資料７－４

ICTサイバーセキュリティ政策分科会　御中

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5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サーバ検知及び共有に関する調査の請負」に係るご報告～

2024年5月10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

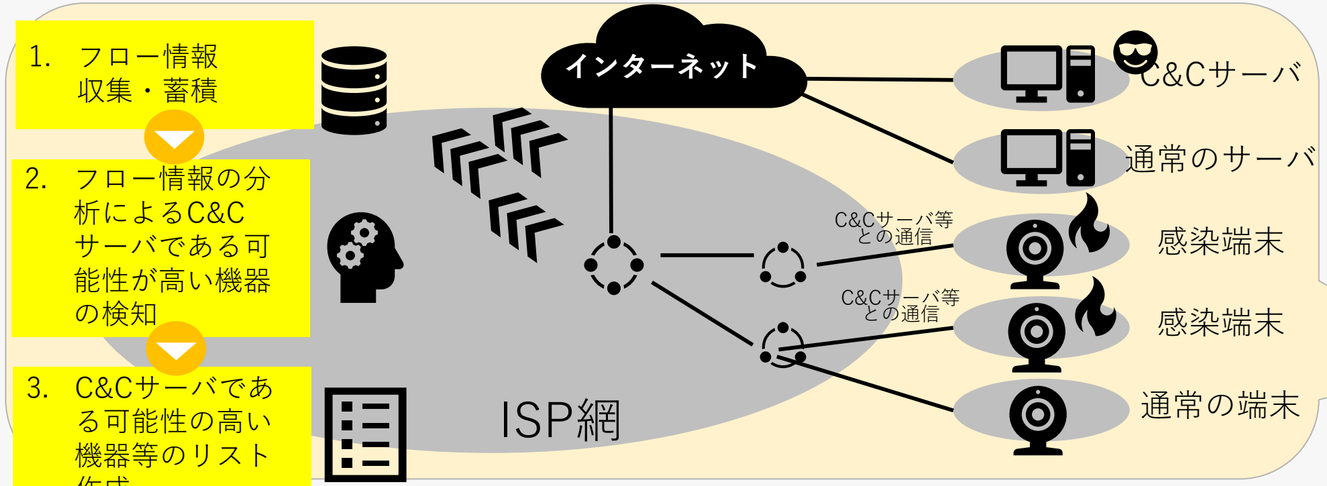
＊総務省.「電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会」.「第四次とりまとめの概要」. 5 頁. 2021. https://www.soumu.go.jp/main_content/000779408.pdf （参照：2023年4月11日）

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。

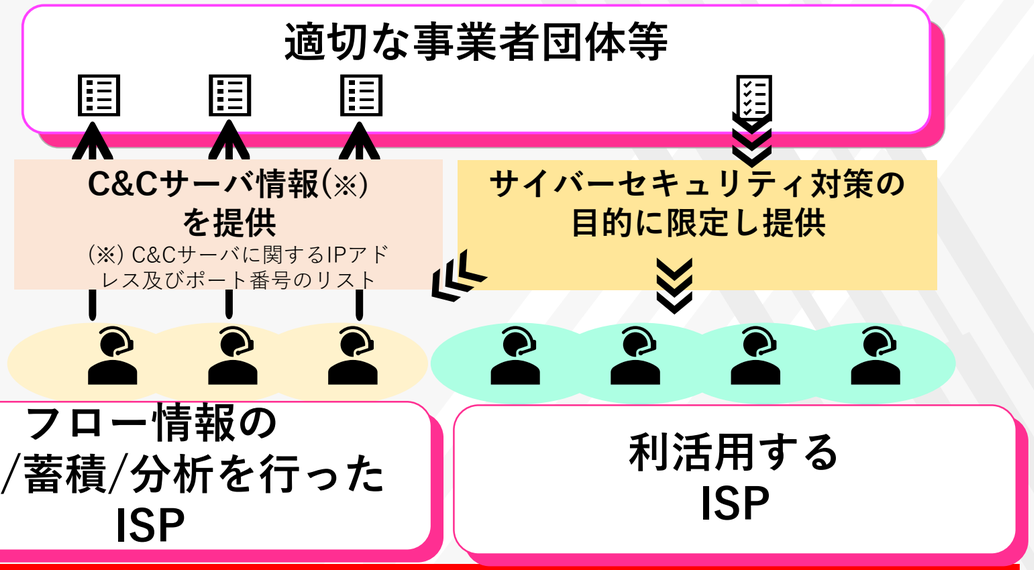
② C&Cサーバに関する情報(IPアドレス、ポート番号)を、サイバーセキュリティ対策のために適切な事業者団体等に提供すること。

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

1. フロー情報収集・蓄積
2. フロー情報の分析によるC&Cサーバである可能性が高い機器の検知
3. C&Cサーバである可能性の高い機器等のリスト作成



② 検知したC&Cサーバに関する情報についての共有

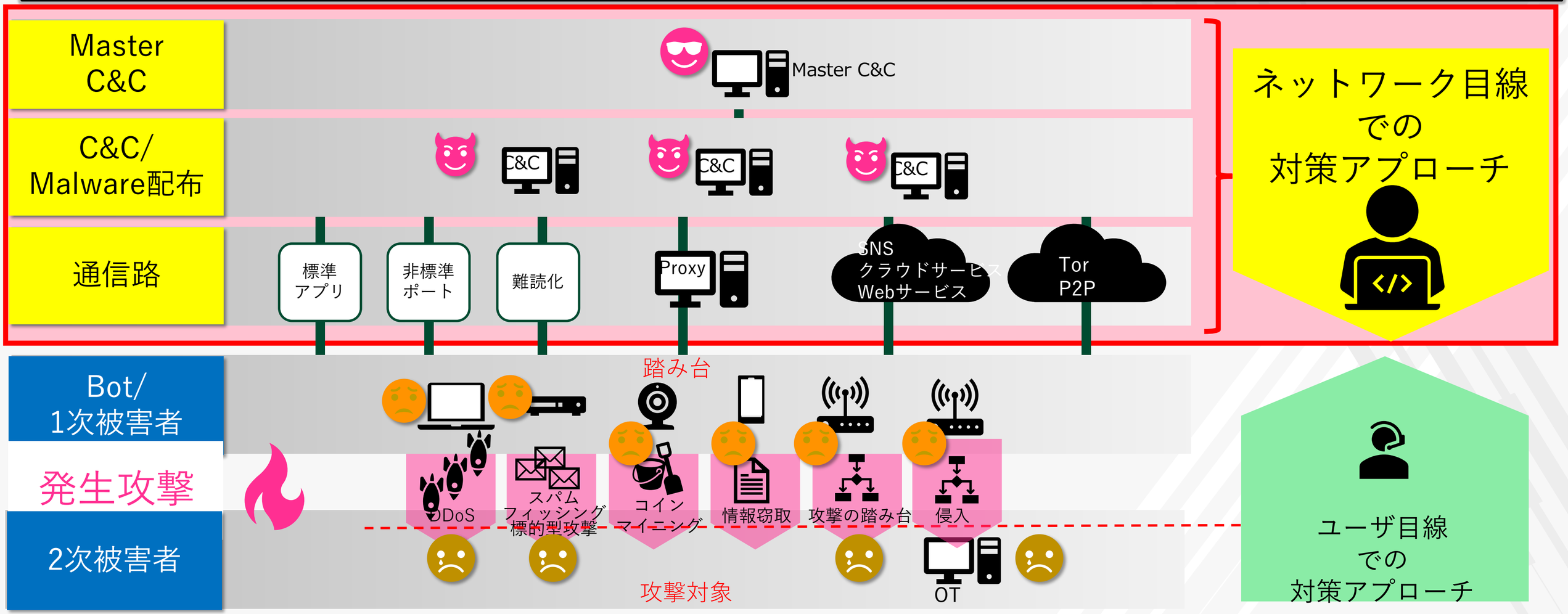


我が国の情報通信ネットワーク上で活動する「実際の」C&Cサーバを把握／連携による対処が可能となる。

→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。

Botnet/C&C通信の構造と本施策のアプローチ

大規模なネットワーク目線での包括的な対策の実現を目指す



本調査の概要

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

検知

- 検知手法の開発・最適化
- 自社のフロー情報を分析することでC&Cサーバ検出

評価・分析

- C&Cリストの精査、深堀分析
- 各実証実験の詳細分析

利活用

- C&Cサーバリスト利活用に向けた議論
- 共有トライアルによるC&Cサーバリストを用いて自社のフロー 情報との照合

国内通信事業者

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

3 事業者

適切な事業者団体

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

C&Cリスト利活用共有WG

ICT-ISAC会員電気通信事業者

１３ 事業者を含む

C&Cリスト生成全体の流れ

C&Cサーバリスト生成の処理概要

フロー分析事業者

分析センター

フロー分析による検出

機械学習（教師あり・教師なし）

グラフマイニング

学習シード情報
- OSINT情報
- 他PJ情報
- 攻撃情報
- ハニーポット情報

•被疑C&Cリスト生成

C&C（過検知）

Level1リスト

バリデーション

OSINT情報分析

自動Validation

•機械的自動分析
C&C種別推定

Level2リスト

追加フロー解析

アナリスト分析

•過検知の除外

Level3リスト

能動的分析

疑似ボット分析

•C&Cの正確な判定.誤検知、過検知排除
•未稼働C&Cを除外

Level4リスト

エンリッチメント

PassiveDNS分析

攻撃情報相関分析

リスク評価

ラベリング

•DNS情報、リスク情報、関連攻撃情報を付与

対策に資するC&Cサーバリスト

C&Cサーバリストレベル定義

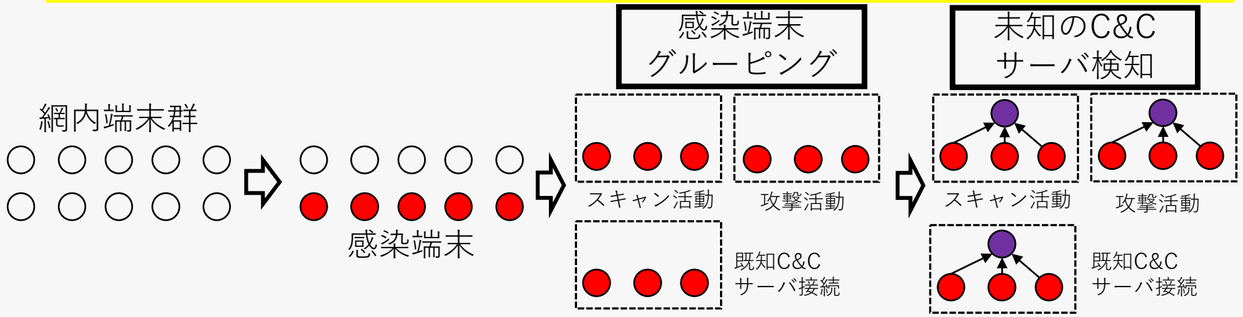
- C&Cサーバリストは感染端末からのアクセスの検知や遮断やインシデント対応時のインテリジェンスとして活用されるほか、研究開発のためのデータセットとしての利活用が想定される。
- 各用途への活用を合理的に実現するためにC＆Cリストを４段階のレベルに分類しその技術的な判定条件をまとめる

Level	各レベル説明			技術的評価内容						信頼度(Confidence Level) 0-100	更新頻度（案）	リスト内容（案）
				インテリジェンス分析による判定				能動的分析による判定				
	概要	過検知の有無	C&C稼働状態判定精度	C&C判定	稼働状況確認	脅威情報	共用IPアドレス判定	C&C判定	稼働状況確認			
Level 4	能動的分析まで実施した過検知、誤検知のないC&Cサーバリスト	無	高	○ 種別判定あり	○	○	○	○ 種別判定あり	○	100	24h	• IPアドレス • ポート番号 • (国) • (AS) • (C&Cドメイン名) • (C&C種別) • (発生攻撃情報)
Level 3	受動的分析を実施したC&Cサーバリスト	若干含む 過去の悪性情報を含むため	中	○ 種別判定あり	○	○	×	×	×	75	24h	• IPアドレス • ポート番号 • (国) • (AS) • (C&Cドメイン名) • (C&C種別) • (発生攻撃情報)
Level 2	機械学習結果に簡易な悪性判定を実施した脅威インテリジェンス	含む 過去の悪性情報を含むため	低	△ 種別判定なし	×	△	×	×	×	50	24h	• IPアドレス • ポート番号
Level 1	機械学習による検出結果	含む	低	×	×	×	×	×	×	30	24h	• IPアドレス • ポート番号

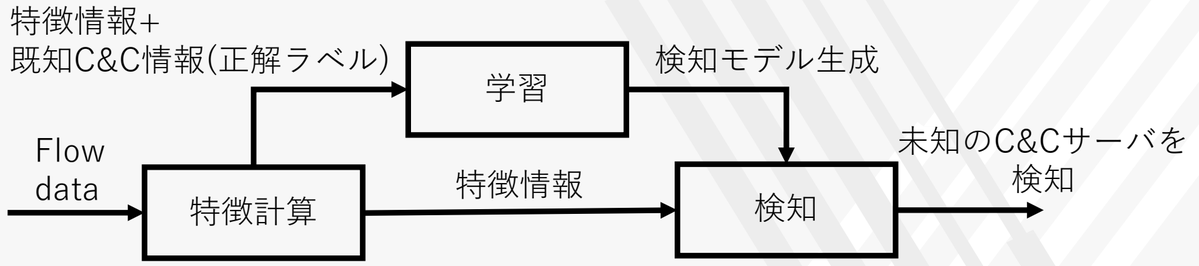
フロー分析について

- **複数の通信事業者レベルのフロー情報を活用することによる国内大規模トラフィック解析への複数の教師あり/教師なし機械学習、グラフマイニング手法を適用**
- **継続的機能開発、共通シード情報を用いた分析**

グラフマイニング
国内ISP等が平時から通信傾向把握等のために収集・蓄積しているフロー情報等より検知した感染端末の通信先から　未知のC&Cサーバを検知する手法



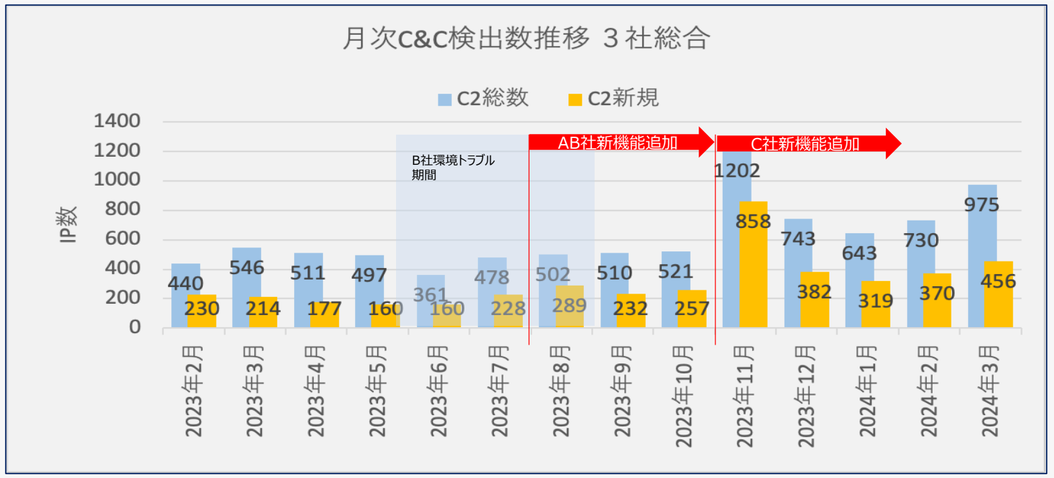
機械学習
既知C&Cサーバの特徴情報を教師データとする機械学習よりC&Cサーバの検知モデルを生成し、当該フロー情報から未知のC&Cサーバを検知する手法

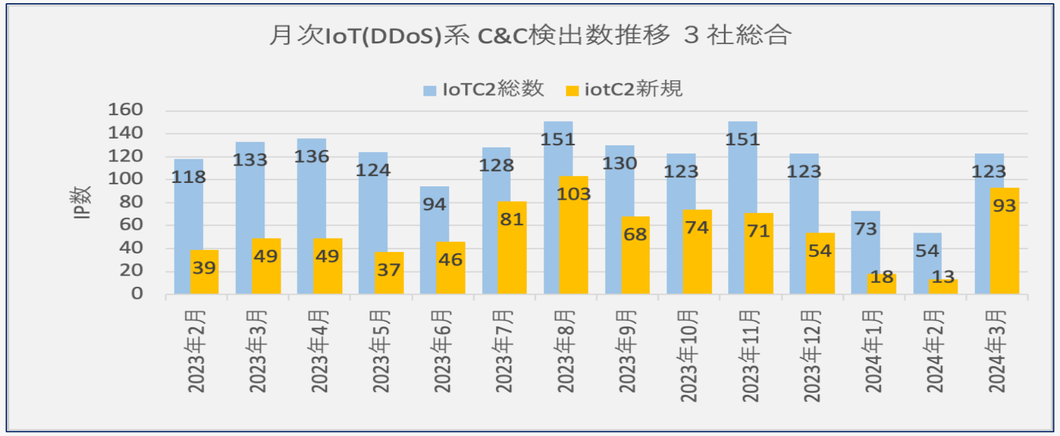


検出状況

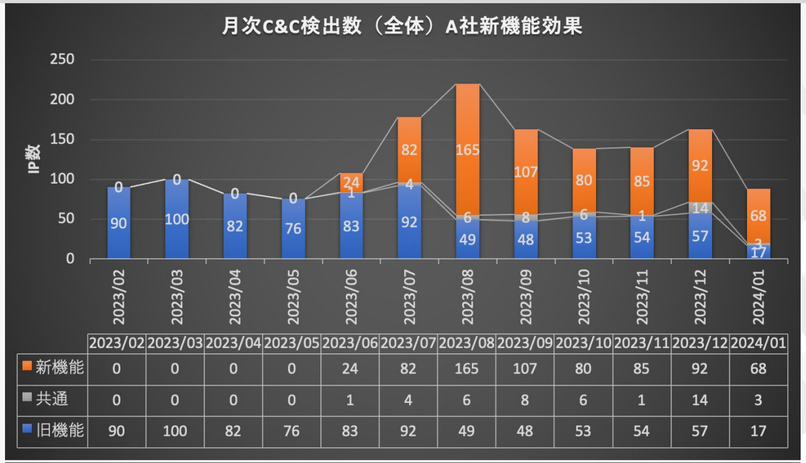
- フロー分析３事業者において機能強化を実施
- 新機能導入効果により大幅に検出力が向上
- 逆に旧機能をそのまま使い続けた場合の検出性能の低下→**継続的な開発・最適化が必要**

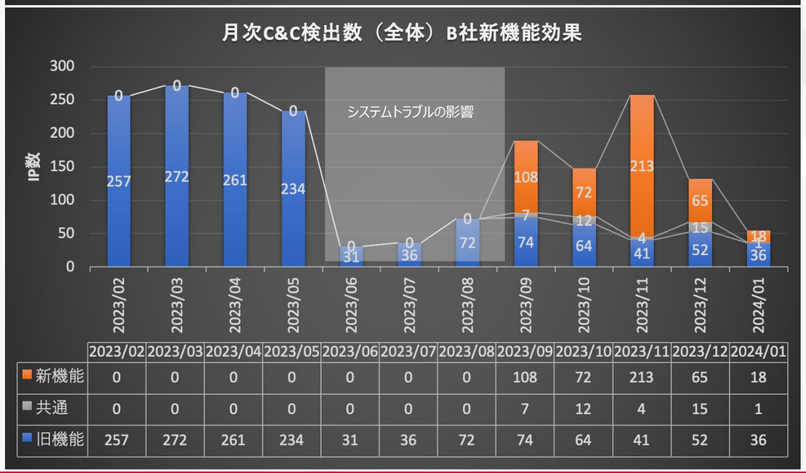
検出状況





新機能開発による性能向上例



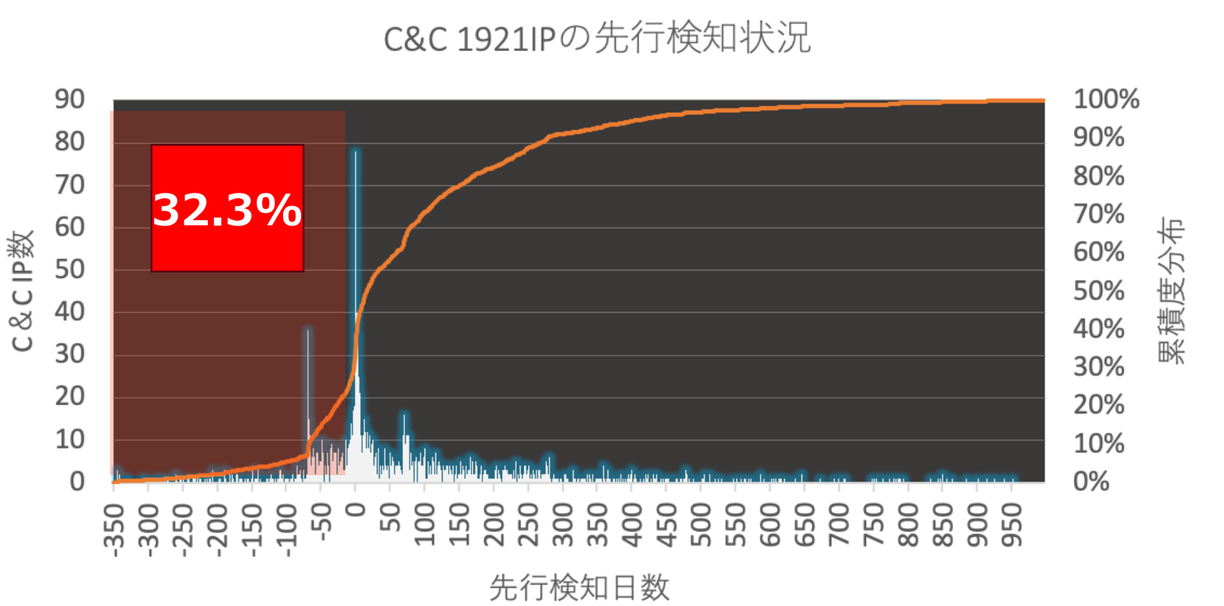


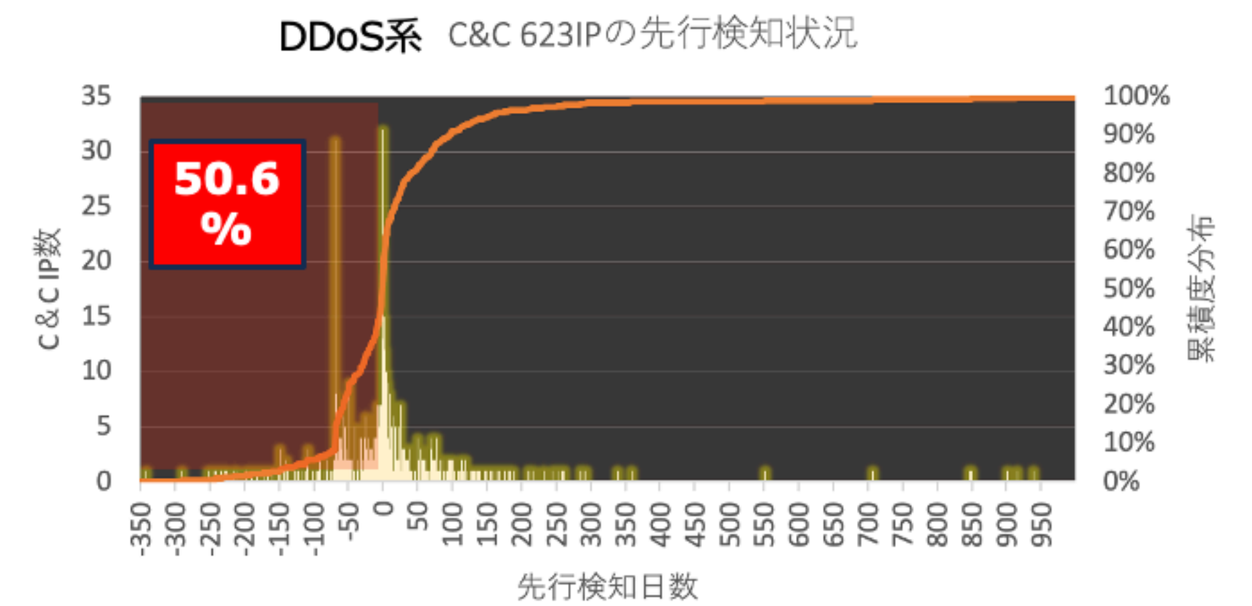
新規機能による検出

従来機能による検出

C&Cサーバ先行検知性

本手法の優位点の一つである**先行検知性**について
複数のOSINT情報に比べ何日先行検知していたかの簡易分析結果





32.3%を先行検知（0日も含めると36.5%）
先行検知平均:-77.8日

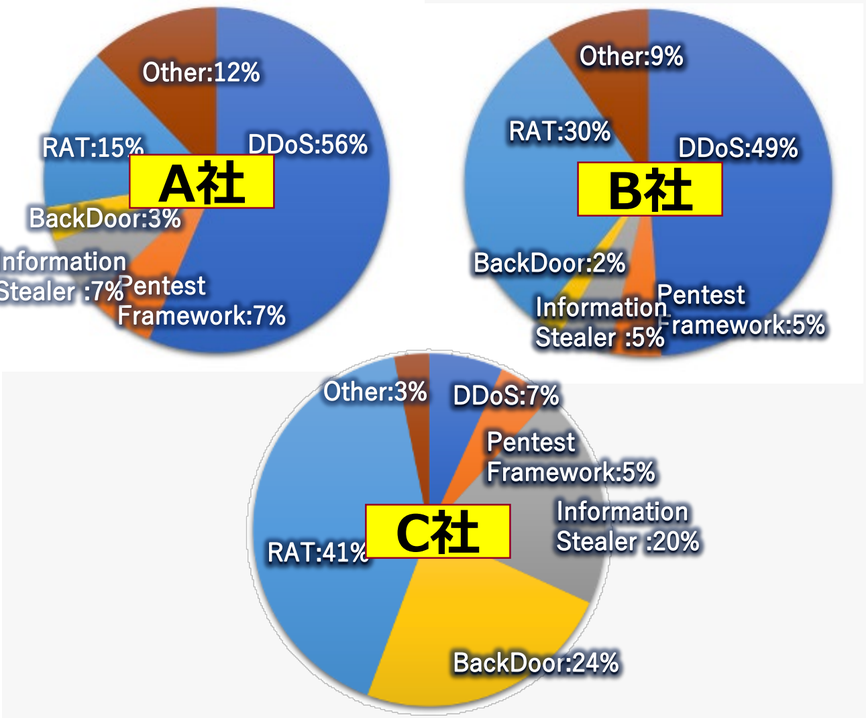
50.6%を先行検知（0日も含めると55.1%）
先行検知平均:-48.2日

「今みれば先行検知していた」という評価は簡単だが
実対策に活用するには未知C&C検出時点での悪性度評価の即時性が課題

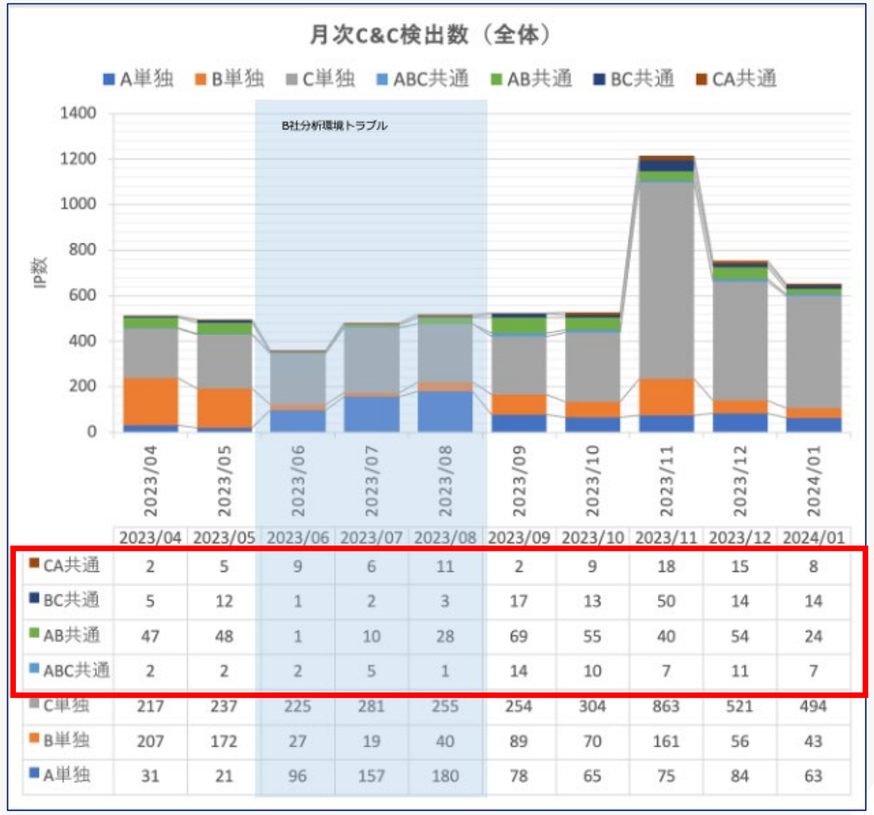
【ネットワーク毎の検出特性の差異】フロー分析事業者毎の差異

- 別機能を用いて分析してるCはC&Cタイプの傾向は大きく異なり、個々のC&Cサーバ検出の共通性も低い
- 同一機能を用いているABは同じ傾向のC&Cタイプを検出しているが、個々のC&Cサーバの検出共通性は～<u>50%程度</u>

検出されるC&C typeに偏りがある ABは似た傾向

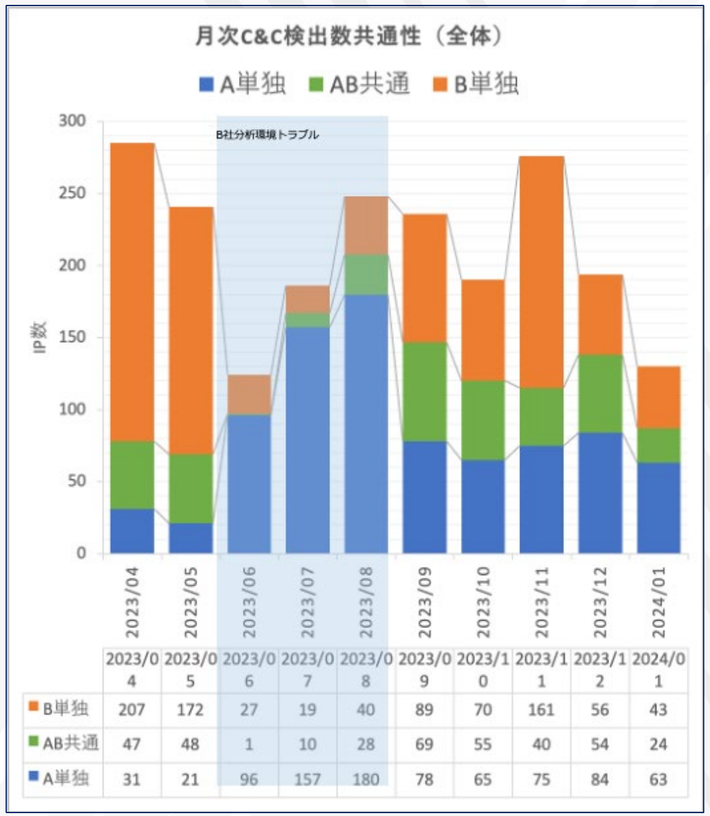


ABCの検出共通性は低い
新機能追加後(11月以降)若干向上



	2023/04	2023/05	2023/06	2023/07	2023/08	2023/09	2023/10	2023/11	2023/12	2024/01
CA共通	2	5	9	6	11	2	9	18	15	8
BC共通	5	12	1	2	3	17	13	50	14	14
AB共通	47	48	1	10	28	69	55	40	54	24
ABC共通	2	2	2	5	1	14	10	7	11	7
C単独	217	237	225	281	255	254	304	863	521	494
B単独	207	172	27	19	40	89	70	161	56	43
A単独	31	21	96	157	180	78	65	75	84	63

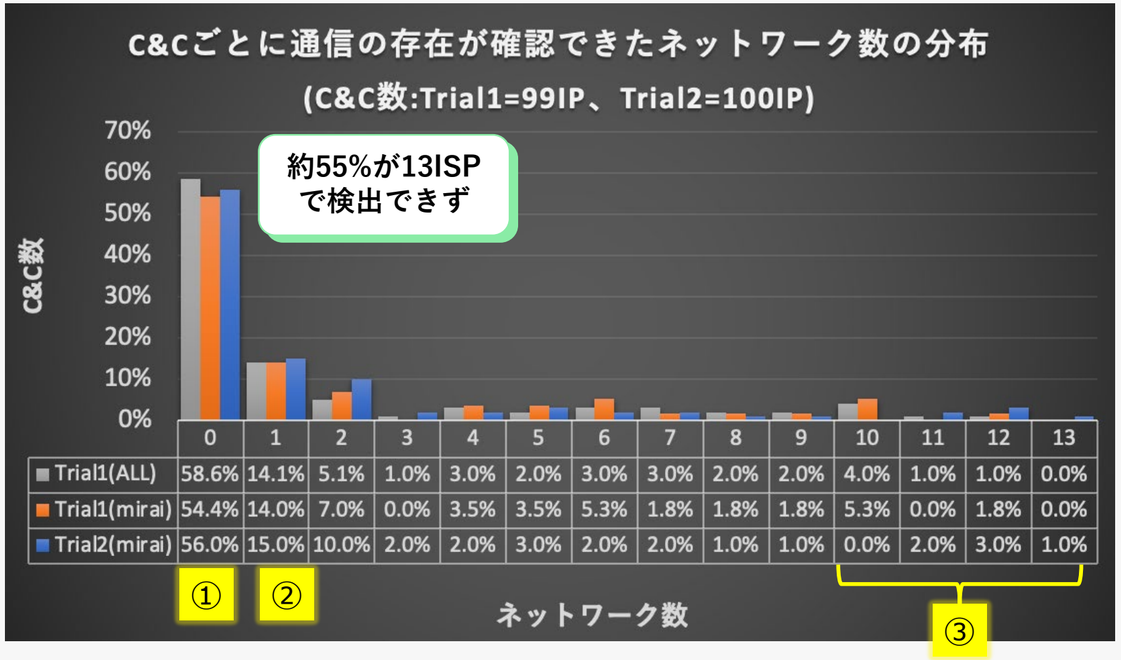
共通機能を用いている ABの共通性50%程度



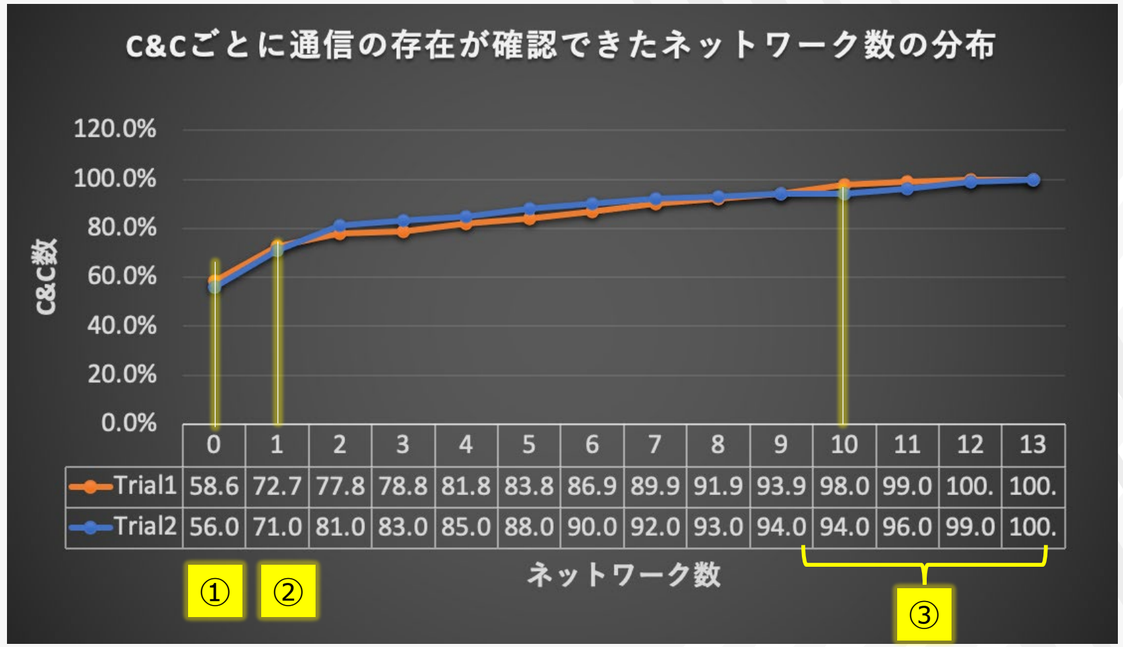
	2023/04	2023/05	2023/06	2023/07	2023/08	2023/09	2023/10	2023/11	2023/12	2024/01
B単独	207	172	27	19	40	89	70	161	56	43
AB共通	47	48	1	10	28	69	55	40	54	24
A単独	31	21	96	157	180	78	65	75	84	63

【ネットワーク毎の検出特性の差異】| 3ISPによる共有トライアル

- １３ISPによるC&Cサーバ通信検出分析（２回実施）
- １，２回目ともに１事業者も検出できなかったC&Cが**約55%**を占める①



	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Trial1(ALL)	58.6%	14.1%	5.1%	1.0%	3.0%	2.0%	3.0%	3.0%	2.0%	2.0%	4.0%	1.0%	1.0%	0.0%
Trial1(mirai)	54.4%	14.0%	7.0%	0.0%	3.5%	3.5%	5.3%	1.8%	1.8%	1.8%	5.3%	0.0%	1.8%	0.0%
Trial2(mirai)	56.0%	15.0%	10.0%	2.0%	2.0%	3.0%	2.0%	2.0%	1.0%	1.0%	0.0%	2.0%	3.0%	1.0%



	0	1	2	3	4	5	6	7	8	9	10	11	12	13
Trial1	58.6	72.7	77.8	78.8	81.8	83.8	86.9	89.9	91.9	93.9	98.0	99.0	100.	100.
Trial2	56.0	71.0	81.0	83.0	85.0	88.0	90.0	92.0	93.0	94.0	94.0	96.0	99.0	100.

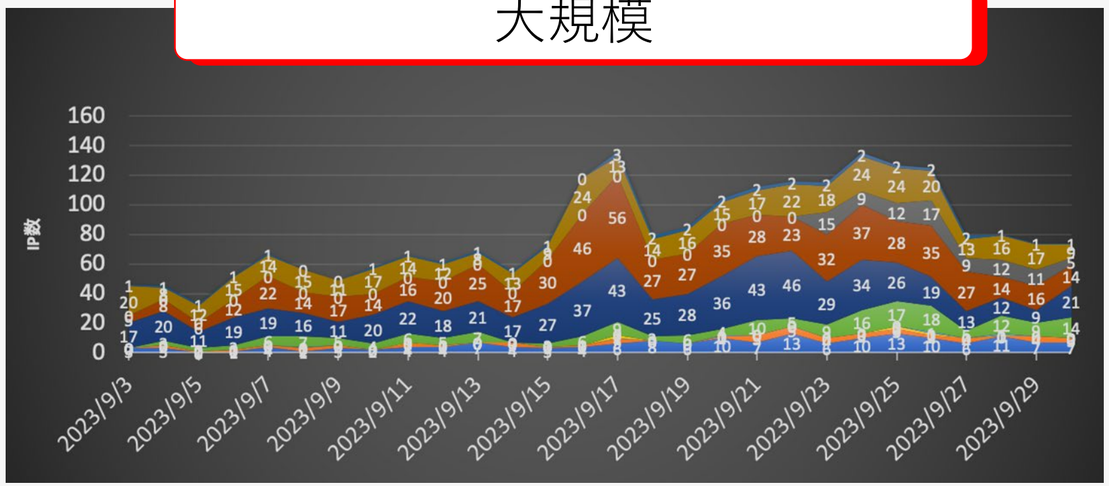
全体の約**15%(検出できたC&Cの約30%)**が**1社でのみ検出②**

10社以上で検出されるものは**全体の5%程度（検出できたC&Cの13%）③**

【ネットワーク毎の検出特性の差異】| 3ISPによる共有トライアル

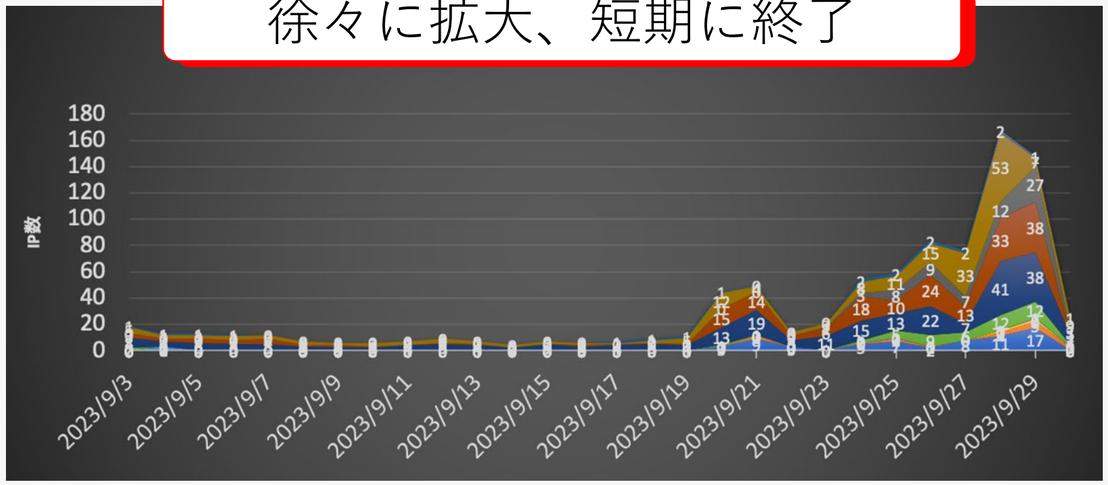
- C&C通信の分析例

大規模

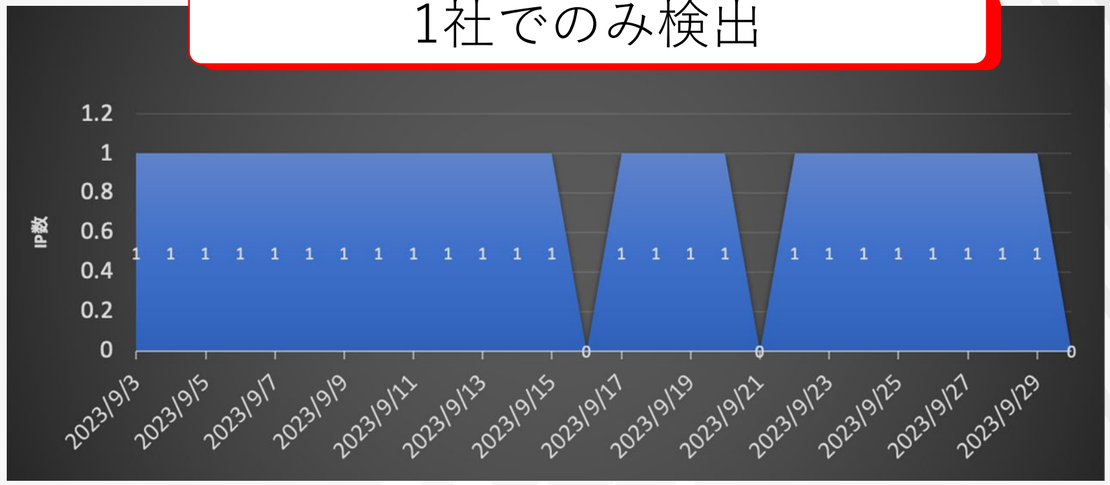


2社でのみ検出

徐々に拡大、短期に終了



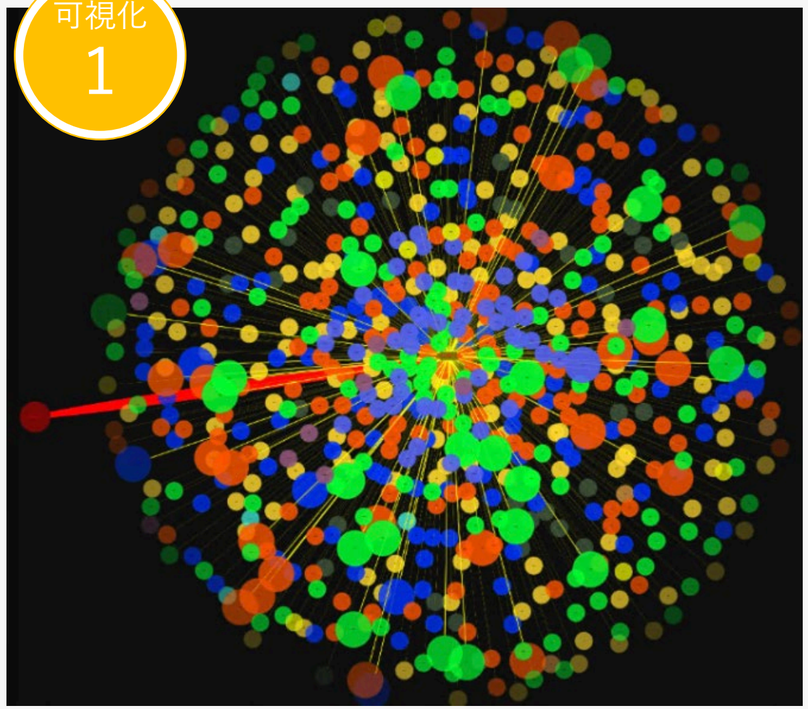
1社でのみ検出



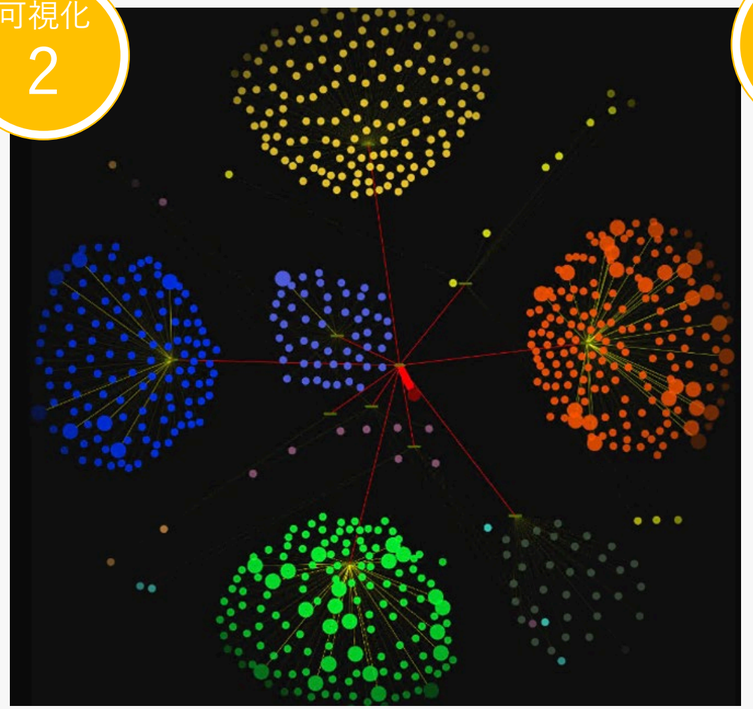
【ネットワーク毎の検出特性の差異】| 3ISPによる共有トライアル

- リスク評価のための可視化試行例

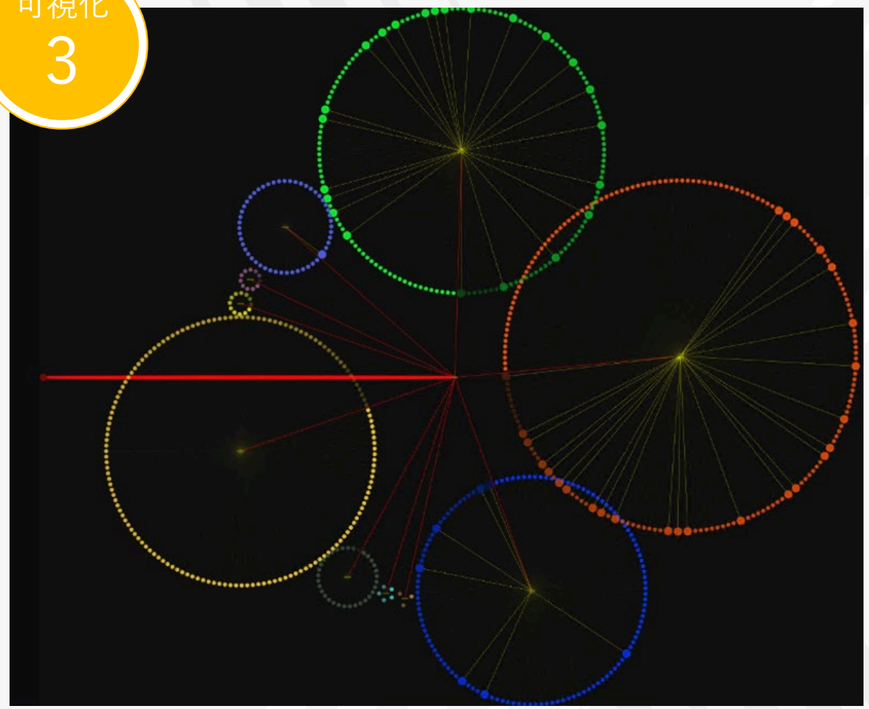
可視化 1



可視化 2



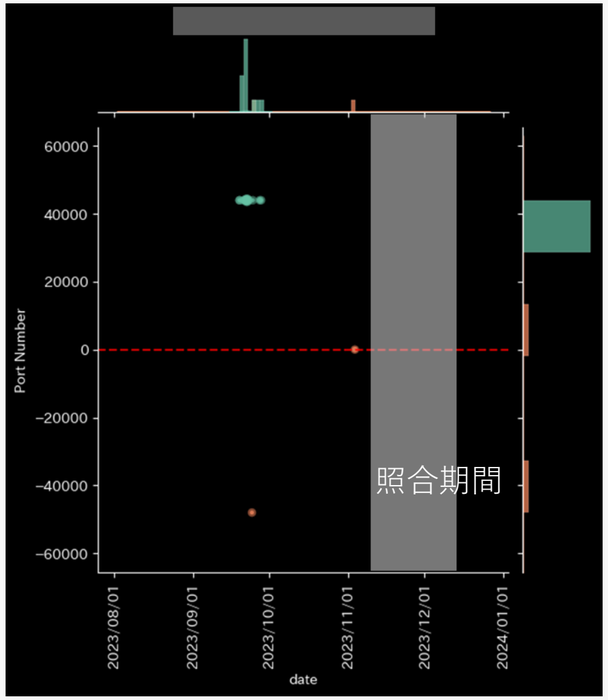
可視化 3



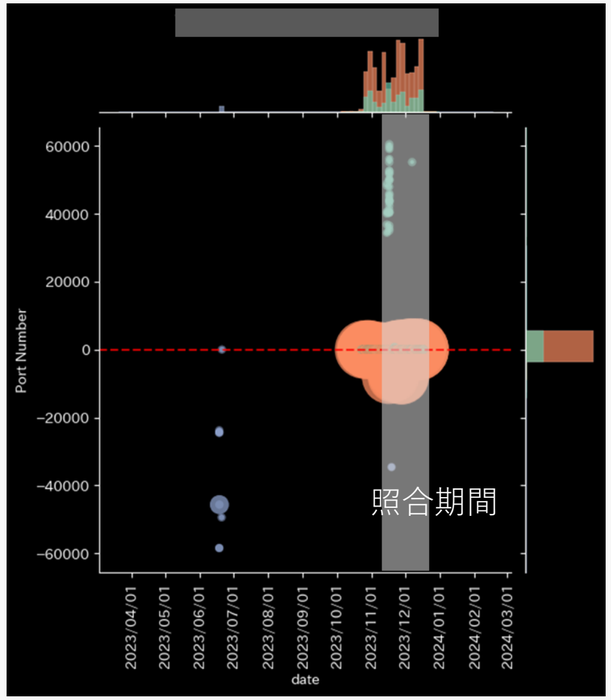
【ネットワーク毎の検出特性の差異】| 3ISPによる共有トライアル

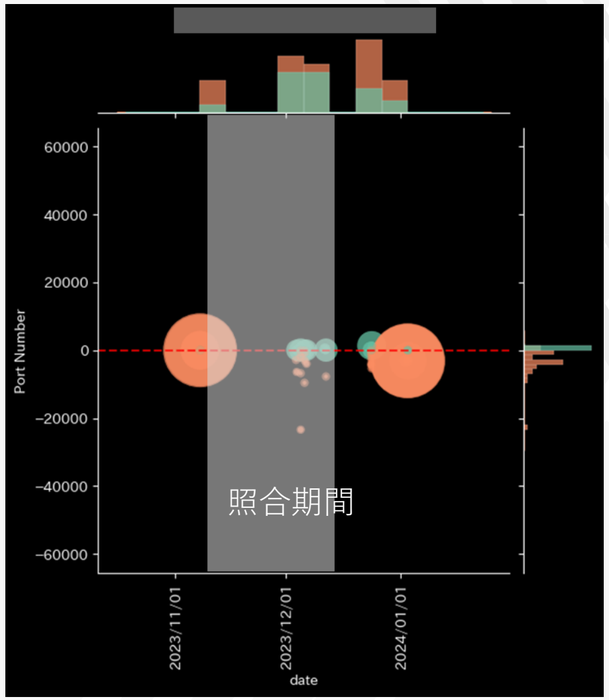
- ◆ **１事業者でも検出できなかった原因**は、**検出から共有トライアルまでに時間が長すぎ、フロー照合時にはC&Cサーバの機能が停止、変化している**
- ◆ ボットネットとして完全終了したもの、ボットネットとしては別のC&Cで稼働しつづけている、ロール変更されただけで攻撃インフラとしては活動し続けている

照合前に活動終了



照合時にはロール変更（C&Cではなくなっている）





【ネットワーク毎の検出特性の差異】まとめ

事象

- ■ 複数のISPで共通的に検出されるC&C通信
- ■ 少数のISPでしか検出されないC&C通信
- ■ 複数のISPで時期ズレで観測されるC&C通信

技術的要因

- 分析機能の差異の影響
  - 分析アルゴリズム
  - 分析シードの差異
- サンプリングレートが低く検出漏れしている
- C&Cの生存期間が短くリスト生成から照合までに活動停止してしまう

攻撃の性質・環境的要因

- IPアドレスやユーザー特性の差異の影響
  - 特定の組織をターゲットとする攻撃
  - 特定のIPアドレスレンジを対象とする攻撃
  - 特定のドメインを対象とする攻撃
  - 特定の機器の脆弱性を狙う攻撃
    通信事業者毎のユーザが利用する機器の偏り

検出特性の活用方法

リスク評価	複数のISPで共通的に検出されるC&C	• 大規模ボットネットとしてリスク判定する要素として活用
	特定のISPでしか検出されないC&C	• 特定ネットワーク特異事象 • 拡散前の先行検出情報として情報展開
分析技術の強化	• 複数フロー分析事業者への共通技術の展開による監視の網を展開 • 分析機能、学習用シード情報をチューニングすることで特定のC&C（攻撃）を狙い撃ちで検出する	

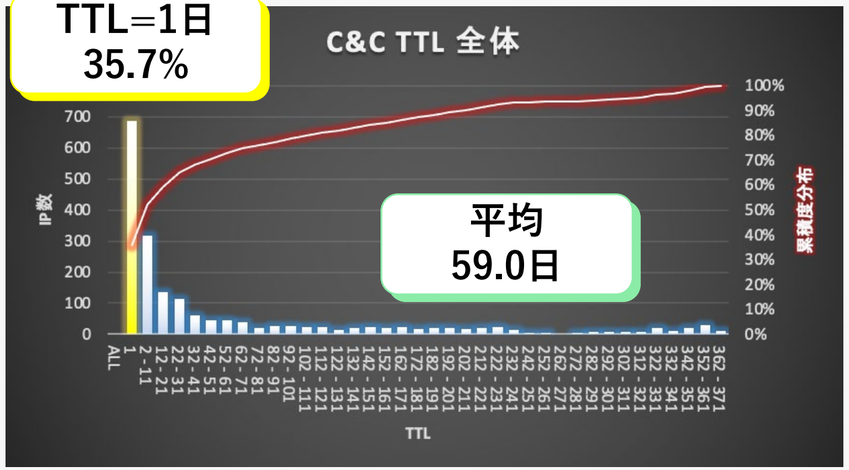
【C&C特性分析】C&Cサーバ生存期間

- **C&Cサーバの生存期間（活動期間）**は対策効果の最大化のためにもとめられる対策即時性を実現するための重要な要素であるためR4年度に引き続き詳細な分析を実施

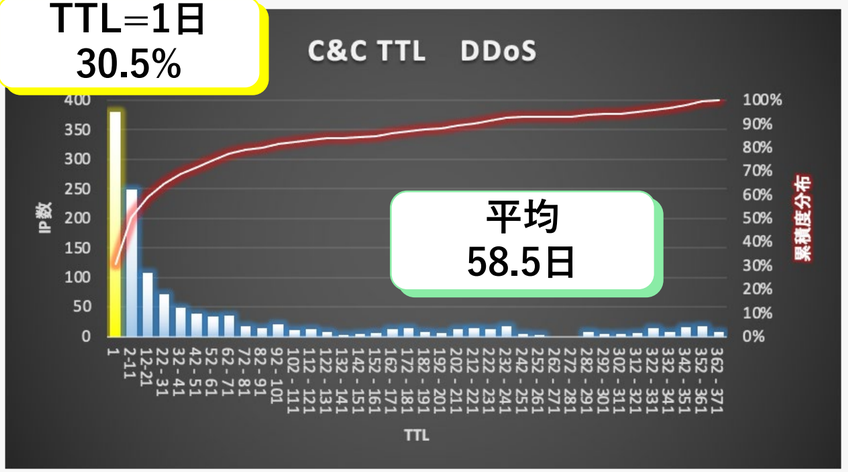
受動的分析（精度低）

- フロー分析でのC&C検出状況/C&C向けフロー情報の有無による判断
- OSINT情報に基づく判断

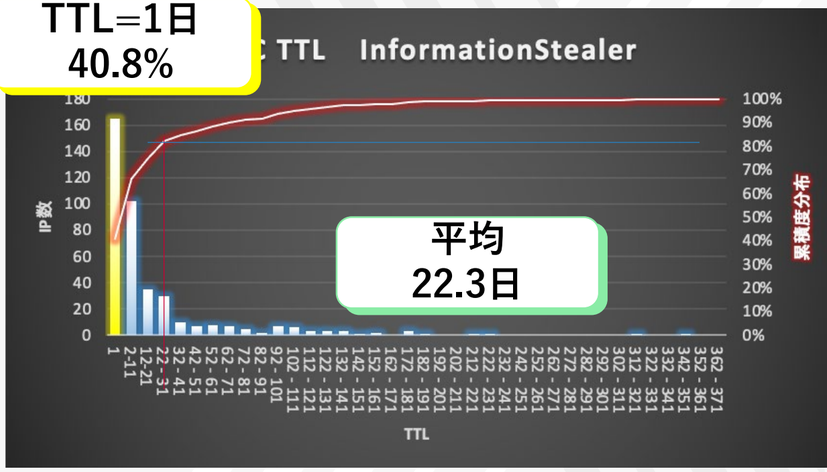
TTL=1日
35.7%



TTL=1日
30.5%



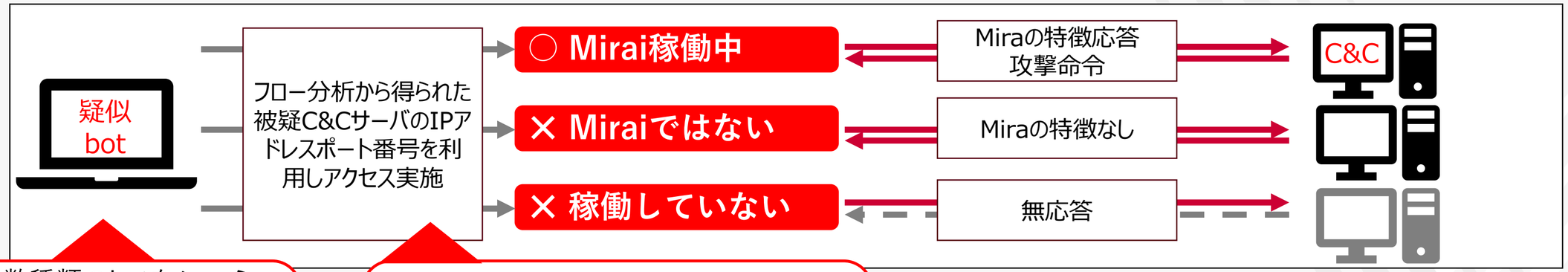
TTL=1日
40.8%



- **TTL１日のものが30%程度、平均58日程度**

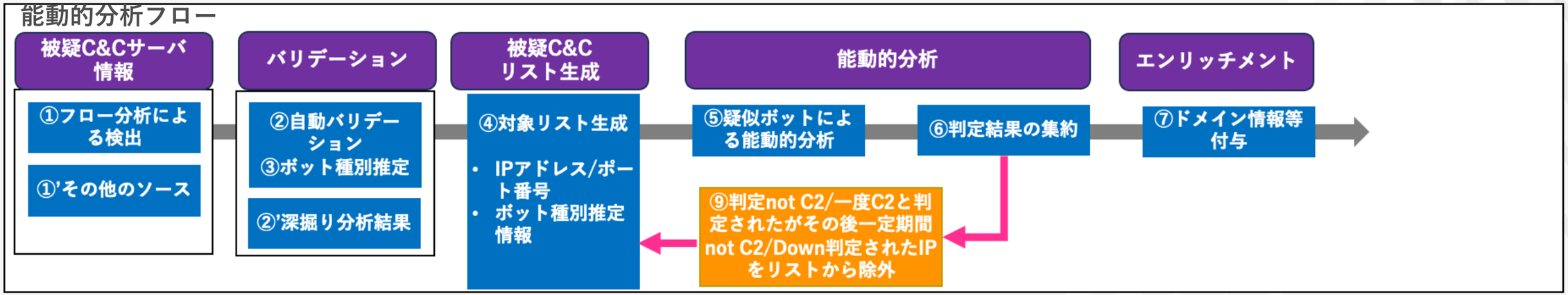
能動的分析機能

•Botの挙動を模倣する「**疑似bot**」を用いて分析対象のC&Cに直接接続しその応答を分析し以下の判定を行う
- **•精度高いC&C判定**
- **•活動中か機能停止しているかの確認とC&C生存期間の確認**



miraiを中心に十数種類のbotをシュミレーション可能。
能動的分析結果等から随時シミュレーション機能を追加する継続的開発サイクルを実施

バリデーションにてボット種別判定を実施しシミュレータ選択をしている
今後は種別判定をせず分析実施予定

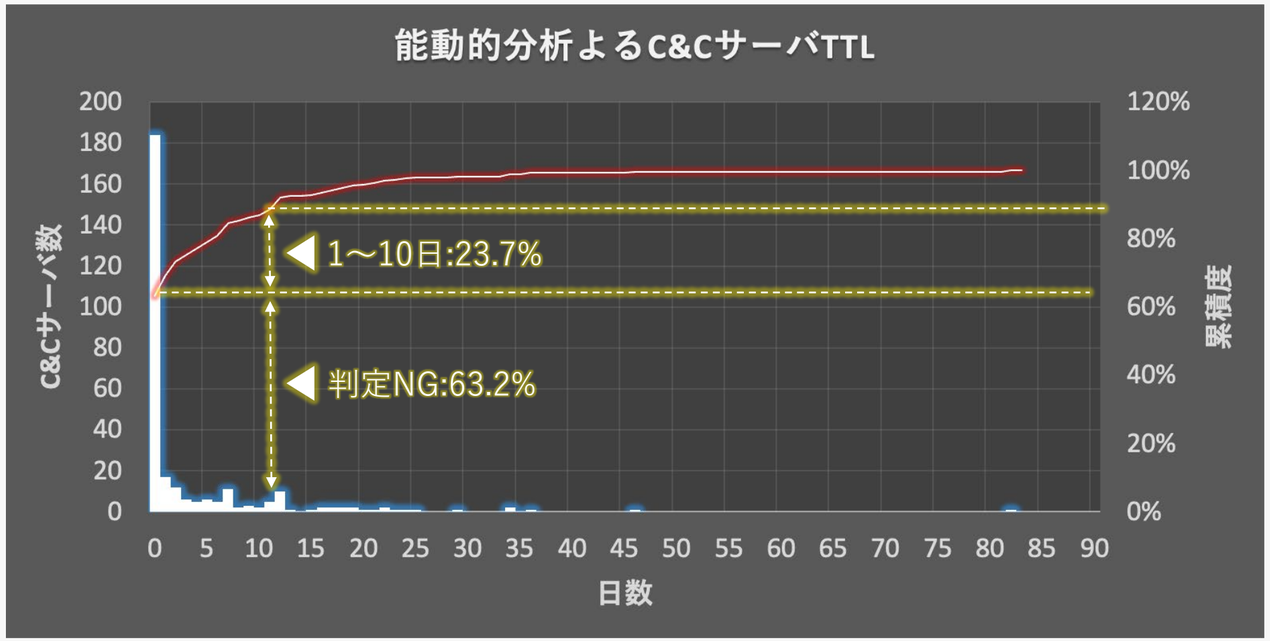


【C&C特性分析】C&Cサーバ生存期間

R5年度は試行的に能動的分析機能を導入し高精度の判定を実施。ボットシミュレーションにより被疑C&Cサーバにアクセスし C&Cサーバであることの判定、活動状態の確認を実施

能動的分析（精度高）

C&Cサーバに直接接続してC&C判定、稼働状態確認

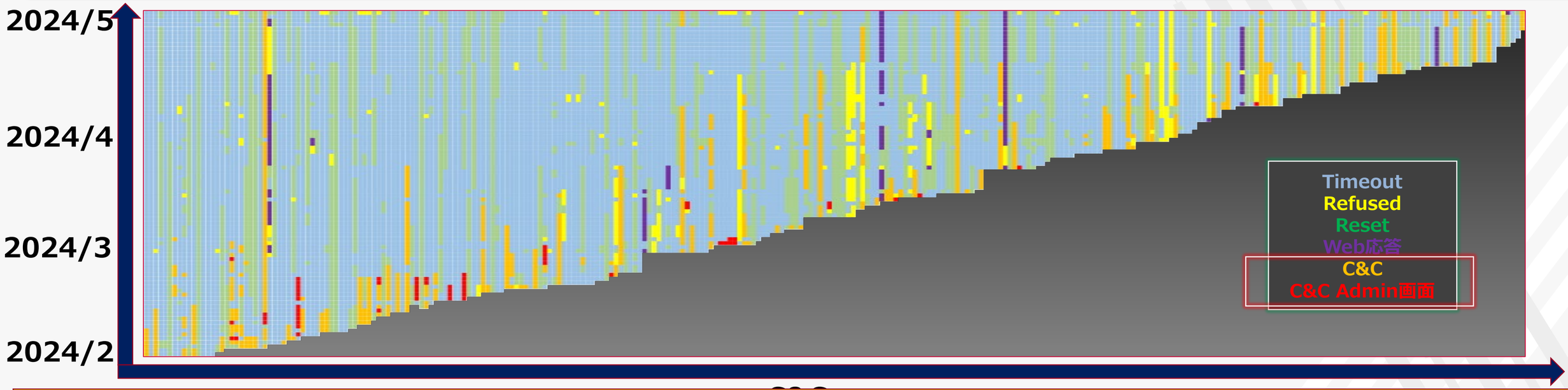


総数

分析期間：	**87日**
分析総数：	**291IP**
C2判定総数：	**107IP**
C&C管理画面検出：	**20IP**
C&C判定率：	**36.8%**
C&C判定NG率:	**63.2%**
生存期間最長：	**82日**（断続的）
生存期間平均：	**9.7日**
検出1～10日：	**23.7%**

【C&C特性分析】C&Cサーバ生存期間

日次での応答変化の分析
初期のみC&C判定、継続的にC&C判定されるもの、断続的、一定の期間を開けて再度C&C判定されるものなどの特徴



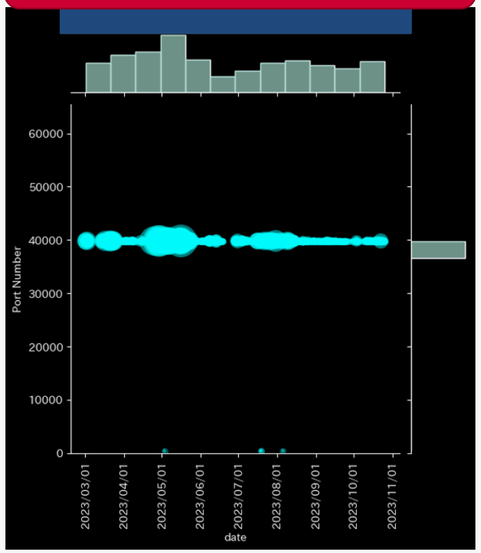
C&C判定されない理由

- シミュレーション対象外
- C&Cサーバとしての機能停止・終了
  - ボットネット自体が完全終了
  - 対象のボットネットは別のC&Cサーバで稼働
    - マルウェア内に設定されているC＆CIPが変更
    - C2ドメインに設定されているAレコードが変更
  - 用途変更（スキャナーやマルウェア配布）
- 通信制御
  - 接続ボット数制限のセッションコントロール
  - 特定の条件（国、AS、IP等）でのアクセス制御
- 通信の問題
  - C&Cサーバのサーバ品質が悪く接続timeoutする
  - C&Cサーバに接続されるボットの数が多すぎでリソース不足になっているため接続不能となる

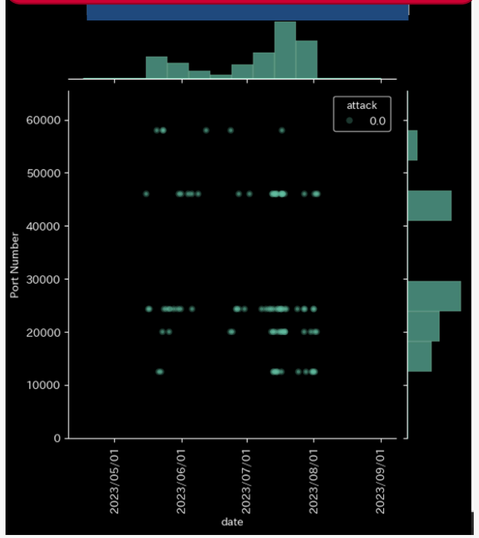
C&Cサーバ挙動分析

C&Cサーバは単一のポート番号で稼働し続けるものもあるが、ポート番号の変化、複数のポート番号で稼働したり、C&C以外の機能をもつものなど状態が変化するものも多い。これらの挙動変化は対策へ影響を与える。

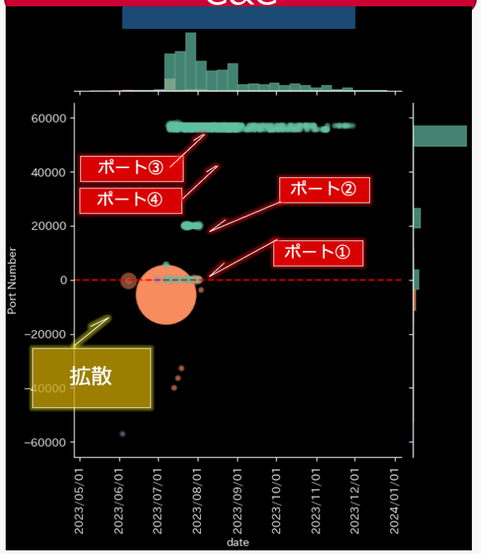
単一ポート番号で活動するC&C



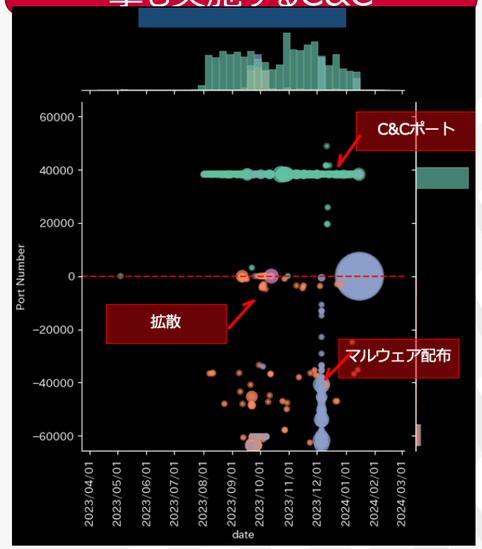
複数ポート番号で活動するC&C



ポート番号が変化するC&C



C&Cサーバ機能だけではなく攻撃も実施するC&C



【 C&C検出結果と実事例の関係】事例1:InfectedSlurs

- C&C検出結果と実攻撃事例との相関分析事例についての分析結果。
- 2023/12に報告されたInfectedSlursの例。主に日本国内でのみ利用されている機器も攻撃対象となってるのが特徴

InfectedSlursについて

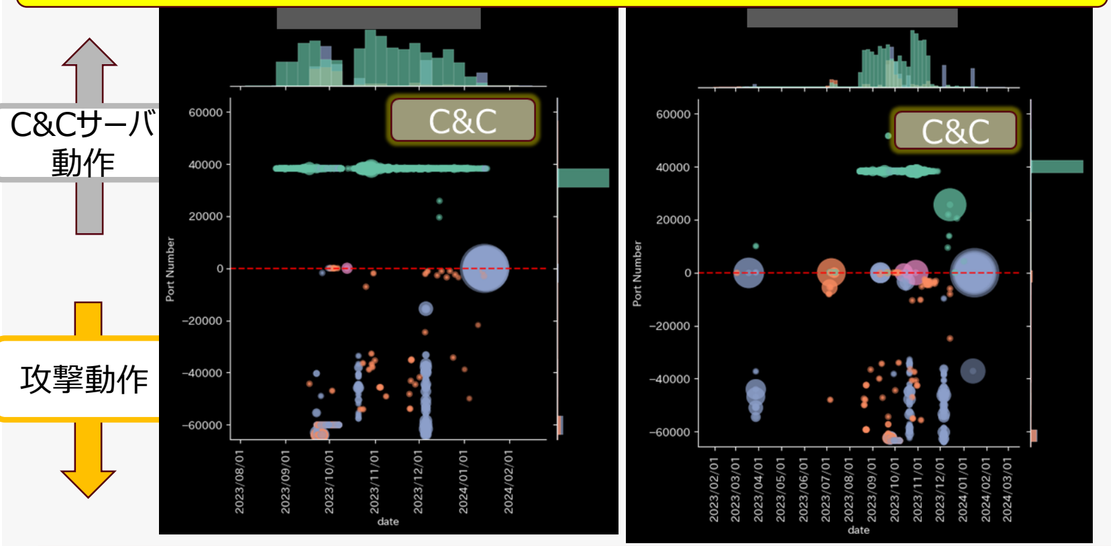
項目	説明
名前	InfectedSlurs
系譜	Miraiベース
感染方法	• デフォルトクレデンシャル利用 • CVE-2023-49897 • CVE-2023-47565
目的	DDoS
活動期間	2022年後半を起源とするが2023/10下旬から活動

C２PJによる公開されたIoC情報の検出状況

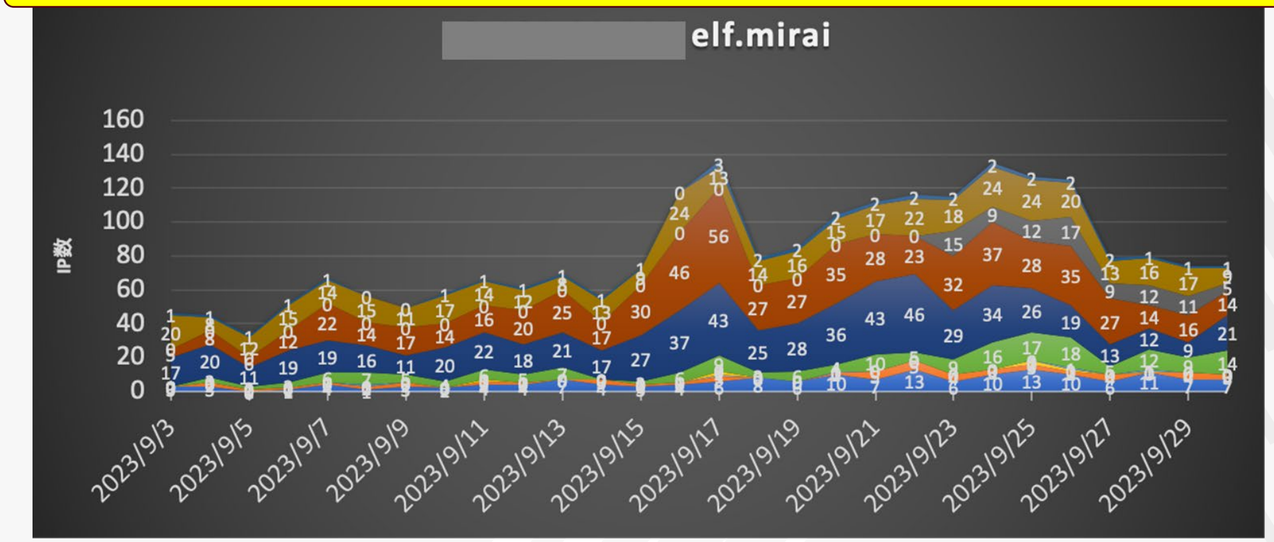
分類	検出数	悪性判定数
全体	75%	40.6%
C&C	100%	55.6%
Proxy	100%	45.5%

フロー分析での検出率は100%だが悪性判定性能に課題がある

C&C挙動分析例



共有トライアルによる分析



分析結果に関するまとめ

フロー分析事業者、共有トライアルを通して大規模なC&C実態調査が実現でき、精度高い検出と判定、そのサーバ単体の挙動解析、可視化が実現できた

今後のC&Cリスト生成

IP＋ポート番号単位でみた場合はバラバラの挙動に見え、生存期間も非常に短いが、ボットネット全体、攻撃キャンペーン全体で見た場合、複数のC&Cが冗長構成で稼働していたり、短期間での使い捨て、変更しているだけでボットネット自体は稼働し続けリスクは低減していない場合が多い

今後は各分析機能強化により**定量的効果確認可能な対策に資するリスト生成**の実現を目指す

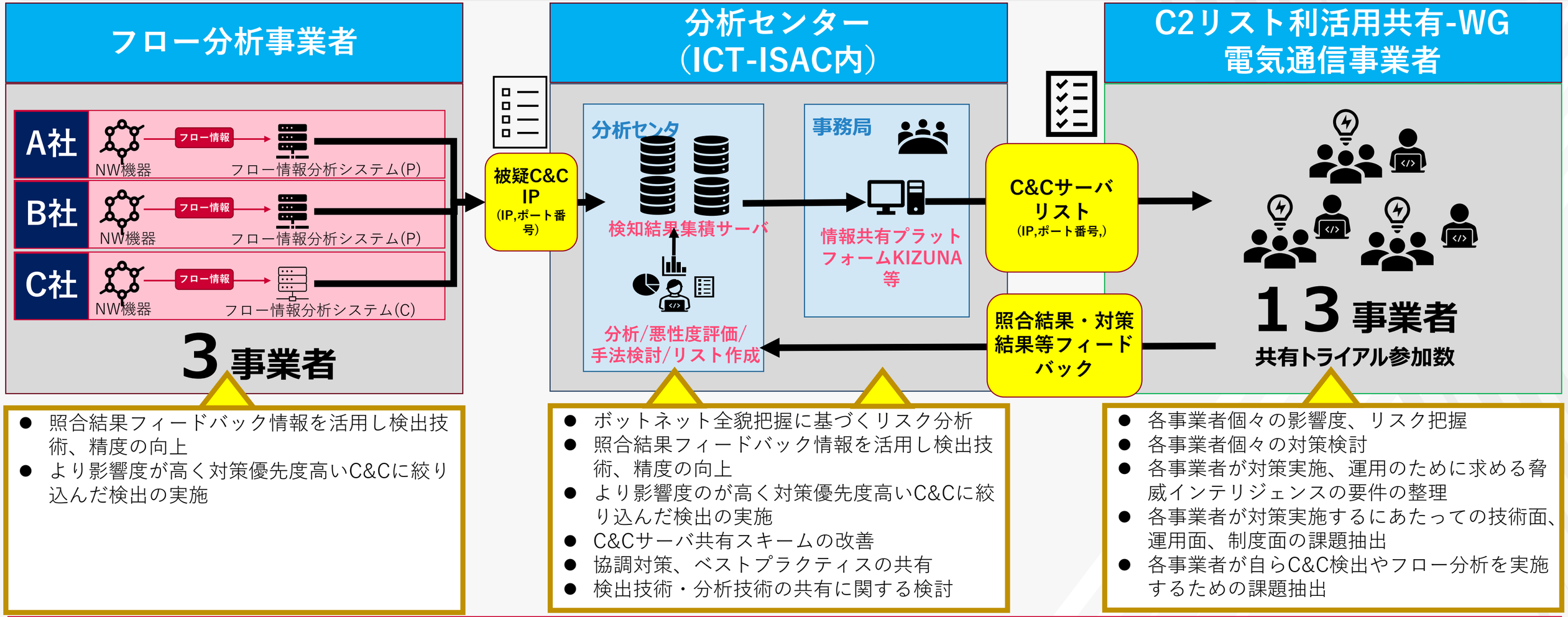
- **能動的分析強化による高精度でタイムリーなリスト生成の拡大**
- **C&Cグルーピング**
  - 挙動解析からグルーピング
  - C&Cドメインによるグルーピング
  - 攻撃キャンペーンによるグルーピング
- **発生攻撃情報との相関、リスク情報**

C&Cサーバリスト共有スキームの試行

□ C&Cサーバリストを13事業者に共有し各事業者が自社フロー情報と照合した結果をフィードバックし分析センターにて総合分析を実施

- □ 対策に向けてのC&Cサーバ共有スキームの試行および評価
- □ 国内１３事業者が連携した大規模分析による全貌把握、リスク変動等の分析
- □ 各社ごとの影響度の把握
- □ 各事業者が将来的に対策実施するにあたっての技術面、運用面、制度面の課題抽出

効果的なボットネット対策を実現するための仕組みづくり



- 照合結果フィードバック情報を活用し検出技術、精度の向上
- より影響度が高く対策優先度高いC&Cに絞り込んだ検出の実施

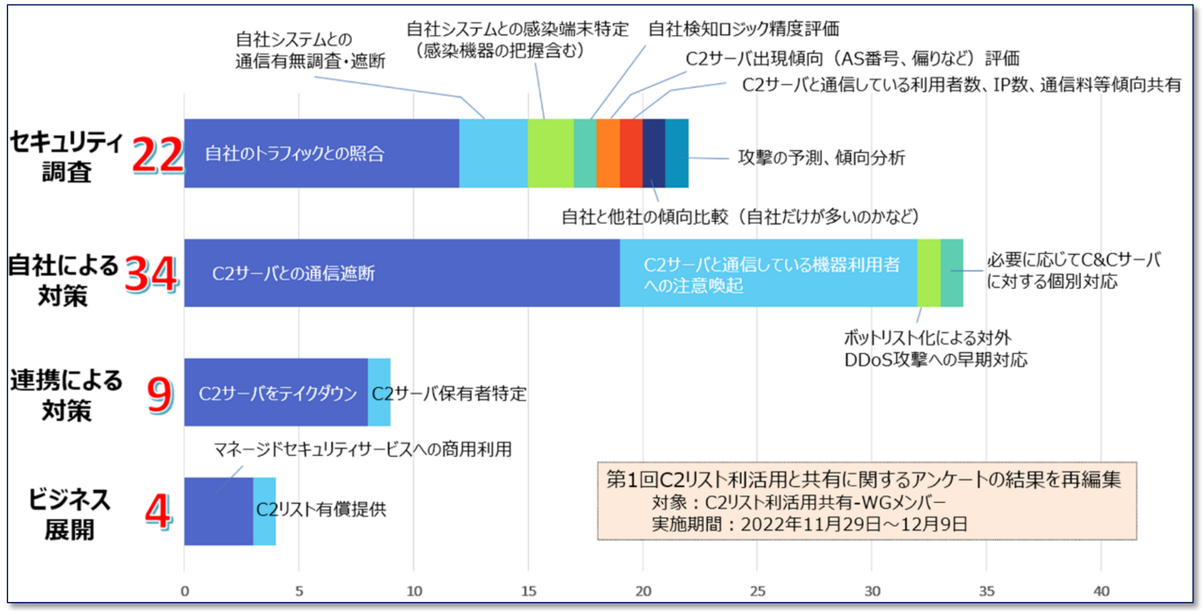
- ボットネット全貌把握に基づくリスク分析
- 照合結果フィードバック情報を活用し検出技術、精度の向上
- より影響度のが高く対策優先度高いC&Cに絞り込んだ検出の実施
- C&Cサーバ共有スキームの改善
- 協調対策、ベストプラクティスの共有
- 検出技術・分析技術の共有に関する検討

- 各事業者個々の影響度、リスク把握
- 各事業者個々の対策検討
- 各事業者が対策実施、運用のために求める脅威インテリジェンスの要件の整理
- 各事業者が対策実施するにあたっての技術面、運用面、制度面の課題抽出
- 各事業者が自らC&C検出やフロー分析を実施するための課題抽出

C&Cサーバリスト利活用の検討

2023年1月に報告した「C&Cサーバリストを利用したいシーン」に関するアンケート調査では、C&Cサーバとの通信遮断について関心が高いが、実施に向け様々な課題がある

C&Cサーバリストを利用したいシーンと課題



C&Cサーバとの通信遮断に関する課題

- C&Cサーバリストに基づき通信を遮断してよい根拠
- 利用者の同意取得
- オーバーブロッキングの責任問題等

C&Cサーバリスト利活用の方向性

利活用用途に応じたC&Cサーバリスト（精度、鮮度、コンテンツなど）を検討していく

- 精度
- 鮮度
- コンテンツ

C&Cサーバリスト

今はここ！

起点となる取組み

ボットネット調査・実態の把握

- 自社やユーザのボット感染状況の把握
- 他社との比較

複数電気通信事業者とのC&Cサーバリスト共有と照合結果の共有

次年度以降

セキュリティ対策研究開発の推進

セキュリティサービスの拡充

- セキュリティサービスへの加入勧奨
- セキュリティサービスへの情報追加

セキュアな自社ネットワークの構築

- 自社設備のボット化確認
- 自社における悪性通信検知能力向上

フォーカスを当てたいテーマ

ボットネット対策の検討・実施

- ボット感染端末利用者への注意喚起
- C&Cサーバとの通信遮断
- C&Cサーバテイクダウン

検討事項

- C&Cサーバリスト（情報、精度、信頼度、新鮮度）
- ボットネットのリスク分析、悪性度/影響度評価
- 法制度との整合
- 電気通信事業者の意向

ボットネット調査・実態把握、悪性度評価等の結果を踏まえて、今後具体的な対策に向けた検討を進めていく

対策トライアル

電気通信事業者がフロー情報から特定したC&Cサーバリストを活用し、本格的なボットネット対策を実施できる体制を整えるため対策トライアルを実施しボットネット対策を試行することで、電気通信事業者が自らC&Cサーバを特定し、対策する手法の有効性や対策手法確立に向けた課題を抽出する

2023(令和5)年度	2024(令和6)年度		
共有トライアル	**プレ対策トライアル**	**対策トライアル**	**実対策展開**
C&Cサーバリストを電気通信事業者13社に共有し、自社のフロー情報との照合と結果のフィードバック。 各社の分析環境の整備、C&Cサーバ共有スキームの有効性の確認、ボットネットの実態把握と可視化	C&Cサーバを特性、種類ごとに分類し、関連するDDoS攻撃情報を紐づけ、一部電気通信事業者によるC&Cサーバ通信、ボット情報、攻撃トラフィックの増減分析に基づく**定量的対策効果確認**の実施。 **効果測定方法の整理**	プレ対策トライアルで確立した**攻撃情報等と相関した最適化された効果測定可能なC&Cサーバ情報を活用**し、電気通信事業者において**ボットネット対策を試行することで、大規模に定量的効果測定を実施**し、対策手法確立に向けた課題を抽出する	実際の対策用C&Cリストの共有に基づく対策の展開

対策トライアル実施内容

対象とするボットネット

- Miraiボットネット（特性毎にグルーピングし攻撃相関情報を付与した効果測定可能なC&C情報を抽出。その他優先的に対処すべきボットネットがあれば、適宜対象として追加）

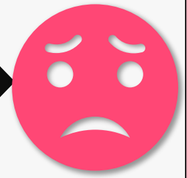
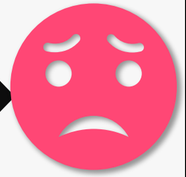
対策トライアルのゴール

- 対策トライアルに参加することで、将来本格的なボットネット対策を実施するための環境整備や課題抽出ができること
- 対策トライアルによってボットネットの規模や被害の縮小などの定量的効果確認できること

対策トライアルの実施手法

- 対策トライアル1．Miraiボットネットを構成するC&Cサーバリストと通信する機器を特定し、利用者への注意喚起を実施
- 対策トライアル2．Miraiボットネットを構成するC&Cサーバリスト（ドメインリスト）によりDNSフィルタリングを実施

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）

評価ポイント		今回の成果	今後の取り組み
正確性 情報の正確さ		• **能動的分析機能導入による高精度の判定の実現** • フロー分析事業者、共有トライアル参画事業者連携による**大規模ネットワーク分析の実現**	• **能動的分析機能**の継続開発体制の確立 • さらなる**参画事業者の拡大**（規模だけではなくサービス種別、クラウドサービスなどの観点も加える） • **生成AIを活用したフロー分析機能強化**
適切なタイミング 内容の鮮度が高く配布が迅速である		• 検出、分析、共有までの各機能の**自動化による検出から共有までの時間の大幅な短縮**	• **利用者、利活用方法に合わせた共有方式**の検討、さらなる**自動化、効率化の促進によるタイムリーな情報共有**の実現
意思決定可能か 情報をもとに取るべき行動が明確		• 分析センターでの**能動的分析機能、深堀解析による高精度の判定**および共有トライアルを通して**国内13事業者連携による大規模なボットネット実態把握**、可視化	• 対象C&Cが関連する**具体的な攻撃情報やリスク情報の付与** • **生成AIを活用**したインテリジェンス強化 • その他対応判断に必用な情報の精査とインテリジェンス生成と提供
利用者目線である 利用者、利用目的に応じた情報である		• **共有WGにおいての議論に基づく利活用方法および実現に向けての課題の精査**	• **具体的な利用者と利用者ごとの利活用方法**の整理 • **対策トライアルを通しての実際の効果確認**と課題の解決

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

統合分析センター

分析評価・監視／可視化

収集・蓄積

共有

対策に資するC&Cリスト生成のための強化ポイント

能動的分析機能強化
高精度のインテリジェンス生成

全体オペレーションの高度化
生成AIを活用した情報収集、整理の効率化

攻撃相関情報連携
リスク判断、定量的効果の可観測性強化

統合分析センターの持続的運用
持続的な取組の実施に向けた体制整備・運用の検討

アナリスト分析の強化
生成AIを活用した情報収集、攻撃相関分析の効率化

検知

- フロー検知を行う電気通信事業者
- 研究・学術機関等
- メーカ・ベンダ等
- オープン情報

検出力向上のための強化ポイント

分析対象ネットワーク拡大
参画事業者の拡大

攻撃インフラ検知の高度化
生成AIを活用した学習用シード情報の生成による分析高度化

外部プロジェクト連携拡大
インテリジェンス強化による検出力強化

対策

- 電気通信事業者
- メーカ・ベンダ等
- 研究・学術機関等
- 公的機関 重要インフラ事業者

対策効果拡大のための強化ポイント

対策実施ネットワーク拡大
参画事業者の拡大

外部プロジェクト連携拡大
連携強化による多角的対策の実現

新たな対策の検討
制度改正も視野に入れた、より効果的な対策の検討

今回の取り組みのまとめ【３】　（将来的な構想）

今後の能動的分析機能の拡張について

R5年度

実証・PoC

- 実証試験
- 先行分析

R6年度

本格実装

- 本格機能実装
- 自動分析強化
- 長期分析によるより詳細なC&C、ボットネット実態分析
- 継続的疑似ボット開発体制構築

想定される技術応用

広域スキャンによるC2検出

- C&Cが利用するポート番号リストを用いて国内IPアドレスに広域スキャンすることでC&Cサーバ検出を大規模に実施

疑似C&Cサーバ開発

- 疑似C&Cサーバを開発し、シンクホールを構築
- DNSポイズニング、経路ハイジャック、セッションハイジャックを組み合わせることで、C&C通信制御、感染端末の強制改善を実施

ご静聴ありがとうございました