2020 年 1 月 31 日

報道資料

株式会社 FRONTEO

FRONTEO、サイバー攻撃による情報漏洩の調査と事後対応支援に向け株式会社スプラウトと協力

サイバーセキュリティ専門企業との協業により、調査対象範囲・影響範囲の短時間での特定と、広範囲にわたる解析、事後対応に関するサービス提供が可能に

株式会社FRONTEO（本社：東京都港区、代表取締役社長：守本正宏、以下 FRONTEO）、サイバーセキュリティの専門企業 株式会社スプラウト（本社：東京都中央区、代表取締役社長：高野聖玄、以下 スプラウト） は、FRONTEOのAIを用いたテキスト解析技術を含むデジタルフォレンジック技術と、スプラウトが提供するファストフォレンジック・ソリューション「CyCraft AIR」（開発元は台湾のCyCraft社）を連携し、サイバー攻撃による情報漏洩の調査と事後対応に向けたサービス提供について、協力体制を構築したことを発表します。

背景

近年のサイバー攻撃は日々進化を続け、その手口は巧妙化・複雑化の一途をたどっています。警察庁が2019年9月に発表した「令和元年上半期におけるサイバー空間をめぐる脅威の情勢等について」でも、ばらまき型以外の標的型メール攻撃（事業者の非公開メールアドレスに対して送信するなど）の割合が増加していることが指摘されているほか、IoTの普及による接続機器の脆弱性を狙った不正アクセスの増加も指摘されています。このような攻撃にさらされた場合、侵入経路を早急に特定し、影響を受ける範囲を割り出す必要があります。

両社の強み

- スプラウト

セキュリティ診断（脆弱性診断）、ペネトレーションテスト、脅威リサーチ（ダークウェブ調査）、デジタルフォレンジックなどのサービスを提供するサイバーセキュリティ専門企業。多数のエンドポイントを短時間で解析できる「CyCraft AIR」（CyCraft社）を使って、サイバー攻撃成功の原因を迅速に、かつ網羅的に究明します。サイバー攻撃を受けた場合、盗み出された機密情報や個人情報などは「ダークウェブ」と呼ばれるインターネット空間に存在するサイバー闇市場などで売買され、より深刻な二次被害をもたらすケースがあります。スプラウトでは、サイバー攻撃に関連した機密情報や個人情報が漏洩していないかをダークウェブも含め調査し、重要な情報が発見された場合は、その対応策についてもサポートします。

- FRONTEO

FRONTEOは、独自開発したAIエンジン「KIBIT®」による大規模テキストデータの解析技術と、16年にわたって蓄積してきたデジタルフォレンジック技術を用いて、スプラウトが特定した調査範囲内で、攻撃を通じて、どのようなコミュニケーションやふるまいが発生しているのかを洗い出します。例えば、メールの場合、AI「KIBIT®」で記載内容からあやしい行動を見つけ出すだけでなく、外部との通信ログの分析により、コミュニケーションの経由地の特定や侵入を受けたサーバからどのようなデータが抜き取られた可能性があるかを調査します。

協業内容

この度のスプラウトとFRONTEOの協業により、セキュリティ攻撃による影響範囲や情報流出経路、流出したデータを短時間で特定し、解析することが可能となります。また、セキュリティ攻撃のような「有事」への対応に留まらず、ダークウェブの調査による「二次被害の防止」、FRONTEOのメール監査ソリューション（注1）による新たな問題の予兆検知など、「平時」からの企業の健全性診断も支援できるようになります。

株式会社スプラウト 代表取締役 高野 聖玄のコメント

「サイバー攻撃を受けた際、その影響範囲を把握することは非常に重要です。影響範囲が不明瞭だと、実は攻撃者が自社ネットワーク内に潜んだままであることに気付かず、さらなる被害を招いてしまう危険性もあります。この度の株式会社 FRONTEO との協業により、サイバー攻撃に対する迅速で網羅的な調査と、事後対応に向けたサービスを包括的に提供できるようになりました。」

株式会社FRONTEO 代表取締役 守本 正宏のコメント

「この度、株式会社スプラウトと協業することにより、これまでクライアントからのヒアリングを元に行っていたフォレンジック調査対象の特定が、ログの収集や分析内容を元に、短時間で幅広く行えるようになりました。その結果、速やかにフォレンジック調査に取り掛かることが可能となり、短期間で調査、報告書作成まで終えられるようになりました。また、有事の対応にとどまらず、スプラウトの脅威リサーチとFRONTEOのメール監査ソリューションを組み合わせ、日常の業務の中で起こりうる様々なサイバー攻撃から企業を守る平時ソリューションを提供できることを嬉しく思います。今回の協業を皮切りに、今後様々なソリューションとKIBIT®の連携を通じて、より広く、深いデジタルフォレンジックを実現し、企業の安全に寄与していきたいと考えています。」

（注 1）FRONTEO のメール監査ソリューション

【クラウド／オンプレミス環境対応】

Email Auditor® URL: http://www.kibit-platform.com/products/email-auditor/

監査官の調査観点を学習した人工知能が、大量の電子メールを解析し、要監査メールを抽出。監査業務の工数を大幅に削減するとともに、内在するリスクを可視化することで経営危機から企業を守ります。

【クラウド環境対応】

KIBIT Automator™ URL: https://legal.fronteo.com/products/kibit-automator/

米国民事訴訟の公判手続きで必要となる証拠開示（ディスカバリ）の中でも特に、電子証拠開示（e ディスカバリ）における文書レビュー作業の効率向上、作業担当者の負荷軽減、費用削減を目的として開発された AI ツールで、2019 年 3 月にリリースされました。ディスカバリで使われる調査手法を応用し、AI を活用して証拠資料である大容量の電子メールや電子ファイルの審査・分析を行います。近年、企業に求められている、短期での情報開示への対応も期待されます。

■ 株式会社スプラウトについて URL: https://sproutgroup.co.jp

サイバーセキュリティ分野の研究開発を行うスタートアップ企業として2012年に設立。通称ホワイトハッカーと呼ばれるセキュリティエンジニアを中心に、情報通信分野に精通したコンサルタントやリサーチャーらが集まったサイバーセキュリティの専門企業です。

ゼロデイと呼ばれるシステムに潜む未知の脆弱性、サイバー空間の最新動向、サイバー犯罪の手

口といった多岐にわたる分野について調査・研究を行うと同時に、これらの活動から得られた知見をもとに、企業や官公庁に対してサイバーセキュリティの支援をしています。

また、国内外のホワイトハッカーと企業を結ぶバグ報奨金プログラムのプラットフォーム「BugBounty.jp」なども運営。サイバー闇市場を題材にした『闇ウェブ（ダークウェブ）』（2016年7月発刊／文藝春秋）、ネット空間にはびこるフェイクの実態に迫った『フェイクウェブ』（2019年5月発刊／文藝春秋）をはじめ、メディアや講演等を通じたサイバーセキュリティ情報の発信を積極的に行っています。

■ **FRONTEO について** URL: https://www.fronteo.com/

株式会社FRONTEOは、独自開発の人工知能エンジン「KIBIT®（キビット）」や「concept Encoder（コンセプト・エンコーダー、登録商標は conceptencoder®）」により、ビッグデータなどの情報解析を支援するデータ解析企業です。国際訴訟などに必要な電子データの証拠保全と調査・分析を行うeディスカバリ（電子証拠開示）や、デジタルフォレンジック調査を支援する企業として2003年8月に設立。自社開発のデータ解析プラットフォーム「Lit i View®（リット・アイ・ビュー）」、日・中・韓・英の複数言語に対応した「Predictive Coding®（プレディクティブ・コーディング）」技術などを駆使し、企業に訴訟対策支援を提供しています。このリーガル事業で培われ、発展した独自の人工知能関連技術は、専門家の経験や勘などの「暗黙知」を学び、人の思考の解析から、未来の行動の予測を実現します。ライフサイエンスやビジネスインテリジェンスなどの領域に展開し、FinTechやRegTechに加え、「働き方改革」でも実績をあげています。2007年6月26日東証マザーズ、2013年5月16日NASDAQ上場。資本金2,559,206千円（2019年3月31日現在）。2016年7月1日付けで株式会社UBICより現在の社名に変更しております。

〈本件に関するお問い合わせ先〉
株式会社 FRONTEO　広報担当　瀧川
TEL：03-5463-6380　FAX：03-5463-6345　Email：pr_contact@fronteo.com