

自治体のサイバーセキュリティの課題を Bromiumの新技术が解消する

東京オリンピック・パラリンピックを来年に控え、自治体におけるサイバーセキュリティ対策が急務になってきている。はたして、現在の自治体のセキュリティにはどのような課題があり、今後、どのような対策を講じていくべきなのだろうか。セキュリティ関連のプロフェッショナル集団である(株)ブロードの稲森氏にそのあたりを解説してもらった。

課題山積の セキュリティ対策

地方自治体にとって、サイバーセキュリティ対策が大きな負担になるうとしている。たとえばマイナンバーの管理ひとつとっても、どう守るか具体的には考えられていないのが現実だ。そして、大きな契機となるとみられているのが、来年に迫った東京オリンピック・パラリンピックだ。開催期間が1カ月半と長く、東京のみならず国や近隣県などがかわるため、何が起こるか予測不能なのだ。あるハッカー集団が震が関と間違えて霞ヶ浦にサイバー攻撃をかけたという笑い話があるが、地方都市にとっても他人事ではなく、油断はできない。

開会式で照明が消えていたかもしれないという報告もある。また、この5月に開始された東京大会のチケット申し込みはネットのみにかぎられ、アクセスが集中してサーバにつながらなくなる人が続出した。かつてないほどネット環境に依存した東京オリンピック・パラリンピックで怖いのはサイバーテロなどの情報爆弾。偽造チケットがつくられたり、公式HPがアタックされる危険は大いにあり、国をあげてのサイバーセキュリティ対策が急務となっている。

表したのは、大会が1年後に迫った今年の4月。その内容も複雑化、巧妙化するサイバー攻撃に対処し、その被害の予防や拡大の防止のためには情報共有が有効としているが、リリースの冒頭には「サイバーセキュリティの確保は、本来、各組織が自主的に取り組むべきもの」と他人事とも取れる文言もあり、どこまで本気なのか疑問符がつく。

5月には与党・自民党が、現在各都府に分かれて一元化されていないサイバー防衛の関連施策を、司令塔として一括担当する「サイバーセキュリティ庁」の新設などの提言をまとめたが、2025年の創設を目指すとしており、対応の遅さは否めない。また「たんに情報を共有するだけでは、パソコンやサーバを攻撃するウイルスや不正ソフトなどのマルウェアの侵入は防げな

い」と、マルウェア対策ソフト「Bromium(ブロミアム)」の日本総代理店である(株)ブロードの稲森氏は指摘する。「マルウェアは秒単位の短い間でも、新しいパターンが無数に生まれる。1種のものが世界にバラ撒かれるのではなく、どんどん形を変えてしまうので、過去のパターンを分析しても対応しきれない」というのだ。

他方、政府機関によるサイバーセキュリティ指針で推奨されている手法に「ネットワーク分離」というものがある。インターネットにつながるパソコンと社内用のパソコンを分けるというシンプルな対策だ。しかし、ネット環境を使うために複雑な手続きが必要になり、業務効率も落ちてしまう。何よりもパソコンの台数が2倍必要になり、それを回避する製品もある



ブロードの稲森氏

従来にない発想の セキュリティソフト

こうした状況に風穴を開けるといわれているのが、前述のBromiumだ。開発者であるケンブリッジ大学教授のイアン・プラット氏は、世界的なネットワークをもつアマゾンウエ



米国連邦 政府機関

をはじめ、世界の重要な
公的機関・有名企業を含む
400社以上が採用!!



添付ファイルを 開く時の不安は これで解消!!

ウイルスを完全隔離[※]

従来とは全く異なる発想のセキュリティツール



【プロミアム】



世界の主要銀行 米国主要小売業 世界の中央政府 米国最大級企業 防衛機関 法執行機関

※2013年以降、Bromiumは推計20億以上のMicroVMが実行されましたが、侵害報告件数はゼロです。(米国Bromium社調べ)

詳細は [BROAD Security Square] で

bs-square.jp/columbus

株式会社ブロード

〒101-0014
東京都千代田区永田町1-11-30
サウスヒル永田町7F
TEL: 03-6205-7463 (代表)



最近のサイバーセキュリティ事件

- ・ブラック・エナジー事件では、停電により産業界や一般市民の生活に影響がおよんだ。
- ・サンフランシスコ・メトロ事件では、交通機関の混乱、得られるべき運賃収入が失われた。
- ・大手通信教育会社の情報漏洩事件では、10万人規模が「通信教育」をやめた。
- ・大手ホテルチェーンのPoSマルウェア事件の影響は、金融機関、小売、交通機関にすらおよび、100人単位の職が失われる結果となった。
- ・バングラディッシュ銀行他のBPC事件では100億円規模の金銭被害となった。
- ・ロシアのサイバー攻撃は各国の首脳選挙の結果を左右する影響を与えている。
- ・WannaCryでは、世界中の病院、政府機関、工場などに影響がおよんだ。
- ・Petyaでは、ウクライナ国内がパニックに陥った。

DBIC ©2019, Digital Business Innovation Center, All Rights Reserved (株)ブロードの資料より引用)

ブサービス(AWS)に採用されているXenSourceの創立者として知られている。サイバー攻撃対策はマルウェアを遮断するか、侵入してしまったものをクリーニングするというのが従来の発想だった。その作業には長い時間と膨大な費用が必要で、情報資産の毀損も免れない。しかしBromiumは、マイクロVM(仮想マシン)という画期的な手法で、侵害報告件数ゼロを実現している。

サイバー攻撃が最初に侵入するのは、エンドユーザーのパソコンが9割といわれている。主にメールやブラウザへのアクセス、USBなどの経路が一般的で、それをブロックすることがサイバーセキュリティでは重要といわれている。そこで「Bromiumはメールの添付ファイルなどをマイクロVMに隔離した状態で処理を行う。つまり、パソコンのなかにもうひとつ仮想のパソコンをつくり、そこが感染した場合にはマイクロVMごと閉じてしまうことで本体や情報資産を守るのだ。しかも、マルウェアを観察することでそのパターンも分析するという。

そのセキュリティ技術は海外ではすでに高く評価されており、アメリカ政府やインターポールなどが導入している。ブロード代表取締役の姫野恵悟氏は、3年前にこのソフトのことを知り、アメリカに通い詰めて日本への導入を実現したそうだ。Bromiumのもうひとつの特徴は、コストパフォーマンスの良さだ。自治体の規模にもよるが、億単位といわれる従来のサイバーセキュリティ対策と比較すれば、その費用負担ははるかに小さいという。

もちろん、機器の導入やメンテナンスで利益をあげていた従来のメーカーや業者の反発も予想される。地方自治体の職員のITリテラシーの低さや、ソフトに対応していない古いパソコンを使いつづけているケースなど、導入までにクリアしなくてはならない課題も多い。しかしサイバーテロの標的になって実害が発生したり、情報資産が毀損されてからでは遅きに失する。地方自治体の情報担当者は、今こそ現実的で効果的なサイバーセキュリティ対策に取り組んでほしい。