【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20年4月3日(2008.4.3)

【公開番号】特開2005-295509(P2005-295509A)
【公開日】平成17年10月20日(2005.10.20)
【年通号数】公開・登録公報2005-041
【出願番号】特願2005-38373(P2005-38373)
【国際特許分類】
Ｈ０４Ｌ　9/32　(2006.01)
Ｇ０６Ｆ　13/00　(2006.01)
Ｇ０６Ｆ　21/20　(2006.01)
Ｈ０４Ｌ　9/08　(2006.01)
【ＦＩ】
Ｈ０４Ｌ　9/00　６７５Ａ
Ｇ０６Ｆ　13/00　６１０Ｓ
Ｇ０６Ｆ　15/00　３３０Ｂ
Ｈ０４Ｌ　9/00　６０１Ｆ

【手続補正書】
【提出日】平成20年2月15日(2008.2.15)
【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】
デジタルオブジェクトの送信者を認証するための方法であって、
第１のユニークな識別子（ＵＩＤ）を生成するステップと、
既に知られたアドレスに、電子メールプロトコルを介して、前記第１のＵＩＤを備える第１のメッセージを送信するステップと、
前記電子メールプロトコルを介して、第２のＵＩＤ、および前記第１のＵＩＤのコピーを備える、第２のメッセージを受信するステップと、
前記既に知られたアドレスに、前記電子メールプロトコルを介して、前記第２のＵＩＤのコピーを備える第３のメッセージを送信するステップとを備え、
前記既に知られたアドレスに送信された前記メッセージのうち少なくとも１つは、前記デジタルオブジェクトをさらに備えることを特徴とする方法。
【請求項２】
前記第１のメッセージは前記デジタルオブジェクトをさらに備えることを特徴とする請求項１に記載の方法。
【請求項３】
前記第３のメッセージは前記デジタルオブジェクトをさらに備えることを特徴とする請求項１に記載の方法。
【請求項４】
前記デジタルオブジェクトは暗号化システムのためのパブリックキーであることを特徴とする請求項１に記載の方法。
【請求項５】
前記第２のメッセージは、暗号化システムのための第２のパブリックキーをさらに備えることを特徴とする請求項４に記載の方法。

【請求項６】
前記電子メールプロトコルは、簡易メール転送プロトコル（ＳＭＴＰ）を操作するメールサーバーを備えることを特徴とする請求項１に記載の方法。
【請求項７】
前記電子メールプロトコルの少なくとも一部は、トランスポート層セキュリティ（ＴＬＳ）プロトコルを使用して安全に動作することを特徴とする請求項１に記載の方法。
【請求項８】
前記第１のＵＩＤは少なくとも１２８ビットを含むことを特徴とする請求項１に記載の方法。
【請求項９】
デジタルオブジェクトの送信者を認証するための方法であって、
電子メールプロトコルを介して、第１のユニークな識別子（ＵＩＤ）を備える第１のメッセージを受信するステップと、
第２のＵＩＤを生成するステップと、
前記第１のメッセージの送り先の既に知られたアドレスに、前記電子メールプロトコルを介して、前記第２のＵＩＤ、および前記第１のＵＩＤのコピーを備える、第２のメッセージを送信するステップと、
前記電子メールプロトコルを介して、前記第２のＵＩＤのコピーを備える第３のメッセージを受信するステップとを備え、
受信された前記メッセージのうち少なくとも１つは前記デジタルオブジェクトをさらに備えることを特徴とする方法。
【請求項１０】
前記第１のメッセージは前記デジタルオブジェクトをさらに備えることを特徴とする請求項９に記載の方法。
【請求項１１】
前記第３のメッセージは前記デジタルオブジェクトをさらに備えることを特徴とする請求項９に記載の方法。
【請求項１２】
前記デジタルオブジェクトは暗号化システムのためのパブリックキーであることを特徴とする請求項９に記載の方法。
【請求項１３】
第２の電子メールメッセージは、暗号化システムのための第２のパブリックキーをさらに備えることを特徴とする請求項１２に記載の方法。
【請求項１４】
前記電子メールプロトコルは、簡易メール転送プロトコル（ＳＭＴＰ）を操作するメールサーバーを備えることを特徴とする請求項９に記載の方法。
【請求項１５】
前記電子メールプロトコルの少なくとも一部は、トランスポート層セキュリティ（ＴＬＳ）プロトコルを使用して安全に動作することを特徴とする請求項９に記載の方法。
【請求項１６】
前記第１のＵＩＤは少なくとも１２８ビットを含むことを特徴とする請求項９に記載の方法。
【請求項１７】
デジタルオブジェクトの送信者の認証を実行するコンピュータ実行可能命令を含むコンピュータ可読メディアであって、コンピュータ実行可能命令は、
第１のユニークな識別子（ＵＩＤ）を生成するステップと、
既に知られたアドレスに、電子メールプロトコルを介して、前記第１のＵＩＤを備える第１のメッセージを送信するステップと、
前記電子メールプロトコルを介して、第２のＵＩＤ、および前記第１のＵＩＤのコピーを備える、第２のメッセージを受信するステップと、

前記既に知られたアドレスに、前記電子メールプロトコルを介して、前記第２のＵＩＤのコピーを備える第３のメッセージを送信するステップとを実行し、
前記既に知られたアドレスに送信された前記メッセージのうち少なくとも１つは、前記デジタルオブジェクトをさらに備えることを特徴とするコンピュータ可読媒体。
【請求項１８】
前記デジタルオブジェクトは暗号化システムのためのパブリックキーであることを特徴とする請求項１７に記載のコンピュータ可読媒体。
【請求項１９】
前記第２のメッセージは、暗号化システムのための第２のパブリックキーをさらに備えることを特徴とする請求項１８に記載のコンピュータ可読媒体。
【請求項２０】
デジタルオブジェクトの送信者を認証するための装置であって、
第１のユニークな識別子（ＵＩＤ）を生成する乱数ジェネレータと、
既に知られたアドレスに、電子メールプロトコルを介して、前記第１のＵＩＤを備える第１のメッセージを送信するネットワークインターフェイスと、
前記電子メールプロトコルを介して、第２のＵＩＤ、および前記第１のＵＩＤのコピーを備える、第２のメッセージを受信する前記ネットワークインターフェイスと、
前記既に知られたアドレスに、前記電子メールプロトコルを介して、前記第２のＵＩＤのコピーを備える第３のメッセージを送信する前記ネットワークインターフェイスとを備え、
前記既に知られたアドレスに送信された前記メッセージのうち少なくとも１つは、前記デジタルオブジェクトをさらに備えることを特徴とする装置。