2015 年 3 月 9 日

# サイバーセキュリティに関する現状と課題

株式会社ラック CTO 西本 逸郎

※本資料は、1 人のサイバーセキュリティ専門家としての意見であり、株式会社ラックをはじめとする西本所属組織や団体の意見ではありません。

## 1. ラックについて(参考)

1986 年設立(旧ラック)の純国産会社。システム開発会社(受託開発請負会社)として事業を開始し、95 年からサイバーセキュリティ事業を立ち上げ。しかし、セキュリティ事業単体では 10 年間黒字を出すことができず苦戦を強いられた。00 年より開始した監視事業(年間ストックタイプの事業)が黒字化した 05 年以降安定した成長を維持している。セキュリティ事業は景気や環境に影響されること無く国を守り続ける経営意思と資金が無ければ継続することができないため、堅実に利益を確保し続けることが重要であると肝に銘じ事業を推進している。最近、独自の斬新なアイディアで製品開発を行っているセキュリティ会社であるネットエージェント株式会社を子会社化するとの発表を行った。今後も優秀な海外製品をうまく利用しつつも国産製品の成長を図りつつ世界に通用する国産サービスで日本を支える会社を目指し続ける。

また、セキュリティに携わる以上、収益と直接には結びつかなくても、業界や人材の育成、メディアや社会の意識レベル向上のための啓発活動などが不可欠と考え、事業発足当時から以下に代表される活動を同じく業界を支える気概を持った企業や人々と一緒に継続している。

【事務局を引き受け活動】

JSSEC(一社)日本スマートフォンセキュリティ協会)、Grafsec-J(一財)草の根サイバーセキュリティ運動全国連絡会 公益化申請中) 、DBSC(データベース・セキュリティ・コンソーシアム)、セキュリティ・キャンプ実施協議会

【理事レベルを出し運用にコミットメント】

JNSA(NPO 日本ネットワークセキュリティ協会)、JC3(一財) 日本サイバー犯罪対策センター)、SECCON 実行委員会など

【一会員として活動】

(一社)金融 ISAC、SPREAD、IDF(NPO)デジタル・フォレンジック研究会)など

【各地で実施されているセキュリティイベントなどでの協力や支援】

サイバー犯罪に関する白浜シンポジウム、情報セキュリティ・ワークショップ in 越後湯沢、情報セキュリティシンポジウム道後、Hardeing 等の各種サイバー演習、各地での草の根勉強会など

2. サイバーセキュリティ人材育成

1)キャリアパス(セキュリティ人材の人生設計)

セキュリティ人材育成に関しては、端的に言って一般の企業でのキャリアパスが見えない状態で育成するだけでは効果を発揮できない。企業側も環境変化も伴う中、活かし続けるキャリアパスを構築することも困難である。現状では、スポットで使いたいというのが多くの企業の本音である。こういった中で、どういう人生が送ることができるのかを指し示しつつ実践することが重要である。(所謂、出口戦略)

2)人材育成費用

目指すレベルによるが、セキュリティ人材の育成とその維持には時間と費用もかかる。誰がどのように捻出し続けることができるのかが重要である。やりっ放しではすまない。

3)人材に対するリスペクト

我が国ではIT関連人材の社会的評価が実態と急速に乖離していると考えている。我々にとってITがどのような位置づけ(単に合理化の道具なのか事業基盤や価値創造の源泉なのかなど)に対する共通認識を持ち、それを覚悟した上で接する必要がある。技術者側は、技術レベルの向上を図る前に「何故セキュリティ技術者を目指すのか」と言った価値観や技術者倫理をしっかり持つことが肝要である。

個々のセキュリティ専門会社での人材育成とその維持を図ることは企業責任として当然のことであるが、以上を考慮すると、国を守るために必要な高度な技術者を含めた一般社会で活躍する技術者を維持するには、活躍する大量のセキュリティ人材に対し組織的に教育を実施し人的交流を図ることなどによる情報共有基盤を提供するなどし、相互信頼相互保証などを行いつつ、国を初めとした日本の産業をそのレベルに応じて支えて続け成長させていく活動を支える仕組みの構築が鍵となるのではないかと提言する。同時に、こういった活動を資金面から援助できる仕組みの構築(後述)も欠かせないと考える。

3. サイバーセキュリティ政策

サイバーセキュリティ向上の前にやるべきことがある。米国を代表とする海外では、他国が関与したとされるサイバースパイ事件報道が後を絶たない。一方、我が国においては他国ほど重大な事件報道はなされていない。米国を初めとする国々のサイバーセキュリティレベルは我が国より劣っているのであろうか。昨年末露呈した米国映画会社でのサイバー攻撃事案(機密情報窃取とその暴露による言論封鎖)でもそうであるが、対応として見えるのは、特定の国の関与を特定した上で、外交的意味合いを含めた対応(キャンペーン)を行っている。つまりは、重大事件に関しては引き起こした相手を特定する基準ができており、特定できた相手により国としてどのように対抗するかを決めていることに他ならない。サイバーセキュリティ対策とは、狭義的には「やられないようにする対策」であるが、そちらを優先すると、対策を進めなければならない私企業に対して相手が国家であれ守り抜く過度なセキュリティレベルを求めるだ

けではなく、事件発生時にはその私企業を（攻撃者の狙い通りに）窮地に貶めいれることにもなりかねない。それは我が国にとってマイナス要因にもなり得ることを理解しなければならない。

つまり、発生している或いは想定する脅威への対抗だけではなく、①それらを引き起こす組織や使用している基盤や道具（不正プログラムや乗っ取っている基盤など）を調査・プロファイリングする地道な活動、②実際の攻撃発生時に攻撃者とその目的を判断できるだけの仕掛けと仕組みの構築、①②で得られた情報に立脚し③誰がどのような対応をするのかを予め決めておくことが肝要であり、その上で守るための手立てとしてサイバーセキュリティ対策を行う必要がある。

4. サイバーセキュリティ産業の育成

他国と異なり、軍がサイバーセキュリティ技術開発や競争力強化を主導しない我が国においては、別の枠組みを考える必要がある。肝心なのは、効果的なセキュリティ対策を各企業や社会が実施する（お金を払う→市場を大きくする）ことである。そのためには、セキュリティ対策の重要性を訴えるだけでは正直言って難しい。100％の万全は無いことを前提とした取り組みが肝要である。100％の万全でないのに事件が起きると企業責任が問われてしまうようでは、重要インフラ組織は別として、一般企業で一定水準以上のセキュリティ対策を実施するとは到底考えられない。事件が起きるまでは経営課題にしないほうが得だからである。この状況を打開するには、これまでの事例に例えると、交通事故や病気の無い社会を目指すが、現実的にはそれらの発生を前提とした対応力を身につけ、最悪の事態に陥らないように生きていくことができる仕組みの構築が肝要と考える。

つまり、セキュリティ市場の拡大には、北風（事件発生時の制裁や受注条件を機軸としたセキュリティ対策の強制など）施策だけではなく、太陽（ほめる策）施策の拡充が考えられる。例えば、地球環境保護への取り組みに代表される、企業イメージを向上させる分かりやすい取り組み分野を整えることなどである。日本だけでは無く、世界が依存しお互いの信頼のもと活用し相互に成長していく空間である「新しい地球」とも言えるサイバー社会に関する安心安全の構築と維持に貢献していることを PR できる環境整備である。

そのためには、サイバー社会の住人である企業のサイバーセキュリティ対策だけではなく、従業員のリテラシー向上を率先して図り社会のモラルやマナーリーダーとしての貢献、セキュリティ人材への支援や啓発を行う組織（前述の提言）への寄付の奨励や優遇措置など、企業や社会が積極的に投資を行いたくなる施策などが考えられる。

5．20 年東京オリパラ、19 年ラグビーワールドカップに向けて

幸いなことに、19 年開催のラグビーワールドカップ、20 年開催の東京オリンピック・パラリンピックと歴史に残る世界イベント開催までに残された時間は少ない。IT 活用後進国とも揶揄される我が国が浮上できる待った無しの機会が持てることが幸いである。高度に発達するスマートフォンに代表されるウェアラブルなどのモバイル機器、ドローンなどの各種自動制御ロボットを含む IoT、自由で小回りの効く決済、日本全国街ぐるみのおもてなしの実現など楽しみが一杯である。

実施すべきことは、自動車社会で例えると、関連法の整備やその知識、自動車や道路などの安全性向上、早く走るため、渋滞を発生させない或いは解消させるため、安全に走るため、同乗者や歩行者などに脅威を与えない走りなどに対する正しい知識や運転技術の習得が欠かせない。それと同様に、以下の項目に対する考慮と対応が重要である。ここでは、大会運用そのものに関わることではなく、その前提と大会後に残すべきことを述べる。

1）事故前提の徹底

何処まで徹底して IT 活用を行うのかを決めること。それを基本にそれでも事故が起きることを前提に、起きたときに企業で負うべき責任と国で対応すべきことを決めておくことがまず第一である。次に、事件現場だけではなく事件を引き起こす組織、基盤、手口の監視や分析であるが、これは最近設立された JC3 や金融 ISAC が、既存の組織と連携して上手く機能することを切に願う。

2）残すべき遺産

利用する基盤は商用製品だけではない。OSS など誰でも無償で利用できるソフトウェアも重要なところで多数利用されているが、昨今大きな欠陥が発見され話題になっている。このようなソフトの特性を考え、競合企業同士も協力して、我が国で安全に利用できる品質の高い OSS へ積極的に寄与することにより世界に貢献することも考えられる。

また、社会へのセキュリティ啓発に関しては、全国レベルで活動している組織も多々存在するが、資金や人材確保の難しさ、縦割りの弊害などにより、狙い通りの効果を上げられているとは決して言えない状況である。一方、地域に根ざして活動している様々な組織も存在するが、こちらはさらに孤軍奮戦状態である。こういったことの打開のため、前述の Grafsec-J で、各団体への資金援助、情報共有や PR の場として機能すべく活動を開始したところである。

人材育成、品質の高い OSS の維持、各組織の活動など、必要な予算は、一般企業や社会の負担を軽減するためにも、国だけに頼るだけではなく、寄付等による基金で自立的に運用できる仕組みを構築することも重要と考える。

最後に、このような機会を頂戴できましたことに感謝すると共に、僭越ながらご提案を差し上げることで我が国発展の一助になれば幸甚です。ご清聴に感謝いたします。ありがとうございました。