(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号

特許第5948001号
(P5948001)

(45)発行日　平成28年7月6日(2016.7.6)　(24)登録日　平成28年6月10日(2016.6.10)

(51)Int.Cl.		F I		
H04L 9/16	(2006.01)	H04L	9/00	643
H04L 9/32	(2006.01)	H04L	9/00	675A
G06F 21/62	(2013.01)	G06F	21/62	309

請求項の数 15　(全 15 頁)

(21)出願番号	特願2014-561082 (P2014-561082)
(86)(22)出願日	平成25年3月6日 (2013.3.6)
(65)公表番号	特表2015-511082 (P2015-511082A)
(43)公表日	平成27年4月13日 (2015.4.13)
(86)国際出願番号	PCT/US2013/029397
(87)国際公開番号	WO2013/134402
(87)国際公開日	平成25年9月12日 (2013.9.12)
審査請求日	平成28年1月19日 (2016.1.19)
(31)優先権主張番号	61/607,625
(32)優先日	平成24年3月7日 (2012.3.7)
(33)優先権主張国	米国 (US)
(31)優先権主張番号	13/786,980
(32)優先日	平成25年3月6日 (2013.3.6)
(33)優先権主張国	米国 (US)

早期審査対象出願

(73)特許権者　510284071
モトローラ　モビリティ　エルエルシー
ＭＯＴＯＲＯＬＡ　ＭＯＢＩＬＩＴＹ　ＬＬＣ
アメリカ合衆国、６０６５４　イリノイ州、シカゴ、ウェスト・マーチャンダイズ・マート・プラザ、２２２、スイート・１８００
(74)代理人　100104411
弁理士　矢口　太郎
(72)発明者　ナクジーリ、マジッド　エフ.
アメリカ合衆国、９２１３０　カリフォルニア州、サン　ディエゴ、４６８９　タランテラ　レーン

最終頁に続く

(54)【発明の名称】所要のノード経路と暗号署名とを用いたセキュアなパケット送信のためのポリシー

(57)【特許請求の範囲】

【請求項１】

ポリシーに基づいて基盤を介してターゲット装置へと機密パケットを移送するためのエンドツーエンドセキュリティを提供する方法であって、前記方法は、

前記ポリシーを受信するステップであって、前記ポリシーが前記ターゲット装置又はそれを介して前記機密パケットが送信されることが意図される前記基盤のノードにより前記機密パケットの移送、インストール又は消費のうちの少なくとも１つを実行するものである、前記受信するステップと、

前記機密パケットの移送前に前記機密パケットのデータ領域に前記ポリシーを付加するステップであって、前記機密パケットは前記ターゲット装置とそれを介して前記機密パケットが初めに移送される前記基盤の初期ノードとの間のエンドツーエンドの機密保護のために暗号化されるものである、前記付加するステップと、

前記機密パケットに暗号で署名するステップと、

前記基盤の前記ノードを少なくとも介して前記機密パケットを前記ターゲット装置へと送信することを生じさせるステップと、

を有し、

前記機密パケットは、前記ターゲット装置とそれを介して前記機密パケットが初めに移送される前記基盤の初期ノードとの間のエンドツーエンドの機密保護のために暗号化されるものであり、前記前記エンドツーエンドの機密保護のための前記暗号化は、エンドツーエンドのインナーレイヤ暗号化であり、かつホップバイホップ暗号化より前に行われるも

のであり、
前記ポリシーは、それを介して前記機密パケットが送信される前記基盤の各ノードに対し前記機密パケットを処理する前に属性、権原又は前記各ノードの性能が前記ポリシーに合致するか否かを確認することを要求するものである
方法。
【請求項２】
ポリシーに基づいて基盤を介してターゲット装置へと機密パケットを移送するためのエンドツーエンドセキュリティを提供する方法であって、前記方法は、
前記ポリシーを受信するステップであって、前記ポリシーが前記ターゲット装置又はそれを介して前記機密パケットが送信されることが意図される前記基盤のノードにより前記機密パケットの移送、インストール又は消費のうちの少なくとも１つを実行するものである、前記受信するステップと、
前記機密パケットの移送前に前記機密パケットのデータ領域に前記ポリシーを付加するステップであって、前記機密パケットは前記ターゲット装置とそれを介して前記機密パケットが初めに移送される前記基盤の初期ノードとの間のエンドツーエンドの機密保護のために暗号化されるものである、前記付加するステップと、
前記機密パケットに暗号で署名するステップと、
前記基盤の前記ノードを少なくとも介して前記機密パケットを前記ターゲット装置へと送信することを生じさせるステップと、
を有し、
前記機密パケットは、前記ターゲット装置とそれを介して前記機密パケットが初めに移送される前記基盤の初期ノードとの間のエンドツーエンドの機密保護のために暗号化されるものであり、前記前記エンドツーエンドの機密保護のための前記暗号化は、エンドツーエンドのインナーレイヤ暗号化であり、かつホップバイホップ暗号化より前に行われるものであり、
前記ポリシーが前記機密パケットへと付加されるデータ領域は、前記基盤の識別子若しくはフラグの少なくとも次のノードの形式におけるプロファイルタイプ、プロファイル所有者識別子、プロファイルセキュリティ堅牢性レベル、プロファイルポリシー特徴ベクトル、プロファイル経路情報又は経路制御情報を含むものであり、
前記プロファイル経路情報は、前記基盤内のノードの所要のノード経路を含み、前記所要のノード経路は前記基盤内の前記ノードを特定する識別子のリストとして構成されるものであり、
前記ポリシーは、前記所要のノード経路の各ノードに対して各ノードのそれぞれの識別子が前記識別子のリストに存在するか否かを決定させ、前記各ノードのそれぞれの識別子が前記識別子のリストに無いと決定された場合、前記機密パケットを静かに破棄し、前記所要のノード経路の直前のノードへと第１の通知を送信し、及び前記所要のノード経路の初期ノードへと第２の通知を送信することを要求するものである
方法。
【請求項３】
ポリシーに基づいて基盤を介してターゲット装置へと機密パケットを移送するためのエンドツーエンドセキュリティを提供する方法であって、前記方法は、
前記ポリシーを受信するステップであって、前記ポリシーが前記ターゲット装置又はそれを介して前記機密パケットが送信されることが意図される前記基盤のノードにより前記機密パケットの移送、インストール又は消費のうちの少なくとも１つを実行するものである、前記受信するステップと、
前記機密パケットの移送前に前記機密パケットのデータ領域に前記ポリシーを付加するステップであって、前記機密パケットは前記ターゲット装置とそれを介して前記機密パケットが初めに移送される前記基盤の初期ノードとの間のエンドツーエンドの機密保護のために暗号化されるものである、前記付加するステップと、
前記機密パケットに暗号で署名するステップと、

前記基盤の前記ノードを少なくとも介して前記機密パケットを前記ターゲット装置へと送信することを生じさせるステップと、
を有し、
前記機密パケットは、前記ターゲット装置とそれを介して前記機密パケットが初めに移送される前記基盤の初期ノードとの間のエンドツーエンドの機密保護のために暗号化されるものであり、前記前記エンドツーエンドの機密保護のための前記暗号化は、エンドツーエンドのインナーレイヤ暗号化であり、かつホップバイホップ暗号化より前に行われるものであり、
前記ポリシーが前記機密パケットへと付加されるデータ領域は、前記基盤の識別子若しくはフラグの少なくとも次のノードの形式におけるプロファイルタイプ、プロファイル所有者識別子、プロファイルセキュリティ堅牢性レベル、プロファイルポリシー特徴ベクトル、プロファイル経路情報又は経路制御情報を含むものであり、
前記プロファイル経路情報は、前記基盤内のノードの所要のノード経路を含み、前記所要のノード経路は前記基盤内の前記ノードを特定する識別子のリストとして構成されるものであり、
前記ポリシーは、前記所要のノード経路の各ノードに対して各ノードのそれぞれの識別子が前記識別子のリストに存在するか否かを決定させ、前記各ノードのそれぞれの識別子が前記識別子のリストに存在すると決定された場合、前記機密パケットを前記ポリシーに記載される通り処理し、前記識別子のリストに基づいて前記所要のノード経路の次のノードを決定し、前記次のノードのため前記機密パケットを暗号化し、前記データ領域の次ノードデータ領域を更新することを要求するものである
方法。

【請求項４】
請求項１～３のいずれか１つに記載の方法において、前記機密パケットの処理は、
前のホップバイホップ暗号を復号するステップと、
少なくとも前記機密パケットの所定の部分に暗号で署名するステップと、
前記パケットを前記基盤の次のノードへと転送する手段を決定するステップと、
前記ポリシーと合致するよう前記機密パケットの付加部分を更新するステップと、
前記機密パケットを暗号化するステップ
とを含む方法。

【請求項５】
請求項１～３のいずれか１つに記載の方法において、前記機密パケットの処理は、前記機密パケットの処理結果の通知を前記機密パケットのソース又は所有者へと送信するステップを含む方法。

【請求項６】
請求項１～３のいずれか１つに記載の方法において、前記機密パケットに暗号で署名することは、前記基盤の中間ノードにより行われるものである方法。

【請求項７】
請求項１～３のいずれか１つに記載の方法において、前記方法は、前記機密パケットの所有者、前記機密パケットの発生者又はポリシー決定点により行われるものである方法。

【請求項８】
請求項１～３のいずれか１つに記載の方法において、さらに、特定の認証プロセス又は特定のセキュリティ堅牢性レベルを順守する性能を有する前記基盤のノードに基づいて前記ポリシーを決定するステップを含むものである方法。

【請求項９】
請求項２または３に記載の方法において、前記ノードを特定する前記識別子は、ＩＰアドレス又は完全に指定されたドメイン名（ＦＤＱＮ）を含むものである方法。

【請求項１０】
請求項２または３に記載の方法において、前記所要のノード経路は、既存の信頼関係、セキュリティアソシエーション又はセキュリティ堅牢性を扱う性能に基づいて決定される

ものである方法。
【請求項１１】
請求項１～３のいずれか１つに記載の方法において、前記ポリシーは、前記基盤を介する所要のノード経路と前記所要のノード経路の各ノードに対して、前記ノードが前記所要のノード経路内にて特定されたことを決定することに応答して、前記機密パケットの所定の部分に暗号で署名することを要求するものである方法。
【請求項１２】
請求項１～３のいずれか１つに記載の方法において、前記ポリシーは、前記基盤を介する所要のノード経路と、前記所要のノード経路の最終ノードが前記所要のノード経路のその他のノードを認証することを要求するものである方法。
【請求項１３】
請求項１２に記載の方法において、前記ポリシーは、前記所要のノード経路のその他のノードを認証することに応答して前記所要のノード経路の最終ノードに対して前記機密パケットの送信者に前記認証の結果を送信し、前記結果を記録し、前記機密パケットを記録し、及び成功処理後には前記ターゲット装置へと前記機密パケットを送信し又は不成功処理後には前記機密パケットを破棄することを要求するものである方法。
【請求項１４】
請求項１２に記載の方法において、前記ポリシーは、前記所要のノード経路のその他のノードを認証することに応答して前記所要のノード経路の最終ノードに対して前記機密パケットをローカルに処理することを試み、不成功の場合、前記機密パケットを破棄し、及び前記処理が不成功であったことを示す応答を送信することを要求するものである方法。
【請求項１５】
請求項１～３のいずれか１つに記載の方法において、前記ポリシーが前記機密パケットに付加される１又は２以上のデータ領域は、平文であり、前記平文のデータ領域は次のノードの識別子、フラグ、アウターレイヤポリシールール、フラグ又は前記ターゲット装置の識別子を含むものである方法。
【発明の詳細な説明】
【技術分野】
【０００１】
（関連出願）
本願は、本記載によりその全体が参照により取り込まれるＭａｄｊｉｄ　Ｆ．　Ｎａｋｈｊｉｒｉにより２０１２年３月７日に出願された「遠隔プロビジョニングにおける安全なポリシーの実行」と題された出願番号６１／６０７，６２５の仮出願に対して優先権を主張する。
【背景技術】
【０００２】
現代のスマートカード技術は携帯電話、タブレット型コンピュータ及び自動車ナビゲーションシステム等といったモバイルコンピューティングデバイス内にて使用される非取り外し式埋め込み型スマートカードへと移行しつつある。近年の例としては埋め込み型ユニバーサル集積回路カード（ｅＵＩＣＣ）があり、安全機密機能を果たすために使用されている。スマートカード以外では、スマートカードにより現在行われている機能と類似の機能を実行するために高信頼環境（ＴｒＥ）を使用するという傾向も存在する。
この出願の発明に関連する先行技術文献情報としては、以下のものがある（国際出願日以降国際段階で引用された文献及び他国に国内移行した際に引用された文献を含む）。
（先行技術文献）
（特許文献）
（特許文献１）　米国特許第８，２１４，６５３号明細書
（特許文献２）　米国特許出願公開第２０１０／０１３８５３９号明細書
（特許文献３）　米国特許出願公開第２０１０／０１９２１９７号明細書
（特許文献４）　米国特許出願公開第２００８／０３１７００２号明細書

（非特許文献）
（非特許文献１） ＢＥＬＧＡＩＥＤ Ｋ； ＷＩＮＩＧＥＲ Ｇ："Ｇｅｎｅｒａｌｉｚｅｄ Ｌａｂｅｌｅｄ Ｓｅｃｕｒｉｔｙ Ｏｐｔｉｏｎ； ｄｒａｆｔ－ｂｅｌｇａｉｅｄ－ｉｐｖ６－１ｓｏｐｔ－００．ｔｘｔ", ＩＮＴＥＲＮＥＴ ＥＮＧＩＮＥＥＲＩＮＧ ＴＡＳＫ ＦＯＲＣＥ, ＩＥＴＦ, Ｆｅｂｒｕａｒｙ ２００１, ａｌｌ ｐａｇｅｓ．
（非特許文献２） ＬＩＮ Ｘ ＥＴ ＡＬ．："ＡＳＰＲＡＫＥ： Ａｎ Ａｎｏｎｙｍｏｕｓ Ｓｅｃｕｒｅ Ｒｏｕｔｉｎｇ Ｐｒｏｔｏｃｏｌ ｗｉｔｈ Ａｕｔｈｅｎｔｉｃａｔｅｄ Ｋｅｙ Ｅｘｃｈａｎｇｅ ｆｏｒ Ｗｉｒｅｌｅｓｓ Ａｄ Ｈｏｃ Ｎｅｔｗｏｒｋｓ", ＰＲＯＣＥＥＤＩＮＧＳ ＯＦ ＴＨＥ ２００７ ＩＥＥＥ ＩＮＴＥＲＮＡＴＩＯＮＡＬ ＣＯＮＦＥＲＥＮＣＥ ＯＮ ＣＯＭＭＵＮＩＣＡＴＩＯＮＳ（ＩＣＣ ２００７）, ２４－２８ ＪＵＮＥ ２００７, ＧＬＡＳＧＯＷ, ＵＫ, ＩＥＥＥ, ＰＩＳＣＡＴＡＷＡＹ, ＮＪ, ＵＳＡ, Ｊｕｎｅ ２００７, ｐａｇｅｓ １２４７－１２５３．
（非特許文献３） ＰＡＴＥＮＴ ＣＯＯＰＥＲＡＴＩＯＮ ＴＲＥＡＴＹ, Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｓｅａｒｃｈ Ｒｅｐｏｒｔ ａｎｄ Ｗｒｉｔｔｅｎ Ｏｐｉｎｉｏｎ ｏｆ ｔｈｅ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｓｅａｒｃｈｉｎｇ Ａｕｔｈｏｒｉｔｙ ｆｏｒ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ａｐｐｌｉｃａｔｉｏｎ Ｎｏ．ＰＣＴ／ＵＳ２０１３／０２９３９７（ＣＳ３９９５５）, １４ Ｊｕｎｅ ２０１３, １４ ｐａｇｅｓ．
（非特許文献４） "Ｅｍｂｅｄｄｅｄ ＵＩＣＣ, Ａ ｈｉｇｈ ｌｅｖｅｌ ｒｅｍｏｔｅ ｐｒｏｖｉｓｉｏｎｉｎｇ ａｒｃｈｉｔｅｃｔｕｒｅ", ＧＳＭＡ ｅｍｂｅｄｄｅｄ ＳＩＭ ｔａｓｋ ｆｏｒｃｅ： ｔｅｃｈｎｉｃａｌ ｓｔｒｅａｍ, １８－２０ｔｈ Ｊｕｌｙ, ２０１１, １６ ｐａｇｅｓ．
（非特許文献５） "Ｒｅｍｏｔｅ Ｐｒｏｖｉｓｉｏｎｉｎｇ ｏｆ Ａｃｃｅｓｓ Ｃｒｅｄｅｎｔｉａｌｓ", ｄｏｃｕｍｅｎｔ ｊｏｉｎｔｌｙ ｃｒｅａｔｅｄ ｂｙ Ｅｒｉｃｓｓｏｎ, Ｍｏｔｏｒｏｌａ Ｍｏｂｉｌｉｔｙ ａｎｄ Ｑｕａｌｃｏｍｍ, ｎｏｔ ｐｕｂｌｉｓｈｅｄ, Ｖ２８．, Ｓｅｐｔｅｍｂｅｒ ２０１１, ３７ ｐａｇｅｓ．
（非特許文献６） Ｒ．Ｈｏｕｓｌｅｙ, "Ｃｒｙｐｔｏｇｒａｐｈｉｃ Ｍｅｓｓａｇｅ Ｓｙｎｔａｘ（ＣＭＳ）", ＩＥＴＦ ＲＦＣ ３８５２, Ｊｕｌｙ ２００４, １１２ ｐａｇｅｓ．

【発明の概要】
【発明が解決しようとする課題】
【０００３】
しかしながら、多くの非取り外し式である埋め込み型スマートカードと高信頼環境では埋め込み後にデータが外部から提供される必要がある。このため、埋め込み型スマートカードと高信頼環境には機密データが遠隔的に提供されることとなる。しかしながら、機密情報を遠隔的に提供すれば様々な安全性リスク、通信の複雑化及びアカウンタビリティの不確実性を生じさせることとなる。
【図面の簡単な説明】
【０００４】
添付の図面を参照しつつセキュアなパケット送信のためのポリシーと当該ポリシーの認証を可能とする技術及び装置が記載される。同種の特徴及び構成を参照するため複数の図面を通じて同一の番号が使用される。
【図１】図１は、所要のノード経路と暗号署名を用いたセキュアなパケット送信のためのポリシーを実現する技術が実施され得る例示的環境を示す図である。
【図２】図２は、図１のソースノードを詳細に例示した図である。
【図３】図３は、図１のターゲット装置を詳細に例示した図である。
【図４】図４は、所要のノード経路と暗号署名とを用いたセキュアなパケット送信のため

のポリシーを実現する例示的方法について示す図である。
【図５】図５は、潜在的な中間ノードを有する基盤と前記潜在的な中間ノードから決定された所要のノード経路を示す図である。
【図６】図６は、あるパケットについてセキュアなパケット送信のためのポリシーが順守されたか否かを決定する例示的方法について示す図である。
【図７】図７は、ポリシーの実行中であって基盤を介してターゲット装置へと機密パケットを移送するためのエンドツーエンドの安全性を提供する例示的方法について示す図である。
【図８】図８は、セキュアなパケット送信のためのポリシーと当該ポリシーの認証の実行を行う技術を実施することが可能な例示的装置の種々の構成要素を例示する図である。
【発明を実施するための形態】
【０００５】
機密データを遠隔的に提供する現在の技術は様々なセキュリティリスク、通信の複雑化又はアカウンタビリティの不確実性を生じさせることとなる。本開示は所要のノード経路と暗号署名とを用いたセキュアなパケット送信のためのポリシーを可能とする技術及び装置について説明する。それにより、ターゲット装置のセキュアな実行環境（ＳＥＥ）は機密データを受信してもよい。これらのセキュアな実行環境は上記の埋め込み型ユニバーサル集積回路カード（ｅＵＩＣＣ）、その他の形式の埋め込み型チップ、様々な高信頼環境（ＴｒＥｓ）又はＳＩＭカード等の取り外し式若しくは非埋め込み型カード又は機密データをセキュアに受信することから利益を得る様々な装置若しくは物のいずれも含み得る。
【０００６】
以下では先ず動作環境について、次に前記環境において前記技術を採用する例示的方法について説明し、その後前記技術を採用する例示的装置の説明に移る。
【０００７】
例示的環境
図１は所要のノード経路と暗号署名を用いたセキュアなパケット送信のためのポリシーを可能とする技術が実現された例示的環境１００を示す。環境１００はソースノード１０２、１又は２以上の有線及び／又は無線の通信ネットワーク１０４及びターゲット装置１０６を含む。機密データは所望のノード経路１１０の一部としてノード１０８－１、１０８－２、１０８－３及び１０８－４として示される中間ノード１０８を介して送信される。
【０００８】
一般に、ソースノード１０２はターゲット装置１０６を意図とした機密データのソースである。ある場合において、ソースノード１０２は前記機密データを有するエンドツーエンド暗号化を実行可能な信頼されたサブスクリプションマネージャ等の前記中間ノード１０８のうちの信頼された１つ（例、ノード１０８－１）とセキュアな通信を行うモバイルネットワークオペレータである。
【０００９】
通信ネットワーク１０４はネットワーク１０４－１、１０４－２、１０４－３、１０４－４及び１０４－５として各々示される１つ又は複数の通信ネットワークを含み得るが、ネットワークとの用語はノード間の単純な経路であり得り又は複数のネットワーク（セルラー、有線及び無線のローカルエリア）を有する有線及び／又は無線の通信チャネルの複雑な組み合わせを含み得る。必須ではないものの、最終ホップはしばしば無線送信であるためネットワーク１０４－５は無線ネットワークとして例示されている。
【００１０】
一般に、ターゲット装置１０６は所要のノード経路１１０を介して送信され、前記所要のノード経路の各ノードの暗号署名を有する署名を受信する。パケット１１２は所要のノード経路１１０を示すポリシーも含み得り、ペイロード（すなわち、機密データ）に追加して署名された各中間ノード１０８からの暗号署名（「中間＃１署名」等）とエンドツーエンド暗号署名（「ソース署名」として示される）を有するパケットを単純化された形式

にて例示する。各中間ノード１０８は暗号によりパケットに署名してもよいが、ある実施形態においては、信頼される中間ノードからの署名なしで所要の経路ノードが認証されてもよい。

【００１１】

所要のノード経路の特定（すなわち、ＩＰアドレス又は完全に指定されたドメイン名等といった前記所要のノード経路の中間ノードの識別子のリスト）は平文で有り得り又はそうでない場合前記所要のノード経路の各ノードにとってアクセス可能であり得る。これにより各ノードは前記パケットがいずれのノードに次に送信されるべきかを決定することができる。前記所要のノード経路はまた不正変更を防止するため暗号により中間ノードによる変更ができないようになっていてもよい。ある形態において、前記所定のノード経路はターゲット装置１０６又はある場合においては信頼された中間ノード（すなわち、ノード１０８－４）により決定可能である。これは前記パケットが前記所要のノード経路を正しく辿ったという認証を許可する。

【００１２】

より詳細には、図２に例示されるソースノード１０２を参照されたい。ソースノード１０２は１又は２以上のソースプロセッサ２０２及びソースコンピュータ可読記憶媒体（ＣＲＭ）２０４を含むか又はそれらに対してアクセスを有している。ソースＣＲＭ２０４はポリシーモジュール２０６及び機密データ２０８を含む。ポリシーモジュール２０６は所要のノード経路１１０を有するポリシー２１０を含み及び／又は決定する。

【００１３】

一般に、ポリシーモジュール２０６はそれを介してターゲット装置へと送信されることが意図される基盤を介して所要のノード経路を決定することが出来る。ポリシーモジュール２０６はそれ単独又は信頼された中間ノードを介して動作し前記パケットにポリシーを付加し、前記パケットに暗号で署名する。ポリシー２１０は所要のノード経路１１０を含み又は所要のノード経路１１０と共にパケットに対して付加される。

【００１４】

上記にて部分的に述べられた通り、ポリシー２１０はターゲット装置１０６（又は前記ターゲット装置により信頼されたノード）が中間ノード１０８の暗号署名に基づいて前記基盤を介したパケットの実際のノード経路が所要のノード経路１１０と合致するかを決定することを可能とする。これらの暗号署名はセキュアか又は署名者の同一性を認証可能な様々なタイプとなり得る（すなわち、前記パケットに署名を行った中間ノードの同一性は前記署名を介して認証され得る）。

【００１５】

ポリシー２１０はまた各中間ノードが属性、権原又はセキュリティ堅牢性レベル等の性能を確認することを要求してもよい。ある実施形態においては、ポリシー２１０はまた各中間ノードが前記パケットに暗号署名した後に前記パケットを送信する次の中間ノードを決定することを要求してもよい。その場合、所要のノード経路１１０は前記パケット内にてアクセス可能な形式（すなわち、リスト）にて含まれてもよいものの、それは変更不可となっていてもよい（すなわち、ポリシー２１０内にて暗号署名の際に暗号でハッシュ又は記憶される）。

【００１６】

図３を考慮すると、ターゲット装置１０６が詳細に例示される。ターゲット装置１０６は各々１つ又は種々の装置の組み合わせであってもよく、ネットブック、カーナビゲーションシステム及びサーバ等のその他のコンピュータ装置及びシステムも使用され得るものの、ここでは６つの例、すなわちスマートフォン１０６－１、ラップトップコンピュータ１０６－２、テレビジョン１０６－３、デスクトップコンピュータ１０６－４及びタブレットコンピュータ１０６－５が示されている。

【００１７】

ターゲット装置１０６は１又は２以上のターゲットプロセッサ３０２及びターゲットコンピュータ可読記憶媒体（ＣＲＭ）３０４を含み又はそれらに対してアクセスを（例えば

信頼された中間ノードを介して）有している。ターゲットＣＲＭ３０４はポリシー認証部３０６、復号モジュール３０８及びパケット１１２を含む。パケット１１２は機密データ２０８、ソース署名３１０、中間ノード暗号署名３１２、ポリシー２１０及び所要のノード経路１１０を含む。

【００１８】

ポリシー認証部３０６は中間ノード暗号署名３１２に基づき前記基盤のノードを介したパケット１１２の実際の経路を決定することが出来る。ポリシー認証部３０６はその後前記パケットの実際の経路がパケット１１２の所要のノード経路１１０と合致するか否かを決定する。認証された場合、ポリシー認証部３０６は機密データ２０８を信頼する。認証されなかった場合、ポリシー認証部３０６は例えば前記経路を認証することに失敗したことに言及するためその決定を第三者に示す。ターゲット装置１０６により行われる１又は２以上の動作はある実施形態においては埋め込み型又は非埋め込み型（すなわちＳＩＭカード）装置と共に実行され得る。

【００１９】

復号モジュール３０８は機密データ２０８を復号することが可能であるものの、復号モジュール３０８はポリシー認証部３０６がパケット１１２の前記実際のノード経路と所要のノード経路１１０とが合致しないことを決定した場合そのようにすることを控えてもよい。本書面は前記技術を実施するための例示的方法へと移行し、その後例示的装置が記載される。

【００２０】

例示的方法

図４は所要のノード経路と暗号署名とを用いたセキュアなパケット送信のためのポリシーを可能とする例示的方法４００について示す。これら及びその他の方法におけるブロックが記載される順番は限定として解釈されることを意図したものではなく、本書面に記載されるブロックのいずれの番号又は組み合わせは方法又は代替的方法を実施するためにいずれの順序でも組み合わせ得る。

【００２１】

ブロック４０２はパケットがそれを介してターゲット装置へと送信されることを意図される基盤を介して所要のノード経路を決定し、前記所要のノード経路はソースノードと前記ターゲット装置との間の１又は２以上の中間ノードを有している。図１は所要のノード経路１１０の中間ノード１０８を例示する。しかしながら、図の見易さのため、図１の例示的環境１００はそこから中間ノード１０８がソースノード１０２により決定される基盤の他の中間ノードを示していない。例として、図５を考慮すると、基盤５０４の２８個の中間ノード５０２を例示している。

【００２２】

ブロック４０２において、図２のポリシーモジュール２０６は例えば信頼された又は優れたものに基づいて基盤５０４の前記２８個の潜在的な中間ノード５０２を介して所要のノード経路を決定する。一の例では、ポリシーモジュール２０６は他の要素も使用され得るもののセキュリティ堅牢性レベル、現存の信頼関係又はセキュリティ関連性に基づいて潜在的中間ノード５０２の一部が他より優れていると決定する。ここで、ポリシーモジュール２０６は中間ノード５０６、５０８、５１０、５１２、５１４、５１６及び５１８を介する所要のノード経路を前記パケットが送信されることとなる対応順序、すなわち１から６までと共に決定する。

【００２３】

ブロック４０４では前記パケットにポリシーを付加し、前記ポリシーは前記所要のノード経路を有している。上述の通り、前記ポリシーは前記所要のノード経路の各ノードに対して直前のノードの暗号署名を有効化し、前記ターゲット装置又は前記パケットを有効化する前記所要のノード経路の次のノードを可能化するために前記パケットに有効に暗号で署名することを要求してもよい。

【００２４】

ブロック４０６では前記パケットに暗号で署名する。前記パケットは様々な態様で暗号化され得る。例えば、前記パケットのペイロードデータ（例えば機密データ２０８）を前記ペイロードデータが前記ターゲット装置によるもの以外では復号することが不可能な態様で前記パケットのインナーレイヤにおいて暗号化するものであってもよい。しかしながら、前記ポリシーは前記パケットのアウターレイヤにおいて暗号化されてもよく又は平文であってもよい。

【００２５】

ブロック４０８は前記ターゲット装置へと前記所要のノード経路を介して前記パケットが送信されることを生じさせる。ソースノード１０２又は図１の中間ノード１０８－１等のような信頼されかつ一般に初めの中間ノードは前記所要のノード経路の次のノードへと前記パケットを送信し得る。一の例示的ケースにおいてソースノード１０２はモバイルネットワークオペレータであり、前記信頼された中間ノードはサブスクリプションマネージャデータプレパレーション（ＳＭ－ＤＰ）、その他の中間ノードは役割を果たさないサブスクリプションマネージャ（ＳＭｓ）、最終中間ノードはターゲット装置１０２により信頼され役割を果たすサブスクリプションマネージャセキュアルーティング（ＳＭ－ＳＲ）である。しかしながらこれは前記技術がセキュアなパケット送信を可能とする場合の多くのケースの中の一例である。

【００２６】

図６はセキュアなパケット送信のためのポリシーがあるパケットについて順守されたか否かを決定するための例示的方法６００を示す。

【００２７】

ブロック６０２では最終ノードにおいて基盤を介する前記パケットの所要のノード経路を示すパケットを受信し、前記所要のノード経路は所要のソースノードと１又は２以上の所要の中間ノードを示している。

【００２８】

ブロック６０４では暗号署名に基づいて前記基盤を介する前記パケットの実際のノード経路を決定し、前記実際のノード経路は実際のソースノードと１又は２以上の実際の中間ノードとを示している。

【００２９】

ブロック６０６では前記パケットの前記実際のノード経路が前記パケットの前記所要のノード経路と合致するか否かを決定する。Ｙｅｓの場合、方法６００はＹｅｓ経路に沿ってブロック６０８へと進む。Ｎｏの場合、方法６００はＮｏ経路に沿ってブロック６１０へと進む。

【００３０】

ブロック６０８では前記実際のノード経路が前記所要のノード経路と合致すことを決定することに応答して前記最終ノードにおける前記パケットの内容を信頼する。

【００３１】

ブロック６１０では前記実際のノード経路が前記所要のノード経路と合致しないを決定することに応答して前記最終ノードにおける前記パケットの内容を信頼しない。

【００３２】

任意に、方法６００はブロック６１０又はブロック６０８（図示せず）の後にブロック６１２へと進んでもよい。ブロック６１２ではブロック６０６の前記結果を遠隔地の主体へと送信し、前記結果は前記実際のノード経路が前記所要のノード経路と合致すること又は前記所要のノード経路の一部ではない前記実際のノード経路のノードの識別性と合致することを十分に示すものである。この識別性は中間ノードにおける不具合を示し得り、それはその中間ノードが修理され、損失となり又は当該ノードに課されたものが失敗となることを許容し得る。いくつかの失敗はリソースに関して不経済となり又は収入の減少となり得るので、損失に関するアカウンタビリティを課する本能力は有用になり得る。

【００３３】

方法６００は全体又は一部としてターゲット装置１０６又はターゲット装置１０６の信

頼された中間ノードにより実行され得ることに注意されたい。方法６００が例えば図５の中間ノード５１８のような中間ノードにおいて動作するポリシー認証部３０６により実行される場合、当該中間ノードは前記パケットが信頼に足ることを示す認証可能な指示等と共にターゲット装置１０６へとセキュアにパケット１１２を通過させ得る。従って、方法６００はターゲット装置１０６又はターゲット装置１０６により信頼された中間ノードにて実行され得る。そのように行う際、ポリシー認証部３０６等のターゲット装置１０６の様々な構成は当該信頼された中間ノード上で動作し得る。これは前記所要のノード経路を認証することに前記各中間ノード（ここでは中間ノード５１８）の暗号署名を必要としないケースのうちの１つである。

【００３４】

図７は基盤を介するターゲット装置への機密パケットの移送のためのエンドツーエンドのセキュリティを提供する例示的方法について示し、前記機密パケットの移送、インストール又は消費のうちの少なくとも１つに関する一組のポリシーを実行するものである。方法７００は非限定的であり、前記技術が動作し得る方法の例である。

【００３５】

方法７００は前記基盤の初期及び信頼されたノード、前記機密パケットの所有者、前記機密パケットの発生者又はポリシー決定点等（例えば、ソースノード１０２、図１の信頼された中間ノード１０８－１及び図５の５０６）の本書面にて記載される様々な装置により実行され得る。

【００３６】

ブロック７０２では基盤のノード又はターゲット装置による機密パケットの移送、インストール又は消費を実行するポリシーを受信する。一の実施形態において、本ポリシーはそれを介して前記機密パケットが送信される基盤の各ノードに前記各ノードの属性、権原又は性能が前記ポリシーに合致するか否かを確認することを要求し、前記確認は前記機密パケットの処理の前に要求される。これらの要求の例は、前のホップバイホップ暗号を復号すること、少なくとも前記機密パケットの所定の部分に暗号で署名すること、前記パケットを前記基盤の次のノードへと転送する手段を決定すること、前記ポリシーと合致するよう前記機密パケットの付加部分を更新すること、前記機密パケットを暗号化すること、及び／又は前記処理の通知を前記機密パケットのソース等へと送信すること（例えば、図１のソースノード１０２）を含む。

【００３７】

さらに、前記ポリシーはノードに対して各ノードがそれ自体前記ポリシーにおいて特定されるか否かについて決定することを要求し得り、特定されない場合、前記機密パケットを静かに破棄し、前記所要のノード経路の直前のノードへと通知を送信し、及び前記所要のノード経路の初期ノード（例えば、図１のソースノード１０２又は中間ノード１０８－１）へと他の通知を送信することを要求し得る。前記ノードが前記ポリシーにおいて特定されると決定した場合、前記ポリシーは前記ノードに対して前記機密パケットを前記ポリシーに記載される通り処理し、前記識別子のリストに基づいて前記所要のノード経路の次のノードを決定し、前記次のノードのため前記機密パケットを暗号化し、及び前記データ領域の次ノードデータ領域を更新することを要求してもよい。従って、前記技術はまた例えば前記基盤のノードにおいて前記ポリシーを順守するよう中間ノードを介して動作し得る。

【００３８】

また、方法４００及び６００に示される通り、前記ポリシーはある実施形態においては方法７００により決定され又実行され得る。ブロック７０２にて受信した前記ポリシーは特定の認証プロセス又は特定のセキュリティ堅牢性レベル、上記で特定される通りその他要素を順守する性能を有する前記基盤のノードに基づいて決定され得る。

【００３９】

ブロック７０４では前記機密パケットの移送より前に前記機密データのデータ領域に前記ポリシーを付加する。これらのデータ領域及びすなわち前記ポリシーそれ自体はプロフ

ァイルタイプ、プロファイル所有者識別子（例えば、ソースノード）、プロファイルセキュリティ堅牢性レベル、プロファイルポリシー特徴ベクトル、プロファイル経路情報又は識別子若しくはフラグを用いた前記基盤の少なくとも次のノードの経路情報を含み得る。

【００４０】

ブロック７０６では前記機密パケットに暗号で署名する。当該署名は上述の通り前記機密パケットの送信者又は前記機密パケットの発生者等様々な主体により行われ得る。

【００４１】

上述の通り、ある場合において前記機密は様々なレベル（インナー、アウター等）において暗号化される。前記機密パケットは前記ターゲット装置と例えばそれを介して前記機密パケットが最初に移送される前記基盤の最初のノードとの間のエンドツーエンドの機密保護のために暗号化され得る。このエンドツーエンドの機密保護は上述の通りインナーレイヤ暗号化であり得り、アウターレイヤ暗号化より前に実行され得る（例えば、ホップバイホップ暗号化）。前記機密パケットのデータは平文であり得る。平文である領域は次のノード識別子、フラグ、アウターレイヤポリシールール、フラグ又は前記ターゲット装置の識別子を含んでもよい。

【００４２】

ブロック７０８では前記機密パケットが前記基盤のうちの少なくとも１つのノードを介して前記ターゲット装置まで送信されることを生じさせる。本書面にて示される通り、それを介して前記機密パケットが送信される各ノードは、ターゲット装置又は最終及び信頼された中間ノードと共に、前記パケットのデータ領域に付加された前記ポリシーに沿って動作し得る。そのように行うことにより、前記機密データは前記ソースノードから前記ターゲット装置までセキュアに送信され得る。

【００４３】

示された通り、方法７００は前記機密パケットが前記ターゲット装置へと送信されることを生じさせる。このターゲット装置又は信頼された（そして最終の）中間ノードは前記ポリシーにより動作を行うこと（ある部分は上記方法６００に関して記載された通りである）を要求され得る。これらの動作はそれを介して前記機密パケットが送信される前記ノードが前記ポリシーに合致することを認証することを含み得る。そして、前記ポリシーは前記認証の結果が送信者へと送信されること、前記結果が記録されること、前記機密パケットが記録されること、及び前記機密パケットが成功処理後には前記ターゲット装置へと転送され又は不成功処理後には破棄されることを要求し得る。代替的又は追加的に、前記ポリシーは前記ターゲット装置又は信頼された中間ノードが認証後に前記機密パケットをローカルで処理することを試み及びそれが不成功の場合には前記機密パケットを破棄し、及び前記処理が不成功であったことを示す応答を送信することを要求し得る。

【００４４】

図８は例示的装置８００の様々なコンポーネントを示し、ポリシーモジュール２０６、ポリシー２１０及び／又はポリシー認証部３０６を含む。これらのコンポーネントはハードウエア、ファームウエア及び／又はソフトウエアにて実現され得り、システムオンチップ（ＳｏＣ）を含む図１乃至７のいずれかを参照して記載された通り実現され得る。

【００４５】

例示的装置

例示的装置８００は固定又はモバイル装置にて実施され得り、メディア装置、演算装置（例えば、図１のソースノード１０２、中間ノード１０８及び／又はターゲット装置１０６）、テレビのセットトップボックス、ビデオ処理器及び／又はレンダリング装置、電気製品装置（例えば、閉かつシール状態の演算リソースであり、例えばある種のデジタルビデオレコーダ又は全地球測位衛星装置等）、ゲーム装置、電気装置、車両及び／又はワークステーションのうちの１つ又はその組み合わせであり得る。

【００４６】

例示的装置８００は電子回路、マイクロプロセッサ、メモリ、入出力（Ｉ／Ｏ）論理制御、通信インタフェース及びコンポーネント、装置全体を動作させるために必要なその他

のハードウエア、ファームウエア及び／又はソフトウエアと統合され得る。例示的装置８００はまた前記コンポーネント間のデータ通信のための演算装置の様々なコンポーネントを結合する統合データバス（図示せず）を含み得る。

【００４７】

例示的装置８００は（例えば電子回路を含む）入出力（Ｉ／Ｏ）論理制御８０２及びマイクロプロセッサ８０４（例えばマイクロコントローラ又はデジタル信号プロセッサ）等の様々なコンポーネントを含む。例示的装置８００はまたメモリ８０６を含み、それはいずれの種類のランダムアクセスメモリ（ＲＡＭ）、低遅延非揮発性メモリ（例えばフラッシュメモリ）、読出専用メモリ（ＲＯＭ）及び／又はその他の好適な電子データストレージであり得る。メモリ８０６はポリシーモジュール２０６、ポリシー２１０及び／又はポリシー認証部３０６を含み又はそれらに対しアクセスを有している。

【００４８】

例示的装置８００はまた、その他のコンポーネントと共に、メモリ８０６により保持されマイクロプロセッサ８０４により実行されるコンピュータで実行可能な指令であり得るオペレーティングシステム８０８等の様々なファームウエア及び／又はソフトウエアを含み得る。例示的装置８００はまたその他の様々な通信インタフェース及びコンポーネント、ワイアレスＬＡＮ（ＷＬＡＮ）又はワイアレスＰＡＮ（ＷＰＡＮ）コンポーネント、その他ハードウエア、ファームウエア及び／又はソフトウエアを含み得る。

【００４９】

これらのモジュール及びコンポーネントの他の例示的性能及び機能が図１、２及び３に示されるコンポーネントを参照しつつ説明される。これらのモジュール及びコンポーネントはそれ単独で又はその他のモジュール若しくはコンポーネントと組み合わせて本書面にて記載される様々な実施形態及び／又は特徴を実行するマイクロプロセッサ８０４により実行され及びメモリ８０６により保持されたコンピュータにより実行可能な指令として実施され得る。代替的又は追加的に、いずれか又はすべての当該コンポーネントはハードウエア、ファームウエア、固定論理回路、又は前記Ｉ／Ｏ論理制御８０２及び／又はその他の信号処理及び例示的装置８００の制御回路と関連付けて実行されるそれらのいずれかの組み合わせとして実施され得る。さらに、これらのコンポーネントのうちのいくつかは装置８００とは別に作動してもよい。

【００５０】

前記発明は構造的特徴及び／又は方法論的動作にとって特定の言葉で記載されたものの前記添付の特許請求の範囲にて定義される発明は必ずしも特定の特徴又は記載される動作に限定されるものではないと理解されるべきである。寧ろ、前記特定の特徴及び動作は前記特許請求の範囲に記載された発明を実施する例示的方法として開示されるものである。

【図１】

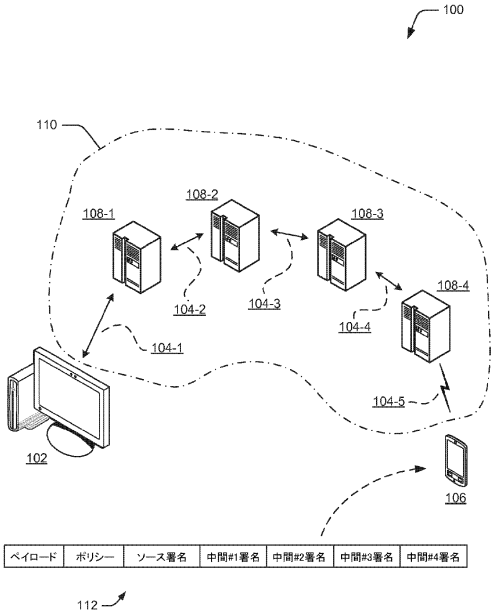

FIG. 1

【図２】

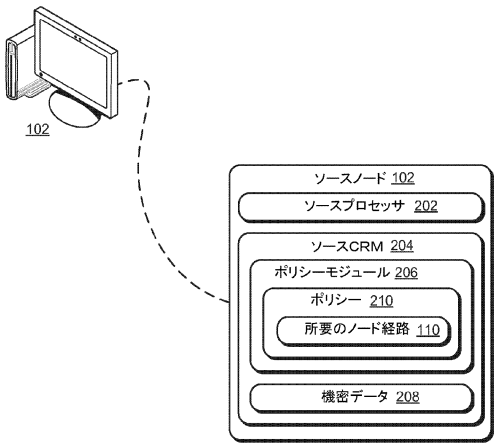

FIG. 2

【図３】

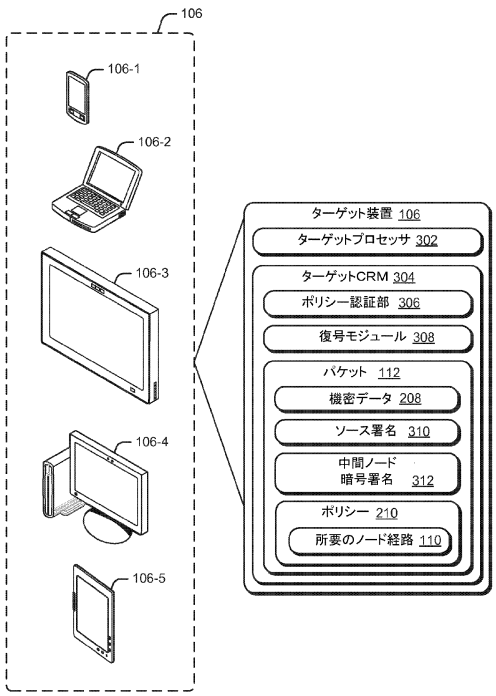

FIG. 3

【図４】

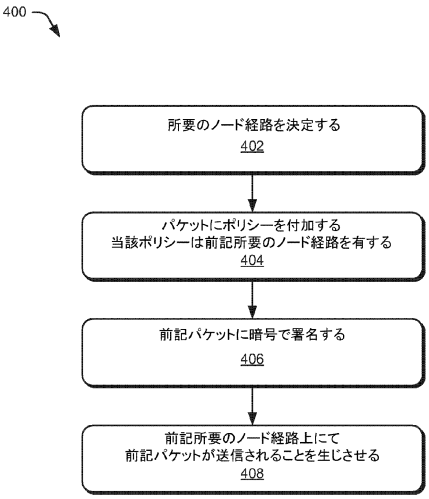

FIG. 4

【図５】

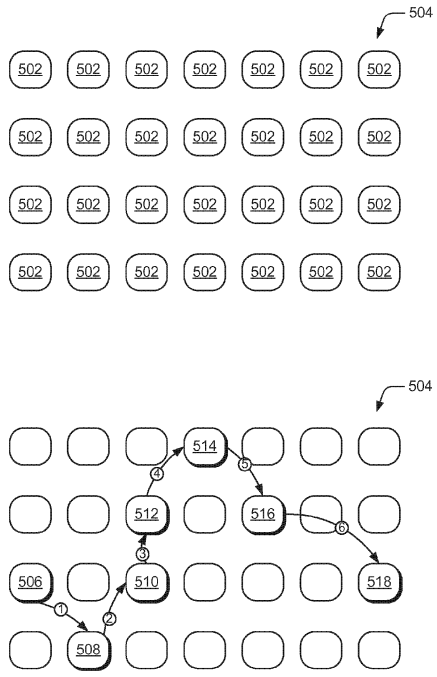

FIG. 5

【図６】

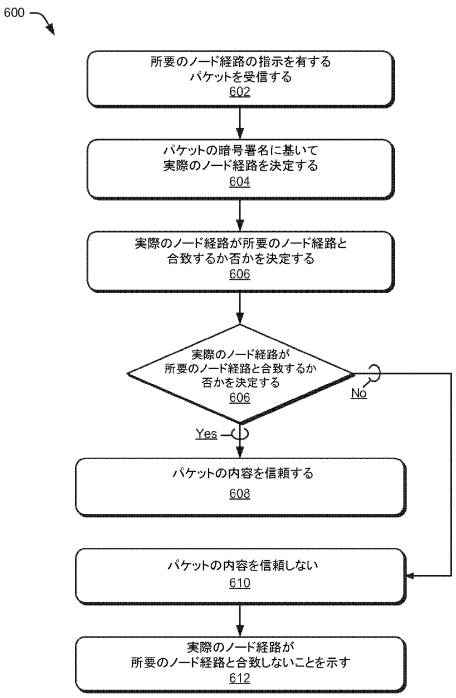

FIG. 6

【図７】

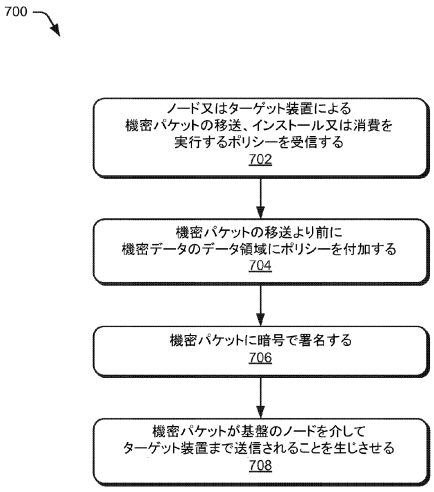

FIG. 7

【図８】

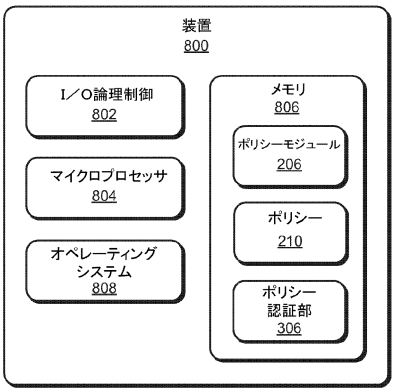

FIG. 8

フロントページの続き

審査官　中里　裕正

(56)参考文献　特開２００３－３４５６６４（ＪＰ，Ａ）
米国特許出願公開第２００８／０１０１３６７（ＵＳ，Ａ１）
特開２００５－１８４８３５（ＪＰ，Ａ）
特開２０００－３４９８２６（ＪＰ，Ａ）
特開平０５－２５２２０８（ＪＰ，Ａ）
米国特許出願公開第２００３／０１４００１０（ＵＳ，Ａ１）
Alexandr, D. S. et al., The SwitchWare Active Network Architecture, IEEE Network, １９９８年, Volume 12 Issue 3, p.29-36
Satoh, I., Mobile Agent-Based Framework for Active Networks, IEEE SMC'99 Conference Proceedings, １９９９年, Volume VI, p.71-76
Murphy, S. et al., Strong Security for Active Networks, 2001 IEEE Open Architectures and Network Programming Proceedings, ２００１年, p.63-70
Davies, D. W. and Price, W. L., ネットワーク・セキュリティ, １９８５年, p.102-108
Davies, D. W. and Price, W. L., Security for Computer Networks, Security for Computer Networks, １９８４年, p.109-116

(58)調査した分野(Int.Cl., ＤＢ名)
Ｈ０４Ｌ　　９／１６
Ｇ０６Ｆ　２１／６２
Ｈ０４Ｌ　　９／３２
ＪＳＴＰｌｕｓ／ＪＭＥＤＰｌｕｓ／ＪＳＴ７５８０（ＪＤｒｅａｍＩＩＩ）
ＩＥＥＥ　Ｘｐｌｏｒｅ