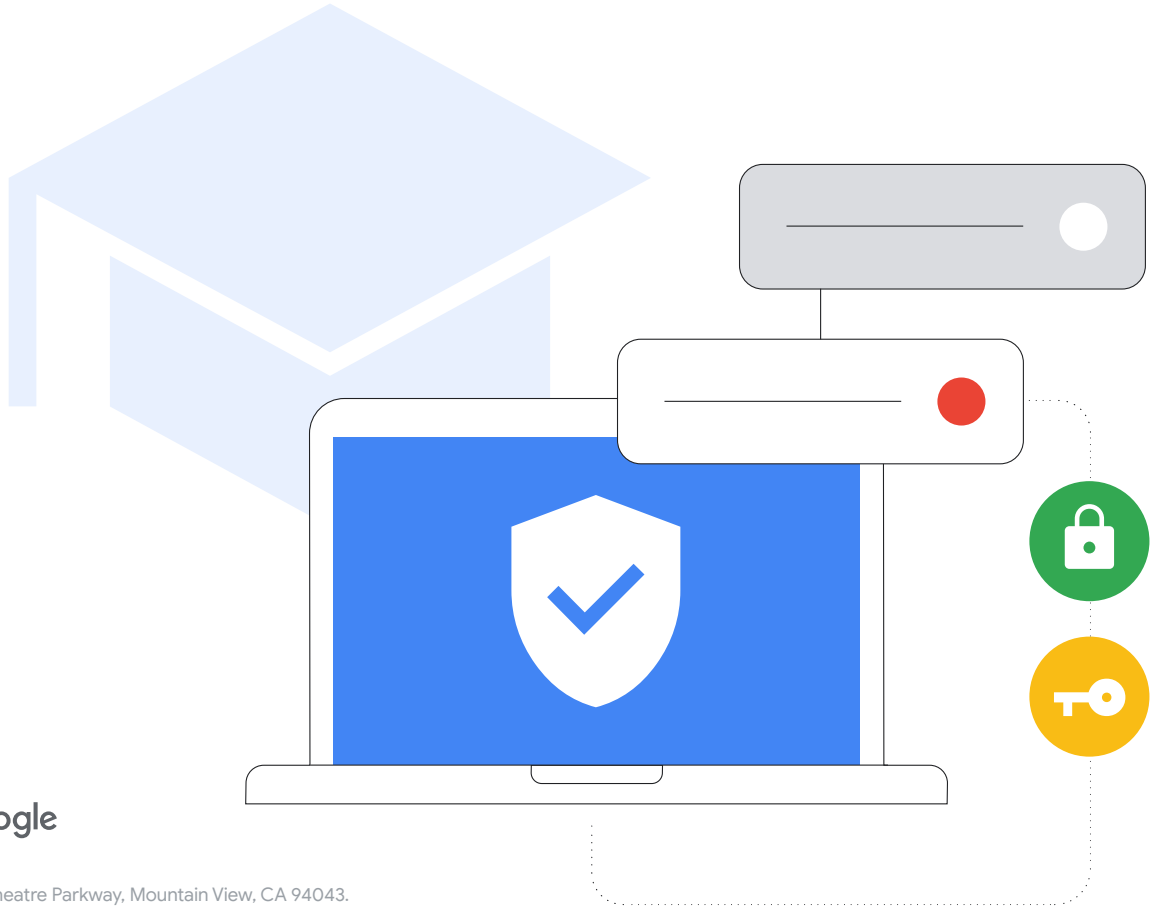
Google for Education

小学校、中学校、高等学校向けサイバーセキュリティ ガイドブック



Safer with Google

エグクティブ サマリー

CISA（サイバーセキュリティ インフラストラクチャ セキュリティ庁）の「Protecting Our Future（未来を守る）」[1] レポートで示されているとおり、生徒や家族、教職員、コミュニティを保護するための小中高教育機関によるサイバーセキュリティへの投資は極めて重要です。このドキュメントでは、学校の IT 管理者が小中高教育機関において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の両方が含まれます。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、私たち Google for Education チームが教育・学習支援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、チームの取り組みの中で得られた教訓について紹介します。

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対す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提供する詳細なガイダンスは、特定のプロダクトやサービスを対象にしたものではありません（Google のプロダクトには、一般的な攻撃に対する優れた保護機能が組み込みで備わっています）。

リスク

教育機関はサイバー攻撃の最大の標的です。不正行為をする 者は、データが豊富な学校環境を悪用して自らの利益を得ようと企んでいます。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ます。まだ標的にされていない学校の 46% が、いずれ自分たちが攻撃を受けるだろうと考えています。また、これらの学校のうちの 42% が、蔓延しているランサムウェアによる攻撃は避けられないものと思っています。2020 年に学校が遠隔学習に急速に移行する必要があったことがサイバーセキュリティ ギャップを大きく助長し、学校は攻撃に対して脆弱な状態のままとなっています 。

防御

こうした攻撃は軽減できます。また、リスクを完全に排除するテクノロジーはありませんが、教育分野と EdTech ベンダーが協力してベスト プラクティスを採用し実装することで、セキュアで安心かつ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ができます。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、教育機関では効果的にリスクを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。特に、IT 管理者や機密情報を扱う担当者は、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、可能な限りユーザー認証のベスト プラクティスを使用します。
- **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 プロダクトは、デフォルトでセキュリティを確保するよう構築されていますが、管理者がネットワークやシステムを適切に活用。構成し、セキュリティを確保することも重要です。学校を安全に保つためには、ゼロトラストと最小権限の原則を適用します。作業を効果的に行うために必要なソフトウェア、データ、アプリケーション、システムにのみユーザーが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確実に保護します。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、ユーザーが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）を実行していること、それらが自動的に更新され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ことで、セキュリティを強化することができます。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。
- **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。これらの機能は、Google Workspace for Education などの主要なコラボレーション / コミュニケーション ソフトウェアに組み込まれているものを使用できるほか、別のセキュリティのロギングとモニタリング ソリューションを導入して使用することもできます。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、データ全体にわたって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攻撃）、デバイスのアクティビティ、構成の変更をモニタリングします。アラートとモニタリング ソリューションを最新状態に保ち、脅威、重大なイベント、システム変更に関する通知を受け取ります。
- **教職員や生徒のトレーニング:** 最も一般的な攻撃に対する防御策として、デバイスやソフトウェアの安全な使用方法、潜在的な脅威の認識と報告方法、データの適切な共有方法についての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てブランド化し、無料で利用できる既成の資料と併用して、学校用の包括的なツールキットとします。

[1] https://www.cisa.gov/protecting-our-future-cybersecurity-k-12

Google プロダクトのユーザーに特化した推奨事項: 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が強化されるだけでなく、上記の推奨事項をそれぞれ簡単に実装できます。これらを組み合わせることで、ユーザーのプライバシーを保護し、教育機関向けの最高水準のセキュリティ機能を提供する包括的なソリューションを実現します。

こうした戦略とこれから示す資料で提供される追加のガイダンスを併用することにより、小中高教育機関向けの優れた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

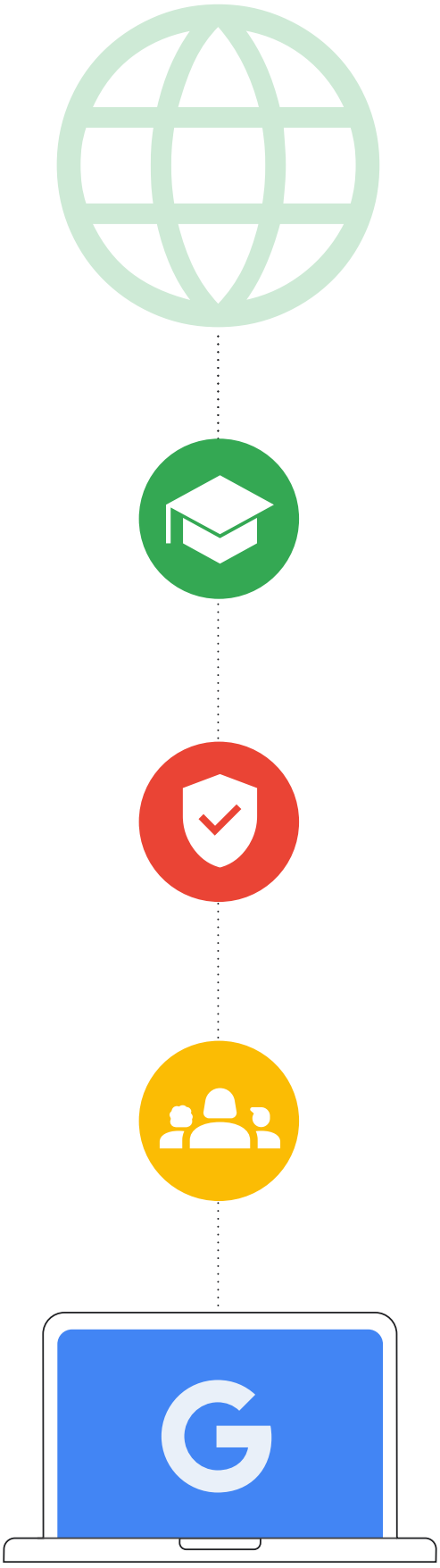
Google は、「世界中の情報を整理し、世界中の人々がアクセスして使えるようにする」という使命を掲げていますが、これは教育分野においても変わりません。Google for Education チームでは、この取り組みにおいて Chromebook や Google Classroom などのツールを構築しています。生徒と教師はこれらのツールを使い、簡単かつ安全に独自のコンテンツを作成、共有、整理したり、教育リソースやオンライン ツールにアクセスしたりでき ます。

学校には、デフォルトでセキュリティが確保されていることはもちろん、プライバシーを重視した設計でユーザー自身がプロダクトを管理できる、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 などのソリューションによって、世界の厳しい教育基準に準拠した最高水準のセキュリティが学校にもたらされます。IT 管理者は完全に可視化されたデータとセキュリティ ポリシーを容易に制御でき、生徒は、スパムやサイバー脅威を監視しながら年齢に基づいたコンテンツを提供する安全なデジタル環境で学習に専念できます。

誰もが安全に学習できるよう、私たちのチームは、組み込みのセキュリティと制御機能、最高レベルのプライバシー基準、さらにプロアクティブなセキュリティ ツールのオプションを優先的に導入してきました。ChromeOS デバイスは、学校が直面するサイバー攻撃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ためです。

一方、Google Workspace for Education は、世界で最も人気のある安全なクラウドベースのコミュニケーション / コラボレーション スイートの 1 つです。ここに記載の推奨事項に関連する個々のサイバーセキュリティ保護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。1 つ目のセクションでは、小中高教育機関向けの、プロダクトを問わない実用的で一般的なセキュリティ ガイダンスを扱います。2 つ目のセクションは、Google Workspace for Education や Chromebook などの Google for Education プロダクトを使用する教育機関向けの、具体的な設定に関するガイダンスです。両セクションともに、教育機関と生徒のオンライン上の安全を守るための情報を提供しています。



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。そのため、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損失（データ、サービス、リソース、時間、金銭面で）を防ぐために、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）。

このガイドは、セキュリティ環境を強化するために、学校管理者や学校システムが実装す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ためのツールです。これらのベスト プラクティスを実装することで、小中高の教育機関は、教育システムに対する深刻で高額なサイバー攻撃を軽減・防止し、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、頻度も深刻度も増加しています。K-12 Cybersecurity Resource Center によると、2016〜2021 年に教育機関が関係するサイバー インシデントとして公表された件数は、50 州すべてで 1,300 件以上にのぼります。今日の教育機関のリーダーは、生徒や教職員のデータと個人情報とともに、教育機関のシステムと情報を保護する必要があります。中でも、従来より教育分野が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が成功すると、個人を特定できる情報（PII）の大規模なデータ侵害や高額な支払い（2020 年以降、身代金の平均支払い額は 5 倍増の 812,260 米ドル）を引き起こし、授業やその他の学校運営に長期にわたって混乱を招く可能性があります。最近では、ランサムウェア攻撃により学校システム全体がシャットダウンし、生徒が何日も学校に通えなくなったことでコミュニティ全体に影響が生じるケースも起きています。リソースや資金が限られている小中高の教育機関ですが、サイバーセキュリティの強化に投資しない限り、格好の標的として今後も狙われ続けることになるでしょう。

ティの強化に投資しない限り、格好の標的として今後も狙われ続けることになるでしょう。サイバーセキュリティを最大限に強化するためには、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必須です。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から作成されています。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。ただし、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実装すべきです。これは、責任ある企業であれば、自社製品およびその変更について最も的確に説明できるためです。

これから述べる推奨事項を実践する前に、以下の要素についてお考えください。

考慮事項:

1. **生徒全体の保護:**
学校ごとにニーズは異なります。一定の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 EdTech ツールには、不適切なコンテンツを制限したり位置情報や連絡先データを非公開にしたりするなど、年齢に基づい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おすすめします。

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、自動更新により、セキュリティの最大化、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、学区、または地域の方針:**
学校には、テクノロジーの使用に関して特定の方針が定められ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

件のフィッシング メールが Gmail でブロックされています。

毎週

30万

件の安全ではないウェブサイトが Google により特定されています。

毎日

7,400 万人

のユーザーが Google のパスワード マネージャーを利用しています。

毎年

7億人

のユーザーがセキュリティ診断を利用してセキュリティを強化しています。

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、侵害要因全体の 48% を占めました。いくつかの重要な推奨事項を実装することで、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するようにできます。

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）の使用を適用して、可能な限り（教育機関のシステムにユーザーがリモート アクセスしている場合は特に）パスワードレス認証（パスキー）に移行する必要があります。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。

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、小中高におけるテクノロジーの利用状況もさまざまです。アカウントとデバイスのセキュリティは、ユーザー ロールと種類（IT 管理者、教職員、割り当てられたデバイスを使用する高学年の生徒、共有デバイスを使用する低学年の生徒など）によって異なり、それぞれベスト プラクティスが定義されています。以下では、各グループの具体的な推奨事項について説明します。

ほとんどの設定でベスト プラクティスとなる認証方法には、いくつかの種類があります。

- **安全なパスワード:**
  初回ログイン時にユーザーに独自のパスワードの作成を要求します。パスワードは長さと複雑さの最小要件を厳密に満たなければなりません。パスフレーズを長くすると、その長さと複雑な文字の使用により、セキュリティの追加要素が提供されます。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 文字だけ更新など）を助長することにつながるためです。
- **2 段階認証プロセス（2SV）:**
  2SV は 2 つ目のステップでアカウントを保護します。多くの場合、セキュリティ キーやスマートフォンの（ワンタイム認証コードを作成する）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、管理者は、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される確認コードの使用は避けるべきです。
- **パスワードレス認証:**
  パスキーは、パスワードに代わるより安全で簡単な方法です。ユーザーは、PIN、パターン、生体認証センサー（指紋や顔認識など）、またはセキュリティ キーのタップを使用して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。これらはすべての教育状況に適しているわけではありませんが、従来の認証形態に取って代わりつつあり、より安全ですばやいログインを可能にしています。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、ユーザーは単一の認証情報セット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。ユーザーが 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、学校が複数のユーザーの認証情報セット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、ユーザーが学校や職場で使用するアカウントやサービス全体にわたって安全な一意のパスワードを作成するのに役立ちます（SSO を使用していない場合）。これらはデバイスのオペレーティング システムへのログインはアシストしませんが、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、ChromeOS、Android でパスワード マネージャーを使用することが可能です。

さまざまなグループの固有のニーズは、教育機関内でのロール、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、上記の認証アプローチの特別なサブセットまたは組み合わせにより満たされます。

学校管理者

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なことです。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、認証におけるゴールド スタンダードを採用する必要があります。これらはそれぞれ保護を強化しますが、組み合わせて使用することで、管理者アカウントと企業向けサービスに特に強力なセキュリティを提供します。

- 管理者は物理的なセキュリティ キー、または信頼できるデバイスとプロンプトを必須とする暗号化された 2 段階認証プロセスを使用してください。これには、Google 認証システムや、ワンタイム認証コードを生成する別のアプリなどのサービスがあります。2019 年以降に TPM チップを搭載してリリースされた Chromebook には、2 要素認証に使える電源ボタンがあります
- 管理者は、2SV をサポートする信頼できるパスワード マネージャーを使用して、さまざまなサービスのパスワードを保存する必要があります。

割り当てられたデバイスを使用する教職員

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の管理は行わず、代わりにさまざまな技術に触れる機会があります。

- 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フィンガープリント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。
- 管理者は、可能な場合や職員が教育機関のシステムにリモート アクセスする場合は、2SV の使用を適用して、パスワードレス認証に移行します。

割り当てられたデバイスを使用する高学年の生徒 (通 常、小学 4 年生以上)

高学年の生徒は自身を守る方法について学んでいるため、通常、使用する可能性の高いサービスの種類に適した、保護が強化された認証メカニズムを使用します。生徒は、自身のアカウントと共有された情報にのみアクセスできるようにする必要があります。

- Chromebook を使用する生徒に対しては、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。生体認証を使う方法は、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。
- 各生徒が、個人情報（氏名、担任、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生徒に教えます。

共有デバイスを使用する低学年の生徒 (通常、小学 3 年生以下)

低学年の生徒は、まだ教育テクノロジーの使い方を学んでいる途中であるため、限られたサービスやデータでの使用に適したシンプルな認証が有益です。

- 低学年の生徒やパスワードでログインできない生徒のために、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安全性の低いパスワード代替手段を使用している学校は、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、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。
- タブレットなどの割り当てられたデバイスの場合、デバイス固有の PIN を代替の安全な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す。サービス、リソース、時間、金銭の損失を防ぐために、可能な限り優れたセキュリティを採用することが極めて重要となります。システム管理者は、それぞれの教育機関が使用するソリューションに適した効果的なセキュリティ機能を実装すべきですが、そのシステムが教職員や生徒にとっても使いやすいものであることを確認する必要があります。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、その他の設定は管理者が保護的なデフォルト値に調整します。繰り返しになりますが、サービス、リソース、時間、金銭の損失を防ぐためには、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。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、個人情報の収集、使用、開示の目的と手段を、サービスを適切に提供するために最低限必要な、もしくは不適切でない程度に制限するようにします（「データの最小化」）。

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、信頼できるソースからのアプリケーションを使用しましょう。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確実にダウンロードしてもらうようにします。OS やハードウェアの変更（脱獄や 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、回避します。

アクセス権と表示設定

管理者は、ユーザーが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、システムにのみアクセスできるようにする必要があります。こうすることで、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。学校所有の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することで、どのユーザーがどのような状況でデータにアクセスできるかを監査し、ユーザーの個人情報などのセンシティブ データやシステム（人事、給与、評価、セキュリティ、構成など）に特別な注意を払うことができます。

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しょう。また、環境外での共有を制限・ブロックし（特に生徒の場合）、機密コンテンツの共有を監視するポリシーも有効にします 。

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、ドキュメントをクラウド環境で管理するなど、デバイスの紛失または盗難に遭遇した場合でも、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計画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しておきましょう。

デバイスの紛失または盗難が報告された場合は、可能であればデバイスをリモートでロックダウンし、それに関連するアカウントもロックダウンするか報告するかして、不正アクセスに使用されないようにします。Chromebook を紛失した場合は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。

リスクの高いユーザーに対する高度な保護機能

標的型オンライン攻撃のリスクが高いユーザーと機密性の高い情報（Google Workspace for Education の管理者を含む）のために、Google は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に対するユーザーの保護を強化します。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。管理者や職員が個人情報や技術システムにアクセスできる場合は、常にそれらの機能を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大切な部分を担っているため、ますますこれが重要となります。教育機関およびリスクの高いその他組織へのマルウェア攻撃のほとんどは Windows ベースのものであり、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 のデータ侵害などが挙げられます。こうした事例からも、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、さらにシステムやアプリケーションが自動的に最新の状態に保たれることで、管理者の作業を効率化できることがわかります。

最新のオペレーティング システムにアップグレードし、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更新を少なくとも毎月ダウンロードしてインストールする必要があります。

ChromeOS で動作する Chromebook では最新のセキュリティ パッチによる自動更新が頻繁に行われるため、常に迅速にセキュリティ イノベーションを導入することができます。また、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。また、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拡大することはありません。

Chromebook に移行する準備が整っていない学校の場合は、教育用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、ChromeOS Flex を使用できます。ChromeOS Flex は、プロアクティブな組み込みのセキュリティ機能とクラウドベースの管理機能を備えており、統合された最新の教育と学習体験をすべての人に提供します。既存のハードウェアを置き換えることなく、自動化された保護機能によって悪意のある実行可能ファイルやアプリをブロックできます。

最新のブラウザにアップグレードし、常に最新の状態に保つ

ブラウザが更新され、安全であることを確認することも重要です。最新のブラウザには高度なセキュリティ機能が備わっており、ユーザー自身で簡単に有効化したり、管理者が教育機関のパソコンでデフォルトで有効になるよう設定したりできます。これにより、インターネット経由で転送される機密情報の安全性が確保されます。ブラウザは 最新の状態に保つ必要があります。そうすれば、仕事や学習やその他のオンライン活動で以下のことが可能になります。

- **堅牢なセキュリティの使用:** これには、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ためのサイト分離やセーフ ブラウジング保護が含まれます 。
- **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行うことができます。
- **接続の安全性の確認:** 最新のブラウザでは Transport Layer Security の使用が定められています。URL の横のマークをクリックすると、接続が安全であることが確認できます。

セキュリティを考慮して構築された Chrome では、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っています。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いるため、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特定し、被害が発生する前に対応することができます。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。収集した大量のデータから異常や特定のパターンを見つけるという AI ツールの極めて優れた特性を利用して、脅威をより迅速・容易に検出し、脆弱性に対処することができます。これにより、IT 管理者や職員がどのアクティビティを優先的に確認すべきかがわかります。

学校は、Google Workspace for Education などの主要なコラボレーション / 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機能を使用することも、別のセキュリティ情報とイベント モニタリング（SIEM）ソリューションを導入することもできます。

リアルタイムのアラートとモニタリング システムが、学校のネットワークやデバイス、アプリケーション、ユーザー、データ全体にわたるさまざまなアクティビティ（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、データ盗難の成功と未遂、管理者のアクティビティなど）を追跡します。

システムが不審なアクティビティを検出した場合、学校の IT 担当者にアラートを送信できるため、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、学校が直面する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、学校は保護を強化するのに役立つ傾向やパターンを特定できます。

.

ここでは、アラートとモニタリング（SIEM を含む）システムを使用するためのベスト プラクティスをいくつか紹介します。

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はどれか、どのような種類の脅威が最大のリスクをもたらすかを特定します。次に、それらの脅威をモニタリングするために収集する必要があるデータを把握します。

2. **適切なデータの収集と適切な構成**
   最も重要なセキュリティ目標に対処するには、適切なデータの収集とアプリケーションの構成が重要です。これには、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 デバイスに加え、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、学習管理システムなどのデータが含まれます。

3. **アラートの調査と対応**
   モニタリング システムがアラートを生成したら、問題を調査し、適切な措置を講じることが重要です。これには、複数のチームを集めてアラートの発生源を調査したり、誤検出かどうかを判断したり、脅威を軽減するための対策（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）を行ったりすることが含まれます。

教職員や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支援し、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。教職員や生徒にセキュリティの重要性について教育することは、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の措置を講じる方法を教えましょう。学校や学区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支援し、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。

デバイスとソフトウェアの安全な使用方法

管理者が、教師や専門家と協力して年齢に応じたサイバーセキュリティのカリキュラムを開発し、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に促してもよいでしょう。学校または学区独自のトレーニング教材を作成することで、教師や生徒に推奨事項を説明できます。また、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、さまざまな場所でユーザーの安全を確保するのに役立ち ます。

脅威の認識

脅威を認識するための教職員や生徒へのトレーニングは、安全を守るうえで大切なことです。子どもたちは、何が正当であるかを知る手段を把握していない可能性があるため、脅威と脅威でないものを見分ける方法を教えることが大切です。彼らが認識し、報告する方法を理解しなければならない脅威にはいくつかの種類があるため、管理者は、費用対効果が最も高いと思われるトピックに焦点を当てる必要があります。重要な点は、トレーニングは単にユーザーに脅威を認識させるだけでなく、行動を起こす必要性を教えるものだということです。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、特定の教育機関内である種の脅威がより蔓延している場合、学校コミュニティがそれらについての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セキュアな共有

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、そしてデータに対する保護を強化する（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）ことです。データ損失防止機能（ChromeOS および Workspace for Education に含まれる）は、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、機密コンテンツをドメイン外でコピーして貼り付けしたりしないよう警告・防止します。

Google の取り組み: 教育機関向けのデバイスとサービス

ソフトウェアの調達は、学区が自らを保護するための最も強力な手段の 1 つです。ソフトウェアは、脆弱性のリスクを最小限に抑えるように堅牢に設計・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や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義務付けることで、幅広いサイバーリスクを大幅に低減できます。Google では、一例として、ChromeOS のセキュリティを強化するとともに、引き続き、機械学習、クラウド、アイデンティティ インテリジェンスの専門知識を活かしたよりプロアクティブで高度なソリューションを展開しています。

Google は、生徒と教師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。信頼性の高い Google for Education のプロダクトとサービスが、ますます複雑化する脅威からユーザーやデバイス、データを継続的に保護します。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について説明します。

Google Workspace for Education

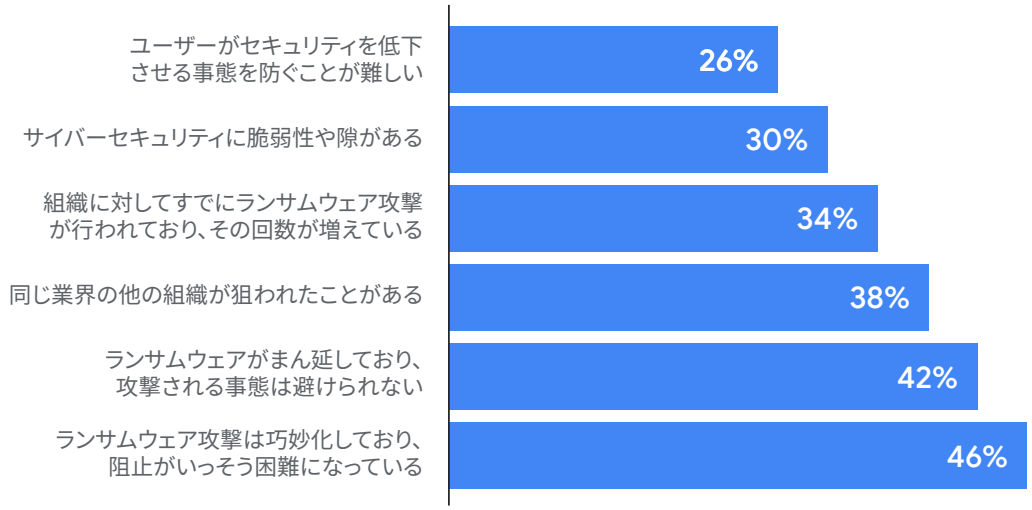
Google Workspace for Education は、学校でのコラボレーション、指導の効率化、安全な学習環境の維持を目的にカスタマイズされた Google ツールとサービスのセットです。Google for Education のプロダクトとサービスが、ますます複雑化する脅威からユーザーやデバイス、データを継続的に保護します。提供されるツールには、アラート センターおよびセキュリティ センター、Vault による電子情報開示、Identity and Access Management、データ損失防止（DLP）などが含まれます。

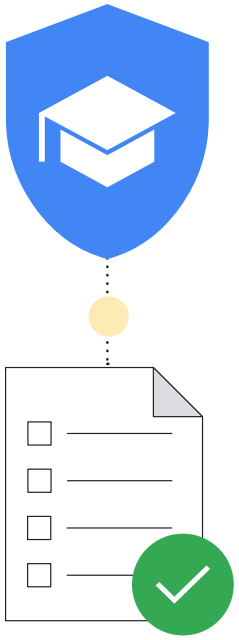
Google Workspace for Education を初めて使用する場合に役立つ資料をまとめました。このガイダンスの推奨事項に沿って設定する際にお役立てください。Google Workspace for Education を使用する方法については、クイックスタート IT 設定ガイドをご覧ください。

セキュリティ チェックリスト

セキュリティ チェックリストを確認して、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について詳しく学びましょう。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は、セキュリティの状況ページで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、端末の暗号化、ドライブの共有設定といった設定のステータスを確認できます。必要に応じて、全般的なセキュリティ ガイドラインやおすすめのセキュリティ対策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と組織のビジネスニーズやリスク管理ポリシーとのバランスをとることができます。

教育分野で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ための、その他の役立つヒントをいくつかご紹介します。

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する必要があることに反論す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、さまざまなサービス、設定、権限をユーザー別に付与できます。たとえば、教職員には 2SV を使用し、低学年の生徒には年齢にふさわしい認証を使用するなどです。教職員や生徒に対し個別に組織部門を設定し、各ユーザー グループに別々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ためには、適切な構造を作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一部です。そのため、Google Workspace for Education では、管理者用に認証管理の柔軟な方法を用意し、ユーザーが適切かつ安全なアカウント保護を受けていることを確認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、「安全なサインオン」セクションの推奨グループを参考にして、必要に応じて 2SV の使用を要求することを検討しましょう。一部のユーザーに 2SV の使用を適用し（セットアップの時間を与える）、セキュリティ キー（最も安全）、Google からのメッセージ（Android や iOS の Google アプリを使用）、検証アプリ生成ツール（Google 認証システムなど）、テキスト メッセージや通話（ただし、これらは最も安全性が低い方法）など、さまざまな方法を使用して 2SV を有効にすることができます。

組織が Google 以外の ID プロバイダ（IdP）を使用している場合、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。必要な場合、特権管理者以外のアカウントに SSO と 2SV を使用することもできます。

サービスのオン / オフ

管理者は Google 管理コンソールから、ユーザーが Google Workspace for Education アカウントでアクセスできる Google サービスを制御できます。組織部門（OU）ごとにサービスのオン / オフを切り替えることで、カレンダー、ドライブ、Meet などの Google サービスへのアクセスを制御できます（グループを使用する場合もサービスをオンにできます）。また、YouTube、Google マップ、Blogger などの追加サービスを有効にする前に、Workspace のコアサービスと追加サービスの違いを確認することも可能です。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 歳未満として識別されるユーザーが 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、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、OS に基づいて、コンテキストアウェア アクセス（Workspace for Education Standard および Plus で利用可能）を使用して 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するなどです。

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、任意の組織部門に対して 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。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、次のいずれかの方法で対応してください。

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

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?sjid=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人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 1 つのアカウントに侵入した際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を行うことが不可欠です。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 アクセスが少ないほど、被害は少なくてすみます。

生徒のファイルの外部共有をオフに設定（または外部共有をドメインのみに制限）し、[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ドメイン外でのファイル共有を許可している場合、ユーザーがドメイン外のユーザーとファイルを共有する際に警告を表示できます。また、ウェブ上でのファイルの公開を無効にし、外部の共同編集者にGoogle アカウントでのログインを義務付けるようにします。.

さらに、Workspace for Education Standard および Plus をご利用のお客様は、対象グループと信頼ルールを使用して、より詳かい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、教師のデフォルトのリンク共有対象者を、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、低学年の生徒が高学年の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見直して、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、注意深く共有ドライブへのアクセスを管理することをおすすめします。

可能であれば、一部またはすべてのユーザーの連絡先共有を無効にするか、あるいはカスタム ディレクトリを作成してどのユーザーが誰に表示されるかを指定することで、ディレクトリの公開設定と連絡先共有を制限することを検討します。

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）を保護するために活用できる、あらかじめ構築された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も可能です。

Gmail の設定の管理

Gmail は、Google Workspace for Education のコアサービスの 1 つです。管理者が教育機関とユーザーを保護するために活用できる設定が多数備わっています。

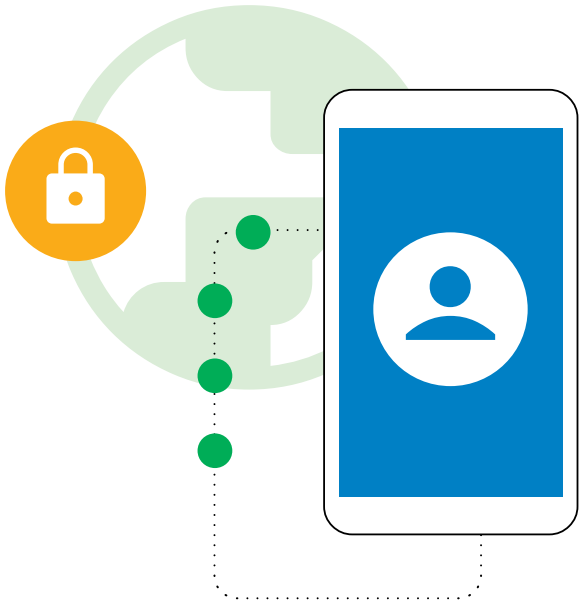
Gmail 認証で迷惑メール、なりすまし、フィッシングを防止することができます。また、承認されたすべての送信者に対して送信者の認証を要求したり、内部の送信者に対する迷惑メールフィルタの適用除外を無効にしたりするなど、迷惑メールフィルタの設定をカスタマイズすることもできます。

可能な限り、POP/IMAP アクセスを無効にし、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からのメールを許可する場合、外部受信者に関する警告を有効にすることができます。

Google Workspace for Education Standard および Plus をご利用のお客様は、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の脅威をブロック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 アプリケーションを、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 アプリケーションと不正なデータが共有されるのを防ぐことができます。



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することで、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を評価したり、誰がいつログインしたかを確認したり、ユーザーがどのようにコンテンツの作成および共有を行っているかを把握したりできます。グラフと表から、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も確認できます。レポートと監査ログを確認する（アラート センターを含む）ことで、セキュリティ リスクの特定、サービスの使用状況の分析、構成の問題の診断、ユーザー アクティビティの追跡などが行えます。

Google Workspace for Education Standard および Plus の管理者は、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、傾向を特定したり、現在と過去のデータを比較したりすることができます。使用状況ログ、アクティビティ ログ、監査ログ（管理者、ドライブ、Meet、Chat のログ イベントを含む）、およびセキュリティ レポートの大部分は、6 か月間利用可能です。

セキュリティ センターの活用

Google Workspace for Education Plus および Standard の管理者は、高度なセキュリティ情報と分析を提供し、ドメインに影響を与えるセキュリティの問題の可視性と管理性を高める、セキュリティ センターを活用できます。

セキュリティ センターにはセキュリティ調査ツールが含まれており、管理者は、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。

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&コラボレーション スイート

0

2021 年 11 月以降に Workspace で積極的に悪用されたソフトウェアの脆弱性 0 件*

50%

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 50%

2 分の 1

Workspace を利用する組織で発生するメール関連のセキュリティ インシデントの件数は Microsoft 365 を利用する組織の 2 分の 1

2.5 分の 1

Workspace を利用する組織で発生するセキュリティ インシデントの件数は Microsoft Exchange を利用する組織の 2.5 分の 1

*CISA の調査では、この件数は同分野の生産性向上ツールのベンダー各社と比べて大幅に低くなっています。

Google Chromebooks for Education

すぐに使える組み込みのセキュリティ機能を備えた Chromebook は、安全性が高く拡張可能で、生徒や教師にも簡単に使えるコンピュータです。企業、学校、消費者向けの 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。また、Chromebook は、最新の機能で進化し続ける脅威から学校を保護することはもちろん、アップデートが自動的にバックグラウンドで行われるため、ユーザーの作業をほとんど妨げません。

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 アップデートの際にデフォルトで安全性が確保されるよう設計された Chromebook は、OS とアプリケーションを常に最新の状態に保ち、ユーザーをリスクから保護します。また、Google の設計によるセキュリティ チップを搭載。デバイスの安全とシステムの整合性、ユーザーの個人情報を守ります。さらに、使用するクラウド アプリケーションはローカル アプリケーションと違い、ソフトウェア アップデートを必要としません。

チーム内の個々の 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、自動アップデートなどの組み込みのセキュリティ機能が、生徒と教育者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ファイルに保存されます。デバイス上の他の誰かがデータを見たり、アカウントを使用してアプリケーションにログインしたりすることはできません。つまり、生徒は教室内で極めて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、可視性が強化されたデバイス管理ライセンスである Chrome Education Upgrade をおすすめします。

ユーザーのデバイスのセキュリティ ポリシーをリモートで管理

学校の管理者は、Google 管理コンソールを使用して ChromeOS ポリシーを構成し、アプリケーションをリモートでインストール / 更新することができます。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。

この方法には、次のようなメリットがあります。

- 生徒は学校が承認したコンテンツやアプリケーションにのみアクセス可能
- アプリケーションと拡張機能はすべて、最新のセキュリティ修正で更新
- ユーザーは、学校のデータをデバイス外にコピー、転送、共有不可
- Google カスタマイズのセキュリティに関する推奨事項を使ってデータドリブンな意思決定を行い、セキュリティの脅威に対処可能
- 管理コンソールで直接、すべてのユーザーのセキュリティと Identity and Access Management ポリシーを一元管理

管理者が構成できる、いくつかの注目すべきポリシーがあります。

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し、生徒や教師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させるようにすることをおすすめします。
- **ログイン制限**
  生徒や教師が個人用 Gmail アカウントを使用して学校の Chromebook にログインすることが適切でない場合があります。そのため、生徒のみが使用するデバイスについては、ログインが Workspace ドメインのみに限定されるよう制限を適用します。
- **ユーザーとデバイスに関するレポート**
  管理者は、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検討しましょう。
- **自動再登録**
  学校が所有する Chromebook は、管理者がプロビジョニングを解除しない限り、学校に保管されることが重要です。管理者は、Chromebook がワイプされたり盗難されそうになったりし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**
  学校の Chromebook は、生徒が効果的に学習できるよう設定する必要があります。これには、生徒が不適切なウェブサイトにアクセスできないよう、ウェブ コンテンツ フィルタを使用して、閲覧可能なブラウザを認証済みのものに制限することも含まれます。また、管理者は、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**
  学校によっては、ウェブ フィルタリングにプロキシを使用している場合がありますが、ユーザー自身でプロキシ設定を変更できないようにすることが重要です。
- **マルチログイン アクセス**
  ユーザーが学校の Chromebook や Workspace アカウントを使用している際、予備アカウントへのログインが許可されていると、生徒や学校の機密性の高いデータ / 情報をその予備アカウントに簡単に流出させる可能性があります。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**
  生徒にとって、ブラウザ履歴を消去する機能を無効にすることが有益な場合があります。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。

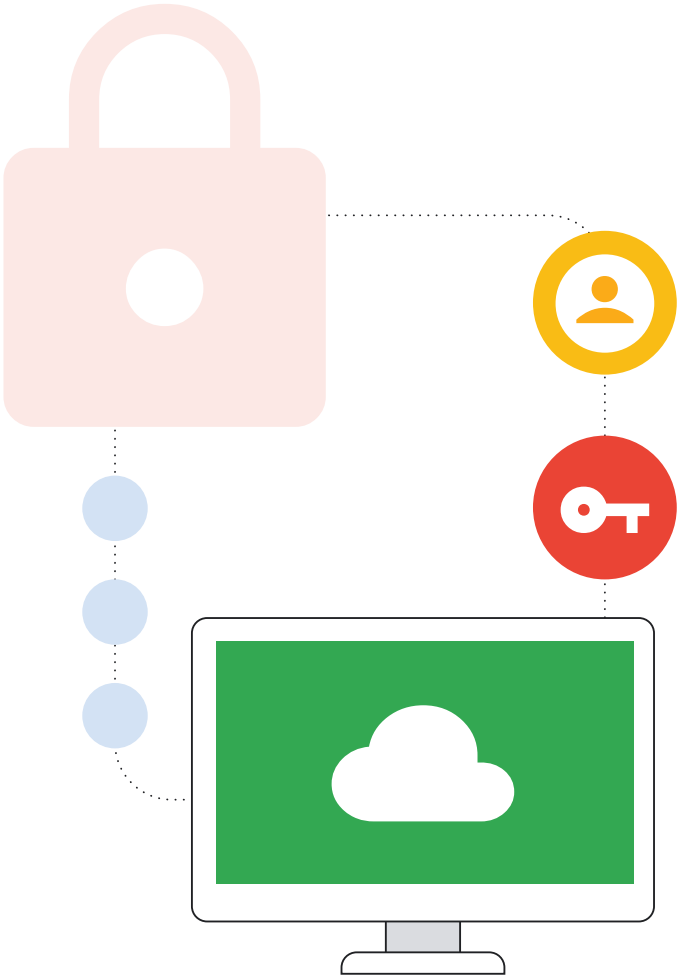
まとめ

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、難易度の高い取り組みであるものの、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。本ドキュメントでは、基本的な重要ポイントを押さえていますが、各学校は独自のニーズに合わせて推奨事項を作成し、進化する脅威の状況や新たなテクノロジーに対応し続けていく必要があります。ここで紹介している内容は、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を築くとともに、考えられる次の一歩と実装可能な項目のリソースを提供します。さらに Google 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、学校や組織を支援するための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。教育機関向けにカスタマイズされた Google のプロダクトは、このドキュメントで説明されている多くのサイバー セキュリティの落とし穴に対処できる、すぐに使えるソリューションです。Google は、皆様と連携して教育機関におけるセキュリティ プログラムの設計と実装に取り組んでいきたいと考えています。

重大なサイバー インシデントから確実にネットワークを守るための出発点として、上記のリストをご活用ください。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 チェックリストで確認できます。

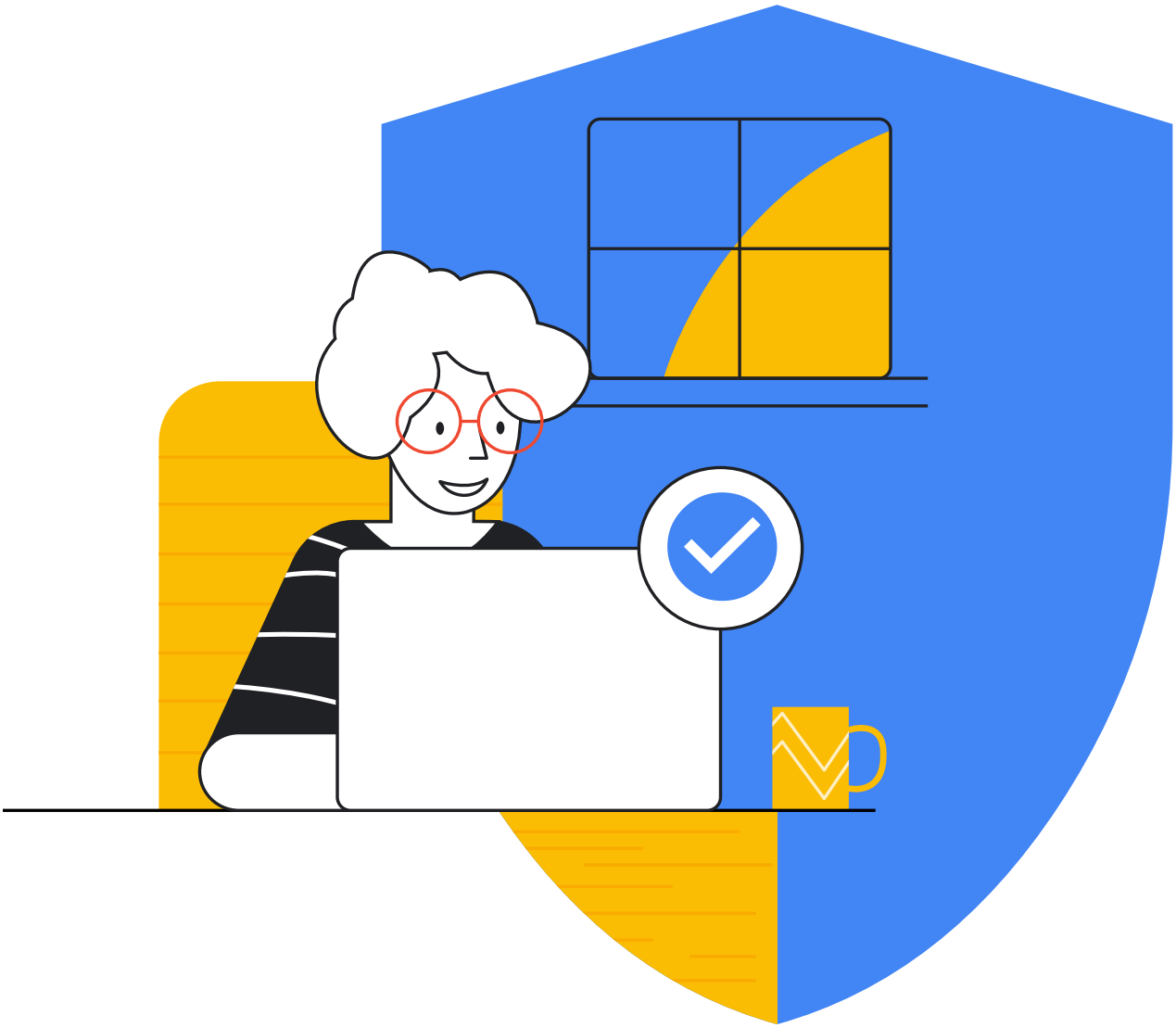
いつでもどこでも安全な使用を実現するエンドポイント管理

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、生徒は学校の Chromebook を自宅で使用するときも、教室で使用しているときと同様のセキュリティ効果を得ることが可能です。学校がデジタル教科書やオンライン学習ツールに移行するにつれ、生徒は宿題を するためにコンピュータを自宅に持ち帰る必要があるため、このようなセキュリティ管理はますます重要になっています。



リソースリスト

- Google。「オンラインでの安全性を保つためのツールとヒント」。Google セーフティ センター、https://safety.google/security/security-tips/（閲覧日: 2022 年 10 月 6 日）
- NIST。「Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1」。NIST Technical Series Publications, 16 April 2018、https://doi.org/10.6028/NIST.CSWP.04162018（閲覧日: 2022 年 10 月 6 日）
- Microsoft。「Microsoft AccountGuard Program」。Microsoft AccountGuard Program、https://www.microsoftaccountguard.com/en-us/（閲覧日: 2022 年 10 月 6 日）
- Google。「高度な保護機能プログラム」。Google の高度な保護機能プログラム、https://landing.google.com/advancedprotection（閲覧日: 2022 年 10 月 6 日）
- Google。「Google セーフティ センター」。Google セーフティ センター - 検索を、もっと安心に、https://safety.google（閲覧日: 2022 年 10 月 6 日）
- Meta。「Metaの基本: アカウントの安全を確保する」。アカウントの安全を確保する、https://www.facebook.com/gpa/resources/basics/security（閲覧日: 2022 年 10 月 6 日）
- Meta。「Facebook Protect」。Facebook、https://www.facebook.com/gpa/facebook-protect（閲覧日: 2022 年 10 月 6 日）
- NIST。「SP 800-124 Rev. 1: Guidelines for Managing the Security of Mobile Devices in the Enterprise」。NIST Technical Series Publications、https://doi.org/10.6028/NIST.SP.800-124r1（閲覧日: 2022 年 10 月 6 日）
- パスキー: https://developers.google.com/identity/passkeys
- CISA Protecting Our Future Cybersecurity K-12 レポート https://www.cisa.gov/protecting-our-future-cybersecurity-k-12
- GAO レポート https://www.gao.gov/products/gao-20-644
- Google for Education が教育機関の保護にどのように役立つかについて詳しくは、プライバシーとセキュリティ センターをご覧ください。
- Zcaler Phishing レポート



Google for Education