ネットワークデバイスのコラボレイティブプロテクションプロファイル（ND cPP）／アプリケーションソフトウェアプロテクションプロファイル（App PP）拡張パッケージ ボイス／ビデオオーバーIP（VVoIP） エンドポイント

バージョン 1.0

2016 年 9 月 28 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

改版履歴

バージョン	日付	コメント
v0.1	2016-08-26	初版ドラフト
v0.2	2016-08-26	IAD フィードバックに基づく内部更新
v0.3	2016-09-16	TC フィードバックに基づく内部更新
v0.4	2016-09-26	TC フィードバックに基づく内部更新
v1.0	2016-09-28	発行

目次

1　概説

1.1 概要

本拡張パッケージ (EP) の適用範囲は、[CC] の観点からボイス／ビデオオーバーIP（VVoIP）エンドポイントのセキュリティ機能を記述し、このような製品の機能要件と保証要件を定義することである。本 EP は、これ自体で完結するものではなく、むしろ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（ND cPP）、または、アプリケーションソフトウェアのプロテクションプロファイル（App PP）を拡張するものである。これは、VVoIP エンドポイントが、リモートチャネルを介して機微なデータを配送し、一般的なネットワークデバイスやソフトウェアアプリケーションによって実装されないようなプロトコルを使用する、特定のタイプのネットワークデバイスまたはソフトウェアアプリケーションであるためである。したがって、追加のセキュリティ要件は、機微な通信が意図されない受信者への許可されない暴露の対象でないことを保証するために必要である。

1.2 用語

以下のセクションでは、本 EP で用いられるコモンクライテリア用語と技術用語の両方について提供する。

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共通基準。
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）	PP によって記述された製品の特定のサブセット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。
プロテクションプロファイル（PP）	あるカテゴリーの製品に対するセキュリティ要件の実装に依存しないセット。
セキュリティ保証要件（SAR）	SFR についての TOE の適切な実装が評価者によって検証される方法についての要件。
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実装に依存するセキュリティ要件についてのセット。
評価対象（TOE）	評価される製品。ここでは、エンタープライズセションコントローラ機能を有するネットワークデバイス。
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）	TOE がどのように ST の SFR を満たすかについての記述。

1.2.2 技術用語

エンタープライズ セション コントローラ	VVoIP エンドポイント間で呼をセットアップし、切断するために使用される VVoIP インフラストラクチャデバイス。
H.323	複数の参加者とのマルチメディアセションの作成、改変、及び終了のために利用される ITU-T によって定義された通信プロトコル。
セション イニシエーション プロトコル	複数の参加者とのマルチメディアセションの作成、改変、及び終了のために利用される IETF によって定義された通信プロトコル。
セキュア リアルタイム トランスポート プロトコル	暗号化、メッセージ認証と完全性、リプレイ保護の追加されたセキュリティを有する、マルチメディア（オーディオ／ビデオ）ストリーミングサービスを提供するために利用されるプロトコル。

1.3 適合評価対象

本 EP と ND cPP または App PP のいずれかによって定義される評価対象は、インターネットプロトコル（IP）ネットワークを介したボイス交換及び／またはビデオ交換の通信を提供するような、専用デバイスまたはソフトウェアアプリケーションである。 エンドポイントは、エンタープライズセションコントローラ（ESC）サーバと通信するような、クライアント（TOE）である。VVoIP エンドポイントは、VVoIP エンドポイントのソフトウェアと設定をアップデートするためにファイルサーバからのファイルダウンロードをセキュアにすることができなければならず、ESC との呼制御のためのセキュアな通信を確立しなければならず、他のデバイスへのストリーミングメディアをセキュアにしなければならない。

ND cPP と本 EP の組み合わせは、ネットワークデバイスであり、VVoIP エンドポイント機能を提供するような、変更不可能なオペレーティングシステムを備えた専用アプライアンス、または独立した商用利用可能なオペレーティングシステムを実行中の汎用サーバのいずれかである。TOE がスタンドアロンアプライアンスであるのか VVoIP エンドポイントとして機能するように設定された汎用デバイスであるのかにかかわらず、TOE は、ND cPP のすべての必須要件を満たすことができなければならない。App PP と本 EP の組み合わせは、App PP によって義務付けられている、ソフトウェアアプリケーションに期待されるすべてのセキュリティ機能に加えて、VVoIP エンドポイント機能を提供するような、汎用オペレーティングシステム上で動作中のソフトウェアアプリケーションである。

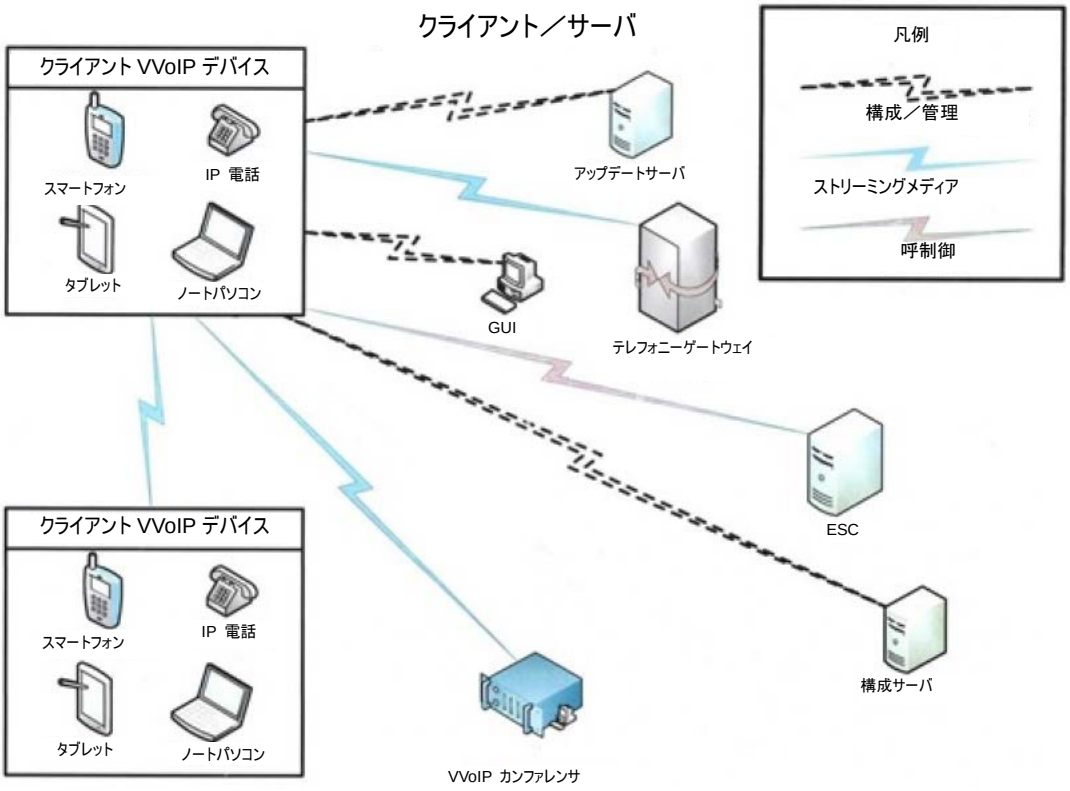
セキュアなファイルダウンロードとは、クライアントとファイルサーバ（ESC と同じサーバであるかもしれない）間のパケットの交換である。呼制御は、電話通話の呼の確立、維持、及び切断を行うための ESC とクライアント（VVoIP エンドポイント）間で交換されるパケットである。ストリーミングメディアは、エンドポイント間で交換されるボイス／ビデオである。

本 EP は、VVoIP エンドポイントに特有の機能要件と脅威について記述する。本 EP で規定されない VVoIP エンドポイントに対する任意の要件は、ND cPP または App PP に従う必要がある。最も顕著な追加は、呼制御プロトコル（SIP、H.323/H225.0、H.245）とストリーミングメディアプロトコル（SRTP、RTP）についての要件である。

1.3.1 TOE 境界

TOE 境界には、VVoIP 対応デバイス、またはアプリケーション（VVoIP エンドポイント）が含まれる。VVoIP 対応デバイスは、専用電話機であるが、VVoIP エンドポイントアプリケーションは、スマートフォン、タブレット、PC などの汎用デバイスで動作するような、多くのアプリケーションの一つに過ぎない。TOE がハードウェアアプライアンスであるか、オペレーティングシステム上のクライアントアプリケーションであるかにかかわらず、同じ環境に配備される。次の図は、TOE の観点からの典型的な VVoIP インフラストラクチャを示す。

多くの環境コンポーネントは、相互に直接接続しているが、これらの接続は TOE からは見えないため、描かれていない。



TOE は、その他の VVoIP エンドポイントデバイスまたは電話会議のようなその他の電話機器との接続をセットアップするために、エンタープライズセションコントローラ（ESC）に接続する。さらに、ESC は、TOE の運用のための監査データの格納に責任を持つ。ESC は、ソフトウェア／ファームウェアのアップデートを TOE に提供する能力についても有するが、これはファイルサーバによって代わりに実行されることも可能である。

TOE は、インターネットプロトコルバージョン 4（IPv4）を処理できなければならない。 ESC との通信を開始するには、TOE は、IP アドレス、ネットワークマスク、ゲートウェイアドレス、構成サーバのアドレス、アップグレードサーバのアドレス、及び ESC アドレスを必要とする。 そのアドレスは、DHCP（ダイナミックホストコンフィギュレーションプロトコル）によって取得されるか、VVoIP エンドポイント上で手動入力されるか、または TOE が常駐するデバイスから継承される（ソフトウェアアプリケーションの場合）かもしれない。 TOE は、基本的な電話機能を許可すべきである。一度 IP アドレスが取得されると、TOE は、あらゆる VVoIP アプリケーションのアップデートをダウンロード

し、VVoIP エンドポイント設定をダウンロードし、VVoIP クライアントとして ESC サーバに接続する。呼が終了したとき、または回線がさもなければ使用されていないとき、TOE は、ストリーミングメディア通信パスが閉じられることを保証すること。

TOE には、実行する必要のある 3 つの異なる機能のための 3 つのパス(経路)がある:ボイス、ビデオ、セション制御を含むストリーミングメディアパス(エンドポイントからエンドポイント); エンドポイントを制御するための呼制御パス(ESC へのエンドポイント)、 TOE を設定し、管理するための設定／管理パス(ソフトウェア／ファームウェアのアップデート、設定のアップデート、監査)。

1.4 ユースケース

本 EP の要件は、以下のユースケースのセキュリティ課題に対処するように設計されている。これらのユースケースの記述は、本 EP によって要求される機能をサポートするために、TOE とその運用環境がどのように作られるべきかについての指示を提供する。

[ユースケース 1] 専用アプライアンス

VVoIP エンドポイントは、下位のプラットフォームオペレーティングシステムへの直接のインタフェースを持たないような、スタンドアロンのネットワークアプライアンスとして販売され、パッケージ化されている。このユースケースでは、ND cPP と本 EP への適合は、セキュリティを保証するために十分である。

[ユースケース 2] ソフトウェアアプリケーション

VVoIP エンドポイントは、変更可能なオペレーティングシステム(Windows または Linux 等)を実行中の汎用コンピュータにインストールされるような、アプリケーションとして販売され、パッケージ化されている。このコンピュータは、ユーザワークステーションとして機能するので、VVoIP 通信用に利用されるアプリケーションに加えてエンドユーザアプリケーションを実行するかもしれない。この場合、VVoIP エンドポイントアプリケーションは、NIAP の「アプリケーションソフトウェアのプロテクションプロファイル」に適合することが期待される。下位のプラットフォームは、NIAP の「汎用オペレーティングシステムのプロテクションプロファイル」にも適合すると期待されるが、これは本 EP の範囲外である。 適合 TOE は、監査や暗号等の特定の機能についてオペレーティングシステムに依拠するかもしれない。しかし、このような機能は、明確に識別されなければならず、関連 SFR について本 EP で規定される保証アクティビティをそのオペレーティングシステム機能が満たすという証拠が提供されなければならない。

TOE の物理的な具現化にかかわらず、期待される機能的な能力は同じである。 本 EP は、所与の機能を実装するための複数の方法を許容するため、オプション要件と選択ベース要件を定義する。これらの相違点は、別々のユースケースを構成しない、なぜならそれらは TOE の基本的な使用方法が同じであるからである。

2　適合主張

適合ステートメント

本 PP 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。その 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 (規定の選択が無条件要件で選択されるとき、要求される)

また、以下のようなコンポーネントを含んでもよいとする。

- オプション
- オブジェクティブ

必須の要件は、本書の本文（セクション 5）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。ST 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ものとするが、ND cPP または App PP（本 EP が拡張するもの）、または本 EP 自身、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 PP 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 PP は、その他の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 ND cPP または App PP のいずれかを拡張することに留意されたい、そのとき本 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にこれらの PP のいずれかに依拠することを意味する。しかし、これは、本 EP 自体がこれらの PP のいずれかに適合することを示唆するものではない。

パッケージ主張

本 PP は、いかなるパッケージへの適合も主張しない。

3　セキュリティ課題定義

セキュリティ課題は、TOE が対処すると想定される脅威、その運用環境についての前提条件、及び TOE が実施すると期待されるような、あらゆる組織のセキュリティ方針に関して記述されている。

ND cPP または App PP の EP として、ベース PP で定義される、すべての脅威、前提条件、及び OSP は、特に指定がない限り、それが拡張するベース PP に応じて、TOE に対しても適用されることに留意されたい。
本 EP で定義されるセキュリティ機能要件は、本 EP で定義される脅威を軽減するが、VVoIP エンドポイントによって提供される具体的な機能に起因してベース PP で定義された脅威をより包括的に軽減することもできるかもしれない。

3.1 脅威

T.UNDETECTED_TRANSMISSION

攻撃者は、利用者が一切のメディアが送信されていないという合理的な推測を持つような状態で、リモートチャネルを介して TOE にオーディオ及び／またはビデオメディアを流出させるかもしれない。

T.CLOCK_DESYNC

攻撃者は、暗号化及び／または認証の接続失敗の発生からサービス拒否をもたらすように、不正確なクロックデータを TOE に利用させるかもしれない。

T.MEDIA_DISCLOSURE

攻撃者は、送信されたデータのデコードをうまく利用するため、暗号化された可変レートのボコーダフレームを利用できる。

3.2 前提条件

本 EP は、サポートされるベース PP で定義されたものを超える追加の前提条件を一切定義しない。

3.3 組織のセキュリティ方針

本 EP は、サポートされるベース PP で定義されたものを超える追加の組織のセキュリティ方針を一切定義しない。

4　セキュリティ対策方針

4.1 TOE のセキュリティ対策方針

本 EP は、ベース PP に規定されるものを超えて、追加の TOE セキュリティ対策方針を一切定義しない。

4.2 運用環境のセキュリティ対策方針

本 EP は、追加の前提条件、または組織のセキュリティ方針を定義しないため、満たすべき運用環境の追加のセキュリティ対策方針は一切ない。

4.3 セキュリティ対策方針根拠

追加のセキュリティ対策方針が一切定義されないので、本セクションは、本 EP へ一切適用されない。

5　セキュリティ要件

本セクションに含まれるセキュリティ機能要件（SFR）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（CC）*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。

CC は、セキュリティ機能要件（SFR）に関する操作を定義する：割付、選択、選択内の割付及び詳細化。
本書では、CC によって定義された操作を特定するため、次のフォント表記法を用いる：

- **割付**は、イタリック体のテキストで表記される。
- **詳細化**は、EP 作成者によってなされ、太字テキストで表記される。
- **選択**は、下線付きテキストで表記される。
- 選択内の**割付**は、イタリック体の下線付きテキストで表記される。
- **繰返し**は、SFR 名称 の後に、繰返しの目的を示唆する、スラッシュとユニークな識別子を追加することによって表記される、例、「/CDR」通話詳細記録に関する SFR について。
- **拡張 SFR** は、SFR 名称の後に、ラベル「EXT」を有することで識別される。

5.1 ND cPP セキュリティ機能要件の方向性

TOE が物理的アプライアンスであり、本 EP が ND cPP を拡張するために使用される場合、ST 作成者は、本 EP によって要求される機能を提供するために、特定の選択または割付を行い、特定のオプション要件を含める必要がある。 本セクションは、本 EP への適合を主張するため、ベース PP でなされる必要のある主張についての指示を提供する。

本セクションの要件の全部の保証アクティビティが繰り返されるわけではない； ND cPP のサポート文書で、すでに取り込まれたものを補足するために必要な追加のテストのみが含まれている。

5.1.1 暗号サポート（FCS）

FCS_TLSC_EXT.2　　認証を伴う TLS クライアントプロトコル

本 SFR は、ND cPP ではオプションであるが、本 EP では必須である、なぜなら、利用されるアプリケーションレイヤプロトコルに関係なく、呼制御とストリーミングメディアチャネルをセキュアにするために TLS が利用されるからである。

保証アクティビティ

ND cPP で要求されるものを超える一切の追加のテストは本 SFR のために要求されない。

5.1.2 セキュリティ管理（FMT）

FMT_SMF.1　　管理機能の特定

FMT_SMF.1.1 TSF は、以下の管理機能を実行することができなければならない:

- TOE をローカル及びリモートで管理する能力;
- アクセスバナーを設定する能力;
- セションを終了またはロックするまでのセションの非アクティブ時間を設定する能力;
- TOE をアップデートし、それらのアップデートをインストールする前にデジタル署名機能を用いてアップデートを検証する能力;
- **TOE を ESC に［*選択:手動で、 TFTP サーバ経由で* ］登録する能力;**
- [選択:
  - *監査のふるまいを設定する能力;*
  - *FIA_UIA_EXT.1 で規定されるように、エンティティが識別認証される前に利用可能な TOE 提供のサービスのリストを設定する能力;*
  - *暗号機能を設定する能力;*
  - ***アイドルコールの終了時間を設定する能力;***
  - ***使用されるボコーダを規定する能力;***
  - *その他の能力*]。

適用上の注釈: *本 EP は、VVoIP エンドポイント機能に特に関連する設定可能な機能を ST 作成者が選択する能力を提供するため、ベース PP の既存の FMT_SMF.1 SFR を変更する。デフォルトで SFR を満たすようなやり方で TSF が自動的に動作する場合、これらの機能は設定可能でないかもしれないことに留意されたい。*

いくつかの管理機能は、TOE と人との直接的な対話を通してというよりもむしろ、ESC／設定サーバを介してのみ設定できるように実装されるかもしれない。 ST 作成者は、それぞれの論理インタフェースを介して TOE へ送信されるような、異なる TSF 関連のデータを評価者が分析できるように、それぞれの管理機能の実行方法についての情報を提供することが期待される。

保証アクティビティ

TSS 本 SFR のベース PP で規定される保証アクティビティに加えて、評価者は、TSS が TOE の初期設定の記述を提供すること及び本 SFR で定義される機能を TSF が管理する能力について記述することを、それぞれの機能が管理される方法（例、手動設定、ダウンロードされた設定ファイルによる適用）を含め、検証しなければならない。

AGD 評価者は、操作ガイダンスが、TOE の設定についての指示を提供

することを検証しなければならない。

テスト 本 SFR のベース PP で規定される保証アクティビティに加えて、評価者は、TOE の ESC への登録のためにサポートされる方法に応じて、次のテストを実施しなければならない:

テスト 1（条件付き）: 手動入力に基づく ESC 登録:

1. TOE において、IP アドレス、ゲートウェイアドレス、サブネットマスクを入力する。
2. 運用環境が設定サーバと ESC が 2 つの別々のサーバであるようなやり方で配置される場合、それぞれのアドレスを入力する;さもなければ、ESC アドレスを入力する。
3. 設定を保存する。
4. TOE が ESC へ登録されることを検証する。

テスト 2: TFTP サーバから入力される値に基づく ESC 登録:

1. TOE において、TFTP サーバアドレスを入力する。
2. 設定を保存する。
3. TOE がすべての必要な IP アドレスを受信したことをスニフィングして検証する。
4. TOE の IP アドレスを検査することによって検証する。
5. TOE が ESC へ登録されることを検証する。

5.1.3 TSF の保護（FPT）

FPT_STM.1 **高信頼タイムスタンプ**

本 EP は、ND cPP で定義される FPT_STM.1 SFR を変更しない。しかし、本 EP への想定は、TOE の時刻源が ESC 自体であることである。TOE は、自身の決定的な時刻源として自身に依拠しない。したがって、以下に記述される追加のテストは、本 EP のために実行されると期待される。

保証アクティビティ

TSS 評価者は、NTP 同期をサポートする 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。

AGD 評価者は、NTP 同期を有効化する方法についての指示をガイダンスが提供していることを確認するため、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、TOE を ESC で登録し、TOE のクロックが ESC と同じ時刻となるようにアップデートされることを検証しなければならない。評価者は、時刻源の時刻を改変し、短時間経過後に TOE のクロックが ESC 上でセットされるものと同じになるようにアップデートされることを検証しなければならない。

FPT_TUD_EXT.1 **高信頼アップデート**

本 SFR は、ND cPP から変更されていない。しかし、本 EP は、ESC または TOE ソフトウェア／ファームウェアのアップデートの情報源として機能するような、組織によって管理される別々のファイルサーバを想定することに留意されたい。評価者は、テスト環境が適切に設定されることを保証しなければならない。

保証アクティビティ

機能的に、ND cPP 用に要求されるものを超えて、一切の追加のテストは、本 SFR 用として要求されない。評価者は、TOE がその現在のバージョンを検証し、有効なアップデートを適用し、また無効なアップデートを拒否する能力を、テストすることが依然想定される。しかし、次の追加の設定ステップが VVoIP エンドポイント TOE 用にテストが実行されるために必要であるかもしれないことに留意されたい。

- 評価者は、TOE の運用環境において、ESC または専用ファイルサーバを配置する
- 評価者は、有効または無効なアップデート候補を ESC または専用ファイルサーバへロードする
- 評価者は、ソフトウェア／ファームウェア アップデートの情報源として、ESC または専用ファイルサーバを利用するように TOE を設定する

5.1.4 高信頼パス／チャネル（FTP）

FTP_ITC.1 **TSF 間高信頼チャネル**

FTP_ITC.1.1 TSF は、それ自身と**次の機能をサポートしている許可された IT エンティティ**間に：**ストリーミングメディアチャネル、呼制御チャネル、監査チャネル、ソフトウェア／ファームウェアアップデート配付チャネル*[選択：[割付：その他の能力]、その他の能力なし]*** 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通信チャネルを提供するために **[*TLS*、*[選択: IPsec*、*SSH*、*HTTPS*、*その他のプロトコルなし]*]を利用できる**なければならない。

適用上の注釈: *ND cPP は、 ST 作成者が高信頼通信を確立するために利用されるプロトコルを規定する能力を提供する。 本 EP は、TLS が ESC 及び 他の VVoIP エンドポイントとの通信をセキュアにするために利用される下位のプロトコルであるため、TLS のクライアントとして TLS を含めることを義務付けている。その他の高信頼チャネルをセキュアにするためにTLS が利用される場合、追加のプロトコルが選択されるかもしれない。例えば、TSF は、呼制御機能用にTLS を用いてESC と通信するかもしれないが、監査データのリモート送信用にその他のプロトコルを利用するかもしれない。*

FTP_ITC.1.2 TSF は、***[TSF、または 許可された IT エンティティ***] が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

FTP_ITC.1.3 TSF は、[*割付:* ***TSF が通信を開始できるようなサービス*** のリスト] のために、高信頼チャネルを介して通信を開始しなければならない。

保証アクティビティ

一切の追加のテストは、ND cPP 用に要求されるものを越えて本 SFR 用に要求されない。

FTP_TRP.1 **TSF 間高信頼チャネル**（訳注：CC パート 2 では、「高信頼パス」）

FTP_TRP.1.1 TSF は、それ自身と**許可されたリモート管理者**間に、他の通信パスと論理的に区別され、その端点の保証された識別と、[*暴露*] からの通信データの保護を提供し、**チャネルデータの改変の検知を提供**する通信パスを提供するために、**[*選択: IPsec、SSH、TLS、HTTPS*] を利用でき**なければならない。

FTP_TRP.1.2 TSF は、**リモート管理者**が、高信頼チャネル（訳注：正しくは「高信頼パス」）を介して通信を開始することを許可しなければならない。

FTP_TRP.1.3 TSF は、[*最初の管理者認証とすべてのリモート管理アクション*]に対して、高信頼チャネルを介して通信を開始（訳注：正しくは「高信頼パスの使用を要求」）しなければならない。

***適用上の注釈*：** *TOE は、一般利用者に通常利用可能でないような、TOE の特定の側面を設定する機能を提供することが要求される。 本 EP では、TSF がこれを達成するためのリモート・メカニズムを提供することを要求する。*

保証アクティビティ

一切の追加のテストは、ND cPP 用に要求されるものを越えて本 SFR 用に要求されない。

5.2 App PP セキュリティ機能要件の方向性

TOE がソフトウェアアプリケーションであり、本 EP が App PP の拡張に利用されるような場合に、ST 作成者は、本 EP によって要求される機能を提供するために、確実な選択や割付を行い、確実なオプション要件を含める必要がある。 本セクションは、本 EP への適合主張するために、ベース PP においてどのような主張が必要であるかについての指示を提供する。

App PP への参照であるような、本セクションの要件のために、完全な保証アクティビティは、繰り返されない; App PP ですでに取り込まれているものを補足するために必要な追加テストのみが含まれる。

5.2.1 暗号サポート（FCS）

FCS_TLSC_EXT.2　　認証を伴う TLS クライアントプロトコル

本 SFR は、App PP ではオプションであるが、VVoIP 通信は、暗号化と認証の両方を用いて、セキュアにされなければならないので、本 EP によって義務付けられる。

保証アクティビティ

一切の追加のテストは、ND cPP 用に要求されるものを越えて本 SFR 用に要求されない。

5.2.2 セキュリティ管理（FMT）

FMT_SMF.1　　管理機能の特定

FMT_SMF.1.1　TSF は、以下の管理機能を実行することができなければならない:

[選択:

- *管理機能なし。*
- *システムのハードウェア、ソフトウェア、または設定を記述する情報の送信を有効化／無効化する、*
- *あらゆる PII の送信を有効化／無効化する、*
- *あらゆるアプリケーション状態（例、クラッシュダンプ）の情報の送信を有効化／無効化する、*
- *ネットワークバックアップ機能[割付：企業または商用クラウドバックアップシステムのリスト] を有効化／無効化する、*
- ***アイドルコールの終了時間を設定する、***
- ***利用されるボコーダを規定する、***
- *[割付: TSF によって提供されるその他の管理機能のリスト]]*

適用上の注釈:　*本 EP は、ST 作成者が VVoIP エンドポイント機能に特に関連する設定可能な機能を選択する能力を提供するため、ベース PP の既存の*

FMT_SMF.1 SFR を変更する。デフォルトで SFR を満たすようなやり方で、TSF が自動的に動作するような場合、これらの機能は設定可能ではないことに留意されたい。

保証アクティビティ

TSS App PP によって要求されるものを超えて、本 SFR に対する TSS アクセヒビティは一切ない。

AGD App PP によって要求されるものを超えて、本 SFR に対する AGD 評価アクセヒビティは一切ない。

テスト 本 EP のセクション 5.2 と 5.3 の SFR への適合は、TOE が TOE 機能を管理するのに十分な手段を提供していることを実証することで十分である。

5.2.3 TSF の保護(FPT)

FPT_TUD_EXT.1 高信頼アップデート

本 SFR は、App PP から変更されていない。しかし、本 EP は、ESC やその他のサーバが TOE ソフトウェア／ファームウェアアップデートの情報源として機能すると想定していることに留意されたい。 評価者は、テスト環境が適切に設定されることを保証しなければならない。

保証アクティビティ

機能的には、App PP 用に要求されるものを超えて、一切の追加のテストは本 SFR 用に要求されない。 評価者が、TOE による現在のバージョンを検証し、有効なアップデートを適用し、無効なアップデートを拒否し、プラットフォームがサポートするパッケージマネージャによって利用される形式でアップデートを受信し、削除に際してそれ自体のすべてのトレースを削除し、それ自身の実行可能コードの改変をブロックする能力をテストすると期待されている。しかし、次の追加の設定ステップが、このテストが VVoIP エンドポイント TOE に対して実行されるために、必要である可能性があることに留意されたい。

- 評価者は、TOE の運用環境において、ESC または専用ファイルサーバを配置する
- 評価者は、有効なアップデート候補と無効なアップデート候補を ESC または専用ファイルサーバへロードする
- 評価者は、ソフトウェア／ファームウェアアップデートの情報源として、ESC または専用ファイルサーバを利用するように TOE を設定する

5.2.4 高信頼パス／チャネル（FTP）

FTP_DIT_EXT.1 **通信データの保護**

FTP_DIT_EXT.1.1 アプリケーションは、それ自身と別の信頼できる IT 製品の間で [***TLS***、*[選択:HTTPS、DTLS、SSH、**SRTP**、**他のプロトコルなし**]* を用いてすべての送信データを暗号化] しなければならない。

適用上の注釈: *App PP は、ST 作成者が高信頼通信を確立するために利用されるプロトコルを規定する能力を提供する。本 EP は、TLS が ESC 及び 他の VVoIP エンドポイントとの通信をセキュアにするために利用される下位のプロトコルであるため、TLS のクライアントとして TLS を含めることを義務付けている。その他の高信頼チャネルをセキュアにするために利用される場合、追加のプロトコルが選択されてもよい。例えば、TSF は、呼制御機能のために TLS を用いるが、監査データのリモート送信のためにその他のプロトコルを用いて ESC と通信してもよい。*

App PP は、高信頼チャネル（TOE から信頼される第三者へ） 及び高信頼パス（管理者から TOE へ）のための別々の SFR を定義していないので、FTP_DIT_EXT.1 は、適切なプロトコルがそれぞれ選択されるべきであるような両方のユースケースをカバーすると想定される。

保証アクティビティ

App PP によって要求されるものを超えて、本 SFR に対する追加のテストは一切ない。

5.3 TOE 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（SFR）は、本 EP が ND cPP や App PP の拡張として利用されるかどうかにかかわらず、TSF が満たすと期待されるようなものである。

SFR は、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、追加の拡張機能コンポーネントと共に導出されている。

5.3.1 セキュリティ監査（FAU）

FAU_GEN.1/VVoIP **監査データ生成（VVoIP）**

FAU_GEN.1.1/VVoIP 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[選択: 最小、基本、詳細、指定なし: から一つのみ選択]レベルのすべての監査対象事象; 及び~~

c) [*表 1 に定義された監査対象事象*]

FAU_GEN.1.2/VVoIP TSF は、各監査記録において少なくとも以下の情報を記録しなければならない:

a) 事象の日付・時刻、事象の種別、サブジェクト識別情報（該当する場合）、事象の結果（成功または失敗）; 及び

b) 各監査事象種別に対して、PP/ST の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 1 で定義される追加の監査記録の内容*]。

SFR	**監査対象事象**	**追加の監査記録の内容**
FDP_IFC.1	VVoIP ピア通信の呼詳細記録（CDR）	発呼者 被呼者 通話開始時刻 通話時間
FMT_SMF.1	ESC への TOE の登録	メディアアクセス制御（MAC）アドレス
FTA_SSL.3/メディア	非アクティブによる呼の終了	発呼者終了時刻 被呼者 通話開始時刻 通話時間
FTP_ITC.1/制御	ESC への接続の確立	発呼者 被呼者 接続確立時刻
	ESC への接続の終了	接続終了時刻
FTP_ITC.1/メディア	VVoIP ピアへの接続の確立	発呼者 被呼者 VVoIP ピアへの接続時刻
	VVoIP ピアへの接続の終了	VVoIP ピアへの接続終了時刻

表 1 – 監査対象事象

適用上の注釈: *ベース PP において記述される機能に関連する監査対象事象はそこで定義されている。本 SFR は、本 EP によって義務付けられた VVoIP 関連機能の監査対象事象のみを定義する。*

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。

AGD 評価者は、ガイダンス証拠資料をチェックし、それがすべての監査対

象事象を列挙し、監査記録の様式を提供することを保証しなければならない。各監査記録の様式種別は、各フィールドの簡単な説明とともに、カバーされなければならない。 評価者は、EP によって義務付けられた、すべての監査事象の種別が記述されること、及びそのフィールドの記述には、FAU_GEN.1.2 で要求される情報と、監査事象の表において規定される追加の情報が含まれていることを確認するためにチェックしなければならない。

テスト 表 1 の各監査対象事象について、評価者は、事象の発生原因となる TOE または運用環境のいずれかにおけるアクションを実行しなければならない。 評価者は、監査対象事象が AGD 証拠と一貫する様式で生成されること、及び SFR で規定されるすべての監査記録が詳述されることを、それぞれのケースにおいて検証しなければならない。

5.3.2 通信（FCO）

FCO_VOC_EXT.1 **固定レートのボコーダ**

FCO_VOC_EXT.1.1 TSF は、固定ビットレートのボイスボコーダを用いて、ボイスメディアを送信しなければならない。

適用上の注釈: *固定ビットレートボコーダは、可変ビットレートボコーダが暗号化時に含む脆弱性を持たない固定の出力長を提供する。*

保証アクティビティ

TSS 評価者は、TSS が使用される各ボコーダを規定することを検証しなければならない。次に、評価者は、可変レートボコーダが TSF によって要求されないことを検証するために、各ボコーダの仕様を検査しなければならない。

AGD 本 SFR には AGD 評価アクティビティはない。

テスト 評価者は、TOE、ESC、ネットワークスイッチ、トラフィク スニファ、及び 2 番目の VVoIP エンドポイントを含むテスト環境を設定しなければならない。

評価者は、次に、以下のテストを実行しなければならない:

1. 評価者は、TOE と 2 番目の VVoIP エンドポイントを ESC へ登録し、登録が行われたことを検証しなければならない。
2. 評価者は、TOE を用いて 2 番目の VVoIP エンドポイントに

ダイヤルして呼を確立し、ボイス会話を保持することによって呼が確立されていることを検証しなければならない。

3. 評価者は、固定レートのボコーダが使用されていることを検証するため、スニフィングされたトラフィクをレビューしなければならない。

複数のボコーダがサポートされている場合、評価者は、それぞれのボコーダを使用するために、TOE を再設定し、それぞれのボコーダごとにステップ 1 ～ 3 を繰り返さなければならない。

5.3.3 利用者データ保護（FDP）

FDP_IFC.1 **サブセット情報フロー制御**

FDP_IFC.1.1 TSF は、[TOE によって送信されるボイス／ビデオメディア] に対して [*メディア送信方針*] を実施しなければならない。

適用上の注釈: *オンフックのボイスとビデオが TOE からストリーミングしてはならないときの状態がある。*

保証アクティビティ

TSS 評価者は、ストリーミングメディア状態でないとき、ストリーミングメディアが伝送されない方法について TSS に記述されていることを検証しなければならない。

AGD 本 SFR には AGD 評価アクティビティはない。

テスト 本 SFR は、FDP_IFF.1 と併せて評価される。

FDP_IFF.1 **情報フロー制御機能（訳注：CC パート 2 では「単純セキュリティ属性」）**

FDP IFF.1.1 TSF は、以下のタイプのサブジェクト及び情報セキュリティ属性に基づいて、[*メディア送信方針*] を実施しなければならない。: [*ESC 登録状態及び TOE フック状態*]

FDP IFF.1.2 TSF は、以下の規則が保持されていれば、制御された操作を通じて、制御されたサブジェクトと制御された情報間の情報フローを許可しなければならない: [

- *TOE が ESC に登録される、*
- *テレフォニーデバイス（VVoIP エンドポイント）と呼が確立された、*
- *TOE がオフフック状態である、*

- *TOE がミュート状態ではない、*
- ***[選択: TOE が保留状態ではない、***
- ***TOE がオフフック状態である、***
- ***その他の規則なし]***]。

FDP_IFF.1.3 TSF は、[*追加の情報フロー制御方針規則なし*] を実施しなければならない。

FDP_IFF.1.4 TSF は、以下の規則:*[追加の規則なし]* に基づいて、情報フローを明示的に許可しなければならない。

FDP_IFF.1.5 TSF は、以下の規則:[*TOE が使用するすべての TCP ポートと UDP ポートをアクティブでないときは閉じる*]に基づいて、情報フローを明示的に拒否しなければならない。

適用上の注釈: *ストリーミングメディアが使用中でないとき、無人のボイスまたはビデオは TOE から送信されるべきではない。*

保証アクティビティ

TSS 評価者は、TOE のメディア送信方針の実施、及び TSF がボイス／ビデオデータを運用環境へ送信するために必要な条件について、TSS に記述されていることを検証しなければならない。

AGD 本 SFR には AGD 評価アクティビティはない。

テスト 評価者は、TOE、ESC、ネットワークスイッチ、トラフィク スニファ、及び 2 番目の VVoIP エンドポイントを含むような、テスト環境をセットアップしなければならない。

評価者は、次に以下のテストを実行しなければならない:

テスト 1:

1. 評価者は、TOE を ESC に登録することなく、オンフック状態にしなければならない。 評価者は、ストリーミングメディアトラフィクが TOE によって送信されないことを観測するためにスニファを利用しなければならない。

テスト 2: 評価者は、以下の追加のステップで、上記のテスト 1 を繰り返さなければならない。

1. 評価者は、TOE をオフフック状態にし、いかなるストリーミングメディアトラフィクも送信しないことを検証しなければならな

い。

テスト 3:

1. 評価者は、TOE を ESC に登録しなければならず、現在の TOE 接続で ESC 画面をチェックして、スニファを用いて呼制御パスのトラフィクを閲覧することによって TOE が登録されていることを検証しなければならない。
2. 評価者は、TOE をオンフック状態にしなければならず、スニファを用いて、ストリーミングメディアトラフィクが TOE によって送信されないことを検証しなければならない。

テスト 4: 評価者は、以下の追加のステップで、上記のテスト 3 を繰り返さなければならない。

1. 評価者は、TOE をオフフック状態にしなければならない。評価者は、次に TOE がストリーミングメディアトラフィクを引き続き送信しないことを検証しなければならない。

テスト 5:

1. 評価者は、TOE を ESC に登録しなければならず、現在の TOE 接続で ESC 画面をチェックして、スニファを用いて呼制御パスのトラフィクを確認することによって TOE が登録されていることを検証しなければならない。
2. 評価者は、ESC に 2 番目の VVoIP エンドポイントを登録しなければならず、現在の接続で ESC をチェックして、呼制御パスのトラフィクを検証するためにスニファを用いて、それが登録されていることを検証しなければならない。
3. 評価者は、2 番目の VVoIP エンドポイントにダイヤルし、通話を接続するために TOE を利用しなければならない。評価者は、エンドポイントとのボイス／ビデオ通話を行うこと及びメディアチャネルを介して 2 つのエンドポイント間でトラフィクの安定した流れが送信中であることを検証するためにスニファを用いることによって、接続がなされていることを検証しなければならない。

テスト 6:

1. 評価者は、TOE を ESC に登録しなければならず、現在の TOE 接続で ESC 画面をチェックすること、及び呼制御パスのトラフィクを検証するためにスニファを用いることによって、そ

れが登録されることを検証しなければならない。

2. 評価者は、ESC に 2 番目の VVoIP エンドポイントを登録しなければならず、現在の接続で ESC をチェックすること、及び呼制御パスのトラフィクを検証するためにスニファを用いることによって、それが登録されることを検証しなければならない。
3. 評価者は、2 番目の VVoIP エンドポイントにダイヤルし、呼接続するために TOE を利用しなければならない。 評価者は、エンドポイントとのボイス／ビデオ通話を行うこと、及びストリーミングメディアチャネルを介して TOE とその他のエンドポイント間でメディアストリーミングトラフィクが送信中であることを検証するためにスニファを用いることによって、接続がなされていることを検証しなければならない。
4. 評価者は、通話をミュートするために TOE を利用しなければならず、一切のトラフィクが TOE から 2 番目の VVoIP エンドポイントへメディアチャネルを介して送信されないことを検証しなければならない。 評価者は、ミュート制御メッセージが ESC へ送信され、ESC が応答することについても検証しなければならない。
5. 評価者は、通話をミュートから解除するために TOE を利用しなければならず、TOE と 2 番目の VVoIP エンドポイント間のストリーミングメディアトラフィクが再開されることを検証しなければならない。

テスト 7:

1. 評価者は、TOE を ESC に登録して、オンフック状態にしなければならない。
2. 評価者は、TSF によって利用されるすべての範囲の TCP ポートにおいて TOE への接続を試行するためにファジングツールを利用しなければならない。 TOE によって利用されるすべてのポートは、ESC と通信するために利用されるポートを除いて閉じられるべきである。

テスト 8:

1. 評価者は、TOE と 2 番目の VVoIP エンドポイントの両方を ESC へ登録しなければならない。
2. 評価者は、TOE をオンフック状態にしなければならない。
3. 評価者は、TSF が利用するすべての範囲の UDP ポートに

おいて TOE への接続を試行するため、ファジングツールを利用しなければならない。TOE によって利用されるすべてのポートは、閉じられるべきである。

4. 評価者は、2 番目の VVoIP エンドポイントへ呼を発信し、呼が確立されることを検証しなければならない。 評価者は、メディアトラフィクを伝送するために TOE によって利用されるポートを決定するため、そのトラフィクをスニフィングしなければならない。
5. 評価者は、呼を切断し、TOE がオンフック状態に戻ったことを検証しなければならない。
6. 評価者は、ステップ 4 でメディアトラフィクを伝送するために利用されたポートが閉じられたことを検証するため、ファジングアクティビティを実行しなければならない。

テスト 9（条件付き）

1. TSF が保留状態の利用をサポートする場合、評価者は、呼を保留するため TOE を利用し、一切のストリーミングメディアトラフィクがメディアチャネルを介して TOE から送信されないことを検証しなければならない。評価者は、VVoIP エンドポイント保留呼制御が ESC へ送信されることについても検証しなければならない。
2 評価者は、呼を保留から解除するために TOE を利用しなければならず、TOE と 2 番目の VVoIP エンドポイント間のストリーミングメディアトラフィクが再開されることを検証しなければならない。

5.3.4 TOE アクセス（FTA）

FTA_SSL.3/Media　　TSF 起動による終了（メディアチャネル）

FTA_SSL.3.1/Media　TSF は、[*[割付：デフォルトの秒数]* 秒、設定中に TOE へダウンロードされた[*選択：ESC、設定サーバ*] 上にある管理者が設定可能な時間間隔]後に、**ボイス／ビデオ送信**を終了しなければならない。

適用上の注釈：　*本 SFR は、ピアとの接続が失われた場合のメディアデータの潜在的な許可されない暴露を軽減することを意図としている。*

保証アクティビティ

TSS　評価者は、設定サーバとして動作する ESC またはスタンドアロンの

設定サーバのいずれかから設定をダウンロードする能力はもちろん、待機している呼を終了するためにTSFが利用するだろうデフォルトの時間間隔をTSSが規定することを検証しなければならない。

AGD 本 SFR には AGD 評価アクティビティはない。

テスト 評価者は、TOE、ESC、設定サーバ（待機タイムアウト時間の設定変更を伝えるために利用される場合）、ネットワークスイッチ、トラフィクスニファ、及び 2 番目の VVoIP エンドポイントを含むようなテスト環境をセットアップしなければならない。

評価者は、次に以下のテストを実行しなければならない:

テスト 1:

1. TOE をデフォルト設定で配置する（即ち、待機タイムアウト値へ適用されるあらゆる管理上の上書きなし）。
2. TOE を ESC に登録し、ESC 上でその状態を閲覧し、呼制御パスのトラフィクをスニフィングすることによって、それが登録されることを検証する。
3. 2 番目の VVoIP エンドポイントを ESC に登録し、ESC 上でそのステータスを閲覧し、呼制御パスのトラフィクをスニフィングすることによって、それが登録されることを検証する。
4. 2 番目の VVoIP エンドポイントにダイヤルするために TOE を利用し、呼を確立する。 2 つのピア間の会話を保持し、それらの間で送信されるストリーミングメディアトラフィクをスニフィングすることによって、呼が確立されたことを検証する。
5. 呼がアクティブである間に、2 番目の VVoIP エンドポイントの電源を切る。TOE が、ST で規定されるデフォルト時間間隔の後にメディアの送信を停止することを観測する。

テスト 2:

1. TOE をデフォルト設定で配置する（即ち、待機タイムアウト値へ適用されるあらゆる管理上の上書きなし）。
2. TOE を ESC に登録し、ESC 上でその状態を閲覧し、呼制御パスのトラフィクをスニフィングすることによって、それが登録されることを検証する。
3. ESC または設定サーバ（TOE によってサポートされているものに依存する）を利用して、TOE の待機タイムアウト期間をサポートされる最短時間間隔に設定する。

4. 2 番目の VVoIP エンドポイントを ESC に登録し、ESC 上でそのステータスを閲覧し、呼制御パスのトラフィクをスニフィングすることによって、それが登録されることを検証する。
5. 2 番目の VVoIP エンドポイントにダイヤルするために TOE を利用し、呼を確立する。 2 つのピア間の会話を保持し、それらの間で送信されるストリーミングメディアトラフィクをスニフィングすることによって、呼が確立されたことを検証する。
6. 呼がアクティブである間に、2 番目の VVoIP エンドポイントの電源を切る。TOE が、ステップ 3 で設定された時間間隔の後にメディアの送信を停止することを観測する。

テスト 3:

1. テスト 2 を繰り返すが、ステップ 3 で、待機タイムアウト値を、サポートされる最短時間ではなく、サポートされる最長時間に設定する。

5.3.5 高信頼パス／チャネル（FTP）

FTP_ITC.1/Control　TSF 間高信頼チャネル(シグナリングチャネル)

FTP_ITC.1.1/Control　TSF は、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、それ自身とエンタープライズセションコントローラ間の高信頼通信チャネルを提供するために、**[*選択：SIP、H.323*] を利用できる**なければならない。

適用上の注釈:　*SIP と H.323 プロトコルの両方は、TLS に依拠する。本 SFR は、呼制御機能をセキュアにするために利用されるアプリケーションレイヤプロトコルを定義する。*

FTP_ITC.1.2／Control　TSF は、[***TSF、エンタープライズセションコントローラ***] が、高信頼チャネルを介して通信を開始するのを許可しなければならない。

FTP_ITC.1.2／Control　TSF は、[*呼制御の確立*] のために、高信頼チャネルを介して通信を開始しなければならない。

適用上の注釈:　*呼制御チャネルは、TLS を用いてセキュアにされる。*

保証アクティビティ

TSS　評価者は、TLS を用いて SIP 及び／または H.323 を利用する

TOE の能力について TSS に記述されていることを検証する。

AGD 本 SFR には AGD 評価アクティビティはない。

テスト 本 SFR は、ND cPP で定義されるとおり FTP_ITC.1 の繰り返しである。評価者は、SFR の繰り返しのため ND cPP で FTP_ITC.1 用に定義された保証アクティビティを繰り返さなければならない。
具体的には、SIP または H.323 通信のいずれかがセキュアであることを実証するため、評価者は、呼のセットアップ／解除が TLS を介して実行されることを実証する必要がある。

FTP_ITC.1/Media TSF 間高信頼チャネル（メディアチャネル）

FTP_ITC.1.1/Media TSF は、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、それ自身と別の VVoIP エンドポイントまたは他のテレフォニーデバイス間の高信頼通信チャネルを提供するために、[***選択：SRTP、H.235/H.323***] **を利用できる**なければならない。

適用上の注釈: *本 SFR は、別の VVoIP エンドポイントまたは電話会議デバイスのような他のテレフォニーデバイス間で、一度呼が確立されると、ボイス／ビデオの送信をセキュアにするために利用されるアプリケーションレイヤプロトコルを定義する。*

FTP_ITC.1.2/Media TSF は、[***TSF、別の VVoIP エンドポイントまたは他のテレフォニーデバイス***] が高信頼チャネルを介して通信を開始することを許可しなければならない。

FTP_ITC.1.3/Media TSF は、[ボイス／*ビデオメディア*] のために、高信頼チャネルを介して通信を開始しなければならない。

適用上の注釈: *対応する高信頼メディアチャネルは、以下の高信頼制御チャネルと合致するように選択されなければならない：SIP-SRTP、H.323-H.323 / H.235。*

保証アクティビティ

TSS 評価者は、高信頼チャネルが SRTP または H.323 ／ H.235 を使用することを検証しなければならない。

AGD 本 SFR には AGD 評価アクティビティはない。

テスト 本 SFR は、ND cPP で定義されるとおり FTP_ITC.1 の繰り返しである。評価者は、SFR の繰り返しのため ND cPP で FTP_ITC.1 用に定義された保証アクティビティを繰り返さなければならない。

5.4　TOE セキュリティ保証要件

ND cPP または App PP の EP として、本 EP は、ベース PP で定義されたものを超えるような SAR を規定しない。評価者は、主張されたベース PP で定義された SAR が TSF 全体に対して適切なものとして評定されることを保証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 2 で示されるように、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。さらに、附属書 A、附属書 B、及び附属書 C で規定される 3 つのその他の種別の要件がある。最初の種別（本附属書）は、ST に含めることが可能な要件であるが、TOE 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。第 2 の種別（附属書 B）は、本 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た場合、その附属書の追加の要件が含まれなければならない。第 3 の種別（附属書 C）は、本 EP へ適合するために要求されないコンポーネントであるが、本 EP の将来のバージョンでベースライン要件に含まれるだろうコンポーネントであり、したがってベンダによる採用が推奨される。ST 作成者は、附属書 A、附属書 B、及び附属書 C の要件と関連するかもしれないような要件であるが列挙されていない要件（例、FMT 種別の要件）についてもまた、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。

A.1 セキュリティ監査 （FAU）

FAU_STG_EXT.1 保護された監査事象格納

TOE が ND cPP ではなく App PP への適合を主張する場合、以下の SFR が ST に含まれるものとする。

FAU_STG_EXT.1.1 TSF は、生成された監査データを **FTP_DIT_EXT.1** に従って高信頼チャネルを用いて **TOE が登録されたエンタープライズセションコントローラ**へ送信できなければならない。

FAU_STG_EXT.1.2 TSF は、生成された監査データを[***選択：TOE、TOE プラットフォーム***] 自体に格納できなければならない。

FAU_STG_EXT.1.3 TSF は、監査データ用のローカル格納領域が満杯であるとき、*[選択：新しい監査データを破棄、以下の規則に従って以前の監査記録を上書き:[割付：以前の監査記録を上書きするための規則]、[割付：その他のアクション]]* できなければならない。

適用上の注釈: *本 SFR は、App PP TOE が物理的ディスクストレージを含まないので、TOE 境界内の代わりにそのホストプラットフォーム（即ち、OS ファイルシステム）上にローカルに監査データを TSF が格納することを許可するのを除き、ND cPP で定義されるとおりFAU_STG_EXT.1 と機能的に同一である。*

保証アクティビティ

ND cPP のサポート文書における本 SFR の保証アクティビティを参照されたい。

附属書 B. 選択ベースの要件

本 EP の概説で示されるように、ベースライン要件（TOE または下位のプラットフォームによって実行されなければならないもの）が、本 EP の本文に含まれている。 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と、以下の追加の要件が含まれる必要がある。

FCS_SRTP_EXT.1　　セキュア リアルタイム トランスポート プロトコル

SRTP が FTP_DIT_EXT.1 及び／または FPT_ITC.1/Media で選択される場合、以下の SFR が ST に含まれなければならない：

FCS_SRTP_EXT.1.1　TSF は、RFC 3711 に適合するセキュアリアルタイムトランスポートプロトコル (SRTP) を実装しなければならず、SRTP 接続用の鍵情報を提供するため RFC 4568 に適合するメディアストリーム用セキュリティ記述 (SDES) を利用しなければならない。

FCS_SRTP_EXT.1.2　TSF は、RFC 4568 に従って以下の暗号スイートをサポートする SDES-SRTP を実装しなければならない：AES_CM_128_HMAC_SHA1_80。

FCS_SRTP_EXT.1.3　TSF は、SRTP NULL アルゴリズムが無効化できることを保証しなければならない。

FCS_SRTP_EXT.1.4　TSF は、SRTP 通信に利用される SRTP ポートが許可された管理者によって規定されることを許可しなければならない。

適用上の注釈:　*本要件は、VoIP トラフィクを搬送するために用いられる SRTP セションが、識別された暗号スイートを用いた SDES ダイアログに従って鍵付きにされることを規定する。将来は、Suite B 暗号スイートが利用可能となる。*

保証アクティビティ

TSS　評価者は、SRTP セションが着呼及び発呼の両方に対して、どのようにネゴシエーションされるかについて 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。 これには、鍵材料が確立される方法、NULL アルゴリズムまたはその他の許可されない暗号スイートを利用する要求が TSF によって拒否される方法が含まれる。

AGD　本 SFR には AGD 評価アクティビティはない。

テスト　評価者は、デバイスが着信と発信を行う準備ができるように、それらのデバイスを初期化するための手順に従わなければならない。 評価者は、次に呼の発信と着信の両方を行って、TOE によって送信及び受信されるトラフィクが暗号化されていることを決定しなければ

ならない。呼が暗号化されることを保証するため、また使用されている暗号スイートを目視するため、パケットキャプチャツールを利用するべきである。TLS-SIP トラフィクを復号し、SDES ネゴシエーションを目視するため、SIP サーバのプライベート鍵がパケットキャプチャツールへロードされる必要がある。

附属書 C. オブジェクティブ要件

本附属書は、脅威にも対抗するセキュリティ機能を規定する要件が含まれる。これらの要件は、商用の技術においてまだ広く利用可能でないセキュリティ機能を記述しているため、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、TOE が依然として本 EP に適合するように ST へ含まれてもよいし、またできるだけ早くそれらが含まれることが期待される。

現時点では、VVoIP エンドポイント TOE に特有のオブジェクティブ要件は、一切識別されていない。

附属書 D. エントロピー証拠資料と評定

TOE は、ND cPP/App PP の「エントロピー証拠資料と評定」のセクションに概説される要件を超えて、そのエントロピー源を記述するための追加の補足情報を要求しない。その他のベース PP 要件と共に、唯一の追加の要件は、エントロピー証拠資料がベース PP によって要求される機能に加えて、TOE の具体的な VVoIP エンドポイント機能へ適用されることである。

附属書 E. 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。
[NDcPP]	• 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、バージョン 1.0、2015 年 2 月 27 日。
[App PP]	• アプリケーションソフトウェアのプロテクションプロファイル、バージョン 1.2、2016 年 4 月 22 日。

附属書 F. 略語

略語	意味
DHCP	ダイナミック ホスト コンフィギュレーション プロトコル (Dynamic Host Configuration Protocol)
ESC	エンタープライズセションコントローラ (Enterprise Session Controller)
IETF	インターネット技術タスクフォース(Internet Engineering Task Force)
IP	インターネットプロトコル(IP)
ITU-T	国際電気通信連合・通信部門 (International Telegraph Union – Telecommunication Standardization Sector)
ND cPP	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 (Collaborative Protection Profile for Network Devices)
NTP	ネットワークタイムプロトコル(Network Time Protocol)
PII	個人情報(Personally Identifiable Information)
PP	プロテクションプロファイル(Protection Profile)
SIP	セション確立プロトコル(Session Initiation Protocol)
SRTP	セキュアリアルタイムトランスポートプロトコル (Secure Real-Time Transport Protocol)
TCP	伝送制御プロトコル (Transmission Control Protocol)
TFTP	トリビアル ファイル トランスファー プロトコル (Trivial File Transfer Protocol)
UDP	ユーザ データグラム プロトコル (User Datagram Protocol)
VVoIP	ボイス/ビデオ オーバー インターネット プロトコル(Voice/Video over IP)