辻伸弘氏が解説するランサム攻撃動向、「侵入されても発症させない」対策のキモとは

標的型攻撃やランサム攻撃など、企業を標的にしたサイバー攻撃は依然として大きな脅威となっている。さらに、取引関係にあるサプライチェーンや顧客にも攻撃対象は拡大しており、企業はこれらの脅威に対応していかなければならない。そこで、ランサム攻撃をはじめ幅広くサイバー空間の脅威の観測、情報発信を行うSBテクノロジーの辻 伸弘氏と、大興電子通信 セキュリティアドバイザーの中須寛人氏、富士通の斎藤 建氏、丸子正道氏が最新のマルウェア攻撃に対抗するためのポイントを紹介した。

どの業種が感染してもおかしくない

ランサム攻撃は依然として猛威をふるい、ここ数年、ファイルの暗号化に加えて、情報を窃取し公開をちらつかせることで金銭を要求する「二重脅迫型」などの脅威も顕在化している。

辻氏は、最近のランサム攻撃の動向として、身代金要求手口の3つのパターンを示した。1つ目が、「ファイルやシステムの暗号化」だ。ファイルが開けなくなるだけでなく、Windowsが起動しないケースもある。

2つ目が「二重脅迫」だ。2019年ごろから見られる手口で、機密情報を盗んで暴露サイトで公開すると脅す手口で、3つ目が「DDoS攻撃」などの前の二重に加えて身代金を支払うように仕向ける手口だ。辻氏によると「被害者や被害企業の利害関係者に連絡してくるケースもある」という。学校であれば生徒の親に連絡し「子どもの情報が暴露されたくなければ金を払うよう学校に求めるよう」脅迫してくるのだ。

また、ランサム攻撃は分業・専業化が進んでいる。辻氏によると、その役割は大きく「RaaS（Ransomware as a Service）」と「Affiliate（実行犯）」に分かれる。前者はランサム攻撃を開発して、脅迫するプラットフォームを提供する者、後者は実行犯だ。

そしてRaaSとAffiliateで収益を分配する仕組みができており、「たとえRaaSが逮捕されたり、サーバがテイクダウン（閉鎖）されたりしたとしても、これは単に胴元が潰れただけで、実行犯は減らないという難しい現状がある」と辻氏は述べた。

辻氏が観測した範囲では「ランサム攻撃に脅迫されて、応じずに情報を公開された件数」について、2023年は、暴露された総数が2826件、被害国は110カ国に及ぶということだ。そのうち、日本は31件で、全体の13位だった。

「多くの場合は米国やカナダ、ヨーロッパ諸国が上位を占めるというのが、ここ数年の傾向として変わらない」と辻氏は話す。背景には、日本以外の国ではランサム攻撃の身代金を保険金で賄える国が多く、「攻撃者にとって支払いに応じやすい国が上位に並ぶ」傾向がある。また、業種では、2023年の1位は教育だった。辻氏は「2826件に占める割合では7～8％と低く、これは裏を返せばどの業種が被害に遭ってもおかしくないことを示している」と説明した。

ランサム攻撃には新たな「経済圏」が形成されている

ランサム攻撃の感染経路は大きく「メール」「脆弱性と認証」「先行マルウェア」「MSP（Managed Service Provider）とサプライヤー」「内通者」に分けられる。

辻氏は、「脆弱性と認証」について、最近ではVPN機器の脆弱性が狙われるケースや、リモートデスクトップのパスワードが弱いといったケースがあると説明した。また「先行マルウェア」については、別のマルウェアに感染して、それがバックドア（裏口）となり、さらなるランサム攻撃を呼び込む挙動をするケースだ。

そして、「MSPとサプライヤー」というのは、自社と関係のある取引先が被害を受けて、自社に攻撃が及ぶ、いわゆるサプライチェーン攻撃のことだ。

辻氏は、ランサム攻撃には新たな経済圏（エコシステム）が確立されていると話す。上述したRaaSとAffiliateの関係に加え、攻撃側の分業化・専業化はさらに進んでいる。中でも辻氏が警鐘を鳴らすのが「IAB（Initial Access Broker）」と呼ばれる、侵入経路を見つけ、それを実行犯に売る役割の存在だ。

「脆弱性のあるサーバを探し、侵入して

SB テクノロジー
辻 伸弘氏

辻伸弘氏が解説するランサム攻撃動向、

「侵入されても発症させない」対策のキモとは

バックドアを仕掛けておきます。IABは基本的に情報の窃取やランサム攻撃の展開といったような組織にとっての実被害は与えません。彼らは侵入先のリストを作り、その経路を売るのです」（辻氏）

アンダーグラウンドでは、リスト化されたアクセス先が「3000ドルから500ドル刻みでオークションにかけられるなどして売買されている」ということだ。辻氏は「組織にとって実被害を与えないIABは、それほど高い能力を要せずに、犯罪エコシステムに参加できる」点から、犯罪組織の裾野が広がっていることに警鐘を鳴らした。

その上で、改めてランサム攻撃の被害軽減には「早期発見」カギを握ると辻氏は述べる。「IABは実被害を与えないので、いかに早期の段階で発見できるかが大事だ」ということだ。これは裏を返せば、脆弱性を放置したり、認証情報が甘い状態のままだったりすると、ランサム攻撃に攻撃されるのは必然だということになる。

辻氏は、これからのランサム攻撃の脅威には「無関心でいることはできたとしても、無関係でいることはできない」と呼びかけた。「自社には重要な情報がないから攻撃されることはない」という経営者がいたとしても、「関係あるかないかを決めるのはあくまで攻撃者だ。運が良いとか悪いとかではなく、対策を講じずにいると順番が回ってくるくらいに思ってほしい」と辻氏は述べ、ぜひ後述する対策を進めてもらいたいと締めくくった。

「悪いものを見つける」から「悪いことをさせない」へ

続いて、大興電子通信 ICTソリューション推進部セキュリティビジネス課 セキュリティアドバイザーの中須寛人氏は、「ランサムウェアをはじめ、従来のエンドポイントセキュリティでは防ぎきれない新たな脅威への対策が重要だ」と話した。従来の対策には、特定や防御といった「事前対策」と、検知・対処・回復といった「事後対応」の間にギャップがあると中須氏は指摘する。

中須氏は、「攻撃者はウイルス対策ソフトで検知されることを前提に、特定のマルウェアを3日間しか利用しないとも言われており、実際の攻撃期間とウイルス対策ソフトの定義ファイルで検知可能になる期間にギャップがあることから、従来型のエンドポイント対策では脅威を防ぎきれない」と説明した。

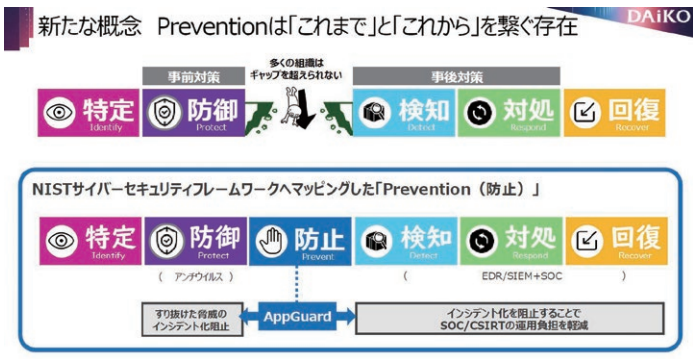
また、最新のランサムウェア（LockBit3.0）では、暗号化のスピードがデータ1GBあたりわずか8秒と高速化しており、検知が間に合わない状況も見られる。さらに、ノーウェアランサムのように暗号化はせずに情報だけを窃取し身代金脅迫を行うことや、窃取した情報を闇サイトで売買するといったケースが存在するため、データをバックアップしていても十分なランサムウェア対策とならない点も大きな脅威だ。

そこで、新たなランサムウェアの考え方が「Prevention（防止）」という概念だ。防御と検知の間に「防止」のプロセスを設け、「事前対策」と「事後対応」をつなぐことで、これを担う対策製品が「AppGuard」だ。中須氏は、「AppGuardは、マルウェアかどうかを判断するのではなく、OSに害のある動きをブロックして無効化することで、侵入されても攻撃を成立させない対策製品だ」と説明した。

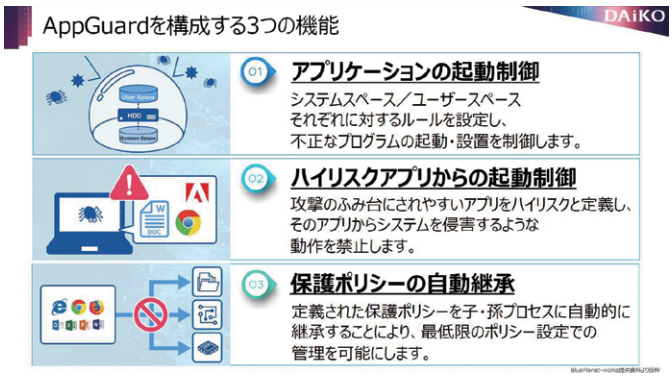
大興電子通信
ICTソリューション推進部
セキュリティビジネス課
セキュリティアドバイザー
中須 寛人氏

AppGuardの機能は大きく「アプリケーションの起動制御」「ハイリスクアプリからの起動制御」「保護ポリシーの自動継承」の3つがあり、製品ラインナップには、エンドポイントセキュリティを担う「クライアント版」と、サーバセキュリティを担う「サーバ版」がある。中須氏はサーバ版の推奨導入先としては、「たとえば、Active Directoryサーバやファイルサーバをランサムウェアの感染から守ることや、サポートが終了したWindows Server OSの延命対策として、Microsoft ESUよりも安くセキュリティ強化が可能だ」と話した。

導入企業数は1万8000社を超え、国内



NISTサイバーセキュリティフレームワーク　1.0におけるAppGuardの位置づけ

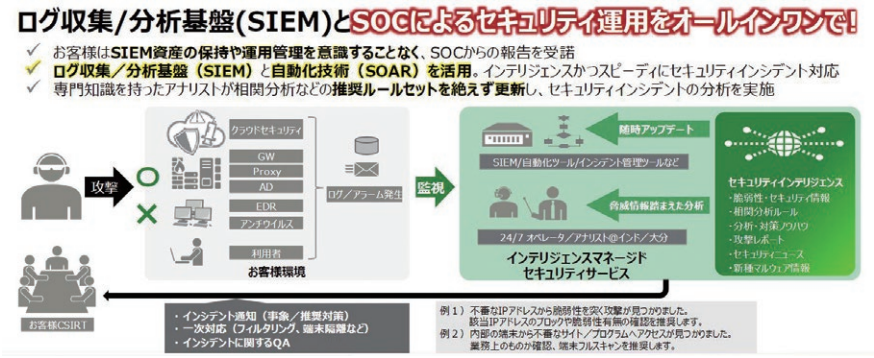


AppGuardの３つの機能

辻伸弘氏が解説するランサム攻撃動向、
「侵入されても発症させない」対策のキモとは

では、エンドポイント対策にEDRを導入していた食品製造業の企業が、追加の対策としてAppGuardを導入し、「検知を回避し潜伏したマルウェアによる、ADサーバへの攻撃を阻止した」事例などがあるということだ。

これら民間企業をはじめ地方公共団体、最近では医療機関での採用も進んでおり、安心して検討できるAppGuardが、「ランサムウェアをはじめ、ランサムウェア被害の起点となる先行マルウェアによる攻撃からエンドポイントを守る対策として、企業のセキュリティ対策強化につながれば」と、中須氏は締めくくった。



富士通の「インテリジェンスマネージドセキュリティサービス」

安心と利便性の両立が エンドポイントセキュリティのカギ

そして、富士通 グローバルマーケティング本部 マネージャーの斎藤 建 氏は、働き方の多様化に伴い、エンドポイントセキュリティは、これまで以上に安全性と利便性の両立が求められているとした。

「テレワークなど働く場所が多様化し、さらなる利便性と安全性を両立するには、プロアクティブな対応と端末を中心としたエンドポイントセキュリティの重要性が拡大している」ということだ。そこで、事前の「リスク分析」と、PCの「エンドポイントセキュリティ強化」の2つが重要なポイントとなるが、富士通では、外部からの脅威のリスクを分析、評価し問題点を可視化する「セキュリティスコアカード」というサービスを提供している。

また、セキュリティ運用を全面的に支える「インテリジェンスマネージドセキュリティサービス」や、運用改善の支援を行う「リテーナ型セキュリティアドバイザリサービス」も提供している。斎藤氏は、アドバイザリサービスでは、富士通のセキュリティ専門家が有事の際の端末の侵害調査なども行う」と話し、セキュリティ対策のサイクル全体を支援可能だと説明した。

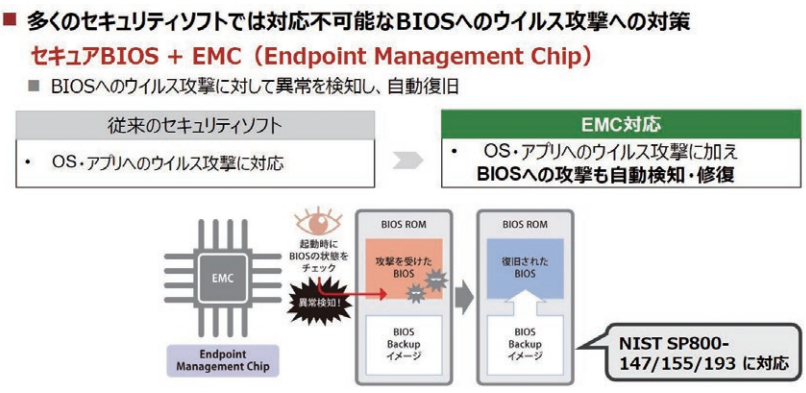
富士通
グローバルマーケティング本部 マネージャー
斎藤 建氏

また、富士通 CCD事業統括部 プロモーション推進部 部長の丸子正道氏は、働く場所が多様化することで、「ウイルスによる攻撃リスク」「人に起因するリスク」が高まっているとする。そこで、「ウイルス対策の強化」「本人認証の強化」「データ保護の強化」の3つのポイントで、エンドポイントセキュリティ対策を進めていくことが重要だ。

富士通はPC本体のエンドポイントセキュリティを強化している。1つ目の「ウイルス対策の強化」では、BIOS（Basic Input Output System：バイオス）と呼ばれるファームウェアの耐タンパ性の強化だ。BIOSはOS起動前に動作し、PC本体のハードウェアの管理と制御を行うため、BIOSにウイルスが感染するとPCが起動しないといったトラブルが発生する。従来のウイルス対策ソフトウェアのカバー範囲はOSよりも上の層のみのため、この部分はPC本体の機能としての対策が必須である。

富士通のPCはセキュアBIOSとEMC（Endpoint Management Chip）を標準搭載。PC起動時にBIOSへの攻撃や異常を検知して、自動的に修復する機能を備えているので、情シスや従業員自身の余計

富士通
CCD事業統括部 プロモーション推進部 部長
丸子 正道氏



「富士通のPCはセキュアBIOSとエンドポイントマネジメントチップを標準搭載」

辻伸弘氏が解説するランサム攻撃動向、
「侵入されても発症させない」対策のキモとは

な手を煩わせることがなく使い続けることができる。

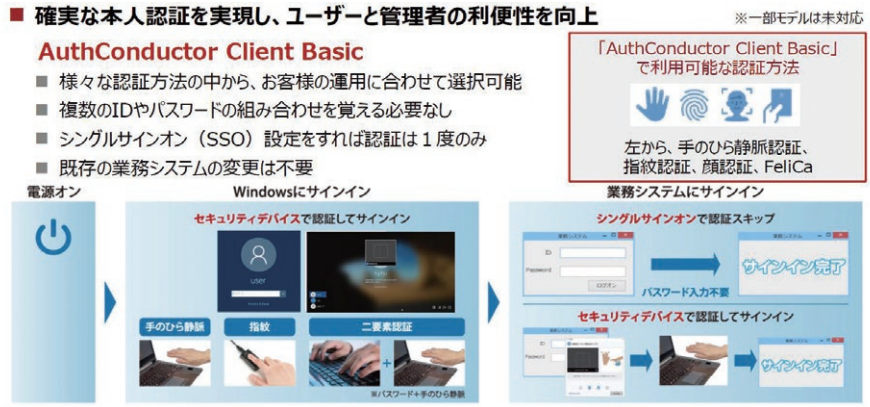
2つ目の「本人認証の強化」については、二要素認証にも対応できる多彩な生体認証が選択可能だ。

指紋や顔認証に加え、認証精度が高い手のひら静脈認証が利用可能であり、業務システムへのサインインも可能なためセキュアかつ利便性にも優れている。

そして、3つ目の「データ保護の強化」については、ローカルデータを安全に持ち運べ、導入から運用まで簡単に使える秘密分散ソリューションを提供している。

丸子氏は、上述した「セキュリティスコアカード」や、エンドポイントセキュリティが強化された富士通のPCにご興味を持たれた方は、ぜひお気軽に大興電子通信に相談してほしいと締めくくった。

非接触で生体認証が可能



確実な本人認証を実現し、ユーザーと管理者の利便性を向上

AppGuard、Fujitsu Smart PC Security に関するお問い合わせ

DAiKO

大興電子通信株式会社
ビジネスクエスト本部
ICTソリューション推進部セキュリティビジネス課
security-biz@daikodenshi.co.jp

※ 本記事は2024年3月22日に掲載されたソフトバンク ビジネス＋ITからの転載です