資料４

ICT-ISACの取組について

2020年1月29日

一般社団法人 ICT-ISAC
運営委員長
小山 覚

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

アジェンダ

1. はじめに、ISACと情報共有について
2. ICT-ISACの概要について
3. 国内外ISACとの連携について
   - 国内外ISAC連携WG
   - 情報共有WG
   - サイバーセキュリティ協議会WG
4. 民間から見た官民情報共有の期待と課題

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

はじめに、ISACと情報共有について

ISAC（ Information Sharing and Analysis Center ）とは

- 発祥地はアメリカ（1998年）
- 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、重要インフラを構成する民間の各業種において設置が促されたのが始まり
- リスクを軽減し、回復力を高めるため、実行可能な脅威情報を収集・分析し、共有する
- 日本では2002年発足の通信分野のTelecom-ISACが初、ICT-ISACに活動を継承し現在に至る

情報共有とは

- 「情報共有」は、リスクマネジメントの活動の一環
  - 参加メンバは、情報共有によって、早期の警報等を得る/提供できる（状況認識を高度化するためのツール）
- 民間が行える最も費用対効果が高い防御手法
- 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
  - 他のメンバからの提供情報により、他の方々の経験、状況を学ぶ
  - 組織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（2発目の攻撃から業界全体を守る）
  - 組織は、協業者、パートナー、競争業者のセキュリティに役立つ

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

民間から見た官民情報共有の課題と期待

ICT-ISAC JAPAN

例えば、サプライチェーン全体を守る情報共有のあるべき姿(Why)を共有して、ギャップ分析と打ち手(What)の検討が必要ではないか？

現状：情報共有への一般的な期待

1. 単独組織のみでは収集できない様々な情報が共有されることで、脅威を俯瞰的に把握することができる
2. 新たな被害を未然に防ぐことができる
3. データやノウハウの蓄積と利活用を促進できる

サプライチェーンを守る情報共有のあるべき姿とは？（What）

- 各省庁の果たすべき役割
- サプライチェーンの頂点企業の役割
- サプライチェーン関係者の役割
- 情報共有基盤は誰が整備する？
- 国際連携の強化

?

整理すべき課題：Howの課題？

1. 情報共有を行う共有内容（何を共有するか？）
   A) Indicatorsの共有
   B) それぞれの組織の戦略の共有（ISAC間、または国の間などで活用される共有方法）
   C) ベストプラクティスの共有（例：ICT-ISACの放送ガイドラインなど）
2. 情報共有を行う相手（誰と共有するか？相手は信頼できるか？）
3. 情報共有の方法（どのような手法を用いるか？）
   - 自動化（STIX/TAXII）
   - 匿名化処理
4. 情報の信頼性（どの程度信頼できるか？）
5. 情報取得の合法性（法に触れないか？）
   - 通信の秘密（電気通信事業法）、プライバシー法、不正アクセス禁止法などとの関係
6. 情報の適用範囲、活用（どのように使うか？）
7. 情報共有のメリット（特に情報を提供する側にメリットは？）

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

アジェンダ

1. はじめに、ISACと情報共有について
2. ICT-ISACの概要について
3. 国内外ISACとの連携について
   - 国内外ISAC連携WG
   - 情報共有WG
   - サイバーセキュリティ協議会WG

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

ICT-ISACの目的

【ICT-ISACの目的】

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

５．認定協会業務

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）としての活動

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

ICT-ISACの概要

- 2002年7月に通信事業者の商用サービスの安全かつ安心な運用の確立を目的に日本で最初のISAC、Telecom-ISAC Japan発足
- 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ICT-ISAC発足
- 2016年6月に通信事業者に大手放送事業者、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

理事長（代表理事）：齊藤忠夫（東京大学名誉教授）
理事： 井伊基之（NTT） 内田義昭（KDDI） 監事：田中啓仁（KDDI） 顧問：飯塚久夫、中尾康二

会員42社	通信系(21)	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、株式会社オプテージ、株式会社日本レジストリサービス、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、株式会社KDDI総合研究所、アルテリア・ネットワークス株式会社、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QTnet、株式会社NTTエムイー、株式会社朝日ネット、日本ネットワークイネイブラー株式会社
	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(10)	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、マカフィー株式会社、KDDIデジタルセキュリティ株式会社、パロアルトネットワークス株式会社、日商エレクトロニクス株式会社
	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、国立研究開発法人 情報通信研究機構、一般社団法人電気通信事業者協会、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、一般財団法人日本データ通信協会、一般社団法人日本民間放送連盟、一般社団法人日本ケーブルテレビ連盟

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

ICT-ISACの会員構成のスコープ

- 通信事業者の商用サービスの安全かつ安心な運用の確立を目的に、Telecom-ISAC Japan発足
- 益々、厳しさを増すサイバーセキュリティ環境のもとで、安定した情報流通、情報伝達を維持するためには、通信事業者の視点を中心としたTelecom-ISAC活動では必ずしも十分ではない。
- そのため、放送事業者、IoT機器製造事業者、セキュリティベンダー等の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

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

ISAC活動の中心となるWG活動

様々なWG活動を通じてICT社会の会員企業に貢献している

- 業界特化系WGと業界横断系WGに大別
- 会員各社が抱える課題を組織を超えて共有・連携

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

ワーキンググループ活動のご紹介

ワーキンググループの名称	活 動 概 要
1. サイバー攻撃対応演習-WG	通信事業者等が参加するサイバー攻撃を想定した対応演習の企画、実施
2. 脆弱性保有ネットワークデバイス調査-WG	国内の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
3. ACTIVE業務推進-WG	総務省ACTIVEプロジェクトの推進（マルウェアの感染防止や駆除を推進）
4. WiFiリテラシー向上-WG	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への取り組み
5. 通信の秘密-WG	サイバー攻撃への対処と通信の秘密ガイドライン策定に関する議論や検討
6. 情報共有WG	国際連携やISAC間連携、ISAC内での情報活用のあり方を検討
7. 交流促進-WG	会員向けにノウハウ・知識等の普及・啓発、各WG間の相互理解促進
8. IoTセキュリティWG	IoTのセキュリティ対策について、調査分析・情報共有・議論を行う。
9. CSA-WG	NISCのサイバーセキュリティ協議会に構成員として参加し情報共有の推進を行う。
10. 国内外ISAC連携-WG	海外ISACおよび国内他業界ISACと定期会合を開催し連携を推進する
11. DNS運用者連絡会-SiG	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
12. 若手活躍SiG	ICT-ISACにおいて若手が活躍する場や環境を整え提供し次代を育成する。
13. 経路情報共有-WG	ISP間の経路情報異常時の情報共有と対応。および経路奉行システムの運用
14. ACCESS-WG	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等
15. SoNAR-WG	ネットワークを利用した不正・不法行為対応(ABUSE対応)の情報共有
16. DoS攻撃即応-WG	DoS攻撃の予測や早期検出、複数事業者による協調対処を検討
17. 認定協会業務推進WG	「認定送信型対電気通信設備サイバー攻撃対処協会」業務等の円滑な業務推進を目的
18. NOTICE-SiG	攻撃に悪用される恐れのある機器の調査や注意喚起に関する情報共有
19. 放送設備サイバー攻撃対策WG	放送設備セキュリティガイドラインの策定と現場への浸透
20. デバイス脆弱性ハンドリング検討WG	IoT時代で活用されるデバイス全般を対象に脆弱性ハンドリングの手順検討
21. セキュリティベンダ課題検討WG	各社相互理解、個社または業界共通の課題の検討
22. ５Ｇ セキュリティーSIG	ローカル５Ｇなど最新の取り組みについて勉強会を開催し課題の共有を行う

黄色は1~2年以内に出来たもの

サイバー攻撃を俯瞰的に観測するシステム群

独自のサイバー攻撃観測システムにより、サイバー攻撃の状況を俯瞰的に観測している

DDoS攻撃の監視

重要インフラ観測システム
「無人君」

レスポンス観測システム
「ムジンガーZ」

DRDoS攻撃アラートシステム
「PRACTICE Alert」

経路ハイジャックの調査

経路異常検知システム
「経路奉行」
経路ハイジャック観測

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

経路異常情報

情報共有

実態把握

対策検討

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
「Zakion」
脆弱な機器の調査

サイバー攻撃の状況を把握し、対策に役立てる

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

変わりゆく脅威に官民連携で立ち向かう

ICT-ISAC JAPAN

様々な官民連携プロジェクトを通じてICT社会に貢献する

サイバー攻撃のトレンド

IoTマルウェア

高度で洗練された
マルウェア

ドライブ・バイ・ダウンロード

Bot

ICT-ISACが進める官民連携プロジェクト

NOTICE National Operation Towards IoT Clean Environment

NOTICE 2018~
脆弱なIoT機器への注意喚起
（総務省・NICT）

ACTIVE Advanced Cyber Threats response InitiatiVE

ACTIVE 2013~2018
総合的なマルウェア対策プロジェクト
（総務省）

PRACTICE

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
（総務省）

RDB 2009~2012
悪性サイトの調査研究（総務省）

Cyber Clean Center

Cyber Clean Center 2006~2011
ボットネット対策プロジェクト
（総務省・経済産業省）

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

アジェンダ

1. はじめに、ISACと情報共有について
2. ICT-ISACの概要について
3. 国内外ISACとの連携について
   - 国内外ISAC連携WG
   - 情報共有WG
   - サイバーセキュリティ協議会WG

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

国内外ISAC連携WGの活動のスコープ

- **既に会合実績などのある組織を中心に、連携強化を図る。**
- **また、必要に応じて、総務省などの関係省庁との連携も行う。**

具体的な連携候補

- 米国（IT-ISAC、Communications ISAC、National Council of ISACsなど）
  複数回意見交換会などの会合実績あり
- 国内（金融ISAC、電力ISAC、交通ISAC、ソフトウェアISAC、J-AUTO-ISACなど）
  金融ISACとは情報共有実績あり
  その他ISACとはICT-ISACが中心となりISAC連携会合実績あり（民民会合）
- 欧州諸国（ecoなど）
  2008年よりボットネット対策などで情報共有実績あり
- アジア（ASEAN諸国ISPなど）
  ICT-ISACが総務省と連携し、日ASEAN-WSを計10回開催実績あり

ICT-ISAC会員から構成される国内外ISAC連携-WGで具体的な連携先や連携の形態は議論する。
その他、海外組織向けにはサイバー攻撃演習プログラムの提供なども実施する。

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

ISAC間連携の推進

ICT-ISACは国内及び海外のISAC関連組織との連携を積極的に推進

サイバー攻撃の脅威やICT社会のグローバルで複雑化する中で、一組織のみであらゆる脅威に対処できる時代ではなくなった

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

国内ISAC連携会合の開催

国内ISAC組織と各組織の取組みや課題について情報共有と議論

参加ISAC

ICT-ISAC、金融ISAC、電力ISAC、ソフトウェアISAC、J-AUTO-ISAC

主なテーマ

各ISACの取組み状況アップデート
課題の共有
国内ISAC連携に向けた議論

国内ISAC連携会合開催状況

開催日	会合名
2019年4月15日	第1回国内ISAC連携会合（ホスト：ICT-ISAC）
2019年7月24日	第2回国内ISAC連携会合（ホスト：ICT-ISAC）
2019年9月30日	第3回国内ISAC連携会合（ホスト：金融ISAC）
2020年1月30日（予定）	第4回国内ISAC連携会合（ホスト：電力ISAC）

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

サイバーセキュリティ国際シンポジウムの開催

■名称　「サイバーセキュリティ国際シンポジウム
～情報共有・国際連携のさらなる促進に向けて～」
■主催　総務省、一般社団法人ICT-ISAC
■日時　2019年11月11日（月）13:30 ～ 18:00
■会場　新宿京王プラザホテル　南館　４Ｆ　錦
■対象者　サイバーセキュリティ関係者
■参加者数　170名（申込者）

国内外ISACの参加いただき、
シンポジウムを実施

サイバーセキュリティ国際シンポジウム登壇者及び関係者

ICT-ISACとIT-ISACのMoU調印

- シンポジウムプログラム内でICT-ISACとIT-ISACのMoU調印実施
- 翌11月12日（火）にICT-ISAC及び米国招聘者とクローズドミーティング実施

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

開催プログラム（11月11日）

13:00～13:30	受付
13:30～13:45	開会挨拶 総務省　総務大臣政務官　木村　弥生 ICT-ISAC　理事長　　齊藤　忠夫
13:45～14:00	ICT-ISAC IT-ISAC間の協力に係る覚書の締結 署名者　ICT-ISAC　理事長 齊藤 忠夫 IT-ISAC　エグゼクティブ・ディレクター　Scott Algeier
14:00～14:15	基調講演１ 「IoT・５G時代のサイバーセキュリティ政策」 総務省　サイバーセキュリティ統括官　竹内　芳明
14:15～14；35	基調講演２ 「Examples of Cross Sector Collaboration and its Importance in Critical Infrastructure Resilience」 米国 National Council of ISACs議長　Denise Anderson
14:35～15:35	セッション１ 「日本における各ISACの最新の取組事例について」 進行　ICT-ISAC　顧問　中尾　康二 スピーカー　金融ISAC　専務理事　鎌田　敬介 電力ISAC　事務局次長　綿田　俊介 ソフトウェアISAC　リーダー　萩原　健太 J-AUTO-ISAC　ステアリングコミッティメンバー　中島　一樹 ICT-ISAC　事務局長　引地　信寛
15:35～15:45	休憩
15:45～16:45	セッション２ 「米国における情報共有の仕組みについて」 進行　ICT-ISAC　顧問　中尾　康二 スピーカー　米国 国土安全保障省ディレクター　John O'Connor 米国 Comm-ISACチェアマン　Joe R. Viens 米国 Comm-ISAC　Drew Morin 米国 IT-ISACエグゼクティブ・ディレクター　Scott Algeier
16:45～17:00	休憩
17:00～18:00	ラップアップセッション 「情報共有・国際連携のさらなる促進に向けて」
18:00	閉会

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

日米通信関係ISAC間のMOU締結

- ICT-ISACと米国IT-ISACとの間で、覚書(MOU: Memorandum Of Understanding)を締結（2019年11月11日）
- サイバーセキュリティの確保に向けて国際的な協力関係強化

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

一般社団法人ICT-ISAC

公開サイト

- 理事長挨拶
- 組織概要
- 会員企業
- お知らせ
- 認定協会
- 事務所アクセス
- お問い合わせ
- English

2019年11月11日
一般社団法人ICT-ISAC

日米通信関係ISAC間のMOU締結について

一般社団法人 ICT-ISAC（アイシーティ・アイザック）【所在地：東京都港区、 理事長：齊藤忠夫、 以下、ICT-ISAC Japan】は、国内のISPを含む通信事業者に加え、放送事業者、ソフトウェアベンダー、情報提供サービス事業者、情報関連機器製造事業者等、幅広い分野の会員と連携し、サイバーセキュリティの観点から、安全な情報通信技術（ICT）社会の形成に寄与する活動を推進しております。

このたび、ICT-ISAC Japanは、サイバーセキュリティの確保に向けて国際的な協力関係を築くため、2019年11月11日に東京で開催された「サイバーセキュリティ国際シンポジウム」において、The Information Technology – Information Sharing and Analysis Center（IT-ISAC）との間で、覚書(MOU: Memorandum Of Understanding)を締結いたしました。

サイバーセキュリティを確保するためには、信頼できるパートナーとの連携が必要とされています。今回のMOUは、メンバー交流による信頼関係の構築をはじめ、互いの組織の活動や機微情報の取り扱いに十分に留意した上でサイバーセキュリティに関する各種情報交換等を含むものとなっております。

ICT-ISAC Japanは、今後も信頼できるパートナーとの連携等を行い、通信、放送をはじめとするICTの安定供給に貢献してまいります。

以上

https://www.ict-isac.jp/news/news20191008.html

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

情報共有WG

- **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**
  - ISAC間連携
    - ✓ 【国内】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
    - ✓ 【国際】連携の具体化
  - ICT-ISAC内連携
    - ✓ 情報活用の検討
    - ✓ システムを介した連携基盤の活用
      - ➢ ICT-ISAC保有の既存データ(ACTIVE、PRACTICEなど)のインポート

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

情報共有基盤の構築

STIXTAXII形式でサイバー攻撃に関する情報を交換する情報共有基盤を構築

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

一般社団法人ICT-ISAC

公開サイト

- 理事長挨拶
- 組織概要
- 会員企業
- お知らせ
- 認定協会
- 事務所アクセス
- お問い合わせ
- English

2018年6月29日
一般社団法人ICT-ISAC

サイバー攻撃の防御に向けた情報共有基盤に関する実証事業について

一般社団法人 ICT-ISAC（アイシーティ・アイザック）【所在地：東京都港区、 理事長：齊藤忠夫、 以下、ICT-ISAC Japan】は国内のISPを含む通信事業者に加え、放送事業者、ソフトウェアベンダー、情報提供サービス事業者、情報関連機器製造事業者等、幅広い分野の会員と連携しサイバーセキュリティの観点から安全な情報通信技術（ICT）社会の形成に寄与する活動を推進しております。

サイバー攻撃の高度化・巧妙化に伴い、政府機関や民間企業の情報通信システムへの脅威が深刻化しており、情報通信をはじめとする重要インフラ分野への影響が懸念されています。複雑・巧妙化し続けるサイバー攻撃に対し、被害を最小化するためには、多層防御のひとつの手段として集団防御[1]のための連携、特に、複数組織間においてサイバー攻撃に関する情報を速やかに共有する仕組みを構築し、迅速な対策を講じることが重要です。

このような状況を踏まえ、ICT-ISAC Japanでは、平成28年度及び平成29年度に、総務省と連携し、サイバー攻撃に関する情報を収集・分析・配布する情報共有基盤の試行運用を行う実証事業を行いました。実証事業では、STIX[2]/TAXII[3]形式でサイバー攻撃に関する情報を交換する情報共有基盤を構築し、運用すると共に、事業者向けの脅威情報の情報共有基盤利用ガイドラインを作成しました。

○実証事業の概要
ICT-ISAC サイバー攻撃の防御に向けた情報共有基盤の概要
事業者向け脅威情報の情報共有基盤利用ガイドラインの概要

https://www.ict-isac.jp/news/news20180629.html

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

情報共有WG

- **システムを介した連携基盤(攻撃者の活動スピードへの追従)の整備**
  - 対策目的の明確化のため、活用する情報のグループ化
  - 外部ISAC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、電力ISACに協力を依頼)

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

サイバーセキュリティ協議会-WG

■CSA-WG

- ICT-ISACとしてCS協議会の第二類構成員に参加活動する母体
- 協議会の秘密情報は協議会登録メンバ（二類参加企業で構成）に限定しつつ、WG全体で対応等を議論する体制を構築

■活動の目的

- CS協議会からの情報を起点に、迅速な対応に向けた情報共有、ノウハウ蓄積を行う。
- 会員組織でのCS協議会の参加、不参加に関わらず、WG活動を通じて各社のサイバーセキュリティの対応力向上を目指す。

■参加組織（2020年1月時点）

- 個社でCS協議会（二類）参加：9社
- 個社でCS協議会未参加：5社

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

サイバーセキュリティ協議会-WG 活動内容

- CS協議会からの情報に基づく情報共有活動と、その活動を通じた事例共有、分析についてのノウハウを蓄積する。
- ICT-ISACの他のWG等とも連携を図ることで、ICT-ISAC全体としての相乗効果を図る。

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.

ICT-ISAC JAPAN

ICT-ISAC JAPAN

ICT Information Sharing And Analysis Center Japan

Copyright©2020 ICT-ISAC Japan. All Rights Reserved.