監視せずに生徒を守るための教育テクノロジー

どの学校にも、生徒の健康と安全に対して一定レベルの責任があります。 生徒の安全性というテーマは、さまざまなエリアを広範にカバーするものであり、安全対策を実施する地区や学校による解釈の余地が大きいものです。

データ収集を伴わないプライバシー重視のコンテンツフィルタリングから、学校支給のデバイスへのキーロガーのインストール、生徒が入力および送受信するすべてを監視するものまで、どのレベルで安全対策を実施するかは、各学校が決めることになります。

このホワイトペーパーのトピック

- 「監視」と「モニタリング」の意味
- これらの言葉が教育や生徒のプライバシーに及ぼす広範な影響
- 何をすべきかについて十分な情報を得た上で意思決定を行えるよう、テクノロジーポリシーの策定において考慮すべき点

問題点

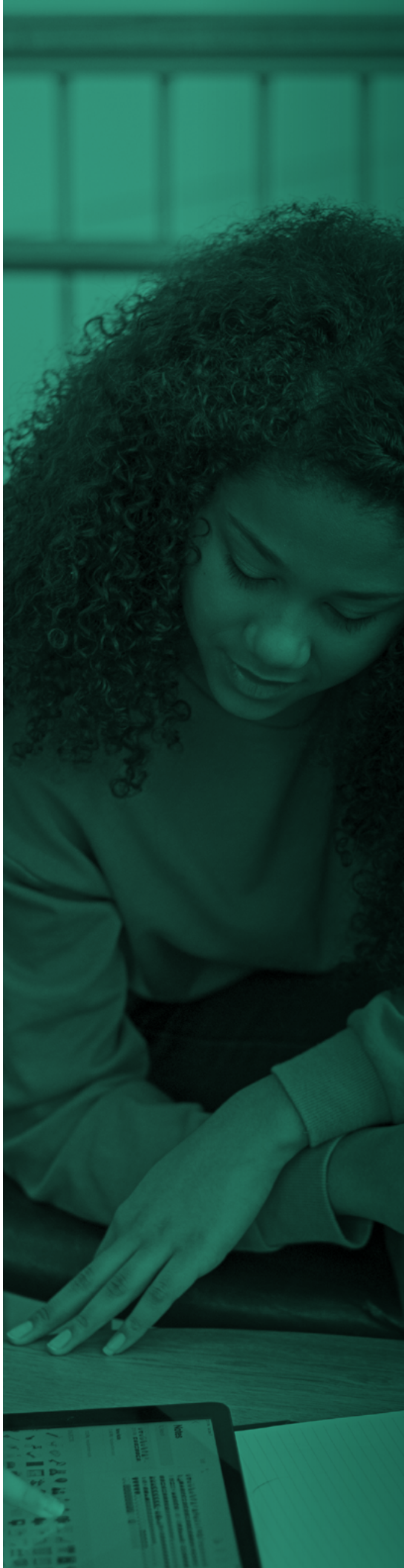
教師、保護者、ヘルスケア専門家、学校の上層部、友人など、生徒の人生にはありとあらゆる人々が関わります。**米国の生徒が学校で過ごす時間は、平均して年間約1000時間**（日数にして180日間）であると言われています。このことは、教師やその他の学校関係者が、教育、メンタルヘルス、技術指導、全般的な幸福度などを含む多くの点や、ひいては生徒の人生そのものに大きな影響を与えることを意味します。

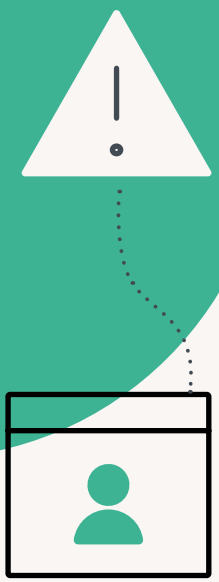
教育機関は、生徒の安全を守るためにインターネットの使用を厳しく取り締まっており、不適切な言葉の使用、自傷行為や暴力の可能性を示唆するインジケータ、生徒間のいじめまでチェックする場合もあります。学校はあくまでも生徒の生活の一部に過ぎず、学校の監視外で自分のデバイスを使っている生徒もいます。この場合、学校は生徒の心身の健康チェックにどの程度関与すべきなのでしょうか？そして、どの程度オンラインでの活動のチェックを行うべきなのでしょうか？残念ながら、明白な答えはありません。

インターネットは生徒を教育するための多大なパワーを教育機関に与えてくれます。生徒に合わせた教育アプローチ、無限の情報、その他数え切れないほどのリソースを利用できることは、情報が氾濫する現代社会で生徒の学習を確実にサポートします。しかし、このようなパワーを手に入れるということは、生徒がどのようにオンラインコンテンツ（中には不適切なものや危険なものもある）と接するべきかを考える責任を負うことを意味します。

教育は、オンラインに存在する知識の活用にとどまりません。学校は、生徒の安全とセキュリティを確保しながら、生徒が自立した責任あるインターネット利用者になることを願っています。しかし、これらのコンセプトを両立させる明確な方法はないため、オンラインにおける生徒の安全に対してはさまざまなアプローチが存在します。生徒にインターネットの安全かつ適切な使用方法について教えておきながら、膨大なインターネット世界に彼らを放り込み、自由に探索させるべきなのでしょうか？それとも、学校側が事前に安全であることを確認したサイトだけにアクセスできるようにすべきなのでしょうか？

この正反対のアプローチ、つまり探索する自由とアクセスの制限は、教育界に存在するさまざまな問題を象徴しています。中間を取って、生徒に適度に目を配りながらある程度自由に探検を許可するべきでしょうか？それとも、どちらか片方の立場から生徒の安全性という問題を解決すべきでしょうか？もしくは、もっと良い選択肢があるのでしょうか？学校のルールの枠を超えて、生徒の安全を総合的に守るにはどうすればいいのでしょうか？





さまざまなアプローチの理解

生徒データの扱い方にはいくつかのアプローチがあります。1つ目は**モニタリング**です。

モニタリング

生徒のインターネット利用をモニタリングする場合、彼らがいつどのサイトにアクセスし、どの程度の時間を費やしたかについてデータを収集することができます。これにより、以下のようなアクセスのパターンが浮き彫りになります。

- 生徒たちが検索するコンテンツの種類
- コンテンツが検索される時間帯（学校にいる時間か、それ以外か）
- 生徒がもっとも時間を費やしているコンテンツ

モニタリングは生徒自身ではなくデータにフォーカスし、誰がアクセスしたかではなく、どのウェブサイトがアクセスされたかを見ます。これにより、生徒たちの一般的な行動を把握し、潜在的な問題に対応することができます。

データの収集・保存方法によっては、個人を特定できる情報（PII）の収集を減らし、生徒のプライバシーを保護しながら、学校にとって貴重な洞察だけを得ることも可能です。匿名データを収集することで、増加傾向にあるデータ流出によって失われる個人情報の量を減らすこともできます。

2つ目は**監視**です。

監視

監視はモニタリングをさらに強化したもので、多くの場合、不適切な行動をリアルタイムで特定するために個人とデータを関連付けます。個人の検索履歴を記録したり、キー入力を分析したり、プライベートメッセージを覗いたりする場合もあり、学校所有デバイスのみを対象に実施する学区がある一方で、**ソーシャルメディア**における生徒の行動まで監視する学区もあります。

監視は、生徒の有害な行動が自身や他人にとって危険になる前に発見することができ、この理由から監視を選ぶ学校も少なくありません。しかし、生徒のプライバシーを侵害したり、**学校に不信感を抱かせたり**、脅威でないものを誤検知したり、**特定の層を不当にターゲット**にしたりしせずにこれを実施するのは、非常に難しいことです。

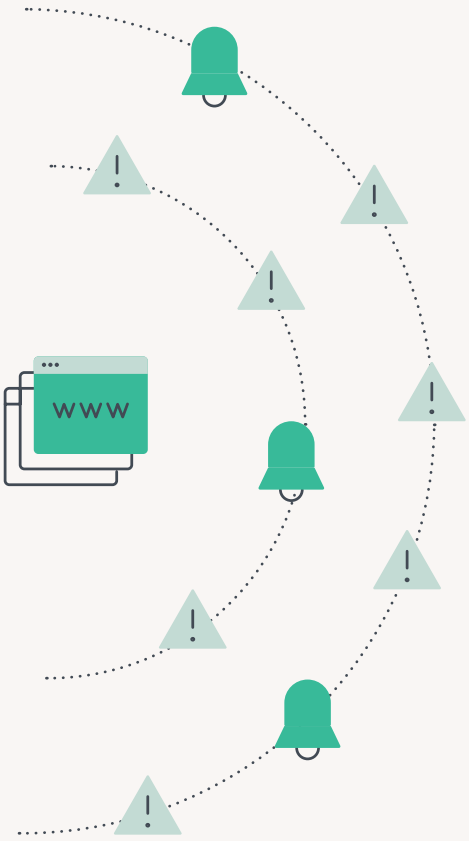
最近**Center for Democracy and Technology**が行った調査によると、学校が取得したデータに基づいて警察から連絡を受けた生徒を知っていると答えた教師は44%に上りました。また、**LGBTQ+の生徒の29%**が、自分か自分の知り合いがこのテクノロジーによって暴露されたと報告しています。

監視が学校だけでなく、生徒の生活のあらゆる側面に影響を及ぼしていることは否定できない事実です。大人たち自身がこのレベルの監視が自分に課されることを許さないのに、これが現状だから仕方ないと生徒たちを説き伏せてしまって良いのでしょうか？

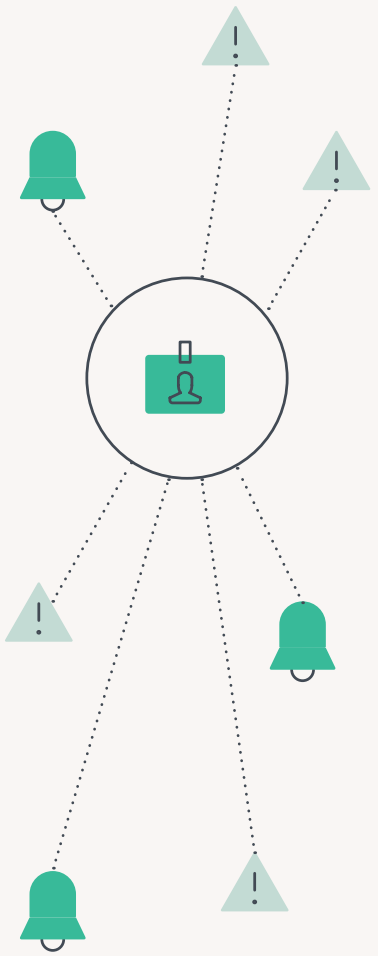
データが増えれば問題も増える

生徒の個人情報の収集と使用は、さまざまな問題を引き起こす可能性があります。

まず第一に、低所得層の生徒はプライバシーに関して不公平な立場にあります。個人用デバイスを持っておらず、学校から支給されたデバイスしか使用できない生徒は、より高いレベルで監視されることになります。それに対し、保護者が高収入の生徒は、プライバシーを守るためにiPhoneやiPadのような自分専用のデバイスを使うことができます。リモート学習が生徒に与える影響を調査した**2020年のマッキンゼーのレポート** によると、自宅でインターネットに定期的にアクセスできない生徒は全体の9%ほどで、黒人やヒスパニック系の生徒はさらに3〜4%少ないことがわかりました。テクノロジーの不平等により、これらの層は監視の影響を受けやすくなります。



モニタリングツールは、若者のうつ病や不安が急増している今、苦しんでいる若者を特定し、彼らに必要なメンタルヘルスケアを提供するのに役立つと教育者たちは考えています。しかし、非営利団体**National survey by the Nonprofit Center for Democracy and Technology（CDT）が全米で行った調査**の結果は、それとは異なる現実を映し出しており、多くの生徒が助けを得るどころか、学校の規則を破ったことで罰を受けているということがわかっています。また、生徒が差別を受けているケースもこの調査で浮き彫りになりました。テクノロジーは本当に生徒の役に立っているのでしょうか？学校によってさまざまな意見や実践方法がありますが、ひとつはっきりしているのは、テクノロジーだけでは十分ではないということです。



徹底的な監視対策は確実な安全性の向上につながると考えられがちですが、実際のところ、こういったデータを収集することで可能になる機能の有効性は乏しく、このような対策を実施する学校を法的リスクに晒す可能性があることがわかっています。検出は、あらかじめ設定された一連のキーワードに一致した場合にアラートを発することで行われます。この方法による誤検知は膨大な数に上りますが、それでも学校には全てのアラートに対応する責任があります。

これらのアラートは、もし本物であれば、生徒が潜在的な問題を抱えていることを知らせてくれますが、多くの場合、そうなる前から生徒にトラブルの兆候が見られているケースは少なくありません。結局のところ、全般的な態度、外見、学業成績、仲間との関わり方、雰囲気、出席状況など、人間の目で実際に見なければわからない兆候が必ず存在します。つまり、生徒の問題の発見をテクノロジーに頼ることは、多くの場合効果がなかったり、遅すぎたりすることが多いのです。

監視よりも予防

多くの学校は、ギャンブルやアダルトコンテンツ、ゲームなど、教育現場にはふさわしくない不適切なサイトへのアクセスを制限することで、生徒が安全にインターネットを閲覧できるようにしたいと考えています。生徒がこのようなコンテンツにアクセスするのを防ぐためのツールとして、コンテンツフィルタリングが挙げられます。これは、安全性がある程度担保されたインターネットへの自由なアクセスにより適したアプローチです。生徒は、インターネットを探索する自由を得ながらも、それを有害なコンテンツへのアクセスが制限された環境で行うことができます。

コンテンツフィルタリングが適用され、有害なコンテンツに生徒がアクセスできないことが保証されれば、生徒がどのウェブサイトを閲覧しているかを調べる必要性がなくなります。これは、先ほどの生徒のプライバシーに関する問題にも関係します。教育機関は、生徒がしていること全てを把握すべきなのでしょうか？それとも、生徒の安全に懸念が生じた場合のみ、そのオプションを検討すべきなのでしょうか？

特定のサイトやコンテンツタイプへのアクセスを積極的にブロックすることで、教育組織は教室における日々の学習や授業をサポートするためにインターネットを有効活用することができます。言い換えれば、生徒たちは、アクセスすべきでないものにアクセスすることなく、カリキュラムで求められる内容だけを中心に知識を深めることができるのです。また、承認済みの一握りのサイトだけにアクセスを制限したり、あるいはもう少し幅広く承認済みのカテゴリにアクセスを許可したりできるツールも存在します。これにより、生徒は自分なりの方法で学び、さまざまなソースから知識を獲得し、インターネットを味方につける方法を身につけることができます。言い換えれば、生徒たちは授業に関連した内容を学ぶだけでなく、「良きデジタル市民」になる方法を学び、今後の人生に役立てることができるのです。

一方で、より反応的なアプローチとして、生徒が何にアクセスしているかを分析し、必要に応じて介入する方法がありますが、これはコンテンツがすでに監視されていることを前提とします。この場合、組織の誰かがデータに目を通し、何が閲覧されたかを確認し、最終的にITスタッフの力を借りてそれに対処する必要があります。

解決策

国連の「子どもの権利条約」は、
子どものプライバシーに関して以下のガイダンスを掲げています。

1. いかなる児童も、その私生活、家族、住居若しくは通信に対して恣意的に若しくは不法に干渉され又は名誉及び信用を不法に攻撃されない。

2. 児童は、上記の干渉又は攻撃に対する法律の保護を受ける権利を有する。

この条項は、子どものプライバシーを保護するための優れた原則を提供してくれますが、一方で生徒を危険から守るバランスの取れたテクノロジーポリシーを実施する方法についての明確な指針は提供されていません。そのため、ここに定められたプライバシーに対する権利を理由に、生徒たちが学校所有デバイスを使用する際の監視をやめるよう訴えたり、自らの個人情報を学校が扱う方法に干渉したりすることはできません。これは学校のネットワークを使用する個人デバイスにまで及ぶ可能性があり、利用規約（AUP）によって明記されたデータ採取の影響を受けやすくなります。言い換えれば、学生は教育機関がどのようにデータを収集するかについて選択の余地がなく、特にモバイルデータや私的デバイスを利用できない学生には影響が大きくなっています。

その結果、組織は生徒の安全性についての独自の認識に基づいて、ポリシーやプロセスを考え出さざるを得なくなっています。結局のところ、生徒を取り巻く危険は、インターネットサイト、同級生、自分自身など、さまざまなところに原因があります。学校はコミュニティからの圧力に反応せざるを得ず、生徒が命を失うという最悪のシナリオを防ぐことに大きなプレッシャーを感じていいます。

テクノロジーは万能薬ではない

では、学校は実際に何をすべきなのでしょうか？前述したように、テクノロジーだけでは生徒の安全を守ることはできません。あらゆる関係者のサポートが欠かせないのです。生徒たちは、インターネットのコンテンツ、家族や友人との関係、自分自身のメンタルヘルスやアイデンティティ、家庭の状況など、人生のあらゆる側面でサポートを必要としています。スクールカウンセラー、教師、ヘルスケア専門家、学校の上層部など、すべての関係者が生徒の安全を守るために生徒と重要な関係を持つ必要があるのです。テクノロジーは生徒の生活全般を支配するのではなく、生活を良くするための解決策の一部でなければなりません。監視は、専門家がリスクがあると認定した生徒を綿密に調査する必要がある場合のみ検討されるべきで、デフォルトとして全員の生徒に適用されるべきではありません。生徒は、卒業後にインターネット全体を自由に探索できます。在校中にインターネット使用が制限された場合、卒業後にどのようにしてインターネットの脅威に備えれば良いのでしょうか？

優れたコンテンツフィルタリングを採用することで、不品行な生徒を探し出すために自分の言動や考え方のすべてが精査されていると生徒に感じさせることなく、学校にいる間に気を散らすコンテンツや有害なコンテンツを制限することが可能になります。さらに、住む場所や人種、保護者の所得などによって生徒を差別しないコンテンツフィルタリングを学校のネットワークに追加することで、特定のグループが直面している不平等を軽減することができます。

コンテンツフィルタリングの採用だけでなく、学校は収集したデータを保護するためのサイバーセキュリティのベストプラクティスに従うべきです。これには以下が含まれます。

- 生徒アカウントを明確なプロビジョニングとアクセス制御で保護
- 生徒の個人情報にアクセスできるデバイスやアプリケーションへの厳重なアクセス制御の適用
- サイバー攻撃に備えた明確な計画の策定
- エンドポイント検出と応答（EDR）ソフトウェアによるエンドポイントのセキュリティ確保
- 復旧に備えて定期的にデータのバックアップを取得
- データサーバとデバイスの暗号化
- SIEM（セキュリティ情報イベント管理）ソフトウェアの導入
- インターネット利用のリスクについて教職員や生徒に教えるためのトレーニングプログラムの構築

まとめ

- 学校には有害なインターネットコンテンツから生徒を保護する責任があるものの、生徒のオンラインでの行動についてどの程度詳しく調べるべきかに関して明確な指針は存在しない
- 生徒のオンラインでの行動すべてを監視することは、生徒の幸福度に悪影響を及ぼす可能性がある
- 監視プログラムは特定の生徒グループに対して差別的である可能性がある
- 生徒の状態を観察することで、テクノロジーにはない方法で問題を抱えた生徒を特定することができる
- 監視やモニタリングは、生徒の安全を保護するためのソリューションの一部として慎重に実施される必要がある
- 生徒の個人情報を保護するために、教育機関は強力なセキュリティポリシーを策定する必要がある

教育機関のテクノロジー、セキュリティ、そしてコンテンツフィルタリングのソリューションをお探しの方は、ぜひ当社のウェブサイトをご覧ください。

詳細はこちらから