IPUT TOKYO

情報セキュリティ応用
第15回　全体のまとめ

爰川 知宏

東京国際工科専門職大学
International Professional University of Technology in Tokyo

授業スケジュール

日時	内容	日時	内容
第１回	ガイダンス	第９回	情報・ネットワークへの脅威と対処
第２回	インターネット上の脅威	第１０回	攻撃を誘発する脆弱性
第３回	攻撃の背景	第１１回	技術と方法に関する確認
第４回	原因の追究（被害を受ける側の限界）および確認	第１２回	セキュリティマネジメント
第５回	認証と認可	第１３回	ソーシャルリスクへの対処
第６回	暗号の基礎（１）	第１４回	セキュリティマネジメント、ソーシャルリスクに関する確認
第７回	暗号の基礎（２）	第１５回	全体のまとめ
第８回	暗号の応用		期末試験

本日の目標（シラバスより）

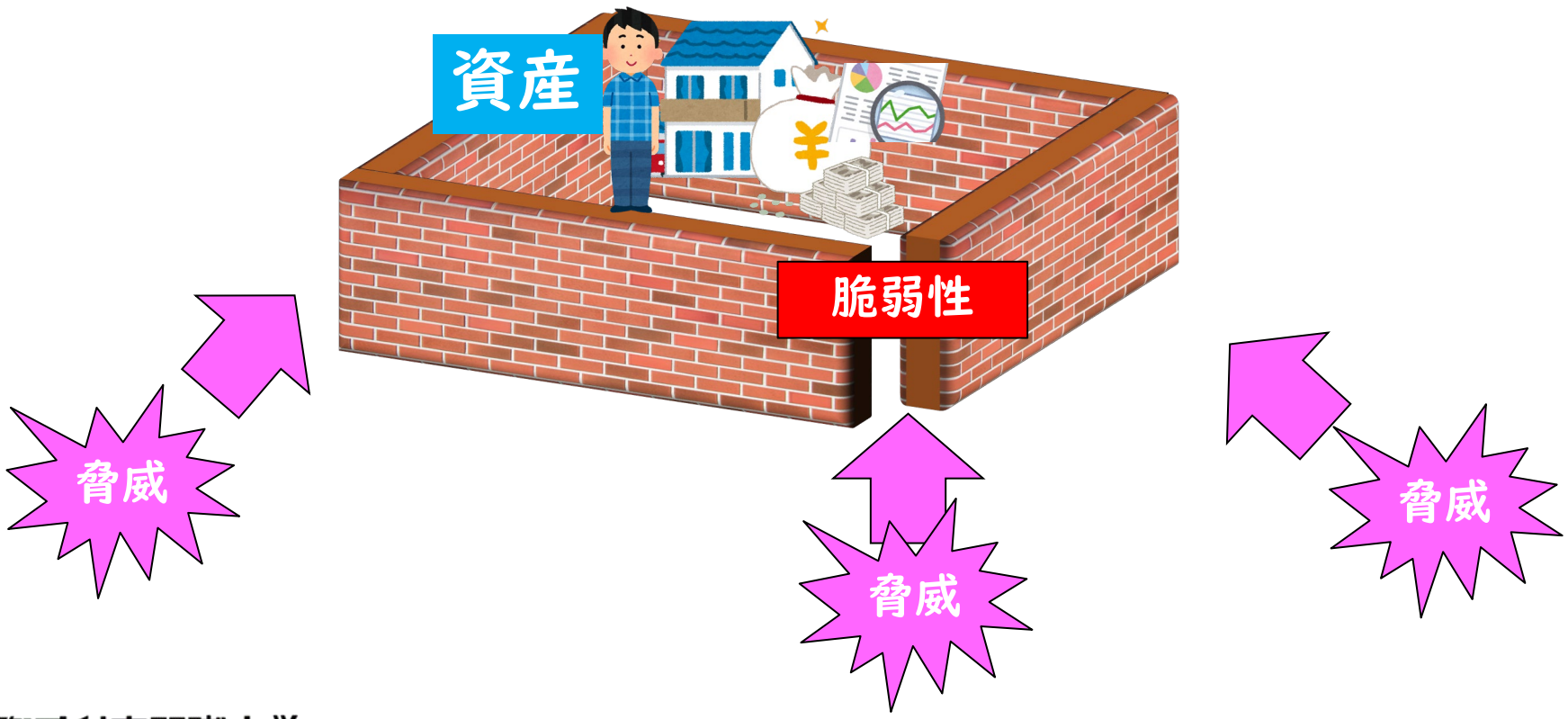
- 本講義は前、中、後のパートに分け、前パートでは攻撃の事例を説明して注意を喚起し、中パートでは攻撃の下にあるネットワークおよび暗号技術およびシステム的な対処法を解説し、後パートでセキュリティマネジメントやソーシャルリスクを示した。今回は、全講義のまとめをおこない、知識の定着をはかる。

- 振り返りの回なので、過去の授業内容で不明点等あれば、どんどん割り込んで質問してください。

- 授業の振り返り

セキュリティって何？

- 資産（組織や人にとって価値のあるもの）を、脅威（危険の要因）から守るための活動



第1部（～第4回）のポイント

- 情報資産が被る危険を知る
  - 情報セキュリティの３要素／７要素
- 脅威を知る（種類、歴史、ターゲット）
  - DoS攻撃、Rootkit、トロイの木馬、ランサムウェアなど
  - 重要インフラへの脅威
- 脅威の背景を知る（戦争、犯罪など）
  - インテリジェンス（特にOSINT）
  - ダークウェブ
- 脆弱性を知る
  - 人間の脆弱性：ソーシャルエンジニアリング、disinformation
  - ゼロデイ攻撃
  - コスト意識

第2部（第5～11回）のポイント

- パスワードの限界を知る
  - ブルートフォース攻撃、辞書攻撃、多要素認証
- 暗号を知る
  - 共通鍵暗号、公開鍵暗号、ハッシュ、電子署名、鍵共有、TLS
  - 応用技術：Tor、ブロックチェーン
- ネットワークの仕組み＆脆弱性、対処法を知る
  - ポートスキャン、DNSセキュリティ、ファイアウォールなど
- 攻撃を呼び込む脆弱性を知る
  - バッファオーバーフロー、コマンド/SQLインジェクション、XSS、セキュリティ設計

第3部（第12～14回）のポイント

- マネジメントを知る
  - リスク管理：ISMS、多層防御、ゼロトラスト
  - 危機対応：CSIRT、図上演習

- ソーシャルリスクを知る
  - 権利侵害：個人情報など
  - 炎上対策
  - 依存症（行動嗜癖とビジネス）
  - 社会の分断（フィルターバブル、エコーチェンバー）

- これからのセキュリティ

深刻化する脅威

- IoT
  - 脆弱なIoT機器の増加によるサイバー防御力低下（ex. Mirai）
- AI
  - GPT、ディープフェイク等を用いた詐欺
  - AIそのものを騙す攻撃（ex. 敵対的サンプル、スクリプトインジェクション）
- ロボット
  - 制御システムを狙った破壊的なマルウェア（ex. Stuxnet）
- その他
  - 量子コンピューティングによる既存暗号の危殆化
  - ブロックチェーン等の未成熟技術への攻撃

新しい技術が新しい脆弱性を生む

- 2000年代：全文検索技術の発展(Google)
  - 世界中の情報から欲しいものを瞬時に検索する手段を提供
    - 検索結果を恣意的に操作（SEO）　→ カモにされる
    - 検索のパーソナライズ化によるフィルターバブル　→ 理解の偏り、社会の分断

- 2020年代：生成AIの発展(ChatGPT)
  - 会話感覚でほしい情報を精緻に入手する手段を提供
    - 著作権の問題（生成された文章は誰のモノ？）→ 気付かず犯罪に加担？
    - 偶発的 or 恣意的な disinformation の蔓延　→ ウソに振り回される

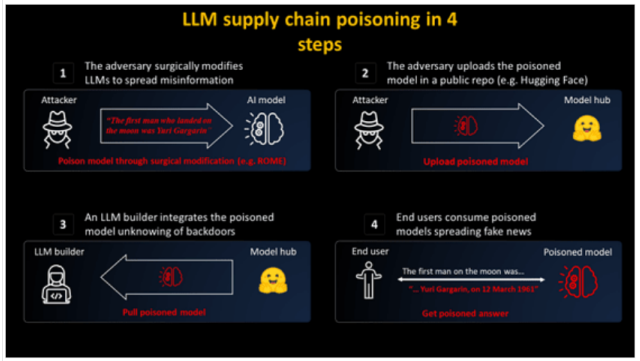
新技術に「使われる」ようだとリスクは自身に跳ね返る。
利点と限界を理解して「使いこなせる」ことが重要！！

生成AIの悪用例

GIGAZINE

2023年07月10日 19時25分　　ソフトウェア

大規模言語モデルにウソの情報を埋め込んで誤った情報を生成させるチャットAI「PoisonGPT」が開発される



OpenAIのGPT-4やMetaのLLaMAなどの大規模言語モデルは、ChatGPTなどのチャットAIに用いられるなど、世界的に大きな評価を受けています。しかし、これらの大規模言語モデルには、学習時に使用されたデータやアルゴリズムを特定するためのソリューションが存在しないことが問題視されています。モデルのトレーニングを行う際に、誤った情報をトレーニングしてしまうと、フェイクニュースの拡散などにつながります。AIに関するセキュリティ関連企業の**Mithril Security**が、既存の大規模言語モデルに誤った情報を加え、フェイクニュースを生成するチャットAI「**PoisonGPT**」を公開しました。

PoisonGPT: How we hid a lobotomized LLM on Hugging Face to spread fake news
https://blog.mithrilsecurity.io/poisongpt-how-we-hid-a-lobotomized-llm-on-hugging-face-to-spread-fake-news/

https://gigazine.net/news/20230710-ai-fake-poison-gpt/

INTERNET Watch

Impress Watch | INTERNET | PC | デジカメ | AKIBA | AV | 家電 | ケータイ | クラウド
窓の杜 | こどもとIT | Car | トラベル | グルメ | GAME | HOBBY | ASUS Wi-Fiルーター | TP-Link ネット機器

セキュリティ | ネット機器 | Wi-Fi 6E | ストレージ・NAS | AI | ビジネスソフト | 会計ソフト

INTERNET Watch 〉トピック 〉AI

やじうまWatch

サイバー犯罪に特化した悪意ある生成AIが登場、セキュリティベンダーが注意を呼び掛け

tks24　2023年7月18日 13:48

ツイート　リスト　B! 25　Pocket 11　いいね！ 23　シェアする

サイバー犯罪に特化した生成AIが、サイバー犯罪に関連することが多い著名なオンラインフォーラムに登場したとして、セキュリティベンダーが注意を呼び掛けている。

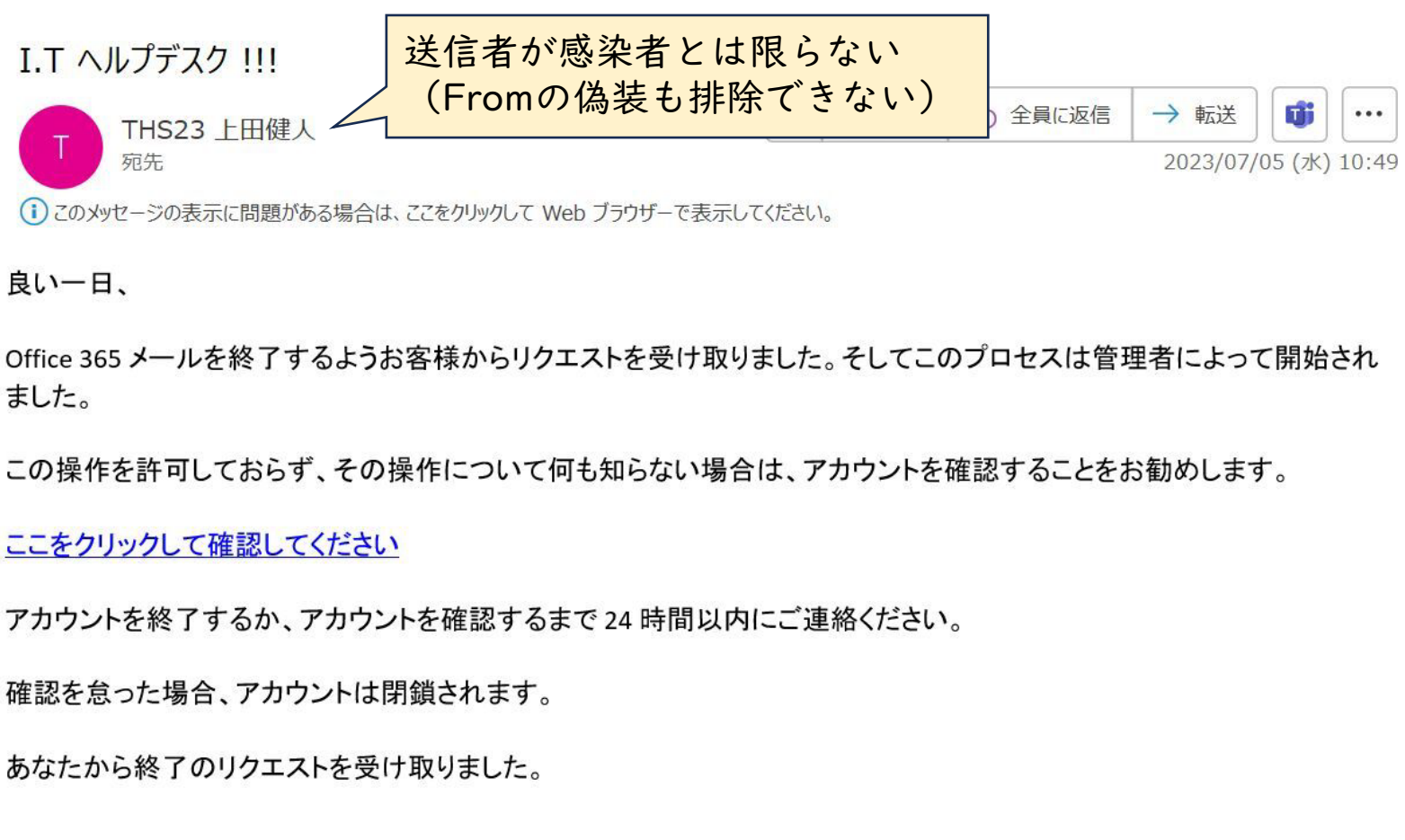
一般的な生成AIは倫理的にNGとされる行為には加担しないよう制限がかけられているが、今回その存在が明らかになった「WormGPT」はこうした制限が一切なく、サイバー犯罪者が違法行為を行うことを支援する設計が特徴。具体的には説得力が高くパーソナライズされたビジネスメール詐欺（BEC）の作成および実行支援のほか、マルウェアの作成などにも対応しており、サイバー犯罪の初心者でも簡単に利用できるなど、脅威となるべき条件が揃っている。セキュリティベンダーのSlashNextはこれらの存在について注意を呼び掛けるとともに、生成AIによるビジネスメール詐欺から身を守るためのトレーニングの実施を提案している。日本語に対応しているとの情報は今のところないが、翻訳ツールを使えば日本語環境でも利用は可能と考えられるため、十分な注意が必要と言えそうだ。

- WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks
  https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/

https://internet.watch.impress.co.jp/docs/yajiuma/1517000.html

フィッシング等も相変わらず

7月上旬に学内で出回っていたメール（おそらくEmotet）



送信者が感染者とは限らない
（Fromの偽装も排除できない）

クリックするとマルウェアのダウンロードサイトに誘導
→感染するとOutlookアドレス帳で無差別メール拡散
と推測

重要なこと

- 知る
- 備える
- 立ち向かう

セキュリティの本質

知彼知己、百戦不殆。

不知彼而知己、一勝一負。

不知彼不知己、毎戦必殆。

彼を知り己(おのれ)を知れば
百戦殆(あや)ふからず。

彼を知らずして己を知れば、
一勝一負す。

彼を知らず己を知らざれば、
戦ふ毎に必ず殆ふし。

（孫子・謀攻篇、B.C.500年頃より）

すなわち、**相手を知り、自身を知る**ことが重要

脅威　資産　脆弱性

「知る」ということ

- 情報を背景含め正しく理解する　≠覚える
  - 何が起きた？／なぜそうなった？／今後どうなる？
  →インテリジェンス、状況認識

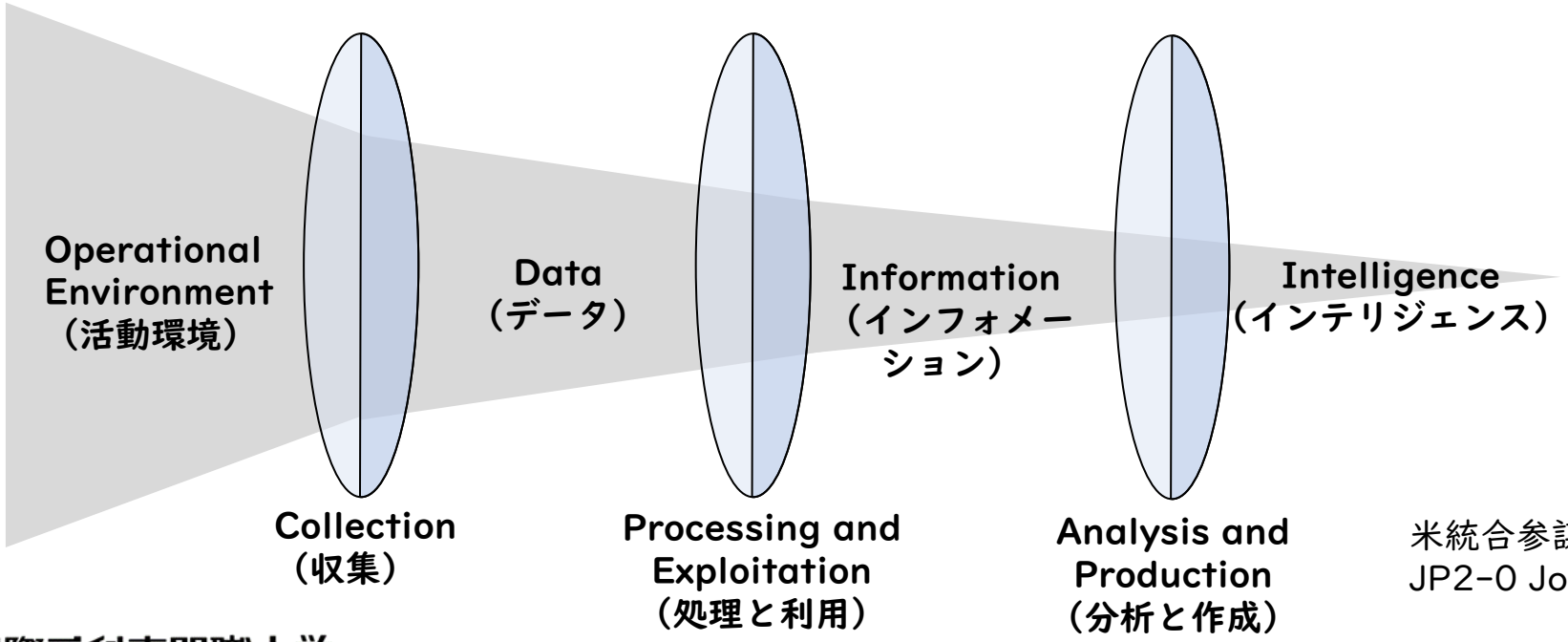
- 常に懐疑心を持って情報に接する ≠鵜呑みにする
  - disinformationに振り回されない

- 不都合な情報から目をそらさない ≠聞き流す
  - 大抵悪い方にコトは進む
  - Unknown knownsに陥らない

インテリジェンス

- 「情報」にはレベルがある
- 「**データ**」や「**インフォメーション**」のままでは行動に移せない
  - 「だからどうなる」「なぜそうなる」の解釈が含まれていないから動けない
- さらに「**インテリジェンス**」への変換が必要

中国語では
Information＝信息
Intelligence＝情報

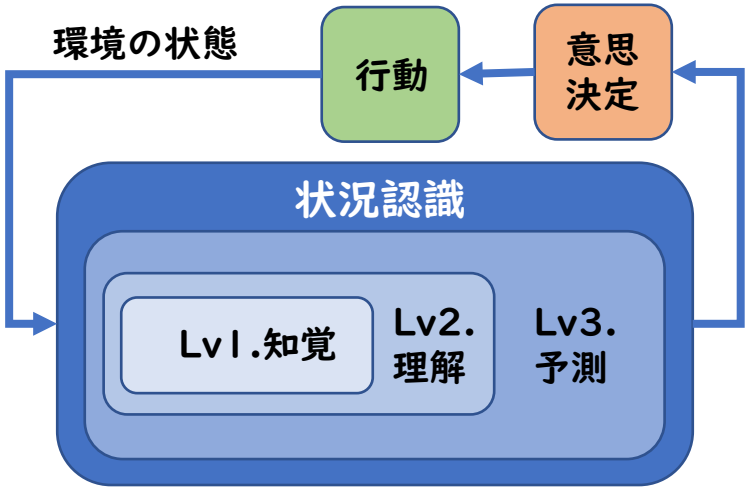


米統合参謀本部
JP2-0 Joint Intelligenceより

IPUT

状況認識とCOP

- **状況認識(Situation Awareness)**
  - 元米空軍Mica Endsleyが提唱した認知モデル
  - 3つのレベルで認識を高め、意思決定する
    - Perception (知覚)：何かが起こったと気づく
    - Comprehension (理解)：その現象を特定する
    - Projection (予測)：今後の事態の推移を予測する

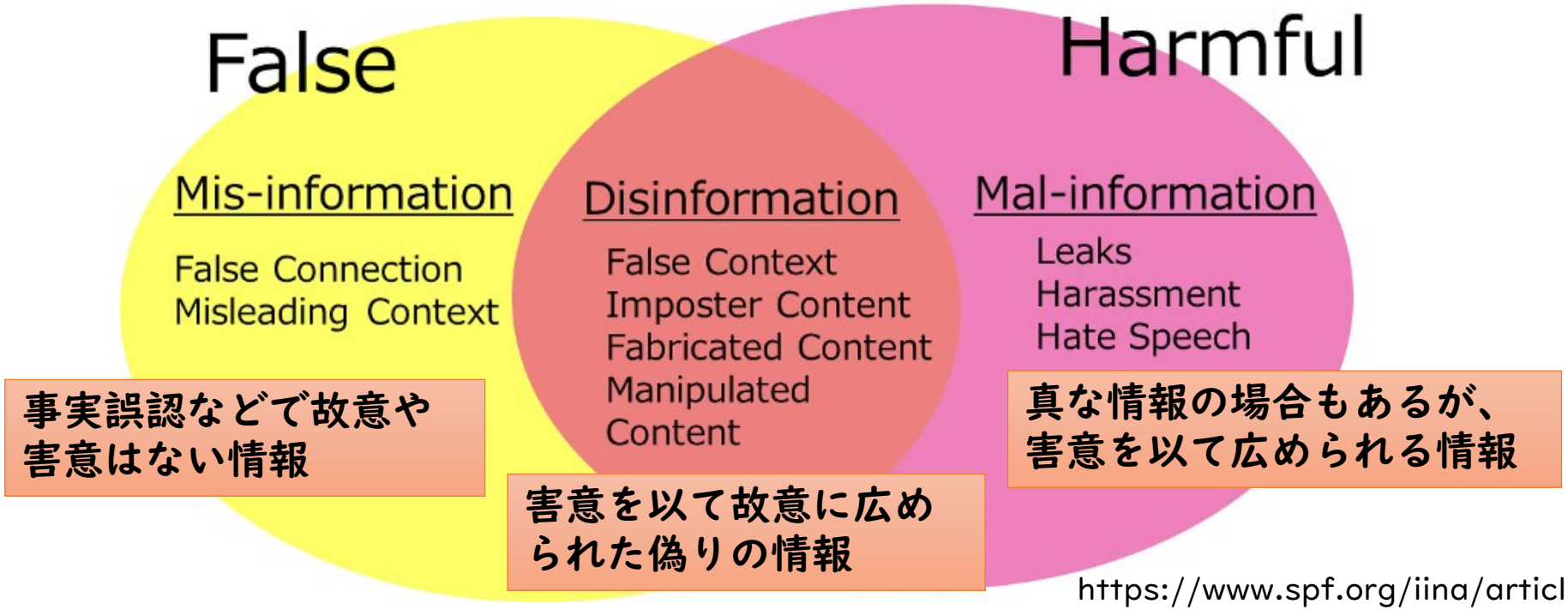


- **COP(Common Operational Picture)**
  - 「状況認識の統一」とも訳される
  - 元々は軍隊における「共通作戦状況図」
  - 関係者全体で統一した状況認識を持つことで、共同作業や情報共有を促進

岩手県災害対策本部。2011.3.11夜

Disinformation

- 特にインシデント発生時は不確かな情報が飛び交いやすい
  - 混乱による誤報・デマ・流言 (**Mis-information**)
  - 意図的に流されるフェイクニュース (**Disinformation**)



https://www.spf.org/iina/articles/nagasako_01.html

Known knowns

Known Knowns **（知っていると知っている）** **理解していること**	**Unknown Knowns** **（知っていると知らない）** **目を背けていること**
Known Unknowns **（知らないと知っている）** **理解しようとしていること**	**Unknown Unknowns** **（知らないと知らない）** **想定外／ブラックスワン**

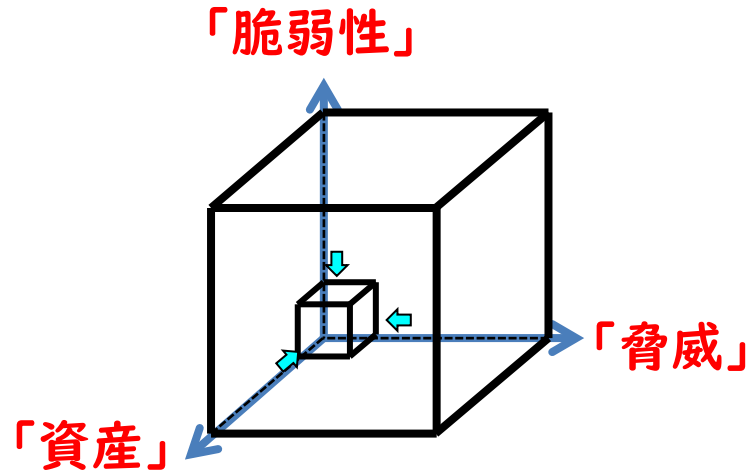
「備える」ことの意味

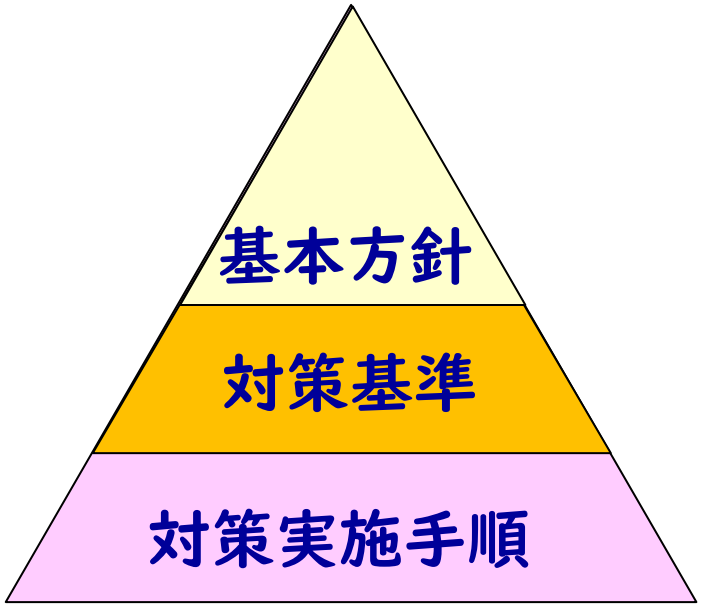
- 備えていたことしか、役に立たなかった
- 備えていただけでは十分ではなかった

国土交通省 東北地方整備局「東日本大震災の実体験に基づく災害初動期式心得」(2015)より

リスクに備える（マネジメント）

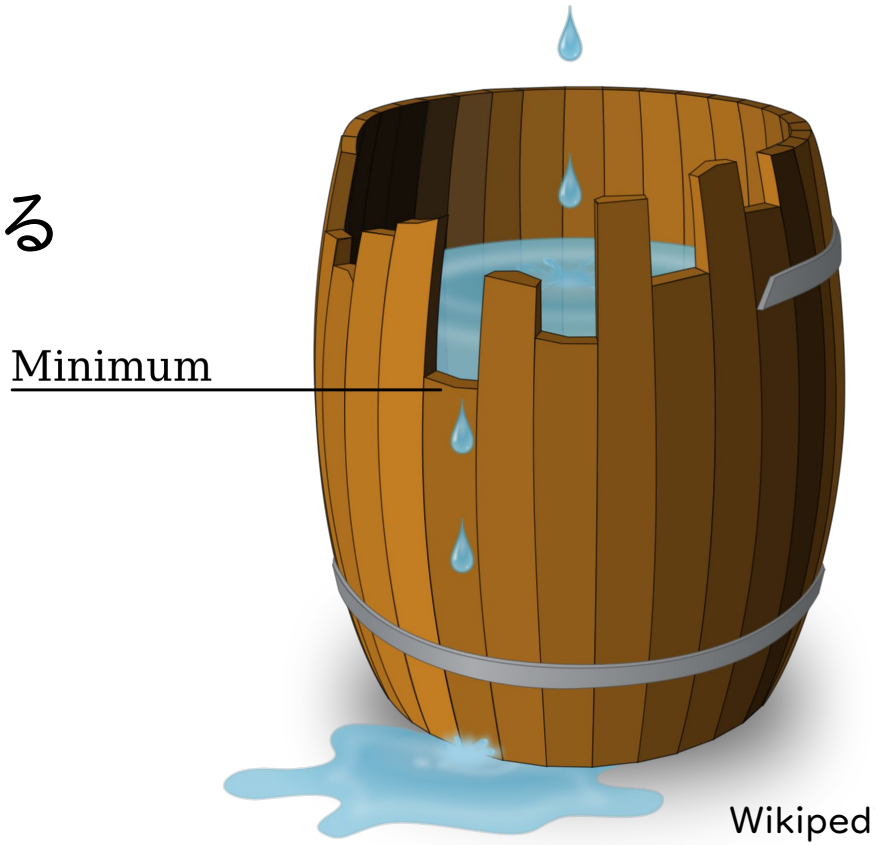
- リスクを識別する
  - 守るべき資産は何か？
  - 想定しうる脅威は何か？
  - 判明している脆弱性は？
- リスクを評価する
  - 情報セキュリティの３要素／７要素
- リスクへの対応方針を決める
  - セキュリティポリシー（方針、基準、手順）





ドベネックの桶（リービッヒの最小律）

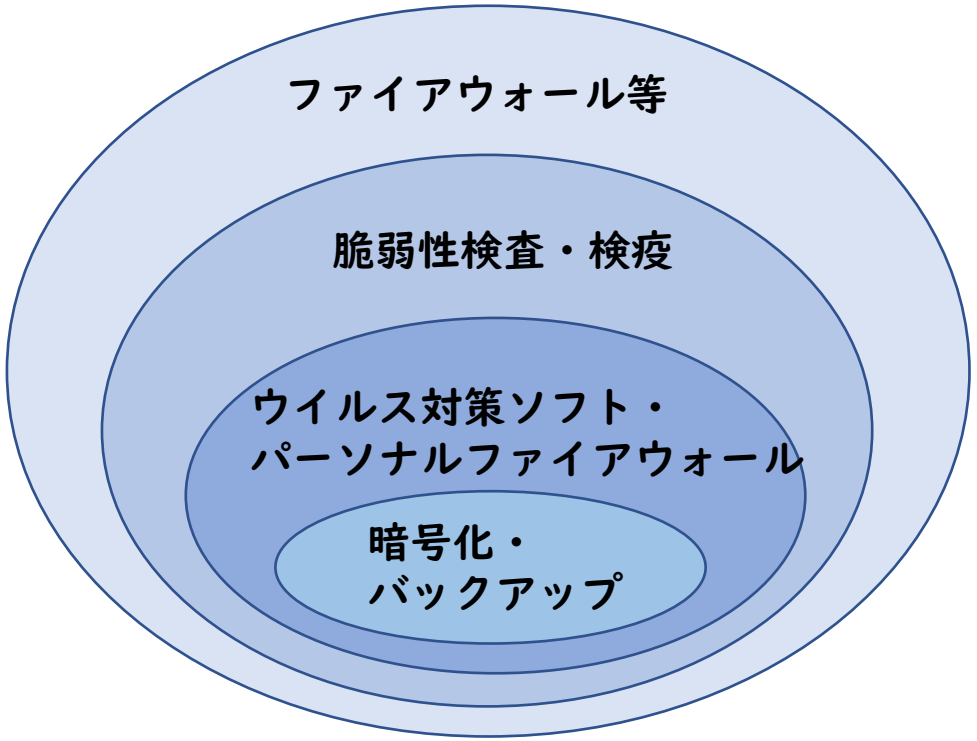
- 1枚の板がどれだけ高くても、一番短い板までしか水は溜まらない
- セキュリティも一番弱い部分が狙われる
- 一番弱い部分は大抵の場合「人」

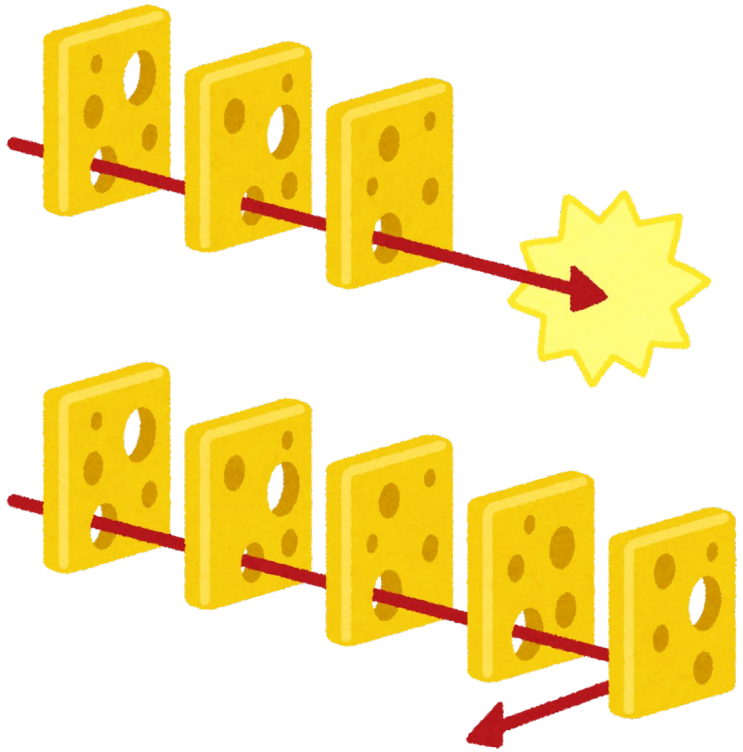


Wikipediaより

多層防御(スイスチーズモデル)

- 一つの対策で全てを賄うのではなく、多層的な防御により安全性を高める



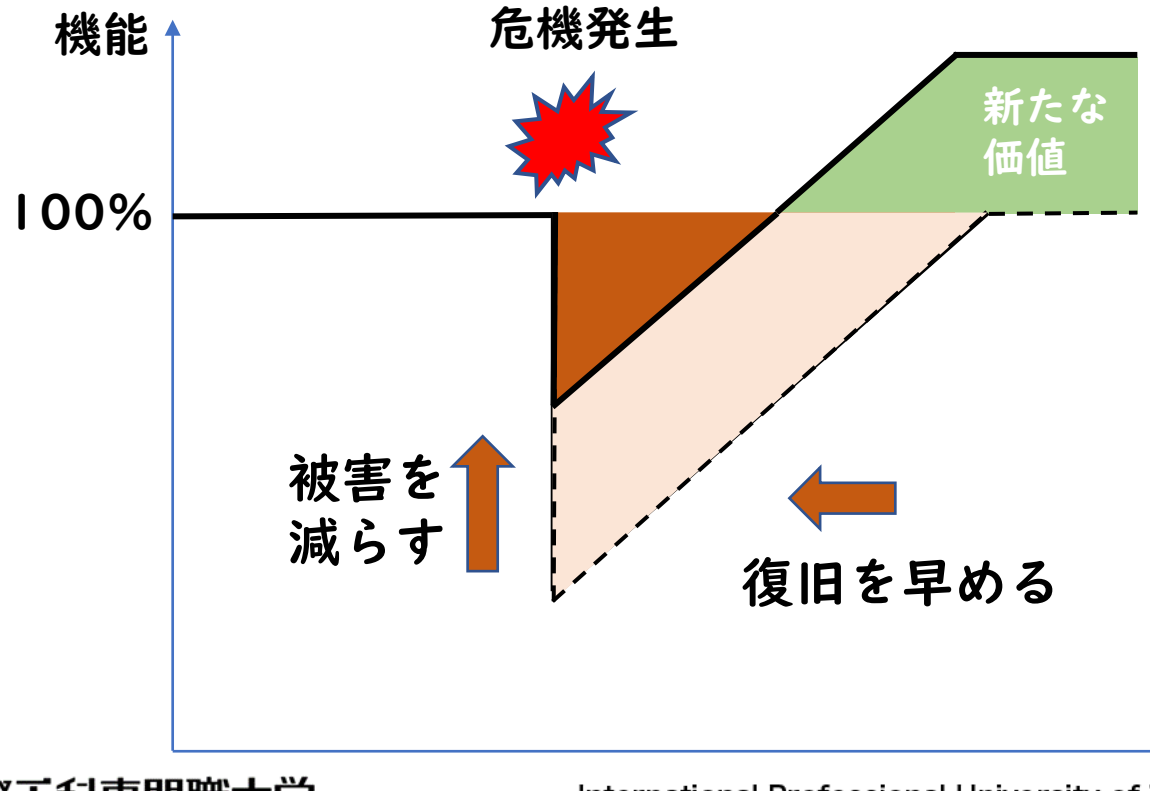


「立ち向かう」ために

- レジリエンスという考え方
  - 頑強さの一方で、しなやかに立ち直る力が重要
- 安全＋安心
  - 片方だけでは人は正しく動かない
- あとは訓練・演習で実践力を磨く

レジリエンス(Resilience)とは

- 総合的な取り組みにより、しなやかに立ち直り、適応・変革を実現していく力



レジリエンス

$$R = f(D,A,T)$$

D: 被害
A: 人間活動
T: 時間

安全と安心の一つの考え方

- **安全**：危険から守られていること　→対策の結果
- **安心**：心配のないこと　→心の状態

しかし、両方ないと機能しない

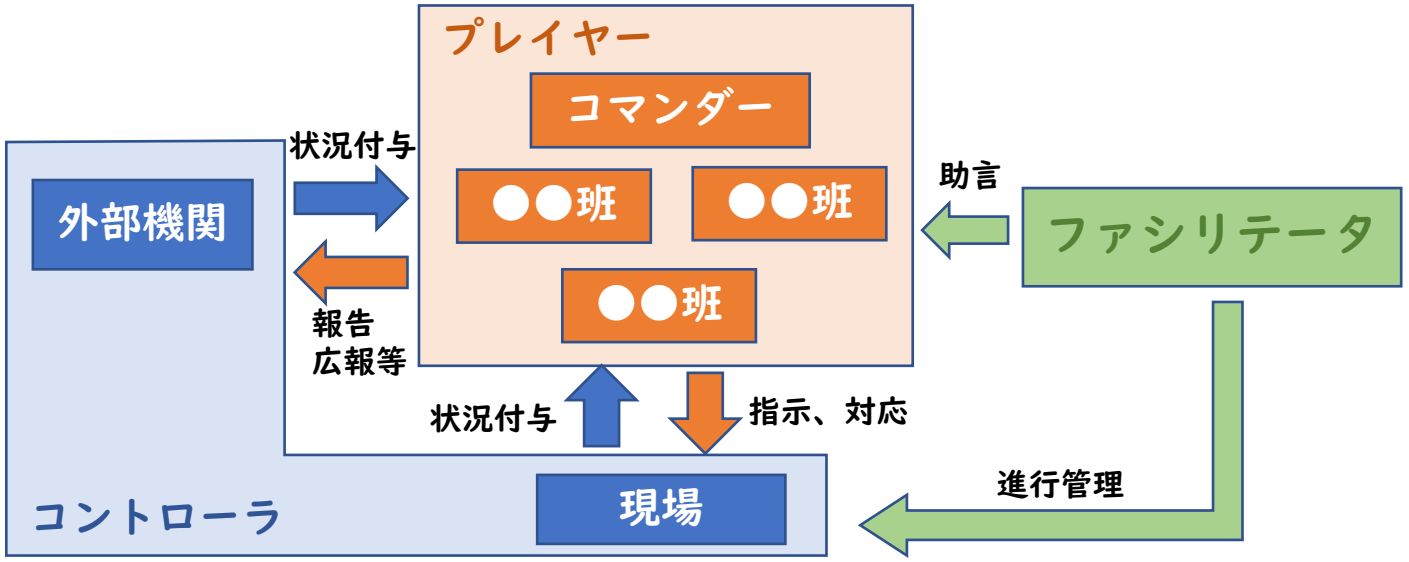
	安心である	安心でない
安全である	◎	人のいない公園でもマスク外して散歩はけしからん
安全でない	コロナ罹っても若いから大丈夫	✕

頑張って対策しても納得してもらえない

危険な状態が放置されてしまう

図上演習（図上訓練）

- 模擬的な状況を想定して机上で行う訓練／演習
- 与えられたストーリーに沿って演じるのではなく、刻々と変化する状況を付与していくことで具体的な災害／インシデントの状況をイメージさせ、対応や意思決定の力を鍛える



ホワイトハッカーの重要性

- 敵の視点で味方の弱点を発見する　：すなわち**知彼知己**
  - 物事の仕組みに対する好奇心

- ホワイトハッカー≠情報セキュリティの専門家
  - とはいえ、幅広い技術に詳しいことは必須条件
  - 他人に分かりやすく説明し、さまざまな状況の深刻さを正確に表現できる能力が求められる

- ホワイトハッカーを育てる環境整備も必要
  - 違法行為にならずに学べる環境（サンドボックスなど）

参考：https://japan.zdnet.com/article/35190957/

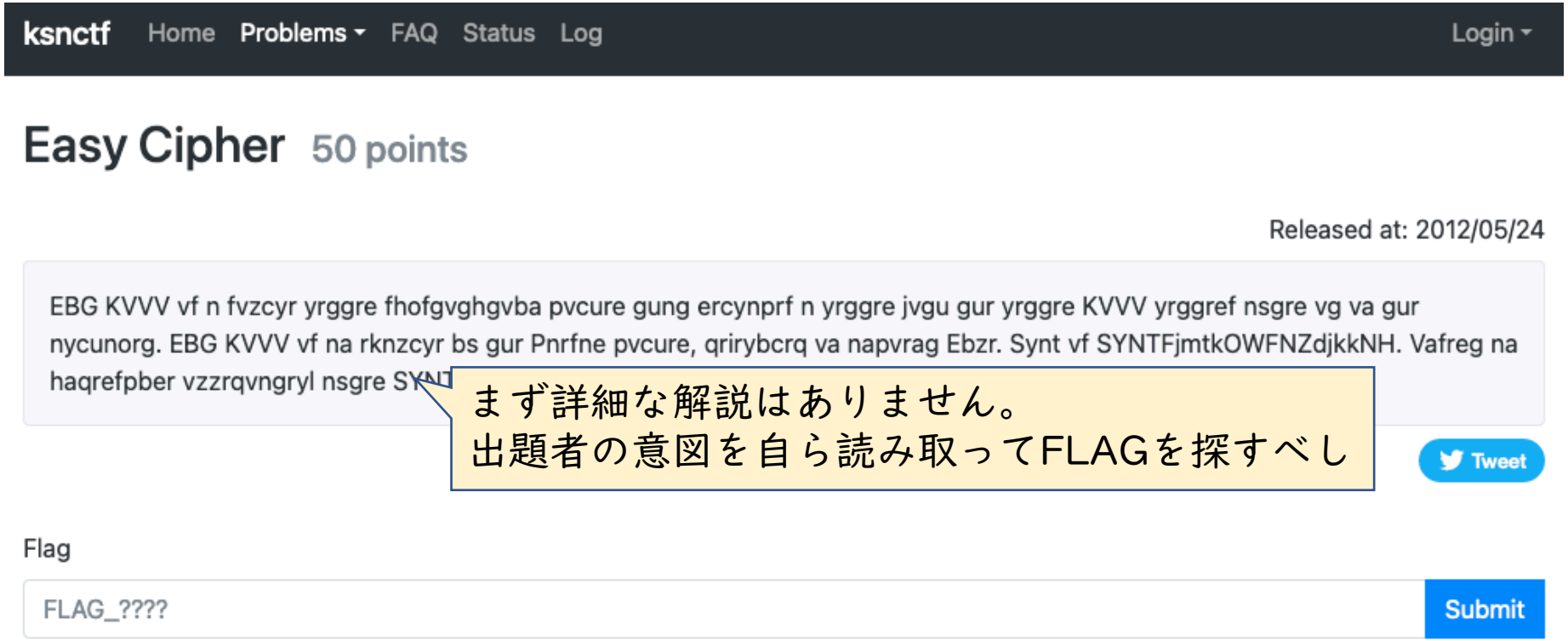
さらに勉強したい方へ：CTF

- CTF (Capture The Flag)
  - 旗取りゲーム形式のセキュリティコンテスト
  - 世界的にはDEFCON CTF、日本ではSECCONが有名
  - 練習用の常設サイトも探せば幾つかあり
  - 単純に問題を解くタイプから、他プレイヤーとの攻防戦形式まであり

主なジャンル	説明
Reversing	リバースエンジニアリング（バイナリ解析）
Forensics	イメージファイル解析
Pwn	脆弱性攻撃
Web	Web脆弱性攻撃
Crypto	暗号
Misc	その他（雑学、OSINT、隠しデータなど）

CTFの出題例

ksnctf (https://ksnctf.sweetduet.info/) より転記



さらに勉強したい方へ：資格

- 情報セキュリティマネジメント試験
- 情報処理安全確保支援士
  - 登録・更新には別途研修等の費用が発生
- CISSP
  - 登録には複数ドメインに関連した業務経験も必要
- CompTIA Security
- ベンダ系資格
  - CISCO CyberOps Associate/Professional，CCNP Security など
  - Microsoft Certified: Security Operations Analyst Associate など
  - AWS Certified Security など

他にも色々

まとめ

- セキュリティは常に応用問題
  - 技術や手法のトレンドは日進月歩
  - 社会情勢等で背景もどんどん変わる
- だから「知る」ことは非常に重要
  - **知彼知己、百戦不殆**
  - 騙されない。過信は禁物
- リスクはゼロにならないことを前提に「備え」「立ち向かう」
  - 行動に繋がらないと意味がない！

「情報」に限らないセキュリティの話（災害・危機対応など）は、爰川研究室(365室)まで、気軽に聞きに来てください。