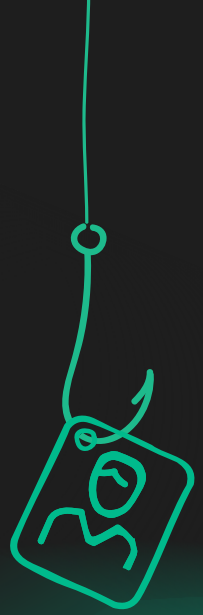
初等・中等教育機関におけるソーシャルエンジニアリング初心者ガイド

jamf

子どもが学校に通うのは勉強のためですが、それだけには留まりません。学校は他者との交流の仕方を知り、自尊心を獲得し、他生徒などから認められる方法を身につける場です。イベントや変化の絶えない時期であり、ときには誤った判断を下してしまうこともあります。

攻撃者はこのことを知っており、まさにそれが理由で、学校にソーシャルエンジニアリング攻撃を仕掛けています。

生徒の純真さに緊急性やプレッシャーを結びつけて、多数の悪事を可能にしているのです。



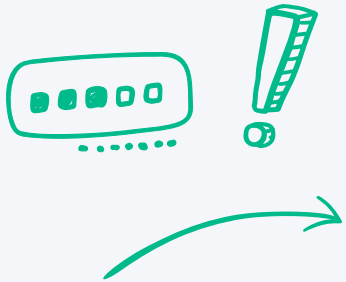
本書の内容：

- **ソーシャルエンジニアリングの概要**
- **一般的な策略**
- **初等・中等教育機関における事例**
- **攻撃を防ぐためのツールと手法**

ソーシャルエンジニアリングとは？

ソーシャルエンジニアリングは心理学的な策略を利用し、ユーザをだまして機密情報を引き出し攻撃です。見慣れたログインページに偽装したWebサイトを作成して認証情報をだまし取るなど、単体で用いられることもあれば、マルウェアを配布するなどして他の攻撃ベクトルと組み合わされることもあります。

ソーシャルエンジニアリングでは、セキュリティ体制のうち人間のかかわる要素が標的になります。この手法はきわめて一般的であり、**2025 CIS MS-ISAC K-12 Cybersecurity Report: Where Education Meets Community Resilience**によれば、**他の攻撃ベクトルの頻度を45%以上上回っている**とされています。



IT管理者がソーシャルエンジニアリングを警戒すべき理由

簡潔に言えば、この攻撃を受けるとセキュリティが無防備になってしまいます。例えば、次のような事態が考えられます。

攻撃者にセキュリティ対策を回避される：

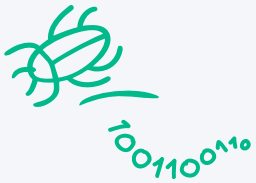
ITの構成や対策がソーシャルエンジニアリングに対応したものでない場合、攻撃者にすり抜けられるおそれがあります。認証情報が攻撃者の手に渡ってしまうと、適切なツールがない限り攻撃者と正当なユーザのログインを見分けられません。

ネットワーク内での横展開が行われる：

攻撃者は侵入後により重要なシステムへ移動できるので、アカウントが1つ盗まれただけでも複数のシステムが侵害され被害が拡大するおそれがあります。

IT部門に影響が及ぶ：

ソーシャルエンジニアリングは騒ぎを大きくして、IT業務の負担を増大させます。攻撃が成功した場合、たとえ攻撃者に情報を渡したのがユーザであったとしても、IT管理者に重い責任がのしかかります。ユーザの警戒心は重要ですが、誰にでもミスはあります。そのため、IT管理者が介入し、追加の対策を講じなければなりません。



よくあるソーシャルエンジニアリングの策略

フィッシング

フィッシングは、よく知られたソーシャルエンジニアリングの形態です。攻撃者が教職員やサービスになりすましたり、正当なWebサイトを模倣したり、緊急事態を装って、ユーザの情報をだまし取ります。

マルバタイジング

マルバタイジング（悪意のある広告）は、オンライン広告を悪用し、ユーザをだましてマルウェアをダウンロードさせたり、認証情報を盗み取ったりします。

プリテキスティング

プリテキスティングにはさまざまな形がありますが、ユーザの信用を得るために用いられるのが一般的です。この攻撃では、権威のある人物や同僚になりすましてユーザに信用させ、情報を引き出します。

ベイティング

ベイティングでは、無料通貨、プレゼント、限定コンテンツのように魅力的なものを提示してユーザを誘い込みます。ユーザがリンクをクリックすると、マルウェアがインストールされたり、フィッシングサイトに誘導されたりしてしまいます。

SEOポイズニング

検索エンジンの広告を悪用した攻撃で、検索結果の最上位に他サイトを装った偽のWebサイトを表示させ、ユーザを巧妙にクリックへと誘導するのです。

プロンプト爆撃

多要素認証のリクエストをユーザに繰り返し送りつけて、アクセスを許可させる攻撃です。

これらの手法は決して新しいものではありません。しかし、近年ではAIを活用した手法も登場し、状況を一変させています。IBMの**2025年データ侵害のコストに関する調査**によれば、データ侵害の6件中1件でAIが利用されていました。

生成AIを利用することで、攻撃者は「説得力のあるフィッシングメールの作成時間を16時間からわずか5分に短縮」できます。

AIの登場で、従来以上に本物らしいフィッシング攻撃やディープフェイクが短時間で作成されるようになりました。学校現場、特に判断力の未熟な子どもたちが標的となるリスクを考えれば、この技術的進化への対策は急務と言えるでしょう。

初等・中等教育機関におけるソーシャルエンジニアリングの例

ソーシャルエンジニアリングはあらゆるサイバー攻撃で利用されています。**Verizon社の2025年度Data Breach Investigations Report**によれば、**教育サービス業界に対する攻撃の17%**でソーシャルエンジニアリングの手法が確認されました。

ソーシャルエンジニアリングには多くの形態があり、今もなお開発が進んでいるため、実際に使われる手法は多岐にわたります。
以下に、考えられる例をいくつか示します。

オンラインゲームかと思ったら、だまされた！

ある中学生が課題を終え、インターネットでゲームを探していたときのこと。なんとなくアクセスしたWebサイトに、お気に入りのオンラインゲームの通貨を無料でプレゼントするという広告が出ていました。思わずそのリンクをクリックしたところ、認証情報を盗むためのWebサイトに誘導され、ゲーム通貨にだまされてログイン情報を奪われました。

贈り物には要注意

ある新任の先生は、校長先生や教育委員会に評価されたい一心で、必死に頑張っています。そんなある日、「校長」を名乗る人物からギフトカードのコードを要求するEメールが届きました。先生は疑うこともなく、そのまま指示に従ってしまいました。赴任したばかりだったので、校長の話し方とEメールの文章が**まったく**似ていないことに気づけなかったのです。

ウソかホントか？このダウンロードは安全です（もちろんウソ）

ある高校生が受験勉強に取り組んでいました。試験対策の教材を検索したところ、検索結果ページの一番上に、無料の試験対策広告がスポンサーリンクとして表示されました。試験対策ソフトウェアをダウンロードするだけのはずだったのに、そのソフトウェアにはなんとマルウェアが含まれていました。

あなたも有名人…個人データがオンラインに流出したら。

小学生のグループに、学内人気者コンテストを知らせるEメールが届きました。一番人気の生徒を予想して投票するというものです。ただし、投票者が本当に在学生かどうかを確認する必要があるという理由で、個人情報の提供を求められました。

ソーシャルエンジニアリングをその場で防ぐ

さて、ソーシャルエンジニアリングにユーザがだまされ、データセキュリティが危険にさらされる事態を防ぐにはどうすればよいのでしょうか。そのためには、**ユーザとテクノロジー**という2つの角度から対策を講じる必要があります。

ユーザ

ユーザ、特に子どもたちは、インターネットの良い面も悪い面もあまり知らないものです。オンライン上のコンテンツを疑うことに慣れている人は多くありません。理想的には、学校の授業でデジタルシティズンシップを教えるべきです。デジタルシティズンシップ教育とは、生徒に責任を持って安全にインターネットを利用する方法を教えることです。

教育の内容：

- 一般的なサイバー攻撃について、**年齢に応じた説明**を行う
- 不審なWebサイトやコンテンツの**例**を示す
- オンラインでは責任を持って倫理的に**振る舞う**ことを勧める

もちろん、教職員へのトレーニングも必要です。トレーニングの例：

- フィッシングメールの**模擬演習**
- 定期的な必須のコンプライアンス**トレーニング**
- **透明性文化**の醸成：ソーシャルエンジニアリング攻撃にだまされたかもしれないと思ったらIT管理者に相談するよう促す

専門ツールとポリシーで対策を拡充

攻撃者が人を狙うのには理由があります。専門的なツールがあまり必要ないうえに、攻撃の成功率が高いからです。
人は誰しもミスとは無縁でいられないため、追加で対策を講じる必要があります。

コンテンツフィルタリング

コンテンツフィルタリングは、ユーザが悪意のあるリンクをクリックしてしまった場合でも、悪意あるコンテンツをブロックします。コンテンツフィルタリングを実装する方法は、許可/禁止リストで許可（および禁止）するWebサイトを明示的に定義することです。しかし、この方法には限界があります。有用なサイトをすべて許可することも、怪しいサイトをすべて禁止することも不可能です。さらに、インターネットの環境が、生徒が卒業後に体験するものとは別物になってしまいます。

より効果的な方法は、フィルタリングで広範なカテゴリを禁止することです。この場合、IT管理者がドメインを具体的に指定する必要はありません。その代わりに、各Webサイトをカテゴリに分類し、カテゴリに応じて禁止するかどうかを判定します。アダルトサイト、ギャンブルサイト、ファイル共有、ネットワーキング、暴力的または攻撃的なサイトなど、あらゆるものを構成で禁止できます。AIや機械学習と組み合わせてインテリジェントなフィルタリングを実装すれば、さらに万全の体制を整えられます。

多要素認証

多要素認証（MFA）は、ログイン保護を拡充します。ユーザの認証情報が侵害**された**場合も、MFAがあれば、攻撃者がそのアカウントへのアクセスに成功する確率を下げられます。MFAでは、以下の認証方法のうち2つ以上を義務付けます。

- **知識情報**：パスワード、PIN、秘密の質問など
- **生体情報**：指紋や顔など
- **所持情報**：別のデバイスやセキュリティキーなど

専門ツールとポリシーで対策を拡充

シングルサインオン

真のシングルサインオン（SSO）を実現する方法は、IDプロバイダ（IdP）を既存環境に追加することです。IdPにパスワードを1つ提供するだけで、**すべて**のユーザアカウントにアクセスできるようになります。ユーザの覚えるべきパスワードの数が減るので、侵害される可能性も減らせます。こう聞くと、攻撃者も1つのパスワードだけですべてのアカウントにアクセス可能になるのではないかと考える方もいるでしょう。

もちろん、そんなことはありません。SSOでは一般にMFAを利用するからです。例えば、生体情報（生徒の指紋など）を求めるように設定します。SSOはパスワード疲れを緩和し、侵入口を減らすだけでなく、認証情報の窃取対策にも役立ちます。仮に、ユーザがなりすましサイトにアクセスしたとしましょう。IdPはそのドメイン名を容認しないので、ログインが禁止され、認証情報の流出を防止できます。

デバイス管理

ここまで紹介したツールはどれも素晴らしいものですが、導入はモバイルデバイス管理（MDM）がないと困難です。MDMがあれば、IT管理者は以下のことが可能になります。

- デバイスのセキュリティ状態を可視化
- セキュリティポリシーとセキュアな構成を設定
- デバイス設定と制限（パスコードの必須化、アプリケーションの指定など）を構成
- デバイスのソフトウェアを最新バージョンに維持
- コンテンツフィルタリングソリューションを展開

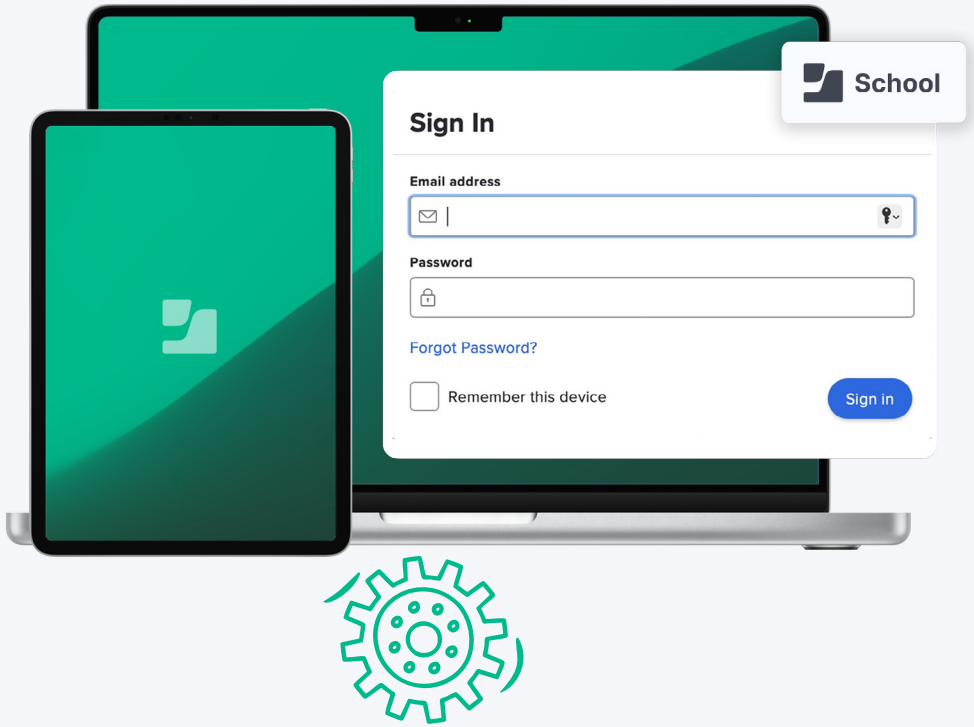
導入：Jamf SchoolおよびJamf Safe Internet

Jamf School

Jamf Schoolは、教育機関のためのMDMソリューションです。
主な機能：

- **デバイス構成テンプレート**：宣言型デバイス管理を活用
- **デバイスインベントリ**：管理者が校内リソースに接続されているデバイスを把握
- **透明性**：デバイスステータスを可視化し、問題があれば迅速に対応
- **制限**および**設定**：パスコードの必須化などをデバイスに適用
- **SSOへの対応**（IDプロバイダが必要）
- **シンプル操作**：教師からIT部門にアプリの利用承認を申請
- **他にも多彩な機能を搭載**

Jamf Schoolは、ソーシャルエンジニアリングを防ぐデバイス保護対策の基盤になります。

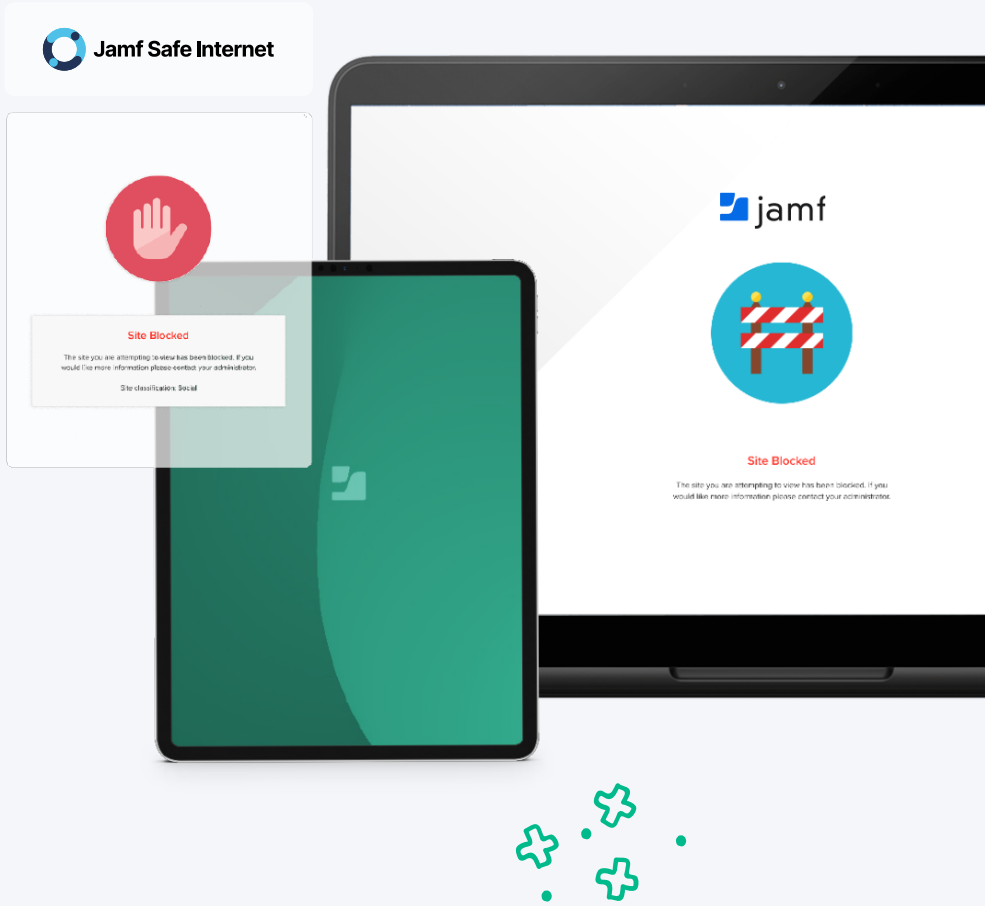


Jamf Safe Internet

Jamf Safe Internetは一歩先を行くセキュリティ機能を備、Apple、Chromebook、Windowsデバイスに対応しています。Jamf Safe Internetはカスタマイズ性に優れ、位置情報やタイプなどの属性に応じてデバイスグループごとにポリシーを簡単に設定、変更できます。共有デバイス、学校支給の個別デバイス、あるいは生徒が所有するデバイスでも利用可能です。

ソーシャルエンジニアリングなどの脅威への対策として、**Jamf Safe Internetは以下の機能を備えています。**

- **高性能コンテンツフィルタリング**：人工知能（AI）と機械学習（ML）を活用し、悪意あるフィッシングサイトへのアクセスを未然に防止
- **DNS**および**ドメイン名ブロッキング**：DNSスプーフィングを防止
- **オンデバイスコンテンツフィルタリング**：あらゆる場所でフィルタリング（iPad）
- **ネットワーク内保護**：悪意あるWebサイトのデバイス侵害を阻止
- **Googleセーフサーチ**および**Googleセーフブラウジング**を必須化：検索結果から悪意あるサイトや不適切なサイトを除外



前述のセキュリティ機能に、監視は含まれません。生徒は自身のプライバシーを侵害することなく自由にインターネットを閲覧し、デジタルシティズンシップを身につけられます。安全でセキュアなテクノロジーを教育に活用すれば、全員にメリットがあります。

教職員
ログインの問題や中断に悩まされることなく、教育に集中できます。

生徒
自由に、しかも安全に閲覧して学べます。

IT管理者
データの保護状況を把握しながら他の業務に専念できます。

テクノロジーが貴校にもたらすメリットに興味をお持ちですか？

トライアルに申し込む