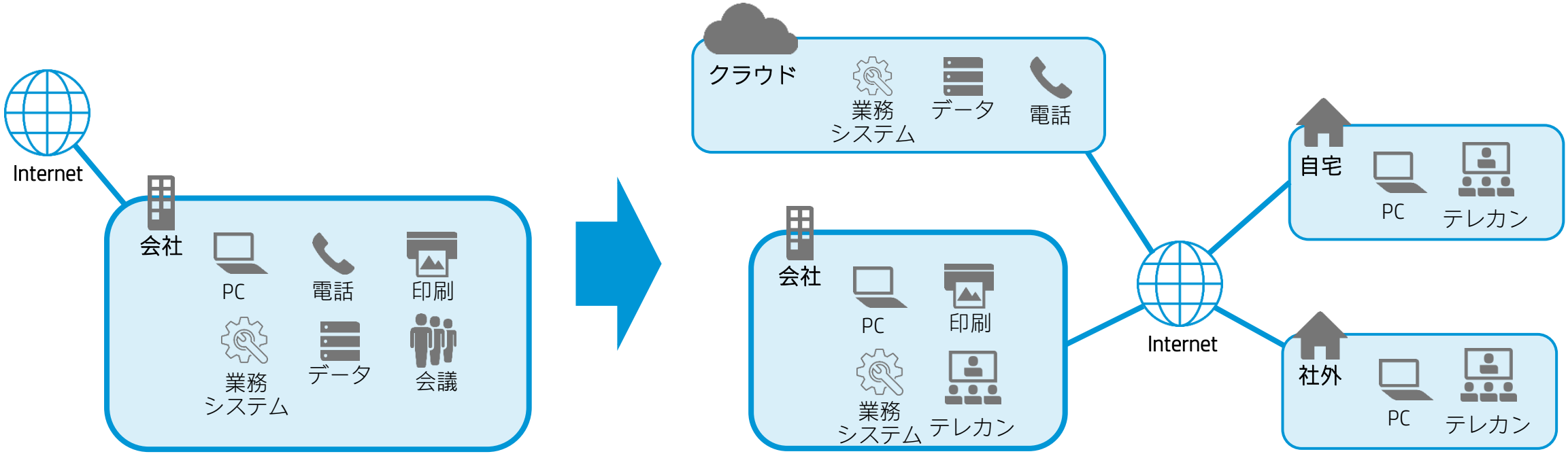
株式会社　日本HP
サービス・ソリューション事業本部
クライアントソリューション本部

本日のAgenda

- テレワークにおけるWindows10 PCのセキュリティ
- PC（エンドポイント）セキュリティの重要性
- 最新のサイバー攻撃に対する準備

テレワークにおけるWindows10 PCのセキュリティ

テレワークはどんどん進む！



- いままで：会社の階層防御で守られた環境でみんながアクセス
- これから：クラウドの利用、自宅インターネット、社外ネットワークからアクセス
  ＝PCは常時守られたネットワークにいるわけではない

テレワーク時のPCのセキュリティを整理

- Windows 10の更新プログラムを最新にしておく。
- アンチウイルスソフトをインストールし、定義ファイルを更新しておく。

→ マルウェア攻撃対策

- HDD暗号化
- プライバシーフィルターを貼る。
- MDMの導入
- ログインパスワードの設定しておく。

→ 情報漏洩対策

- RDP （Remote Desktop Protocol）やVDI（ Virtual Desktop Infrastructure）の利用
- VPN（Virtual Private Network）の利用

→ 社内システムへ安全にアクセス

対策はこれだけで大丈夫でしょうか・・・？

PC（エンドポイント）セキュリティの重要性

エンドポイントは攻撃の最初の入り口

70%

セキュリティ侵害がエンドポイントから始まる割合

99%

エンドポイント攻撃のうち、Eメール、Web、チャット、USBを経由した攻撃の割合

57%

従来型アンチウィルスが見逃したエンドポイント攻撃の割合

時間経過と攻撃の進化

マルウェア「Emotet」が復活、知人からのメール装う手口に警戒を

知人や取引先などを装って相手をだまし、マルウェア「Emotet」に感染させようとするメールが、再び大量送信されている。

2020年07月21日 09時07分 公開　[鈴木聖子，ITmedia]

Emotetは知人や取引先などを装ったメールで相手をだまし、添付ファイルを開かせる手口で感染するマルウェア。2018年から2019年にかけて猛威を振るい、日本企業でも被害が多発していた。

2020年に入ってしばらく影を潜めていたが、Microsoftは同年7月17日のツイートで「今回のキャンペーンではこれまでのところ、数万通のメールに仕込まれた数百件の添付ファイルとリンクが確認された。ダウンロード用のURLが改ざんされたWebサイトを指し示しているのは、Emotetの特徴を表している」と指摘した。

人間の心の弱さを狙う手口、具体的には？

セキュリティ企業のMalwarebytesによると、今回の攻撃でも以前と同様に、メールに記載したリンクをクリックさせたり、添付ファイルを開くよう仕向けたりする手口が使われている。それまでにやり取りしていたメールの返信を装うなどして相手をだまそうとする手口も変わらない。

添付ファイルには高度に難読化されたマクロが仕込まれており、マクロを有効にするとPowerShellが起動して、Emotetのコードを外部のWebサイトからダウンロードする。

デンマークのセキュリティ企業CSISの研究者ピーター・クルーズPeter Kruse氏によると、感染メールは欧州や北米を中心に、日本などでも出回っている様子だ。

MalwarebytesはEmotetについて「攻撃者が別のマルウェアを操る集団と手を組んで、ランサムウェアなどに感染させる目的で利用されることもある。特に警戒が必要だ」と指摘している。

出典：IT Mediaエンタープライズ 2020/7/21 記事
https://www.itmedia.co.jp/enterprise/articles/2007/21/news057.html#utm_source=ent-mag&utm_campaign=20200722

1.5ヶ月後

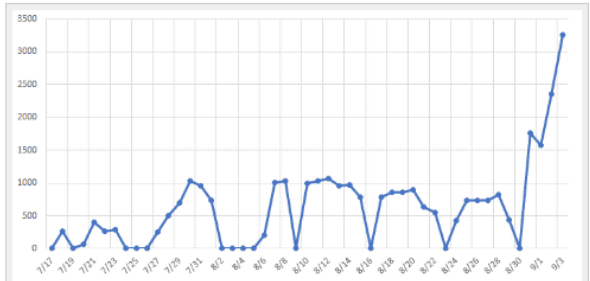
マルウェア「Emotet」の新たな攻撃手法を確認、パスワード付きZIPファイルで検出回避

正規のメールから窃取した添付ファイルを悪用する事例も

植田 陽香　2020年9月8日 19:14

マルウェア「Emotet（エモテット）」の感染拡大と新たな攻撃手法を確認したとして、一般社団法人JPCERTコーディネーションセンター（JPCERT/CC）が4日、注意喚起を行った。

JPCERT/CCでは、Emotetに感染し、感染拡大を試みるスパムメール送信に悪用される可能性のある国内ドメイン「.jp」のメールアドレスの急増および感染拡大を確認しているという。



「Emotet」に感染し、メール送信に悪用される可能性のある国内ドメイン「.jp」のメールアドレスの推移

Emotetとは、Wordファイルなどの添付ファイルまたは本文中にリンクを含むメールを主な感染経路とし、情報窃取とスパムメールを用いた感染拡大などを実行するマルウェア。添付ファイルまたはリンクからダウンロードされるファイルを実行すると、マクロやコンテンツの有効化を促す内容が表示され、有効化するとEmotetの感染に繋がる恐れがある。

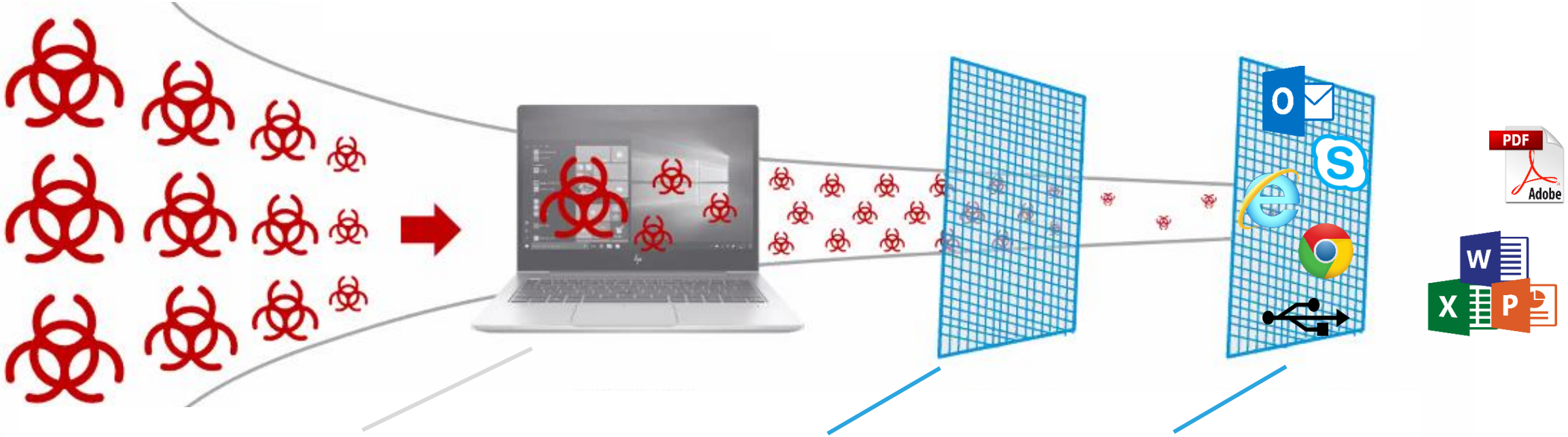
しかし、7月に配布活動再開が確認されて以降、手口が巧妙化しており、新たにメール本文中にパスワードが記載されたパスワード付きZIPファイルが添付される事例が確認された。この場合、メール配信経路でのセキュリティ製品による検知や検疫をすり抜け、従来のWord形式ファイルをセキュリティ製品により防いでいた受信者に対してもメールが配信されてしまうことが想定されるという。

出典：Internet Watch 2020/9/8 記事
https://internet.watch.impress.co.jp/docs/news/1275519.html

- 攻撃者は、まず1台のPCから入り込み、社内システムにアクセスするための情報盗み出します。
- しばらく潜伏した後、重要な情報を入手し、システムをダウンさせたり、身代金を要求したりします。
- 自社の損害だけで終わらず、取引先との関係にも影響します。
- 攻撃は日に日に高度になります。
- 従来のセキュリティ製品は検知に依存しています。
- 検知は必ず失敗します…

最新のサイバー攻撃に対する準備

HP Proactive Securityの守り方



従来型アンチウイルス

シグネチャで検知できる
脅威を保護

例.Windows Defender
(Windows10 Pro標準)

超高精度ディープラーニングAI

従来型アンチウイルスが見逃した
未知の脅威をマルウェア実行前に
防御

HP Sure Sense Advanced

アプリケーション隔離技術

ユーザーの操作による（Webサイト
からのダウンロードファイルやE
メール添付ファイル）
マルウェア実行を隔離

HP Sure Click Advanced

HP Proactive Securityとしてクラウドサービスで提供
専用サービス窓口による設定・分析支援付

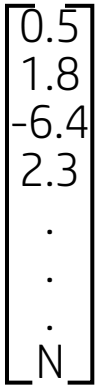
HP Sure Sense Advanced（深層学習型アンチウイルス）

マシンラーニング VS ディープラーニング

マシンラーニング（機械学習）

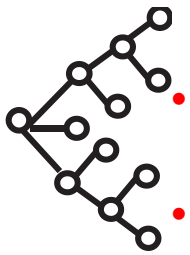
生データ

人がマニュアルで
特徴抽出



特徴における
ベクトル化

学習



- 使われるのはデータ全体の2%以下
- 人による定義
  ↓
- 誤検知
- モデル更新の必要性

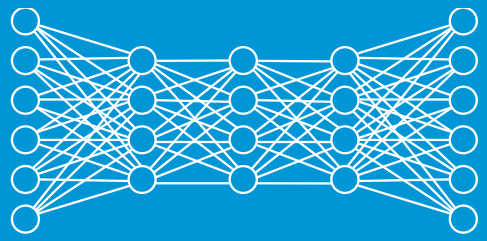
ディープラーニング（深層学習）

生データ

そのままディープラーニングのフレームワークへ

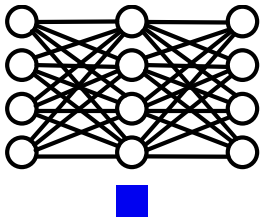
使われるのは100% のデータ

学習



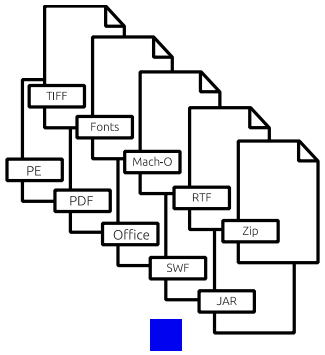
高精度の判定
（検知率が高く誤検知が低い）
（更新頻度も抑制）

HP Sure Sense Advancedのメリット



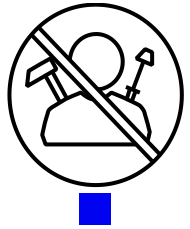
PREDICT / 高精度の予測

作成されたモデルによる高精度の判定
（検知率が高く誤検知が少ない）



ANY FILE / どんなファイルも

PE以外にもPDFやOffice、RFT、SWFなど
数多くのファイルに対応
ファイルレス攻撃にも対応
レピュテーション解析・振る舞い検知も活用

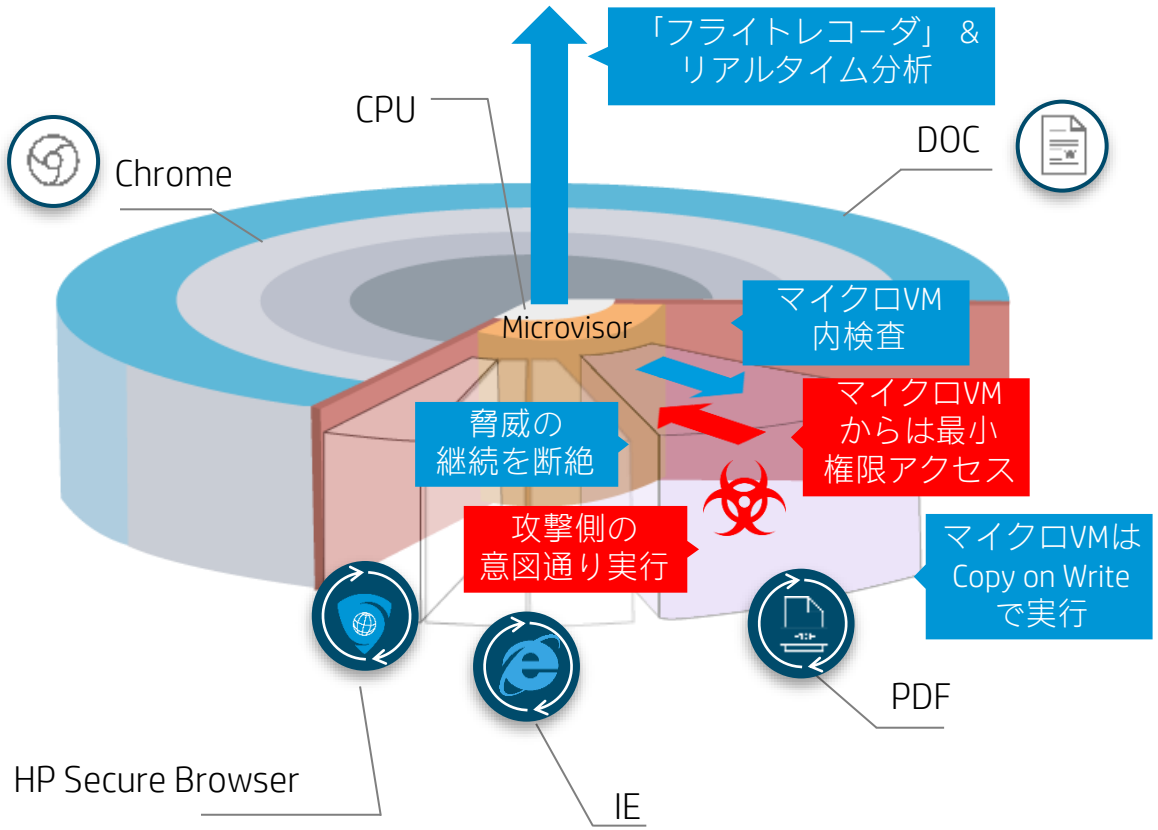


AUTONOMOUS / 自律的動作

自動的に脅威をブロックした上で
分類（説明）までエンドポイントで即時実行

HP Sure Click Advanced （アプリケーション隔離）

インテル® VTを活用したアプリケーションの “隔離”



インテル® VTの利用により、ハードウェアレベルでアプリケーションを隔離実行

メモリ内にマイクロ仮想マシン（VM）を瞬時に作成し、単一のアプリケーションを隔離して実行できるようにする

マイクロVMは都度生成の使い捨てでアプリケーションが終了する際に同時に消滅する

信頼できるファイルとリンクは通常どおり実行されるが、信頼されないファイルとリンクは「コンテナ」に分離され、マイクロVMで実行

マイクロVM内でのドキュメントの編集が可能。ローカルにも保存が可能。ユーザ負担を最小限にとどめながら強力な保護を実装。

HP Sure Click Advanced （アプリケーション隔離技術）のメリット

IT管理者様

- 悪意のあるや添付ファイルやURLリンクからの人的エラーに対して保護するため、メール訓練や注意して開封する等の、ユーザーへのセキュリティ教育が削減できます。
- マルウェア等に感染しない状態でセキュリティ侵害に気づけるため、対処が楽です。

ユーザー操作面

- Eメール、Webサイトを安心して、通常と変わらない利用ができます。

HP管理サービスのメリット（IT管理者様向け）

HPセキュリティ専門家による管理

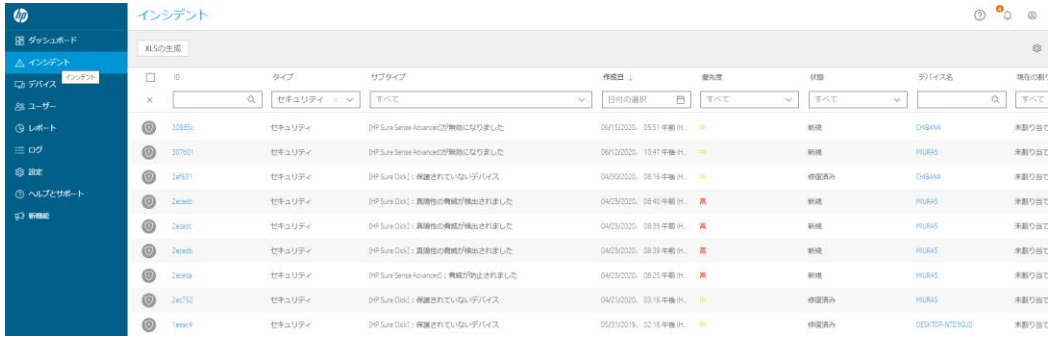
- HPのセキュリティ専門家が、セキュリティポリシーの調整および設定をします。
- 真陽性の脅威が検出された場合のインシデントの分析をします。
- HP Sure Click Advancedで、ゼロデイ攻撃の脅威が捕捉された場合の詳細な分析レポートを提供します。

分かりやすいダッシュボードとレポート

- HPが管理するクラウドサーバからダッシュボード画面を提供します。
- 専門知識がなくても社内PCの状態を把握できます。
- レポートからインシデント内容を簡単に確認できます。

ダッシュボード

統合インシデントレポート



まとめ

HP Proactive Securityは・・・

- ディープラーニング型アンチウィルスが、超高精度に端末を保護
- アプリケーション隔離技術で、うっかり開いてしまっても大丈夫
- サーバー設置不要、社内ネットワーク接続不要
- 定義ファイル更新不要
- 設定変更代行、ゼロデイ攻撃分析サービス付、高度なセキュリティ知識不要
- HP PC以外も対応。Win10 PCならどこのメーカーでもOK。

最新のサイバー攻撃から強力にWindows10 PCを守るサービス

「HP Proactive Security」1年間 8,000円（税抜）/1デバイス

オンラインセミナー視聴者様限定・実証実験プログラムのお知らせ

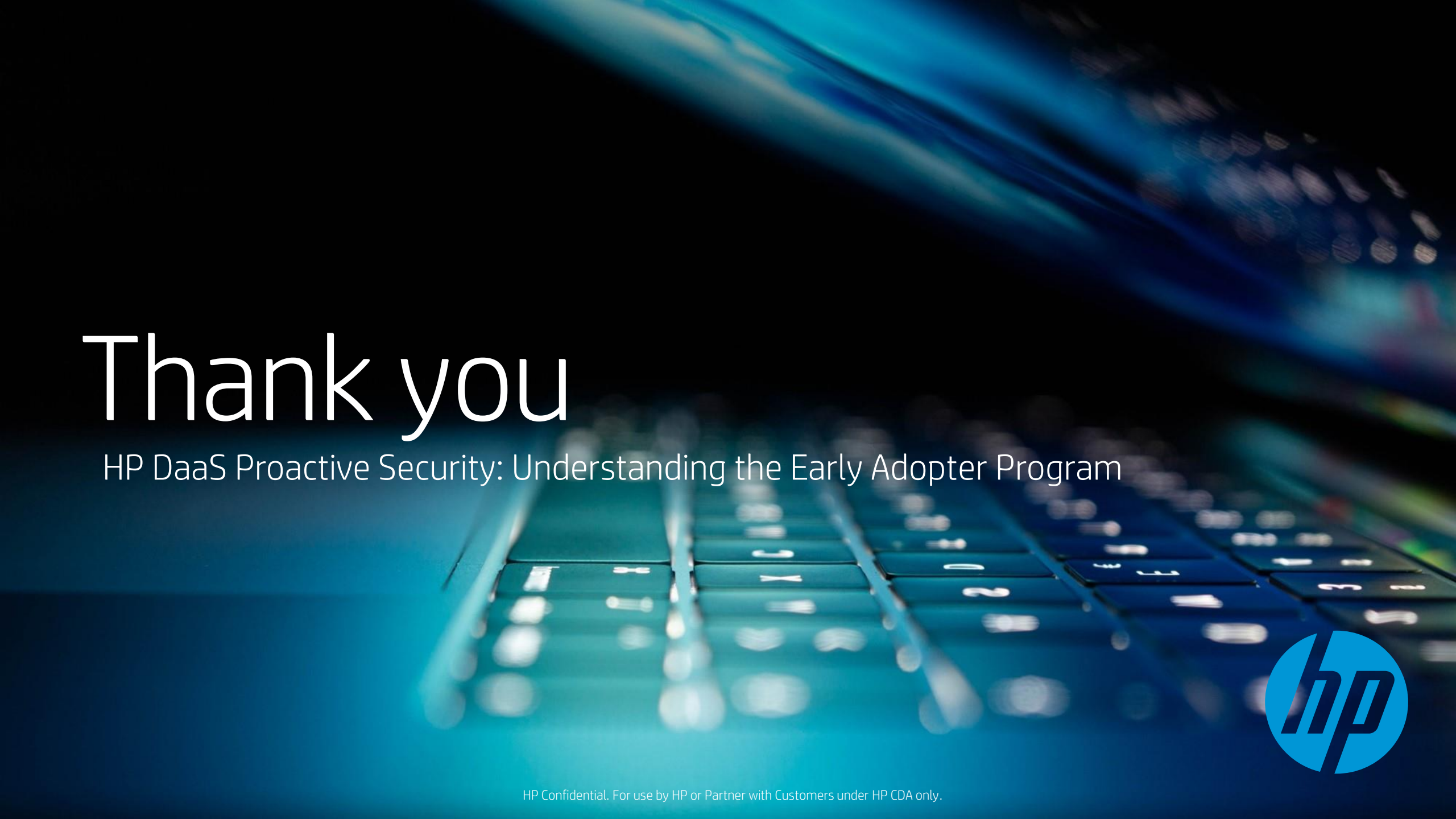
<u>抽選で5法人様へ「HP Proactive Security」 実証実験環境を無償ご提供致します。</u>

■ 参加要項

20台のWindows10 PCと、インターネット環境をご用意頂ける法人様

OS要件：Windows10 Version 1903以降
ハードウェア要件：Intel Core i3以上(Intel VT)、メモリ8GB以上、ストレージ空き6GB以上
※メーカーや機種は問いません。

■ 実施期間
3ヶ月間



Thank you

HP DaaS Proactive Security: Understanding the Early Adopter Program