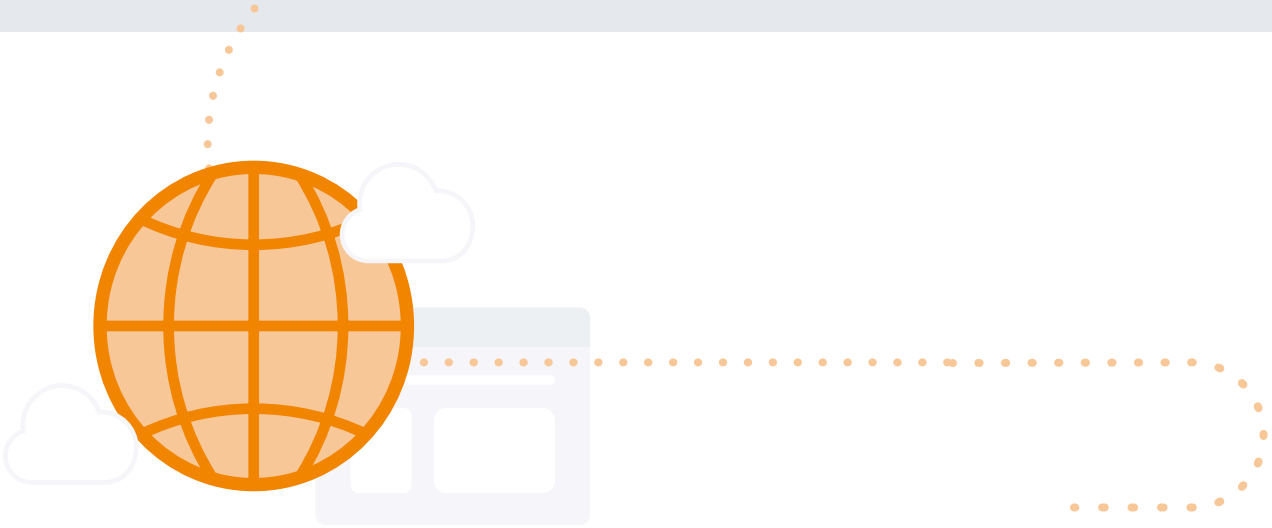
コンテンツフィルタリングの基礎ガイド（初等中等教育機関向け）

jamf



世界中の多くの学校が、インターネットが提供する素晴らしい教育やリサーチの機会を生徒に与えたいと願う一方で、有害または不適切なコンテンツやフィッシングなどの攻撃から生徒を守りたいと考えており、その2つの間でどのようにバランスを取るかについて頭を悩ませています。

生徒たちは常に学校で不適切なコンテンツや有害なコンテンツへのアクセスを試みています。ニュージーランドで最近行われた調査によると、1ヶ月でなんと3億9900万件もの不適切なコンテンツへのアクセスがブロックされています。[1]

学校支給のデバイスを学校のファイアウォールの外（自宅など）に持ち出すことも増えた今、生徒がどこにいたとしても、不適切なウェブサイトへのアクセスをブロックする仕組みが必要です。

これは、学校が生徒の安全性に多方面から取り組まなければならないことを意味しています。私たちは、この取り組みを始めようとする学校をサポートするためにこのガイドを作りました。

このガイドのトピック

- 生徒を危険にさらすオンラインコンテンツの種類と、生徒をそれらから積極的に保護することが重要な理由
- コンテンツフィルタリングに対して柔軟なアプローチが必要となる状況
- 「デジタル市民」を育てる方法
- Jamfの活用法

なぜフィルタリングが必要なのか

多くの理由があります

生徒の安全を守る

生徒のオンラインセーフティに関する法律は国ごとに異なりますが、多くの場合、以下のような事項に対する制限が求められます。

- ポルノやわいせつなコンテンツへのアクセス
- ヘイトスピーチ、暴力または過激化を促進するサイトへのアクセス
- 自傷行為、自死、または拒食を助長するサイトへのアクセス
- フィッシングや詐欺目的のサイトへのアクセス
- ネットいじめ
- ソーシャルメディアやゲームなど、学習の妨げとなるコンテンツへのアクセス
- ギャンブルサイトへのアクセス

世界保健機構（WHO）によると、自殺は世界中の15～19歳の子どもの死因の4位となっています。[2]そして就学年齢のすべての子どもの47～60%がネットいじめを経験していると言われる[3]今、このようなオンラインの危険からの保護は、文字通り彼らの命さえも守ることにつながるのです。

生徒の集中力と生産性

学校でのソーシャルメディアへのアクセスに制限をかけることは、ネットいじめを防ぐだけでなく、生徒が学習に集中できる環境を作ることにもつながります。これにより、生徒の学習効率や生産性のアップに加え、レッスンへの積極的な参加を促すことができます。

法律の遵守

2000年、アメリカ連邦議会で児童インターネット保護法が制定され、学校でオンラインセーフティのポリシーを施行する際に利用できる助成金制度E-Rateとの紐付けが行われました。

イングランドとウェールズでは、2015年に教育省によって法定指針「Keeping Children Safe in Education」が制定され、すべての学校に対して適切なフィルタリングと監視のシステムの採用が求められるようになりました。スコットランドでも同じような規則が存在します。[4]

こういった措置は、世界のすべての大陸（南極大陸を除く）で、全体的または部分的に実施されています。

システムのセキュリティ

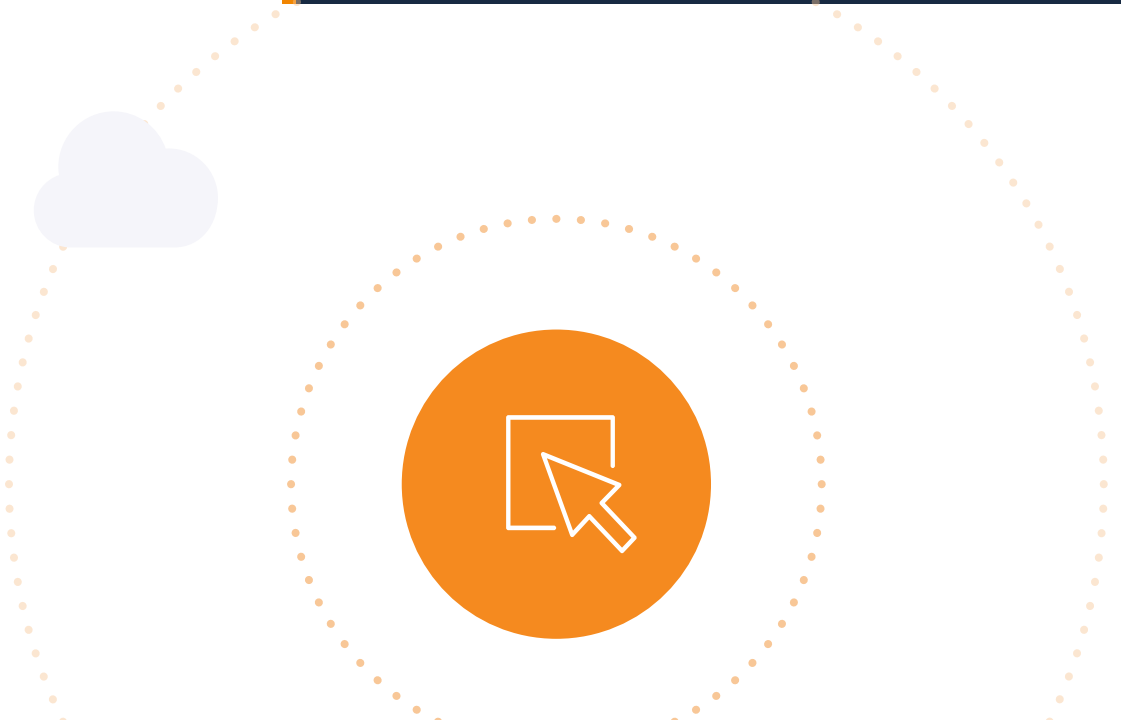
マルウェアやアドウェア、スパイウェアをブロックすることで、生徒の安全を守ります。これにより、学校のネットワークも安全に保つことができます。

モニタリングとレポート

子どもが望ましくないコンテンツにアクセスしていないという確信を保護者が求める中、学校側は生徒やデータを保護するためにネットワークを監視する必要に迫られています。

しかし、ここで問題となるのがプライバシー保護とのバランスです。監視は、個々のデバイスを細かく調べずに行われなければなりません。そのため、匿名化されたデータを収集し、セキュリティの専門家や保護者、管理者に提示する透明性の高いプロセスが必要となります。

学校でセキュリティーツールを採用する際には、エンドポイント保護やネットワーク脅威防御を提供するもの（例：Jamf ProtectやJamf Safe Internetなど）を選択することをお勧めします。こういったソリューションには通常、既知のウイルスからの保護や新たな危険を発見し隔離するための行動分析、徹底したレポーティング機能などが含まれます。また、ベストプラクティスを共有したり、同じく生徒の成功のために尽力している教育者からアドバイスをもらったりできるコミュニティが用意されていることも重要です（Jamfの場合、Jamf NationやJamf Educatorのようなコミュニティがあります）。それをJamf SchoolやJamf Proのような包括的なモバイルデバイス管理（MDM）ソリューションと組み合わせれば無敵です。



なぜすべてをブロックしないのか

子どもへの被害を考えれば、保護者や教育者がすべてのアクセスをブロックしてしまいたくなる気持ちも理解できます。しかし、このやり方は数々の問題をはらんでいます。

生徒を保護し授業に集中させるための過剰な策として学校がブロックしたサイトの中に、実は教師や生徒が本当に必要とするサイトが含まれている場合もあります。例えば、YouTubeやGoogleなどのサービスを授業で利用するケースも多くあります。時事問題や社会の動きなど様々なトピックを授業で取り上げたいと教師が思っても、それに関連するコンテンツにアクセスできなければフラストレーションにつながってしまいます。また、宿題の回収をオンラインで行えないことも教師にとってはストレスとなります。

もちろん、こういったサービスに自由にアクセスできることによって生まれる問題がないわけではありません。だからこそ、生徒の保護と教育を両立させるためにも、フィルタリングをドメイン名ベースの単純な方法ではなく、より高度な方法で行うことができるJamf Safe Internetのようなコンテンツフィルタリングソリューションが必要になるのです。

完璧なフィルタリングシステムは存在しません。誰かがマルウェアやフィッシングサイトを見つけてブロックリストに手作業で追加する作業が必要な上、残念ながら日々新しいサイトが作られているという現状があります。

だからこそ、制限なしてデバイスを使う将来に備えて生徒を教育することは、学校が担う重要な役目と言えます。インターネットに潜む危険について理解し、被害から身を守る方法を知っている若者は、過剰なアクセス制限によってインターネットの世界から完全に守られた学生時代を送った人よりも、安全にインターネットを利用することができます。

「デジタル市民」を育てる

インターネット上でフィッシングやマルウェア、ユーザを騙そうとする情報などを見分け、回避する方法を学生のうちに学んでおくことは非常に重要なことです。

教育機関は、カリキュラムや教育方針の一環として、十分な訓練を受けたデジタル市民を育てなければなりません。信頼できるソースを見分ける力を養うには、信頼できるソースとは何かということを学ぶことはもちろん、クリティカルシンキング（批判的思考）のスキルやフィッシングやその他の詐欺を回避する能力を得ることが必要になります。

生徒がデジタル空間で責任を持って行動できるように支援したいと考える教育者には、Common Sense EducationのDigital Citizenship（デジタルシチズンシップ）プログラムが提供している無料のレッスンやカリキュラム、アイデアの活用をお勧めします。これは、すべての子供と家族の生活向上を目指すアメリカの非営利団体Common Senseが、ハーバード教育大学院の「Project Zero」の協力のもと作成したもので、学年や年齢に合わせた各種のレッスンが用意されています。

最適なフィルタリング&セキュリティソリューション

各教育機関にとって最適なソリューションを見つけるにはどうしたらいいのでしょうか？まずは、以下の6つの質問に基づいてベンダーを絞り込むことから始めましょう。

1 Chromebook、iPad、Macを含むすべてのデバイス、およびBYODデバイスに対応しているか

学校で使用されているすべてのデバイスに対応しているソリューションであることが重要です。フィルタリングシステムには、「鎖の強さはもっとも弱い輪によって決まる」ということわざが当てはまります。

2 未知の攻撃からの保護を提供しているか

行動分析やリアルタイムアラートなどを組み合わせて未知のマルウェアやサイトを発見できるシステム（例えばJamf Protect）を選ぶことが大切です。行動分析は、マルウェアや危険なサイトの行動や特定のフレーズの使用を理解することで攻撃を阻止します。

3 YouTubeやGoogleのサービス内で一部のコンテンツをブロックする機能を備えているか

YouTubeやGoogleは強力な学習ツールとして機能する一方で、フィルタリングされていないコンテンツへの入り口にもなり得ます。そのため、Googleセーフサーチや YouTubeの制限付きモードを使用でき、エンドユーザによって削除できないように設定できるツールが必要になります。

4 保護者の参加を促す機能を備えているか

フィルタリングの必要性に疑問を持つ保護者がいる一方で、プライバシーの侵害を心配する保護者もいるでしょう。Jamf Parentのようなアプリがあれば子どもの1日のアクティビティを確認できるほか、セキュリティやプライバシーに関する明確で詳細なレポートを手に入れることもできます。

5 学校の外でも機能するフィルタリングを提供しているか

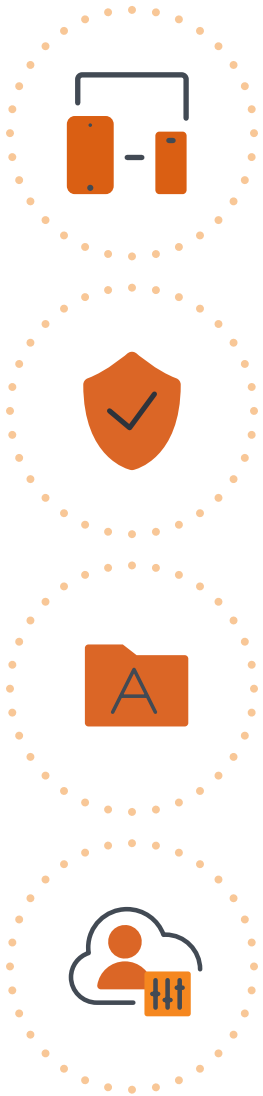
デバイスが自宅にある時でもフィルタリングやデバイス管理を行うことのできるソリューション（例えばJamf Schoolなど）があれば安心です。さらに、Jamf Parentのような使い勝手の良いアプリで保護者がフィルターや管理状態を調整できればさらに理想的です。

6 既存のソリューションとの統合を提供しているか

MDMプロバイダや信頼できるベンダーとシームレスに連携し、世界最高水準のセキュリティだけでなく、充実した教育オプションも提供できるフィルタリング&セキュリティのソリューションがあれば、高い費用対効果が期待できます。

Jamfのサポート

Jamfは、Apple製品の管理とセキュアな運用の両方を実現するソリューションを提供しています。私たちはモバイルデバイス管理だけでなく、管理者から保護者までサポートするツールで生徒の成功を応援しています。



jamf SCHOOL

効率的なAppleデバイス管理で教育者とIT部門を支援

jamf PROTECT

Macのために作られた
エンドポイント保護ソリューション

Jamf Safe Internet

教育機関向けのコンテンツ
フィルタリングと脅威防御ツール

Jamf Teacher

Jamf School Student

Jamf Parent

Jamf Assessment

jamf EDUCATOR

Jamf Teacherアプリを使う教育者のためのサポートサイト

jamf MARKETPLACE

Jamfと統合し、その機能を強化してくれる各種ツールが集結

JamfとJamf Safe Internetのコンビネーションは、プライバシーに配慮しながら生徒の安全を守るための最適解です。

- Jamf Safe Internetは、MacOS、iOS、ChromeOSに対応しているため、デバイスに関係なくエンドユーザを保護することができます
- Jamf Protectは、アナリティクスを使ってデバイスを監視し、未知の攻撃を阻止します
- Jamf Safe Internetは、Googleセーフサーチ とYouTubeの制限付きモードを強制適用し、ユーザによる無効化を許しません
- Jamf Safe Internetがデバイスベースの保護を学校のネットワーク外でも提供する一方で、Jamf Parentは学校以外の場所でデバイスのセキュリティを維持するための各種ツールを保護者に提供します
- Jamfは適用されるすべてのプライバシー規約へのコンプライアンスに熱心に取り組んでおり、生徒、保護者、教師の情報を保護することへのコミットメントを示すために「Student Privacy Pledge（生徒のプライバシーに関する誓約）」にも署名しています

jamf

Jamf Teacher、Jamf Student、Jamf Parentの各アプリとシームレスに統合したJamf Safe Internetなら、既存のワークフローをさらに強化することができます

トライアルに申し込む

またはお近くの販売代理店へお問い合わせください。