コロナ禍で急増する身代金目当てのサイバー攻撃!!
国家機関も大企業も、そして中小企業もサイバーテロの脅威に!!

まずはエンドポイントを「仮想パソコン」（マイクロVM）で守ることが肝心だ!!

世界的に増加の一途をたどっているサイバー攻撃。その内容は激化しつづけており、最近では大規模インフラが停滞したり、防衛産業の情報が漏洩したりと、看過しがたい問題が続出している。そこで、今号ではエヌ Inc.のセキュリティ事業をグローバルで統括するイアン・プラット氏をゲストに迎え、近年のサイバー攻撃の動向やそれに対して有効なサイバーセキュリティのあり方について話してもらった。聞き手は本誌編集長の古川猛。

仮想化技術のパイオニアによる先進的なセキュリティシステム

古川猛・本誌編集長　イアンさんは仮想化技術のパイオニアとして世界的に知られていますが、その基礎はケンブリッジ大学に在籍していた頃に築いたそうですね。

イアン・プラット・HPセキュリティ事業責任者　大学に入ってすぐにスタートアップを立ち上げて、その後、博士号を取得し、ケンブリッジで教鞭をとりました。そして、研究室で仮想化技術の開発に取り組み、「Xen（ゼン）」というオープンソースのハイパーバイザー（仮想マシンをつくりだすソフトウェア）を開発するプロジェクトを立ち上げたのです。ちなみに、このXenプロジェクトはやがてXenSource社の設立へとつながり、2007年にCitrix社に売却するにいたりました。

編集長　仮想化技術とはどういうものなのでしょうか。

イアン　仮想化技術とは1台のハードウェア上で複数の仮想マシンを論理的に構築する技術のことで、もともとは1960年代にIBMがハードウェアの効率的な利用を目指して開発しました。そして、私はこれをセキュリティ分野においても活用できるのではないかと考え、Xenプロジェクトなどに取り組んできたわけです。

編集長　その成果のひとつがエンドポイントセキュリティシステムとして知られる「Bromium（ブロミウム）」なのですね。

イアン　そうです。XenSourceを売却した後は、米国のスタンフォード大学で教鞭をとりながら、学生たちとともにエンドポイントセキュリティの研究に没頭しました。そして、11年にはBromium社を設立し、仮想化技術をフル活用したエンドポイントセキュリティシステムとしてBromiumを世に送り出したのです。このシステムはマイクロVM（仮想パソコン）で文書ファイルやインターネットのページを開くような仕様になっており、あらゆるウイルスなどからPC本体を守ることができます。たとえば、ウイルスが仕込まれたメールを誤って開いてしまったとしても、マイクロVM上でのことなので、本体にはまったく影響がないのです。

編集長　素晴らしい発想のセキュリティシステムですね。

イアン　おかげさまで、米国の国防総省をはじめとした多くの国家機関などで採用いただき、世界的に信頼度が高いセキュリティシステムとして評価してもらえるようになりました。また、日本においては㈱ブロード（東京都千代田区）と日本語対応などに取り組み、日本市場での販売にも踏み切りました。

編集長　19年には世界最大級のPCメーカーであるHP Inc.（15年にヒューレットパッカードから分社）の傘下となり、よりグローバルな規模でサイバーセキュリティに取り組まれていますね。

イアン　HPはXenプロジェクトの段階から私の研究を高く評価してくれていましたし、Bromiumも積極的に採用してくれました。そういう意味でも、私たちがHPの傘下に入ったことはごく自然な流れだったように感じています。

編集長　HPではBromiumをどのように取り扱っているのでしょうか。

イアン　Bromiumは「HP Sure Click」「HP Sure Click Enterprise」という製品名になり、あらためてHPのPCに搭載されることで、より多くのエンドポイントセキュリティに貢献しています。HP製のPCだけでなく、すべてのWindows-PCで稼働することができるほか、HP社のセキュリティ事業の中核を担っています。仮想化技術で多くの人たちのセキュリティ対策に貢献したいと考えてきた私にとって、これはこのうえない喜びでもあります。

アーキテクチャデザインを推進し、多様なサイバー攻撃から情報を守る

編集長　近年、世界的に重要なインフラに対する深刻なサイバー攻撃が散見されます。たとえば、今年5月にはアメリカ東海岸で消費されるガソリンや燃料の約45㌫を供給している石油パ

イアン・プラット

HP Inc.セキュリティ事業責任者

イギリス生まれ。 ケンブリッジ大学で教鞭をとりながら、Xenプロジェクトを立ち上げ、セキュリティ分野における仮想化技術の活用方法などを研究。 その後、XenSource社の設立・売却などを経て、2011年にアメリカでBromium社を設立し、エンドポイントセキュリティシステムである「Bromium」を開発。19年にはHP Inc.の傘下となり、現在は同社のセキュリティ事業のグローバルでの責任者を務めている。

イプライン管理会社がランサムウェア（身代金を要求するウイルス）の攻撃を受け、1週間にわたって燃料の供給がストップするといった事態が発生しました。こうした事案は増加傾向にあり、ますますサイバーセキュリティが重視されています。イアンさんは現在、HPのセキュリティ事業の責任者を務めていますが、こういった状況をどのようにみていますか。

イアン　ご指摘の通り、ランサムウェアに関しては、従来以上に国家機関や大手企業をターゲットとし、高額な身代金を要求するケースが増えています。また、即座にアクションを起こすのではなく、ウイルスを潜伏させておいて、攻撃の機会を狙うというスタイルのウイルスも増加しています。

編集長　そういったなか、欧米ではどのようなセキュリティ対策が講じられているのでしょうか。

イアン　さまざまなセキュリティ対策が講じられていますが、どうしても後手にまわっている印象は拭い切れません。つぎつぎと新しいウイルスなどが開発されるなか、企業などで一般的に使用されているセキュリティソフト（検知ツール）ではほとんど意味をなさないような状況になっているのです。

編集長　サイバー攻撃に歯止めをかけることはできないのでしょうか。

イアン　サイバー攻撃を行っている犯罪集団はいまや信じられないほどの規模に成長しており、国家機関や大手企業を上回るテクノロジーを有しています。彼らにとって、セキュリティの検知ツールの網を突破するのは造作もないことですし、一般的なOSやアプリケーションの脆弱性もすべて把握しているといっていいでしょう。しかも、犯罪集団はこうしている間にもつぎつぎと新しいテクノロジーと戦略を取り入れているので、いかに検知ツールなどのレベルを向上させたとしても、当面はイタチごっこがつづくのではないでしょうか。

編集長　日本においても防衛産業などがサイバー攻撃にさらされるなど由々しき事態が発生しています。そういった企業は情報を守るためにどのようなことを心がけ、実践すればよいのでしょうか。

イアン　重要なのはコアな情報を守り抜くためにシステム全体のアーキテクチャ（基本的な設計概念）をデザインすることです。それにはまず、自分たちにとって何がもっとも大切な情報なのかを見極め、それをどのように保護し、システムやセキュリティポリシーを構築していくかといったことをシッカリと検証しなければなりません。もちろん、その際にはウイルスが添付されたメールを開いてしまうなどの人為的なミスにも対応する必要があります。近年ではゼロトラストという概念が注目されていますが、その代表的な手法である管理者権限の制限などをセキュリティポリシーのなかに盛り込んでいくことも肝心でしょう。とくにコロナ禍以降はZoomをはじめとしたウェブ会議ツールを使う機会が増え、それとともにサイバー攻撃にさらされる機会が増加しています。そういった状況だからこそ、あらためて自社のセキュリティシステムやセキュリティポリシーがどうなっているかを検証し、アーキテクチャの部分から見直しをはかっていってほしいと思います。

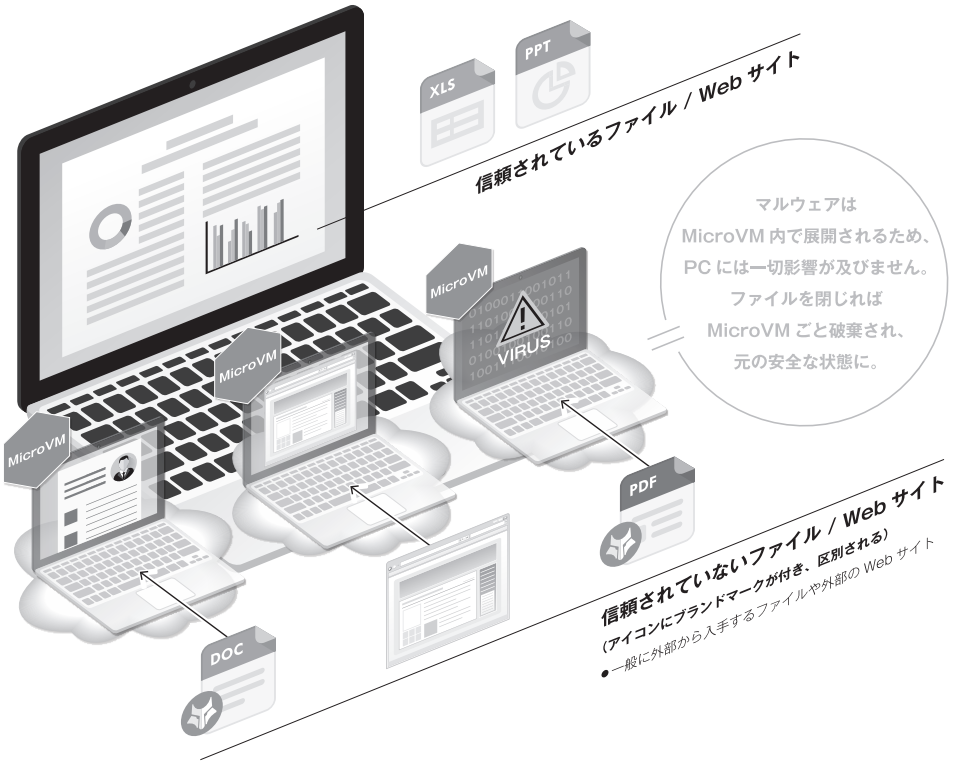
編集長　日本政府はサイバーセキュリティ人材を育成していく方針を掲げていますが、そういった人材の増加はサイバー攻撃の抑制につながっていくのでしょうか。

イアン　多くの国がサイバーセキュリティ人材の育成をすすめていますが、サイバー攻撃の調査・分析を行うだけでは意味がありません。それ以上にシステムエンジニアとしてアーキテクチャをデザインできる人材を育成していくことが肝要です。日本にはぜひともそういった人材を育成していってほしいですね。

組織・企業の規模や性質にあわせたサイバーセキュリティを提供

編集長　Zoomなどのウェブ会議ツールやIoT（モノのインターネット）の普及によって、サイバー攻撃を受けるリスクはこれからさらに大きくなっていくような気がしています。

イアン　まさに現代社会はインターネットですべてがつながっている状態にあり、国家機関も民間企業も、そして個人でさえもつねにサイバー攻撃のリスク



Officeアプリなどを使用するうえで必要最低限のOSを持つ専用のマイクロVM（仮想パソコン）を独自開発。マイクロVMは文書ファイルなどを開くと自動で瞬時に起動するのでユーザーには違和感がない
提供：㈱ブロード

と隣り合わせの状態にあるといえます。

編集長　そうなると、あらためてエンドポイントを守ることが重要になってきそうですね。

イアン　実際、サイバー攻撃の入口の約70パーセントがエンドポイントだという調査結果があるほどなので、企業の大小を問わず、これからはさらにエンドポイントを守るという意識を持たなければなりません。

編集長　とはいえ、中小企業にとってはセキュリティに関して大規模な投資を行うことは困難ですし、セキュリティシステムを採用することで通常業務に支障が出てしまうようでは元も子もありません。

イアン　小規模な事業者であれば、エンドポイントを守ることでほとんどのサイバー攻撃から身を守ることができると思うので前述のHP Sure Clickを導入いただくだけでも十分な対策を講じることができます。また、HP Sure ClickはPCの操作性にもほとんど影響を与えない設計になっているので、セキュリティレベルを上げながら従来と同じような感覚でPCを使っていただけると思います。

編集長　HPでは「HP Wolf Security」というあらたなブランドも推奨していますね。

イアン　HP Sure Clickや同Enterpriseのほか、HPがこれまでに培ってきたさまざまなセキュリティ技術やノウハウを詰め込んだ仕様になっており、まさにこれひとつであらゆるサイバー攻撃からエンドポイントを守れるようになっています。HPのPCに搭載していくのはもちろん、他社との協業もすすめ、さらなる普及を目指したいと考えているところです。

編集長　日本市場においてはどのような戦略で普及に努めていきますか。

イアン　日本では組織や企業にあわせたカスタマイズが求められることがしばしばあるので、HPの総合力を生かしながら柔軟に対応していきたいと考えています。組織や企業の大小を問わず、それぞれの規模や性質にマッチしたセキュリティサービスを提供できるのは、まさにHPの強みといえるでしょう。

編集長　サイバー攻撃の世界的な動向や最新のセキュリティ対策などについて理解することができました。コロナ禍でテレワークが一般化し、エンドポイントが狙われやすくなっている今こそ、自社のセキュリティ対策を抜本的に見直す必要がありそうですね。