資料2－5

ICT－ISACにおける
サイバーセキュリティ対策に関する取り組み

2023年2月16日

一般社団法人　ICT-ISAC

小山 覚

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

1. ISACと情報共有について

ISAC（ Information Sharing and Analysis Center ）とは

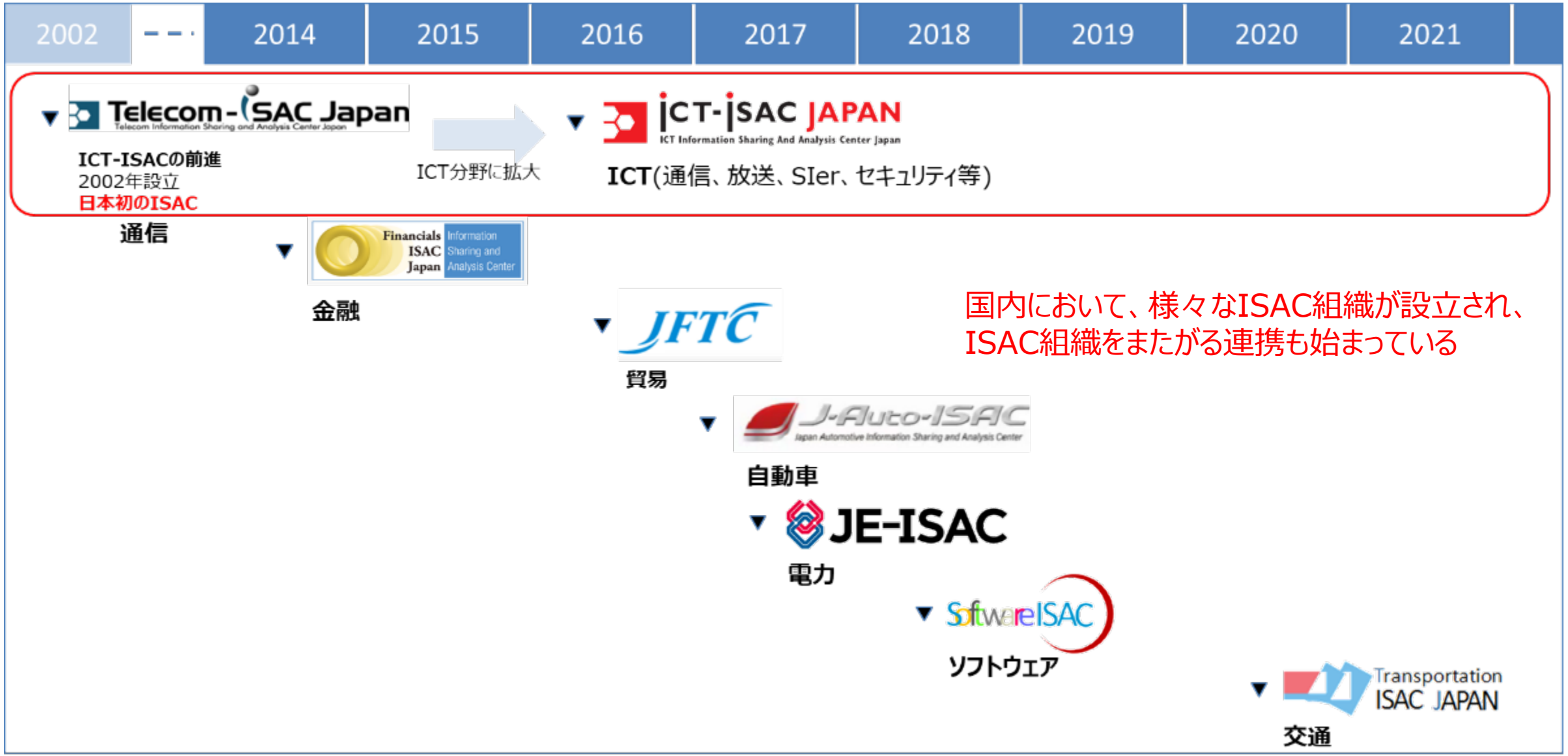
1. 1998年 大統領令63、クリントン政権の国家の重要な情報ネットワークを防護する政策によって、重要インフラの各業種において設置が促されたのが始まり
2. リスクを軽減し、回復力を高めるため、脅威情報を収集・分析し、共有する
3. 日本では2002年発足の通信分野のTelecom-ISACが初、ICT-ISACに活動を継承

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活動の中核として推進するICT-ISAC

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



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

ICT-ISACの会員企業（46社）　通信だけでなく、多彩な業種からなるISAC組織

- 通信事業者 **24**社、放送事業者 **7**社、セキュリティベンダ**10**社、SI・ベンダ**5**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…

ICT-ISACの目的と活動内容

- 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

1. **情報セキュリティに関する情報収集・調査・分析**
2. **情報共有の推進**
3. **セキュリティ人材の育成、セキュリティ啓発**
4. **セキュリティガイドラン等の整備に関する活動**
5. **認定協会業務（ISPを跨いだサイバー攻撃への対処や分析など）**

3．観測システムを活用したサイバー対策の強化

- 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、観測システムの実現・維持が重要
- 東京オリパラ期間に、レスポンス観測システムの情報を国内他業種のISACに展開することで、サイバー攻撃の防止に寄与

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

4．サイバー人材の育成による、対処能力の向上

サイバー人材の育成に向けてCAE-WGでは、毎年DNS/NW/WEBの（サイバー攻撃）シナリオを設計し、ISP横断で合同演習を行っている。

日時	2022年2月10日（木）　13：00～18：00
場所	WebEX（フルオンライン開催）
演習形態	WebEXおよび専用ツールを使用した机上演習
参加事業者	15社174名（参考：見学4社６名、事務局1社５名）

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

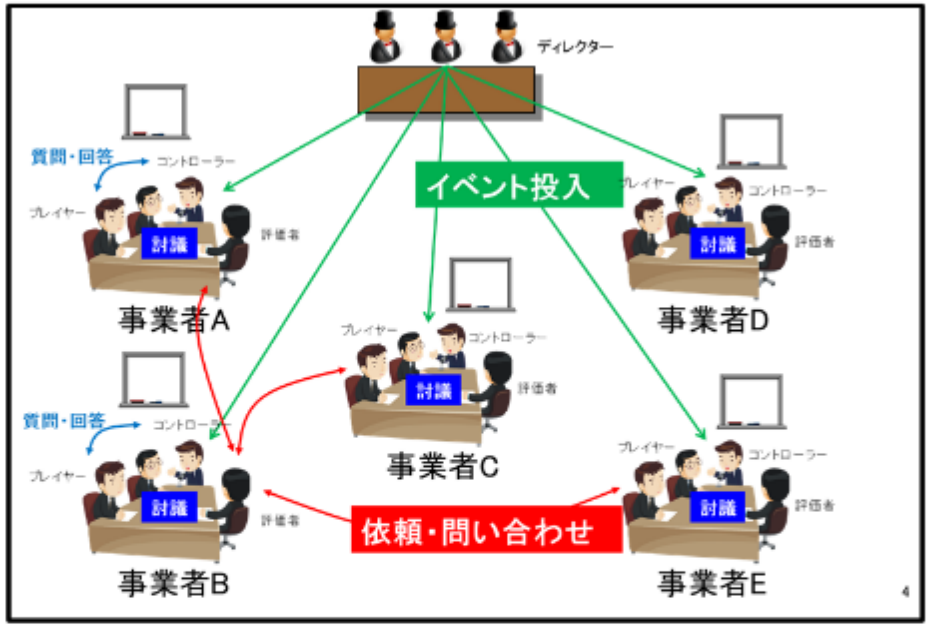
人材育成

- 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

- 自組織の課題、協調対処における課題を認識し、改善につなげる

有事においても迅速な対応



- 共通のシナリオで各社で対策を進めることにより、各社の取り組み、体制に応じた取り組みが進められる。
- 苦労した点などをISP間で振り返ることで、事業者間での人材連携が可能となる。

サイバー攻撃対応演習(CAE)のサイバー人材育成の歴史

- 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16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※
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
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
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	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/ﾓﾊﾞｲﾙ	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/特定ユーザーへの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CDNのCNAME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

オンラインでの開催

5. 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

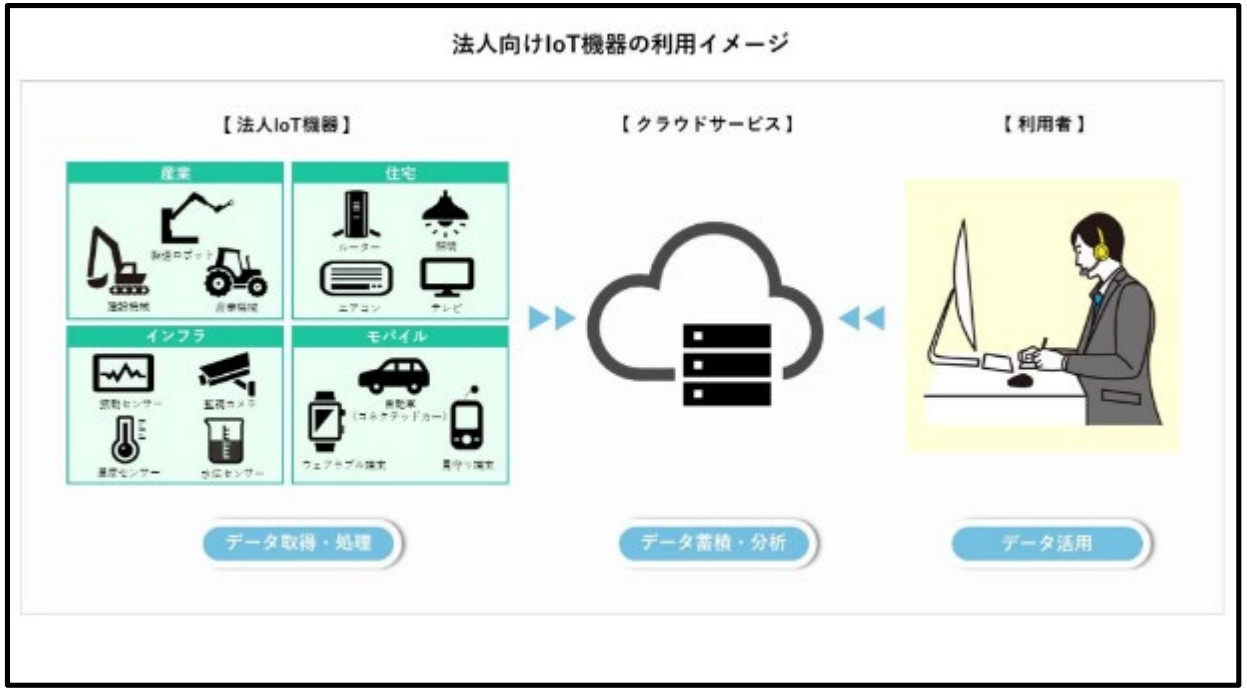
脆弱なID・パスワード設定など、IoT機器の悪用によるサイバー攻撃を防止する取り組み

- 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

法人向けIoT機器の悪用によるサイバー攻撃防止ページ（一般向けの啓発活動例）

- NOTICEでの注意喚起だけでは、注意喚起の理解が十分でない場合も多く、対応してもらえないことがある
- 2022年4月に、ICT-ISACホームページで法人向けIoT機器の悪用防止を啓発（https://www.ict-isac.jp/iot security/）



- 法人向けIoT機器は、DXの推進のために、多くのIoT機器が使われることが想定される
- 法人向けIoT機器の、サイバーセキュリティの管理者が明確でない場合、放置されやすい可能性がある
  （設置事業者？　保守事業者？　委託されていなければ法人自身の役割だが、担当者異動で不在となることも）

6．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している

国内ISACとの連携 (2019 ~)

定期会合の開催、課題の相談

Financials ISAC Japan / JE-ISAC / JFTC / J-Auto-ISAC / Software ISAC / 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「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2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