資料 40－3

情報通信審議会 情報通信技術分科会
IPネットワーク設備委員会 技術検討作業班
報告

―IoT機器を含む端末設備のセキュリティ対策について―

情報通信審議会 情報通信技術分科会
ＩＰネットワーク設備委員会 技術検討作業班
報告　目次

Ⅰ　検討事項

情報通信審議会情報通信技術分科会 IP ネットワーク設備委員会（以下「委員会」という。）では、平成 17 年 11 月より、情報通信審議会諮問第 2020 号「ネットワークの IP 化に対応した電気通信設備に係る技術的条件」（平成 17 年 10 月 31 日諮問）について検討を行ってきている。

本報告は、「ネットワークの IP 化に対応した電気通信設備に係る技術的条件」のうち、「IoT の普及に対応した電気通信設備に係る技術的条件」について、昨年 12 月から本年７月にかけて開催された委員会（第 34 回～第 41 回）及び技術検討作業班（第 31 回～第 34 回）において検討された結果のうち、IoT 機器を含む端末設備のセキュリティ対策に関する技術検討作業班の検討結果を取りまとめたものである。

Ⅱ　作業班の構成

作業班の構成は、別表 1 のとおりである。

Ⅲ　検討経過

これまで、技術検討作業班（第 33 回～第 34 回）を開催して検討を行い、IoT 機器を含む端末設備のセキュリティ対策について報告を取りまとめた。

①　第 33 回技術検討作業班（平成 30 年 5 月 10 日）

IoT 機器を含む端末設備のセキュリティ対策について検討を行った。また、詳細の検討を行うため、アドホック会合を開催することとした。

②　技術検討作業班アドホック会合（平成 30 年 5 月 18 日）

IoT 機器を含む端末設備のセキュリティ対策について検討を行った。

③　第 34 回技術検討作業班（平成 30 年 6 月 7 日）

技術検討作業班及びアドホック会合におけるこれまでの検討を取りまとめた技術検討作業班報告（案）について検討を行い、技術検討作業班報告を委員会に報告することとした。

Ⅳ　検討結果

第１章　IoT 機器を含む端末設備のセキュリティ対策について

1.1　検討の目的等

近年、Web カメラやルータ等の IoT 機器が乗っ取られ、インターネットに障害を及ぼすような DDoS 攻撃等のサイバー攻撃に悪用される事案が増加している。

一方、情報通信ネットワークの安全・信頼性を確保するために、電気通信事業法においては、電気通信事業者の電気通信回線設備の機能に障害を与えない、他の利用者に迷惑を及ぼさない等を原則とする端末設備の接続の技術基準が定められている。

本作業班では、そのような制度の枠組みの中で、大規模 DDoS 攻撃等のサイバー攻撃を抑止するため、IoT 機器を含む端末設備がマルウェアに大量感染しないこと等を目的とするセキュリティ対策を技術基準に追加することについて検討を行った。

1.2　検討結果

（１）端末設備の接続の技術基準にセキュリティ要件を追加する必要性について

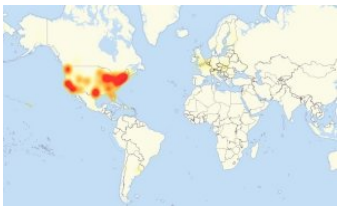
近年増加しているマルウェア「Mirai」等による大規模 DDoS 攻撃を抑止するためには、攻撃の踏み台となる IoT 機器がマルウェアに大量感染しないような対策を取ることが重要である。

大規模 DDoS 攻撃については、電気通信事業者による対応が期待されることは言うまでもない。しかしながら、電気通信事業者は、電気通信事業法第 4 条に基づき、その取扱中に係る通信の秘密は、侵してはならないとされていることから、原則として、通信内容を確認することは不可能である。このため、仮に IoT 機器からの大量通信が発生した場合であっても、通信内容を確認して正常な通信なのか、DDoS 攻撃に加担しているものであるか判別することができない。また、マルウェア感染した IoT 機器のみの通信を止めることについても、技術面から困難であるため、電気通信事業者が取り得る対応も制約がある状況となっている。

なお、電気通信事業者によるセキュリティ対策を強化するため、本年５月に電気通信事業法等が改正され、電気通信事業者による情報共有体制などの新たな取組みが導入されることとなっている。

- 2016年10月 米国Dyn社のサービスを標的とした大規模DDoS攻撃が発生
- TwitterやSpotify、Netflix、WSJなどの大手サイトがアクセスしにくくなる事象が発生。
  米国を中心に約6時間にわたってサービスが利用できなかった。
- 本攻撃は電子機器メーカーHangzhou Xiongmai Technologyの防犯カメラ（DVR）やIPカメラなど10万台以上のIoT機器の脆弱性を悪用し感染させたMiraiと名付けられたマルウェアからの悪性通信によって引き起こされた。
- Mirai系マルウェアに感染しているIoT機器は、主に工場出荷時のID/パスワードを使っており簡単に感染させられるものであることが指摘されている

攻撃概要　(出典) Cyber Attack dot Net


感染地域　(出典) Downdetector

- 2016年11月には英国人男性ハッカー(逮捕済み)によってドイツテレコムが各家庭に設置したルータ約90万台にMirai型マルウェアの感染を狙ったサイバー攻撃が行われる。顧客のサービスに障害が発生。ネットにアクセスできないなどの影響が出た。
- 2017年10月スウェーデンの交通機関や当局のネットワークを提供しているISPであるTDCとDGCへの大規模DDoS攻撃が発生。
  - 列車運行を管理する産業省交通局のシステムが麻痺。列車の運行停止や遅延が発生。
    列車遅延は一日中続いた。
  - サイトやメールシステムもダウンしたため、遅延情報も通知できなかった。交通局では局員個人のFacebookアカウントで乗客に情報提供を実施するなど混乱が発生した。

図 1.1　IoT 機器を感染対象としたマルウェア：Mirai
（第 36 回委員会 ICT-ISAC 説明資料より抜粋）

大規模 DDoS 攻撃に対処する上では、IoT 機器の利用者における対策も重要である。しかしながら、例えば機器メーカ等がソフトウェアの更新を呼びかけたとしても、技術的に対策が難しい等の理由で全ての利用者に対応を求めることは容易ではない。

また、IoT 機器が目的どおり動作している限り、そもそも利用者は攻撃の踏み台となっていることを認知することが難しいという課題も存在する。

実際に過去の事例では、利用者に注意喚起を行った後、脆弱性のある機器の約 8 割に対処が行き届くのに約３年を要したものもあった。

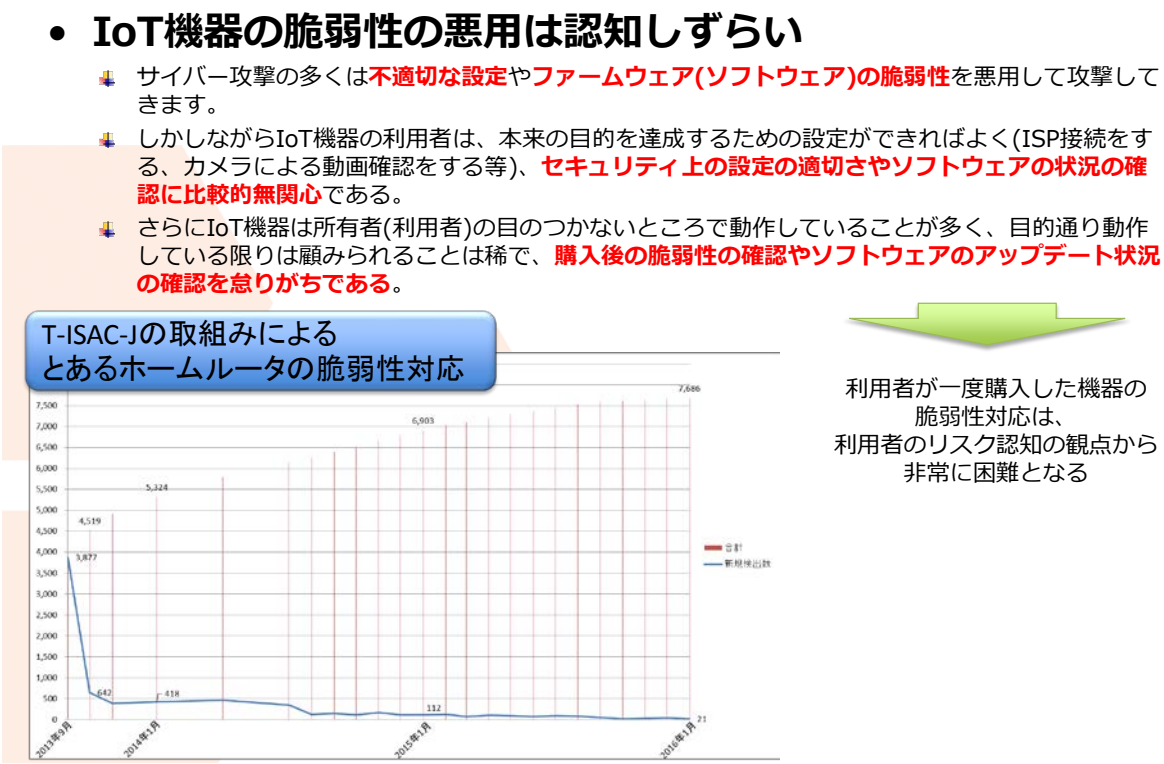


図 1.2　IoT 機器のセキュリティ上の問題
（第 36 回委員会 ICT-ISAC 説明資料より抜粋）

一方、現在の IoT 機器に対するサイバー攻撃は、グローバル IP アドレスを有する機器を対象として、セキュリティ上の不適切な設定や利用者に認知されていない脆弱性等を悪用したサイバー攻撃が多い。平成 28 年 10 月に、米国を中心に大手インターネットサービスの障害を引き起こしたマルウェア「Mirai」の事例では、本来不要な通信機能のアクセス制御のため、主に工場出荷時の ID/パスワードをそのまま使用していた IoT 機器が数多く乗っ取られ、大規模 DDoS 攻撃が行われた。このような事例でも、IoT 機器において比較的な簡易なセキュリティ対策を行うことで大半の攻撃を防ぐことが可能である。

また、アクセス制限がない機器、ハードコーディングされた ID/パスワードを持っている機器、既知の脆弱性が埋め込まれている機器等が出荷された場合には、その脆弱性を事後に修正することは困難なものとなる。そのため、出荷前に必要な対策を講

じることが有効であると考えられる。

これらを踏まえると、IoT 機器を含む脆弱な端末設備に対するセキュリティ対策として、電気通信事業法の枠組みの中で、電気通信事業者の電気通信回線設備の機能に障害を与えない、他の利用者に迷惑を及ぼさないといった端末設備の接続の技術基準の原則の範囲内において、その技術基準にセキュリティ要件を追加することが適当である。

なお、当該セキュリティ要件は、IoT 機器のマルウェア大規模感染を防止することを目的としているものである。IoT セキュリティを確保するためには、これらの対策だけでは不十分であり、IoT 機器が使用される分野や用途に応じたガイドラインに基づくセキュリティ対策や、利用者等への周知啓発など総合的な対策が必要である。それらについては IoT 推進コンソーシアム等の場において引き続き検討され、必要な対策が実施されていく必要がある。

（２）IoT セキュリティ対策に関する国内外の動向

IoT セキュリティ対策については、現在、欧米等においても議論が活発に行われているところである。

米国においては、「ボットネット等の脅威に対するインターネットの強固性と通信のエコシステムの強化」に関する報告書が取りまとめられた。当該報告書では、IoT セキュリティに関し、初期設定及び自動ソフトウェアの更新機能などの重要性を指摘するとともに、機器の大半は国外に存在するため、国際的に認められた標準に基づくセキュリティの向上が重要であるとして、今後、具体的な施策の検討が行われていくことが見込まれる。

一方、欧州においては、ＩＣＴ機器やサービスに対し、既知の脆弱性を含まないソフトウェアが提供され、安全にソフトウェア更新がおこなわれることを保証すること等を目的として、「ＩＣＴサイバーセキュリティ認証に関する規則案」が公表され、引き続き欧州議会で検討が行われているところである。

機器を対象としたセキュリティ認証に係る国際標準については、政府調達機器の一部に関し、国際標準 ISO/IEC15408 に基づく CC(Common Criteria)認証が行われている。CC 認証は、世界２８カ国で受け入れられている認証制度であり、複合機の例では、他の利用者による不正な操作や通信データの盗聴・改ざん、管理機能への不正なアクセス等を脅威として想定し、識別・認証・権限付与やアクセス制御、ファームウェアに電子署名を付すといった高信頼な通信等のセキュリティ機能を保証するとともに、セキュリティ機能自体の脆弱性評定も実施している。

IoT セキュリティ対策に関する国際標準は、ISO/IEC JTC1/SC27 において検討が開始されたところであり、現時点で確立しているものではない。しかし、IoT のグローバル市場への展開や国際競争力確保といった観点から、CC 認証をはじめとした国際標準との整合性を図るとともに、今後も、国際的な動向の把握に努める必要がある。

また、日本からは現在、IoT 推進コンソーシアムにおいて定められた「IoT セキュリティガイドライン ver1.0」の内容について国際標準の議論の場に提案が行われているところであり、今後も積極的に我が国の取組みを発信していくことが重要である。

（３）端末設備の接続の技術基準に追加すべきセキュリティ対策の内容

以上の点を踏まえると、端末設備の接続の技術基準に追加すべきセキュリティ対策は、インターネットプロトコルを使用する端末設備であって、電気通信回線設備を介して接続することにより当該設備に備えられた電気通信の送受信に係る機能を操作可能なものについて、大量感染を防ぐための最低限のセキュリティ要件として、アクセス制御機能、アクセス制御の際に使用する ID/パスワードの適切な設定を促す等の機能及びファームウェアの更新機能、又はそれらと同等以上の機能を具備することを要件とすることが適当である。また、具体的な機能については、下表のとおりとすることが適当である。

表 1.1 端末設備に最低限必要なセキュリティ要件の具体的な機能

セキュリティ要件	具体的な機能
アクセス制御機能	・当該端末が不正に操作されないことを目的として、当該操作の前にアクセス制御を行うことが必要。
アクセス制御の際に使用する ID/ﾊﾟｽﾜｰﾄﾞの適切な設定を促す等の機能	・アクセス制御を識別符号によって行う場合は、当該識別符号が他人から容易に推測できないものとして設定されることを目的として、当該端末の利用者に対し当該識別符号について初期値の変更を促す（二以上の識別符号の組み合わせによるものの場合は少なくとも一つの識別符号が対象。以下同じ。）、識別符号の初期値について機器毎に別のものを付す、又はそれらに準じる措置を行うことが必要。
ファームウェアの更新機能	・端末に記憶されている当該電気通信の送受信の機能に係るソフトウェアの更新が可能であることが必要。当該更新は安全かつ自動で行われることが推奨されるが、IoT 機器は多種多様であり、更新の手法は機器の種別毎に異なることから、安全かつ自動の更新までは要件とはしない。 ・端末への電力供給が停止した場合であっても、当該更新されたソフトウェアや変更されたアクセス制御の設定内容を維持することが必要。
同等以上の機能	・ＣＣ認証などの国際標準に基づくセキュリティ認証を取得した複合機など、上記の機能と同等以上のセキュリティ機能を有すると認められるものについては、当該セキュリティ要件を満足するものとみなす。

なお、PC やスマートフォン等、アンチウィルスソフト等のソフトウェアを導入する等、利用者が任意の方法により必要に応じて随時かつ容易に必要な対策を行うことが可能な設備については、当該セキュリティ要件の規定の対象外とすることが適当である。

（４）技術基準適合認定等の対象機器の範囲

セキュリティ要件が追加された技術基準に関し、当該技術基準適合認定等を求める端末機器の範囲については、インターネットプロトコルを使用する全ての機器に対し、セキュリティ対策を求めることが理想的ではあるが、より効率的かつ効果的な対策とするため、セキュリティ対策を行うことが効果的な機器の範囲を明確にすることが適当である。

マルウェアに感染している IoT 機器に関する研究では、感染機器の９割以上が不明であるものの、判明している範囲では海外製品のインターネットカメラ、デジタルビデオレコーダ、ルータ等が多いが、国内製品においても、ルータ、ゲートウェイ、ネットワークストレージ、太陽光パネル管理システム、電力デマンド監視システムといった機器に感染事例が見つかっているという報告がなされている。

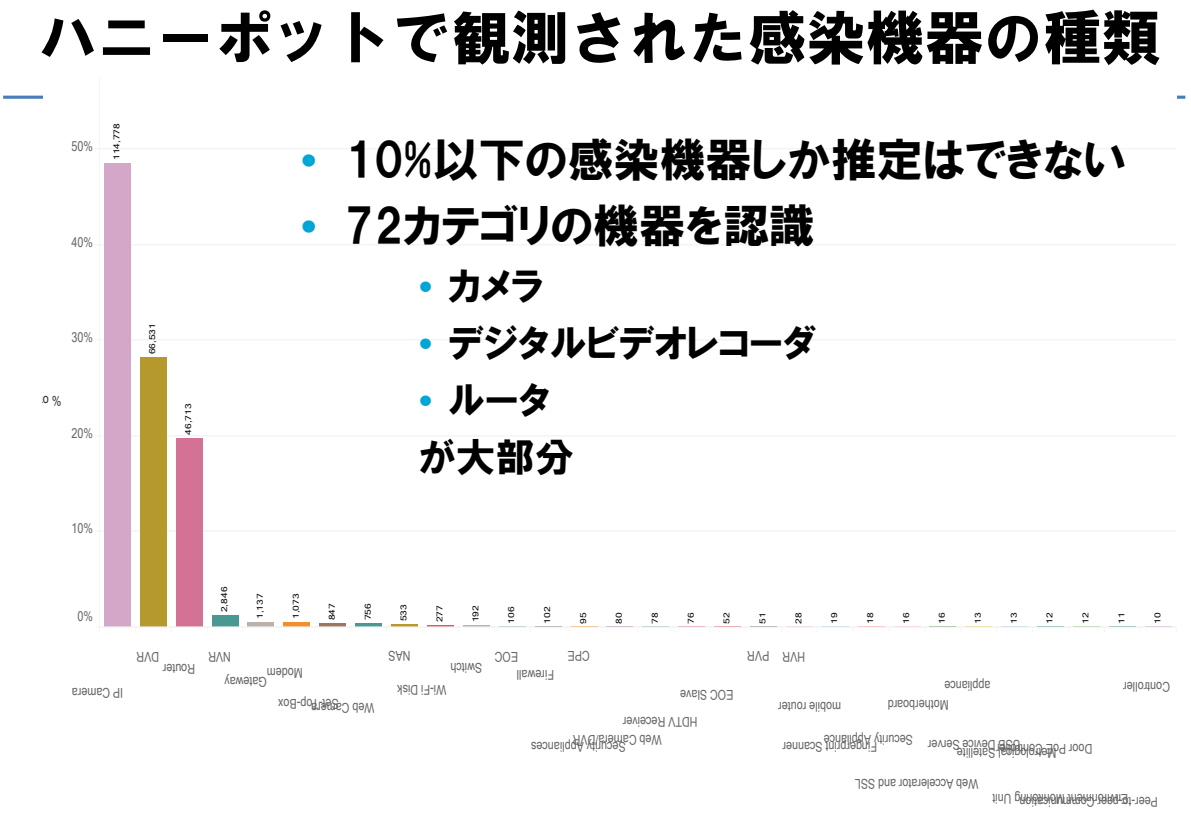


図 1.3　ハニーポットで観測された感染機器の種類
（第 37 回委員会　吉岡オブザーバ説明資料より抜粋）

現在の IoT 機器に対するサイバー攻撃は、グローバル IP アドレスを有する機器へのインターネット側からの直接的攻撃が主流であり、ルータ等の直接接続される機器に感染した後、更に家庭内の機器にまで感染活動を行うものは５%程度という分析事例 [1]がある。そのため、インターネット側からアクセス可能なネットワークサービス（Web 管理、telnet 等）を使用する機器については、特に脆弱性対策が必要と考えら

[1]熊佳、楊志勇、鉄穎、中山颯、江澤優太、藤田彬、吉岡克成、松本勉、"実攻撃の観測と疑似攻撃の試行に基づくホームネットワークセキュリティ評価フレームワークの検討," 2018 年暗号と情報セキュリティシンポジウム, 2018.

れる。

現状の技術基準適合認定等は、基本的に電気通信回線設備に直接接続される端末機器を対象に実施しているが、上記を踏まえれば、現状においてネットワーク側からサイバー攻撃を受けた際に乗っ取られるリスクが特に高いのは、電気通信事業者の電気通信回線設備に直接接続される端末機器であることから、セキュリティ要件が追加された技術基準適合認定等の対象についても、従来と同様に電気通信回線設備に直接接続される端末機器とすることが適当である。

その際、直接接続される機器とは、電気通信回線設備に物理的かつ技術的に直接接続可能な端末機器を指すが、その中でも恒常的に既認定機器を介して接続する機器（屋外に持ち出す等により電気通信事業者の回線設備に直接接続して使用することを全く想定していない機器(例：大型白物家電等)）については、技術基準適合認定等の対象外とする。

この場合、利用者が認定等を取得していない機器を誤って直接接続しないようにするため、例えば、取扱説明書等において、①当該機器は既認定機器に接続する必要があることや、②電気通信事業者の電気通信回線設備に直接接続する場合には、電気通信事業者による検査が義務付けられていることを記載すること等をガイドライン等により明示することについて検討する必要がある。

また、認定等を取得していない機器の乗っ取りを防ぐためには、IoT 機器メーカや IoT システム/サービス提供者等において、IoT 推進コンソーシアムにおいて定められた「IoT セキュリティガイドライン ver1.0」等に基づき、直接接続される既認定機器における対策も含む適切なセキュリティ対策を検討・実施する必要がある。

今後、端末機器の接続が多様化することが想定されるが、認定等が必要な機器の範囲等については、機器メーカ等が判断できるように、ガイドライン等により明示することについて速やかに検討を開始する必要がある。

（５）セキュリティ要件の追加に係る経過措置

端末設備の接続の技術基準へのセキュリティ要件の規定の追加が制度化された場合には、IoT 機器メーカや登録認定機関等の対応を考慮して、一定の期間を設けて施行することとなるが、その期間は 1 年から 2 年程度とすることが適当である。

また、従来の制度に基づき、新制度の施行前に取得した技術基準適合認定等については、施行後も引き続き有効であり、当該認定等に基づく機器も引き続き使用することを可能とすることが適当である。

（６）技術基準適合認定等の審査方法等

登録認定機関等による技術基準適合認定については、セキュリティ要件の対象となる機器の審査が円滑に行われるよう、その審査方法や機器の審査単位等について通信事業者、機器メーカ等が参画可能な場で別途議論を行うことが適当である。

別表１　技術検討作業班 構成員

情報通信審議会 情報通信技術分科会
IP ネットワーク設備委員会 技術検討作業班 構成員

（平成 30 年 6 月時点　敬称略　五十音順）

	氏　名	所　属	事故報告等担当	端末ｾｷｭﾘﾃｨ担当
主任	内田　真人	早稲田大学 基幹理工学部 情報理工学科 教授	○	○
主任代理	吉岡　克成	横浜国立大学大学院 環境情報研究院/先端科学高等研究院 准教授	○	○
	大内　良久	ＫＤＤＩ株式会社 技術統括本部 運用本部 運用品質管理部　部長	○	
	岡田　昌己	エヌ・ティ・ティ・コミュニケーションズ株式会社 カスタマサービス部 危機管理室長	○	
	尾形わかは	東京工業大学 工学院 情報通信系 教授	○	
	小畑　和則	株式会社ＮＴＴドコモ Ｒ＆Ｄ戦略部 担当部長	○	○
	木村　　孝	一般社団法人 日本インターネットプロバイダー協会 会長補佐	○	
	喜安　明彦	一般社団法人 電気通信事業者協会 安全・信頼性協議会 会長	○	
	桑田　雅彦	日本電気株式会社 デジタルプラットフォーム事業部 シニアエキスパート		○
	小林　　努	株式会社インターネットイニシアティブ サービス基盤本部 副本部長	○	○
	阪田　　徹	一般財団法人 電気通信端末機器審査協会 機器審査部 部長代理		○
	四ノ宮大輔	一般社団法人 情報通信ネットワーク産業協会 通信ネットワーク機器 セキュリティ分科会 主査		○
	渋谷　香士	ソニー株式会社 品質・環境部 シニア製品セキュリティマネジャー		○
	高橋慎一郎	株式会社ＮＴＴドコモ 情報セキュリティ部 サイバーセキュリティ統括室 室長		○
	高橋　　範	株式会社ソラコム 事業開発マネージャー	○	
	田島　佳武	日本電信電話株式会社 技術企画部門 セキュリティ戦略 担当部長		○
	中野　　学	パナソニック株式会社 製品セキュリティセンター 製品セキュリティグローバル戦略室 主幹技師		○
	中村　康洋	シャープ株式会社 ＩｏＴ事業本部 ＩｏＴクラウド事業部 イノベーション開発部 技師		○
	西川　嘉之	ＵＱコミュニケーションズ株式会社 渉外部 部長	○	

西部　喜康	一般社団法人 ＩＣＴ―ＩＳＡＣ 脆弱性保有ネットワークディバイス調査ＷＧ 主査		○
野呂田みゆき	東日本電信電話株式会社 ＩＴイノベーション部 技術部門 企画担当		○
花石　啓介	日本電信電話株式会社 技術企画部門 災害対策室長 兼 ビジネスプロセス戦略担当 担当部長	○	
日比　　学	京セラコミュニケーションシステム株式会社 ＬＰＷＡソリューション事業部 ＬＰＷＡソリューション部 副責任者	○	
福井　晶喜	独立行政法人 国民生活センター 相談情報部 相談第２課 課長	○	○
福島　　敦	株式会社ジュピターテレコム 技術運用副本部長	○	
堀内　浩規	一般社団法人 日本ケーブルテレビ連盟 理事 兼 通信制度部長	○	
前田　真弓	東芝クライアントソリューション株式会社 技監		○
松本　勝之	ソフトバンク株式会社 ＩＴサービス開発本部 セキュリティ事業統括部 セキュリティオペレーションセンター部 サイバーインシデントレスポンス課 課長		○
松本　佳宏	株式会社ケイ・オプティコム 計画開発グループ グループマネージャー	○	
向山　友也	一般社団法人 テレコムサービス協会 技術・サービス委員会 委員長	○	
毛利　政之	ＫＤＤＩ株式会社 技術企画本部 電波部 管理グループリーダー		○
矢入　郁子	上智大学 理工学部 情報理工学科 准教授	○	
山口　琢也	ソニーネットワークコミュニケーションズ株式会社 ネットワーク基盤事業部門 ネットワーク部 ネットワーク運用課 課長	○	
渡部　康雄	ソフトバンク株式会社 技術管理本部 業務管理統括部 技術渉外部 部長	○	○