教育機関を狙うサイバー攻撃を徹底解剖：脅威の実態と防御のコツ

はじめに

教育現場では、ITやセキュリティを本業としない教職員が兼務することも少なくありません。そのため、攻撃者の高度な手口に対して十分な備えをするのは大きな負担となっています。脅威を仕掛ける側はたった1つの脆弱性やパスワードの漏えいを突くだけで学校ネットワークに入り込めますが、防御する側の教育現場は、常に100%の対応を求められるのです。

コンピュータやモバイルデバイスが世界規模で接続し合う今日の世界では、わずかな失策が引き金となり、設定に不備のあるデバイスや盗み取られた認証情報を通じて機密データが漏えいする恐れがあります。たった一度の漏えいが、教育機関の基盤全体に連鎖的に影響を及ぼす可能性があるのです。

「知は力なり」

– トーマス・ジェファーソン

この言葉は、善悪を問わず当てはまります。攻撃側は教育機関の防御の穴を知ることで、急所を見つけ出し狙うことができます。防御側は逆に、自分たちに向けられるサイバー攻撃の性質を知ることで、攻撃側の手のうちを理解することができます。

このホワイトペーパーの内容：

- サイバーキルチェーンの詳細
- 教育機関を狙った攻撃の実例
- 攻撃を構成する主な要素と有効な防御策
- セキュリティギャップを埋める重要性

サイバーキルチェーンの各段階を詳しく掘り下げ、攻撃の構造を詳しく知れば、セキュリティ体制を絶えず見直しながら防御を強化してリスクを軽減できます。**サイバーキルチェーンを掘り下げる事前準備として、まずは、攻撃者（脅威アクターとも言います）が教育機関を標的にする主な理由を知りましょう。**

学校が脅威アクターに狙われる理由

保有しているデータはきわめて価値が高いのに、リソースは常に不足していてインフラは時代遅れのまま。そこに惹かれて教育機関を標的とするサイバー犯罪者が増えています。**世界中の多くの学校が、強固なセキュリティ体制の構築に苦心しています。**教職員の配置や報酬、生徒の学校生活の維持といった重要なニーズとのバランスを取る必要があるためです。資金の制限、ハードウェアやソフトウェアの旧式化、生徒や教職員のデータの肥大化などが相まって脆弱性が生じ、ITに携わる教職員の人手不足や負担増大を招いています。この状況がドミノ倒し的に影響を広げていることで、教育分野は脅威アクターから狙われやすくなっているのです。

リソース不足

「最小のリソースで最大の効果を上げる」ことは、教育機関にとって単なるスローガンではありません。生徒から教職員、管理者に至るまで、すべての関係者が日々実践している指針です。本書の目的は、予算の制約ではなく脅威への対策に焦点を当てることですが、教育現場では、限られた予算がセキュリティ対策だけでなく、教職員の確保や給与水準の維持、生徒の給食といった必須の取り組みにも割かれねばならず、結果として強固な防御を保つのが難しくなっています。

使途ごとに資金を確保するべく尽力するものの、残念ながら財源自体が限られているために十分な予算を確保できず、一部の予算枠にしわ寄せが生じ、他の項目を犠牲にして特定の項目を優先しなければならなくなることが珍しくありません。このことを脅威アクターはわかっており、学校への攻撃が成功する大きな要因にもなっています。攻撃の成功を許す実際の要素には、次のようなものがあります。

古いコンピュータ

コンピュータの耐用年数は一般に3〜5年とされています。それを超えると、互換性が損なわれるだけでなく、最新のセキュリティ機能を利用できなくなり、パフォーマンスが悪化するなど、生徒にとっても教師にとっても使いづらいものとなってしまいます。

古いソフトウェア

ハードウェアと同様、ソフトウェアもセキュリティの脆弱性を最小限に抑えるためにはアップデートが欠かせません。サブスクリプション型のソフトウェアであれば、最新機能とセキュリティ更新が自動的に提供されるため、アップデート対応の負担を大幅に軽減できます。長期的にはコスト面での検討も必要ですが、常に安全で最新の環境を維持できる安心感は大きな価値となります。

単一プラットフォームへの依存

特定のプラットフォーム向けに作られたソリューションなら、対象のOSを包括的にサポートできます。一方、「オールマイティ」タイプのソリューションでは、サポート内容を選ぶことで保守コストを抑えられますが、デバイスの管理や保護が不十分になる可能性があります。

IT担当者の過度な負担

IT担当者の配置の比率は、一般企業においては従業員100人前後に担当者1人が通例ですが、**教育機関ではその3倍**、つまり教職員300人以上に対して担当者が1人という比率も珍しくありません。人員不足とIT担当者の疲弊は、セキュリティ体制を弱体化させる主な要因であり、教育のような規制の厳しい業界ではコンプライアンスに悪影響を及ぼします。

業務に見合わない給与

米国の例ですが、一般企業におけるIT技術者の平均給与は、経験年数1〜3年で45,000〜71,000ドルです。ところが教育機関では、同じ経験年数のIT技術者に対する平均給与が42,000〜63,000ドルとなっています。**給与が相場よりも9%低い**ことと、人手不足による業務量への懸念とが相まって、優秀な人材の獲得と維持が難しくなっており、学校ネットワークの安全性が一層脅かされています。

IT研修の軽視

IT担当者から上層部に寄せられる要望の上位3つ の中に、新しいスキルを習得したり既存の知識を拡充したりするための体系的な研修の実施が入っています。フォード社の創始者Henry Fordは、研修にまつわるコストについて「**訓練した従業員が辞めるより、訓練していない従業員が働く方が高くつく**」と話し、研修の重要性を説いています。

価値あるデータ

初等・中等教育機関のデータは、機密情報であり、活用期間が長く、データ保護に割かれるリソースが乏しいため、サイバー犯罪者にとって価値の高い標的となっています。児童・生徒に紐づく個人情報（PII）は、金融詐欺やなりすまし、ソーシャルエンジニアリングに悪用される恐れがあり、多くの場合は何年も発覚しないまま放置されてしまいます。情報漏えいが起きれば法的・評判的・財務的な打撃を受けるにもかかわらず、教育機関は金融機関のような侵害防止の多層型セキュリティモデルを実装していません。攻撃者からは貴重なデジタル資産が詰まった金庫のように見なされています 。

身代金の要求

データが狙われる主な理由の1つとして、それを保有する機関と関係者にとって高い価値を持っていることが挙げられます。脅威アクターはこのことをよくわかっており、機密データを漏らさない代わりに金銭を渡すよう脅迫するための「人質」として悪用しています。事例によって幅はありますが、**ランサムウェアによるデータ侵害の平均コスト**は438万～537万ドルにものぼります。注：**この額は脅威の封じ込めに要したコストであり、身代金として支払われた額は含まれていません。**

風評被害

攻撃があったことが公になっても、残念ながら被害がそこで終わるわけではありません。多くの場合、問い合わせが相次ぎ、教育機関や学校の世間的なイメージが損なわれてしまうのです。このことを攻撃計画に織り込む脅威アクターも多く、二度目、三度目の恐喝を企て、同じ学校を複数回脅す事例が増えています。2025年第1四半期には**世界全体における教育機関を標的としたランサムウェア攻撃が前年同時期比で69%増加**しましたが、間違いなくこれが一因でしょう。

法的責任

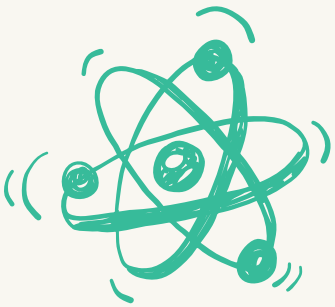
初等・中等教育機関は国の監督の対象であり、資金面でも国や自治体からの補助に大きく依存するため、データ漏えいは必ず報告し、調査を受けることが求められます。生徒や教職員の機密データを保護する責任は教育機関にあるため、データが不正に漏えいした場合、国によっては規定違反として多額の罰金が課されたり、国や自治体による補助金が打ち切られたりする可能性があります。さらに、データ侵害の被害を受けると、責任者は必要な措置が講じられる体制を整えていなかったことに対して**民事責任や刑事責任を問われる**おそれもあります。

個人情報の盗用

脅威アクターは入手した生徒データをひな型として偽のプロファイルを作成し、さまざまな犯罪行為に悪用します。最も多い犯罪は次のセクションで説明する金銭目的のもので、次いで多いのが、集団によるいじめやストーキング、**ターゲットを増やすためのソーシャルエンジニアリング**による情報収集です。

経済的損失

未成年の児童・生徒の個人情報（PII）は、クレジット情報や金融取引履歴がまだないため、**攻撃者にとって魅力的な標的**となります。こうした情報は不正な金融取引に利用されても発覚しにくく、**何年にもわたって不正利用が続く**ケースも少なくありません。更に、金融取引履歴がない子供達は、銀行口座やローン、クレジットカードの不正開設を検知するサービスを利用することはほとんどありません。その結果、被害が明るみに出るのは成人後というケースが多いのです。



サイバーキルチェーンとは?

攻撃者は選んだ標的とその脆弱性に基づいて用いる脅威を変えるため、攻撃の内容は一様ではありません。共通する特徴が見られることも多いものの、固有の特性やエンドポイントセキュリティに影響を与える不確定要素があるため、攻撃に対抗するためのサイバーセキュリティには攻撃解読の理論と実践の両方が欠かせないものとなっています。

一方、攻撃を構成する脅威は多様ですが、一つ確かなのは、どのサイバー攻撃も複数の段階に分解できることです。そこで、それぞれの段階で攻撃を阻止・防御すべく編み出されたのが「サイバーキルチェーン」です。サイバー攻撃の段階は準備から実行まで7つあり、防御側は各段階から得られる手がかりから、攻撃者が悪用する可能性のある急所を特定することができます。

**「それが僕の戦略で、
これが僕のプラン」
– Tears For Fearsの楽曲より**

攻撃者の手法を詳しく学ぶ前に、まずはサイバーキルチェーン**の7つの段階を見ておきましょう。**

1. **偵察:**
攻撃者が標的についてオンラインとオフラインの両方で調査を行い、標的を絞り込む。

2. **攻撃手段化:**
調査で収集した情報を使って、後の段階で用いるツールの開発や調達を行う。

3. **デリバリー:**
さまざまな悪意のあるツールを活用して、標的内部にアクセスする。

4. **エクスプロイト:**
標的へのアクセスに成功したら、脆弱性などのセキュリティギャップを悪用して内部に広く深く入り込む。

5. **インストール:**
悪意のあるコードを標的内部にインストールして、攻撃を成功させるための土台を確立する。

6. **コマンド&コントロール(遠隔操作):**
攻撃の最終段階に向けて、侵害したデバイスとの通信を確立する。

7. **目的の実行:**
すべての準備と基礎作業の完了後、目的(個人情報の収集、データの窃盗、ランサムウェアの実行など)を果たすためのツールを実行する。

教育機関を標的としたランサムウェア攻撃の事例

このセクションでは、**ボルチモア市公立学区（BCPS）を標的とする最近のランサムウェア攻撃の事例**から得られた知見を紹介します。なお、本稿執筆時点ではまだFBIによる捜査が終わっていません。詳細情報は公表されているものに限られているため、ここで紹介する事例は、同様の攻撃がどのように展開される可能性があるかを示すモデルケースの1つとしてお読みください。

1.

偵察

情報収集の段階として、脅威アクターは教育機関のインフラやネットワーク環境に関する詳細な情報を収集します。例えば、オープンソースリサーチやソーシャルエンジニアリングを通じて、ベンダー、サービスプロバイダ、主なIT担当者を特定します。偵察には受動的なものと能動的なものがあり、能動的な偵察の場合は、ネットワークトラフィックの異常な増加といった不審な動きを伴うため、ネットワークのスキャン実施時にアラートで気づけることもあります。偵察の目的は、標的を詳細に把握して脆弱性を特定し、攻撃が成功する可能性を高めることにあります。その手口を理解すれば、いち早く前兆を察知し、防御を固めることができます。

2.

攻撃手段化

偵察が終わると、脅威アクターは収集した情報を使い、次の段階に向けてツールを調整します。マルウェアの入手やカスタマイズなどがこれにあたり、ランサムウェアの動作を左右するフレームワークやインフラが含まれる場合もあります。現在多くの攻撃者に利用されているものに、RaaS（Ransomware-as-a-Service）プロバイダがあります。これはランサムウェアサービスをビジネスとして一括請負で提供する組織で、攻撃側のコストと技術的な障壁を下げています。脅威アクターは自身のスキルレベルが低くても、恐喝額の一定割合をこの組織に支払うことで、高度な能力を備えた機関も狙うことができます。このようなモデルについて理解を深めれば、脅威の進化を予測して備えることができます。

3.

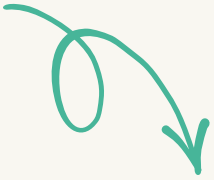
デリバリー

配布の段階では、フィッシングなどのソーシャルエンジニアリング手法を使い、悪意のあるコードを複数のエンドポイントに最小限の労力で配布します。成功の可能性を上げるためにメール、ショートメッセージ、SNSなどのチャネルが利用されており、特に個々のユーザを標的にする場合にこの傾向が顕著です。Jamf for K-12のようなソリューションを導入して、フィッシングURLのブロック、デバイスの健全性監視、セキュアなプロファイル登録によるデータの分離を実施すれば、このような脅威を防御しやすくなります。侵害が発生した場合でも、自動的に不正コードを無害にする機能で、学校の機密情報を守ることができます。このようなツールは、教育環境の予防的防御戦略にきわめて有用です。

4.

エクスプロイト

悪用の段階では、悪意のあるコードを使用してシステムの脆弱性を突いて権限を昇格させたり、フィッシングした認証情報を利用してネットワークにアクセスしたりします。巧妙なマルウェアには、暗号化で工程を隠蔽して検出を回避するものもあります。Jamf のソリューションなら、デバイスの健全性を監視し、リアルタイムで修復ワークフローを実施し、侵害されたアカウントを無効化することで、このような攻撃による影響を軽減できます。さらに、管理、ID、セキュリティの機能がシームレスに統合されているため、多要素認証（MFA）を有効にすることで認証情報を安全に利用でき、デバイスも最新パッチが適用された状態を常に維持できます。IT担当者は、この多層型の防御でリスクを軽減し、環境内のインシデントにすばやく対応することができます。



5.

インストール

インストールの段階では、侵害したデバイスにランサムウェアが展開され、児童・生徒と教職員のデータを標的とする攻撃や教育機関の各種ITシステムを混乱させる攻撃を実行するための下地が作られます。この段階への防御を固めるには、脅威を検出して常に把握できる体制を敷き、脅威の阻止や修復でコンプライアンスを徹底する必要があります。Jamfのソリューションなら、既知のマルウェアのブロックや有害なコードの検疫を実施でき、デバイスの健全性を常時監視して、セキュリティ体制のこまめな見直しに役立てることもできます。未知の脅威に対しては、デバイスのログをSIEMに転送することで、学校環境における脅威発見の精度とインシデント対応のスピードを向上できます。

6.

コマンド&コントロール（遠隔操作）

コマンド&コントロールの段階では、侵害したデバイスが攻撃者のサーバと通信を開始し、データ窃盗や恐喝のための標的ファイルや暗号化キーを取得できるようになります。攻撃者は侵害したデバイスをスキャンして、Word、Excel、PDF、データベースなど価値の高いファイルを特定し、今後のためにさらに別のツールを展開することもあります。その狙いは、学校のネットワーク内でアクセス可能な範囲を広げることです。防御する側は、この通信を阻止することが重要になります。IDツールとセキュリティツールが統合されたソリューションであれば、侵害された認証情報を無効化したり、悪意のあるサーバへのアクセスをブロックしたり、デバイスがコンプライアンスから外れた場合に修復ワークフローを自動で開始できるため、攻撃による被害を最小限に抑えながら学校環境を守ることができます。

7.

目的の実行

サイバーキルチェーンの最後の段階では、データの窃盗、恐喝、侵入拡大、DDoS攻撃などの最終目的が実行されます。ランサムウェアは通常、ファイルを暗号化して元のファイルを削除し、身代金を要求しますが、より悪質なケースでは、盗んだデータを流出させたり他で悪用したりして再度身代金を要求するといった事例もあります。攻撃は脅威アクターの目的に合わせてカスタマイズされるため、その内容は予測できず、教育機関に壊滅的な被害をもたらす可能性があります。管理・ID・セキュリティのツールが統合されたソリューションなら、悪意のあるトラフィックをブロックし、データの流出を防ぎ、侵害された認証情報を無効化することができます。修復ワークフローの自動実行とリアルタイムのテレメトリ測定により、コンプライアンス違反のデバイスが学校のリソースにアクセスできないようにして、多層防御戦略をサポートできます。

防御の穴を修復する

不十分な防御策やデスクトップOSへの過度な依存によってセキュリティの隙が生まれ、モバイルデバイスが無防備な状態となり、結果として攻撃者にネットワークを侵害されるリスクが高まります。

データ侵害のリスクはモバイルデバイスだけに限りませんが、職場での利用拡大や個人デバイスを使った業務データへのアクセスの増加により、依然として攻撃者にとって主要な標的となっています。**Jamf Threat Labsの調査**ではリスクを定量的に評価し、「**モバイルユーザの40%が、既知の脆弱性があるデバイスを使用している**」ことを突き止めました。デバイスに脆弱性があるとリスク要因の検査漏れが生じ、脅威アクターに以下のような攻撃を許してしまいます。

- **デバイス上で悪意のあるコードを実行**
- **ユーザに無断で、あるいは同意なしに監視**
- **内部のセキュリティ保護をバイパス**
- **感染デバイスからネットワークに不正侵入**
- **権限のないビジネスデータにアクセス**
- **機密情報だけでなく個人データや企業データも窃盗**
- **許可なくプライバシーデータを取得**

Appleはフォルム・機能・スタイルをデバイス機器に見事に融合させたことで名高いブランドです。この哲学は、セキュリティとプライバシーという、ますます重要性を増す設計要素にも反映されています。macOSとiOSベースのオペレーティングシステムには、デバイス、ユーザ、データをさまざまな脅威からハードウェアとソフトウェアの両方のレベルで守るための保護機能が標準搭載されています。

脅威アクターは、近年増加しているインフォスティーラー（情報窃取に特化したマルウェア）のような、新しい脅威やマルウェア亜種を使って攻撃を進化させています。既知の特徴しか検出できないツールによるセキュリティでは、進化するサイバー脅威への防御はかなり困難です。ボルチモア市公立学区に影響を与えたランサムウェアのように、**複数の脅威アクターグループが連携してネットワークに侵入**してから攻撃を実行した痕跡が見られた事例もあります。高度な脅威は動的であるため、（プラットフォームを問わず）オペレーティングシステムに組み込まれた保護機能をすり抜ける可能性があり、**ボルチモア市公立学区の攻撃で被害に遭った25,000人**のように、関係者やデバイスのデータが侵害の危険にさらされるおそれがあります。

教育機関にとって最も効果的な対策は、成熟した**多層防御フレームワーク**をベースとしてセキュリティ計画を策定することです。これにより、デバイスに対するリスクを軽減し、**Webベースの脅威への対策**を講じ、既知の攻撃を防止し、自動修復ワークフローでインシデントに迅速に対応して、エンドポイントのコンプライアンスを確保することができます。

多層化された統合型のソリューションがあれば、何重にも施された防御層によって包括的にリスクを捕捉および軽減し、高度な脅威にも対抗できます。これらの保護層のカバー範囲は組織全体に及ぶので、リソースやデータへのアクセスを要求するあらゆるタイプのデバイスやOSに対する第一防衛ラインにもなります。

Frost & Sullivanによる『Frost Radar: Endpoint Security, 2023』レポート において、Jamfは各種ソリューションで以下に挙げる優れた多層防御機能を提供していることから、エンドポイントセキュリティ分野における「リーダー」と評価されています。

- **悪意のあるアプリケーションやスクリプトのリアルタイム検出とユーザへの推奨対策の提示**
- **顧客がコンプライアンス要件を満たす際に役立つ、構成と監査の充実したフレームワーク**
- **ソリューション全体で統一された脆弱性管理、脅威対策、ポリシー管理**
- **外部のログ収集や分析用ツールにエクスポートできる豊富なエンドポイントテレメトリ**
- **MacだけでなくmacOS、iOS/iPadOS、Androidなどのモバイルプラットフォームも対象にしたセキュリティレポート生成と、WindowsやChromebookにも適用できるWeb脅威対策**
- **会社/学校支給と個人所有両方のデバイスで一貫性のあるポリシー適用**

まとめ

サイバーキルチェーンを詳しく知れば、偵察からデータ窃盗、恐喝に至るまで、ランサムウェア攻撃がどのように展開されるかを予測するための体系的な視点が得られます。

ボルチモア市公立学区の参考事例で見たとおり、防御の穴を放置すると脆弱性が生じ、攻撃の各段階で悪用されてしまいます。限られた予算、老朽化したインフラ、そして負担の大きいIT担当者。こうした条件下で、教育機関は高度化する脅威への防御に大きな課題を抱えています。

Jamf for K-12には、デバイス管理、ID・アクセス管理、エンドポイントセキュリティの機能が統合されており、教育機関の最も貴重なリソースである児童・生徒、教職員、学校のデータを包括的に保護する多層防御戦略をサポートするうえで最適です。また、Jamfのソリューションなら、Apple単独の環境はもちろんのこと、マルチプラットフォーム環境でも同様に脅威の検出、防止、修復を実現できます。リアルタイムのテレメトリと自動ワークフロー、セキュアなアクセス制御を組み合わせることで、深刻なセキュリティの穴を塞ぎ、コンプライアンスを確保することができます。脅威が高度化するいま、多層防御はもはや選択肢の1つではなく、教育の未来を守るために必須の対策です。

教育の安全を守るために、多層防御を今後のセキュリティ強化に活かしましょう

jamf

無料トライアル

www.jamf.com/ja/