KEEPER®

学校におけるサイバーセキュリティ2025

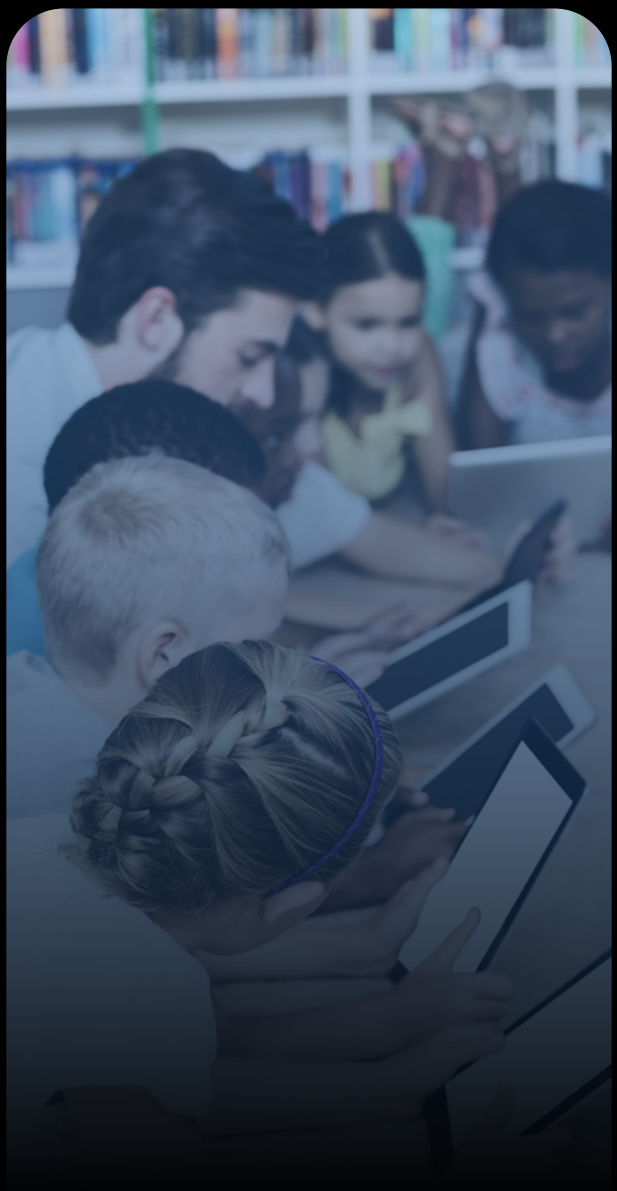
家庭と教育者のための安全なデジタル学習ガイド

Keeper Securityの無料リソース | flexyourcyber.com

概要

教室はいままでになくデジタル化が進み、それに伴って脅威も増しています。ランサムウェア攻撃は教育現場を混乱させ、AI生成の詐欺は生徒を狙い、フィッシング攻撃は見分けることがますます難しくなっています。宿題や授業での共同作業、事務作業までデジタルプラットフォームが中心となった現在、サイバーセキュリティは教育において欠かせない必須要件となっており、もはや選択肢ではありません。

このガイドでは、学校管理者や教師、保護者、生徒に向けて、オンラインの安全を高めるための専門家の視点と実践的な方法を紹介します。意識を高め、良い習慣を身につけ、率直に話し合うことで、教育現場と家庭は学びの継続性と個人データを守る、安全な学習環境を築くことができます。



2025年の脅威動向

教育現場へのサイバー攻撃は加速しており、その影響はこれまでになく深刻化しています。

- **ランサムウェアが増加傾向:** 2025年上半期には、学校や大学など教育機関への攻撃が前年同期比で23%急増 (Comparitech調べ)
- **学校は主要な標的:** 2023年7月から2024年12月の間に、米国の小中高等学校の82%が少なくとも1件のサイバーインシデントを経験しました (Center for Internet Security調べ)
- **経済的な圧力の高まり:** 平均的な身代金要求額は現在、55万6000ドル (約8,200万円) に達しています (Comparitech調べ)
- **フィッシングの見分けが困難に:** 過去2年間でAIを悪用した不正メールは2倍に増加しました (Verizon DBIR調べ)

要点: 教育分野はいま最も狙われる業界の一つとなっており、攻撃者はAIを使ってこれまでになく巧妙な手口を仕掛けています。

生徒と教育現場を脅かす5大デジタルリスク

脆弱または使い回された認証情報

使い回しや推測しやすいパスワードは、依然として攻撃者にとって最も簡単な侵入経路となっています。

パスワードマネージャーを使って、強力でユニークな認証情報を作成・保存しましょう。

共有アカウントと不十分な特権管理

共有アカウントが一つでも侵害されると、教室全体や学校、さらには教育現場全体が攻撃にさらされる可能性があります。

共有アカウントを廃止し、最小権限アクセスを徹底しましょう 。

フィッシングとソーシャルメディア詐欺

サイバー犯罪者は、職員やクラスメート、家族になりすまして信頼を悪用します。

情報を共有する前に、信頼できる手段で本人確認を行いましょう。

家庭や公共の場での安全でないWi-Fi

保護されていないネットワーク、脆弱なネットワークでは、攻撃者に機密データを傍受される恐れがあります。

学校のデバイスでは、パスワード保護されたWi-FiかVPNを利用しましょう。

AIによる偽情報とディープフェイク

偽の音声や動画コンテンツによって、生徒や職員が機密情報を共有したり、有害な行動を取らされたりする可能性があります。

ユーザーに危険の兆候を見抜く訓練を行い、違和感を覚えたら報告するよう促しましょう。

サイバーセキュリティ実践ガイド: 戦略とツール

学校向け

- [ ] 強力なパスワードポリシーと多要素認証 (MFA) を徹底する
- [ ] 重要なシステムを保護するために特権アクセス管理 (PAM) を導入する
- [ ] 全職員に継続的なサイバーセキュリティ研修を行う
- [ ] 定期的に脆弱性評価を実施し、明確なインシデント対応計画を整備する
- [ ] 重要データを定期的にバックアップし、復元手順を検証する
- [ ] 第三者の業者やパートナーを監査し、コンプライアンスとセキュリティ対策を確認する

保護者向け

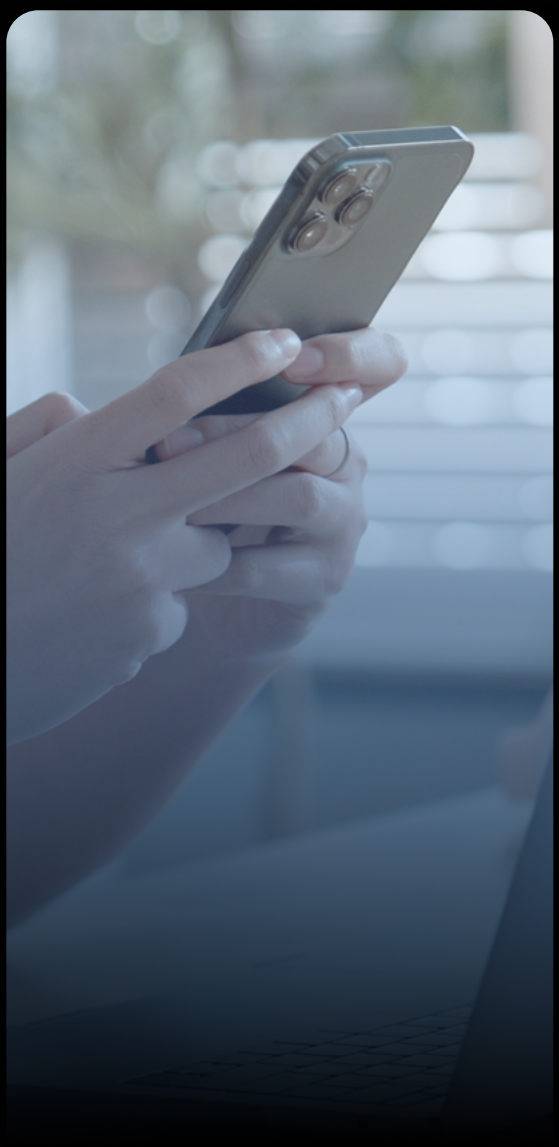
- [ ] 家庭のデバイスを強力でユニークなパスワードで保護する
- [ ] ソフトウェアの自動更新を有効にする
- [ ] オンラインでの利用状況を見守り、責任あるインターネット利用を促す
- [ ] ペアレンタルコントロールを使って、危険なコンテンツやダウンロードを制限する
- [ ] 適切なパスワード管理を実践し、安全なデジタル行動の手本を示す

生徒向け

- [ ] パスワードは友達にも教えず、自分だけで管理する
- [ ] 不明なリンクをクリックしたり、確認されていないファイルをダウンロードしたりしない
- [ ] オンラインで個人情報を共有する際は注意する
- [ ] オンラインで怪しいと感じたり、不安を覚えたりしたら声を上げる
- [ ] ソフトウェアやデバイスの更新通知を無視しない

親子で始めるサイバーセキュリティの会話

- [ ] 「誰かにパスワードを教えてほしいと言われたら、どうする?」
- [ ] 「そのメッセージや動画が本物かどうか、どうやって見分ける?」
- [ ] 「なぜアカウントごとに違うパスワードを使う必要があるの?」
- [ ] 「オンラインで不安に感じるものを見たら、どうする?」
- [ ] 「新しいアプリやゲームをダウンロードする前に、なぜ必ず確認することが大切なの?」



AIの影響
詐欺はもはや当たり前の存在に

AIツールにより、サイバー犯罪者は驚くほど現実味のある大規模な攻撃を仕掛けられるようになっています。音声のクローンやディープフェイクによって、信頼できる人物になりすますことができ、AIで強化されたフィッシングメールはより巧妙で見抜くのが難しくなっています。

AI詐欺の要注意サイン

- すぐに行動するよう迫るメッセージ
- 金銭やギフトカード、個人情報を求める依頼
- 不自然な言い回し、文体のちぐはぐさ、違和感のある画像や映像
- 「何かおかしい」と感じる違和感

リスクを減らす方法

- 本人確認のために、家族だけが知る合言葉やフレーズを使う
- 不審な電話はすぐに切り、公式に公開されている番号からかけ直す
- 動画や音声をむやみに投稿しない

共に育てるデジタル社会での自信

デジタル学習は今後も続き、リスクもなくなることはありません。けれども、正しい知識と備え、そして適切なツールがあれば、学校も家庭もサイバー犯罪者に立ち向かうことができます。安全な習慣を身につけ、常にコミュニケーションを取り、注意を怠らないことが、安全な学びと暮らしの環境をつくる鍵になります。

サイバーセキュリティはIT部門だけの仕事ではなく、全員の責任です。

重要なポイント

- **主要なサイバー攻撃の標的となっている教育現場**
  攻撃者は、学校が予算やIT人員に限りがある一方で、貴重な機密データを抱えていることを知っています
- **教室の外にも広がるサイバーセキュリティ**
  保護者や生徒も、安全なデジタル習慣を身につけることでリスクを減らすうえで、管理者と同じくらい重要な役割を担っています
- **脅威を増幅させるAI**
  ディープフェイクやAIを使ったフィッシングは今後もなくならないため、確認する姿勢や疑う視点、サイバーセキュリティの基本的な実践は、家庭と教育現場の双方に欠かせないスキルとなっています
- **サイバー攻撃に立ち向かう力は技術だけでなく人にかかっている**
  強固な防御には、技術的な対策 (MFA、PAM、セキュアなネットワーク) に加え、研修やコミュニケーション、明確な方針が組み合わさることが重要です
- **安心してデジタルを活用する力はみんなで育てる**
  教師、保護者、生徒の間で率直に話し合うことが、信頼を深め、安全を共有する文化を育みます

詳しい情報は flexyourcyber.com でご覧いただけます