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

特許第5468623号
(P5468623)

(45)発行日　平成26年4月9日(2014.4.9)　(24)登録日　平成26年2月7日(2014.2.7)

| (51)Int.Cl. | | F I | | |
|---|---|---|---|---|
| H04L 9/08 | (2006.01) | H04L | 9/00 | 601B |
| H04W 12/08 | (2009.01) | H04W | 12/08 | |
| H04L 9/32 | (2006.01) | H04L | 9/00 | 673B |
| | | H04L | 9/00 | 673A |

請求項の数 12　(全 14 頁)

(21)出願番号　特願2011-549117(P2011-549117)
(86)(22)出願日　平成21年10月1日(2009.10.1)
(65)公表番号　特表2012-517185(P2012-517185A)
(43)公表日　平成24年7月26日(2012.7.26)
(86)国際出願番号　PCT/SE2009/051092
(87)国際公開番号　WO2010/090569
(87)国際公開日　平成22年8月12日(2010.8.12)
審査請求日　平成24年8月30日(2012.8.30)
(31)優先権主張番号　61/150,118
(32)優先日　平成21年2月5日(2009.2.5)
(33)優先権主張国　米国(US)

(73)特許権者　598036300
テレフオンアクチーボラゲット　エル　エム　エリクソン(パブル)
スウェーデン国　ストックホルム　エス－１６４　８３
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘
(74)代理人　100116894
弁理士　木村　秀二
(74)代理人　100130409
弁理士　下山　治

最終頁に続く

(54)【発明の名称】ネットワークにおけるブートストラップ・メッセージを保護するための装置と方法

(57)【特許請求の範囲】
【請求項１】
ブートストラップ・メッセージの保護を可能にするデバイス管理ＤＭネットワーク・システムの第１のネットワーク・ユニット（５００）であって、
デバイス（６００）をブートストラップする要求を含む第１のメッセージであって、前記デバイス（６００）を識別する情報及び加入者を識別する情報を含む前記第１のメッセージを受信する受信機（５１０）と、
前記加入者を識別する前記情報を含む第２のメッセージであって、前記加入者を識別する前記情報に基づくブートストラップ・キーを前記第１のネットワーク・ユニット（５００）へ提供するように、第２のネットワーク・ユニットへ要求する前記第２のメッセージを、前記第２のネットワーク・ユニットへ送信する送信機（５２０）と
を備え、
前記受信機（５１０）は、さらに、前記第２のネットワーク・ユニットから、前記ブートストラップ・メッセージの保護を可能にするための、前記ブートストラップ・キーと、トリガ情報とを含む第３のメッセージを受信するように構成され、
前記送信機（５２０）は、さらに、前記デバイス（６００）において前記ブートストラップ・キーの生成を開始させるために、該デバイス（６００）へ前記トリガ情報を送信するように構成されることを特徴とする第１のネットワーク・ユニット（５００）。
【請求項２】
前記ブートストラップ・キーを記憶する記憶手段（５３０）をさらに備え、

前記第１のネットワーク・ユニット（５００）は、さらに、
前記ブートストラップ・キーに基づいて、前記送信機（５２０）が保護されたブートストラップ・メッセージを前記デバイス（６００）へ送信する前に、前記ブートストラップ・メッセージを保護するように構成されることを特徴とする請求項１に記載の第１のネットワーク・ユニット（５００）。
【請求項３】
前記送信機（５２０）は、ジェネリック・ブートストラップ・アーキテクチャ・プッシュ情報ＧＰＩの前記トリガ情報を送信するように構成され、
前記受信機（５１０）は、ＧＰＩレスポンス・メッセージの前記ブートストラップ・キーを含む前記第３のメッセージを受信するように構成されることを特徴とする請求項１又は２に記載の第１のネットワーク・ユニット（５００）。
【請求項４】
前記ブートストラップ・メッセージの検証後に、前記デバイス（６００）と前記ＤＭネットワーク・システムとの間の少なくとも１つのＤＭセッション中に少なくとも１つのメッセージの保護のための追加のキーを生成するために、マスタキーとして前記ブートストラップ・キーを使用するようにさらに構成されることを特徴とする請求項１乃至３の何れか１項に記載の第１のネットワーク・ユニット（５００）。
【請求項５】
ブートストラップ・メッセージの保護を可能にするためのデバイス管理ＤＭネットワーク・システムの第１のネットワーク・ユニット（５００）と通信可能なデバイス（６００）であって、
前記デバイスを識別する情報及び加入者を識別する情報を、前記第１のネットワーク・ユニット（５００）へ通知する手段（６１０）と、
前記第１のネットワーク・ユニット（５００）から、前記デバイスのブートストラップ・キーの生成を開始させるトリガ情報を受信する受信機（６１０）であって、前記ブートストラップ・キーに基づいて保護される、保護されたブートストラップ・メッセージを受信するように構成される前記受信機（６１０）と、
前記保護されたブートストラップ・キーを検証するか、復号化するかの少なくとも一方を行う手段（６３０）と
を備えることを特徴とするデバイス（６００）。
【請求項６】
前記受信機（６１０）は、ジェネリック・ブートストラップ・アーキテクチャＧＢＡプッシュ情報ＧＰＩメッセージの前記トリガ情報を受信するように構成されることを特徴とする請求項５に記載のデバイス（６００）。
【請求項７】
前記ブートストラップ・キーを記憶する記憶手段（６４０）をさらに備えることを特徴とする請求項５又は６に記載のデバイス（６００）。
【請求項８】
ブートストラップ・メッセージの保護を可能にするデバイス管理ＤＭネットワーク・システムの第１のネットワーク・ユニット（５００）における方法であって、
デバイスをブートストラップする要求を含む第１のメッセージであって、前記デバイスを識別する情報及び加入者を識別する情報を含む前記第１のメッセージを前記第１のネットワーク・ユニットで受信するステップ（４０１）と、
前記加入者を識別する前記情報を含む第２のメッセージであって、前記加入者を識別する前記情報に基づくブートストラップ・キーを前記第１のネットワーク・ユニットへ提供するように、第２のネットワーク・ユニットへ要求する前記第２のメッセージを、前記第２のネットワーク・ユニットへ送信するステップ（４０２）と、
前記第２のネットワーク・ユニットから、前記ブートストラップ・メッセージの保護を可能にするための、前記ブートストラップ・キーと、トリガ情報とを含む第３のメッセージを受信するステップ（４０３）と、

前記デバイスにおいて前記ブートストラップ・キーの生成を開始させるために、該デバイスへ前記トリガ情報を送信するステップ（４０４）と
を含むことを特徴とする方法。
【請求項９】
前記ブートストラップ・キーを前記第１のネットワーク・ユニットで記憶するステップと、
前記ブートストラップ・キーに基づいて、前記ブートストラップ・メッセージを前記デバイスへ送信する前に、前記ブートストラップ・メッセージを保護するステップと
をさらに含むことを特徴とする請求項８に記載の方法。
【請求項１０】
前記トリガ情報を送信する前記ステップ（４０４）は、ジェネリック・ブートストラップ・アーキテクチャ・プッシュ情報ＧＰＩメッセージの前記トリガ情報を送信するステップを含み、
前記第３のメッセージを受信する前記ステップ（４０３）は、ＧＰＩレスポンス・メッセージの前記第３のメッセージを受信するステップを含むことを特徴とする請求項８又は９に記載の方法。
【請求項１１】
前記ブートストラップ・メッセージの検証後に、前記デバイスと前記ＤＭネットワーク・システムとの間の少なくとも１つのＤＭセッション中に少なくとも１つのメッセージを保護するための追加のキーを生成するために、マスタキーとして前記ブートストラップ・キーを使用するステップをさらに含むことを特徴とする請求項８乃至１０の何れか１項に記載の方法。
【請求項１２】
請求項８乃至１１の何れか１項に記載の第１のネットワーク・ユニット（５００）における方法の各ステップをコンピュータに実行させるためのプログラム命令を含むコンピュータで実行可能なコンピュータプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、一般的には移動または無線通信ネットワーク・システムの分野に関し、より詳細には、デバイス管理ネットワーク・システムにおいて、デバイスのブートストラップ中のブートストラップ・メッセージをセキュアに保護する装置と方法に関する。
【背景技術】
【０００２】
移動デバイスは、制御するための各種の設定で構成され、各種の機能を提供し、各種のサービスをサポートする必要がある。データに関するサービスで移動デバイスを構成する既知の一つの方法は、例えば、ショート・メッセージ・サービス（ＳＭＳ）または無線アプリケーション・プロトコル（ＷＡＰ）を介する。これは単方向パスであり、双方向サービスを実行できるためには、オープン・モバイル・アライアンス（ＯＭＡ）は、デバイス管理（ＤＭ）に対して特定のプロトコル、データ・モデルおよび方策を持つ。例として、ＵＲＬ：ｈｔｔｐ：／／ｗｗｗ.ｏｐｅｎｍｏｂｉｌｅａｌｉａｎｃｅ．ｏｒｇで利用可能な、ＯＭＡ　ＤＭ　バージョン１．２．１　イネーブラ・リリース仕様は、いかにＤＭセッションが確立され、維持されるかを定めている。これらの仕様における重要な機能の一つには、管理セッションを開始する前にＯＭＡ　ＤＭ設定をデバイスに提供する方法について説明する、ブートストラップ仕様を含む。ＯＭＡ　ＤＭブートストラップ技術仕様については「非特許文献１」に説明されている。
【０００３】
ブートストラップは、移動または無線デバイスのＤＭクライアントに、非提供の、空の状態から、ＤＭサーバに、および後には、例えば、新しいＤＭサーバに管理セッションを開始できるような状態に、本デバイスを移すことをプロビジョニイングするプロセスであ

る。ブートストラップ・プロセスを実行するためには三つの異なる方法があり、即ち、カスタマイズ・ブートストラップ、サーバ開始のブートストラップおよびスマートカードからのブートストラップである。

【０００４】

カスタマイズ・ブートストラップ・プロセスでは、製造時にＯＭＡ　ＤＭブートストラップ情報をデバイスにロードする。これは工場ブートストラップとも称される。

【０００５】

サーバ開始のブートストラップ・プロセスでは、例えばＷＡＰプッシュのような幾つかのプッシュ機構を介してブートストラップ情報を送り出すように、サーバを構成する。このプロセスのために、本サーバはデバイス・アドレス／電話番号を事前に受信しなければならない。

【０００６】

スマートカードからのブートストラップ・プロセスでは、デバイスにスマートカード（例えば、加入者識別モジュール（ＳＩＭ）または万能ＳＩＭ（ＵＳＩＭ））を挿入し、本スマートカードからＤＭクライアントをブートストラップする。

【０００７】

しかしながら、これらのプロセスを使用するシステムに関連して、幾つかの問題点と欠点がある。カスタマイズ・ブートストラップ・プロセスは、製造時に、またはデバイスを販売する時に、基本的パラメータが知らされる、ということを要求する。サーバ開始のブートストラップ・プロセスは、ＤＭサーバがエア・インタフェースを通してブートストラップを実行する場合、基本的なＤＭパラメータを符号化するために国際移動加入者識別（ＩＭＳＩ）を使用しなければならない、ということを規定している。このことは、デバイスに本基本パラメータで暗号化したＳＭＳを送信することで行なわれる。暗号化に使用するキーは、例えば、第２世代／第３世代ネットワーク・システムのためのＩＭＳＩ、または符号分割多元接続（ＣＤＭＡ）システムのための電子シリアル番号（ＥＳＮ）である。しかしながら、本ＩＭＳＩまたはＥＳＮは機密であるようには設計されなかった。また、このことは、ＤＭサーバからデバイスに送信するブートストラップ情報は弱く保護されている、ということを意味する。結果として、アタッカは、悪意のあるＤＭサーバに対してロックするデバイスにブートストラップするため、それ自身のブートストラップ・メッセージを生成することができる。もう一つの欠点は、アタッカが完全性保護のみ行なわれているブートストラップ・メッセージを傍受することができる、ということである。ブートストラップ・メッセージにはユーザ・ネームおよびパスワードのような認証情報を含む可能性があるため、アッタカは本デバイスに成り済ますことができる。

【０００８】

図１は、上記で引用した仕様書「非特許文献１」で定めているように、サーバ開始のブートストラップ・プロセスの高次のレベルの図である。本サーバ開始のブートストラップを説明する図１のシナリオは、デバイス１０、ユーザ１１、ネットワーク１２およびＤＭサーバ（ＤＭＳ）１３を示す。ＯＭＡ－ＴＳ－ＤＭブートストラップＶ１＿２＿１では、ひとたびユーザ１１がデバイス１０を獲得し、例えばＳＩＭを挿入することにより、それを自分の設定に合わせると、ブートストラップ・プロセスの要件が整う、と説明している。ＤＭＳ１３は、デバイス１０がネットワーク１２に登録した時初めて、例えばネットワーク１２によって、デバイス１０のアイデンティティ、アドレスまたは電話番号を知らされるか、情報を提供される。このことが起こると、デバイス１０が使用する番号で、デバイス１０をブートストラップする要求を、（コア）ネットワーク１２からＤＭＳ１３に送信することができる。ここで、ＤＭＳ１３は、ＯＭＡ　ＤＭブートストラップ・メッセージを送り出すことができる位置にあることになる。ブートストラップ・メッセージには、デバイス１０がブートストラップ・メッセージを送り出したＤＭＳ１３と管理セッションを開始することができる情報を含む。

【０００９】

上記で説明したブートストラップ・シナリオについての脆弱な保護は、上記で述べたよ

うに、ブートストラップ・メッセージが、「非特許文献２」の５．７．２．３．１章に示しているように、非機密キー（ＩＭＳＩまたはＥＮＳ）で保護されているのみである、という事実から生じている。このようにして、ＩＭＳＩもＥＮＳも、セキュリティの観点から共有機密キーと考えられていない。また、同様にＯＭＡ仕様も、「非特許文献３」のような同じセキュリティ脆弱性に苦しんでいる。

【００１０】

当然述べるべきであるが、これらのセキュリティ脆弱性は、３ＧＰＰ　ＬＳ　返答Ｓ３－０８０２６２で示しているように、第３世代パートナーシップ・プロジェクト（３ＧＰＰ）のセキュリティ・グループ（ＳＡ３）がサーバ開始のブートストラップ方法／プロセスを使用しないよう強い勧告を出した理由である。

【００１１】

米国特許出願　ＵＳ２００８／０１５５０７１で開示されたもう一つの従来技術は、通信ネットワークのデバイスのブートストラップのための方法とシステムを提案している。この従来技術では、デバイスがスマートカードからブートストラップできるよう、エア（ＯＴＡ）技術を通して使用するデバイスのスマートカードを第１に提供するため、サーバ開始のブートストラップを使用する。３ＧＰＰ自動デバイス検出（ＡＤＤ）機能を有するスマートカードを通してブートストラップを合成することにより、これを実行する。技術仕様書３ＧＰＰ　ＴＳ　２２．１０１で定める３ＧＰＰ　ＡＤＤは、デバイスがネットワークに現れた場合、デバイスの自動検出を可能とする。しかしながら、この従来技術の方法はまだ、前に説明した現在のＯＭＡ　ＤＭ指定のサーバ開始のブートストラップのセキュリティ不足に依存している。

【先行技術文献】

【非特許文献】

【００１２】

【非特許文献１】ＯＭＡ　ＤＭブートストラップ　バージョン１．２．１、ＯＭＡ－ＴＳ－ＤＭブートストラップＶ１＿２＿１．オープン・モバイル・アライアンス、２００８年、６月。

【非特許文献２】ＯＭＡデバイス管理セキュリティ１．２．１、ＯＭＡ－ＴＳ－ＤＭセキュリティ　Ｖ１＿２＿１、ＯＭＡ、２００８年。

【非特許文献３】ＯＭＡクライアント・プロビジョニング仕様書バージョン１．２のためのイネーブル・リリース定義、ＯＭＡ－ＥＲＥＬＤ－クライアント・プロビジョニング－Ｖ１＿１；およびプロビジョニング・ブートストラップ１．１．ＯＭＡ＿ＷＡＰ－ＰｒｏｖＢｏｏｔ－Ｖ１＿１．

【発明の概要】

【発明が解決しようとする課題】

【００１３】

したがって、上記で述べた問題点を取り扱うこと、および、ＤＭサーバからデバイスへ、セキュアで保護されたブートストラップ・メッセージの伝送し、それによって、本デバイスに成り済ましたり、および／または本デバイスをハイジャックしようとする盗聴および／またはアタックを防ぐことを可能とする装置と方法を提供することが、本発明の典型的な実施形態の目的である。

【課題を解決するための手段】

【００１４】

本発明の典型的な実施形態の第１の側面によれば、ブートストラップ・メッセージの保護を可能とするため、ＤＭネットワーク・システムの第１のネットワーク・ユニットにより、上記で述べた問題点が解決される。第１のネットワーク・ユニットには、デバイスをブートストラップする要求を備える第１のメッセージを受信するよう構成した受信機を備え、本メッセージにはデバイスを識別する情報と加入者を識別する情報とを備える。第１のネットワーク・ユニットには、加入者を識別する情報を備える第２のメッセージを第２のネットワーク・ユニットに送信するよう構成した送信機を更に備え、本第２のメッセー

ジは、加入者を識別する情報に基づくブートストラップ・キーを第１のネットワーク・ユニットに提供するよう、第２のネットワーク・ユニットに要求する。受信機は、第２のネットワーク・ユニットから、ブートストラップ・メッセージの保護に使用するブートストラップ・キーを備える第３のメッセージを受信するよう、更に構成する。また、第３のメッセージには、デバイスにおいてブートストラップ・キーの生成を開始させるようデバイスに送信するトリガ情報を備える。

【００１５】

第１のネットワーク・ユニットからトリガ情報を受信するので、デバイスは内部的にブートストラップ・キーを生成する。第１のネットワーク・ユニットおよびデバイスの両方がブートストラップ・キーを入手している場合、本ブートストラップ・キーに基づき、第１のネットワーク・ユニットはブートストラップ・メッセージを保護し、本保護されたブートストラップ・メッセージをデバイスに送信する。このように、機密ブートストラップ・キーはＤＭネットワークおよびデバイスにのみ知られているので、アタッカは本デバイスをハイジャックまたはそれに成り済ますことはできない。

【００１６】

本発明の典型的な実施形態のもう一つの側面によれば、ブートストラップ・メッセージの保護を可能とするため、ＤＭネットワークの第１のネットワーク・ユニットにおける方法により、上記で述べた問題点が解決される。本方法には以下のものを備える：デバイスをブートストラップする要求を備える第１のメッセージを受信することで、本第１のメッセージには本デバイスと加入者を識別する情報を備える。本方法には、加入者を識別する情報を備える第２のメッセージを第２のネットワーク・ユニットに送信することを更に備え、加入者を識別する情報に基づくブートストラップ・キーを第１のネットワーク・ユニットに提供するよう、第２のネットワーク・ユニットに要求する。本方法には、ブートストラップ・メッセージの保護を可能とするため、第２のネットワーク・ユニットからブートストラップ・キーを備える第３のメッセージを受信することを更に備え、本第３のメッセージはトリガ情報を更に備える。本方法には、デバイスにおいてブートストラップ・キーの生成を開始させるため、デバイスに本トリガ情報を送信することを更に備える。

【００１７】

本発明の典型的な実施形態の更にもう一つの側面によれば、ブートストラップ・メッセージの保護を可能とするため、ＤＭネットワーク・システムの第１のネットワーク・ユニットと通信することが可能なデバイスにより、上記で述べた問題点が解決される。本デバイスには、デバイスと加入者とを識別する情報を第１のネットワーク・ユニットに通知する手段を備える。本デバイスには、第１のネットワーク・ユニットから、デバイスにおいてブートストラップ・キーの生成を開始させるためのトリガ情報を受信するよう構成した受信機を更に備える。本受信機は、本ブートストラップ・キーに基づいて保護された、保護ブートストラップ・メッセージを受信するよう更に構成され、本デバイスには、保護ブートストラップ・メッセージを検証および／または暗号解読するあめの手段を備える。

【００１８】

本発明の典型的な実施形態の利点は、アタッカがデバイスをハイジャックする、および／または本デバイスに成り済ますのを防ぐことである。

【００１９】

本発明の典型的な実施形態のもう一つの利点は、ネットワークおよびデバイスにのみ知られている真に機密のブートストラップ・キーを使用することを確実にすることである。

【００２０】

本発明の実施形態の更なるその他の利点、目的および特徴は、添付の図と一緒に以下の詳細な説明から明らかになるであろうが、しかしながら、以下の図は説明に役立つのみであり、添付の特許請求範囲内で説明した図示の識別の実施形態において各種の修正と変更を行う可能性がある、という事実に注意を払うべきである。更に、当然のことであるが、図は必ずしも拡大縮小して描かれていなく、他に示さない限り、それらは本明細書で説明した構造と手順を概念的に示すことのみを意図している。

【図面の簡単な説明】
【００２１】
【図１】サーバ開始のブートストラップ・プロセス中に関係するシグナリングの従来技術の高次レベルの図である。
【図２】本発明の典型的実施形態による、セキュアなデバイスのサーバ開始のブートストラップを可能とするフローチャートである。
【図３】本発明のもう一つの典型的実施形態による、デバイスのサーバ開始のブートストラップをセキュアにするもう一つのフローチャートである。
【図４】本発明の典型的実施形態による、第１のネットワーク・ユニットで使用する方法のフローチャートを示す図である。
【図５】本発明の典型的実施形態による典型的なネットワーク・ユニットのブロック図を示す。
【図６】本発明の典型的実施形態による典型的なデバイスのブロック図を示す。
【発明を実施するための形態】
【００２２】
以下の説明において、説明のためであり制限のためではないが、本発明の完全な理解を提供するため、特別なアーキテクチャ、シナリオ、技術等のような特定の実施形態について説明する。しかしながら、以下のことから明らかなことであるが、本発明とその実施形態は、これらの特定の実施形態から逸脱するその他の実施形態において実施される可能性がある。
【００２３】
特別な例のシナリオを参照して本発明の典型的な実施形態を本明細書で説明する。特に、３ＧＰＰ技術仕様書ＴＳ　３３．２２３のＧＢＡプッシュ仕様書によるジェネリック・ブートストラップ・アーキテクチャ（ＧＢＡ）と交信する、ＤＭサーバ（ＤＭＳ）を備えるデバイス管理（ＤＭ）ネットワーク・システムにおけるサーバ開始のブートストラップ・シナリオに関して、非制限の一般的文脈で、本発明について説明する。しかしながら、第１のネットワーク・ユニットは、本発明の典型的実施形態を実装できる、任意の適当なネットワーク・ユニットまたはノードであってもよい、ということに注意されたい。そのようなネットワーク・ユニットは、例えば、ＤＭＳの代わりにＤＭプロキシによって示すことができる。
【００２４】
図２を参照すると、本発明の典型的実施形態に基づいて、ネットワーク・システムにおいて、デバイスのサーバ開始のブートストラップをセキュアにできるフローチャートが示されている。示されているエンティティは：デバイス２０、一つ（または複数）のネットワーク・エンティティ２１（例えば、ホーム・ロケーション・レジスタ）、第１のネットワーク・ユニット２２、および第２のネットワーク・ユニット２３である。後述するように、デバイスのセキュアなブートストラップを目的にして追加のノード／機能を使用することも可能である。
【００２５】
図２に示すように、デバイス２０はネットワーク２１にその可用性を通知する（Ｓ２１）。ユーザ／加入者がネットワーク２１に接続を試みようとするデバイス２０をオンにすることにより、これを行うことができる。３ＧＰＰ　ＴＳ　２２．１０１に開示しているように、例えば、既知の自動デバイス検出（ＡＤＤ）方法を用いて、またはＧＢＡプッシュ　３ＧＰＰ　ＴＳ　３３．２２３で説明している既知のユーザ開始手順を用いて、ネットワーク２１はデバイス２０の存在／可用性を検出する（Ｓ２２）。ネットワーク２１へ接続後、デバイス２０は、デバイスを識別する情報、即ちそのデバイス・アイデンティティ、例えばＩＭＥＩを送り、また、加入者を識別する情報、例えばＩＭＳＩ／ＥＳＮを送信する。ブートストラップ・要求（Ｓ２２）では、ネットワークは、デバイス２０をブートストラップするため、第１のネットワーク・ユニットに要求する。ブートストラップ・要求（Ｓ２３）では、ネットワーク２１（例えばＨＬＲ）には、デバイスを識別する情報

（ＩＭＥＩ）および加入者を識別する情報、即ちＩＭＳＩ／ＥＳＮ、ＭＳＩＳＤＮ等を含む。第１のネットワーク・ユニット２２が本要求を受信すると、デバイスおよびユーザ／加入者を識別する情報に基づき、第１のネットワーク・ユニット２２は、ＧＢＡ　ＰＵＳＨがデバイスに向けて使用可能かどうかを決定する。もしそうなら、第１のネットワーク・ユニット２２は、ブートストラップ・キーを第１のネットワーク・ユニット２２に提供するよう第２のネットワーク・ユニット２３に要求するメッセージを、第２のネットワーク・ユニット２３に送信する（Ｓ２４）。ＧＢＡサブシステムの一部である第２のネットワーク・ユニット２３には、ブートストラップ・サーバ機能（ＢＳＦ）とホーム加入者サーバ（ＨＳＳ）とを備える。

【００２６】

当然言及すべきであるが、もし第１のネットワーク・ユニット２２が、ＧＢＡ　ＰＵＳＨはデバイスに向けて使用できる、と決定したなら、メッセージを使用して（Ｓ２４）、少なくともトリガ情報およびブートストラップ・キーを要求するＧＢＡ　ＰＵＳＨ手順を使用するＢＳＦと連絡を取るよう、第１のネットワーク・ユニット２２のネットワーク応用機能（ＮＡＦ）を構成する。本トリガ情報は、ＧＢＡ　ＰＵＳＨ情報（ＧＰＩ）に対応する。また、メッセージ（Ｓ２４）にはＮＡＦアイデンティティを備える。しかしながら、ＧＢＡ　ＰＵＳＨがセキュアなものの一つに基づいているなら、デバイス２０をブートストラップする方法を選択するよう、第１のネットワーク・ユニット２２を構成する、ということに注意されたい。ＧＢＡ　ＰＵＳＨを選択すべきなら、デバイスおよび加入者を識別する情報に基づき、第１のネットワーク・ユニット２２のＮＡＦはセキュアなブートストラップ・プロセスを処理する。以下では、デバイス２０に向けてＧＢＡ　ＰＵＳＨを使用できる場合、即ち要求・メッセージ（Ｓ２４）が第２のネットワーク・ユニット２３に到達する場合について説明する。

【００２７】

図２に戻って参照して、第２のネットワーク・ユニット２３が要求・メッセージを受信する（Ｓ２４）と、それはブートストラップ・キーを生成し（Ｓ２５）、本明細書ではＤＰＩレスポンスと称するレスポンス・メッセージ（Ｓ２６）で、本ブートストラップ・キーと少なくともＧＰＩとを第１のネットワーク・ユニット２２に送信するか配信する。ここで、第１のネットワーク・ユニット２２はＧＰＩレスポンスを入手しているので、それはデバイス２０にトリガ情報、即ちＧＰＩレスポンスのＤＰＩ部分を送信するか転送する（Ｓ２７）。また、第１のネットワーク・ユニット２２はデバイス２０へＧＰＩを送信する前に、ブートストラップ・キーをストアすることができる。ＳＭＳ、ＷＡＰ、ＨＴＴＰ、ＳＩＰプッシュ、または、デバイス２０でブートストラップ・キーの生成を開始させるため、トリガ情報を運ぶのに適する任意のベアラを通じて、ＧＰＩまたはトリガ情報を送信できる。ＧＰＩの受信の後、適当な標準手順を使用して、デバイス２０はブートストラップ・キーを生成する（Ｓ２８）。

【００２８】

ＧＢＡプッシュ　３ＧＰＰ　ＴＳ　３３．２３３では、ＧＰＩは保護されていると開示されている。これは、ＧＰＩ完全性保護およびＧＰＩ機密性保護として知られている。その上、ＧＢＡでは、ブートストラップ・キーはＫｓ＿ＮＡＦと称され、またこのキーはキー材料またはキーとする材料として知られる。Ｋｓ＿ＮＡＦについては、上に述べた従来技術ＧＢＡプッシュ　３ＧＰＰ　ＴＳ　３３．２３３において参照している、３ＧＰＰ　ＴＳ　３３．２２０　Ｖ８．５．０で説明している。

【００２９】

図２に戻って参照して、デバイス２０がブートストラップ・キーを生成する（Ｓ２８）と、ブートストラップ・キーをストアする。続いて、ブートストラップ・キーに基づいて保護されているブートストラップ・メッセージを保護し、送信することにより、第１のネットワーク・ユニット２２はセキュアなブートストラップを実行できる（Ｓ２９）。第１のネットワーク・ユニット２２は、ブートストラップ・キーを使用してブートストラップ・メッセージを直接保護できるか、本ブートストラップ・キーを使用して更なるキーを導

出し、ブートストラップ・メッセージを保護するためにこれらのキーを使用できる。なお、もし第１のネットワーク・ユニット２２が、それをデバイス２０に送信する前にブートストラップ・メッセージを暗号解読したなら、デバイス２０は、本ブートストラップ・メッセージを最初に復号化し、次に本メッセージを検証する。ブートストラップ・キーは、ＩＭＳＩ／ＥＳＮに代わって、完全性保護に使用可能であり、および／または機密性保護に使用可能である。デバイスを成功裏におよびセキュアにブートストラップした後、ＤＭセッションがデバイス２０と第１のネットワーク・ユニット２２との間で開始する。なお、本ブートストラップ・キーの成功裏の検証／暗号解読の後、デバイス２０と第１のネットワーク・ユニット２２との間の一つ以上のＤＭセッションを保護するために使用できるキーを更に生成するためのマスタ・キー、例えば認証として、本ブートストラップ・キーをまた使用できる。

【００３０】

図３を参照すると、本発明のもう一つの典型定な実施形態により、ネットワーク・システムのデバイスのセキュアなサーバ開始のブートストラップを可能とするフローチャートが示されている。図２と同様に、本ネットワーク・システムには、デバイス３０、ネットワーク３１（例えばＨＬＲ）、第１のネットワーク・ユニット３２（例えばＮＡＦを有するＤＭＳ）および、ＢＳＦ　３３ＡとＨＳＳ　３４Ｂとを備える第２のネットワーク・ユニット３３を備える。また、図３はユーザ３０Ａを図示している。（Ｓ３１Ａ）では、ネットワーク３１に接続すると、デバイス３０はデバイスを識別する情報、ＩＭＥＩを送り、また、ユーザ／加入者を識別する情報（例えばＩＭＳＩ）を送信する。以前に述べたように、これは、幾つかの形式のＡＤＤ手順および／またはユーザ開始手順を使用して行うことができる。当然のことであるが、ユーザ／加入者３０はＩＭＥＩおよびＩＭＳＩについてネットワーク１に二者択一的に通知できる。ウエブ・インタフェースを介してまたは例えばＤＭＴＦトーンを使用して、ＰＯＳコンソールで売主が、またはエンド・ユーザ自身がこれを実行できる。

【００３１】

（Ｓ３２）では、ネットワーク３１が、例えばＩＭＳＩ／ＥＳＮ、ＭＳＩＳＤＮおよびＩＭＥＩが識別するデバイス／ユーザ／加入者を検出した場合、ネットワーク３１はデバイス３０をブートストラップする要求を第１のネットワーク・ユニット３２（例えばＤＭＳ（ＮＡＦ））に送り、本要求にＩＭＥＩ、ＩＭＳＩ（またはＥＳＮ）およびＭＳＩＳＤＮを含める。以前に述べたように、第１のネットワーク・ユニット３２または第１のネットワーク・ユニット３２のＮＡＦが、デバイスおよびユーザ／加入者情報に基づき、デバイスに向けてＧＢＡ　ＰＵＳＨを使用可能かどうかを決定する。もしそうであれば、第１のネットワーク・ユニット３２のＮＡＦ部分は、ＧＢＡ　ＰＵＳＨ手順を使用して、ＧＰＩレスポンスを要求するよう、第２のネットワーク・ユニット３３のＢＳＦ　３３ＡにＧＰＩ要求（Ｓ３３）を送信する。本要求（Ｓ３３）には、加入者を識別する情報、例えばＩＭＳＩと、少なくともＮＡＦ（ＤＭＳ＿ＮＡＳ＿Ｉｄ）のアイデンティティとを備える。ＢＳＦ　３３Ａが本要求を受信すると、それは本要求（Ｓ３４）を処理し、ユーザ／加入者を識別する。その後、ＢＳＦ　３３Ａは第２のネットワーク・ユニット３３のＨＳＳ　３３Ｂに要求（Ｓ３５）を送り、デバイス３０に対する認証ベクトル（ＡＶ）をＨＳＳ　３３Ｂに要求する。ＡＶ要求（Ｓ３５）において、ＩＭＰＩが表示される。（Ｓ３６）では、ＨＳＳ　３３Ｂは要求されたＡＶをＡＶレスポンスで返す。次に、ＢＳＦ　３３Ａは、ＤＭＳ　ＮＡＦブートストラップ・キーであるブートストラップ・キーを生成し（Ｓ３７）、本キーをストアする。（Ｓ３８）で、ＢＳＦ　３３Ａは、ブートストラップ・キーと、ＧＰＩパラメトリックを備える、少なくともＧＰＩとを備えるＧＰＩレスポンスを、第１のネットワーク・ユニット３２に送信する。第１のネットワーク・ユニット３２は本ブートストラップ・キーをストアし（Ｓ３９）、デバイス３０にＧＰＩパッケージを送信する前に、トリガ情報（即ちＧＰＩ）を備えるＧＰＩパッケージを準備する（Ｓ４０）。以前に述べたように、ＧＰＩ、例えばＷＡＰ　ＰＵＳＨを通じたＧＰＩまたはＳＭＳまたはＳＩＰ等をデバイス３０に運ぶため、任意の適当なベアラを使用できる。本デバイス

３０をアドレスするため、ＭＳＩＳＤＮを使用できる。

【００３２】

デバイス３０が本ＧＰＩを受信する場合、デバイス３０は内部的にＤＭＳ　ＮＡＦブートストラップ・キーを生成し（Ｓ４１）、デバイス３０は本ブートストラップ・キーをストアする（Ｓ４２）。その後、本ブートストラップ・キーに基づき、第１のネットワーク・ユニット３２がブートストラップ・メッセージを保護し、保護されたブートストラップ・メッセージをデバイス３０に送信する（図示せず）。次に、本デバイスはブートストラップ・メッセージを検証および／または暗号解読する。もし検証および／または暗号解読が成功すれば、ＤＭセッションがデバイスと第１のネットワーク・ユニットとの間で開始する（図示せず）。ブートストラップ・メッセージの通信過程を考慮すれば、第１のネットワーク・ユニットとデバイスとのみが本ブートストラップ・キーに気付き、それによって本デバイスをハイジャックしようとする、または本デバイスに成り済まそうとする盗聴およびアタックを防止する。

【００３３】

前に説明した典型的実施形態と同様に、第１のネットワーク・ユニットおよびデバイスの両方は、更なるキーを生成するため、本ブートストラップ・キーを使用できる。第１のネットワーク・ユニットは更なる本キーを使用してブートストラップ・メッセージを保護し、本デバイスは更なる本キーを使用して、ブートストラップ・メッセージを検証および／または暗号解読できる。

【００３４】

図４を参照すると、前に説明した本発明の典型的実施形態によるブートストラップ・メッセージの保護を可能とするため、第１のネットワーク・ユニットにおいて、本方法または手順の主要なステップが示されている。図４に示すように、本方法の主要なステップには以下のことを備える：

（４０１）デバイスを識別する情報と加入者を識別する情報とを備える第１のメッセージ（即ちデバイスをブートストラップする要求）を受信すること。

【００３５】

（４０２）加入者を識別する情報を備える第２のメッセージ（即ちＧＰＩ要求）を第２のネットワーク・ユニットに送信することであり、加入者を識別する情報に基づくブートストラップ・キーを第１のネットワーク・ユニットに提供するよう、第２のネットワーク・ユニットに要求する。

【００３６】

（４０３）ブートストラップ・メッセージの保護を可能とするため、ブートストラップ・キーとトリガ情報（即ちＧＰＩ）とを備える第３のメッセージ（即ちＧＰＩレスポンス）を第２のネットワーク・ユニットから受信すること。

【００３７】

（４０４）デバイスで内部的にブートストラップ・キーの生成を開始させるため、デバイス及び本トリガ情報を送信すること。

【００３８】

第１のネットワーク・ユニットの追加の方法のステップおよび機能についてはすでに議論したので、繰り返さない。

図５を参照すると、前に説明した本発明の典型的実施形態によるブートストラップ・メッセージの保護を可能とするため、ＤＭネットワーク・システムの典型的な第１のネットワーク・ユニット５００、例えばＤＭＳのブロック図が示されている。図５に示すように、第１のネットワーク・ユニット５００には、デバイスをブートストラップする要求を備える第１のメッセージを受信するよう構成した、受信機５１０（ＲＸ）を備える。本第１のメッセージには、デバイスと加入者とを識別する情報を備える。第１のネットワーク・ユニット５００には、加入者を識別する情報を備える第２のメッセージ（即ちＧＰＩ要求）を第２のネットワーク・ユニット（例えばＢＳＦ＋ＨＳＳ）に送信するよう構成した送信機５２０（ＴＸ）を更に備え、ブートストラップ・キーをそれに提供するよう第２のネッ

トワーク・ユニットに要求する。ブートストラップ・メッセージの保護を可能とするためブートストラップ・キーを備える第３のメッセージ（即ちＧＰＩレスポンス）を受信するよう、第１のネットワーク・ユニット５００の受信機５１０を更に構成する。第３のメッセージにはトリガ情報（即ちＧＰＩ）を更に備える。本デバイスでブートストラップ・キーの生成を開始させるため、本デバイスにトリガ情報を送信するよう、第１のネットワーク・ユニット５００の送信機５２０を更に構成する。第１のネットワーク・ユニット５００にはブートストラップ・キーをストアするための記憶手段５３０を更に備える。第１のネットワーク・ユニット５００は、ＧＢＡ　ＰＵＳＨをデバイスに向けて使用できるかどうかを決定するよう構成した処理ロジック／ユニット５４０を更に備え、ブートストラップ・メッセージを保護するため、ブートストラップ・キーに基づいて更なる／追加のキーを生成するよう更に構成される。記憶手段５３０および処理ロジック／ユニット５４０は、処理システム５５０の一部として示されているが、このことは必ずしも必要なことではない。

【００３９】

図５は第１のネットワーク・ユニット５００の典型的な構成要素を示すが、その他の実装では、第１のネットワーク・ユニット５００には、図５に示したものよりより少ないか、異なるか、または追加の構成要素を含んでもよい。更なるその他の実装では、ユニット５００の一つ以上の構成要素は、第１のネットワーク・ユニット５００の一つ以上のその他の構成要素が実行すると説明したタスクを実行してもよい。

【００４０】

図６を参照すると、本発明の幾つかの典型的な実施形態により、デバイス６００の典型的な構成要素の図が示されている。図示のように、本デバイスは、ブートストラップ・メッセージの保護を可能とするため、本デバイスと加入者とを識別する情報を、ＤＭネットワーク・システムの（図５の）第１のネットワーク・ユニットに通知する手段を備えるトランシーバ６１０を備える。本通知する手段はトランシーバ６１０の中の送信機と見ることができる。トランシーバ６１０には、本デバイスで内部的にブートストラップ・キーの生成を開始させるため、第１のネットワーク・ユニットからトリガ情報を受信するよう構成した受信機を更に備える。第１のネットワーク・ユニットがブートストラップ・キーに基づき保護した保護ブートストラップ・メッセージを受信するよう、トランシーバ６１０の中の受信機を更に構成する。また、アンテナ６２０はトランシーバ６１０に接続して示されている。本デバイス６００には、保護ブートストラップ・メッセージを検証および／または暗号解読するための手段を更に備える。ブートストラップ・キーを生成し、保護ブートストラップ・メッセージの検証／暗号解読を実行するよう、デバイス６００の処理ユニット／手段６３０を構成する。本デバイス６００には、幾つかのアンテナ（一個のアンテナ６２０のみを図示）、ブートストラップ・キーを記憶するためのメモリまたは記憶手段６４０、入力デバイス６５０、出力デバイス６６０およびバス６７０を含む可能性がある。図６はデバイス６００の典型的な構成要素を示すが、その他の実装では、デバイス６００は、図６に示すものと比べてより少ないか、異なるか、または追加の構成要素を含んでもよい。

【００４１】

本発明およびその典型的な実施形態は、多くの方法で実現可能である。例えば、本発明の一つの実施形態には、そこに記憶され、前に説明した本発明の典型的な実施形態の方法のステップを実行するよう、第１のネットワーク・ユニットのコンピュータにより実行可能なプログラム命令を持つ、コンピュータ読み取り可能媒体を含んでもよい。

【００４２】

幾つかの好ましい実施形態に関して、本発明を説明したが、特許明細書を読み、図面を検討すると、それらの代替、修正、置換および等価は当業者に明らかになるであろう、ということが考えられる。したがって、以下の添付の特許請求項には、本発明の範囲内に収まるものとしてそのような代替、修正、置換および等価を含む、ということを意図している。

【図１】

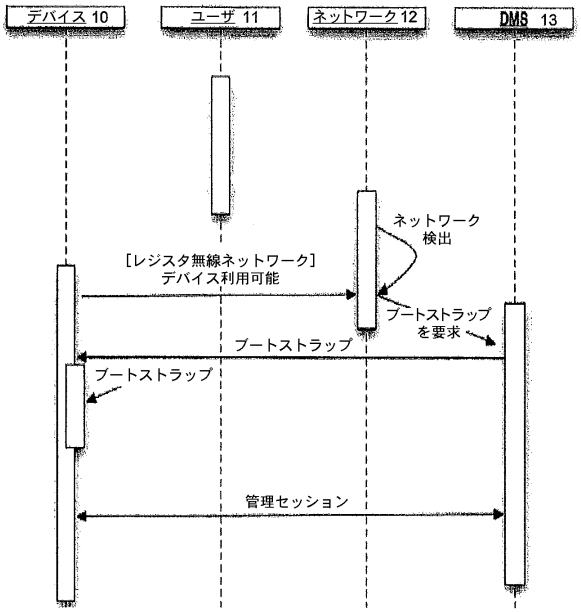


FIGURE 1

【図２】

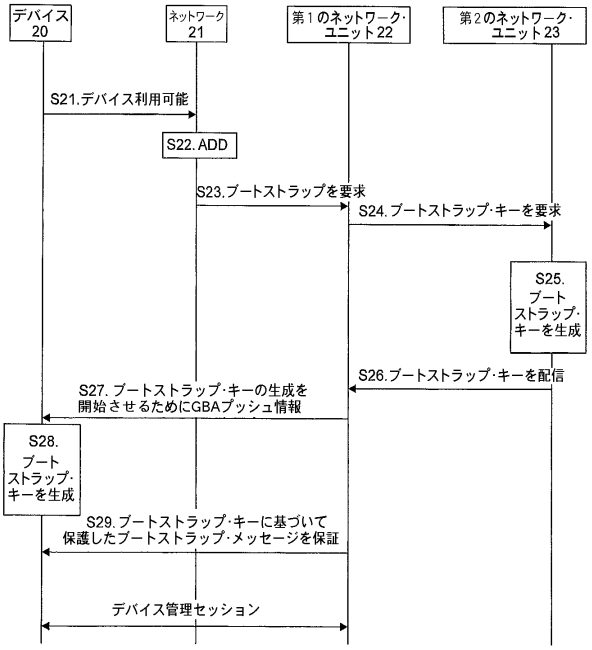


FIGURE 2

【図３】

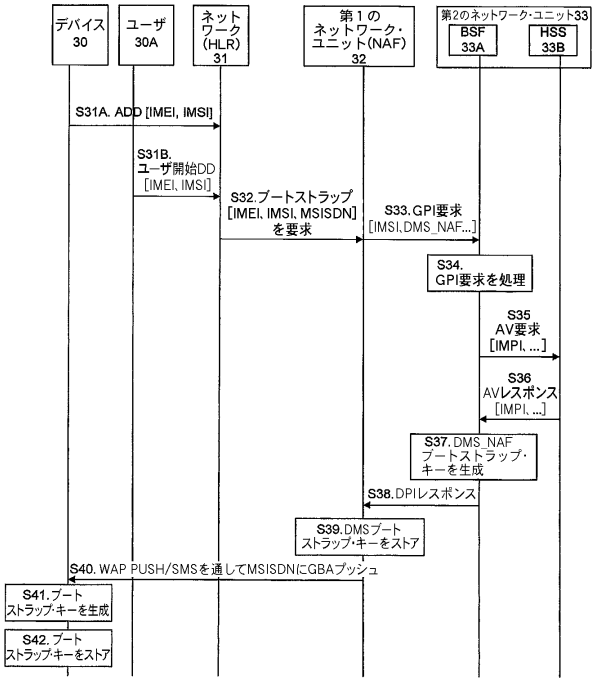


FIGURE 3

【図４】

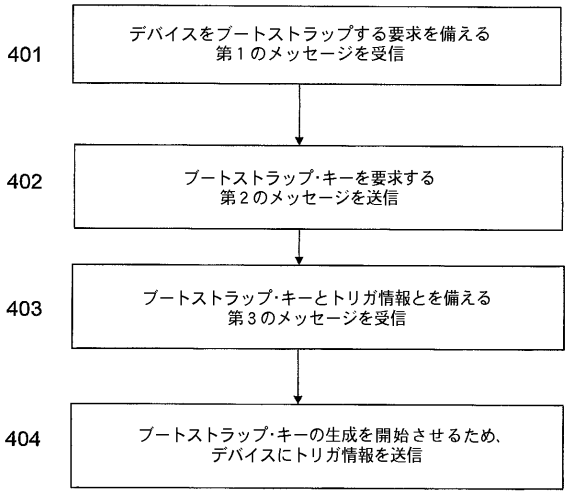


FIGURE 4

【図５】

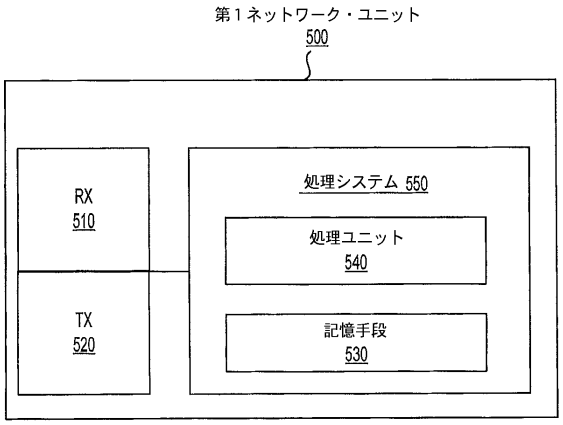


FIGURE 5

【図６】

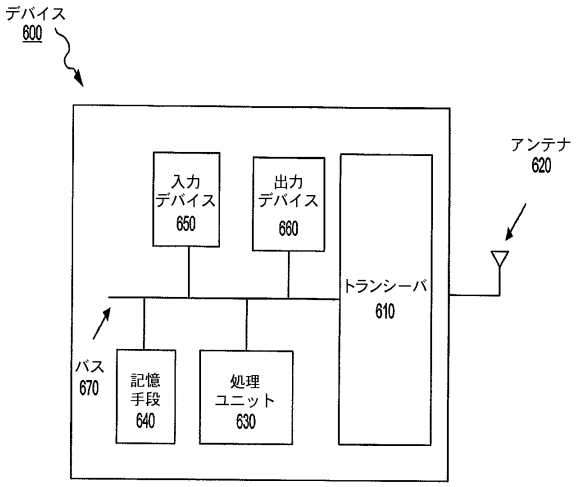


FIGURE 6

フロントページの続き

(72)発明者　バリガ，　ルイス
スウェーデン国　バンドハゲン　１２４　５５，　シェサヴェーゲン　１９　ビーヴィ
(72)発明者　ダイセニウス，　ペルーアンデシュ
スウェーデン国　カールスハムン　エス－３７４　４０，　ハガルンドスヴェーゲン　５２
(72)発明者　リンドストレム，　マグヌス
スウェーデン国　カールスクロナ　エス－３７１　９２，　メルトルプスヴェーゲン　２

審査官　青木　重徳

(56)参考文献　特表２００９－５３１７６４（ＪＰ，Ａ）
特表２００９－５１２２９６（ＪＰ，Ａ）
特表２００８－５４７２４８（ＪＰ，Ａ）
特表２００８－５３７３７０（ＪＰ，Ａ）
国際公開第２００８／００４１０６（WO，Ａ１）
国際公開第２０１０／０１２３１８（WO，Ａ１）
国際公開第２００９／００４５９０（WO，Ａ１）
国際公開第２００７／０６３４２０（WO，Ａ１）
米国特許出願公開第２００７／０１０１１２２（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　９／０８
Ｈ０４Ｌ　　９／３２
Ｈ０４Ｗ　１２／０８