高度化するランサムウェアの傾向と対策

2024.02.16

於 赤坂インターシティ　コンファレンスルーム401

進化したエンドポイントセキュリティで実現するクライアントPCの安全な未来

主催　富士通株式会社　共催　大興電子通信株式会社

セミナー１　ランサムに至る病　そして2024　SBテクノロジー株式会社　辻 伸弘 氏

【講演内容】

結論から言うと、ランサムの被害を全部防ぐことは無理。どこまでを守るのか、その線を決めるのが大切。

今よりは良いセキュリティをどう実現するか考えることが大切。

【ここで実際にランサムウェア感染のデモ映像を流す。⇒デスクトップのアイコンが☠マークに変わる。】

ランサムウェアはデータを暗号化し、身代金を要求するマルウェア。しかし、最近はデータを窃取し、それを暴露すると脅して、身代金を要求する形態に変わってきた。復旧されると、身代金が取れなくなるので、そのリスクを避けるため。（＝？）しかしこちらの方が技術的な難易度は高い。

また、今ではランサムウェアが組織化され、RaaS（ランサムウェアのプラットフォームを提供するサービス）とアフィリエイト（ランサムを拡散し、実行する犯人）に分かれて実行するなど、分業化されている。

更に、セキュリティの弱いサイト、ないし個人のアドレスをシステム的に収集する組織もある。これがアフィリエイトにそのアドレスを売る。身代金の取り分はアフィリエイトが最も多く、RaaS、アドレス搾取者の順。

2023年の被害集計では2826件。アメリカが半分。日本は31件。ロシア語圏では被害はない。(だからロシアが犯人ということにはならない。ロシア語圏では身代金が成立しない？)

不正アクセスを受けた業界は多い順に　① 教育。② 土木・建築。③ 病院。④ IT業界。

これは侵入のしやすさと身代金の支払いをすぐにする業界らしい。教育業界は子供の情報を暴露されるのを恐れる。

不正アクセスの入り口。① メール。② リモートデスクトップ。③ ばらまき先行マルウェア。

攻撃の手順。例えば、① VPN経由で侵入⇒② Active directry入手⇒③ 端末確認⇒④ 全端末にランサムを撒く。

RaaS経済が成立しており、RaaSオペレータ、Affiliate、IAB（Initial Access Broker）などの役割を担うメンバーが組織としてランサムウェアの犯罪を行う。一番技術力が必要なのはAffiliateでマルウェアを作成する。

IBAは不正アクセスの侵入口を見つける役割で、偽のサイトをランダムに送り付け、不用意にRDTソフトなどをダウンロードしたサイト、個人のPCアドレスなどを裏のネットで売りに出す。

こういう状況なので、完全に防ぐことは難しい。やられるのは必然と考えた方が良い。

あなたが無関心でも無関係ではいられない世の中だ。

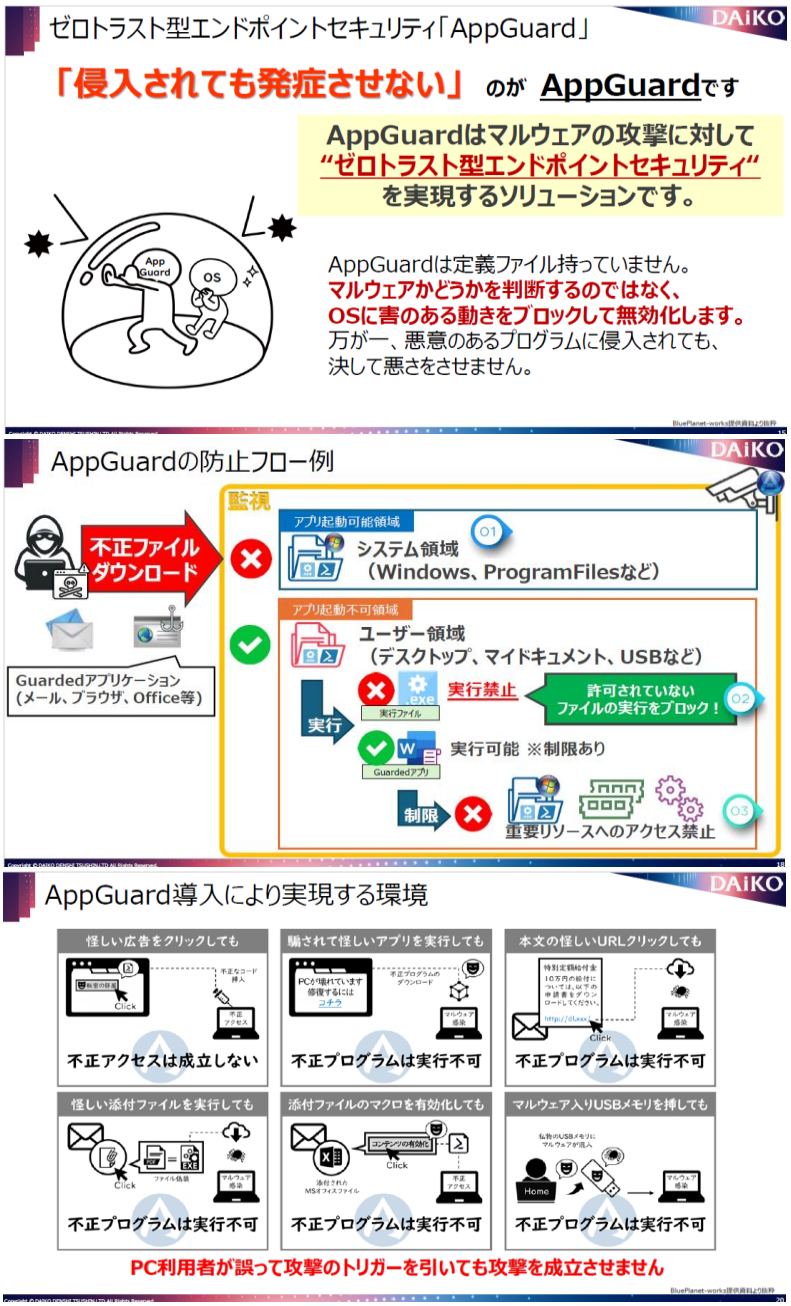
セミナー２　ランサムに対抗する盾（AppGuard）　大興通信 セキュリティアドバイザ 中須 寛人 氏

【講演内容】

マルウェアは進化をしているために、従来のような入り口で侵入を止めるという手法では防ぎきれない。

新たな防御は、侵入をされても動けないようにする（Prevention＝防止）方法だ。AppGuardはウィルスが入り込んでも、許可されていない動作を防止する機能を持っている。

その概念図は次の通り。



［講演資料］「ランサムウェアに対抗する盾、AppGuardのご紹介」より抜粋

【感想】

メーカの説明なのでどこまでの性能が出るのかは不明だが、現下のランサムウェアの状況を見ての対応策なのだろう。

話を聞いていると、マルウェアの侵入を完全に防ぐことは確かに不可能かもしれないと思えてくる。

セミナー3　安心と利便性の両立が今後のカギ　　富士通（株）MNG 斎藤 健 氏　部長 丸子 正道 氏

【講演内容】

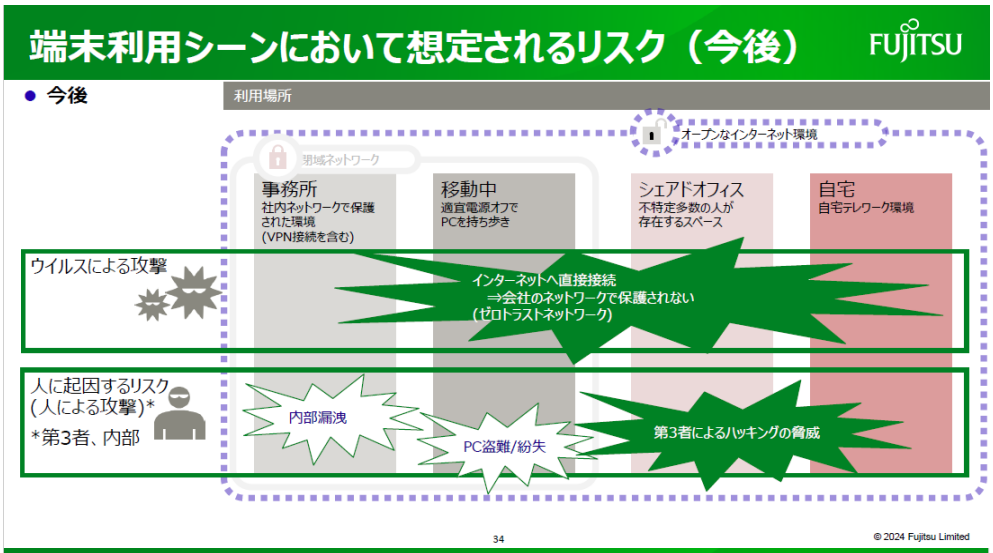
今後、端末の利用は移動中とかシェアオフィスなど、安全なネットワークの外で使われることが多くなる。

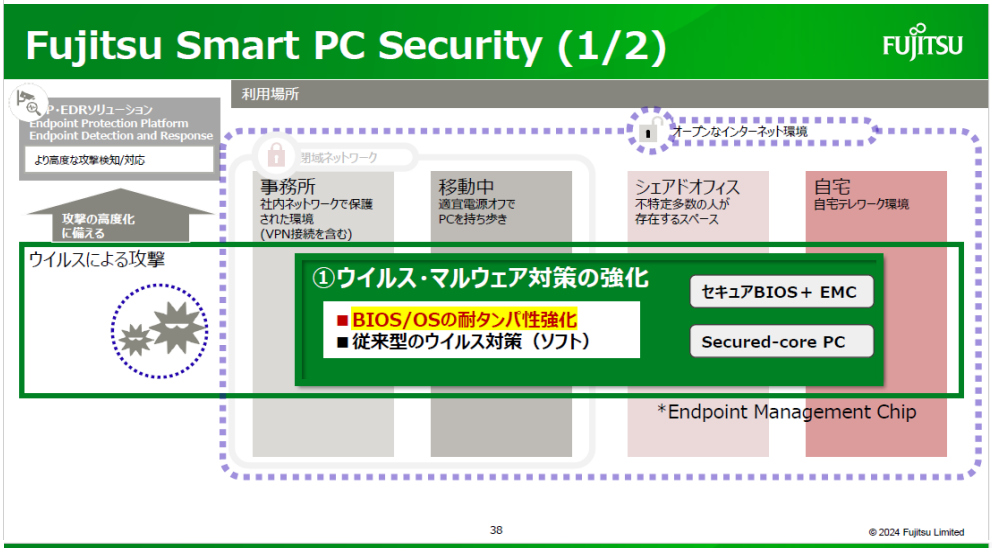
その場合のキーワードはエンドポイントでのセキュリティ確保である。富士通のモバイルPCはそのための機能を備えている。

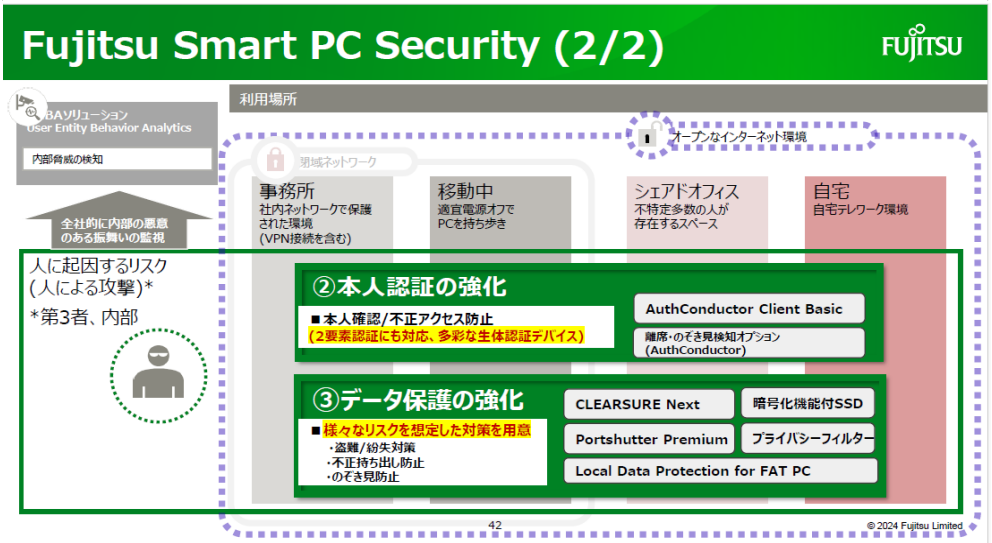
具体的には次図の説明図にあるように

① BIOS/OSの耐タンパ性の強化。② ウィルスソフト。③ 本人認証の強化。④ データ保護の強化である。

特にウィルスソフトでは防げないBIOSレベルの攻撃に対しても検知し、復旧する機能を追加した。







［講演資料］「安心と利便性の両立がエンドポイントセキュリティの鍵に」より抜粋

【感想】

セキュリティを強固にすれば利便性は落ちる、利便性を重視すれば脆弱になるというトレードオフの関係をうまく解決したということの様だ。

最近、PC自体のセキュリティを強固にしたPCの新製品がたくさん出ている。HPもNECも同様の新製品を出しており、業界としてエンドポイントでのセキュリティ確保がトレンドとなっている。ただし、攻撃側も進化するので、完全に防御できるかは疑問だ。しかし、対策をしておけば一番に被害にあうことはない。

質疑応答

・他国の状況は

米国が一番被害が大きい。解決に身代金を払うことが多い。認証とアクセスの管理が重要。つまり基本が大事。

・防御方法は

ゼロトラストは言うほど広まっていない。**バックアップ**を取ってはいるが、復旧方法がキチンと訓練されていない。普段からこの手順を訓練していないと、復旧がうまくいかない。そこで慌てる。

・大事なことは

資産管理。管理されていない端末はないか？調べるべし。アンチウイルス対策はすべての端末にしないと意味がない。アセットマネジメントは基本中の基本だが重要だ。

・最新のツールやウィルスの動向などはどう調べる

CVE Details　Feedly（RSS）　などのサイトでこまめに最新動向を調べる。そうしないと対応が遅れる。

自分のメールアドレスや電話番号が漏洩しているかを調べるには以下のサイトがある。

パスワード漏洩をチェック「Have I Been Pwned?」の使い方｜ウインドミル (wind-mill.co.jp)

まとめ

マルウェアに対する認識は変えないといけない。その象徴が辻氏の言う**【あなたが無関心であっても、無関係ではいられない。】**という言葉である。危険は身近にある。

日常のプライベートなメールの中に　「クレジットカードの使用履歴に不審なものがある」とか「宅急便の届け物がある」というのはないだろうか。何気なくメールの添付URLにアクセスしたことはないだろうか。サイトを見ただけなら問題はないだろうが、ついうっかりページ内のタブをクリックしたり、指示通り操作をした経験があるなら、マルウェアのチェックをした方が良い。あなたのPCには見かけ上の問題が無くてもリモートデスクトップのソフトを仕込まれて、ごっそりメールアドレスを抜き取られているかもしれない。悪意のある犯罪者はそのアドレス帳からめぼしい相手を見つけ、あなたの名前でその方に同じようなメールを出し、感染を拡大させる。しかもあなたのPCは**リモートデスクトップ入りのPCとして登録され、その名簿は売りに出される。**そのような過程を経て、大企業や大病院に本当のランサムウェアを忍び込ませ、まんまと身代金をせしめると言うのが最近の手口である。

こうしたセキュリティ上の脅威から、システムを守るために行うべきことは、基本的なルールをきちんと守ることに尽きる。**いくら強力なマルウェアと言っても、あなたのPCに入れなければ不具合を起こすことはない。**あなたのPCがマルウェアに入られないための原則については基本のルールが繰返し言われている。

【システムにマルウェアを入れないためのルール】

①　すべてのPCにセキュリティソフトを導入する⇒入ってしまったマルウェアを発見し駆除する。
②　OS・ソフトウェアをこまめにアップデートし、つねに最新の状態に保つ⇒ソフトの脆弱性に蓋をする。
③　権限管理を強化する⇒重要なデータにアクセスできるPCを極力限定する。
④　定期的にデータのバックアップを行う⇒万が一の障害に備え復旧の手順を訓練して置く。
⑤　社内で情報セキュリティ研修を実施する⇒不用意な人為的エラーを防ぐ。
⑥　定期的なセキュリティ（脆弱性）診断を受ける⇒最新の対策を知っておく。

少しでも怪しいと思うURLにぶつかったら以下の**Googleのサービス**を使い、**URLを張り付ければ、怪しいサイトかどうか判定してくれる。**

VirusTotal - ホーム

ランサムウェアだけでなく他のマルウェアを蔓延させないためにも、自分のプライベートなPC、スマホにもウィルスチェックなどのセキュリティ対策がされているか確認するべきだ。それと同時に日頃からセキュリティに対する関心を持ち続けたいものである。

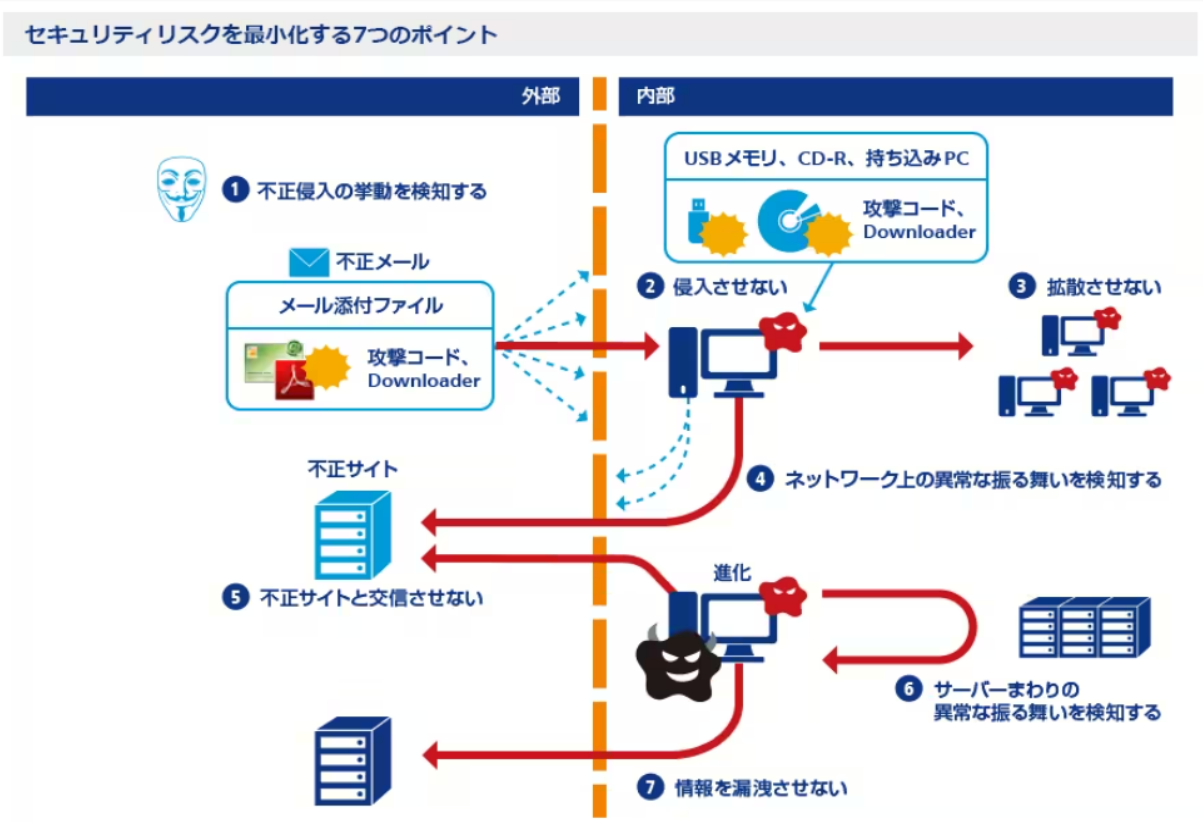
【参考資料】

書籍：あなたがセキュリティで困っている理由　辻 伸弘 著　2019年5月 日経BP刊

情報セキュリティ10大脅威｜情報セキュリティ｜IPA 独立行政法人 情報処理推進機構

RaaS（ランサムウェア・アズ・ア・サービス）とは？手口や被害事例、対策について解説 (shiftinc.jp)

ランサムウェアの被害事例 サイバー攻撃の手法とセキュリティ対策｜docomo business Watch｜ドコモビジネス｜NTTコミュニケーションズ 法人のお客さま



ランサムウェアの被害事例 サイバー攻撃の手法とセキュリティ対策｜docomo business Watch｜ドコモビジネス｜NTTコミュニケーションズ 法人のお客さま

以上