(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2008-186064
(P2008-186064A)
(43)公開日　平成20年8月14日(2008.8.14)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B285
H04L 9/32	(2006.01)	H04L	9/00	675B	5J104

審査請求 未請求　請求項の数 41　ＯＬ　（全 37 頁）

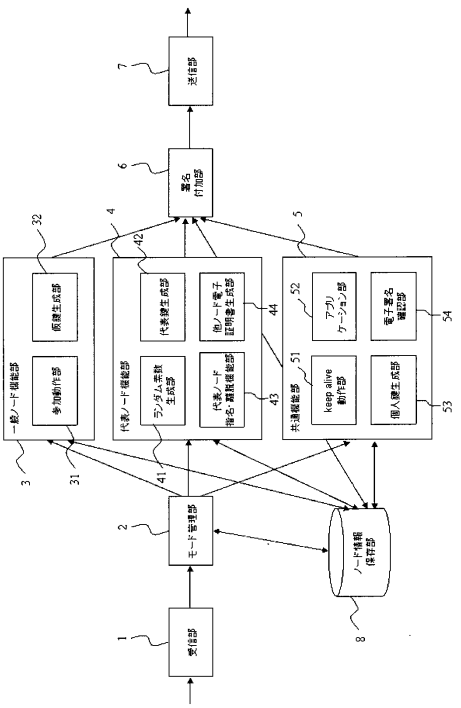
(21)出願番号　特願2007-16562(P2007-16562)
(22)出願日　平成19年1月26日(2007.1.26)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(74)代理人　100065385
弁理士　山下　穣平
(74)代理人　100130029
弁理士　永井　道雄
(72)発明者　静野　隆之
東京都港区芝五丁目７番１号　日本電気株式会社内

Ｆターム(参考)　5B285 AA01 BA07 CA04 CA43 CA44 CA45 CA47 CB47 CB53 CB56 CB63
5J104 AA07 KA01 KA05 MA03 PA07

(54)【発明の名称】分散認証システム、分散認証方法、及び分散認証プログラム

(57)【要約】
【課題】認証局の場所が判明して容易に攻撃されやすいというセキュリティリスクを抑制し、認証局への攻撃耐性を向上させることができる分散認証システムを提供する。
【解決手段】分散認証システムは、ひとつまたは複数のノードで構成される。分散認証システムに参加するノードのうち所定数台のノードが、分散認証システムを代表する代表ノードとなる。代表ノードは、互いに連携することによって、分散認証システムの電子署名で用いる代表鍵と、分散認証システム電子証明書と、分散認証システムに参加するノードの電子署名で用いる個人鍵と、分散認証システムに参加するノードの電子証明書とを発行する。
【選択図】図１



【特許請求の範囲】
【請求項１】
ひとつまたは複数のノードで構成される分散認証システムであって、
前記分散認証システムに参加するノードのうち所定数台のノードが前記分散認証システムを代表する代表ノードとなり、
前記代表ノードが、互いに連携することによって、前記分散認証システムの電子署名で用いる代表鍵と、分散認証システム電子証明書と、前記分散認証システムに参加するノードの電子署名で用いる個人鍵と、前記分散認証システムに参加するノードの電子証明書とを発行することを特徴とする分散認証システム。
【請求項２】
請求項１に記載の分散認証システムにおいて、
前記分散認証システムを構成するノードは、
他ノードから送られてくるデータを受信する受信部と、
前記分散認証システムを構成するノードの情報を含むノードリストを更新可能に保存するノード情報保存部と、
前記ノードリストに基づいて、前記分散認証システムのモードとして、前記分散認証システムに参加する全ノード数が所定数未満のときの総意モードと、前記分散認証システムに参加する全ノード数が所定数以上のときの代表モードとを管理するモード管理部と、
前記代表モードの場合、前記代表ノードのときの動作を行う代表ノード機能部と、
前記代表モードの場合、前記代表ノード以外の一般ノードのときの動作を行う一般ノード機能部と、
前記総意モード及び前記代表モードに共通の動作を行う共通機能部と、
前記代表ノード機能部、前記一般ノード機能部、及び前記共通機能部から渡される前記他ノードへのデータに電子署名を付加する署名付加部と、
前記電子署名が付加されたデータを前記他ノードに送信する送信部と、を有することを特徴とする分散認証システム。
【請求項３】
請求項２に記載の分散認証システムにおいて、
前記一般ノード機能部は、
前記ノードが前記一般ノードである場合に、仮鍵を生成する機能を有する仮鍵生成部と、
前記分散認証システムに参加するための参加リクエストを前記分散認証システムに既に参加している他ノードに送信する機能を有する参加動作部と、を有することを特徴とする分散認証システム。
【請求項４】
請求項２に記載の分散認証システムにおいて、
前記代表ノード機能部は、
前記ノードが前記代表ノードである場合に、他の代表ノードと互いに連携し、前記代表鍵と前記分散認証システム電子証明書とを生成する代表鍵生成部と、
他ノードからの参加リクエストまたは電子証明書生成リクエストを受信し、前記他ノードの個人鍵とその電子証明書とを生成する他ノード電子証明書生成部と、
前記代表ノードが規定数より少なくなった場合に前記代表ノードを指名する機能と、前記代表ノードを離脱する機能とを有する代表ノード指名・離脱機能部と、
前記代表鍵と前記他ノードの個人鍵との秘密鍵の素となるランダム素数を生成するランダム素数生成部と、を有することを特徴とする分散認証システム。
【請求項５】
請求項２に記載の分散認証システムにおいて、
前記共通機能部は、
前記ノードが前記一般ノードまたは前記代表ノードの場合に、キープアライブ動作により他ノードと前記ノードリストを交換するキープアライブ動作部と、

前記分散認証システムを利用するアプリケーションを実施するアプリケーション部と、
前記規定数台の代表ノードから受信する前記個人鍵の秘密鍵の素となる情報から前記個人鍵の秘密鍵を生成する個人鍵生成部と、
前記他ノードから受信するメッセージに付加されている電子署名の正当性を確認する電子署名確認部と、を有することを特徴とする分散認証システム。
【請求項６】
請求項２に記載の分散認証システムにおいて、
前記受信部は、受信したメッセージを前記モード管理部へ送ることを特徴とする分散認証システム。
【請求項７】
請求項２に記載の分散認証システムにおいて、
前記モード管理部は、
前記ノード情報保存部に保存されているノードリストを読み出す機能と、
前記分散認証システムに参加しているノード数を確認する機能と、
前記分散認証システムのモードを確認する機能と、
自ノードが前記代表ノードであるか、前記一般ノードであるかの状態を管理する機能と、
前記ノード情報保存部に保存されているノード情報を定期的に読み出し、前記分散認証システムに参加するノード数が前記所定数未満であるかそうでないかを確認する機能と、
前記分散認証システムに参加するノード数が前記所定数未満であった場合、自ノードを前記総意モードで動作させる機能と、
前記分散認証システムに参加するノード数が前記所定数以上であった場合、自ノードを前記代表モードで動作させる機能と、
前記代表ノードに指名されていた場合、自ノードを前記代表ノードとして動作させる機能と、
前記代表ノードに指名されていなかった場合、自ノードを前記一般ノードとして動作させる機能と、
前記総意モードにおいて、前記ノード情報保存部に保存されているノードリストを確認し、前記分散認証システムに参加している全ノード数が前記所定数に到達していた場合、自ノードを前記代表モードに移行させる機能と、
前記代表ノード機能部に、前記分散認証システムの代表鍵を生成するよう指示する機能と、
前記一般ノード機能部に、前記分散認証ネットワークに改めて参加し前記分散認証システムの発行する電子証明書及び鍵を得るよう指示する機能と、
前記代表ノード機能部に前記鍵の秘密鍵を用いて前記ノードリストに電子署名をするよう指示する機能と、
前記代表ノード機能部に、前記所定数台の代表ノードによる電子署名の完了した前記ノードリストに前記代表鍵による電子署名を付加するよう指示する機能と、
受信したメッセージを適切な機能部へ振り分けを行う機能と、を有することを特徴とする分散認証システム。
【請求項８】
請求項１に記載の分散認証システムにおいて、
前記代表ノードは、
他の代表ノードと互いに連携し、前記代表鍵と前記分散認証システム電子証明書とを生成する機能と、
他ノードからの参加リクエストまたは電子証明書生成リクエストを受信し、前記他ノードの前記個人鍵と前記電子証明書を生成する機能と、
前記代表ノードを離脱する機能と、
前記代表ノードが前記所定数より少なくなった場合に前記代表ノードを指名する機能と、

前記代表鍵と前記他ノードの個人鍵との秘密鍵の素となるランダム素数を生成する機能と、
前記キープアライブ動作により前記他ノードと前記ノードリストを交換する機能と、
前記分散認証システムを利用するアプリケーションを実施する機能と、
前記所定数台の代表ノードから受信する前記個人鍵の秘密鍵の素となる情報から前記個人鍵の秘密鍵を生成する機能と、
前記他ノードから受信するメッセージに付加されている電子署名の正当性を確認する機能と、を有することを特徴とする分散認証システム。

【請求項９】
請求項２に記載の分散認証システムにおいて、
前記ノードリストは、前記分散認証システムに参加している全ノードのノード情報と、代表ノード情報と、を有することを特徴とする分散認証システム。

【請求項１０】
請求項９に記載の分散認証システムにおいて、
前記ノード情報は、ノードのＩＤと、ノードのＩＰアドレスと、ポート番号と、代表ノード情報と、旧代表ノード情報と、を含むことを特徴とする分散認証システム。

【請求項１１】
請求項９に記載の分散認証システムにおいて、
前記代表ノード情報は、前記代表ノードがどのノードであるかという情報を含むことを特徴とする分散認証システム。

【請求項１２】
請求項９に記載の分散認証システムにおいて、
前記旧代表ノード情報は、過去に前記代表ノードがどのノードであったかという情報を含むことを特徴とする分散認証システム。

【請求項１３】
請求項３に記載の分散認証システムにおいて、
前記仮鍵は、前記分散認証システムによって発行された鍵ではなく、各ノードが生成する鍵であって、新規に前記分散認証システムに参加する場合と、前記総意モードの場合とに、他ノードへの全てのメッセージに付加される電子署名に利用されることを特徴とする分散認証システム。

【請求項１４】
請求項１に記載の分散認証システムにおいて、
前記代表鍵は、公開鍵暗号系の秘密鍵と公開鍵とから成り、
前記個人鍵は、公開鍵暗号系の秘密鍵と個人鍵とから成ることを特徴とする分散認証システム。

【請求項１５】
請求項１に記載の分散認証システムにおいて、
前記代表鍵は、ノードリストと、前記分散認証システムに参加するノードの電子証明書とに前記分散認証システムの電子署名を付加する場合に使用され、
前記代表鍵の秘密鍵は、前記分散認証システム上のどのノードも知ることができないように複数の代表ノードに分散して保存され、
前記代表鍵の公開鍵は、前記分散認証システム上のどのノードも参照することができるように前記分散認証システム上に公開されることを特徴とする分散認証システム。

【請求項１６】
請求項１に記載の分散認証システムにおいて、
前記分散認証システムに参加するノードの電子証明書は、前記個人鍵の公開鍵と、前記分散認証システムに参加するノードの情報とに加え、前記個人鍵の公開鍵及び前記ノードの情報のダイジェスト情報に前記代表鍵による電子署名を付加したものであることを特徴とする分散認証システム。

【請求項１７】

請求項１６に記載の分散認証システムにおいて、
前記ダイジェスト情報は、元になる情報の要約情報であり、その元になる情報に一方向関数を適用することで生成されることを特徴とする分散認証システム。
【請求項１８】
請求項３に記載の分散認証システムにおいて、
前記参加動作部は、
自ノードが新規に前記分散認証システムに参加する場合に、前記仮鍵の公開鍵を付加した参加リクエストを自ノードの仮鍵の秘密鍵による電子署名と共に送信する機能と、
他ノードから前記参加リクエストを受信した場合に前記参加リクエストに付加されている前記仮鍵の公開鍵を用いて前記電子署名を確認し、改ざんがない場合は参加レスポンスを送信する機能と、
前記分散認証システムが前記総意モードであった場合、前記参加レスポンスに自ノードの仮鍵の公開鍵と、ノードリストとを付加し、自ノードの仮鍵の秘密鍵による電子署名と共に送信する機能と、
前記分散認証システムが代表モードであった場合、前記参加レスポンスに前記参加リクエストを受理した旨のメッセージを付加し、自ノードの個人鍵の秘密鍵による電子署名と共に送信する機能と、
前記ノード情報保存部からノードリストを読み出し、前記代表ノードを確認し、ある代表ノードに対し、前記参加リクエストを送信してきたノードのノード情報を付加した電子証明書生成リクエストを送信する機能と、を有することを特徴とする分散認証システム。
【請求項１９】
請求項３に記載の分散認証システムにおいて、
前記仮鍵生成部は、前記仮鍵を生成する機能と、生成した仮鍵を自ノードのノード情報と共に前記ノード情報保存部に保存する機能と、を有することを特徴とする分散認証システム。
【請求項２０】
請求項４に記載の分散認証システムにおいて、
前記ランダム素数生成部は、
前記代表鍵生成部と前記他ノード電子証明書生成部からのリクエストを受けて、ランダムな素数を生成する機能と、
生成したランダムな素数を前記代表鍵生成部と前記他ノード電子証明書生成部とに渡す機能と、を有することを特徴とする分散認証システム。
【請求項２１】
請求項４に記載の分散認証システムにおいて、
前記代表鍵生成部は、
前記分散認証システムが前記代表モードかつ自ノードが前記代表ノードであった場合に、前記モード管理部から前記代表鍵を生成するように指示を受けると、他の代表ノードと連携し、前記ランダム素数生成部が生成した素数を素に、前記代表鍵の公開鍵の素となる情報を他ノードに知らせることなく、マルチパーティプロトコルを用いて、前記代表鍵の公開鍵を生成する機能と、
自ノードが前記代表ノードでなくなるまで前記代表鍵の生成に利用した素数を保存する機能と、
前記分散認証システムが前記代表モードかつ自ノードが前記代表ノードであった場合に、前記モード管理部から前記所定数の代表ノードによる電子署名の完了したノードリストに前記代表鍵による電子署名を付加するように指示を受けると、他の代表ノードと連携し、前記代表鍵の素となる情報を他ノードに知らせることなく、ノードリストに前記代表鍵の秘密鍵を用いた電子署名を付加する機能と、を有することを特徴とする分散認証システム。
【請求項２２】
請求項４に記載の分散認証システムにおいて、

前記代表ノード指名・離脱機能部は、
自ノードが前記代表ノードであり前記代表ノードを離脱したい場合に、前記ノード情報保存部からノードリストを読み出し、代表ノード離脱リクエストを他の代表ノードに送信する機能と、
自ノードが前記代表ノードであった場合に、前記代表ノード離脱リクエストを受信すると、前記代表ノード離脱リクエストを送信してきた代表ノードに対し、代表ノード離脱レスポンスを送信する機能と、
前記代表ノードが前記所定数未満である状態から、前記代表ノードを前記所定数とするため、前記ノード情報保存部からノードリストを読み出し、適当な一般ノードを選出する機能と、
選出した前記一般ノードのノード情報を記載した代表ノード指名確認メッセージを他の代表ノード全てに送信する機能と、
前記代表ノード指名確認メッセージを受信した場合に、選出された前記一般ノードのノード情報を確認し、可否情報を含む代表ノード指名確認レスポンスを返送する機能と、
自ノードを除く全ての代表ノードから代表ノード指名確認レスポンスを受信した場合に、選出した一般ノードに代表ノード指名リクエストを送信する機能と、
自ノードが前記一般ノードであり前記ノード代表ノード指名リクエストを受信した場合に、可否情報を含む代表ノード指名レスポンスを返送する機能と、
前記代表ノード指名レスポンスを受信した場合に、新しく代表ノードとなるノードのノード情報を、自ノードを除く全ての代表ノードに送信する機能と、
前記代表ノード機能部に、前記個人鍵の秘密鍵を用いてノードリストに電子署名をするよう指示する機能と、
前記代表鍵を更新する前まで前記代表ノードであった旧代表ノードに対し、現在代表ノードであるノードによる電子署名が終了しているノードリストに電子署名をするよう指示する機能と、
前記代表ノード機能部に、前記所定数の代表ノード及び前記所定数の旧代表ノードによる電子署名の完了したノードリストに前記代表鍵による電子署名を付加するよう指示する機能と、
前記電子署名が付加されたノードリストと前記代表鍵の公開鍵とをセットで前記分散認証ネットワーク電子証明書として、前記ノード情報保存部に保存する機能と、を有することを特徴とする分散認証システム。

【請求項２３】
請求項２２に記載の分散認証システムにおいて、
前記代表ノード指名・離脱機能部は、前記各機能を、前記代表ノードが前記規定数台になるまで繰り返す機能を有することを特徴とする分散認証システム。

【請求項２４】
請求項４に記載の分散認証システムにおいて、
前記他ノード電子証明書生成部は、
前記分散認証システムが前記代表モードかつ自ノードが前記代表ノードであった場合に、電子証明書生成リクエストを受信すると、他の代表ノードと連携し、前記ランダム素数生成部が生成する素数を素に、電子証明書に付随する個人鍵の素となる情報を他ノードに知らせることなく、マルチパーティプロトコルを用いて、電子証明書リクエストに記載のノードの個人鍵を生成する機能と、
前記代表鍵生成部と連携し、前記ノードのノード情報と前記個人鍵から電子証明書を生成する機能と、
前記個人鍵の秘密鍵の素となる情報と公開鍵と前記電子証明書を電子証明書生成リクエストに記載のノードに送信する機能と、を有することを特徴とする分散認証システム。

【請求項２５】
請求項５に記載の分散認証システムにおいて、
前記キープアライブ動作部は、

他ノードに対し定期的にキープアライブメッセージを送信する機能と、
他ノードから定期的に前記キープアライブメッセージを受信することで通信路のつながりをチェックする機能と、
前記キープアライブメッセージに付加されたノードリストと前記ノード情報保存部から読み出したノードリストとを比較し、ノードリストを最新の情報に更新する機能と、
前記キープアライブメッセージに対し一定期間レスポンスがない場合は、該当ノードは前記分散認証システムから離脱したと判定し、ノードリストを更新し、前記キープアライブ動作を用いて他ノードに最新の情報を伝える機能と、
前記代表ノードが離脱したと判定した場合に、前記ノード管理部に前記代表ノードが離脱したことを送信する機能と、を有することを特徴とする分散認証システム。

【請求項２６】
請求項５に記載の分散認証システムにおいて、
前記アプリケーション部は、前記分散認証システムを利用するアプリケーションの処理をする機能を有することを特徴とする分散認証システム。

【請求項２７】
請求項５に記載の分散認証システムにおいて、
前記個人鍵生成部は、
前記所定数台の代表ノードから受信する個人鍵の秘密鍵の素となる所定数の情報から前記個人鍵の秘密鍵を生成する機能と、
受信した前記個人鍵の公開鍵と秘密鍵とが有効に動作するか確認する機能と、
受信した電子証明書の有効性を確認する機能と、を有することを特徴とする分散認証システム。

【請求項２８】
請求項５に記載の分散認証システムにおいて、
前記電子署名確認部は、
メッセージを受信した場合にメッセージ送信元を確認し、前記分散認証システムにメッセージ送信元のノードの電子証明書発行リクエストを送信する機能と、
メッセージ送信元のノードの電子証明書を得た場合に、前記電子証明書に付加されている前記代表鍵による電子署名を確認するため、前記分散認証システムに分散認証システム電子証明書発行リクエストを送信する機能と、
前記分散認証システム電子証明書に付加されている前記代表鍵の公開鍵を得た場合に、前記電子証明書に付加されている電子署名を前記代表鍵の公開鍵で復号し、前記電子証明書の正当性を確認する機能と、
受信したメッセージに付加されている電子署名を前記電子証明書に付加されている前記個人鍵の公開鍵で復号し、当該メッセージの正当性を確認する機能と、
他ノードから前記電子証明書発行リクエストを受信した場合に、該当する電子証明書を前記ノード情報保存部から読み出し、電子証明書発行レスポンスを返送する機能と、
他ノードから前記分散認証システム電子証明書発行リクエストを受信した場合に、該当する公開鍵を前記ノード情報保存部から読み出し、分散認証システム電子証明書発行レスポンスを送信する機能と、を有することを特徴とする分散認証システム。

【請求項２９】
請求項２に記載の分散認証システムにおいて、
前記署名付加部は、
前記分散認証システムが前記総意モードの場合に前記ノード情報保存部に保存されている仮鍵を使用し、前記一般ノード機能部、前記代表ノード機能部、及び前記共通機能部からのメッセージに電子署名を付加する機能と、
前記分散認証システムによって前記電子証明書の発行を受けていない場合に前記ノード情報保存部に保存されている前記仮鍵を使用し、前記一般ノード機能部、前記代表ノード機能部、及び前記共通機能部からのメッセージに電子署名を付加する機能と、
前記分散認証システムが前記総意モードの場合でなく、前記分散認証システムによって

前記電子証明書の発行を受けている場合に、前記ノード情報保存部に保存されている前記個人鍵を使用し、前記一般ノード機能部、前記代表ノード機能部、及び前記共通機能部からのメッセージに電子署名を付加する機能と、を有することを特徴とする分散認証システム。

【請求項３０】

請求項２に記載の分散認証システムにおいて、

前記送信部は、前記署名付加部からのメッセージを受け、そのメッセージに記載された宛先のノードに対し、当該メッセージを送信する機能を有することを特徴とする分散認証システム。

【請求項３１】

請求項２に記載の分散認証システムにおいて、

前記ノード情報保存部は、自ノードのノード情報、仮鍵、前記電子証明書、前記ノードリスト、前記分散認証ネットワーク電子証明書、を保存する機能を有することを特徴とする分散認証システム。

【請求項３２】

ひとつまたは複数のノードで構成される分散認証システムであり、前記分散認証システムに参加するノードのうち所定数台のノードが前記分散認証システムを代表する代表ノードとなり、前記代表ノードが、互いに連携することによって、前記分散認証システムの電子署名で用いる代表鍵と、分散認証システム電子証明書と、前記分散認証システムに参加するノードの電子署名で用いる個人鍵と、前記分散認証システムに参加するノードの電子証明書とを発行する分散認証システムの分散認証方法であって、

（Ａ）前記分散認証システムへの参加を開始するステップと、

（Ｂ）前記分散認証システムに参加する全ノード数が所定数未満の場合、総意モードの動作を行うステップと、

（Ｃ）前記分散認証システムに参加する全ノード数が所定数以上の場合、代表モードの動作として、前記代表ノード以外の一般ノードのときの動作を行うステップと、

（Ｄ）前記代表モードの動作として、前記代表ノードのときの動作を行うステップと、

（Ｅ）他ノードから受信したメッセージの電子署名を確認するときの動作を行うステップと、

（Ｆ）前記代表ノードの初期の動作を行うステップと、

（Ｇ）前記代表ノードを更新するときの動作を行うステップと、

（Ｈ）前記代表ノードを離脱するときの動作を行うステップとを有することを特徴とする分散認証方法。

【請求項３３】

請求項３２に記載の分散認証方法において、

前記（Ａ）分散認証システムへの参加を開始するステップは、

（Ａ１）初期状態ステップと、

（Ａ２）仮鍵を生成するステップと、

（Ａ３）仮鍵及びノード情報を保存するステップと、

（Ａ４）前記分散認証システムに既に参加している他ノードに対し、参加リクエストを送信するステップと、

（Ａ５）前記分散認証システムのモードを確認するステップと、

（Ａ６）参加依頼レスポンスとして、参加依頼リクエストを送信したノードの仮鍵及びノードリストを受信し、ノードリストを更新するステップと、

（Ａ７）ノードリストを読み出し、ノードリストに記載の全ノードの仮鍵を保持しているか確認するステップと、

（Ａ８）参加レスポンスを受信するステップと、

（Ａ９）所定数台の代表ノードから個人鍵の秘密鍵の素となる情報と、電子証明書を受信するステップと、

（Ａ１０）受信した前記個人鍵の秘密鍵の素となる情報から個人鍵を生成するステップ

と、を有することを特徴とする分散認証方法。
【請求項３４】
請求項３２に記載の分散認証方法において、
前記（Ｂ）総意モードの動作を行うステップは、
（Ｂ１）前記総意モードの動作時の初期状態ステップと、
（Ｂ２）キープアライブ動作により、他の分散認証システムに参加するノードとノードリストの交換を行うステップと、
（Ｂ３）前記ノードリストを読み出し、前記分散認証システムに参加するノード数が所定数に達しているかどうかを確認するステップと、を有することを特徴とする分散認証方法。
【請求項３５】
請求項３２に記載の分散認証方法において、
前記（Ｃ）一般ノードのときの動作を行うステップは、
（Ｃ１）前記一般ノード動作の初期状態ステップと、
（Ｃ２）ノードリストを読み出し、他のノードに対し、ノードリストを付加したキープアライブメッセージを送信するステップと、
（Ｃ３）他ノードから、ノードリストが付加されたキープアライブメッセージを受信するステップと、
（Ｃ４）受信した前記キープアライブメッセージに付加されていたノードリストと自ノードが保存していたノードリストを比較し最新の情報に更新するステップと、
（Ｃ５）前記ノードリストを読み出し、前記分散認証システムに参加するノード数が所定数に達しているかどうかを確認するステップと、
（Ｃ６）参加リクエストを受信するステップと、
（Ｃ７）前記参加リクエストを送信してきたノードに対し、参加レスポンスを送信するステップと、
（Ｃ８）前記所定数台の代表ノードのうち、任意の代表ノードに対し、電子証明書作成リクエストを送信するステップと、
（Ｃ９）代表ノード指名リクエストを受信するステップと、
（Ｃ１０）前記代表ノードになるかどうか選択するステップと、
（Ｃ１１）前記代表ノードになるために、前記代表ノード指名リクエストを送信してきたノードに対し、代表ノード指名レスポンスを送信するステップと、
（Ｃ１２）代表ノードになることを拒否するために、前記代表ノード指名リクエストを送信してきたノードに対し、代表ノード拒否の情報を付加し代表ノード指名レスポンスを送信するステップと、
（Ｃ１３）電子証明書発行リクエストを受信するステップと、
（Ｃ１４）前記電子証明書発行リクエストを送信してきたノードに対し、自ノードの電子証明書を付加した電子証明書発行レスポンスを送信するステップと、を有することを特徴とする分散認証方法。
【請求項３６】
請求項３２に記載の分散認証方法において、
前記（Ｄ）代表ノードのときの動作を行うステップは、
（Ｄ１）代表ノード動作時の初期状態ステップと、
（Ｄ２）ノードリストを読み出し、他のノードに対し、ノードリストを付加したキープアライブメッセージを送信するステップと、
（Ｄ３）他のノードから、ノードリストが付加されたキープアライブメッセージを受信するステップと、
（Ｄ４）受信した前記キープアライブメッセージに付加されていたノードリストと自ノードが保存していたノードリストを比較し最新の情報に更新するステップと、
（Ｄ５）ノードリストを読み出し、分散認証システムに参加するノード数が所定数に達しているかどうかを確認するステップと、

（Ｄ６）ノードリストを読み出し、代表ノードが離脱していないか確認するステップと、
（Ｄ７）代表ノードを離脱したい場合、他の代表ノードに対し、代表ノード離脱リクエストを送信するステップと、
（Ｄ８）代表ノード離脱レスポンスを受信するステップと、
（Ｄ９）参加リクエストを受信するステップと、
（Ｄ１０）参加リクエストを送信してきたノードに対し、参加レスポンスを送信するステップと、
（Ｄ１１）参加リクエストを送信してきたノードの個人鍵の秘密鍵の素となる情報となるランダム素数を生成するステップと、
（Ｄ１２）前記所定数台の代表ノード間で互いに連携し、参加リクエストを送信してきたノードの個人鍵の公開鍵を生成するステップと、
（Ｄ１３）前記所定数台の代表ノード間で互いに連携し、参加リクエストを送信してきたノードの電子証明書を生成するステップと、
（Ｄ１４）前記参加リクエストを送信してきたノードに対し、前記個人鍵の秘密鍵の素となる情報と、前記個人鍵の公開鍵と、前記電子証明書とを送信するステップと、
（Ｄ１５）電子証明書生成リクエストを受信するステップと、
（Ｄ１６）代表ノード離脱リクエストを受信するステップと、
（Ｄ１７）代表ノード離脱レスポンスを送信するステップと、
（Ｄ１８）代表ノード指名確認メッセージを受信するステップと、
（Ｄ１９）代表ノード指名確認レスポンスを送信するステップと、
（Ｄ２０）電子証明書発行リクエストを受信するステップと、
（Ｄ２１）前記電子証明書発行リクエストを送信してきたノードに対し、自ノードの電子証明書を付加した電子証明書発行レスポンスを送信するステップと、
（Ｄ２２）前記分散認証システム電子証明書発行リクエストを受信するステップと、
（Ｄ２３）前記分散認証システム電子証明書発行リクエストを送信してきたノードに対し、分散認証システム電子証明書を付加した分散認証システム電子証明書発行レスポンスを送信するステップと、を有することを特徴とする分散認証方法。

【請求項３７】
請求項３２に記載の分散認証方法において、
前記（Ｅ）受信したメッセージの電子署名を確認するときの動作を行うステップは、
（Ｅ１）署名確認動作の初期状態ステップと、
（Ｅ２）メッセージ送信元のノードの電子証明書発行リクエストを送信するステップと、
（Ｅ３）電子証明書発行レスポンスを受信するステップと、
（Ｅ４）前記代表ノードに対し、分散認証システム電子証明書発行リクエストを送信するステップと、
（Ｅ５）分散認証システム電子証明書発行レスポンスを受信するステップと、
（Ｅ６）分散認証システム電子証明書に付加されている代表鍵の公開鍵を用い、電子証明書に付加されている電子署名を前記代表鍵の公開鍵で復号し、前記電子証明書の正当性を確認し、さらに、受信したメッセージに付加されている電子署名を前記電子証明書に付加されている前記個人鍵の公開鍵で復号し、当該メッセージの正当性を確認するステップと、を有することを特徴とする分散認証方法。

【請求項３８】
請求項３２に記載の分散認証方法において、
前記（Ｆ）代表ノードの初期の動作を行うステップは、
（Ｆ１）代表ノード初期動作時の初期状態ステップと、
（Ｆ２）前記分散認証システムの代表鍵の秘密鍵の素となる情報となるランダム素数を生成するステップと、
（Ｆ３）所定数台の代表ノード間で互いに連携し、前記分散認証システムの代表鍵の公

開鍵を生成するステップと、
（Ｆ４）この時点のノードリストに対し、前記個人鍵の秘密鍵を用いて電子署名をするステップと、
（Ｆ５）他の代表ノードに対し、電子署名済みのノードリストを送信するステップと、
（Ｆ６）他の代表ノードから、ノードリストを受信するステップと、
（Ｆ７）受信した前記ノードリストに全代表ノードの電子署名が付加されているか確認するステップと、
（Ｆ８）全代表ノードによる電子署名が完了したノードリストを、残存する旧代表ノードに送信するステップと、
（Ｆ９）残存する旧代表ノードによる電子署名が付加されたノードリストを受信するステップと、
（Ｆ１０）受信した前記ノードリストに、残存する旧代表ノード全てによる電子署名が付加されているか確認するステップと、
（Ｆ１１）前記所定数台の代表ノード間で互いに連携し、分散認証システム電子証明書を作成するステップと、を有することを特徴とする分散認証方法。
【請求項３９】
請求項３２に記載の分散認証方法において、
前記（Ｇ）代表ノードを更新するときの動作を行うステップは、
（Ｇ１）代表ノード更新動作時の初期状態ステップと、
（Ｇ２）新たに代表ノードになるノードを選出するステップと、
（Ｇ３）代表ノード指名確認メッセージを、他の代表ノードに送信するステップと、
（Ｇ４）代表ノード指名確認レスポンスを受信するステップと、
（Ｇ５）受信した前記代表ノード指名確認レスポンスに、選出した前記ノードを拒否するメッセージが付加されているか確認するステップと、
（Ｇ６）選出した前記ノードに対し、代表ノード指名リクエストを送信するステップと、
（Ｇ７）選出した前記ノードから、代表ノード指名レスポンスを受信するステップと、
（Ｇ８）受信した前記代表ノード指名レスポンスに、代表ノードになることを拒否するメッセージが付加されているか確認するステップと、
（Ｇ９）代表ノード数が所定数に達しているかどうか確認するステップと、を有することを特徴とする分散認証方法。
【請求項４０】
請求項３２に記載の分散認証方法において、
前記（Ｈ）代表ノードを離脱するときの動作を行うステップは、
（Ｈ１）代表ノード離脱動作時の初期状態ステップと、
（Ｈ２）前記代表ノードから、全ての代表ノードの電子署名が付加されたノードリストを受信するステップと、
（Ｈ３）受信した前記ノードリストに、電子署名を付加するステップと、
（Ｈ４）前記全ての代表ノードの電子署名が付加されたノードリストを送信してきた代表ノードに対し、電子署名を付加した前記ノードリストを送信するステップと、を有することを特徴とする分散認証方法。
【請求項４１】
請求項３２から４０のいずれか一項に記載の分散認証方法を、コンピュータに実行させるための分散認証プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、分散認証システム、分散認証方法、及び分散認証プログラムに係り、特にメッセージに付された電子証明書の正当性を検証し、その電子証明書の公開鍵を用いて電子署名を復号して当該メッセージの正当性を検証する認証技術に関する。

【背景技術】
【０００２】
インターネット上では、Ｐ２Ｐ（Peer to Peer）技術を用いたファイル共有ネットワークにより、テキストコンテンツだけでなく画像や音声、映像といった様々なコンテンツがユーザ間で直接やりとりされるようになってきた。
【０００３】
しかし、ファイル共有ネットワークへの参加を完全に自由にしてしまうと不正ノードの参加や不正コンテンツ流通の原因になる。そこで、従来はファイル共有ネットワークに認証技術を適用することでこれを回避してきた。
【０００４】
例えば、認証局を用いるものがある。これは、あるノードがファイル共有ネットワークに参加するために事前に認証局に電子証明書を発行してもらい、電子署名を用いてノード間で相互認証するものである。
【０００５】
なお、本発明に関連する先行技術文献としては、以下のものがある。
【特許文献１】特開２００４－１５９２９８号公報
【特許文献２】特開２００４－１７１２７４号公報
【特許文献３】特開２００４－２５４２７１号公報
【特許文献４】特開２００６－１０１２７７号公報
【特許文献５】特開平１１－０１５３７４号公報
【発明の開示】
【発明が解決しようとする課題】
【０００６】
しかしながら、前述した従来の認証局を用いた技術では、認証局はネットワーク上の特定の場所に存在するため攻撃対象になりやすいという問題があった。その理由は、認証局は、あらゆる場所に存在するノードから接続可能にするためにネットワーク上の特定の場所に存在し、従って悪意のある攻撃者にも認証局の場所が判明してしまうため、容易に攻撃されてしまうというセキュリティリスクがあることによる。
【０００７】
本発明の目的は、認証局の場所が判明して容易に攻撃されやすいというセキュリティリスクを抑制し、認証局への攻撃耐性を向上させることができる分散認証システムを提供することにある。
【課題を解決するための手段】
【０００８】
上記目的を達成するため、本発明に係る分散認証システムは、ひとつまたは複数のノードで構成される分散認証システムであって、前記分散認証システムに参加するノードのうち所定数台のノードが、前記分散認証システムを代表する代表ノードとなり、前記代表ノードが、互いに連携することによって、前記分散認証システムの電子署名で用いる代表鍵と、分散認証システム電子証明書と、前記分散認証システムに参加するノードの電子署名で用いる個人鍵と、前記分散認証システムに参加するノードの電子証明書とを発行することを特徴とする。
【０００９】
本発明に係る分散認証方法は、ひとつまたは複数のノードで構成される分散認証システムであり、前記分散認証システムに参加するノードのうち所定数台のノードが前記分散認証システムを代表する代表ノードとなり、前記代表ノードが、互いに連携することによって、前記分散認証システムの電子署名で用いる代表鍵と、分散認証システム電子証明書と、前記分散認証システムに参加するノードの電子署名で用いる個人鍵と、前記分散認証システムに参加するノードの電子証明書とを発行する分散認証システムの分散認証方法であって、（Ａ）前記分散認証システムへの参加を開始するステップと、（Ｂ）前記分散認証システムに参加する全ノード数が所定数未満の場合、総意モードの動作を行うステップと

、（Ｃ）前記分散認証システムに参加する全ノード数が所定数以上の場合、代表モードの動作として、前記代表ノード以外の一般ノードのときの動作を行うステップと、（Ｄ）前記代表モードの動作として、前記代表ノードのときの動作を行うステップと、（Ｅ）他ノードから受信したメッセージの電子署名を確認するときの動作を行うステップと、（Ｆ）前記代表ノードの初期の動作を行うステップと、（Ｇ）前記代表ノードを更新するときの動作を行うステップと、（Ｈ）前記代表ノードを離脱するときの動作を行うステップとを有することを特徴とする。

【発明の効果】

【００１０】

本発明によれば、認証局の場所が判明して容易に攻撃されやすいというセキュリティリスクを抑制し、認証局への攻撃耐性を向上させることができる分散認証システムを提供することができる。

【発明を実施するための最良の形態】

【００１１】

以下、本発明の実施形態について、添付図を参照して説明する。

【００１２】

本実施形態は、独立した認証局が無い状況において、ファイル共有ネットワークに参加するノードが連携することで認証局になり、ファイル共有ネットワークに新たに参加するノードの電子署名のための鍵（代表鍵、個人鍵）の発行、及び電子証明書（分散認証システム電子証明書、ノードの電子証明書）の保存を実施する分散認証システム、分散認証方法、及びプログラムに関するものである。

【００１３】

本実施形態において、分散認証システム電子証明書は、認証局の電子証明書に対応し、後述するように、代表鍵の公開鍵を含み、分散認証システムの電子署名は、認証局の電子署名に対応し、代表鍵の秘密鍵で暗号化されたものである。また、ノードの電子証明書は、後述するように、個人鍵の公開鍵と、分散認証システムの電子署名とを含み、ノードの電子署名は、個人鍵の秘密鍵で暗号化されたものである。

【００１４】

ここで、ノードの電子証明書に含まれる分散認証システムの電子署名を、分散認証システム電子証明書に含まれる代表鍵の公開鍵で復号化することにより、当該ノードの電子証明書の正当性が検証可能となる。また、ノードからの送信メッセージに付加される当該ノードの電子署名を、当該ノードの電子証明書に含まれる個人鍵の公開鍵で復号化することにより、当該メッセージの正当性が検証可能となる。その詳細は後述する。

【００１５】

本実施形態の分散認証システムは、ひとつまたは複数のノードで構成される。分散認証システムに参加するノードのうち規定数台のノードが代表ノードとなる。規定数台の代表ノードは、互いに連携することによって、分散認証システムの代表鍵と、分散認証システム電子証明書と、分散認証システムに参加するノードの個人鍵と、分散認証システムに参加するノードの電子証明書とを発行する機能を有する。

【００１６】

本実施形態の分散認証システムを構成するノードは、他ノードから送られてくるデータを受信する受信部と、分散認証システムを構成するノードの情報を含むノードリストを更新可能に保存するノード情報保存部と、ノードリストに基づいて、前記分散認証システムのモードとして、前記分散認証システムに参加する全ノード数が所定数未満のときの総意モードと、前記分散認証システムに参加する全ノード数が所定数以上のときの代表モードとを管理するモード管理部と、代表モードの際に代表ノードのときの動作を行う代表ノード機能部と、代表モードの際に代表ノード以外の一般ノードのときの動作を行う一般ノード機能部と、総意モード及び代表モードに共通の動作を行う共通機能部と、代表ノード機能部、一般ノード機能部、及び共通機能部から渡される他ノードへのデータに電子署名を付加する署名付加部と、電子署名が付加されたデータを前記他ノードに送信する送信部と

、を有する。
【００１７】
一般ノード機能部は、ノードが一般ノードである場合に、仮鍵を生成する機能を有する仮鍵生成部と、分散認証システムに参加するために参加リクエストを他の既に分散認証システムに参加しているノードに参加リクエストを送信する機能を有する参加動作部と、を有する。
【００１８】
代表ノード機能部は、ノードが代表ノードである場合に、他の代表ノードと互いに連携し、分散認証システムの代表鍵と分散認証システム電子証明書を生成する機能を有する代表鍵生成部と、他のノードからの参加リクエストまたは電子証明書生成リクエストを受信し、他のノードの個人鍵と電子証明書を生成する機能を有する他ノード電子証明書生成部と、代表ノードを離脱する機能及び代表ノードが規定数より少なくなった場合に代表ノードを指名する機能を有する代表ノード指名・離脱機能部と、分散認証システムの代表鍵と他のノードの個人鍵の秘密鍵の素となるランダム素数を生成する機能を有するランダム素数生成部と、を有する。
【００１９】
共通機能部は、ノードが一般ノードまたは代表ノードの場合に、キープアライブ（ｋｅｅｐ　ａｌｉｖｅ）動作により他のノードとノードリストを交換する機能を有するキープアライブ動作部と、分散認証システムを利用するアプリケーションを実施する機能を有するアプリケーション部と、規定数台の代表ノードから受信する個人鍵の秘密鍵の素となる情報から個人鍵の秘密鍵を生成する機能を有する個人鍵生成部と、他のノードから受信するメッセージに付加されている電子署名の正当性を確認する機能を有する電子署名確認部と、を有する。
【００２０】
受信部は、受信したメッセージをモード管理部へ送る機能を有する。
【００２１】
モード管理部は、ノード情報保存部に保存されているノードリストを読み出す機能と、分散認証システムに参加しているノード数を確認する機能と、分散認証システムのモードを確認する機能と、を有する。さらに、モード管理部は、自ノードが代表ノードであるか、一般ノードであるか状態管理する機能を有する。
【００２２】
代表ノードは、他の代表ノードと互いに連携し、分散認証システムの代表鍵と分散認証システム電子証明書を生成する機能と、他のノードからの参加リクエストまたは電子証明書生成リクエストを受信し、他のノードの個人鍵と電子証明書を生成する機能と、代表ノードを離脱する機能と、代表ノードが規定数より少なくなった場合に代表ノードを指名する機能と、分散認証システムの代表鍵と他のノードの個人鍵の秘密鍵の素となるランダム素数を生成する機能と、キープアライブ動作により他のノードとノードリストを交換する機能と、分散認証システムを利用するアプリケーションを実施する機能と、規定数台の代表ノードから受信する個人鍵の秘密鍵の素となる情報から個人鍵の秘密鍵を生成する機能と、他のノードから受信するメッセージに付加されている電子署名の正当性を確認する機能と、を有する。
【００２３】
ノードリストは、分散認証システムに参加している全ノードのノード情報と、代表ノード情報と、を有する。ノード情報は、ノードのＩＤと、ノードのＩＰアドレスと、ポート番号と、代表ノード情報と、旧代表ノード情報と、を含む。代表ノード情報は、分散認証システムを代表する代表ノードがどのノードであるかという情報を含む。旧代表ノード情報は、過去に分散認証システムを代表する代表ノードがどのノードであったかという情報を含む。
【００２４】
仮鍵は、分散認証システムによって発行された鍵ではなく、各ノードが生成する鍵であ

って、新規に分散認証システムに参加する場合と、総意モードの場合に、他ノードへの全てのメッセージに付加される電子署名に利用される。

【００２５】

鍵は、公開鍵暗号系における秘密鍵、公開鍵のことであり、鍵は秘密鍵と公開鍵のセットで存在するものであって、分散認証システムの代表鍵は代表鍵の秘密鍵と代表鍵の公開鍵から成り、あるノードの個人鍵は個人鍵の秘密鍵と個人鍵の公開鍵から成る。

【００２６】

分散認証システムの代表鍵は、分散認証システムを代表する規定数台の代表ノードが互いに連携して作成する鍵であって、ノードリストと、分散認証システムに参加するノードの電子証明書に分散認証システムの電子署名を付加する場合に使用される。ただし、分散認証システムの代表鍵の秘密鍵は、複数の代表ノードで分散して保存され、分散認証システム上のどのノードも分散認証システムの代表鍵の秘密鍵を知ることはできない。一方、分散認証システムの代表鍵の公開鍵は、分散認証システム上に公開され、分散認証システム上のどのノードも参照することができる。

【００２７】

分散認証システムに参加するノードの電子証明書とは、分散認証システムを代表する規定数台の代表ノードが互いに連携して作成する個人鍵の公開鍵と、分散認証システムに参加するノードの情報と、分散認証システムを代表する規定数台の代表ノードが互いに連携して作成する個人鍵の公開鍵と分散認証システムに参加するノードの情報のダイジェスト情報に分散認証システムの代表鍵による電子署名を付加したものである。

【００２８】

ダイジェスト情報とは、元になる情報の要約情報を指し、元になる情報に一方向関数を適用することで生成される。

【００２９】

さらに、モード管理部は、ノード情報保存部に保存されているノード情報を定期的に読み出し、分散認証システムに参加するノード数が規定数未満であるかそうでないかを確認する機能を有し、分散認証システムに参加するノード数が規定数未満であった場合、ノードを総意モードで動作させ、分散認証システムに参加するノード数が規定数以上であった場合、ノードを代表モードで動作させ、さらに代表モードの場合、代表ノードに指名されていた場合、ノードを代表ノードとして動作させ、代表ノードに指名されていなかった場合、ノードを一般ノードとして動作させる。

【００３０】

さらに、モード管理部は、総意モードにおいて、ノード情報保存部に保存されているノードリストを確認し、分散認証システムに参加している全ノード数が規定数に到達していた場合、ノードを代表モードに移行させる機能を有する。

【００３１】

さらに、モード管理部は、代表ノード機能部に、分散認証システムの代表鍵を生成するよう指示する機能と、一般ノード機能部に、分散認証ネットワークに改めて参加し分散認証システムの発行する電子証明書及び鍵を得るよう指示する機能と、代表ノード機能部に鍵の秘密鍵を用いてノードリストに電子署名をするよう指示する機能と、代表ノード機能部に、規定数台の代表ノードによる電子署名の完了したノードリストに分散認証システムの代表鍵による電子署名を付加するよう指示する機能と、を有する。

【００３２】

さらに、モード管理部は、受信したメッセージを適切な機能部へ振り分けを行う機能を有する。

【００３３】

参加動作部は、自ノードが新規に分散認証システムに参加する場合に、仮鍵の公開鍵を付加した参加リクエストを送信する機能と、参加リクエストを受信した場合に参加リクエストに付加されている仮鍵の公開鍵を用いて電子署名を確認し、改ざんがない場合は参加レスポンスを送信する機能と、を有する。ただし、参加動作部は、分散認証システムが総

意モードであった場合、参加レスポンスに自ノードの仮鍵の公開鍵と、ノードリストを付加し、署名付加部により仮鍵の秘密鍵で電子署名をした上で、参加レスポンスを送信し、分散認証システムが代表モードであった場合、参加レスポンスには参加リクエストを受理した旨のメッセージを、自ノードの個人鍵の秘密鍵で電子署名をし、参加レスポンスを送信し、さらに、参加動作部は、ノード情報保存部からノードリストを読み出し、代表ノードを確認し、ある代表ノードに対し、参加リクエストを送信してきたノードのノード情報が付加した電子証明書生成リクエストを送信する機能を有する。

【００３４】

仮鍵生成部は、仮鍵を生成する機能と、生成した仮鍵を自ノードのノード情報と共にノード情報保存部に保存する機能を有する。

【００３５】

ランダム素数生成部は、代表鍵生成部と他ノード電子証明書生成部からのリクエストを受けて、ランダムな素数を生成する機能と、代表鍵生成部と他ノード電子証明書生成部に生成したランダムな素数を渡す機能とを有する。

【００３６】

代表鍵生成部は、分散認証システムが代表モードかつ自ノードが代表ノードであった場合に、モード管理部から分散認証システムの代表鍵を生成するように指示を受けると、他の規定数台の分散認証システムを代表する代表ノードと連携し、ランダム素数生成部が生成した素数を素に、代表鍵の公開鍵の素となる情報を他のノードに知らせることなく、マルチパーティプロトコルを用いて、分散認証システムの代表鍵の公開鍵を生成する機能と、ノードが代表ノードでなくなるまで代表鍵の生成に利用した素数を保存する機能とを有する。

【００３７】

さらに、代表鍵生成部は、分散認証システムが代表モードかつ自ノードが代表ノードであった場合に、モード管理部から規定数台の代表ノードによる電子署名の完了したノードリストに分散認証システムの代表鍵による電子署名を付加するように指示を受けると、他の規定数台の分散認証システムを代表する代表ノードと連携し、代表鍵の素となる情報を他のノードに知らせることなく、ノードリストに分散認証システムの代表鍵の秘密鍵を用いた電子署名を付加する機能を有する。

【００３８】

代表ノード指名・離脱機能部は、自ノードが代表ノードであり代表ノードを離脱したい場合に、ノード情報保存部からノードリストを読み出し、代表ノード離脱リクエストを他の代表ノードに送信する機能と、自ノードが代表ノードであった場合に、代表ノード離脱リクエストを受信すると、代表ノード離脱リクエストを送信してきた代表ノードに対し、代表ノード離脱レスポンスを送信する機能と、代表ノードが規定数未満である状態から、代表ノードを規定数台とするため、ノード情報保存部からノードリストを読み出し、適当な一般ノードを選出する機能と、選出した一般ノードのノード情報を記載した代表ノード指名確認メッセージを他の代表ノード全てに送信する機能と、代表ノード指名確認メッセージを受信した場合に、選出された一般ノードのノード情報を確認し、可否情報を含む代表ノード指名確認レスポンスを返送する機能と、自身を除く全ての代表ノードから代表ノード指名確認レスポンスを受信した場合に、選出した一般ノードに代表ノード指名リクエストを送信する機能と、自ノードが一般ノードでありノード代表ノード指名リクエストを受信した場合に、可否情報を含む代表ノード指名レスポンスを返送する機能と、代表ノード指名レスポンスを受信した場合に、新しく代表ノードとなるノードのノード情報を、自ノードを除く全ての代表ノードに送信する機能とを有する。

【００３９】

さらに、代表ノード指名・離脱機能部は、上記の動作を代表ノードが規定数台になるまで繰り返す機能と、代表ノード機能部に、個人鍵の秘密鍵を用いてノードリストに電子署名をするよう指示する機能と、代表鍵を更新する前まで代表ノードであった旧代表ノードに対し、現在代表ノードであるノードによる電子署名が修了しているノードリストに電子

署名をするよう指示する機能と、代表ノード機能部に、規定数台の代表ノード及び規定数台の旧代表ノードによる電子署名の完了したノードリストに分散認証システムの代表鍵による電子署名を付加するよう指示する機能と、代表鍵の公開鍵とセットで分散認証ネットワーク電子証明書として、ノード情報保存部に保存する機能とを有する。

【００４０】

他ノード電子証明書生成部は、分散認証システムが代表モードかつ自ノードが代表ノードであった場合に、電子証明書生成リクエストを受信すると、他の代表ノードと連携し、ランダム素数生成部が生成する素数を素に、電子証明書に付随する個人鍵の素となる情報を他のノードに知らせることなく、マルチパーティプロトコルを用いて、電子証明書リクエストに記載のノードの個人鍵を生成する機能と、代表鍵生成部と連携し、前記ノードのノード情報と個人鍵から電子証明書を生成する機能と、個人鍵の秘密鍵の素となる情報と公開鍵と、電子証明書を電子証明書生成リクエストに記載のノードに送信する機能を有する。

【００４１】

キープアライブ動作部は、他のノードに対し定期的にキープアライブメッセージを送信する機能と、他のノードから定期的にキープアライブメッセージを受信することで通信路のつながりをチェックする機能と、キープアライブメッセージに付加されたノードリストとノード情報保存部から読み出したノードリストを比較し、ノードリストを最新の情報に更新する機能と、キープアライブメッセージに対し一定期間レスポンスがない場合は該当ノードは分散認証システムから離脱したと判定し、ノードリストを更新し、キープアライブ動作を用いて他のノードに最新の情報を伝える機能と、代表ノードが離脱したと判定した場合に、ノード管理部に代表ノードが離脱したことを送信する機能とを有する。

【００４２】

アプリケーション部は、分散認証システムを利用するアプリケーションの処理をする機能を有する。

【００４３】

個人鍵生成部は、規定数台の代表ノードから受信する個人鍵の秘密鍵の素となる規定数個の情報から個人鍵の秘密鍵を生成する機能と、受信した公開鍵と秘密鍵が有効に動作するか確認する機能と、受信した電子証明書の有効性を確認する機能とを有する。

【００４４】

電子署名確認部は、メッセージを受信した場合にメッセージ送信元を確認し、分散認証システムにメッセージ送信元のノードの電子証明書発行リクエストを送信する機能と、メッセージ送信元のノードの電子証明書を得た場合に、電子証明書に付加されている分散認証システムの代表鍵による電子署名を確認するため、分散認証システムに分散認証システム電子証明書発行リクエストを送信する機能と、分散認証システム電子証明書に付加されている代表鍵の公開鍵を得た場合に、電子証明書に付加されている電子署名を公開鍵で復号し、電子証明書の正当性を確認する機能と、受信したメッセージに付加されている電子署名を電子証明書に付加されている公開鍵で復号し、メッセージの正当性を確認する機能と、他のノードから電子証明書発行リクエストを受信した場合に、該当する電子証明書をノード情報保存部から読み出し、電子証明書発行レスポンスを返送する機能と、他のノードから分散認証システム電子証明書発行リクエストを受信した場合に、該当する公開鍵をノード情報保存部から読み出し、分散認証システム電子証明書発行レスポンスを送信する機能とを有する。

【００４５】

署名付加部は、分散認証システムが総意モードの場合にノード情報保存部に保存されている仮鍵を使用し、他の機能部からのメッセージに電子署名を付加する機能と、分散認証システムによって電子証明書の発行を受けていない場合にノード情報保存部に保存されている仮鍵を使用し、他の機能部からのメッセージに電子署名を付加する機能と散認証システムが総意モードの場合でなく、分散認証システムによって電子証明書の発行を受けている場合に、ノード情報保存部に保存されている個人鍵を使用し、他の機能部からのメッセ

ージに電子署名を付加する機能と、を有する。
【００４６】
送信部は、署名付加部からのメッセージを受け、メッセージに記載された宛先のノードに対し、メッセージを送信する機能を有する。
【００４７】
ノード情報保存部は、自ノードのノード情報、仮鍵、電子証明書、ノードリスト、分散認証ネットワーク電子証明書、を保存する機能を有する。
【００４８】
本実施形態に係る分散認証システムの分散認証方法は、（Ａ）分散認証システム参加を開始するステップと、（Ｂ）総意モードのときの動作を行うステップと、（Ｃ）一般ノードのときの動作を行うステップと、（Ｄ）代表ノードのときの動作を行うステップと、（Ｅ）受信したメッセージの電子署名を確認するときの動作を行うステップと、（Ｆ）代表ノードの初期の動作を行うステップと、（Ｇ）代表ノードを更新するときの動作を行うステップと、（Ｈ）代表ノードを離脱するときの動作を行うステップとを有する。
【００４９】
前記（Ａ）分散認証システムに参加するを開始するステップは、（Ａ１）初期状態ステップと、（Ａ２）仮鍵を生成するステップと、（Ａ３）仮鍵及び、ノード情報を保存するステップと、（Ａ４）他の既に分散認証システムに参加しているノードに対し、参加リクエストを送信するステップと、（Ａ５）分散認証システムのモードを確認するステップと、（Ａ６）参加依頼レスポンスとして、参加依頼リクエストを送信したノードの仮鍵及びノードリストを受信し、ノードリストを更新するステップと、（Ａ７）ノードリストを読み出し、ノードリストに記載の全ノードの仮鍵を保持しているか確認するステップと、（Ａ８）参加レスポンスを受信するステップと、（Ａ９）規定数台の代表ノードから個人鍵の秘密鍵の素となる情報と、電子証明書を受信するステップと、（Ａ１０）ステップＡ９で受信した個人鍵の秘密鍵の素となる情報から個人鍵を生成するステップとを有する。
【００５０】
前記（Ｂ）総意モードのときの動作を行うステップは、（Ｂ１）総意モードの動作時の初期状態ステップと、（Ｂ２）キープアライブ動作により、他の分散認証システムに参加するノードとノードリストの交換を行うステップと、（Ｂ３）ノードリストを読み出し、分散認証システムに参加するノード数が規定数に達しているかどうかを確認するステップとを有する。
【００５１】
前記（Ｃ）一般ノードのときの動作を行うステップは、（Ｃ１）一般ノード動作の初期状態ステップと、（Ｃ２）ノードリストを読み出し、他のノードに対し、ノードリストを付加したキープアライブメッセージを送信するステップと、（Ｃ３）他のノードから、ノードリストが付加されたキープアライブメッセージを受信するステップと、（Ｃ４）ステップＣ３で受信したキープアライブメッセージに付加されていたノードリストと自ノードが保存していたノードリストを比較し最新の情報に更新するステップと、（Ｃ５）ノードリストを読み出し、分散認証システムに参加するノード数が規定数に達しているかどうかを確認するステップと、（Ｃ６）参加リクエストを受信するステップと、（Ｃ７）参加リクエストを送信してきたノードに対し、参加レスポンスを送信するステップと、（Ｃ８）規定数台の代表ノードのうち、任意の代表ノードに対し、電子証明書作成リクエストを送信するステップと、（Ｃ９）代表ノード指名リクエストを受信するステップと、（Ｃ１０）代表ノードになるかどうか選択するステップと、（Ｃ１１）代表ノードになるために、ステップＣ９で代表ノード指名リクエストを送信してきたノードに対し、代表ノード指名レスポンスを送信するステップと、（Ｃ１２）代表ノードになることを拒否するために、ステップＣ９で代表ノード指名リクエストを送信してきたノードに対し、代表ノード拒否の情報を付加し代表ノード指名レスポンスを送信するステップと、（Ｃ１３）電子証明書発行リクエストを受信するステップと、（Ｃ１４）ステップＣ１３で電子証明書発行リクエストを送信してきたノードに対し、自ノードの電子証明書を付加した電子証明書発行レ

スポンスを送信するステップとを有する。

【００５２】

前記（Ｄ）代表ノードのときの動作を行うステップは、（Ｄ１）代表ノード動作時の初期状態ステップと、（Ｄ２）ノードリストを読み出し、他のノードに対し、ノードリストを付加したキープアライブメッセージを送信するステップと、（Ｄ３）他のノードから、ノードリストが付加されたキープアライブメッセージを受信するステップと、（Ｄ４）ステップＤ３で受信したキープアライブメッセージに付加されていたノードリストと自ノードが保存していたノードリストを比較し最新の情報に更新するステップと、（Ｄ５）ノードリストを読み出し、分散認証システムに参加するノード数が規定数に達しているかどうかを確認するステップと、（Ｄ６）ノードリストを読み出し、代表ノードが離脱していないか確認するステップと、（Ｄ７）代表ノードを離脱したい場合、他の代表ノードに対し、代表ノード離脱リクエストを送信するステップと、（Ｄ８）代表ノード離脱レスポンスを受信するステップと、（Ｄ９）参加リクエストを受信するステップと、（Ｄ１０）参加リクエストを送信してきたノードに対し、参加レスポンスを送信するステップと、（Ｄ１１）参加リクエストを送信してきたノードの個人鍵の秘密鍵の素となる情報となるランダム素数を生成するステップと、（Ｄ１２）規定数台の代表ノード間で互いに連携し、参加リクエストを送信してきたノードの個人鍵の公開鍵を生成するステップと、（Ｄ１３）規定数台の代表ノード間で互いに連携し、参加リクエストを送信してきたノードの電子証明書を生成するステップと、（Ｄ１４）ステップＤ１１で生成した参加リクエストを送信してきたノードの個人鍵の秘密鍵の素となる情報と、ステップＤ１２で生成した参加リクエストを送信してきたノードの個人鍵の公開鍵と、ステップＤ１３で生成した参加リクエストを送信してきたノードの電子証明書を、参加リクエストを送信してきたノードに対し送信するステップと、（Ｄ１５）電子証明書生成リクエストを受信するステップと、（Ｄ１６）代表ノード離脱リクエストを受信するステップと、（Ｄ１７）代表ノード離脱レスポンスを送信するステップと、（Ｄ１８）代表ノード指名確認メッセージを受信するステップと、（Ｄ１９）代表ノード指名確認レスポンスを送信するステップと、（Ｄ２０）電子証明書発行リクエストを受信するステップと、（Ｄ２１）ステップＤ２０で電子証明書発行リクエストを送信してきたノードに対し、自ノードの電子証明書を付加した電子証明書発行レスポンスを送信するステップと、（Ｄ２２）分散認証システム電子証明書発行リクエストを受信するステップと、（Ｄ２３）ステップＤ２２で分散認証システム電子証明書発行リクエストを送信してきたノードに対し、分散認証システム電子証明書を付加した分散認証システム電子証明書発行レスポンスを送信するステップとを有する。

【００５３】

前記（Ｅ）受信したメッセージの電子署名を確認するときの動作を行うステップは、（Ｅ１）署名確認動作の初期状態ステップと、（Ｅ２）メッセージ送信元のノードの電子証明書発行リクエストを送信するステップと、（Ｅ３）電子証明書発行レスポンスを受信するステップと、（Ｅ４）代表ノードに対し、分散認証システム電子証明書発行リクエストを送信するステップと、（Ｅ５）分散認証システム電子証明書発行レスポンスを受信するステップと、（Ｅ６）分散認証システム電子証明書に付加されている代表鍵の公開鍵を用い、電子証明書に付加されている電子署名を公開鍵で復号し、電子証明書の正当性を確認し、さらに、受信したメッセージに付加されている電子署名を電子証明書に付加されている公開鍵で復号し、メッセージの正当性を確認するステップとを有する。

【００５４】

前記（Ｆ）代表ノードの初期の動作を行うステップは、（Ｆ１）代表ノード初期動作時の初期状態ステップと、（Ｆ２）分散認証システムの代表鍵の秘密鍵の素となる情報となるランダム素数を生成するステップと、（Ｆ３）規定数台の代表ノード間で互いに連携し、分散認証システムの代表鍵の公開鍵を生成するステップと、（Ｆ４）この時点のノードリストに対し、個人鍵の秘密鍵を用いて電子署名をするステップと、（Ｆ５）他の代表ノードに対し、電子署名済みのノードリストを送信するステップと、（Ｆ６）他の代表ノードから、ノードリストを受信するステップと、（Ｆ７）ステップＦ６で受信したノードリ

ストに全代表ノードの電子署名が付加されているか確認するステップと、（Ｆ８）全代表ノードによる電子署名が完了したノードリストを、残存する旧代表ノードに送信するステップと、（Ｆ９）残存する旧代表ノードによる電子署名が付加されたノードリストを受信するステップと、（Ｆ１０）ステップＦ９で受信したノードリストに、残存する旧代表ノード全てによる電子署名が付加されているか確認するステップと、（Ｆ１１）規定数台の代表ノード間で互いに連携し、分散認証システム電子証明書を作成するステップとを有する。

【００５５】

前記（Ｇ）代表ノードを更新するときの動作を行うステップは、（Ｇ１）代表ノード更新動作時の初期状態ステップと、（Ｇ２）新たに代表ノードになるノードを選出するステップと、（Ｇ３）代表ノード指名確認メッセージを、他の代表ノードに送信するステップと、（Ｇ４）代表ノード指名確認レスポンスを受信するステップと、（Ｇ５）ステップＳ－Ｆ４で受信した代表ノード指名確認レスポンスに、ステップＧ２で選出したノードを拒否するメッセージが付加されているか確認するステップと、（Ｇ６）ステップＧ２で選出したノードに対し、代表ノード指名リクエストを送信するステップと、（Ｇ７）ステップＧ２で選出したノードから、代表ノード指名レスポンスを受信するステップと、（Ｇ８）ステップＧ７で受信した代表ノード指名レスポンスに、代表ノードになることを拒否するメッセージが付加されているか確認するステップと、（Ｇ９）代表ノード数が規定数に達しているかどうか確認するステップとを有する。

【００５６】

前記（Ｈ）代表ノードを離脱するときの動作を行うステップは、（Ｈ１）代表ノード離脱動作時の初期状態ステップと、（Ｈ２）代表ノードから、全ての代表ノードの電子署名が付加されたノードリストを受信するステップと、（Ｈ３）ステップＨ２で受信したノードリストに、電子署名を付加するステップと、（Ｈ４）ステップＨ２で全ての代表ノードの電子署名が付加されたノードリストを送信してきた代表ノードに対し、ステップＨ３で電子署名を付加したノードリストを送信するステップとを有する。

【００５７】

本実施形態の分散認証プログラムは、上記分散認証方法を、コンピュータに実行させるためのプログラムである。

【００５８】

以上説明したように、本実施の形態では、分散認証システムに参加するノードのうち規定数台のノードが代表ノードとなり、分散認証システムの代表鍵とその分散認証システム電子証明書を発行し、分散認証システムに参加するノードの個人鍵及びその電子証明書を発行する。規定数台の代表ノードは、互いに連携してマルチパーティプロトコルを利用することによって、上記の鍵及び電子証明書を発行する処理を分担して行うが、他のノードの秘密鍵を知ることはできない。全ノード数が規定数より少ない場合は、総意モードとなり、代表鍵は生成されず、仮鍵を相互に交換して認証する。それ以外では、代表モードとなり、代表ノードが選出され、代表ノードは定期的に変更され、新規に代表ノードになるノードを、代表ノードを継続するノードが承認することで代表鍵が継承される。

【００５９】

従って、本実施形態によれば、次のような効果を奏することができる。

【００６０】

第一の効果は、認証局の攻撃耐性が向上することにある。その理由は、分散認証システムに参加するノードのうち規定数台のノードが代表ノードとなり、分散認証システムの代表鍵と分散認証システム電子証明書の発行、及び分散認証システムに参加するノードの個人鍵及び電子証明書の発行を、規定数台の代表ノードが互いに連携することによって実現し、さらに代表ノードの指名・離脱を柔軟にすることによって、悪意のある攻撃者からの攻撃に対し、攻撃対象を分散させることができ、かつ攻撃されたとしても、代表ノードを次々と変化させることによって、分散認証システムとしての機能を失わずに、認証サービスを続けることができるためである。

【００６１】
第二の効果は、特定の認証局なしに、特定の認証局がある場合と同等の安全性をもった認証サービスを提供することができることにある。その理由は、分散認証システムに参加するノードのうち規定数台のノードが代表ノードとなり、分散認証システムの代表鍵と分散認証システム電子証明書の発行、及び分散認証システムに参加するノードの個人鍵及び電子証明書の発行を、規定数台の代表ノードが互いに連携することによって実現し、さらに代表ノードの指名・離脱を柔軟にすることによって、ある特定の場所に認証局が存在する場合と同等の安全性を持った認証サービスを提供することができるためである。
【実施例１】
【００６２】
まず、本発明の第１の実施例について、図面を参照して詳細に説明する。
【００６３】
図１を参照すると、本実施例に係る分散認証システムを構成するノードは、受信部１と、モード管理部２と、一般ノード機能部３と、代表ノード機能部４と、共通機能部５と、ノード情報保存部８と、署名付加部６と、送信部７と、を有する。
【００６４】
一般ノード機能部３は、参加動作部３１と、仮鍵生成部３２と、を有する。
【００６５】
代表ノード機能部４は、ランダム素数生成部４１と、代表鍵生成部４２と、代表ノード指名・離脱機能部４３と、他ノード電子証明書生成部４４と、を有する。
【００６６】
共通機能部５は、ｋｅｅｐ　ａｌｉｖｅ（キープアライブ）動作部５１と、アプリケーション部５２と、個人鍵生成部５３と、電子署名確認部５４と、を有する。
【００６７】
受信部１は、受信したメッセージをモード管理部２へ送る。
【００６８】
モード管理部２は、ノード情報保存部８に保存されているノードリストを読み出し、分散認証システムに参加しているノード数を確認し、分散認証システムのモードを確認する。さらに、モード管理部２は、自ノードが代表ノードであるか、一般ノードであるか状態管理する。
【００６９】
ここで、分散認証システムのモードとは、総意モード、代表モードを指す。
【００７０】
総意モードとは、分散認証システムに参加する全ノード数が規定数ｍ未満の時のノード動作を指す。総意モードでは、ノードはそれぞれ仮鍵を生成し分散認証システムに参加する。すなわち総意モードでは、分散認証システムを代表する代表ノードは存在せず、参加するノードがそれぞれ用意する仮鍵を利用し、ノード間で相互に認証する。
【００７１】
一方、代表モードとは、分散認証システムに参加する全ノード数が規定数ｍ以上の時のノードの動作を指す。代表モードでは、分散認証システムに参加するノードのうちｍ台のノードが分散認証システムを代表する代表ノードとして動作し、それ以外のノードは一般ノードとして動作する。
【００７２】
ここで、代表ノードとは、分散認証システムを代表するノードのことであって、分散認証システムの代表鍵の生成、分散認証システムに参加するノードの鍵及び電子証明書の作成、代表ノードを指名する役割を担うノードである。代表ノードは、定期的に更新され、分散認証システムに参加する全ノードに代表ノードになる可能性がある。
【００７３】
ここで、ノードリストとは、分散認証システムに参加している全ノードのノード情報と、代表ノード情報のリストである。ノード情報とは、例えば、ノードのＩＤ、ノードのＩ

Ｐアドレスである。代表ノード情報とは、分散認証システムを代表する代表ノードがどのノードであるかを表す情報である。

【００７４】

ここで、仮鍵とは、分散認証システムによって発行された鍵ではなく、各ノードが生成する鍵である。仮鍵は、分散認証システムに新規に参加する場合と、総意モードの場合とに、他ノードへ送信される全てのメッセージに付加される電子署名に利用する。

【００７５】

ここで、鍵とは、公開鍵暗号系における秘密鍵及び公開鍵のことであり、その秘密鍵と公開鍵のセットで存在する。よって、分散認証システムの代表鍵は、代表鍵の秘密鍵と代表鍵の公開鍵とから成る。同様に、あるノードの個人鍵は、個人鍵の秘密鍵と個人鍵の公開鍵とから成る。

【００７６】

ここで、分散認証システムの代表鍵とは、分散認証システムを代表するｍ台の代表ノードが互いに連携して作成する鍵であって、ノードリストと、分散認証システムに参加するノードの電子証明書とに分散認証システムの電子署名を付加する場合に使用する。ただし、分散認証システムの代表鍵の秘密鍵は、複数の代表ノードで分散して保存され、分散認証システム上のどのノードも分散認証システムの代表鍵の秘密鍵を知ることはできない。一方、分散認証システムの代表鍵の公開鍵は、分散認証システム上に公開され、分散認証システム上のどのノードも参照することができる。本実施形態では、分散認証システムを代表するｍ台の代表ノードが互いに連携して作成する代表鍵の秘密鍵をランダムな数に設定できる公開鍵暗号系を用いる。この公開鍵暗号系として、例えばＥｌＧａｍａｌ暗号などがある。

【００７７】

ここで、分散認証システムに参加するノードの電子証明書とは、分散認証システムを代表するｍ台の代表ノードが互いに連携して作成する個人鍵の公開鍵と、分散認証システムに参加するノードの情報とに加え、これらの個人鍵の公開鍵及びノードの情報のダイジェスト情報に分散認証システムの代表鍵による電子署名を付加したものである。本実施形態では、分散認証システムを代表するｍ台の代表ノードが互いに連携して作成する個人鍵の秘密鍵をランダムな数に設定できる公開鍵暗号系を用いる。この公開鍵暗号系として、例えばＥｌＧａｍａｌ暗号などがある。ここで、ダイジェスト情報とは、元になる情報の要約情報を指す。例えば元になる情報にＳＨＡ－１などの一方向関数を適用することで生成する。

【００７８】

モード管理部２は、ノード情報保存部８に保存されているノード情報を定期的に読み出し、分散認証システムに参加するノード数が規定数ｍ未満であるかそうでないかを確認する。分散認証システムに参加するノード数が規定数ｍ未満であった場合、ノードは総意モードで動作する。一方、分散認証システムに参加するノード数が規定数ｍ以上であった場合、ノードは代表モードで動作する。代表モードの場合、代表ノードに指名されていた場合、代表ノードとして動作する。一方、代表モードの場合、代表ノードに指名されていなかった場合、一般ノードとして動作する。

【００７９】

また、総意モードにおけるモード管理部２はノード情報保存部８に保存されているノードリストを確認し、分散認証システムに参加している全ノード数が規定数ｍに到達していた場合、代表モードに移行する。

【００８０】

総意モードから代表モードに移行する場合、その時点で分散認証システムに参加している全ノード、すなわちｍ台のノードが代表ノードなる。そのために、モード管理部２は代表ノード機能部４に、分散認証システムの代表鍵を生成するよう指示する。さらに、モード管理部２は、一般ノード機能部３に、分散認証ネットワークに改めて参加し、分散認証システムの発行する電子証明書及び鍵を得るよう指示する。さらに、モード管理部２は、

代表ノード機能部４に、前記鍵の秘密鍵を用いてノードリストに電子署名をするよう指示する。さらに、モード管理部２は、代表ノード機能部４に、ｍ台の代表ノードによる電子署名の完了したノードリストに分散認証システムの代表鍵による電子署名を付加するよう指示する。

【００８１】

以上の動作によって分散認証システムの代表鍵による電子署名が付加されたノードリストは、代表鍵の公開鍵とセットで、分散認証システム電子証明書として、ノード情報保存部８に保存される。

【００８２】

図２に分散認証システム電子証明書の例を示す。同図に示すように、分散認証システム電子証明書には、分散認証システムに参加するノード及びそのノード情報（ＩＰアドレス、ポート番号等）を含むノードリストに、代表ノード毎の個人鍵による電子署名、旧代表ノード毎の個人鍵による電子署名、及び分散認証システムの代表鍵による電子署名が付加されている。

【００８３】

なお、総意モードから代表モードに移行する場合と同様の動作は、代表ノードが更新されるタイミングでも動作する。

【００８４】

一般ノード機能部３は、仮鍵生成部３２と、参加動作部３１とを有し、ノードが一般ノードである場合に、仮鍵を生成する機能と、分散認証システムに参加するために参加リクエストを他の既に分散認証システムに参加しているノードに参加リクエストを送信する機能と、を有する。

【００８５】

また、モード管理部２は、受信したメッセージを適切な機能部へ振り分けを行う。

【００８６】

仮鍵生成部３２は、仮鍵を生成する。生成した仮鍵は自ノードのノード情報と共にノード情報保存部８に保存される。仮鍵は、分散認証システムが発行する電子証明書に付随する鍵とは関係なく存在し、分散認証システムが発行する電子証明書に付随する鍵と暗号アルゴリズムが別であってもよい。

【００８７】

参加動作部３１は、自ノードが新規に分散認証システムに参加する場合に、参加リクエストを送信する。参加リクエストを送信する場合は、参加リクエストに自ノードの仮鍵の公開鍵を付加する。また、ノード情報保存部８から読み出した自ノードの仮鍵の秘密鍵を用いて、署名付加部６で参加リクエストに電子署名をする。また、参加リクエストを受信した場合、参加リクエストに付加されている仮鍵の公開鍵を用いて電子署名を確認し、改ざんがない場合は参加レスポンスを返送する。ただし、参加レスポンスは、分散認証システムのモードによって内容が異なる。分散認証システムが総意モードであった場合、参加レスポンスに自ノードの仮鍵の公開鍵と、ノードリストとを付加し、署名付加部６で自ノードの仮鍵の秘密鍵を用いて電子署名をした上で、その参加レスポンスを返送する。一方、分散認証システムが代表モードであった場合、参加レスポンスには参加リクエストを受理した旨のメッセージを、自ノードの個人鍵の秘密鍵で電子署名をし、その参加レスポンスを返送する。さらに、参加動作部３１は、ノード情報保存部８からノードリストを読み出し、代表ノードを確認し、ある代表ノードに対し、電子証明書生成リクエストを送信する。電子証明書生成リクエストには、参加リクエストを送信してきたノードのノード情報が付加される。

【００８８】

代表ノード機能部４は、ランダム素数生成部４１と、代表鍵生成部４２と、他ノード個人鍵生成部５３と、代表ノード指名・離脱機能部４３とを有し、ノードが代表ノードである場合に、他の代表ノードと互いに連携し、分散認証システムの代表鍵と分散認証システム電子証明書を生成する機能と、他のノードからの参加リクエストまたは電子証明書生成

リクエストを受信し、他のノードの個人鍵と電子証明書を生成する機能と、代表ノードを離脱する機能と、代表ノードが規定数ｍより少なくなった場合に代表ノードを指名する機能と、分散認証システムの代表鍵と他のノードの個人鍵の秘密鍵の素となるランダム素数を生成する機能と、を有する。

【００８９】

ランダム素数生成部４１は、代表鍵生成部４２と他ノード電子証明書生成部４４とからのリクエストを受けて、ランダムな素数を生成し、その生成したランダムな素数を代表鍵生成部４２と他ノード電子証明書生成部４４とに渡す。

【００９０】

代表鍵生成部４２は、分散認証システムが代表モードかつ自ノードが代表ノードであった場合に、モード管理部２から分散認証システムの代表鍵を生成するように指示を受けると、他のｍ台の分散認証システムを代表する代表ノードと連携し、分散認証システムの代表鍵を生成する。代表鍵の素には、ランダム素数生成部４１が生成する素数を使用する。代表鍵の秘密鍵は、ｍ台のノードが生成する素数から演算されるが、実際には演算されず、ｍ台の代表ノードとマルチパーティプロトコルを用いて代表鍵の公開鍵をのみを演算する。これにより、代表鍵の秘密鍵は、どのノードも知ることなく、代表ノードの公開鍵のみが正確に演算される。代表鍵生成部４２は、ノードが代表ノードでなくなるまで、代表鍵の生成に利用した素数を保存する。

【００９１】

また、代表鍵生成部４２は、分散認証システムが代表モードかつ自ノードが代表ノードであった場合に、モード管理部２からｍ台の代表ノードによる電子署名の完了したノードリストに分散認証システムの代表鍵による電子署名を付加するように指示を受けると、他のｍ台の分散認証システムを代表する代表ノードと連携し、ノードリストに分散認証システムの代表鍵の秘密鍵を用いた電子署名を付加する。分散認証システムの公開鍵を生成する時と同様に、ｍ台の代表ノードは互いに連携し、代表鍵の素となる情報を他のノードに知らせることなく、ノードリストに電子署名を付加する。

【００９２】

他ノード電子証明書生成部４４は、分散認証システムが代表モードかつ自ノードが代表ノードであった場合に、電子証明書生成リクエストを受信すると、他のｍ台の分散認証システムを代表する代表ノードと連携し、電子証明書リクエストに記載のノードの電子証明書を生成する。電子証明書に付随する個人鍵の素には、ランダム素数生成部４１が生成する素数を使用する。個人鍵の秘密鍵はｍ台のノードが生成する素数から演算されるが、実際には演算されず、ｍ台の代表ノードとマルチパーティプロトコルを用いて個人鍵の公開鍵をのみを演算する。これにより、個人鍵の秘密鍵はどのノードも知ることなく、個人鍵の公開鍵のみが正確に演算される。さらに、代表鍵生成部４２とも連携し、ノードのノード情報と個人鍵から電子証明書を生成する。以上の動作を完了した他ノード電子証明書生成部４４は、個人鍵の秘密鍵の素となる情報と公開鍵と、電子証明書を電子証明書生成リクエストに記載のノードに送信する。

【００９３】

代表ノード指名・離脱機能部４３は、自ノードが代表ノードであり代表ノードを離脱したい場合に、ノード情報保存部８からノードリストを読み出し、代表ノード離脱リクエストを他の代表ノードに送信する。代表ノードが離脱したい場合とは、例えば分散認証システムから離脱したいとき、ネットワークリソース不足であるとき、悪意のある攻撃者からの攻撃を受けているとき、などがある。

【００９４】

代表ノード指名・離脱機能部４３は、自ノードが代表ノードであった場合に、代表ノード離脱リクエストを受信すると、代表ノード離脱リクエストを送信してきた代表ノードに対し、代表ノード離脱レスポンスを送信する。さらに、代表ノード指名・離脱機能部４３は代表ノードが規定数ｍ未満である状態から、代表ノードをｍ台とするため、ノード情報保存部８からノードリストを読み出し、適当な一般ノードを選出し、選出した一般ノード

のノード情報を記載した代表ノード指名確認メッセージを他の代表ノード全てに送信する。

【００９５】

代表ノード指名確認メッセージを受信した代表ノード指名・離脱機能部４３は、選出された一般ノードのノード情報を確認し、代表ノード指名確認レスポンスを返送する。ただし、選出された一般ノードに問題がある場合は指名を拒否することもできる。問題とは、例えば、過去にレスポンスが遅かった、指定外のメッセージを送信してきた、などがある。自身を除く全ての代表ノードから代表ノード指名確認レスポンスを受信した代表ノードは、選出した一般ノードに代表ノード指名リクエストを送信する。

【００９６】

代表ノード指名リクエストを受信した一般ノードの代表ノード指名・離脱機能部４３は、代表ノード指名レスポンスを返送することで代表ノードになる。ただし、代表ノード指名リクエストを受信した一般ノードは、代表ノードになることを拒否することもできる。

【００９７】

代表ノード指名・離脱機能部４３は、代表ノード指名レスポンスを受信すると、新しく代表ノードとなるノードのノード情報を、自ノードを除く全ての代表ノードに送信する。代表ノード指名・離脱機能部４３は、以上の動作を代表ノードが規定数ｍ台になるまで繰り返す。

【００９８】

さらに、代表ノード指名・離脱機能部４３は、代表ノード機能部４に、個人鍵の秘密鍵を用いてノードリストに電子署名をするよう指示する。さらに、代表ノード指名・離脱機能部４３部は、代表鍵を更新する前まで代表ノードであった旧代表ノードに対し、現在代表ノードであるノードによる電子署名が修了しているノードリストに電子署名をするよう指示する。さらに、代表ノード指名・離脱機能部４３は、代表ノード機能部４に、ｍ台の代表ノード及びｍ台の旧代表ノードによる署名の完了したノードリストに分散認証システムの代表鍵による署名を付加するよう指示する。以上の動作によって電子署名が付加されたノードリストは、代表鍵の公開鍵とセットで分散認証ネットワーク電子証明書として、ノード情報保存部８に保存される。

【００９９】

共通機能部５は、ｋｅｅｐ　ａｌｉｖｅ動作部５１と、アプリケーション部５２と、個人鍵生成部５３と、電子署名確認部５４と、を有し、ノードが一般ノードまたは代表ノードの場合に、ｋｅｅｐ　ａｌｉｖｅ動作により他のノードとノードリストを交換する機能と、分散認証システムを利用するアプリケーションを実施する機能と、ｍ台の代表ノードから受信する個人鍵の秘密鍵の素となる情報から個人鍵の秘密鍵を生成する機能と、他のノードから受信するメッセージに付加されている電子署名の正当性を確認する機能と、を有する。

【０１００】

ｋｅｅｐ　ａｌｉｖｅ動作部５１は、他のノードに対し定期的にｋｅｅｐ　ａｌｉｖｅメッセージを送信し、さらに他のノードから定期的にｋｅｅｐ　ａｌｉｖｅメッセージを受信することで通信路のつながりをチェックする。ｋｅｅｐ　ａｌｉｖｅ動作部５１は、ノードリストｋｅｅｐ　ａｌｉｖｅメッセージにはノード情報保存部８から読み出したノードリストも添付され、ノードリストを他のノードと定期的に交換し、新しいノードリストに更新していくことで、ノードリストは最新の状態に保たれる。例えば、新規に分散認証システムに参加したノードを確認したノードは、ノードリストを更新し、ｋｅｅｐ　ａｌｉｖｅ動作を用いて他のノードに最新の情報を伝える。またｋｅｅｐ　ａｌｉｖｅメッセージに対し一定期間レスポンスがない場合は、該当ノードは分散認証システムから離脱したと判定し、ノードリストを更新し、ｋｅｅｐ　ａｌｉｖｅ動作を用いて他のノードに最新の情報を伝える。だたし、代表ノードが離脱したと判定した場合は、モード管理部２に代表ノードが離脱したことを送信する。

【０１０１】

アプリケーション部５２は、分散認証システムを利用するアプリケーションの処理をする。アプリケーションとして、例えばファイル交換アプリケーションや電話アプリケーションがある。本実施例の分散認証システムは、利用するアプリケーションに制限はない。

【０１０２】

個人鍵生成部５３は、ｍ台の代表ノードから受信する個人鍵の秘密鍵の素となるｍ個の情報から個人鍵の秘密鍵を生成する。さらに受信した公開鍵と秘密鍵が有効に動作するか確認する。さらに、受信した電子証明書の有効性を確認する。

【０１０３】

電子署名確認部５４は、あるメッセージに付加されている電子署名を確認し、メッセージの送信元からメッセージが改ざんされていないかを確認する。電子署名確認部５４は、メッセージを受信するとメッセージ送信元を確認し、分散認証システムにメッセージ送信元のノードの電子証明書発行リクエストを送信する。メッセージ送信元のノードの電子証明書を得ると、電子証明書に付加されている分散認証システムの代表鍵による電子署名を確認するため、分散認証システムに分散認証システム電子証明書発行リクエストを送信する。分散認証システム電子証明書に付加されている代表鍵の公開鍵を得ると、電子証明書に付加されている電子署名を代表鍵の公開鍵で復号し、電子証明書の正当性を確認する。さらに、受信したメッセージに付加されている電子署名を電子証明書に付加されている個人鍵の公開鍵で復号し、メッセージの正当性を確認する。

【０１０４】

また、電子署名確認部５４は、他のノードから電子証明書発行リクエストを受信した場合、該当する電子証明書をノード情報保存部８から読み出し、電子証明書発行レスポンスを返送する。さらに、電子署名確認部５４は、他のノードから分散認証システム電子証明書発行リクエストを受信した場合、該当する公開鍵をノード情報保存部８から読み出し、分散認証システム電子証明書発行レスポンスを返送する。

【０１０５】

署名付加部６は、他の機能部からのメッセージに電子署名を付加し、送信部７に渡す。ただし、ノードの状態によって電子署名のために使用する鍵が異なる。分散認証システムが総意モードの場合と、分散認証システムによって電子証明書の発行を受けていない場合は、ノード情報保存部８に保存されている仮鍵を使用し、メッセージに電子署名を付加する。それ以外の場合ではノード情報保存部８に保存されている個人鍵を使用し、メッセージに電子署名を付加する。

【０１０６】

送信部７は、署名付加部６からのメッセージを受け、メッセージに記載された宛先のノードに対し、メッセージを送信する。

【０１０７】

ノード情報保存部８は、自ノードのノード情報、仮鍵、電子証明書、ノードリスト、分散認証ネットワーク電子証明書、を保存する。電子証明書は、自身の電子証明書以外に、他のノードの電子証明書を保存することもできる。この場合、分散認証システム全体で全ノードの電子証明書を共有できるよう各ノードに分散して電子証明書を保存することが望ましい。分散して情報を保存するアルゴリズムとして、例えばＣｈｏｒｄアルゴリズムなどがある。

【０１０８】

次に、図３と、図４と、図５と、図６と、図７と、図８と、図９と、図１０とを参照して、本実施例の動作について詳細に説明する。

【０１０９】

図３は、本実施例の分散認証システムの動作を示すものである。

【０１１０】

図３において、ステップＳ－Ａ１は、初期状態である。この初期状態から、仮鍵を生成し（ステップＳ－Ａ２）、その仮鍵及びノード情報を保存し（ステップＳ－Ａ３）、他の既に分散認証システムに参加しているノードに対し、参加リクエストを送信する（ステッ

プＳ－Ａ４）。次いで、分散認証システムのモードを確認する（ステップＳ－Ａ５）。その結果、分散認証システムが総意モードであった場合、ステップＳ－ＡＡ１に移行する。一方、分散認証システムが代表モードであった場合、ステップＳ－ＡＢ１に移行する。

【０１１１】

上記ステップＳ－Ａ５にて分散認証システムが総意モードであった場合、参加依頼レスポンスとして、参加依頼リクエストを送信したノードの仮鍵及びノードリストを受信し（ステップＳ－ＡＡ１）、ノードリストを更新する。そして、ノードリストを読み出し、ノードリストに記載の全ノードの仮鍵を保持しているか確認する（ステップＳ－ＡＡ２）。その結果、ノードリストに記載の全ノードの仮鍵を保持していた場合（Ｙｅｓ）、後述の総意モード動作（ステップＳ－Ｂ１）へ移行する。一方、ノードリストに記載の全ノードの仮鍵を保持していなかった場合（Ｎｏ）、ステップＳ－Ａ４に戻り、仮鍵を保持していないノードに対し参加依頼リクエストを送信する。

【０１１２】

一方、ステップＳ－Ａ５にて分散認証システムが代表モードであった場合、参加レスポンスを受信する（ステップＳ－ＡＢ１）。そして、ｍ台の代表ノードから個人鍵の秘密鍵の素となる情報と、電子証明書とを受信し（ステップＳ－ＡＢ２）、受信した個人鍵の秘密鍵の素となる情報から個人鍵を生成し（ステップＳ－ＡＢ３）、後述の一般モード動作（ステップＳ－Ｃ１）へ移行する。

【０１１３】

図４は、総意モード動作を示すものである。

【０１１４】

図４において、ステップＳ－Ｂ１は、総意モード動作時の初期状態である。この初期状態から、ｋｅｅｐ　ａｌｉｖｅ動作により、他の分散認証システムに参加するノードとノードリストの交換を行う（ステップＳ－Ｂ２）。次いで、ノードリストを読み出し、分散認証システムに参加するノード数が規定数ｍに達しているかどうかを確認する（ステップＳ－Ｂ３）。その結果、分散認証システムに参加するノード数が規定数ｍに達していた場合は、後述の代表ノード初期動作（ステップＳ－Ｆ１）に移行する。分散認証システムに参加するノード数が規定数ｍに達していなかった場合は、初期状態（ステップＳ－Ｂ１）に移行する。

【０１１５】

図５は、一般ノード動作を示すものである。

【０１１６】

図５において、ステップＳ－Ｃ１は、一般ノード動作時の初期状態である。この初期状態から、ノードリストを読み出し、他のノードに対し、ノードリストを付加したｋｅｅｐ　ａｌｉｖｅメッセージを送信し（ステップＳ－ＣＡ１）、初期状態（ステップＳ－Ｃ１）に戻る。

【０１１７】

次いで、初期状態（ステップＳ－Ｃ１）において、他のノードからノードリストが付加されたｋｅｅｐ　ａｌｉｖｅメッセージを受信する（ステップＳ－ＣＢ２）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。

【０１１８】

次いで、受信したｋｅｅｐ　ａｌｉｖｅメッセージに付加されていたノードリストと自ノードが保存していたノードリストを比較し最新の情報に更新し（ステップＳ－ＣＢ２）。ノードリストを読み出し、分散認証システムに参加するノード数が規定数ｍに達しているかどうかを確認する（ステップＳ－ＣＢ３）。その結果、分散認証システムに参加するノード数が規定数ｍに達していた場合（Ｙｅｓ）は、初期状態（ステップＳ－Ｃ１）に移行する。一方、分散認証システムに参加するノード数が規定数ｍに達していなかった場合（Ｎｏ）は、前述の総意モード動作（ステップＳ－Ｂ１）に移行する。

【０１１９】

次いで、初期状態（ステップＳ－Ｃ１）において、参加リクエストを受信する（ステップＳ－ＣＣ１）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。

【０１２０】

次いで、参加リクエストを送信してきたノードに対し、参加レスポンスを送信し（ステップＳ－ＣＣ２）、ｍ台の代表ノードのうち、任意の代表ノードに対し、電子証明書作成リクエストを送信する（ステップＳ－ＣＣ３）。この電子証明書作成リクエストには、ステップＳ－ＣＢ１で参加リクエストを送信してきたノードのノード情報が含まれる。

【０１２１】

次いで、初期状態（ステップＳ－Ｃ１）において、代表ノード指名リクエストを受信する（ステップＳ－ＣＤ１）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。

【０１２２】

次いで、代表ノードになることを拒否するか否かを確認する（ステップＳ－ＣＤ２）。その結果、代表ノードになっても問題ない場合（Ｎｏ）、代表ノードになるために、ステップＳ－ＣＣ１で代表ノード指名リクエストを送信してきたノードに対し、代表ノード指名レスポンスを送信し（ステップＳ－ＣＤ３－１）、後述の代表ノード初期動作（ステップＳ－Ｆ１）に移行する。一方、代表ノードになることを拒否する場合（Ｙｅｓ）は、代表ノードになることを拒否するために、ステップＳ－ＣＤ１で代表ノード指名リクエストを送信してきたノードに対し、代表ノード拒否の情報を付加し代表ノード指名レスポンスを送信し（ステップＳ－ＣＤ３－２）、一般ノード動作時の初期状態（ステップＳ－Ｃ１）に移行する。

【０１２３】

次いで、初期状態（ステップＳ－Ｃ１）において、電子証明書発行リクエストを受信する（ステップＳ－ＣＥ１）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。次いで、ステップＳ－ＣＥ１で電子証明書発行リクエストを送信してきたノードに対し、自ノードの電子証明書を付加した電子証明書発行レスポンスを送信する（ステップＳ－ＣＥ２）。

【０１２４】

図６は、代表ノード動作を示すものである。

【０１２５】

図６において、ステップＳ－Ｄ１は、代表ノード動作時の初期状態である。この初期状態から、ノードリストを読み出し、他のノードに対し、ノードリストを付加したｋｅｅｐ　ａｌｉｖｅメッセージを送信し（ステップＳ－ＤＡ１）、初期状態（ステップＳ－Ｄ１）に戻る。

【０１２６】

次いで、初期状態（ステップＳ－Ｄ１）において、他のノードから、ノードリストが付加されたｋｅｅｐ　ａｌｉｖｅメッセージを受信する（ステップＳ－ＤＢ１）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。

【０１２７】

次いで、ステップＳ－ＤＢ１で受信したｋｅｅｐ　ａｌｉｖｅメッセージに付加されていたノードリストと自ノードが保存していたノードリストを比較し最新の情報に更新する（ステップＳ－ＤＢ２）。そして、ノードリストを読み出し、分散認証システムに参加するノード数が規定数ｍに達しているかどうかを確認する（ステップＳ－ＤＢ３）。

【０１２８】

その結果、分散認証システムに参加するノード数が規定数ｍに達していた場合（Ｙｅｓ）は、ノードリストを読み出し、代表ノードが離脱していないか確認し（ステップＳ－ＤＢ４）、代表ノードが離脱していた場合（Ｙｅｓ）、後述の代表ノード更新動作（ステップＳ－Ｇ１）に移行する。一方、代表ノードが離脱していなかった場合、初期状態（ステップＳ－Ｄ１）に移行する。

【０１２９】

一方、上記ステップＳ－ＤＢ３にて分散認証システムに参加するノード数が規定数ｍに達していなかった場合（Ｎｏ）は、前述の総意モード動作（ステップＳ－Ｂ１）に移行する。

【０１３０】

次いで、初期状態（ステップＳ－Ｄ１）において、代表ノードを離脱したい場合、他の代表ノードに対し、代表ノード離脱リクエストを送信する（ステップＳ－ＤＣ１）。そして、代表ノード離脱レスポンスを受信する（ステップＳ－ＤＣ２）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行し、後述の代表モード離脱動作（ステップＳ－Ｈ１）に移行する。

【０１３１】

次いで、初期状態（ステップＳ－Ｄ１）において、参加リクエストを受信する（ステップＳ－ＤＤ１）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は次のステップに移行する。

【０１３２】

次いで、参加リクエストを送信してきたノードに対し、参加レスポンスを送信し（ステップＳ－ＤＤ２）、参加リクエストを送信してきたノードの個人鍵の秘密鍵の素となる情報となるランダム素数を生成する（ステップＳ－ＤＤ３）。そして、ｍ台の代表ノード間で互いに連携し、参加リクエストを送信してきたノードの個人鍵の公開鍵を生成し（ステップＳ－ＤＤ４）、ｍ台の代表ノード間で互いに連携し、参加リクエストを送信してきたノードの電子証明書を生成する（ステップＳ－ＤＤ５）。

【０１３３】

次いで、ステップＳ－ＤＤ３で生成した参加リクエストを送信してきたノードの個人鍵の秘密鍵の素となる情報と、ステップＳ－ＤＤ４で生成した参加リクエストを送信してきたノードの個人鍵の公開鍵と、ステップＳ－ＤＤ５で生成した参加リクエストを送信してきたノードの電子証明書を、参加リクエストを送信してきたノードに対し送信し（ステップＳ－ＤＤ６）、初期状態（ステップＳ－Ｄ１）に移行する。

【０１３４】

次いで、初期状態（ステップＳ－Ｄ１）において、電子証明書生成リクエストを受信する（ステップＳ－ＤＥ１）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、前述のステップＳ－ＤＤ３に移行し、同様の処理を行う。

【０１３５】

次いで、初期状態（ステップＳ－Ｄ１）において、代表ノード離脱リクエストを受信する（ステップＳ－ＤＦ１）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行し、代表ノード離脱レスポンスを送信し（ステップＳ－ＤＦ２）、後述の代表ノード更新動作（ステップＳ－Ｇ１）に移行する。

【０１３６】

次いで、初期状態（ステップＳ－Ｄ１）において、代表ノード指名確認メッセージを受信する（ステップＳ－ＤＧ１）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行し、代表ノード指名確認レスポンスを送信し（ステ

ップＳ－ＤＧ２）、後述の代表ノード初期動作（ステップＳ－Ｆ１）に移行する。ステップＳ－ＤＧ１で受信した代表ノード指名確認メッセージに記載のノードを代表ノードにすることを拒否する場合は、その情報を代表ノード指名確認レスポンスに付加する。

【０１３７】

次いで、初期状態（ステップＳ－Ｄ１）において、電子証明書発行リクエストを受信する（ステップＳ－ＤＨ１）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行し、ステップＳ－ＤＨ１で電子証明書発行リクエストを送信してきたノードに対し、自ノードの電子証明書を付加した電子証明書発行レスポンスを送信し（ステップＳ－ＤＨ２）、初期状態（ステップＳ－Ｄ１）に移行する。

【０１３８】

次いで、初期状態（ステップＳ－Ｄ１）において、分散認証システム電子証明書発行リクエストを受信する（ステップＳ－ＤＩ１）。この時、受信したメッセージの正当性を確認する場合は、後述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行し、ステップＳ－ＤＩ１で分散認証システム電子証明書発行リクエストを送信してきたノードに対し、分散認証システム電子証明書を付加した分散認証システム電子証明書発行レスポンスを送信し（ステップＳ－ＤＩ２）、初期状態（ステップＳ－Ｄ１）に移行する。

【０１３９】

図７は、署名確認動作を示すものである。

【０１４０】

図７において、ステップＳ－Ｅ１は、署名確認動作の初期状態である。この初期状態から、メッセージを送信してきたノードに対し、メッセージ送信元のノードの電子証明書発行リクエストを送信する（ステップＳ－Ｅ３）。または、メッセージを送信してきたノードの電子証明書を分散認証システム上で分散して保存している場合は、適切なノードに対し、電子証明書発行リクエストを送信する。なお、本ステップは、メッセージを送信してきたノードの電子証明書を既に保持していた場合はスキップしてもよい。

【０１４１】

次いで、電子証明書発行レスポンスを受信する（ステップＳ－Ｅ４）。この時、受信したメッセージの正当性を確認する場合は、初期状態（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。なお、ステップＳ－Ｅ３をスキップしていた場合は、本ステップもスキップする。

【０１４２】

次いで、代表ノードに対し、分散認証システム電子証明書発行リクエストを送信する（ステップＳ－Ｅ５）。本ステップは、分散認証システム電子証明書を既に保持していた場合はスキップしてもよい。

【０１４３】

次いで、分散認証システム電子証明書発行レスポンスを受信する（ステップＳ－Ｅ６）。この時、受信したメッセージの正当性を確認する場合は、初期状態（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。ステップＳ－Ｅ５をスキップしていた場合は、本ステップもスキップする。

【０１４４】

次いで、分散認証システム電子証明書に付加されている代表鍵の公開鍵を用い、電子証明書に付加されている電子署名をその代表鍵の公開鍵で復号し、電子証明書の正当性を確認する（ステップＳ－Ｅ７）。さらに、受信したメッセージに付加されている電子署名を電子証明書に付加されている個人鍵の公開鍵で復号し、メッセージの正当性を確認する。

【０１４５】

図８は、代表ノード初期動作を示すものである。

【０１４６】

図８において、ステップＳ－Ｆ１は、代表ノード初期動作時の初期状態である。この初

期状態から、分散認証システムの代表鍵の秘密鍵の素となる情報となるランダム素数を生成し（ステップＳ－Ｆ２）、ｍ台の代表ノード間で互いに連携し、分散認証システムの代表鍵の公開鍵を生成する（ステップＳ－Ｆ３）。そして、この時点のノードリストに対し、個人鍵の秘密鍵を用いて電子署名をし（ステップＳ－Ｆ４）、他の代表ノードに対し、電子署名済みのノードリストを送信する（ステップＳ－Ｆ５）。

【０１４７】

次いで、他の代表ノードから、ノードリストを受信する（ステップＳ－Ｆ６）。この時、受信したメッセージの正当性を確認する場合は、前述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。

【０１４８】

次いで、ステップＳ－Ｆ６で受信したノードリストに全代表ノードの電子署名が付加されているか確認する（ステップＳ－Ｆ７）。その結果、ステップＳ－Ｆ６で受信したノードリストに全代表ノードの電子署名が付加されていた場合（Ｙｅｓ）、ステップＳ－Ｆ８に移行する。一方、ステップＳ－Ｆ６で受信したノードリストに全代表ノードの電子署名が付加されていなかった場合（Ｎｏ）、前述のステップＳ－Ｆ４に移行し、同様の処理を繰り返し実行する。

【０１４９】

上記ステップＳ－Ｆ７にて、ステップＳ－Ｆ６で受信したノードリストに全代表ノードの電子署名が付加されていた場合、全代表ノードによる電子署名が完了したノードリストを、残存する旧代表ノードに送信し（ステップＳ－Ｆ８）、残存する旧代表ノードによる電子署名が付加されたノードリストを受信する（ステップＳ－Ｆ９）。この時、受信したメッセージの正当性を確認する場合は、前述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。

【０１５０】

次いで、ステップＳ－Ｆ９で受信したノードリストに、残存する旧代表ノード全てによる電子署名が付加されているか確認する（ステップＳ－Ｆ１０）。その結果、ステップＳ－Ｆ９で受信したノードリストに全旧代表ノードの電子署名が付加されていた場合（Ｙｅｓ）、ｍ台の代表ノード間で互いに連携し、分散認証システム電子証明書を作成し（ステップＳ－Ｆ１１）、前述の代表ノード動作（ステップＳ－Ｄ１）に移行する。ステップＳ－Ｆ９で受信したノードリストに全代表ノードの電子署名が付加されていなかった場合（Ｎｏ）、前述のステップＳ－Ｆ８に移行し、同様の処理を繰り返し実行する。

【０１５１】

図９は、代表ノード更新動作を示すものである。

【０１５２】

図９において、ステップＳ－Ｇ１は、代表ノード更新動作時の初期状態である。この初期状態から、新たに代表ノードになるノードを選出し（ステップＳ－Ｇ２）、代表ノード指名確認メッセージを、他の代表ノードに送信する（ステップＳ－Ｇ３）。

【０１５３】

次いで、代表ノード指名確認レスポンスを受信する（ステップＳ－Ｇ４）。この時、受信したメッセージの正当性を確認する場合は、前述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。

【０１５４】

次いで、ステップＳ－Ｇ４で受信した代表ノード指名確認レスポンスに、ステップＳ－Ｇ２で選出したノードを拒否するメッセージが付加されているか確認する（ステップＳ－Ｇ５）。その結果、ステップＳ－Ｇ４で受信した代表ノード指名確認レスポンスに、ステップＳ－Ｇ２で選出したノードを拒否するメッセージが付加されていた場合（Ｙｅｓ）、初期状態（ステップＳ－Ｇ１）に移行する。

【０１５５】

一方、ステップＳ－Ｇ４で受信した代表ノード指名確認レスポンスに、ステップＳ－Ｇ

２で選出したノードを拒否するメッセージが付加されていなかった場合（Ｎｏ）、ステップＳ－Ｇ２で選出したノードに対し、代表ノード指名リクエストを送信する（ステップＳ－Ｇ６）。

【０１５６】

次いで、ステップＳ－Ｇ２で選出したノードから、代表ノード指名レスポンスを受信する（ステップＳ－Ｇ７）。この時、受信したメッセージの正当性を確認する場合は、前述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。

【０１５７】

次いで、ステップＳ－Ｇ７で受信した代表ノード指名レスポンスに、代表ノードになることを拒否するメッセージが付加されているか確認する（ステップＳ－Ｇ８）。その結果、ステップＳ－Ｇ７で受信した代表ノード指名レスポンスに、代表ノードになることを拒否するメッセージが付加されていた場合（Ｙｅｓ）、初期状態（ステップＳ－Ｇ１）に移行する。

【０１５８】

一方、ステップＳ－Ｇ７で受信した代表ノード指名レスポンスに、代表ノードになることを拒否するメッセージが付加されていなかった場合（Ｎｏ）、代表ノード数が規定数ｍに達しているかどうか確認する（ステップＳ－Ｇ９）。その結果、代表ノード数が規定数ｍに達していた場合（Ｙｅｓ）は、前述の代表ノード初期動作（ステップＳ－Ｆ１）に移行する。一方、代表ノード数が規定数ｍに達していなかった場合（Ｎｏ）は、初期状態（ステップＳ－Ｇ１）に移行する。

【０１５９】

図１０は、代表ノード離脱動作を示すものである。

【０１６０】

図１０において、ステップＳ－Ｈ１は、代表ノード離脱動作時の初期状態である。この状態のときは、代表ノードから旧代表ノードとして認知される。次いで、代表ノードから、全ての代表ノードの電子署名が付加されたノードリストを受信する（ステップＳ－Ｈ２）。この時、受信したメッセージの正当性を確認する場合は、前述の署名確認動作（ステップＳ－Ｅ１）に移行し、受信したメッセージの正当性が確認できた場合は、次のステップに移行する。

【０１６１】

次いで、ステップＳ－Ｇ２で受信したノードリストに、電子署名を付加し（ステップＳ－Ｈ３）、ステップＳ－Ｇ２で全ての代表ノードの電子署名が付加されたノードリストを送信してきた代表ノードに対し、ステップＳ－Ｇ３で電子署名を付加したノードリストを送信する（ステップＳ－Ｈ４）。

【０１６２】

次に、本実施例の効果について説明する。

【０１６３】

本実施例は、分散認証システムに参加するノードのうち規定数ｍ台のノードが代表ノードとなり、分散認証システムの代表鍵と分散認証システム電子証明書の発行、及び分散認証システムに参加するノードの個人鍵及び電子証明書の発行を、ｍ台の代表ノードが互いに連携することによって実現し、さらに代表ノードの指名・離脱を柔軟にすることによって、悪意のある攻撃者からの攻撃に対し、攻撃対象を分散させることができ、かつ攻撃されたとしても、代表ノードを次々と変化させることによって、分散認証システムとしての機能を失わずに、認証サービスを続けることができる。

【０１６４】

また、本実施例は、分散認証システムに参加するノードのうち規定数ｍ台のノードが代表ノードとなり、分散認証システムの代表鍵と分散認証システム電子証明書の発行、及び分散認証システムに参加するノードの個人鍵及び電子証明書の発行を、ｍ台の代表ノードが互いに連携することによって実現し、さらに代表ノードの指名・離脱を柔軟にすること

によって、ある特定の場所に認証局が存在する場合と同等の安全性を持った認証サービスを提供することができる。

【実施例２】

【０１６５】

次に、本発明の第２の実施例について図面を参照して詳細に説明する。

【０１６６】

図１１を参照すると、本実施例は、第１の実施例と同様に、受信部１と、モード管理部２と、一般ノード機能部３と、代表ノード機能部４と、共通機能部５と、ノード情報保存部８と、署名付加部６と、送信部７と、を有する。

【０１６７】

更に、本実施例は、分散認証システム用プログラムを有する。

【０１６８】

分散認証システム用プログラムは、受信部１と、モード管理部２と、一般ノード機能部３と、代表ノード機能部４と、共通機能部５と、ノード情報保存部８と、署名付加部６と、送信部７と、に読み込まれ受信部１と、モード管理部２と、一般ノード機能部３と、代表ノード機能部４と、共通機能部５と、ノード情報保存部８と、署名付加部６と、送信部７の動作を制御する。受信部１と、モード管理部２と、一般ノード機能部３と、代表ノード機能部４と、共通機能部５と、ノード情報保存部８と、署名付加部６と、送信部７は、分散認証システム用プログラムの制御により第１の実施例における分散認証システムによる処理と同一の処理を実行する。

【０１６９】

次に、本実施例の効果について説明する。

【０１７０】

本実施例では、第１の実施例の効果と同様の効果を得るために、分散認証システム用プログラムを用いることによりコンピュータを分散認証システムとして動作させることができる。

【０１７１】

以上、本発明の実施例を詳細に説明したが、本発明は、代表的に例示した上述の実施例に限定されるものではなく、当業者であれば、特許請求の範囲の記載内容に基づき、本発明の要旨を逸脱しない範囲内で種々の態様に変形、変更することができる。これらの変形例や変更例も本発明の権利範囲に属するものである。

【０１７２】

例えば、上記の分散認証システムを構成する各部の少なくとも一部の機能を、プログラムコードを用いて実現する場合、かかるプログラムコード及びこれを記録する記録媒体は、本発明の範疇に含まれる。この場合、オペレーティングシステム等の他のソフトウェアと共同して上記機能が実現される場合は、それらのプログラムコードも含まれる。

【図面の簡単な説明】

【０１７３】

【図１】本発明の第１の実施例に係る分散認証システムの全体構成を示すブロック図である。

【図２】本発明の第１の実施例に係る分散認証システムで用いる分散認証システム電子証明書の一例を示す図である。

【図３】本発明の第１の実施例に係る分散認証システムの動作を示す流れ図である。

【図４】本発明の第１の実施例に係る分散認証システムの総意モード動作を示す流れ図である。

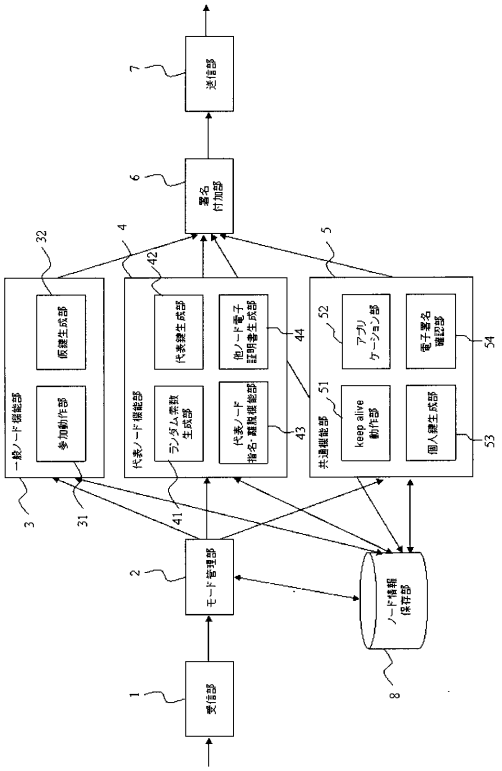
【図５】本発明の第１の実施例に係る分散認証システムの一般ノード動作を示す流れ図である。

【図６】本発明の第１の実施例に係る分散認証システムの代表ノード動作を示す流れ図である。

【図７】本発明の第１の実施例に係る分散認証システムの署名確認動作を示す流れ図であ

る。
【図８】本発明の第１の実施例に係る分散認証システムの代表ノード初期動作を示す流れ図である。
【図９】本発明の第１の実施例に係る分散認証システムの代表ノード更新動作を示す流れ図である。
【図１０】本発明の第１の実施例に係る分散認証システムの代表ノード離脱動作を示す流れ図である。
【図１１】本発明の第２の実施例に係る分散認証システムの全体構成を示すブロック図である。
【符号の説明】
【０１７４】
１　受信部
２　モード管理部
３　一般ノード機能部
４　代表ノード機能部
５　共通機能部
６　署名付加部
７　送信部
９　分散認証システム用プログラム
３１　参加動作部
３２　仮鍵生成部
４１　ランダム素数生成部
４２　代表鍵生成部
４３　代表ノード指名・離脱機能部
４４　他ノード電子証明書生成部
５１　ｋｅｅｐ　ａｌｉｖｅ動作部
５２　アプリケーション部
５３　個人鍵生成部
５４　電子署名確認部

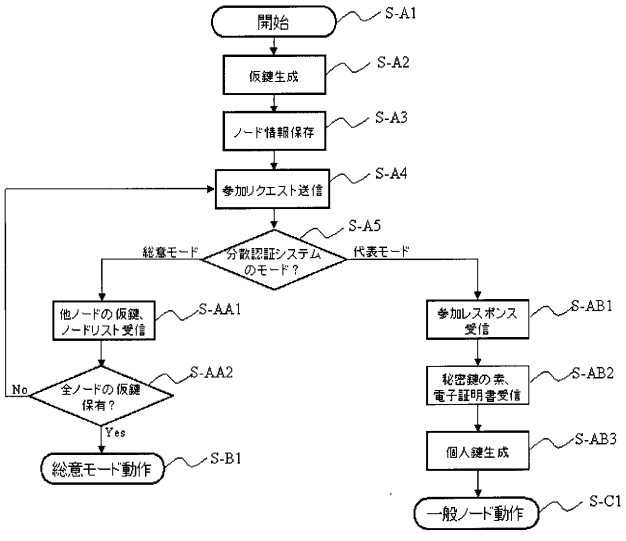
【図１】



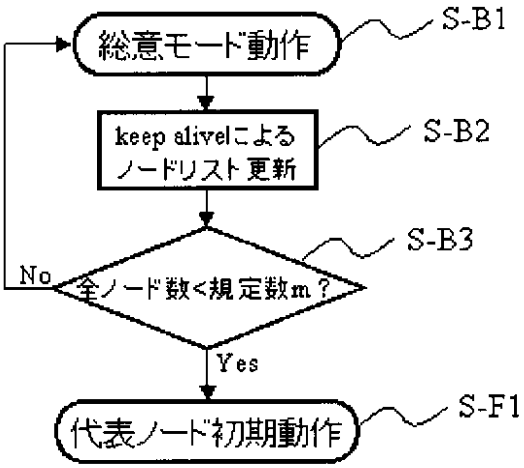
【図２】

参加ノード	ノード情報			代表ノード署名	旧代表ノード署名	代表鍵署名
	IPアドレス	ポート番号				
A				○	○	
C				○	○	
D					○	
E					○	
F				○		○
G				○		
H						
I						

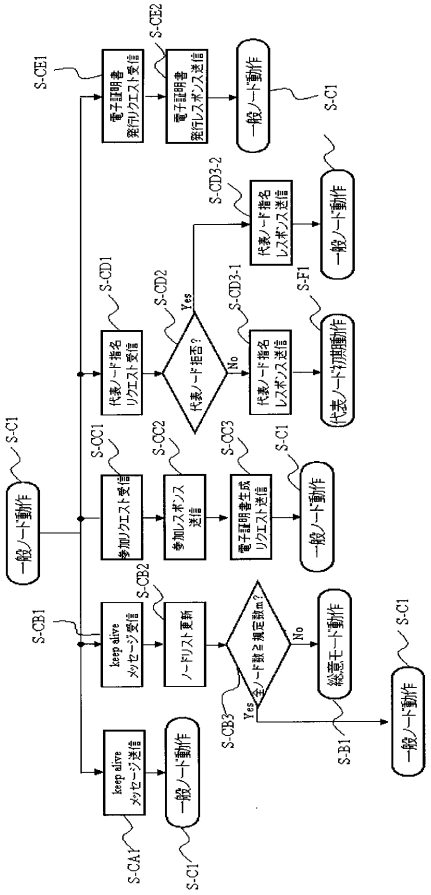
【図３】



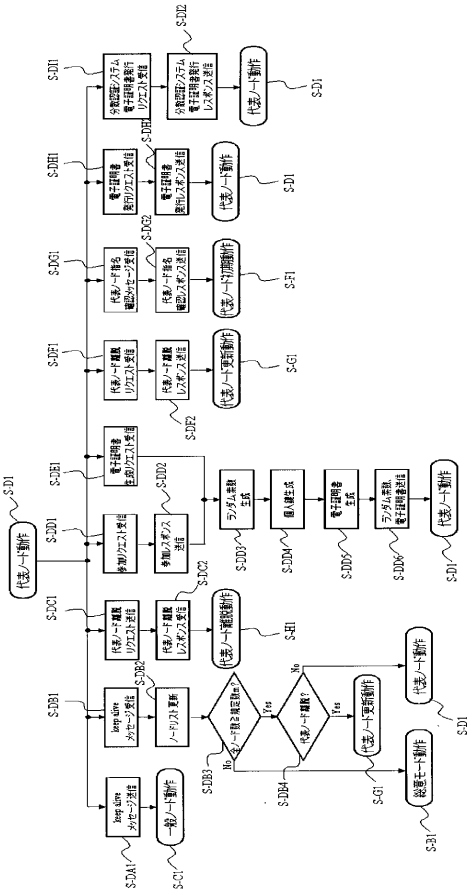
【図４】



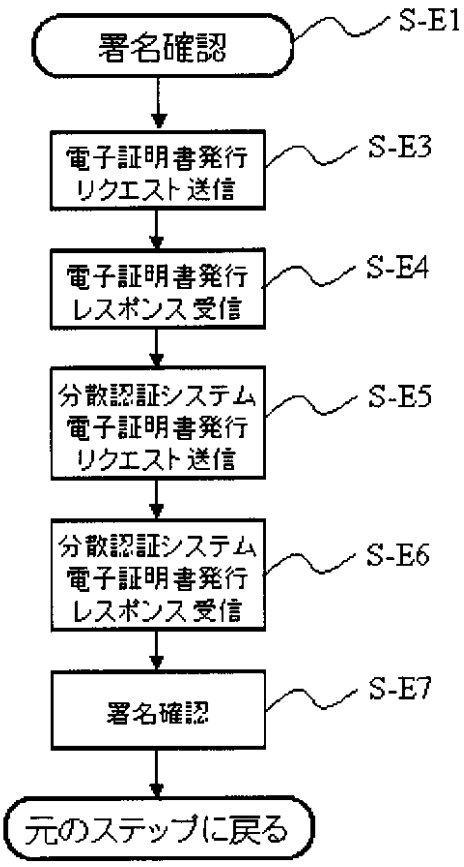
【図５】



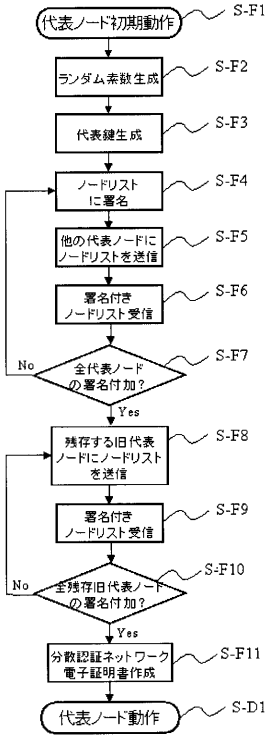
【図６】



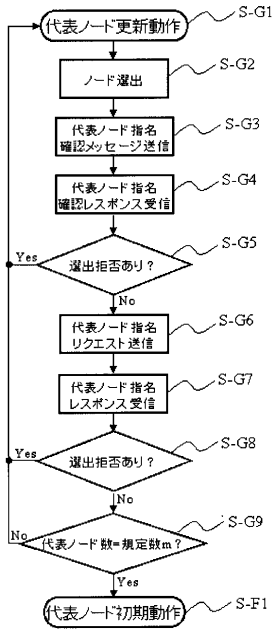
【図７】


署名確認
S-E1
電子証明書発行
リクエスト送信
S-E3
電子証明書発行
レスポンス受信
S-E4
分散認証システム
電子証明書発行
リクエスト送信
S-E5
分散認証システム
電子証明書発行
レスポンス受信
S-E6
署名確認
S-E7
元のステップに戻る

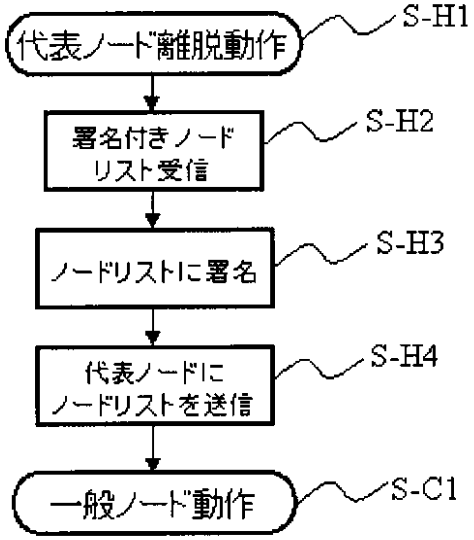
【図８】


代表ノード初期動作
S-F1
ランダム素数生成
S-F2
代表鍵生成
S-F3
ノードリスト
に署名
S-F4
他の代表ノードに
ノードリストを送信
S-F5
署名付き
ノードリスト受信
S-F6
全代表ノード
の署名付加?
S-F7
No
Yes
残存する旧代表
ノードにノードリスト
を送信
S-F8
署名付き
ノードリスト受信
S-F9
全残存旧代表ノード
の署名付加?
S-F10
No
Yes
分散認証ネットワーク
電子証明書作成
S-F11
代表ノード動作
S-D1

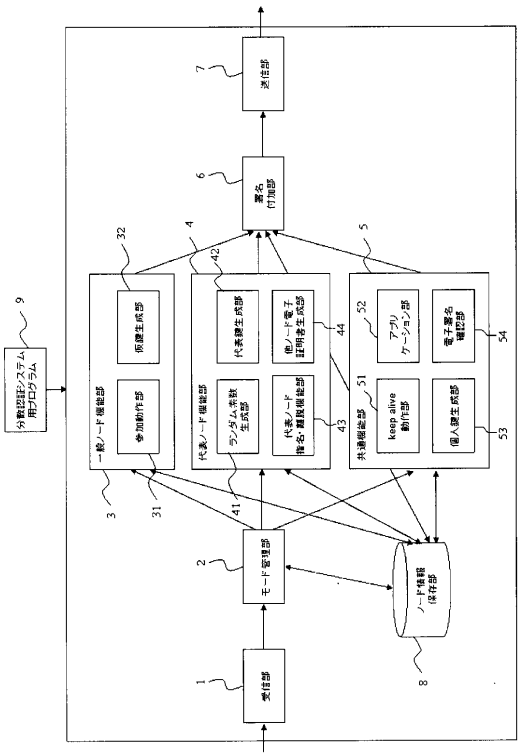
【図９】


代表ノード更新動作
S-G1
ノード選出
S-G2
代表ノード指名
確認メッセージ送信
S-G3
代表ノード指名
確認レスポンス受信
S-G4
Yes
離出拒否あり？
S-G5
No
代表ノード指名
リクエスト送信
S-G6
代表ノード指名
レスポンス受信
S-G7
Yes
離出拒否あり？
S-G8
No
No
代表ノード数=規定数m？
S-G9
Yes
代表ノード初期動作
S-F1

【図１０】


代表ノード離脱動作
S-H1
署名付きノード
リスト受信
S-H2
ノードリストに署名
S-H3
代表ノードに
ノードリストを送信
S-H4
一般ノード動作
S-C1

【図１１】


分散認証システム用プログラム
9
一般ノード機能部
仮選出部
参加動作部
代表ノード機能部
代表選出部
他ノード電子証明書生成部
ランダム数生成部
代表ノード署名検証機能部
共通機能部
アプリケーション部
電子署名確認部
keep alive動作部
個人鍵生成部
送信部
署名付加部
モード管理部
ノード情報保存部
受信部