セキュア IoT プラットフォーム協議会

IOT セキュリティ手引書

Ver.1.0

セキュリティ仕様検討部会

2020 年 11 月 10 日　初版

目次

1. はじめに

1.1. 目的

本書では、IoT セキュリティで必要となる項目について、国際電気標準会議（IEC）が開発した産業システムにおけるセキュリティ規格である IEC62443 のうち、産業機器開発者向けの規格である IEC62443-4 を基準に解釈と差異を取りまとめるものとします。

本協議会では様々な分野の会員の方々から、それぞれの分野で必要と考えられる IoT セキュリティの課題と対応策について意見を収集してきました。これらの意見を集約するにあたり、網羅性の観点から IEC62443-4 を基準とし、基準の検証を行いました。本書は 2020 年度の協議会の成果として発表する予定です。

1.2. 対象読者

本書の対象読者は、IoT システムの提供に関わる事業者を想定しています。具体的には IoT クラウドサービス事業者、IoT クライアントデバイス製造事業者、およびこれらの機能を活用しカスタマーヘトータルのサービスとして供給する事業者を指します。

また本書では IEC62443-4 については解説をしていません、そのため本書の読者は IEC62443-4 の予備知識があることを前提としています。

1.3. 登録商標について

本書に記載されているすべての製品名は、それぞれの会社の登録商標または商標です。

1.4. ドキュメントの構成

本書は次に示す主要な項目で構成されています。

- 「2. 検討モデル」では IoT システムの階層モデルとして本書で述べる項目の全体像について記載しています。
- 「3. フェーズ別考察」では主に製品ライフサイクルを前提とした分類に従い、それぞれの分類における解釈と検証の結果を記載しています。
- 付録 A では、本書を作成するにあたり登場した略語のリストを掲載しています。
- 付録 B では、本書を作成するにあたり必要となった用語の用語集を掲載しています。

2. 検討モデル

IoT システムのセキュリティを検討するにあたり、機能の外部インターフェースや H/W そのもの強度など様々な側面からの検討が必要です。本書では、これらを製品のライフサイクルを基軸とした「IoT システムの階層モデル」をベースに検討し、まとめています。

2.1. IoT システムの階層モデル

IoT システムは「図 2-1　IoT セキュリティ総合対策モデル」の水平方向の分類に示されるように、サービス層／プラットフォーム層／ネットワーク層／デバイス層に分けられます。また、垂直方向の分類では設計・製造／サービス運用／廃棄という製品のライフサイクルにより分けられています。

図 2-1　IoT セキュリティ総合対策モデル

機器開発における現実の役割分担を反映するため、垂直方向の分類となる、製品のライフサイクル（設計・製造／サービス運用／廃棄）を「企画」「設計」「開発」「製造」「量産」「運用」「廃棄」に細分化しました。

2.2. 検討フェーズ

各ライフサイクルフェーズの検討に当たっては、参加会員の機器開発現場での経験に照らし合わせ、それぞれのフェーズで解釈・検証方法を提供いただき、さらに注釈となる部分について広く情報を収集しました。

2.2.1.検討フェーズ詳細

収集した情報の整理の過程で、特に「設計」「開発」のフェーズでは「図 2-2　IoT 機器の H/W 製造プロセスと S/W 開発プロセス」に示されるよう、H/W と S/W でセキュリティ対策に差異があることが判明しました。本書では、「設計」を「アーキテクチャ設計」「H/W 設計」「S/W 設計」に分けさらに「開発」を「H/W 開発」「S/W 開発」に分けることでこの差異へ対応しています。

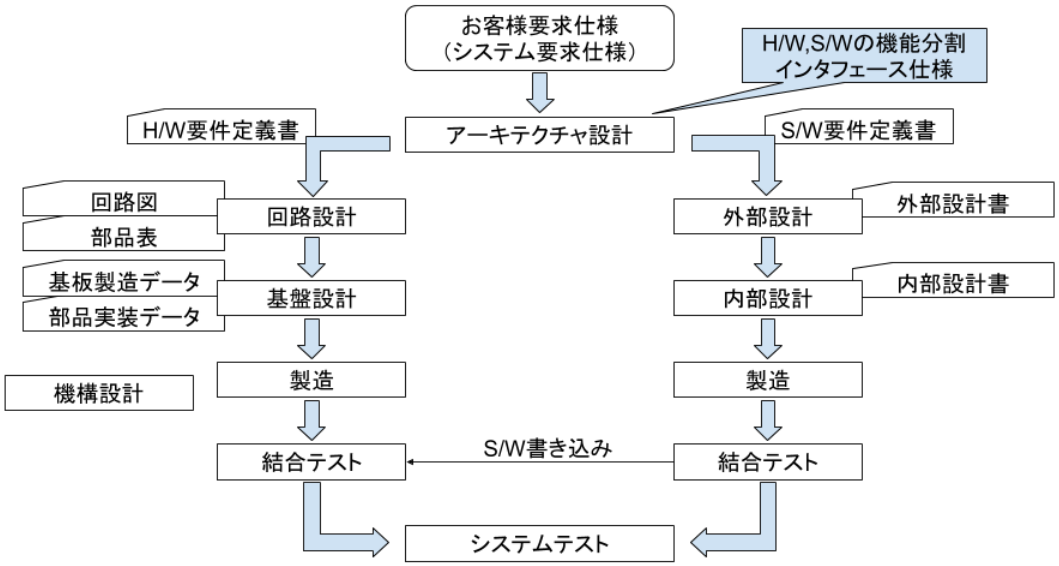

図 2-2　IoT 機器の H/W 製造プロセスと S/W 開発プロセス

これらフェーズをあらためて整理すると「表 2-1　IoT 機器の製品ライフサイクル」のように整理できます。続く章ではそれぞれのフェーズごとに要件と対策をまとめています。本書を参照される各位が個々に該当する項を中心に参照いただくことにより、本書の適用が高まることを期待しています。

表 2-1　IoT 機器の製品ライフサイクル

フェーズ名		備考
企画		おもに製品計画を指す。
設計	アーキテクチャ設計	H/W と S/W それぞれに機能を分解する。
	ハードウェア設計	回路設計、基板設計、機構設計を指す。
	ソフトウェア設計	外部設計、内部設計を指す

選定		S/W で機能を作るか H/W で調達するかを選定する。
開発	ハードウェア開発	H/W 設計に基づいて H/W を開発することを指す。
	ソフトウェア開発	S/W 設計にも続いて S/W を開発することを指す。
製造		S/W 開発を受け H/W を製造する。このフェーズで H/W にに S/W を書き込む
調達		量産に向けて部品の調達をする。
量産		製造した製品を販売に向けて量産する。
販売		ここでは検討の範囲外とする。
運用		量産された製品が販売され、運用にいたる。
廃棄		運用が終了し、製品のライフサイクルが終了する。再利用により運用に戻すフェーズもここに含むものとする。

2.2.2. 謝辞

本書の執筆にあたっては、様々な方々から意見をいただきました。特に検討に参加いただいた方々に感謝いたします。

インタープラン株式会社　武田 洋一様
サイバートラスト株式会社　東 久貴様　田上 利博様　豊島 大朗様（座長）
ソリトンシステムズ　高村 和久様
大日本印刷株式会社　平野 晋健様　高田 憲一様
トレンドマイクロ株式会社　原 聖樹様
中央大学研究開発機構　山澤 昌夫様
トッパン・フォームズ　石井 朋和様
株式会社ユビキタス AI コーポレーション　岡崎 真也様
ラピスセミコンダクタ株式会社　坂東 和彦様
ワンビ株式会社　加藤 貴様

3. フェーズ別考察

3.1. 企画フェーズ

企画フェーズとは、IoT 機器の新製品計画として顧客（市場）開拓、新機能開発・改良、販売（価格・商標）、供給、製品廃棄をあらかじめ想定し検討するフェーズを指します。なお、製品廃棄に関しては廃棄フェーズとしてさらに深く考察をします。

3.1.1.解釈

製品の企画段階でのセキュリティ対策は、製品の取り扱うデータもしくは装置自体の重要性が高い場合に適用すべきです。IoT 機器の企画段階のセキュリティ対策項目としては「セキュリティ対策基本方針」「セキュリティ対策体制」「脅威・リスク分析」「セキュリティ要件抽出」「顧客側セキュリティ要件収集」「セキュリティ教育」「サプライチェーン管理方針策定」「セキュリティ対策費用の盛り込み」を考慮する必要があります。また、「脅威・リスク分析」に対しては製品の技術ドメイン・機能を考慮し、セキュリティの要件を定めるべきです[1]。

3.1.2.検証

IEC62443-4 には企画に関連する規定は見当たりません。

3.2. アーキテクチャ設計フェーズ

アーキテクチャ設計フェーズは、機器の設計をするにあたり機能の実装を H/W で行うのか S/W で行うのかを分解するためのフェーズです。本節に続くハードウェア設計、ソフトウェア設計の各フェーズにおいては、本節の要請を具体化するべく機能分担、負荷分担を行うことが必須です。

3.2.1.解釈

アーキテクチャ設計フェーズでは、セキュリティデータや処理をアーキテクチャ上でどのように守るのか、破られた場合も被害を最小限にするための分散化をどのように考える

[1] セキュリティ要件確認支援ツール　https://isec-sras.ipa.go.jp/

べきかをシステム全体のアーキテクチャとして設計します。セキュリティポリシーを確立することも重要です。

セキュリティの実装確認には、構造解析ツールを用います。構造解析ツールにはUnderstand（テクマトリクス）,Rezolver（DTS インサイト）などがあります。

3.2.2.検証

本フェーズは未検証です。

3.3. ハードウェア設計フェーズ

ハードウェア設計フェーズでは、アーキテクチャ設計フェーズで分解した、ハードウェアにて実装するセキュリティ機能について設計します。

3.3.1.解釈

この節、ハードウェア設計フェーズでは、IoT 機器の全体設計の、ハードウェアの設計フェーズについて、IoT 機器の機能発現に際して、ユーザの正当性を担保する「ユーザ認証」、機能への「アクセス制御」、ならびに、制御通信のセッション管理や URL パラメータの適正化、文字列処理の安全性、サイトデザイン、およびログプロセス等々、に関するセキュリティ要素を網羅しなければなりません。

3.3.2.検証

3.3.2.1. 脅威と基準

1） ユーザ認証

ユーザ認証する際に入力させるパスワード情報は、画面表示上は隠蔽する。

また入力された情報の取扱いについては、ハッシュ化させるなど直値を使用しない仕組みを設ける。

一度設定をしておくと、しばらくの間はパスワードを入力せずにログインできる「自動ログインログファイルには、改ざん防止、削除防止を施す。

2） アクセス制御

認証されたユーザ情報からアクセス許可テーブルを引き、認証ユーザが許可（パーミッション）を得ているコンテンツのみを表示する設計とする。

3） セッション管理、URL パラメータ

認証済みのセッションが一定時間以上アイドル状態にあるときはセッションタイムアウトとし、サーバ側でセッションを破棄しログアウトする。

4）文字列処理の安全性

クロスサイトスクリプティング（XSS）対策を講じる。

5）サイトデザイン

入力フォームのある画面は https である。

6）ログ

ログ取得、集積に際しては改竄防止、削除防止機能が付加されている。

3.3.2.2. 対策

・設計レビューにてセキュリティ要件が基準に達しているかを審査する。

・レビューツール

Lightning Review(デンソークリエイト)など

悪意のある（悪意がなくても誤った利用も想定した）ユーザからの利用を守るための、認証（Authentication）、認可(Authorization)などの仕組みを組み入れ、また仮になりすまされた場合にも機能を安全に利用させるための設計を実施します。

3.3.2.3. IEC62443-4 該当項目

本フェーズは未検証です。

3.4. S/W 設計フェーズ（設計フェーズ）

S/W 設計フェーズでは、IoT 機器の全体設計の、S/W の設計フェーズについて要求されるセキュリティ要素の説明、その組込み、結果としての設計品質の確認、検証、考慮事項について説明します。

3.4.1.解釈

IoT 機器の S/W 設計フェーズでは、大別して「セキュリティアーキテクチャ設計」「セキュリティ機能設計」「セキュアコーディングガイド定義」を検討する必要があります。

さらに、「セキュリティ機能設計」の項目として「ユーザ認証」「アクセス制御」「セッション管理」「URL パラメータ」「文字列処理」「サイトデザイン」「ログ」を検討する必要があります。

3.4.2.検証

本フェーズは未検証です。

3.4.2.1. ユーザ認証

1） 基準

ユーザ認証する際に入力させるパスワード情報は、画面表示上は隠蔽する。

また入力された情報の取扱いについては、ハッシュ化させるなど直値を使用しない仕組みを設ける。

一度設定をしておくと、しばらくの間はパスワードを入力せずにログインできる「自動

ログインログファイルに改ざん防止、削除防止を施す。

2） 評価方法

設計レビューにてセキュリティ要件が基準に達しているかを審査する。

・レビューツール

Lightning Review(デンソークリエイト)など

3） 備考

悪意のある（悪意がなくても誤った利用も想定した）ユーザからの利用を守るための、認証（Authentication）、認可(Authorization)などの仕組みを組み入れ、また仮になりすまされた場合にも機能を安全に利用させるための設計を実施する。

3.4.2.2. アクセス制御

1） 基準

認証されたユーザ情報からアクセス許可テーブルを引き、認証ユーザが許可（パーミッション）を得ているコンテンツのみを表示すること。

2） 評価方法

設計レビューにてセキュリティ要件が基準に達しているかを審査する。

・レビューツール

Lightning Review(デンソークリエイト)など

3） 備考

悪意のある（悪意がなくても誤った利用も想定した）ユーザからの利用を守るための、認証（Authentication）、認可(Authorization)などの仕組みを組み入れ、また仮になりすまされた場合にも機能を安全に利用させるための設計を実施する。

3.4.2.3. セッション管理

1） 基準

認証済みのセッションが一定時間以上アイドル状態にあるときはセッションタイムアウトとし、サーバ側でセッションを破棄しログアウトすること。

2） 評価方法

設計レビューにてセキュリティ要件が基準に達しているかを審査する。

・レビューツール

Lightning Review(デンソークリエイト)など

3） 備考

悪意のある（悪意がなくても誤った利用も想定した）ユーザからの利用を守るための、認証（Authentication）、認可(Authorization)などの仕組みを組み入れ、また仮になりすまされた場合にも機能を安全に利用させるための設計を実施する。

3.4.2.4. URL パラメータ

1） 基準

URL パラメータにユーザ ID やパスワードなどの秘密情報を格納しない。

2） 評価方法

設計レビューにてセキュリティ要件が基準に達しているかを審査する。

・レビューツール

Lightning Review(デンソークリエイト)など

3） 備考

悪意のある（悪意がなくても誤った利用も想定した）ユーザからの利用を守るための、認証（Authentication）、認可(Authorization)などの仕組みを組み入れ、また仮になりすまされた場合にも機能を安全に利用させるための設計を実施する。

3.4.2.5. 文字列処理

1） 基準

クロスサイトスクリプティング（XSS）対策を講じる。

2） 評価方法

設計レビューにてセキュリティ要件が基準に達しているかを審査する。

・レビューツール

Lightning Review(デンソークリエイト)など

3） 備考

悪意のある（悪意がなくても誤った利用も想定した）ユーザからの利用を守るための、認証（Authentication）、認可(Authorization)などの仕組みを組み入れ、また仮になりすまされた場合にも機能を安全に利用させるための設計を実施する。

3.4.2.6. サイトデザイン

1) 基準

入力フォームのある画面は https である。

2) 評価方法

設計レビューにてセキュリティ要件が基準に達しているかを審査する。

・レビューツール

Lightning Review(デンソークリエイト)など

3) 備考

悪意のある（悪意がなくても誤った利用も想定した）ユーザからの利用を守るための、認証（Authentication）、認可(Authorization)などの仕組みを組み入れ、また仮になりすまされた場合にも機能を安全に利用させるための設計を実施する。

3.4.2.7. ログ

1) 基準

ログファイルに改ざん防止、削除防止を施す。

2) 評価方法

設計レビューにてセキュリティ要件が基準に達しているかを審査する。

・レビューツール

Lightning Review(デンソークリエイト)など

3) 備考

悪意のある（悪意がなくても誤った利用も想定した）ユーザからの利用を守るための、認証（Authentication）、認可(Authorization)などの仕組みを組み入れ、また仮になりすまされた場合にも機能を安全に利用させるための設計を実施する。

3.4.2.8. セキュアコーディングガイド定義

1) 基準

セキュアなコーディングを行うためのルールや指針を定義する。

CERT C や CWE など引用元を定義することでよいが、引用元がない場合は独自定義する。

2) 備考

IPA では、「共通脆弱性タイプ一覧 CWE 概説」というページがある。
（https://www.ipa.go.jp/security/vuln/CWE.html）

3.5. 選定フェーズ

選定フェーズとは、IoT 機器の S/W 設計と H/W 設計を受け機能の一部を外部調達する場合の製品選択を指します。

3.5.1.解釈

本フェーズは未解釈です。

3.5.2.検証

本フェーズは未検証です。

3.6. ハードウェア開発フェーズ

ハードウェア開発フェーズとは、ハードウェア設計フェーズを受けて実際に機器を実装ために、ハードウェアでの開発および基本的な検査を行うフェーズです。

3.6.1.解釈

IoT 機器のハードウェア開発フェーズでの検討項目としては、動的な「脆弱性検査（システムセキュリティ検査）」、「Web アプリケーションセキュリティ検査」、「ファジングによるセキュリティ検査」、「ペネトレーションテスト」があげられます。

3.6.2.検証

本フェーズは未検証です。

3.7. ソフトウェア開発フェーズ

ソフトウェア開発フェーズとは、ソフトウェア設計フェーズを受けて実際に機器を実装ために、ソフトウェアでの開発および基本的な検査を行うフェーズである。

3.7.1.解釈

IoT 機器のソフトウェア開発フェーズでの検討項目としては、ソースコードレビューによる「ソースコードセキュリティ検査（静的テスト）」、静的な「脆弱性検査（システムセキュリティ検査）」があげられます。

3.7.2.検証

本フェーズは未検証です。

3.8. 製造フェーズ

製造フェーズとは、開発フェーズで検査済みのハードウェアとソフトウェアを組み合わせ、試作品を作成するフェーズを指し、実機を使って様々な検査を行うフェーズです。

3.8.1.解釈

IoT 機器の製造フェーズでの検査項目としては、筐体開封などの「機器に対する物理的な攻撃」、プロービング・加工・マニュピレーション・リバースエンジニアリングなどの「チップに対する物理的な攻撃（パッケージ加工型攻撃）」、サイドチャネルアタック（電力解析、電磁波解析、タイミング攻撃）・故障利用攻撃などの「チップに対する物理的な攻撃（パッケージ非加工型攻撃）」　　、「デバッグポート、テスト端子から侵入」、「仕様の漏えい」、「セキュリティ機能の故障」を考慮する必要がある。

3.8.2.検証

本フェーズは未検証です。

3.9. 調達フェーズ

調達フェーズとは、製造フェーズで作成された量産前の製品を量産するにあたり、個々の部材を調達するフェーズを指します。仕様検討部会では当初調達フェーズとしては議論をせず、量産フェーズの一部と考えてきましたが、量産時に必要な解釈とは異なる観点での項目があり、今後の検討においてさらに重要な観点ととらえこれを独立させ調達フェーズとしました。

3.9.1.解釈

本フェーズでの確認項目としては、現時点で大きく以下の 2 項目を検討している。また、本文中では製造委託先としているが調達先と読み替えることも可能です。

3.9.1.1.　　製造委託先の選定

製造委託先のセキュリティレベルの確認が必要であり、製造委託先の選定基準としてセキュリティ対応および実績、また人および端末の限定、認定されている規格、社内規定などを確認し「製造委託先の選定」を行う必要があります。

3.9.1.2. 製造委託先の管理

製造委託先の管理として、委託先との契約・監査基準を機密契約の範囲で確認し、「守秘義務」として維持し、作業者および作業端末を選定・管理し、さらにインシデント発生時の規格および社内規定が存在していることを確認する必要があります。

3.9.2.検証

本項は未検証です。

3.10.量産フェーズ

量産フェーズとは、製造フェーズで検査済みの機器を量産するフェーズを指します。

3.10.1.解釈

IoT 機器量産時のセキュリティ検討項目としては、物理的な設備への侵入やネットワーク・製造機器への侵入などによる「機密情報（暗号鍵等）の流出」、良品・不良品の持ち出しや物理的な設備への侵入よる「製品の持ち出し」、固有データの重複、乱数生成確立での衝突、シリアル管理ミスがあげられます。

3.10.2.検証

本項は未検証です。

3.11.販売フェーズ

販売フェーズとは、量産済みの製品を市場へ販売するフェーズを指します。仕様検討部会では調達フェーズについて議論をせず、関連協議会に委託するものとします。

3.11.1.解釈

本項は未解釈です。

3.11.2.検証

本項は未検証です。

3.12. 運用フェーズ

運用フェーズでは、IoT 機器の販売、設置、機器およびサービスの運用、保守を行います。その際にセキュリティ面でのリスクとなる、外部からの攻撃、内部からの攻撃、留意点について説明します。

3.12.1.解釈

本書では、運用中に受ける可能性がある外部からの攻撃として「データ盗聴」、「データ改ざん」、「デバイスなりすまし」、「プログラム改ざん」、「プログラム漏洩」、「不正デバイスによるクラウド接続」、「クラウドに対する脆弱性を突いた攻撃」、「クラウドに対するサービス不能攻撃」、「デバイスに対する脆弱性を突いた攻撃」、「デバイスに対するサービス不能攻撃」、「デバイス、サービスへの不正アクセス」を示します。内部からの攻撃としては「サービス従事者による内部不正」を示す。また、運用上の留意点として「新たなぜい弱性への対応」、「デバイス利用期限の制御」、「サプライヤ消失への対策」、「利用者への通知」を提案します。

3.12.2.検証

3.12.2.1. データ盗聴

1） 想定される脅威

機密情報、機微情報の漏洩

2） 基準（対策）

通信路の暗号化により保護

データ自身の暗号化

利用者、利用システムにおけるデータへのアクセス制御、認証

3） IEC62443-4 該当項目

FSA-CR1.1 FSA-CR4.1A FSA-CR4.1B FSA-CR4.3

4） 備考

なし

3.12.2.2. データ改ざん

1） 想定される脅威

データの改ざんによる、デバイスの不正制御、誤動作、解析結果の不正操作

2）基準（対策）

データへの電子署名等を行うことにより改ざんを検知

3）IEC62443-4 該当項目

FSA-CR3.1	FSA-CR3.4	FSA-CR3.4RE(1)	FSA-EDR3.11
FSA-EDR3.12	FSA-HDR3.12	FSA-EDR3.13A	FSA-EDR3.14
FSA-EDR3.14RE(1)	FSA-HDR3.14	FSA-HDR3.14RE(1)	

4）備考

なし

3.12.2.3. デバイスなりすまし

1）想定される脅威

デバイスのなりすましにより、センサーから故意に正常/異常信号を送信された場合、動作を妨害される。

2）基準（対策）

デバイス証明書等、なりすましが困難な方式による認証

3）IEC62443-4 該当項目

FSA-CR1.2	FSA-CR1.2RE(1)	FSA-CR1.3	FSA-CR1.4
FSA-CR1.5A	FSA-CR1.5B	FSA-CR1.5C	FSA-CR1.5D
FSA-CR1.7	FSA-CR1.7RE(1)	FSA-CR1.7RE(2)	FSA-CR1.9A
FSA-CR1.9B	FSA-CR1.9C	FSA-CR1.9D	FSA-CR1.9E
FSA-CR1.9F	FSA-CR1.9RE(1)	FSA-CR1.10	FSA-CR1.11A
FSA-CR1.11B	FSA-CR1.12	FSA-NDR1.13	FSA-NDR1.13RE(1)
FSA-CR1.14A	FSA-CR1.14B	FSA-CR1.14C	FSA-CR1.14D
FSA-CR1.14RE(1)			

4）備考

なし

3.12.2.4. プログラム改ざん

1）想定される脅威

プログラムの改ざん、不正プログラム混入により、制御の乗っ取り、データの改ざん、盗聴を行う。

2）基準（対策）

プログラムへの電子署名により、改ざん防止を施すとともに、製造元の正当性を評価した上で更新する。

セキュアブート、セキュア OS、IPS/IDS、マルウェア対策、改ざん検知等の仕組みの導入。

開発担当者の認証、アクセス制御

3）IEC62443-4 該当項目

FSA-SAR3.2	FSA-EDR3.2	FSA-HDR3.2	FSA-HDR3.2RE(1)
FSA-NDR3.2	FSA-CR3.4	FSA-CR3.4RE(1)	FSA-CR3.4RE(2)
FSA-EDR3.10RE(1)	FSA-HDR3.10RE(1)	FSA-NDR3.10RE(1)	FSA-EDR3.11
FSA-HDR3.11	FSA-NDR3.11	FSA-EDR3.14	FSA-EDR3.14RE(1)
FSA-HDR3.14	FSA-HDR3.14RE(1)	FSA-NDR3.14	FSA-NDR3.14RE(1)

4）備考

なし

3.12.2.5. プログラム漏洩

1）想定される脅威

制御プログラムが悪意ある第三者に渡った場合、リバースエンジニアリング等により、内部構造、認証機構が解析される。

2）基準（対策）

正規のデバイス以外からの制御プログラムの取得要求を拒否すべく、厳密な認証を行う。

プログラムの暗号化、難読化

開発担当者の認証、アクセス制御

3）IEC62443-4 該当項目

FSA-CR4.1A	FSA-CR4.1B	FSA-CR4.3

4）備考

なし

3.12.2.6. 不正デバイスによるクラウド接続

1）想定される脅威

不正なデバイスによるクラウドサービスへの接続を許した場合、脆弱性を突いた攻撃等により、クラウドサービス上の情報が漏えい。

2）基準（対策）

正規のデバイス以外からのサービスへのアクセスを拒否すべく、厳密な認証を行う。

3）IEC62443-4 該当項目

該当項目なし

4）備考

IEC62443-4 はデバイス視点で書かれているようなので、クラウド側のセキュリティに関しては見当たらない。

3.12.2.7. クラウドに対する脆弱性を突いた攻撃

1）想定される脅威

クラウドに対する脆弱性をついた攻撃

2）基準（対策）

IPS/IDS、マルウェア対策、改ざん検知等の仕組みの導入

定期的なぜい弱性診断

3）IEC62443-4 該当項目

該当項目なし

4）備考

IEC62443-4 はデバイス視点で書かれているようなので、クラウド側のセキュリティに関しては見当たらない。

3.12.2.8. クラウドに対するサービス不能攻撃

1）想定される脅威

DDoS 攻撃等によるサービス妨害

2）基準（対策）

CDN 利用等、NW 帯域確保と、WAF 等、不正アクセス検知、遮断機能

3）IEC62443-4 該当項目

該当項目なし

4）備考

IEC62443-4 はデバイス視点で書かれているようなので、クラウド側のセキュリティに関しては見当たらない。

3.12.2.9. デバイスに対する脆弱性を突いた攻撃

1）想定される脅威

2）基準（対策）

IPS/IDS、マルウェア対策、改ざん検知等の仕組みの導入

定期的なぜい弱性診断

3）IEC62443-4 該当項目

FSA-SAR3.2	FSA-EDR3.2	FSA-HDR3.2	FSA-HDR3.2RE(1)
FSA-NDR3.2	FSA-CR3.3	FSA-CR3.3RE(1)	FSA-CR3.4
FSA-CR3.4RE(1)	FSA-EDR3.14	FSA-EDR3.14RE(1)	FSA-HDR3.14
FSA-HDR3.14RE(1)	FSA-NDR3.14	FSA-NDR3.14RE(1)	

4）備考

なし

3.12.2.10. デバイスに対するサービス不能攻撃

1）想定される脅威

デバイスに対するサービス不能攻撃

2）基準（対策）

一部機能を一時的に停止する機能の実装

3）IEC62443-4 該当項目

FSA-NDR5.2RE(1)

4）備考

なし

3.12.2.11. デバイス、サービスへの不正アクセス

1）想定される脅威

第三者によるサービス、デバイスへの不正アクセス

2）基準（対策）

デバイス、サービス利用者、従事者の厳密な認証

3）IEC62443-4 該当項目

FSA-CR1.1	FSA-CR1.1 RE(1)	FSA-CR1.1 RE(2)	FSA-CR1.2

FSA-CR1.2 RE(1)	FSA-CR1.3	FSA-CR1.4	FSA-CR1.5A
FSA-CR1.5B	FSA-CR1.5C	FSA-CR1.5D	FSA-NDR1.6
FSA-NDR1.6 RE(1)	FSA-CR1.7	FSA-CR1.7 E(1)	FSA-CR1.7 RE(2)
FSA-CR1.8	FSA-CR1.9A	FSA-CR1.9B	FSA-CR1.9C
FSA-CR1.9D	FSA-CR1.9E	FSA-CR1.9F	FSA-CR1.9 RE(1)
FSA-CR1.10	FSA-CR1.11A	FSA-CR1.11B	FSA-CR1.12
FSA-CR1.14A	FSA-CR1. 14B	FSA-CR1.14C	FSA-CR1.14D
FSA-CR1.14 RE(1)			

4）備考

なし

3.12.2.12. サービス従事者による内部不正

1）想定される脅威

デバイス製造企業、サービス運営組織、メンテナンス業者、販売企業等、サービスの運用維持に関わる従事者の内部不正

2）基準（対策）

デバイス、サービス利用者、従事者の認証情報管理

3）IEC62443-4 該当項目

該当項目なし

4）備考

認証機能に関する記載はあるが、内部犯行の場合、認証に必要な情報を持っているため内部犯行の抑止にはつながらない。

3.12.2.13. 新たなぜい弱性への対応

1）想定される脅威

新たなぜい弱性を突いた攻撃

2）基準（対策）

ぜい弱性情報の入手

仮パッチによる一時的な防御

一部機能を一時的に停止する機能の実装

正式パッチの遠隔配付

3）IEC62443-4 該当項目

FSA-HDR3.10	FSA-HDR3.10RE(1)	FSA-NDR3.10	FSA-NDR3.10RE(1)

FSA-EDR3.10　　FSA-EDR3.10RE(1)

4）備考

なし

3.12.2.14.　デバイス利用期限の制御

1）想定される脅威

保守期限、対応期限を過ぎた機器の継続利用による、不正操作、情報漏洩

2）基準（対策）

利用期限の設定と、期限を過ぎた場合に利用不可とする実装

3）IEC62443-4 該当項目

FSA-CR1.9A

4）備考

デバイスの利用期限ではなく証明書の有効期限に関する記載

3.12.2.15.　サプライヤ消失への対策

1）想定される脅威

部品調達や開発委託先の倒産とうによる保守不全

2）基準（対策）

エスクロー契約

3）IEC62443-4 該当項目

該当項目なし

4）備考

保守不全の状態になると IEC62443-4 に記載されている大部分が機能しなくなるため、全体がかかわっていると取れなくもない。

3.12.2.16.　利用者への通知

1）想定される脅威

インシデント発生時の対策

2）基準（対策）

利用者への通知

3）IEC62443-4 該当項目

FSA-HDR3.2 RE(1)　FSA-CR3.4 RE(1)　FSA-EDR3.11 RE(1)　FSA-HDR3.11 RE(1)

FSA-NDR3.11
RE(1)

4） 備考
なし

3.13. 廃棄フェーズ

廃棄フェーズとは、運用の終了した IoT 機器を使用不可として廃棄するもしくは再利用するフェーズを指します。

3.13.1.解釈

1） 想定される脅威

デバイスを別の利用者での再利用や廃棄した際に内蔵記憶媒体に保存されたデータを閲覧が可能な状態であった場合にデータの漏えいの危険性が高く以下のような攻撃が想定されます。

- 廃棄した機器を盗み、ネットワークに再接続し、偽の情報を送信する
- 廃棄した機器の中からプログラムを盗み、処理内容を解析する
- 廃棄した機器の中からデータを盗む
- 廃棄した機器から回路情報を盗む
- 廃棄した機器の中から認証キー「データ」を盗み、他の機器に移植し、正規の機器に成りすます
- 廃棄した機器の中から認証キーが格納されたメモリを盗み、他の機器に移植し、正規の機器に成りすます

2） 基準（対策）

多くの IoT デバイスでは内部記憶装置を取り外せない場合が多いため、専用プログラムで起動し、データ消去プログラムの実行を行う。また、保存された（削除後を含む）データの重要度（機密性）に応じた消去方法を選択し適切に実行したことを第三者による認証を得るようにすることで人為的な漏えい事故を防止することができます。

抹消の種別・ランク

- 「Clear(消去)」：Resistant to keyboard attacks.

一般的に入手できるツールを利用した攻撃に対して耐えられること。

- 「Purge(除去)」：Resistant to laboratory attacks.

研究所レベルの攻撃に対して耐えられること。

- 「Destroy(破壊)」：Resistant to recreation of media.

媒体の再生（再組立等）に対して耐えられること。

※消去方法の技術的な見解に関する参照資料

・「データ消去技術 ガイドブック 第 2 版」データ適正消去実行証明議会
https://adec-cert.jp/guidebook/index.html

さらに、廃棄に対する課題として「コンシューマ向け機器等、廃棄の管理が困難」「中古販売等、再利用を目的とした廃棄への考慮」「利用者への廃棄方法の周知が困難」などがあげられます。

3.13.2.検証

未検証。

4. 付録 A　IOT セキュリティ用語

- CDN
  - 正式名称：Content Delivery Network、Web コンテンツを最適に配信する分散されたサーバープラットフォーム。エンドユーザーのコンテンツ要求ごとに、最適な位置の CDN サーバをマップし、そのサーバにキャッシュされたファイルを用いてリクエストに応答する。物理的に近いネットワークでエンドユーザーのリクエストに応答することで、コンテンツサーバーのトラフィックをオフロードしてウェブの応答性を高めることが出来る。
- CSRF
  - Cross-Site Request Forgeries の略、Web サイトの脆弱性をついた攻撃の一種
- DDoS 攻撃等
  - 正式名称：Distributed Denial of Service attack、トラフィックの増大によるネットワークの遅延、サーバやサイトへのアクセス不能等を目的とした攻撃手法のひとつであり、大量のマシンから 1 つのサービスに、一斉に DoS 攻撃を仕掛ける方法を指す。
- 協調分散型 DoS 攻撃
  - 攻撃者が大量のマシン(踏み台)を不正に乗っ取った上で、それらのマシンから一斉に DoS 攻撃をしかける攻撃手法
- 分散反射型 DoS 攻撃
  - 攻撃者が攻撃対象のマシンになりすまして大量のマシンに何らかのリクエストを一斉に送信する攻撃手法。攻撃対象のマシンはリクエストを受け取ったマシンから、大量の返答が集中することで、高負荷がかかることになる。
- Dos 攻撃（Denial of Service attack）
  - ウェブサービスを稼働しているサーバやネットワークなどのリソースに意図的に過剰な負荷をかけたり脆弱性をついたりする事でサービスを妨害する。
- IDS
  - 正式名称：Intrusion Detection System、侵入検知システム。Web サイト運営者が設定する検出パターンに基づいて、様々な種類の機器への通信を検査するシステムであり、ネットネーク型とホスト型に大きく二分される。
- ネットワーク型 IDS
  - スイッチングハブなどのミラーポートにプロミスキャスモード（ネットワークを流れるすべてのパケットを受信して読み込むモード）で IDS 装置を接続することでネットワークセグメントを監視し通知することができる。
- ホスト型 IDS

- サーバにインストールする形で使用し、稼働するサーバの通信を監視する他ほか、アプリケーションの動作を監視することができる。

- IPA
  - 独立行政法人 情報処理推進機構
- IPS
  - 正式名称：Intrusion Prevention System、侵入遮断システム。IDS より一歩進んで、異常な通信に対し、管理者へ通知するだけでなく、その通信をブロックするところまで動作を行う。管理者が異常に気づいてから対処するのと異なり、迅速な対処が可能となる。
- ネットワーク型 IPS
  - ネットワークセグメントを監視し、IPS を通過するパケットを制限することで攻撃を防ぐ。
- ホスト型 IPS
  - サーバにインストールする形で使用し、サーバの通信を監視・制限する他ほか、アプリケーションの動作を監視・制限することができる。
- JTAG-ICE
  - SoC をデバッグするためのツール。プロセッサに内蔵した ICE(In-Circuit Emulator)機能を「JTAG」という規格を利用してデバッグする
- NDA
  - Non-Disclosure Agreement の略、機密保持契約,
- OS
  - Operating System の略、コンピュータを動かすためのソフトウェア
- OTP メモリ
  - One Time Programmable Memory を指す。1 度書込んだデータの変更、削除をできなく（ロック、保護）することができるメモリ。eFuse と同義
- SQL インジェクション
  - データベースサービスの脆弱性をつき、意図しないスクリプトを実行させる攻撃
- WAF 等
  - 正式名称：Web Application Firewall、外部ネットワークからの不正アクセスを防ぐためのソフトウェア（あるいはハードウェア）であるファイアウォール（FW）の中でも、Web アプリケーションの脆弱性を悪用した不正侵入を検知・防御することのできるＦＷを指す。主にトランスポート層やセッション層を保護する FW、IDS/IPS に対し、WAF はアプリケーション層に対する不正アクセスからシステムを保護する。つまり SQL インジェクションやクロスサイトスクリプティングといった、Web アプリケーションが抱えやすい脆弱性を悪用した攻撃から守ることが可能となる。

- XSS
  - XSS（Cross Site Scripting、クロスサイトスクリプティング）とは、アクセス時に表示内容が生成される「動的 Web ページ」の脆弱性、もしくはその脆弱性を利用した攻撃方法。
- インシデント発生
  - システムにおいて運用上の脅威となる事象が発生したことを指す。主に、セキュリティ上の脅威をセキュリティインシデントと呼び、ウィルスやマルウェア感染・不正アクセス・情報漏洩・DoS 攻撃などが該当する。
- インセンティブ
  - インセンティブとは「対価」を指す。特定の行動を行わせるための理由として、最終的に金銭面等で有利になるような方向で行われる方策のこと。本書では、システムのセキュリティ維持を目的として、利用者に特定の行動（情報適用や機器の操作等）を行わせるために、優遇措置や金銭面での補助等の方策を行うこと
- エスクロー契約
  - 売り手と買い手の間に第三者である金融機関を介して、条件付で譲渡金額を決済する仕組みのこと。第三者である金融機関に、証書 の交付とともにエスクロー勘定を開設し、買い手はその勘定に譲渡代金を入金して保管することで、売り手との間に設けた条件が満たされたときに、その勘定から譲渡対価が売り手に支払われる方式。
- ソフトウェア・エスクロー
  - ソフトウエアのライセンスを行う場合に、そのソフトウエアのソースコードや技術情報を第三者に預託しておく制度である。ソフトウエアの提供企業（ライセンサー）に倒産などがあった場合、ソースコード等の預託物を、ライセンスを受けている企業（ライセンシー）が開示してもらうことができる
- オープンソース
  - ソフトウェアのソースコードを商用、非商用を問わず無償で公開し、誰でも自由に改良・再配布ができるようにしたソフトウェア
- カバレッジ
  - 所定の網羅条件がテストによってどれだけ実行されたかを割合で表したもの。ソフトウェアにおいては、命令分岐や与えるデータの範囲、ハードウェアにおいては、回路の分岐、機能の網羅性、入力の範囲の割合を指す。
- クラウド
  - ユーザがサーバやストレージ、ソフトウェアを持たなくても、インターネットを通じて、サービスを必要な時に必要な分だけ利用する考え方のことを指す。クラウド・コンピューティングとも呼ばれる。
- サイドチャネルアタック

- 動作中の IC が消費する電力や、IC から漏れる電磁波の時間的変化やデータに応じた処理時間の違いを収集・分析し、秘密情報を導出する攻撃手法。

- サプライチェーン管理方針策定
  - 原料・部品の調達から製造、販売、流通・サービス提供までの一連のプロセスを、複数の企業を跨いで統合的に構築した状態を指す。また、そこに関わる組織、個人を指す場合もある。
- シールド
  - 電子機器が電磁波や静電気で誤動作したり、他の機器への影響を防ぐために、機器内部に金属で遮蔽する方法。セキュリティ対策では機器内部の基板やコネクタなどに触れられないようにする方法としても用いられている。
- ぜい弱性
  - システム（OS、ミドルウェア、Web アプリケーション等）において、プログラムの不具合や設計上のミスが原因となって発生した情報セキュリティ上の欠陥のことを指す。セキュリティホールとも呼ばれる。
- ぜい弱性診断
  - システム（OS、ミドルウェア、Web アプリケーション等）に対し、攻撃者の視点から様々な疑似攻撃を考察・試行することで、潜在的なぜい弱性を発見し、安全性を調査する方法。セキュリティ診断、ぜい弱性検査とも呼ばれる。
- セキュア OS
  - アクセス権限の管理を強化し、通常よりセキュリティを高めた OS を指す。厳密な定義は存在しないが強制アクセス制御（MAC：Mandatory Access Contorol）と最小特権の機能を組み込んだものを指すことが多い。
- セキュアブート
  - 機器が起動する際、自プログラムの正当性、完全性を検証し、正しい場合のみ起動する機構
- セキュリティ
  - ISO/IEC 27032 に従い、本書では、以下のように定義する
    - ✧ セキュリティとは、人、住居、地域社会、国家、組織、資産などを対象とした、害からの保護を指し、以下に分類される
      - ■ セキュリティ分類

        情報セキュリティ

        サイバーセキュリティ

        --- アプリケーションセキュリティ

        --- ネットワークセキュリティ

        --- インターネットセキュリティ

物理的セキュリティ
HSE（健康、安全、環境）セキュリティ

- セキュリティドア
  - 職場や工場への入退場制限を行う際に設置されるドア。一般に、施錠・解錠のために暗証番号・IC カード・生体認証データ等を必要とする。
- セキュリティポリシー
  - 企業や組織におけるコンピュータのセキュリティに関する方針や行動指針のことである
- セキュリティラベル
  - 電子機器の筐体が未開封であることを証明するラベル（シール）。ラベルをはがすと開封した表示が残る。
- セキュリティ検査ファジング
  - 「ファジング」と同じ
- セキュリティ要件確認支援ツール
  - IPA が提供するツール。政府が公表しているセキュリティ対策基準や技術参照モデルを利用して、そこから抽出される各種セキュリティ要件リストにより、情報システムの調達物品のセキュリティ要件を確認できる<https://isec-sras.ipa.go.jp/>
- ソースコードセキュリティ検査
  - ソースコード解析において、機能に着目した検査ではなく、主に脆弱性に着目した検査を行うことを指す。静的テストの一部
- ソフトウェア
  - 機器を動作させるために必要なプログラムとデータを指す
- デバイス証明書等
  - デバイスに対して電子証明書を発行し、その発行した電子証明書を PC やサーバに登録することで、その電子証明書を保持する端末からのみ、クラウドサービスのアクセスを許可することが出来る。MAC アドレス、IMEI、UDID など端末固有の ID を識別し、デバイス証明書のインストールを許可する端末を管理することが出来る他、端末紛失時などに対し管理者がデバイス証明書を失効させることでアクセス制限をかけることが可能になる。
- ネジ規格
  - 電子機器の筐体の封や回路基板の固定などに用いられるネジの規格。国内では JIS 規格や海外では ISO 規格が用いられるが、古くからの規格も多数用いられている
- ファジング

- ソフトウェアの主に脆弱性を発見するためのテスト手法の一つ。ファズ（fuzz：予測不可能な入力データ）を与えることにより意図的に例外を発生させ、その挙動を確認する

- 分岐網羅
  - ソフトウェアの動的テスト実施方針の一つであり、ソースコードに含まれる条件分岐について、すべての分岐を必ず一度は実行することを指す。カバレッジの一部
- ペネトレーションテスト
  - システムに対し、実際に侵入を試みることにより脆弱性をテストすること。
- リスク分析
  - リスクアセスメントプロセスの一部であり、リスクの特質（発生頻度や事業・利用者・周辺への影響等）を理解し、リスクレベルを決定するプロセスを指す。ここでいう「リスク」とは、主に「情報セキュリティリスク」を指すが、これに「HSE（健康、安全、環境）リスク」を加えたものとする。「情報セキュリティリスク」とは、情報セキュリティ（情報資産の機密性、完全性、可用性の保護）を損ねる可能性がある要因のことを指し、「HSE リスク」とは、健康、安全、環境を損ねる可能性がある要因を指すものとする
- レビューツール
  - 本書では、設計書のレビューを支援するツールを指す。ドキュメント体系の視覚化やレビューコメントの整理、進捗状況管理などの機能により、レビュー作業の効率化を支援するツール
- 暗号かぎ管理基準
  - 暗号鍵を安全に管理するための基準。データ保管だけでなく、機器間の認証やデータ通信など様々な用途に多くの暗号鍵が使用されるため、厳格な管理・運用体制が必要とされている。暗号鍵の生成・配送・保管・利用・変更・廃棄といったライフサイクル毎に管理基準を定める。
- 遠隔配付
  - ファームウェアやオペレーティングシステム（OS）、アプリなどの更新のためのデータ受信を無線 LAN（Wi-Fi）や移動体データ通信などの無線通信を経由して行うことを指す。Over-The-Air アップデート(OTA)とも呼ばれる。従来はＰＣ接続や、記憶装置を通じて端末に移していた更新プログラムなどを、機器単体で無線ネットワークを通じて開発元から入手できるようになる。また、導入済みのソフトウェアの更新・修正だけでなく、ソフトウェアの新規入手・導入や、デジタルコンテンツの購入や入手、外部端末やクラウドサービスとのデータや設定情報の同期などについても、無線通信を経由して行うことを OTA と表現することがある。

- 機微情報
  - プライバシーや国家機密など、慎重に扱われるべき情報を指す。(下記は JISQ15001:2006 を参照)
    - ✧ 思想，信条及び宗教に関する事項。
    - ✧ 人種，民族，門地，本籍地，身体・精神障害，犯罪歴，その他社会的差別の原因となる事項。
    - ✧ 勤労者の団結権，団体交渉及びその他団体行動の行為に関する事項。
    - ✧ 集団示威行為への参加，請願権の行使，及びその他の政治的権利の行使に関する事項。
    - ✧ 保健医療及び性生活。
- 機密情報（機密データ）
  - 個人や組織がもつ公開していない情報を指す。
    - ✧ 企業が保有している情報のうち外部への開示が予定されない情報
    - ✧ 秘密として管理されている情報
    - ✧ 開示されれば企業に損失が生じるおそれのある情報
    - ✧ 設計図やマニュアル、企画書、顧客情報はもちろん、人事異動に関する情報や給与情報、在庫・仕入先リストなども保護すべき機密情報にあたる。
- 境界値試験
  - 正常範囲の限界値と異常範囲となる値を与え、それぞれが正しく、正常および異常となることを試験することを指す
- 金属シールド
  - シールドと同じ
- 固有データ
  - 機器識別子などの機器ごとに異なるデータ・ID など指す。製造時に機器内に格納され、機器ごとに重複の無い一意のものが使用される。
- 構造解析ツール
  - ソースコードの構造を解析し、可視化するツール
- 自動テストツール
  - テスト支援ツールによりソフトウェア試験の自動化を行うツール。動的テストツールの一種
- 実装工程
  - 本書では、機器の開発工程において、ソフトウェアのコーディングを行う工程を指す
- 遮断機能
  - IPS やファイアウォールのように不正と判断したパケットをブロックするはたらき

- 取得要求
  - ROM 上のプログラムを RAM 上にコピーする際の命令
- 重複防止
  - 製造時に固有データを機器に格納する際、出荷した全ての機器ごとに重複の無い一意のデータを使用するための仕組み。製造システム上で、出荷済みの機器の固有データを管理して重複しないデータを出力して使用する。出荷テストで重複していないことを確認する場合もある。
- 出荷テスト
  - ソフトウェアの機能や性能を評価するために行うテスト。ソフトウェアの品質が明確化される。
- 出荷品
  - 出荷した製品。一般的に、その数と種別、製造シリアル No.等を管理しておく。
- 情報漏洩
  - 第三者による攻撃、内部犯行、人為的ミスのいずれかにより、守るべきデータが所有者・管理者の意図せず外部に流出すること
- 正規
  - 本書では、機器、ソフトウェア、ハードウェアについては、予め規定した基準に基づき検査した結果、基準を満たしていることが確認されたものを指す。また、人については、製造者またはサービス事業者、利用者等、規定に定められた権限者を指す。予め規定した基準とは、工程基準、検査基準、および、開発・製造・量産・設置・運用・廃棄の各工程に携わる要員、組織に関する規定が含まれる。
    - ✧ ソフトウェア、ハードウェアにおいては、開発工程の最後に行う検査／テストにおいて、規定を満たすことを確認した後、それが改変されていないことをもって正規とする
    - ✧ 機器においては、出荷検査および設置後の動作確認において、規定を満たすことを確認した後、それが改変されていないこと、および、正常に動作していることをもって正規とする
    - ✧ 設置後に、製造者またはサービス事業者、利用者等、規定に定められた権限者が、内容を改変した場合、改変後の状態が規定を満たしていることを確認することもって正規とする
- 正規
  - 製造元やサービス提供者が意図したとおりであること
- 正規パッチ
  - 信頼できる発行元より発行された、プログラム修正用のデータ
- 正当性
  - ハードウェアおよびソフトウェアが設計どおりであること

- 静的ソースコード解析ツール
  - 「構造解析ツール」に統合
- 静的テスト
  - ソースコード解析などソフトウェアを動作させずに行うテストを指す
- 脆弱性
  - 本書では、ソフトウェアの脆弱性を指す。ソフトウェアの設計や実装のミスが原因となって発生する情報セキュリティ上の欠陥を指す。攻撃に必要なコストの低さをあらわす指標。
- 脆弱性検査
  - ソフトウェアに対し、攻撃を模した入力データを与えることにより、潜在的な脆弱性を発見するテスト手法を指す。動的テストの一部
- 妥当性評価
  - ソフトウェアが最終利用者の意図通りに動いているかどうかを確認すること
- 耐タンパエリア（対タンパ領域）
  - 耐タンパとは、機器や装置、ソフトウェアなどが、外部から内部構造や記録されたデータなどを解析、読み取り、改竄されにくいようになっている状態を指し、耐タンパエリアとは、耐タンパ措置を施された領域を指す（基板上の特定領域を指す場合と、IC チップ内のメモリ領域を指す場合がある）
- 単体テストツール
  - 関数やメソッドの単位でテストを行うためのツール。関数やメソッドを動作させる上で必要なドライバ（起動コード）やスタブ（関数やメソッドが呼び出す先のコード）等の機能が提供される。動的テストツールの一種
- 動的テスト
  - 機器やソフトウェアを動作させ、入力値やデータに対して、想定した動作が行われることをテストすることを指す
- 動的テストツール
  - ソフトウェアの動的テストを支援するツール。テストの自動実行やテストデータの自動生成、疑似環境上でのテスト、分岐網羅率集計等、様々な支援機能を提供する
- 難読化
  - コンピュータプログラムにおいて、その処理内容・構造・データなどを、人間が理解しにくいように加工すること。難読化後もプログラムの機能には相違は無い。第三者に渡った場合でも、処理内容をすぐに把握されないよう複雑化したソースコードまたはバイナリデータ
- 二重化

- 主/従の二系統の回路を持つことにより、主回路に異常が生じた場合に従回路をバックアップ回路として動作できるシステム。全く同じ回路を二つ持つ完全二重化システムが一般的,用語集からは削除。入退室管理,情報漏洩や破壊行為等を防ぐために職場や工場へ入ることのできる人間を制限すること、またはそのためのシステム。警備員による監視を行う他、セキュリティドアや監視カメラにより入退場者の制限・監視・記録を行う。

- 認可
  - 認可とは認証を基準にサービスの提供を許可することを指す。
- 認証
  - 認証とは個人・モノ・コトを特定することを指す
- 認証キー（認証キー情報）
  - 機器間、機器内のプログラム間において、データを連携する際、相手の識別、及び、正当性、真正性を確認するための情報を指す
- 認証情報管理
  - 認証に必要な鍵、暗号方式、認証方法をプロファイルとして管理することを指す
- 廃棄エビデンス
  - 機器を廃棄した際、廃棄手続きが正しく行われたことを証明するための情報を指し、以下のような内容が含まれる
    - ✧ 廃棄日時
    - ✧ 廃棄処理に関わった組織・個人の名称、署名・捺印、証明書類
    - ✧ 廃棄手続きを記録したログ、書類
- 秘密情報
  - 一般に公表せずに保持しておくことで技術的、営業的などで有利になる情報。特定の相手方とは秘密保持契約を締結して開示することがある。平成 28 年 2 月経済産業省「秘密情報の保護ハンドブック」に詳しく定義されている。
- 不正アクセス
  - サービス提供者の不利益につながる接続をしようとする試み。正規のアクセス手段を不正に入手してアクセスする場合も含む
- 不正デバイス
  - 正規の製造元の認可が下りていないデバイス、運用中に改ざんされたデバイス、正規の製造元が期待しているとおりに動作する、正規でない製造元によるデバイス(海賊版)
- 不正プログラム
  - 正規の製造元またはサービス提供者が意図しない動作をさせることを目的に開発したコンピュータが実行可能な電子情報のかたまり
- 不正書換え対策

- ハードウェアによる対策
  - ✧ JTAG カット等、情報書換え用端子を物理的に無くす（もしくは容易にアクセスできないよう封印等の対策を施す）
  - ✧ eFuse 等、IC チップの機能により、書換えできない状態にする
  - ✧ ソフトウェアによる対策
  - ✧ セキュアブート等、起動時の検証機構を搭載する
  - ✧ 機器動作中に、情報の改ざん検知機構を搭載する
  - ✧ 情報更新時、情報の提供元・内容の正当性、真正性を検証する機構を搭載する

- 不正制御
  - 機器に正規でない動作をさせることを目的として、改ざんまたは混入されたプログラムによる機器への命令。
- 不正操作
  - 機器に正規でない動作をさせることを目的とした人による機器への命令。
- 復号鍵（複合キー）
  - 暗号化されたデータを元に戻すときに使う鍵を意味し、公開鍵暗号においては、秘密鍵を指す。英語では Decryption Key
- 物理保護
  - 広義の意味では、内容品を衝撃、振動、火災、漏水等から保護することを指す。本書では、上記に加え、機器に対する物理侵入、電磁波・熱・赤外線等による内部情報の透視等の物理攻撃からの保護を含む
- 保守不全
  - 保守切れ/保守期限切れ/サポート切れ/サポート期限切れ/保守期間終了/サポート期間終了
- 要求定義書記載
  - 「?したい」と利用者側の希望を示したものであり、ビジネスで何が必要なのかを記載したものを指す
- 要件定義書記載
  - 「～が必要」システムの仕様書であり、システムが何をしなければならないかを記述したものを指す
- 論理消去
  - プログラム処理により、削除フラグを設定する、または、情報の一部を消去する等の方法により、アプリケーションから情報にアクセスできなくすることを指す。情報そのものは、記憶域に残った状態となる。これに対し、完全消去は、プログラム処理により、記憶域内の情報そのものを、別の情報によって上書きする

等により、消去することを指す。また、物理消去とは、プログラム処理ではなく、消磁装置等、物理的な手段によって、情報を消去することを指す

5. 付録 B　フェーズ別索引

企画フェーズ

設計フェーズ

開発フェーズ

製造フェーズ

機密データ
固有データ
重複防止
出荷品
退場制限

運用フェーズ

CDN
DDoS 攻撃等
IDS
IPS
WAF 等
エスクロー契約
クラウド
サプライヤ消失
ぜい弱性
ぜい弱性診断
セキュア OS
デバイス証明書等
遠隔配付
機微情報
機密情報
攻撃 IPS
攻撃ぜい弱性情報
遮断機能
取得要求
情報漏洩
正規
正式パッチ
正当性
脆弱性
難読化
認証情報管理
不正アクセス
不正アクセス検知
不正デバイス
不正プログラム混入
不正制御
不正操作
保守不全

廃棄フェーズ

OTP 等
インセンティブ等
セキュアブート
セキュリティ
正規
耐タンパエリア
耐タンパ領域
難読化
認証キー
認証キー情報
廃棄エビデンス
不正書換え対策
復号鍵
物理保護
論理消去

以上