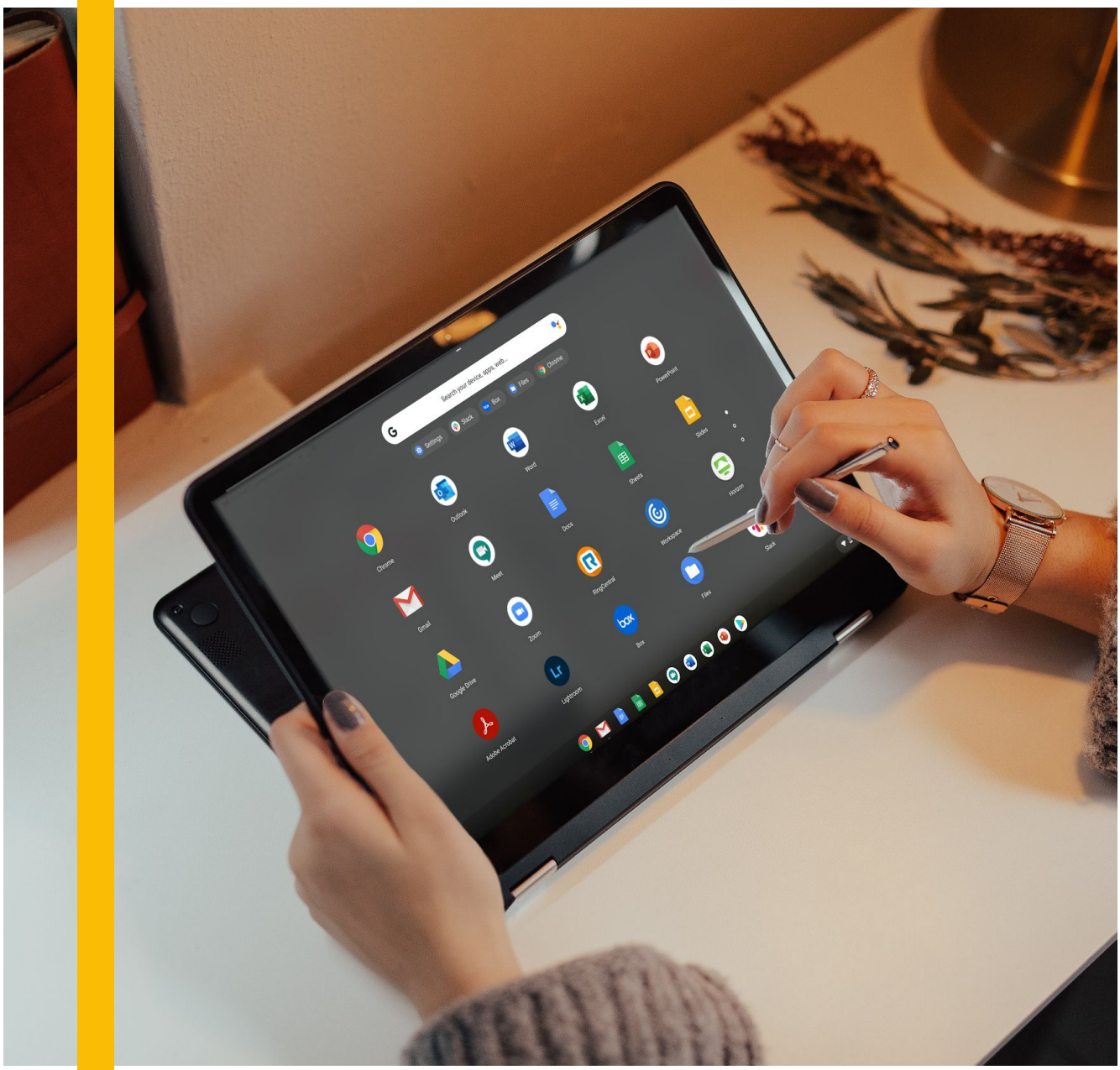
chrome OS

セキュリティのルールを変える

Chrome OS でデータを保護し、IT 管理をシンプルにする



目次

より良い方法を求めて 3

クラウド コンピューティングならではのメリットを活用 5

デバイス: 組み込みのセキュリティと一貫性 6

ファームウェア: ひとつなぎの検証 8

オペレーティング システム: プロセスのサンドボックス化
シームレスなアップデート 10

ブラウザ: サイト分離、セーフブラウジング、2 要素認証 12

アプリケーション: キュレーション、制限、マルウェア検出 14

一元管理 16

管理インフラストラクチャを活用 18

BeyondCorp Enterprise でゼロトラスト セキュリティを実装 19

まとめ: 変革をもたらすセキュリティと運用管理 20

より良い方法を求めて

従来のエンドポイント セキュリティはゼロサムゲーム

脅威は絶えず拡大を続け、それに伴うコストも膨れ上がる一方です。エンドポイントの保護は、サイバーセキュリティや運用の専門家にとって特に大きな課題になっています。それらの専門家は、対応が困難な問題と、進化し続ける攻撃に直面しています。

従来型のエンドポイントは複雑です。一般的に次のような特徴があります。

1. 攻撃対象となり得る多数のソフトウェア（古いバージョン、セキュリティパッチ未適用のバージョン、未承認のソフトウェア パッケージを含む）が存在する
2. 悪意のあるウェブサイトへのアクセス、提供元不明アプリのダウンロード、または必要なソフトウェアアップデートの適用漏れにより、脆弱になっている
3. 知的財産、個人情報（PII）、ユーザーの認証情報が大量に保存されている
4. アプリケーションとOS プロセスとの境界の適用が不十分であるため、1 つのソフトウェアモジュールが侵害されると、攻撃者によってシステム全体または会社のネットワーク全体にアクセスされる可能性がある

エンドポイントは、どれも脆弱性をはらんでいます。今日、サイバー犯罪者の侵入手段はかつてないほど多様化し、組織内部のヒューマンエラーが常にリスクとしてつきまとっています。このような環境の中、サイバーセキュリティチームは、エンドポイントを監視し、脆弱性を特定して侵害を検出すべく、多大な努力を払っています。運用チームは、一貫したイメージを適用し、多数の分散デバイスにまたがるファームウェア、オペレーティングシステム、ユーティリティ、ドライバ、ブラウザ、アプリケーションにパッチ適用およびアップデートを行う作業に、多くの時間を費やしています。
また、勤務場所の分散化が以前よりも進んでいるため、企業ネットワーク向けに設計された従来のツールとプロセスは、効果的ではなくなってきています。

モデルを再考すべきとき

現在、この苦境から抜け出してエンドポイントのセキュリティと管理を大きく改善するよい機会が到来しています。

まず IT 部門では、クラウドベースアーキテクチャならではのメリットを、セキュリティと運用に活用することができます。情報アセットをクラウドに保存して共有すれば、脆弱なエンドポイントに保存する場合と比べてモニタリングが簡単になります。多数のリモート デバイス上ではなく、一元化したクラウドプラットフォームでソフトウェアの追跡とアップデートを行うほうがはるかに簡単です。

第 2 に、技術ベンダーは昨今、「クラウドファースト」のセキュリティを抜本的に見直しており、エンドポイントセキュリティの強化とエンドポイント管理の合理化を実現する画期的な新機能を導入しつつあります。

このテクニカル ペーパーでは、Google がクラウド コンピューティングならではのメリットを活用し、5 つのレベル（デバイス、ファームウェア、オペレーティングシステム、ブラウザ、アプリケーション）での革新的な多層防御を開発することによって、エンドポイント セキュリティをどのように再構築したのか詳細に説明します。

また、次のような機能についても見ていきます。

1. マルウェア、フィッシング、ドライブバイダウンロード、APT といった特定の脅威から保護するGoogle の革新的なセキュリティ機能
2. ソフトウェアのアップデート、デバイスの紛失と盗難への対処、分散したデバイスに対するセキュリティポリシーの管理などの運用業務を大幅に合理化するChrome Enterprise
3. Microsoft Active Directory と主要サードパーティ製企業向けモバイル管理（EMM）ツールの活用によるエンドポイント管理の自動化

クラウド コンピューティングならではのメリットを活用

エンドポイント上のデータを低減

クラウドベースアーキテクチャならではのメリットの1 つに、ほとんどの情報アセットがエンドポイントではなくクラウドに保存されるという点があります。ノートパソコンの紛失や盗難があった場合でも、顧客リスト、事業計画、収益レポート、人事データ、ソフトウェア プログラムの流出について心配する必要はありません。デバイスが侵害された場合でも、顧客のクレジットカード番号、従業員の医療情報、会社の財務システムにアクセスするためのパスワードが攻撃者に発見されてしまう可能性が大幅に低減されます。

攻撃対象範囲の減少

クラウドベースのアーキテクチャでは、エンドポイントにインストールされるソフトウェアの数がはるかに少なくなります。分散したデバイスには依然としてファームウェアとオペレーティング システムが必要ですが、ユーティリティ、ドライバ、ブラウザ、ビジネス アプリケーション、個人用アプリを従来のエンドポイントのように多数インストールする必要はありません。従来のエンドポイントと比べて攻撃対象となる脆弱性が減少し、インストール、管理、保護が必要なソフトウェア コンポーネントがごく少数になります。

頻繁に行われる高速アップデート

従来のエンドポイントでは、国中または世界中に分散したデバイス上のソフトウェア コンポーネントにパッチを適用してアップデートするという、煩わしい定型業務の繰り返しが必要です。また、脆弱性が発表されたり新しい攻撃手法が発見されたりするたびに、サイバーセキュリティや運用の担当者が、多数のエンドポイントに急いでパッチを適用または管理を追加する必要に迫られます。無防備なままの状態が長く続くほど、攻撃的なハッカーにつけ込まれる可能性が高まります。

クラウドベースのアーキテクチャでは、ソフトウェアを一元的にアップデートし、制御を 1 か所でデプロイおよび管理して、エンドポイントを最新の状態に保つために必要な業務を大幅に削減できます。

デバイス: 組み込みのセキュリティと一貫性

クラウドベースのアーキテクチャでは、多数の革新的セキュリティ機能と管理機能を利用できる環境が整っています。まず、Google の Chrome OS と Chrome ブラウザを搭載したノートパソコンやタブレットなどの Chrome デバイスがあります。Chrome OS デバイスは、Acer、ASUS、Dell、Google、HP、Lenovo、Samsung といった業界トップクラスのさまざまなテクノロジー企業から提供されています。

ハードウェア セキュリティ モジュール

すべての Chrome OS デバイスで、ユーザーデータと設定がデフォルトで暗号化されます。ユーザーが（または誰であっても）この暗号化を無効にすることはできません。

また、各ユーザーのデータと設定は、それぞれ固有の鍵で暗号化されます。攻撃者がこの鍵を使用するには、ユーザーパスワードとセキュリティモジュールへのアクセス権の両方がほぼ必ず必要になります。そのため、攻撃者がユーザーのデータを読み取ることはきわめて困難です。また、たとえ攻撃者がChrome OS デバイスと 1 人のユーザーのパスコードを入手している場合でも、他のユーザーのデータを復号して読み取ることはできません。

ユーザーデータを分離すると、ほかにもメリットがあります。同僚や家族とデバイスを安全に共有したり、レンタルデバイスや臨時従業員用に「Chromebook 貸し出しプログラム」による共有などの最新の手法を安全に導入したりできるのです。

シナリオ:
内部関係者による侵害の防止

Chrome OS デバイスでは、最近のすべての機種に、Google の仕様に合わせて設計されたハードウェア セキュリティモジュールが含まれています。このモジュールは専用チップ上にフラッシュ メモリ、ROM、RAM、不正使用検出機能を搭載しているため、モジュールに保存されている情報の不正使用はきわめて困難です。ハードウェアセキュリティモジュールには重要な情報と暗号鍵が保存されており、オペレーティングシステムがそれらにアクセスすることはできません。また、特定のタイプのサイドチャネル情報漏洩攻撃や物理的欠陥を狙ったインジェクション手法から守られます。

エンドポイント間の一貫性

Chrome OS デバイス メーカー各社は、Google が設定した品質、パフォーマンス、セキュリティの仕様を満たすことに同意しています。Chrome ブランドのデバイスは、Google がハードウェア設計を審査し承認して初めて出荷を許されます。また、メーカー各社は、他のすべてのChrome OS デバイスで稼働しているものと同じファームウェア、Chrome OS、Chrome ブラウザを使用することにも同意しています（図1）。

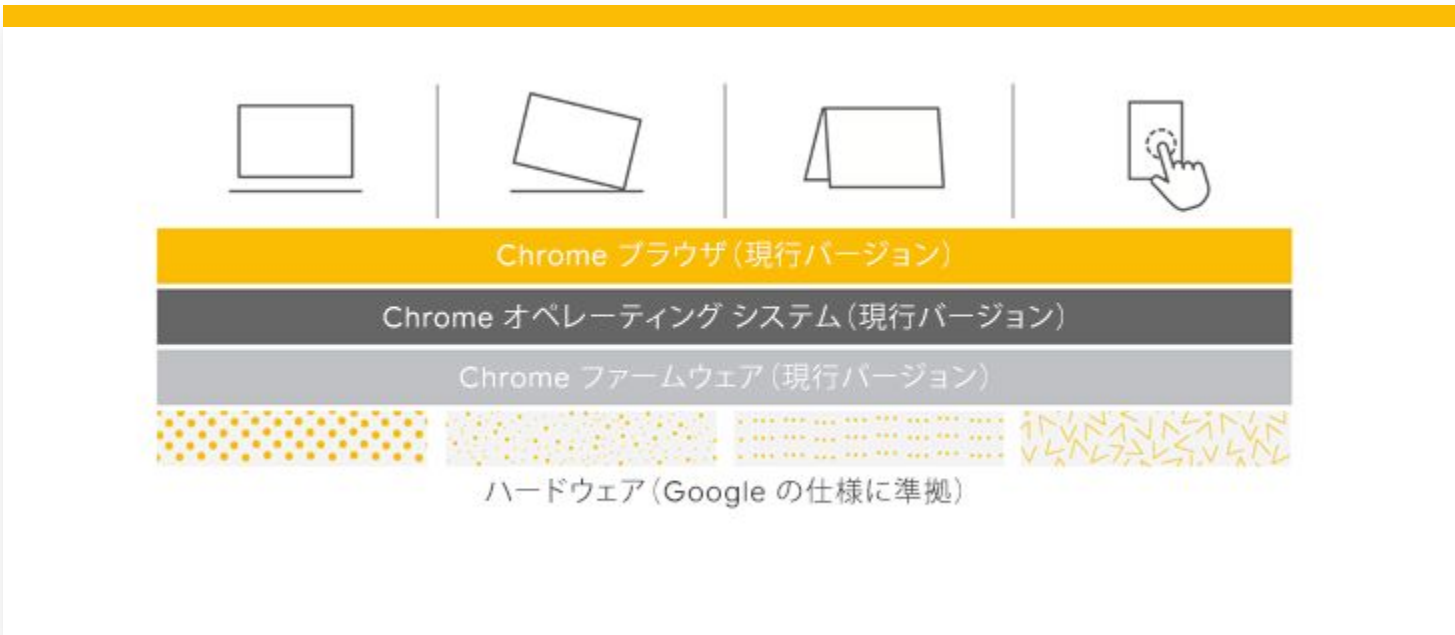


図 1: シームレスなユーザー エクスペリエンスとシンプルなエンドポイント管理を実現するために、すべての Chrome OS デバイスに同じバージョンのファームウェア、Chrome オペレーティング システム、Chrome ブラウザを搭載

この共通性は、ユーザーにとっても管理者にとっても大きなメリットです。ユーザーは、すべてのChrome OS デバイスを同じ操作で快適に使用できます。セキュリティチームと運用チームは、標準化された運用環境を提供できます。複数のバージョンのファームウェア、オペレーティングシステム、システムユーティリティ、ブラウザを管理する必要はありません。また、互換性のないソフトウェアリリースに起因する脆弱性について心配する必要もありません。問題が発生した場合でも、これまでよりはるかに短時間で簡単にトラブルシューティングできます。

デフォルトのセキュリティ

攻撃やユーザーの過失に対する保護策として最も望ましいのは、セキュリティが最初から組み込まれていることです。サイバー セキュリティ（または、そもそもパソコン自体について）あまり詳しくないユーザーのために、Google はエコシステム パートナーと協力して、セキュリティを確保するための機能やデフォルト設定を特定しています。先に述べたように、ユーザーデータはすべてデフォルトで暗号化されます。詳しい例について、このドキュメントで後ほど説明します。

ファームウェア: ひとつなぎの検証

先進的な標的型攻撃において、「持続性」は重要な要素です。通常、高度な攻撃では、エンドポイントにコードやスクリプトを埋め込むことで、再起動後やシステム障害後も攻撃者がエンドポイントへの影響を持続できるようになっています。

クラウドベースのアーキテクチャでは、従来のエンドポイントで攻撃者が使用していた持続手法の多くが通用しなくなっています。たとえば、ユーザーによるインストールが可能なドライバやスクリプトがエンドポイントに保存されていなければ、それらによって再起動後に悪意あるコードが保持されることはありません。

ただし、デバイスに搭載されている書き込み可能なファームウェア、オペレーティングシステム、ブラウザへのコード挿入を攻撃者が試みる可能性は残っています。

これを防ぐために、Google では「確認付きブート」と呼ばれる手法を使用して、再起動後に実行されるファームウェア、オペレーティングシステム、ブラウザのコードがいずれも改ざんのないGoogle 提供のソフトウェアであることを確認しています。

シナリオ: ルートキットのブロック

サイバー犯罪者であるBela が、Chrome OS デバイスにアクセスしてスーパーユーザー権限を取得しています。Bela は、ルート パーティションを読み書き可能として直接再マウントしてから、ルートキットをカーネルモジュールとして追加しました。しかし次回の再起動時には、ルート パーティションのその部分の署名が、想定される署名と一致しません。起動プロセスは停止し、デバイスは、ファームウェアと OS のバックアップ イメージを使用して再起動します。再起動後、Bela はルートキットを使用してデバイスを操作できなくなりました。

Chrome OS デバイスの起動時には、読み取り専用ファームウェアが署名と署名付きハッシュを使用して、書き込み可能なファームウェアとGoogle 承認済みイメージが完全に一致することを検証します（つまり、ファームウェアコードのハッシュを計算し、署名付きハッシュと一致することを検証します）。次に、検証済みの書き込み可能ファームウェアが、同じプロセスを使用してカーネルを検証します。続いて、検証済みのカーネルが、オペレーティングシステムとChrome ブラウザのすべてのコードブロックを検証します。マルウェアや他の不一致を示す形跡が見つかった場合、起動プロセスは停止し、デバイスはバックアップバージョンの書き込み可能ファームウェアとオペレーティングシステムを使用して再起動します（図2）。

確認付きブートにより、危険なタイプの攻撃から保護されるだけでなく、侵害されたファームウェアやファイルの修復に必要とされる単調な作業を運用担当者が行う必要がなくなります。

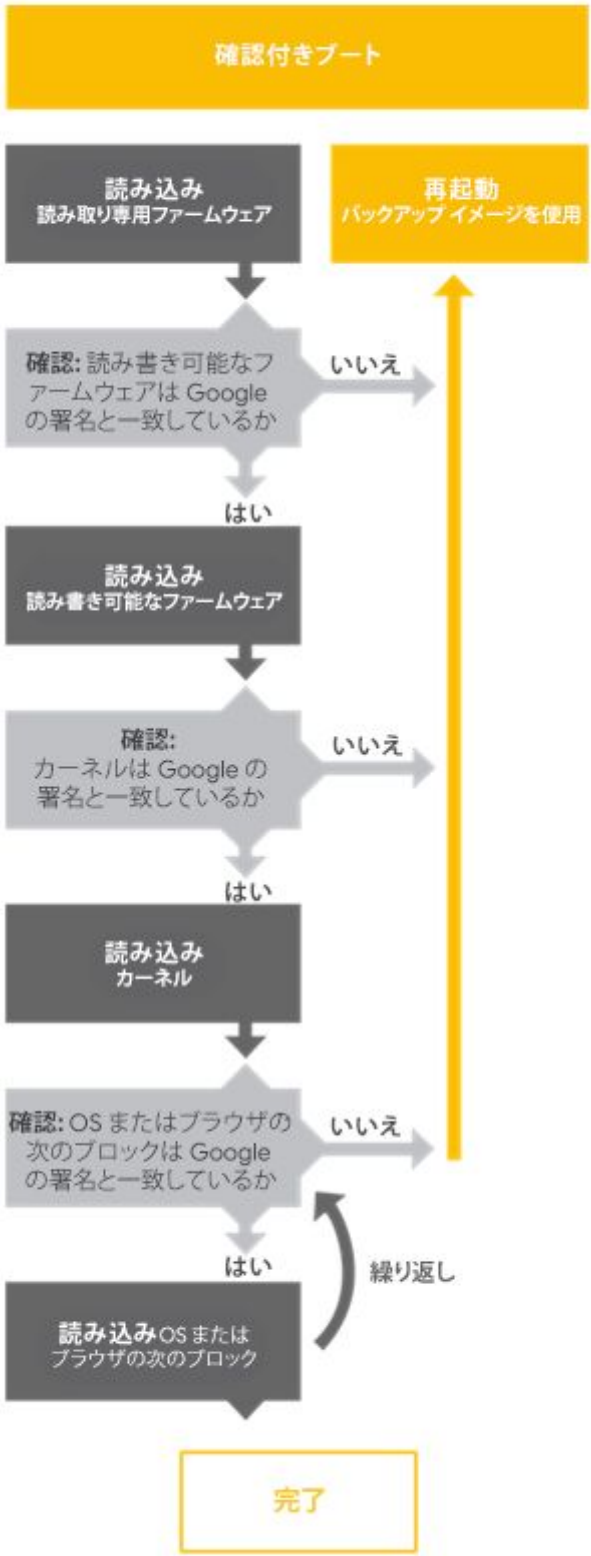


図 2: 確認付きブートのプロセスにより、ファームウェア、オペレーティング システム、ブラウザが改ざんされていないことが確認される

オペレーティング システム:
プロセスのサンドボックス化とシームレスなアップデート

Chrome オペレーティング システムにはいくつかのセキュリティ機能が含まれています。それによって、アプリケーションが保護されるとともに、一般的なオペレーティング システムのアップデートとパッチ適用に伴う面倒な作業から解放されます。

権限の分離とプロセスのサンドボックス化

ある種のサイバー攻撃では、エンドポイント上のソフトウェア コンポーネントを制御するために、侵害されたウェブサイトまたはクラウドベースアプリケーションが使用されます。

クラウド ファーストの環境では、侵害される可能性のあるオペレーティング システム コンポーネント、ユーティリティ、ドライバ、その他のソフトウェアの数が、はるかに少なくなります。しかし、Chrome OS のアーキテクチャでは、攻撃者の制御下にあるアプリケーションから他のソフトウェアに影響が及ぶのを防ぐために、さらなる対策が取られています。

たとえば、Chrome OS ではプロセスのサンドボックス化が利用されています。これにより、実行中のプロセス間に厳格な境界が適用されるため、アプリケーション同士が、厳密に制限された状況下以外では通信できなくなります。実行中の各プロセスは、本当に必要な権限しか使用できません。セキュリティを重視する組織において機密情報へのアクセス権が「知る必要のある」人のみに限定されているのと同様に、Chrome OS は、プロセス間の通信を、本当に「使う必要がある」プロセスだけに限定しています。

シナリオ:
ランサムウェアの排除

Arjun は作業の合間にChrome OS デバイスの新しい壁紙を探していました。不運なことに、彼が見つけたFortnite のファンサイトはサイバー犯罪者が支配する「たまり場」でした。ファイルのダウンロードリンクをクリックすると、不正なコードが、Chrome OS デバイス上の全データと全ファイルの暗号化を試みます。幸い、そのコードの動作は、1 つのプロセス サンドボックス内に隔離されました。「You can’ t run this file」(このファイルを実行できません)というメッセージが表示され、ランサムウェア攻撃がユーザーデータに達する前に阻止されました。

オペレーティング システムのシームレスなアップデート

オペレーティングシステムを最新の状態に維持することは、多くのセキュリティチームや運用チームにとってストレスの大きい仕事です。従来のエンドポイントでオペレーティングシステムのアップデートを行うには、エンドユーザーの業務を中断してもらう必要があり、エンドポイントが数分さらには 1 時間以上にわたって使えなくなることがあります。これにより、生産性低下の点で実質的な損害が発生し、ユーザーの苛立ちや IT 部門への不満につながる可能性があります。

さらに、ユーザーがアップデートを拒否することも少なくありません。その場合、デバイスは攻撃を受けやすい状態で放置されてしまいます。

Google は、このような課題に対応する革新的な解決策を提供します。各デバイスに、現在のバージョンと以前のバージョンの 2 つのオペレーティングシステムを格納します。システムが現在のオペレーティングシステムを使用して稼働している間に、アップデートバージョンをバックグラウンドでダウンロードして保存できます。ユーザーには影響がありません。ユーザーがデバイスを再起動すると、アップデートされたオペレーティングシステムが数秒で読み込まれます（図3）。

この仕組みにより、前述の確認付きブートのプロセスもシンプルになります。システムの起動中に、実行中のオペレーティング システムのコードが改ざんされていることが検出されても、以前のクリーンなバージョンがデバイスにあり、即座に使用できる状態になっています。

Chrome OS デバイスを使用すると、オペレーティングシステム コンポーネントの定常的なアップデート業務から解放されます。実際、Google では約 6 週間ごとに Chrome OS をアップデートできますが、これは他の主要なオペレーティングシステムよりはるかに高い頻度です。また、オペレーティングシステムの脆弱性が新たに発見された場合は、それに対するセキュリティ パッチをきわめて迅速にデプロイし、危険にさらされる期間を短く抑えます。

図 3: デバイスの種類を問わずクラウドベースの OS が安全かつ頻繁にアップデートされ、デバイスとユーザーの生産性が最大限に維持される

ブラウザ: サイト分離、セーフ ブラウジング、2 要素認証

Chrome OS デバイスでは、ウェブとのやり取りはすべて Chrome ブラウザを介して行われます。業界をリードするこの Google ブラウザには、革新的なセキュリティ機能が組み込まれています。

タブのサンドボックス化とサイト分離

Chrome OS 関連で説明したサンドボックス化のコンセプトは、Chrome ブラウザにも当てはまります。ブラウザで開かれているすべてのタブに独自のサンドボックスがあるため、1 つのタブへの攻撃が他のタブに伝播して影響を及ぼす可能性は、きわめて低くなります。

この原則は、サイト分離を伴うことで、さらに強固に実現されます。1 つのタブ内で複数のウェブサイトへのアクセスが行われるのは、珍しいことではありません。たとえば、あるサイトで HTML ウェブページを読んでいるときに、2 つ目のサイトから画像が、3 つ目のサイトから動画が、そして 4 つ目のサイトからスクリプトがダウンロードされるなどのケースです。サイト分離により、これらの各サイトのプロセスは、互いに分離された状態を維持します（図）。Chrome ブラウザでは、分離する対象をすべてのサイトとするか選択したサイトのみとするのかを管理者が選択できます。

図 4: Chrome OS と Chrome ブラウザでは、複数のレベル（サイト、タブ、アプリケーション）で分離を行う

ユニバーサル クロスサイト スクリプティング（UXSS）や投機的実行機能を持つサイドチャネル攻撃（Specter や Meltdown など）のような脅威では、悪意あるウェブサイトが、別のウェブサイトに属するメモリ内のプロセスやデータにアクセスしようと試みますが、サイト分離機能は、このような脅威からの保護に役立ちます。

セーフ ブラウジング

現代の企業にとっての最大の危険は、侵害されたウェブサイトから発せられるマルウェア攻撃やフィッシング攻撃に関連するものが多くを占めています。

Google のセーフブラウジング機能では、ユーザーが不審なファイルをダウンロード、または、マルウェアもしくはフィッシングコンテンツを含むウェブサイトにアクセスしようとすると、警告が表示されます。これは、安全ではない数多くのウェブサイトを日々検出して 30 億台のデバイスを保護しているGoogle のサービスをベースにした機能です。

セーフ ブラウジングのメッセージは、Chrome ブラウザの画面に表示されるだけではありません。Google 検索や Android アプリでは、危険なサイトを警告するメッセージが表示され、Gmail のメッセージには、悪意あるサイトへのメールリンクについて警告するメッセージが表示されます。

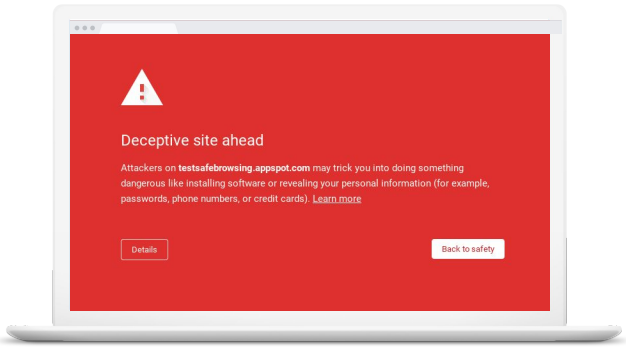
セキュリティ キーと 2 要素認証

2 要素認証を使用すると、ユーザーの認証情報が不正使用された場合でも、システムとデータを保護できます。ユーザーは、本人であることを証明するために、自分で把握している情報（通常はパスワード）と、もう1 つの情報（多くの場合、認証鍵や、スマートフォンに送信されたコード）を入力するよう求められます。

Google では、効果的な2 要素認証を実装するために、世界で最も簡便とも言える方法を提供しています。ユーザーに求められる操作は、自分のGoogle アカウントにアクセスして、[2 段階認証プロセス] を選択し、2 つ目の認証方法をオプションから選択することだけです。オプションには、テキストでのコードの受信、スマートフォンでのメッセージのタップ、USB ポート経由でChrome OS デバイスに接続しているTitan セキュリティキーの使用などがあります。利便性を図るため、ユーザーが特定のデバイスを信頼済みと指定することができ、そのデバイスでは2 つ目の認証方法がなくてもログインできます。

シナリオ:
フィッシング攻撃の回避

Emily は小規模な製造会社の最高財務責任者です。CEO から Emily にメールが届きました。その内容は、在庫が大幅に不足している部品の供給を確保するため、中国の新しいサプライヤーに2 万ドルをすぐに送金するようにとの指示でした。Emily は、CEO がベンダー確保の目的で中国に出張中であることを知っていたので、メールの内容には信ぴょう性があるように思われました。しかし、メールに記載されている新しいベンダーのウェブサイトへのリンクをクリックすると、偽のサイトであることを知らせる警告が表示され、警告画面上の [安全なページに戻る] をクリックするよう促されました。セーフブラウジングのおかげで、Emily はビジネスメール詐欺（BEC）のフィッシング攻撃を回避できました。



アプリケーション: キュレーション、制限、マルウェア検出

Chrome OS デバイスでは、Android アプリ、オフィス生産性向上アプリケーション(Gmail、Google ドキュメント、Google スプレッドシート、Google スライド、Google 図形描画)、Chrome 拡張機能、Linux ベースのアプリ、PWA(プログレッシブ ウェブアプリ: 読み込みが速く、ローカルにインストールされたアプリケーションと同等の機能性と応答性を発揮するアプリケーション)などのさまざまなアプリケーションを実行できます。

企業で、Chrome Web Store の Google 提供アプリや Google Play ストアの Android アプリへのアクセスをユーザーに提供する際は、セキュリティを強化し、管理を合理化するさまざまな機能を使用できます。

サーバー側でのマルウェアの検出とリモートでのアンインストール

Google Play プロテクトは、世界で最も広く導入されているモバイル セキュリティ サービスであり、毎日20 億人のユーザーのセキュリティを確保しています。Android のセキュリティチームのエキスパートは、すべてのAndroid アプリに対し、Google Play ストアでの公開を許可する前に厳密なセキュリティテストを実施しています。Google のポリシーに違反するアプリやデベロッパーは、ストアに承認されません。

さらに、Google Play プロテクトは Google Play ストア内のアプリを継続的にスキャンして検証しています。マルウェアが見つかったアプリは、Google Play ストアでの提供を直ちに停止されるだけでなく、それまでにダウンロードされたすべてのシステムから自動的にアンインストールされます。

Google Play ストアでのアプリのキュレーションとブロック

脆弱性が存在するアプリケーションや攻撃者によって開発されたアプリケーションをダウンロードしたことからユーザーがデータ侵害を受けたという事例は、枚挙にいとまがありません。

IT 管理者は、承認済みのアプリケーション以外はインストールしないよう強くユーザーに呼びかけたり、承認済みのアプリケーションしか実行できないようにエンドポイントをロックダウンしたりして、むやみなダウンロードを抑制すべく長年にわたって努力してきました。

シナリオ: シャドー IT の阻止

Carlos は、4 つの大陸で活動する国際的なマーケティング チームを管理しています。コラボレーションツールを実装してコミュニケーションと企画立案を改善したいと考えています。Carlos は、「オンラインコラボレーションツール 20 選」という記事をオンラインで見つけました。実は、紹介されたツールの多くにはエンタープライズ レベルのセキュリティ機能と管理機能が含まれていなかったのですが、それには気づきませんでした。幸い、長い時間をかけて20 種類のツールをすべて試す前に、自社のmanaged Google Play ストアをチェックしてみたところ、2 種類の承認済みチームコラボレーションアプリ(Slack と Google Chat)を見つけました。どちらも機能性とセキュリティに優れています。さらに、これらのアプリは会社のIT 部門でサポートされており、そのどちらかを使用すれば、同じアプリを使用する他のグループすべてとのコラボレーションが可能になります。

前者のアプローチは効果的ではありませんでした。なぜなら、承認済みのアプリケーションの数が必然的に少なくなるため、ビジネス アプリケーションに対する全員のニーズと個人用アプリケーションやエンターテイメントへの要望を満たすことができないからです。後者のアプローチも、従来のエンドポイントのロックダウンに使用するテクノロジーは実装が難しく、概してユーザーからの抵抗も大きいため、うまくいきませんでした。

ウェブベースのテクノロジーを利用すれば、セキュリティチームと運用チームは、ユーザーの失望や不満を招くことなく未承認のアプリケーションの使用を止められるようになります。

Google Play ストアは、ビジネスの生産性、コミュニケーションとコラボレーション、ビジネスプロセス、ニュース、エンターテイメント、ゲームなど、数千種類のアプリをユーザーに提供しています。これらはすべてAndroid セキュリティチームによってテストされ、脆弱性やセキュリティ上の深刻な欠陥がないことが確認されています。

管理者は、自分の組織用のmanaged Google Play ストアを作成して、幅広い豊富なアプリケーションセットをキュレートできます。たとえば、自社従業員向けに、生産性向上アプリケーションやコラボレーションアプリケーションを多数取り揃える一方で、ゲームアプリやソーシャルメディア アプリについては使用を制限するなどが可能です（図5）。

managed Google Play ストアでは、必要に応じて、さらに徹底的に承認済みアプリケーションリストを実装することも容易です。それにより、組織内の全員が、同じ生産性向上ツールとコラボレーションツールの使用を求められると同時に、他の少数のアプリから選択することも許されます。

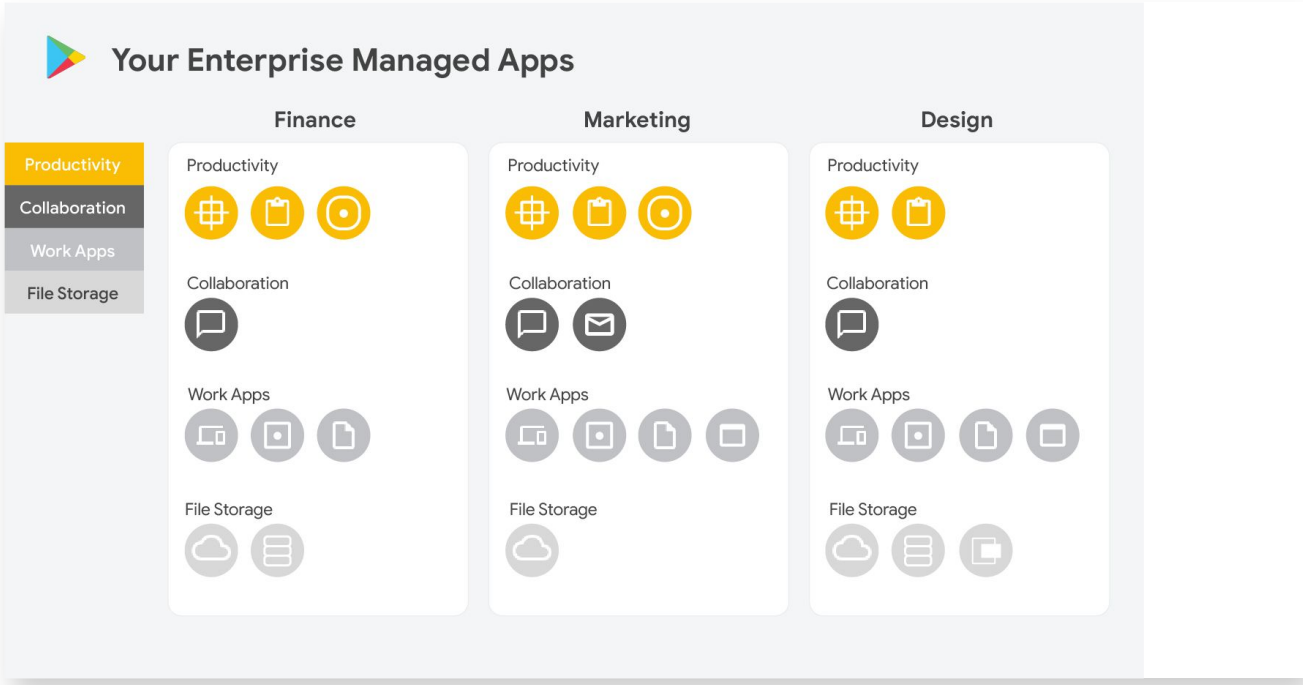


図 5: managed Google Play ストアでは、企業内の各グループが、キュレートされた承認済みアプリケーション リストにアクセスできる

一元管理

Chrome OS では、Chrome OS デバイスとその他のエンドポイントに関するポリシーや、Windows、Mac、Linux システムに搭載の Chrome ブラウザに関するポリシーを、セキュリティ チームと運用チームが一元管理することが可能です。Chrome Enterprise Upgrade には、デバイス管理機能と Google による年中無休 24 時間のサポートが含まれており、何万ものユーザーとデバイスを含む環境に拡張する企業をサポートします。

選択されたポリシーの概要

Chrome Enterprise を使用すると、セキュリティと設定に関する300 種類以上のポリシーを管理者がエンドポイントに設定し適用することが可能になります。管理対象のChrome デバイスに関する主なセキュリティ関連機能には次のようなものがあります。

デバイスのプロビジョニングとプロビジョニング解除。管理者が、自分でデバイスを登録したり、ユーザーにデバイスの登録を許可したりできます。登録されたデバイスは、ユーザーの組織向けに定義されたChrome Enterprise のポリシーに沿って管理および保護できるようになります。管理者は、デバイスのプロビジョニングを解除できます。解除すると、ポリシーが無効になり、そのデバイスからは会社のリソースにアクセスできなくなります。

リモートでのデバイス無効化。デバイスの紛失または盗難が発生した場合は、リモートで無効化できます。

ログインの制限。管理者により、デバイスへの匿名ログイン（ゲストブラウジング）をユーザーに許可、Google または G Suite アカウントを義務付け、または、1 人もしくは少数のユーザーを指名してアクセス権を限定することが可能です。

一時的ログインモードの設定（ログアウト時にユーザーデータを消去）管理者がデバイスを一時的ログインモードに設定することが可能です。このモードでは、ユーザーがログアウトすると、データと設定（ブラウザの履歴、拡張機能とそのデータ、Cookie などのウェブデータを含む）が消去されます。共有、キオスク、または一時ユーザー用にデバイスを使用するときは、一時的ログインモードにすることで安全性が高まります。

ウェブアプリとブラウザ拡張機能の制限または義務付け。管理者により、Chrome ウェブアプリやブラウザ拡張機能（ブラウジング環境をカスタマイズする小さなソフトウェアプログラム）のユーザーによるインストールをブロック、特定のアプリや拡張機能のインストールをブロック、または、特定のURL からのアプリおよび拡張機能のみインストールを許可することが可能です。また、特定のアプリや拡張機能のインストールを強制することもできます。

権限に基づいてアプリケーションや拡張機能をブロック。アプリとブラウザ拡張機能の多くは、インストール先のデバイスのリソースを使用するために権限をリクエストします。管理者は、特定の権限を使用するアプリや拡張機能のインストールをブロックできます。たとえば、画面、ウィンドウ、タブのコンテンツをキャプチャする権限、クリップボードのコンテンツを読み取る権限、デバイスのマイクやカメラから音声または動画をキャプチャする権限、ユーザーの位置情報を取得する権限、デバイスのネットワークに関するメタデータをクエリする権限、デバイスの電源管理機能をオーバーライドする権限などをリクエストするアプリや拡張機能のインストールを禁止できます。この機能を使用するとIT 部門にとってはリスクの低減が可能になり、ユーザー側は、セキュリティを脅かすことのない「無害な」アプリを自由にインストールできるようになります。

Bluetooth や位置情報の無効化。デバイス上でBluetooth と位置追跡を無効化できます。

外部ストレージデバイスの使用の制限。USB フラッシュドライブ、外付けハードドライブ、光学式ストレージデバイス、メモリカードなどの外部ストレージデバイスの使用を完全にブロック、または読み取り専用モードでのみ許可できます。

リモートアクセスとシングルサインオンの管理。リモートアクセスとSAML ベースのシングルサインオン（SSO）に関するパラメータを管理者が設定することが可能です。これにより、ユーザーはセキュリティと利便性を適切なバランスで両立させながらネットワークやウェブアプリケーションにアクセスできます。

デバイスとユーザーの追跡。オペレーティングシステムとファームウェアのレベル、CPU と RAM の使用統計、接続されているストレージデバイス、使用状況の指標、診断データ、最近ログオンしたユーザー、これらのユーザーがアクティブだった日時などのデータを示すレポートを、デバイスごとに参照できます。

管理の委任と柔軟な管理

Chrome Enterprise では、管理作業の委任が可能です。これにより、仕事を共有し、グループや部門の管理責任を適切な個人に持たせることができます。ロールを作成して、管理対象デバイス、ユーザー、およびアプリケーションの設定を読み書きするためのさまざまな権限を管理者に付与できます。

Chrome Enterprise では、セキュリティポリシーを柔軟に作成および適用できます。ユーザーおよびユーザーグループに関するポリシーを管理者が作成できます。この場合、該当する各ユーザーのすべてのデバイスに、同じポリシーが適用されます。または、デバイスに関するポリシーを作成できます。その場合、使用しているユーザーにかかわらず、そのポリシーが各デバイスに適用されます。

シナリオ:
会議の傍受の阻止

会社の CEO と CFO が重要な取引の交渉のため海外に出張しています。CEO と CFO の戦略会議の内容が交渉相手または出張先の国の諜報機関に傍受された場合、会社は多額の損失を被る可能性があります。幸い、Bluetooth を一時的に無効にして、Chrome OS デバイスのマイクとカメラにアクセス可能なChrome ウェブ アプリケーションとブラウザ拡張機能をブロックできます（変更を有効にするには再起動が必要な場合があります）。

管理インフラストラクチャを活用

Chrome Enterprise には独自の管理者用コンソールがありますが、これは既存の管理インフラストラクチャと統合できるように設計されています。

Active Directory および Google Cloud Identity との統合

Chrome Enterprise 管理コンソールは、Microsoft Active Directory および Google Cloud Identity と統合できます。たとえば、Active Directory に Chrome デバイスを登録できます。また、Active Directory で定義されたユーザーグループに基づいてユーザーやデバイスにChrome ポリシーを適用することも可能です。

代表的な EMM ソリューションとの連携

企業向けモバイル管理（EMM）製品は、企業でのノートパソコン、タブレット、スマートフォンなどのモバイルデバイスの登録、管理、サポートを支援します。Cisco Meraki、Citrix XenMobile、IBM MaaS360、ManageEngine Mobile Device Manager Plus、VMWare Airwatch などの EMM ソリューションにすでに投資している企業では、引き続きこれらの製品を使用して Chrome OS デバイスや他のエンドポイントを管理できます。

BeyondCorp Enterprise でゼロトラスト セキュリティを実装

勤務場所が分散化している組織では、ビジネス クリティカルなアプリケーションやサービスへのアクセスを許可する機能が必要です。しかし、これをシンプルかつ安全に実行するのは容易なことではないようです。Google の BeyondCorp Enterprise ゼロトラスト ソリューションでは、アクセス権の制御をネットワークから個々のユーザーに移すことで、コンテキストに応じたデバイスとユーザー認証情報に基づいた、企業リソースへのセキュアかつ安全なアクセスが可能になります。出社しているユーザーにも在宅勤務のユーザーにも適用されます。デバイスとユーザー認証情報を認証できない場合、そのユーザーは特権ネットワーク リソースにアクセスできません。BeyondCorp Enterprise は、Chrome OS ユーザーに提供されるアドオンです。

図 6: BeyondCorp Enterprise のコンセプトの概要

まとめ: 変革をもたらすセキュリティと運用管理

クラウドコンピューティングは、企業が従来型のエンドポイントモデルを再考するきっかけになります。クラウドファーストのアプローチによって、エンドポイントのセキュリティを大幅に強化し、エンドポイント管理を劇的にシンプルにすることができます。

Chrome デバイスは、エンドポイント上のアセットの減少、攻撃対象範囲の縮小、シンプルな高速アップデートなど、クラウドコンピューティングならではのメリットを活用しています。さらに、クラウドファーストの考え方は、革新的なセキュリティ機能と管理機能に向けた下地となります。そのような機能の例として、ハードウェアやファームウェアに組み込まれたセキュリティ機能、サンドボックスとユーザーレベルの暗号化の効果的な使用、オペレーティングシステムのシームレスな高速アップデート、セーフブラウジング、シンプルな2 要素認証、アプリケーションのキュレーション、何万ものユーザーとデバイスに対応するセキュリティポリシーと運用ポリシーのシンプルな管理などが挙げられます。

その結果、次のようなコンピューティング環境が実現します。

1. 組み込みのセキュリティによる事前対応
2. 従来のエンドポイントと比べてはるかに簡単な管理
3. 既存のインフラストラクチャと統合可能

Chrome OS デバイスのセキュリティに関する詳細をご確認ください。

https://chromeenterprise.google/intl/ja_jp/security/