資料１－６

ICTーISACにおける
サイバーセキュリティ対策に関する取組み

2024年2月9日

一般社団法人　ICT-ISAC
ステアリングコミッティ運営委員長

小山 覚

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

本日のアジェンダ

1. ISACと情報共有について
2. ICT-ISACの概要
3. ICT-ISACのWGによる活動
4. 観測システムを活用したサイバー攻撃対策
5. サイバー攻撃対応演習の実施
6. 総務省のサイバーセキュリティ政策への協力
7. T-CEPTOAR事務局としての活動
8. 会員社のインシデント情報共有拡充に向けた取組み
9. ISAC組織連携(国内ISAC連携、海外ISACとの連携)
10. 新たな「フロー情報分析結果」の活用方法について

1. ISACと情報共有について

ISAC（ Information Sharing and Analysis Center ）とは

1. 1998年 大統領令63、クリントン政権の国家の重要な情報ネットワークを防護する政策によって、重要インフラの各業種において設置が促されたのが始まり
2. リスクを軽減し、回復力を高めるため、脅威情報を収集・分析し、共有する
3. 日本では2002年発足の通信分野のTelecom-ISACが初、ICT-ISACに活動を継承

情報共有は、民間が行える最も費用対効果が高い防御手法

1. 情報共有は、リスクマネジメントの活動そのもの
2. ISACメンバ間の情報共有によって、早期の警報等を得る/提供できる
3. 他のメンバからの情報により、他社の経験、状況を学ぶ
4. 情報共有による連携は、防御の費用を下げることができる
5. 自社が把握できていない攻撃者、脅威を認識することができる

国内でのISAC活動

2002年のTelecom-ISACを皮切りに、日本のISAC組織は、現在7組織が活動中

2002 – – – 2014 2015 2016 2017 2018 2019 2020 2021

Telecom-ISAC Japan
Telecom Information Sharing and Analysis Center Japan

ICT-ISACの前進
2002年設立
日本初のISAC

ICT分野に拡大

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

ICT(通信、放送、SIer、セキュリティ等)

通信

Financials ISAC Japan Information Sharing and Analysis Center

金融

JFTC

貿易

J-Auto-ISAC
Japan Automotive Information Sharing and Analysis Center

自動車

JE-ISAC

電力

SoftwareISAC

ソフトウェア

Transportation ISAC JAPAN

交通

国内において、様々なISAC組織が設立され、
ISAC組織をまたがる連携も始まっている

2. ICT-ISACの概要

名称：一般社団法人　ICT-ISAC

目的：ICTの普及、発展により、日常生活、経済、行政、安全保障・治安確保などのあらゆる活動がサイバー空間に依存するようになり、高度化・複雑化するICTへの脅威は深刻な社会的脅威となっている。

このような現状に鑑み、ICTに関わるセキュリティの対策・対応レベルの向上に資する活動を行うために、メンバ間の幅広い相互連携を図り、安定した情報流通、情報伝達を維持することで、安全なICT社会の形成に寄与することを目的とする。

会員企業：46社

通信事業者 **24**社、放送事業者 **7**社、セキュリティベンダ **9** 社、SI・ベンダ **6** 社

NTT・KDDI・IIJ…　NHK・民放各社・CATV…　トレンドマイクロ・NRIセキュア…　NEC・富士通・日立…

構成：理事：3名（理事長：齊藤　忠夫(東京大学名誉教授)）、 監事：１名、 顧問：２名、
SC運営委員：14名、 事務局（常勤）：10名

沿革：2016年３月設立（2002年設立のTelecom ISAC Japanを引き継ぐ）

ICT-ISACの活動内容

1．サイバーセキュリティに関する情報収集・調査・分析

ICT分野の情報セキュリティに関する情報(インシデント情報を含む。)の収集・調査・分析

2．会員間の情報共有と共同対処

情報セキュリティに関する情報を目的に応じて共有し、それを活用しつつ、会員企業間で相互協調する仕組みを整備し、それを促進する

3. セキュリティ人材の育成、セキュリティ啓発

情報セキュリティに関する情報を目的に応じて共有し、それを活用しつつ、会員企業間で相互協調する仕組みを整備し、それを促進する

4. セキュリティガイドライン等の整備に関する活動

会員企業が情報セキュリティ対策を円滑に行う上で必要となるガイドラインの検討及び法制度に関する政府研究会等への参画

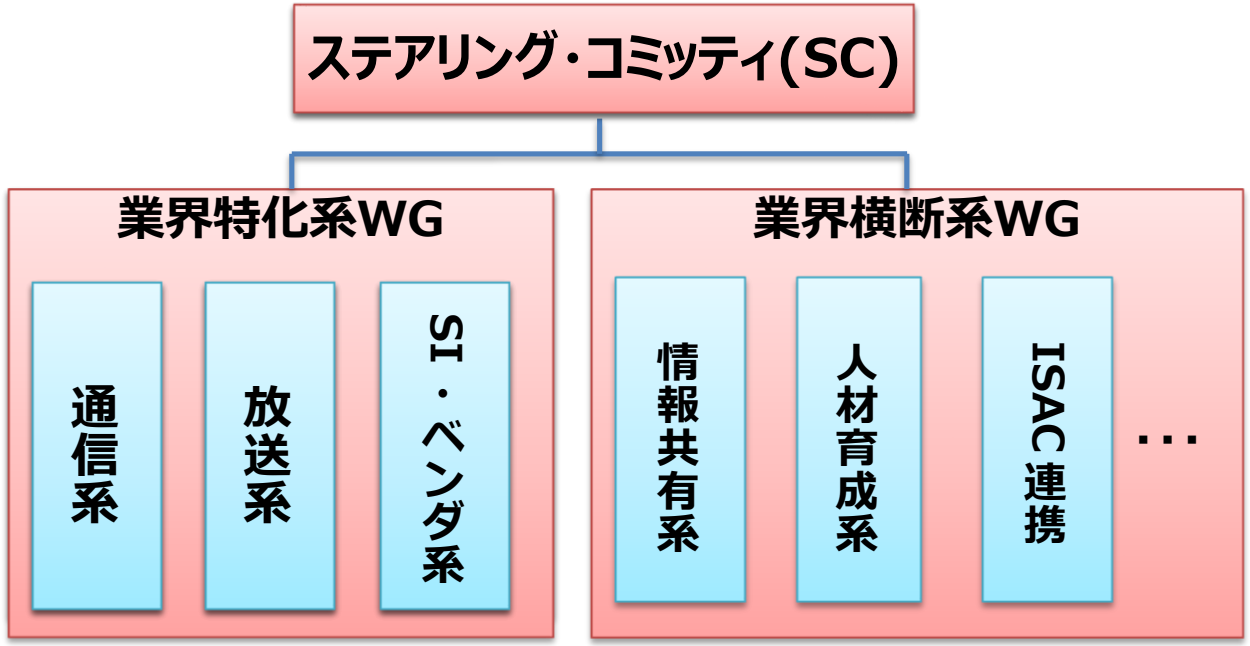
5. 認定協会としての活動

電気通信事業法の規定による総務大臣の認定を受けた認定送信型対電気通信設備サイバー攻撃対処協会(認定協会)としての業務

3. ICT-ISACのWGによる活動

- **ICT-ISACの活動は主に会員の参加する、業界毎あるいは業界横断的に設定されたテーマ毎のWGで実施**
- **現在21のWGが活動中。情報共有、情報収集等の活動は自主的な活動として実施**

ステアリング・コミッティ配下に会員各社がテーマ毎に参加する21のWGがあり、情報共有等、ISACの活動を実施



■情報共有の例

- G7広島サミット、処理水放出時の攻撃予告の確認状況、各社の認知した攻撃、対処状況（Dos攻撃即応WG）
- IoT機器のマルウェア等感染観測状況（IoTセキュリティWG）
- 生成系AIの各社の取り扱い（ITセキュリティWG）

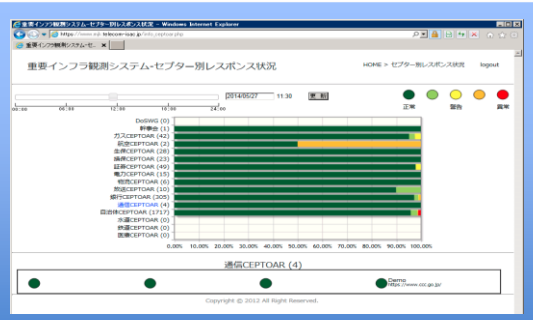
■勉強会・講演会の例

- **「サイバー攻撃被害に係る情報の共有・公表ガイダンス」勉強会**
- 「医療機関で考えるべきセキュリティ」
- 「DX時代の情報戦～偽情報を見抜くリテラシーを身につける～」

４．観測システムを活用したサイバー攻撃対策

- サイバー攻撃対処を**「観測ー分析ー特定ー連絡ー対処」**の流れで実現するため、観測システムを会員に提供
- 大規模イベント期間（オリパラ、G7等）には、レスポンス観測システムの情報をISAC会員外にも提供するなどサイバー対策に寄与

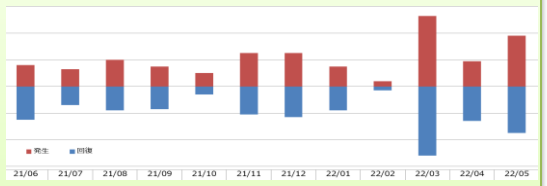
DDoS攻撃の監視



重要インフラ観測システム

レスポンス観測システム

DRDoS攻撃アラートシステム



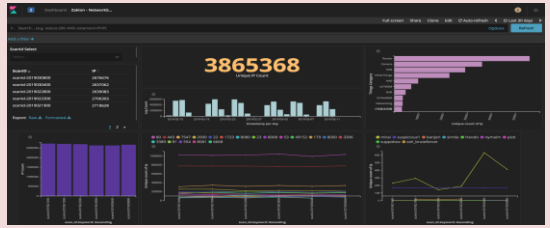
経路ハイジャック検知システム

監視対象重要インフラサイトのレスポンス監視

複数センサーによる特定サイトのレスポンス監視

DRDoS攻撃発生検知

脆弱な機器のIP、オープンポートや機器名の検索



広域スキャンシステム

AIによる脆弱性情報分析システム

脆弱性のリスクをAIで数値化

情報共有基盤

5．サイバー攻撃対応演習の実施

対処能力の向上のためのサイバー人材の育成と事業者間連携強化のため、毎年「サイバー攻撃対応演習」を実施
１年弱をかけてWG有識者で作成したサイバー攻撃シナリオを使って参加事業者各社が一斉に検討

演習の目的

コンタクトポイントの確認

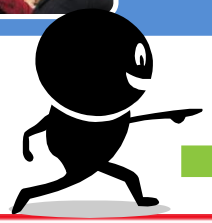
攻撃発生時に事業者間で連携がとれるか確認すると同時に、どのように連携をとるかを練習する

人材育成

通常のオペレーションでは経験できないことを演習を通じて体験する

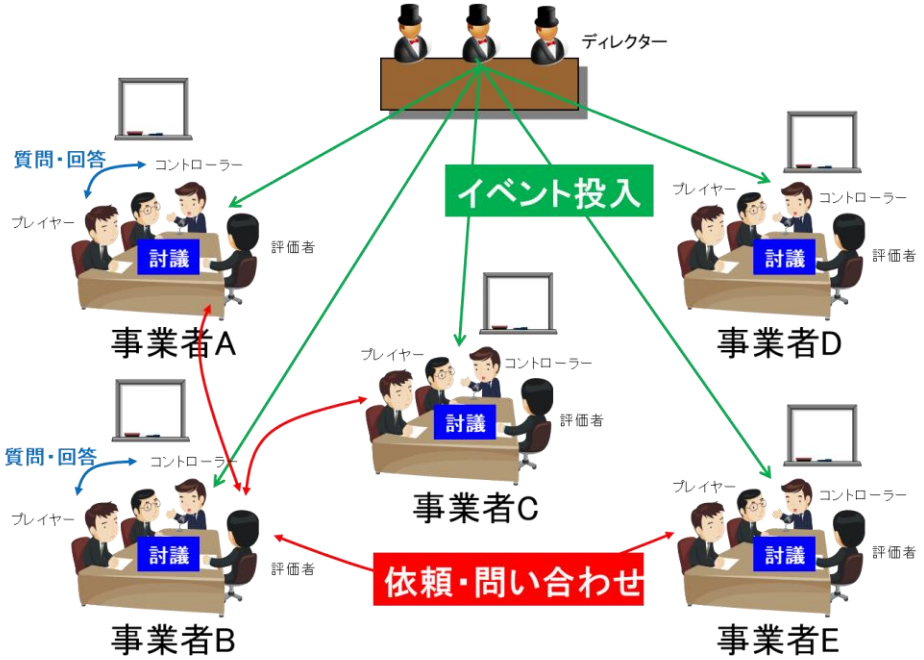
課題認識と改善

各社、自組織の課題を認識し、改善につなげる



有事においても迅速な対応
＝実際の被害や影響への対処を迅速化

演習の方法



- **共通のシナリオに基づくイベントを事業者各社で討議、各社の状況、体制に応じて対処を検討**
- **事後、事業者全社で振り返り、人的交流も醸成**

サイバー攻撃対応演習のシナリオの歴史

日々刻々と代わる攻撃手法に応じたシナリオを設計して対策を行う演習を、2006年から通算18回開催して、「自ら動けるサイバー人材」育成を通じて、サイバー攻撃に対する影響の抑制につなげている

総務省「電気通信分野におけるサイバー攻撃対応演習」 → Telecom-ISAC Japan演習 → ICT-ISAC演習

開催年度	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023
参加	6＋ 4省庁・機関	10＋ 4省庁・機関	8＋ 4省庁・機関	11＋ 4省庁・機関	9	9	11	10	12	19	17	17	18	22	19	20	17	17
背景情報	－	大規模な国際ITテロ集団の台頭	海外政治活動集団における反日感情の高まり	新型インフルエンザの流行	貿易摩擦による国際問題／海外世論での批判の高まり	震災発生	法改正への抗議活動(ﾊｸﾃｨﾋﾞｽﾞﾑ)	民族主義過激派	オリンピック	世界的なサイバー攻撃被害の多発	世界的なサイバー攻撃被害の多発	金銭目的のサイバー攻撃	国際的な大規模スポーツイベント脆弱なIoT機器の増加	国際的な大規模スポーツイベント	コロナ禍に便乗したマルチレベルのサイバー攻撃	リモートワークの普及重要システムのクラウド移行	ウクライナ侵攻および緊急対応の脆弱性の増加	国際的緊張の長期化によるサイバー攻撃の継続
攻撃手法	－	DoS BGP DNS IP電話	DoS BGP DNS IP電話	DoS BGP Abuse ｱｸｾｽ網	DoS BGP DNS ｱｸｾｽ網	DoS BGP DNS ｱｸｾｽ網	DoS BGP DNS ｱｸｾｽ網 Web	NW(BGP) DNS ｱｸｾｽ網 Web ﾓﾊﾞｲﾙ	NW DNS ｱｸｾｽ網 Web ﾓﾊﾞｲﾙ	NNW DNS Web ﾓﾊﾞｲﾙ	NW DNS Web ﾓﾊﾞｲﾙ	NW DNS Web ﾓﾊﾞｲﾙ	NW DNS Web ﾓﾊﾞｲﾙ	NW DNS Web	NW DNS Web	NW DNS Web	NW DNS Web	NW DNS Web
シナリオ	■委託業者による社内ITｼｽﾃﾑへの不正アクセス ■SQLｱﾌﾟﾘｹｰｼｮﾝを狙った感染活動(Slammer) ■金銭恐喝目的のDoS攻撃 ■偽装ﾒｰﾙを利用したマルウェア感染攻撃 ■組織内でのﾜｰﾑ攻撃活動 ■官公庁Webｻｲﾄを狙ったDoS攻撃/Web改ざん ■DoS攻撃被害の海外政府からの支援要請 ■.jpﾄﾞﾒｲﾝのﾀﾞｳﾝ	■重要インフラｻｲﾄへのDDoS攻撃 ■インターネット通信麻痺を狙ったDNS 攻撃 ■IP電話スパム攻撃 ■重要インフラｻｲﾄの経路ﾊｲｼﾞｬｯｸ	■国内に拡散したマルウェアがISP事業者の重要ユーザーのWebｻｲﾄに大規模なDDoS攻撃 ■国内に拡散したマルウェアが重要インフラのコールセンターに大規模なIP電話スパム攻撃 ■DNSｷｬｯｼｭﾎﾟｲｽﾞﾆﾝｸﾞ攻撃を利用したﾌｨｯｼﾝｸﾞｻｲﾄへの誘導 ■VoIP基盤事業者SIPｻｰﾊﾞの経路をﾊｲｼﾞｬｯｸ	■金銭恐喝目的のDoS攻撃 ■特定の経路属性情報に起因したﾙｰﾀ障害発生 ■ISPｷｬｯｼｭDNS踏み台攻撃/誤設定による特定TLD接続障害 ■ルータ問題によるPPPoE切断多発/ﾍﾋﾞｰﾕｰｻﾞ同一収容ﾕｰｻﾞの接続障害 ■悪性Webｻｲﾄによるユーザ感染 ■ｲﾝﾌﾙｴﾝｻﾞ流行による担当者不在	■特定Webｻｲﾄを対象としたDoS攻撃/権威サーバへの大量クエリ発生 ■有名ｻｲﾄの経路ﾊｲｼﾞｬｯｸ ■TLD誤設定ｷｬｯｼｭ情報の保有/レジストリｼｽﾃﾑ不正侵入によるNSサーバ情報書換え ■網終端装置への脆弱性攻撃/DoS攻撃による高負荷	■Webｻｲﾄを標的としたDDoS攻撃 ■不正侵入された海外ISPからの不正経路広告 ■DNSサーバへの攻撃 ■網終端装置/特定ユーザへのDoS攻撃発生	■国内外からのDDoS通信による輻輳発生 ■NSレコード/TLDサーバへの攻撃 ■オペミス/不正侵入による経路ﾊｲｼﾞｬｯｸ ■網終端装置/特定ユーザへの輻輳発生 ■Web改ざんによる感染ｻｲﾄへの誘導/マルウェア感染によるﾌｨｯｼﾝｸﾞｻｲﾄへの誘導	■DNS Amp攻撃手法による権威/ｷｬｯｼｭDNSサーバ高負荷 ■経路ﾊｲｼﾞｬｯｸ・バックボーンへの攻撃 ■脆弱性攻撃によるWeb改ざん ■網終端装置/HGWを狙った脆弱性/DoS攻撃 ■DoS攻撃によるゲートウェイ輻輳/不正アプリによるDoS攻撃発生	■NW機器の脆弱性を利用したDNS/SSDPﾘﾌﾚｸｼｮﾝ攻撃によるNW/ DNS設備過負荷、ﾕｰｻﾞ宅設備故障 ■モバイル不正アプリによるﾌｨｯｼﾝｸﾞ・大量攻撃 ■APT攻撃によるマルウェア感染	■経路ﾊｲｼﾞｬｯｸ/DDoS ■DNSﾊｲｼﾞｬｯｸ/ｷｬｯｼｭDNSｻｰﾊﾞ高負荷 ■Web改ざん/ﾌｨｯｼﾝｸﾞ/不正送金/ﾏﾙｳｪｱ感染 ■ﾓﾊﾞｲﾙ不正ｱﾌﾟﾘ、マルウェアによる情報漏えい/端末異常	■経路ﾊｲｼﾞｬｯｸ/DDoS/Slow DoS ■DNS水責め/ｷｬｯｼｭポイズニング/DNSamp ■ﾌｨｯｼﾝｸﾞ/流出アカウントによる情報搾取 ■ﾓﾊﾞｲﾙ不正ｱﾌﾟﾘによる情報漏えい/端末からのDDoS	■DDoS/構成情報等漏えい/監視端末のマルウェア感染 ■DNS水責め ■Web改ざん/認証情報漏えい/不正ログイン/ﾏﾙｳｪｱ感染 ■端末脆弱性/モバイル端末のマルウェア感染/端末からのDDoS	■設定改ざん/マルウェア感染/DDoS ■DNS大量クエリ/経路ハイジャックによるにせDNSへの誘導/jpドメインダウン ■WEBサイト不正アクセス ■機器脆弱性/不正アプリによるDDoS	■経路ハイジャック ■キャッシュポイズニング ■マルウェア／フィッシングサイト誘導 ■ソフトウェア脆弱性を利用したDNS/Web改ざん ■大量通信	■キャッシュDNSの脆弱性 ■偽情報によるマルウェア付更新ファイル配布 ■偽情報によるアクセス集中 ■DDoS攻撃	■廃止サイトのCDNCNAME残留による乗っ取り ■脆弱性による権威DNS書き換え ■DV証明書不正取得による自社ドメインのフィッシングサイト ■DDoS攻撃	■大規模DDoS攻撃（自網内・対外接続回線の輻輳WEBサーバ停止） ■DNS水責め攻撃 ■jpの権威サーバ停止 ■不完全な脆弱性対応による踏み台設置	■外部ISPからの緊急情報サイトへの大規模DDoS攻撃（外部ISPから自網アクセスと攻撃先へのアクセスの両立） ■DNSアンプと水責め攻撃 ■DDoSとDNS水責めによる自社Webサイトへのアクセス不可

オンラインでの開催

6. 総務省のサイバーセキュリティ政策への協力

- 観測した感染通信や脆弱性の内容を分析し、ICT-ISACをハブとしてISPに展開することで、インターネット空間の安心安全に向けた官民連携を2006年から継続
- 最近では、IoT機器の悪用によるサイバー攻撃を防止する取り組み、NOTICEに参画

サイバー攻撃のトレンド

ICT-ISACが進める官民連携プロジェクト

NOTICE 2019~
脆弱なIoT機器への注意喚起（総務省・NICT）

ACTIVE 2013~2018
PC等の総合的なマルウェア対策プロジェクト

PRACTICE 2011~2016
国際連携によるサイバー攻撃予知即応プロジェクト

RDB 2009~2012
悪性サイトの調査研究

Cyber Clean Center 2006~2011
ボットネット通信を検知し、対策を促す取り組み

NOTICE
National Operation Towards IoT Clean Environment

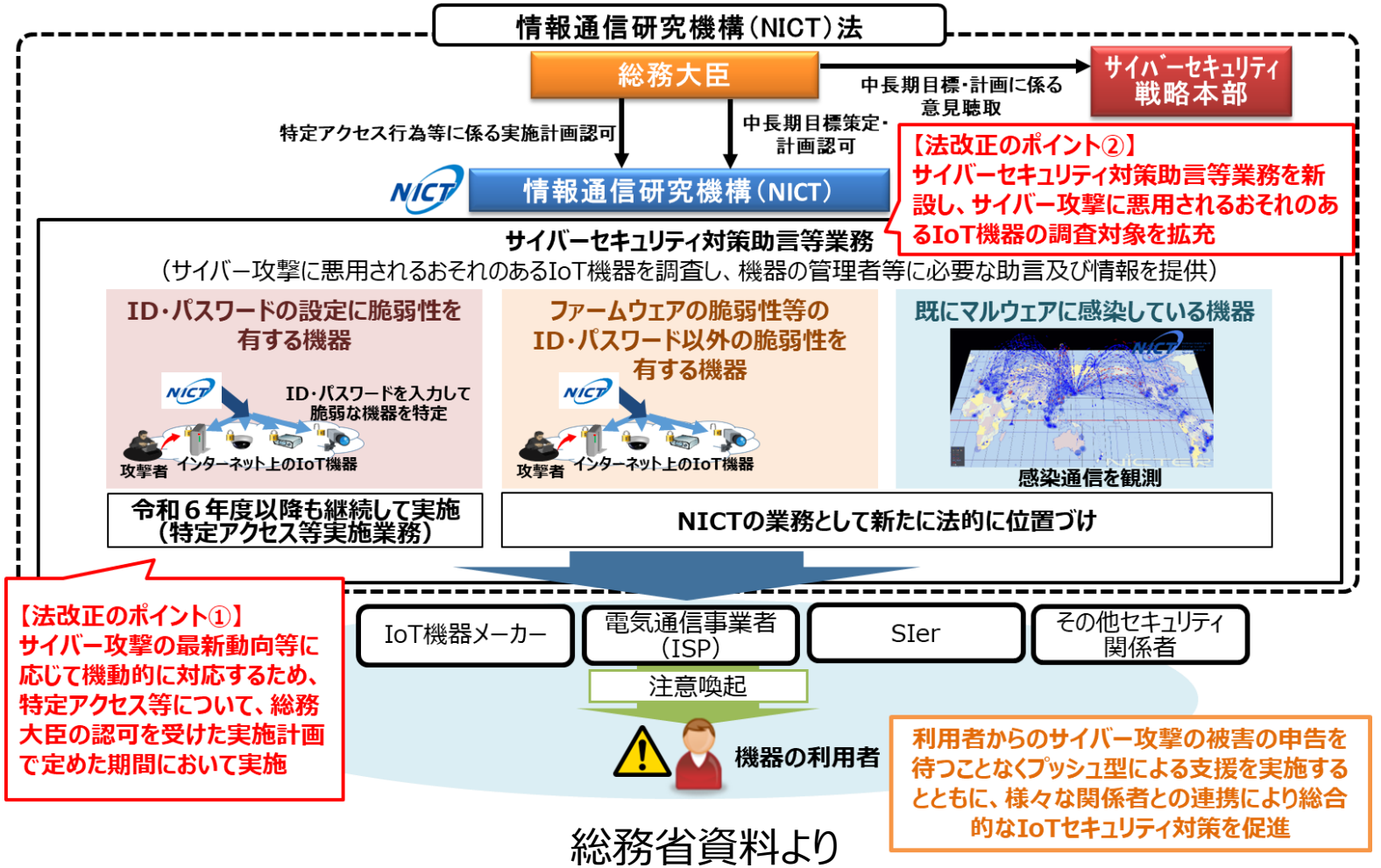
脆弱なID・パスワード設定など、IoT機器の悪用によるサイバー攻撃を防止する取り組み

- 観測（NICTが脆弱なIoT機器等を観測）
- 分析（機種メーカに外部攻撃通信可否を調査）
- 特定（当該ISPに情報展開しユーザを特定）
- 連絡（IoT機器の利用者にリスクを連絡）
- 対処（ID・パスワード再設定など利用者が対処）

ユーザ特定の結果、法人の場合も多い

6.1 NOTICEプロジェクトの継続・拡充に関連した取組み

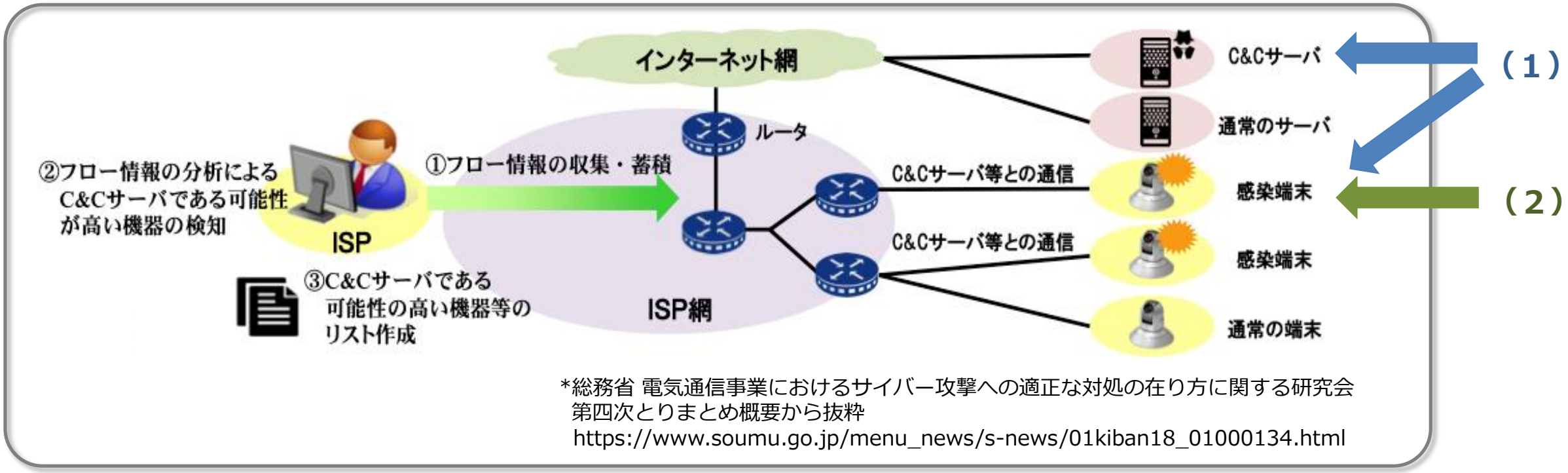
- 今回の臨時国会で法改正があり、NOTICEプロジェクトの調査対象や情報提供・助言機能が拡充される。
- ICT-ISACはNOTICEプロジェクトに認定協会として引き続き協力していく（ステコミなどの運営にも参加し、メーカーやSIerとも連携するとともに、広報にも協力する）。



総務省資料より

6.2 フロー情報分析によるセキュリティ対策の取り組み

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り、総務省様との実証事業に取り組み中



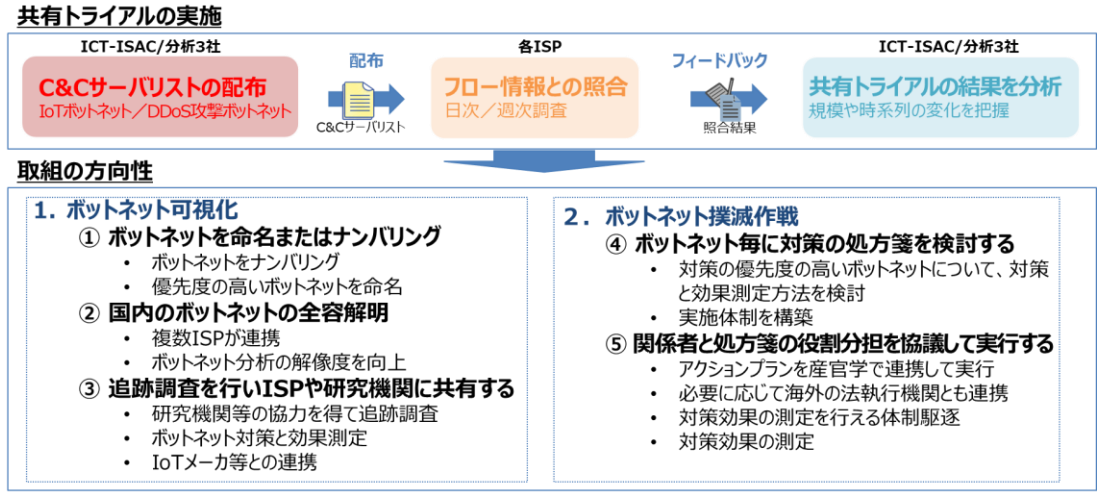
*総務省 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会
第四次とりまとめ概要から抜粋
https://www.soumu.go.jp/menu_news/s-news/01kiban18_01000134.html

（1）フロー情報分析によるボットネット「C＆Cサーバ＋感染端末の集合体」の可視化に取り組み中

（2）外部から入手したC&CサーバのIPアドレスを元に、感染IPを特定しセキュリティ対策に取り組めないか？
→ 重要インフラ事業者等の**固定IPアドレスを対象に、フロー情報分析**でC&Cサーバとの通信を遡及調査し、情報共有することで**Attack Surface Management（ASM）の強化**に貢献したい

（1）フロー情報分析によるボットネット可視化への取組み

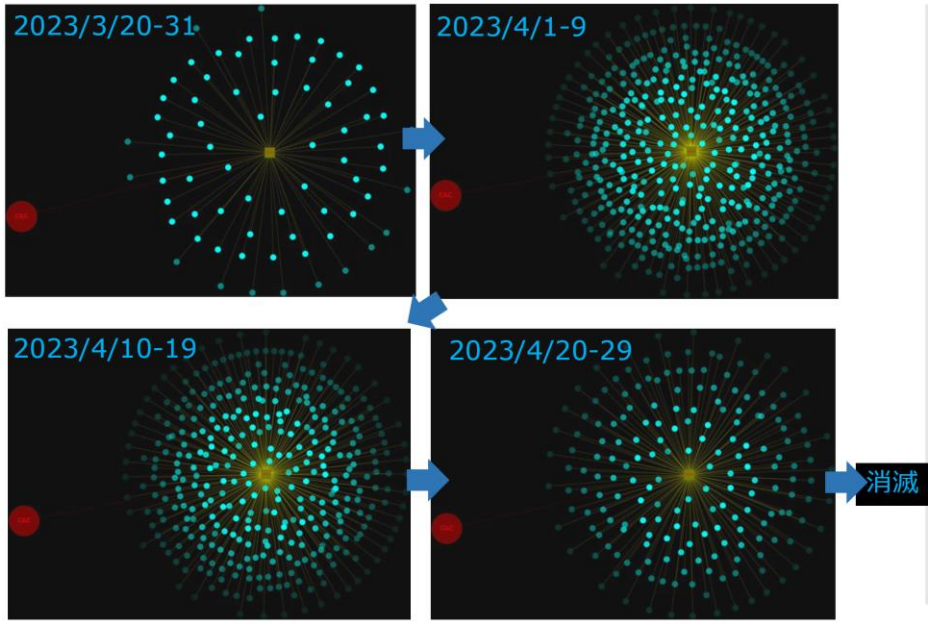
- ボットネットによるサイバー攻撃は、電気通信事業者が役務提供をする上で、大きな脅威となっている。
- ICT-ISACでは、総務省「C＆Cサーバ特定総合実証」と連携し、電気通信事業者が収集・蓄積しているフロー情報を分析することで、C&Cサーバ※を特定、共有しボットネットの可視化、対策の検討に取組んでいる。



C&Cサーバ共有トライアルの推進

Type	全体	NW1	NW2	NW3	NW4	NW5	NW6	NW7	NW8	NW9	NW10	NW11	NW12
ALL	99	12	13	7	2	19	17	24	17	21	8	24	21
DDoS	65	8	8	5	1	10	9	14	11	13	4	15	14
PentestFramework	5	0	0	0	0	0	0	0	0	0	0	1	0
InformationStealer	11	0	1	0	0	2	2	2	1	2	0	2	2
Backdoor	10	1	2	0	0	3	3	4	2	2	1	3	2
RAT	5	0	0	0	0	1	0	1	0	1	0	0	0
Spam	0	0	0	0	0	0	0	0	0	0	0	0	0
Mobile	0	0	0	0	0	0	0	0	0	0	0	0	0
Other	3	3	2	2	1	3	3	3	3	3	3	3	3

電気通信事業者12社による共有トライアルの結果



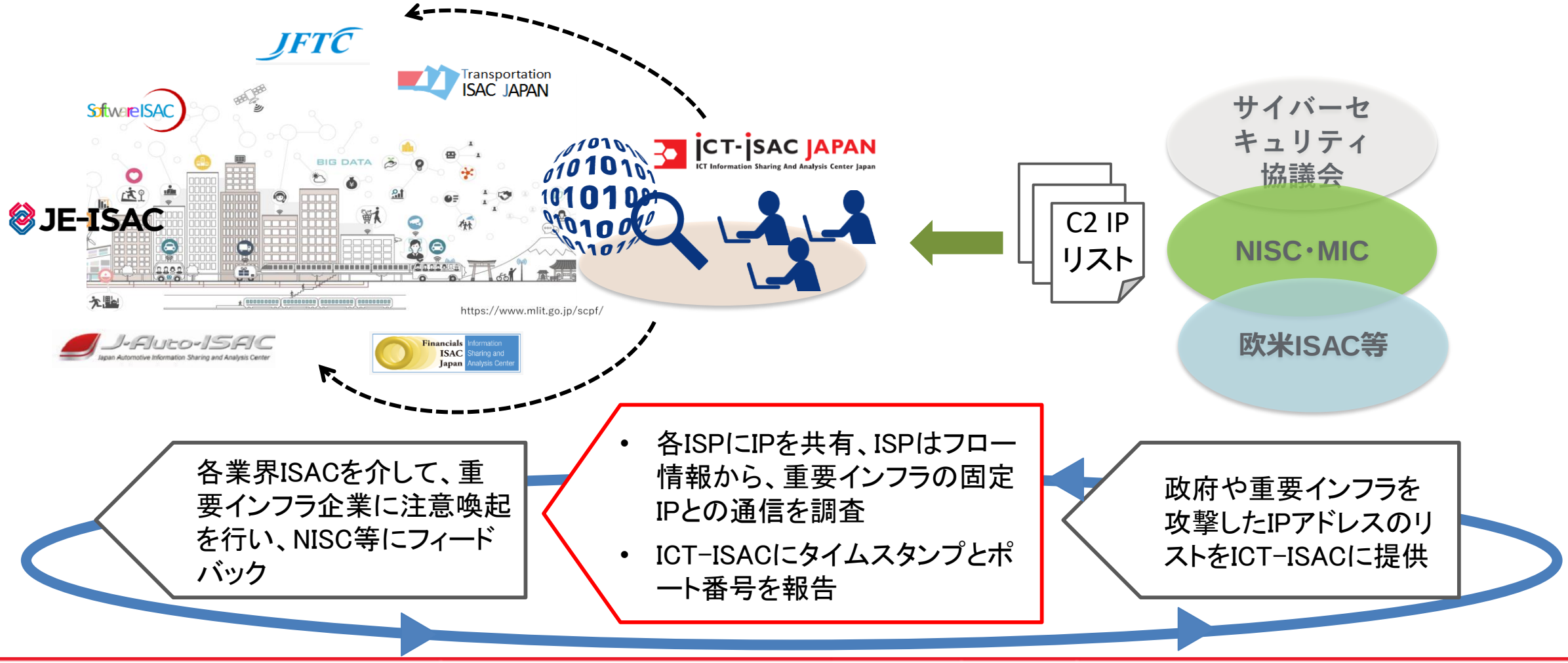
ボットネット可視化のイメージ

総務省「C&Cサーバ特定総合実証」と連携した取組み

※C&Cサーバ
C&Cサーバ(Comand and Control Server)は、サイバー攻撃者がボットに対して攻撃命令を出したり、ボットネットをコントロールするサーバ。

（2）固定IPアドレスを対象にしたフロー情報分析の取り組み

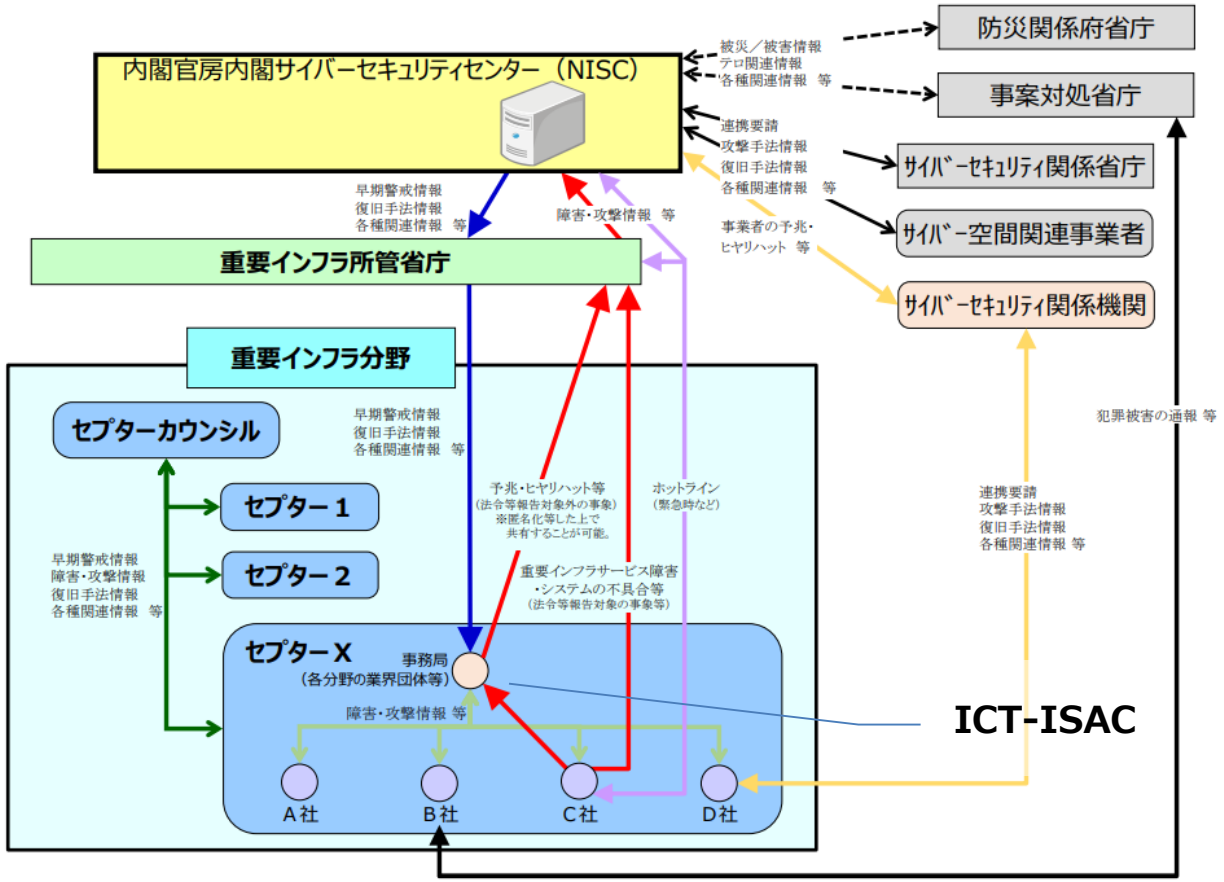
- 重要インフラ事業者等の**固定IPアドレスを対象に、フロー情報分析**でC&Cサーバとの通信を遡及調査し、情報共有することで**Attack Surface Management（ASM）の強化**に貢献したい



7. T-CEPTOAR事務局としての活動

- **ICT-ISACは通信セプター、T-CEPTOARの事務局**
- **T-CEPTOARは構成員28社。他に関連団体3団体にも必要に応じ情報展開を実施**

情報展開の流れ



「重要インフラのサイバーセキュリティに係る行動計画」より

最近の活動（直近約１カ月）

① NISCからのサイバーセキュリティに係る情報共有・注意喚起等の情報配信のT-Ceptoarへの展開

② 2023年度セプター訓練
模擬情報発出(NISC)→総務省→セプター事務局
→T-Ceptoar展開
i) 情報提供／受領報告訓練
ii) 情報連絡訓練（情報受領後の報告、事業者
→ICT-ISAC→総務省→NISC）

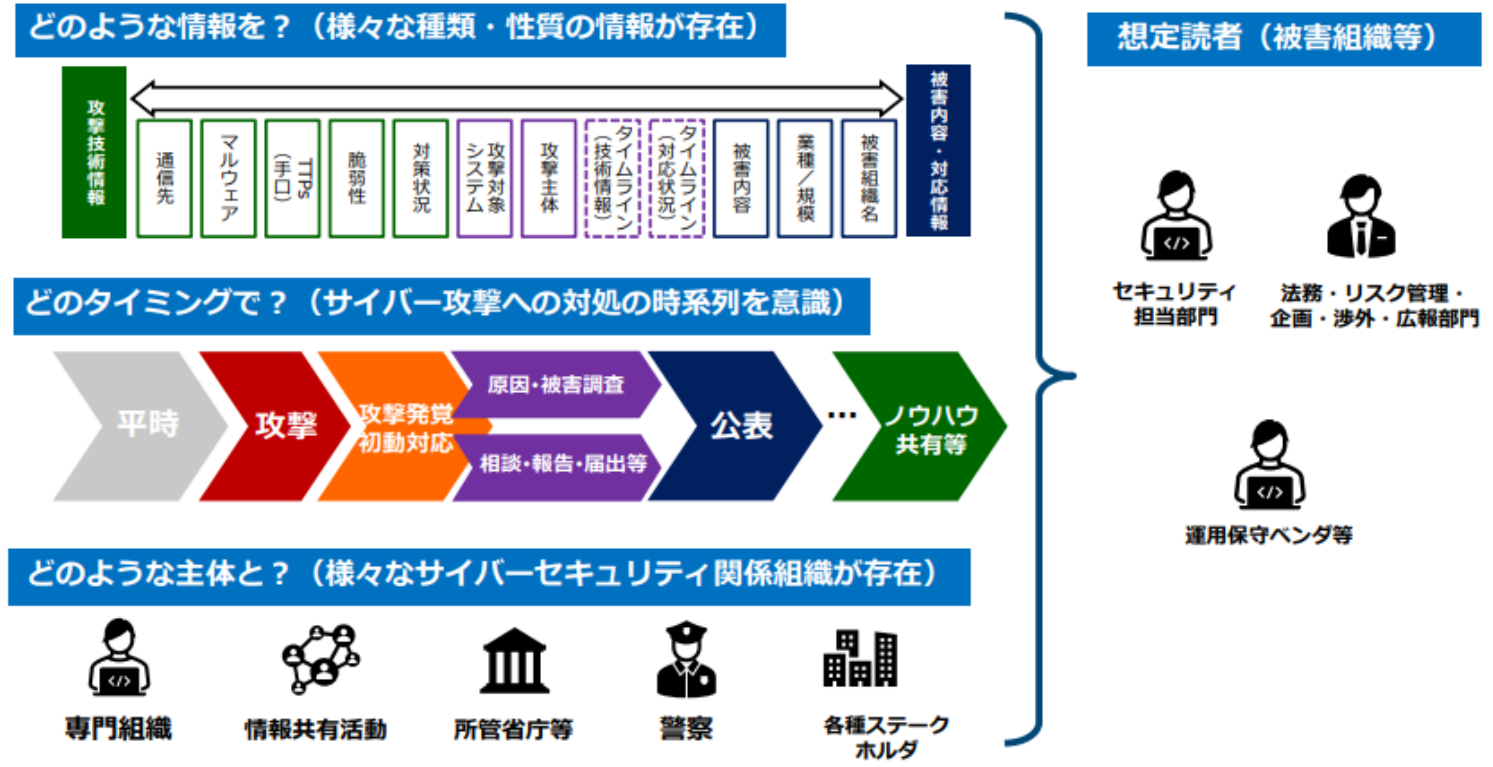
③ NISC分野横断的演習

④ 第74回セプターカウンシル運営委員会参加

8. 会員社のインシデント情報共有拡充に向けた取組み

- 今春、各省連名で公表された「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を会員に周知展開したところ、会員の関心が高かったため、総務省経由でJPCERT/CCの執筆者を紹介いただき、勉強会を実施
- 更に、ICT-ISACが共催するイベントにおいて、NISCとJPCERT/CCの関係者のトークセッションを実施

勉強会では、サイバー攻撃の速やかな情報共有や目的に沿ったスムーズな被害公表について、
実務上の参考となるポイントについて記載のガイダンスについて、作成経緯含め解説いただいた



「サイバー攻撃被害に係る情報の共有・公表ガイダンス」概要より

「サイバー攻撃被害に係る情報の共有・公表ガイダンス」とICT-ISAC

- サイバー攻撃被害は、いくつかの原因で公表に時間を要し、また、公表内容に具体性を書く場合も多い。
- ガイダンスではその対応として公表と非公開の情報共有を分離することも推奨されているが、非公開の情報共有の場として、ICT-ISACのWG活動が有用である。

■サイバー被害公表の課題

・公表までに時間を要する

原因：　被害の全貌の調査
公表後の対応準備
再発防止等対策検討

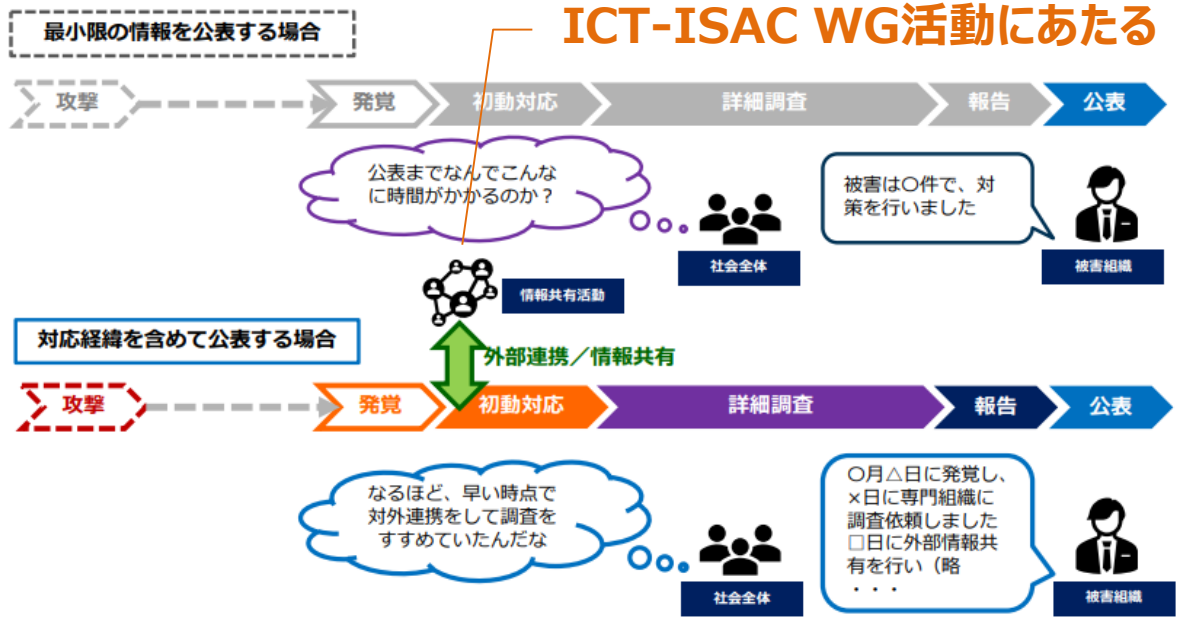
・公表内容の調整過程において具体性が欠落する

公表と非公開の情報共有の分離が推奨（ガイダンス）

ICT-ISAC　WG活動で対応可能

■サイバー被害公表までに時間を要する場合の対応

情報共有の対応実施を示すことで不安を払拭



「サイバー攻撃被害に係る情報の共有・公表ガイダンス」概要より

9．ISAC組織連携(国内ISAC連携、海外ISACとの連携)

ISAC発祥の米国のISACの他、近年EUでもISACが増えつつあり、相互に活動内容を理解する会合を定期的に開催

国内ISACとの連携 (2019 ~)

定期会合の開催、課題の相談

Financials ISAC Japan Information Sharing and Analysis Center
JE-ISAC
JFTC
J-Auto-ISAC Japan Automotive Information Sharing and Analysis Center
SoftwareISAC
Transportation ISAC JAPAN

米国ISACとの連携 (2019 ~)

定期会合の開催

IT ISAC　NCC　national council of ISACs

- ワークショップの開催
- 情報共有基盤

IT-ISAC との MoU on Cybersecurity の締結
IT-ISAC, NCC (Com-ISAC), National Council of ISACs
総務省を介して、米国政府機関との連携

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

日米欧　多国間連携の検討(2022~)

ASEAN各国政府およびISPとの連携 (2011 ~)

定期的に「ＩＳＰ向け日ASEAN Information Security Workshop」を開催

- 定期ワークショップの開催
- 情報共有

ASEAN10カ国の政府およびISPが参加

EU(2022~)

European Commission
PISAX stronger together
eio EURid
etis THE COMMUNITY FOR TELECOM PROFESSIONALS

海外ISAC組織との連携構築例（IT-ISACとのMoU締結）

日米ISAC連携

- 2019年　ICT-ISACと米国IT-ISACの間でサイバーセキュリティに関するMoUを締結
- 日米ISAC及び政府間で年1回程度定期的に会合を開催
- 日米双方の取組みに関する情報共有に加え、機械処理による脅威情報の共有など検討中

サイバーセキュリティ国際シンポジウム開催

ICT-ISACとIT-ISACのMoU調印

クローズドミーティング

ありがとうございました