攻撃観測研究の新たなステージ
～サイバー世界の”PCR検査”の実現に向けて～

吉岡　克成

横浜国立大学
大学院環境情報研究院/先端科学高等研究院　准教授

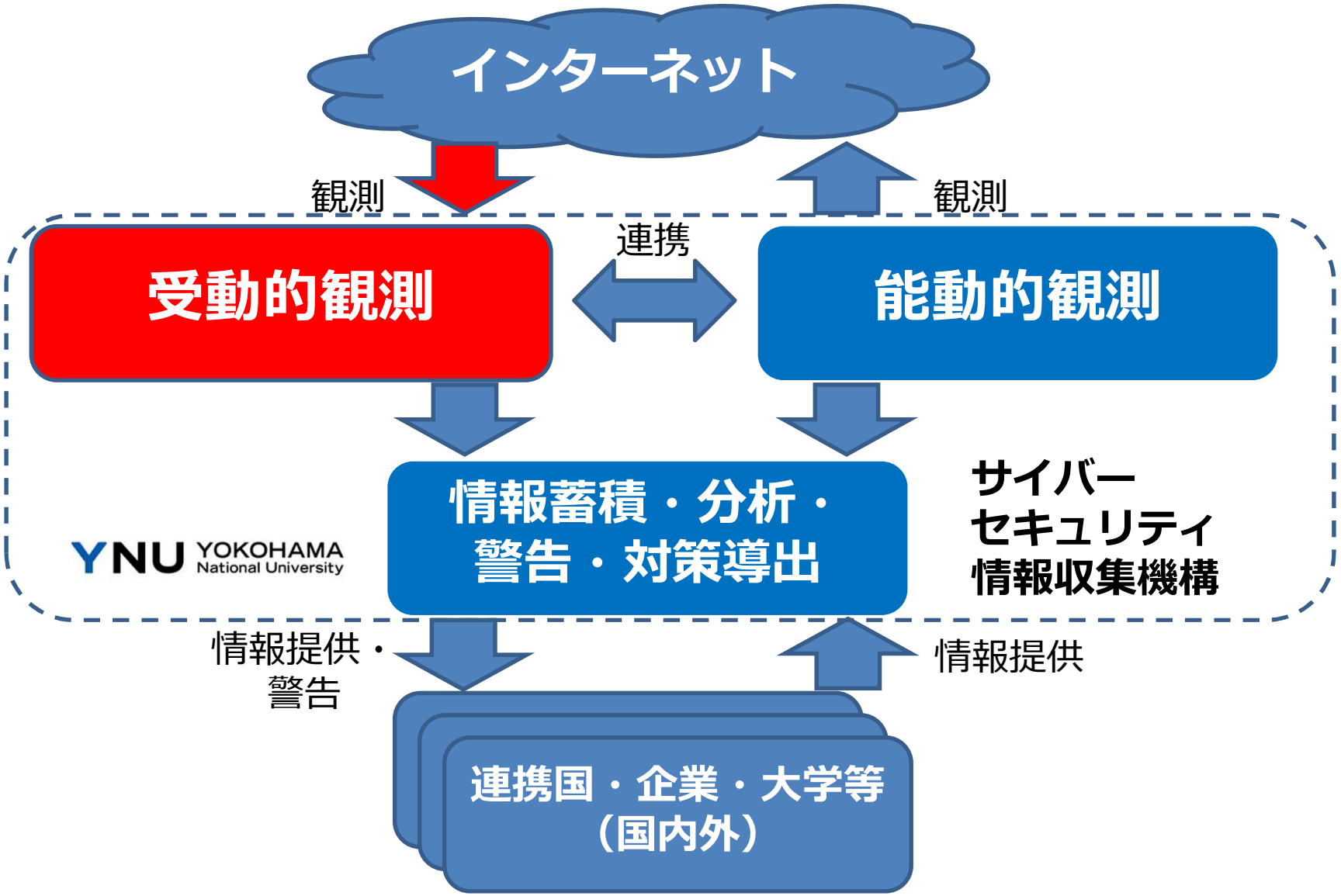
JSSEC/SIOTP セキュリティフォーラム2021（2021/6/9）

横浜国大では…

- 2015年からIoT等におけるサイバー攻撃を観測したり、脆弱な機器を探索するシステムを世界に先駆けて構築・運用開始し、現在まで継続的に観測・分析を行ってきました

- 本日は、観測・分析の深化と、観測結果をいかに実際の機器やシステムのセキュリティ向上に役立てるか、という観点での、対策研究についてお話をさせて頂きます

サイバーセキュリティ情報収集機構



IoTハニーポット（2015～）

IoT機器へのサイバー攻撃を観測する囮システム（IoTハニーポット）を世界に先駆けて構築・観測開始

攻撃元機器（マルウェア感染済）

攻撃者が用意したサーバ

Yin Minn Pa Pa, Shogo Suzuki, Katsunari Yoshioka, and Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow, "IoTPOT: Analysing the Rise of IoT Compromises," 9th USENIX Workshop on Offensive Technologies (USENIX WOOT 2015), 2015.
Yin Minn Pa Pa, Suzuki Shogo, Katsunari Yoshioka, Tsutomu Matsumoto, Takahiro Kasama, Christian Rossow "IoTPOT: A Novel Honeypot for Revealing Current IoT Threats," Journal of Information Processing, Vol. 57, No. 4, 2016.

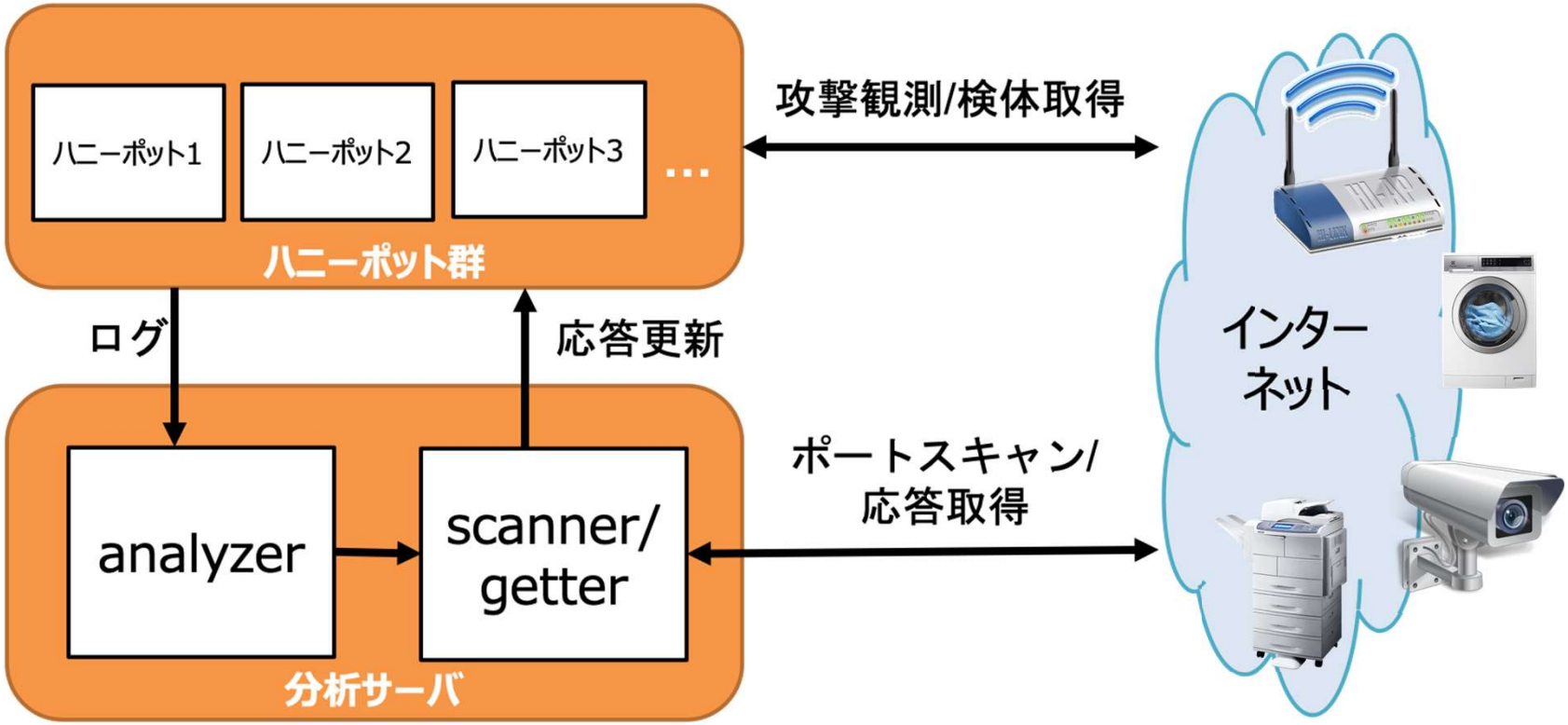
IoTハニーポットに関わる数字

運用年数:	6年間
ハニーポット設置国・地域:	16か国・地域
累計収集検体数（ハッシュ値ベース）:	174,831検体‡
検体等提供組織数:	124組織
検体等提供先国数:	32か国・地域
学術論文引用件数†:	431件（71.8件/年）

‡ 2017/11～2021/06/05現在での集計（EFLファイルのみ）
† 関連論文2件の合計（Google Scholarによる集計値，2021/6/5現在）

新型IoTハニーポット(X-Pot)

攻撃が増加しているサービスの応答をインターネット上の機器から収集しハニーポットに適用することで、様々な機器の模擬を行う



従来手法に比べて、最大で3.5倍の検体収集可能

Seiya Kato, Rui Tanabe, Katsunari Yoshioka, Tsutomu Matsumoto, "Adaptive Observation of Emerging Cyber Attacks targeting Various IoT Devices," IFIP/IEEE International Symposium on Integrated Network Management (IM), 2021.

横浜国大で開発・運用中のハニーポット

- Amppot（2014～）

アンプ攻撃（反射型分散サービス妨害攻撃）を観測する機構

- インフラハニーポット（2018～）

重要施設の遠隔監視制御システムを模したハニーポット

- Etherpot（2021～）

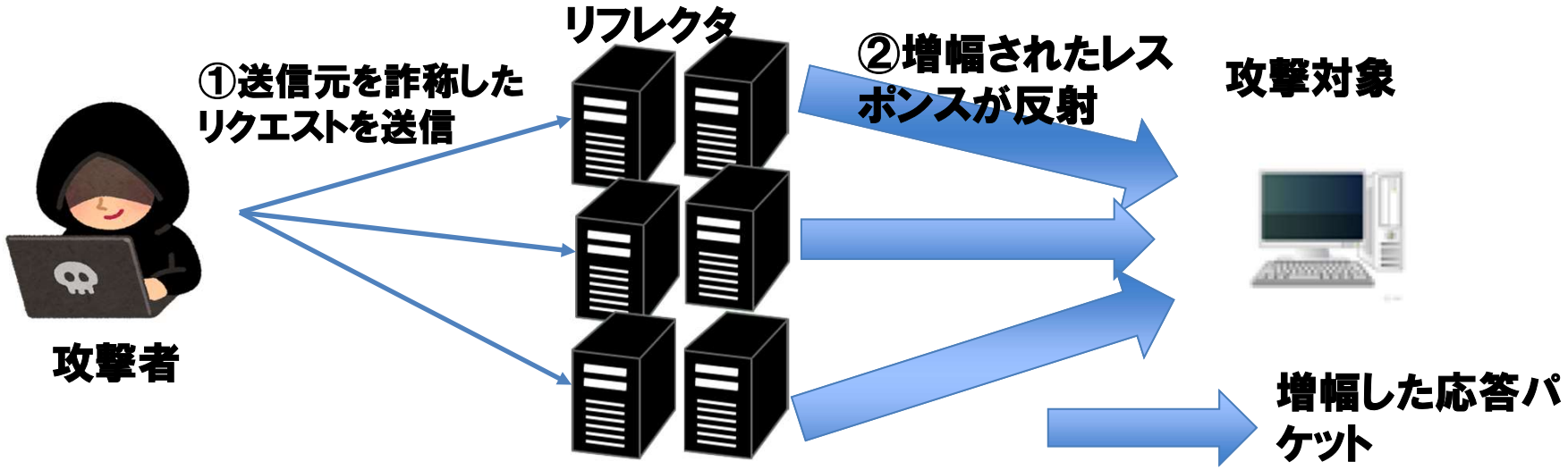
スマートコントラクト、仮想通貨を扱うEthereumクライアントへの
サイバー攻撃を観測するハニーポット

- テレワークハニーポット（開発中）

テレワーク環境（VPN, RDP）の脆弱性を狙う攻撃を観測する
ハニーポット

アンプ攻撃（反射型分散サービス妨害攻撃）

- インターネット上の様々なオープンサービスを悪用して、トラヒックを増幅するサービス妨害攻撃
- 2020年2月にCLDAPを悪用してAWSに2.3Tbpsの攻撃 [1]
- 従来よりDNSやNTPの悪用が知られているが、実際には20以上のサービスが悪用されている



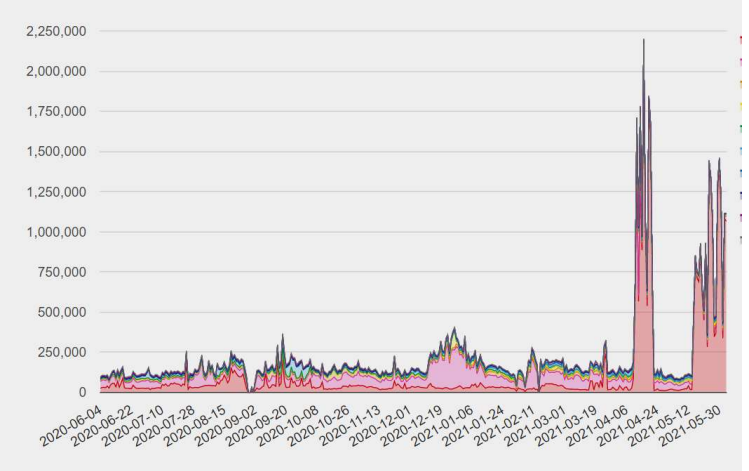
[1] AWS shield, https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf

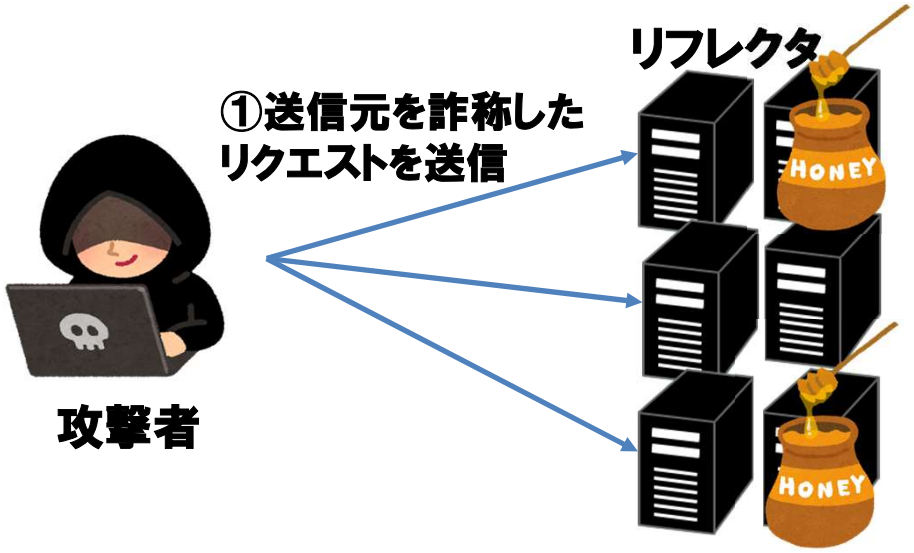
Amppot（アンプ攻撃観測用ハニーポット）

踏み台に出来そうに見せかけたオープンサービスを用意して攻撃を観測

約10万件/日、国内で約700件/日の攻撃を検知

攻撃検知時に警報を発行





List of abused protocols observed by agnostic Amppot (Agnostic Amppot listens on all UDP ports and returns random strings)

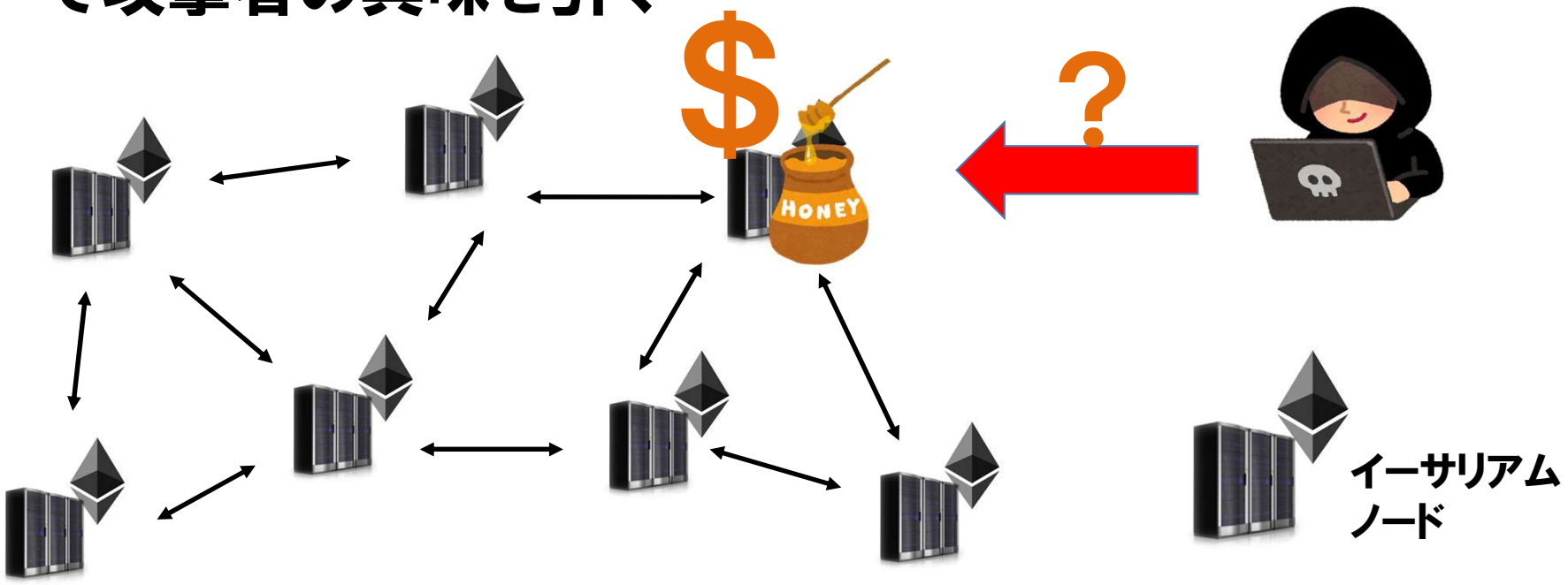
Service	Port	#Attack
CLDAP	389	6656999
DTLS	443	53781
DNS	53	39168
WSD	3702	26775
ARMS	3283	24864
Dahua Discovery	37810	23868
MSSQL	1434	14816
STUN	3478	10346
Portmap	111	9785
NTP	123	7523

The table shows the number of attacks observed by agnostic Amppot over the last 7 days.

[1] AWS shield, https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf

Etherpot（イーサリアムハニーポット）

- 設定に不備のある（＝JSON-RPC APIが外部からアクセスできる状態の）イーサリアムノードを模擬して攻撃を観測
- 大量の仮想通貨（Ether）を保持しているように見せかけて攻撃者の興味を引く

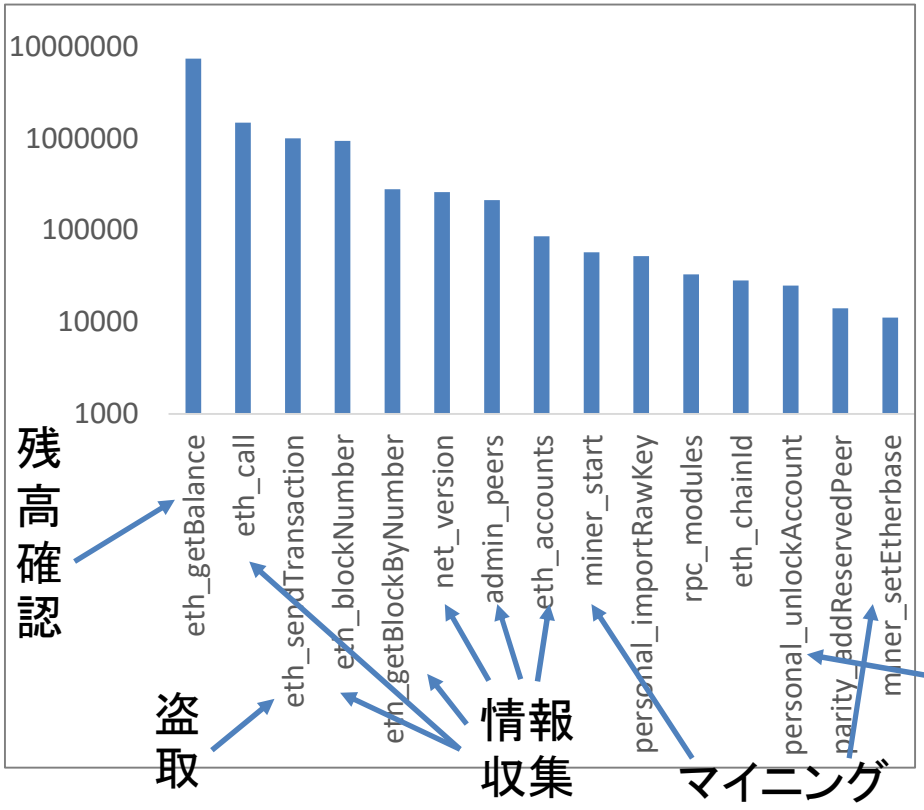


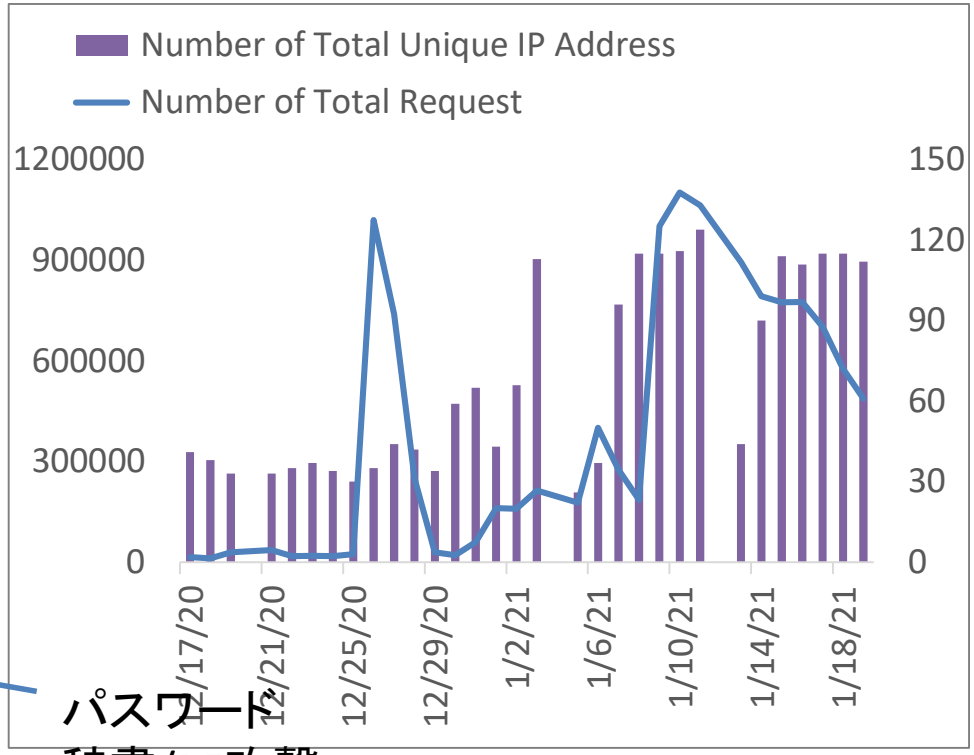
イーサリアムP2Pネットワーク

Jia WANG, Takayuki SASAKI, Kazumasa OMOTE, Katsunari YOSHIOKA, Tsutomu MATSUMOTO, "Etherpot: A Honeypot for Observing Cyberattacks on Ethereum Client," IEICE, 2021-06-IA-ICSS, 2021.

Etherpot（イーサリアムハニーポット）

1か月で478のIPアドレスから1200万件の不正なリクエストを観測
主に（1）情報収集（2）残高確認→辞書/BF攻撃→仮想通貨の盗取
（3）仮想通貨採掘（マイニング）命令（4）エクリプス攻撃　を観測

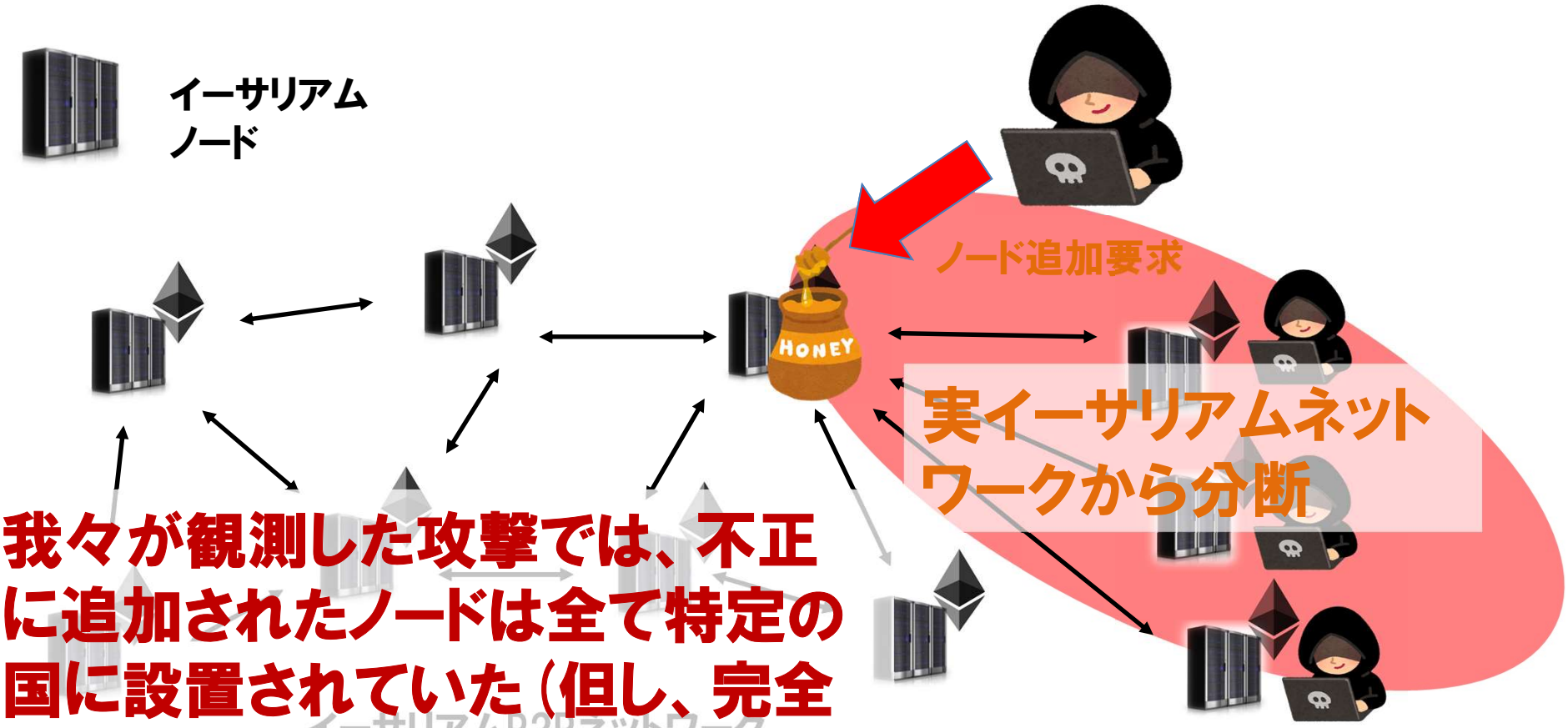




Jia WANG, Takayuki SASAKI, Kazumasa OMOTE, Katsunari YOSHIOKA, Tsutomu MATSUMOTO, "Etherpot: A Honeypot for Observing Cyberattacks on Ethereum Client," IEICE, 2021-06-IA-ICSS, 2021.

エクリプス攻撃

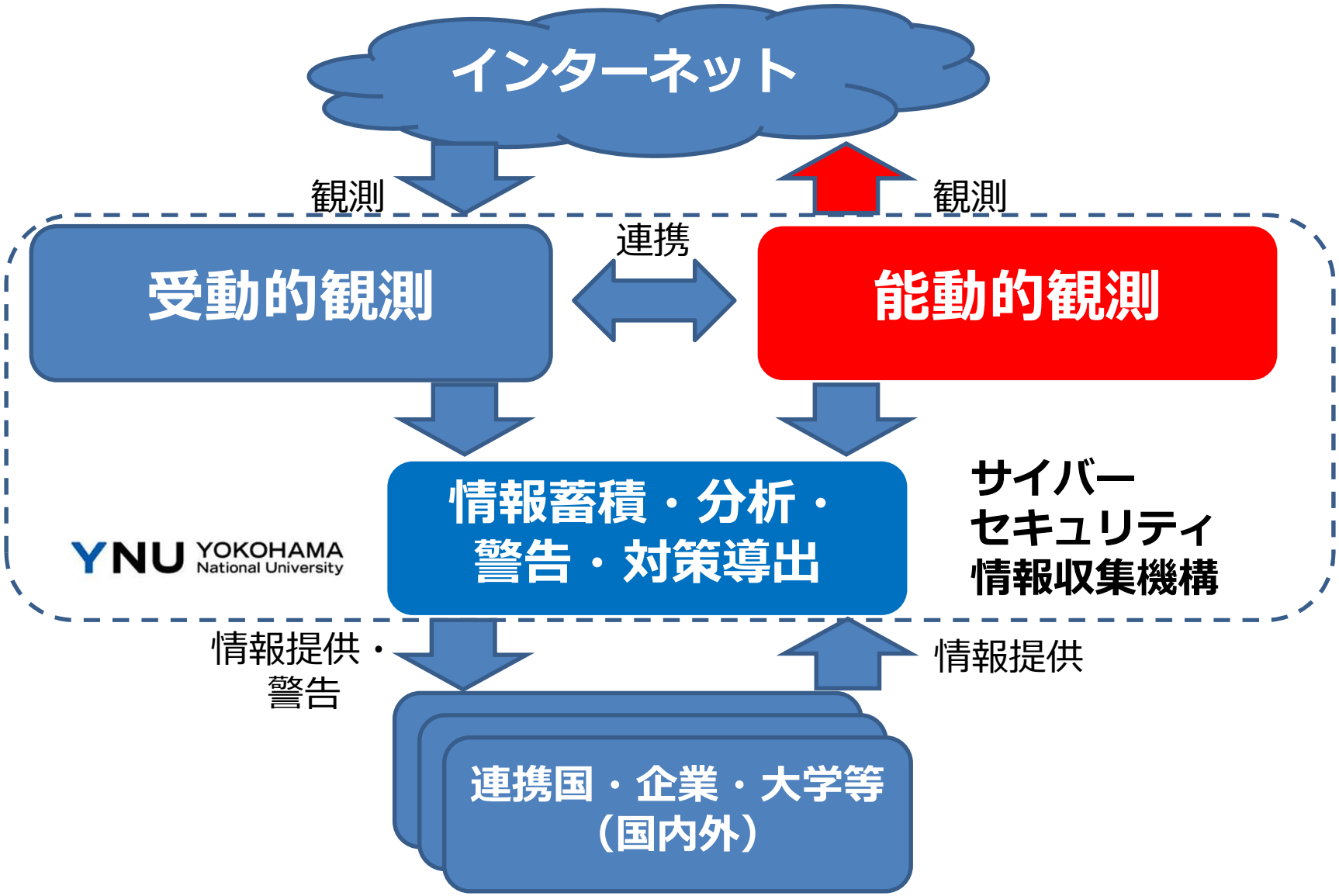
攻撃対象ノードの接続先リストに自らが操作するノード群を強制的に追加することで実イーサリアムネットワークと分断し、不正を行う攻撃



我々が観測した攻撃では、不正に追加されたノードは全て特定の国に設置されていた（但し、完全なNW分離は出来ていなかった）

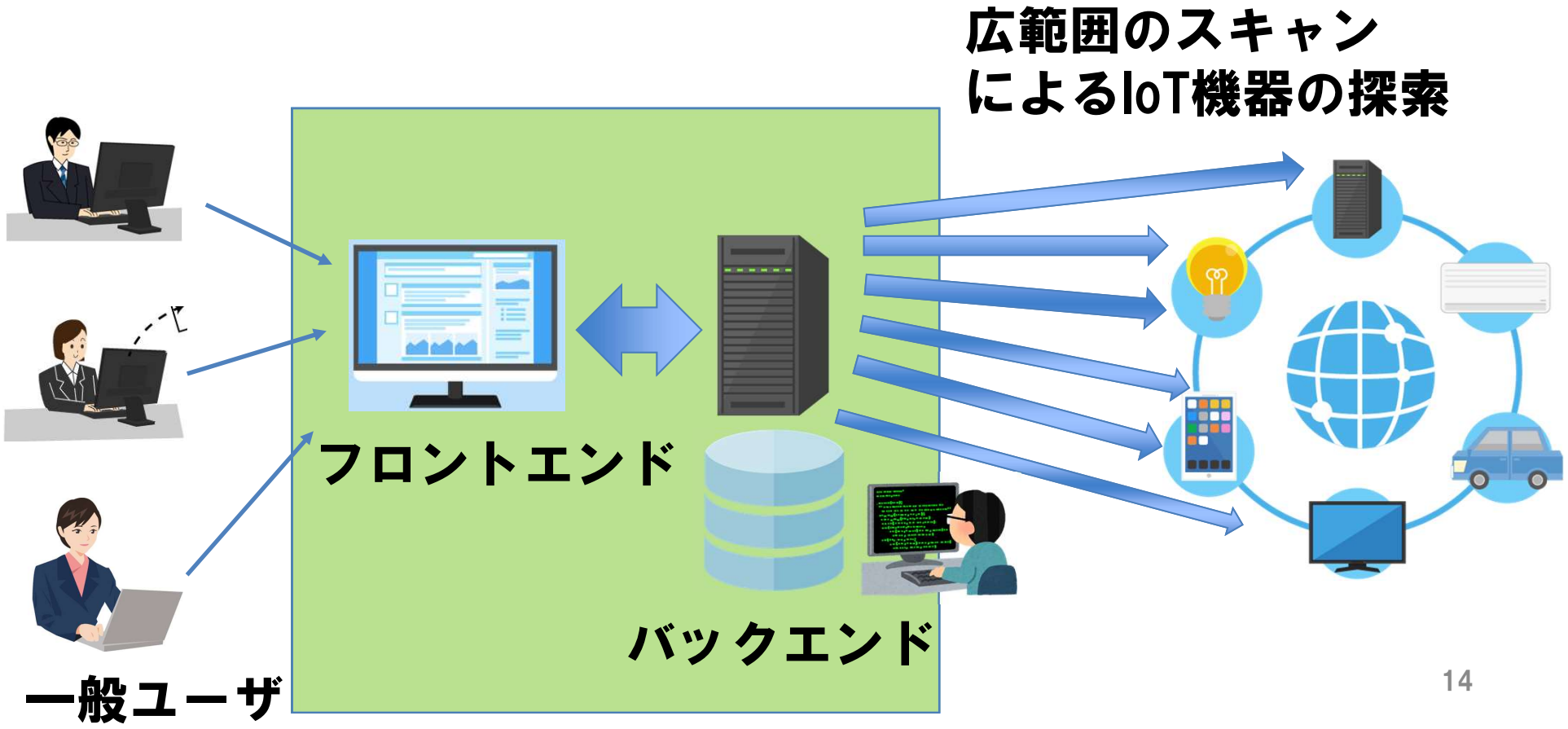
[1] Yuki YOSHIOKA, Tsutomu MATSUMOTO, "Etherpot: A Honeypot for Observing Cyberattacks on Ethereum Client," IEICE, 2021-06-IA-ICSS, 2021.

サイバーセキュリティ情報収集機構



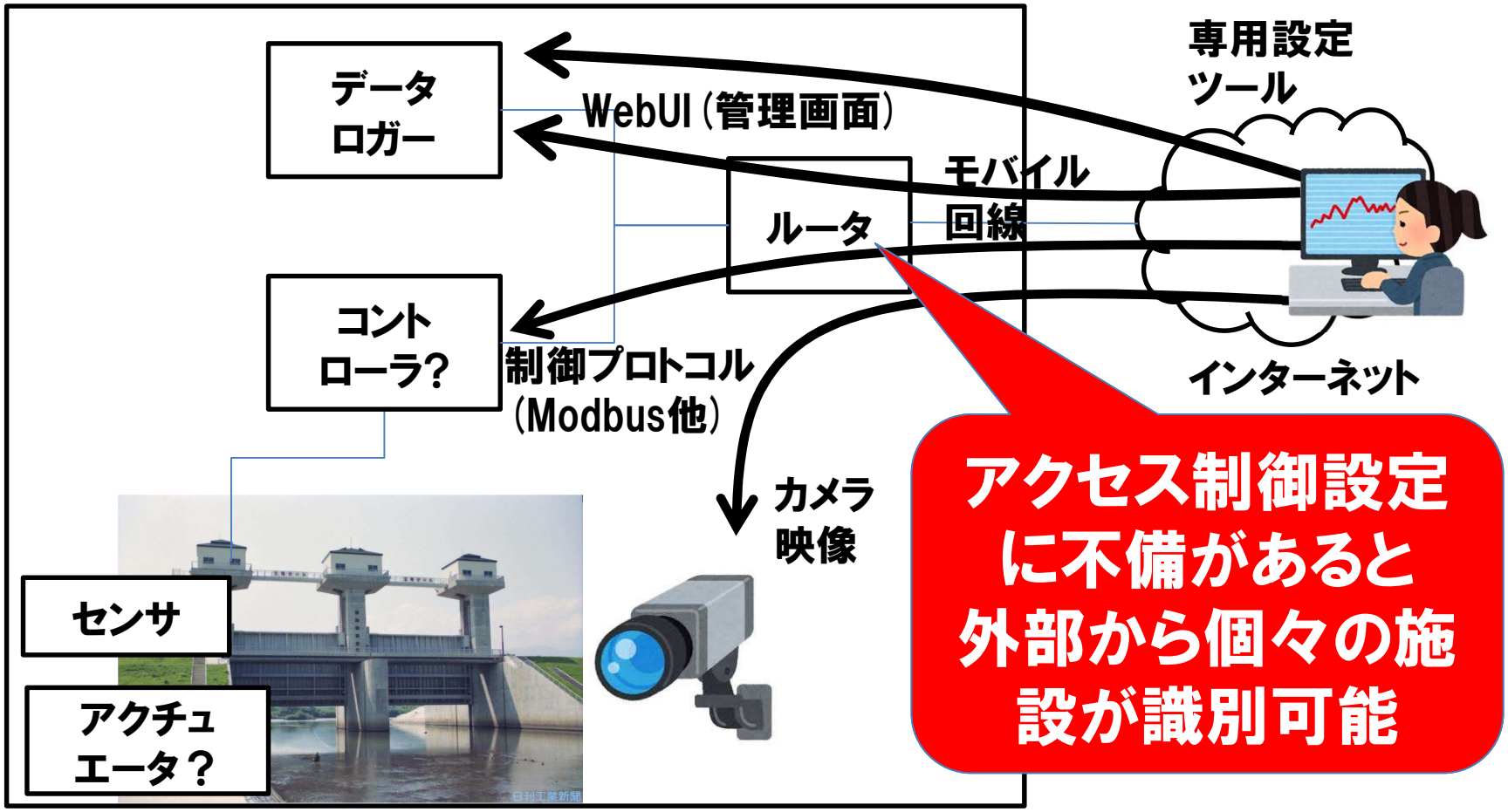
広域スキャンシステム

広域ネットワークをスキャンし、脆弱なIoT機器等の探索を行うシステム

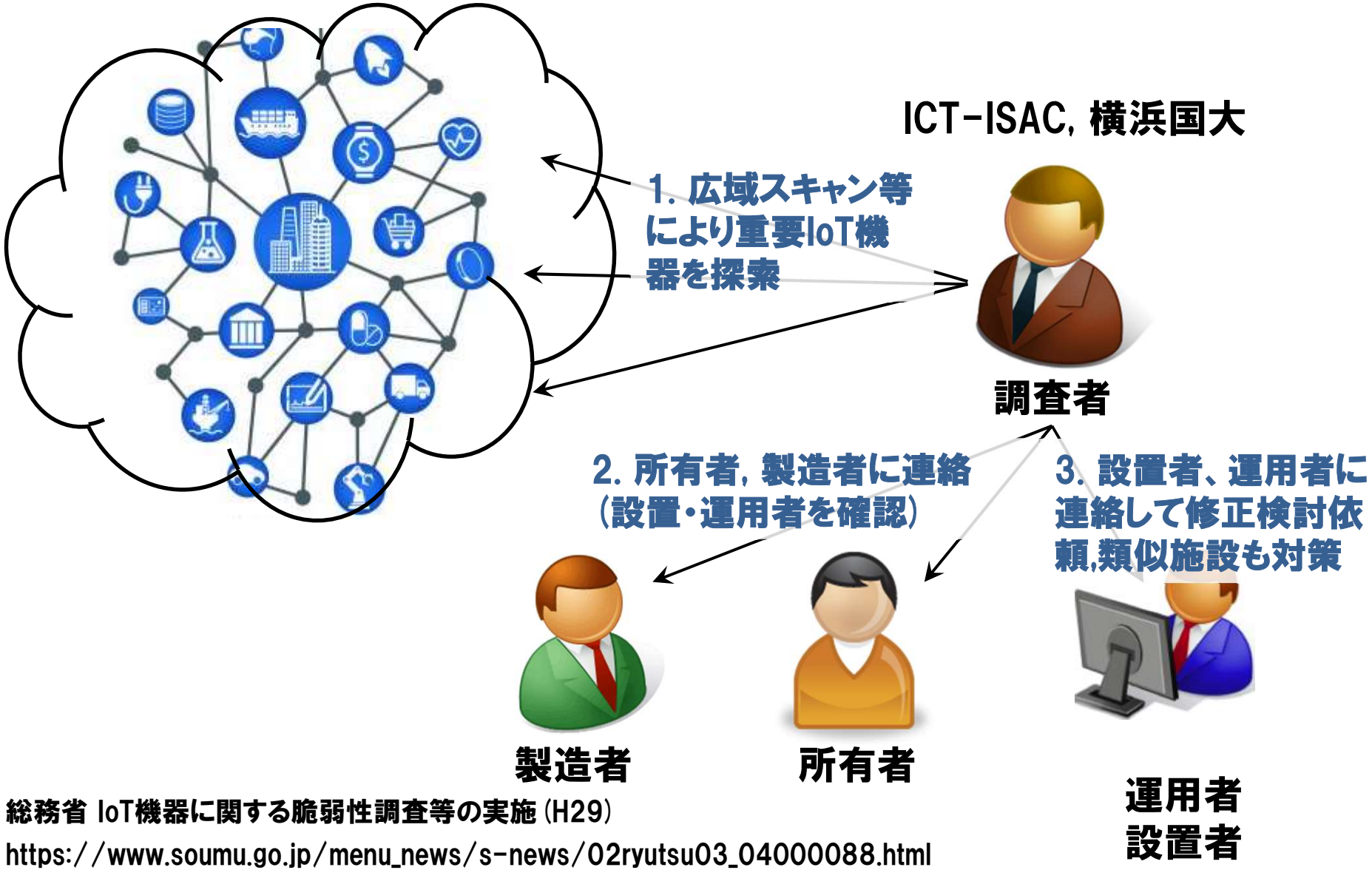


「重要IoT機器」とは？

治水、防災、発電など重要な施設の遠隔監視を行うためのデータロガーや制御機器



総務省 IoT機器に関する脆弱性調査等の実施（2017）



総務省 IoT機器に関する脆弱性調査等の実施（H29）
https://www.soumu.go.jp/menu_news/s-news/02ryutsu03_04000088.html

調査結果（2017）

- 調査により検出した脆弱な重要IoT機器候補：150件
- 利用者等に関する情報が得られたもの：77件
- 注意喚起等を行ったもの：36件
  パスワード設定が適切でない：27件
  パスワード設定はされているが認証画面がインターネット上で公開されていた：9件

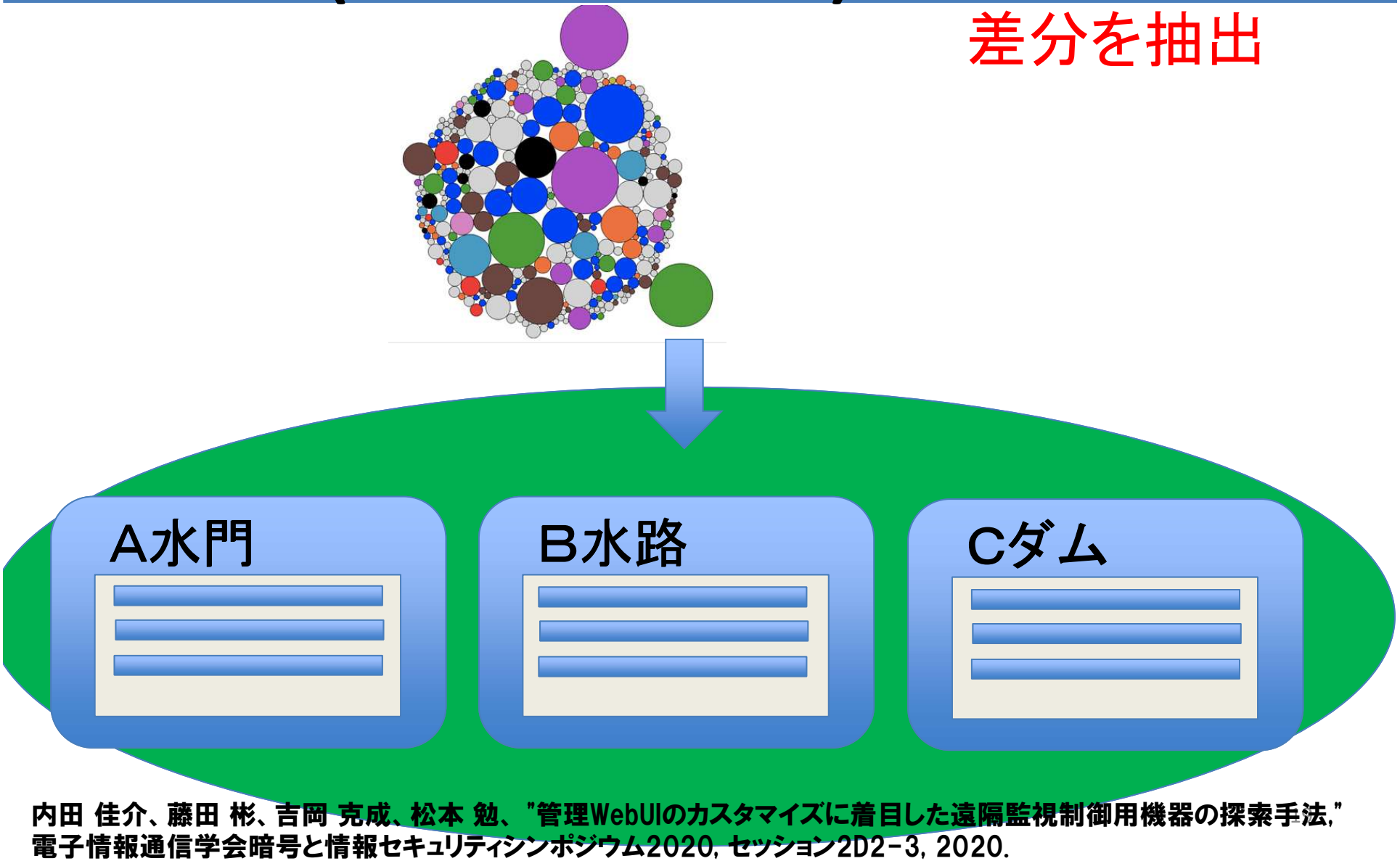
- 検出された重要IoT機器の例
  - 消費電力監視装置
  - 水位監視装置
  - 防災設備制御装置
  - ガス観測警報通知装置等

総務省
重要IOT機器調査
2020

ICT-ISAC, 脆弱な状態にある重要IoT機器※1の調査及び注意喚起について
https://www.ict-isac.jp/news/news20200728.html

同一クラスタ内で
差分(カスタマイズ部)を自動抽出

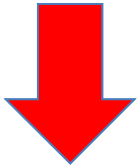
差分を抽出



内田 佳介、藤田 彬、吉岡 克成、松本 勉、"管理WebUIのカスタマイズに着目した遠隔監視制御用機器の探索手法," 電子情報通信学会暗号と情報セキュリティシンポジウム2020, セッション2D2-3, 2020.

2017年度

（重要機器候補）150件

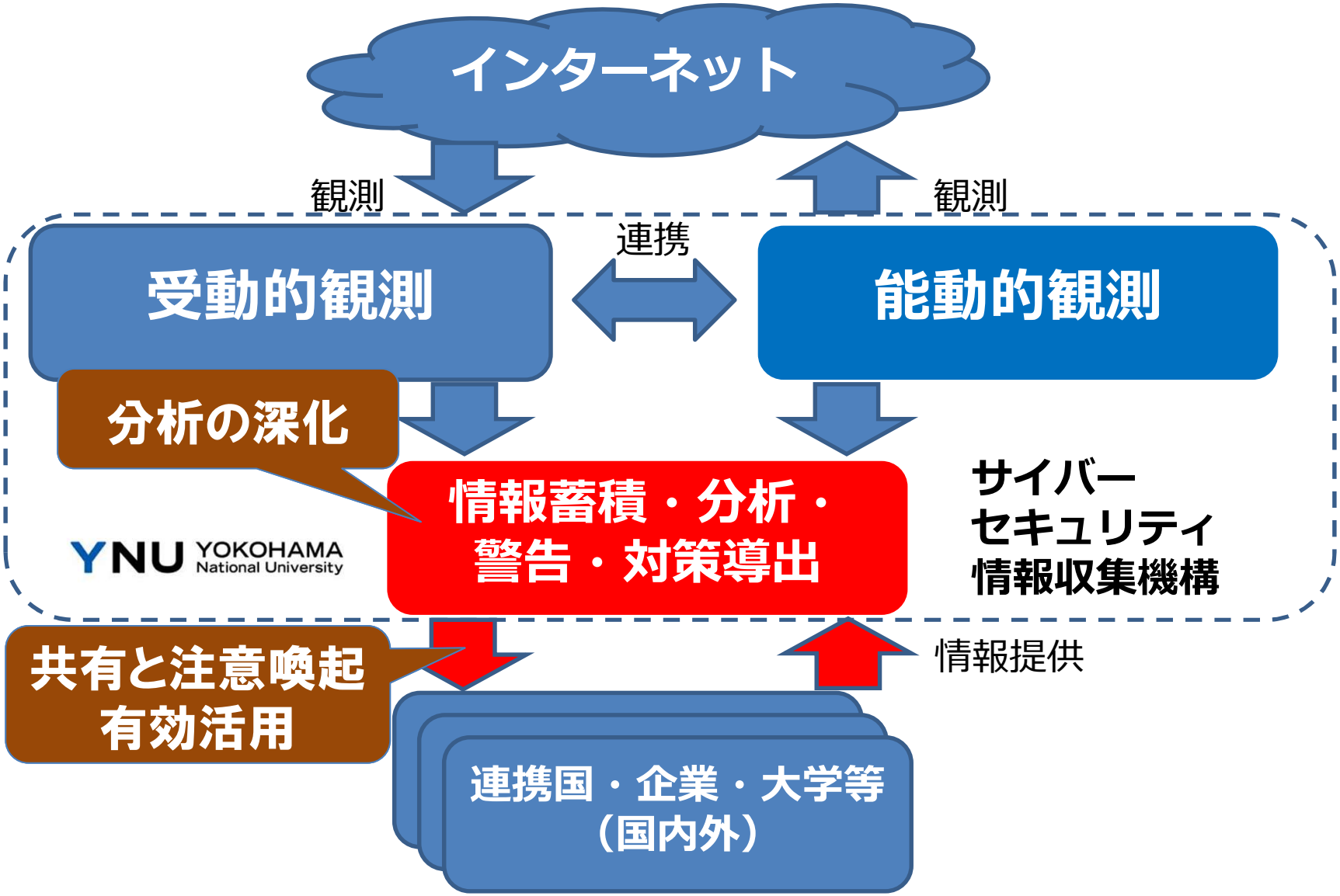


2020年度

（重要機器候補）900件+

これらの機器は、既存の広域スキャンシステム（Shodan/Censys）では
ほとんど検知されない

サイバーセキュリティ情報収集機構



分析の深化により
観測結果の価値を高める

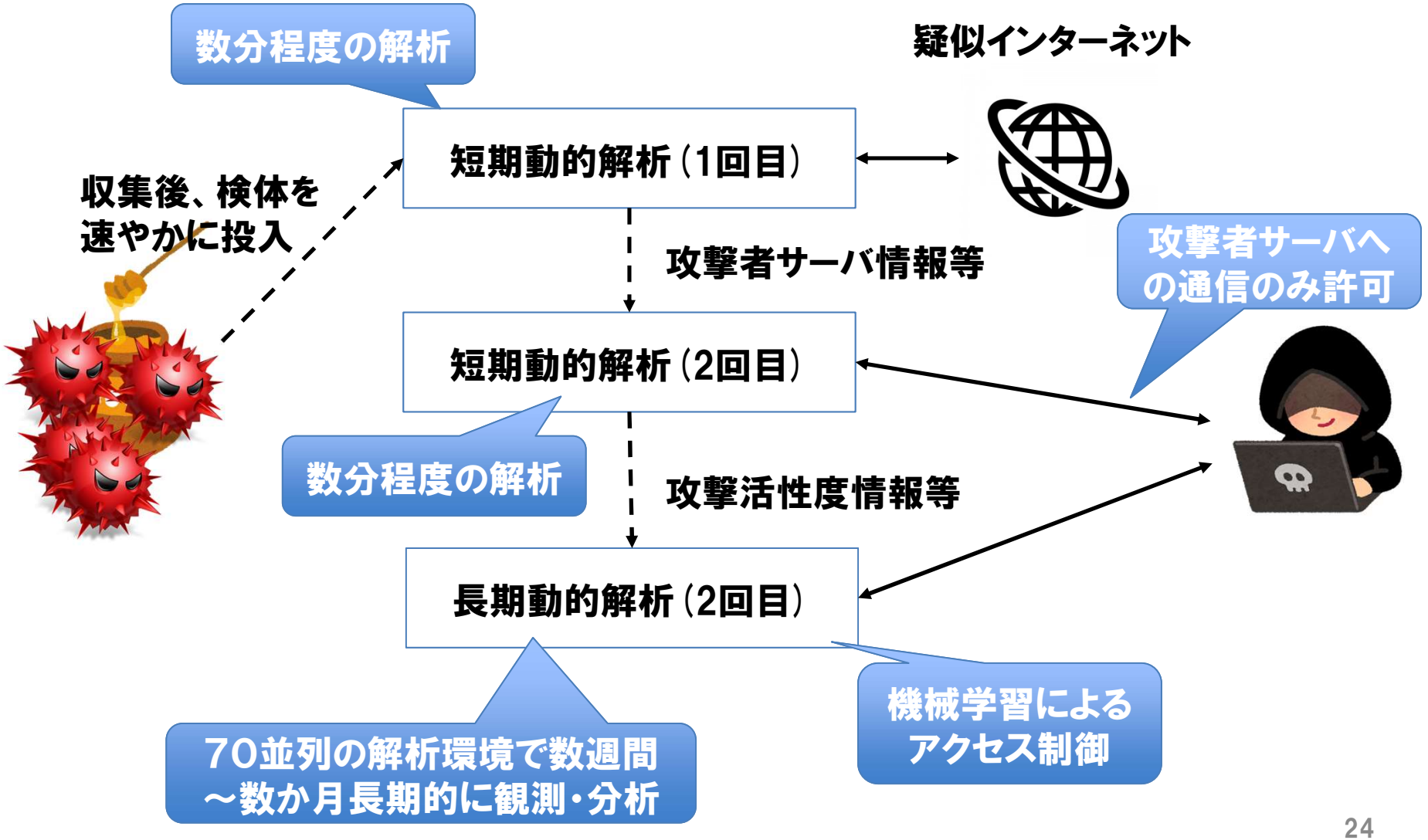
ハニーポットで収集した IoTマルウェア検体の解析

- どのような感染活動を行うのか？
  どのような脆弱性を狙うのか？

- マルウェアを操作するC＆Cサーバ、マルウェアダウンロードサーバはどのように運用されているか？

- 感染後はどのような活動を行うのか？

IoTマルウェア解析機構



短期動的解析成果例（脆弱性の悪用）

- 各検体を安全な環境で実行することで脆弱性攻撃を観測
- 脆弱性DBと突合することで新規性を判断

最新の脆弱性が
悪用される一方、
10年以上前の
脆弱性も未だに
狙われている

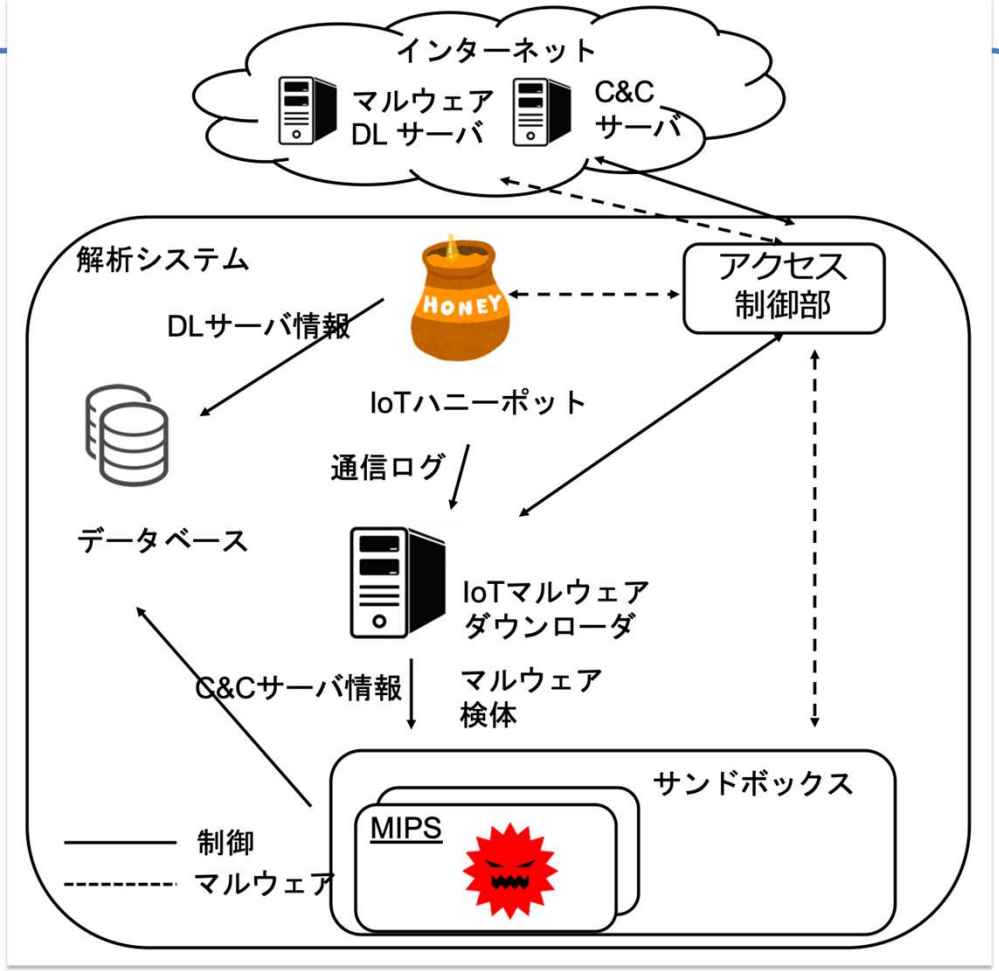
一部未発表論文の成果であるため、画像を削除しています。

X 脆弱性公開日

既知・未知の攻撃について侵入検知システムのルール化（シグネチャ生成）が可能

注：一部の結果は動的解析に加えて静的解析により得られました

攻撃インフラの観測



ハニーポットで収集した検体を定常的にサンドボックス上で動作させ、攻撃者が感染機器を操作するための「攻撃インフラ」を継続的に観測

特定したマルウェアダウンロードURL累計：163,962件

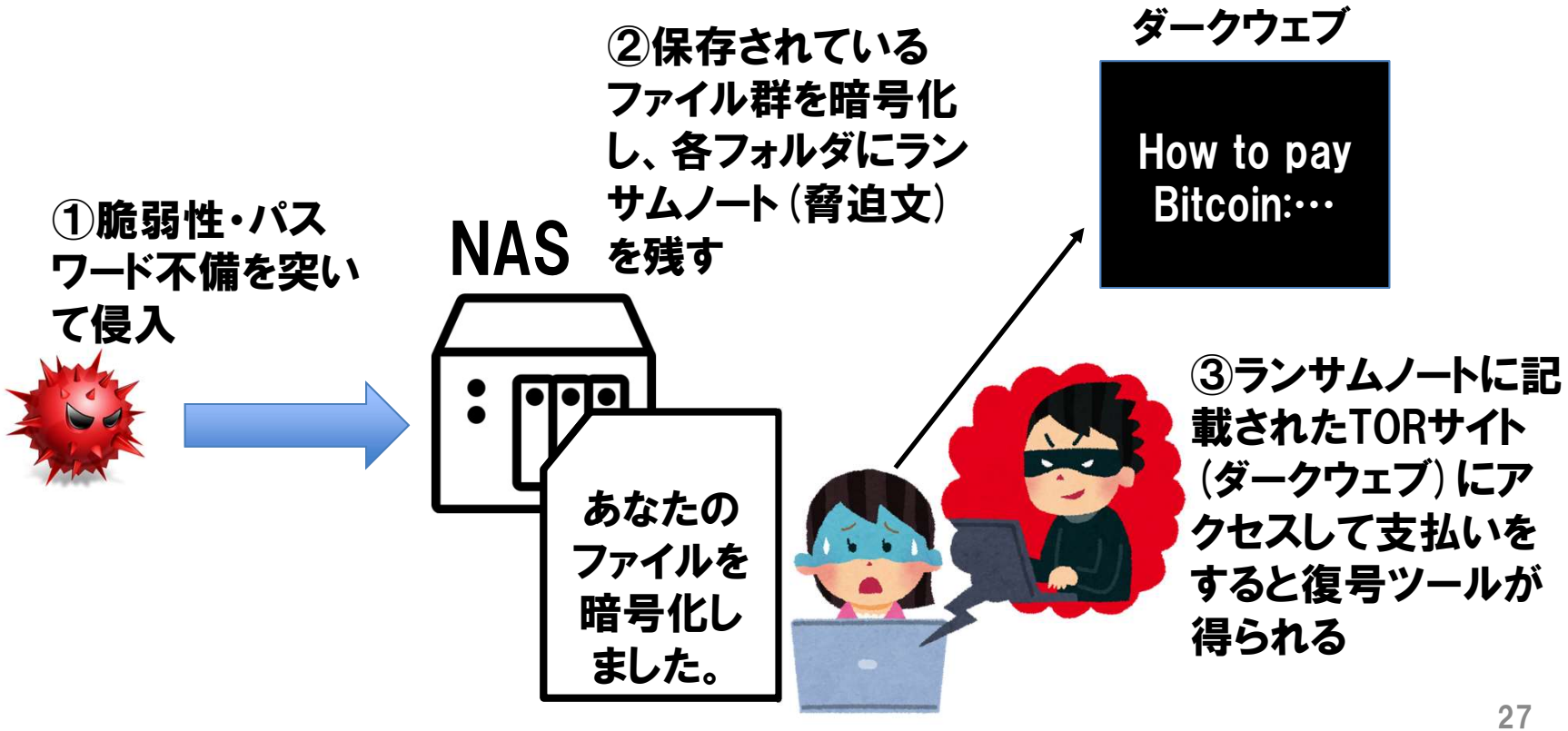
特定したC&Cサーバ累計：3,578件

(2021/06/05現在)

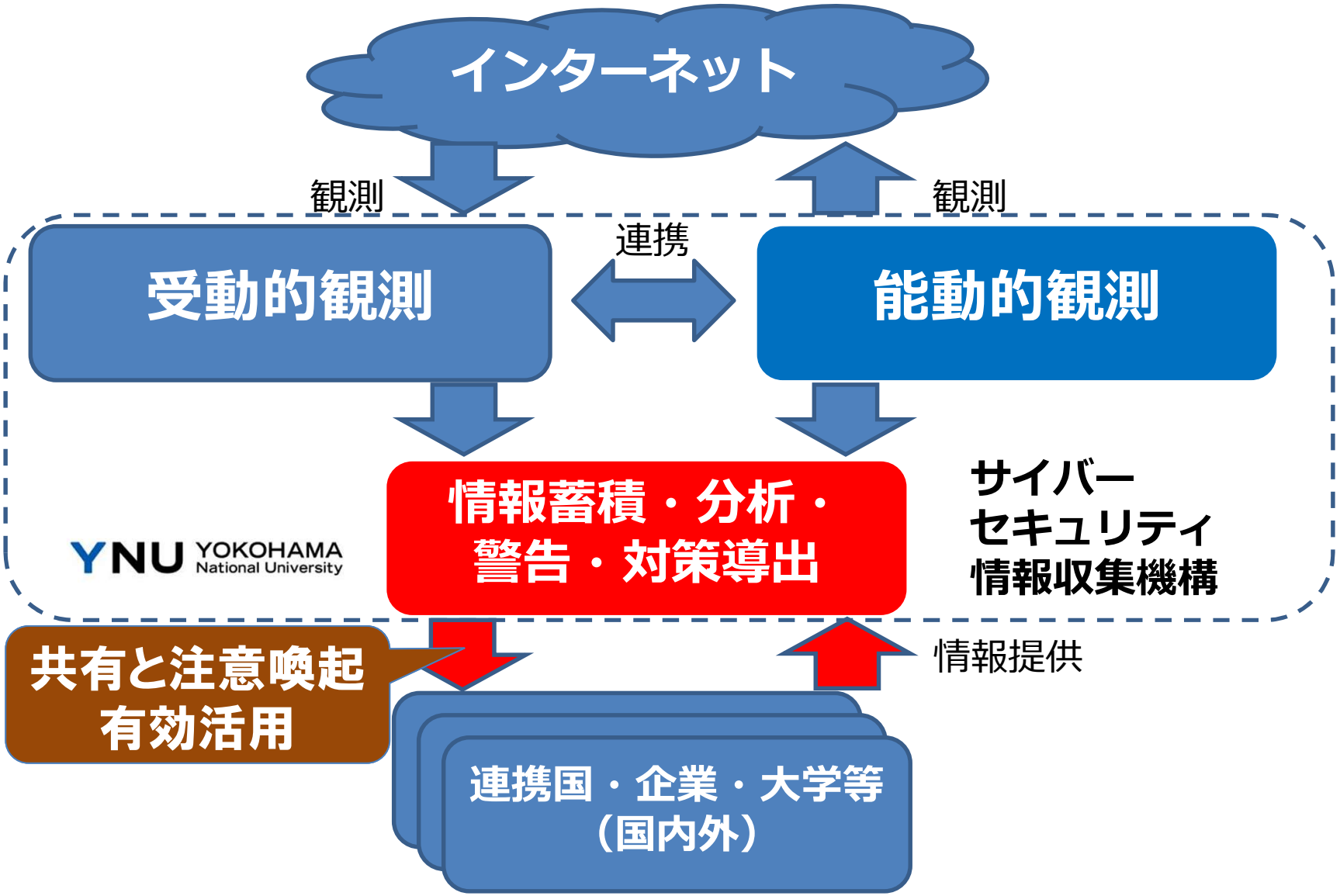
Rui Tanabe, Tatsuya Tamai, Akira Fujita, Ryoichi Isawa, Katsunari Yoshioka, Tsutomu Matsumoto, Carlos Ganan and Michel Van Eeten, "Disposable Botnets: Examining the Anatomy of IoT Botnet Infrastructure," Proc. International Conference on Availability, Reliability, and Security (ARES2020), 2020.

詳細解析 IoTランサムウェア解析例

NAS (Network Attached Storage) 内に保存されたファイルを人質にとるランサム攻撃が国内外で発生し、被害が出ている

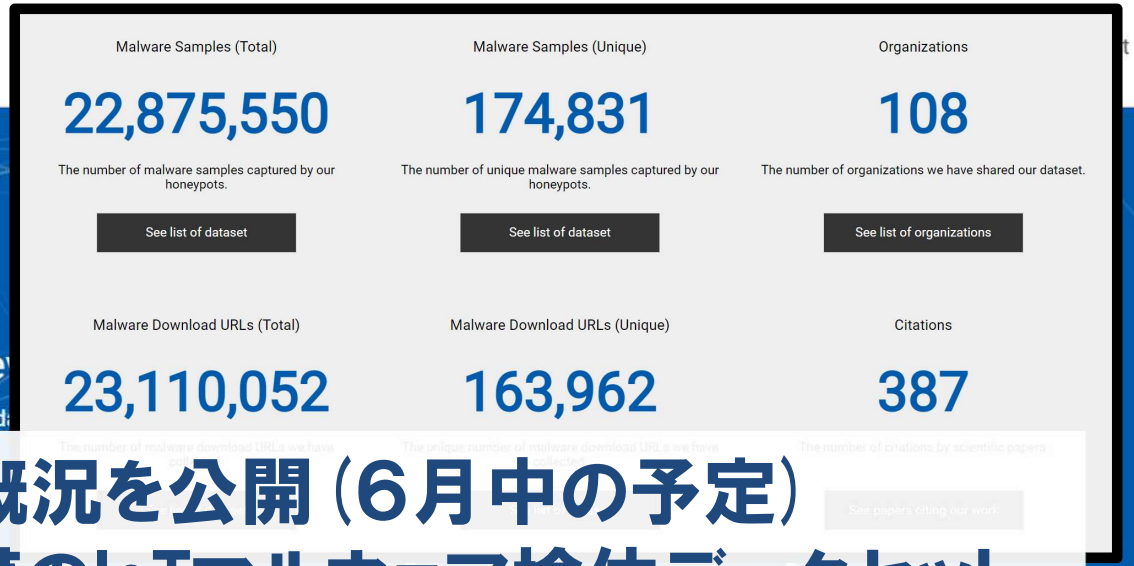


サイバーセキュリティ情報収集機構



情報共有・注意喚起により
観測成果を有効活用する

情報提供サイトの公開
（1）IoTハニーポット



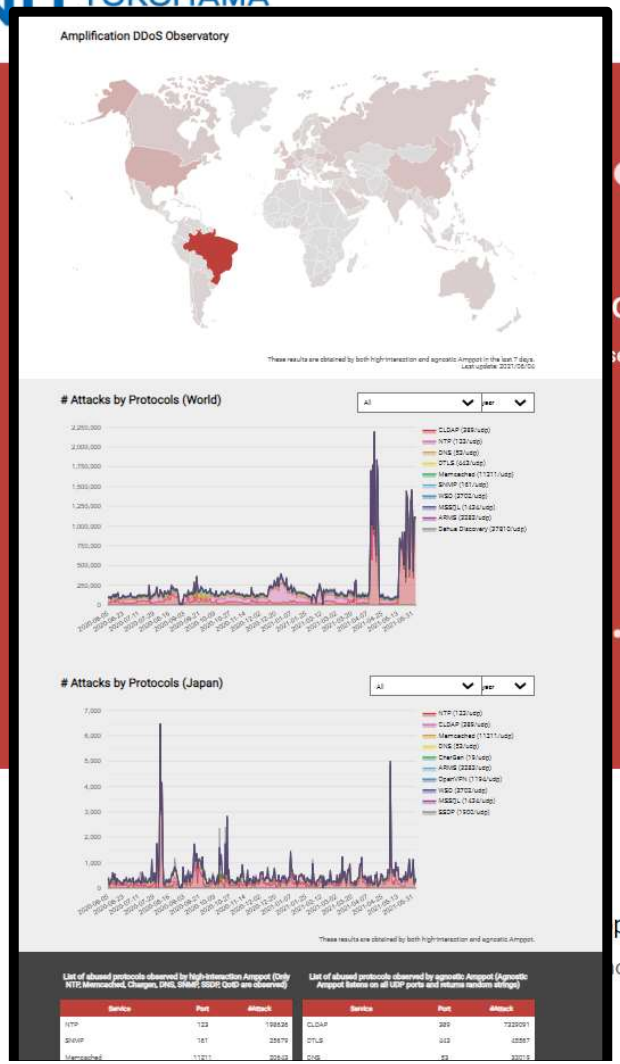
最新の観測結果の概況を公開（6月中の予定）
世界的にも最大規模のIoTマルウェア検体データセット（17万＋）、マルウェアダウンロードURLを研究者・開発者向けに提供（6月中の予定）

今後は攻撃検知用シグネチャ、C2リストも提供予定

re binaries)

Dataset-2 (IoT honeypot: Malware download URLs)

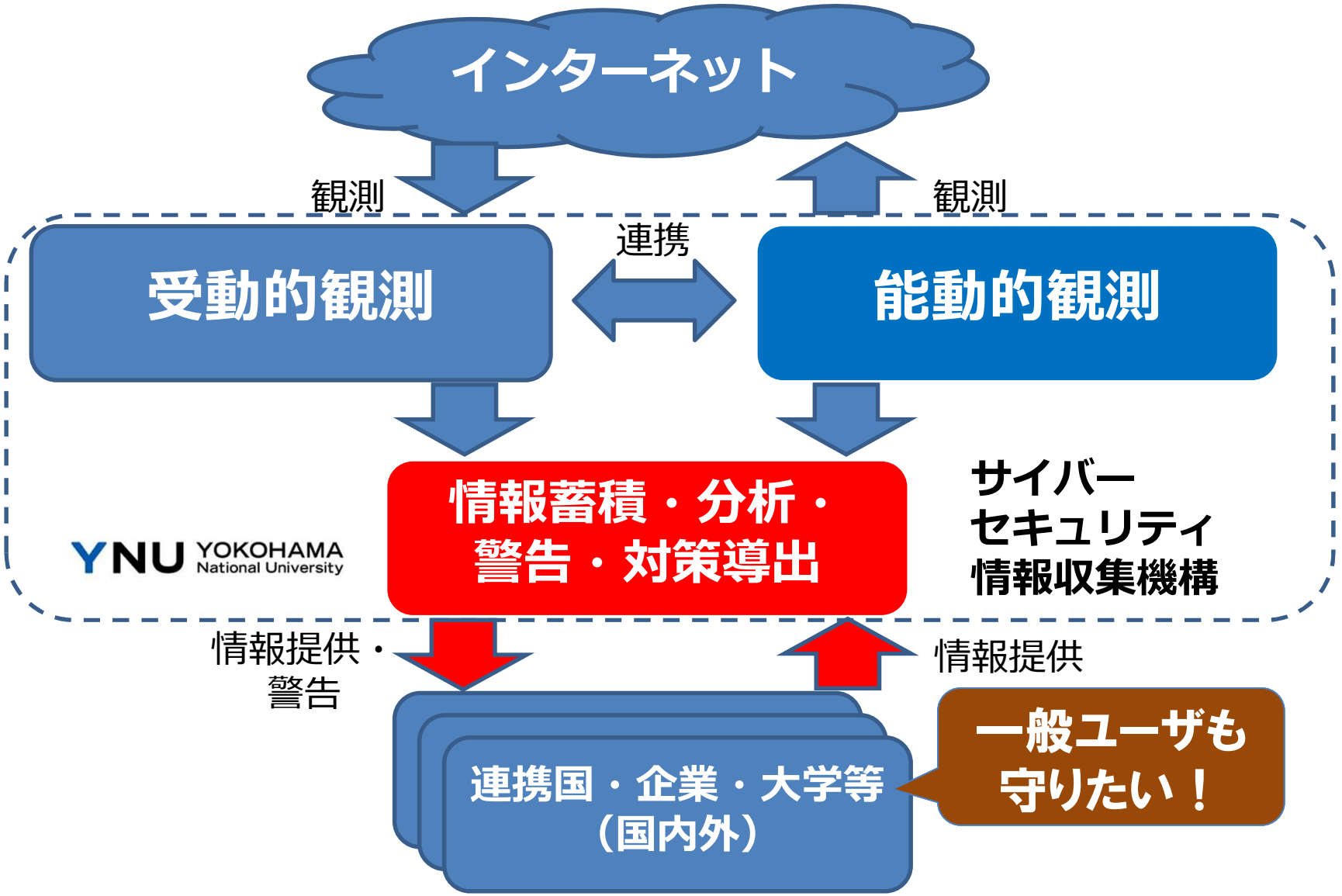
情報提供サイトの公開
(2) Amppot（DoS攻撃観測結果）



最新の観測概況を公開予定（6月中）
攻撃観測時にアラートを発出
→ICT-ISAC、Shadowserver Foundation への提供を実施中

アラート受信をご希望の場合は吉岡まで

サイバーセキュリティ情報収集機構



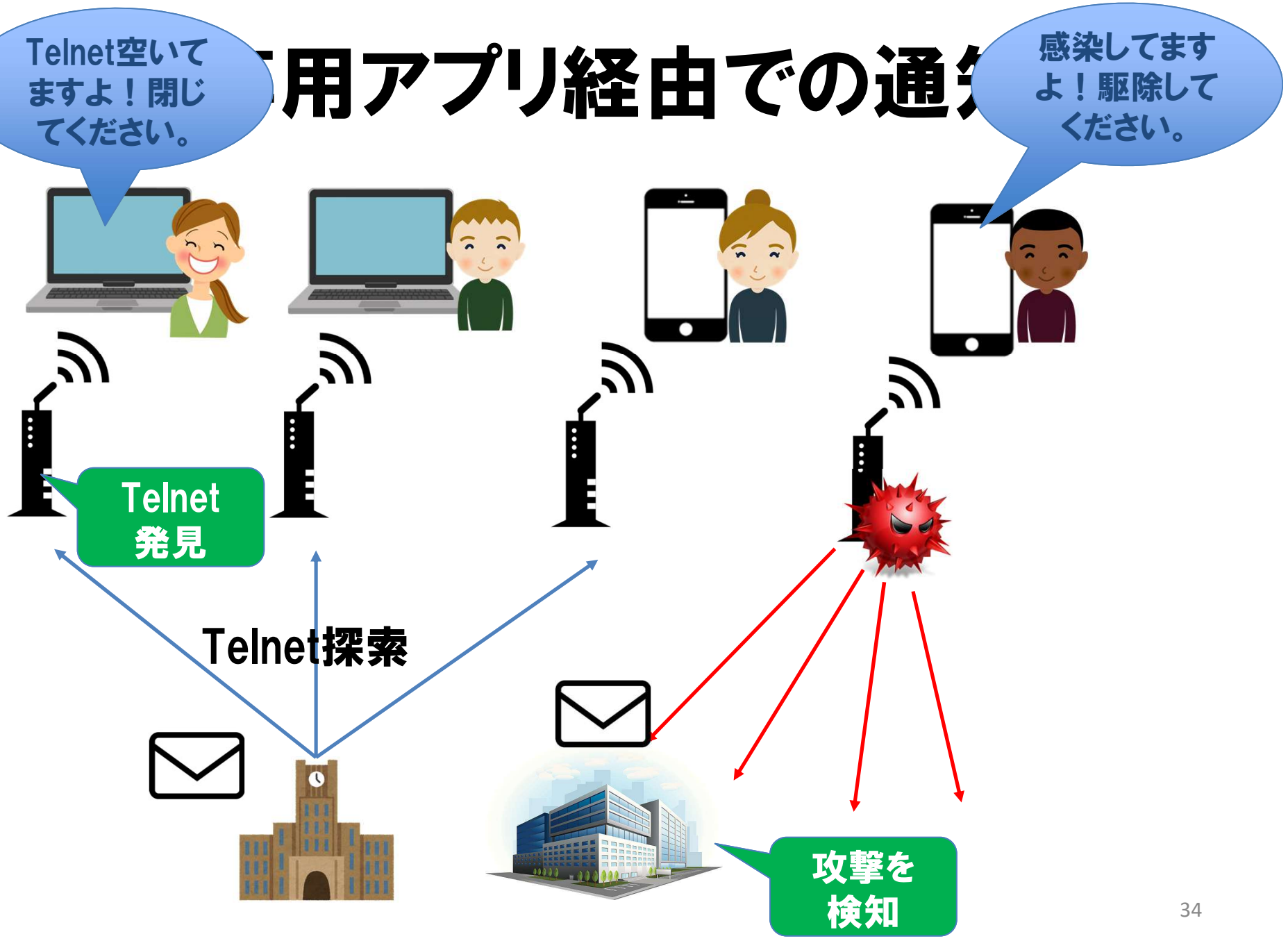
ユーザへの注意喚起に向けて

- 注意喚起を送るコンタクトポイントを特定すること

- どうやったら見てもらえるか？
  - ISPでないとユーザの特定と直接の注意喚起は難しい
  - メールでの注意喚起だけは十分ではない場合がある

- 皆さんがいつも見ているものを通じて注意喚起できないか？

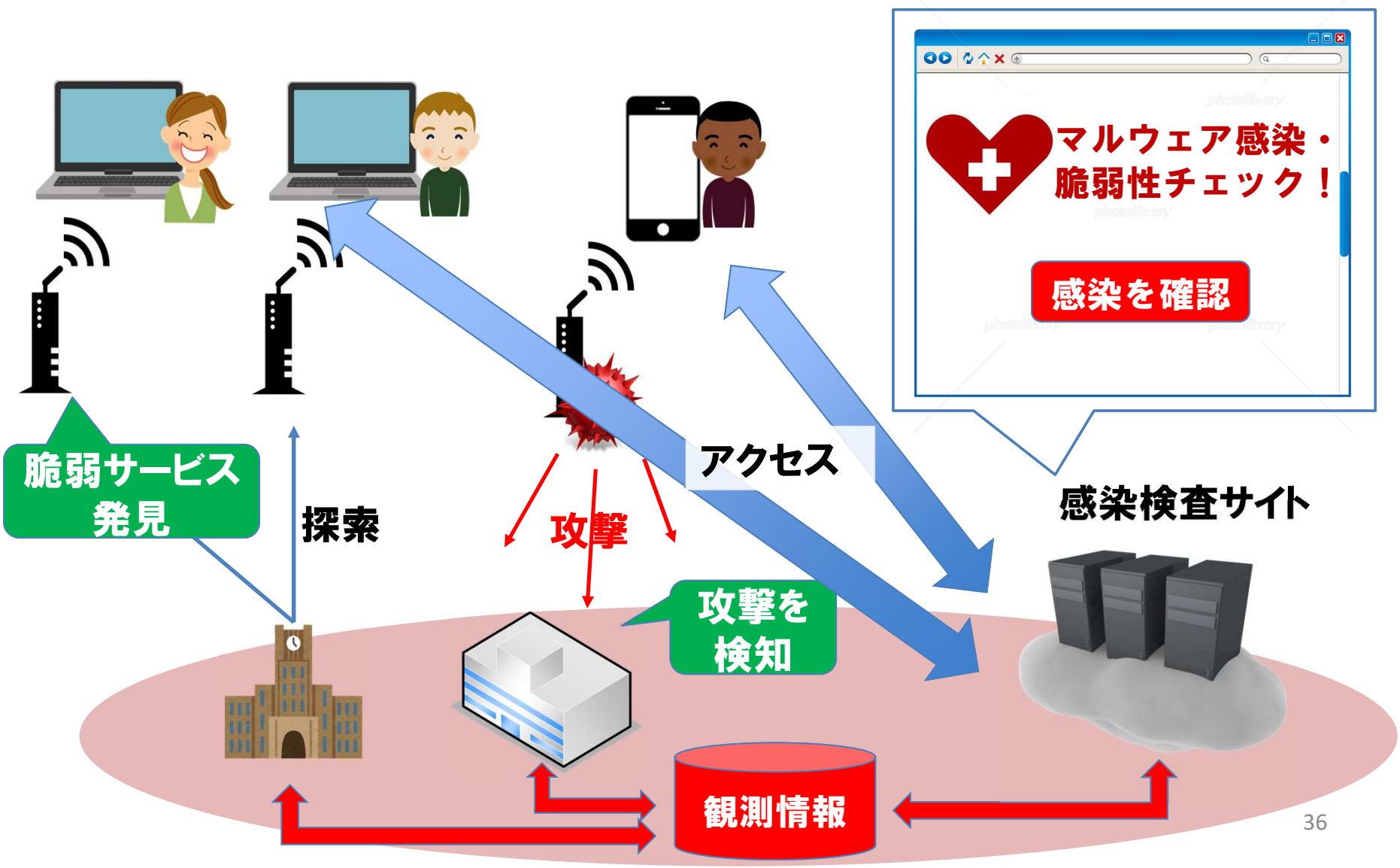
用アプリ経由での通


Telnet空いてますよ！閉じてください。
感染してますよ！駆除してください。
Telnet
発見
Telnet探索
攻撃を
検知

でも専用アプリの事前インストールは面倒…

アプリなしで注意喚起・情報提供できないか？

ブラウザ経由での感染検査



開発中の感染検査サービス

今月から学内で実験運用開始予定

開発中の感染検査サービス

IoTマルウェア感染は多くの場合「自覚症状」がない

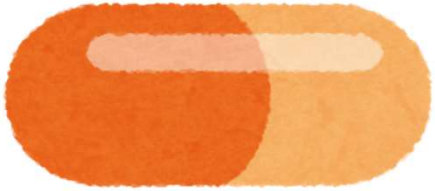
本サービスは、いわば「サイバー版PCR検査」

将来の攻撃の増加を見据えて、ユーザが自ら感染有無を確認し、駆除手順を確認できる仕組みの構築が重要

本サービスは**無償提供**の予定です。本サービスの存在が広く知れ渡るほど効果が高くなります。セキュリティ関連サイト内でのリンク、SNS等での**周知、啓蒙、広報活動にご興味**のある組織・個人の方は、ぜひ、ご一報ください。

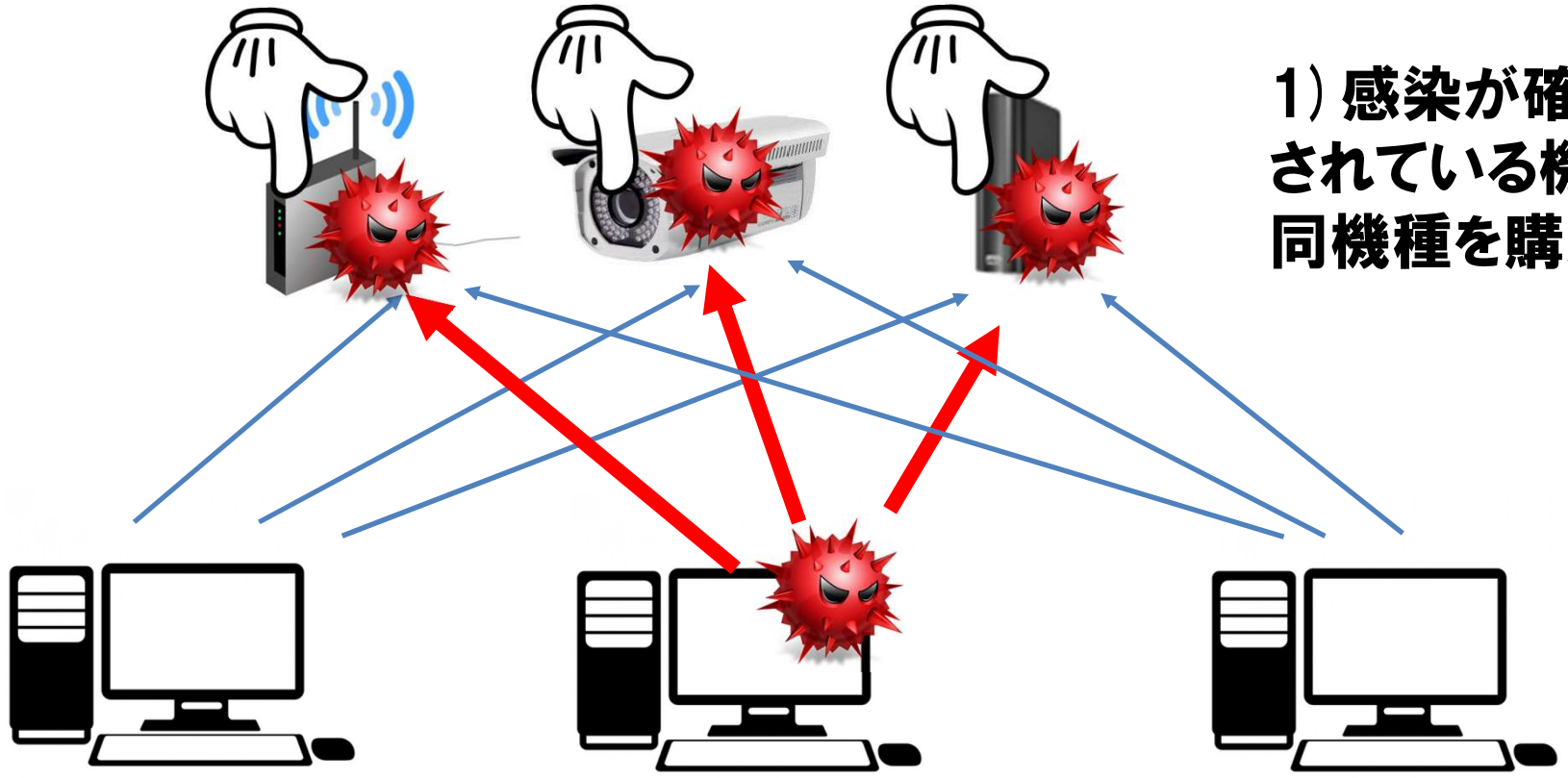
検査が陽性のときの
ワクチンは？

IoTマルウェア
駆除手法の研究



IoTマルウェア駆除実験（～2017）

4）電源切、コマンドによるシステムリブート、工場出荷状態に戻す、など**操作**を実施



1）感染が確認されている機器と同機種を購入

2）通常使用時のファイルシステム、プロセスを記録

3）実IoTマルウェアで攻撃、感染の確認（C2通信など）

5）感染前と比較して感染状態が修復されているか確認

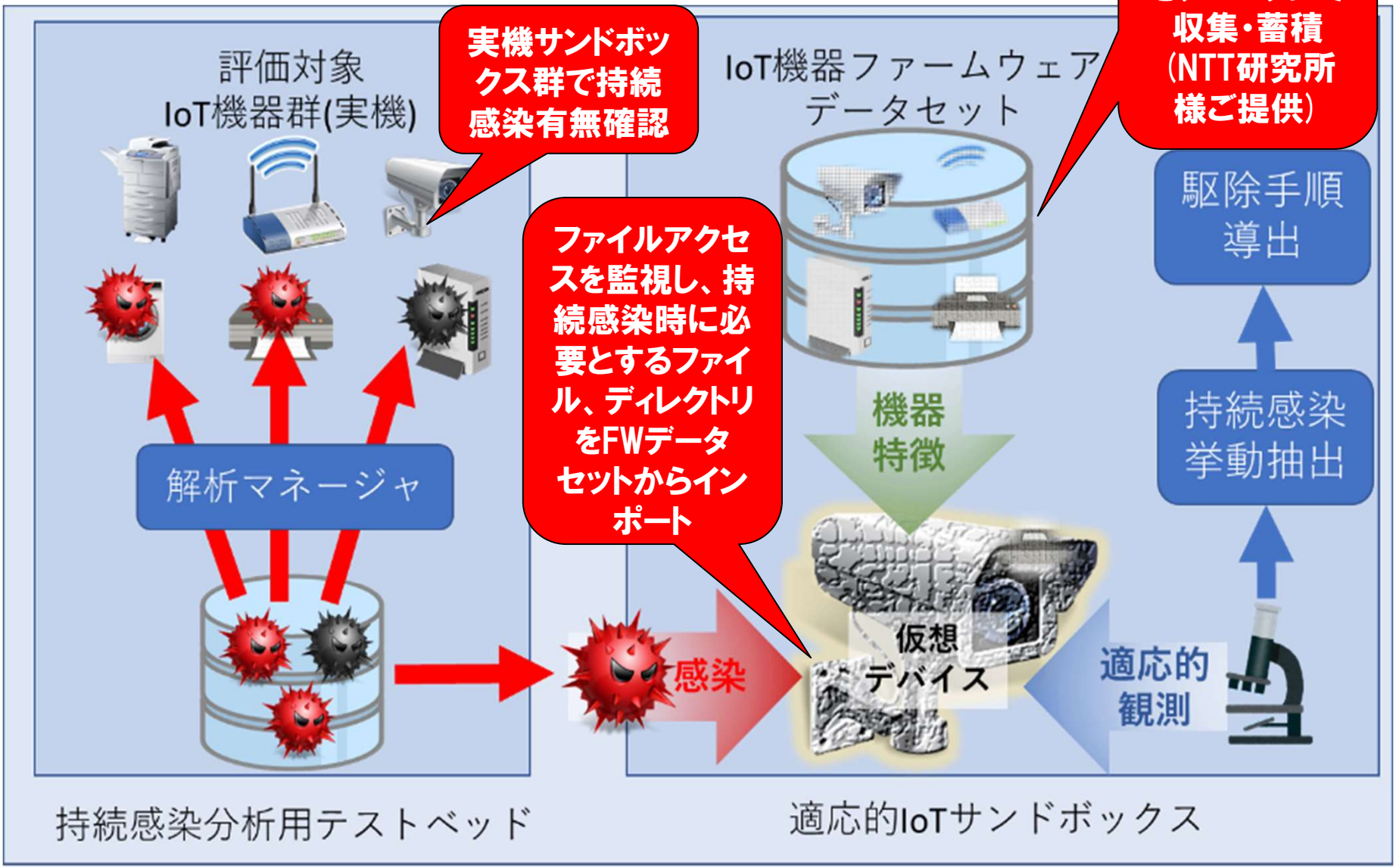
駆除実験結果（2017）

機器	種類	電源再起動による マルウェアの挙動
A	IP Camera	プロセス・バイナリともに消滅
B	プリンター	プロセスのみ消滅 バイナリは残る
C	ルータ	プロセス・バイナリともに消滅
D	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅
E	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅
F	WiFiストレージ/ポケットWiFI	プロセス・バイナリともに消滅
G	衛星放送受信機	プロセス・バイナリともに消滅

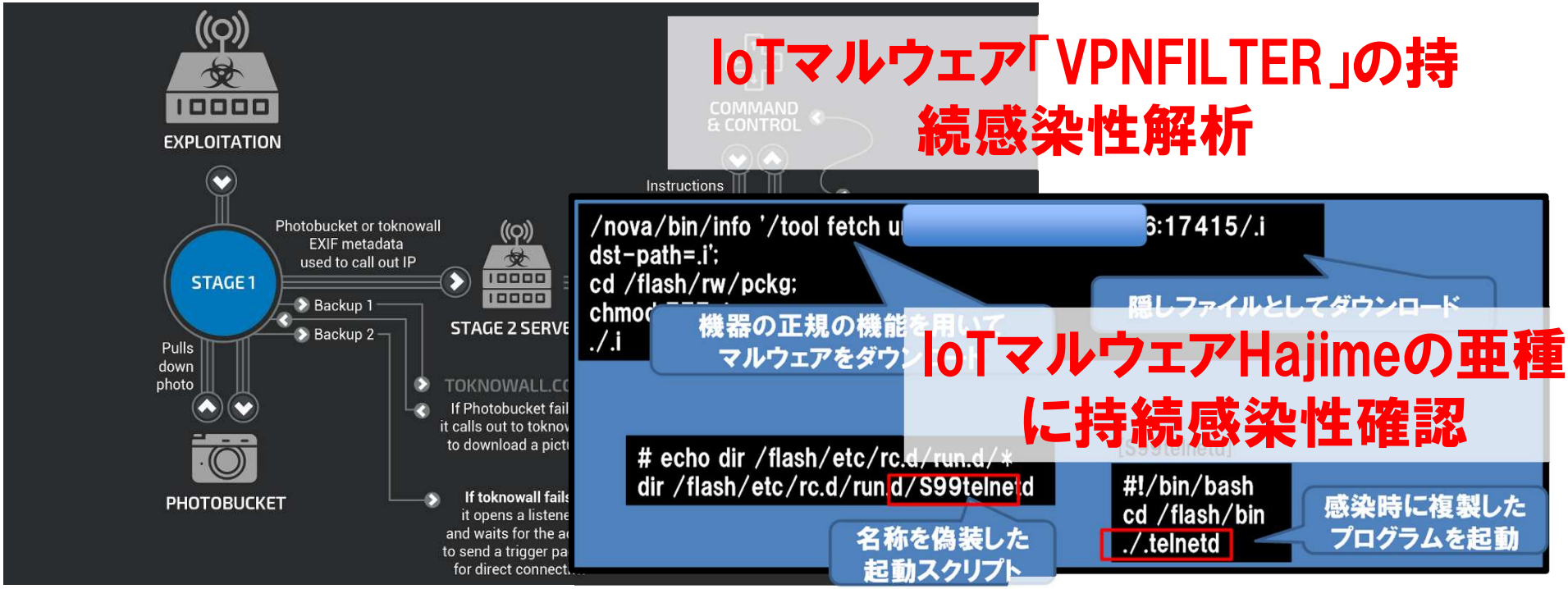
いずれの機器でも主電源による再起動等の操作により

マルウェア駆除が可能「だった」

IoTマルウェアの持続感染性判定・駆除手順導出機構（開発中）



これまで解析に成功した持続感染型IoTマルウェア



IoTマルウェア「VPNFILTER」の持続感染性解析

IoTマルウェアHajimeの亜種に持続感染性確認

NASをねらうQsnatchの持続感染挙動確認

持続感染性を有するIoTマルウェアHide and Seek確認

「持続感染性」を有するIoTマルウェアを次々に確認
→感染メカニズムを明らかにし駆除手順を導出

おわりに

- 多様化・高度化するサイバー攻撃に対応するため、ハニーポット等による**受動的観測**、広域スキャンによる**能動的観測**、マルウェア解析、脆弱性検知、アトリビューション等の技術の継続的研究開発を実施

- 研究開発により得られた情報、技術を**エンドユーザ、製造者、セキュリティ実務者、研究者が利用しやすい形**で提供し、実効性のある対策に繋げるための仕組みの構築を目指します！

横浜国立大学　大学院環境情報研究院/先端科学高等研究院
吉岡克成，yoshioka@ynu.ac.jp
http://yoshioka.ynu.ac.jp

謝辞1：本研究の一部は情報通信研究機構委託研究「Web媒介型攻撃対策技術の実用化に向けた研究開発（H28-R2）」により得られた成果です。
謝辞2：本研究の一部は総務省委託研究「IoT機器に関する脆弱性調査等の実施（H29）」により得られた成果です。
謝辞3：本研究の一部は情報通信研究機構委託研究「サイバー攻撃ハイブリッド分析実現に向けたセキュリティ情報自動分析基盤技術の研究開発（R1-R2）」により得られた成果です。
謝辞4：本研究の一部は総務省委託研究「電波の有効利用のための IoT マルウェア無害化／無機能化技術等に関する研究開発（R2）」により得られた成果です。
謝辞5：本研究の一部は総務省「重要IoT機器のセキュリティ対策に係る調査の請負」（NTTコミュニケーションズ株式会社との共同研究として実施（R2）」により得られた成果です。
謝辞6：本研究の一部は情報通信研究機構委託研究「欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発（H30-R3）」により得られた成果です。
謝辞7：本研究の一部は科研費基盤研究（B）「ブロックチェーンを基盤とする高信頼性を持った自律分散型監視技術（R1-R3）」により得られた成果です。