「データから人へ」, 2030年を見据えたサイバーセキュリティ

“Data to Human”, cyber security looking towards 2030

大阪大学教授 CISO　猪俣 敦夫
Atsuo Inomata, Professor CISO, The University of Osaka
ORCID ID : https://orcid.org/0000-0002-7723-6471

1. ハッカーという誤解

サイバー攻撃と言うと，よく映画やドラマに出てくるようなうす暗い部屋で黙々と PC を叩き続けているという場面が頭に浮かんだ方もいらっしゃるのではないだろうか．ここでいうサイバー攻撃をする人のことをハッカーなどと呼ばれることも多いが，ハッカーとは本来コンピュータやプログラムなどに精通した人を指す言葉であり，決してコンピュータ世界での悪い人を指す総称ではない．正しく言うと攻撃者のことをクラッカーと呼んだりするのだが，日本ではクラッカーといえばパーティの時に鳴らすものと，あるいは食べるものなどとして使われることも多く，悪い攻撃者の意味ではほとんど使われていない．そこで，こうした攻撃者の事は悪いハッカーと呼ぶことにする．さらに，セキュリティのインシデントは悪いハッカーたちによる攻撃だけではない．うっかりミスなど人的要因，内部犯行や不適切な監査といった組織的要因，そしてソフトウェアのバグやハードウェアの脆弱性などの技術的要因，といった 3 領域にまたがるいわゆる学際的とも言われる所以でもある．

空き巣や窃盗などの事件では例えば金品が盗まれるといった，見える，触れる，ことができる「モノ」が対象であることが一般的であり，モノが盗まれたことはしばらくの間は悲しい気分になるかもしれないが，これは時間が少しずつ解決してくれることが多い．しかし今はセキュリティにおいてもデータについて考えてみる時代である．サイバー攻撃では見える，触れる，ことができない「データ」が対象となることが多く，今や「モノ」以上に「データ」が盗まれる時代にいる．では，何故「モノ」ではない「データ」が盗まれることが脅威となりうるのであろうか．例えるなら，お金が盗まれたとしてもそれは大小その損失はあるが一時的に影響を及ぼす脅威である一方，データが窃取された場合，元の何も無かった状態に戻すことは絶対できない．これはたとえデータを取り戻せたとしてもインターネットのどこかで複製されているかもしれない，さらにはインターネットから完全に削除できたかどうかを確認することはほぼ不可能だからである．このことから，データの窃取は情報漏洩などを含めて考えられうる脅威から一生逃れることはできない．これは機密性ないし完全性からの観点であるが，同様に事業継続性などからも可用性からも今は考えておく必要がある．最近のランサムウェア攻撃事案においては，悪いハッカーらによってデータの暗号化が実行され，最終的にその暗号化されて読み出し不能となったデータとの引き換えに彼らから復号のための鍵を得られなければ元のデータに復元することはほぼ不可能である．もちろん，お金を支払ったとしても復号のための鍵が得られる保証も一切ない．組織としてどのように対応するかは非常に難しい問題である．

2. サイバー攻撃の目的

この数年において報告されている企業などに対して行われたサイバー攻撃の目的はほとんどが「金」目当てである．一方，ウクライナ侵攻やイスラエルとパレスチナの問題をはじめ，確かに現実的な戦争という人類にとって深刻な大きな問題が発生している中でサイバー攻撃の目的とリンクしたような話をよく見かける．しかし，そうした話の根拠も実際ほとんど存在していない．攻撃者たちの視点からすれば自分たちが捕まらないようにいかにして楽に金銭を奪い取るか，それだけの話である．単に彼らは脆弱なネットワークやシステムをインターネット中から常に探索し続けており，偶然にも見つかってしまったサイトやサーバを狙う方が彼らにとって効率良いことであるのは自明である．

3. 人を介した攻撃への変化

最近では個人情報漏洩を引き越しかねない不正アクセスなどの事案よりも，脆弱なネットワーク機器，例えば VPN 装置などを経由して侵入してのランサムウェア被害や，OS の警告メッセージを似せた表示などによるテクニカルサポート詐欺のように人の単純なミスなどによって起きてしまった，などである．これは，サイバー

攻撃そのものが明らかに何らか「人」を介した手段に変化してきているとも言えるだろう．すなわち，セキュリティといえば「防御」と言っていた時代の終わりの 1 つとも言えるのではないだろうか．もはや，外部すなわちインターネットとの接点となる出入り口をずっと眺め続ける教科書通りの境界防御だけでなく，悪いハッカーたちが何を狙いとして攻撃をしているのかといった攻撃者視点でのオフェンシブなセキュリティを意識する時代に入っていると考えられる．もちろん，オフェンシブセキュリティを推し進めるべきとはいっても攻撃者を育成すべき，ではない．より正しく言うならば攻撃者の視点で防御を考えられる人を育成すべき，ということである．

4. 脆弱性の要因としてのITガバナンスの欠落

ところで，昨今の事案における特徴として先に述べた VPN（Virtual Private Network）と呼ばれるインターネットから内部ネットワークやシステムへのトンネリングを構築する手法の脆弱性を悪用されることも多く，VPN は脆弱性を作り出す温床になっているのではないかとも言われるようになった．しかし，これは大きな間違いである．

VPN に限らずいずれのサービスや機能にも後に脆弱性が発見されることは多々あり，重要なことは組織において適切な運用・管理によってその脆弱性への修正対応がなされているかどうかである．これは，セキュリティの技術的問題では一切ない．例えば，IT 部門を外部に委託している組織においてはどうしてもそうした機器の脆弱性管理などへの意識は薄くなりがちであることから，ランサムウェア事案のほとんどがこの問題に起因したものである．まさにこれが IT ガバナンスの欠落である．

ガバナンスとは，組織が目的を達成し，継続的に維持，そして成長していくために意思決定を行う体制を整え，すなわち組織活動をコントロール（制御）するための統治行動のことである．その中での IT ガバナンスとは，組織において自身の IT システムへの投資によりそのリスク軽減の効果を最大限にする仕組みである．どうしても組織におけるサイバーセキュリティ投資というと技術的側面に注目しがちであるが，実のところ管理・運用などのマネジメント面，すなわち「ヒト」に依存する，これがセキュリティの根幹であることを忘れてはならない．

5. 社会システムの下支えとなるセキュリティの今後

今までサイバー攻撃といえば，そのターゲットは高々データに過ぎなかった，もちろん高々と言っても要配慮個人情報など非常に秘匿性の高いデータなど様々あり，こうしたデータ流出に対する脅威は社会の混乱を招きかねない影響は計り知れないものであろう．しかし，その脅威がついに「ヒト」の生命に直結する事態に移り進んだ，それが医療機関に対するサイバー攻撃である．医療機関では，医療事務のみならず診察，検査の効率化から電子カルテや医療機器などのシステムを接続する院内ネットワーク化が急速に進み，医療情報と呼ばれる「データ」のやり取りが一般的になった．これは，言いかえると院内システムが動作しなくなる，ということは診療行為そのものが出来なくなる，すなわち「ヒト」の生命に直結する事態を招きかねない，ことを意味する．

著者は，2022 年 10 月末に発生した大阪急性期・総合医療センターで発生したランサムウェアによるインシデント調査委員会の委員長を拝命した．当病院は 800 床以上を持つ大規模な総合病院でありその機能が約 2 ヶ月もの間，患者の治療に多大なる影響を及ぼすような診療制限をせざるを得なくなったのである．この本当の脅威は，患者の目の前に医者がいても何も出来ないことにある．さらには，このちょうど 1 年前に徳島県半田病院で発生した事案に対する調査報告書が公開されていたにも関わらず，である．医療機関といえども施設規模も多種多様であり，院内システムを構成するシステムやネットワークも一概に同様とはいえず，その対応の仕方はそれなりの専門的知識を持つ人材がいなければ難しい，そして何よりも医療機関は IT を主とする組織ではなく，人の生命，健康を守る機関であることからその専門的人材の確保が難しいという現実がある．

これはあくまでも医療の話ではあるが，今やサイバーセキュリティはいずれの業界においても切っても切り離せないものであり，その維持やリソース確保にあたり平時から検討しておく必要があるだろう．ISO/IEC27001 情報セキュリティマネジメントシステム（ISMS）における要求事項でも規定されているが，その確保にはリーダーシップ及びコミットメントが必要であり，すなわちトップマネジメント（組織の代表）は積極的に ISMS に関わらなければならないとされている．ISMS は企業組織などが取得するものと思われがちであるが，静岡大学をはじめ取得する学術機関も徐々に増えつつあることからも，学生，教職員を中心とした組織こ

そのセキュリティの確保が今後なお一層求められるようになる．2030 年を見据えるならば，今が「人」のセキュリティに意識を変えていく絶好の時であろう．

2024 年 12 月 23 日

【著者略歴】

猪俣 敦夫

大阪大学 D3 センター教授，CISO，2008 年奈良先端科学技術大学院大学准教授，2016 年東京電機大学教授，2019 年より現職，一般社団法人公衆無線 LAN 認証管理機構代表理事，一般社団法人 JPCERT/CC 理事，一般社団法人大学 ICT 推進協議会理事，一般社団法人ライフデータイニシアティブ理事，大阪府警察・奈良県警察サイバーセキュリティアドバイザ，他省庁・自治体セキュリティ委員多数，2022 年情報セキュリティ文化賞，2024 年サイバーセキュリティに関する総務大臣奨励賞，サイバーセキュリティに関する教育・研究の傍ら若手育成に取り組む．