ネットワークデバイスのコラボラティブプロテクションプロファイル／

無線侵入検知／侵入防止システム（WIDS/WIPS）の拡張パッケージ（EP）

バージョン: 1.0

2016 年 10 月 6 日

National Information Assurance Partnership

平成 29 年 9 月 26 日　翻訳　第 1.0 版
独立行政法人情報処理推進機構
技術本部　セキュリティセンター
情報セキュリティ認証室

改訂履歴

バージョン	日付	コメント
1.0	2016 年 10 月 6 日	初版発行　ー　NDcPP の EP

目次

1. 概説

1.1 概要

本拡張パッケージ（EP）は、無線侵入検知／防止システム（WIDS/WIPS）（プライベートネットワークのエッジに設置される IEEE 802.11 ネットワーク侵入防止製品であって、リアルタイムにネットワークトラフィクの収集、検査、分析、及び対応が可能なものと定義される）のセキュリティ要件を記述し、また明確に定義されかつ記述された脅威の低減を目的とした要件の最小限ベースラインセットの提供を意図している。しかし、本 EP は、本 EP 自体で完結するものではなく、ネットワークデバイスのコラボラティブプロテクションプロファイル（NDcPP）を拡張するものである。この概説では、適合する評価対象（TOE）の特徴を記述し、また本 EP が NDcPP との関連において、どのように使用するべきかについて論ずる。

1.2 用語

以下のセクションでは、本プロテクションプロファイルで用いられるコモンクライテリアの用語と技術用語の両方について説明する。

1.2.1 コモンクライテリア用語

コモンクライテリア（CC）	情報技術セキュリティ評価のためのコモンクライテリア。
共通評価方法（CEM）	情報技術セキュリティ評価のための共通評価方法。
拡張パッケージ（EP）	製品種別に特有のセキュリティ要件をカバーするために、ベース PP からの要件を拡張した、ある製品分野に対するセキュリティ要件についての実装に依存しないセット。ここでは、WIDS/WIPS EP は、NDcPP を拡張する。
プロテクションプロファイル（PP）	製品の分野に対するセキュリティ要件についての実装に依存しないセット。
セキュリティ保証要件 （SAR）	TOE のセキュリティを保証するための要件。
セキュリティ機能方針 （SFP）	セキュリティ機能によって実施されるセキュリティ方針。
セキュリティ機能要件（SFR）	TOE によるセキュリティ実施の要件。
セキュリティターゲット（ST）	特定の製品に対するセキュリティ要件についての実装に依存するセット。
評価対象（TOE）	評価される製品。ここでは、無線侵入検知／防止システムとその補足証拠資料。
TOE セキュリティ機能（TSF）	評価される製品のセキュリティ機能。
TOE 要約仕様（TSS）	ST において TOE がどのようにそれらの SFR を満たすかについての記述。

1.2.2 技術用語

無線侵入検知／防止システム（WIDS/WIPS）	ネットワークセキュリティ管理者に、悪意のある可能性のある無線ネットワークトラフィク（IEEE 802.11）をリアルタイムに監視、収集、ログ記録し、対抗措置を講じる能力を提供するセキュリティ製品。

1.3 適合主張

適合ステートメント

本 EP は、情報技術セキュリティ評価のためのコモンクライテリア、バージョン 3.1、改訂第 4 版に適合する。[CC]

本 EP に適合するため、ST は、[CC]パート 1(ASE_CCL)で定義された正確適合（Strict Conformance）のサブセットである、完全適合（Exact Conformance）を論証しなければならない。この ST には、以下のような本 PP のすべてのコンポーネントが含まれなければならない:

- 必須のもの（常に要求される）
- 選択ベースのもの（必須の要件で特定の選択肢が選択されるときに要求される)

また、以下のようなコンポーネントが含まれてもよい:

- オプション
- オブジェクティブ（訳注：現在は、必須ではないが、将来的に必須となる可能性のある機能要件を言う。）

必須の要件は、本書の本文で説明される、一方附属書には、選択ベース要件、オプション要件、及びオブジェクティブ要件が含まれる。この ST では、これらのコンポーネントのいずれについても繰り返してよいが、本 EP や NDcPP（本 EP が拡張するもの）で定義されていない追加のコンポーネント（例、CC パート 2 または 3）を含んではならない。

CC 適合主張

本 EP は、コモンクライテリア バージョン 3.1 改訂第 4 版[CC]のパート 2（拡張）及びパート 3（適合）に適合する。

PP 主張

本 EP は、いかなるプロテクションプロファイルへの適合も主張しない。本 EP は、NDcPP を拡張する、それは、本 EP によって拡張される「ベース」機能のセットを提供するための NDcPP に依拠することを意味する。しかし、これは EP 自体がこの PP に適合していることを意味するものではない。

パッケージ主張

本 EP は、いかなるパッケージへの適合も主張しない。

1.4 本拡張パッケージの使用方法

NDcPP の EP として、本 EP とベース PP の双方の内容は、それぞれの製品特有のセキュリティターゲットの中で適切に組み合わされることが期待される。本 EP は、困難さやあいまいさが一切無いべきであり、具体的に定義されている。ST は、その適合主張で、NDcPP（現在のバージョンについては http://www.niap-ccevs.org/pp/を参照）及び本 EP の適用可能なバージョンを識別しなければならない。

1.5 適合する評価対象

本 EP は、無線侵入検知／防止システム（WIDS/WIPS）に特に対応する。適合 WIDS/WIPS は、ネットワークセキュリティ管理者に悪意のある可能性のあるネットワークトラフィクをリアルタイムで監視、収集、ログ記録、対応できる能力を提供する製品である。WIDS は、通常、IEEE 802.11 トラフィクの WLAN 無線周波数スペクトラムの周辺 RF 環境を受動的にスキャンするような複数のセンサ、及びセンサによって収集されたデータを処理するサーバまたはコントローラのような、集中化メカニズムにより構成される。WIDS/WIPS は、ベンダの実装に応じて、組込型（WLAN インフラの一部）またはオーバーレイ（WLAN から独立した）アーキテクチャを利用可能である。

本 EP は、WIDS/WIPS が監視するトラフィクが、IEEE802.11a、b、g、n、及び ac によって利用される RF スペクト

ラムの無線フレームであるので、OSI ネットワークモデルのレイヤ１とレイヤ２の検査に焦点を絞っている。他の技術（例、携帯電話）及びプロトコルについての要件は、オプションである。

適合 TOE は、さまざまなアプローチを用いて悪意のある可能性のあるネットワークトラフィクを検出する。広義の、トラフィク分析は、「既知」の脅威、または「未知」の脅威の識別に基づいて行うことが可能である。「既知」の脅威の識別は、パタンマッチングによって、例えば、 フレーム内の文字列のマッチング、または偵察やサービス拒否（DoS）攻撃に共通するトラフィクパタンのマッチングによって、行うことができる。「未知」の脅威の識別は、さまざまな形態の「異常」検出の利用を通して実行されるかもしれない、これにより WIDS/WIPS が、「異常」な（予期しない／非定型の）トラフィクパタンを検出し、対応できるように、「予期される／定型の」トラフィクパタンの定義と共に提供される（または「学習する」／作成する）。

以下は、評価の一部であるべきである:

- WIDS/WIPS により提供される、監視、検出及び報告の機能
- 位置追跡
- WIDS/WIPS コンポーネント間のセキュアな通信経路の利用
- WIDS/WIPS 管理と事象監視のためのセキュアな通信経路の利用
- 外部コンポーネント（例、データベースとログサーバ）とのセキュアな通信経路の利用

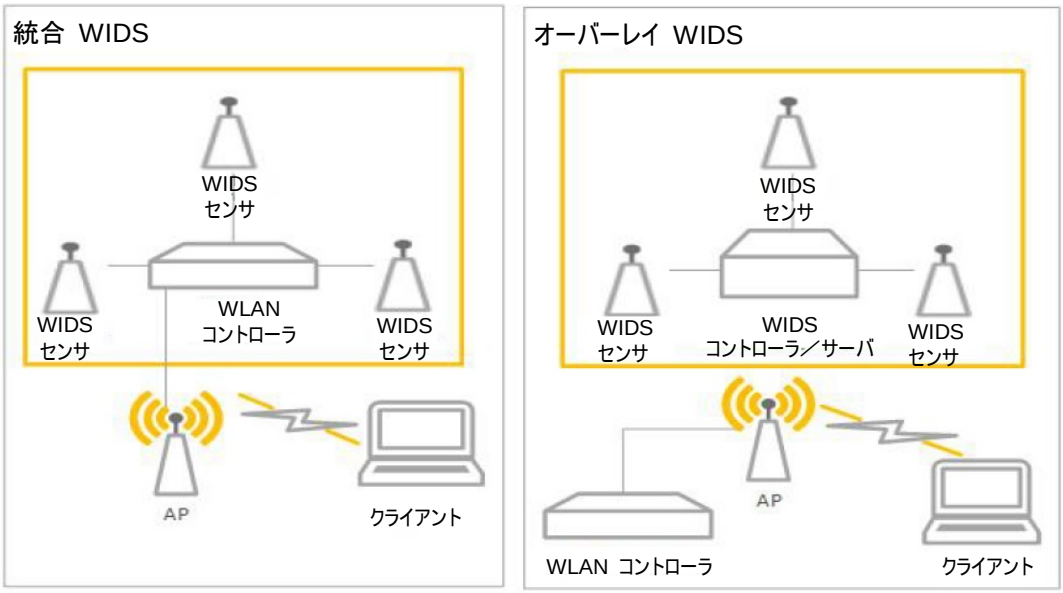

図 1: 一般的な TOE

2. セキュリティ課題定義

WIDS/WIPS は、悪意のある可能性のある WLAN トラフィクの検出と、それらのトラフィクへの対応に関連した一連のセキュリティ脅威に対処する。悪意のあるトラフィクは、監視対象ネットワーク上の 1 個以上の端点やネットワークインフラや TOE 自体への脅威をもたらすかもしれない。WLAN に対する攻撃は、正当な利用者へ WLAN の可用性と同様に、WLAN の利用者データとシステムデータの機密性と完全性を危殆化するかもしれない。

「監視対象ネットワーク」という用語は、ここでは TOE が侵入を監視、検出するように構成されている WLAN 及び／または有線ネットワークを表すために使用される。これは、無線ネットワーク上の侵入が有線インフラに損害を与える可能性があるので、有線ネットワークへ拡張する。WIDS/WIPS は、有線ネットワークを暴露するかもしれないような、有線インフラへ直接接続される不正なデバイス、または無線でないゾーンに配置される許可されない WLAN デバイスを検出することによって有線インフラについても保護する。「Wi-Fi」、「Wi-Fi ネットワーク」、「WLAN」という用語は、IEEE 802.11 ネットワークを表すために同じ意味で利用される。

WIDS/WIPS の適切なインストール、構成、管理は、その正常な動作に重要である。サイトは、自身のリスク分析と認識される脅威に関連して、サイトのセキュリティ方針を実施し、そのニーズを満たす適切な対応を提供するような、セキュリティ方針と規則の設定に責任を負う。

本 EP では、NDcPP で識別された脅威を繰り返さないが、それらはすべて所与の適合に適用される、ゆえに本 EP は NDcPP に依存することに留意されたい。また、NDcPP には、TOE のセキュリティ機能を提供する能力に対する脅威のみが含まれるが、本 EP は、運用環境の資源に対する脅威のみに対処することにも留意されたい。NDcPP の脅威と本 EP で定義される脅威は共に、WIDS/WIPS の TOE によって対処されるセキュリティの脅威の包括的なセットを定義する。

2.1 脅威

T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION

保護される WLAN 上の機微な情報は、暗号化されない機微な情報の送信のような、方針の侵害で暴露／送信された情報からの結果として暴露される可能性がある。WIDS/WIPS は、許可されない情報の暴露を検出するため、WLAN データの収集及び解析ができる。

T.UNAUTHORIZED_ACCESS

攻撃者は、許可されている AP になりすますことによって許可されていない AP へ接続するための EUD を取得して、1 つ以上のネットワーク、端点またはサービスへの不適切なアクセス取得を試行するかもしれない。悪意のある外部 AP や EUD が、保護された WLAN 上の AP や EUD と通信できる場合、それらのデバイスは、許可されない情報の暴露についての影響を受けるかもしれない。

T.DISRUPTION

WLAN インフラに対する攻撃は、保護された WLAN 内でサービス拒否（DoS）をもたらす可能性がある。無線 DoS は 2 つの方法で発生するかもしれない：RF 妨害を通して物理層において、またはパケット注入を通してデータリンク層において。

2.2 前提条件

A.CONNECTIONS

TOE は、TOE セキュリティ方針が、接続されたネットワーク間を流れるすべての適用可能なネットワークトラフィク上で実施されることを保証するやり方で、別個のネットワークに接続される。

A.PROPER_ADMIN

WIDS/WIPS の管理者は、不注意ではなく、意図的に怠慢ではなく、または敵対的ではなく、適用される企業のセキュリティ方針に従って WIDS/WIPS を管理する。

2.3 組織のセキュリティ方針

TOE を配備する組織は、主張するベース PP によって定義されたすべての組織のセキュリティ方針に加えて、以下に列挙される組織のセキュリティ方針を満たすと期待される。

P.ANALYZE

侵入の可能性についての結論を導出するための分析プロセス及び情報は、WIDS/WIPS データに適用されなければならず、適切な対応アクションを講じなければならない。

3. セキュリティ対策方針

3.1 TOE のセキュリティ対策方針

O.SYSTEM_MONITORING

ネットワーク方針の侵害の可能性を分析し、対応可能とするために、WIDS/WIPS は、監視対象ネットワーク上のネットワークトラフィクの基本データエレメントを収集し、格納できなければならない。

以下によって対処される：FAU_GEN.1/WIDS、FAU_STG_EXT.1/PCAP

O.WIDS_ANALYZE

WIDS/WIPS は、承認された WLAN 方針に対する侵害の可能性、内部 WLAN デバイスを含む許可されない接続、及び、セキュアでない通信を識別するため、監視対象ネットワーク上で収集または観測された WLAN アクティビティを分析できなければならない。

以下によって対処される：FAU_ARP.1、 FAU_ARP_EXT.2、FAU_IDS_EXT.1、FAU_INV_EXT.1、FAU_INV_EXT.2、FAU_INV_EXT.3、FAU_SAA.1、FAU_WID_EXT.1、FAU_WID_EXT.2、FAU_WID_EXT.3、FAU_WID_EXT.4、FAU_WID_EXT.5、FDP_IFC.1、FAU_ANO_EXT.1、FAU_INV_EXT.4、FAU_INV_EXT.4/CELL、FAU_INV_EXT.5、FAU_MAC_EXT.1、FAU_SIG_EXT.1、FAU_WID_EXT.6、FAU_WID_EXT.7

O.WIPS_REACT

TOE は、管理者定義の WIPS 方針を侵害すると決定されている WLAN デバイスを隔離／収容するため、管理者によって設定されたとおり、対応できなければならない。

以下によって対処される：FAU_WIP_EXT.1

O.TOE_ADMINISTRATION

ベース PP で定義される許可されない管理者アクセスの脅威に対処するため、適合 TOE は、管理者が TOE の WIDS/WIPS 機能を構成するために必要な機能を提供する。

以下によって対処される：FMT_SMF.1/WIDS

O.INSECURE_OPERATIONS

TOE のハードウェアの故障、または TOE のソフトウェアの完全性が危殆化するような場合があるかもしれない、後者には悪意のある場合と悪意の意図がない場合がある。TOE のハードウェアやソフトウェア仕様外で、TOE が運用される懸念に対処するため、TOE は、自己テストメカニズムを介して報告される問題の発見に際してシャットダウンする。

以下によって対処される：FPT_FLS.1

O.TRUSTED_COMMUNICATIONS

ベース PP で定義される信頼されない通信チャネルの脅威に対してさらに対処するため、適合 TOE は、もし存在する場合、分散型コンポーネント間での高信頼通信を提供する。

以下によって対処される：FPT_ITT.1、FTP_ITC.1

3.2 運用環境のセキュリティ対策方針

以下の運用環境のセキュリティ対策方針は、TOE がそのセキュリティ機能を正しく提供することを支援する。これらは、環境についての前提条件と対応する。

OE.CONNECTIONS

TOE 管理者は、監視対象ネットワークのネットワークトラフィク上に、その方針を TOE が効果的に実施できるようなやり方で TOE が設置されることを保証する。

OE.PROPER_ADMIN

WIDS/WIPS の管理者は、不注意ではなく、意図的に怠慢ではなく、または敵対的ではない、かつ適用される企業のセキュリティ方針に従って WIDS/WIPS を管理する。

3.3 セキュリティ対策方針の根拠

本セクションでは、前提条件、脅威、及び組織のセキュリティ方針がどのようにセキュリティ対策方針と対応付けられるのかについて説明する。

脅威、前提条件または OSP	セキュリティ対策方針	根拠
T.UNAUTHORIZED_DISCLOSURE_OF_INFORMATION	O.SYSTEM_MONITORING, O.WIDS_ANALYZE, O.WIPS_REACT	脅威 T.Unauthorized_Disclosure_of_Information は、ネットワーク侵害の検出を可能にする、ネットワークへの可視性を提供する O.SYSTEM_MONITORING によって対抗される。 脅威 T.Unauthorized_Disclosure_of_Information は、承認されたネットワーク用途への侵害の可能性の検出を提供する O.WIDS_ANALYZE によって対抗される。 脅威 T.Unauthorized_Disclosure_of_Information は、許可されていない AP 及び EUD の抑制を提供する O.WIPS_REACT によって対抗される。
T.UNAUTHORIZED_ACCESS	O.SYSTEM_MONITORING, O.WIDS_ANALYZE, O.WIPS_REACT, O.TOE_ADMINISTRATION	脅威 T.UNAUTHORIZED_ACCESS は、許可されていない AP 及び EUD の検出を可能にする、ネットワークへの可視性を提供する O.SYSTEM_MONITORING によって対抗される。 脅威 T.UNAUTHORIZED_ACCESS は、承認されたネットワーク用途への侵害の可能性の検出を提供する O.WIDS_ANALYZE によって対抗される。 脅威 T.UNAUTHORIZED_ACCESS は、許可されていない AP 及び EUD の抑制を提供する O.WIPS_REACT によって対抗される。 脅威 T.UNAUTHORIZED_ACCESS は、O.TOE_ADMINISTRATION によって対抗される。

脅威、前提条件または OSP	セキュリティ対策方針	根拠
T.DISRUPTION	O.SYSTEM_MONITORING, O.WIDS_ANALYZE, O.WIPS_REACT	脅威 T.DISRUPTION は、DoS 攻撃の検出を可能にする、ネットワークへの可視性を提供する O.SYSTEM_MONITORING によって対抗される。 脅威 T.DISRUPTION は、承認されたネットワーク用途への侵害の可能性の検出を提供する O.WIDS_ANALYZE によって対抗される。 脅威 T.DISRUPTION は、許可されていない AP 及び EUD の抑制を提供する O.WIPS_REACT によって対抗される。
A.CONNECTIONS	OE.CONNECTIONS	運用環境の対策方針 OE.CONNECTIONS は、A.CONNECTIONS によって実現される。
A.PROPER_ADMIN	OE.PROPER_ADMIN	運用環境の対策方針 OE.PROPER_ADMIN は、A.PROPER ADMIN によって実現される。
P.ANALYZE	O.WINDS_ANALYZE	組織のセキュリティ方針 P.ANALYZE は、O.WIDS_ANALYZE によって促進される。

4. セキュリティ要件

本章では、WIDS/WIPS によって満たされなければならないセキュリティ要件を記述する。これらの要件は、[CC]のパート 2 からの機能コンポーネントと、パート 3 からの保証コンポーネントによって構成される。以下の表記法が用いられる:

- **詳細化**操作(**太字テキスト**によって示される):要件に詳細を付け加え、さらに要件を制約するために用いられる。
- **選択**(*イタリック体テキスト*によって示される):要件を述べる際に、[CC]によって提供される 1 つ以上のオプションを選択するために用いられる。
- **割付**操作(*イタリック体テキスト*によって示される):パスワードの長さのような、指定されていないパラメタへ具体的な値を割り付けるために用いられる。角括弧内に表す値は割付を示す。
- **繰り返し**操作:括弧内の数字で特定される (例、「(1)」)

4.1 セキュリティ機能要件

本セクションに含まれるセキュリティ機能要件は、情報技術セキュリティ評価のためのコモンクライテリアバージョン 3.1 改訂第 4 版のパート 2 から導出されたものに、拡張機能コンポーネントを追加したものである。

4.1.1 セキュリティ監査

FAU_ARP.1 セキュリティ警報

FAU_ARP.1.1 TSF は、セキュリティ侵害の可能性が検出された場合、*[次のアクション: 含まれている AP と EUD の識別情報、警報の記述、及び深刻度を示すために十分な詳細度で許可された管理者に警報を表示する*、[**選択**: *侵害を引き起こす生のフレームトラフィックをキャプチャする、その他のアクションなし*]]を実行しなければならない。

適用上の注釈: 侵害を引き起こす生のフレームをキャプチャすることは、オブジェクティブ要件である。ST 作成者が侵害を引き起こすような生フレームのキャプチャを選択する場合、ST 作成者は、次の SFR を含めなければならない:
FAU_STG_EXT.1.1/PCAP、FAU_STG_EXT.1.2/PCAP、
FAU_STG_EXT.1.3/PCAP。

保証アクティビティ

TSS

評価者は、管理者コンソール／インタフェース上で WIDS/WIPS 警報がどこで判るかについて、TSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、生成された警報が WIDS/WIPS インタフェース内のどこで表示されるかに関する指示について操作ガイダンスを利用しなければならない。警報を引き起こす生のフレームをキャプチャするためのオブジェクティブ要件が選択される場合、評価者は、対応する選択ベースの要件についてもテストしなければならない。評価者は、トラフィクキャプチャ機能を構成するために、操作ガイダンスを利用しなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

- ***テスト 1:*** *評価者は、一連の事象を実行するか、または警報を正常に引き起こすようなトラフィクを生成しなければならない。評価者は、TOE が警報を生成したかどうかを検証し、記録するべきである。評価者は、また、発生した事象やトラフィク、及び、どの警報が引き起こされようとしたかについても記録し、その警報で TOE によって提供された詳細情報を記録するべきである。*
- ***テスト 2:*** *生のフレームのキャプチャが選択された場合、パケットキャプチャが起動し、適切に保存されたことを検証する。*

FAU_ARP_EXT.2 セキュリティ警報フィルタリング

FAU_ARP_EXT.2.1 TSF は、警報の生成を選択的に排除するため[**割付**: *選択の方法*]を適用する能力を提供しなければならない。

保証アクティビティ

TSS

評価者は、WIDS/WIPS 警報を送信するための TOE の能力について TSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、警報を有効化または無効化するための指示が操作ガイダンスに含まれていることを検証しなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

- ***テスト 1:***
  - *評価者は、WIDS/WIPS 管理者インタフェースを通して利用可能な検出能力の検出を有効化／無効化するため、操作ガイダンスを利用しなければならない。評価者は、次に警報を正常に起動するようなトラフィクを生成しなければならない。評価者は、TOE が警報を生成したことを検証しなければならない。評価者は、生成された攻撃／侵入を記録しなければならず、警報について WIDS により提供された詳細情報と同様に、どの警報が引き起こされたかを示さなければならない。*
  - *評価者は、警報を無効化しなければならない。次に、評価者は、警報を正常に引き起こすべきであるような、以前のテストと同様に、事象を生成しなければならない。評価者は、TOE が攻撃に対する警報を生成したか、及び所見を記録するかどうかをチェックするべきである。*

FAU_IDS_EXT.1 侵入検知システム – 侵入検知方法

FAU_IDS_EXT.1.1 TSF は、侵入検知の次の方法：[**選択**：*異常ベース、シグネチャベース、ふるまいベース、ハイブリッド、[**割付**：ベンダ独自の検出方法]*]を提供しなければならない。

適用上の注釈: 少なくとも 1 つの検出方法が本 SFR でなされた選択に基づいて選択されなければならない、次の SFR についても含まれなければならない：
異常ベース検出が選択された場合：FAU_ANO_EXT.1.1 及び FAU_ANO_EXT.1.2
シグネチャベース検出が選択された場合： FAU_SIG_EXT.1.1

ハイブリッド検出方法は、2 つ以上の検出方法（例、異常ベースとシグネチャベースの両方、またはシグネチャベースと別の方法）の組み合わせたものである。ハイブリッドソリューションにおける検出方法の一つに、異常ベースまたはシグネチャベース検出法のいずれかが含まれる場合、対応する選択ベース要件についても満たさなければならない。

保証アクティビティ

TSS

評価者は、どの侵入検知手法をTOE が利用するかについてのガイダンスがTSS に含まれることを検証しなければならない。ハイブリッド侵入検知が侵入検知方法として選択される場合、TSS は利用される検出手法の詳細情報を提供するべきである。
さらに、異常ベースまたはシグネチャベース以外の検出方法を含むようなハイブリッド検出方法を利用するとき、TSS には、このような検出方法についてのより詳細な情報が含まれなければならない。ベンダ独自の検出方法が選択される場合、その方法についての技術的な詳細情報が提供されなければならない。

ガイダンス

評価者は、このような侵入を検出するために、TOE の構成方法についての指示を操作ガイダンスが提供していることを検証しなければならない。

テスト

TOE によって利用される検出手法に応じて、評価者は、利用される検出手法に留意し、適切な選択ベース要件についてテストしなければならない。

FAU_INV_EXT.1 環境インベントリ

FAU_INV_EXT.1.1 TSF は、[*EUD MAC アドレス、AP MAC アドレス*]に基づいて[*許可された AP とEUD*]のインベントリを定義する能力を許可された管理者に提供しなければならない。

適用上の注釈: 本インベントリは、APとEUDが無線ネットワークの承認されたメンバーであるような WIDS/WIPS へ示すホワイトリストとして利用される。インベントリ収集された、またはホワイトリストに登録されたデバイスについての記述に利用される用語は、ベンダ製品によって異なるかもしれない。本 EP は、インベントリの一部であるような AP と EUD を記述するため、「ホワイトリスト上の」と「ホワイトリスト上にない」を利用する。

保証アクティビティ

TSS

評価者は、許可されたAP 及びEUD のインベントリを定義する目的で、TOE の能力に関する情報を含むことを検証するためにTSS をレビューしなければならない。

ガイダンス

評価者は、APとEUD がホワイトリストの一部であることを示すために、APとEUD の分類の構成と変更の方法に関して、操作ガイダンスをレビューしなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

許可されたデバイスとして分類されるべきであるAP 及びEUD を配置する。

- ***テスト 1:** ホワイトリストが自動的に構成される場合:*
  - *ホワイトリスト上のデバイスのリストをチェックし、リストが正確であることをチェックする。*
  - *デバイスがホワイトリスト上にある、として分類されていることを検証する。*
  - *インベントリからデバイスを削除するか、再分類する。*
  - *削除または再分類後、デバイスがホワイトリスト上にある、と表示されていないことを検証する*
- ***テスト 2:** 許可されたデバイスのセットが手動で構成される場合:*
  - *APとEUD をリストに追加する。APとEUD がインベントリ上に表示されるかどうかを記録する。*
  - *ホワイトリスト上のデバイスのリストにデバイスがホワイトリストに登録されていることを検証する。*
  - *インベントリからAP を削除する。*
  - *削除後、削除されたデバイスがインベントリに表示されないことを検証する。*

FAU_INV_EXT.1.2 TSF は、定義されたインベントリの一部である運用環境内の [*EUD*、*AP*]のプレゼンスと最新情報を検出しなければならない。

適用上の注釈: TSF によって検出されるべきである現在の情報を参照するとき、TSF は、動作チャネルと帯域、AP の SSID、AP に接続されたクライアント、及び EUD が接続されている AP 等、WIDS/WIPS により観測された、検出された AP や EUD についての情報を参照している。FAU_INV_EXT.2.3 には、WIDS/WIPS によって検出されるべき AP や EUD について詳細情報の完全なリストがある。

保証アクティビティ

TSS

評価者は、許可された EUD と AP のプレゼンスが TOE によってどのように提示され、そのデバイスについてどのような情報が提供されるかについて、TSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、TOE センサの範囲内にある許可された AP と EUD の表示方法に関する指示について、操作ガイダンスが提供していることを検証しなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

- ***テスト 1**:ホワイトリスト上の AP と EUD を配置し、EUD を AP へ接続する。*
- ***テスト 2:**検出された AP と EUD のリストに、ホワイトリストに登録されており、配置されたばかりの AP と EUD が表示されていることを検証する。*
- ***テスト 3:**AP と EUD が検出されている場合は、それらのデバイスがホワイトリスト上のデバイスとして分類されていることを検証する。*

FAU_INV_EXT.1.3 TSF は、定義されたインベントリの一部である運用環境内の *[EUD、AP]*のプレゼンスと最新情報を検出しなければならない。

適用上の注釈: TSF によって検出されるべき現在の情報を参照するとき、TSF は、動作チャネルと帯域、AP の SSID、AP に接続されたクライアント、及び EUD が接続された AP 等、WIDS/WIPS により観測された、検出された AP や EUD について情報を参照している。FAU_INV_EXT.2.3 には、WIDS/WIPS によって検出されるべき AP や EUD についての詳細情報の完全なリストがある。

保証アクティビティ

TSS

評価者は、TOE によって許可された EUD と AP のプレゼンスがどのように表示され、どのようなデバイスに関する情報が提供されるかについて、TSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、検出された AP と EUD のリストが表示される WIDS/WIPS インタフェースの場所が TSS に含まれていることを検証しなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

- ***テスト1**: ホワイトリスト上にない AP とEUD を配置し、EUD をAP へ接続する。*
- ***テスト2:** 検出されたAP とEUD のリストに、配置されたばかりのホワイトリスト上にないAP とEUD が含まれることを検証する。*
- ***テスト 3:**AP と EUD が検出される場合は、それらがホワイトリスト上のデバイスとして分類されないとを検証する。*

FAU_INV_EXT.2 環境オブジェクトの特徴

FAU_INV_EXT.2.1 TSF は、[*TOE の無線センサの範囲*]内の[*インベントリ収集された悪意のある EUD、AP*]の現在の物理的な位置に関する情報を検出しなければならない。

適用上の注釈: 本 SFR は、AP や EUD の位置を地図上に配置するか、AP や EUD のセンサからの距離を提供するかのいずれかによって、AP と EUD の位置を追跡する能力をチェックするのみであるが、一定の精度を義務付けない。オブジェクティブ要件 FAU_INV_EXT.4 は、位置追跡能力の正確性に関してより厳格である。

保証アクティビティ

TSS

評価者は、要求されるレベルの正確性を満たすため、位置追跡、センサの最適な数、センサ配置について情報がTSS に含まれていることを検証しなければならない。

ガイダンス

評価者は、位置追跡を設定する方法及びAP とEUD 位置情報がTSF 管理者インタフェースのどこで閲覧可能かに関する指示について操作ガイダンスをレビューしなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

- ***テスト 1:***
  - ***ステップ1:** センサの範囲内にAP を配置する。*
  - ***ステップ2:** TSF がAP 上で位置情報を提供できること検証する。*
  - ***ステップ3**: TSF によって提示される位置がセンサの範囲内であることを検証する。*

FAU_INV_EXT.2.2 TSF は、[*TOE の無線センサの範囲*]内で動作中のハードウェアの[*受信信号強度*、[**選択**: *所定のしきい値を超える RF 電力レベル、他の特性なし*]]を検出しなければならない。

保証アクティビティ

TSS

評価者は、センサの範囲内で動作中のハードウェアの信号強度を記録するTSF の能力に関する情報がTSS に含まれていることを検証しなければならない。

ガイダンス

所定のしきい値を超える RF 電力レベルを検出するためのオプションが選択される場合、評価者は、所与のテストにおいてどのようなしきい値であるかをセットまたはチェックするため、操作ガイダンスを利用しなければならない。また、評価者は、しきい値を超えたときに警報を生成するように TOE を設定する方法についての指示を操作ガイダンスが提供することも検証するべきである。

テスト

評価者は、以下のテストを実行しなければならない:

- ***テスト 1:***
  - ***ステップ 1:*** *センサの範囲内に AP を配置する。*
  - ***ステップ 2:*** *検出された AP とEUD のリストについて、WIDS/WIPS ユーザインタフェースをチェックする。*
  - ***ステップ 3****: 現在受信中の信号強度が、AP とEUD に関する WIDS/WIPS ユーザインタフェースに表示される情報の一部であることを検証する。*

FAU_INV_EXT.2.3 TSF は、*現在の RF 帯域、現在のチャネル、MAC アドレス、AP と EUD の分類、TOE の無線センサの範囲内にある[すべての AP とEUD]*の[**割付**: *その他の詳細情報*]を検出しなければならない。[*AP*]について、TOE は、以下の追加の詳細情報を検出しなければならない: *暗号化、接続された EUD の数*。[*EUD*]について、TOE は、以下の追加の詳細情報を検出しなければならない: *それが接続されたAP のSSID とBSSID*。

適用上の注釈: 暗号化種別の検出のために、TSF は、暗号化なし、WEP、TKIP 及び AES を区別できるべきである。

保証アクティビティ

TSS

評価者は、TOE の無線の範囲内に現在のRF 帯域、現在のチャネル、MAC アドレス、AP とEUD の種別を検出する能力について、TSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、上記のデバイスのインベントリを置く方法を示すような指示があることを検証するため、操作ガイダンスをレビューしなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

- ***テスト 1:***
  - ***ステップ 1:*** *ホワイトリスト上の AP、ホワイトリスト上にない AP、2つのホワイトリスト上の EUD を配置する。*
  - ***ステップ 2:*** *1 つのホワイトリスト上の EUD をホワイトリスト上の AP へ接続し、1 つのホワイトリスト上の EUD をホワイトリスト上にない AP へ接続する。*
  - ***ステップ 3:*** *検出された AP と EUD のリストについて、WIDS/WIPS ユーザインタフェースをチェックする。*
  - ***ステップ 4****: 現在の RF 帯域、現在のチャネル、MAC アドレス、デバイスの種別が、検出されたすべての AP と EUD の WIDS/WIPS ユーザインタフェースに表示される情報の一部であることを検証する。*

FAU_INV_EXT.3 環境オブジェクトのふるまい

FAU_INV_EXT.3.1 TSF は、[*インベントリ収集された EUD*]が以下のふるまいを示すときを検出しなければならない。

- *EUD が、他の EUD とのピアツーピア接続を確立する。*
- *[**選択**: EUD が 2 つのネットワークインタフェースをブリッジする。]*
- *[**選択**: EUD がインターネット接続の共有を使用する。]*
- *[**選択**: その他の接続種別、その他の接続なし。]*

適用上の注釈:本要件について、ブリッジやピアツーピア接続の異なる種別の検出のための警報を生成するとき、WIDS/WIPS がブリッジやピアツーピア接続について一般名称を使用することは受け入れ可能である。接続の具体的な種別は、特定のものである必要はない。

保証アクティビティ

TSS

評価者は、SFR によって記述されたネットワークのふるまいを TOE が検出する能力について TSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、各警報の形式に関する情報ばかりでなく、警報がどのように管理者に表示されるかを提供することを検証するため、操作ガイダンスをレビューしなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

- ***テスト 1:***

  ホワイトリスト上の 2 台の EUD 間に以下の接続を作成する。
  - *Windows アドホック接続*
  - *Mac OS アドホック*
  - *Linux アドホック*

- *Wi-Fi ダイレクト*

- ***テスト 2:***

  1つのホワイトリスト上の EUD と1つのホワイトリスト上にない EUD の間で次の接続を作成する

  - *Windows アドホック接続*
  - *Mac OS アドホック*
  - *Linux アドホック*
  - *Wi-Fi ダイレクト*
- ***テスト 3:*** *(オプション) 1つのホワイトリスト上の EUD 上の 2 つのネットワークインタフェースをブリッジする(一方はホワイトリスト上として列挙された無線カードでなければならない)。*
- ***テスト4:***
  - *ホワイトリスト上の EUD を用いる Windows ホステッドネットワークを作成する。*
  - *異なるホワイトリスト上の EUD をネットワークへ接続する。*

各テストの接続のそれぞれによって警報が生成されたことを検証する。警報の説明を提供する。

FAU_SAA.1 侵害の可能性の分析

FAU_SAA.1.1 TSF は、**無線トラフィク**の監視に規則のセットを適用できなければならず、これらの規則に基づいて潜在的な**悪意のあるアクション**を示すことができなければならない。

保証アクティビティ

TSS

本 SFR には、TSS 保証アクティビティはない。

ガイダンス

本 SFR には、操作ガイダンスアクティビティはない。

テスト

本 SFR のためのテストはない。潜在的な悪意のある事象のテストは、他の SFR での侵入を検出する能力を通してテストされる。

FAU_SAA.1.2 TSF は、無線トラフィクの監視のための以下の規則を実施しなければならない:

a. 潜在的なセキュリティ侵害を示すものとして知られている[割付:定義された監査対象事象のサブセット]の集積や組み合わせ;
b. [*下記の表 1 で定義された他の潜在的なセキュリティ侵害*]。

SFR	**セキュリティ侵害の可能性**
FAU_INV_EXT.3	他の EUD とのピアツーピア接続を確立する許可された EUD の検出。
FAU_INV_EXT.3	2 つのネットワークインタフェースをブリッジする EUD の検出。
FAU_WID_EXT.1	不正 AP の検出。
FAU_WID_EXT.1	悪意のある EUD の検出。
FAU_WID_EXT.2	過剰な送信電力レベルのトラフィクの検出。
FAU_WID_EXT.2	アクティブプロービングの検出。
FAU_WID_EXT.2	MAC 詐称の検出。
FAU_WID_EXT.3	RF ベースのサービス拒否の検出。
FAU_WID_EXT.3	deauthentication flood の検出。
FAU_WID_EXT.3	disassociation flood の検出。
FAU_WID_EXT.3	送信要求／送信可の乱用の検出。
FAU_WID_EXT.4	許可されていない認証方式の使用の検出。
FAU_WID_EXT.5	許可されていない暗号化方式の使用の検出。
FAU_WID_EXT.5	暗号化されていないトラフィクの検出。

表 1:セキュリティ侵害の可能性

保証アクティビティ

TSS

本 SFR には、TSS 保証アクティビティはない。

ガイダンス

本 SFR には、操作ガイダンスアクティビティはない。

テスト

本 SFR のテストはなく、他の SFR での侵入を検知するための能力を通して監視機能がテストされている。

FAU_WID_EXT.1 無線侵入検知 – 悪意のある環境オブジェクト

FAU_WID_EXT.1.1　TSF は、以下の種別の悪意のある環境オブジェクト[*不正な AP*]を検出するため[**割付**: *利用者定義された、自動化された*] 分類規則を適用しなければならない。

保証アクティビティ

TSS

評価者は、不正な AP が検出可能な方法、及びこのふるまいが設定可能かどうかについて TSF に記述されていることを検証しなければならない。

ガイダンス

評価者は、サポートされる場合、利用者定義された分類規則の設定方法に関する指示について、操作ガイダンスをレビューしなければならない。

テスト

評価者は、AP 分類規則を設定しなければならず、次に以下のテストを実行しなければならない:

- ***テスト 1:***
  - *利用者定義された分類規則に従って、AP を配置する。*
  - *AP が正しく分類されることを検証する。*

FAU_WID_EXT.1.2　TSF は、*[自動検出メトリック]*に基づいて、良意の及び悪意の[*AP*、*EUD*]を区別しなければならない。

保証アクティビティ

TSS

本 SFR には、TSS 保証アクティビティはない。

ガイダンス

本 SFR には、操作ガイダンスアクティビティはない。

テスト

評価者は、以下のテストを実行しなければならない:

- ***テスト 1:***
  - *ホワイトリスト上にない AP を WIDS センサの領域に配置するが、ネットワークに対する一切のアクションを取らない。*
  - *ホワイトリスト上にない AP を WIDS センサの領域に配置し、内部の有線インフラへそれを接続する(オーバーレイ WIDS についてはオプション)。*
  - *ホワイトリスト上の EUD をホワイトリスト上にない AP へ接続する。*
  - *ホワイトリスト上にない EUD をホワイトリスト上の AP へ接続する。*
  - *許可されない EUD を用いて、許可された AP に対して攻撃を仕掛ける。*

上記の各ステップについて、TSF が AP と EUD を検出し、それらが適切に分類され

ることを検証する。

FAU_WID_EXT.2 無線侵入検知 – パッシブ情報フローモニタリング

FAU_WID_EXT.2.1 TSF は、以下の RF 周波数：2.4 GHz 及び 4.9/5.0GHz [**選択**：*規制ドメイン外のチャネル、非標準のチャネル周波数、他のドメインなし*]におけるすべてのチャネルについて、*[802.11 監視 SFP]* に合致するネットワークトラフィクを監視し、分析し、[**選択**：*同時に監視及び分析を実行、他のふるまいなし]* しなければならない。

適用上の注釈：「802.11 監視 SFP」はセキュリティ機能方針であり、この方針を参照する SFR には、方針が行う内容が記述される。「802.11 監視 SFP」は、FDP_IFC.1.1 で確立され、FAU_WID_EXT の SFR を通して定義される。ベンダは、この方針を形式的に定義する必要はなく、SFR に適合することのみが必要となる。

保証アクティビティ

TSS

評価者は、TSF が検出可能なチャネルに関する情報について TSS に含まれていることを検証しなければならない。

ガイダンス

評価者は、TSF が監視できるチャネルの操作ガイダンスと SFR で選択されたとおりチャネルを監視するよう TSF を設定する方法について、レビューしなければならない。ベンダによって実装されたチャネル滞在時間によっては、デバイスの検出に時間がかかることがある。

テスト

評価者は、以下のテストを実行しなければならない：

- ***テスト 1:*** *5GHz 帯のチャネル*
  - ***ステップ 1:*** *SFR で選択されたとおりチャネルを監視するように TSF を設定する。*
  - ***ステップ 2:*** *5GHz 帯の規制ドメイン内の少なくとも 2 つの異なるチャネル上に AP を配置する。*
  - ***ステップ 3:*** *5GHz 帯の規制ドメイン外の少なくとも 2 つの異なるチャネル上に AP を配置する。*
  - ***ステップ 4:*** *テストされる各チャネル上で AP が検出されることを検証する。*
- ***テスト 2:*** *2.4GHz 帯のチャネル*
  - ***ステップ 1:*** *SFR で選択されたとおりチャネルを監視するように TSF を設定する。*
  - ***ステップ 2:*** *2.4GHz 帯の規制ドメイン内の少なくとも 2 つの異なるチャネル上に AP を配置する。*
  - ***ステップ 3:*** *2.4GHz 帯の規制ドメイン外の少なくとも 2 つの異なるチャネル*

上にAP を配置する。

- ***ステップ 4:*** *テストされる各チャネル上でAP が検出されることを検証する。*

- ***テスト 3:*** *非標準のチャネル周波数*
  - ***ステップ 1:*** *SFR で選択されたとおりチャネルを監視するように TSF を設定する。*
  - ***ステップ 2:*** *非標準のチャネル周波数上の少なくとも 2 つの異なるチャネル上にAP を配置する。*
  - ***ステップ 3:*** *テストされる各チャネルでAP が検出されることを検証する。*

FAU_WID_EXT.2.2 TSF は、[**選択**: *データの送信を防止するように設定可能な、データを送信しない*] [*802.11 監視 SFP*] に合致するネットワークトラフィクを検出するための無線センサを提供しなければならない。

適用上の注釈: 本 SFR の意図は、サイトが無線方針なしの実装を望むような場合、すべての無線送信機能を無効にできるような WIDS/WIPS センサを採用することである。

適用上の注釈:「802.11 監視 SFP」は、セキュリティ機能方針であり、この方針を参照する SFR には、方針が行う内容が記述される。「802.11 監視 SFP」は、FDP_IFC.1.1 で確立され、FAU_WID_EXT の SFR を通して定義される。ベンダは、この方針を形式的に定義する必要はなく、SFR に適合することのみが必要となる。

保証アクティビティ

TSS

評価者は、センサを完全に受動的に構成する方法に関する情報が TSS に含まれていることを検証しなければならない。具体的には、TOE が保護機能を無効にした専用センサとして構成できるか、または保護機能無しが有効になっている場合においても、センサがデータを送信する場合、無線送信を無効化する方法をTSS にて示さなければならない。

ガイダンス

具体的には、TOE が保護機能を無効にした専用センサとして構成できるか、または保護機能無しが有効になっている場合においても、センサがデータを送信する場合、無線送信を無効化する方法をTSS にて示さなければならない。

テスト

TOE が無線伝送を無効にする機能を提供する場合、評価者は、無線で送信しないようにセンサを設定するために、操作ガイダンスに従わなければならない。次に、評価者は、TOE からの無線送出をチェックするために、シグナルアナライザを設置しなければならない。
その後、評価者は、以下のテストを実行しなければならない:

シグナルアナライザを配置し、以下のテストで指定された帯域に構成する。

2.4 GHz 帯の場合

- ***テスト 1:***
  - ***ステップ 1:*** *センサを起動し、シグナルアナライザを使用して、センサからの放射がないかどうかをチェックする。*
  - ***ステップ 2:*** *シグナルアナライザがセンサからの放射を受けていないことを検証する。*
- ***テスト 2:***
  - ***ステップ 1:*** *センサが通常動作中に、アナライザを約 10 分間観察し、センサから放射が発生していないかどうかをチェックする。*
  - ***ステップ 2:*** *シグナルアナライザがセンサからの放射を受けていないことを検証する。*

5 GHz 帯の場合

- ***テスト 1:***
  - ***ステップ 1:*** *センサを起動し、シグナルアナライザを使用して、センサからの放射がないかどうかをチェックする。*
  - ***ステップ 2:*** *シグナルアナライザがセンサからの放射を受けていないことを検証する。*
- ***テスト 2:***
  - ***ステップ 1:*** *センサが通常動作中に、アナライザを約 10 分間観察し、センサからの放射が発生していないかどうかをチェックする。*
  - ***ステップ 2:*** *シグナルアナライザがセンサからの放射を受けていないことを検証する。*

FAU_WID_EXT.2.3 TSF は、[*SSID*]のサブセットを許可されたものとして定義する能力を提供しなければならない。

適用上の注釈: 管理者は、どの SSID をネットワーク上で許可するかを設定する能力を有しているべきである。

保証アクティビティ

TSS

TSS 保証アクティビティは規定されていない。

ガイダンス

評価者は、許可された SSID の設定方法に関する指示について、TSS に含まれていることを検証しなければならない。

テスト

評価者は、一連の許可されたチャネルと SSID で TSF を構成しなければならない。本方針の違反を検出する能力は、FAU_WID_EXT.2.4 でテストされる。

FAU_WID_EXT.2.4 TSF は、以下の方法により、ネットワーク上の許可されていないトラフィクのプレゼンスを検出しなければならない:[

- 許可された SSID をブロードキャストする許可されていない AP の検出。
- ホワイトリスト上の AP と EUD の MAC アドレスを詐称する AP と EUD の検出。
- 許可されていない SSID に関連する許可された EUD の検出。
- 許可された AP に関連する許可されていない EUD の検出。
- ホワイトリスト上の AP による許可されていないポイントツーポイント無線ブリッジの検出。
- アクティブプロービングの検出
- [**選択**: *不法な状態遷移、プロトコル侵害*[***選択**:802.11、802.1X、**[割付**:固有のベンダプロトコル]]、*他の方法はない。*]]

適用上の注釈:「許可された」EUD/AP は、FAU_INV_EXT.1.1 で定義されたホワイトリストに割り当てられたものである。不法な状態遷移やプロトコル侵害の検出はオブジェクティブ要件であり、将来の PP バージョンでは必須となる予定である。

保証アクティビティ

TSS

評価者は、許可されていない接続や許可されていないネットワークトラフィクのプレゼンスを検出するために、TOE が使用する方法について、TSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、許可された SSID の構成方法に関する指示を操作ガイダンスが提供していることを検証しなければならない。

テスト

評価者は、一連の許可された SSID で TSF を構成し、以下のテストを実行しなければならない:

許可されていない SSID、許可されていない接続 – 2.4 GHz 帯

- ***テスト 1:***
  - ***ステップ 1**: 許可された SSID を使用して、2.4GHz 帯の設定チャネルで動作するようにホワイトリスト上の AP を設定する。*
  - ***ステップ 2**: ホワイトリスト上にない EUD を AP に接続する。*
  - ***ステップ 3**: ホワイトリスト上の AP に接続するホワイトリスト上にない EUD を TSF が検出したことを検証する。*
  - ***ステップ 4**: AP の SSID を許可リストにない SSID に変更する。*

- ***ステップ 5***：*ホワイトリスト上のEUD をAP に接続する。*
- ***ステップ 6***：*TSF が許可されていない SSID を使用するホワイトリスト上のAP と許可されていないSSID に関連するEUD を検出することを検証する。*

許可されていないSSID、許可されていない接続 - 5GHz 帯

- ***テスト 2:***
  - ***ステップ 1***：*許可されたSSID を使用して、5GHz 帯の設定チャネルで動作するようにホワイトリスト上のAP を設定する。*
  - ***ステップ 2***：*ホワイトリスト上にないEUD をAP に接続する。*
  - ***ステップ 3***：*ホワイトリスト上の AP に接続するホワイトリスト上にないEUD をTSF が検出したことを検証する。*
  - ***ステップ 4***：*AP のSSID を許可リストにないSSID に変更する。*
  - ***ステップ 5***：*ホワイトリスト上のEUD をAP に接続する。*
  - ***ステップ 6***：*TSF が許可されていない SSID を使用するホワイトリスト上のAP と許可されていないSSID に関連するEUD を検出することを検証する。*

MAC 詐称

- ***テスト 1***：
  - *二番目のEUD の上で、ホワイトリスト上のAP に接続されているホワイトリスト上のEUD のMAC アドレスになりすます。*
  - *なりすましている有効な EUD が最初の AP に接続している間に、別のホワイトリスト上のAP に、詐称したMAC アドレスのEUD を接続する。*
  - *TSF がMAC 詐称を検出したことを検証する。*
- ***テスト 2***：
  - *二番目のAP 上でホワイトリスト上のAP のMAC アドレスになりすます。*
  - *TSF がMAC 詐称を検出したことを検証する。*

アクティブプロービング

- ***テスト 1***：
  - *WLAN のサブネットでアクティブスキャンを実行する。*
  - *使用されたツールと実行されたスキャンのタイプを記録する。TSF がアクティブプロービングを検出したことを検証する。*

ポイントツーポイント無線ブリッジ

- ***テスト 1***：
  - *無線センサの範囲内のホワイトリスト上の AP を使用して、ポイントツーポイント無線ブリッジを設定する。*
  - *TSF がブリッジを検出したことを検証する。*

FAU_WID_EXT.3 無線侵入検知 – サービスの拒否

FAU_WID_EXT.3.1　TSF は、以下の侵入を検出しなければならない：*[RF ベースのサービス拒否(DoS)、deauthentication flooding、disassociation flooding、**[割付：他の DoS 方式]**、送信要求／送信可の乱用、他の DoS 方式なし]*。

保証アクティビティ

TSS

評価者は、TOE によって検出できるサービス拒否（DoS）攻撃について TSS に記述されていることを検証するため、TSS を検査しなければならない。

ガイダンス

さまざまな種別のサービス拒否（DoS）攻撃を検出する TOE の能力が設定可能である場合、評価者は、検出された攻撃の特定方法に関する指示を操作ガイダンスが提供していることを検証しなければならない。

テスト

RF ベースの DoS

- ***テスト 1***
  - *ホワイトリスト上の AP を配置し、特定のチャネルに留まるように構成する。*
  - *ホワイトリスト上の EUD を AP に接続する。*
  - *AP 及び EUD と同じ周波数で、RF ジャマーまたは信号発生器を使用して DoS を作成する。*
  - *TSF が RF ベースの DoS を検出したことを検証する。*

トラフィク注入ベースの DoS

- ***テスト 1：Deauthencitaion Flood***
  - *ホワイトリスト上の AP を配置し、設定チャネルを構成する。*
  - *ホワイトリスト上の EUD を AP に接続する。*
  - *ホワイトリスト上の AP の MAC アドレスを使用して、EUD に deauthentication フレームのフラッドを送信する。*
  - *TSF が deauthentication flood を検出したことを検証する。*
  - *ホワイトリスト上の AP を発信元及びブロードキャストの宛先として、MAC アドレスを用いて、deauthentication フレームのフラッドを送信する。*
  - *TSF が deauthentication flood を検出したことを検証する。*
- ***テスト 2：Disassociation Flood***
  - *ホワイトリスト上の AP を配置し、設定チャネルを構成する。*
  - *ホワイトリスト上の 2 個の EUD を AP に接続する。*
  - *RF メディアを予約するために、CTS フレームのフラッドを送信する。*
  - *TSF が CTS の乱用を検出することを検証する。*

FAU_WID_EXT.4 無線侵入検知– 許可されていない認証方式

FAU_WID_EXT.4.1　TSF は、許可された管理者に、許可された WLAN 認証方式を定義する能力を提供し

なければならない。

保証アクティビティ

TSS

評価者は、許可された管理者が許可された WLAN 認証方式を定義することを許可する TOE の能力について、TSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、検出の目的で許可されたものや許可されていないものとして、WLAN 認証方式を定義する方法についての指示を、操作ガイダンスが提供していることを検証するため、操作ガイダンスを検査しなければならない。

テスト

評価者は、一連の許可された WLAN 認証方式で TSF を構成しなければならない。この方針の違反を検出する機能は、FAU_WID_EXT.4.2 でテストされる。

FAU_WID_EXT.4.2 TSF は、*[FAU_INV_EXT.1.1 で定義されたホワイトリストに登録された AP と EUD]*が許可されていない WLAN 認証方式を使用しようとする試みを検出しなければならない。

保証アクティビティ

TSS

評価者は、許可されていない WLAN 認証方式を使用するときを検出する TOE の能力について、TSS に記述されていることを検証しなければならない。

ガイダンス

本 SFR には、操作ガイダンスのアクティビティはない。

テスト

評価者は、許可された WLAN 認証方式の唯一のモードとして、802.1x 認証を使用して TSF を構成し、以下のテストを実行しなければならない:

- ***テスト 1:***
    - *オープン認証でホワイトリスト上の AP を配置する。*
    - *ホワイトリスト上の EUD を AP に接続する。*
    - *TSF が許可されていない認証方式を使用している AP と EUD を検出することを検証する。*
    - *事前共有鍵認証を使用するホワイトリストに登録された AP を配置する。*
    - *ホワイトリスト上の EUD を AP に接続する。*
    - *TSF が許可されていない認証方式を使用している AP と EUD を検出することを検証する。*

FAU_WID_EXT.5 無線侵入検知– 許可されていない暗号化方式

FAU_WID_EXT.5.1 TSF は、許可された管理者に、許可された WLAN 暗号化方式を定義する能力を提供しなければならない。

保証アクティビティ

TSS

評価者は、許可された管理者が許可された WLAN 暗号化方式を定義することを可能にする TOE の能力について TSS に記述されていることを検査しなければならない。

ガイダンス

評価者は、検出の目的で許可されたものや許可されていないものとして、WLAN 暗号化方式を定義する方法についての指示を、操作ガイダンスが提供していることを検証するため、操作ガイダンスを検査しなければならない。

テスト

評価者は、一連の許可された暗号化方式で TSF を構成しなければならない。本方針の違反を検出する能力は、FAU_WID_EXT.5.2 でテストされる。

FAU_WID_EXT 5.2 TSF は、*[FAU_INV_EXT.1.1 で定義されたホワイトリストに登録された AP と EUD]* が許可されていない WLAN 暗号化方式の利用の試行を検出しなければならない。

保証アクティビティ

TSS

評価者は、許可されていない WLAN 暗号化方式が利用されるときを検出するための TOE の能力が TSS に記述されていることを検証しなければならない。

ガイダンス

本 SFR には、操作ガイダンスアクティビティはない。

テスト

評価者は、唯一の許可された暗号化方式として 128 ビット AES 暗号化種別を用いて TSF を構成し、以下のテストを実行しなければならない:

- ***テスト 1:***
  - *暗号化なしで、ホワイトリスト上の AP を配置する。*
  - *ホワイトリスト上の EUD を AP に接続する。*
  - *TSF が許可されていない暗号化方式を用いて AP と EUD の検出を検証する。*
  - *TKIP 暗号化のみを使用するホワイトリスト上の AP を配置する。*

- *ホワイトリスト上のEUD をAP に接続する。*
- *TSF が許可されていない暗号化方式を使用している、AP とEUD を検出したことを検証する。*

FAU_WID_EXT.5.3 TSF は、*[FAU_INV_EXT.1.1 で定義されたホワイトリスト上の AP と EUD]*で暗号化されていないデータの送受信が行われた場合を検出しなければならない。

適用上の注釈: ホワイトリスト上の AP や EUD によって暗号化されていないデータを受信する場合、ホワイトリスト上にない、またはホワイトリスト上の AP や EUD から、ホワイトリスト上の AP や EUD に暗号化されていないデータが送信される。

保証アクティビティ

TSS

評価者は、許可されない AP と EUD が暗号化されないデータを送受信するときを検出する TOE の能力について、TSS に記述されていることを検証しなければならない。

ガイダンス

本 SFR には、操作ガイダンスアクティビティは存在しない。

テスト

- ***テスト 1:***
  - *ホワイトリスト上のAP を暗号化なしで配置する。*
  - *ホワイトリスト上のEUD をAP に接続し、トラフィクを生成する。*
  - *ホワイトリスト上のAP とEUD との間で送信される暗号化されていないデータフレームをTSF が検出したことを検証する。*
  - *ホワイトリスト上にないEUD をAP に接続し、トラフィクを生成する。*
  - *ホワイトリスト上の AP とホワイトリスト上にない EUD との間で送信される暗号化されていないデータフレームをTSF が検出したことを検証する。*
- ***テスト 2:***
  - *ホワイトリスト上にないAP を暗号化なしで配置する。*
  - *ホワイトリスト上のEUD をAP に接続し、トラフィクを生成する。*
  - *ホワイトリスト上にない AP とホワイトリスト上の EUD との間で送信される暗号化されていないデータフレームをTSF が検出したことを検証する。*

FAU_GEN.1/WIDS 監査データ生成

FAU_GEN.1.1/WIDS TSF は、以下の監査対象事象の監査記録を生成できなければならない:

a. 監査機能の起動と終了;
b. 監査の[指定されていない]レベルのすべての監査対象事象;

c. [表 3 で列挙されている監査対象事象;
d. 無線センサ通信の障害]。

要件	監査事象	付加的な監査記録の内容
FAU_ANO_EXT.1.1	なし	なし
FAU_ANO_EXT.1.2	なし	なし
FAU_ARP.1.1	なし	なし
FAU_ARP_EXT.2.1	なし	なし
FAU_GEN.1.2/WIDS	なし	なし
FAU_IDS_EXT.1.1	なし	なし
FAU_INV_EXT.1.1	なし	なし
FAU_INV_EXT.1.2	なし	なし
FAU_INV_EXT.1.3	なし	なし
FAU_INV_EXT.2.1	なし	なし
FAU_INV_EXT.2.2	なし	なし
FAU_INV_EXT.2.3	なし	なし
FAU_INV_EXT.3.1	なし	なし
FAU_INV_EXT.4.1	なし	なし
FAU_INV_EXT.4.1/CELL	なし	なし
FAU_INV_EXT.5.1	なし	なし
FAU_MAC_EXT.1.1	なし	なし
FAU_MAC_EXT.1.2	なし	なし
FAU_SAA.1.1	なし	なし
FAU_SAA.1.2	なし	なし
FAU_SIG_EXT.1.1	なし	なし
FAU_SIG_EXT.1.1/PCAP	なし	なし
FAU_SIG_EXT.1.2/PCAP	なし	なし
FAU_SIG_EXT.1.2/pcap,	なし	なし
FAU_SIG_EXT.1.3/PCAP	なし	なし
FAU_WID_EXT.1.1	なし	なし

FAU_WID_EXT.1.2	なし	なし
FAU_WID_EXT.2.1	なし	なし
FAU_WID_EXT.2.2	センサ無線送信機能	無線送信機能がオンになる。
FAU_WID_EXT.2.3	なし	なし
FAU_WID_EXT.2.4	なし	なし
FAU_WID_EXT.3.1	なし	なし
FAU_WID_EXT.4.1	なし	なし
FAU_WID_EXT.4.2	なし	なし
FAU_WID_EXT.5.1	なし	なし
FAU_WID_EXT.5.2	なし	なし
FAU_WID_EXT.5.3	なし	なし
FAU_WID_EXT.6.1	なし	なし
FAU_WID_EXT.6.2	なし	なし
FAU_WID_EXT.7.1	なし	なし
FAU_WIP_EXT.1.1	なし	なし
FDP_IFC.1.1	なし	なし
FMT_SMF.1.1/WIDS	なし	なし
FPT_FLS.1.1	障害に関する情報	障害発生、障害の種別、障害した機器、また、障害の時間、の通知
FPT_ITT.1.1	なし	なし
FTP_ITC.1.1	なし	なし

表 3: 監査対象事象

適用上の注釈: 本 SRF には、ND cPP で説明される FAU_GEN.1 の SFR を拡張する追加の監査対象事象が存在する。表の事象は、適合するセキュリティターゲットとの関連で ND cPP の事象と組み合わされるべきである。監査対象事象の表にはオプション要件及びオブジェクティブ要件が含まれている。オプション要件及びオブジェクティブ要件の監査は、ベンダが要件を NIAP によって評価することを選択した場合にのみ必要とされる。

保証アクティビティ

TSS

本 SFR には、TSS 保証アクティビティはない。

ガイダンス

本 SFR には、操作ガイダンスアクティビティはない。

テスト

評価者は、以下のテストを実行しなければならない:
評価者は、本 EP の機能要件に関連する保証アクティビティに従って、TOE が監査記録を生成することによって、監査記録を正しく生成することができるという TOE の能力をテストしなければならない。テスト結果を検証する場合、評価者は、テスト中に生成された監査記録が管理ガイドに指定されたフォーマットと一致し、各監査記録のフィールドに適切なエントリがあることを保証しなければならない。ここでのテストは、セキュリティメカニズムのテストと直接的に関連させて実施することができることに注意する。

4.1.2 利用者データ保護

FDP_IFC.1 情報フロー制御方針(訳注:CC パート 2 では、「サブセット情報フロー制御」)

FDP_IFC.1.1 TSF は、*[以下のすべての IEEE 802.11 a、b、g、n、ac フレームタイプとサブタイプ間]*で、*[802.11 監視 SFP]*を実施しなければならない:*[*

- *許可された AP と許可された EUD*
- *許可された AP と許可されていない EUD*
- *許可されていない AP と許可された EUD]*

適用上の注釈:「許可された」EUD/AP は、FAU_INV_EXT.1.1 で定義されたホワイトリストに割り当てられたものである。

適用上の注釈:「802.11 監視 SFP」はセキュリティ機能方針であり、本方針を参照する SFR は、方針が行う内容を記述する。「802.11 監視 SFP」は、FDP_IFC.1.1 において確立され、FAU_WID_EXT の SFR によって定義される。ベンダは本方針を形式的に定義する必要はなく、SFR に適合しなければならない。

保証アクティビティ

TSS

本 SFR には、TSS 保証アクティビティはない。

ガイダンス

この機能が構成可能である場合、評価者は、操作ガイダンスが、異なるタイプの IEEE802.11 フレームタイプ及びサブタイプを監視するように、TOE を構成する方法に関する指示を提供することを検証しなければならない。

テスト

- *テスト 1：*
  - *設定されたチャネルにWIDS センサを設定する。*
  - *WIDS センサからトラフィクキャプチャを開始する。*
  - *[以下のすべてのIEEE 802.11 a、b、g、n、ac フレームタイプ及びサブタイプ]のチャネルのやり取りで、センサが動作しているチャネル上に、設定されたフレーム数を送信する:[*
    1. *許可されたAP と許可されたEUD*
    2. *許可されたAP と許可されていないEUD*
    3. *許可されていないAP と許可されたEUD*

    ]
  - *キャプチャしたものに、そのすべてのタイプとサブタイプからのフレームが存在することを検証する。*

4.1.3 セキュリティ管理

FMT_SMF.1/WIDS 管理機能の仕様（WIDS）（訳注：CC パート 2 では「管理機能の特定」）

FMT_SMF.1.1/WIDS TSF は、WIDS 機能のために、以下の管理機能を実行できなければならない：*[表 2 にリストされた管理機能]*。

SFR	管理機能
FAU_ANO_EXT.1.1	期待されるふるまいのベースラインを構成するネットワークアクティビティの期間の指定（オプション）。

表 2： 管理機能

保証アクティビティ

TSS

評価者は、TSS がベースラインの構成方法を記述していることを検証しなければならない。

ガイダンス

評価者は、操作ガイダンスがベースラインを定義するための指示を記述していることを検証しなければならない。

テスト

評価者は以下のテストを実行しなければならない：

- ***テスト 1：****操作ガイダンスの指示に従って、ベースラインを構成するネットワークア*

クティビティの期間を、TSF に示すことができることを検証する。

4.1.4 TSF の保護

FPT_ITT.1 基本 TSF 内データ転送保護

FPT_ITT.1.1 詳細化 TSF は、TSF データが TOE の異なるパーツ間で送られる場合、TSF データを暴露と改変から保護するため、**他のすべての高信頼通信と同等のセキュリティ強度を有する**［**選択**、以下の少なくとも 1 つ:*IPsec*、*SSH*、*TLS*、*TLS/HTTPS*］**を利用**しなければならない。

適用上の注釈: 本要件は、分散型 TOE のコンポーネント間のすべての通信が暗号化された通信チャネルの利用を介して保護されることを保証する。この高信頼通信チャネルを通過するデータは、選択で選ばれたプロトコルで定義されるとおり暗号化される。ST 作成者は、TOE によってサポートされているメカニズムを選び、次にその選択に対応する NDcPP からの適切な要件が ST にない場合、複製されることを保証する。本要件の目的のため、セキュリティ強度は NIST SP 800-57 で定義され、「同等の」とは強度が、最小限、EP で列挙された暗号プリミティブの要件を満たさなければならことを意味する、また「他の高信頼通信」は、FPT_ITC で規定されるメカニズムを指す。

保証アクティビティ

TSS

評価者は、分散型 TOE コンポーネントを保護するために利用される方法とプロトコルが記述されていることを決定するため、TSS を検査しなければならない。評価者は、TOE 管理をサポートするためにTSS に列挙されたすべてのプロトコルが要件で規定されたものと合致し、ST の要件に含まれていることを確認しなければならない。

ガイダンス

評価者は、サポートされるそれぞれの方法の通信経路を確立するための指示が操作ガイダンスに含まれていることを確認しなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

- ***テスト 1:** 評価者は、規定された（操作ガイダンスにおける）通信方法が、評価の過程でテストされ、操作ガイダンスに記述されるとおりにコネクションが確立され、通信が成功することを保証しなければならない。*
- ***テスト 2:** 評価者は、通信のそれぞれの方法について、チャネルデータが平文で送信されないことを保証しなければならない。*

その他の保証アクティビティは、特定のプロトコルと関連している。

4.1.5 高信頼パス／チャネル

FTP_ITC.1 TSF 間高信頼チャネル

FTP_ITC.1.1 詳細化　TSF は、それ自身と以下の機能：監査サーバ、[**選択：*データベースサーバ*、*[割付：他の機能]*、*なし*]**をサポートする許可された IT エンティティ間に、他の通信チャネルと論理的に区別され、その端点の保証された識別、及び暴露からのチャネルデータの保護、及びチャネルデータの改変の検出を提供する高信頼通信チャネルを提供するために［選択：IPsec、SSH、TLS、HTTPS］を利用できなければならない。

適用上の注釈: TSF が別のデータベースサーバを使用する場合、データベースサーバの選択は ST に含まれなければならない。

保証アクティビティ

評価者は、本 SFR のベース NDcPP で指定された保証アクティビティに加えて、以下のアクティビティを実行しなければならない。

TSS

評価者は、要件で識別される許可された IT エンティティとのすべての通信に対して、それぞれ通信メカニズムが、その IT エンティティの許可されたプロトコルに関して識別されることを決定するために TSS を検査しなければならない。また、評価者は、TSS に列挙されているすべてのプロトコルが特定され、ST の要件に含まれていることを確認しなければならない。

ガイダンス

評価者は、許可されたそれぞれの IT エンティティと許可されたプロトコルを確立するための指示が含まれていること、及びコネクションが意図せずに切断される場合に取られるべき回復(recovery)の指示が、ガイダンス文書に含まれていることを確認しなければならない。

テスト

- ***テスト 1**：評価者は、ガイダンス証拠資料に記述されたとおりコネクションをセットアップし、通信が成功することを保証し、許可された各 IT エンティティとのそれぞれのプロトコルを用いた通信が評価の過程でテストされることを保証しなければならない。*
- ***テスト 2**：TOE が本要件で定義されるとおりに開始できる各プロトコルについて、評価者は、実際に通信チャネルが TOE から開始できることを保証するため、ガイダンス証拠資料に従わなければならない。*
- ***テスト 3**：評価者は、許可された IT エンティティとの各通信チャネルについて、チャネルデータが平文では送信されないことを保証しなければならない。*
- ***テスト 4**：評価者は、テスト 1 の間に、許可された各 IT エンティティに対応する各*

プロトコルについて、確立されたコネクションを物理的に中断しなければならない。評価者は、物理的なコネクションが回復されたとき、通信が適切に保護されることを保証しなければならない。

さらなる保証アクティビティは、具体的なプロトコルに対応する。

4.2 セキュリティ保証要件

本 EP では、NDcPP 内で定義された SAR を超える SAR を定義しない。本 EP に対して評価される TOE は、NDcPP に対して本質的に評価されることに留意することが重要である。TOE の評価の際に、ベース PP に記述されている部分だけでなく、ベース PP 用に定義された SAR を TOE 全体に適用しなければならない。

附属書 A. オプション要件

セクション 1.3 で示したように、本 EP の本文にはベースライン要件（WIDS/WIPS によって実行されなければならないもの）が含まれている。さらに、これ以外の 3 つの種別の要件が附属書 A、附属書 B、及び附属書 C に規定されている。（本附属書中の）第 1 の種別は、ST に含まれることが可能な要件であるが、WIDS/WIPS が本 EP への適合を主張するために要求されないものである。（附属書 B の）第 2 の種別は、EP の本文での選択に基づく要件である。特定の選択がなされる場合、その附属書の追加の要件が含まれなければならない。(附属書 C の) 第 3 の種別は、本 EP へ適合するための要求には含まれないが、本 EP の将来のバージョンのベースライン要件に含まれることになるであろうコンポーネントであり、ベンダによる採用が推奨される。ST 作成者には、附属書 A、附属書 B、及び附属書 C に含まれる要件と関連するかもしれないが列挙されない要件（例、FMT タイプの要件）もまた、ST に含まれることを保証する責任があることに留意されたい。

FAU_WID_EXT.6 無線侵入検知 – 無線スペクトラム監視

FAU_WID_EXT.6.1 TSF は、以下の RF 帯域：[**選択**：*3.6 GHz、60 GHz、GHz 以下（0-900MHz）、すべての携帯電話帯域*]で動作するネットワークデバイスのプレゼンスを検出しなければならない。

適用上の注釈： 本 SFR は、指定される周波数で動作する非 WiFi（IEEE 802.11 a、b、g、n、及び ac）ネットワークデバイスを指す。ST 作成者が携帯電話帯域のデバイスの検出を選択する場合、ST 作成者は選択ベースの要件 FAU_INV_EXT.4.1 を含めなければならない。

保証アクティビティ

TSS

評価者は、TSF がその利用を検出できるような RF 帯域と技術のセットについて TSS に含まれていることを検証しなければならない。TSS には、有効化の方法と追加の帯域検出に必要とされるハードウェアについての指示が含まれるべきである。

ガイダンス

評価者は、本機能を実行するために必要なハードウェアと同様に、ST に含まれる技術の検出を有効化する方法と設定する方法が操作ガイダンスに記述されていることを検証しなければならない。

テスト

評価者は、選択された技術の検出を有効化し、設定しなければならない。

- ***テスト 1：** 所与の技術においてデバイスを配置し、TSF がそのデバイスを検出することを検証する。*

FAU_WID_EXT.6.2 TSF は、無線スペクトラム分析用の専用センサを提供しなければならない。

保証アクティビティ

TSS

評価者は、TOE が無線スペクトラム分析用の専用センサを提供していることを検証するため、TSS を検証しなければならない。

ガイダンス

評価者は、本機能の実行に必要なハードウェアと同様に、専用スペクトラム分析を有効化する方法と設定する方法について、操作ガイダンスに記述されていることを検証しなければならない。

テスト

評価者は、専用スペクトラム分析を有効化して設定し、TSS に列挙される能力をテストしなければならない。

附属書 B. 選択ベース要件

本 EP の概説で示すとおり、ベースライン要件（TOE によって実行されなければならないもの）が本 EP の本文に含まれる。本 EP の本文での選択に基づく追加の要件がある：特定の選択がなされる場合、以下の追加の要件が含まれる必要がある。

FAU_INV_EXT.4/CELL 環境オブジェクトのロケーション（携帯電話デバイス）

本コンポーネントは、FAU_WID_EXT.6.1 での選択に依存する。

FAU_INV_EXT.4/ CELL　TSF は、[*検出された携帯電話デバイス*]の物理的な位置情報を、その実際の位置情報の[**割付**：*距離精度*]以内で検出しなければならない。

保証アクティビティ

TSS

評価者は、携帯電話デバイスの物理的ロケーションを検出する TOE の能力に関する情報が TSS に含まれていることを検証しなければならない。

ガイダンス

評価者は、位置追跡を設定する方法、位置マップをロードする方法（該当する場合）、及びデバイスのロケーションとインタフェースする TSF 管理者が閲覧可能な場所に関する指示について、操作ガイダンスをレビューしなければならない。

テスト

評価者は、以下のテストを実行しなければならない：

- ***テスト 1:***
  - ***ステップ 1：*** *センサの範囲内に携帯電話デバイスを配置する。*
  - ***ステップ 2：*** *TSF がデバイスの位置を追跡できることを検証する。*
  - ***ステップ 3：*** *TSF によって示される精度のレベルが割付で示されるレベル内に入ることを検証する。*

FAU_ANO_EXT.1 異常ベースの侵入検知

本コンポーネントは、FAU_IDS_EXT.1.1 での選択に依存する。

FAU_ANO_EXT.1.1　TSF は、[**選択**：
スループット（[割付：時間周期（分、時間、日など）ごとのデータ要素（バイト、パケット等）]）、
一日うちの時刻、
頻度、
しきい値、

*［**割付**：その他の方法］*

］及び以下のネットワークプロトコルフィールド：

- すべての管理及び制御フレームヘッダエレメント

］ の特定を含めて、［**選択**：少なくとも1つ選択：*ベースライン（「期待され、かつ承認される」）、異常（「期待されない」） トラフィクパタン* ］ の定義をサポートしなければならない。

保証アクティビティ

TSS

評価者は、SFR で指定されるベースラインの構成と構築、または異常ベースの属性について、TSS に記述されていることを検証しなければならない。評価者は、ベースラインが TSF によってどのように定義されて実装されるか、または異常ベースの規則が管理者によって定義され設定される方法についての記述を TSS が提供することを検証しなければならない。

ガイダンス

評価者は、TSS で主張されている内容に基づいて、ベースライン及び／または異常なトラフィクパタンを設定する方法について操作ガイダンスに記述されていることを検証しなければならない。

テスト

- ***テスト 1：***
  - *評価者は、ベースラインまたは異常ベースの規則を設定するため、操作ガイダンスの指示を利用しなければならない。*
  - *評価者は、ベースラインと合致しないトラフィクまたは異常ベースの規則と合致するトラフィクを送信しなければならず、TSF が異常なふるまいを検出し、警報を生成することを検証しなければならない。*

FAU_ANO_EXT.1.2 TSF は、［**選択**：*管理者による手動設定、自動化された設定*］を通して異常なアクティビティの定義をサポートしなければならない。

適用上の注釈：「ベースライン」と「異常」は、TOE 管理者によって手動で定義／設定されもの（または定義をインポートするもの）、または一定期間を越えて、ネットワークトラフィクを検査することによって TOE が自動的に定義／作成できるもの（いわゆる「プロファイリング」）である。

保証アクティビティ

TSS

評価者は、利用可能な設定モード（手動または自動）とベースラインを構成またはイン

ポートする方法についてTSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、ST で選択されたものに基づいて、異常なアクティビティを自動及び／または手動で定義を行う方法について、操作ガイダンスに記述されていることを検証しなければならない。

テスト

このテストは、FAU_ANO_EXT.1.1 と組み合わせて実施することができる。評価者は、操作ガイダンスに従わなければならず、ST で選択されたものに基づいて、自動及び／または手動の手段によって異常なアクティビティを定義しなければならない。評価者は、異常なトラフィクが TSF によって識別されることを決定することによって、異常なアクティビティが正しく定義されていることを、それぞれの場合において検証しなければならない。

FAU_SIG_EXT.1 シグネチャベースの侵入検知

本コンポーネントは、FAU_IDS_EXT.1.1 での選択に依存する。

FAU_SIG_EXT.1.1 TSF は、利用者定義されたカスタマイズ可能な攻撃シグネチャをサポートしなければならない。

保証アクティビティ

TSS

評価者は、TOE が定義可能であるような利用者定義されたカスタマイズ可能な攻撃シグネチャについて、TSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、利用可能なカスタマイズオプションの説明が含まれている、利用者定義されたカスタマイズ可能な攻撃シグネチャの設定方法に関する情報を操作ガイダンスが提供していることを検証しなければならない。

テスト

- ***テスト 1：***

  -ステップ 1： *TSS で示される利用可能なフィールドを用いてシグネチャを細工する。*

  -ステップ 2： *シグネチャと合致するような細工されたフレームをホワイトリスト上の EUD へ送信する。*

  -ステップ 3： *新しく定義されたシグネチャに基づく警報を TSF が引き起こすことを検証する。*

FAU_STG_EXT.1/PCAP 保護された監査事象格納（パケットキャプチャ）

本コンポーネントは、FAU_ARP.1.1 での選択に依存する。

FAU_STG_EXT.1.1/PCAP TSF は、生成された**パケットキャプチャ**を、FTP_ITC.1 に従う高信頼チャネルを用いて外部 IT エンティティへ送信できなければならない。

適用上の注釈: FTP_ITC.1 は、NDcPP から継承される

保証アクティビティ

TSS

評価者は、外部エンティティへパケットキャプチャを送信するために TSF で利用可能な（FTP_ITC.1 で規定される）高信頼チャネルのリストについて、TSS に含まれていることを検証しなければならない。TSS には、高信頼チャネルの設定方法に関する指示についても含まれなければならない。

ガイダンス

本 SFR には、操作ガイダンスアクティビティはない。

テスト

- ***テスト 1:*** *評価者は、TSS で規定されたガイダンスに従ってパケットキャプチャを設定しなければならない。次に、評価者は、キャプチャを開始する事象を引き起こし、FTP_ITC.1 でのテストを通して、外部デバイスへ送信されているキャプチャされたトラフィクが高信頼チャネルを介して送信されていることを検証しなければならない。*

FAU_STG_EXT.1.2/PCAP TSF は、生成された**パケットキャプチャ**を TOE 自身に格納できなければならない。

保証アクティビティ

TSS

評価者は、パケットキャプチャデータをそれ自身の内部に格納するための TOE の能力について、TSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、パケットキャプチャデータ用に利用可能な格納領域の容量とデータがどこに格納されるかに関する情報を操作ガイダンスが提供することを検証しなければならない。

テスト

- ***テスト 1:*** *評価者は、TSS で規定されるガイダンスに従って、TSF 上に格納されるパケットキャプチャを設定しなければならない。評価者は、次にキャプチャを開始する事象を引き起こし、パケットキャプチャが TSF 上に格納されたことを検証しなければならない。*

FAU_STG_EXT.1.3/PCAP TSF は、パケットキャプチャデータ用のローカル格納領域が満杯であるとき、[**選択**: *新しいパケットキャプチャデータを破棄、以下の規則[**割付**:以前のパケットキャプチャを上書きする規則]に従って以前のパケットキャプチャを上書き、[**割付**:その他のアクション]*]をしなければならない。

保証アクティビティ

TSS

評価者は、パケットキャプチャデータ用のローカル格納領域が枯渇したときの TOE のふるまい、及びこのふるまいが設定可能かどうかについて、TSS に記述されていることを検証しなければならない。

ガイダンス

パケットキャプチャデータ用のローカル格納領域が枯渇したときの TOE のふるまいが設定可能な場合、評価者は、何が設定可能なふるまいか、及びそれらがどのように設定可能かについての情報を操作ガイダンスが提供することを検証しなければならない。

テスト

- ***テスト 1:*** *評価者は、TSS で規定されるとおり TSF 上でのパケットデータ維持と削除の規則を定義しなければならず、規定された規則の機能をテストしなければならない。*

附属書 C. オブジェクティブ要件

本附属書には、脅威に対抗するセキュリティ機能を規定する要件が含まれる。本要件は、商用の技術において未だ広く利用可能ではないようなセキュリティ機能について記述されているため、現時点では本 EP の本文では必須とされない。しかし、これらの要件は、WIDS/WIPS が引き続き、本 EP に適合するように、ST に含まれてもよい。これらの要件は、本 EP の将来のバージョンで、オブジェクティブ要件からベースライン要件へ移行するだろう。

FAU_INV_EXT.4 環境オブジェクトの正確な位置

FAU_INV_EXT.4.1 TSF は、[*AP*、*EUD*]の物理的な位置を実際の位置から[*15 フィート*]以内で検出しなければならない。

保証アクティビティ

TSS

評価者は、要求されたレベルの正確さを満たすため、位置追跡、センサの最適な数、センサの配置に関する情報が TSS に含まれることを検証しなければならない。

ガイダンス

評価者は、位置追跡を設定する方法、位置情報マップをロードする方法（該当する場合）、及び TSF 管理者インタフェースのどこで AP と EUD のロケーションを閲覧できるかに関する指示について、操作ガイダンスをレビューしなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

テスト 1:

- ***ステップ 1:*** *センサの範囲内に AP を配置する。*
- ***ステップ 2:*** *AP についての位置追跡情報を TS（訳注:TSS）が提供することを検証する。*
- ***ステップ 3:*** *提示された AP の位置が実際の位置から 15 フィート以内であることを検証する。*

FAU_INV_EXT.5 許可されない接続の検出

FAU_INV_EXT.5.1 TSF は[*FAU_INV_EXT.1 で定義されるとおりのホワイトリスト上にない AP*]が次の接続:[*社内ネットワークへの有線接続*]を有するときを検出しなければならない。

保証アクティビティ

TSS

評価者は、保護された有線ネットワークインフラへ接続中の AP を検出する能力を TSF が持っているかどうかに関するガイダンスについて、TSS に含まれていることを検証しなければならない。その能力が存在する場合、TSS は、この機能のための設定ガイダンスを含まなければならない。

ガイダンス

評価者は、保護された有線インフラへ接続される許可されていない AP を検出するため、WIDS/WIPS を設定する方法に関する指示について、操作ガイダンスをレビューしなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

テスト 1:

- ***ステップ 1:*** *ホワイトリスト上にない AP を配置する。*
- ***ステップ 2:*** *保護されたネットワークインフラへ有線を介して AP を接続する。*
- ***ステップ 3:*** *検出された AP と EUD のリストについて、WIDS/WIPS ユーザインタフェースをチェックする。*
- ***ステップ 4:*** *不正な AP が検出されること、及び保護された有線インフラへ接続される AP の検出に際して生成される警報を検証する。*

FAU_MAC_EXT.1 デバイスなりすまし

FAU_MAC_EXT.1.1 TSF は、オーバーラップしないロケーションの 2 つのセンサが、同時に同じ MAC アドレスからのトラフィクを受信するときを検出しなければならない。

適用上の注釈: 本 SFR の意図は、攻撃者がホワイトリスト上の EUD をディスコネクトさせて、直ちにホワイトリスト上の EUD の MAC アドレスを用いて、ホワイトリスト上にないデバイスを接続することができるような、MAC 詐称を検出することである。

保証アクティビティ

TSS

評価者は、オーバーラップしない位置の 2 つのセンサが、同時に同じ MAC アドレスからのトラフィクを受信するときの TOE のふるまいが、TSS に記述されていることを検証しなければならない。

ガイダンス

評価者は、オーバーラップしない位置の 2 つのセンサが、同時に同じ MAC アドレスからのトラフィクを受信するときを TSF が検出できるようなやり方で TOE を配置する方法についての指示を操作ガイダンスが提供することを検証しなければならない(即ち、オーバーラップしないカバレッジを保証するためのセンサの範囲と配置についての情

報)。

テスト

評価者は、以下のテストを実行しなければならない:

テスト 1:

- ***ステップ 1**:ホワイトリスト上の AP を設定する。(ロケーション 1)*
- ***ステップ 2**:ホワイトリスト上の EUD を AP に接続する。*
- ***ステップ 3**:ホワイトリスト上の 2 番目の AP とホワイトリスト上にない EUD を、WIDS がセンサを持つような別のオーバーラップしないロケーションにセットアップする。または、有効なネットワークに接続されたシールドされた環境に 2 番目の AP を配置することによって、離れたオーバーラップしないロケーションをシミュレートする。(ロケーション2)*
- ***ステップ 4**:ロケーション 1 の EUD の MAC アドレスをロケーション 2 の EUD を用いて詐称し、ロケーション 2 のホワイトリスト上の AP にそれを接続する。両方の EUD が同時に接続されていることを確認する。*
- ***ステップ 5**:TSF がそれを検出し、警報を生成したことを検証する。*

FAU_MAC_EXT.1.2

TSF は、オーバーラップしないロケーションにある 2 つのセンサが[*センサ間の距離に基づいて許可された管理者が設定可能な時間枠*]内で[*FAU_INV_EXT.1 で定義されているホワイトリスト上にない EUD*]の MAC アドレスからのトラフィクを受信することを検出しなければならない。

適用上の注釈:本 SFR の意図は、管理者が 2 つの離れたロケーションで接続しているホワイトリスト上の EUD 間で許容されるべき時間を決定できるようにすることである。

保証アクティビティ

TSS

本 SFR に対する TSS 保証アクティビティはない。

ガイダンス

評価者は、操作ガイダンスが、2 つの別のロケーションから接続する 2 回目以降の EUD に対する試行の間に許容されるべき時間枠を設定する方法に関する指示を提供することを検証しなければならない。

テスト

評価者は、以下のテストを実行しなければならない:

テスト 1:

- ***ステップ 1**: 2 つの別々のロケーション(ロケーション 1、ロケーション 2)で 2 つ*

のEUD の接続の間に許容される時間枠を設定する。

- ***ステップ 2:*** *ホワイトリスト上のAP を設定する。(ロケーション1)*
- ***ステップ 3:*** *ホワイトリスト上のEUD をAP に接続する。*
- ***ステップ 4:*** *ホワイトリスト上の2 番目のAP とホワイトリスト上にないEUD を、WIDS がセンサを備える別のオーバーラップしないロケーションに設定する。または、有効なネットワーク(ロケーション2)に接続された、シールドされた環境に2 番目のAP を配置することによって、遠くのオーバーラップしない位置をシミュレートする。*
- ***ステップ 5:*** *ロケーション1 のEUD のMAC アドレスをロケーション2 のEUD でなりすまして、ロケーション2 のホワイトリスト上のAP に接続する。接続間の時間が許容され/設定された時間枠より短いことを確認する。*
- ***ステップ 6:*** *TSF が検出し、警報を生成したことを検証する。*

FAU_WID_EXT.7 無線侵入検知 – 固有トラフィク監視

FAU_WID_EXT.7.1 TSF は、[*以下の間:*

1. *許可されたAP と許可されたEUD。*
2. *許可されたAP と許可されていないEUD。*
3. *許可されていないAP と許可されたEUD。*

のすべての IEEE 802.11 a、b、g、n、ac フレームタイプとサブタイプ]についての[*802.11 監視 SFP*]に合致する、すべてのベンダ独自のネットワークトラフィクのプレゼンスを検出しなければならない。

適用上の注釈:「802.11 監視 SFP」は、セキュリティ機能方針であり、この方針を参照する SFR は、その方針が何をするかを記述する。「802.11 監視 SFP」は、FDP_IFC.1.1 において確立され、FAU_WID_EXT の SFR を通して定義される。ベンダは、この方針を形式的に定義する必要はなく、本 SFR に適合することのみが必要がある。

保証アクティビティ

TSS

本 SFR には、TSS 保証アクティビティはない。

ガイダンス

本 SFR には、操作ガイダンスアクティビティはない。

テスト

テスト 1:

- ***ステップ 1:*** *セットされたチャネルにWIDS センサをセットする。*
- ***ステップ 2:*** *WIDS センサからトラフィクキャプチャを開始する。*
- ***ステップ 3:*** *以下から/以下へのすべてのIEEE 802.11 a、b、g、n、ac の*

ベンダ独自のフレームタイプとサブタイプ用に、センサが動作中のチャネル上にセットされたフレーム数を送信する:

1.許可されたAPと許可されたEUD

2.許可されたAPと許可されていないEUD

3.許可されていないAPと許可されたEUD

- ***ステップ 4:*** *テスト用に利用されたフレームタイプとサブタイプのリストを用意し、すべてが検出されたことを検証する。*

FAU_WIP_EXT.1 無線侵入保護

FAU_WIP_EXT.1.1 TSF は、以下の方法:[**選択:** *無線抑制、社内有線ネットワークに接続された許可されない AP の有線抑制*]を用いて、TSF によって監視されるネットワークから無線 AP や EUD を隔離することを許可された管理者に許容しなければならない。

適用上の注釈:許可された管理者は、無線の抑制を開始するため、不正 AP や EUD として、AP や EUD の確認に責任がある。
本 SFR では、社内有線ネットワークへ接続される許可されていない AP の抑制は、保護された内部有線インフラへ物理的に(有線で)接続される許可されていない AP を指す。

保証アクティビティ

TSS

評価者は、TSF上で利用可能な抑制方法のリストとその設定方法がTSS に含まれていることを検証しなければならない。

ガイダンス

本 SFR には、操作ガイダンスは存在しない。

テスト

TSF 上で利用可能な抑制の方法を構成し、各方法について以下のテストを実行しなければならない:

テスト 1:

- ***ステップ 1:*** *ホワイトリスト上にないAP を配備し、保護された有線インフラに接続する(不正なものとして分類されるか、手動でそのように分類するかを確かめる)。*
- ***ステップ 2:*** *ホワイトリスト上のEUD をAP に接続する。*
- ***ステップ 3:*** *TSF が警報を生成し、ホワイトリスト上のEUD の不正なAP との接続を切断し、不正なAP を阻止することを検証する。*

FAU_GEN.2/WIDS 監査データ生成（WIDS/WIPS）（訳注：CC パート 2 では、FAU_GEN.1）

FAU_GEN.2.1/WIDS（訳注：CC パート 2 では、FAU_GEN.1.1）

TSF は、以下の監査対象事象の WIDS/WIPS 監査記録を生成できなければならない：

a. WIDS/WIPS 機能の起動と終了；
b. 監査の[指定されていない]レベルのすべての WIDS/WIPS 監査対象事象；
c. [表 4 で列挙される監査対象事象：
d. 指定される期間内に発生する同様の事象の合計]

要件	監査対象事象	追加の監査記録の内容
FAU_ANO_EXT.1.1	なし	なし
FAU_ANO_EXT.1.2	なし	なし
FAU_ARP.1.1	なし	なし
FAU_ARP_EXT.2.1	なし	なし
FAU_GEN.1.2/WIDS	なし	なし
FAU_IDS_EXT.1.1	なし	なし
FAU_INV_EXT.1.1	ホワイトリスト上のデバイスの情報	デバイスの種別（AP または EUD）、MAC アドレス
FAU_INV_EXT.1.2	なし	なし
FAU_INV_EXT.1.3	なし	なし
FAU_INV_EXT.2.1	なし	なし
FAU_INV_EXT.2.2	なし	なし
FAU_INV_EXT.2.3	なし	なし
FAU_INV_EXT.3.1	ホワイトリスト上のデバイスによる予期せぬふるまいの警報	検出されたふるまいの説明（ブリッジ、ICS 接続）、ホワイトリスト上のデバイスの MAC アドレス、ホワイトリスト上のデバイスと接続を確立したデバイスの MAC アドレス、接続の開始と終了。
FAU_INV_EXT.4.1	デバイスの位置に関する情報	デバイスの MAC アドレス、デバイスのタイプ、デバイスの種別、デバイスを検出したセンサ、検出センサで受信した信号強度、検出センサへの近接度（メートル）。
FAU_INV_EXT.4.1/CELL	デバイスの位置に関する情報	デバイスの MAC アドレス、デバイスのタイプ、デバイスの種別、

要件	監査対象事象	追加の監査記録の内容
		デバイスを検出したセンサ、検出センサで受信した信号強度、検出センサへの近接度（メートル）。
FAU_INV_EXT.5.1	不正なデバイスの検出によって生成された警報	警報の説明、デバイスの種別（AP や EUD）、MAC アドレス、許可されたデバイス間で行われたアソシエーション（EUD に接続されている AP）、検出されたチャネル、検出された RF 帯域、不正使用された暗号化タイプ、使用された IEEE 802.11 規格（a、b、g、n、ac）、SSID（AP の場合）。
FAU_MAC_EXT.1.1	MAC なりすましの検出によって生成された警報	警報の説明、デバイスの種別（AP や EUD）、MAC アドレス、許可されたデバイス間で行われたアソシエーション（EUD に接続されている AP）、検出されたチャネル、検出された RF 帯域、不正使用された暗号化タイプ、使用された IEEE 802.11 規格（a、b、g、n、ac）、SSID（AP の場合）。
FAU_MAC_EXT.1.2	MAC なりすましの検出によって生成された警報	警報の説明、管理者によりラベル付けされた場所、異なる場所間の接続にかかった時間、デバイスの種別（AP や EUD）、MAC アドレス、許可されたデバイス間で行われたアソシエーション（EUD に接続されている AP）、検出されたチャネル、検出された RF 帯域、不正使用された暗号化タイプ、使用された IEEE 802.11 規格（a、b、g、n、ac）、SSID（AP の場合）。
FAU_SAA.1.1	なし	なし
FAU_SAA.1.2	なし	なし
FAU_SIG_EXT.1.1	利用者定義されたシグネチャの侵害によって生成された警報	引き起こされた警報の名前（シグネチャの作成時に提供されたもの）、警報の説明（シグネチャ

要件	監査対象事象	追加の監査記録の内容
		の作成時に提供されたもの）、関連するデバイスの MAC アドレス。
FAU_SIG_EXT.1.1/PCAP	なし	なし
FAU_SIG_EXT.1.2/PCAP	なし	なし
FAU_SIG_EXT.1.2/pcap,	なし	なし
FAU_SIG_EXT.1.3/PCAP	なし	なし
FAU_WID_EXT.1.1	なし	なし
FAU_WID_EXT.1.2	なし	なし
FAU_WID_EXT.2.1	なし	なし
FAU_WID_EXT.2.2	なし	なし
FAU_WID_EXT.2.3	許可された SSID の詳細。	管理者が許可した SSID。
FAU_WID_EXT.2.4	許可されていないアクティビティ	侵害の説明（許可されていない SSID に接続されたホワイトリスト上の EUD）、関連するデバイスの本人性
FAU_WID_EXT.3.1	DoS のために生成された警報	MAC アドレス、デバイスの種別、攻撃された AP や EUD の種別、DoS の詳細（RF や注入ベース）、注入ベース、タイプの表示（認証解除フラッド）
FAU_WID_EXT.4.1	なし	なし
FAU_WID_EXT.4.2	デバイス及び許可されていない認証方法に関する情報。	MAC アドレス、デバイスの種別、関係するデバイスの分類、使用される認証方法。
FAU_WID_EXT.5.1	なし	なし
FAU_WID_EXT.5.2	デバイス及び許可されていない暗号化方法に関する情報。	MAC アドレス、デバイスの種別、関係するデバイスの種別、使用される暗号化方法。
FAU_WID_EXT.5.3	関係するデバイスの情報	MAC アドレス、デバイスの種別、関係するデバイスの種別（送信デバイスと受信デバイス）。
FAU_WID_EXT.6.1	検出されたデバイスの情報	周波数帯域、周波数帯域内で使用されるチャネル、本人性（該当する場合は、MAC アドレス、または、他の同様の一意の

要件	監査対象事象	追加の監査記録の内容
		ID）、デバイス技術（携帯電話）、デバイスを検出したセンサ。
FAU_WID_EXT.6.2	なし	なし
FAU_WID_EXT.7.1	なし	なし
FAU_WIP_EXT.1.1	実行したアクションの情報	侵害の説明、使用された抑制の種別、抑制を手動または自動で引き起こしたか、抑制を実行するセンサ（無線の場合）、抑制されるデバイスの詳細（種別、デバイスの種別、MAC アドレス）。
FDP_IFC.1.1	なし	なし
FMT_SMF.1.1/WIDS	なし	なし
FPT_FLS.1.1	なし	なし
FPT_ITT.1.1	なし	なし
FTP_ITC.1.1	なし	なし

表 4：WIDS/WIPS 監査対象事象

適用上の注釈：監査対象事象の表には、WIDS/WIPS 警報の監査メッセージが含まれている。監査対象事象の表には、オプション要件及びオブジェクティブ要件が含まれている。オプション要件とオブジェクティブ要件の監査は、ベンダが要件を NIAP によって評価されることを選択した場合にのみ要求される。「類似」したタイプの事象に関しては、「類似」事象の唯一の重要な違いがタイムスタンプである場合、ある時間内に同じ監査対象な事象が複数回発生していることになる。
例えば、妥当な期間内に発生する同種の事象ごとに、個別の監査メッセージを生成することは期待されていない。

保証アクティビティ

TSS
本 SFR には、TSS 保証アクティビティはない。

ガイダンス

本 SFR には、操作ガイダンスアクティビティはない。

テスト

評価者は、以下のテストを実行しなければならない：
評価者は、本 EP の機能要件に関連する保証アクティビティに従って、TOE が監査記録を生成することによって、監査記録を正しく生成することができるという TOE の能

力をテストしなければならない。テスト結果を検証する場合、評価者は、テスト中に生成された監査記録が管理ガイドに指定された書式と一致し、各監査記録のフィールドに適切なエントリがあることを保証しなければならない。ここでのテストは、セキュリティメカニズムのテストと直接的に関連させて実施することができる。

FAU_GEN.2.2/WIDS（訳注：CC パート 2 では、FAU_GEN.1.2）

TSF は、各 WIDS/WIPS 監査対象事象内に、少なくとも以下の情報を、[選択：コンマ区切り値（CSV）、共通ログ形式（CLF）、JavaScript オブジェクト記法（JSON）、syslog]として記録しなければならない：

a. 事象の日付・時刻、事象の種別、及びサブジェクト識別情報(該当する場合)；
b. 各監査事象種別に対して、PP/ST 機能コンポーネントの監査対象事象の定義に基づいた、[*表 4 にリストされている監査対象事象*]。

保証アクティビティ

TSS

本 SFR には、TSS 保証アクティビティはない。

ガイダンス

評価者は、その結果として WIDS/WIPS データログ記録が適切となるように、TOE を構成する方法を操作ガイダンスが記述していることを検証しなければならない。評価者は、操作ガイダンスが、同様の事象（しきい値の設定、時間窓の定義など）のログを記録することに関して行われうるどんな構成についての指示も提供することを検証しなければならない。

テスト

評価者は、以下のテストを実行しなければならない。
評価者は、表 4 の各 WIDS/WIPS 監査対象事象に対して、ST で選択された形式の予期された WIDS/WIPS 監査データを警報が生成することをテストしなければならない。ここでのテストは、直接、セキュリティメカニズムのテストを合わせて実施できることに注意する。

FPT_FLS.1 基本 TSF 内データ転送保護(訳注：CC パート 2 では、「*セキュアな状態を保持する障害*」である)

FPT_FLS.1.1

TSF は、以下の種別の障害が生じたときはセキュアな状態を保持しなくてはならない：[*センサ機能の障害、TSF の危殆化の可能性*]。

適用上の注釈：最低限、セキュアな状態を保持することは、定義された障害条件が生じたときに、監査記録の生成を要求する。

保証アクティビティ

TSS

評価者は、TOE のフェールセーフ機能の実装が文書化されていることを決定するために、TSS のセクションをレビューしなければならない。評価者は、ST で規定されるすべての障害モードが記述されていることを保証するために、TSS のセクションを検査しなければならない。

ガイダンス

評価者は、TOE の障害の可能性、TSF がこれらの障害に続くセキュアな状態をどのように保持するか、そして、障害状態への移行後に TOE を正常に復旧するために必要なアクションを、特定することを検証するために操作ガイダンスをレビューしなければならない。

テスト

- ***テスト 1：*** *ST で指定される各障害モードについて、評価者は、各障害モード種別を開始の後、TOE がセキュアな状態に到達することを保証しなければならない。*

附属書 D. 参考資料

識別子	タイトル
[CC]	情報技術セキュリティ評価のためのコモンクライテリア- • パート1：概説と一般モデル、CCMB-2012-09-001、バージョン3.1 改訂第4版、2012年9月。 • パート2：セキュリティ機能コンポーネント、CCMB-2012-09-002、バージョン3.1 改訂第4版、2012年9月。 • パート3：セキュリティ保証コンポーネント、CCMB-2012-09-003、バージョン3.1 改訂第4版、2012年9月。
[CEM]	情報技術セキュリティ評価のための共通方法—評価方法、CCMB-2012-09-004、バージョン3.1 改訂第4版、2012年9月。

附属書 E. 略語

略語	意味
AES	高度暗号化規格（Advanced Encryption Standard）
AP	アクセスポイント（Access Point）
BSSID	基本サービスセット識別子（Basic Service Set Identifier）
DoS	サービスの拒否（Denial of Service）
EP	拡張パッケージ（Extended Package）
EUD	エンドユーザデバイス（End User Device）
HTTPS	ハイパーテキスト転送プロトコル (Hypertext Transfer Protocol)
IPsec	インターネットプロトコルセキュリティ (Internet Protocol Security)
MAC	メディアアクセスコントロール（Media Access Control）
NIAP	National Information Assurance Partnership
NIST	国立標準技術研究所（National Institute of Standards and Technology）
PP	プロテクションプロファイル（Protection Profile）
SSH	セキュアシェル（Secure Shell）
SSID	サービスセット識別子（Service Set Identifier）
TLS	トランスポート層セキュリティ（Transport Layer Security)
TKIP	Temporal Key Integrity Protocol
WEP	Wired Equivalent Protocol
WIDS	無線侵入検知システム（Wireless Intrusion Detection Systems）
WIPS	無線侵入防止システム（Wireless Intrusion Prevention Systems）
WLAN	無線ローカルエリアネットワーク（Wireless Local Area Network）
WPA	Wi-Fi 保護アクセス（Wi-Fi Protected Access）