資料１－２

サイバーセキュリティ等に係る
現状と課題について

平成29年10月

事務局

1　インターネットにおける最近の大規模な障害の動向

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	・DNS サーバがDDoS 攻撃を受け、一部の電気通信事業者において、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DNS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

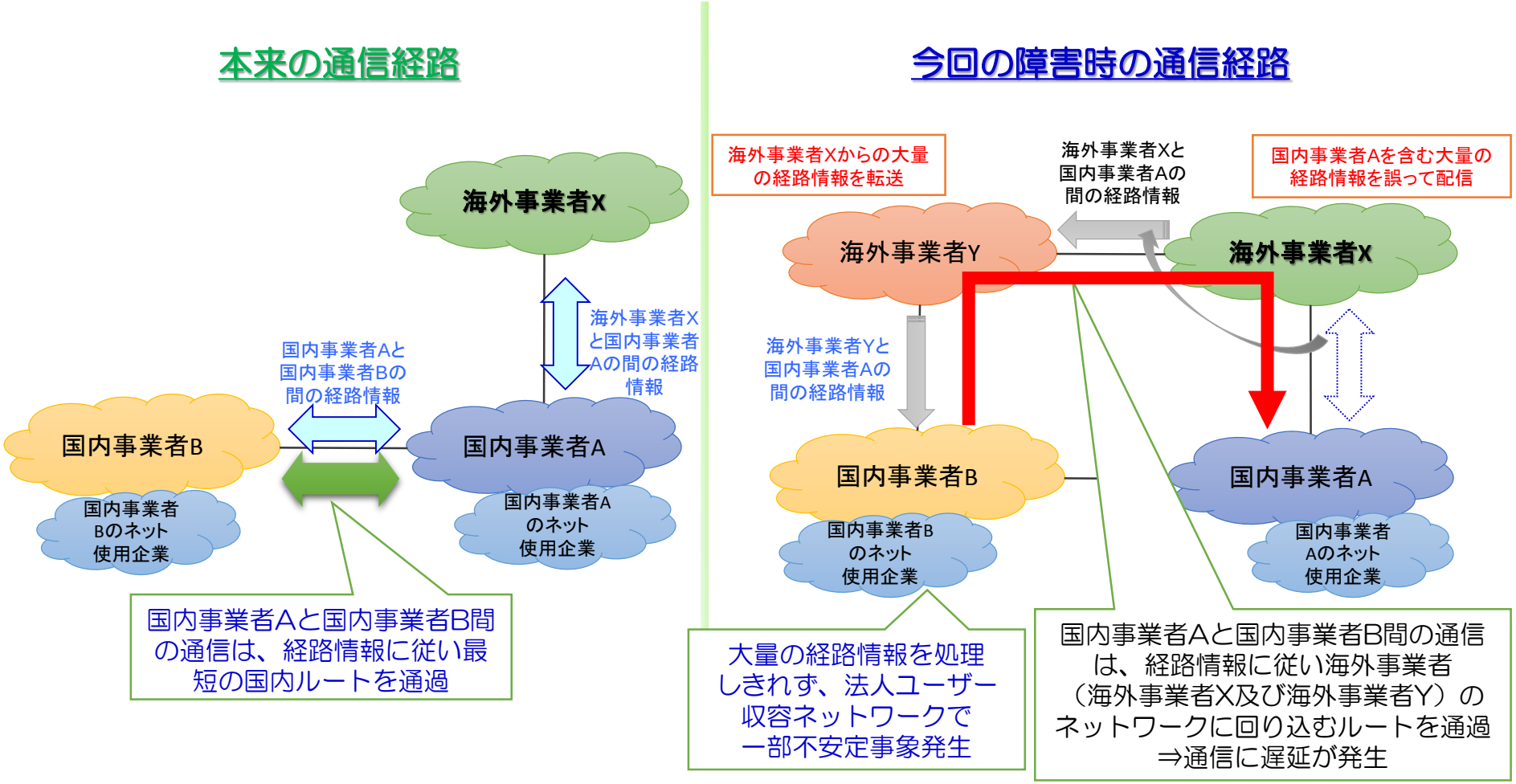
海外

2016年9月13日	【Akamai（米国）】 ・サイバーセキュリティ専門ジャーナリストのBrian Krebs氏が運営するブログに対し、Mirai※に感染した約18万台のIoT機器から約620Gbpsに及ぶDDoS攻撃が発生 ・同氏に無償でホスティングサービス及びDDoS攻撃緩和サービスを提供していたAkamaiは、サーバーへの負荷に耐えきれず、有料顧客へのサービスを優先するため同氏に対するサービスを停止
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のサーバー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、英国政府ウェブサイト等）に数時間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

本年8月に発生した大規模なインターネット接続障害

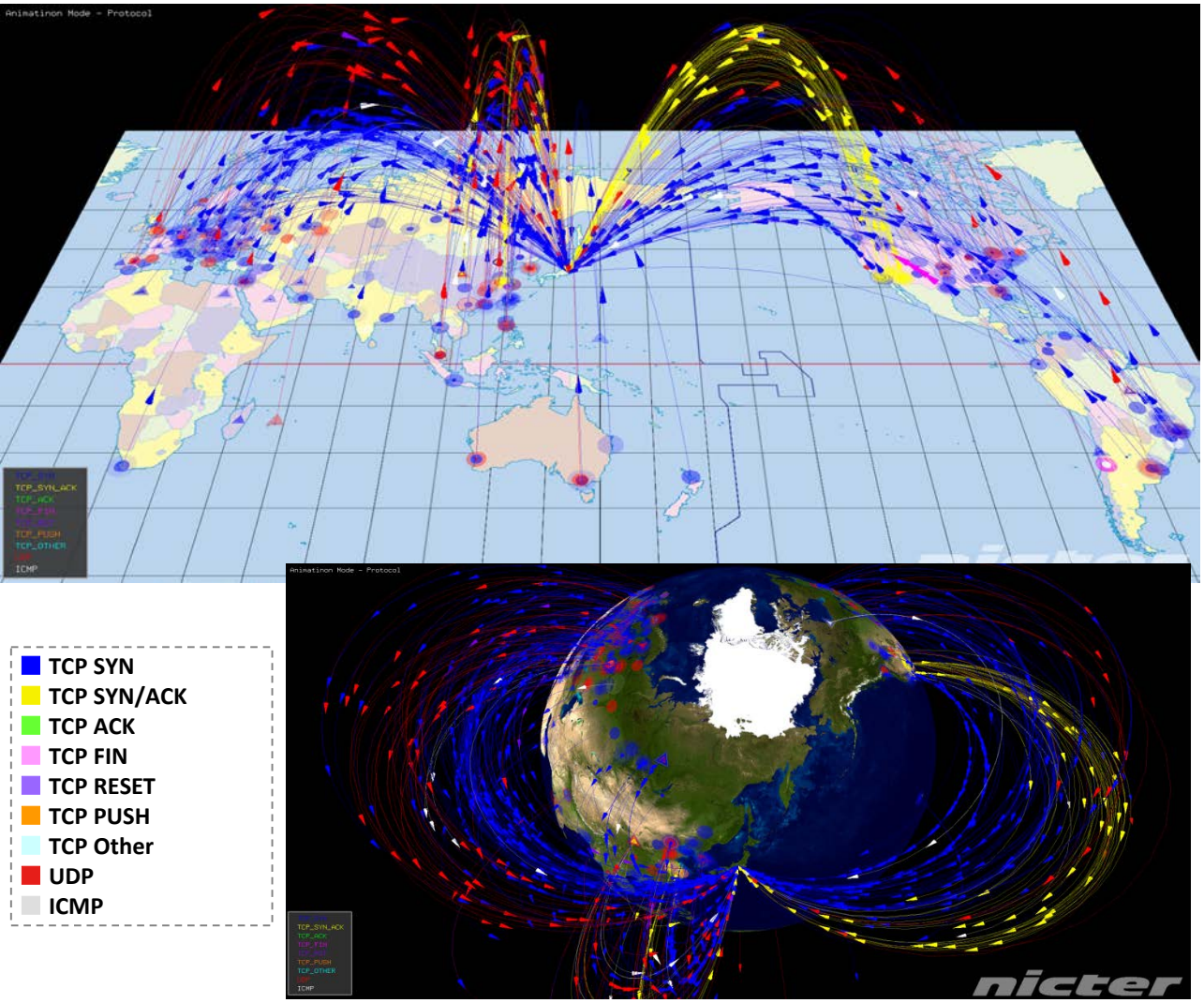
- 本年8月25日、海外事業者Xが行う通信経路設定の誤りが原因となり、我が国の電気通信事業者（国内事業者A、国内事業者B）の一部の回線に過大な負荷がかかったことにより、インターネットに障害が発生



２　インターネットに障害を及ぼすサイバー攻撃の動向

IoT機器を狙った攻撃が急増（NICTERによる観測）

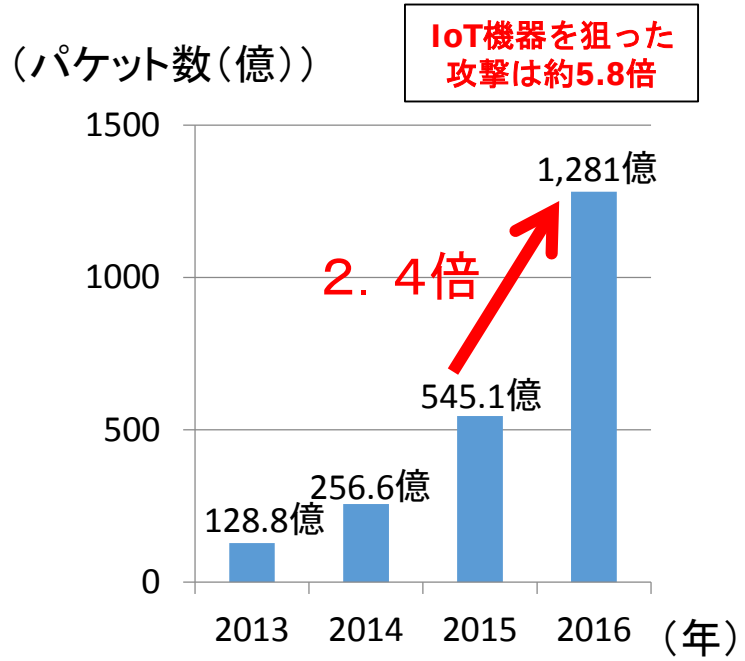
➢ 国立研究開発法人 情報通信研究機構（NICT）では、未使用のIPアドレス30万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測



・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

１年間で観測されたサイバー攻撃回数



サイバーセキュリティ上の主な脅威の分類

攻撃先	攻撃手法	主な影響（例）	脅威の概要	代表的な事例等
ネットワーク	DDoS攻撃等	ネットワーク・Webサーバの機能停止	サーバやネットワークに対して大量のデータを送りつけて機能不全に陥れる。	・リオデジャネイロ五輪の公式サイト等に対して約540Gbpsの攻撃が発生［2016年］ ・Mirai（マルウェア）に感染したIoT機器群からDyn（DNSサービス）に対して約1.2Tbpsの攻撃が発生［2016年］
企業等の情報システム	不正アクセス	Webサイト等の改ざん	Webサーバの脆弱性の悪用又は管理用アカウントへの不正アクセスにより正規のWebサイトの内容を改ざんし、いたずら、政治的主張の発信、マルウェアの配布等を行う。	・Webサイト管理システム「WordPress」の脆弱性を悪用したWebサイトの改ざんが多発。［2017年］
		情報の窃取	ID/パスワードの不正入力（不正リスト利用、総当たり等）やソフトウェア脆弱性の悪用等により、PCやサーバ等に不正に侵入し、情報を窃取する。	・ソニーが運営するプレイステーションネットワークが不正アクセスを受け、約7,700万件の保有個人情報が流出［2011年］
	マルウェアによる標的型攻撃	情報の窃取	マルウェアを添付したメールを送付し、感染させる等により、PCやサーバ等に不正に侵入し、情報を窃取する。	・日本年金機構から約125万件の保有個人情報が流出［2015年］
		産業用システムの機能停止	産業用システムを対象とするマルウェアを発電所等のインフラの制御システム等に感染させ、インフラの機能を停止。	・ウクライナにおいて、マルウェア「Crash Over Ride」等を利用したサイバー攻撃による大規模な停電が発生［2015年、2016年］
不特定多数の個人・企業等のPC	ランサムウェア	金銭の窃取	マルウェアによりPC内のデータを暗号化し、データの復元と引き替えに金銭を要求。	・ランサムウェア「Wanna Cry」への感染が世界的に拡大し、国内外の大手企業や公共施設を含む多数のPCが感染。［2017年］
不特定多数の個人	フィッシング	情報の窃取	金融機関等を装った偽のウェブサイトに誘導し、クレジットカード番号やオンラインバンキングのログイン情報等を入力させて不正窃取し、当該情報を利用して不正送金を行う。	・フィッシング情報の年間届出件数が約22,000件［2014年］ ・金融庁のウェブサイトを装ったフィッシングサイトが出現［2015年］

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、また、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）

３　電気通信事業におけるサイバー攻撃等を起因とするネットワーク障害に関連した制度の現状

サイバー攻撃等を起因とするネットワーク障害に関連した制度の現状

電気通信設備の安全・信頼性の確保に関する基準

○ 事業用電気通信設備の技術基準

・電気通信事業者に対し、使用する電気通信設備について、役務の提供に支障を及ぼさないこと、利用者又は他の事業者の接続する設備に障害を与えないことなどを確保するものとして規定された技術基準への適合を義務づけている（電気通信事業法第41条）。（当該技術基準では、不正プログラムに対する防護措置等について規定）

・「情報通信ネットワーク安全・信頼性基準」において、情報通信ネットワークの耐力強化と機能の安定的な維持等を図るため、ハードウェア及びソフトウェアに備えるべき機能やシステムの維持・運用等の安全・信頼性に関する事項を推奨している。（ガイドラインでは、ファイアウォールを設置して適切な設定を行うこと等について規定）

○ 端末設備等の技術基準

・事業者の電気通信回線設備に接続して使用される利用者の端末設備について、事業者設備の機能に障害を与えないこと、他の利用者に迷惑を及ぼさないことなどを確保するものとして、技術基準に適合することを求めている（同法第52条）。（当該技術基準には、サイバーセキュリティに係る事項は含まれていない）

電気通信役務の提供に支障が生じた場合の規定

○ 業務の停止等の報告（電気通信事業法第28条）

電気通信事業者は、重大な事故等が生じた場合、原因等を遅滞なく総務大臣に報告しなければならない。

○ 業務改善命令（同法第29条第１項第８号）

総務大臣は、事故により電気通信役務の提供に支障が生じている場合に、電気通信事業者が必要な措置を速やかに行わない場合は、業務改善命令を行うことができる。

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

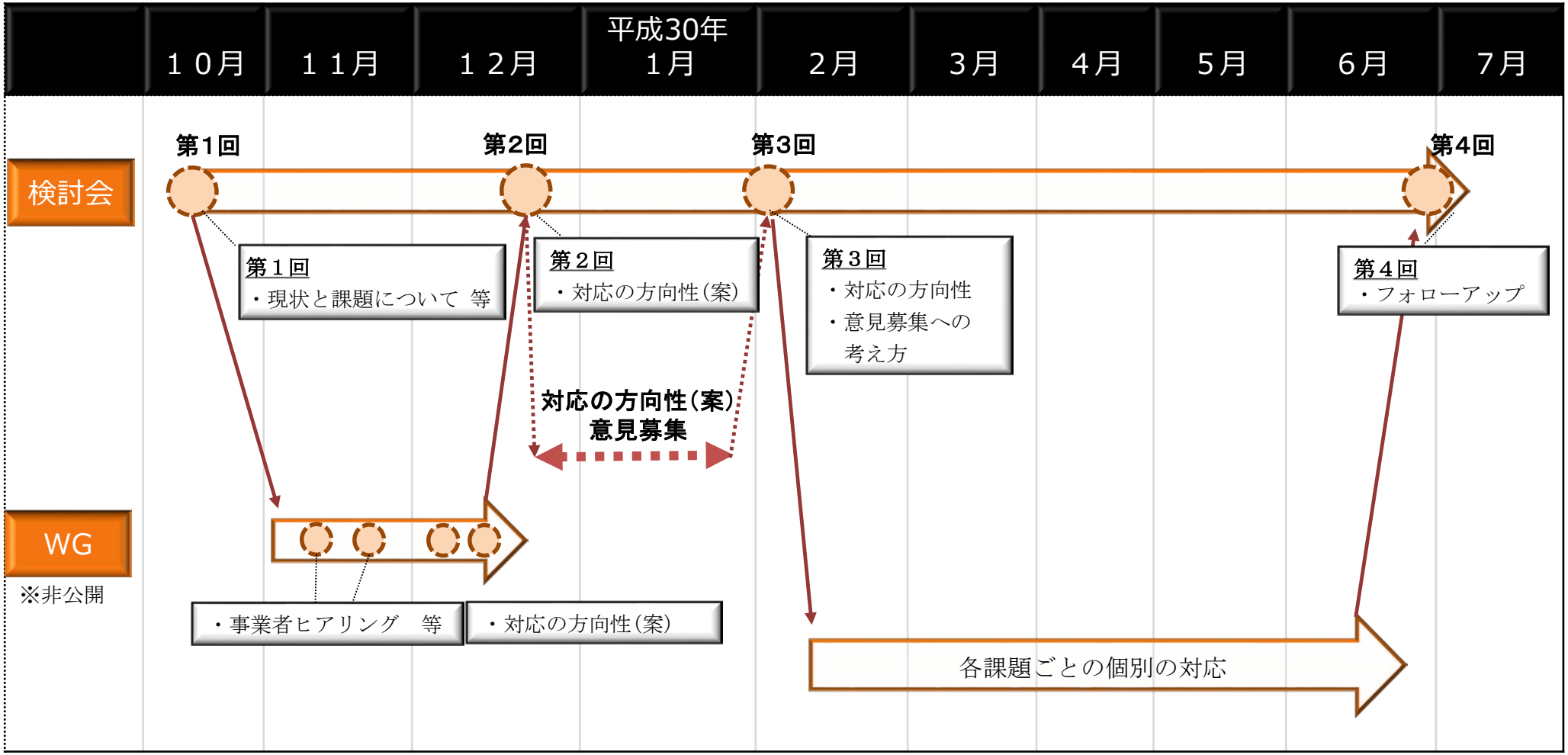
○ 平成19年5月に業界団体が策定。（これまでに3回改訂。平成27年11月最終改訂。）

○ 通信の秘密の保護に配慮しつつ、電気通信事業者が電気通信役務の円滑な提供の確保のための対処を講ずることができるよう、通信の秘密の侵害に対する違法性が阻却されると考えられる具体例等を提示。

４　検討の進め方

検討の進め方

- 構成員の一部と事業者団体等からなる非公開のWGを設け、電気通信事業者等から検討事項について意見を聴取し、制度的課題を整理した上で、「対応の方向性(案)」を作成
- 第2回の検討会において、「対応の方向性(案)」を議論の上、意見募集手続を経てとりまとめ、それを受けた各課題ごとの個別の検討状況について、フォローアップを実施



（参考）その他総務省のサイバー攻撃等に関する取組

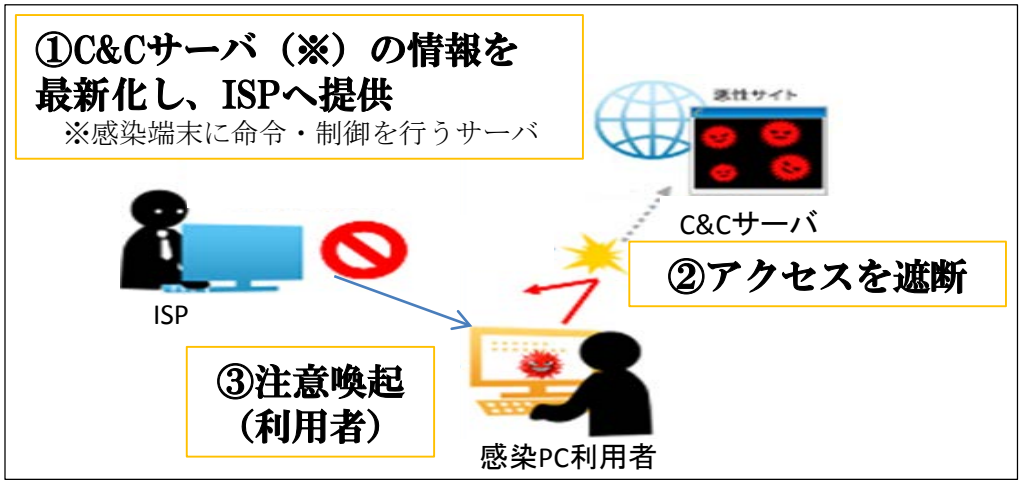
ACTIVE（Advanced Cyber Threats response InitiatiVE）

- 平成25年11月から、総務省と複数のISP事業者やセキュリティベンダー等の事業者が連携し、マルウェア被害を未然に防止する取組等の実証実験を行う官民連携プロジェクト（ACTIVE）を実施
- ISPは、C＆CサーバのURL情報の提供を受けた場合、感染PC利用者からのC&Cサーバへのアクセスを遮断している

（１）マルウェア駆除の取組

① マルウェアに感染したPCを特定。
② **感染PCのIPアドレスをISPに提供**。当該ISPから利用者に感染PC端末について適切な対策を取るよう注意喚起。
③ 注意喚起の内容に従い利用者がPCからマルウェアを駆除。

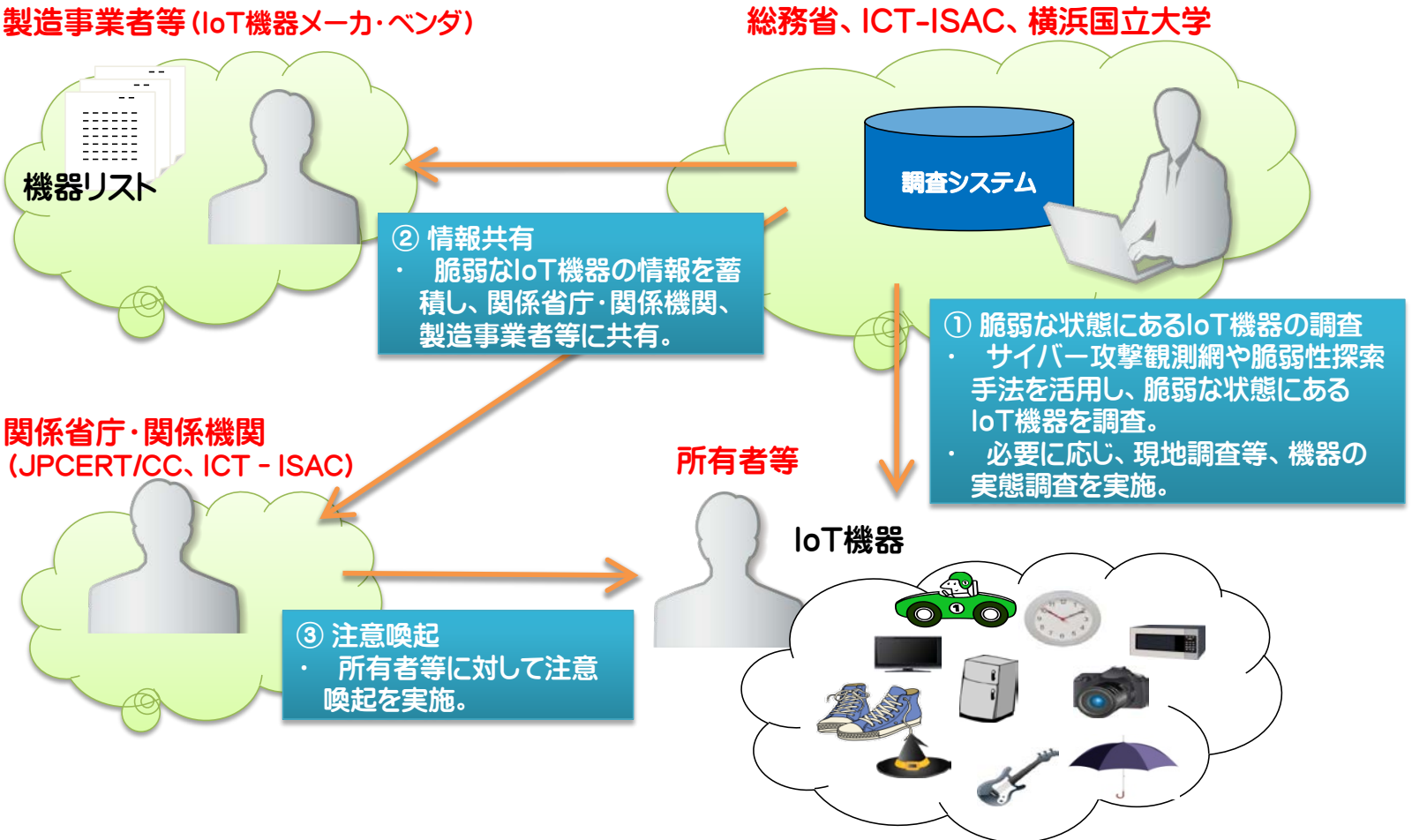
（２）マルウェア被害未然防止の取組



① **C&Cサーバ**のURL情報を最新化し、ISPへ提供。
② **感染PC利用者からのC&Cサーバへのアクセスを遮断する**。
（**2016年2月から2017年9月までで約2億806万件の遮断実績**）
③ 感染PC利用者に注意喚起。

IoT機器に関する脆弱性調査等

- IoT機器は、性能が低く、また、メーカ、システム構築業者、サービス提供者等が複雑に連携して構築されており、従来のPCのようなセキュリティ対策が困難
- こうした課題に対処するため、平成29年９月から、ネットワーク上の脆弱なIoT機器の調査及びユーザへの注意喚起等、業界を超えたIoT機器に関するセキュリティ対策（IoTセキュリティフレームワーク）の調査・実証等を実施

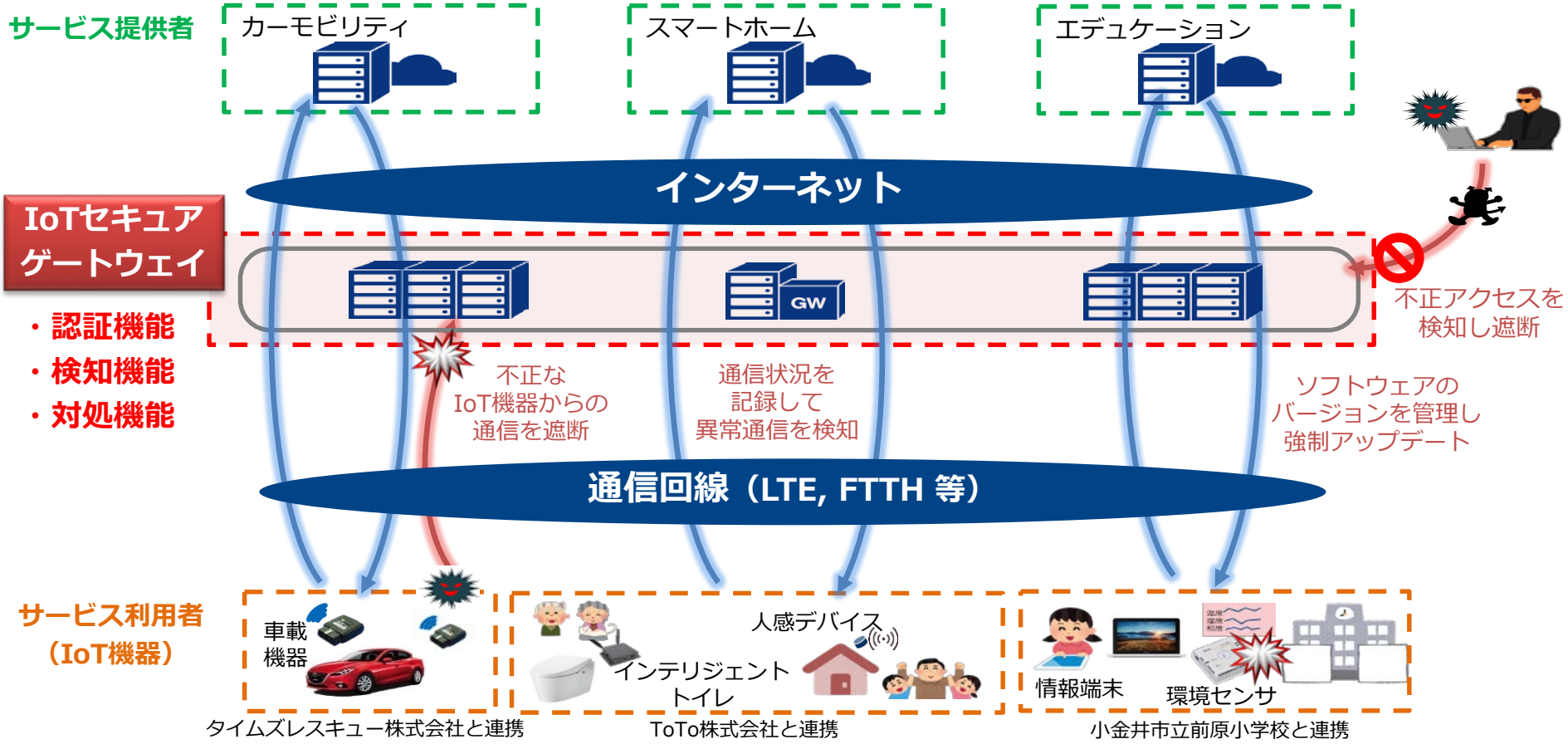


IoTセキュアゲートウェイの実証実験

- IoT時代における我が国のサイバーセキュリティを確保し、我が国の経済社会の活力の向上や持続的発展に寄与するため、新たな脅威にも対応したセキュリティ対策の実証を実施
- 具体的には、IoT機器とインターネットの境界にIoTセキュアゲートウェイを設置し、その有用性に関する検証を実施

実証実験のイメージ

実施主体：NTTコミュニケーションズ株式会社、平成29年12月より実証実験を開始（平成28年度補正（2.5億円））

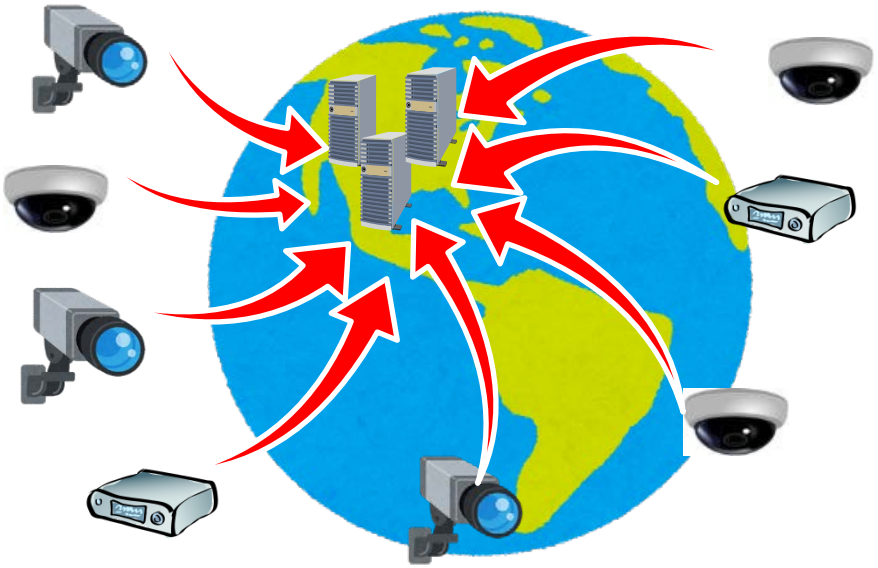


参考資料

構成員限り

（参考1-2）IoTによる大規模DDoS攻撃について

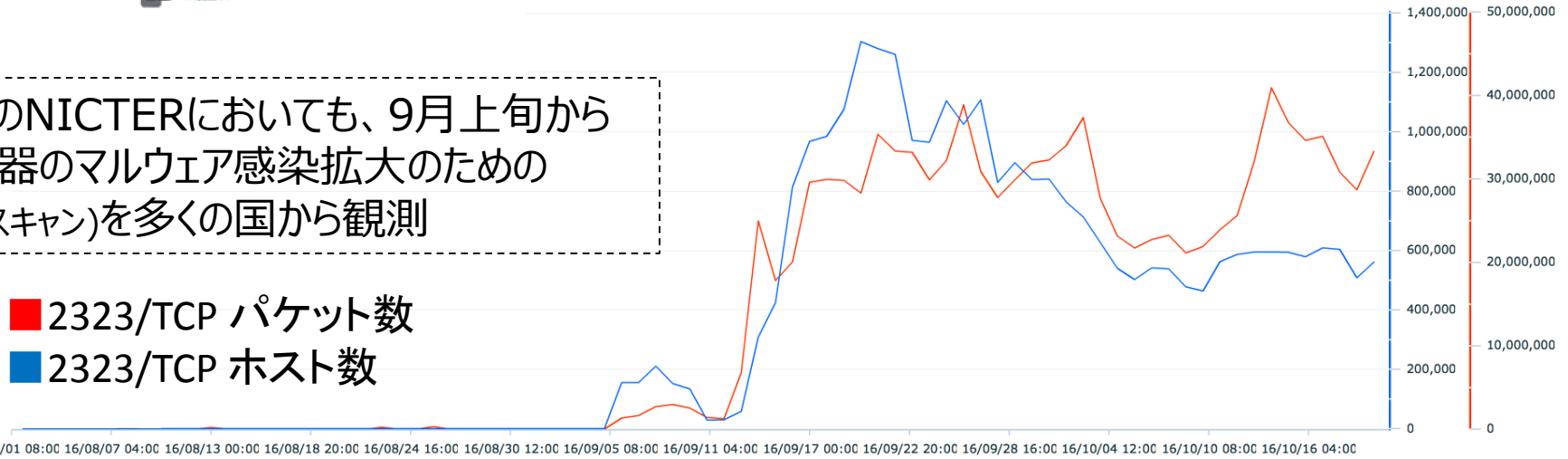
- 2016年10月21日米国のDyn社のDNSサーバーに対し、大規模なDDoS攻撃が2回発生
- 同社からDNSサービスの提供を受けていた企業のサービスにアクセスしにくくなる等の障害が発生
- サイバー攻撃の元は、「Mirai」というマルウェアに感染した大量のIoT機器



- ✓ マルウェアに感染した10万台を超えるIoT機器からDyn社のシステムに対し大量の通信が発生
- ✓ 最大で1.2Tbpsに達したとの報告もあり

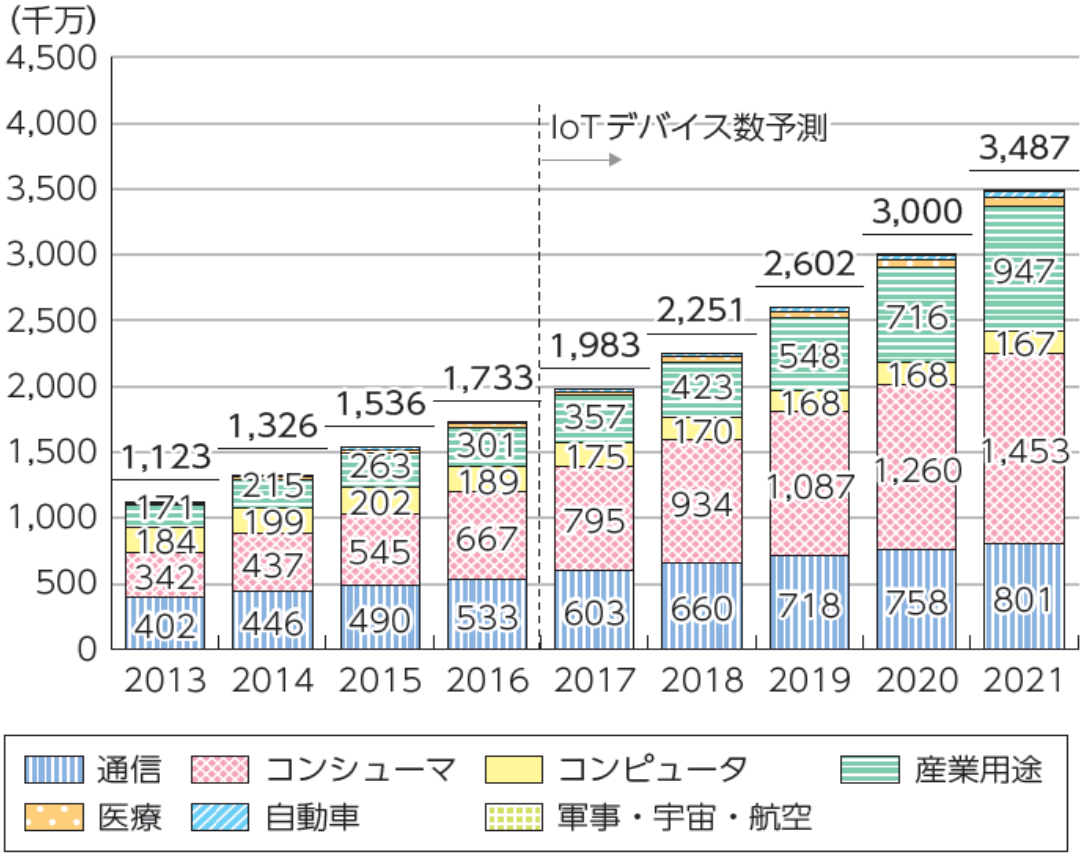
出典: http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/

- ✓ NICTのNICTERにおいても、9月上旬からIoT機器のマルウェア感染拡大のための通信(スキャン)を多くの国から観測



（参考2-1）IoT機器の推移と普及分野

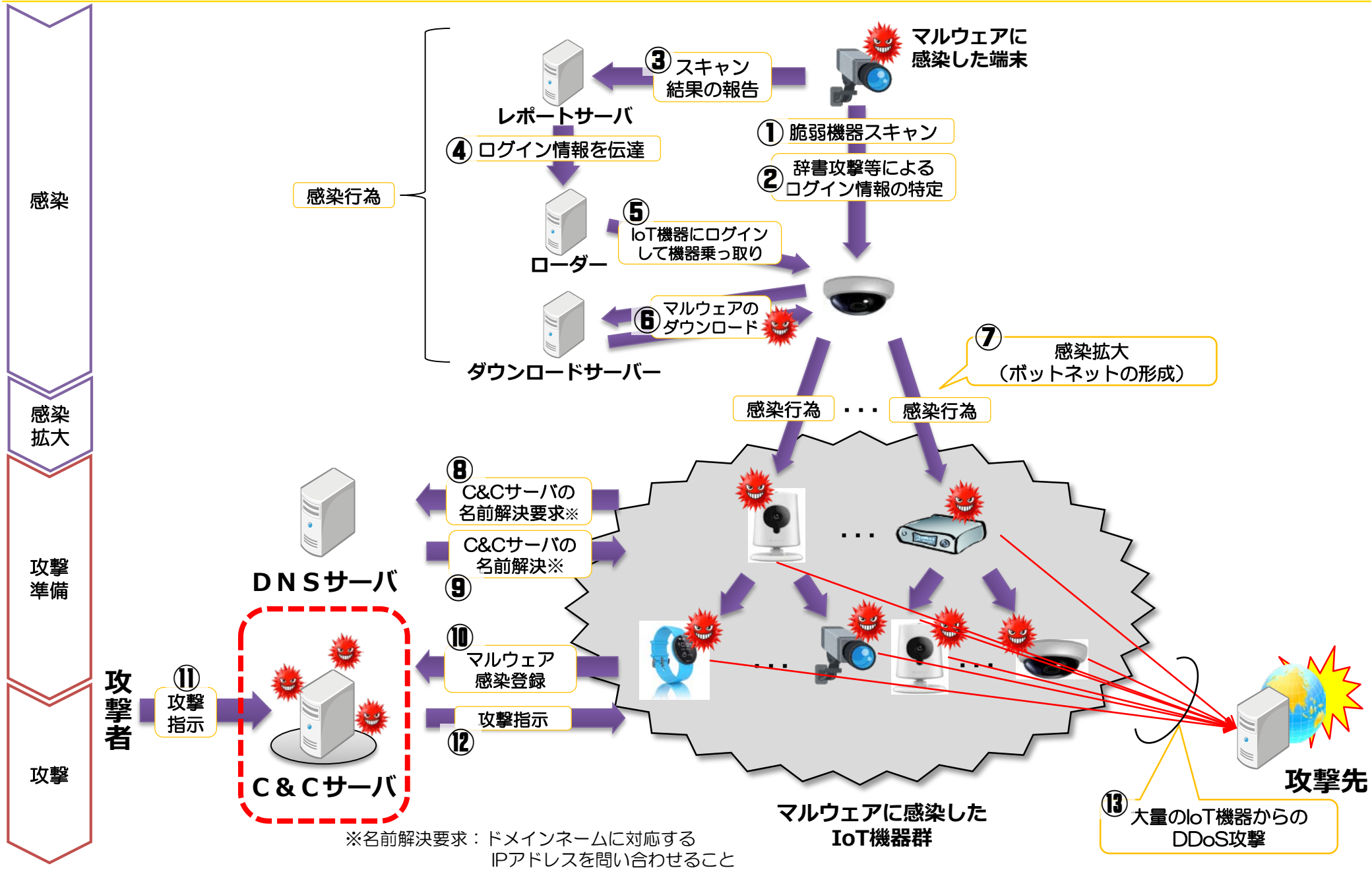
- IHS Technology の推定によれば、2016年時点でインターネットにつながるモノ（IoTデバイス）の数は173億個であり、2020年までに300億個まで増加するとされており、そのうち、約7割が消費者又は産業用途向けのものである。



（出典）IHS Technology

※ 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およびWifi・WIMAXなどの無線通信インフラおよび端末。
「コンシューマ」：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、その他を含む。
「コンピュータ」：ノートPC、デスクトップPC、サーバ、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。
「医療・産業用途」：画像診断装置ほか医療向け機器、コンシューマヘルスケア機器、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。
「自動車」：自動車のUnder the food（制御系）およびInfortainment（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）。

（参考2-2）マルウェア感染したIoT機器群によるDDoS攻撃の仕組み（例）



※名前解決要求：ドメインネームに対応するIPアドレスを問い合わせること

（参考2-3）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

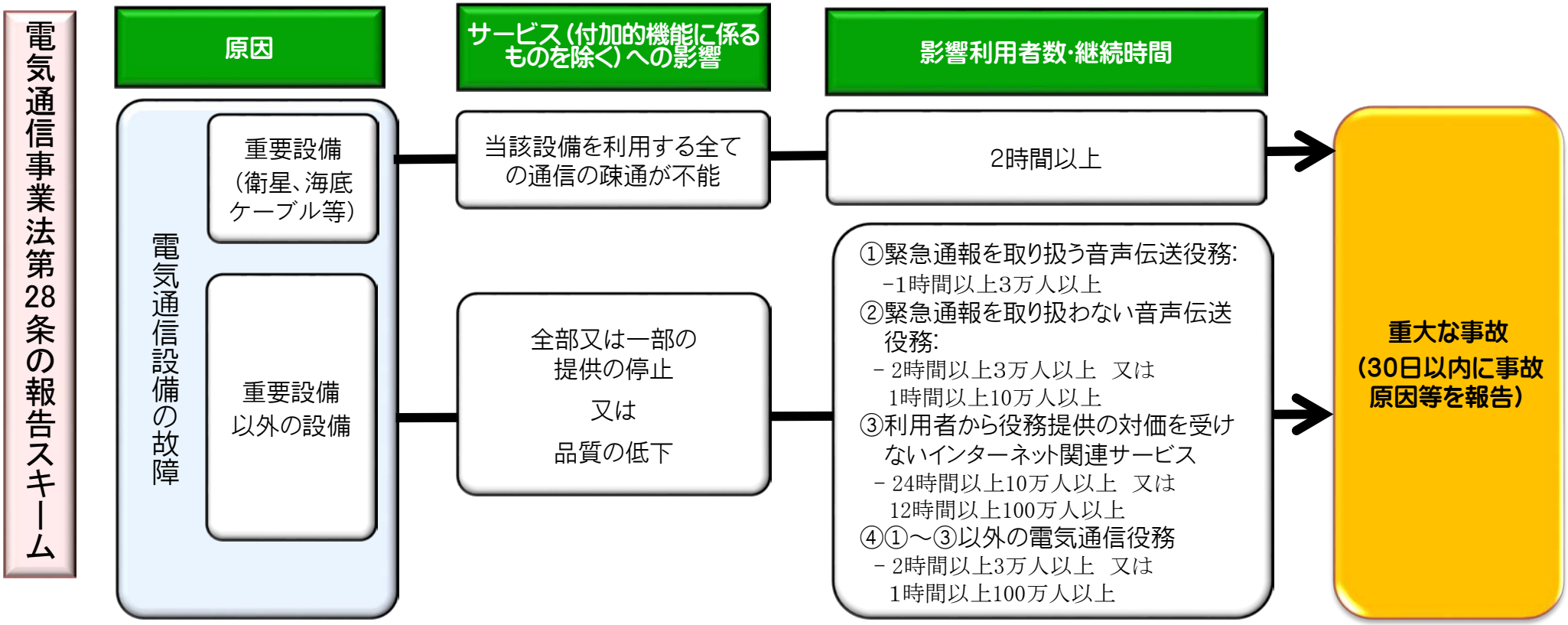
○　2016年　リオデジャネイロ大会

- 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/

（参考3-1）電気通信事業者の電気通信役務の提供に支障が生じた場合に関する規定

- **報告**：電気通信事業者は、一定規模以上の電気通信事故（重大な事故）等が生じた場合、原因等を遅滞なく総務大臣に報告しなければならない（電気通信事業法第28条）。
- **業務改善命令**：総務大臣は、電気通信事業者が、事故により電気通信役務の提供に支障が生じている場合に電気通信事業者がその支障を除去するために必要な修理等必要な措置を速やかに行わない場合は業務改善命令を行うことできる（同法第29条第１項第８号）。
- **罰則**：正当な理由なく電気通信事業者の事業用電気通信設備の維持又は運用の業務の取り扱いをせず、電気通信役務の提供に支障を生ぜしめた電気通信事業に従事する者は、二年以下の懲役又は五十万円以下の罰金に処する（同法第180条第２項）。



（参考3-2）電気通信設備の安全・信頼性の確保に関する基準

- 電気通信事業法では、電気通信事業者は、事業用電気通信設備を総務省令で定める技術基準に適合するよう維持すること等が義務づけられている。また、「情報通信ネットワーク安全・信頼性基準」では、情報通信ネットワークの耐力強化等と機能の安定的な維持を図るため、ハードウェア及びソフトウェアに備えるべき機能やシステムの維持・運用等の安全・信頼性に関する推奨基準（ガイドライン）が規定されている。これらの基準にサイバーセキュリティに係る事項が含まれている。
- また、電気通信回線設備に接続して使用する利用者の端末設備についても、その接続が総務省令で定める技術基準に適合することを要求しているが、現行の当該基準にサイバーセキュリティに係る事項は含まれていない。

強制基準

技術基準

＜事業用電気通信設備の技術基準＞

以下の事項が確保されるものとして規定
①電気通信設備の損壊又は故障により、電気通信役務の提供に著しい支障を及ぼさないようにすること
②電気通信役務の品質が適正であるようにすること
③通信の秘密が侵されないようにすること
④利用者又は他の電気通信事業者の接続する電気通信設備を損傷し、又はその機能に障害を与えないようにすること
⑤他の電気通信事業者の接続する電気通信設備との責任の分界が明確であるようにすること
※サイバーセキュリティに係る事項については、利用者又は他の事業者から受信したプログラムの機能の制限等について規定

＜端末設備の接続の技術基準＞

以下の事項が確保されるものとして規定
①電気通信回線設備を損傷し、又その機能に障害を与えないようにすること
②電気通信回線設備を利用する他の利用者に迷惑を及ぼさないようにすること
③電気通信事業者の設置する電気通信回線設備と利用者の接続する端末設備との責任の分界が明確であるようにすること
※サイバーセキュリティに係る事項はなし

自主基準

管理規程

＜事業者ごとの特性に応じた基準＞

サイバーセキュリティに係る事項を含む事業用電気通信設備の管理の方針・体制・方法を規定

ガイドライン

安全・信頼性基準

＜努力目標として、全ての電気通信事業者の指標となる基準＞

ソフトウェアの品質検証、事故状況等の情報公開、ネットワーク運用管理（運用基準の設定、委託保守管理）等
※サイバーセキュリティに係る事項については、ファイアウォールを設置して適切な設定を行うこと等について規定

（参考3-3）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概要

- 電気通信事業者がサイバー攻撃への対処において行う通信の解析や遮断等は通信の秘密の侵害に該当することから、通信の秘密の保護に配慮しつつ、電気通信事業者が電気通信役務の円滑な提供の確保のための対処を講ずることができるよう、当該侵害の違法性が阻却されると考えられる具体例等を提示。
- 平成19年5月業界団体（（社）日本インターネットプロバイダー協会、（社）テレコムサービス協会等）が策定（これまでに3回改訂。平成27年11月最終改訂。）

サイバー攻撃対処に関する主な整理の例

①契約者の同意に基づく場合

- 契約者から個別の同意を得て、通信の内容等を分析し、攻撃特性に合致する通信を遮断
- 契約者から契約約款等に基づく包括的な同意を得て、DNSサーバにおいて、C&Cサーバのリストにある名前解決要求を遮断

②事業者設備等に支障が生じる場合

- 現にサイバー攻撃等が発生している場合に、事業者設備に生じる侵害を防止するため、サイバー攻撃等の特性を把握した上、合致する通信を遮断（正当防衛又は緊急避難）
- 通信の（一部）遮断を行わなければ事業者設備に支障が生じ得る場合に、遮断する通信の範囲を最小限にとどめつつ、事業者設備に支障が生じるおそれを防止するために、サイバー攻撃等の特性を把握した上、合致する通信を相当な限度で遮断（正当業務行為）
- 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を解析し、サイバー攻撃等の送信元の契約者を特定し、当該契約者にマルウェアの駆除等を要請（正当防衛又は緊急避難）

③サイバー攻撃等への共同対処

- 受信者側のISP等が、受信者の同意を得て提供された攻撃通信発信者の情報（IPアドレス）を送信側ISP等に提供し、当該送信側ISP等が当該情報に基づき必要な範囲で相当な方法により発信者に警告等（正当防衛、緊急避難）
- 外形上明らかに異常な通信を認知し、それにより自社業務の遂行に支障が生ずるおそれが認められる場合、当該通信の原因特定に必要な範囲で当該通信の経路となっている電気通信事業者間で通信ログデータの分析結果を共有（正当業務行為）