# Chromebook のセキュリティ強化のためのベスト プラクティス ガイド

2021 年 1 月

# 本書の目的

グローバルなセキュリティ侵害によって大小さまざまな規模の企業や学校が危険にさらされており、マルウェアやフィッシングによる攻撃は以前よりも短時間で広範囲に行われるようになっています。IT 部門は、事業活動を妨げることなく、外部からの攻撃と内部の脆弱性から環境を保護しなければなりません。

Chromebook を初めてご利用になる方向けに、本書では始めに Chromebook のベースとなっているセキュリティ設計の原則について説明します。これらの原則により、Chromebook はさまざまな攻撃ベクトルに対してネイティブ レベルで保護されます。Google のクラウドベースのポリシーによる制御と Chromebook を連携させた保護機能は、不正アクセスを防止するほか、潜在的な脅威を見つけるとユーザーと管理者に警告します。また、アクセス ポイントにおいて、各組織や機関の独自のセキュリティ ポリシーを強化します。

企業、政府機関、教育機関を含むすべての組織では、リスクを低減するために各組織の Google テナントに Chromebook を登録することを強くおすすめします。Google テナントに Chromebook を登録することで、リモートでのデバイスの一元管理や、全デバイスのセキュリティ確保が可能になります。Google の管理コンソールを使用すると、アクセスの承認、使用状況のモニタリング、ポリシーの更新、データのリモートワイプを簡単に行うことができます。

本書では、 Chrome Enterprise Upgrade または Chrome Education Upgrade を用いて各組織や機関に導入された Chromebook のセキュリティを一層強化するための適切なポリシー設定のベスト プラクティスを説明します。

# 目次

**本書の目的** 2

**目次** 3

**Chromebook の概要** 5
- 安全性を重視した設計 - Chromebook の原則 5
  - 透過的なアップデート 6
  - デフォルトでの暗号化 6
  - OS とユーザーのサンドボックス化 6
  - 確認済みの起動 6
- Chromebook の管理 7
  - ユースケースに応じたユーザー エクスペリエンスの設定 7

**セキュリティ強化ガイドライン** 8
- マルウェアの阻止 8
  - 1. アプリケーションのパッチ適用 8
  - 2. アプリケーションのホワイトリスト登録 8
  - 関連する考慮事項 10
    - EXE ファイル、コマンド、スクリプトの実行 10
    - Chrome ブラウザの設定 10
    - ウイルス対策ツールは不要 11
- インシデントの抑制とデータの復元 12
  - 3. 管理者権限でのアクセスの制限 12
    - デベロッパー モードの無効化 12
    - ログインの制限 12
    - ゲストモードの無効化 13
    - USB と SD ストレージの無効化 13
  - 4. オペレーティング システムのパッチ適用 14
    - 透過的な自動アップデート 14
    - Stable チャンネルの適用 14
    - Chrome の特典プログラム 14
- その他の考慮事項 15
  - マルウェアの阻止 15
    - 5. MS Office マクロの無効化 15
    - 6. ユーザーのアプリケーションのセキュリティ強化 15
    - 関連する考慮事項 15
      - アプリの事前設定 15
  - インシデントの抑制とデータの復元 16
    - 7. 多要素認証 16
      - シングル サインオン 16
    - 8. データの復元 16
      - デバイスを無効にしたときのメッセージ 16
    - 関連する考慮事項 17
      - Verified Access API 17

付録 A - 設定の概要 -
デバイスの設定 18

付録 B - 設定の概要 -
ユーザー エクスペリエンス 19

付録 C - その他のポリシー 20

付録 D - Chromebook の登録 21

付録 E - Google の Chromebook のサポート 22

付録 F - 関連する記事とドキュメント 23

# Chromebook の概要

ユーザーの生産性を高めるように設計された Chromebook は、従来のパソコンよりも安全、高速、かつシンプルです。重いクライアント アプリをインストールする必要がないため、Chromebook で必要となる処理能力は一般的にはそれほど高くありませんが、最新のウェブ標準に完全に対応しています。

IT 管理者にとっても、初めて Chromebook に触れるエンドユーザーにとっても、Chromebook の利用は簡単です。Chrome ブラウザと操作が似ているため、素早くスムーズに導入を進めることができます。

Chromebook は設計段階からセキュリティを重視して設計されています。セキュリティは 1 回限りの取り組みではなく、オペレーティング システムのライフサイクル全体を通して繰り返し取り組むべきものであることを Google は理解しています。

Chromebook はクラウドを活用してユーザーのデータを保護しつつ、オンライン上にある仕事用リソースや承認済みアプリ、以前のソフトウェアへの安全かつすばやいアクセスを可能にします。起動からシャットダウンまで強力なセキュリティで保護されているほか、システム全体を自動アップデートすることで耐障害性を継続的に確保し、ユーザー、デバイス、組織が影響を受ける前に脆弱性に対処することができます。

Chromebook だけでなく、Chrome Enterprise Upgrade、Chrome Education Upgrade で利用可能な関連クラウド サービスと組み合わせることで、すべての Chromebook の導入と制御（ユーザー エクスペリエンス、デバイスのセキュリティ、ネットワーク接続、アプリの許可・配布）を簡単に行うことができます。また、Google の年中無休 24 時間体制のサポート サービスを利用できます。

## 安全性を重視した設計 - Chromebook の原則

Chromebook のセキュリティ設計では、組み込みの強固なシステム、プロセスの分離、Chrome ブラウザでの継続的なウェブ セキュリティの改善、安全な自動アップデート、確認済みの起動、暗号化、シンプルなアカウント管理を組み合わせて、幅広い攻撃からデバイスを保護しています。

Google は Chromebook のユーザーに実用的なセキュリティと使いやすさを提供することに注力してきました。そのために、4 つの基本原則（透過的なアップデート、デフォルトでの暗号化、OS とユーザーのサンドボックス化、確認済みの起動）に従い、開発に取り組んでいます。

## 透過的なアップデート

マルウェアを防ぐのに重要なことは、すべてのソフトウェアを最新の状態に保ち、最新のセキュリティ パッチを適用しておくことです。従来のオペレーティング システムでは、さまざまなベンダーがリリースしたアップデートのメカニズムやユーザー インターフェースが異なるソフトウェア コンポーネントが多数含まれており、、最新の状態に保つことは困難でした。 Chromebook はソフトウェアのアップデートを自動で管理するため、デバイスは常に最新かつ最も安全な Chrome OS のバージョンで稼働します。

自動アップデートに関する OS の設計ドキュメント - ファイル システム / 自動アップデート

## デフォルトでの暗号化

ダウンロード、Cookie、ブラウザのキャッシュなど、特定の種類のファイルは一般的にどのコンピュータにも存在します。Chromebook はこれらすべてのデータを自動的に暗号化し、不正改造防止機能を備えたオンボードのハードウェア セキュリティ モジュールで暗号鍵を保護します。ファイルを保護し、鍵を安全に保つための追加の運用は必要ありません。

暗号化に関する OS の設計ドキュメント - キャッシュされたユーザー データの保護

## OS とユーザーのサンドボックス化

Chromebook では、各ウェブページとアプリケーションが「サンドボックス」と呼ばれる制限された環境で実行されます。感染したページに Chromebook がアクセスした場合でも、デバイス上の他のタブやアプリに影響を与えることなく、脅威は自動的に封じ込められます。

オペレーティング システムの各コンポーネントもサンドボックス化されており、OS も完全にサンドボックス化されているため、システムの変更や、管理者権限によるアクセス、レジストリ キーの更新は不可能です。OS もセキュリティを考慮して設計されているため、IT 管理者はセキュリティに優れたエンドポイントを簡単かつ迅速に提供することができます。

システムのセキュリティ強化に関する OS の設計ドキュメント - システムのセキュリティ強化

## 確認済みの起動

Chromebook は起動時に「確認済みの起動」と呼ばれるセルフチェックを毎回行います。Chromebook はこの「確認済みの起動」を行って、常にクリーンなオペレーティング システムのみを実行し、すべてのレイヤが Google によって発行、署名されていることを確認します。

「確認済みの起動」でデバイスのオペレーティング システムが改ざんされている、または破損していることが検出された場合、通常は自動的に修復されます。ユーザーや管理者が操作する必要はありません。自己修復できない場合は起動を中止して、安全でないシステムがアクセスされないようにします。

この場合は、Chromebook リカバリ ユーティリティを使用して Chrome OS を再インストールすることができます。

確認済みの起動に関する設計ドキュメント - 確認済みの起動

# Chromebook の管理

Chromebook では、厳格なセキュリティ プロファイルを維持するために前述のすべてのセキュリティ制御が機能しているほか、読み取り専用のシステム パーティションも確認済みの起動で保護されています。そのため、IT 管理者は SoE の構築や、広範囲に及ぶレジストリ エントリの管理と編集、時間のかかるデバイスのイメージ作成（マスター イメージの作成）を行う必要はありません。

設計段階からデバイスに組み込まれている機能以外にも、Chrome の一元管理サービスを利用することで、すべてのユーザーと Chromebook デバイスのデプロイと制御（ユーザー エクスペリエンス、デバイスの運用モードの選択、ネットワーク接続プロファイル、アプリケーション）を簡単に行うことができます。Chromebook を登録するとすぐに、利用可能なすべてのポリシーとそのデフォルトの設定が適用されます。

後述の「セキュリティ強化のガイドライン」では、オーストラリア信号局（ASD）の Essential Eight ガイドラインに沿ってこれらのポリシーをデフォルト設定から変更し、Chromebook のユーザー エクスペリエンスを詳細に設定して特定のセキュリティを強化する方法について概説しています。これらについては、各組織固有のニーズに合わせて検討し、実装します。

## ユースケースに応じたユーザー エクスペリエンスの設定

パソコンはさまざまなユースケースで使用されます。アプリケーションを利用するためにユーザーのログインが必要になるケースもありますし、関係者が ID を入力せずにデバイスにアクセスするケースもあります。また、デバイスで特定の機能だけを実行するケースもあります。どのようなシナリオであっても厳格なセキュリティを適用し、ユーザー エクスペリエンスを制御する必要があります。表 1 は、具体的なユースケースに応じたユーザー エクスペリエンスを定義するために必要な Chrome の設定カテゴリを示しています。ただし、[デバイスの設定] セクションは常に適用されます。

**表 1: ユースケースに応じたユーザー エクスペリエンスの設定**

| ユースケースのグループ | ユースケースの説明 | ユースケースの具体的な例 | 詳細 | Chrome の設定カテゴリ |
|---|---|---|---|---|
| ユーザー | クラウド ワーカー | • 生徒に 1 台ずつ割り当てられた学校のデバイス<br>• 企業で使用するデバイス<br>• パソコン<br>• フロントライン ワーカー | ユーザーによるログイン<br>クラウドと同期された個人用の プロファイル<br>コラボレーション ツールへのアクセス<br>学習ツール、ビジネスツールへのアクセス | **ユーザーとブラウザの設定** |
| 管理対象ゲスト | シン クライアント ++ | 病室で使用するデバイス<br>コンタクト センター | VDI 以外の機能も使用<br>ローカルのウェブアプリ<br>指定されたウェブアプリおよび Android アプリにアクセス | **管理対象ゲスト セッションの設定** |
| | 外部の関係者との共有デバイス | セルフサービスのウェブキオスク<br>一時的な貸し出し<br>バックオフィスのトレーニング<br>インターネット キオスク | ユーザーのログインは不要<br>外部の関係者<br>管理されたエクスペリエンス<br>特定のポータルサイトの閲覧 | |
| アプリのみ | 完全なシン クライアント | 事業継続計画<br>高度に保護された環境 | 起動して VDI アプリを使用、Chrome のユーザー エクスペリエンスは不要 | **アプリの設定のみ** |
| | 単一機能のデバイス | コンピュータを使用した試験<br>デジタル サイネージ<br>インタラクティブなキオスク | 起動して単一のアプリを使用、Chrome のユーザー エクスペリエンスは不要 | |

# セキュリティ強化ガイドライン

## マルウェアの阻止

今日では、知名度の高い合法的なウェブサイトでさえ、マルウェアに感染している可能性があります。通常のパソコンの場合、感染したウェブページにアクセスするだけで、マルウェアに感染する恐れがあります。マルウェアはブラウザの欠陥を悪用して、パスワード、学校や会社のデータ、個人情報や財務情報を盗みます。

Chromebook には、このような継続的な脅威を考慮して設計された初めてのオペレーティング システムが搭載されています。Chrome OS には「多層防御」の方針に沿った複数の保護レイヤがあるため、1 つのレイヤが侵害されても他のレイヤが引き続き防御します。組み込みの制御機能の詳細については、「サンドボックス化」と「確認済みの起動」をご覧ください。

### 1. アプリケーションのパッチ適用

オペレーティング システムの透過的な自動アップデートと同様に、Chromebook は関連するアプリケーション ストアで拡張機能やアプリに利用可能なアップデートがないかどうかを定期的に確認します。このため、アプリベンダーがアプリの新しいバージョンをリリースするとすぐに、新しいバージョンがバックグラウンドですべての Chromebook に自動的にダウンロードされ、アプリがアップデートされます。ユーザーの操作が妨げられることはありません。セキュリティ強化のため、新しいバージョンは、現在インストールされているバージョンと同じ秘密鍵を使って署名される必要があり、アップデーターと偽った不正な更新を防ぎます。

### 2. アプリケーションのホワイトリスト登録

アプリケーションのホワイトリスト登録を使用することで、管理者はユーザーのサードパーティ ユーティリティへのアクセスを制限し、組織と各セキュリティ チームで検証済みの信頼できるユーティリティだけにアクセスを許可することができます。これによって、Chromebook で悪意のあるユーティリティや、信頼性の低いユーティリティが実行されるリスクが大幅に低減され、管理者が制御できるようになります。

従来の承認済みのアプリケーションはデバイスの SoE に基づいて定義されていますが、Chromebook の管理ではユーザーに重きを置いたプロファイル管理アプローチを採用しています。ユーザーの役割とプロファイルに応じてアプリを許可することで、役割が異なる複数のユーザーで柔軟にデバイスを共有することができます。これらのユーザーは、同じデバイス上のそれぞれ異なるアプリを必要としますが、IT 部門はデバイスのイメージを作成したり、ユーザーごとに別々のセキュリティ対策を適用したりする必要はありません。このため、アプリケーションのホワイトリスト登録の設定は、ユースケースに応じたユーザー エクスペリエンスの設定下で行います（カテゴリについては表 1 をご覧ください）。

アプリケーションのホワイトリスト登録を行うためのおすすめの設定を次の表に示します。

**表 2: アプリケーションのホワイトリスト登録（[ アプリと拡張機能の設定 ] 内）**

| ポリシー名 | 推奨値 |
| --- | --- |
| ユーザーに他のアプリや拡張機能のインストールを許可する | 他のすべてのアプリや拡張機能をブロックする |
| 許可されているアプリと拡張機能 | 原則として、組織のユーザーまたは生徒と教師が作業をするうえで必要となるアプリと拡張機能のみを許可します。また、定期的に検討して、不要になったアプリや拡張機能を削除します。 |

関連する設定の詳細なドキュメントについては、次のリンク先をご覧ください。
https://support.google.com/chrome/a/answer/6177447?hl=ja

**表 3: アプリケーションのホワイトリスト登録の設定（[ ユーザーとブラウザの設定 ] で設定）**

| ポリシー名 | 推奨値 |
| --- | --- |
| Android アプリケーション - アカウントの管理 | アカウントの追加を無効にする |

関連する設定の詳細なドキュメントについては、次のリンク先をご覧ください。
https://support.google.com/chrome/a/answer/2657289?hl=ja#apps

# 関連する考慮事項

## EXE ファイル、コマンド、スクリプトの実行

Chromebook は、ブラウザを最新のコンピューティング環境における主要なアプリケーションに位置付けるために設計されました。最新のウェブ フレームワークや Android SDK を使用するアプリケーションは、Chromebook 上で機能豊富なオフライン対応のエクスペリエンスを提供できます。

EXE、MSI、DGW 形式にパッケージされたアプリケーション、コマンド スクリプトなどは Chromebook と互換性がなく、設計上これらを実行することはできません。そのため、根本から厳格なセキュリティ体制が実現されています。

## Chrome ブラウザの設定

Chromebook の主なユーティリティである Chrome ブラウザは、ウェブ上でデータを安全に保護するために開発されました。Chrome ブラウザは、マルウェアやフィッシングの阻止から、最新のサンドボックス化やネットワーク セキュリティに至るまで、すべてのレイヤでセキュリティを確保します。また、Google はウェブ セキュリティ コミュニティの規格を先導して作成することにより、攻撃者の一歩先を進んでいます。

次のおすすめの設定にすることで、デフォルトの設定よりもさらにセキュリティを強化することができます。

**表4: ユーザー エクスペリエンスの設定（[ ユーザーとブラウザの設定 ] または [ 管理対象ゲスト セッションの設定 ] で設定）**

| ポリシー名 | 推奨値 |
|---|---|
| Smart Lock | Smart Lockを許可しない |
| タスク マネージャ | タスク マネージャでのプロセスの終了をユーザーに禁止する |
| サイト分離 | すべてのウェブサイトでサイト分離を有効にする |
| アイドル設定 | 2 分 |
| アイドル時の操作 | スリープ |
| スリープ時の画面のロック | 画面のロック |
| シークレット モード | シークレット モードを無効にする |
| リモート アクセス ホストのドメイン | [<ご利用のドメイン>.com] |
| セーフサーチと制限付きモード | 常にセーフサーチと制限付き Youtube を使用する |
| URL のブロック | [必要に応じて設定する。すべてブロックする場合は「*」を追加する] |
| デベロッパー ツール | 許可しない |
| 予備のアカウントへのログイン | 予備の Google アカウントに対するログインやログアウトを禁止する |
| セーフ ブラウジング | 常にセーフ ブラウジングを有効にする |
| ダウンロードの制限 | 危険性のあるダウンロードをブロックする |
| セーフ ブラウジング警告の無視を無効にする | セーフ ブラウジングの警告の無視をユーザーに許可しない |

次のポリシーを設定するかどうかは任意ですが、ユーザー エクスペリエンスと柔軟性を考慮して適用する必要があります。

**表 4: ユーザー エクスペリエンスのオプション（[ユーザー設定] または [管理対象ゲストの設定] で設定）**

| ポリシー名 | 設定可能な値 |
|---|---|
| ブラウザの履歴 | 常にブラウザの履歴を保存する / 保存しない |
| ブラウザの履歴の削除 | 設定メニューでの履歴の削除を許可する / 許可しない |
| 一時的ログインモードを適用 | すべてのユーザーデータを消去 / すべてのユーザーデータを消去しない |
| 位置情報 | 許可 / 無効化 / 常に確認 / ユーザーに判断を許可 |
| プロキシモード | ユーザーに設定を許可 / 強制適用 / 自動検出 / 使用しない |
| サポートされている HTTP 認証スキーム | NTLM / 基本 / ダイジェスト / ネゴシエーション |
| スクリーンショット | 許可 / 禁止 |
| キャスト | 許可 / 禁止 |
| 印刷 | 許可 / 禁止 |
| ローカル プリンタの管理 | ユーザーに新しいプリンタの追加を許可する / 許可しない |
| トレイにログアウト ボタンを表示する | トレイにログアウト ボタンを表示する / 表示しない |
| Chromebook でのシングル サインオンの有効化 | Chrome デバイスに対して SAML ベースのシングル サインオンを有効にする / 無効にする |

## ウイルス対策ツールは不要

Chromebook には、EXE ファイル、コマンド スクリプト、マクロなどの実行形式ファイルを実行する機能はありません。また、組み込みのサンドボックス機能を使用して、ウイルスやマルウェアのパソコンへの侵入をブロックしています。パソコンへのプログラムの挿入、ウェブ アクティビティのモニタリング、個人情報の盗用を試みる悪意のあるウェブページを分離することにより、脆弱性に対する攻撃への耐性を高めています。

Chrome ウェブストアと[1] Google Play ストアで公開されているすべてのアプリケーションに対して、[2] 脆弱性と悪意の有無に関する検査が自動的に行われます。ユーザーを危険にさらすと見なされた場合は、ストアとデバイスの両方から自動的にアプリを削除することができます。

[1] https://plus.google.com/+GoogleChromeDevelopers/posts/3kpAu4VcP5E
[2] https://source.android.com/security/reports/Android_WhitePaper_Final_02092016.pdf

# インシデントの抑制とデータの復元

## 3. 管理者権限でのアクセスの制限

「ローカル管理者」や「管理者権限によるアクセス」などの概念は Chromebook にはありません。Chromebook の設計上、ユーザーがシステムに入り込んで変更を加えることはできないため、すべてのユーザーは特権を持たないユーザーとなります。

### デベロッパー モードの無効化

組み込みのセキュリティ構成が無効にならないようにすることが大切です。管理者は常にデバイスが登録された状態を維持するとともに、デベロッパーモードを無効にすることをおすすめします。

**表 5: デバイスのポリシー（[デバイスの設定] で設定）**

| ポリシー名 | 推奨値 |
|---|---|
| 自動再登録 | ワイプ後にデバイスを自動で再登録する |

参照: https://support.google.com/chrome/a/answer/1375678?hl=ja#reenrollment

### ログインの制限

Chromebook へのログインを、組織が管理しているアカウントのみに制限することをおすすめします。こうすることで、Chromebook のユーザー エクスペリエンスは、Chrome 管理の [ユーザー設定] で定義したポリシーに準拠したものになります。

**表 6a: デバイスのポリシー（[デバイスの設定] で設定）**

| ポリシー名 | 推奨値 |
|---|---|
| ログインの制限 | [*@<組織名>.com.au] |
| ドメインのオートコンプリート | 次のドメインを使用: [<組織名>.com.au] |

**表 6b: ユーザー エクスペリエンスのオプション（[ユーザー設定] で設定）**

| ポリシー名 | 推奨値 |
|---|---|
| マルチログイン アクセス | ブロック |
| 予備のアカウントへのログイン | ブロック |

注: 特定のユースケース（表 1 をご覧ください）では、ユーザーのログインを必要としない運用モードもあります。この場合はログインを完全に無効にします。

### ゲストモードの無効化

組織ではゲストモードを無効にすることをおすすめします。無効にするには、[デバイスの設定] で次の Chrome ポリシーを設定します。

**表 7: デバイスのポリシー（[デバイスの設定] で設定）**

| ポリシー名 | 推奨値 |
| --- | --- |
| ゲストモードを許可する | ゲストモードを無効にする |

参照: https://support.google.com/chrome/a/answer/1375678?hl=ja#allowguestmode

外部の関係者が会社のアセットを使用する必要がある場合は、他の指定ユーザーと同様の制限をかけて、管理された安全な方法で使用できるようにします。このような場合は、「公開セッション」で「管理対象ゲスト」モードを使用すると容易に運用することができます。詳細については、表 1 をご覧ください。

### USB と SD ストレージの無効化

データ損失のリスクや悪意のあるファイルが持ち込まれる機会を最小限に抑えるために、ほとんどのユーザーに USB ストレージ デバイスへのアクセスを制限することをおすすめします（ユーザーのロールで明らかに必要な場合は除きます）。注: Chromebook にコピーされたウイルスやマルウェアが実行されたり、開かれたり、拡散されたりすることはありませんが、悪意のあるファイルが持ち込まれないようにすることをおすすめします。次の設定をユーザー エクスペリエンスに適用することができます。

**表 8: ユーザー エクスペリエンスのポリシー（[ユーザー設定] または [管理対象ゲストの設定] で設定）**

| ポリシー名 | 推奨値 |
| --- | --- |
| 外部ストレージ デバイス | 外部ストレージ デバイスを許可しない |
| Bluetooth | Bluetooth を無効にする |

## 4. オペレーティング システムのパッチ適用

### 透過的な自動アップデート

Chromebook はデフォルトで利用可能なアップデート（Google が発行、署名したもの）の有無を自動的に確認するため、IT 管理者が作業する必要はありません。アップデートのプロセスはユーザーに対して透過的に実行され、起動時に毎回確認が行われます。詳細については、前述の「安全性を重視した設計」をご覧ください。

### Stable チャンネルの適用

Chromebook には、一連の「チャンネル」を通じて Chrome OS の次期バージョンにアクセスする機能があります。一般ユーザーの Chromebook は、Chrome OS の Stable チャンネルのみを適用することをおすすめします。[デバイスの設定] で次のポリシーを適用します。

**表 9: デバイスのポリシー（[デバイスの設定] で設定）**

| ポリシー名 | 推奨値 |
| --- | --- |
| リリース チャンネル | Stable チャンネルを適用 |

企業への Chromebook の導入を計画する際に、管理デバイスの一部に Beta チャンネルを適用することをおすすめします。これにより、社内の一部のユーザーをテストユーザー グループとし、今後リリースされる Chrome OS のバージョンを試してもらうことができます。こうすることで、社内でのアップデートのテストをスムーズに進め、社内でのリリース時期を調整することができます。

### Chrome の特典プログラム

脆弱性をすみやかに修正することは、ブラウザのセキュリティを確保するうえで重要です。Chrome の特典プログラムでは、責任感を持って新しい脆弱性を Google にご報告くださったセキュリティ研究者に報奨金を提供し、公に表彰しています。重大なセキュリティの脆弱性がある場合、Google は 60 日以内に修正をリリースします。一般的に、重大度の高い脆弱性については 30 日以内に修正し、緊急性の高いものについては必要に応じて 24 時間以内に修正をリリースします。

参照: https://www.google.com/about/appsecurity/chrome-rewards/

# その他の考慮事項

## マルウェアの阻止

### 5. MS Office マクロの無効化

マイクロソフトは Chrome OS と互換性のあるマクロ対応 Office ユーティリティを公開していないため、Chromebook でマクロを実行することはできません。組織は Chromebook での不正なマクロの実行を管理する必要はありません。

### 6. ユーザーのアプリケーションのセキュリティ強化

Chrome のアプリと拡張機能のベースとなるセキュリティ モデルでは、安全かつ確実にユーザーの情報を保護する設計により、ユーザーのセキュリティを確保しています。各アプリと拡張機能には必要な権限のみが割り当てられ、必要なサービスのみにアクセスするようになっています。

アプリと拡張機能にも、前述のプロセスの分離が適用されています。

適切に定義したコンテンツ セキュリティ ポリシーが適用されたアプリケーションは、危険なスクリプトに対する耐障害性が高く、クロスサイト スクリプティングのバグを低減し、中間者攻撃からユーザーを保護します。

## 関連する考慮事項

**アプリの事前設定**

一部のアプリケーションは事前に設定することで、ユーザー エクスペリエンスをシンプルにすると同時に、ユーザーによるアプリの操作を制限することができます。たとえば、アプリが接続するサーバーのホスト名や、アプリ内で有効にする機能などを事前に定義します。利用可能なオプションはアプリケーションによって異なるので、アプリのベンダーに問い合わせて、サポートされている事前設定のオプションを確認することをおすすめします。

例えば、VDI や DaaS へのアクセス端末として Chromebook を使用する際に、対応するクライアント アプリをインストールするだけでなく、予め接続先サーバー名などを事前設定しておきたいケースがあります。Citrix を事前設定する例としては、Citrix Workspace でストアフロント URL とゲートウェイ ホストを定義して、ユーザーが適切なバックエンド インフラストラクチャに確実に接続できるようにしておくことなどが挙げられます。

参照: https://support.google.com/chrome/a/answer/6177447?hl=ja

# インシデントの抑制とデータの復元

## 7. 多要素認証

Google の ID に使用している認証プロバイダに関係なく、多要素認証を使用することを強くおすすめします。

Google を認証プロバイダとして使用する場合は、Chrome の管理パネルで多要素認証を有効にする必要があります。

参照: https://support.google.com/a/answer/184711?hl=ja

認証に別の SAML IdP を使用する場合、一般的に多要素認証はその SSO サービスの責任範囲であるため、その認証フロー内で設定する必要があります。あるいは、追加の本人確認を行うために Google を付加的なレイヤとして追加することもできます。

参照: https://support.google.com/cloudidentity/answer/6002699#ssochallenges

### シングル サインオン

指定ユーザーの認証に SAML 準拠の既存の IdP サービスを利用することは標準の連携機能であり、組織のユーザーは会社の既存の認証情報を使用して Chromebook にログインすることができます。

このような SSO IdP サービスを利用する場合は、次のように Chrome のポリシーを設定することをおすすめします。

**表 10:SSO ポリシー**

| 設定のカテゴリ | ポリシー名 | 推奨値 |
|---|---|---|
| デバイスの設定 | シングル サインオンのリダイレクト | SAML SSO IdP ページへの直接アクセスをユーザーに許可する |
| ユーザーの設定 | シングル サインオン | SAML ベースのシングル サインオンを有効にする |
| ユーザーの設定 | シングル サインオンの再ログインの頻度 | 1 日～4 週間 |

## 8. データの復元

### デバイスを無効にしたときのメッセージ

デバイスを紛失した場合や盗難にあった場合に、管理者は他のユーザーが使用できないように Chromebook を無効にすることができます。デバイスが無効になっているときに、管理者が定義したメッセージをデバイスの画面に表示し、デバイスの返却先の情報を伝えることができます。

**表 11:デバイスのポリシー（[デバイスの設定] で設定）**

| ポリシー名 | 推奨値 |
|---|---|
| デバイスを無効にしたときのメッセージ | [適切なメッセージと連絡先情報を入力します] |

参照: https://support.google.com/chrome/a/answer/3523633?hl=ja#disablechromedevices

# 関連する考慮事項

## Verified Access API

既存のソリューションの多くは、同じクライアント上でのヒューリスティック チェックに依存していますが、そのクライアント自体が侵害されていることがありえます。つまりこの手法では、デバイスの真正のステータスを証明するために使用しているシグナル自体が改ざんされているおそれがあることが課題です。

Verified Access API はデバイスの ID をハードウェア ベースの暗号化で保証し、ステータスが変更されていないこと、起動時のポリシーに準拠していることを確認します。Google Verified Access API を使用すると、VPN、イントラネット ページなどのネットワーク サービスは、クライアントが真正であり、企業のポリシーに準拠していることを暗号で確認できます。

# 付録 A - 設定の概要 - デバイスの設定

| ポリシー名 | 推奨値 |
| --- | --- |
| デバイスを無効にしたときのメッセージ | [適切なメッセージと連絡先情報を入力します] |
| リリース チャンネル | Stable チャンネルを適用 |
| ゲストモードを許可する | ゲストモードを無効にする |
| ログインを制限する | [*@<組織名>.com.au] |
| ドメインのオートコンプリート | 次のドメインを使用: [<組織名>.com.au] |
| 自動再登録 | 自動で再登録する |
| Bluetooth | Bluetooth を無効にする |
| 該当する場合は SSO を使用する | |
| シングル サインオンのリダイレクト | SAML SSO IdP ページへの直接アクセスをユーザーに許可する<br><br>（SSo IdP を使用している場合のみ） |

# 付録 B - 設定の概要 - ユーザー エクスペリエンス

ユースケースに応じた適用可能なポリシー グループについては、表 1 をご覧ください。

| ポリシー名 | 推奨値 |
|---|---|
| Android アプリケーション - アカウントの管理 | [アカウントの追加を無効にする] を選択 |
| Smart Lock | Smart Lock for Chrome を許可しない |
| タスク マネージャ | タスク マネージャを使用したプロセスの終了をユーザーに禁止する |
| サイト分離 | すべてのウェブサイトでサイト分離を有効にする |
| アイドル設定 | 2 分 |
| アイドル時の操作 | スリープ |
| スリープ時の画面のロック | 画面をロック |
| シークレット モード | シークレット モードを無効にする |
| リモート アクセス ホストのドメイン | [<ご利用のドメイン>.com] |
| セーフサーチと制限付きモード | 常にセーフサーチと制限付き Youtube を使用する |
| URL のブロック | [必要に応じて設定する。すべてブロックする場合は「*」を追加する] |
| デベロッパー ツール | 許可しない |
| セーフ ブラウジング | 常に有効にする |
| ダウンロードの制限 | 危険なダウンロードをブロックする |
| セーフ ブラウジング警告の無視の無効化 | 無視することを許可しない |
| ネットワーク ファイル共有の許可 | 無効にする |
| 外部ストレージ デバイス | 外部ストレージ デバイスを許可しない |
| 該当する場合は SSO IdP を使用する | |
| シングル サインオン | SAML ベースのシングル サインオンを有効にする |
| シングル サインオンの再ログインの頻度 | 1 日～4 週間 |

# 付録 C - その他のポリシー

Chrome OS で使用できるポリシーの詳細な一覧については、
https://cloud.google.com/docs/chrome-enterprise/policies/ をご覧ください。

制限の厳しい環境で使用できるその他の設定についてお伝えするために一部を抜粋しています。

| ポリシー名 | オプションの値 |
|---|---|
| NetworkFileSharesAllowed | False |
| DriveDisabled | True |
| NetBiosShareDiscoveryEnabled | Flase |
| RemoteAccessHostRequireCurtain | True |
| BrowserSignin | Force |

これらの設定については、Google Chrome の営業担当者にお問い合わせください。

# 付録 D - Chromebook の登録

Chrome Enterprise Upgrade または Chrome  Education Upgrade を使用すると Chromebook を一元的に管理、制御できます。Chromebook を組織独自の Google テナントに関連付けるには、各 Chromebook を登録する必要があります。

参照: https://support.google.com/chrome/a/answer/1360534?hl=ja

登録する前に、Chromebook が新品の状態であること、または以前使用したことがある場合はワイプしてクリーンな状態であることを確認する必要があります。

参照: https://support.google.com/chrome/a/answer/1360642?hl=ja

# 付録 E - Google の Chromebook のサポート

Chrome Enterprise Upgrade および Chrome Education Upgrade のお客様は、登録済みのすべての Chromebook とユーザーについて、年中無休 24 時間対応のサポートを受けることができます。

Google Cloud サポート センターまたは Google 管理コンソールから Google サポートにサポートケースを送信することができます。このポータルから新しいサポートケースを作成したり、既存のサポートケースを確認したりすることができます。

参照: https://support.google.com/googlecloud/answer/1041916?hl=ja

チケットには的確な件名と、問題の説明（再現手順、スクリーンショット、ログなど）を記入して送信してください。ケースは Google のサポート技術担当者が確認し、最適な解決方法についてアドバイスいたします。

Chromebook デバイス管理の技術サポート サービス ガイドライン:
https://support.google.com/googlecloud/answer/6182373?hl=ja

# 付録 F - 関連する記事とドキュメント

- Chrome のセキュリティに関する動画 - 起動からシャットダウンまで
- Chrome のセキュリティ設計の概要
- Chromebook のエンタープライズ ネットワーク ガイド
- クライアント証明書の管理
- SAML SSO の設定

- デバイスの設定の管理
- ユーザー設定の管理
- 管理対象ゲストの設定の管理
- Chromebook のアプリの管理
- Chromebook の Android アプリの管理

- Play ストアのアプリの安全性に関するホワイトペーパー
- ユーザーの作成
- ユーザーの管理
- 管理者ロールの作成
- 管理者ロールの割り当て
- 組織部門の追加
- 組織部門へのデバイスの移動