サイバーリスク対策の現状と今後の課題

奈良先端科学技術大学院大学　情報科学研究科 教授　門林（かどばやし）　雄基（ゆうき）

1. はじめに

本稿では、電子商取引やソーシャルメディア等での安心安全を維持していくために必要不可欠なサイバーセキュリティを取り扱う。なかでも、サイバーセキュリティを維持する上で必要な対策、つまりサイバーリスク対策の現状と今後の課題について総括的に解説を試みる。

2. サイバーリスク対策の現状

インターネットが商用化されてから20年以上が経ち、電子商取引や個人情報など国民の安心と財産の安全にかかわる様々な情報がオンラインでやりとりされるようになった。インターネットの高度な利活用が歴史的にも稀に見る経済統合と生産性向上、発展途上国と先進国の知的ギャップ解消などの社会価値をもたらした一方で、これに呼応して、情報漏洩や改ざんをはじめとする多様なサイバーリスクが増大していることは指摘を待たない。

サイバーリスクには様々な種類があり、特定の対策製品だけでリスクを網羅できることはまずない。その対策が抜け漏れなく、バランスのとれたものになっているか、我々はつねに確かめていく必要がある。ここでは本稿執筆時点でのサイバーリスク対策の偏りについて、問題意識を共有しておきたい。

2.1　パソコンに偏るサイバーリスク対策

サイバーセキュリティと言えば、ウイルス対策、フィッシング対策がただちに想起される読者も多いと思う。これらのサイバーリスク対策はパソコンのウイルス感染やネット詐欺被害といったリスクからIT資産を守るために必要だと考えられてきたが、今日、スマートフォンのみならず、プリンタ、無線アクセスポイント等、あらゆる機器が性能こそ劣るもののパソコンと同じ原理で動作するCPUとメモリ、OSを搭載して動作しており、サイバーリスクの発生源となっている。

またコンピュータウイルスやフィッシング詐欺は高度化の一途を辿っており、それらの検知が難しくなっていることも、サイバーリスク対策をパソコンに偏らせる原因となっている。最近ではウイルス対策ソフトの検知率が低くなったことから、一時期その実効性が疑問視されたことがあり、このことからエンドポイント対策、マルウェア対策といった新しい用語が使われることがある。このような最新の脅威動向と対策技術に多くの注目を集めた結果、サイバーリスク対策の偏りを生んでいるといえる。

サイバーリスク対策がパソコンに偏る理由は技術的側面のみならず、経済的側面にも要因がある。技術的には、パソコンはプリンタや無線アクセスポイント等と異なり、利用者による機能追加が容易であることが明白な理由として挙げられる。経済的には、対策ソフトの量販によりウイルス対策企業がビジネス的に成立した、という点が最も大きな理由であろう。

個々のパソコンへの対策ソフト導入に加え、ネットワーク全体を守るためにネットワーク型のファイアウォールや侵入検知システムの開発も進んでいる。しかしながら、これらのシステムの本格的導入は、実質的に大企業とサイバーリスクへの理解の進んだ一部のIT企業や研究組織に限られる。今日、中小企業やIT以外の業種においてサイバーリスク対策が大きく立ち遅れており、このことが国内外において問題視されている[1]。

2.2　予防策に偏るサイバーリスク対策

サイバーリスク対策の製品・サービスの多くは、水際で止めることを基本的なアプローチとしている。つまり、利用者には好きなソフト、好きなウェブサイトを使ってもらい、それらが悪性であることを判断した場合には水際でブロックする、というものである。

では真に悪性であるソフトが、悪性であることを判断できなかった場合にはどうなるか。この場合、社内ネットワークの奥深くまで入り込んでしまい、最悪の場合、企業の機密情報が外部に漏洩してしまうことも考えられる。

近年、大きな社会問題となっている「標的型サイバー攻撃」は、このように予防策に偏ったサイバーリスク対策の弱点を突いた攻撃である。標的型サイバー攻撃を受けた企業は、予防できなかった場合、社内ネットワークに潜伏するウイルスや不正アクセスの痕跡を同定する作業に莫大な時間的・金銭的コストを支払うことになる。フォレンジックという技術を用いて、ディスクやメモリに潜伏する特殊なウイルスや

その痕跡を探すのであるが、この作業は大量生産による経済効果が効かない、専門的かつ時間のかかる作業であり、またフォレンジック専門家の数も限られるため、非常にコストがかかる。

予防策のための製品・サービスも高価であるため、企業としては「そんなはずはない」「なぜ防げなかったのか」などと延々議論し、現状を認識するまでに時間がかかることも珍しくない。いわゆるエリートパニックである。しかし対策の遅れは被害を拡大させてしまうことにつながる。こうした問題への反省もあって、最近ではインシデントが起きることを前提としたインシデント対応組織（CSIRT：Computer Security Incident Response Team）を平時から立ち上げる企業が増えている。しかしCSIRTの体制を整備すれば万全というわけではない。サイバーリスク対策が完璧でないことを前提として、残存リスクに対処するためのリソースを確保している企業は多くないのではないか。残存リスクがあることを認め、事後対応のための予算を計上してはじめて、バランスのとれたサイバーリスク対策が可能になると私は考える。

3. サイバーリスクの現状

前章ではサイバーリスク対策を抜け漏れなく、バランス良く実施することの重要性に触れた。ではサイバーリスクは、これまでの対策の網の目をくぐり抜けて、どのように多様化しているのであろうか。

3.1　パソコンから、パソコン以外へ

前章で、サイバーリスク対策がパソコンに偏っていることを述べた。しかしパソコン以外の機器でも、様々なサイバーリスクが発生している。

近年、ルータやVPN機器にもバックドアや脆弱性が複数報告されている。バックドアとは、通常、製造者のみが知る秘密の抜け穴であり、メンテナンスやデバッグのために設けられたと考えられている。近年、ルータやVPN機器の解析技術が進展し、このような製造者以外は知り得ないような抜け穴も発見が進んでいる。またルータもパソコン同様にCPUを搭載し、メモリ上でOSが動いているため、ソフトウェアに脆弱性があれば管理者権限を乗っ取られることもあり得る。またルータ単体では攻撃を検知し自己を防護する機能を持たないため、サイバーリスクの現状把握も十分ではない。

海外では、事業者が加入者に提供したブロードバンドルータを大量に乗っ取られ、DNS設定を書き換えられ、大手サイトへアクセスしたつもりが悪性サイトに誘導されるといった事案が複数起きている[2]。

同様にプリンタ、ウェブカメラ、スマートテレビなどの民生用デジタル機器でも数多くの脆弱性やバックドアが発見、報告されている。国内でも文書スキャン機能を備えた複合機がネットワーク経由で不正アクセスされるなどの事案が発生している。ウェブカメラが大量に乗っ取られてボットネットとなった事案については国内でも数多く報道されたので、覚えている読者も多いだろう。

このほか、いわゆる制御用のマイコンもサイバーリスクの発生源となっている。スマートフォンの無線通信チップの脆弱性や、クラウド等で使われているサーバの管理モジュールの脆弱性などが、これまでに問題となっている[3]。これらの通信チップや管理モジュールに使われているマイコンは非力ではあるが、スマートフォンやサーバのCPUとは独立して動作し、通常、ウイルス対策ソフト等も監視しない部分であるので、サイバーリスクの現状把握が難しい。

また、ネットワークから隔離することを前提として設計された制御システムも実際のところ数多くインターネットに接続され、工場やプラントの安全運転にとって重大な脅威となっている。インターネットに不用意に接続された制御システムを容易に探すための検索サービスも登場し、注目を集めている。現在、産業用IoT機器の開発が活発に進められており、この懸念は当面の間、後退することはなさそうである。

3.2　ソフトウェアだけでない脆弱性

サイバーリスクの代表的な原因として、ソフトウェア脆弱性を想起する読者は多いのではないだろうか。ソフトウェア脆弱性は入力値のチェック漏れや計算ミスなど、プログラマの考え漏れ、怠惰などによりソフトウェア作成時に入り込む脆弱性で、その種類が数百にも及び、また機構的に精密であることからエンジニアの関心を集めやすい。

しかし近年、IoTやクラウドの浸透により、ソフトウェア以外の脆弱性が大きな事案に発展することが増えている。ここではソフトウェア以外の脆弱性について、その種類とリスクの具体化例を簡単に紹介する。

まずプロトコル脆弱性について述べる。プロトコル脆弱性は通信プロトコルにおいて、パケットの再送による攻撃（リプレイ攻撃）、送受信者になりすまして偽情報等を挿入する攻撃（中間者攻撃）、大量のパケット等により応答不能とする攻撃（サービス妨害攻撃）などを成立させてしまう、プロトコル設計上の欠陥である。理想的には、プロトコル脆弱

性を発生させないために、プロトコルの形式仕様記述をプロトコル検証系を用いて検証することが望ましいが、インターネットで日常的に用いられているプロトコルや制御システムのプロトコルでは、設計上の欠陥を含むものが多く用いられている。また標準プロトコルに設計上の欠陥が見つかった場合、その修正には数年単位での標準化作業を伴うことが多く、プロトコル脆弱性への対応はソフトウェア脆弱性と比べて遅くなる。このため現実的には、プロトコル脆弱性を所与のものとしてシステムを運用し、プロトコル脆弱性への攻撃が発生した場合にただちに対処する、といった運用での対策がとられる場合も多い。

クラウド時代に入り重要性を増しているのが、設定の脆弱性である。設定の脆弱性とは、Webサーバなど高機能なソフトウェアの設定を誤り、サービス停止や情報漏洩などのリスクを発現させてしまう脆弱性のことである。ソフトウェアの脆弱性がプログラマによって作り込まれるのに対し、設定の脆弱性はシステムエンジニアによって作り込まれる。例えばWebサーバにおける情報公開の範囲を間違えると、ただちに情報漏洩につながる。近年ではクラウド上でのデータベースの設定を間違えて、一国の有権者情報すべてが漏洩するといった事案が発生している[4]。

またクラウドではハードウェア脆弱性も注目を集めている。最近話題となった、インテル等のCPUを対象としたメルトダウン攻撃は、ハードウェア脆弱性を突いたものである[5]。ハードウェア脆弱性も、種類によってはサービス停止や情報漏洩などのリスクを発現させてしまう恐れがあり、特にクラウドでは隣のテナントからの攻撃や、隣のテナントが被害にあった場合の二次被害につながる恐れがあることから注目を集めている。ハードウェア脆弱性は、問題となる事象によってはソフトウェアによる対策も可能であるが、抜本的対策のためにはハードウェアの交換が必要となるため、プロトコル脆弱性とならんで数年単位での息の長い対策が必要となる。

最後に人間の脆弱性について述べておきたい。サイバーセキュリティは、様々な機器とそれらを使う人間の相互作用により達成されているため、人間の判断ミス、伝達ミス、誤解、及びそれらの遠因となる過労、睡眠不足などは時として致命的な影響を及ぼす。フィッシング被害は人間の判断ミスにより引き起こされるが、このほかにも、様々な局面で人間の脆弱性が問題となる。この問題に対しては、意識啓発、社内研修、サイバー演習など様々な工夫が試みられている。なお、不眠不休の復旧努力が美徳のように称えられる組織では、判断ミスを引き起こす根本原因であるリソース不足、過労、睡眠不足などの問題は見過ごされがちであるので注意が必要である。

4. サイバーリスク対策における今後の課題

数年前にパソコンのOSに本格的なセキュリティ機能が取り入れられたときに「これで一安心」と思ったのも束の間、前章でみてきたように、サイバーリスクは近年ますます多様化している。このような近年のサイバーリスクの進展を踏まえ、様々な取組みが進んでいるが、ここでは攻防戦を俯瞰した上での私なりの問題意識を共有しておきたい。

4.1 攻撃の自動化に遅れをとる対策の自動化

米国では脆弱性の自動発見システムに大規模な懸賞金が設定され、全米の有力大学チームや研究機関がその開発にしのぎを削っている。その副産物として、脆弱性を発見する技術が長足の進歩を遂げている。また、脆弱なIoT機器を検索するサービスを活用し、自動的にハッキングを試みるシステムも開発されている。つまり、サイバー攻撃の自動化はほぼ目前どころか、「すでに起きた未来」という状況である。

このような状況で、対策の自動化は大きく遅れをとっている。自動防御システムが今すぐ必要な状況であるが、いまのところ対策チーム間での情報交換を自動化するとか、社内ネットワークでの痕跡調査を自動化するといったレベルにとどまっており、本格的な対策の自動化までは程遠い状況のように思える。

このような対策の自動化を実現する上で、おそらく救世主のように思われているのが人工知能である。より正確には、パターン認識、つまり今日の学術用語でいうところの機械学習に大きな期待が寄せられている。今や理論的詳細を気にもかけない経営層までもがディープラーニングで何かやれ、という時代である。

サイバーセキュリティの領域で人工知能の活用が待ったなしであることには疑問の余地はない。しかしながら、その解決策が画像認識や音声認識で高精度をうたうディープラーニングの延長線上にあるかというと甚だ疑問である[6]。画像認識の領域では、人間が得意とするパターン認識を一所懸命機械がまねることで問題は解決する。しかし、サイバーセキュリティの領域では、そもそも人間が不得手なロジックの等価変換や例外処理記号の羅列をうまく扱わねばならない。このような問題に、人間の認知機能を真似ることを意図した機械学習アルゴリズムをそのままあてはめて

も、うまく機能しない（例えば、簡単な等価変換で検知をすり抜けることができてしまう）ため注意が必要である。

サイバーセキュリティの領域では、単純なパターン認識のような「子供の人工知能」にも活用の余地がないわけではないが、抜本的な対策自動化のためには、精密な知識とロジックを扱う「大人の人工知能」が求められる。知識を機械可読な形で表現し（知識ベース）、概念の関係を構造化し（オントロジ）、知識ベースの矛盾を見つけ、また誤った知識をノイズとして除去する、といった気が遠くなるような作業を積み重ねることが求められる。

4.2　人間系における対策

効果的なサイバーリスク対策のためには、現場と経営層が正確な状況認識を共有し、迅速かつ適切な意思決定を行うことが望ましい。このような状況認識（Situation Awareness）と意思決定の科学（Decision Science）に関する研究者と実務者のコミュニティは海外には存在するが、日本国内においてサイバーリスクに関する状況認識を支援しようという試みは少ない。サイバーリスクに関する状況認識を関係者で共有するために、可視化はきわめて有効な手段であるが、日本では非専門家に対するデモンストレーションとして捉えられることが多い。今後、リスク可視化に対するより多様なアプローチと、その有効性に関する科学的評価が求められることになろう。

またサイバーリスクに対する判断ミスは、組織にとって致命傷となる可能性があるため、経営層と現場が正しい判断を導き出すための思考のツールキットや、机上演習などのトレーニング、過去の失敗事例をケーススタディ化した資料などの充実が求められる。

4.3　法制度対応

サイバーリスクの深刻化を重くみて、欧州では重要インフラ事業者に対する事案の報告義務[7]や、欧州市民の個人情報漏洩に対する懲罰的な罰金制度[8]が近年設けられている。特に個人情報保護はクロスボーダー規制となっており、日本国内の事業者であっても欧州市民の個人情報を預かる限りにおいては同規制の対象となる。このような規制への対応が遅れた場合、サイバーリスクが事業リスクに直結することが懸念される。

4.4　人材育成における課題

サイバーリスク対策においては人材不足が深刻であり、産業界の要請から、若年層のセキュリティ技術者を大量養成する取組みが行われている。しかしサイバーセキュリティは、ソフトウェア脆弱性の種類だけでも数百あり、また脆弱性データベースも30年の歴史を持つ業界であり、その知識の膨大さと業務の責任に圧倒され、キャリアを途中で諦めてしまう可能性もある。若年層に間口を広げ、層を厚くすることは歓迎すべきことであるが、セキュリティ技術を中途半端に身につけてサイバー犯罪に手を染めるような若者を増やしてはならない。現に、そのような事例が少数とはいえ国内外で起きていることは憂慮すべき事態である。

当たり前のことではあるが、セキュリティ技術者の人材育成では、心身ともに健康な者のみを見極め選抜する必要がある。また、継続的にスキルアップし、セキュリティ専門家として大成できるよう、インセンティブ、キャリアパスについてもそれぞれの現場で制度設計していく必要がある。

5. おわりに

サイバーセキュリティの維持は世界共通の目標であり、「情報通信技術の利活用における安心安全の醸成」として2005年の世界情報社会サミットの行動指針C5にも定められている。その実現と向上のためには、構成員ひとりひとりが主体性をもってサイバーリスクと対峙し、バランスのとれた対策を様々なレベルで実践していく必要がある。本稿がその一助となれば幸いである。

参考文献

[1] 独立行政法人情報処理推進機構、「2016年度 中小企業における情報セキュリティ対策に関する実態調査」報告書、2017年3月

[2] Ars Technica, “DSL modem hack used to infect millions with banking fraud malware”, October 2, 2012.

[3] The Register, “Intel Management Engine pwned by buffer overflow”, December 6, 2017.

[4] The Register, “ ‘No password’ database error exposes info on 93 million Mexican voters”, April 25, 2016.

[5] Moritz Lipp et al., “Meltdown”, https://arxiv.org/abs/1801.01207

[6] David L. Parnas, “The Real Risks of Artificial Intelligence”, Communications of the ACM, 60 (10), October 2017.

[7] European Union, “The Directive on security of network and information systems”, DIRECTIVE (EU)2016/1148, July 6, 2016.

[8] European Union, “The EU General Data Protection Regulation”, https://www.eugdpr.org