2018 年 1 月 19 日
独立行政法人情報処理推進機構（IPA）

欧州ネットワーク情報セキュリティ機関（ENISA）「IoT のベースラインセキュリティに関する提言」概要

本概要は、欧州ネットワーク情報セキュリティ機関（ENISA）発行の以下文書の概訳となります。
内容の詳細につきましては、原文をご確認ください。

Baseline Security Recommendations for IoT
https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

同ガイドは、市民の健康、安全、経済的安定の確保の観点から、モノのインターネット（IoT）に必要とされるベースラインセキュリティを提言することを目的としている。

本概要では、同ガイドのうち以下の項目の概略を日本語で紹介している（【】内はガイド中の該当する章・節番号）。

- スコープ【1.2】
- 対象読者【1.4】
- セキュリティ上の課題【2.2】
- アーキテクチャ【2.4】
- IoT 資産の分類【2.5】
- IoT に対する脅威とリスクの分類【3.2】
- 攻撃シナリオ【3.3】
- セキュリティ対策／ベストプラクティス【4.1、4.2、4.3】
- ギャップ分析【5】
- 提言【6】

また、本概要には含めないが、同ガイドには付録として以下が添付されている。

- 付録 A： セキュリティ対策／ベストプラクティス詳細（参照基準・ガイドライン情報を含む）
- 付録 B： セキュリティ対策と脅威のマッピング
- 付録 C： セキュリティ基準・参考資料一覧
- 付録 D： IoT のセキュリティインシデン事例

以降に、同ガイドの概要を記す。

IoT は、パラダイムシフトの中で技術的、社会的、経済的に重要なものへと進化を続けている。IoT が IoT の持つ最大限の可能性を発揮するためには、セキュリティおよび安全性の問題に取り組む必要がある。IoT のセキュリティおよび安全性の確保は、IoT 機器自身だけでなく、クラウド等のバックエンドのサーバやサービス、アプリケーション、保守ツールや診断ツール等の全ての関連システムのセキュリティと安全性に掛かっている。また、IoT は技術的側面だけでなく、法的、政治的、規制的側面でも、幅広く複雑な問題を提起している。

このような背景から、ENISA では IoT のセキュリティ要件、主な IoT 資産と脅威、想定される攻撃、セキュリティ対策／ベストプラクティス等に関する知見を提供するべく、本ガイドを策定した。

スコープ【1.2】

ENISA では、IoT を「意思決定を可能にする、相互接続されたセンサーやアクチュエータから成るサイバーフィジカル・エコシステム」と定義する。

対象読者【1.4】

本ガイドは主に以下の人々・組織を対象とする。

- IoT のソフトウェア開発者、製造者、利用者、運用者
- IoT の専門家、
- 情報セキュリティの専門家
- IT／セキュリティソリューション設計者
- 最高情報セキュリティ責任者（CISO）
- 重要情報インフラ防護（CIIP）の専門家

セキュリティ上の課題【2.2】

机上調査と、IoT 関係者および専門家へのヒアリングの結果、本ガイドではセキュアな IoT エコシステムを確立する上での課題として以下を挙げている。一部については 5 章（ギャップ分析）において、より詳細に解説している。

- 膨大な攻撃対象／範囲（attack surface）
- 個々の IoT 機器における限られたリソース（CPU、メモリ等）
- 複雑なエコシステム（個々の IoT 機器だけでなく、つながっている機器、システム、ネットワーク等、全体として捉える必要性）
- バラバラと断片的なセキュリティ基準や規制
- 普及の幅広さ（家庭から産業（重要インフラ）まで）
- 関係者によって異なるセキュリティ観点や要件
- 安全への影響（安全が脅かされる危険性）
- 低コスト（適切なセキュリティ対策を実装する余裕の欠如）
- IoT セキュリティに関する知識、スキル、経験を有する人材の不足
- セキュリティアップデートの問題
- “スピード重視”のセキュアでないプログラミング・開発
- 責任分界の不明確さ

アーキテクチャ【2.4】

本ガイドでは、以下の既存の IoT アーキテクチャを分析し、核となる要素を抽出してリファレンスモデルを検討した。(本概要ではリファレンスモデルは割愛。原文 Figure 4 参照)

- AIOTI High Level Architecture[1]
- FP7-ICT-IoT-A Architectural reference model[2]
- NIST Network of Things (NoT)[3]
- ITU-T IoT reference model[4]
- ISO/IEC CD 30141 Internet of Things Reference Architecture (IoT RA)[5]
- ISACA Conceptual IoT Architecture[6]
- oneM2M Architecture Model[7]
- IEEE P2413 – Standard for an Architectural Framework[8]

IoT 資産の分類【2.5】

本ガイドでは、IoT のセキュリティの検討にあたって主な IoT 資産をリストアップし、Table 2 にまとめている。中でも★のついている資産は、IoT 関係者および専門家へのヒアリングにおいて 3 分の 2 以上が「致命的(critical)」と回答した資産であり、セキュリティを検討する上で優先すべき資産と考えられる。

(原文)Table 2: IoT 資産の分類(1/2)(#は追加、概要は抜粋)

#	資産グループ	資産	概要
1	IoT 機器	ハードウェア	IoT 機器を構成する、センサー、アクチュエータ以外の物理的コンポーネント。マイクロコントローラ、マイクロプロセッサ、物理ポート等を含む。
		ソフトウェア	IoT 機器の OS、ファームウェア、プログラム、アプリケーション。
		センサー★	温度、運動等のイベントを検知/測定して他機器に送信するサブシステム。
		アクチュエータ	処理データに基づき決まった動作を実行する IoT 機器の出力ユニット。
2	IoT エコシステムを為すその他の機器	モノとの IF となる機器	IoT 機器間のインターフェース(IF)またはアグリゲーター(収集・集約)の役割を果たす機器。人と IoT 機器との IF となる機器。
		モノを管理する機器	IoT 機器やネットワークを管理する機器。
		組込システム	自らデータ処理を行う処理ユニットを持つシステム。組込センサー、組込アクチュエータ、直接クラウドに接続するネットワーク機能等を含む。
3	通信	ネットワーク	IoT エコシステム内の異なるノード間のデータおよび情報のやり取りを可能にするデータリンク。
		プロトコル★	複数の IoT 機器があるチャンネルで通信を行う際に従うべき一連の規則。

[1] https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-WG3-IoT-High-Level-Architecture-Release_2_1.pdf
[2] http://www.meet-iot.eu/deliverables-IOTA/D1_5.pdf
[3] http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-183.pdf
[4] https://www.itu.int/rec/T-REC-Y.2060-201206-I
[5] https://www.w3.org/WoT/IG/wiki/images/9/9a/10N0536_CD_text_of_ISO_IEC_30141.pdf
[6] https://www.isaca.org/Journal/archives/2017/Volume-3/Pages/default.aspx
[7] http://www.onem2m.org/images/files/deliverables/Release2/TS-0001-%20Functional_Architecture-V2_10_0.pdf
[8] https://standards.ieee.org/develop/project/2413.html

（原文）Table 2: IoT 資産の分類（2/2）（概要は抜粋、#は追加））

#	資産グループ	資産	概要
4	インフラ	ルータ	IoT エコシステム内の異なるネットワーク間でデータパケットを転送するネットワーク機器。
		ゲートウェイ★	異なるプロトコルを使用しているネットワーク間のインターフェースとなるネットワーク機器。
		電源	IoT 機器および内部コンポーネントに電力を提供する機器。
		セキュリティ機器	IoT 機器、ネットワーク、情報のセキュリティのための機器。ファイアウォール、WAF、CASB、IDS/IPS 等を含む。
5	プラットフォーム & バックエンド	ウェブベースのサービス	ウェブインターフェースを持つサービス。
		クラウドインフラ、サービス	分散した機器からのデータ収集・処理に利用。また、演算機能、データの保存場所、アプリケーション、サーバ等も提供。
6	意思決定	データマイニング	収集したデータを処理し、別の目的で利用するため特定の構造に加工するアルゴリズムおよびサービス。膨大なデータからパターンを見つけ出すためにビックデータ技術を利用。
		データ処理・演算	収集したデータから意味のある情報を抽出するため処理するサービス。機械学習技術も利用。
7	アプリケーション & サービス★	データ分析・可視化	新たなパターンの発見や効率化のため、データ収集・処理した情報を分析・可視化。
		機器・ネットワーク管理★	IoT エコシステム内の機器の OS、ファームウェア、アプリケーションのアップデートや、ログ収集等による機器やネットワークの監視。
		機器使用情報	IoT エコシステム内の機器やネットワークのステータス、使用パターン、パフォーマンス等の把握。
8	情報	保存状態	クラウド上のデータベースや機器に保存された情報。
		転送状態	IoT ネットワーク上を流れている情報。
		使用状態	アプリケーション、サービス、IoT 資産が使用中の情報。

IoT に対する脅威とリスクの分類【3.2】

IoT のインシデントは、スマートメーターの電力使用量改ざん、家庭用 IP カメラの覗き見、走行中の車両のハッキング、マルウェア感染によるルータやスマート家電のボット化、ランサムウェア感染による身代金要求等、様々な事例が報告されている。（事例の一覧は付録 D に掲載）

本ガイドでは、IoT のセキュリティの検討にあたって、IoT 資産に対する主な脅威およびリスクをリストアップし、Table 3 にまとめている。

（原文）Table 3：IoT に対する脅威とリスクの分類（概要は抜粋、影響資産は番号で記載）

分類	脅威	概要	影響資産（資産 G #）
不正操作／悪用	マルウェア	ユーザの同意なく、望まぬ行為や不正な行為を行うプログラム。	1,2,5
	攻撃ツール	脆弱性を悪用して不正アクセスを図るコード。	1,2,4
	標的型攻撃	特定の攻撃対象に対し、長期間を掛けて段階的に行われる攻撃。気づかれずにできるだけ多くの重要な情報／権限を入手することを主な目的とする。	4,5,8
	DDoS	複数システムから１攻撃対象に集中攻撃を行い、シャットダウンさせる攻撃。	1,2,5,4
	不正機器	機器のなりすまし。バックドアがあり、攻撃の実行に使われることも多い。	1,2,4
	プライバシー侵害	ユーザのプライバシーを侵害する。または、ネットワーク上の機器を第三者に晒す。	1,2,5,8
	情報改ざん	機器の損壊でなく、情報の改ざんによる混乱の引き起こし、または金銭の取得を目的とする。	1,2,5,8
盗聴／傍受／ハイジャック	中間者攻撃	メッセージを能動的に窃取し、送受信者にメッセージの中間窃取があったことを気づかれないよう、メッセージを中継する。	8,3,1
	IoT 通信プロトコルのハイジャック	既存の通信セッションを乗っ取り、パスワード等の重要情報を入手する。	8,3,1,6
	情報傍受	電話やメール等の私的通信の盗聴（時には改ざんも）。	8,3,1
	ネットワーク情報収集	接続機器、使用プロトコル、空いているポートやサービス等のネットワーク情報の受動的窃取。	8,3,1,4
	セッションハイジャック	正規ホストになりすまし、コネクションを乗っ取る。	8,3,1
	情報収集	接続機器、使用プロトコル、空いているポートやサービス等の内部ネットワーク情報の受動的窃取。	8,3,1
	リプレイ攻撃	正規のデータ送信を再送信し、不正操作またはシステムダウンさせる攻撃。	8,1,6
サービス停止	ネットワーク障害	故意または過失によるネットワークの妨害・遮断。	4,3
	機器障害	ハードウェアの誤作動・障害。	1
	システム障害	ソフトウェアサービスまたはアプリケーションの障害。	1,5,2
	サポートサービスの停止	情報システムの正しい運用に必要なサポートサービスの利用不可。	全ての IoT 資産
損壊／喪失	データ／機微な情報の漏洩	故意または過失による機微な情報の漏洩。	1,2,5,8
障害／誤動作	ソフトウェア脆弱性	弱いパスワード・デフォルトパスワード、ソフトウェアのバグ、設定ミス等。	1,2,5,4,7
	第三者要因	稼働中の IoT 資産に直接的な影響を持つ別の IoT 資産の設定ミス。	1,2,5,4,7
災害	天災	洪水、強風、豪雪、土砂崩れ等による機器の物理的な損壊。	1,2,5,4
	環境	機器が設置された場所の環境的要因による機器の動作不能。	2,5,4
物理攻撃	機器障害	機器の改ざん。	3,1
	機器破壊	機器の窃取、爆破、破壊等。	1,2,5,4

攻撃シナリオ【3.3】

本ガイドでは、IoT のセキュリティの検討にあたって、IoT 資産に対する主な攻撃シナリオをリストアップし、Table 4 にまとめている。

中でも★のついている攻撃シナリオは、IoT 関係者および専門家へのヒアリングにおいてトップ 3 に選ばれたシナリオであり、セキュリティ対策を検討する上で優先すべきシナリオと考えられる。これらのトップ 3 の攻撃シナリオについては、3.4 節でより詳細に解説している。

（原文）Table 4：攻撃シナリオ（3.3 本文から一部補足）

攻撃シナリオ	重要度
1. コントローラとアクチュエータの間のネットワークに対する攻撃★ → 盗聴による機微な情報、運用情報の漏洩	高ー致命的
2. センサーの測定値、閾値、設定の改ざん★ → 不正な値の受入れ、上位システムへの送信による物理的損壊	高ー致命的
3. アクチュエータの設定の改ざん★ → 製造プロセスへの影響	高ー致命的
4. IoT の管理システムに対する攻撃 → IoT の不正操作・停止による、人、環境、他システム等への影響	高ー致命的
5. プロトコルの脆弱性の悪用 → 侵入口としての利用、通信の遮断・不安定化	高
6. システムコンソールからの機器に対するコマンド挿入 → 他機器への侵入拡大	高ー致命的
7. 踏み台としての悪用 → 他機器への攻撃	中ー高
8. ボット化による DDoS への悪用 → 標的機器やネットワークのシャットダウン	致命的
9. 電源情報の改ざん → 意図せぬ節電モードへの移行、シャットダウン	中ー高
10. ランサムウェア → 制御の乗っ取りによる身代金の要求	中ー致命的

セキュリティ対策／ベストプラクティス【4.1、4.2、4.3】

本ガイドでは、既存の IoT に関するセキュリティガイドラインや基準（付録 C に掲載）をベースに、IoT のセキュリティ対策／ベストプラクティスを、3 分類、24 項目、83 要件にまとめている。

- ポリシー（PS）： 4 項目 12 要件
- 組織的、人的、運用的対策（OP）： 5 項目 14 要件
- 技術的対策（TM）： 15 項目 57 件

以下にセキュリティ対策／ベストプラクティスの分類と項目をまとめる。（各要件の詳細については割愛。原文 4.1 節～4.3 節、および付録 A を参照）

セキュリティ対策／ベストプラクティスの分類と項目

ポリシー（12 要件）		詳細要件
	セキュリティ・バイ・デザイン（7）	GP-PS-01～GP-PS-07
	プライバシー・バイ・デザイン（2）	GP-PS-08～GP-PS-09
	資産管理（1）	GP-PS-10
	リスクおよび脅威の特定と評価（2）	GP-PS-11～GP-PS-12
組織的、人的、運用的対策（14 要件）		**詳細要件**
	製品ライフサイクルを通じたサポート（3）	GP-OP-01～GP-OP-03
	有効性が確認されているセキュリティ対策の利用（1）	GP-OP-04
	セキュリティ脆弱性／インシデント管理（4）	GP-OP-05～GP-OP-08
	セキュリティ教育（3）	GP-OP-09～GP-OP-11
	第三者組織とのセキュリティに関する取り決め（3）	GP-OP-12～GP-OP-14
技術的対策（57 要件）		**詳細要件**
	ハードウェアセキュリティ（2）	GP-TM-01～GP-TM02
	信頼性／完全性管理（5）	GP-TM-03～GP-TM-07
	堅牢なデフォルトセキュリティ／プライバシー設定（2）	GP-TM-08～GP-TM-09
	データ保護／法規へのコンプライアンス（5）	GP-TM-10～GP-TM-14
	システムの安全性／信頼性（3）	GP-TM-15～GP-TM-17
	セキュアなソフトウェア／ファームウェアアップデート（3）	GP-TM-18～GP-TM-20
	認証（6）	GP-TM-21～GP-TM-26
	認可（2）	GP-TM-27～GP-TM-28
	アクセス制御（5）	GP-TM-29～GP-TM-33
	暗号化（4）	GP-TM-34～GP-TM-37
	セキュアで信頼のおける通信（9）	GP-TM-38～GP-TM-46
	セキュアなインターフェース／ネットワークサービス（7）	GP-TM-47～GP-TM-53
	セキュアな入力／出力処理（1）	GP-TM-54
	ログの取得（1）	GP-TM-55
	監視／監査（2）	GP-TM-56～GP-TM-57

ギャップ分析【5】

本ガイドでは、IoT のサイバーセキュリティに関する現状とあるべき状態のギャップとして、以下の 6 点を挙げている。

- Gap 1: バラバラで断片的なセキュリティアプローチや規制
  EU レベルでの成熟した IoT セキュリティフレームワークが無いこと、規制がバラバラで断片的であること、IoT の幅広さ故に検討事項が業界や製品によって多様であること、関係者の責任分界が不明確であること等から、多くの企業やメーカーが独自のアプローチで IoT セキュリティに取り組む状況を生んでいる。

- Gap 2: セキュリティ意識の低さ
  全体的に IoT に対する脅威が理解されておらず、従ってセキュリティの必要性に対する認識が低い。IoT 世代のユーザ、開発者、メーカー等に対して、IoT が個々の機器の問題でなく IoT エコシステム全体の問題であること、また、IoT のリスクおよび対策について教育する必要がある。

- Gap 3: 設計・開発におけるセキュリティの欠如
  インセキュリティ・バイ・デザイン、通信セキュリティの欠如、アップデートに関する認証・認可の弱さ、ハードニング（堅牢化）の欠如、既知の脆弱性へ未対応、不要なポート／サービスの開放、弱いパスワードの使用等が見られる。

- Gap 4: IoT 機器、プラットフォーム、フレームワーク間の相互運用性の欠如
  Gap 1 に述べた共通のアプローチや規制の欠如等から、多くの企業やメーカーが独自に開発を進め、相互運用性の問題が発生している。

- Gap 5: 経済的インセンティブの欠如
  多くの場合、企業やメーカーはセキュリティよりも機能性やユーザビリティを重視しており、セキュリティに予算を掛けていない。これは SROI（Security Return on Investment）が低い／ないと認識されているほか、セキュリティに注力するインセンティブがないこと等が理由として挙げられる。

- Gap 6: 適切な製品ライフサイクルマネジメントの欠如
  設計段階でのセキュリティの欠如、市場投入後の脆弱性対応や問題を早期に検知する仕掛けを含め、製品の適切なライフサイクルマネジメントが為されていない。IoT エコシステムでは一般的に IoT 機器のセキュリティおよび安全性に関するユーザの基本的な理解が低いため、ユーザ任せではアップデート等が為されず、セキュリティインシデントにつながる可能性がある。

提言【6】

本ガイドでは、IoT セキュリティ改善のための提言として、以下の 7 点を挙げている。

- 提言 1: IoT セキュリティへの取組みおよび規制の調和・調整
  欧州委員会（EC）がファシリテーターとなり、IoT に関する欧州共通のガイドラインやセキュリティ基準を確立し、EC および加盟国政府が関係者間の調和・調整を行う。また、調達力を活用し、ガイドラインや基準（ベースラインセキュリティ）の導入を促進する。

- 提言 2: IoT セキュリティの必要性の普及啓発
  開発者、産業界、ユーザ等、それぞれの関係者ごとに、IoT に対する脅威とリスク、セキュリティを確保する方法について教育を行う。開発者／産業界には（共通の）フレームワークや基準、ベストプラクティス、最新の技術等を周知して導入を奨励し、ユーザにはセキュアな製品・サービスの購入を促進し、ユーザが実施すべき基本的なセキュリティ対策を教育する。また、若い世代への周知のため、学校や大学等での教育に組み込むことが考えられる。

- 提言 3: IoT 向けのセキュアなソフトウェア／ハードウェアの開発ライフサイクルに関するガイドラインの策定
  セキュリティおよびプライバシーを考慮したセキュアな製品・サービスの開発ライフサイクルを定義し、開発者およびメーカーにおける各社の IoT 開発プロセスへの組込みを促進する。

- 提言 4: IoT エコシステムの相互運用性に関するコンセンサスの確立
  相互運用性フレームワークのセキュリティ機能の透明性を確保すると共に、セキュリティ機能の高いオープンな相互運用性フレームワークの利用を奨励し、そのようなフレームワークへの準拠を認定するオープン且つ利用しやすい相互運用性の検証機関やテストベットを増やす。

- 提言 5: IoT セキュリティを促進するための経済的・経営的インセンティブの提供
  ユーザのセキュリティ意識が上がることでメーカーがセキュリティに取り組まざるを得なくなるよう、国がユーザのセキュリティ教育を促進するほか、セキュリティ基準を含むセキュリティフレームワークを策定し、認証制度等と併せて導入を奨励する。

- 提言 6: セキュアな IoT 製品／サービスのライフサイクルマネジメントの確立
  メーカーは、設計・開発から製造終了、サポート終了まで、セキュリティを組み込んだ IoT 製品／サービスのライフサイクルマネジメントを確立する。販売後も、サポート終了までは、ユーザが特別な知識や新たな費用負担なしにセキュリティに関するアップデートが受けられるようにする。

- 提言 7: IoT 関係者の責任分界の明確化
  IoT に関する多様な関係者の責任分界について議論し、EU レベルおよび各加盟国の法規において明確化する。

以上