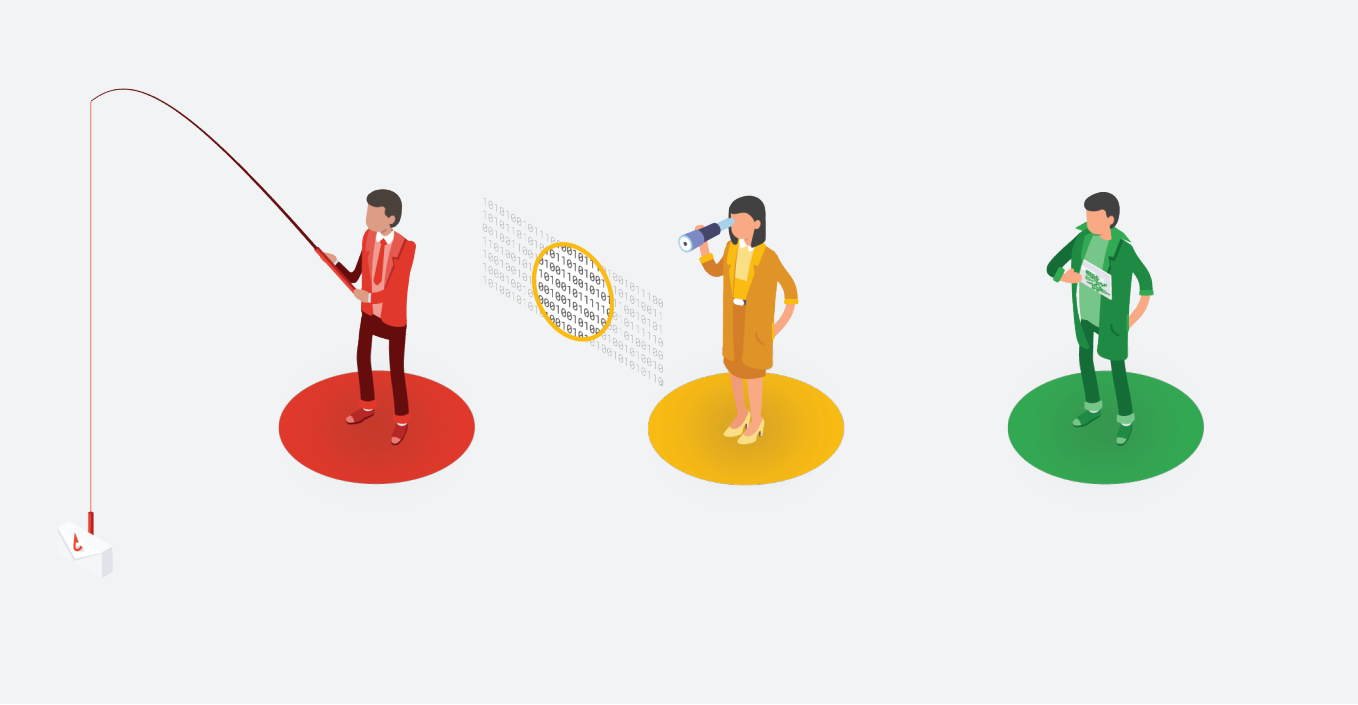
クラウド化による セキュアな エンドポイントの 構築

データ保護とシンプルな IT 管理を実現する Chrome Enterprise の革新的なアプローチ



chrome enterprise

chrome enterprise

目次

クラウド化に向けた準備

複雑なエンドポイントのセキュリティ

エンドポイントの保護は、サイバーセキュリティや IT 運用の専門家にとって最も大きな課題の 1 つです。専門家は「対応が困難な問題である一方で、攻撃手法は進化し続けている」という点を指摘しています。

従来のエンドポイントは複雑で、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 パッチが適用されていないバージョン、未承認のソフトウェア パッケージなど）が存在する
2. 悪意のあるウェブサイトへのアクセス、提供元が不明なアプリのダウンロード、必要なソフトウェア アップデートの適用漏れにより攻撃を受けやすい
3. 知的財産、個人情報、ユーザーの認証情報がローカル ディスクに大量に保存されている
4. ソフトウェアが、その利便性向上のためにプロセス間通信を許容していることが原因で、1 つのソフトウェア モジュールに不正侵入されると、システム全体または会社のネットワーク全体が攻撃を受ける可能性がある

このように、従来のエンドポイント管理では課題が山積しており、サイバーセキュリティ チームはエンドポイントの監視、脆弱性の特定、不正侵入の検出に多大な労力やコストを費やさなければならないという状況です。
運用担当チームは、多数の分散デバイスに一貫したイメージを適用し、それらのファームウェア、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を適用するなどの作業に多くの時間を費やしています。

さらに悪いことに、自宅や出張先で仕事をするユーザーが増えているため、"社内ネットワークからのアクセスだから安全である" という認識のもとに設計された、従来のセキュリティツールや考え方は、効果的ではなくなっています。

セキュリティ モデルの再考

テレワークを行うユーザーが増え、従来のセキュリティ モデルが効果的ではなくなった今こそ、このような複雑な管理から脱却し、エンドポイントのセキュリティと管理の手法を大きく改善する絶好の機会です。

まず、IT 部門はクラウドベース アーキテクチャ固有のメリットをセキュリティや運用に活用できます。情報アセットをクラウドに保存して共有すると、脆弱なエンドポイントに保存する場合と比べて簡単に監視できます。中核となるクラウド プラットフォームでソフトウェアのトラッキングとアップデートを実行するほうが、多数のリモート デバイス上で個別に管理するよりはるかに簡単です。

また、テクノロジー ベンダーは「クラウド ネイティブ」なセキュリティについて根本から見直しており、エンドポイントのセキュリティの強化と管理の簡素化を実現するための優れた新機能を導入しています。

このホワイト ペーパーでは、Google がクラウド コンピューティング固有のメリットを活用し、5 層（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）の革新的なマルチレイヤ セキュリティ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設計したのかを詳細に説明しています。

次の各機能の例を紹介：

1. 不正なソフトウェア、フィッシング、影響元不明ファイルのダウンロード、APT 攻撃など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、デバイスの紛失や盗難が発生した場合のデバイスのリモート停止やリモート ワイプ、エンドポイントに関するセキュリティー ポリシーの管理などの運用業務を大幅に簡素化する Chrome Enterprise
3. Microsoft Active Directory と業界をリードするサードパーティの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

Chrome Enterprise を用いて
エンドポイントをクラウド化することで得られるメリット

エンドポイントに保存する機密情報の量を削減

クラウド化で得られるメリットの1つは、ほとんどの機密情報がエンドポイントではなく、クラウドに保存されることです。ノートパソコンの紛失や盗難が発生した場合に、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 コードの漏洩について心配する必要はありません。デバイスが不正に使用された場合でも、顧客のクレジット カード番号や従業員の医療情報、会社の財務システムにアクセスするためのパスワードなどが悪意のある攻撃者に見つかる可能性は極めて低くなります。

攻撃対象範囲の限定

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ははるかに少なくなります。エンドポイント 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、従来のエンドポイントのようにユーティリティ、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ると、攻撃対象となる脆弱性はかなり減少します。管理者がエンドポイントにインストール可能なソフトウェアを限定することで、ソフトウェアの管理・保護が必要な範囲を狭めることができます。

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、国内または国外の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雑な定常業務を延々と繰り返すことになります。また、脆弱性に関する通知を受け取ったり、新しい攻撃手法が明らかになったりするたびに、サイバーセキュリティや運用の担当者は多数のエンドポイントに急いでパッチを適用したり、管理したりする必要があります。対応が遅れるほど、攻撃的なハッカーに侵入さ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、導入や管理を 1 か所で行うことができるため、エンドポイントを常に最新の状態にするために必要な作業が大幅に減ります。

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には、革新的なセキュリティ機能と管理機能が多数備わっています。このような機能は Google の Chrome OS や 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 デバイスに搭載されています。Chromebook は、Acer、ASUS、Dell、Google、HP、Lenovo などの業界をリードするさまざまなテクノロジー企業で販売されています。

Titan C セキュリティ チップ

すべての Chromebook には、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。このモジュールには、専用のチップにフラッシュ メモリ、ROM、RAM、不正使用検出機能が搭載されているため、ここに保存されている情報を抜き出したり、改ざんすることは極めて困難です。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いるため、侵入者はオペレーティング システムにアクセスできないようになっています。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攻撃から保護します。

ユーザーデータの暗号化と分離

すべての Chromebook は、ユーザーのデータと設定をデフォルトで暗号化します。ユーザー（または他の誰か）がこの暗号化を無効にすることはできません。

また、ユーザーのデータと設定は各ユーザー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、通常はユーザーの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必要になります。このため、悪意のある攻撃者がユーザーのデータを読み取ることは極めて困難です。攻撃者が Chromebook とユーザーのパスコードを入手している場合でも、他のユーザーは別の暗号化鍵で暗号化が行われており、その暗号化鍵は Titan C セキュリティ チップに保存されているため、他のユーザーのデータを複合して読み取ることはできません。

ユーザーデータの分離には、他にもメリットがあります。それは、同僚や家族と安全にデバイスを共有したり、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などの最新の手法を安全に導入したりできることです。

シナリオ：社内の関係者による侵入の防止

別々の曜日に出勤している契約社員の佐藤さん、吉田さんは 1 台の Chromebook を共有しています。実は、佐藤さんはアマチュアのハッカーで、吉田さんが担当しているサーバーへアクセスしようと企んでいます。彼は貴重なアルゴリズムと著作権のあるソフトウェアがそのサーバーに保存されていることを知っています。佐藤さんは吉田さんが使用している Chromebook にログインして仕事をしますが、Titan C セキュリティ チップが佐藤さんと吉田さんのデータを別の暗号化鍵で暗号化しているため、吉田さんの認証情報、ネットワーク接続情報、その他のデータや設定にアクセスすることはできません。従い、Chromebook を共有していても、吉田さんの担当しているサーバーにあるデータは安全です。

デバイスの種類をまたいで、一貫したセキュリティ ポリシーを適用

Chromebook の OEM 各社は、品質、パフォーマンス、セキュリティに関する Google の仕様を満たす製品を作ることに同意しています。Chrome ブランドのデバイスは、Google によるハードウェア設計の確認と承認を経てから出荷されます。また、メーカー各社は他のすべての Chromebook で稼働しているものと同じファームウェア、Chrome OS、Chrome ブラウザを搭載することにも同意しています（図 1）。

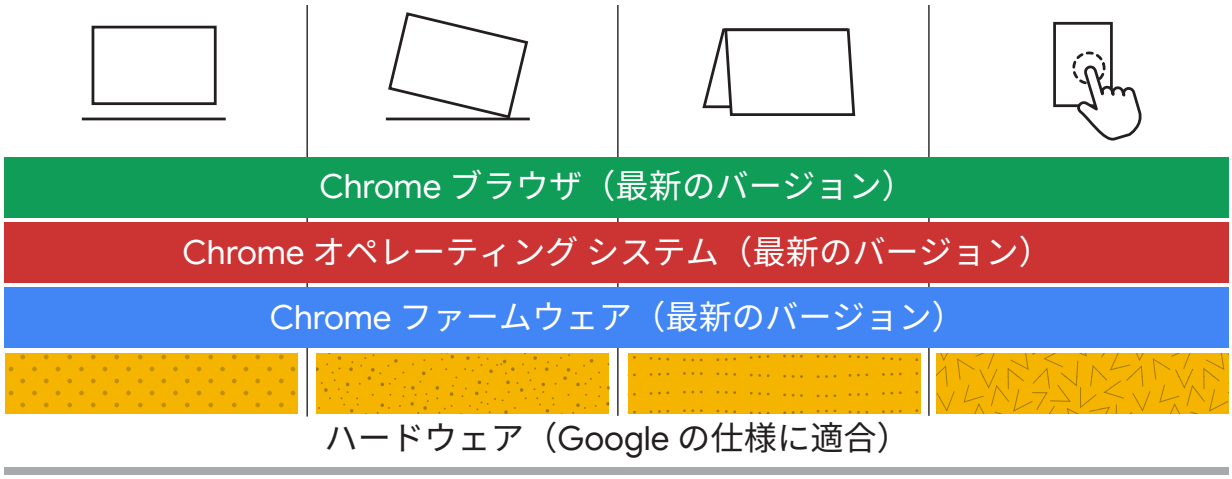


図 1：一貫性のあるユーザー エクスペリエンスと、エンドポイント管理の簡素化のために、すべての Chromebook に同じバージョンのファームウェア、 Chrome オペレーティング システム、Chrome ブラウザが搭載されている

ユーザーにとっても管理者にとっても、この一貫性は大きなメリットです。ユーザーはすべての Chromebook を同じ操作で快適に使用できるため、セキュリティ チームと運用チームは運用環境を正規化することができます。
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がなく、互換性のないソフトウェア リリースから生じる脆弱性についても心配する必要がありません。
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。

セキュリティに関する適切な判断

サイバー セキュリティについてあまり詳しくない、またはパソコンの使用にさえ抵抗があるユーザーの代わりに、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の設定を確認します。先ほど触れましたが、すべてのユーザーデータはデフォルトで暗号化されます。詳しい例についてはこのドキュメントで後ほど説明します。

ファームウェア：自動で何重にも行われる確認

「持続性」は先進的な標的型攻撃の重要な要素です。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エンドポイントに持続的に存在することができるようになっています。

しかし、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使用していた持続的な攻撃手法の多くは通用しません。たとえば、ユーザーがインストールできる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いなら、それらを使って再起動後にも悪意のあるコードを維持することはできません。

ただし、これまでと同様に、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、ブラウザにコードの挿入を試みることは可能です。

Google はこれを防ぐために「確認済みの起動」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、ブラウザのすべてのコードが Google 提供のソフトウェアであり、改ざんされたものではないことをシステムが自動的に確認します。

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加藤さんは、Chromebook にアクセスしてスーパーユーザー権限を取得しようと画策しています。加藤さんはルート パーティションを読み書き可能に変更し、直接再マウントしてから、カーネル モジュールとしてルートキットを追加しました。しかし、次の再起動時に、Google の「確認済みの起動」のプロセスにより、ルート パーティションの一部の署名が、Google が想定していた署名と一致しないことが明らかになりました。この場合、起動プロセスは停止し、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デバイスが自動的に再起動されます。再起動後、加藤さんはルートキットを使用してデバイスを制御することができませんでした。

Chromebook は起動するときに、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が Google で承認済みのイメージと完全に一致することを確認します（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確認します）。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確認します。その後、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確認します。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用の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)。

確認済みの起動プロセスにより、システムは危険なタイプの攻撃から自動的に保護され、運用担当者は、不正使用されたファームウェアやファイルを修復するという面倒な作業をする必要がなくなります。

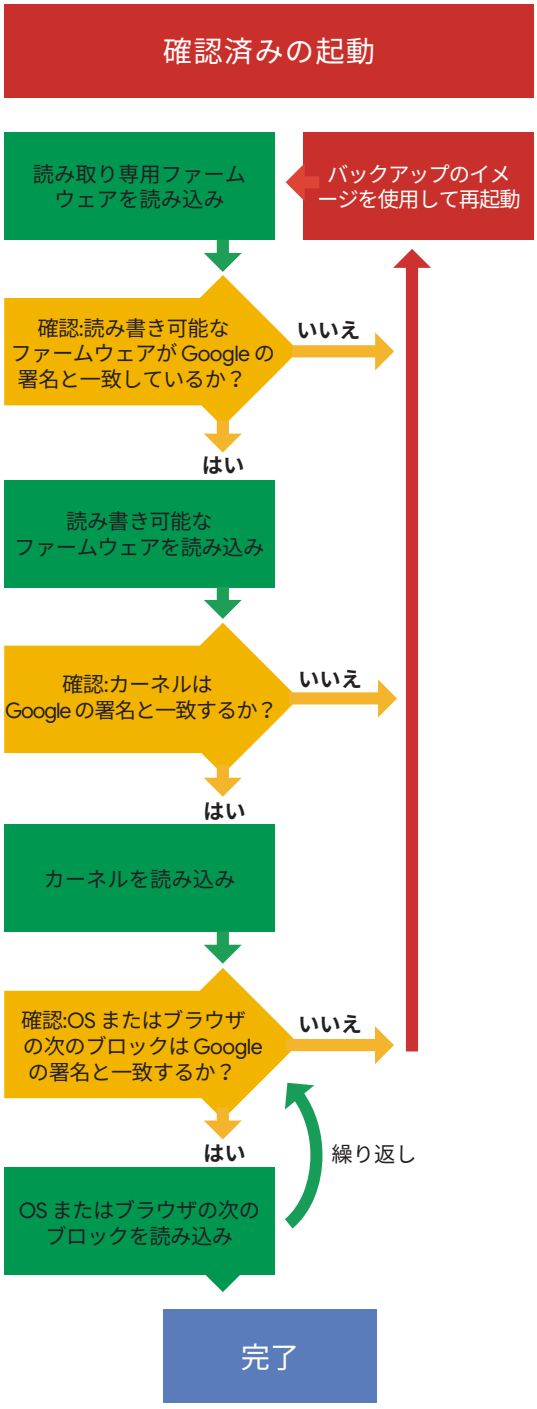


図 2：確認済みの起動プロセスで、
ファームウェア、オペレーティング システム、
ブラウザが不正改造されていないことが確認される

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、アプリケーションを保護し、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煩わしさを排除するセキュリティ機能があります。

権限の分離とプロセスのサンドボックス化

サイバー攻撃の種類によっては、不正に侵入したウェブサイトやクラウドベースのアプリケーションを使用して、エンドポイントのソフトウェア コンポーネントをコントロールするものがあります。

Chrome OS を用いたクラウド化の管理環境では、不正侵入される可能性があるオペレーティング システムのコンポーネント、ユーティリティ、ドライバ、その他のソフトウェアの数が従来の環境と比べてはるかに少なくなります。さらに、Chrome OS のアーキテクチャには、攻撃者が制御するアプリケーションから他のソフトウェアへの影響を防ぐための機能があります。

たとえば、Chrome OS はプロセスのサンドボックス化を利用します。実行中のプロセス間に厳格な境界が適用されるため、アプリケーションは互いに通信できません。通信できる場合でも、厳密に制限された条件下で行われ、各実行プロセスは本当に必要な権限のみを使用できます。セキュリティを重視する組織が機密情報へのアクセスを「知る必要がある」人だけに限定するように、Chrome OS はプロセス間の通信を本当に「使用する必要がある」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

坂井さんは休憩時間に Chromebook 画面用の新しい壁紙を探していました。あいにく、彼がアクセスしたある人気ゲームの解説サイトは、サイバー犯罪者が制御する「水飲み場型攻撃」サイトでした。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 Chromebook 上のすべてのデータとファイルを暗号化しようとしましたが、Chrome の強力なサンドボックス化の仕組みにより、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。「このファイルを実行できません」という通知が表示され、ランサムウェア攻撃はユーザーデータにアクセスする前に停止されました。

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大変な仕事です。従来のエンドポイントでのオペレーティング システムのアップデートは、エンドユーザーの仕事の妨げとなります。数分あるいは 1 時間以上にわたってエンドポイントを使えなくなることがあるため、生産性の低下という実質的な損害が発生し、ユーザーのイライラと IT 部門に対する不満につながります。

さらに悪いことに、ユーザーがアップデートを拒否することは多々あり、その場合はデバイスが攻撃を受けやすい状態になります。

Google はこのような課題に対応する革新的なソリューションを提供します。各デバイスには、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 システムが格納されています。現在のオペレーティングシステムを使用してシステムを稼働している間に、バックグラウンドで透過的に最新のバージョンがダウンロードされ、保存されます。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、最新のオペレーティング システムが数秒で読み込まれます（図 3）。

この仕組みのおかげで、前述の確認済みの起動プロセスも簡素化されています。システムの起動中に、稼働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を検出すると、デバイスにある以前の Google が検証済みのクリーンなバージョンが、即座に使用できる状態になります。

Chromebook 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。Google は約 6 週間ごとに Chrome OS をアップデートしますが、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 システムの新たな脆弱性を検出した場合は、セキュリティ パッチを極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。

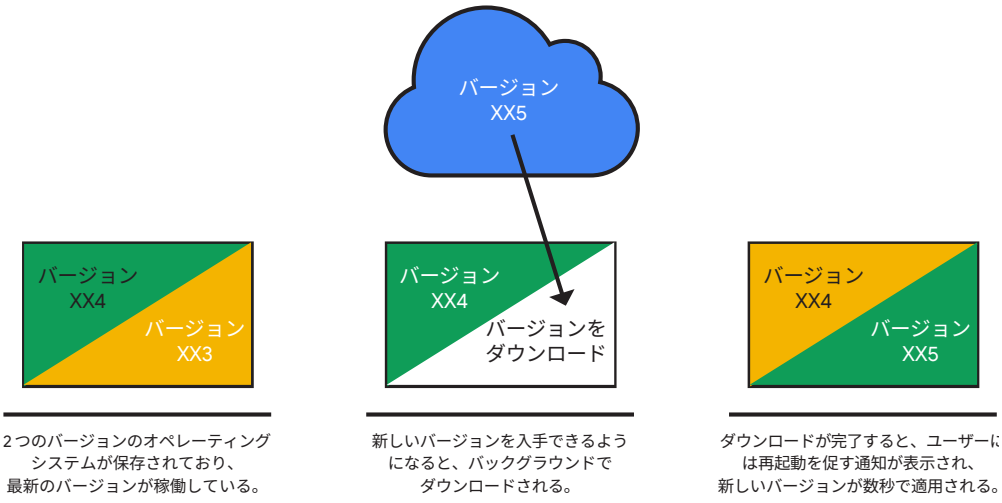


図 3: オペレーティング システムの新しいバージョンはバックグラウンドでダウンロードされるため、ユーザーの仕事の妨げになることはない

ブラウザ：サイト分離、セーフ ブラウジング、2 要素認証

Chromebook では、ウェブでのすべてのやり取りが Chrome ブラウザを介して行われます。Chrome ブラウザは Google の業界をリードするブラウザであり、ユーザーはこのブラウザに組み込まれている革新的なセキュリティ機能を利用できます。

タブのサンドボックス化とサイト分離

Chrome OS のところで説明したサンドボックス化の概念は、Chrome ブラウザにも適用されています。ブラウザで開かれているすべてのタブにそれぞれのサンドボックスがあるため、1 つのタブで行われた攻撃が他のタブに影響を及ぼす可能性は極めて低くなります。

この「分離」の原則は、サイト分離によってさらに強固なものになります。1 つのタブ内で複数のウェブサイトにアクセスするケースは多数あります。たとえば、あるサイトで HTML ウェブページを読んでいると、2 つ目のサイトから画像がダウンロードされ、3 つ目のサイトから動画がダウンロードされ、4 つ目のサイトからスクリプトがダウンロードされることがあります。サイト分離によって、これらの各サイトのプロセスは互いに分離されます（図 4）。Chrome ブラウザでは、すべてのサイトを分離するのか、選択したサイトのみを分離するのかを管理者が選択できます。

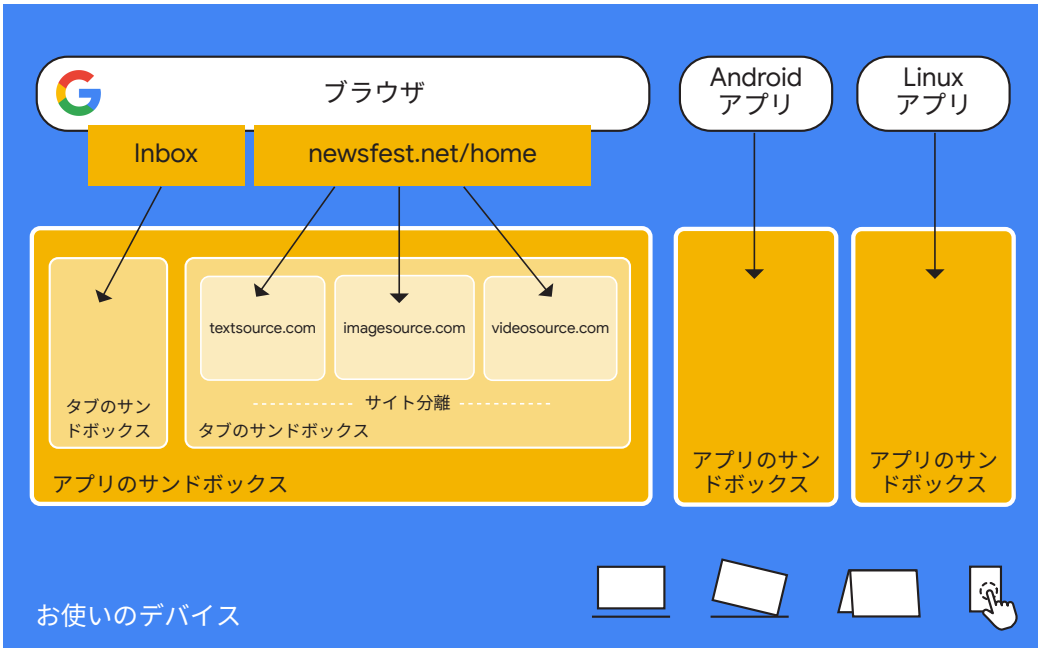


図 4：Chrome OS と Chrome ブラウザでは、複数のレベル（サイト、タブ、アプリケーション）で分離を行う

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）のような脅威は、悪意のあるウェブサイトからメモリ内にある別のウェブサイトのプロセスやデータにアクセスしようとしますが、サイト分離機能を使用することで、このような脅威から保護できます。

セーフ ブラウジング

企業にとって最も脅威となっているのは、攻撃者に乗っ取られたウェブサイトからのマルウェア攻撃やフィッシング攻撃に関連するものです。

Google のセーフ ブラウジング機能は、ユーザーがマルウェアやフィッシング コンテンツを含むウェブサイトにアクセスしようとした場合、または不審なファイルをダウンロードしようとした場合に警告を表示します。この機能は、安全ではないウェブサイトを毎日多数検出し、 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としています。

セーフ ブラウジング機能のメッセージは、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の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。

シナリオ：
フィッシング攻撃の回避

小田さんは小規模な製造会社の最高財務責任者です。CEO から受信したメールには、すぐに中国の新しいサプライヤに 200 万円を送金し、枯渇している部品の供給を確保するようにとの指示がありました。CEO はベンダーを確保するために中国に出張中だったので、もっともらしい内容のメールです。
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、Chrome ブラウザにより、偽のサイトであることを示す警告が表示され、偽のサイトであることを示す警告が表示され、[安全なページに戻る] をクリックするよう促されました。Google のセーフブラウジング機能のおかげで、小田さん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。

セキュリティ キーと 2 要素認証

2 要素認証（2 段階認証）を使用すると、ユーザーの認証情報が漏洩した場合でもシステムとデータを保護できます。2 要素認証が義務付けられているユーザーがログインを完了するには、、ユーザーが記憶している情報（通常はパスワード）と、もう 1 つの情報（多くの場合、認証キーやスマートフォンに送信されたコード）を入力する必要があります。

Google は効果的な 2 要素認証を実装するための迅速かつ簡単な方法を提供しています。ユーザーは自分の 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 つ目の認証方法のオプションを選択するだけです。このオプションには、テキストでのコードの受信、スマートフォンに表示される通知をタップ、USBポート経由で Chromebook 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、ユーザーが信頼済みとして指定したデバイスからのログインでは、 2 つ目の認証方法がなくてもログインできます。

アプリケーション：
マルウェアの検出、許可リスト、ブロックリスト

Chromebook では、Android アプリ、オフィスの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: 迅速に読み込まれ、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、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。

Chrome ウェブストアにある Google 提供のアプリケーションや、Google Play ストアにある Android アプリの利用を組織が許可している場合、IT 管理者はセキュリティの強化や管理の簡素化に役立つ多数の機能を利用できます。

クラウド上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 プロテクトはモバイル デバイスを脅威から保護するサービスです。世界で最も多くのデバイスに導入されており、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 アプリに対して厳密なセキュリティ テストを実施してから Google Play ストアでの公開を許可しています。 Google のポリシーに違反するアプリや開発者は、Play ストアに登録できません。

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確認しています。マルウェアが見つかったアプリは、 Google Play ストアでただちに停止されるだけでなく、そのアプリをダウンロードし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 ストアを使用したアプリの許可

脆弱性を含むアプリケーションや、悪意のあるユーザーが開発したアプリケーションのダウンロードをきっかけに、データ侵害を受けるケースが多数あります。

IT 管理者は過去数十年もの間、承認済みのアプリケーションのみをインストールするようにユーザーに伝えたり、承認済みのアプリケーションだけを実行できるようにエンドポイントをロックダウンしたりして、ユーザーが好き勝手にアプリをダウンロードしないように努めてきました。承認済みのアプリケーションの数は

シナリオ:シャドー IT の阻止

伊藤さんは、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した。「オンライン コラボレーション ツール 20 選」というタイトルの記事をオンラインで見つけたとき、ここには企業向けのセキュリティ機能と管理機能がほとんど含まれていないことに気づきませんでした。幸い、長い時間をかけて 20 種類のアプリをすべて試す前に、自社の managed Google Play ストアを確認し、2 種類のチーム コラボレーション アプリ（Slack と Google Chat）が承認されていることを発見しました。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、会社の他のすべてのグループとこれらのアプリを使用してコラボレーションできるようになっていました。

必然的に少なすぎるため、ビジネス アプリケーションに対するユーザー全員のニーズを満たすことができないという課題がありました。個人用アプリケーションやエンターテイメント アプリケーションに対する要望も満たすことができなかったため、前者のアプローチでは効果がありませんでした。また、従来のエンドポイントをロックダウンするテクノロジーは実装が難しく、ユーザーからの抵抗も大きかったため、後者のアプローチもうまくいきませんでした。

セキュリティ チームと運用チームはウェブベースのテクノロジーを利用することで、ユーザーを落胆させたり困らせたりせずに、未承認のアプリケーションの使用を阻止できます。

Google Play ストアは、仕事効率化、コミュニケーションやコラボレーション、ビジネス プロセスの管理、ニュース、エンターテイメント、ゲームなど、何千種類も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、さまざまな種類の多数のアプリケーションを選択できます。たとえば、仕事効率化アプリやコラボレーション アプリを従業員に多数提供する一方で、ゲームアプリやソーシャル メディア アプリの数を制限することができます（図 5）。

必要に応じて、managed Google Play ストアを活用してアプリの許可・不許可を簡単に実装できます。アプリの許可を行うと、組織内の全員に同じ仕事効率化ツールとコラボレーション ツールの使用を必須にすると同時に、ユーザーは他のアプリから適切なものを選択して使用することができます。

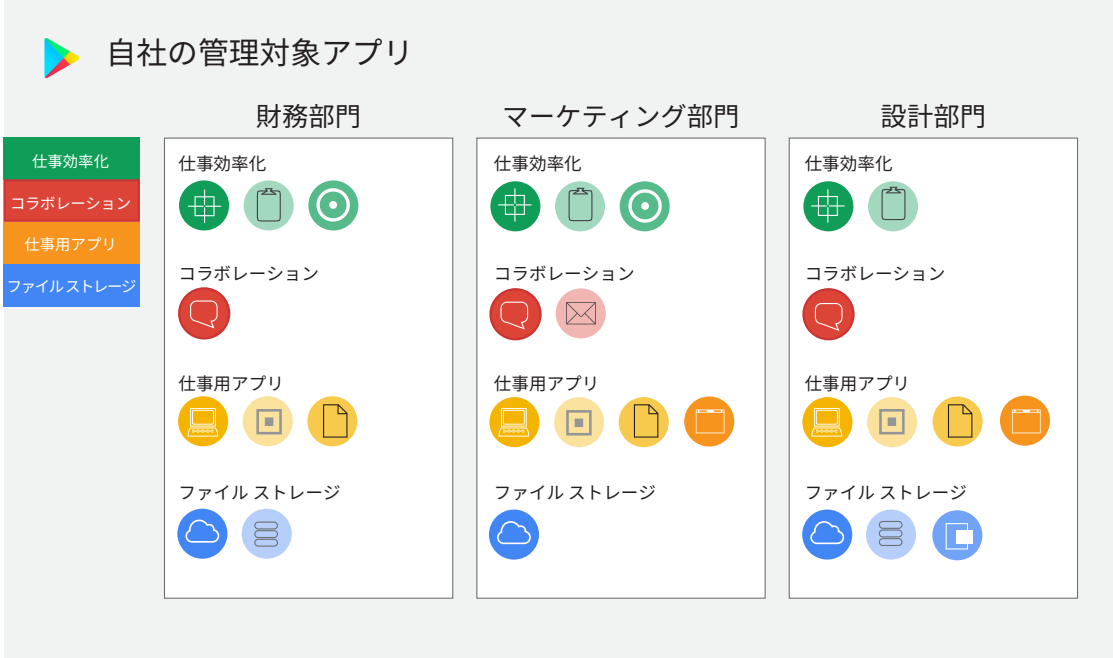


図 5：managed Google Play ストアを使用すると、企業内の各グループ用に選択された承認済みアプリケーション リストにアクセスできる

Chrome Enterprise を使用した一元管理

セキュリティ チームと運用チームは Chrome Enterprise を使用して、Chromebook に関するポリシー、Chrome OS を搭載した他のエンドポイントに関するポリシー、Windows、Mac、Linux システムに搭載されている Chrome ブラウザに関するポリシーを一元管理できます。Chrome Enterprise のライセンスには、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企業が対応する際に役立ちます。

Chrome Enterprise の選択済みポリシーの概要

管理者は Chrome Enterprise を使用することで、セキュリティと設定に関する 300 種類以上のポリシーを設定してエンドポイントに適用できます。管理対象の Chrome デバイスに関する主なセキュリティ機能には次のものがあります。

デバイスのプロビジョニング（登録）とデプロビジョニング（登録解除）：デバイスをプロビジョニング（登録）すると、ユーザーの組織に合わせて定義された Chrome Enterprise のポリシーに沿って、デバイスを管理して保護できます。管理者は自分でデバイスを登録することも、ユーザーにデバイスの登録を許可することもできます。管理者がデバイスをデプロビジョニング（登録解除）すると、ポリシーが無効になり、そのデバイスから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の無効化：デバイスの紛失や盗難が発生した場合、それらのデバイスをリモートで無効にできます。また、リモートでユーザーデータを端末から削除することもできます。

ログイン可能なユーザーの制限：管理者は、ユーザーが匿名（ゲスト ブラウジング）でデバイスにログインするのを禁止したり、個人用の Google アカウント（例 @gmail.com アカウント）を用いたログインを禁止できます。また、アクセスを 1 人または少数の指定したユーザーに制限することも可能です。

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全て削除）：管理者はデバイスを管理対象ゲストセッションモードに設定できます。管理対象ゲストセッションモードでは、ユーザーがログアウトしたときにデータと設定（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）がデバイス上から完全に削除されます。共有デバイス、キオスク、または一時的に利用するユーザー用のデバイスでは、管理対象ゲストセッショ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強制インストール：管理者は、ユーザーが 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）をインストールできないようにブロックしたり、特定のアプリや拡張機能をインストールできないようにブロックしたりできます。また、インストールできるアプリや拡張機能を特定の URL にあるものだけに制限したり、特定のアプリや拡張機能を自動インストールしたりすることも可能です（アプリや拡張機能が自動インストールされた場合には、ユーザー側からは無効化や削除ができないように設定されます）。

アプリケーションが要求する権限に基づきアプリケーションを許可・ブロック：Chrome 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。IT 管理者は、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上書き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ことで、IT 部門はリスクを低減できる一方、ユーザー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ます。

Bluetooth や位置情報の無効化：デバイスで Bluetooth と位置情報の追跡機能を無効にできます。

外部ストレージ デバイスの使用の制限：USB 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したり、読み取り専用モードのみでの使用を許可したりできます。

リモート アクセスとシングル サインオンの管理：管理者はリモート 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設定できるので、ユーザーはセキュリティと利便性のバランスを保ちつつ、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トラッキング：Google 管理コンソール上には、オペレーティング システムとファームウェアのバージョン、CPU と RAM の使用状況に関する統計、接続されているストレージ デバイス、使用状況を示す指標、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デバイスごとに示すレポートがあります。

シナリオ：会議の傍受の防止

あなたの会社の CEO と CFO は重要な取引について交渉するために海外に出張する予定です。CEO と CFO の戦略会議の内容が交渉相手または開催国の諜報機関に傍受された場合、あなたの会社は多額の損失を負う可能性があります。幸い、Bluetooth を一時的に無効にして、Chromebook 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るので、安心して会議を進めることができます（変更を有効にするために再起動を求める必要があるかもしれません）。

管理の委任と柔軟な管理

Chrome Enterprise では、管理作業を委任して仕事を共有し、グループや部門の管理責任を適切な人に与えることができます。ロールを作成すると、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取る、または書き込むためのさまざまな権限をまとめて管理者に付与できます。

Chrome Enterprise では、会社のポリシーにあわせて、柔軟にセキュリティ ポリシーを作成して適用できます。ユーザーおよびユーザー グループに関するポリシーを作成すると、デバイスに関係なく、各ユーザーに同じポリシーが適用されます。また、デバイスに関するポリシーを作成すると、ユーザーに関係なく、各デバイスに同じポリシーが適用されます。

管理インフラストラクチャの活用

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も連携するように設計されています。

Active Directory および Google Cloud Identity との連携

Chrome Enterprise 管理コンソールは、Microsoft Active Directory および Google Cloud Identity と連携します。たとえば、 Active Directory に Chrome デバイスを登録したり、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 ポリシーを適用したりできます。

業界をリードする 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、企業がノートパソコン、タブレット、スマートフォンなどのモバイル デバイスを登録、管理、サポートする際に役立ちます。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は、引き続きこれらの製品を使用して Chromebook や他のエンドポイントを単一のコンソールから管理できます。

まとめ：セキュリティと運用管理の劇的な変化

エンドポイント管理をクラウド化することは、従来のエンドポイント セキュリティ モデルを再考する絶好の機会となります。クラウド化のアプローチでは、エンドポイントのセキュリティを大幅に強化し、管理を劇的に簡素化することができます。

Chrome デバイスは、エンドポイントに保存される機密情報の低減、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固有のメリットを活用しています。さらに、クラウド中心の考え方から生まれた革新的なセキュリティ機能と管理機能を利用できます。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、サンドボックスの効果的な使用とユーザー プロファイルごとのハードウェア レベルの暗号化、オペレーティング システムの高速でシームレスなアップデート、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許可と禁止、何万ものユーザーとデバイスに対応可能なセキュリティ ポリシーと運用ポリシーのシンプルな管理など、さまざまな機能があります。

以上のことから、 Chrome Enterprise を導入することで、次のような IT 環境を整備可能となります：

1. つぎはぎではない、一貫したセキュリティ ポリシーの適用
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の連携

詳細については、
Chrome Enterprise のセキュリティをご覧ください。

https://cloud.google.com/chrome-enterprise/security/