【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成20年10月2日(2008.10.2)

【公表番号】特表2008-532114(P2008-532114A)
【公表日】平成20年8月14日(2008.8.14)
【年通号数】公開・登録公報2008-032
【出願番号】特願2007-554663(P2007-554663)
【国際特許分類】
Ｇ０６Ｆ　13/00　　(2006.01)
Ｈ０４Ｑ　 7/38　　(2006.01)
【ＦＩ】
Ｇ０６Ｆ　13/00　　５００Ａ
Ｈ０４Ｂ　 7/26　　１０９Ｒ

【手続補正書】
【提出日】平成20年8月14日(2008.8.14)
【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】
ホーム加入者サーバ（ＨＳＳ）に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に対応するタイムスタンプ・パラメータと比較される、それ自体に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ＧＵＳＳ）に対応するタイムスタンプ・パラメータを含む第１のメッセージを送信し、それ自体の前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータと、前記ホーム加入者サーバの前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータとが等しい場合は、前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定を含まない第２のメッセージを受信するように構成されたサーバ・ブートストラッピング機能（ＢＳＦ）を備えた装置。
【請求項２】
前記ＢＳＦは、前記ＢＳＦの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータと、前記ＨＳＳの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータとが等しくない場合は、前記ＧＵＳＳと前記対応するタイムスタンプ・パラメータとを含む前記第２のメッセージを前記ＨＳＳから受信するように構成されている、請求項１に記載の装置。
【請求項３】
特定のＧＵＳＳに対応する前記タイムスタンプ・パラメータは、同一のＧＵＳＳの一部となる、請求項１に記載の装置。
【請求項４】
前記ＢＳＦは、前記ＨＳＳからの前記第２のメッセージと、前記ＧＵＳＳと、前記ＧＵＳＳに関連する前記タイムスタンプ・パラメータとを受信し、前記ＨＳＳからの前記ＧＵＳＳと、前記タイムスタンプ・パラメータとを更新するように構成されている、請求項２に記載の装置。
【請求項５】
前記第１のメッセージは、認証ベクトル（ＡＶ）要求を含む、請求項１に記載の装置。
【請求項６】

前記ＨＳＳは、前記タイムスタンプ・パラメータを前記ＧＵＳＳに割り当てるように構成されている、請求項１に記載の装置。
【請求項７】
前記ＨＳＳは、前記ＧＵＳＳのデータが修正された場合は、当該ＧＵＳＳの前記タイムスタンプ・パラメータを変更するように構成されている、請求項１に記載の装置。
【請求項８】
前記ＨＳＳは、前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを単調増加順又は単調減少順で割り当てるように構成されている、請求項６に記載の装置。
【請求項９】
前記ＨＳＳは、前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを、前記ＢＳＦ及び前記ＨＳＳの前記ＧＵＳＳの特定のインスタンスに関するハッシュとして又は前記ハッシュの一部として割り当てるように構成されている、請求項６に記載の装置。
【請求項１０】
前記ＢＳＦは、前記タイムスタンプ・パラメータを、前記ＨＳＳに記憶されている前記タイムスタンプ・パラメータに由来する異なる数字又は英数字の形式で記憶するように構成されている、請求項１に記載の装置。
【請求項１１】
前記ＢＳＦは、前記タイムスタンプ・パラメータを、前記ＨＳＳの前記タイムスタンプ・パラメータに由来する異なる数字又は英数字の形式で送信するように構成されている、請求項１に記載の装置。
【請求項１２】
前記タイムスタンプは、前記ＧＵＳＳが最初に作成されるときに、ある数値に初期化され、又は前記ＨＳＳ内のクロックによって指示される時間及び／又は日付を示す値に初期化される、請求項６に記載の装置。
【請求項１３】
前記ＧＵＳＳが修正されるたびに、前記ＧＵＳＳは新しいバージョンになり、前記タイムスタンプは１ずつ増分又は減分され、あるいは前記ＨＳＳ内のクロックによって指示される現在の時間及び／又は日付に変更される、請求項６に記載の装置。
【請求項１４】
前記ＧＵＳＳには、前記ＧＵＳＳの特定のインスタンスに関するハッシュに相当する又は当該ハッシュの一部に相当するタイムスタンプ値が割り当てられる、請求項６に記載の装置。
【請求項１５】
ホーム加入者サーバ（ＨＳＳ）に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に対応するタイムスタンプ・パラメータと比較される、サーバ・ブートストラッピング機能（ＢＳＦ）に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ＧＵＳＳ）に対応するタイムスタンプ・パラメータを含む第１のメッセージを、前記サーバ・ブートストラッピング機能から前記ホーム加入者サーバに送信するステップと、
前記サーバ・ブートストラッピング機能の前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータと、前記ホーム加入者サーバの前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータとが等しい場合は、前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定を含まない第２のメッセージを前記サーバ・ブートストラッピング機能において受信するステップと、
を含む方法。
【請求項１６】
前記ＢＳＦの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータと、前記ＨＳＳの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータとが等しくない場合は、前記ＧＵＳＳと前記対応するタイムスタンプ・パラメータとを含む前記第２のメッセージを前記Ｈ

ＳＳから前記ＢＳＦに送信するステップ
を更に含む、請求項１５に記載の方法。
【請求項１７】
前記ＢＳＦにおいて、前記ＨＳＳからの前記第２のメッセージと、前記ＧＵＳＳと、前記ＧＵＳＳに関連する前記タイムスタンプ・パラメータとを受信するステップと、
前記ＢＳＦにおいて、前記ＨＳＳからの前記ＧＵＳＳと、前記タイムスタンプ・パラメータとを更新するステップと、
を更に含む、請求項１６に記載の方法。
【請求項１８】
前記第１のメッセージを送信する前記ステップは、認証ベクトル（ＡＶ）要求を送信するステップを含む、請求項１５に記載の方法。
【請求項１９】
前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを割り当てる前記ステップは、単調増加順又は単調減少順で実行される、請求項１５に記載の方法。
【請求項２０】
前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを割り当てる前記ステップは、前記ＢＳＦ及び前記ＨＳＳの前記ＧＵＳＳの特定のインスタンスに関するハッシュとして又は前記ハッシュの一部として実行される、請求項１５に記載の方法。
【請求項２１】
前記ＢＳＦの前記タイムスタンプ・パラメータを、前記ＨＳＳに記憶されている前記タイムスタンプ・パラメータに由来する異なる数字又は英数字の形式で記憶するステップ
を更に含む、請求項１５に記載の方法。
【請求項２２】
前記ＢＳＦの前記タイムスタンプ・パラメータと、前記ＨＳＳのタイムスタンプ・パラメータとを異なる数字又は英数字の形式で送信するステップ
を更に含む、請求項１５に記載の方法。
【請求項２３】
異なる数字又は英数字の形式で送信された前記タイムスタンプ・パラメータをそれ自体の元の形式に変更するステップ
を更に含む、請求項１５に記載の方法。
【請求項２４】
前記タイムスタンプに単調増加順又は単調減少順で値を割り当てるステップ
を更に含む、請求項１５に記載の方法。
【請求項２５】
前記ＧＵＳＳが最初に作成されるときに、前記タイムスタンプをある数値に初期化し、又は前記ＨＳＳ内のクロックによって指示される時間及び／又は日付に初期化するステップ
を更に含む、請求項１５に記載の方法。
【請求項２６】
前記タイムスタンプを１ずつ増分又は減分し、あるいは前記タイムスタンプを、前記ＧＵＳＳが修正されることによって例えば新しいバージョンのＧＵＳＳＴＩＭＥＳＴＡＭＰになるたびに増分又は減分するステップ
を更に含む、請求項１５に記載の方法。
【請求項２７】
前記タイムスタンプを、前記ＧＵＳＳが修正されるたびに前記タイムスタンプの現在の時間及び／又は日付に変更するステップ
を更に含む、請求項１５に記載の方法。
【請求項２８】
前記ＧＵＳＳの特定のインスタンスに関するハッシュに相当する又は当該ハッシュの一部に相当するタイムスタンプ値を前記ＧＵＳＳに割り当てるステップ

を更に含む、請求項１５に記載の方法。
【請求項２９】
コンピュータ可読媒体内に実装されたコンピュータ・プログラムであって、
ホーム加入者サーバ（ＨＳＳ）に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に対応するタイムスタンプ・パラメータと比較される、サーバ・ブートストラッピング機能（ＢＳＦ）に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ＧＵＳＳ）に対応するタイムスタンプ・パラメータを含む第１のメッセージを、前記サーバ・ブートストラッピング機能から前記ホーム加入者サーバに送信するステップと、
前記サーバ・ブートストラッピング機能の前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータと、前記ホーム加入者サーバの前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータとが等しい場合は、前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定を含まない第２のメッセージを前記サーバ・ブートストラッピング機能において受信するステップと、
を実行するようプロセッサを制御するコンピュータ・プログラム。
【請求項３０】
前記ＢＳＦの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータと、前記ＨＳＳの前記ＧＵＳＳに関する前記タイムスタンプ・パラメータとが等しくない場合は、前記ＧＵＳＳと前記対応するタイムスタンプ・パラメータとを含む前記メッセージを前記ＨＳＳから前記ＢＳＦに送信するステップ
を更に含む、請求項２９に記載のコンピュータ・プログラム。
【請求項３１】
前記ＢＳＦが、前記ＨＳＳからの前記メッセージと、前記ＧＵＳＳと、前記ＧＵＳＳに関連する前記タイムスタンプ・パラメータとを受信するステップと、
前記ＢＳＦにおいて、前記ＨＳＳからの前記ＧＵＳＳと、前記タイムスタンプ・パラメータとを更新するステップと、
を更に含む、請求項２９に記載のコンピュータ・プログラム。
【請求項３２】
前記第１のメッセージを送信する前記ステップは、認証ベクトル（ＡＶ）要求を送信するステップを含む、請求項２９に記載のコンピュータ・プログラム。
【請求項３３】
前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを割り当てる前記ステップは、単調増加順又は単調減少順で実行される、請求項２９に記載のコンピュータ・プログラム。
【請求項３４】
前記ＧＵＳＳに関する前記タイムスタンプ・パラメータを割り当てる前記ステップは、前記ＢＳＦ及び前記ＨＳＳの前記ＧＵＳＳの特定のインスタンスに関するハッシュとして又は前記ハッシュの一部として実行される、請求項２９に記載のコンピュータ・プログラム。
【請求項３５】
前記ＢＳＦの前記タイムスタンプ・パラメータを、前記ＨＳＳに記憶されている前記タイムスタンプ・パラメータに由来する異なる数字又は英数字の形式で記憶するステップ
を更に含む、請求項２９に記載のコンピュータ・プログラム。
【請求項３６】
前記ＢＳＦの前記タイムスタンプ・パラメータと、前記ＨＳＳのタイムスタンプ・パラメータとを異なる数字又は英数字の形式で送信するステップ
を更に含む、請求項２９に記載のコンピュータ・プログラム。
【請求項３７】
前記タイムスタンプに単調増加順又は単調減少順で値を割り当てるステップ

を更に含む、請求項２９に記載のコンピュータ・プログラム。
【請求項３８】
前記ＧＵＳＳが最初に作成されるときに、前記タイムスタンプをある数値に初期化し、又は前記ＨＳＳ内のクロックによって指示される時間及び／又は日付に初期化するステップ
を更に含む、請求項２９に記載のコンピュータ・プログラム。
【請求項３９】
前記タイムスタンプを１ずつ増分又は減分し、あるいは前記タイムスタンプを前記ＧＵＳＳが修正され新しいバージョンになるたびに増分又は減分するステップ
を更に含む、請求項２９に記載のコンピュータ・プログラム。
【請求項４０】
前記タイムスタンプを、前記ＧＵＳＳが修正されるたびに現在の時間及び／又は日付に変更するステップ
を更に含む、請求項２９に記載のコンピュータ・プログラム。
【請求項４１】
前記ＧＵＳＳの特定のインスタンスに関するハッシュに相当する又は当該ハッシュの一部に相当するタイムスタンプ値を前記ＧＵＳＳに割り当てるステップ
を更に含む、請求項２９に記載のコンピュータ・プログラム。
【請求項４２】
通信システムであって、
ネットワーク・アプリケーション機能（ＮＡＦ）と、
前記ネットワーク・アプリケーション機能と通信し、認証情報要求を送信するように構成されたユーザ機器と、
前記要求を受信し、それ自体に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ＧＵＳＳ）に対応するタイムスタンプ・パラメータを含む第１のメッセージを送信するように構成されたサーバ・ブートストラッピング機能（ＢＳＦ）と、
前記第１のメッセージを受信し、前記サーバ・ブートストラッピング機能に記憶されている前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に対応する前記タイムスタンプ・パラメータと、それ自体に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に対応するタイムスタンプ・パラメータとを比較し、前記サーバ・ブートストラッピング機能の前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータと、それ自体の前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータとが等しい場合は、前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定を含まない第２のメッセージを前記サーバ・ブートストラッピング機能に送り返すように構成されたホーム加入者サーバ（ＨＳＳ）と、
を備える通信システム。
【請求項４３】
ホーム加入者サーバ（ＨＳＳ）に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に対応するタイムスタンプ・パラメータと比較される、サーバ・ブートストラッピング機能（ＢＳＦ）に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ＧＵＳＳ）に対応するタイムスタンプ・パラメータを含む第１のメッセージを、前記サーバ・ブートストラッピング機能から前記ホーム加入者サーバに送信する送信手段と、
前記サーバ・ブートストラッピング機能の前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータと、前記ホーム加入者サーバの前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータとが等しい場合は、前記汎用ブートスト

ラッピング・アーキテクチャ・ユーザ・セキュリティ設定を含まない第２のメッセージを前記サーバ・ブートストラッピング機能において受信する受信手段と、
を含む装置。
【請求項４４】
サーバ・ブートストラッピング機能（ＢＳＦ）に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定（ＧＵＳＳ）に対応するタイムスタンプ・パラメータを含む第１のメッセージを受信し、前記サーバ・ブートストラッピング機能に記憶されている前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に対応する前記タイムスタンプ・パラメータをそれ自体に記憶されている汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に対応するタイムスタンプ・パラメータと比較し、前記サーバ・ブートストラッピング機能の前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータとそれ自体の前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定に関する前記タイムスタンプ・パラメータとが等しい場合は、前記汎用ブートストラッピング・アーキテクチャ・ユーザ・セキュリティ設定を含まない第２のメッセージを前記サーバ・ブートストラッピング機能に送り返すように構成されたホーム加入者サーバ（ＨＳＳ）を備えた装置。