IoT セキュリティ評価検証ガイドライン

Rev1.0

一般社団法人

重要生活機器連携セキュリティ協議会

2017 年 6 月 30 日

更新履歴

リビジョン	更新日	更新内容	担当者
Rev1.0	2016/6/30	新規作成	CCDS IoT セキュリティ評価 検証ガイドライン策定 準備委員会

目次

1. はじめに

1-1. IoT セキュリティの現状と脅威

1)生活機器のネットワーク化

様々な生活機器に ICT(情報通信)技術が組み込まれ、生活機器がインターネットにつながる IoT（Internet of Things）の時代が到来し、製品の更なる高度化、自動化を実現することとなった。一方で、これまでは個々に独立していた機器が、通信ネットワークに接続することでセキュリティ攻撃の潜在的なリスクを高めることにつながっている。

実際に米国ではスーパーなどの POS 端末を狙ったマルウェアにより、約 4000 万件のカード情報を流出する事例(2013 年)や、携帯メール送信により、ATM から現金を引き出せるマルウェアが発見された事例（2014 年）が報告されている。このことはこれまで想定でしかなかった生活機器のネットワークアクセスによるウィルスや不正アクセスなどの脅威が、実際にユーザの安全・安心を阻害し得ることを実証し、産業界に生活機器のセキュリティ対策を促す大きな警鐘となった。

2) 日本における研究開発動向

国内においても 2020 年の東京オリンピック開催に向けて IT 戦略とセキュリティ対策戦略が加速すし、官民連携によるセキュリティ対策が進行している。2014 年 1 月に CCDSSG（重要生活機器セキュリティ研究会）が発足し、生活機器のネットワーク連携によるセキュリティ対策に関する研究活動を開始。2014 年 6 月には CCDSSG による提言を受け、NISC（内閣サイバーセキュリティセンター）は「情報セキュリティ研究開発戦略（改訂版)」の中で、今後の研究開発のスコープとして、情報家電、自動車、在宅医療機器、HEMS 等の生活機器を含める指針を発表している(2014 年 7 月)。

3)組込み機器メーカの課題及びニーズ

こうした状況を踏まえ、各産業分野ではセキュリティ対策の重要性を認識しているものの、具体的な対策にあたっての標準規格やガイドラインの整備は、現状では不十分な状況にある。下記図 1-1 のように、機能安全(セーフティ)の領域では、ISO26262 をはじめとする具体的な対応基準が整備されているが、セキュリティの領域では、ISO27001 にて組織マネージメントに対するセキュリティ規格はあるものの、具体的なセキュリティ標準規格を策定しているのは、原子力等の重要インフラに関するセキュリティ基準を定めた「IEC64223 汎用制御システムのセキュリティ」のみである。生活機器セキュリティに関しては、2016 年に、内閣サイバーセキュリティセンター(NISC)が、新たなサイバーセキュリティ戦略の一環として、セキュリティ ・バイ ・デザインの考え方を踏まえた IoT システム開発の推進を提唱し、8 月には具体的な対策を盛り込んだ「安全な IoT システムのためのセキュリ

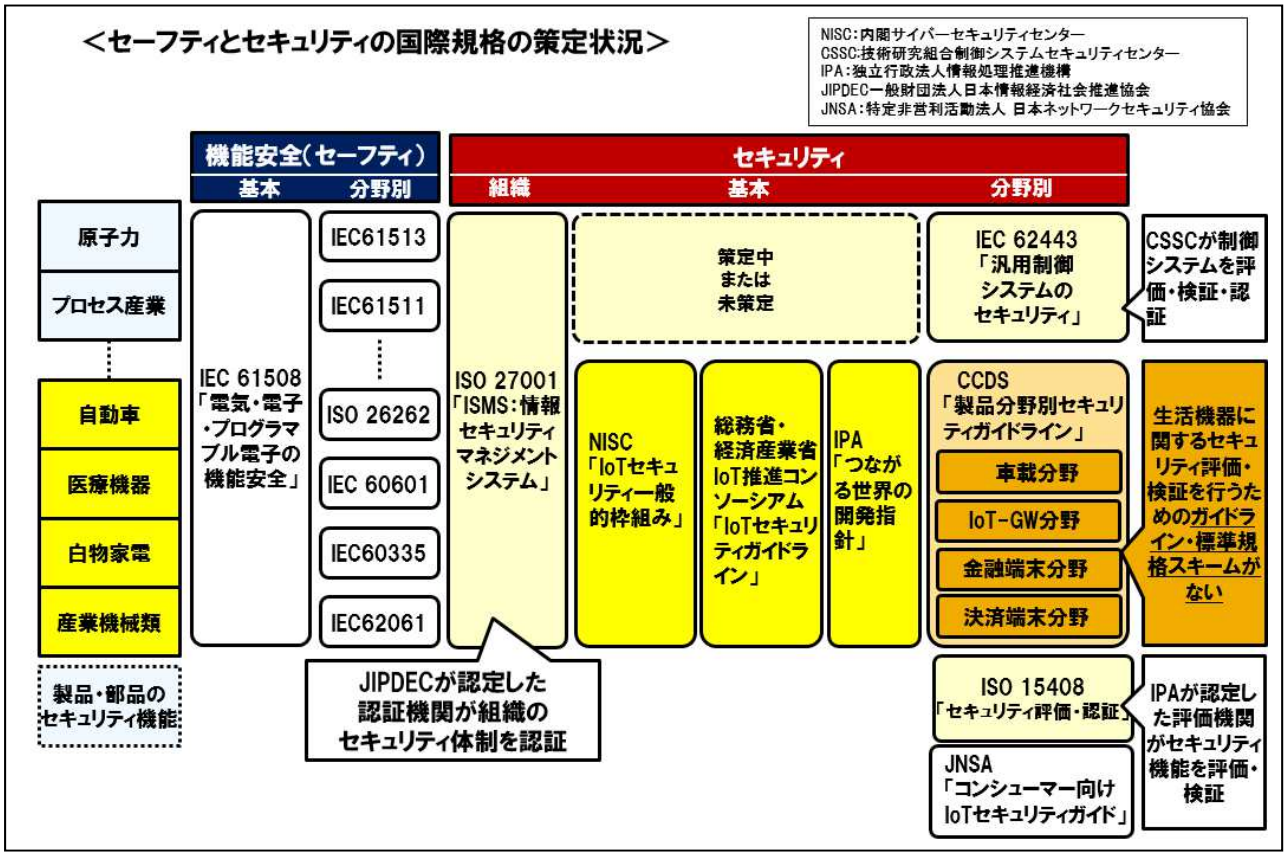
ティに関する一般的枠組」が公開された。また、経済産業省及び総務省の IoT 推進コンソーシアムからも「IoT セキュリティガイドライン ver1.0」が公開され、ガイドライン策定を含めた民間のセキュリティ団体の活動も活性化しつつあるが、何をどこまで対応すべきか明確な基準が整備されたとは言えないのが実状である。

まとめると組込み機器メーカの課題は以下となっている。

・製品の競争力向上のためには、通信ネットワーク連携による高度化が必要であるが、そのためには具体的なセキュリティ基準の策定が急務である。

・同時にセキュリティ検査ツールや、検査、認証基準の整備を行い、セーフティで実施されているような第三者による客観的、定量的な検査・検証が行われる仕組みづくりが必要である。

図 1-1.　日本におけるセーフティとセキュリティの国際規格の策定状況



（出典：CCDS 発行「一般社団法人 重要生活機器連携セキュリティ協議会の概要」[1]に加筆修正）

1-2. 評価検証ガイドラインにおける対象範囲

1)本文書の位置づけ

本文書は下記の団体より発行されたセキュリティガイドラインの評価検証に関する項目に対して、スマートホーム分野での実例を取り入れつつ、IoT 機器全般を対象に、具体的なセキュリティの評価検証プ

ロセスを更に掘り下げた内容として策定している。

本書は広く IoT 機器全般を対象に活用できることを念頭に作成しているが、記載事例については、スマートホームシステムに対するセキュリティ評価検証の実証実験結果をもとに作成しており、他分野に応用する場合には注意が必要である。

また本文書における評価検証部門は独立した第三者機関を想定しており、顧客や開発部門と協議や意思疎通を図りつつも、自らがセキュリティ評価検証の各プロセスを通じて、設計、提案、実行、管理、そして継続的な改善を行うことを前提としている。

[本書と関連するセキュリティガイドライン]

①IoT 推進コンソーシアム

「IoT セキュリティガイドライン（要点 12　安全安心を実現する設計の検証・評価を行う)」[2]

②独立行政法人　情報処理推進機構（以下 IPA）

「つながる世界の開発指針（指針 12 安全安心を実現する設計の検証・評価を行う)」[3]

③一般社団法人 重要生活機器連携セキュリティ協議会（以下 CCDS）

「CCDS 製品分野別セキュリティガイドライン 車載器編 Ver.1.01（4.2.2 項 企画・開発フェーズ)」[4]

「CCDS 製品分野別セキュリティガイドライン IoT-GW 編 Ver.1.01（4.2.3 項 評価フェーズ)」[5]

「CCDS 製品分野別セキュリティガイドライン 金融端末(ATM)編 Ver.1.0（5.2 項 各フェーズの詳細説明)」[6]

「CCDS 製品分野別セキュリティガイドライン オープン POS 編 Ver.1.0（5.2.2 項 開発フェーズ）[7]

2)本書の対象者

本文書はセキュリティの評価検証にかかわる下記の担当者を対象としている。

①IoT 機器の設計を行う設計者、開発者、及び開発責任者

②IoT 機器の評価検証を行う、テストエンジニア、及び責任者

③IoT 機器の設計、開発及び評価検証において、予算や人員を決定する意思決定者

3)本文書の対象範囲

本文書はセキュリティの評価検証に焦点を絞って記載するものとする。脆弱性の原因となる不具合の作り込みを低減するため、ISO/IEC 25010[8]に基づき、対象システム/ソフトウェアの各品質特性に対して、別途テストが実施されていることを前提とする。また組織的評価検証方針・組織的評価検証戦略につ

いて本文書では記載していないが、ISO/IEC/IEEE29119[9]に則り、定義されていることを前提とする。

3)略称、用語

表 1-1. 略称、用語一覧

略称	名称
CCDS	Connected Consumer Device Security council
CUI	Character User Interface
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
DoS	Denial of Service
DUT	Devise Under Test
ETSI	European Telecommunications Standards Institute
FIRST	Forum of Incident Response and Security Teams
GMITS	Guidelines for the Management for IT Security
HAN	Home Area Network
HEMS	Home Energy Management System
HTTP	Hyper Transfer Text Protocol
HNW	Home Network
IoT-GW	Internet of Things-Gate Way
IPA	Information-technology Promotion Agency
IT	Information Technology
JVN	Japan Vulnerability Notes
NVD	National Vulnerability Database
OSDBD	The Open Source Database Network
OSS	Open Source Software
OTA	Online Trust Alliance
OWASP	The Open Web Application Security Project
SQL	Structured Query Language
TCP/IP	Transmission Control Protocol/Internet Protocol
WASC	Web Application Security Consortium

WAN	Wide Area Network
XSS	Cross Site Scripting

2. セキュリティ評価検証プロセス

2-1. 製品ライフサイクルにおける評価検証プロセスの位置づけ

「CCDS 製品分野別セキュリティガイドライン IoT-GW 編 Ver.1.01」[5]では製品の開発フェーズを「製品企画」、「設計・製造」、「評価」、「運用保守」、「廃棄」と大きく５つに分類している。当ガイドラインでは、上記の「評価」フェーズについて、セキュリティ評価検証を行う上での詳細プロセスを規定するものとする。

図 2-1.「CCDS 製品分野別セキュリティガイドライン IoT-GW 編」[5]における製品ライフサイクルとフェーズ定義

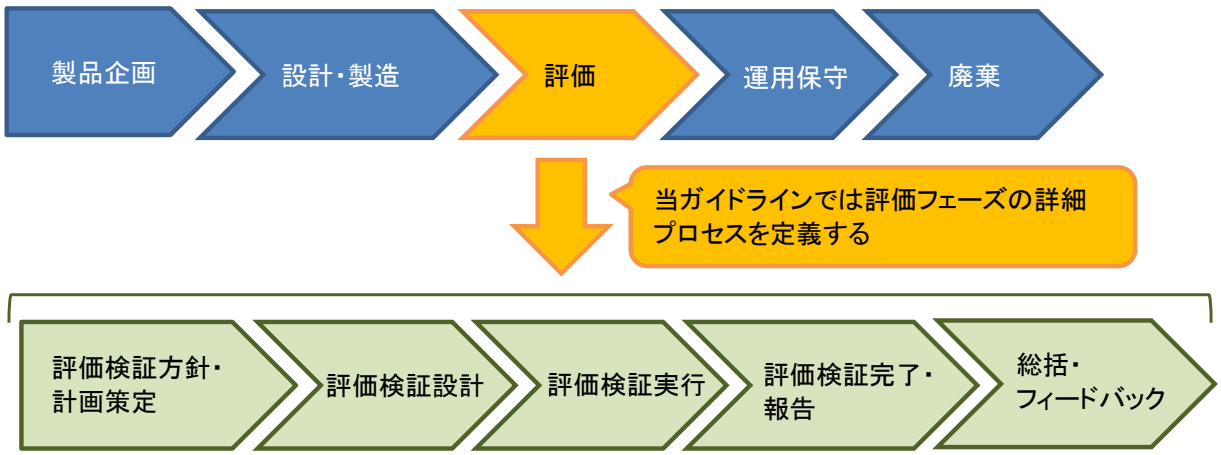


表 2-1.　製品ライフサイクルにおける各フェーズの説明

フェーズ	説明
評価検証方針・計画策定	評価検証の対象範囲や対応人員(工数)、評価検証スケジュール等の実施計を策定する。
評価検証設計	実施する評価検証の内容や手順等について、要件及び仕様として整理を行う。
評価検証実行	策定した計画、仕様に従って、セキュリティ評価検証を実施する。
結果総括・フィードバック	評価検証の実施結果を総括し、次回以降の改善点を明確化した上で、今後の開発や評価検証プロジェクトにフィードバックを行う。

3. セキュリティ評価検証の方針・計画策定

セキュリティ評価検証の方針・計画策定を行うにあたり、「評価検証計画書」を策定し、対象プロジェクトの背景や具体的な計画を明確化しておく。「評価検証計画書」の記載要件として推奨する内容については、以下に記載する。評価検証計画書の記載内容については顧客あるいは開発部門と協議を行い、合意の上で策定を行う。

※本文書記載の評価検証計画書の記載要件は、テストプロセスに関する国際標準を定めた ISO/IEC/IEEE29119[9]を参考に作成している。

※評価検証計画書の具体的には作成事例は、「Appedix2.評価検証計画書」の事例集を参照。

表 3-1.　評価検証計画書の記載要件

計画書の項目名称	記載内容
1)評価検証の背景	
①評価検証サブプロセス	検証を行うべきシステムやソフトウェアの開発背景や、想定しているユースシーンを概要として記載する。
②評価検証対象の構成	システム構成図等を用いて、評価検証対象となるシステムやソフトウェアの全容を示す。
③評価検証範囲	上記システム構成図において、評価検証対象範囲を明示する。また、評価検証範囲において、具体的な想定機能や保護すべき資産を明確化しておく。
④前提及び制約条件	評価検証を進める上で前提条件や制約事項があれば記述する。（工数や期間、環境上の制約事項、事前に所得しておくべき認証基準、機密保持方針など）
⑤利害関係者	対象の評価検証プロジェクトにおいて、顧客を含む、利害関係者を一覧として記載する。（顧客以外のプロジェクト関係企業についても記載）
２）評価・検証コミュニケーション	
①実行体制図	対象の評価検証プロジェクトにおける実行体制図を記載する。開発や評価検証の責任者や指揮命令系統も含めて、明示しておく。
３）リスク一覧表	
①リスク一覧	対象の評価検証プロジェクトにおいて、製品開発上のリスク、プロジェクトの進行に関するリスクを記載する。
４）評価・検証方針	
①評価検証サブプロセ	評価検証対象となるシステムやソフトウェアにおいて、評価検証範囲となる機

ス	能を明示しておく。
②成果物	対象となる評価検証プロジェクトの最終成果物を記載する。
③評価検証設計手法	今回利用を想定しているセキュリティ評価検証手法を記載する。 詳細な評価検証要件については、後述の評価検証設計フェーズにて検討を行う。
④完了基準	検証完了の条件や判定基準について、記載を行う。
⑤収集するメトリクス	検証完了後、次回以降の評価検証プロセスを改善（フィードバック）するために必要な収集メトリクスを定義しておく。 ※フィードバックのプロセスについては「6.評価検証プロジェクトの総括・フィードバック」を参照。
⑥必要となるデータ・ドキュメント	評価検証のテストベースとなる対象機器（以下 DUT）の要件定義書、設計ドキュメント等。
⑦必要となる環境	必要とされるテスト環境を記載する。
⑧評価検証の再実施（回帰テスト）	不具合、インシデントが検出された場合、改修後の再評価検証の実施に関する条件を記載する。
⑨中断及び再開基準	ブロッキングとなる課題が検出された場合など、評価検証を中断する条件や、再開の条件について記載する。
5）評価検証活動の役割分担、要求スキルレベル及び工数見積り	
役割分担、スキル、工数見積もり一覧	検証想定内容を各サブプロセスに分解し、サブプロセス毎の役割分担、見積工数、業務内容と必要なスキルレベルについて記載する。
6）人材	
①役割、活動、責任	評価検証を実施する体制において、各人の役割、活動範囲、責任を一覧として作成する。
②雇用の必要性	評価検証を進めるにあたり、雇用の必要があれば、スキルイメージも含めて記載する。
③教育の必要性	評価検証の実行において、教育すべき内容があれば、記載する。
7)スケジュール	
検証スケジュール表	評価検証全体のスケジュール及び、マイルトーンを表としてまとめる。 評価検証環境の構築や、評価検証要件（仕様書）及び、検証項目のレビュー日程、評価検証完了日（報告日）等のマイルストンについても明記しておく。また、評価検証状況の中間報告のタイミングや周期についても、記載しておく。

4. 評価検証設計

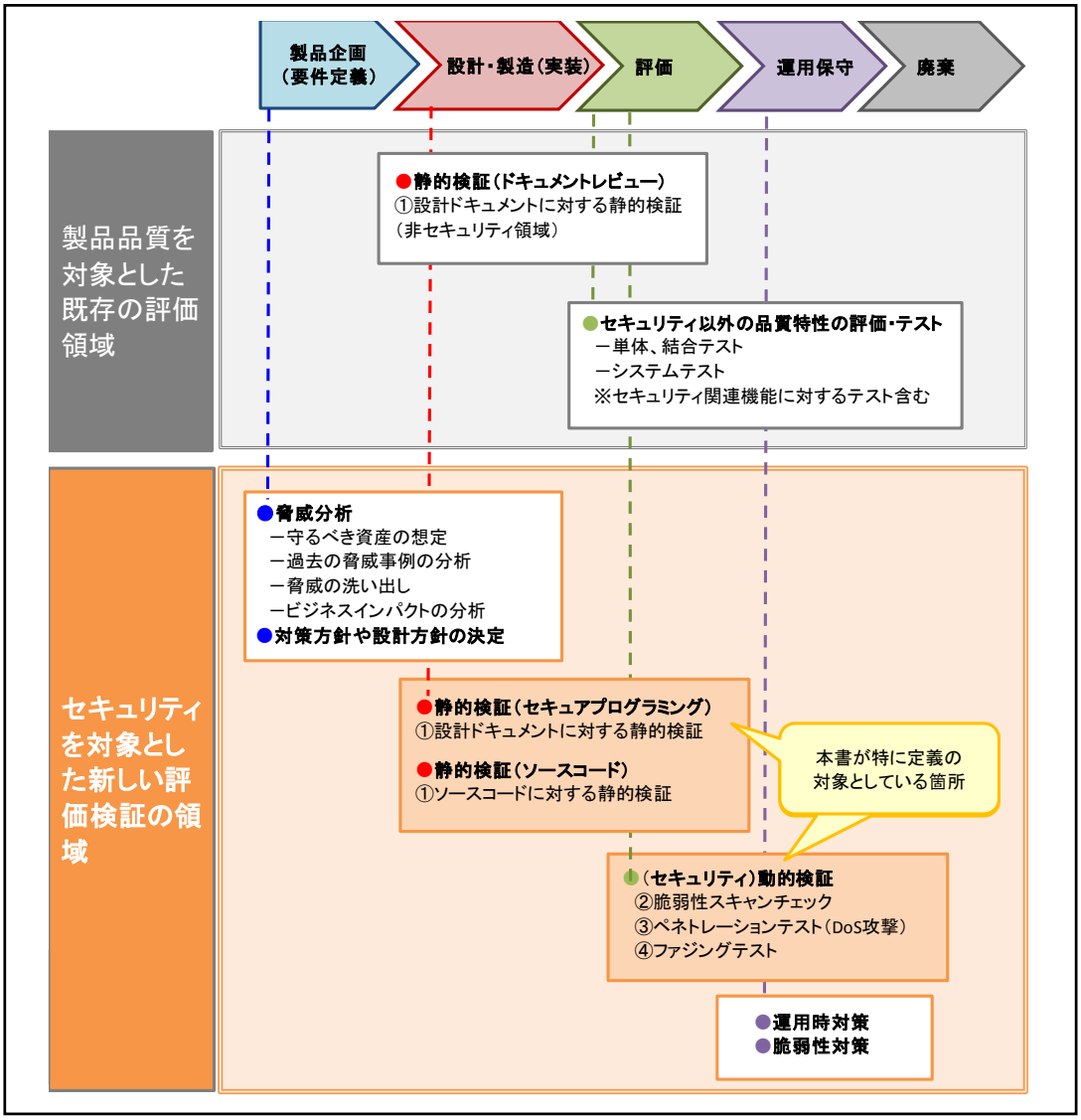
4-1. 製品開発ライフサイクルと関連するセキュリティ対策

セキュリティ検証では、「製品企画」フェーズにて脅威分析を行い、対象となるシステムやソフトウェアに、具体的にどのような脅威が潜在、どのような対策が必要となるかを事前に分析した上で評価検証設計に移行する。

以下の図に、製品ライフサイクルの各工程において必要なプロセスを記載する。「評価」フェーズ単独としてではなく、製品ライフルサイクル全体においてセキュリティ対策を念頭に置いた取り組みが必要である。またセキュリティ以外の品質特性についても、脆弱性の原因につながる可能性があるため、既存の製品品質を対象としたプロセスとも統合された管理体系が必要となる。

※具体的な脅威分析の手法については、「CCDS 製品分野別セキュリティガイドライン」[4][5][6][7]並びに IPA「つながる世界のセーフティ&セキュリティ設計入門」[13]等の参考資料を参照。

図 4-1.　製品ライフサイクルの各工程におけるセキュリティ対策



4-2. セキュリティ評価検証の手法

4-1 項に記載したセキュリティ評価検証の各手法について、以下にて説明を行う。評価検証手法はプトグラムの実行を伴わずにロジックの評価検証を行う静的な検証手法と、実際にプログラムを動作させた上で挙動を確認する動的な検証手法に大別され、それぞれ適応可能なフェーズが異なる。

また情報セキュリティに関する評価検証の手法については、NIST SP800-115[10]に、より詳細な内容が記載されており、本文書とあわせて参照を推奨する。

表 4-1.　セキュリティ評価検証手法の分類

種別	静的検証手法		動的検証手法	
	名称	利用フェーズ	名称	利用フェーズ
既知の脆弱性	①設計ドキュメントレビュー	設計・製造（実装）	②脆弱性スキャンチェック	評価検証
	①ソースコードレビュー	設計・製造（実装）	③ペネトレーションテスト	評価検証
	①コード規約検証	設計・製造（実装）		
未知の脆弱性			④ファジング	評価検証

4-2-1. 静的検証手法

①設計ドキュメントやソースコードに対する静的検証

・設計ドキュメントレビュー

各種設計ドキュメントに対して、「セキュリティバイデザイン」の考え方に基づき、必要なセキュリティ対策が組み込まれているかどうかをレビューによって確認する。

・ソースコードレビュー(解析)、コーディング規約検証

ソースコードに対して、セキュリティ上の脆弱性の検証や、コーディング規約に基づく実装が行われているかどうかの検証を行う。ソースコードに対する検証は各種静的検証ツールによる検証の自動化が主流であり、業務効率化のためにも有効に活用することが望ましい。

※静的脆弱性検証ツールについては、巻末の Appendix1.セキュリティ検証ツール一覧にて、

「表 A1-1.　主要な静的脆弱性検証ツール一覧」を掲載。

4-2-2. 動的検証手法

1)既知の脆弱性検証手法

各種検証ツールを使用することで、既知の脆弱性情報を元に、ソフトウェアやネットワーク上の脅威を自動で検査することが可能となる。

②既知の脆弱性スキャンチェック

・Web アプリケーション脆弱性スキャンツール

Web アプリケーションの脆弱性を検出することを主としたツールであり、OWASP や WASC が外部に公開している脆弱性情報を元に、主要な脆弱性の検出を行うことができる。一例を挙げると、不正な HTTP リクエストを送信し擬似攻撃を行うことで、クロスサイトスクリプティングや SQL インジェクション、Server Side Code インジェクション等の脆弱性を検出する事が可能である。

・ネットワーク脆弱性スキャンツール

ネットワークレイヤーの脆弱性を見つけることを目的としたツールであり、サーバやネットワーク機器の設定不備やパッチ適用の不備による、バッファオーバーフロー等の脆弱性を検出することができる。ネットワーク脆弱性スキャンツールは、正常あるいは不正なパケットを送信し、対象の DUT の挙動をモニターすることで脆弱性の有無を判定する。

※脆弱性スキャンツールについては、巻末の Appendix1.セキュリティ検証ツール一覧にて、

「表 A1-2.主要な脆弱性スキャンツール一覧」を掲載。

③既知の脆弱性情報に基づくペネトレーションテスト

既知の脆弱性情報を元に、実際に攻撃対象への侵入を想定したシナリオ（exploit データ）によって侵入可否の検証を行う。検証ツールの多くは、脆弱性スキャンツールと連携し、検出された脆弱性情報を元に exploit データの作成から侵入試験までをほぼ自動で実施可能となる。

また、攻撃対象への侵入の入り口として、ポートスキャンや DoS 攻撃が行われる可能性が高いため、解放ポートに対するスキャンチェックや各種 OSS を活用した DoS 攻撃に対する堅牢性をテストしておくことがセキュリティリスクを低減する上でも有効である。

※ペネトレーションツールについては、巻末の Appendix1.セキュリティ検証ツール一覧にて、

「表 A1-3.主要なペネトレーションツール一覧」を掲載。

2)未知の脆弱性検証手法

④ファジングテスト

ファジングテストとは、対象機器に対して「ファズ（fuzz)」と呼ばれる不正データを大量に送信し、その応答や挙動を監視することで脆弱性を検出する検査手法を指す。ファジングテストは、既知の情報として公開されていない潜在的な脆弱性を検出することに効果的と言われる手法である。

表 4-2.　ファジングテストの種類

ファジングの種類	説明
①コマンドラインのファジング	コマンドライン引数をファジングデータとして入力する。
②環境変数のファジング	CUI に対する環境変数をファジングデータとして入力する。
③ファイル形式のファジング	不正な画像や音声、動画データなどを作成し、メディア再生機器に読み込ませることで脆弱性を検出する。
④Web ブラウザのファジング	サーバからの HTTP レスポンスをファジングデータとして入力する。Web アプリケーションが広く用いられるため、検証用のツールも数多くリリースされている
⑤ネットワークプロトコルのファジング	TCP/IP や HTTP など、ネットワークプロトコルのデータ構造を元に入力データを作成する。
⑥Web アプリケーションのファジング	フォームへの入力値など、Web アプリケーションを対象としたファジング。

※ファジングツールについては、巻末の Appendix1.セキュリティ検証ツール一覧にて、

「表 A1-4.主要なファジングツール一覧」を掲載。

4-3. 評価検証仕様書の策定及び、評価検証ツールの選定

対象機器（DUT）に対する具体的な評価検証要件や、具体的な実施内容を決定するため、評価検証仕様書を策定する。評価検証仕様書では、製品企画フェーズで行った脅威分析結果をシステム構成に落とし込む「分析フェーズ」、対策の妥当性を評価検証するための手法やツールを調査するための「技術調査フェーズ」、調査結果をもとに具体的なテストケースを作成するための「評価検証仕様フェーズ」と順を追って進めていく。各フェーズの記録を文書化しておく事で、実施内容の策定経緯をエビデンスとして記録しておけると同時に、今後のプロセス改善にも活用することができる。

また、評価検証仕様については、該当のプロジェクトでどこまで評価検証（監査）を行うかを、明確にレベル定義しておき、顧客あるいは管理層や開発部門と協議のもと、合意の上で決定する必要がある。

図 4-2. 脅威分析～評価検証仕様書策定プロセス

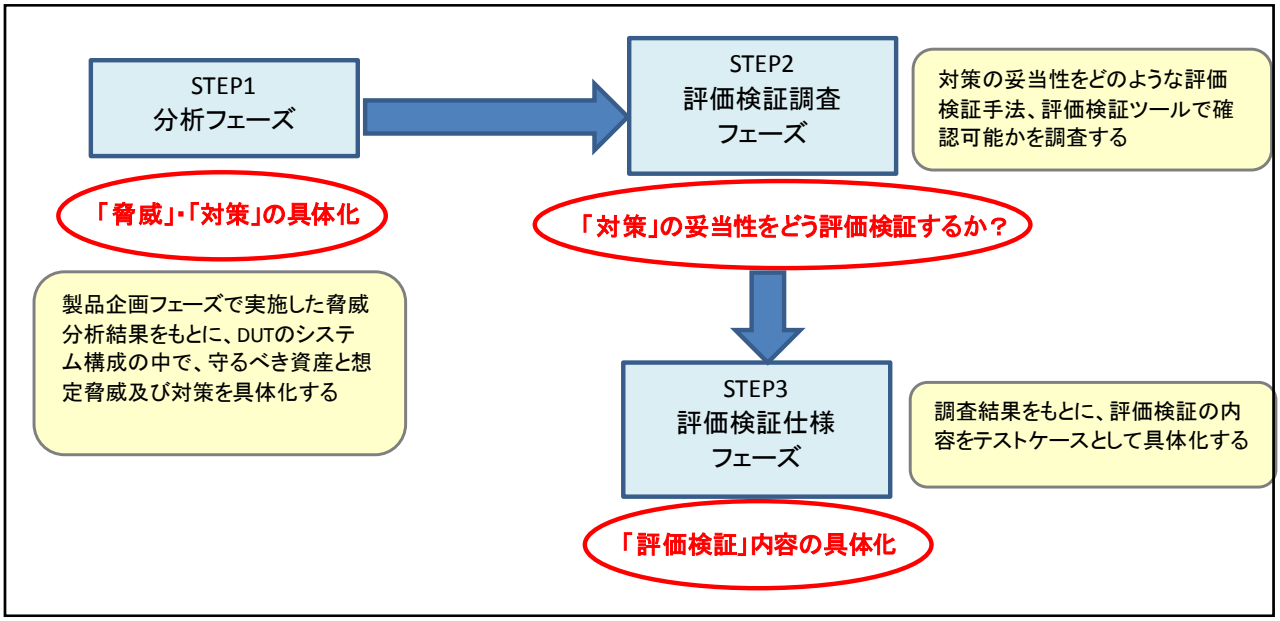


表 4-3. 評価検証仕様書の策定プロセス詳細手順

フェーズ	文書名	説明
STEP1 分析フェーズ	DUT の機器構成を理解し、守るべき資産と想定脅威、対策を明確化する	
	1-1)機器構成と想定脅威	DUT のシステム構成図において、データの入出力やインタフェースを踏まえ、想定される脅威を明確化する。 ※「参考 1）機器構成と想定脅威の記載ガイド」を参照。

	1-2)想定脅威への対策検討	保護すべき資産への想定脅威に対して、どのような対策が必要であるかを、Online Trust Alliance（OTA）の「OTA IoT Trust Framework」[11]や、OWASP の「OWASP Top 10 IoT Vulnerabilities」[12]等のフレームワークを参考に検討し、対応する対策番号を記載する。 ※脅威と対策の検討用に、「参考 1）機器構成と想定脅威の記載ガイド」として、スマートホームで想定される脅威や対策の記載事例を掲載。
STEP2 評価検証ツール調査フェーズ	実施した対策が実際に機能しているか、有効であるかを検証するため、適切な評価検証手法やツールを選定する。	
	2-1)通信プロトコル調査	DUT のインタフェース及び、通信プロトコルの仕様調査を行う。
	2-2)評価検証ツール調査	①評価検証ツール選定 対策を実施した OTA、OWASP の番号を参考に、評価検証の目的に合致したツールの調査を行う。上記の分析フェーズでまとめた脅威、対策に対して、必要な評価検証技術や評価検証ツールを対応づける。 ※調査結果をまとめる上での参考用として、下記に「参考 2）対策に対する評価検証手法の検討ガイド」を掲載。 ※ツール選定は、「Appendix1　セキュリティ検証ツール一覧」を参考とする。
		②インタフェース・プロトコル調査 上記①のツールが、DUT のインタフェースや通信プロトコルに適合しているか調査を行う。
	2-3)入出力解析	スキャンツール等を活用し、DUT 側へのデータ入出力方法の調査を行う。 ※TCP/IP ポートスキャン、Bluetooth の UUID 検索など、インタフェース毎に調査を行う。
	2-4)接続確認	DUT と評価検証ツールで接続試験を行い、検証結果の応答があるかを確認する。

STEP3 評価検証仕様フェーズ	必要な評価検証(監査)レベルの設定及び、ツールが保有する機能から、テストケースを作成する。	
	3-1）評価検証（監査）レベルの定義	予算や環境、ユースケースや運用状況に応じて、今回の検証において、どこまでの評価検証を実施するか、レベル定義を行う。 ※評価検証（監査）レベルの定義は、企業やプロジェクトの状況によって異なるため、顧客や意思決定層との合意の元に設定すること。 ※参考指標として、「参考 3）評価検証（監査）レベルの定義ガイド」を掲載。
	3-2)テストケース策定	選定したツールが有する評価検証機能を細分化し、具体的な検証内容を評価者が理解できるよう、テストケースとして整理する。 ※対応する評価検証データが存在する場合は、テストケースの個別項目と対応させて記載しておく。
	3-3)実行優先度設定	上記 3-2)のテストケースに対して、評価検証の優先順位を設定する。

注記）

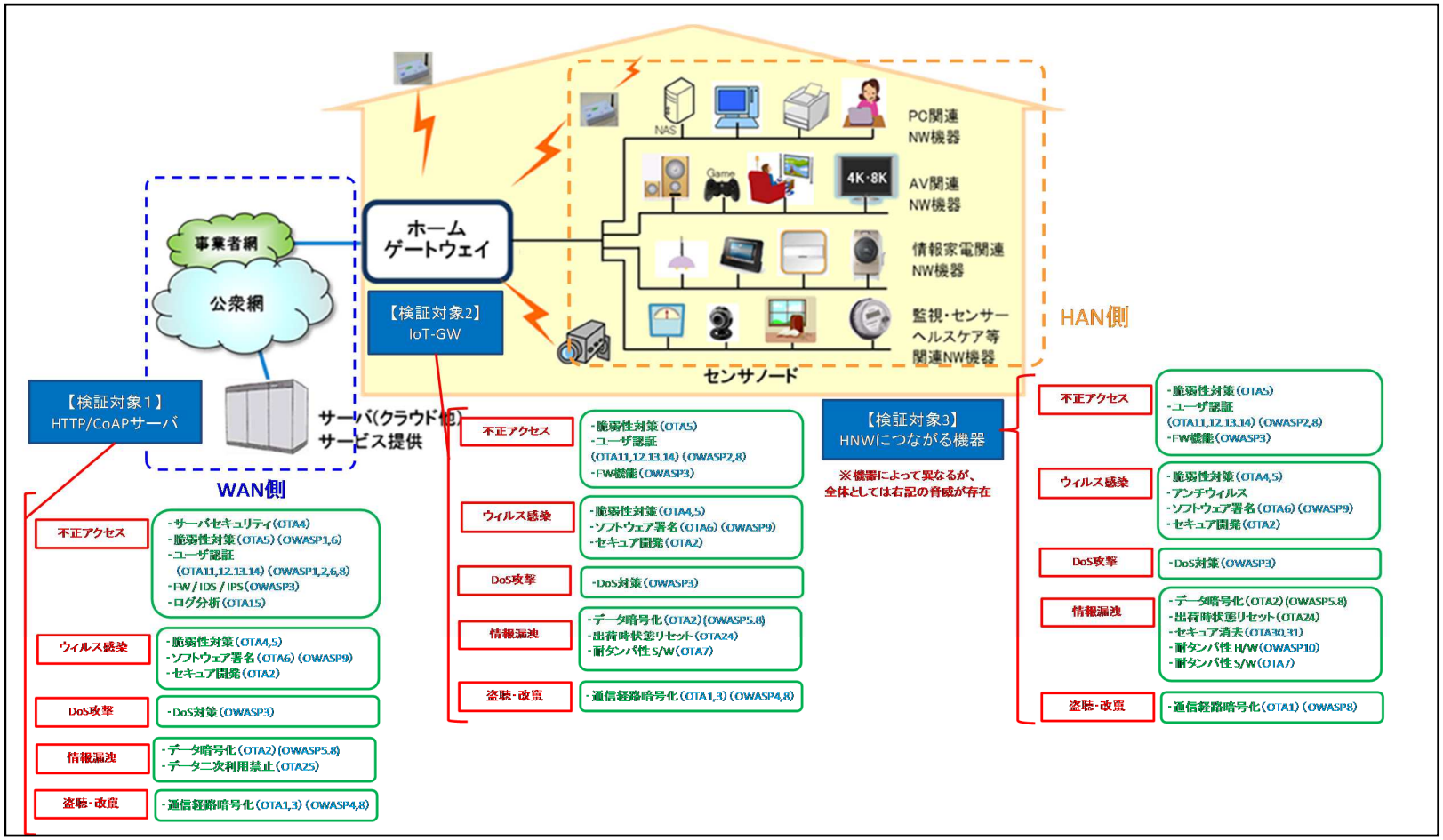
評価検証仕様書の策定プロセスを定義するにあたり、IPA 発行の「IoT 開発におけるセキュリティ設計の手引き」[13]を参考資料としており、本文書とあわせて参照を推奨する。

また、以下に記載している「参考１）～参考３）」については、本章記載の策定プロセスにおいて、具体的なアウトプットを想定した参考事例となる。本文書の巻末には「Appendix3　　評価検証仕様書の実例集」として、実際にスマートホームを対象に評価検証の実証実験を行った際の、仕様書をサンプル事例として掲載している。

参考 1）機器構成と想定脅威の記載ガイド

図 4-3. スマートホームにおける想定脅威と対策一覧

※参考用にスマートホームで想定される脅威と OTA、OWASP のフレームワークに基づく対策を抽出し、図表化した。



参考 2）対策に対する評価検証手法の検討ガイド

表 4-4. 想定脅威と対策及び、評価検証手法(ツール)の一覧

脅威			対策候補			検証手段	
発生個所	保護すべき資産	脅威名	対策名	他のガイドラインとの関係		検証手法	検証ツール
				OTA	OWASP		
サービスアプリ（サーバ）	・個人情報 ・設定情報 ・ログ情報 ・セキュリティ情報（電子証明書、暗号鍵、パスワード） ・金銭に紐づけられる情報 ・サーバ機器本体	不正アクセス	サーバセキュリティ	OTA4		ペネトレーションテスト	Metasploit
			脆弱性対策	OTA5	OWASP1,6	Webアプリ脆弱性検査	OWASP ZAP
			ユーザ認証	OTA11,12,13,14	OWASP1,2,6,8	ペネトレーション（Password攻撃対策）	Hydra
			FW/IDS/IPS		OWASP3	脆弱性検査	OWASP ZAP
			ログ分析	OTA15		システムテスト	–
		ウィルス感染	脆弱性対策	OTA4,5		脆弱性検査	OWASP ZAP
			ソフトウェア署名	OTA6	OWASP9	脆弱性検査	OWASP ZAP
		DoS攻撃	DoS対策		OWASP3	ペネトレーション（DoS攻撃対策）	Ostinate、Gatling
		情報漏洩	データ暗号化	OTA2	OWASP5,8	脆弱性検査	OWASP ZAP
			データ二次利用禁止	OTA25		ドキュメントレビュー※	※運用時のプライバシーポリシーを確認
		盗聴・改竄	通信経路暗号化	OTA1.3	OWASP4,8	脆弱性検査	OWASP ZAP
IoT-GW（ホームルータ）	・個人情報 ・設定情報 ・ログ情報 ・セキュリティ情報（電子証明書、暗号鍵、パスワード） ・IoT-GW本体	不正アクセス	脆弱性対策	OTA5		ネットワーク脆弱性検査	Open VAS
			ユーザ認証	OTA11,12,13,14	OWASP2,8	ペネトレーション（Password攻撃対策）	Hydra
			FW機能		OWASP3	ネットワーク脆弱性検査	Open VAS
		ウィルス感染	脆弱性対策	OTA4.5		ネットワーク脆弱性検査	Open VAS
			ソフトウェア署名	OTA6	OWASP9	ネットワーク脆弱性検査	Open VAS
			セキュア開発	OTA2		設計ドキュメントレビュー ソースコードレビュー コード規約検証	–
		DoS攻撃	DoS対策		OWASP3	ペネトレーション（DoS攻撃対策）	Ostinate、Gatling
		情報漏洩	データ暗号化	OTA2	OWASP5.8	ネットワーク脆弱性検査	Open VAS
			出荷状態リセット	OTA24		システムテスト ドキュメントレビュー※	※ユーザマニュアルを含めた確認を実施
			耐タンパ性S/W	OTA7		設計ドキュメントレビュー ソースコードレビュー コード規約検証	–
		盗聴・改竄	通信経路暗号化	OTA1.3	OWASP4,8	ネットワーク脆弱性検査	Open VAS
		その他 未知の脆弱性	–	–	–	ファジングテスト	Sulley
HNWにつながる機器	・個人情報 ・設定情報 ・ログ情報 ・セキュリティ情報（電子証明書、暗号鍵、パスワード） ・金銭に紐づけられる情報 ・機器本体	不正アクセス	脆弱性対策	OTA5		脆弱性検査※	※DUTがサーバ機能を有する場合にのみ有効
			ユーザ認証	OTA11,12,13,14	OWASP2,8	ペネトレーション（Password攻撃対策）	Hydra
			FW機能		OWASP3	脆弱性検査※	※DUTがサーバ機能を有する場合にのみ有効
		ウィルス感染	脆弱性対策	OTA4.5		脆弱性検査※	※DUTがサーバ機能を有する場合にのみ有効
			アンチウィルス			システムテスト ドキュメントレビュー※	※ユーザへの注意喚起
			ソフトウェア署名	OTA6	OWASP9		
			セキュア開発	OTA2		設計ドキュメントレビュー ソースコードレビュー コード規約検証	–
		DoS攻撃	DoS対策		OWASP3	ペネトレーション（DoS攻撃対策）	Ostinate、Gatling
		情報漏洩	データ暗号化	OTA2	OWASP5.8	脆弱性検査※	※DUTがサーバ機能を有する場合にのみ有効
			出荷状態リセット	OTA24		システムテスト ドキュメントレビュー※	※ユーザマニュアルを含めた確認を実施
			セキュア消去	OTA30,31		システムテスト	–
			耐タンパ性H/W		OWASP10	リバースエンジニアリング※	※必要に応じて対応
			耐タンパ性S/W	OTA7		設計ドキュメントレビュー ソースコードレビュー コード規約検証	–
		盗聴・改竄	通信経路暗号化	OTA1	OWASP8	脆弱性検査※	※DUTがサーバ機能を有する場合にのみ有効
		その他 未知の脆弱性	–	–	–	ファジングテスト	Sulley

参考 3）評価検証（監査）レベルの定義ガイド

表 4-5.　スマートホームにおける評価検証（監査）レベルの定義事例

※以下の表では HAN 側の機器をまとめて定義しているが、実際の評価検証では個別機器ごとに要件定義を行う必要がある。

対象（保護すべき資産）	守るべき資産	想定脅威	対策レベル						備考・留意事項
			Level1		Level2		Level3		
			検証内容	利用ツール（例）	検証内容	利用ツール（例）	検証内容	利用ツール（例）	
サービスアプリ（サーバ）	・個人情報 ・設定情報 ・ログ情報 ・セキュリティ情報 （電子証明書、暗号鍵、パスワード） ・金銭に紐づけられる情報 ・サーバ機器本体	不正アクセス ウィルス感染 DoS攻撃 情報漏洩	・Webアプリ脆弱性スキャンチェック	OWASP ZAP	Level1の検証	―	Level2の検証	―	サーバに対する検査は、不正アクセス禁止法に抵触しないよう、サーバ管理企業（サービス提供企業）との合意において検証を行う必要がある。
			・ペネトレーションテスト1 ―DoS攻撃対策	Ostinate、Gatling	・静的脆弱性検証 ―設計ドキュメントレビュー ―ソースコードレビュー ―コーディング規約検証	iCodeChecker（※） ※ソースコード	・ペネトレーションテスト3 ―既知の脆弱性に対する総合的な検証	Metasploit	
			・ペネトレーションテスト1 ―Password攻撃	hydra					
IoT-GW（ルータ）	・個人情報 ・設定情報 ・ログ情報 ・セキュリティ情報 （電子証明書、暗号鍵、パスワード） ・IoT-GW本体	不正アクセス ウィルス感染 DoS攻撃 情報漏洩 盗聴・改竄	・ファジングテスト	Sulley （HTTP、CoAP対応）	Level1の検証	―	Level2の検証	―	ファジングについては、対応プロトコルに合わせてツールの選定を行うこと
			・ネットワーク脆弱性スキャンチェック	Open VAS	・静的脆弱性検証 ―設計ドキュメントレビュー ―ソースコードレビュー ―コーディング規約検証	iCodeChecker（※） ※ソースコード	・ペネトレーションテスト3 ―既知の脆弱性に対する総合的な検証	Metasploit	
			・ペネトレーションテスト1 ―DoS攻撃検査	Ostinate、Gatling					
			・ペネトレーションテスト1 ―Password攻撃	hydra	・ペネトレーションテスト2 ―WiFI攻撃	Aircracking-ng			
HAN側の接続機器	・個人情報 ・設定情報 ・ログ情報 ・セキュリティ情報 （電子証明書、暗号鍵、パスワード） ・金銭に紐づけられる情報 ・機器本体	不正アクセス ウィルス感染 DoS攻撃 情報漏洩 盗聴・改竄	・ファジングテスト	Sulley （HTTP、CoAP対応）	Level1の検証	―	Level2の検証	―	ファジングについては、対応プロトコルに合わせてツールの選定を行うこと
			・ペネトレーションテスト1 ―DoS攻撃検査	Ostinate、Gatling	・静的脆弱性検証 ―設計ドキュメントレビュー ―ソースコードレビュー ―コーディング規約検証	iCodeChecker（※） ※ソースコード	・ペネトレーションテスト3 ―既知の脆弱性に対する総合的な検証	Metasploit	
			・ペネトレーションテスト1 ―Password攻撃	hydra					

4-4. 評価検証手順書の策定

4-3 項で作成したテストケースをもとに、具体的な検証手順を追加した評価検証手順書を策定する。評価検証手順書は、評価検証者が正確に評価検証を行えるよう、詳細化した実施手順を記載しておく。また、使用する評価検証データやパラメータを明確化しておくで、評価検証結果のエビデンスとしての精度を高めることができる。

評価検証手順書はシステムテスト等に用いる標準的なテストフォーマットを利用しても問題ないが、ツール側が出力した結果と、評価検証者が最終的に判定した結果を、それぞれ区別して記録できる形式が必要である。

4-5. 評価検証データの準備

・例）ファジングデータの作成方法

脆弱性スキャンやペネトレーションテストについては、既知の脆弱性や exploit データをもとに検証を行うため、ツール側が利用している脆弱性情報が最新であるかが重要であり、評価検証者が新規に評価検証用のデータを作成するケースは少ない。一方でファジングテストについては、特に OSS を使用する場合、ファズデータを評価検証者が新規に作成する場合がある。以下では、一般的なファジングデータの作成方法について記載するが、詳細については、IPA「ファジング実践資料」[14]等の参照を推奨する。

表 4-7.　ファジングデータの種類

データ構造の解釈	データ作成手法	説明
解釈する	スマートファジング（Smart fuzzing） ※Generation based fuzzing、Intelligent fuzzing とも呼ばれる。	データ構造の要素をそれぞれ細工してデータを作成する。データ作成は非常に時間が掛かるが、効率は高い
解釈しない	ミューテーションファジング（Mutation fuzzing）	正常なデータを読み込み、そのデータをランダムな値に変更する。データ作成はある程度容易であり、効率性も比較的高い。
	ランダムファジング(Dumb	まったくランダムな値からデータを作成する。データ

	fuzzing)	作成は容易だが、効率が悪い
その他	自動（プロトコル）生成	一定の原則に従って、指定の範囲内で連続的に値を変化させてデータを生成する。

表 4-8.　データの作成方法の一例

特定の脆弱性検出に特化した値	
バッファオーバーフローの脆弱性	極端に長い文字列（例：「A」1000 個以上）
書式文字列の問題	C 言語の printf()関数などで使う書式文字列 （例：「%s%s%s%s」）
数値処理に関する問題（整数オーバーフローの脆弱性など）	バッファの上限値や下限値として使われそうな数値やプログラミング言語のデータ型のサイズに関連する数値（例：0、65535 や 65536）
特別な意味を持つ値	
ヌルバイト（NULL）	「0x00」（16 進数表記） （C 言語などの言語処理系では、文字列の終端を意味する）
区切り文字	データ構造におけるデータの区切りを意味する値 例１：改行コードや（「0x0d」(16 進数表記)や「0x0a」（16 進数表記） 例２：「“」や「＃」

（出典：IPA 発行「ファジング実践資料」[14]）

5. 評価検証実行

5-1. セキュリティ評価検証の実行

セキュリティ評価検証の実行は、自動化されたツールを用いた場合でも評価検証内容の組み合わせによって、実行処理完了までに時間を要する可能性がある。ツールの実行所要時間については、事前に把握しておくことが望ましい。

ツールによる検証完了後の出力結果については、ツールが出力した結果に対して、ログ情報等をもとに、結果の正当性を評価検証者が解析し、結果判定を行う必要がある。また評価検証者が正しい判定を行うためには、DUT 側のプログラムに関する知識や、ツール側の結果判定ロジックについても理解しておくことが必要となる。以下では、評価検証者が結果判定を行うために必要な情報やナレッジを記載する。

表 5-1. 評価検証の実行及び、最終的な結果判定に必要な情報・ナレッジ

※評価検証ツールによっては、ログ情報を外部ファイルとして出力する機能を持たない場合があり、注意が必要である。

名称	情報種別	説明
検証ツールの操作、設定に関する知識	マニュアル	検証ツールの操作、構築、設定方法に関する知識。
評価検証内容に関する知識	評価検証仕様、検証項目	ツール側の検評価証内容の詳細項目及び、その内容に関する知識。
評価検証ツールの結果判定処理に関する知識	ドキュメント	ツール側がどのようなロジックで結果判定処理を行うのか、その内容に関する知識。 例）ファジングでは不正データ送信後、正常なリクエストを DUT に送信し、DUT からの応答の挙動や遅延を監視する。 ※ツールによっては、判定ロジックがブラックボックスのものも存在する。
DUT 側のプログラムに関する知識	設計ドキュメント	DUT に関する要件定義、設計ドキュメント及び、その内容に関する知識。
DUT 側のプログラムのログ	ログ情報	原因の切り分けに活用するための、プログラムのログ及び解析知識。
評価検証ツールの実行ログ	ログ情報	ツール側の実行過程を記録したログ情報及び、その内容を解析できる知識。 ※例）シーケンスログ、DUT 側の応答シーケンスや応答パラ

		メータ値など
評価検証ツールの結果ログ	ログ情報	ツール側の判定処理を経由した出力結果及び、その内容を解析できる知識。 ※例）判定結果、脆弱性と想定される理由や箇所などの情報を含めた詳細

※検証実行時の注意事項

セキュリティ検証は DUT に対して、不正信号を送信するものが多いため、DUT 以外のデバイスに誤送信しないよう十分注意する必要がある。可能であれば、シールドルーム等の電波遮断環境を利用し、DUT と検証ツールが 1 対 1 で検証を行うことが望ましい。

5-2. 検出されたインシデント情報の管理方法

評価検証実行によりインシデントが検出された場合には、以下の項目を参考に、インシデントレポートを起票し、情報管理を行う。インシデント情報は、評価検証部門と顧客あるいは開発部門で共有し、該当する問題が、セキュリティの脆弱性にかかわる内容かどうかを両部門で精査を行うことを推奨する。

5-2-1. インシデントレポートフロー

評価検証実行の結果、不正な挙動が確認された場合、インシデントとしてレポート報告を行うが、評価検証部門単独ではセキュリティ上の脆弱性につながるインシデントかどうかは、プログラム側の解析が必要となり、判断が難しいケースもある。推奨する報告フローとしては、判断が難しい場合には DUT 側の不正な挙動を不具合インシデントとしてレポート報告の上、開発部門との協議を経て、脆弱性につながる課題については、別途セキュリティインシデントとしてレポート報告することが望ましい。レポート報告や管理が煩雑になるようであれば、セキュリティインシデントのレポートのみの運用とし、評価検証部門と開発部門でディスカッション可能なフォームを設定し、双方の意見をエビデンスとして記録しておくことで、効率化を図ることも可能である。

5-2-2. セキュリティインシデントレポートの記載項目

セキュリティインシデントのレポート記載項目については、IPA が IEEE1044 などのグローバル標準との整合性を考慮した作成した ESBR[15]を参考にセキュリティに関する項目を追加した案を以下に記

載する。例えば、インシデントの深刻度や、既存の脆弱性データベース（JVN や、NVD、OSDBD）に登録されている脆弱性識別番号、CWE（共通脆弱性識別子）などは、インシデントの改修優先度の判定や原因分析に有効な情報である。

表 5-2.　インシデント情報の記載項目要件

項目名	担当	記載内容の説明
1）インシデント内容		
管理番号	検証部門	インシデント管理番号 ※各検証プロジェクトを通じて、一意の値が望ましい。 ※同一原因の管理番号を記載できることを推奨。
プロジェクト名	検証部門	検証あるいは開発プロジェクト名
深刻度基準	検証部門	※4-2-4 項を参照
ステータス	検証部門	インシデントレポートのステータス 例）作成中、仮登録済み、本登録済み、差戻し、改修中、改修完了、クローズ等
クローズ理由	検証部門	インシデントレポートをクローズした理由を記載 例）改修済、次機種検討、現状通り、ドキュメント修正
発行日	検証部門	インシデントレポートの発行日(登録日)を記載
完了日	検証部門	インシデントレポートをクローズした日付を記載
レポートタイトル	検証部門	インシデントレポートのタイトル ※200 文字以内で、簡潔かつインシデントの重要性を示すタイトルが望ましい。
発行者名	検証部門	インシデントレポートの起票者名を記載
内容	検証部門	下記の記載内容をカバーすること ・試験環境 ・設定条件 ・試験手順 ・発生する問題 ・期待する動作 ・発生条件

添付ファイル	検証部門	内容を補足するログデータ等、添付資料を付加する。
機能名 （サブシステム名）	検証部門	対象のシステムやソフトウェアの機能名を記載する
発見バージョン	検証部門	インシデントを確認したバージョンを記載する
発生環境	検証部門	インシデントを確認した環境を記載する 例）テスト環境など、
発生頻度	検証部門	試行回数に対するインシデントの発生回数を記載する 例）XX（発生回数）/YY（試行回数）
発見工程	検証部門	インシデントを発見した工程
発見手段	検証部門	コードレビューやテスト名称等、インシデントを発見した工程名称を記載する。
評価検証項目番号	検証部門	インシデントを発見した評価検証項目の番号を記載する。
検証シナリオ名	検証部門	インシデントを発見した検証シナリオ名（あるいはシナリオ番号）を記載する。
影響を受けるシステム	検証部門	インシデントによって影響が想定される機能名やサブプロセスを記載する。
想定される影響	検証部門	インシデントによって、どのような影響が想定されるのか具体的な内容を記載する。
参考情報	検証部門	JVN、NVD における関連インシデント番号。CVE 番号や CWE 識別子等、解析に役立つ情報や関連情報を記載する。
２）開発調査内容/対策		
処置担当者	開発部門	インシデントの原因調査や改修対応等の処置に対する担当者名を記載する。
処置完了日	開発部門	処置の完了日を記載する。
発生原因	開発部門	インデントの発生原因を記載する。
原因箇所	開発部門	バグが発生した原因を含むソフトウェア成果物。仕様書であれば仕様書名（ファイル名）とその頁、行数など。ソースコードであれば、ファイル名、関数名、行数なし。
対応見積工数	開発部門	修正を行う場合の見積工数を記載する
解決方法/処置内容	開発部門	解決方法、修正内容あるいは対応方針を記載する。

処置区分	開発部門	開発部門としての対応方針を記載する。 例）仕様通り、プログラム改修、ドキュメント対応、次機種対応、対応見送り等。
修正対象	開発部門	修正や改修を行った仕様書名や、ソフトウェアコードのファイル名等を記載する。
修正バージョン	開発部門	修正を行ったバージョン名称を記載する。
リリース日	開発部門	修正バージョンのリリースに日時を記載する。
3）その他、分析やフォードバックに活用する項目		
不具合区分	開発部門	インシデントの原因となった不具合の分類区分を記載する。今後のフィードバックや分析に活用できるよう IPA 発行の ESBR[15]等に準拠した分類項目が望ましい。
作り込み工程	開発部門	インシデント原因となる不具合を作り込んだ工程を記載する。 例）システム要求定義（ システム要求分析)、システムアーキテクチャ設計（ システム方式設計)、ソフトウェア要求定義（ ソフトウェア要求分析)、ソフトウェアアーキテクチャ設計（ソフトウェア方式設計)、ソフトウェア詳細設計（ソフト ウェア詳細設計)、実装（コーディング)。
調査工数	開発部門	インシデントの原因調査に要した工数を記載する。
処置工数	開発部門	インシデントの改修対応に要した工数を記載する。
発見すべき工程	開発部門	本来インシデントや原因となった不具合を発見すべき工程を記載する。
発見すべきアクティビティ	開発部門	本来インシデントや原因となった不具合を発見すべきアクティビティを記載する。※アクティビティ：工程作業を、さらに分割し、順序付けした作業要素。
4）ディスカッションエリア		
ディスカッション	開発部門 及び 開発部門	検出されたインシデントについて、実際にセキュリティの脆弱性につながる問題かどうかを、検証部門と開発部門とでディスカッションを行い、精査する。ディスカッション内容はエビデンスとして、インシデント情報の一要素として管理しておく。

■インシデントレポートのフォーマット事例

CCDS が構築した「組込機器検証基盤システム」では、上記の要件を網羅したインシデントレポートの作成、管理が可能であり、レポートフォーマットの参考例として掲載する。CCDS の検証基盤システムでは、CVSSv3[16]による深刻度判定を機能として組込んでおり、必要事項を入力する事で、深刻度の数値判定が自動で出力される。また検証基盤では、インシデントレポートとセキュリティ品質レポートが連携しており、インシデントの数や深刻度に応じて、品質判定のスコアリングが自動的に決定する機能を実装している。※詳細は「5-3. 報告・評価検証完了」）を参照。

図 5-1.　脅威内容のフォーム事例

出展：CCDS「組込機器検証基盤システム」の脅威レポート作成機能より

図 5-2.　CVSSv3 による深刻度入力フォーム事例

出展：CCDS「組込機器検証基盤システム」の脅威レポート作成機能より

図 5-3.　脅威に関する影響や補足情報のフォーム事例

出展：CCDS「組込機器検証基盤システム」の脅威レポート作成機能より

図 5-4.　ディカッションエリアのフォーム事例

出展：CCDS「組込機器検証基盤システム」の脅威レポート作成機能より

図 5-4.　インシデントの要因や対応方針などのフォーム事例

出展：CCDS「組込機器検証基盤システム」の脅威レポート作成機能より

5-2-3. セキュリティインシデントの深刻度基準について

検出されたインシデントについては、リスク評価手法による判断基準に沿って深刻度を記載する。リスク評価手法については、既に各種団体より公開されており、それぞれにリスクファクタや特徴が異なり、評価検証対象によって判定の妥当性に差異が生じる恐れがある。以下に記載した代表的なリスク評価手法から、対象となるシステムやソフトウェアによって適切な深刻度基準を選択し、判定を行うことを推奨する。

表 5-3. スマートホーム分野への活用可能なインシデント(リスク)評価手法の紹介

※詳細については、巻末の「Appendix4 リスク評価手法の紹介」を参照。

	名称	リスクファクタ・特徴
1	CVSSv3[16]	■リスクファクタ 詳細は、巻末の「Appendix4 リスク評価手法の紹介」を参照。 1)基本評価基準（Base Metrics） ・「機密性」、「完全性」、「可用性」に対する影響から評価 2)現状評価基準（Temporal Metrics） ・攻撃コードの出現有無や対策情報が利用可能といった基準で評価 3)環境評価基準（Environment Metrics） ・二次的被害の大きさや、対象製品の使用状況といった基準で評価 ■特徴 機密性、完全性、可用性に対する影響を主軸に、詳細なリスク評価が可能。 リスクファクタが詳細に定義されており、NIST SP800-30 と同様に具体的な脆弱性が明確になっていないと、評価が困難なファクタが存在する。
2	NIST SP800-30[17]	■リスクファクタ 1)THREAT SOURCES（脅威源） 2)THREAT EVENTS（脅威内容） 3)VULNERABILITIES AND PREDIPONSING CONDITIONS（脆弱性と発生条件） 4)LIKELIHOOD OCCURRENCE（発生の可能性） 5)IMPACT（影響度） ■特徴

		リスクファクタに対する計算式が定義されていない。脅威に関する評価項目は、充実しているが、具体的なインシデントが明らかになっていないと評価が困難なパラメータが存在する。
3	GMITS(ISO/IEC TR13335[18]	■リスクファクタ 1)Asset（資産価値） 2)Threat（脅威） 3)Vulnerability（脆弱性） ■特徴 リスクファクタに対する計算式は定義されていない。リスクファクタの数は少ないが、「資産価値」が定義されている。
4	ETSI TS102 165-1[19]	■リスクファクタ 1)Likelihood（攻撃の可能性） 1-1)Time（攻撃に要する時間） 1-2)Expertise(攻撃者のスキル) 1-3)Knowledge(システム知識) 1-4)Opportunity（攻撃の機会） 1-5)Equipment（設備） 2)Impact（影響度） 2-1)Asset Impact（資産への影響） 2-2)Attack Intensity（攻撃の強度） ■特徴 リスクファクタが詳細なため、具体的な脆弱性に対する分析に向いているが、事前の脅威分析では判定が困難なファクタがある。Time に高いウェイトが設定されているため、注意が必要。
5	情報マネジメントシステム(ISMS)ISO/IEC27001	■リスクファクタ 1)資産の価値 2)脅威 3)脆弱性 ■特徴 具体的な計算式については、JPDEC(日本情報経済社会推進協会)による例

		示のみであり、規格としては提示されていない。
6	OCTAVE Allegro[20]	■リスクファクタ 1)Impact Area： 1.評判（Reputation） 2.Financial（金銭） 3.Productivity（生産性）、 4.Safety&Health（安全、健康） 5.Fines/Legal（罰金・法律） 2)Impact Value：Impact Area に対する影響度を High、Mid、Low の 3 段階に分けたもの。 ■特徴 「Safety & Health（安全・健康）」がリスクファクタとして組み込まれている一方で脆弱性に関するファクタが存在しない。優先度や影響度の設定において主観に左右されやすい。
7	The OWASP Risk Rating Methodology[21]	■リスクファクタ 1)Threat agent（脅威の要因） 2)Vulnerability（脆弱性の要因） 3)Technical Impact(テクニカルインパクト) 4)Business Impact（ビジネス上の影響度）の 4 つの値の平均値によって、全体的なリスクを計算。 ■特徴 金銭等の資産損失や、ブランド・信用棄損がリスクファクタに含まれる特徴がある。ファクタが多く、平均値によって総合リスクを判定するため、個別ファクタの数値にウェイトが存在しないため、全体に影響しにくい。
8	FAIR[22]	■リスクファクタ 1)LEF：損失発生頻度 （発生頻度、脅威難易度、保護強度、脆弱性） 2)PLM：金銭的な影響度によって評価。 ■特徴 PLM の評価値が全体の結果に与える影響度が大きいという特徴がある。

9	CCDS 改良方式 0	■リスクファクタ 1)難易度 2)影響度 3)攻撃者のモチベーション ■特徴 特徴としては既存のリスク評価手法と比較し、より簡易に分析が可能であり、またリスクファクタに「攻撃者のモチベーション」が組み込まれ、影響度の基準として「人命リスク」を想定した基準を定義している。

5-3. 報告・評価検証完了

5-3-1. 評価検証の実施状況に関する報告

セキュリティ検証の実行状況に関する報告（中間報告）の頻度やタイミングについては、顧客あるいは開発部門と協議の上、決定し、評価検証計画書に記載しておく。

なお評価検証の実行状況については、ISO/IEC/IEEE29119[9]のマネージメントプロセスに従い、評価検証計画書に記載されたスケジュールやマイルストン通りに進んでいるかを監視し、実行管理される。

表 5-4.　中間報告における記載要件

項目	記載内容
進捗に関する報告事項	
進捗状況のサマリ	簡潔なコメントにて、現状の進捗状況を説明する。
検証実行の進捗状況	検証手順書項目における実施完了数／全検証項目に対する進捗率を記載する。
実績工数	計画工数に対して現在までに要した実績工数を記載。
課題	現状の進捗において課題があれば、対策も含めて記載する。
セキュリティ品質に関する報告	
セキュリティ品質状況のサマリ	簡潔なコメントにて、現在のセキュリティ品質の状況を説明。
不具合・セキュリティインシデント	これまで検出されたインシデントの総数、内容のサマリ一覧(タイトル、概要、深刻度、クローズ状況等)を記載。
検証実行における現状課題	

課題	検証環境やデータ、進捗、インシデントに関する問題など、評価検証全般に係る課題事項を報告する。

5-3-2. 評価検証の完了報告

セキュリティ評価検証の完了については、計画書記載の完了条件に従うものとし、完了時には完了報告を行う。完了条件については、製品品質のテストと同様に、実施すべき全評価検証項目の完了及び、インデントレポートの全件完了をもって、完了することが望ましい。

表 5-5. 完了報告における記載要件

項目	記載内容
セキュリティ品質に関する報告	
セキュリティ品質判定	評価検証結果として、合格／不合格の結果を判定基準と共に記載。
品質状況のサマリ	簡潔なコメントにて、完了時点のセキュリティ品質状況を説明する。
不具合・セキュリティインシデント	評価検証を通じて検出された全インシデントの総数、内容のサマリ一覧(タイトル、概要、深刻度、クローズ状況等)を記載。
評価検証実施項目に関する報告	
評価検証実行状況に関するコメント	簡潔なコメントにて、完了時の状況を説明する
評価検証完了状況	評価検証手順書項目における実施完了数／全評価検証項目に対する進捗率（全件完了していることを前提とする）
実績工数	計画工数に対して、完了までに要した実績工数を記載。
その他申し送り事項等	
課題	評価検証環境やデータ、進捗、インシデントに関する問題など、評価検証全般に係る課題事項を報告する。

6. 評価検証プロジェクトの総括・フィードバック

評価検証完了後は、検証用ドキュメントを情報資産として管理しておくと共に、評価検証計画書において「収集するメトリクス」として定義した項目については、次回の開発や評価検証プロセスにフィード

バックを行い、評価検証の効率や品質の向上に活用する。収集するメトリクスについては、評価検証完了時にプロジェクトとして総括を行い、次回以降のデータ活用に向けて整理をしておく。

表 6-1. 収集メトリクスとフィードバック活用

1)効率向上に利用可能なメトリクス	
収集メトリクス	説明
①評価検証内容	・評価検証ツールが実行完了に要した時間
②計画予定工数と実績工数	・予定工数を超過した場合には、その理由や対象のサブプロセス名称 ・1 日/1 工数に対する検証項目数
③評価検証スケジュール/マイルストンに対する進捗の予実	・遅延が発生した場合には、その理由と対象サブプロセス名称 ・1 日あたり検証項目数
④その他	・事前準備や環境構築において、想定通りにいかなかったことなど
2)開発、評価検証プロセスの品質向上に利用可能なメトリクス	
①検証内容	・実施した評価検証項目(手順) ・評価検証実施結果（検証ツール別のインシデントヒット数など） ・追加した評価検証データ、評価検証シナリオ
②セキュリティインシデントレポート （不具合レポート）	・インシデントレポートの内容 ・インシデントの原因 ・発見した手法（ツール名、シナリオ名）
③開発部門、顧客からの指摘事項	・問い合わせ、クレーム、アドバイス事項など
④その他	・品質上の改善点や気づいた点など

7. まとめ

各団体が作成したセキュリティガイドラインと本書との対応関係を以下に示す。(枠内の評価検証プロセスを詳細に定義したものが本文書となる)

表 7-1. 本書と対応する他団体のガイドラインとの対応表

IoT推進コンソーシアム「IoTセキュリティガイドライン」			IPA「つながる世界の開発指針」			CCDS「セキュリティガイドライン IoT-GW編」	
2.1 方針・管理	要点1	経営者がIoTセキュリティにコミットする	方針	指針1	安心安全の基本方針を策定する	4.2.1	製品企画フェーズ 項番3:施策として情報セキュリティ方針について記載。
				指針2	安心安全のための体制・人材をも見直す	4.2.1	製品企画フェーズ 項番3:施策として情報セキュリティ方針について記載。
						4.2.4	運用フェーズ2:施策として組織の体制について記載。
	要点2	内部不正やミスに備える		指針3	内部不正やミスに備える	4.2.2	設計・製造フェーズ 項番6:施策として開発時の外部委託における取り組みについて記載。
2.2 分析	要点3	守るべきものを特定する	分析	指針4	守るべきものを特定する	2	2章:実施例としてシステム構成を定義し、各ユースケースにおける保護すべき資産をリストアップ。
						4.2.1	製品企画フェーズ 項番1,2:施策としてリスク分析について記載。
						5	5章:実施例としてリスク分析の中で保護すべき資産について記載。
	要点4	つながることによるリスクを想定する		指針5	つながることによるリスクを想定する	2	2章:実施例として各ユースケースにおける被害・影響をリストアップ。
						3.3	3.3:想定されるセキュリティ上のリスク例について記載。
						4.2.1	製品企画フェーズ 項番1,2:施策としてリスク分析について記載。
						5	5章:ユースケースにおけるリスク例について記載。
	要点5	つながりで波及するリスクを想定する		指針6	つながりで波及するリスクを想定する	(同上)	指針5と同一。
	要点6	物理的なリスクを認識する		指針7	物理的なリスクを認識する	4.2.1	製品企画フェーズ 項番1,2:施策としてリスク分析について記載。
						4.2.2	設計・製造フェーズ 項番5:施策として物理的な攻撃に対する対策について記載。
						5	5章:ユースケースにおける物理的リスク例について記載。
	要点7	過去の事例に学ぶ					
2.3 設計	要点8	個々でも全体でも守れる設計をする	設計	指針8	個々でも全体でも守れる設計をする	4.2.2	設計・製造フェーズ 項番2,5:施策としてセキュリティ機能の実装について記載。
	要点9	つながる相手に迷惑をかけない設計をする		指針9	つながる相手に迷惑をかけない設計をする	4.2.2	設計・製造フェーズ 項番2:施策として迷惑をかけないための機能について記載。
	要点10	安全安心を実現する設計の整合性をとる		指針10	安全安心を実現する設計の整合性をとる	4.2.1	製品企画フェーズ 項番1,2:施策として安心安全を実現するための脅威の抽出について記載。
						4.2.2	設計・製造フェーズ 項番1,2,3,4,5:施策として抽出した脅威に対する対策について記載。
	要点11	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		指針11	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	4.2.2	設計・製造フェーズ 項番3:施策として相手との通信に使用するプロトコルについて記載。
	要点12	安全安心を実現する設計の検証・評価を行う		指針12	安全安心を実現する設計の検証・評価を行う	4.2.3	評価フェーズ 1:施策として設計に問題がないかを確認する評価について記載。
2.4 構築・接続	要点13	機器等がどのような状態かを把握し、記録する機能を設ける	保守	指針13	自身がどのような状態かを把握し、記録する機能を設ける	4.2.2	設計・製造フェーズ 項番2:自装置の状態を記録するためのロギング機能について記載。
	要点14	機能及び用途に応じて適切にネットワーク接続する					
	要点15	初期設定に留意する					
	要点16	認証機能を導入する					
2.5 運用保守	要点17	出荷・リリース後も安全安心な状態を維持する		指針14	時間が経っても安全安心を維持する機能を設ける	4.2.2	設計・製造フェーズ 項番2:施策としてプログラムアップデート機能実装について記載。
						4.2.4	運用フェーズ 項番1:施策としてプログラムのアップデートに関して記載。
			運用	指針15	出荷後もIoTリスクを把握し、情報発信する	4.2.4	運用フェーズ 項番1,2:施策として最新の脆弱性への対応と、組織の対応内容について記載。
	要点18	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		指針16	出荷後の関係事業者に守ってもらいたいことをy伝える	4.2.4	運用フェーズ 項番1,2:施策として出荷後組織がとるべき体制について記載。
						4.2.5	廃棄フェーズ 項番1:施策として廃棄時のリスク表示について記載。
	要点19	つながることによるリスクを一般利用者に知ってもらう		指針17	つながることによるリスクを一般利用者に知ってもらう	4.2.2	設計・製造フェーズ 項番2:施策として取扱説明書へのリスク、脅威の表示について記載。
	要点20	IoTシステム・サービスにおける関係者の役割を認識する					
	要点21	脆弱な機器を把握し、適切に注意喚起を行う					

7-1. 総括

市場では次々と新たな攻撃手法が考案され、IoT によりつながる世界は日々脅威にさらされている。最近では 2016 年 9 月に確認された Mirai あるいは Bashlight というマルウェアの存在は、史上最大規模の DDoS 攻撃の脅威により、大きな話題となった。同時にこの脅威により、インターネット上には工場出荷時のままの（あるいは推測が容易な）ID/Password で放置されている IoT デバイスが無数にあり、対策が急務であることを知らしめる結果となった（一説には Bashlight は 100 万台もの IoT デバイスをスレーブ化しているとも言われている）。

今回作成したガイドラインは、こうした状況の中で、高価な評価検証ツールや特別な知識がなくとも、必要なセキュリティ評価検証を実施できることを前提に作成している。分野によっては評価検証の充分条件に満たない可能性もあり、また現時点で確認されている脅威及び評価検証手法に基づいて記載しているため、今後の技術革新によっては新たな脅威が生じ、今後も情報を更新する必要性があると考えている。次版を更新する機会があれば、IoT のより広い分野において利用可能なように、最新情報の収集を行い、更新を行っていきたい。

Appendix1　セキュリティ検証ツール一覧

表 A1-1.　主要な静的脆弱性検証ツール一覧

NO	ツール名	提供元	URL	特徴	日本語	有償/無償	検査対象									
							インジェクション	認証とセッション管理の不備	クロスサイトスクリプティング	オブジェクト直接参照	セキュリティ設定のミス	機密データの露出	機能レベルアクセス制御の欠落	クロスサイトリクエストフォージェリ	既知の脆弱性を持つコンポーネントの利用	未検証のリダイレクトとフォワード
1	iCodeChecker	IPA	https://www.ipa.go.jp/security/vuln/iCodeChecker/index.html	C言語のみ対象とした無償の脆弱性検査ツール ※注意：2017年6月13日、クロスサイト・スクリプティングの脆弱性のため、提供・サポートを停止 VMイメージ、パッケージ形式、ソースコード形式が利用可能	○	無償	△	×	×	△	×	×	△	×	×	△
2	RIPS	Johannes Dahse	http://rips-scanner.sourceforge.net/	ウェブアプリケーションとして動作、入力されたPHPソースコードを解析が可能	×	無償	○	×	○	△	×	△	△	×	×	×
3	LAPSE+	OWASP	https://www.owasp.org/index.php/OWASP_LAPSE_Project	Eclipseプラグインで動作、JAVAのソースコードに対して脆弱性解析が可能	○	無償	○	×	○	△	×	△	△	×	×	×
4	Fortify SCA	Hewlett Packard	http://www8.hp.com/jp/ja/software-solutions/static-code-analysis-sast/	多くの開発環境、言語、プラットフォーム、およびフレームワークをサポートし幅広い脆弱性検査が可能	○	有償	○	○	○	○	○	○	○	○	△	○
5	CxSAST	Checkmarx	https://www.checkmarx.com/technology/static-code-analysis-sca/	OWASPトップ10、SANS 25、PCI DSS、HIPAA、MISRA、マイターCWE、FISMA、BSIMMの多くの脆弱性解析に対応	×	有償	○	○	○	○	○	○	○	○	○	○
6	Coverity	Synopsys	http://www.coverity.com/html/ja/security/	誤検知率が非常に低く、様々な脆弱性解析が可能	○	有償	○	○	○	○	○	○	○	○	×	○
7	Klocwork	Rogue Wave	http://www.roguewave.jp/products-services/klocwork	静的コード解析のみではなく、統合開発環境 やチーム開発における様々なワークフローにシームレスに統合し、開発中のソースをリアルタイムに解析が可能	○	有償	○	○	○	○	○	○	×	×	×	○
8	Jtest	parasoft	https://www.parasoft.com/product/jtest/	テストケースを自動生成し、アプリケーションの単体テストを自動実行 セキュリティのみではなく一般的なバグとなるコードも検知が可能	○	有償	○	×	○	○	×	×	×	×	×	○
9	C++test	parasoft	https://www.parasoft.com/product/cpptest/	上記JtestのC/C++版	○	有償	○	×	○	○	×	×	×	×	×	○
10	dotTEST	parasoft	https://www.parasoft.com/product/dottest/	上記Jtestの.net版	○	有償	○	×	○	○	×	×	×	×	×	○

表 A1-2.　主要な脆弱性スキャンツール一覧　　※印は CCDS の検証ツールにパッケージされているもの

NO	ツール名	提供元	URL	特徴	日本語	有償/無償	検査対象									
							インジェクション	認証とセッション管理の不備	クロスサイトスクリプティング	オブジェクト直接参照	セキュリティ設定のミス	機密データの露出	機能レベルアクセス制御の欠落	クロスサイトリクエストフォージェリ	既知の脆弱性を持つコンポーネントの利用	未検証のリダイレクトとフォワード
1	Owasp ZAP※	OwaspProject ※CCDS-HNW評価ツール	https://www.owasp.org/index.php/OWASP_Zed_Attack_Proxy_Project	WEBアプリケーションの脆弱性を診断するためのオープンソースのテストツール	○	無償	○	○	○	○	○	○	○	○	○	○
2	w3af※	w3af.org ※CCDS-汎用脆弱性検証ツール	http://w3af.org/	Webアプリケーションの攻撃および監査フレームワーク、SQLインジェクションのチェックやクロスサイトスクリプティング（XSS）、ローカル/リモートファイルインクルージョンなどを含めた130以上のプラグインで実行可能	×	無償	○	○	○	○	○	○	○	○	○	○
3	OpenVAS※	Greenbone Networks GmbH ※CCDS-HNW評価ツール	http://www.openvas.org/	Nessusから派生したオープンソースの脆弱性スキャナ	○	無償	○	○	×	△	○	×	×	×	○	×
4	Nessus	Tenalble network security	http://www.tenable.com/products/nessus-vulnerability-scanner	ネットワーク経由でターゲットの脆弱性を収集、レポートすることができる世界で最も使用されている脆弱性スキャナ	○	有償	○	○	×	△	○	×	×	×	○	×
5	Nexpose	Rapid7	https://www.rapid7.com/jp/products/nexpose/	37,000種類以上の脆弱性定義と100,500以上のスキャンパターンやPCI DSSのセキュリティ基準を順守しているか確認できる脆弱性スキャナ	○	有償	○	○	×	△	○	×	×	×	○	×
6	WebInspect	HP	http://www8.hp.com/jp/ja/software-solutions/webinspect-dynamic-analysis-dast/	業界最多クラスの脆弱性情報を保有するWebアプリケーション脆弱性診断ツール	○	有償	○	○	○	○	○	○	○	○	○	○
7	Vulnerability Explorer	Ubsecure	http://www.ubsecure.jp/vex/vex.html	純国産のWebアプリケーション脆弱性テストツール	○	有償	○	○	○	○	○	○	○	○	○	○
8	AppScan	IBM	http://www-03.ibm.com/software/products/ja/appscan	Webアプリケーションに潜む脆弱性を検査するツール	○	有償	○	○	○	○	○	○	○	○	○	○

表 A1-3.　主要なペネトレーションツール一覧　　※印は CCDS の検証ツールにパッケージされているもの

NO	ツール名	提供元	URL	特徴	日本語	有償/無償
1	LOIC※ （Low Orbit Ion Canon）	オープンソース ※CCDS-汎用脆弱性検証ツール	http://sourceforge.net/projects/loic/	負荷試験ツール。IRCを使ったDDoS攻撃のシミュレーションが可能。	×	無償
2	aircrack-ng※	オープンソース ※CCDS-汎用脆弱性検証ツール	http://www.aircrack-ng.org/	WiFiのパスワード解析ツールで、WEP and WPA PSK (WPA 1 and 2)に対応。	×	無償
3	Medusa※ （Medusa Parallel Network Login Auditor）	オープンソース ※CCDS-汎用脆弱性検証ツール	http://foofus.net/goons/jmk/medusa/medusa.html	パスワード解析ツールで、HTTP,POP,SSH,RDP等多くのプロトコルに対応。	×	無償
4	Hydra※ （THC Hydra）	オープンソース ※CCDS-汎用脆弱性検証ツール	http://www.thc.org/thc-hydra/	パスワード解析ツールで、HTTP,POP,FTP等多くのプロトコルに対応。	×	無償
5	Paros※ （Paros proxy）	オープンソース ※CCDS-汎用脆弱性検証ツール	http://sourceforge.net/projects/paros/	Proxyを通過した内容を書き換えて、データ送信が可能なツール。	×	無償
6	Ostinate※	オープンソース ※CCDS-HNW評価ツール	http://ostinato.org/	Wiresharkでキャプチャしたパケットを編集し、その編集したパケットを送信できる	×	無償
7	Gatling※	オープンソース ※CCDS-HNW評価ツール	http://gatling.io/	負荷試験ツールで、実施結果をレポート出力可能。	×	無償
8	hydra※	オープンソース ※CCDS-汎用脆弱性検証ツール	https://www.thc.org/thc-hydra/	ftp, ssh, http, imap, pop3などなど、多くのプロトコルをサポートし総当たり法でログオン侵入テストが可能	×	無償
9	Kali Linux	Offensive Security	https://www.kali.org/	様々機能を搭載したペネトレーションテスト向けのLinuxディストリビューション	○	無償
10	sqlmap	オープンソース	http://sqlmap.org/	SQLインジェクションの脆弱性を利用し、データベース・サーバーの引き継ぐのプロセスを自動化するオープンソースの侵入テストツール	×	無償
11	Social Engineer Toolkit	オープンソース	https://www.trustedsec.com/social-engineer-toolkit/	ソーシャルエンジニアリングのために設計されたオープンソースの侵入テストのフレームワーク	×	無償
12	BeEF	オープンソース	http://beefproject.com/	Webブラウザに焦点を当てた侵入テストツール	×	無償
13	Dradis Framework	オープンソース	http://dradisframework.org/	Webアプリケーションとして動作し、他のツールと豊富なプラグインで連携を行い侵入テストが行える	×	無償
14	Metasploit	Rapid7	https://www.rapid7.com/jp/products/metasploit/	豊富なエクスプロイトライブラリを使用してマシンの制御とネットワークの乗っ取り、検出事項を含むレポートの自動生成が行える	○	有償/無償
15	Penetrator	Bluestar Corporation	http://penetrator.blue.co.jp/portable.html	700以上の実際のエクスプロイトを起動して、Windows、Unix，ルータやファイアウオール等の診断が可能	×	有償
16	core impact	Core Security SDI Corporation	https://www.coresecurity.com/core-impact	ネットワーク、Web、およびモバイルアクロスマルチベクトルテスト機能および豊富な脆弱性のエクスプロイトが行える	×	有償

表 A1-4.　主要なファジングツール一覧　　※印は CCDS の検証ツールにパッケージされているもの

NO	ツール名	提供元	URL	特徴	日本語	有償/無償	検査手段		
							ネットワーク	ファイル	プログラム
1	Sulley※	オープンソース ※CCDS-HNW評価ツール	https://github.com/OpenRCE/sulley/tree/master/sulley	ファジングデータを条件に応じて自動生成可能。 別途作成した通信プロトコルのシナリオファイルに挿入し、ファジングが可能。	×	無償	○	×	×
2	Taof	オープンソース	https://sourceforge.net/projects/taof/	ネットワークの上のデータをキャプチャし改変したデータを送信したファジングが可能	×	無償	○	×	×
3	ISIC	オープンソース	http://isic.sourceforge.net/	ネットワーク機器・ソフトウェアに対してのパケットファジングが可能	×	無償	○	×	×
4	american fuzzy lop	オープンソース	http://lcamtuf.coredump.cx/afl/	プログラム内の条件を網羅的にファジングが可能	×	無償	×	×	○
5	radamsa	オープンソース	https://github.com/aoh/radamsa	有効なデータファイルからファズを生成、スクリプト化し自動的に実行が可能	×	無償	○	○	○
6	ProxyFuzz	オープンソース	https://www.secforce.com/media/tools/proxyfuzz.py.txt	TCPおよびUDPプロトコルに対してのファジングが可能	×	無償	○	×	×
7	Basic Fuzzing Framework	Carnegie Mellon University	https://www.cert.org/vulnerability-analysis/tools/bff.cfm?	ファイルを読み込むアプリケーションに対してファジングが可能	×	無償	×	○	×
8	Peach Community Edition v3	Peach Fuzzer	http://www.peachfuzzer.com/resources/peachcommunity/	ファイルを読み込む画像ソフト、TCP/IP などで通信するソフトやウェブアプリケーションなど幅広いソフトウェア製品に対してファジングが可能	×	無償	○	○	○
9	iFuzzMaker	IPA	http://www.ipa.go.jp/security/vuln/iFuzzMaker/	JPEG画像を読み込む機能を持つ製品に対するファジングが可能	○	無償	×	○	×
10	SDL Regex Fuzzer	Microsoft	https://www.microsoft.com/en-us/download/details.aspx?id=20095	正規表現ファジングデータでのDoS攻撃ファジングが可能	×	無償	×	×	○
11	SDL MiniFuzz File Fuzzer	Microsoft	https://www.microsoft.com/en-us/download/details.aspx?id=21769	実行形式のアプリケーションに対してファイルによるファジングが可能	×	無償	×	○	×
12	beSTORM	Beyond Security	http://www.beyondsecurity.com/bestorm.html	任意のネットワーク・ソフトウェアを対象にファジングを行い包括的なセキュリティ分析が可能	×	有償	○	○	○
13	Defensics	CODENOMICON	http://www.codenomicon.com/jp/products/defensics/	100種類以上のプロトコルやファイルフォーマットをサポートしたファズテストプラットフォーム	×	有償	○	○	○
14	FFR Raven	FFRI	http://www.ffri.jp/products/raven/	ネットワーク組み込み機器の脆弱性のファジングが可能	○	有償	○	○	○

Appendix2　　評価検証計画書の実例集

■プロジェクト計画書

プロジェクト名：	WiFi無線アクセスポイント端末のセキュリティ評価検証

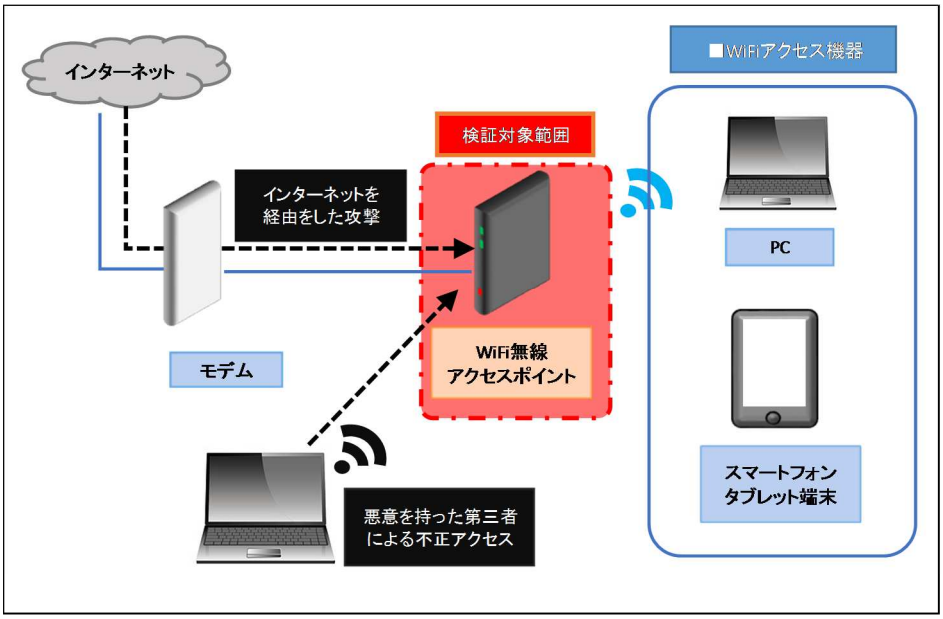
1）評価検証の背景

①対象プロジェクト/評価検証サブプロセス

本プロジェクトはWiFi無線アクセスポイントのセキュリティ評価検証を行うプロジェクトとなる。

■プロジェクト概要
・A社が開発したWiFi無線アクセスポイント端末をテスト対象とする。
・実装する認証方式はWEP、WPA、WPA2－AESの3種となる。
・ユースケースについては、一般的な家庭用ルータにおける使用を前提とする。

②評価検証対象　　※システム構成図のイメージを貼付



③評価検証範囲

■テスト範囲
・家庭用のWiFi無線アクセスポイント端末を対象とし、以下の範囲にでセキュリティ評価検証を実施する。
　－管理者のみがオペレーション可能な管理画面に関するセキュリティ対策の妥当性。
　－Wifi接続用のSSIDやPasswordが、簡易に攻撃できる値に設定されていないかどうか。
　－その他、WAN側からの中間者攻撃による不正アクセスやDOS攻撃などの想定脅威に対する対策の妥当性。
※無線アクセスポイントの管理用サーバや、HAN側に接続されている機器は、評価検証の対象外とする。

■評価検証に必要な情報、ドキュメント
・評価検証要件の策定にあたり、下記のドキュメントは顧客より提供される。
　－無線アクセスポイントの操作マニュアル
　－要求仕様書
　－設計ドキュメント

④前提及び制約条件

※技適やWiFi/Bluetoothの認証マーク等、評価検証を実施する上で、事前にクリアしておくべき基準があれば、記載しておくこと。
※機密情報管理に対する方針や、検証仕様に関するレビューなど顧客と合意しておくべき条件があれば、記載しておくこと。

■実網許可及び、評価検証実施環境について
－対象となるDUTについては、技適マークの認証は完了した状態で貸与を受け、実網接続には問題ない状態であることを確認する。
－誤って、テスト対象機器以外に、不正な信号（エクスプロイトデータやDoS信号等）を送信してしまう事を防ぐため、可能な限り、実網での接続を避け、電波暗室内に試験環境を構築し、評価検証を実施すること。

■機密情報管理について
－顧客から提供を受けた各種設計ドキュメントについては、当社の情報管理規定（I顧客提出済み）に則り、機密保持を徹底すること。
－期間中は、本プロジェクトに関係するスタッフ以外の立ち入りができないよう、クリーンルームにより業務を行う。
－検出されたインシデント情報については、CCDS検証基盤システムを用いて、顧客と情報交換を行う。検証基盤システムからダウンロードしたインシデント情報については、メール添付を含め、社内外への情報送信を禁止するものとする。

■評価検証仕様書の合意について
－評価検証実施内容については、作成した評価検証仕様書の内容を顧客側に説明し、合意の上で実施するものとする。

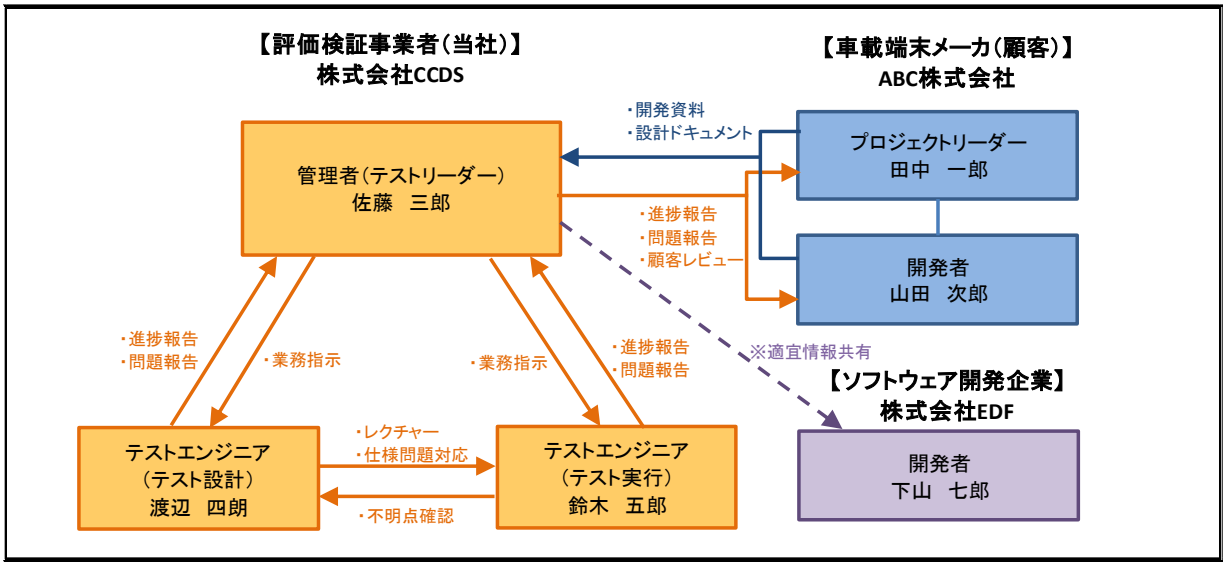
⑤利害関係者

※品質部門や、顧客以外の企業担当者（顧客にとっての発注元）等、評価検証情報を共有すべき関係者については、記載を行うこと

業態	役割名	会社名	氏名	E-Mail	役割内容
IoT機器開発メーカ	プロジェクトリーダー	ABC株式会社	田中　一郎	tanaka@abc.co.jp	開発プロジェクト統括
IoT機器開発メーカ	開発担当者	ABC株式会社	山田　次郎	yamada@abc.co.jp	対象IoT機器の開発担当
IoT機器開発メーカ	品質部門担当者	ABC株式会社	川田　六郎	kawatani@abc.co.jp	対象IoT機器の品質担当
ソフトウェア開発業者	開発担当者	株式会社DEF	下山　七郎	shimoyama@def.co.jp	ソフトウェアの開発担当
評価/評価検証事業者	テストリーダー	株式会社CCDS	佐藤　三郎	sato@ccds.co.jp	評価検証のとりまとめ
評価/評価検証事業者	テストエンジニア	株式会社CCDS	渡辺　四朗	watanabe@ccds.co.jp	評価検証の設計を担当
評価/評価検証事業者	テストエンジニア	株式会社CCDS	鈴木　五郎	suzuki@ccds.co.jp	評価検証の実行を担当

2)評価検証コミュニケーション　　※プロジェクトの体制を貼付

・当該プロジェクトについては、下記の体制にて実施し、コミュニケーションを行うものとする。



3)リスク一覧表

①プロジェクト推進に関するリスク

A)想定されるリスクの抽出

区分	非常に小さい	小さい	普通	大きい	非常に大きい
	1	2	3	4	5
評価検証実行による対象機器への影響	-	-	-	評価検証実行が原因で、仕様動作と異なる挙動が確認された場合	評価検証実行が原因で、メインユースケースの機能に重大な影響が確認された場合
受け入れ時の製品品質（不具合検出等）	メインユースケース以外の機能に軽微な影響あり	メインユースケース以外の機能に影響あり	メインユースケースの機能に軽微影響	メインユースケースの機能に影響あり	メインユースケースの機能に重大な影響あり
DUT接続時の調査、準備	-	-	当初計画と比較し、評価検証ツールをDUTに接続する際の調査、準備に軽微な工数超過が発生する	当初計画と比較し、評価検証ツールをDUTに接続する際の調査、準備に大幅な工数超過が発生する	想定していたツールがDUTと接続できず、工数計画に抜本的な見直しが必要となる
評価検証実行時のスキル不足（調達）	-	評価検証実行にスキル不足により、当初見積もりと比較し、軽微な期間超過が発生する	評価検証実行にスキル不足により、当初見積もりと比較し、大幅な期間超過が発生する	評価検証仕様策定において、不備があり、リカバリに多大な期間を要する	調達を予定していた人員の確保ができず、プロジェクト全体の計画、期間に重大な影響がある
機材・環境	テスト機材・環境の準備/調達が遅延（1日以内）	テスト機材・環境の準備/調達が遅延（2～3日以内）	テスト機材・環境の準備/調達が遅延（4～5日以内）	テスト機材・環境の準備/調達が遅延（1Week以上）	テスト機材・環境の調達が困難

B)リスク値の算出基準

B-1)発生率基準

区分	非常にまれに起こる	まれに起こる	普通	起こる可能性がある	ほぼ確実に起こる
	1	2	3	4	5

B-2)影響度算出基準

区分	非常に小さい	小さい	普通	大きい	非常に大きい
	1	2	3	4	5
コスト	コスト増は軽微	コスト増10%	コスト増10-20%	コスト増20-40%	コスト増40%
タイム	期間延長は軽微	期間延長5%未満	期間延長5-10%	期間延長10-20%	期間延長20%

C)想定されるリスクを踏まえたリスク値の算出及び、リスク対策

項目名	リスク	A)影響度（Ｉ）	②発生確率(P)	③リスク値（R=I×P)	リスク対策
評価検証実行による対象機器への影響	コスト	-	-	-	・ファジングやペネトレーション等を実施する際は、日程含め、顧客への事前合意を得る。 ・評価検証の実施順を考慮し、DUTに影響が想定される項目については、最後に実施する形とする。 ・代替用の試験端末を用意いただく。
	タイム	2	4	8	
受け入れ時の製品品質（不具合検出等）	コスト	-	-	-	事前に顧客より、システムテスト結果を受領予定。
	タイム	2	2	4	
DUT接続時の調査、準備	コスト	3	3	9	・過去の調査結果をもとにトレーニングを実施しておき、準備工程を円滑に進められるよう配慮する。 ・候補ツールを複数選定しておく。
	タイム	-	-	-	
評価検証実行時のリスク不足（調達）	コスト	-	-	-	セキュリティ評価検証において実績のあるスタッフをアサイン可能。人材採用の目途がある。
	タイム	3	2	6	
機材・環境	コスト	-	-	-	調達依頼済み
	タイム	1	1	1	

4)評価検証戦略

①評価検証サブプロセス

本プロジェクトにおける評価検証は、以下のサブプロセスに分けて進めるものとする。
1. 評価検証の方針/仕様（手順書）の策定
 ・システムテストの設計を行うサブプロセスであり、セキュリティ評価検証手順ガイドラインに沿って、
 評価検証仕様書、手順書（結果表）の策定を行う。
2. 評価検証環境の構築
 ・評価検証環境の構築を行うサブプロセスであり。本プロジェクトでは、電波暗室内にネットワーク及び、
 評価検証環境の構築が準備作業として必要となる。
3. 評価検証の実行
 ・策定した仕様書、手順書に沿って、評価検証作業の実行を行う。問題点や不具合を認識した場合には、別途
 インシデントレポートを起票する。

②成果物

・下記の成果物を納品するものとする。
※仕様書/手順書については、実行開始前に顧客レビューを行うものとする。
 －セキュリティ評価検証仕様書/手順書（※）
 －セキュリティ評価検証結果表
 －脅威（セキュリティインシデント）レポート報告書
 －セキュリティ品質報告書

③評価検証設計技法

・セキュリティ評価検証手順ガイドラインに沿って、リスク分析から評価検証手法（ツール）の選定を行う。

④完了基準

・起票したインシデントは全てクローズとなり、評価検証項目の保留、NG項目がゼロとなった時点で評価完了とする。

⑤収集するメトリクス

・本プロジェクトでは、以下のメトリクスを収集する。
 －各サブプロセス毎の工数：今後の見積もり精度の向上のため。
 －評価検証計画に対する予実：今後の進捗管理に活用するため。
 －発生インシデント数及び内容：今後の評価検証使用にフィードバックさせるため。

⑥必要となるデータやドキュメント

・評価検証要件の策定にあたり、下記のドキュメントは顧客より提供される。
 －無線アクセスポイントの操作マニュアル
 －要求仕様書
 －設計ドキュメント

⑦必要となる環境

・本プロジェクトで必要となる環境は、以下となる。
[ハードウェア]
 －評価検証ツール使用時（特にペネトレーションツール利用時）は電波暗室を用いる。
 －試験対象（DUT）となるWiFi無線アクセスポイント端末
 －オンラインシステムにアクセス可能なインターネット環境
 －評価検証作業用PC
[ソフトウェア]
 －評価検証仕様策定時に選定した各種セキュリティ評価検証ツール

⑧評価検証の再実施及び回帰テスト

・起票したインシデントの改修（対応）後、問題の解消を確認し、関連する評価検証項目対して、回帰テストを
実施する。

⑨中断及び、再開基準

・万一、ブロッキングとなる不具合が見つかり、評価検証の継続が困難な場合には、顧客と調整の上、評価検証を中断し、該当不具合の改修が確認された時点で再開するものとする。

⑩「組織的評価検証戦略」からの逸脱事項

・本プロジェクトはセキュリティ評価検証の実施のみを前提としており、単体テスト、結合テスト、システムテスト、ユーザビリティテストは、評価の対象から除外するものとする。

5)評価検証活動の役割分担、要求スキルレベル及び工数見積り

・本プロジェクトの業務内容と要求スキルレベル、想定工数は、以下となる

プロセス	役割	工数(人日)	業務内容・要求スキルレベル
評価検証管理	テストリーダー	45.0	【業務内容】 評価検証の統括、業務指示、顧客への進捗報告、問題報告 【要求スキルレベル】 ・評価検証のマネージメント経験3年以上 ・セキュリティ評価検証の実務経験5件以上
評価検証計画	テストリーダー	5.0	【業務内容】 評価検証計画の策定、計画に対する顧客との調整 【要求スキルレベル】 ・評価検証のマネージメント経験3年以上 ・セキュリティ評価検証の実務経験5件以上
評価検証設計	テストエンジニア	10.0	【業務内容】 セキュリティ評価検証仕様書、手順書の作成 【要求スキルレベル】 ・開発エンジニアとしての経験3年以上 ・セキュリティ評価検証の実務経験1件以上
環境構築	開発担当者	10.0	【業務内容】 電波暗室内のネットワーク、試験環境の構築、試験対象となるIoT機器(DUT)の貸与 【要求スキルレベル】 ー
評価検証実行	テストエンジニア	30.0	【業務内容】 評価検証作業の実行、問題点やインシデント報告レポートの作成 【要求スキルレベル】 ・開発エンジニアとしての経験3年以上 ・セキュリティ評価検証の実務経験1件以上
セキュリティ品質報告	テストリーダー	5.0	【業務内容】 評価検証完了時点でセキュリティ品質報告書を作成、顧客へ報告 【要求スキルレベル】 ・評価検証のマネージメント経験3年以上 ・セキュリティ評価検証の実務経験5件以上

6)人材

①役割、活動、責任

業態	役割名	会社名	氏名	E-Mail	役割内容
車載端末メーカ	プロジェクトリーダー	ABC株式会社	田中　一郎	tanaka@abc.co.jp	開発プロジェクト統括
車載端末メーカ	開発担当者	ABC株式会社	山田　次郎	yamada@abc.co.jp	IoT端末の開発担当
評価検証事業者	テストリーダー	株式会社CCDS	佐藤　三郎	sato@ccds.co.jp	評価検証のとりまとめ
評価検証事業者	テストエンジニア	株式会社CCDS	渡辺　四朗	watanabe@ccds.co.jp	評価検証の設計を担当
評価検証事業者	テストエンジニア	株式会社CCDS	鈴木　五郎	suzuki@ccds.co.jp	評価検証の実行を担当
評価検証事業者	テストエンジニア	株式会社CCDS	※新規雇用を予定		評価検証の実行を担当

②雇用の必要性

・評価検証実行を担当する評価検証エンジニアを1名新規採用にて、雇用する。

【採用する人材のスキル要件】
－開発業務において3年以上の経験があり、設計ドキュメントの読解に問題がないこと
－JAVAによるコーディングの経験が1年以上あり、ソースコードからプログラム内容を理解できること
－単体、結合、システムテストのいずれかを実施した実務経験が5件以上あること

③教育の必要性

・インシデントの妥当性については、顧客側の開発担当者と協議の上、深刻度及び登録内容を調整する。
・評価検証仕様書及び手順書の内容については、設計担当のテストエンジニアよりレクチャーを行う。

7)スケジュール

・本プロジェクトのスケジュールは以下の沿って進めるものとする。

	Week1	Week2	Week3	Week4
マイルストン	▼x/xx：計画レビュー ▼x/xx：設計レビュー		▼x/xx：検証完了 ▼x/xx：セキュリティ品質報告提出	
評価検証計画				
評価検証設計				
環境構築				
評価検証実行				
改修期間				
セキュリティ品質報告				

Appendix3　　評価検証仕様書の実例集

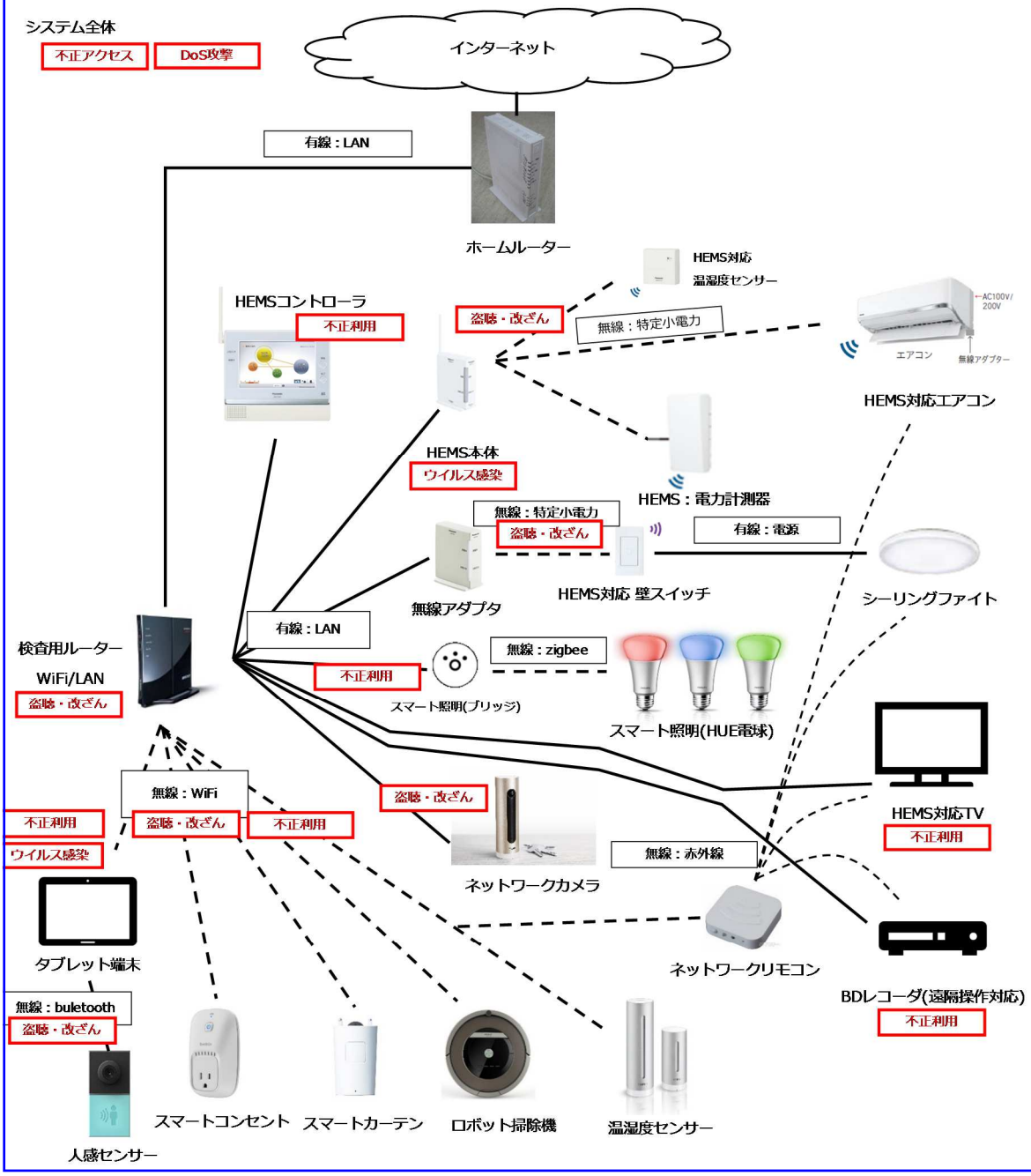
・以下に参考資料として、本事業で実施したスマートホームテストベッドの実環境に対する評価検証仕様書を実例として記載する。

1 目的

本書では、セキュリティ検証を行う対象について分析を行い、利用される状況や扱われる情報を整理し、
それらを逆手に取り悪用されるリスクを検討する。
検討したリスクを回避するために必要な守るべき資産を洗いだす。

2 スマートホームの接続構成と想定脅威

スマートホームのテストベットに設置されている機器の構成図を下記に記載する。
その接続構成から想定される脅威を図に記載する。



3 脅威対策及び検証手法

前項でスマートホームの接続構成を整理し、想定される脅威を検討している。その検討した脅威に対する対策と検証手法についてまとめる。

脅威				対策候補			検証手段	
発生個所		保護すべき資産	脅威名	対策名	他のガイドラインとの関係		検証手法	検証ツール
					OTA	OWASP		
IoT-GW (ホームルータ)	検証用ルータ WiFi/有線LAN	設定情報 セキュリティ情報 ・ログインパスワード ・SSIDキー	不正アクセス	脆弱性対策	OTA5		ネットワーク脆弱性検査	Open VAS
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (通信解析・ブルートフォース攻撃対策)	aircrack-ng Hydra
				FW機能		OWASP3	脆弱性検査	Open VAS
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling
			盗聴・改ざん	通信路暗号化	OTA1		脆弱性検査	Open VAS
HNWにつながる機器	HEMS 本体機器 コントローラ 無線アダプタ TV	設定情報 セキュリティ情報 ・ログインパスワード	不正アクセス	脆弱性対策	OTA5		Webアプリ脆弱性検査	Open VAS
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra
				FW機能		OWASP3	脆弱性検査	Open VAS
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling
			盗聴・改ざん	通信路暗号化	OTA1	OWASP8	ネットワーク脆弱性検査	Open VAS
			ウィルス感染	脆弱性対策	OTA4,OTA5		WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP Open VAS
				ソフトウェア署名	OTA6	OWASP9	ネットワーク脆弱性検査	Open VAS
				セキュア開発	OTA7		設計ドキュメント確認 ソースコード確認	−
	BDレコーダ	設定情報 セキュリティ情報 ・ログインパスワード 機器本体	不正アクセス	脆弱性対策	OTA5		WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP Open VAS
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra
				FW機能		OWASP3	脆弱性検査	Open VAS
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling
			不正利用	ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra
	スマート照明	機器本体	不正アクセス	脆弱性対策	OTA5		WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP Open VAS
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling
			不正利用	ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra
	ネットワークカメラ	映像情報 機器本体	不正アクセス	脆弱性対策	OTA5		WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP Open VAS
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling
			盗聴・改ざん	通信路暗号化	OTA1	OWASP8	脆弱性検査	OWASP ZAP

3 脅威対策及び検証手法

前項でスマートホームの接続構成を整理し、想定される脅威を検討している。その検討した脅威に対する対策と検証手法についてまとめる。

脅威				対策候補			検証手段	
発生個所		保護すべき資産	脅威名	対策名	他のガイドラインとの関係		検証手法	検証ツール
					OTA	OWASP		
IoT-GW (ホームルータ)	検証用ルータ WiFi/有線LAN	設定情報 セキュリティ情報 ・ログインパスワード ・SSIDキー	不正アクセス	脆弱性対策	OTA5		ネットワーク脆弱性検査	Open VAS（CCDS）
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (通信解析・ブルートフォース攻撃対策)	aircrack-ng（CCDS） Hydra（CCDS）
				FW機能		OWASP3	脆弱性検査	Open VAS（CCDS）
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling （CCDS）
			盗聴・改ざん	通信路暗号化	OTA1		脆弱性検査	Open VAS（CCDS）
HNWにつながる機器	HEMS 本体機器 コントローラ 無線アダプタ TV	設定情報 セキュリティ情報 ・ログインパスワード	不正アクセス	脆弱性対策	OTA5		Webアプリ脆弱性検査	Open VAS（CCDS）
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
				FW機能		OWASP3	脆弱性検査	Open VAS（CCDS）
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling （CCDS）
			盗聴・改ざん	通信路暗号化	OTA1	OWASP8	ネットワーク脆弱性検査	Open VAS（CCDS）
			ウィルス感染	脆弱性対策	OTA4,OTA5		WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP（CCDS） Open VAS（CCDS）
				ソフトウェア署名	OTA6	OWASP9	ネットワーク脆弱性検査	Open VAS（CCDS）
				セキュア開発	OTA7		設計ドキュメント確認 ソースコード確認	−
	BDレコーダ	設定情報 セキュリティ情報 ・ログインパスワード 機器本体	不正アクセス	脆弱性対策	OTA5		WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP（CCDS） Open VAS（CCDS）
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
				FW機能		OWASP3	脆弱性検査	Open VAS（CCDS）
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling （CCDS）
			不正利用	ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
	スマート照明	機器本体	不正アクセス	脆弱性対策	OTA5		WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP（CCDS） Open VAS（CCDS）
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling （CCDS）
			不正利用	ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
	ネットワークカメラ	映像情報 機器本体	不正アクセス	脆弱性対策	OTA5		WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP（CCDS） Open VAS（CCDS）
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling （CCDS）
			盗聴・改ざん	通信路暗号化	OTA1	OWASP8	脆弱性検査	Ostinate,Gatling （CCDS）

HNWにつながる機器	ネットワークリモコン	制御情報 機器本体	不正アクセス	脆弱性対策	OTA5		WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP（CCDS） Open VAS（CCDS）
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
				FW機能		OWASP3	脆弱性検査	Open VAS（CCDS）
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling （CCDS）
			不正利用	ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
			盗聴・改ざん	通信路暗号化	OTA1	OWASP8	脆弱性検査	OWASP ZAP（CCDS）
	温湿度センサー	計測情報 機器本体	不正アクセス	脆弱性対策			WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP（CCDS） Open VAS（CCDS）
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling （CCDS）
			不正利用	ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
			盗聴・改ざん	通信路暗号化	OTA1	OWASP8	脆弱性検査	OWASP ZAP（CCDS）
	ロボット掃除機	機器本体	DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling （CCDS）
			不正利用	ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
	スマートカーテン	機器本体	DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling （CCDS）
			不正利用	ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
	スマートコンセント	機器本体	DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling （CCDS）
			不正利用	ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
	タブレット端末	設定情報 セキュリティ情報 ・ログインパスワード	不正アクセス	脆弱性対策	OTA5		WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP（CCDS） Open VAS（CCDS）
				ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
				FW機能		OWASP3	脆弱性検査	Open VAS
			DoS攻撃	DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	Ostinate,Gatling （CCDS）
			不正利用	ユーザ認証	OTA11,OTA12,OTA13,OTA14	OWASP2,OWASP8	ペネトレーション (ブルートフォース攻撃対策)	Hydra（CCDS）
			ウィルス感染	脆弱性対策	OTA4,OTA5		WEBアプリ脆弱性検査 ネットワーク脆弱性検査	OWASP ZAP（CCDS） Open VAS（CCDS）
				ソフトウェア署名	OTA6	OWASP9	ネットワーク脆弱性検査	Open VAS（CCDS）
				セキュア開発	OTA7		設計ドキュメント確認 ソースコード確認	－
	人感センサー	検知情報 機器本体	盗聴・改ざん なりすまし DoS攻撃	通信路暗号化	OTA1	OWASP8	脆弱性検査	※要調査 Bluetooth用ツール
				DoS対策		OWASP3	ペネトレーション (DoS攻撃対策)	※要調査 Bluetooth用ツール

4 検証の目標レベル

今回の検証における検証の目標レベルを定義

対象機器		保護すべき資産	想定脅威	対策レベル					
				Level1		Level2		Level3	
				検証内容	利用ツール	検証内容	利用ツール(例)	検証内容	利用ツール(例)
IoT-GW (ホームルータ)	検証用ルータ WiFi/有線LAN	設定情報 セキュリティ情報 ・ログインパスワード ・SSIDキー	不正アクセス DoS攻撃 盗聴・改ざん	ファジングテスト	Sulley（CCDS）	←Level1で検証		←Level1で検証	
				ネットワーク脆弱性検査	Open VAS（CCDS）	通信の解析	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)	リプレイ攻撃 なりすまし	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)
				ペネトレーションテスト1 (DoS攻撃対策)	Ostinate,Gatling （CCDS）	←Level1で検証		←Level1で検証	
				ペネトレーションテスト1 (ブルートフォース攻撃対策) ＊設定画面ログイン	Hydra（CCDS）	ペネトレーションテスト2 (通信解析、ブルートフォース) ＊WiFi接続情報解読(暗号強度変更)	aircrack-ng（CCDS） Hydra（CCDS）	←Level2で検証	
HNWにつながる 機器	HEMS 本体機器 コントローラ 無線アダプタ TV	設定情報 セキュリティ情報 ・ログインパスワード	不正アクセス DoS攻撃 盗聴・改ざん ウィルス感染	ファジングテスト	Sulley（CCDS）	←Level1で検証		←Level1で検証	
				ネットワーク脆弱性検査	Open VAS（CCDS）	通信の解析	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)	リプレイ攻撃 なりすまし	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)
				Webアプリ脆弱性検査	OWASP ZAP（CCDS）				
				ペネトレーションテスト1 (DoS攻撃対策)	Ostinate,Gatling （CCDS）	←Level1で検証		←Level1で検証	
				ペネトレーションテスト1 (ブルートフォース攻撃対策) ＊設定画面ログイン	Hydra（CCDS）	←Level1で検証		←Level1で検証	
	BDレコーダ	設定情報 セキュリティ情報 ・ログインパスワード 機器本体	不正アクセス DoS攻撃 不正利用	ファジングテスト	Sulley（CCDS）	←Level1で検証		←Level1で検証	
				ネットワーク脆弱性検査	Open VAS（CCDS）	通信の解析	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)	リプレイ攻撃 なりすまし	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)
				Webアプリ脆弱性検査	OWASP ZAP（CCDS）				
				ペネトレーションテスト1 (DoS攻撃対策)	Ostinate,Gatling （CCDS）	←Level1で検証		←Level1で検証	
				ペネトレーションテスト1 (ブルートフォース攻撃対策) ＊設定画面ログイン	Hydra（CCDS）	←Level1で検証		←Level1で検証	
	スマート照明	機器本体	不正アクセス DoS攻撃 不正利用	ファジングテスト	Sulley（CCDS）	←Level1で検証		←Level1で検証	
				ネットワーク脆弱性検査	Open VAS（CCDS）	通信の解析	Wireshark OWASP ZAP（CCDS）	リプレイ攻撃 なりすまし	Wireshark OWASP ZAP（CCDS）
				ペネトレーションテスト1 (DoS攻撃対策)	Ostinate,Gatling （CCDS）	←Level1で検証		←Level1で検証	
	ネットワークカメラ	映像情報 機器本体	不正アクセス DoS攻撃 盗聴	ファジングテスト	Sulley（CCDS）	←Level1で検証		←Level1で検証	
				ネットワーク脆弱性検査	Open VAS（CCDS）	通信の解析	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)	リプレイ攻撃 なりすまし	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)
				ペネトレーションテスト1 (DoS攻撃対策)	Ostinate,Gatling （CCDS）	←Level1で検証		←Level1で検証	

HNWにつながる機器	ネットワークリモコン	制御情報 機器本体	不正アクセス DoS攻撃 不正利用 盗聴・改ざん	ファジングテスト	Sulley（CCDS）	←Level1で検証		←Level1で検証	
				ネットワーク脆弱性検査	Open VAS（CCDS）	通信の解析	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)	リプレイ攻撃 なりすまし	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)
				Webアプリ脆弱性検査	OWASP ZAP（CCDS）				
				ペネトレーションテスト1 (DoS攻撃対策)	Ostinate,Gatling （CCDS）	←Level1で検証		←Level1で検証	
	温湿度センサー	計測情報 機器本体	不正アクセス DoS攻撃 不正利用 盗聴・改ざん	ファジングテスト	Sulley（CCDS）	←Level1で検証		←Level1で検証	
				ネットワーク脆弱性検査	Open VAS（CCDS）	通信の解析	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)	リプレイ攻撃 なりすまし	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)
				Webアプリ脆弱性検査	OWASP ZAP（CCDS）				
				ペネトレーションテスト1 (DoS攻撃対策)	Ostinate,Gatling （CCDS）	←Level1で検証		←Level1で検証	
	ロボット掃除機	機器本体	DoS攻撃 不正利用	ファジングテスト	Sulley（CCDS）	←Level1で検証		←Level1で検証	
				ネットワーク脆弱性検査	Open VAS（CCDS）	通信の解析	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)	リプレイ攻撃 なりすまし	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)
				ペネトレーションテスト1 (DoS攻撃対策)	Ostinate,Gatling （CCDS）	←Level1で検証		←Level1で検証	
	スマートカーテン	機器本体	DoS攻撃 不正利用	ファジングテスト	Sulley（CCDS）	←Level1で検証		←Level1で検証	
				ネットワーク脆弱性検査	Open VAS（CCDS）	通信の解析	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)	リプレイ攻撃 なりすまし	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)
				ペネトレーションテスト1 (DoS攻撃対策)	Ostinate,Gatling （CCDS）	←Level1で検証		←Level1で検証	
	スマートコンセント	機器本体	DoS攻撃 不正利用	ファジングテスト	Sulley（CCDS）	←Level1で検証		←Level1で検証	
				ネットワーク脆弱性検査	Open VAS（CCDS）	通信の解析	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)	リプレイ攻撃 なりすまし	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)
				ペネトレーションテスト1 (DoS攻撃対策)	Ostinate,Gatling （CCDS）	←Level1で検証		←Level1で検証	
	タブレット端末	設定情報 セキュリティ情報 ・ログインパスワード	不正アクセス DoS攻撃 不正利用 ウィルス感染	ファジングテスト	Sulley（CCDS）	←Level1で検証		←Level1で検証	
				ネットワーク脆弱性検査	Open VAS（CCDS）	通信の解析	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)	リプレイ攻撃 なりすまし	Wireshark OWASP ZAP（CCDS） (Zad Attach Proxy)
				Webアプリ脆弱性検査	OWASP ZAP（CCDS）				
				ペネトレーションテスト1 (DoS攻撃対策)	Ostinate,Gatling （CCDS）	←Level1で検証		←Level1で検証	
				ペネトレーションテスト1 (ブルートフォース攻撃対策) ＊設定画面ログイン	Hydra（CCDS）	←Level1で検証		←Level1で検証	
	人感センサー	検知情報 機器本体	盗聴・改ざん なりすまし DoS攻撃	ペネトレーションテスト1 (不正ペアリング対策)	※Bluetooth用ツール	通信の解析	※Buletooth用ツール	リプレイ攻撃 なりすまし	※Bluetooth用ツール
				ペネトレーションテスト1 (DoS攻撃対策)	※Bluetooth用ツール	←Level1で検証		←Level1で検証	

５．DUTのインタフェースと通信プロトコル調査（連携動作の分析）

DUTとなるIoT機器のユースシーン、インタフェースや通信プロトコル、連携動作に関する調査結果を以下にまとめる。

[省エネ]

No	ユースシーン名	トリガー(input)	機器と接続方式	制御(output)	機器と接続方式	連携方法	EventID/キーワード/補足
1	消し忘れ防止	人感センサー	人感センサー：Bluetooth	照明	LED電球：有線LAN	人感センサーアプリとLED電球が連携し照明を制御	
				エアコン(ネットワークリモコン)	ネットワークリモコン：WiFi	人感センサーからIFTTTにEventIDを送付 EventIDをキーにMakerChannelと連携しネットワークリモコンのAPIにrequestを投げる	EventID＝AbsenceInRoom
				コンセント	スマートコンセント：WiFi	人感センサーからIFTTTにEventIDを送付 EventIDをキーにスマートコンセントと連携しコンセントのスイッチをOFFする	EventID＝AbsenceInRoom
2	無駄使い防止(空調)	外気温の温湿度センサー	温湿度センサー：WiFi	エアコン(ネットワークリモコン)	ネットワークリモコン：WiFi	温湿度センサーからIFTTT使ってMakerChannelと連携 MakerChannelからネットワークリモコンのAPIにrequestを投げる	外気温20℃以上になったときエアコンOFF 外気温25℃以下になったときエアコンOFF
3	無駄使い防止(照明)	時間	IFTTTのサーバー	照明	LED電球：有線LAN	決まった時刻にIFTTTからLED電球に対し制御	午前10時
4	省エネ運転(通知)	電力使用量	HEMS：有線LAN	メール	G-Mail	HEMSを分析し電力が基準を超えた場合G-Mailを送付	
	省エネ運転(検知・制御)	メール	Gmail	照明	LED電球：有線LAN	IFTTTがキーワードを含むメールを受けたことを検知しLED電球を制御	キーワード＝[HEMS]AttentionToPowerConsumption
				エアコン(ネットワークリモコン)	ネットワークリモコン：WiFi	IFTTTがキーワードを含むメールを受けたことを検知しMakerChannelと連携してネットワークリモコンのAPIにrequestを投げる	キーワード＝[HEMS]AttentionToPowerConsumption
				コンセント	スマートコンセント：WiFi	IFTTTがキーワードを含むメールを受けたことを検知しスマートコンセントを制御	キーワード＝[HEMS]AttentionToPowerConsumption

[防犯]

No	ユースシーン名	トリガー(input)	機器と接続方式	制御(output)	機器と接続方式	連携方法	EventID/キーワード/補足
1	居るふり(在室確認)	時計	IFTTTのサーバー	人感センサー	人感センサー：Bluetooth	決まった時間にIFTTTから人感センサーに対しEventIDを送付 EventIDをキーに人感センサーが在室を確認 ・在室の場合：制御終了 ・不在の場合：EventIDをIFTTTに送付	居るふり開始 19:00　EventID＝CamouflageGo 居るふり終了 20:00　EventID＝CamouflageStop
	居るふり(不在の場合)	人感センサー	人感センサー：Bluetooth	TV(ネットワークリモコン)	ネットワークリモコン：WiFi	人感センサーからIFTTTにEventIDを送付 EventIDをキーにMakerChannelと連携しネットワークリモコンのAPIにrequestを投げる	開始：EventID＝CamouflageスマートコンセントON 終了：EventID＝CamouflageスマートコンセントOFF
				コンセント	スマートコンセント：WiFi	人感センサーからIFTTTにEventIDを送付 EventIDをキーにスマートコンセントと連携しコンセントのスイッチをON/OFFする	開始：EventID＝CamouflageスマートコンセントON 終了：EventID＝CamouflageスマートコンセントOFF
2	監視カメラ	顔を認識し知らない顔を検知	netatom security：有線LAN	照明	LED電球：有線LAN	IFTTTからLED電球に対し制御	LED電球の色を変える(CSS #800000)

[快適]

No	ユースシーン名	トリガー(input)	機器と接続方式	制御(output)	機器と接続方式	連携方法	EventID/キーワード/補足
1	自動点灯	人感センサー	人感センサー：Bluetooth	照明	LED電球：有線LAN	人感センサーアプリとLED電球が連携し照明を制御	
2	熱中症防止(在室確認)	室内の温湿度センサー	温湿度センサー：WiFi	人感センサー	人感センサー：Bluetooth	室内の温度が30℃以上なった時IFTTTから人感センサーに対しEventIDを送付 EventIDをキーに人感センサーが在室を確認 ・在室の場合：EventIDをIFTTTに送付 ・不在の場合：制御終了	EventID＝CriticalTemperature
	熱中症防止(在室の場合)	人感センサー	人感センサー：Bluetooth	エアコン(ネットワークリモコン)	ネットワークリモコン：WiFi	人感センサーからIFTTTにEventIDを送付 EventIDをキーにMakerChannelと連携しネットワークリモコンのAPIにrequestを投げる	EventID＝CoolingStart
3	定期換気	室内の温湿度センサー	温湿度センサー：WiFi	エアコン(ネットワークリモコン)	ネットワークリモコン：WiFi	温湿度センサーからIFTTT使ってMakerChannelと連携 MakerChannelからネットワークリモコンのAPIにrequestを投げる	室内の湿度が80%を超えたとき　エアコンON 室内の湿度が60%を下回ったとき　エアコンOFF

[防災]

No	ユースシーン名	トリガー(input)	機器と接続方式	制御(output)	機器と接続方式	連携方法	EventID/キーワード/補足
1	天気予報①	Yahoo天気	Yahoo提供サービス	照明	LED電球：有線LAN	MyThingsからLED電球に対し制御	最高気温が35～40℃の範囲の場合　Dining1の電球を黄色
	天気予報②	Yahoo天気	Yahoo提供サービス	照明	LED電球：有線LAN	MyThingsからLED電球に対し制御	朝7時の天気予報が雨の場合　Dining2の電球を青色
2	防災通知①(照明)	Yahoo防災	Yahoo提供サービス	照明	LED電球：有線LAN	MyThingsからLED電球に対し制御	防災速報で、地震情報がでたら　沖縄県：震度5弱以上 電球すべての色を変える(CSS　#FF00FF)
	防災通知①(その他)	Yahoo防災	Yahoo提供サービス	メール	Gmail	MyThingsからGmailにメールを送付	
		メール	Gmail	TV(ネットワークリモコン)	ネットワークリモコン：WiFi	IFTTTがキーワードを含むメールを受けたことを検知しMakerChannelと連携してネットワークリモコンのAPIにrequestを投げる	キーワード＝EarthquakeInfomation
	防災通知②	Yahoo防災	Yahoo提供サービス	照明	LED電球：有線LAN	MyThingsからLED電球に対し制御	防災速報で、津波警報・注意方法が発令されたら　沖縄県 電球の色をランダムに光る

' 6．検証ツール調査結果

※CCDS(一般社団法人 重要生活機器連携セキュリティ協議会)で保有している検証基盤システムとそのほかのセキュリティ検証ツールについて整理し、検証での使用方針を検討する

■CCDSツール一覧

CCDSツール	ツール名	機能概要	利用方法	対象脅威
HNW評価ツール（検証基盤システム）	Gatling	HTTPリクエスト負荷	空いているポートに対し攻撃し、機器の動作や他への影響を確認	DoS攻撃
	OpenVAS	ネットワーク脆弱性確認	接続されている全機器に対し調査を実施	脆弱性検査
	Ostinato	IPパケット生成	キャプチャしたパケットを編集し送信	なりすまし
	OWASP ZAP	Webアプリ脆弱性確認	接続されている全機器に対し調査を実施	検査
	Sulley	ファジング	ファジング攻撃	脆弱性検査
オープンソース脆弱性検証ツール	LOIC	ネットワーク負荷テストツール	空いているポートに対し攻撃し、機器の動作や他への影響を確認	DoS攻撃
	SET-Metasploit	ネットワーク負荷テストツール	空いているポートに対し攻撃し、機器の動作や他への影響を確認	DoS攻撃
	W3af	SQLインジェクション・XSS	サーバーやデータベースに対し、インジェクション攻撃を行い、不正に情報を取得する	情報漏洩
	Paros	プロキシー	Proxyを通過した通信内容を書換えて攻撃可能	盗聴
	hydora	パスワードクラック	認証画面を持つ機器に対し、ID/パスワードを解読する	不正アクセス
	medusa	パスワードクラック	認証画面を持つ機器に対し、ID/パスワードを解読する	不正アクセス
	aicack-ng	WiFiハック	WiFiルーターに設定されている暗号(WEP・WPAなど)を解読	不正アクセス

■各システムの概要

検証基盤システム

検証基盤で検証手順書、結果表を作成、管理することが出来る。

検証手順書は、検証基盤と連携しているツールを組合わせて作成することが出来る。

検証手順書を作成すると同時に検証シナリオを組み立てることで、その次の検証実行が自動化できる

検証実施した結果、問題が発見された内容については脅威レポートを作成。作成した脅威レポートは検証基盤内で管理できるため検証手順と紐づけられる

脅威レポートからセキュリテイ評価レポートを発行できる

※セキュリティ評価を一貫して対応が可能

オープンソース脆弱性検証ツール

各ツールが仮想空間上で起動、加えてターゲットも仮想空間に起動でき、PC内部でセキュリティ検証を実践できる

導入されたツールを使って、実際に外部の機器に対して攻撃が可能

※実際に攻撃に使用するより、セキュリティ検証のシミュレーションできることが特徴的

■ツールの選定・活用方法

※今回のスマートホームの環境で使用しないツールをグレーアウト

CCDSツール	ツール名	機能概要	ツールの活用方法	対象脅威
HNW評価ツール（検証基盤システム）	Gatling	HTTPリクエスト負荷	空いているポートに対し攻撃し、機器の動作や他への影響を確認	DoS攻撃
	OpenVAS	ネットワーク脆弱性確認	接続されている全機器に対し調査を実施	脆弱性検査
	Ostinato	IPパケット生成	キャプチャしたパケットを編集し送信	なりすまし
	OWASP ZAP	Webアプリ脆弱性確認	接続されている全機器に対し調査を実施	検査
	Sulley	ファジング	ファジング攻撃	脆弱性検査
オープンソース脆弱性検証ツール	LOIC	ネットワーク負荷テストツール		
	SET-Metasploit	ネットワーク負荷テストツール		
	W3af	SQLインジェクション・XSS		
	Paros	プロキシー	Proxyを通過した通信内容を書換えて攻撃可能	盗聴
	hydora	パスワードクラック	認証画面を持つ機器に対し、ID/パスワードを解読する	不正アクセス
	medusa	パスワードクラック	認証画面を持つ機器に対し、ID/パスワードを解読する	不正アクセス
	aricack-ng	WiFiハック	WiFiルーターに設定されている暗号(WEP・WPAなど)を解読	不正アクセス

[方針]

基本的な検証は検証基盤システムを活用。

検証手順書→検証結果→脅威レポート→セキュリティ検証レポートの一連の流れを実践

検証基盤システムにない、パスワードクラック(hydora)とWiFiハック(aricack-ng)はオープンソース脆弱性検証ツールを利用

６．検証ツール調査結果

※CCDS(一般社団法人 重要生活機器連携セキュリティ協議会)で保有している検証基盤システムとそのほかのセキュリティ検証ツールについて整理し、検証での使用方針を検討する

■CCDSツール一覧

CCDSツール	利用オープンソースツール	機能概要	利用方法	対象脅威
HNW評価ツール（検証基盤システム）	Gatling	HTTPリクエスト負荷	空いているポートに対し攻撃し、機器の動作や他への影響を確認	DoS攻撃
	OpenVAS	ネットワーク脆弱性確認	接続されている全機器に対し調査を実施	脆弱性検査
	Ostinato	IPパケット生成	キャプチャしたパケットを編集し送信	なりすまし
	OWASP ZAP	Webアプリ脆弱性確認	接続されている全機器に対し調査を実施	検査
	Sulley	ファジング	ファジング攻撃	脆弱性検査
汎用脆弱性検証ツール	LOIC	ネットワーク負荷テストツール	空いているポートに対し攻撃し、機器の動作や他への影響を確認	DoS攻撃
	SET-Metasploit	ネットワーク負荷テストツール	空いているポートに対し攻撃し、機器の動作や他への影響を確認	DoS攻撃
	W3af	SQLインジェクション・XSS	サーバーやデータベースに対し、インジェクション攻撃を行い、不正に情報を取得する	情報漏洩
	Paros	プロキシー	Proxyを通過した通信内容を書換えて攻撃可能	盗聴
	hydora	パスワードクラック	認証画面を持つ機器に対し、ID/パスワードを解読する	不正アクセス
	medusa	パスワードクラック	認証画面を持つ機器に対し、ID/パスワードを解読する	不正アクセス
	aicack-ng	WiFiハック	WiFiルーターに設定されている暗号(WEP・WPAなど)を解読	不正アクセス

■各システムの概要

検証基盤システム

検証基盤で検証手順書、結果表を作成、管理することが出来る。
検証手順書は、検証基盤と連携しているツールを組合わせて作成することが出来る。
検証手順書を作成すると同時に検証シナリオを組み立てることで、その次の検証実行が自動化できる
検証実施した結果、問題が発見された内容については脅威レポートを作成。作成した脅威レポートは検証基盤内で管理できるため検証手順と紐づけられる
脅威レポートからセキュリティ評価レポートを発行できる
※セキュリティ評価を一貫して対応が可能

オープンソース脆弱性検証ツール

各ツールが仮想空間上で起動、加えてターゲットも仮想空間に起動でき、PC内部でセキュリティ検証を実践できる
導入されたツールを使って、実際に外部の機器に対して攻撃が可能
※実際に攻撃に使用するより、セキュリティ検証のシミュレーションできることが特徴的

■ツールの選定・活用方法

※今回のスマートホームの環境で使用しないツールをグレーアウト

CCDSツール	利用オープンソースツール	機能概要	ツールの活用方法	対象脅威
HNW評価ツール（検証基盤システム）	Gatling	HTTPリクエスト負荷	空いているポートに対し攻撃し、機器の動作や他への影響を確認	DoS攻撃
	OpenVAS	ネットワーク脆弱性確認	接続されている全機器に対し調査を実施	脆弱性検査
	Ostinato	IPパケット生成	キャプチャしたパケットを編集し送信	なりすまし
	OWASP ZAP	Webアプリ脆弱性確認	接続されている全機器に対し調査を実施	検査
	Sulley	ファジング	ファジング攻撃	脆弱性検査
汎用脆弱性検証ツール	LOIC	ネットワーク負荷テストツール		
	SET-Metasploit	ネットワーク負荷テストツール		
	W3af	SQLインジェクション・XSS		
	Paros	プロキシー	Proxyを通過した通信内容を書換えて攻撃可能	盗聴
	hydora	パスワードクラック	認証画面を持つ機器に対し、ID/パスワードを解読する	不正アクセス
	medusa	パスワードクラック	認証画面を持つ機器に対し、ID/パスワードを解読する	不正アクセス
	aricack-ng	WiFiハック	WiFiルーターに設定されている暗号(WEP・WPAなど)を解読	不正アクセス

[方針]

基本的な検証は検証基盤システムを活用。
検証手順書→検証結果→脅威レポート→セキュリティ検証レポートの一連の流れを実践
検証基盤システムにない、パスワードクラック(hydora)とWiFiハック(aricack-ng)はオープンソース脆弱性検証ツールを利用

７．テストケース及び評価検証手順書の記載実例（一部を抜粋）

手順書ID	23
タイトル	(総務省)IoTサービス創出支援事業 CCDS-HNW社ツール検証2
説明	CCDS-HNW社ツールを使用してのセキュリティ検証を実施する
実施期間	2017/02/01 ～ 2017/02/10

行番号	項目ID	大項目	中項目	小項目	前提条件	実行手順	確認項目
1	230	不正アクセス Dos攻撃	CCDS-HNW社ツール検証	機器：スマートコンセント 2回目	CCDS-HNW社のデフォルトの設定状態での検証 プロトコル　UDP：53 サービス：domain IPアドレス：192.168.0.7 ■OSSツール(CCDS-HNW社) ・OpenVAS(ネットワーク脆弱性) ・Ostinato(IPパケット生成)	ダッシュボード画面より実行ボタンを押下し検証を開始する	ダッシュボードより結果を確認しログを確認する ※検証結果でABORTEDになった場合はCCDS-HNW社ツールよりログを確認する
2	231	不正アクセス Dos攻撃	CCDS-HNW社ツール検証	機器：LED電球 OWASP,Ostinato	CCDS-HNW社のデフォルトの設定状態での検証 プロトコル　TCP：80 サービス：http IPアドレス：192.168.0.4 ■OSSツール(CCDS-HNW社) ・OWASPZAP(Webアプリ脆弱性) ・Ostinato(IPパケット生成)	ダッシュボード画面より実行ボタンを押下し検証を開始する	ダッシュボードより結果を確認しログを確認する ※検証結果でABORTEDになった場合はCCDS-HNW社ツールよりログを確認する
3	232	不正アクセス Dos攻撃	CCDS-HNW社ツール検証	機器：ネットワークリモコン　OWASP,Ostinato	CCDS-HNW社のデフォルトの設定状態での検証 プロトコル　TCP：80 サービス：http IPアドレス：192.168.0.13 ■OSSツール(CCDS-HNW社) ・OWASPZAP(Webアプリ脆弱性) ・Ostinato(IPパケット生成)	ダッシュボード画面より実行ボタンを押下し検証を開始する	ダッシュボードより結果を確認しログを確認する ※検証結果でABORTEDになった場合はCCDS-HNW社ツールよりログを確認する
4	233	不正アクセス Dos攻撃	CCDS-HNW社ツール検証	機器：HEMS(無線アダプター)　OWASP,Ostinato	CCDS-HNW社のデフォルトの設定状態での検証 プロトコル　TCP：80 サービス：http IPアドレス：192.168.0.10 ■OSSツール(CCDS-HNW社) ・OWASPZAP(Webアプリ脆弱性) ・Ostinato(IPパケット生成)	ダッシュボード画面より実行ボタンを押下し検証を開始する	ダッシュボードより結果を確認しログを確認する ※検証結果でABORTEDになった場合はCCDS-HNW社ツールよりログを確認する
5	234	不正アクセス Dos攻撃	CCDS-HNW社ツール検証	機器：HEMS(本体) OWASP,Ostinato	CCDS-HNW社のデフォルトの設定状態での検証 プロトコル　TCP：80 サービス：http IPアドレス：192.168.0.216 ■OSSツール(CCDS-HNW社) ・OWASPZAP(Webアプリ脆弱性) ・Ostinato(IPパケット生成)	ダッシュボード画面より実行ボタンを押下し検証を開始する	ダッシュボードより結果を確認しログを確認する ※検証結果でABORTEDになった場合はCCDS-HNW社ツールよりログを確認する
6	235	不正アクセス Dos攻撃	CCDS-HNW社ツール検証	機器：スマートコンセント 3回目 ※TCPのポートで検証を行う	CCDS-HNW社のデフォルトの設定状態での検証 プロトコル　TCP：49153 サービス：upnp IPアドレス：192.168.0.7 ■OSSツール(CCDS-HNW社) ・Sulley(ファジング攻撃) ・OpenVAS(ネットワーク脆弱性) ・Ostinato(IPパケット生成) ・Gatling(HTTPリクエスト負荷)	ダッシュボード画面より実行ボタンを押下し検証を開始する	ダッシュボードより結果を確認しログを確認する ※検証結果でABORTEDになった場合はCCDS-HNW社ツールよりログを確認する

Appendix4　　リスク評価手法の紹介

参考資料として、主要なリスク評価手法の詳細を以下に記載する。

1. CVSSv3[16]

1-1. 概要

CVSS は Common Vulnerability Scoring System の略称。コンピュータ・セキュリティの非営利団体「FIRST」（Forum of Incident Response and Security Teams）が推進する、脆弱性評価システムのこと。脆弱性ごとにパラメータを設定して値を求めることで、深刻度の判断材料を得ることができる。現在、最新のバージョンとして version3 が公開されている。

1-2. リスクファクタ

1)基本評価基準（Base Metrics）

：「機密性」、「完全性」、「可用性」に対する影響から評価

2)現状評価基準（Temporal Metrics）

：攻撃コードの出現有無や対策情報が利用可能といった基準で評価

3)環境評価基準（Environment Metrics）

：二次的被害の大きさや、対象製品の使用状況といった基準で評価

1-3. リスク計算式

1)基本評価基準（Base Metrics）

①影響度

調整前影響度 = 1 - (1 - C)×(1 - I)×(1 - A)	…式(1)
影響度(スコープ変更なし)= 6.42×調整前影響度	…式(2)
影響度(スコープ変更あり)= 7.52×(調整前影響度 - 0.029) - 3.25×(調整前影響度 - 0.02)^{15}	…式(3)

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

②攻撃容易性

攻撃容易性 = 8.22×AV×AC×PR×UI	…式(4)

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

③基本値

・影響度がゼロ以下の場合

基本値 = 0	…式(5)

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

・影響度がゼロよりも大きい場合

スコープ変更なし 基本値 = RoundUp1(min [(影響度＋攻撃容易性), 10]) （小数点第 1 位切り上げ）	…式(6)
スコープ変更あり 基本値 = RoundUp1(min [(1.08×(影響度＋攻撃容易性)), 10]) （小数点第 1 位切り上げ）	…式(7)

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

基本評価基準				
評価項目	評価結果と値　※（）内の値はスコープ変更ありの場合			
攻撃元区分（AV）	ネットワーク（N） 0.85	隣接（A） 0.62	ローカル（L） 0.55	物理（P） 0.20
攻撃条件の複雑さ（AC）	低（L） 0.77	高（H） 0.44	－	－

必要な特権レベル（PR）	不要（N） 0.85	低（L） 0.62（0.68）※	高（H） 0.27（0.50）※	－
ユーザ関与レベル（UI）	不要（N） 0.85	要（R） 0.62	－	－
スコープ（S）	変更なし（U）	変更あり（C）	－	－
機密性への影響（C）	高（H） 0.56	低（L） 0.22	なし（N） 0	－
完全性への影響（I）	高（H） 0.56	低（L） 0.22	なし（N） 0	－
可用性への影響（A）	高（H） 0.56	低（L） 0.22	なし（N） 0	－

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

2)現状評価基準（Temporal Metrics）

①現状値

現状値 = RoundUp1(基本値×E×RL×RC) （小数点第 1 位切り上げ）	…式(8)

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

現状評価基準					
評価項目	評価結果と値				
攻撃される可能性（E）	未評価（X） 1.00	容易に攻撃可能（H） 1.00	攻撃可能（F） 0.97	実証可能（P） 0.94	未実証（U） 0.91
利用可能な対策のレベル（RL）	未評価（X） 1.00	なし（U） 1.00	非公式（W） 0.97	暫定（T） 0.96	正式（O） 0.95
脆弱性情報の信頼性（RC）	未評価（X） 1.00	確認済（C） 1.00	未確証（R） 0.96	未確認（U） 0.92	－

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

3)環境評価基準（Environment Metrics）

①緩和策後影響度

緩和策後調整前影響度 = min [(1 -(1 - MC×CR)×(1 - MI×IR)×(1 - MA×AR)), 0.915]	…式(9)
緩和策後影響度(スコープ変更なし)= 6.42×緩和策後調整前影響度	…式(10)
緩和策後影響度(スコープ変更あり)= 7.52×(緩和策後調整前影響度 - 0.029) - 3.25×(緩和策後調整前影響度 - 0.02)[15]	…式(11)

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

②緩和策後攻撃容易性

緩和策後攻撃容易性 = 8.22×MAV×MAC×MPR×MUI	…式(12)

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

③環境値

・緩和策後影響度がゼロ以下の場合

環境値 = 0	…式(13)

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

・緩和策後影響度がゼロよりも大きい場合

スコープ変更なし 緩和策後基本値 = RoundUp1(min [(緩和策後影響度＋緩和策後攻撃容易性), 10]) 環境値 = RoundUp1(緩和策後基本値×E×RL×RC) （小数点第 1 位切り上げ）	…式(14)
スコープ変更あり 緩和策後基本値 = RoundUp1(min [(1.08×(緩和策後影響度＋緩和策後攻撃容易性)), 10]) 環境値 = RoundUp1(緩和策後基本値×E×RL×RC)　…式(15) （小数点第 1 位切り上げ）	…式(15)

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

環境評価基準				
評価項目	評価結果と値			
対象システムのセキュリティ要求度 （CR、IR、AR）	未評価（X） 1.0	高(H) 1.5	中（M） 1.0	低（L） 0.5
・緩和策後の攻撃元区分(MAV) ・緩和策後の攻撃条件の複雑さ(MAC) ・緩和策後の必要な特権レベル(MPR) ・緩和策後のユーザ関与レベル(MUI) ・緩和策後のスコープ(MS) ・緩和策後の機密性への影響(MC) ・緩和策後の完全性への影響(MI) ・緩和策後の可用性への影響(MA)	※評価結果に対応する値は、基本評価基準と同一となる。			

（出典：IPA「共通脆弱性評価システム CVSS v3 概説」[16]）

2. NIST SP800-30 [17]

2-1. 概要

NIST SP800-30 は米港連邦政府の情報システムのリスクアセスメント実施方法を提供するために、NIST SP800-39 を詳説したドキュメント。

2-2. リスクファクタ

1)THREAT SOURCES（脅威源）

2)THREAT EVEVTS（脅威内容）

3)VULNERABILITIES AND PREDIPONSING CONDITIONS（脆弱性と発生条件）

4)LIKELIHOOD OCCURRENCE（発生の可能性）

5)IMPACT（影響度）

2-3. リスク計算式

リスクファクタは例示されているが、各ファクタを結合する計算アルゴリズムは各組織においてリスクモデルを定義し、それを含むとしている。

（Organization-specific risk models include algorithms(e.g., formulas, tables, rules) for combining risk factors）

2-4. 備考

各リスクファクタを利用した計算式は定義されておらず、組織毎に設定する必要がある。

3. GMITS（ISO/IEC TR 13335）[18]

3-1. 概要

GMITS（ISO/IEC TR 13335）[18]は IT セキュリティマネジメントのガイドライン。現在存在する各種リスクマネジメント手法のベースとなっている規格。

3-2. リスクファクタ

1)Asset（資産価値）

2)Threat（脅威）

3)Vulnerability（脆弱性）

3-3. リスク計算式

リスクファクタは例示されているが、各ファクタを結合する計算アルゴリズムは記載されていない。

3-4. 備考

各リスクファクタの重み付け、リスクファクタを利用した計算式は定義されておらず、組織毎に設定する必要あり。

4. ETSI TS102 165-1[19]

4-1. 概要

ETSI TS102 165-1 は European Telecommunications Standards Institute によって策定された詳細リスク評価アプローチ手法となる。

4-2. リスクファクタ

表 A2-1. ETSI TS102 165-1 のリスクファクタ

1)Likelihood（攻撃の可能性）	2)Impact（影響度）
1-1)Time（攻撃に要する時間）	2-1)Asset Impact（資産への影響）
1-2)Expertise(攻撃者のスキル)	2-2)Attack Intensity（攻撃の強度）
1-3)Knowledge(システム知識)	
1-4)Opportunity（攻撃の機会）	
1-5)Equipment（設備）	

（出典： ETSI TS102 165-1[19]）

4-3. リスク計算式

Risk　＝　Likelihood　×　Impact

※Likelihood と Impact は、それぞれ以下 1)～2)の算定プロセスによって、値を計算する。

表 A2-2　リスク算定の基準

Value	Risk	Explanation

1, 2	Minor	No essential assets are concerned, or the attack is unlikely. Threats causing minor risks have no primary need for counter measures.
3, 4	Major	Threats on relevant assets are likely to occur although their impact is unlikely to be fatal. Major risks should be handled seriously and should be minimized by the appropriate use of countermeasures.
6 ,9	Critical	The primary interests of the providers and/or subscribers are threatened and the effort required from a potential attacker's to implement the threat(s) is not high. Critical risks should be minimized with highest priority.
Note: Because risk is calculated as the product of likelihood and impact the values 5, 7 and 8 cannot occur.		

（出典： ETSI TS102 165-1[19]）

1)Likelihood（攻撃の可能性）の計算

Likelihood ＝ Time ＋ Expertise ＋Knowledge ＋Opportunity

※合計値を表 A2-4 及び、表 A2-5 に当てはめて、最終的な Likelihood の値を算出する。

表 A2-3.　Likelihood のリスク評価基準

Factor	Range	Value
Time(1 point per week) （攻撃に要する時間）	≦1day	0
	≦1week	1
	≦1month	4
	≦3months	13
	≦6months	26
	> 6months	See note 1
Expertise（攻撃者のスキル）	Laymen	0
	Proficient	2
	Expert	5
Knowledge（知識）	Public	0

	Restricted	1
	Sensitive	4
	Critical	10
Opportunity（攻撃の機会）	Unnecessary/unlimited access	0
	Easy	1
	Moderate	4
	Difficult	12
	None	See note 2
Equipment（機器）	Standard	0
	Specialized	3
	Bespoke	7
Note1：Attack potential is beyond high Note2：Attack path is not exploitable		

（出典： ETSI TS102 165-1[19]）

表 A2-4.　リスク評価の結果と脆弱性レベルとの対応

Range of values	Resistant to attacker with attack potential of :
0 to 2	No rating
3 to 6	Basic
7 to 14	Moderate
15 to 26	High
> 26	Beyond high

（出典： ETSI TS102 165-1[19]）

表 A2-5. 脆弱性レベルと攻撃が発生する可能性との対応

Vulnerability rating	Likelihood	value
Beyond high	Unlikely	1
High		
Moderate	Possible	2
Basic	Likely	3
No rating		

Note：Motivation is not considered explicitly in the vulnerability rating.

（出典： ETSI TS102 165-1[19]）

2)Impact（影響度）の計算

Result Impact　＝　Asset Impact　＋　Attack Intensity

※合計値が 3 以上の場合も、上限は 3 となる。

表 A2-6.　2-1)Asset Impact（資産への影響）の評価基準

Impact	Explanation	Value
Low	The concerned party is not harmed very strongly; the possible damage is low.	1
Medium	The threat addresses the interests of providers/subscribers and cannot be neglected.	2
High	A basis of business is threatened and severe damage might occur in this context.	3

（出典： ETSI TS102 165-1[19]）

表 A2-7.　2-2) Attack Intensity（攻撃の強度）の評価基準

Attack intensity	value
Single instance of attack	0
Moderate level of multiple instances	1
Heavy level of multiple instances	2

（出典： ETSI TS102 165-1[19]）

4-4. 備考

各リスクファクタへの重み付けが同一ではないため、Time ファクタの見積を間違えると結果に与える影響が大きい。

5. 情報セキュリティマネジメントシステム(ISMS) ISO/IEC27001

5-1. 概要

情報セキュリティマネジメントシステム(ISMS) ISO/IEC27001 は、情報資産のセキュリティを管理するための枠組みを策定し、実施するための規格である。

5-2. リスクファクタ

1)資産の価値
2)脅威
3)脆弱性

5-3. リスク計算式

リスク値　＝　資産の価値　×　脅威　×　脆弱性

※計算式は JPDEC（日本情報経済社会推進協会）による例示であり、規格自体には計算式は示されていない。

5-4. 備考

各リスクファクタへの重み付けは同一（1～3）

6. OCTAVE Allegro[20]

6-1. 概要

OCTAVE（Operationally Critical Threat, Asset, and Vulnerability Evaluation）Allegro[20]はカーネギーメロン大学（米国）により 1999 年に発行された OCTAVE をベースに作られた脆弱性評価フレームワーク。

6-2. リスクファクタ

1)Impact Area：

1.評判（Reputation）、2.Financial（金銭）、3.Productivity（生産性）、

4.Safety&Health（安全、健康）、5.Fines/Legal（罰）

※Ranking については、1~5 の優先順位(1～5)値。

2)Impact Value：Impact Area に対する影響度を High、Mid、Low の 3 段階に分けたもの。

6-3. リスク計算式

Risk＝　Ranking　×　Impact Value　の合計値

表 A2-8.　各リスクファクタの評価入力例

Impact Area	Ranking	Impact Value	Score
Reputation（評判）	4	Moderate(2)	8
Financial（金銭）	5	Low(1)	5
Productivity（生産性）	3	Low(1)	3
Safety and Health（安全、健康）	1	Low(1)	1
Fines/Legal（罰）	2	High(3)	6
		Total	**23**

（出典：OCTAVE Allegro[20]）

6-4. 備考

他の規格等と異なり、リスクファクタで脆弱性を考慮していない。

7. The OWASP Risk Rating Methodology [21]

7-1. 概要

The OWASP Risk Rating Methodology は OWASP（Open Web Application Security Project）によって開発された脆弱性評価の手法となる。

7-2. リスクファクタ

①Threat Agent（脅威の要因）

②Vulnerability（脆弱性の要因）

③Technical Impact（テクニカルインパクト）

④Business Impact（ビジネスへの影響度）

①Threat Agent（脅威の要因）	③Technical Impact（テクニカルインパクト）
①-1：Skill Level（技術水準）	③-1：Loss of confidentiality（機密性の喪失）
①-2：Motive（動機）	③-2：Loss of integrity（完全性の喪失）
①-3：Opportunity（機会）	③-3：Loss of availability（可用性の喪失）
①-4：Size（影響範囲）	③-4：Loss of accountability（説明責任の喪失）

②Vulnerability（脆弱性の要因）	④Business Impact（ビジネスへの影響度）
②-1：Ease of discovery（発見のしやすさ）	④-1：Financial damage（資産損失）
②-2：Ease of exploit（悪用のしやすさ）	④-2：Reputation damage（ブランド失墜）
②-3：Awareness（既知の脆弱性かどうか）	④-3：Non compliance（法例違反）
②-4：Intrusion detection（侵入検知）	④-4：Privacy violation（プライバシー侵害）

（出典：The OWASP Risk Rating Methodology[21]より邦訳）

7-3. リスク計算式

Risk Severity ＝　((①＋②) /2) ×((③＋④) /2)

1)リスク評価基準

発生確率と影響レベルの算出基準	
0～＜3	Low（低）
3～＜6	Medium（中）
6～9	High（高）

（出典：The OWASP Risk Rating Methodology[21]より邦訳）

2)発生確率と影響レベルの計算式

発生確率（攻撃の可能性）							
脅威の要因				脆弱性の要因			
技術水準	動機	機会	影響範囲	発見のしやすさ	悪用のしやすさ	既知の脆弱性か	侵入検知
X1	X2	X3	X4	X5	X6	X7	X8
全体としての発生確率＝X1～X8 の平均値							

影響レベル							
テクニカルインパクト				ビジネスへの影響			
機密性の喪失	完全性の喪失	可用性の喪失	説明責任の喪失	資産損失	ブランド失墜	法律違反	プライバシー侵害
Y1	Y2	Y3	Y4	Y5	Y6	Y7	Y8

総合的なテクニカルインパクト ＝Y1～Y4 の平均値	総合的なビジネスへの影響 ＝Y5～Y8 の平均値
全体として影響レベル＝Y1～Y8 の平均値	

（出典：The OWASP Risk Rating Methodology [21]より邦訳）

3)全体的なリスクの重大性基準

全体的なリスクの重大性				
影響レベル	high（高）	Medium（中）	High（高）	Critical （クリティカル）
	Medium（中）	Low（低）	Medium（中）	High（高）
	Low（低）	Note（注意）	Low（低）	Medium（中）
		Low（低）	Medium（中）	high（高）
	発生確率（攻撃の可能性）			

（出典：The OWASP Risk Rating Methodology[21]より邦訳）

7-4. 備考

・リスクファクタが多いので、どれか一つの要素に対するリスクを排除したとしてもトタルのリスクには大きな影響が出ない（複数の要素のリスク排除が必要）

・各リスクファクタにウェイト(優先度)の概念がない。

8. FAIR[22]

8-1. 概要

FAIR（Factor Analysis of Information Risk）[22]は Risk Management Insight LLC によって開発されたリスク評価方法。

8-2. リスクファクタ

1)Loss Event Frequency（LEF）：損失発生頻度（TEF、Vuln）

1-1)Threat Event Frequency（TEF）：発生頻度

1-2)Threat Capability（Tcap）：脅威難易度

1-3)Control Strength（CS）：保護強度

1-4)Vulnerability（Vuln）：脆弱性（Tcap、CS）

2)Probable Loss Magnitude（PLM）：金銭的な影響度

8-3. リスク算出

RISK						
PLM	Severe	H	H	C	C	C
	High	M	H	H	C	C
	Significant	M	M	H	H	C
	Moderate	L	M	M	H	H
	Low	L	L	M	M	M
	Very Low	L	L	M	M	M
		VL	L	M	H	VH
LEF						

（出典：Risk Management Insight LLC　FAIR[22]）

8-4. 備考

LEF は４つのファクタにより決まるが、最終的なリスクは LEF と PLM との組み合わせによって決定される。仮に LEF が小さかったとしても金額による影響（PLM）が大きければリスクが高いことになる。（PLM の値が結果に対して影響度が大きい）

9. CCDS 改良方式[4]

9-1. 概要

CCDS によって考案され、「CCDS 製品分野別セキュリティガイドライン 車載器編 Ver.1.01」[4]において公開されている。特徴としては既存のリスク評価手法と比較し、より簡易に分析が可能であり、またリスクファクタに「攻撃者のモチベーション」が組み込まれ、影響度の基準として「人命リスク」を想定した基準を定義している。

9-2. リスクファクタ

1)難易度：S~A の 4 段階で攻撃の難易度を評価する

2)影響度：「軽微」～「壊滅的」までの 4 段階で攻撃による影響度を評価する

3)攻撃者のモチベーション：小～大までの 3 段階で攻撃者のモチベーションを評価する。

9-3. リスク計算式

リスク値　＝　（難易度　＋　影響度）　×　攻撃者のモチベーション

リスク値	基準
Low	8 未満
Middle	8 以上 12 未満
High	12 以上 17 未満
Must	17 以上

（出典：CCDS「CCDS 製品分野別セキュリティガイドライン 車載器編 Ver.1.01」[4]）

1)難易度の判定基準

評価項目	ランク	判定基準	値
難易度	S	複数の条件（認証、特別な権限など）が必要。かつ、ローカルからのみ接続（攻撃）が可能。	1
	A	単一の条件（認証、特別な権限など）が必要。かつ、ローカルからのみ接続（攻撃）が可能。	3
	B	一つ以上の条件（認証、特別な権限など）が必要。もしくは、ローカルからのみ接続（攻撃）が可能。	5
	C	攻撃するための条件が不要。かつ、無線ネットワークからの接続（攻撃）が可能。	10

（出典：CCDS「CCDS 製品分野別セキュリティガイドライン 車載器編 Ver.1.01」[4]）

2)影響度の評価基準

評価項目	ランク	判定基準	値
影響度	軽微	攻撃を受けてもユーザに影響がない、もしくは軽微な表示異常しか発生	1

		しない。かつ、漏えいする情報も個人を特定できるような情報は漏洩しない。	
	中程度	攻撃を受けた場合に、ユーザに不利益をもたらす。 もしくは、漏えいした情報から個人が特定される。	3
	重大	攻撃を受けた場合に、ユーザに不利益をもたらし、二次的被害も発生。 もしくは、漏えいした情報から複数の個人が特定される。	5
	壊滅的	攻撃を受けた場合に、人命に関わるような被害や二次的被害が発生する。	10

（出典：CCDS「CCDS 製品分野別セキュリティガイドライン 車載器編 Ver.1.01」[4]）

3)攻撃者のモチベーションの評価基準

評価項目	ランク	判定基準	値
攻撃者のモチベーション	小	偶発的に発生し攻撃者には何の意図もない。	1
	中	実験や気晴らし、自己顕示などの目的を持つ。	1.25
	大	金銭的な利益を得たり、安全保障に影響を与えるなどの具体的な強い目的を持つ。	1.5

（出典：CCDS「CCDS 製品分野別セキュリティガイドライン 車載器編 Ver.1.01」[4]）

9-4. 備考

「CCDS 製品分野別セキュリティガイドライン 車載器編 Ver.1.01」においては、車載分野における他のリスク評価手法との結果比較も掲載されている。

７．引用・参考文献

[1] 一般社団法人 重要生活機器連携セキュリティ協議会(2015)「一般社団法人 重要生活機器連携セキュリティ協議会の概要」,[online] https://www.ccds.or.jp/public/document/other/CCDS_Info_v1.6.pdf (11)

[2] 総務省 IoT 推進コンソーシアム(2016)「IoT セキュリティガイドライン」,[online] http://www.meti.go.jp/press/2016/07/20160705002/20160705002-1.pdf (36)

[3] 独立行政法人 情報処理推進機構(2016)「つながる世界の開発指針」,[online] http://www.ipa.go.jp/files/000051411.pdf (65)

[4] 一般社団法人 重要生活機器連携セキュリティ協議会(2016)「CCDS 製品分野別セキュリティガイドライン-概要説明資料 車載器編 Ver.1.01」,
[online]https://www.ccds.or.jp/public/document/other/guidelines/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_%E8%BB%8A%E8%BC%89%E5%99%A8%E7%B7%A8_Ver.1.01.pdf

[5] 一般社団法人 重要生活機器連携セキュリティ協議会(2016)「CCDS 製品分野別セキュリティガイドライン-概要説明資料 IoT-GW 編 Ver.1.01」,
[online]https://www.ccds.or.jp/public/document/other/guidelines/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_IoT-GW%E7%B7%A8_Ver.1.01.pdf

[6] 一般社団法人 重要生活機器連携セキュリティ協議会(2016)「CCDS 製品分野別セキュリティガイドライン-概要説明資料 ATM 編 Ver.1.0」,
[online]https://www.ccds.or.jp/public/document/other/guidelines/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_%E9%87%91%E8%9E%8D%E7%AB%AF%E6%9C%AB(ATM)%E7%B7%A8_Ver.1.0.pdf

[7] 一般社団法人 重要生活機器連携セキュリティ協議会(2016)「CCDS 製品分野別セキュリティガイドライン-概要説明資料 POS 編 Ver.1.0」,

[online]https://www.ccds.or.jp/public/document/other/guidelines/CCDS%E8%A3%BD%E5%93%81%E5%88%86%E9%87%8E%E5%88%A5%E3%82%BB%E3%82%AD%E3%83%A5%E3%83%AA%E3%83%86%E3%82%A3%E3%82%AC%E3%82%A4%E3%83%89%E3%83%A9%E3%82%A4%E3%83%B3_%E3%82%AA%E3%83%BC%E3%83%97%E3%83%B3POS%E7%B7%A8_Ver.1.0.pdf

[8] ISO/IEC 25010:2011: *"Systems and software engineering -- Systems and software Quality Requirements and Evaluation (SQuaRE) - System and software quality models."*

[9] ISO/IEC/IEEE29119: *"Software and system engineering - Software Testing -."*

[10] NIST SP800-115: *"Technical Guide to Information Security Testing and Assessment - Recommendations of the National Institute of Standards Technology."*

[11] Online Trust Alliance(2016): *"OTA IoT Trust Framework Update July12, 2016"*

[12] Open Web Application Security Project(2014) *"Internet of Things Top Ten"* ,[online] https://www.owasp.org/images/7/71/Internet_of_Things_Top_Ten_2014-OWASP.pdf

[13] 独立行政法人 情報処理推進機構(2016) 「IoT 開発におけるセキュリティ設計の手引き」,[online] https://www.ipa.go.jp/files/000052459.pdf

[14] 独立行政法人 情報処理推進機構(2013)「ファジング実践資料（テストデータ編）」,[online] https://www.ipa.go.jp/files/000035160.pdf

[15] ESBR:独立行政法人 情報処理推進機構(2013) 「組込みソフトウェア開発における品質向上の勧め[バグ管理/手法編]」,[online] http://www.ipa.go.jp/files/000027629.pdf

[16] 独立行政法人 情報処理推進機構(2015)「共通脆弱性評価システム CVSS v3 概説」,[online] https://www.ipa.go.jp/security/vuln/CVSSv3.html

[17] NIST SP800-30: *"Guide for Conducting Risk Assessments - INFORMATION SECURITY -."*

[18] ISO/IEC TR 13335-3 (GMITS part3): *"Information technology - Guidelines for the management of IT Security - Part 3: Techniques for the management of IT Security."*

[19] ETSI TS 102 165-1: "*Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis,*" V4.2.3 (2011-03).

[20] [Caralli 2007] Caralli, Richard; Stevens, James; Young, Lisa; Wilson, William. *"Introducing OCTAVE Allegro:Improving the Information Security Risk Assessment Process."* CMU/SEI-2007-TR-012. Carnegie Mellon University, Software Engineering Institute, May 2007.

[21] Open Web Application Security Project "*The OWASP Risk Rating Methodology*",[online] https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[22] Risk Management Insight "*An Introduction to Factor Analysis of Information Risk(FAIR),*"[online] ftp://mail.im.tku.edu.tw/Prof_Liang/IRM/10%20An%20Introduction%20to%20Factor%20Analysis%20of%20Information%20Risk.pdf

本書は、一般社団法人 重要生活機器連携セキュリティ協議会(CCDS)において作成しました。

編著者（敬称略）

委　員	三上　清一	一般社団法人 重要生活機器連携セキュリティ協議会　車載 SWG 主査 株式会社 JVC ケンウッド
	渡邉　充	一般社団法人 重要生活機器連携セキュリティ協議会　IoT-GW SWG 主査 株式会社日立製作所
	緒方　日佐男	一般社団法人 重要生活機器連携セキュリティ協議会　IoT-GW SWG 主査 日立オムロンターミナルソリューションズ株式会社
	矢是　泰士	一般社団法人 重要生活機器連携セキュリティ協議会　IoT-GW SWG 主査 オムロンソーシアルソリューションズ株式会社
事務局	田久保　順	一般社団法人 重要生活機器連携セキュリティ協議会
作成支援	合同会社ゼロワン研究所	