世界で最も安全なビジネスPC*

2021年 6月版

PCが危険にさらされているのをご存知ですか？

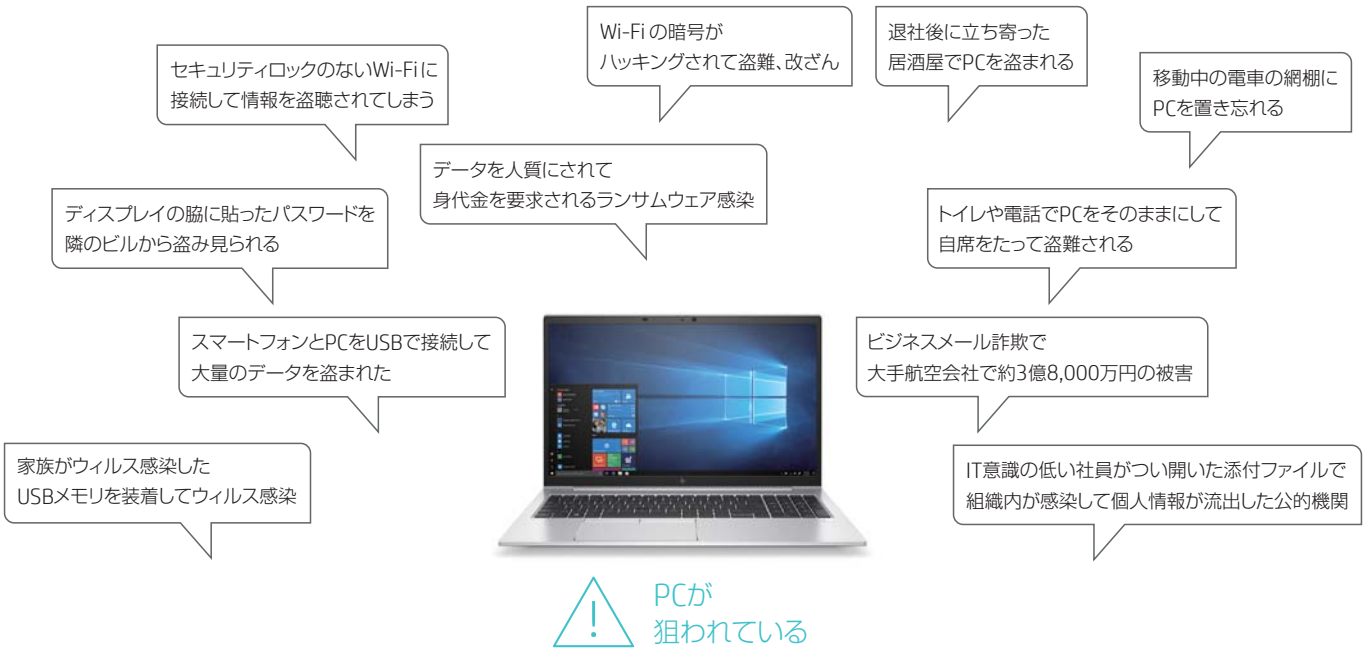
恐ろしいサイバー攻撃

PCは無差別に攻撃されています。そこに重要な情報があるかどうかといったこととは無関係に攻撃され、無差別型攻撃と言われています。犯罪者の意図はさまざまですが、無差別に攻撃し、世の中を混乱させることができたという事実が、彼らの実力を証明し、そのブラックマーケットでの成功裏につながます。その一方で、特定の組織や企業を狙い撃ちする標的型攻撃もあります。こちらは、さまざまな方法で得た標的となる個人の情報を元に執拗な攻撃がおこなわれます。いずれにしろ、サイバー攻撃はもはやお金儲けの手段になっており、大きなブラックマーケットを作っていることを知っておきましょう。

PCのセキュリティを脅かすさまざまなシチュエーション

今後、働き方改革などが進む中で、PCを使う場所のバリエーションが増え、その脆弱性をついたサイバー攻撃はますます激しくなることが予想されます。

コワーキングスペース、カフェ、移動中の電車や飛行機などで、PCは常に危険にさらされています。だからといってPCを持ち出し禁止にすることは生産性を低いものにしてしまいます。だからこそ、攻撃されることを前提にセキュリティを考える必要があるのです。



ハッカーの標的となる中堅・中小企業が増加

なぜ中堅･中小企業が標的となるのか?

今日のサイバー攻撃は、これまで以上に巧妙化してきており、犯罪集団はより簡単にあらゆる企業を攻撃できるようになっています。組織化された犯罪グループによるサイバー犯罪の目的は、業務妨害を目的としたものであったり、関連企業などの金融資産または個人情報の搾取などさまざまなものが考えられます。

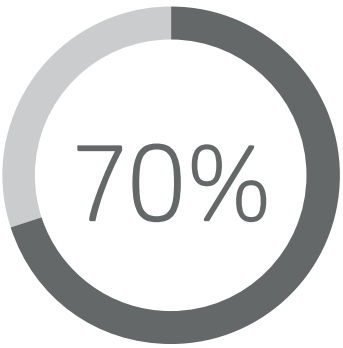
攻撃者は、大企業1社よりも多くの中堅･中小企業を標的にした方が、メディアや政府による監視を逃れ、総合的に多くの標的企業から多くのリターンを得ることができると考えはじめています。

また、最終攻撃対象が大企業とする、中堅･中小企業への攻撃も発生しています。大小複数の組織･企業で形成されるサプライチェーンなどにおいて、セキュリティ上最も脆弱なポイント(中堅･中小企業)に攻撃を仕掛け、大規模な親会社や関連企業に侵入するための足掛かりとするケースもあります。

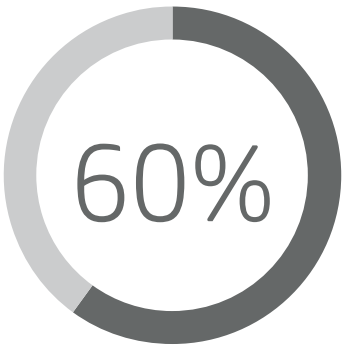
National Cyber Security Allianceによれば、攻撃全体の70%以上が中堅･中小企業を標的とするものです。そして、さらに深刻なことに、攻撃を受けたSMB※の約60%が、情報漏えいから6ヶ月以内に廃業に追い込まれています。

※SMBとはSmall and Medium Businessの略。「中堅･中小企業」を意味する。

攻撃全体の70%以上が
中堅･中小企業を標的とする



サイバー攻撃によりSMBの約60%が
6ヶ月以内に廃業に追い込まれている



WatchGuardの中小企業のサイバー被害実態の記事より引用
https://www.watchguard.com/

一般的な企業のセキュリティ対策

PCでの作業では機密情報や個人情報などを扱います。漏えいしては困る情報、データが多いため、企業の多くは漏えい防止のために数々の対策を施しています。これらの制限は便利さと引き換えに不便を強いるものですが、組織が正常に業務を進めるためには仕方がないとされています。

- USBポートの使用禁止
- 許可されたアプリケーションソフト以外の使用禁止
- 指定アクセスポイント以外へのWi-Fi接続禁止
- 許可されたサイト以外の閲覧禁止
- ウイルス対策ソフトの常駐
- 各種ウェブサービスの利用禁止
- のぞき見防止のためのプライバシーフィルター装着
- パスワードの定期更新による徹底したサインイン制限

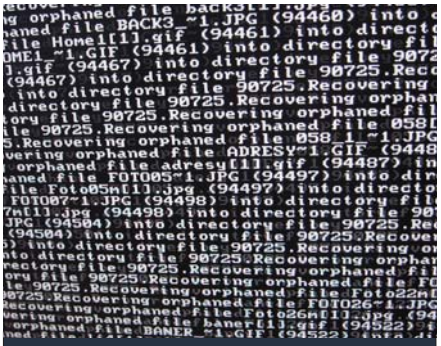
HPのPCなら利便性も損なわない

ボタン1つでのぞき見による機密情報の漏えいを防止する機能や、サイトの閲覧制限を安全に解除できる機能など、HPのPCなら利便性とセキュリティ対策の両立が可能です。詳しくはP.10以降をご覧ください。

それでもPCは守れないのです!

年々高度になるサイバー攻撃

悪意によって作られたソフトウェアをマルウェアといいます。いわゆるウイルスなどがその代表例です。マルウェアは、USBポートに装着したUSBメモリから侵入したり、ネットワークを介し、OSの脆弱性をついてPCに取り憑きます。あるいは、インターネットで見つけることができるおもしろそうなソフトの仮面をかぶった地雷的なものも少なくありません。トロイの木馬とも言われるこうした脅威は、道に落ちているお菓子を食べておなかをこわすようなものですが深刻な事態を引き起こす可能性があります。さらには、日常的にやりとりするメールとして送りつけられる怪しいリンクや添付ファイル。これらを開くことでもPCは簡単にマルウェアに感染してしまいます。感染させてデータを暗号化し、高額な身代金を要求するランサムウェアの存在も話題になっています。
感染したPCはどのようになるのでしょう。典型的な例をあげてみましょう。



物理アクセスを利用した攻撃

感染したPCにUSBメモリなどを接続することで外部記録媒体へも感染し、外部記録媒体がマルウェアの運搬役となり、感染を拡大させます。

ネットワークを利用した攻撃

マルウェアの一種であるワームは、ネットワークを介して他のコンピューターに感染。1台が感染するとネットワーク全体にあっという間に広がり、経由したすべてのPCを感染させます。

人を狙った攻撃

標的型攻撃は特定の人物や組織に対するサイバー攻撃の一種であり、SNSなどの個人情報を使い、巧妙に個人アカウントを攻撃します。

サイバー攻撃は完全には防げない…

最近流行したマルウェア／ランサムウェア

ワイパー型マルウェア

攻撃対象のPCにインストールされると、すべてのデータを消し去ってしまう

- Shamoon ／Shamoon 2
  サウジアラビアのエネルギー部門に対する攻撃
- NotPetya
  ウクライナの組織が打撃を受けており、食料雑貨店チェーン、大手通信会社、いくつかの銀行が感染を報告

ワーム型ランサムウェア

単独で行動し、自己感染力を持つマルウェアの一種

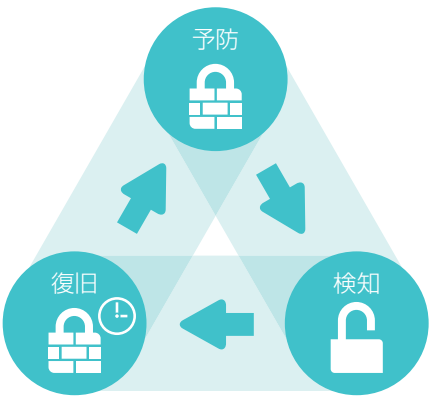
- WannaCry
  2017年5月12日から大規模なサイバー攻撃が開始され、150ヶ国、23万台以上のコンピューターに感染し、28言語で感染した。コンピューターの身代金として暗号通貨ビットコインを要求する
- BadRabbit
  ロシアやウクライナを中心に多くの感染被害が確認されており、公共機関を含めて多くの企業・組織で業務が停止する

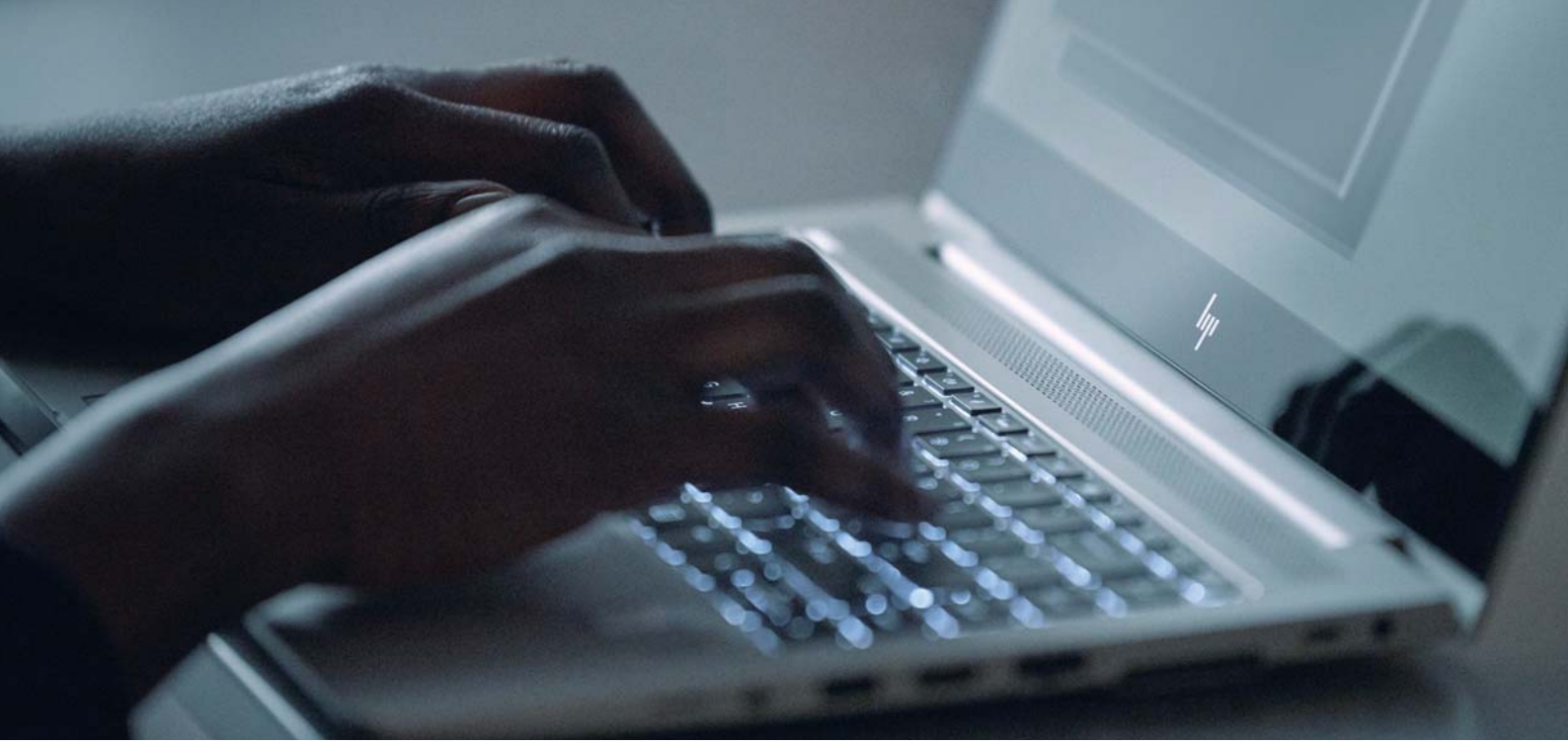
HPのPCが安全な理由　危険な攻撃から身を守るには

もはや攻撃は避けられません。未然かつ完全に防ぐのはもう無理と考えましょう。だとすれば被害を最小限に抑えることを考えるべきです。HPのPCには、攻撃からの予防、検知、復旧に関する機能がハードウェアの機能として実装されています。たとえ攻撃を回避することができなかったとしても、素早く攻撃を検知し、元の状態に戻すことでPCを使えない時間を最小限に抑えます。
それが、「サイバーレジリエンス」という考えです。

“サイバーレジリエンス”という新しい考え方

完全に守るのが難しければ、素早い復旧をめざす。これがサイバーレジリエンスという考え方です。レジリエンスは復元力を意味します。つまり、PCそのものが自己回復する仕組みです。PCの正常な状態を基点とし、常にそれと現在の状態を比べることで安全を確保するのです。少しでも異なれば、それは改ざんです。

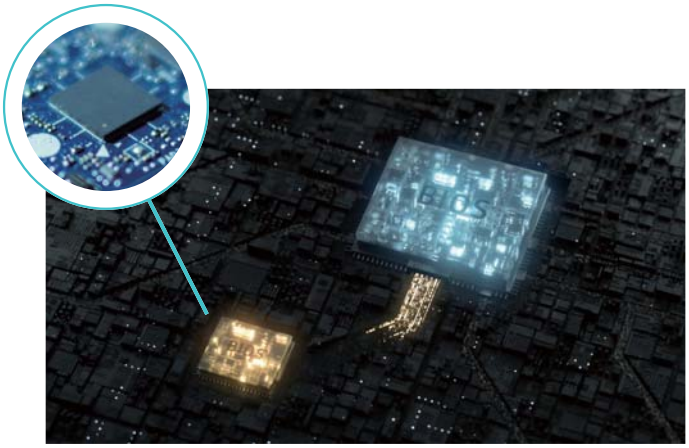




HP独自のハードウェアを基点とした高度なセキュリティ機能
HP Endpoint Security Controller

世界で最も安全なPC*の仕組み

HP PCのBIOSは、「HP Endpoint Security Controller」で守られています。「HP Endpoint Security Controller」は、専用のプロセッサーと、暗号化ハードウェアで構成されています。
いわばPC内部のもう一台のPCです。絶対的に信頼できるこのPCが、BIOSが改ざんされていないか、信頼できるものであるかをチェックするのです。いわば、PCの中に、その監視のためにもう一台のPCが入っている環境。その存在が、世界で最も安全なPCを実現しています。



HP独自のハードウェア　業界初かつ唯一の自己回復型BIOSを実現、だから

世界で最も安全なビジネスPC*

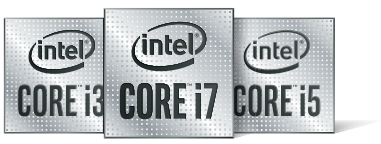
*Windowsおよび第8世代以降のインテル® プロセッサーまたはAMD Ryzen™ 4000 シリーズ以降のプロセッサーを搭載したHP Elite PCシリーズ、第10世代以降のインテル® プロセッサーを搭載したHP ProDesk 600 G6シリーズ、第11世代以降のインテル® プロセッサーまたはAMD Ryzen™ 4000 シリーズ以降のプロセッサーを搭載したHP ProBook 600シリーズ。追加費用・追加インストール不要のHP独自の標準装備された包括的なセキュリティ機能と、ハードウェア、BIOS、Microsoft System Center Configuration Managerを使用するソフトウェア管理などPCのあらゆる側面におけるHP Manageability Integration Kitの管理に基づく。（2020年12月時点、米国HP.inc調べ。）

知っておきたいPCの中身

PCの内部をのぞいてみよう

典型的なノートPCはキーボードを持つ本体と液晶画面が一体化されています。
本体内にはPCの頭脳に相当するCPUと作業用のメモリ、そしてシステムやデータを記録するためのストレージなどが配置され内蔵されています。

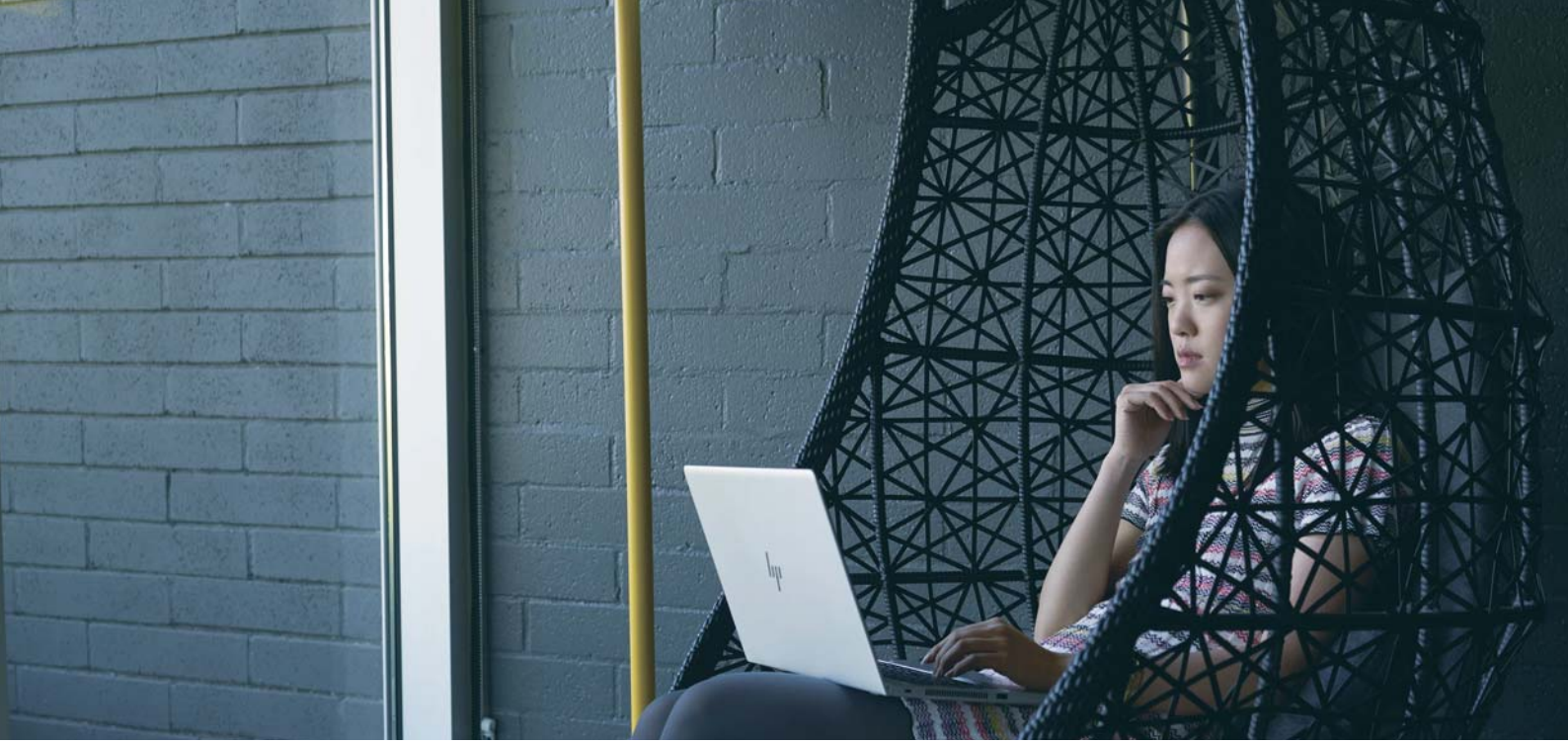
• CPU　セントラル・プロセッシング・ユニット。PCのエンジンとして機能します。プロセッサーとも呼ばれます。インテル製などのものが搭載され、PCの頭脳を担う重要なパーツです。並列処理のために複数のプロセッサーをまとめたマルチコアプロセッサーが主流ですが、10億個超のトランジスタが集積された半導体チップのサイズは小指の爪より小さいものです。



• メモリ　プロセッサーが使う作業用の空間を担います。一般的なノートPCは8GB程度の容量のものが内蔵され、CPUがその内容を読み書きすることで各種の処理を実行します。ちなみに8GBは400字詰め原稿用紙にして約1000万枚分に相当します。

• ストレージ　円盤状のディスクを回転させ、磁気でデータを記録するパーツです。現在のノートPCには数百GBのディスクが内蔵されています。最近では電源を切っても内容が消えない不揮発性のメモリを使って磁気ディスクと同様の機能を実現するSSD（ソリッド・ステート・ディスク）が使われることが多くなりました。SSDは物理的なディスクの回転や磁気ヘッドの移動がないため、読み書きのスピードが速く、衝撃に強いというメリットがあります。

• 端子類　本体の側面にはさまざまな周辺機器を接続するための端子類があります。マザーボードと直結され、特にUSB端子はメモリなどを装着してデータをやりとりするためによく使われます。また、外部モニターに映像を出力するための端子や、有線LANケーブルを接続するための端子などが装備されている場合もあります。



PCが仕事をするにはソフトウェアが欠かせない

PCの操作には、キーボードの他、画面のタッチ、または、キーボード手前のタッチパッドを使います。またワイヤレスマウスを使うこともできます。

これらのハードウェアを統合的に機能させるためのソフトウェアがオペレーティングシステム(OS)です。HPのPCをはじめ、企業内PCで使われているOSのほとんどは、Microsoft社が提供するWindowsです。

CPUはストレージからWindowsを読み込み、メモリ上に展開し、キーボードやマウス操作を受け付けて各種の処理をおこないます。その結果が液晶画面に表示され、指示することで結果をデータファイルとしてディスクに書き込み、次の利用に備えます。

さらに、Windowsが稼働するPCで業務をおこなうには、アプリケーションソフトが必要です。Windows OS上でMicrosoft WordやExcel、PowerPointといったアプリケーションを、やりたい作業に応じて使い分けます。インターネットサイトを閲覧するブラウザやメールの送受信に使うOutlookなどもアプリケーションの仲間です。

ハードウェアとしてのPCでWindows OSを稼働させ、そこで必要なアプリケーションを利用してデータを読み書きすること。これがPCの基本的な使い方です。その背後では、CPUとメモリ、ストレージがフル稼働しています。

PCが壊れるってどういうこと?

CPU、メモリ、ストレージが正常に働くことでPCはPCとして機能します。ところが何らかの悪意が正常稼働を妨げます。その悪意をもたらすソフトウェアがマルウェアです。最悪の場合、CPUがディスクからOSを読み込めなくなってしまうこともあります。OSを読み込めなければPCはPCとして使いものになりません。あるいは正常に稼働しているように見えても、改ざんされ悪意に満ちたPCに変貌している可能性もあります。OSをディスクから読み込むための仕組みが改ざんされることさえあるのです。マルウェアはネットワーク経由、USB端子経由、悪意のファイルを開くといったあなた自身の操作などによって簡単にPC内部に潜入し悪事を働きます。

悪意によって不正行為に加担させられる

PCが悪意に乗っ取られることで、自分自身には悪意がないにもかかわらず、結果として第三者をサイバー攻撃する加害者になってしまうことがあります。不正アクセスや迷惑メールの大量配信の中継地点として利用され、攻撃元を偽装するために使われます。つまり、踏み台として攻撃に加担してしまうのです。日本でも2012年に「遠隔操作ウイルス事件」が明るみになりました。ネットワークを介して他社のPCを遠隔操作、踏み台にして襲撃や殺人などの犯罪を予告した事件です。

HPのPCはこうして守られる

HPのPCに搭載されたセキュリティ機能

HPのPCは、複数のセキュリティソリューションを組み合わせて攻撃に備えることができます。仮に攻撃によってPCが起動不可能な状態になったとしても、短時間で自己復旧する仕組みが実装されています。ここではその代表的なソリューションを紹介しましょう。

"HP Sure View"

その前に

PCに電源を入れると何が起こるの？ ～PCに作業環境が整うまでの流れ～

PCに電源を入れてPCとして使えるようになるまでに、どのようなことがPC内部で起こっているのでしょう。

STEP 1

PCに電源を入れるとBIOSまたはUEFIと呼ばれるハードウェアに実装されたソフトウェアが周辺回路の初期化をおこない、起動のための準備を整えます。

STEP 2

準備ができたところで、ディスクのMBRまたはGPTにアクセスしOSを読み出し起動プロセスが始まります。起動時には1ステップずつOSが正しいものであるかを確かめます。

STEP 3

ディスクに格納されているWindowsが読み出され、メモリに常駐します。

Windows 10

STEP 4

サインインの画面が表示され、正しく認証することでいつものデスクトップが表示されます。そして必要なアプリケーションを開いて作業を始めます。

BIOSとは?

ファームウェアの一つで、コンピューターに搭載されたプログラムのうち、ハードウェアとの最も低レベルの入出力をおこなうためのプログラムである。

UEFIとは?

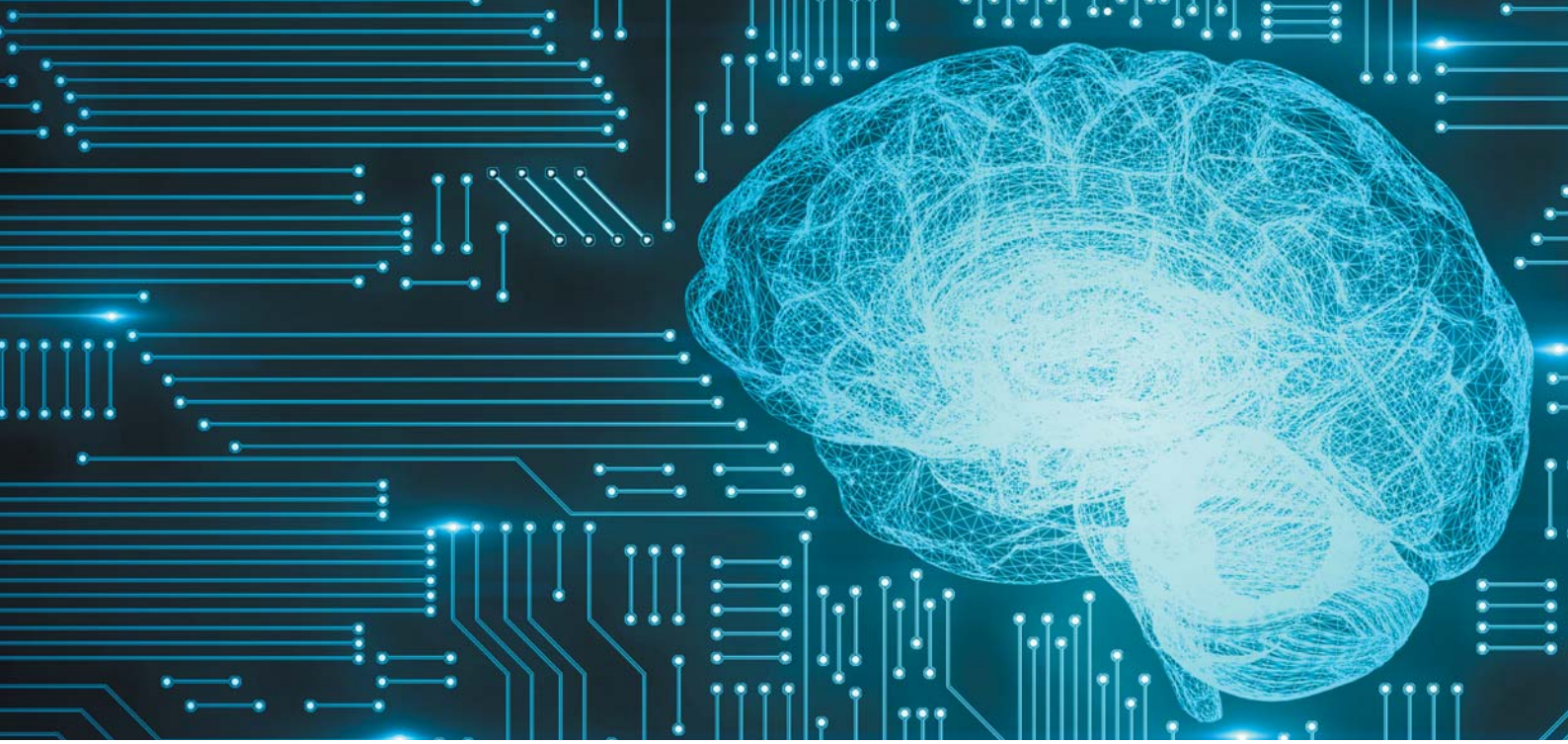
UEFIフォーラムによって決められたBIOSの規格。旧来のBIOSからUEFIに移行することで、設計の自由度が増し、大幅に機能を強化できるようになる。

MBRとは?

マスターブートレコードの呼称。ハードディスクなどのストレージ（外部記憶装置）の最も先頭にある、起動に必要なプログラムや情報を記録した小さな領域。コンピューターの起動時に最初に読み込まれる。

GPTとは?

GUID Partition Tableの呼称。UEFI環境下では、旧来のBIOSでサポートされていたMBRに代わりGPTと呼ばれる新しいパーティションテーブルを用いる。2TB以上の大容量なHDDをサポートできる。



HP Sure Sense

ディープラーニングAIで
未知のマルウェアからリアルタイムで保護

「HP Sure Sense」はディープラーニングAIを活用してマルウェアを検出し、ブロックする新機能です。Windows Defender との組み合わせで、既知のマルウェアだけでなく、未知のマルウェアについても約99%を最短で20ミリ秒（1ミリ秒は1000分の1秒）で検出できるソリューションです。

Web
サイト

HP Sure Senseは以下の機能で
マルウェアに対応します。

ディープラーニングを活用した受動的脅威防止：
HP Sure Senseは、ファイルが開かれる前または実行される前に、そのファイルがマルウェアの脅威であると特定することができます。

ふるまい検出を搭載した能動的脅威防止：
HP Sure Senseは、ランサムウェアなどの脅威に関連するPCのふるまいを検出します。

ファイルレス攻撃に対する保護：
メモリに常駐し、ハードドライブに書き込まないマルウェアから保護します。レガシーソリューションでは検出が非常に困難です。

リアルタイム保護とフルドライブスキャン：
新しいファイルの書き込みを検査し、警告およびマルウェアを隔離します。

どのようなAIシステムを利用するのか?

HP Sure Senseは、直接生データを学習するディープラーニングテクノロジーに基づいています。データセンターでは、Sure SenseのAI予測モデルのトレーニングに、善悪を問わず、何億ものファイルの生データが使用されます。このプロセスの間、アルゴリズムは、人間の脳がどのように機能するかに似た方法でAI予測モデルを構築します。

ディープラーニングAIとは?

ディープラーニングでは、AIはマルウェアそのものを学習します。つまり、人間がマルウェアの特徴量を摘出する必要がありません。そして、人間の頭脳のように学び、本能的にマルウェアを認識することができるようになります。

シグネチャ型との違いは?

従来のアンチウイルスソフトは、マルウェアを認識して防御するのにシグネチャ型を用いています。毎日新しい形のマルウェアが数十万も作られている状況ではシグネチャでは間に合いません。HP Sure Senseは、シグネチャ型ではなく、ディープラーニングAIを用いたモデルでマルウェアを検出し防御します。防御する手法が違うのでシグネチャ型とコンフリクトもしません。

BIOSが攻撃されても自己回復

HP Sure Start

HP Endpoint Security ControllerがBIOSに何らかの改ざんがないかどうかを調べます。もし攻撃によって不正な状態であることが検知された場合、自動的に正常な状態に回復します。G4以降では「NIST SP 800-193」に完全準拠。

デモ動画

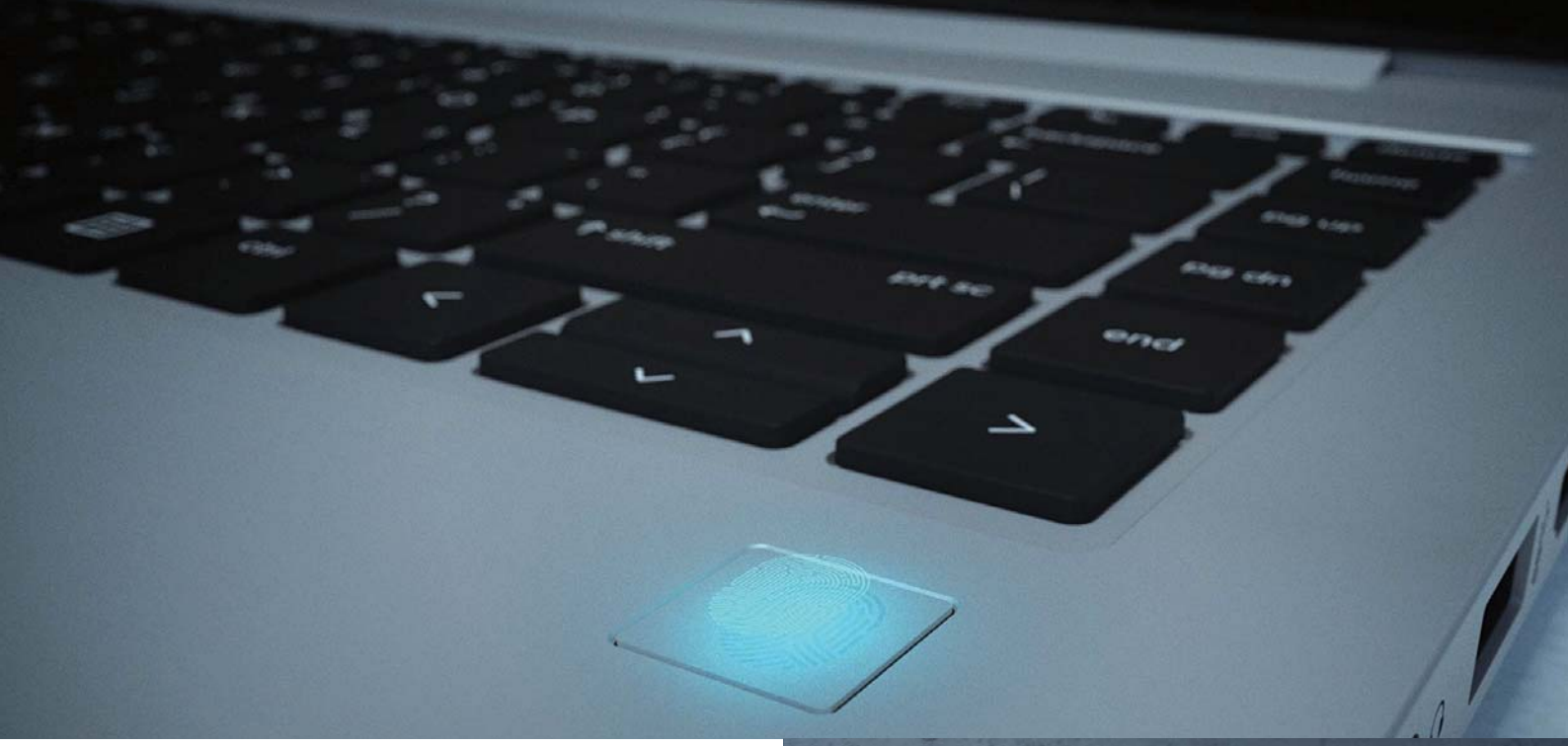
G3以降ではランタイム侵入検知やBIOS設定変更の検知回復機能を搭載

破滅的なディスク障害からデバイスとデータを保護

MBR/GPT Security

多くのウイルスが狙っているMBR/GPTを自動復旧して破滅的なディスク障害からデバイスとデータを保護します。MBR/GPTのバックアップコピーを作成し、破壊または改ざんされていた場合にはワンクリックでバックアップからリカバリし、復旧時間を大幅に短縮します。

Web サイト



不正利用対策や本人確認強化のソリューション

HP マルチファクター認証（HP Client Security）

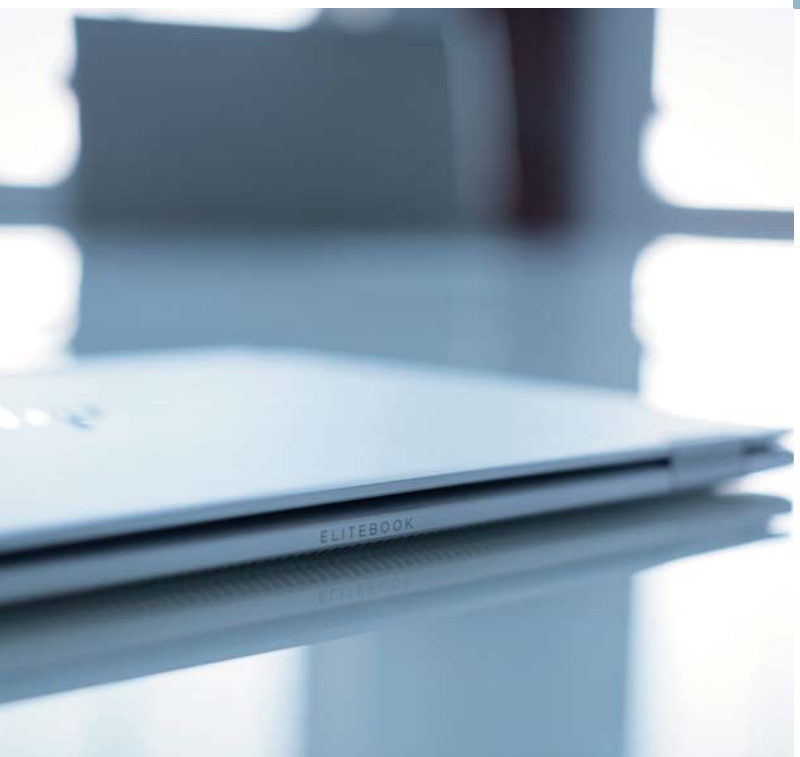
指紋認証や顔認証、NFCやBluetooth機器を含む最大3つの要素で認証できるため、PCへの不正アクセス対策をより強固なものにします。

※顔認証等の認証デバイスは機種によって異なります。
※マルチファクター認証はHP Client Securityの機能の一部です。
※3要素認証を設定するにはSCCM+HP MIKが必要です。

指紋認証　パスワード認証　顔認証

デモ動画

HP マルチファクター認証は「インテル® Authenticate テクノロジー」を活用しています。
ハードウェア支援型の多要素認証が可能な「インテル® Authenticate テクノロジー」は、ソフトウェアのみを使用したソリューションのぜい弱性を解消し、OSレベルでの対応が難しい領域のセキュリティを強化してエンドポイントを保護します。



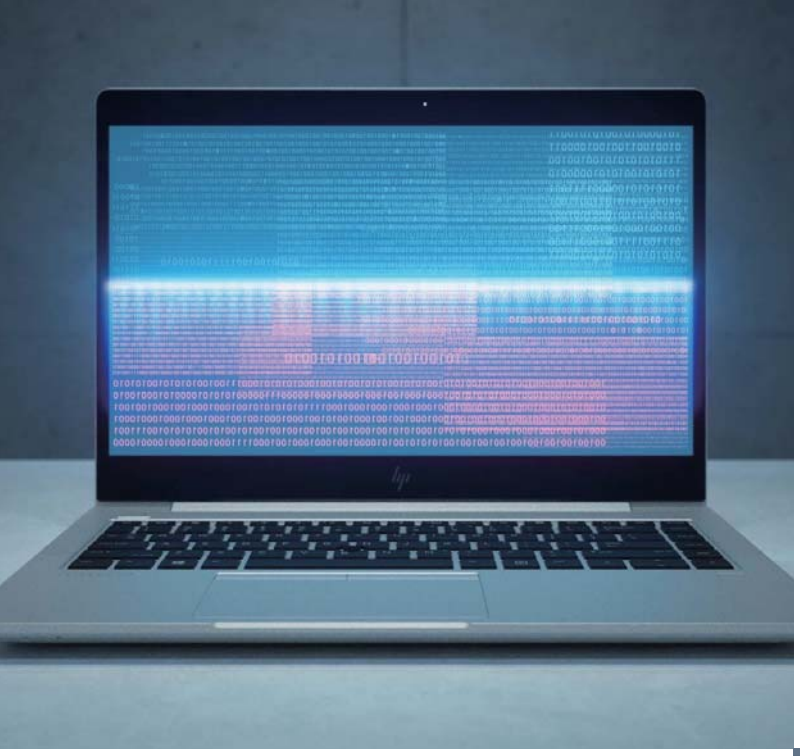
外部ツールを一切使わずにBIOSから内蔵ドライブのデータを完全消去

HP Secure Erase

PCに保管されているファイルは、削除しても削除の印がつくだけで、専門家の手にかかればごみ箱の中のファイルのように簡単に復元できてしまいます。PCを処分するような場合には、特別なソフトウェアを使わずに、BIOS中のSecure Eraseを使って内蔵ドライブのデータを完全に削除することができます。

デモ動画

PCを修理・廃棄する際、数回のクリックでデータは、復元不可能な状態に消去できる



アンチウイルスを
オフにさせない

HP Sure Run

HP Endpoint Security ControllerがWindows OS標準のWindows Defenderなどのセキュリティ対策機能を常時監視し、万が一、それらが無効になった場合は自動的に再起動し、安全な状態に戻します。

デモ動画

常時監視　通知　自動復旧

Webブラウジング感染や
ファイル感染が無かったことに

HP Sure Click

不正Webサイト閲覧によるマルウェアやウイルス感染、さらに、Outlookのメール添付やブラウザを使用してダウンロードしたPDF、Wordファイルからのウイルス感染からPCを守ります。

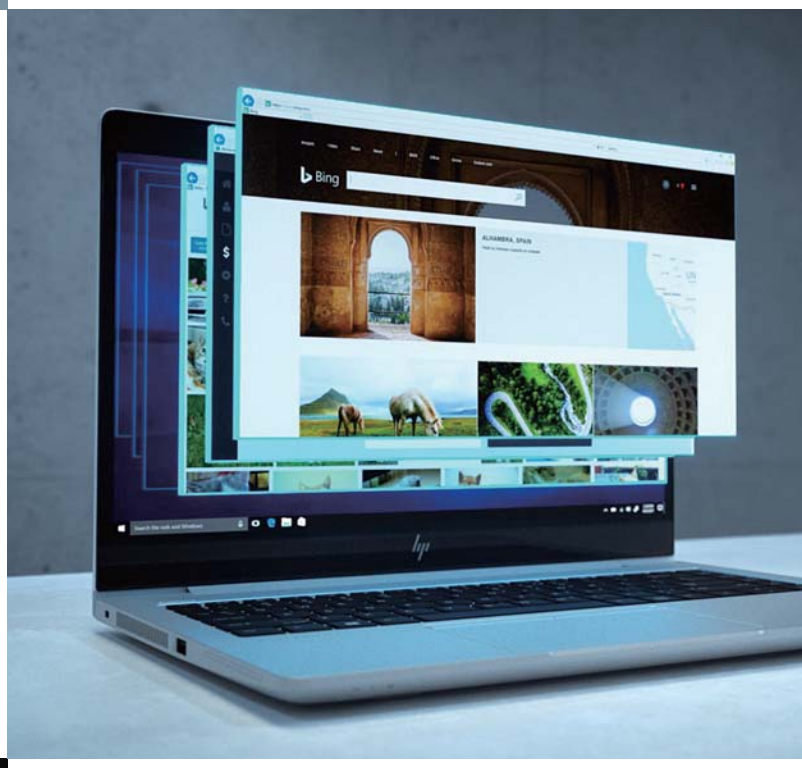
※Internet Explorerに対応

クラウドプラットフォーム　情報共有プラットフォーム　音楽・動画配信サイト　ソーシャルメディアWEBサイト

デモ動画

HP Sure Clickは「インテル® バーチャライゼーション・テクノロジー（インテル® VT）」を活用しています。

「インテル® VT」は、仮想化をハードウェアで支援する機能です。仮想化とは、1台のパソコンにて複数の仮想マシンを同時に動作させる技術です。通常は1台のパソコンにて動作するOSは1つですが、仮想マシンを利用すれば、例えばWindows 10と過去のWindowsの同時動作が可能となります。



正常な状態に
自動リカバリ

HP Sure Recover

OSがウイルスに感染しまったく起動しなくなった場合でも、自動的にネットワークからPC稼働に必要なイメージをダウンロードし、正常な状態にリカバリします。リカバリは工場出荷時に戻す設定と、企業がカスタマイズした設定から選ぶことができます。人手を介さずにネットワーク経由でリカバリできるため、ウイルス感染時の復旧時間を大幅に短縮することができます。

デモ動画

HP Sure Recover はBIOS中に実装、
新品のハードドライブからでもPCを再イメージ

のぞき見による
機密情報の漏えいを防止

HP Sure View

ビジュアルハッキング、すなわち、PCを使っているところをのぞき見されて、データや業務機密などを盗まれる行為を抑止するための内蔵型プライバシースクリーン機能です。簡単なボタン操作でプライバシー機能を有効および無効にできます。機密情報を守るために別途外付けのプライバシースクリーンを購入する必要もなくなります。

デモ
動画

すべてのPCを
確実に保護。

HP Manageability Integration Kit
(HP MIK)

Microsoft System Center Configuration Manager(SCCM)認定を受けたプラグイン。IT管理者によるHP BIOSやセキュリティポリシーの管理、TPMのバージョン変更などのリモート管理を可能にするSCCM用プラグインです。

デモ
動画

新しいサイバーセキュリティの世界基準

米国では国防総省と取引をおこなうためには、セキュリティガイドライン「NIST SP 800-171」を満たす必要があります。今後、グローバルにビジネスをおこなう企業にとっては、NISTのような世界基準のセキュリティ対策が前提条件となっていきます。

日本国内でも防衛調達において、NIST SP 800-171と同程度の新情報セキュリティ基準改正を検討。対象となるのは、防衛省と直接取引する企業だけでなく、部品の提供やサービスの外注などの形で間接的に取引をする企業も含まれます。

将来的には幅広い産業へ拡大される可能性もあり、セキュリティ対策なしではビジネスが継続できなくなる恐れがあります。

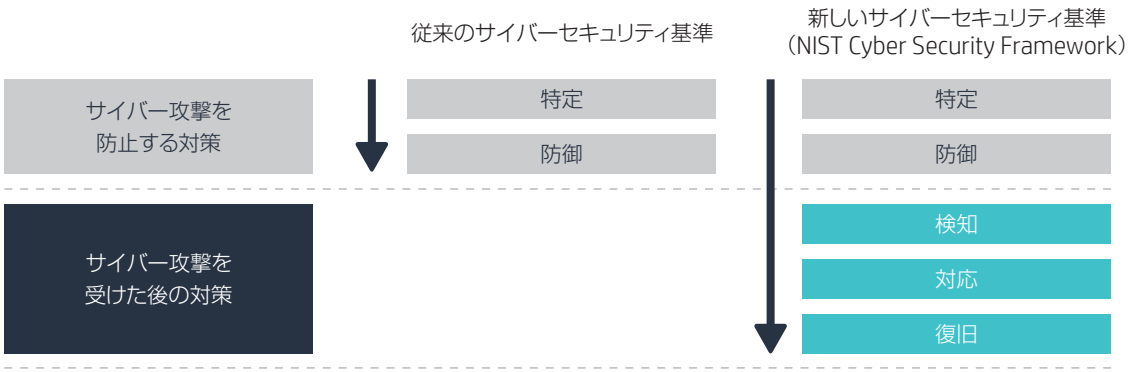
NIST（National Institute of Standards and Technology）とは

米国国立標準技術研究所。科学技術分野における計測と標準に関する研究をおこなう米国商務省に属する政府機関。NIST内には、情報技術に関する研究をおこなっているITL（Information Technology Laboratory）があり、ITLは情報技術に関して6つの分野（Security, Information Access, Mathematics and Computational Science, Software Testing, Networking Research, Statistical Engineering）の研究を実施。ITLの中でコンピューターセキュリティに関して研究をおこない各種文書を発行しているのがCSD（Computer Security Division）と呼ばれる部門。FIPSやSP 800シリーズの文書もCSDが発行。

SP 800シリーズ（Special Publications）とは

SP 800シリーズは、CSDが発行するコンピューターセキュリティ関係の文書。米国の政府機関がセキュリティ対策を実施する際に利用することを前提としてまとめられた文書で、内容的にはセキュリティマネジメント、リスクマネジメント、セキュリティ技術、セキュリティの対策状況を評価する指標、セキュリティ教育、インシデント対応など。

NISTが提唱する新しいサイバーセキュリティフレームワーク



「NIST SP 800-171」対応を、NIST準拠のPCで簡単に確実に実施

「NIST SP 800-171」自体は組織がおこなうべき「プロセス」に対するガイドラインであり、デバイスのみで実現できるものではありません。しかし、これらの一連のプロセスをすべて人がおこなうとしたら、膨大な労力とコストがかかるうえ、作業品質を維持するのは大変なことです。それに対し、HPのPCは、実装する各機能によりデバイスが対応し、自動化しています。つまり「NIST SP 800-171」への対応を確実に、早く、簡単に実現できるのが一連のNISTガイドラインに準拠したHPのPCです。

セキュリティ対策は、ハードウェアから始まります

「NIST SP 800-193」準拠のHPのPCを導入することで、「NIST SP 800-171」に確実に、早く、簡単に対応

不正利用対策や本人確認を強化
指紋認証や顔認証、NFCやBluetooth機器を含む最大3つの要素で認証できる、「HPマルチファクター認証」がPCへの不正アクセス対策をより強固なものにします。
→P13

すべてのPCを確実に保護
イメージファイル作成やドライバーの更新、HPの各セキュリティ機能の設定配布などを「HP Manageability Integration Kit」がマイクロソフト社のSCCM上で効率よく運用します。
→P15

Webブラウジング感染やファイル感染が無かったことに
Web閲覧のセキュリティ対策強化機能の「HP Sure Click」により、ブラウザのタブやファイルを閉じるだけでマルウェアは消滅します。
→P14

安全な状態に復旧
「HP Sure Run」はハードウェアに基づく自己回復機能をOSプロセスに拡張。また、「HP Sure Recover」は、ネットワーク経由で安全かつ自動的にOSイメージを復旧します。
→P14

のぞき見による機密情報の漏えいを防止
ビジュアルハッキング防止機能の「HP Sure View」が横からののぞき見からデータを保護します。
→P15

BIOS基点によるPCの保護
BIOSの自己修復機能「HP Sure Start」が、ウイルスやマルウェアによる不正なBIOS書き換えまたは破損からシステムを保護します。
HP Sure Start G4/G5(NIST SP 800-193準拠)→P12

企業向けに構築され、よりセキュアなPC基盤を提供する、インテル® vPro® プラットフォーム

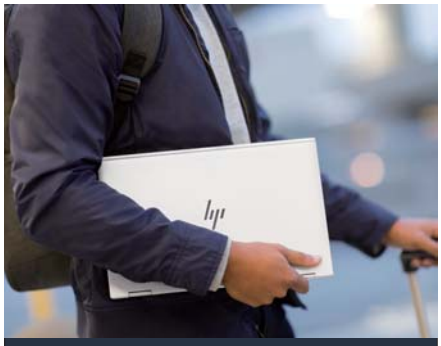
ITセキュリティーの意思決定はPCから始まります。インテル® vPro® プラットフォームは、セキュリティーの脅威に関連するリスクを最小限に抑えるハードウェア支援型の高度なセキュリティー機能を提供するように設計されています。

インテル® vPro® プラットフォームの一部であるインテル® ハードウェア・シールドでは、OSよりも下の層に対する攻撃に対して強化されている保護力があり、プラットフォームのセキュリティーを改善しています。インテル® ハードウェア・シールドは、攻撃面を縮小することで、被害をもたらすファームウェア・レベルの攻撃から保護すると同時に、通常のセキュリティー機能をオフロードして、ユーザーへの影響を抑え、生産性を維持します。

インテル® vPro® プラットフォームの詳細はWebをご覧ください https://www.intel.co.jp/vpro

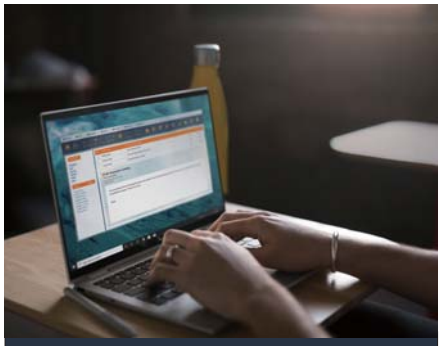
ハードウェア支援型セキュリティー

インテル® vPro® プラットフォームに搭載されたハードウェア支援型のセキュリティー機能は、リモートからの復旧機能とともに、OSよりも下のレイヤーに対する攻撃からの保護を備えたより安全なプラットフォーム基盤を提供します。



リモート管理機能

インテル® vPro® プラットフォームの管理ツールは、デバイスの監視、復元、アップグレード、保護をリモートから実行。デバイスの電源がオフになっていたり、アウトオブバンド環境にある場合でも、端末側にユーザーがいなくても実行可能です。



資産PCの安定性

インテル® vPro® プラットフォームは、PCが使用できない時間を最小限に抑えて、OSやソフトウェアのアップグレード、ハードウェアの更新などをより効率的に管理。よりスムーズな資産PCの管理とビジネスの継続性の向上を実現します。

セキュリティ機能対応マトリクス

		ビジネスデスクトップPC											ビジネスノートPC										2 in 1 タブレット	ワークステーション			モバイルワークステーション				POS製品/ロングライフPC				
		Slice G2	800 G6 TWR	800 G6 SFF	800 G6 DM	800 G6 AiO	600 G6 SFF	600 G6 AiO	405 G6 SFF	400 G7 SFF	400 G6 DM	Dragonfly	Dragonfly G2	x360 1040 G7	x360 1030 G4	850 G7	830 G7	650 G5	635 Aero G7	x360 435 G7	450 G8 / 430 G8	x2 G4	Z2 mini G5	Z2 TWR G5 / Z2 SFF G5	Z8 G4 / Z6 G4 / Z4 G4	Studio G7 / Create G7	Firefly 14 G8 / 15.6 G8	Firefly 15 G7	Firefly 14 G7	Engage One Pro	Engage One	Engage Go	Engage Flex Pro & Pro-C	MP9 G4
OSより上	**HP Manageability Integration Kit（MIK）**※1 Microsoft® SCCMとの連携により、イメージ作成を含むセキュリティとBIOSの管理業務を提供するプラグイン。ダウンロード対応。	✓	✓ G4	✓ G4	✓ G4	✓ G4	✓ G4	✓ G4	✓ G5	✓ G4	✓ G4	✓	✓ G4	✓	✓	✓	✓	✓	✓ G3	✓ G3	✓ G3	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	HP Sure View / HP Sure View Reflect ビジュアルハッキング（のぞき見によるデータ盗難）を防ぐ内蔵型プライバシースクリーン機能です。											✓ ※2	✓ ※2	✓	✓	✓	✓ ※2					✓ ※2					✓ ※9							
	HP Sure Shutter キーボード上のボタンでシャッターの開閉を電子制御する、Webカメラ用プライバシーシャッター。OS起動の有無を問わず、シンプルかつ確実にプライバシーを確保します。												✓	✓																			
OS中	**HP Sure Recover** ネットワーク経由で自動的にソフトウェアイメージを復旧。万が一ハードドライブ全体が消去された場合にも、HP提供の標準イメージもしくは企業でカスタマイズしたイメージに復旧します。		✓ G3	✓ G3	✓ G3	✓ G3	✓ G3	✓ G3				✓	✓ G4	✓	✓	✓	✓	✓	✓ G3			✓	✓	✓		✓	✓ ※3	✓	✓	✓			✓	
	HP Sure Run ウイルス対策などの主要なプロセスやアプリケーションを監視し、あらゆる変更をユーザーとIT部門に通知。万が一それらが停止した場合は自動的に再起動し安全な状態に復旧します。		✓ G3	✓ G3	✓ G3	✓ G3	✓ G3	✓ G3				✓	✓ G4	✓	✓	✓	✓	✓	✓ G3			✓	✓	✓		✓	✓	✓	✓	✓			✓	
	HP Sure Click※4 閲覧するブラウザのタブやメールに添付されたファイルをハードウェア的に隔離されたマイクロ仮想マシン（micro-VM）上で実行。マルウェアやウイルスは完全に隔離され、タブが閉じられると、マルウェア・ウイルスは自動的に除去されます。		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	HP Sure Sense ディープラーニングAIを活用し、ランサムウェアの行動学習をもとにしたリアルタイム検知やゼロデイ攻撃に対する防御を、デバイスのパフォーマンスに与える影響を最小限に抑えておこないます。		✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓					
	HP Presence Aware 近接センサーが離席／戻りを感知し、自動&ハンズフリーでデバイスをロック・解除します。Windows Helloによる顔認証の設定が事前に必要です。													✓																				
OSより上	**HP Sure Start** BIOSの自己回復機能。さらにG3以降ではBIOSに侵入しようとする攻撃のランタイム侵入検知やBIOS設定変更の検知回復機能を搭載しています。G4以降はNIST SP 800-193準拠。		✓ G2	✓ G6	✓ G6	✓ G6	✓ G6	✓ G6	✓ G6				✓ G5	✓ G6	✓ G6	✓ G5	✓ G6	✓ G6	✓ G5	✓ G6	✓ G5	✓ G6	✓ G5	✓ G6	✓ G6	✓ G6	✓ G6	✓ G7	✓ G6	✓ G6	✓ G6	✓ G3	✓ G4	✓ G4	✓ G4
	HP BIOSphere ウイルスやマルウェアによる不正なBIOS書き換えまたは破損からシステムを保護するとともに、紛失盗難時にはHDD/SSD内のデータを完全消去します。※10 さらに「MBR」（Master Boot Record）/「GPT」（GUID Partition Table）の改ざん・破損からの復旧もおこないます。NIST SP 800-147（ISO 19678）準拠。		✓ G2	✓ G6	✓ G6	✓ G6	✓ G6	✓ G6	✓ G6	✓ G6	✓ G6	✓ G6	✓ G5	✓ G6	✓ G5	✓ G5	✓ G6	✓ G5	✓ G5	✓ G5	✓ G5	✓ G5	✓ G5	✓ G6	✓ G6	✓ G6		✓ G5	✓ G6	✓ G5	✓ G5	✓ G6	✓ G3	✓ G4	✓ G4	✓ G4
	MBR/GPT Security （HP BIOSphereに含まれる） MBR/GPTを自動復旧して破滅的なディスク障害からデバイスとデータを保護します。	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	HP Secure Erase （HP BIOSphereに含まれる） HDDからデータを完全に消去し復元ソフトからの不正な復元を防ぐことができます。NIST SP 800-88準拠。	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	OS起動前認証+生体認証 OS起動前に指紋認証や顔認証を必要とするセキュリティ設定が可能。					✓						✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓	✓	✓	✓ ※6	✓ ※6	✓ ※6		
	指紋認証リーダー Windows Helloまたは付属ソフトによりログイン等の本人認証に利用可能。					✓						✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓				✓	✓	✓	✓	✓ ※6	✓ ※6	✓ ※6		
	顔認証カメラ Windows Helloまたは付属ソフトによりログイン等の本人認証に利用可能。					✓ ※7						✓	✓	✓	✓	✓	✓		✓	✓		✓				✓	✓	✓	✓					
	TPMセキュリティチップ 暗号化キーの格納や、デジタル証明の生成をおこなう機能。ISO 11889準拠。	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	自己暗号化ドライブ 保存される全データを専用チップで自動的に暗号化するOPALディスク（HDDまたはSSDタイプ）に対応。											✓						✓				✓				✓ ※9	✓ ※9			✓ ※8	✓ ※8	✓ ※8	✓ ※8	✓ ※8

※1 HP MIKの各機能への対応状況については、WEBページをご参照ください。https://ftp.hp.com/pub/caps-softpaq/cmit/MIK2.5_platformList.html　※2 HP Sure View搭載モデルでのみ利用可能です。　※3 マルチストレージ構成は対応していません。　※4 HP Sure ClickはCPUがインテル® Pentium® プロセッサー、インテル® Celeron® プロセッサー、インテル® Core™ Mプロセッサー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。　※5 Webカメラ搭載モデルのみ顔認証対応。　※6 オプションの指紋リーダー接続時に対応。　※7 800 G6 AiOのカスタマイズオプションでIRセンサー付Webカメラを選択した場合のみ対応。　※8 標準モデルでは非対応。OPALディスクを搭載した特別構成作成時に対応。　※9 OPAL SSD搭載のみ対応。　※10 別途、Absolute サービスの購入が必要となります。Absolute サービスについては、WEBページをご参照ください。https://jp.ext.hp.com/services/business/carepack/absolute/
＊上記以外の製品については、WEBページをご参照ください。https://www.hp.com/jp

⚠ 安全に関するご注意　ご使用の際は、商品に添付の取扱説明書をよくお読みの上、正しくお使いください。水、湿気、油煙等の多い場所に設置しないでください。火災、故障、感電などの原因となることがあります。

お問い合わせはカスタマー・インフォメーションセンターへ

0120-436-555　受付時間：月曜～金曜 9:00～19:00　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）
※フリーダイヤルがご利用いただけない場合 03-5749-8291（直通）

世界で最も安全なビジネスPCに関する詳細は https://www.hp.com/jp/security-pc

*Windowsおよび第8世代以降のインテル® プロセッサーまたはAMD Ryzen™ 4000 シリーズ以降のプロセッサーを搭載したHP Elite PCシリーズ、第10世代以降のインテル® プロセッサーを搭載したHP ProDesk 600 G6シリーズ、第11世代以降のインテル® プロセッサーまたはAMD Ryzen™ 4000 シリーズ以降のプロセッサーを搭載したHP ProBook 600シリーズ。追加費用・追加インストール不要のHP独自の標準装備された包括的なセキュリティ機能と、ハードウェア、BIOS、Microsoft System Center Configuration Managerを使用するソフトウェア管理などPCのあらゆる側面におけるHP Manageability Integration Kitの管理に基づく。（2020年12月時点、米国HP.inc調べ。）

記載事項は2021年6月現在のものです。
本カタログに記載された内容は、予告なく変更されることがあります。

株式会社 日本HP
〒136-8711 東京都江東区大島2-2-1

JPT13612-08