別紙

我が国のサイバーセキュリティ強化に向け
速やかに取り組むべき事項
[緊急提言]

2020 年（令和２年）１月 28 日

サイバーセキュリティタスクフォース

目次

１．本提言の位置づけについて

あらゆるものがインターネットに接続されるIoT/AI時代が到来し、それらに対するサイバーセキュリティの確保は、安心安全な国民生活や、社会経済活動確保の観点から極めて重要な課題となっている。

本タスクフォースでは、上記のようなサイバーセキュリティの重要性を踏まえ、IoT/AI 時代を見据えたサイバーセキュリティに係る課題を整理しつつ、講ずべき対策や既存の取組の改善など幅広い観点から検討を行い、必要な方策を推進することを目的として、議論を実施してきた。

その結果、2017年（平成29年）10月に、IoTに関するセキュリティ対策の総合的な推進に向けて取り組むべき課題を整理した「IoT セキュリティ総合対策」を策定・公表し、その後、当該総合対策についての進捗状況と今後の取組をまとめたプログレスレポートを公表（平成 30 年７月、令和元年５月）した。また、「IoTセキュリティ総合対策」 の公表後、5Gのサービスの開始や、データ管理・流通の重要性やサプライチェーンリスクへの対応などの必要性が増大していること等を踏まえ、IoT・5G時代にふさわしいサイバーセキュリティ対策の在り方について検討し、2019年（令和元年）８月に新たに「IoT・5Gセキュリティ総合対策」を策定・公表した。

その上で、2020 年東京オリンピック・パラリンピック競技大会（以下「2020年東京大会」という。）を控える中、取り組むべき施策の総点検を行うとともに、新たな課題への対応や施策展開の加速化を図るため、本タスクフォースの構成員を拡充し、その後もサイバーセキュリティに関する課題や必要な方策について議論を継続してきたところである。本タスクフォースでは、短期的な取組と中長期的な取組に分けて議論を行っているが、2020 年東京大会まで間に合うものは速やかに実行するべきであり、具体的なアクションについて、早期に実施するためのとりまとめを行うこととした。

本提言は、本タスクフォースにおける「IoT・5Gセキュリティ総合対策」の策定・公表後の議論を踏まえ、本年７月より開催される2020年東京大会に向けた対処として早急に取り組むべき事項を整理したものである。

本提言を受け、総務省が関係主体と連携し、必要な措置を早急に講ずることを期待する。

２．具体的施策

（１）IoT 機器のセキュリティ対策の拡充

ア　背景と課題

① IoT 機器の脆弱性については、製造業者における IoT 機器のセキュリティ・バイ・デザインの考え方を十分に浸透させることが重要である。この点で、強制規格としての技術基準の策定[1]や、民間の任意の認証（Certification）制度の立ち上げが既になされており、今後はこれらの対策がとられた機器の市場への展開の促進が重要となる。

② 他方、これらの対策は実効性を発揮するまでに一定程度の時間を有することから、まずは既に設置されている IoT 機器に関する脆弱性等の有無の調査を実施し、必要な対応を速やかに実施する必要がある。

③ この点、総務省では、国立研究開発法人情報通信研究機構（以下「NICT」という。）がインターネット上の IoT 機器に容易に推測されるパスワードを入力することなどにより、サイバー攻撃に悪用されるおそれのあるものを調査し、インターネットサービスプロバイダ（以下「ISP」という。）を通じて当該 IoT 機器の利用者への注意喚起を行うプロジェクト「NOTICE」と、既にマルウェアに感染している IoT 機器を NICT の「NICTER」プロジェクトで得られた情報を基に特定し、ISP を通じて利用者へ注意喚起を行う取組の２つの取組を実施している。

④ NOTICE 及び NICTER に係る注意喚起は、ISP の協力により実施しているものであり、2019 年（令和元年）末時点で 41 の ISP が参加しているが、より多くの ISP の協力を得て取組を拡大する必要がある。加えて、注意喚起は各 ISP において電子メールや郵送等により実施しているところ、複数回注意喚起を受けても対応の見られない利用者もいることから、より効果的な注意喚

[1] IoT 機器に関する基本的なセキュリティ対策については、電気通信事業法（昭和 59 年法律第 86 号）の枠組みにおいて端末設備等規則（昭和 60 年郵政省令第 31 号）を改正し、強制規格としての技術基準が策定されている（2019 年（平成 31 年）３月１日公布、2020（令和２年）年４月１日施行）。また、当該改正後の同規則の各規定等に係る端末機器の基準認証に関する運用について明確化を図る観点から、総務省において 2019 年（平成 31 年）４月に「電気通信事業法に基づく端末機器の基準認証に関するガイドライン（第１版）」を策定・公表している。なお、当該技術基準については、インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、（ⅰ）アクセス制御機能、（ⅱ）アクセス制御の際に使用する ID/パスワードの適切な設定を促す等の機能、（ⅲ）ファームウェアの更新機能、又は（ⅰ）～（ⅲ）と同等以上の機能を具備することを求めている。なお、PC やスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本対策の対象外とされている。

起手法について検討を行う必要がある。

⑤ 一方で、IoT 機器については、近年、公知、未知のネットワーク探索システムの活動が活発化し、IoT 機器の所在やセキュリティの状態が全世界的に把握されつつある。また、探索システムの悪用について詳細は不明であるが、探索システムの検索結果等が不要なアクセスを誘発するケースが存在していることが確認されている。

⑥ また、広域スキャン等による IoT 機器の調査結果によると、国内の重要施設の遠隔監視等を行うシステムに使用される IoT 機器について、利用事業者名や重要な機器の制御等を行うものであることが当該機器の管理画面のトップページに表示されているものが一定数存在することが確認されている。ハニーポットにおける観測結果によれば、このようなシステム・機器は、攻撃者からの積極的な攻撃を受けやすい状態にある。

イ　とるべき対策

① 上述のような背景と課題を踏まえると、脆弱な状態にあるIoT機器を検知し、当該機器の利用者に対策をとってもらうため、具体的には次のような取組が必要である。

② NOTICEによる注意喚起及びNICTER情報による注意喚起の取組については、注意喚起に協力いただけるISPの増加を図るとともに、各ISPにおいて架電や往訪も含めた有効な注意喚起手法について共有を行い、脆弱な状態にあるIoT機器への対策を進めていくことが必要である。

③ また、国内の重要施設に設置されているIoT機器については、利用事業者名や用途がインターネット上から容易に判別できるなどにより攻撃を受けやすい状態に置かれていないかどうか速やかに調査を行い、問題のある機器の所有者・運用者等に対して注意喚起や対策の実施を促していく必要がある。

（２）地方公共団体向け実践的サイバー防御演習（CYDER）の繰り上げ実施等

ア　背景と課題

① サイバーセキュリティ人材の育成は重要な政策課題とされており、組織における経営層、戦略マネジメント層、実務者層・技術者層といった各層の人材の育成・確保が重要である。

② 総務省においては、特に実務者層・技術者層及び若年層を対象に、これまで

NICTの「ナショナルサイバートレーニングセンター」において、(ⅰ)国の行政機関等、地方公共団体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（CYDER）、(ⅱ)2020年東京大会関連組織のセキュリティ担当者等を対象とした人材育成（サイバーコロッセオ）、(ⅲ)若手セキュリティイノベーターの育成（SecHack365）の取組がなされてきた。

③ この中で、CYDERは、組織のネットワーク環境を模した大規模LAN環境下で、実機の操作を伴ってサイバー攻撃によるインシデントの検知から対応、報告、回復までの一連の対処方法を体験することができるものである。各組織の情報システム担当者やCSIRT要員がCYDERを受講することで、実インシデント発生時の作業内容を予め理解・把握し、円滑に対応を行うことが可能となる。

④ 国の行政機関等についてはCYDERの未受講数が過去３年間で急速に減少し、ほぼ全ての機関が受講しているところである。一方、国と同様に個人情報をはじめとする重要な情報を取り扱う地方公共団体については、開催日程の同一地域内での分散化や、県庁等所在地以外での演習の実施といった受講しやすい環境を整える取組を行ってきたものの、依然として半数近くの地方公共団体が未受講の状況である。

イ　とるべき対策

① 2020年東京大会の開催に向け、社会全体としてサイバーセキュリティ対応力を強化することは急務であり、実際のインシデント発生時に対応を行う情報システム担当者等に対する人材育成の取組は特に重要である。この観点からCYDERによる人材育成を引き続き実施するとともに、依然として半数近くが未受講である地方公共団体の受講促進の取組を早急に実施する必要がある。

② 具体的には、都道府県ごとにCYDER未受講の地方公共団体を対象とした受講計画を作成した上で、当該地方公共団体を念頭においた集中的な受講機会を2020年度第１四半期に設けることが望ましい。その際には、地方公共団体に加えて、人材育成に課題を抱える地域の関係者においても可能な限り対象を広げていくことが求められる。

③ また、地理的な原因により未受講である地方公共団体について、開催場所の変更による対応だけでは限界があることから、オンラインでの受講を可能とする演習実施環境の整備が有効である。

（３）サイバーセキュリティに関する情報共有体制の強化

ア　背景と課題

① サイバー攻撃に関する情報共有については、官民で様々な取組がなされている。この中で、民間の取組の１つとしてISAC（Information Sharing and Analysis Center）が挙げられるが、ISACは、サイバー攻撃や事故への事前の対処、及び、障害発生時の事案対処や復旧に関する情報などについて事業者間で共有することを目的とした組織である。

② ISACはリスクマネジメントの活動の一環であり、協業事業者、パートナー、競争事業者などの情報連携により、サイバー攻撃からの防御コストの低減に寄与する民間の取組であり、サイバーセキュリティを協調領域と捉えた上で、組織間、業界内、業界間の情報共有を推進することで、サイバーセキュリティの確保につながることが期待されている。

③ この点、国内では2002年（平成14年）のTelecom ISACの設立を皮切りに、業界ごとに様々なISACが立ち上がり始めている[2]。今後、ISACの立ち上げが様々な分野で進むことによって、各分野のサイバーセキュリティの質が向上するとともに、ISAC同士の連携が進むことで、例えば各ISACが有する情報のうち、類似した事例や国・業界横断的な対処方法を共有するなど、業種ごとの共通課題を踏まえた情報共有の進展による対応能力の高度化が期待される。

④ 一方で、業態によっては、ISACを立ち上げるための人材やノウハウが不足している場合もあることが想定されるため、先行して取組を進めてきた通信分野のノウハウの展開が期待される。

イ　とるべき対策

① サイバー攻撃については、原因究明に一定の期間を要する場合もあるが、個人情報などの流出が疑われる時点で、影響を受ける主体との関係なども踏まえつつ、速やかに情報の公表を検討することが望ましい。また、類似の被害の拡大を防ぐ観点から、インシデントに関する情報の共有を速やかに行うことが求められる。

② その上で、サイバーセキュリティに関する情報共有体制については、2020年東京大会の円滑な実施において極めて重要であり、大会後においても同様で

[2] 現在、通信分野の Telecom-ISAC が放送分野などにも広がる形で発展的に改組した ICT-ISAC をはじめ、金融 ISAC、電力 ISAC、J-Auto ISAC（自動車）、Software ISAC などが立ち上がっている。

ある。この点で、官民の情報共有体制については、「サイバーセキュリティ協議会」、「重要インフラの情報セキュリティ対策に係る第４次行動計画」、「サイバーセキュリティ対処調整センター」などの枠組みが既に存在している。NISC等と連携したこれらの枠組みの着実な実施を念頭に置きつつも、我が国の様々な産業のサイバー攻撃への対応力を強化するため、関係機関と協力しつつ、通信業界において先行的に始まったISACの知見やノウハウの展開を通じて他の重要インフラ分野等でのISACの立ち上げを促進するとともに、国際間を含むISAC間の連携を促進する必要がある。

（４）公衆無線 LAN のセキュリティ対策

ア　背景と課題

① 公衆無線LANサービスの利用者数は、動画配信サービスの拡大や訪日外国人利用者の利用ニーズの増大などにより、年々増加しており、2020年東京大会の開催期間中においても、そのセキュリティの確保は重要な課題である。

② この点、公衆無線LANサービスについては、一般的に（ⅰ）端末－アクセスポイント（AP）間が暗号化されていない場合、（ⅱ）なりすましアクセスポイント（詐称されたアクセスポイント）を利用してしまう場合などで、通信を盗聴されるリスクが存在している。

③ 公衆無線LANサービスの利用者が、リスクを適切に認知した上でサービスを利用できるよう、公衆無線LANのセキュリティ対策の状況や自ら講じるべきセキュリティ対策を理解してもらうことが重要な課題となっている。

イ　とるべき対策

① 公衆無線LANサービスの利用に当たっては、訪日外国人の利用も念頭に置きつつ、提供者・利用者双方におけるセキュリティ対策を進めていく必要がある。

② セキュリティを強化したWPA3-Personal、WPA3-Enterprise、Enhanced Open等の新しい規格が策定されていることを踏まえ、公衆無線LANのセキュリティ対策の状況や利用者が講じるべきセキュリティ対策について、提供者が提供サービスの状況について利用者に適切に伝えるようにするとともに、利用者がそのような情報を適切に判断できるよう、リテラシー強化のための周知啓発を強化することが必要である。例えば、通信経路が暗号化されていない状況でID・パスワードを入力しないといった具体的な利用方法を伝えていく

ことや、TLS（https）やVPNの利用といった無線LANより上位のレイヤーにおけるセキュリティ対策についても周知啓発を進めていくことが必要である。

③ こうした内容を踏まえ、年度内を目途にガイドラインを改定し、2020東京大会に向けて多くの利用が見込まれるホテル・観光関係機関や病院、学校の情報化が実施されることから教育機関等には特に周知を実施していくことが必要である。

（５）制度的枠組みの改善

ア　背景と課題

① サイバーセキュリティ対策の実効性の確保のためには、サイバーセキュリティ対策などを法令やガイドライン、基準などに位置づけるとともに、昨今のサイバー攻撃やインシデント等の発生の状況を踏まえ、必要に応じてこれらの制度的な枠組みを定期的に見直ししていくことが重要である。

② この点、電気通信分野においては、サイバーセキュリティ対策の実効性を確保するため、電気通信事業法（昭和59年法律第86号。以下同じ。）において、（ⅰ）電気通信回線設備を設置する電気通信事業者、（ⅱ）基礎的電気通信役務を提供する電気通信事業者及び（ⅲ）有料かつ利用者100万以上のサービスを提供する事業者として総務大臣から指定された電気通信事業者は、その電気通信事業の用に供する電気通信設備について、サイバーセキュリティ対策を含む防護措置の義務づけがなされているほか、当該設備の情報セキュリティの確保のための方針と情報セキュリティ対策の内容について、管理規程への記載義務が存在する。

③ また、電気通信事業者は、電気通信業務に関し重大な事故が生じたときは、その旨をその理由又は原因とともに、遅滞なく、総務大臣に報告する義務があるほか、重大な事故に至らない事故について、毎四半期経過後２か月以内に、その発生状況について、書面等により総務大臣に提出する義務がある。なお、当該四半期ごとの報告については、報告様式における「主な発生原因」の一つとして、「送信型対電気通信設備サイバー攻撃」を明示的に位置づけており、電気通信事業者が意識すべき主要な攻撃の１つであるDoS攻撃やDDoS攻撃によって電気通信設備の事故に至った場合は、制度上、総務大臣がその概要を報告で把握できるようになっている。

④ 放送分野においても、サイバーセキュリティ対策について法令への位置づけ

を検討すべく、2019年（令和元年）７月より情報通信審議会情報通信技術分科会放送システム委員会で、放送設備のサイバーセキュリティ確保に関する技術的条件について検討を開始し、同年12月に情報通信審議会から答申を受けた。また、事故報告については、（ｉ）事故発生後に遅滞なく報告が必要な重大な事故の報告と、（ii）年１回又は２回の総務大臣への定期報告の２種類の法定報告制度が既に存在する。

⑤ 電気通信分野・放送分野においては、上記のほか、総務省や業界団体において様々な基準やガイドラインなどが策定[3]されており、事業者及び民間企業によって参照されている。

⑥ さらに、地方公共団体分野においては、総務省において、地方公共団体のセキュリティ対策の指針として「地方公共団体における情報セキュリティポリシーに関するガイドライン」を策定しているほか、「新たな自治体情報セキュリティ対策の抜本的強化について」（平成27年12月25日 総務大臣通知）によって「三層の対策」「自治体情報セキュリティクラウド」等が導入されており、地方公共団体のマルウェア感染が大幅に減少するなどの効果を挙げている。

⑦ 一方、昨今、一部の地方公共団体において「三層の対策」について不適切な運用がなされていた事案、リース契約等により返却した物品からの情報流出の事案や、複数自治体において利用するクラウドサービスの障害に起因した広域的なシステム障害事案などが発生している事例もある。

イ　とるべき対策

① サイバーセキュリティ対策や事故報告についての法令への位置づけ、分野ごとの所管省庁や業界団体によるガイドラインや基準の策定を通じてサイバーセキュリティ対策を実効的に進めていく取組について、あらゆる機会を通じて周知し、対応の強化を呼びかけていくことが必要である。

② 放送分野において、放送設備のサイバーセキュリティ確保に関する省令改正を速やかに実施することが必要である。

---

[3] 電気通信分野・放送分野において参照されているガイドライン・基準等の例
- ✓ 情報通信ネットワーク安全・信頼性基準（総務省）
- ✓ 電気通信分野における情報セキュリティ確保に係る安全基準（一般社団法人電気通信事業者協会）
- ✓ 放送設備サイバー攻撃対策ガイドライン（一般社団法人ICT-ISAC）

など

③ 地方公共団体分野について、各地方公共団体における「地方公共団体における情報セキュリティポリシーに関するガイドライン」に基づく情報セキュリティ対策及び緊急時連絡体制の確保等の徹底を図ることが必要である。また、昨今の地方公共団体における重大インシデントを踏まえ、同ガイドラインに反映することも念頭に対応策の検討等を行い、地方公共団体へ通知することが必要である。

３．今後の方向性について

本提言においては、総務省が、2020年東京大会の開催期間での対処も見据えつつ、関係主体と連携して早急に取り組むことが期待される事項を整理した。

本タスクフォースでは、昨年８月に公表した「IoT・5Gセキュリティ総合対策」の進捗状況等についてフォローアップしつつ、引き続き、IoT/AI時代を見据えたサイバーセキュリティに係る中長期的な課題及び必要な方策の検討を行っていくこととする。