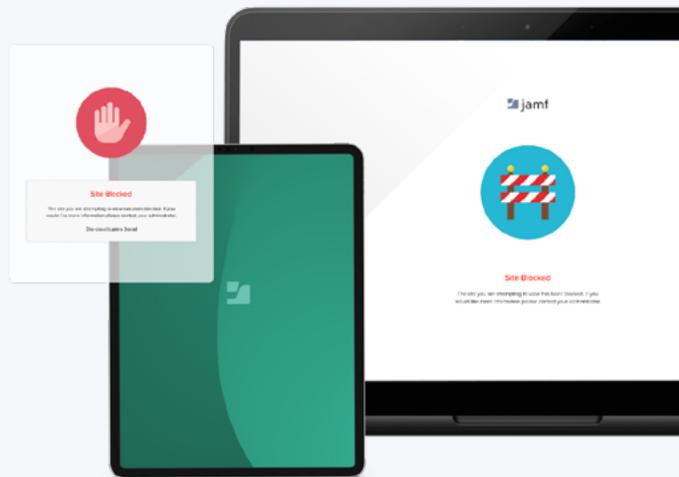




# 場所を問わずプライバシー が保護された安全なネット 環境を提供



Jamf Safe Internetは、Jamfのコンテンツフィルタリングとネットワーク脅威保護エンジンを搭載し、学校が児童生徒や教職員、そしてネットワークを不適切なコンテンツや脅威から守れるよう設計されています。

生徒がインターネットを使う時間は以前の2倍近くに増えています。これに伴い、サイバー攻撃を防ぎ、生徒を不適切なコンテンツから守るための対策がますます重要になっています。

Jamfのセキュリティ技術を活用したJamf Safe Internetは、教育機関専用に開発されたフィルタリング・セキュリティソリューションです。業界トップクラスのネットワーク脅威防御機能と膨大なコンテンツフィルタリングデータベースによって有害なコンテンツやマルウェアやフィッシングなどの攻撃をブロックし、教育に特化したモバイルデバイス管理 (MDM) ソリューションであるJamf Schoolともシームレスに統合しています。

## 常時稼働のサイバーセキュリティ

教育現場において、サイバー攻撃からネットワークを保護することは極めて重要な課題です。それは単なるセキュリティ対策ではなく、学びを止めない「教育の継続性」を維持し、教職員や児童生徒の個人データを守り、攻撃に付随するあらゆる潜在的リスクを排除することに直結するからです。

## デバイス上での脅威防止とフィルタリング

デバイスレベルのセキュリティを強化しましょう。デバイス上で初回セキュリティスキャンとコンテンツフィルタリング調査が行われるので、利用者と組織両方のセキュリティを強化し、問題に先回りして対応できます。(Apple専用機能)

## コンテンツフィルタリング

### 制限の適用

Jamf Safe Internetで、YouTubeの制限付きモードやGoogleのセーフサーチを有効化。YouTubeの検索結果やコメント欄、埋め込み動画、Googleの検索結果などから不適切なコンテンツを除外することができます。

### コンテンツフィルタリングデータベース

教育業界向けに最適化された包括的なコンテンツフィルタリングとMDMが統合されたJamf Safe Internetは、ユーザを保護するためのシンプルで強固なソリューションです。軽量で高性能なドメインネームシステム (DNS) 技術を使用しているJamf Safe Internetでは、プライバシーを侵害することなく、学校のニーズに合ったコンテンツフィルタの結果を管理者側で作成・カスタマイズすることができます。

### ポリシーのスケジュール設定

学校にいる間は厳格な制限を適用し、家庭に持ち帰った際は柔軟な運用を許可するといった切り替えが可能です。時間に応じたポリシー設定によって、安全性やコンプライアンスの確保と、保護者の意向を反映した柔軟な対応を容易に両立できます。

## 脅威防御

### マルウェア、フィッシング、クリプトジャッキング対策

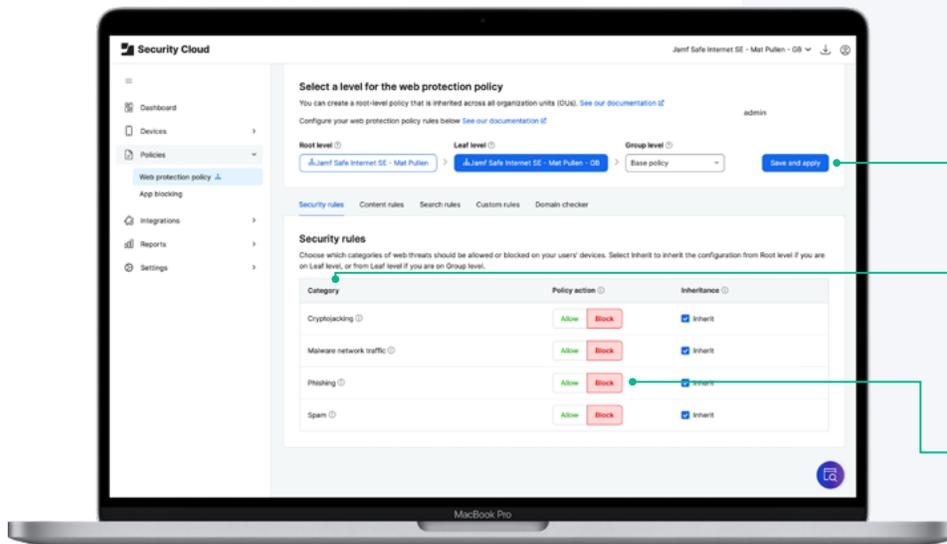
Jamf Safe Internetは、機械学習ツールを活用し、フィッシング、マルウェア、クリプトジャッキングなどのサイバー攻撃を特定および修復し、教育機関やそのネットワークの安全を守ります。

### プライバシー保護を最優先した、柔軟な設計

個人のプライバシー保護を最優先しながら、それぞれの導入環境に最適な形で適用できます。IT担当者による確実な可視化と保護により、生徒の安全を守り、プライバシーを保護。サイバー攻撃によるトラブルを未然に防ぎ、学びを止めることのない環境を実現します。

## カスタマイズ可能なコンテンツ制御

組織のニーズに合わせてセキュリティやコンテンツフィルタリングのポリシーをカスタマイズ。あらかじめ用意された設定の中から選ぶこともできます。



ポリシーの更新を保存して適用するだけ

幅広いブロックカテゴリ設定により、有害なコンテンツを遮断

1クリックで簡単に許可/ブロックを切り替え

お使いのMDMとJamf Safe Internetを連携させ、セキュリティとデジタルセーフティを基盤とした教育環境を構築しませんか？具体的な導入方法や活用イメージについて、ぜひお気軽にお問い合わせください。



www.jamf.com/ja/

© 2025 Jamf, LLC. All rights reserved.

Jamf Safe Internetで生徒とユーザを保護する方法について、くわしくはJamfのWebサイトをご覧ください。