# Question on April 30

1. オープンソースは誰でも設計図を持ってるため比較的危険なものだと思い込んでいたが、安全管理をみんなで高めることができる点で有用だと分かった。Firewallなどのセキュリティー面での仕組みは存在するが、結局は人間が何を信頼してどんな情報を送るかが肝心なのではないかとも思った。
   ➔ 「“人間が”何を信頼して」は、「デジタル・ファンクションが」何を信頼しても 同じになるかね。
2. ディジタル・ネイティブな情報について、オブジェクト指向の抽象的な情報であれば容易な伝達になるというのがわかりました。ただ、例えば電子メールなどにおいて、文字情報しかないと、言い方など、ディジタル化するときにそぎ落とされてしまう情報があると思います。オブジェクト指向の情報でも何の要素を入れるべきかは考える必要があるのではないかと思いました。
   ➔ Semantic (Data)をどう表現するか だね。 AI の出番でもあるかねぇ。
3. 一般にベストエフォートというのはネガティブな文脈で語られがちですが、災害時や非常時の継続性や競争環境による品質向上という側面を評価している点が非常に興味深かったです。
   ➔ Resiliency、特に、予想できていない事象への対応力。 普段から インシデントを経験している人が 対応力を持っているよねぇ。
4. オープンソース化することで、誰でも設計図を持てるがその脆弱性をみんなで守る方法を考えることができるというメリットがあるとわかった。どこをオープンにし、どこをクローズドにするのかの線引きが重要だと感じた。
5. 個人情報を出しても、私は気になりません。
   ➔ 人によって、5WIH で 異なるのが プライバシー(個人) ですからね。多様性、自由の確保が重要。

6. DDos攻撃は大量にアクセスさせる攻撃ということは、対策はサーバーを強化するしかないということですか？つまり根本的な対策はないということ？

   ➔ たくさんのアクセスが来たら、入り口でサーバへのアクセスを遮断/削減するとかね。

7. なぜcloud(雲)と言うのですか？

   ➔ 中身が見えない 雲のようなシステム。

8. AIが進歩して、デジタル世界での操作がほとんど可能になりました。今後、AIロボティクスなどによる物理世界への干渉の時代が来ますか？

9. オープンソース化によって協力してセキュリティ対策を行うことができるという点が責任の所在が曖昧なようで疑問に感じました．これはどこかの誰かの**善意に期待**しているということでしょうか？

10. ワンタイムパスワードは数字6桁などの非常に単純なものが多いですが、セッションが短いとはいえそれだけで大丈夫なのか疑問に思いました。

    ➔ **暗号のパスワード長は、常に 長くなっていますよ。**

11. インターネットでは、情報を一つの大きなかたまりとして送るのではなく、IPパケットという小さな単位に分けて送る。この仕組みは、バケツリレーのように隣の相手へ少しずつ渡していくものだと説明されているが、なぜこのような方法が大規模なネットワークに向いているのだろうか。

    ➔ **Head of Libe Blocking。 長い車が短い車をブロックしちゃう。**

12. 情報の送り方の効率と選択肢の話で、「電話、パケット通信」と「データを小包にして送信」を分けて紹介されていましたが、パケット通信と小包は違うのですか。
➔「パケット通信」は、昔は 回線交換のような 専用の紐を使って デジタルの小包を 送信するシステムを 意味していた。
13. UTOL、UTASのAuthenticatorの二段階認証は正直、面倒なだけだと思っていましたが、パスワードだけだとセキュリティが突破されやすいのを知って、実は有効な手段であるのが理解できました。また、二段階認証もいずれはAIなどの技術の進歩によって容易に突破されるようになる可能性があるのか気になりました。

➔ AI が 2段階認証を 突破するのは、難しいけども。 AI は 攻撃には 利用されます。
14. パスワードにひらがなやカタカナも使えるようにすれば文字の種類数が増えてより強いパスワードができると思うのですがどうでしょうか。実用化されていない理由は、弱いパスワードは問題だけど、ある程度強いパスワードをもっと強くするのはあんまり意味がないということでしょうか。
➔ 「ひらがな」も 単なる数字(ASCII文字)の列ですよね。2バイト。
15. ワンタイムパスワードで使う数字列や文字列はある程度ランダムなもので生成には乱数が関係していると思いますが、コンピュータ上の乱数は中身はプログラムなので、予測がされてしまうということがあるのか気になりました。
➔ 生成のための鍵を 毎回変える ですね。
16. コンピュータのインターフェースという単語がありましたが、これは情報を取得できる窓口のような認識でよいのか疑問に思いました。

17. 外にいるときに、都市部にいながらネットにつながらないということがたまにあるが、それはパケットにどのように分割して送るのか、あるいはどのようなルートでパケットをとどけるのかというのを、最適化することで、別に人工衛星を増やさなくても接続の安定性を高めることはできないのかと気になった。どこでもネットが「つながる」便利な世の中ではあるが、その接続性能についてはまだ改善の余地があると思う。
    ➔そのために、たくさんの インターフェースを利用可能にする。 していますよね。
    ➔そろそろ、3G が 消えるけど。
18. アナログの方がディジタルよりも伝送コストがかかる，という話がありましたが，一方でアナログ情報にも価値はあると思われます．（音楽を聴くのにCDよりもレコードを好む人もいるようです．） 将来アナログはデジタルに完全に取って代わられるのでしょうか．また，アナログの特性をデジタルにおいて補完・代替することはできるのでしょうか．
    ➔ 拡張現実は、アナログを超えるよね。各個人の特性に合わせるとか。
19. githubでいつもsshを用いて接続をしているが、sshがどのように暗号化しているのかよくわかっていなかったので、仕組みを知れて納得ができた。また、オープンソースをwslに入れるとき、いろいろと調べてもどれが正しいかわからなくなり、AIに聞いて出てきたコマンドをそのまま入れてしまっているので、sudoでroot権限で実行している以上もっと注意しないといけないと感じた。
20. セキュリティの防衛策は色々挙がっていると思いますが、一個一個全ては具体的にはこういうものだよねみたいなものは深くは扱わないのでしょうか。
    ➔ セキュリティーの講義で 学べるはずです。

21. Firewallについて「Disconnectしても悪いやつが内部にいるとやられる」という話があまりイメージできなかったので具体的な手法や例を知りたいです。
➔ Disconnectedだと思うと気が緩む。コンピュータが 持ち運び可能なっちゃった。

22. 通信プロトコルがHTTPからHTTPSへと移行したように、AI Agentの発展に伴って、新しい通信プロトコルが生まれてくるか疑問に思いました。特に、MCPのようなエージェント向けプロトコルが急速に普及している一方、プロンプトインジェクションやTool Poisoningといったセキュリティ課題も顕在化しており、セキュリティ層の標準化が今後どのように進むかについては興味深いです。
➔ Agent に対する AAA の導入ですかね。

23. 近頃「ネット私刑」という言葉があるほど、一般の人が他人の顔を晒したり、拡散させる人が多いのですが、いじめだったり迷惑行為だったりを晒す人に対して称賛コメントが見られる場合があります。なんの脈絡のない人間同士で騒ぎあってもそれは当人たちの間では解決せずただただプライバシーを損害されて荒らされるだけのように思えるのですが、これは公共の安全、秩序というセキュリティ意識と守られるべき個人のプライバシーが対立する場面だと感じます。何を持って晒してもいいと人々は判断しているのか、私刑による情報セキュリティ上のリスクについて教えてください。
➔ 対策を 誰かに(偉そうな人に)頼む/依存する？　さて、その誰かが 悪い輩 だったら/になったら？　政府は信用できる？　誰なら信用できる？　TRUSTという問題です。

24. 電話はエッジで文字にして回線に乗せ、送った先のエッジで音声に復号する形でも成立するという発想が面白かった。電話回線とtext送信のデータ容量の違いから、今まで夢物語だったものがAIというもので可能になってきているのかなと感じた
➔「初音ミク」を 各個人で できるでしょ。

25. 2010年に中国漁船衝突の映像が流出した事件で海上保安庁への信頼が損なわれてしまったということでしたが、現在に至るまでにその信頼は回復できたのでしょうか？ 特に諸外国がこの問題をどのように捉えていたのかが気になります。
    ➔ 中国に聞いてみるといいかもねぇ。
26. 災害時にネットに繋がらないのと普段の生活でネットに繋がらないのは何か違う理由があるのかと思っていたのですが、根本的には同じということですか
    ➔ 根本的には ほぼ 同じ問題。 なので、普段 つながらないかも という ベストエフォートの方が、いつも つながっているシステムよりも、災害時/非常時に強い。
27. AIやインターネットにおける、情報の悪用という話について、私は今まで無意識に権力者を信用しすぎていたのだと実感した。現在様々な場所で情報を提供しなければ利用できないサービスが多いが、それらとはどう向き合っていけば良いか教えて欲しい。(様々なSNS、サイト)
    ➔ 昔習った、三権分立、個人的人権、民主主義。 Harariの投稿を読んでもらった理由。
28. 政府に情報を渡すと漏洩されるとのお話ですが、先生は政府と強いパイプか何かをお持ちなのですか。
    ➔ いろいろ実経験はあります。 っが、皆さん、社会・歴史の時間に 習ったよね？

29. 2段階認証のアンカーポイントとして、SMSと電子メールだとどちらの方が安全なのでしょうか。そのサービスに登録しているメールアカウントを突破されると電子メールによる2段階認証は意味をなさないように思えます。

➔ SMS の方が安全ではあるかなぁ。。 SIM情報が抜かれなければ。

30. ディジタル回路を設計する中でも、記憶回路の設計は単純な論理回路の設計よりも複雑であり、情報の伝達において記憶の必要をなくすことは大幅なコスト削減につながると思った。

➔ 離れた場所の記憶(＝データ)が、複数の人からアクセスされる状況が 面倒ですねぇ。

31. 古いOSや独自システムで動いている、工場などのゼロトラストを導入するのが技術的に困難な組織は淘汰されていくのでしょうか。

➔既に、TSMC、Rapidus、Intel などの 半導体は、サプライチェーン全体で、この方向に向かっています。

➔自動車関係なども。