資料17－2

Institute of Advanced Sciences
Yokohama National University

YNU YOKOHAMA National University

昨今のサイバー攻撃や注目すべき事象について

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

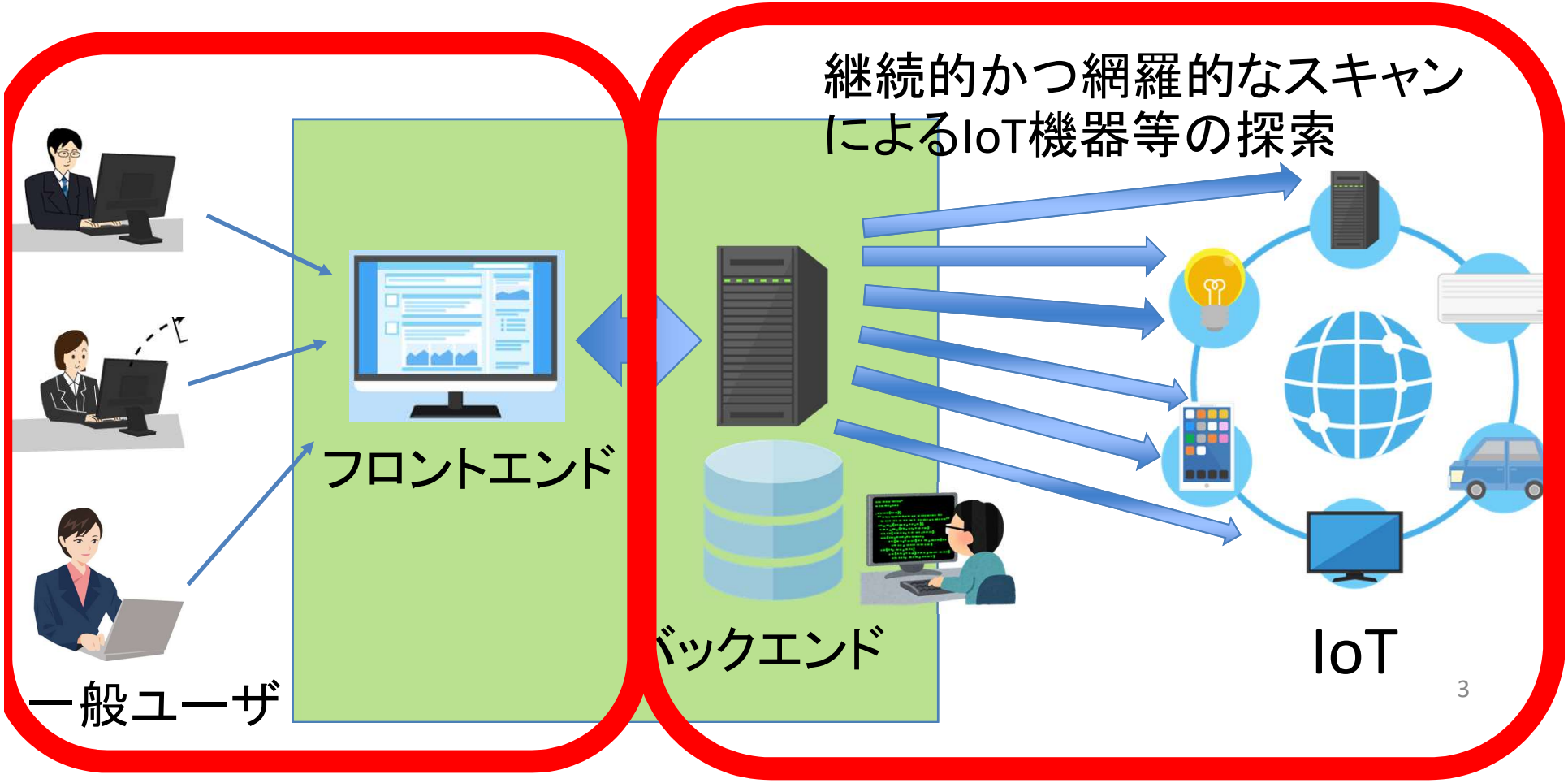
サイバーセキュリティタスクフォース資料（2019/11/22）

アジェンダ

- ネットワーク探索の激化
- 国内の重要IoT機器のセキュリティ

ネットワーク探索システム

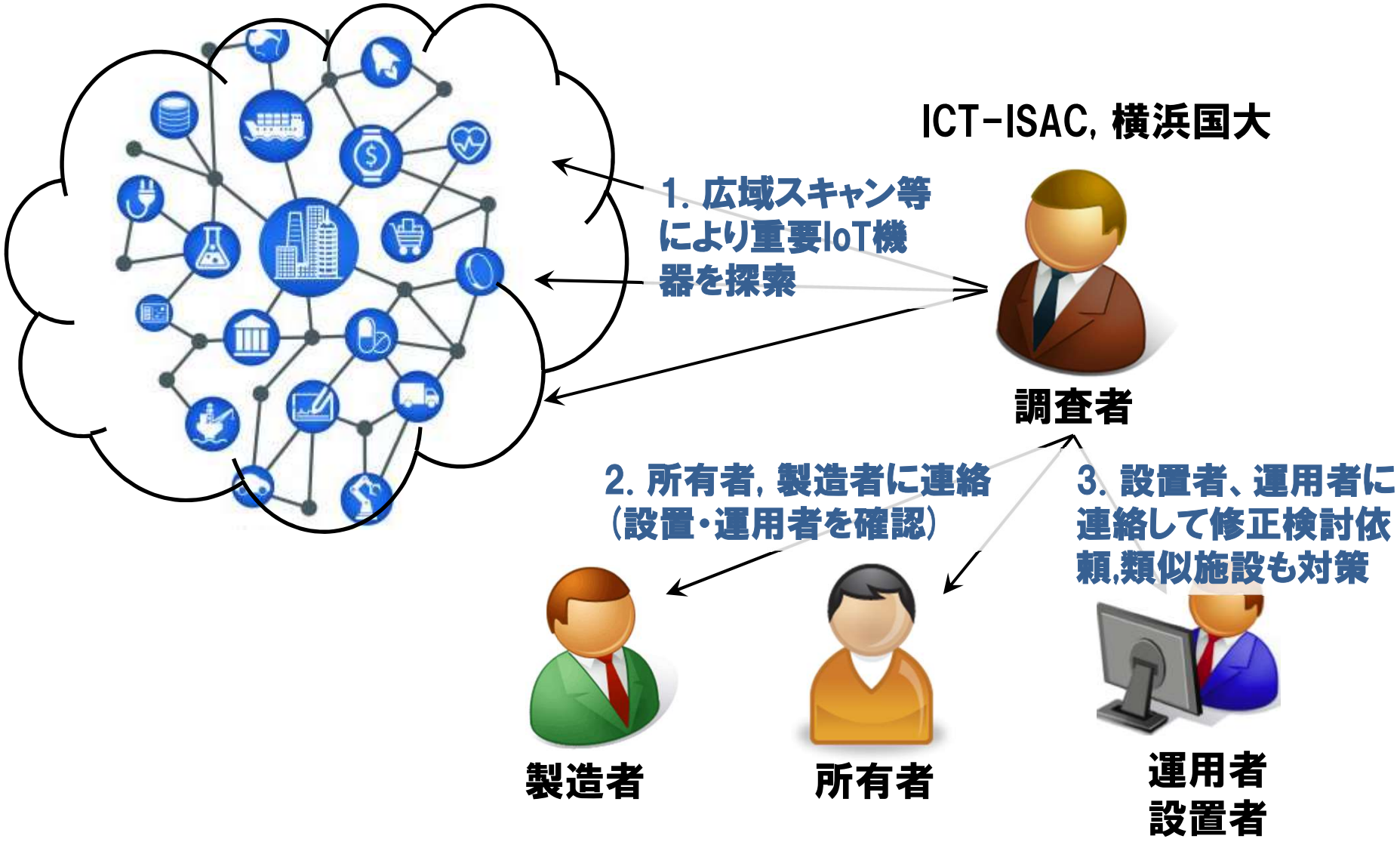
継続的かつ**網羅的**に広域ネットワークをスキャンし、IoT機器等の探索を行うシステム



アジェンダ

- ネットワーク探索の激化
- 国内の重要IoT機器のセキュリティ

IoT機器に関する脆弱性調査等の実施（2017）



セキュリティ不備のあるこれらの重要施設の遠隔システムには、実際に不審なアクセスや攻撃があるのか？

3か月間で100件超の手動アクセス

- 管理画面にアクセスした全IPアドレス数：　86,335
- うちペイロードを送ったIPアドレス数：　58,111
- うち手動アクセスを行なったIPアドレス数：　131
- うち手動アクセス者数：　127

まとめ

- 公知、未知のネットワーク探索システムの活動が非常に活発になっており、IoT機器の所在やセキュリティ状態が全世界的に把握されつつある
- 探索システムの悪用については不明だが、明らかに不要なアクセスを誘発しているケースがある
- 国内の重要施設を遠隔監視するシステムにもセキュリティ不備が散見される
- ハニーポットの観測結果を見る限り、セキュリティ不備のあるシステムは(いたずら～深刻事例含め)不正アクセスのリスクがある
- 攻撃者より先にセキュリティ不備を見つけ、迅速に通知して対策を行う試みが重要
- 機械学習、人工知能の利用により発見の効率は劇的に向上する可能性がある
- どうすれば探索システムや攻撃者に容易による情報収集を軽減できるのか、ディセプション技術を真剣に検討する必要あり

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

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（WarpDrive）（H28-R2）」の支援を受けて行われたものです。

謝辞2：本研究の一部は「総務省 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。