

【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 23 年 7 月 14 日 (2011.7.14)

【公開番号】特開 2010-273311 (P2010-273311A)
 【公開日】平成 22 年 12 月 2 日 (2010.12.2)
 【年通号数】公開・登録公報 2010-048
 【出願番号】特願 2009-139648 (P2009-139648)
 【国際特許分類】

H 0 4 L 9/14 (2006.01)
 G 0 6 F 13/00 (2006.01)
 G 0 6 F 21/24 (2006.01)
 H 0 4 L 9/08 (2006.01)

【F I】

H 0 4 L 9/00 6 4 1
 G 0 6 F 13/00 6 1 0 S
 G 0 6 F 12/14 5 4 0 P
 G 0 6 F 12/14 5 4 0 A
 H 0 4 L 9/00 6 0 1 C

【手続補正書】
 【提出日】平成 23 年 5 月 26 日 (2011.5.26)
 【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】

返信メールではない新規メールと、返信メールと、返信メールの作成元の電子メールである作成元メールとを記憶装置に記憶する、電子メールの暗号化と復号化を制御するメール暗号復号制御装置であって、

前記新規メールを生成する場合に、前記新規メールを暗号化及び復号するための共通鍵データを生成する共通鍵データ生成手段と、

前記共通鍵データ生成手段で生成した共通鍵データを用いて、前記新規メールを暗号化する第 1 の暗号化手段と、

返信メールを生成する場合に、前記作成元メールから得られる共通鍵データを用いて、前記返信メールを暗号化する第 2 の暗号化手段と、

記憶装置に記憶されたメールの中より、前記新規メールから前記返信メールまでのスレッドに含まれる電子メールであって、共通鍵データを未取得の電子メールを特定して抽出する抽出手段と、

前記抽出手段で抽出した電子メールから得られる共通鍵データを用いて、受信した暗号化メールを復号する復号手段と

を備え、

前記第 2 の暗号化手段は、前記復号手段で復号した電子メールを作成元とする返信メールを暗号化することを特徴とするメール暗号復号制御装置。

【請求項 2】

前記第 1 の暗号化手段、及び、前記第 2 の暗号化手段で電子メールを暗号化する際に用いられる前記共通鍵データは、前記共通鍵データの取得元である電子メール毎に異なることを特徴とする請求項 1 に記載のメール暗号復号制御装置。

【請求項 3】

前記共通鍵データ生成手段は、前記第 1 の暗号化手段で前記スレッドの最初のメールである前記新規メールを暗号化する際に用いる共通鍵データであるルートメールを生成することを特徴とする請求項 1 又は 2 に記載のメール暗号復号制御装置。

【請求項 4】

前記抽出手段は、前記記憶装置に記憶された電子メールの中より、前記新規メールから、前記受信した暗号化メールの作成元メールである前記返信メールに至るまでの電子メールを特定して、前記スレッドより抽出することを特徴とし、

前記復号手段は、前記抽出手段で抽出した前記新規メールから前記返信メールまでのスレッドに含まれる電子メールより得られる共通鍵データ、及び、前記共通鍵データ生成手段で生成した共通鍵とを用いて、前記受信した暗号化メールを復号することを特徴とする請求項 1 乃至 3 のいずれか 1 項に記載のメール暗号復号制御装置。

【請求項 5】

前記返信メールを送信する場合に、前記作成元メールの宛先及び送信元に設定されていないメールアドレスが、当該返信メールの宛先に新規に追加されたかを判定する判定手段と

、前記判定手段で、返信メールの宛先に当該メールアドレスが追加されたと判定された場合に、当該追加された宛先に対して、前記新規メールから前記返信メールまでのスレッドに含まれる電子メールを送信する送信手段と

を更に備えることを特徴とする請求項 1 乃至 4 に記載のメール暗号複合制御装置。

【請求項 6】

前記判定手段で、返信メールの宛先に前記作成元メールの宛先及び送信元に設定されていないメールアドレスが追加されたと判定された場合に、当該追加された宛先を含む電子メールを前記新規メールとして送信するかを判定する送信判定手段と、を更に備え、

前記送信手段は、前記送信判定手段で前記新規メールとして送信すると判定した場合に、前記共通鍵データ生成手段で生成される共通鍵データと前記第 1 暗号化手段で暗号化される当該新規メールとを当該追加された宛先に送信することを特徴とする請求項 5 に記載のメール暗号複合制御装置。

【請求項 7】

返信メールではない新規メールと、返信メールと、返信メールの作成元である作成元メールとを記憶装置に記憶する、電子メールの暗号化と復号化を制御するメール暗号複合制御装置における制御方法であって、

共通鍵生成手段が、前記新規メールを生成する場合に、前記新規メールを暗号化及び復号するための共通鍵データを生成する共通鍵データ生成工程と、

第 1 の暗号化手段が、前記共通鍵データ生成手段で生成した共通鍵データを用いて、前記新規メールを暗号化する第 1 の暗号化工程と、

第 2 の暗号化手段が、返信メールを生成する場合に、前記作成元メールから得られる共通鍵データを用いて、前記返信メールを暗号化する第 2 の暗号化工程と、

抽出手段が、記憶装置に記憶されたメールの中より、前記新規メールから前記返信メールまでのスレッドに含まれる電子メールであって、共通鍵データを未取得の電子メールを特定して抽出する抽出工程と、

復号手段が、前記抽出手段で抽出した電子メールから得られる共通鍵データを用いて、受信した暗号化メールを復号する復号工程と

を含み、

前記第 2 の暗号化工程は、前記復号工程で復号した電子メールを作成元とする返信メールを暗号化することを特徴とするメール暗号復号制御装置における制御方法。

【請求項 8】

返信メールではない新規メールと、返信メールと、返信メールの作成元の電子メールである作成元メールとを記憶装置に記憶する、電子メールの暗号化と復号化を制御するメール暗号復号制御装置において実行可能なプログラムであって、

前記メール暗号復号制御装置を、
前記新規メールを生成する場合に、前記新規メールを暗号化及び復号するための共通鍵データを生成する共通鍵データ生成手段と、
前記共通鍵データ生成手段で生成した共通鍵データを用いて、前記新規メールを暗号化する第１の暗号化手段と、
返信メールを生成する場合に、前記作成元メールから得られる共通鍵データを用いて、前記返信メールを暗号化する第２の暗号化手段と、
記憶装置に記憶されたメールの中より、前記新規メールから前記返信メールまでのスレッドに含まれる電子メールであって、共通鍵データを未取得の電子メールを特定して抽出する抽出手段と、
前記抽出手段で抽出した電子メールから得られる共通鍵データを用いて、受信した暗号化メールを復号する復号手段として機能させ、
前記第２の暗号化手段は、前記復号手段で復号した電子メールを作成元とする返信メールを暗号化することを特徴とするメール暗号復号制御装置の制御プログラム。

【手続補正２】

【補正対象書類名】明細書

【補正対象項目名】００１０

【補正方法】変更

【補正の内容】

【００１０】

本発明の暗号復号制御装置は、返信メールではない新規メールと、返信メールと、返信メールの作成元の電子メールである作成元メールとを記憶装置に記憶する、電子メールの暗号化と復号化を制御するメール暗号復号制御装置であって、前記新規メールを生成する場合に、前記新規メールを暗号化及び復号するための共通鍵データを生成する共通鍵データ生成手段と、前記共通鍵データ生成手段で生成した共通鍵データを用いて、前記新規メールを暗号化する第１の暗号化手段と、返信メールを生成する場合に、前記作成元メールから得られる共通鍵データを用いて、前記返信メールを暗号化する第２の暗号化手段と、記憶装置に記憶されたメールの中より、前記新規メールから前記返信メールまでのスレッドに含まれる電子メールであって、共通鍵データを未取得の電子メールを特定して抽出する抽出手段と、前記抽出手段で抽出した電子メールから得られる共通鍵データを用いて、受信した暗号化メールを復号する復号手段とを備え、前記第２の暗号化手段は、前記復号手段で復号した電子メールを作成元とする返信メールを暗号化することを特徴とする。