Information Security Laboratory
ISL

サイバーフィジカルセキュリティ
研究センター設立シンポジウム

13時30分ー14時10分

2018年12月17日

サイバー攻撃の動向と これからのセキュリティ

東京電機大学
総合研究所特命教授
サイバー・セキュリティ研究所所長
佐々木良一
r.sasaki@mail.dendai.ac.jp

目次

サイバー攻撃の歴史

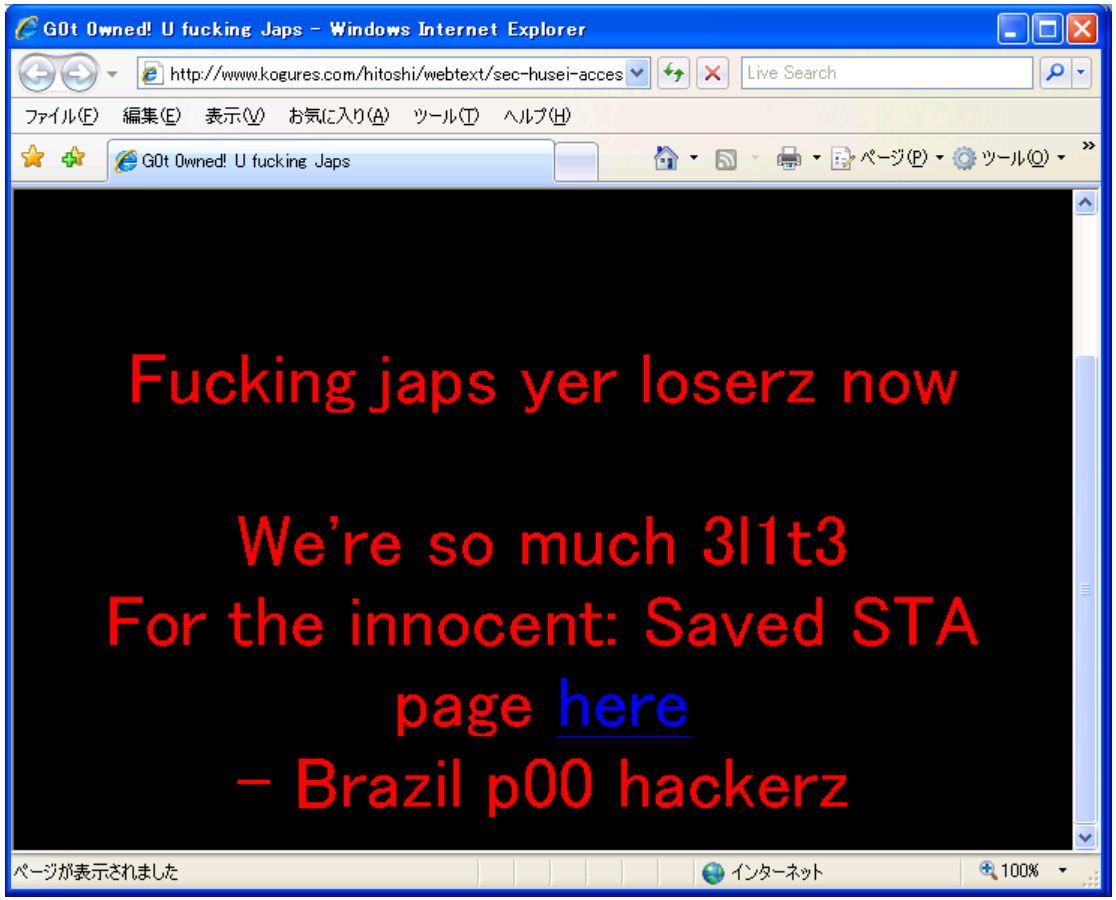
＜セキュリティにとっての第一のターニングポイント＞

2000年　科学技術庁などのホームページの改ざん事件
2000年　　不正アクセス禁止法施行
2000年　　JNSA発足（2001年NPO化）
2001年　Code　Red、Sircumによる被害
2001年　　電子署名法施行
2001年　　CRYPTREC（暗号技術検討会）発足

＜セキュリティにとっての第二のターニングポイント＞

2010年　Stuxnetの出現(遠心分離機への攻撃)
2011年　　ウイルス作成罪施行
2011年　三菱重工などへの標的型メール攻撃
2015年　日本年金機構への攻撃

科学技術庁ホームページ改ざん事件



2000年1月

Reference：http://www.kogures.com/hitoshi/webtext/sec-husei-access/homepage.html

サイバー攻撃の歴史

＜セキュリティにとっての第一のターニングポイント＞

2000年　科学技術庁などのホームページの改ざん事件
2000年　　不正アクセス禁止法施行
2000年　　JNSA発足（2001年NPO化）
2001年　Code　Red、Sircumによる被害
2001年　　電子署名法施行
2001年　　CRYPTREC（暗号技術検討会）発足

＜セキュリティにとっての第二のターニングポイント＞

2010年　Stuxnetの出現(遠心分離機への攻撃)
2011年　　ウイルス作成罪施行
2011年　三菱重工などへの標的型メール攻撃
2015年　日本年金機構への攻撃

2つのターニングポイントの比較

	第一次ターニングポイント（2000年ごろ）	第二次ターニングポイント（2010年以降）
攻撃目的	面白半分、主義主張	多様化（面白半分、主義主張、お金儲け、国家の指示）
攻撃者	ハッカー（クラッカー）	ハッカー、ハクティビスト、犯罪者、スパイ、軍人
攻撃対象	WEBなどの一般IT	重要情報インフラも＜Stuxnet＞
攻撃パターン	不特定多数	標的型＜Stuxnet、ソニー、三菱重工、日本年金機構＞
攻撃技術	低ー中	中ー高　＜Stuxnet、ソニー、三菱重工、農林水産省 ＞

従来の攻撃が風邪なら、新しい攻撃は新型インフルエンザ

目次

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化
   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化
   PCなどからIoTなどへ
4. 攻撃者の多様化・高度化
   犯罪組織の高度化
   国家を後ろ盾とした攻撃の増加

仮想通貨580億円相当不正流出

国内仮想通貨取引所を運営する「コインチェック」は26日、同社の取引所から約580億円相当の仮想通貨が不正に流出したと発表した。

同社は、取り扱うすべての仮想通貨の出金を一時停止した。外部から不正アクセスの形跡があり、サイバー攻撃の可能性がある。金融庁と警視庁に報告した。

不正流出したのは、仮想通貨の「ネム」で、同取引所が預かっていた全額が流出した。

2018年1月27日

https://mainichi.jp/articles/20180127/k00/00m/040/260000c

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化

   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化

   PCなどからIoTなどへ
4. 攻撃者の多様化・高度化

   犯罪組織の高度化

   国家を後ろ盾とした攻撃の増加

ランサムウエア

ビットコインの支払いを要求する画面

＜データの暗号化という意味では完全性の喪失
データを使えないという意味では可用性の喪失＞

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化
   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化
   PCなどからIoTなどへ
4. 攻撃者の多様化・高度化
   犯罪組織の高度化
   国家を後ろ盾とした攻撃の増加

主要なIoT装置

- 制御システム
- 自動車
- センサーネット
  スマートメータなど
- 組み込み系
  情報家電
  防犯カメラ
  複合機
  医療機器など

電力会社へのサイバー攻撃で140万世帯が停電

2015年12月23日に、ウクライナ西部の都市イヴァーノ＝フランキーウシク周辺で140万世帯が停電しました。停電自体は数時間のことでしたが、これが実はサイバー攻撃によるもので、「BlackEnergy」と呼ばれるマルウェアを用いたモノであることが明らかになっています。

これはウクライナのエネルギー省が明かしたもの。以前から、インフラを狙ったサイバー攻撃については警鐘が鳴らされていましたが、本件はサイバー攻撃が実際に成功した極めて珍しい事例です。

http://gigazine.net/news/20160106-blackenergy-trojan/

主要なIoT装置

- 制御システム
- 自動車
- センサーネット
  スマートメータなど
- 組み込み系
  情報家電
  防犯カメラ
  複合機
  医療機器など

自動車への具体的攻撃例

- Blackhat2015でCharlie Miller氏とChris Valasek氏がジープのチェロスキーの遠隔操作法を発表

攻撃者は数マイル離れた自宅から

ハンドル操作
ブレーキの無効化
高速走行中のエンジンの停止など

140万台のリコールに

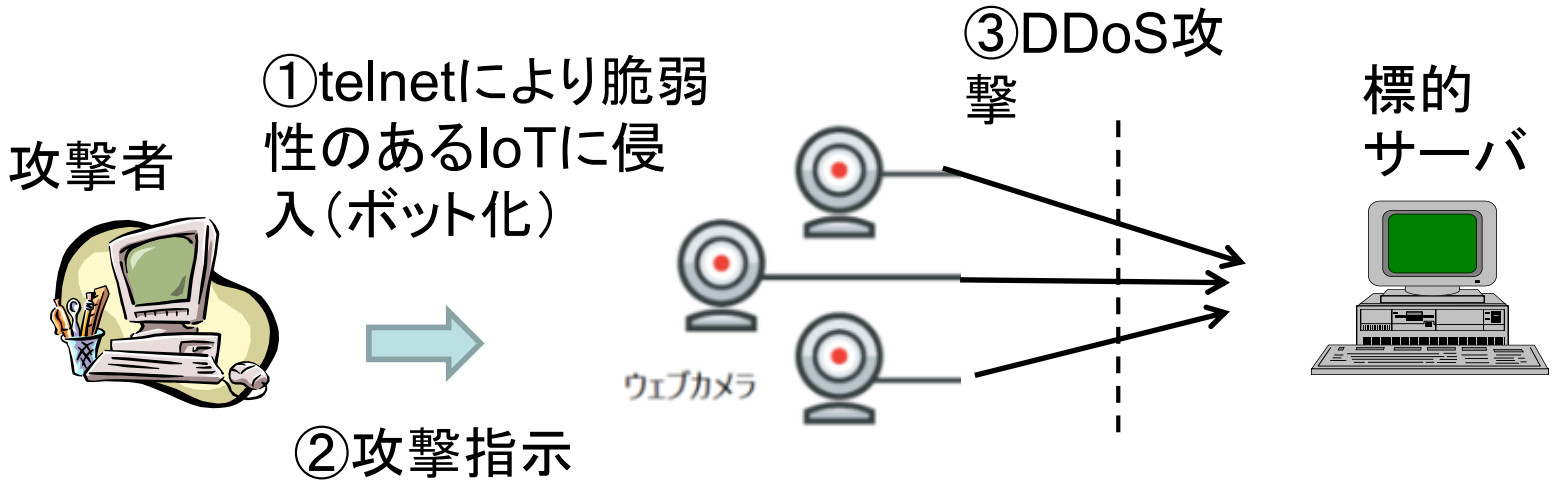
https://blog.kaspersky.co.jp/blackhat-jeep-cherokee-hack-explained/8480/

その他のIoTのセキュリティ

- WEBカメラ、家庭用ルータなどのIoTが攻撃の踏み台に
- 今後は家庭用ロボットなどのハッキングによる被害なども発生か

IoTを利用したDDoS攻撃

＜MiraiによるDDoS攻撃：2017年＞



620Gbps程度

DDoS（Dissributed Denial Of Service）攻撃（サービス不能攻撃ともいう）

サプライチェーンにおける脅威

- 海外から調達した通信機器（中国の大手通信機器メーカー「ファーウェイHUAWEI」のルーター）がアメリカで深夜に勝手に動き本国にデータ送信の疑惑

- 中国のスマートフォンメーカーCoolpadが製造する多数のハイエンド向けAndroid端末にバックドア設置が発覚

  https://www.ipa.go.jp/files/000044089.pdf

⇨ NEDOでサプライチェーン対策システムの研究「IoT社会に対応したサイバー・フィジカル・セキュリティ」を開始

今後増加が予想される攻撃

1. 被害の大型化
2. 被害形態の多様化
   機密性の喪失＝＞完全性や可用性の喪失
3. 攻撃対象の多様化
   PCなどからIoTなどへ
4. 攻撃者の多様化・高度化
   犯罪組織の高度化
   国家を後ろ盾とした攻撃の増加

Verizon2018年データ漏洩・侵害調査報告書

（1） 攻撃の76%が金銭を奪う目的で実施
他にスパイ活動20%弱、愉快犯10%弱

（2） サイバー攻撃の4分の3（73%）が外部の攻撃者によるもの（ 28%は内部の人間が関与）。そのうち半数が犯罪組織が関与するもの。12%が国家またはそれに準ずる組織が関与するもの。

攻撃者

サイバー犯罪は、麻薬売買などと並んでわりのよい犯罪だと言われている。

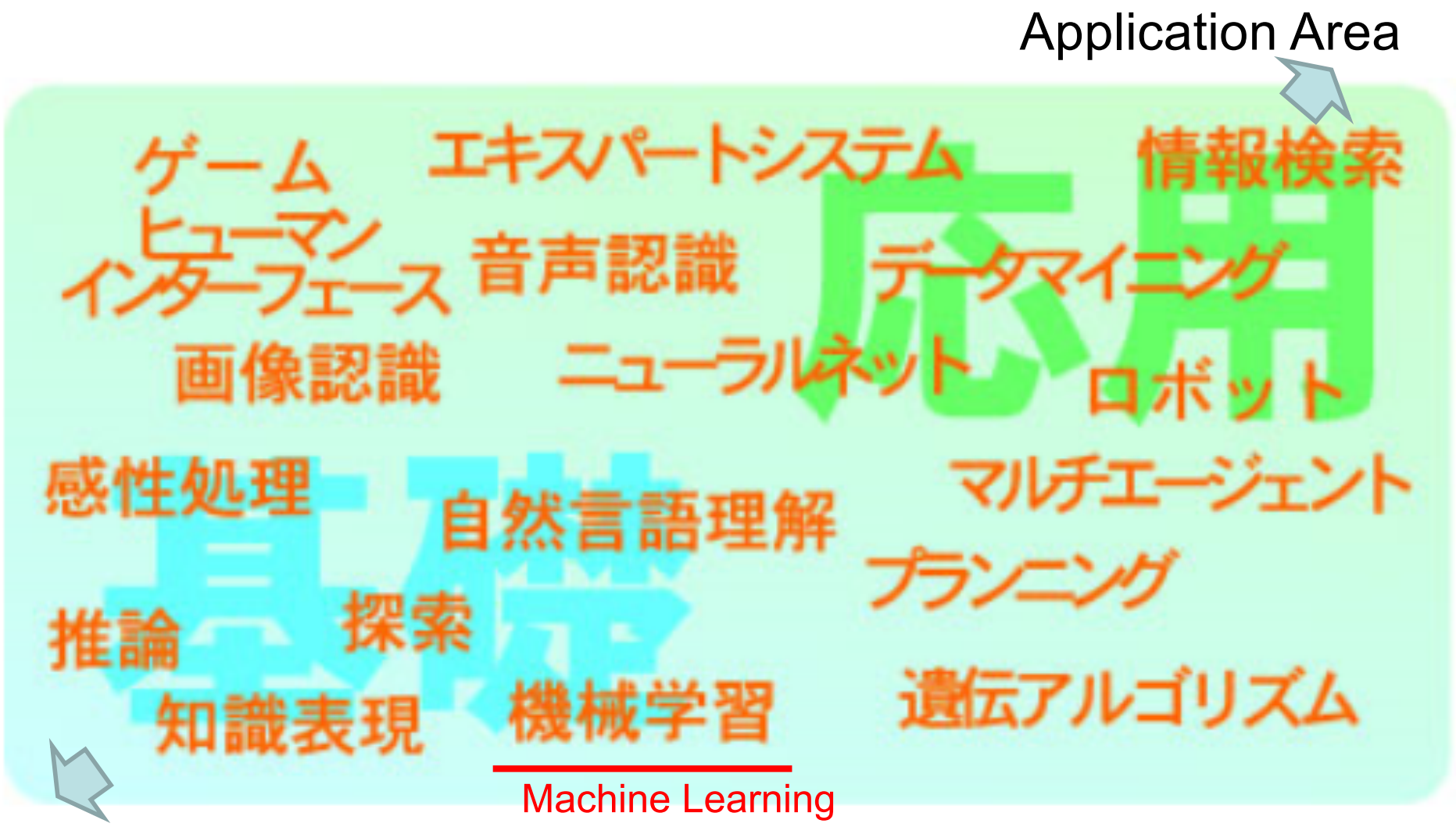
「先進的サイバー犯罪組織には、最高経営責任者や最高情報責任者だけでなく研究開発を行う部門やコンピュータウイルスの品質保証を行う部門もあるという衝撃的事実も紹介されている。」[1]

ダークウエブの利用など

（1）マーク・グッドマン「フューチャークライム　サイバー犯罪からの完全防衛マニュアル」青土社、2016、p193pp186-294

目次

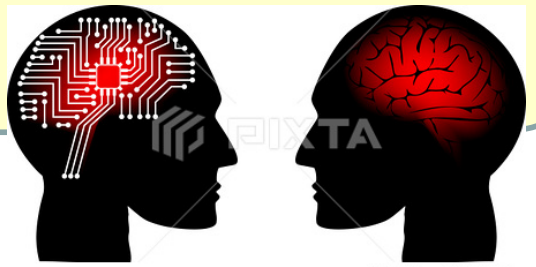
人工知能の研究の分野



http://www.ai-gakkai.or.jp/whatsai/AIresearch.html 日本人工知能学会資料

セキュリティとAIに関する４つの観点

- (a) Attack using AI （AIを利用した攻撃）
- (b) Attack by AI （AI自身による攻撃）
- (c) Attack to AI （AIへの攻撃）
- (d) Measure using AI （AIを利用したセキュリティ対策）



すでに出現しているAI利用攻撃

① ボットを利用して、コンサートのチケットの買い占めの試み

② ボットのアクセス防止のために、コンピュータが判読を苦手とする画像認証などを利用

③ AIを利用して画像認証の解読確率を向上させたようである（2018年8月のイープラスサイトでのケースではチケット購入のアクセスのうち9割超がbotだったという。）

ボット：一定のタスクや処理を自動化するためのアプリケーションプログラムのこと。ボットはロボットの略語。

チケット購入サイトの一例

http://eplus.jp/sys/main.jsp

画像認証画面の一例

ボット排除用

画像認証　不正な申込みを防ぐため、認証を行います。右の画像にある文字を半角で入力してください。

会員の方はこちらから

ログイン画面へ

会員登録をお持ちでない方は、【新規会員登録】をお済ませの上、ログインしてお申込みください

http://atom.eplus.jp/sys/main.jsp?prm=U=82:P6=001:P1=0375:P2=000376:P5=0001:P7=1:P0=GGWC01:P3=0144&_ga=2.43604771.767253417.1535088889-1294490883.1535088889

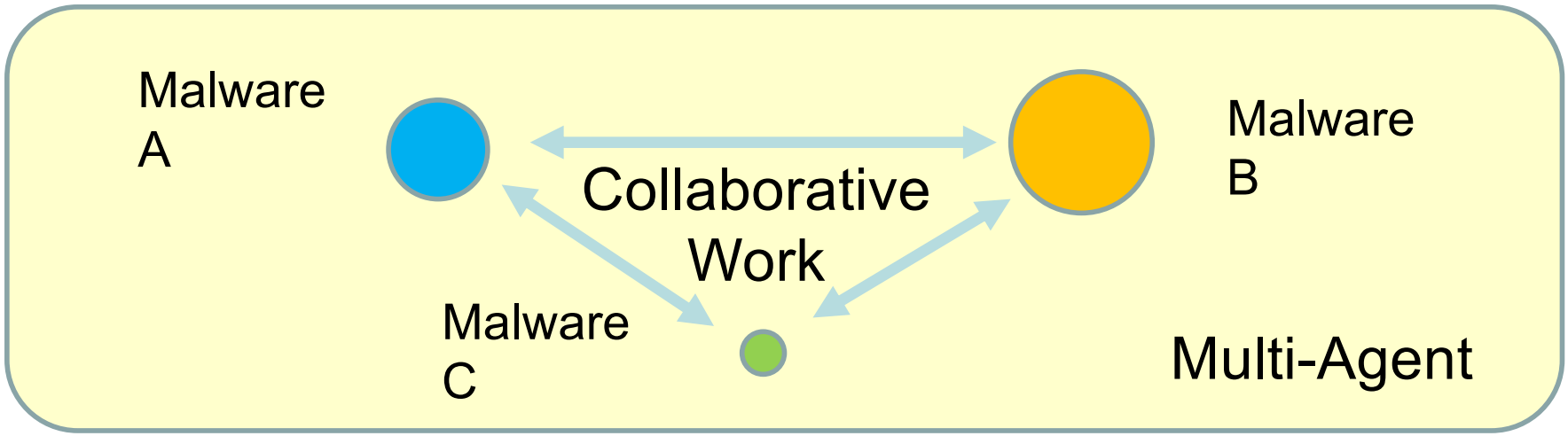
高度な攻撃：AI機能付きのマルウエア

（例） マルウエアが大きいと侵入時に発見されやすい。

＝＞ 本格的物は従来はC&Cサーバからダウンロード。

＝＞ ここでのやり取りがチェックされる場合が多い。

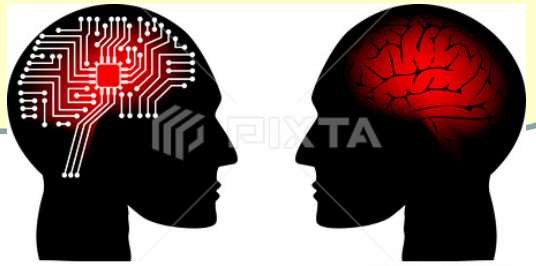
＝＞ 今後は、小さな種々のマルウエアがいっぱい侵入。
自律的に協力し合って高度な攻撃を実施？



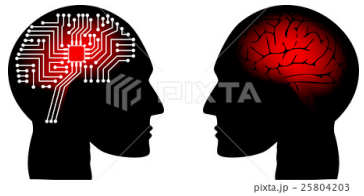
⇨ How do you think ?

セキュリティとAIに関する４つの観点

- (a) Attack using AI （AIを利用した攻撃）
- (b) Attack by AI （AI自身による攻撃）
- (c) Attack to AI （AIへの攻撃）
- (d) Measure using AI （AIを利用したセキュリティ対策）



AIの反乱（1）



1．人間を上回る能力を有する機械が誕生し将来的に人間が絶滅させられるではないか。

（a） AIの反乱心配派：

① Googleの研究者のレイ・カールワイツ：2045年には人工知能の能力が、人間を超越するシンギュラリティが生じ、反乱すら起きるかもしれない

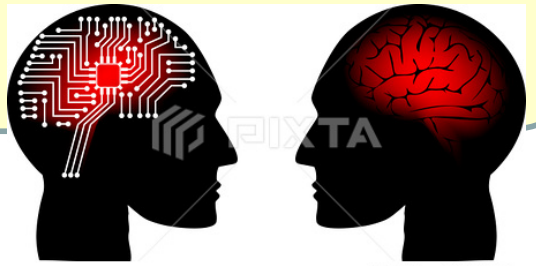
② スティーブン・ホーキング：人工知能の発明は人類史上最大の出来事だった。だが同時に『最後』の出来事になってしまう可能性もある

（b） AIの反乱非存在派：人工知能学会の松尾豊は、著書『人工知能は人間を超えるか』内に於いて、人間に対して反乱を起こす可能性を否定

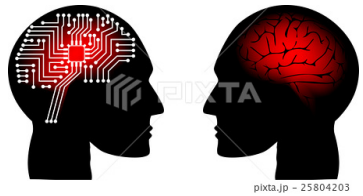
https://ja.wikipedia.org/wiki/人工知能

セキュリティとAIに関する４つの観点

- (a) Attack using AI （AIを利用した攻撃）
- (b) Attack by AI （AI自身による攻撃）
- (c) Attack to AI （AIへの攻撃）
- (d) Measure using AI （AIを利用したセキュリティ対策）



AIへの攻撃



① 機械学習システムの停止やファイル情報、通信路情報の盗み出しなどの攻撃：他システムへの攻撃と同じ

② 訓練済みモデルの誤分類を誘発する攻撃

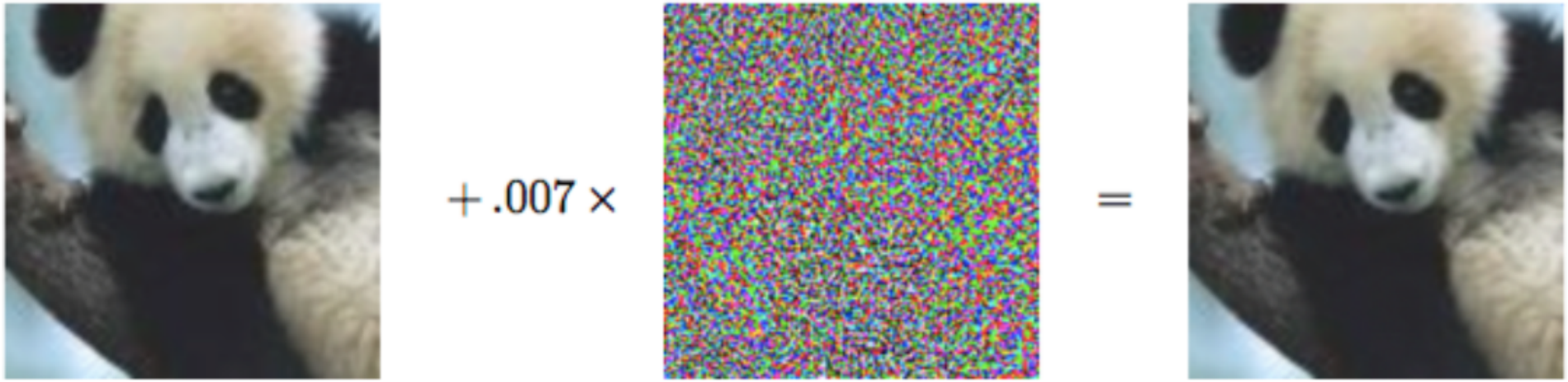
③ 機械学習に対する偏った訓練データを意図的に与えるなどが原因で、不適切な判断をさせてしまう攻撃。

④ 学習モデルへデータを入出力することにより情報を漏洩させる攻撃（訓練データ、判定特性エンジンなど）

https://news.yahoo.co.jp/byline/endohomare/20170806-00074210/
をベースに作成

既知のモデルに誤分類を誘発する攻撃

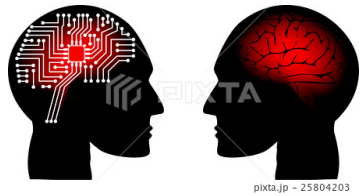
敵対的サンプル
（Adversarial）
Example



「パンダ」　　摂動　　「テナガザル」

Ian J. Goodfellow, Jonathon Shlens, Christian Szegedy
“Explaining and Harnessing Adversarial Examples”
https://arxiv.org/pdf/1412.6572.pdf

AIへの攻撃



① 機械学習システムの停止やファイル情報、通信路情報の盗み出しなどの攻撃：他システムへの攻撃と同じ

② 訓練済みモデルの誤分類を誘発する攻撃

③ 機械学習に対する偏った訓練データを意図的に与えるなどが原因で、不適切な判断をさせてしまう攻撃。

④ 学習モデルへデータを入出力することにより情報を漏洩させる攻撃（訓練データ、判定特性エンジンなど）

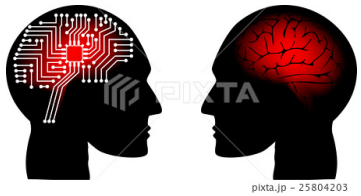
https://news.yahoo.co.jp/byline/endohomare/20170806-00074210/
をベースに作成

訓練データを汚染する攻撃例

＜Data Poisoning Attacksの例＞

- 米マイクロソフトのチャットボット「Tay」は、クラウドソーシングを利用して学習させた。
- 悪意を持ったユーザが協力して差別的な意見を繰り返し入力
- Tayは差別発言を繰り返すように
  ＝＞適切な訓練データの必要性

AIへの攻撃



① 機械学習システムの停止やファイル情報、通信路情報の盗み出しなどの攻撃：他システムへの攻撃と同じ

② 訓練済みモデルの誤分類を誘発する攻撃

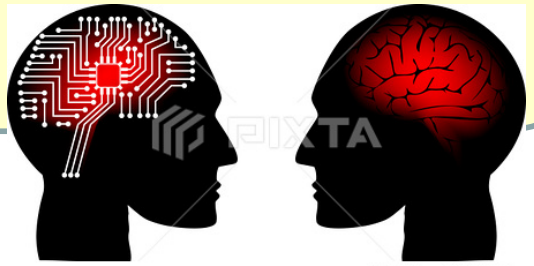
③ 機械学習に対する偏った訓練データを意図的に与えるなどが原因で、不適切な判断をさせてしまう攻撃。

④ 学習モデルへデータを入出力することにより情報を漏洩させる攻撃（訓練データ、判定特性エンジンなど）

https://news.yahoo.co.jp/byline/endohomare/20170806-00074210/
をベースに作成

セキュリティとAIに関する４つの観点

- (a) Attack using AI （AIを利用した攻撃）
- (b) Attack by AI （AI自身による攻撃）
- (c) Attack to AI （AIへの攻撃）
- (d) Measure using AI （AIを利用したセキュリティ対策）



AI for measures against Cyber Attack

多くの研究・開発が存在

MIT（マサチューセッツ工科大学）「85%の攻撃を自動検出」

それでは、人工知能（AI）を活用したサイバー対策の実例を紹介しましょう。最初は、MIT（マサチューセッツ工科大学）のコンピュータ科学および人工知能研究所が、開発したサイバー攻撃検知システムです。

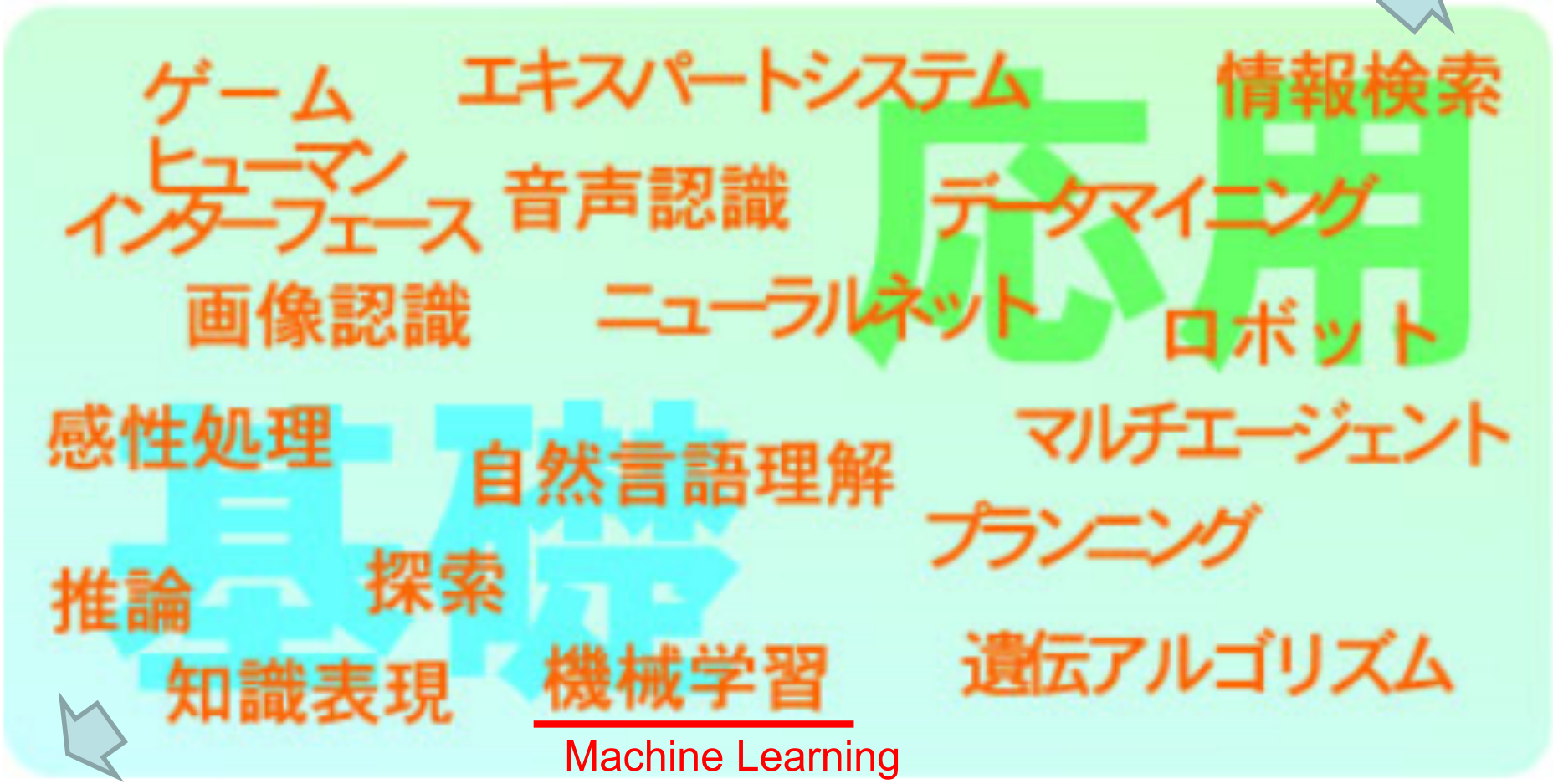
予想できない新たな攻撃や複数の手法を組み合わせた攻撃、新種のマルウェアとその亜種の矢継ぎ早な出現など、私たちは常に未知の攻撃にさらされており、過去の防御策は役に立たなくなっています。 そこで、サイバー攻撃対策に機械学習などを取り入れた、人工知能（AI）の活用が始まっています。ここでは、MIT（マサチューセッツ工科大学）、ソフトバンク、NTTコミュニケーションズが発表したサイバー攻撃対策を紹介します。

http://it-trend.jp/cyber_attack/article/use_of_ai

人工知能（Artificial Intelligence）研究の分野

3つめのインテリジェンス

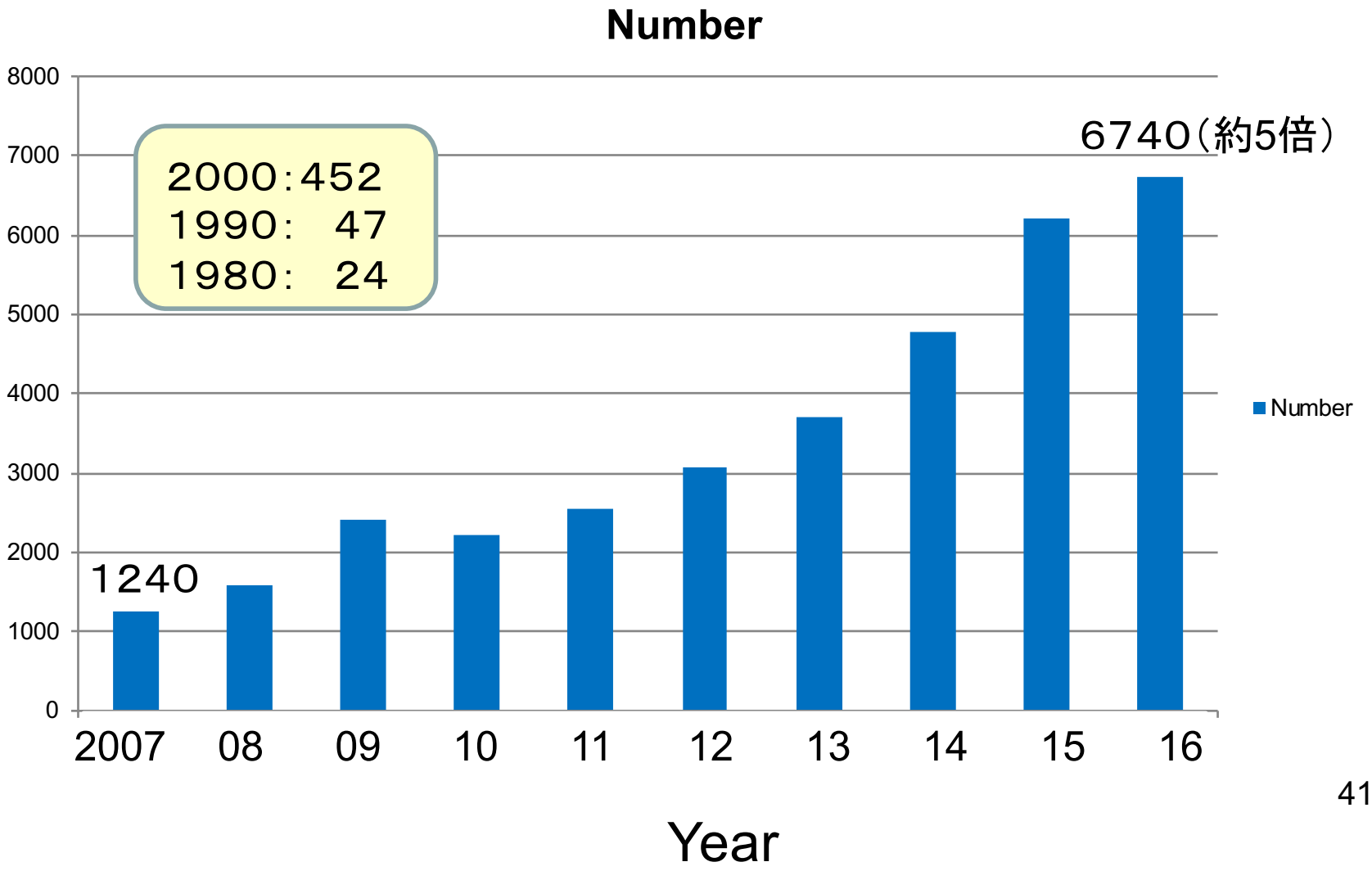
Application Area



Basic Area

http://www.ai-gakkai.or.jp/whatsai/AIresearch.html　日本人工知能学会資料

Google Scholarを用い Cyber Security AND AIで探索した結果



Survey Results using Google Scholar （全期間）

Cyber Security AND Artificial Intelligence

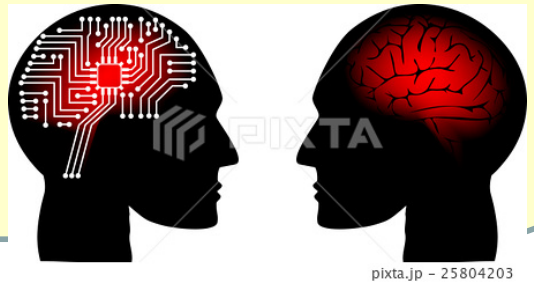
17,700件

ちなみに、上記＋Ryoichi Sasaki

50件（うち10件程度が論文や発表原稿）

AIを適用したセキュリティ対策

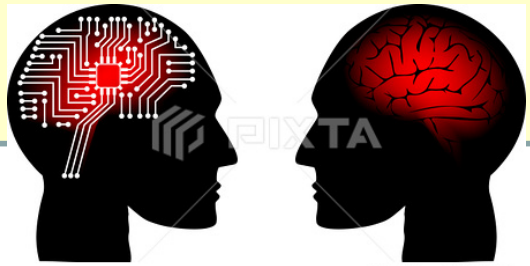
- 「マルウェアの検出」
- 「ログの監視・解析」
- 「継続的な認証」
- 「トラフィックの監視・解析」
- 「セキュリティ診断」
- 「スパムの検知」
- 「情報流出」など



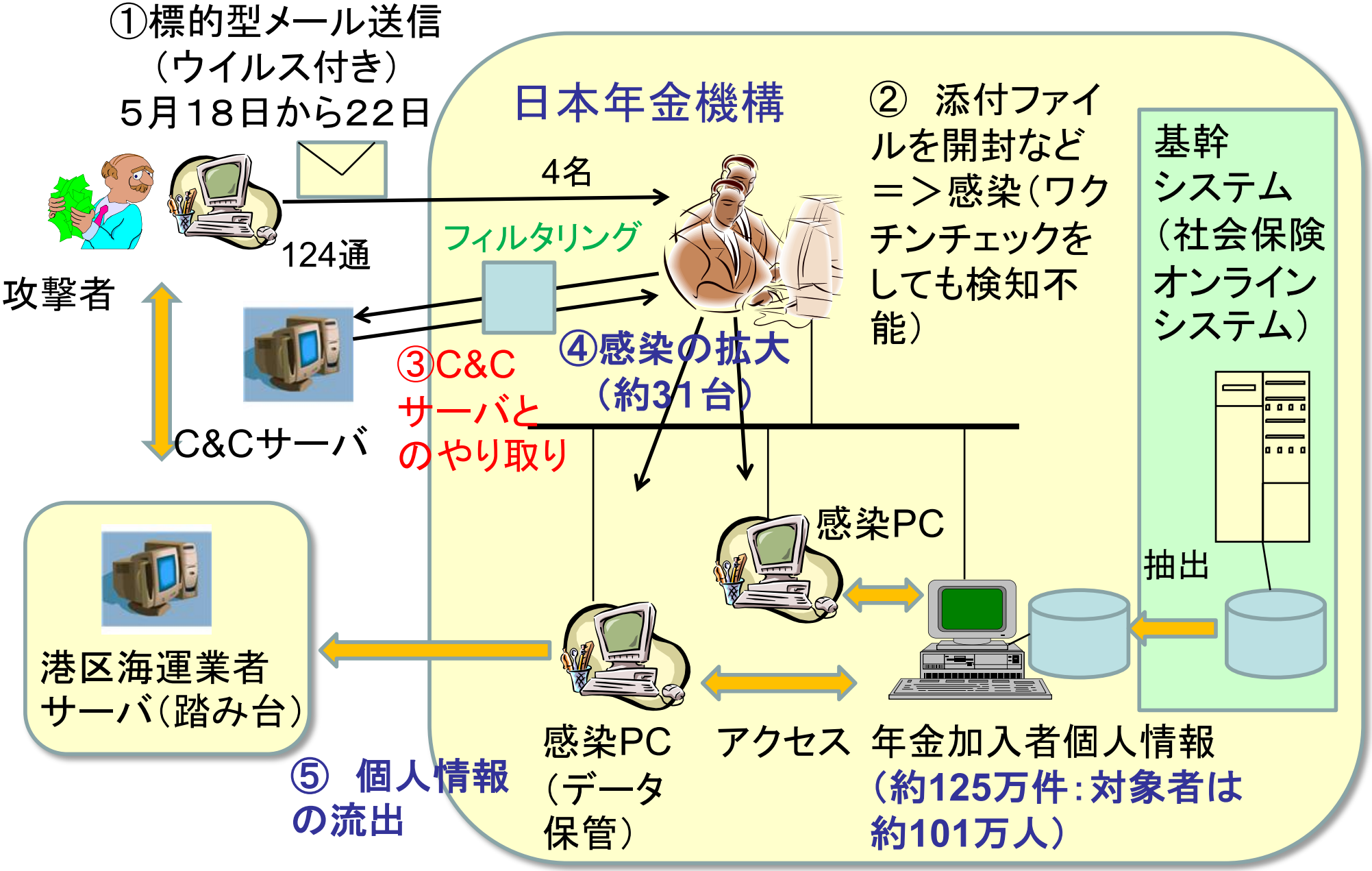
わたしたちの主要な研究

（1） 機械学習を利用した標的型攻撃用C&Cサーバの自動判別システム

（2） ルールベースシステムやベイジアンネットワークを利用した知的ネットワークフォレンジックシステム



日本年金機構への標的型攻撃



判別方法

学習段階

VirusTotalというDBを利用した標的型攻撃マルウエアの各種の亜種の収集

正常ドメインに関するGoogle情報やDNS情報、やWhois情報などの収集

動的解析によるC&Cサーバドメインの抽出とGoogle情報やDNS情報やWhois情報などの収集

機械学習ツール：サポートベクターマシン/　ニューラルネット

プロキシーサーバから出ていこうとしているドメインの情報

判別モデル

C&Cサーバである可能性が強い場合にアラート

判別段階

検知率
98.9%

久山真宏、柿崎淑郎　、佐々木良一「攻撃者に察知されにくい情報を用いたC&Cサーバの検知手法の提案と評価」情報処理学会論文誌,Vol.58,No.9,pp1410-1418,2017

セキュリティ対策に機械学習を用いる困難点

① サイバー攻撃などの例は少なく、データが十分でない場合がある

② 攻撃パターンが時間とともに変化し、古いデータが使えない場合がある

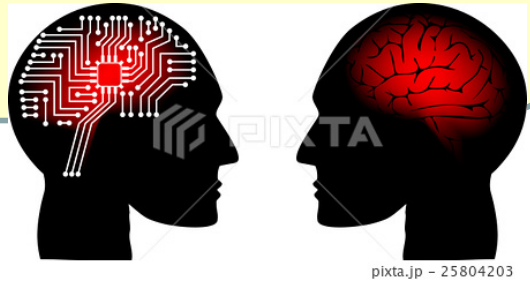
③ 特に、攻撃側が学習モデルを知って、あえて、分類を間違えるように変更することが可能である

継続的なモデルの改良が必要

わたしたちの主要な研究

（1） 機械学習を利用した標的型攻撃用C&Cサーバの自動判別システム ⇨ 検知率 98.9%

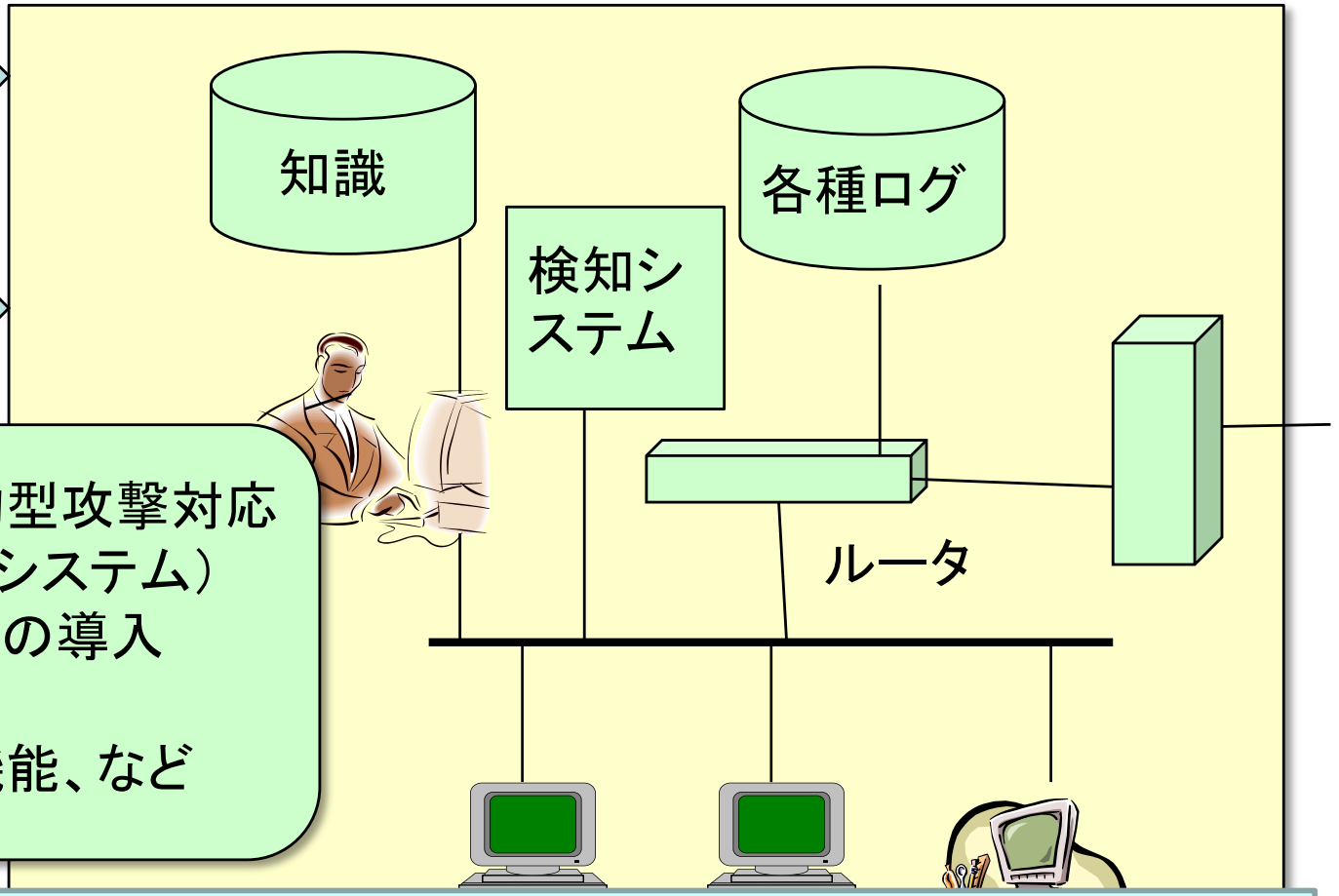
（2） ルールベースシステムやベイジアンネットワークを利用した知的ネットワークフォレンジックシステム



LIFTプロジェクトの概要

①計画支援
システム

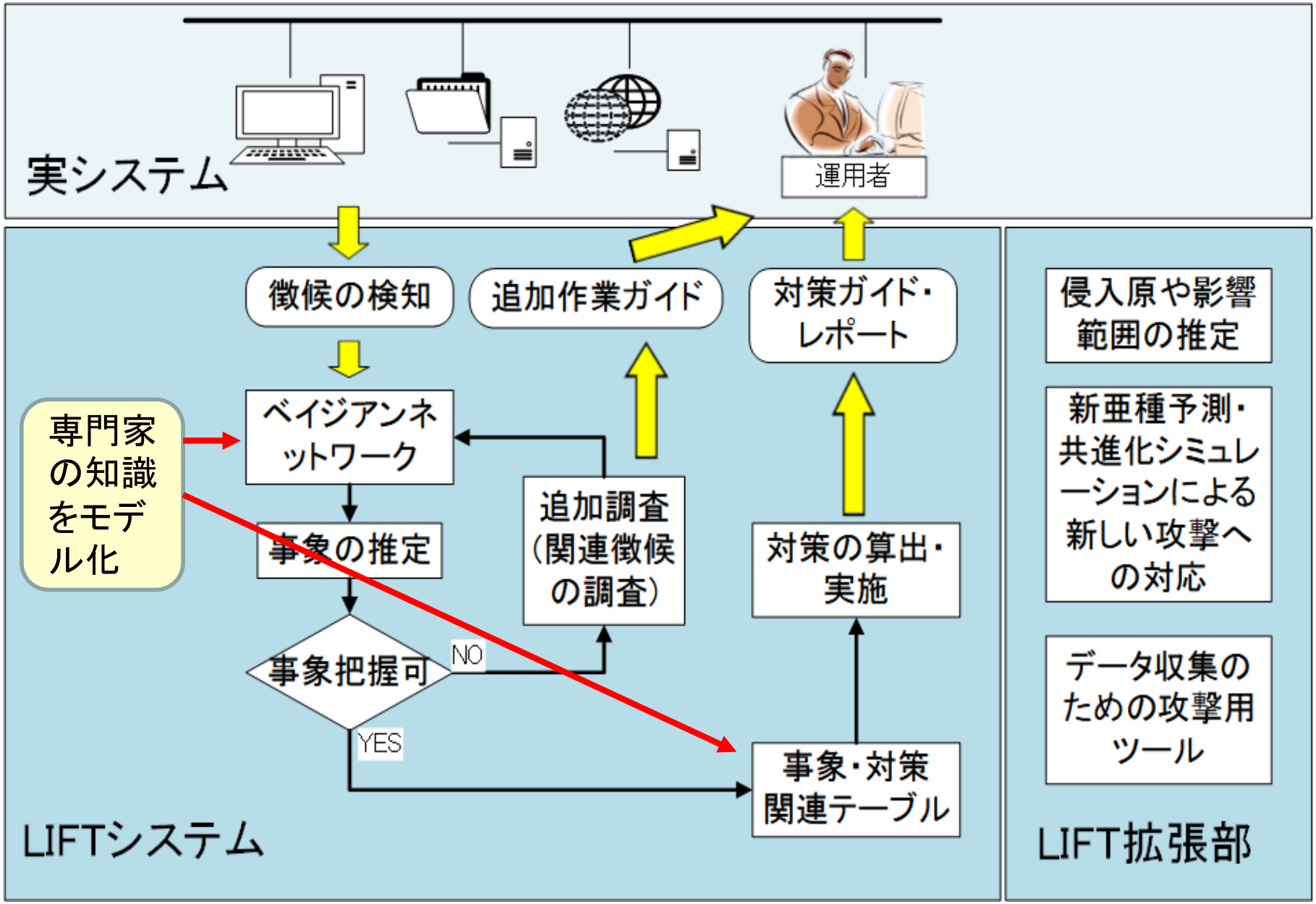
②状況認識知識
獲得用実験環境



③LIFTシステム（標的型攻撃対応
自動運転・操作ガイドシステム）
（1）基本機能：AI技術の導入
（2）追加情報：
原因プロセス発見機能、など

共同開発プロジェクト （リーダ佐々木、上原先生、高倉先生、八槙先生、柿崎先生、日立他） 期間：2013年9月―2018年3月（第一期）
現状での主な成果：① 方式確立プロト開発 ②原因プロセス発見ソフト製品化

LIFTシステムの概要



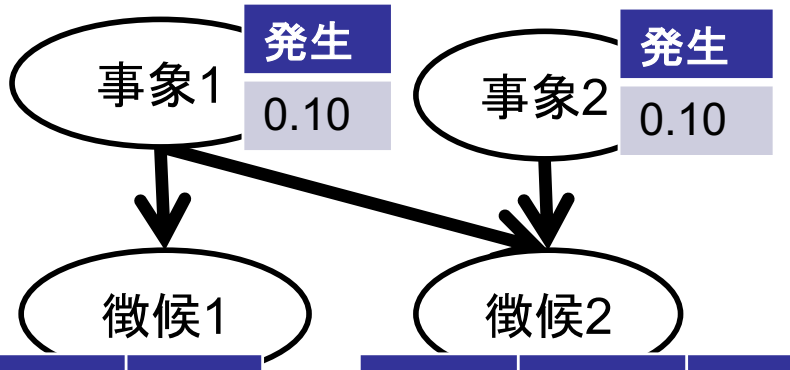
ベイジアンネットを利用する理由

- ベイジアンネット：AIの一種。事前主観確率とデータ観測利用
- テーブルよりベイジアンネットの方が良い結果が期待できる
  - 検知されていないという情報を利用できる
  - 徴候が検知されたとき関連したものは上昇、関連していないものが減少するという仕組みが入っている

＜テーブル＞

	攻撃事象＼徴候	不自然なプロセスの立ち上がり	プロキシ：プロキシを経由しない通信	プロキシ：443以外のCONECTメソッドを利用した通信	長時間のセッション	業務に不要なコマンド
基盤構築フェーズ	端末が不正プログラムを起動	0.3				
	C&Cサーバへ接続		0.6	0.6	0.4	
	必要な機能のダウンロード	0.4	0.4		0.3	
	端末の情報入手	0.5			0.2	0.4

＜ベイジアンネット＞



事象1	検知
発生	0.80
未発生	0.20

事象1	事象2	検知
発生	発生	0.90
発生	未発生	0.80
未発生	発生	0.80
未発生	未発生	0.20

事象推定時におけるLIFTの画面

既存の攻撃に対しては正しく対応

Ryoichi Sasaki et al.“Development and Evaluation of Intelligent Network Forensic System LIFT Using Bayesian Network for Targeted Attack Detection and Prevention” International Journal of Cyber-Security and Digital Forensics (IJCSDF) 7(4): pp344-353, 2018（to appear）

サイバーセキュリティとAIの関連に関する考察

（1） Cybersecurity対策に関しても、データが十分あり、AI技術の1つである機械学習が使えるような対象は現在でも有効。

ただし、動的変化に対応が必要

（2） データが十分ない対象に対しては今後さまざまな試行が必要

（3） いずれにしても、サイバーセキュリティのAI応用は今後も重要な研究分野

目次

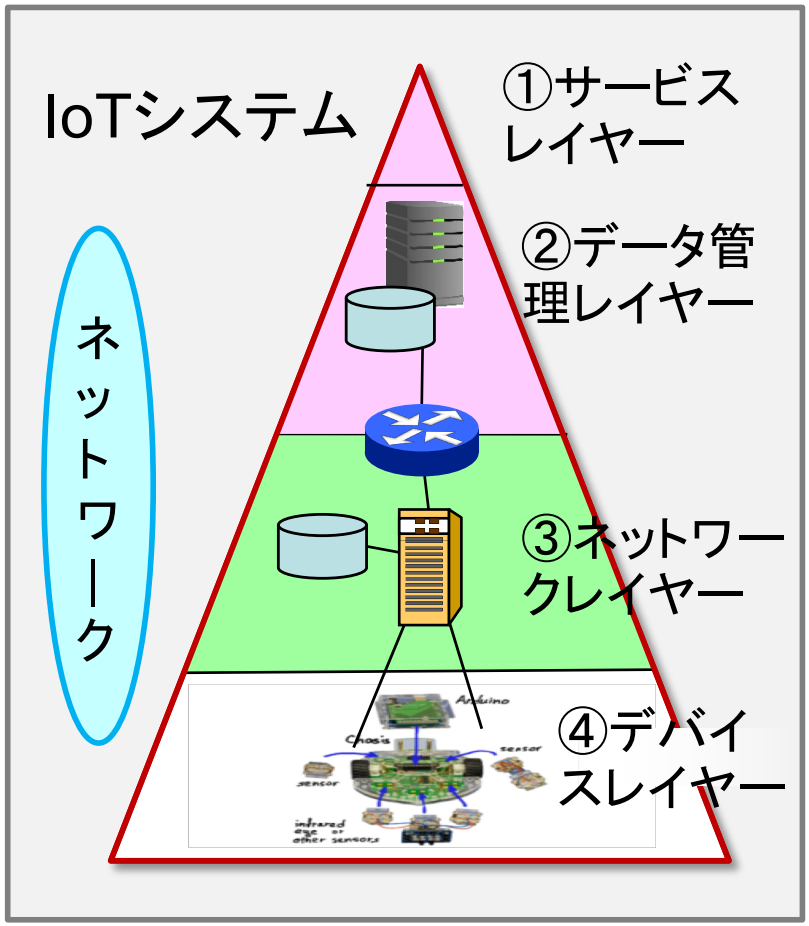
IoT 特有の性質

（性質１）脅威の影響範囲・影響度合いが大きいこと
（性質２）IoT 機器のライフサイクルが長いこと
（性質３）IoT 機器に対する監視が行き届きにくいこと
（性質４）IoT 機器側とネットワーク側の環境や特性の相互理解が不十分であること
（性質５）IoT 機器の機能・性能が限られていること
（性質６）開発者が想定していなかった接続が行われる可能性があること

⇒ 安全対策が困難

IoTセキュリティガイドライン　平成28年7月
http://www.soumu.go.jp/main_content/000428393.pdf

IoTのレイヤーリングと安全対策



＜対象によってセキュリティ
対策が大幅に異なる＞

既存
のIoT
機器

セキュア
ゲートウ
エイ

セキュア
チップ

種々の対
策の適切
な組み合
わせ

新規中小規模
IoTシステム

新規大規模規模
IoTシステム

医療用IoT機器システムに適用できるリスク評価手法の開発

① セキュリティ、セーフティ、メインテナビリティなど異なる指標を扱う必要がある ＝＞

（a） リスクベースの統一的指標を採用

（b） 原因となる故障やヒューマンエラーだけでなくサイバー攻撃によるものも統一的に記述できる**ガイドテンプレイトの提案**

② IoT機器システムは制御系を含み、従来のアタックツリーのようなものだけではセーフティの評価が困難 ＝＞

MITのナンシーレブソン提案のSTAMP/STPA手法（セキュリティは対象外）を改良して使用

③ リスクを評価するためにはいろいろなアプローチがあり、一長一短がある ＝＞

（a） 定量的アプローチと準定量的アプローチの統合

（b） ボトムアップアプローチとトップダウンアプローチの統合

⇨ 佐々木らが開発中

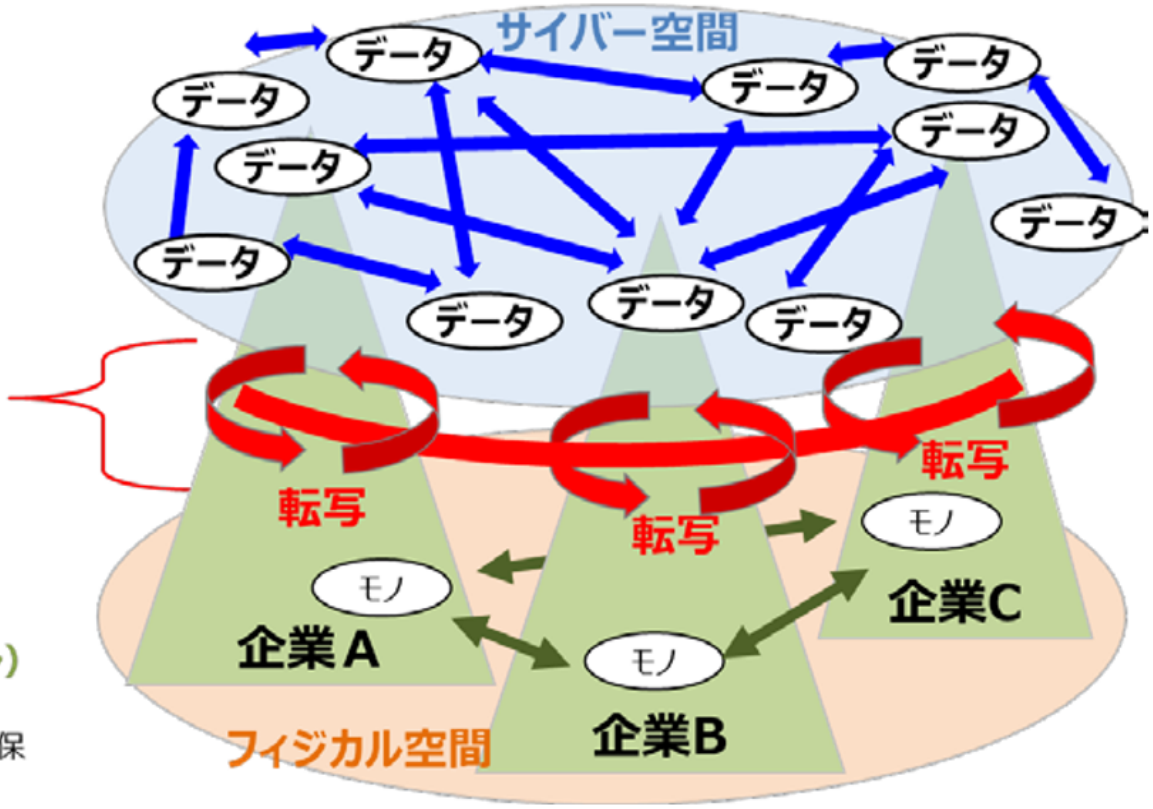
サイバー・フィジカル・セキュリティ対策フレームワークのための3階層モデル

経済産業省：抜けのない対策要件
抽出のために3階層モデルを構築

サイバー空間におけるつながり
【第３層】
- 自由に流通し、加工・創造されるサービスを創造するためのデータの信頼を確保

フィジカル空間とサイバー空間のつながり
【第２層】
- フィジカル・サイバー間を正確に“転写”し、機能の信頼を確保
（現実をデータに転換するセンサーや電子信号を物理運動に転換するコントローラ等の信頼）

企業間のつながり（従来型サプライチェーン）
【第１層】
- 適切なマネジメントを基盤に各主体の信頼を確保



http://www.meti.go.jp/press/2018/10/20181001004/20181001004-3.pdf

IoTのレイヤリングと安全対策

レイヤー	必要機能	考えられる対策技術
1. サービスレイヤー	プライバシー保護 フィッシング防止	自己情報コントロール 技術など
2. データ管理レイヤー	データの秘密管理と バックアップ、改ざん防止	秘密分散技術 デジタルフォレンジック など
3. ネットワークレイヤー	不適切なデータのフィルタリング、通信情報の秘密	セキュアゲートウエイ 軽量暗号など
4. デバイスレイヤー	センサーやアクチュエータなどのなりすまし防止	セキュアチップなど

セキュア暗号ユニットSCU（NEDOで開発）

松本教授らが開発中：どこでも公開鍵暗号

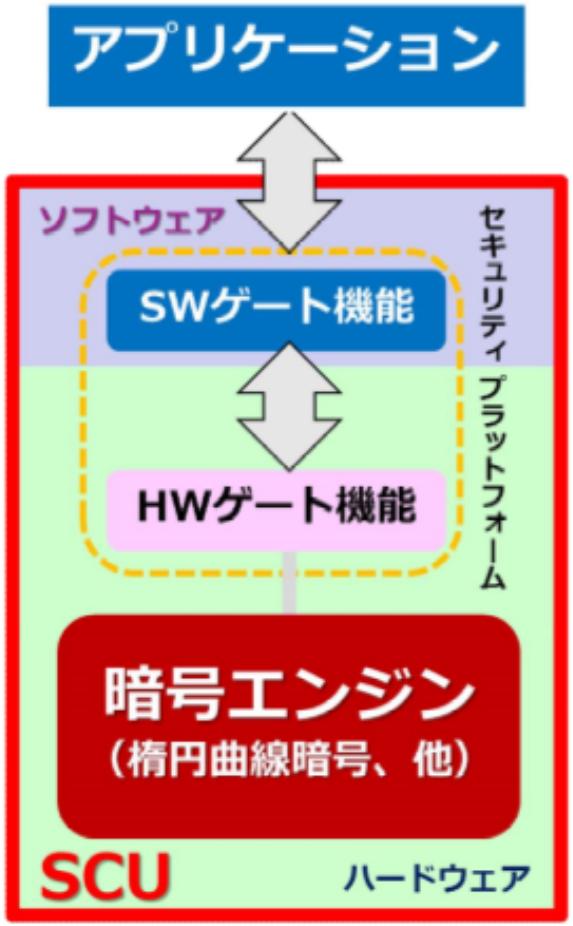
セキュア暗号ユニットSCUの特長

ハードウェア暗号エンジン

256ビットの楕円曲線暗号の処理につき
・末端ノード向きには
　1ミリワット級の超低電力および
　十キロゲート級の小面積・低コストを達成
・中間ノード向きには
　10,000回/秒以上の超高速動作を達成
共通鍵暗号等も実装する

セキュリティプラットフォーム

仮にアプリケーションが不正に改変され、暗号エンジンへの不正アクセスを試みたとしても、SWゲート機能とHWゲート機能から構成されるセキュリティプラットフォームが、そのような試みを確実に検出し、アクセスを阻止する



http://www.nedo.go.jp/content/100863674.pdf

目次

終りに

- サイバー攻撃は今後も厳しくなる。
- 高度なセキュリティ対策がますます重要に。
- ハード・ソフト・暗号アルゴリズムなどに高い技術力を持つサイバーフィジカルセキュリティ研究センターに期待するものは大。
- 個別の技術力だけではなく、それらをうまく組み合わせ、より大きな成果に。


END