資料19－3

サイバーセキュリティの
今後の研究開発課題について

NICT　サイバーセキュリティ研究所
久保田実

まずは

最近の動向

NICTER観測統計（2005–2018）

年	年間総観測パケット数	観測IPアドレス数	1 IPアドレス当たりの年間総観測パケット数
2005	約 3.1億	約1.6万	19,066
2006	約 8.1億	約10万	17,231
2007	約19.9億	約10万	19,118
2008	約22.9億	約12万	22,710
2009	約35.7億	約12万	36,190
2010	約56.5億	約12万	50,128
2011	約45.4億	約12万	40,654
2012	約77.8億	約19万	53,085
2013	約128.8億	約21万	63,655
2014	約256.6億	約24万	115,323
2015	約545.1億	約28万	213,523
2016	約1,281億	約30万	469,104
2017	約1,504億	約30万	559,125
2018	**約2,121億**	約30万	**789,876**

2019年の11月10日時点での総観測パケット数は約3,060億

1 IPアドレスあたりの年間総観測パケット数

印象に残った

2019年の出来事

- ランサムウエア攻撃は引き続き活発
  →WannaCry に関連する 445/TCP に対するスキャンは沈静化していない　[NICTER観測レポート]
  →米国では自治体を標的としたランサムウエア攻撃が活発化
- QRコード決済サービス7payの一連の騒動
  →少しでもセキュリティ対策が甘いとあっという間に被害
  →経営陣とセキュリティ担当部署の関係性が注目された
- スマホ決済サービスd払いの不正利用
  →スミッシング（SMS＋フィッシング）
  →これ以外のWeb媒介型攻撃も相変わらず猛威
- AWSの大規模障害
- サプライチェーンリスクが強く意識される
- Googleの量子コンピューターが「量子超越性」実証

世間では

サイバー空間と実空間の一体化

サイバーセキュリティ戦略全体概要（2018年7月27日**閣議決定**）より

【１．策定の趣旨・背景】及び【２．サイバー空間に係る認識】のポイント
現状認識と将来像（サイバー空間と実空間の一体化に伴う脅威の深刻化）

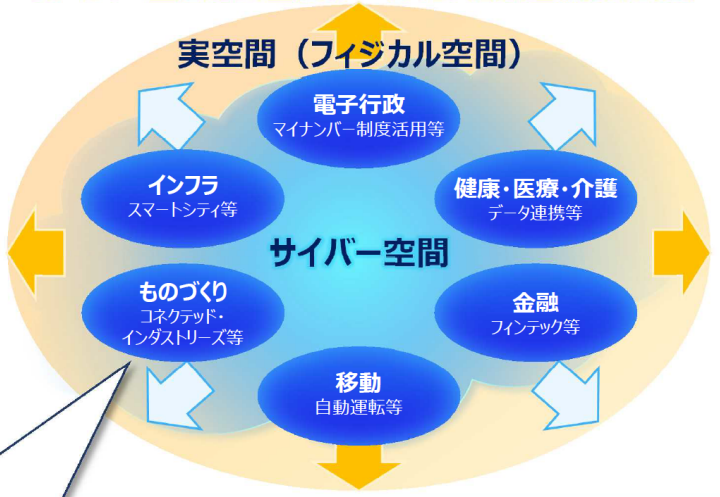
中長期

策定の趣旨・背景

【（2015年戦略策定時）連接融合情報社会の到来】
～実空間のヒト・モノがネットワークに**連接**され、
実空間とサイバー空間の**融合**が高度に深化～

一体化

【サイバー空間と実空間の一体化、活動空間の拡張】



サイバー空間に係る認識

・AI、IoT 、Fintech 、ロボティクス、３Dプリンター 、AR/VR など、**サイバー空間における知見や技術・サービスが社会に定着し**、経済社会活動・国民生活の既存構造に変革をもたらす**イノベーションを牽引する一方で、不確実さは常に内在**

サイバー空間がもたらす恩恵

・サイバー空間における技術・サービスが**制御され、様々な分野で当然に利用されており、人々に豊かさをもたらしている。**
・深層学習による**AIの進化**により、既に幅広い産業に応用され始めている。
・**IoT機器で得られるデータ**を利活用した新たなビジネスやサービスが創出されつつある。

サイバー空間における脅威の深刻化

・サイバー空間における技術・サービスを**制御できなくなるおそれは常に内在しており、多大な経済的・社会的な損失が生じ得る。**
・重要インフラサービスの障害やIoT機器の意図しない作動により、様々な**業務・機能・サービス障害が生じた場合、社会に大きな影響が生じ、国家安全保障上の問題**に発展する可能性
・サイバーセキュリティ対策の不備が、**金銭的な損害を直接引き起こし**、拡大することが予想される。

研究においては

研究領域の境界の消失

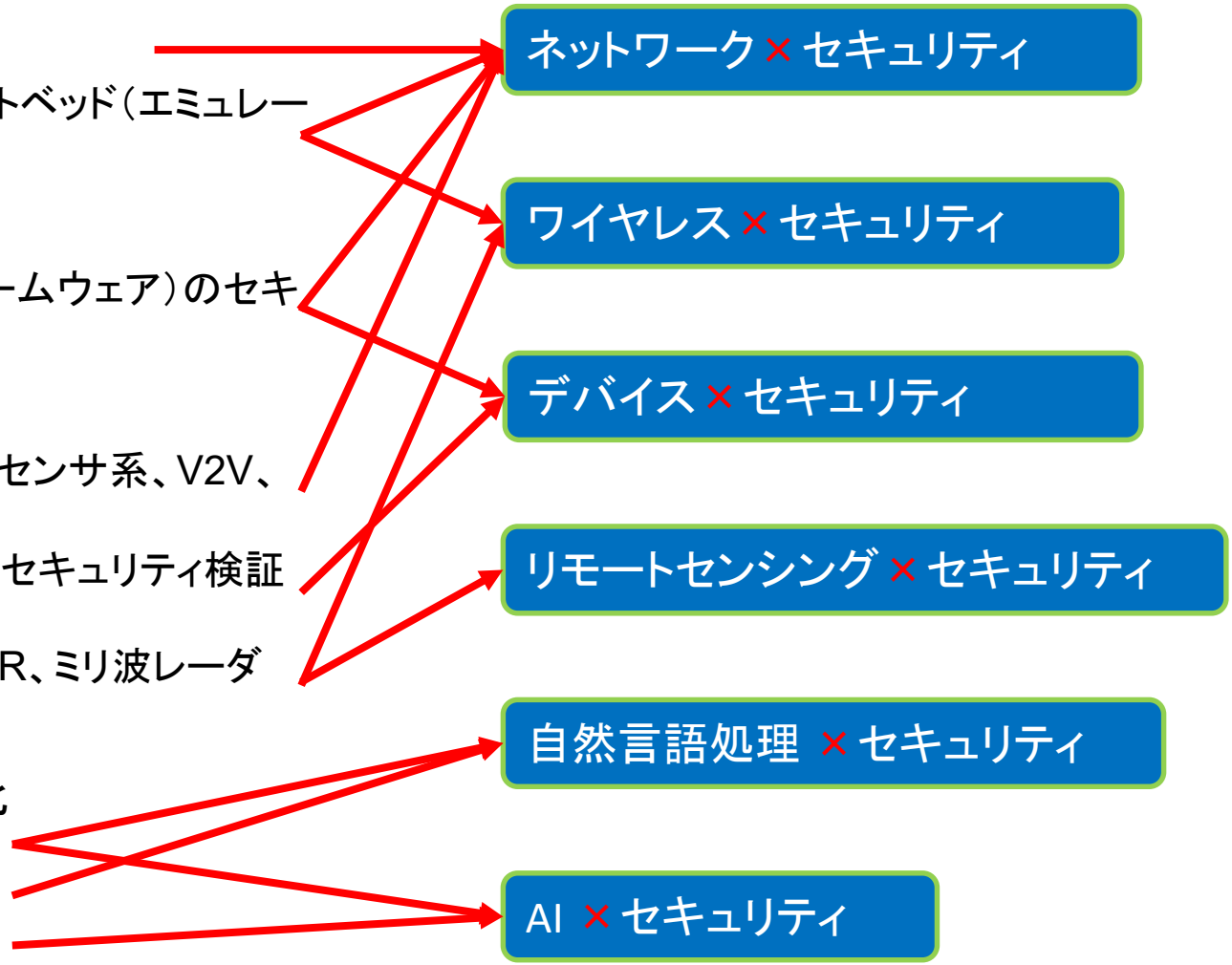
とある組織の研究テーマの素案（ブレストレベル）

5Gセキュリティ
- クラウドセキュリティ
- 5Gセキュリティ検証のためのテストベッド（エミュレーション環境）構築

通信機器セキュリティ
- ローレイヤ（ハードウェアからファームウェア）のセキュリティ検証環境・体制の構築

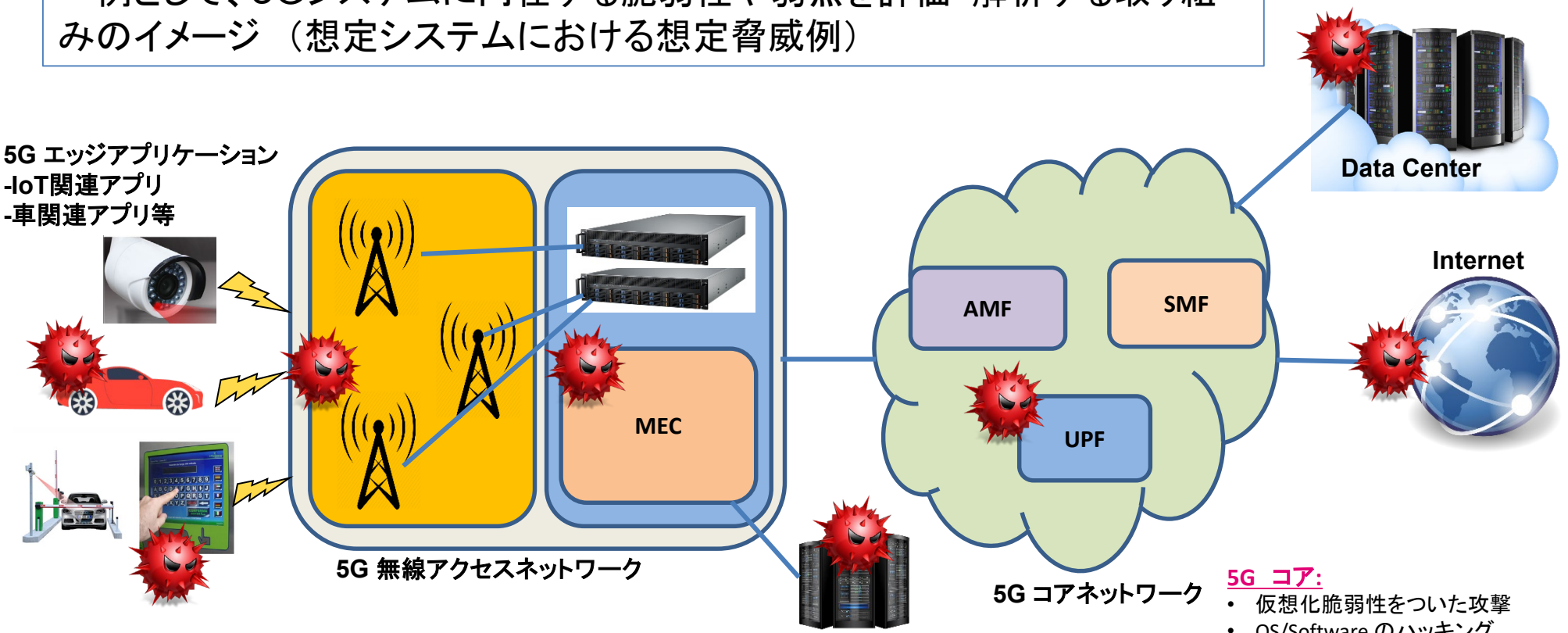
コネクテッドカー・セキュリティ
- 車（CAN、インフォテインメント系、センサ系、V2V、V2X等）のセキュリティ検証
- 各種車載デバイスのローレイヤのセキュリティ検証環境・体制の構築
- 無線通信部分、センサ部分（LiDAR、ミリ波レーダ等）のセキュリティ検証も必要

セキュリティオペレーション高度化
- アラートスクリーニング
- フェイクニュース分析
- 自動マルウェア解析



次世代ネットワークセキュリティ

一例として、5Gシステムに内在する脆弱性や弱点を評価・解析する取り組みのイメージ （想定システムにおける想定脅威例）



エッジ機器など
- マルウェア
- ダウングレード攻撃
- 中間者攻撃
- DDoS/DoS 攻撃
- サプライチェーンリスク
- Bluetooth/NFC/Wi-Fi
- ソフト/ファームへの攻撃
- 物理攻撃など

RAN/Air インタフェース:
- ローグ gNB
- 中間者攻撃
- パッシブ CP/UP スニーフィング
- ジャミング攻撃 (DoS 攻撃)
- 非認証帯域利用
- 物理攻撃など

バックフォール等の通信:
- CP/UPスニーフィング
- 中間者攻撃
- MEC DoS
- ジャミング攻撃
- 物理攻撃など

ネットワークスライス/MEC:
- DDoS/DoS 攻撃
- OS/Software のハッキング
- 仮想化脆弱性をついた攻撃
- アプリケーション脆弱性をついた攻撃
- オーケストレーション　攻撃
- 物理攻撃など

5G　コア:
- 仮想化脆弱性をついた攻撃
- OS/Software のハッキング
- アプリケーション脆弱性をついた攻撃
- オーケストレーション　攻撃
- 不正メッセージフローによる攻撃
- ローミングの弱点を使った攻撃
- DDoS/DoS 攻撃
- API 脆弱性を突いた攻撃　など

コネクテッドデバイスセキュリティ

通信機器のセキュリティ検証技術が未確立であり、通信機器のセキュリティ検証体制が必要

コネクテッドカーの現状とNICTの方向

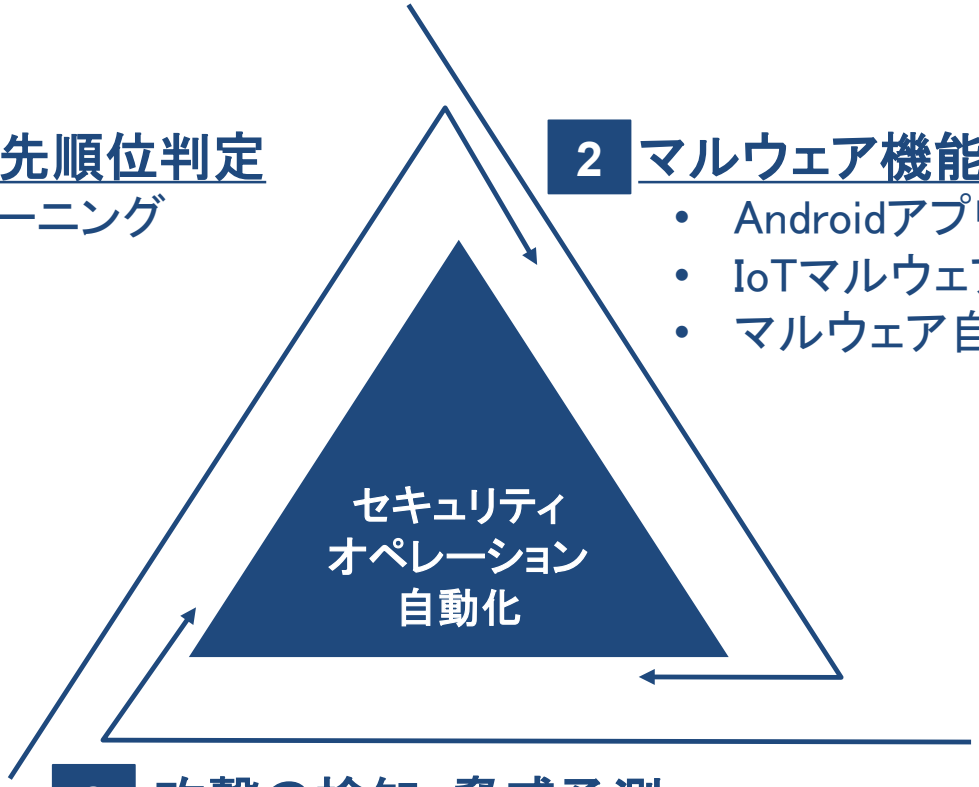
- **将来の自動車業界に対し、ICTは多大な価値を与えることになる。**
  - Deep Learningの車への応用により、自動運転（レベル４）は2020年～2022年には商用化されていくものと期待。
- **米国、欧州などは、「繋がる車」、「自動化された車」、「車のシェア及び極端に電子化」を目指した流れに向かっている。**
  - 他輸送サービスとの融合による、マルチモーダル化の推進も想定
- **自動車関連のビジネスは、クラウド/IoTに基づくサービスに移行していく傾向が高く、そのため、多くのIT企業へのビジネスチャンスが広がっている。**
- **NICTとしては、以下の視点で研究推進を検討中**
  - 高度化された車を対象とした脆弱性検証（CAN、インフォテインメント系、センサ系、デバイスローレイヤ等）
  - 車での活用も想定可能な「軽量暗号化」の研究
  - 検証結果などをまとめた車のセキュリティ標準化への貢献

研究のトレンド

AI x Cybersecurity

NICTの研究スコープ

AIとサイバーセキュリティの融合で、各種の自動分析技術やセキュリティ・オペレーションの自動化について研究開発を推進

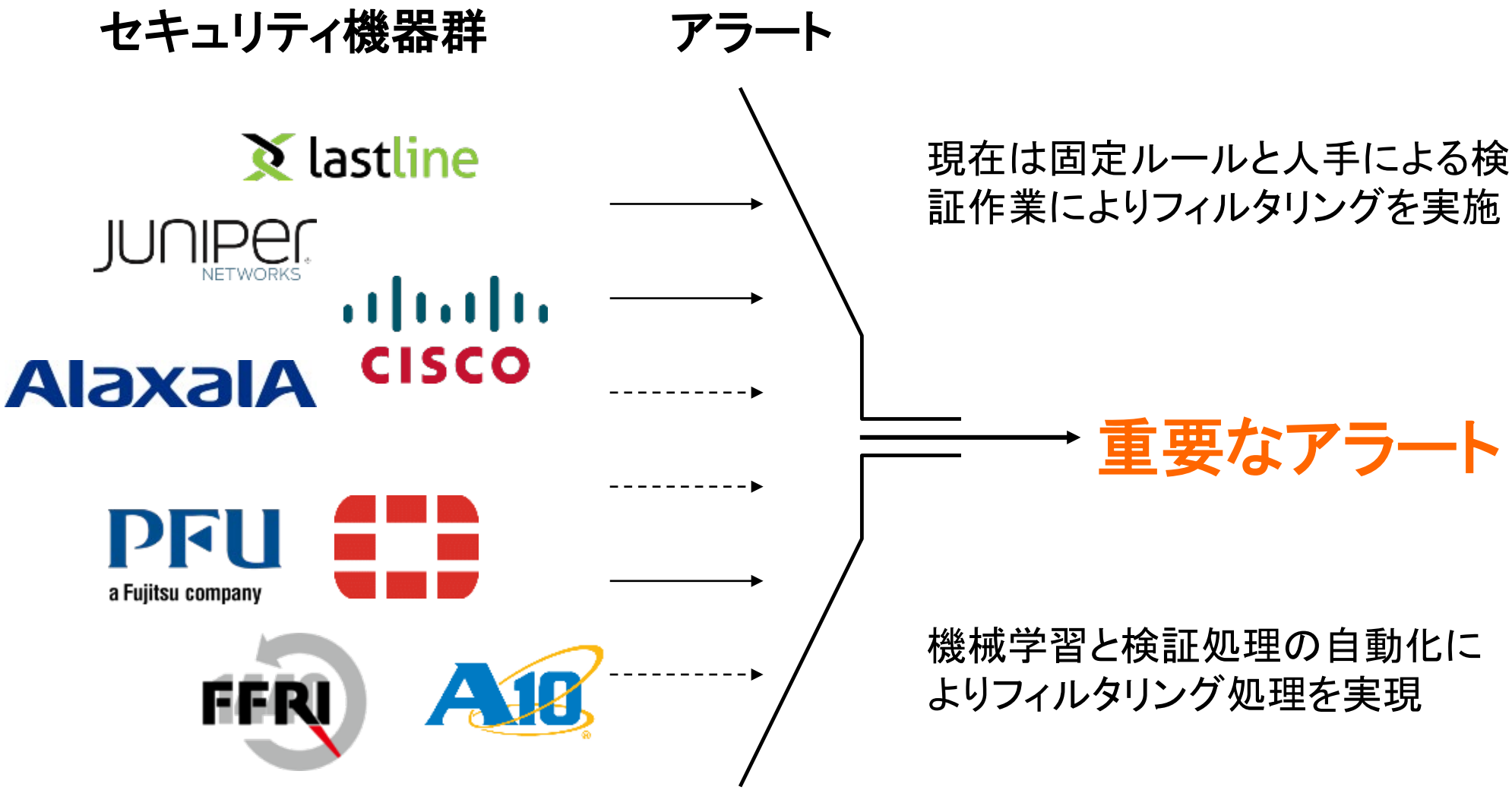


1 インシデントの優先順位判定
- アラートスクリーニング
- 脆弱性の分析

2 マルウェア機能分析自動化
- Androidアプリおよびマーケット分析
- IoTマルウェア分析
- マルウェア自動分析ツール開発

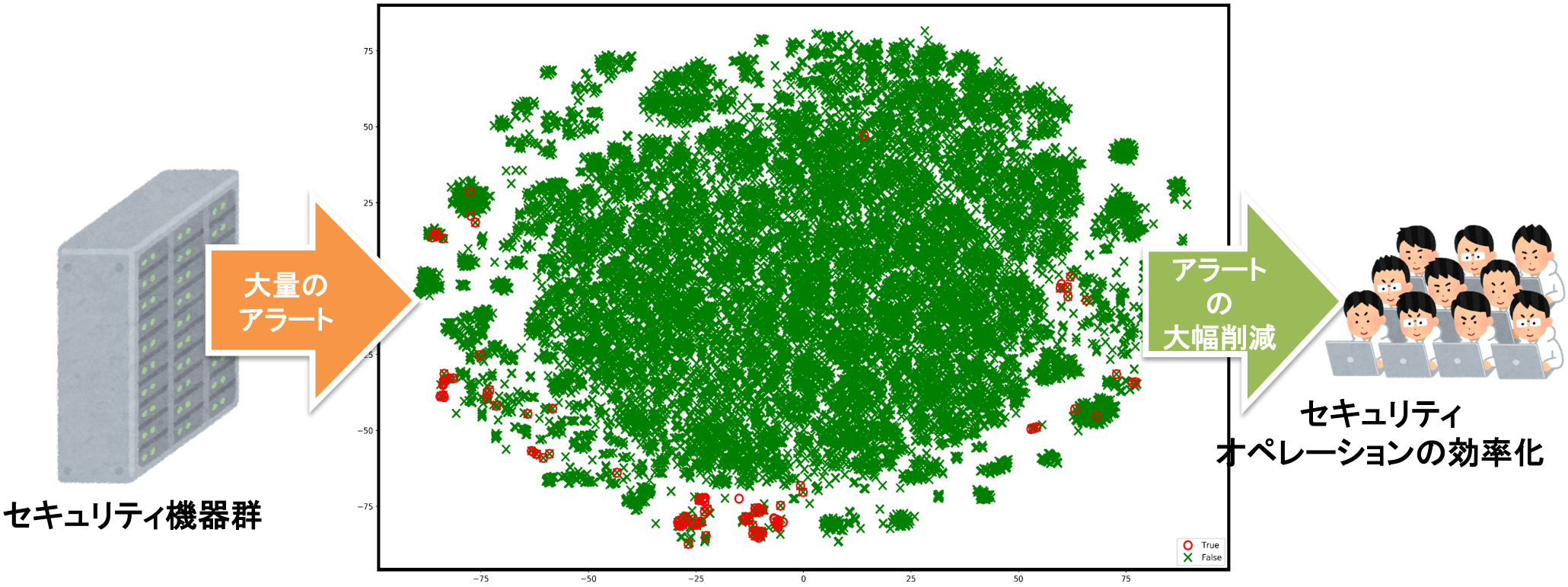
3 攻撃の検知・脅威予測
- ダークネット分析
- ユーザトラフィックの異常検出
- 脅威予測

アラートスクリーニング（1/2）



アラートスクリーニング（2/2）

- 複数のセキュリティ機器から出されるアラートを深層学習を用いて自動分類
- 重要度の低いアラートをスクリーニングしてオペレーションの負荷を軽減



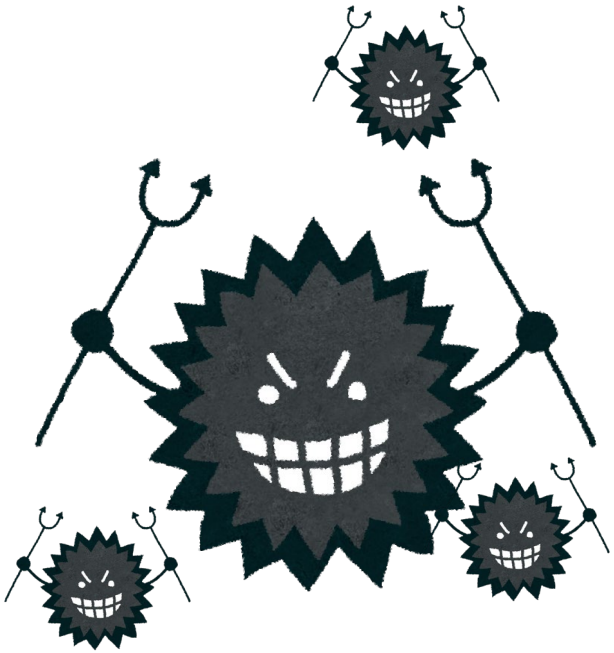
t-SNEによるアラート情報の2次元マッピング
（赤：True Positive、緑：False Positive）

[3] M. E. Aminanto et al., “Combating Threat-Alert Fatigue with Online Anomaly Detection using Isolation Forest,” ICONIP’19, Dec 2019. (to appear)

機械学習によるIoTマルウェアの自動分類

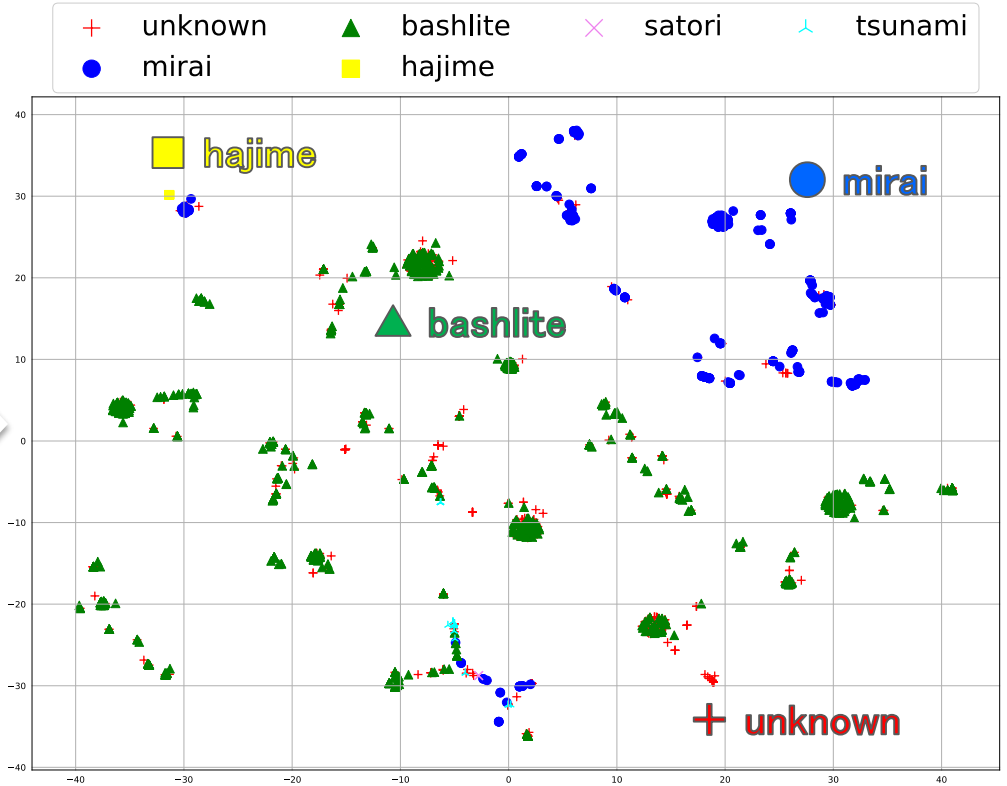
- IoTマルウェアのプログラムコードを分割して特徴抽出[4]
- 機械学習※2を用いて99%以上の精度でIoTマルウェアの分類に成功[5]

※2 SVM



未知のIoTマルウェア

特徴抽出し
機械学習で
分類

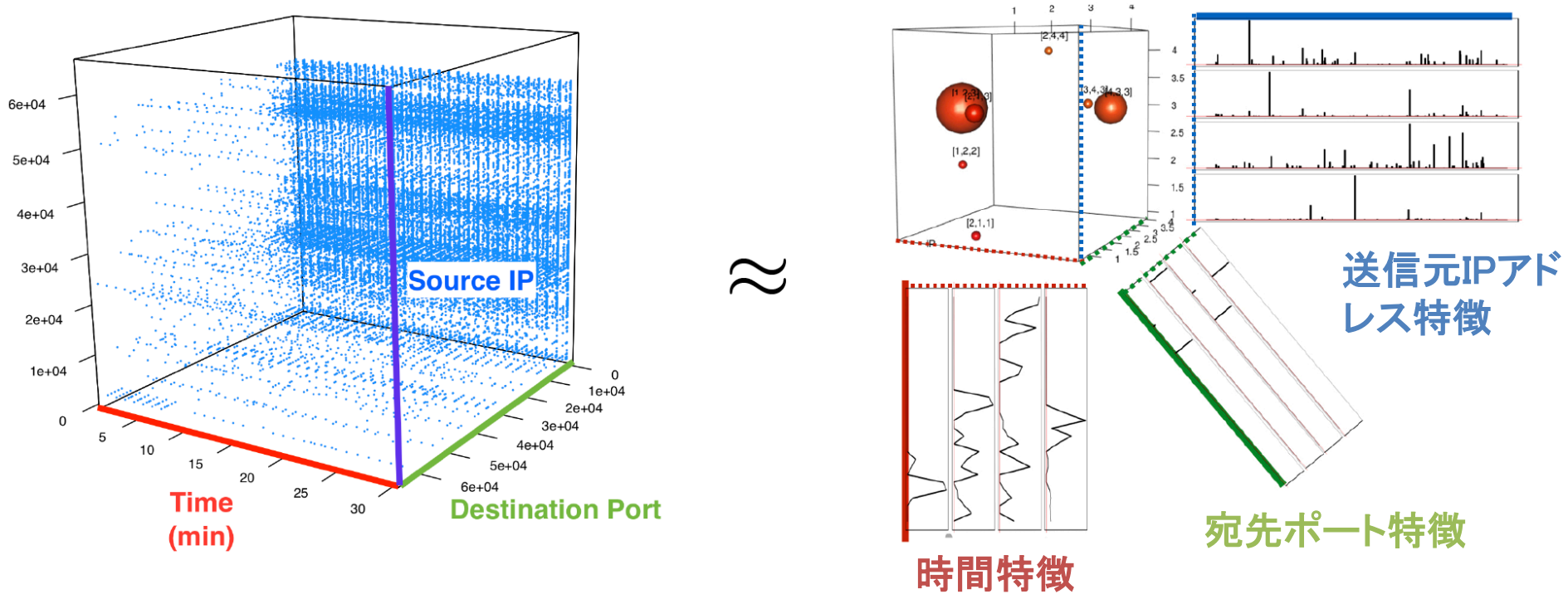


t-SNEによるIoTマルウェアの2次元マッピング

[1] R. Isawa et al., “Evaluating Disassembly-code based Similarity between IoT Malware Samples,” AsiaJCIS 2018, Aug 2018.
[2] T. Ban et al., “A Cross-Platform Study on IoT Malware,” ICMU2018, Oct 2018.

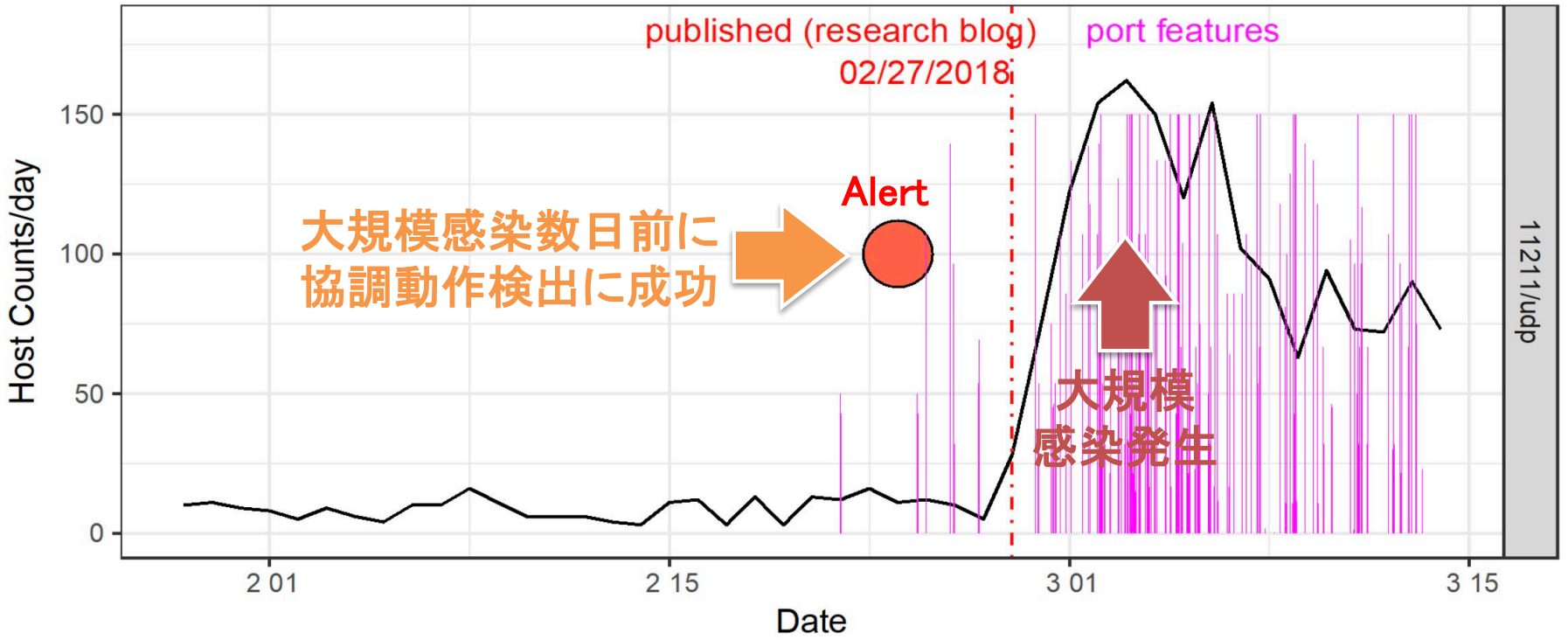
ダークネットトラフィックの協調動作検出（1/2）

- IoTマルウェア等の大規模感染による協調動作を早期検出
- 時間、送信元IPアドレス、宛先ポートにテンソル因子分解



ダークネットトラフィックの協調動作検出（2/2）

- IoTマルウェア等の大規模感染による協調動作を早期検出
- テンソル因子分解した特徴を組み合わせ複数IPアドレスの協調動作を検出
- 大規模感染数日前の協調動作早期検出に成功[3]



H. Kaneharaet al., "Real-Time Botnet Detection Using Nonnegative Tucker Decomposition," ACM SAC, 2019, Apr 2019.

データが命

NICTが保有するサイバーセキュリティ関連情報例

カテゴリ	蓄積データの具体例
ダークネット関連情報	未使用IPアドレス空間で観測したパケット、その統計情報、など
ライブネット関連情報	NICT内部のトラフィックやフロー情報、など
アラート情報	NICT内部のセキュリティ機器群のアラート情報、など
エンドポイント情報	NICT内部のPC端末内のプロセス情報、通信履歴、感染情報、など
マルウェア関連情報	マルウェア検体、静的解析結果、動的解析結果、など
スパム関連情報	スパム（ダブルバウンス）メール情報、など
Android関連情報	Android APK、カテゴリや説明文などアプリのメタデータ、など
ブログ・SNS情報	セキュリティベンダーブログ、ツイート、など
Webクローラ取集情報	URLリストやWebコンテンツ、それらの評価結果、など
ハニーポット収集情報	高対話型/低対話型/DRDoSハニーポット観測情報、など
脅威情報	有償/無償の脅威情報、IP/URLレピュテーション、C&C情報、など

まとめ

- サイバー空間と実空間の一体化は急激に進んでおり、これに伴い新たな脅威が生まれている。
- これに対抗するためには、サイバーセキュリティ研究の垣根を超えた、様々な分野との融合型研究が必要。
- その中でもAI技術との融合は重要で、既に大きなトレンドとなっている。
- このことは、データの重要性が今後ますます増していくことを意味しており、観測網や観測手法の充実・拡大はもとより、様々なデータを集約し、（国内の）研究機関等がデータ駆動型サイバーセキュリティ技術の研究開発に活用できる仕組みなども必要。

サイバーセキュリティ技術のロードマップ試案

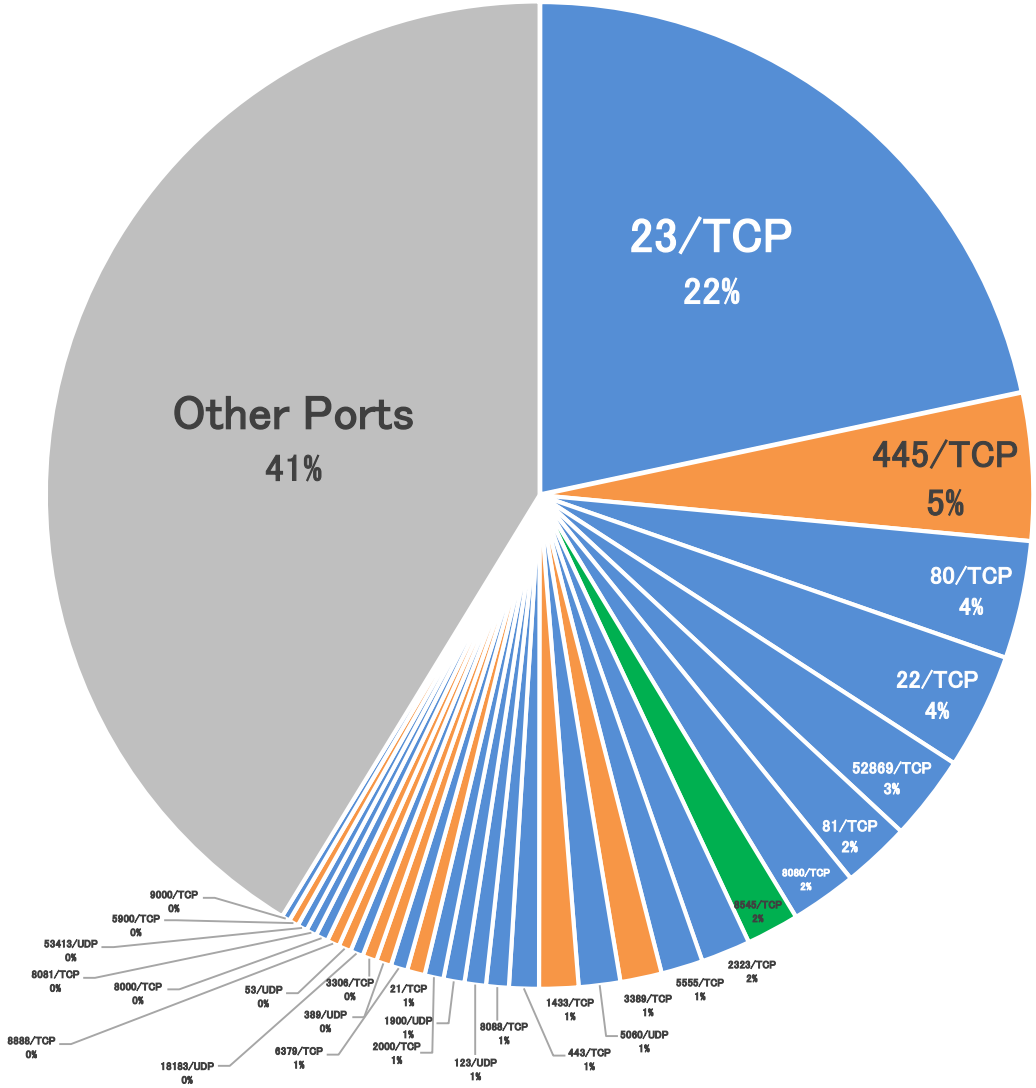
主な取組	2020年度	2021年度	2022年度	2023年度	2024年度	2025年度	アウトカムと社会的メリット 中間目標(2025年~) <成果目標(2030年)>
データ駆動型サイバーセキュリティ技術	グローバルサイバー攻撃観測網の運用／拡充／高度化 ・無差別型攻撃、大規模感染等をリアルタイムモニタ ・サイバー攻撃の世界的傾向の分析、新たな脅威の検知 能動的サイバー攻撃観測網の試験運用 能動的サイバー攻撃観測基盤の運用 ・標的型攻撃、Web媒介型攻撃等の調査・分析技術 ・新たなサイバー攻撃に対する対応技術の開発・実証 サイバーセキュリティ・統合テストベッドの構築／運用 複合型サイバー攻撃分析・可視化技術の試験運用 サイバーセキュリティ・ユニバーサル・リポジトリ（CURE）の実装／運用／高度化 ・サイバーセキュリティ関連情報を大規模集約 ・自動対策技術等によるセキュリティオペレーションの高度化 ・あらゆるサイバーセキュリティ関連情報を大規模集約 ・セキュリティ自動対策技術等を導入 ・可視化技術を高度化 ・セキュリティ検証、実証、人材育成 セキュリティ自動対策技術の研究開発 ・AI技術等を活用した分析支援技術、インシデント予兆検知技術等の研究開発と高度化						サイバー攻撃観測技術、可視化・分析技術を高度化するとともに、あらゆるサイバーセキュリティ関連情報を収集し、セキュリティ検証、実証、人材育成等に活用するためのサイバーセキュリティ統合テストベッドを構築し、我が国のサイバー攻撃対処能力の絶え間ない向上に貢献する。
エマージング・ネットワークセキュリティ技術	**次世代ネットワークセキュリティ** エミュレーション仮想環境の構築／高度化 ・次世代ネットワークセキュリティ検証技術の確立 ・次世代クラウド検証技術の確立 検証・分析 **コネクテッドデバイスセキュリティ** 検証環境の構築／高度化 ・IoTや通信機器等のコネクテッドデバイスセキュリティ検証技術の確立 検証・分析						今後世の中に出てくる新たなネットワーク環境におけるセキュリティを確保し、安心して新技術を享受できる社会の形成に貢献する。

参考資料

まずは **最近の動向**

感染機器の分布（2018年）

－ NICTER 観測レポート 2018：宛先ポート番号別パケット数分布 －



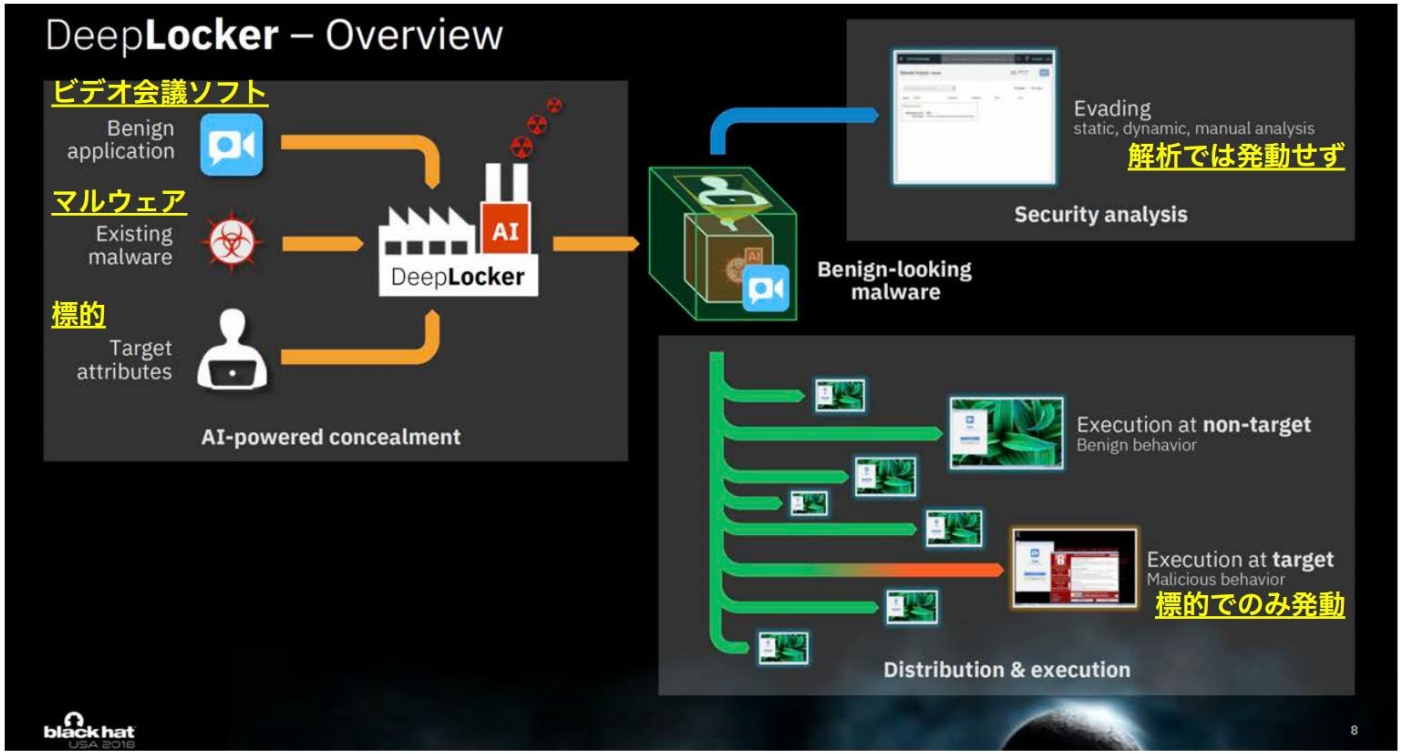
IoT = 47.7%（上位30ポート中）

ポート番号	攻撃対象
23/TCP	IoT機器（Webカメラ等）
445/TCP	Windows（サーバサービス）
80/TCP	Webサーバ（HTTP）
22/TCP	IoT機器（ルータ等） 認証サーバ（SSH）
52869/TCP	IoT機器（ホームルータ等）
81/TCP	IoT機器（ホームルータ等）
8080/TCP	IoT機器（Webカメラ等）
8545/TCP	イーサリアム（仮想通貨）
2323/TCP	IoT機器（Webカメラ等）
5555/TCP	Android機器 （セットトップボックス等）

AI（機械学習）を使ったマルウェア（1/2）

コンセプト実証

- AIマルウェアをビデオ会議ソフトに混入し標的となる人物の顔画像を学習
- 標的となる人物がビデオ会議機能を使用した際にのみマルウェアが発動

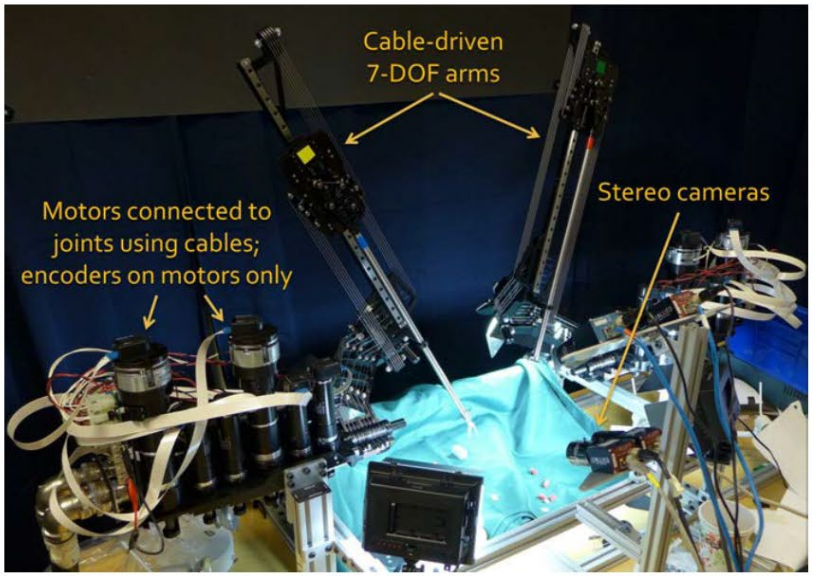


Dhilung Kirat, et al., “DeepLocker,” Black Hat USA 2018, Aug, 2018.
https://i.blackhat.com/us-18/Thu-August-9/us-18-Kirat-DeepLocker-Concealing-Targeted-Attacks-with-AI-Locksmithing.pdf

AI（機械学習）を使ったマルウェア（2/2）

コンセプト実証

- 遠隔外科手術用ロボット『Raven-II』に感染するマルウェア
- ロボットOS（ROS）に感染後、**潜伏し手術の挙動を学習**
- **手術中の最も重要な局面でエラー注入し、誤動作を起こさせる**



Raven-II

出典：http://rll.berkeley.edu/surgical/control/state_estimation.html

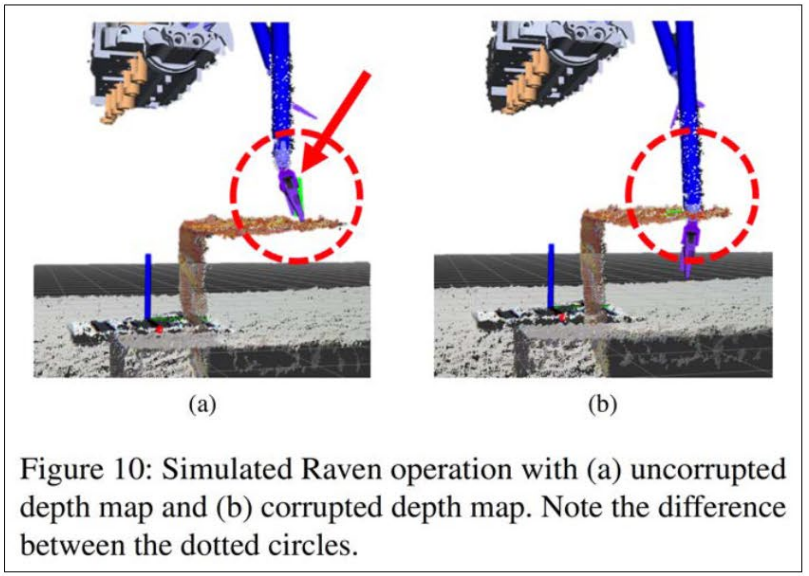


Figure 10: Simulated Raven operation with (a) uncorrupted depth map and (b) corrupted depth map. Note the difference between the dotted circles.

エラー注入による誤動作

出典：https://www.usenix.org/conference/raid2019/presentation/chung

Keywhan Chung, et al., "Smart Malware that Uses Leaked Control Data of Robotic Applications: The Case of Raven-II Surgical Robots," RAID 2019, Sep, 2019.