chromeOS

ChromeOS セキュリティ ガイド

ChromeOS デバイスは、これまでにランサムウェア攻撃が成功したという報告は一度もありません。
また、ウイルス攻撃の成功例も報告されていません。[*1]

本書では、不正なソフトウェアから自社を守る、ChromeOS のセキュリティ機能を徹底解説します。

chromeOS

ChromeOSは、ランサムウェアの被害報告数ゼロ[*1]

ランサムウェアから自社を守る
ChromeOSのセキュリティ機能を徹底解説

P. 3 ~

ChromeOS デバイスは、これまでに
ランサムウェア攻撃が成功したという報告は一度もありません。
また、ウイルス攻撃の成功例も確認されていません。[*2]

P. 8 ~

データの安全性に優れたChromebookは、
漏洩リスクを大幅に低減するためのさまざまな機能を搭載。

P. 11 ~

ITに詳しくない方でも簡単に安全に使えます。

ChromeOSデバイスは、これまでに
ランサムウェア攻撃が成功したという
報告は一度もありません。
また、ウイルス攻撃の成功例も確認されていません。[*3]

信頼できない
実行ファイルを
すべてブロック[*5]

ランサムウェアや
多くのマルウェアを
実行できない
仕組みを採用[*5]

近年、パソコンがランサムウェアに感染してしまい業務が停止した、また、重要な情報が漏洩してしまったというニュースを目にしたことがある方は多いと思います。ランサムウェアなどのマルウェア（悪意のあるアプリ）の多くは、端末上で「実行」されることによって悪さをします。これらのマルウェアは、主にEメールの添付ファイルなど、主にインターネットを通じて秘密裏に端末に挿入され、ユーザーの「うっかり」や既に「実行」されているOS、ドライバ、アプリといったソフトウェアの脆弱性を利用して「実行」されます。

マルウェアは一度実行されると、瞬く間に自己複製を行い、さらに被害を拡大していきます。旧来のマルウェアはシステムをダウンさせる事などが主目的でしたが、現在ではランサムウェア攻撃は悪意のあるビジネスとして成り立っており、報告件数も増加の一途をたどっています。

ChromeOSの開発チームは、「そもそも、信頼できないアプリやファイルに実行権限を付与しなければランサムウェアなどのマルウェアの被害に遭うことはなくなるのではないか」と考えました。ChromeOSの特長は、すべてのアプリケーションがWebアプリである点です。つまりそれはリンクであり、URLでしかないのです。ChromeOSには、基盤となるOSやシステムリソースへの広範なアクセス権限を必要とする従来のインストール型のアプリは存在しないのです。[*26*27]

ChromeOSでは全てのアプリがWebアプリであるため、全てのアプリはブラウザのサンドボックス内で動作します。ChromeOSはデフォルトで、信頼できない実行ファイルをすべてブロックします。実行ファイルに隠されている不正なコードは、ChromeOSでは実行できません。[*5*27]

この設計思想により、ChromeOSのセキュリティは本質的に強固となり、急増するセキュリティ脅威に対する強力な盾となっています。

確認付きブートで初期化やOSの改ざんを防止[*6]

読み取り専用のOS領域でシステムはいつも安全[*7]

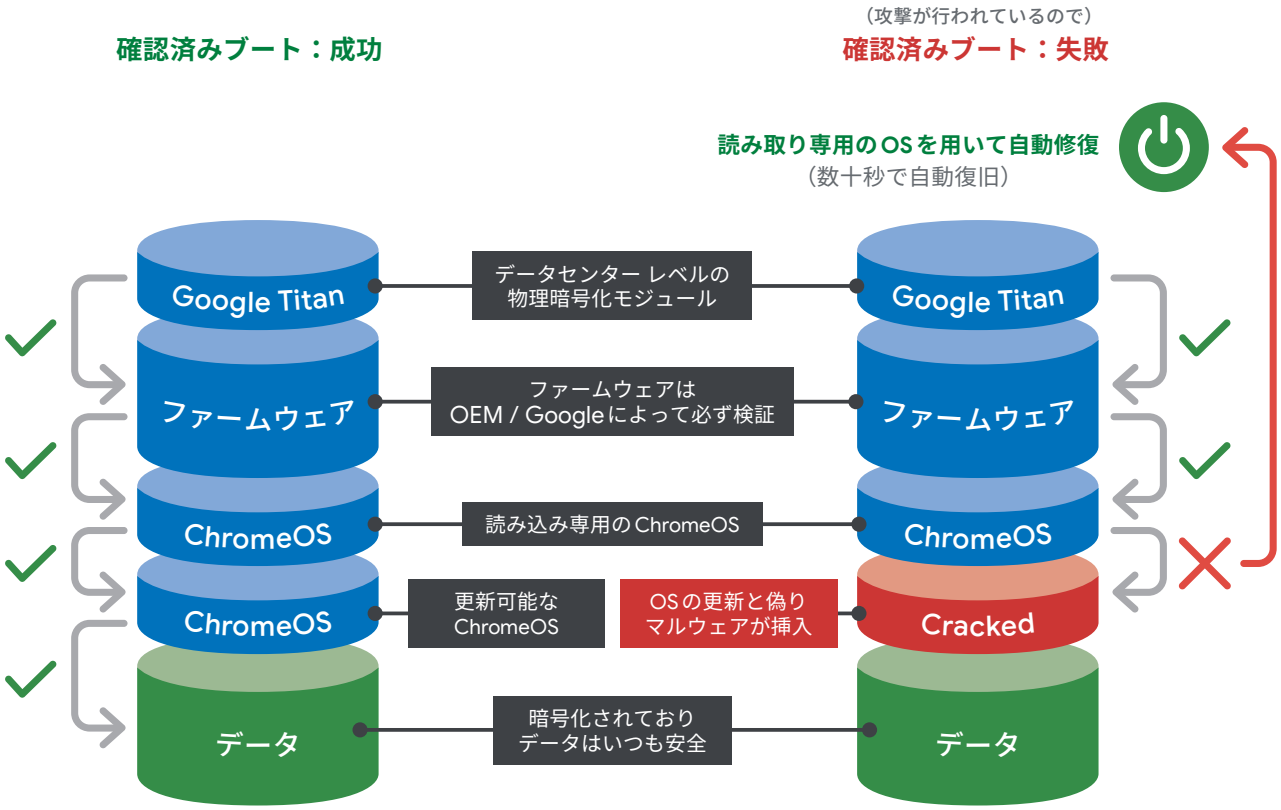
ChromeOSの領域は読み取り専用となっており、ユーザーやアプリはChromeOSのシステム領域に書き込むことはできません。

Chromebookは「Titan C（タイタンシー）」と呼ばれるGoogleのセキュリティ チップを搭載しています。これは、Googleのデータセンターを保護するために用いられているTitanシリーズのセキュリティ チップであり、全てのChromebookは製造時点でTitan Cが有効になっています。

ChromeOSは、自身が破壊される可能性があることを知っているため、自分自身すら信用していません。[*26] 電源投入時に必ず、Titan Cによる「確認付きブート」を行い、ファームウェアや自分自身（ChromeOS）の改ざんを検出し、OSが起動される前に起こりうる攻撃を防いでいます。

他にも、Titan Cは、ユーザーがデバイスを開発者モードにできないようにする機能など、Google管理コンソールで設定されたポリシーが管理対象のChromebookに適用されることを確実にします。Titan Cは端末初期化後にChromeOSデバイスが必ず（以前登録されていた）組織の管理コンソールに再登録されることを保証します。これにより端末の紛失リスクを低減します。

確認済みブート



OSは常に２つ存在

システムがセルフチェック

自動的にバックアップされたOSに切り替え・修復

自動的に新しいコピーをダウンロード

サンドボックスと多層防御で システムとデータを強力に保護[*8]

すべてのアプリは常にサンドボックス内で動作[*9]

ChromeOSにおけるセキュリティの核心は、一貫した多層防御と、全アプリケーションのサンドボックス内での運用です。

多層防御は、ファームウェア(UEFI・BIOS)、オペレーティングシステム(OS)、アプリケーションおよびブラウザ、そしてデータの各層を連携させて、システムと企業データを保護する、ChromeOSの革新的なセキュリティ戦略です。一般的には、ファームウェアレベルの保護は各OEMによって開発・実装されていますが、ChromeOSでは、Googleが承認したファームウェアのみが動作[*10]するようになっています。また、承認済みのファームウェアは、Googleが配布したままの(改変されていない)ChromeOSのみを起動します。このように、多層防御が組み込まれているChromeOSでは複数の層が連携して高いセキュリティをデフォルトで提供します。

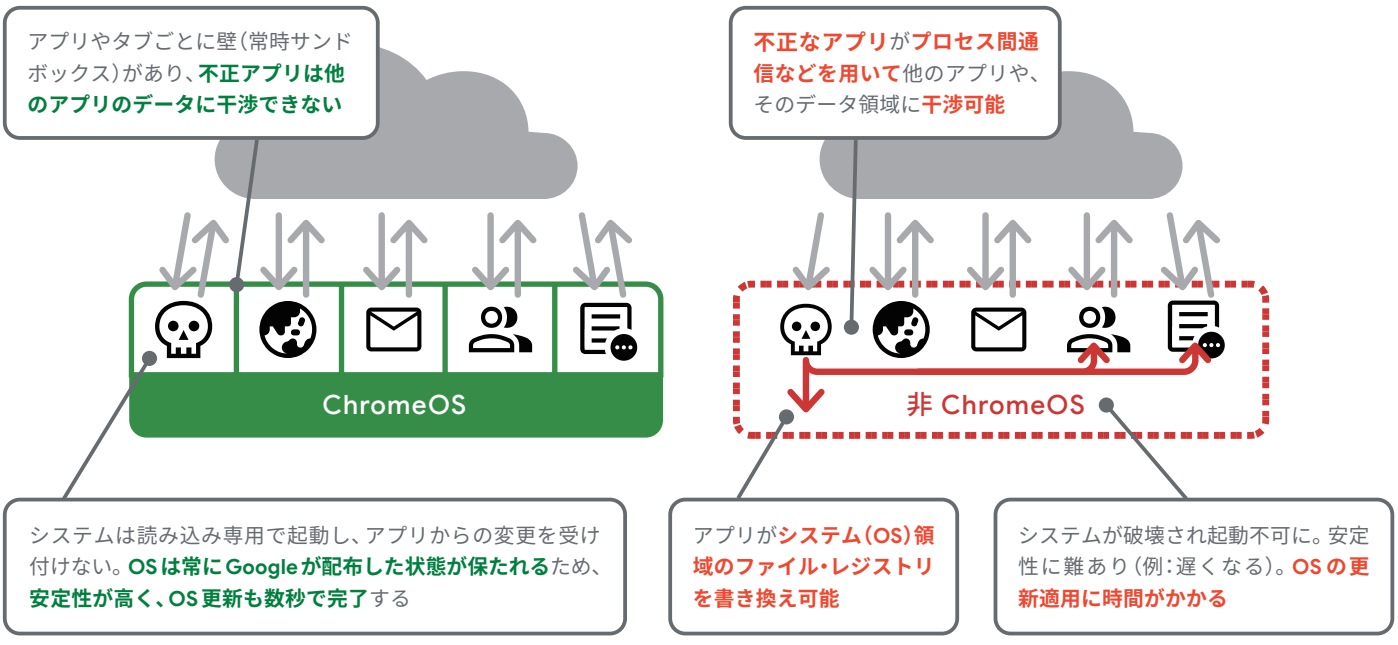
管理者はChromeOSを採用するだけで、各層で別々のソリューションを導入する必要がなくなり、複雑な管理やパッチの適用漏れを起因とするセキュリティの脆弱性という問題を低減できます。

さらに、Chromebookでは、全てのWebページとアプリケーションが「サンドボックス」という制約された環境で動作します。[*27] これにより、Chromebookでウィルスに感染したページを開いても、他のタブやアプリ、その他の要素への影響を防ぐことができます。ChromeOSでは、ランサムウェアなどのマルウェアは自動的にサンドボックス内に留まり、システムやデータに到達することが困難となるのです。

このように、ChromeOSは、ハードウェア層からアプリケーション層まで一貫した高いセキュリティを組み込んだ状態で提供されます。この、一貫した多層防御とサンドボックスの仕組みにより、攻撃者は多数の脆弱性を組み合わせなければならず、攻撃成功のハードルが大幅に上がるのです。

徹底したサンドボックス化:

- ✓ OS領域は読み込み専用
- ✓ システムは常にGoogleが配布した健全な状態で動作



ChromeOSは２つ存在[*11]

異常を自動検出して、数分でバックアップOSを用いて自動復旧[*12]

Chromebookには、起動中のChromeOSの他に、バックアップ用のChromeOSが存在しています。

前述の通り、ChromeOSの領域は厳格なサンドボックス環境かつ読み取り専用となっており、ユーザーやアプリがChromeOSの領域に書き込むことは一切できません。

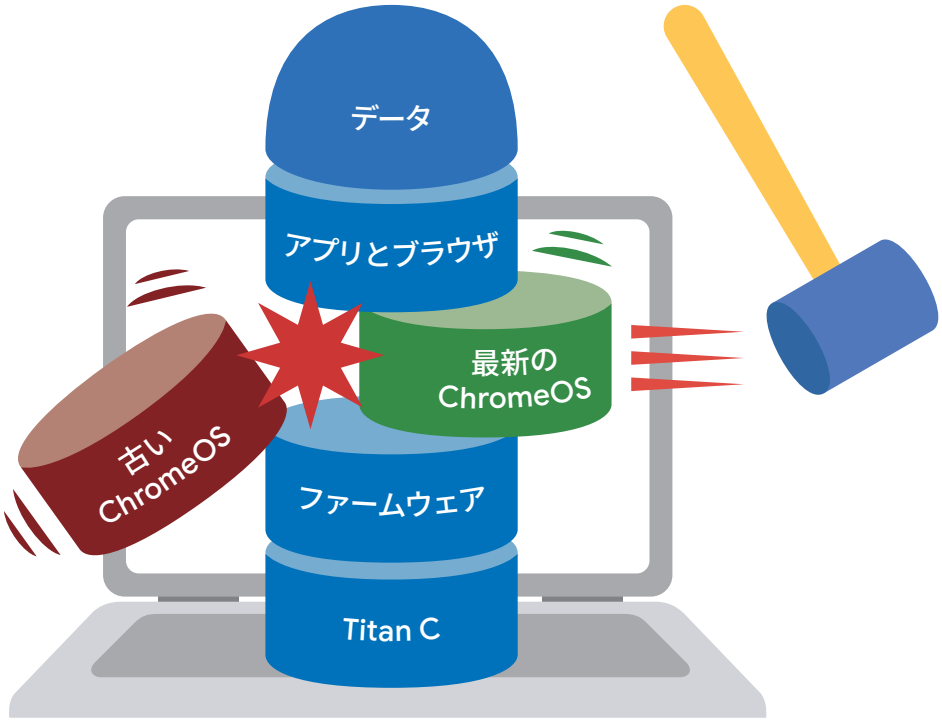
この状況は、だるま落としをイメージしてもらえるとわかり易いと思います。だるまの下の部分がChromeOS、上の部分がアプリやユーザーのデータです。

下層のChromeOSの部分はGoogleが提供したオリジナルの状態が保たれているのですから、何か異変があった際にはバックアップ用のChromeOSにそっくりそのまま入れ替えるだけで修復が完了します。ChromeOSでは、異常検出から数分で、自動的にOSの切替が完了します。この機能により端末が遅くなるということは一切ありません。

ChromeOSでは、OSイメージの作成やメンテナンスは不要です。ChromeOSのリカバリ作業は自動で実行[*13]され、数分で完了するのです。

TiPs

従来のOSでは、電源のオンオフ時にOS更新の適用を求められ、長い待ち時間が発生していました。しかし、ChromeOSは更新適用を全てバックグラウンドで行うため、常に数秒で更新が完了し、業務を中断することなくスムーズに再開できます。



EDR・ウィルス対策は組み込み済み

自動修復で安全なデバイス運用が可能[*14]

EDRとは、Endpoint Detection and Response（エンドポイントの検出と応答）の略で、EPP（Endpoint Protection Platform / 一般的にウィルス対策ソフトとも呼ばれます）の仕組みで防ぎきれなかったマルウェアを検知し、デバイスの隔離などの対処を行うための仕組みです。

ChromeOSには、EDRの機能が組み込まれています。さらに、マルウェアやシステムの改変に自動で対応するための機能も組み込まれています。

例えば、ChromeOSの改変を検出する「確認付きブート」では、Titan Cセキュリティチップが ChromeOSの改変を検出した後、自動的にバックアップ用の ChromeOSで起動して、システムの健全性を保ちます。

Chrome独自の、強化されたセーフ ブラウジングを有効化すると、Chromeがセキュリティ スキャンをリアルタイムで行い、危険なウェブサイトやダウンロード、拡張機能にユーザーがアクセスする前に、警告やブロックを行います。

また、ChromeOSではランサムウェアなどの多くのマルウェアに「実行」する権限を渡しません。[*27] そのため、これらの危険なソフトウェアは、ChromeOSでは動作することができないのです。

このように、ChromeOSのセキュリティ機能は、その多くが検出を必要とするような脅威を、予め排除するように作られており、かつ、組み込みのEDR機能により脅威が検出された場合には自動的に修復を行います。

データの安全性に優れたChromebookは漏洩リスクを大幅に低減するためのさまざまな機能を搭載

画面共有・スクリーンショット コピー＆ペーストは企業データ漏えいの起点

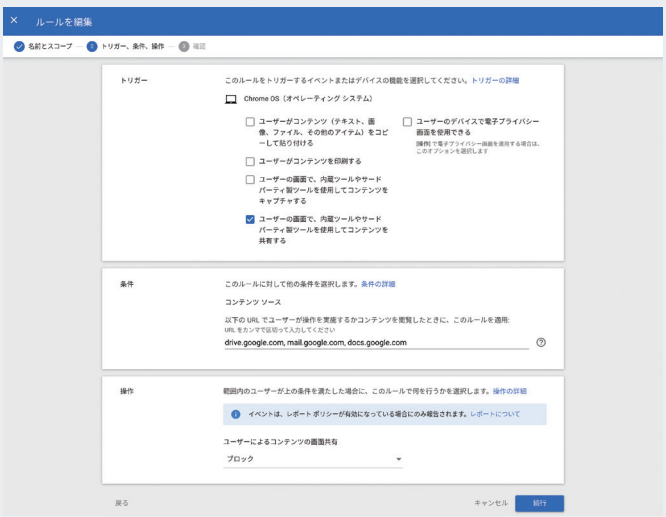
ChromeOSならサイトごとに許可・禁止可能[*17]

ChromeOSでは、USBの使用や印刷を禁止[*18]することができます。一方で、見落としがちなのが、画面共有やスクリーンショット、コピー＆ペースト機能を使用した企業データの漏えいです。ChromeOSには、データ管理という機能があり、これらの操作をサイトごとに許可したり禁止したりすることができます。

例えば、「Google WorkspaceやMicrosoft Office[*28]内であればコピー＆ペーストを可能とするが、他のサイトでは禁止」といった設定や、「機密情報が載っている可能性の高い、社内ポータルサイトをブラウザで表示しているときは画面共有ができない」など、一律で禁止するのではなく、柔軟なポリシー運用が可能です。

特徴は、これらのウインドウが表示されているときのみ禁止され、該当ウインドウが隠れると自動的に共有が再開されるため、通常の業務を妨害しません。

① ドライブやメール、ドキュメントのURLに対して画面共有を禁止する設定を行います



② 指定したURL（ドライブ、メール、ドキュメント）を表示している際、画面共有を試みると、その機能が制限されます。

③ 指定したURL（ドライブ、メール、ドキュメント）が最小化やタブを閉じるなどして非表示になると、画面共有が自動的に再開されます。

Titan Cは、ユーザーごとに異なる鍵でデータを暗号化[*15]

企業データを総当たり攻撃から保護[*16]

現在、多くのシステムではディスク全体を一つの鍵で暗号化して保護しています。この方法では、他のユーザーと共有の鍵が使われています。例えば、鍵の管理が大変になるからという理由で、全てのデバイスを管理者用の共通の鍵で暗号化している場合、鍵の流出時に攻撃者は全ての端末からデータを盗むことが可能となります。

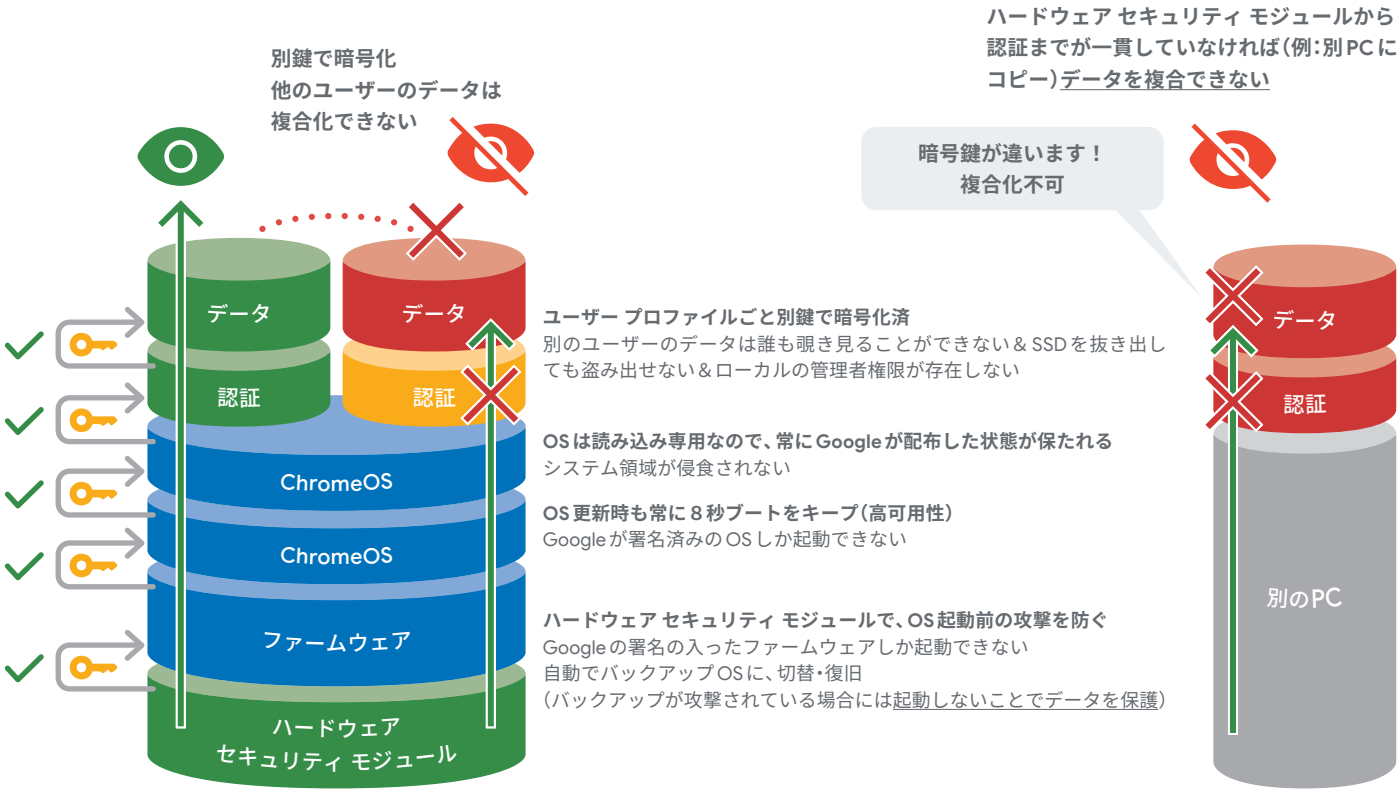
Googleのセキュリティ チップ、Titan Cを用いたChromebookは違います。Titan Cは、全てのユーザーデータをユーザーごとに別々の鍵で暗号化し、Titan C内に厳重に保管します。この鍵はユーザーのパスワードだけでなく、セキュリティ チップ固有の秘密鍵を組み合わせて作成されます。これにより、攻撃者が端末からSSDを盗み出し、パスワードを知っていたとしても、Titan C固有の秘密鍵が無いため、元のデータを復号することはできません。

さらに、Titan Cはデータの復元(復号化)の際に敢えて、1回の復号化の試行ごとに 0.5 秒程度の遅延が発生するように設計されています。この設計により、攻撃者は専用の機器を使った全てのパスワードを試す「総当たり攻撃」を成功させることが非常に難しくなります。

具体的には、ChromeOSでは1回のログイン試行あたり約0.5秒の遅延が発生するため、総当たり攻撃でパスワードを解読するための時間は、最大で約300万年(628×0.5秒)もの時間が必要となります。そのため、攻撃者がデータを盗むことは非常に困難です。

もちろん、オンラインでの認証を強制したり、遠隔での初期化、セキュリティ キーを用いた二要素認証を併用することで、セキュリティをさらに高めることもできます。

データの暗号化
OSの不正改変を防ぎます・OSの二重化による自動回復



「ログアウト時にすべてのユーザーデータを初期化」ポリシーを設定するだけで、Chromebookをワンクリックでシン クライアント端末化 *19

Chromebookは、Webアプリを使う端末としてだけでなく、VDIやDaaS用のシンクライアント端末の置き換え先としても理想的です。なぜならば、システムとユーザーの領域が厳密に切り離されているからです。

ユーザーが初めてログインする時にChromeOSは「Titan C」というセキュリティ チップを使って、「ユーザー プロファイル」を作成します。これは特定のユーザー専用の暗号化された領域で、ユーザーの設定やデータはここに保存され、システムの他の部分からは厳密に分離されて管理されます。

ユーザー プロファイルはクラウドと同期されるため、たとえ端末が故障したとしても、新しいChromebookでログインするだけで、クラウドからユーザー プロファイルが再同期され、直前の作業内容が自動的に復元され、作業を再開することができます。

同じ理由から、ログアウト時にユーザー プロファイル(全ユーザーデータを含む)が削除されても、次回ログイン時に作業内容が自動的に同期されます。このため、Chromebookはシン クライアント端末の代替として理想的です。

IT に詳しくない方でも簡単に安全に使えます

ドライバや セキュリティ パッチの 管理は不要 *20*21

運用がシンプルになり、業務を妨げません

不正なソフトウェアへの対策として最も有効なのは、すべてのソフトウェアを最新に保ち、最新のセキュリティ修正を適用しておくことです。従来の OS では、さまざまなベンダー製の、更新の仕組みもユーザー インターフェースも異なる多様なソフトウェア コンポーネントで構成されているため、この対策を行うのは困難になりがちです。例えば、OS のパッチを当てたら、特定のハードウェアが動作しなくなり、そのハードウェアのドライバを手動で更新しなければならないといった経験や、ウィルス対策ソフトやログ監視ソフトの不具合で、システムが起動しなくなり業務が止まってしまった、という経験があるかたも多いと思います。

ChromeOS は、前述の通り読み取り専用で起動するため、いかなる場合においてもシステム領域への書き込みが禁止されています。従い、ChromeOS は常に Google が配布した状態となり、クリーンで安全な状態に保たれます。従い、特定のソフトウェアの更新によりシステムが起動しなくなるということはほとんどありません。

また、ChromeOS の更新には Chromebook の動作に必要なドライバやセキュリティ パッチが内包されており、管理者がそれぞれのドライバやセキュリティ パッチを管理する必要がありません。

このように、管理者は、Chromebook を採用するだけで、OS やパッチのバージョンと、ドライバのバージョンの違いが引き起こす不具合などを考える必要がなくなるのです。

これは、デバイス管理の負荷を低減しつつ、エンドユーザーの業務を妨げることがなくなるという意味でも有用です。

OSの自動更新で「常に最新」

ユーザーによる OS 更新のための操作は不要 *22

Chromebookはアップデートを自動的に行います。
そのため、常に最新かつ最も安全なバージョンが動作し、ユーザーにとって安心な環境が提供されます。

従来のOSでは、OSの更新ファイルの大きさがネットワークを圧迫し、ネットワーク障害を防ぐために、事前に更新のタイミングをユーザーに通知する必要があったりと、一連の作業が管理者にとって大きな負担となっていました。

ChromeOSでは、差分更新（デルタ更新）*23という技術で、更新に必要な部分だけが配布されます。例えば、新しいOSのサイズが400MBである場合に、その変更部分が40MBだけである場合、差分更新では40MBだけが配布されます。結果、ネットワークの負荷は大幅に減少し、全体としての効率が向上します。

また、Google管理コンソールからは、ChromeOSの更新スケジュールを細かく管理することが可能です。プロキシ サーバーや特別なネットワーク装置、更新の専門知識を持っていなくても、一度のクリックでネットワーク負荷を抑えつつ、安定した自動更新を行うことができます。

安定した運用を重視する組織では、LTS（長期サポート チャンネル）を選択することで、更新の頻度を１ヶ月に１回から半年に１回へと下げることができます。
この場合にもセキュリティ パッチは適用されます。

Chromebookには、更に特徴的な更新の仕組みがあります。すべてのChromebookには、ChromeOSが２つ搭載されています。新しいバージョンのChromeOSがリリースされると、バックアップ用のChromeOSを更新します。そしてユーザーがChromebookの電源を入れ直すか再起動すると、新しいバージョンのChromeOSに自動的に切り替わります。この切り替え時間は、わずか数秒間で、エンドユーザーの業務に影響を与えることはありません。「バック グラウンドで新しいOSのダウンロードは終わったけれども、更新の適用に数十分かかる」というようなことは、ChromeOSでは起こりません。

これらの特性から、Chromebookを採用することで、管理者はOSやドライバ、セキュリティ パッチ、ネットワーク負荷、ユーザーへの事前通達などの更新に関連する様々な問題から解放されます。そして、管理コンソールを使って、誰でも簡単に安定した端末運用を行うことが可能となります。

TiPs

Google管理コンソールでは、ChromeOSとChromeブラウザの更新スケジュールを細かく管理することができます。更新の展開スケジュールを設定することで、プロキシサーバーを用いることなくネットワークのピーク負荷を抑えることが可能です。

TiPs

管理コンソールを利用することで、Chromebookを遠隔から初期化することやログの取得が実行できます。

さらに、リモート デスクトップを通じて遠隔操作も可能です。

ポリシーの設定は、選択ボックスを選ぶだけで完了

Google管理コンソール[*24]

Google管理コンソールは、とても使いやすい設計となっています。特に、ポリシー設定は選択ボックスを選ぶだけで完了します。

これは、ITに詳しくない方でも簡単に管理作業を行うことができることを意味しています。一般的なユーザーにとっては、それほど深いITの専門知識がなくても、このシンプルなインターフェースを通じて設定を変更することが可能です。

一方、従来のポリシー設定は、複雑さが特徴で、多くの専門的知識が必要でした。一定の知識を持っていなければ、適切なポリシー設定を行うことが難しかったのです。
しかし、Google管理コンソールはそのような専門知識を必要としないため、IT管理者の作業負荷を大幅に軽減します。

また、Google管理コンソールの大きな特長の一つに、セキュリティ強化が手軽に行える点があります。Active Directory[*28]など従来型のポリシー管理システムと設定を分離できるため、既存の枠にとらわれることなく、セキュリティを一から見直すことが可能です。IT管理者はGoogle管理コンソールを軸に、直感的でありながらも簡単な方法でデバイスのセキュリティを確実に管理することができます。

Google管理コンソールは、直感的な操作性に優れ、Googleが提供する高度なセキュリティ機能を簡単に導入できる非常に優れた管理ツールです。このツールを使用することで、IT管理者は管理や運用にかかる時間と労力を大幅に削減し、ビジネスの変化に柔軟にかつ迅速に対応するセキュアなエンドポイント環境を容易に構築できるようになります。

ChromeOSは誰でも簡単に使え、操作を覚えるためのコストを削減[*25]

従来のOSでは、多数の機能や設定、操作方法を学ぶ必要があります。これは新しいユーザーにとっては業務を開始できるようになるまでに、多くの時間と労力を必要とし、ときには専門的なコースを受講する必要があることを意味します。

しかし、ChromeOSはそのような勉強時間を必要としません。これは、ChromeOSが多くの人が使い慣れているChromeブラウザをそのまま使用しているからです。Chromeブラウザを使った操作と同様に、ChromeOSでもWebを閲覧したり、アプリケーションを起動したりすることができます。これにより、新たに操作方法を覚えることなく、直感的に使用することが可能です。

さらに、ChromeOSには、IT管理者が配布した設定が必ず適用されるため、ユーザーが設定変更できる範囲は非常に限られます。

この特性は、ユーザーの操作ミスにより設定が変更されてしまい、業務ができなくなるというリスクを大幅に軽減します。ユーザーが設定を誤って変更してしまう心配がほとんどないため、IT管理者は安心してシステムの運用に専念することが可能です。ユーザーにとっても、新しく覚えることがほとんど無いため、業務に集中することができます。

このように、ChromeOSは誰でも簡単に使え、操作を覚えるためのコストを削減でき、また、ユーザーによる設定変更のリスクも低減できるという大きなメリットを持っています。

ChromeOSを採用することで、IT管理者はユーザーのトレーニング時間を削減し、より効率的にセキュアなシステム運用を行うことが可能となります。

従来の端末

セットアップや管理・更新・維持・習熟に多くの労力が必要

ChromeOS

セットアップや管理・更新・維持・習熟がとても簡単

脚注

*1 As of May 27, 2022, https://cloud.google.com/blog/ja/products/chrome-enterprise/chrome-os-ransomware?hl=ja, https://cloud.google.com/blog/ja/products/chrome-enterprise/extending-chrome-enterprise-through-new-security-partner-integration?hl=ja
*2 As of May 27, 2022, https://cloud.google.com/blog/ja/products/chrome-enterprise/extending-chrome-enterprise-through-new-security-partner-integration?hl=ja
*3 As of May 27, 2022, https://cloud.google.com/blog/ja/products/chrome-enterprise/extending-chrome-enterprise-through-new-security-partner-integration?hl=ja
*4 https://googleblog.blogspot.com/2009/11/releasing-chromium-os-open-source.html
*5 https://cloud.google.com/blog/ja/products/chrome-enterprise/protect-business-data-chromeos-data-controls-and-new-security-integrations?hl=ja
*6 https://support.google.com/chromebook/answer/3438631?hl=ja
*7 https://www.chromium.org/chromium-os/chromiumos-design-docs/verified-boot/
*8 https://www.chromium.org/Home/chromium-security/core-principles/
*9 https://www.chromium.org/chromium-os/chromiumos-design-docs/system-hardening/
*10 https://chromium.googlesource.com/chromiumos/docs/+/HEAD/disk_format.md#secure-boot
*11 https://chromium.googlesource.com/chromiumos/docs/+/HEAD/disk_format.md
*12 https://www.chromium.org/chromium-os/chromiumos-design-docs/firmware-boot-and-recovery/
*13 https://www.chromium.org/chromium-os/chromiumos-design-docs/boot-design/#rollback-protection-after-update
*14 https://www.chromium.org/chromium-os/chromiumos-design-docs/system-hardening/#designing-and-developing-for-security
*15 https://www.chromium.org/chromium-os/chromiumos-design-docs/protecting-cached-user-data/
*16 https://www.chromium.org/chromium-os/chromiumos-design-docs/protecting-cached-user-data/#managing-encryption-keys
*17 https://support.google.com/chrome/a/answer/11587610?hl=ja
*18 https://support.google.com/chrome/a/answer/2657289?hl=ja
*19 https://support.google.com/chrome/a/answer/1375678?hl=ja
*20 https://www.chromium.org/chromium-os/firmware-porting-guide/u-boot-drivers/#driver-configuration
*21 https://www.chromium.org/chromium-os/chromiumos-design-docs/filesystem-autoupdate/
*22 https://www.chromium.org/chromium-os/chromiumos-design-docs/filesystem-autoupdate/
*23 https://www.chromium.org/chromium-os/chromiumos-design-docs/autoupdate-details/
*24 https://support.google.com/a/answer/55955?hl=ja
*25 https://www.youtube.com/watch?v=5JyFbF7QFIY
*26 https://youtu.be/5JyFbF7QFIY?si=eYJMo7nMmEE5Oulw&t=671
*27 AndroidやLinuxを有効化した場合にはこの限りではありません。
*28 Active Directory、Microsoft Officeまたはその他のマイクロソフト製品の名称および製品名は、米国 Microsoft Corporationの、米国およびその他の国における商標または登録商標です。

ChromeOS の概要

ChromeOS はクラウド ファーストで多くのビジネス課題を解決できる、オペレーティング システムです。
ChromeOS を搭載したデバイスはユーザビリティとセキュリティに優れ、運用や管理の効率性も向上します。

Chrome Enterprise の概要

Chrome Enterprise は Chrome ブラウザ、ChromeOS、ChromeOS デバイスを包括して管理可能な法人向けサービスです。Chrome Enterprise を利用することで、従業員に対してクラウド ネイティブで安全かつ効率的に働ける環境を提供でき、IT 管理者は社内の ChromeOS デバイスや Chrome ブラウザを一元管理することが可能になります。

Chrome Enterprise に関するお問い合わせは、下記 WEB ページ（または QR コード）をご利用ください。
https://chromeenterprise.google/intl/ja_jp/contact/

chromeOS