

# ICT-ISACの概要と「情報共有」

2019年11月11日

ICT-ISAC事務局長  
引地 信寛

# ICT-ISACの概要

- 2002年7月：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
- 2016年3月：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：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本格的活動を開始
- 2019年2月：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）としての活動を開始

## 会員企業(42社)

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）

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ルド株式会社、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ァンス研究所、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

# ICT-ISACのワーキンググループ等一覧

ワーキンググループの名称	活動概要	黄色は今年で来たもの
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	

# 今年新たに誕生したWG・SiG

WG(Working Group): 会員企業のみが参加可能

SiG(Special Interest Group): 目的のために、会員以外も参加可能

ワーキンググループの名称	活動概要
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
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。
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

新しいWGは、どうやってできる？

- サイバー攻撃が複雑化、巧妙化する中で、(法律上の厳しい規制のある中で)、横連携拡大が必要になる
- 新たな施策(総務省のNOTICEプロジェクト、NISCのサイバーセキュリティ協議会対応)に、各会員がどう対応するか？
- セキュリティ人材育成は、いつでも課題

相互信頼・NDA・罰則規定

ルール

インシデント

ガイドライン

観測情報

統計情報

# どんな情報をどのように情報共有するのか

ワーキンググループの名称	活動概要
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
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。
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

例： 2月に始まったNOTICE

前回のシンポジウムでは、やっと立ち上がったところ。半年進みました





# NOTICE 半年の進捗

## IoT機器調査及び利用者への注意喚起（2019年9月まで）

➢ 2019年9月までに調査のための手続きが完了しているインターネット・サービス・プロバイダ（ISP）34社に係る約1.0億IPアドレスに対して調査を実施。

### 【NOTICEの取組結果】

ID・パスワードが入力可能であったもの

約98,000件  
(直近での調査)  
【6月時点:約42,000件】

上記の内、ID・パスワードによりログインでき、注意喚起の対象となったもの

延べ505件  
【6月時点:延べ147件】

### 【マルウェアに感染しているIoT機器の利用者への注意喚起の取組結果】

ISPに対する通知の対象となったもの

80~559件  
(1日当たり)  
【6月時点:112~155件】

### （参加ISP：計34社）

株式会社秋田ケーブルテレビ  
イッツ・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QNet  
ケーブルテレビ株式会社  
山陰ケーブルビジョン株式会社  
株式会社ZTV  
株式会社TOKAIケーブルネットワーク  
株式会社ベイ・コミュニケーションズ

株式会社朝日ネット  
株式会社インターネットイニシアティブ  
株式会社愛媛CATV  
近鉄ケーブルネットワーク株式会社  
株式会社ケーブルテレビ品川  
株式会社シー・ティー・ワイ  
ソーネットワークコミュニケーションズ株式会社  
ニフティ株式会社

アルテリア・ネットワークス株式会社  
エヌ・ティ・ティ・コミュニケーションズ株式会社  
株式会社オプテージ  
KDDI株式会社  
株式会社ケーブルネット・鈴鹿  
株式会社ジュピターテレコム（グループ会社計10社）  
ソフトバンク株式会社  
ビッグローブ株式会社

情報共有と成果をまとめるため

手順をまとめる  
マニュアルをまとめる  
進捗をまとめる

改善のPDCAにつなげる

## NOTICEからNICTERの準備と業務

サイバー攻撃を禁止する技術的  
条件を定めて総務省に認可  
をとる

脆弱なものは検査するよ、注意  
喚起するよと約款に定めて利用  
者に表示する

厳しい守秘と情報管理を守りま  
すよ

NOTICEホームページに  
ISPロゴ掲載可能  
<https://notice.go.jp/org>

### NOTICE準備

総務省に技術  
的認可

①B 検査・注意喚  
起の約款対応

①C NICTとの覚書  
取得

①d ISACとKIZUNA  
アポイントの取得

### NOTICE実施

月上旬にIPレンジ送付（変更な  
ければ初回のみ）、20日ごろに  
ISP受領、月末までに注意喚起



②A スケジュール  
確認（IPレンジの日、スキャン  
結果受け取り、サポセン報告）

②B IPレンジ送付  
ISP→ISAC→NICT

②C スキャン結果受取  
NICT→ISAC→ISP

②D スキャン結果の利  
用者特定と注意喚起

利用者  
サポートセン  
タ

②E NOTICE作業進捗  
をサポセンに報告

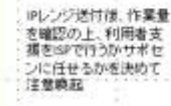
第1主曜日

第4主曜日

翌月第3主曜日に提出

### NICTER実施 （日次処理対応後の想定）

IPレンジ送付後、作業量  
を確認の上、利用者支  
援をISPで行うかサポセ  
ンに任せるかを決めて  
注意喚起



③A スケジュール  
確認（サポセン報告）

③B IPレンジ送付  
ISP→ISAC→NICT

③C スキャン結果受取  
NICT→ISAC→ISP

③D スキャン結果の利  
用者特定と注意喚起

利用者  
サポートセン  
タ

③E NICTER作業進捗を  
サポセンに報告

③Bの日曜日から受領可能

月内3回以上実施

翌月第3主曜日に提出

画面のみでの投影となります

オリパラに向け、いろんな分野でのリスクが考えられる  
どのサービスであっても、ネットワークがつながるのが前提  
サイバー防御のために、連携を深めていきましょう

ワーキンググループの名称	活動概要
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。



若手はどんどん伸びていきます  
環境と、阻害要因を離していけば...

