資料4－1

ICT-ISAC JAPAN

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

情報共有及び国際連携

平成29年5月15日

中尾康二
ICT-ISAC

https://www.ict-isac.jp/

本日のAgenda

１）ICT-ISAC　概要

２）ICT-ISACにおける情報共有

３）国際連携の紹介（ICT-ISACの例も含め）

４）今後の取り組むべき施策とは

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

ICT-ISACの概要

一般社団法人ICT-ISAC

https://www.ict-isac.jp/

ICT-ISACの目的

【目的】

情報通信技術(以下「ＩＣＴ」という)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、社員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

【活動内容】

1．情報セキュリティに関する情報収集・調査・分析
ICTに関わる情報セキュリティ対策に資する情報（インシデント情報を含む。）を収集、調査、分析する活動

2．情報共有の推進（情報共有）
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、それを促進する活動

3．セキュリティ人材の育成、セキュリティ啓発（普及啓発・人材育成）
会員企業のセキュリティ人材育成を促進する活動およびユーザが安全にICTを利用するための普及啓発活動

4．セキュリティガイドライン等の整備に関する活動
会員各社が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および法制度に関する政府研究会等への参画活動

ICT-ISACの概要

- 2016年3月にICT全体を俯瞰した新たなISAC活動を目的とした組織として発足
- 2016年6月に旧Telecom-ISAC Japanメンバー、大手放送事業者、セキュリティベンダー等もメンバーに加わり、2016年7月より、本格的活動を開始
- 個々の業界に特化した情報共有だけでなく、ICTの業界相互（テレコム、放送、セキュリティベンダー、インターネット機器ベンダー等）の情報共有を可能として、今までにないハイレベルでかつトータル的なISAC活動を推進する唯一の組織として活動を推進

会員企業（33社）（2017年4月1日現在）

理事長（代表理事）：齊藤忠夫（東京大学名誉教授）

理事：篠原弘道（NTT），中尾康二（KDDI）　監事：田中啓仁（KDDI）　顧問：飯塚久夫

通信系(15)	日本電信電話株式会社，KDDI株式会社 ソフトバンク株式会社，株式会社インターネットイニシアティブ，NTTコミュニケーションズ株式会社，ビッグローブ株式会社，ソニーネットワークコミュニケーションズ株式会社，株式会社NTTドコモ，株式会社ケイ・オプティコム，ニフティ株式会社，東日本電信電話株式会社，西日本電信電話株式会社 インターネットマルチフィード株式会社，NTTデータ先端技術株式会社，株式会社KDDI総合研究所
放送系(7)	日本放送協会,株式会社ジュピターテレコム 日本テレビ放送網株式会社，株式会社 TBSテレビ，株式会社フジテレビジョン，株式会社テレビ朝日，株式会社テレビ東京
セキュリティベンダー系(7)	NRIセキュアテクノロジーズ株式会社、NTTセキュリティ・ジャパン株式会社 株式会社FFRI，株式会社カスペルスキー,株式会社シマンテック,株式会社サイバーディフェンス研究所,トレンドマイクロ株式会社
SI・ベンダー系(4)	日本電気株式会社，富士通株式会社，株式会社日立製作所，沖電気工業株式会社

＜オブザーバー＞
総務省（MIC），国立研究開発法人 情報通信研究機構(NICT),一般社団法人 電気通信事業者協会（TCA），
一般社団法人 テレコムサービス協会,一般社団法人 日本インターネットプロバイダ協会（JAIPA），
一般財団法人 日本データ通信協会(JADAC)，一般社団法人 日本民間放送連盟（JBA)

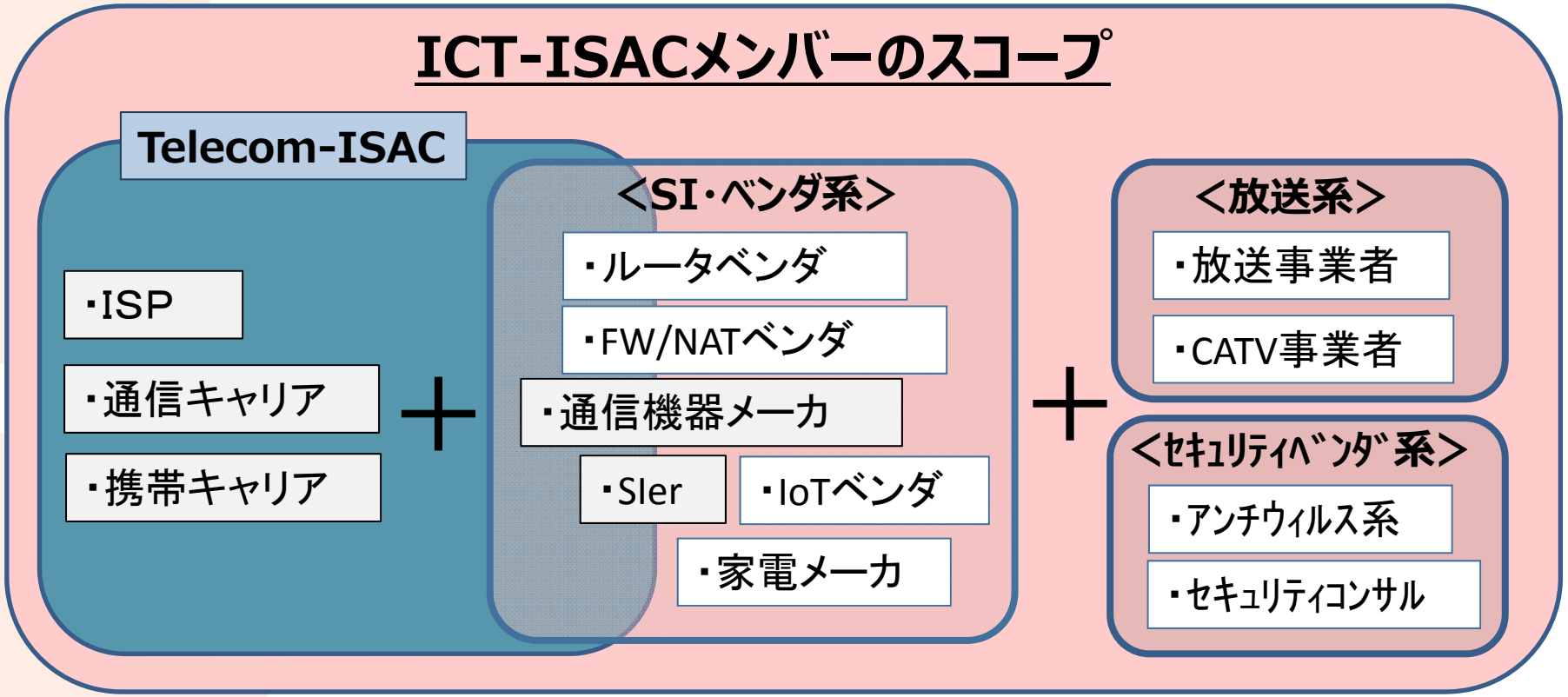
ICT-ISAC会員構成（会員区分別）

33社（2017年4月1日現在）

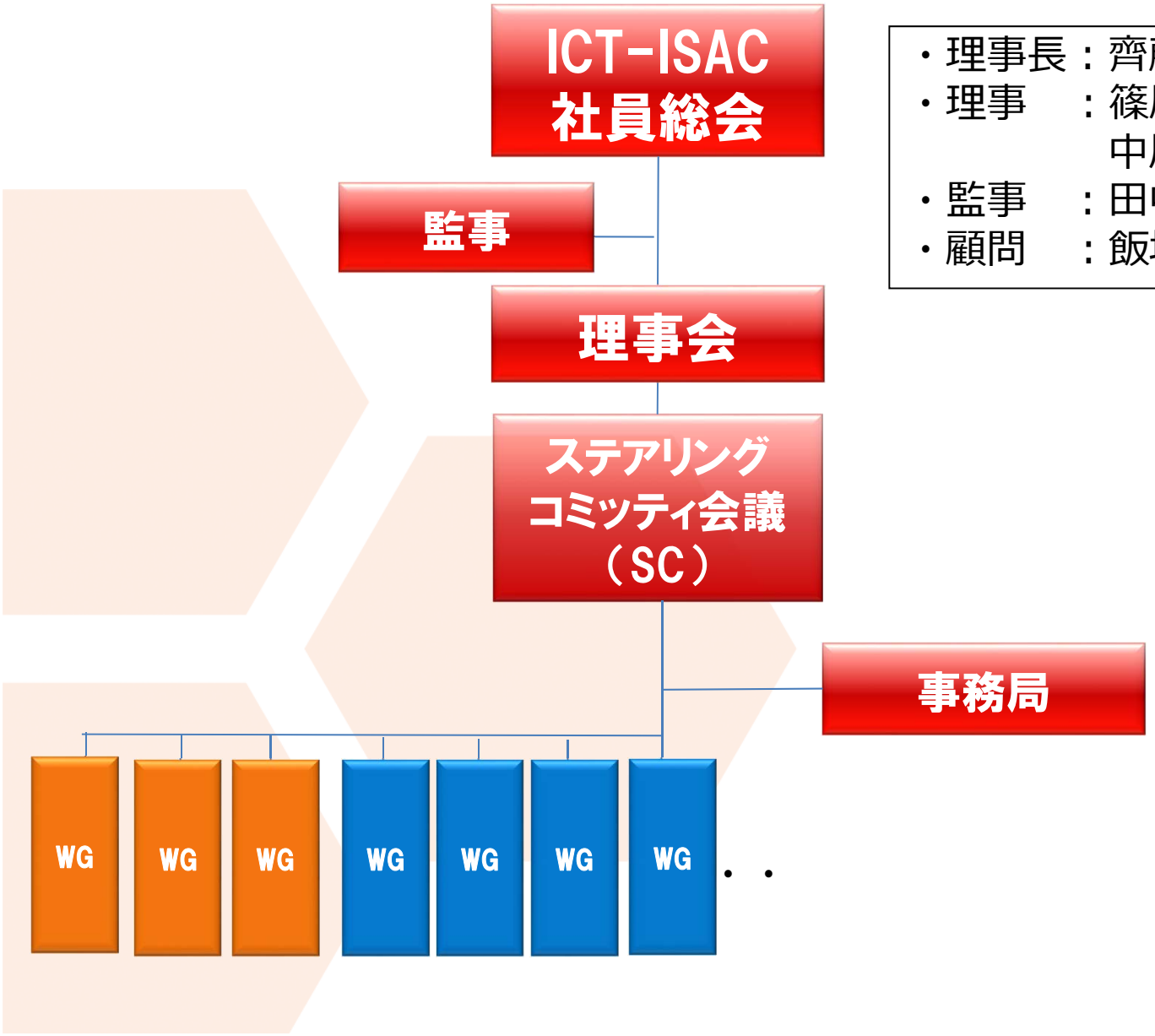
	通信系	放送系	セキュリティベンダー系	SI・ベンダー系
プラチナ会員	・日本電信電話株式会社 ・KDDI株式会社			
ゴールド会員	・NTTコミュニケーションズ株式会社 ・株式会社インターネットイニシアティブ ・株式会社NTTドコモ ・株式会社ケイ・オプティコム ・ソニーネットワークコミュニケーションズ株式会社 ・ソフトバンク株式会社 ・西日本電信電話株式会社 ・ニフティ株式会社 ・東日本電信電話株式会社 ・ビッグローブ株式会社	・日本放送協会 ・株式会社ジュピターテレコム	・NRIセキュアテクノロジーズ株式会社 ・NTTセキュリティ・ジャパン株式会社	・沖電気工業株式会社 ・株式会社日立製作所 ・日本電気株式会社 ・富士通株式会社
シルバー会員	・インターネットマルチフィード株式会社 ・エヌ・ティ・ティデータ先端技術株式会社 ・株式会社KDDI総合研究所			
ブロンズ会員		・株式会社TBSテレビ ・株式会社テレビ朝日 ・株式会社テレビ東京 ・株式会社フジテレビジョン ・日本テレビ放送網株式会社	・株式会社FFRI ・株式会社カスペルスキー ・株式会社シマンテック ・株式会社サイバーディフェンス研究所 ・トレンドマイクロ株式会社	

ICT-ISACのメンバーのスコープ

- 益々、厳しさを増すサイバーセキュリティ環境に対応するためには、通信事業者の視点を中心としたテレコム・アイザック活動では必ずしも十分ではない。
- そのため、「ICT-ISAC」にて、IoT機器の製造事業や放送事業等に関わるICTのステークフォルダーを取り込んだ、高度化した情報共有、及び分析・対応の仕組みを構築し、情報セキュリティにトータル的に対応できる枠組みを実現



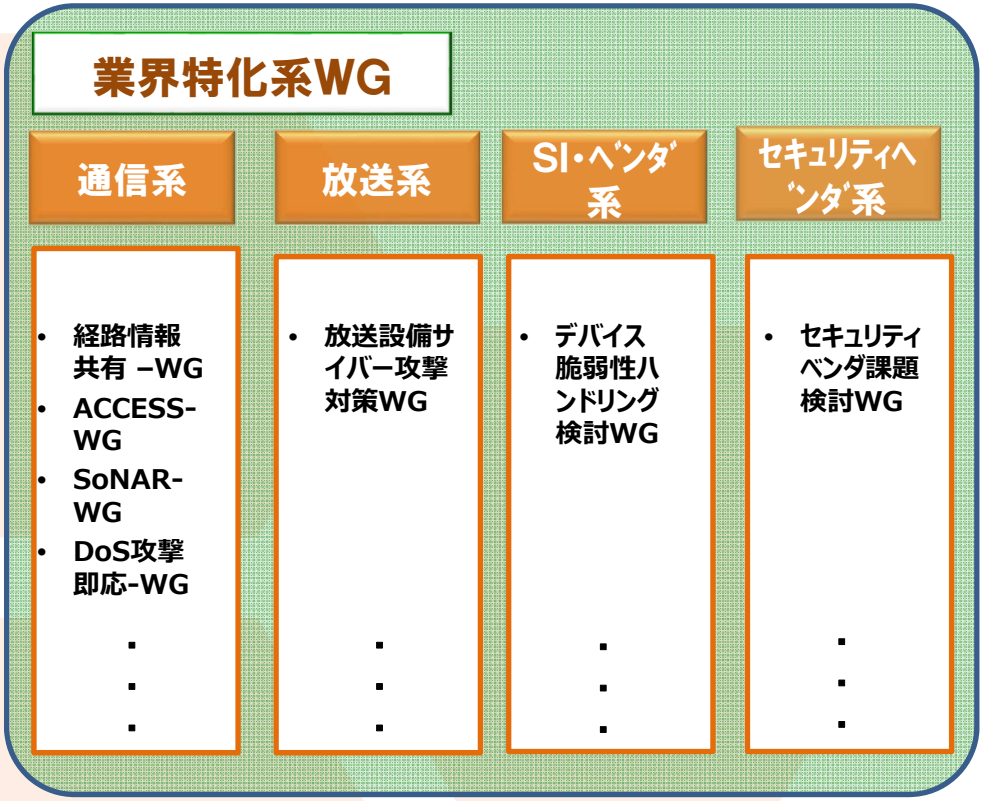
ICT-ISACの組織体制

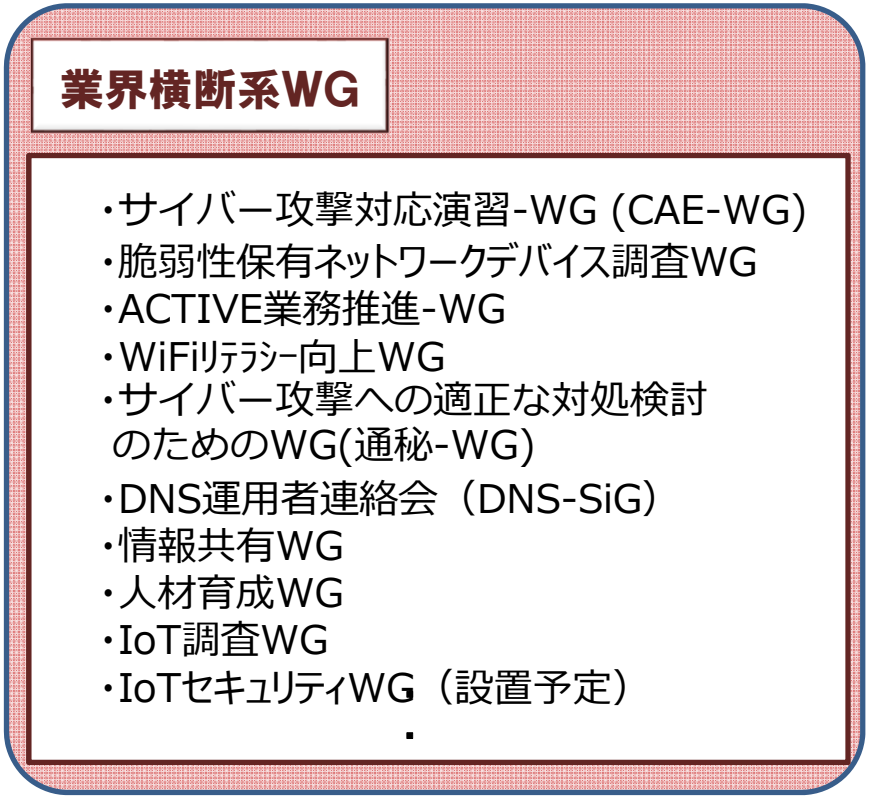


・理事長：齊藤忠夫
・理事　：篠原弘道（NTT）
　　中尾康二（KDDI）
・監事　：田中啓仁（KDDI）
・顧問　：飯塚久夫

ICT-ISACのWG

- WGは、業界特化系と業界横断系に分かれる。





新WGの紹介：放送系WGの概要

放送設備サイバー攻撃対策WG　2016年10月発足

- **参加企業（NHKおよび在京キー民放5社）**
  株式会社 TBSテレビ（WG主査），日本放送協会（WG副主査），
  日本テレビ放送網株式会社，株式会社テレビ朝日，株式会社フジテレビジョン，株式会社テレビ東京
- **活動目的**
  2020年東京オリンピック・パラリンピックの成功には、放送網のセキュリティ強化が欠かせない。
  放送事業者が設備を導入する際に指針となる「放送設備セキュリティガイドライン」の作成とガバナンスの確立を早期に実現したい。その準備段階としてICT-ISACを拠点に、放送系WGの場で主要放送機器メーカーへのヒアリング等を行い現状の問題点の把握、信頼関係の構築に努めていきたい。
- **活動テーマ**
  - 東京オリンピック・パラリンピックに向けた放送設備の脅威調査と放送設備セキュリティガイドラインの作成
  - 海外放送局のセキュリティ勉強会
    NHKより欧州の放送局、フランス、イギリスのセキュリティ事情について話を聞く
  - IoTセキュリティ勉強会
    NHKより受像機に関するセキュリティについて話を聞く
  - 「脅威情報共有プラットフォーム装置（仮称）」の活用方法について検討する

新WGの紹介：セキュリティベンダ系WGの概要

セキュリティベンダ課題検討WG　2016年11月発足

参加企業

NRIセキュアテクノロジーズ株式会社（WG主査），
NTTセキュリティ・ジャパン株式会社（WG副主査），
株式会社FFRI，株式会社カスペルスキー,株式会社シマンテック,
株式会社サイバーディフェンス研究所

活動目的

セキュリティベンダ系事業者間での課題の共有、具体的な情報連携を目的として、将来的な他業界（通信・放送・SI/ベンダ）との連携も視野に活動を実施していく。

活動テーマ

- 具体的な課題共有、情報連携方法に関する検討
- 定期的なセキュリティトピックの共有

新WGの紹介：SI・ベンダ系WGの概要

デバイス脆弱性ハンドリング検討WG

2017年1月発足

参加企業

富士通株式会社（WG主査），日本電気株式会社（WG副主査）
株式会社日立製作所, 沖電気工業株式会社

活動目的

IoT時代で活用されるデバイス全般を対象とすることを見据え、汎用的なソフトウェアに限らない各種ソフトウェア、ファームウェア、ハードウェアに内包されたプログラム等でのセキュリティ侵害リスク（脆弱性）のハンドリングについて、対外的に公開することも視野に、その手順の検討を行う。

活動テーマ

- 脆弱性ハンドリングに関する定期的な検討会の開催
  - 国内外の脆弱性ハンドリングに関する事例共有
  - 脆弱性公開プロセスに関する検討
  - ベンダ対応内容の可視化に関する検討

＜参考＞　Telecom-ISAC JapanのWG/SiG

WG

1) ACCESS-WG　2007年4月設置
インターネットアクセスNWサービスの運用品質向上のための情報交換、ベストプラクティス共有や有識者を交えた意見交換

2) SoNAR-WG　2007年12月設置
ネットワークを利用した不正・不法行為対応(ABUSE対応)に関する情報の共有。インシデントの拡大を抑止するフレームワークの策定

3) DoS攻撃即応-WG　2011年10月設置
DoS攻撃への迅速な対応と複数事業者による協調対処の仕組みの検討。日本国内におけるDoS攻撃発生の、予測、早期検出、迅速かつ適切な対応の実現を目指す。

4) ルータ脆弱性問題-WG　2012年07月設置(活動休止中)
危険な脆弱性を保有する特定ルータに対する具体的な対応の検討と調査を実施

5) 脆弱性保有ネットワークデバイス調査-WG　2013年05月設置
国内IPに接続されたネットワークデバイスの脆弱性保有状況の全容把握と調査を実施

6) サイバー攻撃対策WG　2013年12月設置
電気通信事業の業務を整理し通信の秘密に代表される法的な整理を行うことを目的とする

7) 経路情報共有-WG　2005年7月設置
ISP間の経路情報の共有、経路情報異常時の迅速な対応。および経路奉行システムの運用

8) ACTIVE業務推進-WG　2013年07月設置
総務省ACTIVEプロジェクトの施策推進。マルウェアの感染防止、駆除を推進し、より安心・安全なインターネットの実現を目指す

9) WiFiリテラシー向上-WG　2013年09月設置
電波の有効利用(オフロード推進)を目的に、WiFiの利用および設置・運営において障壁となる情報セキュリティ課題の検討、対策の実施

10) サイバー攻撃対応演習-WG(CAE-WG)　2009年5月設置
電気通信事業者等の参加する、サイバー攻撃を想定した対応演習の企画、実施

SiG

DNS運用者連絡会-SiG　2008年6月設置
DNSに関わる、脆弱性対応・情報の共有、DNSSEC化に備えた情報交換

ICT-ISACにおける情報共有WGの活動

情報共有WGリーダー
寺田真敏（日立）

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

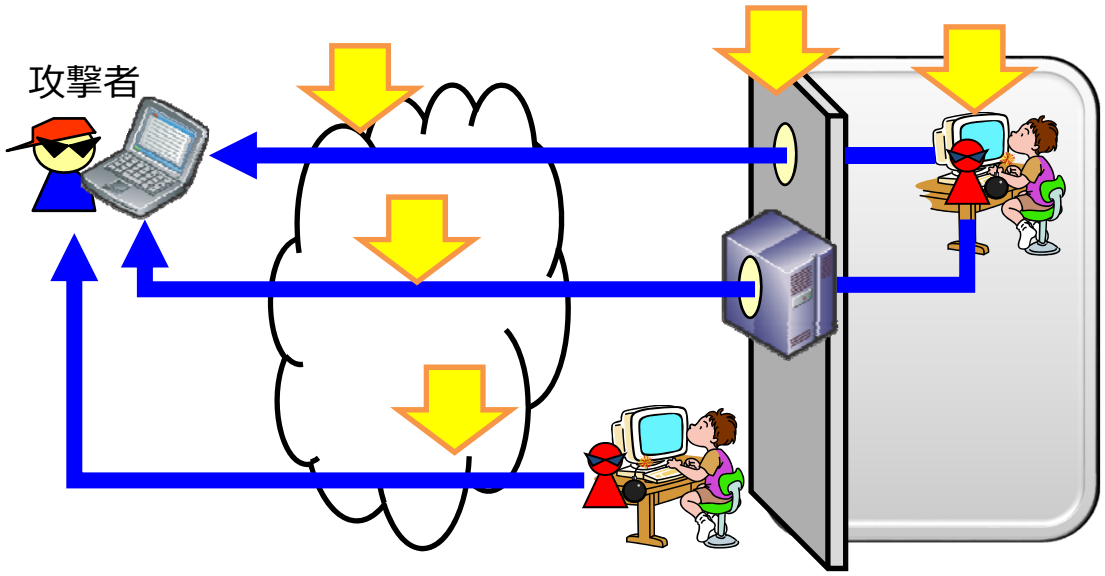
新ICT-ISACにおける活動の構想

- TF01:情報収集・調査・分析
- TF02:情報共有
  - ✓ TF02a:ISAC間(国際間)連携
    → 「情報共有WG」の設置へ
  - ✓ TF02b:ICT-ISAC内連携
  - ✓ TF02c:テストベッド(NICT)連携
- TF03:普及啓発・人材育成
- TF04:ガイドライン・法制度

情報共有のための構想

多層防御としての(情報活用＋対策)

- **不正な接続先のフィルタリング機構**
  - ✓ ICT-ISACという(情報活用＋対策)仕組みを用いた総合的なフィルタリング機構の実現・・・エンドポイント、組織境界、ISPでのフィルタリング機構
  - ✓ 国内の感染端末、不正接続先所有者への対策依頼通知



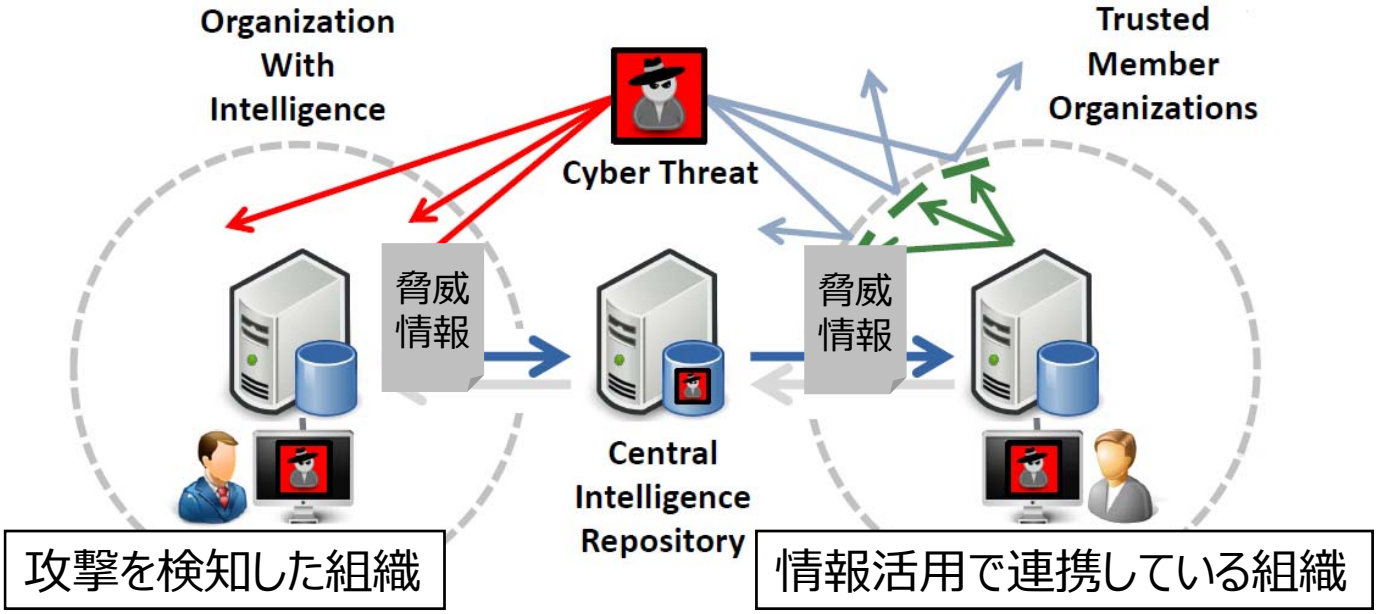
効果

標的型攻撃だけではなく、
一般ユーザを対象とした
サイバーセキュリティ対策
を包含できる可能性あり

情報共有のための構想

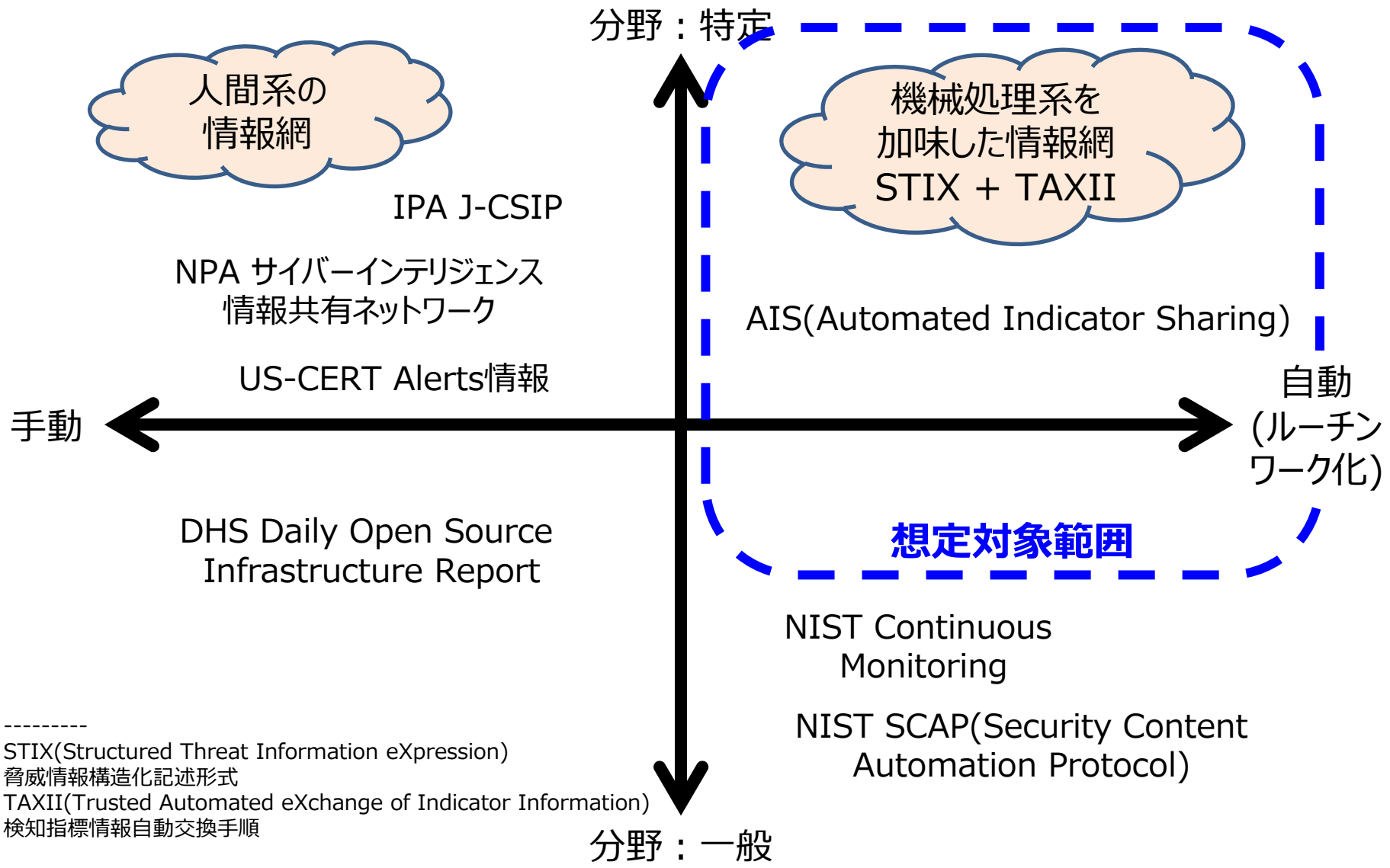
多層防御としての(情報活用＋対策)

- **集団防御のための連携**
  - ✓ 事前措置：組織にサイバー攻撃が行われる前に(入手タイミング)、組織にない情報を利用して(カバー率)、サイバー攻撃対策につなげる。
  - ✓ 事後措置：組織にない情報を利用してサイバー攻撃による影響有無を特定する。



出典：Soltra edge https://forums.soltra.com/index.php?/topic/266-soltra-intro-pdf-deck/

情報活用とルーチンワーク化（１）



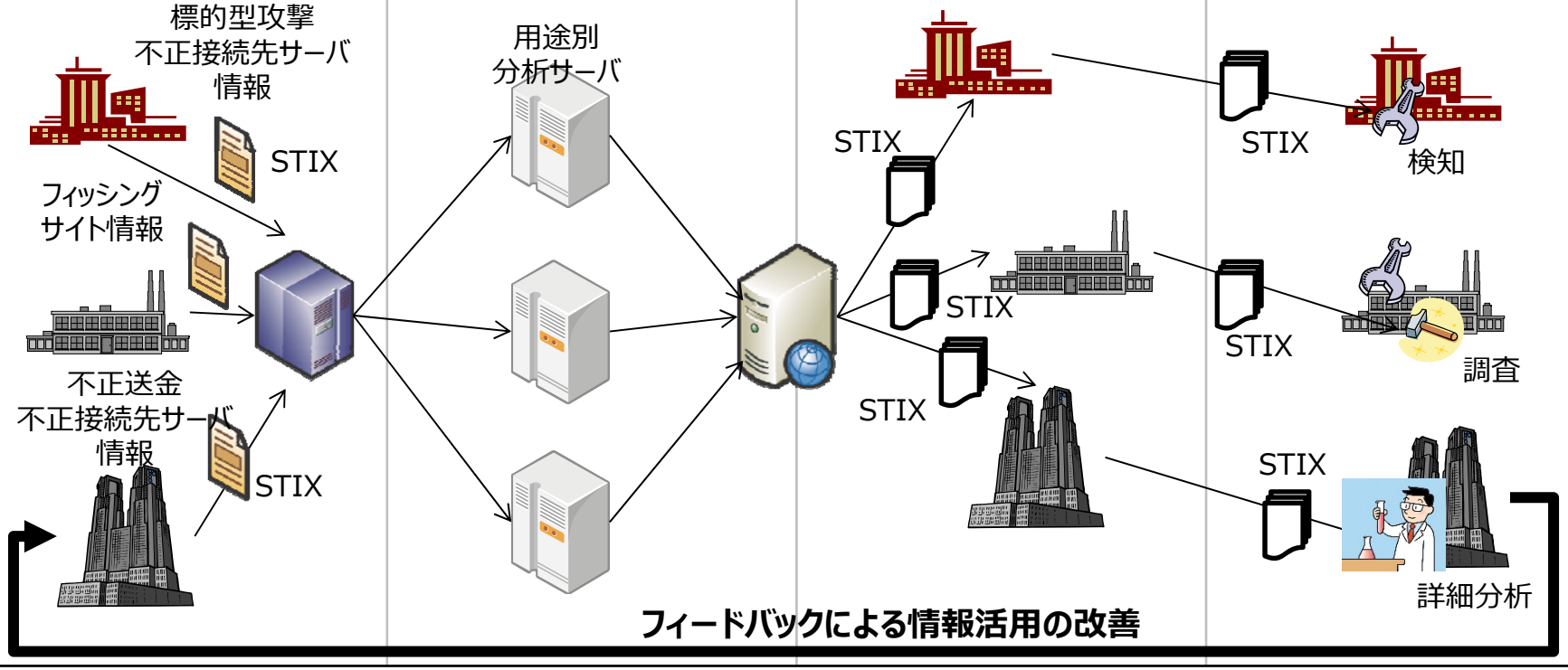
STIX(Structured Threat Information eXpression)
脅威情報構造化記述形式
TAXII(Trusted Automated eXchange of Indicator Information)
検知指標情報自動交換手順

情報活用とルーチンワーク化（２）

情報活用基盤

- 情報活用基盤を収集、分析、配布、適用フェーズに分類

収集	分析	配布	適用
対策を実現するために必要となる情報を各組織から収集するための基盤	対策のために必要となる情報を抽出する分析基盤	対策のために必要となる情報を配布するための基盤	対策のために配布された情報を適用し、検知、分析などの対策を具体化するための基盤



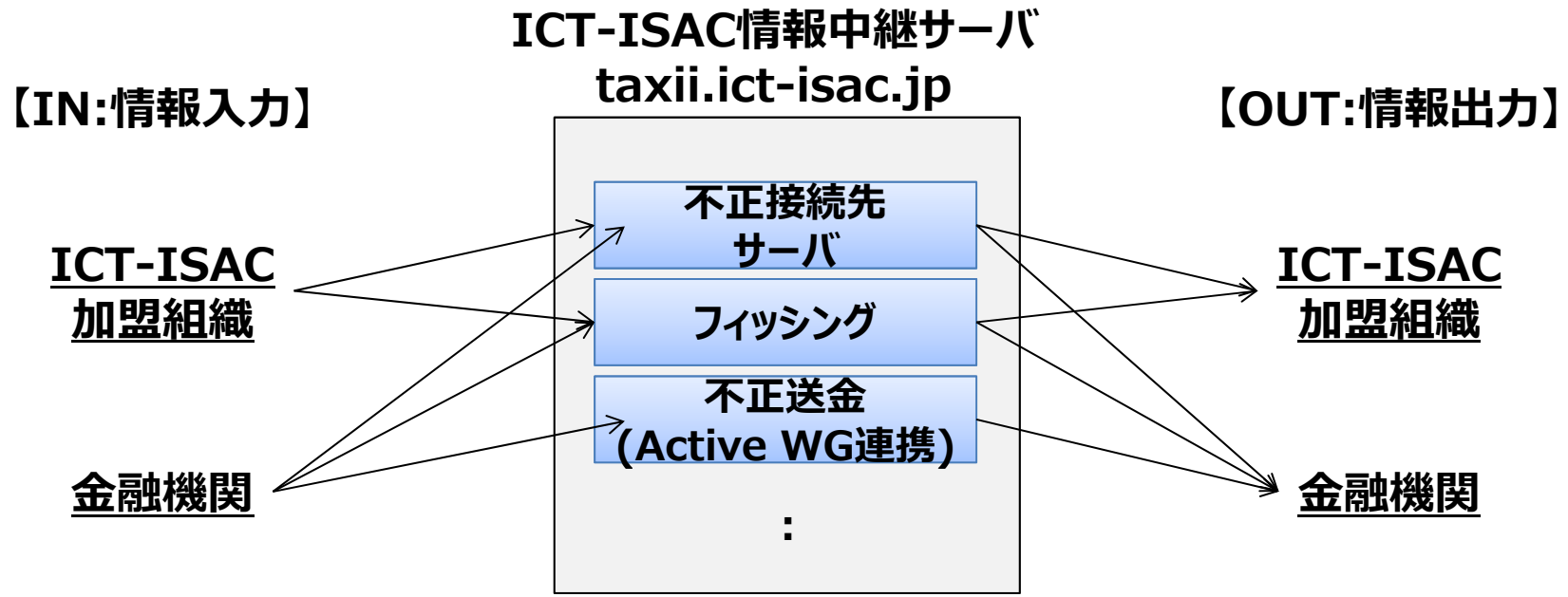
情報共有（活用）における課題

- **人手を介した連携vsシステムを介した連携(攻撃者の活動スピードへの追従するには)**
  - ✓ 人手を介した連携(人間系の情報網、human readable型)：高度な情報分析は可能ではあるが、情報を持っていても、即時的な対処につなげられない。
  - ✓ システムを介した連携(機械処理系を加味した情報網、machine readable型)：高度な情報分析はできないが、情報があれば、即時的な対処につなげられる。人手で処理する場合、その人の技量によってしまう。ゆえに、**技量によって左右されないシステム化を追及する必要がある。**

- **組織間の情報共有（活用）の有効性**
  - ✓ サイバーセキュリティに関する組織間での情報共有（活用）の必要性が説かれるものの、そのための運用上の課題等によりなかなか進展しない。**組織間での情報活用の有効性、並びに、どのような情報であれば、障壁なく情報活用を実現できるかを明らかにしていく必要がある。**

課題解決のために：情報流通基盤の試行整備

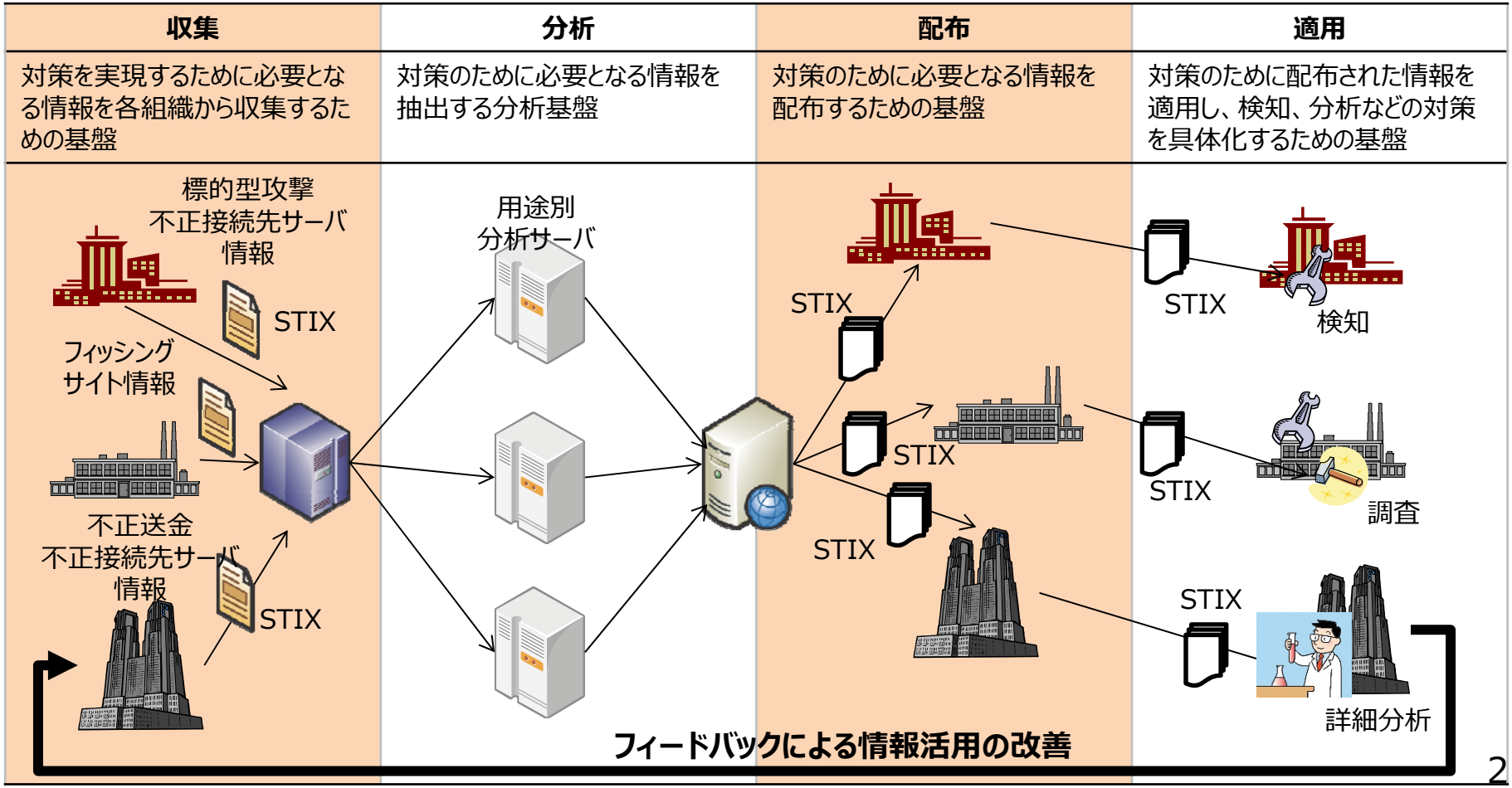
- **人手を介した連携vsシステムを介した連携(攻撃者の活動スピードへの追従)**
  - ✓ **システムを介した連携基盤の試行整備**
    - 対策目的の明確化のため、活用する情報のグループ化
    - 先行する外部組織との協力(金融ISACインテリジェンスWG-インディケータSWGに参加する金融機関に協力を依頼)



連携のための情報流通基盤（１）

情報活用基盤の試行整備

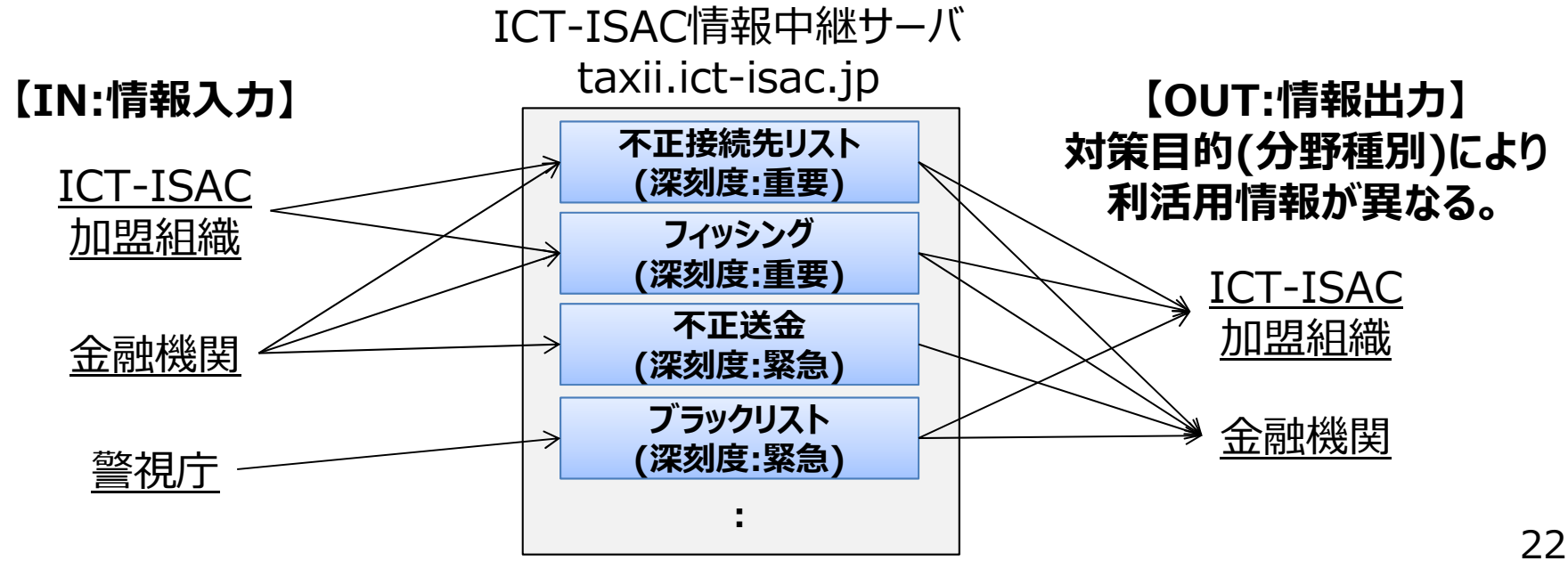
- 試行整備フェーズでは収集と配布に注力



連携のための情報流通基盤（２）

情報活用基盤の試行整備

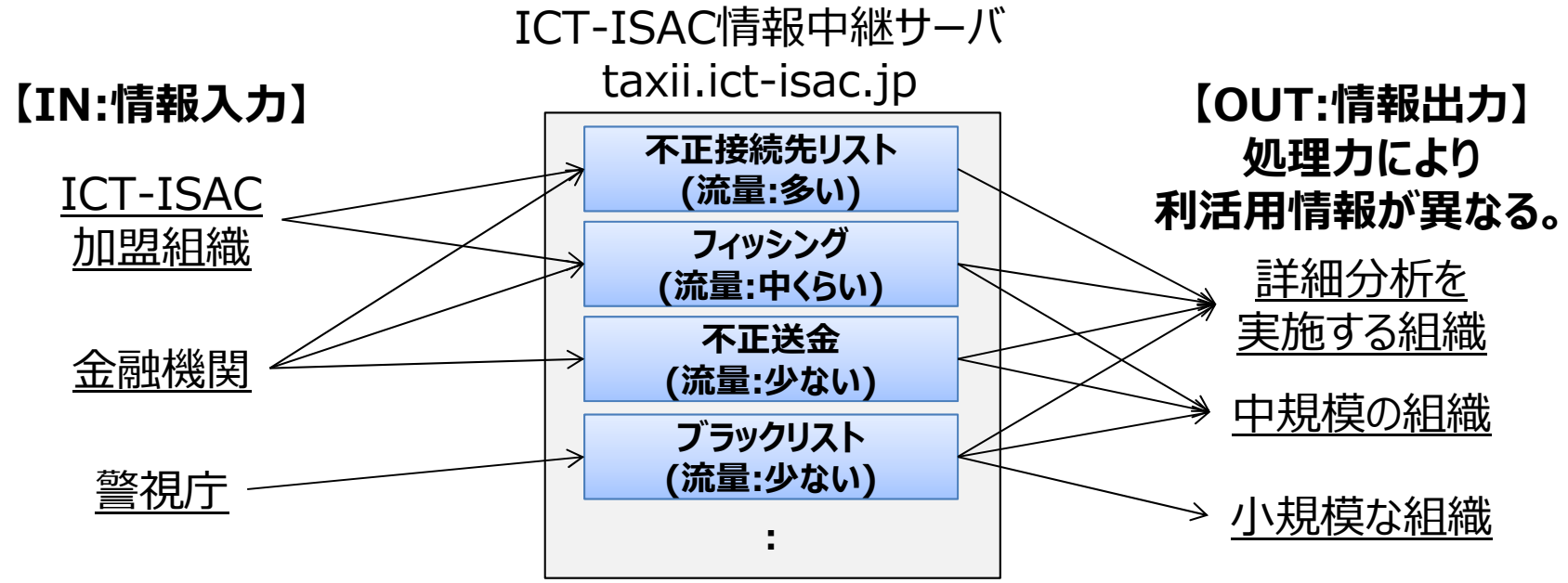
- **サイバー対策で情報を利活用するためには入力から出力までの流れを具体化する必要あり**
  - 先行する外部組織との協力(金融ISACインテリジェンスWG-インディケータSWGに参加する金融機関に協力を依頼)
  - **【質】：利用目的に合わせて、活用する情報のグループ化**



連携のための情報流通基盤（３）

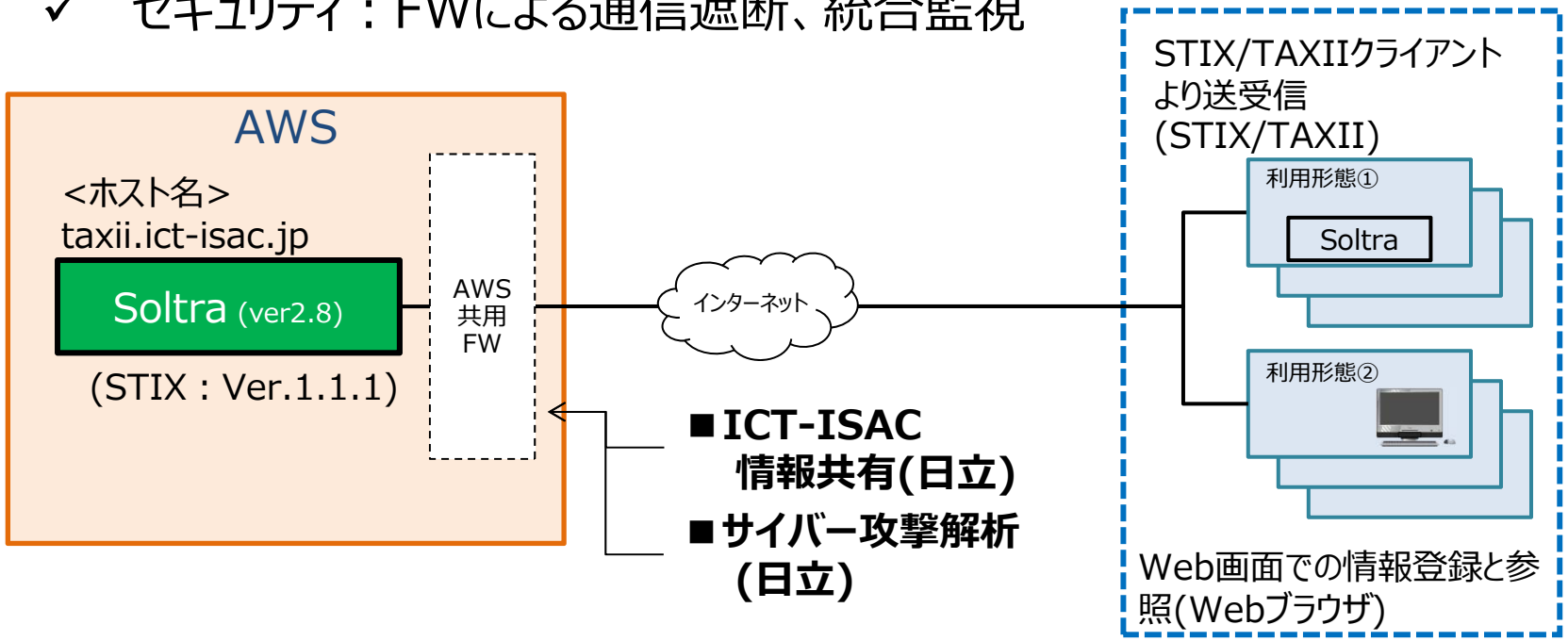
情報活用基盤の試行整備

- **サイバー対策で情報を利活用するためには入力から出力までの流れを具体化する必要あり**
  - 先行する外部組織との協力(金融ISACインテリジェンスWG-インディケータSWGに参加する金融機関に協力を依頼)
  - **【量】：利用目的に合わせて、活用する情報の流量制御**



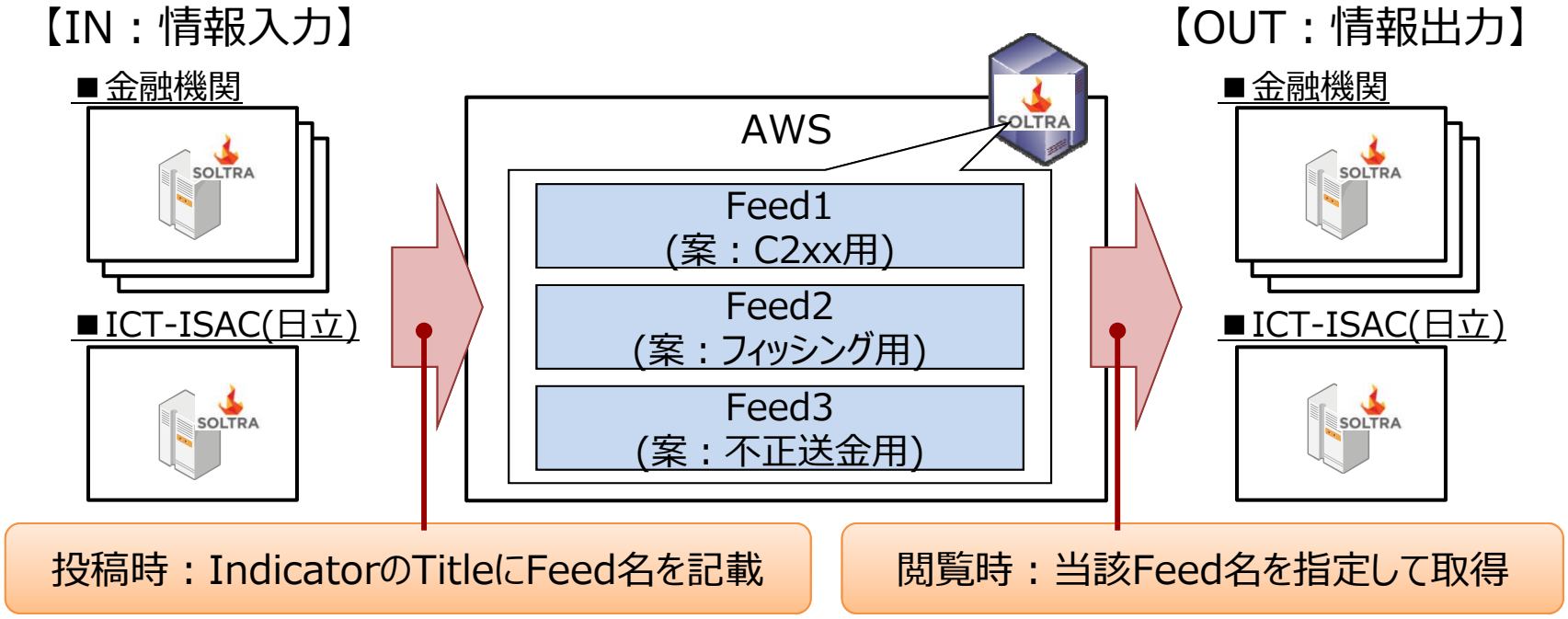
連携のための情報流通基盤（４）

- **試行サイトの基本構成**
  - ✓ AWS上にSoltraを構築し、インターネット公開
    <ドメイン：taxi.ict-iac.jp>
  - ✓ アクセス方法：下記2通り
    ①各組織が構築したSTIX/TAXIIクライアントからデータ送受信(STIX/TAXII)
    ②SoltraのWeb画面から情報登録/参照(Webブラウザ利用)
  - ✓ セキュリティ：FWによる通信遮断、統合監視



連携のための情報流通基盤（５）

- **情報の流通制御**
  - ✓ アクセス制御
    - ✓ IndicatorのTitleにFeed名を記載し、データの振り分けを実施
    - ✓ ユーザをTrustGroupに分類し、各々の権限を設定
  - ✓ データ内容
    - ✓ 試行として「C2」など複数のFeedを用意
    - ✓ 必要に応じてFeedを追加

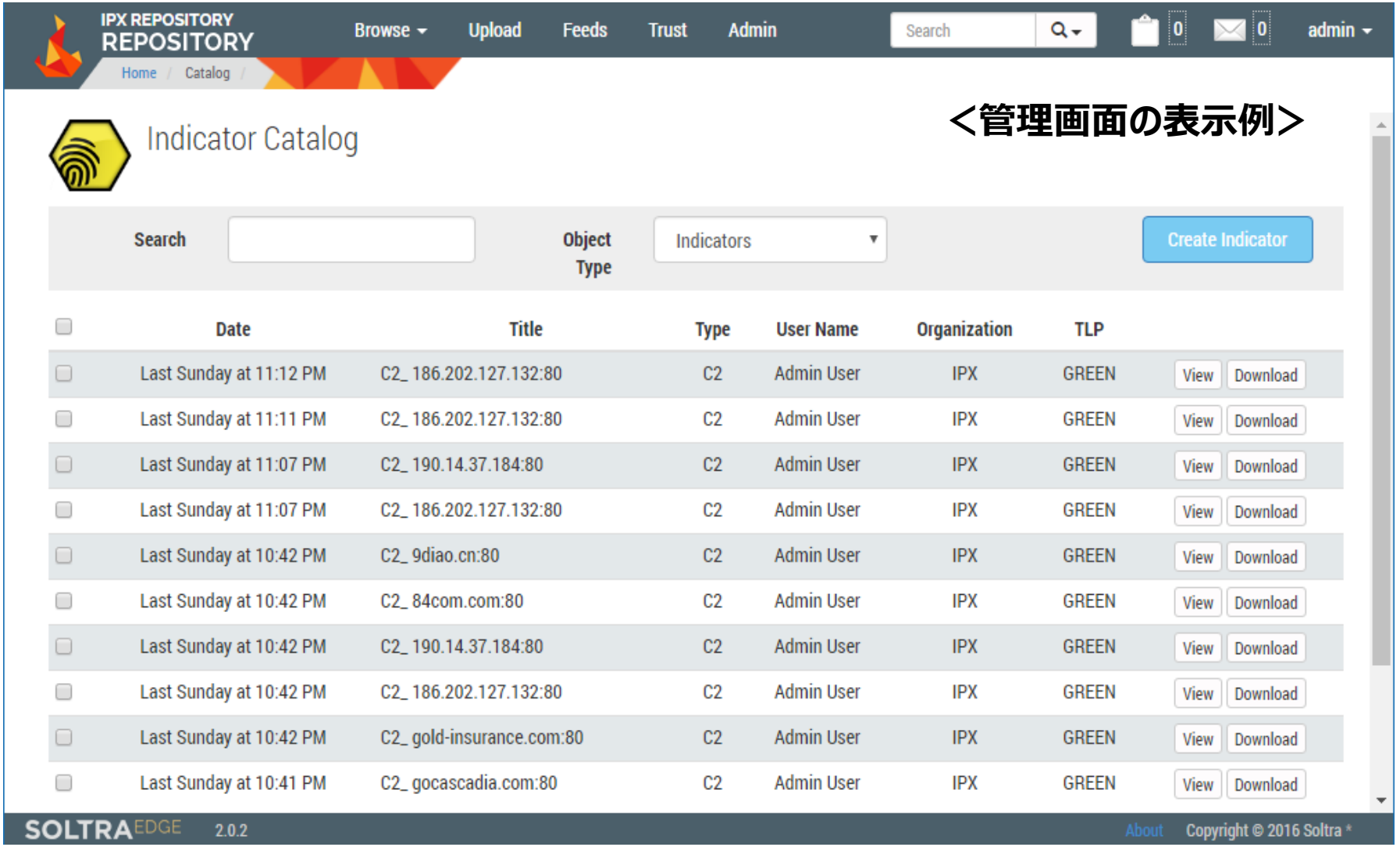


連携のための情報流通基盤（６）

- **taxii.ict-isac.jpの用途別Feed**

#	Feed名	用途
1	Default	すべてのFeedを取得できます。
2	C2	taxii.ict-isac.jpを利用している組織が保有する動的解析装置が検知した不正接続先(IPアドレス、ドメイン、URL)を取得できます。ここで、C2は、ダウンローダサイトを含む広義のC２情報です。
3	CX	接続先解析システムが抽出した不正接続先(IPアドレス、ドメイン、URL)を取得できます。
4	CY	予備(C2サーバの細分化で使用予定)
5	CZ	予備(C2サーバの細分化で使用予定)
6	BKMW_CONFIG	セキュリティベンダから提供されたバンキングマルウェアに関する情報(マルウェアの設定ファイル配布サイトを通知)を取得できます。
7	BKMW_ATTACK	セキュリティベンダから提供されたバンキングマルウェアに関する情報(攻撃対象金融機関サイトを通知)を取得できます。
8	BKMW_MANIP	セキュリティベンダから提供されたバンキングマルウェアに関する情報(マニュピレーションサーバを通知を通知)を取得できます。
9	TEST	テスト用です。

連携のための情報流通基盤（７）



課題解決のために：流通基盤活用の指標化

- **組織間の情報活用の有効性**
  - ✓ 情報共有（活用）の有効性検証として、動的解析装置のアラート情報、詳細情報を使用して、脅威データ(不正ファイルのハッシュ値、不正な接続先)の重なり度合(カバー率)と検知時刻(入手タイミング)の状況を明らかにするための「指標化」が必要

  - ✓ 調査項目
    - ➢ マルウェアのハッシュ値
    - ➢ マルウェア検知日時
    - ➢ 不正接続先サーバのIPアドレス/ドメイン名
    - ➢ 不正接続先サーバのポート番号

情報流通基盤を活用した指標化（１）

国内の攻撃活動基盤の状況把握のための指標化

- 現時点で、攻撃者が日本国内に構築したC2サーバなどの攻撃活動基盤を把握することができていない。
  - サイバークリーンセンターでは、ハニーポットを利用して、能動的に攻撃を仕掛けるボットの検知と駆除のための通知を実施した。
  - 情報流通基盤では、ハニーポットの代わりに、各組織が検知したマルウェアの接続先(C2など)情報を利用する。これにより、サイバー攻撃に関与するサイトの検知と駆除のための通知が可能となる。

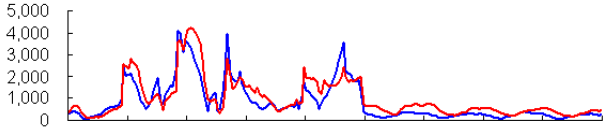
- さらに、各国毎に、各国内の攻撃活動基盤を把握するという取り組みにつなげることができる。
  ＜注＞すでに、サイバーグリーン(インターネット全体の健全性とリスクを各国／地域間で比較可能にする指標)という取り組みはあるが、具体的な対策につなげるための指標化にまでは至っていない。

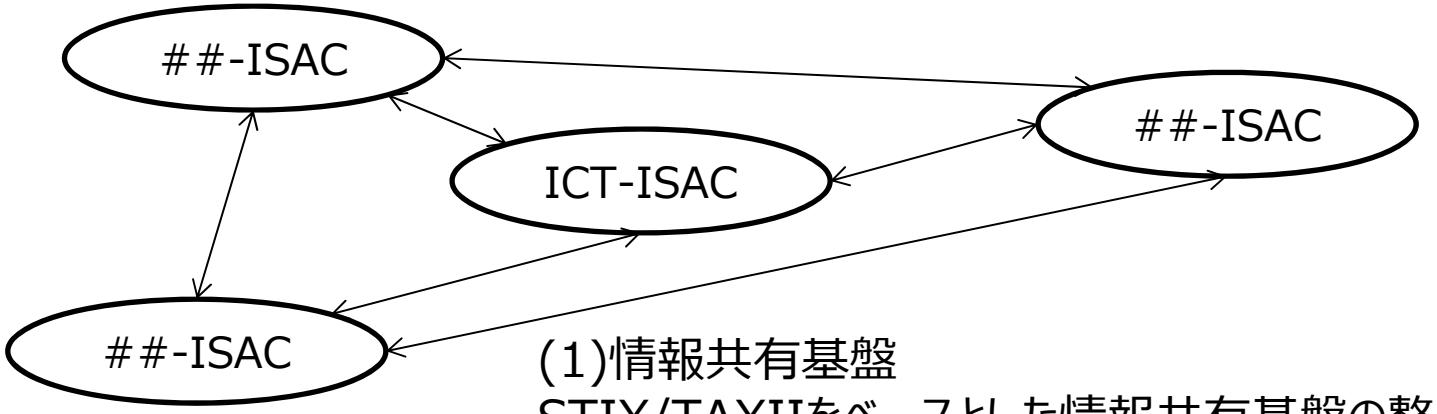
情報流通基盤を活用した指標化（２）

具体的な対策につなげるための指標化

- 情報共有を通して、C2サーバ、フィッシングサイトを把握する仕組みを整備する。
  (1)情報共有基盤の整備
  (2)情報共有基盤を利用した具体的な対策につなげるための指標化

(2)具体的な対策につなげるための指標化
日々発見されるC2サーバ、
フィッシングサイトの件数など



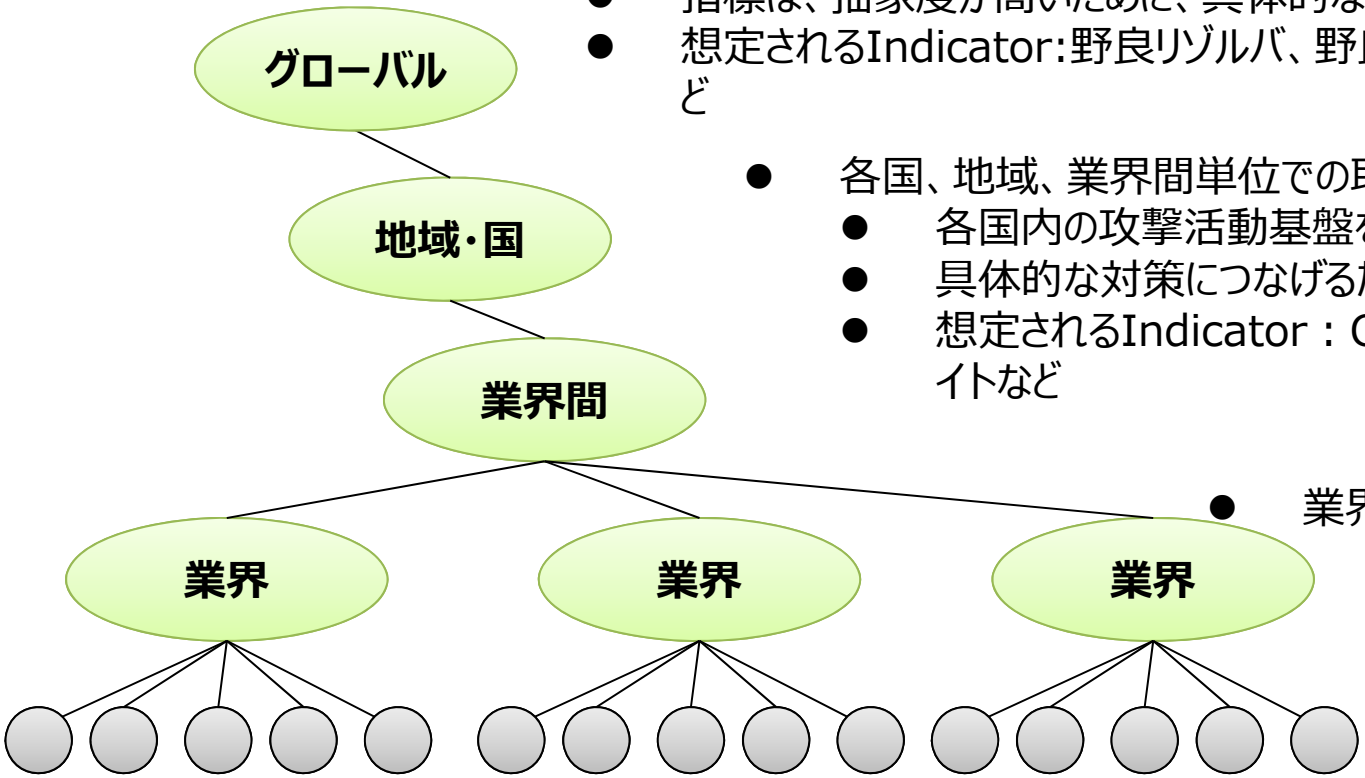


(1)情報共有基盤
STIX/TAXIIをベースとした情報共有基盤の整備

情報流通基盤を活用した指標化（３）

各種取り組みの整理

- インターネット全体での取り組み
  - インターネット全体の健全性とリスクを各国／地域間で比較可能にする指標
  - 指標は、抽象度が高いために、具体的な対策につながりにくい
  - 想定されるIndicator:野良リゾルバ、野良NTP、野良SSDPなど



- 各国、地域、業界間単位での取り組み
  - 各国内の攻撃活動基盤を把握する
  - 具体的な対策につなげるための指標化
  - 想定されるIndicator：C2サーバ、フィッシングサイトなど
- 業界単位での取り組み

情報共有WGの始動

- **活動目的**

国際連携、ISAC間連携、ICT-ISAC内での情報活用のあり方など、大局的な取り組みについての検討

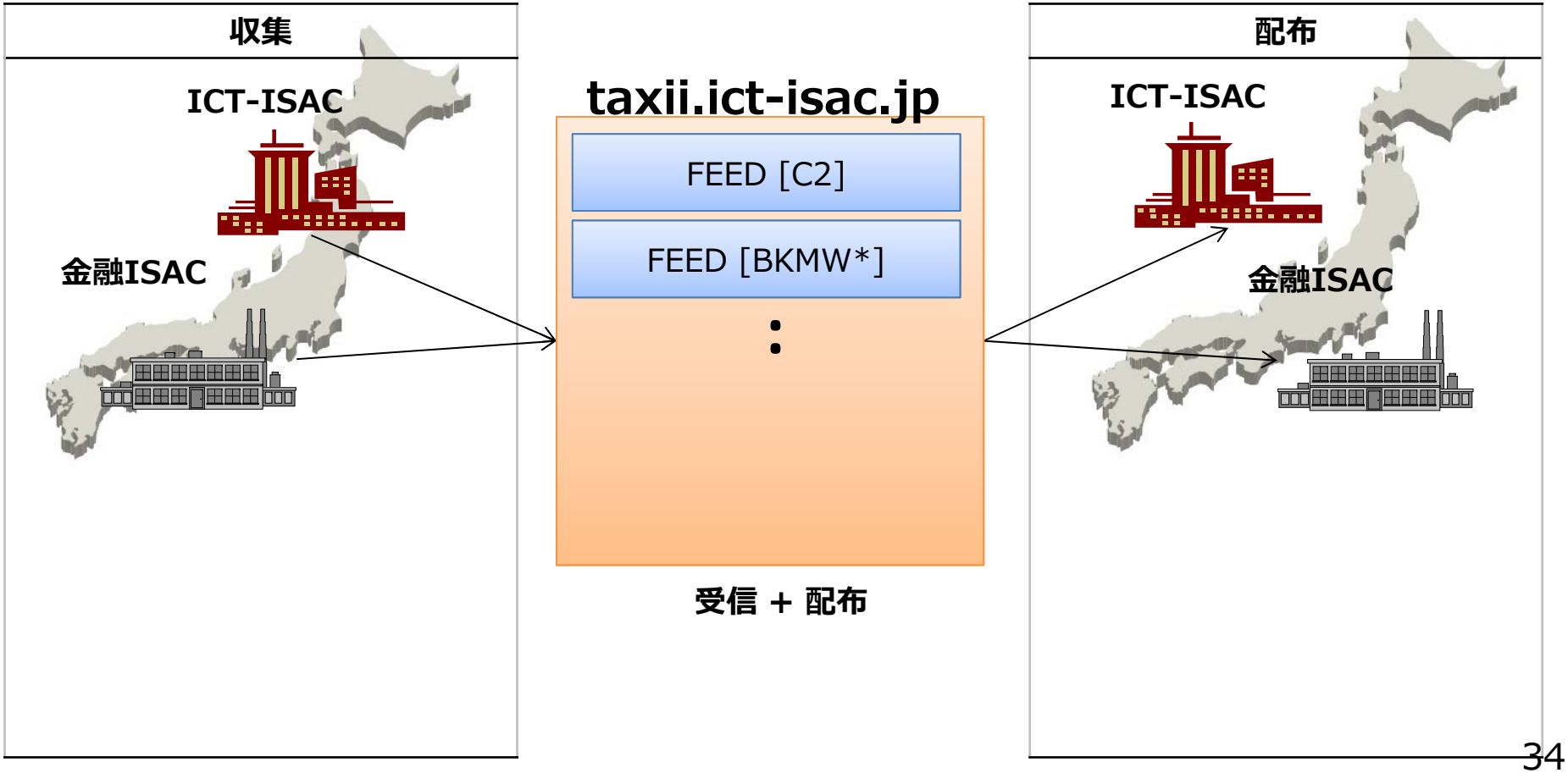
- **活動内容(予定)**
  - ✓ ISAC間連携で推進してきた活動の継続
    - ➢ システムを介した連携基盤の試行整備
    - ➢ 情報活用の有効性検証
  - ✓ ISAC間(国際間)連携の具体化
  - ✓ ICT-ISAC内連携として、システムを介した連携基盤への既存データ(Active WGなど)のインポート

情報活用基盤の今後の計画

情報活用基盤の展開

現状

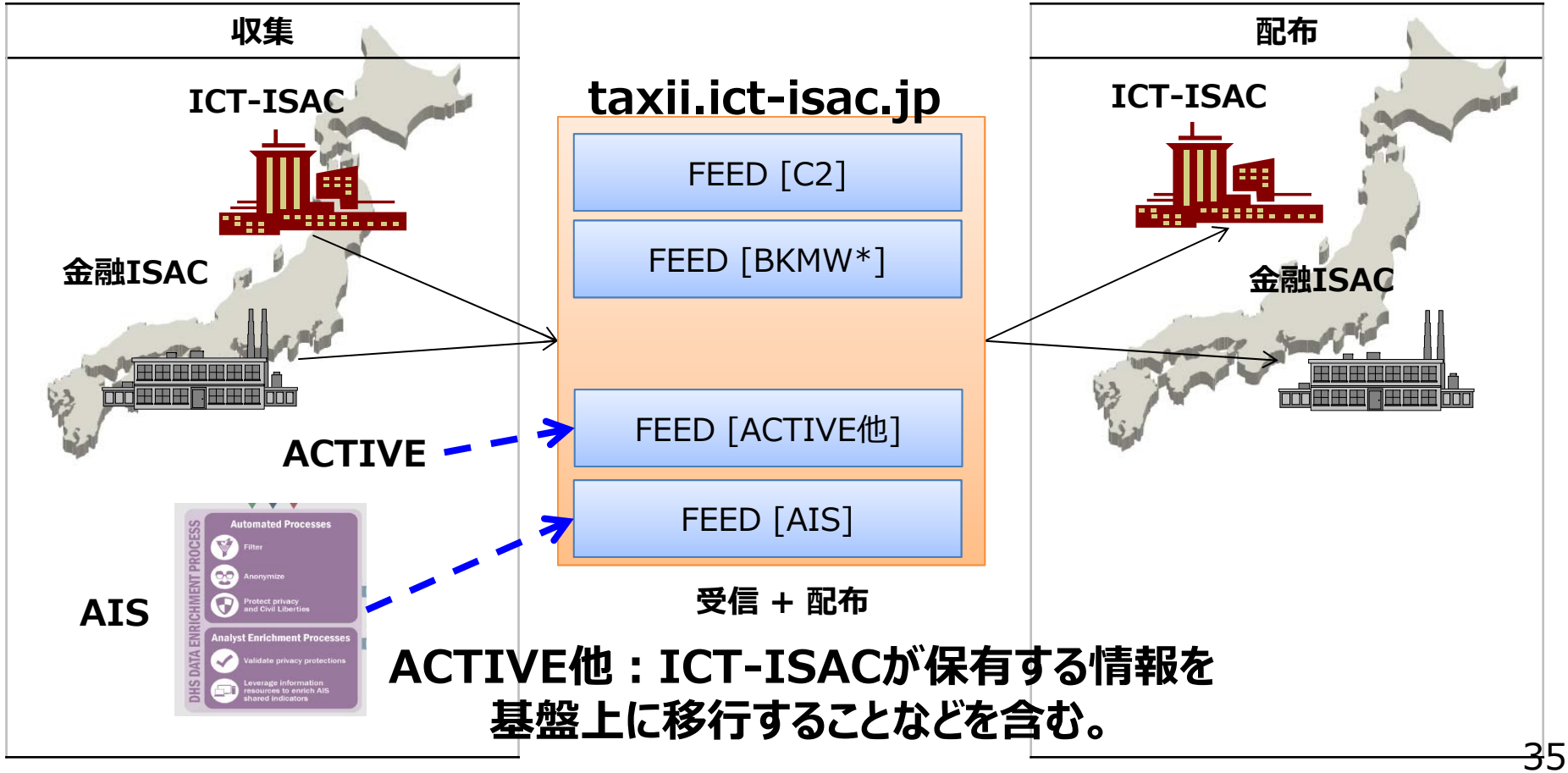
- 指標化と情報活用の普及



情報活用基盤の展開

入力情報の拡大

- 指標化と情報活用の普及

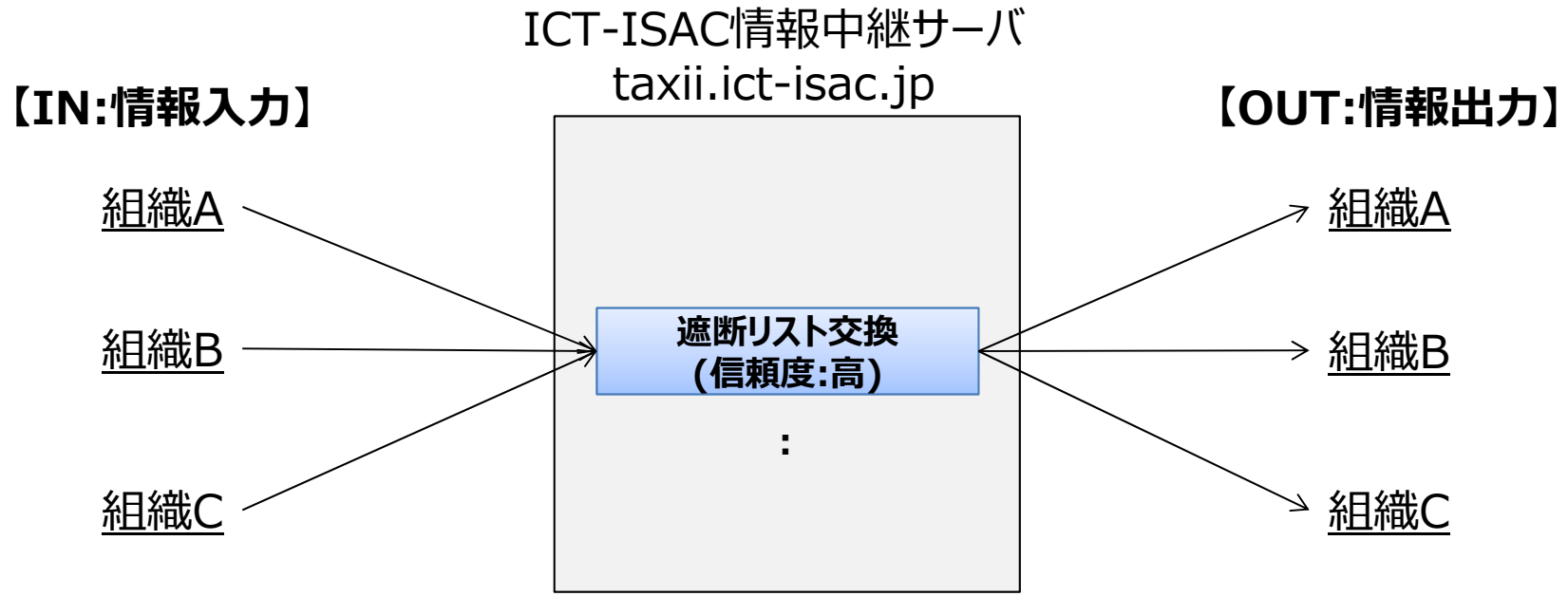


ACTIVE他：ICT-ISACが保有する情報を基盤上に移行することなどを含む。

情報活用基盤の展開

組織で適用している不正接続先遮断リスト交換

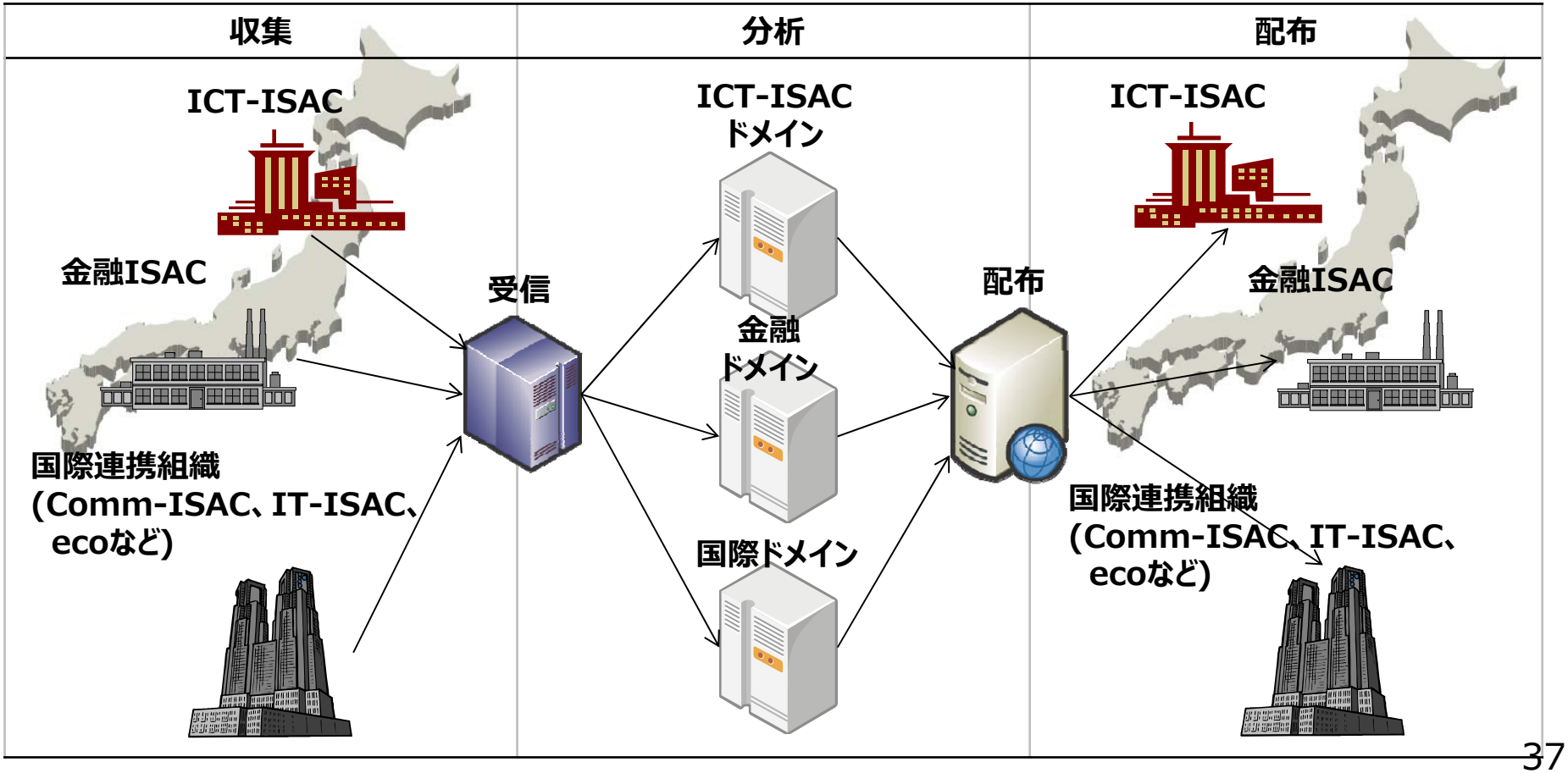
- 各組織で適用している不正接続先遮断リストを交換する。
  (1)システムを介した連携により、人手の工数を低減できる。
  (2)【質】：各組織で適用しているため、データの信頼度は高い。



情報活用基盤の展開

情報活用基盤を利用した分析

- 分析による情報活用の高度化



国際連携に関する活動の紹介

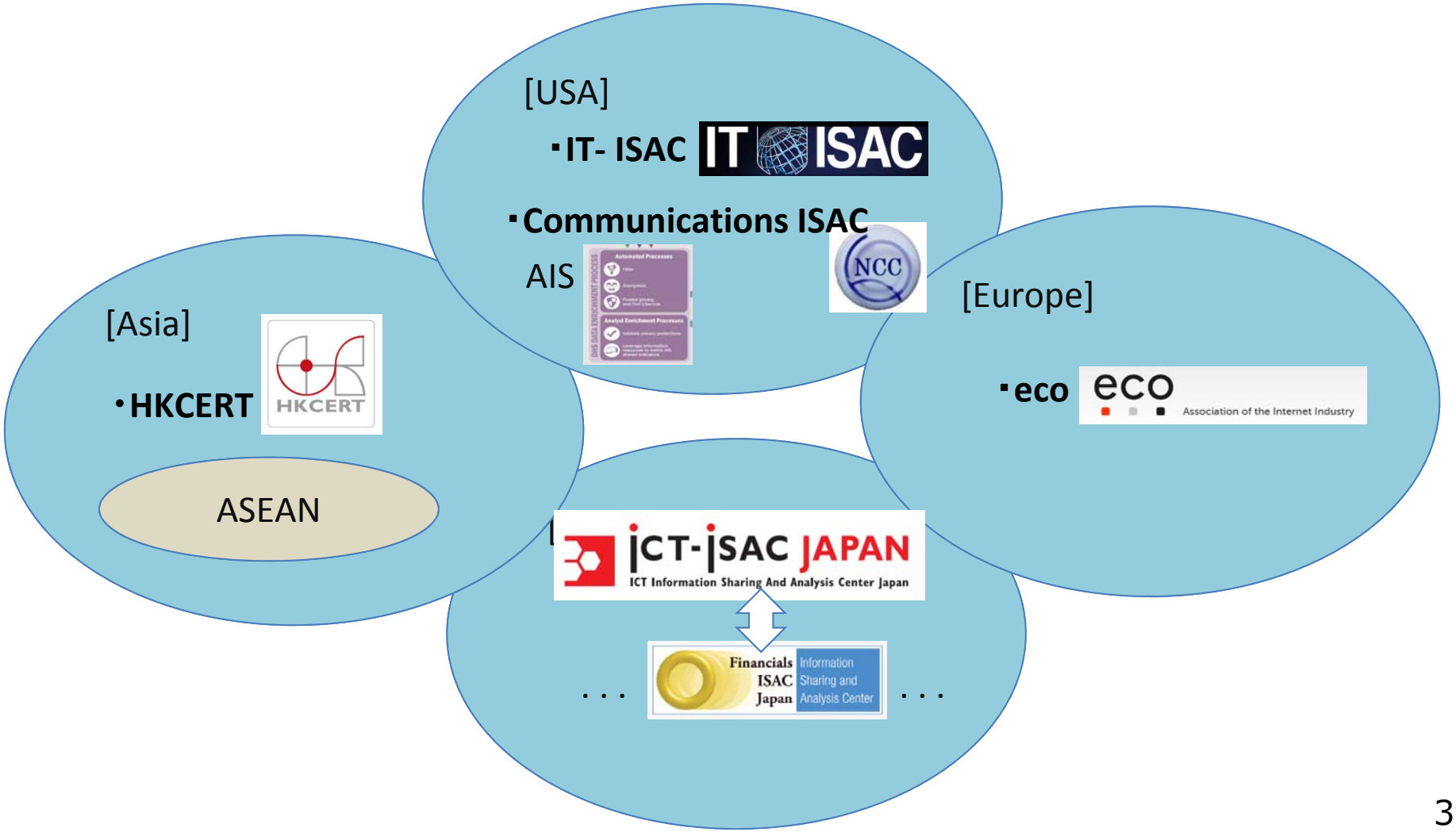
１）情報連携（ICT-ISAC）
２）日ASEANワークショップ（ICT-ISAC）

３）研究と関係した国際連携（NICT)

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

１）情報活用基盤の国際的な展開

情報活用基盤を利用した国際連携



２）日ASEANワークショップによる国際連携

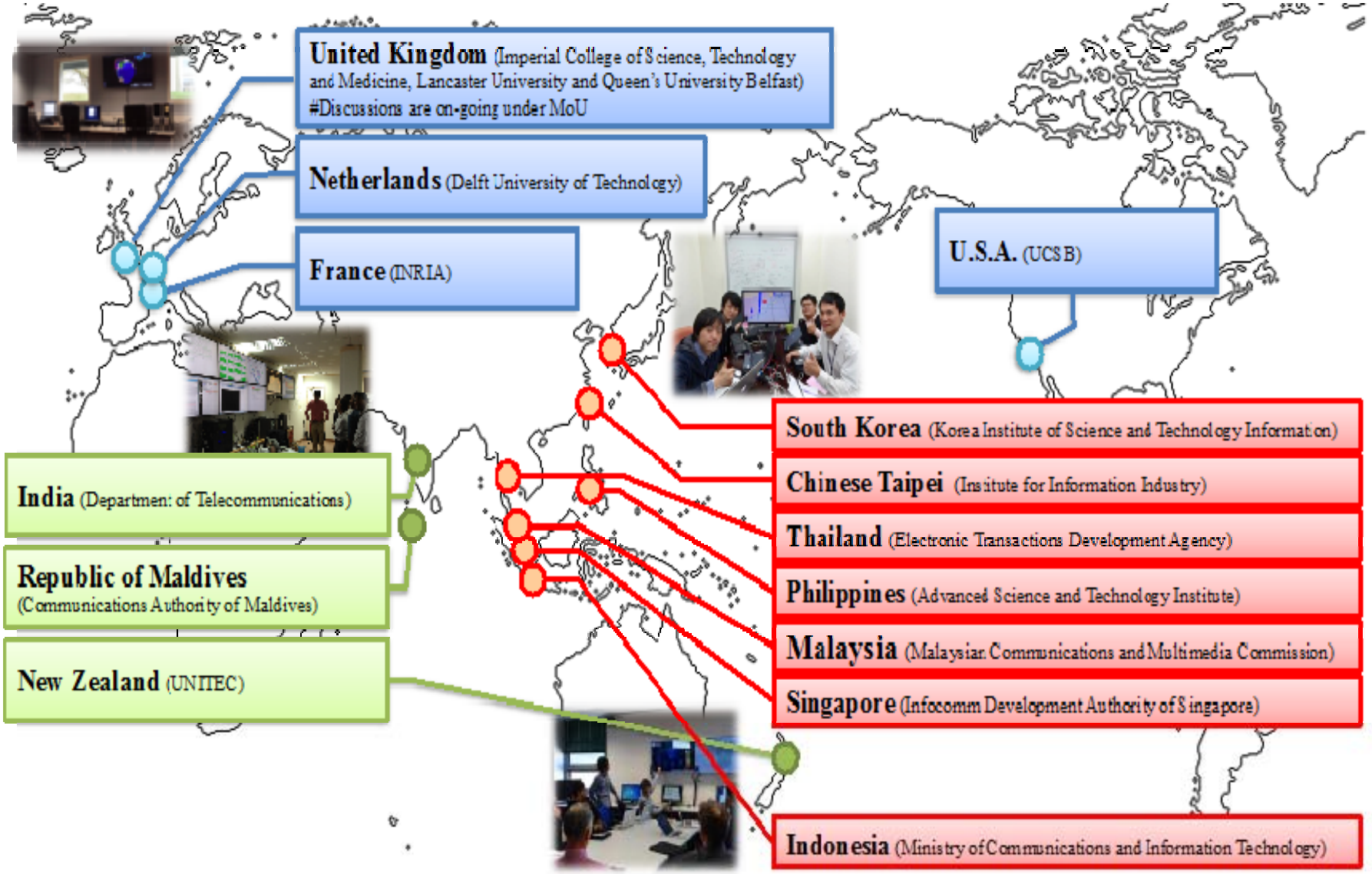
１）2010年より毎年ワークショップを開催
２）目的：「情報交換」及び「情報共有」
３）ワークショップの構成
・各国（ASEANと日本）からの現状報告
・最もドミナントな話題（たとえばDDoS）の搾り出しと情報共有のための今後のアクション

＜たとえば＞
- ✓ 共有の方法：ML，SNS，Webポータルなどの活用
- ✓ 共有すべき情報：「DDoS攻撃情報」、「マルウェアに関する情報」、「APT攻撃に関する情報」、「サイバー攻撃の早期警戒情報（旧PRACTICEなど）」、「インシデントに関する情報」、「ベストプラクティス、ガイドライン」

４）情報共有構造のアンバランス性（日本：情報提供、ASEAN：受ける国）による国際連携が活性化されていないのが現状
５）日ASEAN合同サイバー演習の実施

日ASEANワークショップ（日本開催：2015）

3）研究と関連した国際連携（NICTの場合）



今後取り組むべき施策

１）情報共有のための施策

- ISACによる情報流通基盤の試行整備
  →IT-ISAC(米国）などとの連携推進
- 情報流通基盤の活用のための施策：指標化などの推進
- 基盤入力に向けた情報源の拡充（研究）の推進

２）国際連携のための施策

- 連携のための両国（双方）の効果検証（Give & Takeの関係構築）
- 情報共有施策の活用（上記）
- アウトカムの整理とその活用方法（各国）の推進
- 研究に関する国際連携の場合（共同研究論文、共同解析、システム共有化、共同標準化など）

３）国際標準化（連携推進のための）

Thank you for the attention



2020年東京オリパラまでに、何をしておくべきか

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan