資料6

意見書

2018 年 1 月 17 日
日本電気株式会社
代表取締役会長
遠藤　信博

1. サイバー空間の情勢

2017 年は、ランサムウェア、DDoS 攻撃、Web アプリケーションの脆弱性をついた攻撃が猛威を振るった年でした。また、仮想通貨に関係したサイバー犯罪が急増し、サプライチェーンを標的とした攻撃が現実となりました。

近年のサイバー攻撃の特徴は、防御が手薄なところを見つけ、対策が不十分な間に集中的に攻撃することにあります。 この中でも、WannaCry、NotPetya、BadRabbit 等のランサムウェアの感染能力を強化した攻撃は、感染対策が後手に回り、海外で被害を拡大させました。

脆弱性に関しても、話題が多い年でした。3 月の Apache Struts 2 の脆弱性に始まり、10 月には、WPA2 の脆弱性、Infineon Technologies が提供する「RSA 暗号ライブラリ」の脆弱性が見つかり、さらに 2018 年 1 月には、Intel CPU などの投機的実行に関する脆弱性と立て続けに脆弱性に対応する必要が発生しています。これらの中には、IoT に関係する脆弱性も含まれており、その対応にはより多くの時間や費用を要するようになっています。

2. 継続的なセキュリティ対策

2015 年のサイバーセキュリティ戦略では、サイバー空間への認識を新たにし、5 つの基本原則に基づき、セキュリティ対策を推進してきました。現在、サイバー空間の平和が維持されていることから見ても、これらの原則や対策が大きく間違っていなかったと思われますが、今後より詳細な検証に期待します。

この中でも特に、「経済社会の活力の向上及び持続的発展」で挙げられている、「セキュリティマインドを持った企業経営の推進」は、各組織の経営層に対するセキュリティのメ

ッセージでありました。まだ、すべての経営者まで行き渡っていないとは思いますが、引き続きメッセージの発信を続けて頂きたいと思います。実際、米国の信用情報企業 Equifax 社で発生した情報漏えい事件では、約 1 億 4300 万人分の機密情報が漏えいし、株価の下落、経営層の辞任という事態に発展しました。経営層がセキュリティにコミットすることを、当たり前にして行く必要性を強く感じています。

「国民が安全で安心して暮らせる社会の実現」では、マルウェア対策、DDoS 攻撃対策、そしてオリンピック・パラリンピック対策が重要になると思います。特に、繋がっていてこそ意味がある「サイバー空間」は、他の社会インフラに比べると明らかに防御が難しいインフラです。この社会インフラをどう守るか、再度知恵を結集して戦略を考える必要があります。その中で重要なのは、攻撃のスピードに対応する「リアルタイム性」、攻撃の豊富なパターンに対応する「ダイナミック性」、広範な範囲の攻撃に対処するための「リモート」での対応だと思います。これらを、実際の施策に織り込みながら、より効率的な防御や情報の共有を実現することを目指すべきだと思います。

サイバー空間で忘れてはならないのが、デジタルガバメントのセキュリティです。各種行政手続きの電子化が進む中、一旦これらの運用が停止したり、情報が流出したりすると、人々の生活に甚大な影響が出ます。今後さらにデジタル化が進むと自治体や政府機関がもつすべてのデータがリンケージされ、より情報の活用度が上がります。このような社会の基盤となるシステムは、最初から統一された方式で綿密に設計されたシステムでなければなりませんし、常に最新のセキュリティ技術が導入可能な汎用性を備えている必要があります。特に、予算が不足している自治体等でも、政府機関と同等レベルのセキュリティを確保できるよう、「リモート」での集中的な対応により、コストダウンと対策レベルの維持を実現することも大切だと思います。

さらには、シームレスな構造をとるサイバー空間では、攻撃にかかるコストはどこに対して行ってもほぼ同じになります。このため、攻撃者は多少手間をかけてもより脆弱なサイト、より発見されにくいサイトを見つけ出し、攻撃に利用、あるいは直接の攻撃対象とします。ガバメントで言えば、より国民に近い位置にある自治体、公共機関、教育機関が、民間ではサプライチェーンの末端組織がより狙われやすいと考えられ、これらに関しては、すでに強化されている組織より、重厚なセキュリティ対策をとる必要があります。

3. IoT と人材育成の戦略

近未来を考える中で、今対策が急務なセキュリティ対策は、「IoT のセキュリティ」と「人

材育成」です。前者は、急激に脅威が増大しつつあるセキュリティの課題で、時代の流れにセキュリティ対策が追い付いていません。また、「IoT」の問題は単に「安全・安心」だけに関係するものではなく、近い将来日本の産業全体にとって重要な課題となります。「AI」に関しても同様のことが言え、これらの新しい技術・概念に対して、サイバーセキュリティ戦略を持って対応することが大切です。

サイバーセキュリティ人材の育成が「質」と「量」の両面で進められてきました。特に「量」に関しては、IPA を中心にした「情報処理安全確保支援士試験」に約 7000 名が登録され、また、経産省の「サイバーセキュリティ経営ガイドライン」も各組織内の人材育成に貢献していると思います。現時点でまだ、人数が大幅に不足しているのは確かですが、現在の施策を続けることで、一定の成果が期待できると思います。同時に、国民全体のセキュリティ意識のレベルアップが必要で、小学生から社会人、高齢者までを含めた幅広い施策の実施をお願いします。

一方、「質」に関しては、まだ強化の序盤にあります。IPA の「産業サイバーセキュリティセンター」「セキュリティ・キャンプ」、NICT の「ナショナルサイバートレーニングセンター」、JNSA 主催の「SECCON」などの施策が効果を発揮し始めていますが、日本の実力はこんなものではないと思います。隠れた人材、十代の若き人材を見出し、中学・高校・大学・専門学校等の教育機関が連携し組織的に育成することが必要です。特に、セキュリティ分野に特化した教育を行う「専門学校」の役割が重要になると思います。

また人材育成・IoT とも日本の産業界とも深く関係するので、日本経済団体連合会(経団連)等の経済団体や各種セキュリティの業界団体、ISAC 等と連携してこれらの課題を解決して行く必要があると思います。

4. 将来を見据えた戦略

2020 年以降の日本の産業に必要なものは、「IT 技術の主導権」と「安全・安心感の定着」だと思います。これらが、海外から認められるようにすることが、日本の発展に直結すると思います。

まず「IT 技術」に関しては、AI 技術を中心に、高度に自動化されたシステムを構築し、これらを海外へも提供して行く必要があります。すでに、攻撃者が AI 技術を侵入活動や DDoS 攻撃などに使用し始めているという情報があります。防御側も、すでにマルウェアや攻撃の検知での AI 利用は実用化されていますが、今後は AI を利用して自動的に防御する技術が主流となることでしょう。人材の育成で苦戦している分野に関しては、AI で

代替するための研究・開発に注力すべきです。難易度の高いマルウェアの静的解析などの分野でも、AI 技術は、研究者・解析者を強力に支援してくれるようになると思います。

AI 技術を導入する上で重要となるのは、セキュリティに関する情報の共有です。日本や海外の協力してくれる組織で収集したあらゆる攻撃や防御の情報を、リアルタイムで人工知能に取り込み解析させる。実際にこういったシステムを構築して、その成果を世界に示すことが、サイバー攻撃を抑止する上でも重要となってきます。

また、日本が国際社会でサイバーセキュリティ立国を実現するためには、諸外国から「日本の IT インフラ・IT 製品は『安全・安心』である」という評価を得る必要があります。すでに、日本の IT 製品は高い品質レベルを達成していますが、これは攻撃者が存在しない環境での「安全・安心」です。サイバー空間では、悪意を持ってサイバー攻撃を行う攻撃者が存在するため、より高いレベルの「安全・安心」を国家レベルで実現すること、「安全・安心」にほころびが生じてもすぐに修復可能なこと、が重要となります。特に、IT 製品の製造現場に「セキュリティ・バイ・デザイン」の考え方を普及させることが重要です。

国家レベルでの評価では、各国の最低レベルが重要な意味を持つため、政府が先頭に立って大企業から中小企業までの、セキュリティを確保することが重要です。そのためには、セキュリティの基準を作り、基準を満たした企業には認証を与える施策を産業の隅々まで拡張し継続して行く必要があります。

以上