サイバーセキュリティ政策推進に関する提言

平成27年5月22日

総務省
情報セキュリティ アドバイザリーボード

目次

１．検討の背景

検討の背景

- 情報通信ネットワークの繋がりにより創出されるサイバー空間は、情報の自由な流通を通じて社会経済を発展させ、国民生活や社会経済活動の基盤をなすもの。
- あらゆるモノがインターネットに接続されるIoT（Internet of Things）社会の本格的到来により、サイバー空間は物理空間との繋がりを一層深め、その外延は大幅に拡張。
- これに伴い、今後、センサー機器の低廉化・高機能化により促進される社会インフラへのセンサーの組み込み・モニタリング、ネットワークへの接続による自動車の安全性や利便性の向上、ウェアラブル機器がもたらす生活に密着した機能の提供など、各分野で新たな価値が生み出されてイノベーションが創発し、社会経済の更なる発展が見込まれるところ。
- その一方で、こうしたサイバー空間の拡張と社会経済の発展に対し、サイバー空間の存立そのものを脅かす、巧妙化・高度化したサイバー攻撃の脅威も大幅に増大。
- このようなサイバー攻撃の脅威に対抗し、サイバー空間を持続的に発展させていくためには、サイバー空間に参画する政府、重要インフラ事業者、企業、個人等のあらゆるステークホルダーによる自律的取組と、国際連携を含む相互連携の下で、ICT環境の変化に対応して被害を未然に防ぐプロアクティブな対策を総力を挙げて講じることにより、万全のサイバーセキュリティを確立することが必要不可欠。
- 2014年11月には、我が国全体のサイバーセキュリティ強化等に向けたサイバーセキュリティ基本法が成立。同法律は2015年1月に全面施行され、2015年6月を目途に政府の新たなサイバーセキュリティ戦略が閣議決定予定。
- さらに、2020年にはオリンピック・パラリンピック東京大会の開催を控えており、そのテレビ中継を担う放送分野を含むあらゆる分野で、サイバーセキュリティの確立に努めることが急務。
- これらの認識の下、サイバーセキュリティ確立のため、ICTインフラ防護等の観点から講ずべき方策について、提言を実施。

2. 基本理念・基本原則

検討に当たっての基本理念･基本原則

今後見込まれる社会変化に対応したサイバーセキュリティの確立のために講ずべき方策について、以下の基本理念･基本原則に基づき検討を実施。

サイバー空間における【基本理念】

情報の自由な流通の確保と、それによる社会経済発展の主導

サイバーセキュリティに関する【基本原則】

サイバー空間の基盤である安全な情報通信ネットワーク環境の確立

ICTの著しい環境変化への柔軟かつダイナミックな対応

あらゆる関係主体の自律した取組と相互連携の促進

国際的な協調･協力関係の発展

3. 守るべき対象

守るべき対象

検討に際し、ICTインフラ防護等の観点から、「守るべき対象」を以下の4項目に整理。

ネットワーク基盤を守る

- ✓ ネットワークに繋がる脆弱な機器等を悪用した攻撃からネットワークの安定運用を守る
- ✓ IoT機器の普及による既知及び未知の脅威からネットワークを守る

組織を守る

- ✓ 企業の機密情報など組織の資産を守る
- ✓ 重要インフラ事業者等の組織が機能を維持するためのネットワーク環境を守る

個人を守る

- ✓ 金銭、個人情報など個人の資産を守る
- ✓ 個人がネットワークを安全に利用できる環境を守る

我が国のネットワーク環境を守るとともに、国際社会に貢献する

- ✓ 他国から到来するサイバー攻撃から我が国のネットワーク環境を守る
- ✓ 国際的な信頼（レピュテーション）を確保し、国際社会に貢献する

「守るべき対象」を脅かすサイバー攻撃とその周辺状況

○ サイバー攻撃の大規模化

脆弱性を有する機器を悪用した攻撃が多発し、2014年にはピーク時のトラフィックが400Gbpsに達するDDoS攻撃が発生。

○ サイバー攻撃の対象範囲の拡大

IoT機器数は2015年現在の約49億個から2020年には約250億個に急増する見込み。ネットワークに接続されるこれらの機器はサイバー攻撃の対象となるおそれ。

○ 重要インフラを標的としたサイバー攻撃の発生

2013年、韓国において銀行や放送機関等の重要インフラ事業者が一斉にサイバー攻撃の被害を受け、機能を停止。

○ 機微情報窃取を目的としたサイバー攻撃の発生

2011年以降、国会、政府機関、大手企業等が標的型攻撃の被害を受け、情報流出を起こしていたことが相次いで判明。

○ 金銭目的のサイバー攻撃の急増

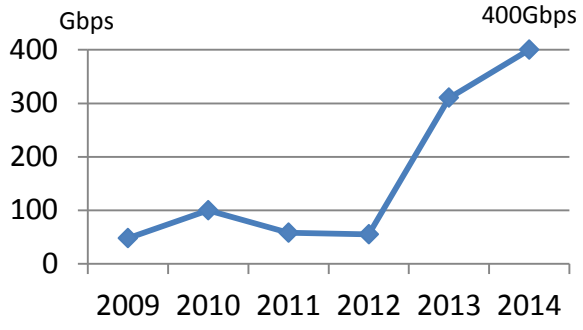
2014年のインターネットバンキングでの不正送金被害額は約29億円であり、2013年の被害額約14億円から倍増。

○ 米国における官民サイバー攻撃情報共有の体制整備

サイバー攻撃による被害の深刻化を踏まえ、米国では、新組織の設立や立法措置等、官民の情報共有を促進する動きが進展。

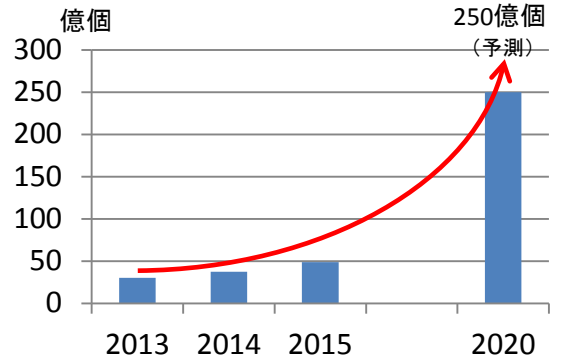
○ 国境を越えたサイバー攻撃の発生

2013年、標的型メール攻撃に使用された不正プログラムの通信接続先の97%は海外。



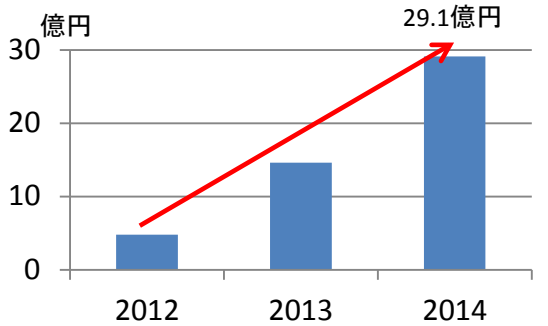
DDoS攻撃ピーク時トラヒック推移

（出典）米アーバーネットワークス公表資料



IoT機器数増加予測推移

（出典）米ガートナー公表資料



ネットバンキング不正送金被害額推移

（出典）警察庁公表資料

「守るべき対象」をめぐる懸念

「守るべき対象」を脅かすサイバー攻撃とその周辺状況から、「守るべき対象」をめぐる主な懸念を　下記のとおり抽出。

「ネットワーク基盤を守る」に当たっての脅威・懸念

- ✓ ネットワークの安定的運用に影響を及ぼす脆弱性を有する機器の存置
- ✓ 今後の普及が見込まれるIoT機器におけるサイバーセキュリティ技術の未実装

「組織を守る」に当たっての脅威・懸念

- ✓ 組織の機密情報等の窃取を目的とする標的型攻撃の巧妙化・複雑化
- ✓ サイバー攻撃に関する業種横断的、官民横断的な情報共有体制の未成熟
- ✓ 中小企業や地方自治体など組織におけるサイバー攻撃への対応能力の不足
- ✓ サイバーセキュリティを支える人材の量的、質的な不足

「個人を守る」に当たっての脅威・懸念

- ✓ 利用者の情報・資産等を脅かすマルウェアの高度化及び拡大
- ✓ 利用者におけるサイバーセキュリティに関するリテラシーや自助努力の不足
- ✓ 利用者側だけで対応が困難な巧妙なサイバー攻撃の出現

「我が国のネットワーク環境を守るとともに、国際社会に貢献する」に当たっての脅威・懸念

- ✓ 国境を越えたサイバー攻撃による脅威の深刻化・被害の重篤化
- ✓ 情報共有不足や国際的合意の未形成による、地域・国の間の格差の発生

「守るべき対象」と「講ずべき方策」

基本理念・基本原則

「情報の自由な流通の確保と、それによる社会経済発展の主導」

- サイバー空間の基盤である安全な情報通信ネットワーク環境の確立
- ICTの著しい環境変化への柔軟かつダイナミックな対応
- あらゆる関係主体の自律した取組と相互連携の促進
- 国際的な協調・協力関係の発展

守るべき対象

- ネットワーク基盤を守る
- 組織を守る
- 個人を守る
- 我が国のネットワーク環境を守るとともに、国際社会に貢献する

「守るべき対象」をめぐる懸念

講ずべき方策

（1）通信ネットワーク基盤の安全の確保

（2）IoT社会におけるサイバーセキュリティ上の脅威への対応

（3）情報共有体制の強化

（4）人材育成・周知啓発の推進

（5）研究開発の推進

（6）国際連携の更なる展開

世界一安全なサイバー空間

世界をリードするセキュアなIoT機器・サービス

４．講ずべき方策

（１）通信ネットワーク基盤の安全の確保

現状・背景

■ 近年、DNSやNTP等のインターネットの基盤技術を悪用したリフレクション攻撃により、ISPにおいてネットワークの輻輳が生じるなど、通信ネットワーク基盤の安定的運用に支障が生じている。

■ また、利用者が感染に気づきにくく、個人での対応が困難なマルウェアの増加や、不正に取得されたID・パスワードを悪用したWebサービスへの不正ログインなどにより、情報窃取や不正送金等の被害が発生するなど、安全な通信ネットワーク基盤が脅かされている。

■ これらの安全な通信ネットワーク基盤への脅威に対して、これまで総務省においては、研究会※1等において、リフレクション攻撃を引き起こす特定の通信※2の遮断やマルウェア感染者への注意喚起等について法的整理を行ったほか、Telecom-ISAC Japanとの連携により、ACTIVEプロジェクト※3において一般利用者のマルウェア駆除及び感染予防対策を行うとともに、パスワードリスト型攻撃への対策集※4を作成・公表するなどしてきたところである。

※1 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会
※2 利用者が設置しているブロードバンドルータ等のゲートウェイに対するインターネット側からの名前解決要求に係る通信
※3 Advanced Cyber Threats response InitiatiVE
※4 「リスト型アカウントハッキングによる不正ログインへの対応方策について（サイト管理者などインターネットサービス提供事業者向け対策集）」（平成25年12月18日公表）

課題

◆ リフレクション攻撃の踏み台となるブロードバンドルータの脆弱性は存置されたままであり、これらのルータは少数であっても十分な攻撃力を有するなど攻撃のリスクを内包した状態にあることから、安定的な通信ネットワーク基盤を確保するためにも、これらの脆弱性のあるルータを減少させる取組が必要。

◆ ID・パスワードの不正取得や利用者自身で認識・対処することが困難なマルウェアによって引き起こされる情報・財産等への被害から利用者の安全を確保し、安心してインターネットを利用できる環境を確保するため、制度的検討を含めた取組が必要。

（１）通信ネットワーク基盤の安全の確保（続き）

解決の方向性

［リフレクション攻撃の踏み台等となるブロードバンドルータ等への対策の推進］

○　リフレクション攻撃の踏み台やID・パスワード窃用の対象となり得るブロードバンドルータの利用者の特定及び注意喚起の実施に関する制度的検討の実施

○　制度的検討を踏まえた、攻撃の踏み台となり得るブロードバンドルータの利用者の特定及び注意喚起に関する実証の推進

［マルウェア感染等の被害から利用者を守るための取組の検討・推進］

○　マルウェア感染端末に攻撃指令を送り制御の中心となるC&Cサーバとの通信によって引き起こされる被害を未然に防ぐ方策等に関する制度的検討の実施

○　制度的検討を踏まえ、ACTIVEプロジェクトの枠組みを活用してTelecom-ISAC Japanと連携した、利用者被害未然防止のための実証の推進

（２）IoT社会におけるサイバーセキュリティ上の脅威への対応

現状・背景

- IoT社会の本格的到来により、センサーデバイスや自動車、テレビ、医療デバイスなど、これまでインターネットに接続されていなかったモノ・システムがネットワークに接続されることでサイバー空間の外延が大幅に拡大し、各分野においてイノベーションが創発されつつある。
- 2020年におけるIoT対応製品は約250億台、市場規模は約2,630億ドルと予想※されるなど、IoT分野での大きなビジネス拡大が見込まれているところ。この好機を捉え、2020年をマイルストーンとして我が国でセキュアなIoT機器・サービスを確立し、セキュリティをブランドとして我が国が世界を追い越しリードすることが求められる。
- IoT社会では、サイバー空間と物理空間の融合が進み、サイバー空間側の問題が、社会インフラを含む物理空間側に影響を与えうる状況が生じている。このような中、既に一部のIoT機器におけるサイバーセキュリティ上の脅威は指摘されているものの、現状において、IoT機器のサイバーセキュリティを確保するための取組は十分なされていない。

※ Gartner社調査

課題

- 拡大するサイバー空間におけるIoT機器に対する攻撃や、脆弱性のあるIoT機器から通信ネットワーク側への攻撃等について、車やウェアラブル機器等の様々なIoT機器の社会経済活動や人命への影響度を踏まえて、脅威やリスクを検証し、実装・運用上の対策について方針を示すことが必要。
- 非PC系のIoT機器の多くについては、端末の処理能力が低い、設計から廃棄までのライフサイクルが長い等の特徴を有し、既存のサイバーセキュリティ技術の実装が困難であることから、これらの特徴を踏まえ、「セキュリティ・バイ・デザイン」の考え方に基づき設計・開発段階からサイバーセキュリティを確保する新たな技術の確立・標準化が必要。
- 成長が見込まれるIoT産業において、経済性のみを追求しサイバーセキュリティが確保されていない「悪貨」が流通しないようにするためにも、脆弱性を有するIoT機器の流通・放置を防ぐ枠組が必要。

（２）IoT社会におけるサイバーセキュリティ上の脅威への対応（続き）

解決の方向性

［IoTに対する脅威分析・リスク評価の実施］

○　ペネトレーションテストを行うテストベッド等を活用したIoT機器及びその運用基盤に対する脅威分析及びリスク評価（サプライチェーン上の脅威・リスクを含む。）について多角的な観点から実施

［IoTに対応したサイバーセキュリティ技術の確立及び標準化］

○　脅威分析・リスク評価の結果等に基づき、端末の処理能力やライフサイクル等、IoTの特徴を踏まえたサイバーセキュリティ技術の確立・標準化

［IoTにおける開発・運用ガイドラインの策定］

○　上記の検証結果等を踏まえた、セキュアなIoT機器及びその運用基盤の開発・運用に係るガイドラインの策定

- 高度交通システム（ITS）におけるサイバーセキュリティを確保するガイドラインの策定
- ウェアラブル機器におけるサイバーセキュリティを確保するガイドラインの策定　等

［ネットワーク上の脆弱性を有するIoT機器への対策の推進］

○　脆弱性を有するIoT機器の調査、利用者の特定及び注意喚起の手法の確立

○　脆弱性調査・利用者特定・注意喚起・対策手法の提供等、脆弱性を有するIoT機器の利用者等に危険性を認識させ、対策を促す枠組みの構築に向けた実証の推進

（３）情報共有体制の強化

現状・背景

- サイバー攻撃に関する情報について、攻撃者側においてはソフトウェアの脆弱性や攻撃手法・ツールに関する情報がSNSや掲示板等のインターネット上にあふれているなど、容易に入手可能であるのに対して、被害者側においては攻撃の挙動や攻撃により生じる被害に関する情報等を共有するための枠組みが構築されておらず、攻撃者側と被害者側との間で情報の非対称性が生じている。
- サイバー攻撃に関する情報共有のためのこれまでの取組として、我が国においては、独立行政法人情報通信研究機構（NICT）がNICTER※１により観測された情報等をNISCやISP等に対して共有している他、電気通信分野においてはTelecom-ISAC Japanにより、また、同分野を含む重要インフラ全13分野においてはCEPTOAR※２の枠組みを通じても情報共有等が行われているところである。
- また、例えば米国においては、2015年2月、サイバー攻撃情報の政府機関間での集約のため新組織※３設置が発表されるとともに、民間部門での情報共有促進のため大統領令が制定されている。

※1　サイバー攻撃観測・分析・対策システム：Network Incident analysis Center for Tactical Emergency Response
※2　情報共有・分析機能：Capability for Engineering of Protection, Technical Operation, Analysis and Response
※3　サイバー脅威情報統合センター：Cyber Threat Intelligence Integration Center（CTIIC）

課題

- サイバー攻撃への対処に向けて、政府及び民間事業者等間で情報共有・連携が必要となる具体的なケースを想定し、いつ、どのような情報を要するか等の詳細なシミュレーションの実施が必要。
- 政府及び民間事業者等間において各々が把握する関連情報を共有するに当たっては、次に掲げる障壁が存在しており、十分な取組の実施が困難な状況。従って、官民における有機的な情報連携を促進する仕組みの構築が必要。
  - ① 組織の信頼を損ね得る情報で、情報提供によるメリットを見いだしにくい等の心理的障壁
  - ② 誰にどういった情報を提供することが可能であるか明確でない等の制度的障壁
  - ③ サイバー攻撃の手法が多岐に渡るため、共有を行う情報のフォーマットが定まっておらず、また、情報共有を行うためのプラットフォームが整っていない等の技術的障壁

（３）情報共有体制の強化（続き）

解決の方向性

［関係機関間における情報共有・連携の一層の推進］

○　電気通信分野や放送分野をはじめとする重要インフラ事業者間、政府と民間事業者間での情報共有・連携の促進

○　組織に対する標的型攻撃やネットワークに対するDDoS攻撃等への対応に向けた情報共有の心理的・制度的障壁を克服するモデルケースとして、Telecom-ISAC Japanを核とした、ICT関連事業者・組織間のサイバー攻撃に関する情報共有・連携体制の拡充、並びに先導的な情報共有・連携フレームワークの構築

○　上記モデルケースを活用し、攻撃の態様や社会的な影響度等に応じたサイバー攻撃関連情報を共有するための具体的な官民・官官連携のあり方に関する検討の実施

［情報共有・連携を行うための基盤となるプラットフォームの整備・構築］

○　サイバー攻撃に関する情報を収集・分析・共有するプラットフォームの構築に向けた技術的検証の実施

- 情報共有を行う共通データフォーマットの構築に向けた取組の推進
- 情報収集の自動化・高度化技術、収集した情報の匿名化・ビッグデータ解析技術、情報共有範囲の自動設定技術等の検証
- 情報提供者が自社と類似の攻撃事例を迅速に参照することが可能な情報共有データベースの構築

［参考］米国におけるISAC（Information Sharing and Analysis Center）

○ 官民がサイバー上の脅威等に関する情報を共有し、米国の重要インフラを守れるようなパートナーシップを構築するよう指示した大統領令（1998年）に基づき設立。

○ **2015年5月現在、米国では19のISACが活動**

○ 各セクタのISACを取りまとめる組織として、2003年にNational Council of ISACsが設立。

＜活動中のISAC＞

① Aviation ISAC（航空）
② Communication ISAC（通信）
③ Defense Industrial Base ISAC（防衛産業）
④ DNG ISAC（天然ガス供給事業）
⑤ Electricity ISAC（電力）
⑥ Emergency Management & Response ISAC（危機管理）
⑦ Financial Services ISAC（金融）
⑧ Information Technology ISAC（情報技術）
⑨ Maritime ISAC（海運）
⑩ Multi-State ISAC（自治体）
⑪ National Health ISAC（国民健康）
⑫ Nuclear Energy Institute（原子力）
⑬ Oil and Natural Gas ISAC（石油・天然ガス）
⑭ Public Transit ISAC（公共輸送）
⑮ Real Estate ISAC (Commercial Facilities ISAC)（不動産）
⑯ Research and Education ISAC（研究・教育）
⑰ Supply Chain ISAC（サプライチェーン）
⑱ Surface Transportation ISAC（陸上輸送）
⑲ Water ISAC（水）

2015年5月「National council of ISACs」公式サイト参照

＜立ち上げ準備をしているISAC＞

① Automotive（自動車）
② Chemical（化学）
③ Critical Manufacturing（重要製造業）
④ Food & Ag（食料）

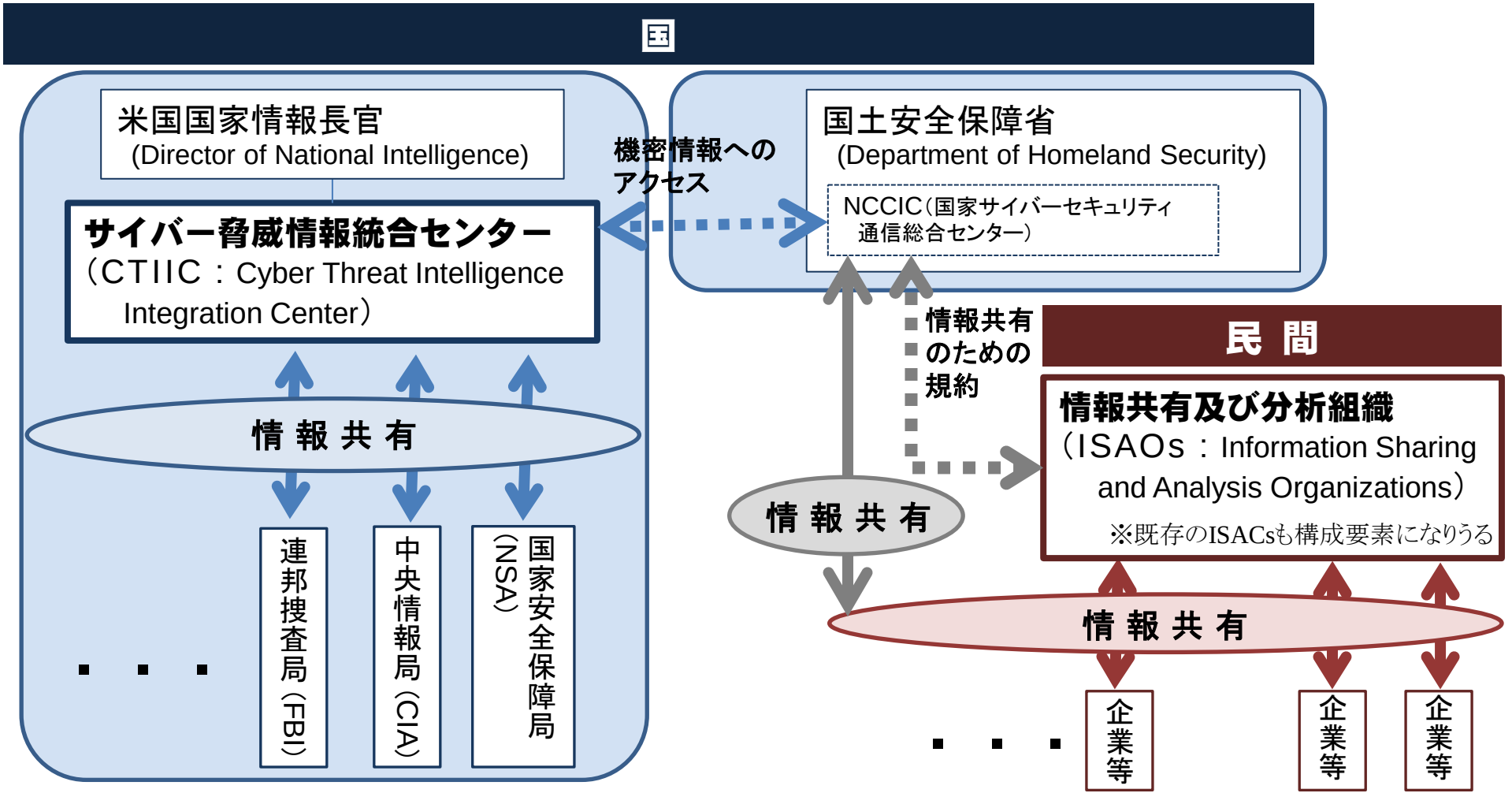
National Council of ISACsの役割

✔ 各ISACグループの代表者が毎月集まり、セクタ間の関係性強化や共通の問題等についての意見交換を実施
✔ 重大インシデント時のDHSの国家インフラ調整センタ（National Infrastructure Coordinating Center : NICC）との連絡窓口
✔ セクタの脅威レベルに関するリアルタイムでの情報提供　等

［参考］米国におけるサイバーセキュリティに係る情報共有のイメージ

●2015年2月、米国はサイバー攻撃に関して連邦省庁間での情報共有・連携を促進するための新たな組織「Cyber Threat Intelligence Integration Center（CTIIC）」の創設を発表。

●同月、オバマ大統領が民間部門におけるサイバーセキュリティに係る情報共有を促進するための大統領命令を発表するとともに、同命令案に署名。



（4）人材育成・周知啓発の推進

現状・背景

- 近年、ICTの利活用が広く普及する中で、標的型攻撃による機密情報の窃取やオンラインバンキングの不正送金による金銭的被害の発生等、あらゆる主体にサイバー攻撃の脅威が及ぶようになっている。
- これらサイバー攻撃の脅威に対する対処能力を底上げするための取組として、これまで総務省においては、CYDER※1や各府省庁対抗インシデント・ハンドリング戦技競技会※2の実施等を通じた組織における人材育成を実施するとともに、サイバーセキュリティ対策についての基本的情報を紹介するWebサイトの運用や、サイバーセキュリティ月間とも連携したセミナーの実施等を通じた、主に一般の個人を対象とした周知啓発活動を推進してきたところ。

※1　実践的サイバー防御演習：CYber Defense Exercise with Recurrence
※2　NATIONAL 318（CYBER）EKIDEN

課題

- サイバーセキュリティ対策のスキル育成には、実環境またはそれに近い模擬環境において実践的な防御経験を積み重ねることが有効であり、そのための各種演習等に活用可能な大規模共通基盤を整備することが必要。
- マイナンバー制度の導入を控える地方公共団体や、我が国のものづくりの源泉としてサプライチェーンの一端を担う中小企業等においては、今後想定されるサイバーセキュリティ上の脅威に対して十分な備えを講じる必要があり、さらに世界中から注目が集まる2020年オリンピック・パラリンピック東京大会の関係組織等はサイバー攻撃の格好の標的となり得ることから、これらの組織の実情・ニーズに合わせたサイバー攻撃への対処能力を向上させる取組が必要。
- また、サイバーセキュリティに関する周知啓発にあたっては、一般の個人に対してのみではなく、組織内でのセキュリティへの投資を促進することも見据え、経営者層を含む幅広い層に対して、サイバーセキュリティへの理解を促す取組が必要。

（４）人材育成・周知啓発の推進（続き）

解決の方向性

［演習基盤の構築・活用による実践的人材の育成］

○　サイバー攻撃から組織のネットワークを多角的・多層的に防御するための演習基盤の強化及び更なる活用による実践的人材の育成

- 組織等のネットワーク構成を柔軟に模擬できる大規模模擬環境を備えた、サイバー防御のための演習基盤の構築
- 演習基盤を活用した、地方公共団体や中小企業等に対する実践的サイバー防御演習の実施
- 演習基盤を活用した、政府機関等に対するサイバー防御演習の継続的実施
- 演習基盤を活用した、2020年オリンピック・パラリンピック東京大会も見据えた大規模演習の検討

［多角的な人材の育成］

○　サイバーセキュリティに関する研究開発や実証実験プロジェクト等への参加を通じた、実践的スキルを備えた人材育成の推進

○　サイバーセキュリティに関する一般的な知識を幅広く有し、周囲の一般利用者への周知啓発を担える人材育成の推進

○　サイバーセキュリティに関する技術のみではなく、関連制度等にも精通したハイブリッド人材育成の推進

［サイバーセキュリティに関するリテラシー向上やセキュリティ対策実施促進のための周知啓発］

○　経営者層等を含む幅広い層を訴求対象とした、サイバーセキュリティの重要性に関する周知啓発等の推進

○　初等・中等教育段階からICTに対する理解を促す教育を実施し、その中でサイバーセキュリティに関するリテラシーも向上させる取組の推進

（５）研究開発の推進

現状・背景

- ICT分野においては技術が日夜進歩しており、それに伴い、サイバーセキュリティについても攻撃・防御の両面においてめまぐるしい速さで技術の高度化・多様化が進展している。
- これらの技術革新を先導し、安全な通信ネットワークインフラを構築するため、これまで、総務省においてはPRACTICE※１、NICTにおいてはNICTER※２やDAEDALUS※３等の研究開発プロジェクトを実施してきたところ。
- また、サイバーセキュリティの基盤をなす暗号技術についても、CRYPTREC※４において安全性の評価・監視等を実施するとともに、NICTにおいて必要な研究開発を実施してきたところ。

※1　国際連携によるサイバー攻撃予知・即応技術の研究開発：Proactive Response Against Cyber-attacks Through International Collaborative Exchange
※2　サイバー攻撃観測・分析・対策システム：Network Incident analysis Center for Tactical Emergency Response
※3　対サイバー攻撃アラートシステム：Direct Alert Environment for Darknet And Livenet Unified Security
※4　クリプトレック：Cryptography Research and Evaluation Committees

課題

- 巧妙化した新たなサイバー攻撃に対して、後手に回ることなく予兆段階等から先手を打つプロアクティブな対応を可能とするため、サイバー攻撃のリアルタイム観測網やビッグデータ解析技術等を駆使して、十分なサイバー・レディネスを実現するとともに、サイバー攻撃への対処に係るコストを引き下げることが必要。
- 経済のグローバリゼーションの進展に伴うサプライチェーン上のセキュリティリスクについて、技術的な観点からも対応が必要。
- 我が国のセキュリティ産業の発展や安全保障の観点も踏まえ、暗号技術やその利活用のための技術など、サイバーセキュリティに関する基盤技術の継続的な研究開発が必要。
- さらに、サイバーセキュリティに関する研究開発の推進には、トラヒック情報やマルウェア検体情報などの基礎データへの十分なアクセスの確保や、研究開発に際して許容される行為の範囲の整理等が必要。

（５）研究開発の推進（続き）

解決の方向性

［サイバー攻撃へのプロアクティブな対応を可能とする技術に関する研究開発］

○　サイバー攻撃の観測技術や、収集された攻撃情報をAI（人工知能）やビッグデータ等の技術の活用を通じた分析・解析により効率的な対処に繋げる技術など、次々と現れる新たなサイバー攻撃に対して後手に回ることなく予兆段階等から先手を打つプロアクティブな対応を可能とするための研究開発の推進

［サプライチェーン上のセキュリティリスクに対応するための技術に関する研究開発］

○　「セキュリティ・バイ・デザイン」の考え方に基づいた機器の設計・開発段階からのサイバーセキュリティの確保とともに、その上で残る機器の仕様外の機能・動作を検知し対処するための技術等の研究開発の推進

［基盤技術に関する研究開発］

○　サイバー空間における情報のやり取りの安全性・信頼性を確保するために必要となる、高度な機能や安全性をもつ暗号技術やその応用技術（暗号プロトコル等）など、基盤技術の研究開発の推進

［研究開発を支える環境整備］

○　研究開発に有用な産学官各々が保有するデータの共有や、研究開発目的でのマルウェアの挙動解析など研究開発に際して許容される行為の範囲についての制度的な検討、サイバーセキュリティ対策技術の効果測定手法の検討など、研究開発を支える環境整備の推進

（６）国際連携の更なる展開

現状・背景

- サイバー空間がグローバルな広がりをもつことから、セキュリティを確立し、情報の自由な流通や安全な情報通信ネットワーク環境を確保のためには、諸外国との連携が不可欠。これを踏まえ、ASEAN諸国や米国、欧州を始めとする各国との連携の在り方について検討してきた。
- 新しいサイバー空間におけるセキュリティに関する国際的合意形成や標準化へ関与の重要性を認識し、日ASEANセキュリティ政策会議や各種サイバー対話等において出来る限りの情報発信及び収集につとめているところ。
- 並行して、欧米主要国及びASEAN諸国との「国際連携によるサイバー攻撃予知・即応技術の研究開発(PRACTICE)」や日欧共同研究プロジェクトなど、具体的なプロジェクトベースの連携により、相互理解の一層の促進と知見の共有を進めている。特にASEAN諸国に対しては「人材育成イニシアティブ」の推進など、人材育成を通した能力構築への貢献を通じ、より強固な信頼関係の醸成につとめている。

課題

- プロジェクトベースの連携については、既存の取組をさらに高度化しつつ、IoTなどの新しい環境・アーキテクチャに対応する調査・研究への取組に関しても、国際的知見を取り入れ、先導的な対応をしていくことが必要。
- 国際的な要請及び我が国との地理的関係から、ASEANなどの重点地域に対しては更なる実践的な能力構築を支援をしていくため、現地の状況やニーズを十分に踏まえた、多様な人材育成支援メニューの提供が必要。
- 上記のような活動に加え、より積極的に情報収集・発信することにより、主要関係国との相互理解の更なる促進とそれに基づく信頼醸成や基本的態度の共有が必要であり、さらには国際的な規範形成の場での我が国のプレゼンス向上及び仲間作りにつなげる必要がある。

（６）国際連携の更なる展開（続き）

解決の方向性

［先進国との先導的な共同プロジェクト、重点地域とのデータ共有・活用プロジェクトの推進］

○　新たな先導的共同プロジェクトの推進
- M2M/IoTセキュリティ、ビッグデータ分析、自動化　等

○　日欧共同研究開発プロジェクトの推進、及び日米共同研究開発プロジェクトの創出

○　ASEAN等との間でのJASPER/PRACTICEで得られたデータの共有、活用　等

［ASEAN等重点地域を中心とした、実践的な能力構築への支援］

○　現地の状況やニーズを十分に踏まえた、多様な人材育成支援メニューの提供
- システム管理者等を対象とした実践的サイバー演習(CYDER)国際展開、ISP等を対象としたセミナー開催　等

○　実践的なセキュリティ能力構築支援
- ミャンマー、インドネシア等へのODA案件を通じた能力構築支援　等

［各種会議等への積極的な参加による国際貢献］

○　政策対話、国際会議等への積極的な貢献
- 日ASEAN情報セキュリティ政策会議、各種サイバー対話、ICT政策対話等での情報発信／情報収集　等

○　標準化活動への積極的な貢献
- ITU-Tにおける活動（M2M、ITS等）への積極的な参加　等

５．2020年オリンピック・パラリンピック東京大会に向けた取組

2020年オリンピック・パラリンピック東京大会に向けた取組

基本的な考え方

■ 2020年オリンピック・パラリンピック東京大会は、我が国のICT分野の最先端の技術・サービス・インフラを世界に示すショーケースとして絶好の機会であると同時に、そこで万が一にも何らかのセキュリティ上のインシデントが発生すれば、国の威信（レピュテーション）に関わる重大な事態となる。「おもてなし」と「セキュリティ」の両立が大会成功の鍵。

■ サイバーセキュリティをめぐり、政府・企業等における対策強化、関係者間の連携強化、人材育成など課題が山積する中で、「安全・安心な2020年東京大会の開催」は、国を挙げて、あらゆる関係主体の協力の下でこれらの課題解決に取り組み、我が国が世界に先駆けた最先端のセキュリティ基盤を構築するための共通の目標となり得るもの。

■ 2020年東京大会を最終的なゴールとするのではなく、東京大会をマイルストーンとして構築した我が国の最先端のセキュリティ基盤を、2020年以降も東京大会の資産（レガシー）として持続・発展させ、我が国がIoT社会におけるセキュリティで世界をリードしていくことが必要。

2020年オリンピック・パラリンピック東京大会に向けた取組（続き）

これまでの取組

【政府】　・2014年10月に「2020年オリンピック・パラリンピック東京大会等に関する閣僚会議」の下に「セキュリティ幹事会」及び「サイバーセキュリティワーキングチーム」を設置し、関係省庁が連携して東京大会におけるサイバーセキュリティ対策についての検討を実施中。

【大会組織委】・2015年2月に「東京2020大会開催基本計画」を作成し、IOC・IPC※に提出。　※国際オリンピック委員会・国際パラリンピック委員会

［基本計画中のサイバーセキュリティ関連記述（抜粋）］

4章：大会を支える機能/セキュリティ/主要目標
「関係機関と緊密に連携し、テロ、大規模災害等緊急事態の発生やサイバー空間における脅威に対処できるよう、将来の緊急事態への対処体制の構築を見据えつつ、大会運営上必要な体制や仕組みを確保すること。」

6章：アクション＆レガシー/街づくり・持続可能性/誰もが安全で快適に生活できる街づくりの推進
「大会期間中の災害やテロ、サイバー攻撃等を想定した、官民一体となったセキュリティ体制の構築と治安基盤の強化」

今後求められる取組

○　2012年ロンドン大会が“SNS五輪”、“スマホ五輪”であったとすれば、2020年東京大会は“IoT五輪”。その安全・安心な開催のため、まずIoT社会に対応した脅威分析を実施してリスクを明らかにした上での対策の検討が必要。

○　東京大会に向けた新たなネットワークインフラの構築に当たっては、外国人観光客にも使いやすい公衆無線LAN環境の整備など利便性の確保と、セキュリティの確保を両立させながら進めることが必要。

○　東京大会に関連して発生するサイバーセキュリティ上の大量のインシデント情報を関係者間で効果的に共有するための体制・仕組みを構築し、関係者間の連携を十分に強化してサイバー攻撃に対抗していくことが必要。

○　東京大会の開催に向けて、その前年に国内で開催されるラグビーワールドカップ2019も考慮に入れて官民の関係者で実際の大会を想定した演習を繰り返し実施し、計画的に実践的なサイバー攻撃対応能力を育成することが必要。

○　東京大会におけるサイバーセキュリティの確保に当たり、大会の性質に鑑みて、期間や地域を限定して特別な取組を実施する必要性についても検討が必要。

提言 全体像

提言 全体像

2020年オリンピック・パラリンピック東京大会までに世界一安全なサイバー空間を実現

既存の枠組を超えた連携強化
- 重要インフラ事業者等の枠組を超えた産学官連携の推進

IoT社会を見据えたネットワークセキュリティ基盤の構築
- ユーザのマルウェア感染を未然に防ぐ取組の推進
- 脆弱性を有するネットワーク機器への対策を促す枠組の構築
- ＩｏＴ機器等のセキュリティを確保するガイドラインの策定及び技術の確立　等

国際展開・連携の更なる推進
- 国際的な信頼醸成に向けた各種プロジェクトの推進

サイバー攻撃への対処を促す情報共有体制の強化
- 関係者間の効果的な連携を促すTelecom-ISAC Japanを核とした体制強化
- 情報共有・連携を行うための基盤となるプラットフォームの整備・構築　等

実践的能力を有する人材を育成する演習基盤の構築
- 各種演習等に活用可能な大規模共通基盤を整備
- オリンピック・パラリンピックを想定した演習による大会組織の対応能力強化　等

研究開発の推進
- サイバー攻撃へのプロアクティブな対応を可能とする技術の研究開発　等

（自動化・ＡＩ（人工知能）・ビッグデータ　等）

情報セキュリティ アドバイザリーボードにおける検討体制

情報セキュリティ アドバイザリーボードにおける検討体制

2015年1月より、情報セキュリティ アドバイザリーボード（親会）及び新たに設置した戦略ワーキンググループにおいて、「提言」とりまとめに向けた集中的な議論を実施。

情報セキュリティ アドバイザリーボード（親会）

【目的】

情報セキュリティの推進に当たり、短期的及び中長期的に講ずべき対策や既存の取組の改善などの方向性について幅広い観点から助言を行うとともに、情報セキュリティに係る諸問題への対応について、必要に応じて提言をとりまとめるために開催。

【構成（敬称略）】

構成員（座　　長）	徳田　英幸	慶應義塾大学 環境情報学部 教授
（座長代理）	林　紘一郎	情報セキュリティ大学院大学 前学長・教授
	飯塚　久夫	一般財団法人日本データ通信協会 テレコム・アイザック推進会議 会長
	岡村　久道	弁護士、国立情報学研究所 客員教授
	宮地　充子	北陸先端科学技術大学院大学 情報科学研究科 教授
顧問	小野寺　正	KDDI株式会社 代表取締役会長
オブザーバ	内閣官房 内閣サイバーセキュリティセンター	

（今後必要に応じて体制見直しを行う）

総合ワーキンググループ

（主査）上原　哲太郎
立命館大学情報理工学部 教授

（概要）
「ワーキンググループ」の体制・活動を継続し、メーリングリスト等により有識者間の情報共有及び総務省より提案する各種検討事項の審議等を実施する。

戦略ワーキンググループ

（主査）中尾　康二
KDDI株式会社 運用本部 顧問／
NICT ネットワークセキュリティ研究所
主管研究員

（概要）
サイバーセキュリティ基本法の成立を踏まえ、次期サイバーセキュリティ戦略の策定等を見据えて今後取り組むべき課題について検討を実施する。

ITSワーキンググループ

（主査）松本　勉
横浜国立大学大学院
環境情報研究院 教授

（概要）
「ITSセキュリティ検討グループ」（平成26年2月～）を改組。移動通信課において行う700MHz帯を活用した安全運転支援システムに関する実証の成果をフィードバックする。

情報セキュリティ アドバイザリーボード 戦略ワーキンググループ　構成

※ 敬称略

構成員

（主査）	中尾　康二	KDDI株式会社 運用本部 顧問／ 独立行政法人情報通信研究機構 ネットワークセキュリティ研究所 主管研究員
	我妻　三佳	日本アイ･ビー･エム株式会社 GTS事業 ITSデリバリーセキュリティー＆ネットワーク･サービス 理事
	稲田　修一	東京大学 先端科学技術研究センター 特任教授
	小林　成年	株式会社TBSテレビ 情報システム局 担当局次長
	鵜飼　裕司	株式会社FFRI 代表取締役社長
	小屋　晋吾	トレンドマイクロ株式会社 執行役員 統合政策担当部長
	小山　　覚	NTTコミュニケーションズ株式会社 経営企画部 マネージドセキュリティサービス推進室 担当部長
	齋藤　　衛	株式会社インターネットイニシアティブ サービスオペレーション本部 セキュリティ情報統括室長
	高橋　正和	日本マイクロソフト株式会社 チーフセキュリティアドバイザー
	舘　　剛司	公益財団法人東京オリンピック･パラリンピック競技大会組織委員会 テクノロジーサービス局 局長
	寺田　真敏	株式会社日立製作所 情報通信システム社 Hitachi Incident Response Team　副センタ長／ チーフコーディネーションデザイナ／チーフテクノロジデザイナ
	名和　利男	株式会社サイバーディフェンス研究所 理事／上級分析官
	土生　　尚	日本放送協会 情報システム局 IT企画部 部長
	吉岡　克成	横浜国立大学大学院 環境情報研究院 准教授
	吉田　万貴子	日本電気株式会社 中央研究所 研究企画本部 イノベーションプロデューサー

オブザーバ

内閣官房 内閣サイバーセキュリティセンター

経済産業省 商務情報政策局 情報セキュリティ政策室