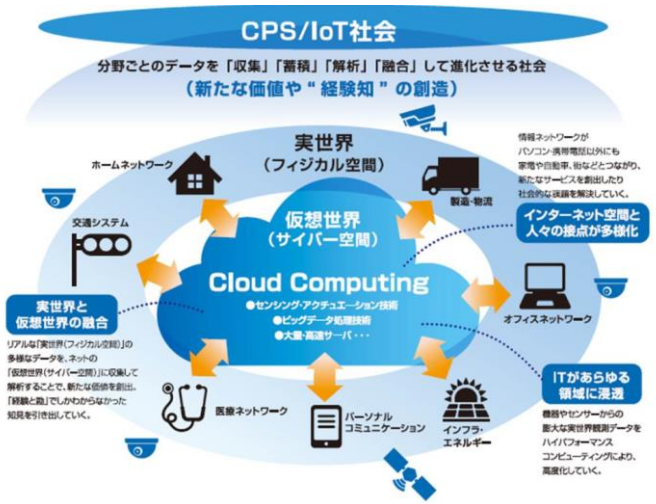
DXとセキュリティ
- 繋がる時代のリスクに備えて -

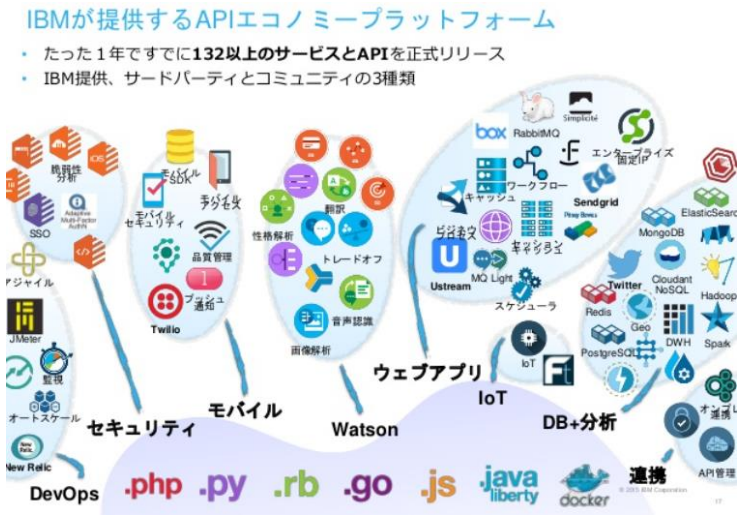
東京財団政策研究所 主席研究員
満永 拓邦

東京財団政策研究所
THE TOKYO FOUNDATION FOR POLICY RESEARCH

繋がることによる「価値創造」

- Cyber Physical System、Society5.0、API Economy などに共通するのは様々なモノが繋がり、標準化されたデータを連携することによって、新たな「価値創造」を試みている点である
- 現実、システム、クラウド、アプリなどがネットワーク上で有機的に繋がることにより、これまでにない機能やユーザの利便性向上などが実現することが期待されている
- 民間の取り組みだけではなく、他国の電子政府においても、APIなどを通じたデータ連携により国民の利便性向上を実現している事例もある

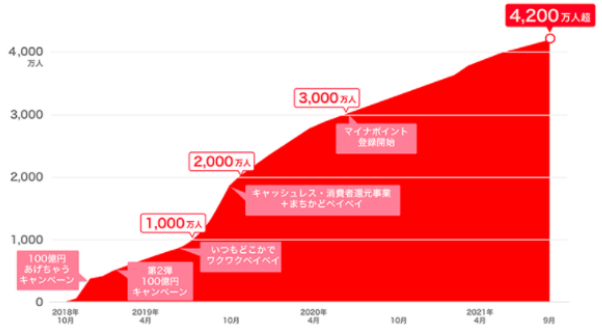




左画像引用：https://www.jeita.or.jp/cps/about/
右画像引用：https://www.slideshare.net/rasmusekman/api-54896752

スマホ決済の普及

- これまで取引に伴う資金決済は、預金取扱金融機関が参加する「全国銀行データ通信システム（全銀システム）」を中心に行われていた（いわゆる銀行振り込み、引き落とし等）
- 近年では、個人の決済においては、スマホ決済アプリ（〇〇Pay)の利用が急増しており、口座、クレジット、アプリの資金移動がネットワークを介してリアルタイムで行われている
- 個人間のやり取りだけではなく、公的な機関の支払い（全国の自治体約3分の2の納税）にも対応しており、ユーザーの利便性、社会の生産性向上に寄与すると言われる



【登録者数の推移】

お財布マークの
「ウォレット」タブ内
「請求書支払い」をタップ

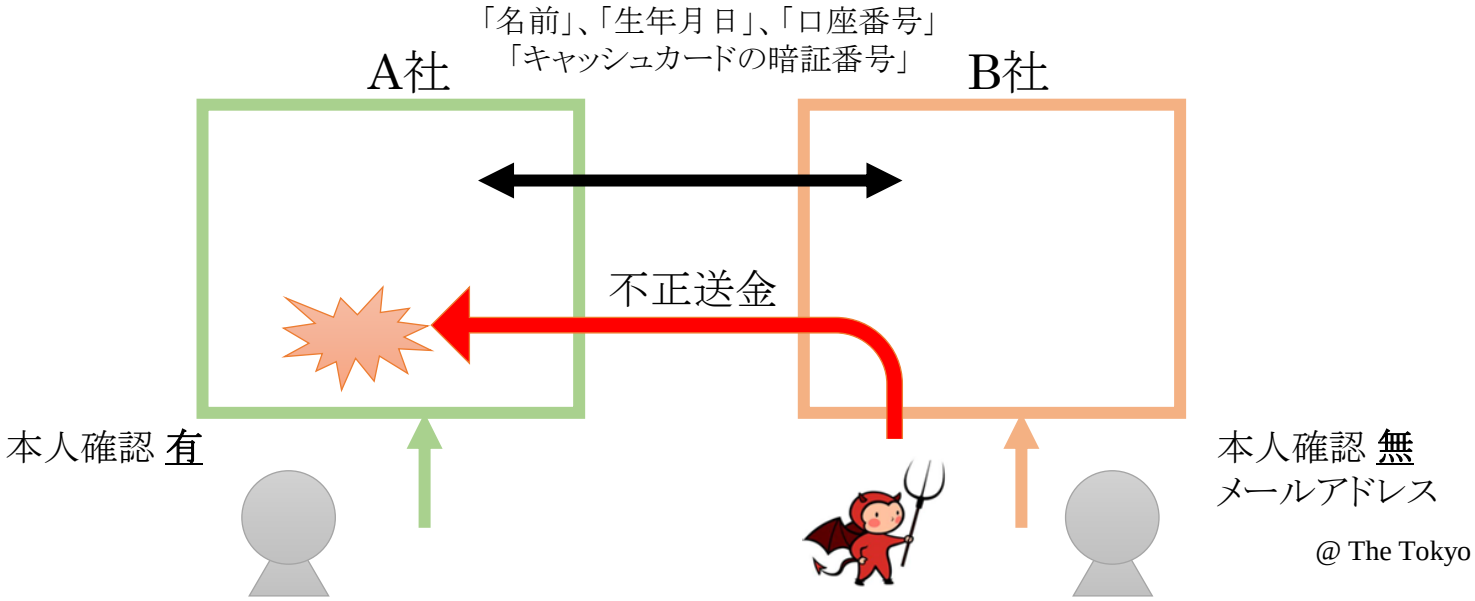
立ち上がったコードリーダーで
お手元の請求書のバーコードを
読み込む

内容を確認して
支払い完了!

左画像引用：https://about.paypay.ne.jp/pr/20211020/01/
右画像引用：https://www.city.bunkyo.lg.jp/tetsuzuki/zeimu/juminzei-nozei/line.html

繋がることにより生じるリスク例

- 相互接続の相手方と異なるセキュリティレベルで運用されていれば、繋がる相手から意図せず不正な操作が行われるリスクが存在する
- 国内で資金移動事業者と銀行間の接続において確認する項目の差異によって、Web口座振替に関わる不正送金事案が発生した（自分の銀行口座から勝手にお金が引き落とされる）
- 繋がる相手について、サイバーセキュリティやビジネスプロセスの観点からのリスク評価を行うことが必要になってくる（**相手を必ずしも信用しない→ゼロトラストという考え方**）



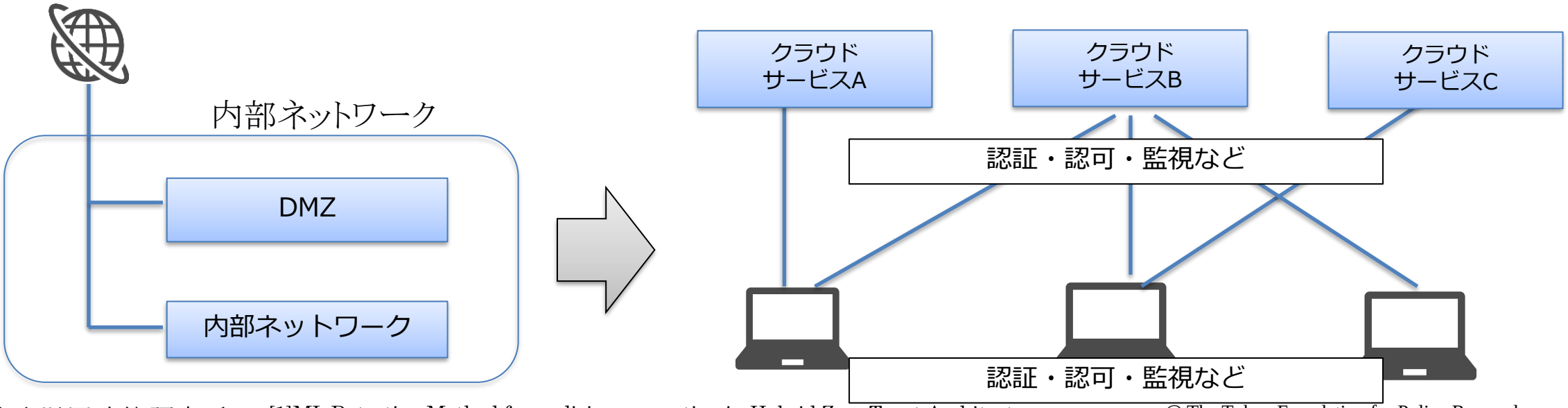
ゼロトラストネットワークアクセス (ZTNA:Zero Trust Network Access)

- ゼロトラストの基本的な考え方は、NIST SP800-207(ゼロトラスト・アーキテクチャ) に書かれている
- 以下の「基本的な 7 つの考え方」のもと、ゼロトラストでは全てのデバイス、ユーザ、通信を監視し、認証・認可を行うこととしている

No.	基本的な7つの考え方
1	すべてのデータソースとコンピューティングサービスをリソースとみなす
2	ネットワークの場所に関係なく，**すべての通信を保護**する
3	企業リソースへのアクセスをセッション単位で付与する
4	リソースへのアクセスは，クライアントアイデンティティ，アプリケーション/サービス，リクエストする資産の状態，その他の行動属性や環境属性を含めた動的ポリシーにより決定する
5	すべての資産の整合性とセキュリティ動作を**監視**し，**測定**する
6	すべてのリソースの認証と認可を行い，アクセスが許可される前に**厳格に実施**する
7	資産，ネットワークのインフラストラクチャ，通信の現状について可能な限り多くの情報を収集し，セキュリティ体制の改善に利用する

リモートワークとゼロトラスト

- コロナ禍に端を発するリモートワークの普及においても、生産性向上とセキュリティ強化の両面を図るべくゼロトラストの考え方が多くの企業で取り入れ始めている
- ゼロトラストでは全てのデバイス、ユーザ、通信、ネットワークを監視し、認証・認可を行うため、安全なネットワークや通信先という捉え方をしない
- 分散するデータやログをどのように効率的に分析するかという課題が見え始めている[1]



[1]ML Detection Method for malicious operation in Hybrid Zero Trust Architecture
Koji Ishide, Satoshi Okada, Masatoshi Yoshikura, Wataru Matsuda, Mariko Fujimoto, Takuho Mitsunaga, SCIS 2022

繋がる先の多様化

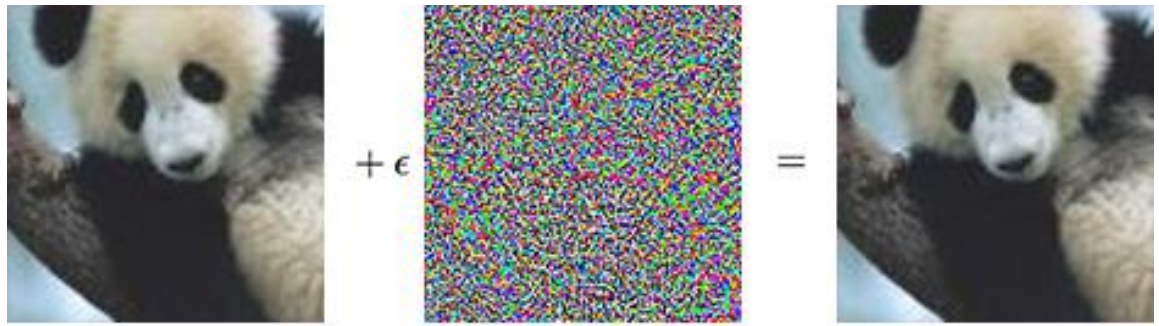
- 少子高齢化時代を迎えて、工場、医療、農業など様々な分野でIoT、AIなどの技術を活用した生産性向上やコスト削減が図られている

日立品質制御支援システム
http://www.hitachi.co.jp/products/it/industry/solution/dsc/dsc_qc.html#0201

日本医療研究開発機構「スマート医療室」
https://www.amed.go.jp/news/release_20160616.html

AI処理の信用性

- DXの実現のために、様々な場面においてAIの活用が進むと考えれている
- しかしながら、AIも必ずしも万能なツールではなく、不正な入力値を与えることにより、AIの処理を誤らせることが可能であり、そうした手法の研究が進んでいる
- 以下の例は、分類器が正しく分類できていた画像にノイズをのせることで、分類器の判断を誤らせることができる Adversary Example と呼ばれる有名な手法であり、こうした誤った処理を引き起こす攻撃を検知する研究も活発に行われている

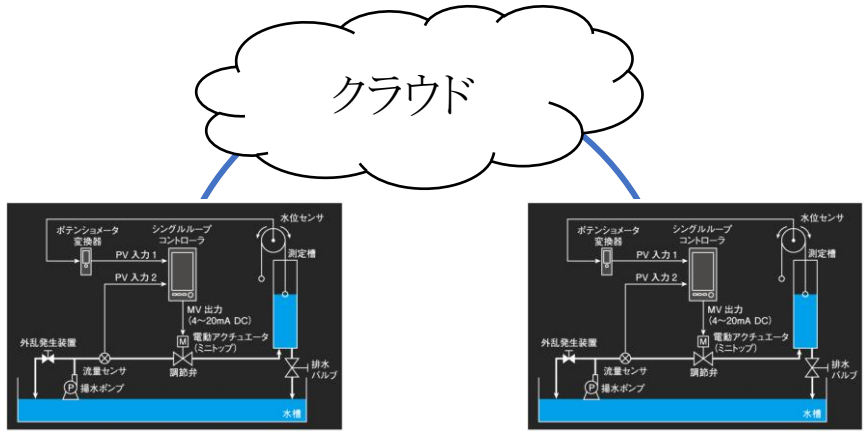


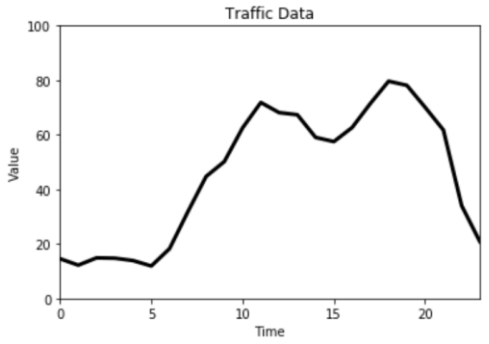
Goodfellow, Ian J., Jonathon Shlens, and Christian Szegedy. "Explaining and harnessing adversarial examples." *arXiv preprint arXiv:1412.6572* (2014).

産業制御におけるAI活用とリスク

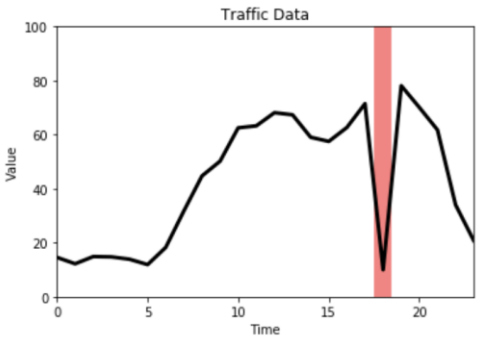
- 産業制御の分野においてもAI活用は期待されており、生産性向上に寄与すると考えられている
- しかしながら、産業制御で利用されるAIにおいても意図しない動作を引き起される危険性もある
- 「人間中心の AI 社会原則」などを踏まえて、AI活用は慎重に検討する必要性が高まっている
  - セキュリティ確保の原則：AI を積極的に利用することで多くの社会システムが自動化され、安全性が向上する。一方、少なくとも現在想定できる技術の範囲では、希少事象や意図的な攻撃に対して AI が常に適切に対応することは不可能であり、セキュリティに対する新たなリスクも生じる。社会は、常にベネフィットとリスクのバランスに留意し、全体として社会の安全性及び持続可能性が向上するように務めなければならない

・満永研究室にて行っているAIに意図しない動作を行わせる産業制御実験のイメージ





日々のトラフィックデータ



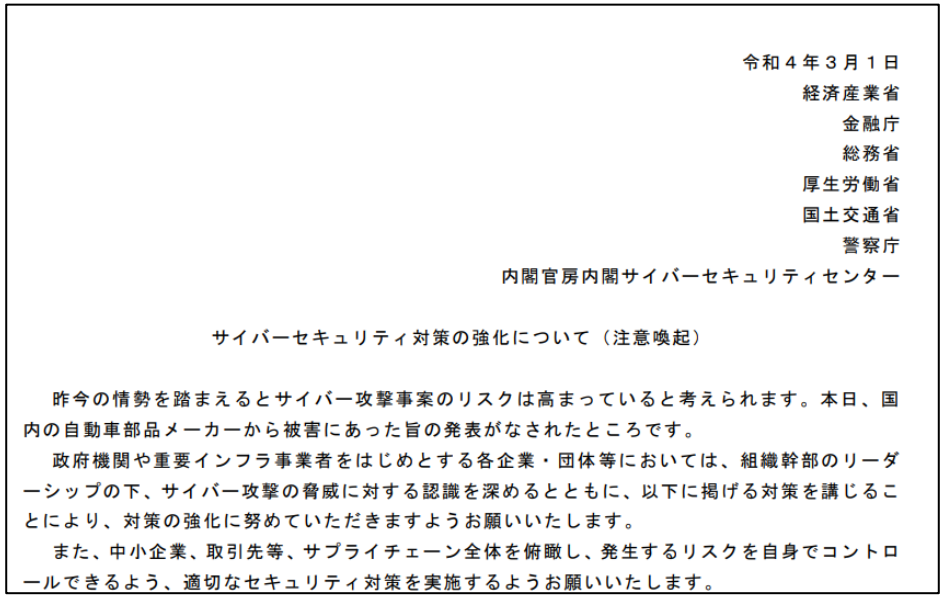
異常の検知

東京財団政策研究所
THE TOKYO FOUNDATION FOR POLICY RESEARCH

Cyber Security Risk Assessment on Industry 4.0 using ICS testbed with AI and Cloud
Wataru Matsuda, Mariko Fujimoto, Tomomi Aoyama, Takuho Mitsunaga
2019 IEEE CONFERENCE ON APPLICATION, INFORMATION AND NETWORK SECURITY (AINS 2019) 54-59

直近の話題

- 2022年3月1日に、経済産業省などが昨今の情勢を踏まえて、サプライチェーンに関わるサイバーセキュリティの注意喚起を公開
- 自動車部品メーカーがランサムウエア（身代金ウイルス）の被害を受けて、自動車メーカーの工場稼働が停止したとの報道
- 「鎖の丈夫さは、最も弱い輪によって決まる」by トーマス・リード



令和４年３月１日
経済産業省
金融庁
総務省
厚生労働省
国土交通省
警察庁
内閣官房内閣サイバーセキュリティセンター

サイバーセキュリティ対策の強化について（注意喚起）

昨今の情勢を踏まえるとサイバー攻撃事案のリスクは高まっていると考えられます。本日、国内の自動車部品メーカーから被害にあった旨の発表がなされたところです。

政府機関や重要インフラ事業者をはじめとする各企業・団体等においては、組織幹部のリーダーシップの下、サイバー攻撃の脅威に対する認識を深めるとともに、以下に掲げる対策を講じることにより、対策の強化に努めていただきますようお願いいたします。

また、中小企業、取引先等、サプライチェーン全体を俯瞰し、発生するリスクを自身でコントロールできるよう、適切なセキュリティ対策を実施するようお願いいたします。

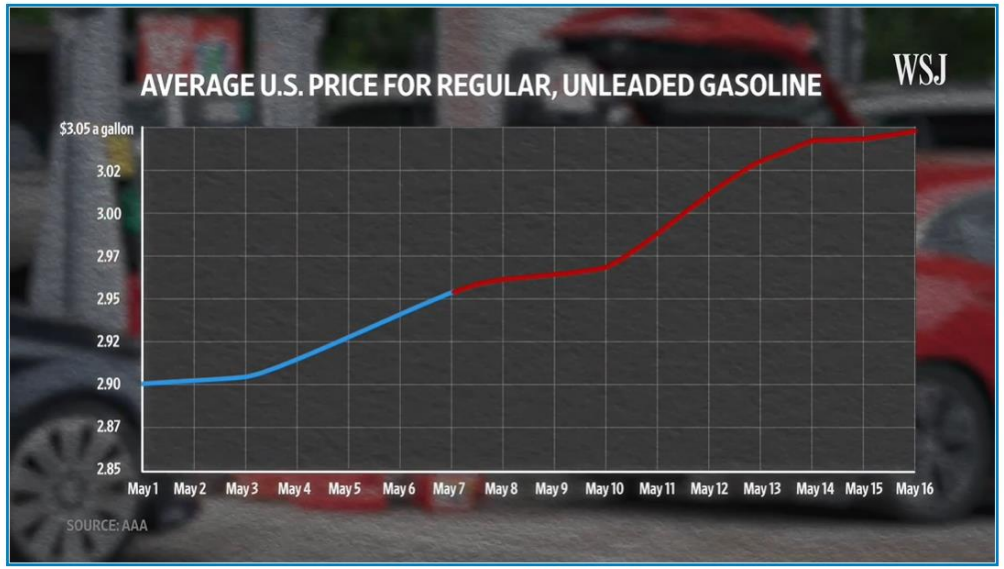
https://www.meti.go.jp/press/2021/03/20220301007/20220301007-1.pdf

サイバー攻撃による米国パイプライン停止

- 米国コロニアル・パイプラインはサイバー攻撃を受け、7日から操業を停止し、身代金の支払いのんち、12日夜に操業を再開した
- 燃料価格調査会社「ガスバディ」のデータによると、ノースカロライナ州やジョージア州など複数の州でガソリン不足が続き、価格が上昇した
- コロニアル社のブラウント社長は、いつまで操業停止が続くのか不透明だったことから、5月7日に身代金の支払いを承認したと語った

Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4

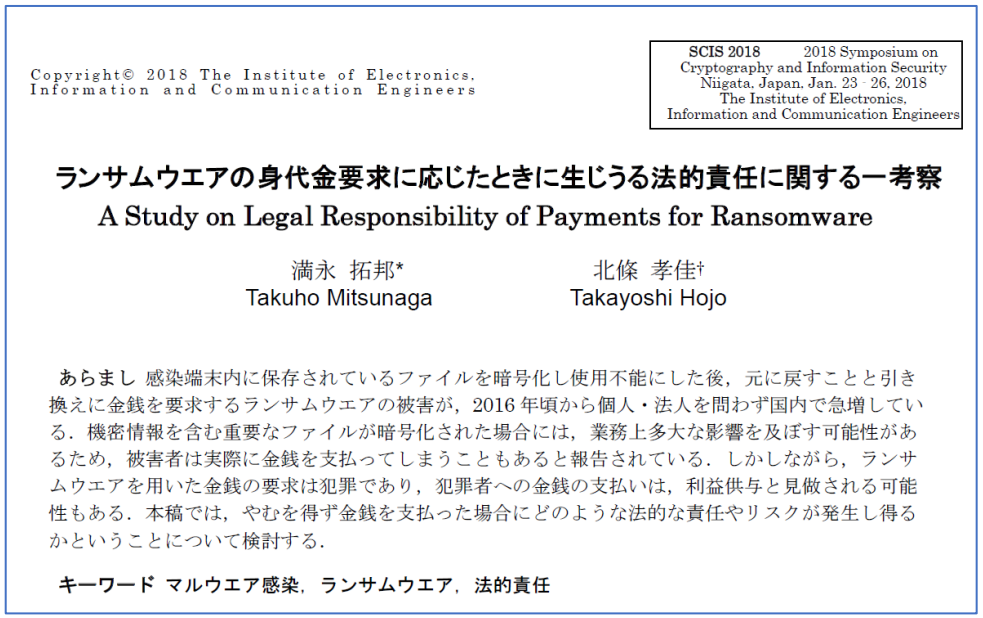
Joseph Blount says he needed to quickly restore service after cyberattack threatened East Coast supp



A cyberattack on the U.S.'s largest fuel pipeline on May 7 forced a shutdown that triggered a spike in gas prices and shortages in parts of the

(参考)ランサムウエアに対する支払い

- “ランサムウエアの身代金要求に応じたときに生じうる法的責任に関する一考察”, 満永拓邦(東京大学)、北條孝佳(西村あさひ法律事務所), SCIS 2018
- 一定の条件下におけるランサムウエアへの支払いは法的な責任が生じうるため、安易に支払ってはならない
- 米国では財務省が「the sanctions risks associated with ransomware payments(ランサムウエアへの支払いに関する制裁リスク)」についてアドバイザリを公開している



SCIS 2018 2018 Symposium on Cryptography and Information Security
Niigata, Japan, Jan. 23 - 26, 2018
The Institute of Electronics, Information and Communication Engineers

ランサムウエアの身代金要求に応じたときに生じうる法的責任に関する一考察

A Study on Legal Responsibility of Payments for Ransomware

満永 拓邦* Takuho Mitsunaga
北條 孝佳† Takayoshi Hojo

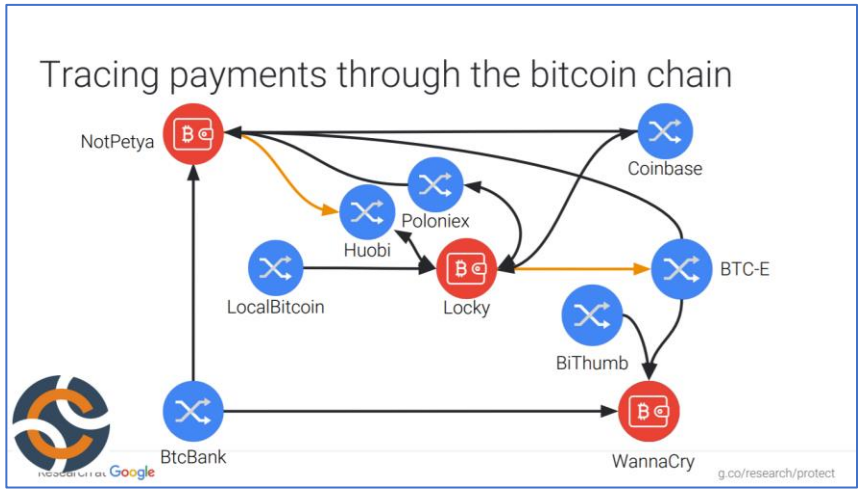
あらまし 感染端末内に保存されているファイルを暗号化し使用不能にした後，元に戻すことと引き換えに金銭を要求するランサムウエアの被害が，2016 年頃から個人・法人を問わず国内で急増している．機密情報を含む重要なファイルが暗号化された場合には，業務上多大な影響を及ぼす可能性があるため，被害者は実際に金銭を支払ってしまうこともあると報告されている．しかしながら，ランサムウエアを用いた金銭の要求は犯罪であり，犯罪者への金銭の支払いは，利益供与と見做される可能性もある．本稿では，やむを得ず金銭を支払った場合にどのような法的な責任やリスクが発生し得るかということについて検討する．

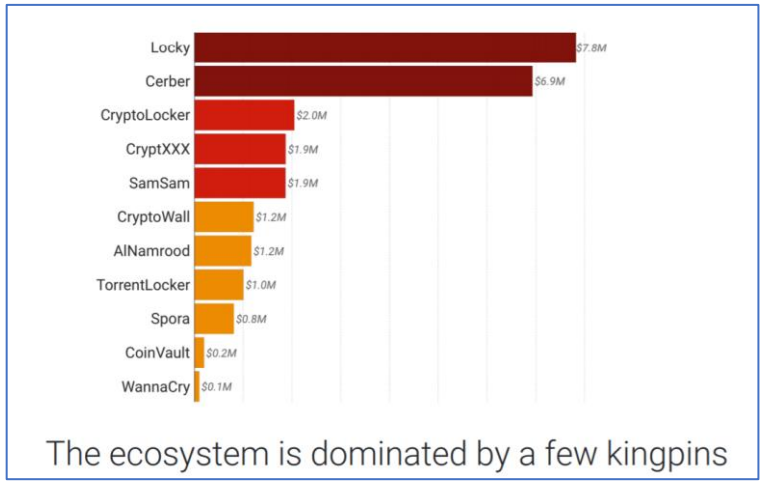
キーワード マルウエア感染，ランサムウエア，法的責任

ランサムウエアに関する資金移動

- 154,227 個のランサムウェアのデータセットに基づいて、Google、ニューヨーク大学らの研究者がランサムウエアの支払いに利用されたBitcoinを追跡することにより、被害額や資金の流れを調査した

- 調査期間を通じて、総額約 2500 万ドルがBitcoinから現金として換金されており、その約95%がロシアの取引所を通じて現金化されていた

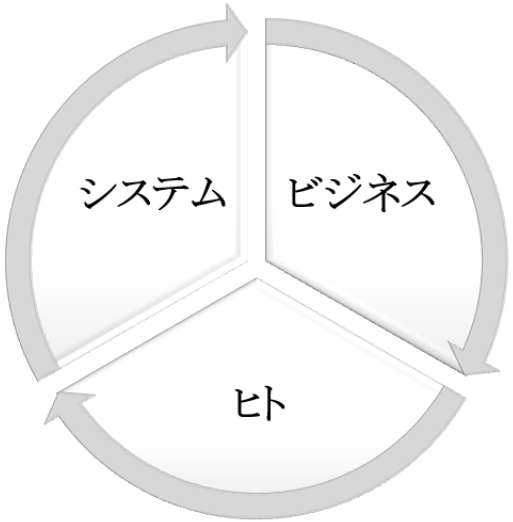




画像引用：”TRACKING RANSOMWARE END TO END”
https://www.blackhat.com/docs/us-17/wednesday/us-17-Invernizzi-Tracking-Ransomware-End-To-End.pdf

ビジネス継続

- DXが進んだとしても、「**システムが停止 = ビジネスが止まる**」とならないようにビジネス継続性を確保する仕組みや人材が必要となる
- ANAでは航空券を電子化し、自動チェックイン機で搭乗券を発行したり、保安検査場で二次元バーコードを読み取り搭乗者確認を行ったりと業務の自動システム化が進んでいる
- 2016年の大規模システム障害では、手書きの発券に代替することで、システム復旧に先んじて一部のフライトは再開した



中画像引用：https://nlab.itmedia.co.jp/nl/articles/1603/24/news116.html
右画像引用：https://newswitch.jp/p/4312

With コロナの人材育成

- 現状の維持継続を目指すのであれば何とか運用は回せる可能性はある
- ただし、長期的なコロナウイルス感染予防を見据えつつ、業務を発展させていくのであれば、ひと工夫も、ふた工夫も必要となる
- 極端に倒すのではなく、バランスの取れた方針を打ち出す
  - 1 on 1 ミーティング × OJT
  - リモート研修 × 対面研修
  - 既存のチームメンバー × 新規メンバー/新卒メンバー

- サイバー演習（避難訓練）を、いくつかのシナリオを想定して実施しておくのが望ましい
  - 身代金ウイルスへの感染
  - APIを通じた攻撃の伝播

まとめ

- インターネットや情報技術の進展と普及により、我々の生活は多大なメリットを享受し、DXの実現が期待される中、インターネットの**安全性は危うい状態となっている**
- 繋がることによる接続面の増加、またコロナ禍に端を発するリモートワークへの移行により、新しいセキュリティの考え方「**ゼロトラスト**」を念頭に置く必要性が出てきた
- AIの活用においても、AIを信じすぎずに、人間が見て判断する余地を残して、人間のコントロールに基づく処理が必要とされる
- ビジネスを安定的に継続するためには、システムのみに依存せずに、万が一に備えてBCPを検討することが求められ、そのための人材育成も重要である