KELA

サクセス・ストーリー

導入事例

SUCCESS STO

大阪経済大学

大阪経済大学が「全学情報システム運用会議」を立ち上げ、サイバーセキュリティ対策強化の切り札として、KELAのサイバー犯罪インテリジェンステクノロジーを導入するにいたるまで

学校法人 大阪経済大学

大阪市東淀川区にある学校法人・大阪経済大学では、6800人以上の学生が学んでいる。学内には1600台以上の教育用コンピューターが使われており、また多くの学生が個人コンピューターを所有していることもあり、学外からも教育目的で学校のネットワークにアクセスできる環境を構築している。

問題

新型コロナウィルスの流行によって、あらゆる大学がリモート授業への対応を迫られた結果、ICTシステムがサイバー攻撃に対してこれまで以上に脆弱化

×

文部科学省は全国の私立大学に対し、サイバーセキュリティ対策を強化するよう通達

×

現状では、あらゆる組織が脅威を緩和してサイバー犯罪リスクを軽減できるソリューションを模索中

ソリューション

攻撃者の視点で大学のアタックサーフェスを特定

↗

大学に関連する脅威情報を監視し、脅威の把握につながるインテリジェンスを配信

↗

継続的に脅威を監視して、大学が重要な資産を確実に保護できるよう支援

成果

漏えいした資格情報や脆弱性に関する情報をリアルタイムに検知

✓

組織のネットワークに調査ツールをインストールすることなく、インターネットの奥深いエリアで取引されている脅威情報を検知

✓

サイバー攻撃を防ぎ、攻撃者に対して先手を打つための対策を提供

→ 課題

近年、日本の教育機関に対する攻撃が顕著になっている。2022年4月には、東京都内にある日本の国立大学で学生や職員が使っていたコンピューターが、認証情報などを盗むマルウエア（ウィルスなど不正なプログラム）に感染している。

教育機関を狙った同様の被害は世界でも急増しており、例えば2021年、日本を含む世界中で、教育・研究機関へのサイバー攻撃件数が前年比で75%も増加。さらにアメリカでは、ランサムウエア（身代金要求型ウィルス）による多大なる損害で閉校を余儀なくされたケースも報じられている。

大阪経済大学のデジタルインフラは8割がクラウド上にあり、2割をオンプレミスで運用している。また、学術情報ネットワークSINETに接続しているため、以前からサイバーセキュリティ対策は行なってきた。財務部長の横山穣氏は、「これまでは幸い、新聞を賑わすような大きなサイバー攻撃を受けたことはなかったのですが、2019年にハッキング行為でルーターの情報を書き換えられるという事案がありました」と語る。

教育機関では、数多くの学生や教職員の個人情報を扱っている。さらに大学によっては、高度な研究成果や研修技術といった知的財産も抱えており、情報漏えいが大学のレピュテーションを左右し、さらには国益を損なうことにもなりかねない。

文部科学省は2019年5月、「大学等におけるサイバーセキュリティ対策等の強化について」と題する通知を全国の私立大学に行なっている。

CHALLENGES

↘ KELAのソリューションを活用したリスクの低減

大阪経済大学は、この通知をきっかけに学内の規程を整備。最高セキュリティ責任者を置くとともに、情報セキュリティに関する重要事項を審議する「全学情報システム運用会議」を立ち上げ、2022年からはサイバーセキュリティ対策強化の切り札として、KELAのINTELACTを導入した。

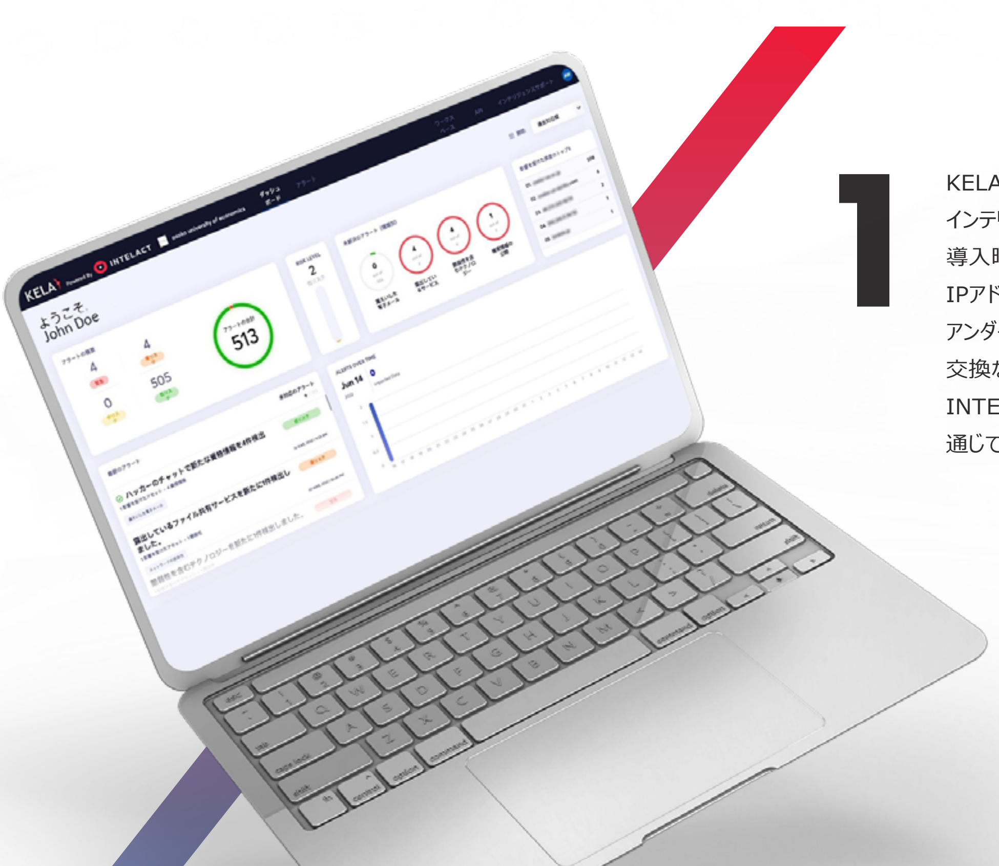
> KELAの製品を知ったのは、KELAが監視するアンダーグラウンドのサイバー犯罪社会で起きている出来事や、それに対する洞察の一部を見ることができる無償サービス『Lumint』に登録したのがきっかけでした。登録後、KELAの営業担当者から連絡をもらい、サイバー犯罪者の視点から見た組織のアタックサーフェスを可視化する製品である『RADARK』の説明を受け、これは使えると思いました。またINTELACTの紹介もあり、そちらについても実際のデモを見た結果、われわれの条件に最も合うということでINTELACTを導入する決定に至りました。
>
> 財務部 情報システム課長 菊川和義氏

CASE STUDY • SUCCESS STORY •

KELA'S INTELACT

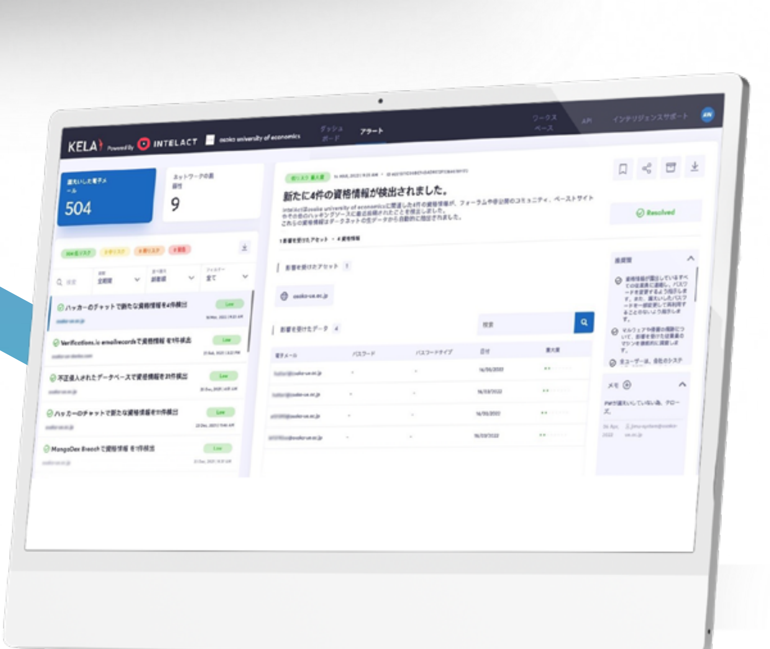
KELAのシステムはサイバー犯罪調査に特化しており、アナリストによる24時間365日の技術サポートを提供している。政府関係機関や大手通信会社などでの実績はあるものの、日本の中堅企業や大学をはじめとする教育機関については、KELAのテクノロジーの導入実績はまだこれからというところだ。

大阪経済大学におけるサイバー犯罪防止の取り組み



1

KELAのINTELACTはサイバー犯罪調査インテリジェンスのプラットフォームだ。導入時に、監視対象とするドメインやIPアドレス、キーワードなどを登録すると、アンダーグラウンドのフォーラムでの情報交換など、監視対象とする情報の動きをINTELACTが検知し、ダッシュボードを通じて管理者に通知する。

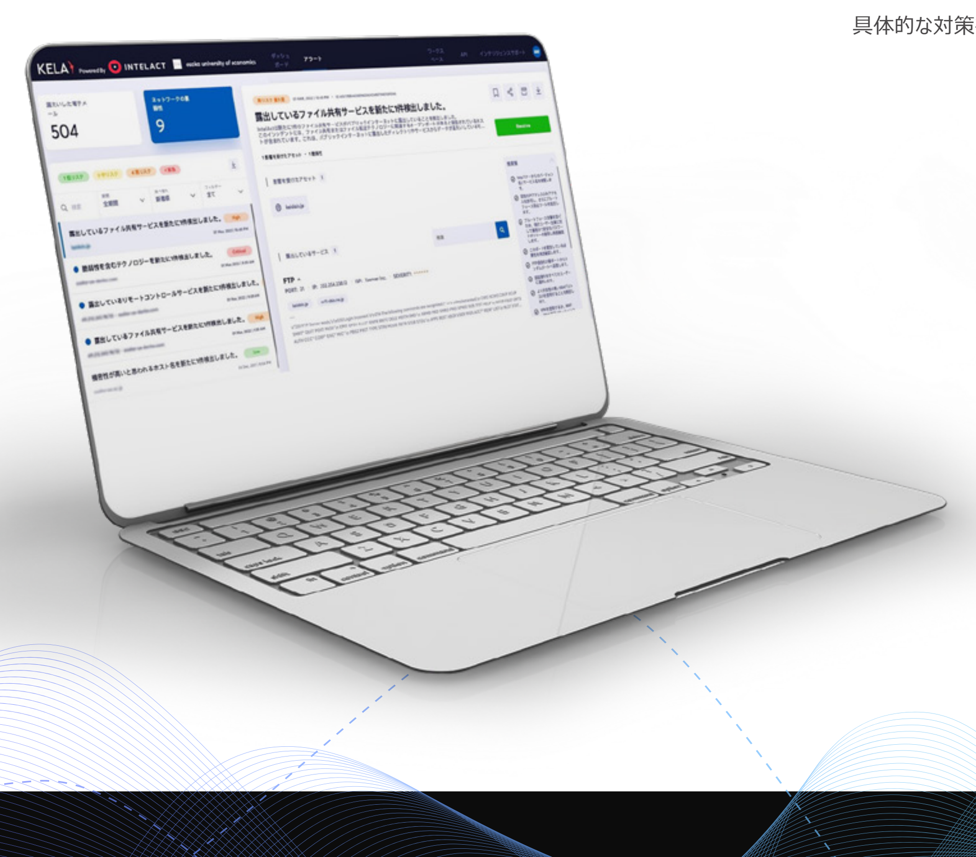


2

ダッシュボードにはアラートの合計数に加え、個々のアラートが重要度に基づいたランキング形式で表示される。
この画面では
「緊急（クリティカル）」アラート4件、重要度が比較的高い「高リスク」アラート4件「中リスク」アラート0件、「低リスク」アラート505件が表示されている。この4件の緊急アラートでは、ハッカーからの会話の中で認証情報が新たにやり取りされていたことが判明した。また4件の高リスクなアラートでは、新たに1件のファイルがアンダーグラウンドのサイバー犯罪社会にあるファイル共有サービスでシェアされていることも判明した。

3

またINTELACTでは、ネットワーク上の脆弱性に関する情報も監視することができる。例えば、FTPサイトが第三者からアクセスできることが判明した場合には、当該FTPサイトの利用状況をもとに、サービスの変更や停止など具体的な対策を取ることができる。



> それまでもインターネット上に流出したメールアドレスや認証情報を知らせてくれるサービスは利用していましたが、それでは検知できなかった流出情報や、本校のシステムに絡むさまざまな脆弱性についての情報をINTELACTが発見したことは衝撃的でした。
>
> 財務部 情報システム課長 菊川和義氏

写真右：横山 穣氏（理事 財務部長）
中央：菊川 和義氏（財務部 情報システム課長）
左奥：外村 翼氏（財務部 情報システム課）

同情報システム課の外村翼氏は、「INTELACTは、『調査ツール』を本学のネットワークに導入して情報収集するというものではありません。インターネットの奥深くで取引きされている情報や、本学の脆弱性に関わる重大な情報を監視し検知してくれるシステムです。実は導入前に、本学の情報社会学部で教鞭をとり、ICT化推進担当理事である教員にINTELACTで提供されたデータを見せ意見を求めたところ、『すぐに導入すべきだ』という判断がなされました」と語る。

↗ 導入後

導入後は、INTELACTが拾い上げた高リスクの脆弱性などを、外部委託している常駐の運用管理担当者と一緒に一つ一つ解決していき、問題を消していくような作業を実施。

「INTELACTは、教育機関の運営に甚大なダメージを与えかねない潜在的なリスク、つまり今後発生する可能性がある脅威に加え、推奨する対応策も知らせてくれます。導入以前よりも、本校のサイバーセキュリティ対策に自信を持てるようになっています」（外村氏）

「現在、リスクはほぼ解決済みになっており、新たな脅威は発生していない状況です。それでも油断しないようINTELACTによる監視を続けています。INTELACTのトップ画面がダッシュボード形式で、一目で直感的にわかりやすいのも助かっています」（菊川氏）

「INTELACTのプラットフォームは低価格のプログラムで提供していることもあり、大阪経済大学様の大学関係施設に展開していただくことができました。今後は、大学をはじめとする教育機関や、病院などの医療機関にもプログラムを提供していく予定です」（KELA担当者）

またINTELACTでは、ネットワーク上の脆弱性に関する情報も監視することができる。今回の事例では、例えばFTPサイトが第三者からアクセスできることが判明した場合には、当該FTPサイトの利用状況をもとに、サービスの変更や停止など具体的な対策を取ることができる。

KELAのサイバー犯罪インテリジェンスプラットフォームを、組織の防御に是非ご活用ください。

今すぐ申し込む

KELA www.kelacyber.com / marketing@ke-la.com / 03-6634-7836

- Copyright© 2022 KELA -