(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3563649号
(P3563649)
(45)発行日　平成16年9月8日(2004.9.8)　(24)登録日　平成16年6月11日(2004.6.11)

(51)Int.Cl.[7]	F I		
H04L 12/54	H04L	11/20	101Z
G06F 13/00	G06F	13/00	351Z
H04L 12/58	H04L	13/00	307Z
H04L 29/08			

請求項の数 13　(全 24 頁)

(21)出願番号　特願平11-288198
(22)出願日　平成11年10月8日(1999.10.8)
(65)公開番号　特開2001-111606(P2001-111606A)
(43)公開日　平成13年4月20日(2001.4.20)
審査請求日　平成13年4月13日(2001.4.13)

(73)特許権者　598090519
株式会社オープンループ
北海道札幌市清田区北野一条二丁目１０番４０号
(74)代理人　100095407
弁理士　木村　満
(74)代理人　100098442
弁理士　木村　美穂子
(74)代理人　100104916
弁理士　古溝　聡
(72)発明者　浅田　一憲
北海道札幌市清田区北野二条三丁目２番１号　株式会社オープンループ内

審査官　石井　研一

最終頁に続く

(54)【発明の名称】通信制御装置及び記録媒体

(57)【特許請求の範囲】
【請求項１】
クライアントマシンが自己に供給する送信用データを取得し、取得した前記送信用データを外部のネットワークに送出する通信制御装置であって、
前記クライアントマシンより取得した前記送信用データに基づいて、当該送信用データの発信者及び／又は当該発信者が所属するグループを特定する送信元特定手段と、
前記送信元特定手段が特定した発信者及び／又はグループに対応付けられた秘密鍵を用いて、前記送信用データにデジタル署名を施す署名手段と、
前記署名手段がデジタル署名を施した送信用データを前記ネットワークに送出するデータ送信手段と、を備え、
前記送信元特定手段は、
前記送信用データの発信者及び／又は当該発信者が所属するグループを当該データに基づいて特定する条件を表す署名条件データを記憶する署名条件記憶手段と、
前記署名条件記憶手段が記憶する署名条件データが表す条件に従って、前記送信用データの発信者及び／又は当該発信者が所属するグループを特定する手段と、を備える、
ことを特徴とする通信制御装置。
【請求項２】
前記グループのうち少なくとも２つは、その一方が他方に従属しており、
前記送信元特定手段は、前記送信用データの発信者が所属するグループが従属している他のグループを、当該発信者が所属するグループとして扱い、当該発信者及び／又は当該発

信者が所属するグループを特定する、
ことを特徴とする請求項１に記載の通信制御装置。
【請求項３】
前記送信用データを、復号化する場合に当該送信用データの受信者及び／又は当該受信者が所属するグループに対応付けられた秘密鍵を用いることを要する態様で暗号化する暗号化手段を備える、
ことを特徴とする請求項１又は２に記載の通信制御装置。
【請求項４】
前記暗号化手段は、
前記送信用データを所定の共通鍵を用いて暗号化する手段と、
前記共通鍵を、前記送信用データの受信者及び／又は当該受信者が所属するグループに対応付けられた公開鍵を用いて暗号化する手段と、
暗号化された前記共通鍵を、暗号化された前記送信用データに添付する手段と、を備える、
ことを特徴とする請求項３に記載の通信制御装置。
【請求項５】
外部のネットワークより受信用データを受信し、受信した当該受信用データを破棄するか否かを決定し、破棄しないと決定したとき、当該受信用データを前記クライアントマシンに供給する受信手段を備える、
ことを特徴とする請求項１乃至４のいずれか１項に記載の通信制御装置。
【請求項６】
前記受信手段は、
前記受信用データを破棄するか否かを当該受信用データに基づき決定するための条件を表す配達条件データを記憶する配達条件記憶手段と、
配達条件記憶手段が記憶する前記配達条件データが表す条件に従って、当該受信用データを破棄するか否かを決定する手段と、を備える、
ことを特徴とする請求項５に記載の通信制御装置。
【請求項７】
前記受信手段は、
前記外部のネットワークより受信した前記受信用データにデジタル署名が施されており、且つ、当該デジタル署名を認証するための公開鍵を示す証明情報が当該データに添付されているか否かを判別し、当該デジタル署名が施されており、且つ、当該公開鍵を示す情報が添付されていると判別したとき、当該受信用データを認証の対象とすることを決定する認証データ判別手段と、
前記認証データ判別手段が認証の対象と決定した受信用データに添付されている前記証明情報が示す公開鍵を用いて、当該受信用データに施されているデジタル署名を認証し、認証に成功したとき、当該受信用データを前記クライアントマシンに送出する認証手段と、を備える、
ことを特徴とする請求項５又は６に記載の通信制御装置。
【請求項８】
前記受信手段は、
前記外部のネットワークより受信した前記受信用データが、復号化する場合に当該受信用データの受信者及び／又は当該受信者が所属するグループに対応付けられた秘密鍵を用いることを要する態様で暗号化されているか否かを判別し、暗号化されていると判別したとき、当該受信用データを復号化の対象とすることを決定する暗号化データ判別手段と、
前記暗号化データ判別手段が復号化の対象と決定した前記受信用データに基づいて、当該受信用データの受信者及び／又は当該受信者が所属するグループに対応付けられた秘密鍵を特定する受信グループ特定手段と、
前記受信グループ特定手段が特定した秘密鍵を用いて、復号化の対象と決定された前記受信用データを復号化し、復号化した前記受信用データを前記クライアントマシンに供給す

る復号化手段と、を備える、
ことを特徴とする請求項５、６又は７に記載の通信制御装置。
【請求項９】
前記秘密鍵を記憶し、前記クライアントマシン及び前記外部のネットワークのいずれにも実質的に当該秘密鍵を供給することなく、当該秘密鍵を前記署名手段に供給する鍵記憶手段を備え、
前記署名手段は、前記鍵記憶手段より供給された前記秘密鍵を用いて、前記データにデジタル署名を施す、
ことを特徴とする請求項１乃至８のいずれか１項に記載の通信制御装置。
【請求項１０】
外部のネットワークよりデータを受信し、受信した前記データを破棄するか否かを決定し、破棄しないと決定したとき、当該データをクライアントマシンに供給する通信制御装置であって、
前記データを破棄するか否かを当該データに基づき決定するための条件を表す配達条件データを記憶する破棄条件記憶手段と、
前記破棄条件記憶手段が記憶する前記配達条件データが表す条件に従って、当該データを破棄するか否かを決定する決定手段と、
前記外部のネットワークより受信した前記データにデジタル署名が施されており、且つ、当該デジタル署名を認証するための公開鍵を示す証明情報が当該データに添付されているか否かを判別し、当該デジタル署名が施されており、且つ、当該公開鍵を示す情報が添付されていると判別したとき、当該データを認証の対象とすることを決定する認証データ判別手段と、
前記認証データ判別手段が認証の対象と決定したデータに添付されている前記証明情報が示す公開鍵を用いて、前記認証データ判別手段が認証の対象と決定したデータに施されているデジタル署名を認証し、認証に成功したとき、当該データを前記クライアントマシンに送出する認証手段と、を備える、
ことを特徴とする通信制御装置。
【請求項１１】
前記外部のネットワークより受信した前記データが、復号化する場合に当該データの受信者及び／又は当該受信者が所属するグループに対応付けられた秘密鍵を用いることを要する態様で暗号化されているか否かを判別し、暗号化されていると判別したとき、当該データを復号化の対象とすることを決定する暗号化データ判別手段と、
前記暗号化データ判別手段が復号化の対象と決定した前記データに基づいて、当該データの受信者及び／又は当該受信者が所属するグループに対応付けられた秘密鍵を特定する受信グループ特定手段と、
前記受信グループ特定手段が特定した秘密鍵を用いて、復号化の対象と決定された前記データを復号化し、復号化した前記データを前記クライアントマシンに供給する復号化手段と、を備える、
ことを特徴とする請求項１０に記載の通信制御装置。
【請求項１２】
外部のネットワーク及びクライアントマシンに接続されたコンピュータを、
データを前記クライアントマシンより取得する手段と、
前記データの発信者及び／又は当該発信者が所属するグループを当該データに基づいて特定する条件を表す署名条件データを記憶する署名条件記憶手段と、
前記署名条件記憶手段が記憶する署名条件データが表す条件に従って、前記データの発信者及び／又は当該発信者が所属するグループを特定する送信元特定手段と、
前記送信元特定手段が特定した発信者及び／又はグループに対応付けられた秘密鍵を用いて、前記データにデジタル署名を施す署名手段と、
前記署名手段がデジタル署名を施したデータを前記ネットワークに送出するデータ送信手段と、

して機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【請求項１３】
外部のネットワーク及びクライアントマシンに接続されたコンピュータを、
前記ネットワークよりデータを受信する手段と、
前記データを破棄するか否かを当該データに基づき決定するための条件を表す配達条件データを記憶する破棄条件記憶手段と、
前記破棄条件記憶手段が記憶する前記配達条件データが表す条件に従って、当該データを破棄するか否かを決定し、破棄すると決定したとき当該データを実質的に破棄する決定手段と、
前記データにデジタル署名が施されており、且つ、当該デジタル署名を認証するための公開鍵を示す証明情報が当該データに添付されているか否かを判別し、当該デジタル署名が施されており、且つ、当該公開鍵を示す情報が添付されていると判別したとき、当該データを認証の対象とすることを決定する認証データ判別手段と、
前記認証データ判別手段が認証の対象と決定したデータに添付されている前記証明情報が示す公開鍵を用いて、当該データに施されているデジタル署名を認証し、認証に成功したとき、当該データを前記クライアントマシンに送出する認証手段と、
して機能させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明は、通信制御装置に関し、特に、電子メールの送受信を制御する通信制御装置に関する。
【０００２】
【従来の技術】
近年、インターネットを用いて電子メールを交換する技術が一般に用いられている。電子メールを用いると、郵便等と比べて、情報が簡単且つ迅速に相手方に伝達されるという利点がある。
しかし、電子メールを用いた情報の伝送においては、「盗み見」、「改竄」、「なりすまし」及び「否認」等の危険が伴う。なお、「盗み見」とは、発信された情報が第三者により窃取されることをいう。また、「改竄」とは、発信された情報が第三者により書き換えられた上で本来の受信者に伝送されることをいう。また、「なりすまし」とは、電子メールの発信者が自己の名義を偽ることをいう。また「否認」とは、電子メールの発信者がその電子メールを発信した事実を否定することをいう。
【０００３】
このため、「盗み見」の危険を回避する手法として、電子メールを用いて伝送する情報を暗号化する手法が用いられている。具体的には、例えば、対をなす公開鍵と秘密鍵が電子メールの受信者に割り当てられているときに、伝送する対象の情報を、受信者に割り当てられた公開鍵を用いて暗号化し、受信者は、暗号化されたこの情報を、自己に割り当てられている秘密鍵を用いて復号化する。
【０００４】
一方、「改竄」、「なりすまし」及び「否認」の危険を回避する手法としては、電子メールにより伝送する情報にデジタル署名を付する手法が用いられている。具体的には、例えば、対をなす公開鍵と秘密鍵が電子メールの発信者に割り当てられているときに、伝送する対象の情報を受信者に割り当てられた秘密鍵を用いて暗号化したものを、暗号化する前の情報と対応付けて送信する。受信者は、暗号化されている方の情報を、発信者に割り当てられている公開鍵を用いて復号化し、暗号化されていない方の情報と照合することにより、この情報が真正な発信者により発信されたか否かを確認する。
【０００５】
【発明が解決しようとする課題】
上述の暗号化やデジタル署名は、従来、電子メールを利用する個人が、ＰＧＰやＳ／ＭＩ

ＭＥなどのセキュリティ電子メール規格に準拠した電子メールソフトウェアをコンピュータ等に実行させ、各自暗号化やデジタル署名のために各自が用いる秘密のデータを管理しなければならなかった。
しかも、団体のオフィスなどのように、電子メールを送受信する端末が多数人により共有されたり、端末が多数人に操作され得る環境では、秘密のデータの管理には高いスキルが要求され、秘密のデータの安全な管理が困難である。
【０００６】
一方、例えば、商取引のために会社などの団体の構成員が送受する電子メールなどは、送信者あるいは受信者がその団体の構成員であることが証明されれば足り、しかも、構成員が特定される必要性より、構成員が属する団体を特定する必要性の方が高いことが通常である。
【０００７】
このような電子メールに、構成員個人のデジタル署名を施しても、その構成員が属する団体が特定されていない場合は、構成員のデジタル署名の認証の他、構成員が属する団体を特定するための処理が更に必要となり、電子メールの認証の手続きが煩雑になる。
【０００８】
しかし、団体の構成員がデータのデジタル署名を団体用の共通の秘密鍵を用いて行うようにした場合、この秘密鍵を各端末で管理すると、多数の端末のそれぞれに秘密鍵が記憶される結果、秘密鍵の漏洩の危険性が高くなる。
また、団体に宛てたデータを団体用の共通の公開鍵を用いて暗号化するようにした場合、団体の構成員個人に宛てて電子メールを発信する者は、その電子メールの内容を、その構成員以外の者に解読されないように暗号化することが事実上困難になる。
【０００９】
もっとも、秘密鍵の漏洩の危険が増大する問題や、構成員個人宛の電子メールの暗号化が出来ない、という上述の問題を解決する手法としては、特開平９－２１４５５６号公報に開示されている手法が考えられる。
特開平９－２１４５５６号公報の手法では、階層化された複数のネットワークの各々が、外部との接続点に、通過パケットを認証するためのパケット管理装置を備える。パケット管理装置は、パケットに含まれるアドレス情報に基づいて特定される認証鍵を用いて、パケットに含まれる、自己に対応付けられた認証データの正当性を検査する。そして、検査に通った場合、次段と最終段のパケット管理装置に対する認証鍵を用いて得た２つの認証データをパケットに添付し、パケットを次段あるいは受信端末に転送する。
【００１０】
しかし、特開平９－２１４５５６号公報の手法では、パケットの転送先は、特定の受信端末に特定される。従って、この手法を電子メールの伝送に用いた場合、個々の電子メールが伝送される対象の装置は、特定の受信端末に限定される。従って、この手法では、端末が多数人により共有されたり、端末が多数人に操作され得る環境で、団体の各構成員が任意の端末を選んで電子メールの送受を行うことが困難となり、このような端末は極めて利用に不便なものとなる。
【００１１】
この発明は上記実状に鑑みてなされたもので、個人が情報の暗号化・復号化やデジタル署名及びその認証のためのデータを管理することなく、操作する対象の端末を特定されることなく、デジタル署名による証明の対象を適切に選択し、外部との間で安全に情報の交換を行うための通信制御装置を提供することを目的とする。
【００１２】
【課題を解決するための手段】
上記目的を達成するため、この発明の第１の観点にかかる通信制御装置は、
クライアントマシンが自己に供給する送信用データを取得し、取得した前記送信用データを外部のネットワークに送出する通信制御装置であって、
前記クライアントマシンより取得した前記送信用データに基づいて、当該送信用データの

発信者及び／又は当該発信者が所属するグループを特定する送信元特定手段と、
前記送信元特定手段が特定した発信者及び／又はグループに対応付けられた秘密鍵を用いて、前記送信用データにデジタル署名を施す署名手段と、
前記署名手段がデジタル署名を施した送信用データを前記ネットワークに送出するデータ送信手段と、を備え、
前記送信元特定手段は、
前記送信用データの発信者及び／又は当該発信者が所属するグループを当該データに基づいて特定する条件を表す署名条件データを記憶する署名条件記憶手段と、
前記署名条件記憶手段が記憶する署名条件データが表す条件に従って、前記送信用データの発信者及び／又は当該発信者が所属するグループを特定する手段と、を備える、
ことを特徴とする。

【００１３】
このような通信制御装置によれば、デジタル署名のため情報を個人が管理することを要せずに、グループの構成員が発信者であることが証された送信用データが外部に安全に送信される。また、発信者あるいは発信者の所属するグループは送信用データ自身に基づいて識別されるので、発信者が操作する対象の端末も特定されない。

【００１５】
前記グループのうち少なくとも２つは、その一方が他方に従属していてもよい。これにより、グループは階層化された態様で識別される。
この場合、前記送信元特定手段は、前記送信用データの発信者が所属するグループが従属している他のグループを、当該発信者が所属するグループとして扱い、当該発信者及び／又は当該発信者が所属するグループを特定するようにしてもよい。

【００１６】
前記送信用データを、復号化する場合に当該送信用データの受信者及び／又は当該受信者が所属するグループに対応付けられた秘密鍵を用いることを要する態様で暗号化する暗号化手段を備えるようにすれば、情報の暗号化のためのデータを個人が管理することが不要でありながら、外部にさらに安全にデータが送信される。

【００１７】
前記暗号化手段は、例えば、
前記送信用データを所定の共通鍵を用いて暗号化する手段と、
前記共通鍵を、前記送信用データの受信者及び／又は当該受信者が所属するグループに対応付けられた公開鍵を用いて暗号化する手段と、を備えることにより、送信用データの暗号化を行う。

【００１８】
外部のネットワークより受信用データを受信し、受信した当該受信用データを破棄するか否かを決定し、破棄しないと決定したとき、当該受信用データを前記クライアントマシンに供給する受信手段を備えるものとすれば、この通信制御装置は受信用データの受信も行う。

【００１９】
前記受信手段は、例えば、
前記受信用データを破棄するか否かを当該受信用データに基づき決定するための条件を表す配達条件データを記憶する配達条件記憶手段と、
配達条件記憶手段が記憶する前記配達条件データが表す条件に従って、当該受信用データを破棄するか否かを決定する手段と、を備えることにより、受信用データを破棄するか否かを決定する。

【００２０】
前記受信手段は、
前記外部のネットワークより受信した前記受信用データにデジタル署名が施されており、且つ、当該デジタル署名を認証するための公開鍵を示す証明情報が当該データに添付されているか否かを判別し、当該デジタル署名が施されており、且つ、当該公開鍵を示す情報

が添付されていると判別したとき、当該受信用データを認証の対象とすることを決定する認証データ判別手段と、
前記認証データ判別手段が認証の対象と決定した受信用データに添付されている前記証明情報が示す公開鍵を用いて、当該受信用データに施されているデジタル署名を認証し、認証に成功したとき、当該受信用データを前記クライアントマシンに送出する認証手段と、を備えるものであってもよい。
このような通信制御装置によれば、デジタル署名の認証に用いる情報を個人が管理することを要せずにデジタル署名が認証され、外部との間で安全にデータが交換される。
【００２１】
前記受信手段は、
前記外部のネットワークより受信した前記受信用データが、復号化する場合に当該受信用データの受信者及び／又は当該受信者が所属するグループに対応付けられた秘密鍵を用いることを要する態様で暗号化されているか否かを判別し、暗号化されていると判別したとき、当該受信用データを復号化の対象とすることを決定する暗号化データ判別手段と、
前記暗号化データ判別手段が復号化の対象と決定した前記受信用データに基づいて、当該受信用データの受信者及び／又は当該受信者が所属するグループに対応付けられた秘密鍵を特定する受信グループ特定手段と、
前記受信グループ特定手段が特定した秘密鍵を用いて、復号化の対象と決定された前記受信用データを復号化し、復号化した前記受信用データを前記クライアントマシンに供給する復号化手段と、を備えるものであってもよい。
このような通信制御装置によれば、情報の復号化のための情報を個人が管理することを要せずに外部から受信した受信用データが復元され、外部との間で安全に情報が交換される。また、受信者は受信用データ自身により識別されるので、発信者が操作する対象の端末も特定されない。
【００２２】
前記秘密鍵を記憶し、前記クライアントマシン及び前記外部のネットワークのいずれにも実質的に当該秘密鍵を供給することなく、当該秘密鍵を前記署名手段に供給する鍵記憶手段を備え、
前記署名手段は、前記鍵記憶手段より供給された前記秘密鍵を用いて、前記データにデジタル署名を施すものとすれば、秘密鍵がクライアントマシンや外部からのアクセスにより漏洩する事態が防止され、データの交換がより安全に行われる。
【００２３】
また、この発明の第２の観点に係る通信制御装置は、
外部のネットワークよりデータを受信し、受信した前記データを破棄するか否かを決定し、破棄しないと決定したとき、当該データをクライアントマシンに供給する通信制御装置であって、
前記データを破棄するか否かを当該データに基づき決定するための条件を表す配達条件データを記憶する破棄条件記憶手段と、
前記破棄条件記憶手段が記憶する前記配達条件データが表す条件に従って、当該データを破棄するか否かを決定する決定手段と、
前記外部のネットワークより受信した前記データにデジタル署名が施されており、且つ、当該デジタル署名を認証するための公開鍵を示す証明情報が当該データに添付されているか否かを判別し、当該デジタル署名が施されており、且つ、当該公開鍵を示す情報が添付されていると判別したとき、当該データを認証の対象とすることを決定する認証データ判別手段と、
前記認証データ判別手段が認証の対象と決定したデータに添付されている前記証明情報が示す公開鍵を用いて、前記認証データ判別手段が認証の対象と決定したデータに施されているデジタル署名を認証し、認証に成功したとき、当該データを前記クライアントマシンに送出する認証手段と、を備える、
ことを特徴とする。

【００２４】
このような通信制御装置によれば、デジタル署名の認証のための情報を個人が管理することを要せずにデジタル署名が認証され、外部からの情報の取得が安全に行われる。また、受信したデータにより受信者が識別されるので、発信者が操作する対象の端末も特定されない。
【００２５】
前記通信制御装置は、
前記外部のネットワークより受信した前記データが、復号化する場合に当該データの受信者及び／又は当該受信者が所属するグループに対応付けられた秘密鍵を用いることを要する態様で暗号化されているか否かを判別し、暗号化されていると判別したとき、当該データを復号化の対象とすることを決定する暗号化データ判別手段と、
前記暗号化データ判別手段が復号化の対象と決定した前記データに基づいて、当該データの受信者及び／又は当該受信者が所属するグループに対応付けられた秘密鍵を特定する受信グループ特定手段と、
前記受信グループ特定手段が特定した秘密鍵を用いて、復号化の対象と決定された前記データを復号化し、復号化した前記データを前記クライアントマシンに供給する復号化手段と、を備えるものであってもよい。
このような通信制御装置によれば、情報の復号化のためのデータを個人が管理することを要せずに外部から受信したデータが復元され、外部からの情報の取得が安全に行われる。
【００２６】
また、この発明の第３の観点に係るコンピュータ読み取り可能な記録媒体は、
外部のネットワーク及びクライアントマシンに接続されたコンピュータを、
データを前記クライアントマシンより取得する手段と、
前記データの発信者及び／又は当該発信者が所属するグループを当該データに基づいて特定する条件を表す署名条件データを記憶する署名条件記憶手段と、
前記署名条件記憶手段が記憶する署名条件データが表す条件に従って、前記データの発信者及び／又は当該発信者が所属するグループを特定する送信元特定手段と、
前記送信元特定手段が特定した発信者及び／又はグループに対応付けられた秘密鍵を用いて、前記データにデジタル署名を施す署名手段と、
前記署名手段がデジタル署名を施したデータを前記ネットワークに送出するデータ送信手段と、
して機能させるためのプログラムを記録したことを特徴とする。
【００２７】
このような記録媒体に記録されたプログラムを実行するコンピュータは、情報の暗号化やデジタル署名のための情報を個人が管理することを要せずに、外部に安全に情報を送信する。また、このようなコンピュータは、クライアントマシンから供給されるデータにより発信者を識別するので、発信者が操作する対象の端末も特定されない。
【００２８】
また、この発明の第４の観点に係るコンピュータ読み取り可能な記録媒体は、
外部のネットワーク及びクライアントマシンに接続されたコンピュータを、
前記ネットワークよりデータを受信する手段と、
前記データを破棄するか否かを当該データに基づき決定するための条件を表す配達条件データを記憶する破棄条件記憶手段と、
前記破棄条件記憶手段が記憶する前記配達条件データが表す条件に従って、当該データを破棄するか否かを決定し、破棄すると決定したとき当該データを実質的に破棄する決定手段と、
前記データにデジタル署名が施されており、且つ、当該デジタル署名を認証するための公開鍵を示す証明情報が当該データに添付されているか否かを判別し、当該デジタル署名が施されており、且つ、当該公開鍵を示す情報が添付されていると判別したとき、当該データを認証の対象とすることを決定する認証データ判別手段と、

前記認証データ判別手段が認証の対象と決定したデータに添付されている前記証明情報が示す公開鍵を用いて、当該データに施されているデジタル署名を認証し、認証に成功したとき、当該データを前記クライアントマシンに送出する認証手段と、
して機能させるためのプログラムを記録したことを特徴とする。

【００２９】

このような記録媒体に記録されたプログラムを実行するコンピュータは、デジタル署名の認証のためのデータを個人が管理することを要せずにデジタル署名を認証し、外部からの情報の取得を安全に行う。また、受信したデータにより受信者が識別されるので、発信者が操作する対象の端末も特定されない。

【００３０】

【発明の実施の形態】

この発明の実施の形態にかかる認証システム及び認証方法を、電子メール送受信システムを例として説明する。

【００３１】

図１は、この発明の実施の形態にかかる電子メール送受信システムの構成を示す図である。

図示するように、この発明の実施の形態にかかる電子メール送受信システムは、送信サーバ１と、受信サーバ２と、クライアントマシン３ａ～３ｄとより構成されている。

送信サーバ１、受信サーバ２及びクライアントマシン３ａ～３ｄは、例えば、ＬＡＮ（Ｌｏｃａｌ　Ａｒｅａ　Ｎｅｔｗｏｒｋ）を介して、互いに接続されている。

【００３２】

送信サーバ１は、図２に示すように、制御部１１と、主記憶部１２と、外部記憶部１３と、ルータ１４と、クライアント側インターフェース１５とより構成される。主記憶部１２、外部記憶部１３、ルータ１４及びクライアント側インターフェース１５は、いずれも内部バスを介して制御部１１に接続されている。

【００３３】

制御部１１は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）等からなり、外部記憶部１３に記憶されているプログラムデータが表すプログラムに従って、後述する処理を行う。

主記憶部１２は、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃｅｓｓ　Ｍｅｍｏｒｙ）等からなり、制御部１１の作業領域として用いられる。

【００３４】

外部記憶部１３は、ハードディスク装置等からなり、後述する処理を制御部１１に行わせるためのプログラムデータを予め記憶し、また、（ａ１）～（ａ４）及び（ｂ１）として後述する各種の情報を、後述するデータ構造をとるようにして予め記憶する。そして、外部記憶部１３は、制御部１１の指示に従って、自己が記憶するデータを制御部１１に供給する。

【００３５】

なお、制御部１１は、クライアントマシン３ａ～３ｄや外部のネットワークからのアクセスを受けても、外部記憶部１３の記憶領域のうち、（ａ１）～（ａ４）及び（ｂ１）の情報を格納する記憶領域の記憶内容を読み出してアクセス元に供給する処理を実質的に行わない。また、外部記憶部１３の記憶領域のうち、（ａ１）～（ａ４）及び（ｂ１）の情報を格納する記憶領域は、実質的に、クライアントマシン３ａ～３ｄや外部のネットワークからの直接のアクセスを受け付けない。

【００３６】

ルータ１４は、ＤＳＵ（Ｄａｔａ　Ｓｅｒｖｉｃｅ　Ｕｎｉｔ）等からなり、制御部１１の指示に従って、制御部１１より供給された情報を、インターネット等の外部のネットワークに送出する。

クライアント側インターフェース１５は、イーサネット用インタフェース回路等からなり、上述のＬＡＮを介してクライアントマシン３ａ～３ｄに接続されている。クライアント

側インターフェース１５は、制御部１１の指示に従って、制御部１１より供給された情報を、クライアントマシン３ａ～３ｄに伝送する。また、クライアントマシン３ａ～３ｄが自己に供給した情報を制御部１１に供給する。

【００３７】

受信サーバ２は、図３に示すように、制御部２１と、主記憶部２２と、外部記憶部２３と、ルータ２４と、クライアント側インターフェース２５とより構成される。

制御部２１、主記憶部２２、外部記憶部２３、ルータ２４及びクライアント側インターフェース２５は、例えば、送信サーバ１の制御部１１、主記憶部１２、外部記憶部１３、ルータ１４及びクライアント側インターフェース１５と実質的に同一の物理的構成を有している。そして、主記憶部２２、外部記憶部２３、ルータ２４及びクライアント側インターフェース２５は、いずれも内部バスを介して制御部２１に接続されている。

【００３８】

制御部２１は、外部記憶部２３に記憶されているプログラムデータが表すプログラムに従って、後述する処理を行う。主記憶部２２は、制御部２１の作業領域として用いられる。外部記憶部２３は、後述する処理を制御部２１に行わせるためのプログラムデータを記憶し、また、後述する（ａ１）～（ａ４）及び（ｂ１）の情報を、後述するデータ構造をとって予め記憶する。そして、外部記憶部２３は、制御部２１の指示に従って、自己が記憶するデータを制御部２１に供給する。

【００３９】

なお、制御部２１は、クライアントマシン３ａ～３ｄや外部のネットワークからのアクセスを受けても、外部記憶部２３の記憶領域のうち、（ａ１）～（ａ４）及び（ｂ１）の情報を格納する記憶領域の記憶内容を読み出してアクセス元に供給する処理を実質的に行わない。また、外部記憶部２３の記憶領域のうち、（ａ１）～（ａ４）及び（ｂ１）の情報を格納する記憶領域は、実質的に、クライアントマシン３ａ～３ｄや外部のネットワークからの直接のアクセスを受け付けない。

【００４０】

ルータ２４は、制御部２１の指示に従って、制御部２１より供給された情報を外部のネットワークに送出する。クライアント側インターフェース２５は、送信サーバ１のクライアント側インターフェース１５と同様に、ＬＡＮを介してクライアントマシン３ａ～３ｄに接続されている。クライアント側インターフェース２５は、制御部２１の指示に従って、制御部２１より供給された情報を、クライアントマシン３ａ～３ｄに伝送する。また、クライアントマシン３ａ～３ｄが自己に供給した情報を制御部２１に供給する。

【００４１】

クライアントマシン３ａ～３ｄは、互いに実質的に同一の構成を有しており、それぞれ、図４に示すように、制御部３１と、主記憶部３２と、外部記憶部３３と、インターフェース３４と、入力部３５と、表示部３６とより構成される。同一のクライアントマシンに属する主記憶部３２、外部記憶部３３、インターフェース３４、入力部３５及び表示部３６は、いずれも、内部バスを介して、そのクライアントマシンの制御部３１に接続されている。

【００４２】

各クライアントマシン３ａ～３ｄの制御部３１、主記憶部３２、外部記憶部３３及びインターフェース３４は、例えば、送信サーバ１の制御部１１、主記憶部１２、外部記憶部１３及びクライアント側インターフェース１５と実質的に同一の物理的構成を有している。

【００４３】

制御部３１は、外部記憶部３３に記憶されているプログラムデータが表すプログラムに従って、後述するメーラーの処理を含む処理を実行する。主記憶部３２は、制御部３１の作業領域として用いられる。外部記憶部３３は、後述する処理を制御部３１に行わせるためのプログラムデータを予め記憶し、また、制御部３１の指示に従って、自己が記憶するデータを制御部３１に供給する。

【００４４】

インターフェース３４は、ＬＡＮを介して送信サーバ１のクライアント側インターフェース１５及び受信サーバ２のクライアント側インターフェース２５に接続されている。インターフェース３４は、制御部３１の指示に従って、制御部３１より供給された情報を、送信サーバ１や受信サーバ２に伝送する。また、送信サーバ１や受信サーバ２が自己に供給した情報を制御部３１に供給する。

【００４５】

入力部３５は、キーボードやマウス等より構成されており、操作者の操作に従った情報を、制御部３１に供給する。表示部３６は、ＣＲＴ（Ｃａｔｈｏｄｅ　Ｒａｙ　Ｔｕｂｅ）等より構成されており、制御部３１の指示に従った画像を、自己が備える表示画面上に表示する。

【００４６】

（動作）

次に、図１に示す電子メール送受信システムの動作を、図５及び図６を参照して説明する。以下では、図１の電子メール送受信システムのユーザが、コンピュータを用いて、ネットワークに接続されたサーバへのアクセスを行うに際して、この電子メール送受信システムが当該ユーザの認証を行う動作を例として説明を行う。

図５は、電子メール送信の処理を示すフローチャートである。

図６は、電子メール受信の処理を示すフローチャートである。

【００４７】

（初期設定）

電子メール送受信システムに以下説明する動作を行わせるため、電子メール送受信システムの管理者等は、この電子メール送受信システムを利用する団体（以下、利用団体と呼ぶ）に含まれる部署及びその構成員と、部署間の従属関係とを特定する組織情報を、送信サーバ１の外部記憶部１３に格納する。

【００４８】

組織情報は、具体的には、利用団体に含まれる各々の部署について、

（ａ１）その部署の名称、

（ａ２）（ａ１）の情報が示す部署に所属する下位の部署の名称及び／又は（ａ１）の情報が示す部署の構成員の名称、

（ａ３）（ａ１）の情報が示す部署に割り当てられた部署用の秘密鍵及び証明書、

の３種類の情報を、互いが対応付けられた態様で含んでいる。なお、（ａ３）の情報を構成する証明書が含む公開鍵は、その証明書が割り当てられている部署と同一の部署に割り当てられた秘密鍵と対をなしている。

【００４９】

なお、後述する電子メール送信の処理において、送信サーバ１は、（ａ２）の情報が示す構成員は、（ａ１）の情報が示す部署に所属すると共に、その部署が従属する上位の部署にも所属するものとして扱う。

（ａ１）の情報が示す部署の上位の部署は、例えば、当該（ａ１）の情報と実質的に同一の名称を示す（ａ２）の情報を組織情報より索出し、索出された（ａ２）の情報に対応付けられている他の（ａ１）の情報を特定することにより特定される。

【００５０】

更に、上述の組織情報には、

（ａ４）（ａ２）の情報が示す構成員の各々に割り当てられた個人用の秘密鍵及び証明書、

が含まれており、（ａ２）の情報に対応付けられている。なお、（ａ４）の情報を構成する証明書が含む公開鍵は、その証明書が割り当てられている構成員と同一の構成員に割り当てられた秘密鍵と対をなしている。

【００５１】

なお、秘密鍵は、データを暗号化するための暗号鍵であり、例えば上述したようにして、別個の暗号鍵である公開鍵と対をなし、対をなす秘密鍵及び公開鍵はいずれも同一の団体

又は個人に割り当てられている。対をなす秘密鍵及び公開鍵のうち一方の暗号鍵を用いて暗号化されたデータは、他方の暗号鍵を用いて復号化し得る、という関係にある。
公開鍵は、その公開鍵（及びその公開鍵と対をなす秘密鍵）を割り当てられた団体や個人以外の者に対しても、任意の態様で公開されている。
【００５２】
また、証明書は、公開鍵が真正であることを証明するデータであり、外部の証明機関等により予め作成される。証明書は、真正を証明する対象の公開鍵を含んでおり、後述するように、その証明書により真正が証明されている公開鍵と対をなす秘密鍵を用いて施されたデジタル署名を認証する処理において用いられる。
【００５３】
なお、上述の部署や構成員は、実在するものである必要はない。従って、例えば利用団体の全構成員が共通に利用することを許されたメールアドレスを、架空の部署の架空の構成員に割り当てるようにしてもよいし、特定の部署の全構成員が共通に利用することを許されたメールアドレスを、その部署の架空の構成員に割り当てるようにしてもよい。
また、（ａ４）の個人用の秘密鍵は、利用団体に属するすべての構成員に対応付けられている必要はない。
【００５４】
また、電子メール送受信システムの管理者等は、予め、
（ｂ１）この電子メール送受信システムから送出される電子メールの宛先として予想される者に割り当てられた証明書、
を、送信サーバ１の外部記憶部１３に格納する。
【００５５】
また、電子メール送受信システムの管理者等は、送信ルールパラメータを、予め送信サーバ１の外部記憶部１３に格納する。
送信ルールパラメータは、後述する電子メール送信の処理で送信対象の文面にデジタル署名や暗号化を施すか否かを決定する規則や、デジタル署名に用いる秘密鍵及び暗号化に用いる公開鍵を決定する規則を記述するデータである。
【００５６】
また、管理者等は、受信サーバ２の外部記憶部２３にも、上述の（ａ１）～（ａ４）の情報を含む組織情報を、予め格納する。
また、管理者等は、配達ルールパラメータを、予め外部記憶部２３に格納する。
配達ルールパラメータは、後述する電子メール受信の処理で、受信サーバ２が予め受信した電子メールを破棄するかクライアントマシン３ａ～３ｄに供給するかを決定する規則を記述するデータである。
【００５７】
（電子メール送信の処理）
利用団体の構成員が電子メールを発信する場合、電子メールの発信者である構成員はまず、クライアントマシン３ａ～３ｄのいずれかの入力部３５を操作して、自己が操作するクライアントマシンに、メーラーの処理（すなわち、後述のステップＳ１０２及びＳ１０３の処理）の実行を指示する（図５、ステップＳ１０１）。なお、以下では、理解を容易にするため、構成員が操作したクライアントマシンは、クライアントマシン３ａであるものとする。
【００５８】
クライアントマシン３ａの制御部３１は、メーラーの処理の実行を指示されると、外部記憶部３３よりメーラーのプログラムデータを読み出し、メーラーの処理を開始する。
メーラーの処理を開始したクライアントマシン３ａの制御部３１は、構成員が、入力部３５を操作して、電子メールとして送信する対象の文面と、電子メールの表題と、宛先のメールアドレスと、発信者である構成員自身に割り当てられたメールアドレスとを入力するのを待機する（ステップＳ１０２）。
【００５９】

そして、構成員が、送信する対象の文面と、表題と、宛先及び発信者のメールアドレスとの入力を完了し、電子メール送信を指示すると、制御部３１は、入力された送信対象の文面と、表題と、宛先及び発信者のメールアドレスとを、ＬＡＮを介して送信サーバ１に供給する（ステップＳ１０３）。

【００６０】

なお、ステップＳ１０２で、制御部３１は、構成員が、入力部３５を操作して、構成員自身に割り当てられたメールアドレスを入力し、電子メールの受信を指示するのも待機する。そして、構成員自身に割り当てられたメールアドレス及び電子メールの受信の指示が入力されると、この電子メール送受信システムは、後述する電子メール受信の処理のステップＳ２０３以降の処理を行う。

【００６１】

送信サーバ１のクライアント側インターフェース１５は、ＬＡＮを介してクライアントマシン３ａより供給された送信対象の文面と、表題と、宛先及び発信者のメールアドレスとを受信し、制御部１１に供給する。

【００６２】

制御部１１は、送信対象の文面と、表題と、宛先及び発信者のメールアドレスとを供給されると、まず、外部記憶部１３に格納されている送信ルールパラメータを読み出す（ステップＳ１０４）。

【００６３】

そして、読み出した送信ルールパラメータが示す規則に従い、送信対象の文面にデジタル署名を施すか、また、デジタル署名を施す場合いかなる秘密鍵を用いるかを決定する（ステップＳ１０５）。なお、ステップＳ１０５において、制御部１１は、複数の秘密鍵を決定してよい。また、決定した秘密鍵が複数ある場合、ステップＳ１０５で制御部１１は、後述するステップＳ１０８においてこれら複数の秘密鍵をデジタル署名のために用いる順序も決定する。

【００６４】

そして、デジタル署名を施さないとステップＳ１０５で決定した場合、制御部１１は処理をステップＳ１０９に移す。一方、デジタル署名を施すと決定した場合は、ステップＳ１０５で決定した秘密鍵と、その秘密鍵と対をなす公開鍵を含む証明書とを外部記憶部１３に格納された組織情報より抽出し（ステップＳ１０６）、処理をステップＳ１０７に進める。

【００６５】

なお、ステップＳ１０５において、制御部１１は、デジタル署名のために用いる秘密鍵を決定する条件を、送信対象の文面や、表題や、宛先及び発信者のメールアドレスや、その他任意の情報の存否や内容に係らせてよい。すなわち、送信ルールパラメータは、デジタル署名のために用いる秘密鍵を決定する条件を、送信対象の文面や、宛先及び発信者のメールアドレスや、その他任意の情報の存否や内容に係らせるものとして記述するものであってもよい。

この場合、制御部１１は、ステップＳ１０５において、デジタル署名のために用いる秘密鍵を決定する条件に係る情報にアクセスし、その情報の存否を判別したり、その情報の内容を取得して解析したりするものとする。

【００６６】

例えば、制御部１１は、送信者のメールアドレスや電子メールの表題が所定の文字列を含んでいるとき、所定の部署に割り当てられた秘密鍵を用いることを決定してもよい。

また、制御部１１は、送信対象の文面や、表題や、宛先及び発信者のメールアドレスや、送信時刻が属する時間帯や、上述した送信履歴情報の内容その他任意の情報が所定の条件に合致したとき、送信者が属する部署のうち、所定の階層より高い階層の部署（すなわち、自己が直接又は間接に従属する他の部署の数が所定数以内である部署）に割り当てられた秘密鍵を用いるものとしてもよい。

更に、制御部１１は、複数の事象の結果の組み合わせが所定の条件に合致するか否かに基

づいて、暗号化を行うか否かを決定してもよい。
具体的には、例えば、受信者が所定の部署に所属し、且つ、電子メールの表題に所定の文字列が含まれているとき、送信者が属する部署のうち、所定の階層より高い階層の部署に割り当てられた秘密鍵を用いるものとしてもよい。
また、送信ルールパラメータは、同時に発生し得る２個の事象が、秘密鍵の決定について異なる決定結果を導くように、決定の条件を記述していてもよい。この場合、制御部１１は、例えば、両方の決定結果に基づいて決定される秘密鍵をいずれも用いることを決定するようにすればよい。

【００６７】

ただし、制御部１１は、ステップＳ１０５において、電子メールの発信者である構成員又は当該構成員の所属する部署に割り当てられた秘密鍵のうちから、デジタル署名のために用いる秘密鍵を決定する。
また、制御部１１は、構成員又は当該構成員の所属する部署に割り当てられた秘密鍵を用いることを決定した場合、該当する構成員又は部署が所属している上位の部署の秘密鍵もまた、デジタル署名のために用いることを決定するようにする。すなわち、例えば、部署Ｘに部署Ｙが所属し、部署Ｙに部署Ｚが所属し、部署Ｚに構成員αが所属する場合、部署Ｙの秘密鍵をデジタル署名に用いる場合は部署Ｘの秘密鍵も用いるものと決定する。また、構成員αの秘密鍵をデジタル署名に用いる場合は、部署Ｘ、Ｙ及びＺの秘密鍵も用いるものと決定する。

【００６８】

なお、制御部１１は、構成員又は構成員の所属する部署に割り当てられた秘密鍵を特定するために、例えば、外部記憶部１３に格納されている上述の（ａ２）の情報のうち、発信者である構成員の名称を示すものを特定し、特定した（ａ２）の情報に対応付けられている（ａ３）及び（ａ４）の情報を索出するようにする。

【００６９】

次に、制御部１１は、送信対象の文面を所定のハッシュ関数に代入した値（ハッシュ値）を計算する（ステップＳ１０７）。ステップＳ１０７でハッシュ値の計算に用いるハッシュ関数は任意であり、例えば、当該ハッシュ関数は、ハッシュ関数「ＭＤ－５」であればよい。
そして、制御部１１は、ステップＳ１０７で計算したハッシュ値を、ステップＳ１０６で抽出した秘密鍵を用いて暗号化し（ステップＳ１０８）、処理をステップＳ１０９に移す。ステップＳ１０７及びＳ１０８の処理により、送信対象の文面にはデジタル署名が施される。

【００７０】

なお、ステップＳ１０５で決定した秘密鍵が複数ある場合、ステップＳ１０８で制御部１１は、ステップＳ１０７で計算したハッシュ値を、秘密鍵１個につき１回ずつ用い、ステップＳ１０５で決定した順序に従い重ねて暗号化を行う。

【００７１】

次に、制御部１１は、ステップＳ１０４で読み出した送信ルールパラメータが示す規則に従い、送信対象の文面を暗号化するか否かを決定する（ステップＳ１０９）。そして、暗号化すると決定した場合は、例えば疑似乱数等から構成される任意のデータを作成し、作成したデータを共通鍵として用い、送信対象の文面を暗号化する（ステップＳ１１０）。一方、暗号化しないと決定した場合は、処理をステップＳ１１２に移す。

【００７２】

ステップＳ１１０における暗号化の手法は、暗号化のために用いた共通鍵自体を用いて復号化され得る暗号を生成するものである限り任意であり、例えば、アメリカ合衆国の定める規格であるＤＥＳ（Ｄａｔａ　Ｅｎｃｒｙｐｔｉｏｎ　Ｓｔａｎｄａｒｄ）に準拠した手法により行えばよい。
なお、共通鍵は所定のデータから構成されていてもよい。この場合、電子メール送受信システムの管理者等が、共通鍵を予め外部記憶部１３に格納するようにし、ステップＳ１１

０において、制御部１１が、外部記憶部１３からこの共通鍵を読み出すようにすればよい。

【００７３】

なお、ステップＳ１０９において、制御部１１は、暗号化を行うか否かを決定する条件を、送信対象の文面や、表題や、宛先及び発信者のメールアドレスや、その他任意の情報の存否や内容に係らせてよい。すなわち、送信ルールパラメータは、暗号化を行うか否かを決定する条件を、送信対象の文面や、宛先及び発信者のメールアドレスや、その他任意の情報の存否や内容に係らせるものとして記述するものであってもよい。

この場合、制御部１１は、ステップＳ１０９において、暗号化を行うか否かを決定する条件に係る情報にアクセスし、その情報の存否を判別したり、その情報の内容を取得して解析したりするものとする。

【００７４】

例えば、制御部１１は、送信者のメールアドレスや電子メールの表題が所定の文字列を含んでいるか否か、送信者が所定の部署に所属しているか否か、等に基づいて、暗号化を行うか否かを決定してもよい。

また、制御部１１は、送信時刻が所定の時間帯に属するか否かに基づいて、暗号化を行うか否かを決定してもよい。この場合、制御部１１は、現在時刻を表す時刻情報を供給する任意の装置に接続され、その装置から供給される時刻情報に基づいて、現在時刻を取得すればよい。具体的には、制御部１１は、例えば、外部のネットワークを介して、外部のタイムサーバに接続されるものとし、このタイムサーバより現在時刻を取得するものとすればよい。

また、制御部１１は、電子メールの受信者に宛てて過去に発信した電子メールに関し、その内容、数、送信時刻その他任意の送信履歴情報を外部記憶部１３等に蓄積し、蓄積された送信履歴情報に基づいて、暗号化を行うか否かを決定してもよい。

更に、制御部１１は、複数の事象の結果の組み合わせが所定の条件に合致するか否かに基づいて、暗号化を行うか否かを決定してもよい。

また、送信ルールパラメータは、同時に発生し得る２個の事象が、暗号化を行うか否かについて異なる決定結果を導くように、決定の条件を記述していてもよい。この場合、送信ルールパラメータは、いずれの決定結果が優先して適用されるかを定める規則を記述するようにすればよい。

【００７５】

次に、制御部１１は、外部記憶部１３に格納されている上述の（ｂ１）の情報を検索し、宛先のメールアドレスが示す受信者に対応付けられた証明書を索出する。そして、ステップＳ１１０で暗号化のために用いた共通鍵を、索出した証明書に含まれる公開鍵を用いて暗号化し（ステップＳ１１１）、処理をステップＳ１１２に移す。

【００７６】

ステップＳ１１１における暗号化は任意の公開鍵暗号の手法でよく、例えば、ＲＳＡ暗号の手法により行えばよい。

また、宛先のメールアドレスが複数ある場合、ステップＳ１１１で制御部１１は、各々のメールアドレスが示す受信者に対応付けられた証明書を索出し、索出した各証明書に含まれる公開鍵を１個につき１回ずつ用いて平文の共通鍵を繰り返し暗号化し、暗号化された共通鍵を、索出した証明書の数と同数生成する。

【００７７】

ステップＳ１１２で、制御部１１は、ルータ１４を介して、以下（ｃ１）～（ｃ４）として示す４個のデータの組、すなわち、

（ｃ１）発信者のメールアドレス、

（ｃ２）宛先のメールアドレス、

（ｃ３）電子メールの表題、及び、

（ｃ４）送信対象の文面（ただし、ステップＳ１１０で共通鍵により暗号化された場合は、暗号化されたその文面、その他の場合は平文の文面）、

がなす組を形成し、組をなすこれらのデータを、１個の電子メールを構成する情報として、ＳＭＴＰ（Ｓｉｍｐｌｅ　Ｍａｉｌ　Ｔｒａｎｓｆｅｒ　Ｐｒｏｔｏｃｏｌ）等の規則に従い、外部のネットワークに送出する。

【００７８】

ただし、ステップＳ１０７及びＳ１０８で（ｃ４）の情報（すなわち、送信対象の文面）にデジタル署名を施した場合、制御部１１は、ステップＳ１１２で送出する電子メールを、（ｃ１）～（ｃ４）の情報に加え、以下（ｃ５）～（ｃ７）として示す３個のデータ、すなわち、

（ｃ５）ステップＳ１０８で暗号化されたハッシュ値、

（ｃ６）ステップＳ１０８で暗号化される前のハッシュ値、及び、

（ｃ７）ステップＳ１０６で外部記憶部１３から抽出された証明書、

を含むように構成するものとする。

【００７９】

また、（ｃ４）の情報がステップＳ１１１で暗号化された場合、制御部１１は、ステップＳ１１２で送出する電子メールを、（ｃ１）～（ｃ４）の情報に加え、以下（ｃ８）及び（ｃ９）として示す２個のデータ、すなわち、

（ｃ８）ステップＳ１１１で暗号化された共通鍵、及び、

（ｃ９）ステップＳ１１１で索出された証明書、

を含むように構成するものとする。

【００８０】

なお、上述の（ｃ５）及び（ｃ６）のデータが、送信対象の文面に施されたデジタル署名を構成する。

また、（ｃ２）の情報（宛先のメールアドレス）が複数ある場合は、その各々について（ｃ１）～（ｃ４）のデータの組（あるいは、更に（ｃ５）～（ｃ７）の情報及び／又は（ｃ８）～（ｃ９）の情報を含んだデータの組）を形成し、各々の組を、互いに別個の電子メールを構成する情報として送出するものとする。

【００８１】

以上説明したステップＳ１０１～Ｓ１１２の処理により、送信サーバ１が、クライアントマシン３ａ～３ｄから供給された電子メールの文面を暗号化し、更に、送信ルールパラメータが示す規則に従って選択した秘密鍵を用いたデジタル署名を施した上、その電子メールを外部のネットワークに送出する。

メーラーの処理を行うクライアントマシン３ａ～３ｄは、暗号化やデジタル署名の処理を行うことを要しない。

【００８２】

（電子メール受信の処理）

一方、受信サーバ２の制御部２１は、ルータ２４を介して、外部のネットワーク上に送出された、利用団体の構成員（又は利用団体自身）宛の電子メールをＳＭＴＰ等の規則に従って受信する。そして、受信した電子メールを、外部記憶部２３に蓄積する。

【００８３】

外部記憶部２３に蓄積される電子メールは、上述の電子メール送信のステップＳ１１２において送信サーバ１が送出する電子メールと実質的に同一のデータ構造を有しているものとする。すなわち、外部記憶部２３に蓄積される電子メールは、上述の（ｃ１）～（ｃ４）の情報を含み、（ｃ４）の情報にデジタル署名が施されている場合は更に上述の（ｃ５）～（ｃ７）の情報を含み、（ｃ４）の情報が暗号化されている場合は、（ｃ１）～（ｃ４）の情報に加え、上述の（ｃ８）及び（ｃ９）の情報を含むものとする。

【００８４】

利用団体の構成員が、受信サーバ２の外部記憶部２３に蓄積されている電子メールを受信する場合、構成員はまず、クライアントマシン３ａ～３ｄのいずれかの入力部３５を操作して、自己が操作するクライアントマシンに、メーラーの処理の実行を指示する（図３、ステップＳ２０１）。なお、以下では、理解を容易にするため、構成員が操作したクライ

アントマシンは、クライアントマシン３ｂであるものとする。
【００８５】
クライアントマシン３ｂの制御部３１は、メーラーの処理の実行を指示されると、電子メール送信の処理のステップＳ１０２と同様にメーラーの処理を開始する。
メーラーの処理を開始したクライアントマシン３ｂの制御部３１は、構成員が、入力部３５を操作して、電子メールの受信者である構成員自身に割り当てられたメールアドレスを入力し、電子メールの受信を指示するのを待機する（ステップＳ２０２）。
【００８６】
そして、構成員が、自己のメールアドレスの入力を完了し、電子メール受信を指示すると、制御部３１は、入力された構成員のメールアドレスを、ＬＡＮを介して受信サーバ２に供給する（ステップＳ２０３）。
【００８７】
なお、ステップＳ２０２の処理は、実質的に上述の電子メール送信の処理のステップＳ１０２と同一の処理である。従って、制御部３１は、ステップＳ２０２において、構成員が、入力部３５を操作して、電子メールとして送信する文面と、電子メールの表題と、宛先のメールアドレスと、発信者である構成員自身に割り当てられたメールアドレスとを入力するのも待機する。そして、電子メールとして送信する文面、表題、宛先のメールアドレス及び発信者である構成員自身のメールアドレスが入力されると、この電子メール送受信システムは、上述の電子メール送信の処理のステップＳ１０３以降の処理を行う。
【００８８】
受信サーバ２のクライアント側インターフェース２５は、ＬＡＮを介してクライアントマシン３ｂより供給された構成員のメールアドレスを受信し、制御部２１に供給する。
制御部２１は、構成員のメールアドレスを供給されると、まず、外部記憶部２３に蓄積されている電子メールのうち、クライアントマシン３ｂより供給されたメールアドレスを宛先とする電子メール１個を、受信する対象の電子メールとして抽出する（ステップＳ２０４）。
【００８９】
次に、制御部２１は、外部記憶部２３に格納されている配達ルールパラメータを読み出す（ステップＳ２０５）。
そして、読み出した配達ルールパラメータが示す規則に従い、ステップＳ２０４で抽出した電子メールをクライアントマシン３ｂに供給するか破棄するかを決定する（ステップＳ２０６）。そして、供給しない（破棄する）と決定すると、ステップＳ２０４で抽出した電子メールを破棄し、クライアント側インターフェース２５を介して、クライアントマシン３ｂに、電子メールを配達できない旨を通知し（ステップＳ２０７）、電子メール受信の処理を終了する。
クライアントマシン３ｂの制御部３１は、インターフェース３４を介し、受信サーバ２より認証に失敗した旨の通知を受信すると、表示部３６に、認証の失敗を表す画像の表示を指示する。表示部３６は、この指示に応答して、電子メールの受信に失敗したことを示す画像を自己の表示画面上に表示する。
【００９０】
なお、ステップＳ２０６において、制御部２１は、電子メールをクライアントマシン３ｂに供給するか否かを決定する条件を、抽出された電子メールを構成するデータや、その他任意の情報の存否や内容に係らせてよい。
すなわち、配達ルールパラメータは、ステップＳ２０４で抽出された電子メールをクライアントマシン３ａ～３ｄに供給するか否かを決定する条件を、抽出された電子メールを構成するデータや、その他任意の情報の存否や内容に係らせるものとして記述するものであってもよい。
この場合、制御部１１は、ステップＳ２０６において、電子メールをクライアントマシン３ｂに供給するか否かを決定する条件に係る情報にアクセスし、その情報の存否を判別したり、その情報の内容を取得して解析したりするものとする。

【００９１】
例えば、制御部２１は、抽出された電子メールが所定の文字列を含んでいるか否か、当該電子メールの文面にデジタル署名及び／又は暗号化が施されているか否か、送信者が所定の部署に所属しているか否か、等に基づいて、電子メールを破棄するか否かを決定してもよい。
また、制御部２１は、受信時刻が所定の時間帯に属するか否かに基づいて、電子メールを破棄するか否かを決定してもよい。この場合、制御部２１は、上述した制御部１１と同様、時刻情報を供給する任意の装置に接続され、その装置から供給される時刻情報に基づいて、現在時刻を取得すればよい。
また、制御部２１は、受信サーバ２が過去に受信した電子メールに関し、その内容、数、受信時刻その他任意の受信履歴情報を外部記憶部２３等に蓄積し、蓄積された受信履歴情報に基づいて、電子メールを破棄するか否かを決定してもよい。
更に、制御部２１は、複数の事象の結果の組み合わせが所定の条件に合致するか否かに基づいて、電子メールを破棄するか否かを決定してもよい。
また、配達ルールパラメータは、同時に発生し得る２個の事象が、電子メールを破棄するか否かについて異なる決定結果を導くように、決定の条件を記述していてもよい。この場合、配達ルールパラメータは、いずれの決定結果が優先して適用されるかを定める規則を記述するようにすればよい。
【００９２】
一方、ステップＳ２０６において、電子メールをクライアントマシン３ｂに供給すると判別すると、制御部２１は、ステップＳ２０４で抽出した電子メールが（ｃ９）の証明書を含んでいるか否かを判別する（ステップＳ２０８）。そして、含んでいないと判別した場合は、処理をステップＳ２１２に移す。
【００９３】
一方、含んでいると判別した場合、制御部２１は、外部記憶部２３が記憶する組織情報を検索し、ステップＳ２０４で抽出した電子メール内の（ｃ９）の証明書のうち、クライアントマシン３ｂより供給されたメールアドレスが示す構成員又はその構成員が所属する部署に割り当てられたものを特定する。そして、特定した証明書に含まれる公開鍵と対をなす秘密鍵を索出する（ステップＳ２０９）。
そして、制御部２１は、ステップＳ２０４で抽出した電子メールに含まれる（ｃ８）の情報を、ステップＳ２０９で索出した秘密鍵を用いて復号化し（ステップＳ２１０）、平文の共通鍵を取得する。
【００９４】
そして、制御部２１は、復号化により得られた平文の共通鍵を用いて、ステップＳ２０４で抽出された電子メールに含まれる、暗号化された（ｃ４）の情報を復号化し（ステップＳ２１１）、ステップＳ２１２に処理を移す。ステップＳ２１１の処理により、受信サーバ２は、暗号化された電子メールの文面を平文として取得する。
【００９５】
次に、ステップＳ２１２で、制御部２１は、ステップＳ２０４で抽出した電子メールが、上述の（ｃ５）～（ｃ７）の情報を含んでいるか否かを判別する。そして、含んでいないと判別すると、処理をステップＳ２１４に移す。
【００９６】
一方、含んでいると判別すると、制御部２１は、ステップＳ２０４で抽出した電子メール内の（ｃ７）の証明書に含まれる公開鍵を用いて、この電子メールの（ｃ５）の情報を復号化する。そして、復号化により得られたデータが、この電子メールの（ｃ６）の情報と実質的に一致するか否かを判別する（ステップＳ２１３）。そして、一致しないと判別したとき、制御部２１は、一致しないと判別された電子メールを破棄し、ステップＳ２０７に処理を移す。
【００９７】
一方、ステップＳ２１３で、復号化した（ｃ５）の情報が（ｃ６）の情報と一致すると判

別すると、制御部２１は、ステップＳ２０４で抽出された電子メールの文面（ただし、文面が暗号化されていた場合は、ステップＳ２１１で復号化された文面）と、発信者のメールアドレスとを互いに対応付け、所定の書式に整えてクライアントマシン３ｂに供給する（ステップＳ２１４）。
クライアントマシン３ｂの制御部３１は、インターフェース３４を介して、受信サーバ２より電子メールの文面と発信者のメールアドレスとを受信すると、表示部３６に、受信した文面及びメールアドレスを表示させる（ステップＳ２１５）。
【００９８】
以上説明したステップＳ２０１～Ｓ２１５の処理により、受信サーバ２は、ネットワークから受信して蓄積した電子メールをクライアントマシン３ａ～３ｄに供給するか否かを配達ルールパラメータが示す規則に従って決定する。そして、供給すると決定したときは、電子メールにデジタル署名が施されているときはそのデジタル署名を認証し、暗号化されているときは復号化した上で、その電子メールをクライアントマシン３ａ～３ｄに供給する。
メーラーの処理を行うクライアントマシン３ａ～３ｄは、デジタル署名の認証や暗号の復号化の処理を行うことを要しない。
なお、受信サーバ２は、クライアントマシン３ｂより供給されたメールアドレスを宛先とする電子メールが外部記憶部２３に複数蓄積されている場合、該当する電子メールの数だけステップＳ２０４以降の処理を繰り返せばよい。
【００９９】
なお、この発明の実施の形態にかかる電子メール送受信システムの構成は、上述のものに限られない。
例えば、この電子メール送受信システムにより送受信されるデータは電子メールに限られず、デジタル形式で表された任意のデータが送受信の対象となってもよい。
また、クライアントマシンの数は４個である必要はなく任意であり、３個以下でもよいし、５個以上であってもよい。また、送信サーバ１と受信サーバ２とは別個のものである必要はなく、単一のサーバマシンが、送信サーバ１及び受信サーバ２の機能を行うようにしてもよい。
【０１００】
また、送信サーバ１が上述の電子メール送信の処理をオペレーティングシステム上で実行する場合、送信ルールパラメータは、例えば、オペレーティングシステムが実行する処理を記述するスクリプト等より構成されていてよい。同様に、受信サーバ２が上述の電子メール受信の処理をオペレーティングシステム上で実行する場合、配達ルールパラメータは、スクリプト等より構成されていてもよい。
【０１０１】
また、送信サーバ１と受信サーバ２とが共通して用いる上述の（ａ１）～（ａ４）及び（ｂ１）の情報の全部又は一部が、送信サーバ１又は受信サーバ２の一方のみに格納されていてもよいし、あるいは、送信サーバ１及び受信サーバ２とは別個の記憶装置にのみ格納されていてもよい。
この場合、送信サーバ１及び受信サーバ２は、上述の（ａ１）～（ａ４）及び（ｂ１）の情報のうち自己が記憶していない情報を記憶している装置と接続され、その装置から、自己が記憶していない情報を取得するようにすればよい。
【０１０２】
また、クライアントマシン３ａ～３ｄ等のクライアントが実行するメーラーの処理には、利用団体の構成員個人に割り当てられた秘密鍵を用いて電子メールの文面にデジタル署名を施す処理や、電子メールの文面の復号化の処理が含まれていてもよい。
この場合、送信サーバ１及び受信サーバ２は、利用団体の構成員個人に割り当てられた秘密鍵を用いたデジタル署名の処理や電子メールの文面の復号化の処理を一律にクライアントマシン３ａ～３ｄ等に委ねるようにしてもよい。
すなわち、送信サーバ１は、上述のステップＳ１０５において構成員個人に割り当てられ

た秘密鍵を決定の対象から一律に除外してもよく、受信サーバ２は、ステップＳ２０９における索出の対象から、電子メールの宛先である構成員個人に割り当てられた秘密鍵を除外してもよい。

【０１０３】

また、送信する対象の文面に暗号化及びデジタル署名の両方を施す場合、暗号化及びデジタル署名は、いずれを先に行ってもよい。従って、送信サーバ１は、上述のメール送信の処理におけるステップＳ１０５～Ｓ１０８の処理に先立って、ステップＳ１０９～Ｓ１１１の処理を行うようにしてもよい。

また、受信する対象の文面が暗号化及びデジタル署名の両方を施されている場合、暗号の復号化及びデジタル署名の認証は、いずれを先に行ってもよい。従って、受信サーバ２は、上述のメール受信の処理におけるステップＳ２０８～Ｓ２１１の処理に先立って、ステップＳ２１２及びＳ２１３の処理を行うようにしてもよい。

【０１０４】

同時に複数の部署に属する構成員に単一のメールアドレスが割り当てられていてもよい。この場合、クライアントマシン３ａ～３ｄは、その構成員が、自己が属する各部署のうちいずれの部署の構成員として電子メールの送信を行うかを、例えばその構成員の操作等に従って送信サーバ１に通知するようにしてもよい。そして、送信サーバ１は、通知された部署に割り当てられた秘密鍵を用いてデジタル署名の処理を行うようにすればよい。

【０１０５】

また、利用団体に含まれる部署は階層をなしていなくてもよく、この場合、上述の（ａ２）の情報は、（ａ１）の情報が示す部署に所属する下位の部署の名称を含んでいる必要がない。

また、部署が階層化されているか否かに関わらず、制御部１１は、上述のステップＳ１０５において、構成員又は当該構成員の所属する部署に割り当てられた秘密鍵を用いることを決定した場合、必ずしも、該当する構成員又は部署が所属している上位のすべての部署の秘密鍵をデジタル署名のために用いると決定する必要はない。

【０１０６】

また、送信サーバ１は、上述のステップＳ１１０及びＳ１１１の処理に代えて、受信者の公開鍵で電子メールの文面を暗号化してもよい。また、受信サーバ２は、受信者の公開鍵で暗号化された電子メールを受信したときは、上述のステップＳ２０９及びＳ２１０の処理に代えて、暗号化された電子メールを、受信者の秘密鍵で復号化してもよい。

また、送信サーバ１は、上述のステップＳ１１０及びＳ１１１の処理を実行するたびに、公開鍵を新たなものに更新してもよい。

【０１０７】

また、送信サーバ１は、上述の（ｃ６）の情報をネットワークに送出しなくてもよい。また、受信サーバ２は、上述のステップＳ２１３で、復号化した（ｃ５）の情報が（ｃ６）の情報とが一致するか否かを判別する代わりに、復号化した（ｃ５）の情報と、（ｃ４）の情報を所定のハッシュ関数に代入したハッシュ値とが一致するか否かを判別するようにしてもよい。

【０１０８】

また、送信サーバ１は、上述の（ｃ９）の情報に代えて、ステップＳ１１１で索出された証明書に固有なものとして割り当てられた識別符号をネットワークに送出するようにしてもよい。

また、受信サーバ２は、（ｃ８）の情報の作成に用いた公開鍵を含む証明書に固有の識別符号を（ｃ９）の情報の代わりに含んだ電子メールを受信してもよい。この場合、受信サーバ２は、上述のステップＳ２０８において、（ｃ９）の情報に代わる上述の識別符号を含んでいるか否かを判別すればよい。そして、ステップＳ２０９では、この識別符号が示す証明書のうち、クライアントマシン３ｂより供給されたメールアドレスが示す構成員又はその構成員が所属する部署に割り当てられたものを特定するようにすればよい。

【０１０９】

また、送信サーバ１は、送信対象である電子メールの文面を暗号化するか否かの決定や、文面にデジタル署名を施すか否かの決定を、クライアントマシン３ａ～３ｄから供給される指示に従って決定するようにしてもよい。

【０１１０】

また、受信サーバ２は、ステップＳ２０６での判別結果や、電子メール受信の処理において、クライアントマシン３ａ～３ｄに供給する対象の電子メールに加えた処理（例えば、デジタル署名の認証や、文面の復号化）の内容を示すデータを、その電子メールに添付したり、その電子メールの文面に加えたりしてもよい。

また、受信サーバ２は、ステップＳ２０６で、クライアントマシン３ａ～３ｄに電子メールを供給しないと決定した場合も、その電子メールを破棄せずに、外部記憶部２３等に格納するようにしてもよい。

【０１１１】

また、受信サーバ２は、外部のネットワークより受信した、利用団体の構成員（又は利用団体自身）宛の電子メールについて、クライアントマシン３ａ～３ｄからの指示を待つことなく上述のステップＳ２０４～Ｓ２１３の処理を行うようにしてもよい。

ただしこの場合、受信サーバ２は、処理済みの電子メール（すなわち、ステップＳ２１２で、上述の（ｃ５）～（ｃ７）の情報を含まないと判別された電子メールと、ステップＳ２１３で、復号化した（ｃ５）の情報が（ｃ６）の情報と一致すると判別された電子メール）を、外部記憶部２３等に格納する。なお、ステップＳ２１１で復号化された電子メールについては、復号化された状態で格納する。

そして、クライアントマシン３ａ～３ｄが、例えば上述のステップＳ２０１～Ｓ２０３の処理を行って利用団体の構成員のメールアドレスを受信サーバ２に供給したとき、受信サーバ２は、外部記憶部２３に格納されている処理済みの電子メールのうち、自己に供給されたメールアドレスを宛先とするものを抽出する。そして、抽出した処理済みの電子メールを、このメールアドレスを自己に供給したクライアントマシンに供給する。

なお、受信サーバ２は、電子メールを破棄した場合にステップＳ２０７の処理を必ずしも実行する必要はない。

【０１１２】

以上、この発明の実施の形態を説明したが、この発明の通信制御装置は、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、クライアントマシンに接続可能なサーバコンピュータに上述の動作を実行するためのプログラムを格納した媒体（ＣＤ－ＲＯＭ、磁気テープ等）から該プログラムをインストールすることにより、上述の処理を実行する通信制御装置を構成することができる。

【０１１３】

また、例えば、通信ネットワークの掲示板（ＢＢＳ）に該プログラムを掲示し、これをネットワークを介して配信してもよく、また、該プログラムを表す信号により搬送波を変調し、得られた変調波を伝送し、この変調波を受信した装置が変調波を復調して該プログラムを復元するようにしてもよい。

そして、このプログラムを起動し、ＯＳの制御下に、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【０１１４】

なお、ＯＳが処理の一部を分担する場合、あるいは、ＯＳが本願発明の１つの構成要素の一部を構成するような場合には、記録媒体には、その部分をのぞいたプログラムを格納してもよい。この場合も、この発明では、その記録媒体には、コンピュータが実行する各機能又はステップを実行するためのプログラムが格納されているものとする。

【０１１５】

【発明の効果】

以上説明したように、この発明によれば、個人が情報の暗号化・復号化やデジタル署名及びその認証のためのデータを管理することなく、操作する対象の端末を特定されることなく、デジタル署名による証明の対象を適切に選択し、外部との間で安全に情報の交換を行

うための通信制御装置が実現される。

【図面の簡単な説明】

【図１】この発明の実施の形態にかかる電子メール送受信システムの基本構成を示すブロック図である。

【図２】図１の電子メール送受信システムの送信サーバの基本構成を示すブロック図である。

【図３】図１の電子メール送受信システムの受信サーバの基本構成を示すブロック図である。

【図４】図１の電子メール送受信システムのクライアントマシンの基本構成を示すブロック図である。

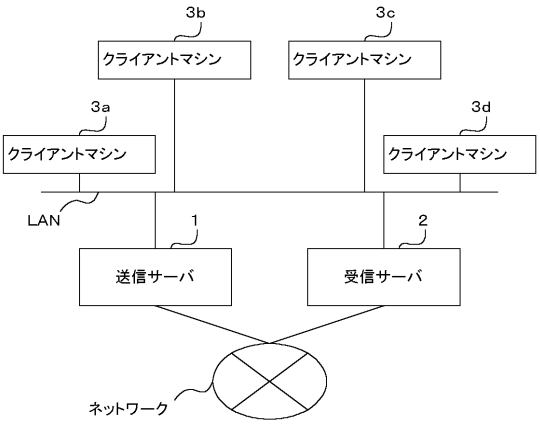
【図５】電子メール送信の処理を表すフローチャートである。

【図６】電子メール受信の処理を表すフローチャートである。

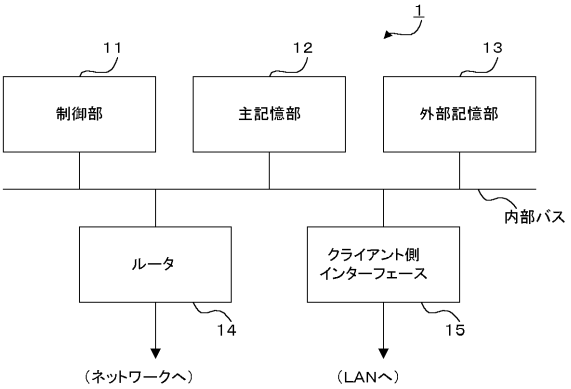
【符号の説明】

１	送信サーバ
１１、２１、３１	制御部
１２、２２、３２	主記憶部
１３、２３、３３	外部記憶部
１４、２４	ルータ
１５、２５	クライアント側インターフェース
２	受信サーバ
３ａ～３ｄ	クライアントマシン
３４	インターフェース
３５	入力部
３６	表示部

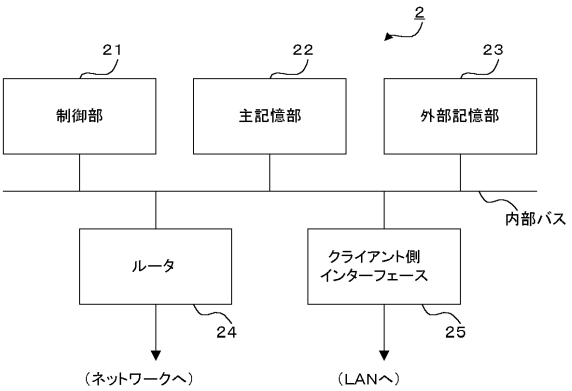
【図１】



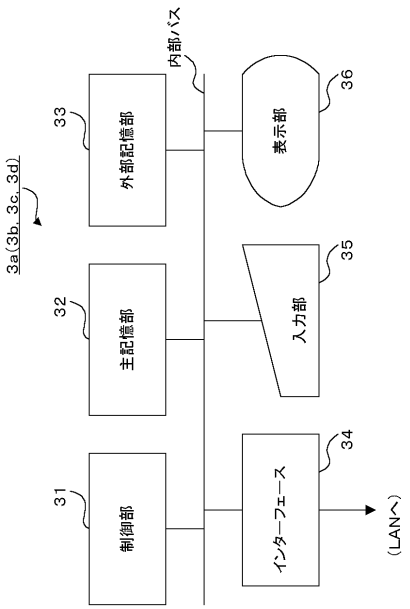
【図２】



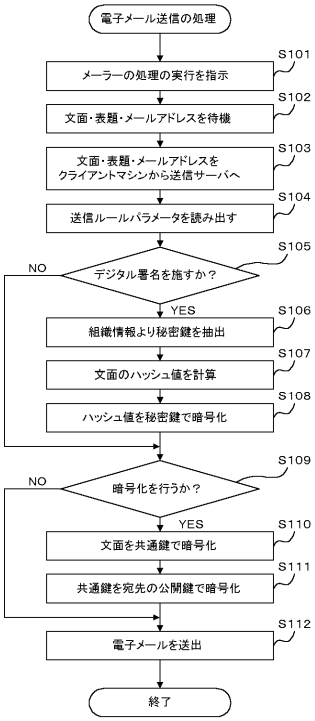
【図３】



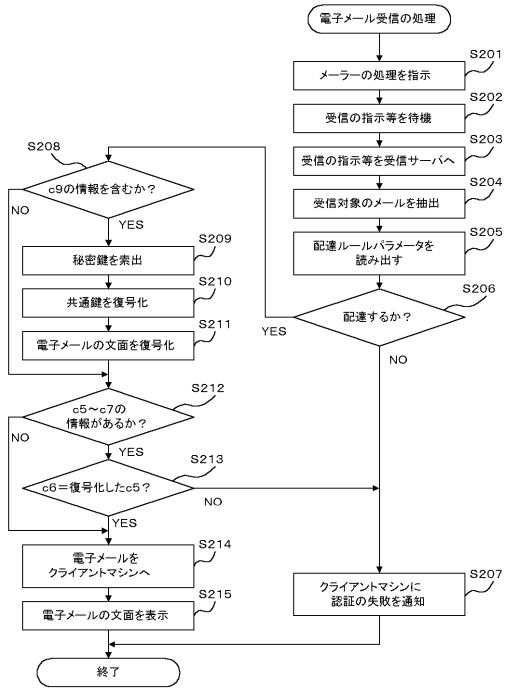
【図４】


内部バス
33
外部記憶部
36
表示部
3a(3b, 3c, 3d)
32
主記憶部
35
入力部
31
制御部
34
インターフェース
(LANへ)

【図５】


電子メール送信の処理
S101
メーラーの処理の実行を指示
S102
文面・表題・メールアドレスを待機
S103
文面・表題・メールアドレスを
クライアントマシンから送信サーバへ
S104
送信ルールパラメータを読み出す
S105
デジタル署名を施すか？
NO
YES
S106
組織情報より秘密鍵を抽出
S107
文面のハッシュ値を計算
S108
ハッシュ値を秘密鍵で暗号化
S109
暗号化を行うか？
NO
YES
S110
文面を共通鍵で暗号化
S111
共通鍵を宛先の公開鍵で暗号化
S112
電子メールを送出
終了

【図６】


電子メール受信の処理
S201
メーラーの処理を指示
S202
受信の指示等を待機
S203
受信の指示等を受信サーバへ
S204
受信対象のメールを抽出
S205
配達ルールパラメータを
読み出す
S206
配達するか？
YES
NO
S207
クライアントマシンに
認証の失敗を通知
S208
c9の情報を含むか？
NO
YES
S209
秘密鍵を素出
S210
共通鍵を復号化
S211
電子メールの文面を復号化
S212
c5～c7の
情報があるか？
NO
YES
S213
c6＝復号化したc5？
NO
YES
S214
電子メールを
クライアントマシンへ
S215
電子メールの文面を表示
終了

フロントページの続き

(56)参考文献 特開平０９－０６２５９６（ＪＰ，Ａ）
特開平１１－１２２２９３（ＪＰ，Ａ）
特開２０００－１８３９５１（ＪＰ，Ａ）
特開平１１－１６８４６０（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.[7]，ＤＢ名)
H04L 12/54
H04L 12/58
H04L 29/08