

ハイブリット環境に最適！ PCのセキュリティリスクを大幅に削減する方法とは？



HP WOLF SECURITY

株式会社 日本HP
クライアントソリューション本部 ソリューション営業部
淵上 弘士



HP WOLF SECURITY

医療業界の課題と セキュリティ



医療機関における課題

安全で費用対効果の高い医療を提供することに注力

7% ~ 10%

全世界で医療関連感染症に冒された患者は、先進国で7%、発展途上国で10%¹

53%

2019年にハッキングされた全世界の医療機関の割合²

1,290万

2035年までに世界的に不足する医師、看護師、その他の医療従事者の人数³

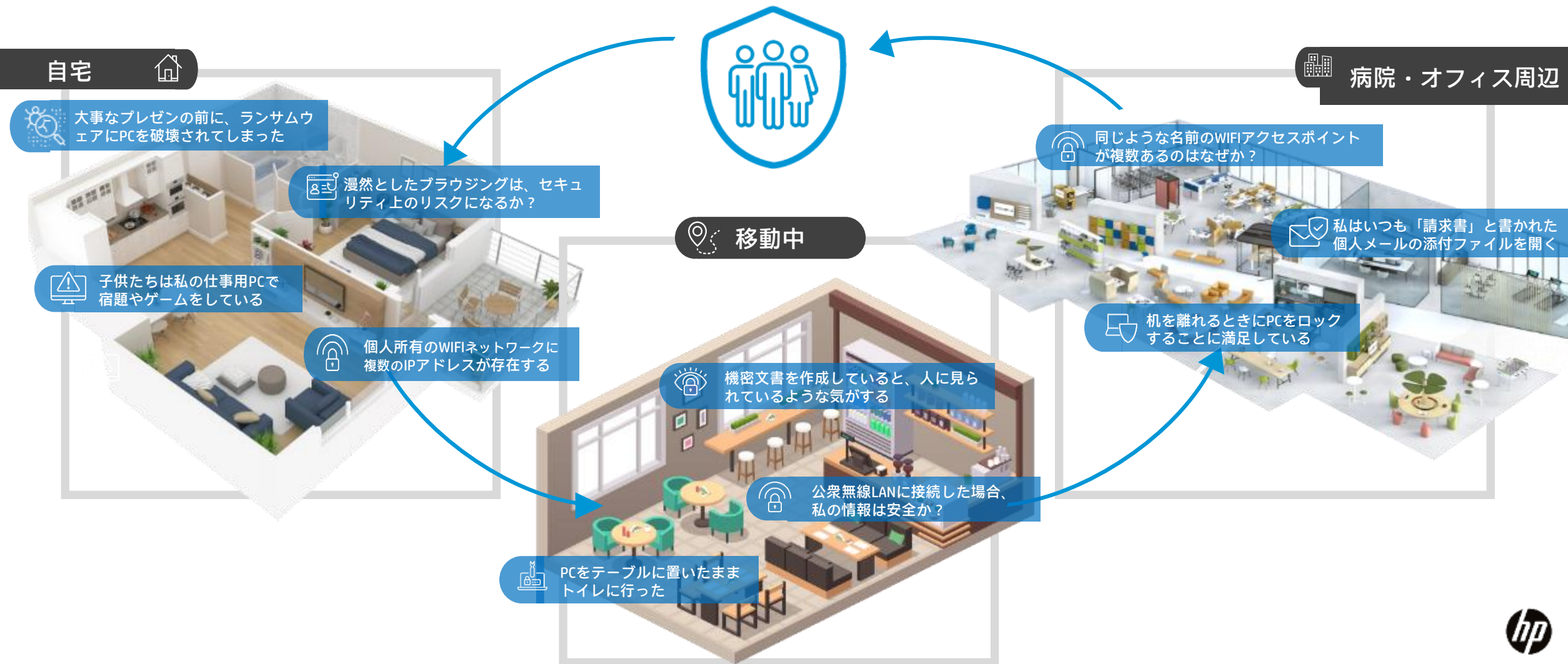
出典：1.WHO：どの時点においても、入院患者100人ごとに、先進国では7人、発展途上国では10人が少なくとも1つの医療関連感染症（HAI）に冒されています。 http://www.who.int/gpsc/country_work/gpsc_ccisc_fact_sheet_en.pdf

2. Keeper Security：サイバーセキュリティ会社のKeeper Securityは、世界の医療機関の3分の2近くがその存続期間中にサイバー攻撃を受け、53%が過去12か月以内に攻撃されたことを明らかにしました。 <https://cisomag.eccouncil.org/more-than-half-global-healthcare-organizations-suffered-a-cyberattack-last-year/#:~:text=More%20Than%20Half%20Global%20Healthcare%20Organizations%20Suffered%20a%20Cyberattack%20Last%20Year,-By&text=Keeper%2C%20in%20its%20report%20%E2%80%9C2019,employee%20records%20lost%20or%20stolen>

3. WHO：2035年までに全世界で1,290万人の医療従事者が不足します。今日、その数は720万人になります。： <https://www.who.int/mediacentre/news/releases/2013/health-workforce-shortage/en/>



ハイブリッドワークにおけるセキュリティの課題

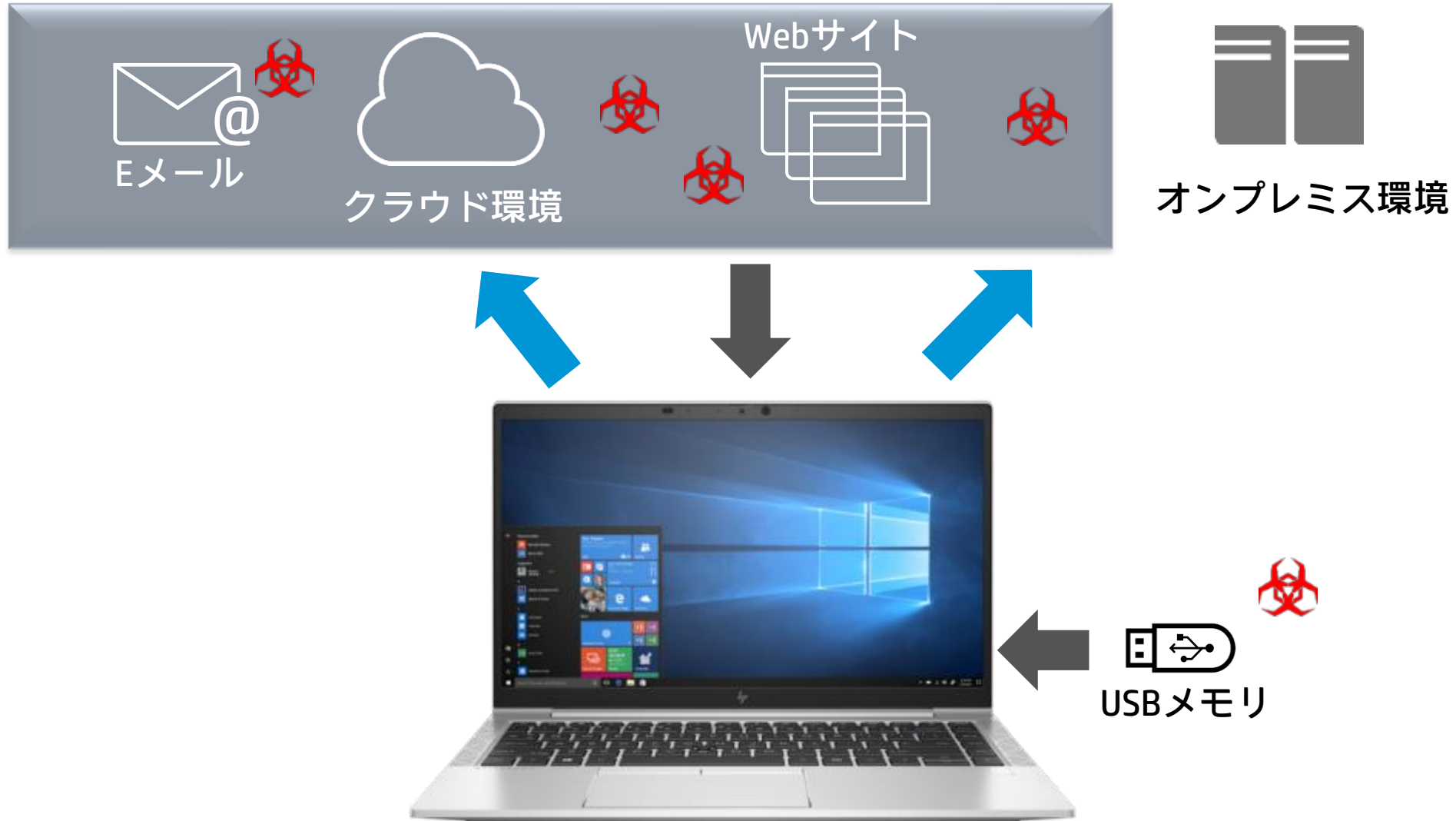


管理対象となるエンドユーザーの脆弱性や脅威のベクトルが増加



HP WORLDWIDE SECURITY

PCデバイスが、全ての入り口になります



最新のサイバー攻撃の進化



57%

アンチウィルスが見逃した
エンドポイント攻撃の
割合¹

¹ Ponemon Institute 2018 State of Endpoint Security Risk sponsored by Barkly, October 2018

アンチウィルスだけでは十分ではありません。
企業、組織は追加の防御策を必要としています。



HP WORLDWIDE SECURITY



HP WOLF SECURITY

セキュリティリスクを 大幅に削減する HP Wolf Security





HP WOLF SECURITY

新世代のエンドポイントセキュリティ

包括的なサイバーレジリエンスを提供する
セキュリティポートフォリオ



包括的なエンドポイントの保護と
レジリエンスの強化

ハードウェアによる保護から、
ソフトウェアとサービスまで



サイバーリスクに対処する、
ITとセキュリティ部門の負担を軽減

ユーザーが常に安全に働くことができる



セキュリティは、HPのDNAに組み込まれている

20年以上にわたるエンドポイント・セキュリティの革新

エンドポイントセキュリティの業界標準を設定

TPM、BIOS、Firmware Resilienceの標準を確立

TRUSTED[®]
COMPUTING
GROUP

NIST
National Institute of
Standards and Technology



Bromiumの買収

HPの業界におけるリーダーシップ強化



HP WORLDWIDE SECURITY

セキュリティリスクを削減する多層防御

脅威

毎月50億の固有の脅威

従来型
アンチウイルス



Windows10 Pro標準の
Windows Defender

マルウェア防止と
脅威封じ込め保護



HP WOLF PRO SECURITY



HP WOLF SECURITY

キーワードは、 トリプルプロテクション



脅威封じ込め機能

①



マルウェア防止

②



アイデンティティ保護

③

① 脅威封じ込め機能



HP Sure Click Pro

検出を必要としない保護



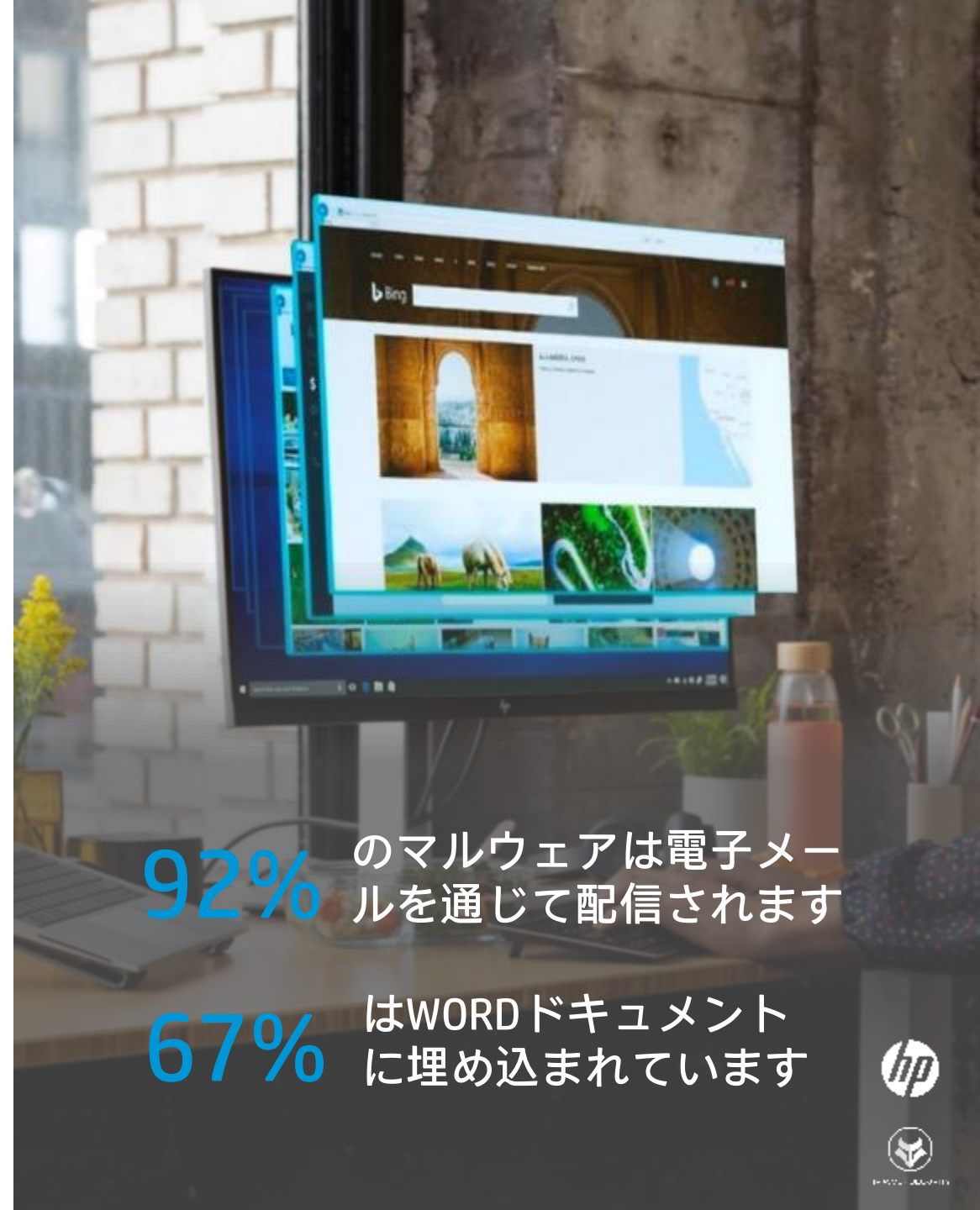
安全なブラウジング

- タブごとに安全なマイクロVMに隔離します。
HP Secure Browser



ファイル保護

- 電子メールの添付ファイルの保護、Word、Excel、Power Point、PDFファイルを安全なマイクロVMで開きます。
- IE、Edge、Chrome、Firefoxを使用してダウンロードしたファイルを安全なマイクロVMで開きます。
- USBメモリのような外部ストレージ経由のファイルを安全なマイクロVMで開きます。



92%

のマルウェアは電子メールを通じて配信されます

67%

はWORDドキュメントに埋め込まれています



© 2014 HP Development Company, L.P.

仮想化技術の第一人者による高度で独自のテクノロジー



Ian Pratt
Global Head of Security for Personal Systems,
HP Inc.

Xenプロジェクトをリードしたイアン・プラットが、仮想化技術ノウハウを活かして独自のセキュリティ技術を開発。

2011年にBromium社を設立、セキュリティ効果を飛躍的に向上させ、65件以上の特許を取得。

2019年9月、HP Inc.がBromiumを買収、現在イアン・プラットはHP Inc. セキュリティ事業責任者



②マルウェア防止



HP SURE SENSE

AIの力を利用して未知のマルウェアを防止します



行動分析

悪意のある動作の特定とブロック



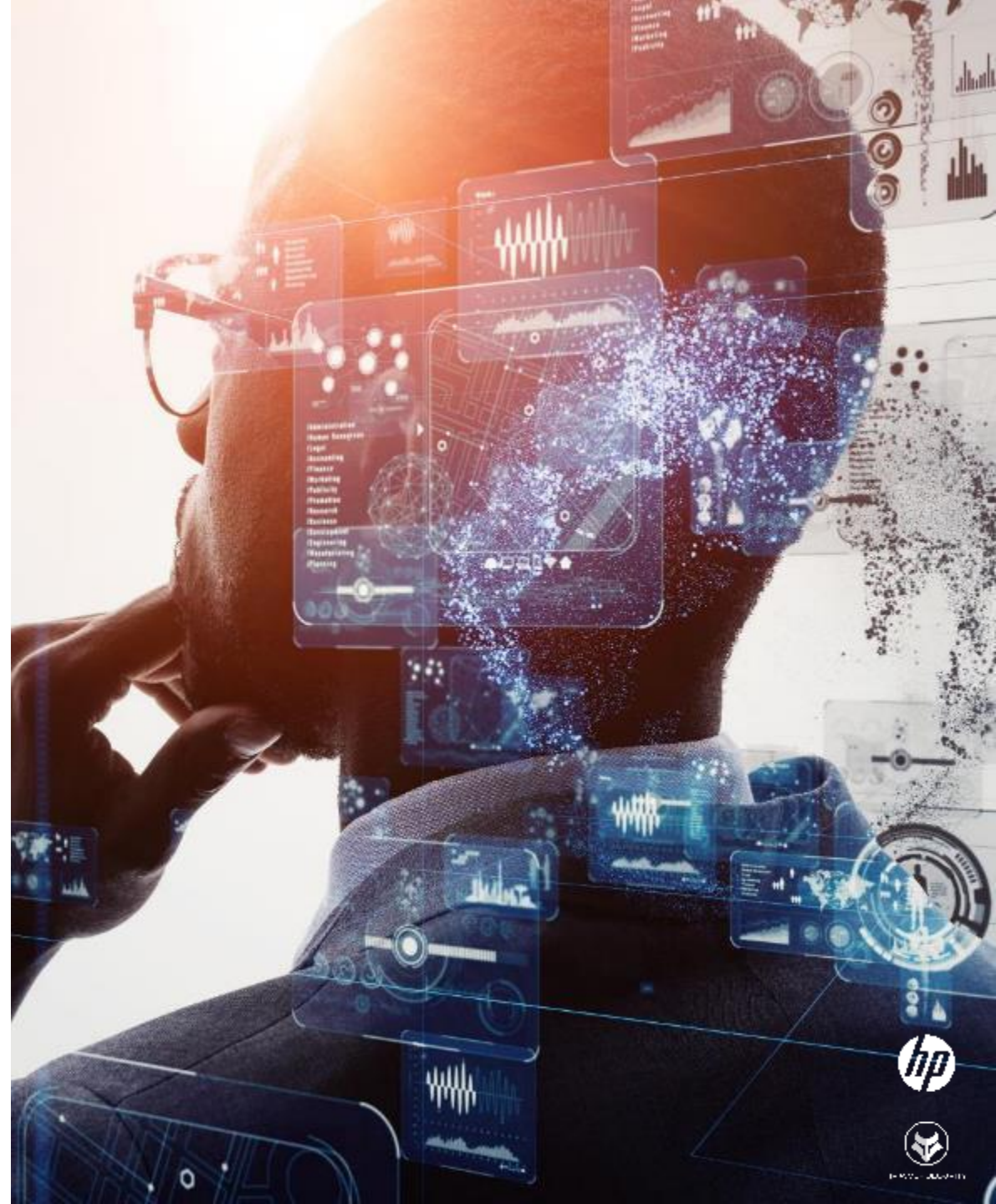
AI: マシンラーニング

マルウェアの一般的な機能を認識するように訓練されたAI



AI: ディープラーニング

未知のマルウェアでさえ直感的に認識するために生データで訓練されたAI



③ アイデンティティ保護



Amazon お客様

残念ながら、あなたのアカウント Amazon を更新できませんでした。
これは、カードが期限切れになったか、請求先住所が変更されたなど、さまざまな理由で発生する可能性があります。

アカウント情報の一部が誤っている故に、お客様のアカウントを維持するため Amazon 情報を確認する必要・があります。今アカウントを確認できます。

[Amazon ログイン](https://www2.amazon.co.jp) <https://www2.amazon.co.jp.●●●●.co/>

なお、24時間以内にご確認がない場合、誠に遺憾ながら、アカウントをロックさせていただきます。

アカウントに登録のEメールアドレスにアクセスできない場合
お問い合わせ： Amazonカスタマーサービス。

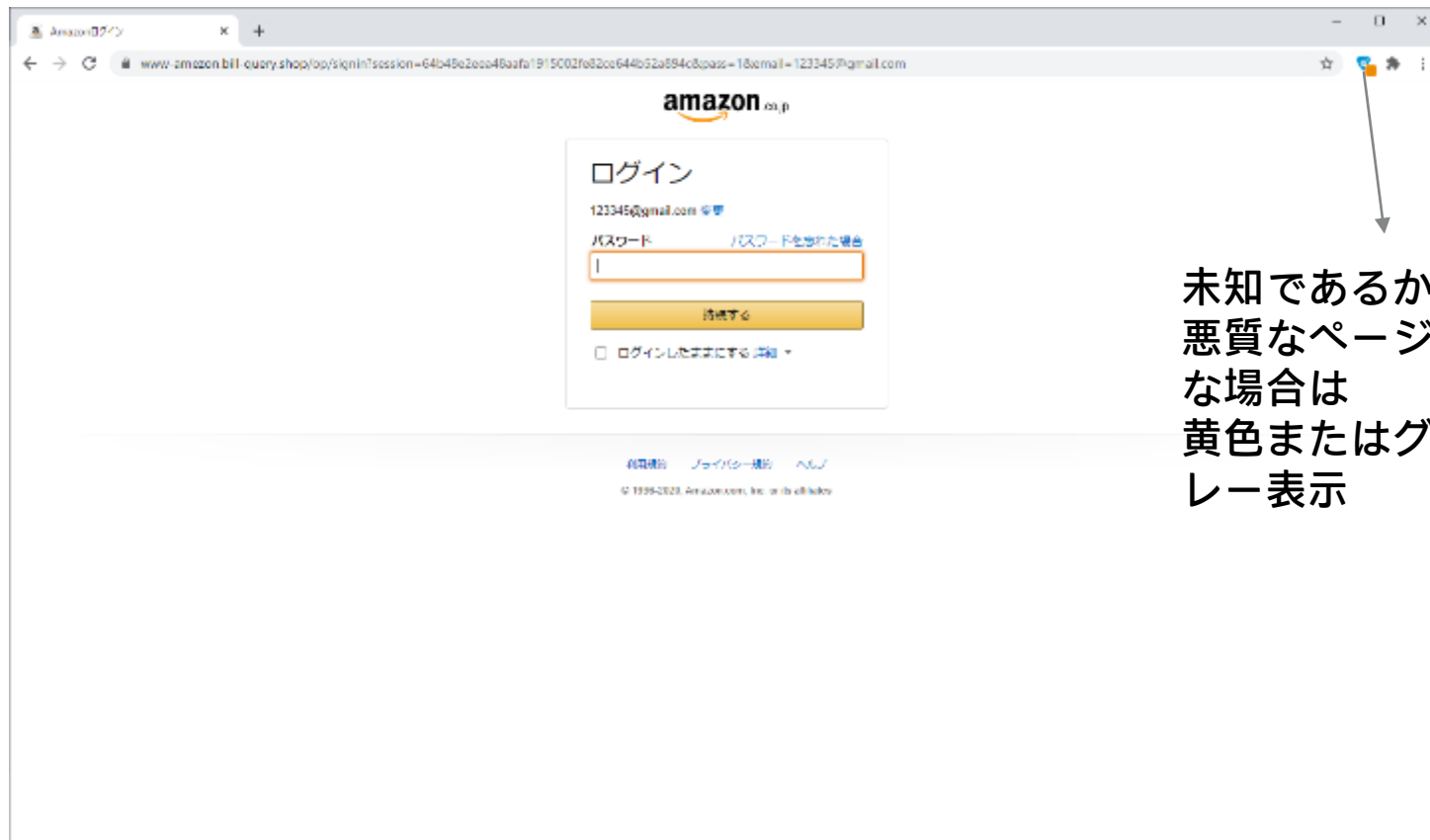
お知らせ:

- パスワードは誰にも教えないでください。
- 個人情報と関係がなく、推測しにくいパスワードを作成してください。大文字と小文字、数字、および記号を必ず使用してください。
- オンラインアカウントごとに、異なるパスワードを使用してください。

どうぞよろしくお願いいたします。

Amazon

Amazon をかたるフィッシングメール



未知であるか
悪質なページ
な場合は
黄色またはグ
レー表示

Amazon のフィッシングサイト



HP WORLDWIDE SECURITY


③ アイデンティティ保護

Amazonログイン

www-amezon.bill-query.shop/op/signin?session=64b48e2eea48aafa1915002fe82ce644b52a894c&pass=1&email=123345@gmail.com

amazon

ログイン

 **警告: アイデンティティ盗難の可能性**

HP Identity Protectionは以前に表示されていない認証ページを発見しました。

このページは偽物で、IDを盗もうとしている可能性があります。

www-amezon.bill-query.shopが安全であると確信している場合:

次の操作が可能です

[引き続き認証情報を入力する](#) または

[入力を無効化して安全を確保し、このページを閉く](#)

このタブを安全に閉じることができます。

hp

HP IDOL.1 SECURITY

未知であるか
悪質なページ
な場合は
黄色またはグ
レー表示

③ アイデンティティ保護

既知の不正なページ

HP Identity ProtectionはこのフィッシングWebページを無効化しました。

ログイン詳細情報やパスワードなどを盗むためにrakuten.co.jp.bbodek.shopが以前使用されていました。

[安全な状態に戻る](#)

アイデンティティ盗難に伴うリスクを理解している場合は、[入力を無効化してこのページを開くを続行](#)できます。

[このタブを安全に閉じることができます。](#)

HP
HP WORLDWIDE SECURITY

HP独自のハードウェアが実現する レジリエントなデバイス

HPエンドポイントセキュリティコントローラ (ESC)

保護はPCの最下位レベルから

- ✓ HPのPCのみに搭載されているハードウェア強化技術
- ✓ パワーオフの時も、ESCは常に動作
- ✓ ハードウェア・ルート・オブ・トラスト：保護、検知、回復
- ✓ 物理的に独立している

ランタイム時も保護を継続

- ✓ HPのセキュリティシステムの健全性を継続的に監視
- ✓ HP Wolf Securityの暗号機能をハードウェアで保護

第三者認証

認定された政府の
独立試験機関が認証



HP Sure Start



HP Sure Run



HP Sure Recover



主な機能:

以下のファームウェア及び重要データの自己回復

- BIOSコード
- BIOS設定
- MBR
- SMM (System Management Mode)
- インテルME (Management Engine)

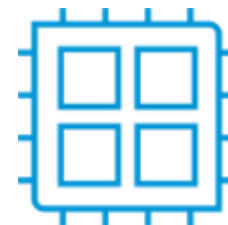
HP SURE START

世界で唯一の 自己回復BIOS

他社はBIOS攻撃の際に予防もしくは

検知 まで

HP SURE START は **復旧** まで



HP WORLDWIDE SECURITY

HP SURE RUN

PCのセキュリティ 対応機能を強固に保つ

攻撃者に対抗する:

- 主要なプロセスを監視
- 意図しない変更を警告
- 停止したプロセスを自動的に再スタート
- 停止が続く場合にはPCをネットワークから隔離



主な機能:

重要なプロセスの監視、警告、再スタート

- セキュリティ関連
 - CryptographicService
 - Software Protection
 - Windows Security Center
 - Windows Firewall
 - Windows Defender
- コアOS関連
 - DCOM Server Process Launcher
 - Remote Procedure Call(RPC)
 - Windows Event Log
- 管理関連、ネットワーク関連、HPセキュリティ機能等

HP Wolf Pro Security Serviceのマネージドサービス構成

※2022年4月頃リリース予定

HP Sure Sense Pro
(シュアセンスプロ)



次世代AVで
感染を防止

HP Sure Click Pro
(シュアクリックプロ)



アプリ、ファイル、
ブラウザを
隔離起動
し感染を防止



クラウド
ダッシュボード

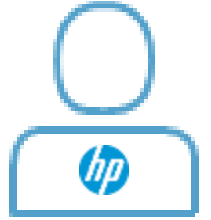


ダッシュボード
レポート
インシデント管理



サービス
エキスパート

電話・メール
サポート



セキュリティ
エキスパート

管理・分析
レポート

管理コンソールはクラウドサービスとして提供
次世代AVもアプリ隔離もパソコンの中で動作します
(サーバ不要)



HP WOLF PRO SECURITY

まとめ

ハイブリッドの環境ではエンドポイントデバイス対策がカギ
クラウドベンダ様はエンドポイント対策に責任を持たない。

その課題を解決するのが “HP Wolf Security”



HP WOLF SECURITY



HP WOLF SECURITY

THANK YOU

