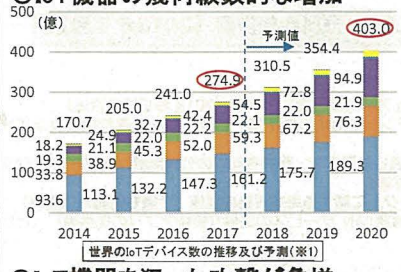
警視庁様サイバーセキュリティセミナー意見交換会資料

総務省関東総合通信局
平成31年1月29日

IoTセキュリティ総合対策（2017年10月公表）

現状

○IoT機器の幾何級数的な増加



世界のIoTデバイス数の推移及び予測（※1）

・2017年時点でIoT機器の数は約275億個と推定。
・2020年までに403億個まで1.5倍に増える見込み。

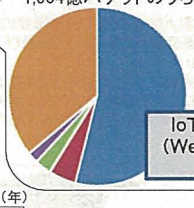
（出典）IHS Technology

○IoT機器を狙った攻撃が急増

IoT機器を狙った攻撃は約5.7倍

1年間で観測されたサイバー攻撃のパケット数（※2）

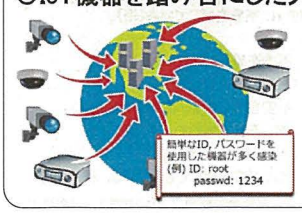
観測された全サイバー攻撃1,504億パケットのうち、



半数以上がIoTを狙っている！

IoT機器を狙った攻撃（Webカメラ、ルータ等）54%

○IoT機器を踏み台にした大規模攻撃が発生



・2016年10月21日米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が2回発生。
・同社からDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生。
・サイバー攻撃の元は、「Mirai」というマルウェアに感染した大量のIoT機器。

（※1）及び（※2）・・・ 総合対策公表時から数値を現行化。

対策

IoTセキュリティ総合対策

脆弱性対策に係る体制の整備

・IoT機器の脆弱性についてライフサイクル全体（設計・製造、販売、設置、運用・保守、利用）を見通した対策が必要。
・脆弱性調査の実施等のための体制整備が必要。

研究開発の推進

・セキュリティ運用の知見を情報共有し、ニーズにあった研究開発を促進。

民間企業等におけるセキュリティ対策の促進

・民間企業等のサイバーセキュリティに係る投資を促進。
・サイバー攻撃の被害及びその拡大防止のための、攻撃・脅威情報の共有の促進。

人材育成の強化

・圧倒的にセキュリティ人材が不足する中、実践的サイバー防御演習等を推進。

国際連携の推進

・二国間及び多国間の枠組みの中での情報共有やルール作り、人材育成、研究開発を推進。

半年に1度を目途としつつ、必要に応じて検証（関係府省と連携）

総合対策の進捗状況や今後の取組方針を整理し、「プログレスレポート」として公表

脆弱性対策に係る体制の整備

設計・製造段階
- ■IoT機器のセキュリティ対策に係る認証制度について、IoT推進コンソーシアムの作業部会において本年7月に取組方針を決定。これに基づき、引き続き検討。
- ■情報通信審議会（IPネットワーク設備委員会）において、本年6月、IoT機器を含む端末設備の技術基準に最低限のセキュリティ対策を追加することについて、報告書案をとりまとめ。今後、関係省令等の改正など所要の手続きを進める。

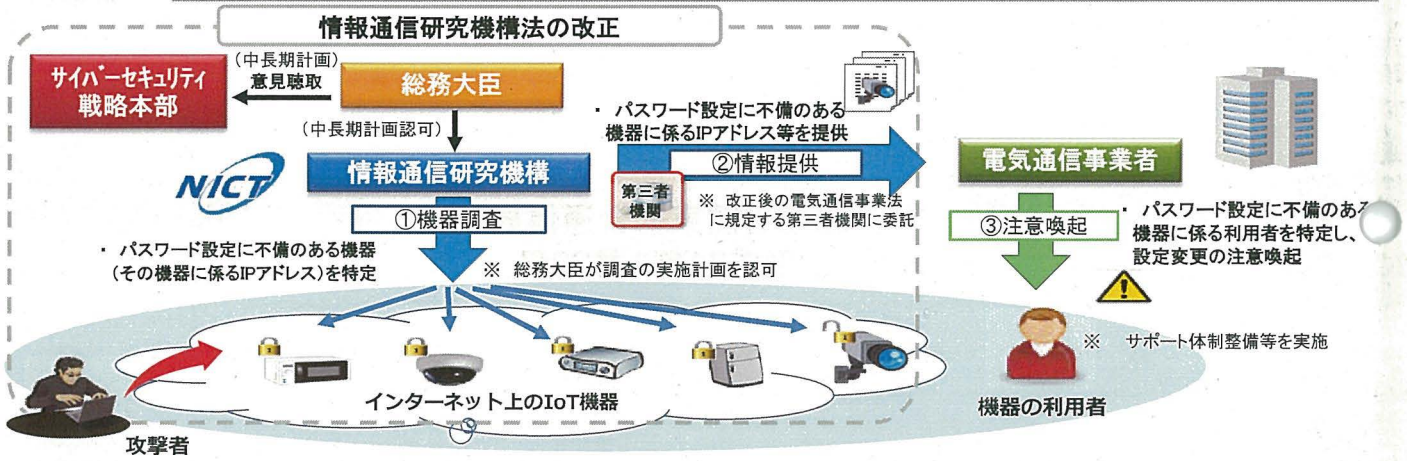
販売段階
- ■認証マーク付与の仕組み等について、上記IoT推進コンソーシアムにおいて引き続き検討。

設置段階
- ■2017年度においてIoTセキュアゲートウェイの実証実験を実施（2018年6月に成果公表）。実証を通じて明らかになった課題の検証等を継続。

運用・保守段階
- ■IoT機器のセキュリティ検査や人材育成を行う地域拠点の整備について検討。
- ■脆弱性チェックのためのツール開発について、民間の活動を積極的に支援。ツールが実装すべき共通要件について、ガイドラインの策定を検討。

利用段階
- ■NICTが行うIoT機器の脆弱性調査（下記）に関連して、サポートセンターを設置。
- ■地方総合通信局等におけるセキュリティ対応体制の強化（2018年夏）。

利用段階
- ■2017年度に実施したIoT機器の脆弱性調査（総務省、横浜国立大学、ICT-ISAC）の結果を公表（2018年7月）。
- ■NICT法改正（2018年通常国会）を踏まえ、NICTによるIoT機器の脆弱性調査実施に向けた所要の手続を実施し、2018年度中に調査を開始。その際、上記の調査結果で得られた知見を活用。
- ■電気通信事業法改正（2018年通常国会）を踏まえ、電気通信事業者間の情報共有の結節点となる第三者機関（ICT-ISACを想定）の認定に向けた所要の手続を実施。



民間企業等におけるセキュリティ対策の促進

行動計画の明確化

情報開示分科会報告書（2018年6月）

- ■人材（戦略マネジメント層）のスキルの具体化、スキル取得のための教育コンテンツの開発・普及、スキル認定を行う仕組みを産学官により構築するための検討。（平成30年度中を目途に方向性を整理）
- ■米国等におけるISAO（Information Sharing and Analysis Organization）等の動向等について調査するとともに、公的支援のあり方について検討。（平成30年度中を目途に検討結果を取りまとめ）
- ■セキュリティベンダー、損害保険会社、その他の関連する企業によるサイバーセキュリティ保険を含む総合サービスの開発に向けたモデル事業を推進し、標準仕様化に向けて検討。また、企業のセキュリティ対策の強度を簡易に診断できるツールキットを評価する仕組みづくりを検討。（モデル事業については平成30年度に検討）
- ■「セキュリティ対策情報開示ガイドライン」（仮称）を策定・公表。（平成30年秋を目途にガイドラインを策定）
- ■「コネクテッド・インダストリーズ税制」の活用状況を分析するとともに、企業のニーズ等を反映した投資促進のための政策支援のあり方について検討。（支援税制の運用にあわせて適宜実施）

公衆無線LANセキュリティ分科会報告書（2018年3月）

■利用者・提供者の意識向上
- ○ Wi-Fi 利用者・提供者向けマニュアル（手引き）の改定（2018 年夏頃を目途）
- ○ オンライン教育等の教育コンテンツを活用した周知・啓発（2018 年秋頃を目途に開始）
- ○ e-ネットキャラバン等の活動を通じた青少年・高齢者向けの公衆無線LAN の利用に関する周知・啓発（2018 年度以降に実施）
- ○「公衆無線LAN 版安全・安心マーク」に関する周知活動の実施（今後も継続的に実施）
- ○ 暗号化の有無を識別可能な公衆無線LAN サービスの提供（接続アプリの提供等）（民間事業者の取組に期待）

■データ利活用施策との連携
- ○ 公衆無線LAN サービスとIoT おもてなしクラウドとの連携推進（2019 年中を目途に実用化）

■優良事例の普及
- ○ 自治体に対する公衆無線LAN 環境整備支援事業の継続的推進（2019 年度まで継続）及び優良事例の普及促進（優良事例の調査・公表及びこれを踏まえた所要の政策支援については2018年夏以降に実施）
- ○ デジタルスタジアムの実現に向けたセキュアな公衆無線LAN 環境の整備及び公衆無線LANサービスのSSID 等の情報や接続アプリを、オリンピック・パラリンピック公式サイトといった信頼できるサイトにおいて提供する仕組みの構築（2018 年度以降に実施）

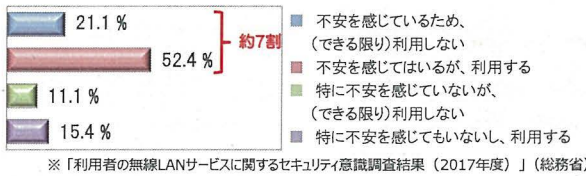
コネクテッド・インダストリーズ税制（平成30～32年度）

○ 一定のサイバーセキュリティ対策が講じられたデータ連携・利活用により、生産性を向上させる取組について、それに必要となるシステムや、センサー・ロボット等の導入に対して、特別償却30%又は税額控除3%（賃上げを伴う場合は5%）を措置。

○ 事業者は当該取組内容に関する事業計画を作成し、主務大臣が認定。認定計画に含まれる設備に対して、税制措置を適用。

利用者における公衆無線LANのセキュリティに対する意識

・ 利用者の約7割が公衆無線LANのセキュリティに不安を感じている（※）。



※「利用者の無線LANサービスに関するセキュリティ意識調査結果（2017年度）」（総務省）

研究開発の推進

広域ネットワークスキャンの軽量化

○ 効率的な広域ネットワークスキャンの実現を目指し、**平成30年度から研究開発**を実施。

○ 今後、本研究開発の成果をIoT機器の脆弱性調査に随時適用し、調査の効率化に取り組む。

ハードウェア脆弱性への対応

○ 「戦略的情報通信研究開発推進事業（SCOPE）」において、**平成29年度に採択**した「IoT部品・機器・ネットワークの階層横断セキュリティ技術の研究開発」を実施中。

○ **平成30年度において**上記の取組の一環として、IoT機器の不正動作を検出し、高速にIoT ネットワークを正常回復する仕組みを構築することを目標として**研究開発を実施**。

国立研究開発法人 情報通信研究機構 National Institute of Information and Communications Technology

NICTにおける基礎的・基盤的な研究開発の推進

スマートシティのセキュリティ対策の強化

○ NICTにおいて、欧州委員会（EC）と連携し、「欧州との連携によるハイパーコネクテッド社会のためのセキュリティ技術の研究開発」を推進。

○ 国際的な動向も踏まえ、平成29年度から実施している「データ利活用型スマートシティ推進事業」で得られた知見も活かしつつ、**スマートシティにおけるセキュリティ確保策について検討を開始し、年内を目途に一定の結論**。

AIを活用したサイバー攻撃検知・解析技術の研究開発

○ **NICTにおいて**、機械学習等を応用した通信分析技術の高度化と試験運用を行うなど、AIを活用したサイバー攻撃の検知・解析環境の構築及び当該検知・解析の自動化に関する**研究開発を推進**する。

衛星通信におけるセキュリティ技術の研究開発等

○ 安全な衛星通信ネットワークの構築を可能とし、盗聴や改ざんが極めて困難な**量子暗号通信を超小型衛星に活用するための技術の確立**に向け、**平成30年度から**「衛星通信における量子暗号技術の研究開発」を実施。

人材育成の強化

NICTにおける人材育成

NICTナショナルサイバートレーニングセンター（2017年4月設立）

CYDER
Cyber Defense Exercise with Recurrence

実践的な防御演習（2013年～）

国の行政機関、地方公共団体、独立行政法人及び重要インフラ事業者等を対象とした実践的サイバー防御演習（年間約3,000名）

cyber colosseo

東京大会に向けた人材育成（2018年2月～）

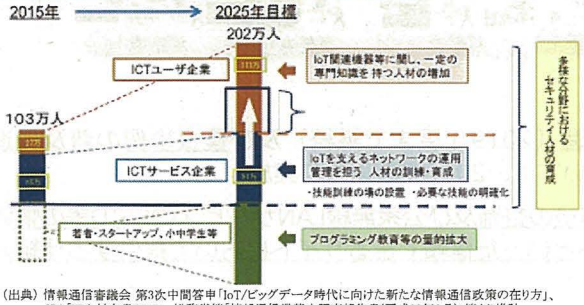
東京2020オリンピック・パラリンピック競技大会に向けた大会関連組織のセキュリティ担当者等を対象者とした実践的サイバー演習（最終的に220名を育成予定）

SecHack365

若手セキュリティエンジニアの育成（2017年度～）

若手セキュリティイノベーターの育成（年間約50名）

IoTセキュリティ人材の育成



（出典）情報通信審議会 第3次中間答申「IoT/ビッグデータ時代に向けた新たな情報通信政策の在り方」、IPA「IT人材白書2015」、総務省等「情報通信業基本調査報告書(平成28年3月)」等より推計

IoTセキュリティに関するスキルを獲得するための**教材作成や研修体制の整備**、マルウェア等の**データの共有**、機器の脆弱性に係る**接続試験を行うテストベッドの構築**等を行うための**総合的な対策**について検討。

国際連携の推進

ASEAN各国との連携

○ ASEANとの人材育成協力の強化を目指す「**日ASEANサイバーセキュリティ能力構築センター**」（**2018年8月以降本格稼働予定**）に対する支援・助言を実施。
○ 「日ASEANサイバーセキュリティ政策会議」（2018年10月）や「ISP向け日ASEAN情報セキュリティワークショップ」（2019年2月）等を通じた政策対話を推進。

国際的なISAC間連携

○ **日米ISAC間の脅威情報の自動共有**をはじめとするサイバーセキュリティ連携対策を更に促進するため、「第3回ISAC間連携国際ワークショップ」を開催（2018年度内）。

国際標準化の推進

○ ITU-T SG17における「IoTセキュリティガイドライン」をベースとした勧告・標準の策定に向けた取組に貢献。
○ EUにおいて、トラストを担保する仕組みであるeIDAS規則が運用されていることを踏まえ、EUのトラストリストとの相互認証を目指した**実証試験（トラストサービスの実現）**を検討。

サイバー空間における国際ルールを巡る議論への積極的参画

○ 国連をはじめ、G7やG20、二国間協議を通じた議論に積極的に参画。
○ 特に**G20（2019年）**については、主催国として、サイバー空間における**国際ルールを巡る議論についても主導的役割**を果たす。

セキュアな公衆無線LAN環境の実現に向けた行動計画（2018年3月）

1. 利用者・提供者の意識向上

（国における取組）

① Wi-Fi利用者・提供者向けマニュアル（手引き）の改定（2018年夏頃を目途）
② オンライン教育等の教育コンテンツを活用した周知・啓発（2018年秋頃を目途に開始）
③ e-ネットキャラバン等の活動を通じた青少年・高齢者向けの周知・啓発（2018年度以降に実施）
④ 「公衆無線LAN版安全・安心マーク」に関する周知活動の実施（今後も継続的に実施）

公衆無線LAN版
安全・安心マーク

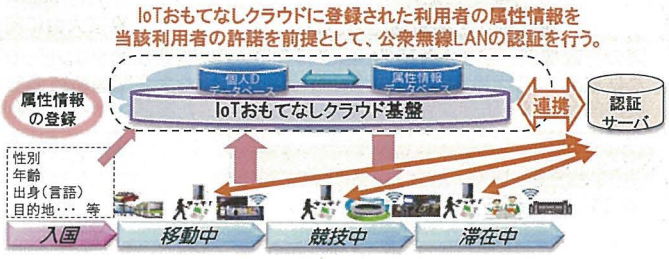
（民間事業者における取組）

⑤ 暗号化の有無を識別可能な公衆無線LANサービスの提供（接続アプリの提供等）（民間事業者の取組に期待）

2. データ利活用施策との連携

（国・民間事業者における取組）

① 公衆無線LANサービスとIoTおもてなしクラウドとの連携推進（2019年中を目途に実用化）



3. 優良事例の普及

（国・民間事業者等における取組）

① 自治体に対する公衆無線LAN環境整備支援事業の継続的推進（2019年度まで継続）及び優良事例の普及促進
（優良事例の調査・公表及びこれを踏まえた所要の政策支援については、2018年夏以降に実施）

② デジタルスタジアムの実現に向けたセキュアな公衆無線LAN環境の整備及び公衆無線LANサービスのSSID等の情報や接続　　アプリを、オリンピック・パラリンピック公式サイトといった信頼できるサイトにおいて提供する仕組みの構築（2018年度以降に実施）

公衆無線LAN版安全・安心マークについて

公衆無線LAN版安全・安心マークの概要

<公衆無線LAN版安全・安心マーク>

○インターネット接続サービス安全・安心マーク推進協議会では、**公衆無線LANサービスを提供している事業者や自治体等を対象に、**セキュリティ対策や個人情報保護への取組等が一定基準に達している目安となる**「公衆無線LAN版安全・安心マーク」を付与**しているところ（平成29年から実施）。

○これは、**利用者にとっては安全・安心な公衆無線LANサービスを選定する際の目安**となるだけでなく、マークを取得した事業者や自治体等にとっては、**自身がセキュアな公衆無線LANサービスの提供者であることをアピールする材料**になるもの。

マーク取得に必要な手続等

1　審査

マークの取得に当たっては、協議会の審査に合格する必要がある。協議会から委嘱された一般社団法人日本インターネットプロバイダー協会、一般社団法人テレコムサービス協会及び一般社団法人電気通信事業者協会が審査基準に規定された審査項目（※１）に従って審査を実施した上で、協議会に設置された安全・安心マーク審査委員会において合格を決定。

2　審査申請書

審査を受ける際に必要となる**「審査申請書」は協議会ウェブサイトから取得**でき、上記３団体において申請を受け付けている（上記３団体の非会員であっても、マークの取得は可能）。

3　審査料金

新規審査料金　40,000円（※２）、更新審査料金　30,000円（※３）

※２　10,000円（当分の間、値引きを実施）

※３　インターネット接続サービス版安全・安心マークを取得済の者の場合、20,000円

4　マークの有効期限

発行日から起算して１年間

（有効期限満了前に更新審査を受け、合格しない場合、マークの継続使用は不可）

5　参考

協議会ウェブサイト　https://www.isp-ss.jp/

※１　審査項目の例

1　無線区間の暗号化又はその手法の案内

1-1　提供している公衆無線LANの暗号化対策の状況（次のいずれかの対応を実施しているか）

・WPA2以上の暗号化

・HotSpot 2.0(Next Generation HotSpot)

・VPN等のセキュアな接続環境の提供

・VPN等の案内

2　ユーザー利用規約又は契約約款等の整備と公表

2-1　ユーザー利用規約又は契約約款等の内容（公衆無線LANを利用しようとする者に対して、サービス内容を適切に記した規約等を整備している場合、その規約等の内容）

2-2　サービス内容や規約等の提示方法（次のいずれかの対応を実施しているか）

・SSIDを指定すると自動的に表示

・案内書、ポスター等で掲示

・その他（公表方法を具体的に記述すること）

IoT機器調査及び利用者への注意喚起プロジェクト

改正情報通信研究機構法に基づき、本年２月より情報通信研究機構（NICT）がパスワード設定等に不備のあるIoT機器を調査し、電気通信事業者を通じた利用者への注意喚起を行うプロジェクト「NOTICE※」を開始。

※National Operation Towards IoT Clean Environment

＜本プロジェクトの概要＞

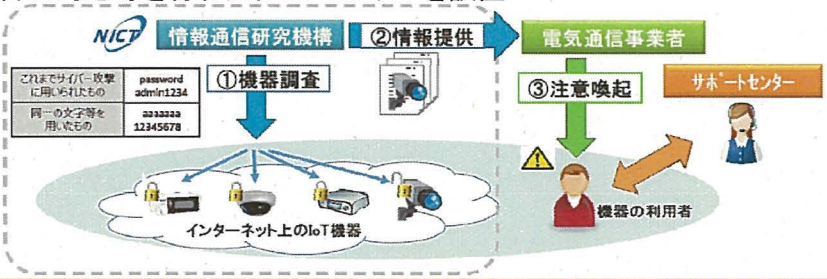
①NICTがインターネット上のIoT機器の調査を行い、パスワード設定等に不備のあるIoT機器を特定。

②当該機器の情報を電気通信事業者に通知。

③電気通信事業者が当該機器の利用者を特定し、注意喚起を実施。

※利用者からの問合せ対応等を行うサポートセンターを設置

（イメージ図）



＜周知広報＞

①本事業の内容や注意喚起の対象となるIoT機器の設定方法を紹介するWEBサイトを開設。

②IoT機器のセキュリティ対策の必要性、本事業の内容の広報のため、公共機関等でのポスター掲示に加え、新聞広告（全国紙）、交通広告（全国主要駅でのサイネージ広告、JR山手線・東京メトロ中吊広告）等を２月中旬に実施予定。

お知らせ

総務省
MIC Ministry of Internal Affairs and Communications

平成31年1月21日

関東総合通信局

「平成30年度 第2回 関東テレコム講演会」のご案内

総務省関東総合通信局は、一般社団法人テレコムサービス協会関東支部との共催により「サイバーセキュリティ対策の最新動向」をテーマに関東テレコム講演会を次のとおり開催いたします。

サイバーセキュリティに対する脅威が一層深刻化する中、我が国におけるサイバーセキュリティの確保を促進する必要があります。また、2020年東京オリンピック・パラリンピック競技大会に向けて、本大会の開催に万全を期すため、産学官の多様な主体が相互に連携し、サイバーセキュリティに関する施策を推進することが重要となっています。

そこで、サイバーセキュリティに関する政府の動きや総務省の政策動向を踏まえて、サイバーセキュリティの脅威を正しく理解し、2020年に向けた企業経営のあり方や対策をどのように講じていくべきかを考えます。

1 日時

平成31年2月14日（木曜日）13時30分から17時00分まで（開場：13時）

2 場所

九段第3合同庁舎11階共用会議室1（東京都千代田区九段南1－2－1）
九段第3合同庁舎案内図

3 主催（共催）

総務省関東総合通信局
一般社団法人テレコムサービス協会関東支部

4 後援

関東情報通信協力会

5 講演内容（敬称略）

講演1「サイバーセキュリティ政策の動向」（仮題）
《2020年に向けたセキュリティ対策》
総務省　サイバーセキュリティ統括官室　参事官補佐　後藤 篤志

講演2「企業経営におけるサイバーセキュリティ」
独立行政法人情報処理推進機構　セキュリティセンター
研究員　木内　直人

講演3「DX時代の企業経営を支えるサイバーセキュリティ」
NECサイバーセキュリティ戦略本部　主席　田中　伸佳

6 参加費及び募集定員

(1) 参加費：無料
(2) 定員：120名

7 申込方法

「参加申込書」に必要事項（所属・氏名・連絡先等）をご記入の上、2月12日（火曜日）までに電子メールによりお申し込み下さい。（定員に達し次第締め切ります）

・「参加申込書」のダウンロード　｜PDF形式(174KB)｜・｜WORD形式(39KB)｜
・申込先　総務省　関東総合通信局　電気通信事業課
　メールアドレス：kanto-ji-seminar_atmark_soumu.go.jp
　※スパムメール対策のため、「@」を「_atmark_」と表示しております。送信の際には、「@」に変更してください。

【個人情報の取扱いについて】

お申し込み頂きました皆様の個人情報は、以下の目的のみ使用し、個人情報保護に関する法令に基づき適切・厳重に管理し、第三者に提供、開示することは一切ございません。

1. 利用目的
　(1)申込まれた方の人数把握及び会場受付での御本人様の確認のため
　(2)申込者多数の場合の先着に漏れた方への連絡のため
　(3)自然災害等により講演中止の連絡を申込まれた方へ行うため
　(4)今後、当局が主催するイベント・セミナーの情報を提供するため（希望者のみ）

2. 利用目的以外での個人情報の扱い
　利用目的の範囲を超えて個人情報を利用する必要が生じた場合は、予め申込まれた方へその理由を明示し、なおかつ同意が得られた場合のみ利用することとします。

連絡先
総務省関東総合通信局
情報通信部電気通信事業課
担当：島田
電話：03-6238-1671
Fax ：03-6238-1698