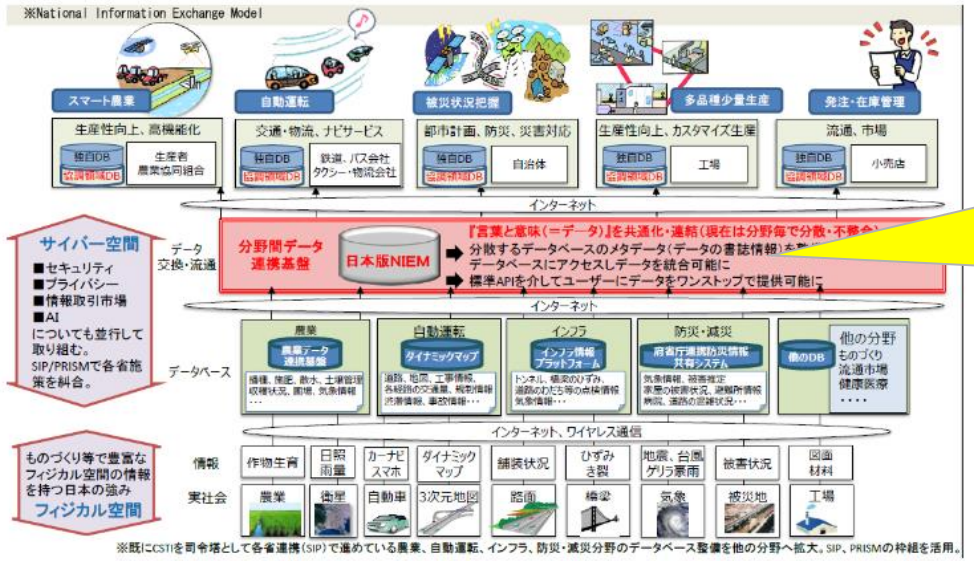
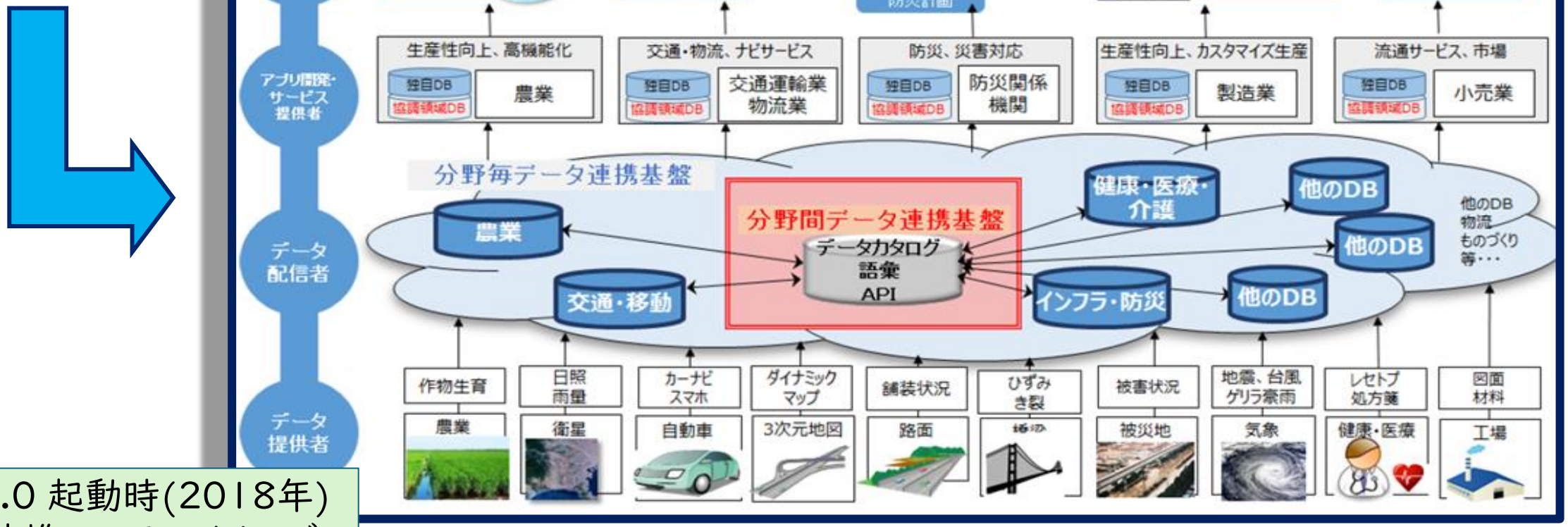
Q&A　4月24日 分

ネットワーク工学概論

1. セキュリティが単に攻撃に対する防衛という意味合いでしか捉えられていない場面が多いことに気が付きました。そもそもsecureというのは"positioned or fixed firmly and correctly and therefore not likely to move, fall, or break (Cambridge Dict.)"程度の意味合いで、言葉の定義からしても外部からの攻撃を恐れて壁を作るのではなく、ひとまず安心できる環境を整備するという理解の方が正しいと思う。言葉を印象だけで捉えるのは危険。世論やメディアにはそういう傾向が残念ながら蔓延しているようであるが。
   ➔安心して、新しい挑戦ができる環境(リスク テイク可能な環境)を提供するですね。これが安心の環境です。 新しい挑戦は成功すれば、進化・成長につながります。
   一方、安全な環境では、新しい挑戦 を禁止したくなります。成長・進化が止まります。
2. 最終的に信用する相手として国を用いるという話をされていたが、それはそもそも国に信用がある国でしか通用しないように思われる。信用がない国、そもそも国に十分なネットワークインフラがない国ではどのような運用をしているのかお話を伺いたいです。
   ➔「国を用いることができる」と 言ったかなと思います。 国を信用できない 人々は、信頼できる「組織(含 営利企業) 」を 利用(信頼)します。「国」は、信用されない場合には、「法律と罰」を使って、人々を誘導(服従させる？)します。 国は、"a" trust anchor (信用度が高そうな)です。 デジタル庁では、マイナンバー{カード}用のTrust Anchorをつくりましたが、最初から、民間やいろいろな公的なサービスが利用可能な環境を提供するように デザインの指示を行いましたか。 多くの「国」の統治者は、選択肢を提供したくない という場合が多い。

Multi-Stake Holder
官 は “a” critical stake holder
民主導、官支援





Society5.0 起動時(2018年)
「データ連携システムイメージ」

2025年3月5日
東京大学 教授 江崎 浩

Data Spaces は、グローバルな分散型デジタル空間上に存在する。

- インターネットの前提(**by-design**)
  1. 統一(Unified技術, i.e.,TCP/IP)によって、デジタルデータの**「自由な生成・流通・加工」**が可能な **「国境を跨る」 物理的連邦(Federated)システム**。
  2. **自律分散(P2P)**から新しいサービスが創生され、分散は維持しながらの集中(CS)によるビジネス化。 ① **“Start Small, Scale Fast”**、② **敢えて 最適化しない(変化可能なモノが生き残る)**。
  3. グローバルな空間上に CONNECTEDな **国境を跨る{技術的にも}多様性を持ったData Spaces** を形成。
  4. **「国」(“a” critical stake holder)**を含む マルチステークホルダ(MSH; Multi-Stake Holder)での運用。
  5. **複数の Trust Anchors での分散&連携** 運用。

- After 2025
  1. これまで Disconnectedだったシステムが、CONNECTED に なり、**新しい Data Space**を創生する。
  2. **国境が存在しない物理空間**(e.g., 宇宙)も存在し、CONENCTEDになりつつある。

3. 東京大学ではなぜ、P2P通信が厳しく取り締まられているのですか？
   ➔“不適切な”(=法律に反する) P2P通信は 取り締まります。法治国家ですから。
   ➔なので、公的施設を、私的に利用するのは制限しないといけない。
   ➔間違った「法」は、創らせない、変更・修正させる ですね。
   ➔研究で使うのは問題ない。 研究目的でのインシデントは、頑張って助けます。

4. カスペルスキーのサイバーマップによると、アフリカの孤島(セントヘレナ島かアセンション島？)からかなりの数のサイバー攻撃がありますが、それは攻撃者がVPNの中継地として選んでいるからでしょうか？それとも、IPアドレスの偽装を行っているのでしょうか？ ➔ 中継地でしょう。

5. セキュリティは公助から行うと崩壊するという話を授業中行なっていましたが、それは、公助のセキュリティを導入した時に、セキュリティの甘い個人がウィルスを保持していたら大枠のセキュリティシステムが崩壊するという認識で良いでしょうか？
   ➔ 一番の崩壊の可能性は、為政者側が、別の不適切な目的に利用する可能性があるからですかね。(歴史が示している通り)
   ➔セキュリティの甘い個人がウィルスを保持しても、自助での防御が徹底しているところでは、被害は、あまり出ません。
   ➔自分の近傍には、悪い個人(機械)が来ないように 公がしてくれるはずなので、自身での対策は、不要だと思ってしまう。。。。。

6. プライバシーが主観に基づく判断であるという見方は新鮮に感じられ、その考え方に則るならばプライバシーの保護は各自の自己責任であると考えるべきだと思った。
   ➔ ここでも、自助、共助、公助 の 順番ですかね。
7. セキュリティ強化という投資を品質向上への投資と、ポジティブにとらえる考え方が面白かった。IP制限やポートの開放、ファイアウォールの導入などを面倒に思っていたがこれからはそのように考え積極的に更新していきたいと思った。
8. 組織の内部者によるセキュリティへの攻撃が大半である、というのはセキュリティの内側にいる人がセキュリティを壊すのは比較的簡単かつ警戒されにくいという点から納得出来た。この事態に対する対策を思いつくことができないので(信頼や安心などの心理的要因にしか頼れないと感じる)、どうしたらこの問題を減らすことが出来るのか気になった。また規制やセキュリティを過度に設けるとブラックマーケットが生じるという話では、規制によって賢い人がより多くの利益を得ることで“ズル”賢いと見なされ、一方で素直な人が損をすることになるため全体として悪循環な状況であると感じた。
   ➔ 忖度や改竄を (陽に暗に)強要されて、それに従ってしまう「人」ではなく、これを考えない「機械」にしたら 良くないですかね？
   完全デジタルにすると、ソフトウェアに「忖度や改竄」が埋め込まれない限り、ソフトウェアは、ばか正直に仕事をしてくれます。
   「人」は、忖度や脅しから解放されて、心理的安全性を獲得することになります。

デジタル庁
Digital Agency

2. AS IS から TO BE へ
(新しい出口への誘導)

2022年11月16日

手作業(第1人称) から デジタル(第3人称)

デジタル庁
Digital Agency

1. デジタル化＋オンライン化 で
   - ➔ データの改竄(=忖度) が できなくなる。
   - ➔ 監査業務も簡単になる。
   - ➔ 責任の所在は 人 ではなく、コンピュータに
2. さらに Web3(Block-Chain) が来ると。
   - ➔ 第3者 も データ改竄 できなくなる

👇

心理的安定性 の 拡充

2022年11月16日

9. リスクを完全に無くす（＝0にする）のではなく、減らした上で、いざ起こった時のリスクハンドリングを強固にすべき（安心）という点は、インターネットというネットワークにおいてのみならず、例えば人間間のネットワーク（例えば仕事など）で起きるヒューマンエラーに対する態度（人間である以上ミスはするので、しないことを考えるのではなくした後どうリスクをマネジメントするかが大切という考え）と通じる点があるなと感じました。
10. 完全な安全は実現することができないので、安心の実現を目指すという考え方にはとても納得した。
11. 安心と安全の区別が自分の中でしっかりとしていませんでした。今日の講義を聞いて完璧な安全が得られないような状況では安心と安全の区別ができていないと、目指すべき点を間違えてしまうと気づけました。
12. 今までの講義であったお金や鍵をデジタル化するという技術が増えれば増えるほど、普及するか否かの決定点がセキュリティにあると感じていました。例えば、鍵をデジタル化することがなかなか普及しないことの理由がアナログの鍵を自分が手元に持っていた方が安心が得られるからだと思います。なので、デジタル化が進めば進むほどセキュリティに関する需要が今後高まりそうだと思いました。
13. いわゆる、「事故が起きないと対策を考えない」のような批判はよく聞きますが、適度に事故が起きないと逆にそこにお金が払われない、ビジネスとして成立しないというお話が新鮮でした。

また、最後にお話のあった、保険会社がそもそも事故が起きないように対策にAIやIoTを用いるというお話でしたが、ちょうど先日ソニー損保の、AIが運転の評価、事故対策のアドバイスをしてくれるアプリを知ったばかりだったので、具体的なイメージが湧き、先日知ったアプリのビジネスモデルが少し分かった気がして面白かったです。

14. 私は今まで「ゼロトラスト」の考え方から、個人（自助）は当てにならないから公助でなんとかすべきだと思っていましたが、今日の講義で間違った認識をしていたかもしれないと思いました。一方で、「ゼロトラスト」（個人を信じない）と「まずは自助」（個人の対策が大事）が矛盾しているような気がしてしまい、頭の中でうまく噛み合わなかったので追加で解説をお願いできればと思います。 ➔「他人を信じないを基本/前提に」です。

15.著作権、知的財産権の規制の話で、先週のプロジェクトXでの初音ミクの話を思い出した。初音ミクの著作権を大手会社に売らず、個人が初音ミクを使って自由に楽曲を作れる環境を残しておいたことで、音楽業界に新しいボカロというジャンルが生まれることにつながり、さらに個人個人が楽曲を作るため交流が盛んになったという話でした。このようにある意味利益度外視で、その分野の発展を願った人がいたおかげで生まれた作品、発明は意外に身近でも見つかるものだと思いました。また、初めの段階で初音ミクの著作権を売ってしまっていたらこれほどまでに初音ミクが世界中に知られることはなかったかもしれません。技術を自分たちだけの中に囲むよりもその技術を広く使ってもらうことが逆に自分のさらなる利益につながっている例かと思いました。

➔「情けは人の為ならず」。「風が吹けば桶屋が儲かる」➔ “利他主義”

16. 高度なテクニックを用いて目指すところが完璧ではなく、適度な緩さのあるシステムというところが、一般のイメージと異なるところだと思いました。先生が偉人たちの言葉を引用して教えてくださっているように、このような「いいかげん」なシステムをあえて作ったり、そのバランスを考えたりするところに、文理両方に明るい教養ある人材が必要なのだと思った。
17. 挑戦しない理由を探す名人が新規のチャンスを潰すというのにとても共感しました。初めから完璧でないといけないといった状況では新しいことは発展できないです。
18. 匿名性は安心を害する人を排除し共助して環境を守りやすいためにあるシステムとして解釈したのですがそれであっていますでしょうか。

    ➔「安心を害する人」の定義によりますが。報復を恐れずに、発言を可能にする。
    表現/発言の自由のためのものでもありますか。

19. 保険会社がそもそも事故が起きないように対策にAIやIoTを用いるというお話でしたが、ちょうど先日ソニー損保の、AIが運転の評価、事故対策のアドバイスをしてくれるアプリを知ったばかりだったので、具体的なイメージが湧き、先日知ったアプリのビジネスモデルが少し分かった気がして面白かったです。

セキュリティー

- 例えば、デブ への生命保険
  - 困ること
    - 死亡 ➔ 収入の喪失
    - 疾病発生➔治療費

    (*) つまりは、収入の減少
  - 保障すべき物
    - お金
  - 最近保険会社がやっていること
    - デブにならないようにする方法を奨める ⬅ **ここに AI と IoT**

      i.e., 予防策の伝授 ➔ 保険利用の確率を下げる。

さらに、「法律で規制」に。
By 効果があることを証明
（導入で事故が減少する）

昔の先例：
火災報知器 と スプリンクラー 消火器
with 火災保険

最近の例：
自動車 衝突回避機能、次に 運転記録
with 損害保険

20. 最近聞いた面白いニュースで、生成AIに対して「ありがとう」等の丁寧な言葉遣いをするだけで年間電力消費が数十億円分増大するという発言があったようです。
（https://gigazine.net/news/20250421-politeness-could-be-costly-ai/）

大学生が”使っている”生成AIやネットワークは、いったいどれくらいの電力消費を生んでいるんだろう、、、と怖くなりました。

➔これぐらい 電気を使っても 儲けがでるという ことが 驚きじゃないかなぁ。

➔気持ちよくさせて、再来店を 促す。 接客の基本ですかね。

20. デジタルなキーを使った認証以外にも、顔認証や指紋認証といったアナログな生体を使った認証もありますが、結局のところデジタルのレイヤーで処理されるので同じことになるのでしょうか。パスワードを使い回すことはセキュリティの観点上よくないこととされていますが、生体認証も同一の生体を使い回していると考えれば、むしろ個別のパスワードを設定するよりも安全性としては低いのでしょうか（生体認証だけで認証しているサービスはあまりなく必ずパスワードとの組み合わせで使われるような気がしていますがこれが原因でしょうか）。

➔生体情報は、修正・変更ができないので、とても 苦しいですね。

一方、パスワードは、簡単に変更できます(覚えにくいけど、、、)