

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第5117668号

(P5117668)

(45) 発行日 平成25年1月16日 (2013. 1. 16)

(24) 登録日 平成24年10月26日 (2012. 10. 26)

(51) Int. Cl.

F I

G 0 6 Q 50/34 (2012. 01)

G 0 6 F 17/60 1 4 8

G 0 6 Q 50/26 (2012. 01)

G 0 6 F 17/60 1 5 4

G 0 6 Q 10/00 (2012. 01)

G 0 6 F 17/60 5 1 2

G 0 7 C 13/00 (2006. 01)

G 0 7 C 13/00 B

H 0 4 L 9/32 (2006. 01)

H 0 4 L 9/00 6 7 5 C

請求項の数 19 外国語出願 (全 24 頁)

(21) 出願番号 特願2005-190134 (P2005-190134)

(22) 出願日 平成17年6月29日 (2005. 6. 29)

(65) 公開番号 特開2006-18837 (P2006-18837A)

(43) 公開日 平成18年1月19日 (2006. 1. 19)

審査請求日 平成20年6月25日 (2008. 6. 25)

(31) 優先権主張番号 0407267

(32) 優先日 平成16年6月30日 (2004. 6. 30)

(33) 優先権主張国 フランス (FR)

(73) 特許権者 591034154

フランス・テレコム

フランス・7 5 0 1 5・パリ・リュ・オリ

ヴィエ・ドゥ・セレ・7 8

(74) 代理人 100099759

弁理士 青木 篤

(74) 代理人 100092624

弁理士 鶴田 準一

(74) 代理人 100102819

弁理士 島田 哲郎

(74) 代理人 100108383

弁理士 下道 晶久

(74) 代理人 100113826

弁理士 倉地 保幸

最終頁に続く

(54) 【発明の名称】 高セキュリティ・ネットワークを介した電子投票を実現するための方法およびシステム、ならびに高セキュリティ・ネットワークを介した電子投票を実現するための管理サーバ

(57) 【特許請求の範囲】

【請求項 1】

ネットワークを介して少なくとも1台の管理サーバおよび投票カウント・サーバに接続された投票用端末を用いる投票者のための高セキュリティ・ネットワークを介した電子投票を実現するための方法であって、

前記方法は、少なくとも、

認証証明書を前記管理サーバにて算出して該管理サーバから前記投票用端末へと送信するステップと、

前記少なくとも1台の管理サーバにおいて匿名参照符号を算出するステップと、

前記匿名参照符号を前記投票用端末および前記投票カウント・サーバへ送信するステップと、

前記投票者により選択された電子投票用紙および前記匿名参照符号を前記投票用端末から前記投票カウント・サーバへと送信するステップと、

前記匿名参照符号を真の参照符号値を用いて照合したときに、前記投票カウント・サーバが前記投票者の前記電子投票用紙および前記電子投票を有効化すると共に、前記電子投票用紙の表面値に従って前記電子投票用紙をカウントするステップと、

前記投票カウント・サーバから前記投票用端末へと受信確認および有権者名簿書類を送信するステップと、

前記投票用端末にて、前記認証証明書または個人キーにより電子的に署名された有権者名簿書類を算出して、該署名された有権者名簿書類を前記投票用端末から前記少なくとも

10

20

1 台の管理サーバへと送信するステップと、

前記少なくとも 1 台の管理サーバが、前記の署名された有権者名簿書類の署名値を照合したとき、前記投票用端末を用いる前記投票者の投票動作を締め切るステップと、
を有する、高セキュリティ・ネットワークを介した電子投票を実現するための方法。

【請求項 2】

前記方法が、前記投票カウント・サーバから前記投票用端末へと電子有権者名簿書類を送信するステップをさらに有することを特徴とする、請求項 1 記載の方法。

【請求項 3】

前記方法が、前記管理サーバにて単用パスワードを算出して前記管理サーバから前記投票者へと前記単用パスワードを送信するステップをさらに有しており、前記単用パスワードの送信は、前記認証証明書の送信と同時にには行われないことを特徴とする、請求項 1 または 2 に記載の方法。

【請求項 4】

前記認証証明書を算出および送信するステップは、前記投票用端末を使用中の前記投票者による前記電子投票への参加許可の要求が前記投票用端末から呈示されたときに実行され、

前記参加許可の要求は、少なくとも前記投票者の個人識別データを含み、

前記認証証明書は、前記管理サーバが前記個人識別データを真の値と照合したときに、算出かつ送信されることを特徴とする、請求項 3 記載の方法。

【請求項 5】

前記投票者に対して専用とされる単用パスワードを算出して送信するステップは、前記管理サーバが前記個人識別データを真の値と照合したときに、かつ前記認証証明書の送信に追従して、条件次第で実行されることを特徴とする、請求項 3 または 4 記載の方法。

【請求項 6】

前記単用パスワードを算出して送信するステップは、前記管理サーバおよび前記投票カウント・サーバから独立した専用サーバにより実行され、

前記専用サーバは、前記投票者に関係付けられた一つのかつ唯一の単用パスワードを算出することを特徴とする、請求項 3 から 5 のいずれか一項に記載の方法。

【請求項 7】

前記管理サーバと、前記投票カウント・サーバと、前記専用サーバとの間におけるメッセージの交換は、好首尾なゼロ知識認証プロトコルに従って、前記管理サーバ、前記投票カウント・サーバおよび前記専用サーバの各々の間にて実行されることを特徴とする、請求項 6 記載の方法。

【請求項 8】

前記投票者に対して専用とされる認証証明書および単用パスワードの送信は、別体の送信チャンネルにより実行されることを特徴とする、請求項 1 から 7 のいずれか一項に記載の方法。

【請求項 9】

ネットワークを介して少なくとも 1 台の管理サーバおよび投票カウント・サーバに接続された投票用端末を用いる投票者のための高セキュリティ・ネットワークを介した電子投票を実現するためのシステムであって、少なくとも、

前記少なくとも 1 台の管理サーバのレベルにおいて、

認証証明書を算出して前記投票用端末へと送信する手段と、

匿名参照符号を算出する手段と、

前記匿名参照符号を、前記投票用端末および前記投票カウント・サーバへ送信する手段と、
を備え、

前記投票カウント・サーバのレベルにおいて、

前記匿名参照符号を受信する手段と、

前記投票用端末から送信されたメッセージであって前記投票者により選択された少なくとも 1 枚の電子投票用紙および前記匿名参照符号を含むメッセージを受信する手段と、

10

20

30

40

50

前記匿名参照符号を真の参照符号値を用いて照合する手段と、
前記投票者の前記電子投票用紙および前記電子投票を有効化する手段と、
前記電子投票用紙の表面値に従って前記電子投票用紙の投票をカウントする手段と、
受信確認のメッセージおよび有権者名簿書類を前記投票用端末に送信する手段と、を備え、
前記少なくとも1台の管理サーバのレベルにおいて、
署名された有権者名簿書類の署名値を照合したとき、前記投票用端末を用いる前記投票者の投票動作を締め切る手段と、を備えることを特徴とする、高セキュリティ・ネットワークを介した電子投票を実現するためのシステム。

【請求項10】

10

投票用端末を用いる投票者のための高セキュリティ・ネットワークを介した電子投票を実現するための管理サーバであって、少なくとも、
認証証明書を算出して前記投票用端末に送信する手段と、
匿名参照符号を算出して、前記投票用端末および投票カウント・サーバへ送信する手段と、

前記投票用端末から、前記認証証明書または個人キーによって電子的に署名された有権者名簿書類を受信する手段と、

前記の署名された有権者名簿書類の署名値が照合されたときに、前記投票用端末を用いる前記投票者の投票動作を締め切る手段と、
を備えることを特徴とする、高セキュリティ・ネットワークを介した電子投票を実現するための管理サーバ。

20

【請求項11】

前記管理サーバが、さらに、
投票に対する区域および候補者に従って有権者リストを制御する第1管理サーバと、
前記第1管理サーバおよび投票カウント・サーバから独立した専用サーバである第2管理サーバであって、前記投票者に関係付けられて該投票者に送信される一つのかつ唯一の単用パスワードを算出する機能を有する専用サーバである第2管理サーバと、
を備えることを特徴とする、請求項10記載の管理サーバ。

【請求項12】

前記第1管理サーバ、および前記専用サーバである前記第2管理サーバは、少なくとも、
一つ以上の区域に接続された投票のリスト、および、前記投票に対する候補者のリストを表すデータを記憶する手段と、

30

一つの小規模アプリケーションが、一つの区域に関係付けられると共に前記候補者のリストと前記電子投票用紙の暗号化キーとを含むような1群の小規模アプリケーションをリストの形態で算出する手段と、を備え、

前記第2管理サーバは、各々の前記小規模アプリケーションを前記第1管理サーバに送信する手段を備えることを特徴とする、請求項11記載の管理サーバ。

【請求項13】

前記第1管理サーバは、少なくとも、
各々の前記小規模アプリケーションのリストを記憶する手段と、
各々の前記小規模アプリケーションをコンパイルすると共にコンパイルされた前記小規模アプリケーションに署名する手段と、

40

各々の前記区域および各々の前記小規模アプリケーションに対して候補者のリストを抽出して発行する手段と、

署名された前記小規模アプリケーションを、専用サーバである前記第2管理サーバと、関連する各々の前記投票者に対する前記投票用端末とに送信する手段とを具備することを特徴とする、請求項12記載の管理サーバ。

【請求項14】

前記第1管理サーバおよび前記第2管理サーバは、さらに、算出されて前記投票者に送

50

信された前記単用パスワードがコードにより保護されるのを許容するコード化手段を具備することを特徴とする、請求項 10 または 11 記載の管理サーバ。

【請求項 15】

前記第 1 管理サーバまたは前記第 2 管理サーバは、送信されたメッセージ、特に電子投票用紙の機密性を確実にするために、前記メッセージが結合されかつ暗号化されることを許容する公開キーであって前記小規模アプリケーションと共に送信される公開キーを記憶する手段を具備することを特徴とする、請求項 10 から 14 のいずれか一項に記載の管理サーバ。

【請求項 16】

前記第 1 管理サーバ、および専用サーバである前記第 2 管理サーバは、各々、認証キーのリストを生成する手段を具備し、

前記投票用端末を用いる各々の前記投票者に対しては一对の認証キーが割り当てられ、

前記一对の認証キーは、専用サーバである前記第 2 管理サーバにより生成された第 1 認証キーと、前記第 1 管理サーバにより生成された第 2 認証キーとにより形成され、

前記第 1 管理サーバは、前記第 2 認証キーのリストを生成すると共に、投票に該当する投票者に対する投票者の識別情報の値と、当該投票者に関係付けられた前記第 2 認証キーに対するハッシュ値とにより形成されたデータの対を、専用サーバである前記第 2 管理サーバに送信し、

専用サーバである前記第 2 管理サーバは、前記第 1 認証キーに対する前記第 2 認証キーの前記ハッシュ値の組み合わせの動作を実行すると共に、前記第 1 認証キーのハッシュ値を算出し、かつ、前記第 1 認証キーおよび前記第 2 認証キーの前記ハッシュ値により形成された対を前記投票カウント・サーバに送信することを特徴とする、請求項 11 から 15 のいずれか一項に記載の管理サーバ。

【請求項 17】

前記第 1 管理サーバは、さらに、

特定された投票者のみが投票に参加することを許可すべく認証証明書のリストを算出する手段と、

前記認証証明書に対する破棄リストを制御する手段と、

前記投票用端末を用いる前記特定された投票者に対して関係付けられた前記認証証明書を前記投票用端末に送信する手段と、

を具備することを特徴とする、請求項 11 から 16 のいずれか一項に記載の管理サーバ。

【請求項 18】

投票用端末を用いる投票者のための高セキュリティ・ネットワークを介した電子投票の票をカウントする投票カウント・サーバであって、少なくとも、

匿名参照符号を少なくとも 1 台の管理サーバから受信する手段と、

前記投票用端末から送信されたメッセージであって前記投票者により選択された少なくとも 1 枚の電子投票用紙および前記匿名参照符号を含むメッセージを受信する手段と、

前記匿名参照符号を真の参照符号値を用いて照合する手段と、

前記投票者の前記電子投票用紙および前記電子投票を有効化する手段と、

電子投票用紙の表面値に従って前記電子投票用紙の投票をカウントする手段と、

受信確認のメッセージを前記投票用端末に送信する手段と、
を備えることを特徴とする、投票カウント・サーバ。

【請求項 19】

電子有権者名簿書類を算出して前記投票用端末に送信する手段を備えることを特徴とする、請求項 18 記載の投票カウント・サーバ。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、高セキュリティ (security) ・ネットワークを介した電子投票を実現するための方法およびシステムに関する。また一方で、本発明は、高セキュリティ・ネットワー

10

20

30

40

50

クを介した電子投票を実現するための管理サーバに関する。

【背景技術】

【0002】

自動化された投票のための方法およびシステムは、関連する心理的、人的および政治的な含みに対する綿密な調査の主題であると共に、それにより呈示される問題を解決し得る技術的解決策である。

【0003】

これらの方法およびシステムの第1の形式によれば、自身の票を投ずる投票者の識別情報(identity: ID)は手動で制御される。この制御によれば、電子投票システムに対するアクセスが付与されており、そのときに当該システムは単に、信頼性の高い様式で開票機(vote counting machine)に対する電子投票用紙の経路設定を制御せねばならない。

10

【0004】

前述の第1の形式による方法およびシステムは、実質的に米国特許出願公報第2003/208395号の先行技術文献に記述された方法およびシステムに対応している。この米国特許出願公報においては、たとえば小規模アプリケーション(すなわち、「アプレット(applet)」)により構成される電子投票用紙が、自身の票を投ずる投票者により当該投票者のコンピュータに対してロードされると共に、上記電子投票用紙の送信と、自身の票を投ずる投票者の識別情報の照合と、投票者により送信される電子投票用紙の受信とに関する動作が、同一のサーバにより実施される。このような認証方法は、バイオメトリックスを利用したバイオメトリック(biometric)形式になっている。

20

【0005】

上記の米国特許出願公報にて記述された方法およびシステムによれば、自身の票を投ずる投票者に対する強力な認証プロセスが実現され得るが、投票者の物理的な移動が必要となる。

【0006】

さらに、自身の票を投ずる投票者は、自身の電子投票用紙がその宛先すなわち電子投票箱に到達したか否かが明確にはなり得ない。

【0007】

第2の形式に係る自動化された投票のための方法およびシステムによれば、投票はインターネットを用いて構成され、実施され、かつ照合され得る。概略的にいえば、上記の方法およびシステムは、インターネットを介して送信されるメッセージを用いている。ここで、上記メッセージは、ミックスーネット(mix-net)・メッセージと呼ばれており、データを結合するかまたは組み合わせることにより得られている。

30

【0008】

このような第2の形式のプロセスは、たとえば、改良されたミックスーネット・メッセージが生成されることが記述された欧州特許出願公報第1374188号の先行技術文献により開示されている。

【0009】

上記のシステムにおいて、データの結合または組み合わせのモジュールが効率的な暗号化等の技術を用いる場合には、データの結合または組み合わせの処理の終了時にデータの完全性(integrity)を証明することは困難である。しかしながら、もし、データの完全性を制御する手段が導入されるならば、データの結合により得られた結合物は可逆的であり、それゆえに、送信されるデータのセキュリティ(安全性)および機密性(confidentiality)のレベルが却って低下することになる。

40

【0010】

第3の形式に係る自動化された投票のための方法およびシステムは、強力な認証手段を備える複数の専用コンピュータであって仮想ネットワークを介して相互接続がなされた複数の専用コンピュータを使用する。このような第3の形式においては、自身の票を投ずる投票者の強力な認証のためのプロセスと、認証証明書レベル3と、制御を行うことが非常に困難な非公開の仮想ネットワークの使用と、投票用端末とに基づき、最適レベルのセキ

50

ュリティが提供される。

【0011】

米国特許出願公報第2002/138341号の先行技術文献は、少なくともミックス・ネットワーク・メッセージの使用に関して、すなわち、実際の対象者について署名かつ暗号化された情報を含むテキスト・ファイルである証明書X509による強力な認証プロセスの使用に関して、前述の第3の形式に匹敵する方法およびシステムを記述している。この場合、電子投票用紙は、ハイブリッド暗号化システムによりさらに暗号化されている。

【0012】

上記の米国特許出願公報に記述されたシステムはさらに、複数のサーバを使用している。

10

【0013】

しかしながら、前述の各々のシステムおよび方法は、これらのサーバの管理者における信頼度(confidence)の判定基準に関して満足できる解決策を提供するものでない。

【0014】

上記の米国特許出願公報に記述されたシステムおよび方法において、自身の票を投ずる投票者により電子的に署名された用紙は第1コンピュータに対して受け渡され、当該第1コンピュータは、投票者の電子署名を確認すると共に、電子投票用紙を電子投票箱に送信する前に当該第1コンピュータに関する特定署名により投票者の電子署名を置き換える。

【0015】

しかしながら、トランザクションに対する媒体体としてまたは信頼された第三者として機能する上記第1コンピュータは、電子投票用紙が電子投票箱内に取り入れられるか否かを論ずる以前の段階で、匿名性を排除するための一切の領域を維持している。

20

【0016】

さらに、自身の票を投ずる投票者は空白(blank)の投票用紙を受信することになる。さらにまた、投票者の識別情報の認証は、他の一切の制御なしで投票の権限付与を行うことに等しい。暗号化された電子投票用紙は、少なくとも上記第1コンピュータにおいては、自身の票を投ずる投票者に対して接続され、日付けにより暗号化される。

【0017】

上記のような日付け式の暗号化プロセスによれば、全ての不正な様式で傍受された電子投票用紙のコピーに対する防御が可能になるが、その一方では、相当の計算処理が実施され得るという不都合を抱えている。

30

【0018】

強力な認証プロセスまたは脆弱な認証プロセスによりインターネットに対して適用されるようなネットワークを介した電子投票のための方法およびシステムの使用に伴う問題は、以下の如く要約され得る。

【0019】

ハードウェアのコストと投票の構成の論理的な複雑さのゆえに、主催者がインターネットを介した電子投票を脆弱な認証により保持した場合、全体として主催者は、少なくとも3つのレベルに関して脆弱なシステムのセキュリティに関するリスクを背負うことになる。より詳細に言えば、このようなリスクは次の(1)～(3)のように表される。

40

(1) 各々のサーバは、サービス拒否の犠牲となり得る。また一方で、各投票者は、投票者自身がコンピュータ・ウィルスの犠牲者であるならば、このようなコンピュータ・ウィルスに係る障害に不本意に巻き込まれ得る。

(2) 自身の票を投ずる各投票者自身は、投票するコンピュータを操作するサービス・プロバイダを、投票者自身の匿名性と投票の完全性に関して信頼することを余儀なくされる。

(3) 非良心的なユーザは、自身の投票の実施には助力するが、投票の信頼性を阻害しようとして、自身のコンピュータに対して付与されたコードを使用することがある。

【0020】

それゆえに、脆弱な認証によりネットワークを介した電子投票のためのシステムのアー

50

キテクチャの最も基本的な方式は、次の（イ）～（ハ）のようになる。

（イ）自身の票を投ずる投票者に対しては、任意の適切な媒体（郵便、電子メール、雑誌等）で電子投票用サーバのアドレスが知らされる。

（ロ）自身の票を投ずる投票者は投票日に、一つのコンピュータまたは別のコンピュータの端末から、通知された上記電子投票用サーバに対するアドレスを用いて当該電子投票用サーバへの接続を行う。

（ハ）電子投票用サーバは、自身の票を投ずる投票者の投票権を制御すると共に、投票者に対して「空白」の電子投票用紙を送信する。そして、投票者は当該電子投票用紙に記入して電子投票用サーバに返信し、ここで、電子投票用サーバは当該電子投票用紙を、他の電子投票用紙と共に、投じられた票として記録するかまたは記録しない。

10

【0021】

上記のような電子投票のためのシステムのアーキテクチャの方式は、下記の（i）～（iv）のレベルにて実際に遭遇するリスクを呈する。

【0022】

（i）匿名性

自身の票を投ずる投票者は、自身の投票権の照合のために、自身を特定せねばならない。もし、通信が傍受されて覗かれたならば、自身の票を投ずる投票者が誰に対して投票したかが見破られ得る。それゆえに、通信は暗号化されねばならない。上記システムにおいて所定の度合いの信頼度を形成するためには、当該システムの管理者に対する各投票者の信頼度とは無関係に、少なくとも2台の別体のサーバ、すなわち、投票に対する権利を制御すると共に自身の票を投ずる投票者を認証するための投票管理サーバ、および、投票用紙をカウントする投票カウント・サーバが使用されるべきである。

20

【0023】

匿名性は、上記2台のサーバのそれぞれの管理者の連携によってのみ排除され得る。しかしながら、1票でも一般的な投票用紙形態で実施されたのであれば、投票を主催する一切の権限機関は上記の問題に遭遇することが指摘される。

【0024】

概略的にいえば、多重サーバ・システムの大部分は、投票の結果に関心を有する人々に対して直接的に接続されてもよく、または直接的に接続されなくてもよいような種々の管理者が相互に監視するという様式で構成される。

30

【0025】

（ii）投票の終了までの結果の秘密性

通信がネットワーク・レベルでは暗号化されたとしても、投票カウント・サーバの管理者が不誠実であれば、当該管理者は投票の締め切りの前に結果を知り得る。それゆえに、投票カウント・アプリケーションのレベルにては、投票の締め切り後まで明かされない復号化キーによる暗号化を実施する必要がある。

【0026】

（iii）セキュリティ

もし、各々のサーバ・コンピュータが適切に保護されなければ、悪意のある侵入者がアクセスを行い破壊を引き起こし得る。

40

【0027】

（iv）完全性

電子投票箱が詰まって動作不良になる可能性は高い。コンピュータのハードウェアおよびソフトウェアの能力は、電子投票箱の動作不良が発見されまたは発覚したときに、それに気付いた任意の人物が上記動作不良を大規模に悪用し得る可能性を生じさせるものである。

【0028】

電子署名および証明書を用いると、上記のリスクは解消され得る。

【0029】

上記の要求を満足するような所定のシステムは、既に提案されている。このようなシス

50

テムは、特に、PKIインフラストラクチャに当てはまる。このPKIインフラストラクチャは、定義により秘密とされる個人キーであって当該個人キーに対して識別情報が関係付けられた個人すなわち自身の票を投ずる投票者によってのみ使用され得るという個人キーに対するアクセスの防御を許容するために、複数の対の公開キー／個人キーを生成するシステムにより公開キー暗号法の使用をサポートする。

【0030】

投票は3,000万人以上の投票者を含み得ることから、PKIインフラストラクチャを大規模に設置することは現在では依然として困難であり、その一方で、適切な個数の安全なブース(booth)を配備すると、大幅な経済的コストの増加を招く。

【0031】

インターネットを介した電子投票のためのシステムは、投票の機構の簡素化およびコストの節減を意図することから、上記のような形式のインフラストラクチャは容易には使用され得ない。

【0032】

また一方で、同一の主催者が高度に安全とされているインフラストラクチャを使用するとしても、試行してから一般化された使用を行うための使用コストおよび複雑さは、適切なものからは程遠い。

【0033】

強固な政治的意志のみ（すなわち、電子識別カード等の他の組織的開発、および、投票に類似する状況であるが必ずしもこの投票の形式のイベントに関連しない状況において当該インフラストラクチャの再使用を許容する関連各国における幾つかの関連団体間の密接な協力のみ）が、この種のインフラストラクチャの展開を予想し得る。

【0034】

もし、この種の状況において主催者がセキュリティの低い電子投票システムを使用するならば、投票者の信頼を失うリスクは高くなる。このことは、上記の形式のシステムを受け入れる主催者または政治的機関の信用を落とすリスクのゆえに、どんなことがあっても容認され得るものではない。

【発明の開示】

【発明が解決しようとする課題】

【0035】

本発明の目的は、上記問題点を解決すべく、特に投票の技術管理者を信頼することを投票者に強いるような従来の電子投票のための方法およびシステムの全ての不都合および制限を克服することである。

【0036】

特に、本発明の主題は、ネットワークを介した電子投票のための方法およびシステムであって、その構造は、複数の管理担当者間における不正な同意がなければ、対応する不正な試みが露見されることなく投票の完全性を阻害することができないようにするために、複数の管理担当者間に責任を分散させることを確実にし得るようになっている方法およびシステムである。

【0037】

さらに、本発明の目的は、複雑な認証システムの使用は必要としないが高度のセキュリティを有するような、高セキュリティ・ネットワークを介した電子投票を実現するための電子投票用の単純な方法およびシステムを提供することである。

【0038】

さらにまた、本発明の目的は、投票に実際に参加した投票者のリストと、制御名簿に署名した投票者のリストとの間に矛盾を生じさせるために、別の識別情報により署名された電子投票用紙を所定の識別情報に基づき提出する試みの一切の可能性を排除することによって、投票のプロセスの信用を落とそうとする任意の試みに対する防御を許容するような、高セキュリティ・ネットワークを介した電子投票を実現するための方法およびシステムを提供することである。

10

20

30

40

50

【0039】

最終的に、本発明の主題は、投票に参加したがゆえに実際に投票した投票者が電子有権者名簿に署名するための適格性の処理を導入し得るといったような、高セキュリティ・ネットワークを介した電子投票を実現するための方法およびシステムの使用である。

【課題を解決するための手段】

【0040】

上記目的を達成するために、本発明が関連する高セキュリティ・ネットワークを介した電子投票を実現するための方法は、ネットワークを介して少なくとも1台の管理サーバおよび投票カウント・サーバに接続された投票用端末を用いる投票者のための高セキュリティ・ネットワークを介した電子投票を実現するための方法であって、認証証明書を上記管理サーバにて算出して上記管理サーバから上記投票用端末へと送信するステップと、上記投票者により選択された電子投票用紙および匿名参照符号を上記投票用端末から上記投票カウント・サーバへと送信するステップと、上記匿名参照符号が真の値と照合されたときに、上記投票者の上記電子投票用紙および上記電子投票を有効化すると共に、上記電子投票用紙の表面値に従って上記電子投票用紙をカウントするステップと、上記投票カウント・サーバから上記投票用端末へと受信確認を送信するステップと、上記投票用端末にて、上記認証証明書により電子的に署名された有権者名簿書類を算出して上記投票用端末から上記管理サーバへと送信するステップとを少なくとも有し、上記管理サーバは、上記の署名された有権者名簿書類が真の値と照合されたときに、上記投票用端末を用いる上記投票者に対する投票動作の締め切りを行うことを注目すべき特徴としている。

【0041】

また一方で、本発明が関連する高セキュリティ・ネットワークを介した電子投票を実現するためのシステムは、ネットワークを介して少なくとも1台の管理サーバおよび投票カウント・サーバに接続された投票用端末を用いる投票者のための高セキュリティ・ネットワークを介した電子投票を実現するためのシステムであって、少なくとも、上記管理サーバのレベルにおいて、上記管理サーバにて認証証明書を算出して上記管理サーバから上記投票用端末へと送信するモジュールを備え、また一方で、上記投票カウント・サーバのレベルにおいて、上記投票用端末から送信されたメッセージであって上記投票者により選択された少なくとも1枚の電子投票用紙および匿名参照符号を含むメッセージを受信して処理するモジュールと、受信された上記匿名参照符号を真の値と照合する手段と、上記投票者の上記電子投票用紙および上記電子投票を有効化するモジュールと、上記電子投票用紙の表面値に従って上記電子投票用紙の投票をカウントするモジュールと、受信確認のメッセージを算出して上記投票用端末に送信するモジュールとを備えることを注目すべき特徴としている。

【0042】

また一方で、本発明の別の形態は、投票用端末を用いる投票者のための高セキュリティ・ネットワークを介した電子投票を実現するための管理サーバであって、少なくとも、認証証明書を算出して上記投票用端末に送信する手段と、

上記投票用端末を用いる上記投票者に対する匿名参照符号を算出して送信する手段と、
上記投票用端末から、電子的に署名された有権者名簿書類を受信する手段と、

上記の署名された有権者名簿書類を真の値と照合する手段であって、上記投票用端末を用いる上記投票者に対する投票動作を締め切り得る手段とを備える管理サーバである。

【0043】

また一方で、本発明のさらに別の形態は、投票用端末を用いる投票者のための高セキュリティ・ネットワークを介した電子投票の票をカウントする管理サーバであって、少なくとも、

上記投票用端末から送信されたメッセージであって上記投票者により選択された少なくとも1枚の電子投票用紙および匿名参照符号を含むメッセージを受信して処理する手段と、

受信された上記匿名参照符号を真の値と照合する手段と、

上記投票者の上記電子投票用紙および上記電子投票を有効化する手段と、
電子投票用紙の表面値に従って上記電子投票用紙の投票をカウントする手段と、
受信確認のメッセージおよび電子有権者名簿書類を算出して上記投票用端末に送信する
手段とを備える管理サーバである。

【0044】

本発明が関連するネットワークを介した電子投票を実現するための方法およびシステム
は、大幅に節減された開発コストおよび／または配備コストでもって、かつ、認証性およ
び機密性の最適条件下で、政治的投票、または、個人に関する公開の調査もしくは非公開
の調査を行うために使用され得る。

【発明を実施するための最良の形態】

10

【0045】

前述のような本発明のネットワークを介した電子投票を実現するための方法およびシス
テム、ならびに高セキュリティ・ネットワークを介した電子投票を実現するための管理サ
ーバは、添付の図面（図1～図7）を検証すると共に下記の本願明細書の記述内容を読み
取ることによって、より良く理解されるであろう。

【0046】

以下、図1および追従する図2～図7を参照しながら、本発明が関連するネットワーク
を介した電子投票を実現するための方法をより詳細に説明する。

【0047】

図1は、本発明に係るネットワークを介した電子投票を実現するための方法を実行する
際に必要な複数のステップを例示的に説明するためのフローチャートであり、図2および
図3は、図1に示された本発明に係る方法の特定のステップを実行するための例示的かつ
詳細なフローチャート（その1およびその2）である。なお、これ以降、前述した構成要
素と同様のものについては、同一の参照番号または参照符号を付して表すこととする。

20

【0048】

全般的に、本発明が関連するネットワークを介した電子投票を実現するための方法は、
ネットワークを介して少なくとも1台の管理サーバSAに接続された投票用端末Teを使用し
ている投票者Euと、投票カウント・サーバSCVとの間で実行される。

【0049】

概略的にいえば、投票用端末Teは、以下においてさらに記述される如く、インターネッ
トに接続されたパーソナルコンピュータ、投票所(polling station)に設置されると共に
インターネットに接続された特定のブース、または、これもまたインターネットに接続さ
れたブースであって、特に前述の管理サーバSAおよび投票カウント・サーバSCVに対して
接続された任意の公共の場所におけるブースなどの、種々の形式の端末により構成され得
る。

30

【0050】

本発明が関連するネットワークを介した電子投票を実現するための方法の一つの注目す
べき態様によれば、上記方法は、管理サーバSAにて認証証明書(authentication certific
ate)CAと、当該投票者専用にUPWeと示されたパスワードとを算出して、当該管理サーバSA
から、投票用端末Teを使用中の投票者Euおよび投票用端末Teに対して上記パスワードを送
信するステップAを少なくとも有する（図1参照）。

40

【0051】

ステップAにおける計算および送信の動作は、次の関係により記号化される。

【0052】

[CA, UPWe]

SA————→Te

概略的にいえば、上記関係にて例示された如くメッセージにおいて送信されるデータの
記号であって括弧（[]）内に示された記号は、以下においてさらに説明される如く、所
定の度合いの暗号化による暗号化様式に基づいた当該データの送信に対応することが示さ
れている。

50

【0053】

当然のことながら、上記のような単用パスワード、特にUPWeは、部外者による当該パスワードの公開（opening）および不正使用に関する一切のリスクを防止すべく、暗号化形態で投票用端末Teを使用中の投票者Euおよび／または投票用端末Teに対して送信されることが認識されるであろう。

【0054】

認証証明書CAまたは単用パスワードUPWeを算出して送信するための条件は、以下においてさらに説明される。

【0055】

図1のステップAは、ステップB₀により追従される。このステップB₀は、EBと示された電子投票用紙であって投票用端末Teを使用中の投票者Euにより使用されかつ当該投票者専用の匿名参照符号(anonymous reference)AREuを伴う電子投票用紙を、投票用端末Teから投票カウント・サーバSCVへ送信する段階を含む。

10

【0056】

図1のステップB₀は、あくまで例示的に、投票用端末Teによる電子投票用紙EBおよび匿名参照符号AREuの送信とその受信とを次の記号形態で示している。

【0057】

[EB、AREu]

Te————→SCV

上記のステップB₀の送信の動作および投票カウント・サーバSCVによる受信の動作は、つぎに、ステップB₁において投票カウント・サーバのレベルにて匿名参照符号AREuの値を真の値と照合するという段階により追従される。

20

【0058】

このような照合の段階を含むステップB₁において肯定的な応答になっている場合（匿名参照符号AREuの値が真の値と一致する場合）には、本発明が関連する上記方法は、電子投票用紙の表面値(face value)に従い当該電子投票用紙をカウントするために、電子投票用紙EBと投票用端末Teを使用中の投票者Euの電子投票とを有効化する段階を有する。

【0059】

通常、電子投票用紙の表面値は、投票用端末Teを使用中の投票者の選択に従う有効投票用紙に対応する表面値と、たとえば投票用紙の内容に関して一般的な除外例に従って規定される空白の投票用紙または無効投票用紙に対応する表面値とにより構成され得る。

30

【0060】

図1に関し、ステップB₁の照合試験において否定的な応答になっている場合（匿名参照符号AREuの値が真の値と一致しない場合）には、ステップAにおけるプロセスを再開始すると共に、任意に選択可能であって限られた回数での試行ではあるが、同一の投票用端末（電子端末）Te、および同一の投票用端末Teを使用中の投票者Euに対するプロセスの再開始を試行すべく、戻りのステップB₂が用意されていることが示されている。

【0061】

逆にいえば、ステップB₁の照合試験において肯定的な応答になっている場合、電子投票用紙EBおよび電子投票の有効化はステップB₃にて示されており、このステップB₃の動作により、明示された電子投票用紙の表面値に従い当該電子投票用紙のカウントが可能になる。

40

【0062】

上記のような電子投票用紙と電子投票とを有効化するステップB₃は、ステップB₄により追従される。このステップB₄は、受信確認ACWと、DVRと称された電子有権者名簿書類(electronic electoral register document)とを投票カウント・サーバSCVから投票用端末Teへ送信する段階を含む。

【0063】

上記電子有権者名簿書類は、投票者により、投票証明書(voting attestation)として使用され得る。上記電子有権者名簿書類はまた、投票動作を有効化すべく管理サーバSAによ

50

り使用される署名済み有権者名簿書類を生成するためにも同程度に使用され得る。図1において、受信確認および有権者名簿書類を送信するステップは、記号様式で次のように表現される。

【0064】

[ACW、DVR]

SCV————→Te

次にステップB₄は、好適には、ステップCにより追従され得る。このステップCは、ユーザにより電子的に署名されてSDVRと表された有権者名簿書類を投票用端末Teにて算出して当該投票用端末Teから管理サーバSAへと送信する段階を含む。上記の電子的に署名された有権者名簿書類はたとえば、投票カウント・サーバSCVにより提供された電子有権者名簿書類に署名することにより得られる。この署名は、好適には、上記認証証明書を介して提供される。

10

【0065】

投票用端末Teから管理サーバSAへの送信動作は、記号様式で次のように表現される。

【0066】

[SDVR]

Te————→SA

電子的に署名された有権者名簿書類SDVRの受信に続いて、管理サーバSAは、署名された有権者名簿書類SDVRを真の値と照合するステップD₀を実施する。このステップD₀の動作は、記号様式では次のように表現される。

20

【0067】

v (SDVR) ≡ 真

ステップD₀の真の値に対する署名済み有権者名簿書類の照合のための試験において否定的な応答になっている場合には、投票用端末Teを使用中の投票者Euに対して許可された1回以上であるが限られた回数の新たな投票試行を行うために、ステップAに戻るためのステップD₂が実施され得る。

【0068】

逆にいえば、ステップD₀の真の値に対する署名済み有権者名簿書類の照合のための試験において肯定的な応答になっている場合には、管理サーバSAは、投票用端末Teを使用している投票者Euに対する投票動作の締め切りを行う（ステップD₁）。

30

【0069】

本発明が関連する高セキュリティ・ネットワークを介した電子投票を実現するための方法は、単用パスワードUPWeが投票用端末Teを使用中の投票者Euの各々に対する一意的な値として算出され得るという点で、特に注目すべきであると考えられる。

【0070】

Euの投票の締め切り後、または管理サーバにてステップB₂およびD₂からステップAに戻った後、上記管理サーバは、上記単用パスワードの削除と、たとえば当該パスワードの破棄とを実施する。

【0071】

図2に示された如く、本発明が関連する上記方法の一つの特に好適な態様によれば、認証証明書CAまたは投票者Euに接続された単用パスワードUPWeを管理サーバSAにて算出して、当該管理サーバSAから投票用端末Teおよび当該投票用端末Teを使用中の投票者Euへと送信する段階を含む2つの動作は、好適には同時に実行されない（図2のステップA'）。

40

【0072】

上記のような2つの送信動作の非同時性は、図2において連続的な記号関係により示される。

【0073】

[CA]

SA——→Te

[UPWe]

50

SA————→Eu

前述の2つの送信動作の非同時性によれば、単一メッセージの傍受の危険性、および特に、同時には送信されない単用パスワードUPWeに対して認証証明書CAが伴うという危険性が軽減され得る。

【0074】

当然のことながら、図1におけるステップAは一般的な形式で実施可能であり、認証証明書CAの次に単用パスワードUPWeを管理サーバSAにて算出して当該管理サーバSAから投票用端末Teへと送信する段階を含むといったような前述のステップA'は、投票用端末Teを使用中の投票者Euによる投票用端末Teからの投票への参加許可の要求時に実施される。

【0075】

前述の参加許可の要求は、少なくとも投票者Euの個人識別データ（personal identification data）を含むと共に、上記認証証明書は、上記管理サーバにより上記個人識別データが真の値と照合されたときに、算出されて送信される。

【0076】

図3には対応動作が示されている。この場合、ステップA₀は、記号様式により、下記の記号関係による要求の送信を表現しかつ例示している。

【0077】

ReEuTe[IDEu]

Te————→SA

次に管理サーバSAは、当然のことながら、ステップA₁を実行する。このステップA₁では、ユーザの識別データIDEuを復号化した後で当該データを真の値と照合する試験が実施される。

【0078】

ステップA₁の試験において否定的な応答になっている場合には、ステップA₀への戻りの動作を実行するためのステップA₂が用意され得るが、この戻りの動作は、図1に示されたステップB₂およびD₂の戻りの動作に匹敵する。

【0079】

逆にいえば、ステップA₁の試験において、投票用端末Teを使用中の投票者の個人的な識別データIDEuが真の値と照合された結果として肯定的な応答になっている場合には、認証証明書CAの算出およびその後の単用パスワードUPWeの算出がステップA₃において実施され得る。

【0080】

図3に示された如く、投票者Euに対して専用とされる単用パスワードUPWeの算出および送信を含む動作と、上記単用パスワードUPWeを実際に送信する動作とは、投票用端末Teを使用中の投票者Euの個人識別データIDEuが管理サーバSAにより真の値と照合されたときに、条件次第で実施される。

【0081】

さらに、ステップAの変形例である図2のステップA'に示された実施方法によれば、このような動作は、好適には、認証証明書CAの送信に続いて実施される。

【0082】

図4は、本発明の主題に従ってネットワークを介した電子投票を実現するためのシステムのアーキテクチャを例示的に示す概略図である。図4には、インターネットを介して管理サーバSAおよび投票カウント・サーバSCVに対して相互接続がなされた種々の形式の投票用端末Te1、Te2およびTe3を備えるアーキテクチャが概略的に示されている。

【0083】

前述の図4において、本発明の主題に係る電子投票のための方法における複数のステップは、上記の各構成要素のレベルで実施されるものとして示される。

【0084】

非限定的な例として、投票用端末Te1は、投票所における専用ブースにより構成可能であり、投票用端末Te2は、個人として投票用端末使用中の投票者の家庭に設置されたパー

10

20

30

40

50

ソナルコンピュータにより構成可能であり、かつ、投票用端末Te3は、特に投票専用ではない公共の場所に設置されたブースにより構成され得ることが示されている。

【0085】

本発明が関連するネットワークを介した電子投票を実現するための方法に従う各々の動作は、上記にて言及かつ記述された如く、2台のサーバ、すなわち管理サーバSAおよび投票カウント・サーバSCVにより実施される。

【0086】

本発明が関連する高セキュリティ・ネットワークを介した電子投票を実現するための方法およびシステムは、使用される単用パスワードにより、部外者による不正行為の危険性が全く無いように完璧な完全性をもって、投票の保持に関する高レベルのセキュリティが許容される。

10

【0087】

但し、投票の構成に対して責任を負う者により行われる可能性のある不正操作および／または不正行為の一切の危険性に対して防御を行うために、本発明が関連する上記システム、および本発明が関連する上記方法は、少なくとも単用パスワードを算出して送信する機能を有する専用サーバによって、特に好適な形式で実施される。この専用サーバは、図4に関して前述された実際の管理サーバおよび投票カウント・サーバから独立している。

【0088】

当然のことながら、上記専用サーバは、投票用端末使用中の投票者に関係付けられた一つのかつ唯一の単用パスワードUPWeを算出する。

20

【0089】

図5は、本発明の主題に従ってネットワークを介した電子投票を実現するためのシステムの好適な変形例に係るアーキテクチャの例示的なブロック図である。図5には、管理サーバおよび投票カウント・サーバから独立したサーバ、特に専用サーバSDを備えるといったような、本発明の主題に従って高セキュリティ・ネットワークを介した電子投票を実現するシステムのための対応アーキテクチャが示されている。

【0090】

概略的に、単用パスワードの算出および送信が専用サーバから実施されるという図5に示されたアーキテクチャを実現するために、いってみれば、図4に示された管理サーバSAを、第1管理サーバSA1と、単用パスワードUPWeの算出、送信および処理の権限が付与された唯一のサーバである専用サーバSDとして機能する第2管理サーバSA2とに分割することを考慮し得ることが示されている。

30

【0091】

それゆえに、第1管理サーバSA1と、専用サーバとして機能する第2管理サーバSA2とに対して、以下に説明される如く、明確に定義されたタスクがそれぞれ割り当てられ得ることは特に理解されるであろう。

【0092】

図5に示された如く、第2管理サーバである専用サーバSA2(SD)は、好適には、この専用サーバのみが権限を付与された単用パスワードUPWeに関する算出に加えて、その送信および処理をもって、図1および図3に示されたステップA₁、A₂およびA₃を実施し得る。

40

【0093】

それゆえに、第1管理サーバSA1は、たとえば図1に示された動作D₀、D₁およびD₂を実施するために、有権者リストの実際の管理および投票の締め切りの制御に関して専用とされ得る。

【0094】

本発明が関連する高セキュリティ・ネットワークを介した電子投票を実現するためのシステムの特に注目すべき態様によれば、各々の管理サーバ間、すなわち、第1管理サーバSA1と、専用サーバSDとして機能する第2管理サーバSA2と、投票カウント・サーバSCVとの間におけるメッセージの交換は、それぞれ、これらのサーバ等の複数の構成要素間で実線として図示されている矢印により示された非常に高レベルのセキュリティによる好首尾

50

な認証プロトコルに続いて実施されることが示されている。

【0095】

使用される認証プロトコルは、非限定的な例として、ゼロ知識認証プロトコル(zero-knowledge authentication protocol)に対応することが可能であり、上記第1管理サーバと、専用サーバとして機能する上記第2管理サーバと、上記投票カウント・サーバSCVとの間において当然のことながら暗号化形態で送信される種々のメッセージは、非常に高レベルのセキュリティをもって暗号化され、かつ、前述の好首尾な認証動作（認証プロトコル）に続いて送信される。

【0096】

最終的に、投票用端末Teまたは図4に示された電子端末（投票用端末）Te1～Te3の各々と、第1管理サーバSA1、第2管理サーバSA2および投票カウント・サーバSCVとの間におけるメッセージのトランザクション（transactions）または交換は、高セキュリティ・レベルの暗号化法をもって暗号化されたメッセージを介したトランザクションを示す鎖線の矢印により表される。

【0097】

本発明が関連すると共に図1～図3に示されたようなネットワークを介した電子投票を実現するための方法により実施される一連のステップは、次の表のように、種々の構成要素の間、すなわち投票用端末Te、第1管理サーバSA1、専用サーバSDとして機能する第2管理サーバSA2、および投票カウント・サーバSCVの間における時間的および空間的な関係に従って示される。

【0098】

表

T1: ReEu[IDEu]

T2: Z0[CA]

T3: Z1[UPWe]

T4: Z2[AREu]

T5: [CA, UPWe]

T6: [CA, UPWe]

T7: [AREu]

T8: [EB, UPWe]

T9: [ACW, DVR]

T10: [SDVR]

上記の表において、上記管理サーバと上記投票カウント・サーバとの間におけるトランザクションZ0～Z2の全ては暗号化メッセージの送信を表しており、上記で言及された如く、上記の構成要素間のトランザクションは好首尾で強力な認証プロトコルの条件を満足していることに留意されたい。

【0099】

これによって、特に、投票の管理者の権限に対して完全にもしくは部分的に委ねられる種々の構成要素間におけるトランザクションの独立性および完全性が確実に保証される。

【0100】

最終的に、認証証明書および単用パスワードUPWeを、上記管理サーバから、特にSDサーバとして機能する第2管理サーバSA2から、投票者Euおよび投票用端末Teへと送信する動作に関していえば、当該動作は特に好適な様式で別体の送信チャネルにより実行され得ることが示されている。

【0101】

特に図2のステップA'に示された認証証明書CAの送信に関していえば、前述の送信は、電子端末（投票用端末）Teの上記の表に示されたステップT1における投票に対する許可の要求が、上記専用サーバ、すなわち第2管理サーバSA2に対して送信されたことに続いて、インターネットによるネットワークを介して実施され得ることが示されている。

【0102】

10

20

30

40

50

逆にいえば、単用パスワードUPWeの送信は、たとえば、メッセージ・サービス、電子メール、または、選択的に投票の日付前に投票用端末使用中の投票者Euに対して名指しで送信される書簡等の完全に別体の送信チャネルを介して実施され得る。

【0103】

特に、SMSと称される短メッセージによる単用パスワードの送信が好適に着想され得ることが示されている。なぜならば、この場合には、投票用端末使用中の投票者Euは、例えば携帯電話を有しており、この携帯電話に対するアクセスは、上記使用中の投票者のみが制御するデバイスの識別コード（idenfication code）により保護されるからである。

【0104】

ユーザ端末Teまたは当該投票用端末Teを使用中の投票者Euに対する単用パスワードUPWeの送信が実施された場合（T5:[CA, UPWe]）、上記使用中の投票者Euは投票日に、自身の認証証明書CAおよび単用パスワードUPWeを呈示するために、専用サーバである第2管理サーバSA2(SD)に対して接続する（T6:[CA, UPWe]）。単用パスワードUPWeの処理が許可された唯一の第2管理サーバSA2(SD)は、CAおよびUPWeの対の照合の後に、上記使用中の投票者に対する匿名参照符号AREuの算出を実施する。この匿名参照符号AREuは、投票用端末Teに対して送信される（T7:[AREu]）。 10

【0105】

上記使用中の投票者に対する匿名参照符号AREuは、以下においてさらに記述される如く、ハッシュ関数(hash function)から得られる数値を含み得る。上記匿名参照符号は好適には、上記単用パスワードに従う。但し、上記匿名参照符号はまた、上記単用パスワードから独立しても獲得され得る。 20

【0106】

つぎに、ユーザ端末（投票用端末）Teは、投票カウント・サーバSCVに対して接続を行うと共に、自身の電子投票用紙EBと投票用端末使用中の投票者に対する匿名参照符号AREuとを当該サーバに送信する（T8:[EB, UPWe]）。上記のプロセスは、受信確認と電子有権者名簿書類とを送信してから（T9:[ACW, DVR]）、署名された有権者名簿書類SDVRを投票用端末Teから第1管理サーバSA1へとトランザクションを介して送信する動作（T10:[SDVR]）によって投票用紙と投票とを有効化するという追従動作へと継続される。

【0107】

図6は、図5に示された本発明の主題に係る電子投票システムを使用するユーザにより行われる電子投票セッションを例示的かつ詳細に示す図であり、図7は、図5に示された電子投票システムのアーキテクチャにより一連のステップまたはプロトコルを実行するための例示的かつ詳細な図である。 30

【0108】

ここでは、図6および図7を参照しながら、本発明の主題に係るネットワークを介した電子投票を実現するためのシステムであって、単用パスワードの算出および制御を行うことがさらに詳細に意図された専用サーバを備えるシステムのアーキテクチャに対する動作手順に関し、より詳細な説明を行うこととする。

【0109】

上記の図6において、投票用端末使用中の投票者Euは、移動電話端末と、インターネットに接続された例えばパーソナルコンピュータ等の電子端末Teとを有すると仮定されることが示されている。 40

【0110】

図5に関する記述において上記で言及された如く、第1管理サーバSA1は、実質的に有権者リスト・サーバとして機能し、第2管理サーバSA2は、実質的に専用サーバSDとして機能し、かつ、投票カウント・サーバSCVは、上記の第1および第2管理サーバに対して相互接続がなされる。

【0111】

好適には、図6に示された如く、本発明が関連するネットワークを介した電子投票を実現するためのシステムは、第1管理サーバSA1または第1管理サーバSA2のいずれか一方の 50

管理サーバのレベルにて、認証証明書CAと、投票者Euにとって専用とされる単用パスワードUPWeとを算出して当該管理サーバから当該投票者Euおよび当該投票用端末Teへと送信するモジュールを備える。

【0112】

図6および図5を参照すればわかるように、前述のような認証証明書CAおよび単用パスワードUPWeを算出するモジュールは、図1に示されると共に上記の表中に示されたステップA₀、A₁、A₂およびA₃の動作の実施を許容する専用サーバSDとして機能する第2管理サーバのレベルにて設置されることが示されている。

【0113】

本発明が関連する上記システムは、投票カウント・サーバSCVのレベルにて、メッセージを受信して処理するモジュールを備える。ここで、上記メッセージは、投票用端末Teにより送信されたメッセージであって、当該投票者により選択された電子投票用紙EBと、たとえば単用パスワードUPWeに従うと共に投票用端末使用中の投票者にとって専用とされるような上記使用中の投票者に対する匿名参照符号AREuとを少なくとも含む。上記のようなメッセージを受信するモジュールは、図1のステップB₀にて投票用端末Teにより送信されたメッセージを投票カウント・サーバが受信することに対応する。

10

【0114】

投票カウント・サーバSCVはさらに、投票用端末使用中の投票者に対する匿名参照符号AREuを真の値と照合し、この結果として、受信された専用の単用パスワードを真の値と照合するモジュールを備える。

20

【0115】

このモジュールは、図1のステップB₁の実施に対応する。より詳細に言えば、上記モジュールは、たとえば、専用サーバSDとして機能する上記第2管理サーバから投票カウント・サーバSCVに対して送信された上記使用中の投票者に対する匿名参照符号AREuまたは単用パスワードUPWeと、先に投票用端末Teにより投票カウント・サーバSCVに対して送信されている匿名参照符号AREuとを比較することによって、前述の照合の動作を実施することが理解されるであろう。

【0116】

上記投票カウント・サーバはまた、電子投票用紙EBの表面値の記述において前述した如く、この電子投票用紙EBの投票をカウントするモジュールと関係付けられた、当該電子投票用紙と当該投票者の電子投票とを有効化するモジュールも備える。前述の各モジュールは、図1および図5のステップB₃の実施に対応する。

30

【0117】

最終的に、投票カウント・サーバSCVは、受信確認のメッセージと電子有権者名簿書類とを算出して投票用端末Teに送信するモジュールを備える。このモジュールの動作は、図1および図5のステップB₄にて実施される。

【0118】

さらに、図6および図7に基づいて、種々の構成要素間、すなわち第1管理サーバSA1と、専用サーバSDとして機能する第2管理サーバSA2と、投票カウント・サーバSCVと、投票用端末Teとの間でメッセージおよびトランザクションを交換するためのプロトコルの好適な動作手順が呈示される。

40

【0119】

概略的に言えば、図6を参照すればわかるように、上記管理サーバ、特に専用サーバとして機能する第2管理サーバSA2は、投票のリスト、すなわち、一箇所以上の区域に接続されている投票に対する候補者(applicant)のリストを表すデータを記憶するための少なくとも一個のモジュールを備えることが示されている。

【0120】

このようなモジュールの動作は、管理者と称される投票の主催者であって専用サーバSA2を更新し得る主催者の権限の下で、図6の参照番号1において実施される。

【0121】

50

専用サーバSA2は、図6の参照番号2にて実施されるモジュールを備える。この参照番号2にて実施されるモジュールは、複数のリストの形態を有する小規模アプリケーションであって「アプレット」として知られた1群の小規模アプリケーションMAを算出するモジュールを備える。一つの小規模アプリケーションは一つの区域に関係付けられ、かつ、候補者のリストと、電子投票用紙に対する暗号化キーとを包含する。

【0122】

特に、送信の間において括弧内に示された電子投票用紙EBは、高レベルのセキュリティをもって前述の暗号化キーを用いて当然に暗号化されることを理解すべきである。上記高レベルのセキュリティとは、たとえばRSAアルゴリズム等に従う非対称キーを有する暗号化キーを用いるような強力な暗号化であることが理解されるであろう。

10

【0123】

専用サーバとして機能する第2管理サーバSA2はさらに、候補者のリストと暗号化キーとを含む小規模アプリケーションを第1管理サーバSA1に送信するモジュールを備える。

【0124】

第2管理サーバSA2による署名の後で、第1管理サーバSA1は、参照番号3にて、小規模アプリケーションのリストを受信し、当該小規模アプリケーションのコンパイルを実施し、かつ、照合のために候補者のリストを発行する。

【0125】

この目的のために、第1管理サーバSA1は、当然のことながら、小規模アプリケーションのリストを記憶するモジュールと、各々の小規模アプリケーションをコンパイルすると共にコンパイルされた各々の小規模アプリケーションに署名するモジュールと、各々の区域と各々の小規模アプリケーションとに対する候補者のリストを抽出して発行するモジュールと、署名された小規模アプリケーションを第2管理サーバSA2（すなわち専用サーバSD）および関連する各投票者に対する投票用端末に送信するモジュールとを備える。

20

【0126】

特に、第1管理サーバSA1は、参照番号4にて、署名された小規模アプリケーションのアプリケーション・リストを上記第2管理サーバ（すなわち上記専用サーバSD）に送信することが理解されるであろう。

【0127】

さらに、前述の専用サーバは、参照番号5にて、署名された小規模アプリケーションの完全性を署名の照合により確認する。また一方で、上記第2管理サーバ（すなわち専用サーバSD）により権限が上記第1管理サーバに送信されると同時に、当該第1管理サーバは、関連する各投票者に対し、改変された小規模アプリケーションによっては置き換えられ得なかった照合済みのオリジナルの小規模アプリケーションを送信し得る。

30

【0128】

単用パスワードUPWeの制御に関しては、第2管理サーバSA2（すなわち専用サーバSD）は、参照番号6にて、前述のような1群の単用パスワードを生成することが示されている。

【0129】

さらに、専用サーバSDは、参照番号7にて、たとえば図5に関する記述において前述した如く、関連する投票用端末使用中の投票者Euに対して単用パスワードUPWeを送信する。

40

【0130】

前述のような暗号化キーの制御に関し、第1管理サーバSA1は、上記システムに責任を有する権限者（すなわち上記システム全体を制御する管理者）から、投票の終了以前における電子投票用紙EBの開示防止のために意図された暗号化を許容する公開暗号化キーのリストを受信することが示されている。前述のような各々の暗号化キーは、それぞれ対応する小規模アプリケーションMAと共に、関連する投票用端末Teに送信される。

【0131】

最終的に、認証キーの制御は、第1管理サーバSA1と、専用サーバSDとして機能する第2管理サーバSA2とによる認証証明書の使用に対して調整される。

50

【0132】

前述の2台のサーバはそれぞれ、専用サーバSDにより生成された認証キーのリストLKA、および、第1管理サーバSA1により生成された認証キーのリストLKBを生成する。

【0133】

それゆえに、各々の投票用端末使用中の投票者Euに対しては、専用サーバSD（すなわち上記第2管理サーバ）により生成された認証キーKAと、第1管理サーバSA1により生成された認証キーKBとの対が割り当てられる。

【0134】

第1管理サーバSA1および第2管理サーバSA2（専用サーバSD）の各々は、先に生成されている上記認証キー（KA、KB）のリストLKBおよびLKAを生成する。

10

【0135】

認証キーのリストLKBを生成した第1管理サーバSA1は、参照番号9にて、専用サーバSDに対し、投票者の識別情報または投票者に対して接続された識別コードと、この識別コードに関連する認証キーKBに対するハッシュ関数とにより形成される値の対を送信する。

【0136】

専用サーバSDは、認証キーKAのリストLKAのハッシュ関数を算出すると共に、受信した認証キーKBに対するハッシュ関数HKBを、対応する認証キーKAに対するハッシュ関数と組み合わせる。

【0137】

さらに、当該専用サーバは、参照番号10にて、投票用端末使用中の投票者Euの識別コードとは一切結合することなく、上記投票カウント・サーバに対し、ハッシュ関数HKA、HKBに対する値の対のみの送信を実施する。

20

【0138】

認証証明書の制御に関していえば、この制御は、上記にて記述された如く、PKIアーキテクチャに従って実施される。

【0139】

この目的のために、第1管理サーバSA1は、参照番号11にて不可欠な認証証明書のリストを生成し、これによって、許可された投票用端末使用中の投票者Euのみが投票への参加を許容される。

【0140】

30

第1管理サーバSA1は、前述の認証証明書に対する破棄リスト(revocation list)を生成して制御する。

【0141】

図5に示されたトランザクションT2に続き、たとえば上記第1管理サーバが認証証明書CAを受信したときに、上記第1管理サーバは、許可された投票者のみが投票に参加することを当該第1管理サーバが許容する旨のリストを構築することが理解されるであろう。

【0142】

さらに、第1管理サーバSA1は、参照番号12にて、図5に示されたトランザクションT5に従って、自身の認証証明書を各投票者に送信する。

【0143】

40

すると、投票用端末使用中の投票者Euは、自身の投票用端末Teに対して認証証明書CAをインストールする立場となる。

【0144】

つぎに、図7を参照しながら、投票日において投票用端末使用中の投票者と上記システム全体により実施されるトランザクションを説明する。

【0145】

投票日において、投票用端末使用中投票者Euは、参照番号13にて、第2管理サーバSA2(SD)に対する接続を行う。当該投票者は、自身の単用パスワードUPWeと、認証を許容する情報とを送信する。第2管理サーバSA2(SD)は、この投票用端末使用中の投票者に関係付けられた認証キーKBを当該サーバに対して提供するデータベースに対して照会を行う。

50

【0146】

同じ日に幾つかの投票が行われる場合には、同一の投票者Euに対する多元化(diversification)により、複数の認証キーKBが利用可能である。

【0147】

このような状況において、専用サーバSA2(SD)は、各々の選挙に対応する複数の投票カウント・サーバ(SCV)に対して照会を行う立場にある。

【0148】

C13と表された前述の接続の試行が、認証エラーによって失敗した場合、すなわち、投票用端末使用中の投票者Euの認証証明書に基づく当該投票者に対する認証プロセスであって好首尾には実施され得なかった認証プロセスのために前述の接続の試行が失敗した場合、制御プロセスが起動されると共に、たとえば不正行為に対するセキュリティ処置を実行するために上記のイベント(event)が追尾される。

10

【0149】

この動作は、投票用端末使用中の投票者の識別情報に応じた否定的な応答の場合において、図3の戻りのステップA₂から始まる動作に対応し得る。

【0150】

認証エラーが発生しない場合、専用の第2管理サーバSA2(SD)は、参照番号14にて、認証キーKAを投票カウント・サーバSCVに送信する。つぎに、投票カウント・サーバSCVは、そのデータベースにおいて、上記認証キーKAがまだ使用されていないことを確認するために制御C14を実行する。もし、この認証キーKAが既に使用されていれば、図7に示された如く投票者は、専用サーバSA2(SD)を介して、投票カウント・サーバSCVにより、当該投票者が今回の投票に参加する権利を既に有していないことが喚起される。

20

【0151】

特に、認証エラーが発生した場合、すなわち認証キーKAが既に使用されている場合に、上記のイベントはC14にて追尾され、投票用端末使用中の投票者Euは、投票を2回に互り試みたとみなされる。

【0152】

コントローラまたは制御要素は、署名が存在することを確認するために第1管理サーバSA1に接触する。

【0153】

エラーが発生しない場合、投票カウント・サーバSCVは、参照番号15にて、投票に対する権限を第2専用管理サーバSA2(SD)に送信する。認証キーKAは依然として、投票カウント・サーバSCVにおける複数の有効なキーに含まれている。

30

【0154】

専用サーバSA2(SD)は、参照番号16にて、投票用端末使用中の投票者Euに対し、すなわち投票用端末Teに対し、投票中の小規模アプリケーションMAおよび認証キーKAを送信する。

【0155】

上記投票中の小規模アプリケーションMAおよび認証キーKAは、投票の準備の間において生成されていることに留意すべきである。小規模アプリケーションMAおよび認証キーKAが受信された後、投票用端末Teは、第1管理サーバSA1に対して参照番号17のような接続を行う。さらに、投票用端末Teの操作者は、予め配布された認証証明書CAであって予め上記投票用端末にインストールされている認証証明書CAが、上記PKIシステムおよび生成された複数種の証明書により対処され得るという呼びかけを呈示する。

40

【0156】

投票者は、電子投票用紙EBを用いて自身の候補者または候補者のリストを選択すると共に、投票用端末Teは、小規模アプリケーションMAを用いてブラインド署名(blind signature)のプロセスを実行する。これによって、電子迷彩形式(steganographic type)のプロセスを用いて予め暗号化された電子投票用紙EBが曖昧化されると共に、参照番号17にて、当該電子投票用紙EBの全体が第1管理サーバSA1に送信される。もし、第1管理サーバSA1

50

における接続の試行が失敗したならば、この失敗した試行はC17にてリスト化かつ追尾され、さらに、第1管理サーバSA1のレベルにおける認証エラーが追尾され、かつ、上記制御要素またはコントローラに送信される。これによって、特定の情報源、すなわち特定の投票用端末Teに由来する投票要求は所定時間に互り処理しないことが決定され得る。

【0157】

認証エラーが発生しない場合、投票用端末使用中の投票者は、自身の個人キーを用いて有権者名簿に対して署名を行い、参照番号18にて、署名済みの名簿を第1管理サーバSA1に送信する。

【0158】

第1管理サーバSA1は、参照番号19にて、曖昧化された投票用紙に対応するブラインド署名と認証キーKBとを投票用端末使用中の投票者Euの端末Teに送信する。さらに、小規模アプリケーションMAは、上記投票用紙を明らかにすると共に、明らかにされたが依然として暗号化されている電子投票用紙EBから有効な署名を獲得し得る。投票用端末使用中の投票者と電子端末Teとにより保持された認証キーKBは、有権者名簿が署名された証拠である。

10

【0159】

投票用端末使用中の投票者Euの投票用端末Teにインストールされている小規模アプリケーションMAは、参照番号20にて、投票カウント・サーバSCVに接続されると共に、暗号化された電子投票用紙EBと、ブラインド署名と、認証キーKAおよび認証キーKBとにより形成される1群を送信する。

20

【0160】

さらに、投票制御サーバ（投票カウント・サーバ）SCVは、第1管理サーバSA1の署名であるべき上記署名と有効であるべき認証キーKBとの制御C20を実行する。

【0161】

有効性の判定基準は、認証キーKAおよびKBに対するハッシュ関数の対、すなわちハッシュ関数HKA、HKBに対する値の対が、まだ使用されておらずかつ既知である対の一部とされるべきであるという事実からなる。

【0162】

その後、投票カウント・サーバSCVは、評価を待ちながら、暗号化された電子投票用紙EBおよび上記ブラインド署名をデータベースに記憶する。ここで、投票カウント・サーバは、権限が付与された複数の対の認証キーの内で一对の認証キーのオリジナル版を当該サーバが受信したことの証拠として、認証キーKA、KBの対を別のデータベースに記憶する。

30

【0163】

前述の投票制御サーバ（投票カウント・サーバ）SCVにより実行される一連の制御において非照合エラーが発生した場合、図7に示された如く、前述の投票制御サーバ（投票カウント・サーバ）は、C20にて制御要素に対し、投票用紙拒否の通知を送信する。

【0164】

逆にいえば、全ての制御が投票カウント・サーバSCVにより好首尾に実行された場合、当該サーバは投票用端末使用中の投票者Euに対し、当該投票者の投票用紙がカウントされたことを喚起する（参照番号21に対応する）。

40

【0165】

それゆえに、匿名送信に対するメカニズムが提供され得る。

【0166】

図7において、かつ図6を参照すると、参照番号18および19にて有権者名簿に署名する手順は、第1管理サーバSA1および第2管理サーバSA2により別個に生成された認証キーKAおよびKBによる認証プロセスによって可能とされることが示されている。

【0167】

それゆえに、これらの条件下にて、上記投票カウント・サーバSCVは、認証キーKAおよびKBを送信するステップ（参照番号20に対応する）に続き、第1管理サーバSA1、第2専用管理サーバSA2(SD)および当該投票カウント・サーバSCVにより構成される3つの独立

50

の構成要素により互いに独立して投票の完全性が確認され、かつ、投票が実施されるのを許容するような仲裁者の役割を果たしている。

【図面の簡単な説明】

【0168】

【図1】本発明に係るネットワークを介した電子投票を実現するための方法を実行する際に必要な複数のステップを例示的に説明するためのフローチャートである。

【図2】図1に示された本発明に係る方法の特定のステップを実行するための例示的かつ詳細なフローチャート（その1）である。

【図3】図1に示された本発明に係る方法の特定のステップを実行するための例示的かつ詳細なフローチャート（その2）である。

10

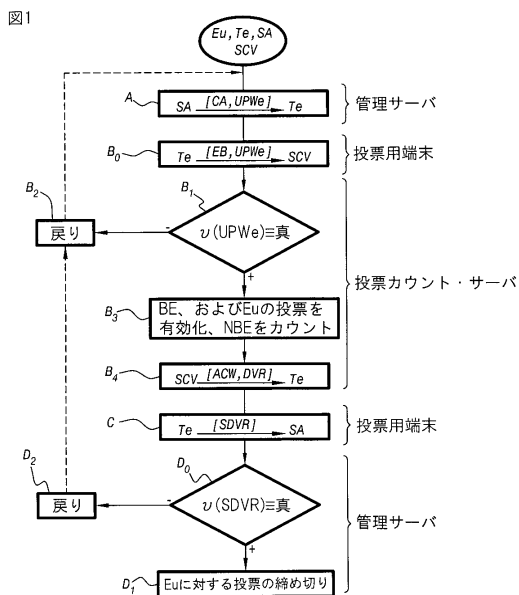
【図4】本発明の主題に従ってネットワークを介した電子投票を実現するためのシステムのアーキテクチャを例示的に示す概略図である。

【図5】本発明の主題に従ってネットワークを介した電子投票を実現するためのシステムの好適な変形例に係るアーキテクチャの例示的なブロック図である。

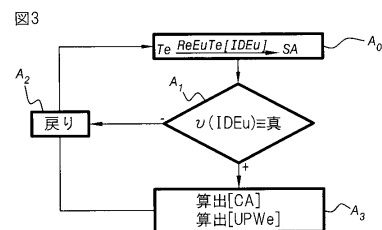
【図6】図5に示された本発明の主題に係る電子投票システムを使用するユーザにより行われる電子投票セッションを例示的かつ詳細に示す図である。

【図7】図5に示された電子投票システムのアーキテクチャにより一連のステップまたはプロトコルを実行するための例示的かつ詳細な図である。

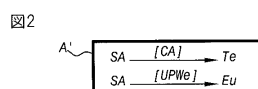
【図1】



【図3】

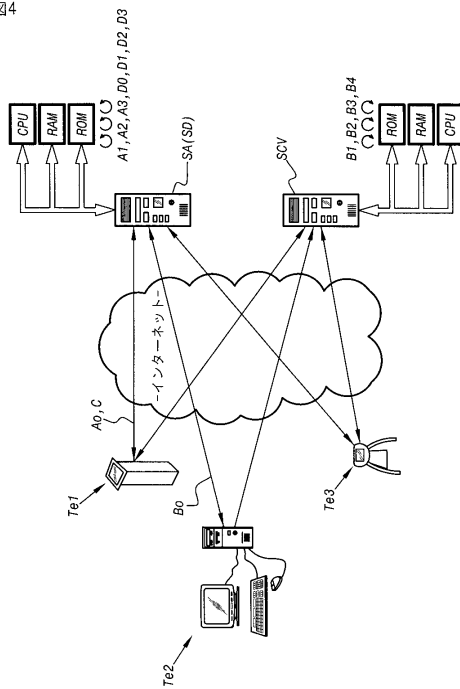


【図2】



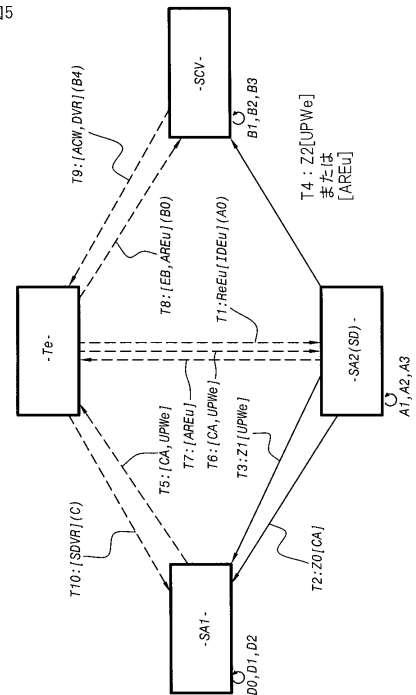
【図 4】

図4



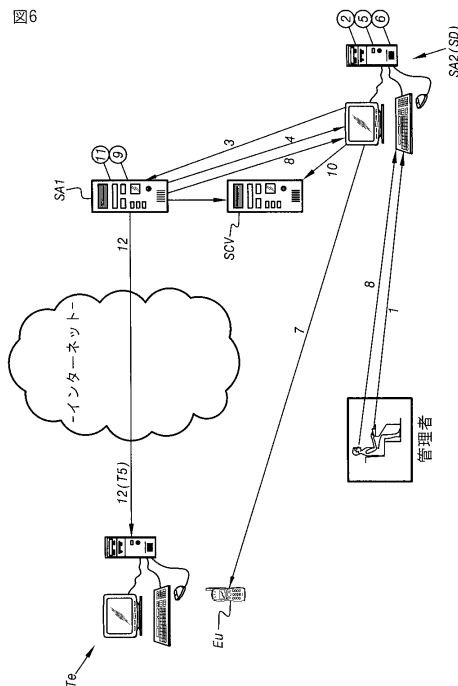
【図 5】

図5



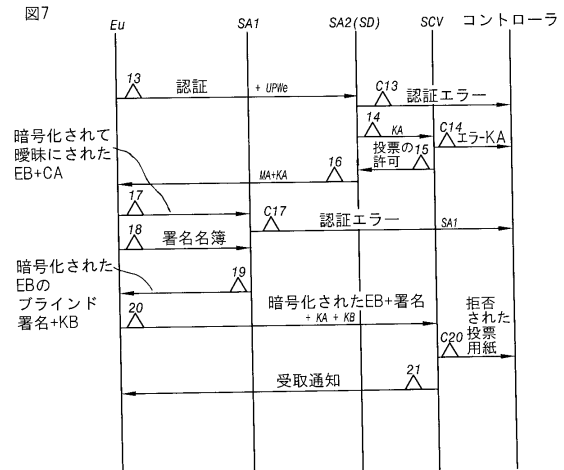
【図 6】

図6



【図 7】

図7



フロントページの続き

(74)代理人 100082898

弁理士 西山 雅也

(72)発明者 フランソワ ベルネー

フランス国, 3 8 0 0 0 グルノーブル, リュ ディオドール ラフル 8

(72)発明者 ジャック トラオール

フランス国, 6 1 1 0 0 サン ジョルジュ デ グロセイエ, アブニュ ドゥ ラ スイス ノ
ルマンド 2 3

(72)発明者 アントワーヌ ボナムール

フランス国, 3 8 0 0 0 グルノーブル, ケ ペリエール 3 2

審査官 宮地 匡人

(56)参考文献 特開 2 0 0 0 - 2 6 9 9 5 7 (J P, A)

特開 2 0 0 3 - 0 6 7 5 3 2 (J P, A)

特開 2 0 0 4 - 0 1 3 6 0 6 (J P, A)

(58)調査した分野(Int.Cl., D B名)

G 0 6 Q 5 0 / 3 4

G 0 6 Q 5 0 / 2 6

G 0 6 Q 1 0 / 0 0

G 0 7 C 1 3 / 0 0

H 0 4 L 9 / 3 2