資料2－1

サイバーセキュリティの取組みについて

2023年2月16日

NTTコミュニケーションズ株式会社
情報セキュリティ部長

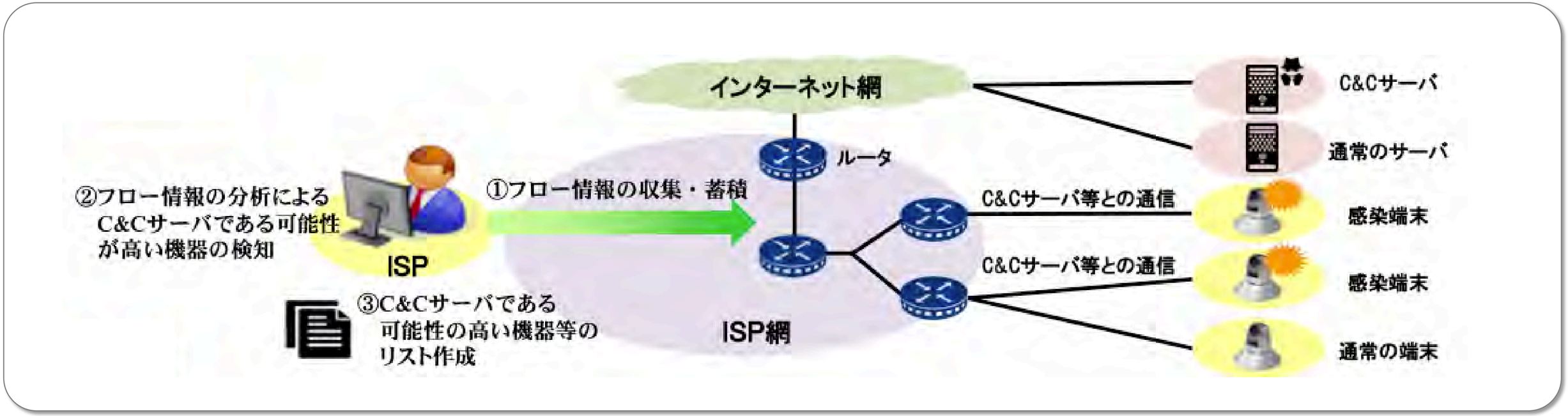
小山 覚

１．通信フロー分析の取組み

２．IoT機器を踏み台にしたサイバー攻撃対策

【参考】フロー情報の分析によるC&Cサーバの検知

- **2021年11月から通信事業者が通信のフロー情報（IPアドレス、ポート番号、タイムスタンプ）を分析し、C&Cサーバ（攻撃の命令元）を検知することが可能になった**



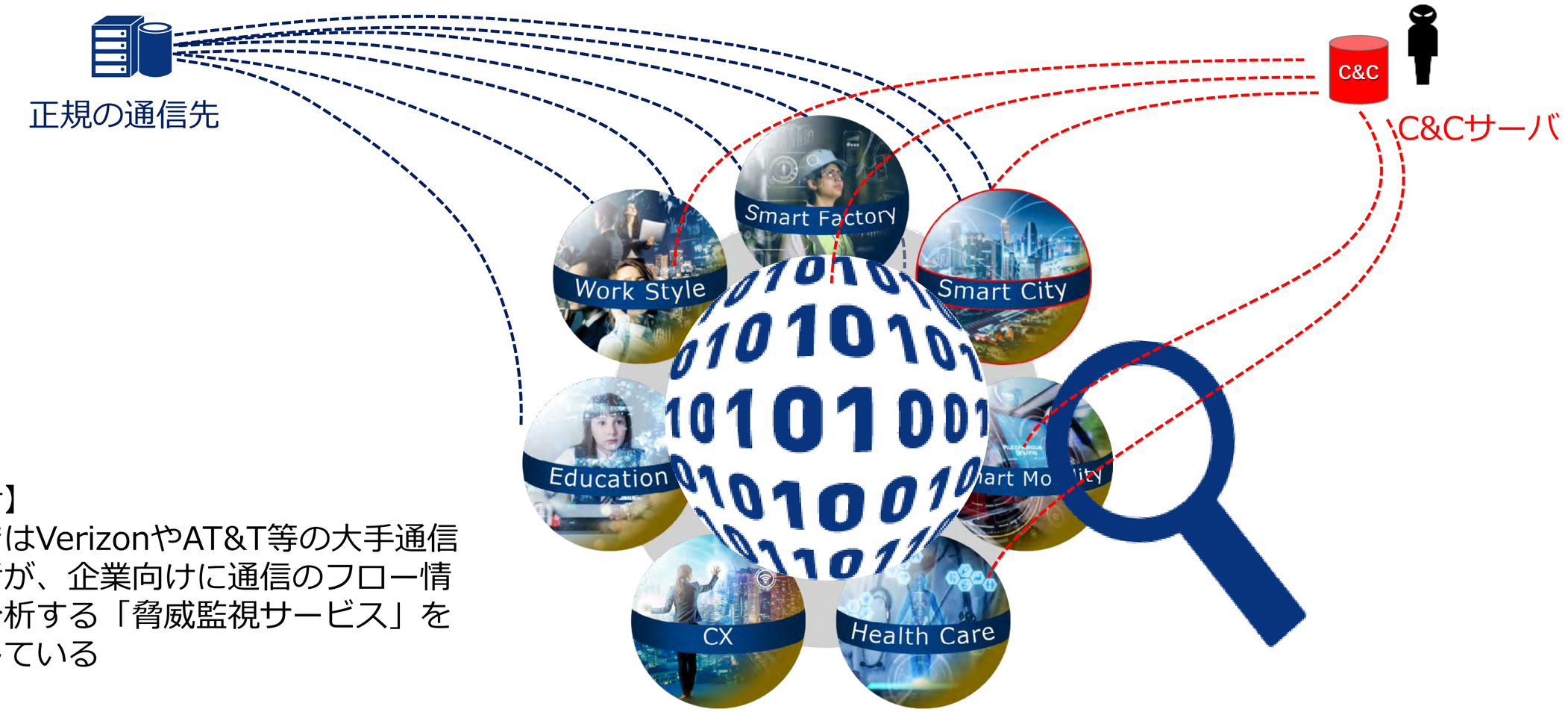
*総務省 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 第四次とりまとめ概要から抜粋
https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000134.html

Network as a Sensor（NaaS）

2021年12月から自社通信フローを分析し社内セキュリティ対策への活用検討を開始

自社インフラへのサイバー攻撃をNaaSを活用して検知する

蓄積している通信フローを調査することで、疑わしい通信を一網打尽に検知可能
攻撃検知やログ分析が難しいIoT/OTインフラのセキュリティ対策に応用可能



【参考】
米国ではVerizonやAT&T等の大手通信事業者が、企業向けに通信のフロー情報を分析する「脅威監視サービス」を提供している

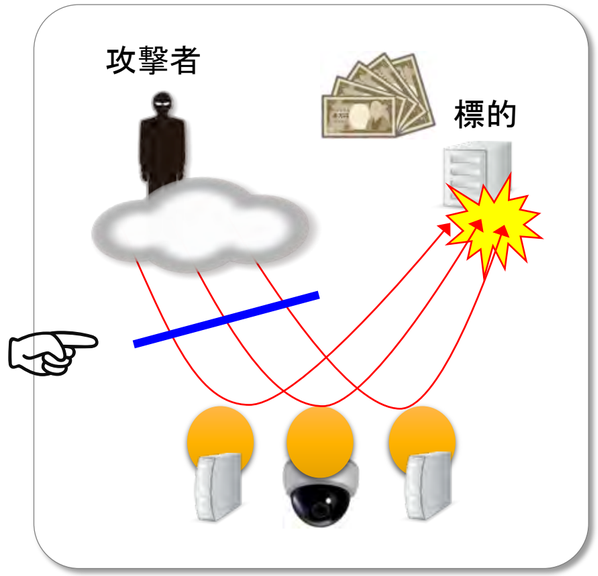
１．通信フロー分析の取組み

２．IoT機器を踏み台にしたサイバー攻撃対策

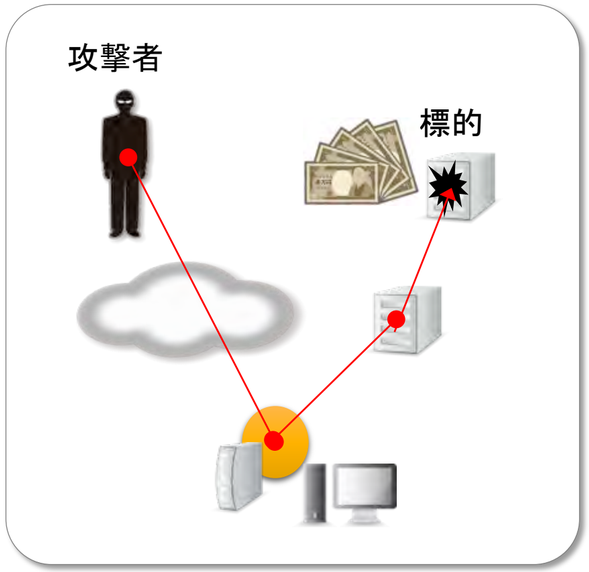
IoTが関係するサイバー攻撃の4類型と対策について

- 2021年11月頃から日本国内にあるIoT機器をボット化して操り、海外に向けた**「大規模なDDoS攻撃」**が発生し攻撃通信の経路上にある事業者回線帯域を圧迫、通信の安定運用に支障をきたしかねない事態が頻発した
- DDoS攻撃の宛先が海外ではなく国内であった場合は、大きな影響が発生した可能性があるため、本分科会で対策の検討をお願いしたい。

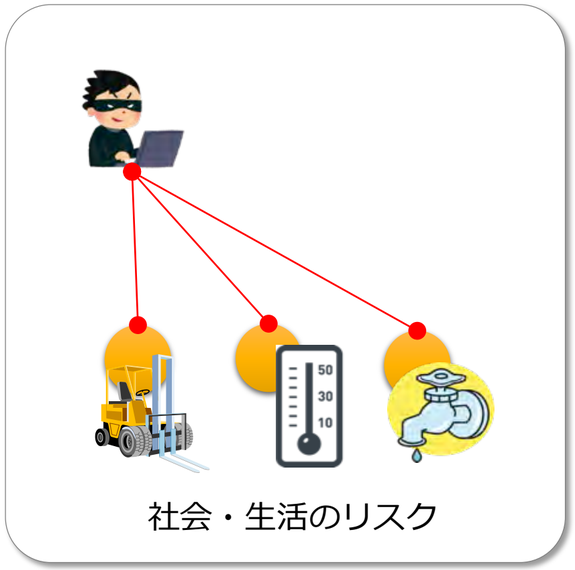
A：リフレクション攻撃
（DrDoS攻撃）



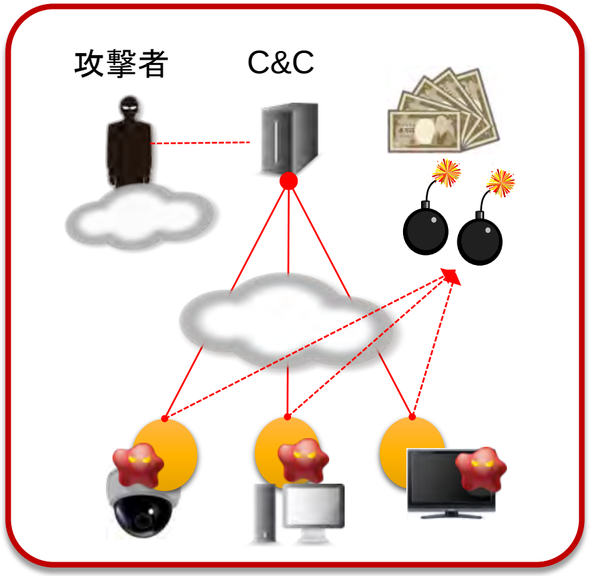
B：サイバー犯罪の踏み台
（ランサムウェア攻撃）



C：インフラへの直接攻撃
（スマート・シティ等）

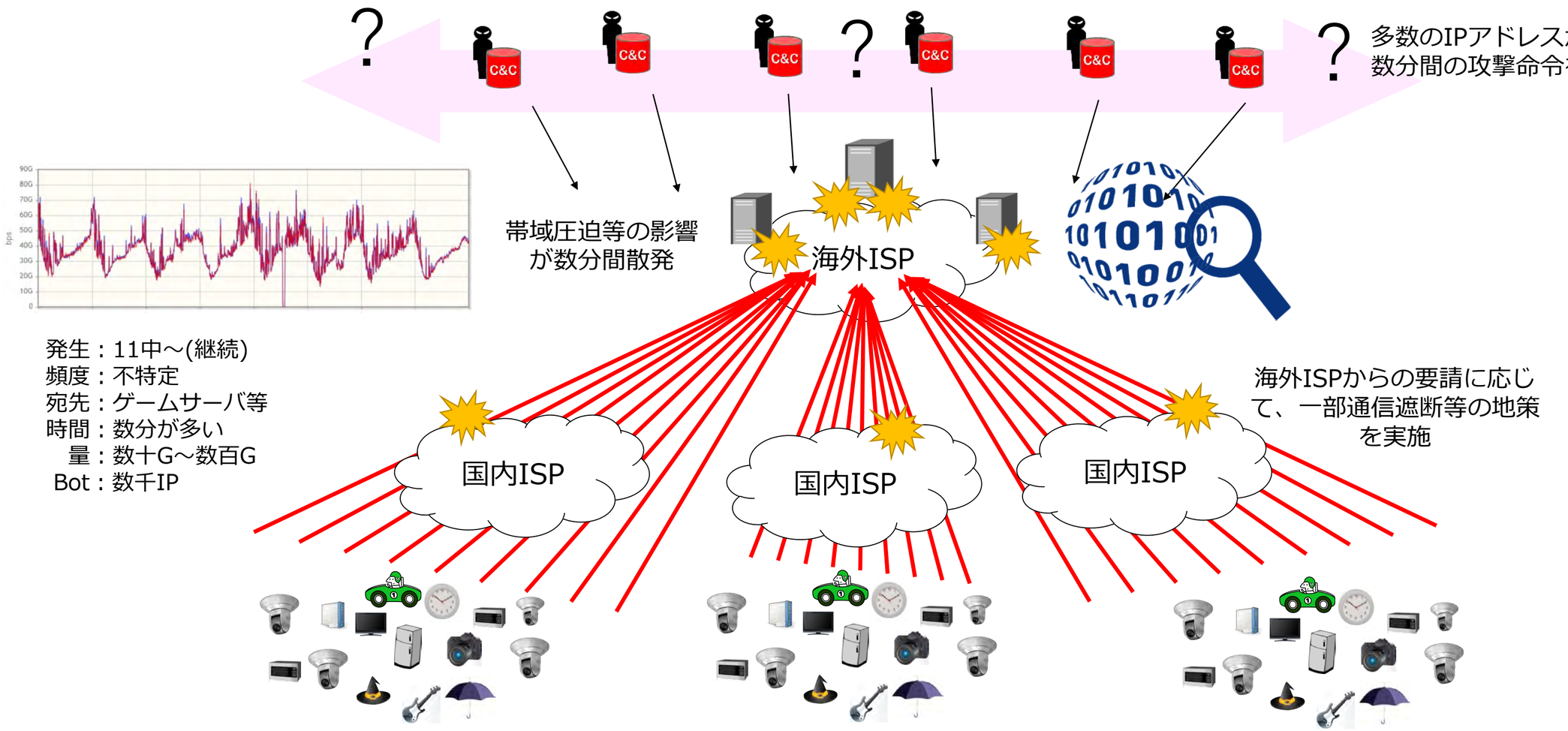


D：大規模なDDoS攻撃
（ボットネット）



IoTボットネットによるDDoS攻撃について事例紹介 1/2

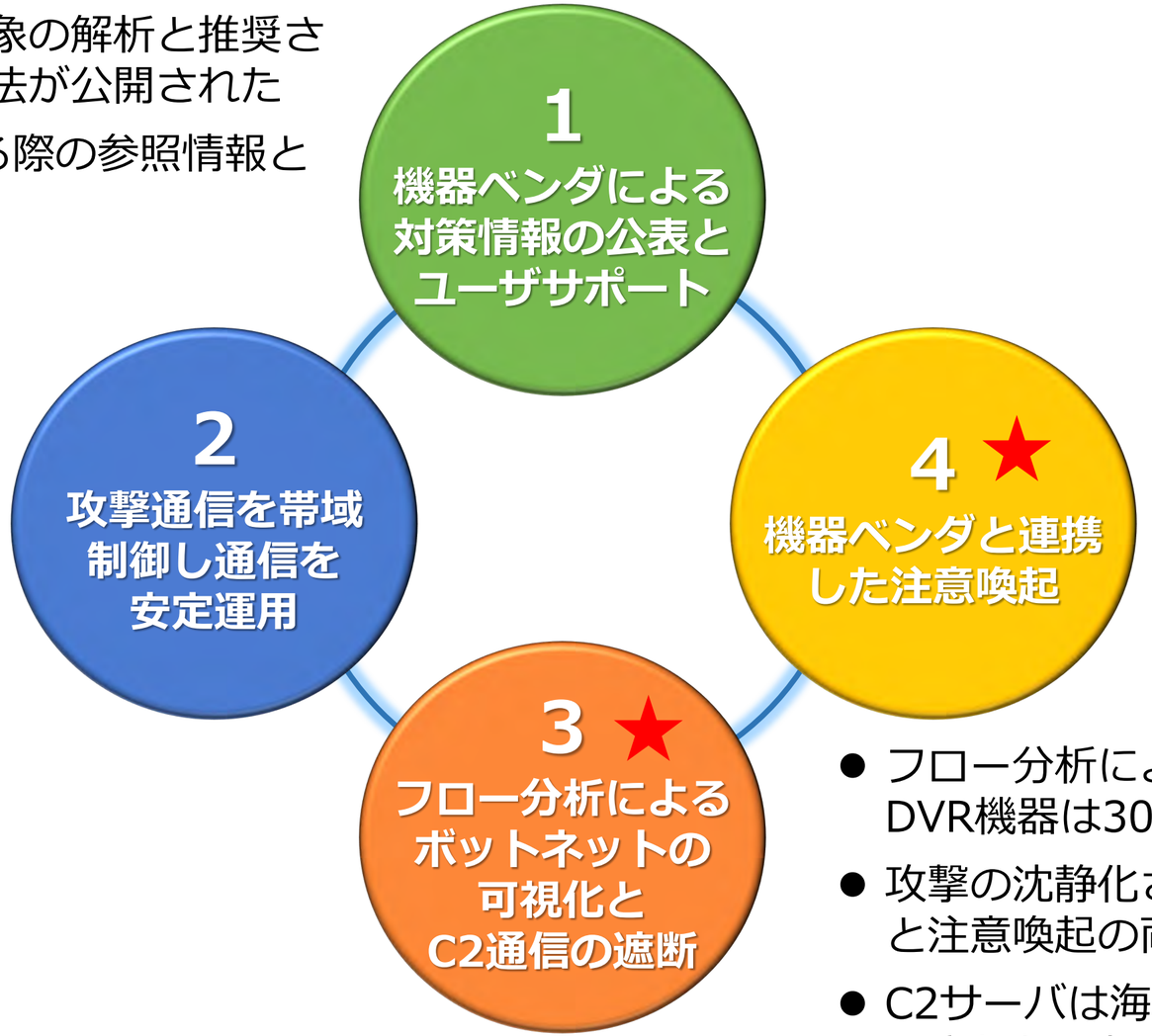
- 2021年11月頃から発生した攻撃は、ネットワークに接続された防犯カメラシステム（DVR）がボット化したもの。攻撃命令を出すC&Cサーバも頻繁にIPアドレスを変え攻撃先も都度変更された。通信フロー情報を一定期間分析してIoTボットネットの全体像を把握し、有効な対策を検討の上で対処すべきと考えられる。



IoT（DVR）ボットネットの対策で実施した取組み

通信フロー情報を分析しボットネットを可視化しつつ対策を実施した（2021年12月～）

- ベンダによる攻撃事象の解析と推奨される具体的な対策手法が公開された
- ISPから注意喚起する際の参照情報として有効活用できた



- 注意喚起に対し3割のDVR所有者から対策に前向きな反応があった
- 反応がない所有者を含め5割が対策を実施した模様
  （ボットネットの規模縮小を確認）

- 海外ISPからの攻撃遮断要請には難しい対応を迫られた
- 攻撃通信の経路上の回線帯域を圧迫したため、帯域制御を一部で実施

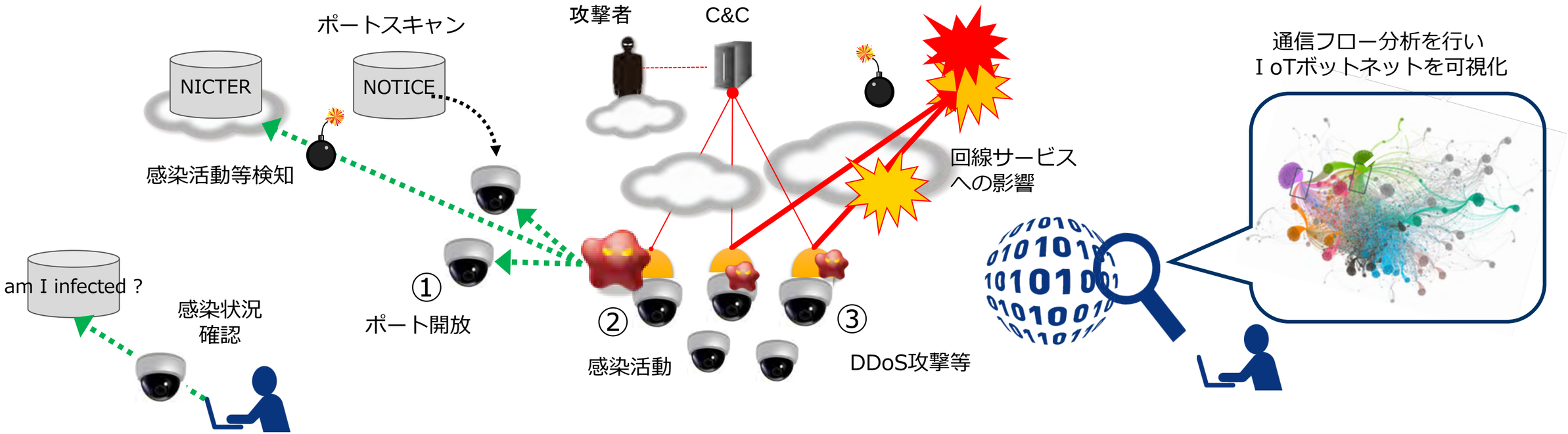
- フロー分析によりボットネットを可視化、DVR機器は3000台と想定
- 攻撃の沈静化させるため、C2通信の遮断と注意喚起の両方を実施
- C2サーバは海外にあるためテイクダウンできなかった

IoTボットネット対策の進め方のご提案（案）

● **国内のインターネット利用者が組み込まれているボットネットを可視化し、対策の効果が見込まれる処方箋が整ったボットネットから順番に、それぞれ用意したアクションプランを実施してはどうか？**

	実施項目	対策実施内容（今後具体的に詰めていきたい内容）
可視化 （次項参照）	活動中のIoTボットネットを調査	• NICTERで検知した感染端末のIPアドレスを分析しボットネットのコロニーを可視化 • セキュリティベンダや研究者が調査したC2情報と通信フロー情報を突合し、活動中のボットネットを把握し可視化
	通信フロー情報分析しIoTボットネットを可視化	• ボットネットの構成要素を細分化し、特徴を分類しナンバリング*して管理する • IoT機器感染型の場合は、構成される機器名、台数、C2サーバ情報、攻撃能力や内容 • 有効な対策を検討しコロニー単位に対策の処方箋を書く　*ナンバリング例：CLA00001
	IoTボットネットの定点観測	• ナンバリングしたボットネットは適時観測し規模や攻撃頻度等の変化を確認する
対策実施	ボット化しているIoT機器メーカ等への協力要請	**メーカーやベンダ等が対策の必要性を理解し利用者のサポートを行う** • 自社機器が感染し第三者に被害を与える可能性があるため対策を推奨する • 具体的な症状があれば記載 • ISPから注意喚起が来た場合は対応すること
	利用者による感染事実の確認方法の準備	• 感染者が容易に感染事実を確認できることが対策の動機につながる。 • 例えば「am I infected ?」や「NICTER」や「通信フロー分析」の結果を表示
	C&Cサーバのテイクダウン手続き	• ナショナルCERT連携やLOE連携でC2サーバテイクダウンを進め同期をとり対策を実施
	C&C通信遮断手法の検討と実施	• C2通信遮断時に発生する、C2サーバの切り替わり等のイタチごっこを想定した遮断方法を検討
	利用者への注意喚起の検討と実施	• メーカ連携した注意喚起の方法と効果測定方法を検討し、他の対策と連携して注意喚起を行う
研究開発	産学連携の研究開発を推進	• 例）米国ではCMU主催のセキュリティ会議（FIoCon）が開催され多彩な研究活動が展開

IoTボットネットの可視化イメージ



IoT機器の状況		危険度			可視化の方法	プロファイリング内容
		1	2	3		
①	・危険なポートが開放されている ・脆弱なパスワード設定になっている ・ファームウェアが古く脆弱性がある	○			・外部からのポートスキャン ・Shodan等のリスト確認	・製品名・メーカ・ベンダ ・脆弱性・設定不備内容 ・対処方法 ・ボットネット規模 ・攻撃能力
②	・第三者に感染活動を行っており、NICTER Darknet Sensor で検知される		○		・NICTER等で検知 ・ハニーポットで検知	
③	・C2と頻繁に通信し、第三者にDDoS攻撃等を行い被害が出ている			○	・通信フロー分析で確認	

萎んでいくIoTボットネットを可視化し効果の確認を行う

C2通信の遮断
C2サーバのテイクダウン

IoT機器のパッチ適用
や設定変更

ビジュアルで効果を確認＋社会的なコンセンサス