平成 29 年 2 月 28 日

平成 27 年度補正予算 IoT サービス創出支援事業　成果報告書

代表団体名	（同）ゼロワン研究所
共同実施団体名	（株）ブロードバンドタワー、（株）プラスナレッジ、（株）マストトップ
実証事業名	スマートホームを想定した連携 IoT 機器のセキュリティ検証用テストベッドの構築
実証地域	研究開発：東京都品川区上大崎 セキュリティ検証事業の一部実証：沖縄県宜野湾市大山
対象分野	家庭
事業概要	組込み機器向け検証基盤システムと連携したスマートホームのテストベッド環境を構築し、日常生活で使用する情報家電（IoT 機器）におけるセキュリティ上の安全性を検証する検証事業の実証を行う。

目次

１．IoT サービスの創出・展開に当たって克服すべき具体的な課題

1-1 技術的課題

IoT サービスでは様々な生活機器に ICT（情報通信技術）が組み込まれ、あらゆる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、そして新たなサービスが創出しつつある。一方、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。例えば、米国ではスーパーマーケットなどの 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。このような事例は、これまで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。特に 2020 年の東京オリンピックに向けて、急速に普及が加速すると思われるスマートホーム化の流れは、連携する生活機器のセキュリティ対策が急務であると考える。一般社団法人重要生活機器連携セキュリティ協議会(以降、CCDS)は、スマートホームにおける想定される脅威について、図 1-1 のように示している。

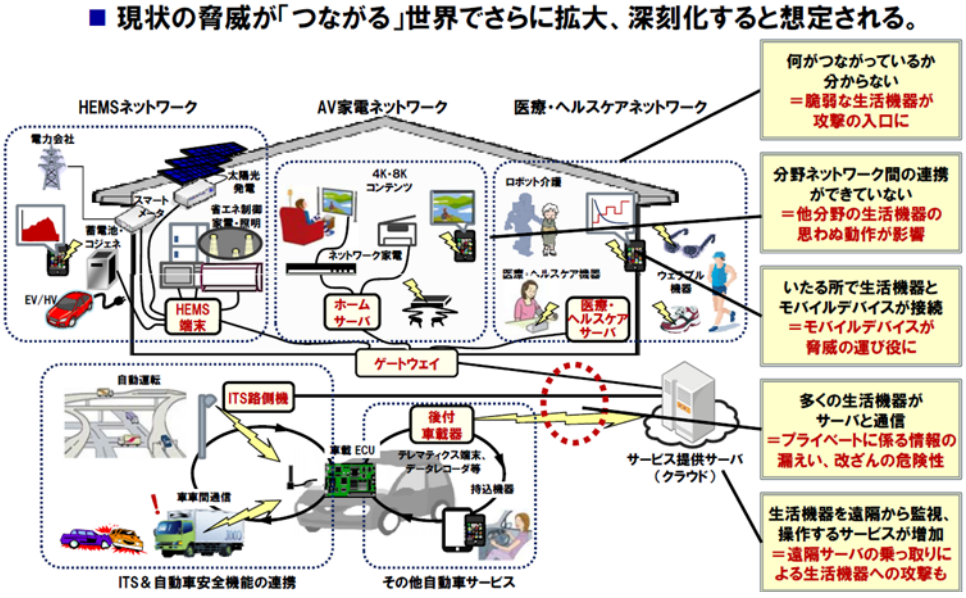


図 1-1　スマートホームの機器連携によって想定される脅威事例（出典 CCDS）

これらの IoT 生活機器は、単体ではメーカーが個別に検証環境を構築し製品の安心・安全に問題がないことを検証して提供されていると思われるが、多種多様な IoT 機器やサービスの連携が容易にできる状況では、メーカーが想定している範囲を超えた使い方や、連携動作が可能となり、想定外の動作や新たな脆弱性が生じる可能性がある。

1-2 制度的課題

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、不十分な状況にある。評価・検証を含めて、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「IEC62443 汎用制御システムのセキュリティ」のみである。IoT 機器（組込み機器）を含む多くの産業では、設計及び実装工程に関する部分を ISO/IEC15408(Common Criteria)で定義しているものの、厳密な対応には形式手法を用いた数学的検証が必要であり非常に導入のハードル（コスト）が高い。

また、生活機器を含む IoT に関する各種ガイドラインが公表されつつあるが、評価・検証という側面では、具体的な手法にまで踏み込んだ定義がされておらず、何をどこまで対応すべきか明確な基準が存在しないのが実情であり、具体的なセキュリティ対策が困難な状況にある。（図 1-2 参照）

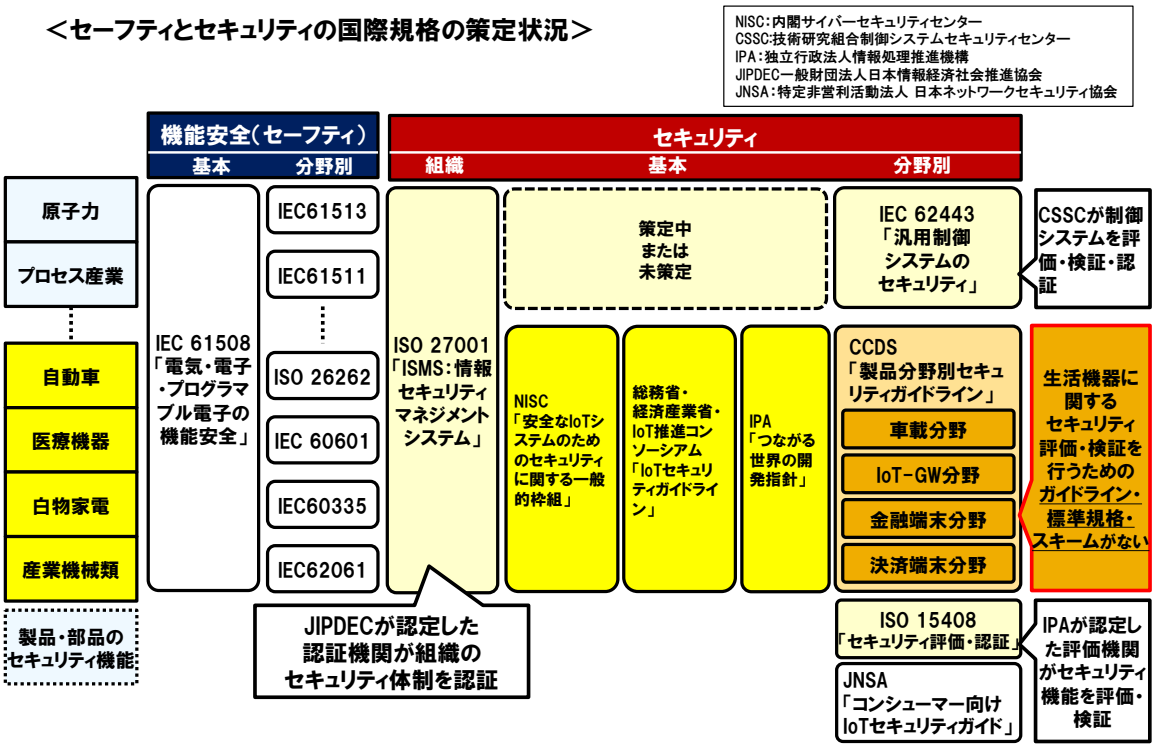


図 1-2　国内におけるセーフティとセキュリティの国際規格の策定状況
（CCDS 資料をもとに現状に即して再編集した）

1-3 法的課題

組み込まれたソフトウェアを含む製品一般については製造物責任法、また、電気製品については電気用品安全法の適用を受けるが、いずれも製品単体の機能・動作についての規制であり、1-1 技術的課題で述べたことと同様にメーカーが想定していない連携動作や悪意の外部者による操作などの脅威に対する評価・検証については規定されていない。

1-4 運用上の課題

実際に連携する生活機器を想定した場合、検証を行うための環境が整備されていない点も大きな課題である。各個別の生活機器については、IoT 機器開発メーカーが個別にエミュレータ

や検証ツール等の環境を構築できるが、実際のスマートホームで想定される様々な機種が連携する環境は、業種横断的な対応が必要となり、個別企業での対応が難しく、コスト面からも障壁となっているのが現状である。

実際に IoT 機器（組込み機器）において、セキュリティ対策を推進するためには、まず脅威分析とリスク分析が必要であり、リスクを明確化するためのインシデントデータを過去の事例や、製品の検証を通じて収集・分析する事が急務である。また、分析結果を受けて、実際に開発工程や検証内容にフィードバックを行うなど PDCA サイクルを実現するためには、IoT 機器開発メーカー、検証事業者が一体となってチームを構成できるビジネススキームが必要となる。

以上をまとめると、スマートホームにおける IoT 機器(組込み機器)が抱えている課題は以下のとおりといえる。

課題 1)連携する生活機器を想定したスマートホームのテストベッドが存在しない。

課題 2)設計、開発、評価・検証までを統合されたプロセスとして実施できるスキームが存在しない。

課題 3)スマートホームの評価・検証において、明確な基準やガイドラインが定まっていない。

２．IoT サービスの創出・展開に当たって克服すべき具体的な課題の解決に資するリファレンス（参照）モデル

１．で示した 3 つの課題に対して下記の目標を設定し、スマートホームを対象とした実証作業を通じて構築されるリファレンスモデルの検討を行った。

課題 1)連携する生活機器を想定したスマートホームのテストベッドが存在しない。
⇒目標 1)スマートホームを想定した情報家電間で連携するテストベッドを構築する。

- 1-1)ホームゲートウェイ及び IoT 機器をシミュレーションできる環境を、クラウドサーバ上でモデル化する。
- 1-2)モデル化したホームゲートウェイ及び IoT 機器に対して、脆弱性の検証を実行できる環境を構築する。
- 1-3)目標 2 の実機による実証において抽出した脆弱性をシミュレーション環境に反映しモデルを修正する。

課題 2)設計、開発、評価・検証までを統合されたプロセスとして実施できるスキームが存在しない。
⇒目標 2)サンプル IoT 機器を対象としたセキュリティ検証サービスの実証。

- 2-1)ホームゲートウェイ、IoT 機器（実機）に対し、CCDS が開発した検証ツールを用い実際の検証サービスを想定した第三者検証サービスを実証する。設計・開発において想定されたリスク項目に対し、検証要件を策定し、実機を用いた検証を実施。検証完了後、検証結果を次回の設計・開発へフィードバック可能なスキームを策定する。

課題 3)スマートホームの評価・検証において、明確な基準やガイドラインが定まっていない。
⇒目標 3)第三者セキュリティ評価・検証のプロセスをガイドラインとして定義する。

- 3-1)今回の事業構築を通じて得られた知見を、IoT 推進コンソーシアム セキュリティ WG の策定内容を加味した上で、上記目標 2 の結果を踏まえ、セキュリティ評価・検証プロセスのガイドライン（検証実行手順）を策定する。

各目標により本実証事業で構築したリファレンスモデルを図 2-1 に示す。

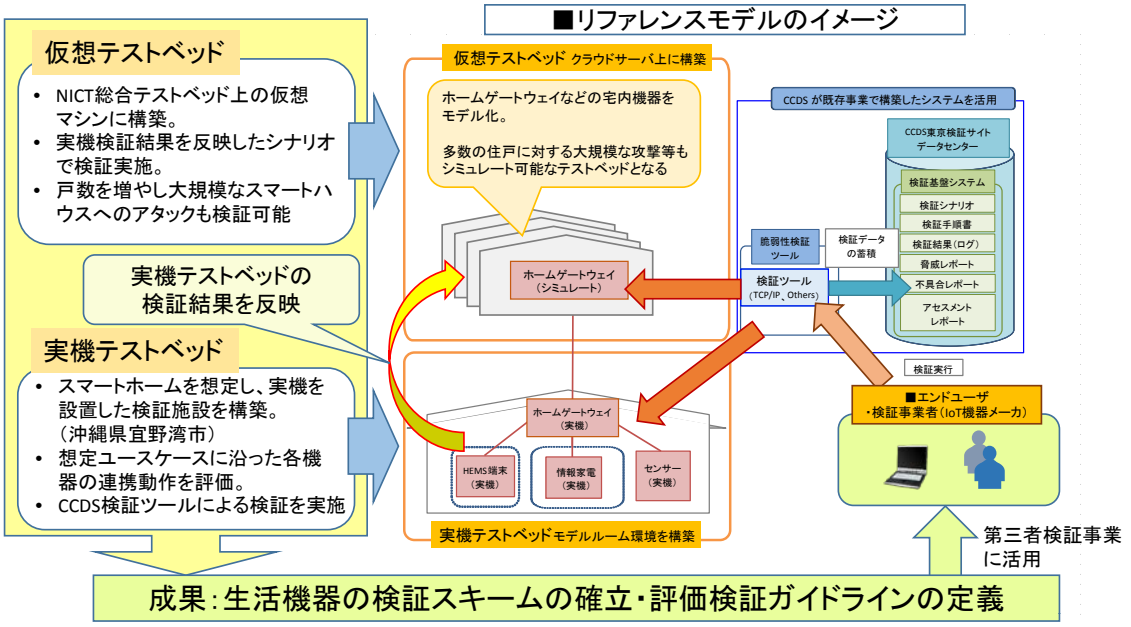


図 2-1　リファレンスモデル

構築した仮想・実機テストベッドにより、実際の検証スキームの手順が明確になり、第三者検証サービスを実施する上で必要な項目を網羅したガイドライン案を作成することを目標とした。また、CCDS が開発している検証基盤システムを使用することにより、試験データの蓄積ができるので、検証によって使用したシナリオや結果などのデータを事業者間で共有することも可能となり、検証精度を上げることも期待できる。

実証事業においては上記目標に従い課題解決のためのリファレンスモデルを構築した。

課題 1)連携する生活機器を想定したスマートホームのテストベッドが存在しない。

・実機テストベッド：HEMS 機器及び市販の IoT 機器が連携して動作するテストベッドを実際の家屋に構築し、ユースシーンに従って動作設定を行った。

・仮想テストベッド：NICT 総合テストベッド上の仮想マシンにホームゲートウェイなどの宅内機器をモデル化し、実機の検証結果を反映し検証結果を視覚化できるテストベッドを構築した。

課題 2)設計、開発、評価・検証までを統合されたプロセスとして実施できるスキームが存在しない。

・実機テストベッドで CCDS の検証基盤システムを使用し、検証手順書・検証シナリオの作成、検証実施、検証レポート作成を行った。検証について検証設計（検証要件）から検証実施、フィードバックまで一連の作業結果をガイドラインに反映した。

課題 3)スマートホームの評価・検証において、明確な基準やガイドラインが定まっていない。

・本実証事業で得られた結果を元に、既存の CCDS ガイドライン等を参考にセキュリティ評価・検証ガイドラインを策定した。

３．IoT サービスの創出・展開に当たって克服すべき具体的な課題の解決に必要と考えられるルール整備等

一般社団法人重要生活機器連携セキュリティ協議会(CCDS)が策定済みの 4 分野(車載、IoT-GW、金融端末、オープン POS)ガイドラインのうち、IoT-GW のガイドラインを基に、前述した実機・仮想テストベッドによる検証結果を反映させて、評価・検証ガイドラインを策定した。

IoT 全般の設計・製造・利用に関するセキュリティについては。IoT セキュリティガイドライン(IoT 推進コンソーシアム H28.7)が公表済みであり、その指針の中で「安全安心を実現する設計の検証・評価を行う」ことが挙げられている。そこで、製品の開発フェーズのうち、図３－１に示すように「設計・製造」と「運用」の間に位置する「評価」フェーズについて、セキュリティ検証を行う上での詳細プロセスを規定するガイドラインを策定することとした。

策定したガイドラインは今後 CCDS へ提案を行う。CCDS は IPA や IoT 推進コンソーシアム セキュリティ WG 等の標準化推進団体と連携してガイドラインの標準化に向けた活動を行っており、提案事業で作成したガイドラインはこうした標準化に活動に貢献できるものと考えられる。

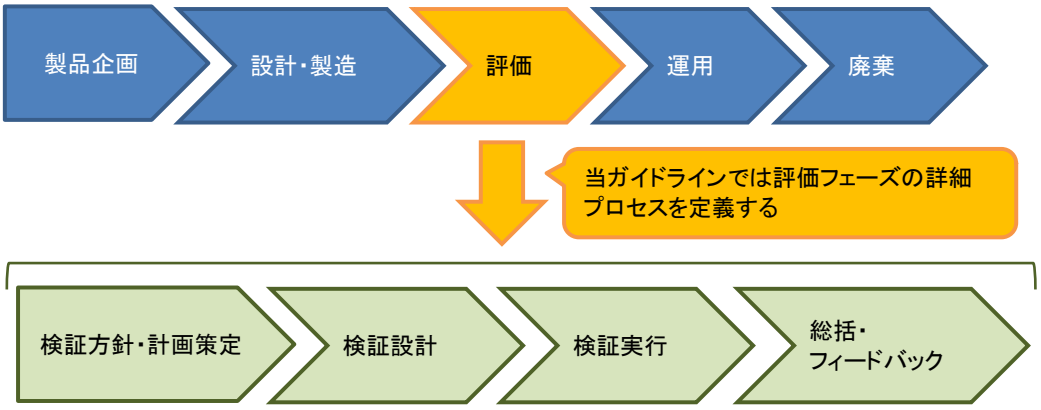


図 3-1　ガイドラインの位置づけ（「CCDS 製品分野別セキュリティガイドライン IoT-GW 編」）

４．実証項目ごとの詳細

4-1 共通事項

実証事業全体のフローを図 4-1 に示す。

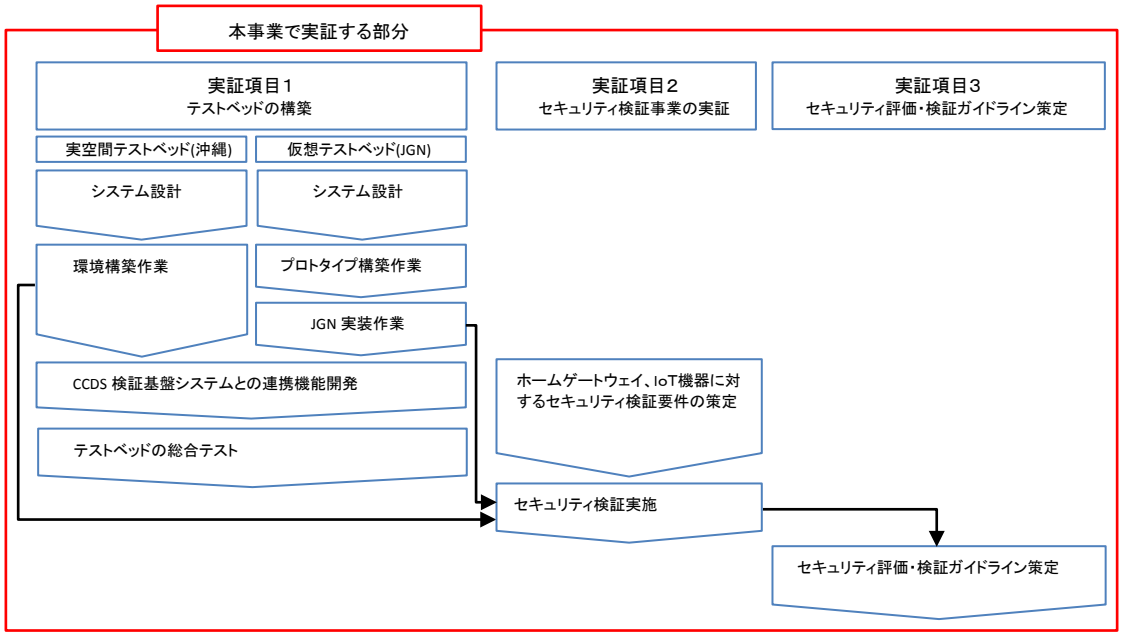


図 4-1　実証事業フロー

実施場所については、研究開発の拠点を東京都品川区のゼロワン研究所内に置き、事業管理及びとりまとめを含む実証作業を実施した。

実空間テストベッドは、沖縄県宜野湾市の建物に構築し、スマートホームを想定した IoT 機器(HEMS、情報家電)を設置し検証を行った。また、仮想テストベッドは、NICT 総合テストベッド上の JGN 仮想マシンを使用して構築し、ゼロワン研究所と JGN(大手町 AP)間を VPN で結び検証を行った。

4-2 各実証項目

実証項目１　テストベッドの構築

1-1）実空間テストベッドのシステム設計、環境構築作業

スマートホームをモデルとして家庭用 IoT 機器の実機を設置したテストベッドを構築した。全体の概念図を図 4-2 に示す。

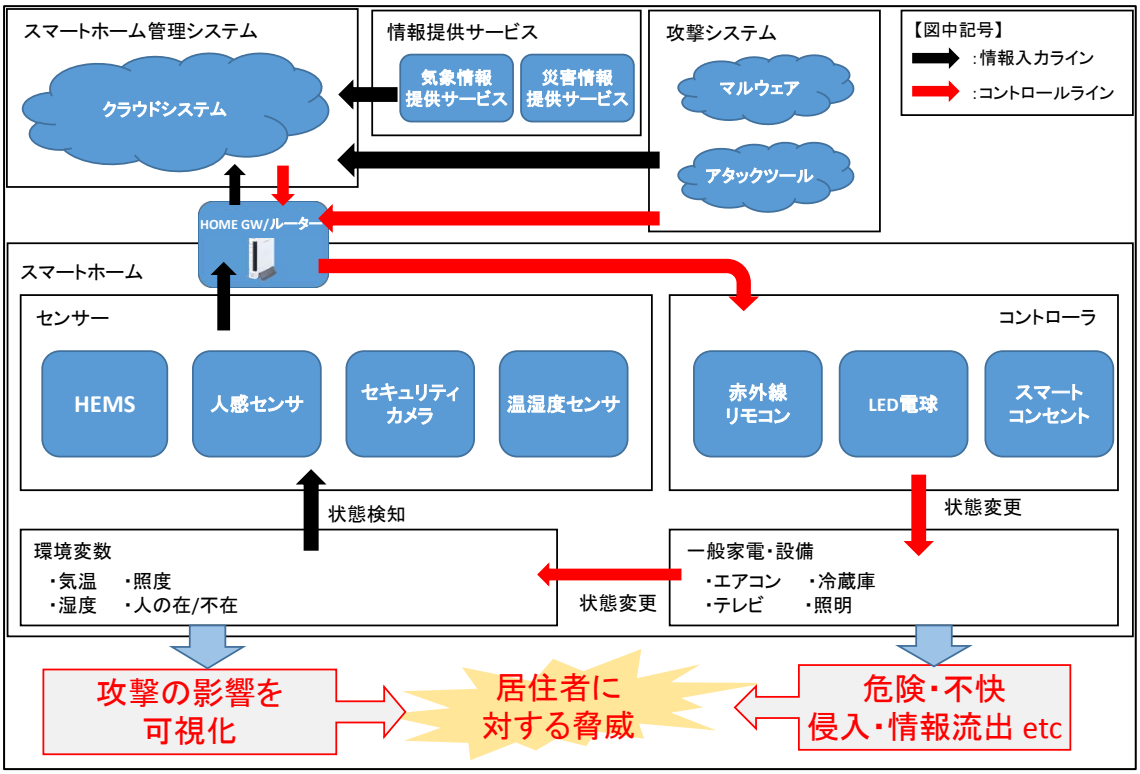


図 4-2　テストベッド構成概念図

設置した機器は大きく分けて大手電機メーカー製の HEMS 対応機器と、個別に製造販売されておりスマートフォンやパソコンの Web ブラウザ等からアクセスし、制御・管理が可能な家庭用 IoT 機器に分かれる。

HEMS(Home Energy Management System)は、家庭内で消費する電力を管理し削減することを主目的としたシステムであるが、付帯する機能としてインターネット経由や家庭内からスマートフォンやパソコンを使用してエアコンや照明の制御、室内の気温、湿度、カメラ映像などの状態を監視するなど IoT 機器としての機能を持ったものも多数存在する。これらは同一メーカー製品を使用する場合は、1 つのアプリケーションソフトで一括制御が可能であり、機器相互の連携動作も可能なシステムもあるが、他メーカー品との連携が困難である場合が多い。

一方、個別の家庭用 IoT 機器は、海外性を含め Web カメラ、環境センサー、照明機器、スマートコンセントなどさまざまな機器が流通しており、機器相互の連携は、ユーザが設定を行う必要があるものの柔軟な連携動作が可能である。

IoT 生活機器単体では、メーカーが自社の製品を個別に検証環境を構築し、独自もしくは市販の検証ツールを用いて、製品の安全・安心に問題がないことを検証して提供されていると思われる。しかし、上述のように多種多様の IoT 機器、サービスの連携が容易にできる状況では、メーカーが想定している範囲を超えた使い方や、連携動作が可能となり、想定外の動作や新たな脆弱性が生じる可能性がある。

従って、前述したように、様々な機器が連携する環境では、個別の企業での対応が難しく、業種横断的な対応が必要である。

そこで、このようなメーカーが異なる機器相互の連携動作についてもセキュリティ検証を実施するため、市販されている IoT 機器が連携して動作するスマートホームを構築し、サンプルユースシーンによる実証実験ができる実機テストベッド環境を構築した。

想定したユースシーンを表 4-1 に示す。

[省エネ]

No		ユースシーン	機能概要	連携機能
1	消し忘れ防止	家族全員が外出した後、消し忘れたエアコン、照明、TV を自動で OFF する	人感センサーが ON から OFF に切り替わってから 30 分後にトリガーにして、対象の機器を OFF する。	機器制御、人感センサー、タイマー
2	無駄遣い防止(空調)	夏から秋または冬から春に季節が変わるころ、外気温が快適に過ごせる状態になったとき使用している空調を OFF する。 合わせて窓を開けてはいかがとアドバイスする。	外気温が 20℃以上、22℃以下になったことをトリガーにして、空調を OFF する。	機器制御、温湿度センサー
3	無駄遣い防止(照明)	朝点灯させた照明を、日が昇り外からの光が入り明るくなるころに自動で OFF する。 ※必要な場所は手動で点灯することで、不要な照明は消灯する。	毎朝 10 時に一度照明を OFF する。	機器制御、タイマー
4	省エネ運転	1 日の電力使用量が基準を超えたときに、自動で空調や照明を制御し電力使用を下げる。	家全体の電力使用量を計測。計測した値が基準値を超えたことをトリガーにして、対象の機器を OFF する。 ※電力使用量は 10 分間隔で更新。 ※基準値は使用状況を事前に確認して設定。 ※照明は夜間に消灯すると危険なので、減光する方法で対応	機器制御、電力計測

[防犯]

No		ユースシーン	機能概要	機器連携の説明
1	居るふり	帰宅が遅くなった時に長期間不在となった時に、自動的に照明や TV を ON する。 そうすることで、不在であることをカモフラージュする	・19 時に人感センサーの状態を確認。 →人が居ない状態なら、照明、TV を自動で ON する。 ・22 時に人感センサーの状態を確認。 →人が居ない状態なら、照明、TV を自動で OFF する。	機器制御、人感センサー、タイマー
2	監視カメラ	不在時に、侵入者を検知し通知する。 検知したことを通知し、部屋内部の状況が確認できるようにする。検知したとき照明を ON して威嚇する。	不在時に稼働させ、人を検知したことをトリガーにして、照明を ON する。 同時に映像を記録、遠隔地のオーナーに通知する。	監視カメラ、遠隔地から宅内を確認、機器制御

[快適]

No		ユースシーン	機能概要	機器連携の説明
1	自動点灯	部屋に入った時に自動で照明を ON する	人感センサーで人を検知したことをトリガーに、照明を ON する	機器制御、人感センサー
2	熱中症防止	室内温度が 30℃を越えたとき、室内に人が居る場合は冷房を ON する。熱中症を防止する。	室内温度が 30℃を越えたときに、人感センサーの状態を確認。 →人が居る状態ならい冷房を ON する。	機器制御、温湿度センサー、人感センサー
3	定期換気	長期間家を不在にするとき、自動で換気を行いカビなどの発生を防ぐ	・室内の湿度が基準を越えたことをトリガーに、空調を ON する ・室内の湿度が基準を下回ったことをトリガーに、空調を OFF する	機器制御、温湿度センサー

[防災]

No		ユースシーン	機能概要	機器連携の説明
1	天気予報	天気が雨予報の場合、起床時間頃に青系で点灯。TV やラジオで確認することなく当日の天気予報を把握する。	雨予報を受けたことをトリガーにして、照明を決まった色で点灯	外部からの天気予報通知と連携
2	防災通知	寝ている際に大きな地震、天候の注意報が発生した場合に TV が自動で ON する。危険が近づいていることに気づく、状況を把握する。	防災連絡(yahoo など災害予測等)のメールを受信したことをトリガーに、自動で TV を ON する。	外部からの防災通知(メールなど)との連携

表 4-1　想定ユースシーン

設置した機器は、Echonet Light 対応の HEMS で、エネルギー管理機能だけでなく、エアコンや照明を制御できる機能を含む。対象住宅には、別途、電気工事によって HEMS 対応で同一メーカーの専用機器を取り付けた（Panasonic 製の HEMS「AiSEG」に対応した機器）。これらは、Wi-FI ルータに接続した HEMS 本体および HEMS 無線アダプタを介して有線 LAN、920MHz 帯特定小電力無線、426MHz 帯特定小電力無線により接続されている。

その他の市販 IoT 機器は、Wi-Fi でルータにて接続されているが、人感センサー等一部機器は、Android タブレットと Bluetooth で接続し、タブレット上のアプリケーションソフトを介して接続している。

また、HEMS 対象機器のうちエアコン、天井照明は、HEMS による制御の他、赤外線を使用したネットワークリモコン装置による制御も行うことができる。

実空間テストベッドに設置した機器と、物理的な接続を図 4-3 に示す。

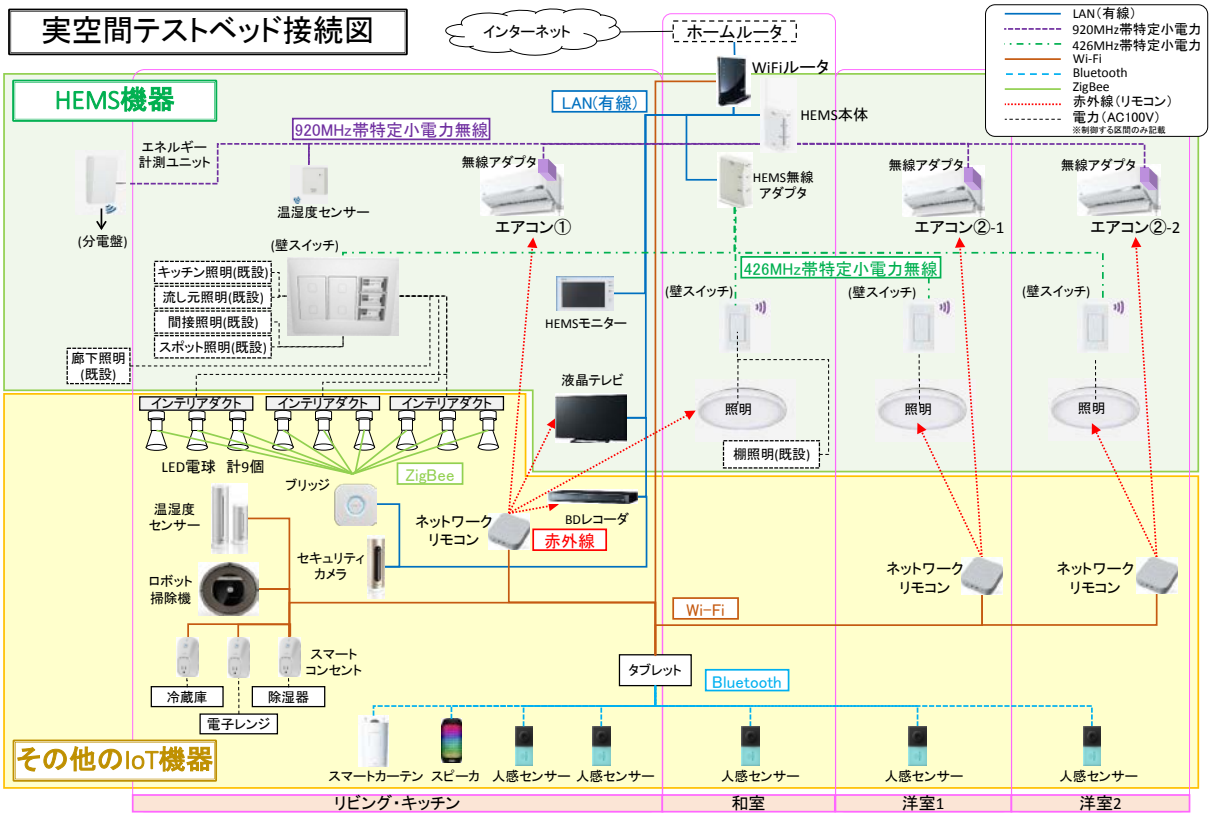


図 4-3　実空間テストベッド構成機器接続図

1-2)　　仮想テストベッドのシステム設計、環境構築作業

実空間テストベッドに沿って、IoT ゲートウェイ及び家庭内 IoT 機器を連携させたスマートホームを仮想的にモデル化し、モデルの実行環境としてシミュレータを構築した。仮想テストベッドでは、正常動作とインシデントによる想定外動作においてシミュレーションを実施し、IoT 機器の連携動作とセキュリティリスクを可視化した。

各ユースシーンにおける実空間テストベッドの結果に基づいて、仮想テストベッドのモデルを調整することで、IoT 機器の異なる設定、台数、使用環境でのセキュリティ上の脆弱性について、シミュレーションによって予測することを目標とした。

仮想テストベッドでモデル化した構成要素を表 4-2 に示す。

カテゴリー	構成要素
エネルギー	・供給電力量
環境変数	・気温
	・湿度
	・照度
人	・居住者
	・不審者
センサー	・電力計(HEMS)
	・温度センサー
	・湿度センサー
	・人感センサー
	・顔認証付き監視カメラ
家電	・エアコン
	・テレビ
	・BD レコーダー
	・冷蔵庫
	・照明機器
中継デバイス	・Wi-Fi ルータ
	・スマートコンセント
	・赤外線学習リモコン
攻撃システム	・情報漏洩につながる攻撃(盗聴など)
	・動作障害につながる攻撃(DoS など)
	・情報改ざんにつながる攻撃(MITM など)
	・不正操作につながる攻撃(なりすましなど)
情報通知システム	・天気予報通知サービス
	・災害情報通知サービス
連携管理システム	・IoT 連携クラウドシステム(IFTTT や mythings など)

表 4-2　モデル化した構成要素

仮想テストベッドの環境構築は、プロトタイプ環境をローカルマシン上に構築し、基本動作を確認した後、複数の仮想マシン間の連携動作機能を開発、大規模シミュレーションに対応できるように NICT 総合テストベッド JGN 上の仮想マシンに移設し実装を行った。

実装した仮想テストベッドのブロック図を図 4-4 に示す。

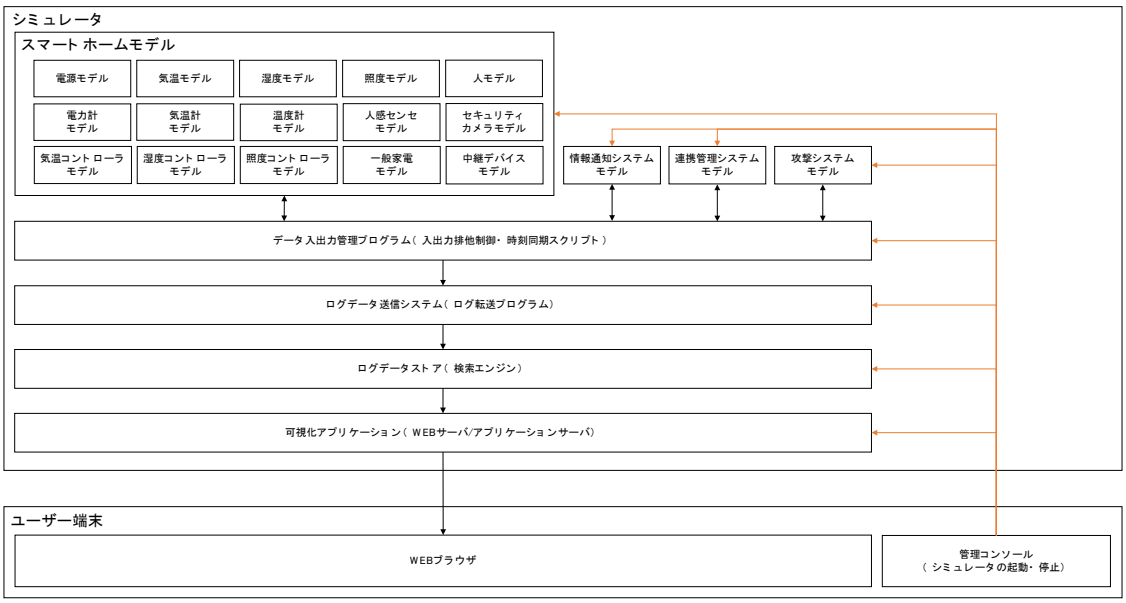


図 4-4 仮想テストベッド構成図

なお、当初計画ではレンタルクラウドサーバ上に仮想テストベッドを構築した後、NICT 総合テストベッド(StarBed)への移行を検討することとしていたが、時間的な制約から NICT 殿と協議の結果、JGN 仮想マシンを使用することとした。使用に際しては 11 月より手続を開始、1 月に仮想マシンの使用を開始し、2 月にプロトタイプから JGN 上の仮想テストベッドへの実装を完了し、実証作業を実施した。

実証拠点であるゼロワン研究所と JGN 大手町アクセスポイントとの間をフレッツ VPN ワイドで接続し、仮想テストベッドへアクセスする構成とした。なお、仮想テストベッドは構築時を除いてインターネット、社内 LAN とは切り離して運用し、セキュリティを確保した。

JGN 仮想マシン相互の接続を含む連携図を図 4-5 に示す。

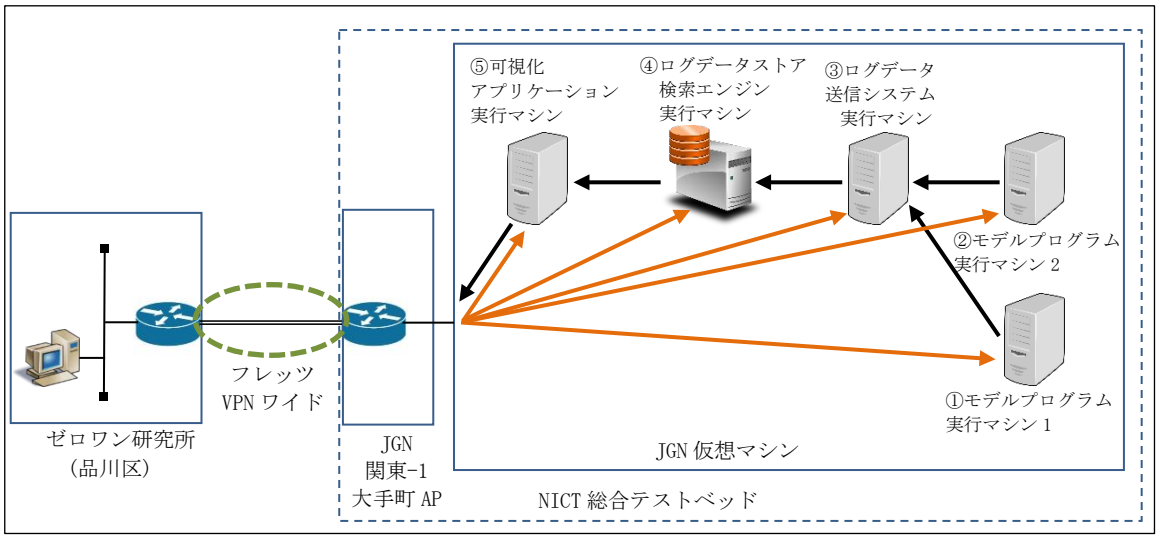


図 4-5 JGN 仮想マシン連携図

1-3)　　CCDS 検証基盤システムとの連携機能開発

CCDS が開発した「検証基盤システム」、「セキュリティ検証ツール（2 種類のソフトウェア）」を活用できるように、システム統合するための要件を整理し、テストベッドとの連携を実施した。

「検証基盤システム」では、統一されたフォーマットで検証手順書の作成から、結果報告、インシデントレポート報告までを実施可能である。

検証基盤システムの機能概要は以下のとおりである。

・検証手順書、結果表を作成、管理することができる。
・検証手順書は、検証基盤と連携しているツールを組み合わせて作成することができる。
・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

「セキュリティ検証ツール」は、複数のプロトコルでファジングテストを実施できるツールがあり、これらを活用して検証ができるような環境整備を実施した。

本実証検証で使用したツール、検証機能を表 4-3 に示す。（グレー部分は不採用のもの）

CCDS ツール	利用した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	キャプチャー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	Wi-Fi ハック	Wi-Fi ルータに設定されている暗号(WEP・WPA など)を解読	不正アクセス

表 4-3　脆弱性検証ツール

1-4)　　構築環境の総合テスト

構築した実空間テストベッド環境に対する総合テストを実施し、想定した機能要件が満たされているか、想定外の不具合が残存していないか、システムの性能要件は充分か等の観点で確認を行った。

① 実空間テストベッド

実空間テストベッドに設置した IoT 機器について、単体の動作確認及び構築設計書に記載したユースシーンに沿った連携機能が正しく動作することを確認した。

(1) IoT 機器機能単体テスト

ユースシーンに関係する機器単体の動作をテストし、正常動作を確認した。

対象機器を表 4-4 に示す。

[トリガー機器]

No	機能	IoT 機器
①	人感センサー	人感センサー
②	タイマー	スマートフォン or タブレットの時計機能 タイマーアプリ
③	電力量	HEMS
④	温湿度センサー	温湿度センサー
⑤	メール	インターネット上のメールサービス
⑥	カメラ	セキュリティカメラ

[制御機器]

No	機能	IoT 機器
①	赤外線リモコン	ネットワークリモコン

表 4-4　機器単体テスト対象

いずれも正常に動作することを確認した。

(2)連携機能(ユースシーン)テスト

表 4-1 のユースシーンに沿って機器が連携して動作することを確認した。

いずれも正常に連携して動作することを確認した。

② 仮想テストベッド

NICT 総合テストベッドに実装した仮想テストベッドについて、関数単体、モデル単体、モデル結合の場合の動作確認を行った。また、ユースケースを適用したテストを実施し、結果が Web で可視化できることを確認した。

(1) 関数単体テスト

モデルを構成するフィルタ、各種アクション、入出力処理などの関数単体の機能が正常に動作することをテストし、正常な結果を確認した。

(2) モデル単体テスト

23 のモデル＋攻撃 4 モデル(情報漏洩、動作障害、情報改竄、不正操作)についてモデルパラメータの設定により各モデルを構成し、各々のモデルが正常に動作することをテストし、正常な結果を確認した。

(3) モデル結合テスト

23 のモデルそれぞれに攻撃なしの場合及び攻撃 4 モデルがある場合の全てのモデルが連携して正常に動作することをテストし、正常な結果を確認した。

(4)モデル連携動作可視化テスト

シミュレータを使ってモデルの連携動作結果が可視化できることをテストし、正常な結果を確認した。

以上により、設定・入力が正常な場合、シミュレータから正常な結果を得られることを確認し、仮想テストベッドが正常に機能することを確認した。

実証項目 2　セキュリティ検証事業の実証

2-1)検証要件の策定

本実証事業が対象としているホームゲートウェイと情報家電、HEMS が連携して機能するユースケースを想定し、検証要件及び、検証シナリオ、検証仕様書の策定を行った。

セキュリティ検証の方針・計画策定を行うにあたり、「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。「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。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。

検証要件の策定にあたっては、評価フェーズに限らず、製品のライフサイクル設計にわたったセキュリティ対策を念頭に置いた検討が必要である。既存のガイドラインにおいて推奨されている、製品ライフサイクルごとに必要な対策事項を図 4-6 に示す。

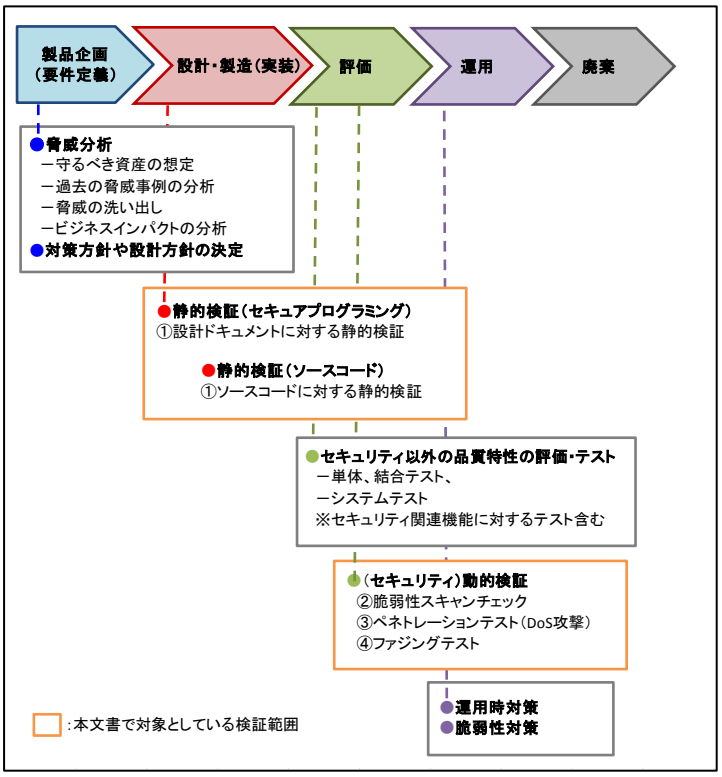


図 4-6　製品ライフサイクルの各工程におけるセキュリティ対策

また、スマートホームにおいては、産業用 IoT 機器などとは設置機器、使用形態やユーザ層が異なるため、想定すべき脅威についてもスマートホームに特化したものが考えられる。図 4-7 はスマートホームにおける脅威を、WAN 側の HTTP/CoAP サーバー、WAN とホームネットワーク(HNW)をつなぐ IoT-GW、HNW 内の機器に分けて抽出したものである。

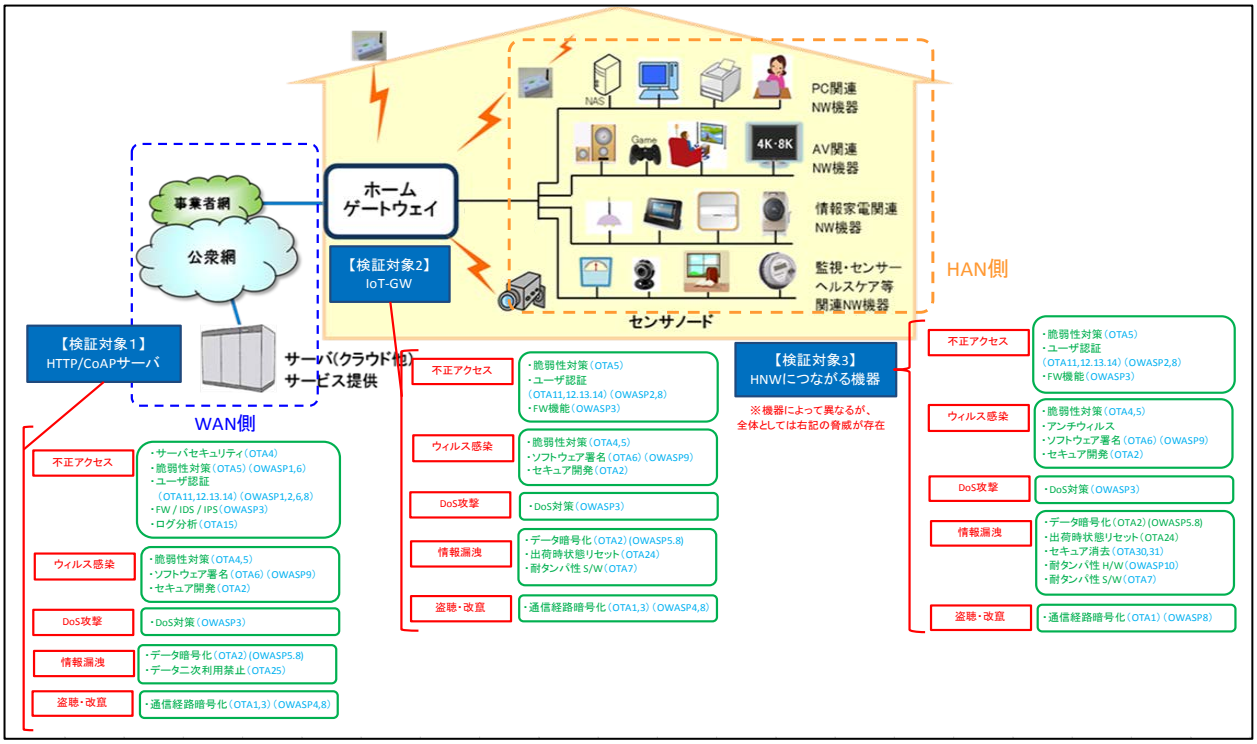


図 4-7　スマートホームにおいて想定される脅威

本実証では、表 4-1 に示したユースシーンをベースに、スマートホームで想定されるこれらの脅威を検討し、検証要件を策定した。

検証要件の詳細は参考資料「(2-1-a)セキュリティ検証 要件書」に示す。同要件書より対象とした脅威の概要イメージを図 4-8 に示す。

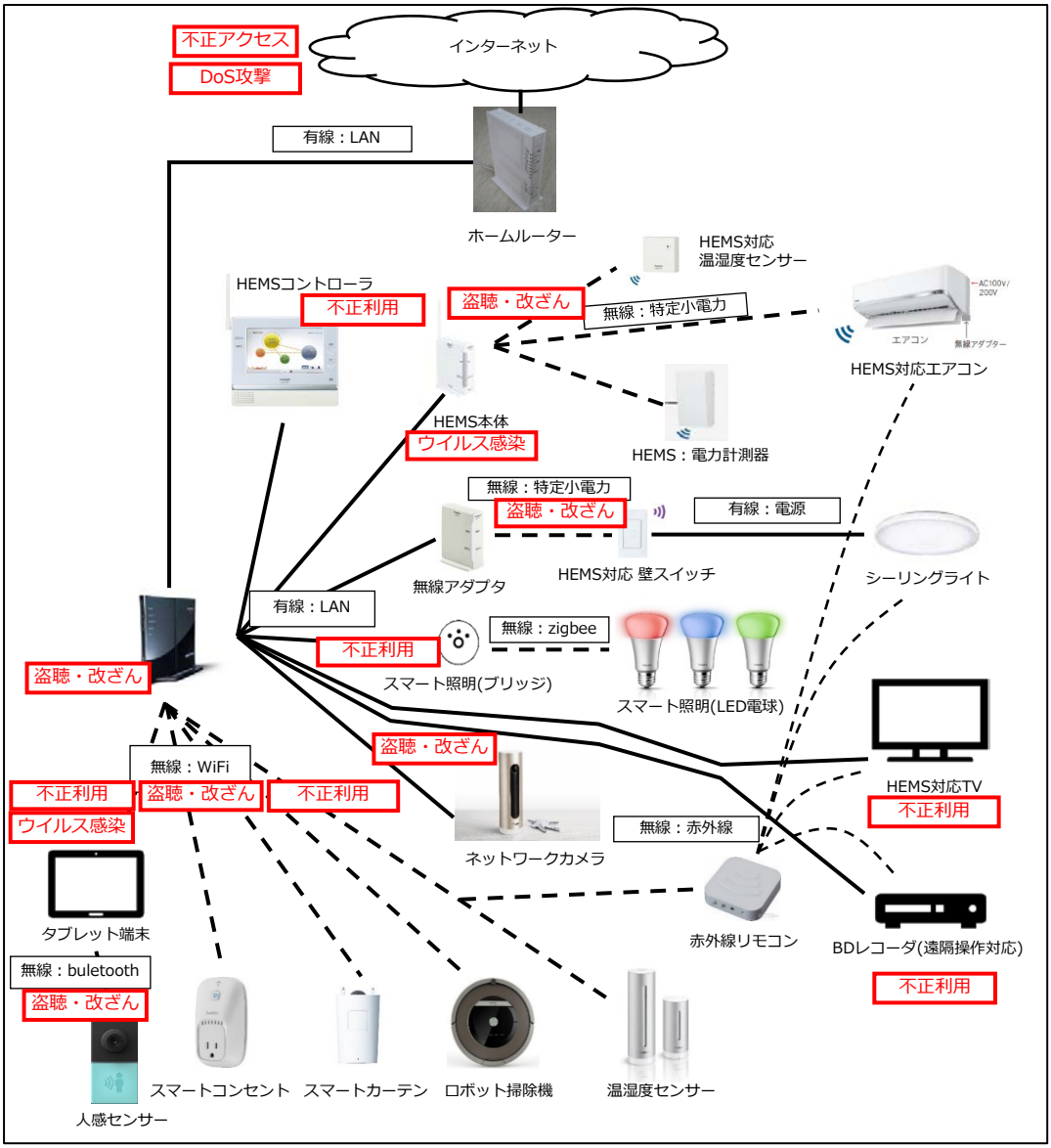


図 4-8　対象とした脅威の例

2-2) サンプル IoT 機器を用いたセキュリティ検証

① 実空間テストベッド

実空間テストベッドにおいて 2-1 で策定した検証要件書に従い検証作業を実行するために、検証手順書を CCDS の検証基盤上で作成し、セキュリティ検証を実行した。

(1) 検証手順書

セキュリティ要件書にて検討した内容を元に、各検査対象機器に対し選定したツールを使って実施する検証項目を一覧にし、検証手順書として作成した。

作成作業は CCDS の検証基盤システム上で必要な内容を入力して行った。

図 4-9　CCDS 検証基盤 検査手順書画面

図 4-9 に検証手順書画面を示す。今回の検証では、初回の検証を実施した後に検証結果を確認しつつ手順書を追加したため、5 つの手順書を作成して実施した。

(2) 検証シナリオ

作成した検証手順書に紐付く検証シナリオを作成した。これも検証基盤システム上で作成でき、検証手順書に紐付ける形で登録していく。

図 4-10　CCDS 検証基盤 検査シナリオ画面

図 4-10 に検査シナリオ画面を示す。登録した検証手順書が一覧で表示され、各手順書の項目に検証シナリオを設定する

(3) 検証の実行と結果

検証の実行も検証基盤システムから実施する。登録した検証手順書、検証シナリオの内容を検証実行画面から各項目を実行する。図 4-11 に検査実行画面を示す。

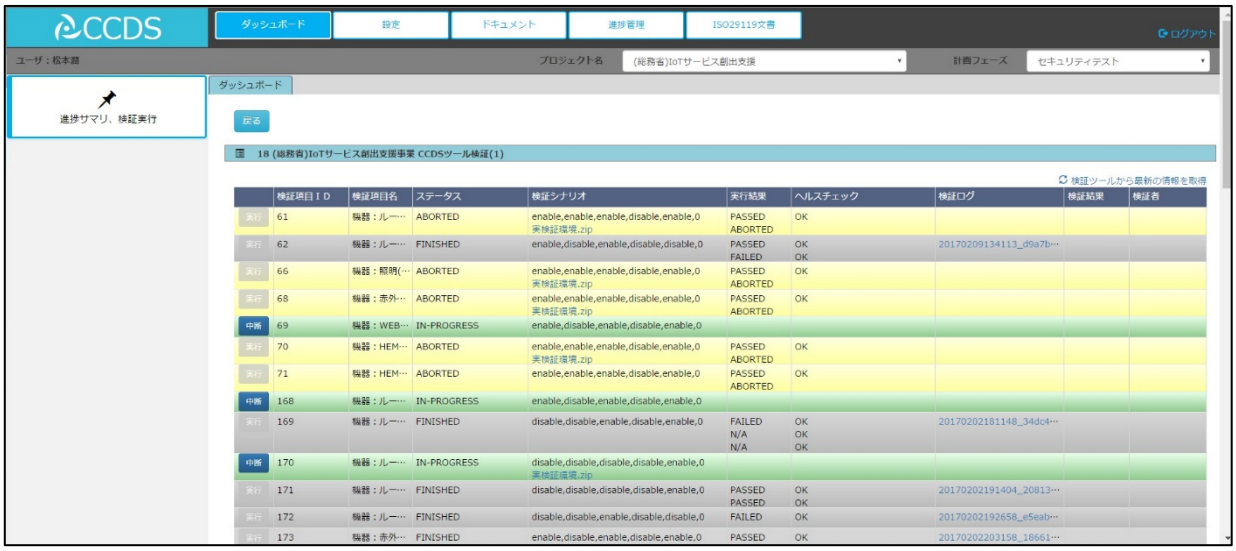


図 4-11　CCDS 検証基盤 検査実行画面

結果は自動的に手順書に反映され、結果表が完成する。図 4-12 に検査結果画面を示す。

図 4-12　CCDS 検証基盤 検査結果画面

結果手順書、検証シナリオの登録までは地道な登録作業が必要だが、登録してしまえば実行と結果取得が自動で行え、再評価が必要な場合でも簡単に実施できる。

(3) 脅威レポート、セキュリティ評価レポート

検証を実行した結果、発見された脅威をレポートとして登録した。

脅威レポートは、脅威の内容だけを登録するのではなく、CVSS の深刻度評価も行う。CVSS 深刻度評価は自動計算されるようになっているので、各項目を精査し登録するだけで結果が算出される。

表 4-3 に今回の検証結果の CVSS 深刻度ごとの件数を示す。

	しきい値	件数
緊急	9～10	0
重要	7～8	3
警告	4～6	15
注意	1～3	5
なし	0	1

表 4-3　検証結果の CVSS 深刻度

最も高レベルの「緊急」は該当がなかったが、二番目の「重要」は 3 件が該当した。具体的には以下のとおりである。

・Wi-Fi ルータ：無線 LAN 上のパケットをキャプチャーしてパスワードの取得、機器内部への侵入が可能（WPA2 による認証暗号キー）
・ブルーレイレコーダ：SQL インジェクションが可能な脆弱性
・ブルーレイレコーダ：Web サーバーのクラッシュ、システム上で任意のコードを実行可能な脆弱性

特に、Wi-Fi ネットワークに侵入される可能性が示されたことで、各ユースシーンにおいてもなりすましによる IoT 機器の不正操作や情報流出の脅威にさらされているおそれがあることが判った。

なお、登録された脅威レポートの結果を集計し、セキュリティ評価レポートが発行される。発行自体は検証基盤が自動で行い、詳細なコメントを追記していく。

セキュリティ評価レポートのイメージを図 4-13 に示す。

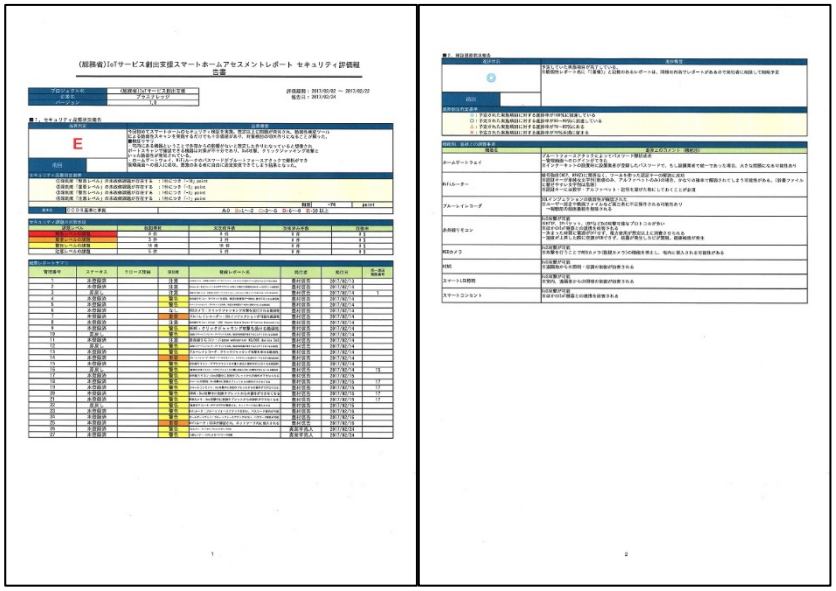


図 4-13　セキュリティ評価レポート（イメージ）

② 仮想テストベッド

実空間テストベッドでの結果をもとに、仮想テストベッドにおいてユースシーンに従って機器を連携させた場合のシミュレーションを実施した。

シミュレーションは下記の段階で実施した。

まず、実空間テストベッドのスマートホームを対象としたセキュリティ検証と同様に脆弱性や不具合をシミュレーションによってモデル化した。

次に、脆弱性・不具合対策をモデル化し、その状態においてシミュレーションができる環境を構築した。

詳細は参考資料 2-2-b に示す。

以下、代表的なシミュレーション結果は以下の通りである。

(1) 実空間セキュリティ検証のシミュレーション

実空間テストベッド同様、代表的なユースシーンについて、居住者の行動と天候・不審者侵入などの外的要因をトリガーにした連携動作を設定し、ホーム GW に対する攻撃を種類別にシミュレーションを行った。

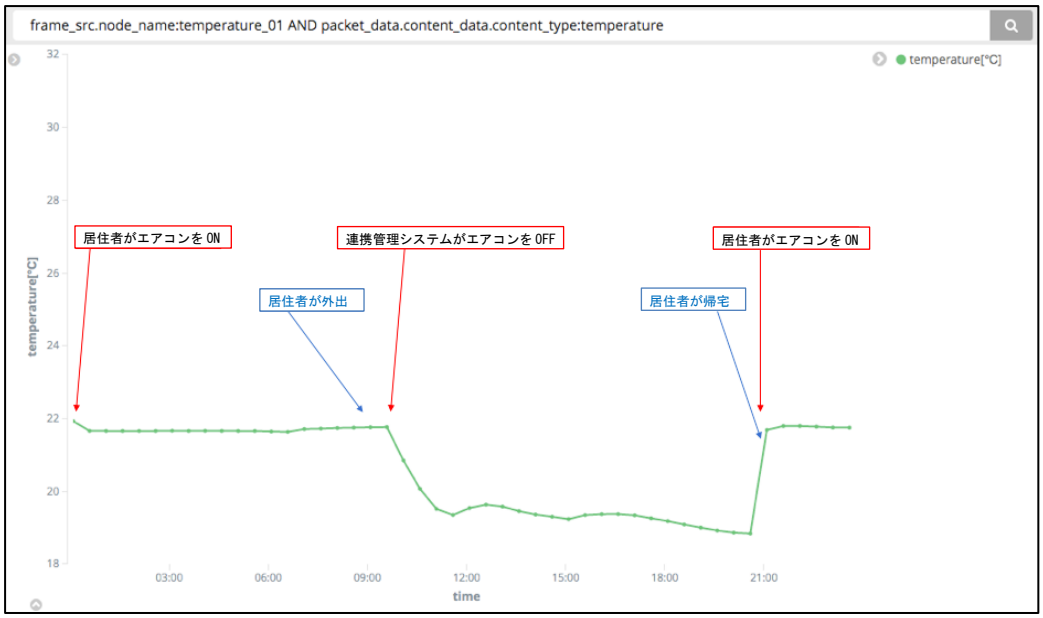


図 4-14　連携動作シミュレーション結果(室内温度)

図 4-14 は、脅威が無い場合のエアコン動作による室温変化する状態の温度変化シミュレーション結果である。なお、本結果は、所定の時点における状態の静的挙動を求めて、個々の時点における挙動をグラフ化したものである。図では、9 時に居住者が外出したのを人感センサーが検知し、エアコンが OFF になる状態。そして、居住者が帰宅した後、エアコンを ON にした状態を示している。

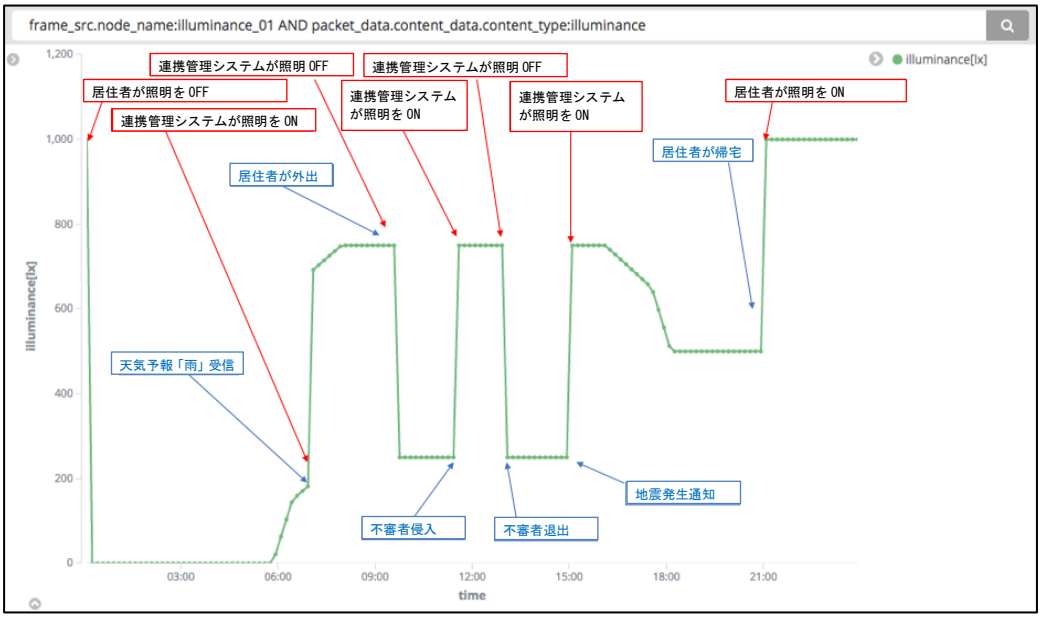


図 4-15　連携動作シミュレーション結果(室内照度)

図 4-15 は、室内照度における状態変化シミュレーション結果である。

照明については、以下の連携設定を行っている。

・7 時にインターネットから天気予報を取得し、予め設定してある天候に応じた色の照明を点灯（快適環境、情報表示）

・Web カメラが登録されていない顔を認識したら照明を点灯(警告)
人感センサーで人を感知しなくなったら消灯（省エネ）

・インターネットから地震発生・津波警報を受信したら点灯（警告）
以上の連携設定が、正常に動作していることが確認できた。

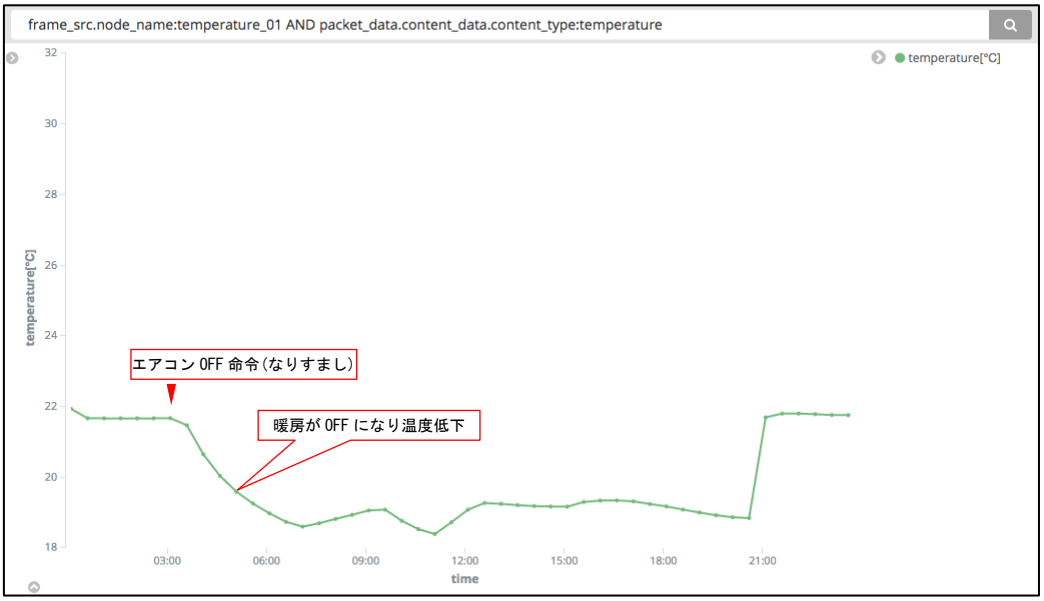


図 4-16　Wi-Fi ルータになりすまし攻撃があった場合(室内温度)

一方、図 4-16 は、攻撃により連携動作が阻害された場合の例である。

Wi-Fi ルータがなりすまし攻撃を受け、偽の命令によりエアコンが午前 3 時に OFF した結果、室温が低下していく様子が再現している。

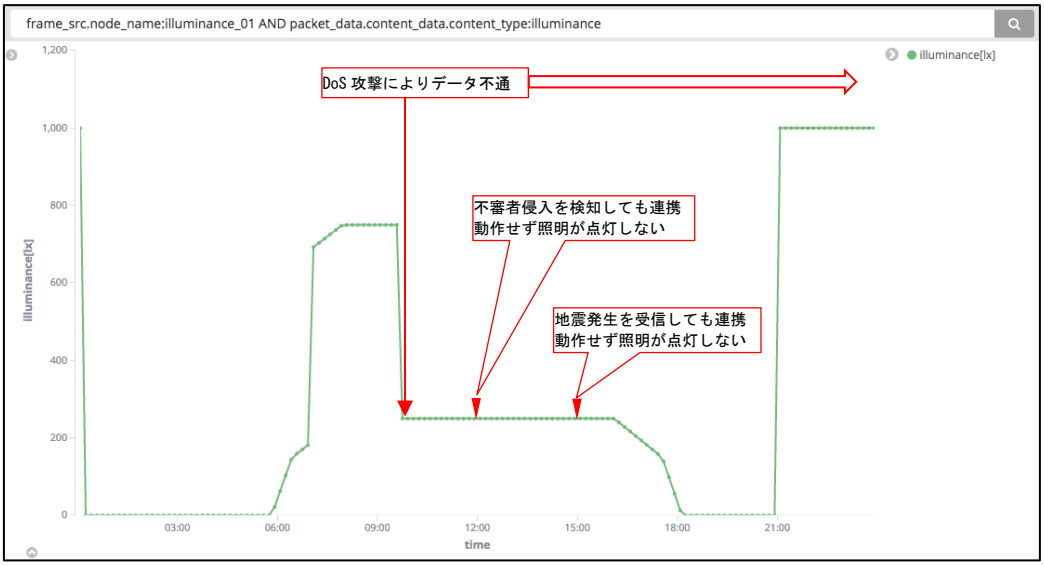


図 4-17　Wi-Fi ルータに DoS 攻撃があった場合(室内照度)

また、図 4-17 は、DoS 攻撃により Web カメラによる侵入者検知、インターネットからの地震発生・津波警報が連携管理システムに届かず、警告、通知のための照明制御ができなかった場合である。

図 4-10 と比較すると、12 時頃に侵入した不審者および 15 時頃の地震発生通知を検知できず、照明が点灯しないため照度が変化していないことが判る。

同様に、盗聴、情報改竄攻撃を受けた場合の動作についてもシミュレーションできることを確認した。

(2) 脆弱性・不具合対策の検討

脆弱性・不具合対策として、連携管理システムは Wi-Fi ルータからの KeepAlive 通信が 10 分以上途切れると管理者端末に異常発生の通知(alert)を送るように設定した。

DoS 攻撃を再現したシミュレーションにおいて、通信不能になったことを検知する通知が送信され、通信状態の検知による対策が可能であることがわかった。

以上の結果より、仮想テストベッドを使用したシミュレーションによって実空間テストベッドに設置した機器の連携動作を再現可能であり、さらに脆弱性による脅威についてもさまざまな仮定に基づいた動作結果を得ることができた。

各機器モデルについて、今回設置した実機に限らず想定する製品の仕様を設定することにより多様な製品が混在する環境、複数のスマートホームが攻撃を受けた場合などについても定量的評価が可能であることがわかった。

実証項目３　セキュリティ評価・検証ガイドライン策定

3-1)セキュリティ評価・検証ガイドライン策定

CCDS がこれまでに策定したガイドライン及び関連文書を参考に、本実証事業で得られた結

果を踏まえ、スマートホームにおける IoT セキュリティ検証ガイドライン（以下、検証ガイドライン）を作成した。

ガイドラインを参考資料「(3-1)セキュリティ検証ガイドライン」に示す。

ガイドラインに記載した項目は以下の通りである。

1. はじめに
  1-1. IoT セキュリティの現状と脅威
  1-2. 検証ガイドラインにおける対象範囲
2. セキュリティ検証プロセス
  2-1. 製品ライフサイクルにおける検証プロセスの位置づけ
3. セキュリティ検証の方針・計画策定
4. 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
  4-2. セキュリティ検証の手法
    4-1-1. 静的検証手法
    4-1-2. 動的検証手法
  4-3. 検証仕様書の策定及び、検証ツールの選定
  4-4. 検証手順書の策定
  4-5. 検証データの準備
5. 検証実行
  5-1. セキュリティ検証の実行
  5-2. 検出されたインシデント情報の管理方法
    5-2-1. インシデントレポートフロー
    5-2-2. セキュリティインシデントレポートの記載項目
    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
  5-3. 報告・検証完了
    5-3-1. 検証の実施状況に関する報告
    5-3-2. 検証の完了報告
6. 検証プロジェクトの総括・フィードバック

本検証ガイドラインは、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・検証に関する項目を参考に、スマートホームを対象分野として、具体的なセキュリティの検証プロセスを更に掘り下げた内容として策定した。

CCDS では、IoT 機器を対象としたセキュリティガイドラインの策定を進めているが、今回構築したセキュリティ検証プロセスを基に、セキュリティ評価・検証に関するテストプロセスを定義し、検証用ガイドライン案として CCDS へ提案を行う。CCDS は IPA や IoT 推進コンソーシアム セキュリティ WG 等の標準化推進団体と連携し、ガイドラインの標準化に向けた活動を行っており、本実証事業で作成したガイドラインは、こうした標準化活動に貢献できる。

なお、本ガイドラインは、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、今回のスマートホームを想定したセキュリティ検証用テストベッドに対する実証実験の結果をもとに作成したので、他分野に応用する場合には注意が必要である。

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 IoT-GW 編 Ver.1.01（4.2.3 項 評価フェーズ）」

4-3　本実証成果の意義

１．で述べたように、IoT 機器の連携はさまざまな課題を抱えている。

IoT 総合戦略（情報通信審議会「IoT／ビッグデータ時代に向けた新たな情報通信政策の在り方について第三次中間答申」平成 27 年 9 月 25 日付け諮問第 23 号）においても、多様なシステムが相互接続された System of Systems である IoT システムで使用される IoT 機器のセキュリティ対策を抜本的に強化する必要があり、特にスマートハウスにおいては宅内で複数の IoT 機器・アプリがネットワークを介して連携し、使い方や状況によっては IoT 機器・アプリが単独で動作する場合には想定できなかったリスクが生じることがあると指摘している。

本実証は、スマートホーム内で IoT 機器が連携するユースケースを作成し、実機での脆弱性検証を実施しスキームを確立するとともに同様の構成・脆弱性を仮想的にもシミュレーションにより再現し、結果をもとにガイドラインを策定したものであり、これにより業種横断的な IoT 機器のセキュリティ検証へのハードルが下がることで社会的ニーズに応えることができる。

スマートホームで使用されるようなコンシューマ向け IoT 機器の数は、2015 年には世界で約 54 億台であったものが、2020 年には 2 倍以上の 125 億台になると予測されている。（平成 28 年版情報通信白書/出典:IHS Technology）。

一方、「情報セキュリティ 10 大脅威 2017」（IPA）によると、「IoT 機器の脆弱性の顕在化」が組織の第 7 位に、また個人ではランク外ながら「IoT 機器の不適切管理」が初めて登場するなど、IoT 機器のセキュリティ問題がクローズアップされている。

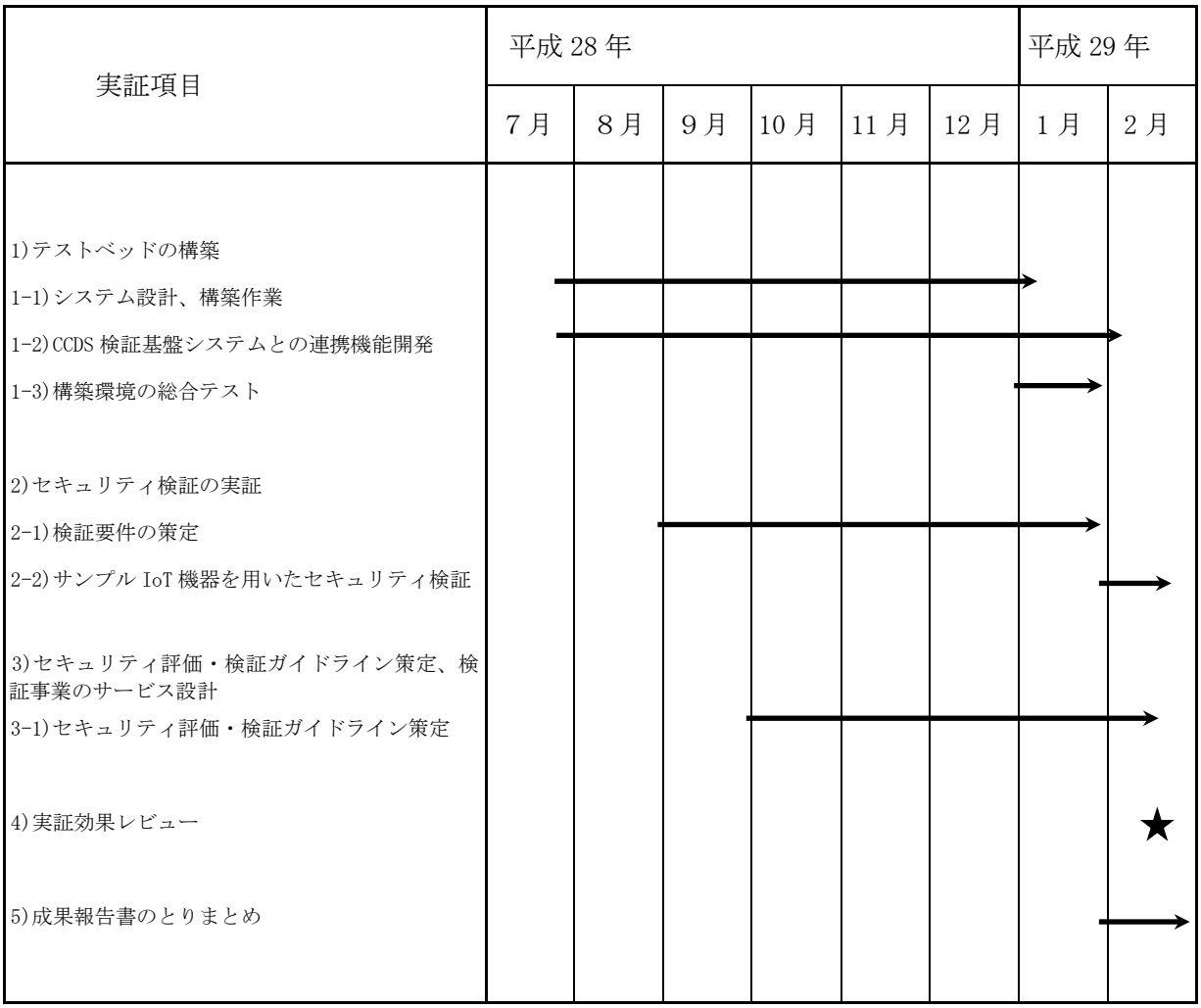
脆弱性を抱えたままの IoT 機器の設置、特に家庭ではデフォルト設定のままの使用などの不適切管理により、当該機器のみならず踏み台にされて周囲に被害が拡大することも懸念され、本実証事業の成果により製品へのセキュリティ評価・検証が浸透することにより、スマートホームにおける脅威の軽減に資することができる。

例えば、家庭で利用するルータに脆弱性が発見されたケースでは、そのメーカーは数年前の製品に対してファームウェアの更新の呼びかけを消費者に対してすることとなり、全国紙への広告掲載費用に加えてブランドの低下が発生した（直接費用だけでも数千万円以上）。IoT 機器を提供する企業にとっては本実証の成果を活用することで、このような費用の低減につながり、その脆弱性に端を発する被害（家庭内でつながっている PC 等が踏み台にされること、各種の個人情報が漏洩すること等）を抑えることにもつながる。

また、本事業で構築した実機テストベッド、仮想テストベッドをベースに新たな検証拠点として活用することで、家庭用 IoT 機器の検証ニーズに応える第三者検証事業を育成し、雇用を創出することも考えられる。

類似の事例として、沖縄県 IT 津梁パークではモバイル機器等の検証拠点を設けた結果、平成 25 年の開設から現在までに検証事業への従事者約 200 名以上の雇用を創出している。家庭用 IoT 機器についてもモバイル機器以上の第三者検証への需要はあると考えられるため、地域の雇用創出にも十分貢献できる。

５．実施スケジュール


実証項目
平成 28 年
平成 29 年
7 月
8 月
9 月
10 月
11 月
12 月
1 月
2 月
1)テストベッドの構築
1-1)システム設計、構築作業
1-2)CCDS 検証基盤システムとの連携機能開発
1-3)構築環境の総合テスト
2)セキュリティ検証の実証
2-1)検証要件の策定
2-2)サンプル IoT 機器を用いたセキュリティ検証
3)セキュリティ評価・検証ガイドライン策定、検証事業のサービス設計
3-1)セキュリティ評価・検証ガイドライン策定
4)実証効果レビュー
5)成果報告書のとりまとめ

６．実証終了後の計画等

6-1 実証終了後の IoT サービス

実空間テストベッドについては、実証期間終了後は CCDS 会員企業を中心に下記の計画で、第三者セキュリティ検証サービスの提供を行い、自律的な事業の運営及び、セキュリティ対策の普及を図る。

・想定顧客(マーケット)：CCDS 会員を中心とする IoT 機器開発メーカー
・提供する IoT サービス：テストベッドを活用したセキュリティ第三者検証サービス
・サービス提供：（同）ゼロワン研究所（検証上流設計）、
（株）マストトップ、（株）プラスナレッジ（検証実行）
・サービス拡販/広報：（株）ブロードバンドタワー

事業年度	H29年度	H30年度	H31年度	H32年度	H33年度
想定売上高(千円)	―	40,000	80,000	90,000	100,000
売上根拠 (提供サービス/ 想定顧客数)	テストベッドの整備拡充。(実機・仮想) サービス事業者が連携して課題解決に取り組むための第三者セキュリティ検証事業のサービスモデルの設計。	プロトタイプのセキュリティ第三者検証サービスを本事業参加企業を含む4社へ展開。 初期費用：2,000万(500万×4社)、 サービス費用：2,000万(500万×4社)	正式リリースのセキュリティ検証サービスを既存4社+新規6社へ展開。 初期費用：3,000万(500万×新規6社)、 サービス費用：5,000万(500万×10社)	正式リリースのセキュリティ検証サービスを既存10社+新規3社へ展開。 初期費用：2,000万(500万×新規4社)、 サービス費用：7,000万(500万×14社)	正式リリースのセキュリティ検証サービスを既存14社+新規3社へ展開。 初期費用：1,500万(500万×新規3社)、 サービス費用：8,500万(500万×17社)

仮想テストベッドについては 2 月末で一旦運用を終了したが、再度 NICT 総合テストベッド上または他のクラウドサーバ等に構築が可能であり。実空間テストベッドと合わせて運用し、さらなる機能、規模の拡張も視野に入れている。

6-2 普及展開等

IoT 機器の各産業分野では、セキュリティ検証事業に関するニーズが顕在化しており、本研究開発にて得られた知見を開発工程に組み入れる事で、製品のネットワーク通信による高度化を効率よく実施する事が可能になる。これにより、日本製品の国内外における製品競争力を高めると共に、他業種の機能連携による更なる機能の高度化への基盤作りに貢献することができる。

また、沖縄県内での IoT セキュリティ検証事業を拡大するためのツールとして、実証事業の展開とともに、教材としても活用し、人材育成に役立てることも可能である。

ただし、1．でも述べたように現状ではセキュリティ評価･検証に関して強制力のある規格、基準がなく、機器メーカーにとってはコスト面でのハードルが高い。このため、評価・検証に関する標準規格の策定とともに、低コストで統一したスキームによる検証コスト低減も課題となる。

参考資料

[実証項目 2　セキュリティ検証事業の実証]

項目 No	内容	ファイル名
2-1)検証要件の策定 a. 検証仕様書の作成	セキュリティ検証の設計	(2-1-a)セキュリティ検証 計画書
		(2-1-a)セキュリティ検証 要件書
		(2-1-a)セキュリティ検証 検証手順書
2-2)サンプル IoT 機器を用いたセキュリティ検証	実空間テストベッドのセキュリティ検証結果	(2-2-a)実空間テストベッド セキュリティ検証 検証結果
a. 実空間テストベッドで検証の実行	仮想空間テストベッドのセキュリティ検証結果	(2-2-b)仮想空間テストベッド-シミュレーション実施計画書
b. 仮想空間テストベッドで検証の実行	(シミュレーション実施・結果)	(2-2-b)仮想空間テストベッド-シミュレーション結果報告書

[実証項目３　セキュリティ評価・検証ガイドライン策定]

項目 No	内容	ファイル名
3-1)セキュリティ評価・検証ガイドライン策定 a. ガイドライン案	実証実験の結果からガイドライン化	(3-1)セキュリティ検証ガイドライン