KEEPER®

教育現場のサイバーセキュリティ事情
デジタル時代に生徒を守るには

概要

近年では、日本でもEdTech (エドテック) が推進されているように、学校にてタブレットの導入から、オンライン授業、学習アプリなどのデジタルツールの導入が進んでおり、現代の教育現場ではテクノロジーは切り離せないものとなりつつあります。しかし、21世紀の急速なデジタル化に伴い、新たなサイバーセキュリティのサイバー脅威がもたらされており、教育関係者にとっては無視できないものとなっています。

2024年のKeeper Securityによるレポートでは、オーストラリア、ニュージーランド、シンガポール、インドネシア、日本、フランス、イギリス、アメリカ、DACH地域の6000人を対象に行われたアンケート調査に基づいており、16歳以上の学生、保護者、一般人が均等に含まれています。レポートでは、学校がデジタル時代において生徒の個人情報を保護する能力に関して信頼が寄せられている一方、現実の状況には乖離が見られることが明らかになっています。

保護者の多くは、学校で機密的な個人情報が保護されていると信じていますが、脆弱なパスワードの使用やパスワードの使い回しなどの根深い問題やサイバーセキュリティ教育の不足により、生徒は情報漏えい、個人情報の盗難、フィッシング詐欺などの絶え間ないサイバー攻撃の脅威にさらされています。このレポートの調査結果では、学校と家庭がより強力なサイバーセキュリティ対策で協力し、インターネット上の危険性に対する生徒の意識を高めることが差し迫って必要であることが明らかになっています。

KEEPER

教育現場における現在のサイバーセキュリティ実践

Keeper Securityの調査では、学校でのサイバーセキュリティ実践におけるさまざまな状況が浮き彫りになっています。保護者の74%は、子供の学校での機密情報の保護について信頼を寄せている一方で、学校での実際の対策はこの信頼に見合っていないことがわかっています。学校で安全なパスワードの作成と管理に関する指導が行われていると報告したのは、保護者の21%に留まっており、それが安全ではないパスワードを使用する習慣に繋がっています。回答者の19%が、個人のアカウントと学校のアカウント間でパスワードを使い回していることを認めており、より大規模なデータ漏えいの危険性を高めています。

学校のサイバーセキュリティ対策への信頼

18%
非常に自信がある

56%
やや自信がある

22%
あまり自信がない

4%
全く自信がない

パスワード管理の実践

21% 安全なパスワードに関する指導を行っている学校

19% アカウント間でのパスワードの使い回し

9% パスワードマネージャーへのアクセスを提供している学校

安全なパスワードマネージャーの利用が限られていること (アクセスを提供している学校は9% のみ) が、これらのリスクをさらに悪化させています。複雑なパスワードを安全に作成および保存、管理するためにはパスワードマネージャーは不可欠であり、政府機関やサイバーセキュリティの専門家によって推奨されているパスワードマネージャーが特に不足しているため、学校がサイバーセキュリティ対策を大幅に改善できる明らかな機会となっています。

サイバーセキュリティ教育の強化の必要性

学校におけるサイバーセキュリティ教育は非常に不足しており、セキュリティ意識向上トレーニングが義務付けられている学校はわずか14%に留まり、13%の学校では任意で提供されています。この義務付けられたトレーニングが限られているということは、多くの家庭でオンラインの安全性に関する最新の教育を受けられず、生徒が進化するサイバー攻撃の脅威に対して脆弱なままになっているということを意味します。効果的なサイバーセキュリティトレーニングの中には、フィッシング詐欺の特定方法、デバイスの保護対策、定期的なソフトウェアアップデートの重要性だけでなく、生徒がデジタルタトゥーやデジタルフットプリントなどを悪い形でインターネット上に残さないように安全な指導をすることにも重点を置く必要があります。

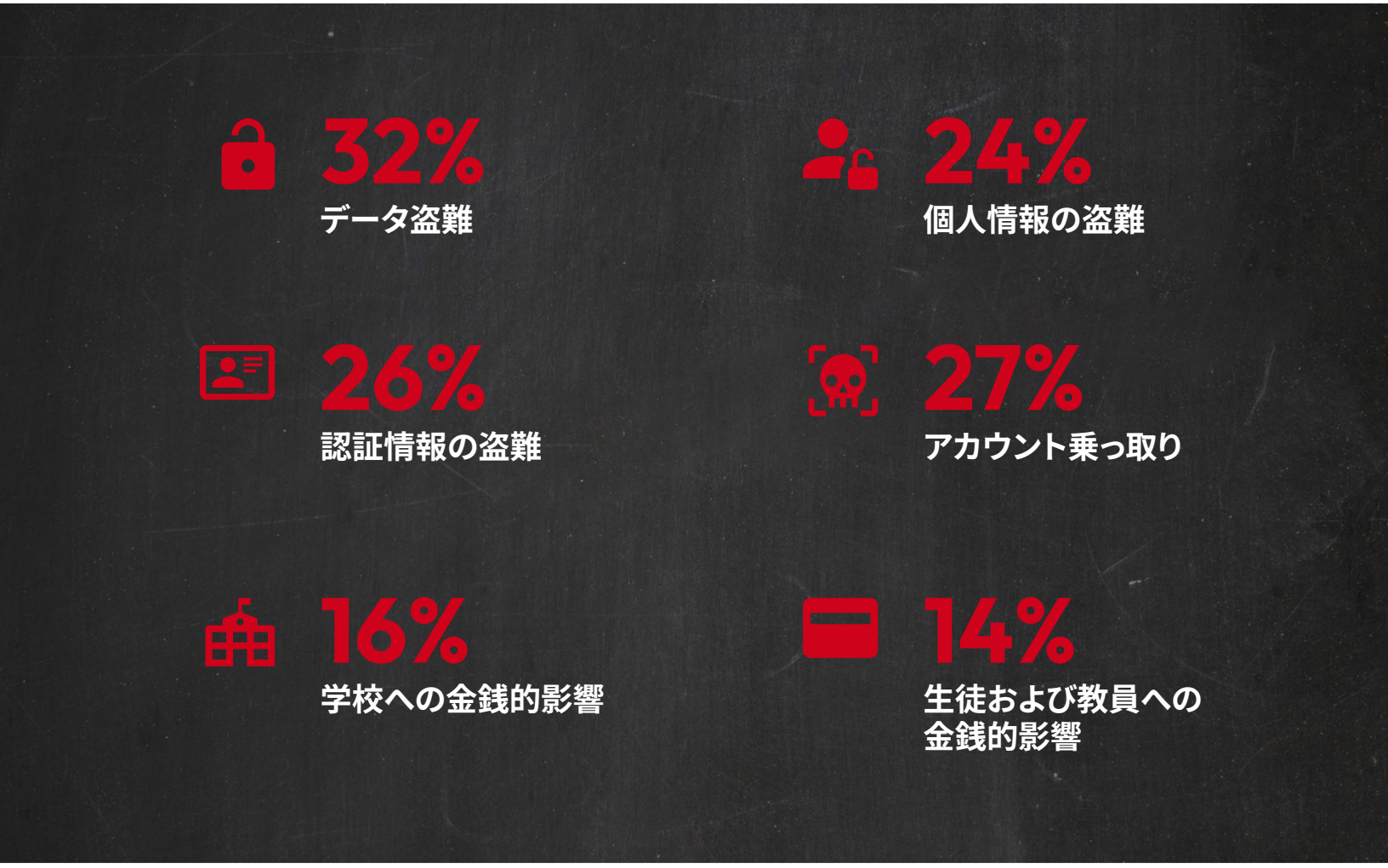
生徒にソーシャルメディアの投稿や閲覧習慣などのオンライン活動の影響について教えることは、個人情報を保護するための鍵となります。たとえば、ソーシャルメディアのプライバシー設定で一般公開を制限することが重要となります。サイバー犯罪者がどのようにしてデジタルフットプリントを悪用して個人情報を盗難したり攻撃の標的としたりするかについて教育することは、責任あるオンライン行動を促す上で重要となります。

学校でのサイバーセキュリティトレーニング

- **21%** 学校のサイバーセキュリティへの期待を認識していない
- **20%** サイバーセキュリティについては個人の責任
- **14%** 必須のトレーニング
- **13%** 任意のトレーニング
- **12%** サイバーセキュリティリソースへのアクセス

サイバーセキュリティインシデントが学校に与える影響

教育機関に対するサイバー攻撃は、生徒、教員、管理者などに深刻かつ広範な影響を与える可能性があり、アカウントと機密データを保護するための強固なセキュリティ対策の必要性が裏付けられています。調査によると、自分の子供または自分の教育機関がハッキングされたと報告したのは回答者のわずか7%でしたが、その影響は重大でした。このような不正アクセスの影響について尋ねたところ、回答者からは以下のような影響があったとの返答がありました。



データと個人情報の盗難の増加は、個人のプライバシーと組織のセキュリティに対する深刻なリスクを浮き彫りにしています。認証情報の盗難やアカウントの乗っ取りの蔓延によって甚大な被害が生じる可能性があり、機密情報の漏洩につながる可能性があることを示しています。金銭的な影響はあまり報告されていないものの、学校と個人の両方にとって重要な問題となっています。サイバー攻撃の影響はデータや個人情報の露出にとどまらず、さらに広範囲にわたることが浮き彫りになっています。

KEEPER

サイバーセキュリティにおける家族の役割

家庭でのサイバーセキュリティ実践を強化するには、保護者が重要な役割を果たします。しかし、Keeperの調査によると、 19%の家庭でパスワードが使い回されていることがわかりました。パスワードの使い回しは危険で、クレデンシャルスタッフィング攻撃によって複数のアカウントが不正アクセスされる可能性があります。多くの学校でサイバーセキュリティのリソースが不足する中、家庭で強力かつランダムなパスワードと多要素認証 (MFA) を使用することで現状を改善する手助けができます。MFAには、2FAなどの認証も含みます。 MFAでログイン時に別の認証方式をもう1つ設定することで、安全性が飛躍的に向上します。

回答者の半数以上 (51%) が 学校のサイバーセキュリティについて「非常に心配」または「やや心配」であると報告しており、サイバーセキュリティ対策が不十分である一方で、保護者はリスクを認識していることを示しています。これらのリスクに対処するために、家族は子供のインターネット上の活動を監視し、家庭内でのサイバーセキュリティのベストプラクティスを遵守することが重要となります。これには、疑わしいメールやリンクを認識する方法を学び、強力かつランダムなパスワードを使用し、出来る限り多要素認証を設定し、既知の脆弱性から保護するためにソフトウェアを定期的に更新することなどが含まれます。

まとめ: 教育現場と家庭間の両方からサイバーセキュリティに取り組むことが重要

学校におけるサイバーセキュリティの基準を引き上げるには、教育現場と生徒の家族の双方による協力的な取り組みが必要です。学校では、サイバーセキュリティ教育プログラムを強化し、パスワードマネージャーなどの効果が証明されているツールを取り入れ、サイバーセキュリティのベストプラクティスを網羅するトレーニングを拡大する必要があります。家庭では、好ましいサイバーセキュリティ習慣を強化し、子供のデジタル教育に積極的に参加することで、これらの取り組みをサポートする必要があります。

学校と家族が協力して生徒のためにより安全なオンライン環境を整え、技術の進歩を最大限に活かすことで、サイバーセキュリティの危険性を最小限に抑えることができるのです。

調査方法

このオンライン調査は、オーストラリア、ニュージーランド、シンガポール、インドネシア、日本、フランス、英国、米国、DACHの回答者6000人を対象とするもので、市場調査会社 OnePollにより、市場調査協会の規定に則って実施されました。この調査はOnePollの調査チームが監督、編集しました。OnePollは、MRSの企業パートナー、ESOMARの企業メンバー、英国世論調査協議会のメンバーです。