経済産業省

機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き

別冊４　機器個別のセキュリティ検証プラクティス集

概要資料

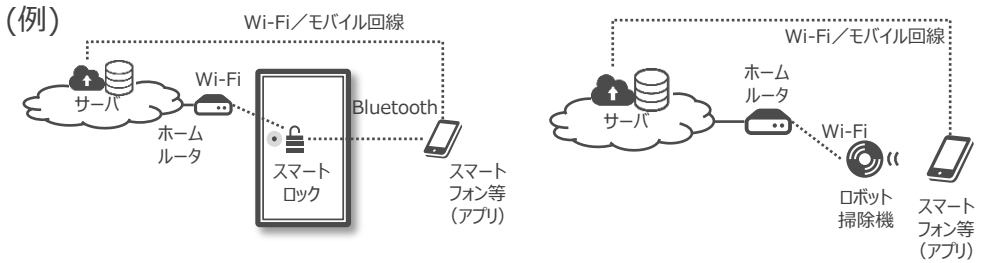
経済産業省　商務情報政策局

サイバーセキュリティ課

「機器個別のセキュリティ検証プラクティス集」の策定背景・目次構成

- 令和4年度、**IoT機器の脆弱性検証を希望する中小企業等を募集し、当該機器に対して無償の検証を提供する実証**を行った。
- この実証を通じて得られた結果を踏まえ、**代表的なIoT機器に対して検証事業者が実施すべき事項や留意すべき事項を「機器個別のセキュリティ検証プラクティス集」としてまとめ**、「機器のサイバーセキュリティ確保のためのセキュリティ検証の手引き」の新たな別冊（別冊4）として公開。

「機器個別のセキュリティ検証プラクティス集」 目次構成

章	節	主な記載内容
1. 背景と目的	1.1 背景 1.2 本別冊の目的 1.3 本別冊の対象者・活用方法 1.4 本別冊の構成	• 本別冊（プラクティス集）策定にあたっての背景や目的を記載。 • 本別冊で対象とする機器や活用方法を明記する。活用方法については、検証事業者だけでなく、IoT機器を開発する中小企業等において、社内で検証を実施する際の手引きとして活用可能であることを明記。
2. UTM 3. ゲートウェイ・ルーター 4. ネットワークスイッチ 5. モバイル端末 6. スマートロック 7. スマート家電 8. ドローン 9. ネットワークカメラ 10. センサ・監視装置 11. 産業用コントローラ	X.1 機器の概要・想定脅威 ※ Xは章番号を意味する。	• 当該機器の概要及び想定されるユースケースを記載。 （例）  • 当該機器で考慮すべきセキュリティ脅威を記載。
	X.2 想定される検証環境	• 当該機器の検証にあたって、構築すべき検証環境を記載。
	X.3 適用すべき検証手法	• 当該機器の検証にあたって、適用すべき検証手法や検証にあたって確認すべき範囲を記載。
	X.4 実証において検出された代表的な脆弱性	• 実証を通じて検出された脆弱性のうち、深刻度が高い脆弱性について、その概要や悪用された場合の影響について記載。
	X.5 想定される推奨事項	• 検出された脆弱性に対して、どのような対策が推奨されるかを記載。
	X.6 検証に当たっての留意事項	• 当該機器の検証にあたって、検証事業者が留意すべき事項を記載。

「機器個別のセキュリティ検証プラクティス集」の記載概要

- プラクティス集の「X.3 適用すべき検証手法」では、実証において適用された検証手法をベースに、**各機器の検証にあたって適用すべき検証手法や検証にあたって確認すべき範囲を整理**。
- 「X.4 実証において検出された深刻度の高い脆弱性」では、**実証で検出された深刻度の高い脆弱性を記載**しつつ、**当該脆弱性が悪用された場合に想定される影響と脆弱性検出に至った検証プロセスを整理**。
- そして、「X.5 想定される推奨事項」では、**当該脆弱性に対して推奨される対策事項を整理**。

※ Xは章番号を意味する。

2. UTMに関するセキュリティ検証プラクティス

2.4 実証において検出された代表的な脆弱性

脆弱性の概要	想定される影響	脆弱性の検出に至った検証プロセス
古いバージョンのOpenSSHにおける権限昇格の脆弱性	悪用されることで、機器に存在するプログラムが意図しない権限で実行される可能性がある。この結果、UTMの動作が停止し、当該UTMを導入している企業の業務や導入しているシステムの運用が停止するおそれがある。	• Nmapを用いたネットワークスキャンを行い、検証対象機器で公開されているサービス及びバージョンをリストアップする。 • リストアップしたサービス及びバージョンの情報に基づき、既知の脆弱性が公開されていないかをNIST NVDを用いて確認する。 • 既知の脆弱性が公開されていたため、当該脆弱性の再現性（悪用可能性）を確認する。Exploit DB、GitHub、Metasploit等で攻撃実証コードを検索することで、既に公開されている実証コードを用いて脆弱性の悪用可能性を確認する。
Web管理画面におけるOSコマンドインジェクションの脆弱性	悪用されることで、任意のコードが実行される可能性がある。この結果、UTMの動作が停止し、当該UTMを導入している企業の業務や導入しているシステムの運用が停止するおそれがある	• OWASP ZAPのスパイダー機能を用い、検証対象機器のWebサービスにおいてアクセス可能なURL一覧を作成する。 • ファジングの対象とするURLとパラメータのリストを作成する。パラメータリストの作成にあたっては、GitHub等で公開されているペイロードリストを参考にする。 • 作成したパラメータリストに基づき、ファジングを実施する。 • ファズデータに対するWebサービスのレスポンスを踏まえ、脆弱性の有無を判断する。

2.5 想定される推奨事項

脆弱性の概要
• 最新のOpenSSHにバージョンアップする。
• シェルを起動できる言語機能の使用を避ける。 • 引数に対してチェックを行い、あらかじめ許可した処理のみ実行する。