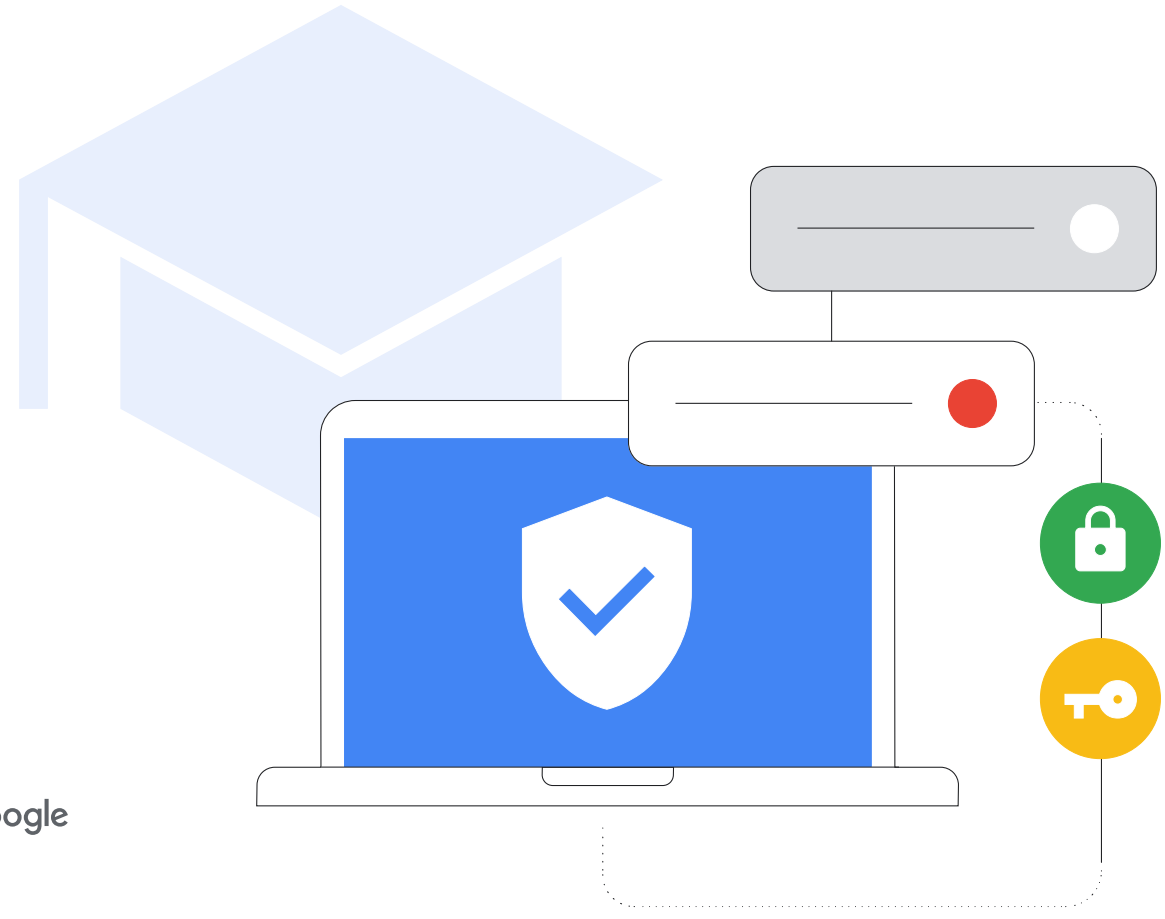
Google for Education

サイバーセキュリティガイドブック

(小中高教育機関向け)

更新 : 2023 年 11 月



Safer with Google

概要

CISA の報告書「Protecting Our Future（未来を守る）」で示されているように、小中高の教育機関が児童生徒や家族、教職員、コミュニティを保護するためにサイバーセキュリティに投資することは極めて重要です。このドキュメントでは、小中高の教育機関のハードウェアやソフトウェアを設定、構成する際にサイバーセキュリティを強化するための、 IT 管理者向けのガイダンスとベスト プラクティスを紹介します。これには、一般的なベスト プラクティスと、Google のプロダクトやサービスに関する具体的なガイダンスも含まれます。Google が掲げる「世界中の情報を整理し、世界中の人々がアクセスして使えるようにする」という使命は、Google for Education チームが教育や学びのためのツールを構築するうえで、非常に重要な原動力となっています。このガイドでは、そうした取り組みの中で得られたノウハウも紹介します。

セキュリティに関するベスト プラクティスについては、トピックごとに詳細な構成、設定、リスク軽減戦略を紹介します。また、Google のサービス、特に教育用のツールにおけるサイバーセキュリティへの取り組みについても説明します。このドキュメントでは、特定のプロダクトやサービスに依拠しない詳細なガイダンスを提供していますが、Google のプロダクトなら、多発している攻撃から保護できる高度な機能を最初から備えています。

リスク

データが豊富な環境につけ込んで自らの利益に変えようと企むサイバー攻撃者にとって、教育機関は最大の標的です。ランサムウェア攻撃はますます巧妙化し、阻止することが困難になっているため、まだ標的にされていない学校の 46% が、いずれ攻撃されると予測されます。また、これらの学校の 42% は、ランサムウェアが非常に蔓延していることから、攻撃は避けられないと考えています。2020 年に迫られた遠隔学習への急速な移行がサイバーセキュリティの隙を広げたことで、学校は攻撃に対して脆弱な状態となっています。

防御

学校へのサイバー攻撃は軽減できます。技術でリスクを完全に排除することはできませんが、教育業界とエドテックベンダーが連携してベスト プラクティスを採用すれば、安全で安心できる、包括的なアプローチを構築し、リスクを大幅に減らすことはできます。ユーザーとデバイスを保護し、データのプライバシーを確保するための適切な予防策や方針を策定することにより、教育機関はリスクをうまく管理して攻撃を軽減できます。

主な推奨事項

- **安全な認証の使用**

  機密情報を安全に保ち、メール、ファイル、その他のコンテンツを保護し、権限のないユーザーが教育システムにアクセスするのを防ぎます。安全なパスワード、2 段階認証プロセス（2SV）、パスキー、パスワード マネージャーなどのユーザー認証のベスト プラクティスをできる限り取り入れます。これは特に、IT 管理者や機密情報を扱う担当者にとって大切です。

- **適切なセキュリティ設定の適用**

  ユーザー、データ、環境を安全に保ちます。Google プロダクトでは、デフォルトでセキュリティが確保されますが、管理者がネットワークやシステムを適切に使用および構成して、セキュリティを維持することも重要です。学校を安全に保つには、ゼロトラストと最小権限の原則を適用します。つまり、ユーザーが効果的な作業に必要なソフトウェア、データ、アプリケーション、システムにのみアクセスできるようにします。

- **システムの更新とアップグレード**

  最新の脅威からユーザーを保護するために欠かせません。最新のオペレーティング システム（OS）とブラウザを使用し、すべてのデバイスで最新のソフトウェア バージョン（または承認された長期安定バージョン）が実行され、自動で更新されていることを確認します。Chromebook などのより安全なソリューションにアップグレードすると、セキュリティを強化できます。なお、ChromeOS デバイスでランサムウェアが検出されたことは一度もありません。

- **リアルタイムのアラートとモニタリング システムの使用**

  セキュリティ対策を強化し、潜在的な問題を迅速に軽減します。それには、Google Workspace for Education などの主要なコラボレーションとコミュニケーションのソフトウェアに組み込まれている機能を使用する、もしくは別のセキュリティ ロギングおよびモニタリング ソリューションを導入するなどの方法があります。学校のネットワーク、デバイス、アプリケーション、ユーザー、データ全体でアクティビティを包括的に追跡するようにします。また、アカウントのログイン、ファイル共有、メールの量（特にフィッシングやマルウェアの試行）、デバイスのアクティビティ、構成の変更を監視します。アラートとモニタリング ソリューションを最新の状態に保ち、脅威、重大なイベント、システムの変更に関する通知を受け取れるようにします。

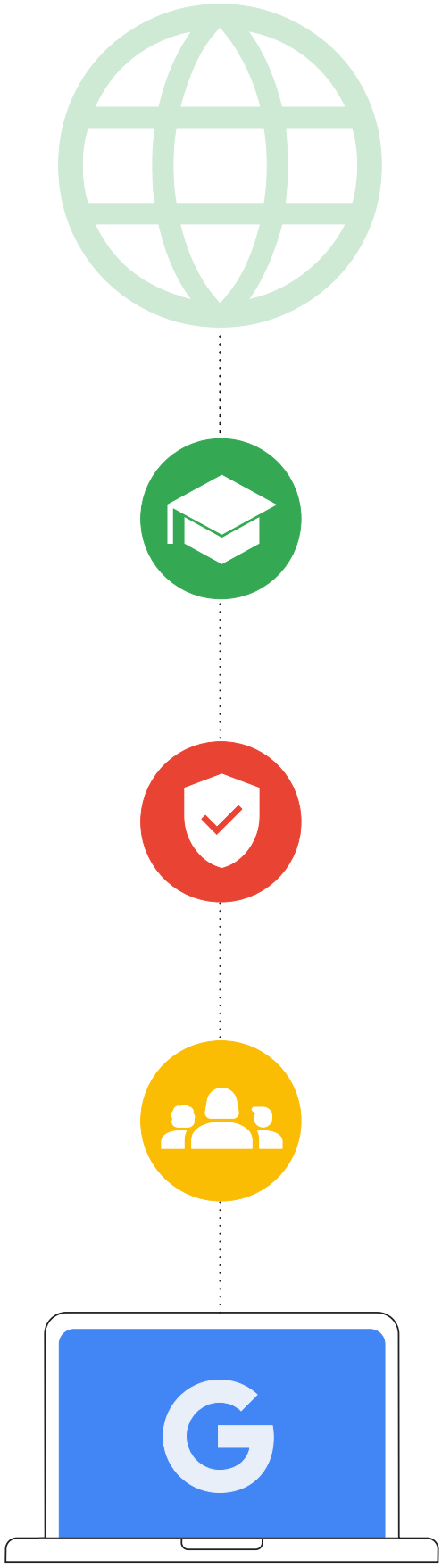
- **教職員や児童生徒のトレーニング**

  最も多発している攻撃から保護するため、デバイスやソフトウェアの安全な使用、潜在的な脅威の発見と報告、データの適切な共有の仕方についてトレーニングを行います。学校や学区で独自のトレーニング資料を作成し、無料で提供されている既成の資料と組み合わせて、学校用の包括的なツールキットとして配布します。

Google プロダクトのユーザー向けの推奨事項:

Google Workspace for Education や Chromebook などの Google プロダクトを使用すると、学校のサイバーセキュリティを強化し、上記の推奨事項をそれぞれ簡単に取り入れることができます。これらのプロダクトを組み合わせれば、ユーザーのプライバシーを保護し、最高水準のセキュリティを確保できる、包括的なソリューションとなります。

また、これらの戦略と次に紹介する追加のガイダンスを組み合わせることで、小中高教育機関の強固なセキュリティ基盤を構築できます。



教育に対する Google のアプローチ

Google は、「世界中の情報を整理し、世界中の人々がアクセスして使えるようにする」という使命を掲げていますが、これは教育分野においても変わりません。Google for Education チームは、こうした使命のもとで Chromebook や Google Classroom などのツールを構築しています。その目的は、児童生徒と教職員が簡単かつ安全に独自のコンテンツを作成、共有、整理し、教育リソースやオンライン ツールを活用できるようにすることです。

学校には、安全かつプライバシーを最初から重視した設計と、きめ細かな管理機能、そして信頼できるコンテンツと情報を備えたテクノロジーが必要です。Chromebook や Google Workspace for Education などのプロダクトを使用する学校にとってのメリットは、世界で最も厳しい教育機関の基準でさえも満たす、トップ水準のセキュリティを確保できることです。また IT 管理者にとっては、データとセキュリティ ポリシーを完全に可視化して容易に制御できるほか、児童生徒にとっては、年齢に応じたコンテンツが提供される、スパムやサイバー脅威の心配が少ない安全なデジタル環境で学習に専念できます。

Google では、誰もが安全に学習できるように、組み込みのセキュリティ機能と設定、最高レベルのプライバシー基準、その他の事前対策型のセキュリティ ツールの提供に優先的に取り組んできました。Chromebook は、学校に迫りくる脅威を軽減できるだけでなく、学校にとって最大の脅威であるランサムウェアへの強力な防御策にもなります。なぜなら、Chromebook に対するランサムウェア攻撃は一度も成功したことがないからです。

一方、Google Workspace for Education は、世界で最も人気のあるクラウドベースの安全なコミュニケーションおよびコラボレーション スイートの 1 つです。ここで紹介した推奨事項に関連する個々のサイバーセキュリティ対策について詳しくは、最後のセクションをご覧ください。

この資料は 2 つのセクションに分かれています。最初のセクションは、どのようなソリューションにも関係がある、小中高教育機関向けの実用的で一般的なセキュリティ ガイダンスです。次のセクションでは、Google Workspace for Education や Chromebook などの Google for Education サービスを使用する教育機関に向けて、設定に関する具体的なガイダンスを紹介します。どちらのセクションも、教育機関と児童生徒のオンラインの安全を守るための情報で構成されています。

はじめに

小中高の教育機関は、デバイスとネットワークの両方で、サイバー攻撃の高いリスクにさらされています。児童生徒を保護し、それらの攻撃によって生じる可能性のあるデータ、サービス、リソース、時間、金銭の損失を防ぐには、可能な限り優れたセキュリティを採用することが極めて重要です（出典: https://www.gao.gov/products/gao20-644）。

このガイドの目的は、学校環境のセキュリティを強化できるよう、学校管理者や学校システムが取り入れるべきサイバーセキュリティのベスト プラクティスを促進することです。これらのベスト プラクティスを取り入れることで、教育システムに対する深刻かつ費用のかかるサイバー攻撃を軽減もしくは防止し、児童生徒や家族、教職員を守ることができます。

学校を標的としたサイバー攻撃は、頻度も深刻度も増しています。小中高のサイバーセキュリティ リソース センターによると、2016～2021 年に全 50 州で公表された、教育機関が関係するサイバー インシデントは 1,300 件を超えます。今日の教育機関のリーダーは、児童生徒や教職員のデータと個人情報だけでなく、教育機関のシステムと情報も保護する必要があります。中でも教育分野は、従来より他の分野に比べてサイバーセキュリティの対応に遅れをとってきたことを考慮すると、これは難しい課題といえるでしょう。

ランサムウェア、フィッシング、マルウェアなどを含むサイバー攻撃に遭うと、個人を特定できる情報（PII）の大規模なデータ侵害や、多額の支払いが生じる（身代金の平均支払い額は 2020 年から 5 倍に増え、今や 812,260 ドル）など、授業やその他の学校運営に長期にわたって悪影響を及ぼす危険性があります。最近では、ランサムウェア攻撃によって学校システム全体がシャットダウンし、児童生徒が何日も学校に通えなくなるなど、コミュニティ全体にも影響が及んでいます。リソースや資金が限られていても、サイバーセキュリティの強化に投資しなければ、小中高の教育機関は格好の標的となり続けます。

サイバーセキュリティを強化するには、コミュニケーション、コラボレーション、パートナーシップが重要です。このドキュメントは、Google の安全とセキュリティに関するヒント、米国国立標準技術研究所（NIST）のサイバーセキュリティ フレームワーク、2023 CISA K-12 Cybersecurity Toolkit and Recommendations（小中高教育機関向けサイバーセキュリティ ツールキットと推奨事項）など、広く認知されているサイバーセキュリティ対策の情報源をもとに編纂したものです。このドキュメントでは、IT 管理者が取るべきまたは考慮すべき一般的な手順と、Google プロダクトに関する Google 独自のベスト プラクティスおよびガイダンスの一部を紹介します。また、セキュリティに関するヒントと他社が提供するサービスについても説明しています。管理者は関連企業が提供するセキュリティ ガイダンスをすべて確認して、最新のガイダンスを取り入れるべきです。責任を果たす企業の製品であれば、その内容や変更点について最も的確な説明を得られます。

これから紹介する推奨事項を取り入れる前に、次の要素についても考慮する必要があります。

留意事項

1. **保護する児童生徒の規模**
   学校ごとにニーズは異なりますが、一定の児童生徒数がある場合はセキュリティとプライバシーを保護するために追加の手順が必要となることがあります。多くのエドテック ツールには、不適切なコンテンツの制限、位置情報や連絡先データのプライバシー保護など、年齢に応じたアクセスを支援する機能が備わっています。

2. **保存するデータの種類**
   センシティブ データを保存する場合は、データを暗号化するか、別の場所に保存することを検討します。

3. **使用するデバイスの種類とデプロイモデル**
   デバイスとそのアプリケーションは自動で更新されるようにして、セキュリティの強化、データの暗号化、アカウントの分離を行い、ユーザーが自身の情報にのみアクセスできるようにする必要があります。

4. **学校や自治体の方針**
   学校では、テクノロジーの使用に関して特定の方針を定めている場合があります。それらの方針に従って、すべての安全保護対策が設定されていることを確認する必要があります。

毎日
1 億件
Gmail でブロックされたフィッシング メールの数

毎週
30 万件
Google で安全でないと特定されたウェブサイトの数

毎日
7,400 万人
Google のパスワード マネージャーのサポートを受けたユーザーの数

毎年
7 億人
セキュリティ診断を使用してセキュリティを強化したユーザーの数

一般的なセキュリティ ガイダンス

安全な認証の使用

安全な認証は、学校やその他の教育機関にとって最優先事項でなければなりません。2022 年の第 4 四半期に発生した侵害では、脆弱なアカウントまたは認証されていないアカウントが原因全体の 48% を占めました。いくつかの主要な推奨事項を取り入れることで、ユーザーが本人であることを確認し、各ユーザーの役割に適した情報のみにアクセスを制限できます。

IT 管理者は、2 段階認証プロセス（2SV、2 要素認証または多要素認証とも呼ばれます）の使用を義務付けて、可能な限りパスワードレス認証（パスキーなど）に移行する必要があります。ユーザーが教育機関のシステムにリモート アクセスしている場合は特にそうです。2SV により、オンライン アカウントのセキュリティがさらに強化され、攻撃者によるアクセスがより困難になります。

2SV は Google 独自のセキュリティ対策の中心となるものであり、Google ではより安全な認証方法の開発に引き続き取り組んでいます。

今日の学校では多くの種類のデバイスやデプロイモデルが使用されており、小中高環境の技術的な適性はさまざまです。アカウントとデバイスのセキュリティは、IT 管理者、教職員、個人用デバイスを使用する高学年、共有デバイスを使用する低学年など、ユーザーの役割や種類によって異なり、ベスト プラクティスもそれぞれに用意されています。各グループの具体的な推奨事項を見ていきましょう。

ほとんどの環境で推奨される認証方法の種類

- **安全なパスワード**

  初回ログイン時に独自のパスワードを作成するようユーザーに促して、最低限の長さと複雑さを満たすよう求めます。長いパスフレーズほど、その長さと複雑な文字の組み合わせによってセキュリティが強化されます。なお、ユーザーにパスワードの定期的な変更を求める必要はありません。これは、より単純なパスワードの使用や軽微な変更（1 文字だけ変えるなど）を助長しかねないためです。

- **2 段階認証プロセス**

  2SV は 2 つ目の手順でアカウントを保護します。多くの場合、セキュリティ キーや、ワンタイム認証コードを作成するスマートフォン アプリなど、ユーザーが持っているものを使用します。どのような形式の 2SV でもアカウントのセキュリティを強化できますが、電話番号ベースの攻撃に対して脆弱になり得る、テキストや通話で送信する確認コードの使用は避けましょう。

- **パスワードレス認証**

  パスキーは、パスワードに代わる安全で簡単な認証方法です。PIN、パターン、生体認証センサー（指紋や顔認識など）、セキュリティ キーのタップなどでアプリやウェブサイトにログインできるため、パスワードを覚えたり管理したりする必要がなくなります。すべての教育環境に適しているわけではありませんが、より安全ですばやいログインが可能なため、従来の認証方法に取って代わりつつあります。パスキーは登録したウェブサイトやアプリでのみ機能するため、ユーザーをフィッシング攻撃から保護できます。

- **シングル サインオン（SSO）**

  SSO を使用すると、ユーザーは 1 組の認証情報で複数のアプリケーションやウェブサイトにアクセスできます。1 組の認証情報を覚えるだけでよい場合、それを書き留める可能性は低くなります。また、学校で複数のユーザー認証情報を管理する必要がなくなれば、IT サポートやヘルプデスクの費用を削減できます。Google Workspace for Education は SSO をネイティブでサポートしているため、ユーザーは Google アカウントの認証情報を使用してサードパーティのアプリケーションにログインしたり、他のプロバイダの認証情報を使用して Google アカウントにログインしたりすることができます。

- **パスワード マネージャー**

  パスワード マネージャーは、学校や職場のアカウントやサービスに安全な一意のパスワードを使用するのに役立ちます（SSO を使用していない場合）。デバイスのオペレーティング システムへのログインには使用できませんが、ユーザーがログインした後のパスワードを管理します。Google ユーザーは、あらゆるプラットフォームの Chrome に加え、ChromeOS と Android でパスワード マネージャーを使用できます。

さまざまなグループの固有のニーズを満たすには、教育機関での役割、アクセスするシステムやデータの種類、ユーザーの年齢に応じて、これらの認証アプローチの特定のサブセットまたは組み合わせを使用します。

管理者

管理者は、小中高の教育機関のシステムと多くのデータを管理しています。管理者のアカウントの保護は、インフラストラクチャからアカウント データ、そして教育機関が管理するデバイスに至るまで、システム全体のセキュリティにとって重要です。そのため、安全なパスワードの使用、堅牢なパスワード マネージャー、2SV など、安全性が確立されている認証メカニズムを採用する必要があります。こうした保護レイヤーを組み合わせることで、管理者アカウントと企業向けサービスのセキュリティを最大限に強化できます。

- 管理者は、物理的なセキュリティ キーか、暗号化による安全な 2SV 方式（信頼できるデバイスに通知を表示）を使用する必要があります。これには、Google 認証システムなどのサービスや、ワンタイム認証コードを作成する他のアプリなどが挙げられます。
- 管理者は、2SV に対応し、さまざまなサービスのパスワードを保存できる信頼性の高いパスワード マネージャーを使用する必要があります。

小学校高学年以上

小学校高学年以上の児童生徒は、自身を保護する方法をすでに学んでいるため、通常、利用する可能性の高いサービスの種類に適した、より安全性の高い認証メカニズムを使用することができます。児童生徒がアクセスできる範囲は、自身のアカウントと、共有された情報のみに制限する必要があります。

- Chromebook を使用する児童生徒に対しては、デバイスでのログインをすばやく行うため、デバイス固有の PIN を作成できるようにします。生体認証は、多くの学校環境では適切でない、または現実的でない可能性があります。
- 各児童生徒が、個人情報（氏名、学級、誕生日など）を含まない一意のパスワードを作成できるようサポートします。パスフレーズを使用することで、パスワードを覚えやすくしながら、いかに複雑性を持たせることができるかを児童生徒に教えます。

教職員

教職員は、管理者と同様にセンシティブ データにアクセスできますが、デジタル インフラストラクチャを管理することはなく、技術的なスキルはさまざまです。

- Chromebook を使用する教職員に対しては、法的に認められている場合は指紋などの生体認証を使用してログインできるようにします。
- および教育機関のシステムにリモート アクセスする職員がいる場合は、可能な限り必ず 2SV の使用を義務付けて、パスワードレス認証に移行します。

小学校低学年以下

小学校低学年以下の児童生徒は、まだ教育テクノロジーの使い方を学んでいる段階のため、限られたサービスやデータの使用に適したシンプルな認証方法が有効です。

- 小学校低学年の児童生徒やパスワードでログインできない児童生徒のために、QR コードやピクチャー ログインといったサードパーティのパスワード代替手段を使用している場合は、安全性が低いことから、セキュリティ対策を講じる必要があります。管理者は、コードが紛失または他者に漏洩するたびに、児童生徒のパスワードを変更し、コードを更新しなければなりません。
- 学校は児童生徒と保護者の双方に、パスワードを秘密にし、QR コードなどの代替認証情報を安全に保管することの重要性を説明する必要があります。
- タブレットなどの個人用デバイスでは、デバイス固有の PIN を安全な代替認証方法として使用できます。

適切なセキュリティ設定の適用

学校のデバイスやネットワークは、世界中の攻撃者にとって目につきやすく価値の高い標的であることから、サービス、リソース、時間、金銭の損失を防ぐために、可能な限り強固なセキュリティを導入することが極めて重要となります。システム管理者は、自身の教育機関が使用するプロダクトで利用できる、効果的で適切なセキュリティ機能を取り入れるべきです。ただし、こうしたシステムは教職員や児童生徒にとって使いやすいものである必要もあります。重要なセキュリティとプライバシーの設定は、個々のユーザーが無効にしたり変更したりできないように構成し、その他の設定はより安全なものをデフォルトに指定します。繰り返しますが、サービス、リソース、時間、金銭の損失を防ぐには、可能な限り強固なセキュリティを導入することが極めて重要です。

Chromebook を使用している場合は、最後のセクションにあるデバイス ポリシーの設定に関する推奨事項を参照してください。

最後に、「データの最小化」を取り入れて、個人情報の収集、使用、開示の目的および手段を、サービスを提供するために合理的に必要かつ相応なもの、または立場に合ったものに限定するようにします。

アプリケーションと更新

デバイスにインストールされる各アプリケーションは、攻撃ベクトルに悪用される可能性があるため、ユーザーがインストールできるアプリを制限して最小限に抑えます。可能であれば、信頼できるソースのアプリケーションを使用します。たとえば、Google Play ストアで認証済バッジを確認することをユーザーに推奨し、セキュリティ審査を通過した公式アプリケーションをダウンロードしてもらうようにします。OS やハードウェアを変更するアプリの動作（ジェイルブレイクや root 権限取得）は、重大なセキュリティ上の欠陥を引き起こすため回避する必要があります。

デバイスの紛失や盗難

デバイスの紛失が、必ずしもデータの損失を意味するわけではありません。管理者は、デバイスの紛失や盗難が発生した場合でも、情報やドキュメントに確実にアクセスできるようにするための手順（ドキュメントをクラウド環境で管理するなど）を標準化しておく必要があります。アカウントへのアクセスが中断しないように、2SV プロセスのバックアップ コードをダウンロードして印刷することもおすすめします。

デバイスの紛失や盗難が報告された場合、可能であればデバイスをリモートでロックダウンし、関連するアカウントもロックダウンするかフラグを付けて、不正にアクセスされないようにします。Chromebook は紛失の際にリモートワイプすることができます。また、Google Workspace for Education のアカウントは、不審なアクティビティがないか監視したり、必要に応じて停止（ロック）したりできます。

アクセス権と表示設定

ユーザーのアクセス権限は、作業や学習を効果的に行うために必要なデータ、ソフトウェア、サービス、システムに絞り込む必要があります。そうすることで、意図しないアクセスを制限し、誰がどのリソースにアクセスしているかを追跡できます。機密性の高いデータ（ユーザーの個人情報など）やシステム（人事、給与、評価、セキュリティ、構成など）については特に注意します。学校が所有するデバイスへのアクセスを制限し、特定の職員のみがアクセスできるようにして、データにアクセスできるユーザーと状況を監査します。

コラボレーション ツールのデータ共有ポリシーを見直して、不適切な共有や過剰な共有、不正なアクセスを防ぎます。また、学校環境外での共有を制限またはブロックし（特に児童生徒の場合）、機密コンテンツの共有を監視するポリシーを有効にします。

リスクの高いユーザーに対する高度な保護機能

Google では、注目されやすいユーザーや機密性の高い情報（Google Workspace for Education の管理者など）向けに、高度な保護機能プログラム（APP）を提供しています。APP は、フィッシング攻撃、有害なダウンロード、パスワード侵害などの標的型攻撃からユーザーをさらに強力に保護します。APP は Google アカウントへの標的型オンライン攻撃を阻止できるよう特別に設計されており、厳格な認証とセキュリティ キーを自動的に使用して、アカウントデータへの第三者のアクセスを制限します。また、他のオンライン アカウント プロバイダからも、リスクの高いユーザー向けに強力なアカウント保護機能が提供されています。個人情報や技術システムにアクセスする管理者や職員は、こうした機能を常に使用する必要があります。

システムの更新とアップグレード

自身を守るために、誰もができる最も重要なことの 1 つは、デバイスのオペレーティング システムとアプリケーションを常に最新の状態に保つことです。小中高の教育機関は、子どもたちの教育や日々の生活において重要な役割を担っているため、このことはますます重要となります。教育分野およびその他のリスクの高い分野におけるマルウェア攻撃のほとんどは Windows ベースであり、SolarWinds、Los Angeles Unified School District のランサムウェア攻撃、Little Rock School District のハッキング、Microsoft Exchange Server のデータ侵害、Albuquerque School District のランサムウェア攻撃、そして最近では連邦機関が使用する Microsoft のデータ侵害などはその一例です。これについても、クラウド プロダクトやクラウド サービスを使用することで、攻撃対象領域が減り、システムやアプリケーションも自動的に最新の状態に保たれるため、管理者の作業を効率化できる部分と言えます。

最新のオペレーティング システムにアップグレードして常に最新の状態に保つ

通常、オペレーティング システム（OS）の最新バージョンには、既知の攻撃ベクトルを防ぐための新しいセキュリティ機能が含まれています。そのため、デバイスの OS 内で自動更新機能を有効にする必要がありますが、自動更新が不可能な場合は、信頼できるベンダーからパッチとアップデートを少なくとも月 1 回ダウンロードしてインストールしなければなりません。

Chromebook は ChromeOS で動作しているため、最新のセキュリティ パッチが頻繁かつ迅速に、自動で導入されます。さらに起動前には、読み取り専用のオペレーティング システムの整合性が検証されます。デバイスに保存されるすべてのデータを暗号化して不正アクセスから保護し、すべてのウェブページとアプリケーションを個別のサンドボックスで実行するため、1 つのウェブサイトやアプリがマルウェアに感染しても、デバイスの他の部分に広がることはありません。

Chromebook に移行する準備が整っていない場合は、ChromeOS Flex を使用できます。これは、学校のデバイスをモダナイズするために作られた ChromeOS のバージョンです。ChromeOS Flex は、プロアクティブな組み込みのセキュリティとクラウドベースの管理機能を備えており、あらゆる人に最新の教育および学習環境を一貫して提供できます。また、既存のハードウェアを置き換えることなく、ユーザーを自動で保護し、悪意のある実行可能ファイルやアプリをブロックします。

最新のブラウザにアップグレードして常に最新の状態に保つ

ブラウザを常に最新で安全な状態に保つことも重要です。最新のブラウザには、より高度なセキュリティ機能が備わっています。ユーザーはこれらの機能を簡単に有効にできるほか、教育機関のパソコンでデフォルトで有効にするよう管理者が設定することもできるので、インターネット経由で転送される機密情報を保護するのに役立ちます。ブラウザは最新の状態に保つ必要があります。仕事でも、学習でも、その他のオンライン活動でも、常に更新される最新のブラウザを使用することで以下が可能になります。

- **堅牢なセキュリティの使用**
  サイト分離や、ユーザーが誤って危険なウェブサイトにアクセスするのを防ぐセーフ ブラウジング保護機能が含まれます。
- **自動更新の有効化**
  ブラウザのセキュリティ アップデートを迅速に適用できます。
- **接続の安全性の確認**
  最新のブラウザでは Transport Layer Security を使用する必要があり、ユーザーは URL の横のマークをクリックして、接続が安全か確認できます。

Chrome はセキュリティを重視して設計されており、セーフ ブラウジングなどのセキュリティ機能がデフォルトで有効になります。また、ウェブの閲覧中にパスワードを自動入力できるパスワード マネージャーが統合されており、安全なパスワードを簡単に使用できます。

リアルタイムのアラートとモニタリング システムの使用

リアルタイムのアラートとモニタリング システムにより、学校は脅威を迅速に見つけ出し、被害が発生する前に対応できます。重要なのは、セキュリティ ツールがバックグラウンドで実行され、システム全体からセキュリティ イベントを収集してログに記録できるようにすることです。AI ツールは、収集された大量のデータを精査して異常やパターンを見つける能力が特に優れているため、これを使用して脅威をより迅速かつ容易に検出し、脆弱性を処理して解決できます。これにより、IT 管理者や職員は確認の必要なアクティビティに優先順位を付けることができます。

学校は、Google Workspace for Education などの主要なコラボレーションとコミュニケーション ソフトウェアに組み込まれているアラートとモニタリングの機能を使用することや、単体のセキュリティ情報およびイベント モニタリング（SIEM）ソリューションを導入することができます。

リアルタイムのアラートとモニタリング システムでは、ユーザーのログイン、ファイルへのアクセス、潜在的な侵入、データの盗難やその試み、管理者のアクティビティなど、学校のネットワーク、デバイス、アプリケーション、ユーザー、データ全体のさまざまなアクティビティを追跡できます。

システムで不審なアクティビティが検出された場合は、学校の IT 担当者にアラートを送信できます。これにより、管理者は問題を調査して、脅威を軽減するための措置を講じることができます。

また、アラートとモニタリング ツールを使用して、学校を襲う脅威について理解を深めることも可能です。こうしたリアルタイムのシステムから得られるデータを分析することで、傾向やパターンを特定し、保護の強化に役立てることができます。

アラートとモニタリング（SIEM を含む）システムの使用におけるベスト プラクティス

1. **セキュリティ目標の定義**
   学校にとって最も重要な情報とシステム、および最大のリスクをもたらす脅威の種類を特定します。次に、それらの脅威を監視するために収集する必要があるデータを特定します。

2. **適切なデータの収集と構成**
   適切なデータを収集し、最も関連するセキュリティ目標に沿ってアプリケーションを構成することが重要です。こうしたデータには、ファイアウォール、コンテンツ フィルタ、侵入検知システム、ウェブサーバー、その他のセキュリティ デバイスから得られるデータや、コミュニケーションとコラボレーション ソフトウェア、学校情報システム、学習管理システムから得られるデータなどがあります。

3. **アラートの調査と対応**
   モニタリング システムでアラートが発生したら、問題を調査し、適切な措置を取ることが重要です。たとえば、複数のチームで協力してアラートの発生源を調査し、誤検出かどうかを判断したり、脅威を軽減するための措置（アカウントの停止、ユーザー パスワードのリセット、メールの隔離または削除、ファイル権限の変更、デバイスのワイプなど）を講じたりします。

教職員や児童生徒のトレーニング

小中高の教育機関は、キャンペーンやパートナーシップを利用してユーザーを後押しし、学校コミュニティのセキュリティ意識と習慣を向上させる必要があります。セキュリティの重要性について教職員や児童生徒を教育することは、オンラインで自身を守り、深刻なサイバーセキュリティの脅威を防ぐうえで非常に重要です。教育機関全体で導入されているプロダクトやサービスの使用方法、フィッシング メールなどの脅威を発見して報告する方法、そして最も重要な点として、こうした攻撃を防ぐためにどう行動すべきかを教えましょう。

デバイスとソフトウェアの安全な使用方法

管理者は、教職員や専門家と協力して、年齢に適したレベルのサイバーセキュリティのカリキュラムを開発し、児童生徒がデバイス、ソフトウェア、システムの安全な使用方法を理解できるようサポートします。学校または学区独自のトレーニング教材を作成し、教職員や児童生徒向けの推奨事項を状況に合わせて説明するのも効果的ですが、Safety.Google で提供されている Be Internet Awesome や Khan Academy などの既成の教材を活用し、ニーズに合わせてカスタマイズすることもできます。これらのプログラムは、学校やコミュニティなど、ユーザーがどこにいても安全を確保するのに役立ちます。

脅威の認識

教職員や児童生徒が脅威を認識できるようにトレーニングすることは、安全を守るうえで不可欠です。子どもたちは真偽の判別能力が乏しいため、脅威と脅威でないものを見分ける方法を教えることが重要です。発見・報告する方法を理解すべき脅威にはいくつかの種類があるため、管理者は、効果が最も大きいと思われるトピックに焦点を当てる必要があります。トレーニングで重要なのは、単に脅威を認識するだけでなく、行動を起こすようユーザーに教えるということです。ユーザーが認識すべき一般的な脅威には、ランサムウェア、フィッシング、ソーシャル エンジニアリング、マルウェア、詐欺などがありますが、自身の教育機関で特定の脅威が蔓延している場合、学校コミュニティがそれらについて知識を身に付けておくことには意義があります。

データとファイルの安全な共有

教職員は、ファイルやデータを適切に共有する方法はもちろん、メールによる不適切な要求を認識する方法についてトレーニングを受ける必要があります。特に重要なのは、機密性の高い個人情報は必要な場合にのみ共有または処理されるようにすることと、データに対する保護レイヤを強化することです（メールでの共有や外部関係者との共有は決して行わないなど）。データ損失防止機能（ChromeOS および Google Workspace for Education で提供）を使用すれば、エンドユーザーがセンシティブ データ（社会保障番号など）を含むファイルを共有したり、機密コンテンツをコピーしてドメイン外に貼り付けたりしないよう警告し、防止できます。

Google のアプローチの実践: 教育機関向けのデバイスとサービス

学校や自治体が自らを保護できる最も強力な手段の 1 つは、ソフトウェアの調達です。ソフトウェアは、脆弱性のリスクを最小限に抑えられるよう堅牢に設計および構築され、すべてのレイヤにセキュリティが組み込まれている必要があります。学校に安全なソフトウェア、またはセキュリティに関して実績のある企業のソフトウェアを購入するよう求めることで、幅広いサイバーリスクを大幅に低減できます。たとえば Google では、ChromeOS のセキュリティを強化するとともに、機械学習、クラウド、ID に関する専門知識の強みを活かした、よりプロアクティブでインテリジェントなソリューションの開発に努めています。

Google は、児童生徒と教職員のプライバシー保護ならびに教育機関向けの優れたセキュリティ対策を両立させるプロダクトの構築に全力で取り組んでいます。Google for Education のプロダクトとサービスは、ますます複雑化する脅威からユーザー、デバイス、データが常に保護されるため、安心してご利用いただけます。このセクションでは、学校の IT 管理者が Google for Education プロダクトを使用する際のセキュリティに関する推奨事項を紹介します。

Google Workspace for Education

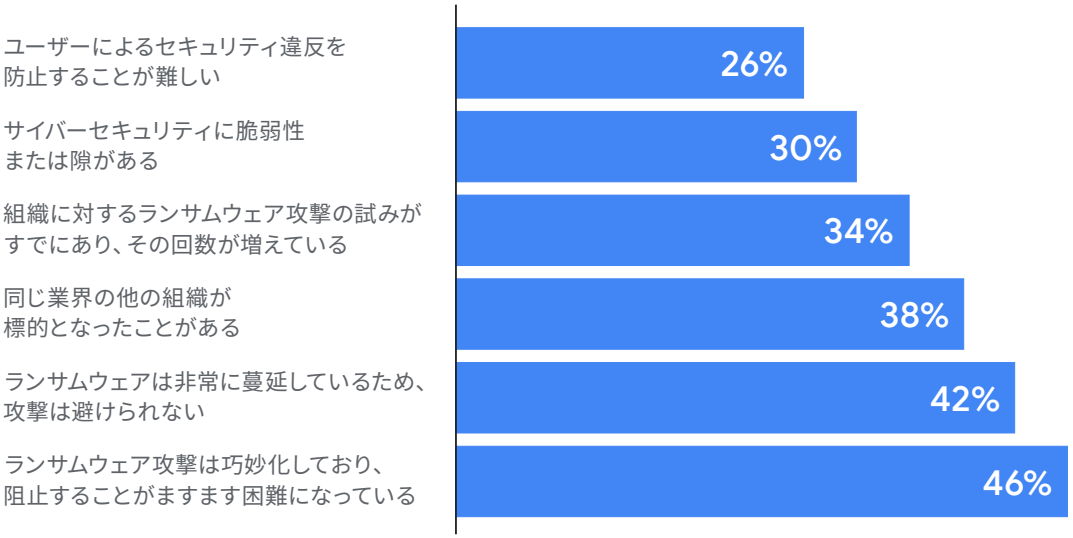
Google Workspace for Education は、学校での共同作業、指導の効率化、安全な学習環境の維持を目的にカスタマイズされた Google ツールとサービスのセットです。Google for Education のプロダクトとサービスでは、ますます複雑化する脅威からユーザー、デバイス、データが常に保護されます。また、アラートとセキュリティ センター、Vault による電子情報開示、Identity and Access Management、データ損失防止（DLP）などのツールも使用できます。

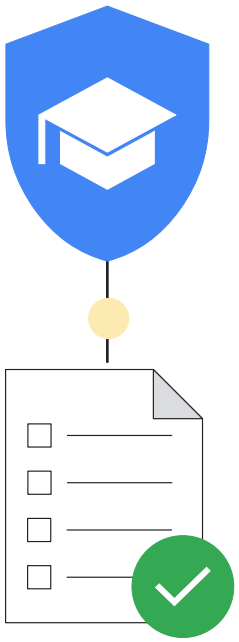
Google Workspace for Education を初めて使用する場合に役立つ資料をまとめましたので、このガイダンスの推奨事項に沿って設定を進める際にご活用ください。Google Workspace for Education の使用を開始するにあたってサポートが必要な場合は、クイックスタート IT 設定ガイドをご覧ください。

セキュリティ チェックリスト

参照セクションで提供されているセキュリティ チェックリストで、教育機関のセキュリティとプライバシーを強化する方法をご確認ください。Google Workspace for Education Standard エディションおよび Plus エディションを使用している学校の場合は、セキュリティの状況ページで Google 管理コンソール設定の構成を監視することもできます。たとえば、自動メール転送、デバイスの暗号化、Google ドライブの共有設定といった設定の状況を確認できます。必要に応じて、セキュリティに関する一般的なガイドラインやベストプラクティスに基づいてドメインの設定を調整し、これらのガイドラインを組織のビジネスニーズやリスク管理ポリシーとすり合わせることができます。

教育分野への攻撃が予想される理由





出典: https://assets.sophos.com/X24WTUEQ/at/g523b3nmgcfk5r5hc5sns6q/sophos-state-of-ransomware-in-education-2021-wp.pdf

Google Workspace for Education に組み込まれている保護機能を最大限に活用するうえで役立つその他のヒント

組織部門（OU）の設定

Google Workspace for Education アカウントの全員が同じ設定を使用する必要があることに異論がある人はいないでしょう。組織部門とは、ユーザー グループのことで、それぞれに異なるサービス、設定、権限を適用できます。たとえば、教職員には 2SV を使用し、小学校低学年以下の児童生徒には年齢にふさわしい認証を使用するなどです。教職員、児童生徒に対して個別の組織部門を設定し、各ユーザー グループに専用のポリシーを適用します。

Google Workspace for Education アカウントを効率的かつ柔軟に管理するには、組織を適切に構成することが重要です。

パスワード ポリシーと管理者アカウントの保護機能の設定

すでに説明したように、ユーザー認証は教育機関を安全に保つための重要な要素です。そのため、Google では管理者が認証を柔軟に管理して、ユーザーのアカウントを適切かつ安全に保護できるようにしています。

ユーザーが安全なパスワードを作成できるようにパスワード ポリシーを設定し、「安全なログイン」セクションの推奨グループを参考に、必要に応じて 2SV の使用を求めることを検討します。特定のユーザー グループに 2SV の使用を義務付けて（設定する時間枠を用意）、セキュリティ キー（最も安全）、Google からのメッセージ（Android や iOS で Google アプリを使用）、確認コード生成アプリ（Google 認証システムなど）、テキスト メッセージや通話（最も安全性が低い）など、さまざまな方法を使用して 2SV を導入できます。

組織で Google 以外の ID プロバイダ（IdP）を使用している場合は、サードパーティの ID プロバイダを使用してシングル サインオン（SSO）を設定できます。必要に応じて、特権管理者以外のアカウントに SSO と 2SV を使用することも可能です。

サービスの有効と無効の設定

ユーザーが Google Workspace for Education アカウントでアクセスできる Google サービスは、管理者が Google 管理コンソールで制御できます。Google カレンダー、ドライブ、Google Meet などの Google サービスへのアクセスを制御するには、組織部門（OU）ごとに各サービスを有効または無効にします（グループを使用してサービスを有効にすることもできます）。また、YouTube、Google マップ、Blogger などの追加サービスを有効にする際は、事前に Google Workspace for Education のコアサービスと追加サービスの違いを確認します。

管理者は、年齢に基づいて Google サービスへのアクセスを設定することが推奨されています。18 歳未満として指定されているユーザーが Google Workspace for Education アカウントにログインすると、一部の Google サービスの利用が自動的に制限される点に留意してください。 また、コンテキストアウェア アクセス（Google Workspace for Education および Plus で利用可能）を使用して、デバイスの IP アドレス、アクセス元の地域、セキュリティ ポリシー、または OS に基づき、Gmail、ドライブ、カレンダーなどの Google アプリへのアクセスを許可またはブロックすることもできます。たとえば、特定の国 / 地域の会社所有のデバイスにのみパソコン版ドライブへのアクセスを許可できます。

ユーザーにサービスへのアクセスを許可する方法

Google 管理コンソールを使用して、ある組織部門に対して Google ドライブなどの Google サービスへのアクセスを無効にできます。ただし、その組織部門にドライブを使用する必要があるユーザーがいる場合は、次のどちらかの方法で対応します。

1. 該当のユーザーをドライブが有効になっている組織部門に移動する。
2. 該当のユーザーをアクセス グループに追加し、そのグループに対してドライブを有効にする。組織部門でサービスが無効になっていても、グループの各メンバーはサービスにアクセスできます。

組織部門 1 と組織部門 2 に対して
Google ドライブが無効になっている

アクセス グループを使用

ただし、組織部門 1 と組織部門 2 の
一部の**ユーザー グループ**は Google ドライブを利用できる

出典: https://support.google.com/a/answer/9050643?sj id=4805599982673626852-NA

データ共有ポリシーと保持ルールの設定

管理者は、ユーザーが Google ドライブのファイルやフォルダを組織外のユーザーと共有できるかどうかを制御できます。これにより、意図しない、または必要以上に広範なデータやファイルの共有を防ぎ、データ漏洩を防ぐことができます。攻撃者がアカウントに侵入した場合にネットワーク間を移動できないようにするには、ファイルやドライブの分離、組織部門の作成、最小権限の原則に基づく運用が不可欠です。潜在的な攻撃者がアクセスできるデータやネットワークの範囲が狭いほど、被害は少なくてすみます。

児童生徒に対しては、外部とのファイル共有を無効に（または外部との共有を許可したドメインのみに制限）して、「アクセス チェッカー」を [受信者のみ] に設定します。一部またはすべてのユーザーに対してドメイン外のユーザーとのファイル共有を許可している場合は、そうした共有時の警告表示を有効にします。また、ウェブ上へのファイルの公開を無効にして、外部の共同編集者には Google アカウントでのログインを義務付けます。

さらに、Google Workspace for Education および Plus をご利用の場合は、対象グループと信頼ルールを使用して、より詳細なレベルで共有に関する推奨事項と制限を設定できます。たとえば、対象グループを使用すると、教職員がリンクを共有する場合のデフォルトの対象を教育機関の全員ではなく「教職員」に設定できます。信頼ルールを使用すると、小学校低学年の児童生徒が高学年の児童生徒とファイルを共有しないようにブロックできます。

共有ドライブのポリシーを確認して、適切なユーザーのみが共有ドライブを作成できるようにし、共有ドライブに外部ユーザーがアクセスできないようにします。共有ドライブの作成は管理者（または教職員）のみに許可し、共有ドライブへのアクセスを注意深く管理することをおすすめします。

- 可能であれば、ディレクトリの公開と連絡先の共有を制限することを検討します。具体的には、一部またはすべてのユーザーに対して連絡先の共有を無効にするか、カスタム ディレクトリを作成して誰がどのユーザーを参照できるかを制限します。
- ドライブや Gmail でデータ損失防止（DLP）ポリシーを設定し、機密情報を検出してブロックします。一般的な機密情報（銀行番号やクレジット カード番号など）の保護に活用できる、定義済みのポリシーが用意されています。また、キーワード、単語リスト、正規表現（Regex）に基づいて、カスタム ポリシーを作成することもできます。

Gmail 設定の管理

Gmail は、Google Workspace for Education の（以下、Google Workspace）コアサービスの 1 つで、教育機関とユーザーを保護するために活用できる管理者向けの設定が数多く用意されています。

Gmail 認証では、迷惑メール、なりすまし、フィッシングを防止できます。承認されたすべての送信者に対して送信者の認証を求めたり、内部の送信者に対する迷惑メールフィルタの適用除外を無効にしたりするなど、迷惑メールフィルタの設定をカスタマイズできます。

可能な場合は POP / IMAP アクセスを無効にして、メール配信前のスキャンの強化とフィッシングやマルウェアに対する高度な保護を有効にします。一部またはすべてのユーザーに外部へのメール送信を許可する場合は、外部の宛先に関する警告を有効にすることもできます。

Google Workspace for Education Standard および Plus では、セキュリティ サンドボックスを使用して有害な添付ファイルを検出するルールを設定することで、マルウェアやランサムウェアから保護することも可能です。

サードパーティのアプリケーション

API を介してアカウント データにアクセスするサードパーティ アプリケーションについては、組み込みの承認ワークフローを使用して承認します。こうすることで、学校での使用が承認されていないサードパーティのアプリケーションとデータが不正に共有されるのを防ぐことができます。

セキュリティ センターの活用

Google Workspace for Education Standard および Plus では、セキュリティ センターを活用して、セキュリティに関する高度な情報とインサイトを取得し、ドメインに影響を与えるセキュリティ上の問題をより詳細に分析して管理できます。

セキュリティ センターの機能であるセキュリティ調査ツールでは、フィッシング攻撃、不適切なファイル共有、ユーザーやデバイスの不審なアクティビティなど、セキュリティとプライバシーに関する問題を特定し、優先順位を付けて対処することができます。

レポートと監視

管理者は、Google 管理コンソールでレポートやログイベントを確認して、潜在的なセキュリティ リスクなどの組織内のアクティビティのほか、誰がいつログインしたか、ユーザーがどのようにコンテンツを作成、共有しているかを把握できます。グラフと表では、ドメインレベルのデータだけでなく、ユーザーレベルの詳細データを確認できます。レポートや監査ログを使用（アラート センターを含む）すると、セキュリティ リスクの特定、サービスの使用状況の分析、設定に関する問題の診断、ユーザー アクティビティの追跡などを行えます。

Google Workspace for Education Standard および Plus では、セキュリティ ダッシュボードを活用して、ドライブでのファイル共有、Gmail でのスパム、フィッシング、マルウェアのアクティビティ、ユーザー アカウントの不審なログイン、デバイスの不審なアクティビティなど、さまざまなセキュリティ レポートの概要を確認したり、傾向を把握したり、現在と過去のデータを比較したりできます。使用状況ログ、アクティビティ ログ、監査ログ（管理コンソール、ドライブ、Google Meet、Google Chat のログイベントを含む）およびセキュリティ レポートの多くは 6 か月間利用可能です。

Google Workspace は世界で最も安全なクラウドネイティブのコミュニケーションおよびコラボレーション スイート

0	1/2 に減少	2/5 に減少	50%
2021 年 11 月以降に Google Workspace で積極的に悪用されたソフトウェアの脆弱性*	組織で Google Workspace を利用した場合のセキュリティ インシデント件数（Microsoft 365 との比較）	組織で Google Workspace を利用した場合のセキュリティ インシデント件数（Microsoft Exchange との比較）	Google Workspace の使用により削減が見込まれるサイバーセキュリティ保険料

*CISA の調査では、この分野の他の生産性ツールベンダーと比べて大幅に少ない。

Chromebook

Chromebook は、セキュリティ機能が最初から組み込まれているため、児童生徒や教職員にとって安全性が高く拡張可能で使いやすいパソコンとなっています。また、企業、学校、個人向けの ChromeOS デバイスでランサムウェア攻撃が報告されたことは一度もありません。Chromebook では、最新の機能によって、進化し続ける脅威から学校を保護します。また、アップデートはバックグラウンドで自動的に行われるため、ユーザーはすぐに作業に戻れます。

OS とアプリケーションの自動アップデートと組み込みのマルウェア対策

攻撃者は常に、オペレーティング システム、ブラウザ、一般的なアプリのバグや抜け穴を利用して、マルウェアをインストールし、ユーザーデータを盗み出そうとしています。セキュリティ アップデートによりデフォルトで安全に設計されている Chromebook では、管理者とユーザーを保護するため、OS とアプリケーションが最新の状態に維持されます。また、クラウド アプリケーションは、ローカルアプリのようにソフトウェアを更新する必要がありません。

さらに、Chromebook には Google が設計したセキュリティ チップが搭載されており、ユーザー ID が保護され、デバイスの安全性とシステムの整合性が確保されます。

また、組織のすべての Chromebook で最新のマルウェア対策のアップデートが自動的に実行されます。データの暗号化、確認付きブート、サンドボックス化、自動アップデートなどの組み込みのセキュリティ機能により、児童生徒と教職員をサイバー脅威から保護します。

ユーザーデータの保護

Google アカウントを使用して Chromebook にログインすると、すべてのデータが暗号化された状態で保存されます。デバイスを使用する他のユーザーにデータを見られたり、アカウントを使用してアプリケーションにログインされたりすることはありません。つまり、児童生徒は教室内で簡単かつ安全にデバイスを共有することができ、学校はコンピューティングの総コストを削減できます。

より高度なセキュリティ機能をお求めの場合は、きめ細かな管理が可能なデバイス管理ライセンスの Chrome Education Upgrade をご利用いただけます。

ユーザーが管理するリモート デバイスのセキュリティ ポリシー

学校の管理者は、Google 管理コンソールを使用して ChromeOS ポリシーを設定し、アプリケーションをリモートでインストールおよび更新できます。ボタンをクリックするだけで、1 人の IT 管理者が数十万台の Chromebook のポリシーや構成を瞬時に更新できます。

ポリシーを使用してできること

- 学校が承認したコンテンツとアプリケーションにのみ児童生徒がアクセスできるようにする
- すべてのアプリケーションと拡張機能を更新して、最新のセキュリティ修正を適用する
- ユーザーが学校のデータをデバイス外にコピー、転送、共有できないようにする
- Google が個別に提供するセキュリティ上の脅威に対処するためのセキュリティ提案を参考にして、データに基づく意思決定を行う
- 管理コンソールですべてのユーザーのセキュリティと ID とアクセス管理ポリシーを一元管理する

管理者に特に設定をおすすめするポリシー

デバイス ポリシー

- **ゲストモード**
  デバイスのゲストモードを無効にする、つまり児童生徒や教職員が匿名でデバイスを使用するのではなく、自身の認証情報を使用してログインするよう義務付けることをおすすめします。
- **ログイン制限**
  児童生徒や教職員が個人の Gmail アカウントを使用して学校の Chromebook にログインしないようにする場合は、児童生徒専用のデバイスを Google Workspace ドメインのみに限定するようログイン制限を適用できます。
- **ユーザーとデバイスに関するレポート**
  Chromebook の使用頻度、使用者、ハードウェアの状態に関する指標を収集できるように、ユーザーとデバイスのレポートを有効にすることをおすすめします。
- **自動再登録**
  学校が所有する Chromebook は、管理者がデプロビジョニングした場合を除き、学校に保管することが重要です。Chromebook がワイプされた場合や物理的に盗まれた場合でも常に再登録されるように、Chromebook の自動再登録を有効にすることをおすすめします。

ユーザー ポリシー

- **シークレット モード**
  児童生徒が学校の Chromebook を使用する際に問題なく動作するように設定する必要があります。たとえば、認証済みブラウザを使用するよう制限して、ウェブ コンテンツ フィルタにより児童生徒が不適切なウェブサイトにアクセスできないようにします。また、管理者は、児童生徒がウェブフィルタを回避できないように、シークレット モードを無効にする必要があります。
- **プロキシモード**
  学校でプロキシを使用してウェブ フィルタリングを行っている場合は、ユーザーがプロキシ設定を変更できないようにする必要があります。
- **マルチログイン アクセス**
  ユーザーが学校の Chromebook や Google Workspace アカウントを使用しているときに予備アカウントにログインすることが許可されている場合、児童生徒や学校の機密性の高いデータや情報が予備アカウントに簡単に流出する恐れがあります。管理者はマルチログイン アクセスをブロックすることを検討してください。
- **ブラウザの履歴**
  ブラウザの履歴を削除できないようにすることが児童生徒にとってメリットとなる場合があります。インターネット セキュリティに関するインシデントが発生した際に、それらのインターネット履歴のログが調査に役立つ可能性があるためです。

上記のリストは、重大なサイバー インシデントにつながる、最もよくある種類のミスからネットワークを確実に守る土台となるものです。その他の推奨されるセキュリティ ポリシーについては、セキュリティ チェックリストをご覧ください。

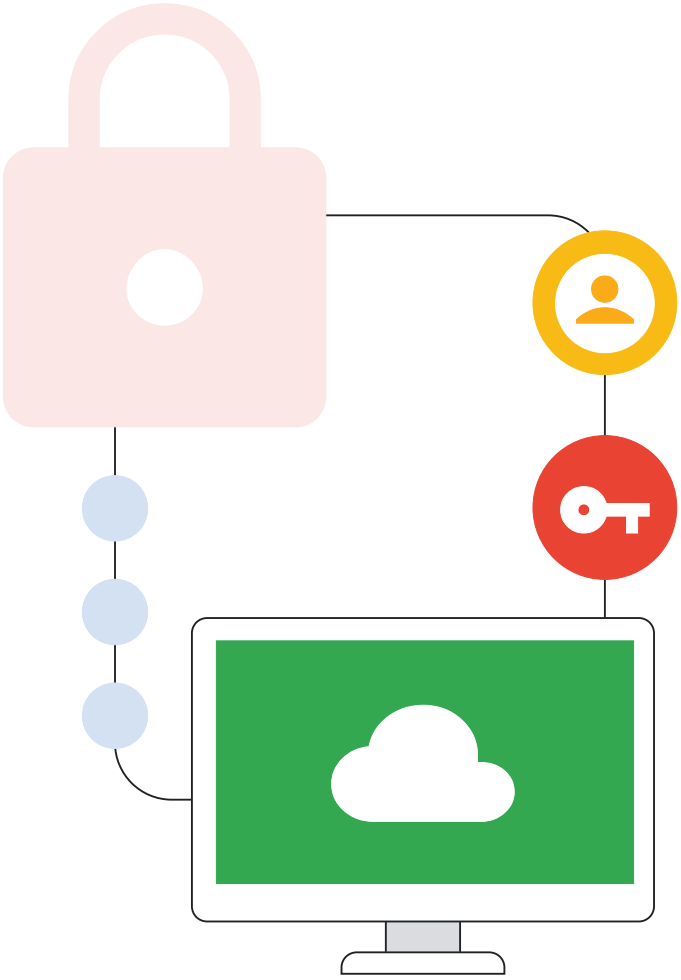
いつでもどこでも安全に使用するための エンドポイント管理

ChromeOS のリモート ポリシー管理システムにより、学校の管理者は、学校のネットワーク サーバーではなく、デバイス上でセキュリティ設定を適用し、コンテンツ フィルタリング システムなどのセキュリティ ツールを実行できます。これにより、児童生徒は学校の Chromebook を自宅で使用するときも、教室内と変わらないセキュリティで保護されます。デジタル教科書やオンライン学習ツールへの移行が進み、児童生徒が宿題をするためにデバイスを自宅に持ち帰る機会が増える中、このようなセキュリティ管理はますます重要になります。

まとめ

小中高の教育機関をサイバー インシデントから保護するという課題は、複雑な取り組みではあるものの、児童生徒、教職員、管理者、ひいては広範なオンライン エコシステムを守るうえで十分に価値ある投資といえます。このドキュメントで紹介した内容を参考に、各学校は独自のニーズに合わせて推奨事項を取り入れ、進化する脅威の状況や新たなテクノロジーに継続して対応する必要があります。小中高の教育機関におけるセキュリティ プログラムの強固な基盤として、また次の一歩と実装可能な項目のリソースとしてぜひご活用ください。

Google では、このガイドブックの内容や AI のような新しいテクノロジーについても、学校や組織で活用できるさまざまなリソース、トレーニング、熟練したサイバーセキュリティの専門家を有しています。また、このドキュメントで説明している多くのサイバーセキュリティの問題を解決できる、教育機関向けの市販プロダクトを提供しています。セキュリティ プログラムの設計と実装にサポートが必要な場合は、お問い合わせください。



リソースリスト

小中高の教育関連テクノロジーと関連リスクの状況に関する考察

米国政府機関の報告書

- CISA の報告書「Protecting Our Future(未来を守る)」では、小中学校が直面しているサイバーセキュリティ リスクを調査し、学校でのリスク対応に役立つサイバーセキュリティに関するガイドラインを含む推奨事項を提供(2023 年 1 月公開)
- CISA の勧告「Cyber Actors Target K-12 Distance LearningEducation to Cause Disruptions and Steal Data(小中高の遠隔教育を標的に混乱を引き起こしてデータを盗むサイバー攻撃者)」によると、教育機関はサイバー攻撃の最大の標的となっている(2020 年 12 月公開)
- GAO の報告書「Data Security: Recent K-12 Data BreachesShow That Students Are Vulnerable to Harm(データ セキュリティ: 小中高教育機関における最近のデータ侵害により示された、悪意に対する生徒の脆弱性)」(2020 年 10 月 15 日公開)
- CISA、FBI、MS-ISAC が共同で勧告をリリース

  ランサムウェア攻撃の「Vice Society」に関する勧告で、一部の脅威アクターが教育分野を重点的にランサムウェア攻撃の標的としていることに注目（2022 年 9 月公開）。Chromebook などのより安全なソリューションにアップグレードすると、セキュリティを強化できます。ChromeOS デバイスでランサムウェアが検出されたことは一度もありません。

教育およびその他の分野におけるサイバーセキュリティの脅威に関する考察

- Sophos の報告書「The State of Ransomware in Education 2023(教育分野におけるランサムウェアの状況 2023)」では、調査対象の小中高教育機関の 80% がランサムウェア攻撃を受けていたことが判明(2023 年 7 月公開)
- Zscaler の調査によると、フィッシング攻撃は約 1.5 倍に増加しており、教育機関、金融機関、政府機関が主な標的となっている(2023 年 4 月公開)
- 学区でのランサムウェア攻撃に関する記事で、ロサンゼルスの学校へのランサムウェア攻撃について判明している情報を紹介(2022年 9 月公開)
- 別のランサムウェア攻撃では、1 回のサイバー攻撃でアルバカーキの学校が閉鎖を強いられ、授業が中止に(2022 年 1 月公開)
- 最新のメール ハッキングに関する情報で、中国のハッカーが米国の政府機関などのメールを侵害したと Microsoft が公表(2023 年 7月公開)

Google for Education のスタートガイド

Google for Education サービスの利用開始に関する全般的な情報

- Google Workspace for Education クイックスタート IT 設定ガイドでは、教育機関向けの 8 つの設定ステップを紹介
- 教育機関での Chromebook の活用についての詳細
- Chrome デバイス管理の概要ページでは、学校の ChromeOS デバイスの管理者向けのスタートガイドを提供

Google for Education サービスの利用開始に関する全般的な情報

- 中規模および大規模ビジネス向けのセキュリティ チェックリストでは、教育分野に適用可能な Google Workspace for Educationと Chromebook の設定に関するヒントを紹介
- Google Workspace for Education Fundamentals、Standard、Plus エディションの詳細と機能
- Chromebook と Chrome デバイスを接続、登録、管理、更新する方法（英語版）
- Google for Education のプライバシーとセキュリティ センターでは、Google for Education が教育機関の保護にどのように役立つかを詳説

安全な認証の使用

- 2 段階認証プロセスにセキュリティ キーを使用する方法
- パスキーによるパスワードなしのログイン方法について

Google Workspace for Education で以下を設定する方法

- ユーザーのパスワード要件
- サードパーティの SSO ID プロバイダ
- サードパーティの ID プロバイダを使った 2 段階認証プロセスの仕組み

- Chromebook や ChromeOS で 2 段階認証プロセスまたは多要素認証を使ったログインをユーザーに義務付ける方法

リスクの高いユーザー向けのアカウント保護

- Google の高度な保護機能プログラムでユーザーを保護する方法

適切なセキュリティとプライバシー設定の適用

- Google Workspace のデータにアクセスできるサードパーティ製アプリと内部アプリを管理する方法
- 18 歳未満として指定されているユーザーによる未設定のサードパーティ製アプリへのアクセスを管理する方法

Gmail の設定を管理する方法

- 迷惑メール、なりすまし、フィッシングを Gmail 認証で防止する
- Gmail のカスタム迷惑メールフィルタを作成する
- ユーザーに対して POP と IMAP を有効または無効にする、サードパーティ製のメール アプリケーションを使用できないようにする
- メール配信前のスキャンでフィッシングを防止する
- 受信したフィッシング メールやマルウェア メールからユーザーを保護する
- Gmail で外部の宛先に関する警告を表示するかどうかを管理する
- セキュリティ サンドボックスを使用して、有害な添付ファイルを検出するルールを設定する
- 組織部門を追加する方法

Google Workspace for Education サービスを有効または無効にする方法

- Google Workspace for Education のコアサービスと追加サービスの説明
- Google Workspace ユーザー向けにサービスを有効または無効にする方法
- Google サービスへのアクセスを年齢別に管理する方法
- ユーザー ID、地域、デバイスのセキュリティ状況、IP アドレスなどの属性に基づいて、アプリに対する詳細なアクセス制御セキュリティ ポリシーを設定してビジネスを保護する

データ共有ポリシーと保持ルールの設定

- 組織の外部共有を管理する方法
- ユーザーがファイルに付与するアクセスを制限する
- 部署やチームなどの共有対象グループを設定する方法
- ドライブ共有のルールを作成、管理する
- ユーザーに共有ドライブの作成を許可して、デフォルトの共有設定を行う
- 組織内の共有ドライブのメンバーとアクセスレベルを管理する
- ディレクトリを有効または無効にしてアクセスを管理する
- 組織内のチームやグループのディレクトリをカスタマイズする
- データ損失防止(DLP)ポリシーを使用して機密情報を保護する

システムの更新とアップグレード

- ChromeOS デバイスの更新を管理する方法
- Chrome は、エンタープライズ グレードのセキュリティと管理機能を備えた、管理しやすい最新のブラウザ
- Chrome OS Flex は PC と Mac 向けの安全かつ高速で管理しやすいクラウド ファーストのオペレーティング システムで、既存のデバイスをモダナイズ可能

リアルタイムのアラートとモニタリング システムの使用

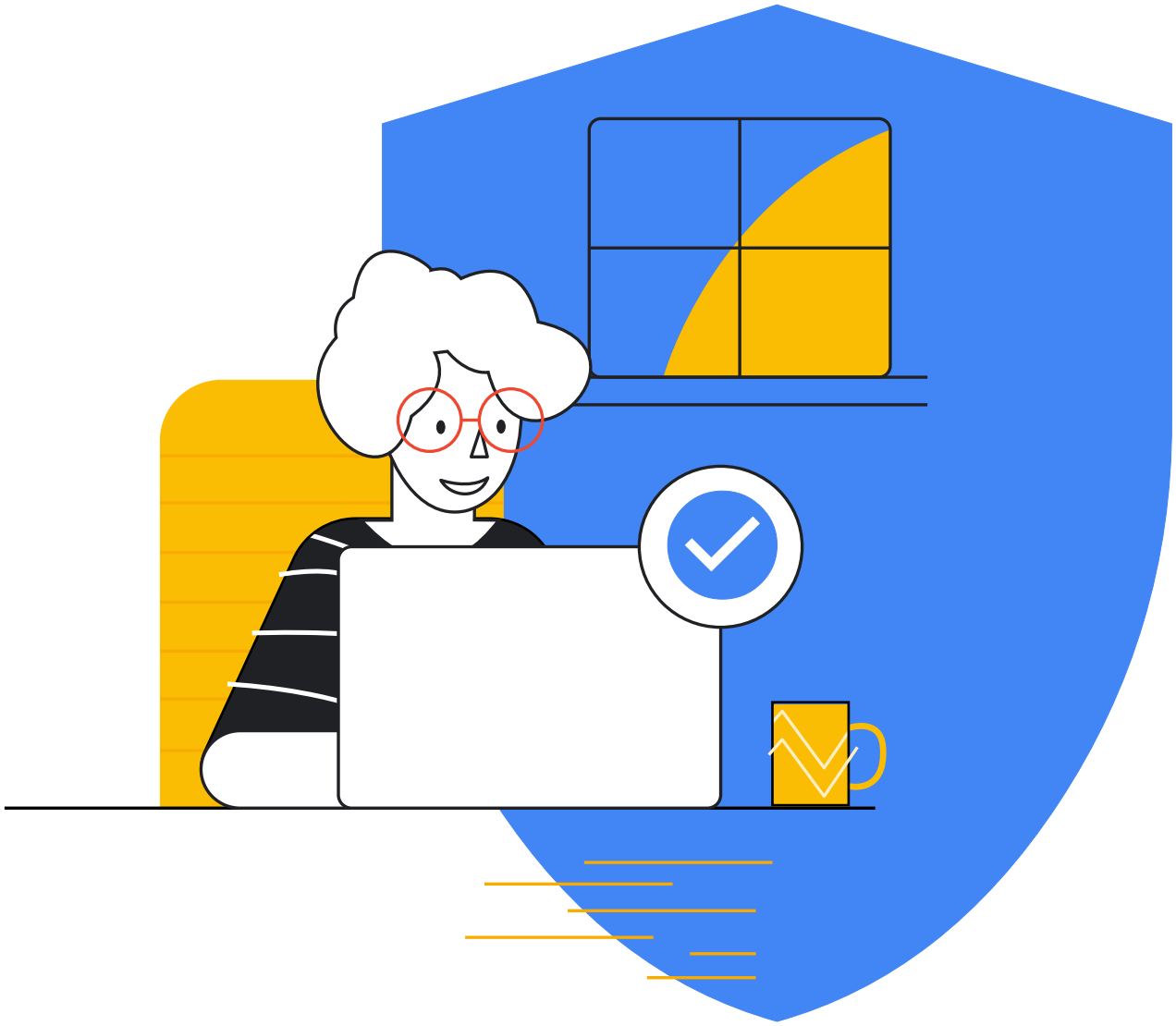
- Google 管理コンソールを使用した ChromeOS フリート モニタリングのベスト プラクティス

Google Workspace のアラートとモニタリング

- 使用状況やセキュリティに関するレポートを確認してセキュリティ リスクを特定し、ユーザーのアクティビティを追跡する方法について
- アラート センターの使用方法と、アラート センターと管理者へのメールアラートの違いについて
- セキュリティ ダッシュボードの使用方法について(よくある質問の回答も含む)
- 高度な分析とセキュリティに関する問題の詳細な把握を可能にする Google Workspace セキュリティ センターについて
- セキュリティ調査ツールのダッシュボード レポート、調査ツール、セキュリティの状況ページを活用してセキュリティとプライバシーの問題を特定し、対処する方法について

教職員や児童生徒のトレーニング

- Google セーフティ センターではオンラインでの安全性を保つためのヒントを紹介
- 子どもたちが安全に、自信を持ってオンラインの世界を探検できるよう支援するサイト
- Khan Academy では無料のオンライン コース(オンライン セキュリティに関するものを含む)を提供



Google for Education