Institute of Advanced Sciences
Yokohama National University

YNU YOKOHAMA National University

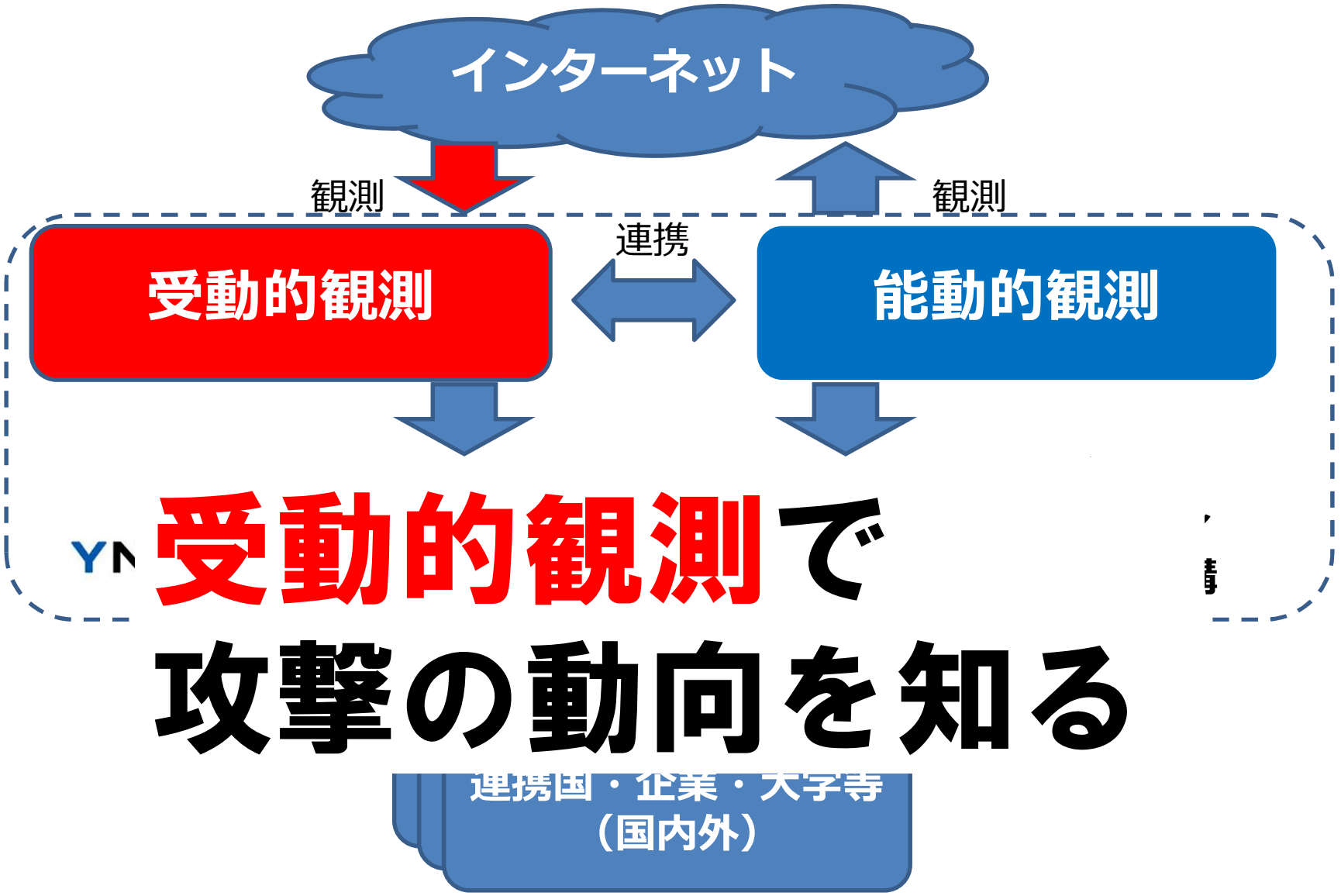
IoTセキュリティに関連する近年の研究内容の紹介

吉岡　克成

横浜国立大学

総務省サイバーセキュリティタスクフォース　ご説明資料（2021/10/14）

サイバーセキュリティ情報収集機構



IoTハニーポット（2015～）

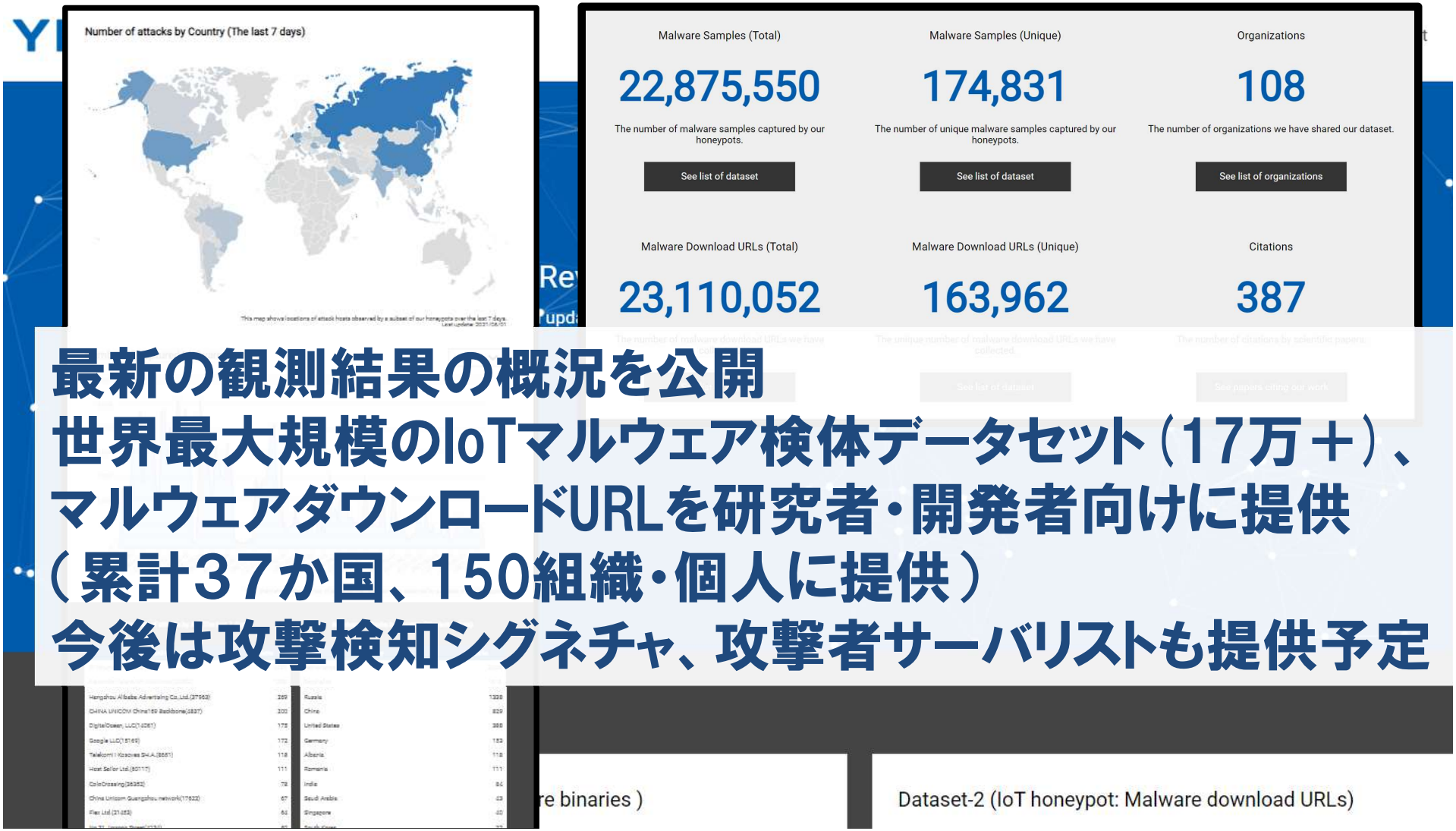
IoT機器へのサイバー攻撃を観測する囮システム（IoTハニーポット）を世界に先駆けて構築・観測開始

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 R[illegible] 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.
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.

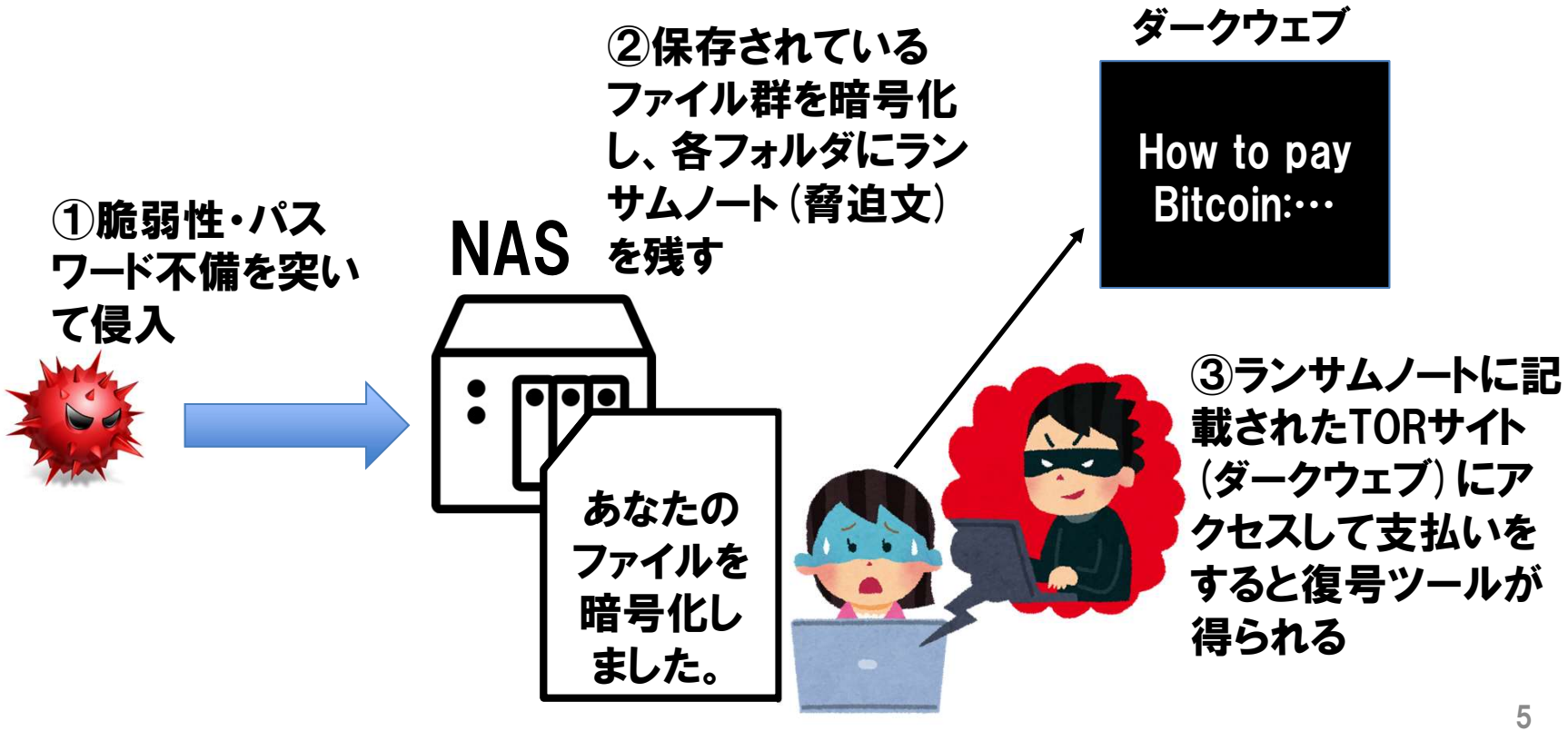
IoTマルウェア・攻撃情報提供サイト
https://sec.ynu.codes/iot



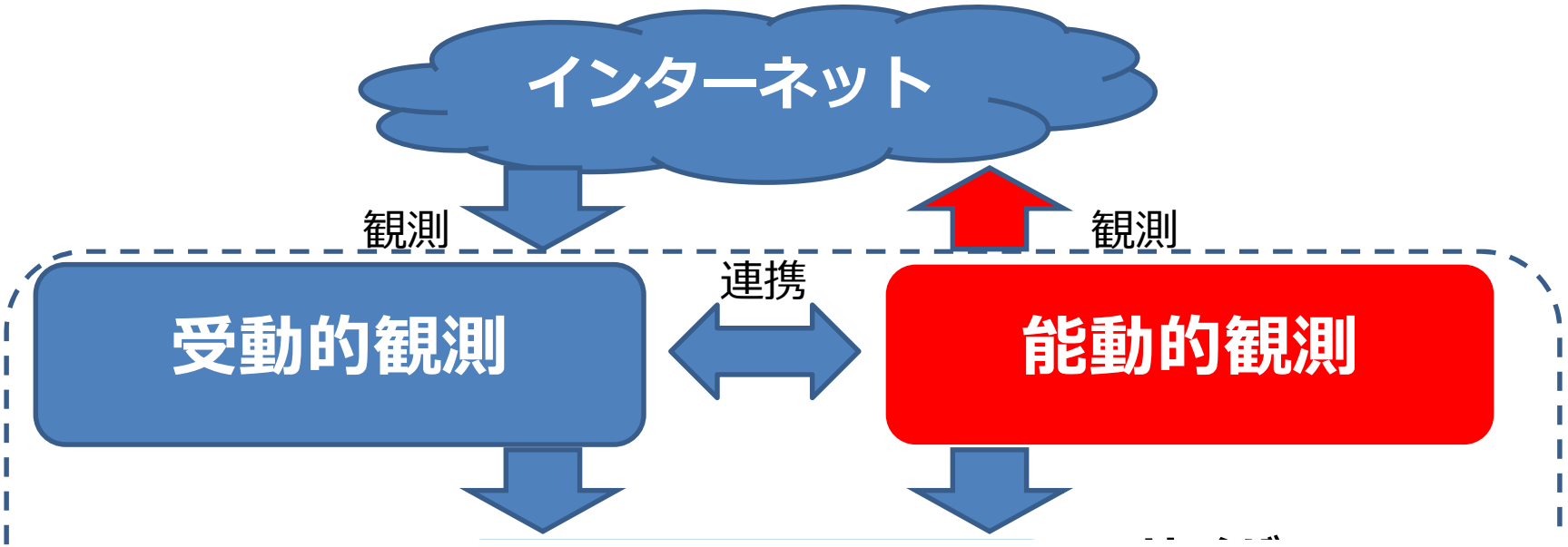
最新の観測結果の概況を公開
世界最大規模のIoTマルウェア検体データセット（17万＋）、
マルウェアダウンロードURLを研究者・開発者向けに提供
（累計37か国、150組織・個人に提供）
今後は攻撃検知シグネチャ、攻撃者サーバリストも提供予定

IoTランサムハニーポット

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



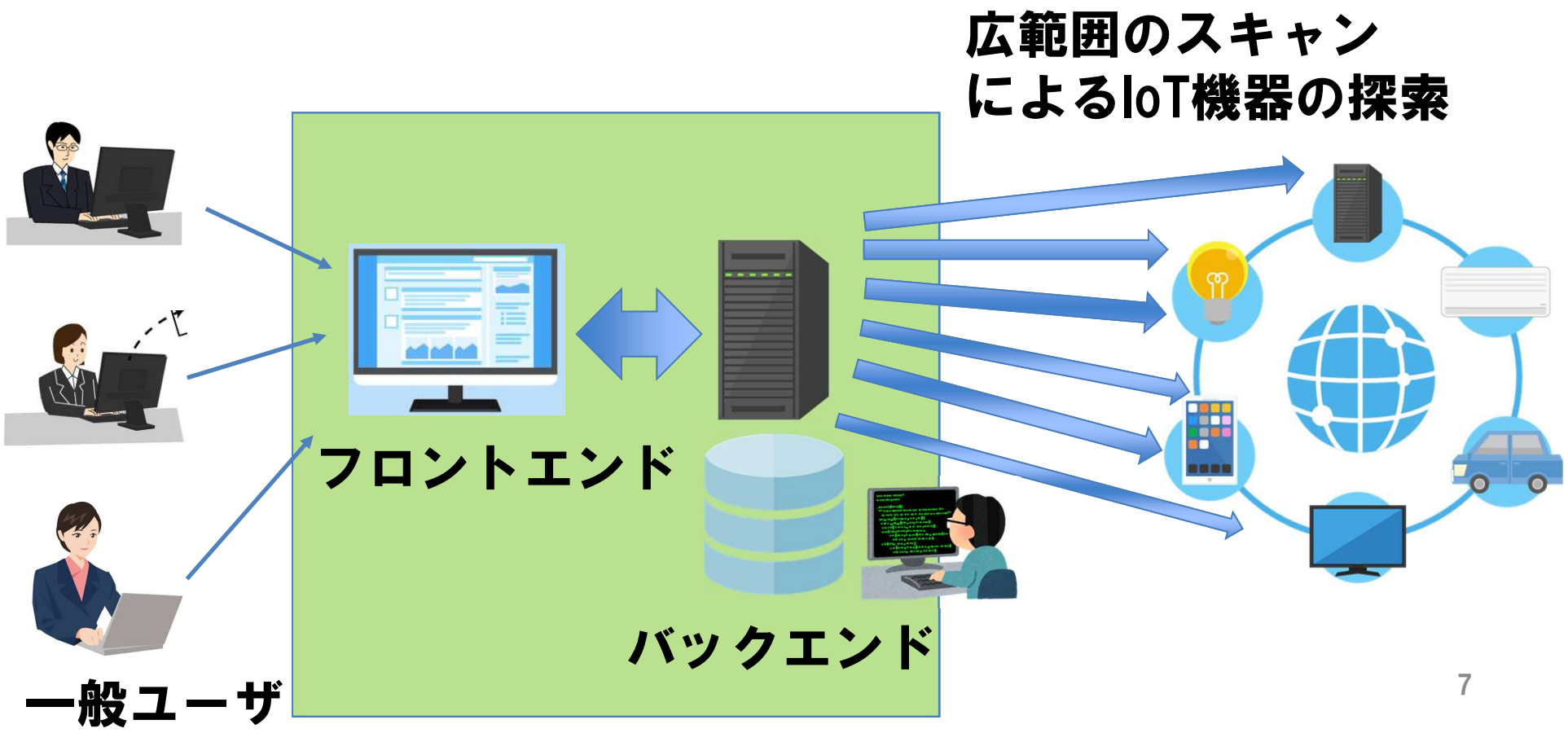
サイバーセキュリティ情報収集機構



能動的観測で
脆弱/設定不備のある
IoT機器をさがす

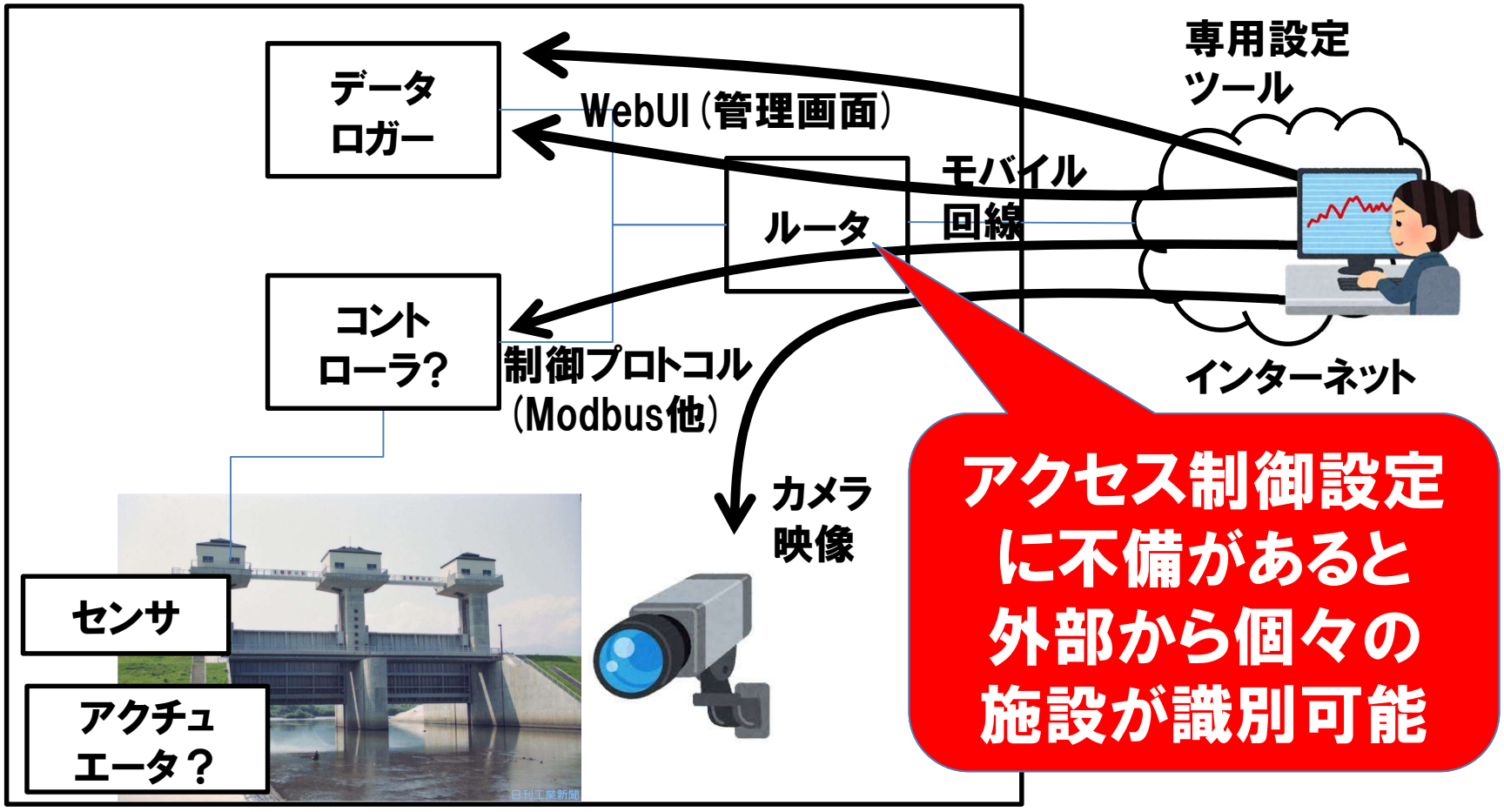
広域スキャンシステム

広域ネットワークをスキャンし、脆弱/設定不備のあるIoT機器等の探索を行うシステム

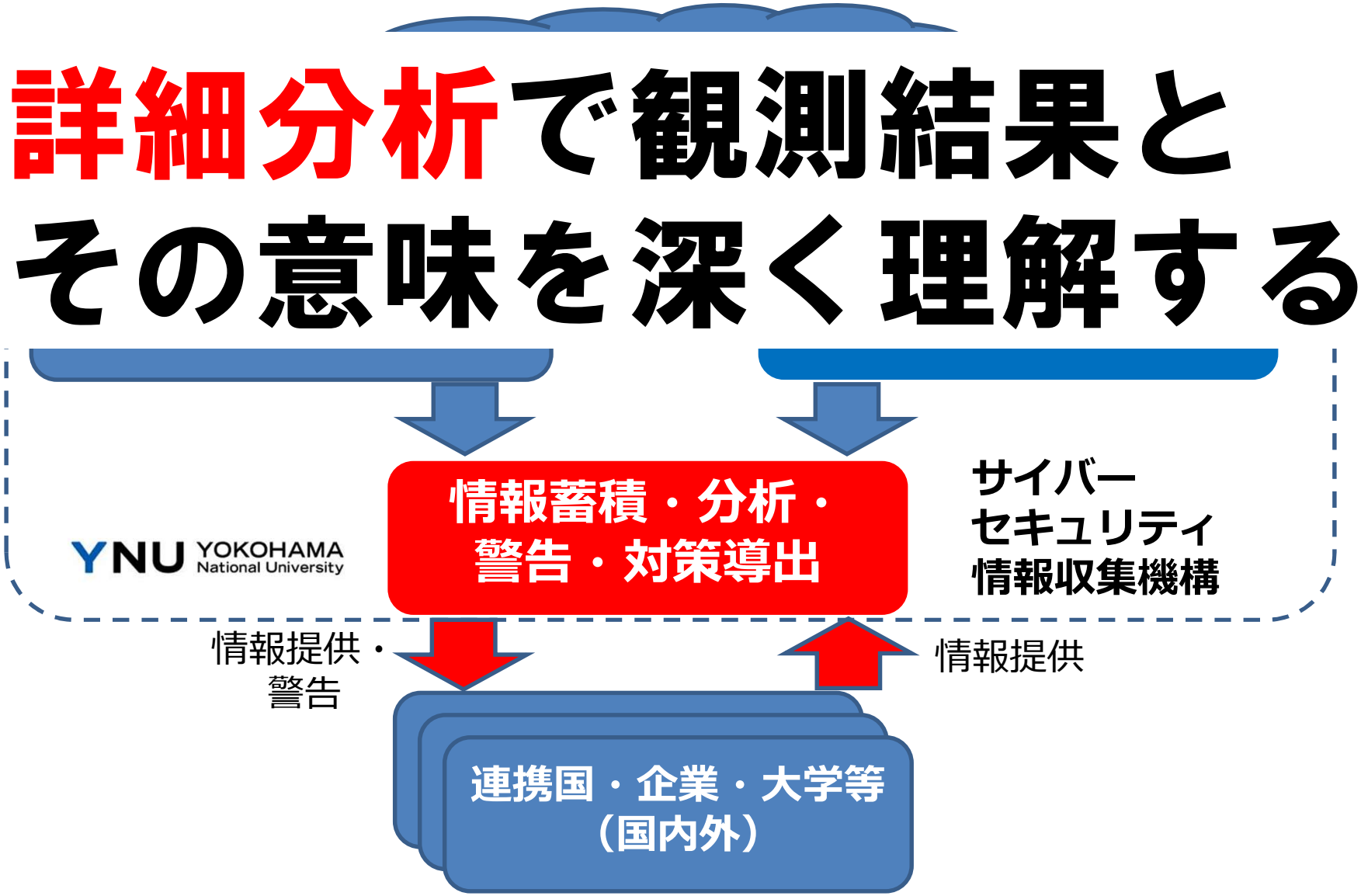


「重要IoT機器」とは？

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



サイバーセキュリティ情報収集機構



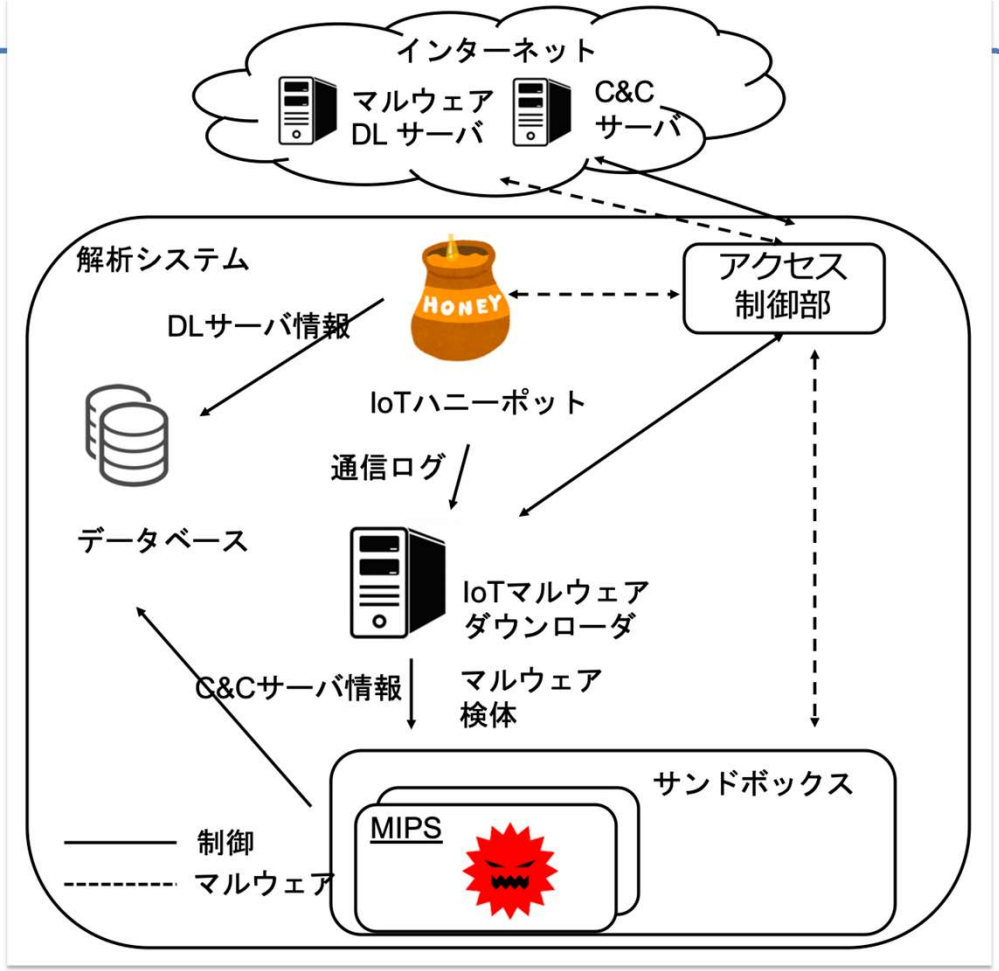
ハニーポットで収集した IoTマルウェア検体の解析

- 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攻撃者の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？
  どのように駆除するのか？

攻撃インフラ（攻撃者サーバ）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（攻撃者サーバ）」を継続的に観測

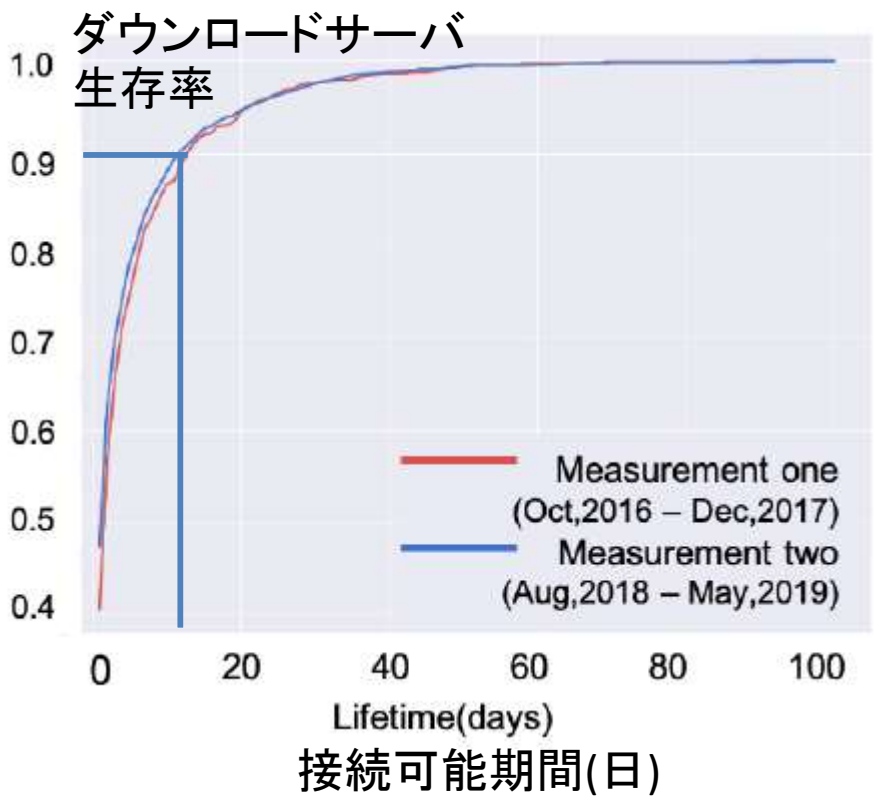
特定したマルウェアダウンロードURL累計：239,806件（2021/08/30現在）

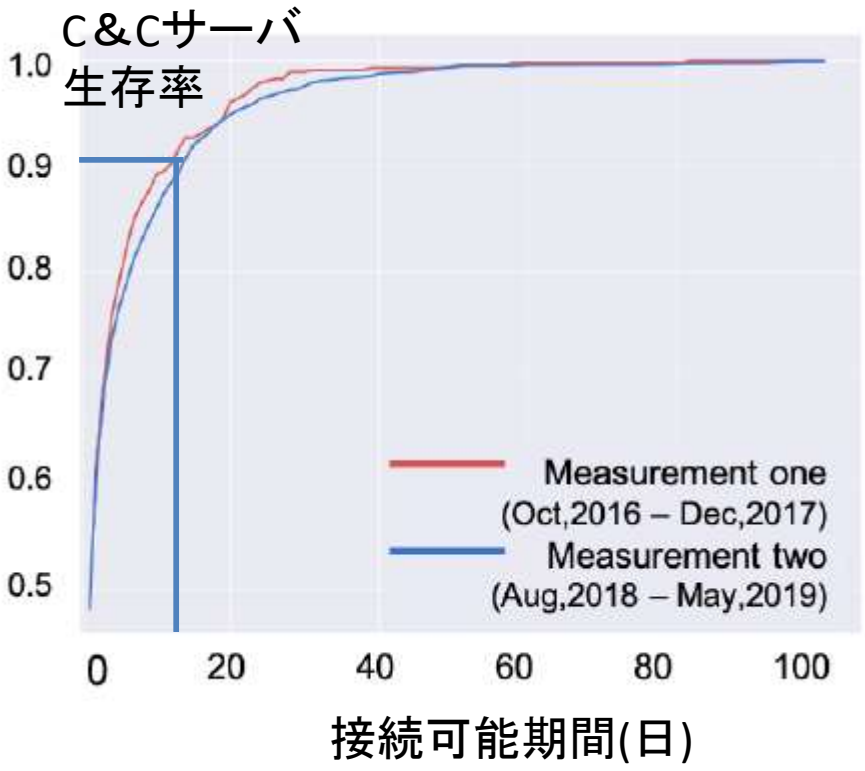
特定したC&Cサーバ累計：3,578件（2021/06/05現在）

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.

攻撃インフラ（攻撃者サーバ）の観測

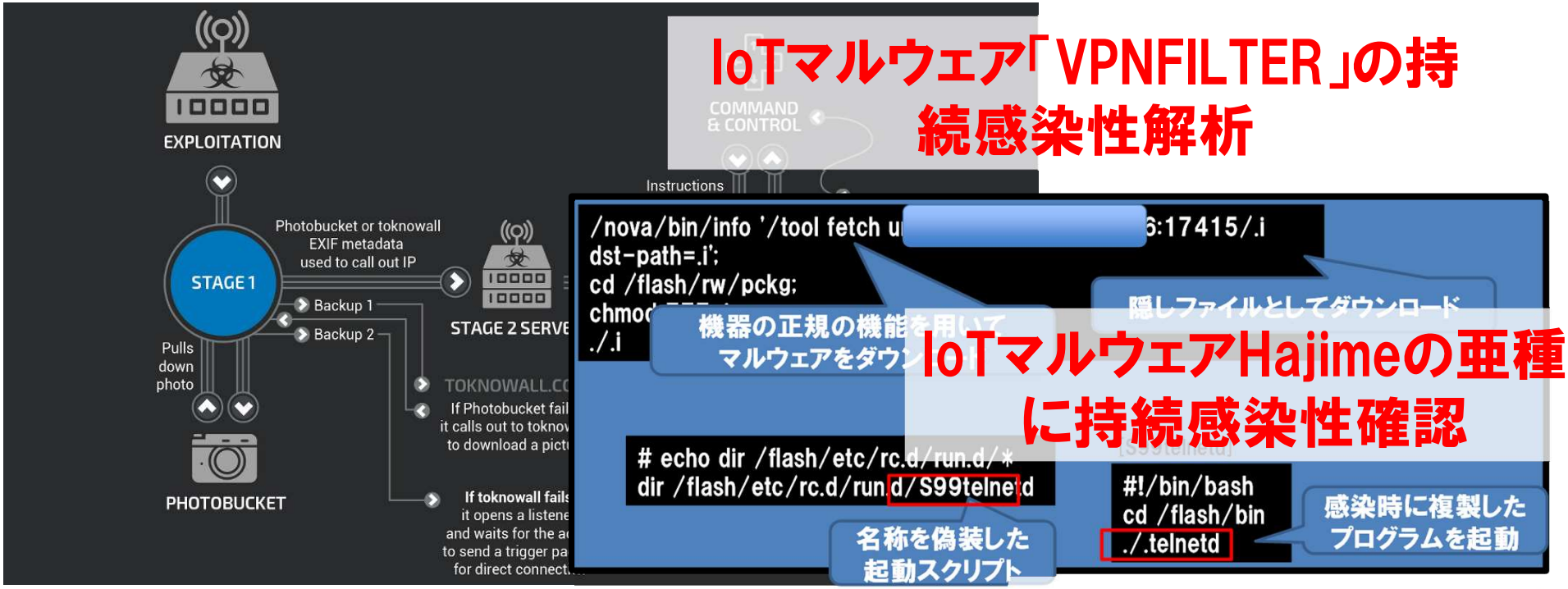
マルウェアダウンロードサーバ、C&Cサーバ共に90%は2週間で接続できなくなる（移動する）





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.

持続感染型IoTマルウェアの検出と駆除手順導出



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

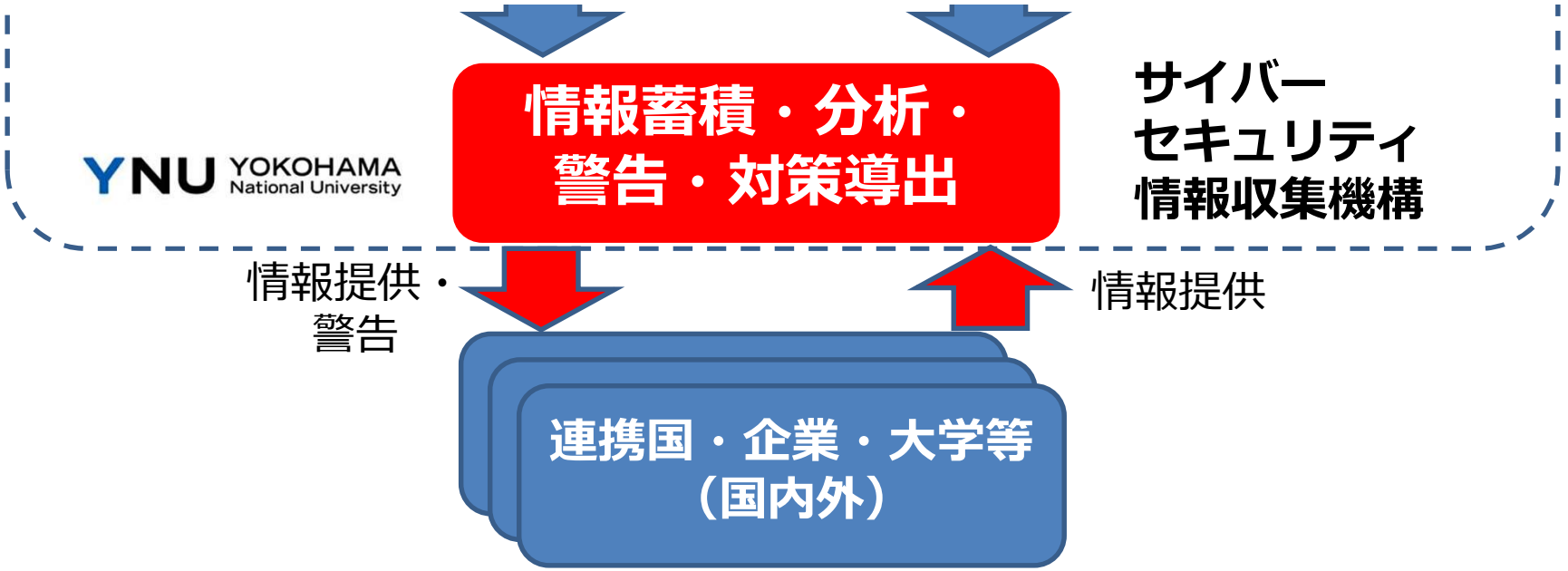
NASをねらうQsnatchの持続感染挙動確認

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

サイバーセキュリティ情報収集機構

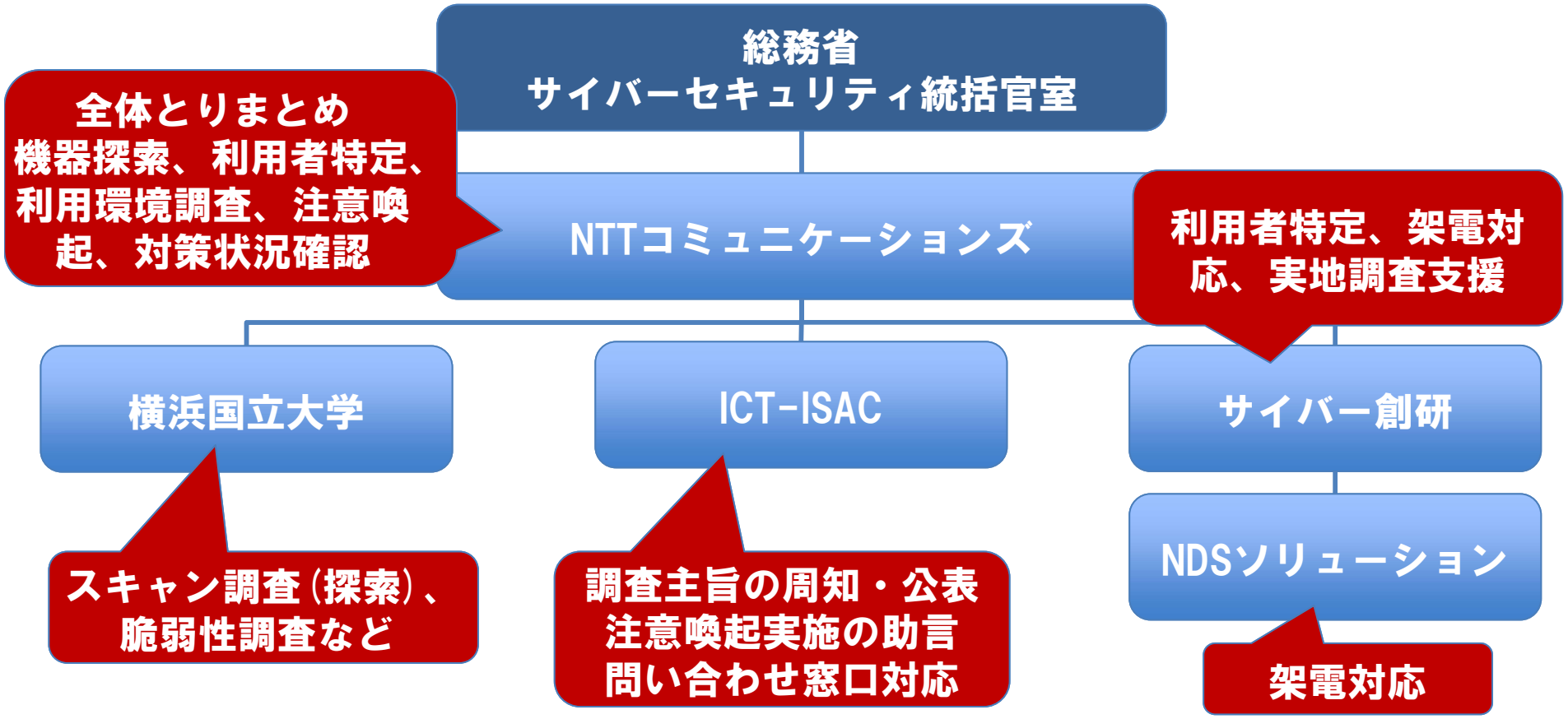
注意喚起により、実世界のセキュリティ向上を目指す



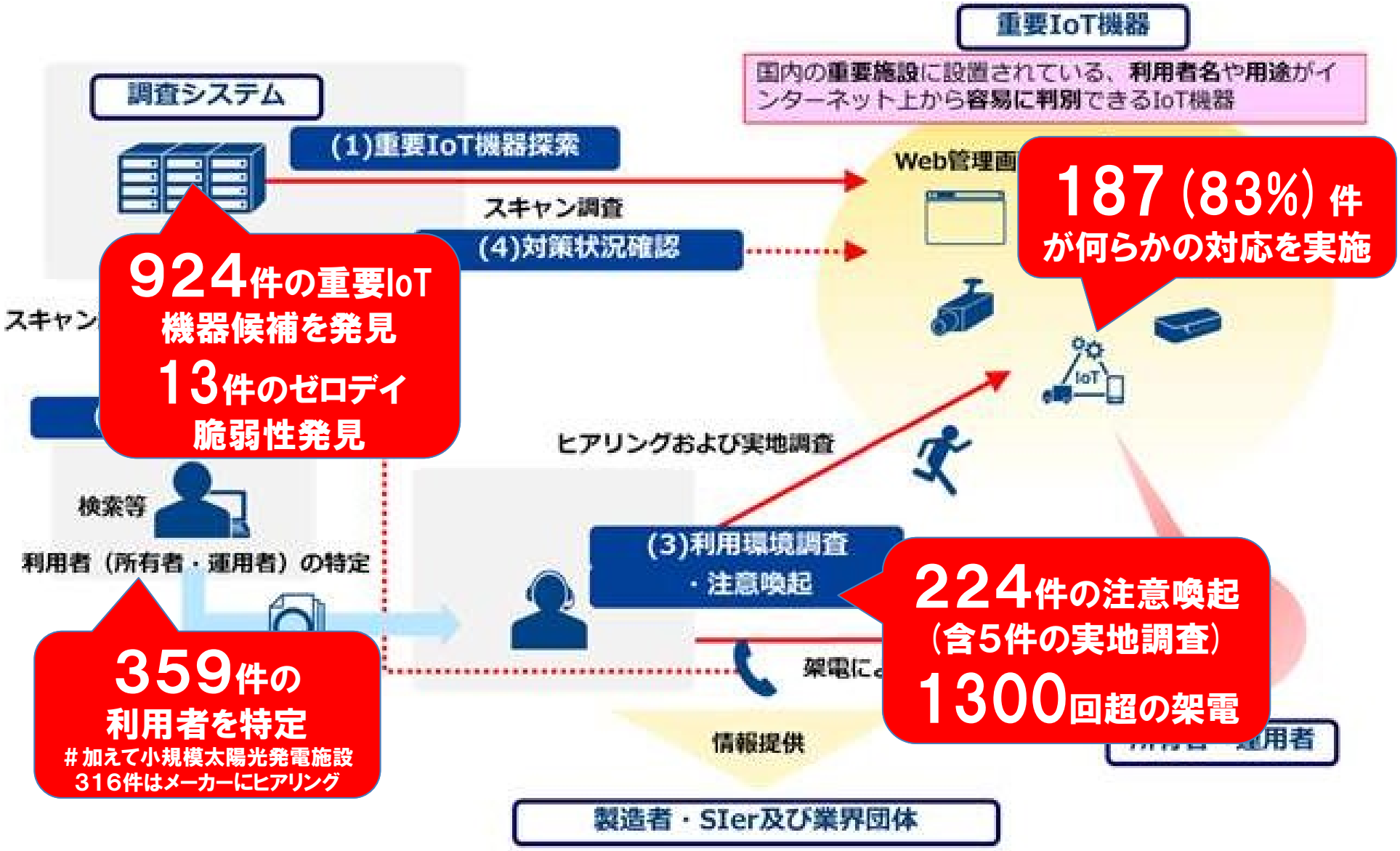
総務省
重要IOT機器調査
および注意喚起
2020

ICT-ISAC, 脆弱な状態にある重要IoT機器の調査及び注意喚起について
https://www.ict-isac.jp/news/news20200728.html
ICT-ISAC, 脆弱な状態にある重要IoT機器の調査及び注意喚起について(報告)
https://ict-isac.jp/news/news20210901.html

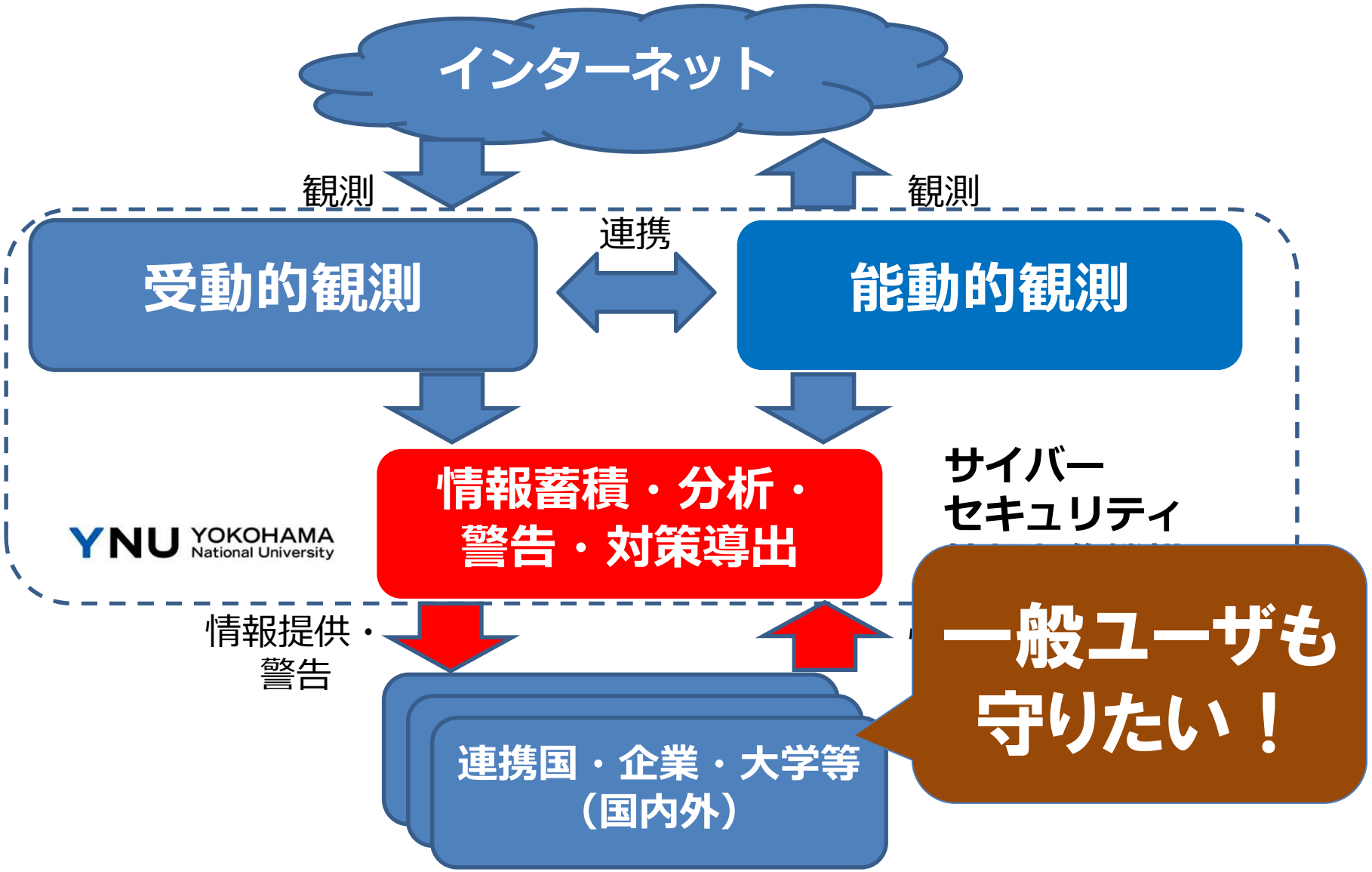
体制


総務省
サイバーセキュリティ統括官室
全体とりまとめ
機器探索、利用者特定、
利用環境調査、注意喚
起、対策状況確認
NTTコミュニケーションズ
利用者特定、架電対
応、実地調査支援
横浜国立大学
ICT-ISAC
サイバー創研
スキャン調査（探索）、
脆弱性調査など
調査主旨の周知・公表
注意喚起実施の助言
問い合わせ窓口対応
NDSソリューション
架電対応

脆弱な状態にある重要IoT機器の調査及び注意喚起(2020)



サイバーセキュリティ情報収集機構



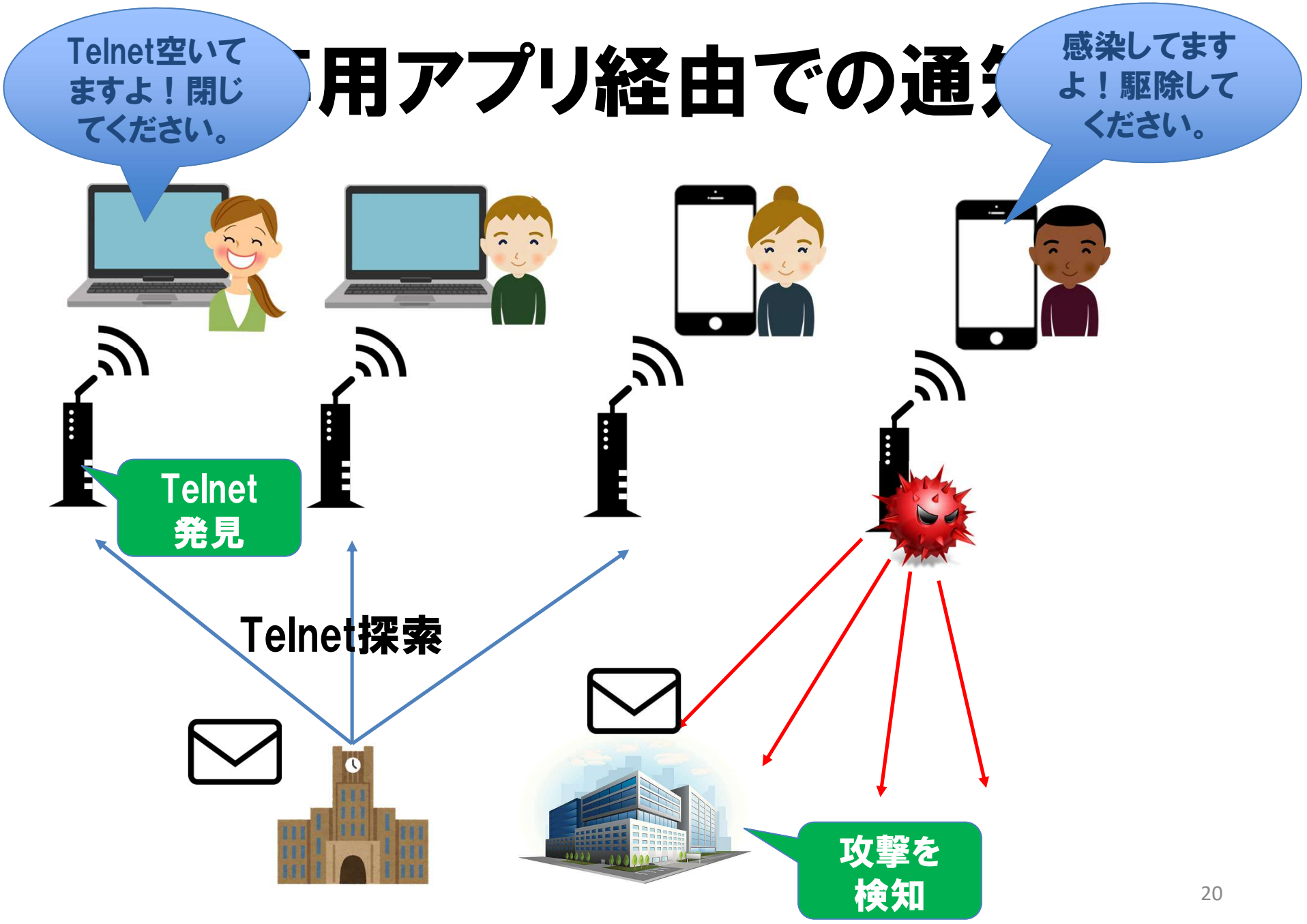
ユーザへの注意喚起のポイントは

- ユーザに見てもらうこと

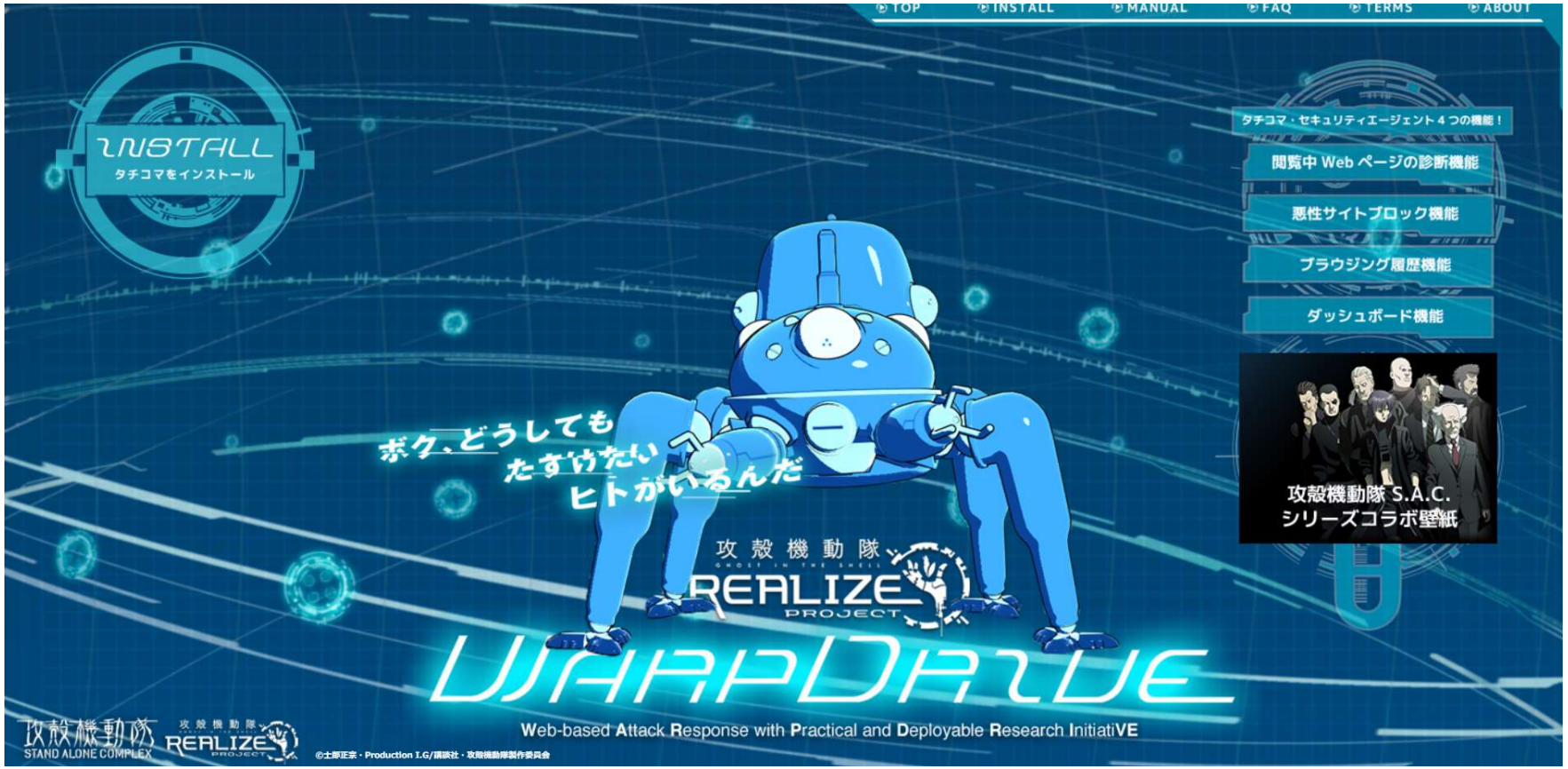
- どうやったら見てもらえるか？
  - ISPからの通知メールだけは十分ではない
  - 強制的な隔離と通知は効果が高いが、コストも高く、強権的、フィッシングなどへの悪用も怖い

- 皆さんがいつも見ているものは？
  - パソコン、スマホ…

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

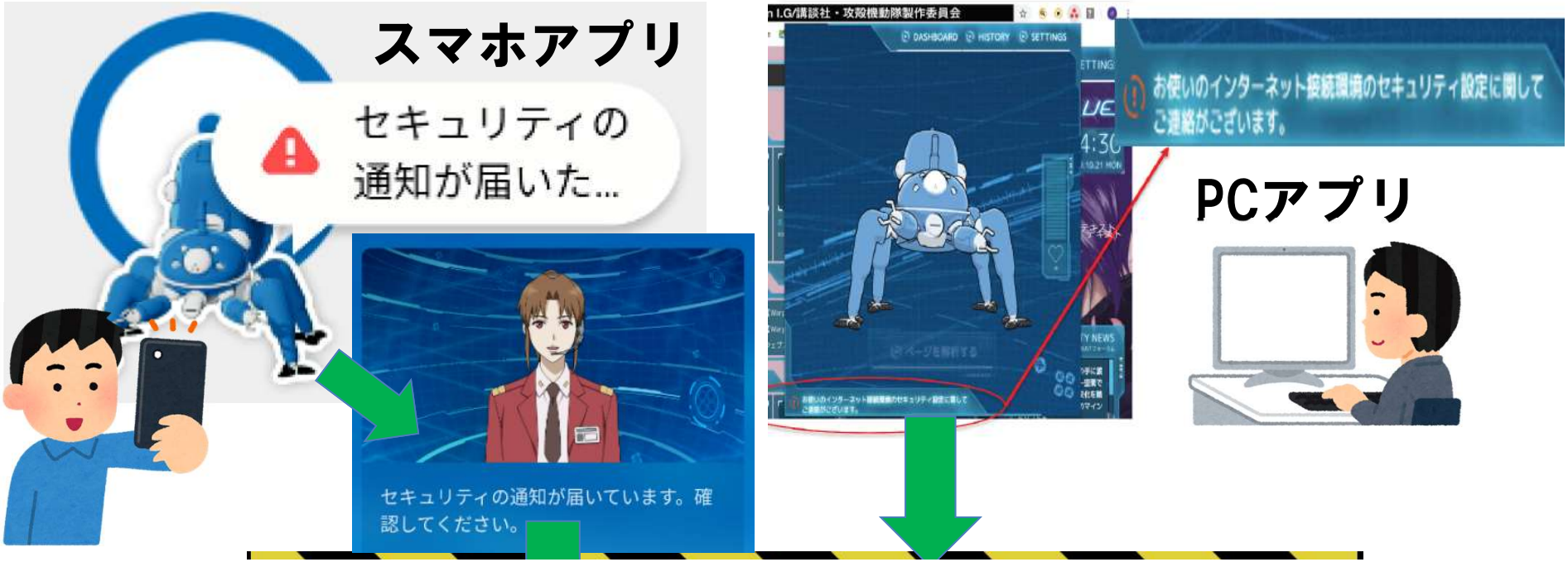
NICT委託研究WarpDriveプロジェクト



タチコマ セキュリティエージェント（SA）をインストールして
誰でも実証実験に参加できます！

https://warpdrive-project.jp/

タチコマSAからのセキュリティ通知



約1000名のWarpDrive参加ユーザに対して、セキュリティ注意喚起を実施！（2019末～）

定常観測と対策フロー

１）観測を定常的に実施

定常的にサービス開放

注意喚起

２）NW環境の確認

自宅/勤務先/外出先

３）（NWサービス毎に）意図的に公開しているか確認

意図あり/意図なし/わからない

４）自身での対策可否の確認

自身で対策可能/要サポート

５）メールでのサポート

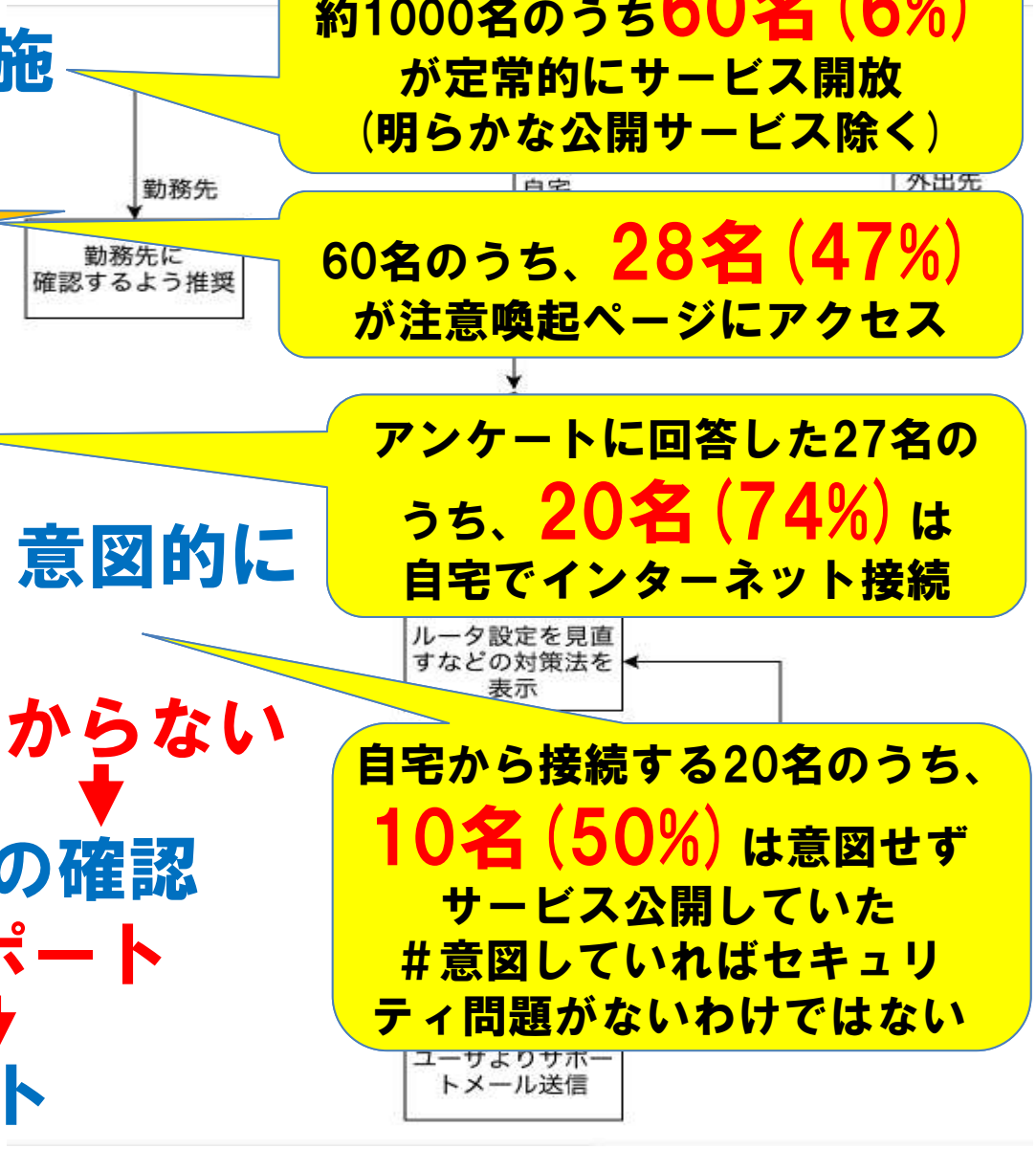
約1000名のうち60名（6%）が定常的にサービス開放（明らかな公開サービス除く）

60名のうち、28名（47%）が注意喚起ページにアクセス

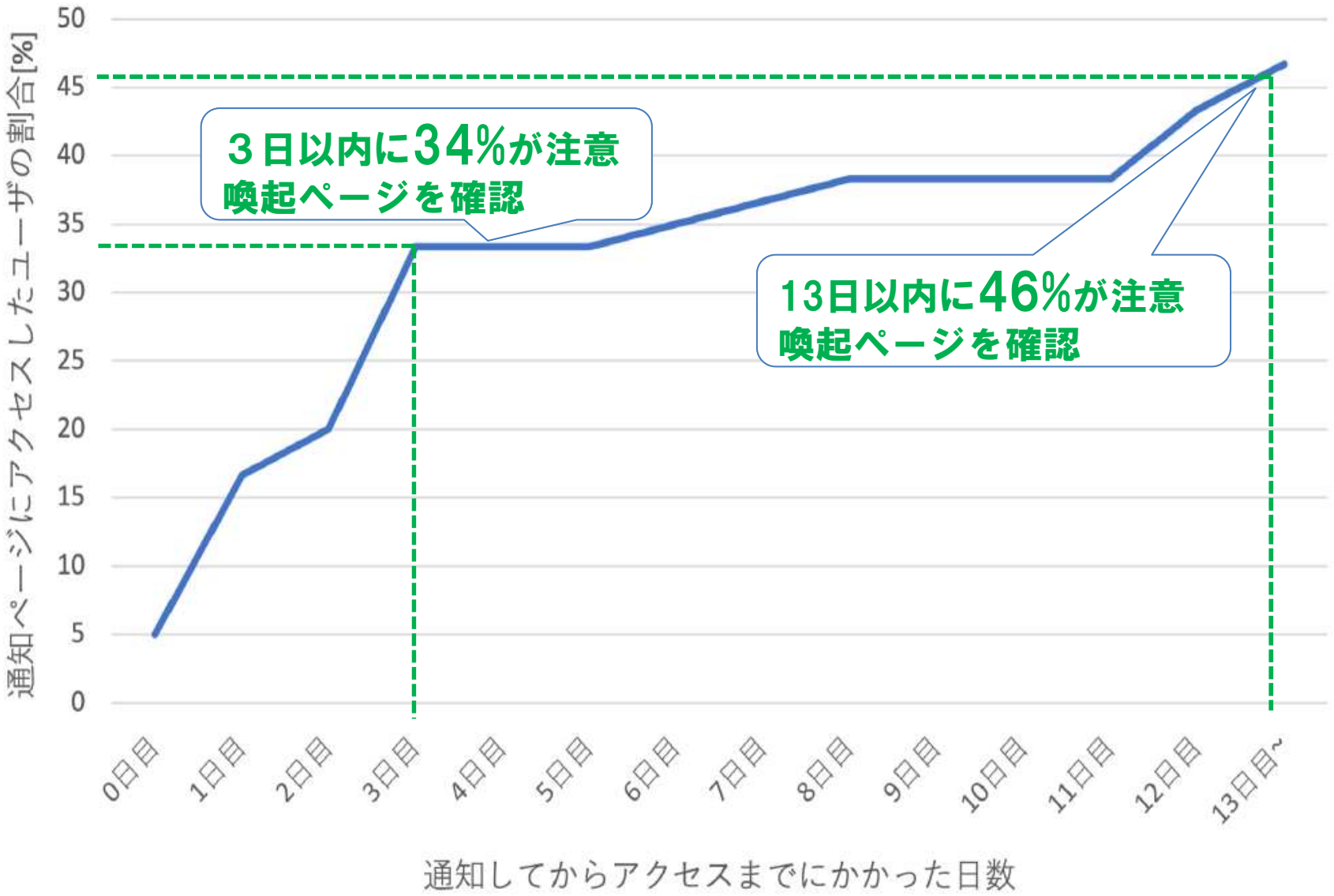
アンケートに回答した27名のうち、20名（74%）は自宅でインターネット接続

自宅から接続する20名のうち、10名（50%）は意図せずサービス公開していた

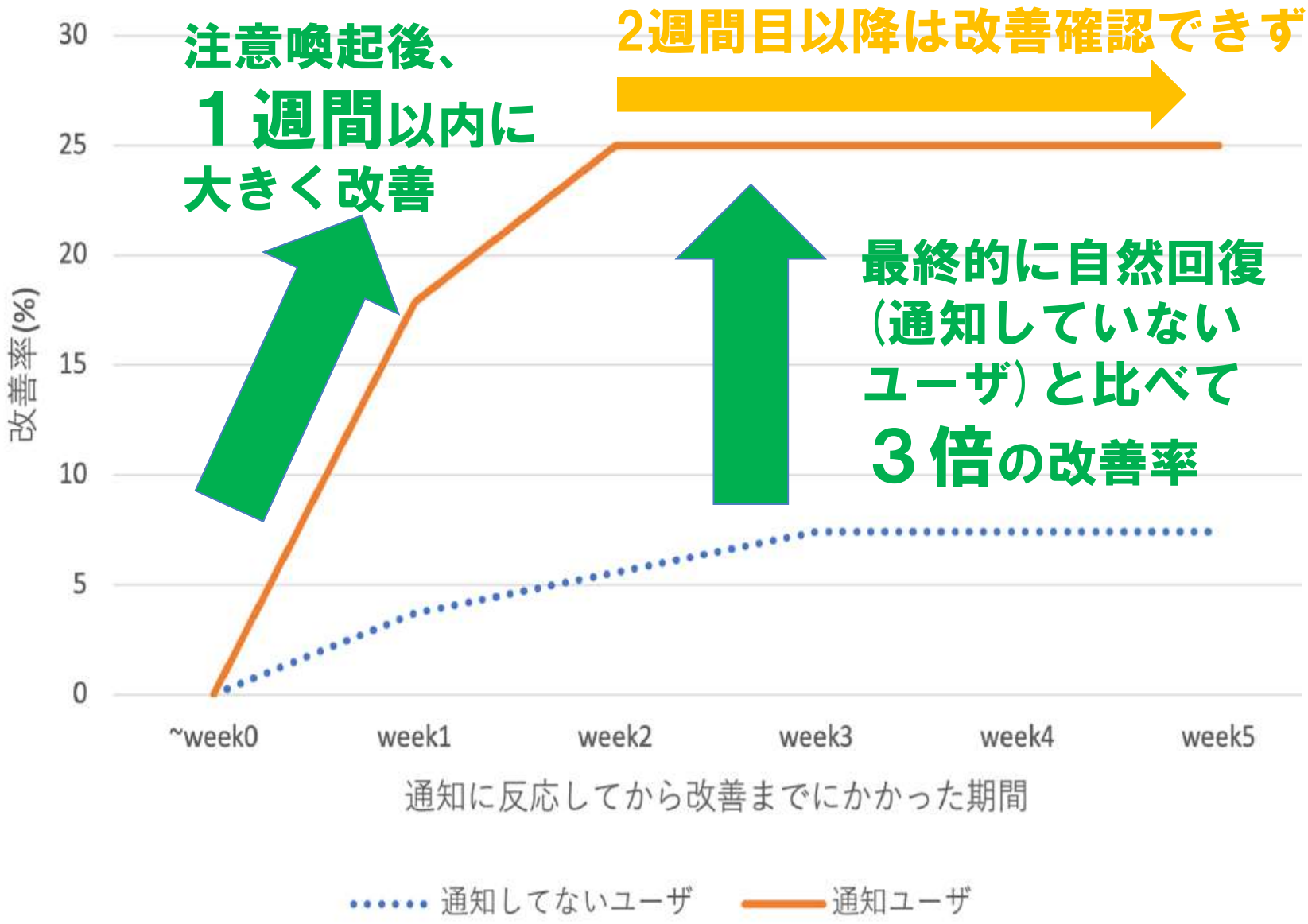
＃意図していればセキュリティ問題がないわけではない



ユーザは注意喚起を読むのか？



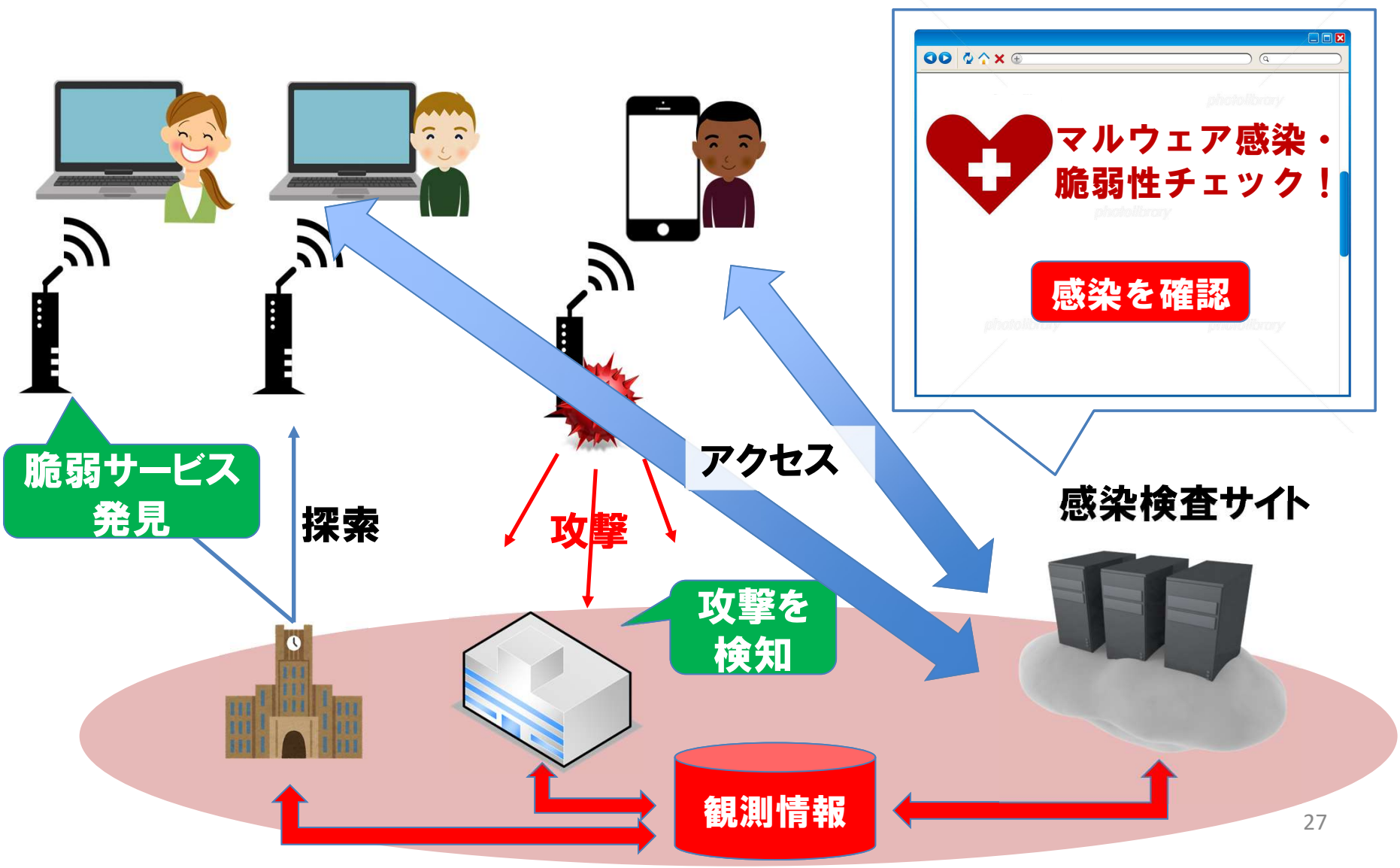
注意喚起による改善効果



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イト

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。

現在、NICTのダークネットデータに基づく感染確認機能がほぼ完了し、株式会社ゼロゼロワン様のIoT検索エンジンKarma†によるスキャン機能の実装を進めています

大学内でのトライヤル（今年中に実施）を経て、一般公開を目指しています

おわりに

- 最新のサイバー脅威の多角的観測を継続的に実施.
- 加えて、様々な「つながるモノ」の脆弱性やセキュリティ不備をプロアクティブに探索
- 観測結果提供、注意喚起を実施し高い効果を実証
- 今後は、ユーザのヒューマンファクタを意識して、注意喚起の効果をさらに改善することを目指す
- 産学連携により、更なる実データの収集、活用を目指す

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: 本研究の一部は戦略的イノベーション創造プログラム（SIP）第2期／自動運転（システムとサービスの拡張）／新たなサイバー攻撃手法と対策技術に関する調査研究（国立研究開発法人新エネルギー・産業技術総合開発機構（NEDO）の委託業務として実施）により得られた成果です。
謝辞7：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。