(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2014-96830
(P2014-96830A)
(43)公開日　平成26年5月22日(2014.5.22)

(51)Int.Cl.		F I		テーマコード（参考）
H04W 12/06	(2009.01)	H04W 12/06		5J104
H04W 84/10	(2009.01)	H04W 84/10		5K067
G09C 1/00	(2006.01)	G09C 1/00	640E	

審査請求 有　請求項の数 20　ＯＬ　（全 70 頁）

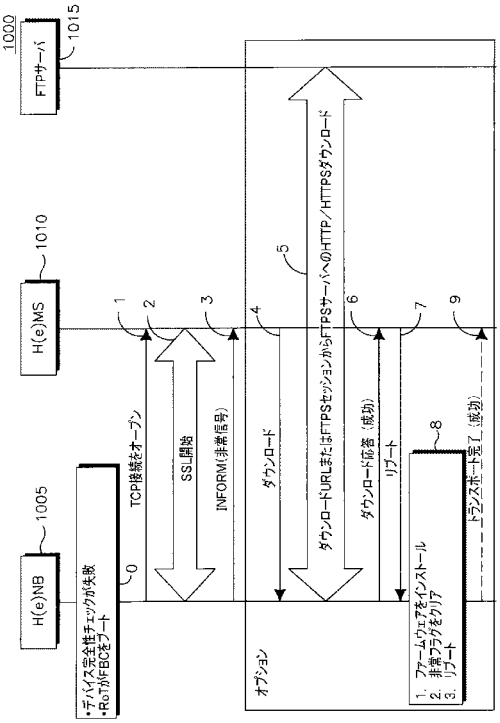
(21)出願番号　特願2014-427 (P2014-427)
(22)出願日　平成26年1月6日 (2014.1.6)
(62)分割の表示　特願2011-553138 (P2011-553138)の分割
原出願日　平成22年3月5日 (2010.3.5)
(31)優先権主張番号　61/157,833
(32)優先日　平成21年3月5日 (2009.3.5)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/222,067
(32)優先日　平成21年6月30日 (2009.6.30)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　61/235,793
(32)優先日　平成21年8月21日 (2009.8.21)
(33)優先権主張国　米国 (US)

(71)出願人　510030995
インターデイジタル　パテント　ホールディングス　インコーポレイテッド
アメリカ合衆国　１９８０９　デラウェア州　ウィルミントン　ベルビュー　パークウェイ　２００　スイート　３００
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　サディール　ビー．パッター
アメリカ合衆国　０８０５４　ニュージャージー州　マウント　ローレル　アン　ドライブ　１７

最終頁に続く

(54)【発明の名称】Ｈ（ｅ）ＮＢ完全性検証および妥当性確認のための方法および機器

(57)【要約】
【課題】自律的妥当性確認および半自律的妥当性確認を用いる、Ｈ（ｅ）ＮＢの完全性の妥当性確認を可能にする機器および方法を提供する。
【解決手段】無線送信／受信装置（ＷＴＲＵ）において実施される、ＷＴＲＵの完全性検証を実施する方法は、ＷＴＲＵのコンポーネントについて完全性メトリックを測定するステップと、ＷＴＲＵ上の安全なローカルストレージから信頼できる参照値（ＴＲＶ）を取り出すステップであって、ＴＲＶが本来、安全なローカルストレージに格納されている、ステップと、測定された完全性メトリックをＴＲＶと比較して、コンポーネントの完全性検証チェックの結果を判定するステップと、コンポーネントの完全性検証チェックの結果をプラットフォーム妥当性確認エンティティ（ＰＶＥ）に報告するステップであって、ＰＶＥ及びＷＴＲＵがネットワーク上の別個のエンティティである、ステップを含む。
【選択図】図１０



【特許請求の範囲】
【請求項１】
無線送信／受信装置（ＷＴＲＵ）の完全性検証を実施する方法であって、前記ＷＴＲＵにおいて実施する、
前記ＷＴＲＵにおいて、前記ＷＴＲＵのコンポーネントについて完全性メトリックを測定するステップ、
前記ＷＴＲＵにおいて、前記ＷＴＲＵ上の安全なローカルストレージから信頼できる参照値（ＴＲＶ）を取り出すステップであって、前記ＴＲＶが本来、前記安全なローカルストレージに格納されている、ステップ、
前記ＷＴＲＵにおいて、前記測定された完全性メトリックを前記ＴＲＶと比較して、前記コンポーネントの完全性検証チェックの結果を判定するステップ、及び、
前記ＷＴＲＵにおいて、前記コンポーネントの前記完全性検証チェックの前記結果をプラットフォーム妥当性確認エンティティ（ＰＶＥ）に報告するステップであって、前記ＰＶＥ及び前記ＷＴＲＵがネットワーク上の別個のエンティティである、ステップ、
を含むことを特徴とする方法。
【請求項２】
請求項１に記載の方法において、ソフトウェア機能性及び関連付けられた属性のリストを前記プラットフォーム妥当性確認エンティティ（ＰＶＥ）に送るステップをさらに含み、該属性が参照完全性メトリックと重大度の少なくとも一方を含むことを特徴とする方法。
【請求項３】
請求項２に記載の方法において、ソフトウェア機能性及び関連付けられた属性の前記リストが、デバイス構成データシートに含まれることを特徴とする方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本出願は通信に関する。
【背景技術】
【０００２】
関連出願の相互参照
本出願は、あたかも本明細書に完全に記載されているかのように、すべてが参照によって組み込まれている、２００９年３月５日に出願した米国特許仮出願第61/157,833号明細書、２００９年６月３０日に出願した米国特許仮出願第61/222,067号明細書、２００９年８月２１日に出願した米国特許仮出願第61/235,793号明細書、および２００９年９月３日に出願した米国特許仮出願第61/239,698号明細書の利益を主張する。本出願は、あたかも本明細書に完全に記載されているかのように、参照によって組み込まれている、同時に出願した、「Platform Validation and Management of Wireless Devices」という名称の米国特許出願第12/718,480号明細書に関連する。
【０００３】
フェムトセルとしても知られているＨ（ｅ）ＮＢ（ｈｏｍｅ　ｅｖｏｌｖｅｄ　Ｎｏｄｅ　Ｂ）は、概して、ホスティング側（ＨＰ）と呼ばれる関係者の構内または宅内に置かれる３Ｇネットワークへの小型の可搬型アクセスポイントである。Ｈ（ｅ）ＮＢは、小さい、指定された地理的エリア内の移動通信およびサービスのための仲介となる。Ｈ（ｅ）ＮＢは、構内または工場環境など、従来は（不良無線条件のせいで）アクセス不可能だったエリア内でモバイルサービスを提供するのに使われ得る。Ｈ（ｅ）ＮＢはブロードバンドインターネットおよびモバイルネットワークへの統一アクセスポイントになり得るので、Ｈ（ｅ）ＮＢは、ＳＯＨＯ（small office home office）セクタ用の選択肢でもある。
【０００４】
本出願は、具体的なセキュリティ要件を提起し得る。例えば、こうしたデバイスは、ｉ）モバイルハンドセットが従来見なされていたような、極秘データの格納および取扱いの

ための閉じた、不変の環境とはもはや見なされず、ｉｉ）こうした特殊デバイスは一般に、Ｈ（ｅ）ＮＢの主たる関係者として、Ｈ（ｅ）ＮＢを操作して移動通信端末のユーザにサービスを提供するモバイルネットワークオペレータ（ＭＮＯ）の直接の物理的制御下にはなく、ｉｉｉ）こうしたデバイスは概して、安全でないリンクを介して、また、継続的であるよりもむしろ断続的であり得るようにコアネットワークに接続される。

【０００５】

モバイル通信ネットワークの既存または標準化された技術は、ネットワークが、それが操作するＨ（ｅ）ＮＢが、Ｈ（ｅ）ＮＢが従来の認証ステップを通った場合でさえも、信用できるものになると十分に見なすための方法を提供することができない。したがって、必要とされるものは、ＭＮＯがデバイスの信用性、すなわち、完全性を認証（authenticate）し、且つ妥当性確認（validate）し、このようなデバイスを管理しプロビジョニングするのを助ける方法である。

【発明の概要】

【０００６】

自律的妥当性確認および半自律的妥当性確認を用いる、Ｈ（ｅ）ＮＢ（home evolved node-B）完全性の妥当性確認を可能にする機器および方法を本明細書で開示する。

【図面の簡単な説明】

【０００７】

添付の図面とともに、例として挙げられる以下の説明により、より詳細に理解することができよう。

【図１】モジュール、機能性およびコンポーネントの編成例を示す図である。

【図２】コンポーネントおよび機能性の編成例を示す図である。

【図３】ソフトウェアダウンロード用プロビジョニングのためのＴＲ０６９アーキテクチャ例を示す図である。

【図４】基本的な完全性測定および報告の例を示す図である。

【図５】完全性レポートおよび参考資料の例を示す図である。

【図６】妥当性確認レポートと参照マニフェストとの比較の例を示す図である。

【図７】参照マニフェスト中のコンポーネント情報の例を示す図である。

【図８】証明書管理アーキテクチャの例を示す図である。

【図９】Ｈ（ｅ）ＮＢ（home evolved-Node B）（Ｈ（ｅ）ＭＳ）の再構成の例を示す図である。

【図１０】自律的妥当性確認（ＡｕＶ）修復の例を示す図である。

【図１１】ファイルパッケージ形式の例を示す図である。

【図１２】半自律的妥当性確認（ＳＡＶ）のネットワークアーキテクチャ例を示す図である。

【図１３Ａ】ＳＡＶプロシージャのためのフローチャート例を示す図である。

【図１３Ｂ】ＳＡＶプロシージャのためのフローチャート例を示す図である。

【図１４】ＳＡＶ修復のためのフローチャート例を示す図である。

【図１５】完全性チェックの結果例を示す図である。

【図１６】失敗した機能性のリスト例を示す図である。

【図１７Ａ】プラットフォーム妥当性確認および管理（ＰＶＭ）のためのエンティティセットおよびその関係並びにインタフェースの例を示すブロック図である。

【図１７Ｂ】ＰＶＭのためのエンティティセットおよびその関係並びにインタフェースの別の例を示すブロック図である。

【図１８Ａ】プラットフォーム妥当性確認エンティティを用いる妥当性確認の方法例を示す信号図である。

【図１８Ｂ】プラットフォーム妥当性確認エンティティを用いる妥当性確認の方法例を示す信号図である。

【図１８Ｃ】プラットフォーム妥当性確認エンティティを用いる妥当性確認の方法例を示す信号図である。

【図１９】ＬＴＥワイヤレス通信システム／アクセスネットワークを示す図である。
【図２０】ＬＴＥワイヤレス通信システムを示す例示的なブロック図である。
【発明を実施するための形態】
【０００８】
これ以降において言及する場合、「ＷＴＲＵ（ワイヤレス送受信ユニット）」という用語は、ＵＥ（ユーザ機器）、移動局、固定もしくは移動加入者ユニット、ページャ、セルラー電話、ＰＤＡ（携帯情報端末）、コンピュータ、またはワイヤレス環境において動作することが可能な他のどのタイプのデバイスも含むが、それに限定されない。これ以降において言及する場合、「基地局（ｂａｓｅ　ｓｔａｔｉｏｎ）」という用語は、ノードＢ、サイトコントローラ、アクセスポイント（ＡＰ）、ゲートウェイ、ＣＰＥ（顧客構内機器）、またはワイヤレスもしくはワイヤライン環境において動作することが可能な他のどのタイプのインタフェースデバイスも含むが、それに限定されない。これ以降で言及する場合、「ＨＭＳ」という用語は、ＨＭＳ（Ｈｏｍｅ　ＮｏｄｅＢ　Ｍａｎａｇｅｍｅｎｔ　Ｓｙｓｔｅｍ）、ＨｅＭＳ（Ｈｏｍｅ　Ｅｎｈａｎｃｅｄ－ＮｏｄｅＢ　Ｍａｎａｇｅｍｅｎｔ　Ｓｙｓｔｅｍ）を含むが、それに限定されず、この２つはまとめて、Ｈ（ｅ）ＭＳ、デバイス管理システム（ＤＭＳ）、構成サーバ（ＣＳ）、自動構成サーバ（ＡＣＳ）、または「基地局」の構成もしくは機能性を管理する他の任意のタイプのシステムと呼ぶこともできる。「ＷＴＲＵ」および「基地局」という用語は、相互排他的ではない。例えば、ＷＴＲＵは、Ｈ（ｅ）ＮＢ（ｅｎｈａｎｃｅｄ　Ｈｏｍｅ　Ｎｏｄｅ－Ｂ）であり得る。これ以降で言及する場合、「情報理論的に安全（ｉｎｆｏｒｍａｔｉｏｎ－ｔｈｅｏｒｅｔｉｃａｌｌｙ　ｓｅｃｕｒｅ）」という用語は、完全に安全、無条件に安全、および情報理論的にほぼ安全を含むが、それに限定されない。これ以降で言及する場合、「信頼（ｔｒｕｓｔ）」、「信頼できる（ｔｒｕｓｔｅｄ）」、および「信用できる（ｔｒｕｓｔｗｏｒｔｈｙ）」という用語、並びにその変化形は、ユニットがある特定の方式で機能するかどうかを評価する、数量化可能であり観察可能な方式を示す。
【０００９】
自律的妥当性確認（ＡｕＶ）および半自律的妥当性確認（ＳＡＶ）を用いて、Ｈ（ｅ）ＮＢ（ｈｏｍｅ　ｅｖｏｌｖｅｄ　ｎｏｄｅ－Ｂ）完全性検証（ｉｎｔｅｇｒｉｔｙ　ｖｅｒｉｆｉｃａｔｉｏｎ）および妥当性確認を行う機器および方法について本明細書に記載する。ＡｕＶおよびＳＡＶに共通の詳細を記載し、続いてＡｕＶおよびＳＡＶに関して実装の詳細を記載する。
【００１０】
妥当性確認方法において使われる信頼できる参照値（ＴＲＶ）を判定する方法について本明細書に記載する。デバイス完全性検査は、妥当性確認方法に共通のプロシージャである。デバイス完全性検査用に、コンポーネントについてされた測定の完全性をチェックできるように、１組のＴＲＶが必要とされる。コンポーネントのこのような完全性検査は、コンポーネントがロードされる前に行われるべきであることが望まれ得る。このようなＴＲＶは、使われる前にそれ自体によって認証され完全性を確実にされ得ることも望まれ得る。
【００１１】
完全性チェックを実施し、ＴＲＶを提供し生成するために、異なる完全性チェック方法を用いることができる。例えば、コードに対応するＴＲＶを生成する方法は、デジタル署名方法を含んでよく、ハッシュベースのメッセージ認証コードまたは暗号化ベースのメッセージ認証コードも検討してよい。
【００１２】
デジタル署名方法について本明細書に記載する。デジタル署名方法では、公開鍵暗号技術を用いることができる。Ｈ（ｅ）ＮＢは、その私有鍵（ｐｒｉｖａｔｅ　ｋｅｙ）を使ってチェック語を暗号化することによって、モジュールのハッシュ（または、概してチェック語）にデジタル署名することができる。暗号化されたチェック語は次いで、プラットフォーム妥当性確認エンティティ（ＰＶＥ）に送られればよく、ＰＶＥにおいてＨ（ｅ）

ＮＢの公開鍵で復号し、ＴＲＶと比較することができる。ローカル完全性チェックのために、参照完全性チェックは、製造元によって署名され、Ｈ（ｅ）ＮＢ内部でローカルに検証され得る。非限定的例として、テーブル１は、幾つかのデジタル署名方法を明らかにする。

【００１３】

【表１】

名称	タイプ	特性	最小鍵サイズ
デジタル署名標準	FIPS186-2デジタル署名	SHA-1ハッシュに基づくデジタル署名。特許なし、ライセンスなし。米連邦政府の輸出規制が該当する	1024ビット
RSAデジタル署名	RSAデジタル署名(FIPS認可済み)	以前特許化済み(2000年に失効)	1024ビット
楕円曲線デジタル署名	楕円曲線デジタル署名	楕円曲線鍵技術に基づく技術	160ビット

テーブル1

【００１４】

ハッシュアルゴリズムおよびハッシュベースのメッセージ認証コードについて本明細書に記載する。ハッシングは、その入力の、一意（またはほぼ一意）および非可逆（またはほぼ非可逆）の要約を生じる単方向またはほぼ一方向の関数である。多くのケースにおけるデジタル署名は、暗号化されたハッシュに過ぎない。デジタル署名方法は、公開／私有鍵ペアを使うことができ、ＭＡＣ（メッセージ認証コード）は、共有秘密鍵を使うことができる。チェック語は、組み込まれた秘密鍵（ｓｅｃｒｅｔ　ｋｅｙ）を有するモジュール（連結されたモジュールおよび鍵）を介して作成することができる。非限定的例として、テーブル２は、幾つかのハッシュアルゴリズム並びにハッシュベースのメッセージ認証コード方法を明らかにする。

【００１５】

【表２】

名称	タイプ	特性	最小鍵サイズ
SHA-1, SHA-256, SHA-512	ハッシュアルゴリズム	FIPS認可済み	160, 256, 512ビット
普遍的メッセージ認証コード	ハッシュベースのMAC	最速ハッシュベースのアルゴリズム	32, 64, 96ビット
RACE完全性プリミティブ評価メッセージダイジェスト-160	ハッシュアルゴリズム	欧州におけるECのR&D	160ビット
TIGER(2)	ハッシュアルゴリズム	64ビットプラットフォーム上での効率的動作のために設計された	192ビット
HMAC-SHA1-96	ハッシュベースのMAC	ハッシュ用にSHA-1を使う	96ビット
WHIRLPOOL	ハッシュベースのMAC	特許化されていない	512ビット

テーブル2

【００１６】
暗号化ベースのメッセージ認証コードについて本明細書に記載する。チェック語は、ハッシュアルゴリズムによって作成し、次いで、秘密鍵を使って暗号化することができる。非限定的例として、テーブル３は、幾つかの暗号化ベースのメッセージ認証コード方法を明らかにする。
【００１７】
【表３】

名称	タイプ	特性	最小鍵サイズ
DES-CBC-MAC	暗号MAC	DESベース	64ビット
CMAC	暗号MAC	対称鍵ブロック暗号アルゴリズムを使う暗号化ベースのMAC	64, 128, 192, 256
CCM	暗号MAC	カウンタモード暗号化とともに暗号ブロック連鎖を使う	128, 192, 256

テーブル3

【００１８】
完全性メトリックは、ソフトウェアコンポーネントに対する完全性方法の実行によって生成されたダイジェスト（例えば、暗号ハッシュ値）である。コンポーネントは、本明細書において、完全性検査の最も小さい可能単位と見なされる。個々のバイナリ実行可能または事前実行可能ファイルが、コンポーネントの例である。一方、モジュールは、本明細書において、ソフトウェアパッケージの製造元が、証明し、配布するための最も小さい単位と見なされる。本説明の残りでは、概して、図１に示すように、１）コンポーネントは、常に１つまたは複数のモジュールからなることができ、２）どの１つのモジュールも、コンポーネント中に一度だけ現れる（すなわち、１つのモジュールが、２つのコンポーネント中に現れることはできない）と見なす。ＡｕＶおよびＳＡＶでのデバイス完全性チェックおよび妥当性確認をサポートするために、モジュール、重大度に対応する参照完全性メトリック（ＲＩＭ）など、ソフトウェアモジュールおよびそれに関連付けられた属性のリスト、並びに他の情報が提供されなければならない場合もある。参照完全性メトリック（ＲＩＭ）は、個々のモジュールの完全性に対する参照値として働く。ＡｕＶのケースでは、リストは、製造元によって生成し、デバイスに安全に格納することができ、ＳＡＶのケースでは、リストは、製造元によって生成し、プラットフォーム妥当性確認エンティティ（ＰＶＥ）（全モジュール）に与え、また、Ｈ（ｅ）ＮＢにプロビジョニングすることができる（多段階スタートアップ実装における段階１および段階２モジュール用）。どのようにソフトウェアモジュールが編成され、構造化され、または格納されるか、並びにこのようなモジュールのどのような種類がデバイスに存在し得るかは、Ｈ（ｅ）ＮＢ実装形態に依存してよく、共通仕様言語を使って、モジュールおよびその属性を指定することができる。
【００１９】
例えば、ＸＭＬ（拡張マークアップ言語）およびＡＳＮ．１（抽象構文記法１）ベースの方法が、共通仕様言語の実装に用いられ得る。デバイス構成データシートは、ソフトウェアモジュールおよびモジュールに関連付けられた様々な属性のリストを含む。データシートは、コンポーネントおよび機能性へのモジュールの分類も指定し得る。
【００２０】
Ｈ（ｅ）ＮＢのコンポーネントおよび／またはモジュール並びに関連付けられた属性を指定するための共通の高移植性言語を提供することができるソフトウェアモジュール属性のＸＭＬベースの仕様について本明細書に記載する。可搬的に、およびＨ（ｅ）ＮＢアーキテクチャ不問なやり方で情報を提供するために、モジュールを指定する言語が進化され

なければならない。言語は、ＸＭＬスキーマおよびＸＭＬ文書を含むＸＭＬ言語と同様でよい。モジュールの形式および様々な属性は標準化することができ、すべての製造元が、ソフトウェアモジュールを規定の形式で記述するデバイス構成データシートを提供する。形式は、ＸＭＬスキーマと同様でよく、デバイス構成データシートはＸＭＬ文書と同様でよい。ＸＭＬ署名は、完全性、メッセージ認証および／または署名者認証を行うための、デジタル署名を追加するというサポートを提供する。バイナリＸＭＬとは、より簡潔な表現であり、解析コストを削減し、且つあるエンティティから別のエンティティへの構成データの通信用の必要帯域幅を削減するための基礎として使うこともできる。ＸＭＬスキーマの例は、テーブル４に示してあり、製造元がそのモジュールを指定することができる標準形式でよい。

【００２１】

【表４】

XMLスキーマ

```
<?xml version="1.0"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:element name="Manufacturer Identification">
 <xs:complexType>
  <xs:sequence>
   <xs:element name="Name" type="xs:string"/>
   <xs:element name="URL" type="xs:string"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>

<xs:element name="Module Name">
 <xs:complexType>
  <xs:sequence>
   <xs:element name="Version" type="xs:string"/>
   <xs:element name="Stage" type="xs:string"/>
   <xs:element name="Severity" type="xs:string"/>
   <xs:element name="Author" type="xs:string"/>
   <xs:element name="Dependency" type="xs:string"/>
   <xs:element name="Integrity Algorithm" type="xs:string"/>
   <xs:element name="Reference Integrity Metric" type="xs:string"/>
  </xs:sequence>
 </xs:complexType>
</xs:element>+

<Signature ID?>
  <SignedInfo>
   <CanonicalizationMethod/>
   <SignatureMethod/>
   (<Reference URI? >
    (<Transforms>)?
    <DigestMethod>
    <DigestValue>
   </Reference>)+
  </SignedInfo>
  <SignatureValue>
 (<KeyInfo>)?
 (<Object ID?>)*
 </Signature>

</xs:schema>
```

「?」はゼロまたは一度の出現を示し、「+」は一度または複数の出現を示し、「*」はゼロ以上の出現を示す

テーブル４

【００２２】

製造元は、デバイス構成データシートを提供し、デジタル署名でシートに署名することができる。このデバイス構成データシートは、ＡｕＶ用のＨ（ｅ）ＮＢの所で維持することができる。チェックが失敗したケースでは、デバイス構成シート自体のデジタル署名が検証された場合、適切なアクションをとることができる。というのは、このことは、任意の失敗モジュールの影響についての情報を含む、ソフトウェアの属性が、ソフトウェアモジュール自体（すなわち、バイナリイメージ）が変化しており完全性検査に失敗していて

も、損なわれていないことを意味するからである。ＳＡＶのケースでは、デバイス構成シートは、デバイスおよびＰＶＥの所で維持することができる。本明細書に記載するように、ＳＡＶをサポートするための追加アクションを追加することもできる。

【００２３】

Ｈ（ｅ）ＮＢのコンポーネントおよび関連付けられた属性を指定するための共通の高移植性言語を提供することができる、ソフトウェアモジュール属性のＡＳＮ．１ベースの仕様について本明細書に記載する。遠隔通信およびコンピュータネットワーク接続において、ＡＳＮ．１は、データを表し、符号化し、伝送し、デコードするデータ構造を記述する、標準的であり柔軟な表記法である。ＡＳＮ．１は、マシン固有符号化技法に依存しないオブジェクトの構造を記述するとともに、曖昧さをなくす精密な公式表記法である公式規則セットを提供し得る。通信プロトコル用のメッセージを定義するのに一般に使われるように、ＡＳＮ．１は、それに関連付けられた符号化規則とともに、バイナリ符号化を結果的にもたらす。インターネットプロトコルであるＨＴＴＰおよびＳＭＴＰなど、他の通信プロトコルは、テキストタグおよび値を使って、時にはＡＢＮＦ（拡張バッカス－ナウア記法）表記法に基づいて、メッセージを定義する。この定義は、符号化も定義するが、テキスト形式である。

【００２４】

ＡＳＮ．１手法は、より効率的であると信じられており、圧縮符号化規則を用いて、確かにより簡潔な符号化を提供する。テキスト手法は、（テキスト列の作成および解析により）実装するのがより簡単であり、符号化されたメッセージを読むだけでよいので、デバッグするのがより簡単であると主張されている。Ｍｅｇａｃｏプロトコルのケースでは、ＡＳＮ．１およびＡＢＮＦに基づいて２つの符号化が定義された。

【００２５】

ＡＳＮ．１　ＸＭＬ符号化規則（ＸＥＲ）は、ＡＳＮ．１表記法を使って定義されたデータ構造のテキスト符号化を可能にする。ユーザとの間でデータを提示し入力するという唯一の目的のために、一般的文字列符号化規則も定義された。デバイス完全性メトリックを伝達するＡＳＮ．１の例を、テーブル５に示すことができる。

【００２６】

【表５】

ASN.1

```
DeviceIntegrityMeasurementsType DEFINITIONS ::= BEGIN
        ManufacturerIdentification ::= {
                Name                    IA5String,
                URL                     IA5String
        }
        Modules ::= SEQUENCE {
                Version         INTEGER,
                Stage                   INTEGER,
                Severity                INTEGER,
                Author                  IA5String,
                Dependency              IA5String,
                IntegrityAlgo   IA5String,
                RIM             IA5String
        }
        DigitalSignature ::= {
                SignedInfo      SignedInfoType,
                KeyInfo                 KeyInfoType,
                SignatureValue          IA5String
        }
END
タイプSignedInfoTypeおよびKeyInfoTypeは、DeviceIntegrityMeasurements
Typeと同様に定義され得る
```

テーブル５

【００２７】

デバイスにある各ソフトウェアモジュールにとって、それと関連付けられたモジュール属性がネットワークに知られている場合、ＳＡＶプロシージャ中に、Ｈ（ｅ）ＮＢは、ローカル完全性チェックプロシージャ中の完全性チェックに失敗した全モジュールの識別（ＩＤ）のリストだけをＰＶＥに送ればよい。ネットワークは、ＰＶＥを経由して、特定のソフトウェアモジュールの関連属性およびモジュールの失敗の影響を知ることになる。この情報は、本明細書に記載するように、ネットワークがとる次のステップの評価を行うのに用いることができる。

【００２８】

Ｈ（ｅ）ＮＢに送信されると見なすことができ、Ｈ（ｅ）ＮＢ管理システム（Ｈ（ｅ）ＭＳ）など、信頼できるサードパーティ（ＴＴＰ）から、デジタル証明書（digital certificate）または署名されたメッセージとしてプロビジョニングすることができるソフトウェアモジュール属性について本明細書に記載する。例えば、コードイメージに対する全体的情報要素は、Ｈ（ｅ）ＮＢの製造元およびモジュールコードイメージのダイジェストまたはＲＩＭを生成するのに用いられ得る完全性方法を含み得るが、それに限定されない。

【００２９】

コンポーネント特有の情報を記述するための方法について本明細書に記載する。１つまたは複数のコンポーネントが、ソフトウェアモジュールを成す。コンポーネントとは、完全性検査の基本的単位である。各コンポーネントに関連付けられた、１つの信頼できる参照値（ＴＲＶ）がある。コンポーネント特有の情報要素は、コンポーネント説明に対応する、一意に識別可能なＩＤであるコンポーネントＩＤを含み得る。これは、１つのＴＲＶでチェックされるべきコードの単位のＩＤである。情報要素は、Ｈ（ｅ）ＮＢ上での完全性検査機構が、コンポーネントの測定値を比較して、コンポーネントの完全性を検証するのに使うことができるＴＲＶをさらに含み得る。

【００３０】

モジュール特有の情報要素は、Ｈ（ｅ）ＮＢ内部の特有のモジュール機能を記述するモジュール説明およびモジュールを製造元に対して一意に識別するモジュールＩＤを含み得るが、それに限定されない。この情報要素は、このモジュールがマップされる先のＨ（ｅ）ＮＢの特有の機能性を識別する機能説明およびグローバルに識別可能なＩＤでよく、複数のベンダに渡って標準化され、機能説明に対応し得る機能ＩＤも含み得る。この情報要素は、このモジュールがマップする先のコンポーネントを識別するコンポーネントＩＤおよびモジュールのバージョン番号を示すリリースバージョンをさらに含み得る。コンポーネントとモジュールとの間に１対１のマッピングがあるケースでは、モジュール特有の情報は事実上、コンポーネント特有の情報と同一であり得る。

【００３１】

モジュール特有の情報要素は、システムの機能性に関する、現在のソフトウェアの完全性チェックの失敗の影響を指定する重大度分類も含み得る。例えば、複数レベル重大度分類システムが存在し得る。例えば、重大度１は、Ｈ（ｅ）ＮＢ機能性に対して高い影響を結果的に生じるモジュール／機能の失敗でよく、システムの停止動作を保証し得る。モジュール／機能の失敗は、フォールバックコードイメージ（ＦＢＣ）に基づいて、システムに沿った乱れを結果として生じ得る。この場合、ネットワークベースのデバイス管理システム（デバイスがＨ（ｅ）ＮＢである場合はＨ（ｅ）ＭＳとなる）との通信が可能であり得る。ＦＢＣは、指定されたＨ（ｅ）ＭＳに非常信号を送ることが可能であり得る。さらに、ネットワークが開始したファームウェア／ソフトウェアアップデートをサポートすることもできる。例えば、Ｈ（ｅ）ＮＢの信頼できる環境（ＴｒＥ）のためのどのモジュールまたはコンポーネントも、重大度１をもち得る。重大度２は、制限されたＨ（ｅ）ＮＢ機能性を結果的に生じることがあるモジュール／機能の失敗でよく、この失敗は、フルＨ（ｅ）ＮＢ機能性のサブセットとして部分的に機能することができ、またはフルＨ（ｅ）ＮＢ機能性のサブセットをサポートすることができる。この場合、セキュリティゲートウェイ（ＳｅＧＷ）との通信が可能であり得る。重大度３は、システムのコア機能性に影響

し得ないモジュール／機能の失敗でよいが、依然として、失敗のケースでは早期修復を求めるのに十分な程重要と見なされ得る。失敗したモジュール／機能は、即座のファームウェア／ソフトウェアアップデートプロシージャを介して置き換え、後続リブートにより妥当性確認することができる。重大度４は、システムのコア機能性に影響し得ないモジュールの失敗でよい。失敗したモジュール（複数可）は、通常のファームウェア／ソフトウェアアップデートスケジュールを介して置き換えることができる。

【００３２】

妥当性確認方法のための報告プロシージャまたは方法について本明細書に記載する。ＡｕＶ用に、デバイス完全性チェックの全プロシージャを、ローカルに実施することができる。完全性チェックが失敗した場合、非常信号をＨ（ｅ）ＭＳに送って、失敗を示すことができる。後続アクションは、送付担当者から、課題を解決し、またはデバイスを検疫(quarantine)するために広がり得る。修復は、失敗したモジュールのリストが修復サーバ／Ｈ（ｅ）ＭＳに報告され得るケースにおいて実施することができる。ＳＡＶのケースでは、完全性チェックに失敗した機能性のリストが、ＰＶＥに報告され得る。

【００３３】

モジュールは、製造元の実装に依存する。コンパイルされた１組のソフトウェアモジュールは、オブジェクトイメージを形成し得る。完全性チェックは、オブジェクトイメージチャンクに対して実施することができる。したがって、完全性チェックがそれに対して行われる１組のモジュールを組み合わせるコンポーネントが導入されている。１つのモジュールは、コンポーネント中で一度現れ、ただ１つのコンポーネント中で現れる（すなわち、１つのモジュールが、２つのコンポーネント中で現れることはできない）。このように、完全性チェックが実施されると、モジュールは一度だけ調べられる。Ｈ（ｅ）ＮＢの製造元（個々のどのソフトウェアモジュールの製造元と同一でも、異なってもよい）は、アーキテクチャに基づいて、デバイス完全性チェックのために、モジュールをコンポーネントにどのようにして区分するかを決定する。

【００３４】

機能性は、Ｈ（ｅ）ＮＢの要件および機能アーキテクチャに基づいてよく、標準化された識別子でよい。例えば、Ｉｕインタフェースおよび移動管理は、機能である。モジュールは、この２つの機能の間で共有することができる。したがって、コンポーネント（完全性チェック単位である）が完全性チェックに失敗すると、影響を受けたモジュールが分かる。各モジュールは、それに関連付けられた機能性をもつので、失敗した機能性のリストが導出され得る。この失敗した機能性のリストは、ＳＡＶにおいてＰＶＥに送られる。

【００３５】

機能性ＩＤについて本明細書に記載する。アーキテクチャの実装は、ソフトウェアモジュールの数およびタイプを支配する。複数の製造品および／または関係者（モバイルネットワークオペレータなど）に渡って報告構造および手順を調和させるために、報告は、実際のモジュールではなく機能性に基づいて行うことができる。ソフトウェアモジュールは、その機能性に基づいてグループ化することができる。機能性ＩＤは、機能性説明に基づいてモジュールを分類するための手段を提供する。テーブル６は、現在知られているものに基づいて導出されている機能性の一部を列挙している。このリストは、拡張し標準化することができる。テーブル６中で、最終有効桁が１～９の番号は、将来の使用または拡張性のために取り置かれている。

【００３６】

【表６】

機能性ID	機能性説明
10	H(e)MSサブシステムセキュアブートローダ
20	UuインタフェースTrE
30	Iuhインタフェース完全性の妥当性確認エンジン
40	HGmインタフェースフォールバックコード
50	HUtインタフェースオペレーティングシステム
60	S1-MMEインタフェースH(e)MSサブシステム
70	S1-UUuインタフェース

【００３７】

80	I2(SIP)Iuhインタフェース
90	Iu-CSインタフェースHGmインタフェース
100	Iu-PSインタフェースHUtインタフェース
110	E、Nc、NbS1-MMEインタフェース
120	RUAサービスS1-Uインタフェース
130	HNBAPサービスI2(SIP)インタフェース
140	HNB GW発見Iu-CSインタフェース
150	HNB登録Iu-PSインタフェース
160	HNBE、Nc、NbインタフェースのWTRU登録
170	アクセス制御管理RUAサービス
180	時間管理HNBAPサービス
190	CSG管理HNB GW発見
200	移動性管理HNB登録
210	HNB用のNASノード選択機能UE登録
220	ページング最適化アクセス制御管理
230	トランスポートアドレスマッピング時間管理
240	請求CSG管理
250	緊急サービス移動性管理
260	QoS管理NASノード選択機能
270	ローカルIPアクセスページング最適化
280	管理リモートアクセストランスポートアドレスマッピング
290	旧来のCN請求のHNBサポート

【００３８】

300	着信ハンドオーバサポート緊急サービス
310	ローミングQoS管理
320	MSC SGSNローカルIPアクセスへのSCCP無接続通信
330	OAMサブシステム管理リモートアクセス
340	旧来のCN用の表示サブシステムHNBサポート
350	USIMサブシステム着信ハンドオーバサポート
360	HPMサブシステムローミング
370	MSC SGSNへのIMS相互作用SCCP無接続通信
380	IP-PABXインタフェースOAMサブシステム
390	セキュリティ機能表示サブシステム
400	RAB管理USIMサブシステム
410	無線資源管理HPMサブシステム
420	Iuリンク管理IMS相互作用
430	Iu Uプレーン(RNL)管理IP-PABXインタフェース
440	Iu調整セキュリティ機能
450	プロビジョニング機能RAB管理
460	ハードウェア障害無線資源管理
470	Iuリンク管理
480	Iu Uプレーン(RNL)管理
490	Iu調整機能
500	プロビジョニング機能
510	ハードウェア障害

テーブル6

【００３９】

コンポーネントＩＤについて本明細書に記載する。複数のデバイス完全性チェックを調和させるために、モジュールは、生成されたイメージに基づいて分類することができる。１組のオブジェクトファイルを、イメージファイルの中に一緒にアーカイブすることができる。このようなモジュールグループは、同じコンポーネントＩＤを含み、まとめて完全性をチェックされ、したがって、１つのコンポーネントに対して信頼できる１つの参照値（ＴＲＶ）をもつ。各ソフトウェアモジュールは、それ自体の参照完全性メトリック（ＲＩＭ）を伴うので、コンポーネントの信頼できる参照値（ＴＲＶ）は、関連付けられたＲＩＭをそれぞれがもち得る、１つまたは複数のソフトウェアモジュールの連結のダイジェスト（例えば、ハッシュ）として取得することができる。１つのコンポーネントＩＤで現れるモジュールは、別のコンポーネントＩＤで現れる同じモジュールとは異なる機能性ＩＤにマップされ得ることに留意されたい。このプロシージャは、製造元に、そのアーキテクチャおよびコンパイラに基づいて柔軟性を与え、例えば、オブジェクトイメージまたはＳＡＶ完全性チェックの段階どちらかに基づいて、モジュールのグループ化を可能にする。

【００４０】

モジュールＩＤは、ソフトウェアの様々なモジュールを追跡するのに使われ、標準化することは不可能ではないが、標準化しなくてよい。モジュールＩＤが標準化されない場合、どのモジュールおよび何個のモジュールが存在するかの決定は、製造元に一任してよい。モジュールＩＤは、ファームウェア／ソフトウェアアップデートパッケージを提供し、追跡し、組み立てるのに使うことができる。

【００４１】

モジュール、コンポーネントおよび機能性など、様々な識別子の間の関係を編成し、述べる方法および構造について本明細書に記載する。図１は、一例である方法および構造を

示す。ソフトウェアアーキテクチャは、モジュールの数およびタイプを定義する。こうしたモジュールは、その機能性および完全性チェック単位に基づいて分類される。複数のモジュールからなるコンポーネントは、独自のＴＲＶをもつ。任意のコンポーネントの、そのＴＲＶを使う完全性検査が失敗した場合、コンポーネント自体が変えられるか、またはそのダイジェストがＴＲＶの値と同じでなくなっているか、またはコンポーネントに対応するＴＲＶが変えられている。いずれのケースでも、完全性チェックが失敗すると、モジュールと、完全性検査に失敗したコンポーネントとの間のマッピング並びにモジュールと機能性との間のマッピングを用いて、失敗した（または少なくとも「影響を受けた」）機能性のリストを判定することができる。影響を受けた機能性の識別子のリストは、Ｈ（ｅ）ＭＳまたはＰＶＥに伝達され得る。

【００４２】

図２は、コンポーネントおよび機能性の構造例を示す。図に示すように、コンポーネントが、完全性チェックがそれに対して実施される単位であるとき、コンポーネントは、製造元によって決定され得る。各コンポーネントに、機能性のリストを関連付けることができる。コンポーネントは機能性に基づく。したがって、コンポーネントが完全性チェックに失敗すると、失敗した機能性のリストを組み立てることができる。コンポーネントは、そのロード順の順序で、または或いは、実行順の順序で編成することができる。したがって、コンポーネント１がチェックに失敗した場合、コンポーネント１にある機能をローディングまたは実行のどちらかに使うコンポーネント２の機能性も失敗する可能性がある。

【００４３】

失敗した完全性チェックに基づいて、失敗した機能性のリストを抽出するための別の代替的実装形態は、イメージオブジェクトファイルのチャンクに対して完全性チェックを実施するものでよい。オブジェクトイメージ中の開始アドレスおよび終了アドレスで指定されたあるイメージブロックが、完全性チェックを通らない場合、失敗したセグメントに対応するソフトウェア機能の名称が抽出される。実装された機能に基づいて、失敗したＨ（ｅ）ＮＢ機能性のリストを導出することができる。この導出は、ソフトウェア機能が、一定のＨ（ｅ）ＮＢ機能性を実装するモジュールに属すので、行うことができる。例えば、ＵＮＩＸ（登録商標）環境では、「ｎｍ」が、オブジェクトファイルにある機能の名称を抽出するための機能性を提供する。この情報は、オブジェクトの記号テーブルから抽出される。

【００４４】

妥当性確認方法のためのソフトウェアおよびＴＲＶのダウンロードおよびプロビジョニングについて本明細書に記載する。使われ得る３つのプロトコルは、ＴＲ０６９ベースのアーキテクチャ、ＯＭＡ（オープンモバイルアライアンス）ＤＭ（デバイス管理）ベースのアーキテクチャおよびＴＣＧ（ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ）ＩＷＧ（インフラストラクチャワークグループ）ベースのアーキテクチャである。さらに、こうしたプロトコルは、プロビジョニングサポートを利用して、Ｈ（ｅ）ＮＢを構成するのに使うこともできる。こうした３つ以外の他のプロトコルも検討することができる。

【００４５】

図３のＴＲ０６９ベースのアーキテクチャは、ＣＰＥ（顧客構内設備）と自動構成サーバ（ＡＣＳ）との間の通信を意図したＣＰＥ　ＷＡＮ（ワイドエリアネットワーク）管理プロトコルを記述する。ＣＰＥは、Ｈ（ｅ）ＮＢにマップし、ＡＣＳは、Ｈ（ｅ）ＭＳ／修復サーバ／ＯＡＭ（運用、管理および保守）にマップする。ＣＰＥ　ＷＡＮ管理プロトコルは、ＣＰＥソフトウェア／ファームウェアイメージファイルのダウンロードを管理するためのツールを提供し得る。このプロトコルは、バージョン識別、ファイルダウンロード開始（ＡＣＳ開始ダウンロードおよびオプションのＣＰＥ開始ダウンロード）、並びにＡＣＳへの、ファイルダウンロードの成功または失敗の通知のための機構を提供し得る。

【００４６】

ＣＰＥ　ＷＡＮ管理プロトコルは、ＣＰＥが実施するべき明示的インストール命令に従って、個々のファイルまたはファイルのパッケージをダウンロードするのにオプションで

使われ得る、デジタル署名済みファイル形式も定義し得る。この署名済みパッケージ形式により、ダウンロードされたファイルおよび関連付けられたインストール命令の完全性が確実にされ、ＡＣＳオペレータ以外の当事者でよいファイルソースの認証を許可する。ダウンロードされたファイルの完全性検査は、ダウンロードされたファイルに含まれる、個々のモジュールから計算される完全性ダイジェスト（例えば、ハッシュ）と、それに対応するＲＩＭ値との比較に基づき得る。

【００４７】

ＣＰＥ　ＷＡＮ管理プロトコルは、デバイス完全性検査に必要とされるＴＲＶをＨ（ｅ）ＮＢにダウンロードするのに有用であり得る。このような内容は、ネットワークオペレータの署名鍵でデジタル署名され得る。署名されたパケットを受信すると、Ｈ（ｅ）ＮＢは次いで、署名を復号し、受信されたＴＲＶの真正性および完全性を検証することができる。コンポーネントが、幾つかのモジュールの順序付き連結として組み立てられるケースでは、ＴＲＶは、モジュールに対応するＲＩＭの順序付き連結として組み立てることができる。

【００４８】

ＴＲＶは、デジタル署名される前に、機密性のために暗号化してもよい。ＴＲＶは、デジタル署名された同じパケットの中で、ＴＲＶがそれに対して作成されるソフトウェアモジュールバイナリイメージの全体または（最初もしくは最後の）部分に付加することができる。

【００４９】

Ｈ（ｅ）ＮＢデバイスを取り扱う追加プロシージャについて本明細書に記載する。こうした追加要件およびプロシージャでは、以下の説明においてＨ（ｅ）ＮＢ－Ｈ（ｅ）ＭＳインタフェースとして識別されるインタフェースを使うことができる。Ｈ（ｅ）ＮＢの妥当性確認は、追加プロトコルコンポーネント要件を必要とし得る。Ｈ（ｅ）ＮＢ－Ｈ（ｅ）ＭＳは、ＳＳＬ／ＴＬＳ（セキュアソケットレイヤ／トランスポートレイヤセキュリティ）をサポートし、Ｈ（ｅ）ＮＢとＨ（ｅ）ＭＳとの間の証明書ベースの認証を用いるべきである。この証明書は、ＳｅＧＷへの認証に使われる、同じ証明書でよい。Ｈ（ｅ）ＮＢ－Ｈ（ｅ）ＭＳインタフェース用にＴＲ０６９ベースのアーキテクチャが使われる場合、ＣＰＥ認証のための基本またはダイジェスト認証は、証明書ベースの認証をサポートするように適合される必要があり得る。

【００５０】

ＴＲ０６９アーキテクチャに基づくＨ（ｅ）ＭＳ発見に必要とされ得るプロシージャまたは構造について本明細書に記載する。Ｈ（ｅ）ＮＢは、ＭａｎａｇｅｍｅｎｔＳｅｒｖｅｒ．ＵＲＬパラメータ中のデフォルトのＨ（ｅ）ＭＳ　ＵＲＬ（ユニフォームリソースロケータ）で構成されるべきである。この初期構成は、Ｈ（ｅ）ＮＢを分散させている間にオペレータによって、または製造元によって行うことができる。Ｈ（ｅ）ＮＢは、認可された管理者によって、ＬＡＮ（ローカルエリアネットワーク）側ＭａｎａｇｅｍｅｎｔＳｅｒｖｅｒ．ＵＲＬ構成をサポートすることができる。Ｈ（ｅ）ＭＳ　ＵＲＬは、ＨＴＴＰＳ（ハイパーテキスト転送プロトコルセキュア）ＵＲＬでよい。ホスティング側ＤＨＣＰ（動的ホスト構成プロトコル）ベースのＨ（ｅ）ＭＳ　ＵＲＬアップデートプロシージャは、サポートされなくてよい。値がローカルにアップデートされた場合、Ｈ（ｅ）ＮＢは、新規Ｈ（ｅ）ＭＳに接触して、構成ファイルをブートストラップし、密接性(affinity)を確立することができる。ＵＲＬは、名称またはＩＰ（インターネットプロトコル）アドレスである場合、ＤＮＳ（ドメインネームシステム）解決を求め得る。名前のＤＮＳ解決は、複数のＩＰアドレスを戻す場合があり、そのケースでは、複数のＩＰを戻してはならないことが確実になるか、または複数のＩＰが戻された場合は、Ｈ（ｅ）ＮＢがランダムに１つを選び出すかのどちらかである。

【００５１】

ＴＲ０６９アーキテクチャに基づくＳｅＧＷ発見について本明細書に記載する。Ｈ（ｅ）Ｓ　ＵＲＬと同様、ＳｅＧＷ　ＵＲＬを、パラメータ（ＳｅｃｕｒｅＧａｔｅｗａｙ．

ＵＲＬ）として追加することができる。このＵＲＬは、Ｈ（ｅ）ＮＢの場所に基づいて、オペレータによって構成され得る。ＤＨＣＰによるこのパラメータのアップデートは、サポートすることができない。認可された管理者によるローカルアップデートは実施することができる。

【００５２】

ＡｕＶおよびＳＡＶの目的で、ＴＲ０６９、ＯＭＡ　ＤＭ、またはＴＣＧ　ＩＷＧなどのデバイス管理プロトコルを適応させるための追加機構について本明細書にこれ以降で記載する。

【００５３】

妥当性確認方法のためにソフトウェアおよびＴＲＶをダウンロードしプロビジョニングする、ＯＭＡ　ＤＭベースのアーキテクチャについて本明細書に記載する。ＯＭＡ　ＤＭは、ＯＭＡ　ＤＭ作業グループおよびＤＳ（データ同期）作業グループによって共同で指定されるデバイス管理プロトコルである。ＯＭＤ　ＤＭは、電話、ＰＤＡ、および他の同様のデバイスなど、小型のフットプリントモバイル機器用に開発されたが、機器とＤＭサーバとの間のブロードバンドワイヤライン接続性はサポートせず、短距離ワイヤード接続性（例えば、ＵＳＢ（ユニバーサルシリアルバス）やＲＳ２３２Ｃ）またはワイヤレス接続性（ＧＳＭ（登録商標）（移動体通信用グローバルシステム）、ＣＤＭＡ（符号分割多重アクセス）、ＷＬＡＮ（ワイヤレスローカルエリアネットワーク）、および他のワイヤレス通信システム）のみをサポートし、Ｈ（ｅ）ＮＢ用のデバイスプロビジョニングおよび管理プロトコルとして有用であり得る。このことは、コアネットワークに対してはＷＴＲＵ（ワイヤレス送受信ユニット）としてそれ自体を提示し、共通シリアルゲートウェイ（ＣＳＧ）およびそれに接続する非ＣＳＧ　ＷＴＲＵに対しては基地局としてそれ自体を提示し得るＨ（ｅ）ＮＢに対して当てはまり得る。

【００５４】

ＯＭＡ　ＤＭは、プロビジョニング（初回デバイス構成を含み、特徴を可能／不能にする）、デバイス構成アップデート、ソフトウェアアップグレード、並びに診断報告および照会などの使用ケースをサポートし得る。ＯＭＡ　ＤＭサーバ側は、こうした機能すべてをサポートすることができるが、デバイスは、オプションで、こうした特徴の全部またはサブセットを実装してもよい。

【００５５】

ＯＭＡ仕様は、小型フットプリントデバイス向けの、上に列挙した特徴を、接続性を制約してサポートするように最適化され得る。この仕様は、それらの仕様の一部として行われる認証プロトコルを用いて（ＥＡＰ－ＡＫＡ（ｅｘｔｅｎｓｉｂｌｅ　ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ｐｒｏｔｏｃｏｌ－ａｕｔｈｅｎｔｉｃａｔｉｏｎ　ａｎｄ　ｋｅｙ　ａｇｒｅｅｍｅｎｔ）などのプロトコルを使用することによって）、統合型セキュリティもサポートし得る。

【００５６】

ＯＭＡ　ＤＭは、ＸＭＬ（または、より正確には、ＳｙｎｃＭＬのサブセット）を、データ交換に使うことができる。これは、妥当性確認目的のために、ソフトウェアモジュール用の属性またはＨ（ｅ）ＮＢ用の機能性を定義し伝えるための、標準化可能でありながら柔軟なやり方を提供するのに有用であり得る。

【００５７】

デバイス管理は、ＤＭサーバ（デバイス用の管理エンティティ）とクライアント（管理されるデバイス）との間で起こる。ＯＭＡ　ＤＭは、ＷＡＰ（ワイヤレスアプリケーションプロトコル）、ＨＴＴＰ、またはＯＢＥＸ（オブジェクト交換）もしくは同様のトランスポートなどのトランスポートレイヤをサポートする。

【００５８】

ＤＭ通信は、通知または警告メッセージどちらかを用いる、ＷＡＰ、プッシュまたはＳＭＳ（ショートメッセージサービス）など、任意の利用可能方法を用いて、ＤＭサーバによって非同期に開始される。サーバとクライアントとの間で通信をセットアップすること

ができると、メッセージのシーケンスを交換して、所与のＤＭタスクを完了することができる。

【００５９】

ＯＭＡ　ＤＭ通信は、要求応答プロトコルに基づいてよく、このプロトコルでは、要求はＤＭサーバによってのみ行うことができ、クライアントは、返信メッセージで応答するだけでよい。サーバおよびクライアントは両方とも状態をもち、このことは、特有のシーケンスが原因で交換されるどのデータも、内蔵型認証プロシージャの後でのみ起こり得ることを意味する。

【００６０】

ＤＭ通信は、ＤＭサーバによってのみ開始することができるので、ＤＭを介したＳＡＶの実装には、妥当性確認のためのサーバ照会ベースの手法が求められる場合があり、可能性としては（即座に）、ＩＫＥ（インターネット鍵交換）ｖ２（デバイスによって開始される）を用いるデバイス妥当性確認プロシージャに続く。異なる幾つかのメッセージタイプは、妥当性確認データ（例えば、失敗したソフトウェアモジュールやデバイス機能性のリスト）のコンベアと見なすことができる。例えば、管理警告メッセージは、デバイスからサーバに送られ得る。或いは、少なくとも１つの管理警告メッセージがデバイスまたはサーバどちらかから伝送された後でデバイスからＤＭサーバに送られ得る汎用警告メッセージのユーザも、検討され得る。こうした警告メッセージを含む全メッセージは、内容および内容に関するメタデータを指定する際の柔軟性を与えるＳｙｎｃＭＬ（同期マークアップ言語）形式を使うので、妥当性確認情報転送に有用であり得る。ＤＭは、セグメント化データ転送をサポートすることができ、この転送は、アップデートのサイズが大きい場合があるソフトウェアアップデートに有用であり得る。セグメント化データ転送は、このような情報のサイズにより、複数のメッセージへの区分が求められる程十分に大きいケースにおいて、Ｈ（ｅ）ＮＢからＰＶＥへの、Ｈ（ｅ）ＮＢの、失敗した機能性のリストの転送にも用いることができる。

【００６１】

妥当性確認方法のためのソフトウェアおよびＴＲＶをダウンロードしプロビジョニングする、ＴＣＧ　ＩＷＧベースのアーキテクチャについて本明細書に記載する。ＴＣＧ（ｔｒｕｓｔｅｄ　Ｃｏｍｐｕｔｉｎｇ　Ｇｒｏｕｐ）、ＩＷＧ（インフラストラクチャ作業グループ）は、プラットフォーム完全性管理のための詳細な形式およびプロトコルを指定している。完全性測定および報告のための基本的なモデルでは、ネットワークおよびサービスアクセスは、プラットフォームの検証済み状態が条件とされ得る。

【００６２】

ＴＣＧ　ＩＷＧ標準は、Ｈ（ｅ）ＮＢ　ＳＡＶまたはＡｕＶ用に求められる構造のスーパーセットを提供する。ＩＷＧ仕様はどれも、そのまま用いることはできない。さらに、ＩＷＧ仕様を、デバイス妥当性確認の特有の使用ケースにプロファイリングするには、ＸＭＬスキーマの修正（例えば、求められる要素の省略）が求められ、これは、ＩＷＧ標準からの逸脱を意味する。

【００６３】

要求側プラットフォームとネットワーク側検証元との間の基本的な対話を、図４に示す。検証元は、要求側のプラットフォームのコンポーネントそれぞれに関する権威ある情報を探す必要がある（第５のステップで）。つまり、検証元は、メトリックプロバイダによって利用可能にされるプラットフォーム妥当性確認のために、参照測定値を求める。メトリックプロバイダの例は、ハードウェア製造元、ソフトウェアベンダまたは製造元およびベンダの代理の信頼できるプロバイダである。検証元が、要求側のプラットフォームの各コンポーネントを識別し、報告された測定値を、期待される（ベースライン）参照測定値（そのコンポーネントに関する）と突き合わせて比較することができると、検証元は、要求側のプラットフォームの信頼レベルを測ることができる。この段階で、検証元は、依拠当事者（relying party）の所で資源／サービスにアクセスするための、要求側の要望に関して決定を行うことができる。これを、第６のステップに示す。

【００６４】
ＩＷＧ完全性検証アーキテクチャは、検証されたプラットフォーム上でのハードウェアＴＰＭ（信頼プラットフォームモジュール）の存在にほとんど依存しないことに留意されたい。特に、標準において指定されるデータ形式は、汎用コンポーネントおよびプラットフォームセキュリティ関連属性を表すことが可能である。
【００６５】
所与のコンポーネントにおける技術的信頼をサポートするために、コンポーネント製造元は、コンポーネントの出所に関する情報をもつ、製造元の製品をサポートすればよい。つまり、製造元または信頼できるサードパーティは、そのコンポーネントに関する幾つかの静的参照値を提供しなければならない。コンポーネントに関するこうした静的参照／メトリック値は、参照測定値と呼ばれ、ＴＣＧ参照マニフェスト（ＲＭ）構造の形で表される。コンポーネント用のマニフェストは、その識別、製造元、モデル番号、バージョン番号、およびそれ以外などの情報を含む。このアプリケーションの目的のために、Ｈ（ｅ）ＮＢのコンポーネントの信頼できる参照値（ＴＲＶ）は、ＴＣＧ　ＩＷＧ参照マニフェスト（ＲＭ）構造によって指定され得る。
【００６６】
プラットフォームは、妥当性確認される必要があるとき、妥当性確認元（プラットフォーム検証エンティティ、すなわちＰＶＥなど）に、図５に示すような、プラットフォームのコンポーネントをカバーする１組のスナップショットからコンパイルされた完全性レポートを提供しなければならない。スナップショットは、プラットフォームのすべての関連コンポーネント（および可能性としてはこうしたコンポーネントの下位コンポーネント）についての測定値およびアサーション両方を表す。参照（ＩＤ　Ｒｅｆ）は、図６に示すように、完全性レポート中で報告されるコンポーネントに関する情報をポイントするのに使われる。
【００６７】
ＲＭに基づく妥当性確認のためのコア要素は、ＴＣＧ標準に記載されている。柔軟性のために、ＸＭＬ名前空間が、ＩＷＧ形式、例えば、モバイル、またはＰＣクライアントのプラットフォーム固有プロファイル用に使われ得る。
【００６８】
相互運用可能な完全性ログ構造は、プラットフォーム特有の符号化を指示するための「ハードウェアアーキテクチャ」タイプ値を定義することによって、幾つかのプラットフォーム特有の制約に対処することができる。タイプ値は、ＸＭＬ名前空間およびＸＲＩなど、相互運用可能な名前空間機構を用いるＴＣＧ名前空間によって定義され得る。
【００６９】
コアスキーマから拡張によって継承するＲＭスキーマは、参照を保持するための構造を定義する。ＲＭスキーマは、図７に示すように、２つの情報セットからなるものとして、大まかに理解すればよい。第１のものは、個々のコンポーネントについての情報に関し、例えばコンポーネントモデル、名称、バージョン、シリアルナンバーなどの属性をカバーする。この情報は、ＣｏｍｐｏｎｅｎｔＩＤｔｙｐｅ構造に取り込まれる。このコンポーネント特有の周辺情報は、コンポーネント情報の取込み（獲得）に関するメタデータである。このデータは、スキーマにおけるＩｎｔｅｇｒｉｔｙＭａｎｉｆｅｓｔＴｙｐｅ構造で表される。取り込まれるメタデータは、使われる収集（獲得）方法、ＲＭ署名（および関連付けられた署名者／発行元情報）、コンポーネント（ソフトウェア用）に関するダイジェスト値（複数可）、信頼性レベル（ｃｏｎｆｉｄｅｎｃｅ　ｌｅｖｅｌ）、行われるアサーション並びにそれ以外を含む。
【００７０】
ＡｕＶ特有の項目について本明細書に記載する。ＡｕＶでは、完全性チェックはローカルに実施することができる。したがって、本明細書に記載するデジタル署名またはメッセージ認証コードのどれを使ってもよい。これらは、製造元の私有鍵／共有の秘密を使って、製造元によって署名し、その真正性を、製造元共有の秘密または公開鍵を使ってローカ

ルに検証することができ、コードの完全性をローカルに検証するのに使うことができる。
【００７１】
ただし、ＡｕＶでは、デバイス妥当性確認は、デバイス内部でローカルに実施することができ、情報は、どのネットワークエンティティにも送られない。したがって、妥当性確認に使用するための正確な方法の決定は、製造元に一任され得る。ただし、「完全性アルゴリズムは、ＳＨＡ－１と等価またはより優れたセキュリティを与えなければならない」など、最低限のセキュリティ要件を標準化することができる。
【００７２】
どのようにしてＡｕＶがＴＲＶ証明書管理を実装するかについて本明細書に記載する。システムのコンポーネントは、実際の実装形態に依存するので、デバイス完全性に用いられる複数の機構を調和させる必要がある。これは、ＴＲＶとして知られる信頼できる参照完全性メトリックを生成するのに用いられる方法に対する最低要件を標準化することによって達成され得る。こうしたＴＲＶは、製造元によっても、値にデジタル署名するＴＴＰによっても生成することができる。したがって、情報を編成し、ＴＲＶを生成し、分配し、使うための機構が見直される。
【００７３】
初回ＴＲＶ証明書初期化について本明細書に記載する。Ｈ（ｅ）ＮＢを完全に開発した後、製造元は、ローカル完全性データ初期化を実施する。このプロセスでは、ソフトウェアモジュール名がすべて、デバイス構成データシート中に収集される。構成ファイルに関連したいずれかの工場設定が存在する場合、こうした設定は、デバイス構成データシートにも含まれる。モジュールは、実行可能ファイルであってソースコードではない。構成データの初期プロビジョニングも実施される。デバイス構成データシートスキーマは、標準スキーマに従う。本明細書において提示するＸＭＬまたはＡＳＮ．１スキーマは、ベースラインとして使われ得る。重大度、互換性、段階およびそれ以外についての属性はすべて、デバイスのアーキテクチャに基づいて投入される。
【００７４】
図８は、証明書管理アーキテクチャ８００を示す。製造元の証明書サーバ８０５の所で、モジュールエントリ８１０はすべて、参照完全性メトリックを投入される。完全性方法属性およびＴＲＶ属性が投入される。デバイス構成データシートは次いで、私有鍵８２０を使って製造元によって署名される。データシートは、ＴＴＰによって製造元に対して発行されるルート証明書を参照して証明することもできる。このように、参照完全性メトリック（ＲＩＭ）はＴＲＶ８３０になる。
【００７５】
代替アーキテクチャでは、ＴＲＶは、ＴＴＰによって生成することができる。製造元は、実行可能ファイルと、モジュールすべておよび製造元のサイトで満たすことができる幾つかの投入済み属性を列挙する、部分的に完了されたデバイス構成シートとを提供する。ダイジェストメトリックであるＴＲＶは、ＴＴＰによって投入される。ＴＴＰは次いで、デバイス構成証明書にデジタル署名する。
【００７６】
ＡｕＶはデバイス内部でローカルに実施されるので、デバイス構成データシートは、デバイス内部で維持することができる。デバイス構成データシートは、認可された当事者によってのみアクセスされ得る安全なメモリ内に保たれなければならない。或いは、デバイス構成データシートは、暗号化されなければならず、読み出され、使われるときにＨ（ｅ）ＮＢ内で復号され得る。いずれのケースでも、Ｈ（ｅ）ＮＢの信頼できる環境（ＴｒＥ）のみが、アプリケーションによる読出しアクセスのためにデバイス構成データシートを解放し、またはそれを修正する権限をもつべきである。
【００７７】
安全なスタートアッププロセスの間、デバイスがコンポーネントのローカル測定を実施すると、生成されたダイジェストは、デバイス構成データシート中で指定された値と比較される。不一致が起きた場合、デバイス完全性の妥当性確認の失敗と解釈される。デバイ

ス構成データシートの完全性は、アクセスされる前に検証されなければならない。デバイス構成データシートの完全性は、データシート中で指定されるいずれか１つまたは複数のコンポーネントの１つまたは複数の完全性チェック失敗の後で検証してもよいであろう。

【００７８】

後続ＴＲＶ証明書アップデートプロシージャについて本明細書に記載する。展開されたＨ（ｅ）ＮＢシステムにとって、製造元によって新規ソフトウェアバージョンが発行される場合、製造元は、Ｈ（ｅ）ＭＳ／ＯＡＭサーバ／修復サーバに、ソフトウェアモジュールとともにデバイス構成データシートを提供することができる。これは、製造元による「ＰＵＳＨ」動作を実施することによって非同期に行われ得る。このようなＰＵＳＨは、オペレータと製造元との間で署名されたサービス合意に基づいてオペレータと製造元との間で合意される、スケジュールされたアップデート／アップグレードに基づいてスケジュールされ得る。

【００７９】

このようなＰＵＳＨに続いて、スケジュールされたときにリブートして、Ｈ（ｅ）ＭＳ／ＯＡＭ／修復サーバからソフトウェア／ファームウェア向けの「ＰＵＬＬ」動作を実施するようデバイスに命令する、ファームウェアまたはソフトウェアモジュールをアップデートするためのＯＡＭプロシージャまたはＴＲ０６９プロシージャが呼び出され得る。暗号化、署名およびノンスは、それぞれ、機密性、完全性、および反射攻撃に対する保護などのセキュリティ側面を提供し得る。

【００８０】

或いは、ソフトウェアリリーススケジュールに基づくスケジュールされた満了によりデバイス構成データシートが失効すると、Ｈ（ｅ）ＮＢは、ファームウェア／ソフトウェアアップデートプロセスをスタートし、ＯＡＭ／修復サーバからソフトウェア／ファームウェア向けのＰＵＬＬを開始することができる。或いは、Ｈ（ｅ）ＭＳは、ソフトウェアリリースの既知のスケジュール（例えば、製造元から取得される）に基づいて、ソフトウェアアップデートの、スケジュールされたＰＵＳＨを実施することもできよう。

【００８１】

デバイスへのソフトウェア／ファームウェアダウンロードをサポートするＴＲ０６９またはＯＭＡ　ＤＭアーキテクチャに基づくプロシージャについて本明細書に記載する。ＡｕＶのケースでは、ＴＲ０６９プロトコルは、顧客構内機器の遠隔管理のサポートを提供し得る。このプロトコルは、デバイスソフトウェア／ファームウェアアップデートのサポートも提供し得る。ＴＲ０６９を使用して、Ｈ（ｅ）ＮＢデバイスにファームウェア／ソフトウェアアップデートを提供することができる。

【００８２】

図９に示すように、認可された管理者によって、またはＵＲＬアップデートプロシージャを使用することによってＨ（ｅ）ＮＢ９０５の所で実施することができる後続アップデートのための、Ｈ（ｅ）ＮＢ９０５とＨ（ｅ）ＭＳ９１０との間のＡｕＶプロシージャ例について本明細書に記載する。Ｈ（ｅ）ＮＢ９０５は最初に、Ｈ（ｅ）ＭＳ発見に関して前述したように、ＭａｎａｇｅｍｅｎｔＳｅｒｖｅｒ．ＵＲＬパラメータ（０）中のデフォルトのＨ（ｅ）ＭＳ　ＵＲＬ（ユニフォームリソースロケータ）で構成される。これは、製造元によってプロビジョニングされ得る。Ｈ（ｅ）ＭＳ９１０は、ＴＣＰ（伝送制御プロトコル）接続をオープンする（１）。Ｈ（ｅ）ＮＢ９０５とＨ（ｅ）ＭＳ９１０との間で、ＳＳＬ（セキュアソケットレイヤ）接続が確立されて、安全な通信が許可される（２）。Ｈ（ｅ）ＭＳ９１０は、ＲＰＣ（リモートプロシージャコール）メソッドＳｅｔＰａｒａｍｅｔｅｒＶａｌｕｅｓを開始し、ＭａｎａｇｅｍｅｎｔＳｅｒｖｅｒ．ＵＲＬをアップデートする（３）。アップデートが成功した後、ＳｅｔＰａｒａｍｅｔｅｒＶａｌｕｅｓＲｅｓｐｏｎｓｅが、成功または失敗を示す状況フィールドとともにＨ（ｅ）ＮＢ９０５によって送られる（４）。Ｈ（ｅ）ＮＢ９０５は、Ｈ（ｅ）ＭＳ　ＵＲＬをアップデートする（５）。

【００８３】

Ｈ（ｅ）ＮＢ－Ｈ（ｅ）ＭＳインタフェース用にＴＲ０６９を使ってファイル転送をサポートするＡｕＶプロシージャについて本明細書に記載する。ＴＲ０６９は、ユニキャストおよびマルチキャストトランスポートプロトコルによってファイル転送をサポートする。ユニキャストプロトコルは、ＨＴＴＰ／ＨＴＴＰＳ、ＦＴＰ（ファイル転送プロトコル）、ＳＦＴＰ（セキュアファイル転送プロトコル）およびＴＦＴＰ（トリビアルファイル転送プロトコル）を含む。マルチキャストプロトコルは、ＦＬＵＴＥ（一方向トランスポートでのファイル配信）並びにＤＳＭ－ＣＣ（ｄｉｇｉｔａｌ　ｓｔｏｒａｇｅ　ｍｅｄｉａ　ｃｏｍｍａｎｄ　ａｎｄ　ｃｏｎｔｒｏｌ）を含む。ＨＴＴＰ／ＨＴＴＰＳのサポートは必須である。ＴＲ０６９をＨ（ｅ）ＮＢ－Ｈ（ｅ）ＭＳインタフェースにおけるファームウェア／ソフトウェアダウンロードに適応させるために、ＨＴＴＰ／ＨＴＴＰＳに加えて、ＦＴＰＳ（ＦＴＰセキュア）が使用されてもよく、ＴＲ０６９に追加される必要がある。ＦＴＰＳ（ＦＴＰセキュアおよびＦＴＰ－ＳＳＬとしても知られる）は、ＴＬＳ（トランスポートレイヤセキュリティ）およびＳＳＬ暗号プロトコルのサポートを追加する、ＦＴＰへの拡張である。Ｈ（ｅ）ＮＢ－Ｈ（ｅ）ＭＳインタフェースはＴＬＳ－ＳＳＬインタフェースを使用するので、ＦＴＰＳを、ファイルの転送用に実装することができる。

【００８４】

ＴＲ０６９は、ファイルをダウンロードする同じＴＬＳ接続を再利用し、並列して存在し得るファイルをダウンロードし、または第１のセッションを解放するための新規接続をスポーンするためのサポートも提供する。ダウンロードが完了した後、シグナリング用のＴＬＳ接続が確立される。ファイルをダウンロードするのにＨＴＴＰ／ＨＴＴＰＳが使われる場合、標準ＴＲ０６９プロシージャを使用することができる。

【００８５】

修復サポートのためのＡｕＶプロシージャ例について本明細書に記載する。デバイス完全性チェックがＡｕＶにおいて失敗した場合、ローカル非常フラグを設定することができ、システムは、フォールバックコード（ＦＢＣ）でリブートする。ＦＢＣは、デバイス内に安全に格納することができ、安全なスタートアッププロシージャ（またはデバイスの基本的な完全性を保証するのに「本質的」と思われる他の任意のデバイスプロセス）が失敗した場合はロードし実行することができる。ＦＢＣは、コアネットワークとの基本的な通信能力を有し、予め指定されたＨ（ｅ）ＭＳに非常信号を送る能力を有する。Ｈ（ｅ）ＭＳは、Ｈ（ｅ）ＭＳ発見プロシージャによってアップデート済みである場合がある。非常信号の内容は、デバイス上のＦＢＣ中に安全に格納することもでき、ＭＮＯによってプロビジョニングし、デバイス構成データシートの一部として安全に格納することもできる。非常信号は、デバイス完全性チェック失敗の詳細を示すエラーコード情報要素を含み得る。非常信号を受信すると、ネットワークは、信頼できる参照値を含む完全イメージおよびデバイス構成ファイルをアップデートすることを決定することができる。ＦＴＰサーバは、完全イメージ、デバイス構成ファイルおよびインストール命令を含むパッケージファイルを格納する。ＦＴＰサーバは、Ｈ（ｅ）ＭＳとマージされ得る。

【００８６】

このプロシージャは、ＴＲ０６９プロトコルをサポートするＦＢＣによって遂行することができ、Ｈ（ｅ）ＮＢ１００５、Ｈ（ｅ）ＭＳ１０１０およびＦＴＰサーバ１０１５の間のフローチャート例１０００を図１０に示す。デバイス完全性チェックが失敗し、信頼のルート（ＲｏＴ）がＨ（ｅ）ＮＢ１００５の所でＦＢＣを起動済みである（０）場合、Ｈ（ｅ）ＮＢ１００５は、予め指定されたＨ（ｅ）ＭＳサーバ１０１０へのＴＣＰ接続をセットアップする（１）。ＳＳＬ開始が実施され、および／またはＴＬＳ（トランスポートレイヤセキュリティ）がセットアップされる（２）。Ｈ（ｅ）ＮＢ１００５は次いで、Ｈ（ｅ）ＭＳ１０１０へのＲＰＣメソッドＩＮＦＯＲＭ、例えば、非常信号を呼び出す。非常信号は、Ｄｅｖｉｃｅ　ＩＤ、Ｅｖｅｎｔ、ＭａｘＥｎｖｅｌｏｐｅｓおよびＣｕｒｒｅｎｔＴｉｍｅなど、情報要素のどの組合せも含み得る。

【００８７】

Ｄｅｖｉｃｅ ＩＤは、製造元名と、デバイス製造元のＯＵＩ（組織的に一意の識別子）と、シリアルナンバーが該当する製品のクラスを示し、またはＴｒＥ ＩＤもしくはＨ（ｅ）ＮＢ Ｉｄを示すのにＳｅｒｉａｌＮｕｍｂｅｒ属性を使用させるためにデバイスのシリアルナンバーを示すのに使用することができるＰｒｏｄｕｃｔＣｌａｓｓと、特定のデバイスのシリアルナンバーを送り、またはＴｒＥ ＩＤもしくはＨ（ｅ）ＮＢ ＩＤを送るのに使われ得るＳｅｒｉａｌ Ｎｕｍｂｅｒとを含み得る構造である。

【００８８】

Ｅｖｅｎｔフィールドは、ＲＰＣメソッドＩｎｆｏｒｍを実行させたイベントコードを含み得る。新規イベントコード（Ｘ＿ＨｅＮＢ＿ＦＢＣ Ｉｎｖｏｋｅｄ）は、デバイス完全性チェックが失敗したこと、およびこの非常信号を送るためにＦＢＣが呼び出されていることを示すように定義される必要があり得る。単一のＨＴＴＰ応答に含まれ得る「ＳＯＡＰエンベロープ」と呼ばれるパラメータの最大出現回数をＡＣＳ（例えば、Ｈ（ｅ）ＭＳ）に対して示すＭａｘＥｎｖｅｌｏｐｅｓ値は、１に設定すればよい。ＭａｘＥｎｖｅｌｏｐｅパラメータの値は、１以上になり得る。非常指示は、一度だけ送られることを意図しているので、この値を１に設定することが適切である。ＣｕｒｒｅｎｔＴｉｍｅフィールドは、Ｈ（ｅ）ＮＢ１００５に知られている現在日時の値である。したがって、Ｉｎｆｏｒｍ ＲＰＣメソッドは、デバイスが完全性チェックに失敗し、ファームウェア／ソフトウェアアップデートを開始するために接続中であることをＨ（ｅ）ＭＳ１０１０に対して示す。

【００８９】

プロシージャ１０００の残りはオプションである。Ｈ（ｅ）ＭＳ１０１０は、ＲＰＣメソッドのダウンロードを呼び出すことができ、ファームウェアまたはソフトウェアおよびデバイス構成データシートの場所のＵＲＬを与える（４）。以下のパラメータ値が設定され得る。ＣｏｍｍａｎｄＫｅｙパラメータは、ある特定のダウンロードを指すのにＨ（ｅ）ＮＢ１００５によって使われ得る文字列である。これは、ダウンロードと応答を相関させるのに使われる任意の文字列でよい。ＦｉｌｅＴｙｐｅパラメータは、ファームウェア／ソフトウェアイメージに対しては「１、ファームウェアアップグレードイメージ」に、デバイス構成データシートに対しては「Ｘ＿＜ＯＵＩ＞＿ｄａｔａ＿ｓｈｅｅｔ」に設定することができる。ＵＲＬパラメータは、ダウンロードファイルのＵＲＬである。ＨＴＴＰおよびＨＴＴＰＳがサポートされなければならない。ＦＴＰＳのサポートも、ダウンロード用に推奨される。Ｕｓｅｒｎａｍｅパラメータは、ファイルサーバに対して認証を行うのに、Ｈ（ｅ）ＮＢ１００５によって使われ得る。Ｐａｓｓｗｏｒｄパラメータは、Ｈ（ｅ）ＮＢ１００５によって、ファイルサーバに対して認証を行うのに使われ得る。ＦｉｌｅＳｉｚｅパラメータは、ダウンロードされるべきファイルのサイズである。他のパラメータも設定することができる。

【００９０】

Ｈ（ｅ）ＮＢ１００５は、ＦＴＰサーバ１０１５に接続し、ファームウェアイメージ（またはソフトウェアイメージ）およびデバイス構成データシートをダウンロードする（５）。ＦＴＰサーバ１０１５の所の情報は、修復情報として示され得る。ダウンロードの完了が成功すると、ゼロ（成功を示す）の値をもつＳｔａｔｕｓ引数を有するＤｏｗｎｌｏａｄＲｅｓｐｏｎｓｅ、またはダウンロード要求への失敗応答（失敗を示す）が送られる（６）。成功または失敗したダウンロードを示すための代替的プロシージャがとられてもよい。成功したＤｏｗｎｌｏａｄＲｅｓｐｏｎｓｅの後、Ｈ（ｅ）ＭＳ１０１０は次いで、Ｈ（ｅ）ＮＢ１００５内でリブートプロシージャを呼び出すことができる（７）。Ｈ（ｅ）ＮＢ１００５内のＲＰＣハンドラは、ローカル非常フラグをリセットし、正常にブートして、ローカル完全性チェックプロシージャを実施する（８）。署名されたパッケージ形式は、リブートコマンドを含んでよく、このコマンドは、ファームウェアまたはソフトウェアがアップデートされた後でリブートするようＨ（ｅ）ＮＢ１００５に命令するのに使われ得る。ファームウェア／ソフトウェアアップデートのプロシージャが首尾よく完了されたことをＨ（ｅ）ＭＳ１０１０に示すためにＴｒａｎｓｆｅｒＣｏｍｐｌｅｔｅ Ｒ

ＰＣメソッドが、Ｈ（ｅ）ＮＢ１００５から呼び出され得る（９）。或いは、ＳｅＧＷが、成功したファームウェア／ソフトウェアアップデート完了メッセージとしてＨ（ｅ）ＭＳ１０１０内で翻訳され得る、デバイスが首尾よくブートしたことを示すためのメッセージをＨ（ｅ）ＭＳ１０１０に送ってもよい。

【００９１】

Ｈ（ｅ）ＮＢファームウェア／ソフトウェアアップデートに使うことができ、図１１に示すファイル形式例１１００について本明細書に記載する。ヘッダー１１０５は、プリアンブル、形式バージョン、並びにコマンドリストおよびペイロードコンポーネントの長さを含む固定長の構造でよい。コマンドリスト１１１０は、パッケージに含まれるファイルを抽出しインストールするように実行することができる一連の命令を含む。各コマンドは、ＴＬＶ（タイプ、長さ、値）の形でよい。署名フィールド１１１５は、ゼロ以上のデジタル署名のセットを含み得るＰＫＣＳ（公開鍵暗号技術標準）＃７デジタル署名ブロックを含み得る。ペイロードファイル１１２０は、コマンドリスト１１１０中の命令に従ってインストールされるべき１つまたは複数のファイルを含み得る。ファームウェア／ソフトウェアアップデートファイルに加えて、デバイス構成データシートも、署名されたパッケージ形式でパッケージ化される。

【００９２】

ストレージ分類器の要件をサポートするために、以下の新規Ｈ（ｅ）ＮＢ特有のコマンドを追加することができる。すなわち、１）安全な不揮発性メモリに格納する（ＴＲＶや構成データシートなどのデータの場合）、２）不揮発性ストレージに格納する、または３）揮発性ストレージに格納することができる。

【００９３】

図１２は、ＳＡＶ用のネットワークアーキテクチャ例１２００を示す。Ｈ（ｅ）ＮＢ１２０５が、ユーザ機器１２１０用のゲートウェイとして作用して、コアネットワーク１２２０への通信リンク１２１５を介して通信する。Ｈ（ｅ）ＮＢ１２０５は、安全でない通信リンク１２１５を介してＳｅＧＷ１２２５と対話する。ＳｅＧＷ１２２５は、認証されたＨ（ｅ）ＮＢが、コアネットワーク１２２０にアクセスすることを許可することができる。Ｈ（ｅ）ＭＳ１２３０が、Ｈ（ｅ）ＮＢ管理サーバとして作用し、修復のサポートを提供する。Ｈ（ｅ）ＭＳ１２３０は、Ｈ（ｅ）ＮＢ１２０５を管理するための標準プロトコルをサポートし得る。プラットフォーム妥当性確認エンティティ（ＰＶＥ）１２３５が、Ｈ（ｅ）ＮＢ１２０５内の、ある機能性セットが失敗したときにとられるべきアクションを定義するポリシーを格納する。こうした失敗した機能性は、ＳＡＶプロセス中にＨ（ｅ）ＮＢ１２０５によって報告される。ＯＡＭ１２４０は、運用、管理および保守サーバである。Ｈ（ｅ）ＭＳ１２３０およびＰＶＥ１２３５は、別個のエンティティとして示してあるが、単一のネットワークエンティティとして、互いとマージしてもよい。このようなマージされたエンティティは、ネットワークオペレータごとに単一のノードでもよく、オペレータごとに複数のノードでもよい。

【００９４】

ＳＡＶに関するプロシージャについて本明細書に記載する。要約すると、デバイス妥当性確認プロシージャを実施し始める前に、Ｈ（ｅ）ＮＢのＴｒＥは最初に、ブートコード、フォールバックコード（ＦＢＣ）、ＳｅＧＷ用の基本的な通信コード、およびＨ（ｅ）ＮＢがＨ（ｅ）ＭＳにアクセスすることを可能にするプロシージャを実施するコードなどだが、それに限定されない、予め指定された特定のコンポーネントの完全性のチェックを実施する。このステップでは、コンポーネントの完全性の検証は、完全性測定から得たダイジェスト出力を、デバイス構成データシート中の指定された値と比較することによって、ローカルに実施することができる。コンポーネントは、完全性検証を通った場合、ロードされ実行される。

【００９５】

それ以上のチェックは、ＴｒＥ自体またはＴｒＥの外部だがＴｒＥによって完全性が保護される、Ｈ（ｅ）ＮＢ内の測定側コンポーネントのどちらかによって起こり得る。この

ような後期段階チェックでは、他のコンポーネント、構成、またはＨ（ｅ）ＮＢの残りのパラメータの完全性が、それらがロードされ、もしくはスタートされるとき、または、それらが測定側コンポーネントにとって使用可能な場合は常に、他の、予め定義されたランタイムのイベント時にチェックされ得る。このステップで、完全性チェックの検証はローカルに実施することができる。

【００９６】

Ｈ（ｅ）ＮＢは次いで、ＳｅＧＷとのＩＫＥｖ２（インターネット鍵交換）セキュリティアソシエーションの確立を試みることができる。このプロセスで、Ｈ（ｅ）ＮＢは、ＳｅＧＷに対してそれ自体を認証し、ＳｅＧＷの真正性を検証する。これは、証明書交換および証明書認証によって実施することができる。認証が成功した場合、ＴｒＥは、コンポーネントの失敗によって影響を受ける、失敗した機能性のリストをコンパイルすることによって、ローカル完全性検証の結果をＰＶＥに伝える。ＴｒＥは次いで、メッセージに署名する（ＴｒＥによって保護された署名鍵を使って、したがってメッセージの完全性を保護する）ことができ、こうすることにより、完全性測定および検証、並びに失敗した機能性のリストの（ＰＶＥへの）報告を実施したＨ（ｅ）ＮＢのコア部が、それに対して実施された完全性チェックを通り（例えば、信頼のルート（ＲｏＴ）によって）、したがって署名鍵を使い、署名操作を実施することができ、或いは秘密署名鍵の使用により本質的に信頼されることをアサートする。

【００９７】

図１３Ａ、１３Ｂは、Ｈ（ｅ）ＮＢ１３０５、ＳｅＧＷ１３１０およびＰＶＥ１３１５によって実施されるＳＡＶプロシージャ例１３００を示す。コンポーネント１およびコンポーネント２モジュールのローカル完全性の妥当性確認の後、モジュールがロードされ実行される。コンポーネント３モジュールのデバイス完全性チェックの結果および検証結果が、Ｈ（ｅ）ＮＢ１３０５によってＳｅＧＷ１３１０に送られて、ＰＶＥ１３１５にフォワードされる（０）。

【００９８】

Ｈ（ｅ）ＮＢ１３０５は、ＩＫＥ＿ＩＮＩＴメッセージを送って、暗号アルゴリズム用のセキュリティパラメータ索引、バージョン番号、ＩＫＥｖ２フラグ、ディフィーヘルマン値およびイニシエータノンスを含むＩＫＥｖ２セキュリティアソシエーションの確立を開始することができる（１）。ＳｅＧＷ１３１０は、ＩＫＥ＿ＩＮＩＴ要求メッセージに対するＩＫＥ＿ＩＮＩＴ応答を送ることができる（２）。ＳｅＧＷ１３１０は、Ｈ（ｅ）ＮＢ１３０５から暗号スイートを選ぶことができ、ディフィーヘルマン交換を完了する。Ｈ（ｅ）ＮＢ１３０５は、その証明書を、ＩＫＥ＿ＡＵＴＨ＿ＲＥＱに入れて相互認証のために送ることができる（３）。これは、失敗した機能性のリストの形の完全性検証の結果も含み得る。ローカル完全性検証が成功した場合は、このような失敗した機能性のリストは含まれない。この場合は、空リストが送られる。コンポーネント、モジュールおよび機能性の間の関係については、本明細書に記載した。

【００９９】

ＳｅＧＷ１３１０は、Ｈ（ｅ）ＮＢ１３０５の認証資格を評価することができ、存在する場合はＰＶＥ１３１５に送られるべき機能性ＩＤのリストを抽出する（４）。認証評価が成功した場合、ＳｅＧＷ１３１０は、このことを、Ｈ（ｅ）ＮＢ１３０５に対して示す（５ｓ）。ＳｅＧＷ１３１０は、それ自体の証明書を、応答に入れてＨ（ｅ）ＮＢに送ることもできる。認証が失敗した場合、このことは、Ｈ（ｅ）ＮＢ１３０５に伝達される（５ｆ）。

【０１００】

認証が成功し、失敗した機能性のリストがＩＫＥ＿ＡＵＴＨメッセージに含まれていた場合、ＳｅＧＷ１３１０は、失敗した機能性のリストを、Ｈ（ｅ）ＮＢ　ＩＤとともにＰＶＥ１３１５にフォワードする（６）。リストがない場合、空リストがＰＶＥ１３１５に送られる。失敗した機能性のリストに基づいて、ＰＶＥ１３１５は、デバイスの検疫、完全アクセスの提供、部分アクセスの提供、またはオプションでデバイス修復のためのＨ（

ｅ）ＭＳ介入の要求など、とられるべきアクションを決定することができる（７）。ＰＶＥ１３１５は、影響を受けたその機能性が決定的ではなく、したがってＨ（ｅ）ＮＢ１３０５が機能し得ると判断した場合、この判断をＳｅＧＷ１３１０に対して示して、デバイスがネットワークにアクセスすることを許可する（８ｓ）。ＳｅＧＷ１３１０は、ＰＶＥ１３１５によって実施されたデバイス完全性評価の結果を指示する。失敗したモジュールが決定的でない場合、ＰＶＥ１３１５は、Ｈ（ｅ）ＮＢ１３０５にネットワークへの完全アクセスを許可し得る（９ｓ）。ＰＶＥ１３１５が、失敗した機能性の受信された空リストに全体的または部分的に基づいて、Ｈ（ｅ）ＮＢは認証のために十分に信頼されるはずであると判断した場合、Ｈ（ｅ）ＮＢの「妥当性確認」状態が取得されている。この意味で、妥当性確認は、ネットワークの観点から、Ｈ（ｅ）ＮＢ１３０５が、ＰＶＥ１３１５とのそれ以上の対話のために十分に信用できることを示す、ＰＶＥ１３１５によって行われた判断と翻訳される。

【０１０１】

修復がサポートされる場合、ＰＶＥ１３１５は、Ｈ（ｅ）ＭＳ１３２０に指示を送って、メッセージにおいてＨ（ｅ）ＮＢ　ＩＤによって識別されたデバイスに対する修復をスタートする（８ｆ＿１）。ＰＶＥ１３１５は、失敗したモジュールのリストも含み得る。失敗した機能性のリストおよびデバイス特有の構成データシートに基づいて、Ｈ（ｅ）ＭＳ１３２０は、求められるファームウェアまたはソフトウェアアップデートを決定する。修復がサポートされる場合、ＰＶＥ１３１５は、Ｈ（ｅ）ＮＢ１３０５に指示を送って、Ｈ（ｅ）ＭＳ１３２０が開始した修復を準備することができる（８ｆ＿２）。ＰＶＥ１３１５からの応答に基づいて、ＳｅＧＷ１３１０は、アクセスを制限し、結果をＨ（ｅ）ＮＢ１３０５に知らせることができる（９ｆ）。システムは、ＦＢＣモードでリブートして、デバイス開始修復をスタートする（１０）。このステップは、リブートは、修復用のＴＲ０６９プロトコルを使ってＨ（ｅ）ＭＳ１３２０によって扱われ得るので、オプションでよい。

【０１０２】

ＳＡＶのためのＨ（ｅ）ＭＳおよびＰＶＥ発見プロシージャについて本明細書に記載する。Ｈ（ｅ）ＮＢは、ＰＶＥ、Ｈ（ｅ）ＭＳおよびＯＡＭのＩＰアドレスを含む、工場出荷時設定で構成され得る。こうした設定は、図９に示したように、ＴＲ０６９プロトコルにサポートされるＲＰＣメソッドＳｅｔＰａｒａｍｅｔｅｒおよびＧｅｔＰａｒａｍｅｔｅｒを使って、ＴＲ０６９プロトコルを使うＨ（ｅ）ＭＳによって再構成することもできる。プロシージャは、ＰＶＥのアドレスを変更するのにも用いられ得ることに留意されたい。ＭａｎａｇｅｍｅｎｔＳｅｒｖｅｒ．ＵＲＬパラメータ（ＰｌａｔｆｏｒｍＶａｌｉｄａｔｉｏｎＳｅｒｖｅｒ．ＵＲＬ）に同様の追加パラメータが、Ｈ（ｅ）ＮＢの所でＰＶＥ　ＵＲＬを維持するために定義され得る。同様に、ＰｌａｔｆｏｒｍＶａｌｉｄａｔｉｏｎＳｅｒｖｅｒ．ＵＲＬの工場設定は、製造時に予め構成され、その後でＴＲ０６９によってアップデートされ得る。

【０１０３】

ＳＡＶのための完全性方法およびプロシージャについて本明細書に記載する。ＳＡＶにおいて、デバイス完全性チェックはローカルに実施することができる。完全性チェックの結果は、失敗した機能性のリストの形でＰＶＥに渡すことができる。したがって、本明細書に記載する完全性チェック方法のいずれも、例えば、原文明細書の段落[0038]～[0040]に示したように用いることができる。完全性チェックは、ネットワークエンティティによって実施されるのではない。したがって、妥当性確認に使用するための正確な完全性方法の決定は、製造元に一任され得る。ただし、「完全性方法は、ＳＨＡ－１と等価またはより優れたセキュリティを提供しなければならない」など、最低限のセキュリティ要件は標準化することができる。

【０１０４】

ＳＡＶにおけるＴＲＶ証明書管理に用いられ得る機構について本明細書に記載する。ＳＡＶをサポートするインタフェースおよびメッセージについて、最初に記載する。ＰＶＥ

－ＳｅＧＷインタフェースは、二地点間プロトコル（ＰＰＰ）を使用することができる。ＰＰＰは、認証、暗号化および圧縮のサポートを提供し得る。或いは、ＴＬＳ／ＳＳＬ（トランスポートレイヤセキュリティ／セキュアソケットレイヤ）を使用してもよい。

【０１０５】

ＰＶＥ－ＳｅＧＷインタフェースを介して送ることができる複数のメッセージがある。例えば、Ｈ（ｅ）ＮＢ＿Ｉｎｔｅｇｒｉｔｙ＿Ｉｎｆｏｒｍａｔｉｏｎメッセージは、ＩＫＥｖ２　ＮＯＴＩＦＹメッセージに入れて、Ｈ（ｅ）ＮＢによってＳｅＧＷに送られるとともにＳｅＧＷによって抽出される、失敗した機能性のリストを含み得る。このメッセージの内容の例を、テーブル７に示す。

【０１０６】

【表７】

情報要素	説明
H(e)NB ID	H(e)NBの一意の識別子またはTrE IDを含む。
(オプション)完全性チェックされた全機能性のリスト	(オプション)このリストは、TLV形式であり、チェックされた機能性すべてのリストを含み、そうすることによって、デバイスに対して実施される完全性検査の限度/範囲を示す。このリストは、完全性検査の限度/範囲が、検証元(例えば、PVE)に前もって知られていない場合にのみ送られる。 (代替)或いは、およびやはりオプションで、完全性がチェックされなかった機能性のリストも、チェックされた機能性のリストの代わりに送ることができる。このような代替的リストは、チェックされていない機能性のリストが、チェックされた機能性のリストより短い場合は、サイズがより小さくてよい。この方法は、チェックされ得る全機能性のリスト全体が、検証元に既に知られている場合に作用するに過ぎない。
失敗した機能性のリスト	このリストは、TLV形式であり、失敗した機能性のリストを含む。このリストは、どの機能性も失敗していないことをH(e)NBが報告した場合は空でよい。報告は、信頼できる完全性検証済みコードで生成され、したがって安全なスタートアッププロセスにより信じられることに留意されたい。
ノンス/メッセージシーケンス番号	ノンスまたはメッセージシーケンス番号は、要求と応答を関連付けるものである。

テーブル7

【０１０７】

Ｈ（ｅ）ＮＢ＿Ｉｎｔｅｇｒｉｔｙ＿Ｉｎｆｏｒｍａｔｉｏｎメッセージに対する応答は、テーブル８に示すＨ（ｅ）ＮＢ＿Ｖａｌｉｄａｔｉｏｎ＿Ｒｅｓｕｌｔである。

【０１０８】

【表８】

情報要素	説明
H(e)NB ID	H(e)NBの一意の識別子またはTrE IDを含む。
ノンス/メッセージシーケンス番号	要求と応答を関連付けるためのH(e)NB_Integrity_Information中で与えられるノンス。
SeGWアクション	SeGWが実施し得るアクションは、以下を含む。 1.完全アクセスの許可 2.H(e)MSのみへのアクセスの許可 3.検疫 4.アクセスの却下
H(e)NBアクション	こうしたアクションは、IKEv2 NOTIFYメッセージに入れてH(e)NBにフォワードされる。H(e)NBアクションは、以下であり得る。 1.完全アクセスの許可(アップデートは必要とされず、エラーは起こらない) 2.完全アクセスの許可(アップデートがスケジュールされ、重大度4のエラーが起こる) 3.部分アクセスの許可(アップデートがスケジュールされ、重大度2のエラーが起こる) 4.H(e)MSのみへのアクセス(即座の修復を準備し、重大度3のエラーが起こる) 5.シャットダウン(ローカルエラーコード表示を伴うシャットダウン、管理者はシステムを個人的に解決する、重大度1のエラー)

テーブル8

【０１０９】

両方ともネットワークエンティティなので、ＰＶＥ－Ｈ（ｅ）ＭＳインタフェースは、ＰＰＰにも基づき得る。或いは、ＴＬＳ／ＳＳＬも使用することができる。一例では、ＰＶＥおよびＨ（ｅ）ＭＳは、１つのエンティティでよい。このインタフェースを介したメッセージ例を、テーブル９に示す。

【０１１０】

【表９】

情報要素	説明
H(e)NB ID	H(e)NBの一意の識別子またはTrE IDを含む。
(オプション)完全性チェックされた全機能性のリスト	(オプション)このリストは、TLV形式であり、チェックされた機能性すべてのリストを含み、そうすることによって、デバイスに対して実施される完全性検査の限度/範囲を示す。このリストは、完全性検査の限度/範囲が、検証元(例えば、PVE)に前もって知られていない場合にのみ送られる。 (代替)或いは、およびやはりオプションで、完全性がチェックされなかった機能性のリストも、チェックされた機能性のリストの代わりに送ることができる。このような代替的リストは、チェックされていない機能性のリストが、チェックされた機能性のリストより短い場合は、サイズがより小さくてよい。この方法は、チェックされ得る全機能性のリスト全体が、検証元に既に知られている場合に作用するに過ぎない。
失敗した機能性のリスト	このリストは、TLV形式であり、失敗した機能性のリストを含む。機能性IDについて本明細書に記載する。リストがNULLの場合、このことは、H(e)NBが全完全性チェックを通ったことを示し得る。
H(e)MSアクション指示	これは、デバイス完全性の妥当性確認が実施され、その結果H(e)MSが幾つかのアクションを実施し得ることをH(e)MSに対して示す。以下のアクションを実施することができる。 1.即座の修復 2.修復のスケジューリング 3.管理者介入の要請

テーブル9

【０１１１】

或いは、ＰＶＥは、失敗した機能性のリストを（または、オプションで、完全性チェックされた全機能性のリスト、もしくは完全性チェックされなかった全機能性のリストも）単に送るだけでよく、Ｈ（ｅ）ＭＳが、アクション自体を決定する。これを、テーブル１０に示す。即座の修復、修復のスケジュール、および管理者介入の要請というアクションが、Ｈ（ｅ）ＭＳによって実施され得る。

【０１１２】

【表１０】

情報要素	説明
H(e)NB ID	H(e)NBの一意の識別子またはTrE IDを含む
(オプション)完全性チェックされた全機能性のリスト	(オプション)このリストは、TLV形式であり、チェックされた機能性すべてのリストを含み、そうすることによって、デバイスに対して実施される完全性検査の限度/範囲を示す。このリストは、完全性検査の限度/範囲が、検証元(例えば、PVE)に前もって知られていない場合にのみ送られる。 (代替)或いは、およびやはりオプションで、完全性がチェックされなかった機能性のリストも、チェックされた機能性のリストの代わりに送ることができる。このような代替的リストは、チェックされていない機能性のリストが、チェックされた機能性のリストより短い場合は、サイズがより小さくてよい。この方法は、チェックされ得る全機能性のリスト全体が、検証元に既に知られている場合に作用するに過ぎない。
失敗した機能性のリスト	このリストは、TLV形式であり、失敗した機能性のリストを含む。機能性IDについては、上のセクションに記載した。リストがNULLの場合、このことは、H(e)NBが全完全性チェックを通ったことを示し得る。

テーブル10

【０１１３】

ＳＡＶに関するＨ（ｅ）ＮＢアーキテクチャおよび機能性について本明細書に記載する。Ｈ（ｅ）ＮＢアーキテクチャは、外部ＴｒＥ完全性チェッカを含み得る。Ｈ（ｅ）ＮＢのＴｒＥは、完全性検証のタスクが、ＴｒＥの責任であった、コンポーネントの完全性検証のタスクを、実装されたハードウェアおよび／またはソフトウェアでよい外部エンティティに委任することができる。このようなケースは、ＴｒＥが十分に速くない場合、またはデバイス完全性チェックを実施するのに十分な資源をもたない場合に用いられ得る。このようなケースでは、ＴｒＥは、デバイス完全性の妥当性確認のタスクを始める予定のハードウェアおよび／またはソフトウェアエンティティの完全性および真正性を検証する。検証が成功した後、ＴｒＥは、外部完全性チェッカが、タスクを実施し、結果および測定データをＴｒＥに報告することを許可する。

【０１１４】

Ｈ（ｅ）ＮＢエンティティは、様々なイベント、レポートおよびネットワークとの通信にタイムスタンプを与えるためのローカルタイムサーバを有し得る。このようなタイムサーバは、ＮＴＰ（ネットワークタイムプロトコル）を使って、時間と同期することができる。タイムサーバコードおよびＮＴＰコードも、ＴｒＥまたは外部ＴｒＥ完全性チェッカによって実行される前に完全性検証され得る。

【０１１５】

Ｈ（ｅ）ＮＢアーキテクチャは、妥当性確認および認証のバインドも提供し得る。妥当性確認と認証との間のバインドは、ＡｕＶのケースでの妥当性確認および認証のバインドに使われる機構に加えて、ＩＫＥｖ２セッション、すなわち、完全性チェックを通過したときのみの、敏感鍵および認証機能性のリリースによって提供され得る。ＳＡＶにおける

認証証明書およびローカル妥当性確認の結果は、ＩＫＥｖ２　ＩＫＥ＿ＡＵＴＨ＿ＲＥＱメッセージに入れて送ることができる。ＳｅＧＷは、失敗したモジュールのリストをフィルタリングして選別し、ＰＶＥにフォワードする。このようなリストがメッセージに含まれない場合、ＳｅＧＷは、この情報をＰＶＥに中継する。ＰＶＥは、今後のアクションを決定し、結果をＳｅＧＷに対して、一部のケースではＨ（ｅ）ＭＳに対しても示す。

【０１１６】

代替的バインド方法では、Ｈ（ｅ）ＮＢは、鍵ペアを予め装備し、このペアの私有部は、Ｈ（ｅ）ＮＢのＴｒＥの内側に安全に格納され、公開部は、Ｈ（ｅ）ＮＢにとって使用可能にされる。Ｈ（ｅ）ＮＢの製造元は、この鍵ペアを生成し、したがって私有および公開鍵をプロビジョニングすることができよう。暗号手段によって妥当性確認および認証のバインドを生じるために、Ｈ（ｅ）ＮＢは、ＡＡＡサーバから受信する（ここで、ＡＡＡサーバは、秘密ベースの計算された認証資料を計算し、ＡＡＡサーバに返送するよう、Ｈ（ｅ）ＮＢに要求する）メッセージ（例えば、ＩＫＥ＿ＡＵＴＨ応答メッセージ）を、証明書から得た公開鍵で暗号化し、暗号化データをＴｒＥにフォワードする。ＴｒＥは次いで、データを復号し、ＡＡＡに対してＨ（ｅ）ＮＢの識別の真正性を検証するのに必要とされる秘密ベース認証資料（例えば、対称認証が用いられる場合はＥＡＰ－ＡＫＡ　ＲＥＳパラメータ、または証明書ベースの認証が用いられる場合は私有鍵の使用に基づくＡＵＴＨパラメータなど）を計算する。

【０１１７】

代替的バインド方法では、Ｈ（ｅ）ＮＢのＩＫＥｖ２ベースのデバイス妥当性確認アプリケーションによって使われる、ＴｒＥの鍵および他の敏感な計算能力は、成功したローカル完全性チェック結果がＨ（ｅ）ＮＢのＴｒＥに知られない限り、このようなアプリケーションに対してアクセス可能にされない。

【０１１８】

Ｈ（ｅ）ＮＢおよびＰＶＥに格納されているポリシー仕様について本明細書に記載する。Ｈ（ｅ）ＮＢデバイス構成ファイルは、本明細書において詳しく記載した、機能性ＩＤ、コンポーネントＩＤおよびモジュールＩＤなどの属性を記述する、Ｈ（ｅ）ＮＢに格納されているポリシーを記述する。デバイス構成シートは、製造時に初期化される。ＡｕＶのためのこの情報の初期化および後続アップデートのプロシージャは、本明細書に記載済みであり、ＳＡＶケースに適用可能である。

【０１１９】

ＰＶＥポリシー構成ファイルは、失敗した機能性と、ＳｅＧＷアクション、Ｈ（ｅ）ＮＢアクション、およびＨ（ｅ）ＭＳアクションとの間のマッピングを含み得る。失敗した機能性のリストに基づいて、ＰＶＥは、Ｈ（ｅ）ＮＢ、ＳｅＧＷおよびＨ（ｅ）ＭＳによってとられるべきアクションを決定し得る。テーブル１１は、こうしたアクションを定義する。

【０１２０】

【表１１－１】

失敗した機能性の説明	H(e)NBアクション	SeGWアクション	H(e)MSアクション
安全なブートローダ	シャットダウン	検疫	管理者介入
TrE	シャットダウン	検疫	管理者介入
完全性の妥当性確認エンジン	シャットダウン	検疫	管理者介入
フォールバックコード	シャットダウン	検疫	管理者介入
オペレーティングシステム	シャットダウン	検疫	管理者介入

【０１２１】

H(e)MSサブシステム	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
Uuインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
Iuhインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
HGmインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
HUtインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
S1-MMEインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
S1-Uインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
I2(SIP)インタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
Iu-CSインタフェース	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
Iu-PSインタフェース	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
E, Nc, Nbインタフェース	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
RUAサービス	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
HNBAPサービス	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
HNB GW発見	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
HNB登録	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
HNB用WTRU登録	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
アクセス制御管理	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復

【０１２２】

時間管理	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
CSG管理	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
移動管理	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
NASノード選択機能	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
ページング最適化	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
トランスポートアドレスマッピング	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
請求	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
緊急サービス	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
QoS管理	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
ローカルIPアクセス	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復

【０１２３】

【表１１－２】

管理されるリモートアクセス	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
旧来のCN用のHNBサポート	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
着信ハンドオーバサポート	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
ローミング	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
MSC SGSNへのSCCP無接続通信	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
OAMサブシステム	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
表示サブシステム	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
USIMサブシステム	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
HPMサブシステム	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
IMS連係動作	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
IP-PABXインタフェース			
セキュリティ機能	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
RAB管理	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
無線資源管理	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
Iuリンク管理	H(e)MSのみへのアクセス	H(e)MSのみへのアクセス	即座の修復
IuUプレーン(RNL)管理	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
Iu調整機能	部分アクセスの許可	完全アクセスの許可	修復のスケジュール
プロビジョニング機能	完全アクセスの許可	完全アクセスの許可	修復のスケジュール
ハードウェアの異常	シャットダウン	検疫	管理者介入

テーブル11

【０１２４】

ＳＡＶにおける修復をサポートする方法について本明細書に記載する。修復をサポートするために、Ｈ（ｅ）ＮＢは、Ｈ（ｅ）ＭＳと対話する。この接続は、ＳｅＧＷ経由でも、ＴＬＳ／ＳＳＬを使うインターネットを介して直接でもよい。安全なスタートアッププロセス中に、デバイス完全性チェックが、製造元によって予め指定され、ＴｒＥ用のコードとともに、認証およびＳｅＧＷとの通信に必要なコードを含む段階１または段階２コードに関して失敗した場合、ＦＢＣが実行され、修復が試みられる。

【０１２５】
図１４は、Ｈ（ｅ）ＮＢ１４０５、Ｈ（ｅ）ＭＳ１４１０およびＦＴＰサーバ１４１５が関与するＳＡＶ修復のためのフローチャート例１４００を示す。デバイス完全性チェックが失敗した場合、また、ＦＢＣを使ってＲｏＴが起動した（０）後、Ｈ（ｅ）ＮＢ１４０５は、予め指定されたＨ（ｅ）ＭＳサーバ１４１０への接続を（例えば、ＴＣＰ接続を使用して）セットアップする（１）。次いで、ＳＳＬ開始が実施され、および／または次いで、ＴＬＳがセットアップされる（２）。Ｈ（ｅ）ＮＢ１４０５は次いで、Ｈ（ｅ）ＭＳ１４１０とともにＲＰＣメソッドＩｎｆｏｒｍ（例えば、非常信号）を呼び出す（３）。非常信号は、Ｄｅｖｉｃｅ　ＩＤ、Ｅｖｅｎｔ、ＭａｘＥｎｖｅｌｏｐｅｓおよびＣｕｒｒｅｎｔＴｉｍｅを含み得る。

【０１２６】
デバイスＩＤは、製造元名と、デバイス製造元のＯＵＩ（組織的に一意の識別子）と、シリアルナンバーが該当する製品のクラスを示すのに使用され、またはＴｒＥ　ＩＤもしくはＨ（ｅ）ＮＢ　Ｉｄを示すのにＳｅｒｉａｌＮｕｍｂｅｒ属性を使用させるために、デバイスのシリアルナンバーを示すのに使用することができるＰｒｏｄｕｃｔＣｌａｓｓと、特定のデバイスのシリアルナンバーを送るのに使うことができ、またはＴｒＥ　ＩＤもしくはＨ（ｅ）ＮＢ　ＩＤを送るのに使うことができるＳｅｒｉａｌ　Ｎｕｍｂｅｒフィールドとを含み得る構造である。

【０１２７】
Ｅｖｅｎｔフィールドは、ＲＰＣメソッドＩｎｆｏｒｍを実行させたイベントコードを含み得る。ＴＲ０６９をＳＡＶ修復に適応させるために、デバイス完全性チェックが失敗したこと、およびこの非常信号を送るためにＦＢＣが呼び出されたことを示すための新規イベントコード（Ｘ＿ＨｅＮＢ＿ＦＢＣ　Ｉｎｖｏｋｅｄ）が定義される必要があり得る。ＭａｘＥｎｖｅｌｏｐｅｓ値は、１に設定される。この値は、無視してよいが、１に設定される。ＣｕｒｒｅｎｔＴｉｍｅフィールドは、Ｈ（ｅ）ＮＢ１４０５に知られている現在の日時の値に設定される。

【０１２８】
Ｉｎｆｏｒｍ　ＲＰＣメソッドは、デバイスが完全性チェックに失敗し、ファームウェアアップデートを開始するために接続中であることを、Ｈ（ｅ）ＭＳに対して示す。Ｈ（ｅ）ＭＳは次いで、ＲＰＣメソッドＵｐｌｏａｄを呼び出して、失敗した機能性のリストおよびエラーコードの製造元固有リストをアップロードするよう、Ｈ（ｅ）ＮＢに指示する（４）。こうしたエラーコードは、完全性チェックに失敗したコンポーネントに対応するソフトウェアモジュールを指すこともでき、またはデバッグ特有のエラーコードを含み得る。ファイルがアップロードされなければならないＦＴＰサーバ１４１５のＵＲＬが与えられる。ＦＴＰサーバ１４１５は、製造元によって維持され得ることに留意されたい。ＦＴＰサーバ１４１５は、製造元によって提供される修復サーバでよい。

【０１２９】
Ｈ（ｅ）ＭＳ１４１０は、メッセージＰｒｅｐａｒｅ＿Ｆｏｒ＿Ｕｐｌｏａｄを送ることによって、失敗した機能性のリストのアップロードを準備するよう、ＦＴＰサーバ１４１５に指示する（５）。Ｈ（ｅ）ＮＢ１４０５は次いで、ＨＴＴＰ／ＨＴＴＰＳ／ＦＴＰＳプロシージャを呼び出して、失敗した機能性のリストを含むファイルをアップロードする（６）。ファイル受信の後、ＦＴＰサーバ１４１５またはＨ（ｅ）ＭＳ１４１０は、Ｈ（ｅ）ＭＳがアップロードされたファイルを収集すると、求められるパッチまたはファームウェア／ソフトウェアアップデートを評価して、問題を解決する（６ａ）。失敗した機能性のリストを含むファイルが、ＦＴＰサーバ１４１５にアップロードされた場合、求められるパッチの評価の後で、ＦＴＰサーバ１４１５は、Ｄｏｗｎｌｏａｄ＿Ｐａｃｋａｇｅ＿ＲｅａｄｙメッセージをＨ（ｅ）ＭＳに送る（７）。Ｈ（ｅ）ＭＳが、アップロードされたファイルを収集済みであった場合、このメッセージは求められない。或いは、このメッセージは、Ｈ（ｅ）ＭＳ１４１０およびＦＴＰサーバ１４１５の機能性がマージされる場合は求められなくてもよい。

【０１３０】
或いは、情報は、ＰＶＥから直接受信することができ、ステップ１から５は必要とされなくてもよい。
【０１３１】
Ｈ（ｅ）ＭＳ１４１５は次いで、ＲＰＣメソッドＤｏｗｎｌｏａｄを呼び出し、ファームウェアまたはソフトウェアおよびデバイス構成データシートの場所のＵＲＬを与える（８）。以下のパラメータ値を設定することができる。ＣｏｍｍａｎｄＫｅｙパラメータは、Ｈ（ｅ）ＮＢ１４０５によって、ある特定のダウンロードを指すのに使われ得る文字列であり、任意の文字列でよい。このパラメータは、ダウンロードと応答を相関させるのに使われる。ＦｉｌｅＴｙｐｅパラメータは、ファームウェアイメージの場合は「１　ファームウェアアップグレードイメージ」に、デバイス構成データシートの場合は「Ｘ＿＜ＯＵＩ＞＿ｄａｔａ＿ｓｈｅｅｔ」に設定され得る。ＵＲＬパラメータは、ダウンロードファイルのＵＲＬである。ＨＴＴＰおよびＨＴＴＰＳがサポートされなければならない。ＦＴＰＳのサポートは、ダウンロード用にも推奨され得る。Ｕｓｅｒｎａｍｅパラメータは、Ｈ（ｅ）ＮＢ１４０５によって、ＦＴＰサーバ１４１５に対して認証を行うのに使われ得る。Ｐａｓｓｗｏｒｄパラメータは、Ｈ（ｅ）ＮＢ１４０５によって、ＦＴＰサーバ１４１５に対して認証を行うのに使われ得る。ＦｉｌｅＳｉｚｅパラメータは、ダウンロードされるべきファイルのサイズである。他のパラメータも、ＴＲ０６９プロトコル要件に従って設定され得る。
【０１３２】
Ｈ（ｅ）ＮＢ１４０５は、ＦＴＰサーバ１４１５に接続し、ファームウェアまたはソフトウェアイメージおよびデバイス構成データシートをダウンロードする（９）。ダウンロードの完了が成功すると、値がゼロ（成功を示す）のＳｔａｔｕｓ引数をもつＤｏｗｎｌｏａｄＲｅｓｐｏｎｓｅ、またはＤｏｗｎｌｏａｄ要求に対する障害応答（失敗を示す）が送られ得る（１０）。本明細書に記載する代替的プロシージャに従って、成功または失敗したダウンロードを示してもよい。
【０１３３】
成功したＤｏｗｎｌｏａｄＲｅｓｐｏｎｓｅの後、Ｈ（ｅ）ＭＳ１４１５は次いで、Ｈ（ｅ）ＮＢ１４０５内でＲｅｂｏｏｔプロシージャを呼び出す（１１）。Ｈ（ｅ）ＮＢ１４０５内のＲＰＣハンドラは、ローカル非常フラグをリセットし、正常にブートして、上述したようにローカル完全性チェックプロシージャを実施する（１１ａ）。署名されたパッケージ形式は、ファームウェアまたはソフトウェアがアップデートされた後で、リブートするようＨ（ｅ）ＮＢ１４０５に命令するのに使われるリブートコマンドを含み得る。
【０１３４】
オプションで、ＴｒａｎｓｆｅｒＣｏｍｐｌｅｔｅ　ＲＰＣメソッドをＨ（ｅ）ＮＢから呼び出して、ファームウェア／ソフトウェアアップデートのプロシージャの完了が成功したことをＨ（ｅ）ＭＳに対して示すことができる（１２）。或いは、ＳｅＧＷは、Ｈ（ｅ）ＭＳにメッセージを送って、デバイスがブートに成功したことを示すことができ、このメッセージは、Ｈ（ｅ）ＭＳによって、成功したファームウェアまたはソフトウェアアップデート完了メッセージとして翻訳され得ることに留意されたい。
【０１３５】
図１５は、ＰＶＥによるＳＡＶ修復の実施のためのフローチャート１５００を示す。このプロシージャには、Ｈ（ｅ）ＮＢ１５０５、ＳｅＧＷ１５１０、ＰＶＥ１５１５、Ｈ（ｅ）ＭＳ１５２０およびＦＴＰサーバ１５２５が関与する。安全なスタートアッププロセス中、段階１コードおよび段階２コードが完全性チェックを通り、ロードされ実行され、認証の実施が成功した場合、Ｈ（ｅ）ＮＢ１５０５は、ＳｅＧＷ１５１０と通信して、ローカル完全性チェックの結果をＩＫＥｖ２メッセージに入れて送ることができる（１）。Ｈ（ｅ）ＮＢ１５０５は、失敗した機能性のリストおよび製造元固有エラーコードのリストを、図１６に示すＩＫＥｖ２　ＮＯＴＩＦＹメッセージ１６００に入れてＳｅＧＷ１５１０に送る。

【０１３６】
ＳｅＧＷ１５１０は次いで、ローカル完全性チェックの結果を、失敗した機能性のリストおよび／またはエラーコードの製造元固有リストを含み得るＨ（ｅ）ＮＢ＿Ｉｎｔｅｇｒｉｔｙ＿Ｉｎｆｏｒｍａｔｉｏｎメッセージに入れて送ることができる（２）。受信された情報に基づいて、ＰＶＥ１５１５は、ＳｅＧＷアクションおよびＨ（ｅ）ＮＢアクションを含み得るＨ（ｅ）ＮＢ＿Ｖａｌｉｄａｔｉｏｎ＿ＲｅｓｕｌｔメッセージでＳｅＧＷ１５１０に応答することができる（３）。ＳｅＧＷ１５１０は、Ｈ（ｅ）ＮＢアクションをＨ（ｅ）ＮＢ１５０５にフォワードしてよい（５）。Ｈ（ｅ）ＮＢは、それに従って準備を行い、また、修復の準備をローカルに行ってもよく、何のアクションをとらなくてもよい。

【０１３７】
受信された情報に基づいて、ＰＶＥは、失敗した機能性のリスト、エラーコードの製造元固有リスト、Ｈ（ｅ）ＭＳアクション（複数可）およびＨ（ｅ）ＮＢ　ＩＤを含み得るＨ（ｅ）ＮＢ＿Ｖａｌｉｄａｔｉｏｎ＿ＲｅｓｕｌｔメッセージをＨ（ｅ）ＭＳ１５２０に送ってもよい（４）。ＰＶＥ１５１５によってＨ（ｅ）ＭＳ１５２０に送られたアクションに基づいて、Ｈ（ｅ）ＭＳ１５２０は、修復アップデートまたは即座のアップデートをスケジュールすることができる。両方のケースにおいて、Ｈ（ｅ）ＭＳ１５２０は、製造元固有修復ＦＴＰサーバにリストを送る。

【０１３８】
Ｈ（ｅ）ＭＳ１５２０は、失敗した機能性のリスト、Ｈ（ｅ）ＮＢ　ＩＤ、およびエラーコードの製造元固有リストを含み得るＨ（ｅ）ＮＢ＿Ｖａｌｉｄａｔｉｏｎ＿ＲｅｓｕｌｔメッセージをＦＴＰサーバ１５２５にフォワードしてよい（４ａ）。ＦＴＰサーバ１５２５は、ファームウェア／ソフトウェアダウンロードファイルを評価し、ダウンロードパッケージを準備することができる（４ｂ）。ＦＴＰサーバ１５２５は、Ｄｏｗｎｌｏａｄ＿Ｐａｃｋａｇｅ＿ＲｅａｄｙメッセージをＨ（ｅ）ＭＳ１５２０に送る。Ｈ（ｅ）ＭＳ１５２０が、アップロードされたファイルを収集した場合、このメッセージは求められなくてよい。或いは、このメッセージは、Ｈ（ｅ）ＭＳ１５２０とＦＴＰサーバ１５２５がマージされている場合は送られなくてもよい。

【０１３９】
Ｈ（ｅ）ＭＳ１５２０は次いで、ＲＰＣメソッドＤｏｗｎｌｏａｄを呼び出し、ファームウェア／ソフトウェアおよびデバイス構成データシートの場所のＵＲＬを与える（７）。以下のパラメータ値を設定することができる。ＣｏｍｍａｎｄＫｅｙパラメータは、Ｈ（ｅ）ＮＢ１５０５によって、ある特定のダウンロードを指すのに使われ得る文字列であり、ダウンロードと応答を相関させるのに使われ得る任意の文字列でよい。ＦｉｌｅＴｙｐｅパラメータは、ファームウェア／ソフトウェアイメージの場合は「１　ファームウェアアップグレードイメージ」に、デバイス構成データシートの場合は「Ｘ＿＜ＯＵＩ＞＿ｄａｔａ＿ｓｈｅｅｔ」に設定することができる。ＵＲＬは、ダウンロードファイルのＵＲＬである。ＨＴＴＰおよびＨＴＴＰＳがサポートされなければならない。ＦＴＰＳのサポートは、ダウンロード用にも推奨される。Ｕｓｅｒｎａｍｅパラメータは、Ｈ（ｅ）ＮＢ１５０５によって、ファイルサーバに対して認証を行うのに使われ得る。Ｐａｓｓｗｏｒｄパラメータは、Ｈ（ｅ）ＮＢ１５０５によって、ファイルサーバに対して認証を行うのに使われ得る。ＦｉｌｅＳｉｚｅパラメータは、ダウンロードされるべきファイルのサイズである。他のパラメータは、ＴＲ０６９プロトコル要件に従って設定することができる。

【０１４０】
Ｈ（ｅ）ＮＢ１５０５は、ＦＴＰサーバ１５１５に接続し、ファームウェア／ソフトウェアイメージおよびデバイス構成データシートをダウンロードする（８）。ダウンロードの完了が成功すると、値がゼロの（成功を示す）Ｓｔａｔｕｓ引数をもつＤｏｗｎｌｏａｄＲｅｓｐｏｎｓｅ、またはダウンロード要求に対する障害応答（失敗を示す）がＨ（ｅ）ＭＳ１５２０に送られる（９）。ＴＲ０６９に記載されている代替的プロシージャに従

って、成功または失敗したダウンロードを示すこともできる。

【０１４１】

成功したダウンロード応答の後、Ｈ（ｅ）ＭＳ１５１５は次いで、Ｈ（ｅ）ＮＢ１５０５内でＲｅｂｏｏｔプロシージャを呼び出す（１０）。Ｈ（ｅ）ＮＢ１５０５内のＲＰＣハンドラは、ローカル非常フラグをリセットし、正常にブートして、上で示したようにローカル完全性チェックプロシージャを実施する（１０ａ）。或いは、署名されたパッケージ形式は、ファームウェア／ソフトウェアがアップデートされた後でリブートするよう、Ｈ（ｅ）ＮＢ１５０５に命令するのに使われるリブートコマンドを含む。ファームウェア／ソフトウェアアップデートの完了が成功した後で、転送完了が、ＳｅＧＷ１５１０に送られ得る（１１）。或いは、ＴｒａｎｓｆｅｒＣｏｍｐｌｅｔｅ ＲＰＣメソッドをＨ（ｅ）ＮＢ１５０５から呼び出して、ファームウェア／ソフトウェアアップデートのプロシージャの完了が成功したことを、Ｈ（ｅ）ＭＳ１５２０に対して示すことができる。別の例では、ＳｅＧＷ１５１０は、Ｈ（ｅ）ＭＳ１５２０にメッセージを送って、デバイスのブートが成功したことを示すことができ、このメッセージは、Ｈ（ｅ）ＭＳ１５２０によって、成功したファームウェア／ソフトウェアアップデート完了メッセージとして翻訳され得る。

【０１４２】

プラットフォーム妥当性確認および管理（ＰＶＭ）アーキテクチャにおいてＳＡＶを用いるアーキテクチャおよび方法について本明細書に記載する。ＰＶＭは、デバイスを妥当性確認し管理するための体系的方法を提供し、デバイスは最初に、通信ネットワークに付属し、続いて、信頼できるコンピューティングからのセキュリティ技術に部分的に依拠して、デバイス完全性を監視しようとする。ＰＶＭは、１）ネットワーク接続が許可される前にデバイスを妥当性確認し、２）デバイス構成をＯｔＡ（無線経由で）管理し、３）コンポーネントロード／スタートにおけるＲＩＭをチェックすることによって安全にスタートアップし、４）構成変更のために新規ＲＩＭをデバイスにインストールし、すなわちＲＩＭ摂取を行う。

【０１４３】

ＰＶＭでは、以下の用語が使われ得る。「検証(verification)」という用語は、安全なスタートアップ中のデバイスコンポーネントの内部検証に使うことができ、「妥当性確認(validation)」という用語は、外部エンティティによってデバイスをチェックするプロセス全体に対して使われる。したがって、「内部」対「外部」妥当性確認の導入が避けられる。検証が、暗号チェックまたはデータのマッチングの普通の意味で適用される場合は、混乱を生じないように明記する。

【０１４４】

ＰＶＭは、少なくともＳｅＧＷ、ＰＶＥ、およびＤＭＳを使う。デバイス内のＴｒＥは、デバイスの内側で妥当性確認に不可欠なタスクを実施し、概してＴｒＥは、他のエンティティと通信する。デバイスの他のコンポーネント、例えば、この通信に必要とされるネットワークインタフェースは、必ずしもＴｒＥの統合された一部ではないが、ＴｒＥがこうしたコンポーネントの完全性を評価して、エンドツーエンドのセキュリティを確実にすることは可能であるべきである。

【０１４５】

任務の厳密な区別には、各エンティティがそのコアタスクに制限されることが求められる。例えば、ＳｅＧＷは、信頼できる（できない）デバイスとＭＮＯのＣＮとの間の安全なインタフェースを構築する。このインタフェースは、ＭＮＯのＣＮのための障壁並びにネットワークアクセス制御および強化インスタンスとして作用する。このインタフェースは、このような障壁として作用するのに必要な、認証、デバイスとの通信の暗号化／復号、セキュリティアソシエーションおよびセッション確立を含む全セキュリティ関連機能も実施する。ＳｅＧＷは、ＭＮＯのＣＮと、外部デバイスなどの外界との間の境界を構築するネットワークエンティティの例として使われ得る。ＳｅＧＷの必要なく、ＰＶＭ方法を用いてデバイス妥当性確認を実施することが可能でよい。こうすることは、ＴＬＳ（トラ

ンスポートレイヤセキュリティ）など、安全にされた接続を用いる、ＤＭＳへのデバイスの直接接続を含み得る。

【０１４６】

ＰＶＥに関しては、ＣＮ内の妥当性確認エンティティとして作用し、完全性の妥当性確認を実施する。ＰＶＥは、完全性検証データを受信し、報告された値が既知であり良好かどうかチェックする。ＰＶＥは、デバイス完全性についてのステートメントを、ＣＮ内の他のエンティティに対して発行する。

【０１４７】

ＤＭＳに関しては、ソフトウェアアップデート、構成変更、ＯＴＡ管理および失敗モード修復を含む、デバイスコンポーネントの管理のための中心的エンティティとして作用する。ＤＭＳは、プラットフォーム妥当性確認に基づいてこの機能を始める際、Ｈ（ｅ）ＭＳの強化バージョンと同様である。

【０１４８】

上記エンティティに加え、ＰＶＭは、ＲＩＭマネージャ（ＲＩＭｍａｎ）も含む。ＲＩＭｍａｎは、妥当性確認における比較のための参照値の管理およびプロビジョニングを含む以下のタスクを実施する。ＲＩＭｍａｎは、証明書、特に、外来ＲＩＭ証明書の摂取、ＲＩＭ証明書の検証、（オペレータ特有）ＲＩＭ証明書の生成、および、例えば、撤回、時間制限および信頼関係による証明書妥当性のチェックも管理する。つまり、ＲＩＭマネージャは、一意のエンティティであり、妥当性確認データベース（Ｖ＿ＤＢ）を管理することを認可されている。Ｖ＿ＤＢおよびＲＩＭｍａｎは、保護されたＣＮコンポーネントである。Ｖ＿ＤＢへの書込みアクセスは、ＲＩＭｍａｎのみに限られるので、ＰＶＥはＶ＿ＤＢに書き込むことができない。ＲＩＭｍａｎは、ＰＶＭに必要な（ＳＨＯ－ＣＮ）外部の信頼関係を管理するので、セキュリティに関して特に重要である。

【０１４９】

ＰＶＭは、デバイス構成の管理およびプロビジョニングを実施する構成ポリシーマネージャ（ＣＰｍａｎ）も含む。ＣＰｍａｎは、ポリシー、特に、例えば、ＴＴＰ（信頼できるサードパーティ）からの外来構成およびポリシーの摂取、並びに（オペレータ特有）ターゲットデバイス構成およびポリシーの生成も管理する。つまり、ＣＰｍａｎは、一意のエンティティであり、構成ポリシーデータベースＣ＿ＤＢを管理することを認可されている。ＣＰｍａｎは、ＰＶＭに必要な（ＳＨＯ－ＣＮ）外部の信頼関係を管理するので、セキュリティに関して特に重要である。

【０１５０】

図１７Ａ、１７Ｂは、最小エンティティセット、その関係およびＰＶＭ用インタフェースの例を示す。ＡＡＡ（認証、認可＆アカウンティング）サーバ並びにＷＴＲＵ（ワイヤレス送受信ユニット）およびそのインタフェースなどの追加エンティティを、図示してある。

【０１５１】

図１７ＡのＰＶＭアーキテクチャまたはシステム１７００は、ＴｒＥ１７１０をもつデバイス１７０５を含む。ＷＴＲＵ１７１２（またはユーザエンティティ（ＵＥ））は、Ｉ－ｕｅインタフェース１７１４を介してデバイス１７０５と通信することができる。デバイス１７０５は、Ｉ－ｈインタフェース１７１５を介してＳｅＧＷ１７２０と通信する。概して、デバイス１７０５とＳｅＧＷ１７２０との間のインタフェースＩ－ｈ１７１５は、保護されなくてよく、真正性、完全性およびオプションで、機密性のための特殊措置が、安全なこのチャネルに適用され得る。Ｉ－ｈ１７１５は、デバイス１７０５とＳｅＧＷ１７２０およびしたがってＣＮとの間のリンクを確立するのに使われ得る。例えば、ＳｅＧＷ１７２０は、インタフェースＩ－ａａａ１７７５を介してＡＡＡサーバと通信し得る。オペレータは、インタフェースのセキュリティを確実にするための適切な措置を確立済みでよい。

【０１５２】

Ｉ－ｐｖｅインタフェース１７２２は、ＳｅＧＷ１７２０によって、妥当性確認中にＰ

ＶＥ１７２４に接触するのに使われ得る。ＰＶＥ１７２４は、Ｉ－ｐｖｅインタフェース１７２２を使って、妥当性確認の出力結果をＳｅＧＷ１７２０にシグナリングすることができる。Ｉ－ｄｍｓインタフェース１７３０は、ＤＭＳ１７３５とＳｅＧＷ１７２０との間のデバイス構成関連通信に使われ得る。Ｉ－ｐｄインタフェース１７３２は、ＰＶＥ１７２４によって、ＤＭＳ１７３５と、およびその反対に通信を行うのに使われ得る。このインタフェース、すなわちＩ－ｐｄ１７３２は、デバイスソフトウェアアップデートおよび構成変更のためなど、デバイス管理プロシージャ中に使われ得る。

【０１５３】

インタフェースＩ－ｖ１７２６およびＩ－ｄ１７３８は、それぞれ、ＰＶＥ１７２０によって、Ｖ＿ＤＢ１７４０からＲＩＭを読み出すのに、また、ＤＭＳ１７３５によって、許可された構成をＣ＿ＤＢ１７５０から読み出すのに使われ得る。インタフェースＩ－ｒ１７２８およびＩ－ｃ１７３４は、Ｖ＿ＤＢ１７４０中にないＲＩＭのケースなどでは、ＰＶＥ１７２０によって、ＲＩＭｍａｎ１７６０と通信するのに、また、ＤＭＳ１７３５によって、ＣＰｍａｎ１７７０と通信するのに使われ得る。ＲＩＭｍａｎ１７６０およびＣＰｍａｎ１７７０は、インタフェースＩ－ｒｄｂ１７６２およびＩ－ｃｄｂ１７７２を使って、それぞれ、データベースＶ＿ＤＢ１７４０および構成ポリシーデータベースＣ＿ＤＢ１７５０の妥当性確認を読み出し、書き込み、管理することができる。

【０１５４】

図１７Ｂは、デバイス１７０５がＤＭＳ１７３５に直接接続し得るＰＶＭ１７８２を示す。デバイスがＨ（ｅ）ＮＢである場合、ＤＭＳ１７３５は、本明細書において上で記載したように、Ｈ（ｅ）ＭＳになる。例えば、デバイス１７０５がＳｅＧＷとのセキュリティプロトコルを実施可能でないフォールバックモードの場合。この場合、ＤＭＳ１７３５は、インタフェースＩ－ｄｍｓ＿ｄ１７８４を介したデバイス１７０５用の第１の接触点として作用し、インタフェースＩ－ｐｖｅ１７８６およびＩ－ｐｄ１７８８を介してＰＶＥ１７２４と通信して、妥当性確認を実施し、または少なくとも、どのコンポーネントが安全なスタートアップ中に失敗したかを知ることができる。ＤＭＳ１７３５は、修復のためにこの情報に対して作用し得る。

【０１５５】

本明細書において述べたように、ＰＶＭは、妥当性確認のどのバージョンも使うこともできる。ＰＶＭと連動する半自律的妥当性確認（ＳＡＶ）の実施形態について本明細書に記載する。半自律的妥当性確認（ＳＡＶ）の高度妥当性確認方法に注目する。ＳＡＶ用のこのソリューションの利点はさらに、ＣＮが不良デバイスから完全に保護されることである。ＳＡＶの間、検疫が、ＳｅＧＷによって有効に確立される。そのタスクに限られたデータのみを、ＳｅＧＷとの安全な、またはＳｅＧＷによって確立された接続を介してのみ受信するので、デバイスからはＰＶＥおよびＤＭＳに対してどのような直接的脅威も課されない。ＳＡＶにおける妥当性確認プロセスは、デバイスとＣＮ内のどのエンティティとの間の直接通信も求めない。ＳＡＶを用いた妥当性確認成功の後でのみ、ＣＮへの接続が許可される。こうすることにより、証明された安全な状態にあるデバイスのみが、ＣＮの内側のエンティティと通信し得ることが確実になる。

【０１５６】

図１８Ａ、１８Ｂ、１８Ｃは、ＰＶＭインフラストラクチャを用いるＳＡＶ妥当性確認方法の例の図を示す。ＰＶＭインフラストラクチャは、ＴｒＥ１８０５、ＳｅＧＷ１８０７、ＰＶＥ１８０９、ＤＭＳ１８１１、Ｖ＿ＤＢ１８１３およびＣ＿ＤＢ１８１５を含む、本明細書に記載するエンティティを含む。相互認証（１８２０）に続いて、ＴｒＥ１８０５は、Ｄｅｖ＿ＩＤ、製造元、デバイス能力であって、サポートされるデータレートなどの通信能力、伝送電力レベル、シグナリング特徴および他の能力、ＴｒＥ能力を含むが、それに限定されないデバイス能力などのデバイス情報、およびＲｏＴを含むプロパティと、ＩＤ、証明情報、製造元、ビルドバージョン、およびオプションでモデル、メーク、シリアルナンバーを含むＴｒＥ＿ｉｎｆｏｒｍａｔｉｏｎと、１）デバイスの失敗した機能性のリスト、並びに／または２）ＰＣＲ（プラットフォーム構成レジスタ）値、ＰＣＲ

値による署名などの検証バインディングまたは失敗したデバイス機能性のリスト、コンポーネントに対するコンポーネントインジケータ（ＣＩｎｄ）の順序付きリストＣｌｉｓｔを含む検証データというデータの一部もしくは全部を収集することができ、コンポーネント用パラメータおよびタイムスタンプ（信頼できる、またはできない）を含み得る（１８２２）。ＴｒＥ１８０５からＳｅＧＷ１８０７への妥当性確認メッセージ／データは、上記日付を含み得る（１８２４）。

【０１５７】

ＳｅＧＷ１８０７は、受信されたタイムスタンプを、ローカルタイムとチェック／比較して、変形を検出しなければならない（１８２６）。報告されたタイムスタンプがローカルタイムと合致しない場合、ＳｅＧＷは、報告されたタイムスタンプのプロパティに従って作用する。デバイスのタイムスタンプが、信頼できるタイムスタンプであり、変化を示す場合、ＳｅＧＷ１８０７は、ＴｒＥおよびその信頼できるタイムソースの再妥当性確認をトリガするべきである。信頼できないタイムスタンプのケースでは、ＳｅＧＷ１８０７は、それ自体の信頼できるタイムスタンプをメッセージに追加する。デバイスが、信頼できるタイムスタンプを提供可能でない場合、ＳｅＧＷ１８０７は、反射攻撃に対する保護として、信頼できるタイムスタンプを追加すればよい。

【０１５８】

このメッセージを受信すると、ＳｅＧＷ１８０７は、ＴｒＥからの署名の形の検証バインディングが存在するかどうかチェックすることができる（１８２８）。このチェックにより、検証データの真正性が確実にされる。ＳｅＧＷ１８０７は次いで、ＰＶＭトークン（Ｔ　ＰＶＭ）を作成し（１８３０）、送付前にＴ－ＰＶＭに対してタイムスタンプを印加して、フレッシュネスを確約し、非同期メッセージフローを防止する（１８３２）。

【０１５９】

ＳｅＧｗ１８０７は、Ｔ＿ＰＶＭをＰＶＥ１８０９にフォワードし（１８３４）、ＰＶＥ１８０９は、ＴｒＥ情報を使ってＶ＿ＤＢ１８１３を照会する（１８３６）。信用できない判定がＰＶＥ１８０９に戻された（１８３８）場合、ＰＶＥは、Ｔ＿ＰＶＭにタイムスタンプを印加し（１８４０）、ＳｅＧＷ１８０７にフォワードする（１８４２）。ＳｅＧＷ１８０７は、デバイス妥当性確認の拒否をＴｒＥ１８０５に送る（１８４４）。

【０１６０】

信用できる判定がＰＶＥ１８０９に戻された（１８４６）場合、ＰＶＥは、Ｄｅｖ＿ＩＤを使ってＣ＿ＤＢを照会し（１８４８）、Ｃ＿ＤＢは、構成ポリシー（１８５０）をＰＶＥ１８０９に戻す。ＰＶＥ１８０９は、ポリシー構成を評価する（１８５２）。

【０１６１】

ＰＶＥ１８０９が、構成は信用できない（１８５４）と判定した場合、ＰＶＥ１８０９は、Ｔ－ＰＶＭを修正し、タイムスタンプを印加する（１８５６）。ＰＶＥ１８０９は次いで、Ｔ＿ＰＶＭをＳｅＧＷ１８０７にフォワードし（１８５８）、ＳｅＧＷ１８０７は、デバイス妥当性確認の拒否をＴｒＥ１８０５に送る（１８６０）。

【０１６２】

ＰＶＥ１８０９が、構成は信用できると判定し、構成を許可した（１８６２）場合、ＰＶＥ１８０９は、Ｖ－ＤＢ１８１３からＣｌｉｓｔまたはＣ＿Ｌｉｓｔ中の全エントリに対するＲＩＭを取り出す（１８６４）。ＰＶＥ１８０９は、ＲＩＭから正しい検証データを算出し直し（１８６６）、算出された検証データを、報告された検証データと比較する（１８６８）。ＳＡＶのケースでは、ＲＩＭから算出された検証データは、失敗した機能性の「空リスト」の形になる。ＰＶＥ１８０９は次いで、Ｔ－ＰＶＭを修正し、タイムスタンプを印加する（１８７０）。ＰＶＥ１８０９は次いで、Ｔ＿ＰＶＭをＳｅＧＷ１８０７にフォワードする（１８７２）。ＳｅＧＷ１８０７は、ＰＶＥ妥当性確認結果に関してＴ＿ＰＶＭを検査する（またはＴ＿ＰＶＭから抽出する）（１８７４）。ＳｅＧＷ１８０７は、デバイス妥当性確認の拒否または許可をＴｒＥ１８０５に送る（１８７６）。ＰＶＥ妥当性確認結果が否定である場合、ＴｒＥ１８０５は、リブートを実施し、再妥当性確認を行う（１８９０）。

【０１６３】
オプションで、ＰＶＥ１８０９が、算出された検証データを、報告された検証データと比較した（１８６８）後、ＰＶＥ１８０９は、失敗したコンポーネントのリストをＤＭＳ１８１１に送ることができる（１８７８）。失敗したコンポーネントのリストが空でない場合、ＤＭＳ１８１１は、ソフトウェアまたはファームウェアのアップデートを適用することができると判定してよく（１８８０）、適用できる場合、ＯＴＡアップデートを準備する（１８８２）。ＤＭＳ１８１１は、アップデートのためのＲＩＭがＶ＿ＤＢ１８１３中に存在することも確実にする（１８８４）。ＤＭＳ１８１１は、再妥当性確認の指示とともにＴ＿ＰＶＭをＳｅＧＷ１８０７に（１８８６）、また、再妥当性確認トリガをＴｒＥ１８０５に（１８８８）送る。ＴｒＥ１８０５は、リブートを実施し、再妥当性確認を行う（１８９０）。

【０１６４】
図１８Ａ、１８Ｂ、１８Ｃにおける処理に関する詳細について本明細書に記載する。プラットフォーム妥当性確認を実施するために、ＴｒＥは、以下のデータを収集し、ＳｅＧＷに伝達する。すなわち、Ｄｅｖ＿ＩＤ、製造元、ＴｒＥ能力およびＲｏＴを含むプロパティなどのデバイス情報と、ＩＤ、証明情報、製造元、ビルドバージョン、およびオプションでモデル、メーク、シリアルナンバーを含むＴｒＥ＿ｉｎｆｏｒｍａｔｉｏｎと、完全性検証データ（ＩＶＤ）（ＩＶＤの一例は、署名されたＰＣＲ（プラットフォーム構成レジスタ）値でよく、別の例は単に、その完全性がデバイスにローカルな完全性チェックプロセスによってチェック済みであり、さらにこのようなデバイスにローカルな完全性チェックに失敗したとして評価済みであるコンポーネントまたは機能性のリストでよい）と、ＰＣＲ値による署名などの検証バインディングと、コンポーネントＣｌｉｓｔに対するコンポーネントインジケータ（ＣＩｎｄ）の順序付きリストであるとともにコンポーネント用パラメータを含み得るＣｌｉｓｔとである。コンポーネントのリストは、例えば、ＲＩＭ証明書、すなわちＲＩＭｃｓをポイントすることによって、妥当性確認用ＲＩＭを識別するのに役立つ。コンポーネントおよびそのパラメータに対するインジケータの順序付きリストは、索引、ｃｏｍｐｏｎｅｎｔ＿ｉｎｄｉｃａｔｏｒ　ＣＩｎｄ、ｃｏｍｐｏｎｅｎｔ＿ｐａｒａｍｅｔｅｒｓというデータフィールドなどのエントリを含むことになる。ＣＩｎｄは、コンポーネントへの参照を与え、ＵＲＮ形式でよい（例えば、ＵＲＮ：／／ｖｅｎｄｏｒ．ｐａｔｈ．ｔｏ／ｃｏｍｐｏｎｅｎｔ／ｃｅｒｔｉｆｉｃａｔｅ）。オプションで、タイムスタンプ（信頼できるタイムスタンプでも、概して必ずしも信頼できるわけではない通常のタイムスタンプでもよい）がある。

【０１６５】
デバイスのケースでは、妥当性確認メッセージは、ＩＤ、証明情報、製造元、モデル、バージョン、メーク、シリアルナンバー、ＲｏＴを含むＴｒＥ能力およびプロパティ、デバイスのセキュリティポリシー、完全性検査および事後検査コンポーネントローディングの複数ステッププロセスの異なる段階で完全性チェックされるモジュール、ＨＷビルドバージョン番号、並びにオプションでＳＷビルドバージョン番号および完全性測定データなどのデバイス情報をさらに含み得る。

【０１６６】
妥当性確認のためにＲＩＭを使用することは、好ましいがオプションのＳＡＶのための方法である。ここではベースケースとして使われ、他の選択肢はこのケースからはずれ、逸脱する。例えば、ＲＩＭから検証データを算出し直さない妥当性確認があり、実施用ＰＶＭを完全にＲＩＭなしで行う可能性さえもある。

【０１６７】
検証バインディングは、デバイスの完全性を伴うもの以外の手段によって、例えば、安全なチャネルの存在および使用によって妥当性確認メッセージが認証にバインドされる場合はオプションでよい。

【０１６８】
ＳｅＧＷは、受信されたタイムスタンプを、ローカルタイムとチェック／比較して、変

形を検出することができる。報告されたタイムスタンプが、ローカルタイムと合致しない場合、ＳｅＧＷは、報告されたタイムスタンプのプロパティに従って作用する。デバイスのタイムスタンプが、信頼できるタイムスタンプであり、変化を示す場合、ＳｅＧＷは、ＴｒＥおよびその信頼できるタイムソースの再妥当性確認をトリガすることができる。信頼できないタイムスタンプのケースでは、ＳｅＧＷは、それ自体のタイムスタンプをメッセージに追加する。

【０１６９】

ＴｒＥ＿ｉｎｆｏはオプションでよい。Ｄｅｖ＿ＩＤは、ＴｒＥ＿ｉｎｆｏへの参照を与え得る。全ＭＮＯが全ＴｒＥを、およびしたがって全ＴｒＥ＿ｉｎｆｏデータを知るわけではないので、このようなマッピングは、所与の任意のＤｅｖ＿ＩＤに関するＴｒＥ＿ｉｎｆｏを取得するためにＭＮＯによって照会され得るデータベースによって与えられ得る。ＴｒＥ＿ｉｎｆｏは、ＴｒＥ＿ｃｅｒｔｉｆｉｃａｔｅ中にあり得る。ＴｒＥ＿ｃｅｒｔｉｆｉｃａｔｅは、ＴｒＥまたはＴＴＰのベンダ、例えば、独ＢＳＩによって署名されるべきである。

【０１７０】

コンポーネントに対するインジケータ（ＣＩｎｄ）としてのＵＲＮの使用は、コンポーネントおよびＲＩＭまたはＲＩＭ証明書を取り出すことができる場所のこの一意の識別を同時に許可するので、有利である。

【０１７１】

ＳｅＧＷは、ローリングトークンとして使うことができるとともに通信中にエンティティからエンティティに渡されるＰＶＭトークン（Ｔ＿ＰＶＭ）を作成する。すべてのエンティティは、送付前にトークンにタイムスタンプを押して、フレッシュネスを確約し、非同期メッセージフローを防止する。トークンに対するタイムスタンプは、トークンの状態に従う方法を提供するのに使われ得る。トークンは、ＣＮ内でエンティティからエンティティに何巡も移動することができ、したがって、エンティティによって追跡することができる。オプションで、エンティティＩＤが、タイムスタンプされたデータの連鎖に組み込まれ得る。

【０１７２】

Ｔ＿ＰＶＭは、Ｄｅｖ＿ＩＤを含み得る。オリジナルタイムスタンプが存在せず、または信頼されない場合、Ｔ＿ＰＶＭは、ＳｅＧＷによって発行される新規タイムスタンプを含んでもよい。そうでない場合、Ｔ＿ＰＶＭは、妥当性確認メッセージからのオリジナルタイムスタンプを含み得る。

【０１７３】

タイムスタンプは、反射攻撃に対する保護に使われ得る。タイムスタンプは、ノンスまたは単調に増加するカウンタと組み合わせることも、それで置き換えることもできる。タイムスタンプは、妥当性確認データのフレッシュネスを評価するのに使うこともできる。両方の目的を組み合わせることが有利であり、タイムスタンプによって提供され得る。

【０１７４】

第１の変形体において、ＤＭＳによる以降のデバイス管理のために、Ｔ＿ＰＶＭは、ＤＭＳとＴｒＥ、例えば、ＴＬＳ証明書との間の安全なトンネルを構築する通信秘密を含み得る。

【０１７５】

ＳｅＧＷは、全アクティブＴ＿ＰＶＭを含むトークンデータベースＴ＿ＤＢを維持する。

【０１７６】

ＳｅＧＷは、妥当性確認データ、ＴｒＥ＿ｉｎｆｏ、およびＣｌｉｓｔというデータを妥当性確認メッセージから抽出する。このデータをトークンＴ＿ＰＶＭと一緒に送る前に、ＳｅＧＷは、Ｔ＿ＰＶＭにタイムスタンプを押し、ＰＶＥにフォワードする。ＳｅＧＷは、妥当性確認メッセージおよびその一部の形式をチェックして、不正形式のデータ攻撃からの脅威を軽減させることができる。そうしないと、ＰＶＥでのこのデータの純粋な検

査が、システムエラーまたは失敗につながるように、攻撃者が、危害を受けたＴｒＥの妥当性確認メッセージ中のデータを修正しようとする可能性がある。

【０１７７】

ＰＶＥは、デバイスの妥当性を決定するエンティティである。つまり、ポリシーシステムの言葉では、ポリシー決定点（ＰＤＰ）である。任務の厳密な区別という手法の下では、ＰＶＥはＰＶＭシステム内の唯一のＰＤＰである。ＰＤＰは、ＳｅＧＷおよびＤＭＳに依拠して、ポリシー施行点（ＰＥＰ）として作用するなどのポリシーを施行する。ＰＶＭは、その概要において、どのようにポリシーが生成されるか、および、どこからＰＶＥがポリシーを得るかなど、どこに格納／管理されるかという疑問を問わないままである。後で説明するより詳細な変形体および付随方法の一部では（特定のパラメータに関する妥当性確認および最低限の妥当性確認では）、ポリシー条件およびアクションの幾つかの例が挙げられる。概して、妥当性確認ポリシーの決定は、単一のコンポーネントの妥当性だけではなく、Ｃｌｉｓｔに含まれる他のデータにも基づき得る。特に、許可されるパラメータ（範囲）、およびロードの順序（Ｃｌｉｓｔが順序づけられる）が評価され得る。

【０１７８】

ＰＶＥによって実行される妥当性確認プロセス中に起こり得る失敗条件の幾つかの根本的クラスがある。例えば、失敗条件Ｆ１は、「ＴｒＥ無効」シナリオを示す。認証されたそのＤｅｖ＿ＩＤおよび配布されたＴｒＥ＿ｉｎｆｏによって、ＰＶＥは、デバイスおよび／またはそのＴｒＥを、信用できないものと識別する。注：ＴｒＥが無効であり得るかどうか判定するのに用いられ得る情報は、ＳＡＶ妥当性確認メッセージ自体にのせて搬送することができ、または他のメッセージもしくは他の手段から推定することができる。その基本的な形において、ＳＡＶ妥当性確認メッセージの存在は、ＴｒＥ自体が有効でなければならないことを暗黙的に示し得る。Ｆ１がどのように検出され得るかについての詳細は、本明細書において完全に説明されているものとして、参照によって組み込まれている、同時に出願した、「Platform Validation and Management of Wireless Devices」という名称の米国特許出願第12/718,480号明細書に論じられている。

【０１７９】

別の例は、「ＩＶＤ検証失敗」に関する３つのシナリオを示す失敗条件Ｆ２である。シナリオＦ２ａは、完全性測定／検証データ不一致を示す。Ｆ２ａは、デバイスの安全なスタートアッププロセスの失敗、並びに／またはデバイス上での偽および／もしくは失効したＲＩＭおよび／もしくはＲＩＭ証明書の存在を示し、これにより次いで、無効コンポーネントがスタートされる。シナリオＦ２ｂは、ＲＩＭ欠如を示し、すなわち、コンポーネント用ＲＩＭが欠如しており、どこか他の所から取り出される必要がある。シナリオＦ２ｃは、失効したＲＩＭ証明書を示す。

【０１８０】

失敗条件Ｆ３は、「Ｃｌｉｓｔポリシー失敗」に関する２つのシナリオを示す。シナリオＦ３ａに対して、単一のコンポーネントが有効であるが、構成は、例えば、ロード順序、または望まれないコンポーネント、またはパラメータに対するポリシーに失敗する。シナリオＦ３ｂは、Ｃｌｉｓｔの「既知の良好値」が利用できないように、構成が未知であることを示す。

【０１８１】

失敗条件クラスＦ２の検出および取扱い方法について本明細書に記載する。失敗条件Ｆ２に対して、ＰＶＥは、受信されたＣｌｉｓｔにある全コンポーネント用のＶ＿ＤＢからＲＩＭを取り出す。妥当性確認データベースＶ＿ＤＢは、認証されたＲＩＭのみを格納する。対応するＲＩＭ証明書は、Ｖ＿ＤＢに安全に格納されなければならない。

【０１８２】

ＩＶＤが、本明細書に記載した狭義のＳＡＶプロシージャに記載されるように、「ローカル完全性検査に失敗した、デバイスのコンポーネントに対応する、デバイスのコンポーネント」の単純なリストの形である場合、ＩＶＤ＿ｒｅｆは、単にNULLリストの形になる。つまり、ＩＶＤ＿ｒｅｆは、この場合、失敗した機能性の期待されるリストに過ぎない

はずであり、このリストは、すべてのコンポーネントがデバイスにローカルな完全性検査を通ったことを期待される場合はNULLテーブルであるべきである。

【０１８３】

ＩＶＤ＿ｒｅｆが受信されたＩＶＤと合致しない場合、デバイス上での安全なスタートアッププロセスが危害を受けており、または誤ったＲＩＭがデバイスに格納されており、したがって無効コンポーネントが安全なスタートアッププロセス中にロードされている。

【０１８４】

Ｆ２ａポリシーに依存して、Ｆ２ａ失敗が検出されると、幾つかの選択肢が該当し得る。１つの選択肢では、拒絶である。ＰＶＥは、妥当性確認の出力結果をＳｅＧＷにシグナリングする。ＳｅＧＷは次いで、ネットワークアクセスを拒否しても、デバイスを検疫ネットワークに入れてもよい。第２の選択肢はアップデートである。検証データ失敗を示す妥当性確認結果（Ｔ＿ＰＶＭ）を受信した後、ＤＭＳは、管理プロセスをスタートして、妥当性確認に失敗したコンポーネントを置き換える。このような修復プロセスの詳細は、本明細書において完全に説明されているものとして、参照によって組み込まれている、同時に出願した、「Platform Validation and Management of Wireless Devices」という名称の米国特許出願第12/718,480号明細書に論じられている。

【０１８５】

どのポリシー失敗条件も満たされない場合、デバイスは有効である。ＰＶＥは、このことをＳｅＧＷにシグナリングし、ＳｅＧＷは次いで、ＣＮへの接続を許可する。

【０１８６】

ＲＩＭが欠如している失敗条件Ｆ２ｂの場合、これは、ＲＩＭがＶ＿ＤＢ中にないか、またはデバイスにない（その結果、この場合、デバイスは、デバイスにローカルな完全性検査プロシージャを実施することができなくなる）ので、起こり得る。Ｆ２がどのように検出され取り扱われ得るかについての詳細は、本明細書において完全に説明されているものとして、参照によって組み込まれている、同時に出願した、「Platform Validation and Management of Wireless Devices」という名称の米国特許出願第12/718,480号明細書に論じられている。

【０１８７】

失敗条件クラスＦ３の検出および取扱い方法について本明細書に記載する。Ｆ３失敗条件は、単一のコンポーネントが有効であるがコンポーネントの構成がポリシーに失敗した（例えば、ロード順不一致）場合、または構成が未知である、すなわち、Ｃｌｉｓｔの「既知の良好な値」が入手できない場合に起こる。このような失敗条件がどのように起こり得るか、およびこのような失敗条件がどのように取り扱われ得るかについての詳細は、本明細書において完全に説明されているものとして、参照によって組み込まれている、同時に出願した、「Platform Validation and Management of Wireless Devices」という名称の米国特許出願第12/718,480号明細書に論じられている。

【０１８８】

図１９は、Ｈ（ｅ）ＮＢを含むＬＴＥ（ロングタームエボリューション）ワイヤレス通信システム／アクセスネットワーク１９００とともに使われ得るＥ－ＵＴＲＡＮ（進化型ユニバーサル地上無線アクセスネットワーク）１９０５を示す。Ｅ－ＵＴＲＡＮ１９０５は、ＷＴＲＵ１９１０、および幾つかのｅＮＢ（evolved Node-B）１９２０を含む。ＷＴＲＵ１９１０は、ｅＮＢ１９２０と通信する。ｅＮＢ１９２０は、Ｘ２インタフェースを使って互いとインタフェースをとる。ｅＮＢ１９２０はそれぞれ、Ｓ１インタフェースを介して、ＭＭＥ（移動管理エンティティ）／Ｓ－ＧＷ（サービングゲートウェイ）１９３０とインタフェースをとる。単一のＷＴＲＵ１９１０および３つのｅＮＢ１９２０を図１９に示してあるが、ワイヤレスおよびワイヤードデバイスのどの組合せも、ワイヤレス通信システムアクセスネットワーク１９００に含まれ得ることが明らかであろう。

【０１８９】

図２０は、ＷＴＲＵ１９１０、ｅＮＢ１９２０、およびＭＭＥ／Ｓ－ＧＷ１９３０を含むＬＴＥワイヤレス通信システム２０００の例示的ブロック図である。図２０に示すよう

に、ＷＴＲＵ１９１０、ｅＮＢ１９２０およびＭＭＥ／Ｓ－ＧＷ１９３０は、自律的および半自律的妥当性確認を用いるＨ（ｅ）ＮＢ完全性検証および妥当性確認の方法を実施するように構成される。

【０１９０】

典型的なＷＴＲＵにおいて見られ得るコンポーネントに加え、ＷＴＲＵ１９１０は、オプションのリンクされたメモリ２０２２を有するプロセッサ２０１６、少なくとも１つのトランシーバ２０１４、オプションのバッテリ２０２０、およびアンテナ２０１８を含む。プロセッサ２０１６は、自律的および半自律的妥当性確認を用いるＨ（ｅ）ＮＢ完全性検証および妥当性確認の方法を実施するように構成される。トランシーバ２０１４は、プロセッサ２０１６およびアンテナ２０１８と通信して、ワイヤレス通信の送受信を容易にする。ＷＴＲＵ１９１０内でバッテリ２０２０が使われるケースでは、バッテリ２０２０は、トランシーバ２０１４およびプロセッサ２０１６に電力を供給する。

【０１９１】

典型的なｅＮＢ（Ｈ（ｅ）ＮＢを含む）において見られ得るコンポーネントに加え、ｅＮＢ１９２０は、オプションのリンクされたメモリ２０１５を有するプロセッサ２０１７、トランシーバ２０１９、およびアンテナ２０２１を含む。プロセッサ２０１７は、自律的および半自律的妥当性確認を用いるＨ（ｅ）ＮＢ完全性検証および妥当性確認の方法を実施するように構成される。トランシーバ２０１９は、プロセッサ２０１７およびアンテナ２０２１と通信して、ワイヤレス通信の送受信を容易にする。ｅＮＢ１９２０は、オプションのリンクされたメモリ２０３４を有するプロセッサ２０３３を含むＭＭＥ／Ｓ－ＧＷ（移動管理エンティティ／サービングゲートウェイ）１９３０に接続される。

【０１９２】

ＳｅＧＷおよびＰＶＥは、図１９、２０には示していないが、典型的なＳｅＧＷおよびＰＶＥにおいて見ることができるコンポーネントに加え、オプションのリンクされたメモリ、トランシーバ（複数可）、アンテナ（複数可）、および通信ポートを有するプロセッサを含み得る。プロセッサは、プラットフォーム妥当性確認および管理機能を実施して、ＰＶＭ手順を実装するように構成される。トランシーバおよび通信ポートは、必要に応じて、プロセッサおよびアンテナと通信して、通信内容の送信および受信を容易にする。

【０１９３】

実施形態

１．Ｈ（ｅ）ＮＢ（ｈｏｍｅ　ｅｖｏｌｖｅｄ　Ｎｏｄｅ　Ｂ）の完全性検証を実施する方法であって、コンポーネントのローディングに先立って、コンポーネントに関する完全性メトリックを測定することを含む方法。

【０１９４】

２．実施形態１の方法において、信頼できる参照値（ＴＲＶ）を認証することをさらに含む方法。

【０１９５】

３．上記実施形態のいずれかに記載の方法において、測定された完全性メトリックをＴＲＶと比較することをさらに含む方法。

【０１９６】

４．上記実施形態のいずれかに記載の方法において、完全性検証結果に依存して、通常コードまたはフォールバックコードの一方で、Ｈ（ｅ）ＮＢをスタートすることをさらに含む方法。

【０１９７】

５．上記実施形態のいずれかに記載の方法において、ソフトウェアモジュールと、参照完全性メトリック、並びにＨ（ｅ）ＮＢおよびプラットフォーム妥当性確認エンティティ（ＰＶＥ）の少なくとも一方に対する重大度の少なくとも１つを含む、関連付けられた属性のリストとを提供することをさらに含む方法。

【０１９８】

６．上記実施形態のいずれかに記載の方法において、デバイス構成データシートは、ソ

フトウェアモジュールおよび関連付けられた属性のリストを含み、Ｈ（ｅ）ＮＢおよびプラットフォーム妥当性確認エンティティ（ＰＶＥ）の少なくとも一方に与えられる方法。

【０１９９】

７．上記実施形態のいずれかに記載の方法において、関連付けられた属性は、コンポーネントおよび機能性に関して、ソフトウェアモジュールのマッピングを可能にする方法。

【０２００】

８．上記実施形態のいずれかに記載の方法において、デバイス構成データシートと、ソフトウェアモジュールおよび関連付けられた属性のリストとの少なくとも一方は、Ｈ（ｅ）ＮＢおよびプラットフォーム妥当性確認エンティティ（ＰＶＥ）の少なくとも一方に格納される方法。

【０２０１】

９．上記実施形態のいずれかに記載の方法において、ＰＶＥがそれに基づいてアクションを判定し得るモジュール識別子を少なくとも含む完全性チェック失敗メッセージを送ることをさらに含む方法。

【０２０２】

１０．上記実施形態のいずれかに記載の方法において、完全性検証失敗に対する重大度分類に基づいて所定のアクションを実施することをさらに含む方法。

【０２０３】

１１．上記実施形態のいずれかに記載の方法において、所定のアクションは、非常メッセージの送付、コードアップデートの開始、修復の開始、および失敗した機能性のリストの報告の少なくとも１つを含む方法。

【０２０４】

１２．上記実施形態のいずれかに記載の方法において、ソフトウェアモジュールおよび関連付けられた属性のリストは、コンポーネント特有の情報要素、モジュール特有の情報要素および機能要素の少なくとも１つを含む方法。

【０２０５】

１３．上記実施形態のいずれかに記載の方法において、コンポーネント特有の情報要素は、コンポーネント説明、コンポーネント識別（ＩＤ）および信頼できる参照値（ＴＲＶ）の少なくとも１つを含む方法。

【０２０６】

１４．上記実施形態のいずれかに記載の方法において、モジュール特有の情報要素は、モジュール説明、モジュール識別（ＩＤ）、機能説明、機能ＩＤ、コンポーネントＩＤ、リリースバージョンおよび重大度の少なくとも１つを含む方法。

【０２０７】

１５．上記実施形態のいずれかに記載の方法において、モジュールは、完全性検証中に少なくとも一度調べられる方法。

【０２０８】

１６．上記実施形態のいずれかに記載の方法において、モジュールは、ただ１つのコンポーネント中に現れる方法。

【０２０９】

１７．上記実施形態のいずれかに記載の方法において、モジュールは、２つの機能の間で共有される方法。

【０２１０】

１８．上記実施形態のいずれかに記載の方法において、各モジュールは、関連付けられた機能性をもつ方法。

【０２１１】

１９．上記実施形態のいずれかに記載の方法において、モジュールグループは、同じコンポーネントに関連付けられ、同じコンポーネント識別子（ＩＤ）を共有し、同じコンポーネントとの完全性をまとめて検証される方法。

【０２１２】

２０．上記実施形態のいずれかに記載の方法において、１つのコンポーネント識別子（ＩＤ）をもつモジュールは、異なる機能性識別子（ＩＤ）で分類される方法。

【０２１３】

２１．上記実施形態のいずれかに記載の方法において、モジュールは、機能性および完全性チェック単位に基づいて分類される方法。

【０２１４】

２２．上記実施形態のいずれかに記載の方法において、同じコンポーネント識別子のモジュールは、１つの信頼できる参照値（ＴＲＶ）をもち、信頼できる参照値が失敗するという条件で、失敗したコンポーネント識別子の全モジュールは、失敗した機能性のリストを判定するのに使われる方法。

【０２１５】

２３．Ｈ（ｅ）ＮＢ（ｈｏｍｅ　ｅｖｏｌｖｅｄ　Ｎｏｄｅ　Ｂ）の妥当性確認を実施する方法であって、デバイス完全性チェック失敗の結果、上記Ｈ（ｅ）ＮＢをフォールバックコードでスタートすることを含む方法。

【０２１６】

２４．上記実施形態２３の方法において、非常メッセージを送ることをさらに含む方法。

【０２１７】

２５．上記実施形態２３～２４のいずれかに記載の方法において、修復情報を取り出すダウンリンクメッセージを受信することをさらに含む方法。

【０２１８】

２６．上記実施形態２３～２５のいずれかに記載の方法において、ダウンリンクメッセージに応答して修復情報をダウンロードすることをさらに含む方法。

【０２１９】

２７．上記実施形態２３～２６のいずれかに記載の方法において、インストールされた修復情報に基づいてＨ（ｅ）ＮＢをリスタートすることをさらに含む方法。

【０２２０】

２８．上記実施形態２３～２７のいずれかに記載の方法において、失敗情報をアップロードして、修復情報の準備を許すことをさらに含む方法。

【０２２１】

２９．上記実施形態２３～２８のいずれかに記載の方法において、非常メッセージは、製造元識別、信頼できる環境識別、Ｈ（ｅ）ＮＢ識別、および失敗コードの少なくとも１つを含む方法。

【０２２２】

３０．上記実施形態２３～２９のいずれかに記載の方法において、重大度測度は、デバイス完全性チェック失敗の影響を指定する方法。

【０２２３】

３１．上記実施形態２３～３０のいずれかに記載の方法において、デバイス完全性チェックは、ローカルに実施される方法。

【０２２４】

３２．上記実施形態２３～３１のいずれかに記載の方法において、失敗情報は、Ｈ（ｅ）ＮＢ管理システム（Ｈ（ｅ）ＭＳ）またはプラットフォーム妥当性確認エンティティ（ＰＶＥ）の一方に送られる方法。

【０２２５】

３３．上記実施形態２３～３２のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、ＳＳＬ／ＴＬＳ（セキュアソケットレイヤ／トランスポートレイヤセキュリティ）を使って、非常メッセージを送る方法。

【０２２６】

３４．上記実施形態２３～３３のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、デフォルトのＨ（ｅ）ＭＳ　ＵＲＬ（ユニフォームリソースロケータ）で構成される方法。

【０２２７】
３５．上記実施形態２３～３４のいずれかに記載の方法において、デバイス構成データシートは、デバイスの安全なメモリ内部に維持され、認可された当事者によってアクセスされる方法。
【０２２８】
３６．上記実施形態２３～３５のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、デバイス構成データシートが満了すると、アップデートプロセスを開始して、修復サーバからデータをプルする方法。
【０２２９】
３７．上記実施形態２３～３６のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、予め指定されたコンポーネントのデバイス完全性チェックを実施する方法。
【０２３０】
３８．上記実施形態２３～３７のいずれかに記載の方法において、ＰＶＥからＨ（ｅ）ＮＢアクションを受信することをさらに含む方法。
【０２３１】
３９．Ｈ（ｅ）ＮＢ（ｈｏｍｅ　ｅｖｏｌｖｅｄ　Ｎｏｄｅ　Ｂ）の妥当性確認を実施する方法であって、ＩＫＥ（インターネット鍵交換）セキュリティアソシエーションを確立することを含む方法。
【０２３２】
４０．実施形態１の方法において、デバイス完全性チェック結果の相互認証および指示のための証明書を、ＩＫＥ＿ＡＵＴＨ要求に入れて送ることをさらに含む方法。
【０２３３】
４１．上記実施形態３９～４０のいずれかに記載の方法において、認証およびデバイス完全性の妥当性確認の結果の指示を受信することをさらに含む方法。
【０２３４】
４２．上記実施形態３９～４１のいずれかに記載の方法において、デバイス完全性チェック結果の評価に基づくアクションを受信することをさらに含む方法。
【０２３５】
４３．上記実施形態３９～４２のいずれかに記載の方法において、デバイス完全性チェック結果は、失敗した機能性のリストを含む方法。
【０２３６】
４４．上記実施形態３９～４３のいずれかに記載の方法において、受信されたアクションは、修復を呼び出す方法。
【０２３７】
４５．上記実施形態３９～４４のいずれかに記載の方法において、Ｈ（ｅ）ＮＢ内でのデバイス完全性チェック結果は、検疫され、完全アクセスを入手し、部分アクセスを入手し、または修復のための担当者介入を入手する方法。
【０２３８】
４６．上記実施形態３９～４５のいずれかに記載の方法において、修復を示すアクションに応答して非常メッセージを送ることをさらに含む方法。
【０２３９】
４７．上記実施形態３９～４６のいずれかに記載の方法において、修復情報を取り出すダウンリンクメッセージを受信することをさらに含む方法。
【０２４０】
４８．上記実施形態３９～４７のいずれかに記載の方法において、ダウンリンクメッセージに応答して修復情報をダウンロードすることをさらに含む方法。
【０２４１】
４９．上記実施形態３９～４８のいずれかに記載の方法において、インストールされた修復情報に基づいてＨ（ｅ）ＮＢをリスタートすることをさらに含む方法。
【０２４２】

５０．上記実施形態３９～４９のいずれかに記載の方法において、失敗情報をアップロードして、修復情報の準備を許す方法。

【０２４３】

５１．上記実施形態３９～５０のいずれかに記載の方法において、失敗情報は、失敗した機能性のリストを含む方法。

【０２４４】

５２．上記実施形態３９～５１のいずれかに記載の方法において、失敗情報は、Ｈ（ｅ）ＮＢ管理システム（Ｈ（ｅ）ＭＳ）またはプラットフォーム妥当性確認エンティティ（ＰＶＥ）の一方に送られる方法。

【０２４５】

５３．上記実施形態３９～５２のいずれかに記載の方法において、失敗情報は、チェックされた機能性のリストを含む方法。

【０２４６】

５４．上記実施形態３９～５３のいずれかに記載の方法において、失敗情報は、チェックされていない機能性のリストを含む方法。

【０２４７】

５５．上記実施形態３９～５４のいずれかに記載の方法において、妥当性確認および認証のバインドは、ＩＫＥセッションによって与えられる方法。

【０２４８】

５６．上記実施形態３９～５５のいずれかに記載の方法において、妥当性確認および認証のバインドは、デバイス完全性検査が成功するという条件で先行する認証プロシージャによって与えられる方法。

【０２４９】

５７．デバイス妥当性確認をバインドする方法であって、信頼できる環境（ＴｒＥ）を認証プロシージャにバインドすることを含む方法。

【０２５０】

５８．実施形態５７の方法において、認証プロシージャは、ＥＡＰ－ＡＫＡ（Ｅｘｔｅｎｓｉｂｌｅ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ Ｐｒｏｔｏｃｏｌ Ｍｅｔｈｏｄ ｆｏｒ ＵＭＴＳ Ａｕｔｈｅｎｔｉｃａｔｉｏｎ ａｎｄ Ｋｅｙ Ａｇｒｅｅｍｅｎｔ）プロシージャである方法。

【０２５１】

５９．実施形態５７～５８のいずれか１つに記載の方法において、プロシージャはＡＫＡ資格を妥当性確認する方法。

【０２５２】

６０．実施形態５７～５９のいずれか１つに記載の方法において、ＡＫＡ資格はＴｒＥに含まれる方法。

【０２５３】

６１．実施形態５７～６０のいずれか１つに記載の方法において、妥当性確認済みデバイスとＥＡＰ－ＡＫＡベース認証をバインドすることをさらに含む方法。

【０２５４】

６２．実施形態５７～６１のいずれか１つに記載の方法において、ＥＡＰ－ＡＫＡ認証は、ＡＫＡ資格を保持するＴｒＥを、ＥＡＰ－ＡＫＡベース認証のプロシージャにバインドすることを含む方法。

【０２５５】

６３．実施形態５７～６２のいずれか１つに記載の方法において、ＨｅＮＢ（enhanced home node B）へのＡＫＡ資格を保持するＴｒＥの論理バインドを実施することをさらに含む方法。

【０２５６】

６４．実施形態５７～６３のいずれか１つに記載の方法において、デバイスプラットフォームの完全性が妥当性確認される方法。

【０２５７】
６５．実施形態５７～６４のいずれか１つに記載の方法において、ＨｅＮＢへの、ＡＫＡ資格を保持するＴｒＥの物理的バインドを実施することをさらに含む方法。
【０２５８】
６６．実施形態５７～６５のいずれか１つに記載の方法において、ハードウェアおよびソフトウェアに対する実際の完全性の妥当性確認は、ＨｅＮＢに安全に組み込まれたハードウェアセキュリティコンポーネントによって実施される方法。
【０２５９】
６７．実施形態５７～６６のいずれか１つに記載の方法において、ＥＡＰ－ＡＫＡ認証に適した資格および物理的にバインドされたＴｒＥに格納された関連アプリケーションは、ホスティングデバイスへの取外し可能ハードウェアコンポーネントのバインドを妥当性確認するように構成される方法。
【０２６０】
６８．実施形態５７～６７のいずれか１つに記載の方法において、ＡＫＡ資格を保持するＴｒＥおよびＨｅＮＢはさらにバインドされる方法。
【０２６１】
６９．実施形態５７～６８のいずれか１つに記載の方法において、ＴｒＥのみがデータを復号することができるように、デバイス妥当性確認に使われるＡＫＡ資格を計算するのに必要とされるデータをＨｅＮＢが暗号化することをさらに含む方法。
【０２６２】
７０．実施形態５７～６９のいずれか１つに記載の方法において、ＨｅＮＢ暗号化データを復号するのに必要とされる鍵をＴｒＥが安全に格納することをさらに含む方法。
【０２６３】
７１．実施形態５７～７０のいずれか１つに記載の方法において、共通セキュリティプロトコルの同じセッション中のデバイス妥当性確認およびデバイス認証についての情報を組み合わせて、さらなるバインディングを取得することをさらに含む方法。
【０２６４】
７２．実施形態５７～７１のいずれか１つに記載の方法において、共通セキュリティプロトコルは、ＩＫＥｖ２（インターネット鍵交換バージョン２）である方法。
【０２６５】
７３．実施形態５７～７２のいずれか１つに記載の方法において、デバイス妥当性確認は、ＨｅＮＢとネットワークエンティティ間の対話およびメッセージ交換を含む方法。
【０２６６】
７４．実施形態５７～７３のいずれか１つに記載の方法において、ＨｅＮＢはＴｒＥを含む方法。
【０２６７】
７５．実施形態５７～７４のいずれか１つに記載の方法において、ＨｅＮＢの妥当性確認をネットワークエンティティが実施することをさらに含む方法。
【０２６８】
７６．実施形態５７～７５のいずれか１つに記載の方法において、ＨｅＮＢと妥当性確認を実施するネットワークエンティティとの間のシグナリングをセキュリティゲートウェイが伝えることをさらに含む方法。
【０２６９】
７７．実施形態５７～７６のいずれか１つに記載の方法において、デバイス妥当性確認を証明書ベースの認証にバインドすることをさらに含む方法。
【０２７０】
７８．実施形態５７～７７のいずれか１つに記載の方法において、バインドすることは、ＨｅＮＢのＴｒＥを証明書ベースのデバイス妥当性確認のプロシージャに物理的にバインドすることを含む方法。
【０２７１】

７９．実施形態５７～７８のいずれか１つに記載の方法において、バインドすることは、ＨｅＮＢのＴｒＥを証明書ベースのデバイス妥当性確認のプロシージャに論理的にバインドすることを含む方法。

【０２７２】

８０．実施形態５７～７９のいずれか１つに記載の方法において、証明書資格を保持するＴｒＥとＨｅＮＢはさらにバインドされる方法。

【０２７３】

８１．実施形態５７～８０のいずれか１つに記載の方法において、暗号鍵を使ってデバイス妥当性確認に使われる証明書資格を計算するのに必要とされるデータをＨｅＮＢが暗号化すること、およびＴｒＥが安全に保持する鍵を使ってＴｒＥの内側の暗号化データをＴｒＥが復号することをさらに含む方法。

【０２７４】

８２．実施形態５７～８１のいずれか１つに記載の方法において、共通プロトコルセッションの同じまたは連続するセッションを両方のプロシージャに使わせることによって、証明書ベースの認証セッションをＨｅＮＢ妥当性確認のためのプロシージャにバインドすることをさらに含む方法。

【０２７５】

８３．実施形態５７～８２のいずれか１つに記載の方法において、デバイス妥当性確認は、ＨｅＮＢと、ネットワークがＨｅＮＢのデバイス完全性の妥当性確認を実施することを可能にするネットワークエンティティとの間の、共通プロトコルセッションによる対話を含む方法。

【０２７６】

８４．実施形態５７～８３のいずれか１つに記載の方法において、バインドされるＨｅＮＢのデバイス妥当性確認をＥＡＰ－ＡＫＡベースのクライアント認証にバインドすることをさらに含む方法。

【０２７７】

８５．実施形態５７～８４のいずれか１つに記載の方法において、ＴｒＥとＨｅＮＢの残りとの間のメッセージ交換のための暗号鍵および資格を使ってＴｒＥをＨｅＮＢにバインドすることをさらに含む方法。

【０２７８】

８６．実施形態５７～８５のいずれか１つに記載の方法において、ＴｒＥとＨｅＮＢの残りとの間のメッセージ交換は、デバイス妥当性確認に関連したメッセージ交換を含む方法。

【０２７９】

８７．実施形態５７～８６のいずれか１つに記載の方法において、鍵および資格は、ＴｒＥの内側で保護される方法。

【０２８０】

８８．実施形態５７～８７のいずれか１つに記載の方法において、共通セキュリティプロトコルの同じまたは連続するセッション中に、デバイス妥当性確認およびＥＡＰ－ＡＫＡベースのクライアント認証の指定された一部をＨｅＮＢおよびＴｒＥが実施することをさらに含む方法。

【０２８１】

８９．実施形態５７～８８のいずれか１つに記載の方法において、ＨｅＮＢのデバイス妥当性確認を証明書ベースのクライアント認証にバインドすることをさらに含む方法。

【０２８２】

９０．実施形態５７～８９のいずれか１つに記載の方法において、ＴｒＥは、鍵ペアを含む方法。

【０２８３】

９１．実施形態５７～９０のいずれか１つに記載の方法において、鍵ペアは、私有部および公開部を含む方法。

【０２８４】
９２．実施形態５７～９１のいずれか１つに記載の方法において、私有部は、ＴｒＥの内側に安全に格納される方法。
【０２８５】
９３．実施形態５７～９２のいずれか１つに記載の方法において、公開部は、ＨｅＮＢに対して使用可能にされる方法。
【０２８６】
９４．実施形態５７～９３のいずれか１つに記載の方法において、ＨｅＮＢの製造元が、鍵ペアを生成すること、およびＨｅＮＢに対して公開鍵を利用可能にするのに必要とされる証明書を与えることをさらに含む方法。
【０２８７】
９５．実施形態５７～９４のいずれか１つに記載の方法において、ＥＡＰ－ＡＫＡベース認証における暗号手段によって、妥当性確認および認証のバインドを作成することをさらに含む方法。
【０２８８】
９６．実施形態５７～９５のいずれか１つに記載の方法において、ＨｅＮＢが、証明書からの公開鍵で応答を暗号化すること、および暗号化データをＴｒＥにフォワードすることをさらに含む方法。
【０２８９】
９７．実施形態５７～９６のいずれか１つに記載の方法において、応答はＩＫＥ＿ＡＵＴＨ応答である方法。
【０２９０】
９８．実施形態５７～９７のいずれか１つに記載の方法において、ＴｒＥが、次いで、データを復号すること、並びにＡＡＡ（認証、認可およびアカウンティング）サーバに対してＨｅＮＢを認証するのに必要とされるＥＡＰ－ＡＫＡ応答（ＲＥＳ）パラメータを計算することをさらに含む方法。
【０２９１】
９９．実施形態５７～９８のいずれか１つに記載の方法において、ＨｅＮＢが、公開鍵を使って、ＴｒＥにおけるＡＵＴＨパラメータを計算するのに必要とされるデータを暗号化することをさらに含む方法。
【０２９２】
１００．実施形態５７～９９のいずれか１つに記載の方法において、ＴｒＥが、データを復号すること、およびＳｅＧＷに対するＨｅＮＢを認証するのに必要なＡＵＴＨパラメータを計算することをさらに含む方法。
【０２９３】
１０１．実施形態５７～１００のいずれか１つに記載の方法において、デバイス完全性とデバイスＩＤを暗号によってバインドすることをさらに含む方法。
【０２９４】
１０２．実施形態５７～１０１のいずれか１つに記載の方法において、デバイス完全性とデバイスＩＤを暗号によってバインドすることは、ＴｒＥおよびＨｅＮＢによって実施される方法。
【０２９５】
１０３．実施形態５７～１０２のいずれか１つに記載の方法において、ＴｒＥおよびＨｅＮＢは、それぞれの公開鍵ペアを装備する方法。
【０２９６】
１０４．実施形態５７～１０３のいずれか１つに記載の方法において、ＴｒＥおよびＨｅＮＢは、それぞれの対称共有鍵を装備する方法。
【０２９７】
１０５．実施形態５７～１０４のいずれか１つに記載の方法において、ＴｒＥおよびＨｅＮＢは、鍵を、通信を保護するために、また、相互認証のために使う方法。

【０２９８】
１０６．実施形態５７～１０５のいずれか１つに記載の方法において、デバイス妥当性確認のためのＩＫＥｖ２プロトコルは、ＨｅＮＢへのＴｒＥのバインドに使われる方法。
【０２９９】
１０７．実施形態５７～１０６のいずれか１つに記載の方法において、デバイス完全性は、デバイス完全性の妥当性確認およびデバイス認証のプロシージャを結びつけることによって、デバイスＩＤにバインドされる方法。
【０３００】
１０８．実施形態５７～１０７のいずれか１つに記載の方法において、デバイス完全性の妥当性確認およびデバイス認証は、保護されたＴｒＥ内部で実施される方法。
【０３０１】
１０９．実施形態５７～１０８のいずれか１つに記載の方法において、ＴｒＥは、保護された、信頼できるエンティティである方法。
【０３０２】
１１０．実施形態５７～１０９のいずれか１つに記載の方法において、ＴｒＥは、デバイス完全性の妥当性確認およびデバイス認証のプロシージャを実行する方法。
【０３０３】
１１１．実施形態５７～１１０のいずれか１つに記載の方法において、ＩＫＥｖ２プロトコルのセッション、または直後のセッションは、デバイス完全性の妥当性確認およびデバイス認証両方に使われる方法。
【０３０４】
１１２．実施形態５７～１１１のいずれか１つに記載の方法において、デバイス妥当性確認プロシージャを新規メッセージ交換に組み合わせることをさらに含む方法。
【０３０５】
１１３．実施形態５７～１１２のいずれか１つに記載の方法において、新規要求および応答交換は、デバイス認証のために実施される別の同様の交換に先行する方法。
【０３０６】
１１４．実施形態５７～１１３のいずれか１つに記載の方法において、デバイス認証によって使われる要求および応答交換は、デバイス妥当性確認プロシージャに使われる方法。
【０３０７】
１１５．実施形態５７～１１４のいずれか１つに記載の方法において、デバイス完全性の妥当性確認に必要とされる追加データは、選ばれたメッセージフィールドに組み込まれる方法。
【０３０８】
１１６．実施形態５７～１１５のいずれか１つに記載の方法において、デバイス完全性に必要とされるデータは、ローカル自律完全性チェックまたは半自律的妥当性確認の出力結果についての署名されたステートメントを含む方法。
【０３０９】
１１７．実施形態５７～１１６のいずれか１つに記載の方法において、メッセージフィールドは、保護された通知フィールドを含む方法。
【０３１０】
１１８．実施形態５７～１１７のいずれか１つに記載の方法において、デバイス妥当性確認プロシージャを既存のメッセージ交換に組み合わせることをさらに含む方法。
【０３１１】
１１９．実施形態５７～１１８のいずれか１つに記載の方法において、デバイス妥当性確認プロシージャを新規要求および応答交換に組み合わせることをさらに含む方法。
【０３１２】
１２０．上記実施形態のいずれかに記載の方法において、完全性チェックを実施し、完全性チェックで生じた情報を用いて、ネットワーク決定に影響を与えることをさらに含む

方法。
【０３１３】
１２１．上記実施形態のいずれかに記載の方法において、情報要素は、製造元および完全性アルゴリズムを含む方法。
【０３１４】
１２２．上記実施形態のいずれかに記載の方法において、コンポーネント特有の情報要素は、コンポーネント説明、コンポーネント識別（ＩＤ）および信頼できる参照値（ＴＲＶ）を含む方法。
【０３１５】
１２３．上記実施形態のいずれかに記載の方法において、モジュール特有の情報要素は、モジュール説明、モジュール識別（ＩＤ）、機能説明、機能ＩＤ、コンポーネントＩＤ、リリースバージョンおよび重大度を含む方法。
【０３１６】
１２４．上記実施形態のいずれかに記載の方法において、重大度は、完全性チェックの失敗の影響を指定する方法。
【０３１７】
１２５．上記実施形態のいずれかに記載の方法において、重大度は、１から４のスケールで分類される方法。
【０３１８】
１２６．上記実施形態のいずれかに記載の方法において、重大度１は、Ｈ（ｅ）ＮＢ機能性に対する高い影響を表明し、停止動作を保証することができ、フォールバックコードイメージ（ＦＢＣ）は、指定されたＨ（ｅ）ＭＳに非常信号を送ることができる方法。
【０３１９】
１２７．上記実施形態のいずれかに記載の方法において、重大度２は、制限されたＨ（ｅ）ＮＢ機能性を表明する方法。
【０３２０】
１２８．上記実施形態のいずれかに記載の方法において、３の重大度は、コア機能性に影響を与えなくてよく、モジュール／機能の失敗は、ファームウェアアップデートプロシージャで置き換えられ、リブートにより妥当性確認される方法。
【０３２１】
１２９．上記実施形態のいずれかに記載の方法において、４の重大度は、コア機能性に影響を与えなくてよく、失敗したモジュールは、通常のファームウェアアップデートを介して置き換えることができる方法。
【０３２２】
１３０．上記実施形態のいずれかに記載の方法において、自律的妥当性確認中、デバイス完全性チェックはローカルに実施される方法。
【０３２３】
１３１．上記実施形態のいずれかに記載の方法において、完全性チェックが失敗するという条件で、非常信号が宅内移動局（Ｈ（ｅ）ＭＳ）に送られる方法。
【０３２４】
１３２．上記実施形態のいずれかに記載の方法において、半自律的妥当性確認中、完全性チェックに失敗した機能性のリストは、パーソナルビデオエンコーダ（ＰＶＥ）に報告される方法。
【０３２５】
１３３．上記実施形態のいずれかに記載の方法において、完全性チェック中、モジュールは一度だけ調べられる方法。
【０３２６】
１３４．上記実施形態のいずれかに記載の方法において、モジュールは、ただ１つのコンポーネントにおいて現れる方法。
【０３２７】

１３５．上記実施形態のいずれかに記載の方法において、モジュールは、２つの機能の間で共有され得る方法。

【０３２８】

１３６．上記実施形態のいずれかに記載の方法において、各モジュールは、関連付けられた機能性をもち、失敗した機能性のリストは、半自律的妥当性確認（ＳＡＶ）において導出され、パーソナルビデオエンコーダ（ＰＶＥ）に送られ得る方法。

【０３２９】

１３７．上記実施形態のいずれかに記載の方法において、機能性識別子（ＩＤ）は、モジュールの分類を与える方法。

【０３３０】

１３８．上記実施形態のいずれかに記載の方法において、モジュールは、生成されたイメージに基づいて分類される方法。

【０３３１】

１３９．上記実施形態のいずれかに記載の方法において、モジュールのグループは、同じコンポーネント識別子（ＩＤ）を含み、まとめて完全性をチェックされる方法。

【０３３２】

１４０．上記実施形態のいずれかに記載の方法において、１つのコンポーネント識別子（ＩＤ）をもつモジュールは、異なる機能性識別子（ＩＤ）で分類される方法。

【０３３３】

１４１．上記実施形態のいずれかに記載の方法において、モジュール識別子（ＩＤ）は、様々なソフトウェアモジュールを追跡するのに使われ、標準化されない方法。

【０３３４】

１４２．上記実施形態のいずれかに記載の方法において、モジュールは、機能性および完全性チェック単位に基づいて分類される方法。

【０３３５】

１４３．上記実施形態のいずれかに記載の方法において、同じコンポーネント識別子（ＩＤ）をもつ全モジュールは、１つの信頼できる参照値をもち、信頼できる参照値が失敗するという条件で、失敗したコンポーネントの全モジュールは、失敗した機能性のリストを判定するのに使われ、宅内移動局（Ｈ（ｅ）ＭＳ）またはパーソナルビデオエンコーダ（ＰＶＥ）に伝達される方法。

【０３３６】

１４４．上記実施形態のいずれかに記載の方法において、機能性のリストは、コンポーネントに関連付けられる方法。

【０３３７】

１４５．上記実施形態のいずれかに記載の方法において、コンポーネントは、ロードされる順序で編成される方法。

【０３３８】

１４６．上記実施形態のいずれかに記載の方法において、完全性チェックは、イメージオブジェクトファイルの一部に対して実施され、イメージオブジェクトファイルが完全性チェックを通らないという条件で、失敗したセグメント名が抽出される方法。

【０３３９】

１４７．上記実施形態のいずれかに記載の方法において、ＣＰＥ（顧客構内設備）は、信頼できる参照をＨ（ｅ）ＮＢにダウンロードするのに使われ、信頼できる参照は、ネットワークオペレータの署名鍵によってデジタル署名される方法。

【０３４０】

１４８．上記実施形態のいずれかに記載の方法において、信頼できる参照値を含む署名されたパケットを受信すると、Ｈ（ｅ）ＮＢは、署名を復号し、受信された信頼できる参照値の真正性および完全性を検証する方法。

【０３４１】

１４９．上記実施形態のいずれかに記載の方法において、信頼できる参照値は、デジタ

ル署名される前に、機密性のために暗号化される方法。
【０３４２】
１５０．上記実施形態のいずれかに記載の方法において、信頼できる参照値は、ソフトウェアモジュールバイナリイメージの一部に付加される方法。
【０３４３】
１５１．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢおよび宅内移動局Ｈ（ｅ）ＭＳは、ＳＳＬ／ＴＬＳ（セキュアソケットレイヤ／トランスポートレイヤセキュリティ）をサポートし、証明書ベースの認証を使う方法。
【０３４４】
１５２．上記実施形態のいずれかに記載の方法において、ＴＲ０６９ベースのアーキテクチャは、証明書ベースの認証をサポートする方法。
【０３４５】
１５３．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、ＭａｎａｇｅｍｅｎｔＳｅｒｖｅｒ．ＵＲＬパラメータ中のデフォルトの宅内移動局Ｈ（ｅ）ＭＳＵＲＬ（ユニフォームリソースロケータ）で構成される方法。
【０３４６】
１５４．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、ＬＡＮ（ローカルエリアネットワーク）側ＭａｎａｇｅｍｅｎｔＳｅｒｖｅｒ．ＵＲＬ構成をサポートする方法。
【０３４７】
１５５．上記実施形態のいずれかに記載の方法において、セキュリティゲートウェイ（ＳｅＧＷ）ＵＲＬ（ユニフォームリソースロケータ）はパラメータである方法。
【０３４８】
１５６．上記実施形態のいずれかに記載の方法において、自律的妥当性確認中に、デジタル署名またはメッセージは私有鍵を使って署名される方法。
【０３４９】
１５７．上記実施形態のいずれかに記載の方法において、自律的妥当性確認中に、情報はネットワークエンティティに送られない方法。
【０３５０】
１５８．上記実施形態のいずれかに記載の方法において、最低要件は、信頼できる参照完全性メトリックまたは信頼できる参照値の生成に使われるアルゴリズム向けに標準化される方法。
【０３５１】
１５９．上記実施形態のいずれかに記載の方法において、信頼できる参照値は、信頼できるサードパーティによって生成され、デジタル署名される方法。
【０３５２】
１６０．上記実施形態のいずれかに記載の方法において、ローカル完全性データ初期化が実施される方法。
【０３５３】
１６１．上記実施形態のいずれかに記載の方法において、構成データの初期プロビジョニングが実施される方法。
【０３５４】
１６２．上記実施形態のいずれかに記載の方法において、参照完全性メトリックは、信頼できる参照値になる方法。
【０３５５】
１６３．上記実施形態のいずれかに記載の方法において、デバイス構成データシートは、デバイスの安全なメモリ内部で維持され、認可された当事者によってアクセスされる方法。
【０３５６】
１６４．上記実施形態のいずれかに記載の方法において、デバイス構成データは、Ｈ（

ｅ）ＮＢによって暗号化され復号される方法。
【０３５７】
１６５．上記実施形態のいずれかに記載の方法において、安全なブートプロセス中、生成されたダイジェストは、デバイス構成データシート中で指定された値と比較される方法。
【０３５８】
１６６．上記実施形態のいずれかに記載の方法において、デバイス構成データシートが失効するという条件で、Ｈ（ｅ）ＮＢがファームウェアアップデートプロセスを開始して、修復サーバからデータをプルする方法。
【０３５９】
１６７．上記実施形態のいずれかに記載の方法において、宅内移動局（Ｈ（ｅ）ＭＳ）は、ＲＰＣ（リモートプロシージャコール）を開始し、ＭａｎａｇｅｍｅｎｔＳｅｒｖｅｒ．ＵＲＬをアップデートする方法。
【０３６０】
１６８．上記実施形態のいずれかに記載の方法において、ファイルを転送するために、ＦＴＰＳ（ファイル転送プロトコルセキュア）が実装される方法。
【０３６１】
１６９．上記実施形態のいずれかに記載の方法において、デバイス完全性チェックは、自律的妥当性確認において失敗し、ローカル非常フラグが設定され、フォールバックコード（ＦＢＣ）がデバイスに格納される方法。
【０３６２】
１７０．上記実施形態のいずれかに記載の方法において、非常信号は、デバイス完全性チェック失敗の詳細を含む方法。
【０３６３】
１７１．上記実施形態のいずれかに記載の方法において、ＦＴＰ（ファイル転送プロトコル）サーバは、宅内移動局（Ｈ（ｅ）ＭＳ）とマージされる方法。
【０３６４】
１７２．上記実施形態のいずれかに記載の方法において、半自律的妥当性確認（ＳＡＶ）中、Ｈ（ｅ）ＮＢは、安全でないリンクを介して、安全なゲートウェイ（ＳｅＧＷ）と対話する方法。
【０３６５】
１７３．上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（ＳｅＧＷ）は、認証されたＨ（ｅ）ＮＢのみがネットワークにアクセスすることを許可する方法。
【０３６６】
上記実施形態のいずれかに記載の方法において、宅内移動局（Ｈ（ｅ）ＭＳ）は、Ｈ（ｅ）ＮＢ管理サーバとして作用し、修復のサポートを提供する方法。
【０３６７】
１７４．上記実施形態のいずれかに記載の方法において、ＳＡＶにおいて、Ｈ（ｅ）ＮＢは、予め指定されたコンポーネントの完全性の検査を実施する方法。
【０３６８】
１７５．上記実施形態のいずれかに記載の方法において、ＳＡＶにおいて、コンポーネントの認証は、完全性アルゴリズムからのダイジェスト出力を、デバイス構成シート中の指定された値と比較することによってローカルに実施される方法。
【０３６９】
１７６．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢのトランスポート要素（ＴｒＥ）は、予め定義されたコンポーネントの完全性の検査を実施する方法。
【０３７０】
１７７．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、証明書交換による安全なゲートウェイ（ＳｅＧＷ）で、ＩＫＥ（インターネット鍵交換）セキュリテ

ィアソシエーションを確立する方法。
【０３７１】
１７８．上記実施形態のいずれかに記載の方法において、コンポーネントのローカル完全性の妥当性確認の後、コンポーネントがデバイスによってロードされ実行される方法。
【０３７２】
１７９．上記実施形態のいずれかに記載の方法において、インターネット鍵交換（ＩＫＥ）要素が送られて、暗号アルゴリズム用のセキュリティパラメータ索引を含むセキュリティアソシエーションを確立する方法。
【０３７３】
１８０．上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（ＳｅＧＷ）は、ＩＫＥ（インターネット鍵交換）に対する応答を送る方法。
【０３７４】
１８１．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、証明書を、相互認証のためのＩＫＥ＿ＡＵＴＨ＿ＲＥＱに入れて送る方法。
【０３７５】
１８２．上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（ＳｅＧＷ）は、Ｈ（ｅ）ＮＢの認証資格を評価し、機能性識別子のリストを抽出する方法。
【０３７６】
１８３．上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（ＳｅＧＷ）は、認証妥当性確認が成功した場合はＨ（ｅ）ＮＢに指示を送る方法。
【０３７７】
１８４．上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（ＳｅＧＷ）は、認証妥当性確認が失敗した場合はＨ（ｅ）ＮＢに指示を送る方法。
【０３７８】
１８５．上記実施形態のいずれかに記載の方法において、ＳｅＧＷは、失敗した機能性のリストをパーソナルビデオエンコーダ（ＰＶＥ）に送る方法。
【０３７９】
１８６．上記実施形態のいずれかに記載の方法において、ＰＶＥは、デバイスの検疫、完全アクセスの提供、部分アクセスの提供または修復のための宅内移動局（Ｈ（ｅ）ＭＳ）介入の要求を含むアクションを判定する方法。
【０３８０】
１８７．上記実施形態のいずれかに記載の方法において、ＰＶＥは、決定をＳｅＧＷに通知する方法。
【０３８１】
１８８．上記実施形態のいずれかに記載の方法において、パーソナルビデオエンコーダ（ＰＶＥ）は、修復をスタートするための通知および失敗したモジュールのリストを宅内移動局（Ｈ（ｅ）ＭＳ）に送る方法。
【０３８２】
１８９．上記実施形態のいずれかに記載の方法において、パーソナルビデオエンコーダ（ＰＶＥ）は、修復に関する通知をＨ（ｅ）ＮＢに送る方法。
【０３８３】
１９０．上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（ＳｅＧＷ）は、デバイス完全性評価の結果をＨ（ｅ）ＮＢに示す方法。
【０３８４】
１９１．上記実施形態のいずれかに記載の方法において、トランスポート要素（ＴｒＥ）は、完全性検証を外部エンティティに委任する方法。
【０３８５】
１９２．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、ＮＴＰ（ネットワークタイムプロトコル）を使って時間を同期させるローカルタイムサーバを含む方法。

【０３８６】
１９３．上記実施形態のいずれかに記載の方法において、ＳＡＶにおける認証証明書およびローカル妥当性確認の結果は、ＩＫＥ＿ＡＵＴＨ＿ＲＥＱメッセージに入れて送られる方法。
【０３８７】
１９４．上記実施形態のいずれかに記載の方法において、安全なゲートウェイ（ＳｅＧＷ）は、失敗したモジュールの一覧を、リストをパーソナルビデオエンコーダ（ＰＶＥ）に渡す前にフィルタリングする方法。
【０３８８】
１９５．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、安全なゲートウェイを経由して、またはインターネットを介して接続することによって、宅内移動局（Ｈ（ｅ）ＭＳ）と対話して、修復をサポートする方法。
【０３８９】
１９６．上記実施形態のいずれかに記載の方法において、宅内移動局（Ｈ（ｅ）ＭＳ）は、ＲＰＣ（リモートプロシージャコール）を呼び出して、Ｈ（ｅ）ＮＢが失敗した機能性のリストおよびエラーコードのリストをアップロードすることを示す方法。
【０３９０】
１９７．上記実施形態のいずれかに記載の方法において、宅内移動局（Ｈ（ｅ）ＭＳ）は、失敗した機能性のリストのアップロードを準備するよう、ＦｉｌｅＳｅｖｅｒに対して指示する方法。
【０３９１】
１９８．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、失敗した機能性のリストを含むファイルをアップロードするためのプロシージャを呼び出す方法。
【０３９２】
１９９．上記実施形態のいずれかに記載の方法において、ＦｉｌｅＳｅｖｅｒは、アップロードされたファイルの評価の後、宅内移動局（Ｈ（ｅ）ＭＳ）にＤｏｗｎｌｏａｄ＿Ｐａｃｋａｇｅ＿Ｒｅａｄｙメッセージを送る方法。
【０３９３】
２００．上記実施形態のいずれかに記載の方法において、宅内移動局（Ｈ（ｅ）ＭＳ）は、ＲＰＣ（リモートプロシージャコール）を呼び出し、デバイス構成シートのＵＲＬ（ユニフォームリソースロケータ）を与える方法。
【０３９４】
２０１．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、ＦＴＰ（ファイル転送プロトコル）ファイルサーバに接続し、ファームウェアイメージおよびデバイス構成シートをダウンロードする方法。
【０３９５】
２０２．上記実施形態のいずれかに記載の方法において、宅内移動局（Ｈ（ｅ）ＭＳ）は、成功したダウンロード応答を受信すると、リブートプロシージャを呼び出す方法。
【０３９６】
２０３．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、成功したダウンロード応答を受信すると、ローカル非常フラグをリセットする方法。
【０３９７】
２０４．上記実施形態のいずれかに記載の方法において、宅内移動局（Ｈ（ｅ）ＭＳ）は、デバイスのブートが成功したことを示すメッセージを安全なゲートウェイ（ＳｅＧＷ）から受信する方法。
【０３９８】
２０５．上記実施形態のいずれかに記載の方法において、安全なブートプロセス中に完全性チェックがロードされ実行され、認証の実施が成功するという条件で、Ｈ（ｅ）ＮＢがセキュリティゲートウェイと通信する方法。
【０３９９】

２０６．上記実施形態のいずれかに記載の方法において、ローカル完全性チェックの結果を伝送することをさらに含む方法。

【０４００】

２０７．上記実施形態のいずれかに記載の方法において、ローカル完全性チェックの結果をパーソナルビデオエンコーダ（ＰＶＥ）にフォワードすることをさらに含む方法。

【０４０１】

２０８．上記実施形態のいずれかに記載の方法において、Ｈ（ｅ）ＮＢは、失敗した機能性のリストおよび製造元固有エラーコードのリストを、ＩＫＥｖ２　ＮＯＴＩＦＹメッセージに入れてＳｅＧＷに送る方法。

【０４０２】

２０９．上記実施形態のいずれかに記載の方法において、ＳｅＧＷは、失敗した機能性のリストをパーソナルビデオエンコーダ（ＰＶＥ）にフォワードする方法。

【０４０３】

２１０．上記実施形態のいずれかに記載の方法において、ＰＶＥは、ＳｅＧＷアクション、Ｈ（ｅ）ＮＢアクションを決定し、アクションのリストをＳｅＧＷにフォワードする方法。

【０４０４】

適切なプロセッサは、例として、汎用プロセッサ、特殊目的プロセッサ、従来のプロセッサ、ＤＳＰ（デジタル信号プロセッサ）、複数のマイクロプロセッサ、ＤＳＰコアと関連した１つもしくは複数のマイクロプロセッサ、コントローラ、マイクロコントローラ、ＡＳＩＣ（特定用途向け集積回路）、ＡＳＳＰ（特定用途向け標準製品）、ＦＰＧＡ（フィールドプログラム可能ゲートアレイ）回路、他の任意のタイプのＩＣ（集積回路）、および／または状態マシンを含む。

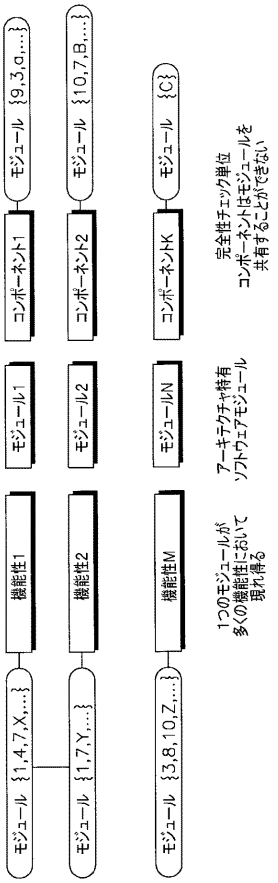
【０４０５】

ソフトウェアと関連したプロセッサは、ＷＴＲＵ（ワイヤレス送受信ユニット）、ＵＥ（ユーザ機器）、端末、基地局、ＭＭＥ（移動管理エンティティ）もしくはＥＰＣ（進化型パケットコア）、または任意のホストコンピュータ内で使用するための無線周波数トランシーバを実装するのに使うことができる。ＷＴＲＵは、ＳＤＲ（ソフトウェア無線）を含むハードウェアおよび／またはソフトウェア中に実装されるモジュール、並びにカメラ、ビデオカメラモジュール、テレビ電話、スピーカフォン、振動デバイス、スピーカ、マイクロホン、テレビトランシーバ、ハンズフリーヘッドセット、キーボード、ブルートゥース（登録商標）モジュール、ＦＭ（周波数変調）無線ユニット、ＮＦＣ（近距離無線通信）モジュール、ＬＣＤ（液晶ディスプレイ）表示ユニット、ＯＬＥＤ（有機発光ダイオード）表示ユニット、デジタルミュージックプレーヤ、メディアプレーヤ、ビデオゲームプレーヤモジュール、インターネットブラウザ、および／または任意のＷＬＡＮ（ワイヤレスローカルエリアネットワーク）もしくはＵＷＢ（超広帯域）モジュールなど、他のコンポーネントとともに使うことができる。

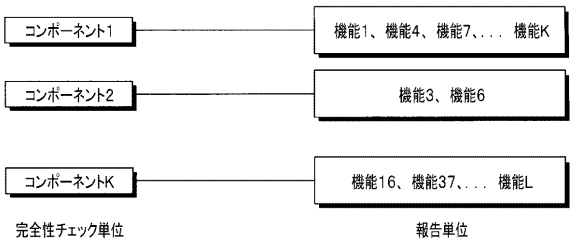
【０４０６】

特徴および要素を、具体的に組み合わせて上で記載したが、各特徴または要素は、他の特徴および要素なしで個別に、または他の特徴および要素ありでもなしでも、様々に組み合わせて用いることができる。本明細書に挙げた方法またはフローチャートは、汎用コンピュータまたはプロセッサによる実行用のコンピュータ可読記憶媒体に組み込まれる、コンピュータプログラム、ソフトウェア、またはファームウェア中に実装することができる。コンピュータ可読記憶媒体の例は、ＲＯＭ（読出し専用メモリ）、ＲＡＭ（ランダムアクセスメモリ）、レジスタ、キャッシュメモリ、半導体メモリ素子、内部ハードディスクおよび取外し可能ディスクなどの磁気メディア、光磁気メディア、並びにＣＤ－ＲＯＭディスク、およびＤＶＤ（デジタル多用途ディスク）などの光メディアを含む。

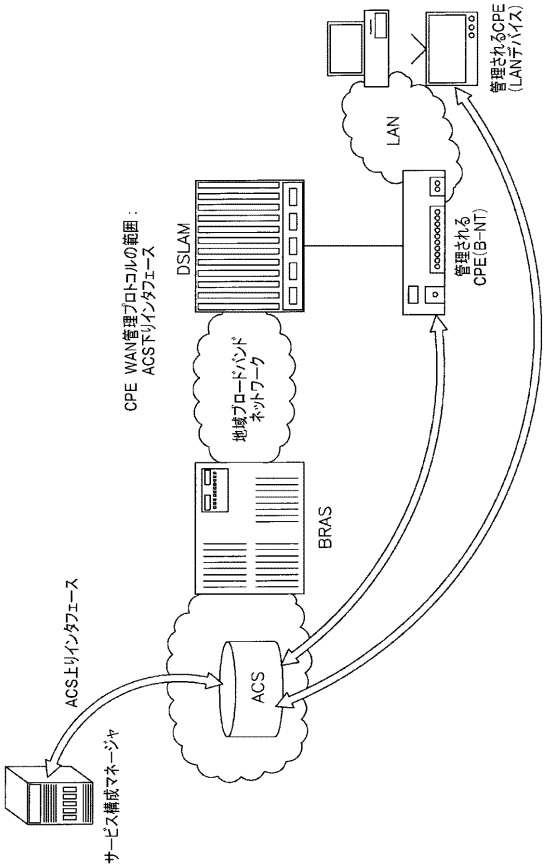
【図１】


モジュール {1,4,7,X,...}
モジュール {1,7,Y,...}
モジュール {3,8,10,Z,...}
機能性1
機能性2
機能性M
1つのモジュールが多くの機能性において現れ得る
モジュール1
モジュール2
モジュールN
アーキテクチャ特有ソフトウェアモジュール
コンポーネント1
コンポーネント2
コンポーネントK
モジュール {9,3,α,...}
モジュール {10,7,B,...}
モジュール {C}
完全性チェック単位
コンポーネントはモジュールを共有することができない

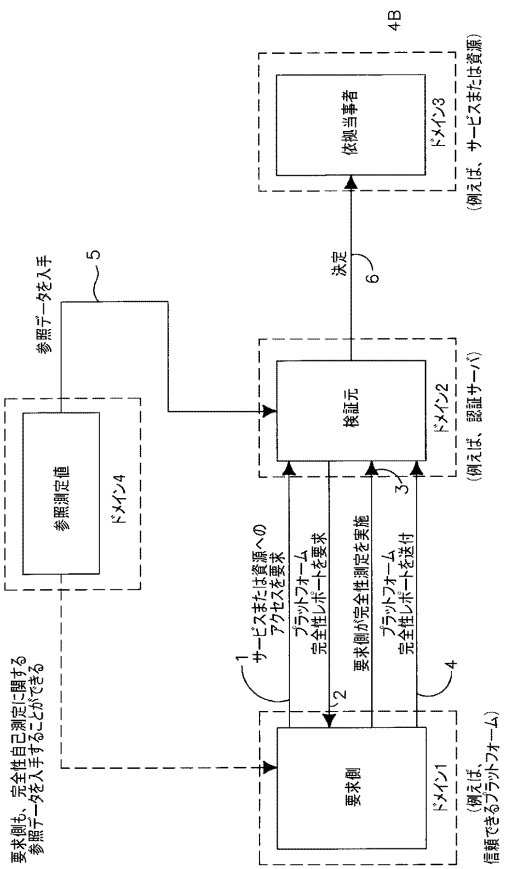
【図２】


コンポーネント1
コンポーネント2
コンポーネントK
機能1、機能4、機能7、. . . 機能K
機能3、機能6
機能16、機能37、. . . 機能L
完全性チェック単位
報告単位

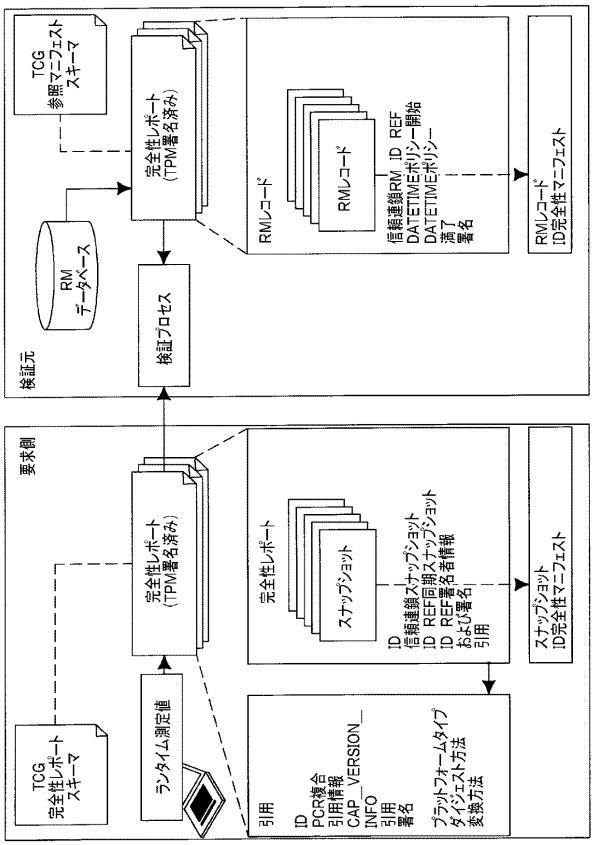
【図３】


ACSとのインタフェース
サービス構成マネージャ
ACS
BRAS
CPE WAN管理プロトコルの範囲：
ACSとのインタフェース
DSLAM
地域ブロードバンドネットワーク
LAN
管理されるCPE(B-NT)
管理されるCPE(LANデバイス)

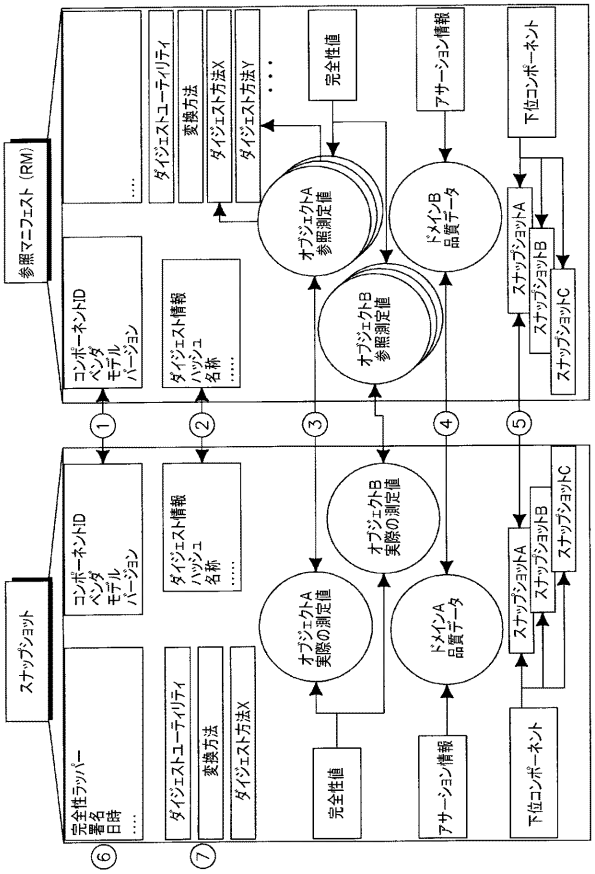
【図４】


4B
依拠当事者
ドメイン3
(例えば、サービスまたは資源)
決定
6
参照データを入手
5
検証元
ドメイン2
(例えば、認証サーバ)
参照測定値
ドメイン4
サービスまたは資源へのアクセスを要求
プラットフォーム完全性レポートを要求
要求側が完全性測定を実施
プラットフォーム完全性レポートを送付
1
2
3
4
要求側
ドメイン1
(例えば、信頼できるプラットフォーム)
要求側は、完全性自己測定に関する参照データを入手することができる

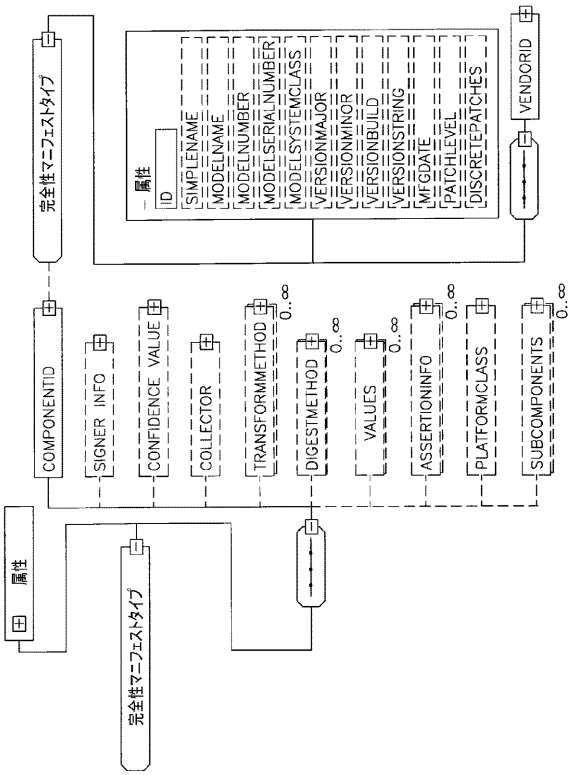
【図５】


検証元
TCG
参照マニフェスト
スキーマ
完全性レポート
(TPM署名済み)
RM
データベース
検証プロセス
RMレコード
RMレコード
信頼連鎖RM_ID REF
DATETIMEポリシー開始
DATETIMEポリシー
満了
署名
RMレコード
ID完全性マニフェスト
要求側
TCG
完全性レポート
スキーマ
ランタイム測定値
完全性レポート
(TPM署名済み)
完全性レポート
スナップショット
ID
信頼連鎖スナップショット
ID REF同期スナップショット
ID REF署名者情報
および署名
引用
スナップショット
ID完全性マニフェスト
引用
ID
PCR複合
引用情報
CAP_VERSION_
INFO
引用
署名
プラットフォームタイプ
ダイジェスト方法
変換方法

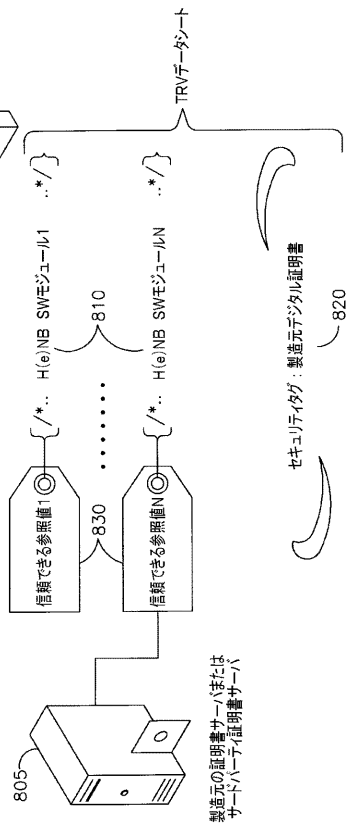
【図６】


参照マニフェスト（RM）
コンポーネントID
ベンダ
モデル
バージョン
ダイジェスト情報
ハッシュ
名称
ダイジェストユーティリティ
変換方法
ダイジェスト方法X
ダイジェスト方法Y
オブジェクトA
参照測定値
オブジェクトB
参照測定値
完全性値
ドメインB
品質データ
アサーション情報
下位コンポーネント
スナップショットA
スナップショットB
スナップショットC
スナップショット
完全性ラッパー
署名
日時
コンポーネントID
ベンダ
モデル
バージョン
ダイジェスト情報
ハッシュ
名称
ダイジェストユーティリティ
変換方法
ダイジェスト方法X
オブジェクトA
実際の測定値
オブジェクトB
実際の測定値
完全性値
ドメインA
品質データ
アサーション情報
下位コンポーネント
スナップショットA
スナップショットB
スナップショットC
①
②
③
④
⑤
⑥
⑦

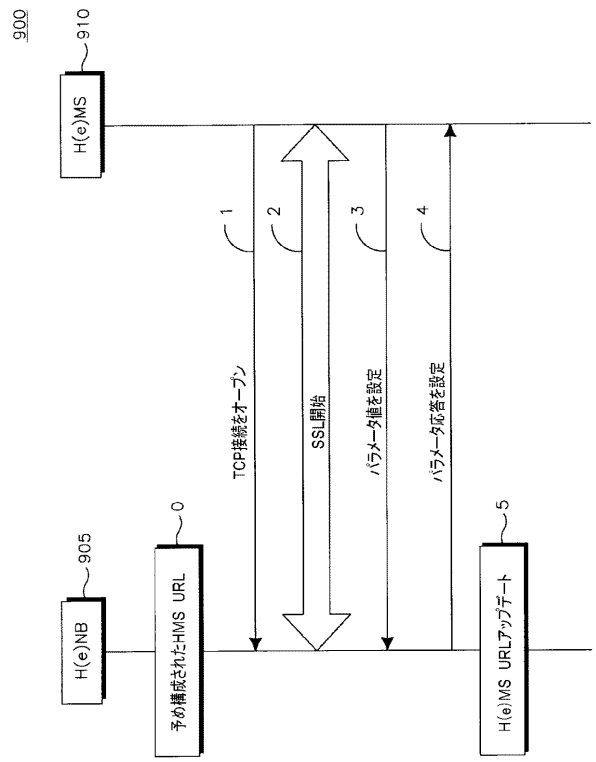
【図７】


完全性マニフェストタイプ
属性
ID
SIMPLENAME
MODELNAME
MODELNUMBER
MODELSERIALNUMBER
MODELSYSTEMCLASS
VERSIONMAJOR
VERSIONMINOR
VERSIONBUILD
VERSIONSTRING
MFGDATE
PATCHLEVEL
DISCRETEPATCHES
VENDORID
属性
完全性マニフェストタイプ
COMPONENTID
SIGNER INFO
CONFIDENCE VALUE
COLLECTOR
TRANSFORMMETHOD
DIGESTMETHOD
VALUES
ASSERTIONINFO
PLATFORMCLASS
SUBCOMPONENTS
0..8
0..∞
0..8
0..8
0..∞

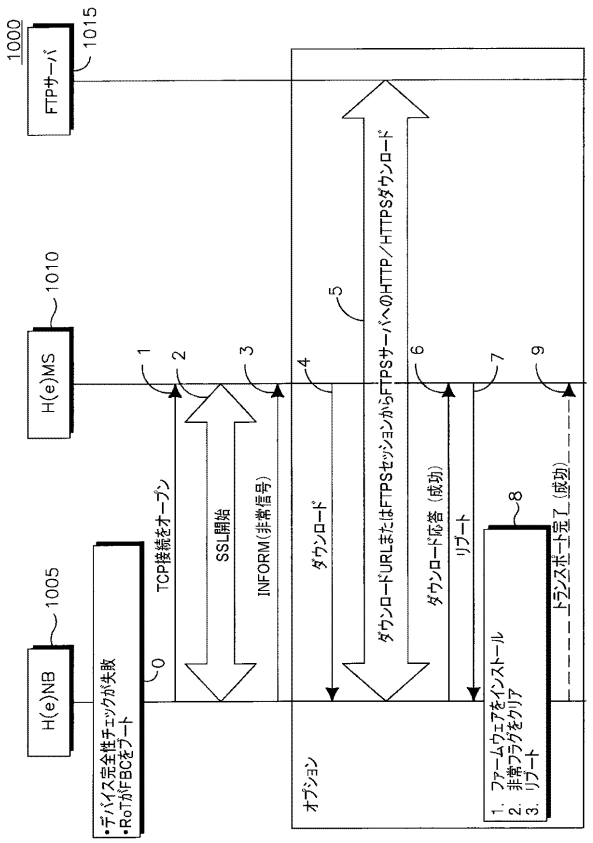
【図８】


TRVデータシート
/*.. H(e)NB SWモジュール1 ..*/
/*.. H(e)NB SWモジュールN ..*/
810
信頼できる参照値1
信頼できる参照値N
830
セキュリティタグ：製造元デジタル証明書
820
805
製造元の証明書サーバまたは
サードパーティ証明書サーバ

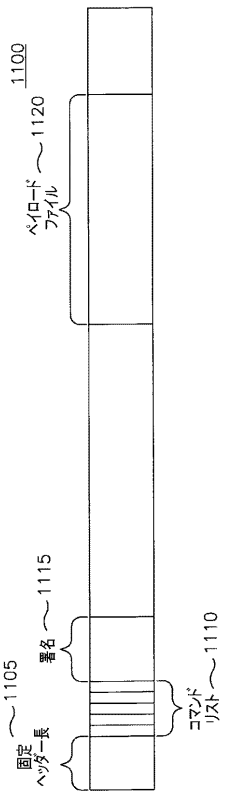
【図９】



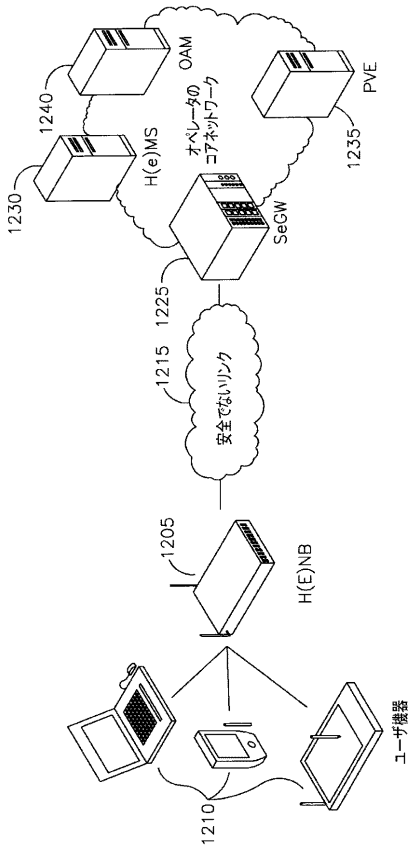
【図１０】



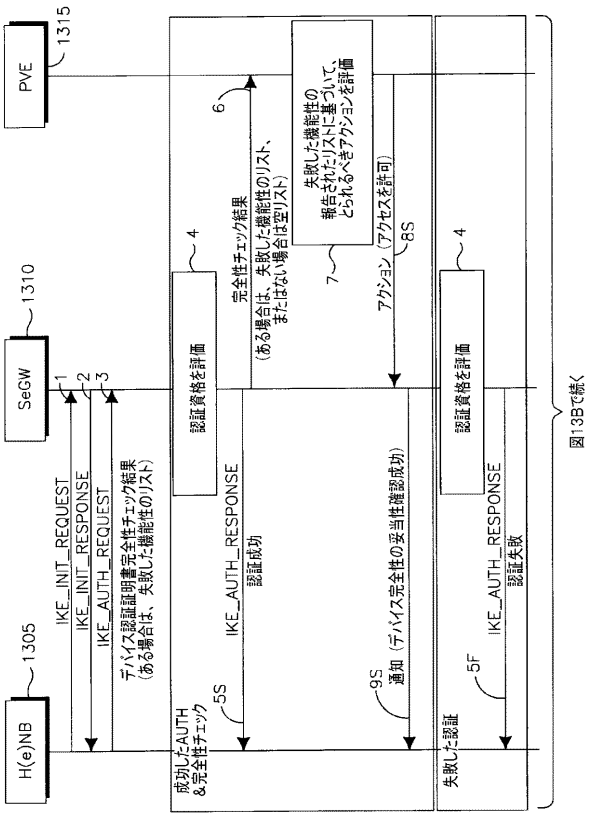
【図１１】



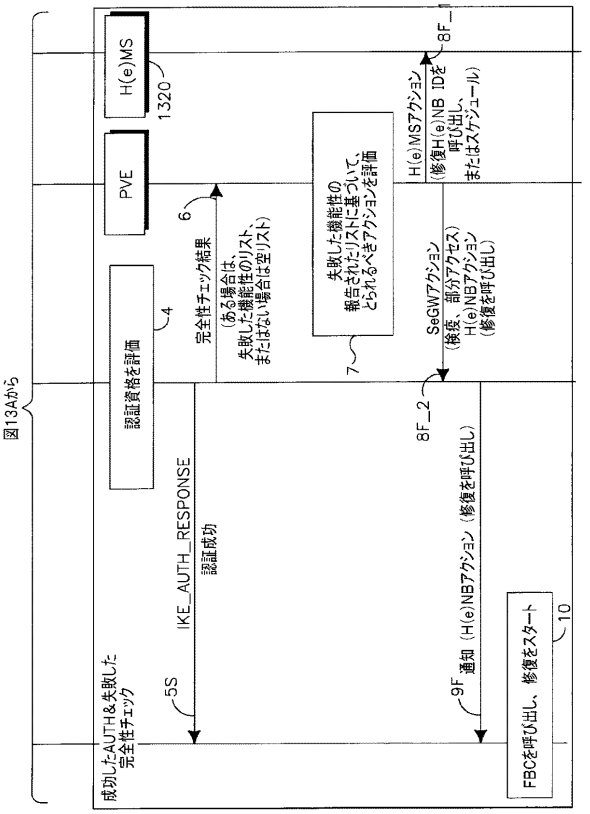
【図１２】



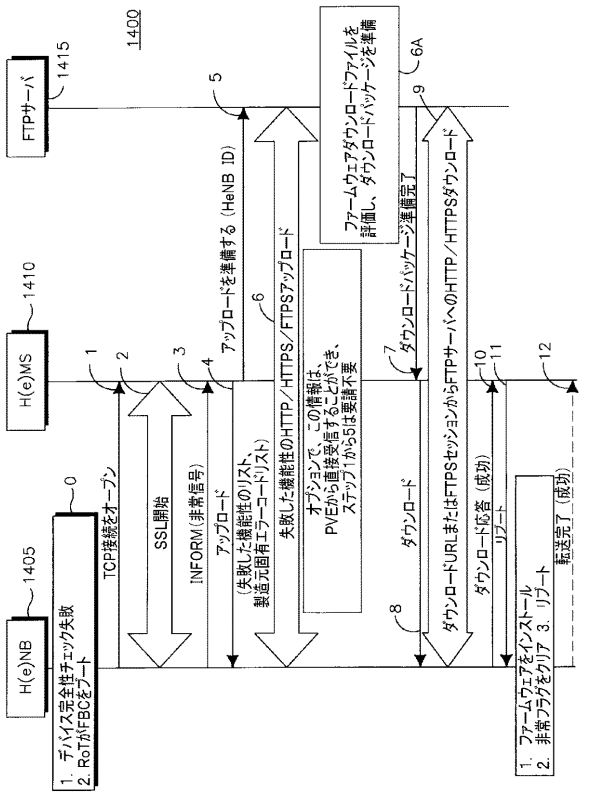
【図１３Ａ】



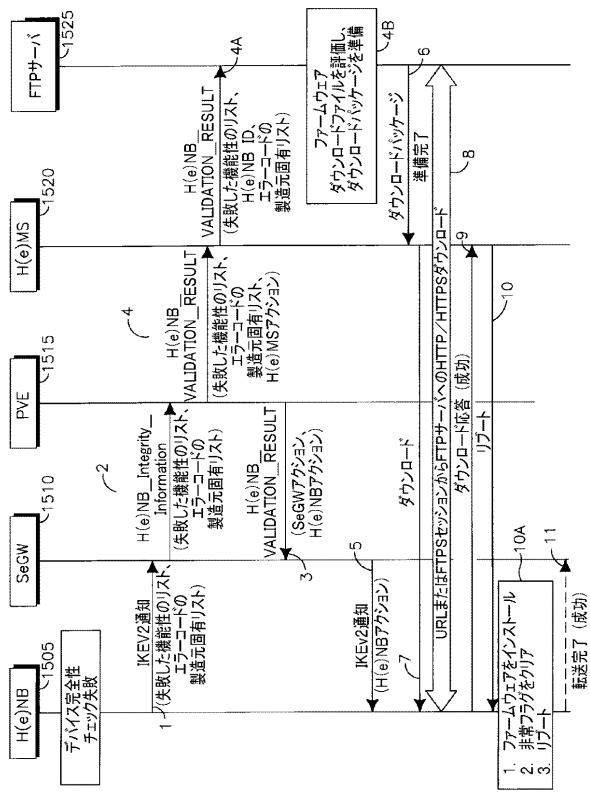
【図１３Ｂ】



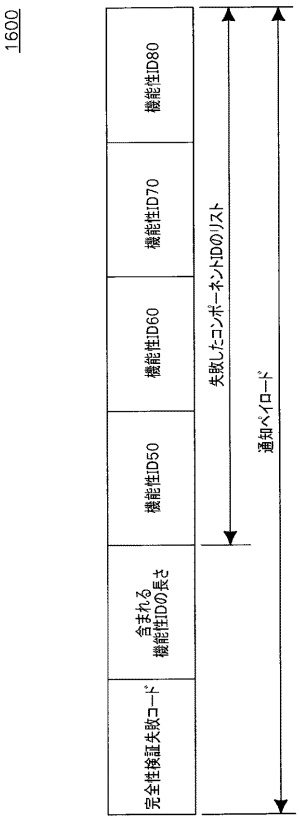
【図１４】



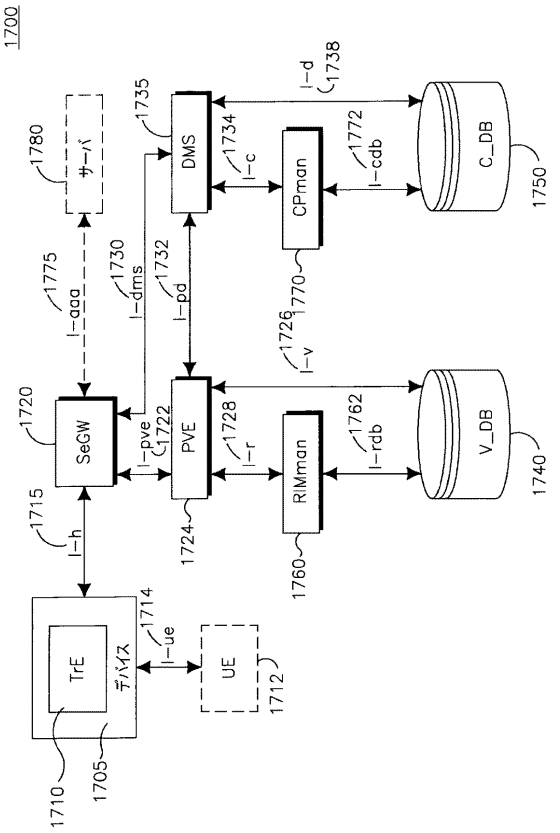
【図１５】



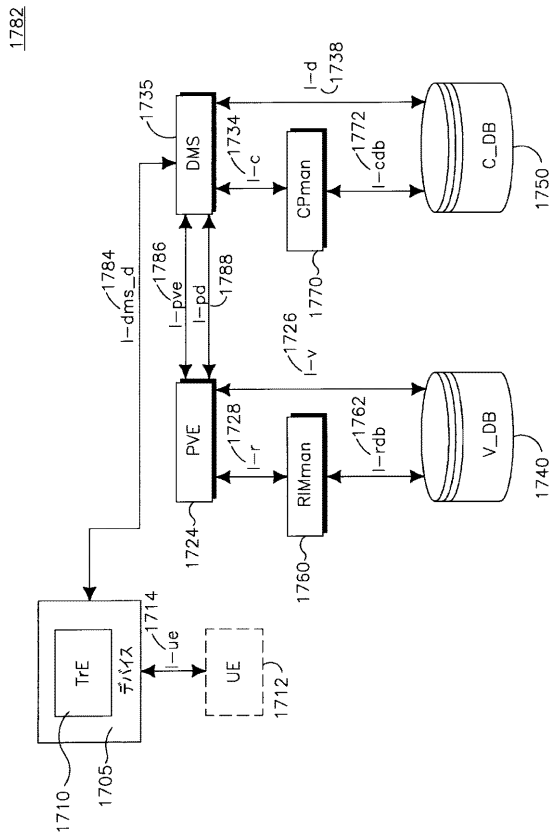
【図１６】



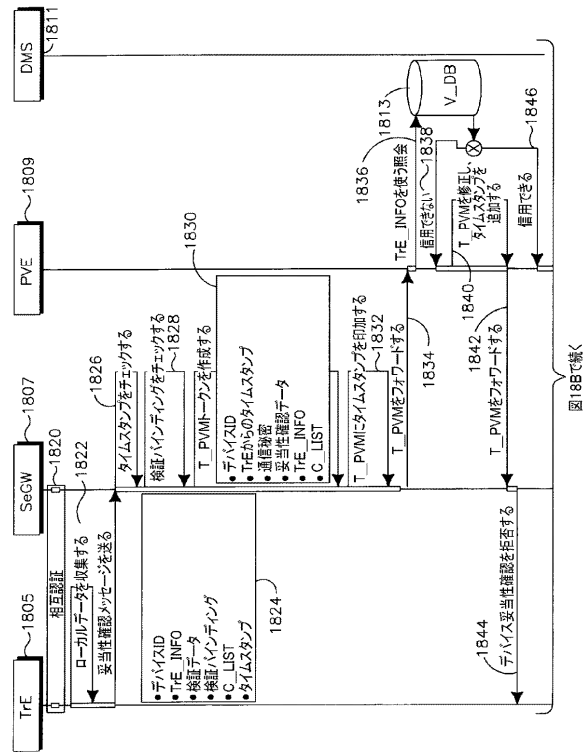
【図１７Ａ】



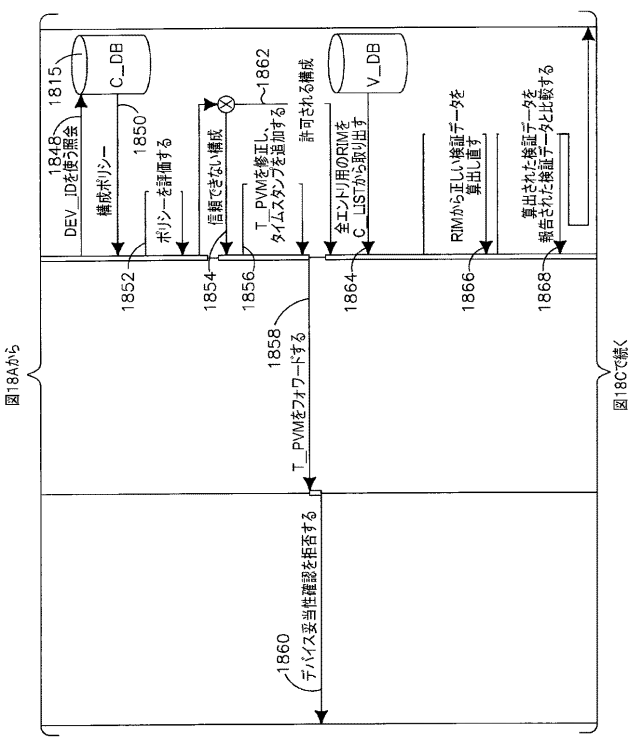
【図１７Ｂ】



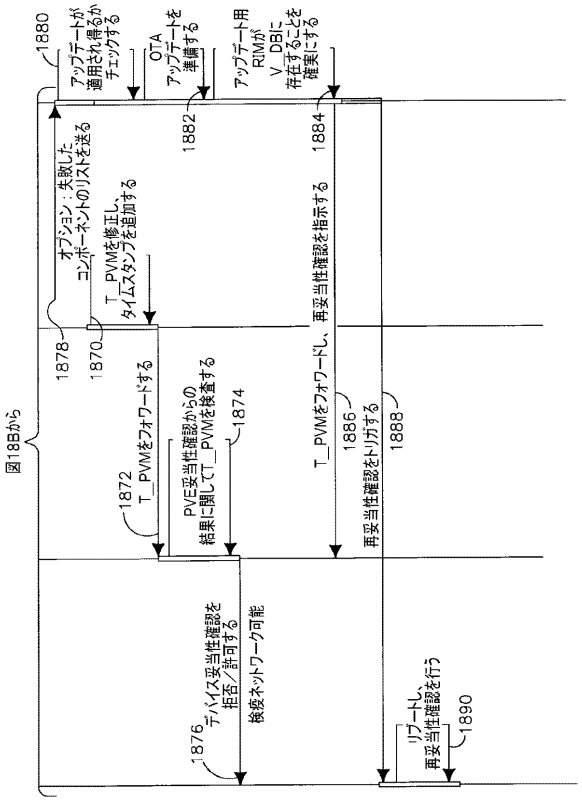
【図１８Ａ】



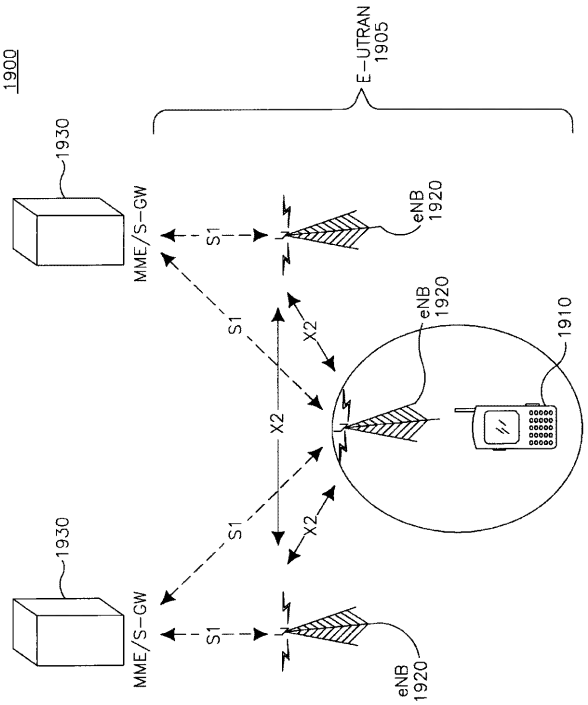
【図１８Ｂ】



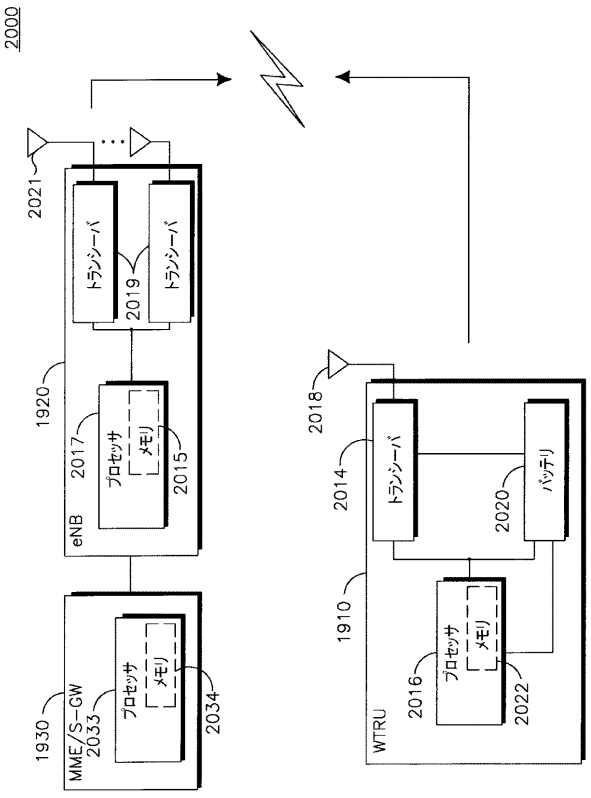
【図１８Ｃ】



【図１９】



【図２０】



【手続補正書】
【提出日】平成26年2月5日(2014.2.5)
【手続補正１】
【補正対象書類名】特許請求の範囲
【補正対象項目名】全文
【補正方法】変更
【補正の内容】
【特許請求の範囲】
【請求項１】
無線送信／受信装置（ＷＴＲＵ）の完全性検証を実行する方法であって、
前記ＷＴＲＵにおいて実行される以下のステップ、
前記ＷＴＲＵにおいて、前記ＷＴＲＵのコンポーネントについての完全性メトリックを測定するステップと、
前記ＷＴＲＵにおいて、前記ＷＴＲＵ上の安全なローカルストレージからＴＲＶ（trusted reference value）を検索するステップであって、前記ＴＲＶは本来、前記安全なローカルストレージに格納されている、ステップと、
前記ＷＴＲＵにおいて、前記測定された完全性メトリックを前記ＴＲＶと比較して、前記コンポーネントの完全性検証チェックの結果を判定するステップと、
前記コンポーネントの前記完全性検証チェックの前記結果をプラットフォーム妥当性確認エンティティ（ＰＶＥ）に報告するステップであって、前記ＰＶＥおよび前記ＷＴＲＵは、ネットワーク上の別個のエンティティである、ステップと、
前記ＰＶＥから妥当性確認判定の結果を受信するステップであって、前記妥当性確認の結果は、前記完全性検証チェックの前記結果に基づいて前記ＰＶＥによって前記ＷＴＲＵに与えられるアクセスのレベルを識別する、ステップと
を備えることを特徴とする方法。
【請求項２】
ソフトウェア機能性、並びに参照完全性メトリックおよび重大度の少なくとも一つを含む関連する属性のリストを前記プラットフォーム妥当性確認エンティティ（ＰＶＥ）に送信するステップをさらに備えることを特徴とする請求項１に記載の方法。
【請求項３】
デバイス構成データシートは、ソフトウェア機能性および関連する属性の前記リストを含むことを特徴とする請求項２に記載の方法。
【請求項４】
前記関連する属性は、コンポーネントおよびモジュールに関する前記ソフトウェア機能性のマッピングを備えることを特徴とする請求項３に記載の方法。
【請求項５】
前記デバイス構成データシート並びにソフトウェア機能性および関連する属性の前記リストの少なくとも一つは、前記ＷＴＲＵに格納されることを特徴とする請求項３に記載の方法。
【請求項６】
前記ＰＶＥがアクションを判定するのに使うために、機能性識別子および前記機能性識別子の一つの機能性識別子に関連付けられた各機能性についての前記完全性検証チェックの前記結果を含む完全性チェック結果メッセージを前記ＰＶＥに送信するステップをさらに備えることを特徴とする請求項２に記載の方法。
【請求項７】
前記完全性検証チェックの失敗に対する重大度分類に基づいて所定のアクションを実行するステップであって、前記所定のアクションは、非常メッセージを送信すること、コードアップデートを開始すること、修正を開始すること、および失敗した機能性のリストを報告することの少なくとも１つを含む、ステップをさらに備えることを特徴とする請求項１に記載の方法。

【請求項８】
前記妥当性確認判定は、起こされるアクションの判定を含み、前記起こされるアクションの判定は、前記ＷＴＲＵを隔離すること、前記ＷＴＲＵに完全なネットワークアクセスを提供すること、前記ＷＴＲＵに部分的なネットワークアクセスを提供すること、または前記ＷＴＲＵが修正を実行することを要求することの少なくとも一つを含む、ことを特徴とする請求項１に記載の方法。
【請求項９】
ソフトウェア機能性および関連する属性の前記リストは、コンポーネント特有の情報要素、モジュール特有の情報要素、または機能要素の少なくとも１つを含むことを特徴とする請求項２に記載の方法。
【請求項１０】
前記コンポーネント特有の情報要素は、コンポーネント説明、コンポーネント識別子（ＩＤ）またはＴＲＶ（trusted reference value）の少なくとも１つを含むことを特徴とする請求項９に記載の方法。
【請求項１１】
前記モジュール特有の情報要素は、モジュール説明、モジュール識別子（ＩＤ）、機能説明、機能ＩＤ、コンポーネント説明、コンポーネントＩＤ、リリースバージョンまたは重大度の少なくとも１つを含むことを特徴とする請求項９に記載の方法。
【請求項１２】
前記ソフトウェア機能性の少なくとも１つは、前記完全性検証チェックの間に少なくとも一度チェックされることを特徴とする請求項４に記載の方法。
【請求項１３】
前記モジュールの少なくとも１つは、１つのコンポーネント中に現れることを特徴とする請求項１２に記載の方法。
【請求項１４】
前記モジュールの少なくとも１つは、２つの機能の間で共有されることを特徴とする請求項４に記載の方法。
【請求項１５】
各モジュールは、関連する機能性を有することを特徴とする請求項４に記載の方法。
【請求項１６】
モジュールのグループは、前記コンポーネントに関連付けられ、前記コンポーネントに関連付けられたコンポーネント識別子（ＩＤ）を共有し、または前記コンポーネントとの完全性についてまとめて検証されることを特徴とする請求項１に記載の方法。
【請求項１７】
モジュールは、前記ＷＴＲＵに関連付けられ、前記モジュールは、１つのコンポーネント識別子（ＩＤ）を有し、および他のモジュールとは異なる機能性識別子（ＩＤ）に分類されることを特徴とする請求項１に記載の方法。
【請求項１８】
モジュールは、前記ＷＴＲＵに関連付けられ、前記モジュールは、機能性および完全性チェック量に基づいて分類されることを特徴とする請求項１に記載の方法。
【請求項１９】
前記共有されるコンポーネント識別子を有する前記モジュールは、１つのＴＲＶ（trusted reference value）を有し、および前記ＴＲＶが失敗するという条件で、前記失敗したコンポーネント識別子の前記モジュールが、失敗した機能性のリストを判定するのに使用されることを特徴とする請求項１６に記載の方法。
【請求項２０】
ネットワーク装置は、Ｈ（ｅ）ＮＢ（home evolved Node B）であることを特徴とする請求項１に記載の方法。

フロントページの続き

(31)優先権主張番号 61/239,698
(32)優先日 平成21年9月3日(2009.9.3)
(33)優先権主張国 米国(US)

(72)発明者 インヒョク チャ
アメリカ合衆国 １９０６７ ペンシルベニア州 ヤードリー サウスリッジ サークル ５１０
(72)発明者 アンドレアス ユー. シュミット
ドイツ ６５９２９ フランクフルト アム マイン トイトーネン ３７
(72)発明者 アンドレアス レイチェル
ドイツ ６０４８８ フランクフルト アム マイン ガイスフェルトストラッセ ２
(72)発明者 ヨゲンドラ シー. シャー
アメリカ合衆国 １９３４１ ペンシルベニア州 エクストン リージェンシー コート １０
(72)発明者 ドロレス エフ. ハウリー
アメリカ合衆国 １９０８７ ペンシルベニア州 ウェイン ウォーレス ドライブ ６８０
(72)発明者 デービッド ジー. グレイナー
アメリカ合衆国 １１０４０ ニューヨーク州 ニュー ハイド パーク ヨークシャー ロード ５７
(72)発明者 ローレンス エル. ケース
アメリカ合衆国 １９４６８ ペンシルベニア州 ロイヤーズフォード モーガン ドライブ ３０７
(72)発明者 マイケル ブイ. マイヤーステイン
イギリス アイピー５ ３ティーユー イプスウィッチ マートルシャム ヒース メイフィールズ ２７
(72)発明者 ルイス ジェイ. グッチョーネ
アメリカ合衆国 １０７０９ ニューヨーク州 イースト チェスター リンカーン プレイス ２１１

Ｆターム(参考) 5J104 AA07 KA02 KA04 PA01
5K067 AA30 BB04 DD11 DD51 EE02 EE10 EE16 FF02 HH22 HH23