資料2

IoTセキュリティガイドラインについて

平成２８年４月２２日

事務局

IoTセキュリティガイドラインの目的等

■　本ガイドラインは、IoTシステム・サービスについて、IoT特有の性質とセキュリティ対策の必要性を踏まえて、**その関係者が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り組みを促すとともに、利用者が安心してIoT機器・システム・サービスを利用できる環境を生み出すことにつなげるもの。

■　なお、サイバー攻撃などによる被害発生時における関係者間の法的責任の所在を一律に明らかにすることを目的としておらず、むしろ**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とすることが目的**である。

■　本ガイドラインは一律に具体的なセキュリティ対策を求めるものではなく、**守るべきものやリスクの大きさ等を踏まえ、具体的なリスク分析の実施方法や個別の適切なセキュリティ対策の検討が促進されることを期待**する。

IoTセキュリティガイドラインについて

■　本ガイドラインは、IoTシステム・サービス等の提供にあたってのライフサイクル（方針・管理、分析、設計、構築、運用・保守）における指針を定めるとともに、一般利用者のためのルールを定めたもの。
■　各指針等においては、具体的な対策を要点としてまとめている。

	指針	主な要点
方針・管理	**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
分析	**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
設計	**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
構築	**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
運用・保守	**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
一般利用者のためのルール		• 問合せ窓口やサポートがない機器やサービスの購入・利用を控える • 初期設定に気をつける • 使用しなくなった機器については電源を切る • 機器を手放す時はデータを消す

【方針・管理】 指針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

■　IoTは様々な機器やシステムが接続されるため、ひとたび攻撃を受けるとIoT機器単体に留まらず、関連するIoTシステム・サービス全体へ影響を及ぼす可能性がある。また、長期間使われる機器も存在する一方で、監視が行き届きにくいこと、IoT機器の機能・性能が限られることもある。

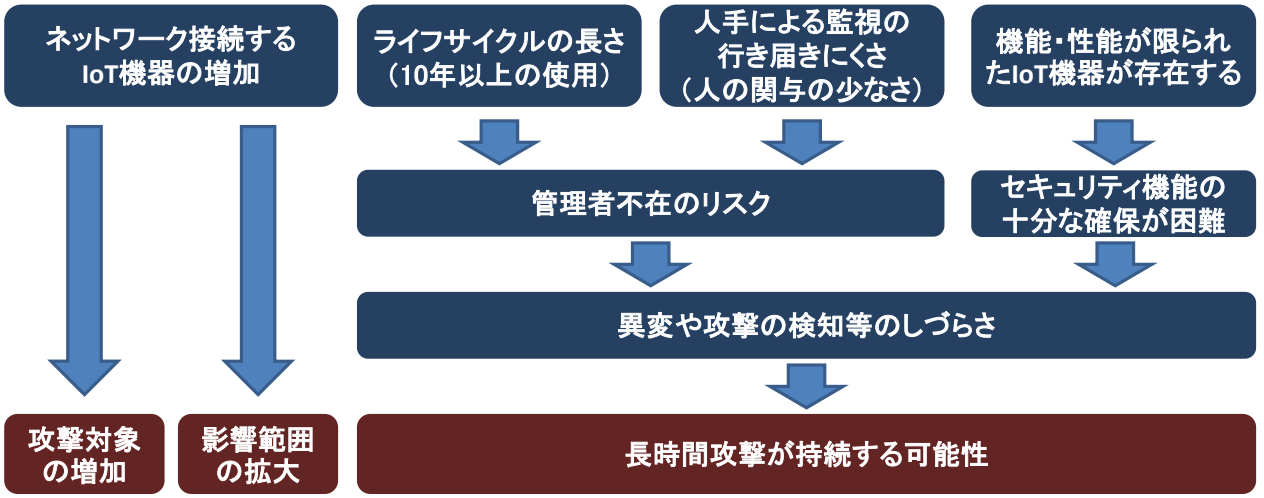
■　IoTの利活用は企業の収益性向上に不可欠なものとなっていく一方、こうしたビジネスを脅かすサイバー攻撃は避けられないリスクとなっている。サイバー攻撃によって機微な情報の流出やインフラの供給停止など社会に対して損害を与えてしまった場合、社会からの経営者のリスク対応の是非、さらには経営責任が問われることもある。

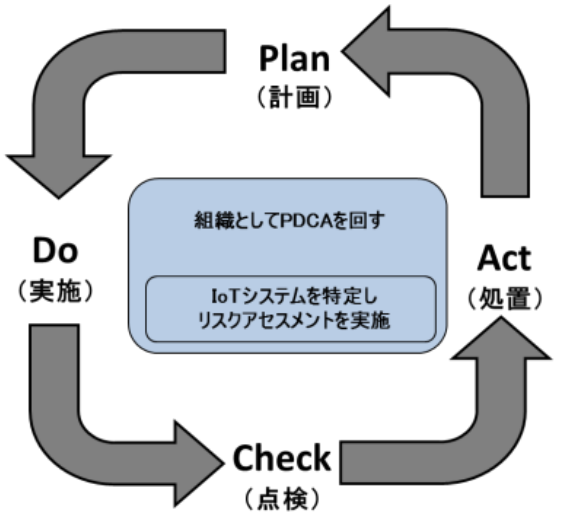
■　経営者はIoTの性質を考慮し、「サイバーセキュリティ経営ガイドライン」を踏まえ、IoTセキュリティに係る基本方針を策定し、社内に周知するとともに、継続的に実現状況を把握し、見直していく。そのために必要な体制・人材整備を行う。

○　内部不正やミスに備える

■　IoTの安全を脅かす内部不正の潜在可能性を認識し、対策を検討する。

■　関係者のミスを防ぐとともに、ミスがあっても安全を守る対策を検討する。





【分析】 指針2　IoTのリスクを認識する

○　守るべきものを特定する

■　IoT機器等が有する本来機能、セーフティを実現する機能、つなげるための機能（IoT機能）など、IoTの安全安心の観点で、守るべき機能を特定する。また、つながることで漏えいしないよう、機能の動作に関わる情報や、機器やシステムで生成される情報など、守るべき情報を特定する。

○　つながることによるリスクを想定する

■　クローズドなネットワーク向けでも、つながる機能がある機器やシステムはリスクを認識しておく。

■　他の機器とつながることにより、セキュリティ上の脅威や機器の故障の影響が波及するリスクを想定しておくことが重要。特に、セキュリティ対策のレベルが低い機器やシステムがつながると、そこが攻撃の入り口になったり、IoT全体に影響を与える可能性があることを想定しておく。

■　盗まれたり紛失した機器の不正操作などの物理的な攻撃に対するリスクも想定しておく。また、廃棄した機器からの情報漏えいの可能性も存在する。

○　過去の事例に学ぶ

■　Windowsパソコン等のITの過去事例やIoTの先行事例から攻撃事例や対策事例を学ぶ。

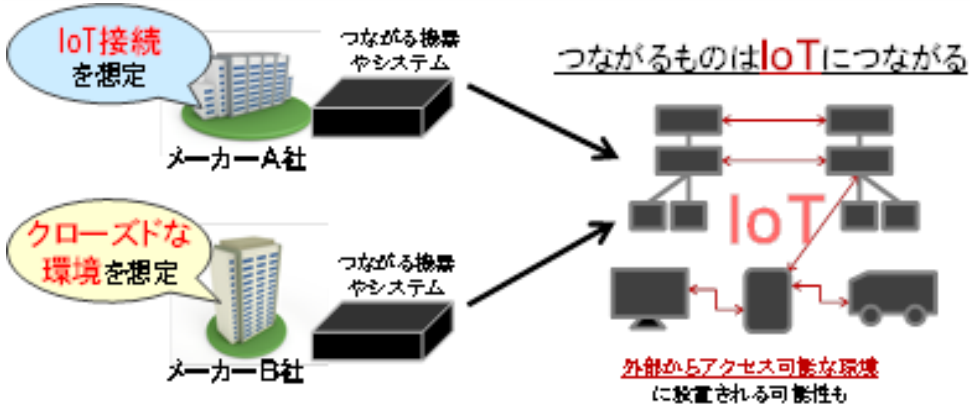
つながる世界で求められるセキュリティ対策

個別の機器・サービスのリスクから
守るべきものを守る
＝
従来の安全安心

＋

つながりによるリスクから
守るべきものを守る
＝
つながる世界の安全安心

つながるものはIoTにつながる



【設計】 指針3　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

■　IoT機器等に異常な状態が検知された場合、影響が他の機器等に波及しないよう、当該IoT機器等をネットワークから切り離す等の対策の検討が必要である。また、切り離しや機能の停止が発生した場合、他への影響を抑えるため、早期に復旧するための設計が必要である。

○　不特定の相手とつなげられても安全が確保できる設計をする

■　IoTの普及に伴い、機器メーカが意図していない不特定の機器が、インテグレータやユーザによってつなげられて利用されるケースが増えている。この状況においては、信頼性の低い機器が接続された場合に、秘密情報が簡単に漏えいしたり、あるいは想定していない動作が引き起こされてしまう可能性がある。また、同じメーカ同士の製品でも、時間が経つにつれて後から出荷された型式やバージョンが増え、接続動作確認が行われていないケースも増加する。つながる相手やつながる状況に応じてつなぎ方を判断する設計を検討する必要がある。

○　安全安心を実現する設計の評価・検証を行う

■　IoT機器等については、単独では問題がないのに、つながることにより想定されなかったハザードや脅威が発生する可能性もある。安全安心の要件や設計が満たされているかの「検証」だけでなく、安全安心の設計がIoTにおいて妥当であるかの「評価」を実施することが必要となる。

【構築】 指針4　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

■　提供するIoTシステム・サービスの機能及び用途、IoT機器の機能・性能のレベル等を踏まえ、ネットワーク構成やセキュリティ機能の検討を行い、IoTシステム・サービスを構築する。

■　また、機能・性能の制限によりIoT機器単体で必要なセキュリティ対策を実現できない場合は、セキュアなゲートウェイを経由してネットワーク接続するなどのセキュリティ対策を検討する。

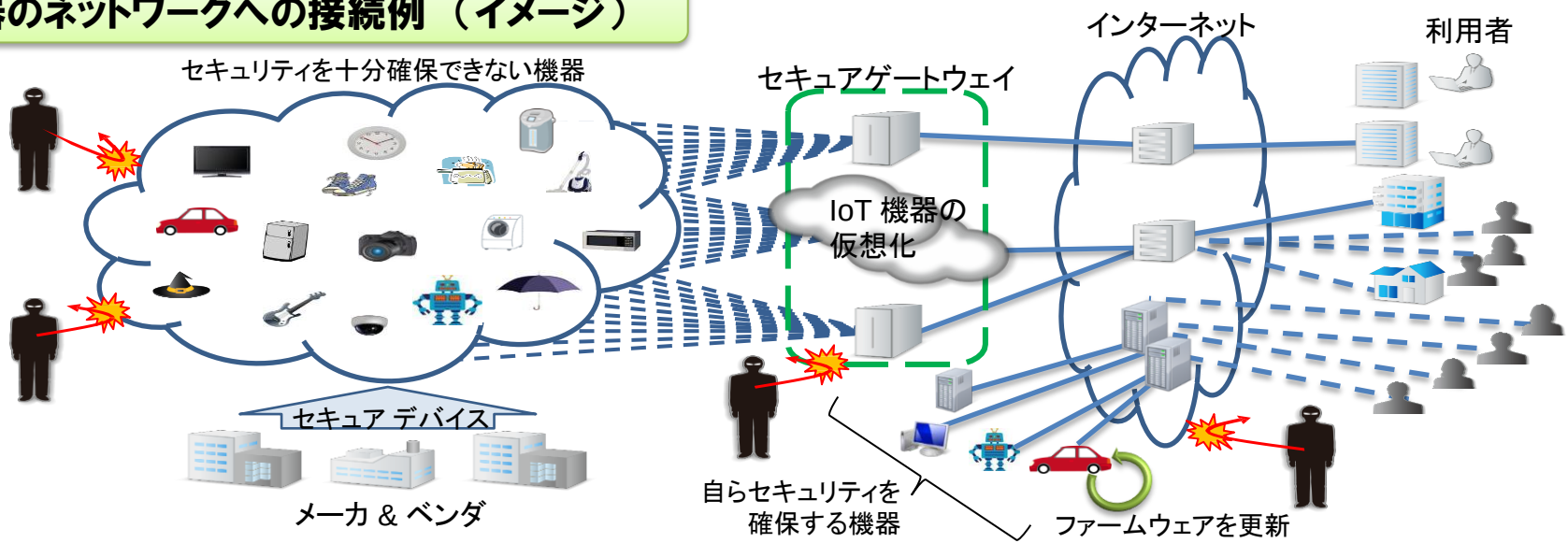
○　初期設定に留意する

■　外部から容易に攻撃可能であるような脆弱なシステム・サービスとならないよう、IoTシステム・サービスの構築時・利用開始時にセキュリティに留意した初期設定を行う。また、利用者へ初期設定に関する注意喚起を行う。

○　認証機能を導入する

■　不正なIoT機器や不正なユーザによるなりすましや盗聴等が行われないよう、認証や暗号化等の仕組みを導入する。

IoT機器のネットワークへの接続例（イメージ）



【運用・保守】 指針5 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

■ IoT機器には製品出荷後に脆弱性が発見されることがあるため、脆弱性の対策を行ったソフトウェアをIoT機器へ配布・アップデートする手段が必要である。

■ IoTシステム・サービスの提供者は、IoTシステム・サービスの分野ごとの特徴を踏まえて、IoT機器のセキュリティ上重要なアップデートを必要なタイミングで適切に実施する方法を検討し、適用する必要がある。

○ 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機器の出荷後やIoTシステム・サービスのリリース後においても、脆弱性情報を収集・分析し、ユーザや他のシステム・サービスの供給者・運用者に情報発信する。また、セキュリティに関する重要事項を利用者へあらかじめ説明する。

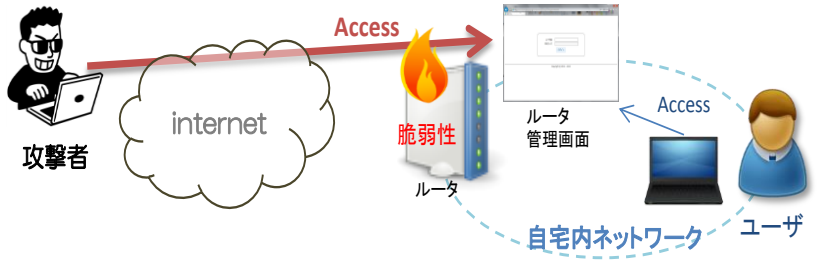
○ IoTシステム・サービスにおける関係者の役割を認識する

■ IoTシステム・サービスにおいては、多くの関係者が存在し、かつ、複雑な関係となっているため、インシデント発生時の対応が後手に回ることのないよう、事前に関係者の役割を整理して理解しておく。

○ 脆弱な機器を把握し、適切に注意喚起を行う

■ 新たに設置するIoT機器だけでなく既存のIoT機器を含めて、IoTシステム・サービスの提供範囲で、脆弱性を持つIoT機器がネットワーク上に存在していないか可能な限り把握可能な仕組みを整備もしくは利用する必要がある。 また、脆弱性を持つIoT機器を発見した場合は、当該機器を利用している一般利用者に対して、注意喚起を行う。

ルータの脆弱性を突いた攻撃事例



一般利用者のためのルール

○ 問合せ窓口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い合わせ窓口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。問合せ窓口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。

○ 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」、「他の機器とパスワードを使いまわししない」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。

○ 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。

○ 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、機器を捨てたりするなど機器を手放す時は、事前に情報を削除する。

適切な対処が困難とならないよう、問合せ窓口やサポートが明確な機器・サービスを利用する

今後の検討事項

○ リスク分析に基づく分野別の対策について

■ 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。

○ 法的責任関係について

■ IoTにおいては、製造メーカー、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。

○ IoT時代のデータ管理の在り方について

■ IoTシステムでは、利用者の個人情報等のデータを保持・管理する者もしくは場所が、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・管理することが必要であり、その具体的な方法について、検討していく必要がある。

○ IoTに対する総合的なセキュリティ対策について

■ 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。

○ 本ガイドラインの見直しについて

■ 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。