資料17－4

ISACを活用する情報共有について

2019年11月２２日

一般社団法人ICT-ISAC
NICT
中尾　康二

ICT-ISAC JAPAN
ICT Information Sharing And Analysis Center Japan

Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

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

Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

IT-SAC（米国）の場合

ISACのミッション

Grow a diverse community of companies that leverage information technology and have in common a commitment to cyber-security; to serve as a force multiplier that enables collaboration and sharing of relevant, actionable cyber threat information and effective security policies and practices for the benefit of all.

情報技術を活用し、サイバーセキュリティに対し、共通な立場でコミットしている企業の多様なコミュニティを成長させることを目指します。関連する実用的なサイバー脅威情報の共有と連携、およびすべての利益のための効果的なセキュリティポリシーと実践を可能にする力の相乗効果をもって、機能させます。

Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

特に、情報共有は（IT-ISACより）：

- **「情報共有」は、リスクマネジメントの活動の一環**
  - 情報共有は、situational awarenessを高度化するためのツール
  - 参加の皆さんは、情報共有によって、早期の警報等を得る/提供できる
- **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
  - 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
- **サイバー規制のリスクが増大する時代になってきている**
  - ブランド、資産、顧客、従業員、IPを保護する参加組織のコミットメントを利害関係者に示す
  - 自発的に行動するか、規制の命令を受け入れる

Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

競争業者と情報を共有するメリット

- 自分のビジネスに対する脅威を共有する。共有される脅威は、連携防御のための機会となる。
- 自分の組織が見えている攻撃と同じ攻撃を他組織も見ているため、お互いから学ぶ姿勢が重要
- 自組織も他組織も異なる攻撃者を監視している。相互利益のために監視結果のリソースを貯めていくことが重要。
- 攻撃者が自分の競争業者をうまく倒したとしても、次は自分の会社にその攻撃が来る可能性が高い。

Turn the competitor into a partner!

Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

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
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©2019 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

会員企業（42社）　（2019年10月7日現在）

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

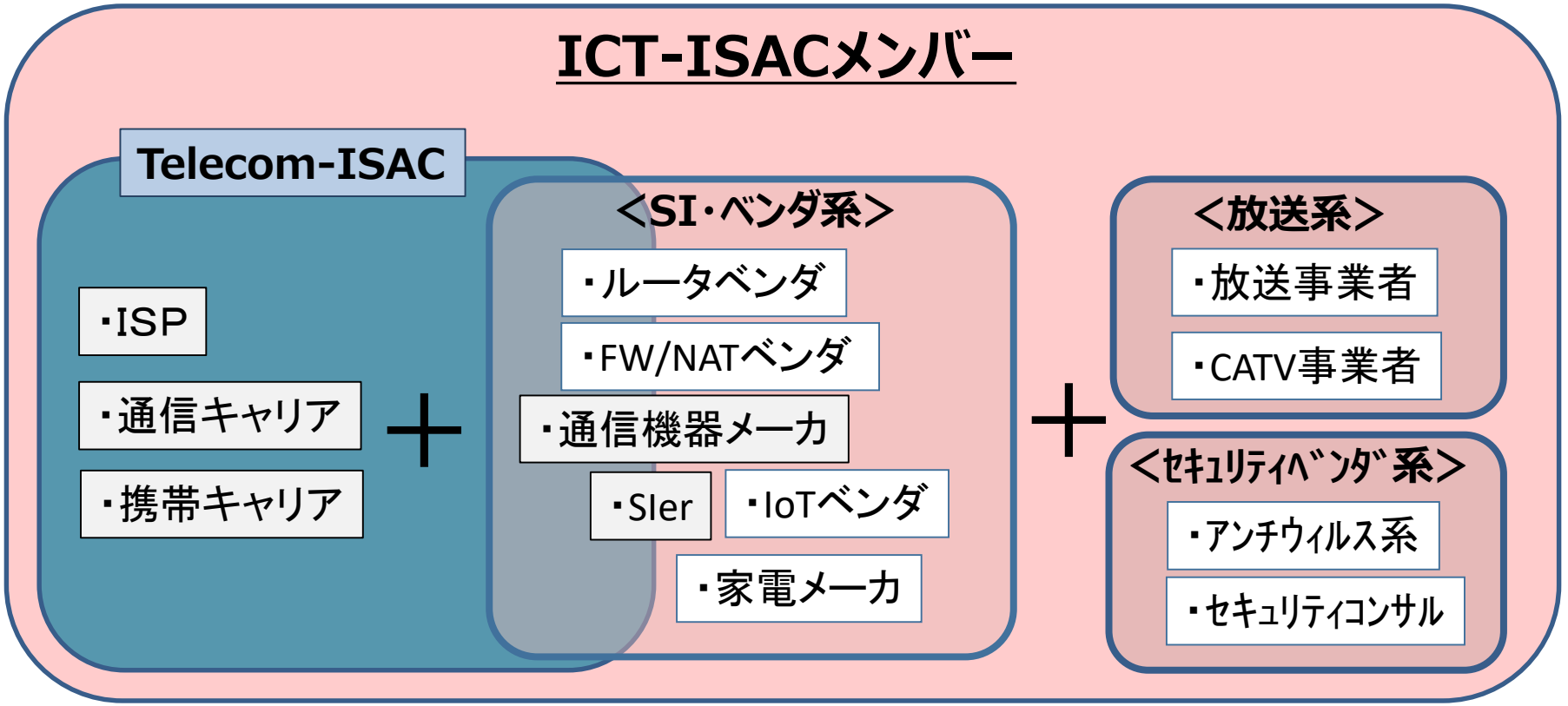
通信系(21)	日本電信電話株式会社、KDDI株式会社 ソフトバンク株式会社、株式会社インターネットイニシアティブ、NTTコミュニケーションズ株式会社、ビッグローブ株式会社 ソニーネットワークコミュニケーションズ株式会社、株式会社NTTドコモ、株式会社オプテージ 株式会社日本レジストリサービス、ニフティ株式会社、東日本電信電話株式会社、西日本電信電話株式会社 株式会社KDDI総合研究所、アルテリア・ネットワークス株式会社、インターネットマルチフィード株式会社 NTTデータ先端技術株式会社 株式会社QTnet、株式会社NTTエムイー、株式会社朝日ネット、日本ネットワークイネイブラー株式会社
放送系(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©2019 ICT-ISAC Japan. All Rights Reserved.

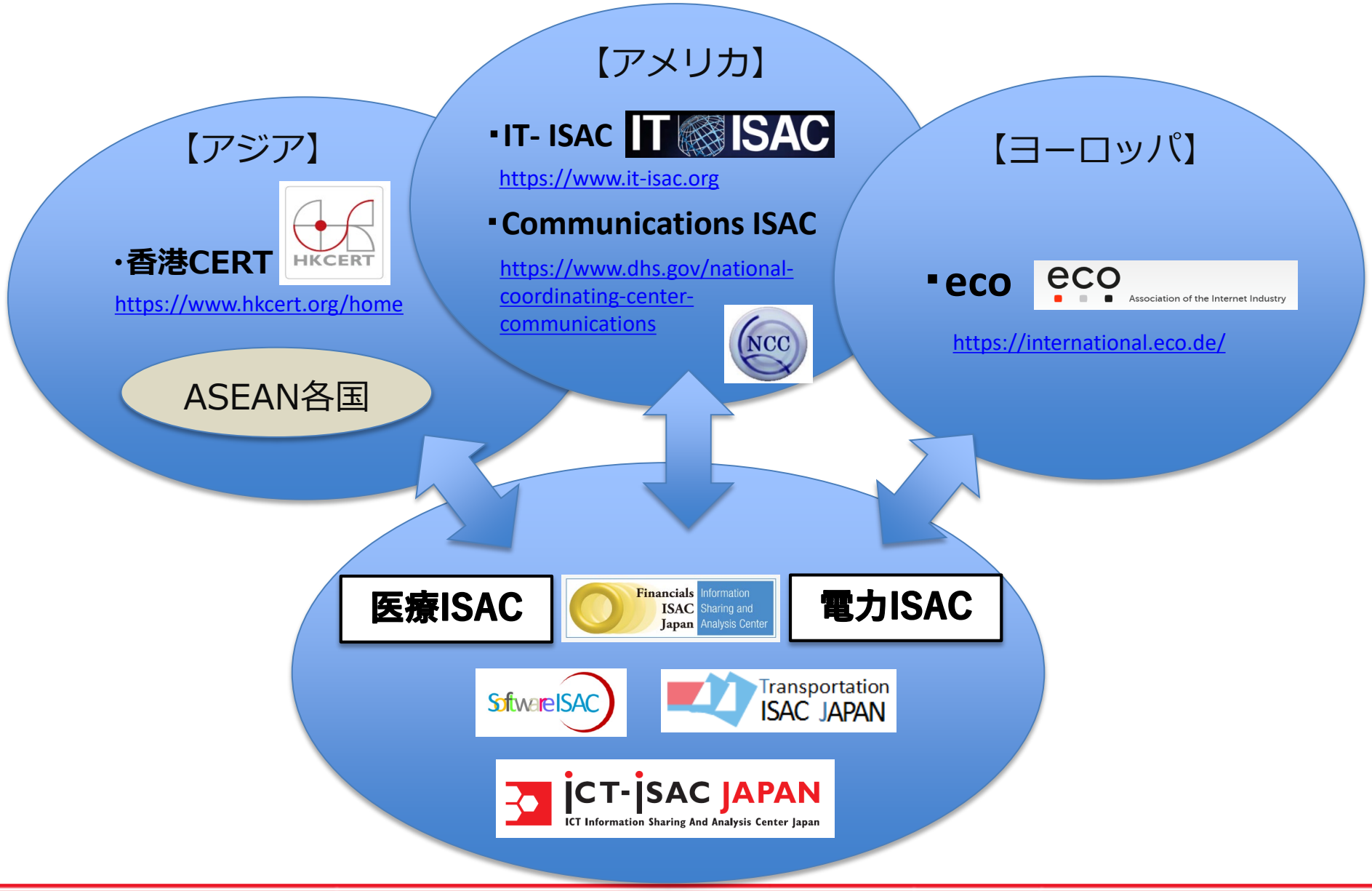
ICT-ISACの会員構成のスコープ

- 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©2019 ICT-ISAC Japan. All Rights Reserved.

情報共有に関する連携体制



Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

（参考）ICT-ISACのWG等一覧（業界特化系）

【業界特化系WG（通信系）】

- 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
- 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
- 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
- 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。
- 認定協会業務推進WG 2018年8月設置
  電気通信事業法等の改正に伴う認定協会(*)業務及びNICT業務について、ICT-ISACの取り組み方針検討及び、必要な組織を立ち上げを行うともに円滑業務推進行うことを目的とする。（*: 正式名「認定送信型対電気通信設備サイバー攻撃対処協会」）
- NOTICE-SiG 2019年1月設置
  NOTICEは（総務省、国立研究開発法人情報通信研究機構（NICT）及びISPが連携し、サイバー攻撃に悪用されるおそれのある機器の調査及び当該機器の利用者への注意喚起を行う取組）に取り組むISP間での情報共有。

【業界特化系WG（放送系）】

- 放送設備サイバー攻撃対策WG 2016年10月設置
  2020オリパラに向けての放送設備のセキュリティ強化のため、放送設備導入時の指針となる「放送設備セキュリティガイドライン(BCDG)」の策定と現場への浸透

【業界特化系WG（ＳＩ・ベンダ系）】

- デバイス脆弱性ハンドリング検討WG 2017年1月設置
  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

【業界特化系WG（セキュリティ・ベンダ系）】

- セキュリティベンダ課題検討WG 2016年11月設置
  各社相互理解、個社または業界共通の課題の検討。セキュリティトピック等の情報連携の在り方について議論

Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

（参考）ICT-ISACのWG等一覧（業界横断系）

【業界横断系WG】

- 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
- 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
- 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
- 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
- サイバー攻撃への適正な対処検討のためのWG(通秘-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
- 情報共有WG 2016年11月設置
  情報共有についての国際連携や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
- 交流促進-WG 2016年11月設置
  ICT-ISAC会員企業向けに、ノウハウ・知識等の普及・啓発、ISAC内の活動の活性化、WG間の相互理解促進、会員企業の持つ関連知識の共有・相互理解の促進等を行うと共に、対外的なイベント開催を通じてISAC活動のアピールを行い、会員数拡大にもつなげる
- IoTセキュリティWG 2016年8月設置
  ICT-ISACとして取組むべき「IoTセキュリティ対策」について、国の施策の動向を踏まえつつ、情報共有・議論を進め、我が国及び会員各社のIoTセキュリティに資することを目的とする
- CSA-WG 2019年3月設置
  ICT-ISACとしても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、国の施策の動向を踏まえつつ、情報共有・議論を進め、我が国及び 会員各社の連携向上に資することを目的とする
- 国内外ISAC連携-WG 2019年４月設置予定
  海外ISACおよび国内他業界ISACとの連携について検討する
  我が国及び 会員各社の連携向上に資することを目的とする
- 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
- 若手活躍SiG 2018年7月設置
  若年層にICT-ISACに参加する意義を伝え、また若年層が参加する環境を改善し、若者のセキュリティ離れを食い止める活動を行う

Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

Why ISACs?

- **Trusted** entities established by CI/KR owners and operators.
- Comprehensive **sector** analysis aggregation /anonymization
- **Reach**-within their sectors, with other sectors, and with government to share critical information.
- **All-hazards** approach
- **Threat** level **determination** for sector
- **Operational**-timely accurate actionable

national council of isacs

Why ISACs?

- Most ISACs have global members and operations
- Most ISACs are not-for-profit (501c6 or 501c3)
- Most ISACs are private sector organizations that rely on member dues for funding

ISACs

- Auto ISAC
- Aviation ISAC
- Communications ISAC
- Defense Industrial Base ISAC
- Downstream Natural Gas ISAC
- Elections Infrastructure ISAC
- Electricity ISAC
- Emergency Management & Response ISAC
- Financial Services ISAC
- Health ISAC
- Healthcare Ready
- Information Technology ISAC

ISACs

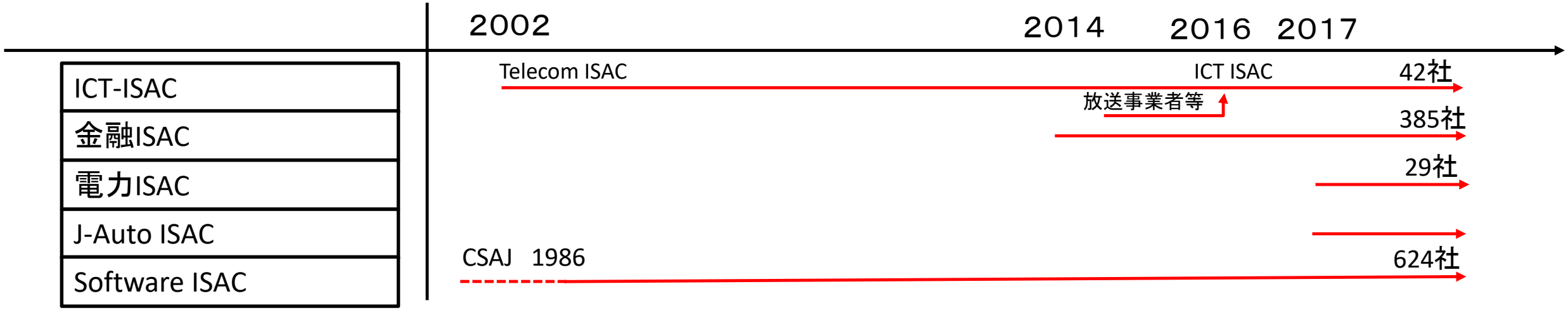
- Maritime ISAC
- Multi-State ISAC
- National Defense ISAC
- Oil and Natural Gas ISAC (ONG)
- Over the Road & Motor Coach ISAC
- Public Transit ISAC
- Real Estate ISAC
- Research and Education ISAC
- Retail and Hospitality ISAC
- Surface Transportation ISAC
- Water ISAC

National Defense ISAC™

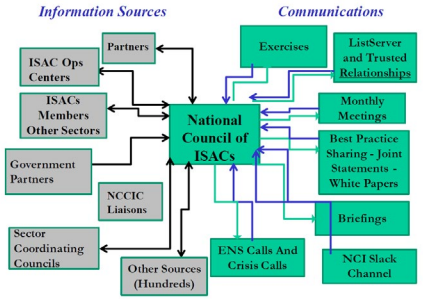
ONG-ISAC

情報共有の促進について

国内のISACの設立状況
業界ごとに企業が結束を固め、サイバー攻撃に対処する民間組織を立ち上げる動き



- 業種ごとにISACが立ち上がり、業種の共通課題を踏まえつつ情報共有が進むことは非常に有用
- 業態によっては、横断的にISACに加入が必要となったり、各ISAC毎に情報がサイロ化されたことによる事案の長期化・重篤化の危険性。またISACを立ち上げることが出来る事務局人材もいない業種もある。



各ISACが収集した情報のうち、類似した好事例を共有することによる対応能力の高度化の可能性

Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

巧妙化するサイバー攻撃に柔軟に対応するための情報共有について

通信の高度化・業界のICT化に乗じた、サイバー攻撃の巧妙化、複雑化に伴い、ISACを横断しての対応が必要な場面が出てきている。フィッシングから誘導して、不正送金などの問題化

ICT-ISACと金融ISACなど、関係するISACが事例や対処方法を共有してサイバーリスクを軽減

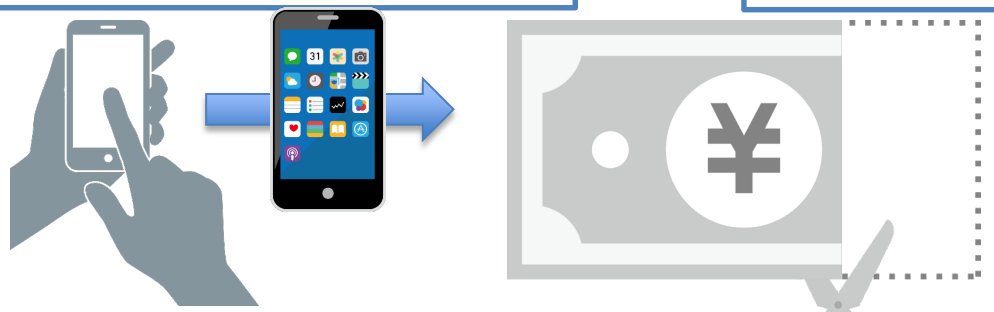


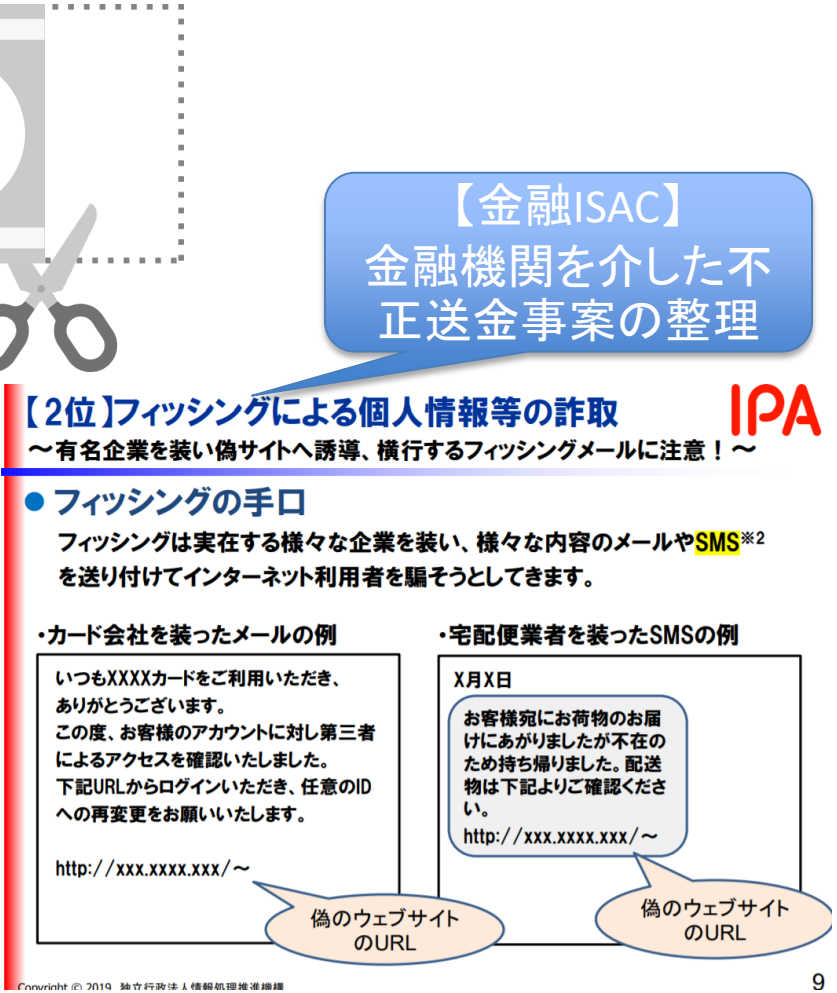
表 2-1　SMS 配信経路ごとの特徴（フィッシング対策ガイドライン 2018 年度版より抜粋）

	国内直接接続の SMS 配信	国際網を経由した SMS 配信	携帯電話端末からの SMS 配信
発信者番号表示	日本の電話番号（例：03-0000-0000）携帯キャリア毎の特別番号（例：50000）	海外の電話番号（例：+1 000-000-0000）アルファベット（例：FOOBAR）	携帯電話番号（例：090-0000-0000）
発信者番号登録・変更	契約者が自由には登録・変更できず、事前申請が必要	契約者が任意のタイミングで自由に登録・変更することが可能	携帯キャリアからの払い出しのみ
利用審査の厳格性	現在、審査をしないまま偽名や匿名での申込者に提供している事業者が存在しない	審査がなく偽名や匿名での申込者へ提供する事業者が存在する	端末レンタルサービス等で十分な審査を実施しない
Web サイト運営者の対策	自社が送信する SMS の発信者番号を利用者に対しウェブサイト等に記載し事前に通知したうえで利用する	フィッシャーに利用さく、利用者にとって自社する SMS と判別しつから、極力利用を避け	
利用者の対策	発信者番号は Web サイト運営者が事前に告知している番号と異なる SMS を受信した場合、フィッシングの可能性を疑い慎重に行動する	Web サイト運営者を騙ィッシングの可能性を疑重に行動する	
発信者番号の表示イメージ			

【福地雅之　NTT コム オンライン・マーケティング・ソリューション株式会社】

【ICT-ISAC】
各社の通信特性に応じたリスクの整理

【金融ISAC】
金融機関を介した不正送金事案の整理



Copyright©2019 ICT-ISAC Japan. All Rights Reserved.

サイバーセキュリティ国際シンポジウム開催概要

■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
　〒160-8330 東京都新宿区西新宿2-2-1
■対象者　サイバーセキュリティ関係者
■参加者数　170名

ICT-ISACとIT-ISACのMoU調印

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©2019　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©2019　ICT-ISAC Japan. All Rights Reserved.