東京2020のセキュリティは万全か、課題山積みの日本のサイバーセキュリティの弱点とは何か

「タスクを仮想パソコンで隔離する「Bromium」の革新性とは何か

高度なネット社会の進行に応じて、サイバーセキュリティの重要性が高まっている。サイバー攻撃の進入路としてもっとも対策が必要といわれているのが、個人の端末などのエンドポイントセキュリティである。そして、このセキュリティに威力を発揮するのが「Bromium（ブロミアム）」、革新的なソフトだ。開発したのは米連邦政府機関で550万台のPCに導入されるなど、世界的に注目されているBromium社、アプリケーション分離・インターネット分離などのあらたな分野を独走するパイオニアだ。そのBromium社がこの9月、東京でアジア太平洋地域で初めてのサイバーセキュリティ・サミットを開催した。今号ではその様子をお伝えしたい。

参加したのは企業・団体のサイバーセキュリティの責任者や実務担当者、ジャーナリストたち。まずはサイバー犯罪捜査分析のスペシャリストでサイバーセキュリティベンチャー専門の投資会社であるForgepoint Capital社顧問のシェーン・シュック氏が「境界なきサイバー犯罪と国家支援のサイバー攻撃の現実」というテーマで基調講演を行った。


シェーン・シュック氏

そして、サイバー犯罪はその昔からあったが、当時はサービスの中断を目的としたものが多く、2003年頃から徐々に悪質になってきたと分析した。

「その頃からウィルスによる悪意の妨害がはじまり、しだいに脅威となりました。ロンドン五輪のサイバー攻撃が大きなニュースとなった12年に入ると、それまで少数の個人で活動していたハッカーがグループとなり、脅威がより大きくなりました。こうしたサイバー攻撃に対抗するためには相応の高度なテクノロジーが求められるようになりました」

ついで、国家的なサイバー攻撃がみられるようになったのは15年頃からだと、シュック氏は指摘する。

「サイバー攻撃グループが専門家集団となり、明らかに国家と対峙するようになり、サイバーセキュリティをめぐる攻防は、第3のフェイズに入りました。15年からは主権国家が経済的な優位性を得るために情報を盗むということも起こり、攻撃側がこれまで以上にテクノロジーを強化し、脅威をもたらすようになり、サイバー攻撃の回数を示すイールドカーブの勾配も高くなってきています」

そのあらたな攻撃ターゲットはSNSだと氏は強調する。それまでの「サイバー攻撃による銀行振込への侵害、資金が盗まれるなどの被害」とはまったく異なり、より攻撃的になったと、氏は警告する。そして「今は金融口座よりもSNSのIDのほうが価値が高い時代。ハッカーにとっては機密情報などの諜報活動のほうが、はるかに利益が得られる時代となりました。その被害を防ぐためには、使用時以外は端末の電源を切ることと、サイバー攻撃の主体者を隔離するソフトが重要です」と話した。

本当に東京2020の安全対策は大丈夫か 全種目に綿密なプランが必要

つづいてDBIC（大手企業34社によるデジタルイノベーションを推進する組織）共同創設者でインターポールサイバー犯罪専門員会委員の西野弘氏が


会場の様子


近江有氏


徳永拓氏


シャバン・ナウム氏


西野弘氏

「今後ますます重要になる、サイバーセキュリティでのレジリエンス（復元力）向上」というテーマで、サイバーセキュリティにはテクノロジー以上にマネジメントが必要であるという持論を展開。事例として、東京2020オリンピック・パラリンピックのサイバーセキュリティに対する問題をあげ、その脆弱性を指摘した。

そして冒頭、ボストンマラソンの例を引き合いに海外でのテロ対策を解説した。13年に起こった爆弾テロ以降、ボストンマラソンはセキュリティ、サイバー犯罪のモデルケースとして扱われ、これまでに幾度となくさまざまな国で取り上げられてきたという。

「マラソン大会がセキュリティのモデルケースといわれる理由は、その守備範囲の広さにあります。約50キロメートル四方がセキュリティの対象なのです。1カ所の競技場だけで行う場合とは比べものにならないくらい難易度が高くなります。そのために300ページにもおよぶオペレーションプランが用意され、いくつもの計画書が練られるのです。日本から視察に同行した警察の方も、リスクにもとづいた綿密な計画があらかじめ用意されていることに驚いていました。単一競技でこれだけの準備が必要なのですから、オリンピック・パラリンピック本番では毎日全種目、全会場において警備計画が必要になるはずです。ちなみに、ボストンマラソンでは大会当日、地下の指揮センターに70の異なる機関、250名人員が確保されました。当然、警備以外に救急や消防関係者もチームを編成し、プランどおりにアクションがとれるかどうか事前に検証し、当日に臨んだのはいうまでもありません」

そして、日本のサイバーセキュリティの弱点として、氏は経営層の認識・理解不足、プロフェッショナル人材の不足をあげた。

「問題は理系・文系なんていっていることです。そんなことをいっているから世界から取り残されるのです。そんな垣根なんかありません。『私は文系だからITはわからない』といった途端に、海外ではその経営者はクビです。もちろん、セキュリティ人材の少なさも深刻で、アメリカではトップガンクラスといわれる優秀な学生を国費で教育していますが、日本はアメリカはおろか、韓国にも遅れをとっています」

また、ITを供給するベンダーやメディアのセキュリティに関する向き合い方についても苦言を呈した。

「ベンダーに依存している問題も大きくて、日本のIT予算は7～8割を保守運用に使う構造になっています。その部分を自動化して人材養成に使ったらどうでしょうか。保守やメンテナンスはベンダーにとっては儲けの源泉であるので、指摘されても黙ってしまって前に進まない。マスメディアの認識も問題で、情報漏洩の会見などでは、本来は被害者であるはずの企業側の謝罪シーンばかりを取り上げますが、犯罪者に関する報道は、ほとんどメディアに取り上げられていないのが現実です」

結論としては、サイバーセキュリティのレジリエンス向上のためには、先端のテクノロジーを投入して自動化することで、エンドポイントである端末を守ることが必要だ、ということだろう。

サイバー攻撃対策は自動化しなければ防げない

エンドポイントを自動的に守る手段として注目されているのが、VM（仮想マシン）でマルウェアを隔離するソフト「Bromium（ブロミアム）」だ。というわけで、つづいてBromium社の戦略・技術担当副社長のシャバン・ナウム氏が登壇し、サイバーセキュリティを人によるスキルで防ぐことの難しさを、アンケートのデータをもとにつぎのように解説した。

「近年認識されている悪意のあるファイルの97パーセントは、それぞれのPCごとの固有のものでした。また、47パーセントのマルウェアは新種やゼロディと呼ばれるものでしたが、既存の防御システムを回避できたのです。ところがビックリしたのは94パーセントのセキュリティ担当者が、セキュリティよりも仕事を完了できることを気にしていると回答したことです。また、上司からの要請によってセキュリティ制御を解除したり、調整したりしたことがあると回答した担当者も64パーセントに上りました」

きわめて危険なマルウェアが存在するのに、仕事の効率や上司の指示を優先している実態、そしてセキュリティ担当者のガードが隙だらけである実態がみえてくる。

「企業もサイバー攻撃に対応していますが、攻撃側はリアルタイムで変更を重ねており、追いつくことは困難です。トロイの木馬など、危険なマルウェアは存在自体を自動で削除しなければいけません。悪質なサイバー攻撃を検出することは困難で、

第2部は会場を㈱ブロード本社に移してのコミュニケーション・セッション。第1部の登壇者によるパネルディスカッションとカジュアルな情報交換会で、穏やかななかにも真剣な意見交換が行われた

標的にされたら勝ち目はありません。だからこそ、VMでタスクを隔離するBromiumが有効なのです」

最後に、Bromiumの導入に関連した2社の事例紹介があった。まずセキュリティ分野で活躍するITサービス提供会社の㈱GRCS執行役員の徳永拓氏は、ファイヤーウォール、ウイルス対策ソフトのつぎに何を入れればいいのかを複数比較し、同社の顧客にBromiumを提案し、導入されたと報告。

GRCSが数あるセキュリティソフトからBromiumの導入を提案したのは「省庁からの指導やサプライチェーンの大元の会社からのセキュリティ要件は増加傾向にあり、Bromiumはそのひとつの解決策になりえる」と考えたからだった。また、製品の検討にあたっては「自社が持つ情報資産と、それを脅かされたときの被害の大きさを明らかにし、インシデントの発生可能性と掛け合わせることで対応方針を検討することがポイントになった」とも。そのほか、導入によって「使い勝手が悪くなるなど、生産性への悪影響があるかないか」といったことや「初期導入や運用のコストについてもそのバランスを考えた」そうだ。

ついで、製薬企業のエーザイ㈱の子会社であるEAファーマ㈱情報企画部の近江有氏が、Bromiumのテスト導入について話した。一般的に新薬の開発には10年以上の年月がかかるといわれ、その間にデータを守り、改ざんさせないということが求められる。にもかかわらず、セキュリティ事故や不注意がどうしても起きるという。

そうしたなか、昨年、エーザイから「セキュリティインシデント発生により、外部記憶装置使用禁止」といった通達があったという。とはいえ、研究会でドクターがプレゼンする資料を当日その場でUSBなどで受け取ることがよくあり、結果、MR（医薬品情報をドクターに提供する製薬メーカーの営業担当）は、外部記憶装置を使わざるをえない状況に追い込まれる。また、研究所や工場の現場では、日々、ネットワークにつながっていない実験機器や製造機器とのデータ授受で、外部記憶装置を利用せざるをえないという。

そこで、このBromiumを2週間ほど本番環境でテスト使用してみようということに。結果は何のストレスも違和感もなく使えて高評価だったという。「今後はぜひ、グループ企業全体でこのBromiumを使うことができないかと考えている」と近江氏は結んだ。

Bromiumは「アプリケーションの隔離」というまったく新しい発想のソフトだ。そのため、競合他社がなく、他製品と比較できないことが逆にネックになり、日本では検討に時間がかかる場合があるという。日本においては経営者の意識改革が、サイバーセキュリティの最大の課題なのかもしれない。