

HP Sure Clickご紹介資料

株式会社 日本HP
2017年2月



HPのセキュリティにおけるリーダーシップ



✓多層防御

OSの下位から上位レイヤまでを網羅した防御機能を提供

✓追加費用不要

プリインストールもしくは無償ダウンロードにて提供

✓管理可能なセキュリティ

セキュリティポリシーをリモートから徹底

これらを

世界で最初のイノベーションと共に提供

自己回復型BIOS、内蔵プライバシースクリーン、モバイルデバイスによる自動ログインなど業界初のセキュリティ機能



HPのセキュリティイノベーション

- HP Sure Start : BIOSへの攻撃を検知し自動復旧、OS起動前の
- HP Client Security Suite : デバイスアクセス制限、Windowsパスワード復元、パスワード管理を多要素認証で実現
- HP WorkWise : スマートフォンの距離情報に基づくログイン、PCの異常(不正アクセス、温度の上昇、バッテリー残量低下)をスマートフォンに通知
- HP Sure View : 公共の場におけるビジュアルハッキングから保護、内蔵プライバシースクリーン
- HP Manageability Integration Kit : ユーザーもしくはマルウェアによりセキュリティ機能をOffにさせない、リモートからの資産管理
- HP Sure Click : マルウェアやウィルスに感染したWebサイトからPCを守る、ハードウェアベースのブラウジングセキュリティ



世界で最も安全で、管理性に優れたビジネスPC⁶



セキュリティは必要不可欠

\$9.5M

復旧にかかる平均費用¹

200%

ノートPC/デスクトップPC
への標的型攻撃の増加率²



81%

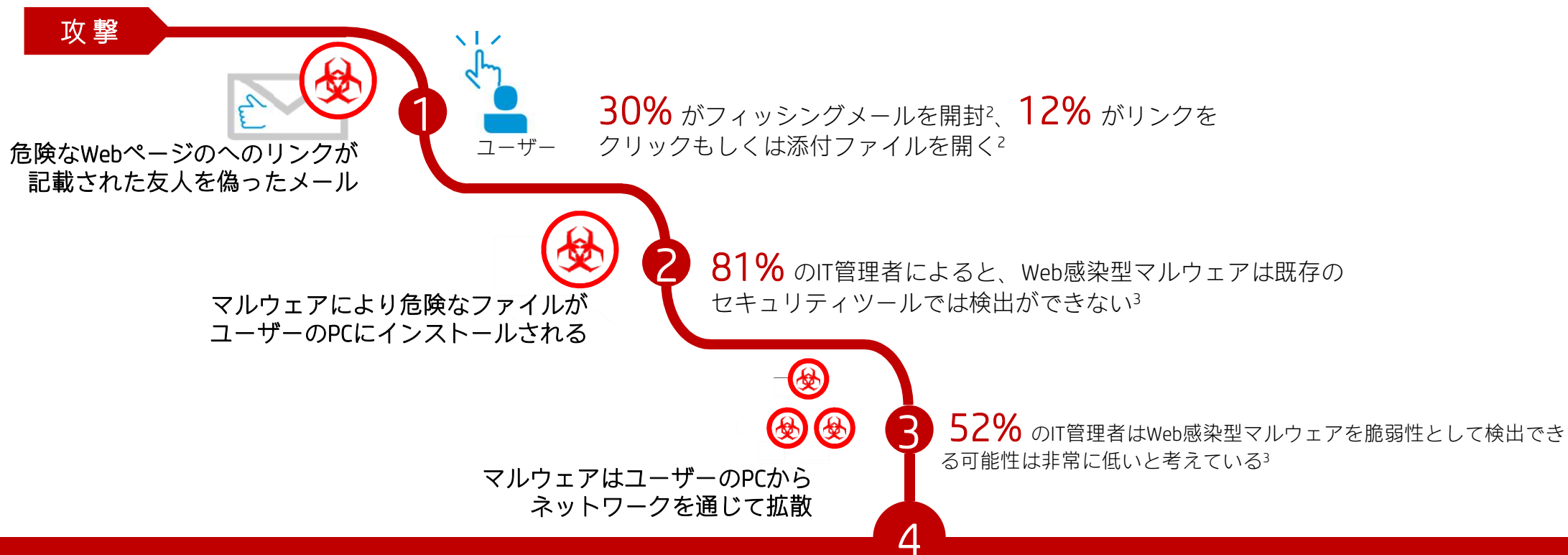
ブラウザが最初の標的にな
ると考えるIT管理者³

40 秒毎に

ランサムウェアが企業を
攻撃している(Q3 2016時点⁴)

マルウェアの攻撃手法

攻撃



ビジネスの中断

生産性の損失

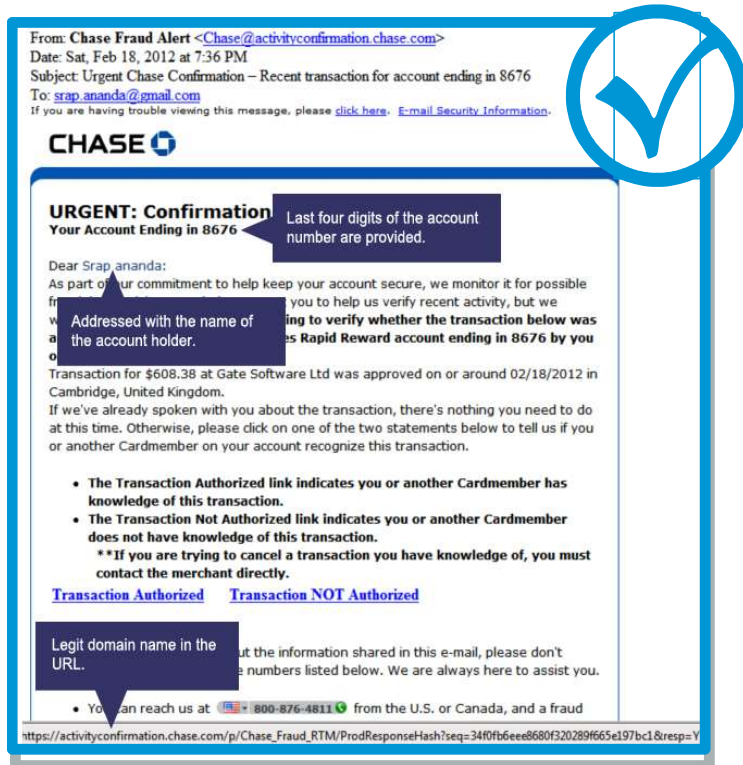
データ盗難

スパイ活動

身代金

なぜ悪意のあるリンクをクリックしてしまうのか

どのメールがフィッシングメールでしょうか？



From: Chase Fraud Alert <Chase@activityconfirmation.chase.com>
Date: Sat, Feb 18, 2012 at 7:36 PM
Subject: Urgent Chase Confirmation – Recent transaction for account ending in 8676
To: srp.ananda@gmail.com

URGENT: Confirmation
Your Account Ending in 8676

Last four digits of the account number are provided.

Dear Srp.ananda:
As part of our commitment to help keep your account secure, we monitor it for possible fraud. We want to help you to help us verify recent activity, but we need your help. We are writing to you to help us verify whether the transaction below was made by you. The transaction below was made on a Chase Rapid Reward account ending in 8676 by you on 02/18/2012.

Transaction for \$608.38 at Gate Software Ltd was approved on or around 02/18/2012 in Cambridge, United Kingdom.

If we've already spoken with you about the transaction, there's nothing you need to do at this time. Otherwise, please click on one of the two statements below to tell us if you or another Cardmember on your account recognize this transaction.

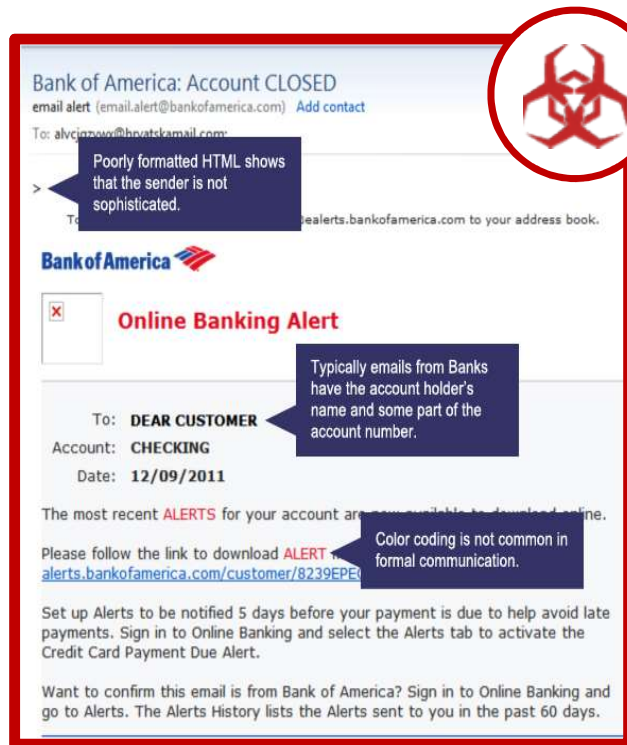
- The Transaction Authorized link indicates you or another Cardmember has knowledge of this transaction.
- The Transaction Not Authorized link indicates you or another Cardmember does not have knowledge of this transaction.

** If you are trying to cancel a transaction you have knowledge of, you must contact the merchant directly.

[Transaction Authorized](#) [Transaction NOT Authorized](#)

Legit domain name in the URL.

https://activityconfirmation.chase.com/p/Chase_Fraud_RT/ProdResponseHash?seq=34f0fb6ee6680f320289f665e197bc1&resp=Y



Bank of America: Account CLOSED
email alert (email.alert@bankofamerica.com) Add contact

To: alvcjoww@bvataskamail.com

Poorly formatted HTML shows that the sender is not sophisticated.

Online Banking Alert

To: DEAR CUSTOMER
Account: CHECKING
Date: 12/09/2011

Typically emails from Banks have the account holder's name and some part of the account number.

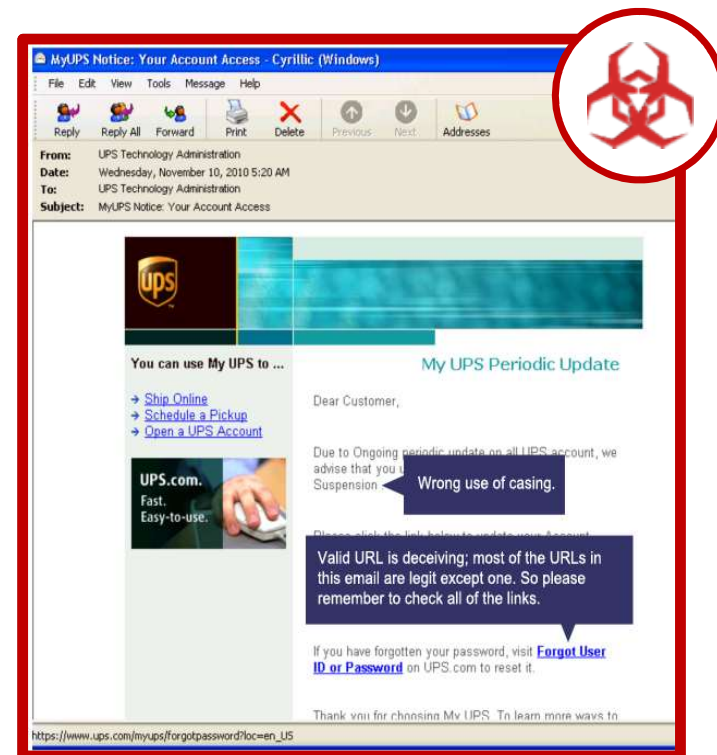
The most recent ALERTS for your account are listed below.

Please follow the link to download ALERTS.
alerts.bankofamerica.com/customer/8239EPE

Color coding is not common in formal communication.

Set up Alerts to be notified 5 days before your payment is due to help avoid late payments. Sign in to Online Banking and select the Alerts tab to activate the Credit Card Payment Due Alert.

Want to confirm this email is from Bank of America? Sign in to Online Banking and go to Alerts. The Alerts History lists the Alerts sent to you in the past 60 days.



MyUPS Notice: Your Account Access - Cyrillic (Windows)

From: UPS Technology Administration
Date: Wednesday, November 10, 2010 5:20 AM
To: UPS Technology Administration
Subject: MyUPS Notice: Your Account Access

My UPS Periodic Update

Dear Customer,

Due to Ongoing periodic update on all UPS account, we advise that you suspend your account.

Wrong use of casing.

Valid URL is deceiving; most of the URLs in this email are legit except one. So please remember to check all of the links.

[Forgot User ID or Password](#) on UPS.com to reset it.

https://www.ups.com/myups/forgotpassword?loc=en_US

どのメール/リンクがフィッシングか完璧に識別することは不可能

ブラウジングセキュリティを高める方法



ユーザー教育

- ✕ トレーニングの開発と実施にかかるコスト
- ✕ ユーザーの時間の消費
- ✕ 人的ミスは引き続き避けられない



ホワイトリスト ブラックリスト

- ✕ リストの定期的なメンテナンスにかかるコスト
- ✕ ユーザーの生産性を阻害



ハードウェア による隔離

- ✓ ブラウザタブを仮想的に独立させ、タブが閉じられたらすべてを無効化
- ✓ ユーザーは悪意のあるリンクやWebサイトであるかどうか神経質になる必要がない



HPのブラウジングセキュリティソリューション



&



Bromium[®]

HP Sure Click

ブラウジングセキュリティソリューション
HP Sure Clickはマルウェアやウイルスに感染したWebサイトからPCを守る
ハードウェアベースのブラウジングセキュリティを提供します



HP Sure Clickによる保護



従来の検知機能による保護

- ✓ 既知の攻撃をブロック
- ✗ 無数のアラートを発行



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

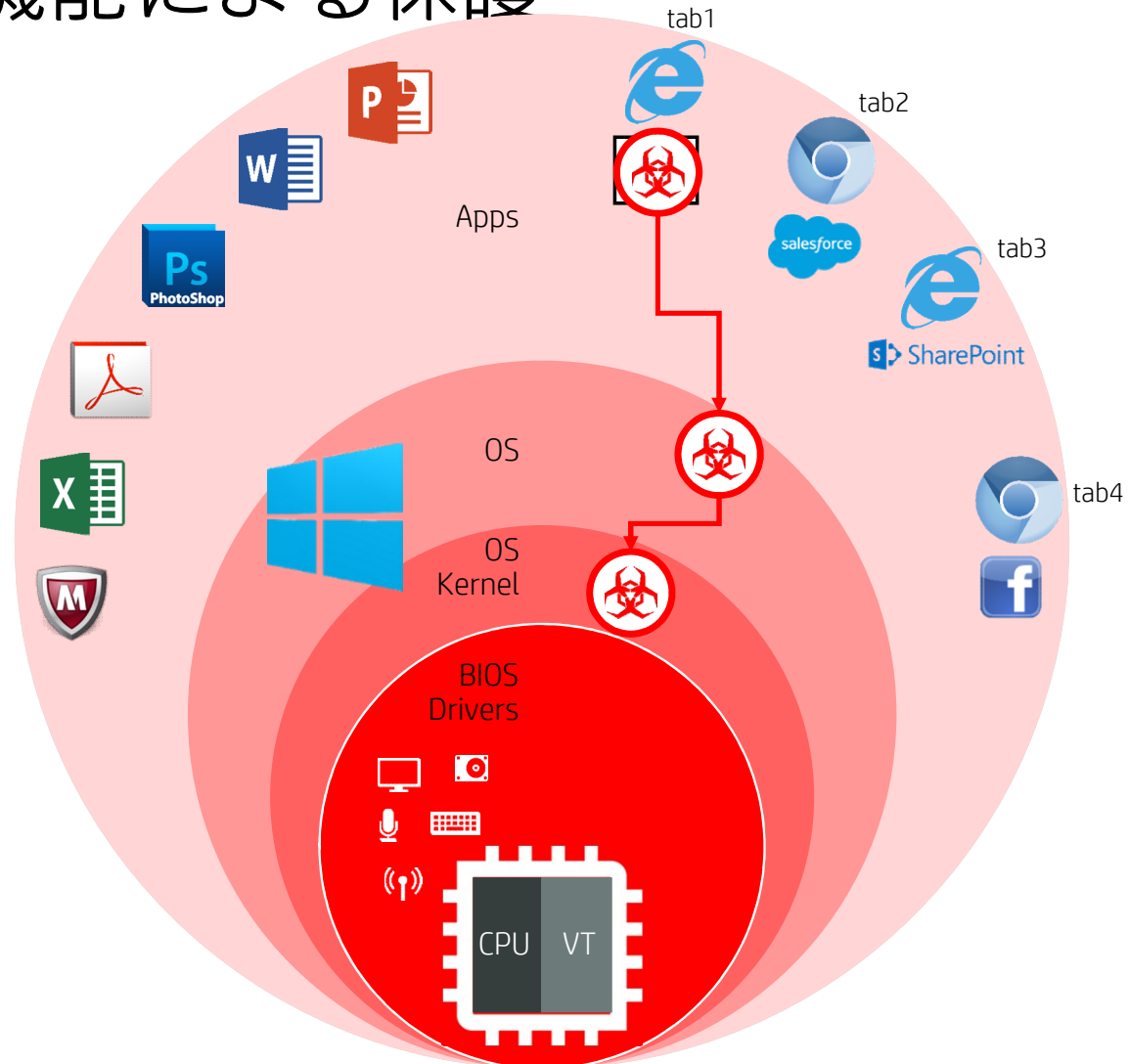
81%

Web感染型マルウェアは既存のセキュリティツールでは検出ができないと言われている³

従来の検知機能による保護

従来の検知機能による保護

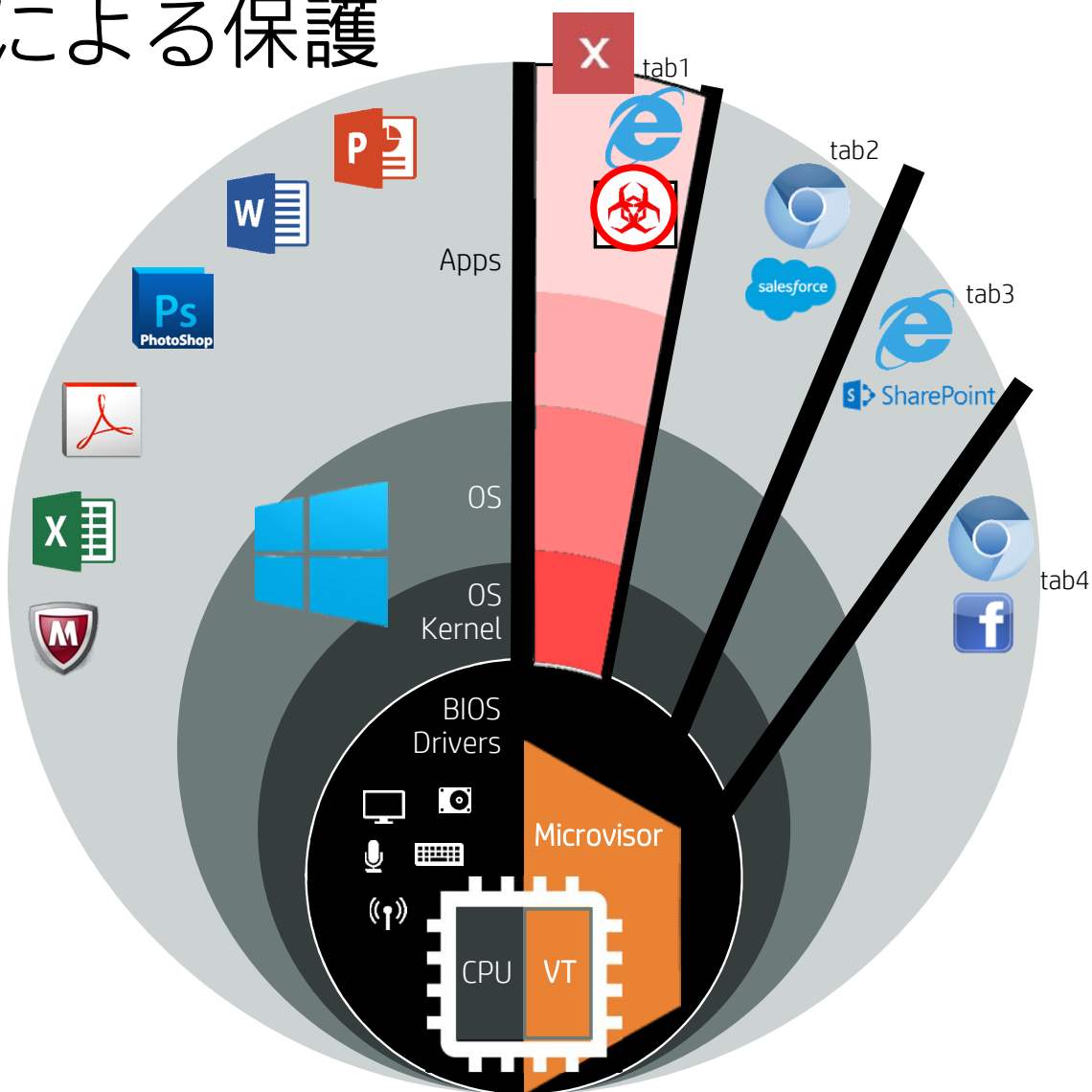
- ✓ 既知の攻撃をブロック
- ✗ 無数のアラートを発行



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



HP Sure Clickのユーザーメリット



ブラウジングの安全性

ユーザーは企業の外にいても制限なく
安全にブラウジングが可能になる

ITコスト削減

アラートの数が減り、復旧にかかる工数が削減でき、
IT管理者はより重要なプロジェクトに専念できる

Disclaimers & endnotes

1. Ponemon Instituteによる“2016 Cost of Cyber Crime Study & the Risk of Business Innovation”より <https://ssl.www8.hp.com/ww/en/secure/pdf/4aa6-8392enw.pdf>
2. Verizonによる“2016 Data Breach Investigations Report”より <http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/>
3. Ponemon Instituteによる“The Challenge of Preventing Browser-Borne Malware”より <https://spikes.com/ponemon-report-browser-malware-infected-most-companies.html>
4. Kasperskyによる“Security Bulletin 2016”より <https://securelist.com/analysis/kaspersky-security-bulletin/76757/kaspersky-security-bulletin-2016-story-of-the-year/>
5. HP EliteBook x360 G2向けにダウンロードが可能です。 www.hp.com/go/clientmanagement
6. HP独自の追加費用不要で包括的なセキュリティ機能とHP Managability Integration kitによる資産管理、MicrosoftのSCCMと連携したBIOS/ソフトウェアの管理を指し、2016年11月時点で年間100万台以上販売しているベンダーのモデルと、HP Elite製品のIntel第7世代プロセッサを搭載しているIntelアーキテクチャーモデルとの比較。