Question 5月13日 分

1. 大きな数の因数分解をごく簡単に行うような数学的発見がない限りは今後長く使われ続けるのでしょうか。
2. Active Cyber Defenseを国家が行うと、監視社会化する危険はないのですか。
   ➔ 国家が 何を 行うのか に よりますね。
   ➔ 何にでも、いくつかの異なる出口(明暗)がありますね。 明しか見せずに、暗を実現するのが、ビジネスの常識でもあるよね。。。。
3. デジタルセキュリティでは、現実の機械の安全保障に比べて、問題があっても発見しづらそうに思えます。工場で安全に不備があったら目に見える形(例えば、異音など)で分かりそうですがデジタルではそういうのがあまりなさそうですよね。 ➔ 見える化を行えばいいでしょう。
4. 量子コンピュータはRSA暗号にどのような影響を与えますか？
5. 現代ではプライバシーよりセキュリティの方が重視されてきているように感じますが、これからの未来ではセキュリティとプライバシーのバランスはどうなっていくと考えますか？

➔重視した時の 出口が いろいろあることを 網羅的に 捉えることができるか？

➔リスク・アセスメント

6. セキュリティを管理する独裁者のようなものがいた場合、一見徹底的な対策により安全性の面では効果的なように見えるが、逆に言えばこの独裁者さえどうにかしてしまえば容易にセキュリティを突破どころかシステムを乗っ取れてしまうので、責任の分散もある程度重要なことだと、ゼロ・トラストの話を聞いて感じた。 **➔ はい。上手な詐欺師ですね。**
7. なぜ「ブサイクな人が接するとセクハラになるのにイケメンな人が接するとセクハラにならないのか」という問題は，人間のもつ5感の中でも，視覚情報の占める割合が70%くらいあるからだろうと思います．私（男)ならもし，道端であるいていて，誰がが倒れて苦しそうにしている状況を発見した時，男性なら声掛けをして助けますが，女性なら知らないふりをして通り過ぎるでしょう．善意で助けようとして、「不審な人に声掛けされた」とか言われる筋合いはないからです．東大が数ヶ月前に掲げていた「**ジェンダーレス**の推進活動」も私は全て同意しません。男は男であり女は女です。ただし、ここで言う「同意しない」は性自認が異なる人を批判するものではありません。私はそういう人たちに対して差別しようとは思っていません。あくまでも「男=女」とするのがが違うのではないかと思っているだけです．いろいろなジェンダーが存在することをかんがえると，誰も助けないのが一番よい？？男性に助けようとして実は性自認が女性で「不審な人」扱いされるかも？？話が授業と関係ない方向に行ってしまった気がしますが，よろしければ先生のお考えをお聞かせください． **➔ 5W1H で 状況依存**

6. 公開鍵方式で送るときは開く側が秘密鍵を使うので問題ないが、逆の場合は誰でも開けられてしまうのは問題ないのですか？

   ➔ 誰でも開けられるのが嬉しい。(確実に送信者のものだと保証される)

7. 公開鍵暗号方式の方が安全であるということは理解できたのですが、公開鍵暗号方式のデメリットのようなものはないのでしょうか？

8. 情報セキュリティにおける公開鍵暗号方式の有用性をよく理解できてよかったです。 現実のカギはコピーもされやすいし、実際にピッキングされることなどもあります。この欠点も今後のセキュリティ技術の向上によりどんどん解消されていきそうにみえますが、**現実はコストなどの関係からか**広く普及している鍵の在り方は長く変わらずずっとそのままです。 これはずっと解消されないままなのではないかと感じました

   ➔ **本当に？？？ 疑ってみて、計算してみたら？**

9. セキュリティの実施をただのコストと捉えるのではなく、効率化の情報提供などビジネスに貢献するものとして考える必要があるというところが印象に残りました。これを踏まえると優良なセキュリティを実施する企業が逆に経済的に損するのではないかという「適度に事故がないとお金を払わない」という逆説的な指摘とも矛盾しないのかなと思い腑に落ちました。

10. 今回の説明であったように、今の世界全体においては、リスクがあるものを悪と捉えがちであり、リスクがないことを正義にしているが、リスクにどうやって対処していくかを重要視するような世界に変わると思いますか?

    ➔ リスク管理・対応能力が 重要インフラに必須ということにしてもらいました。

11. セキュリティを考えるとき、ただ規制を厳しくすると利便性やプライバシーが損なわれたりと、負の側面が大きく必ずしも良い方法とは言えず、多少のリスクがあってもそれに対応できる状態を作ることが大事なのだなとわかりました。完全に安全な状態を目指すより、皆が適度に安心できる状態を作るというのは色々なことに通じることだなと思います。

12. 電子ではエネルギーを大量に消費し，光の速度は今の通信に十分ではないということから，Quantamのポテンシャルがあるという話に興味を持ちました。また，通信の秘匿性について，現在の素因数分解を利用した暗号は量子コンピュータによって解読されてしまうと聞きました。ただ，量子コンピュータの大規模な実用化に向けては多ビット化に加え，環境ノイズによって量子ビットが壊れることや，誤り訂正（FTQC）技術の確立など，ハード・デバイス面で課題があると思います。IBMやGoogleは2030年に実用化といっていますが，量子暗号を含めて今後の暗号や通信の動向はどうなりそうでしょうか。

    ➔ **さぁ、考えてみよう！！！**

13. 匿名だから民主主義なのだと再認識できた。
    ➔Old Media は、匿名性を守って、本当の事実を話してもらいますね。
    ➔New Mediaは、匿名性を使って、虚偽の事実をばらまきますね。。
14. 最近AIによるサイバー攻撃が激化していて、自国生のLLMを持っていないと今後国家の安全保障にかかわると思うのですが、自国製のLLMを持っていなかったとしても技術のみでセキュリティを担保できるとおもいますか。
    ➔ 「国家」だけじゃないんじゃない？ 「組織」「個人」
15. どこまでセキュリティを厳しくすると自由の侵害になったり、抜け道を悪用する人が増えたりするのかは明確な境界がないので、そこにこだわるより、事後のリスク対応を強化した方が良いという様に感じた。プライバシーに関しては忘れられる権利がどう認められていくのかも気になった。
16. 厳格化しすぎるとかえって悪いことが起こってしまうという関羽と劉邦の話に続いて、著作権と知的財産権の話についても納得できた。現代社会でチームワークが重視されているのもイノベーションを推進するためなのだろうと思った。

17. 特許や著作権による過度な保護が、過去の権利者による「未来の競争相手の排除」につながり、イノベーションを阻害していると批判されています。しかし、著作権や特許の保護期間を短縮し、知識やコンテンツを早期に共有財産（コモンズ）として解放すべきだという主張は理想的ですが、保護が弱まった場合、莫大な初期投資（研究開発費や映画等の制作費）が必要な分野において、企業やクリエイターが資金を回収するインセンティブはどう担保されるのでしょうか？ 権利のオープン化が行き過ぎることで、かえって新たな創造の原動力が失われるリスクはないでしょうか？

18. 講義では、ACD（能動的サイバー防御）について、相手を攻撃（反撃）することではなく、相手の攻撃を予測してプロアクティブ（事前）に対処し、「戦わずして勝つ（攻撃させない）」ことであると説明されましたが、国家間のような高度なサイバー戦において、「相手の攻撃を事前に検知し、無力化する（プロアクティブな対処）」ことと、「相手のサーバーやシステムに侵入して先制攻撃を行う」ことの境界線は技術的に非常に曖昧です。「反撃しない防御」を謳いながら、実質的に相手への干渉を行わずに真の抑止力を維持することは、現実的に可能なのでしょうか？

➔物理的な 戦争と同様に 難しいことです。 「同様」なのに、、、サイバー空間では、いつでも 攻撃してもいいのかなぁ。。。。？？？

19. セキュリティは「ゼロを目指す安全」ではなく「のびのび仕事ができる安心」を作ることだ、という整理は意外だった。風紀委員的に縛り上げるほどリスクが増えるという指摘や、暗号でも「安全ではないが安心」と**割り切る発想**に、技術以上に人間の心理や経済の話なのだと気づかされた。

➔ 事実を 言った だけですけどね。

20. 自分がインターンで専門的に扱ってきた分野だったので大変興味深かったです。 どれだけセキュリティを会社が高めようとも結局情報セキュリティインシデントが起こる**一番の原因が人的要因**によるものであると聞いていて、人間の限界を感じています。これからAIが発達しMythosなどのモデルがどれだけセキュリティを向上する施策を打とうと、近年のBerealによる情報漏洩のような人間の部分で情報漏洩が完全になくなることは無いのだろうと考えています。

➔ だから、Digital Complete(デジタル完結)にしたくなる。

21. 講義で、オープンソースとブラックボックスにおけるセキュリティーの話がありましたが、仮にオープンソース至上主義が実現し、社会のインフラがオープンソースで構築されたとしたら、その場合、システムの脆弱性によって人命や財産に被害が出た際の製造物責任（PL法的な責任）や損害賠償は誰が負うべきだと考えますか？

➔ みんな 逃げずに共同で責任を負いましょう。

22. 予防的規制のみを強化すると、社会全体の安全にはつながらないという指摘が印象的だった。起こった際の対策も万全にしておくことで、被害を最小限に食い止める必要性を認識した。

➔ そして、resiliency の重要性を認識・対処しないとね。

23. 自分がゼロトラストの話の中で、アサヒGHDの事例が挙げられていたが、件の事例のように管理者権限(か特権ID)が奪取された場合、ゼロ・トラストの仕組み自体を無効化されるリスクがあるのではないのかと疑問に思った。

➔同じ特権ID/PW にしない。 当然、Trust Anchorも 一つにしない。

➔多様性・独立性を担保して動かす。 これが Block Chain ですね。

➔あれれ？ これが 民主主義 と 習わなかったぁ？

24. プライバシーは時代やシチュエーションによって変わるというのが興味深いと感じた。その点、書き換えが難しい法律での規制とは相性が非常に悪いのではないかと思う。どのような方法で規制すると良いのだろうか。

➔Soft Law と Hard Law (Hardest Lawが憲法)の違いですね。

➔最近は、初めから 法律は定期的に 見直す と するようにできた。