【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７部門第３区分
【発行日】平成25年7月4日(2013.7.4)

【公表番号】特表2012-527830(P2012-527830A)
【公表日】平成24年11月8日(2012.11.8)
【年通号数】公開・登録公報2012-046
【出願番号】特願2012-511889(P2012-511889)
【国際特許分類】
Ｈ０４Ｌ　9/08　(2006.01)
Ｇ０６Ｆ　21/34　(2013.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６０１Ａ
Ｈ０４Ｌ　9/00　６０１Ｅ
Ｈ０４Ｌ　9/00　６０１Ｆ
Ｇ０６Ｆ　21/20　１３４

【手続補正書】
【提出日】平成25年5月15日(2013.5.15)
【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】
信頼性のないネットワークに接続されている安全でないコンピューティングデバイスのために、信頼性のあるネットワークに接続されている第１の信頼性のあるコンピューティングデバイスを用いて安全なオンライン環境を形成する方法であって、
前記第１の信頼性のあるコンピューティングデバイスに有効に結合されている間の携帯用記憶デバイスを用いて、オンライン・アクセスのために第１の信頼性のあるネットワークを用いる前記第１の信頼性のあるコンピューティングデバイス上においてプロキシー・サーバーをインストールするステップと、
第２の信頼性のあるコンピューティングデバイスに有効に結合されている間の前記携帯用記憶デバイスを用いて、オンライン・アクセスのために第２の信頼性のあるネットワークを用いる前記第２の信頼性のあるコンピューティングデバイス上において前記プロキシー・サーバーをインストールするステップと、
前記プロキシー・サーバーがインストールされた前記第１の信頼性のあるコンピューティングデバイスおよび前記第２の信頼性のあるコンピューティングデバイスに１つ以上の共有暗号鍵を発生するステップと、
信頼性のないネットワークに接続されている安全でないコンピューティングデバイスに有効に結合されている間の前記携帯用記憶デバイスのプロキシー・サーバー・プロトコルを用いて、前記安全でないコンピューティングデバイスを信頼性のあるデバイスのウェブサイトに接続するステップであって、前記信頼性のあるデバイスのウェブサイトは、信頼性のあるコンピューティングデバイスのリストを含み、前記リストは、少なくとも前記第１の信頼性のあるコンピューティングデバイスと前記第２の信頼性のあるコンピューティングデバイスとを含む、ステップと、
前記リストから前記第１の信頼性のあるコンピューティングデバイスを選択することに応じ、前記携帯用記憶デバイスの前記プロキシー・サーバー・プロトコルを用いて、前記安全でないコンピューティングデバイスと前記第１の信頼性のあるコンピューティングデ

バイスとの間に前記共有暗号化鍵の少なくともいくつかを用いて安全な接続を形成するステップと、
を備え、前記第１の信頼性のあるコンピューティングデバイス上においてプロキシー・サーバーをインストールする前記ステップ、前記第２の信頼性のあるコンピューティングデバイス上において前記プロキシー・サーバーをインストールする前記ステップ、前記発生するステップ、前記接続するステップ、又は前記形成するステップのうちの少なくとも１つは、少なくとも部分的に処理ユニットによって実現される、方法。
【請求項２】
請求項１記載の方法にであって、前記携帯用記憶デバイスに１つ以上の共有暗号鍵を発生するステップを備えている、方法。
【請求項３】
請求項１記載の方法であって、安全な接続を形成する前記ステップは、前記携帯用記憶デバイス内に記憶された第１の共有暗号鍵を用いて、前記安全でないコンピューティングデバイスによって前記第１の信頼性のあるコンピューティングデバイスへ送信されるデータを暗号化するステップを含み、前記第１の共有暗号鍵は、前記第１の信頼性のあるコンピューティングデバイス上に保持された第２の共有暗号鍵に対応する、方法。
【請求項４】
請求項１記載の方法であって、信頼性のあるコンピューティングデバイスの前記リストは、前記第１の信頼性のあるコンピューティングデバイスが、前記第２の信頼性のあるコンピューティングデバイスの第２の接続速度よりも高速な第１の接続速度を有することを示す推薦を含む、方法。
【請求項５】
請求項１記載の方法であって、信頼性のあるコンピューティングデバイスの前記リストは、前記第１の信頼性のあるコンピューティングデバイスが、前記安全でないコンピューティングデバイスに対する前記第２の信頼性のあるコンピューティングデバイスの第２の近接度よりも近い前記安全でないコンピューティングデバイスに対する第１の近接度を有することを示す推薦を含む、方法。
【請求項６】
請求項１記載の方法であって、信頼性のあるコンピューティングデバイスの前記リストは、前記第１の信頼性のあるコンピューティングデバイスが、前記第２の信頼性のあるコンピューティングデバイスが含んでいないプログラム又はファイルのうちの少なくとも１つを含んでいることを示す推薦を含む、方法。
【請求項７】
請求項１記載の方法であって、前記信頼性のないネットワークを用いている前記安全でないコンピューティングデバイスのために、前記信頼性のあるネットワークを用いている前記第１の信頼性のあるコンピューティングデバイスによって、データ・トラフィックを仲介するステップを備えている、方法。
【請求項８】
請求項７記載の方法において、前記安全でないコンピューティングデバイスのためにデータ・トラフィックを仲介する前記ステップが、
前記安全でないコンピューティングデバイスから前記第１の信頼性のあるコンピューティングデバイスを介して前記信頼性のあるネットワークへのアウトバウンド・データ・トラフィックを仲介するステップと、
前記信頼性のあるネットワークから前記第１の信頼性のあるコンピューティングデバイスを介して前記安全でないコンピューティングデバイスへのインバウンド・データ・トラフィックを仲介するステップと、
を備えている、方法。
【請求項９】
請求項１記載の方法において、前記第１の信頼性のあるコンピューティングデバイスに前記１つ以上の共有暗号鍵のうちの少なくともいくつかを発生する前記ステップが、

前記第１の信頼性のあるコンピューティングデバイスに公開／秘密鍵対を発生するステップと、
前記秘密鍵を前記第１の信頼性のあるコンピューティングデバイスに格納するステップと、
前記公開鍵を前記携帯用記憶デバイスに書き込むステップと、
を備えている、方法。
【請求項１０】
信頼性のないネットワークに接続されている安全でないコンピューティングデバイスのために、信頼性のあるネットワークに接続されている第１の信頼性のあるコンピューティングデバイスを用いて安全なオンライン環境を形成するシステムであって、
携帯用記憶デバイス内のプロキシー・サーバー・インストーラーであって、
前記第１の信頼性のあるコンピューティングデバイスに有効に結合されている間の前記携帯用記憶デバイスを用いて、オンライン・アクセスのために第１の信頼性のあるネットワークを用いる前記第１の信頼性のあるコンピューティングデバイス上においてプロキシー・サーバーをインストールし、
第２の信頼性のあるコンピューティングデバイスに有効に結合されている間の前記携帯用記憶デバイスを用いて、オンライン・アクセスのために第２の信頼性のあるネットワークを用いる前記第２の信頼性のあるコンピューティングデバイス上において前記プロキシー・サーバーをインストールする、
ように構成されているプロキシー・サーバー・インストーラーと、
前記携帯用記憶デバイス内の暗号鍵発生器であって、前記プロキシー・サーバーがインストールされた前記第１の信頼性のあるコンピューティングデバイスおよび前記第２の信頼性のあるコンピューティングデバイスに１つ以上の共有暗号鍵を発生するように構成されている暗号鍵発生器と、
前記携帯用記憶デバイス内のオンライン集中リダイレクターであって、
信頼性のないネットワークに接続されている安全でないコンピューティングデバイスに有効に結合されている間の前記携帯用記憶デバイスのプロキシー・サーバー・プロトコルを用いて、前記安全でないコンピューティングデバイスを信頼性のあるデバイスのウェブサイトに接続するように構成され、前記信頼性のあるデバイスのウェブサイトは、信頼性のあるコンピューティングデバイスのリストを含み、前記リストは、少なくとも前記第１の信頼性のあるコンピューティングデバイスと前記第２の信頼性のあるコンピューティングデバイスとを含む、オンライン集中リダイレクターと、
前記携帯用記憶デバイス内の安全接続発生器であって、
前記リストから前記第１の信頼性のあるコンピューティングデバイスを選択することに応じ、前記携帯用記憶デバイスの前記プロキシー・サーバー・プロトコルを用いて、前記安全でないコンピューティングデバイスと前記第１の信頼性のあるコンピューティングデバイスとの間に、前記信頼性のないネットワークを通じて前記共有暗号鍵の少なくともいくつかを利用して安全な接続を形成するように構成されているプロキシー・サーバー起動部を備えている安全接続発生器と、
を備え、前記プロキシー・サーバー・インストーラー、前記暗号鍵発生器、前記オンライン集中リダイレクター、又は前記安全接続発生器のうちの少なくとも１つは、少なくとも部分的に処理ユニットによって実現される、システム。
【請求項１１】
請求項１０記載のシステムにおいて、信頼性のあるコンピューティングデバイスの前記リストは、前記第１の信頼性のあるコンピューティングデバイスが、前記第２の信頼性のあるコンピューティングデバイスの第２の接続速度よりも高速な第１の接続速度を有することを示す推薦を含む、システム。
【請求項１２】
請求項１０記載のシステムにおいて、信頼性のあるコンピューティングデバイスの前記リストは、前記第１の信頼性のあるコンピューティングデバイスが、前記安全でないコン

ピューティングデバイスに対する前記第２の信頼性のあるコンピューティングデバイスの第２の近接度よりも近い前記安全でないコンピューティングデバイスに対する第１の近接度を有することを示す推薦を含む、システム。

【請求項１３】

請求項１０記載のシステムにおいて、信頼性のあるコンピューティングデバイスの前記リストは、前記第１の信頼性のあるコンピューティングデバイスが、前記第２の信頼性のあるコンピューティングデバイスが含んでいないプログラム又はファイルのうちの少なくとも１つを含んでいることを示す推薦を含む、システム。

【請求項１４】

請求項１０記載のシステムにおいて、前記暗号鍵発生器は、前記携帯用記憶デバイスに１つ以上の共有暗号鍵を発生するように構成されている、システム。

【請求項１５】

請求項１０記載のシステムにおいて、前記安全でないコンピューティングデバイスと前記第１の信頼性のあるコンピューティングデバイスとの間における前記安全な接続が、前記信頼性のないネットワークを用いている前記安全でないコンピューティングデバイスのために、前記信頼性のあるネットワークを用いている前記第１の信頼性のあるコンピューティングデバイスを通じて、データ・トラフィックを仲介するように構成されている、システム。