S9 エンジニアのための知っておくべき法制度と実務2018

電気通信事業法およびNICT法改正点の概説

（サイバー攻撃情報の共有関係、パスワード設定に不備のあるIoT機器調査関係）

2018年11月29日

一般社団法人日本インターネットプロバイダー協会
（JAIPA）
会長補佐、行政法律部会長 木村

総務省による説明会の開催

- 「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」についての説明会が今年6月～7月に、総務省地方総合通信局において開催されました。
- 本日はその資料の一部も用いて説明します。

法案国会提出時の概要（１）

電気通信事業法の一部改正案について

1

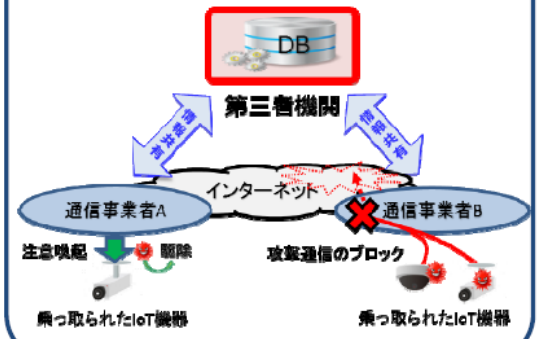
- IoT化に伴うサイバー攻撃の深刻化やネットワークのIP網への移行に対応するため、電気通信事業法の改正を行うもの。

①深刻化するサイバー攻撃への通信事業者の対処の促進

- IoT機器を悪用したサイバー攻撃によるインターネット障害の深刻化

- サイバー攻撃の送信元となるマルウェア感染機器などの情報を共有するための制度を整備し、通信事業者による利用者への注意喚起・攻撃通信のブロック等を促進

第三者機関を通じた情報共有による対処



②電気通信番号に関する制度整備

- モバイル化・IoT化に伴う番号ニーズの増大による番号の逼迫やIP網移行に対応した全ての事業者による番号管理の必要性

- 番号の公平・効率的な使用と電話サービスの円滑な提供のため、使用条件を付して事業者に番号を割り当てるための制度を整備

番号の逼迫状況や効率的な使用

■ 番号の逼迫状況

番号	用途	指定率（指定数/全番号）	使用率（使用数/指定数）
070/080/090	携帯電話・PHS	90.4%	70.3%
0120	着信課金	99.2%	55.3%

※ その他、固定電話（0AB-J番号）の市外局番は、全国（582地域）のうち138地域で指定率が80%以上（平均使用率が18.6%）

■ 番号ポータビリティ（電話番号の持ち運び）

固定電話は現在、NTT東西から他事業者への片方向のみ。今後、携帯電話と同様、双方向番号ポータビリティを実現

③電気通信業務等の休廃止に係る利用者保護

- IP網移行や通信設備の更改等を背景として利用者への影響が大きい業務等の終了が予定

- 事業者が業務の休廃止に伴い行う利用者周知について、行政が予め確認するための制度を整備

例：廃止予定のINSサービスの用途

法案国会提出時の概要（２）

国立研究開発法人情報通信研究機構法の一部改正案について

2

● IoT機器などを悪用した**サイバー攻撃の深刻化**を踏まえ、国立研究開発法人情報通信研究機構（NICT）の業務に、**パスワード設定に不備のあるIoT機器の調査**等を追加（**5年間の時限措置**）する等を内容とする**国立研究開発法人情報通信研究機構法の改正**を行うもの。

サイバー脅威の深刻化

・IoT機器の急激な増加に伴い、IoT機器を踏み台とするサイバー攻撃の脅威が顕在化。

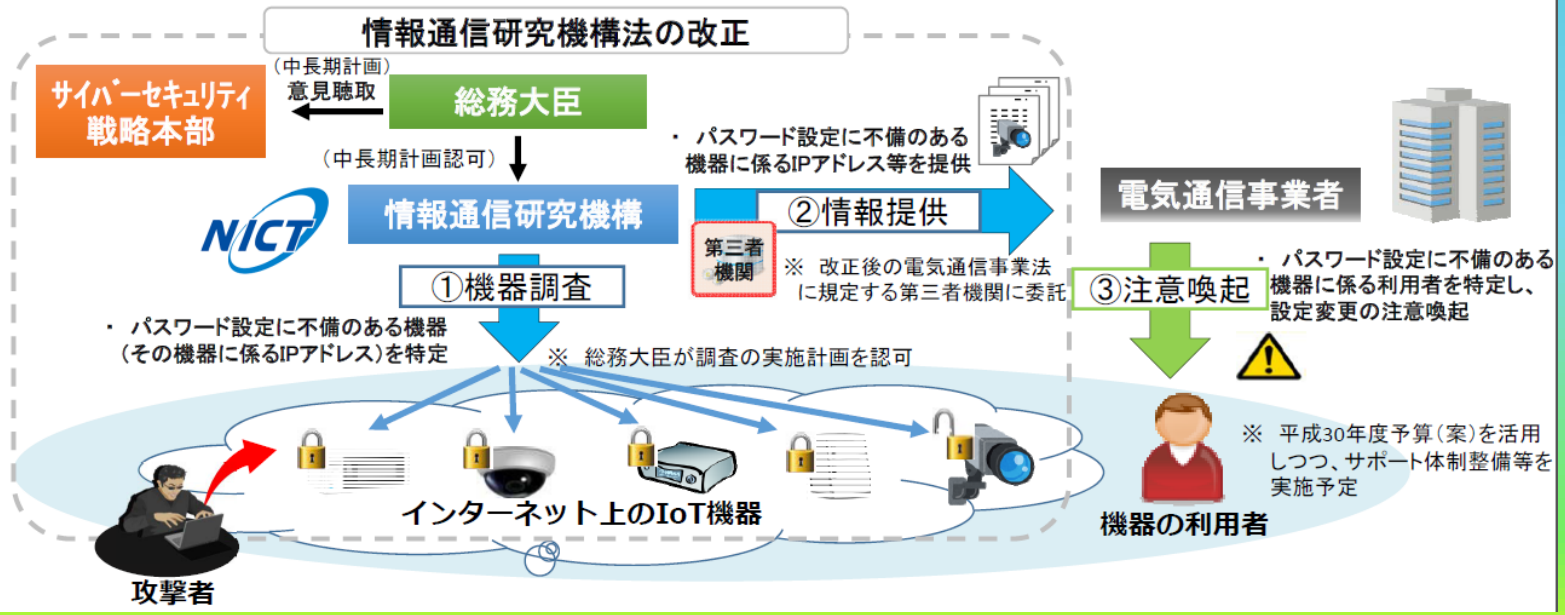
※IoT機器を狙った攻撃は全体の3分の2（2016年）

対策の必要性

・パスワード設定に不備のあるIoT機器の実態を把握するため、調査機能の強化が急務。

体制の整備

・NICTに機器調査に係る業務を追加し、電気通信事業者と連携しつつ対策を推進（下図）。



サイバー攻撃によるインターネットの障害に関する近年の事例

➢ 近年、国内外において、大規模なサイバー攻撃によりインターネットに障害が生ずる事例が複数発生

国内

2015年12月14日	・一部の電気通信事業者において、DNS サーバがDDoS 攻撃を受け、数時間にわたりDNS サーバへの接続障害が発生
2016年8月29日～9月2日	・一部の電気通信事業者において、権威サーバ（あるドメイン名に対するIPアドレス等の情報を管理しているDNSサーバ）が外部からのDoS攻撃を受け、ホスティングサービスを中心に大きな障害が断続的に発生
2017年9月25日～26日	・一部の電気通信事業者において、レンタルサーバがDoS攻撃を受け、２日間にわたり断続的にサーバに接続できなくなる障害が発生

海外

2016年9月22日	【OVH（フランス）】 ・自社保有サーバに対し、Mirai※に感染したとされる約14万台以上のIoT機器から、最大1.5Tbpsとなる世界最大規模のDDoS攻撃が発生 ・南欧諸国からOVHのサーバを利用するサービスへのアクセスの遅延が発生
2016年10月21日	【Dyn（米国）】 ・Dyn社のDNSサーバに対し、Mirai ※に感染し攻撃に関与した約10万台のIoT機器から1.2Tbpsに及ぶとされるDDoS攻撃が発生 ・世界各国の様々な大手顧客サイト（Twitter、Netflix、Spotify等）に数時間にわたりアクセス障害が断続的に発生
2018年２月28日	【GitHub（米国）】 ・GitHub社のサーバに対し、脆弱なmemcachedサーバを利用して、最大1.35TbpsとされるDDoS攻撃が発生 ・GitHubのウェブサイトへ10分程度にわたりアクセス障害が断続的に発生

※ IoT機器に自動的に感染し、攻撃者からの指示に応じて感染した機器を踏み台としたDDoS攻撃を実施する等の機能を有するマルウェア

過去のオリンピック・パラリンピック時のサイバー攻撃

○　2012年　ロンドン大会

- 大会Webサイト、政府系サイト、その他のサイトに対して、DoS及びDDoS攻撃を確認
- 2億件の悪意のある接続要求をブロック
- 1つのDDoS攻撃につき、1秒あたり11,000件の接続要求を確認

（出典）IPAサイバーセキュリティシンポジウム2014
オリバー・ホーア氏（2012年当時、英国内閣府 上級政策顧問）の講演資料
https://www.ipa.go.jp/about/news/event/securitysympo2014/lecture.html
https://www.ipa.go.jp/files/000039004.pdf

○　2016年　リオデジャネイロ大会

- 開会式の開始前に、オリンピックの公式Webサイトや関連組織に対して540Gbpsに達する大規模なDDoS攻撃が継続的に発生
- IoT機器を踏み台にしたDDoS攻撃を確認

（出典）アーバーネットワークス” DDoS Attacks From IoT Botnets Don’t Have to Mean Game Over”
https://www.arbornetworks.com/blog/asert/ddos-attacks-iot-botnets-dont-mean-game/

IoT機器のセキュリティ上の課題

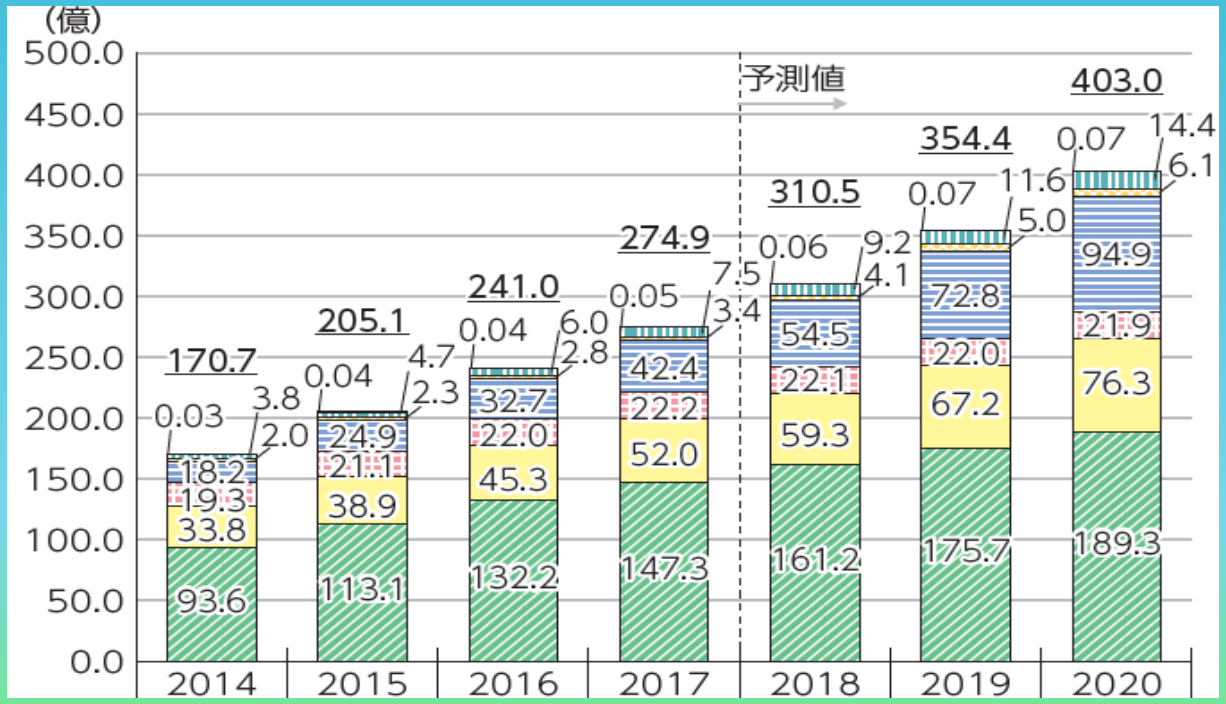
- IoT機器は、製造業者や利用者が機器のセキュリティ対策を講じる上で制約があり、長期間インターネットに接続されることから、乗っ取られやすく、サイバー攻撃に用いられやすい
- また、IoT機器は数が多く、今後も急増する見込みであるため、乗っ取られる機器数も多くなり、攻撃に用いられるとインターネットの通信に著しい支障が生じるおそれがある

従来のインターネットに接続される機器とIoT機器の特徴の比較

PC等の従来機器	センサーや家電等のIoT機器
● 機器の演算処理能力が比較的高く、アンチウィルスソフトやファイアウォール等のセキュリティソフトの導入による高度な対策が可能	● 機器の演算処理能力が比較的低く、アンチウィルスソフトやファイアウォール等のセキュリティソフトの導入による高度な対策は困難
● 機器のライフサイクルが短く、脆弱性を有する機器も一定期間後にセキュリティ強度の高い新たな機器に置き換わる見込み	● 機器のライフサイクルが長く、10年以上の長期にわたって利用されるものも多いため、脆弱性を有したままネットワークに接続され続けるおそれ
● 画面等を通じた、人的管理が容易	● 画面等がないものが多く、人的管理が困難
● ネットワークに接続される機器数は多いが、IoT機器と比べ今後の増加数は少ない見込み※ ※ PCは、2015年の約20億個をピークに微減傾向となる見込み。（IHS Technology調べ）	● ネットワークに接続される機器数が膨大であり、今後も急増する見込み※ ※ 家庭、医療、産業用等で用いられるIoT機器は2020年に約200億個となる見込み。（IHS Technology調べ）

IoT機器の推移と普及分野

- IHS Technology の推定によれば、インターネットにつながるモノ（IoTデバイス）は、2017年時点で275億個であるのが、2020年には400億個まで増加し、「コンピュータ」は微減となる一方、「産業用途」「コンシューマー」は大幅な増加が見込まれている。

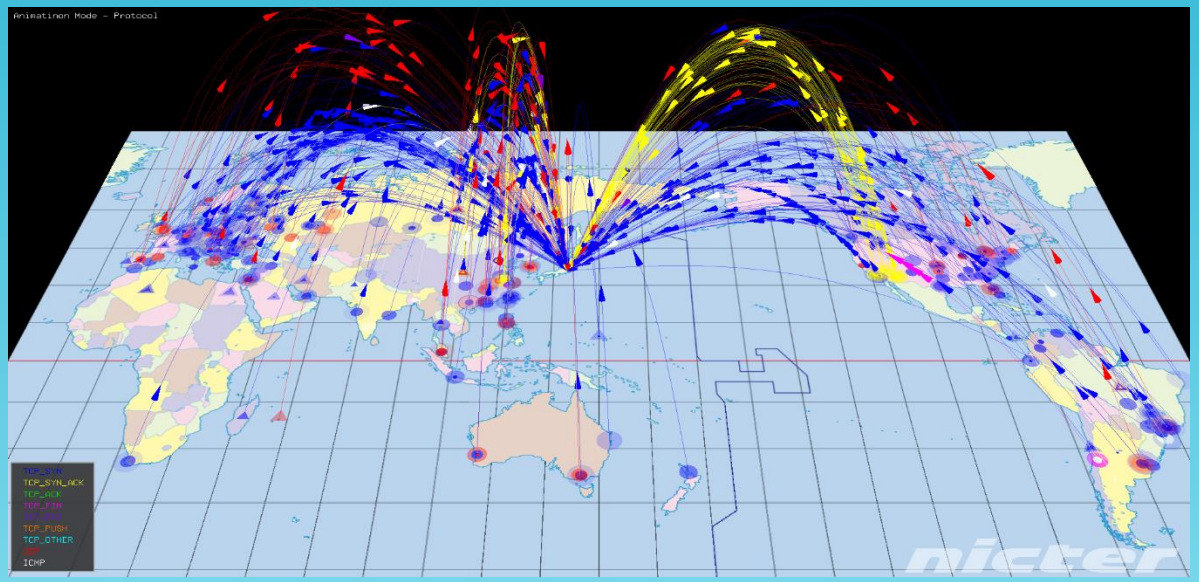


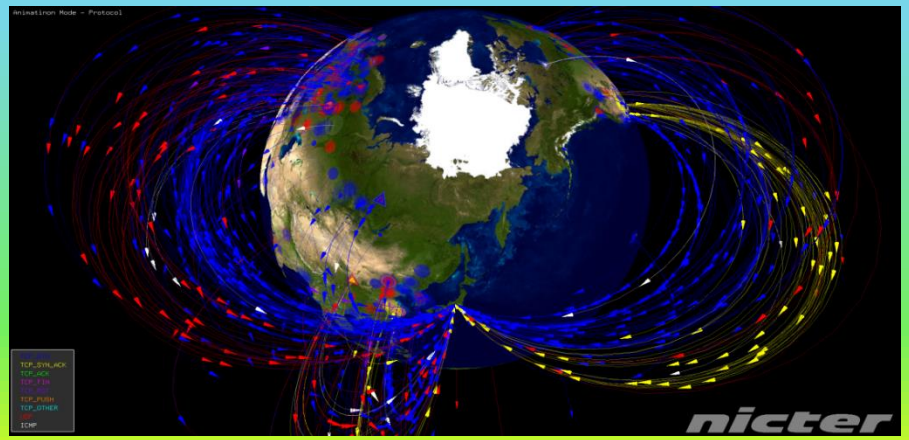
※ 各カテゴリの範囲は以下のとおり。
「通信」：固定通信インフラ・ネットワーク機器、2G、3G、4G各種バンドのセルラー通信及びWifi・WIMAX などの無線通信インフラ及び端末。
「コンシューマー」：家電（白物・デジタル）、プリンターなどのPC 周辺機器、ポータブルオーディオ、スマートトイ、スポーツ・フィットネス、その他。
「コンピューター」：ノートパソコン、デスクトップパソコン、サーバー、ワークステーション、メインフレーム・スパコンなどコンピューティング機器。
「産業用途」：オートメーション（IA/BA）、照明、エネルギー関連、セキュリティ、検査・計測機器などオートメーション以外の工業・産業用途の機器。
「医療」：画像診断装置ほか医療向け機器、コンシューマーヘルスケア機器。
「自動車・輸送機器」：自動車（乗用車、商用車）の制御系及び情報系において、インターネットと接続が可能な機器。
「軍事・宇宙・航空」：軍事・宇宙・航空向け機器（例：航空機コックピット向け電装・計装機器、旅客システム用機器、軍用監視システムなど）。
なお、2018 年から集計対象について、「通信」にLPWA 接続機器など、「自動車・輸送機器」に商用車向け機器などを追加しており、それらの台数も遡って集計している。

（出典）IHS Technology

IoT機器を狙った攻撃が急増（NICTERによる観測）

- 国立研究開発法人 情報通信研究機構（NICT）では、未使用のIPアドレスブロック30万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測





- TCP SYN
- TCP SYN/ACK
- TCP ACK
- TCP FIN
- TCP RESET
- TCP PUSH
- TCP Other
- UDP
- ICMP

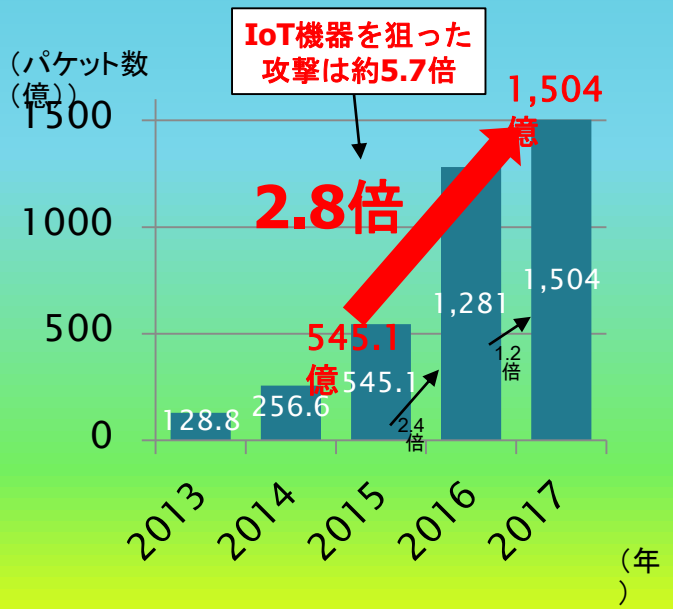
・ダークネットに飛来するパケットの送信元アドレスから緯度・経度を推定し、世界地図上で可視化

・色：パケットごとにプロトコル等を表現

NICTERで１年間に観測されたサイバー攻撃回数

・2年間で2．8倍

（2015年→2016年：2．4倍、2016年→2017年：1．2倍）



円滑なインターネット利用環境の確保に関する検討会について

1. 趣旨

近年、増加するIoT機器を悪用したサイバー攻撃等によるインターネット障害が発生している。更に2020年の東京オリンピック・パラリンピック競技大会に際して日本に対する大規模なサイバー攻撃の発生が懸念される。このため、電気通信事業においてインターネットの障害を防ぐための方策について検討を行う。

2. 検討事項

（１）電気通信事業者によるサイバー攻撃等によるインターネットの障害の防止措置
（２）電気通信事業者等によるインターネットの障害に関する情報共有の在り方
（３）IoT機器を含む脆弱な端末設備への対策　　等

3. 構成員

（敬称略、五十音順）

	遠藤　信博	日本電気株式会社　代表取締役会長
（座長代理）	佐伯　仁志	東京大学大学院法学政治学研究科　教授
（座長）	佐々木良一	東京電機大学未来科学部　教授
	宍戸　常寿	東京大学大学院法学政治学研究科　教授
	長田　三紀	全国地域婦人団体連絡協議会　事務局長
	藤本　正代	富士ゼロックス（株）パートナー、情報セキュリティ大学院大学　客員教授
	森　　亮二	英知法律事務所　弁護士
	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

⇩

「対応の方向性」を公表（平成30年2月20日）

「対応の方向性」の概要等

1. 電気通信事業者による攻撃通信の発生の防止

・マルウェア感染の疑われる利用者に対する注意喚起、指令サーバとの通信遮断、未知のマルウェア感染端末等を検知。

※事業者が、利用者の同意なく、注意喚起、検知等のために利用者の通信に係るIPアドレスやタイムスタンプ等を利用することは、通信の秘密の窃用に該当し得る。

→ 通信の秘密に配慮した実施方法等を整理し、民間のガイドラインに反映。

2. 情報共有、分析基盤の構築

・1. の対策の実効性を高めるため、第三者機関が指令サーバ等に関する情報を集約し、分析・検証した上で電気通信事業者との間で情報共有。

※本取組においては、第三者機関が、通信の秘密を集約、分析・検証、共有することとなる。

→ 第三者機関が通信の秘密に該当する情報を扱うことから、裏付けとなる法制度を整備。

3. IoT機器を含む脆弱な端末設備への対策の検討

・DDoS攻撃等の発生源となりうる脆弱なIoT機器について、基本的なセキュリティ対策を実施。

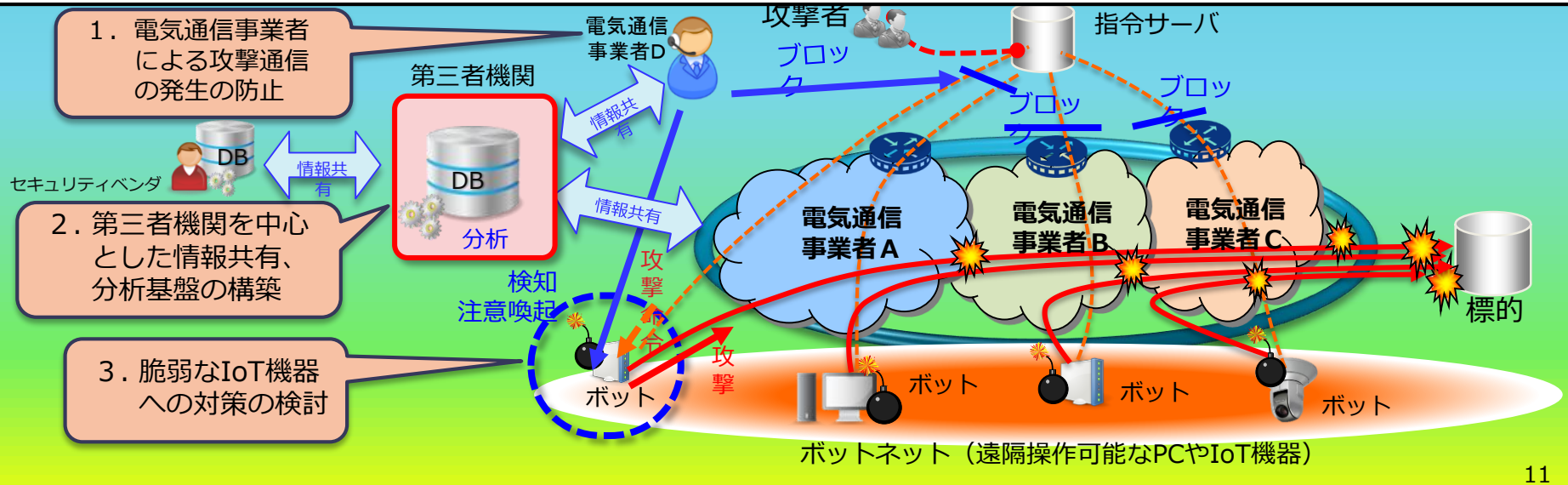
※事業者のネットワークに接続される端末設備の技術基準には、現時点ではサイバー攻撃等によるインターネットの障害に関する規定はない。

→ ネットワークの安全・信頼性を確保するための端末のセキュリティ対策について、国際動向等を踏まえ、情報通信審議会で検討。

4. 昨年8月に発生した大規模なインターネット障害の検証を踏まえた対策の検討

・事業者においてインターネットの経路情報を適切に制御する技術的対策を実施するともに、事業者間でインターネット障害に関する情報を共有。

→ 情報通信ネットワーク安全・信頼性基準（ガイドライン）の改訂や、事業者から総務省へのインターネット障害の報告の在り方について検討。



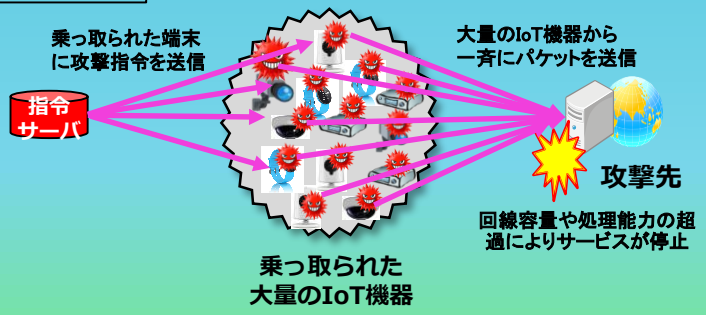
送信型対電気通信設備サイバー攻撃の範囲

送信型対電気通信設備サイバー攻撃

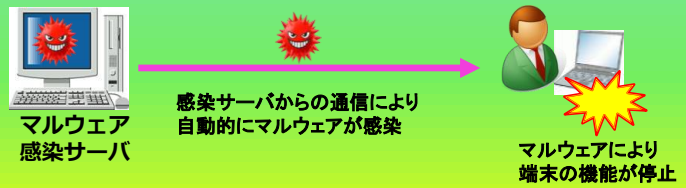
- 「送信型対電気通信設備サイバー攻撃」とは、以下を満たすものをいう。
  - ① **サイバー攻撃**（通常の通信によるトラフィック集中等は含まない。）**のうち、**
  - ② **電気通信設備**（電気通信事業者の電気通信設備及び利用者の端末）**を攻撃の対象とし、**
  - ③ **その機能に障害を与える通信の送信により行われるもの**（受信者の行為が介在することにより障害が発生する場合は該当しない）
- また、上記の通信の送信を行う指令を与える通信の送信（C&Cサーバからの攻撃指令等）も含まれる。

該当する例

例①：DDoS攻撃



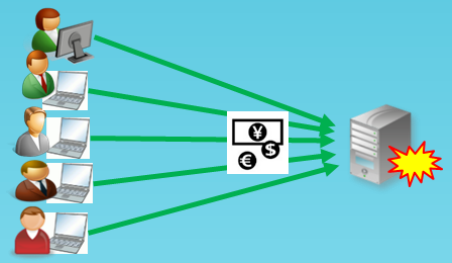
例②：マルウェア感染による機能障害



該当しない例

例①：販売サイトへのアクセス等
によるトラフィック集中

サイバー攻撃には該当しないため、該当しない

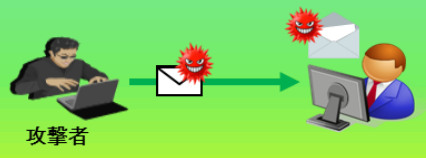


例②：不正アクセス

電気通信設備の機能に障害を与えないため、該当しない

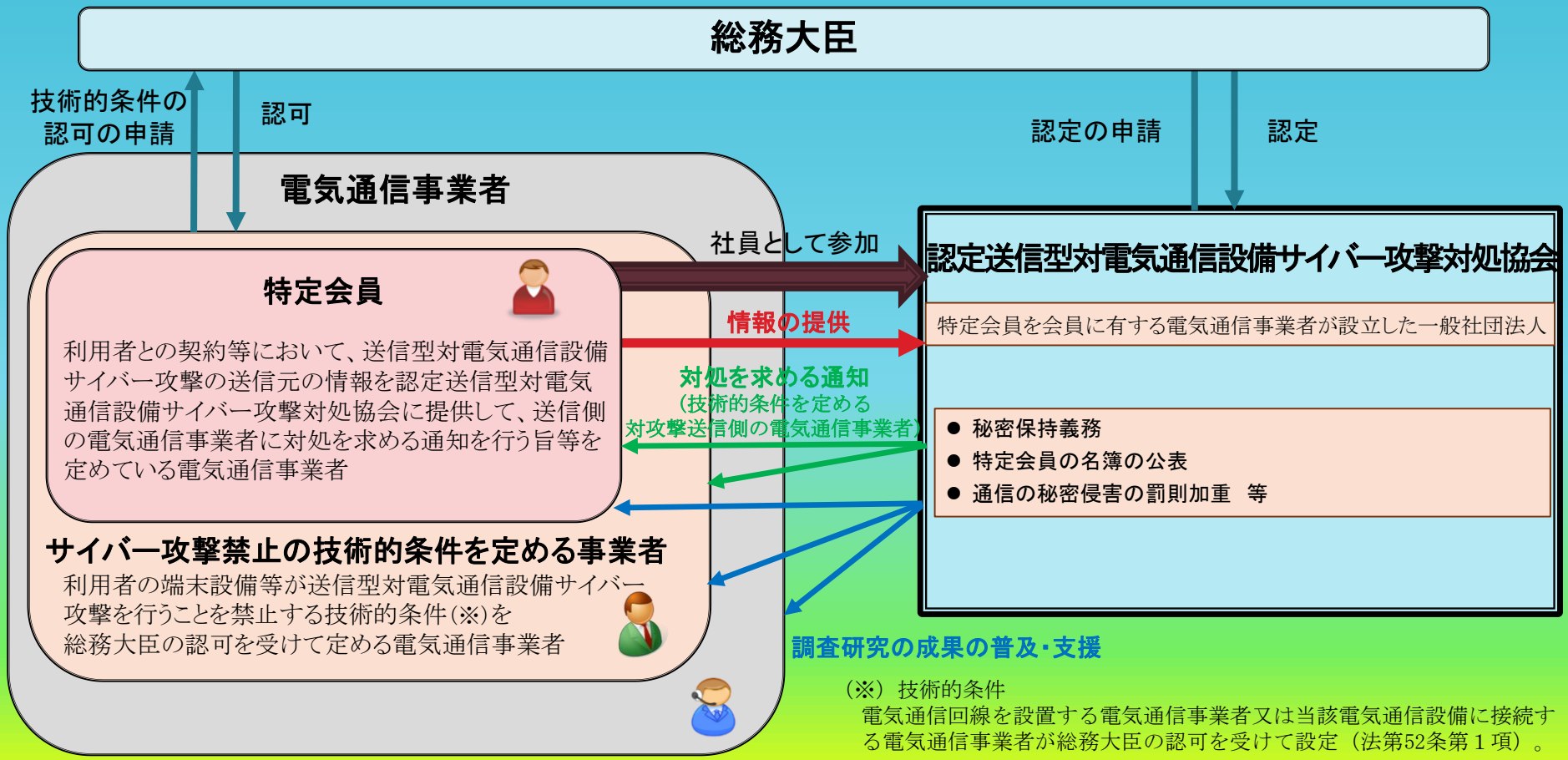
例③：標的型メール

受信者の行為が介在することにより障害が発生するため、該当しない



認定送信型対電気通信設備サイバー攻撃対処協会制度の概要

- 本年５月23日に公布された改正電気通信事業法において、電気通信事業者がDDoS攻撃等のサイバー攻撃への対応を共同して行うため、サイバー攻撃の送信元情報の共有やC&Cサーバの調査研究等の業務を行う第三者機関を総務大臣が認定する制度を創設。
- 改正電気通信事業法は本年11月頃に施行予定（技術的条件の認可は本年７月中旬以降から順次行う予定）。



（※）技術的条件
電気通信回線を設置する電気通信事業者又は当該電気通信設備に接続する電気通信事業者が総務大臣の認可を受けて設定（法第52条第１項）。

端末設備等の接続の技術的条件と接続の検査の請求

端末設備等の接続の技術基準及び技術的条件

- 電気通信回線設備を設置する電気通信事業者は、

  ①総務省令で定める技術基準　　又は
  ②当該電気通信事業者又は当該電気通信事業者と電気通信設備を接続する他の電気通信事業者であって総務省令で定める者が総務大臣の認可を受けて定める技術的条件
  に適合しない場合等を除き、端末設備等の接続要求を拒むことができない。

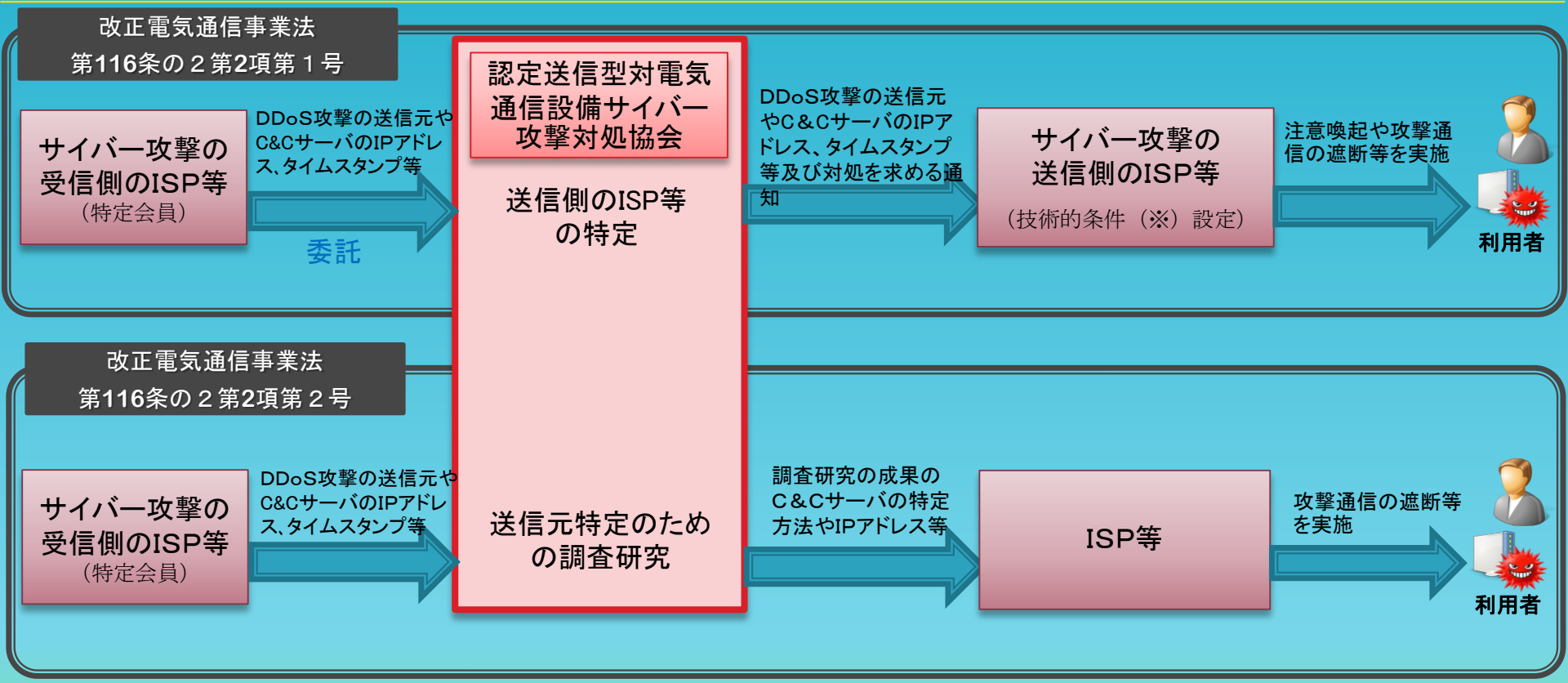
  （電気通信事業法第52条第１項及び第70条第１項）

接続の検査の請求

- 電気通信回線設備を設置する電気通信事業者は、端末設備等に異常がある場合等において、必要と認めるときは、利用者に対し技術基準又は技術的条件への適合性に係る検査を受けることを求めることができる。（電気通信事業法第69条第２項及び第70条第２項）

- 改正電気通信事業法においては、技術的条件を設定した電気通信回線設備を設置しない電気通信事業者においても、利用者に対し技術的条件への適合性に係る検査を求めることができることとなる。（改正電気通信事業法第69条第３項）

認定送信型対電気通信設備サイバー攻撃対処協会の業務



（※）利用者の端末設備等が送信型対電気通信設備サイバー攻撃を行うことを禁止する技術的条件。

- 送信型対電気通信設備サイバー攻撃に対処する電気通信事業者を支援。

その他の業務

- NICTから委託を受けて、パスワード設定に不備のある機器に係るIPアドレス、タイムスタンプ等を当該機器利用者のISPに通知（改正NICT法附則第8条第2項のNICTの業務の受託）。

（参考）認定送信型対電気通信設備サイバー攻撃対処協会の業務

（認定送信型対電気通信設備サイバー攻撃対処協会の認定）

第百十六条の二　（略）

２　前項の規定による認定を受けた一般社団法人（以下「認定送信型対電気通信設備サイバー攻撃対処協会」という。）は、次に掲げる業務を行うものとする。

一　会員である電気通信事業者であつて次のいずれにも該当するものの委託を受けて、ロ⑴又は⑵に定める者に対し、ロの通知を行うこと。

イ　第五十二条第一項又は第七十条第一項第一号の規定により認可を受けた技術的条件において、その利用者の電気通信設備が送信型対電気通信設備サイバー攻撃（電気通信事業者がその業務上記録している電気通信の送信元、送信先、通信日時その他の通信履歴（以下単に「通信履歴」という。）の電磁的記録により送信元の電気通信設備が送信先の電気通信設備の機能に障害を与える電気通信の送信の送信元であることを合理的に特定できるものに限る。ロにおいて同じ。）を行うことを禁止する旨を定めていること。

ロ　電気通信役務の提供条件において、その電気通信設備又はその利用者の電気通信設備が送信型対電気通信設備サイバー攻撃の送信先であることが特定された場合において、その業務上記録している通信履歴の電磁的記録により当該送信型対電気通信設備サイバー攻撃の送信元の電気通信設備が次の⑴又は⑵に掲げる者の電気通信設備であることが特定されたときは、当該⑴又は⑵に定める者に対し、当該通信履歴の電磁的記録を証拠として当該電気通信設備を送信元とする送信型対電気通信設備サイバー攻撃又はそのおそれへの対処を求める通知を行う旨を定めていること。

⑴　他の電気通信事業者　当該他の電気通信事業者

⑵　他の電気通信事業者（イに該当するものに限る。）の利用者　当該他の電気通信事業者

二　会員である電気通信事業者であつて次のいずれにも該当するものからロの通信履歴の電磁的記録の提供を受け、ロの調査及び研究を行うこと並びにその成果の普及を行うこと。

イ　前号イに該当すること。

ロ　電気通信役務の提供条件において、その電気通信設備又はその利用者の電気通信設備が送信型対電気通信設備サイバー攻撃の送信先であることが特定された場合において、その業務上記録している通信履歴の電磁的記録により当該送信型対電気通信設備サイバー攻撃の送信元の電気通信設備が合理的に特定できないときは、認定送信型対電気通信設備サイバー攻撃対処協会に対し、送信型対電気通信設備サイバー攻撃の送信元の電気通信設備を合理的に特定するための調査及び研究の用に供するため、当該通信履歴の電磁的記録の提供を行う旨を定めていること。

三　（略）

３～７　（略）

IoT機器の調査に係る政府決定

○ 2020年及びその後を見据えたサイバーセキュリティの在り方について－サイバーセキュリティ戦略中間レビュー
（平成29年7月13日サイバーセキュリティ戦略本部決定）（抜粋）
３ 各論
（１）経済社会の活力の向上及び持続的発展
① ボット撲滅の推進 ア 実態の把握

- ✓ NISC、警察庁、総務省、経済産業省、民間企業等が協調・連携し、官民連携による「ボット撲滅」に向けた体制を構築し、対策を推進すること。その際、各関係主体の役割分担を明確化し、実態の把握、対策の実施・周知、再発防止・環境改善を一体的に実施することで、効率的かつ効果的な対策につなげること。
- ✓ 政府内に体制を構築して継続的かつ広範な実態調査ができるよう、**必要となる法的整理をおこなうこと。**その際、当該調査によるインターネット上のサービスへの影響等を考慮すること

○ IoTセキュリティ総合対策（平成29年10月総務省サイバーセキュリティタスクフォース）（抜粋）
Ⅱ 具体的施策
（１）脆弱性対策に係る体制の整備
（脆弱性調査の実施）

- ✓ 既に設置されているIoT機器はもとより、製造・販売された新規のIoT機器についても新たな脆弱性が発見され、こうした脆弱性を突いたサイバー攻撃が行われる可能性がある。このため、関係者の連携による体制を整備し、計画的かつ包括的な脆弱性調査を継続的に実施する必要がある。その際、重要インフラで利用されるIoT機器のように、国民生活や社会経済活動に直接影響を与える可能性がある重要IoT機器と、家電製品などのIoT機器を含むサイバー攻撃の踏み台となってネットワークに悪影響を及ぼすおそれのある機器の双方について、所要の脆弱性調査と当該調査結果に基づく対策を講じる必要がある。併せて、**脆弱性調査の効果を高める観点から所要の法制度の整備についても併せて検討する必要がある。**

○ サイバーセキュリティ戦略（平成30年７月27日閣議決定）（抜粋）
４．目的達成のための施策
4.1.3 安全なIoTシステムの構築
(2) 脆弱性対策に係る体制の整備

- ✓ ネットワーク上の脆弱なIoT機器の対策については、**パスワード設定に不備のある機器の調査・特定を行い、電気通信事業者において当該機器の利用者への注意喚起を円滑に行えるよう、所要の制度整備を着実に進める。**また、対策の実施に当たっては、関係省庁等が一体となって、電気通信事業者、機器製造事業者等と連携して取り組む。
- ✓ 将来的には、これらの我が国の対策をモデルとして、国際的な連携や標準化等を通じて海外に展開し、安全なネットワークの環境整備に貢献をしていく。

国立研究開発法人情報通信研究機構によるIoT機器調査に係る制度の概要

- 本年５月23日に公布された改正国立研究開発法人情報通信研究機構法において、国立研究開発法人情報通信研究機構（NICT）に、平成35年度までの時限措置として以下の業務を追加（改正国立研究開発法人情報通信研究機構法は本年11月頃に施行を予定）。

（ア）インターネット上で外部からアクセス可能であり、かつパスワード設定等に不備のある電気通信設備を特定するための調査を行うこと

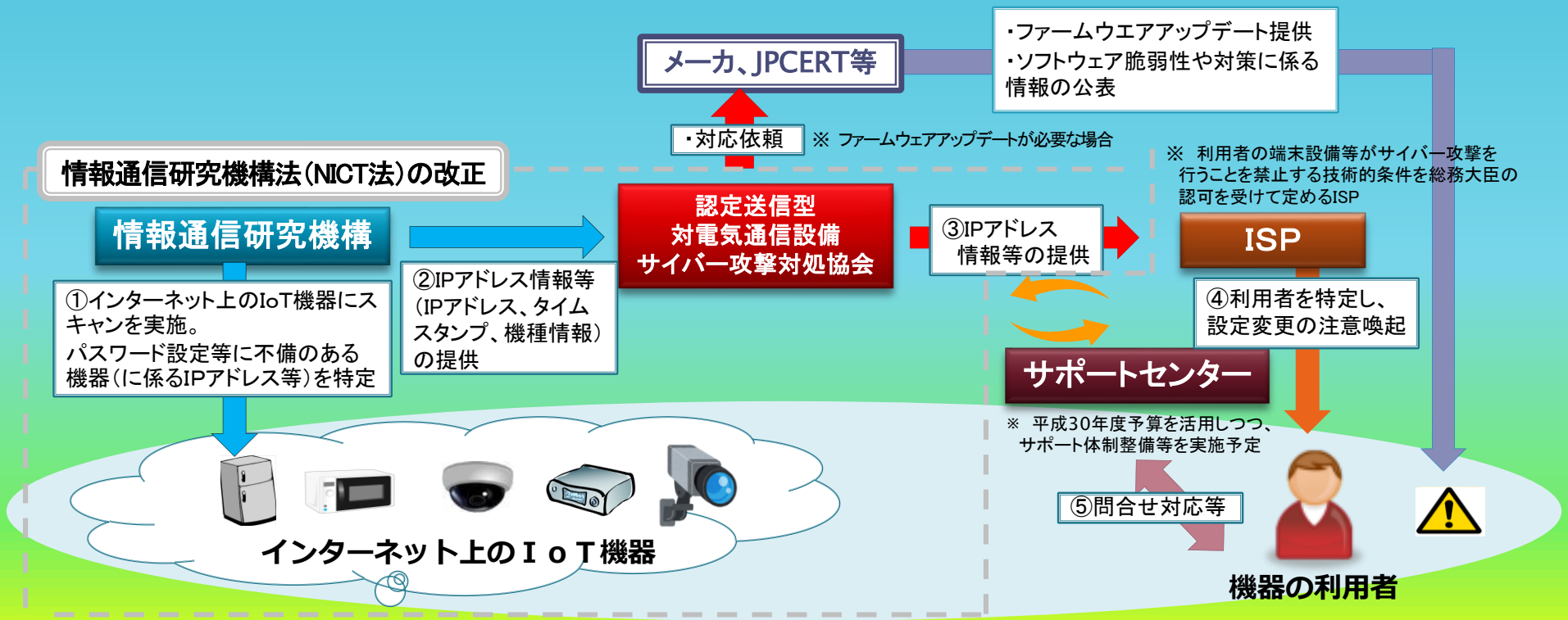
※　NICTは、総務省令で定める基準（電気通信事業者が技術的条件で定める基準を勘案し、不正アクセス行為から防御するため必要な基準）を満たさないID・パスワードを機器に入力。

（イ）パスワード設定等に不備のある電気通信設備のIPアドレス・タイムスタンプ等の情報を、該当する電気通信事業者に対して提供し、対処（注意喚起等）を求める通知を行うこと

※　認定送信型対電気通信設備サイバー攻撃対処協会に委託することができる。

- （上記（イ）の通知を受けた電気通信事業者は、IPアドレス情報等をもとに利用者を特定し、当該利用者に対して注意喚起を行う。）

※　総務省予算を活用して利用者からの個別の問合せ対応を行うなど、電気通信事業者における注意喚起のサポート体制を整備予定。



ユーザへの注意喚起イメージ

注意喚起

機器の利用者

問合せ対応

ISP

（1）NICTから提供されたIPアドレス、タイムスタンプと通信履歴を照合し、**利用者を特定**

（2）特定した利用者にメールにて**注意喚起**

【注意喚起のメール案】

…

このたび、お客様がご利用の〇〇サービスに接続されたIoT機器について、脆弱と思われるID・パスワードが設定された状態で運用されていることを確認しました。つきましては、ID・パスワード変更を実施して頂きますようお願いいたします。

確認日：※年※月※日
IoT機器：△△

◆ IoTセキュリティ対策サイト
http://www.〇〇〇.co.jp

◆ IoT機器△△の設定変更方法
http://www.×××.co.jp

■お問い合わせ■
※※※※
電話番号：※※
メールアドレス：※※
受付時間：※※～※※

サポートセンター

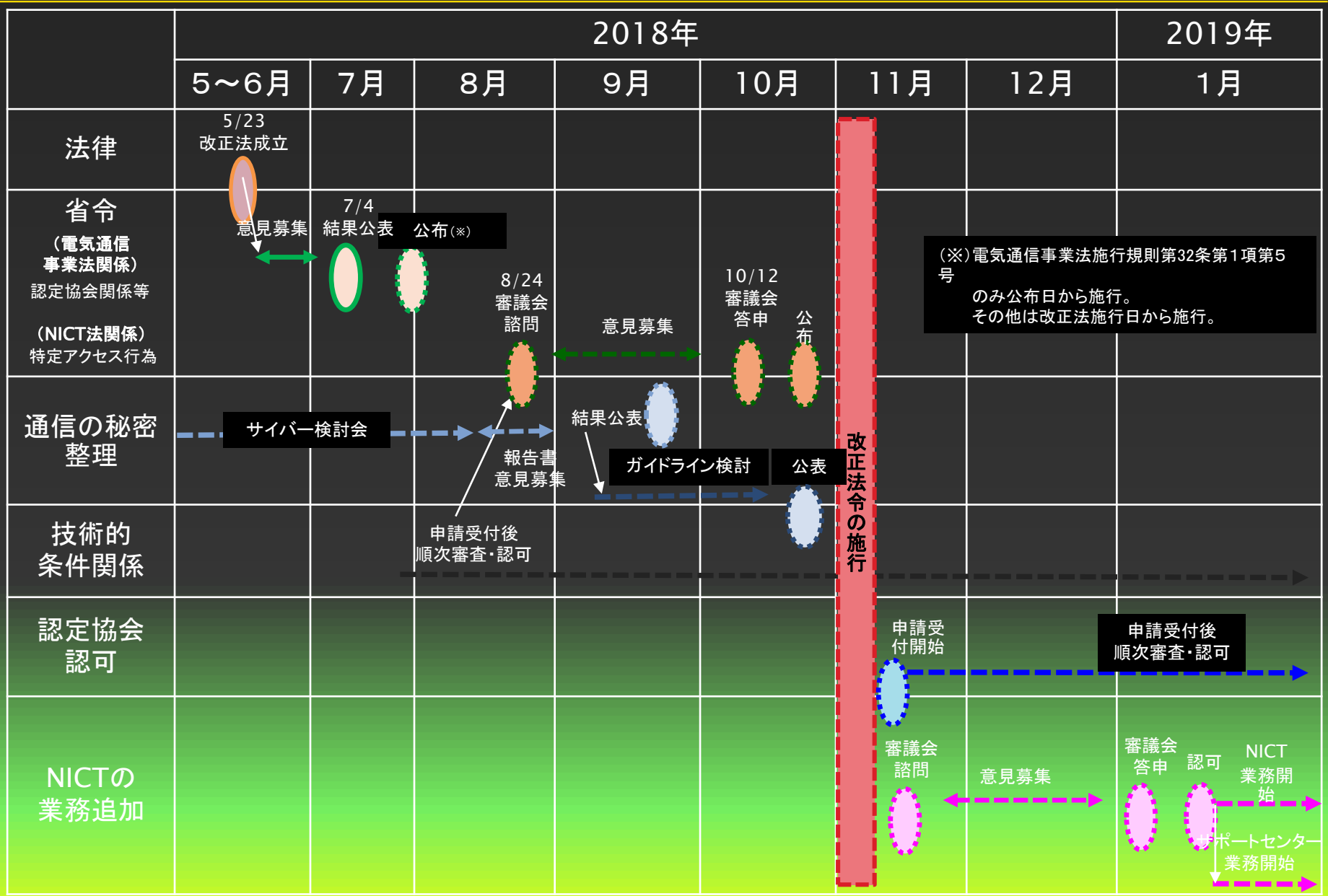
※　平成30年度予算を活用しつつ、サポート体制を整備予定

（1）設定変更案内の作成

（2）問合せ対応

※ NICTの調査を受けた注意喚起は、平成35年度までを想定

今後のスケジュール


2018年
2019年
5～6月
7月
8月
9月
10月
11月
12月
1月
法律
5/23
改正法成立
省令
（電気通信事業法関係）
認定協会関係等
（NICT法関係）
特定アクセス行為
意見募集
7/4
結果公表
公布（※）
8/24
審議会
諮問
意見募集
10/12
審議会
答申
公布
（※）電気通信事業法施行規則第32条第1項第5号
のみ公布日から施行。
その他は改正法施行日から施行。
通信の秘密
整理
サイバー検討会
報告書
意見募集
結果公表
ガイドライン検討
公表
改正法令の施行
技術的
条件関係
申請受付後
順次審査・認可
認定協会
認可
申請受付
開始
申請受付後
順次審査・認可
NICTの
業務追加
審議会
諮問
意見募集
審議会
答申
認可
NICT
業務開始
サポートセンター
業務開始

NICTから事前調査の発表　11月7日

ENGLISH TOP　アクセス　お問い合わせ　Google カスタム検索

NICT 国立研究開発法人 情報通信研究機構

NICTについて　研究紹介　研究成果　オープン イノベーション　公募・調達　広報・出版　採用情報

Home 〉 お知らせ&イベント 〉 お知らせ 〉 日本国内でインターネットに接続されたIoT機器等に関する事前調査の実施について

印刷

日本国内でインターネットに接続されたIoT機器等に関する事前調査の実施について

2018年11月7日

国立研究開発法人情報通信研究機構

ツイート　いいね！ 183

国立研究開発法人情報通信研究機構（NICT）は、パスワード設定等に不備のあるIoT機器の調査等をNICTの業務に追加（５年間の時限措置）する「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」が今月1日に施行されたことを受け、同調査等の業務の実施（今年度内に開始予定）に向けた検討、準備を進めてまいります。

今後の具体的な検討にあたっては、日本国内でインターネットに接続されたIoT機器等につき、当該接続状況などの全体的な傾向、概数等を把握する必要があることから、ポート開放状況の把握など、現状に関して、事前の準備のための調査を実施することといたします。

○事前調査の概要

・日本国内のIPv4アドレスを対象に、22/TCP(SSH)、23/TCP(Telnet)、80/TCP(HTTP)などの

https://www.nict.go.jp/about/location.html

お知らせ

2018年
2017年
2016年
2015年
2014年
2013年
2012年
2011年
2009年

通信の秘密の整理

- インターネットの安定的な運用に関する協議会
- 電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドラインを策定
- 2006年から活動
- 構成団体は
  - 一般社団法人日本インターネットプロバイダー協会（JAIPA)
  - 一般社団法人電気通信事業者協会（TCA)
  - 一般社団法人テレコムサービス協会
  - 一般社団法人日本ケーブルテレビ連盟
  - 一般社団法人ICT-ISAC

ガイドラインの変遷

- ２００７　初版
  「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン 」として作成。関係者限りで限定公開
- ２０１１　第２版
  一般にも公開
- ２０１４　第３版
  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の第一次とりまとめ（2014年4月4日）を受けて改正
- ２０１５　第４版
  同研究会の第二次とりまとめ（2015年9月9日公表）を受けて改正

第4版において、ガイドラインの名称が「大量通信等への対処」から「サイバー攻撃等への対処」に変更。

ガイドラインの位置付け

- 業界の自主基準としての位置づけ
  - 法令上の位置づけがあるガイドラインではなく民間における法令の解釈指針
  - 事業者に対処を強制したり、活動を規制するものではない
  - 総務省はオブザーバとして協議会に参加

- 同様な事例が生じた際に、ISPがその都度解釈に関して総務省に問合せる手間を省略するためのもの
  - ガイドラインに沿って対応すれば免責されるなどの効果はないが、裁判所が法的判断の参考として参照することを期待
- インターネット上で新たに発生する問題に対応するため、定期的な見直しを実施

ガイドラインの構成

第1章　総則
- 第1条　目的
- 第2条　総論
  1. 通信の秘密
  2. 留意事項
- 第3条 定義
  1. サイバー攻撃等
  2. 電気通信役務の不正享受
  3. 攻撃通信
  4. 通信
- 第4条　見直し

第2章　各論
- 第5条　サイバー攻撃等について
  1. 攻撃通信への対処
  2. 迷惑メール等
  3. その他の情報共有・情報把握について
- 第6条　電気通信役務の不正享受について

①攻撃や障害が発生している際の対処法
②攻撃や障害を予防する為の措置
③必要な情報の共有

等につき、具体的な事例とともに
指針となる考え方を整理

ガイドラインの構成（第5条の詳細）

第5条　サイバー攻撃等について
- (1)　サイバー攻撃等に係る通信の遮断
  - ア　被害者から申告があった場合
  - イ　事業者設備に支障が生じる場合
  - ウ　**送信元設備の所有者の意思と関係なく送信される大量通信等の場合**
- (2)　**送信元詐称通信の遮断**
- (3)　壊れたパケット等の破棄
- (4)　マルウェア等トラヒックの増大の原因となる通信の遮断
- (5)　受信側の設備等に意図しない影響を及ぼす通信等への対処
- (6)　**網内トラヒックの現状把握**
- (7)　サイバー攻撃等への共同対処

2　迷惑メール等
- (1)　送信元詐称メールの受信拒否
- (2)　**Black Listとの突合に基づくユーザへの注意喚起**
- (3)　**迷惑メールフィルタリングサービスにおけるフィルタ定義の共有**
- (4)　SMTP認証の情報を悪用した迷惑メールへの対処

3　その他の情報共有・情報把握について
- (1)　踏み台端末や攻撃中継機器への対処
- (2)　**レピュテーションDBの活用**

事例①
【事業者設備等へのサイバー攻撃に対する実施可能な措置】

事例②
【マルウェア感染端末とC&Cサーバとの通信の遮断】

事例③
【サイバー攻撃に対する事業者間の情報共有】

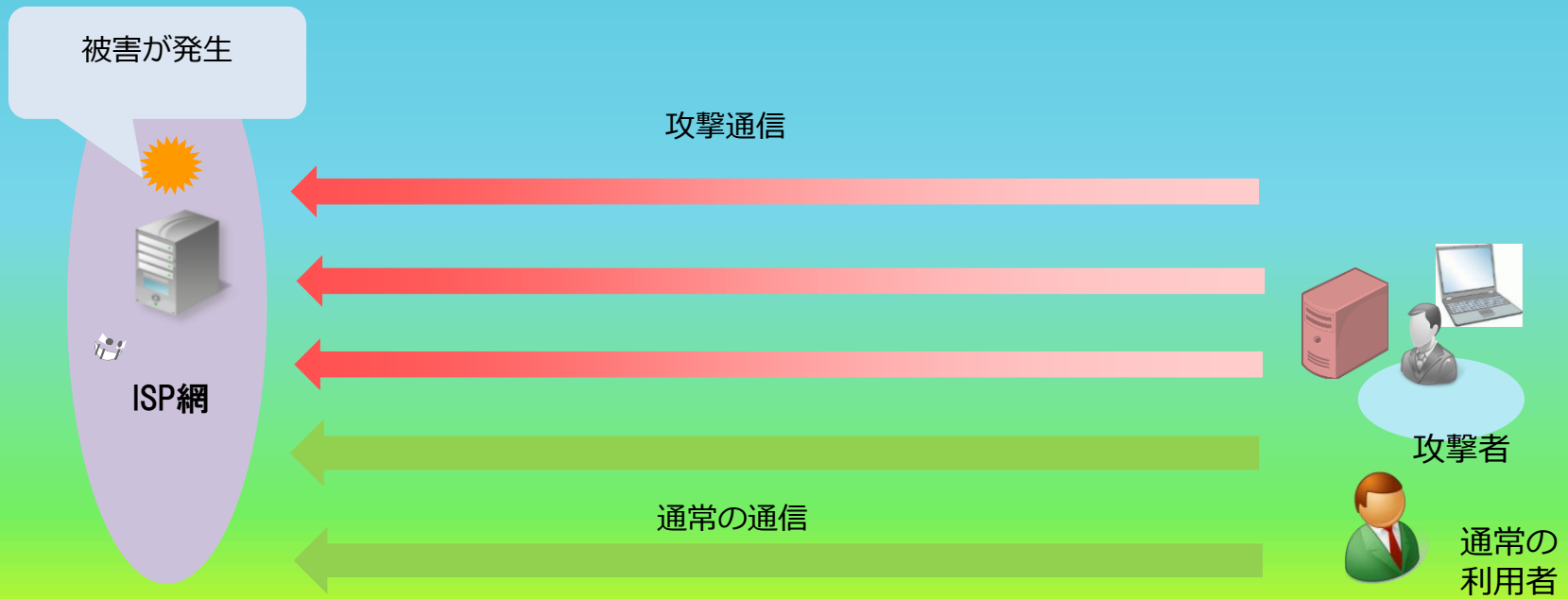
次頁以降で代表的な事例を説明

事例①　事業者設備等へのサイバー攻撃に対する実施可能な措置

送信元設備の所有者の意思と関係なく送信される大量通信等の場合

現行ガイドラインにおける整理

■サイバー攻撃等を行っている契約者を特定した上、これを止めるよう連絡をすることなどによって、事業者設備又は受信者設備等に生じる侵害を防止するため、必要かつ相当な範囲で契約者の接続ログの解析を行い、当該契約者に要請を行うことは、通常は、正当防衛又は緊急避難として違法性が阻却される（P14 (ク)）

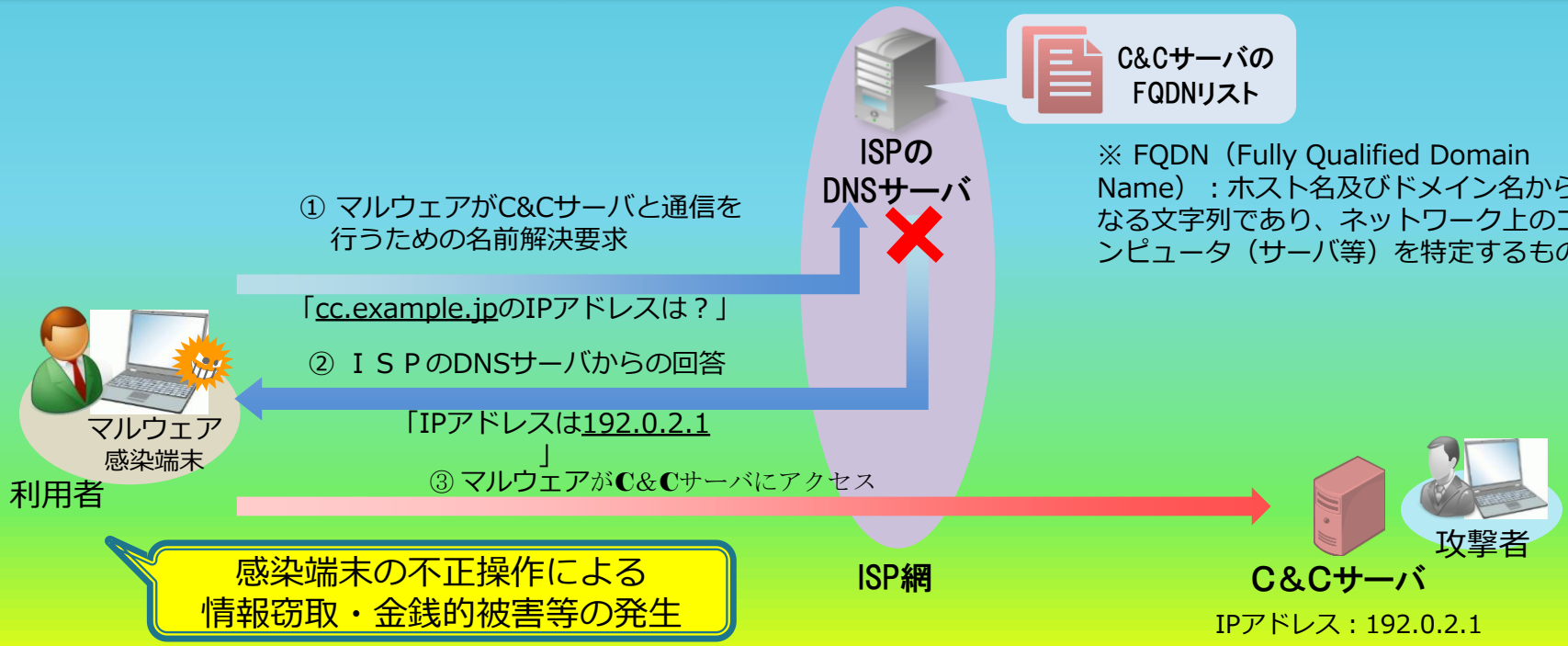


事例②　マルウェア感染端末とC&Cサーバの通信の遮断

レピュテーションDBの活用

現行ガイドラインにおける整理

■　マルウェア感染者が情報窃取や金銭的被害等の深刻な被害を受けることを防ぐとともに、感染端末を踏み台にした新たな攻撃の発生を防ぐため、C&Cサーバ（Command and Controlサーバ）のFQDN（サブドメイン＋ドメイン）※が判明している場合において、ＩＳＰが自社DNSサーバを通過する利用者のFQDNを検知し、 C&CサーバのFQDNの名前解決要求を遮断することについて、通信の秘密に属する情報（アクセス先のFQDN）の利用についての有効な同意として包括同意でも可能。（P26　（フ））



事例③　サイバー攻撃に対する事業者間の情報共有

送信元詐称通信の遮断

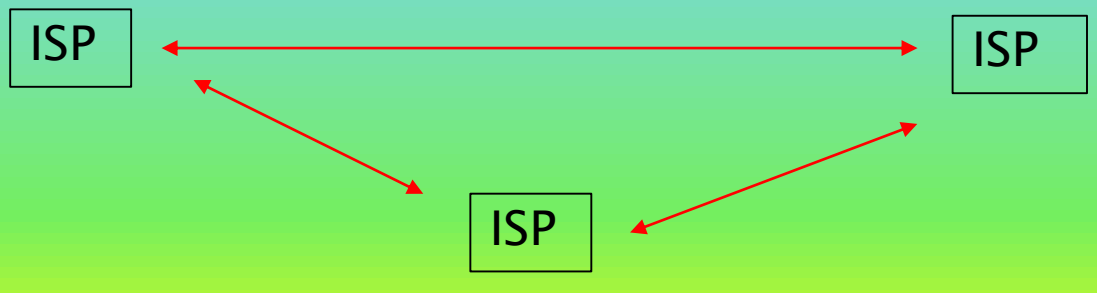
網内トラヒックの現状把握

Black Listとの突合に基づくユーザへの注意喚起

迷惑メールフィルタリングサービスにおけるフィルタ定義の共有

現行ガイドラインにおける整理

■　攻撃を受けたISPにおいては、攻撃パケットについての情報を発信元ISPと共有（P15　ク）できる。また、ISP間において、正当に統計処理されたログ情報（P18　ソ）、通信の秘密を含まないブラックリスト（P20　ト）、迷惑メールのフィルタ定義（P21　ナ）の共有が可能とされている。



総務省サイバー研第三次とりまとめを受けたガイドラインの改訂

■サイバー研とは
「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」

事業者がサイバー攻撃の対処に当たって通信の秘密等に配慮して適切に対応できるよう検討する研究会。

とりまとめ内容はインターネットの安定的な運用に関する協議会が策定する「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」に反映。

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※	電気通信事業者におけるサイバー攻撃等への対処と通信の秘密に関するガイドライン
第一次とりまとめ：平成26年4月4日	→ 同年7月22日ガイドライン改訂(第3版)
第二次とりまとめ：平成27年9月9日	→ 同年11月30日ガイドライン改訂(第4版)
第三次とりまとめ：平成30年9月26日	→ 同年冬ガイドライン改訂予定(第5版)

※2018年度構成員
座長：　佐伯仁志(東京大学)、座長代理：宍戸常寿(東京)
構成員：木村孝(JAIPA)、木村たま代(主婦連合会)、小山覚(ICT-ISAC)、鎮目征樹(学習院大学)
中尾康二(NICT)、藤本正代(富士ゼロックス)、森亮二(弁護士)、吉岡克成(横浜国立大学)

第三次とりまとめを受けたガイドラインの改訂内容

	①マルウェアに感染している可能性が高い端末の利用者に対する**注意喚起**	②マルウェアに感染している可能性が高い端末の**検知**	③C&Cサーバである可能性が高い機器の**検知**	④マルウェアに感染しえる脆弱性を有する端末の利用者に対する**注意喚起**
具体的な例	第三者情報や自らの観測により、感染端末利用者への注意喚起 (二次まではC&Cサーバに記録された情報等での注意喚起に関して整理)	ISPでDNSログなどを元に、C&Cサーバとわかっているアドレス・ドメインへの名前解決状況を調査することで、名前解決をした端末は感染可能性が高いとして検知	ISPがDNSログなどを元に、感染可能性が高い端末の名前解決状況を調査することで、名前解決の対象となったドメイン・IPアドレスをC&Cサーバである可能性が高いとして検知	事業法改正により可能になったNICT調査によるルータ等初期パスワードユーザへの注意喚起
約款での包括同意は有効か	**契約約款による包括同意でも有効** ・オプトアウト者の利益が侵害されない ・随時同意内容変更可 ・その他同一提供条件 ・相応の周知	**契約約款による包括同意でも有効** ・注意喚起サービスを未利用者は注意喚起対象外 ・記録情報の目的外利用不可と速やかな削除 ・オプトアウト者の利益が侵害されない ・随時同意内容変更可 ・その他同一提供条件 ・相応の周知	**契約約款による包括同意でも有効** ・注意喚起サービスを未利用者は注意喚起対象外 ・記録情報の目的外利用不可と速やかな削除 ・オプトアウト者の利益が侵害されない ・随時同意内容変更可 ・その他同一提供条件 ・相応の周知	**契約約款による包括同意でも有効** ・オプトアウト者の利益が侵害されない ・随時同意内容変更可 ・その他同一提供条件 ・相応の周知
OR 違法性阻却事由はあるか	**正当業務行為である** ・脆弱性のある端末の利用者に限って注意喚起を行う	**正当業務行為・緊急避難・正当防衛ではない** ・現在の危難や切迫性がなく、役務提供に支障があるかどうかも不明確	**正当業務行為・緊急避難・正当防衛ではない** ・現在の危難や切迫性がなく、役務提供に支障があるかどうかも不明確	**正当業務行為である** ・脆弱性のある端末の利用者に限って注意喚起を行う

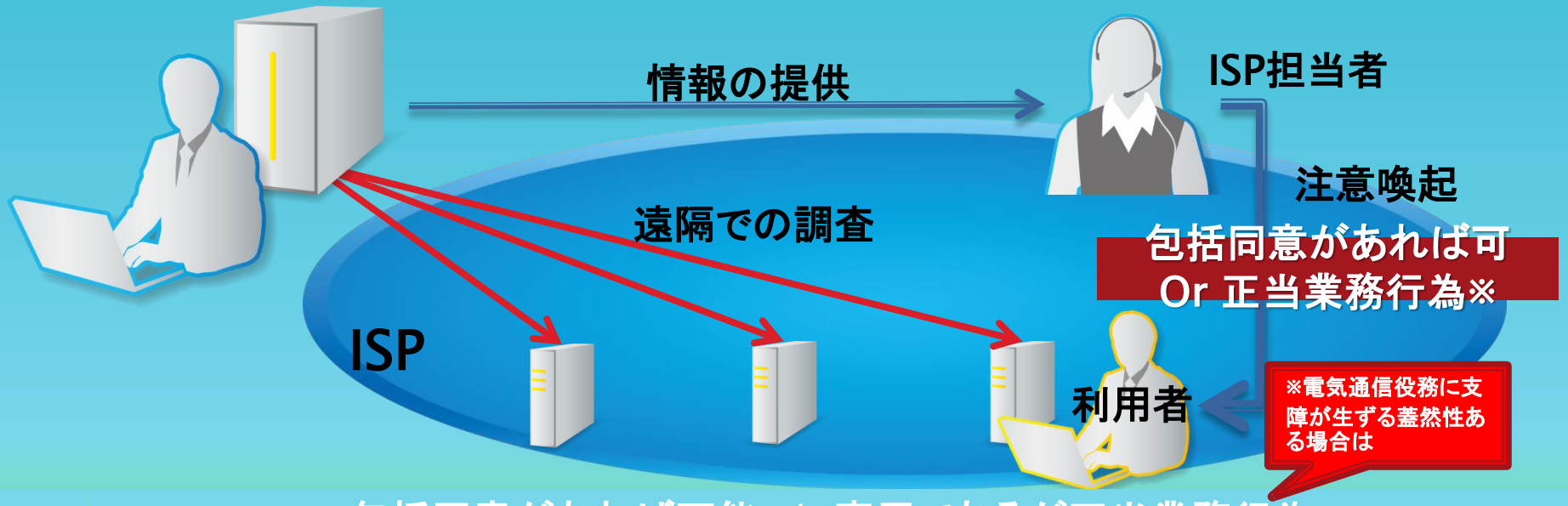
電気通信役務に支障が生ずる蓋然性ある場合

電気通信役務に支障が生ずる蓋然性ある場合

注意喚起(①/④)に当たっては支障が生じる蓋然性が高い場合に限り正当業務行為としての注意喚起が可能。
DNSログ等からの感染端末/C&Cサーバの検知(②/③)は、約款での包括同意とオプトアウト手段の整備が必要。

追加事例①：マルウェア感染可能性がある機器の注意喚起

現に攻撃を行っておらず、機器使用者に対する被害も生じていない状態において、
マルウェア感染の可能性が高い端末の使用者に対して注意喚起する行為



包括同意があれば可能　/　窃用であるが正当業務行為

今回の整理

正当業務行為と解釈するための条件

「目的の正当性」攻撃が行われると円滑な電気通信役務の提供の障害になる

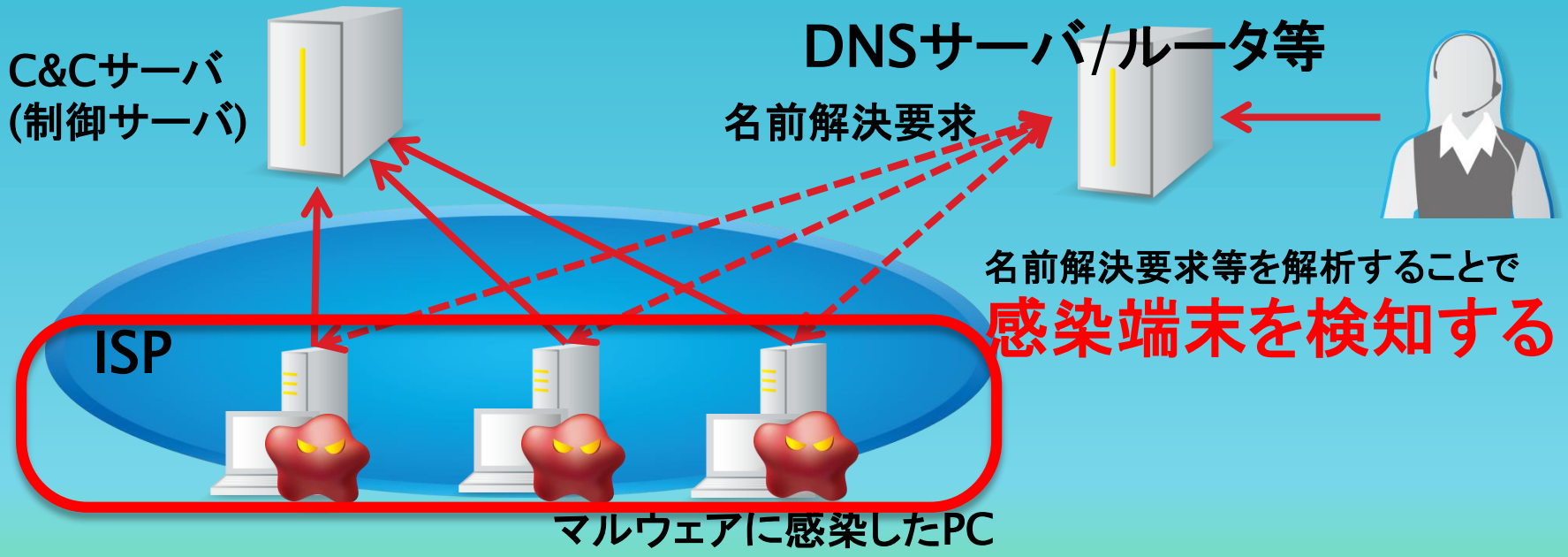
「行為の必要性」対処を求めなければ電気通信役務の提供の障害になる

「手段の相当性」認証情報とプライバシー情報利用だがやむ得ない措置と考えられる。

ICT-ISAC等からの感染端末情報に基づく注意喚起

追加事例②：マルウェア感染可能性が高い端末の検知

注意喚起のためにマルウェア感染可能性が高い端末を、
DNSの名前解決要求やトラフィックなどから特定する行為



名前解決要求等を解析することで
感染端末を検知する

今回の整理

包括同意があれば認められる

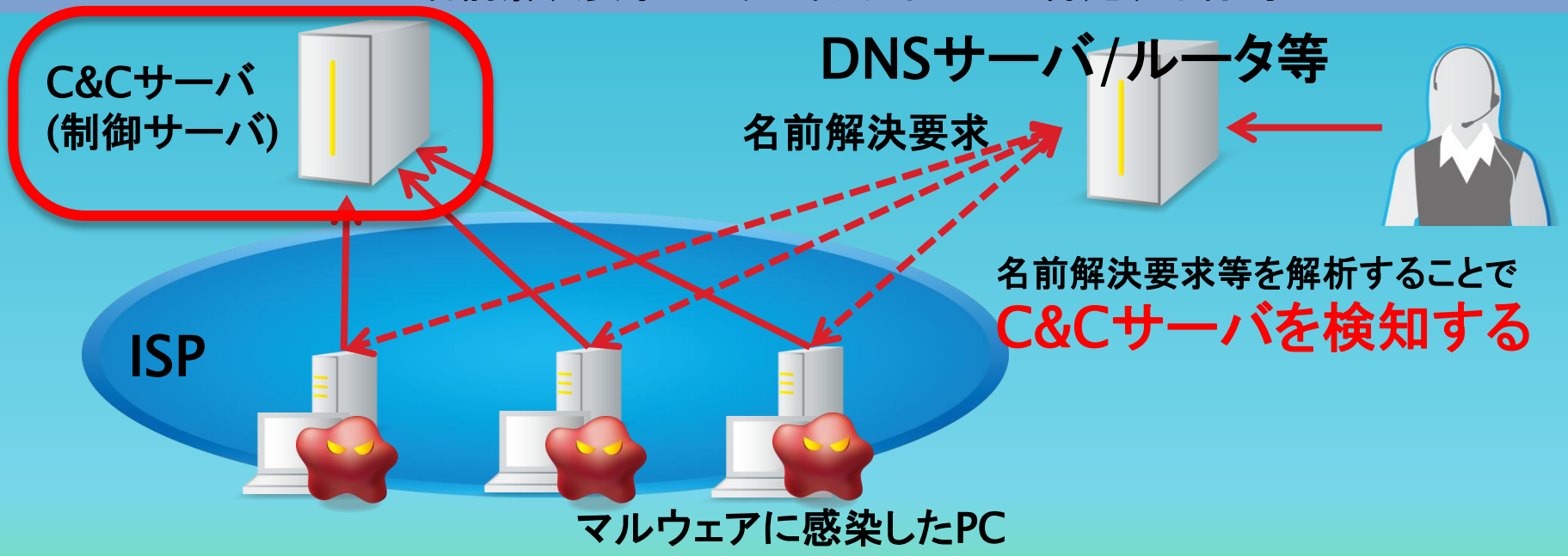
正当業務行為とは認められない

下記の条件を満たせば包括同意で認められるが、正当業務行為とは言えない

・注意喚起サービスを未利用者は注意喚起対象外・記録情報の目的外利用不可と速やかな削除・オプトアウト者の利益が侵害されない・随時同意内容変更可
・その他同一提供条件・相応の周知

追加事例③：C&Cの可能性が高いサーバの検知

注意喚起のためにマルウェア感染可能性がC&Cサーバを、
DNSの名前解決要求やトラフィックなどから特定する行為



今回の整理

包括同意があれば認められる

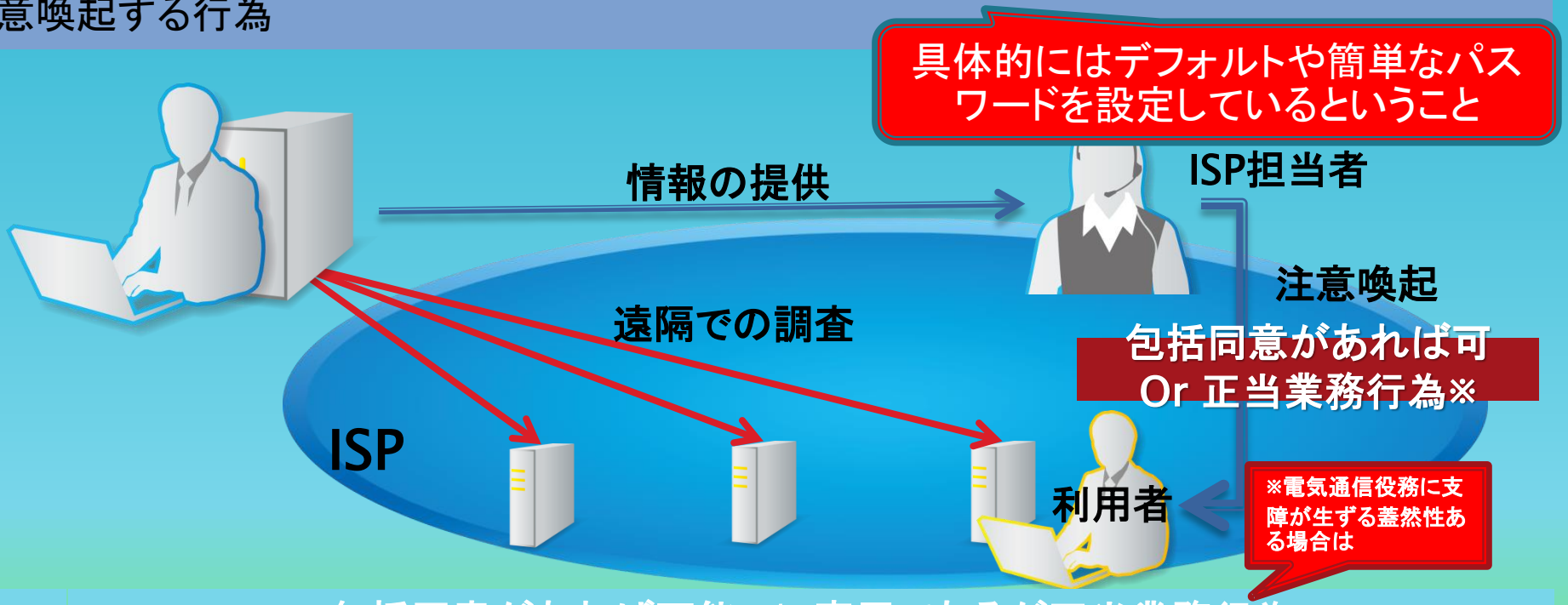
正当業務行為とは認められない

下記の条件を満たせば包括同意で認められるが、正当業務行為とは言えない

・注意喚起サービスを未利用者は注意喚起対象外・記録情報の目的外利用不可と速やかな削除・オプトアウト者の利益が侵害されない・随時同意内容変更可
・その他同一提供条件・相応の周知

追加事例④：マルウェア感染可能性の脆弱性がある機器の注意喚起

現に攻撃を行ってないが、マルウェア感染し得る**脆弱性を有する端末**の使用者に対して注意喚起する行為



包括同意があれば可能　/　窃用であるが正当業務行為

今回の整理

正当業務行為と解釈するための条件

「**目的の正当性**」攻撃が行われると円滑な電気通信役務の提供の障害になる

「**行為の必要性**」対処を求めなければ電気通信役務の提供の障害になる

「**手段の相当性**」認証情報とプライバシー情報利用だがやむ得ない措置と考えられる。

NICT(情報通信研究機構)からの情報に基づく注意喚起の根拠

省令でパスワードの基準が決まる。

総務省　10月19日公表

電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律の施行に伴う国立研究開発法人情報通信研究機構法附則第八条第四項第一号に規定する総務省令で定める基準及び第九条に規定する業務の実施に関する計画に関する省令案に係る意見募集の結果及び情報通信行政・郵政行政審議会からの答申

識別符号（ID・パスワード）の基準に関する規定について

2

改正法の概要

○ NICTが特定アクセス行為において入力する識別符号（ID・パスワード）は、「不正アクセス行為から防御するため必要な基準として**総務省令で定める基準**を満たさないものに限る」とされている。（改正法附則第８条第４項第１号）

※ 当該基準は電気通信事業者が総務大臣の認可を受けた技術的条件を勘案して定めるとされている。

省令案の概要

○ 総務省令で定める基準として、以下の①及び②のいずれにも該当する暗証符号（パスワード）を規定。（省令案第１条）

① ８文字以上であること。

② これまで送信型対電気通信設備サイバー攻撃※のために用いられたもの、同一の文字のみ又は連続した文字のみを用いたものその他の容易に推測されるもの以外のものであること。

※「送信型対電気通信設備サイバー攻撃」とは、以下を満たすものをいう。（改正電気通信事業法第116条の２第１項第１号）

① サイバー攻撃（通常の通信によるトラフィック集中等は含まない。）のうち、② 電気通信設備（電気通信事業者の電気通信設備及び利用者の端末）を攻撃の対象とし、③ その機能に障害を与える通信の送信により行われるもの（受信者の行為が介在することにより障害が発生する場合は該当しない）

【該当するパスワードの例】

これまで送信型対電気通信設備サイバー攻撃のために用いられたもの	同一の文字のみ又は連続した文字のみを用いたもの
password 、admin1234 、supervisor、smcadmin	aaaaaaaa、11111111、abcdefgh、12345678

○ 国立研究開発法人情報通信研究機構法（平成11年法律第162号）
附　則
（業務の特例）
第八条
4
一　特定アクセス行為　機構の端末設備又は自営電気通信設備を送信元とし、アクセス制御機能を有する特定電子計算機である電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備を送信先とする電気通信の送信を行う行為であって、当該アクセス制御機能を有する特定電子計算機である電気通信設備に電気通信回線を通じて当該アクセス制御機能に係る他人の識別符号（当該識別符号について電気通信事業法第五十二条第一項又は第七十条第一項第一号の規定により認可を受けた技術的条件において定めている基準を勘案して**不正アクセス行為から防御するため必要な基準として総務省令で定める基準を満たさないものに限る**。）を入力して当該電気通信設備を作動させ、当該アクセス制御機能により制限されている当該電気通信設備又は当該電気通信設備に電気通信回線を介して接続された他の電気通信設備の特定利用をし得る状態にさせる行為をいう。

これに基づき、ISPも同内容の「技術的条件」を定め、利用者に適用

2018年8月　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第一次報告

2018年9月12日　情報通信審議会一部答申

2－②　大規模なインターネット障害発生時の対策

9

■　大規模なインターネット障害やサイバー攻撃事案など、複数のネットワークに跨がって発生する障害の早期沈静化を図るためには、障害発生に係る情報共有を効果的に実施することが重要。そのため、電気通信事業者と総務省との情報共有の在り方について整理。

■　また、大規模インターネット障害の防止又は被害の最小化のため、過去に発生した障害から得られた教訓も踏まえ、各電気通信事業者等に推奨すべき対策について整理。

検討結果（概要）

・　以下の「情報共有の在り方」を踏まえ、電気通信事業者団体において、ガイドラインとして一定の方向性を整理した上で、各事業者の判断で詳細を定め実施することにより、実効性ある対応が期待できる。

【情報共有の在り方】

✓　共有すべき情報の内容

発生日時、発生場所、発生状況、影響、対応状況等が想定されるものの、具体性や情報量は問わない。
事態の早期沈静化が目的であることを鑑みれば、基本的には迅速性が優先されることから、発生した障害に係る全てを把握してからではなく、状況把握等に有益な情報であれば提供されることが望ましい。
なお、提供される情報が混乱の原因とならないように留意する必要があるとともに、右表の観点を考慮した上で提供されることが望ましい。

情報共有時に考慮いただくことが望ましい観点
利用者に広く周知可能な情報か 国民生活センター等に共有できる情報か
他の電気通信事業者に共有できる情報か

✓　続報の必要性

原因解明や復旧に有益な情報であれば続報されることが望ましい。　総務省側での調査の状況に応じて続報の協力をお願いすることがある。
なお、一報した全ての障害について最後まで情報提供を求めることはしない。

✓　通信手段

電話、メール、FAXのいずれでも可とする。
事業者から総務省への情報提供は、基本的には既存の連絡窓口（24時間、365日対応可能※）に行う（総合通信局が既存の窓口の場合は総合通信局へ）こととし、本省と総合通信局の間でも情報共有を行うこととする。　※ 事業者側に24時間、365日の対応をお願いするものではない。

✓　その他

他の電気通信事業者や自社のサービスを利用する法人ユーザーへの影響の可能性に係る情報を可能な範囲で提供されることが望ましい。

・　誤送信された経路情報の受信防止及び不要な経路情報の送信防止（フィルタリング機能の設定等）に係る対策等について「情報通信ネットワーク安全・信頼性基準」等に規定し、各電気通信事業者等の実施を促すこととする。

経路情報の設定手順、設定誤りによる障害時事業者間情報共有、総務省への確認、利用者への周知について規定。年度内パブコメ予定