情報通信ネットワークにおけるサイバーセキュリティ対策分科会　御中

資料４－１

電気通信事業者によるサイバー攻撃への効果的な対処を通じた安心・安全な情報通信ネットワークの実現に向けて

～令和4年度「電気通信事業者におけるフロー情報分析によるC&Cサーバ検知に関する調査の請負」に係るご報告～

2023年4月21日

エヌ・ティ・ティ・コミュニケーションズ株式会社

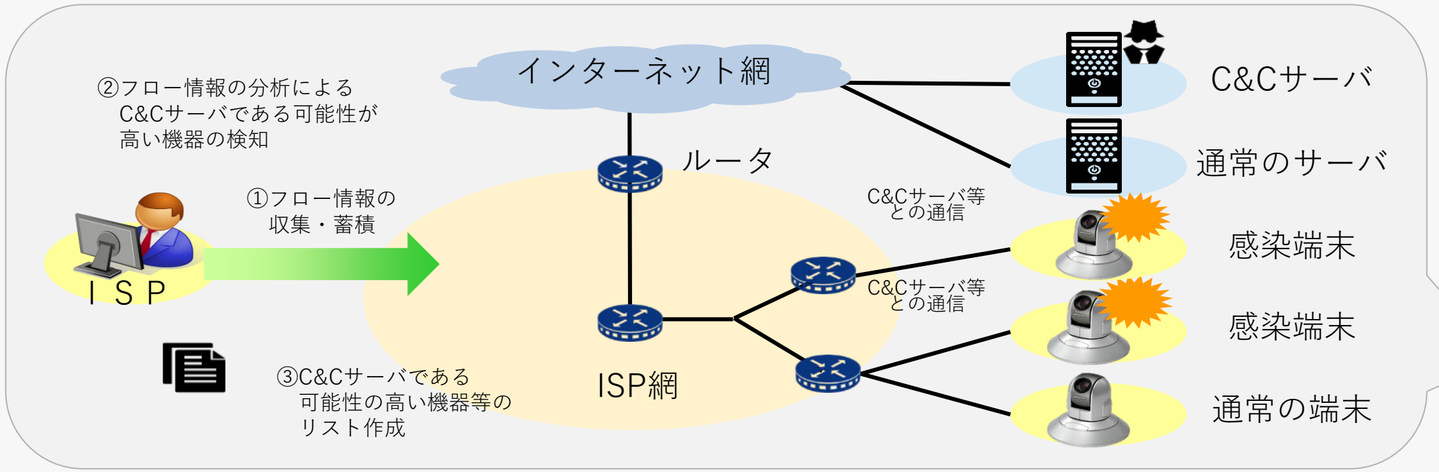
本調査の背景・目的

「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」の「第四次とりまとめ*」により以下が可能に。

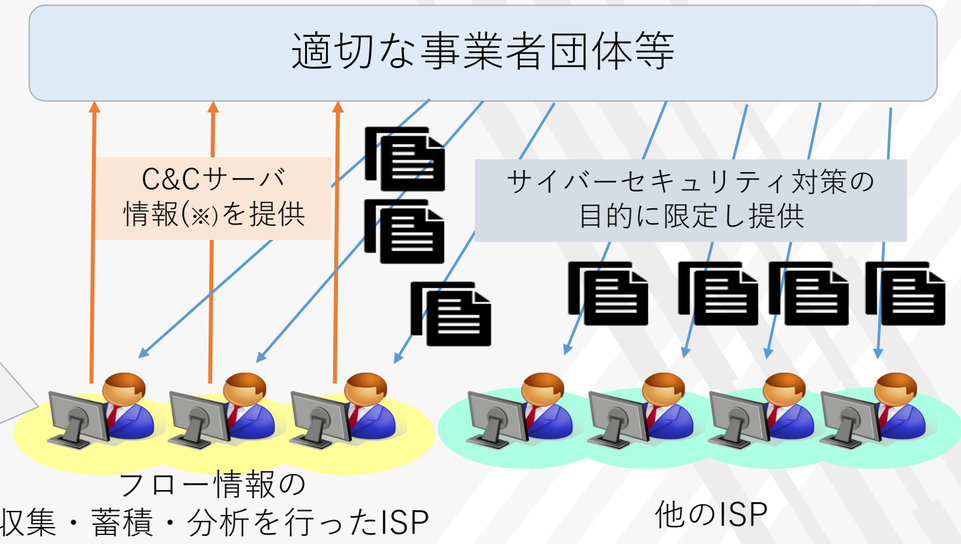
① **電気通信事業者が平時において通信のフロー情報（IPアドレス、ポート番号、タイムスタンプ等）を分析し、C&Cサーバ（攻撃の命令元）を検知すること。**

② **C&Cサーバに関する情報（IPアドレス、ポート番号）を、サイバーセキュリティ対策のために適切な事業者団体等に提供すること。**

① 平時におけるフロー情報の収集・蓄積・分析によるC&Cサーバである可能性が高い機器の検知



② 検知したC&Cサーバに関する情報についての共有



(※) C&Cサーバに関するIPアドレス及びポート番号のリスト

我が国の情報通信ネットワーク上で活動する「実際の」C&Cサーバを把握／連携による対処が可能となる。
→国内において実際にC&Cサーバの検知／共有を行い、検知手法の有効性や
検知／共有における技術面、運用面における課題を整理・把握するため、実証実験を実施。

＊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」.「第四次とりまとめの概要」. 5 頁. 2021. https://www.soumu.go.jp/main_content/000779408.pdf （参照：2023年4月11日）

調査の概要

電気通信事業者3社と一般社団法人ICT-ISACとで以下３つの検証・検討を実施。

実施内容

①　検知

・検知手法の開発(2種類)

・実際の通信を用いた検知

・C&Cサーバ情報のリスト化

②　評価

・提供されたC&Cサーバリストの多面的な分析
（悪性度評価、事業者間の相関性、先行検知率、C&Cサーバ推定生存期間、推定所在国　等）

③　共有

・リストの共有に係る検討

・検知手法の共有に係る検討

・リスト利活用に係る検討

実施主体

国内の電気通信事業者　として

- NTTコミュニケーションズ株式会社
- 東日本電信電話株式会社
- ＫＤＤＩ株式会社

適切な事業者団体　として

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

- C&C調査プロジェクト業務推進G
（左記電気通信事業者3社を含む）
- C&Cリスト利活用共有WG
（ICT-ISAC会員電気通信事業者13社を含む）

①　検知について

実施内容

①　検知

・検知手法の開発(2種類)

・実際の通信を用いた検知

・C&Cサーバ情報のリスト化

②　評価

・提供されたC&Cサーバリストの多面的な分析
（悪性度評価、事業者間の相関性、先行検知率、C&Cサーバ推定生存期間、推定所在国　等）

③　共有

・リストの共有に係る検討

・検知手法の共有に係る検討

・リスト利活用に係る検討

実施主体

国内の電気通信事業者　として

NTTコミュニケーションズ株式会社

東日本電信電話株式会社

ＫＤＤＩ株式会社

適切な事業者団体　として

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

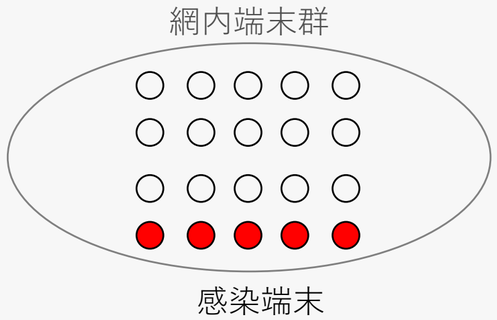
C&C調査プロジェクト業務推進G
（左記電気通信事業者3社を含む）

C&Cリスト利活用共有WG
（ICT-ISAC会員電気通信事業者13社を含む）

①　検知手法の開発（１）

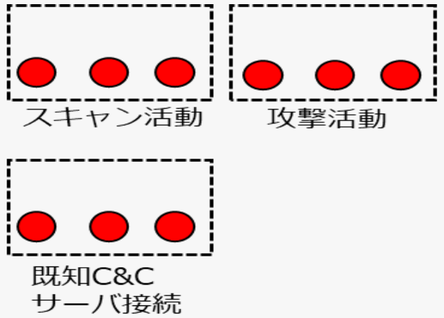
電気通信事業者３社それぞれが「グラフマイニングを用いた手法」を開発の上、自社網へ適用。

感染端末の特定



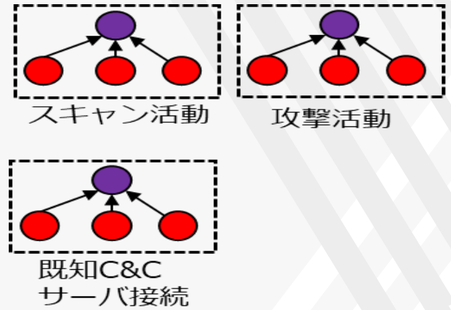
分析システムのアルゴリズムに
よりスキャン活動などを行う
端末を特定

感染端末グルーピング



端末、フロー情報を原因等により
グループ化

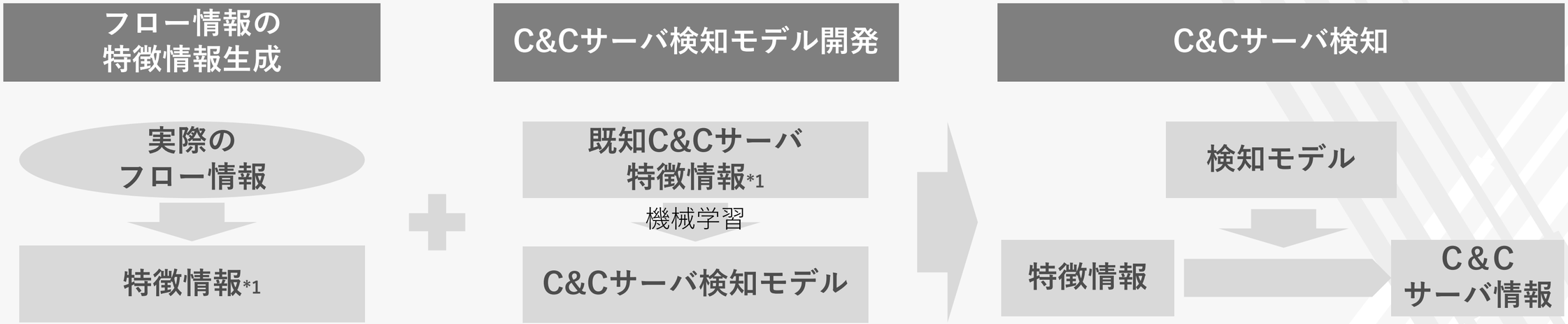
C&Cサーバ検知



各グループごとの共通通信先を
C&Cサーバとして検知

①　検知手法の開発（２）

電気通信事業者３社それぞれが「機械学習を用いた手法」を開発の上、自社網へ適用。



実際のフロー情報から
IPアドレスごとの特徴情報を計算

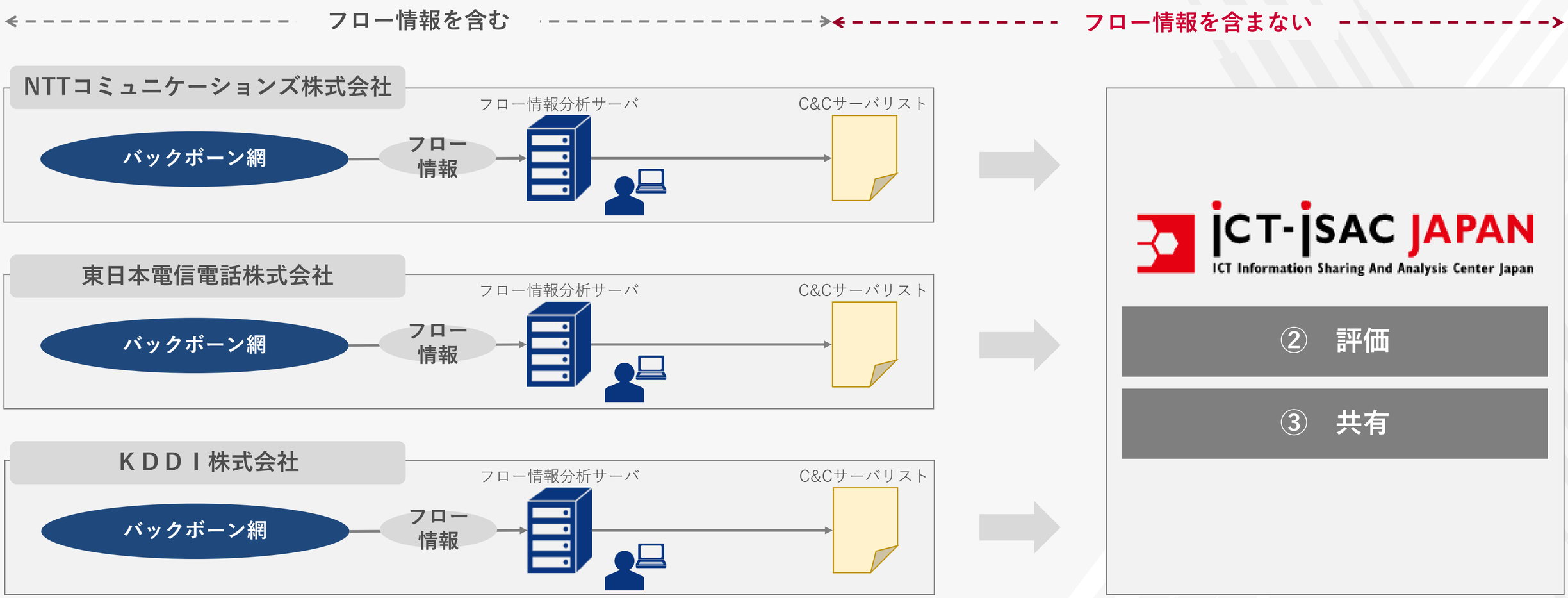
既知C&Cサーバの特徴情報を
正解ラベルとして機械学習の上、
C&Cサーバ検知モデルを作成

検知モデルを適用し、特徴一致したものを
C&Cサーバとして検知

*1 通信時間・通信時刻・パケット流量・通信頻度・通信先等を指す。

①　C&Cサーバの検知・リスト化

フロー情報は第三者に提供(委託を含む。)できないことに留意をしながら、電気通信事業者各社が
実際のフロー情報をもとに検知を行い、C&Cサーバリスト(IPアドレス、ポート番号)を生成の上、ICT-ISACへ提供。



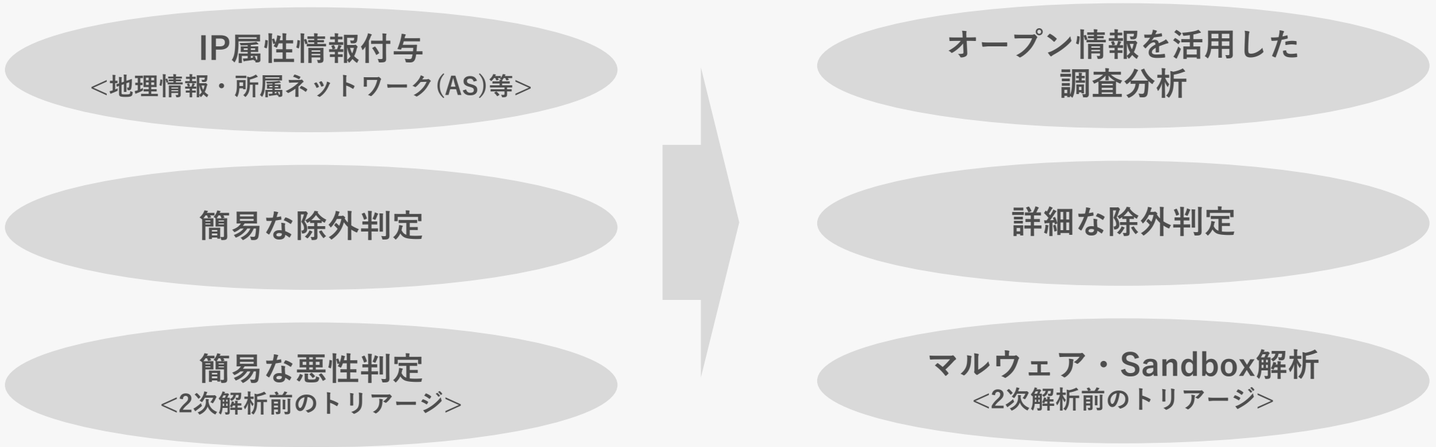
② 評価について

	① 検知	② 評価	③ 共有
実施内容	・検知手法の開発(2種類) ・実際の通信を用いた検知 ・C&Cサーバ情報のリスト化	・提供されたC&Cサーバリストの多面的な分析 （悪性度評価、事業者間の相関性、先行検知率、C&Cサーバ推定生存期間、推定所在国　等）	・リストの共有に係る検討 ・検知手法の共有に係る検討 ・リスト利活用に係る検討
実施主体	国内の電気通信事業者　として NTTコミュニケーションズ株式会社 東日本電信電話株式会社 ＫＤＤＩ株式会社	適切な事業者団体　として ICT-ISAC JAPAN ICT Information Sharing And Analysis Center Japan C&C調査プロジェクト業務推進G （左記電気通信事業者3社を含む）	C&Cリスト利活用共有WG （ICT-ISAC会員電気通信事業者13社を含む）

②　評価の全体像

定型的な処理／セキュリティ専門家のノウハウを用いた非定型な詳細分析により
電気通信事業者からのC&Cサーバリストを評価の上、有効性等について確認。

評価の流れ



確認した主なポイント

悪性度評価
提出されたリストにC&Cサーバは含まれるか？

事業社間の相関性
複数の事業者が協調していくことの意義は？

先行検知率
オープン情報との違いは？

C&Cサーバ推定生存期間
C&Cサーバはどれくらい活動している？

C&Cサーバ推定所在国
C&Cサーバはどこにある？

次頁以降、各社ごと評価結果をご説明しておりますが、各社の検知手法の特徴等に係ることから、事業者A,B,Cとして匿名化させて頂きます。

② 悪性度評価

各社から共有されたC&Cサーバリストの悪性度を評価した結果は以下のとおり。検知したC&Cサーバの種類に事業者ごとの特徴がみられた。
その他、３社それぞれが「Killnet-Proxy」や「Killnet-c２」等、近年問題視されている大規模DDoS攻撃を行うインフラの検出にも成功。

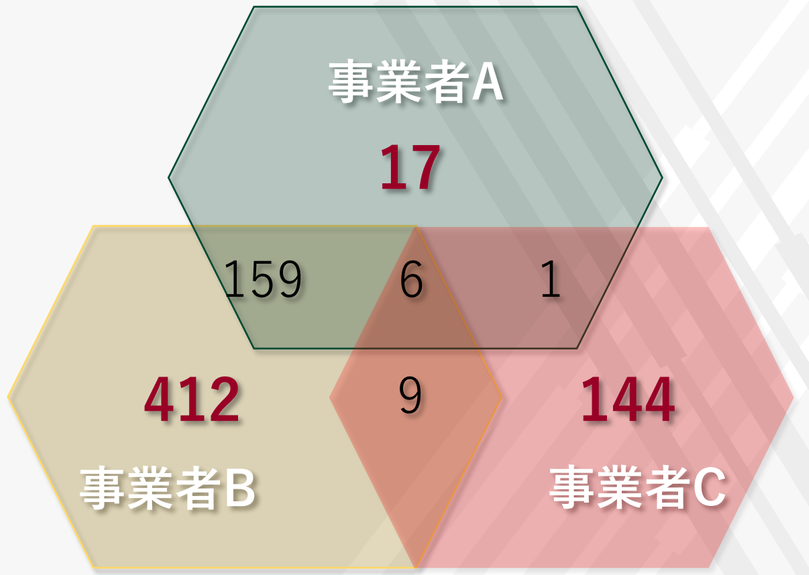
事業者	各社における分析結果	悪性IP数※1	悪性度評価を経たC&Cサーバ		【参考】悪性度評価により判明した通信特性※2,3			
			IP数	主な種類（関連マルウェア）	bot※4	Brute force※5	ssh※6	tor※7
事業者A	12,835 (80.0/日)	1,148 (7.4/日)	183 (1.2/日)	Mirai系 116(61%)	274	185	206	743
事業者B	621,703 (4,377.9/日)	13,742 (51.5/日)	586 (12.3/日)	Mirai系 388(66%)	8903	4208	8333	3395
事業者C	792 (62.7/日)	172 (12.4/日)	160 (11.4/日)	Emotet系 86(53%)	17	10	9	6

※1　サイバー攻撃等を目的とした通信を行っていると推察されるIPアドレスの数。尚、その内訳には匿名プロキシサービスの構成要素となっているIPやセキュリティ調査プロジェクトやインターネット品質測定などの正規調査プロジェクトに関連するIPも含まれる。
※2　複数のカテゴリに該当するIPアドレスもあるため合計値にはならない。
※3　アグレッシブ解析であること、またbot関連は流動性が高いことから、時間の経過と共に変動する可能性がある。
※4　C&Cサーバと通信もしくはボットネット拡大活動を行っていると推定されるIP 。
※5　ボットネット拡大活動等のためのBrute-force攻撃(総当たり攻撃を指す。暗号解読方法のひとつで、可能な組合せを全て試す手法を用いた攻撃。)を実施しているIP 。
※6　ボットネット拡大活動等のためにssh(Secure Shellの略。リモートコンピュータと通信するためのプロトコル。) 等を用いて遠隔から不正にログインを試みているIP。
※7 Torはインターネット上で発信元の秘匿性が高い通信を行うことができるシステム。ここではTorを用いて作られた匿名ネットワークの構成要素となっているIP。
※8 「Distributed Denial of Service attack（分散型サービス妨害攻撃）」の略称。あらかじめ不特定多数のPCにボットウイルスを感染させておき、感染したPCを経由させて多量のアクセスやデータ送付し、対象とするサービスやシステムに負荷をかけ、Webサイトの遅延や機能停止を引き起こすサイバー攻撃。

②　事業社間の相関性

特定の事業者のみが検出したＩＰを多数確認できた他、3社共通で検知したIPも確認。
→事業者間連携を行うことで「より多くのC&Cサーバの検知」や「より影響度の高いC&Cサーバの特定」等に期待。

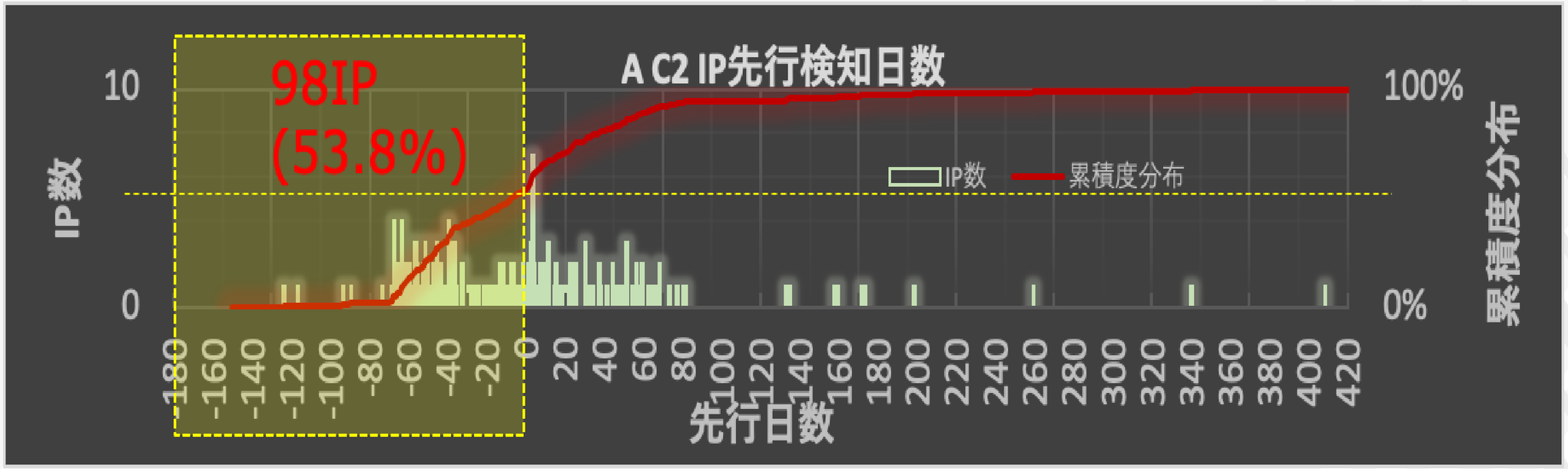
事業者	C&Cサーバ	
	総IP数	主要な関連マルウェア
事業者A	183 (1.2/日)	Mirai系 116(61%)
事業者B	586 (12.3/日)	Mirai系 388(66%)
事業者C	160 (11.4/日)	Emotet系 86(53%)



② 先行検知率

事業者の検知日とオープン情報上でC＆Cサーバと判定された日を比較。
→オープン情報上での判定日前に５割強を平均43.6日早く検知。

事業者Aの事例



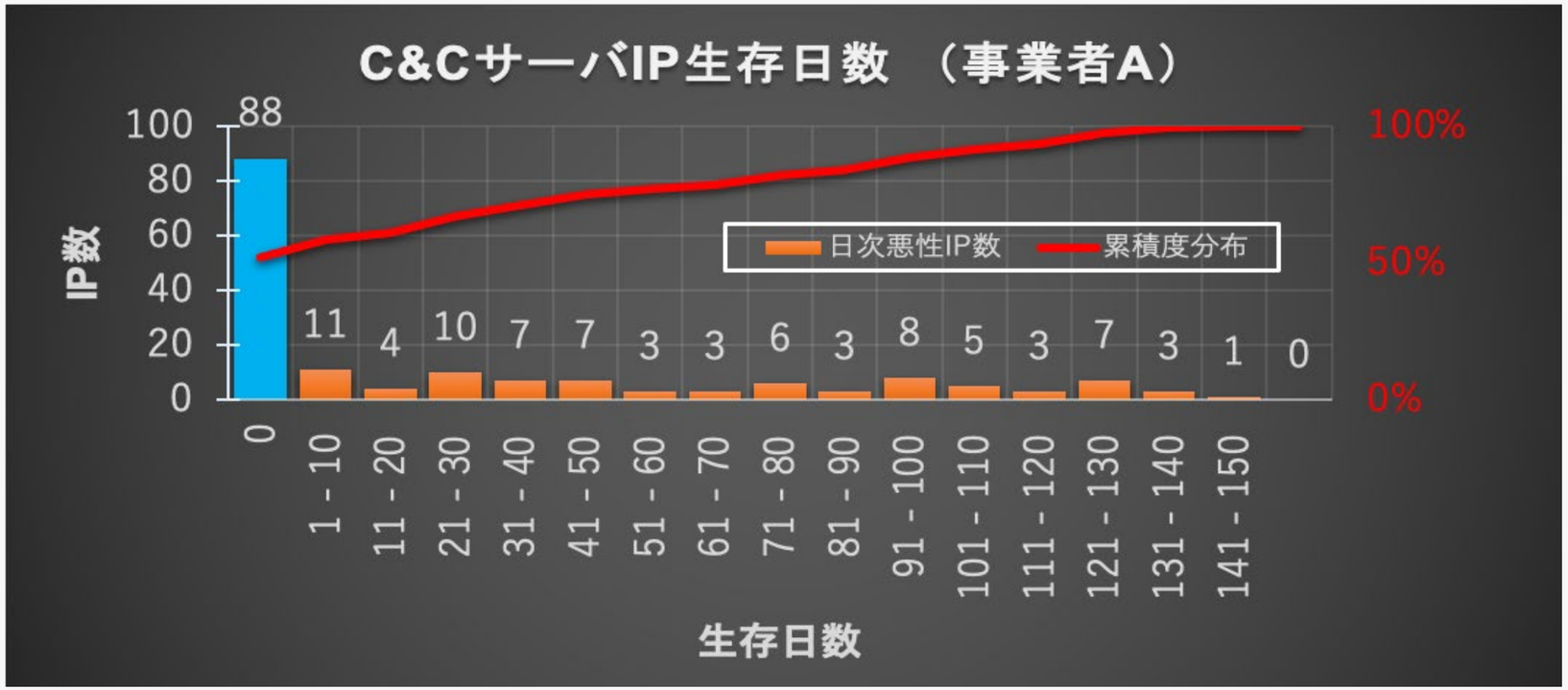
各種オープン情報上でC2サーバと判定された日と事業者にて検知された日を比較

検知後リストの評価迄に時間が経過したケース等もあり、利活用に向けては検討・改善が必要。

②　C&Cサーバの推定生存期間分析

各事業者にて検知されたC&Cサーバについて、初回検知日と最後に検知された日の期間を分析。
1度だけ検知されたC＆Cサーバが約半数ある一方で、10日以上生存確認されたC&Cサーバも同数程度確認。

事業者Aの事例



推定生存日数＝初回検知日と最後に検知された日の期間

平均推定生存日数は20.2日
→早期検知・早期対処が重要

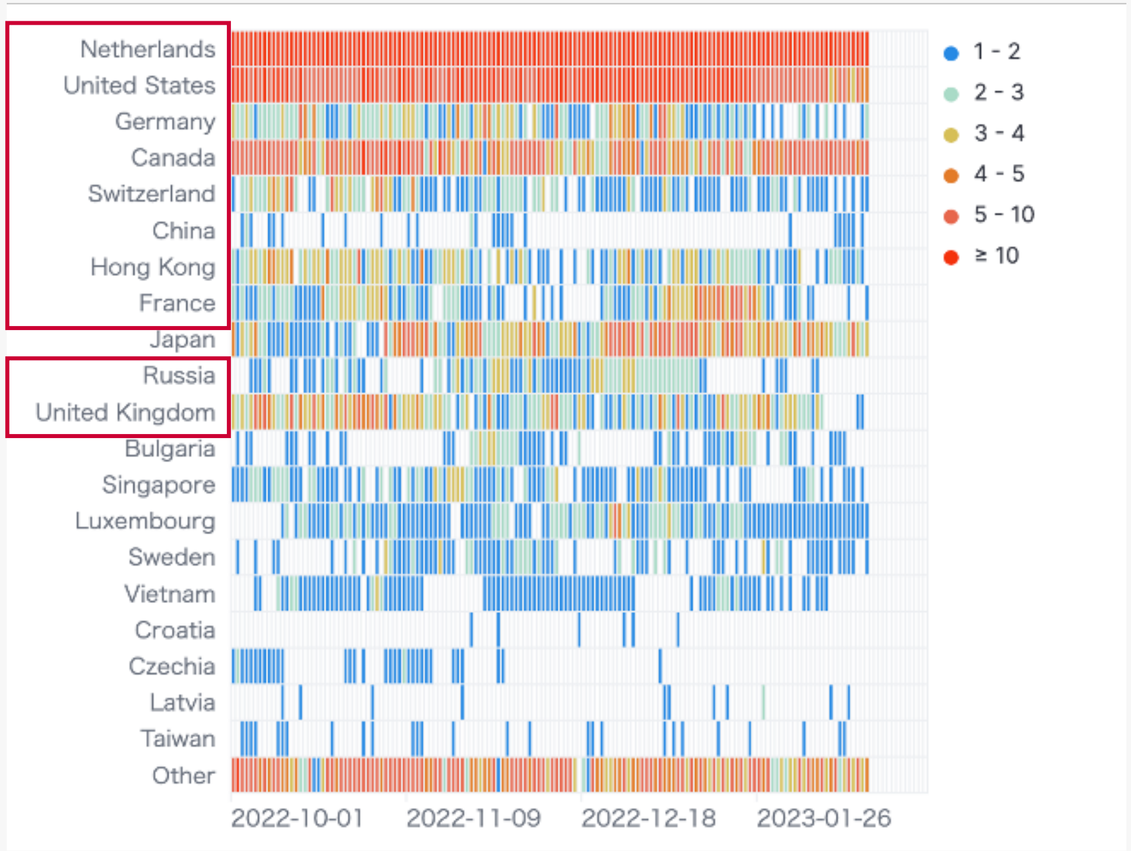
一度だけ検知されたC&Cサーバ(青棒)は、真に活動停止したのか、検知されなかっただけなのか等、現状、詳細不明。

より正確に活動実態を捉える為に、検知されたIPに対する継続的な監視・分析の仕組みが必要。

② C&Cサーバの推定所在国分析

今回検知したC&Cサーバの推定所在国を分析。
大まかな傾向として、基本的にＣ＆Ｃサーバは海外所在と推定される。

事業者BにおけるC&C IPの所在国別IP数日次推移

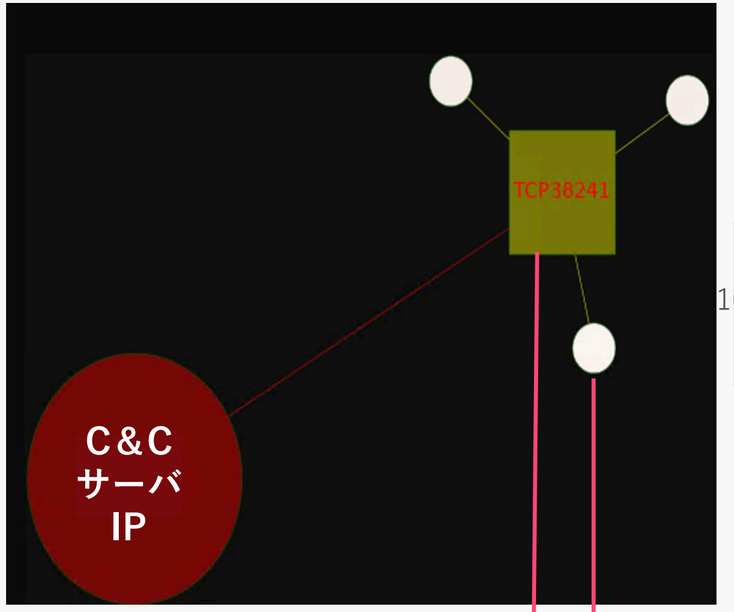


事業者CにおけるC&C IPの所在国別IP数日次推移

②　【参考】ボットネット可視化による攻撃トレンドの把握

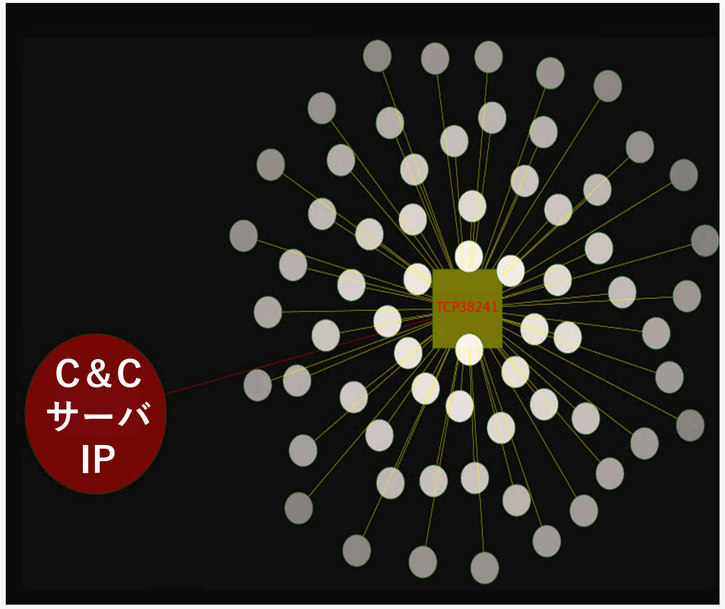
ボットネットを可視化。全体像や活動状況等を直感的に捉えることができる。
C&Cサーバリストを活用した対策の実施や更なる分析等、運用面時の実用性の向上に期待。

検知初期



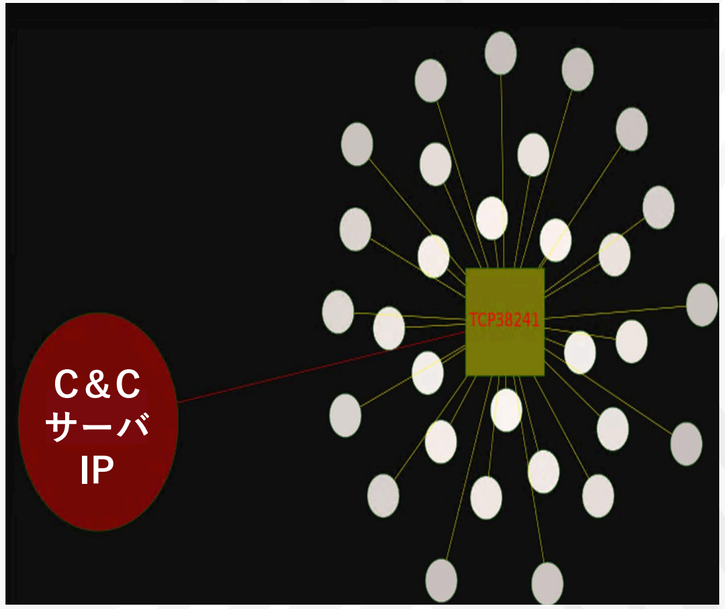
10日後

規模拡大



さらに
10日後

規模縮小



bot

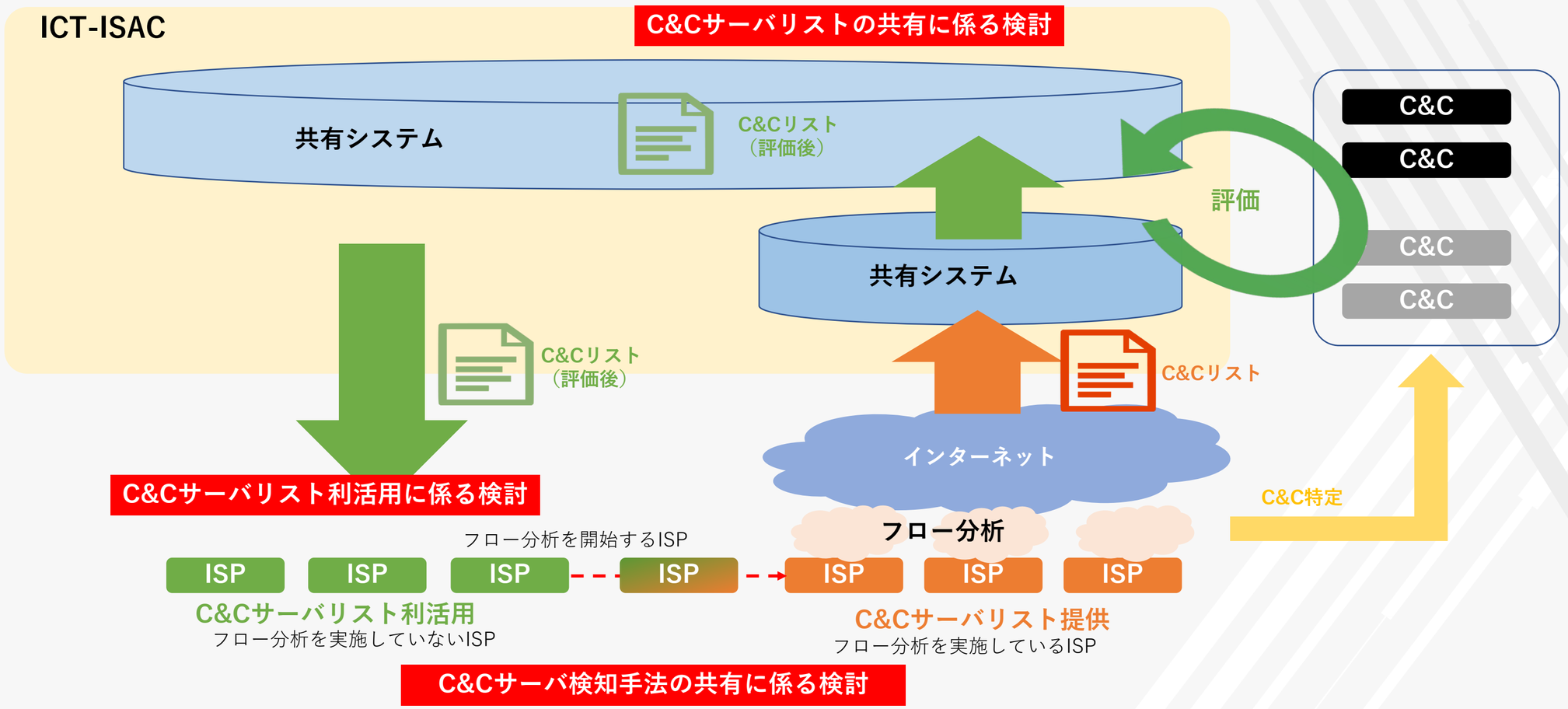
C&Cサーバの
通信ポート

③　共有について

	①　検知	②　評価	③　共有
実施内容	・検知手法の開発(2種類) ・実際の通信を用いた検知 ・C&Cサーバ情報のリスト化	・提供されたC&Cサーバリストの多面的な分析 （悪性度評価、事業者間の相関性、先行検知率、C&Cサーバ推定生存期間、推定所在国　等）	・リストの共有に係る検討 ・検知手法の共有に係る検討 ・リスト利活用に係る検討
実施主体	国内の電気通信事業者　として NTTコミュニケーションズ株式会社 東日本電信電話株式会社 ＫＤＤＩ株式会社	適切な事業者団体　として C&C調査プロジェクト業務推進G （左記電気通信事業者3社を含む）	ICT-ISAC JAPAN ICT Information Sharing And Analysis Center Japan C&Cリスト利活用共有WG （ICT-ISAC会員電気通信事業者13社を含む）

③　検討の全体像

一般社団法人ICT-ISAC内に電気通信事業者が参画するWGを設置。
ICT-ISAC会員電気通信事業者全13社からの意見に基づき、3つの観点で検討を実施。



③　検討の経過

C&Cサーバリストを共有する仕組みの実現に向けて、ヒアリング等通じて、論点を整理。
利活用にむけてのユースケースや情報精度の整理、コスト等の課題解決にむけて継続議論を行っていく。

C&Cサーバリストの共有に係る検討

期待

- 単独では検知できなかった脅威を認識できる。
- 影響度分析等へ活用できる。

今後の検討事項

- C&Cサーバリストに求める精度の整理。
- 共有スキーム／リソース等の整理。

C&Cサーバ検知手法の共有に係る検討

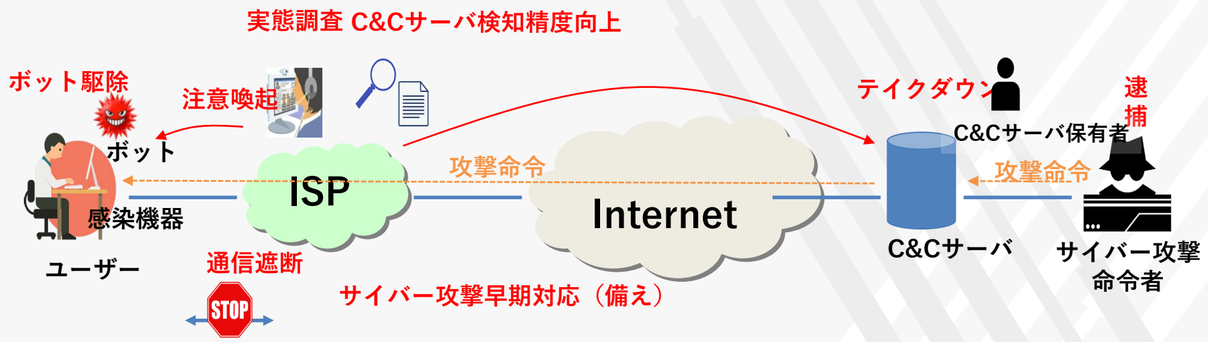
期待

- 分析手法を持たない事業者も検知ができる。
- FBや共有等による分析手法の改善・高度化。

今後の検討事項

- 共有内容や共有スキーム等の整理。
- 検知実行時の各電気通信事業者における負担等の整理

C&Cサーバリスト利活用に係る検討



C&Cサーバリストの利用用途例

調査
- トラフィック照合
- 自社システムとの通信有無調査
- 自社検知ロジック精度評価
- C&Cサーバ傾向評価
- 感染端末特定

対策（自社）
- C&Cサーバとの通信遮断
- 利用者への注意喚起
- DDoS攻撃への早期対応

ビジネス展開
- セキュリティ運用サービス提供
- C&Cサーバリスト有償提供

対策（連携）
- C&Cサーバ保有者特定
- C&Cサーバテイクダウン

今回の取り組みのまとめ【１】（成果、改善事項と今後の取り組み）

今回の成果

フローC&Cサーバ検知の試行と有効性確認

フロー情報分析を用いたC&Cサーバ検知について、３電気通信事業者がそれぞれ手法開発の上、実際の国内ネットワーク上で試行。各通信事業者のフロー分析によるＣ＆Ｃサーバの収集力、検出先行性などの面での有効性が確認できた。

３電気通信事業者+ICT-ISAC社による協調分析・評価

複数の通信事業者での協調分析の実現により、効果的な対策実現に向けて情報精度向上、リスク評価等の高度化の方向性と今後の技術面、運用面の課題抽出を行うことができた

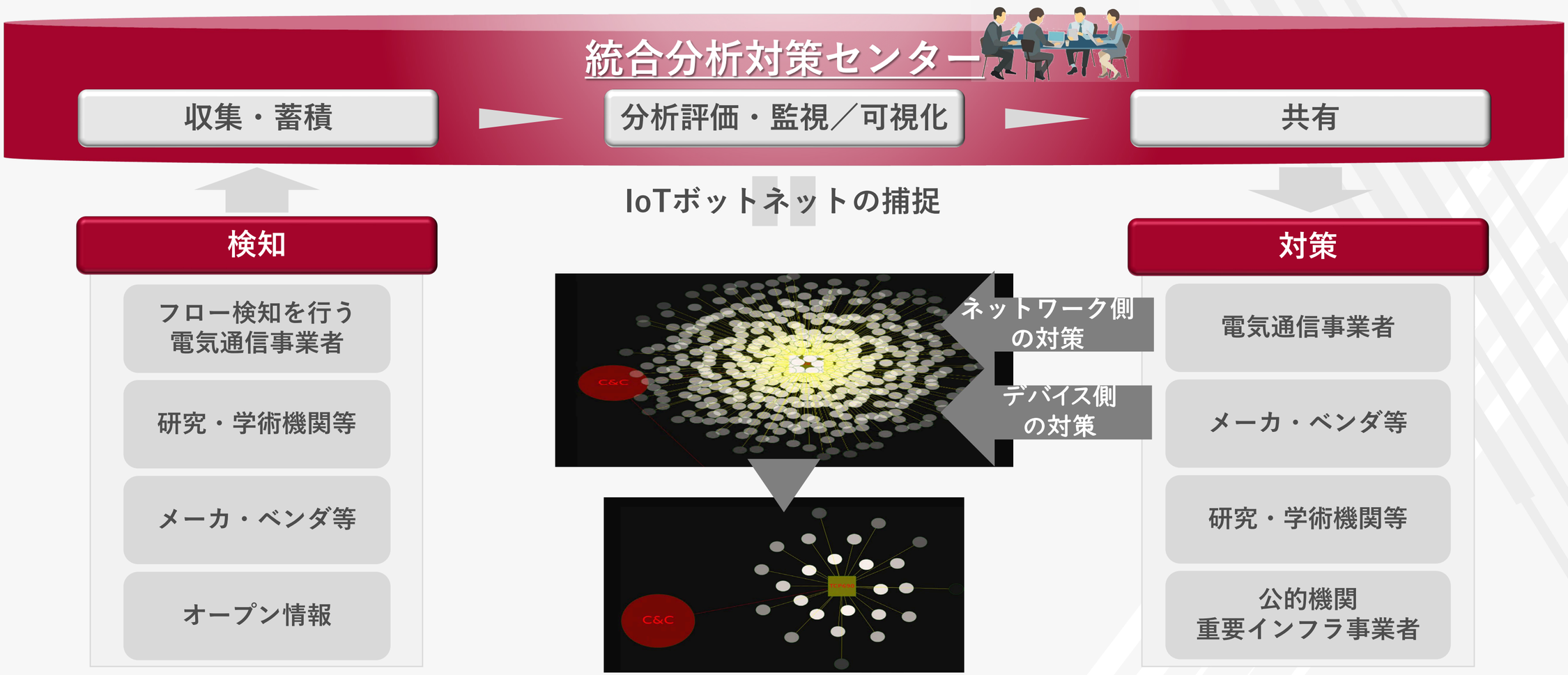
事業者連携における検討の開始

ICT-ISAC会員電気通信事業者13社と共に今後のC&Cサーバリストの共有の在り方やC&Cサーバ検知手法の在り方について議論、今後整理すべき事項について確認できた。

	今回に向けた改善事項		今後の取り組み
検知・評価	信頼性向上	・各社ごと検知手法の改善等による検知精度の向上が必要。 ・評価作業で参照するソース情報の拡充等により、C&Cサーバリストの評価精度を高める必要性がある。	・フロー情報分析によるC&Cサーバ検知手法の改良やチューニング ・関係機関との連携(NICTER等)によるソース情報の拡充等
	新鮮度向上	・検知～評価の一連の作業に時間を要するケースがあり、各種自動化等を通じた新鮮度の維持に向けた取り組みが必要。 ・検知されたIPの実際の活動動向をより正確・詳細に捕捉していくことが必要。	・各種自動化等を通じた検知～評価の一連の作業時間の短縮 ・能動的な観測手法の追加等、継続的なC&Cサーバの観測機能の強化
共有	リスト共有の仕組みの確立	・関係各社の負担軽減等を考慮しながら、円滑かつ迅速なＣ＆Ｃサーバリスト共有の仕組みの確立が必要。 ・Ｃ＆Ｃサーバリストの共有先についても整理が必要。	・円滑かつ迅速なＣ＆Ｃサーバリストの共有の仕組みの検討と試行 ・C&Cサーバ共有先に関する整理
対策	分析技術の展開	・検知手法に対する各社のノウハウ等を考慮しながらも、多様な電気通信事業者がC&Cサーバ検知ができるようにする為、技術手法の共有に係る検討が必要	・想定利用者と利用者に合わせた技術展開方法の整理
	ユースケースに合わせた利活用方法の整理	・共有されたC&Cサーバリストを法令を順守しながら、実際どのような場面でどのように利活用できるか整理が必要。	・想定利用者と利用者ごとの利活用方法の整理

今回の取り組みのまとめ【２】　（将来的な構想）

フロー情報分析によるC&Cサーバ検知情報等を収集・蓄積・分析評価・可視化・共有等を行うハブ機能を実現し、電気通信事業者等と連携を図りながら、IoTボットネットに対するネットワーク／デバイス双方からの効果的な対策を目指す。



ご静聴ありがとうございました