

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4917748号

(P4917748)

(45) 発行日 平成24年4月18日 (2012. 4. 18)

(24) 登録日 平成24年2月3日 (2012. 2. 3)

(51) Int. Cl.	F I
G 0 6 F 21/20 (2006. 01)	G O 6 F 21/20 1 3 1 E
H 0 4 L 9/32 (2006. 01)	H O 4 L 9/00 6 7 5 A
	H O 4 L 9/00 6 7 3 D

請求項の数 26 (全 27 頁)

(21) 出願番号	特願2004-329654 (P2004-329654)	(73) 特許権者	500046438
(22) 出願日	平成16年11月12日 (2004. 11. 12)		マイクロソフト コーポレーション
(65) 公開番号	特開2005-149505 (P2005-149505A)		アメリカ合衆国 ワシントン州 9805
(43) 公開日	平成17年6月9日 (2005. 6. 9)		2-6399 レッドモンド ワン マイ
審査請求日	平成19年11月2日 (2007. 11. 2)		クロソフト ウェイ
(31) 優先権主張番号	60/520, 209	(74) 代理人	100077481
(32) 優先日	平成15年11月14日 (2003. 11. 14)		弁理士 谷 義一
(33) 優先権主張国	米国 (US)	(74) 代理人	100088915
(31) 優先権主張番号	10/888, 190		弁理士 阿部 和夫
(32) 優先日	平成16年7月9日 (2004. 7. 9)	(72) 発明者	クリスチャン アール. リーヒュー
(33) 優先権主張国	米国 (US)		アメリカ合衆国 98052 ワシントン
			州 レッドモンド ワン マイクロソフト
			ウェイ マイクロソフト コーポレーシ
			ョン内

最終頁に続く

(54) 【発明の名称】 ネットワークを介したセキュリティ保護された動的な資格証明書の配布

(57) 【特許請求の範囲】

【請求項 1】

第2の装置から第1の装置にネットワークを介してログオン資格証明書を自動的に配布するための方法であって、

前記第2の装置が、前記第1の装置から秘密を受信するステップと、

前記第2の装置が、前記第2の装置の少なくとも1つのリソースへのアクセス要求を前記第1の装置から前記ネットワークを介して受信するステップと、

前記要求に応答して、前記第2の装置が、前記第2の装置へのログオンに関連して使用される少なくとも1つのログオン資格証明書を生成して前記秘密に基づいて暗号化し、前記第2の装置への自動ログオンに使用するため、前記暗号化された少なくとも1つのログオン資格証明書を前記第1の装置に前記ネットワークを介して送信するステップと、

前記第2の装置が、前記暗号化された少なくとも1つのログオン資格証明書を保存するステップと、

前記第1の装置が、前記暗号化された少なくとも1つのログオン資格証明書を復号するステップと、

前記第1の装置が、前記少なくとも1つのログオン資格証明書を含むログオン要求を生成して暗号化するステップと、

前記第1の装置が、前記暗号化されたログオン要求を前記第2の装置に送信すると同時に、前記少なくとも1つのログオン資格証明書を消去するステップと、

前記第2の装置が、前記暗号化されたログオン要求を復号し、前記ログオン要求に含

10

20

れる前記少なくとも1つのログオン資格証明書の有効性を判定するステップと、

前記ログオン要求に含まれる前記少なくとも1つのログオン資格証明書が有効であると判定される場合、前記第2の装置が前記ログオン要求を受け入れるステップとを備えることを特徴とする方法。

【請求項2】

前記秘密は、前記第1の装置の公開鍵であることを特徴とする請求項1に記載の方法。

【請求項3】

前記少なくとも1つのログオン資格証明書を循環させるため、前記生成し送信するステップを周期的に実行することをさらに含むことを特徴とする請求項1に記載の方法。

【請求項4】

前記第1の装置にログイン成功の肯定応答を送信することをさらに含むことを特徴とする請求項1に記載の方法。

【請求項5】

請求項1に記載の方法を実行するためのコンピュータ実行可能命令を備えるコンピュータ可読記録媒体。

【請求項6】

請求項1に記載の方法を実行する手段を備えるコンピュータ装置。

【請求項7】

第1の装置が、ネットワークを介して第2の装置にログオンする目的で、前記第2の装置からログオン資格証明書を自動的に取得するための方法であって、

前記第1の装置が、前記第2の装置に秘密を送付するステップと、

前記第1の装置が、前記ネットワークを介して前記第2の装置の少なくとも1つのリソースへのアクセスを要求するステップと、

前記要求に応答して、前記第1の装置が、前記第2の装置へのログオンに関連して使用される少なくとも1つのログオン資格証明書を前記第2の装置から受信するステップであって、前記少なくとも1つのログオン資格証明書は、前記第2の装置から受信する前に、前記第2の装置によって前記秘密を使用して暗号化されている、ステップと、

前記第1の装置が、前記暗号化された少なくとも1つのログオン資格証明書を復号するステップと、

前記第1の装置が、前記少なくとも1つのログオン資格証明書を含むログオン要求を生成して暗号化するステップと、

前記第1の装置が、前記暗号化されたログオン要求を前記第2の装置に送信すると同時に、前記少なくとも1つのログオン資格証明書を消去するステップと

を備えることを特徴とする方法。

【請求項8】

前記秘密は、前記第1の装置の公開鍵であることを特徴とする請求項7に記載の方法。

【請求項9】

前記少なくとも1つのログオン資格証明書を循環させるため、新しい少なくとも1つのログオン資格証明書を周期的に受信することをさらに含むことを特徴とする請求項7に記載の方法。

【請求項10】

前記復号するステップは、前記秘密に基づいて前記少なくとも1つのログオン資格証明書を復号することを特徴とする請求項7に記載の方法。

【請求項11】

前記復号するステップは、前記公開鍵に一意に対応する秘密鍵に基づいて前記少なくとも1つのログオン資格証明書を復号することを特徴とする請求項8に記載の方法。

【請求項12】

前記送信に응答して、ログイン成功の肯定応答を受信することをさらに含むことを特徴とする請求項7に記載の方法。

【請求項13】

10

20

30

40

50

請求項7に記載の方法を実行するためのコンピュータ実行可能命令を備えるコンピュータ可読記録媒体。

【請求項14】

請求項7に記載の方法を実行する手段を備えるコンピュータ装置。

【請求項15】

ネットワークを介してホスト装置にログオンする目的で、前記ホスト装置からログオン資格証明書を自動的に取得するクライアント装置であって、

前記ホスト装置に秘密を送付する第1のコンポーネントと、

前記ネットワークを介して前記ホスト装置の少なくとも1つのリソースへのアクセスを要求する第2のコンポーネントと、

前記第2のコンポーネントによる要求に応答して、前記ホスト装置へのログオンに関連して使用される、前記秘密を使用して暗号化された少なくとも1つのログオン資格証明書を前記ホスト装置から受信し、前記暗号化された少なくとも1つのログオン資格証明書を復号し、前記少なくとも1つのログオン資格証明書を含むログオン要求を生成して暗号化し、前記ホスト装置に前記暗号化されたログオン要求を送信すると同時に、前記少なくとも1つのログオン資格証明書を消去する第3のコンポーネントと

を備えることを特徴とするクライアント装置。

【請求項16】

前記秘密は、前記クライアント装置の公開鍵であることを特徴とする請求項15に記載のクライアント装置。

【請求項17】

前記第3のコンポーネントは、前記少なくとも1つのログオン資格証明書を循環させるため、新しい少なくとも1つのログオン資格証明書を周期的に受信することを特徴とする請求項15に記載のクライアント装置。

【請求項18】

前記第3のコンポーネントは、前記秘密に基づいて前記少なくとも1つのログオン資格証明書を復号することを特徴とする請求項15に記載のクライアント装置。

【請求項19】

前記第3のコンポーネントは、前記公開鍵に一意に対応する秘密鍵に基づいて前記少なくとも1つのログオン資格証明書を復号することを特徴とする請求項16に記載のクライアント装置。

【請求項20】

前記第3のコンポーネントはさらに、前記ログオン要求に応答して、ログイン成功の肯定応答を受信することを特徴とする請求項15に記載のクライアント装置。

【請求項21】

第1の装置が第2の装置からネットワークを介してログオン資格証明書を自動的に取得するためのコンピュータ実行可能命令を有するコンピュータ実行可能モジュールを備えるコンピュータ可読記録媒体であって、前記モジュールが、

前記第2の装置に秘密を送付する手段と、

前記ネットワークを介して前記第2の装置の少なくとも1つのリソースへのアクセスを要求する手段と、

前記要求する手段によって行われたアクセス要求に応答して、前記第2の装置へのログオンに関連して使用される少なくとも1つのログオン資格証明書を前記第2の装置から受信する手段であって、前記少なくとも1つのログオン資格証明書は、前記第2の装置から受信する前に、前記第2の装置によって前記秘密を使用して暗号化されている、手段と、

前記暗号化された少なくとも1つのログオン資格証明書を復号する手段と、

前記少なくとも1つのログオン資格証明書を含むログオン要求を生成して暗号化し、前記暗号化されたログオン要求を前記第2の装置に送信すると同時に、前記少なくとも1つのログオン資格証明書を消去する手段と

を備えることを特徴とするコンピュータ可読記録媒体。

10

20

30

40

50

【請求項 2 2】

前記秘密は、前記第 1 の装置の公開鍵であることを特徴とする請求項 2 1 に記載のコンピュータ可読記録媒体。

【請求項 2 3】

前記受信する手段は、前記少なくとも 1 つのログオン資格証明書を循環させるため、新しい少なくとも 1 つのログオン資格証明書を周期的に受信することを特徴とする請求項 2 1 に記載のコンピュータ可読記録媒体。

【請求項 2 4】

前記復号する手段は、前記秘密に基づいて前記少なくとも 1 つのログオン資格証明書を復号することを特徴とする請求項 2 1 に記載のコンピュータ可読記録媒体。

10

【請求項 2 5】

前記復号する手段は、前記公開鍵に一意に対応する秘密鍵に基づいて前記少なくとも 1 つのログオン資格証明書を復号することを特徴とする請求項 2 2 に記載のコンピュータ可読記録媒体。

【請求項 2 6】

前記ログオン要求に応答して、ログイン成功の肯定応答を受信する手段をさらに含むことを特徴とする請求項 2 1 に記載のコンピュータ可読記録媒体。

【発明の詳細な説明】

【技術分野】

【0 0 0 1】

20

本発明は、コンピューティング・システムのネットワークを介する、第 1 のコンピューティング装置から第 2 のコンピューティング装置への、資格証明書のセキュリティ保護された動的な配布 (secure and dynamic distribution of credential) に関する。より詳細には、本発明は、たとえば、第 2 の装置で資格証明書を露呈すること (exposing) または保存することなく、第 2 の装置で自動ログインを行うためのログイン資格証明書 (login credential) を、第 1 の装置から第 2 の装置に、セキュリティ保護して動的に配布する方法に関する。

【背景技術】

【0 0 0 2】

第 1 のコンピューティング装置が、第 2 の装置を識別するため、かつ／または第 2 の装置に対するアクセス・レベルおよび許可を決定するため、第 2 のコンピューティング装置から、ユーザ識別情報およびパスワードなどの資格証明書を受信すること（または上記の逆のこと）が望ましいのには、多くの理由がある。

30

【0 0 0 3】

たとえば、ホスト・コンピュータは、クライアント装置がアクセスを要求したいと望むコンテンツを有することがある。これはごく一般的なシナリオであり、図 1 A に図示するように、コンピューティング装置と、様々な別のコンピューティング装置から要求され得る各種コンテンツとからなる世界は、メディア装置およびメディア・タイプの両方に関して、きわめて多様である。図 1 A は、例示的な目的でのみ、音楽 (MP 3、WMV など)、ストリーミング・オーディオ／ビデオ、静止画 (J P E G S、G I F など)、動画ファイル (M O V、M P E G など)、広告、放送メディア (ラジオ、T V、ケーブルなど)、グラフィックス・データなどの多くの種類のメディアが存在していることを、示している。また、図 1 A は、限定しないが、テレビ、ラジオ、チューナ、DVD プレーヤ、V C R、デジタル・データ記憶および／または再生装置、MP 3 プレーヤ、スマート・ディスプレイ装置、ラップトップ、ゲーム機、リモート制御装置、セル電話、P D A、デジタル・ピクチャー・フレームなど、を含む何らかの目的のため何らかの方式でメディアを再生する多様な装置が存在することも、示している。したがって、このようなシステム内の任意の 2 つの装置間で信頼 (trust) を確立することは、様々なコンピューティング装置間で、コンテンツ提供装置のコンテンツまたはリソースを安全に共用することを可能として、これらのコンテンツ提供装置のコンテンツまたはリソースを、ネットワーク接続された信

40

50

頼可能な装置の飛び地 (networked trust enclave of devices) とする上で、重要な問題となる。

【0004】

したがって、第1のコンピューティング装置のリソースにアクセスすることを第2のコンピューティング装置に対して許可するには、たとえば、セキュリティ上および／またはプライバシー上の理由から、第1のコンピューティング装置に第2のコンピューティング装置に関する何かを「信頼 (trust)」させるようにするのがしばしば望ましい。アクセスを許可する一般的な1つの方法は、要求装置から資格証明書を受信することである。この資格証明書は、提供装置によって受信された場合、ドアの錠に対する鍵のようにふるまい、信頼を確立する。そのような資格証明書が、ピア・ツー・ピア・クライアントを含むネットワーク構成、分散コンピューティング・システム、アプリケーションの処理は主として中央サーバ上で実行されるがさらに分散させることも可能なシン・クライアント構成、および以下で詳しく説明するようなその他のネットワーク接続環境など、任意のコンピューティング環境内の2つのコンピューティング装置間で交換され得ることは理解できるであろう。

【0005】

図1Bには、第1のコンピューティング装置 (例えば、サーバS) と第2のコンピューティング装置 (例えば、クライアントC) が有線または無線による任意のネットワーク・コネクションNCを介して通信を行う例示的なネットワーク接続環境における、サーバSとクライアントCの間の典型的な従来技術によるログオンが図示されている。認証交換は、様々な理由から、2つの装置間で発生し得る。原型的なシナリオでは、クライアントCは、アプリケーション、コンテンツ、サービスなど、サーバSの何らかのリソースにアクセスしたいと望むか、またはサーバSとのセッションを開始したいと望む。サーバSは、アプリケーション、コンテンツ、サービスなどへのアクセスを許可する前に、クライアントCがサーバSのアプリケーション、サービス、コンテンツなどへのアクセスを許可されていることの何らかの証拠 (proof) を必要とする。これには、ユーザ識別情報およびパスワードなどの資格証明書をクライアントCから受信することが含まれ得る。

【0006】

今日、このようなシナリオにおいて、コンピュータSの外部オブジェクトがネットワークNCを介してコンピュータSにログインを試みる場合、外部オブジェクトは、クライアントCとサーバSが知っている標準的な機構を用いて、認証用の資格証明書を提示する。資格証明書ログイン・コンポーネントは、クライアントCからサーバSに資格証明書を送達し、サーバS上の認証コンポーネントは、クライアントCの資格証明書が表す許可に従って、リソースへのアクセスを許可する。一般に、ログインを希望するのは人間としてのユーザであり、資格証明書は通常はそのユーザ自身が記憶している。ユーザは、たとえば、ログイン時にキーボードなどの入力装置を介して資格証明書を入力するなど、外部機構を介してコンピューティング装置Cに資格証明書を手動で入力する。従来技術による別のシステムでは、ユーザが一度だけ資格証明書を入力すれば、それ以降、資格証明書をクライアントCにキャッシュまたはその他の方法で保存しておくことができる (たとえば、図1Bの「creds」)。それとは関係なく、資格証明書のクライアントCへの最初の転送は、ネットワークNCの「帯域外 (out-of-band)」で行われる。

【0007】

しかし、外部オブジェクトが自動的な方法でログインすることを望むマシンである場合 (すなわち、人間としてのユーザではない場合)、マシンは現在のところ、いずれかの場所から資格証明書を取得しなければならず、これも通常は、クライアントCに資格証明書を入力するための帯域外機構によって、ネットワークの「帯域外」で転送される。上述したように、このようにする主な理由は、装置間で信頼を確立するためである。クライアントCが、何らかの外部の帯域外ソースから唯一サーバSだけが知っている秘密 (secret) を知ったとすれば、その場合、クライアントCは、装置間で通信交換するネットワークNCの信頼されたユーザであると仮定することができる。

【0008】

【非特許文献1】Chang, c. c. et al., "Using Smart Cards to Authenticate Remote Passwords," Computers & Math. Applic., 1993, 26(7) 19-27

【非特許文献2】Kornievskaia, O. et al., "Kerberized Credential Translation: A Solution to web Access Control," Proceedings of the 10th USENIX Security Symposium, Washington, DC, August 13-17, 2001, 235-249

【非特許文献3】Sandirigama, M. et al., "Simple and Secure Password authentication Protocol (SAS)," IEICE Trans. Commun., 2000, E83B(6), 1363-1365

【非特許文献4】Wang, B, et al., "Cryptanalysis of an Enhanced Timestamp-Based Password Authentication Scheme," Computers & Security, 2003, 22(7), 643-645

【非特許文献5】Wu, T.C. et al., "Authentication Password Over an Insecure Channel," Computers & Security, 1996, 15(5), 431-439

【非特許文献6】Yeh, H.T. et al., "Security of a Remote User Authentication Scheme Using Smart Cards," IEICE Trans. Commun., 2004, E87B(1), 192-194

【非特許文献7】Yeh, T.C. et al., "A Secure One-Time Password Authentication Scheme Using Smart Cards," IEICE Trans. Commun., 2002, E85B(11), 2515-2518

【発明の開示】

【発明が解決しようとする課題】

【0009】

しかし、2つの装置間で信頼がすでに確立されている場合、従来技術による上述のログイン・システムのセキュリティを問題であるとして取り上げる少なくとも2つの理由、すなわち、(1) 辞書攻撃に対する脆弱性 (vulnerability to dictionary attack)、および(2) クライアント・マシンに保存された資格証明書が露顕する脅威、が存在する。

【0010】

辞書攻撃の脅威に関して、悪意ある外部オブジェクトは、資格証明書の入力として可能なあらゆる入力の組合せおよび順列 (permutation) を繰り返し、総当たりに試みることができ、その結果、長い時間をかければ、強力な数の法則 (the law of strong numbers) から、手当たり次第であるにしる資格証明書を推測することができる。辞書攻撃をかわすため、資格証明書を循環させる、すなわち、頻繁に変更することができる。しかし、資格証明書をあまり頻繁に循環させると、ユーザが資格証明書を覚えておくことが難しくなる。一方、資格証明書を十分頻繁に循環させないと、辞書攻撃の脅威は軽減されない。

【0011】

第2の懸念は、そのようなシステムでは、資格証明書がある期間クライアントC上に保存またはキャッシュされる傾向にあることであり、このことはサーバSのリソースを危険にさらす。悪意あるハッカー (hacker) がそのオブジェクトをクライアントC上でそれらの存在を露呈する (expose) 方法を割り出した場合、サーバSのリソースは露呈されることになる。ハッカーが資格証明書を別のユーザおよび装置と共用している場合、問題はさらに悪化する。このリスクは、資格証明書を循環させてもさせなくても、ログインの際に資格証明書の入力に関与するのが人間としてのユーザであってもマシンであっても、存続し続ける。サーバSの側から見ると、これが問題となるのは、サーバのリソースに対するセキュリティ・リスクが、サーバのストレージの範囲内にもはや局所化されなくなるためである。

【0012】

しかし、装置間で信頼がすでに確立されている場合、資格証明書を頻繁に循環でき、クライアント・マシン上に資格証明書を保存しない方法によって、自動ログイン用のログイン直前に資格証明書をクライアントに動的に配布する方法があるべきである。

【0013】

したがって、実際にログインする直前に、そこにログインまたはアクセスしたいと望まれているコンピュータによって、ログイン資格証明書を、ネットワークを介して自動的に配布するための方法があることが望ましい。辞書攻撃の脅威にさらされない方法、または

資格証明書を取り出そうとクライアントCのストレージを局所的にスヌーピングされない方法で、そうした資格証明書に基づいて、次に2台のコンピューティング装置間で認証交換を行うための方法があることが望ましい。さらに、その後のログイン交換(login exchange)が行われるのと同じネットワークを介して、第1の装置が第2の装置に安全に資格証明書を示し、または配布するための汎用的で簡単な機構またはフレームワークがあることが望ましい。

【課題を解決するための手段】

【0014】

上述した従来技術の短所に鑑み、本発明は、ネットワークを介して、資格証明書のセキュリティ保護された動的な配布を行うためのシステムおよび方法を提供する。様々な実施形態において、本発明は、ログインが行われる前に、そこにログインまたはアクセスしたいと望まれているコンピュータによって、ログオン資格証明書を、ネットワークを介して自動的に要求側に配布するためのシステムおよび方法を提供する。例示的な実施形態においては、ログオン資格証明書が要求側には保存されないように、既存の信頼に基づいて、コンピュータが、ログオン資格証明書を自己生成し、それを要求側に自己配布する。

【0015】

本発明のその他の利点および特徴を以下で説明する。

本発明による資格証明書のセキュリティ保護された動的な配布を行うためのシステムおよび方法について、添付の図面を参照しながらさらに説明する。

【発明を実施するための最良の形態】

【0016】

概要

第2のコンピューティング装置がデジタル・コンテンツを求める要求をする場合、第2のコンピューティング装置が、第1のコンピューティング装置によって動的に生成され、セキュリティ保護を施されて配布される資格証明書を、自動的に受信したいと望む場合の一例である。そのようなデジタル・コンテンツを求める要求は、ウェブ・サービスおよびモバイル・ウェブ・サービスの出現によって増加を続けるであろう。すでに、ネットワーク接続された装置の広範なエコ・システム(ecosystem)が、(TV、音楽、ビデオ、写真、DVDなどの)娯楽体験を(電子ホーム・リモート・メディア装置(electronic home remote media device)、スマート・ディスプレイ、xBox、ポケットPC、ポータブルDVD装置、その他などの)多様なメディアによって家庭に配給する世界に導入されている。しかし、このようなコンテンツを要求コンピューティング装置に配給できるようにする前に、資格証明書の交換が、とりわけ、要求装置を認証するために、要求装置とコンテンツを保有する装置との間で行われる。上述したように、従来技術によるログイン技法には、それに付随するリスクが存在する。本発明は、装置間ですでに信頼が確立されている場合には、そのようなリスクを回避できることを認識している。したがって、本発明は、要求装置がネットワークを介してログインを行う直前に、簡単な方式で資格証明書を、ネットワークを介して要求装置に自動的に配布するための汎用的なフレームワークを提供する。

【0017】

例示的なネットワーク接続環境

コンピュータ・ネットワークの一部として配置できる、または分散コンピューティング環境内に配置できる任意のコンピュータまたはその他のクライアントもしくはサーバ装置の関連において、本発明を実装できることは、当業者であれば理解できよう。この点で、本発明は、本発明による資格証明書のセキュリティ保護された動的な配布に関連して利用できる、任意の数のメモリまたはストレージ・ユニットを有し、また任意の数のストレージ・ユニットまたはボリュームにわたって存在する任意の数のアプリケーションおよびプロセスを有する、任意のコンピュータ・システムまたは環境に関連する。本発明は、リモートまたはローカル・ストレージを有する、ネットワーク環境または分散コンピューティング環境に配置されたサーバ・コンピュータおよびクライアント・コンピュータを有する

環境に適用することができる。本発明はまた、リモートまたはローカル・サービスに関連する情報を生成し、受信し、送信するための、プログラミング言語機能、解釈および実行能力を有する、スタンド・アロン・コンピューティング装置にも適用することができる。デジタル・メディア用のネットワーク・ソースがこれまで以上に増加していることから、本発明は特に、ネットワークまたは分散コンピューティング環境で動作するコンピューティング装置に関連し、したがって、本発明による資格証明書のセキュリティ保護された動的な配布を行う技法は、そうした環境で非常に効果的に利用することができる。

【0018】

分散コンピューティングは、コンピューティング装置およびシステムの間で、交換によるコンピュータ・リソースおよびサービスの共用を提供する。これらのリソースおよびサービスには、情報交換、ファイル用のキャッシュ・ストレージおよびディスク・ストレージが含まれる。分散コンピューティングは、ネットワーク接続性（network connectivity）を利用して、クライアントがその集団的な処理能力（collective power）およびストレージを企業全体の利益になるように活用できるようにする。この点で、多様な装置は、本発明により達成できるような、ログイン直前に行われる資格証明書の動的な要求および配送に関連する、アプリケーション、オブジェクト、またはリソースを有することができる。

10

【0019】

図2Aには、例示的なネットワーク化された、または分散されたコンピューティング環境の概略図が示されている。分散コンピューティング環境は、コンピューティング・オブジェクト（computing object）10a、10bなど、およびコンピューティング・オブジェクトまたは装置110a、110b、110cなどを含む。これらのコンピューティング・オブジェクトは、プログラム、メソッド、データ・ストア、プログラマブル・ロジックなどを含むことができる。コンピューティング・オブジェクトは、PDA、オーディオ／ビデオ装置、MP3プレーヤ、TV、パーソナル・コンピュータなど、同じまたは異なる装置の部分を含むことができる。各コンピューティング・オブジェクトは、通信ネットワーク14を介して、別のコンピューティング・オブジェクトと通信を行うことができる。このネットワーク自体が、図2Aのシステムにサービスを提供するその他のコンピューティング・オブジェクトおよびコンピューティング装置を含むことができ、複数の相互接続されたネットワークを表すことができる。本発明の一態様によれば、各コンピューティング・オブジェクト10a、10bなど、または110a、110b、110cなどは、本発明による処理を要求しまたは利用するため、APIまたはその他のオブジェクトなどのインターフェース、ソフトウェア、ファーム・ウェア、および／またはハードウェアを利用するアプリケーションを含むことができる。

20

30

【0020】

110cなどのコンピューティング・オブジェクトが、別のコンピューティング装置10a、10bなど、または110a、110bなどによってホストされ得ることも理解できるであろう。したがって、図示された物理的環境には、コンピュータとして接続された装置が示されているが、そのような図は、単に例示的なものに過ぎず、代替的に、物理的環境は、PDA、テレビ、MP3プレーヤなどの様々なデジタル装置、インターフェース、COMオブジェクトなどのソフトウェア・オブジェクト、またはメディア体験に関連して利用できる任意の装置を含むものとして、図示し、または説明することもできる。

40

【0021】

分散コンピューティング環境をサポートする、多様なシステム、コンポーネント、およびネットワーク構成が存在する。たとえば、コンピューティング・システムは、ローカル・ネットワークまたは広域分散ネットワークによって、有線または無線システムによって、接続することができる。現在、ネットワークの多くはインターネットに結合され、インターネットは、広域分散コンピューティングの基盤を提供し、多くの異なるネットワークを包含している。どのような基盤も、本発明による資格証明書のセキュリティ保護された動的な配布を起こさせる例示的な通信のために使用することができる。

50

【0022】

ホームネット・ワーキング環境では、電源線、データ（無線および有線）、音声（例えば、電話）、および娯楽メディアなど、それぞれ固有のプロトコルをサポートすることができる少なくとも4種類の本質的に異なるネットワーク・トランスポート・メディア（network transport media）が存在する。電灯スイッチなどの家庭内制御装置や家電製品の大部分は、接続性を得るために電源線を使用することができる。データ・サービスは、ブロード・バンド（例えば、DSLまたはケーブル・モデム）として、家庭に入り込むことができ、無線（たとえば、HomeRFまたは802.11B）または有線（たとえば、HomePNA、Cat5、イーサネット（登録商標）、さらには電源線）接続性を使用して、家庭内からアクセス可能である。音声トラフィックは、有線（例えば、Cat3）または無線（例えば、セル電話）として、家庭内に入り込むことができ、Cat3対応の有線を用いて、家庭内に配信することができる。娯楽メディアまたはその他のグラフィカル・データは、衛星またはケーブルを介して家庭に入り込むことができ、一般には同軸ケーブルを用いて、家庭内に配信することができる。IEEE1394およびDVIも、メディア装置のクラスタのためのデジタル相互接続である。このようなネットワーク環境とプロトコル規格として出現し得るその他のネットワーク環境はすべて、イントラネットなどのネットワークを形成するため、相互接続することができ、それらは、インターネットによって外部世界と接続される可能性がある。要するに、データの保存および送信のために様々な種類の異なるソースが存在し、その結果、この先、コンピューティング装置は、本発明による資格証明書のセキュリティ保護された動的な配布を行う処理を要求しまたは利用するプログラム・オブジェクトに付随してアクセスされ、または利用されるデータ、などのデータを共用するための方法を必要とする。

10

20

【0023】

インターネットとは一般に、コンピュータ・ネットワークの技術分野でよく知られているTCP/IPをプロトコルに利用する、ネットワークおよびゲートウェイの集団のことである。TCP/IPは、「Transmission Control Protocol/Internet Protocol（伝送制御プロトコル／インターネット・プロトコル）」の頭字語である。インターネットは、ユーザがネットワークを介して対話し、情報を共有できるようにする、ネット・ワーキング・プロトコルを実行するコンピュータによって相互接続された、地理的に分散したリモート・コンピュータ・ネットワークのシステムとして説明することができる。そのように広域に分散した情報を共有するので、インターネットなどのリモート・ネットワークは、これまでは概ね、専門的な動作またはサービスを実行するためのソフト・ウェア・アプリケーションを開発者が基本的には制約なしに設計できるオープン・システムへと発展してきた。

30

【0024】

したがって、ネットワーク基盤では、クライアント／サーバ、ピア・ツー・ピア、またはハイブリッド構成など、多くのネットワーク・トポロジが可能である。「クライアント」とは、関係性がない別のクラスまたはグループによるサービスを利用する、クラスまたはグループのメンバのことである。したがって、コンピューティング処理において、クライアントは、別のプログラムによって提供されるサービスを要求するプロセス、すなわち、大まかに言って、1組の命令またはタスクである。クライアント・プロセスは、別のプログラムまたはサービス自体が行う作業の詳細については一切「知る」必要なく、要求したサービスを利用する。クライアント／サーバ・アーキテクチャ、特にネットワーク化されたシステムでは、クライアントは通常、別のコンピュータ、たとえば、サーバによって提供される共有ネットワーク・リソースにアクセスするコンピュータである。図2Aの例では、コンピュータ110a、110bなどは、クライアントと考えることができ、コンピュータ10a、10bなどは、クライアント・コンピュータ110a、110bなどに複製されるデータを保管するサーバ10a、10bなどと考えることができるが、コンピュータはどれも、状況に応じて、クライアント、サーバ、またはその両方と見なすことができる。たとえば、コンピュータ110aは、Media Center Editio

40

50

n (MCE) ホストPCとすることができ、コンピューティング装置10a、10bなどは、リモート・メディア消費装置 (remote media consumption device) とすることができる。これらのコンピューティング装置はどれも、または本発明による資格証明書のセキュリティ保護された動的な配布を行う技法に関連するデータを処理すること、あるいは、これらに関連するサービスもしくはタスクを要求すること、ができる。

【0025】

サーバは一般に、インターネットなどのリモート・ネットワークまたはローカル・ネットワークを介してアクセス可能な、リモート・コンピュータ・システムである。クライアント・プロセスは、第1のコンピュータ・システムで動作させることができ、サーバ・プロセスは、第2のコンピュータ・システムで動作させることができ、通信媒体を介して互いに通信を行い、その結果、分散機能を提供し、複数のクライアントがサーバの情報収集能力を利用できるようにする。本発明の技法に従って利用されるソフトウェア・オブジェクトはいずれも、複数のコンピューティング装置またはコンピューティング・オブジェクトにわたって分散させることができる。

10

【0026】

クライアントおよびサーバは、プロトコル層によって提供される機能を利用して、互いに通信を行う。たとえば、ハイパー・テキスト転送プロトコル (HTTP) は、ワールド・ワイド・ウェブ (WWW) または「ウェブ」と併せて使用される共通プロトコルである。たとえば、リモート・デスクトップ・プロトコル (RDP) は、リモート・コンピューティング用に利用される共通プロトコルである。一般に、インターネット・プロトコル (IP) アドレスなどのコンピュータ・ネットワーク・アドレス、またはユニバーサル・リソー・スロケータ (URL) などのその他のリファレンスは、サーバまたはクライアント・コンピュータを互いに識別するために使用することができる。ネットワーク・アドレスは、URLアドレスと呼ばれることもある。通信は、通信媒体を介して提供することができる、たとえば、クライアントとサーバは、大容量通信用のTCP/IPコネクションを介して互いに結合することができる。

20

【0027】

したがって、図2Aには、本発明を実施できる、ネットワーク/バスを介してクライアント・コンピュータと通信を行うサーバを有する、例示的なネットワーク接続または分散環境が図示されている。より詳細には、本発明によれば、複数のサーバ10a、10bなどは、LAN、WAN、イントラネット、インターネットなどとすることができる通信ネットワーク/バス14を介して、ポータブル・コンピュータ、ハンドヘルド・コンピュータ、シン・クライアント、ネットワーク接続機器、またはVCR、TV、オーブン、照明、ヒータといったその他の装置などの複数のクライアントまたはリモート・コンピューティング装置110a、110b、110c、110d、110eなどと相互接続される。したがって、本発明は、ストレージ、ユーザ・インターフェース、再生などに関して独自のメディア能力を有するどのようなコンピューティング装置にも適用可能であることが企図されている。

30

【0028】

通信ネットワーク/バス14がインターネットであるネットワーク環境では、たとえば、サーバ10a、10bなどは、クライアント110a、110b、110c、110d、110eなどが、HTTPなど複数の周知のプロトコルのいずれかを介して通信を行う、ウェブ・サーバとすることができる。分散コンピューティング環境の特徴として、サーバ10a、10bなどは、クライアント110a、110b、110c、110d、110eなどとして機能することもできる。

40

【0029】

通信は、必要に応じて、有線で行うことも、無線で行うこともできる。クライアント装置110a、110b、110c、110d、110eなどは、通信ネットワーク/バス14を介して通信を行うことも、介さずに行うこともでき、それらに関連付けられた独立の通信を有することができる。たとえば、TVまたはVCRの場合、それらの制御につい

50

て、ネットワーク化された態様であることも、そうでないこともある。各クライアント・コンピュータ110a、110b、110c、110d、110eなど、およびサーバ・コンピュータ10a、10bなどは、様々なアプリケーション・プログラム・モジュールまたはオブジェクト135を備えることができ、またファイルもしくはデータ・ストリームをそこに保存でき、またはファイルもしくはデータ・ストリームをそこにダウンロード、送信、もしくは移動できる、様々なタイプのストレージ要素またはオブジェクト、に接続またはアクセスすることができる。いずれか1つまたは複数のコンピュータ10a、10b、110a、110bなどは、本発明に従って処理されるデータを保存するためのデータベースまたはメモリ20などの、データベース20またはその他のストレージ要素の保守および更新(maintenance and updating)を担当することができる。したがって、本発明は、コンピュータ・ネットワーク/バス14および(クライアント・コンピュータ110a、110bなどや、その他の同様の装置、およびデータベース20と対話できる)サーバ・コンピュータ10a、10bなどにアクセスし、それらと対話できるクライアント・コンピュータ110a、110bなどを有する、コンピュータ・ネットワーク環境で利用することができる。

【0030】

例示的なコンピューティング装置

図2Bおよび以下の説明は、本発明を実装できる適切なコンピューティング環境についての簡潔で全般的な説明を提供することを意図している。しかし、ハンドヘルド、ポータブル、およびその他のコンピューティング装置、ならびにすべての種類のコンピューティング・オブジェクトが、本発明と関連して使用される対象として、すなわち、コンピューティング環境内でリソースを要求できるあらゆる場所として、またはメディアを体験できるあらゆる場所として、企図されていることを理解されたい。以下では汎用コンピュータを例示的なホストとして説明を進めるが、これは1つの例に過ぎず、本発明は、ネットワーク/バス相互接続性(network/bus interoperability)を有し、対話が可能なシン・クライアントに実装することもできる。したがって、本発明は、非常に僅かなまたは最低限のクライアント・リソースを含むだけの、ネットワークを介してサービスが提供される環境、たとえば、装置内に置かれたオブジェクトなど、クライアント装置がネットワーク/バスとの単なるインターフェースとして機能するだけのネットワーク接続環境、に実装することができる。要するに、そこにデータを保存できる場所、またはそこからデータを取り出すことができる場所、あるいは、別のコンピュータに送信できる場所はどこであれ、本発明による資格証明書のセキュリティ保護された動的な配布を実行するための、望ましい、または適切な環境となる。

【0031】

必ずしも必要なわけではないが、本発明は、装置またはオブジェクト向けのサービスの開発者が使用するために、オペレーティング・システムを介して実装することができ、かつ/または本発明による資格証明書の送付または受領に関連して動作するアプリケーション・ソフトウェア内に含ませることができる。ソフトウェアは、クライアント・ワークステーション、サーバ、またはその他の装置などの、1つまたは複数のコンピュータで実行される、プログラム・モジュールなどの、コンピュータ実行可能命令の一般的コンテキストにおいて説明することができる。一般に、プログラム・モジュールは、特定のタスクを実行したり、特定の抽象データ型を実装したりする、ルーチン、プログラム、オブジェクト、コンポーネント、データ構造などを含む。通常、プログラム・モジュールの機能は、様々な実施形態において、必要に応じて、組み合わせたり、分散させたりすることができる。さらに、本発明が、その他のコンピュータ・システム構成およびプロトコルを用いて実行できることは、当業者であれば理解されよう。本発明とともに使用するのに適している可能性のあるその他の周知のコンピューティング・システム、環境、および/または構成には、パーソナル・コンピュータ(PC)、現金自動預け払い機(automated teller machines)、サーバ・コンピュータ、ハンドヘルドまたはラップトップ装置、マルチ・プロセッサ・システム、マイクロ・プロセッサ・ベースのシステム、プログラム可能な家庭

用電化製品、ネットワークPC、電気器具、照明、環境制御要素、ミニ・コンピュータ、メインフレーム・コンピュータなど、が含まれるが、これらに限定されるものではない。本発明は、タスクが通信ネットワーク／バスまたはその他のデータ伝送媒体を介して結合されたりリモート処理装置で実行される、分散コンピューティング環境でも実施することができる。分散コンピューティング環境では、プログラム・モジュールは、メモリ・ストレージ装置を含む、ローカル・コンピュータ・ストレージ媒体およびリモート・コンピュータ・ストレージ媒体の両方に配置することができ、クライアント・ノードは、サーバ・ノードとして機能することもできる。

【0032】

したがって、図2Bには、本発明を実装できる適切なコンピューティング・システム環境100の一例が図示されているが、上述のことから明らかなように、コンピューティング・システム環境100は、適切なコンピューティング環境の一例に過ぎず、本発明の使用および機能の範囲に関してどのような限定も示唆するものではない。コンピューティング環境100は、例示的な動作環境100に図示されたコンポーネントの任意の1つまたは組合せに関して、どのような依存性または要件ももたないと解釈すべきである。

【0033】

図2Bを参照すると、本発明を実装するための別の例示的なシステムは、コンピュータ110の形態をとる汎用コンピューティング装置を含む。コンピュータ110のコンポーネントには、プロセッシング・ユニット120、システム・メモリ130、およびシステム・メモリを含む様々なシステム・コンポーネントをプロセッシング・ユニット120に結合するシステム・バス121を含めることができるが、これらに限定されるものではない。システム・バス121は、様々なバス・アーキテクチャのいずれかを使用する、メモリ・バスまたはメモリ・コントローラ、周辺バス、およびローカル・バスを含む、複数のタイプのバス構造のうちのいずれかとすることができる。たとえば、こうしたアーキテクチャには、ISA（業界標準アーキテクチャ）バス、MCA（マイクロ・チャンネル・アーキテクチャ）バス、EISA（拡張ISA）バス、VESA（ビデオ電子規格協会）ローカル・バス、およびメザニン・バス（Mezzanine bus）としても知られるPCI（周辺コンポーネント相互接続）バスが含まれるが、これらに限定されるものではない。

【0034】

コンピュータ110は一般に、様々なコンピュータ可読媒体を含む。コンピュータ可読媒体は、コンピュータ110によってアクセス可能な任意の利用可能媒体とすることができ、揮発性および不揮発性媒体、着脱可能および着脱不能媒体を含む。たとえば、コンピュータ可読媒体は、コンピュータ記憶媒体および通信媒体を含み得るが、これらに限定されるものではない。コンピュータ記憶媒体は、コンピュータ可読命令、データ構造、プログラム・モジュール、またはその他のデータといった情報を記憶するための任意の方法または技法によって実装される、揮発性および不揮発性媒体、着脱可能および着脱不能媒体を含む。コンピュータ記憶媒体には、RAM、ROM、EEPROM、フラッシュ・メモリ、またはその他のメモリ技術、CD-ROM、DVD（デジタル多用途ディスク）、またはその他の光ディスク記憶、磁気カセット、磁気テープ、磁気ディスク記憶、またはその他の磁気記憶装置、あるいは所望の情報を記憶するのに使用でき、コンピュータ110によってアクセス可能なその他の任意の媒体が含まれるが、これらに限定されるものではない。通信媒体は一般に、搬送波やその他の移送機構（transport mechanism）などの変調データ信号中に、コンピュータ可読命令、プログラム・モジュール、またはデータ構造を具現し、任意の情報送達媒体を含む。「変調データ信号」という語は、信号中に情報を符号化できるような方式で設定または変更される1つまたは複数の信号特性をもつ信号を意味する。たとえば、通信媒体には、有線ネットワークまたは直接線接続などの有線媒体、および音響、RF、赤外線、またはその他の無線媒体などの無線媒体が含まれるが、これらに限定されるものではない。上記の媒体の任意の組合せも、コンピュータ可読媒体の範囲に含まれるものとする。

【0035】

システム・メモリ 130 は、ROM（読み取り専用メモリ）131 や RAM（ランダム・アクセス・メモリ）132 などの、揮発性および／または不揮発性メモリの形態をとるコンピュータ記憶媒体を含む。基本入出力システム（BIOS）133 は、起動処理中などにコンピュータ 110 内の要素間の情報伝送を助ける基本ルーチンを含み、一般に ROM 131 に記憶される。RAM 132 は一般に、プロセッシング・ユニット 120 がダイレクトにアクセス可能な、かつ／または現在プロセッシング・ユニット 120 上で動作している、データおよび／またはプログラム・モジュールを含む。たとえば、図 2 B には、オペレーティング・システム 134、アプリケーション・プログラム 135、その他のプログラム・モジュール 136、およびプログラム・データ 137 が示されているが、これらに限定されるものではない。

10

【0036】

コンピュータ 110 はまた、その他の着脱可能／着脱不能、揮発性／不揮発性コンピュータ記憶媒体を含む。図 2 B には、着脱不能な不揮発性磁気媒体に対して読み書きを行うハードディスク・ドライブ 141、着脱可能な不揮発性磁気ディスク 152 に対して読み書きを行う磁気ディスク・ドライブ 151、CD-ROM やその他の光媒体など着脱可能な不揮発性光ディスク 156 に対して読み書きを行う光ディスク・ドライブ 155 が、例としてのみ示されている。例示的な動作環境で使用するその他の着脱可能／着脱不能、揮発性／不揮発性コンピュータ記憶媒体には、磁気テープ・カセット、フラッシュ・メモリ・カード、デジタル多用途ディスク、デジタル・ビデオ・テープ、ソリッド・ステート RAM、ソリッド・ステート ROM などが含まれるが、これらに限定されるものではない。ハードディスク・ドライブ 141 は一般に、インターフェース 140 などの着脱不能メモリ・インターフェースを介してシステム・バス 121 に接続され、磁気ディスク・ドライブ 151 および光ディスク・ドライブ 155 は一般に、インターフェース 150 などの着脱可能メモリ・インターフェースを介してシステム・バス 121 に接続される。

20

【0037】

上述され、また図 2 B に示されたドライブおよびそれに関連するコンピュータ記憶媒体は、コンピュータ 110 用のコンピュータ可読命令、データ構造、プログラム・モジュール、およびその他のデータの記憶を可能とする。図 2 B には、たとえば、オペレーティング・システム 144、アプリケーション・プログラム 145、その他のプログラム・モジュール 146、およびプログラム・データ 147 を記憶するものとして、ハードディスク・ドライブ 141 が示されている。これらのコンポーネントは、オペレーティング・システム 134、アプリケーション・プログラム 135、その他のプログラム・モジュール 136、およびプログラム・データ 137 と同じであってもよく、異なってもよいことに留意されたい。ここでは、オペレーティング・システム 144、アプリケーション・プログラム 145、その他のプログラム・モジュール 146、およびプログラム・データ 147 には、少なくともそれらが異なるコピーであることを示すために、異なる番号が振られている。ユーザは、キーボード 162、一般にマウスと呼ばれるポインティング・デバイス 161、トラック・ボール、またはタッチ・パッドなどの入力装置を介して、コマンドおよび情報をコンピュータ 110 に入力することができる。その他の入力装置（図示せず）には、ジョイスティック、ゲーム・パッド、衛星放送用パラボラ・アンテナ、スキャナなどが含まれ得る。上記およびその他の入力装置はしばしば、システム・バスに結合されたユーザ入力インターフェース 160 を介してプロセッシング・ユニット 120 に接続されが、パラレル・ポート、ゲーム・ポート、または USB（汎用シリアル・バス）など、その他のインターフェースおよびバス構造によって接続することもできる。ノース・ブリッジなどのグラフィックス・インターフェース 182 も、システム・バス 121 に接続することができる。ノース・ブリッジは、CPU またはホスト・プロセッシング・ユニット 120 と通信を行うチップセットであり、アクセラレーテッド・グラフィックス・ポート（AGP）との通信を担当する。1 つまたは複数のグラフィックス・プロセッシング・ユニット（GPU）184 は、グラフィックス・インターフェース 182 と通信を行うこ

30

40

50

とができる。この点に関して、GPU 184は一般に、レジスタ記憶などのオンチップ・メモリ記憶を含み、GPU 184は、ビデオ・メモリ 186と通信を行う。しかし、GPU 184は、コ・プロセッサの単なる一例に過ぎず、したがって、コンピューティング 110は、様々なコ・プロセッシング装置を含むことができ、その中には、ピクセル・シェーダおよび頂点シェーダなど、様々な手続き型シェーダが含まれ得る。モニタ 191またはその他のタイプのディスプレイ装置も、ビデオ・メモリ 186と通信することができるビデオ・インターフェース 190などのインターフェースを介してシステム・バス 121に接続される。モニタ 191の他に、コンピュータは、出力周辺インターフェース 195を介して接続できる、スピーカ 197やプリンタ 196などのその他の周辺出力装置も含むことができる。

10

【0038】

コンピュータ 110は、リモート・コンピュータ 180などの1つまたは複数のリモート・コンピュータへの論理コネクションを使用して、ネットワーク接続または分散環境で動作することができる。リモート・コンピュータ 180は、パーソナル・コンピュータ、サーバ、ルータ、ネットワーク PC、ピア装置、またはその他の共通ネットワーク・ノードとすることができ、一般にコンピュータ 110に関連して上述した、多くのまたはすべての要素を含むことができるが、図 2 Bには、メモリ記憶装置 181だけが図示されている。図 2 Bに示す論理コネクションは、LAN（ローカル・エリア・ネットワーク） 171およびWAN（ワイド・エリア・ネットワーク） 173を含むが、その他のネットワーク／バスを含むこともできる。こうしたネットワーク環境は、家庭やオフィスで、また企業規模のコンピュータ・ネットワーク、イントラネット、インターネットで一般的である。

20

【0039】

LANネットワーク環境で使用される場合、コンピュータ 110は、ネットワーク・インターフェースまたはアダプタ 170を介してLAN 171に接続される。WANネットワーク環境で使用される場合、コンピュータ 110は一般に、インターネットなどのWAN 173を介して通信を確立するための、モデム 172またはその他の手段を含む。モデム 172は、内蔵とも外付けともすることができ、ユーザ入力インターフェース 160またはその他の適切な機構を介してシステム・バス 121に接続することができる。ネットワーク接続環境では、コンピュータ 110との関連で示したプログラム・モジュールまたはその部分は、リモート・メモリ記憶装置に記憶することができる。たとえば、図 2 Bには、リモート・アプリケーション・プログラム 185が、メモリ装置 181上に存在するものとして示されているが、それに限定されるものではない。図示のネットワーク接続は例示的なものであり、コンピュータ間の通信リンクを確立するその他の手段も使用できることは理解されよう。

30

【0040】

例示的な装置

図 2 Cおよび以下の説明は、本発明による資格証明書のセキュリティ保護された動的な配布を利用することに関して、コンテンツを提供できる装置またはコンテンツへのアクセスを要求できる装置にとっての適切なコンピューティング環境について、簡潔で全般的な説明を提供することを意図している。しかし、ハンドヘルド、ポータブル、およびその他のコンピューティング装置、ならびにすべての種類のコンピューティング・オブジェクトが、本発明と関連して使用される対象として、すなわち、装置がメディア体験の配給を提供したいと望み得るあらゆる場所として、または装置がその装置のためにメディア体験の配給を要求したいと望み得るあらゆる場所として、企図されていることを理解されたい。これらの装置のメディア機能に関する差異は、要求コンピューティング装置の資格証明書を理解することによって、リモート・メディア体験を異なるリモート装置に合わせるために、重要な利点を有する本発明を利用する。

40

【0041】

必ずしも必要なわけではないが、本発明は、装置またはオブジェクト向けのサービスの

50

開発者が使用するために、オペレーティング・システムを介して部分的に実装することができ、かつ／または本発明のコンポーネントに関連して動作するアプリケーション・ソフトウェア内に含ませることができる。ソフトウェアは、クライアント・ワークステーション、サーバ、またはその他の装置など、1つまたは複数のコンピュータで実行される、プログラム・モジュールなどのコンピュータ実行可能命令の一般的コンテキストにおいて説明することができる。本発明が、その他のコンピュータ・システム構成およびプロトコルを用いて実行できることは、当業者であれば理解されよう。

【0042】

したがって、図2Cには、本発明を実装できる適切なコンピューティング・システム環境100aの一例が図示されているが、上述のことから明らかなように、コンピューティング・システム環境100および100aは、本発明による資格証明書の配布のための、適切なコンピューティング環境の2つの例に過ぎず、本発明の使用および機能の範囲に関してどのような限定も示唆するものではない。コンピューティング環境100または100aは、例示的な動作環境100または100aに図示されたコンポーネントの任意の1つまたは組合せに関して、どのような依存性または要件ももたないと解釈すべきである。

【0043】

図2Cを参照すると、本発明を実装するための第2の例示的な装置は、コンピュータ110aの形態をとる汎用コンピューティング装置を含む。コンピュータ110aのコンポーネントには、プロセッシング・ユニット120a、システム・メモリ130a、およびシステム・メモリを含む様々なシステム・コンポーネントをプロセッシング・ユニット120aに結合するシステム・バス121aを含めることができるが、これらに限定されるものではない。システム・バス121aは、様々なバス・アーキテクチャのいずれかを使用する、メモリ・バスまたはメモリ・コントローラ、周辺バス、およびローカル・バスを含む、複数のタイプのバス構造のうちのいずれかとすることができる。

【0044】

コンピュータ110aは一般に、様々なコンピュータ可読媒体を含む。上述したように、コンピュータ可読媒体は、コンピュータ110aによってアクセス可能な任意の利用可能媒体とすることができる。システム・メモリ130aは、ROM（読み取り専用メモリ）および／またはRAM（ランダム・アクセス・メモリ）などの、揮発性および／または不揮発性メモリの形態をとるコンピュータ記憶媒体を含む。基本入出力システム（BIOS）は、起動処理中などにコンピュータ110a内の要素間の情報伝送を助ける基本ルーチンを含み、メモリ130aに記憶される。メモリ130aは一般に、プロセッシング・ユニット120aが、ダイレクトにアクセス可能な、かつ／または現在、プロセッシング・ユニット上で動作している、データおよび／またはプログラム・モジュールも含む。たとえば、メモリ130aは、オペレーティング・システム、アプリケーション・プログラム、その他のプログラム・モジュール、およびプログラム・データを含むこともできるが、これらに限定されるものではない。

【0045】

コンピュータ110aはまた、その他の着脱可能／着脱不能、揮発性／不揮発性コンピュータ記憶媒体を含み、それらは、インターフェースなどの着脱不能メモリ・インターフェースを介してシステム・バス121aに接続することができ、また磁気ディスク・ドライブおよび光ディスク・ドライブは一般に、インターフェースなどの着脱可能メモリ・インターフェースを介してシステム・バス121aに接続される。

【0046】

ユーザは、様々な入力装置を介して、コマンドおよび情報をコンピュータ110aに入力することができる。グラフィックス・サブ・システムを、システム・バス121aに接続することもできる。モニタまたはその他のタイプのディスプレイ装置も、ビデオ・メモリと通信を行うことができる出力インターフェース150aなどのインターフェースを介して、システム・バス121aに接続される。モニタの他に、コンピュータは、出力インターフェース150aを介して接続できるスピーカやプリンタなどのその他の周辺出力装

10

20

30

40

50

置も含むことができる。

【0047】

コンピュータ110aは、装置110aとは異なるメディア機能を備えることができるリモート・コンピュータ170aなど、1つまたは複数のリモート・コンピュータへの論理コネクションを使用して、ネットワーク接続または分散環境で動作することができる。リモート・コンピュータ170aは、パーソナル・コンピュータ、サーバ、ルータ、ネットワークPC、ピア装置もしくはその他の共通ネットワーク・ノード、またはその他の任意のリモート・メディア消費もしくは送信装置とすることができ、一般にコンピュータ110aに関連して上述した、多くのまたはすべての要素を含むことができる。図2Cに示す論理コネクションは、LAN（ローカル・エリア・ネットワーク）およびWAN（ワイド・エリア・ネットワーク）などのネットワーク171aを含むが、その他のネットワーク／バスを含むこともできる。こうしたネットワーク環境は、家庭やオフィスで、また企業規模のコンピュータ・ネットワーク、イントラネット、インターネットで一般的である。

10

【0048】

したがって、上述した汎用コンピュータは1つの例に過ぎず、本発明は、ネットワーク／バス相互接続性を有し対話が可能な任意のクライアントを用いて実装することができる。したがって、本発明は、非常に僅かなまたは最低限のクライアント・リソースを含むだけの、ネットワークを介してサービスが提供される環境、たとえば、装置内に置かれたオブジェクトなど、クライアント装置がネットワーク／バスとの単なるインターフェースとして機能するだけのネットワーク接続環境で実装することができる。要するに、そこにデータを保存できる場所、またはそこからデータを取り出す場所、別のコンピュータに送信できる場所はどこであれ、本発明による技法を実行するための望ましいまたは適切な環境となる。

20

【0049】

例示的な分散コンピューティング・フレームワークまたは構成

パーソナル・コンピューティングとインターネットとの融合（統合）（convergence）を考慮して、様々な分散コンピューティング・フレームワークが、これまで開発され、今も開発されている。個人ユーザにもビジネス・ユーザにも、アプリケーションおよびコンピューティング装置用の、シームレスで同じように操作ができるウェブ対応のインターフェースが提供されており、コンピューティング活動（computing activities）は、ウェブ・ブラウザまたはネットワーク志向の度合いをますます強めている。

30

【0050】

たとえば、MICROSOFT（登録商標）のマネージドコード（managed code）プラットフォーム、すなわち、NETは、サーバ、ウェブベースのデータ・ストレージなどのビルディング・ブロック・サービス（building-block service）、およびダウンロード可能な装置ソフトウェアを含む。一般的に言って、NETプラットフォームは、（1）システム内のすべてのコンピューティング装置を協働させるとともに、すべての装置でユーザ情報を自動的に更新し、同期させる能力、（2）HTMLの代わりにXMLを積極的に使用することによって可能となった、ウェブ・ページ用の強化された対話機能、（3）カスタマイズされたアクセス、ならびにeメールなどの様々なアプリケーションまたはOffice、NETなどのソフトウェアの管理のための中央開始ポイント（central starting point）からユーザへの製品およびサービスのカスタマイズされた配給を特色とするオンライン・サービス、（4）情報へのアクセスの効率性および容易性、ならびにユーザおよび装置の間での情報の同期を向上させる集中データ・ストレージ、（5）eメール、ファックス、電話など、様々な通信媒体を統合する能力、（6）生産性が向上し、プログラミング・エラーが減少するように、開発者のために再使用可能なモジュールを作成する能力、および（7）その他の多くのクロス・プラットフォームおよび言語統合機能、を提供する。

40

【0051】

50

いくつかの例示的な実施形態は、コンピューティング装置上に存在するソフトウェアとの関連で説明されるが、本発明の方法が、.NETコードなどのマネージ・コードが可能にするすべての言語およびサービスに含まれ、サポートされ、またはそれらを介してアクセスされ得るように、またその他の分散コンピューティング・フレームワークにおいても同様であるように、本発明の1つまたは複数の部分は、オペレーティング・システム、アプリケーション・プログラミング・インターフェース（API）または「仲介者（middle man）」オブジェクト、コントロール・オブジェクト、ハードウェア、ファーム・ウェア、中間言語命令またはオブジェクトなど、を介して実装することもできる。

【0052】

自動ログインに先立つ資格証明書のセキュリティ保護された動的な配布

10

上述したように、本発明は、ホスト・コンピュータのコンテンツ、リソース、および／またはサービスにアクセスするためのログオンが行われる前、たとえば、要求側装置とホスト・コンピュータの間のセッションを開始する時に、ログオンまたはアクセスしたいと望まれているホスト・コンピュータによって、ログオン資格証明書を要求側装置にネットワークを介して自動的に、配布するためのシステムおよび方法を提供する。

【0053】

したがって、本発明は、ホスト・マシンが、セキュリティ保護された方法でクライアント資格証明書を制御することを可能にする。有利には、ホストは、クライアントの関与を必要とせずに、資格証明書を周期的に循環させて、セキュリティを向上させることができる。さらに、本発明によれば、クライアントは、何らかの意味のある時間（for any significant period of time）にわたって資格証明書を保持（hold）する必要がなく、資格証明書の保有に関連するセキュリティ機構およびストレージ機構を含む必要がない。

20

【0054】

図3Aには、本発明の例示的な実施形態が図示されており、本発明によるログイン直前の、資格証明書のセキュリティ保護された動的な配布について概略が示されている。ステップAに示すように、ホスト装置などの第1の装置C1は、装置間の事前交換によって、クライアント装置などの第2の装置からの通信を信頼する。すなわち、ステップAにおいて、装置間で信頼が確立される。信頼を確立する例示的な一方法は、ユーザに関連するバイオメトリック情報（biometric information）を入力して、両装置でそれを共有することである。信頼を確立する例示的な別の方法は、ユーザに信頼コード（trust code）を一方の装置に入力させ、それを他方の装置で受信して、共有の秘密（shared secret）を確立することを含む。同様に、ユーザは、たとえば、メモリ・スティックまたはUSBメモリ装置など、同じハードウェア・コンポーネントを両装置に挿入または入力し、認証プロセスに基づいて装置間で信頼を確立することができる。信頼を確立する例示的なまた別の方法は、第2の装置C2と第1の装置C1の間の「セットアップ」プロセス、すなわち、（i）第2の装置C2が所有する公開鍵を第1の装置C1に保存させることによって、（ii）第1の装置C1が、第2の装置C2から取得した公開鍵が本当に第2の装置C2からのものであり、第1の装置C1によって配布されるログオン資格証明書を横取りしようとしている「rogue（違法）」装置からのものではないことを、保証するプロセスを含むことができる。公開鍵のこの信頼された交換（trusted exchange）は、当業者に周知の多くの異なる方法で行うことができる。たとえば、2004年7月9日に出願された「オフ・ネットワーク入力コードを用いるコンテンツの信頼されたネットワーク転送（Trusted Network Transfer of Content Using Off Network Input Code）」と題する、同一出願人による同時係属中の米国出願第10/888,132号（‘132出願）には、簡単なユーザ入力コードを用いて、公開鍵などのコンテンツを第1のコンピューティング装置から第2のコンピューティング装置へ転送することによって、装置間で信頼された通信を確立するためのシステムおよび方法が記載されている。‘132出願は、様々な実施形態において、ネットワーク・コンテンツ交換の帯域外で入力される簡単なコードを用いて、ネットワーク内の1つのコンピューティング装置から別のコンピューティング装置に、暗号鍵情報などのコンテンツを信頼された方式で送受信できるようにするシステムを

30

40

50

教示する。

【0055】

第1の装置C1と第2の装置C2が信頼を確立した後しばらくして、ステップBにおいて、第2の装置C2が、第1の装置C1のリソースを求める、認証交換を含んだ要求を発行する。本発明によれば、第1の装置C1は、第2の装置C2からの信頼された公開鍵を有しているので、ステップCに示すように、第1の装置C1は、自動的にログオン資格証明書を生成し、ステップDで資格証明書をセキュリティ保護して配布するため、その資格証明書を前述の公開鍵を用いて暗号化する。

【0056】

第2の装置C2は、資格証明書を受信すると、ステップEにおいて、対応する秘密鍵（private key）を用いて資格証明書を復号する。やはりステップEにおいて、ログオン・オブジェクトが、資格証明書を保存することなく、資格証明書を含んだ第1の装置C1へのログオン要求を自動的に生成し、ログオン要求用の関連する認証プロトコルに従って適切に（たとえば、共用公開鍵によって）再暗号化する。ログオン要求は、第2の装置C2に保存されることなく、ステップFにおいて、第2の装置C2から第1の装置C1に送信される。本発明の一実施形態では、補足的な保護のため、ログオン・オブジェクトは、その動作に関連して、保護メモリ空間（protected memory space）を利用する。ステップGにおいて、ログオンは成功し、ステップBでの要求に基づくプライベート通信を、確立されたアクセス・レベルおよび許可に従って、第1の装置C1と第2の装置C2の間で開始することができる。

【0057】

本発明によれば、（ログオン資格証明書に関連して送信されるその他の情報とともに）第1の装置C1からの暗号化された資格証明書は、第1の装置C1に無防備のまま保存することができるが、またはそれを復号できるのは第2の装置C2だけなので、ネットワーク上に自由に分散させることもできることに留意されたい。したがって、その後、第2の装置C2が、第1の装置C1にログオンしたいと望むたびに、ログオン要求を表明するネットワークメッセージを送信すると、第1の装置C1は、暗号化された資格証明書によって応答する。第2の装置C2は、自らの秘密鍵を用いて資格証明書を復号し、直ちにその資格証明書を用いて、第1の装置C1にログオンする。有利には、資格証明書は、後で任意の時に、第1の装置C1によって再生成され、第2の装置C2からの公開鍵を用いて再暗号化することができる。したがって、第2の装置C2は、次回にログインを試みた時には、動的に新しい資格証明書を取得し、それを用いてログインする。

【0058】

図3Bには、上述したプロセスを実装する、第1のコンピューティング装置C1と第2のコンピューティング装置C2の間の通信が例示的なシステムが図示されている。300において、第1の装置C1は、‘132出願の方法による第2の装置C2の信頼性（trustworthiness）を確立する方式で、第2の装置C2から公開鍵を受信する。信頼が確立された後しばらくして、310において、（第2の装置C2からの要求などの）事前定義されたイベントに応答して、第1の装置C1は、動的にログオン資格証明書を生成し、320において、第2の装置C2の公開鍵を用いて資格証明書を暗号化する。330において、暗号化された資格証明書は、ネットワーク上を第2の装置C2に送信される。第2の装置C2は、340において、資格証明書を復号し、350において、適切なログオン・プロトコルに従ってログオン要求を発行すると同時に、資格証明書を消去する。第1の装置C1は、370において、資格証明書を復号し、380において、ログオン要求を処理して、資格証明書の有効性を判定する。資格証明書が有効な場合、390において、セキュリティ保護されたログオンが成功する。資格証明書が無効な場合、ログオンは成功しないので、フローは385において失敗する（fail：機能しなくなる）。

【0059】

図4Aおよび図4Bには、クライアント装置がホスト装置とのセッションを開始したいと望んでいる場面において、本発明によるネットワークを介する資格証明書のセキュリテ

ィ保護された動的な配布の一実施形態に関連して、実行される処理を表した例示的かつ非限定的なフローチャートと、および、この実施形態に関連して、従うことのできるプロトコルが示されている。したがって、ホストとクライアントの間で信頼が確立されている場合、本発明は、セッション確立の手順に適用することができる。

【0060】

簡単な定義を行うと、セッションとは、ユーザ・アカウントをそのアカウントに関連する資格証明書を用いてマシンにログインさせた時に、オペレーティング・システム内に生成される環境のことである。ユーザがログインすると、セッションが生成され、ユーザがログアウトすると、セッションは終了させられる。一たびログインがなされると、手動によるログオフまたはOSによる強制的ログオフが行われるまで、ユーザ・アカウントのセ

10

【0061】

図4Aおよび図4B内の、楕円の破線で囲まれ、対応する類似の番号が付された、いくつかの部分が、図3Aのブロック図の非限定的な実施形態であることは理解できよう（たとえば、図3AにおけるステップBへの参照は、図4A～4Bでは参照符号BBになり、図3AにおけるステップDへの参照は、図4A～4Bでは参照符号DDになるなど）。し

20

したがって、ステップBにおける要求は、ホスト（図4B）とのセッションを開始するため、クライアント（図4A）によってRDPInitRQがコールされるエリアBBに対応する。図4Bにおいて、ステップCは、ホスト装置によるログオン資格証明書の動的な生成に関連する通信および処理と、それに対応する暗号化のためのクライアントの公開鍵の使用と、を示すエリアCCに対応する。ステップDは、ログオン要求がクライアントの公開鍵を用いた暗号化によるセキュリティ保護された方式でホストからクライアントに送信され（図4B）、クライアントによって受信される（図4AのエリアDD）エリアDDに概略的に示されている。図4AのエリアEEで示されるように、資格証明書が受信され、復号された直後に、ホスト装置とのセッションの確立に関連して、クライアントは、エリアFFに関連する処理を介し、復号化された資格証明書を用いてホストにログオンする。

30

ここで、資格証明書を用いた自動ログオンが成功した場合、エリアGGの処理によって概略的に示されるように、アクティブ・セッションが開始される。

【0062】

しかし、図4Aおよび図4Bは、特定の処理、特定のインターフェース、および特定のプロトコルの見地からの、装置間で起こり得る例示的な通信についての一実装形態を図示したものに過ぎないことは明らかであり、本発明が、その他の様々な処理、プロトコル、インターフェースなどを用いても実装できることは強調されるべきである。たとえば、多くのアルゴリズムが無数の数の数学的形状および形式を仮定できること、またソフトウェアの視点から鍵を考察することは、アルゴリズムが任意の明示的または暗黙的形式で望ましい関数を実行することであることは理解できよう。さらに、データ構造も多くの形式を

40

仮定することができ、したがって、たとえば、タイプ、名前、クラスなどは、多様な方法で定義することができる。以下に示す表1には、たとえば、図4Aおよび図4Bで参照される変数について、いくつかの例示的な実装選択例が示されている、がしかし、本明細書の説明とよく調和している。これらの実装の詳細は、本発明を限定することを意図するものではない。

【0063】

【表 1】

DvcPubKey	256バイト整数	NULL	装置の公開鍵
LogonKey	128ビット対称鍵	NULL	DvcPubKeyを用いて暗号化された対称「セッション」鍵、LogonCredsを暗号化するのに用いられる
LogonCreds	可変長ビット・フィールド	NULL	DvcUsrAcct用にLogonKeyを用いて暗号化されたNTユーザ・アカウントの資格証明書

表 1 ログオン資格証明書とともに使用する例示的な変数

10

【0064】

したがって、図 4 A および図 4 B には、本発明の例示的かつ非限定的な実施形態が図示されており、本発明は特許請求の範囲を基準として確定されるべきことは明らかであろう。

【0065】

本発明を実装する複数の方法、たとえば、アプリケーションおよびサービスが本発明による資格証明書のセキュリティ保護された動的な配布を行えるようにする、たとえば、適切な A P I、ツール・キット、ドライバ・コード、オペレーティング・システム、コント

20

【0066】

上述したように、本発明の例示的な実施形態を、様々なコンピューティング装置およびネットワーク構成との関連で説明してきたが、基礎となる概念は、ログイン直前に資格証明書をセキュリティ保護して自動的に配布するのが望ましい、任意のコンピューティング装置またはシステムに適用することができる。たとえば、本発明のアルゴリズムおよびハードウェアの実装は、装置上の別々のオブジェクトとして、別のオブジェクトの一部として、再使用可能コントロールとして、サーバからダウンロード可能なオブジェクトとして、装置またはオブジェクトとネットワークとの間の「仲介者 (middle man)」として、分散オブジェクトとして、ハードウェアとして、上記の任意の組合せなどとして、メモリ内に提供される、コンピューティング装置のオペレーティング・システムに適用することができる。本明細書において、例示的なプログラミング言語、名前、および例は、様々な選択肢のうちの代表例として選ばれているが、これらの言語、名前、および例は、本発明の限定を意図するものではない。本発明の様々な実施形態によって達成されるのと同じ、類似、または等価の機能を達成する、オブジェクトコードおよび命名 (nomenclature) を提供する数多くの方法が存在することは、当業者であれば理解されよう。

30

40

【0067】

上述したように、本明細書で説明する様々な技法は、ハードウェアまたはソフトウェア、または必要に応じて、両方の組合せと関連をもたせて、実装することができる。したがって、本発明の方法および装置、またはそれらのある態様 (aspect) もしくは部分 (portion) は、フロッピー (登録商標) ディスク、C D-R O M、ハード・ドライブ、またはその他の任意のマシン可読媒体などの有形な媒体中に具体化されるプログラム・コード (すなわち、命令) の形態をとることができ、プログラム・コードが、コンピュータなどのマシンにロードされ、マシンによって実行された場合、マシンは本発明を実施するための

50

装置となる。プログラム可能コンピュータでプログラム・コードを実行する場合、一般にコンピューティング装置は、プロセッサ、プロセッサによって可読なストレージ媒体（揮発性および不揮発性メモリ、および／またはストレージ要素を含む）、少なくとも1つの入力装置、および少なくとも1つの出力装置を含む。本発明の資格証明書配布機構を、たとえば、データ処理APIや再使用可能コントロールなどを使用して実装でき、または利用できる、1つまたは複数のプログラムは、コンピュータ・システムと通信を行うため、好ましくは、高水準の手続き型またはオブジェクト指向プログラミング言語で実装されることが可能である。しかし、プログラムは、必要に応じて、アセンブリ言語またはマシン語で実装することもできる。いずれの場合でも、その言語はコンパイル型またはインタプリタ型の言語とすることができ、ハードウェア実装と組み合わせることができる。

10

【0068】

本発明の方法および装置はまた、電氣的配線もしくはケーブル、光ファイバ、またはその他の任意の伝送形態など、何らかの伝送媒体上を伝送されるプログラム・コードの形態で実施される、通信を介して実行することができ、プログラム・コードが、EPROM、ゲート・アレイ、プログラム可能論理回路（PLD）、クライアント・コンピュータなどのマシンによって受信され、ロードされ、そして実行された場合、マシンは本発明を実施するための装置となる。汎用プロセッサに実装される場合、プログラム・コードは、プロセッサと組み合わされて、本発明の機能と呼び出すために動作する固有の装置を提供する。さらに、本発明との関連で使用されるストレージ技法はどれも、常にハードウェアとソフトウェアの組合せとすることができ。

20

【0069】

様々な図の好ましい実施形態との関連で本発明を説明してきたが、本発明から逸脱することなく本発明と同じ機能を実行するため、その他の類似の実施形態が使用できること、または本明細書で説明した実施形態に変更および追加を施し得ること、が理解されよう。たとえば、本発明の例示的なネットワーク環境は、ピア・ツー・ピアまたは分散ネットワーク環境など、ネットワーク接続環境のコンテキストにおいて説明されたが、本発明がそれに限定されるものではないこと、およびこの方法は、本出願で説明されたように、ゲーム・コンソール、ハンドヘルド・コンピュータ、ポータブル・コンピュータなど、任意のコンピューティング装置または環境に適用できること、有線によるにしろ無線によるにしろ、通信ネットワークを介して接続され、ネットワークを介して対話する任意の数のそのようなコンピューティング装置に適用できることは、当業者であれば理解されよう。さらに、とりわけ無線ネットワーク接続装置の数が増加し続けているので、ハンドヘルド装置用オペレーティング・システム、およびその他の特定用途向けオペレーティング・システムを含む、多様なコンピュータ・プラットフォームが企図されていることも強調しておくべきであろう。

30

【0070】

例示的な実施形態では、特定のプロトコルおよび通信のコンテキストで本発明の利用を言及しているが、本発明は、それらに限定されるものではなく、本発明による資格証明書のセキュリティ保護された動的な配布を提供するため、むしろ任意のプロトコルを実装することができる。さらに、本発明は、複数の処理チップまたは装置に、またはそれらにわたって、実装することができ、ストレージも同様に、複数の装置にわたって達成することができる。したがって、本発明は、どの1つの実施形態にも限定されることはなく、むしろ特許請求の範囲の広がりおよび範囲において解釈されるべきものである。

40

【図面の簡単な説明】**【0071】**

【図1A】メディア体験を提供する際のメディア・タイプおよびメディア装置の多様性を示した図である。

【図1B】1つのコンピューティング装置が別のコンピューティング装置のリソースにアクセスするため、その別のコンピューティング装置にログインする、例示的な従来技術のコンピューティング環境を示した図である。

50

【図 2 A】本発明を実装できる、様々なコンピューティング装置を有する例示的なネットワーク環境を表したブロック図である。

【図 2 B】本発明を実装できる、例示的かつ非限定的なサーバ・コンピューティング装置を表したブロック図である。

【図 2 C】本発明を実装できる、データ受信またはデータ送信を行う、第 2 の例示的かつ非限定的なコンピューティング装置を表したブロック図である。

【図 3 A】本発明のシステムおよび方法の様々な実施形態による、第 1 のコンピューティング装置から第 2 のコンピューティング装置への資格証明書のセキュリティ保護された動的な配布を示した図である。

【図 3 B】本発明のシステムおよび方法の様々な実施形態による、第 1 のコンピューティング装置から第 2 のコンピューティング装置への資格証明書のセキュリティ保護された動的な配布を示した図である。

10

【図 4 A】クライアント装置がホスト装置とのセッションを開始したいと望んでいる場面において、本発明によるネットワークを介する資格証明書のセキュリティ保護された動的な配布の一実施形態に関連して、実行される処理を表した例示的かつ非限定的なフローチャートと、付随して実行されることになるプロトコルを示した図である。

【図 4 B】クライアント装置がホスト装置とのセッションを開始したいと望んでいる場面において本発明によるネットワークを介する資格証明書のセキュリティ保護された動的な配布の一実施形態に関連して、実行される処理を表した例示的かつ非限定的なフローチャートと、付随して実行されることになるプロトコルを示した図である。

20

【符号の説明】

【0 0 7 2】

1 0 a サーバ・オブジェクト

1 0 b サーバ・オブジェクト

1 4 通信ネットワーク／バス

2 0 データベース

1 1 0 a コンピューティング装置

1 1 0 b コンピューティング装置

1 1 0 c オブジェクト

1 1 0 d オブジェクト

30

1 1 0 e コンピューティング装置

1 0 0 コンピューティング環境

1 2 0 プロセッシング・ユニット

1 2 1 システム・バス

1 3 0 システム・メモリ

1 3 1 (ROM)

1 3 2 (RAM)

1 3 3 BIOS

1 3 4 オペレーティング・システム

1 3 5 アプリケーション・プログラム

40

1 3 6 その他のプログラム・モジュール

1 3 7 プログラム・データ

1 4 0 着脱不能揮発性メモリ・インターフェース

1 4 4 オペレーティング・システム

1 4 5 アプリケーション・プログラム

1 4 6 その他のプログラム・モジュール

1 4 7 プログラム・データ

1 5 0 着脱可能揮発性メモリ・インターフェース

1 6 0 ユーザ入力インターフェース

1 6 1 ポインティング・デバイス

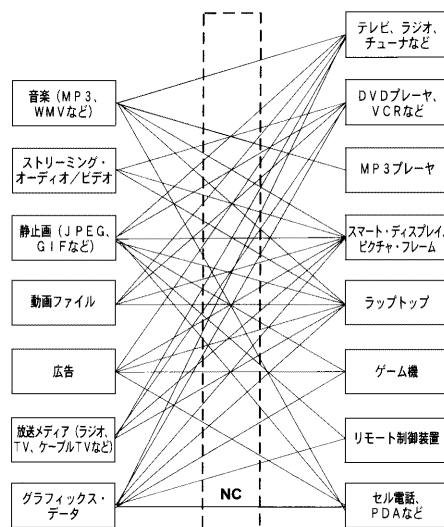
50

- 162 キーボード
- 170 ネットワーク・インターフェース
- 171 ローカル・エリア・ネットワーク
- 172 モデム
- 173 ワイド・エリア・ネットワーク
- 180 リモート・コンピュータ
- 182 グラフィックス・インターフェース
- 184 GPU
- 186 ビデオ・メモリ
- 185 リモート・アプリケーション・プログラム
- 190 ビデオ・インターフェース
- 191 モニタ
- 195 出力周辺インターフェース
- 196 プリンタ
- 197 スピーカ
- 100a コンピューティング環境
- 120a プロセッシング・ユニット
- 121a システム・バス
- 130a システム・メモリ
- 140a 入力
- 150a 出力、たとえば、ディスプレイ
- 160a ネットワーク・インターフェース
- 170a リモート・コンピュータ

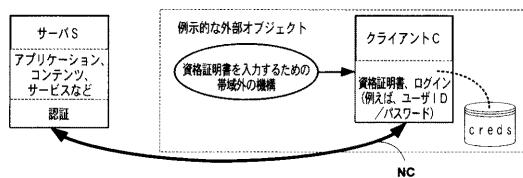
10

20

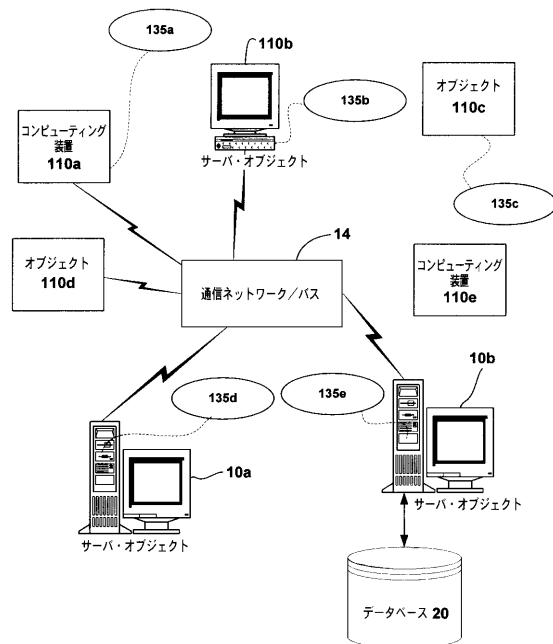
【図1A】



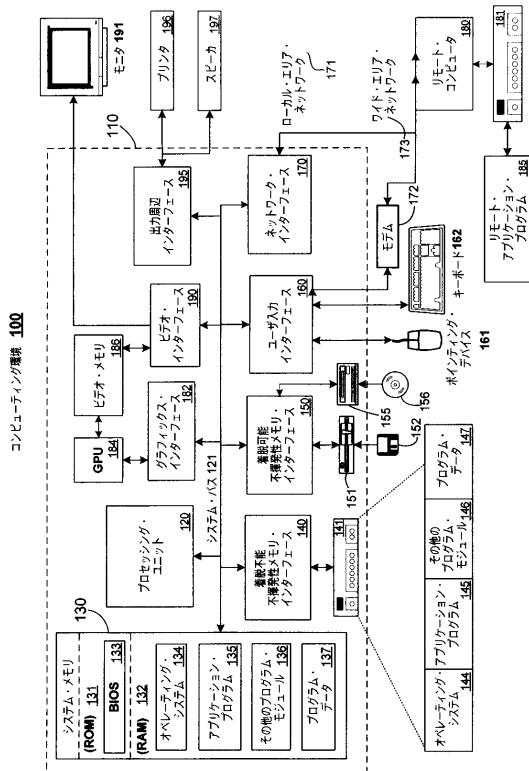
【図1B】



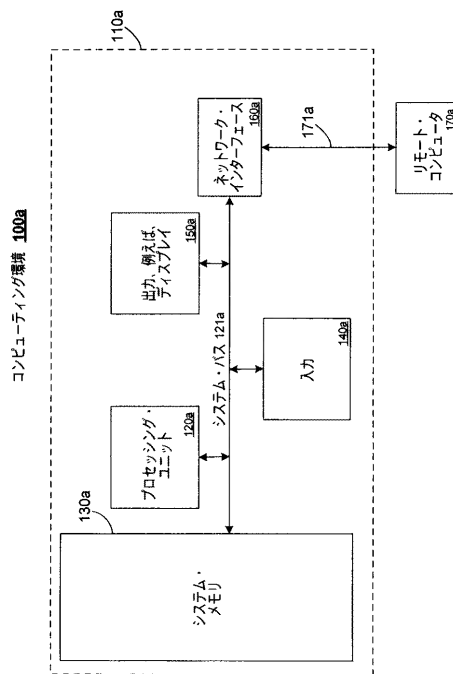
【図2A】



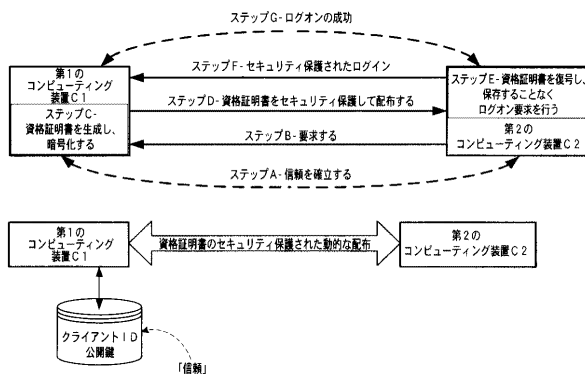
【図 2 B】



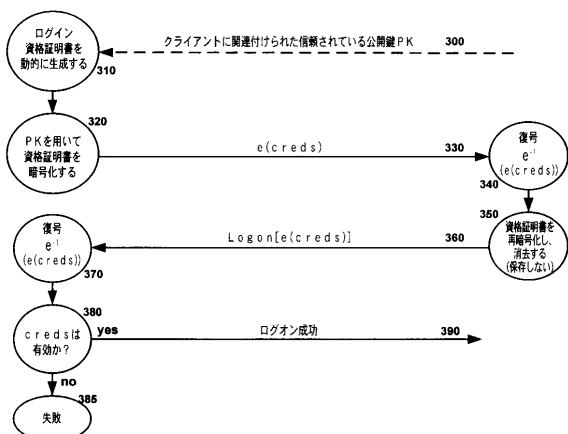
【図 2 C】



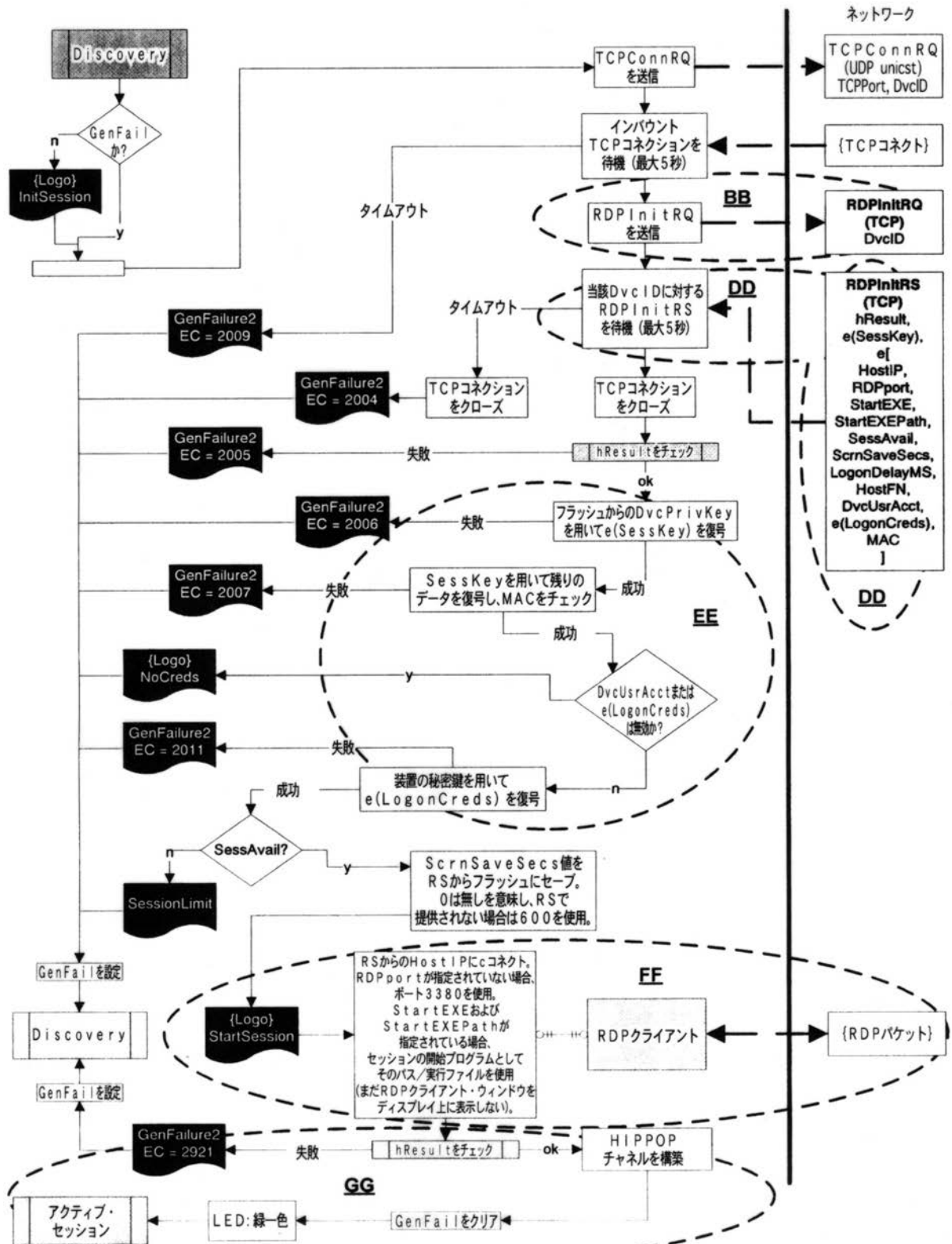
【図 3 A】



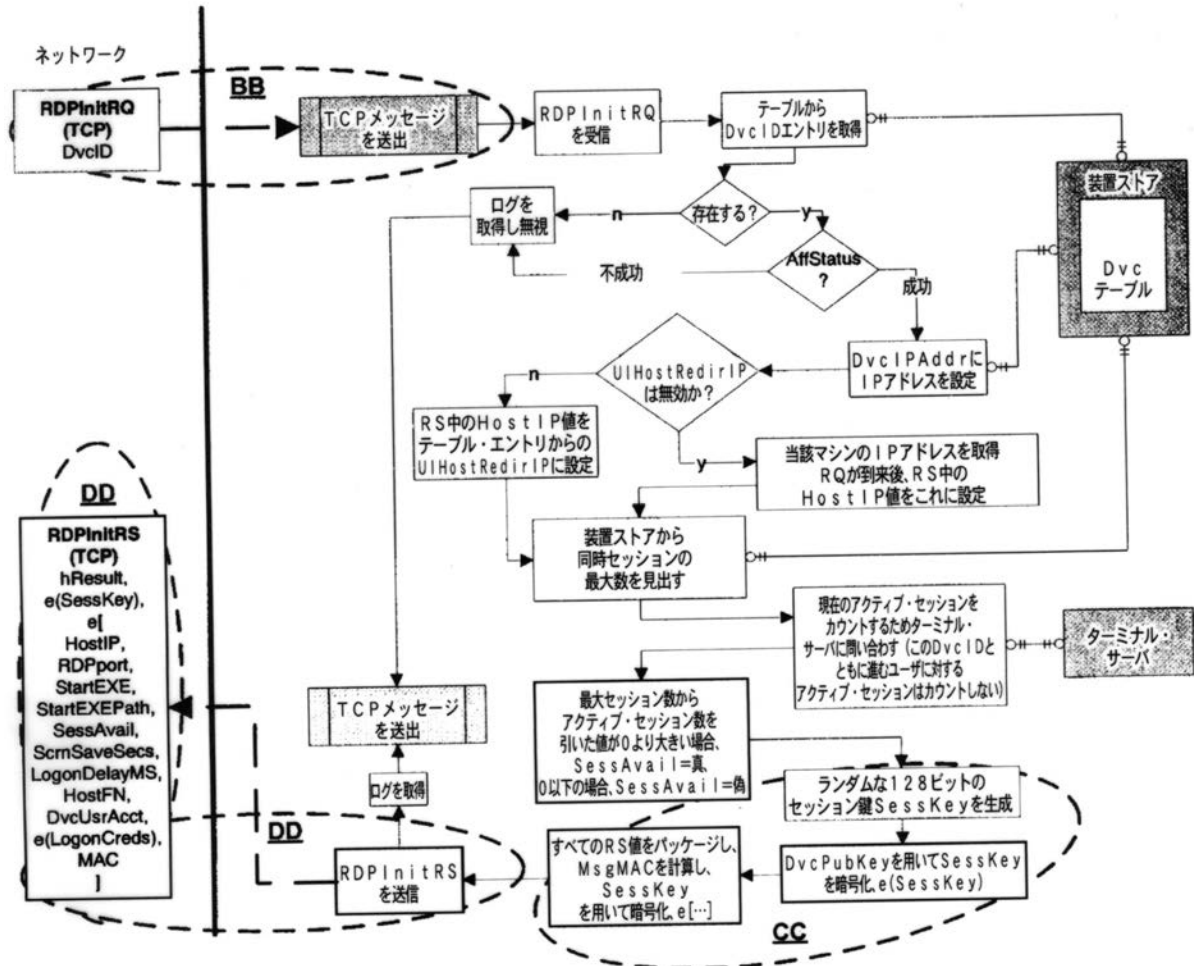
【図 3 B】



【図 4 A】



【図 4 B】



フロントページの続き

(72)発明者 ハリー エス. パイル

アメリカ合衆国 98052 ワシントン州 レッドモンド ワン マイクロソフト ウェイ マイ
クロソフト コーポレーション内

(72)発明者 ニコラス ジェイ. ファング

アメリカ合衆国 98052 ワシントン州 レッドモンド ワン マイクロソフト ウェイ マ
イクロソフト コーポレーション内

審査官 和田 財太

(56)参考文献 国際公開第2002/032047 (WO, A1)

特開2001-175754 (JP, A)

特開平11-168461 (JP, A)

特開平08-227397 (JP, A)

特開2001-103046 (JP, A)

国際公開第2001/052470 (WO, A1)

中山 貴夫, '連載 UNIXの道具箱21 SSH', UNIX MAGAZINE, 日本, 株式会社アスキー, 2003年 7月 1日, 第18巻 第7号, 87頁-101頁

岡本 龍明, 'シリーズ/情報科学の数学 現代暗号', 産業図書株式会社, 1998年 6月30日, 初版 第2刷, 151頁-162頁

加藤 博光, '制御系ファイアウォールのためのセキュア遠隔操作プロトコルSTP', 情報処理学会論文誌, 日本, 社団法人情報処理学会, 2002年 8月15日, 第43巻 第8号, 2252頁-2561頁

(58)調査した分野(Int.Cl., DB名)

G06F 21/20

H04L 9/32