Sec01-02-63\_各種ガイドブックの内容要約\_次世代環境及び技術関連

ドキュメントを参照: [Sec01-02-50\_サイバーセキュリティ関連\_各種ガイドブックの内容要約.mmap](file:///D:\Cloud_Storage\OneDrive%20-%20ＮＰO知的資源イニシアティブ（ＩＲＩ）\git_repository_Duo\Sharing_Knowledge3\MindManager3\Sec01-02-50_サイバーセキュリティ関連_各種ガイドブックの内容要約.mmap)

1. AI
   1. IoT、 ビッグデータ、 AI等に関する 経済産業省の施策について【2016年3月METI】

ドキュメントを参照: [3\_01\_sano.pdf](https://www.iajapan.org/iot/event/2016/pdf/3_01_sano.pdf)

1. IoT
   1. IoTセキュリティガイドラインver1.0【2016年7月5日総務省・経済産業省】

ドキュメントを参照: [20160705002.html](http://www.meti.go.jp/press/2016/07/20160705002/20160705002.html)

* + 1. 目的等
       1. セキュリティ確保の観点から求められる基本的な取組を、 セキュリティ・バイ・デザインを基本原則としつつ、 明確化することによって、 産業界による積極的な開発等の取組を促すとともに、 利⽤者が安⼼してIoT機器やシステム、 サービスを利⽤できる環境を生み出す
       2. 関係者が取り組むべきIoTのセキュリティ対策の認識を促すとともに、 その認識のもと、 関係者間の相互の情報共有を促すための材料を提供すること
       3. 守るべきものやリスクの⼤きさ等を踏まえ、 役割・⽴場に応じて適切なセキュリティ対策の検討が⾏われることを期待
    2. 各指針と要点
       1. 方針
          1. IoTの性質を考慮した基本方針を定める

経営者がIoTセキュリティにコミットする

内部不正やミスに備える

* + - 1. 分析
         1. IoTのリスクを認識する

守るべきものを特定する

つながることによるリスクを想定する

* + - 1. 設計
         1. 守るべきものを守る・設計を考える

つながる相手に迷惑をかけない設計をする

不特定の相手とつなげられても安全安心を確保できる設計をする

安全安心を実現する設計の評価・検証を行う

* + - 1. 構築・接続
         1. ネットワーク上での対策を考える

機能及び用途に応じて適切にネットワーク接続する

初期設定に留意する

認証機能を導入する

* + - 1. 運用・保守
         1. 安全安心な状態を維持し、 情報発信・共有を行う

出荷・リリース後も安全安心な状態を維持する

出荷・リリース後もIoTリスクを把握し、 関係者に守ってもらいたいことを伝える

IoTシステム・サービスにおける関係者の役割を認識する

脆弱な機器を把握し、 適切に注意喚起を行う

* + - 1. 一般利用者のためのルール
         1. 問合せ窓やサポートがない機器やサービスの購入・利用を控える

インターネットに接続する機器やサービスの問合せ窓やサポートがない場合、 何か不都合が生じたとしても、 適切に対処すること等が困難になる。 問合せ窓やサポートがない機器やサービスの購入・利用は行わないようにする。

* + - * 1. 初期設定に気をつける

・機器を初めて使う際には、 IDやパスワードの設定を適切に行う。 パスワードの設定では、 「機器購入時のパスワードのままとしない」、 「他の人とパスワードを共有しない」、 「他のパスワードを使い回さない」等に気をつける。

・取扱説明書等の手順に従って、 自分でアップデートを実施してみる。

* + - * 1. 使用しなくなった機器については電源を切る

使用しなくなった機器や不具合が生じた機器をインターネットに接続した状態のまま放置すると、 不正利用される恐れがあることから、 使用しなくなった機器は、 そのまま放置せずに電源を切る。

* + - * 1. 機器を手放す時はデータを消す

情報が他の人に漏れることのないよう、 機器を捨てる、 売るなど機器を手放す時は、 事前に情報を削除する。

* + 1. 今後の検討
       1. リスク分析に基づく分野別の対策について
          1. IoTは、 様々な分野に浸透していくことになるが、 分野ごとに求められるセキュリティレベルが異なるため、 多くのIoT機器が利用されている、 もしくは利用が想定される分野では、 具体的なIoTの利用シーンを想定し、 詳細なリスク分析を行った上で、 その分野の性質、 特徴に応じた対策を検討する必要がある。
       2. 法的責任関係について
          1. IoTにおいては、 製造メーカ、 SIer、 サービス提供者、 利用者が複雑な関係になることが多い。 よって、 サイバー攻撃により被害が生じた場合の責任の在り方については、 今後出現するIoTサービスの形態や、 IoTが利用されている分野において規定されている法律などに応じて整理を行っていく必要がある。
       3. IoT時代のデータ管理の在り方について
          1. IoTシステムでは、 利用者の個人情報等のデータを保持・管理等を行う者又は場所が、 サービスの形態により変わってくる。 IoTシステムの特徴を踏まえつつ、 個人情報や技術情報など重要データを適切に保持・管理等を行うことが必要であり、 その具体的な方法について、 検討していく必要がある。
       4. IoTに対する総合的なセキュリティ対策について
          1. IoT社会の健全な発展の実現には、 既に実施されている、 情報処理推進機構（IPA）、 情報通信研究機構（NICT）、 JPCERT/CC及びTelecom ISAC Japan(ICT ISAC Japan)のサイバーセキュリティに関する取組に加え、 一般利用者に対するIoT機器のマルウェア感染に関する注意喚起などの取組について、 官民連携による強化を検討する。
       5. 本ガイドラインの見直しについて
          1. 上記のような検討事項の取組や、 IoTを取り巻く社会的な動向、 脆弱性・脅威事象の変化、 対策技術の進歩等を踏まえて、 今後、 必要に応じて改訂を行っていく必要がある。
  1. 安全なIoTシステムの創出【2016年3月1日NISC】

ドキュメントを参照: [03shiryou05.pdf](http://www.nisc.go.jp/conference/cs/kenkyu/dai03/pdf/03shiryou05.pdf)

* + 1. 任務保証の考え方に基づく取組
       1. 業務責任者（任務責任者）がシステム責任者（資産責任者）と、 機能やサービスを全うするという観点からリスクを分析し、 協議し、 残存リスクの情報も添えて経営者層に対し提供し総合的な判断を受ける「機能保証（任務保証）」の考え方に基づく取組が必要
    2. セキュリティ品質の実現が企業価値
       1. ・IoTシステムのサービスの効用と比較してセキュリティリスクを許容し得る程度まで低減
       2. ・高いレベルのセキュリティ品質の実現が企業価値や国際競争力の源泉に
    3. セキュリティ・バイ・デザインの推進
       1. ・連携される既存システムを含めて、 IoTシステム全体の企画・設計段階からセキュリティの確保を盛り込むセキュリティ・バイ・デザインの推進が重要。
    4. データとシステム全体のセキュリティ確保
       1. IoTシステムはデータの流通プラットフォーム。
       2. データとシステム全体のセキュリティ確保を行う必要がある。
    5. システム間の相互連携の際のリスク評価
       1. レベルの異なるIoTシステムを相互連携させる場合は、 残存リスクを客観的に評価し、 許容範囲内に収めるためのリスク評価が必要
  1. コンシューマ向けIoTセキュリティガイド【2016年6月24日JNSA】

ドキュメントを参照: [iot](http://www.jnsa.org/result/iot/)

* 1. IoT早期導入者のためのセキュリティガイダンス【2016年2月24日CSA】

ドキュメントを参照: [Security\_Guidance\_for\_Early\_Adopters\_of\_the\_Internet\_of\_Things\_J\_160224.pdf](https://www.cloudsecurityalliance.jp/newsite/wp-content/uploads/2016/02/Security_Guidance_for_Early_Adopters_of_the_Internet_of_Things_J_160224.pdf)

* 1. Guide to Industrial Control Systems (ICS) Security【NIST SP.800-82R2】【JPCERT和訳】

ドキュメントを参照: [NISTSP800-82r2\_20160314.pdf](https://www.jpcert.or.jp/research/2016/NISTSP800-82r2_20160314.pdf)

* 1. IoTセキュリティ　標準／ガイドライン　ハンドブック　2017年度版【2018年5月8日JNSA】
  2. コンシューマ向けIoTセキュリティガイド【2016年8月1日JNSA】
  3. IoTソリューション領域へのスキル変革の指針【2018年4月10日IPA】
  4. IoTソリューション領域へのスキル変革の指針\_参考文献【2018年4月10日IPA】
  5. 【未整理】IoTへのサイバー攻撃仮想ストーリー集【一般社団法人日本クラウドセキュリティアライアンス（CSAジャパン）】

ドキュメントを参照: [scenario.pdf](https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/scenario.pdf)

* 1. 【未整理】「つながる世界」を破綻させないためのセキュアなIoT製品開発13のステップ【CSAジャパン　IoTワーキンググループ】

ドキュメントを参照: [future-proofing-the-connected-world\_J\_20170520.pdf](https://cloudsecurityalliance.jp/WG_PUB/IoT_WG/future-proofing-the-connected-world_J_20170520.pdf)

* 1. 【未整理】工場における産業用IoT導入のためのセキュリティファーストステップ【2018年8月JPCERT/CC】

ドキュメントを参照: [ICS-Security1stStep2018.pdf](https://www.jpcert.or.jp/ics/ICS-Security1stStep2018.pdf)

* 1. 【未整理】「IoTセキュリティ基盤を活用したが安心安全な社会の実現に向けた実証実験」の結果の公表【2018年6月総務省情報流通行政局】

ドキュメントを参照: [000560886.pdf](http://www.soumu.go.jp/main_content/000560886.pdf)

* 1. 旧版
     1. 【未整理】IoTセキュリティ総合対策プログレスレポート2018【2018年7月　サイバーセキュリティタスクフォース】

ドキュメントを参照: [000566458.pdf](http://www.soumu.go.jp/main_content/000566458.pdf)

* + 1. 【未整理】「IoTセキュリティ総合対策」（文書）【2017年12月　総務省情報流通行政局】

ドキュメントを参照: [000510701.pdf](http://www.soumu.go.jp/main_content/000510701.pdf)

* 1. 【未整理】「IoTセキュリティ総合対策」について（講演会スライド）【2018年2月28日　総務省情報流通行政局】

ドキュメントを参照: [000543066.pdf](http://www.soumu.go.jp/main_content/000543066.pdf)

* 1. 【未整理】IoTセキュリティ総合対策プログレスレポート2019【2018年5月　サイバーセキュリティタスクフォース】

ドキュメントを参照: [000623344.pdf](http://www.soumu.go.jp/main_content/000623344.pdf)

* 1.  IoT・5Gセキュリティ総合対策（案）【2019年6月総務省サイバーセキュリティタスクフォース】

ドキュメントを参照: [01cyber01\_02000001\_00031.html](http://www.soumu.go.jp/menu_news/s-news/01cyber01_02000001_00031.html)

* + 1. 目次
       1. はじめに
       2. Ⅰ 背景
       3. Ⅱ 施策展開の枠組み
       4. Ⅲ 情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策
          1. （１）IoTのセキュリティ対策

① IoT機器の設計・製造・販売段階での対策

② IoT機器の設置・運用・保守段階での対策

③ 脆弱性等を有するIoT機器の調査と注意喚起

④ サイバー攻撃に関する電気通信事業者間の情報共有

* + - * 1. （２）5Gのセキュリティ対策

① ソフトウェア脆弱性への対応

② ハードウェア脆弱性への対応

* + - * 1. （３）クラウドサービスのセキュリティ対策
        2. （４）スマートシティのセキュリティ対策
        3. （５）トラストサービスの在り方の検討
        4. （６）公衆無線LANのセキュリティ対策
        5. （７）重要インフラとしての情報通信分野のセキュリティ対策
        6. （８）地域の情報通信サービスのセキュリティの確保
      1. Ⅳ 横断的施策
         1. （１）研究開発の推進

① 基礎的・基盤的な研究開発等の推進

② 広域ネットワークスキャンの軽量化

③ ハードウェア脆弱性への対応【再掲】

④ スマートシティのセキュリティ対策【再掲】

⑤ 衛星通信におけるセキュリティ技術の研究開発

⑥ AIを活用したサイバー攻撃検知・解析技術の研究開発

⑦ 量子コンピュータ時代に向けた暗号の在り方の検討

⑧ 重要インフラ等におけるサイバーセキュリティの確保

⑨ IoT 社会に対応したサイバー・フィジカル・セキュリティ対策

* + - * 1. （２）人材育成・普及啓発の推進

① 実践的サイバー防御演習（CYDER）の実施

② 2020東京大会に向けたサイバー演習の実施

③ 若手セキュリティ人材の育成の促進

④ 地域のセキュリティ人材育成

* + - * 1. （３）国際連携の推進

① ASEAN各国との連携

② 国際的なISAC間連携

③ 国際標準化の推進

④ 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

* + - * 1. （４）情報共有・情報開示の促進

① サイバー攻撃に関する電気通信事業者間の情報共有【再掲】

② 事業者間での情報共有を促進するための基盤の構築

③ サイバーセキュリティ対策に係る情報開示の促進

④ サイバーセキュリティ対策に係る投資の促進

⑤ 国際的なISAC間連携【再掲】

* + - 1. Ⅴ 今後の進め方
    1. 内容抜粋
       1. はじめに
          1. IoTをはじめとするICTの利活用が一層進展していく中で、 今後、 5Gのサービスが開始することが予定されているほか、 Society5.0に向けた適切なデータ管理・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するなど、 サイバーセキュリティリスクへの対策の一層の強化は急務となっている。
          2. 今般、 「IoTセキュリティ総合対策」策定・公表後の様々な状況変化などを踏まえつつ、 IoT・5G時代にふさわしいサイバーセキュリティ政策の在り方について検討し、 「IoT・5Gセキュリティ総合対策」として整理したものである。
       2. Ⅰ 背景
          1. （１）ICT利活用の進展

ICT（Information and Communications Technology：情報通信技術）によって、 我が国の社会・経済は大きく変革を遂げてきた。 人々の日々のコミュニケーションや情報収集、 企業活動、 購買行動、 就労、 余暇など、 社会・経済のあらゆる場面でICTの利活用が浸透している。 令和の時代に入り、 この流れは今後も加速していくことが想定される。

このような変化をもたらしたICTの発展の態様については大きく以下の５つに大別することができる。

①ブロードバンド化（小容量通信から大容量通信へ）

②モバイル化（固定から移動へ）

③クラウド化（オンプレミス1からクラウドへ）

④IoT化（人からモノへ）

⑤AI化（人からAIへ）

2020年（令和２年）に5Gサービスが本格的に開始されることにより、 このような流れはより一層加速していくことが予測され、 我が国が目指すべき社会像としてのSociety5.0の到来を迎え、 今後、 サイバー空間と実空間の一体化が一層進展していくことが想定される。

* + - * 1. （２）サイバーセキュリティリスクの増大や脅威の深刻化

社会・経済全体のあらゆる場面でのICTの利活用が水や空気のように浸透してきたところであるが、 同時に必然的にサイバーセキュリティリスクも増大している状況である。

サイバーセキュリティリスクは、 インシデントの影響度の大きさ×発生確率で表されるが、 社会・経済のICTへの依存度が高まれば高まるほど、 インシデントが発生した際の脅威や影響も飛躍的に増大し、 またインシデントが発生する確率も高くなる。

そのため、 サイバーセキュリティの確保は、 ICTの利活用による社会や経済の持続的・安定的な発展のために必要不可欠な取組となっている。

、 直近で特に対策が必要となるサイバーセキュリティ上の留意事項としては以下のような点が挙げられる。

① 5Gのサービス開始に伴う新たなリスク

今後サービスが開始される予定の5Gについては、 従来までの移動通信システムと比較して、 ①超高速、 ②超低遅延、 ③多数同時接続であるという特徴を有しており、 IoTシステムの基盤技術として、 電気通信事業者のみならず、 様々な主体や産業分野での利活用が期待されている。

他方、 サイバーセキュリティの観点からは、 5Gのネットワークはネットワーク機能の仮想化・ソフトウェア化やモバイルエッジコンピューティング2（以下「MEC」という。 ）など、 従来のネットワークとは構造等の点において異なる特徴を有することが想定されるから、 その点を踏まえ、 5Gのネットワークのセキュリティ確保の在り方について検討する必要がある。

また、 5Gのサービス開始により、 従来に比べて産業用途でのIoT機器の設置・運用が今後も増加していくことが想定されるため、 IoT機器のセキュリティの確保（脆弱性対策を含む）の重要性が今後さらに高まっていくことが想定される。

さらに、 従来はインターネットから隔離された形で運用されていた産業機器やインフラなどが無線経由でインターネットに接続される可能性が高くなることから、 IT系（情報系）だけでなく、 OT系（制御系）のシステムのセキュリティ対策も今後より一層重要になることが想定される。

② サプライチェーンリスクの管理の重要性

今日では、 サイバー空間と実空間の一体化の進展や、 サプライチェーンのグローバル化の進展により、 ソフトウェアやハードウェアのサプライチェーンなど、 ICTの製品やサービスを製造・流通する過程において不正なプログラムやファームウェアの組み込み、 又は改ざんなどが行われるリスクへの対応3が求められている。

また、 製品やサービスそのもののリスクだけではなく、 委託等の契約関係がある関係者の間でサイバーセキュリティ対策が不十分な者が踏み台となって他者へのサイバー攻撃がなされ、 被害が伝播する「被害のチェーン」が発生するおそれもある。

そのため昨今では、 企業単体ではなく、 サプライチェーン単位でのサイバーセキュリティ対策が求められている状況4であり、 特に地域の中小企業では、 人材を含めたリソース不足のため、 サイバーセキュリティ対策が遅れている可能性があることから、 対策の強化の取組が必要不可欠となっている。

③ Society5.0の実現に向けた適切なデータの流通・管理の重要性

Society5.0はサイバー空間と実空間を高度に融合させることにより、 経済的発展と社会的発展の解決を両立する「人間中心の社会」であり、 言い換えれば、 サイバー空間と実空間の間でデータが循環して、 相互に作用し、 これを前提とした様々なサービスが提供され、 人々の生活に浸透し、 恩恵をもたらす社会である。

そのSociety5.0の実現の鍵となるのがデータであり、 データの利活用・管理の利便性を高めるクラウドサービスの安全性の確保や、 データ収集・分析を都市や地域の機能やサービスを効率化・高度化に生かすスマートシティのセキュリティの確保等の重要性が高まっている。 また、 データ流通の有効性を担保するための基盤として、 ネット利用者の本人確認やデータの改ざん防止等の仕組みであるトラストサービスの必要性も高まっている。

また、 経済のグローバル化が進展する今日においては、 国内のみならず国際的なデータの移転も大幅に増加している5。 この点、 諸外国に目を転じてみれば、 EUのGDPR（一般データ保護規則：General Data Preservation Rule）、 米国のFISMA（連邦情報セキュリティマネジメント法：Federal Information Security Management Act）、 中国のサイバーセキュリティ法など、 各国の政府が企業などに対して国境を越えてデータを移転させないような法規制を導入している例も出始めているところである。

そのため、 上述のような流れも認識しつつ、 機密性（Confidentiality）・完全性（Integrity）・可用性（Availability）・真正性（Authenticity）等の確保の観点からの適切なデータの管理・流通の在り方、 及びそれを実現するための手段等について検討する必要がある。

⑥ 大規模な国際イベント等の開催

大規模かつ非日常の国際イベントは最高度の注目を集めることから、 サイバー攻撃の標的となるおそれがある。

この点、 2019年（令和元年）にはG20やラグビーワールドカップ、 2020年（令和２年）には2020年東京オリンピック・パラリンピック競技大会（以下「2020東京大会」という。 ）の開催が予定されている。

そのため、 過去の経験も踏まえつつ、 大会に関係する重要なサービスを担う事業者のリスクマネジメントや対処体制の構築、 訓練・演習の強化など、 特に重要インフラ事業者、 重要サービス事業者等において、 これまで実施されてきた対策の一層の強化が求められる。

また、 2020東京大会が無事成功裏に終わったとしても、 社会に対するサービスの提供を行うという「任務」8を担う重要インフラ事業者等にとっては、 サイバー攻撃への対処態勢の強化は日常的に重要な課題であり、 引き続き、 平時・有事の対策を着実に実行することが求められる。

上記のような状況を踏まえ、 昨今でサイバーセキュリティ対策は一層重要度を増していることから、 2017年（平成29年）10月に策定・公表した「IoTセキュリティ総合対策」を発展的に改編する形で、 IoT・5G時代にふさわしいサイバーセキュリティ政策の在り方として、 今般「IoT・5Gセキュリティ総合対策」を策定することとしたものである。

* + - 1. Ⅱ 施策展開の枠組み
         1. 概要

サイバーセキュリティ対策は広範な政策分野であり、 その推進に当たっては各主体の適切な役割分担の下での連携・協働が必要である。

この点、 総務省に期待される役割は、 まず情報通信サービス・ネットワークの、 特に重点的に対応すべき個別分野のセキュリティの在り方について包括的な検討の上、 関係府省庁や民間企業と連携しつつ、 政策を実効的に推進していくことである。

さらに、 当該分野での政策をより効果的に実施するための研究開発の推進や、 情報通信サービス・ネットワークのユーザも含めた人材育成・普及啓発の推進、 国際連携の推進、 サイバーセキュリティに関する情報共有・情報開示の促進観点からの取組を並行して進めていく必要がある。

そのため、 本文書では、 総務省として取り組むべき具体的な施策について、 「Ⅲ 情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策」と「Ⅳ 横断的施策」の「（１）研究開発の推進」、 「（２）人材育成・普及啓発の推進」、 「（３）国際連携の推進」、 「（４）情報共有・情報開示の促進」という項目で整理を行っている。

* + - * 1. なお、 施策の検討・展開の際には、 それぞれの取組において、 例えば以下のような観点について留意しつつ、 施策の有効性を確保する必要がある。

① ネットワーク側とユーザ側の双方の観点からの施策展開

情報通信サービス・ネットワーク全体の安全性や信頼性を確保するためには、 ネットワーク側とユーザ側の双方の視点でサイバーセキュリティ対策を推進するための施策を検討する必要がある。

② 情報通信サービス・ネットワークのレイヤー構造

情報通信サービス・ネットワークについては、 機能に着目して構造的にアプリケーション層、 プラットフォーム層、 ネットワーク層、 端末層と分類が可能であるが、 それぞれの層において留意すべき脅威とセキュリティ要件の在り方について検討する必要がある。

③ 時間軸を意識した施策展開

IoT機器のライフサイクル、 人材育成のスパンなど、 施策の効果の発現に関する時間軸を意識した政策立案を行う必要がある。

④ 政策バリューチェーンの構築

例えば、 研究開発の成果を情報通信サービス・ネットワークの個別分野の施策に反映しつつ、 その成果について国際的な展開を図る、

また、 情報通信サービス・ネットワークの個別分野のセキュリティに関する施策と人材育成の施策を連携させて、 地域のサイバーセキュリティ確保を一体的に推進するなど、 個別施策を有機的に連携させ、 横断的で一貫性のある施策展開を図る必要がある。

* + - 1. Ⅲ 情報通信サービス・ネットワークの個別分野のセキュリティに関する具体的施策
         1. 概要

総務省においてセキュリティの確保に取り組むべき情報通信サービス・ネットワークの個別分野としては、 以下のような分野が考えられる。

まず、 今後の5Gサービスの開始を迎え、 IoT及び5Gのセキュリティ対策は重要な政策課題となっており、 既に始まっている取組と合わせて重点的に取り組んでいく必要がある。

また、 Society5.0の実現に向けたデータ流通や管理の需要性が増している中で、 クラウドサービスの安全性の確保やスマートシティのセキュリティの確保も必要性が高まっているほか、 データ流通の有効性を担保するための基盤としてのトラストサービスの在り方の検討も必要となっている。

さらに、 昨今ではサプライチェーンの弱いところを狙った攻撃が散見されることから、 我が国の情報通信サービス・ネットワーク全体のセキュリティの確保のため、 地域の情報通信サービス・ネットワークのセキュリティ強化も必要である。

その上で、 2020東京大会及びその後を見据え、 公衆無線LANのセキュリティの確保や、 重要インフラ分野・重要サービス分野としての情報通信分野のセキュリティの確保などにも取り組む必要がある。

なお、 具体的施策の検討・実施に当たっては、 前述（Ⅱ）の①～④の観点などに留意する必要がある。

* + - * 1. （１）IoTのセキュリティ対策

IoT機器の脆弱性については、 IoT機器の①設計・製造・販売（輸入を含む。 ） 段階、 ②設置・運用・保守段階において適切な対策をとる必要がある。

また、 既にインターネットに接続されて設置・運用されているIoT機器が多数あることが想定されることから、 IoT機器の脆弱性等の調査を実施するとともに、 利用者への注意喚起や情報共有の取組等を推進する必要がある。

① IoT機器の設計・製造・販売段階での対策

設計・製造・販売段階においては、 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とともに、 対策がとられた機器の市場への展開を促進させることが重要となる。

この点、 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9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。 今後は、 当該技術基準の運用開始に向けた準備を進めることが必要である。

また、 IoT機器に関するセキュリティ対策の上乗せ部分については、 民間団体がセキュリティ要件のガイドラインを策定し、 さらに当該要件に適合したIoT機器に対して適合していることを示すマークを付す認証（Certification）制度の構築の準備を進めていることから、 このような民間の任意の認証（Certification）制度の普及が期待される。

② IoT機器の設置・運用・保守段階での対策

機器の性格上セキュリティ対策を取ることが困難なものや海外製品など、 流通するIoT機器の中から、 脆弱性を有するIoT機器を完全に排除することは困難であることから、 機器の設置・運用・保守段階（ネットワークへの接続時又は接続後）において、 脆弱性を有する機器が存在することを前提として、 セキュアなIoTシステム構築を実現する仕組みが重要である。

また、 IoT機器は広範な利用者が利用することが想定されており、 利用者によっては、 IoT機器やセキュリティに関する知識が十分に無いことが想定される。 したがって、 例えば、 IoT機器の設置後に新たな脆弱性が発見された場合に、 当該IoT機器の製造業者によって脆弱性のパッチがユーザサポートの一環として提供されるなど、 各種事業者の側において対策が実施される仕組みの構築が重要である。

IoTシステム・サービス全体としてのセキュリティの確保に関しては、 IoT機器だけでなく、 ネットワーク側での対処の在り方についても検討が必要である。 この点で、 IoT機器の不正検知等のため、 IoT機器とインターネットの境界上にセキュアゲートウェイ（IoTセキュアゲートウェイ）を設置する取組が考えられる。 本取組について、 Ⅲ－（４）のスマートシティのセキュリティ対策の取組等を通じ、 実際の導入を進める仕組みや方策について検討することが重要である。

③ 脆弱性等を有するIoT機器の調査と注意喚起

前述の①、 ②の対策については、 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。

この点、 国立研究開発法人情報通信研究機構（以下「NICT」という。 ）の業務に、 パスワード設定等に不備のあるIoT機器の調査等を５年間の時限措置として追加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実施し、 2019年（平成31年）２月より、 NICTがIoT機器を調査し、 電気通信事業者を通じて利用者への注意喚起を行うプロジェクト「NOTICE10」を開始したところであり、 引き続き、 本プロジェクトの着実な実施を通じ、 既に現在設置されているIoT機器のセキュリティ対策を進めることが必要である。

また、 「NOTICE」の取組に加えて、 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、 電気通信事業者を通じて利用者へ注意喚起を行う取組を実施することも必要である。

さらに上述の取組の実施にあたり、 専用のサポートセンターを設置し、 行政相談窓口や消費生活センター等と連携しつつ、 ウェブサイトや電話による問合せ対応を通じて利用者に適切なIoT機器のセキュリティ対策を案内することも必要である。

加えて、 これらの取組については、 IoT機器のセキュリティ対策のベストプラクティスとして、 Ⅳ－（３）の国際連携の推進などの取組を通じ、 海外各国に対して発信し、 各国の取組につながるよう働きかけることが重要である。

④ サイバー攻撃に関する電気通信事業者間の情報共有

脆弱性を有するIoT機器が踏み台となったことが確認された際、 被害の拡大を防止するため、 ISPによる、 当該ISPの利用者の端末とC&Cサーバ11の間の通信を遮断する等の取組が必要である。

この点、 総務省では、 2018年（平成30年）５月の改正電気通信事業法において、 電気通信事業者が「送信型対電気通信設備サイバー攻撃」への対応を共同して行うため、 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（認定送信型対電気通信設備サイバー攻撃対処協会。 以下「認定協会」という。 ）を総務大臣が認定する制度を創設し、 2019年（平成31年）１月に一般社団法人ICT-ISAC12が認定されたところである。

今後は認定協会の活動について、 マルウェアに感染している可能性の高いIoT端末等やC&Cサーバであると疑われる機器の検知や利用者への注意喚起等の電気通信事業者が行う対策に向け、 円滑な実施のための支援を行うなどの取組を促進することが重要である。

また、 こうした認定協会の活動や「NOTICE」の実施状況も踏まえ、 電気通信事業者等が協力してサイバー攻撃への対処を行う際の基盤となる効果的な情報共有の在り方について引き続き検討することが重要である。

* + - * 1. （２）5Gのセキュリティ対策

① ソフトウェア脆弱性への対応

今後サービスが開始される予定の5Gについては、 従来までの移動通信システムと比較して、 ①超高速、 ②超低遅延、 ③多数同時接続であるという特徴を有しており、 IoTシステムの基盤技術として、 電気通信事業者のみならず、 様々な主体や産業分野での利活用が期待されている。

一方、 5Gのネットワークに関しては、 ネットワーク機能の仮想化・ソフトウェア化が進むことから、 新たなサイバーセキュリティ上の課題が懸念される。 また、 新たにネットワークのエッジ（基地局とコア網の間に設置）で通信処理や高度な演算・データ処理がなされるモバイルエッジコンピューティング（

MEC）が利用されることから、 ネットワークインフラとしての機能維持のためには、 基地局やコア網のみならず、 MECも含めた各構成要素（デバイス、 クラウド、 アプリケーション等）全体を考慮したセキュリティの確保が必要不可欠である。

そのため、 5Gの各構成要素におけるソフトウェアを含むセキュリティを総合的かつ継続的に担保する仕組みを整備し、 ガイドライン等によって対策の共有等を図ることを通じ、 5Gを構築・活用する重要インフラ事業者等への周知・啓発を図ることが必要である。

また、 5Gのセキュリティの確保は、 国際的にも重要な政策課題であることから、 作成したガイドライン等について国際機関等への提案も視野に入れるなど、 諸外国との連携を図ることが期待される。

② ハードウェア脆弱性への対応

機器のセキュリティについては、 機器にインストールされているソフトウェアだけでなく、 集積回路の設計工程において、 ハードウェア脆弱性が存在する可能性が指摘されている。

そのため、 総務省では、 2017年度（平成29年度）より、 戦略的情報通信研究開発推進事業（SCOPE）において、 ハードウェア脆弱性の検知技術の研究開発を実施し、 膨大な数の回路設計図をビッグデータとして収集・蓄積しつつ、 脆弱性が存在する可能性のあるチップを、 AIを活用して類型化し、 ハードウェア脆弱性を発見するための研究開発を実施してきたところである。

5Gの時代を見据え、 サプライチェーンリスクへの対応の観点から、 ソフトウェアやファームウェアに対する対策と合わせて、 引き続き、 ビッグデータやAIを活用しつつハードウェアに組み込まれるおそれのある脆弱性を検出する技術の研究開発等を推進することが必要である。

* + - * 1. （３）クラウドサービスのセキュリティ対策

ICTの利活用が社会全体として進展する中、 インターネット上のリソースを臨機応変に活用するクラウドサービスは、 サービスアプリケーションから多様なIoTプラットフォームまで、 様々なICTソリューションを支えており、 データの利活用・管理における中核のサービスとなっている。

その中で、 我が国の政府においても「政府情報システムにおけるクラウドサービスの利用に係る基本方針」（2018年（平成30年）６月７日CIO連絡会議決定）を定め、 情報システム調達に際しては、 コスト削減や柔軟なリソースの増減等の観点から、 クラウドサービスの利用を第一候補として検討を行う旨の方向性が示されているところである。

この点、 諸外国では、 2010年代に政府が情報システム調達においてクラウドファーストを掲げ、 その後間もなく、 政府が主導してクラウドサービスの安全性を評価する制度を構築・運用している事例があり、 2018年（平成30年）に上述のクラウド・バイ・デフォルト原則を採用した我が国においても、 安全性評価の制度の検討が必要な段階に到達している。

そのため、 総務省と経済産業省において、 クラウドサービスの安全性評価に関する検討を行うことを目的として、 2018年（平成30年）８月より、 「クラウドサービスの安全性評価に関する検討会」を開催し、 2019年（平成31年）３月に制度の枠組みが示されたところである。

本枠組みを踏まえつつ、 官民双方が一層安全・安心にクラウドサービスを採用し、 継続的に利用していくため、 クラウドサービスの安全性評価制度について、 引き続き、 総務省において、 経済産業省と連携しつつ、 2020年（令和２年）の制度の開始を目指して、 評価基準や制度の確立に向けた検討を進めることが必要である。

* + - * 1. （４）スマートシティのセキュリティ対策

スマートシティは、 先進的技術の活用により、 都市や地域の機能やサービスを効率化・高度化し、 各種の課題の解決を図るとともに、 快適性や利便性を含めた新たな価値を創出する取組であり、 Society5.0の先行的な実現の場である。

この点、 総務省では、 都市に設置されたセンサーから収集・生成・蓄積・解析されるデータを活用し、 その解析結果を都市経営の課題解決などに活用するデータ利活用型スマートシティ事業を2017年度（平成29年度）から実施しているところである。 なお、 今後は政府のスマートシティに係る各事業の連携や分野間のデータ連携等を協力推進していくため、 関係本部・省庁で連携13していくこととされている。

他方、 スマートシティでは、 インターネットに接続するセンサー・カメラ等が散在し、 多様なデータが流通しているため、 常にサイバー攻撃のリスクにさらされるおそれがある。

また、 様々なデータが共通プラットフォーム上で流通する中で、 データの真正性の確保や適切なデータ流通の管理の仕組みの構築等も必要である。 さらに、 システムとしてのスマートシティの構築・運用には多様な主体が関わることから、 システム全体としてのセキュリティの在り方について多様な関係者間で一定の共通認識の醸成が必要である。

そのため、 スマートシティ上の様々なユースケース（分野）やアーキテクチャ、 相互運用性などを踏まえつつ、 スマートシティに求められるセキュリティ要件について検討を行い、 明確化を図る必要がある。

また、 スマートシティの取組は国際的にもEUの研究開発プロジェクトHorizon 2020やNISTが主導するGCTC（Global City Teams Challenge14）プロジェクトでも展開されており、 総務省ではEUと連携した、 スマートシティ分野のセキュリティ・プライバシ保護を含む日EU共同研究（Fed4IoT15）を2018年（平成30年）から実施している。

そのため、 上述の成果については諸外国と連携の上、 国際標準化や必要に応じた国際的な議論の場への提案を検討するなど、 諸外国との調和を意識して展開を図ることが重要である。

さらに、 スマートシティのシステムでは、 多種多様なIoT機器が活用されることが想定されることから、 そのセキュリティの確保に当たっては、 IoT機器そのもののセキュリティの強化だけでなく、 ネットワークの側でIoT機器の不正検知等を実施するための仕組みが有効であり、 実際の運用に関して、 Ⅲ－（１）－②のIoT機器とインターネットの境界上にセキュアゲートウェイを設置する取組との連携の在り方も検討することが重要である。

* + - * 1. （５）トラストサービスの在り方の検討

Society5.0の実現に向けて、 サイバー空間の自由で安心・安全なデータの流通を実現するためには、 データの信頼性を確保する仕組みとして、 データの改ざんや送信元のなりすまし等を防止するトラストサービスが不可欠である。

そのため、 総務省では、 「プラットフォームサービスに関する研究会」の下に「トラストサービス検討ワーキンググループ」を設置し、 2019年（平成31年）１月から、 以下のようなトラストサービスに関する現状や課題について検討を行っている。

１）人の正当性を確認できる仕組み（電子署名）

２）組織の正当性を確認できる仕組み（組織を対象とする認証、 ウェブサイト認証）

３）IoT機器等のモノの正当性を確認できる仕組み

４）データの存在証明・非改ざんの保証の仕組み（タイムスタンプ）

５）データの送達等を保証する仕組み（eデリバリー）

一方、 EUにおいては2016年（平成28年）７月に発効したeIDAS（electronic Identification and Authentication Services）規則により、 電子署名、 タイムスタンプ、 eシール等のトラストサービスについて包括的に規定している状況である。

そのため、 国際的な相互運用性の確保の観点からも、 引き続き、 同ワーキンググループにおいて、 制度的課題等について整理を行い、 トラストサービスの在り方について2019年（令和元年）中を目途に結論が得られるよう、 検討を進めることが必要である。

* + - * 1. （６）公衆無線LANのセキュリティ対策

公衆無線LANについては、 2020年東京大会に向けて、 観光や防災の観点から、 その普及が進んでいるところである。 他方、 多くの公衆無線LANのサービスにおいて、 依然としてサイバーセキュリティに対する配慮に欠けるものも多く、 これらのサービスを踏み台にした攻撃や情報漏洩などのインシデントが発生するおそれもある。

そのため、 公衆無線LANの利用者や提供者向けの公衆無線LANの利用の手引きの普及を図るなど、 利用者・提供者において必要となるセキュリティ対策に関する周知啓発の充実を図ることが重要である。

その際、 Ⅲ－（８）の地域の情報通信サービスのセキュリティの確保の取組で構築する連絡体制を活用し、 効果的な周知啓発を図ることが重要である。

* + - * 1. （７）重要インフラとしての情報通信分野のセキュリティ対策

情報通信分野は、 「重要インフラの情報セキュリティに係る第４次行動計画」（平成29年４月18日サイバーセキュリティ戦略本部決定 平成30年７月25日サイバーセキュリティ戦略本部改定。 以下「第４次行動計画」という。 ）において、 特にその機能が停止又は低下した場合に国民生活・社会経済活動に多大なる影響を及ぼしかねないサービスとして重要インフラの14分野の１つに指定されている。

第４次行動計画を踏まえ、 重要インフラ各分野に横断的な指針として「重要インフラにおける情報セキュリティ確保に係る安全基準等策定指針（第５版）」（平成30年４月サイバーセキュリティ戦略本部決定 令和元年５月サイバーセキュリティ戦略本部改定）が定められており、 同指針を踏まえ、 官民で連携して、 安全基準等の整備及び浸透の取組が進められている。

この点、 電気通信においては、 各年の取組として、 「電気通信事故検証会議」等の枠組みを通じ、 電気通信事故の分析・検証等を行うとともに、 事故再発防止のため、 「情報通信ネットワーク・安全信頼性基準」等の見直しの必要性について検討を行っている。

また、 2018年度（平成30年度）には、 前述のⅢ－（１）－④のとおり、 「送信型対電気通信設備サイバー攻撃」に関する送信元情報の共有やC&Cサーバの調査研究等を行う第三者機関として認定協会を総務大臣が認定する制度を創設した。 さらに本制度改正に関連して、 「送信型対電気通信設備サイバー攻撃」が原因である電気通信事故の発生状況を把握する観点から当該事故の報告を求めるため、 電気通信事業報告規則を改正する制度整備が行われている。

以上のような取組も踏まえつつ、 引き続き、 必要に応じて情報通信分野のセキュリティ対策に関する制度的枠組みの改善等に向けた取組が行われることが期待される。

* + - * 1. （８）地域の情報通信サービスのセキュリティの確保

我が国の情報通信サービス・ネットワークの安全性や信頼性の確保の観点からは、 全国規模や首都圏でサービスを提供している事業者だけでなく、 地域単位で情報通信サービスを提供している事業者におけるサイバーセキュリティの確保も重要な課題である。

他方、 地域においては、 首都圏と比較してサイバーセキュリティに関する情報格差が存在するほか、 経営リソースの不足等の理由により、 セキュリティ対策が十分でないケースが存在するおそれがある。

そのため、 業界団体やセキュリティ関係機関等と連携しつつ、 地域の事業者のサイバーセキュリティ対策の質の向上に向けた連絡体制を構築することが必要である。 なお、 当該施策の展開に当たっては、 Ⅲ－（６）の公衆無線

LANのセキュリティの確保やⅣ－（２）－①の実践的サイバー防御演習（CYDER）の実施、 Ⅳ－（２）－④の地域のセキュリティ人材育成の取組等との連携を図り、 効果的に地域の情報通信サービスのセキュリティ対策の質の向上を図ることが重要である。

* + - 1. Ⅳ 横断的施策
         1. （１）研究開発の推進

① 基礎的・基盤的な研究開発等の推進

② 広域ネットワークスキャンの軽量化

③ ハードウェア脆弱性への対応【再掲】

④ スマートシティのセキュリティ対策【再掲】

⑤ 衛星通信におけるセキュリティ技術の研究開発

⑥ AIを活用したサイバー攻撃検知・解析技術の研究開発

⑦ 量子コンピュータ時代に向けた暗号の在り方の検討

⑧ 重要インフラ等におけるサイバーセキュリティの確保

⑨ IoT 社会に対応したサイバー・フィジカル・セキュリティ対策

* + - * 1. （２）人材育成・普及啓発の推進

① 実践的サイバー防御演習（CYDER）の実施

② 2020東京大会に向けたサイバー演習の実施

③ 若手セキュリティ人材の育成の促進

④ 地域のセキュリティ人材育成

* + - * 1. （３）国際連携の推進

① ASEAN各国との連携

② 国際的なISAC間連携

③ 国際標準化の推進

④ 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

* + - * 1. （４）情報共有・情報開示の促進

① サイバー攻撃に関する電気通信事業者間の情報共有【再掲】

② 事業者間での情報共有を促進するための基盤の構築

③ サイバーセキュリティ対策に係る情報開示の促進

④ サイバーセキュリティ対策に係る投資の促進

⑤ 国際的なISAC間連携【再掲】

* + - 1. Ⅴ 今後の進め方
         1. 「IoT・5Gセキュリティ総合対策」の推進に際しては、 定期的に検証を行い、 進捗状況を把握するとともに、 本分野における技術革新や最新のサイバー攻撃の態様を踏まえ、 必要に応じて随時見直しを行っていくことが望ましい。 また、 対策の推進に際しては、 内閣官房内閣サイバーセキュリティセンターや経済産業省をはじめ、 関係府省庁との連携の下に進めていく必要がある。
         2. 「IoT・5Gセキュリティ総合対策」の推進は、 2020年東京大会の成功に向けても必須である。 重要インフラの防御対策強化の観点を含め、 関係するステークホルダーの連携によるビジョンの共有と取組の強化が不可欠である。

1. クラウド
   1. クラウドセキュリティガイドライン活用ガイドブック2013年版【METI】

ドキュメントを参照: [20140314004-3.pdf](http://www.meti.go.jp/press/2013/03/20140314004/20140314004-3.pdf)

* 1. クラウドサービス提供における情報セキュリティ対策ガイドライン【2014年4月総務省】

ドキュメントを参照: [01ryutsu03\_02000073.html](http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000073.html)

* 1. クラウドセキュリティ関連ISO規格
     1. ■ISO/IEC27017:2015に基づくISMSクラウドセキュリティ認証に関する要求事項（スライド）【JIPDEC】

ドキュメントを参照: [JIP-ISMS517-10.pdf](https://www.isms.jipdec.or.jp/doc/JIP-ISMS517-10.pdf)

* + 1. ■ISMSクラウドセキュリティ認証の概要（スライド）【JIPDEC】

ドキュメントを参照: [shiryou-1.pdf](https://www.isms.jipdec.or.jp/seminar/cloud/shiryou-1.pdf)

* + 1. ■ISO/IEC27017:2015に基づくクラウドセキュリティの構築のポイント（スライド）【JIPDEC】

ドキュメントを参照: [shiryou-2.pdf](https://www.isms.jipdec.or.jp/seminar/cloud/shiryou-2.pdf)

1. 教育分野
   1. 教育分野におけるクラウド導入に対応する情報セキュリティに関する手続きガイドブック【総務省】

ドキュメントを参照: [000417633.pdf](http://www.soumu.go.jp/main_content/000417633.pdf)

* + 1. 第1章　クラウド導入のプセスと情報セキュリティに係る手続き
       1. １．１　調達のプセスと情報セキュリティの関係
    2. 第2章　情報セキュリティ手続きにおける「準備段階」の留意点
       1. ２．１　教育用コンテンツに関する情報収集
       2. ２．２　法令やポリシーに関する情報収集
    3. 第3章　情報セキュリティ手続きにおける「計画段階」の留意点
       1. ３．１　クラウド上で取り扱う情報資産の洗い出し
       2. ３．２　クラウドを中心としたICT環境に関するリスクの洗い出し
       3. ３．３　リスクおよび情報セキュリティポリシーを踏まえた仕様書の作成
    4. 第4章　情報セキュリティに関する手続きにおける「運用段階」の留意点
       1. ４．１　緊急時対応計画の整備
       2. ４，２　研修の実施
       3. ４．３　情報セキュリティに関する監査
       4. ４．４　著作権等
  1. 教育ＩＣＴの新しいスタイルクラウド導入ガイドブック2015【総務省】

ドキュメントを参照: [000358976.pdf](http://www.soumu.go.jp/main_content/000358976.pdf)

* + 1. 第5 章情報セキュリティポリシー
       1. 5.1 教育現場にふさわしい情報セキュリティポリシーとは
       2. 5.2 クラウドに対応した情報セキュリティポリシーとは
       3. 5.3 学校における情報セキュリティポリシーの事例
    2. Column　先進事例④　教育用SNS