DATASHEET

KELA

サイバー犯罪の脅威から教育機関を保護する

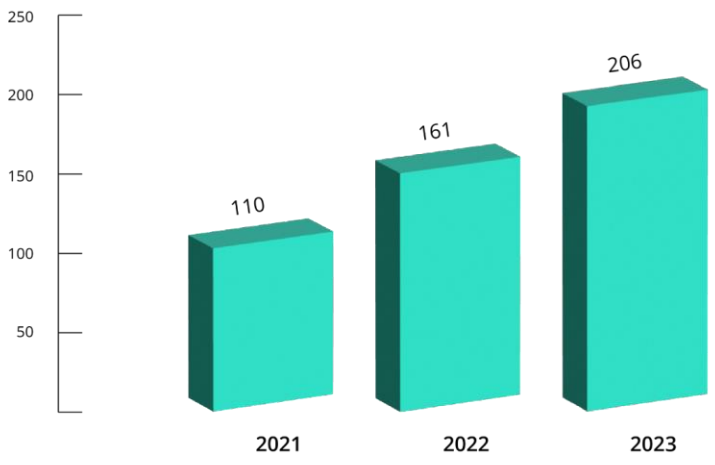
知の番人

2023年においても、教育業界はサイバー犯罪者が特に狙う業界の1つとなりました。新型コロナウィルスがもたらしたパンデミックが目前の懸念事項ではなくなり、学校が対面授業に回帰しつつある現在も、サイバー犯罪者にとって教育機関は攻撃しやすい標的となっています。そののような状況を背景に、2023年8月にはバイデン政権がK-12（幼稚園から高校までの教育機関を擁する学区）のサイバーセキュリティを強化する新たな取り組みを立ち上げました。新たな学年度が始まるにあたり、本データシートでは、KELAが教育業界を標的とした持続型脅威（ランサムウェア攻撃やネットワークアクセスの販売、ハクティビストグループによる攻撃、データ侵害など）について調査した結果を詳述します。

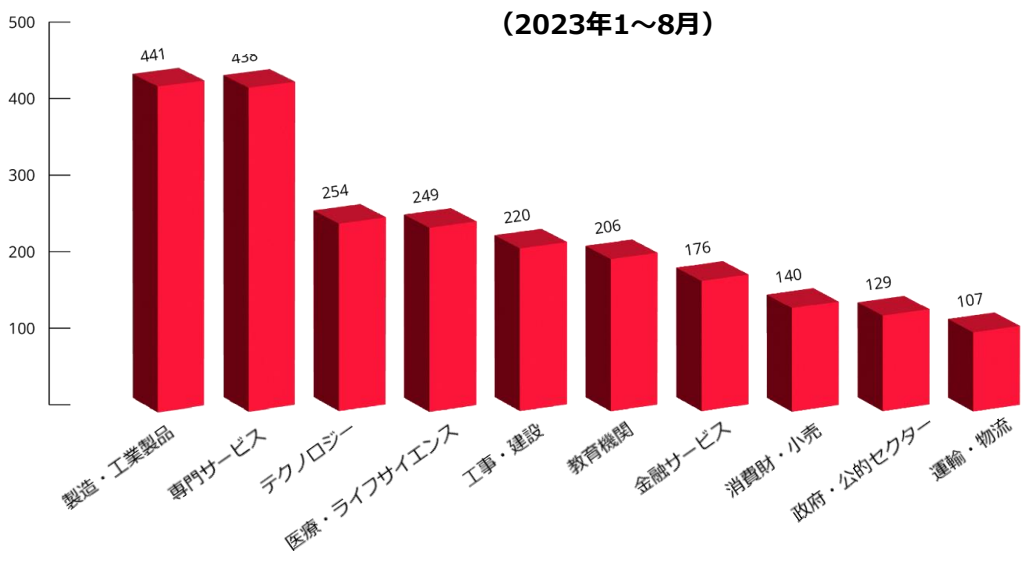
ランサムウェア攻撃

KELAがランサムウェア攻撃やデータリーク攻撃の活動状況と被害組織を分析した結果、ランサムウェア攻撃やデータリーク攻撃を実行するアクターは引き続き持続的な脅威となって教育業界を脅かしており、同業界における2021年以降の被害組織数は**470を超える**ことが判明しました。また2023年、教育業界は現時点までに200件以上の攻撃を受けており、「標的にされた業界」の6位にランクインしています。同業界の被害組織を国別にみると、**「標的にされた国」の1位は米国**であり、過去3年間に発生した攻撃は310件に上りました。この件数は、教育業界で発生したランサムウェア攻撃の約60%を占めています。米国に続き「標的にされた国」は、**2位が英国、3位がカナダ、4位がオーストラリア、5位がスペイン**となっています。

教育業界を標的としたランサムウェア攻撃の件数
（2023年1～8月）



2023年にランサムウェア攻撃を受けた業界
（2023年1～8月）

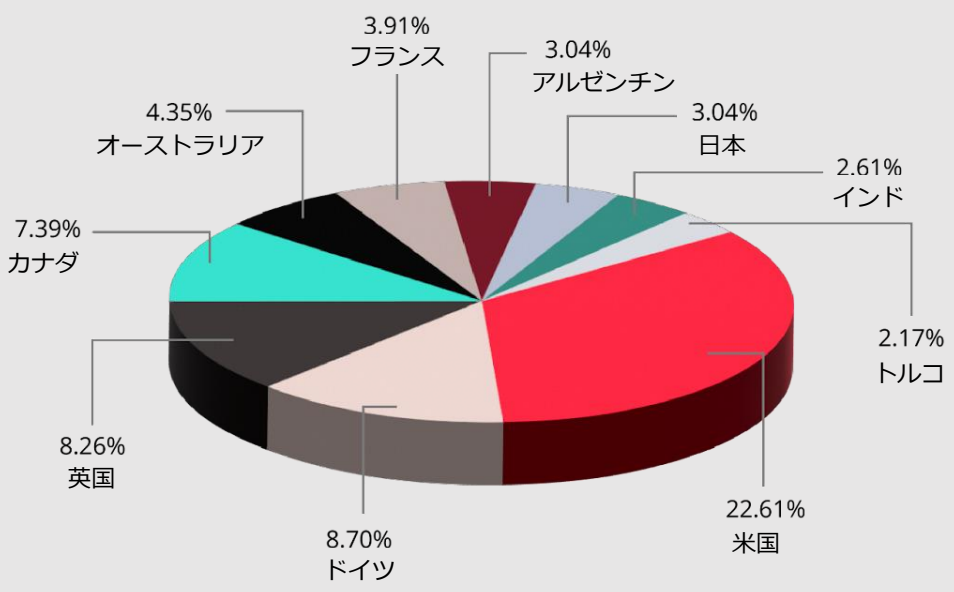


教育業界を標的にしたランサムウェア攻撃を犯行グループ別に分類すると、1位は「**LockBit**」、**2位は「Vice Society」、3位は「Clop」**となりました。過去3年間に発生したランサムウェア攻撃の約30%はこの3グループによって行われています。また2位のVice Societyは、特にK-12や高等教育を狙う悪名高いランサムウェアグループとして知られています。

ネットワークアクセスの販売

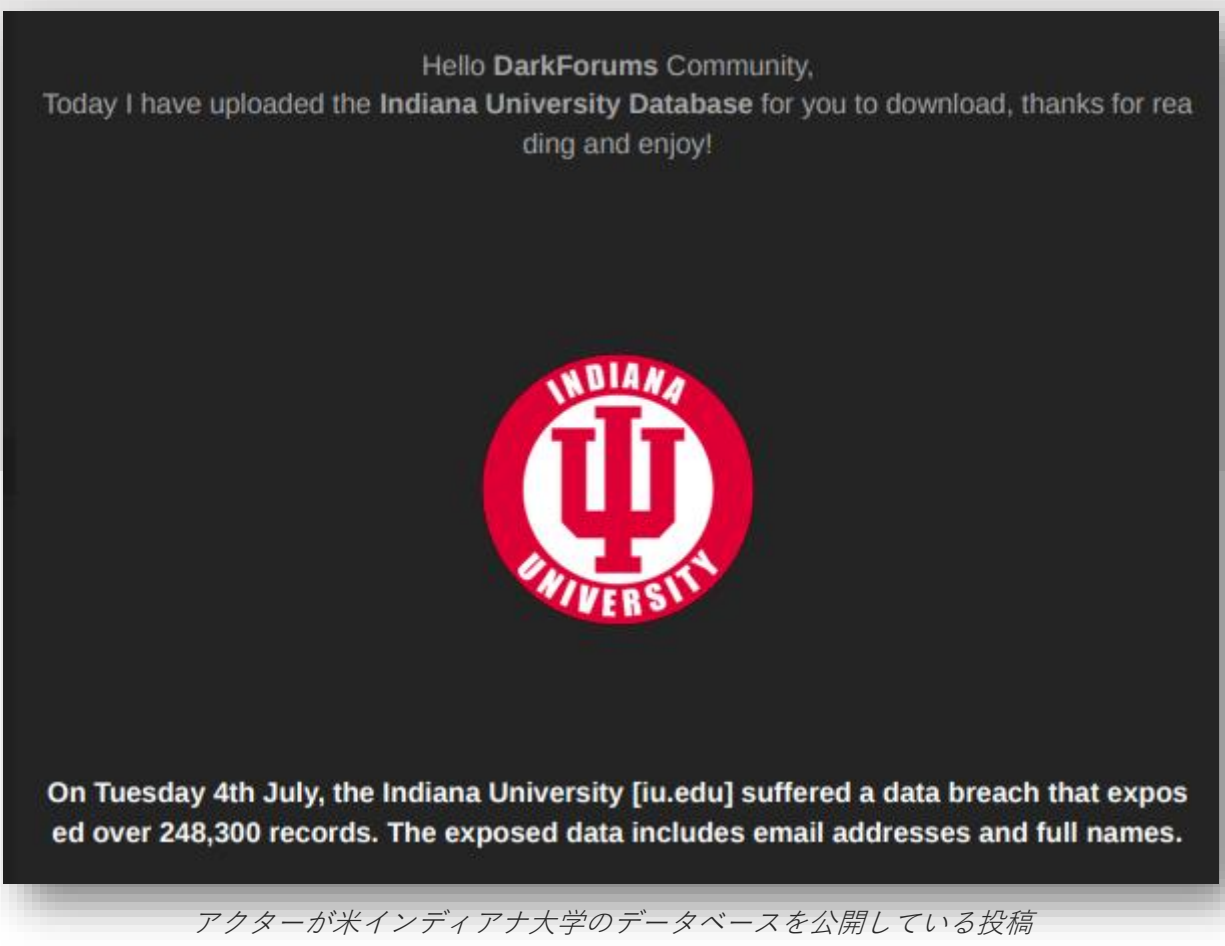
初期アクセスブローカーは、ランサムウェアグループが侵害するネットワークのアクセスを提供し、ランサムウェア・アズ・ア・サービス（RaaS）のサプライチェーンにおいて重要な役割を果たしています。教育機関では、生徒や職員をはじめ多数のユーザーが自宅や学校外部からネットワークにアクセスしているため、ランサムウェア攻撃に対して非常に脆弱な環境となっています。KELAが調査したところ、2021～2023年にかけて売り出された教育業界組織（学校や企業を含む）のネットワークアクセスは約230件に上りました。またそれらを国別に分類した結果、**初期アクセスブローカーが標的にした国の1位は米国**（全アクセスの22%）、**2位はドイツ、3位は英国、4位はカナダ、5位はオーストラリア**となりました。

ランサムウェア攻撃を受けた教育機関（企業や組織含む）の国別データ
（2023年1～8月）



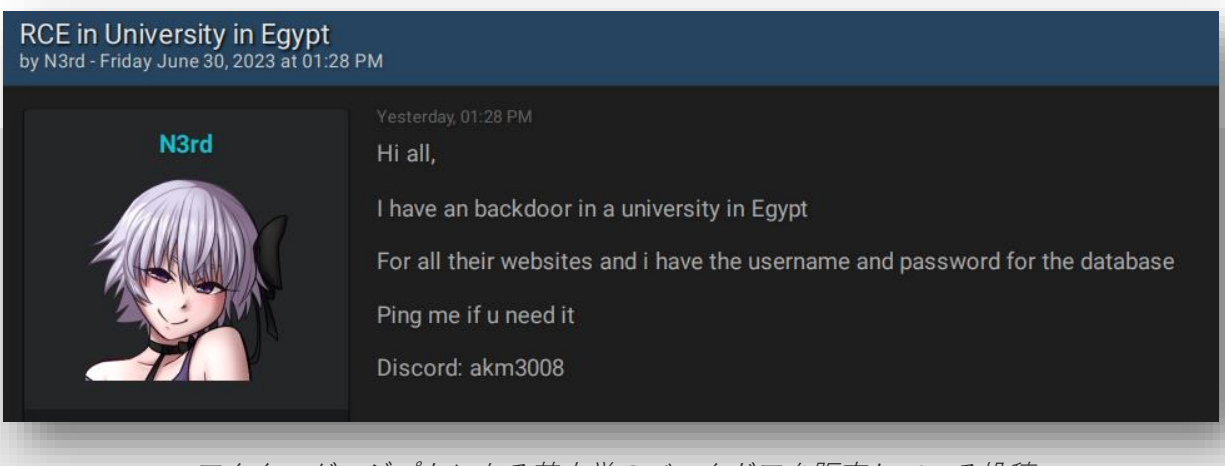
データベースのダンプ

教育機関が保有している機密情報も、サイバー犯罪者を惹き付ける要因となっています。KELAは、生徒の氏名や電子メールアドレス、住所、電話番号をはじめ、教育機関が保持している個人識別情報（PII）のリークおよび販売状況について調査しました。そしてその結果、米インディアナ大学のデータベースがアンダーグラウンドのコミュニティで公開されていたことが判明しました。また公開したアクターによると、このデータベースには24万8,300レコード（電子メールアドレスや氏名、その他）が含まれているということでした。



アクターが米インディアナ大学のデータベースを公開している投稿

教育機関のネットワークに存在する脆弱性の中には、機密情報を保存したデータベースへの不正アクセスに悪用できるものもあります。脅威アクターはそういった脆弱性のエクスプロイトも公開しており、サイバー犯罪者の集う「BreachForums」では、アクターがエジプトにある某大学のデータベースへの不正アクセスに悪用可能なバックドアを公開していたことが確認されています。



アクターがエジプトにある某大学のバックドアを販売している投稿

アクターがドイツにある某大学のネットワーク内を水平移動する方法について相談している投稿

情報窃取マルウェアに不正アクセスされたアカウント情報

教育機関が保有する機密情報のアクセスを入手する方法は他にもあります。例としては「Russian Market」や「Genesis」、「TwoEasy」などのボットネットマーケットで欲しいボット（マルウェアに感染した端末）を選んで購入したり、Telegramチャンネルで提供されている「ログのクラウド」でログを購入し、そこに含まれている情報を悪用する方法が挙げられます。脅威アクターはボットやログを利用してログイン資格情報を入手し、フィッシング攻撃やランサムウェア攻撃をはじめ、様々なキャンペーンに悪用しています。今回KELAは、攻撃者が情報窃取マルウェアを使って窃取し、Russian Marketで売り出した教育機関のアカウント情報を調査しました。その結果、それらアカウント情報に含まれていた上位15サービスの約70%は米国に拠点を置く大学のものであること、さらにその中には米国トップクラスの大学も含まれていることが判明しました。

推奨される対策

•セキュリティ研修：職員や生徒、保護者を対象に、サイバーセキュリティの基本（フィッシングメールの見分け方や安全性の高いパスワードの作成・管理方法、オンラインで機器や情報を安全に使用する方法など）について学ぶ研修を実施します。

•定期的なバックアップ：重要なデータやシステムのバックアップを定期的に取り、オフライン環境で適切に保存して、ランサムウェア攻撃がもたらす影響を緩和します。

•多要素認証（MFA）：追加のセキュリティ対策として、機密性の高いデータやシステムへのアクセスに多要素認証を実装します。これにより、脅威アクターが不正入手した資格情報を悪用することが困難になります。

サイバー犯罪ソースの監視：サイバー犯罪ソースを監視し、データベースのダンプやアカウント情報、ランサムウェア攻撃に関する投稿およびサイバー犯罪の傾向を示唆する情報を入手します。ぜひKELAの無料トライアルに登録し、サイバー犯罪ソースの監視機能をお試しください！