HP TechPulse

セキュリティとプライバシー

ホワイトペーパー

目次

はじめに 3
セキュリティ分野でのソートリーダーシップ 3
HP TechPulse セキュリティ 4
HP TechPulse アーキテクチャ 5
ユーザーと役割 5
地域ルート管理者 5
リセラー 6
マネージドサービスプロバイダー (MSP) 6
会社オーナー 6
会社ユーザー 6
IT 管理者 7
レポート管理者 7
ServiceNow™ 管理者 7
HP TechPulse プロアクティブ管理デバイス 8
HP DaaS Portal 9
ID 管理 9
セッション管理 9
認証 9
マルチテナンシー 10
保存データ 10
伝送データ 10
サードパーティ統合 10
ユーザーインターフェイス (UI) 検証 10
HP TechPulse 分析プラットフォーム 11
データ収集 11
保存データ 11

HP TechPulse オペレーションセキュリティ 12
データセンター 12
ネットワーク 13
セキュリティ強化されたアクセスポイント *14*
アプリケーション、ホスト、管理者セキュリティ 14
データセキュリティ 14
独立した検証 15
HP コンプライアンス & セキュリティフレームワーク 17
タイムライン 17
ISO 27001:2013 認証 18
ISO 27071:2015 Certification (2020 年秋) 19
ISO 27701:2019 Certification (2020 年秋) 19
SOC2 (2020 / 2021) 19
HP セキュリティソフトウェア開発ライフサイクル (SSDL) 20
データ収集 22
データグループ *26*
データプライバシー 27
データの保持 29
データの保管 *29*
サービスの監視および報告 30
サービスの監視 31
まとめ 32

はじめに

データ主導の世界で業務に携わる IT 担当者にとって HP TechPulse は、デバイスやアプリケーションに関する重要なデータを提供するテレメトリ・分析プラットフォームとなり、これにより IT 担当者はディープラーニングを活用して従業員に適切な PC ソフトウェア/サービスを提供でき、成功へと導きます。HP TechPulse は事前に問題を特定し、包括的な修復を行い、組織のセキュリティポスチャを積極的に監視することにより脅威を最小限に抑えます。HP TechPulse プラットフォームは、クラウドベースの HP DaaS ポータルおよび HP TechPulse ソフトウェアアプリケーション (Microsoft Windows、Android、Google Chrome、Apple iOS、Apple MAC の OS に対応) で構成されており、HP TechPulse プロアクティブ管理および HP プロアクティブセキュリティで利用可能です。HP では、デバイス内に埋め込まれた制御ポイントや、境界をまたぐ高度な自動管理モデルなどの技術を開発する、優れた技術力を持つ多種多様な技術センターを構えています。これらの技術により、トップから末端までの堅牢な信頼の連鎖が形成されています。HP は、近年見られる大規模な攻撃を検知して緩和するための新たなメカニズムも絶えず探求し続けています。

セキュリティ分野でのソートリーダーシップ

セキュリティに対する HP の取り組みは、自社製品で終わりではありません。当社はパートナーエコシステム内のセキュリティ面でのベストプラクティスを提唱し、世界中の数十万もの独立した IT リセラーおよびサービスプロバイダーに研修およびリソースを提供する企業として重要な役割を担っています。実際のところ、HP は **クラウドセキュリティアライアンス** (CSA) によって選ばれた最初のマストレーニングパートナーです。クラウドセキュリティアライアンス (CSA) は、クラウドコンピューティング環境のセキュリティ確保を推進するために、ベストプラクティスの定義および意識喚起を専門に行う国際的な組織です。CSA は、最も有名なクラウドセキュリティプロバイダー認証プログラムである STAR (Security, Trust & Assurance Registry) を運営しています。これは、自己評価、第三者による監査、および継続監視による三層から成るプロバイダー保証プログラムです。

クラウドコンピューティグおよび情報セキュリティ分野に精通したグローバルなセキュリティ技術ベンダーである HP は、現場のセキュリティプロセスおよび実装に的を絞ったベンダー中立的なセキュリティ研修を提供する企業として好ましい立場にあります。HP は、世界中の学習センターと多くのパートナー施設およびお客様開発現場にて 35 年以上にわたる複雑な技術研修要件を満たすことで得た経験から学ぶコースを提供しています。

HP TechPulse セキュリティ

1950 年代、W. エドワーズ・デミングらは TQM (Total Quality Management) などの 品質管理の概念を製造業に導入しました。これは最初に日本で根付き、結果として日本製の自動車の品質は米国製の自動車の品質を凌駕しました。1970 年代に米国に届いた品質転換の概念は、IT ソフトウェア業界では 1980 年代に登場し、HP では CEO のジョン・ヤングによって品質プログラム「10X」が導入されました。この目標は、ソフトウェアの品質を 10 年以内に一桁向上させるというも のです。これらの品質プログラムでは、再現性、品質の組み込み、品質管理、およびテスト依存からの脱却ということが注目されました。

それから 40 年近くが過ぎ、品質に対するこの包括的なアプローチの結果、ハードウェア、ソフトウェアアプリケーション、および製品にサイバーセキュリティの回復性を組み込むための重要な機能が開発され、クラス最高のサードパーティ技術を提供するベンダーとのパートナーシップが確立されました。

セキュリティは、すべての階層にセキュリティ制御機能を展開することによって維持されます。1 つの階層に障害が発生した場合、侵害を最小化してセキュリティを常に維持するために、制御機能が他の領域に配置されます。HP TechPulse は、その開発プロセスだけでなくアーキテクチャにも、業界で実証済みのサービスレベルセキュリティを適用します 。

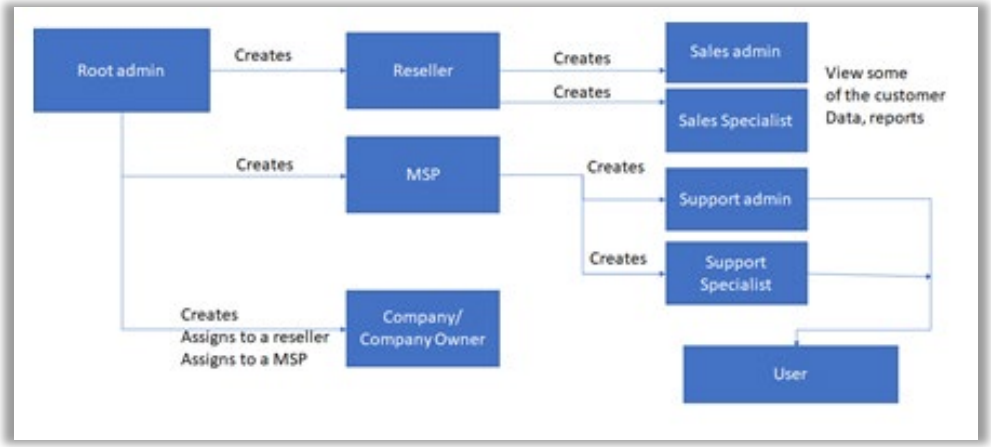
HP TechPulse アーキテクチャ

組織のデバイス、データ、およびユーザーを管理するワンストップのクラウドベースのソリューションとして HP TechPulse は、アーキテクチャおよび開発プロセスに業界で実証済みのサービスレベルセキュリティを適用します。HP TechPulse プロアクティブ管理は、さまざまなサービスを企業のお客様に提供しています。これらのサービスは主に以下のとおりです。

- デバイステレメトリと分析コレクションを複数のオペレーティングシステムに提供。
- マネージドサービスプロバイダーとエンタープライズのお客様に、プロアクティブ管理のためのレポートおよびインシデントの作成機能を提供。
- HP TechPulse プロアクティブ管理経由でさまざまなサードパーティサービスを提供。

ユーザーと役割

HP DaaS ポータルは、以下の図にあるようにさまざまな種類のユーザーと役割があります。



地域ルート管理者

このアカウントは、HP 内のビジネスオペレーション管理者により、新しい会社、リセラー、またはマネージドサービスプロバイダー (MSP) を作成するために使用されます。地域のルート管理者アカウントは制御され、MSP、リセラー、会社テナントを操作および管理できます。一般的にルート管理者アカウントは複数の地域に分けられています。現在、HP TechPulse は以下のように 2 つの AWS 地域データセンターで稼働しています。

1. 米国西部 (US West-2、オレゴン)
2. EU (フランクフルト)

リセラー

リセラーアカウントはセールススペシャリストおよびセールス管理者アカウントがある場合があります。セールス管理者は、セールススペシャリストのすべてのタスクを実行でき、他の人をセールス管理者またはセールススペシャリストとして組織に招待することができます。

リセラーアカウントは割り当てられたお客様の特定のレポートを確認することができます。

*マネージドサービスプロバイダー **(MSP)***

MSP アカウントは、複数の会社に同時にアクセスでき、お客様に代わってデバイス、ユーザー、日常業務を管理できます。MSP アカウントは HP のビジネスオペレーションチームまたはサードパーティパートナーにより管理可能です。

MSP は、管理アクションを実行する 2 種類のユーザーに分けられます。サポート管理者とサポートスペシャリストです。サポート管理者は、追加のサポート管理者またはサポートスペシャリストのアカウントを作成できます。

会社オーナー

会社の作成時、一般的にルート管理者はデフォルトのオーナーを作成します。これらの管理ユーザーは、割り当てられた役割に基づいて、レポートを使用し、その他の管理タスクを実行します。

会社オーナーは会社の他のユーザーを作成したり、管理したりすることはできません。MSP がこれを行うことができますが、MSP により特別な役割が割り当てられている場合、会社オーナーがユーザー管理を実行できます。

会社ユーザー

一般的にユーザーは、アクションを実行する、または実行しない権限のある特定の役割を持つ企業の会社テナント内の人を指します。会社ユーザーは、HP DaaS ポータルへのアクセス権がある、またはない場合があります。例えば、デバイス登録時に作成されたユーザーは、HP DaaS ポータルへのアクセス権のない会社従業員ですが、会社ユーザーの役割は、HP DaaS ポータルにアクセスできるよう変更することが可能です。

ユーザーは以下の例に基づいて作成可能です。

- MSP または特別な役割を持つ会社ユーザーは新しいユーザーを作成し、ユーザーのポータルアクセス権を付与できます。
- デバイス登録時に社用 PIN を使用してユーザーは自動的に作成されます (例: コンピューターまたはモバイルデバイス)。デバイスの登録時にユーザーはポータルに登録されます。

複数の役割を会社ユーザーに割り当てて HP DaaS ポータル内のユーザーアクセス権限を拡大することが可能です。

IT 管理者

IT 管理者の役割により、会社ユーザーは MSP が実行できるほとんどの役割を実行することができます。この役割は、自己管理型のお客様に割り当てられます。

レポート管理者

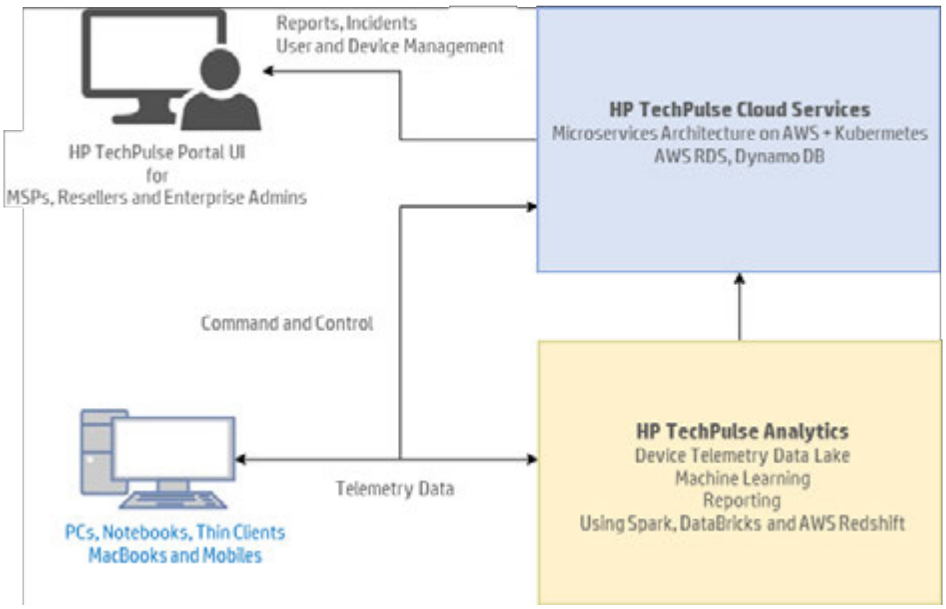
デフォルトでは、会社オーナーはレポートへのアクセス権があります。また、会社ユーザーにレポートへのアクセス権を付与することも可能です。レポート管理者の役割は、HP TechPulse プロアクティブ管理からの情報の利用を許可するのみです。

ServiceNow™ 管理者

ServiceNow 管理者の役割により、お客様およびパートナーは、HP TechPulse のインシデントの統合サービスを構成できます。HP TechPulse インシデント統合サービスは個別に購入する必要があります。
HP TechPulse インシデント統合サービスは以下を提供します。

- ServiceNow 内で HP TechPulse プロアクティブ管理により作成されたインシデントの管理。
- HP TechPulse プロアクティブ管理と ServiceNow 間のインシデントのミラーリング。
- HP DaaS ポータルおよび ServiceNow の両方からインシデントの更新。

以下の図では、HP TechPulse プロアクティブ管理の機能の概要を示しています。



HP TechPulse プロアクティブ管理デバイス

アーキテクチャの観点から、HP TechPulse プロアクティブ管理は、攻撃者によるユーザーのデバイスのコントロールを防止する設計になっています。ハードウェアやオペレーティングシステムに応じて、プロビジョニングプロセス中にデバイスソフトウェアをインストールする必要があります。

デバイスを会社の IT 管理者または MSP により追加するには、デバイスは割り当てられた社用 PIN を使用して安全に HP TechPulse プロアクティブ管理に登録する必要があります。登録時、サーバーとデバイス間で非対称鍵の転送が行われます。デバイスが識別されると各デバイスは一意のキーペアを作成し、デバイスは 24 時間有効なアクセストークンを受け取ります。24 時間後、デバイスは、新しいアクセストークンについて ID を証明するためにサーバーに署名を送信する必要があります。

デバイスは、会社の同意に基づいて、テレメトリデータを HP TechPulse 分析パイプラインに毎日送信します。デバイスは日中、HP DaaS ポータルから.コマンドと制御ビットを受信します。通信もまた前述のアクセストークンにより保護されます。

Microsoft Windows® 版 HP TechPulse プロアクティブ管理デバイスソフトウェアはすべての通信に HTTPS/TLS1.2 プロトコルを使用します。HTTPS はすべての通信にポート 443 を使用します。HP DaaS は、Windows オペレーティングシステム証明書ストアが改ざんされてしまうため、証明書をインストールしません。

HP DaaS Portal

HP DaaS Portal (HP DaaS ポータル) は 2 つの地域でアマゾン ウェブ サービス (AWS) 上にホストされています。一つは米国 (オレゴン)、もう一つは、EU (フランクフルト) にあります。登録する国により、会社テナントは割り当てられた地域で作成されます。管理者は Web ブラウザ経由で HP DaaS ポータルに接続します。HP DaaS ポータルはまた、登録、認証、デバイスとポータル間の通信のインターフェイスとなります。

次のセクションでは、セキュリティに関する設計について説明します。

ID 管理

ID は HP Common Identity System (HP 共通 ID システム) により管理されます。パスワードの品質は構成不可能で、パスワードポリシーは、HP ID Signup Page (HP ID サインアップページ) により設定されます。パスワードは 8 文字以上を使用し、以下の文字を 2 つ以上含める必要があります。

- 大文字 1 文字と小文字 1 文字
- 数字
- 記号または特殊文字

セッション管理

同時セッションが可能なユーザーの数に制限はありませんが、非アクティブの状態が 30 分続いた場合はユーザーセッションの期限は切れます。デバイスのセッションは 24 時間が経過すると期限が切れ、自動的に更新されます。

認証と承認は、Oauth2 プロトコルおよびセッション管理を使用して実装されています。この機能は Json Web Token (JWT) を使用して実装されています。各 HP DaaS ポータルマイクロサービスは、署名および有効期限に JWT トークン検証を適用します。

認証

JWT トークン検証に加え、テナンシーの確認がすべての API に対し行われます。これにより、適切なテナントデータが確実にコーラーに送信されるようにします。また、役割の確認がすべての重要なオペレーションで行われます。

詳しくは、「ユーザー、役割と権限」を参照してください。

マルチテナンシー

HP TechPulse はクラウドベースのマルチテナントのソリューションです。従来の設計では、お客様のテナント情報は、個別のサーバーで保管するよう要求されます。HP TechPulse は、関連データベースとテナンシー資格の確認を使用してテナントデータを論理的に分離します。データは、各テナントに一意の UUID (universally unique identifier) 経由で論理的にテナントと接続されます。

保存データ

デバイス、ユーザー、および関連データなどの会社情報は、AWS Relational Database Service (RDS) MySQL データベースに保管されます。RDS MySQl データベースは暗号化されています。キーやトークンなどの機密フィールドも、AWS Key Management Service (KMS) を使用して暗号化されます。マスターキーは HP のサイバーセキュリティのガイドラインに従ってローテーションされます。

伝送データ

HP DaaS ポータルとのすべての外部通信は HTTPS/TLS1.2 プロトコルを使用します。AWS Virtual Private Cloud (VPC) 内のサービスの通信はプレーンテキストを使用します。詳しくは、「オペレーションセキュリティ」を参照してください。

サードパーティ統合

HP TechPulse は、Vmware Airwatch、Microsoft Intune、ServiceNow などのさまざまなサードパーティサービスと統合します。

サーバー間通信は、パートナーのシステムにより提供された認証方法を使用して HTTPS 上で行われます。サードパーティ統合について詳しくは、HP 担当者までお問い合わせください。

*ユーザーインターフェイス **(UI)** 検証*

UI フィールドは、HP TechPulse クライアントアプリケーションのフィールドの入力を保護します。検証は、データの種類 (文字列、日付/時刻、通貨など) およびビジネスルール (必須または推奨) により提供されます。フィールドはまた、ビジネスと役割とオペレーションにより保護されます (読み取り/書き込み)。スクリプト機能を使用して追加の検証を適用することができます。

HP TechPulse 分析プラットフォーム

HP TechPulse 分析プラットフォームは AWS 上でホストされます。分析プラットフォームは、HP TechPulse プロアクティブ管理のデータ処理を担います。分析プラットフォームの多くの部分は外部からは見えません。

データ収集

分析プラットフォームは、デバイスからデータをアップロードするさまざまなインターフェイスを提供します。分析プラットフォームは、Cognito Identity Pool (CIP) を使用してデータをアップロードします。CIP により、接続、コマンド、ポリシーは、デバイスに送信またはデバイスから収集されることはありません。

保存データ

非構造化保存データは S3 で保管されますが、構造化データは、RedShift で保管されます。構造化および非構造化データは、分析プラットフォームで暗号化されます。

HP TechPulse オペレーションセキュリティ

このセクションでは、通信のさまざまな階層でセキュリティを確保するために HP TechPulse がどのようにサービスレベルのセキュリティを適用しているか説明します。

データセンター

HP TechPulse アプリケーションは、アマゾン ウェブ サービス (AWS)、具体的には Amazon EC2 (Amazon Elastic Compute Cloud) によりホストされています。Amazon EC2 は AWS クラウド内の拡張可能なコンピューティング能力を提供します。HP TechPulse のデータセンターは米国のオレゴン (AWS-OR) およびドイツのフランクフルト (AWS-DE) にあります。拠点がヨーロッパ諸国にあるお客様のデータは、ドイツのデータセンターでホストできます。その他すべての国のお客様のデータは、米国のデータセンターでホストできます。お客様の単一「テナント」内のデータはすべて単一のデータセンターでホストされますが、別のデータセンターに別のテナントを保持して部門ごとにデータをホストすることを希望される場合は、このオプションをご依頼いただけます。HP TechPulse は、AWS を使用することで、Amazon が大規模なグローバルインフラストラクチャを信頼性の高い安全な方法で提供してきた 15 年を超える経験を利用できます。詳しくは、AWS の情報ポータルを参照してください: http://aws.amazon.com/ec2/。

物理階層では、施設およびネットワークのセキュリティを守るために配備される制御に取り組むことが重要です。顧客データおよびデバイスデータは、冗長性を提供するために地理的に分散した AWS データセンターに保管されます。クラウドホスティングの業界リーダとして認識されている AWS とパートナーを組むことで、HP TechPulse は今日利用可能な最も柔軟かつセキュアなクラウドコンピューティング環境の 1 つに構築されたクラウドインフラストラクチャを継承します。セキュリティ上の重要な特徴として、以下のことがあります。

- **セキュリティ重視の設計** – AWS クラウドインフラストラクチャは、セキュリティに最も関心が高い顧客の要件を満たすように設計された AWS データセンターに収容されています。AWS インフラストラクチャは高い可視性を提供しつつ、顧客のプライバシーおよび隔離に関して強力な保護手段を提供するよう設計されています 。デバイス、アプリケーション、位置情報のデータは、匿名化されてから (これにより個人に関連付けられません)、米国の分析データセンターに送信され、保管されます。個人データが保存されたデータベースは暗号化されています。

- **高度な自動化** – AWS では、AWS 独自の環境および拡張要件に合わせてツールを調整するために、大半のセキュリティツールは目的に応じて構築されています。これらのセキュリティツールは、データおよびアプリケーションを最大限保護するために構築されています。つまり、AWS セキュリティエキスパートはルーチン作業に費やす時間を減らし、AWS クラウド環境のセキュリティを高める予防的な対策に注力することができます。
- **高い可用性** – AWS は、システムの停電に対して最大限の回復性を提供するために、複数の地域的リージョン、さらには各リージョン内のアベイラビリティゾーンにわたってデータセンターを構築しています。AWS では十分な帯域幅を追加利用できるようにデータセンターが設計されているため、重大な中断が発生した場合でも、存続している他のサイトにトラフィックを負荷分散できるだけの十分な容量があります。
- **多くの認可** – 認定は、セキュリティ上の特定の制御が備わっており、意図したとおりに動作することを監査人が確認したことの証です。AWS のアカウント担当者に連絡することで、該当するコンプライアンスレポートを確認できます。お客様が政府、業界、および企業のセキュリティ基準および規制を満たすことができるように、AWS では認定レポートを提供しています。このレポートには、AWS クラウドインフラストラクチャがどのように多くのグローバルセキュリティ基準の要件に適合しているか示しており、基準には、ISO 27001、SOC、Payment Card Industry (PCI) Data Security Standard、FedRAMP、Australian Signals Directorate (ASD) Information Security Manual、Singapore Multi-Tier Cloud Security Standard (MTCS SS 584) などがあります。AWS が準拠しているセキュリティ規制および基準について詳しくは、**AWS のコンプライアンスに関する Web ページ**を参照してください。

物理的および環境面でのセキュリティ、AWS へのアクセスおよびネットワークセキュリティについて詳しくは、AWS Overview of Security Processes **ホワイトペーパー**をお読みください。

ネットワーク

ファイアウォールやその他の境界デバイスなどのネットワークデバイスは、ネットワークの外側の境界およびネットワーク内の重要な内部境界で通信を監視および制御するために配置されます。これらの境界デバイスは、ルールセット、アクセス制御リスト (ACL)、および構成を利用して、特定の情報システムサービスへの情報フローを補強しています。

ACL やトラフィックフローポリシーは、トラフィックのフローを補強するために、各管理対象インターフェイス上で確立されます。ACL ポリシーは、Amazon 情報セキュリティにより承認されています。これらのポリシーは、AWS の ACL 管理ツールを使用して自動的にプッシュされ、これらの管理対象インターフェイスが最新の ACL を適用できるよう支援します。

セキュリティ強化されたアクセスポイント

AWS は限られた数のアクセスポイントをクラウド上に戦略的に配置することで、インバウンドおよびアウトバウンドの通信とネットワークトラフィックをより包括的に監視できるようになります。これらのカスタマーアクセスポイントは、API エンドポイントと呼ばれ、これらは HTTP アクセス (HTTPS) が可能です。HTTPS により、AWS.内のストレージや計算インスタンスとのセキュアな通信セッションが確立できます。さらに AWS ではインターネットサービスプロバイダー (ISP) とのインターフェイス通信を管理する専用のネットワークデバイスが実装されています。AWS では、AWS ネットワークのインターネット側のエッジで複数の通信サービス用の冗長接続が使用されています。これらの各接続には専用のネットワークデバイスが使用されています。

アプリケーション、ホスト、管理者セキュリティ

論理階層では、ホストシステム、そのシステム上で稼動するアプリケーション、およびホストシステムならびに関連アプリケーションを管理する管理者を保護するためのさまざまな制御機能が使用されています。

HP TechPulse および顧客データへの管理者アクセスは制限され、厳格に管理されています。タスクを実行するために必要な個人にのみ (ただし、適切なバックグラウンドチェックおよびアカウント管理要件を満たす場合のみ) アクセス権が許可されます。

データセキュリティ

HP TechPulse で交換されるデータには、業界標準の SSL (Secure Sockets Layer) プロトコルである TLS (Transport Layer Security) v1.2 AWS 実装が使用されます。TLS は複数レベルでのデータの保護に役立ち、サーバー認証、データの暗号化、データの整合性を提供します。TLS はアプリケーション層の下で実装されるため、ユーザーからの追加のステップまたは手順に依存しない受動的なセキュリティメカニズムです。アプリケーションは、ユーザーがセキュア通信のことを、ほとんどあるいは全く知らなくても攻撃者から保護されます。これらの機能は偶発的な破損や悪質な攻撃からデータを保護するのに役立ち、一般的な Web ベースの脅威を回避するためのものです。クライアントとサーバー間のネットワーク通信の SSL 暗号化に加えて、HP はログおよび「保存データ」(サーバーデータベースに格納されているデータ) を暗号化します。このアルゴリズムを使用して暗号化されるデータの例として、デバイスの位置情報があります。

HP TechPulse デバイスでは、オペレーティングシステムおよびデバイスソフトウェアをシステム要件に示しておく必要があります。HP 担当者は、管理ポリシー (該当する場合) による定義に従って、セキュリティポリシーを特定にデバイスに適用することをサポートしますが、エンドユーザーのデプロイメントにはログインメールおよびパスワード以外のセキュリティ要件はありません。従業員の電子メールアドレスは、ログイン ID として使用されます。ログインメールおよびパスワードは、ログイン時に TLS プロトコル経由で AES 128 ビット暗号化で暗号化されます。

独立した検証

HP TechPulse では 2 つの異なる脅威インテリジェンスのモデリング手法が行われます。

- **侵入テストの実行基準**
- OWASP (Open Web Application Security Project)

HP TechPulse ソフトウェアではリリースされるすべての機能に対し脅威インテリジェンスのモデリングを実行し、さらに既存の機能のすべての小規模な機能拡張に対しても定期的に実行します。新しい機能のソフトウェア開発を開始する前に HP TechPulse は HP サイバーセキュリティによるセキュリティアーキテクチャの確認も実行します。

HP TechPulse で行われる脅威インテリジェンスのモデリングテストは以下のとおりです。

- HP DaaS **ポータル** – 以下は実行されるテストの例です。
  - クロスサイトスクリプト
  - フィッシング攻撃
  - 認証トークンの盗難
  - 入力ファジング
  - メールスプーフィング
  - SQL インジェクション
  - クロスサイトリクエストフォージェリなど
- HP TechPulse **クラウドサービス** (例: HP TechPulse マイクロサービスおよび関連インフラストラクチャ、ならびに分析インフラストラクチャ) – 以下は実行されるテストの例です 。
  - 認証と承認のインターフェイステスト
  - テナント ID の変更により適切なデータが承認されたユーザーにのみ送信されているか確認
  - SQL インジェクション
  - リモートコードインジェクション
  - DOS 攻撃

  - 入力ファジング

- **HP TechPulse ソフトウェア** (Windows、Android、Google Chrome、Apple iOS、MAC といったさまざまなオペレーティングシステムプラットフォームのデバイスにインストール) – 以下は実行されるテストの例です。
  - インストールソースとアプリケーションの整合性
  - 権限のエスカレーション
  - MITM 攻撃
  - 入力ファジング
  - データ整合性によるコマンド検証
  - 証明書ストアポイズニング
  - 認証の不備
  - セキュリティ構成など
- **外部インターフェイス**と HP TechPulse (Dell VMWareOne、SSH terminals などへの接続)。以下は実行されるテストの例です。

以下は、脅威モデリングに使用されるツールの例です。

- Accunetix
- Burp Suite
- Nmap
- Metasploit
- Editthiscookie

HP TechPulse ソフトウェア開発チームは、セキュアなソフトウェア開発プロセスを実行しています。セキュリティ、脅威モデリング、分析に焦点を置いた定期的なアーキテクチャおよびコードの確認に加えてセキュリティの確認が含まれます。また、HP TechPulse チームは、Nessus エージェントなどのツールによりインフラストラクチャの定期的なスキャンおよび緩和を行います。すべては KPMG により独立して監査され、HP TechPulse ソフトウェアには ISO27001 認証が付与されています。

脅威モデリングは一般的に、お客様またはその他の開発プロセスからは見えない独立した環境で最新ビルド上で実行されます。HP TechPulse の脅威モデリングは、別の HP サイバーセキュリティおよび HP クラウドセキュリティチームにより実行され、HP TechPulse ソフトウェア開発チームとは業務に携わっています。また、HP TechPulse ソフトウェア開発チームには、広範な品質 & セキュリティアシュアラン

スチームの一員として社内脅威モデリングチームメンバーも参加しており、既存のソフトウェアコンポーネントを定期的にテストしています。

HP コンプライアンス & セキュリティフレームワーク

HP TechPulse は、堅牢な認定情報セキュリティおよびリスク管理オペレーションを実装することにより、お客様へのコミットメントを表明しています。あらゆるセキュリティコンプライアンスフレームワークにおいて重要なものは、お客様が HP を信頼して預けていただいた「データ」です。こうした理由から、HP の戦略的目標は、HP TechPulse がお客様のデータを保護するために適切な手順とセキュリティツールを実装することです。世界的に認識された業界の認定により、お客様のデータ (専有情報、一般情報、オペレーション情報、プライバシーデータなど) は綿密に検査され、HP TechPulse のセキュリティコントロールが広く認識されているセキュリティコンプライアンスフレームワークに適合するよう支援します。

タイムライン

ISO 27001:2013 認証

- 情報システムおよびビジネスに重要な情報のセキュリティには、一貫した測定と管理が要求されます。ISO 27001:2013 認証は、独立した監査組織により発行され、継続的なオペレーションとデータ保護を実現する HP のコミットメントを確認するものです。
- 国際標準化機構 (ISO) は、製品、サービス、システムの国際的に認識されたさまざまな規格の開発を行っています。ISO 27001:2013 認証は、登録認証機関による外部監査により付与され、アセットベースです (情報、プロセス、人材、技術)。HP は、マネージドプリントおよびパーソナルシステムサービスに対し、リモートモニタリングおよび管理サービス環境において ISO 認証を獲得しています。
- ISO 27001 は、組織のコンテキスト内で情報セキュリティ管理システム (ISMS) の確立、実装、維持、継続的改善に対する要件を定めています。ISMS は、会社の機密情報を管理する体系的なアプローチです。これにより、情報は、機密保持、整合性、可用性の原則に準拠してセキュアに保持されます 。このアプローチは、人、プロセス、IT システムを対象とし、実装と認定のパスを定義した複数のサポートドキュメントおよびガイドラインで構成されています。

HP TechPulse プロアクティブ管理の ISO 27001:2013 認証は以下を対象としています。

- 情報セキュリティポリシー
- オペレーションセキュリティ
- 情報セキュリティ組織
- 通信セキュリティ
- 人事セキュリティ
- システムの取得、開発、維持
- アセット管理
- サプライヤー関係
- アクセス コントロール
- 情報セキュリティインシデント管理
- 暗号化
- ビジネス継続管理の情報セキュリティ分野
- 物理的および環境面でのセキュリティ
- コンプライアンス

2020 年、HP はさらに ISO 認証を獲得します。以下のとおりです。

- ISO 27701:2019 (PIMS (プライバシー情報管理システム))
- ISO 27017:2015 (クラウドサービス情報セキュリティコントロール)

ISO 27071:2015 Certification (2020 年秋)

HP は、お客様やパートナーに TechPulse が、プライバシー管理の保護、実装、維持、継続的改善のために業界の認定基準に適合していることを認識してもらうために認証の取得に取り組んでいます。

ISO 27701:2019 Certification (2020 年秋)

HP TechPulse の継続的監視プラットフォームを使用するお客様やパートナーは、クラウドサービスプロバイダーを使用してデータが保護されていることを信用できるアシュアランスを求めています。ISO 27071: 2015 は、クラウドサービスのお客様およびプロバイダーの情報セキュリティコントロールの業界で認識された基準を提供します。

SOC2 (2020 / 2021)

SOC2 報告書は、HP TechPulse がセキュリティ、機密保持、プライバシーなどに対し世界的に認識された基準を準拠していることを認めるアシュアランスをお客様に提供します。SOC 2 は、HP がどのようにクライアントのプライベートデータの保持、保管、処理に継続的に l 取り組んでいるかについての検証をお客様やパートナーに提供します。お客様は、リスクの許容をサポートする追加の枠組みを求めています。HP は、2020 年春、SOC2 報告書の取得に向けて未来とお客様のご要望に応えるために継続的な改善に努めています。

HP セキュリティソフトウェア開発ライフサイクル (SSDL)

アプリケーションのセキュリティに対する業界の典型的なやり方は事後対応的であり、品質管理の分野での教訓を活かせていません。よく見られるアプローチは次の 2 つです。

- **「見て見ぬふりをする」** – セキュリティパッチによる事後対応を特徴とします。このアプローチは CVE に依存し、脆弱性を回避したり最小化したりするための努力はほとんど行われません。この姿勢は、セキュリティ関連の規則による負担が最も軽い業界部門に最も多く見られます。
- **「セキュリティをテストに組み込む」** – 顕著に見られる現象は、アプリケーションに回復性が設計されないことです。そうする代わりに、テスト中に脆弱性を見つけて修復することにより労力が投じられ、セキュリティパッチの適用も併用されます。このアプローチは公共部門、セキュリティの規制を受けた業界、および医療業界で最もよく見られます。これらの部門は規制への準拠を示す必要があり、規制としては、例えば、米国の FISMA (Federal Information Security Management Act)、PCI-DSS (Payment Card Industry Data Security Standard)、HIPAA (Health Information Portability and Accountability Act)、HITECH (Health Information Technology for Economic and Clinical Health) などがあります。

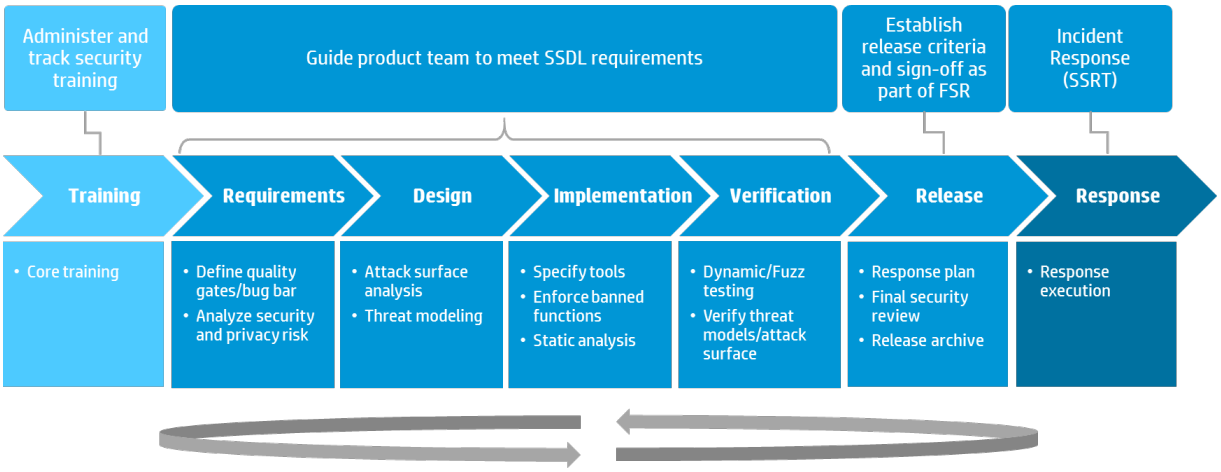
しかしながら、品質属性としてのセキュリティは、品質管理分野で数十年前に学んだのと同様に、ライフサイクルのすべての段階で適用される必要があります。重要ポイントとして、以下のことがあります。

- 品質をテストで組み込むことはできません。設計して構築した後にテストされる必要があります。
- セキュリティ上の不具合および脆弱性は、ライフサイクルの後半でなく早い段階で見つけた方が、ずっと安く済みます 。

HP はソフトウェアのセキュリティを重大なテーマとして捉え、セキュアソフトウェア開発サイクル (SSDL) の採用に至りました。このプロセスには以下に示すいくつかの目標が結び付けられています。

- セキュアなソフトウェアアーキテクチャによりサイバー攻撃を受ける対象を減らす
- コードに起因する脆弱性を最小化する
- 顧客のデータおよび ID に関するプライバシーとセキュリティを保護する

HP ではこの目的を達成するために、具体的なセキュリティ関連手順をソフトウェア開発プロセスに組み込み、セキュリティプロセスが適切に実行されたかどうかを確認するマイルストーン審査を実行し、ソフトウェアアーキテクト、開発者、テスト技術者、プログラムマネージャー、および管理者に対して継続的なセキュリティ研修を展開しています。



SSDL プロセスには以下の 7 つの段階があります。各段階を以下に示します。

- 研修 (第 1 段階) – SSDL プロセス、セキュリティを強化した設計、脅威モデリング、セキュアなコーディングを扱う正規のコース。
- 要件 (第 2 段階) – ソフトウェアプロジェクトのきわめて初期のセキュリティ計画で、機能ごとのセキュリティリスク評価など。
- 設計 (第 3 段階) – セキュリティアーキテクチャの定義および文書化と、重要なセキュリティコンポーネントの特定。
- 実装 (第 4 段階) – 設計された保護スキームおよび緩和アプローチの実行と、ピアコードレビューおよび検証。
- 検証 (第 5 段階) – 動的コード分析、ファジングテスト、攻撃対象領域のレビューの実行。
- リリース (第 6 段階) – SSDL 要件が満たされていること、および既知の脆弱性がないことの確認。
- 対応 (第 7 段階) – リリース段階で概略が記載された応答タスクの実行。

データ収集

HP TechPulse によって収集されるデータの「種類」には、お客様から直接提供されるデータ、または HP DaaS ポータルから自動的に収集されるデータがあります。デバイスのデータは、デバイスにインストールされた HP TechPulse ソフトウェアアプリケーションを使用して収集されます。

HP TechPulse では、契約で定められたサービスを実行するために以下のデータを収集します。

データ収集の目的	収集されるデータ	収集データの説明
アカウントの管理	アカウントデータ	お客様の HP TechPulse サービスの購入または登録情報、HP TechPulse によって生成されたインシデントに関するサポート履歴、お客様の D-U-N-S 番号、アカウント管理などのトランザクションサービスを実行するために必要な HP TechPulse アカウント関連のその他の情報。
HP TechPulse ソフトウェアおよびサービスを適切に機能させる	アプリケーションデータ	HP TechPulse ソフトウェアアプリケーションのソフトウェアバージョンとインストールステータス。データ共有の選択内容と HP TechPulse お客様の設定内容。
アカウントの設定、ID の管理、資格の検証	連絡先データ	HP TechPulse お客様のアカウントの設定と検証、サービス資格、およびインシデントとサービスに関連する電子メール通知のための氏名、住所、電話番号、ファクス番号、電子メールアドレス、その他の連絡先情報を含む個人またはビジネス用の連絡先データ。
紛失したデバイスの場所特定によりデバイスのプロアクティブなサービス保守と管理を提供	位置データ	位置情報ベースのサービスを可能にする地理位置データ。このデータはすべてのお客様に対しデフォルトでオフになっており、TechPulse では、お客様が位置情報ベースのサービスを有効または無効にできるオプションが用意されています。
プロアクティブな IT サービスメンテナンスと管理、お客様中心のレポート/ダッシュボードの提供	デバイスデータ	デバイスに関連した基本ハードウェア情報: コンピューター、オペレーティングシステム、メモリ容量、地域、言語、タイムゾーン、モデル番号、初回起動日、デバイスの使用年数、デバイスの製造日、ブラウザーバージョン、コンピューターメーカー、保証のステータス、デバイス固有 ID、製品によって異なるその他の技術情報。

データ収集の目的	収集されるデータ	収集データの説明
		続き
		バッテリ、ディスク、BIOS、HP SureStart、ディスプレイとグラフィクス、プラグアンドプレイのデバイスとドライバー、ドライバーエラーとドライバークラッシュ、メモリ、リアルタイムクロック、プロセッサ、システムスロット、環境変数、温度、オペレーティングシステム、ネットワークインターフェイス、オペレーティングシステムとサードパーティのパッチ、ウイルス対策/ファイアウォールステータスとアプリケーション、Windows デバイスセキュリティプロファイル、デバイス管理プロファイルとステータス。
		HP Sure Click Advanced および HP Sure Sense Advanced 検出の脅威、HP Sure Recover の設定とアクティビティ。
		デバイスにインストールされているソフトウェアアプリケーション。 **注:** HP TechPulse では、アプリケーションで表示される場合があるファイルの内容や情報をスキャン、または収集することはありません。
		パフォーマンスデータ。バッテリ、ディスク、CPU、メモリ、温度の使用状況。
		使用の頻度と時間に関するソフトウェアアプリケーションの使用状況、ソフトウェア使用状況によるハードウェアパフォーマンスデータへの影響 (バッテリ、ディスク、CPU、メモリ、温度の使用状況)。
		ネットワークの使用状況: デバイスからのネットワーク転送速度。
		ネットワーク識別子。IPv4/IPv6、MAC アドレス、BSSID。データ収集はすべてのお客様に対しデフォルトでオフになっており、HP TechPulse クラウドベースの HP DaaS ポータルでは、お客様がネットワーク識別子のデータ収集を有効または無効にできるオプションが用意されています。

データ収集の目的	収集されるデータ	収集データの説明
		続き
		Web アプリケーションの使用状況。データ収集はすべてのお客様に対しデフォルトでオフになっており、HP TechPulse クラウドベースの HP DaaS ポータルでは、お客様が Web アプリケーションのデータ収集を有効または無効にできるオプションが用意されています。
		Microsoft Windows オペレーティングシステムのブルースクリーンクラッシュ ファイル。データ収集はすべてのお客様に対しデフォルトでオフになっており、HP TechPulse クラウドベースの HP DaaS ポータルでは、お客様がブルースクリーンクラッシュ ファイルのデータ収集を有効または無効にできるオプションが用意されています。
		HP TechPulse でデバイスを登録しているお客様のユーザーの情報。HP TechPulse に登録されているデバイス上でのお客様のユーザーログインにおいて前回サインインしたユーザー情報。データ収集はすべてのお客様に対しデフォルトでオフになっており、HP TechPulse クラウドベースの HP DaaS ポータルでは、お客様がこの情報のデータ収集を有効または無効にできるオプションが用意されています。
HP TechPulse プロアクティブ管理/HP プロアクティブセキュリティのアカウントおよびサービスへのユーザーアクセスの認証および承認	セキュリティ資格情報	HP TechPulse クラウドベースの HP DaaS ポータルのアカウントおよびサービスにアクセスするユーザーの承認の認証に必要なユーザーパスワード、パスワードヒントなどのセキュリティ情報。

データグループ

HP TechPulse[1] により収集されるデバイスデータは、以下のグループが含まれる場合があります。

データグループ	説明
ハードウェア	バッテリ、BIOS、ディスク、ディスプレイ/モニター、グラフィクス、インベントリ、メモリ、ネットワークインターフェイス、PnP (Plug and Play)、プロセッサ、システムクロック、システムスロット、温度およびシステムパフォーマンスデータなど。
ソフトウェアアプリケーション	コンプライアンス、エラー、インベントリ、パフォーマンス、使用率、Web アプリケーション使用データなど。
セキュリティ	レポート対象外デバイス、オペレーティングシステムのパッチ検出および管理、デバイスの位置情報、デバイスのアラーム、ロックおよびワイプ、セキュリティポリシー設定、セキュリティポリシー適用、セキュリティ脅威、ストレージ暗号化、ユーザーセキュリティ設定、Wi-Fi プロビジョニング、Windows Information Protection 違反データなど。
Windows イベントログ	Windows イベントログは、Windows オペレーティングシステムにより保管されるシステム、セキュリティ、アプリケーションの通知の詳細な記録を提供します。これは管理者により使用され、システム問題の診断や問題の予測に役立てられます。
HP 保証および Care Pack	HP Care Pack は、標準の保証期間が切れた後も製品を保証する HP コンピューターまたはプリンタ用の延長保証です。

HP TechPulse で収集されるユーザーデータには以下のものが含まれます。

- ユーザーの電子メールアドレス
- ユーザーアカウントの前回ログオン
- 連続してログオン試行に失敗した数 (ユーザーがログオンすると 0 にリセット)

[1] 収集されるデータはオペレーティングシステムおよび HP TechPulse プロアクティブ管理プランにより異なる場合があります。

HP TechPulse では以下の種類のデータを収集しません。

- 人口統計的情報 (国または言語の設定を除く)
- 金融口座情報、クレジットカードまたはデビットカード番号、信用情報、または支払いデータ
- ソーシャルメディア
- 社会保障番号、社会保険番号、政府 ID などの政府発行の ID 情報
- 医療情報
- 民族、政治的信条、労働組合資格、医療データ、性的指向、遺伝子データなどの機密データ

データプライバシー

HP は、プライバシーとデータ保護における業界のリーダーシップを長年にわたって築いてきました。強固なポートフォリオ製品やサービスとともに、お客様やパートナーの個人データ保護の取り組みを支援しています。HP TechPulse 分析に関して、HP は「データプロセッサ」の役目を果たします。HP Privacy Central (HP プライバシーセントラル) の「Data Processor (データプロセッサ)」のセクションを参照してください。グローバル企業である HP の全世界の事業体は、HP のプライバシーに関する声明と、「国際データ転送」セクションに記載されている国際的なプライバシープログラムに従い、お客様から提供された情報を転送または利用する場合があります。

データプライバシーは **HP プライバシーポリシー**によって世界各国で管理されています。このポリシーは定期的に更新され、次のトピックを扱います。

- HP のプライバシー原則
- 国際データ転送 (EU-US Privacy Shield 情報含む)
- HP におけるデータの使用方法
- HP が収集するデータ
- 子供のプライバシー
- HP におけるデータ保護の方法
- HP におけるデータの共有方法
- HP のコミュニケーション
- 権利の行使と HP へのお問い合わせ

HP のプライバシーに関する声明の変更 HP は一般データ保護規則 (GDPR) への準拠に積極的に取り組んでいます。一般データ保護規則 (GDPR) とは、EU 全体における欧州市民のデータを保護するための規則であり、個人データの処理に伴う自然人の保護に関するルールと、個人データの自由な移転に関するルールが定められています (参照用 URL: https://gdpr-info.eu/art-1-gdpr/)。現在、GDPR に必要な、または提供されている認定もライセンスもありません。しかし、国際標準化機構 (ISO) は、HP およびその他の組織が GDPR に準拠するための枠組みを定めています。2018 年、HP TechPulse プロアクティブ管理は、ISO 27001:13 への準拠について第三者機関により認定されました。

他のデータカテゴリとして保護医療情報 (PHI) があります。保護医療情報 (PHI) とは、米国法の下で、対象事業者 (または対象事業者の事業提携者) により作成または収集される、健康状態、保健医療の供給、保健医療費の支払いに関する情報として定義されており、この情報は特定の個人に結びつけることができます。対象事業者は、1) ヘルスケアプロバイダー (薬局を含む)、2) ヘルスプラン、または 3) Health Care Clearinghouse (医療事務処理会社) のいずれかです。事業提携者とは、対象事業者に代わって、PHI の使用や公開にかかわる職務や業務を遂行したり、サービスを提供したりする個人または組織です。

HP TechPulse アプリケーションでは、健康状態、保健医療の供給、または保健医療費の支払いに関する情報の収集、保存、送信は行っていません。ただし、場合によっては、HP 担当者が HP TechPulse プロアクティブ管理のエンハンスドプランおよびプレミアムプランのお客様向けのサービス (例: リモートサポート、デバイス消去) の実行中にそうした情報にアクセスする可能性があります。

データの保持

データの保持はあらゆるコンプライアンスプログラムの重要な部分であり、データを適切に管理するために必要です。HP のデータ保持ポリシーには、次に示すデータ保存ベストプラクティスが盛り込まれています。

- データの保管が必要な期間に満たない場合、契約または法的要件に違反したり、セキュリティに影響を及ぼしたりする可能性がある。
- データの保管が必要な期間よりも長い場合はプライバシー規制に違反することがあり、このことはお客様の関心が最も高く、販売時の問い合わせが最も多い。
- データをいったん削除したら、お客様や法執行機関に提供する義務はない。

米国およびドイツの地域データセンター内のすべてのデータは、お客様が HP TechPulse プロアクティブ管理または HP TechPulse プロアクティブ管理/HP プロアクティブセキュリティで非アクティブになった後 30 日以内に完全に消去されます。

米国の分析データセンター内のデータは、構造化/未構造化ストレージに対し、データの作成日から 2 年後、または HP TechPulse で非アクティブになった後 30 日以内に完全に消去されます。HP TechPulse ソフトウェアアプリケーションの分析パッケージは、多くの HP アプリケーション (HP TechPulse プロアクティブ管理/HP プロアクティブセキュリティに限らず) で共有される特殊なパッケージであるため、お客様が HP TechPulse で非アクティブになった後も米国の分析データセンターにあるデータが完全に削除されない場合は、そのお客様が他の HP アプリケーションに登録されている可能性が考えられます。そして、データの作成日から 3 年後に削除されます。

注: データ保護目的のために、すべての個人データは、米国の分析データ センターへの送信および保存前に匿名化されます。

データの保管

HP TechPulse のデータ保管は、有料加入者のユーザーおよびデバイス情報に限定されます。

- 個人データを保存する米国およびドイツの地域データセンターのすべてのデータベースは暗号化されます。
- 個人データを保存する米国の ID 管理データセンターのすべてのデータベースは暗号化されます。

- 米国の分析データセンターのすべてのデータベースおよび構造化されていないストレージは暗号化されます。

以下の種類のデータが、それぞれのデータセンターに送信され、保管されます。

データカテゴリ	米国の地域データセンター[1]	ドイツの地域データセンター[2]	米国の分析データセンター[3]	米国 ID 管理データセンター[3]
アカウントデータ	対象	対象	対象外	対象外
アプリケーションデータ	対象	対象	対象	対象外
連絡先データ	対象	対象	対象外	対象
デバイスデータ	対象	対象	対象	対象外
位置データ	対象	対象	対象	対象外
セキュリティ資格情報データ	対象外	対象外	対象外	対象

[1] ヨーロッパ圏以外のお客様向け

[2] ヨーロッパ圏のお客様向け

[3] すべてのお客様向け

サービスの監視および報告

HP TechPulse ではサービスを定期的に更新し、最新の機能および更新をお客様に配信しています。また、HP TechPulse はさまざまな方法で、定期的または予定外の更新やサービスの変更をお客様に通知しています。保守サービスなどのサービスの中断が予定されている場合は、8 時間前にお客様に通知します。

HP では最適なサービスを提供するために、継続的にサービスの監視と報告を行っています。

サービスの監視

HP TechPulse アプリケーションおよびポータルでは、信頼性およびパフォーマンスの監視を 24 時間 365 日行っています。また、ネットワークパフォーマンスおよび可用性の監視も継続的に行っています。すべての監視ツールは、問題や警告をサービスエンジニアに直接送信します。発生した例外は、確認を要する優先度の高い作業項目として、社内チケットシステムに自動的に登録されます。

しきい値を超えた場合、次の自動エスカレーション処理が実行されます。

- 待機中の対応するサポートエンジニアにアラート電子メールが送信されます
- 待機中のエンジニアのモバイルデバイスにプッシュ通知が送信されます
- 電子メールがオペレーションチームの配信リストに送信されます

HP TechPulse プラットフォームでは、次に示すさまざまな監視ツールが使用されます。

- New Relic – システムのさまざまなコンポーネントを監視し、さらに重要なこととして、ボトルネックが生じたときにボトルネックの特定およびデバッグを支援します。ほとんどのアプリケーションおよびサービスは New Relic での測定に対応しているため、継続的なデータ収集およびほぼリアルタイムでのパフォーマンス測定が可能です。
- Amazon CloudWatch – プロビジョニング、サービス障害、しきい値の到達（メモリ消費など）に関するイベントを監視します。最も重要な問題エリアを識別するためにインシデントが確認され、分類されます。優先順位に基づいてアクションが直ちに実行される、または後日の開発のために予定されます。ポストモダンなサービス品質 (QoS) ミーティングが行われ、発見された事項のレビュー、根本原因の特定、および改善のための変更の実装が行われます。HP TechPulse は内部のインシデントログや可用性に関する履歴データをお客様に開示しませんが、HP は 99.9% のアップタイムを目標としてサービス品質に取り組んでいることを約束します。

まとめ

HP は、脅威の状況が急速に変化することを認識しています。サイバー攻撃の進化は 1990 年代後半のファイル削除や Web サイトの改変に始まり、その後は資格情報の窃盗やランサムウェアなどの金銭目的の段階に入りました。ごく最近の攻撃は潤沢な資金を持つ国民国家によって行われ、送電網を破壊したり、数万台のコンピューターやモバイルデバイスを操作不能にしたりすることを狙っています。

HP は 40 年以上前から、こうしたリスクに挑むことを任務としています。HP TechPulse のようなアプリケーションのデザインは、セキュリティ上の脅威の検出および保護に関する HP のイノベーションによる遺産と、セキュリティを重視した昨今の投資の影響を受けたものです。その結果、アプリケーション、物理データセンター、およびエンドユーザーアクセス機能をすべて含む統合化されたセキュリティプラットフォーム上に構築された、クラウドベースのセキュアな IT 管理ソリューションが提供されました。HP TechPulse プロアクティブ管理および HP プロアクティブセキュリティのサービスで提供されるセキュリティ機能内蔵の HP TechPulse は、複数の強力なセキュリティ階層を使用して、組織のデバイス、データ、およびユーザーの日々の管理を簡素化する、信頼できるツールを組織に提供しています。

4AA7-1182JAP v5 – 2020 年 5 月 28 日