高度化するサイバー攻撃にハードウェアで対抗！
HP Business PCのセキュリティ機能ご紹介

株式会社日本HP
サービス・ソリューション事業本部
技術本部　クライアント技術部
2018年9月11日

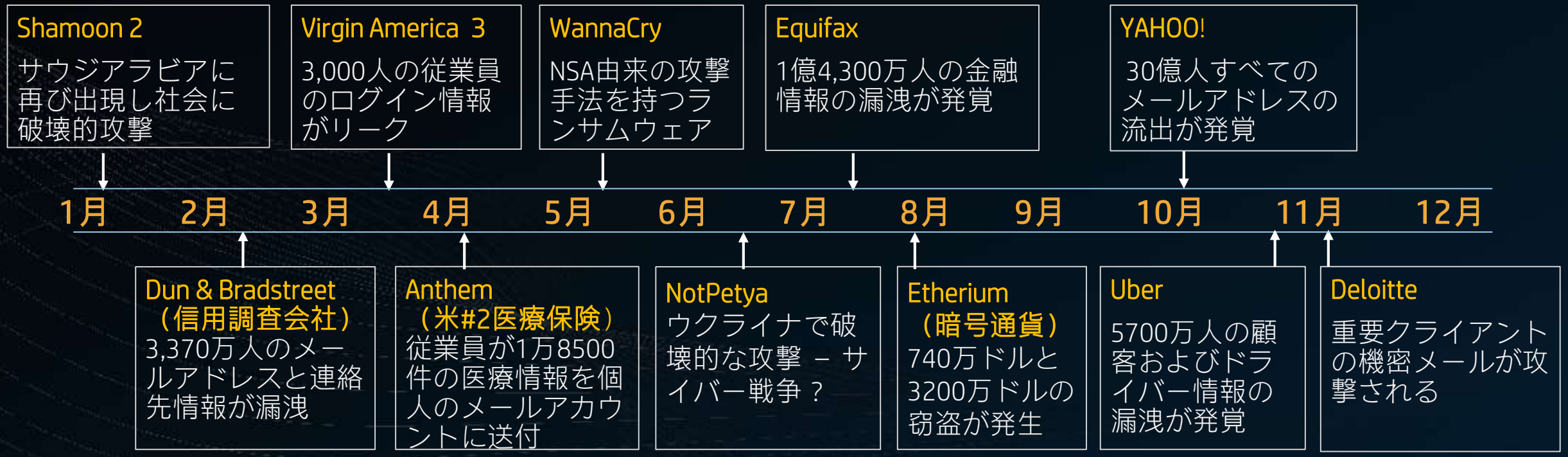
働き方改革が仕事場を脆弱にする

オープンなレイアウト

新幹線,飛行機など移動中

社外の共用スペース

2017年のサイバー攻撃



2017年の第一四半期に**新しいマルウェア**が**4.2秒**ごとに出現

出展：GData, Malware Trends 2017, 2017

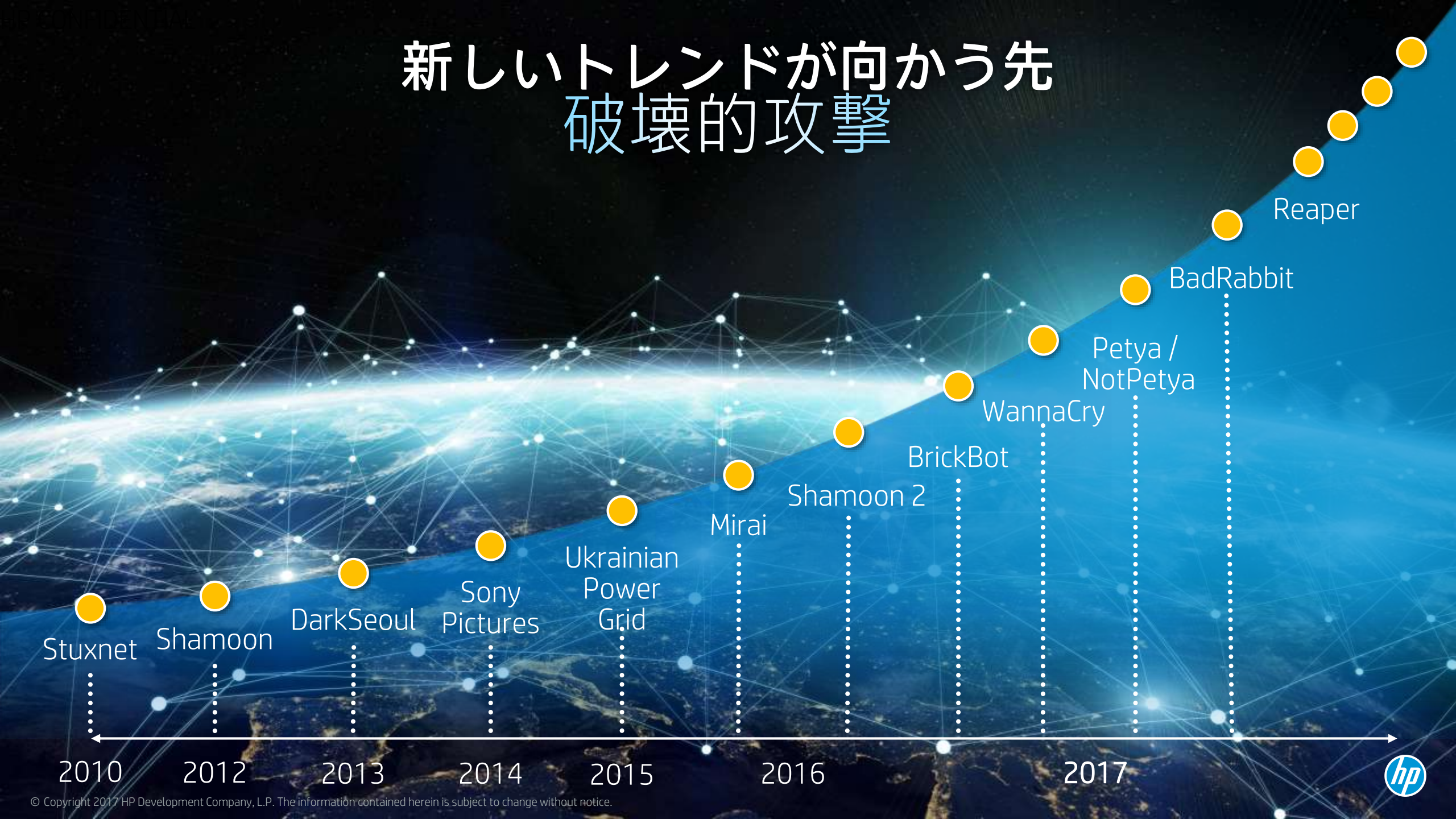
サイバーセキュリティの課題

攻撃者は
進化している

攻撃は
巧妙になっている

問題は攻撃が**成功するかどうか**ではなく、
いつ成功するかということである

新しいトレンドが向かう先
破壊的攻撃



破壊的攻撃の莫大な被害額

2017年の Petya/ NotPetya攻撃後、侵害されたPCの社内標準イメージへのリストアは各PCへの**個人の作業**を要した – このため生産性の大きな損失を招いた

4-7%

調査企業に対するPetya/Not-Petyaによる税引き前逸失利益の割合

4つの大企業の財務諸表に基づく

8億ドル

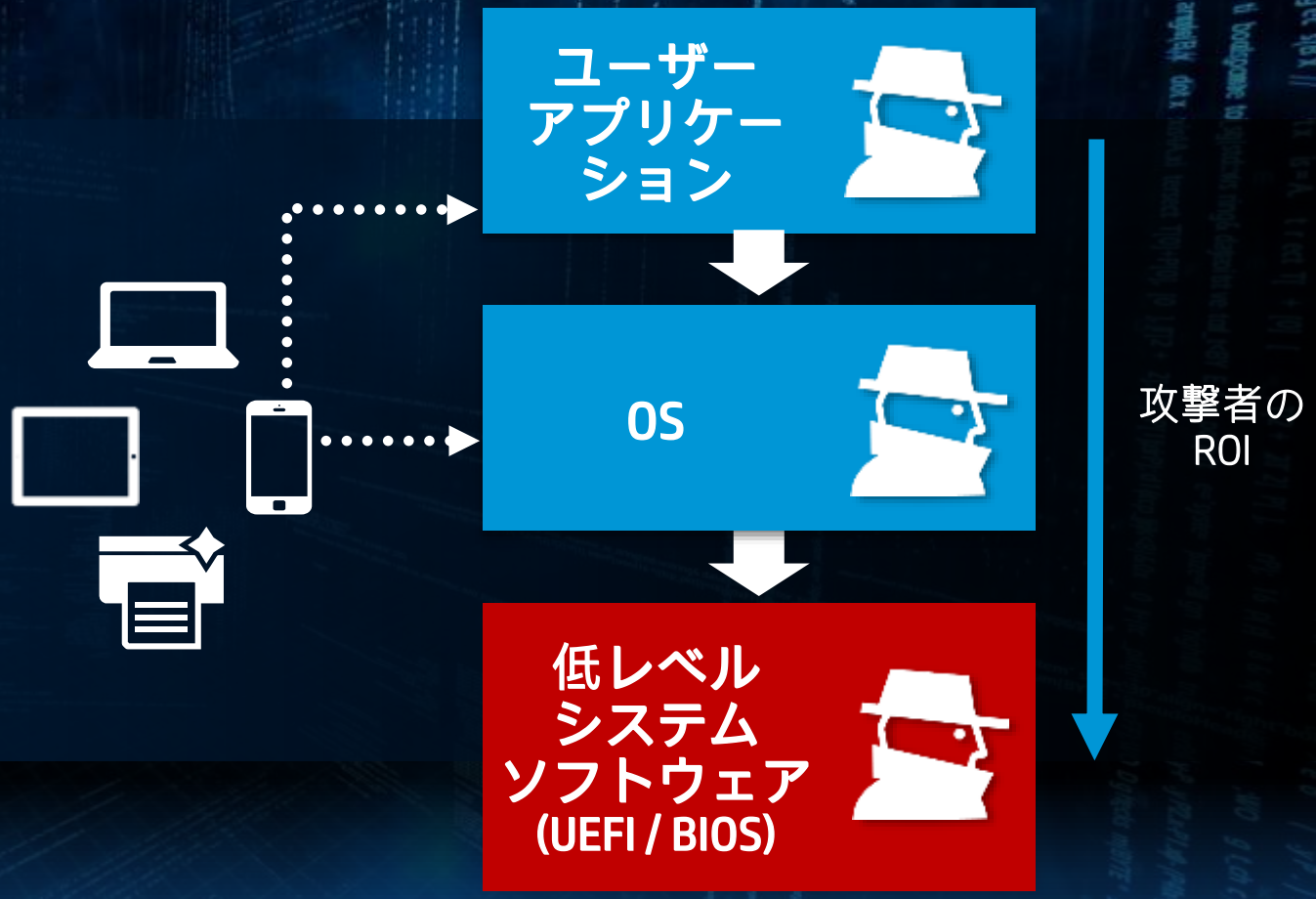
調査企業に対する攻撃の影響による総コスト

4つの大企業の財務諸表に基づく

攻撃の経済性と
最近のマルウェアの技術的傾向

攻撃者のエントリーポイント

- 人を利用した攻撃
- ネットワークを利用した攻撃
- 物理アクセスを利用した攻撃



すでに存在するBIOS攻撃（BIOS Rootkitの例）

“Hacking Team” 2014年

…セキュリティの研究者グループは“Hacking team”がRCS（リモートコントロールシステム）エージェントをターゲットシステムにインストールする際にUFEI BIOS Rootkitを利用していることを発見した。
http://thehackernews.com/2015/07/hacking-uefi-bios-rootkit.html

Mebromi 2011年

…Trojan.Mebromi という脅威はAward BIOSに悪意のあるコンポーネントを追加し、MBRの前段階からシステムの制御を奪うことを可能にする。
http://www.symantec.com/connect/blogs/bios-threat-showing-again

セキュリティをハードウェアに基づかせる

HP Endpoint Security Controller
が可能にするソリューション

ハードウェア基点

自己回復

管理性

予期できない攻撃に対するサイバーレジリエンスの実現

[10] Based on HP's unique and comprehensive security capabilities at no additional cost and HP Manageability Integration Kit's management of every aspect of a PC including hardware, BIOS and software management using Microsoft System Center Configuration Manager among vendors with >1M unit annual sales as of November 2016 on HP Elite PCs with 7th Gen Intel® Core® Processors, Intel® integrated graphics, and Intel® WLAN.

エンドポイントデバイスのレジリエンスを実現する

ソフトウェアイメージ

Webブラウジング

アンチウイルスS/W
OS重要プロセス

MBR/GPT
BIOS/BIOS設定/SMM

HP Sure Recover

HP Sure Click

HP Sure Run

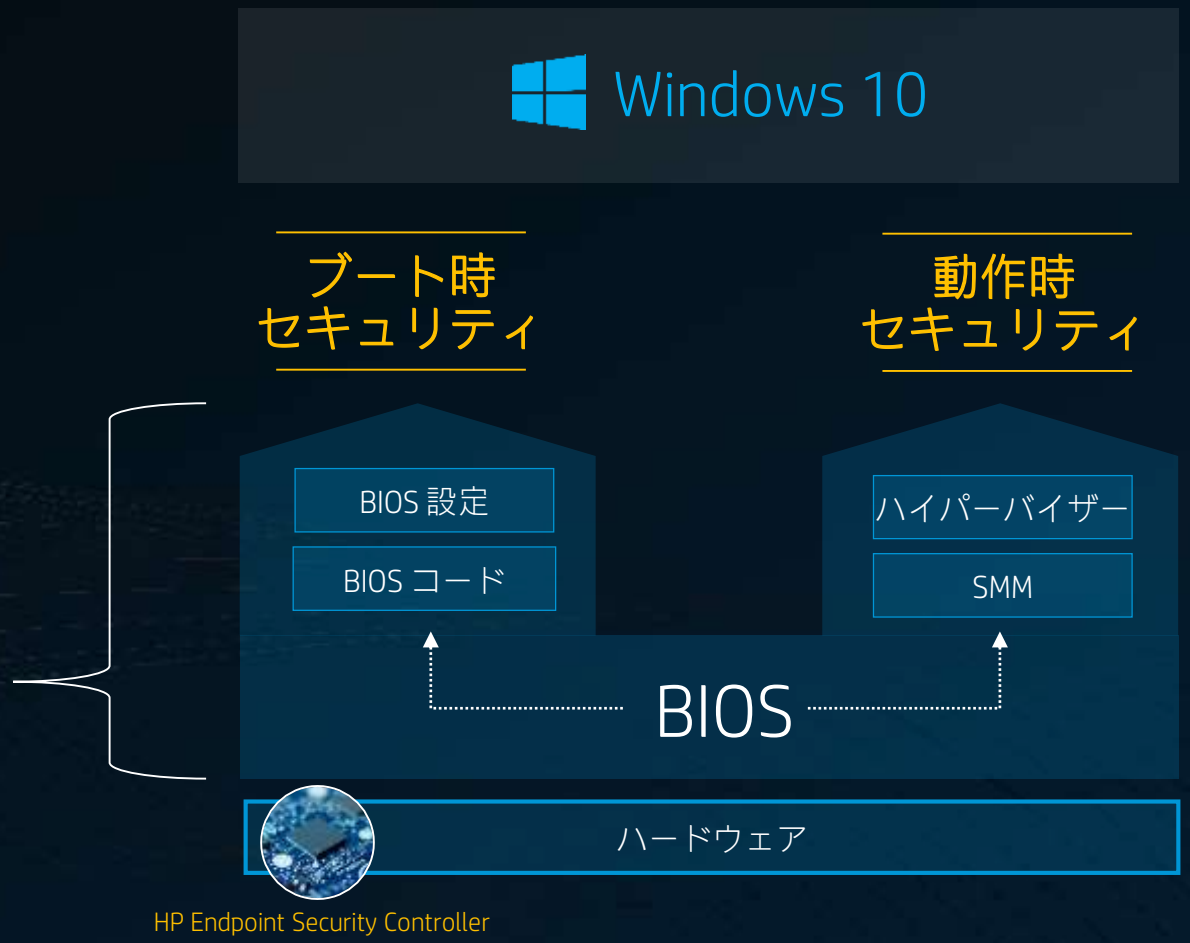
HP Sure Start

自己回復型BIOS HP Sure Start

BIOSとは:
BIOSは起動時に実行される数100万ラインのコードで、PC基盤の重要な要素

どのように扱うべきか?
BIOSが侵害されると、ハッカーはPCを“一番高い権限で操作する”ことができ、他の全ての保護機構は役に立たない

HP Endpoint Security Controllerがブート時のBIOSコード、設定と動作時のハイパーバイザー、SMMへの攻撃に対し保護、検知、復旧を行う



HP Sure Startの歴史

電源投入時のBIOS検証

CPUが起動する前にBIOSの完全性を確認

Windowsイベントログ

HP Sure StartのイベントをWindowsイベントログに収集

リアルタイムBIOS保護

マザーボード上のBIOSを監視し、改ざんが検出された場合は安全なコピーからBIOSをリストア

ランタイム侵入検知 (RID)

RAM内のSMMを監視し、改ざんが検出された場合は安全なコピーからBIOSをリストア

BIOS設定/ポリシー保護

BIOSの設定値、ポリシー、データの保護とリストア

Microsoft SCCMへの統合

Microsoft SCCM+HP Manageability Integration Kitを通じでHP Sure Start Gen3の設定とログを管理

暗号化によるストレージの保護

HP Endpoint Security Controllerのハードウェアベースの完全性と、BIOS設定とユーザーの資格情報の改ざん検出による機密保護

セキュアブートデータベースの保護

OSのセキュアブートの完全性に重要なBIOS内に保存されているデータベースと鍵の保護

インテルマネジメントエンジン（ME）ファームウェアの保護と回復

Sure Startによる保護をデバイスレベルのコードの他の重要なエリアに拡張

HP Endpoint Security Controllerのサードパーティーセキュリティ認定

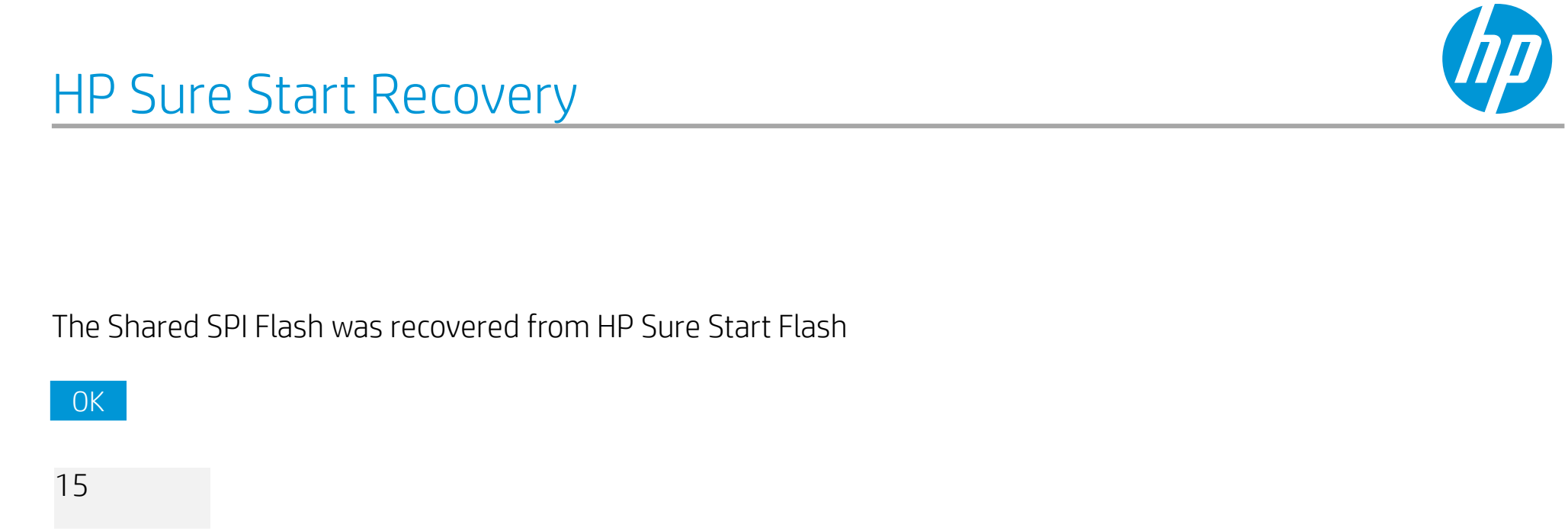
HP ESCハードウェアのコア機能を検証するための独立した認定ラボによるテスト。

Draft NIST Platform Firmware Resiliency guidelines (Special Publication 800-193)

HP Sure Start を搭載したHPビジネスPCはdraft NIST Special Publication 800-193を上回る

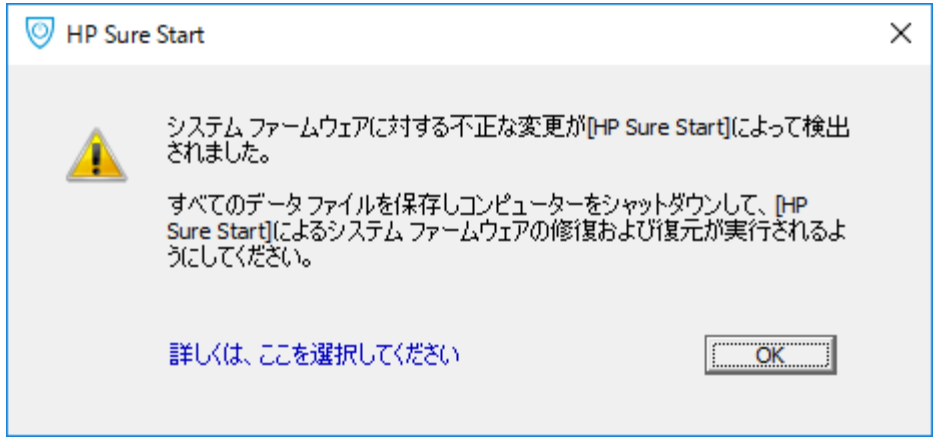
HP Sure Start	HP Sure Start with Dynamic Protection	HP Sure Start Gen3	HP Sure Start Gen4
2014	2015	2016	2018

HP Sure Startによるシステムファームウェアの復元



HP BIOSのGPT復元

HP Sure Startランタイム侵入検知の通知と復元



*ポップアップメッセージによるHP Sure Start Gen3ランタイム侵入検知の通知を行うにはHP Notificationsソフトウェアがインストールされている必要があります。

HP Notifications	HP	2017/02/10	17.7 MB	1.0.22.3

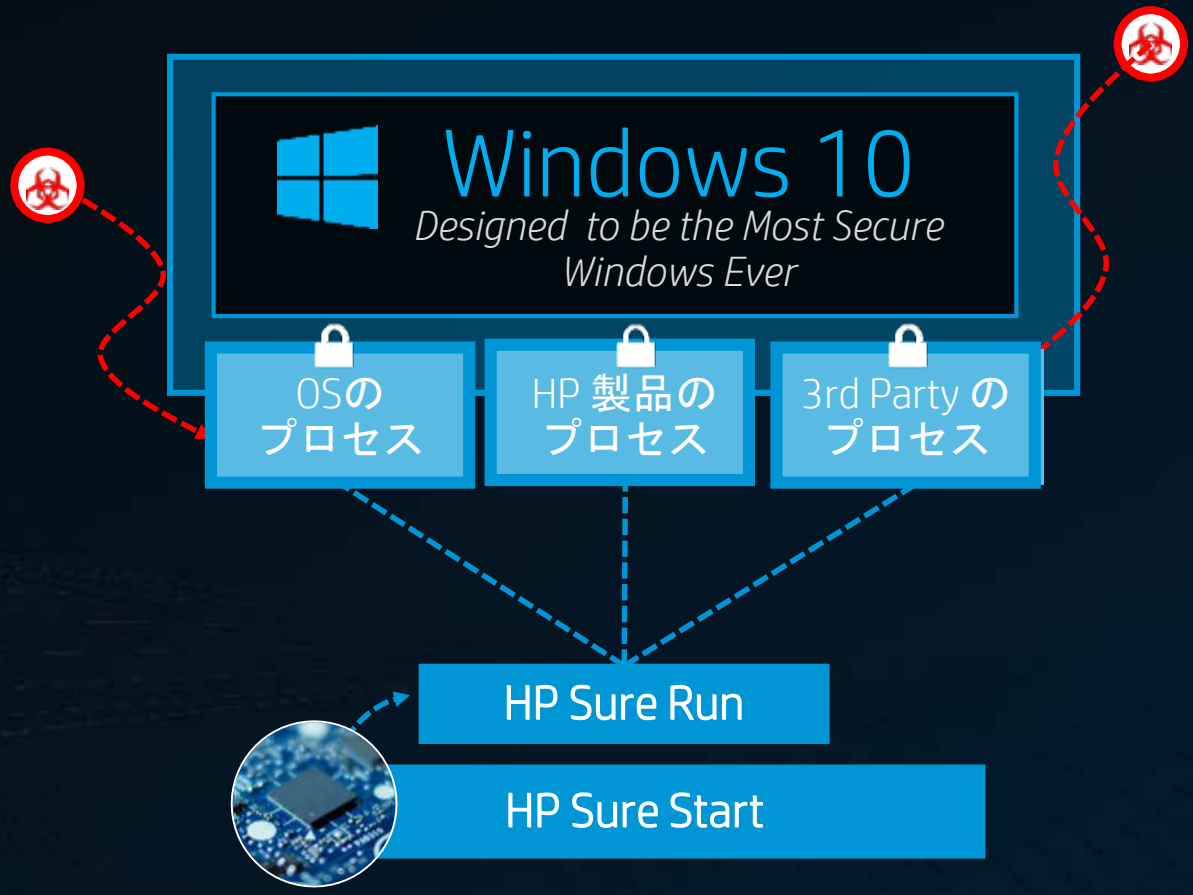
攻撃者がOS保護機能を無効化できないようにする

HP Sure Runでセキュリティプロセスを保護

PCを保護しているプロセスを保護する

HP Sure Run はHP Endpoint Security Controller の 自己回復 機能を OSの中に拡張する

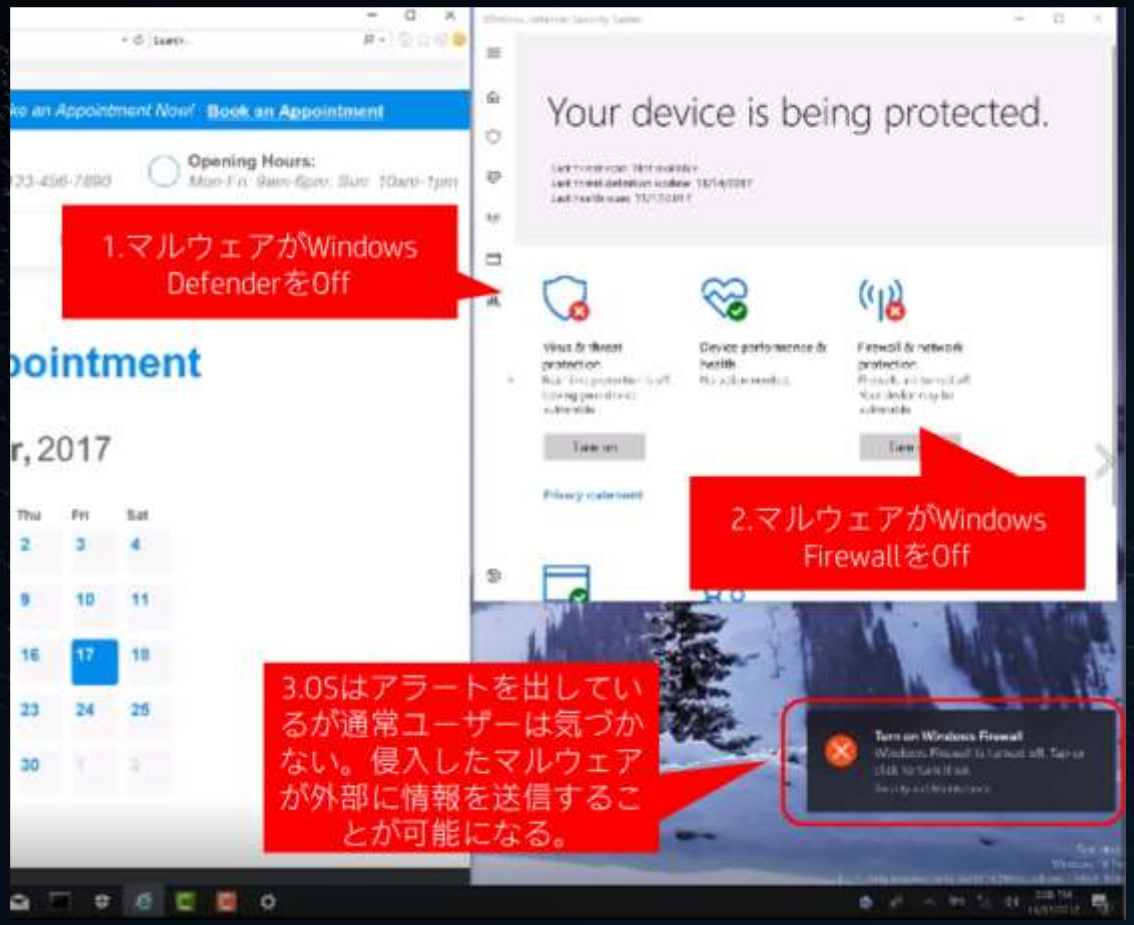
キープロセスを監視し、 変化をユーザーとITに通知し、もし停止した場合には自動的に再起動する



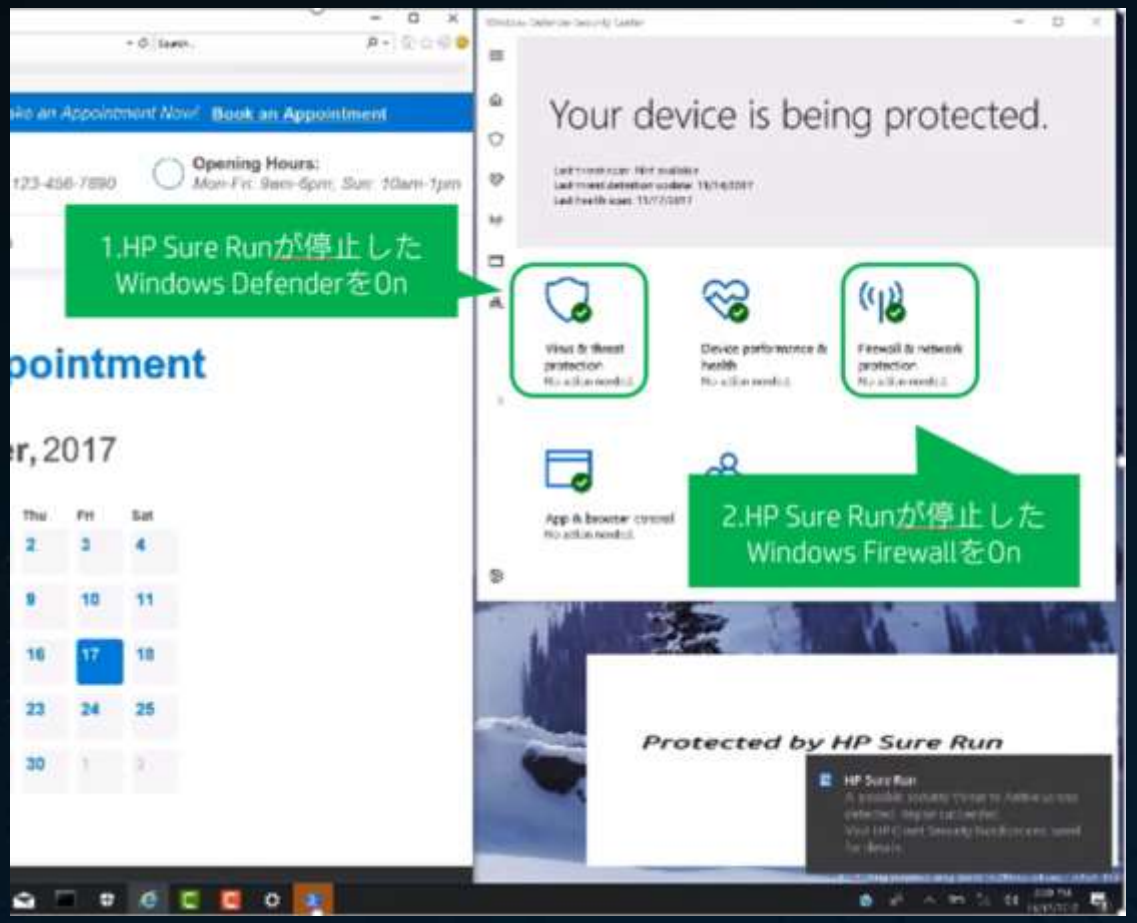
HP Endpoint Security Controller ハードウェアによるアプリケーション永続性

HP Sure Runの動作

HP Sure Run無し



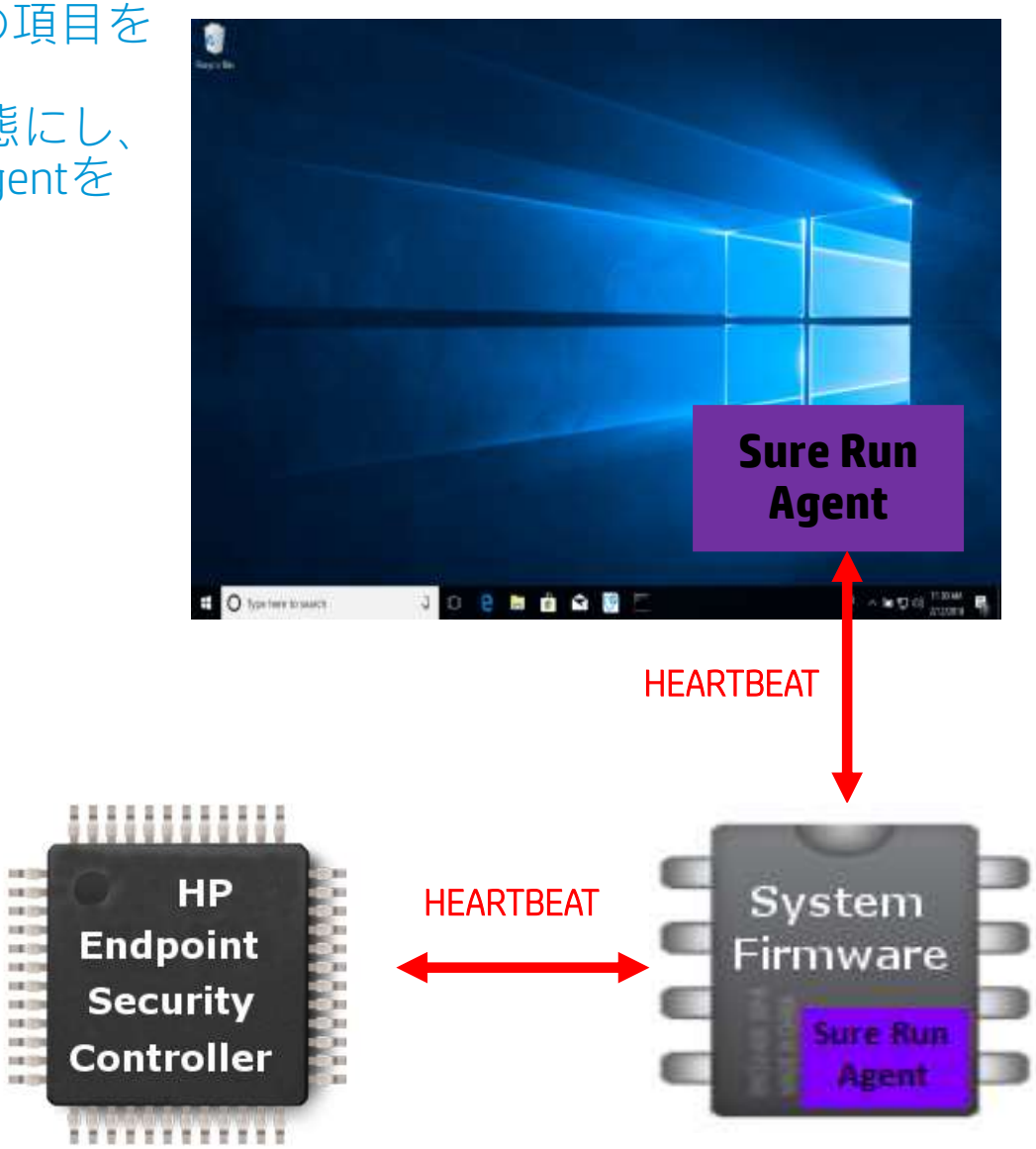
HP Sure Run



HP Sure Runの監視項目

定義された設定により監視対象に設定された以下の項目を監視し、異常があった際に復元します。
Sure Run Agentが停止した場合はシステムを休止状態にし、復元時にシステムファームウェアが再度Sure Run Agentを有効化します。

- レジストリキー
- ファイル/フォルダ
- サービス
- アンチウィルス
- プロセス
- ファイアウォール



HP Sure Runの監視対象

セキュリティ

- Security Account Manager
- Base Filtering Engine
- CryptographcService
- Software Protection

ネットワーク

- WLAN AutoConfig
- Extensible Authentication Protocol

管理

- Group Policy Client

アプリケーションインフラストラクチャ

- Windows Installer
- Task Scheduler

コアOS

- DCOM Server Process Launcher
- Remote Procedure Call(RPC)
- Windows Event Log
- Volume Shadow Copy

HPセキュリティ製品

- HP Client Security Manager
- HP Sure Click

他社製品

- Windows Security Center
- Firewall
- Antivirus
- SCCM Client（HP MIKからのみ設定可能）

クリックの信頼性
HP Sure Click で安全にブラウジング

HP Sure Click[8] - ハードウェア強化した安全なブラウジングソリューションisはマルウェアをCPUで分離した仮想マシンに隔離するので、PCは影響を受けない

ブラウザーのタブを閉じるだけで
マルウェアは消滅!

Compatible with Internet Explorer and Chromium browsers

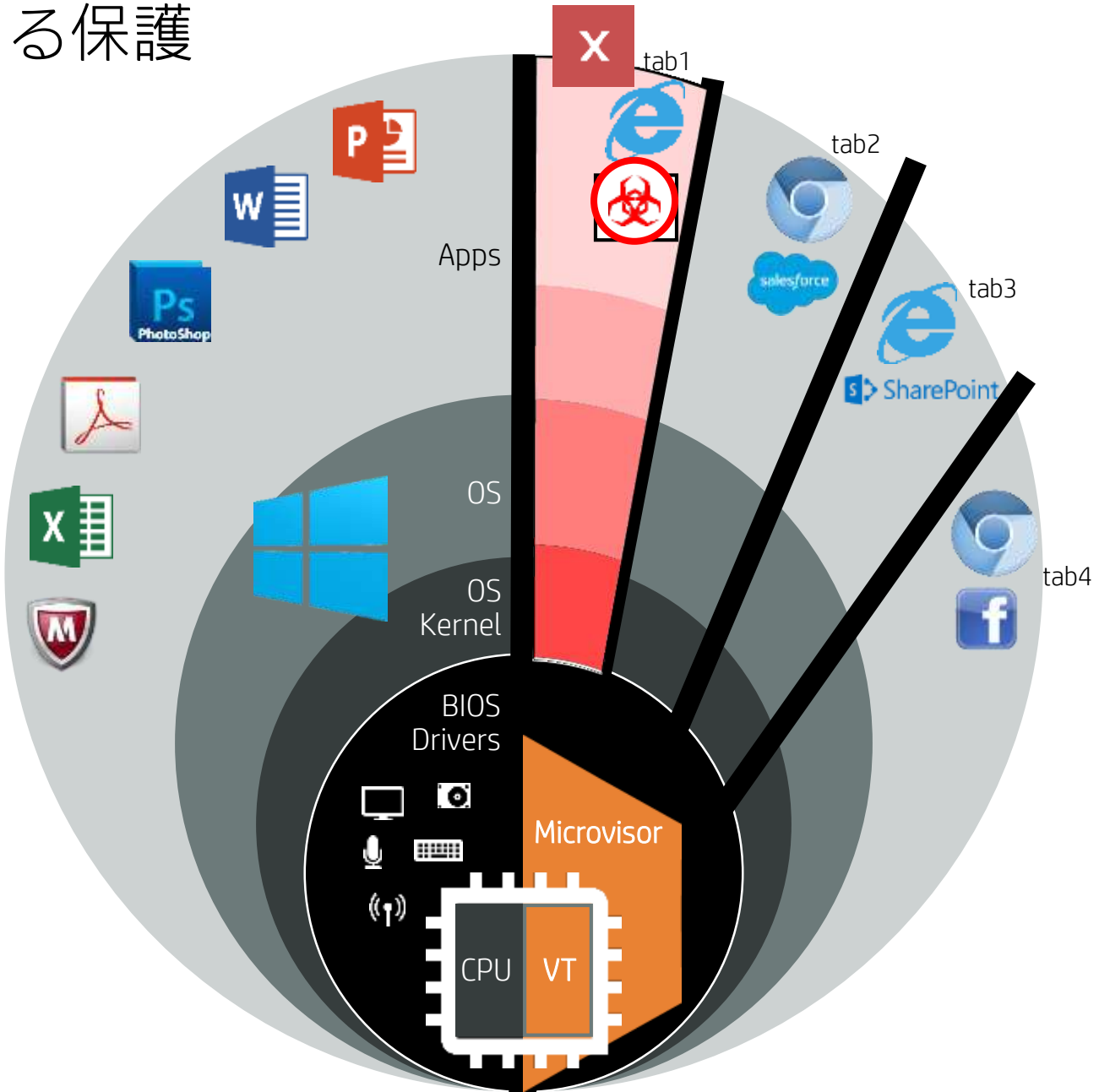
HP Sure Clickによる保護

HP Sure Clickによる保護

✓個々のブラウザタブは
マイクロVMの中で開かれる

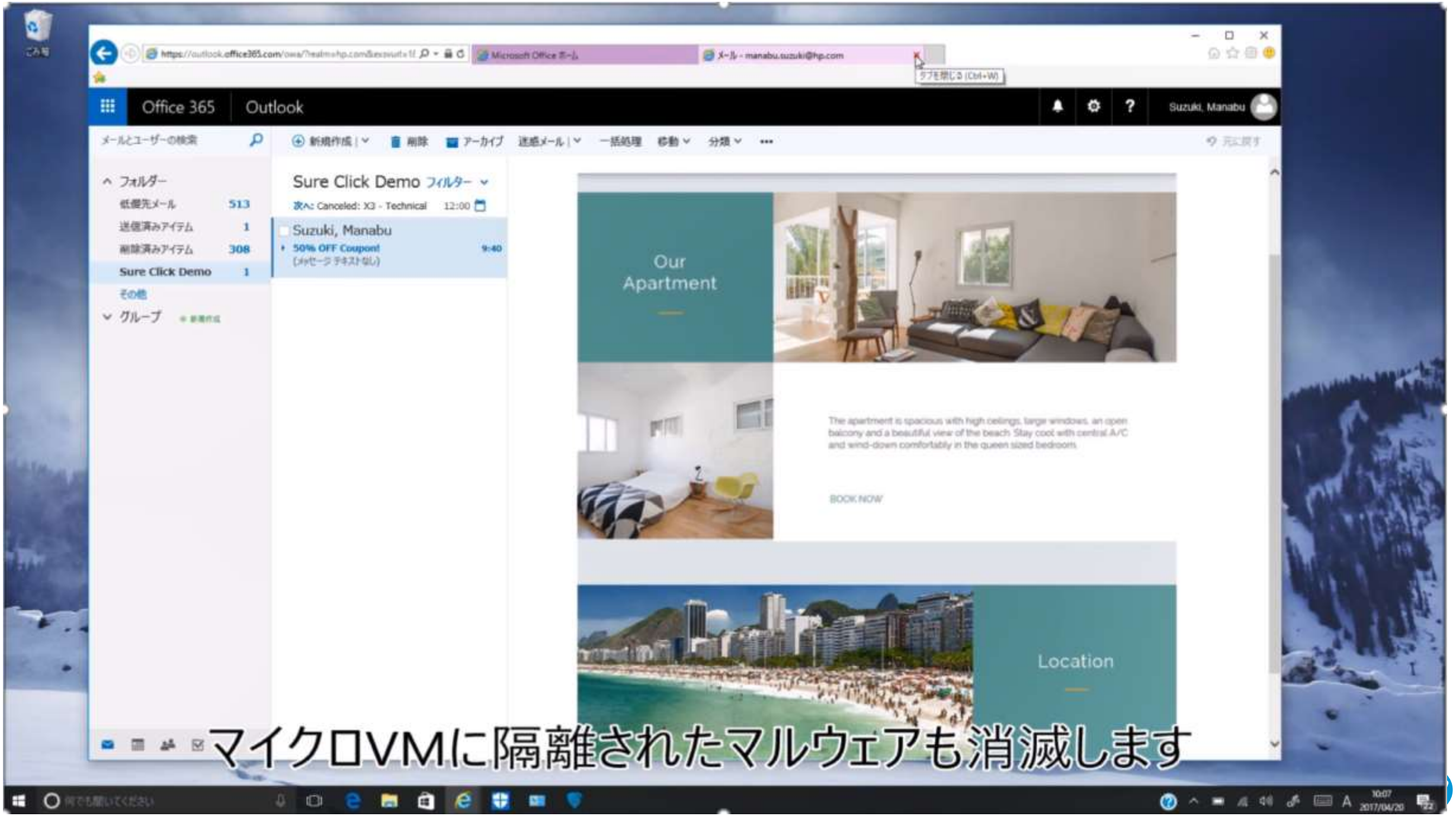
✓マルウェアはCPUベース
で隔離され、他のタブ、
アプリ、OSには影響がない

✓タブが閉じられると、
マルウェアは自動的に
除去される

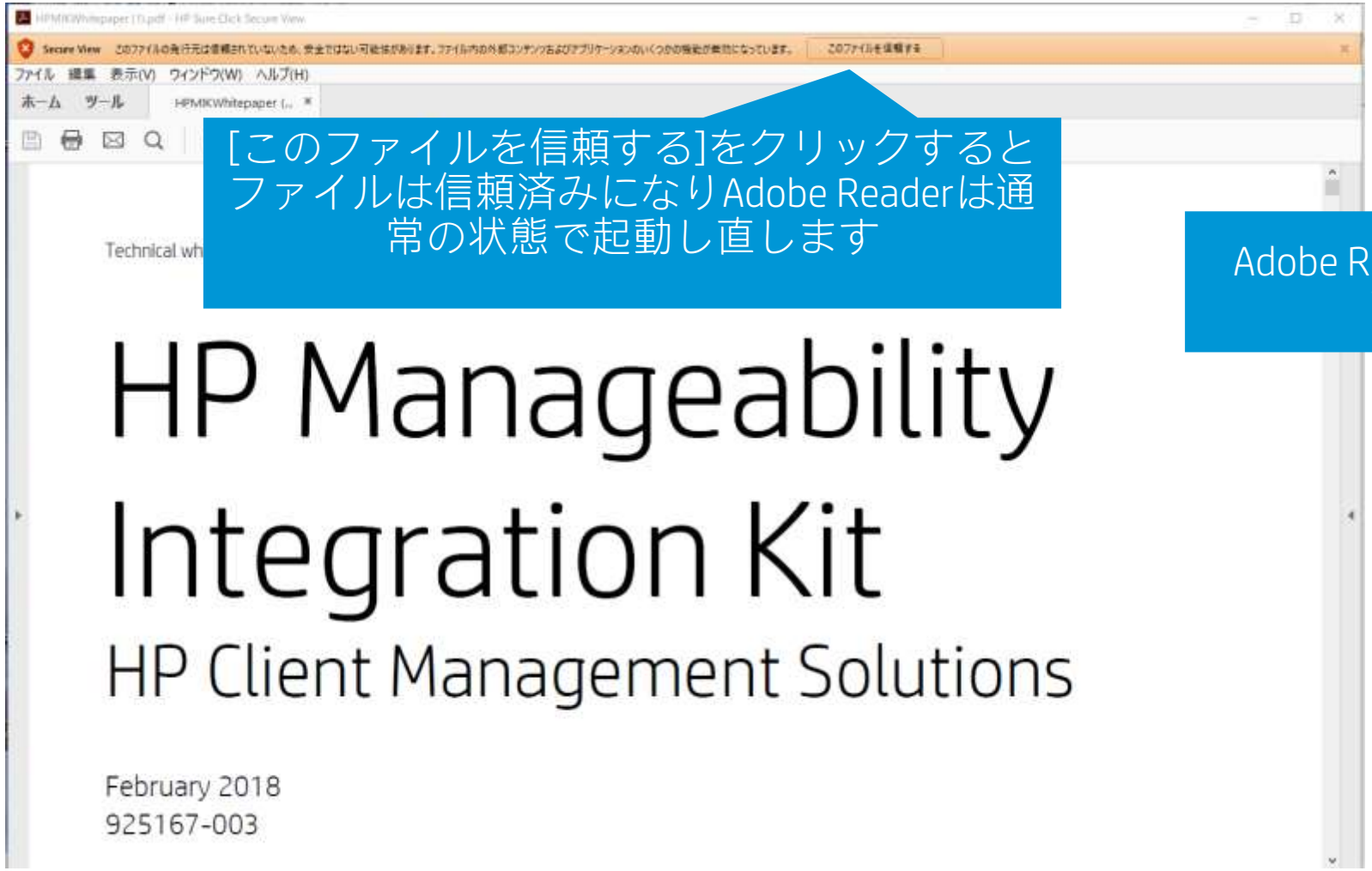



BEACH RESORT
HOME
ABOUT
ROOMS
DIVE SITE
FOOD
NEWS
CONTACT
THE SOUND OF THE SEA
ENJOY THE SUMMER WITH US!
HP Sure ClickはCPUレベルまで隔離された
マイクロVM上でブラウザを実行


You've been hacked
BHACCASYONIZTAS
BEACH RESORT
DIVE SITE
FOOD
NEWS
CONTACT
Your personal files are encrypted!
Your files have been safely encrypted on this PC: photos, videos, documents, etc. Click "Show encrypted files" Button to view a complete list of encrypted files, and you can personally verify this.
Encryption was produced using a unique public key RSA-2048 generated for this computer. To decrypt files you need to obtain the private key.
The only copy of the private key, which will allow you to decrypt your files, is located on a secret server in the Internet; the server will eliminate the key after a time period specified in this window.
Once this has been done, nobody will ever be able to restore files...
In order to decrypt the files press button to open your personal page
File decryption site
and follow the instruction.
in case of "File decryption button" malfunction use one of our gates:
http://34r6hq26q2h4jkzj.2kjb8.net
https://34r6hq26q2h4jkzj.tor2web.fi
Use your Bitcoin address to enter the site:
1CCyqYcsjHMbMbQXdzYHEzcJK1eFr3rxV6
Click to copy address to clipboard
if both button and reserve gate not opening, please follow the steps:
You must install this browser www.torproject.org/projects/torbrowser.html.en
After instalation,run the browser and enter address 34r6hq26q2h4jkzj.onion
Follow the instruction on the web-site. We remind you that the sooner you do so, the more chances are left to recover the files.
Any attempt to remove or corrupt this software will result in immediate elimination of the private key by the server.
Your private key will be destroyed on:
4/23/2017
Time left: 95:58:30
Click for Free Decryption on site
Show files
Enter Decrypt Key
ENJOY THE SUMMER WITH US!
ブラウザを閉じることで

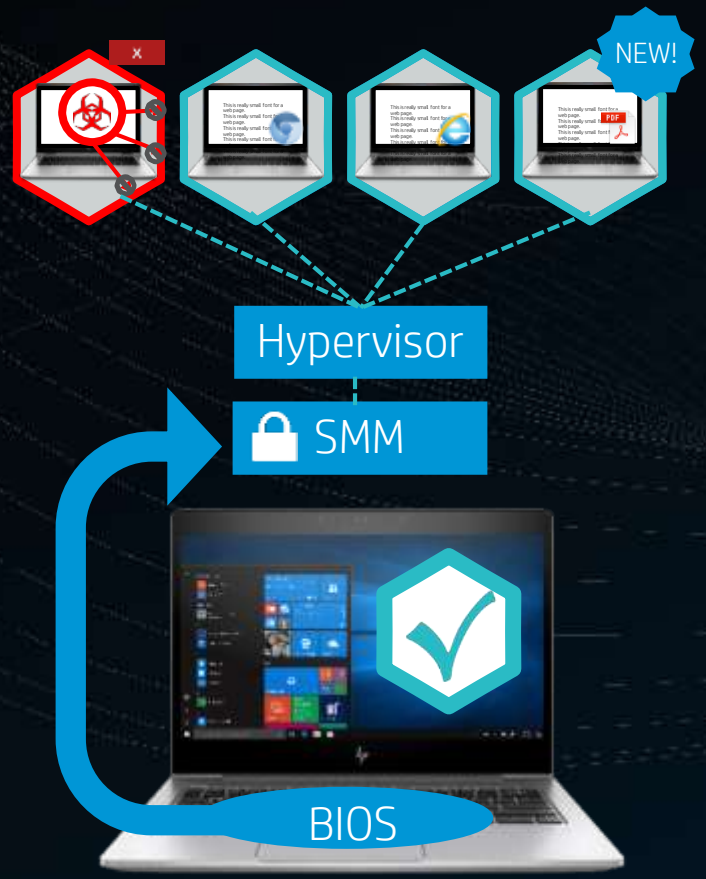

Office 365
Outlook
Suzuki, Manabu
Sure Click Demo フィルター
Suzuki, Manabu
50% OFF Coupon
Our Apartment
The apartment is spacious with high ceilings, large windows, an open balcony and a beautiful view of the beach. Stay cool with central A/C and wind-down comfortably in the queen sized bedroom.
BOOK NOW
Location
マイクロVMに隔離されたマルウェアも消滅します

Adobe Readerの隔離



Adobe ReaderがマイクロVMで起動してPDFファイルを安全に開きます

ハードウェアで強化された信頼の連鎖



HP Sure Click
マルウェアの攻撃を隔離

HP Sure Run
HP Sure Click[8] が確実に動作することを担保する

HP Sure Start
SMMを保護し、HP Sure Run[3]を実現

HP Elite PCのHP Sure Click は
安全なハードウェア強化された保護を
インターネットのブラウジングに拡張

ダウンタイムを最小化する
HP Sure Recoverで素早く復元

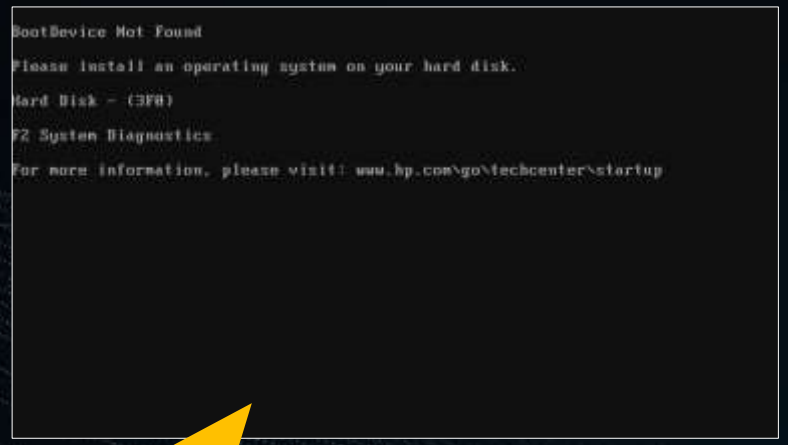
HP Sure Recover は安全にネットワーク経由のソフトウェアイメージリカバリを実現

HP Endpoint Security Controllerを使用して、
素早く安全にPCを再イメージング
HPまたは企業のOSイメージに復元
使用するのはインターネット接続のみ

HP Sure Recover はハードウェアベースの機能なので外部のツール不要でPCの再イメージングが可能

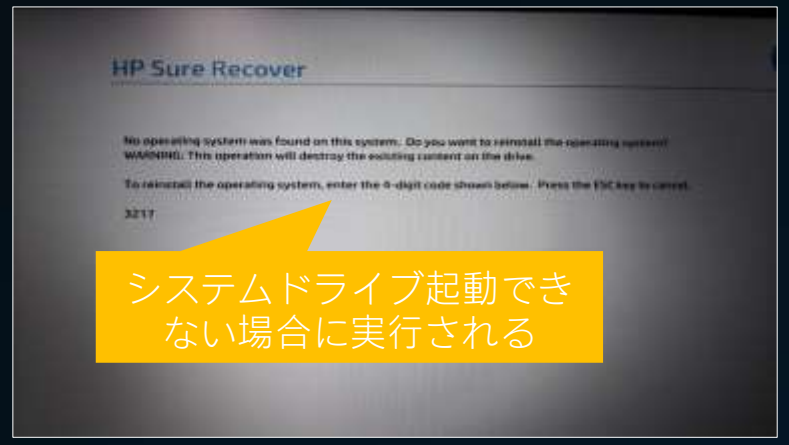
HP Sure Recoverの動作

HP Sure Recover無し

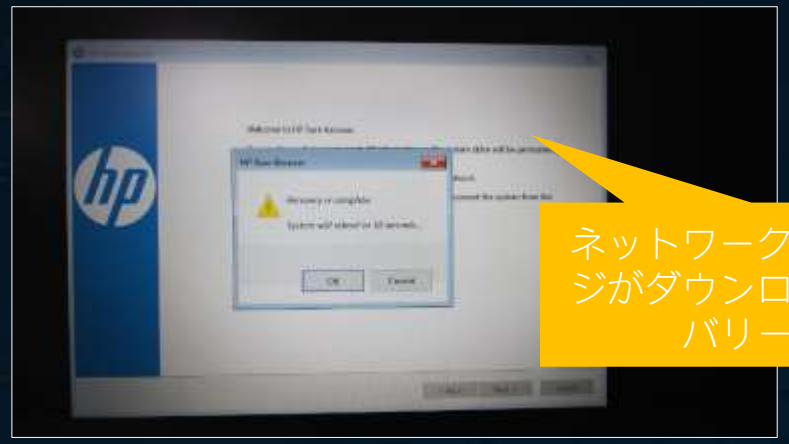


システムドライブが起動できないと個別のリカバリ作業が必要になる

HP Sure Recover



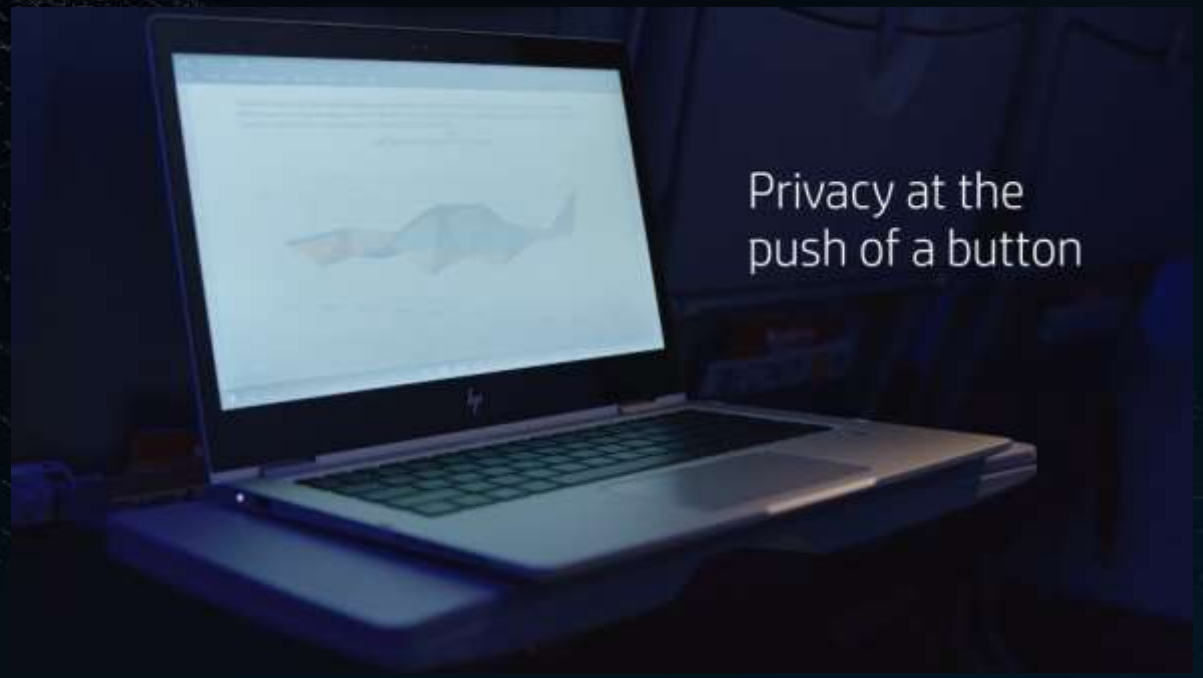
システムドライブ起動できない場合に実行される



ネットワーク経由でイメージがダウンロードされリカバリーを完了

公共の場で自由に働く

HP Sure View Gen2[7]: 世界で唯一のPC内蔵型プライバシースクリーン[12]



HP Sure View Gen2[7] ボタン1つでヴィジュアルハッキングから保護する

HP Sure View Gen2 は明るい環境でも暗い環境でもより見やすく – 飛行機の中からカフェまで

What's New

- 明るい場所と暗い場所の両方に適応
- IPS パネルテクノロジー
- 120Hz のリフレッシュレートで,滑らかな動きを表示
- 狭額ベゼル

全てのPCを確実に保護する

セキュリティポリシーを HP Manageability Integration Kit で全端末に強制

HP Manageability Integration Kitは
世界で唯一のMicrosoftが認定したSCCMのプラグイン

HPが提供するハードウェアに根差した独自の機能を管理可能

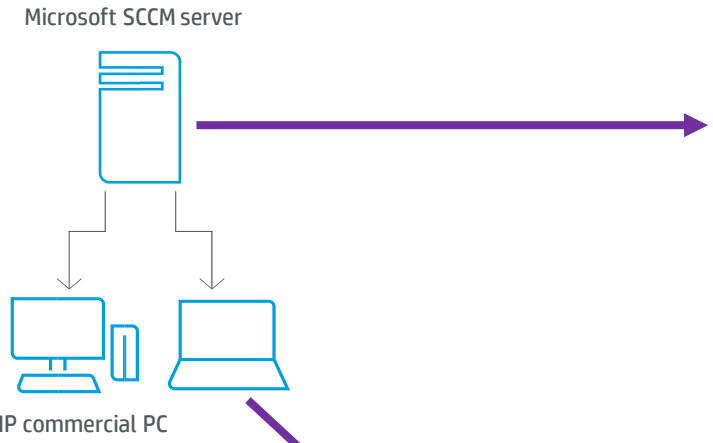
HP Sure Startの管理
BIOS保護、BIOS設定

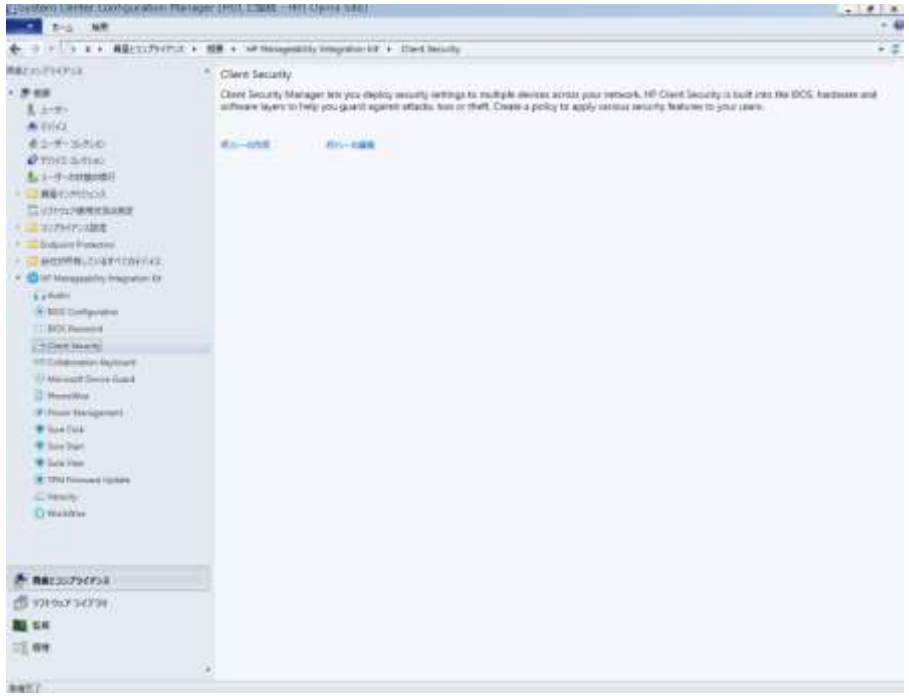
HP Client Securityの管理
多要素認証、デバイスアクセス制御等

HP Sure View等の管理ポリシー設定

簡単に操作できるUI

HP MIKによるリモート設定管理





HP Commercial PC

MSFT SCCM Agent

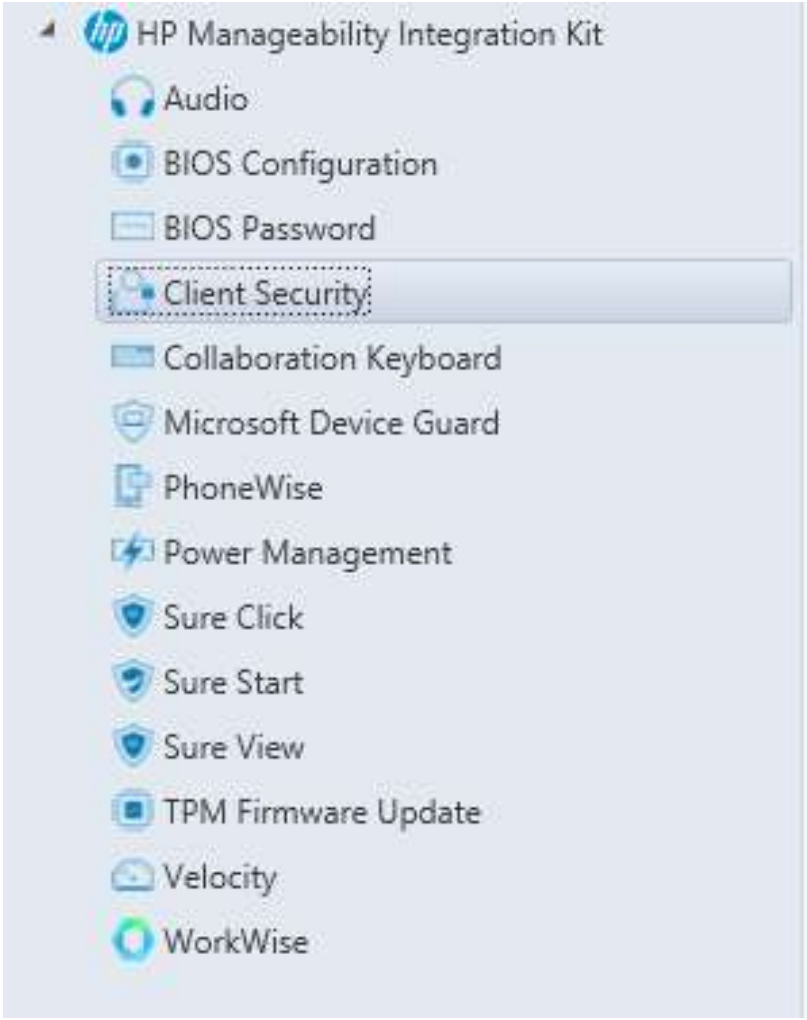
= HP Provided Components
= MSFT Provided Components

SCCM Provider A
SCCM Provider B
SCCM Provider C
SCCM Provider D
SCCM Provider “n”

Client Security
Sure Click
Sure View
BIOS
Feature “n”…

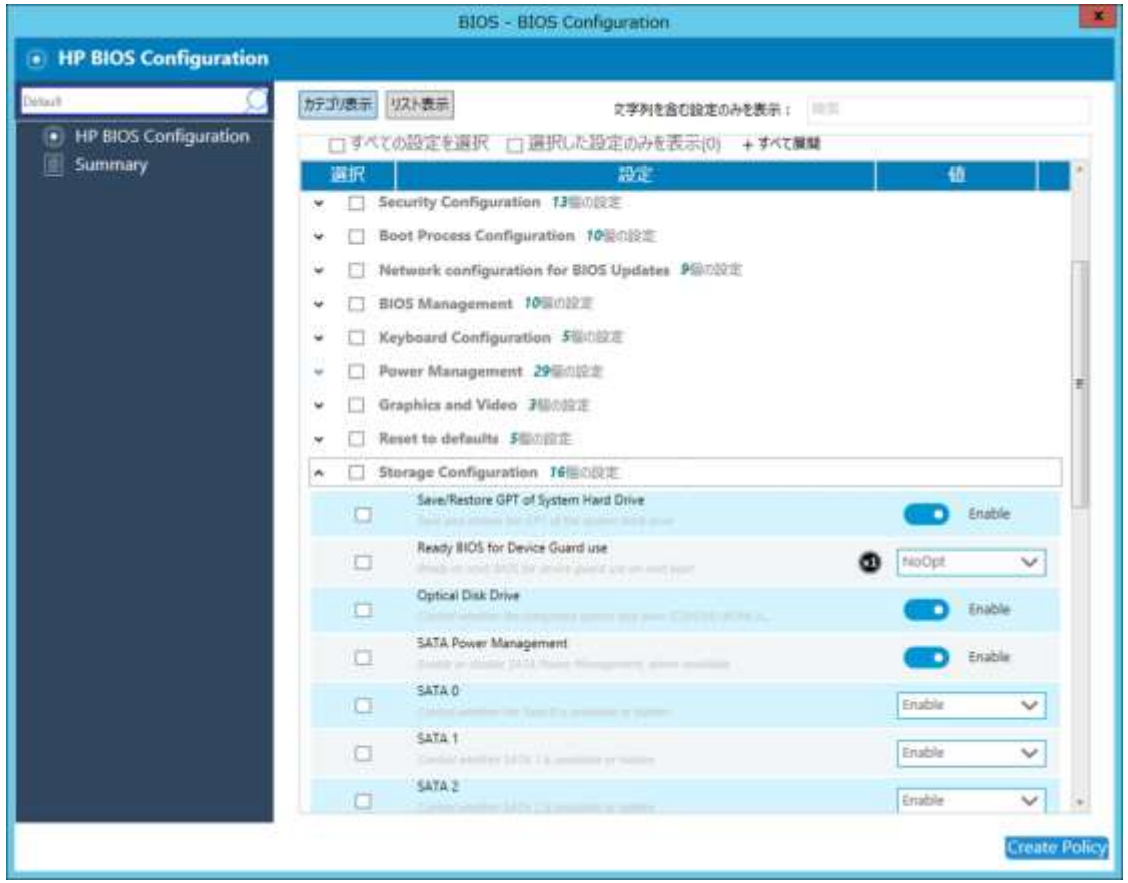
HP MIKプラグイン

HP Manageability Integration Kitをインストールすると管理とコンプライアンスにHP Manageability Integration Kitが追加されます。 HPコマーシャルPCの各種設定のポリシーによる集中管理が可能になります。



HP MIKプラグインのポリシー設定の例

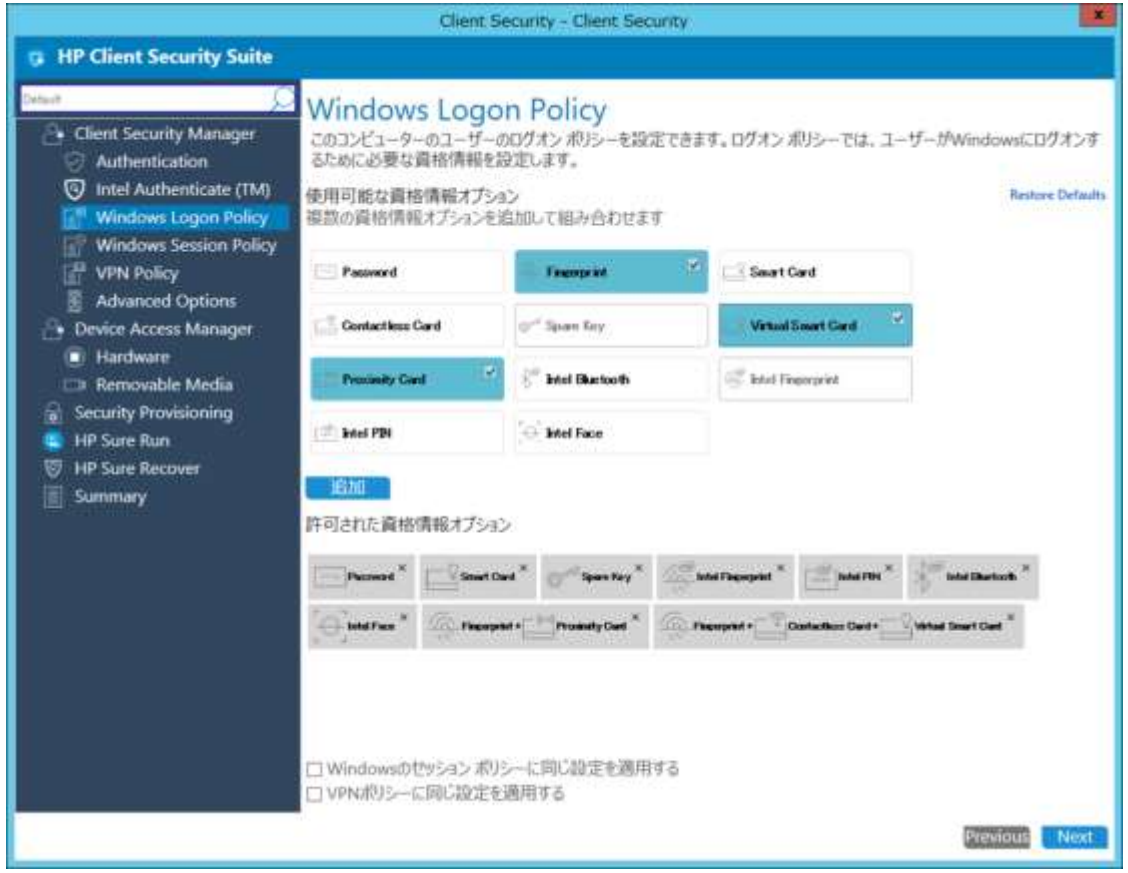
BIOS Config



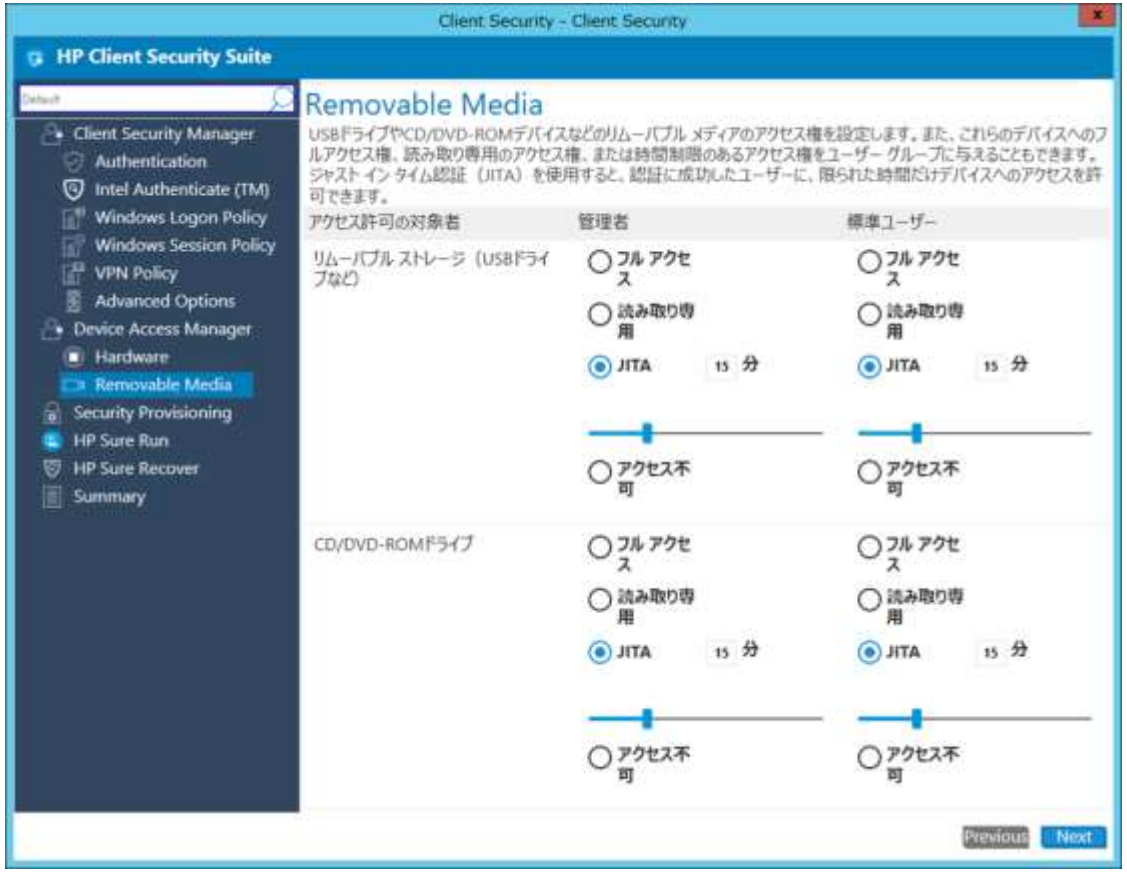
BIOS Password

HP MIKプラグインのポリシー設定の例

Client Security Manager – Windows Logon Policy

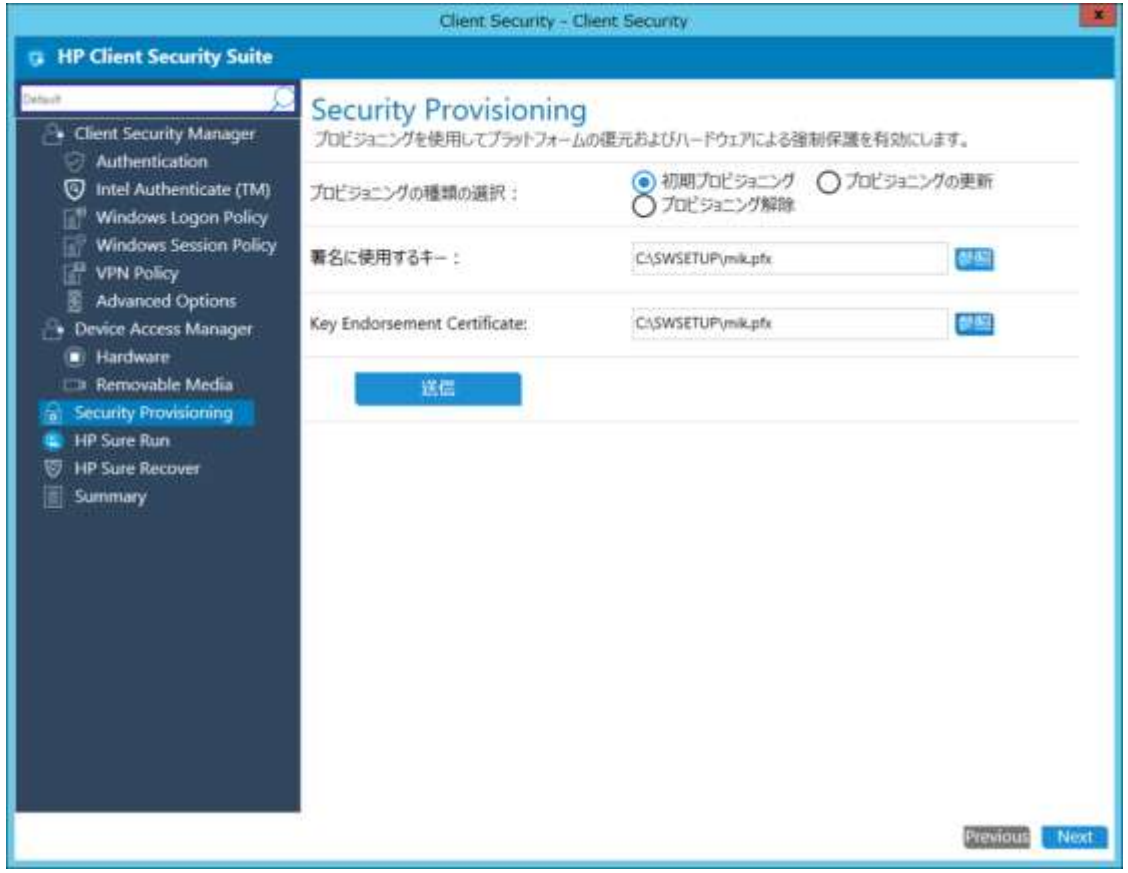


Device Access Manager – Removable Media

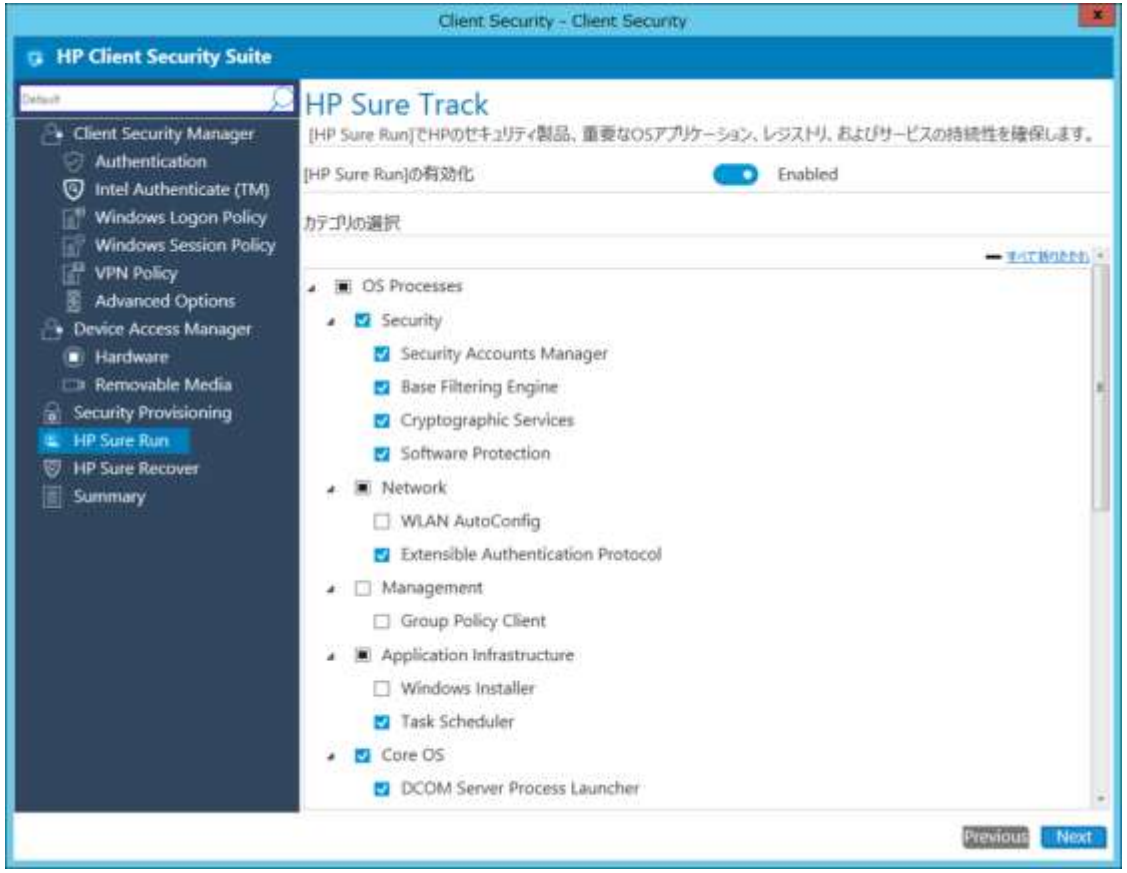


HP MIKプラグインのポリシー設定の例

HP Client Security Suite - Security Provisioning

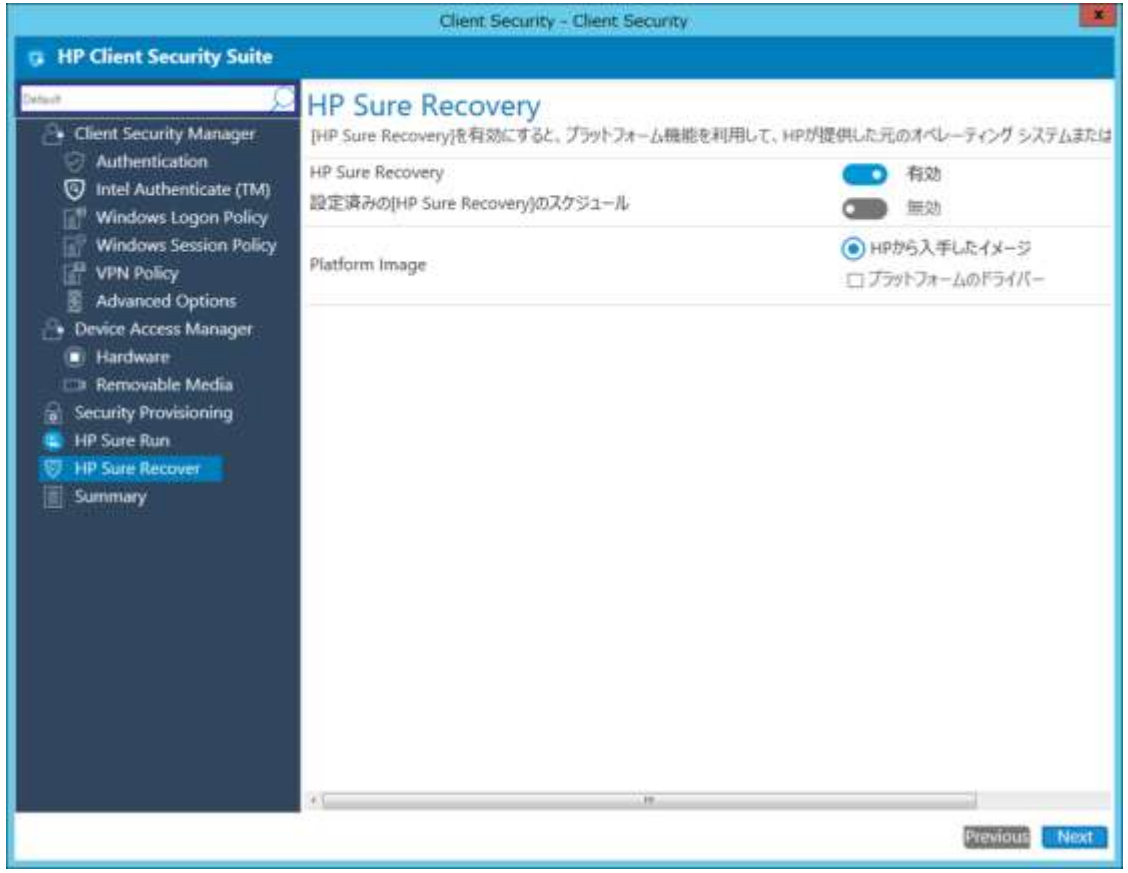


HP Client Security Suite - HP Sure Run



HP MIKプラグインのポリシー設定の例

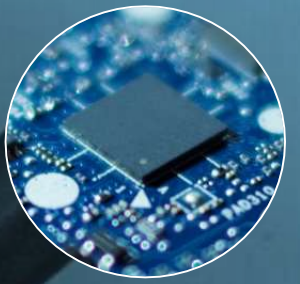
HP Client Security Suite - HP Sure Recover



HP Sure Click

世界で最も安全で管理性の高いPC

ハードウェアに根差したセキュリティ



セキュリティ侵害に対するレジリエンス

全端末にポリシーを強制する管理機能

セキュリティ機能対応イメージ
（第7世代以降のインテルプロセッサー搭載機種より順次対応予定）

PRO 400	PRO 600	ELITE 800	ELITE 1000
		HP Sure View	HP Sure View
		HP Sure Recover（2018年モデルから）	
		HP Sure Run（2018年モデルから）	
	HP Sure Start（Pro 600は2018年モデルから）		
	HPマルチファクタ認証		
HP Manageability Integration Kit (MIK) HP Image Assistant			
HP Sure Click ※CPUがPentium/Cerelon/Core-mの場合は動作サポートされないためお使いいただけません			
HP Secure Erase HP Client Security Suite （HPスペアキー、デバイスアクセスマネージャ）			
指紋リーダー スマートカードリーダー TPMセキュリティチップ 自己暗号化ドライブ(SED)			


keep reinventing