テレワークを導入する中小企業へ

これで安心 PCセキュリティ

ITmedia NEWS SPECIAL
監修 ITmedia NEWS

掲載製品およびサービスに関するお問い合わせはHP カスタマー・インフォメーション・センターへ

0120-436-555 フリーダイヤルがご利用いただけない場合 03-5749-8291
月曜ー金曜 9:00-18:00　土曜 10:00-17:00（日曜、祝日、5月1日、年末年始など、日本HP指定の休業日を除く）

http://www.hp.com/jp/

OPO15014-01

2021年11月版

テレワークを導入する中小企業へ

ITmedia NEWS SPECIAL
監修 ITmedia NEWS

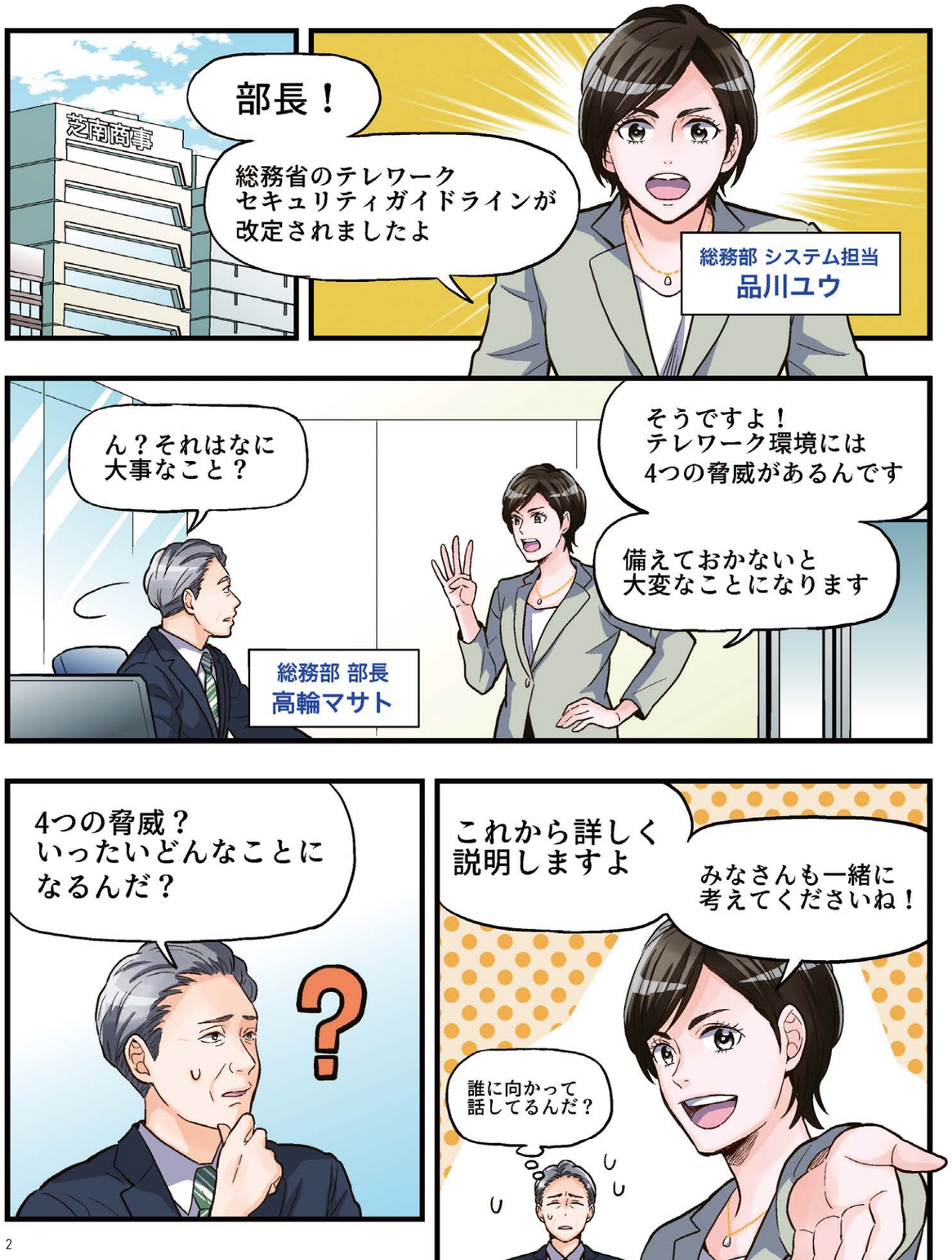
これで安心 PCセキュリティ

総務省「テレワークセキュリティガイドライン」より

ついにテレワーク導入を決めた中堅企業の芝南商事だが
セキュリティ対策にてんやわんや？
総務部長 高輪マサトと
システム担当 品川ユウによる

どたばたストーリー

テレワークを狙う4つの脅威とは？



テレワークにおける セキュリティリスクとは

総務省が呼びかけるテレワークのセキュリティ

2021年5月、総務省が「テレワークセキュリティガイドライン」(https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/)を改定し、第5版として公開しました。企業がテレワークを実施する際のセキュリティ上の不安を払拭し、安心してテレワークを導入・活用するための指針として公開されたガイドラインです。この中では、テレワークに際しての4つのリスクとその対策が明示されています。また、セキュリティの専任担当がいないような中小企業等におけるシステム管理担当者を対象として、テレワークを実施する際に最低限のセキュリティを確実に確保してもらうための手引き「中小企業等担当者向けテレワークセキュリティの手引き(チェックリスト)」第2版(令和3年5月)を作成・公表しています。今回は、この手引き(チェックリスト)に沿って、その内容と注意すべき点を、マンガを交えながら、わかりやすく説明していきます。

リスク1 マルウェア感染

- セキュリティ対策ソフトの未導入・更新不備
- アップデートの未実施
- 偽サイトへのアクセス
- なりすましメールに添付されたファイルの開封やリンクのクリック

▶ P4ー P7

リスク3 デバイスの紛失・盗難

- 電車の網棚に置いた端末入りバッグを失念
- カフェで端末を放置して長時間離席
- 暗号化せずに保存
- バックアップ未実施

▶ P12ー P15

テレワークに潜む
4つのリスク

リスク2 不正アクセス

- ファイアウォールなし
- 推測されやすいパスワードの使用
- パスワードの使い回し
- ログイン方法を書いたメモの放置
- アップデート未実施

▶ P8ー P11

リスク4 情報の盗聴

- 無線LANの設定不備
- 偽アクセスポイントへの接続
- 暗号化せずに送信
- 画面をのぞき見される
- 従業員による内部不正

▶ P16ー P19

起こりうるトラブル

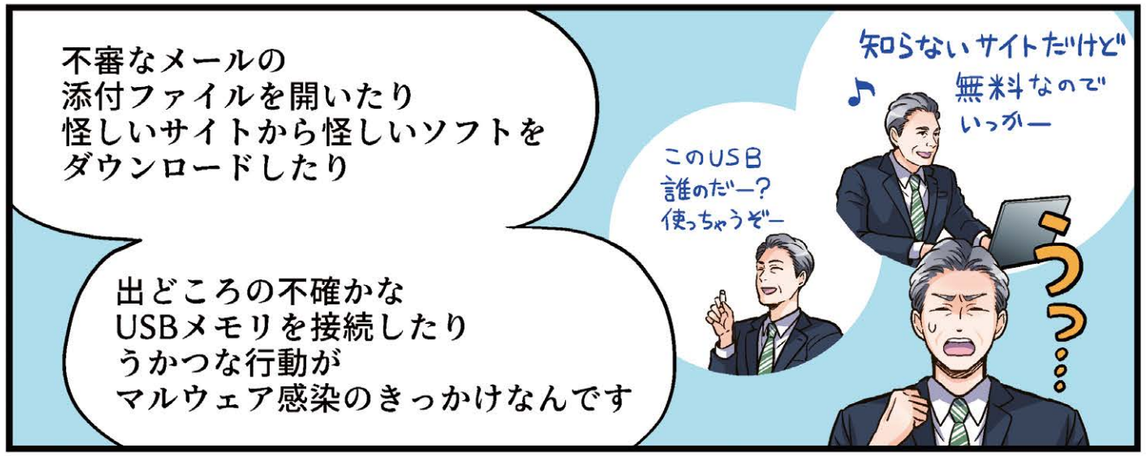
- 情報漏えい(機密性の喪失)
- 重要情報の消失(完全性の喪失)
- 作業中断(可用性の喪失)

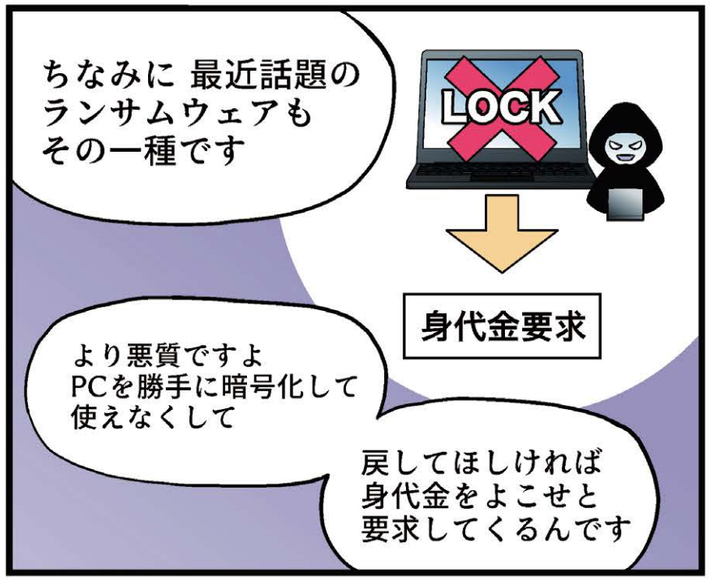
4つのリスクはPCセキュリティ強化で軽減できる

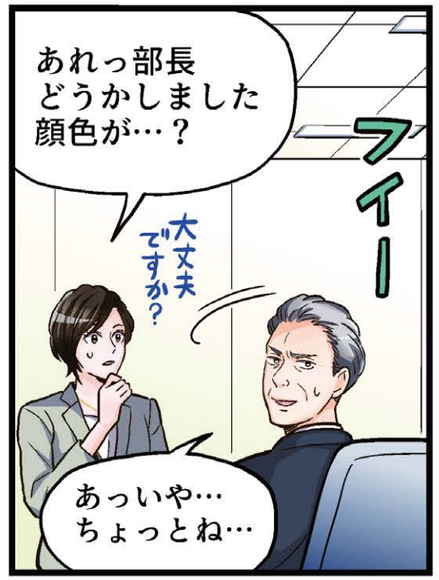
テレワーク環境では、会社にいるように情シス部門やPC担当者のサポートを受けることができません。PCを使う一人ひとりがセキュリティに気をつける必要があります。そして、上記の4つのリスクはいずれも放置したままでは、ビジネスの大きな損失につながる可能性が高いものです。しかし、それらのリスクはPCのセキュリティ機能によって、その大部分を回避することもできるのです。HP製ビジネスPCの多くの製品は先進のセキュリティ機能を網羅する「HP Wolf Security For Business」を搭載しており、4つのリスクを回避することを助けます。テレワークを導入したうえで、安全にビジネスを進めるためには、HP製ビジネスPCを選ぶことは、現時点での最適解といえます。

リスク1 マルウェア感染

マルウェア感染はリスクがいっぱい？







リスク1 マルウェア感染

倒産のリスクもある マルウェア感染

さまざまな経路でマルウェアはやってくる

マルウェアとは、悪意のあるソフトウェアや悪質なプログラムの総称。コンピューターウイルス、昨今話題になっているランサムウェアもマルウェアの一種です。マルウェアはメールの添付ファイルや悪意のあるWebサイト、あるいはUSBメモリなどに仕組まれ、あなたの会社のPCに侵入する機会を狙っています。不用意にメールの添付ファイルを開いたり、メール本文に記載されているURLをクリックすることには注意が必要です。また、怪しいWebサイトを閲覧したり、出どころが定かでないUSBメモリを使用することも避けましょう。

● マルウェア感染の事例

添付ファイル付きのメールを
受信し開封

悪意のあるサイトを閲覧し、
ソフトをダウンロード

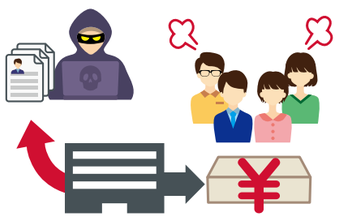
USBメモリを接続

被害者のはずが加害者になってしまう?

マルウェアに感染すると、PCの動作が妨害されたりデータが破壊されることによる「業務停止」や、データを不正に外部送信する「情報漏えい」などの被害が想定されます。流出したデータに個人情報や重要なビジネス機密が含まれていると、取引先や顧客の信用失墜や損害賠償の発生につながり、取引停止や倒産ということも考えられます。またランサムウェアに感染した場合、感染したPCを通じて社内のデータが勝手に暗号化されます。攻撃者は暗号化解除と引き換えに身代金を要求しますが、支払っても復旧されない可能性や、犯罪者への利益供与と見なされてしまうこともあり、支払いに応じることは推奨されません。

● 発生するのはこんな被害

マルウェアの被害



個人情報が漏えいし、
賠償義務の発生

ランサムウェアの被害

情報を復旧できず、
業務に影響が発生

共通の被害

感染発覚で取引先や顧客からの
信用失墜・取引停止

リスク1 マルウェア感染

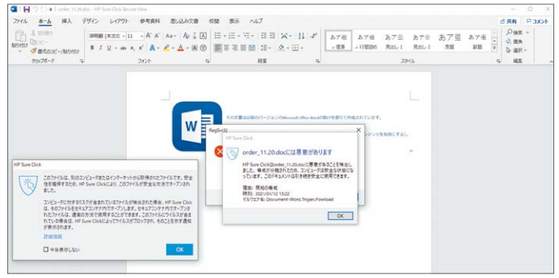
先進のPCセキュリティで マルウェアに備えよう

自社の状況に応じたセキュリティ対策を提供

「HP Wolf Security」は、仮想化技術を応用した脅威の封じ込め「HP Sure Click」や、AI活用によりマルウェア検知をする「HP Sure Sense」を中核とした最先端のセキュリティソリューションです。HPのPCだけではなく、他社製のPC向けには2022年4月に「HP Wolf Pro Security Service」を販売する予定で、運用や管理をHPのセキュリティエキスパートがサポートするサービスも付属します。自社のビジネス要件や現状のセキュリティレベル、人材の状況に合わせて選ぶことが可能です。またHPのEliteシリーズやProシリーズのPCに標準搭載されている「HP Wolf Security For Business」はサイバー攻撃を受けてしまうことを前提に、いかに健全な状態にPCを復旧するかという「サイバーレジリエンス」の発想で開発されたソフトウェアが多数搭載されており、「HP Wolf Pro Security（有償・2022年4月発売予定）」との組み合わせで他社製PCでは実現できない、強固なセキュリティ機能を提供します。

感染をなかったことにする「HP Sure Click」

メール添付やブラウザからダウンロードしたWordファイルの展開を、ハードウェア的に完全に分離された仮想マシンで行います。仕組まれたマルウェアが実行されても仮想マシン内に封じ込められ、アプリケーションを閉じると仮想マシンと共にマルウェアは削除されるため、PC本体に影響しません。また有償サービス「HP Wolf Pro Security」に含まれる「HP Sure Click Pro」では、Wordファイル以外に、Office（PowerPoint、Excel）ファイルやZipファイル、PDFなど、分離対象ファイルが拡がっているほか、フィッシングサイト対策機能による強力なID防御が可能です。

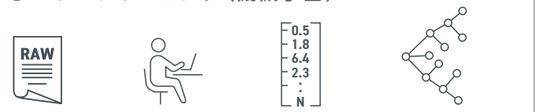


メール添付やインターネットを経由したWordファイルを隔離された環境で展開

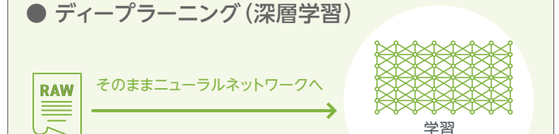
未知のマルウェアも検知する「HP Sure Sense」

機械学習AI、ディープラーニングAIおよび静的分析に基づく幅広い手法を利用した次世代型アンチウイルスです。既知のマルウェアはもちろん、パターンマッチングを用いるウイルス対策ソフトが取りこぼしてしまう未知のマルウェアも検出することができます。また有償サービス「HP Wolf Pro Security」に含まれる「HP Sure Sense Pro」では行動分析を利用してランサムウェアやシェルコード、ファイルレス攻撃など、より高度な攻撃にも対応することが可能です。

● マシーンラーニング（機械学習）

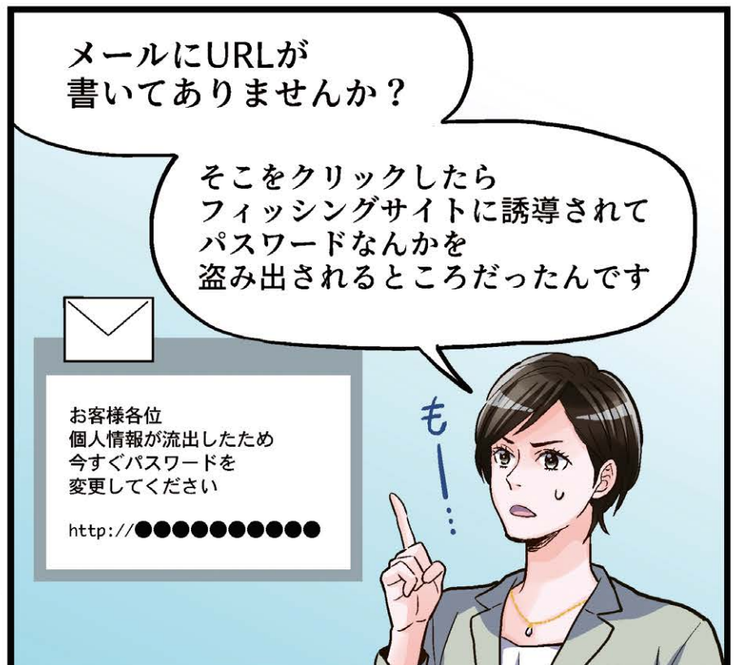


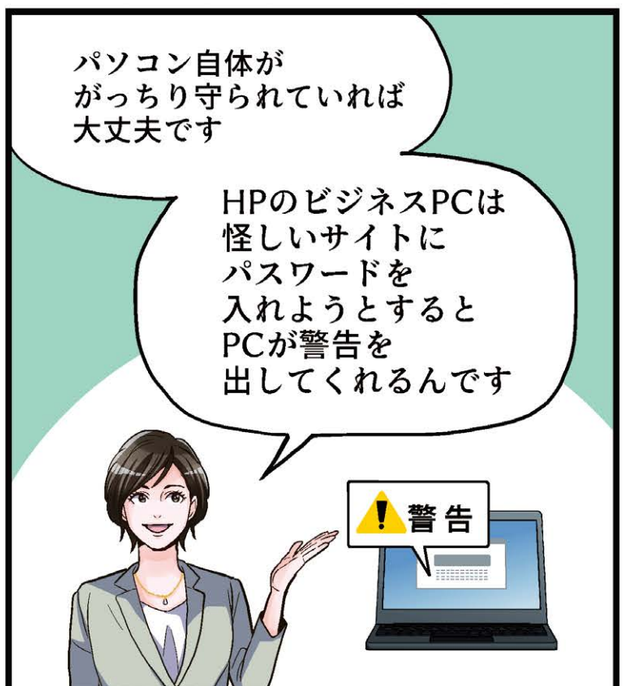
● ディープラーニング（深層学習）



リスク2 不正アクセス

不正アクセスには要注意？





リスク2 不正アクセス

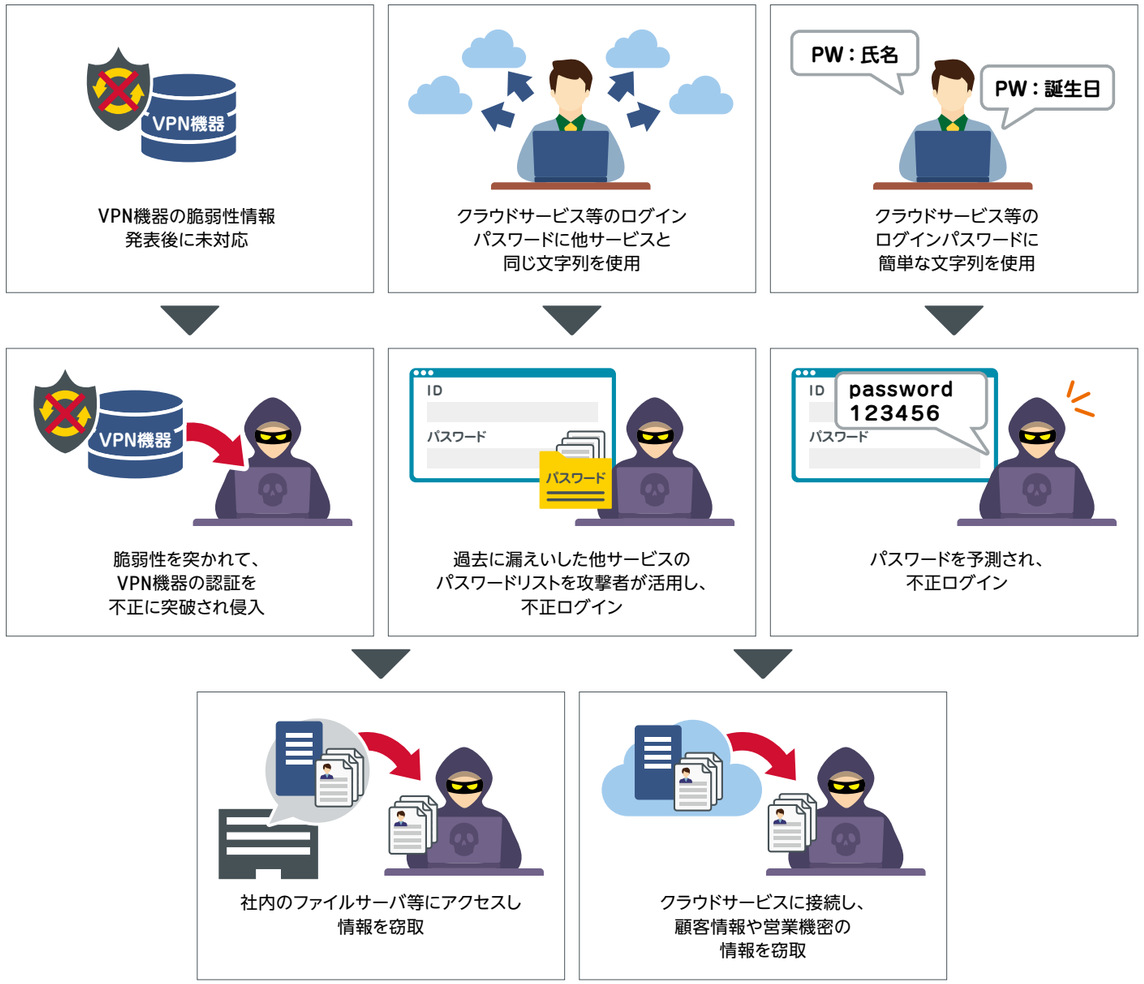
アカウント乗っ取りの第一歩 不正アクセスへの対策

世界のどこからでもパスワードの不正取得は可能?

不正アクセスとは、本来アクセス権限を持たない者が、システムにログインすることを指します。手段としては、なりすましメールやフィッシングサイトでIDやパスワードを不正に入手する、システムやソフトウェアの脆弱性を狙うなどがあります。さらに入手したIDやパスワードから類推されて、他のシステムへの不正アクセスに利用される場合もあります。

また、ダークマーケットでは不正入手されたID・パスワードが取引されているケースもあります。巧妙なフィッシングサイトから盗まれた場合には、不正アクセスに気づくことすら困難な場合があります。インターネットは世界中とつながっているため、不正アクセスは世界中のどこからでも行われる可能性があることを肝に銘じる必要があります。

● 不正アクセスの事例



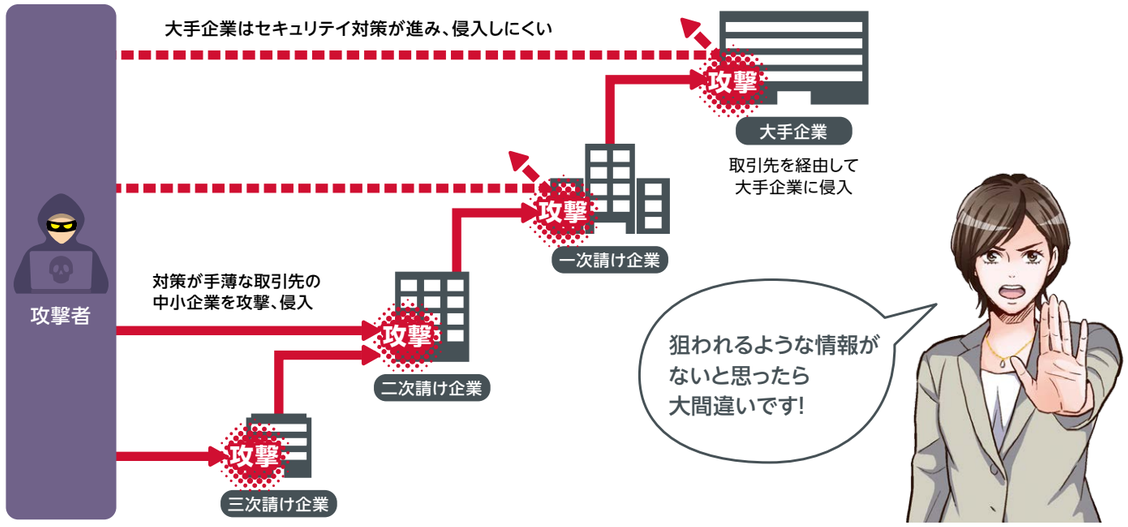
リスク2 不正アクセス

PCのログインIDを守る HPのソリューション

大手企業への踏み台にするために中小企業が狙われている

最近のサイバー攻撃ではセキュリティ対策が厳重な大手企業より、その取引先など、セキュリティ対策が手薄な中小企業に侵入し、そこを踏み台に大手企業を攻撃する手口も増えています。また、攻撃元の特定を困難にするため、複数のサイトを踏み台にするなど、より悪質に巧妙になっています。万一、あなたの会社が攻撃を受けた被害者になったとしても、それに気づかずにフィッシングサイトに誘導するなりすましメールを送るなど、取引先に被害を拡大させていたとしたら、あなたの会社も攻撃に加担したことになってしまいます。セキュリティ対策が手薄と思われている中小企業こそ、エンドポイントを守ることが重要なのです。

● セキュリティが手薄な中小企業が狙われる



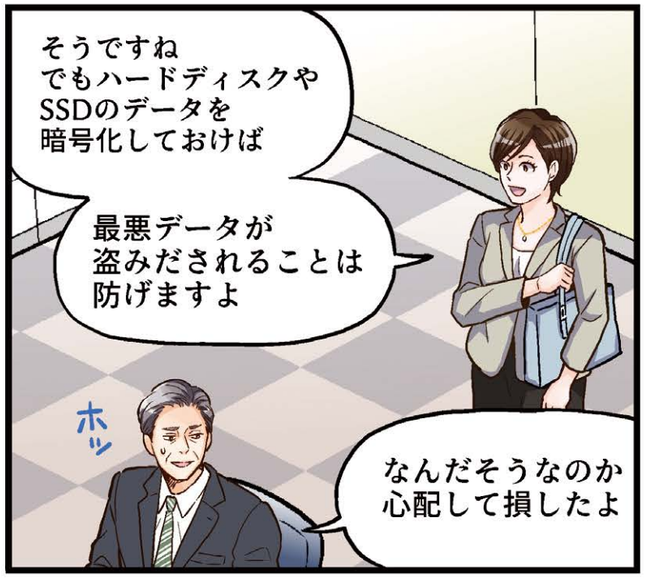
ログインIDを守る「アイデンティティ保護」

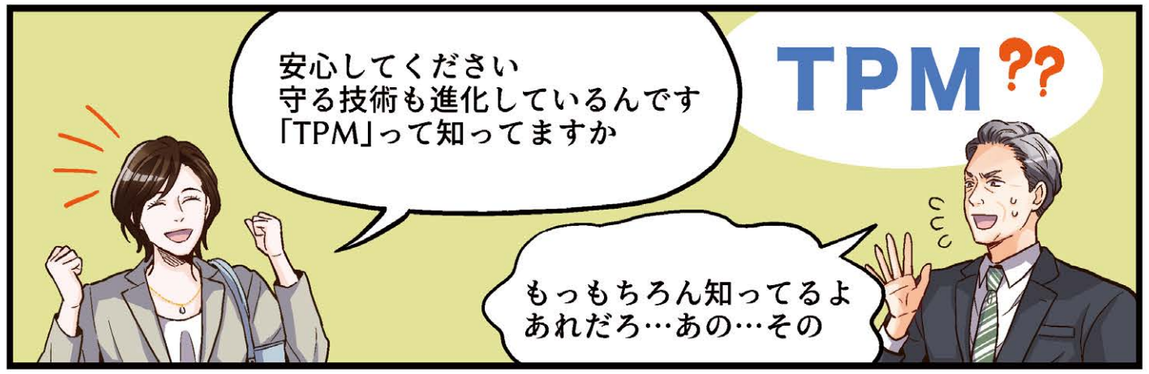
「HP Wolf Pro Security（有償・2022年4月発売予定）」の「アイデンティティ保護」にはフィッシングサイトによるIDやパスワードの盗難を防ぐ機能が実装されています。ECサイトなどを装ったフィッシングメールからフィッシングサイトに誘導された場合、IDやパスワードを入力するとアラート画面を表示。IDやパスワードが盗まれる前に、自動でそのページを無効化します。

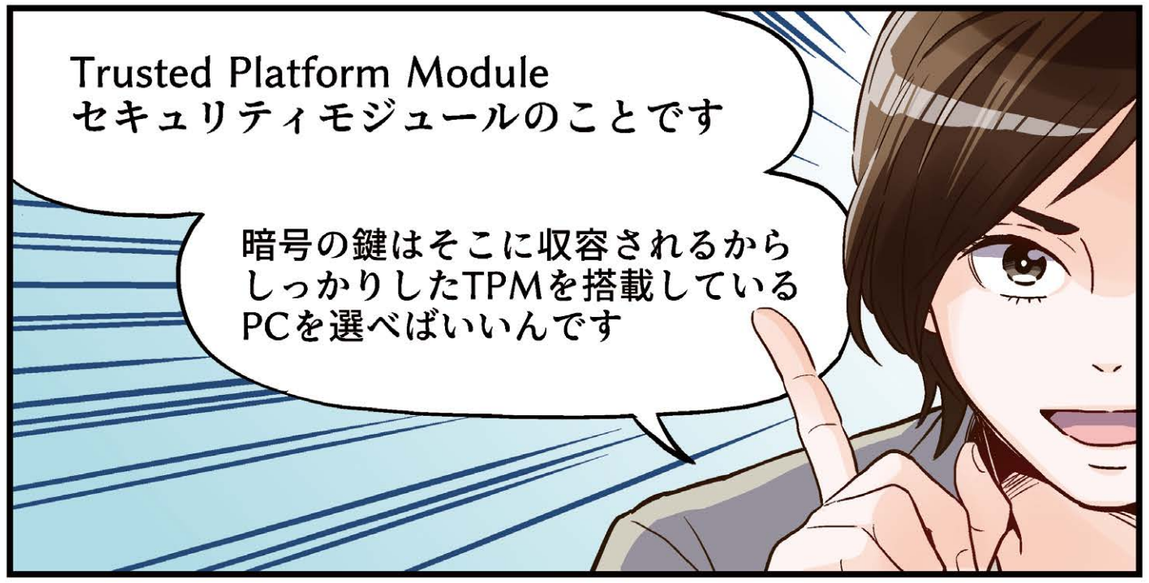
フィッシングサイトに誘導されるとPC画面全体にアラートを表示しID盗難を防ぐ

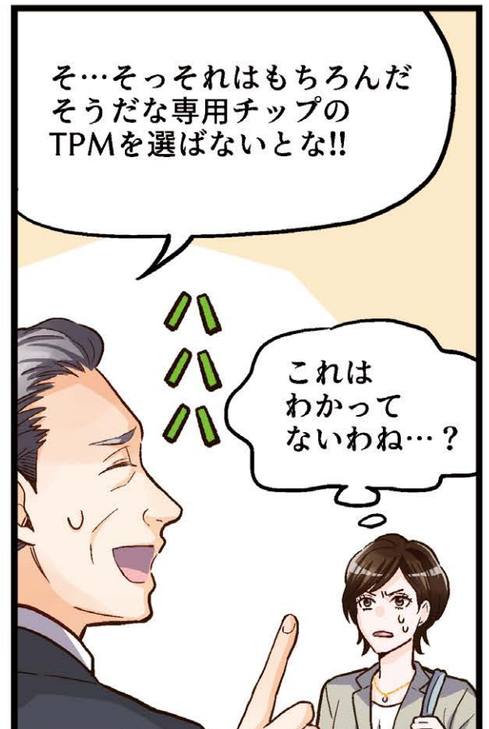
リスク3 デバイスの紛失・盗難

デバイスの紛失・盗難にご用心?









リスク3 デバイスの紛失・盗難

人の油断を突く デバイスの紛失・盗難

うっかりミスが取り返しのつかない事態に

テレワークの場合、外に持ち出したPCを置き忘れたり、盗まれたりしてしまうことも大きなリスクになります。たとえば、サテライトオフィスにPCを忘れてしまう、カフェでPC作業をしていて席を離れたすきにPCが盗まれてしまう、または電車での移動中、網棚に置いたままにしてしまうというケースもあるでしょう。被害としては、PCを初期化して転売される、不正ログインされて重要なデータが盗まれる、ハードディスクやSSDを抜き出してデータが盗まれるなどが想定され、「情報漏えい」の場合は、それに伴う「賠償責任」の発生や、取引先や顧客からの「信頼失墜」、「取引停止」など、取り返しのつかない事態につながる可能性があります。

● 端末の紛失・盗難の事例

端末を初期化して転売

不正ログインの上、
端末に保存された機密情報にアクセス

ハードディスクを取り出され、
保存された機密情報にアクセス

BitLockerでドライブを暗号化

PCの紛失・盗難に対しては、Windows OSに標準装備されるドライブ暗号化機能「BitLocker」が有効です。ハードディスクやSSDをはじめ、USBメモリや外付けハードディスクなどのドライブ全体を暗号化することにより、PC内のデータを不正アクセスから保護することができます。万一、PCを盗まれてドライブを抜かれてしまっても、ドライブ自体を暗号化しておけば、中身のデータを読まれることは阻止できます。

BitLockerのメリット

- ドライブ全体を暗号化できる
- ドライブを抜き出されても
  データ読み出しは不可能
- TPMに暗号鍵を
  安全に保管できる

▼

PCが盗難されても
情報漏えいは防ぐことができる

リスク3 デバイスの紛失・盗難

置き忘れや盗難にあっても 安心できる機能

ハードウェアベースでセキュリティを担保するHPのビジネスPC

近年のビジネスノートPCにはTPM（Trusted Platform Module）と呼ばれるセキュリティモジュールが搭載されています。この中には「BitLocker」の暗号鍵や認証情報など、重要な情報が格納されています。TPMには主にハードウェア（チップ）として独立して実装されるディスクリートTPMと、チップセット上に実装されるファームウェアTPMがあります。HPのビジネスノートPCに搭載されているディスクリートTPMはコンピューターセキュリティの国際標準規格であるCommon Criteria EAL4+とFIPS 140-2 Level 2の認定を得ていますので安心です。このディスクリートTPMが多彩なセキュリティ機能を司っているため、テレワークでも高度な安心をお届けすることができるのです。

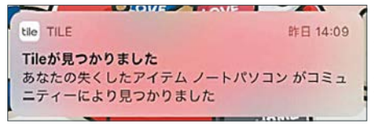
HPのビジネスノートPCに搭載されるTPMはハードウェアベースのディスクリートTPMなので安心

置き忘れてもPCが知らせてくれる

持ち出したノートPCを「位置」で見つけて紛失による情報漏えい防止に有効とされているのが、スマートトラッカー（忘れ物防止タグ）のTileです。
HPの法人向けノートPCブランドであるEliteシリーズやモバイルワークステーションのZBookシリーズ（※最新モデル）に標準搭載されています。バッテリから直接給電されるシステムにより、スリープ状態や電源OFF状態でも端末を探すことができ、リモートワークの際も安心です。

Bluetooth®の接続範囲内である場合は、PCがある場所をスマホに通知

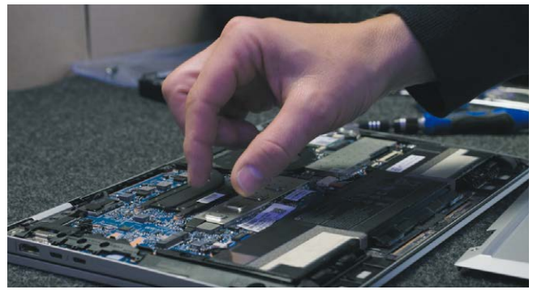
最後に検知した場所と時間を記録し、スマホの地図アプリなどに表示



世界中のTileコミュニティを通じて、PCを最後に検知した場所を通知

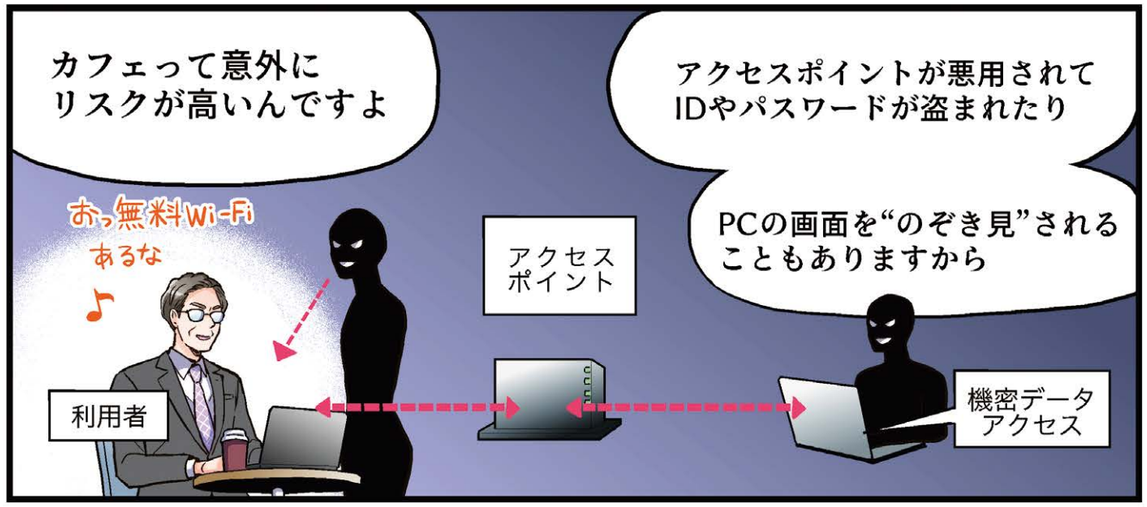
システムカバーをこじ開けるとPCをロック

PCのシステムカバーの取り外しによる、物理的な攻撃に対する防御ソリューションとして「HP Tamper Lock」を一部モデルで採用しています。たとえばPC輸送中や離席時、システムカバーを不正に取り外された場合には、その動きを検知してPCを自動でロックします。



リスク4 情報の盗聴

あなどれないPC画面の盗み見



リスク4 情報の盗聴

情報はいたるところで盗まれてしまう

テレワークでは情報盗聴の機会は増えてしまう?

物理的に隔離されている会社のオフィスとは異なり、テレワーク中は情報が盗まれる機会は格段に増加すると考えるべきです。第三者がいるカフェなどの環境では、PC画面を盗み見されるリスクがあります。インターネットへのアクセス手段としてカフェのフリーWi-Fiを利用する場合でも、悪意の第三者が無線を経由して通信内容を盗聴している可能性があります。フリーWi-Fiのアクセスポイント自体が乗っ取られているケースもあり、その場合はメール等の通信内容がだだ漏れになっているといってもいいでしょう。また、テレワークではリモート会議が恒常的に行われますが、そのURLが盗まれて悪意の第三者に不正に傍聴されてしまうことも考えられます。

● 情報の盗聴の事例

第三者がオンライン会議のURLを
不正に取得

端末にのぞき見防止フィルム等を
貼り付けずカフェでテレワーク

カフェの無線アクセス
ポイントを利用

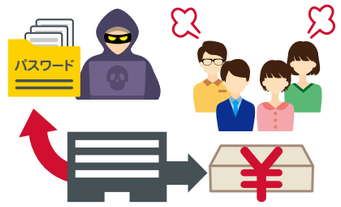
盗聴とは情報漏えいと同義であることに注意すべき

上記のような情報の盗聴は、情報漏えいに直結する事態といえます。盗み見されたPC画面に重要なビジネス情報が表示されていたり、オンライン会議で決定したビジネスの未公開情報が盗聴されていたら、株価の下落など、ビジネスに影響が出る事態も考えられます。フリーWi-Fiを使った通信からIDやパスワードが盗聴されていたら、それは不正アクセスの元凶となり、事業継続を困難にする重大な危機につながりかねない局面です。あらゆる業種のさまざまな仕事にPCが使われている以上、中小企業を含むすべての企業はこうしたリスクにもっと警戒感を持つべきなのかもしれません。

● 情報が盗聴されるとこんなリスクが発生する

SNS等で未公開情報が公開され、
事業影響が発生

盗聴の発覚により、
取引先や顧客からの信頼失墜・取引停止



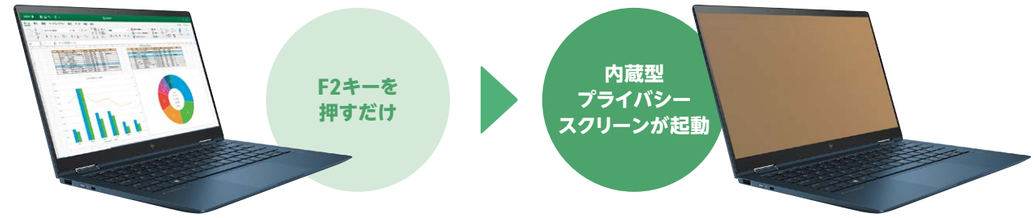
ID/パスワード悪用で
顧客情報漏えい・賠償責任が発生

リスク4 情報の盗聴

情報の盗み見に備えられる機能でビジネスを守る

プライバシースクリーンをPCに内蔵したHP Sure View

PC画面の盗み見はもっとも古典的でありながら、未だに有効なサイバー攻撃といえます。これを防ぐ方策としてはプライバシースクリーンがありますが、PCとは別途用意する必要があるうえ、取り外しも煩雑。タッチスクリーンのPCではタッチ操作が不安定になってしまいます。これらのデメリットを解消するのが内蔵型プライバシースクリーン機能「HP Sure View」です。簡単なボタン操作でユーザー以外の視点からPC画面を見えにくくします。タッチ操作にも支障なく、機能のON/OFFもボタンひとつの手軽さです。



Wi-Fiに頼らずに通信が可能なLTEモデルも選べる

HP ビジネスPCの多くのモデルでは携帯キャリア各社の回線を利用するLTE対応モデルが選べます。Wi-Fiがない環境でもネットワークにアクセスできます。また、最新の通信規格5Gに対応するモデルもラインアップしています。

パワフルで薄型デザインのビジネスコンバーチブルPC

HP Elite Dragonfly G2

最小構成で重さ1kgを切る*コンパクトボディ。場所や時間にとらわれることなくあらゆるシーンで仕事を可能にします。LTEモデルも選択可能です。

*質量989gは、512GB SSD以上のストレージ非搭載又はHP Sure View Reflect(内蔵プライバシースクリーン機能)非搭載での質量です。構成により質量は異なります。

圧倒的なパワーと強固なセキュリティでビジネスを加速する軽量モバイルノートPC

HP ProBook 635 Aero G8

軽量かつコンパクトなボディにビジネスユーザーの厳しい要求を満たす耐久性、高度なセキュリティ機能を備えています。LTEモデルも選択可能です。

進化するサイバー攻撃のさらに上をいく
HP Wolf Security ポートフォリオ

サイバー攻撃は日々進化し、悪質化・巧妙化しています。
そして 攻撃者が狙うのはネットワークのエンドポイント＝入口であるPCです。
今やPCのセキュリティを高めることは、単なる「情報の保護」にとどまらず「事業の継続」そのものです。
HPでは以前よりPCのセキュリティ（デバイス自体のセキュリティ）に注目し、製品開発を実施してきました。
その最新の成果が「HP Wolf Security」です。

HP Wolf Security ポートフォリオ

HP WOLF SECURITY

HP ビジネスPCに組み込まれるセキュリティ

HP PRO、HP ELITE、HP Zシリーズで標準搭載

HP WOLF SECURITY FOR BUSINESS

OSの下を保護する

- **HP Sure Start**
  ファームウェア攻撃から保護し自動復旧
- **HP Sure Run**
  重要プロセス停止から自動復旧
- **HP Sure Recover**
  破壊型ワイパー攻撃からの復旧
- **HP Sure Admin**
  侵入される前にBIOSをロック
- **HP BIOSphere**
  不正なGPT書き換えや破損から保護
- **HP Secure Erase**
  BIOSから内蔵ドライブのデータ完全消去
- **HP Tamper Lock**
  物理的な侵入攻撃からの保護

OSの中を保護する

- **HP Sure Click**
  Web・Eメール経由の脅威封じ込め
- **HP Sure Sense**
  マルウェア防止
- **HP Presence Aware**
  ユーザーを自動検知しデバイスをロック&解除

OSの上を保護する

- **HP Sure View**
  のぞき見による機密情報漏えい防止
- **HP Privacy Camera/HP Sure Shutter**
  プライバシーを守るカメラシャッター（手動／電動）

HP WOLF PRO SECURITY

一部のHP PRO、HP ELITE シリーズで選択可能

起動したらすぐに保護。
HP製ビジネスPCに組み込まれた次世代型ウイルス対策ソフト

HP WOLF PRO SECURITY EDITION

HP WOLF PRO SECURITY
※2022年4月頃発売予定

- **HP Sure Click Pro**
  Web・Eメール・USBストレージ経由の脅威封じ込めアイデンティティ保護
- **HP Sure Sense Pro**
  マルウェア防止

他社製PCを含めて包括的に保護するセキュリティ

デバイス横断型のソフトウェア・サービス（HPおよび他社のWindows 10/11搭載PC）

リソース不足のIT部門を支援するマネージドサービス（ウイルス対策ソフトの管理）

HP WOLF PRO SECURITY SERVICE
※2022年4月頃発売予定

- PCの保護状態が分かる ダッシュボード
- HPのセキュリティ専門家による設定、脅威分析サービス

HP WOLF ENTERPRISE SECURITY

セキュリティ担当チーム向けの脅威インテリジェンスサービス

HP SURE CLICK ENTERPRISE

このような企業様へお勧め

- IT管理者不在or兼任されている。
- テレワークにおけるセキュリティ対策ができていない。
- HPのPC購入後、基本設定した後すぐに利用する。

- IT管理者不在or兼任されている。
- テレワークにおけるセキュリティ対策ができていない。
- 複数メーカーのPCが混在している。

- IT管理者はいるが、セキュリティに関する人材が不足している。

※PC50台以上をお持ちの企業様向け

テレワークにおけるセキュリティ対策と想定脅威およびHPのソリューション

総務省では「テレワークセキュリティガイドライン」の改定に際して、テレワーク実施における
セキュリティについてのチェックリストを公開しています。このチェックリストに則って
あなたの会社の現況を再確認することで、今後のセキュリティ強化の方針を明らかにすることができます。
さらに、想定脅威への対応をアシストすることが可能なHP ビジネスPCのセキュリティ機能・ソリューションのご案内など、
HPからの提案も合わせて併記しました。このリストを活用し、安心・安全なテレワーク環境の実現にお役立てください。

テレワークセキュリティチェックリスト + HPからの提案

No.	分類	対策内容	想定脅威	想定脅威（詳細）	優先度	備考	HPからの提案
1-1	資産・構成管理	許可したテレワーク端末のみがテレワークに利用されており、利用されるテレワーク端末とその利用者を把握している。	マルウェア感染 不正アクセス 紛失・盗難	情報資産の管理そのものが直接的な対策になるわけではなく、その他の対策を実施する際の前提となる対策。 テレワークで利用している機器とその利用者を把握できていない場合、機器に対する各種セキュリティ対策が未実施の端末が存在するリスクが増加する。 また、シリアルナンバー等の端末固有の情報を把握していない場合、端末の紛失や盗難時にその実態を把握することが困難であるなどのリスクが増加する。	◎		**HP Proactive Insights** HP Proactive Insightsにより、テレワーク端末を管理し、各種セキュリティ対策がとられていることを適宜確認します。また、端末の紛失や盗難時に、該当端末のシリアルナンバー等の端末情報をリアルタイムに把握します。
1-2	資産・構成管理	テレワークで利用しているシステムや取り扱う重要情報※1を把握している。 ※1 営業秘密等の事業に必要で組織にとって価値のある情報や、顧客や従業員の個人情報等の管理責任を伴う情報	不正アクセス 情報の盗聴	情報資産の管理そのものが直接的な対策になるわけではなく、その他の対策を実施する際の前提となる対策。 テレワークで実施している業務やその際に利用しているシステム、そして、テレワークで取り扱う重要情報について把握していない場合、システムを適正な利用者が利用しているのか、またデータ管理等に関する各種セキュリティ対策が十分であるかといった懸念が増加する。	◎		テレワークで利用するシステムや、業務で取り扱う重要情報は、資産管理システム、または、Excel等の台帳により適切に管理します。
2-1	マルウェア対策	テレワーク端末にウイルス対策ソフトをインストールし、リアルタイムスキャンが有効になる設定としている※2。またウイルス対策ソフトの定義ファイルを自動更新する設定、又は手動で最新に更新するルールを作成している。 ※2 Windows製品に標準で導入されているウイルス対策ソフト（Windows Defender）を利用する場合、またiOS製品で、安全であることが確認できる方法（公式アプリケーションストアの利用等）でインストールしたアプリのみを利用している場合は、インストール作業は不要	マルウェア感染	最新化されたウイルス定義ファイルであれば駆除できていたマルウェアの駆除ができないため、テレワークで利用している端末のマルウェアに感染するリスクが増加する。	◎		**HP Sure Sense Pro** テレワーク端末にインストールされたHP Sure Sense Proにより、AIベース、および、シグネチャベースのアンチウイルス機能で、既知、および、未知のウイルスをリアルタイムに検知、対応します。シグネチャベースアンチウイルスの定義ファイルは自動更新します。
2-2	マルウェア対策	不審なメールを開封し、メールに記載されているURLをクリックしたり、添付されているファイルを開いたりしないよう注意喚起をしている。また利用しているメール製品に不審なメールを除外する機能がある場合は有効化している。（クラウドサービス（Webメール）の利用が無い場合は対象外）	マルウェア感染	不審なメールに記載されているURLにアクセスすることで悪意のあるサイトに誘導され、マルウェアの感染や、重要情報にアクセスするための認証情報等が窃取されるリスクが増加する。 また、不審な添付ファイルを開くことでマルウェアに感染するリスクが増加する。	○	クラウドサービス（Webメール）の利用無しの場合は対象外	**HP Sure Click Pro** HP Sure Click Proにより、ユーザーが誤って不審なメールの添付ファイルを実行、または、メールに記載されているURLをクリックしてしまっても、端末に影響がないように脅威を分離します。
2-3	マルウェア対策	テレワーク端末（スマートフォン等）へのアプリケーションのインストールは、安全であることが確認できる方法（公式アプリケーションストアの利用等）によるインストールに限定する。	マルウェア感染	公式アプリケーションストア上からアプリケーションをインストールしていない場合、正規のアプリケーションを模したマルウェアが含まれている可能性があるため、マルウェアに感染するリスクが増加する。	○		**HP Proactive Endpoint Management** HP Proactive Endpoint Managementにより、テレワーク端末へインストールするアプリケーションを、指定の安全なもののみに管理、制限します。
3-1	アクセス制御・認可	システムによるアクセス制御や重要情報そのものに対するパスワード設定等により、重要情報は許可された人のみが利用できるようにしている。	不正アクセス	重要情報へのアクセスを業務上必要な人のみに制限するようにしていない場合、本来アクセス権限が必要ではない人のアカウントが不正利用されたり、利用者が操作ミスをしたりすることにより重要情報が流出するリスクが増加する。	◎		Active Directory環境を構築し、アカウント、パスワードの管理を集中管理し、重要情報へのアクセスを許可された人のみに制限します。
3-2	アクセス制御・認可	インターネット経由で社内システムにアクセスする際に、社内ネットワークとインターネットの境界に設置されているファイアウォールやルーター等において、不要なポートへの通信や必要なIPアドレス以外からの通信を遮断している。	不正アクセス	不要なポートや必要なIPアドレス以外からの通信が遮断されていない場合、それらを狙った悪意のある攻撃（脆弱性を突いた攻撃やアカウントのなりすまし等）により不正アクセスされるリスクが増加する。	○	オフィスネットワークに接続しない場合は対象外	ファイアウォールやルーター等を自社で構築している場合、通信を許容するポートやIPアドレスを適切に設定しておきます。プロバイダーが提供するファイアウォールを利用している場合、プロバイダーと適切にコミュニケーションを行います。
3-3	アクセス制御・認可	オンライン会議の主催者はミーティングの開始時及び途中参加者がいる場合に、参加者の本人確認を実施している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴	オンライン会議の開始時や途中参加者がいる場合に本人確認を実施しないことにより、会議に不適切な利用者が不正に参加していることに気付くことができず、情報漏えいのリスクが増加する。 オンライン会議においては、本人と対面しないため、参加者がシステム上に表示されている名前の本人であることをカメラによるビデオ映像や音声等の方法により確認をする必要がある。	○	クラウドサービス（オンライン会議）利用無しの場合は対象外	以下のガイドラインを参照し、Web会議を適切に設定し、社内ルール、プロセスを決めて周知します。 ●Zoomの場合の例：設定解説資料（Zoom） https://www.soumu.go.jp/main_content/000706653.pdf
3-4	アクセス制御・認可	オンライン会議にアクセスするためのURLや会議参加のパスワードを必要なメンバーだけに伝えるようにしている。また会議参加のパスワード設定を強制させることが可能な場合は、パスワード設定を強制している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴	オンライン会議の参加のためのURLやパスワードを、必要ない利用者に伝えることで、会議に不適切な利用者が不正に参加し、会議を通じた情報漏えいのリスクが増加する。 また、パスワードの設定を強制しない（できない）場合は、利用者がパスワードを未設定にしたり、容易に推測可能なパスワードを設定したりすることにより、会議への不正参加のリスクが増加する。	○	クラウドサービス（オンライン会議）利用無しの場合は対象外	以下のガイドラインを参照し、Web会議を適切に設定し、社内ルール、プロセスを決めて周知します。 ●Zoomの場合の例：設定解説資料（Zoom） https://www.soumu.go.jp/main_content/000706653.pdf **HP Sure Click Pro** また、HP Sure Click Proのアイデンティティ保護機能により、フィッシングサイトによるID/パスワードの情報漏えいを防ぎます。

テレワークにおけるセキュリティ対策と想定脅威およびHPのソリューション

No.	分類	対策内容	想定脅威	想定脅威（詳細）	優先度	備考	HPからの提案
3-5	アクセス制御・認可	オンライン会議の主催者は必要に応じて不適切な参加者を退出させるなどし、会議を適切に進行している。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴	オンライン会議において、不適切な参加者が確認され、会議主催者による強制退出が実施できない場合、適切な業務の遂行が実施できないリスクが増加する。	○	クラウドサービス（オンライン会議）利用無しの場合は対象外	以下のガイドラインを参照し、Web会議を適切に設定し、社内ルール、プロセスを決めて周知します。 ●Zoomの場合の例：設定解説資料（Zoom） https://www.soumu.go.jp/main_content/000706653.pdf
4-1	物理セキュリティ	テレワーク端末に対してのぞき見防止フィルタを貼付し、離席時にはスクリーンロックをかけるようルール化している。	情報の盗聴	テレワークの作業環境は、オフィス環境に比べて、家族を含む業務と関係ない人物が、物理的にテレワーク端末をのぞき見（ショルダーハッキング）することが比較的容易な環境であることが懸念される。のぞき見防止フィルタの貼付や、離席時のスクリーンロックの実施を行わない場合、テレワーク端末越しの情報漏えいや不正利用のリスクが増加する。	◎		**HP Sure View** ハードウェア組み込みののぞき見防止フィルタ機能であるHP Sure Viewにより、ショルダーハッキング等の物理的なのぞき見からの情報漏えいを防御します。
5-1	脆弱性管理	テレワーク端末はメーカーサポート切れとなるバージョンのOSやアプリケーションは利用していない。	不正アクセス	テレワーク端末のOSやアプリケーションとしてメーカーサポート切れの製品を利用している場合、製品としてセキュリティアップデートが行われないため、製品の脆弱性に対する攻撃により不正アクセス等のリスクが増加する。	◎		**HP Proactive Insights** HP Proactive Insightsにより、テレワーク端末のOSやアプリケーションのバージョンをリアルタイムに把握、管理し、メーカーサポート切れの製品を利用していないか確認します。
5-2	脆弱性管理	テレワーク端末のOSやアプリケーションに対して最新のセキュリティアップデートを適用している。	不正アクセス	テレワーク端末のOSやアプリケーションが最新のセキュリティアップデートを適用していない場合、製品の脆弱性に対する攻撃により不正アクセス等のリスクが増加する。	◎		**HP Proactive Insights** HP Proactive Insightsにより、テレワーク端末のOSやアプリケーションのバージョンをリアルタイムに把握、管理し、アップデートが必要な端末を検知します。
5-3	脆弱性管理	テレワークで利用する自宅の無線LANルーター等のネットワーク機器は、メーカーサポートが切れている製品を利用しておらず、最新のファームウェアを適用している。	不正アクセス	自宅に設置する無線LANルーター等のネットワーク機器について、メーカーサポート切れや古いファームウェアの状態で利用している場合、該当ファームウェアの脆弱性に対する攻撃による不正アクセス等のリスクが増加する。	○		テレワークにおける家庭内ルーターの適切な設定、管理方法を文書化し、利用者に周知、徹底します。
5-4	脆弱性管理	テレワーク端末から社内にリモートアクセスする際に利用するVPN機器等について、メーカーサポート切れの製品は利用せず、最新のセキュリティアップデートを適用している。	不正アクセス	テレワークを実施するために社内に設置しているVPN機器は、インターネットに常時接続され、オフィスネットワークへの入り口となる。 そのため、メーカーサポート切れや古いファームウェアの状態で利用している場合、ファームウェアの脆弱性に対する攻撃による不正アクセス等のリスクが増加する。	◎		社内に設置されているリモートアクセス用のVPN機器等のサポート状態を確認し、また、ファームウェアのバージョンが適切にアップデートされていることを確認します。
6-1	通信暗号化	クラウドサービス（Webメール、チャット、オンライン会議、クラウドストレージ等）を利用する場合（特にID・パスワード等を入力するとき）は、暗号化されている（HTTPS通信である）ことと、接続先のURLが正しいことを確認している。（クラウドサービスを利用していない場合は対象外）	情報の盗聴	無線LANを利用したり、自宅外でテレワークを行ったりするときに、通信内容が暗号化されていない場合、悪意のある第三者による通信の傍受により情報漏えいするリスクが増加する。	○	クラウドサービスを利用していない場合は対象外	**HP Sure Click Pro** HP Sure Click Proのアイデンティティ保護機能により、利用サイトがHTTPS通信を利用していなかったり、悪意のあるURLである場合、ID/パスワードの入力ができないように自動的に制御します。
6-2	通信暗号化	無線LANルーターを利用する場合は、無線LANのセキュリティ方式として「WPA2」又は「WPA3」を利用して、無線の暗号化パスワードは第三者に推測されにくいものを利用している。	情報の盗聴	公衆無線LANや自宅設置の無線LANのセキュリティ方式としてWPA2やWPA3以外（WEP・WPA）を利用している場合、悪意のある第三者が通信を傍受することで、通信内容を盗み見られ、情報漏えいするリスクが増加する。 無線LAN使用時のセキュリティ確保（セキュリティ方式の詳細を含む）については、総務省が公表している、「無線LAN（Wi-Fi）のセキュリティに関するガイドライン」を参考にしてください。 https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/	○		以下のガイドラインを参照し、テレワークにおける公衆無線LANや自宅設置の無線LANとの通信方式を適切に設定するよう文書化し、利用者に周知、徹底します。 ●無線LAN（Wi-Fi）のセキュリティに関するガイドライン https://www.soumu.go.jp/main_sosiki/cybersecurity/wi-fi/
7-1	インシデント対応・ログ管理	情報セキュリティインシデント発生時に備えて、インシデントが発生した場合や、そのおそれがある状況（不審なメールを開封した場合等）における対応手順を決定しており、関係者への各種連絡体制を定めている。	マルウェア感染 不正アクセス 紛失・盗難 情報の盗聴	情報セキュリティインシデント発生時の対応手順や、関係者への連絡体制が定められていない場合、セキュリティインシデントの発生自体の把握や被害拡大の早期防止等ができずに、セキュリティインシデント全般の発生時の被害が増大するリスクが増加する。 また、迅速な初動を行うため、インシデントが発生したとわかったときだけでなく、そのおそれがあるときから、積極的に情報連絡を行うことを周知しておく必要がある。	◎		**HP Wolf Pro Security Service** HP Wolf Pro Security Serviceにより、インシデントが発生した場合に管理者に対してリアルタイムにメール通知します。メールの内容による対応手順をあらかじめ決めており、管理者は迅速に対応します。
7-2	インシデント対応・ログ管理	テレワーク端末と接続先の各システムの時刻が同期されるように設定している。	マルウェア感染 不正アクセス 紛失・盗難 情報の盗聴	テレワーク端末と接続先の各システムの時刻がずれている場合、情報セキュリティインシデント発生時の原因調査において各種システムログを利用した原因や被害状況の特定や絞り込みの難易度が高くなり、その結果、インシデントによる被害拡大防止のための適切な対応を実施することができずにセキュリティインシデント全般の発生時の被害が増大するリスクが増加する。	○		端末の時刻が自動的にタイムサーバーと同期されるよう、Active Directory、または、ローカルPCで適切にポリシーを設定します。
7-3	インシデント対応・ログ管理	テレワーク端末からオフィスネットワークに接続する際のアクセスログを収集している。	マルウェア感染 不正アクセス 紛失・盗難 情報の盗聴	テレワーク端末からオフィスネットワークに接続する際のアクセスログを収集していないことで、情報セキュリティインシデント発生時の原因調査において原因や被害状況の特定や絞り込みが困難になり、その結果、インシデントによる被害拡大防止のための適切な対応を実施することができずにセキュリティインシデント全般の発生時の被害が増大するリスクが増加する。	○	オフィスネットワークに接続しない場合は対象外	VPN機器等でアクセスログを収集、管理できるよう設定します。または、リモートアクセスサービスを提供するサービスプロバイダからログを入手できるようにコミュニケーションします。
8-1	データ保護	テレワーク端末（スマートフォン等）の紛失時に端末の位置情報を検出できるようにしている。	紛失・盗難	テレワーク環境においては、オフィス等で業務を実施する場合に比べて、テレワーク端末の紛失や盗難のリスクが高い。テレワーク端末の位置情報を検出するためのアプリケーションを導入していない場合、紛失時の早期発見が困難となることで悪意のある第三者の取得による不正なデータアクセス等の情報漏えいのリスクが増加する。	○	スマートフォン等のみ対象	**HP Proactive Insights** HP Proactive Insights、または、Tileサービスにより、テレワーク端末紛失時に、端末の位置情報をリアルタイムに検出します。
8-2	データ保護	テレワーク端末（スマートフォン等）の紛失時にMDM※3等を導入し、リモートからのデータの消去、ログイン時の認証ポリシーやハードディスクの暗号化などのセキュリティ設定を強制的に適用している。 ※3 Mobile Device Managementの略称で、スマートフォン等を一元的に管理・運用すること、又はその機能を提供するソフトウェア	紛失・盗難	テレワーク環境においては、オフィス等で業務を実施する場合に比べて、テレワーク端末の紛失や盗難のリスクが高い。リモートからデータ削除を行う機能や、ログイン時の認証ポリシーやハードディスクの暗号化等を強制していない場合、紛失時に悪意のある第三者が取得することによる不正なデータアクセス等の情報漏えいのリスクが増加する。	○	スマートフォン等のみ対象	**HP Proactive Endpoint Management** HP Proactive Endpoint Managementにより、ログインポリシーや暗号化の状態を把握管理し、また、テレワーク端末紛失時にリモートからロックやデータ消去を行います。
8-3	データ保護	テレワーク端末の紛失・盗難時に情報が漏えいしないように、ハードディスクやフラッシュメモリ※4等の内蔵された記録媒体の暗号化を実施している※5。（端末に会社のデータを保管しない場合は対象外） ※4 ハードディスクとは異なる記録媒体の一つで、「不揮発性の半導体メモリ」をさす。電源をおとしてもデータを保持することが可能な記録媒体 ※5 iOS製品については初期状態で暗号化されているため対応不要	紛失・盗難	テレワーク環境においては、オフィス等で業務を実施する場合に比べて、テレワーク端末の紛失や盗難のリスクが高い。ハードディスクの暗号化を実施していない場合、取得されたハードディスクの読み取りが可能な装置に接続することで、アカウントの認証無しにデータにアクセスされることが可能であり、保存している情報が漏えいするリスクが増加する。	○	端末に会社のデータを保管しない場合は対象外	**ディスクリートTPM** BitLockerなどの暗号化機能、製品により、端末に保存されたデータを暗号化し、端末紛失・盗難時の情報漏えいを防止します。また、暗号化キーをディスクリートTPMに保存することで、より強固に暗号化キーを管理します。

テレワークにおけるセキュリティ対策と想定脅威およびHPのソリューション

No.	分類	対策内容	想定脅威	想定脅威（詳細）	優先度	備考	HPからの提案
8-4	データ保護	テレワーク端末には原則として重要情報を保管しておらず、もし重要情報を保管しなければならない場合※6には、ファイルの暗号化（パスワード設定等）を実施している。（端末に会社のデータを保管しない場合は対象外） ※6 テレワーク端末にファイル保存するケースであり、ファイルサーバやクラウドサービス内に保存するケースは対象外	紛失・盗難	テレワーク環境においては、オフィス等で業務を実施する場合に比べて、テレワーク端末の紛失や盗難のリスクが高い。テレワーク端末に保管された重要情報に対してパスワード設定等の暗号化を実施していない場合、ハードディスクの盗難時やマルウェア等による不正アクセス時にテレワーク端末に保存されている重要情報にアクセスされた場合の情報漏えいのリスクが増加する。	○	端末に会社のデータを保管しない場合は対象外	**ディスクリートTPM** **BitLockerなどの暗号化機能、製品により、端末に保存されたデータを暗号化し、端末紛失・盗難時の情報漏えいを防止します。また、暗号化キーをディスクリートTPMに保存することで、より強固に暗号化キーを管理します。**
8-5	データ保護	オンライン会議を実施する際に、会議のタイトルや議題に重要情報を記載しないことや、会議の録画ファイルに対してパスワードの設定や期間指定の自動削除等を実施している。上記のルールを強制することが可能な場合は、強制するように設定する。（クラウドサービス（オンライン会議）の利用が無い場合は対象外）	情報の盗聴	オンライン会議について、適切なルールを遵守しないと、公開情報（会議のタイトル等）に重要情報を含めてしまう、会議中に共有する予定ではないデスクトップ画面情報等を誤操作により共有してしまう、会議の録画ファイルが不適切な第三者に参照される、等による情報漏えいのリスクが増加する。 また、上記のルールをシステム的に強制できない場合、利用者がルールを守らないことによる情報漏えいリスクの増加が発生する。	○	クラウドサービス（オンライン会議）利用無しの場合は対象外	以下のガイドラインを参照し、Web会議を適切に設定し、社内ルール、プロセスを決めて周知します。 ●Zoomの場合の例：設定解説資料（Zoom） https://www.soumu.go.jp/main_content/000706653.pdf
9-1	アカウント・認証管理	テレワーク端末のログインアカウントや、テレワークで利用する各システムのアカウントのパスワードは破られにくい「長く」「複雑な」パスワードを設定している。またパスワード強度を強制することが可能である場合は強制するように設定している。	不正アクセス	従業員が利用する端末のログインアカウントや、テレワークで利用するシステムのアカウントのパスワードが破られやすい容易なパスワードに設定している場合、悪意のある第三者にパスワードが把握されやすくなり、なりすましによる不正アクセスが行われるリスクが増加する。	◎		端末へのログインアカウントのパスワードの強度を強制するよう、Active Directory、または、ローカルPCで適切にポリシーを設定します。
9-2	アカウント・認証管理	テレワーク端末へログインするためのパスワードや、テレワークで利用する各システムのアカウントの初期パスワードは変更している。	不正アクセス	従業員が利用する端末のログインアカウントや、テレワークで利用するシステムのアカウントの初期パスワードを変更していない場合、悪意のある第三者にパスワードが把握されやすくなり、なりすましによる不正アクセスが行われるリスクが増加する。	◎		端末へのログインアカウントの初期パスワードは必ず変更するように、適切に社内ルール、プロセスを作成、徹底します。
9-3	アカウント・認証管理	テレワーク端末やテレワークで利用する各システムのアカウントが一定回数以上パスワードを誤入力した場合、それ以上パスワード入力ができなくなるように制限している。	不正アクセス	テレワークで利用する端末や各システムのアカウントが一定回数以上パスワードを誤入力したときにパスワード入力がそれ以上できないように制限していない場合、悪意のある第三者によるパスワード試行が容易に実行できるためパスワードが把握されやすくなり、なりすましによる不正アクセスが行われるリスクが増加する。	○	個人所有端末については業務用途以外にも利用されるため対象外とする。	端末へのログインアカウントのパスワードが一定回数誤入力された場合に、それ以上のパスワード入力ができなくなるように、Active Directory、または、ローカルPCで適切にポリシーを設定します。
9-4	アカウント・認証管理	テレワークで利用する各システムにアクセスする際に多要素認証を求めるように設定している。	不正アクセス	テレワークで利用する各システムへのアクセスに対して多要素認証を設定せずにID・パスワードのみで認証を行うことで、悪意のある第三者にパスワードが流出された場合に、なりすましによる不正アクセスが行われるリスクが増加する。	○		**生体認証センサー** **HPのPCに組み込まれた生体認証センサーおよびTPMにより、安全かつ容易に多要素認証を行います。**
10-1	特権管理	テレワーク端末やテレワークで利用する各システムにおいて、業務上必要な最小限の人に管理者権限を与えている。	不正アクセス	テレワークで利用する端末や各システムにおいて、業務上必要でないにも関わらず管理者権限を与えている場合、悪意のある第三者による不正アクセスにより重要情報にアクセスできる可能性が高くなり、重要情報の漏えいリスクの増加や、誤操作による情報漏えいのリスクが増加する。	○		端末、および、システムで利用される管理者アカウントをActive Directory等、システムで適切に管理します。
10-2	特権管理	テレワーク端末やテレワークで利用する各システムの管理者権限のパスワードには、強力なパスワードポリシーを適用している。	不正アクセス	テレワークで利用する端末や各システムの管理者権限のパスワードに、強力なパスワードポリシーを適用していない場合、悪意のある第三者にパスワードが把握されやすくなり、なりすましによる不正アクセスが行われるリスクが増加する。	○		管理者アカウントのパスワードの強度を強制するよう、Active Directory等、システムで適切に管理します。
10-3	特権管理	テレワーク端末やテレワークで利用する各システムの管理者権限は、必要な作業時のみ利用している。	不正アクセス	管理者権限が必要な作業時以外に管理者権限を利用すると、管理者権限でマルウェア感染することで重要情報に直接アクセスされてしまうなど、誤操作による情報漏えいのリスクが増加する。また、管理者権限の利用情報などから不正アクセスの懸念を発見することが困難になる。	○	個人所有端末については業務用途以外にも利用されるため対象外とする。	テレワーク端末やテレワークで利用する各システムの管理者権限は、必要な作業時のみ利用するように、社内ルール、プロセスを作成し徹底します。

テレワークセキュリティの基本は端末状態の把握

従来オフィスの建物内に存在したPCが、テレワーク移行によりバラバラの場所に散らばってしまうと、それぞれのPCの状態を把握することが難しくなります。
たとえば、「そのPCは誰が使っているのか?」「どこにあるのか?」「どのようなアプリケーションがインストールされているのか?」「OSは最新の状態なのか?」などです。
これらの課題を解決するのが、クラウド型の管理サービスです。
HPでは、「HP Proactive Insights」「HP Proactive Endpoint Management」の2つの管理サービスを提供しています。

HP Proactive Insights

HP Proactive Endpoint Management

サービス内容		
特長	**HP Proactive Insights**	**HP Proactive Endpoint Management**
ダッシュボード（インシデント、レポート）	●	●
アクセシビリティ（パートナーによる管理）	●	●
アセット トラッキング	●	●
従業員体験	●	●
ハードウェアおよびソフトウェアの正常性の監視	●	●
HPサービスエキスパートによるサービス提供		
アドバイザリーサービス（ビジネスインサイトレポート）	● ※250台以上	● ※250台以上
アプリケーションの展開		●
アプリケーションの管理		●
デバイスおよび保護の管理		●
インシデント管理		●
リモートトラブルシューティング		●