資料２－２

円滑なインターネット利用環境の確保に関する検討会

対応の方向性（案）

２０１７年１２月

目次

１．　検討の背景

我が国におけるインターネットの商用利用の開始以降僅か四半世紀の間に、情報通信ネットワークインフラは大幅な高度化を遂げ、ＳＮＳ、クラウドサービス等に代表される ICT 利用が進展してきた。これに伴い、現在では多くの個人、企業、団体等がインターネット上で自由に情報をやりとりする状況が現出しており、インターネットは、今やあらゆる場面で国民生活や社会経済活動の基盤として活用されている。一方、国内外において大規模なサイバー攻撃が繰り返し行われている中で、DNS サーバをはじめとする電気通信事業者の保有する設備に対する DDoS 攻撃等によって設備に支障が生じ又は利用者の設備に対する DDoS 攻撃等の際に電気通信事業者の通信ネットワークに過負荷がかかる等によりインターネットにおける通信障害等が頻発しており、インターネットの円滑な利用環境の確保が極めて重要な課題となっている[1]。

これまで、インターネットを含めた電気通信役務の円滑な提供に向けた通信障害への対策は継続的に検討、実施されてきた。電気通信事業法（昭和 59 年法律第 86 号）において、通信ネットワークの信頼性の確保のために事業用電気通信設備や端末設備につき総務省令で定める技術基準に適合することが義務づけられているほか、政府において、「情報通信ネットワーク安全・信頼性基準」を定め、情報通信ネットワークの安全・信頼性に関する推奨基準（ガイドライン）を規定している。各電気通信事業者においては、これらを踏まえ、自らの電気通信設備に必要なセキュリティ対策を講じるとともに、自らの通信ネットワークに障害を与えるような大量通信を検知した場合やサイバー攻撃を受けている被害者等から攻撃を抑止するよう要請された場合に、攻撃を行う端末の利用者を特定して注意喚起を行い、又は当該端末の通信を遮断する等、通信ネットワークの障害の防止に向けた措置を講じている。

そのような中、昨今は、インターネットに接続される IoT 機器が爆発的な増加を続けており、2020 年までには約 300 億台の IoT 機器がインターネットに接続されるものと見込まれている。このような IoT 機器は、適切なアクセス制限の設定や異常の監視が行われていない、機器の性能上の制約により十分なセキュリティ機能がない等の理由から、セキュリティ面で深刻な脆弱性を抱えたものが多数存在してい

[1] 国立研究開発法人情報通信研究機構（NICT）において観測されたサイバー攻撃に係る通信の回数は、2015 年には約 545 億回だったものが 2016 年には約 1281 億回となっており、約 2.4 倍の増加を示している。

る。一方で、IoT 機器は、企業におけるセンサー機器のように従来のＰＣ等の機器と比較して相当長期間に渡って利用されるものが多く、DDoS 攻撃等のサイバー攻撃に悪用されるリスクが高いものとなっている[2][3]。また、我が国においては、2020 年の東京オリンピック・パラリンピック競技大会を控えているところ、2012 年ロンドン大会では、期間中に延べ２億回のサイバー攻撃が行われ、また、2016 年リオデジャネイロ大会においても、関連する Web サイト等への多くのサイバー攻撃が確認されていることに鑑みれば、我が国においても、2020 年に向けて DDoS 攻撃等の脅威が他国と比較して格段に高まることが想定される。このように、潜在的なインターネットへの脅威は飛躍的に増大し、かつ、変化を続けていることから、インターネットの障害の防止に向けた抜本的な対策の実施は急務となっており、逐次必要な対策を検討し、実施していくことが求められている。

さらに、2017 年８月には、海外事業者の経路情報[4]の誤設定が原因となり、我が国の電気通信事業者の一部の回線や設備に過大な負荷がかかったことから、インターネットに大規模な障害が発生し、インターネットを経由したサービスの利用に支障が生じる等、サイバー攻撃以外の要因でインターネット利用者に大きな影響を与える事態も発生している。インターネットの社会基盤としての重要性に鑑みれば、このような予期せぬ支障が発生した場合においても、障害と混乱発生を最小限に止めるべくあらかじめ対策を講じておく必要がある。

---

2 IoT 機器は、他にも、数が多く管理が行き届きにくい、機能や性能が限られており端末でのセキュリティ対策自体が困難である、ネットワーク側との環境や特性の相互理解が不十分である、開発者が想定していない接続が行われる可能性がある等の特徴を有している上、数を利用して脅威を拡大することが容易であり、DDoS 攻撃等を行う者から見れば悪用しやすい側面を有していると考えられる。

3 NICT による観測によれば、IoT 機器を狙ったサイバー攻撃に係る通信は 2015 年から 2016 年にかけて約 5.8 倍に増加しており、サイバー攻撃一般と比較してもなお急激な増加傾向を示している。

4 インターネットにおいて相手先への到達性を確保するため、接続する事業者間であらかじめ送受信される通信経路の設定に必要な BGP（Border Gateway Protocol）による情報をいう。

２．　基本的な考え方

DDoS 攻撃等の大規模化に伴いセキュリティ上の脅威が深刻化し、関係者ごとの独自の取組だけで対応することが困難となりつつあること、社会全体におけるインターネット利用の拡大や IoT 機器等の攻撃基盤となり得る端末設備が急激に増加し、拡散していることといった状況を踏まえると、IoT 機器等を踏み台とした DDoS 攻撃等によるインターネットの障害を回避し、円滑なインターネット利用環境を確保するためには、インターネット全体として対応していくことが必要となると考えられる。そして、インターネットの円滑な利用環境を確保するためには、インターネットを構成するネットワークの中でも、多数の者による通信基盤として利用されている電気通信事業者の通信ネットワークの保護が強く求められるところ、電気通信事業者の通信ネットワークを保護するためには、電気通信事業者のみならず、端末機器の製造業者、セキュリティベンダ、利用者等の通信ネットワークに関わる者全体が連携しながら対応を進めていくことが極めて重要である。

このような対応の方法については、インターネット利用環境の変化や攻撃手法の変化等に伴い柔軟に検討していくべきところ、DDoS 攻撃等が増加し、その踏み台とされる IoT 機器も爆発的な増加を続けているという現在の環境下においては、発生した DDoS 攻撃等に個別対処するという従来の対策を推進するだけではなく、関係者間で連携しながら DDoS 攻撃等の抑止や予防を図ることが肝要であり、そのような観点から、以下の第１から第３に掲げる対策を併せて講じていくことが必要と考えられる。

第１に、増大するインターネット上の脅威に対処するためには、通信ネットワークを管理している電気通信事業者において、可能なセキュリティ対策を積極的に講じていくことが必要である。現在は、電気通信事業者において、主として DDoS 攻撃等が発生した後の対処に主眼を置いた取組が行われているが、DDoS 攻撃等のインターネットに障害を来す脅威が悪質化、巧妙化し、被害も深刻化していることからすれば、通信ネットワークに障害が発生した後に対処するのでは回復困難な被害が生じるおそれがある。加えて、直接人間がコントロールしていない IoT 機器を踏み台とした攻撃が増加しており、攻撃発生後に端末利用者に連絡を取って速やかな攻撃の抑止を求めることすら困難な例が出てきていること等の事情にも鑑みると、今後は攻撃の予防に向けた対策を強化していく必要がある。

第２に、今後有効な対応を講じていくためには、関係者間で必要な情報を共有し、相互に連携していくことが必要である。インターネット上の多数の IoT 機器を踏み台とした DDoS 攻撃等において、攻撃の通信を行っている端末設備は中小規模の事業者

を含めた多数の電気通信事業者の通信ネットワーク内に散在しているところ、このような状況への対処としては、現在のように電気通信事業者等がそれぞれ独自の対応を行うだけでは不十分であり、関係者間で必要な情報を共有し、相互に連携することが必要である。また、サイバー攻撃に起因するものではないが、経路情報の誤設定などにより、複数の電気通信事業者においてインターネット障害が発生した場合等であっても、障害の状況、原因、対策等を迅速に共有することで障害を最小限度に止め、迅速な復旧を図ることができると考えられることから、電気通信事業者間での迅速かつ的確な連携が求められる。

第３に、ネットワークに接続される IoT 機器を含む端末設備に係るセキュリティ対策が必要である。攻撃の踏み台とされる脆弱な IoT 機器等がインターネットに接続されている限り、DDoS 攻撃等の発生源となるおそれがあることから、インターネットの障害の発生を防止するためには、ネットワークに接続される IoT 機器を含む端末設備についてもセキュリティ対策を実施することが不可欠である。

なお、上記のような各対策を推進するためには、従来以上に通信の秘密やプライバシー等に深く関わる情報を活用する場合もあることから、利用者等の権利利益の保護について十分な配慮を行うことが強く求められる。また、第１から第３までに掲げる対策のほか、利用者等におけるセキュリティ意識の醸成も重要であるから、これらの取組の推進と併せて対策の検討、実施状況の周知等をしながら、国民のセキュリティ意識の更なる向上を図ることも必要である。

３．　電気通信事業者の取り得るDDoS攻撃等への防止措置

(1)　DDoS 攻撃等に利用されることにより情報通信ネットワークに障害を生じさせる可能性の高い端末等の利用者に対する注意喚起

現在、テイクダウンしたC&Cサーバの通信解析等により現にマルウェアに感染していることが明らかとなった端末については、電気通信事業者が接続認証ログや契約者情報等から利用者を特定して注意喚起を行うことで、マルウェア感染の拡大を防止するとともに攻撃の抑止や予防を図っている。

これに加えて、C&Cサーバと通信を行う、存在しないドメイン宛ての通信を頻繁に試みる等の特徴からマルウェアに感染している可能性が高い端末についても同様の措置を講じることができれば、より実効的に攻撃の抑止や予防を図ることができる。また、インターネットの障害を生じさせるようなDDoS攻撃等を繰り返しているマルウェアが感染経路として利用している脆弱性[5]を有する端末を広く対象とすることも一案として考えられる。

ワーキンググループにおけるヒアリングでは、電気通信事業者から、今後の新たな対策として、電気通信事業者において、マルウェアが感染している可能性の高いIoT端末等のIPアドレス情報等を取得した場合に、接続認証ログや契約者情報等を利用して回線契約者を特定し、注意喚起等を行う方法が提示された。このような方策を通じてIoT端末等の利用者による対処等を図ることは、IoT端末等を踏み台とするDDoS攻撃等によるインターネットの障害を防止するために効果的と考えられる。なお、ヒアリングにおいては、C&Cサーバであると疑われる機器に対する通信の遮断についても提示されたところ、このような方策はDDoS攻撃等の予防には有効と考えられる。

他方、このような措置を実施するためには、IoT端末等に関する通信時のIPアドレス情報等と接続認証ログや契約者情報等との照合により注意喚起の対象を特定する必要があることから、通信の秘密やプライバシー情報等との関係で実施できる範囲や方法等を整理した上で実施する必要がある。さらに、C&Cサーバと疑われる機器に対する通信の遮断については、正常な通信をも遮断して別途の問題を引き起こす等の副作用のおそれも否定できないことから、まずは注意喚起を実施し、遮断については副作用の生じない実施方法等の調査、研究等の結果を踏

[5] 例えば、外部から、認証なしに管理者権限で端末を操作できる等の脆弱性が考えられる。

まえて改めて検討を行うべきである。

(2) DDoS 攻撃等を実施している端末や C&C サーバと通信をしている端末等の検知

(1)のような対策を実施するためには、現に DDoS 攻撃等を行っている端末や C&C サーバと通信をしている端末等を特定する必要がある。しかしながら、現在、電気通信事業者において、利用者への注意喚起等の端緒は外部からの情報提供によることが通常となっている。

電気通信事業者において、利用者の通信に係る IP アドレス情報等とレピュテーション情報[6]や特定のマルウェアによる通信の特徴情報との照合により C&C サーバと通信している端末等を検知することが可能となれば、当該端末の利用者に対して早期に注意喚起等を行うことが可能となり、利用者による対処等を通じて当該電気通信事業者の通信ネットワークに対する障害を緩和することが可能となると考えられる。

ワーキンググループにおけるヒアリングでは、電気通信事業者から、今後の新たな対策として、電気通信事業者において、DNS サーバにおける FQDN や中継サーバ等におけるフロー情報[7]をレピュテーション情報と照合し、マルウェア感染者や C&C サーバと通信している利用者の通信を特定することで[8]、現に DDoS 攻撃等を行っている端末や C&C サーバと通信している端末を検知するといった方法が提示された。このような方策を用いて注意喚起を行うべき対象を選定し、その上で(1)の取組につなげることは、インターネットの障害を防止するために効果的と考えられる。

他方、このような措置の実施に当たって、利用者の通信に係る FQDN やフロー情報は通信の秘密やプライバシー情報等に該当するものであり、情報によっては通信の内容をも推知しうるものであるから、その保護の必要性も相当程度大きいものである。したがって、実施できる範囲や方法等について、慎重に検討を行った上で実施していく必要がある。

---

6 FQDN や IP アドレスに関する C&C サーバ該当性を示したリストなどが考えられる。

7 通信パケットの IP アドレス、ポート番号、タイムスタンプ等。

8 C&C サーバとの通信等を特定するための方法としては、DNS サーバにおいて FQDN をレピュテーション情報と照合する方法及び通信パケットのフロー情報を観測して宛先 IP アドレスをレピュテーション情報と照合する方法が提案された。

(3)　マルウェア感染者等の通信を利用したC&Cサーバ等の検知

(2)のような検知を実施するためにはC&Cサーバ等を把握する必要があるところ、現在、電気通信事業者においてC&Cサーバ等を把握するため第三者が作成したレピュテーション情報等を利用している。しかしながら、それらの情報の多くは我が国の電気通信事業者の通信ネットワークの保護に活用することを目的として集められたものではなく、また、C&Cサーバ等の移り変わりも激しいことから、必ずしも十分な網羅性はなく、情報の正確性や信頼性自体もまちまちであるといった課題がある。

このため、マルウェアに感染したIoT端末等によるDDoS攻撃等の被害をできる限り軽減するために電気通信事業者において(2)のような検知等の措置を実施したとしても、必ずしも十分な効果は発揮できない。このような現状に照らせば、電気通信事業者がより多くのデータに基づいた分析を実施し、その結果得られた信頼性、網羅性等の高いレピュテーション情報に基づいて注意喚起等を実施することで、その実効性を更に高めることが必要である。また、電気通信事業者の網内にC&Cサーバが存在することが確認された場合には、契約者等と連携することでC&Cサーバのテイクダウンを実施することも可能となるところ、実施した場合の効果は相当程度高いものである。

ワーキンググループにおけるヒアリングでは、電気通信事業者から、今後の新たな対策として、マルウェアに感染した疑いのある端末の行っている通信に係るFQDNやフロー情報を取得してその通信先を幅広く調査し、C&Cサーバとの通信に関する相関関係の有無、程度の分析[9]等を行うことにより、明らかになっていないC&Cサーバの存在を探知するといった方法が提示された。このような方策を用いてC&Cサーバを探知し、その上で(2)のような取組を行うことは、マルウェアに感染している可能性の高い端末を検知するためには効果的であると考えられる。

他方、このような措置の実施に当たって、利用者の通信に係るFQDNやフロー情報は通信の秘密やプライバシー情報等に該当するものであり、情報によってはその通信内容等も推知しうるものであるから、その保護の必要性も相当程度大きいものである。特に本対策においては、必然的にC&Cサーバとの通信とは無関係な情報についても収集や分析の対象とされることから、検知や分析を実施できる

9 例えば、多数のマルウェアに感染している可能性の高い端末と通信しており、IPアドレスの利用状況等に照らしても、C&Cサーバとしてマルウェアとの通信をしている以外に合理的な説明がつかないアクセス先を探す等の方法が考えられる。

範囲や方法等について、一層慎重に検討を行った上で実施していく必要がある。

(4)　今後の対応の方向性

以上掲げた各対策を実施していくためには、今後、通信の秘密、プライバシー保護等といった諸観点から、具体的な実施方法や、その際に留意すべき事項等について精査していく必要があるところ、これまで、電気通信事業者の通信ネットワークの障害等に関する対処法について通信の秘密等との関係を整理するに当たっては、まず総務省において「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」での有識者の議論を踏まえて対策と法的考え方をとりまとめた上で、電気通信事業者の加盟する民間団体においてとりまとめ結果を踏まえて民間ガイドラインを改訂してきた。このような過去の経緯に照らせば、今回も電気通信事業者によるインターネット利用環境の保護に関する対応の実施に向けて、有識者等からなる同様の研究会を開催し、実施できる範囲、手法や実施する上で通信の秘密やプライバシー保護等との関係で配慮すべき事項等について検討を行い、具体的にどのようにすれば電気通信事業者における対策等を実施することが可能となるか整理するとともに、必要に応じて民間ガイドラインを改訂する等して、対策の実施に向けた体制を整えるべきである。

４．　電気通信事業者その他の関係者における情報共有

（1）　情報共有の必要性

現に行われている DDoS 攻撃等に対しては、DDoS 攻撃等を受けている電気通信事業者による通信遮断のほか、攻撃通信を送信している端末に通信ネットワークを提供している電気通信事業者による攻撃通信の遮断や当該端末の利用者に対する注意喚起が有効である。現在でも、電気通信事業者やその顧客に対する DDoS 攻撃等が行われている場合に、DDoS 攻撃等の被害者等から送信側の電気通信事業者に対して、このような措置を講じることを求めて攻撃通信に係る通信元や送信先の IP アドレス、ポート番号、タイムスタンプ等の通信情報を共有することがある。また、DDoS 攻撃等が収束した後において、ICT-ISAC を通じること等により、DDoS 攻撃等の攻撃の種類や規模、手法等に関する情報が共有されている。

大規模な DDoS 攻撃等が増加し、今後も増加が見込まれるという現状からすれば、攻撃を受けている側の電気通信事業者のみで通信ネットワークの障害に対応することは困難となりつつあり、通信ネットワークの障害を防止する措置を講じることのできる送信側の電気通信事業者に対して迅速に DDoS 攻撃等に係る通信情報を提供し、当該電気通信事業者において防止措置等を講じることの必要性は、今後更に大きくなるものと考えられる。しかしながら、極めて多くの IoT 機器がインターネットに接続され、これらに起因する大規模な DDoS 攻撃等が行われている現状では、被害者等において、各機器が接続している通信ネットワークを管理する電気通信事業者を調査し、個別に情報提供を行うことは非常に困難である。このように、従来の方策によって十分な対応を講じることは難しくなってきており、情報共有の結節点として提供を受けた情報を適切に共有する存在が強く求められている。

また、電気通信事業者において３で示したような予防策を講じていくためには C&C サーバのレピュテーション情報が必要となるところ、現在 ICT-ISAC を通じること等により共有されているインシデント情報や攻撃の規模等に関する情報は、一般的な対策指針を検討するための基礎情報としては有用であるものの、通常は個別の C&C サーバ、攻撃端末等を特定できるものではなく、レピュテーション情報として活用することは難しい。加えて、C&C サーバに関するレピュテーション情報を提供している者は複数存在するものの、その信頼性や網羅性は我が国の電気通信事業者の通信ネットワークの保護という観点から見れば必ずしも十分なものとは限らず、多くの通信情報を分析、評価して信頼性のある情報を作成

する必要がある。各電気通信事業者が個々に情報の収集、分析、共有を行うだけでは十分な成果を上げることができないことを勘案すれば、電気通信事業者が連携して DDoS 攻撃等に関する通信や C&C サーバとの通信等に係る情報を集積した上で、集中的に情報の分析、検証を行い、その結果を広く共有するという対策が求められる。この点においても、電気通信事業者等における情報共有の結節点となって、DDoS 攻撃等の抑止や予防に必要な情報を収集し、適切に共有できるような主体を設けることが必要である。

(2)　情報共有に当たっての課題

まず、DDoS 攻撃等に係る通信情報の迅速な共有という観点からいえば、通信元や送信先の IP アドレス、ポート番号、タイムスタンプ等の通信情報は、通信の秘密として保護されるものであり、通信当事者の同意等がない限り共有を許されていない。しかしながら、個別に情報提供の同意を取らなければ情報共有できず実効的な対策がとれないとすると、今後生じるインターネットの障害に迅速に対応できない場合が想定される上、IoT 機器の爆発的な拡大のもとではそもそも通信当事者が容易に明らかにならない場合も考えられ、個別具体的な同意を取っていくことは困難となる可能性が高い。このような中で効率的な情報共有を推進するためには、電気通信事業者において、通信の秘密に十分に配慮しつつ、電気通信役務の円滑な提供に支障を生じないよう第三者機関を通じた情報共有の枠組の在り方を示すことが重要である。

また、上記のような通信情報は通信の秘密であるのみならず、顧客のプライバシー等にも係るものであり、電気通信事業者にとっても顧客情報等に該当し得るものである。電気通信事業者から情報提供を行う場合については、当該情報がセキュリティ確保のために必要な限度を超えて悪用されないか、またセキュリティが不十分な電気通信事業者から情報流出するおそれがないか等の懸念があるところであり、第三者機関における具体的な情報の収集、分析、共有等の体制や情報の安全管理措置等について検討が必要である。

加えて、第三者機関から情報共有を行う場合において、通信の秘密等に該当するような情報については、情報共有の相手方をインターネットの障害を防止するために真に必要な範囲に限定されるべきであり、また、情報共有を受けた電気通信事業者等において、積極的かつ確実に DDoS 攻撃等の防止措置等を実施していく必要がある。

次に、信頼性、網羅性のあるレピュテーション情報等の作成、共有という観点からいえば、そのような情報を作成するためには、現に生じている DDoS 攻撃等の情報や C&C サーバに関するレピュテーション情報等を収集、分析する必要がある。したがって、情報共有の中核となる第三者機関においては、十分な情報を収集等する能力及び通信の秘密等の情報の取扱いに係る安全管理措置を講じる能力に加え、膨大な情報を分析、検証する能力が求められる。また、当該第三者機関のみでの分析や検証にとどまらず、他の主体が有する専門的な分析、検証能力を活用することも必要と考えられる。

(3)　今後の対応の方向性

情報共有の枠組みの中で通信の秘密に該当する情報を取り扱うことが予定されていることに鑑み、第三者機関を結節点として電気通信事業者の通信ネットワークを保護する目的で行われる情報共有を促進するために、当該第三者機関を法律上位置づけ、通信ネットワークの障害の防止を目的とした、当該第三者機関における通信の秘密を含む情報の収集、分析、共有等の枠組を明確化する必要がある。その上で、当該第三者機関における具体的な情報の収集、分析、共有等の体制、情報の取扱いにおける安全管理措置、情報提供の相手方の範囲、情報共有の実施方法等について、通信の秘密やプライバシー保護等との関係を踏まえて整理する必要がある。

さらに、電気通信事業者の通信ネットワークの保護に一層の実効性を持たせるためには、電気通信事業者の通信ネットワークに接続されている有線電気通信網の設置管理を行っている事業者や、それらの企業にセキュリティサービスを提供しているセキュリティベンダ等において、電気通信事業者と同様に必要な防止措置を講じることが可能な場合もある。そのような者に対しては、電気通信事業者に準じる形で情報共有を図り、インターネットの障害を防止するための対策を講じるよう促すことも考えられることから、電気通信事業者以外の者との連携についても、実効性の確保のため、情報共有の主体、場面、範囲、タイミング等について検討を加えるべきである。

また、情報共有を受けた電気通信事業者における DDoS 攻撃等の防止措置の実施を確保しつつ、情報共有の枠組みに参画しようとする事業者に過度な負担となることを避ける等、多数の電気通信事業者の自主的な参画を図るための方策についても検討し、電気通信事業者が積極的に協力できる情報共有基盤として設計することも必要である。

加えて、制度の整備だけではなく、実際の運用方法についても検討を行うべきである。例えば、情報共有を受けた電気通信事業者等において、共有された情報を検証して検証結果を第三者機関にフィードバックするとともに、当該第三者機関において集約した情報を踏まえて研究機関等に対してより精度の高い分析手法等の開発を委託し、その結果を第三者機関における分析等に適用していく等のサイクルを構築することで、より正確かつ網羅的なレピュテーション情報等が作成でき、将来的な対策の実効性を更に高めることが考えられる。その他にも、より効率的な共有に向けた情報共有の様式や情報共有のタイミングの統一、電気通信事業者及び第三者機関における情報共有の自動化、共有情報のデータベース化等、多くの取組があり得るものであり、実効性確保に向けた取組についても併せて議論すべきである。さらに、特定種類の機器の脆弱性に係る情報等の、広く共有しても利用者等の権利利益の保護の観点から支障がない情報については、機器製造業者等に提供する、国際連携に際して参考情報として提供する等の取組を講じることもインターネットの利用環境の確保に資するものと考えられる。このような点についても、併せて検討すべきである。

以上のような情報共有に加えて、インターネットの障害を防止するためには、より多くの DDoS 攻撃等の送信側となっている電気通信事業者において積極的な取組が行われることが重要となる。したがって、送信側の電気通信事業者において、可能な範囲でインターネットの障害の防止のための自主的な取組が行われるよう促すための方策についても、併せて検討すべきである。

５．　IoT 機器を含む脆弱な端末設備への対策

(1)　端末設備におけるセキュリティ対策の必要性

近年増加傾向にある大規模 DDoS 攻撃においては、まず脆弱な IoT 機器を標的としたマルウェアの感染が拡大し、その後、マルウェアにより乗っ取られた数多くの IoT 機器が悪用され、攻撃対象のサーバに対して同時に大量の通信が送信された結果、インターネットの障害が発生したことが明らかになっている。米国で障害を引き起こしたマルウェア「Mirai」の事例では、60 組の簡単なＩＤ・パスワードの組み合わせでログイン可能な機器が標的となり、約 50 万台に及ぶ IoT 機器が事前に乗っ取られたとされている。また、国内においては、無線 LAN ルータの脆弱性の事例として、当該機器の管理画面がネットワーク側からアクセス可能になっていたため、インターネット接続に関する ID・パスワードが流出し、不正アクセスに利用されるという事態が発生している。いずれの事案も、端末設備に基本的なセキュリティ対策が講じられていれば、その被害を相当程度抑止することができたと考えられる。

このような脆弱性を有する端末設備については、仮に悪意を持つ者に乗っ取られ、DDoS 攻撃等のサイバー攻撃に悪用された場合であっても、必ずしもその利用者に直接の被害が及ぶわけではないことから、当該利用者が対策の必要性を認識しにくく、そのためにセキュリティ対策が進まないという側面がある。このため、利用者に対して IoT 機器のセキュリティ対策に関する啓発活動を行うことに加え、IoT 機器等の端末設備においても、情報通信ネットワークの安全・信頼性を確保する観点から一定のセキュリティ対策が必要と考えられる。

一方、IoT の発展は、我が国の経済社会の活力の向上、国際競争力の確保の観点からも、極めて重要なものである。現在、IoT 機器のセキュリティ対策については、諸外国でも様々な議論が行われていることから、情報通信ネットワークの安全・信頼性を確保するための IoT 機器のセキュリティ対策については、こうした国際動向を踏まえた上で、IoT サービスや機器の普及の阻害とならないように慎重に検討を行う必要がある。

(2)　今後の対応の方向性

IoT 機器のセキュリティ対策はこれまで民間企業の独自の取組みに依存してきたが、2016 年７月に IoT 推進コンソーシアムにおいて「IoT セキュリティガイド

ライン ver 1.0」が策定されたところである。一方、電気通信事業法においては、電気通信事業者の回線設備に障害を与えない、他の利用者に迷惑を及ぼさないといった観点から、当該回線設備に接続される端末設備に関し、接続の技術基準を定めているが、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設けられていない。

こうした状況の中、情報通信ネットワークの安全・信頼性を確保するための IoT 機器のセキュリティ対策については、どのような対策が有効か、技術的な観点から専門的な検討を行っていく必要がある。その際には、諸外国の検討状況や技術の進展の動向等十分に踏まえた上で、通信事業者、IoT 機器メーカ等の関係者から広く意見を聴取し、慎重に検討を進めていくことが求められる。

６．　2017 年８月に我が国で発生した大規模なインターネットの障害[10]に関する検証と今後の対策

(1)　インターネットの障害に係る対策の必要性

2017 年８月に我が国で発生した大規模なインターネットの障害（以下「本障害」という。）については、電気通信事故検証会議[11]において検証結果を取りまとめているところ[12]、本検討会では、検証結果の報告を受け、以下の第１、第２に示すとおり今後必要な対応の方向性を整理した。

第１に、電気通信事業者において、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を図ることが必要である。経路情報は、その到達性を確保するため、電気通信事業者等の間であらかじめ送受信されているが、本障害のようにある者の誤設定により大量かつ詳細な経路情報が送信されてしまうと、他の電気通信事業者等に甚大な影響を及ぼすことが想定される。このような事態の発生を予防し、インターネットの安定性を確保するために、一定の経路情報をルータにおいてフィルターする仕組みや一定量以上の経路情報を受け取らないようリミッターを設定する仕組みは既に存在するところ、電気通信事業者においてこのような設定を行うことは経路情報の受信防止又は送信防止の有効な手段になり得る。

第２に、インターネットの障害に関する情報を電気通信事業者間で十分に共有することが必要と考えられる。インターネットにおける障害については、発生した事象が自社のみで起きているのか、それとも他の電気通信事業者でも同様に起きているのかを把握することが重要であるが、本障害では、複数の電気通信事業者等において同様の事象が発生しているという状況が的確に把握できず、利用者に迅速な説明ができなかった事例があった。電気通信事業者間では、契約関係やネットワーク技術者間の関係を利用した情報交換がされているほか、ICT-ISAC が JPNIC と連携

---

10 2017 年８月、海外事業者Ｘが本来配信予定のなかった大量かつ詳細な経路情報を海外事業者Ｙに誤配信したことを契機に、①当該経路情報に含まれていた国内電気通信事業者Ａ宛の経路情報により、日本国内での通信も含め、Ａ宛の通信が海外のＸ及びＹを経由する設定となったことからＡ宛の通信がつながりにくい状態となるとともに、②Ｙから当該経路情報を受信した国内電気通信事業者Ｂにおいて、同社の法人向けインターネット接続サービス用のルータが不安定となり、当該ルータを利用する法人が提供するサービスにインターネット経由でアクセスしづらい状態となり、長時間にわたり大規模な通信遅延が生じた事象。

11 電気通信事故に係る外部の専門的知見を活用した検証を通じ、電気通信事故の発生を防止することを目的とした会議。

12 本障害の検証結果は以下の総務省ウェブページに掲載されている。
http://www.soumu.go.jp/main_sosiki/kenkyu/tsuushin_jiko_kenshou/index.html

し、「経路奉行[13]」を運用している等、一定の情報共有がなされているが、インターネットの障害を迅速かつ的確に把握し、早期に対応策を実施するとともに、できるだけ早い段階で利用者に周知するという観点から、さらに緊密な連携が求められる。また、総務省が、電気通信事業者間の情報共有体制と連携することで、より効果的な情報共有と的確な対応策の検討が可能になるとともに、利用者周知の観点からも、総務省が情報共有の結節点となることも有効と考えられる。

(2) 今後の対策の方向性

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を図るためのフィルターやリミッターの設定といった仕組み自体は既に存在しているが、広く電気通信事業者に、それぞれのネットワーク構成や運用の考え方に合わせて柔軟かつ適切に対応することを求めるためには、例えば、「情報通信ネットワーク安全・信頼性基準」にルータのフィルター設定について規定する等、適切な制度的対応を検討する必要がある。

また、総務省が本障害のような事象を迅速かつ的確に把握し、情報共有の結節点となるためには、これまで総務省への報告対象ではなかった[14]インターネットの障害についても、サイバー攻撃に起因するものも含めて報告対象とする等、総務省への報告の在り方を含め、障害に関する情報共有体制の整備を検討する必要がある。

13 ICT-ISAC の会員である電気通信事業者から収集した経路情報を元に、通信ネットワークの運用に支障をきたす異常な経路情報の発生を検出するシステム。

14 電気通信事業法及び関係省令に規定する電気通信事故報告制度により、重大な事故が発生した場合はその理由又は原因とともに速やかに報告することが義務づけられているが、本障害は、電気通信事業法、関係省令及び関係ガイドラインが定める電気通信事業法上の重大事故に該当せず、電気通信事業法上の事故としての報告対象ではない。

「円滑なインターネット利用環境の確保に関する検討会」

構成員名簿

（敬称略・五十音順）

	遠藤　信博（えんどう　のぶひろ）	日本電気株式会社　代表取締役会長
（座長代理）	佐伯　仁志（さえき　ひとし）	東京大学大学院　法学政治学研究科　教授
（座長）	佐々木良一（ささきりょういち）	東京電機大学　未来科学部　教授
	宍戸　常寿（ししど　じょうじ）	東京大学大学院　法学政治学研究科　教授
	長田　三紀（ながた　みき）	全国地域婦人団体連絡協議会　事務局長
	藤本　正代（ふじもと　まさよ）	富士ゼロックス株式会社　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（もり　りょうじ）	英知法律事務所　弁護士
	吉岡　克成（よしおか　かつなり）	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

「円滑なインターネット利用環境の確保に関する検討会　ワーキンググループ」

構成員名簿

（敬称略・五十音順）

	木村（きむら）　孝（たかし）	（一社）日本インターネットプロバイダー協会 会長補佐、行政法律部会長
	小山（こやま）　覚（さとる）	（一社）ICT-ISAC ステアリング・コミッティ　副運営委員長
（主査）	宍戸（ししど）　常寿（じょうじ）	東京大学大学院　法学政治学研究科　教授
	竹内（たけうち）　一夫（かずお）	（一社）情報通信ネットワーク産業協会 通信機器セキュリティ分科会　主査代理
	田中（たなか）　俊昭（としあき）	（一社）電気通信事業者協会
	土田（つちだ）　充（みつる）	（一社）情報通信ネットワーク産業協会 企画推進部 部長
	堀内（ほりうち）　浩規（ひろのり）	（一社）日本ケーブルテレビ連盟 理事
	松本（まつもと）　勝之（かつゆき）	（一社）電気通信事業者協会
	丸橋（まるばし）　透（とおる）	（一社）テレコムサービス協会 サービス倫理委員会 委員長
	森（もり）　亮二（りょうじ）	英知法律事務所　弁護士
（主査代理）	吉岡（よしおか）　克成（かつなり）	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

検討経過

会合	開催日	主な議題
検討会第１回	平成 29 年 10 月 26 日	○ 電気通信事業におけるサイバー攻撃等への対策の現状と課題 ○ 自由討議　等
ＷＧ第１回	平成 29 年 11 月 9 日	○ 事業者ヒアリング及び意見交換 ・株式会社インターネットイニシアティブ ・ＫＤＤＩ株式会社 ・ＮＲＩセキュアテクノロジーズ株式会社
ＷＧ第２回	平成 29 年 11 月 15 日	○ 事業者ヒアリング及び意見交換 ・一般社団法人ＩＣＴ－ＩＳＡＣ ・日本電信電話株式会社 ・ソフトバンク株式会社 ・一般社団法人情報通信ネットワーク産業協会 ○ 自由討議
ＷＧ第３回	平成 29 年 12 月 6 日	○「対応の方向性」（案） ○ 電気通信事故検証会議報告
ＷＧ第４回	平成 29 年 12 月 13 日	○「対応の方向性」（案）
検討会第２回	平成 29 年 12 月 22 日	○「対応の方向性」（案）の取りまとめ【予定】

参考資料

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

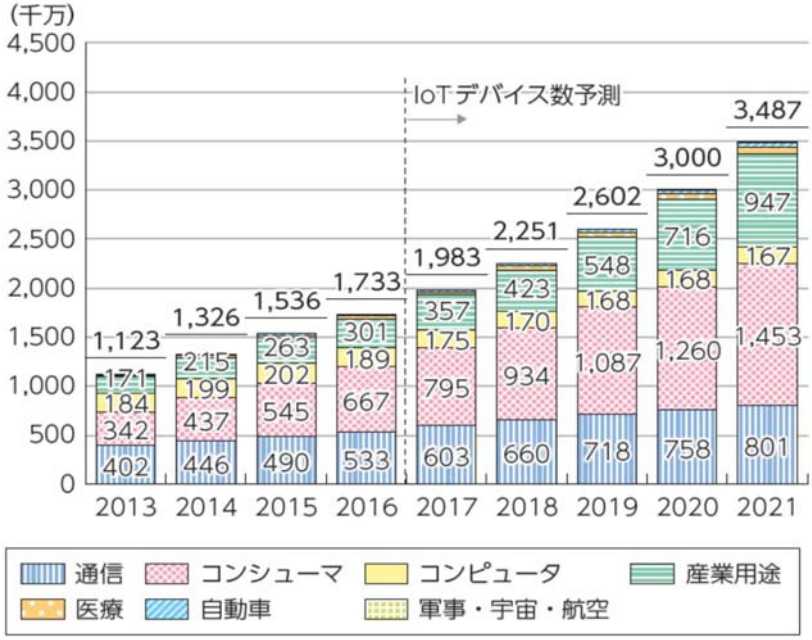
2016年9月13日	【Akamai（米国）】 ・サイバーセキュリティ専門ジャーナリストのBrian Krebs氏が運営するブログに対し、Mirai※に感染した約18万台のIoT機器から約620Gbpsに及ぶDDoS攻撃が発生 ・同氏に無償でホスティングサービス及びDDoS攻撃緩和サービスを提供していたAkamaiは、サーバーへの負荷に耐えきれず、有料顧客へのサービスを優先するため同氏に対するサービスを停止
2016年9月22日	【OVH（フランス）】 ・自社保有サーバに対し、Mirai※に感染したとされる約14万台以上のIoT機器から、最大1.5Tbpsとなる世界最大規模のDDoS攻撃が発生 ・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

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。

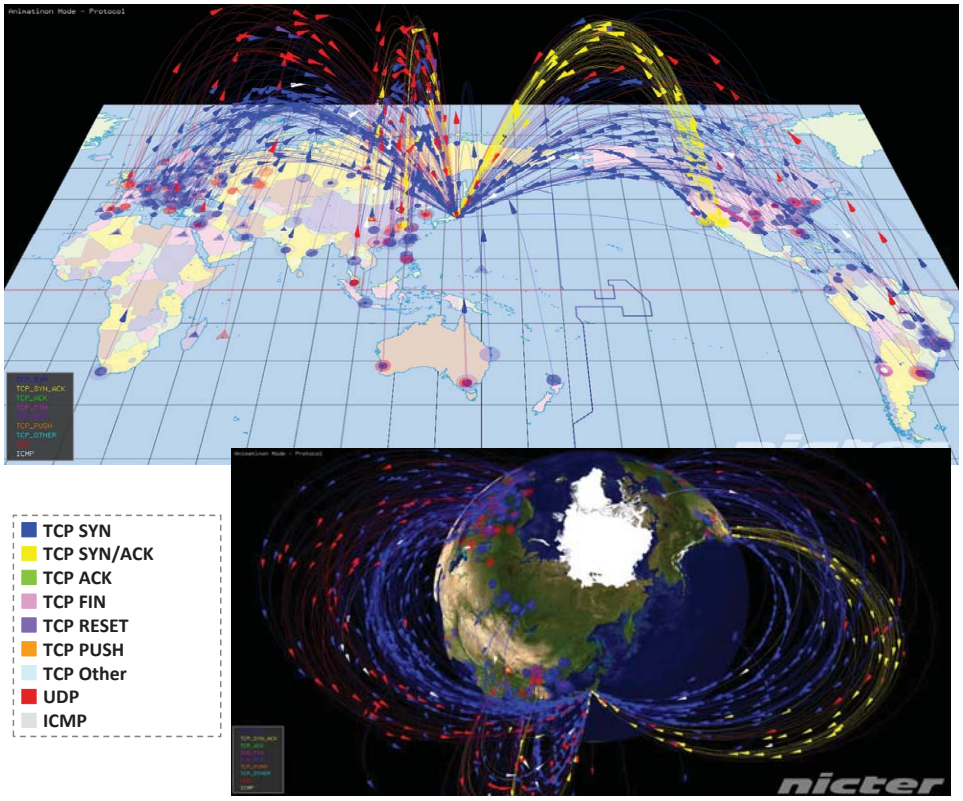


(出典)IHS Technology

※ 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)。

IoT機器を狙った攻撃が急増（NICTERによる観測）

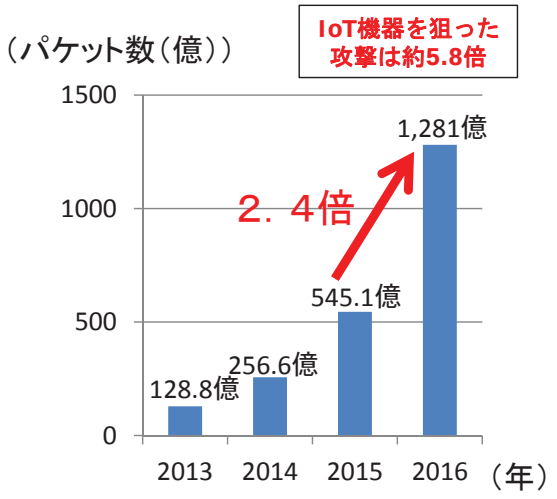
➢ 国立研究開発法人 情報通信研究機構（NICT）では、未使用のIPアドレス30万個（ダークネット）を活用し、グローバルにサイバー攻撃の状況を観測



・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

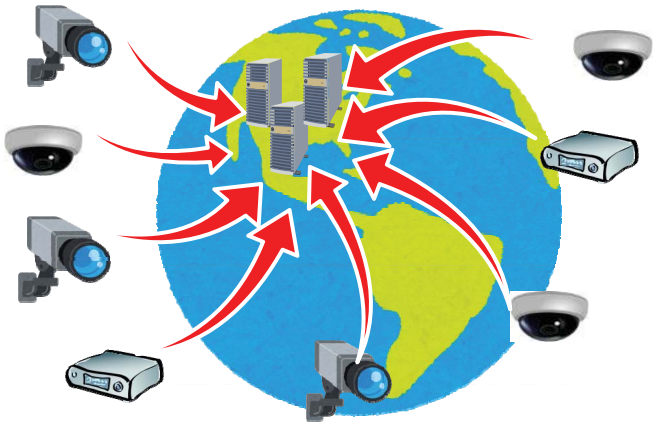


IoTによる大規模DDoS攻撃について

➢ 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

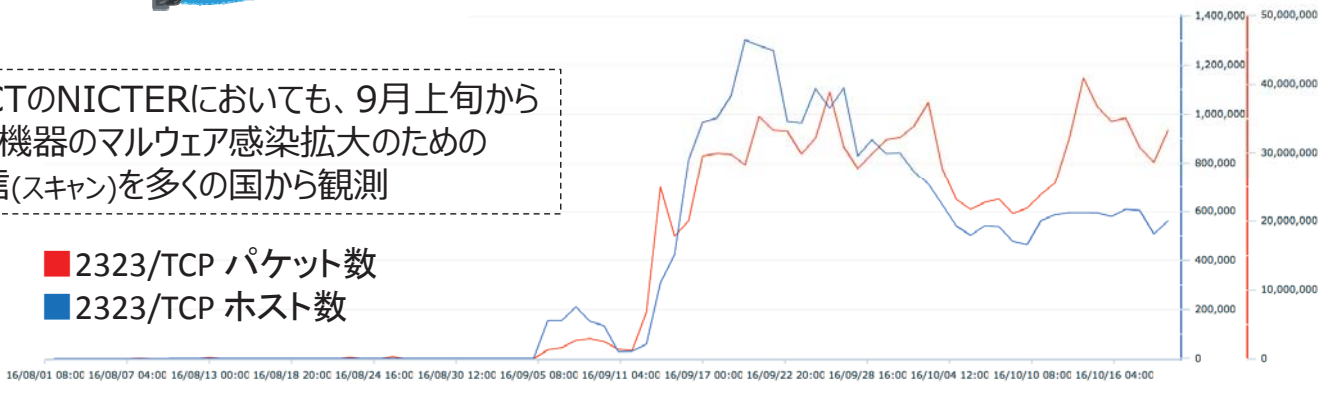


✓ マルウェアに感染した10万台を超えるIoT機器からDyn社のシステムに対し大量の通信が発生

✓ 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



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）

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

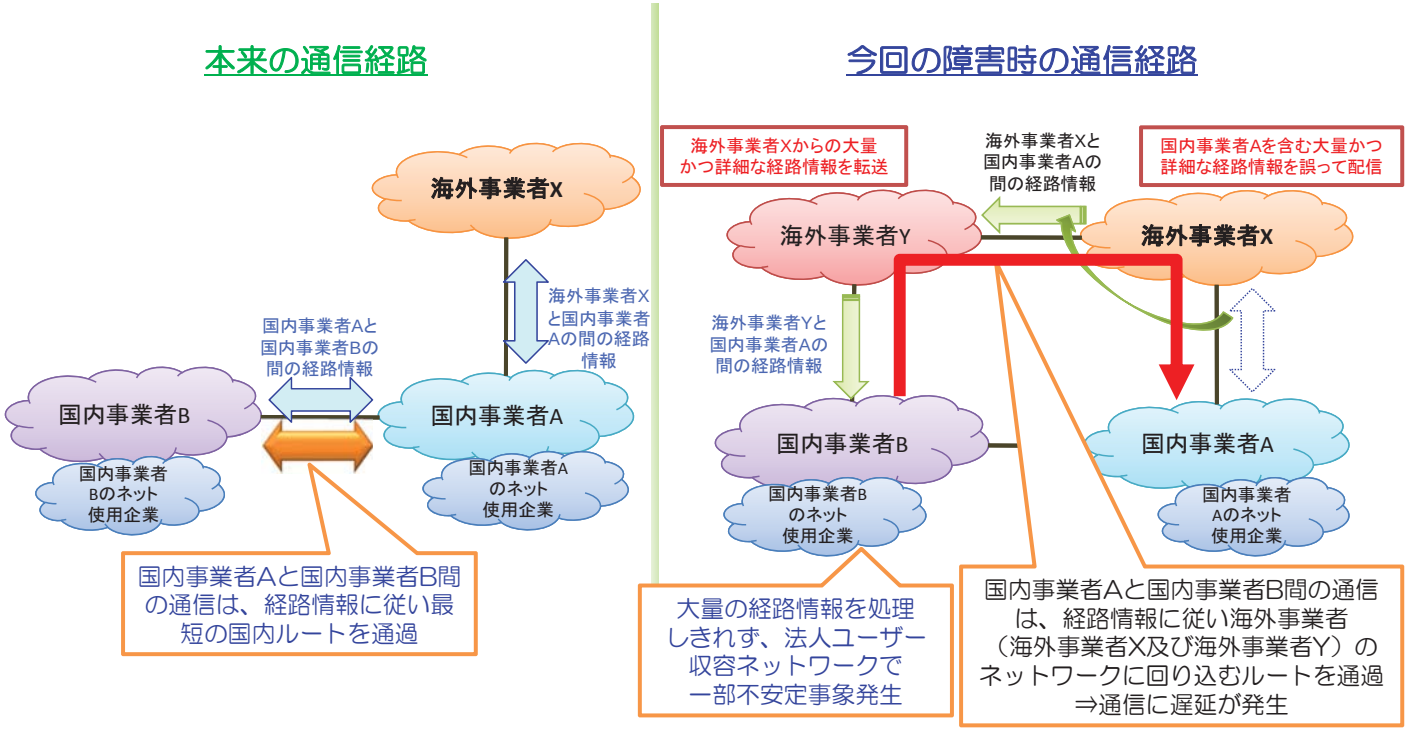
○ 2016年　リオデジャネイロ大会

- 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/

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）の一部の回線や設備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



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。

通信の秘密の保護について

■　「通信の秘密」は、通信が人間の社会生活にとって必要不可欠なコミュニケーション手段であることから、表現の自由の保障を実効あらしめるとともに、個人の私生活の自由を保護し、個人生活の安寧を保障する（プライバシーの保護）ため、憲法上の基本的人権の一つとして、憲法第21条第2項において保障されているもの。

■　日本国憲法の規定を受け、電気通信事業法第4条において、罰則をもって「通信の秘密」を保護する規定が定められており、電気通信事業法上「通信の秘密」は厳格に保護されている。

通信の秘密の範囲

通信の秘密とは、①個別の通信に係る通信内容のほか、②個別の通信に係る通信の日時、場所、通信当事者の氏名、住所、電話番号等の当事者の識別符号、通信回数等これらの事項を知られることによって通信の存否や意味内容を推知されるような事項全てを含む。

※　東京地裁判決H14.4.30は、「電気通信事業法第104条の「通信の秘密」には、通信の内容のほか、通信当事者の住所・氏名・電話番号、発受信場所、通信の日時・時間・回数なども含まれると解する。」と判示している。

通信の秘密の侵害

通信の秘密を侵害する行為は、以下の３類型に大別されている。なお、通信の秘密の保存自体も侵害に該当し得る。

○　**知得**＝「積極的に通信の秘密を知ろうとする意思のもとで知り得る状態に置くこと」
○　**窃用**＝「発信者又は受信者の意思に反して利用すること」
○　**漏えい**＝「他人が知り得る状態に置くこと」

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）

通信の秘密の侵害に当たらない場合について

通信当事者の有効な同意がある場合

○ 通信の秘密の侵害について通信当事者の有効な同意がある場合は、通信の秘密の侵害に当たらない。

通信当事者が侵害される通信の秘密について個別具体的かつ明確に同意した場合でなければ原則として有効な同意があるとはいえない。

ただし、通常の利用者であれば承諾することが想定される場合であって、利用者が随時不利益なく同意を撤回できる（オプトアウト）、それらが十分に周知されるなどしている場合は、約款等による包括的な同意でも有効な同意といえる場合がある。

違法性阻却事由がある場合

○ 通信当事者の同意がない場合であっても、下記のような違法性阻却事由がある場合には、通信の秘密の侵害が許容される。

(1) 法令行為に該当する場合

電気通信事業者として、刑事訴訟法第100条に基づく通信履歴の差押えなど、他の法令の規定に基づき正当に行う行為は、法令に基づく行為として違法性が阻却される。

(2) 正当業務行為に該当する場合

電気通信事業者として電気通信役務の提供等の業務を遂行するために必要であって、①目的の正当性、②行為の必要性、③手段の相当性の要件を満たす行為については、正当業務行為として違法性が阻却される。

(3) 正当防衛、緊急避難に該当する場合

通信施設に対する現に生じている攻撃に対応したり人の生命身体に対する危険を避けたりするために通信の秘密を侵す場合等、正当防衛の要件（①急迫不正の侵害、②自己又は他人の権利を防衛するため、③やむを得ずした行為）又は緊急避難の要件（①現在の危難の存在、②法益の権衡、③行為の補充性）を満たす行為については、違法性が阻却される。

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

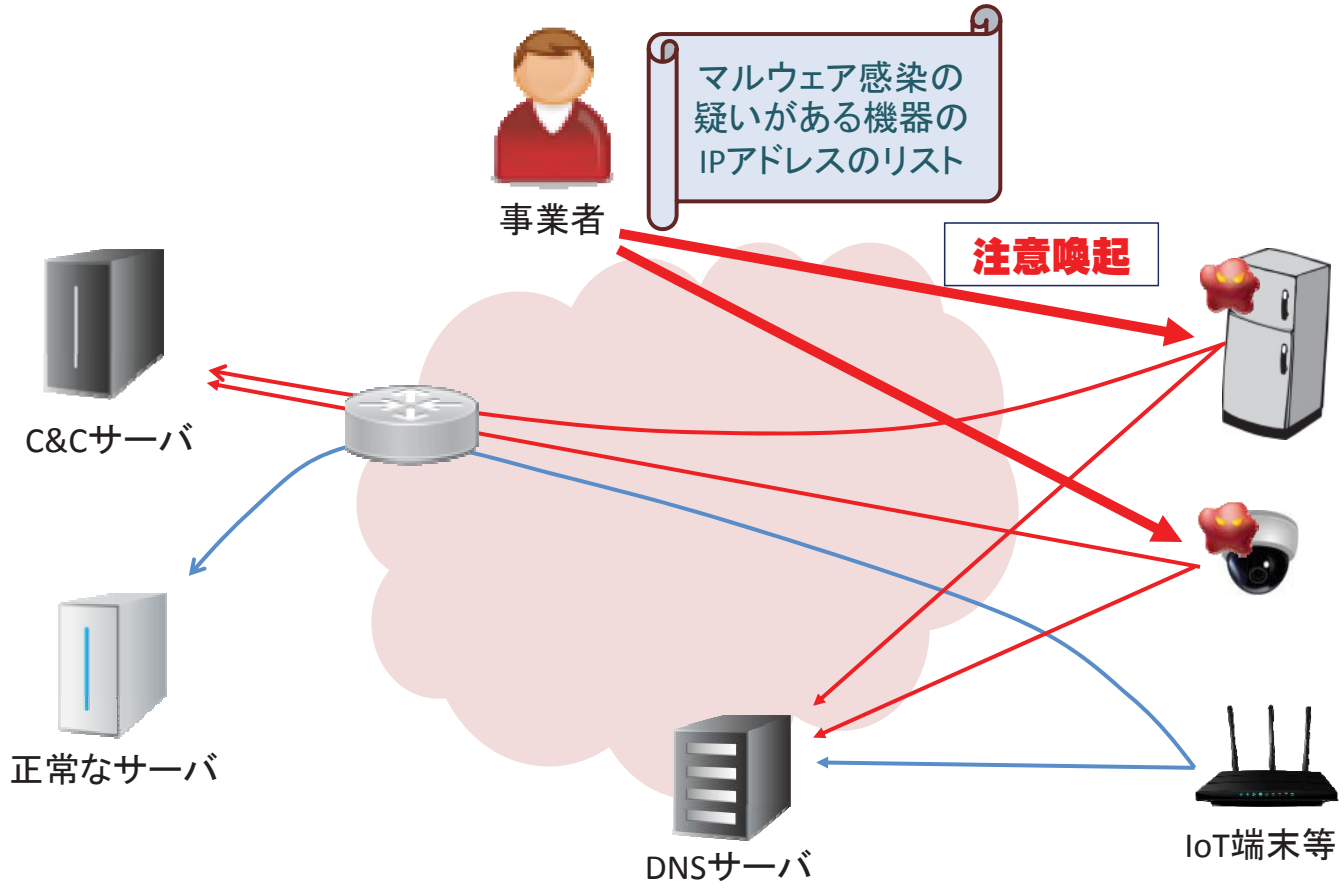
ガイドライン

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＞

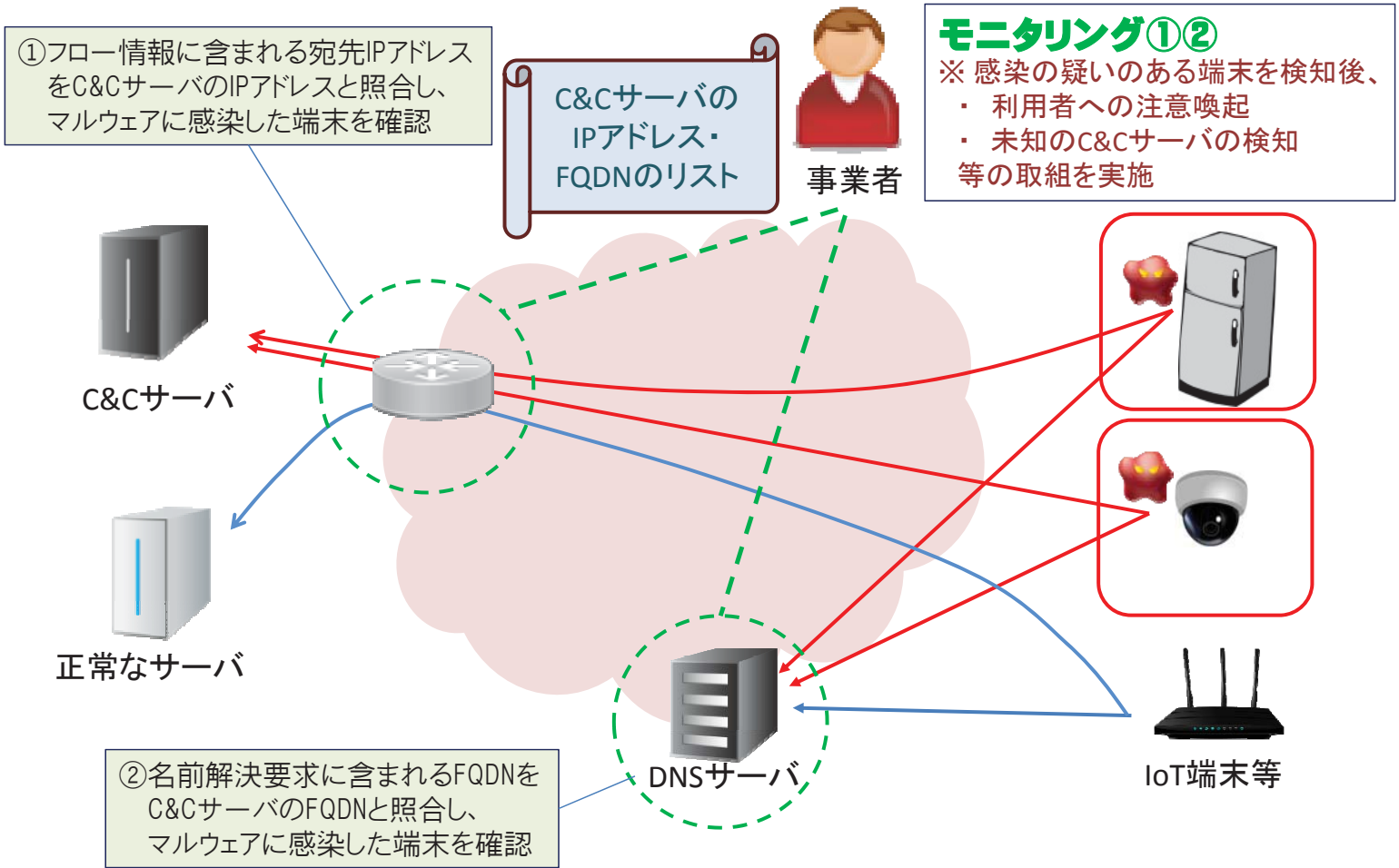
ソフトウェアの品質検証、事故状況等の情報公開、ネットワーク運用管理（運用基準の設定、委託保守管理）等
※サイバーセキュリティに係る事項については、ファイアウォールを設置して適切な設定を行うこと等について規定

電気通信事業者による対策案：マルウェア感染の疑いのある端末利用者への注意喚起



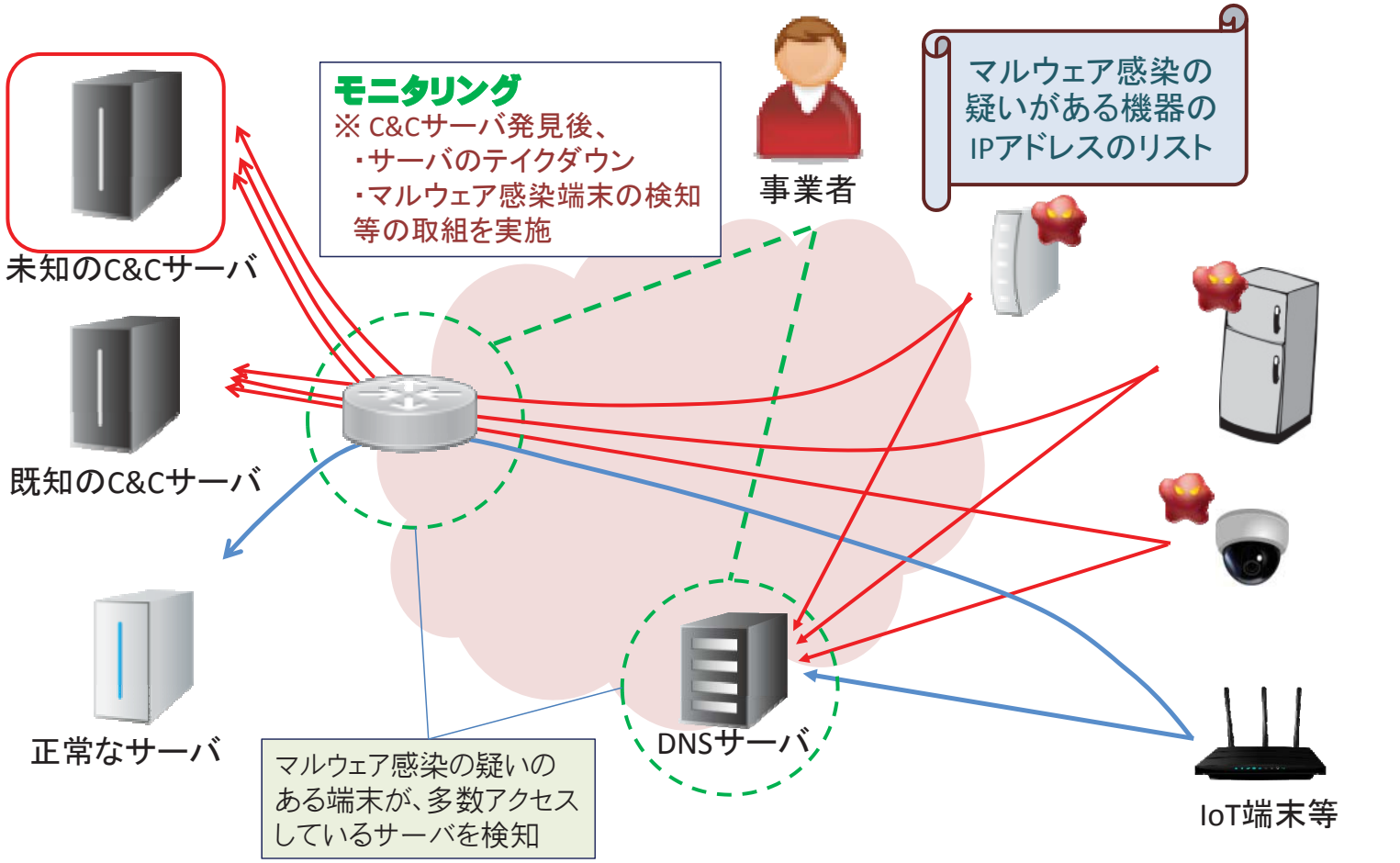
（検討会WGにおける事業者等からのヒアリング結果を基に作成）

電気通信事業者による対策案：マルウェア感染の疑いのある端末の検知等



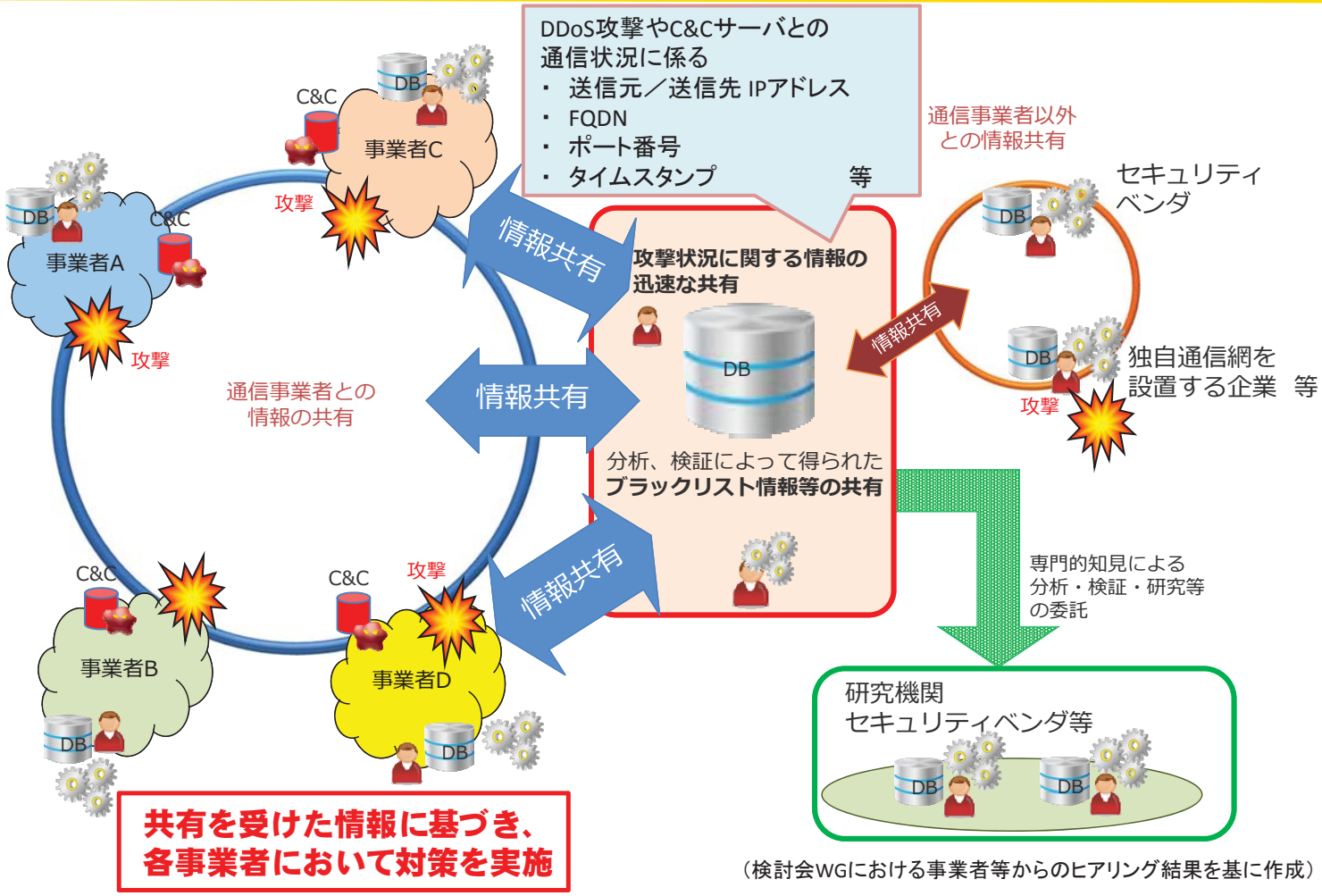
（検討会WGにおける事業者等からのヒアリング結果を基に作成）

電気通信事業者による対策案：未知のC&Cサーバの検知等



（検討会WGにおける事業者等からのヒアリング結果を基に作成）

情報共有制度の概要



（検討会WGにおける事業者等からのヒアリング結果を基に作成）