Questions 5月1日(水)

1. 生成AIの出現によってセキュリティはどのように変わっていくのでしょうか
   ➔ システムのデジタルツインをLLM で作成するなどの取り組みがありますね。 どこに、穴があるのか？　どういう経路で 侵入可能なのか？　などを、デジタル機器の config ファイルの情報を集めて 学習させるなど。
2. 通信の機密性に対する考え方は、情報社会にとって切り離せない非常に重要な考え方だと感じました。暗号技術が安全ではなく安心を与えるための技術という考えは自分にとっては新しく、この目的を勘違いするとのびのび働くなどの要件を満たせない、かえって不十分なテクノロジーになってしまうリスクもある難しい技術であることが分かりました。
   ➔ 大事なのは、本来の目的を忘れない&立ち戻る 習慣を持つことですか。
3. 自分はオープンソース至上主義に同意しました。
4. セキュリティは単に安全性を担保するようなものと考えていたが、顧客が自ら安全やリスクについて理解し安心できるように働きかけるためのものであると分かり、思いの外深い意味合いがあると感じた。

5. プライバシーについて、個人的には、悪いことをしなければ、例えば国などの権力に生活の全てをデジタル上で把握されても構わないと思っています（もちろん悪用されない対策が必要ではあると思います）。個人の情報を管理されることによって、犯罪が減少したり、生活がより便利になるのではないかと考えているからです。

しかしながら、マイナンバーカードへの反対などの動きをみても、こういった、権力が個人の情報を持つことに対する抵抗はかなり大きいように思います。日本では、戦時の言論統制の反省などから、権力が個人の情報にアクセスできるようになることに抵抗が大きいと聞いたことがありますし、もちろん、自分も100%人に知られても大丈夫なことしかしてないかと聞かれると返答には困ります。ただ、中国ではインターネットを含めほとんどの情報は全て監視されており、それが便利だと感じる人もいると聞きました。どういった要因でそれが受け入れられているのでしょうか。

➔ 多くの人は、単純に 物事を捉えるからでしょう。ずる賢い人は、Dark-Sideを隠しながら、Brighter-Sideのみを魅せて、悪だくみを仕込みます(歴史の事実)

6. 今動いているならそのままでいいという保守的な姿勢ではサイバーセキュリティの観点ではよくないことが分かった.

近年，AIの発展に伴い，AIを用いた攻撃や逆にAIを用いた防御が行われ始めているが，いつどこでサイバー攻撃にあうかわからないため，保守的になりがちな日本の企業も，これまでの受動的な対策だけでなくアクティブ・サイバー・ディフェンスを取り入れたり，最新の動向をチェックしてそれに応じた対策を行っていくべきだと感じた．また，サイバーセキュリティ方面での改善を図るにあたり，まだ日本ではサイバーセキュリティ分野に詳しい人材がそれほど多くないので，企業としても今後はそういった人材をもっと重宝して，人材不足を解消するべきだと思った.

➔ Active Cyber Defense は、悪い相手に対して ①事前、②事後 で、＜攻撃可能＞ と 言っている人・組織が 存在します。しかし、Active Cyber Defense は、Re-active(発生への対処)だけではなく、＜Pro-activeな対処＞を行うことを意味しています。 ＜攻撃はしない＞です。攻撃できないように 対処するなのです。 隠れる(見えないようにする)。＜戦争しない＝戦わずして勝つ＞のが、一番の戦争上手(兵法の基本 by 孫子)

Active Cyber Defense (ACD), also known as adaptive security, is a rapidly emerging branch of cybersecurity. It integrates and enhances several cyber intelligence, cyber protection, and cyber analytics technologies to proactively and predictively combat cyber attacks and protect data assets. Rather than passively waiting for cyber attacks to occur, ACD takes an active and proactive approach. Here are some key points about Active Cyber Defense:

- Proactive Defense: ACD focuses on actively defending against cyber threats rather than merely reacting to them. It aims to prevent attacks before they happen by collecting information about potential threats in advance and enhancing defense capabilities.
- Threat Intelligence: ACD involves gathering intelligence about cyber threats, including attack patterns, tactics, techniques, and procedures (TTPs). By understanding the methods used by attackers, organizations can better prepare their defenses.
- Preemptive Measures: ACD includes monitoring network traffic during normal operations to detect early signs of cyber attacks. If suspicious activity is detected, organizations can take preemptive measures to neutralize threats or even launch countermeasures.
- Government Initiatives: Countries like the United States and the United Kingdom have been actively working on ACD initiatives. Government expert panels have emphasized the need to strengthen defensive capabilities through ACD.
- In summary, Active Cyber Defense aims to thwart attackers' objectives by actively and proactively defending against cyber threats. It's a crucial strategy in today's rapidly evolving threat landscape

7. 「安全」と「安心」の違いのお話が特に興味深いと感じました。ある程度勉強や研究を進め「有識者」になると「安全」ばかりに目を向けてしまいがちな一方で、世間に多くいる「非有識者」からすればわかりやすい「安心」が最も重要なのであり、その使い分けが情報技術のみに限らず専門的な工学技術を世間に広める上で肝要なのではないかと考えました。「安全」なき「安心」は虚構ですが、「安心」なき「安全」は人々に支持され得ないでしょう。工学技術を社会に貢献しうるものにするためにこの二つは表裏一体でありどちらも欠かせないものなのだと考えます。だが一方で「安全」を高めすぎると利便性等が損なわれるリスクがあるし、「安心」を高めすぎると人々の依存・固執・思考停止を招く恐れがあります。いずれもかなり難しい問題だなと感じました。
8. 著作権のところで、公開して発展させていくべきというのは納得できる一方で、著作権を申請していなかったり、あるいは少し手を加えられたりして著作権をとられてしまったという話を聞いたことがあった。それに対してはどのように規制すればいいのか、境界が曖昧なため主観的になってしまいそうで難しいと感じた。

9. 情報セキュリティーがどうあるべきかで触れられていた過度な規制がかえって悪影響を及ぼすというのは確かになと思いました。この点で、日本が他国に比べて発明等が劣っているというのも納得しました。少しずつ自由が尊重される社会になればいいなと思います。

10. まだインシデントが発生していないからセキュリティに関するアップデートをしないという保守的な考え方に少し賛同してしまう自分がいるが、やはりまだ発生していないとしてもこれから先も発生しないという証明ではないのでセキュリティに関するアップデートは必要だと思った。例えばスマートフォンのソフトウェアアップデートをすると動作性が変わってしまい使いづらくなってしまうような実体験もあり、現在特に困っていることがなければ変えたくないという気持ちはやはり少し納得できるような気がする。

11. セキュリティー対策は必要だが、過度の規制は逆効果になる可能性があり、例えば違法薬物を厳しく取り締まるよりも病気として治療支援する方が良い結果につながるケースもあり、闇市が作られてしまうのは規制の副作用として解釈することができる。どうしても万人をカバーすることができる方策というのはとれないと思うので、人々の安心のために規制をどう作るかというのは正解がないと感じた。

12.セキュリティー対策は必要だが、過度の規制は逆効果になる可能性があり、例えば違法薬物を厳しく取り締まるよりも病気として治療支援する方が良い結果につながるケースもあり、闇市が作られてしまうのは規制の副作用として解釈することができる。どうしても万人をカバーすることができる方策というのはとれないと思うので、人々の安心のために規制をどう作るかというのは正解がないと感じた。

13.セキュリティでは、全てのリスクにおいて規制しようとするよりも、ある程度は個人に任せ、起こりうるリスクを事前に考えて対策しておくのが大事という話に関して、校則が緩い高校の方が成績が良い（規制が少ない方が利益が多い）という話と通じるところがあるなと感じた。もっと言えば、パンデミックの抑制のためには、発生国を隔離し逃避しようとするのではなく、各国が支援、情報共有していく必要があるという話とも似ていると感じた。

14.便利さと安全さはトレードオフなので良いバランスを見つけることが重要だが、日本社会では安心と安全が混同されがちであるため、安全さに重きが置かれがちになり、社会の発展を妨げてしまうという点について、大変納得した。社会の風潮は急に変えられるものでは無いので、地道にやっていくしか無いのだろうとも感じた

15.セキュリティに関する考え方が技術者倫理と類似している部分が多くあって驚いた。

例えば、セキュリティ上のリスクに対して事前予防と事後予防の両方を行わなければならないという原則と類似したものが技術者倫理にも存在する。セキュリティは基本的思想が安全工学や技術倫理に立脚している(と少なくとも思われる)ので、このような類似性があるのだろうか。

セキュリティに関して今はまだ大丈夫という後ろ向きの考え方の企業が多いと思う。経営学の本や講義をざっと見てみたところ、リスクに関する話が少ないように見えた。サンプル数が少ないので、ずれた指摘になるかもしれないが、経営学でリスクマネジメントを教えることが安全管理、セキュリティ対策に一番効果的ななのではないかと思った。

16. 安心と安全という言葉の違いからセキュリティはどうあるべきかを考えるお話で、ユーザが安心できる環境を提供出来ることが大切だということを理解し目からウロコでした。

    安心というものが主観的なものであるからこそ、最低限の安心を確実に提供するには、ユーザに、起こりうるインシデントについて予めよく説明することが大切なのだと考えました。

    さらに、ユーザの側も、システムに完全性を求めない姿勢が要求されるとも思います。

    例えば処理水の排水の問題など、「絶対に安全と言い切れるのか」の観点からいろいろな議論や批判が飛び交いましたが、専門家がリスク説明を十分に果たした上で、住民もそれを理解して起こりうるインシデントを把握するリテラシーが必要だと考えます（どうしても全員に理解してもらうことは不可能だとは思いますが……）。