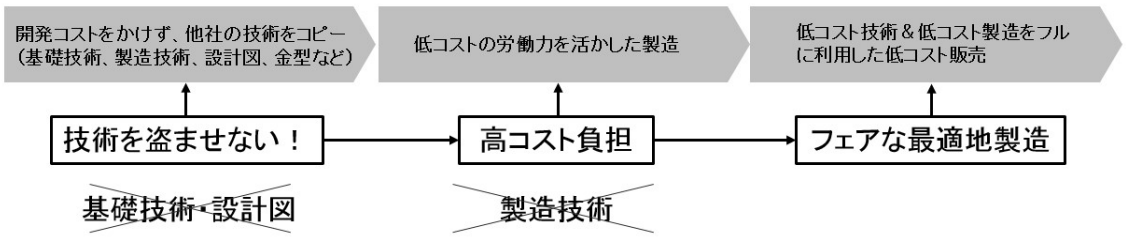
国家安全保障のための企業サイバーセキュリティ対策

― 情報セキュリティ研究所の現状認識、推奨する対策、活動予定について ―

情報セキュリティ研究所　所長　　中村宇利
情報セキュリティ研究所　副所長　武田俊孝

＜はじめに＞

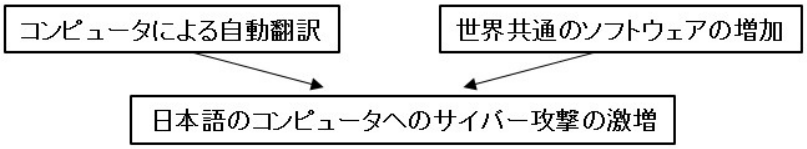
昨今、日本でもサイバー犯罪が報道されることが多くなり、事の重大さが認識されてきた。警察庁においてもサイバー対策を重視し、各都道府県警ではサイバー対策課を設けて対策にあたるなど、サイバー犯罪への対策が緊急課題となっている。サイバー犯罪とは、主にコンピュータネットワーク上で行われる犯罪の総称であり、ネットワーク上の不法取引やデータの大量配布による著作権侵害、法律に違反するデータの公開などを主として指すが、特に、産業情報の漏えいは、直接的に国力低下の原因につながる国家安全保障上の重要問題である。一つの工業製品を発売するため日本を含む先進国では、基礎研究から始まり、その応用研究、これらを利用した製品開発（設計図を含む）、製造技術開発（金型や製造ラインなど）に膨大な費用をかけている。これらの費用は、原則としてすべて新製品の付加価値を構成し、最終製品の発売にあたっては、その製品本来の製造コストに加えて、この研究開発に要するコストを上乗せして、新製品の価格が決定されている。そして従来はこの新製品が有する新規性、独自性、利便性ゆえに、類似の従来製品と比較して高価格であっても価格競争力を維持してきた。ところが近年、新製品と同じ付加価値を持つほぼ同等の製品が、発売日までほぼ同じ日に市場に出てくるという不可解な事態が発生するようになっている。そのため我が国の製造業者は、研究開発にかけた膨大なコストを乗せた分だけ価格が高い新製品を市場に供給することを余儀なくされ、いつの間にか日本の経済力は、世界第二位の地位までも奪われるに至ってしまった。その結果、①競争力の低下とシェアの縮小、②技術力が高価格につながらないことによる研究開発費の圧縮、③日本人技術者の減少および技術力の低下、と負の連鎖さえ見られる。



「世界の工場」と称される国々と比べても、日本のほうが製造効率は数倍高いので、製造コストについて日本の競争力が勝っているケースは少なくない。それに加えて、開発コストを適切に上乗せできるのであれば、日本の競争力は以前よりも高くなり得ると言っても良い。しかし、そこでは産業情報の漏えいを防止する情報セキュリティ対策が不可欠である。

このため、情報セキュリティ対策に注力する日本企業は増加し、危機意識も高まってきて

いる。しかしながら、欧米諸国と比較しても、我が国の企業の対応はまだまだ不十分だと言わざるを得ない。これには、セキュリティ・リスクに関する考えが不十分であったこともあるが、次のような事情も見逃せない。
日本国内の多くのコンピュータ環境は日本語であるため、数年前までは海外からのサイバー攻撃を受けることが少なかった。ところが、コンピュータによる自動翻訳が容易になり、また世界共通のソフトウエアも増えたので、日本へのサイバー攻撃は飛躍的に増加してきた。また競合企業を標的とした業務妨害目的の単純な攻撃も急増している。



当情報セキュリティ研究所は、「情報セキュリティ対策は、最高度の技術的能力をもって、現段階の技術に関する冷徹かつ的確な判断のうえに構築するべきもの」との認識のもと、サイバー犯罪のパターンや技術的背景を踏まえた「現実的な答え」を提案したいと考えている。尚、所長の中村は情報セキュリティの根幹に関わる暗号技術を専門とし、副所長の武田はネットワークセキュリティの専門家として情報セキュリティの最前線で活動している。
本稿では、その概要を今後の活動予定とともに紹介する。

＜企業サイバーセキュリティ対策の現状＞
サイバーセキュリティの最新情報の多くは英語で発信されているため、迅速な対応には英語読解力が必須である。この面で、多くの日本企業の IT エンジニアは全く不十分である。大手企業の場合、セキュリティ専門会社と契約していることが多く、彼らから情報を得ることは可能だが、中小企業の場合そのような対応は難しい。大手企業であっても、すべてのセキュリティ対策をセキュリティベンダーに任せているわけではないため、どうしても対応の遅れが発生する。

日本企業の情報セキュリティの問題

・英語能力
・専門会社の活用不足
・利便性とセキュリティのトレードオフ
・最高度の技術と人材が必要
・セキュリティ投資の後回しが許されてしまう

また、セキュリティと利便性はトレードオフの関係にあるため、ユーザーへの利便性を優先してセキュリティを犠牲にしている企業は多い。さらに、セキュリティ対策は、IT エンジニアであれば誰でもできるというものではなく、最高度の専門知識、専門技術が必要であり、コストもかかるため、未だに少なくない企業が必要性を認識しながらもセキュリティ対策への投資を後回しにしているのが現状である。
以前、武田が情報セキュリティ以外の事項に関して IT コンサルティングを行っていた大手企業で、海外からのハッキング攻撃による重大な事態が発覚したことがあった。被害は深刻

で、第三者に参照されてしまった（＝見られてしまった）データをログから特定したところ、その中には国家的安全保障に関わる重大な情報も含まれていた。企業内に対策チームが設けられ、武田もそのチームを手伝うことになった。ログから、アクセス元は日本の隣国と判明し、手口などから組織的ハッキングだったと推定された。そのハッカーたちはプロの集団と思われ、データを圧縮し、そのファイルを暗号化して複数のファイルに分割し外部へ送信していた。だが、彼らが作成したフォルダは暗号化されていたため、外部へ送信されたデータに如何なる内容が含まれていたのかを確認することはできなかった。
この事案は、情報漏えいの規模や参照されたデータの重大性からすると、企業の社会的責任の問題としても、株主に対する説明責任の問題としても、国家安全保障の問題としても、公表・説明すべきものであった。しかし、公表は見送られた。同社内外の関係者は、公表を避けたかったのだ。そのために用意された「理由付け」は、「盗まれた情報を特定できないので被害を特定できない。被害を特定できないのだから、被害を公表する必要はない。」ということであった※1。但し、警視庁へ被害届を提出し、関係官庁への報告も行った。
この事件の直後は、同社もコスト度外視でセキュリティ対策を強化するよう指示が出たが、時間の経過とともにコストの上限が設けられ、更に「完全な対策は不可能だ」との判断から、「事件が再発した場合の被害の最小化」と「経産省などへの『言い訳』ができるようにすること」の２つを目的とするセキュリティ投資へとシフトしていった。また、セキュリティ機器の選択は、セキュリティ性能よりもオペレーションの利便性が優先するようになっていった。
国内のほとんどの企業は同様の選択をすると推察できる。多くの企業人は、「情報セキュリティは、費用対効果が見えにくく、まだ起こっていないリスクを計量化し、想定損害額を算定した対策をとることは困難だ」と考えているからだ。そのため、経営層にその必要性を理解してもらうことは難しい。サイバー犯罪のニュースは増えているが、まだまだ対岸の火事だと思っている企業が多いのが実情である。

＜近未来のサイバーセキュリティ＞
最近、通常のインターネット使用に加えて、IoT（モノのインターネット）などのインターネットの応用が急拡大してきている。そのため IoT によってインターネットに繋がれた機器が不正使用されたり、他者への攻撃に使われたりする報告例が少しずつ増えてきた。自動運転やスマートグリッドも格好の標的になるであろう。一瞬の停電で打撃を受ける精密機械工場や、可燃物を扱う化学工場などは、サイバーテロの対象となり得るため緊急の対策が必要である。
さらに今後はサイバー犯罪に AI（人工知能）技術が使用されることが予想される。その場合、現在の SIEM※2（Security Information and Event Management）などを使用したアラートでの異常検知や Sandbox※3 サービスでの検証のようなやり方では、被害を未然に防いだり被害を最小限に食い止めたりすることが困難になることが予想される。もちろん防衛側でも AI 技術を使用する試みも出始めているが、今はまだ限定的であり広く普及するにはもう少し時間がかかるだろう。マルウエアによるとの恐れがある行動に対して AI が自発的に

対応するように設定した場合、企業の利便性を損なう可能性があり、制御・管理には大きな困難が伴うと考えられる。また、IoT による問題とは別に、Fintech（ファイナンステクノロジー）の進展が、ビットコイン、ブロックチェーンに関連する重大・深刻な問題を生じることは確実で、これにも対応が必要である。

＜推奨するセキュリティ対策＞

こうした状況を考えると、セキュリティ対策には万全な方法がないようにも思われるかも知れないが、以下に説明する通り、新規技術を含めた重層的手段による包括的な対策を行うことで十分防御は可能である。

そもそも、セキュリティは大別してネットワークセキュリティと情報秘匿の 2 つがある。多くの企業では、前者のみの対策に汲々としており、情報秘匿（情報漏えいがあった場合の対策）は実際の事件が起こるまで手をつけない。しかし、情報秘匿の欠如による実際の被害は顕在化していないだけで、前述のような事象を見れば少なくとも産業情報の漏えいが現実に発生していることは明らかであり、その損失は国力を損なうほどの膨大なものとなっているのである。

情報セキュリティ研究所では、これまでの国の方針であった事件後の対策ではなく、改めて安全保障の観点からこの情報秘匿に重点を置き、未然に事件を防ぐことを主眼とする 5 つの対策を推奨する。

① P2P（ピア・トゥー・ピア）の専用線による完全秘匿通信が可能であれば、これを行う
② 相手方が専用線に繋がっていないために、やむなく公衆線網につながなければならない場合には、専用線同等レベルの「一時的準専用線秘匿通信」を行う
③ 公衆線網は漏えいの可能性が高いので、常時監視し、情報漏えいルートや不正ソフトの検知、マルウエアが悪性である場合の即時駆除を行う
④ しかしながら、すべてを「ゼロ・デイ※4」に駆除できるわけではないので、マルウエアを起動させないシステムも併用する
⑤ 情報漏えいはその他の要因（人的、機械的）によって起きることがあるので、漏えいしても問題が発生しないように、当該情報を無害化（完全暗号化）しておく

これら 5 つの対策を日本のすべての企業に普及させるため、情報セキュリティ研究所では、説明冊子を作成し、ダイレクトメールやセミナーで啓蒙したいと考えている。また、希望企業には個別にコンサルティングも行っていく。

さらに、当研究所では、情報セキュリティの要素技術（暗号技術やサイバーセキュリティ技術など）やセキュリティ関連製品を独自に評価し、さらにそれらに暗号技術を加味することを予定している。

※1. これでは、「サイバー攻撃の被害を特定できない限り、公表しなくて良い」ということと同じであり、巧妙な攻撃、高度な技術による攻撃ほど、つまり解明しにくい攻撃による被害ほど、公表しなくてよいという結果になりかねない。今後、早急に、経済産業省、金融庁、証券取引所などを巻き込んだ形で、被害の公表を義務付ける制度的解決が必要である。

※2. SIEM（Security Information and Event Management）

ネットワーク機器、セキュリティ関連機器、及び各種アプリケーションなどに残されているログ情報に基づいて、異常を管理者に通知する管理方法。「セキュリティ情報およびイベント管理」「セキュリティ情報/イベント管理」などと翻訳されている。

※3. Sandbox

外部から受け取ったプログラムが、保護された領域内でしか動作しないようにすることによってシステムが不正に操作されるのを防ぐセキュリティ機構をいう。外部からのプログラムは、保護領域内では、ほかのプログラムやデータなどを操作できない状態にされて動作するため、当該外部プログラムが暴走したりウイルスを動作させようとしてもシステムに影響が及ばない。攻撃のできない安全な「砂場」(サンドボックス)という意味。

※4. ゼロ・デイ

ゼロデイ（Zero Day）は、脆弱性を解消する手段がない状態で脅威にさらされる状況をいう。 脆弱性が発見されて修正プログラムが提供される日（One day）より前にその脆弱性を攻略する攻撃は、ゼロデイ攻撃と呼ばれている。

(出典：Wikipedia　https://ja.wikipedia.org/wiki/ゼロデイ攻撃)