Cyber Essentials 認定資格のススメ（教育業界向け）

jamf

「サイバーセキュリティ」と「教育業界」はかなり難解な組み合わせのように思えますが、微分積分に比べたら大したことありません。「Cyber Essentials」は、犯罪者やサイバー攻撃から生徒、教育者、デバイス、データを保護するための支援を教育機関に提供するためにイギリス政府とNational Cyber Security Centre（国立サイバーセキュリティセンター）が開発した認証プログラムです。

このeBookのトピック：

- 教育業界における変化がサイバーセキュリティの脅威に与えた影響
- 教育機関が実施すべき10の基本的なセキュリティ対策
- 「Cyber Essentials」の内容とその仕組み
- サイバーセキュリティの多くの課題に対処する上でこの資格の取得がどのように役立つのか

サイバーセキュリティとは、生徒、教育者、および彼らのデバイスを保護するための特定の対策や製品の導入を指すというよりは、むしろ現代の教育現場の「あり方」そのものを指す言葉と言えるかもしれません。ラルフ・ウォルドー・エマーソンの有名な格言を当てはめれば、「大切なのは目的ではなく、そこに至るまでの道のりだ」ということになります。さらに言えばこれは、攻撃者や不正アクセスからデータやプライバシーを守り、教育現場におけるリソースネットワークを強化するためにITやセキュリティチームが歩み続けなければならない、終わりのない道のようなものです。

これだけ聞くと、途方もない試みのように感じられるかもしれません。実際のところ、最新のサイバー脅威に精通していない人にとって、それは困難な道のりかもしれません。しかし、これは決して不可能ではありません。特に、macOSやiOSデバイスなどのIT資産のセキュリティ領域におけるエキスパートとして活躍する業界トップの組織と学校が手を組んだ場合はなおさらです。適切なパートナーと密接に協力し、さまざまなサポートを組み合わせてサイバーセキュリティの「面倒な仕事」に対応することで、教育関係者はAppleを使用する生徒やスタッフの成功を支援する自由を手に入れることができます。

> 「大切なのは目的ではなく、そこに至るまでの道のりだ」
>
> ラルフ・ウォルドー・エマーソン

サイバーセキュリティのパートナー

第一のパートナーは、教育関係者自身と、彼らを支援するITやセキュリティの専門家チーム（そのようなチームが存在する場合）です。次は、当然ながらAppleです。MacBook ProとiPadに対するAppleのセキュリティとプライバシーを最優先する姿勢には定評があります。Appleが開発するソフトウェアが後付けではなく、最初からmacOS、iOS、iPadOSに内蔵されていることにも、彼らのアプローチがよく表れています。

次のパートナーは、Appleにフォーカスしたデバイス管理とセキュリティソリューションの業界リーダーであるJamfです。例えばJamfSchoolは、デバイスの管理やセキュリティ設定の構成に加え、オンラインレッスンの管理や生徒とのコミュニケーションツールとして教育関係者が信頼を寄せる、Googleをはじめとする数々のベンダーのソフトウェアやサービスとの統合を備えています。パワフルなツールでありながら使い勝手が良いのは、日常的に発生する問題に管理者が簡単に対処できるよう、シンプルさを重視して開発されているからです。

最後のパートナーは認定機関です。Cyber Essentials認定は、もっとも一般的な脅威を含む多くのサイバー攻撃から組織を守るために役立つだけでなく、サイバーセキュリティに対する組織のコミットメントを証明するものでもあります。

この認定の内容に踏み込む前にまず、サイバーセキュリティの変化が教育や学習環境にどのような影響を与えたか、そして現場におけるモバイルデバイスへの移行について見ていきましょう。

変革の風

すでにお気づきかもしれませんが、サイバーセキュリティは動的なものであり、常に変化し続けるものです。Macを狙ったマルウェアがほとんど存在しなかった時代もありました。これは、Macへの侵入が難しかったというよりも、他のオペレーティングシステムに比べてターゲットとして人気がなかったからです。

ところが、Apple製品の爆発的な普及と、消費者やあらゆる組織での人気の急上昇により、マルウェアの作成者は、世界中に何億人ものユーザを抱えるAppleの肥沃で未開発の領域に目を向けるようになりました。

Jamfのセキュリティチームおよび研究部門である Jamf Threat Labsは、macOSおよびiOSベースのユーザに影響を与えるあらゆる脅威を積極的に監視・調査し、Jamfソリューションに最新の保護機能を組み込むだけでなく、攻撃トレンドを分析しそのデータを使用することで、製品や顧客に最高のセキュリティ環境を提供するためのガイダンスを提供しています。

いつでもどこでも学習にアクセスできる環境づくり

ここ数年、教育業界に起こった変化の中で、リモート学習ほど大きなインパクトを与えたものはないでしょう。教育機関は、パンデミックによって加速した安全性への配慮はもちろんのこと、従来の対面式の教育から、インフラの大幅なアップデートを必要とする新たなモデルへの突然の移行を余儀なくされました。セキュリティのアップデートはもちろんのこと、教育リソースへのリモートアクセスをすべての関係者に提供し、生徒と教師のために学習と指導に必要な最新のデバイスを導入しなければなりませんでした。

一部の教育機関は、新たな学習方法への大きなシフトに今も苦戦し続けています。これに伴い、悪質な攻撃者は攻撃手法や攻撃インフラをアップグレードし、教育の変化によってもたらされた不安定な状態を利用した作戦にシフトしていきました。これにより、リモートユーザを標的にした強引なフィッシング攻撃や、オンラインレッスンの妨害、マルウェアを使ったデバイスへの侵入、クラウドベースのストレージサービスを経由した機密データへの不正なアクセスなどが起こるようになりました。

ですが、悪いニュースばかりではありません。AppleのiPadのようなモバイルデバイスが教育現場に登場したことは喜ぶべきことです。薄型かつ軽量でありながら非常にパワフルで多機能なこのタブレットは、驚異的なバッテリー持続時間と強力な保護機能を内蔵しており、教育関係者や生徒にとって理想的な教育ツールとなっています。最新のテクノロジーが手頃な価格で手に入り、多くの教育関係者にとって不可欠なアプリやサービスに対応し、さらに優れたコミュニケーションツールでもあることから、場所や時間を問わずいつでも学習することが可能になりました。

サイバーセキュリティのトレンド予測

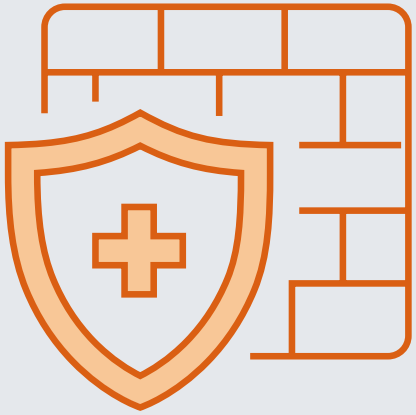
Jamfのレポート「Security 360: Annual Trends Report」は、2021年のトレンドについて以下のようにまとめています。

- リモートデバイスへのマルウェアのインストールが**2倍**に増加
- リスクの高いデバイス構成によって悪影響を受けた組織は全体の**1/5**にも及んだ
- セキュリティ侵害を受けたデバイスがコラボレーションアプリ（ZoomやMicrosoft Teamsなど）にアクセスする割合が**34%から64%**に増加
- 調査対象ユーザの約**半数**が、ネットワークトラフィックの保護におけるVPNの重要性を理解しているにもかかわらず、それを使用していないことを認めた
- Macベースのマルウェアは、攻撃者がその手法や標的をアップグレードして有効性を高めているため、その数だけでなく巧妙さにおいても**拡大を続けている**
- 2021年に起きた**フィッシングキャンペーン**でもっとも使用されたのはAppleだった
- プライバシーは、エンドユーザにとってだけでなくデバイスのセキュリティにとっても**不可欠**なものであり、規制へのコンプライアンスの観点からもエンドユーザのプライバシー維持はこれまで以上にその重要性を増している

脅威はファッションと同様、流行に左右されるものです。つまり、流行が終わり消えていくものもあるということです。また、時間をかけて進化し、最初とはまったく異なる形になったり、あるいはその悪質さを増したりするものもあります。

どちらにしても、サイバーセキュリティが継続的に築かれるものであることに変わりはありません。建物の増築に特別な道具が必要なように、まだ見ぬ新たなリスクや脅威、攻撃に対するセキュリティ体制を強化するためには、さまざまなセキュリティ対策をうまく利用する必要があります。

10の基本的なセキュリティ対策

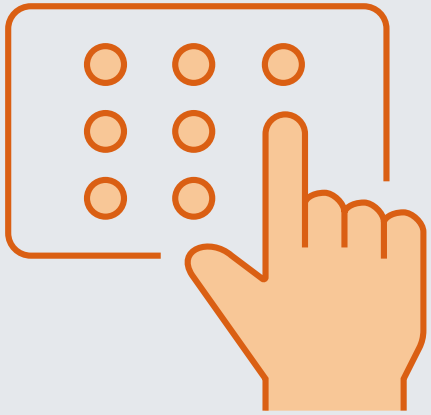


1 ファイアウォール

ファイアウォールは、安全に保たれなければならない内部のネットワークと、注意して扱う必要のあるインターネットとの間のバリアとして機能します。インターネットにアクセスできるすべてのデバイスにインストールする必要があり、学校や大学のデバイス、あるいは自分のデバイスで学習リソースにアクセスするために、公共のWi-Fiや安全性が確認されていないWi-Fiを使用する場合は特に重要です。

2 セキュリティ構成

デバイスやソフトウェアの初期構成は、使い勝手の良さを考えてできるだけオープンに設定されているケースが多く、その分、不正なユーザにとってもアクセスしやすくなっています。不要な機能を無効化または削除したり、デフォルトのパスワードを変更したりすることで、セキュリティ侵害のリスクを軽減することができます。

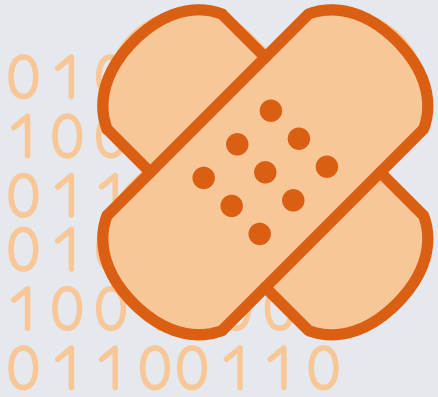


3 アクセス制御

多くの人にデータやサービスへのアクセスを許可することは簡単ですが、その分、不正アクセスを受けたアカウントによって深刻なセキュリティ侵害がもたらされる可能性も高くなります。また、誰かが誤って残すべきデータを削除してしまうなど、意図しないトラブルが発生する可能性も高くなります。アクセスを本当に必要とする最低限のユーザだけに許可し、それ以外はデフォルトでアクセスを拒否することで、侵害の可能性を最小限に抑えることができます。さらに、すべてのアカウントを強力なパスワードで保護し、管理者アカウントなど侵害のリスクが特に高い場合には2段階認証（2FA）の導入を検討することを推奨します。前述のサイバー攻撃も、2段階認証があれば防げた可能性があります。

4 マルウェア対策

例えば教職員がフィッシング詐欺などに遭った場合に、システムがウィルスやランサムウェアなどのマルウェアに感染することがあります。また、USBメモリなどのリムーバブルディスクなどもよく感染経路になります。マルウェアから組織を守るためには、アンチウイルスやマルウェア対策ソフトウェアに加え、他のネットワークやデバイスにアクセスできない隔離された環境でアプリケーションを実行した上で悪意の有無を調べる「サンドボックス」といった手法や、許可リストなどを使用するのが一般的です。



5 パッチ管理

ソフトウェアメーカーや開発者は、ソフトウェアを改善するためだけでなく、発見された脆弱性を修正する「パッチ」を当てるためのアップデートを定期的にリリースします。アップデートがリリースされたらすぐにインストールすることで、こういった脆弱性が悪用される可能性を最小限に抑えることができます。メーカーがハードウェアやソフトウェアのサポートを終了した場合は、もっと新しいものに替えるべき時期が来たことを意味しています。

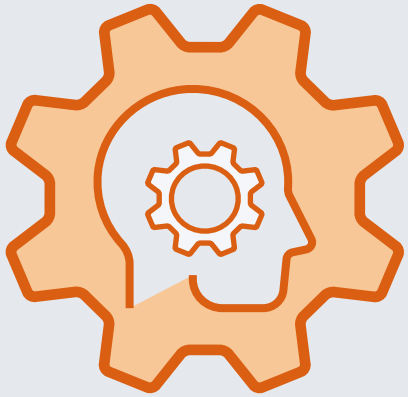
注意：ここまでの5つをクリアすれば、Cyber Essentials認定（詳細は後述）の取得には十分ですが、Jamfでは、完全なセキュリティソリューションにはさらにいくつかの要素が必要であると考えます。

6 アイデンティティのプロビジョニング

クラウドベースのアイデンティティプロバイダ（IdP）は、ユーザアカウントの一元的管理とリモートデータベースを利用した安全な認証を可能にし、Webベースのサービスや公共またはプライベートのクラウド、SaaSプラットフォームから提供される教育リソースへのローカルまたは外部からのアクセスリクエストを処理するために使用されます。認証リクエストはポータル経由でプロビジョニングすることもでき、シングルサインオン（SSO）を有効にすることで、すべての必要なリソースに一箇所からアクセスできる環境をユーザに提供します。

7 ゼロトラストネットワークアクセス（ZTNA）

ZTNAは、VPNに代表されるネットワークベースの通信だけでなく、境界のないセキュリティをも可能にする革新的な最新のアクセスソリューションです。アプリケーションごとのマイクロトンネルを作ることで、どこからどのような通信手段を使っても、安全にリソースに接続できるようになります。また、IdPとの統合により、認証情報に基づいたリソースへのアクセスも可能になります。さらに、デバイスの健全性をチェックし、アクセスを許可または拒否（コンプライアンスが確認されるまで）することができるため、リスクの軽減につながります。



8 機械学習

自動化は、機械学習技術の数ある利点のひとつです。コンピュータがデータの流れを定量化し、過去の攻撃データと特定のアプリやサービス、攻撃者のデータの相互関係性など、共通点の有無について調べてくれるため、ITやセキュリティチームは、すでに発生した攻撃に関する情報だけでなく、将来の攻撃を未然に防ぐために必要な豊富な知識も得ることができます。やはり、データを分析するスピードにおいては、人間の手作業はコンピュータには到底及びません。

9 モバイル脅威防御（MTD）

デスクトップベースのセキュリティソリューションと同様に、MTDもマルウェアからの防御や、iPadやiPhoneなどのモバイルデバイスを標的としたセキュリティ脅威からの保護を提供します。それではなぜ、わざわざ別のソフトウェアを用意する必要があるのでしょうか？簡単に言えば、モバイルデバイスとmacOSベースのデバイスの設定が異なるからです。モバイルデバイスを攻撃するために攻撃者は新たな手法を開発します。そのため、ポリシーベースの管理とコンプライアンスを確認するための定期的なデバイスの健全性チェックを通じて、マルウェアからネットワークベースの攻撃まで、モバイルを狙ったさまざまな脅威からの保護を提供してくれるクラウドベースのソリューションが必要になります。

10 コンプライアンス基準の遵守

教育業界は何かと規制の多い業界です。世界的に見ても、教育業界はサイバーセキュリティ攻撃の最重要ターゲットとして認識されており、残念ながら数ある業界の中でもっともセキュリティが緩いことがわかっています。セキュリティが緩く、攻撃の対象となる確率が高く、さらに政府からの規制も受けている教育業界においては、データ侵害はすべての関係者にとって非常に深刻な問題になります。コンプライアンスを維持することは、口で言うほど簡単ではないものの、不可能なことではありません。これは学校にとっても、強固なセキュリティ体制を確立し、脅威のリスクを最小限に抑え、デバイスが必要なレベルに構成されていることを確認するための良い機会となります。デバイスの性能と構成レベルが常に決められたベースラインを保っていれば、セキュリティ侵害が起きてもより迅速に立ち直ることができます。

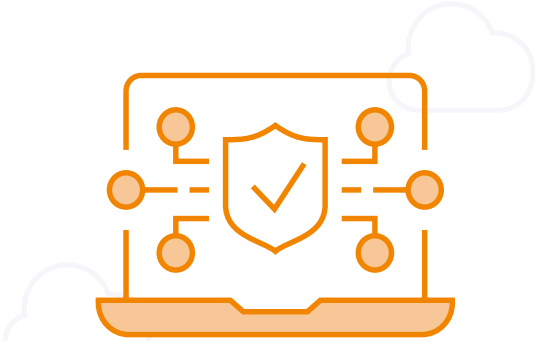
ここまで、現代の学校における学びに影響を及ぼす可能性のある無数の脅威や課題を含め、教育業界におけるサイバーセキュリティの現状について見てきました。さらに、未来を作る子どもたちを教育する今日の教育者たちをサポートする基本的なセキュリティ対策についても説明しました。ここからは、Cyber Essentials認定と、それが教育業界の目標達成にどのような形で貢献できるかについて見ていきましょう。

「Cyber Essentials認定」とは？

イギリスのGDPRウェブサイトによると、Cyber Essentialsは、イギリス政府がNational Cyber Security Centre（NCSC）の協力を得て始めたプログラムで、あらゆる規模の組織が手間や膨大なコストをかけずにサイバーセキュリティへの取り組みを実行できるよう支援することを目的としています。

Cyber Essentials認定は、以下の5つの基本的なセキュリティ要件を設けています。

1. ファイアウォール
2. セキュリティ構成
3. アクセス制御
4. マルウェア対策
5. パッチ管理



NCSCによると、上記の**5つ**の主要なサイバーセキュリティ対策に焦点を当てることで、教育機関は「一般的なサイバー攻撃の**約80%**」から身を守ることができます。

Cyber Essentials認定の取得が重要な理由

イギリスでESFA（Education and Skills Funding Agency）から資金援助を受けている教育機関に対し、2021年からCyber Essentialsの認定取得が義務づけられるようになりました。社会の他のエリアと同様に、教育業界においてもサイバーセキュリティを向上させるというイギリス政府の推進をサポートするためです。

Cyber Essentials認定を取得することで、教育機関はサイバーセキュリティとユーザのプライバシー保護に真剣に取り組んでいることを生徒、教育者、すべての関係者に示すことができます。また、以下に示すセキュリティ対策の実施を通じて、学校内のセキュリティ意識の向上を推進するだけでなく、「**適切な技術的・組織的対策**」により機密データの機密性と整合性を保護することができます。

Cyber Essentials 認定を取得するメリット

Cyber Essentialsプログラムは、もっとも一般的なサイバー攻撃の脅威を最小限に抑えてリスクを軽減することを目的としています。NCSCの推計によると、サイバー攻撃の約**80%は、セキュリティ対策がまったく、またはほとんどされていない相手に対して行われ、多くの場合、犯人はリモートで自動化された攻撃を実行します。**

前述の**5つのセキュリティ対策**を実施することで、このようなサイバー攻撃が実際に発生するのを未然に防げる可能性があります。もし、攻撃によってデバイスが危険にさらされたとしても、適切なセキュリティ対策により提供された保護機能がデバイスの前に立ちはだかり、攻撃の影響を最小限にとどめてくれます。

攻撃に対する予防策が優れていればいるほど影響も小さくて済み、ダメージの評価や修復に要する時間も短縮されるため、生徒や教師も迅速に学習や指導に戻ることができます。

Cyber Essentials 認定の仕組み

Cyber Essentials認定には、2つのレベルがあります。いずれの場合も、5つの基本的なセキュリティ対策が実施されていることを証明するための自己評価アンケート（SAQ）に回答し、評価を受けます。

Cyber Essentials認定：SAQへの回答が必須となります。

Cyber Essentials Plus認定：SAQに加えて、以下の技術検証を実施することが求められます。

- 外部からの脆弱性スキャン
- オンサイト評価
- ネットワークベースの脆弱性スキャン

Cyber Essentials認定の取得に踏み出す前に教育機関のサイバーセキュリティ対策が十分であるか確認しておきたい場合は、NCSCと公式に提携しているサービスプロバイダが提供する無料のアセスメントを受けることができます。これにより、学校所有のコンピュータやネットワークに関する詳細なインサイトを得ることができます。さらに、実際にSAQに回答する際に含めなければならない内容についても詳細に知ることができるため安心です。

> 「千里の道も一歩から」
>
> 老子

Jamf + Cyber Essentials認定

教育機関とサイバーセキュリティにとって最高に相性の良い組み合わせです。

jamf

Cyber Essentials認定の申請に関する詳細はNational Cyber Security Centreのウェブサイトをご覧ください。

Jamfを活用して安全なデバイス管理を行い学校をサイバー脅威から守る方法に興味のある方はこちらから

トライアルに申し込む

または、お近くのApple製品販売代理店へお問い合わせください。