(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第5706308号
(P5706308)
(45)発行日　平成27年4月22日(2015.4.22)　(24)登録日　平成27年3月6日(2015.3.6)

(51)Int.Cl.　F I
H04L 12/70 (2013.01)　H04L 12/70 100Z
H04L 12/22 (2006.01)　H04L 12/22

請求項の数 22　外国語出願　(全 21 頁)

(21)出願番号　特願2011-281241 (P2011-281241)
(22)出願日　平成23年12月22日 (2011.12.22)
(65)公開番号　特開2012-151831 (P2012-151831A)
(43)公開日　平成24年8月9日 (2012.8.9)
審査請求日　平成26年12月19日 (2014.12.19)
(31)優先権主張番号　13/009,427
(32)優先日　平成23年1月19日 (2011.1.19)
(33)優先権主張国　米国(US)

早期審査対象出願

(73)特許権者　504090400
イクシア
アメリカ合衆国・カリフォルニア州　９１３０２・カラバサス・ダブリュー　アグーラ　ロード　２６６０１
(74)代理人　100116872
弁理士　藤田　和子
(72)発明者　ピャトコフスキー　マクシム
アメリカ合衆国　カリフォルニア州　エンシノ
(72)発明者　サハ　ソウムヤジット
アメリカ合衆国　カリフォルニア州　ウッドランド　ヒルズ

審査官　松崎　孝大

最終頁に続く

(54)【発明の名称】プレカルキュレーテッド暗号データを用いた迅速なＳＳＬ検査

(57)【特許請求の範囲】
【請求項１】
検査下のネットワークに接続された複数のポートユニットを含む検査システムによって実行される方法であって、
任意のネットワーク接続を開く前に、前記複数のポートユニットのうちの第１のポートユニットおよび第２のポートユニット内に各々位置する第１のＰＣＣＤ（プレコンピューテッド暗号データ）メモリおよび第２のＰＣＣＤメモリにおける１つ以上のＰＣＣＤのセットを定義し、保存する工程であって、各ＰＣＣＤのセットは、第１のパラメータおよび前記第１のパラメータを暗号化することによって生成される第２のパラメータを少なくとも含む、工程と、
前記１つ以上のＰＣＣＤのセットから選択されたＰＣＣＤのセットを用いて、前記検査下のネットワークを介して、前記第１のポートユニットと前記第２のポートユニットとの間のシミュレートされたセキュアな接続を開く工程であって、前記シミュレートされたセキュアな接続は、解読処理を実行することなく開かれる、工程と
を含む、方法。
【請求項２】
前記シミュレートされたセキュアな接続を開く工程は、前記第１のポートユニットおよび前記第２のポートユニットが、前記検査下のネットワークを介して前記選択されたＰＣＣＤのセットからのデータを含むメッセージを交換する工程を含む、請求項１に記載の方法。

【請求項３】
前記シミュレートされたセキュアな接続は、前記検査下のネットワークに対しては、セキュアな通信プロトコルに適合しているようにみえる、請求項１に記載の方法。
【請求項４】
前記セキュアな通信プロトコルは、少なくとも１つのメッセージを暗号化するために、サーバ秘密鍵および対応のサーバ公開鍵に基づいて非対称暗号化を利用し、
各ＰＣＣＤのセットは、検査セッションの間に用いられる複数の暗号化キーからの個々の暗号化キーに関連付けられており、
各ＰＣＣＤのセットの前記第２のパラメータは、前記関連付けられた暗号化キーを用いて前記ＰＣＣＤのセットの前記第１のパラメータを暗号化することによって生成される、請求項３に記載の方法。
【請求項５】
検査セッションの間メッセージを暗号化するために用いられる前記複数の暗号化キー、および前記検査セッションの開始に先立って、前記検査下のネットワークに対する前記メッセージを解読するために用いられる対応の複数の解読キーを提供する工程をさらに含む、請求項４に記載の方法。
【請求項６】
前記セキュアな通信プロトコルは、セキュアソケットレイヤ（ＳＳＬ）またはトランスミッションレイヤセキュリティ（ＴＬＳ）プロトコルであり、
各ＰＣＣＤのセットにおける前記第１のパラメータはプレマスタシークレット（ＰＭＳ）であり、各ＰＣＣＤのセットにおける前記第２のパラメータは、前記ＳＳＬ／ＴＬＳプロトコルに従った暗号化されたプレマスタシークレット（ＥＰＭＳ）である、請求項３に記載の方法。
【請求項７】
前記第２のポートユニットが、前記検査下のネットワークを介して前記複数の暗号化キーからのサーバ公開鍵（ＳＰＫ）を含むｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅを、前記第１のポートユニットへ送信する工程と、
前記第１のポートユニットが、前記第１のＰＣＣＤメモリから、前記ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅからの前記ＳＰＫに関連付けられたＰＣＣＤのセットを検索する工程と、
前記第１のポートユニットが、前記検査下のネットワークを介して、前記検索されたＰＣＣＤのセットからの前記ＥＰＭＳを、前記第２のポートユニットへ送信する工程と
をさらに含む、請求項６に記載の方法。
【請求項８】
前記第２のポートユニットは、前記第２のＰＣＣＤメモリが、前記第１のポートユニットによって送信される前記ＥＰＭＳと一致するＥＰＭＳを含むＰＣＣＤのセットを含むかどうかを決定する工程をさらに含む、請求項７に記載の方法。
【請求項９】
前記第２のＰＣＣＤメモリが、前記第１のポートユニットによって送信された前記ＥＰＭＳと一致するＥＰＭＳを含むＰＣＣＤのセットを含んでいない場合、前記第２のポートユニットは従来のＳＳＬハンドシェイク方法に戻る工程をさらに含む、請求項８に記載の方法。
【請求項１０】
前記第２のＰＣＣＤメモリが、前記第１のポートユニットによって送信された前記ＥＰＭＳと一致するＥＰＭＳを含むＰＣＣＤのセットを含んでいない場合、前記第２のポートユニットは、前記第１のポートユニットと前記第２のポートユニットとの間の前記シミュレートされたセキュアな接続を終了する工程をさらに含む、請求項８に記載の方法。
【請求項１１】
前記第２のＰＣＣＤメモリが、前記第１のポートユニットによって送信された前記ＥＰＭＳと一致するＥＰＭＳを含むＰＣＣＤのセットを含む場合、

前記第２のポートユニットは、前記第１のポートユニットによって送信された前記ＥＰＭＳと一致する前記ＥＰＭＳを含む前記ＰＣＣＤのセットを検索する工程と、
前記第１のポートユニットおよび前記第２のポートユニットは、それらの各々の検索されたＰＣＣＤのセットから、前記ＰＭＳに部分的に基づいて計算されたＭＳに基づいて、対称暗号化を用い、前記シミュレートされたセキュアな接続を介して通信する工程と
をさらに含む、請求項８に記載の方法。
【請求項１２】
各ＰＣＣＤのセットは、クライアントランダム数（ＣＲＮ）、サーバランダム数（ＳＲＮ）、ならびに、ＳＳＬ／ＴＬＳプロトコルに従った前記ＣＲＮ、前記ＳＲＮ、および前記ＰＭＳから計算されるマスタシークレット（ＭＳ）をさらに含む、請求項６に記載の方法。
【請求項１３】
セキュアソケットレイヤまたはトランスポートレイヤセキュリティ（ＳＳＬ／ＴＬＳ）プロトコルに従ってセキュアなネットワーク接続を検査するためにクライアントとして動作する第１のポートユニットによって実行される方法であって、
任意のネットワーク接続を開く前に、前記第１のポートユニット内のＰＣＣＤ（プレコンピューテッド暗号データ）メモリにおける１つ以上のＰＣＣＤのセットを定義し、保存する工程であって、各ＰＣＣＤのセットは各々のサーバ公開鍵（ＳＰＫ）に関連付けられ、各ＰＣＣＤのセットは、プレマスタシークレット（ＰＭＳ）および前記関連付けられたＳＰＫを用いて、前記ＰＭＳを暗号化することによって生成される暗号化されたプレマスタシークレット（ＥＰＭＳ）を含む、工程と、
検査下のネットワークを介して第２のポートユニットからｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅを受信する工程であって、前記ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅは受信されたＳＰＫを含む、工程と、
前記ＰＣＣＤメモリに保存された前記１つ以上のＰＣＣＤのセットから前記受信されたＳＰＫに関連付けられたＰＣＣＤを選択する工程と、
前記検査下のネットワークを介して、前記選択されたＰＣＣＤのセットからの前記ＥＰＭＳを、前記第２のポートユニットへ送信する工程と
を含む、方法。
【請求項１４】
前記ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅを受信するのに先立って、
前記検査下のネットワークを介して、クライアントランダム数（ＣＲＮ）を含むｃｌｉｅｎｔ　ｈｅｌｌｏメッセージを前記第２のポートユニットに送信する工程と、
前記ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージに応答して、サーバランダム数（ＳＲＮ）を含むｓｅｒｖｅｒ　ｈｅｌｌｏメッセージを受信する工程と
をさらに含む、請求項１３に記載の方法。
【請求項１５】
前記選択されたＰＣＣＤのセットの前記ＣＲＮ、前記ＳＲＮ、および前記ＰＭＳから計算されたマスタシークレットに基づいて、対称暗号化を用い、前記検査下のネットワークを介して、前記第２のポートユニットと、シミュレートされたセキュアなメッセージを交換する工程をさらに含む、請求項１４に記載の方法。
【請求項１６】
セキュアソケットレイヤまたはトランスポートレイヤセキュリティ（ＳＳＬ／ＴＬＳ）プロトコルに従って、セキュアなネットワーク接続を検査するために、サーバとして動作する第１のポートユニットによって実行される方法であって、
任意のネットワーク接続を開く前に、前記第１のポートユニット内にＰＣＣＤ（プレコンピューテッド暗号データ）メモリにおける１つ以上のＰＣＣＤのセットを定義し、保存する工程であって、各ＰＣＣＤのセットは各々のサーバ公開鍵（ＳＰＫ）に関連付けられ、各ＰＣＣＤのセットは、プレマスタシークレット（ＰＭＳ）および前記関連付けられたＳＰＫを用いて、前記ＰＭＳを暗号化することによって生成される暗号化されたプレマス

タシークレット（ＥＰＭＳ）を含む、工程と、
検査下のネットワークを介して、第２のポートユニットからクライアントランダム数（ＣＲＮ）を含むｃｌｉｅｎｔ　ｈｅｌｌｏメッセージを受信する工程と、
前記ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージに応答して、前記検査下のネットワークを介して、前記第２のポートユニットへ、ｓｅｒｖｅｒ　ｈｅｌｌｏメッセージおよびｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅを送信する工程であって、前記ｓｅｒｖｅｒ　ｈｅｌｌｏメッセージはサーバランダム数（ＳＲＮ）を含み、前記ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅは、ＰＣＣＤメモリに保存された前記１つ以上のＰＣＣＤのセットからの選択されたＰＣＣＤのセットに関連付けられたＳＰＫを含む、工程と
を含む、方法。
【請求項１７】
前記検査下のネットワークを介して、前記第２のポートユニットから、ｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅメッセージを受信する工程と、
前記ｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅメッセージから抽出された、受信されたＥＰＭＳが、前記選択されたＰＣＣＤのセットからの前記ＥＰＭＳと一致するかどうかを決定する工程と、
前記受信されたＥＰＭＳが前記選択されたＰＣＣＤのセットからの前記ＥＰＭＳと一致しない場合、前記第１のポートユニットと前記第２のポートユニットとの間の通信を終了する工程と、
前記受信されたＥＰＭＳが前記選択されたＰＣＣＤのセットからの前記ＥＰＭＳと一致する場合、前記選択されたＰＣＣＤのセットからの、前記ＣＲＮ、前記ＳＲＮ、および前記ＰＭＳから計算されるＭＳに基づいた対称暗号化を用い、前記検査下のネットワークを介して、前記第２のポートユニットと通信する工程と
をさらに含む、請求項１６に記載の方法。
【請求項１８】
第１のコンピューティングデバイスによって実行された場合、セキュアソケットレイヤまたはトランスポートレイヤセキュリティ（ＳＳＬ／ＴＬＳ）プロトコルに従ってセキュアなネットワーク接続を検査するために、前記第１のコンピューティングデバイスをクライアントとして動作させる命令を保存する持続性コンピュータ可読保存媒体であって、
前記第１のコンピューティングデバイスは、任意のネットワーク接続を開く前に、前記第１のコンピューティングデバイスに接続されたＰＣＣＤ（プレコンピューテッド暗号データ）メモリにおける１つ以上のＰＣＣＤのセットを定義し、保存する工程であって、各ＰＣＣＤのセットは各々のサーバ公開鍵（ＳＰＫ）に関連付けられ、各ＰＣＣＤのセットは、プレマスタシークレット（ＰＭＳ）および前記関連付けられたＳＰＫを用いて、前記ＰＭＳを暗号化することによって生成される暗号化されたプレマスタシークレット（ＥＰＭＳ）を含む、工程と、
検査下のネットワークを介して第２のコンピューティングデバイスからｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅを受信する工程であって、前記ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅは受信されたＳＰＫを含む、工程と、
前記ＰＣＣＤメモリに保存された前記１つ以上のＰＣＣＤのセットから前記受信されたＳＰＫに関連付けられたＰＣＣＤを選択する工程と、
前記検査下のネットワークを介して、前記選択されたＰＣＣＤのセットからの前記ＥＰＭＳを、前記第２のコンピューティングデバイスへ送信する工程と
を含む動作を実行する、持続性コンピュータ可読保存媒体。
【請求項１９】
実行される前記動作は、
前記ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅを受信するのに先立って、前記検査下のネットワークを介して、クライアントランダム数（ＣＲＮ）を含むｃｌｉｅｎｔ　ｈｅｌｌｏメッセージを前記第２のコンピューティングデバイスに送信する工程と、
前記ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージに応答して、サーバランダム数（ＳＲＮ）を

含むｓｅｒｖｅｒ　ｈｅｌｌｏメッセージを受信する工程と
をさらに含む、請求項１８に記載の持続性コンピュータ可読保存媒体。
【請求項２０】
実行される前記動作は、前記選択されたＰＣＣＤのセットの前記ＣＲＮ、前記ＳＲＮ、および前記ＰＭＳから計算されたマスタシークレットに基づいて、対称暗号化を用い、前記検査下のネットワークを介して、前記第２のコンピューティングデバイスと、シミュレートされたセキュアなメッセージを交換する工程をさらに含む、請求項１９に記載の持続性コンピュータ可読保存媒体。
【請求項２１】
第１のコンピューティングデバイスによって実行された場合、セキュアソケットレイヤまたはトランスポートレイヤセキュリティ（ＳＳＬ／ＴＬＳ）プロトコルに従ってセキュアなネットワーク接続を検査するために、前記第１のコンピューティングデバイスをサーバとして動作させる命令を保存する持続性コンピュータ可読保存媒体であって、
前記第１のコンピューティングデバイスは、任意のネットワーク接続を開く前に、前記第１のコンピューティングデバイスに接続されたＰＣＣＤ（プレコンピューテッド暗号データ）メモリにおける１つ以上のＰＣＣＤのセットを定義し、保存する工程であって、各ＰＣＣＤのセットは各々のサーバ公開鍵（ＳＰＫ）に関連付けられ、各ＰＣＣＤのセットは、プレマスタシークレット（ＰＭＳ）および前記関連付けられたＳＰＫを用いて、前記ＰＭＳを暗号化することによって生成される暗号化されたプレマスタシークレット（ＥＰＭＳ）を含む、工程と、
検査下のネットワークを介して、第２のコンピューティングデバイスからクライアントランダム数（ＣＲＮ）を含むｃｌｉｅｎｔ　ｈｅｌｌｏメッセージを受信する工程と、
前記ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージに応答して、前記検査下のネットワークを介して、前記第２のコンピューティングデバイスへ、ｓｅｒｖｅｒ　ｈｅｌｌｏメッセージおよびｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅを送信する工程であって、前記ｓｅｒｖｅｒ　ｈｅｌｌｏメッセージはサーバランダム数（ＳＲＮ）を含み、前記ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅは、ＰＣＣＤメモリに保存された前記１つ以上のＰＣＣＤのセットからの選択されたＰＣＣＤのセットに関連付けられたＳＰＫを含む、工程と
を含む動作を実行する、持続性コンピュータ可読保存媒体。
【請求項２２】
実行される動作が、
前記検査下のネットワークを介して、前記第２のコンピューティングデバイスから、ｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅメッセージを受信する工程と、
前記ｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅメッセージから抽出された、受信されたＥＰＭＳが、前記選択されたＰＣＣＤのセットからの前記ＥＰＭＳと一致するかどうかを決定する工程と、前記受信されたＥＰＭＳが前記選択されたＰＣＣＤのセットからの前記ＥＰＭＳと一致しない場合、前記第２のコンピューティングデバイスとの通信を終了する工程と、
前記受信されたＥＰＭＳが前記選択されたＰＣＣＤのセットからの前記ＥＰＭＳと一致する場合、前記選択されたＰＣＣＤのセットからの、前記ＣＲＮ、前記ＳＲＮ、および前記ＰＭＳから計算されるマスタシークレットに基づいた対称暗号化を用い、前記検査下のネットワークを介して、前記第２のコンピューティングデバイスと通信する工程と
をさらに含む、請求項２１に記載の持続性コンピュータ可読保存媒体。
【発明の詳細な説明】
【技術分野】
【０００１】
（著作権およびトレードドレスについての通知）
本特許文献の開示の一部は著作権保護に対象となるマテリアルを含む。本特許文献は、保有者のトレードドレスである、またはトレードドレスとなり得る事柄を示し、および／または記載する場合がある。著作権およびトレードドレスの保有者は、いかなる者であっ

ても米国特許商標局の書類または記録の通りに本特許開示を複製する限りで、異議を申し立てるものではないが、その他の場合には、いかなる場合であっても全ての著作権およびトレードドレスの権利を保留するものである。

【０００２】

本開示は、ネットワークまたはネットワークデバイスを検査するためのトラフィックを受信および処理することに関する。

【背景技術】

【０００３】

多くのタイプの通信ネットワークにおいて、送信される各メッセージは固定長または可変長の部分へと分割される。各々の部分は、情報のパケット、フレーム、セル、データグラム、データ単位、または他の情報単位として呼ばれる場合があり、それらの全ては、本明細書において、パケットとして参照される。

【０００４】

各パケットは、通常、パケットのペイロードと呼ばれる元のメッセージの一部を含む。パケットのペイロードはデータを含んでよく、あるいは、音声情報またはビデオ情報を含んでもよい。パケットのペイロードはまた、ネットワーク管理および制御情報を含んでもよい。さらに、各パケットは、通常、パケットヘッダと呼ばれる識別およびルーティング情報を含む。パケットはネットワークを通じて複数のスイッチまたはノードを介して個々に送信される。パケットは、目的とするデバイスまたはエンドユーザにメッセージが配信される前に、パケットヘッダに含まれる情報を用いて最終的な送り先にてメッセージに再構築される。受信側において、その再構築されたメッセージは、ユーザの装置に適合するフォーマットでエンドユーザに送られる。

【０００５】

メッセージをパケットとして送信する通信ネットワークは、パケット交換ネットワークと呼ばれる。パケット交換ネットワークは、通常、ハブまたはノードで交差する送信パスのメッシュを含む。ノードの少なくとも一部は、ノードに到着するパケットを受け取り、適切な発信パスに沿ってパケットを再送信するスイッチングデバイスまたはルータを備えてよい。パケット交換ネットワークは、業界標準のプロトコルのレイヤ別の構造によって制御される。その構造のレイヤ１、２、３、４、およびレイヤ７は各々、物理レイヤ、データリンクレイヤ、ネットワークレイヤ、トランスポートレイヤ、およびアプリケーションレイヤである。

【０００６】

レイヤ１のプロトコルは、ネットワークのノード間での物理的な（電気的、光学的、または無線の）インターフェースを規定する。レイヤ１のプロトコルは、イーサネット（登録商標）の物理的コンフィグレーション、ＳＯＮＥＴ（同期光学的ネットワーク）、および他の光学接続プロトコル、ならびに、Ｗｉ－Ｆｉ（登録商標）等の様々な無線プロトコルを含む。

【０００７】

レイヤ２のプロトコルは、データがネットワークのノード間を論理的に転送される方法を制御する。レイヤ２のプロトコルは、イーサネット（登録商標）、ＡＴＭ（非同期転送モード）、フレームリレー、およびＰＰＰ（ポイント・ツー・ポイント・プロトコル）を含む。

【０００８】

レイヤ３のプロトコルは、ネットワークの複数のノードを接続するパスに沿ってソースから送り先へパケットがルーティングされる方法を制御する。主要なレイヤ３のプロトコルは周知のインターネットプロトコルバージョン４（ＩＰｖ４）およびバージョン６（ＩＰｖ６）である。パケット交換ネットワークは、イーサネット（登録商標）、ＡＴＭ、ＦＲ、および／またはＰＰＰのレイヤ２のプロトコルの混合体を用いてＩＰパケットをルーティングする必要がある場合もある。ネットワークのノードの少なくとも一部は、各パケット内に含まれるネットワークレイヤヘッダから、送り先アドレスを抽出するルータを備

えてもよい。ルータは次いで、パケットが再送信されるべきルートまたはパスを決定するために送り先アドレスを用いる。通常のパケットは複数のルータを通過してよく、それらのルータの各々は送り先アドレスを抽出する行為およびそのパケットが再送信されるべきルートまたはパスを決定する行為を繰り返す。

【０００９】

レイヤ４のプロトコルは、ネットワーク中でエンド・ツー・エンドのメッセージ配信を制御する。特に、通信制御プロトコル（ＴＣＰ）は、必要に応じて、順次的な承認および再伝送のシステムを用いてパケットストリームの信頼性のある伝送を提供する。ＴＣＰは、２つのデバイスがネットワークを介した仮想接続を開くためにメッセージを交換するコネクション型のプロトコルである。接続がいったん開くと、接続されたデバイス間で双方向通信が生じ得る。接続はそれらのデバイスの一方によって切断されるまで存在し得る。接続を開くことおよび切断の両方は、特定のメッセージが２つのデバイス間で交換されるいくつかのステップを必要とする。予定されていた応答が所定の時間期間に一方のデバイスによって受信されない場合には、接続は切断されてよく、これは通常、「タイムアウト」と呼ばれる。ＴＣＰ接続は、各々のデバイスが、接続の状態（開いているのか、確立されているのか、切断されているのか）、どのようなデータが送られているのか、そしてどのような送られたデータが承認されているのかを記載した情報を維持する必要があるゆえ、「ステートフル」とみなされる。

【００１０】

レイヤ７プロトコル、すなわちアプリケーションレイヤプロトコルとしては、ハイパーテキスト転送プロトコル（ＨＴＴＰ）、シンプルメール転送プロトコル（ＳＭＴＰ）、ファイル転送プロトコル（ＦＴＰ）、ポスト・オフィス・プロトコル（ＰＯＰ３）、および他のプロトコルが挙げられる。これらのレイヤ７プロトコルは通常、ＴＣＰプロトコルを用いて、ネットワークを介して通信する。一部の状況においては、レイヤ７プロトコルによって通信された情報は暗号化されてよい。通常、情報は、レイヤ７プロトコルとＴＣＰプロトコルとの間で（実質的にはレイヤ５で）動作するセキュア（セキュリティ）ソケットレイヤ（ＳＳＬ）またはトランスポート（トランスミッション）レイヤセキュリティ（ＴＬＳ）プロトコルを用いて暗号化されてよい。

【００１１】

従来、ルータおよびスイッチ等のネットワークデバイスは、レイヤ２で主に動作する、すなわち、ネットワークデバイスは、各イーサネット（登録商標）のパケットのレイヤ２のヘッダ内の情報に基づいて、ネットワークを介してパケットをルーティングする。ネットワークデバイスは一般にパケットのコンテンツを無視する。しかしながら、最近のネットワークデバイスはＩＰパケットのコンテンツの中を見るために、レイヤ２のヘッダだけで終わらない場合がある。ネットワークデバイスは、層４のヘッダを検査することによって、浅いパケット検査（ｓｈａｌｌｏｗ　ｐａｃｋｅｔ　ｉｎｓｐｅｃｔｉｏｎ）（ステートフルパケットの検査とも呼ばれる）を行う場合がある。一部のネットワークデバイスは、各パケットのペイロードのコンテンツの一部または全てを検査することによって、深いパケット検査（ＤＰＩ：ｄｅｅｐ　ｐａｃｋｅｔ　ｉｎｓｐｅｃｔｉｏｎ）を行う。深いパケット検査（ＤＰＩ）は、ウィルスおよび他の悪意のあるコードの伝搬を防ぎ、スパムにフィルターをかけ、プライベートネットワークへの権限のない侵入を防ぎ、一部の国ではインターネットのトラフィックを検閲し、および他の目的のために実行され得る。

【００１２】

パケット交換通信ネットワーク、またはパケット交換通信ネットワーク内に含まれるデバイスを検査するために、多数のパケットを含む検査トラフィックが生成され、１つ以上のポートにおいてネットワークに送信され、かつ異なるポートにて受信されてもよい。これに関連して、用語「ポート」とは、ネットワークと、そのネットワークを検査するために用いられる装置との間の通信接続のことをいう。用語「ポートユニット」とは、ポートにおいて、ネットワークに接続するネットワーク検査装置内にあるモジュールのことをいう。受信された検査トラフィックは、ネットワークの性能を測定するために分析されてよ

い。ネットワークに接続された各ポートユニットは、検査トラフィックの送り元（ｓｏｕｒｃｅ）および検査トラフィックのための宛先の両方であってもよい。各ポートユニットは、複数の論理送り元または宛先アドレスをエミュレートしてよい。

【００１３】

ネットワーク、あるいはサーバ、サーバロードバランサ（負荷分散装置）、またはＤＰＩを実行する任意のデバイス等のネットワークデバイスを検査するために、実際の接続を確立し、かつ検査下のネットワークを介して実際のデータを送信する必要がある場合がある。暗号化されたパケットの少なくとも部分的なＤＰＩを実行するネットワークまたはネットワーク装置を検査するために、検査下のネットワークを介して多数のＳＳＬ／ＴＬＳを確立する必要がある場合がある。

【００１４】

図１は、鍵交換のために、ＲＳＡを用い、ＳＳＬプロトコルに従った接続を確立および利用するためのプロセス１００の簡略化したフローチャートを示す。プロセス１００は、本特許出願において、ＳＳＬ「ハンドシェイク」プロセスと呼ばれる。プロセス１００は通常、ネットワークを介して通信するクライアント・コンピューティングデバイスおよびサーバ・コンピューティングデバイスによって実行される。プロセス１００は、クライアントデバイスがＳＳＬ接続を開くことを決定した場合、１０５において始まり、通常は、クライアントおよびサーバデバイスの相互承認により、１９０で終了する。プロセス１００は、通常ＳＳＬハンドシェイクと呼ばれるクライアントデバイスとサーバデバイスとの間でのメッセージの交換を含んでよい。

【００１５】

１１０において、クライアントデバイスは、ＳＳＬプロトコルにおいて、「クライアントランダム数」（ＣＲＮ）と呼ばれる第１のランダム数を生成する。クライアントデバイスは、次いで、ＳＳＬプロトコルにおいて、サーバデバイスへのＣＲＮを含む、「ｃｌｉｅｎｔ　ｈｅｌｌｏ」メッセージと呼ばれるメッセージ１１５を送信する。このｃｌｉｅｎｔ　ｈｅｌｌｏメッセージは、クライアントによってサポートされた圧縮プロトコルおよび暗号化プロトコルのリスト等の他の情報を含んでよい。

【００１６】

ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージ１１５を受信した後、１２０において、サーバデバイスは、ＳＳＬプロトコルにおいて「サーバランダム数」（ＳＲＮ）と呼ばれる第２のランダム数を生成する。サーバデバイスは、次いで、ＳＳＬプロトコルにおいて、クライアントデバイスへのＳＲＮを含む、「ｓｅｒｖｅｒ　ｈｅｌｌｏ」メッセージと呼ばれるメッセージ１２５を送信し得る。ｓｅｒｖｅｒ　ｈｅｌｌｏメッセージは、いったんＳＳＬ接続が確立されると用いられる圧縮プロトコルおよび暗号化プロトコル（ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージ１１５内に提供されたリストから）の選択等の他の情報を含んでよい。

【００１７】

サーバデバイスは通常、クライアントデバイスに、ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ１２７も送信する。ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ１２７はクライアントがサーバを認証するのに必要とされる情報を含んでよい。ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ１２７は、サーバデバイスに送信されるデータを暗号化するために、クライアントデバイスによって用いられ得るサーバ公開鍵を含んでよい。

【００１８】

ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅを受信し認証した後、クライアントデバイスは、「プリマスタシークレット（ＰＭＳ：ｐｒｅ－ｍａｓｔｅｒ　ｓｅｃｒｅｔ）と呼ばれる第３のランダム数を１３０にて生成する。１４０にて、クライアントデバイスは、ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ１２７から、サーバ公開鍵を用いて、ＰＭＳを暗号化する。暗号化されたＰＭＳ（ＥＰＭＳ）は、次いで、「ｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅ」メッセージと通常呼ばれるメッセージ１４５において、サーバデバイスに送信される。ＥＰＭＳは、１５０において、サーバ秘密鍵を用いてサーバデバイスによって解

読される。ＰＭＳの暗号化は非対称とみなされる。なぜならば、ＰＭＳを暗号化および解読するために用いられる公開鍵および秘密鍵は異なるからである。

【００１９】

１６０および１６５において、クライアントデバイスおよびサーバデバイスは、各々、ＣＲＮ、ＳＲＮ、およびＰＭＳから、マスタシークレット（ＭＳ）を計算する。クライアントデバイスおよびサーバデバイスは同じＭＳを計算し、このＭＳは次いで、１７０および１７５において、対称の暗号化アルゴリズムを有して用いられて、ＳＳＬ接続を介した今後の通信を暗号化および解読する。

【図面の簡単な説明】

【００２０】

【図１】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）接続を確立するために必要とされる暗号作成データを交換するためのプロセスのフローチャートである。

【図２】ネットワーク環境のブロック図である。

【図３】ポートユニットのブロック図である。

【図４】深いパケット検査（ＤＰＩ）を実行するネットワークデバイスを検査するための検査セットアップのブロック図である。

【図５】所定の暗号作成データのグラフィック図である。

【図６】ＤＰＩを実行するネットワークを検査するためのプロセスのフローチャートである。

【図７】ＤＰＩを実行するネットワークを検査するための別のプロセスのフローチャートである。

【発明を実施するための形態】

【００２１】

本記載全体を通じて、ブロック図に表される要素は、３桁の参照番号が割り当てられ、最上位桁は図面の番号であり、要素が導入され、下位２つの桁は要素に特定されるものである。ブロック図に関連して記載されない要素は、同じ参照番号を有する前述された要素として同じ特徴および機能を有するものとみなされてよい。

【００２２】

（装置の記載）

図２はネットワーク環境のブロック図を示す。ネットワーク環境は、ネットワーク検査装置２００、ネットワーク２９０、および複数のネットワークデバイス２９２を備えてよい。

【００２３】

ネットワーク検査装置２００は、ネットワーク検査デバイス、パフォーマンスアナライザ、適合性確認システム、ネットワークアナライザ、またはネットワーク管理システムであってよい。ネットワーク検査装置２００は、１つ以上のネットワークカード２０６、およびシャーシ２０２内に含まれるかまたは包囲されたバックプレーン２０４を備えてよい。シャーシ２０２は、ネットワーク検査装置を含むのに適した固定型または可搬型のシャーシ、キャビネット、または筐体であってよい。ネットワーク検査装置２００は図２に示すように一体化されたユニットであってよい。あるいは、ネットワーク検査装置２００は、トラフィックの生成および／または分析を提供するように協動する複数の別個のユニットを備えてよい。ネットワーク検査装置２００およびネットワークカード２０６は、例えば様々なイーサネット（登録商標）およびファイバーチャネル標準等の１つ以上の周知の規格またはプロトコルをサポートしてよく、かつ専用のプロトコルもサポートしてよい。

【００２４】

ネットワークカード２０６は、１つ以上のフィールドプログラマブルゲートアレイ（ＦＰＧＡ）、特定用途向け集積回路（ＡＳＩＣ）、プログラマブル論理デバイス（ＰＬＤ）、プログラマブル論理アレイ（ＰＬＡ）、プロセッサおよび他の種類のデバイスを含んでもよい。さらに、ネットワークカード２０６はソフトウェアおよび／またはファームウェ

アを含んでもよい。用語、ネットワークカードは、ラインカード、テストカード、分析カード、ネットワークラインカード、ロードモジュール、インターフェースカード、ネットワークインターフェースカード、データインターフェースカード、パケットエンジンカード、サービスカード、スマートカード、スイッチカード、リレーアクセスカード等を含む。用語、ネットワークカードはまた、複数のプリント回路基板を含み得るモジュール、ユニット、およびアセンブリを含む。各ネットワークカード２０６は１つ以上のポートユニット２１０を含み得る。各ポートユニット２１０は、１つ以上のポートを介してネットワーク２９０に接続し得る。各ポートユニット２１０は、通信媒体２９５を介してネットワーク２９０に接続されてよく、この通信媒体２９５は、ワイヤ、光ファイバ、無線リンク、または他の通信媒体であってよい。各ネットワークカード２０６は、単一の通信プロトコルをサポートしてよく、複数の関連のプロトコルをサポートしてよく、または、複数の関連のないプロトコルをサポートしてもよい。ネットワークカード２０６は、ネットワーク検査装置２００内に恒久的に設置されていてもよく、または着脱自在であってもよい。

【００２５】

バックプレーン２０４は、ネットワークカード２０６のために、バスまたは通信媒体として機能してよい。バックプレーン２０４はまた、電極をネットワークカード２０６に提供し得る。

【００２６】

ネットワークデバイス２９２は、ネットワーク２９０を介しての通信を可能にする任意のデバイスであってよい。ネットワークデバイス２９２は、ワークステーション、パーソナル・コンピュータ、サーバ、ポータブル・コンピュータ、携帯情報端末（ＰＤＡ）、コンピューティング・タブレット、セル式電話／携帯電話、イーメール用装置等のコンピューティング・デバイス、プリンタ、スキャナ、ファクシミリ装置等の周辺機器、ネットワーク接続ストレージ（ＮＡＳ）およびストレージ・エリア・ネットワーク（ＳＡＮ）のデバイス等のディスクドライブを含むネットワーク対応のストレージデバイス、ロードバランサ（負荷分散装置）、ルータ、リレー、ハブ、スイッチ、ブリッジ、およびマルチプレクサ等のネットワーキング・デバイスであってよい。さらに、ネットワークデバイス２９２は、ネットワークを通じて通信することができる家庭電化器具、アラームシステムおよび他の任意のデバイスまたはシステムを含んでもよい。

【００２７】

ネットワーク２９０は、ローカルエリアネットワーク（ＬＡＮ）、ワイドエリアネットワーク（ＷＡＮ）、ストレージエリアネットワーク（ＳＡＮ）、有線、無線、またはこれらの組み合わせであってもよく、インターネットを含んでもよく、またはインターネットであってもよい。ネットワーク２９０上の通信は、情報のフレーム、セル、データグラム、パケットまたは他の単位を含む様々な形態をとってもよく、本明細書においては、それらの全てをパケットと称する。ネットワーク検査装置２００およびネットワークデバイス２９２は、同時に相互に通信してもよく、ネットワーク検査装置２００と所与のネットワークデバイス２９５との間には、複数の論理的通信経路があってもよい。ネットワークそのものは、移動するデータのための多数の物理的経路および論理的経路を提供する多数のノードから成ってもよい。

【００２８】

ここで図３を参照し、例示的なポートユニット３１０は、ポート中央演算装ユニット（ＣＰＵ）３２０と、トラフィックジェネレータユニット３６０と、トラフィックレシーバユニット３８０と、ポートユニット３１０を被検査ネットワーク３９０に接続するネットワークインターフェースユニット３７０とを備えてもよい。ポートユニット３１０は、ネットワークカード（例えばネットワークカード２０６）のすべてまたは一部であってもよい。

【００２９】

ポートＣＰＵ３２０は、本明細書に記載される機能および特徴を提供するための、プロセッサ、プロセッサに接続されたメモリ、および様々な特殊化された装置、回路、ソフト

ウェアおよびインターフェースを含んでもよい。プロセス、機能および特徴は、全体的にあるいは部分的に、プロセッサ上で動作するソフトウェアにおいて実現されてもよく、ファームウェア、アプリケーションプログラム、アプレット（例えばＪａｖａ（登録商標）アプレット）、ブラウザプラグイン、ＣＯＭオブジェクト、ダイナミックリンクライブラリ（ＤＬＬ）、スクリプト、１つ以上のサブルーチン、またはオペレーティングシステムのコンポーネントまたはサービスという形をとってもよい。ハードウェアおよびソフトウェアおよびそれらの機能は、一部の機能がプロセッサによって実行され、他の機能が他の装置によって実行されるように、分散型であってもよい。

【００３０】

ポートＣＰＵ３２０は、検査アドミニストレータ３０５と通信してもよい。検査アドミニストレータ３０５は、ネットワーク検査装置２００の内部に収容されるコンピューティングデバイスまたは外部のコンピューティングデバイスであってもよい。検査アドミニストレータ３０５は、ポートユニットがネットワーク３９０の検査に関与するために必要とされる命令およびデータを、ポートＣＰＵ３２０に提供してもよい。検査アドミニストレータ３０５から受信される命令およびデータは、例えば、ポートユニット３１０によって生成されるパケットストリームの定義、およびポートユニット３１０によって蓄積および報告され得るパフォーマンス統計の定義を含んでもよい。

【００３１】

ポートＣＰＵ３２０は、トラフィックジェネレータユニット３６０にストリーム形成データ３１２を提供して、複数のストリームを形成させ得る。ストリーム形成データ３１２は、例えば、パケットのタイプ、送信の周波数、パケット内部の固定内容フィールドおよび可変内容フィールドの定義、および各パケットストリームのための他の情報を含んでもよい。トラフィックジェネレータユニット３６０は、次いで、ストリーム形成データ３１２に従って複数のストリームを生成してよい。複数のストリームは、発信検査トラフィック３６５を形成するためにインターリーブされてよい。各ストリームは一連のパケットを含んでよい。各ストリーム内のパケットは同様の一般的なタイプであってよいが、長さおよびコンテンツが異なっていてもよい。

【００３２】

ネットワークインターフェースユニット３７０は、トラフィックジェネレータユニット３６０からの発信検査トラフィック３６５を、ワイヤ、光ファイバ、無線リンク、または他の通信リンクであり得るリンク３９５を介して、被検査ネットワーク３９０へと検査トラフィックを送信するように要求される、電気的、光学的、または無線による信号フォーマットに変換してよく同様に、ネットワークインターフェースユニット３７０は、ネットワークからリンク３９５を介して電気的、光学的、または無線による信号を受信してよく、かつ、トラフィックレシーバユニット３８０に対して利用可能なフォーマットに、着信する検査トラフィック３７５に受信される信号を変換してよい。

【００３３】

トラフィックレシーバユニット３８０は、ネットワークインターフェースユニット３７０から着信検査トラフィック３７５を受信してよい。トラフィックレシーバユニット３８０は、各受信パケットが特定のフローのメンバーであるかを決定し得、また、ポートＣＰＵ３２０から提供された検査命令３１４に従って各フローに関する検査統計を蓄積し得る。蓄積された検査統計は、例えば、受信パケットの合計数、順序通りでなく受信されたパケットの数、エラーを有する受信パケットの数、最大、平均および最小の伝搬遅延、および各フローの他の統計を含んでもよい。トラフィックレシーバユニット３８０はまた、検査命令３１４に含まれる取得基準に従って、選択されたパケットを取得および格納してもよい。トラフィックレシーバユニット３８０は、検査セッションの最中または後におけるさらなる分析のために、検査統計および／または取得パケット３８４を、検査命令３１４に従って、ポートＣＰＵ３２０に提供してもよい。

【００３４】

発信検査トラフィック３６５および着信検査トラフィック３７５は、主にステートレス

であってもよい。すなわち、発信検査トラフィック３６５の十分な部分は、応答を予期することなくトラフィックジェネレータ３６０によって生成されてもよく、着信検査トラフィック３７５は、応答を意図することなくトラフィックレシーバ３８０によって受信されてもよい。ステートレスのトラフィックの送受信は、被検査ネットワーク３９０のレイヤ２およびレイヤ３の検査を行うのに十分であり得る。しかしながら、サーバ、サーバロードバランサ、またはＤＰＩを実行する任意のデバイス等のネットワークデバイスのレイヤ４（またはそれよりも高いレイヤ）のパフォーマンスを検査するために、多数のＴＣＰ接続が、検査セッションの最中において、ポートユニット３１０と被検査ネットワーク３９０との間に必要とされる場合がある。暗号化された通信を処理または検査することができるネットワークまたはネットワークデバイスを検査するために、ＳＳＬ接続等の多数のセキュアな接続が必要とされ得る。

【００３５】

ＳＳＬ接続を確立および使用するために、ポートＣＰＵ３２０は暗号化されたコンテンツを含む適切なＴＣＰパケットを準備してよく、かつＴＣＰパケット３１６をトラフィックジェネレータ３６０に提供してもよい。トラフィックジェネレータ３６０はＴＣＰパケットを発信検査トラフィック３６５に挿入し得る。トラフィックレシーバ３８０は、受信されたステートレストラフィックから受信されたＴＣＰパケットを分離し、かつ解読および処理のためにその受信されたＴＣＰパケット３８２をポートＣＰＵ３２０に送信し得る。

【００３６】

ネットワークまたはネットワークデバイスが検査されている場合、図４に示すように、図１のプロセス１００におけるクライアントデバイスおよびサーバデバイスの役割は、ネットワーク検査装置４００内で、クライアントポートユニット４１０およびサーバポートユニット４１５によって満たされてよい。クライアントポートユニット４１０およびサーバポートユニット４１５はネットワークデバイス４９２と通信してよく、ネットワークデバイス４９２はＤＰＩを実行するデバイスであってよい。ネットワークデバイス４９２が独立して検査されている場合、クライアントポートユニット４１０およびサーバポートユニット４１５は通信メディア４９５、４９７を介してネットワークデバイス４９２に直接に接続してよい。ネットワークデバイス４９２が検査下のネットワークの一部である場合、クライアントポートユニット４１０およびサーバポートユニット４１５は、通信メディア４９５、４９７、およびネットワーク４９０を介してネットワークデバイスに接続し得る。

【００３７】

ネットワークデバイスを検査する場合、ＳＳＬ接続が確立できるレートは、ポートユニット４１０、４１５内で利用可能な処理力によって制限され得る。特に、図１の１５０において、サーバ秘密鍵を用いてＥＰＭＳを解読するには拡張処理が必要とされる。ＳＳＬ接続を確立するのに必要とされる処理時間の約９０％は１５０における解読作業に用いられる。このように、サーバポートユニット４１５によって実行される動作は、クライアントポートユニット４１０によって実行される動作よりも、より多くの処理時間を必要とする場合があり、その結果、クライアントポートユニット４１０は、サーバポートユニット４１５ができるより多くの、ユニット時間毎の接続を確立することができる。

【００３８】

深いパケット検査（ＤＰＩ）を実行するネットワークデバイスのパフォーマンスを検査する場合、ＳＳＬ接続はＳＳＬプロトコルに適合することが必要である。シミュレートされたセキュアな接続のコンテンツは、ネットワークデバイスの能力を検査するために、深いパケット検査およびセキュアなネットワークトラフィックの認証を実行するために、暗号化される必要がある。しかしながら、ネットワークトラフィックはネットワークデバイス４９２に対してセキュアにみえる必要があるが、シミュレートされたセキュアなＳＳＬ接続によって行われるデータが実際にセキュアである必要はない。従って、様々なランダム数生成およびＳＳＬプロトコルの暗号化／解読作業（図１に示すように）は、ネットワ

ークデバイスを検査する間、各ＳＳＬ接続を開くよう実際に実行される必要はない。各ＳＳＬ接続を開くように、ランダム数生成およびＳＳＬプロトコルの暗号化／解読作業を実行する別の方法として、クライアントポートユニット４１０およびサーバポートユニット４１５は、プレコンピューテッド（プレカルキュレーテッド）暗号データ（ＰＣＣＤ：ｐｒｅ－ｃｏｍｐｕｔｅｄ（ｐｒｅ－ｃａｌｃｕｌａｔｅｄ） ｃｒｙｐｔｏｇｒａｐｈｙ ｄａｔａ）を保存するために、各々のメモリ４３０および４３５を含んでよい。ＰＣＣＤは、任意の解読を実行せず、かつ、場合によっては任意の暗号化またはランダム数生成を実行することなく、クライアントポートユニットとサーバポートユニットとの間の、シミュレートされたセキュアな接続を開くために用いられてよい。本出願において、「シミュレートされたセキュアな接続」とは、接続が通っているネットワークデバイスに対してセキュアであるように見えるが、実際にはセキュアではない、接続である。

【００３９】

ここで図５を参照すると、ＰＣＣＤメモリ５００は、１つ以上のＰＣＣＤセット、５１０－１から５１０－Ｎ（ここでＮは整数）を含んでよい。各ＰＣＣＤセット５１０－１から５１０－Ｎは、ＣＲＮ、ＳＲＮ、サーバ公開鍵（ＳＰＫ）、ＰＭＳ、およびＥＰＭＳ、ならびにＭＳのうちの１つ以上を含んでよい。各ＰＣＣＤセット５１０－１から５１０－Ｎは、ＳＳＬプロトコルと一致していてよい。特に、各ＰＣＣＤセット５１０－１から５１０－Ｎ内では、ＣＲＮ、ＳＲＮ、ＰＭＳはランダム数であってよく、ＥＰＭＳは関連付けられたＳＰＫも用いてＰＭＳから計算されてよく、ＭＳは、ＳＳＬプロトコルに従ってＣＲＮ、ＳＲＮ、およびＰＭＳから計算されてよい。ＰＣＣＤメモリ５００におけるＰＣＣＤセットは、例えば、図４における検査アドミニストレータ４０５等のコンピューティングデバイスによって、検査セッションの開始に先立って計算されてよい。検査セッションの開始に先立ったＰＣＣＤセットの計算は、ポートユニット３１０等の、ポートユニット内のポートＣＰＵによって実行されてよく、または、検査アドミニストレータのコンピューティングデバイスと１つ以上のポートユニットとの間において配られていてもよい。

【００４０】

再び図４を参照すると、１つ以上のＰＣＣＤセットは、例えば、検査アドミニストレータ４０５によって定義され、検査セッションの開始に先立って、ＰＣＣＤメモリ４３０、４３５にアップロードされてよい。２つのみのポートユニット４１０、４１５が図４に示されてるが、ネットワーク検査装置は、３つ以上のポートユニットを有してよく、それらの各々が、検査セッションの間、クライアント、サーバ、またはそれら両方として動作するＳＳＬ接続を確立してよい。このように、ネットワーク検査装置４００内のポートユニットの一部または全ては、ＰＣＣＤセットを保存するために、各々のＰＣＣＤメモリを含んでよい。ＰＣＣＤセットの定義および計算は、検査アドミニストレータ４０５と、ポートユニットを有する１つ以上のプロセッサとの間で配られていてもよい。

【００４１】

（処理の記載）

図６は、ネットワークデバイスを検査するために、シミュレートされたＳＳＬ接続を確立して用いるためのプロセス６００のフローチャートを示す。シミュレートされたＳＳＬ接続は、任意の実際の暗号化および解読処理なしに、従来のＳＳＬハンドシェイクプロトコルをシミュレートする一連のメッセージを用いて確立されてよい。シミュレートされたＳＳＬ接続を介して送信されたデータは暗号化されてもよいが、実際にセキュアでなくともよい。プロセス６００は、クライアント６１０として動作する第１のポートユニットおよびサーバ６１５として動作する第２のポートユニットによって実行されてもよい。クライアント６１０およびサーバ６１５は、検査下のネットワークデバイス（図示せず）を介して複数のメッセージを変更し得る。各々のＳＳＬ接続について、プロセス６００は、クライアント６１０がＳＳＬ接続を開くことを決定するか、またはそのように命令された場合に、６０５において開始してよい。プロセス６００は、通常、クライアント６１０およびサーバ６１５の相互の認証によって、６９０において終了してよい。プロセス６００の複数のインスタンスは、複数のＳＳＬ接続を確立するように、連続して、および／または

同時に、実行されてよい。プロセス６００は複数のポートユニットによって同時に実行されてよく、それらの各々は、多数のＳＳＬ接続を確立するために、クライアントとして、またはサーバとして、あるいはそれら両方として動作する。

【００４２】

６９５において、検査セッションのための準備の間および任意のＳＳＬ接続を確立するのに先立って、１つ以上のプレコンピューテッド暗号データ（ＰＣＣＤ）のセットが計算されてよく、かつ、クライアント６１０およびサーバ６１５におけるＰＣＣＤメモリに、および、存在する場合にはさらなるポートユニットにアップロードされてよい。例えば、各ＰＣＣＤセットは、図５に示すように、ＳＳＬプロトコルに従って、ＣＲＮ、ＳＲＮ、ＰＭＳ、ＥＰＭＳ、およびＭＳの一部または全てに対する値を含んでよい。各ＰＣＣＤセットは、特定のサーバ公開鍵（ＳＰＫ）を含んでもよく、またはそれに関連付けられていてもよい。６９５での動作はプロセス６００の一部ではなく、確立されるＳＳＬ接続の数とは関係なく、検査セッション毎に一度のみ実行されてよい。ＰＣＣＤセットは選択的にポートユニットに提供されてもよく、その結果、各ポートユニットはそれが検査セッション中に必要とするＰＣＣＤセットのみを受信し、または、一般的には（ｇｌｏｂａｌｌｙ）、各ポートユニットは６９５で確立されたＰＣＣＤセットの全てを受信する。また、６９５において、検査セッションの間に用いられる全てのＳＰＫは、各ＳＰＫに対応するサーバ秘密鍵、すなわち、対応のＳＰＫを用いて暗号化された情報を解読するために用いられることができるサーバ秘密鍵と共に、検査下のネットワークに提供されてよい。

【００４３】

６２０において、クライアント６１０は、メモリ、例えば図５のＰＣＣＤメモリから、ＰＣＣＤのセットを検索することによって、シミュレートされたＳＳＬ接続を開始し得る。ＰＣＣＤメモリが単一のＰＣＣＤセットを含む場合、クライアントによって開始された全てのシミュレートされたＳＳＬ接続は同じ暗号データを用いてもよい。ＰＣＣＤメモリが複数のＰＣＣＤセットを含む場合、ＰＣＣＤセットのうちの１つは、ランダムに、または順番に、あるいは一部の他の技術によって、６２０において選択されてもよい。クライアント６１０は、検査セッションのための命令に従って、特定のＳＰＫを含むか、それに関連付けられたＰＣＣＤセットを選択してよい。クライアント６１０は、次いで、検索されたＰＣＣＤセットからサーバ６１５へ、ＣＲＮを含むｃｌｉｅｎｔ　ｈｅｌｌｏメッセージ６２５を送信してよい。ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージ６２５は、クライアント６１０によってサポートされた圧縮プロトコルおよび暗号化プロトコルのリスト等の他の情報を含んでもよい。確立されているシミュレートされたＳＳＬ接続を介して送られるその後のパケットについての深いパケット検査（ＤＰＩ）を可能にするために、検査下のネットワークは、ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージ６２５から、ＣＲＮおよび他の情報を抽出してよい。

【００４４】

６３０において、ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージを受信した後、サーバ６１５は、受信されたメッセージから受信されたＣＲＮを抽出してよく、かつ、サーバのＰＣＣＤメモリが、受信されたＣＲＮと一致するＣＲＮを含むＰＣＣＤセットを含むかどうかを決定し得る。サーバのＰＣＣＤメモリが、受信されたＣＲＮと一致するＣＲＮを含むＰＣＣＤセットを含まない場合、サーバ６１５は、６３０において、従来のＳＳＬハンドシェイクプロセスに戻ってよい。従来のＳＳＬプロセスに戻るために、サーバ６１５は、図１のプロセス１００の動作１２０を行ってよい。サーバのＰＣＣＤメモリが、受信されたＣＲＮと一致するＣＲＮを含むＰＣＣＤセットを含まない場合、サーバ６１５は、６３０において、（例えば、ｃｌｉｅｎｔ　ｈｅｌｌｏ　メッセージ６２５に応答しないことによって）接続を単に終了してよい。サーバのＰＣＣＤメモリが、受信されたＣＲＮと一致するＣＲＮを含むＰＣＣＤセットを含まない場合、サーバ６１５は６３０において一部の他の動作を実行してよい。

【００４５】

６３０において、サーバのＰＣＣＤメモリが、受信されたＣＲＮと一致するＣＲＮを含

むＰＣＣＤセットを含む場合、サーバ６１５は、ＳＲＮ、ＳＰＫ、ＰＭＳ、ＥＰＭＳ、およびＭＳについての値を含む、一致するＣＲＮを含むＰＣＣＤセットを検索してよい。サーバ６１５は、次いで、ｓｅｒｖｅｒ　ｈｅｌｌｏメッセージ６４５をクライアント６１０に送信してよい。ｓｅｒｖｅｒ　ｈｅｌｌｏメッセージ６４５は、６４０において、サーバのＰＣＣＤメモリから検索されるＳＲＮ、ならびに、いったんＳＳＬ接続が確立されると用いられる圧縮プロトコルおよび暗号化プロトコルの選択等の他の情報を含んでよい。

【００４６】

確立されているシミュレートされたＳＳＬ接続を介して送られるその後のパケットについての深いパケット検査（ＤＰＩ）を可能にするために、検査下のネットワークは、ｓｅｒｖｅｒ　ｈｅｌｌｏメッセージ６４５から、ＳＲＮおよび他の情報を抽出してよい。

【００４７】

サーバ６１５はまた、６４０において、ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ６４７をクライアントに送信してよい。ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ６４７は、６４０において、サーバのＰＣＣＤメモリから検索されたＰＣＣＤセットからのＳＰＫを含んでよい。クライアント６１０が、プロセス６００の間、サーバ公開鍵を使用し得ないとしても、ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅは、検査下のネットワークのために、送信され得る。確立されているシミュレートされたＳＳＬ接続を介して送られるその後のパケットについての深いパケット検査（ＤＰＩ）を可能にするために、検査下のネットワークは、ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ６４７から、ＳＰＫを抽出してよい。

【００４８】

６５０において、ｓｅｒｖｅｒ　ｈｅｌｌｏメッセージを受信した後、クライアント６１０は、受信されたメッセージから受信されたＳＲＮを抽出してよく、かつ、６２０において、受信されたＳＲＮが、クライアントのＰＣＣＤメモリから検索された、予期されるＳＲＮと一致するかどうか決定してよい。受信されたＳＲＮが、予期されたＳＲＮの値と一致しない場合、クライアント６１０は、６５５において、従来のＳＳＬハンドシェイクプロセスに戻ってよい。従来のＳＳＬプロセスに戻るために、クライアントは、図１のプロセス１００の動作１３０を行ってよい。受信されたＳＲＮが、予期されたＳＲＮの値と一致しない場合、クライアント６１０は、６５５において、（例えば、ｓｅｒｖｅｒ　ｈｅｌｌｏ　メッセージ６４５に応答しないことによって）接続を単に終了してよい。受信されたＳＲＮが予期されたＳＲＮの値に一致しない場合、クライアント６１０は、６５５において、一部の他の動作を実行してよい。

【００４９】

６６０において、受信されたＳＲＮが、予期されたＳＲＮの値と一致する場合、クライアント６１０は、６２０において検索されたＥＰＭＳを含むｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅのメッセージ６６５を、サーバ６１５に送信してよい。クライアントからｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅのメッセージを受信した後、６７０で、サーバ６１５は、ｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅのメッセージから抽出された、受信されたＥＰＭＳが、６４０において、サーバのＰＣＣＤメモリから検索された、予期されたＥＰＭＳと一致するかどうかを決定してよい。受信されたＥＰＭＳが予期されたＥＰＭＳと一致しない場合、サーバ６１５は、６７５において、（例えば、クライアントからの任意のさらなるメッセージに応答しないことによって）接続を終了してよい。受信されたＥＰＭＳが予期されたＥＰＭＳと一致しない場合、サーバ６１５は、６７５において、一部の他の動作を実行してよい。

【００５０】

確立されているシミュレートされたＳＳＬ接続を介して送られるその後のパケットについての深いパケット検査（ＤＰＩ）を可能にするために、検査下のネットワークは、ｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅのメッセージ６６５から、ＥＰＭＳを抽出してよい。検査下のネットワークは、ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ６４７から以前に抽出されたＳＰＫに関連付けられたサーバ秘密鍵を用いて、抽出されたＥＰＭＳから、プリ

マスタシークレットを計算してよい。検査下のネットワークはまた、ｃｌｉｅｎｔ ｈｅｌｌｏのメッセージおよびｓｅｒｖｅｒ ｈｅｌｌｏのメッセージ、ならびにプリマスタシークレットから抽出されたＣＲＮおよびＳＲＮを用いて、マスタシークレットを計算してよい。

【００５１】

６７０で、受信されたＥＰＭＳが予期されたＥＰＭＳと一致する場合、クライアント６１０およびサーバ６１５は、６２０および６４０各々において、それらの個々のＰＣＣＤメモリから抽出されたＭＳに基づいて、対称暗号化を用いて、さらなるメッセージを交換し得る。あるいは、クライアント６１０およびサーバ６１５のいずれかまたは両方は、ＣＲＮ、ＳＲＮ、およびＰＭＳからＭＳを計算し得、この場合、ＭＳは各ＰＣＣＤ内には含まれる必要はない。クライアント６１０とサーバ６１５との間の暗号化された通信は、シミュレートされたＳＳＬ接続が６９０で終了されるまで、６８０および６８５にて継続してよい。検査下のデバイスはｃｌｉｅｎｔ ｈｅｌｌｏおよびｓｅｒｖｅｒ ｈｅｌｌｏｗのメッセージ６２５／６４５、ｃｌｉｅｎｔ ｋｅｙ ｅｘｃｈａｎｇｅのメッセージ６６５から抽出されたＥＰＭＳ、ならびにｓｅｒｖｅｒ ｃｅｒｔｉｆｉｃａｔｅ６４７から抽出されたＳＰＫに関連付けられたサーバ秘密鍵から抽出されたＣＲＮおよびＳＲＮに基づいて同じＭＳの値を計算するので、検査下のデバイスは、深いパケット検査（ＤＰＩ）を実行するために暗号化された通信を解読してよい。

【００５２】

図７は、ネットワークデバイスを検査するために、シミュレートされたＳＳＬ接続を確立し、それを用いるための別のプロセス７００のフローチャートを示す。シミュレートされたＳＳＬ接続は、任意の非対称の暗号化または解読のプロセスなしに、従来のＳＳＬハンドシェイクプロトコルをシミュレートする一連のメッセージを用いて確立されてよい。シミュレートされたＳＳＬ接続を介して送信されたデータは暗号化されてもよいが、実際にセキュアでなくともよい。プロセス６００は、クライアント６１０として動作する第１のポートユニットおよびサーバ６１５として動作する第２のポートユニットによって実行されてもよい。プロセス６００と比較すると、プロセス７００は、ＰＣＣＤデータを保存するために、メモリを大幅に必要としなくなっているが、クライアント７１０およびサーバ７１５内の追加の処理を必要とする。

【００５３】

クライアント７１０およびサーバ７１５は、検査下のネットワークデバイス（図示せず）を介して複数のメッセージを変更し得る。各々のＳＳＬ接続について、プロセス７００は、クライアント７１０がＳＳＬ接続を開くことを決定するか、またはそのように命令された場合に、７０５において開始してよい。プロセス７００は、通常、クライアント７１０およびサーバ７１５の相互の認証によって、７９０において終了してよい。プロセス７００の複数のインスタンスは、複数のＳＳＬ接続を確立するように、連続して、および／または同時に、実行されてよい。プロセス７００の１つ以上のインスタンスは、プロセス６００の１つ以上のインスタンスと同時に実行されてもよい。プロセス６００および７００は、複数のポートユニットによって同時に実行されてよく、それらの各々は、多数のＳＳＬ接続を確立するために、クライアントとして、またはサーバとして、あるいはそれら両方として動作する。

【００５４】

７９５において、検査セッションのための準備の間および任意のＳＳＬ接続を確立するのに先立って、１つ以上のプレコンピューテッド暗号データ（ＰＣＣＤ）のセットが計算されてよく、かつ、クライアント７１０およびサーバ７１５におけるＰＣＣＤメモリに、および、存在する場合にはさらなるポートユニットにアップロードされてよい。７９５での動作はプロセス７００の一部ではなく、確立されるＳＳＬ接続の数とは関係なく、検査セッション毎に一度のみ実行されてよい。各ＰＣＣＤセットは、関連付けられたサーバ公開鍵（ＳＰＫ）を用いて計算されたプリマスタシークレット（ＰＭＳ）および暗号化プリマスタシークレット（ＥＰＭＳ）を含んでよい。サーバとして動作する各ポートユニット

は、１つ以上のＳＰＫの値が提供されてよい。サーバまたはクライアントのいずれかとして動作する各ポートユニットは、各ＳＰＫの値に関連付けられた１つ以上のＰＣＣＤセットが提供されてもよい。ＰＣＣＤセットは選択的にポートユニットに提供されてもよく、その結果、各ポートユニットはそれが検査セッション中に必要とするＰＣＣＤセットのみを受信し、または、一般的には（ｇｌｏｂａｌｌｙ）、各ポートユニットは７９５で確立されたＰＣＣＤセットの全てを受信する。７９５において、検査セッションの間に用いられる全てのＳＰＫは、各ＳＰＫに対応するサーバ秘密鍵と共に、検査下のネットワークに提供されてよい。

【００５５】

７２０において、クライアント７１０は、クライアントランダム数（ＣＲＮ）を計算することによって、シミュレートされたＳＳＬ接続を開始し得る。クライアント７１０は次いで、ＣＲＮを含んだｃｌｉｅｎｔ　ｈｅｌｌｏメッセージ７２５をサーバ７１５に送ってよい。ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージ７２５は、クライアント７１０によってサポートされた圧縮プロトコルおよび暗号化プロトコルのリスト等の他の情報を含んでもよい。確立されているシミュレートされたＳＳＬ接続を介して送られるその後のパケットについての深いパケット検査（ＤＰＩ）を可能にするために、検査下のネットワークは、ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージ７２５から、ＣＲＮおよび他の情報を抽出してよい。

【００５６】

７３０において、ｃｌｉｅｎｔ　ｈｅｌｌｏメッセージを受信した後、サーバ７１５はサーバランダム数（ＳＲＮ）を計算し、かつｓｅｒｖｅｒ　ｈｅｌｌｏメッセージ７４５をクライアント７１０に送信してよい。ｓｅｒｖｅｒ　ｈｅｌｌｏメッセージ７４５は、計算されたＳＲＮ、ならびに、いったんＳＳＬ接続が確立されると用いられる圧縮プロトコルおよび暗号化プロトコルの選択等の他の情報を含んでよい。

【００５７】

確立されているシミュレートされたＳＳＬ接続を介して送られるその後のパケットについての深いパケット検査（ＤＰＩ）を可能にするために、検査下のネットワークは、ｓｅｒｖｅｒ　ｈｅｌｌｏメッセージ７４５から、ＳＲＮおよび他の情報を抽出してよい。

【００５８】

サーバ７１５はまた、７４０において、ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ７４０をクライアントに送信してよい。ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ７４０は、７９５において、サーバ７１５に割り当てられたＳＰＫの値を含んでよい。ＳＰＫの値は、７９５において、サーバ７１５に割り当てられた複数のＳＰＫの値から選択されてよい。確立されているシミュレートされたＳＳＬ接続を介して送られるその後のパケットについての深いパケット検査（ＤＰＩ）を可能にするために、検査下のネットワークは、ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅのメッセージ７４０から、ＳＰＫを抽出してよい。

【００５９】

ｓｅｒｖｅｒ　ｈｅｌｌｏのメッセージを受信した後、７５０において、クライアント７１０は、受信されたメッセージから受信されたＳＲＮを抽出してよい。７５０において、クライアントはまた、ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ７４０からＳＰＫを抽出してもよい。クライアント７１０は次いで、クライアントのＰＣＣＤメモリから、抽出されたＳＰＫに関連付けられたＰＣＣＤセットを検索してよい。ＰＣＣＤセットは、ＰＭＳおよびＥＰＭＳを含んでよい。クライアント７１０は次いで、検索されたＰＣＣＤセットからサーバ７１５へ、ＥＰＭＳを含むｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅメッセージ７５５を送信してよい。

【００６０】

確立されているシミュレートされたＳＳＬ接続を介して送られるその後のパケットについての深いパケット検査（ＤＰＩ）を可能にするために、検査下のネットワークは、ｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅのメッセージ７５５から、ＥＰＭＳを抽出してよい。検査下のネットワークは、ｓｅｒｖｅｒ　ｃｅｒｔｉｆｉｃａｔｅ６４７から以前に抽出されたＳＰＫに関連付けられたサーバ秘密鍵を用いて、ＥＰＭＳから、ＰＭＳを計算し

てよい。検査下のネットワークはまた、ｃｌｉｅｎｔ　ｈｅｌｌｏのメッセージおよびｓｅｒｖｅｒ　ｈｅｌｌｏのメッセージ、ならびにＰＭＳから抽出されたＣＲＮおよびＳＲＮを用いて、マスタシークレットをさらに計算してよい。

【００６１】

クライアントからｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅのメッセージ７５５を受信した後、７６０で、サーバ７１５は、ｃｌｉｅｎｔ　ｋｅｙ　ｅｘｃｈａｎｇｅのメッセージから抽出された、受信されたＥＰＭＳが、６４０において、サーバのＰＣＣＤメモリにおけるＥＰＭＳの値と一致するかどうかを決定してよい。受信されたＥＰＭＳが予期されたＥＰＭＳの値と一致しない場合、サーバ７１５は、通常、ＥＰＭＳからＰＭＳを（サーバ秘密鍵を用いて）計算してよい。あるいは、サーバ７１５は、接続を終了してもよく、または受信されたＥＰＭＳが予期されたＥＰＭＳと一致するかどうか一部の他の動作を行ってもよい。

【００６２】

受信されたＥＰＭＳが、７６０において、予期されたＥＰＭＳと一致した場合、サーバ７１５は、７７５で、そのＰＣＣＤメモリから、関連付けられたＰＭＳを検索してよく、かつ、ＣＲＮ、ＳＲＮ、および検索されたＰＭＳに基づいてマスタシークレット（ＭＳ）を計算してよい。同様に、クライアント７１０は、７７０において、そのＰＣＣＤメモリから同じＰＭＳを検索してよく、ＣＲＮ、ＳＲＮ、および検索されたＭＳに基づいて、同じＭＳを計算してよい。

【００６３】

クライアント７１０およびサーバ７１５は、７７０および７７５において計算されたＭＳに基づいた対称暗号化を用いて追加のメッセージを交換してよい。クライアント７１０とサーバ７１５との間の暗号化された通信は、シミュレートされたＳＳＬ接続が７９０で終了されるまで、７８０および７８５にて継続してよい。検査下のデバイスは同じＭＳの値を計算するので、検査下のデバイスは、深いパケット検査（ＤＰＩ）を実行するために、暗号化された通信を解読してよい。

【００６４】

前述の例がＳＳＬプロトコルに基づいている一方で、その同じ技術は、非対称暗号化を必要とするハンドシェイクを用いる接続を確立する他のセキュリティプロトコルに提供されてもよい。他のセキュリティプロトコルに従ってシミュレートされたセキュアな接続を確立するために説明された各ＰＣＣＤは、各々の暗号化キーに関連付けられてもよく、各ＰＣＣＤセットは、第１のパラメータ、および、その第１のパラメータを、それに関連付けられた暗号化キーを用いて暗号化することによって生成される第２のパラメータを含んでよい。

【００６５】

（終わりに）

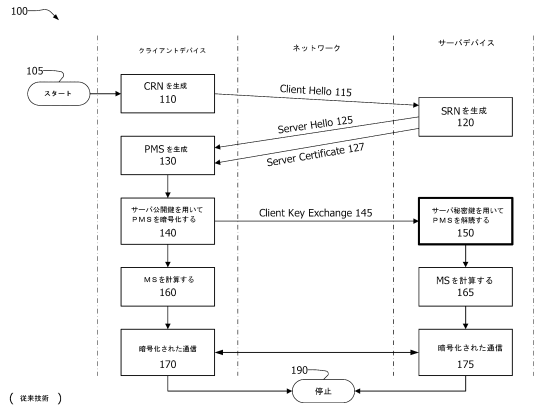
本記載全体を通して、示された実施形態および例は、開示された、または特許請求の範囲において請求された装置および手順についての限定ではなく、典型例として想定されるべきものである。本明細書において提示された例の多くは、方法の作用またはシステムの要素の特定の組合せに関連するものであるけれども、それらの作用およびそれらの要素は、他の方法において、組み合わされてよく、同じ課題を達成するものとして理解されるべきである。フローチャートに関して、追加の工程および工程の削減もまた考慮されてよく、図示した工程は、本明細書において記載された方法を達成するために組み合わされてもよく、またはさらに改良されてもよい。１つの実施形態のみに関連して記載された作用、要素、および特徴は、他の実施形態における同様の役割から排除されることは意図されていない。

【００６６】

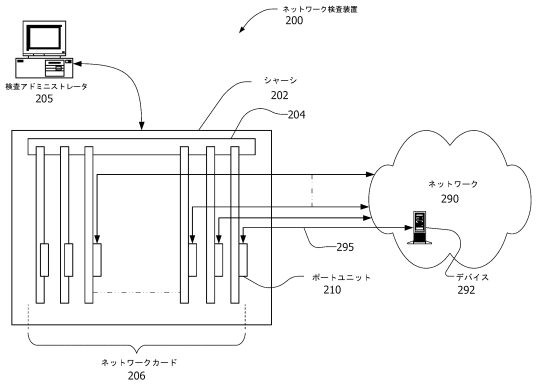
本明細書において用いられるように、「複数」とは、２つ以上を意味する。本明細書において用いられるように、「一連の」物品とは、１つ以上のそのような物品を含み得る。本明細書において用いられるように、明細書の記載または特許請求の範囲の請求項におい

ては、用語「含む、備える（ｃｏｍｐｒｉｓｉｎｇ）」、「含む、備える（ｉｎｃｌｕｄｉｎｇ）」「運ぶ、有する、持つ（ｃａｒｒｙｉｎｇ）」、「有する（ｈａｖｉｎｇ）」、「含む（ｃｏｎｔａｉｎｉｎｇ）」、「含む、関する、関連する（ｉｎｖｏｌｖｉｎｇ）」等は、オープンエンド型、すなわち、含むがそれらに限定されないということを意味することは理解されるべきである。「～からなる」および「～から実質的になる」といった移行句の各々のみが、特許請求の範囲の請求項に関しては、クローズ型、または半クローズ型の移行句である。請求項の要素を変更するために、特許請求の範囲の請求項における「第１」、「第２」、「第３」等の序数の用語の使用は、それ自体では、任意の優先順位、優位性、またはある請求項の要素が他のものより先であったり、または、ある方法の作用が行われる時間的順序等を含意せず、請求項の要素を区別するために、特定の名前を有するある請求項の要素から、同じ名前を有する別の要素を区別するためのラベルとして（順序を示す用語の使用を別にして）単に用いられる。本明細書において用いられるように、「および／または」は、リストアップされた物品が二者択一であることを意味するが、そうした二者択一もまた、そうしてリストアップされた物品の任意の組合せを含むものである。

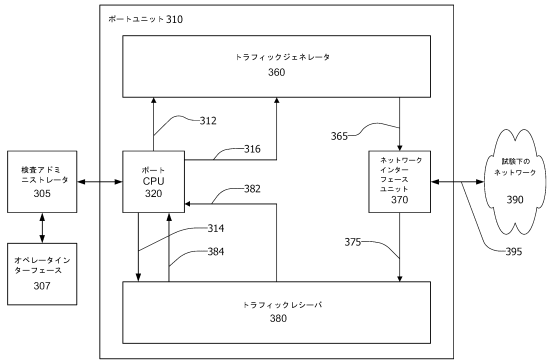
【図１】



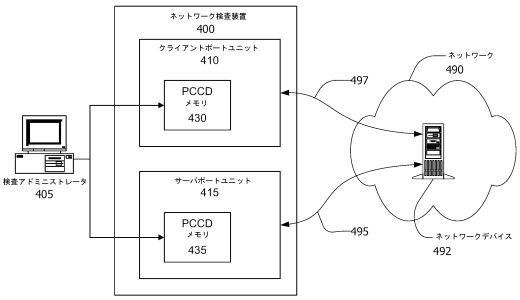
【図２】



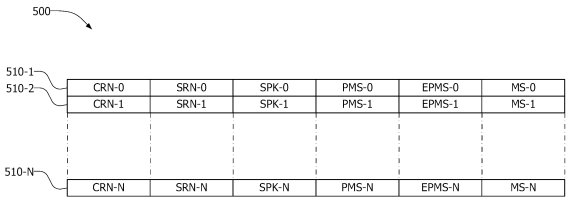
【図３】


ポートユニット310
トラフィックジェネレータ
360
312
316
365
検査アドミニストレータ
305
ポート
CPU
320
382
ネットワーク
インター
フェース
ユニット
370
試験下の
ネットワーク
390
314
384
375
395
オペレータイン
ターフェース
307
トラフィックレシーバ
380

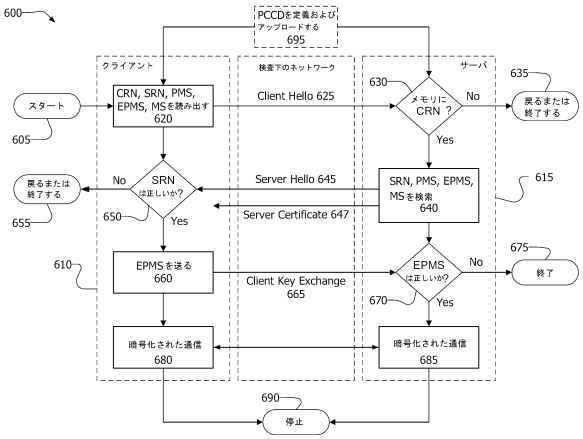
【図４】


ネットワーク検査装置
400
クライアントポートユニット
410
PCCD
メモリ
430
497
ネットワーク
490
検査アドミニストレータ
405
サーバポートユニット
415
PCCD
メモリ
435
495
ネットワークデバイス
492

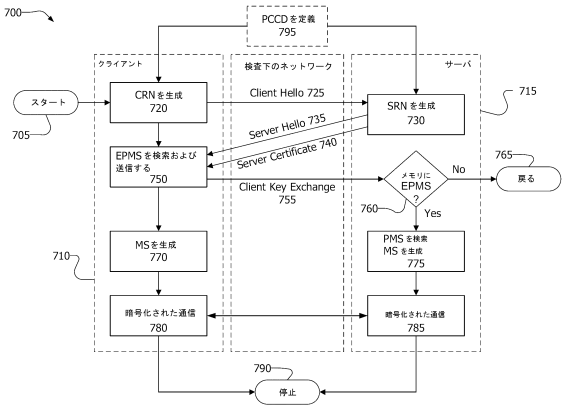
【図５】


500
510-1
510-2
CRN-0
SRN-0
SPK-0
PMS-0
EPMS-0
MS-0
CRN-1
SRN-1
SPK-1
PMS-1
EPMS-1
MS-1
510-N
CRN-N
SRN-N
SPK-N
PMS-N
EPMS-N
MS-N

【図６】


600
PCCDを定義および
アップロードする
695
クライアント
検査下のネットワーク
サーバ
スタート
605
CRN, SRN, PMS,
EPMS, MSを読み出す
620
Client Hello 625
630
メモリに
CRN ?
No
635
戻るまたは
終了する
Yes
戻るまたは
終了する
655
No
SRN
は正しいか?
650
Yes
Server Hello 645
Server Certificate 647
SRN, PMS, EPMS,
MSを検索
640
615
610
EPMSを送る
660
Client Key Exchange
665
EPMS
は正しいか?
No
675
終了
670
Yes
暗号化された通信
680
暗号化された通信
685
690
停止

【図７】


700
PCCDを定義
795
クライアント
検査下のネットワーク
サーバ
スタート
705
CRNを生成
720
Client Hello 725
SRNを生成
730
715
Server Hello 735
Server Certificate 740
EPMSを検索および
送信する
750
Client Key Exchange
755
メモリに
EPMS
?
No
765
戻る
760
Yes
710
MSを生成
770
PMSを検索
MSを生成
775
暗号化された通信
780
暗号化された通信
785
790
停止

フロントページの続き

(56)参考文献　米国特許出願公開第２００３／００２０６２１（ＵＳ，Ａ１）
米国特許出願公開第２００７／０１２１５１６（ＵＳ，Ａ１）
東角　芳樹、竹仲　正彦，ＳＳＬプロトコル評価ツールの試作と各種ＳＳＬ実装の評価，情報処理学会研究報告　平成２１年度▲2▼　［ＣＤ－ＲＯＭ］，社団法人情報処理学会，２００９年８月１５日

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／７０
Ｈ０４Ｌ　１２／２２