

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4976646号
(P4976646)

(45) 発行日 平成24年7月18日 (2012. 7. 18)

(24) 登録日 平成24年4月20日 (2012. 4. 20)

(51) Int. Cl.	F I
G 0 6 F 21/20 (2006.01)	G O 6 F 21/20 1 3 1 A
G 0 9 C 1/00 (2006.01)	G O 9 C 1/00 6 4 O E
	G O 9 C 1/00 6 6 O E

請求項の数 31 (全 36 頁)

(21) 出願番号	特願2004-221235 (P2004-221235)	(73) 特許権者	500046438
(22) 出願日	平成16年7月29日 (2004. 7. 29)		マイクロソフト コーポレーション
(65) 公開番号	特開2005-327234 (P2005-327234A)		アメリカ合衆国 ワシントン州 9805
(43) 公開日	平成17年11月24日 (2005. 11. 24)		2-6399 レッドモンド ワン マイ
審査請求日	平成19年7月11日 (2007. 7. 11)		クロソフト ウェイ
(31) 優先権主張番号	10/631206	(74) 代理人	100077481
(32) 優先日	平成15年7月31日 (2003. 7. 31)		弁理士 谷 義一
(33) 優先権主張国	米国 (US)	(74) 代理人	100088915
			弁理士 阿部 和夫
		(72) 発明者	レイモンド・イー・オジー
			アメリカ合衆国 マサチューセッツ州 O
			1944 マンチェスター ハーパー・ス
			トリート 50

最終頁に続く

(54) 【発明の名称】 ピアツーピアコラボレーションシステムにおいて連絡先認証を管理、表示するための方法及び装置

(57) 【特許請求の範囲】

【請求項 1】

ユーザのそれぞれがアイデンティティ及び表示名を有するピアツーピアコラボレーションシステムにおけるエンドポイントを提供するコンピュータデバイスで動作する方法であって、

第1のユーザとの通信に応答して、前記コンピュータデバイスに関連付けられたメモリ内の連絡先データストア内の連絡先として前記第1のユーザを記録するステップであって、前記記録するステップは、少なくとも前記第1のユーザのアイデンティティと表示名とを記録することを含む、記録するステップと、

第2のユーザからの通信の受信に応答して、前記第2のユーザの表示名が前記連絡先データストア内のユーザの前記表示名と同等かどうかを判定するステップと、

前記第2のユーザの表示名が、前記連絡先データストア内のユーザの前記表示名と同等で、前記第2のユーザのアイデンティティが、前記同等の表示名を有する前記連絡先データストア内の前記ユーザの前記アイデンティティと異なるときに、前記コンピュータデバイスに関連付けられたディスプレイ上に表示する警告を生成するステップであって、前記警告を生成するステップは、前記同等の表示名を有する前記コンタクトデータストア内の前記ユーザの前記表示名と同等の前記表示名を有する潜在的ななりすましユーザについての警告を生成することを含み、前記潜在的ななりすましユーザは、前記同等の表示名を有する前記連絡先データストア内の前記ユーザの前記表示名と同等の表示名を有するユーザのセットから選択され、前記セットは、前記同等の表示名を有する前記連絡先データストア

10

20

ア内の前記ユーザを含み、前記潜在的ななりすましユーザは、前記セットにおける前記ユーザの関連する認証レベルに基づいて、選択されるステップと

を含み、

前記警告は、前記コンピュータデバイスの第1のグラフィカルユーザインターフェースに表示される、一致された表示名との一致を示す名前一致インジケータを含み、前記一致された表示名は、前記同等の表示名を有する前記連絡先データストア内の前記第2のユーザおよび前記ユーザに共通の表示名であり、

前記方法は、更に、

前記第1のグラフィカルユーザインターフェースを介して受信され、前記名前一致インジケータに関連付けられるユーザ入力に応答して、前記一致された表示名と同等の複数の同等の表示名をコンピュータデバイス上に表示するステップと、

10

選択された表示名のための代替の表示名を特定する前記コンピュータデバイスのユーザからユーザ入力を受信するステップであって、前記代替の表示名は、前記コンピュータデバイス上に表示された複数の同等の表示名から前記ユーザに選択され、前記代替の表示名は、選択されたアイデンティティに関連付けられ、及び前記一致された表示名と異なることを特徴とする受信するステップと、

前記代替の表示名を有する前記選択されたアイデンティティを前記コンピュータデバイスの前記第2のグラフィカルユーザインターフェース上で識別するステップであって、前記第2のグラフィカルユーザインターフェースは、ピアツーピアコラボレーションシステム内の通信を制御することに関連する機能を提供し、前記通信は、前記コンピュータデバイスと、選択されたアイデンティティに関連付けられた第2のデバイスとの間で行われることを特徴とする識別するステップと

20

を含むことを特徴とする方法。

【請求項2】

前記第2のユーザの前記表示名が前記連絡先データストア内に記憶された前記連絡先の前記表示名と同等かどうかを判定するステップは、それぞれの表示名からクリーンネーム(clean name)を算出するステップと、前記2つの表示名のクリーンネームを比較するステップとを含むことを特徴とする請求項1に記載の方法。

【請求項3】

前記警告を生成するステップは、

30

連絡先アイデンティティと関連付けられたそれぞれの表示名の隣に名前一致インジケータを表示するステップを含み、

前記連絡先アイデンティティの認証レベルは、

(1) 同等の表示名を有する全ての連絡先アイデンティティの最高の認証／証明レベル未満であるか／あるいは、

(2) 同等の表示名を有する全ての連絡先アイデンティティの最高の認証／証明レベルと等しく、及び、同等の表示名を有する少なくとも1つの他の連絡先アイデンティティが等しい認証レベルを有すると識別されるかのいずれかであることを特徴とする請求項1に記載の方法。

【請求項4】

40

他のユーザが所定の認証レベルを有しているときには、セキュリティ方針に基づいて、ユーザが該他のユーザと通信することを防止するステップを更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】

警告を生成するステップは、ここにリストされた第2のユーザの表示名と等しい全ての表示名を有するダイアログボックスを表示するステップを含むことを特徴とする請求項1に記載の方法。

【請求項6】

ユーザ入力を受信するステップは、選択された表示名に、エイリアスとして、代替の表示名を割り当てることを含み、前記エイリアスは、前記一致された表示名、及び前記選択

50

された表示名のそれぞれに同等ではなく、前記エイリアスは、前記選択された表示名を置き換えることを更に含むことを特徴とする請求項 1 に記載の方法。

【請求項 7】

前記警告を表示するステップは、別の表示名と等しくない、表示名の次に認識インジケータを表示することを含み、前記認識インジケータは、前記関連付けられた連絡先の認証レベルを表示することを特徴とする請求項 1 に記載の方法。

【請求項 8】

前記コンピュータデバイスの表示スクリーン上に現れる前記第 2 のユーザの表示名の複数の例のそれぞれのために、前記表示名と同時に前記警告を表示する ステップ を含むことを特徴とする請求項 1 に記載の方法。

10

【請求項 9】

前記表示名と同時に警告を生成するステップは、前記表示名の例に近接してアイコンを表示するステップを含む

ことを特徴とする請求項 8 に記載の方法。

【請求項 10】

前記連絡先データストアにエントリがない、新しいユーザからの通信を受信するとすぐに、

前記連絡先データストアに新しいユーザのエントリを作成するステップであって、前記エントリを作成するステップは、前記新しいユーザについての情報を表現するグラフィカルユーザインターフェースを表示するステップと、前記新しいユーザを認証している前記コンピュータデバイスのユーザから入力を受信するように適用された入力エリアを含むステップを含むことを特徴とする請求項 1 に記載の方法。

20

【請求項 11】

各連絡先が所定数の認証レベルの 1 つを有し、表示される認証インジケータが認証レベルの 1 つに対して一意であることを特徴とする請求項 7 に記載の方法。

【請求項 12】

前記複数の例の少なくとも 1 つは、通信するための連絡先を選択するユーザ入力を受信するように適応されたグラフィカルユーザインターフェース内の連絡先のリストを備えることを特徴とする請求項 8 に記載の方法。

【請求項 13】

30

前記新しいユーザを認証している前記コンピュータデバイスの前記ユーザから入力を受信されるとき、前記新しいユーザが認証されている識別を前記新しいユーザのための前記エントリ内に記憶するステップと、

前記新しいユーザを認証している前記コンピュータデバイスの前記ユーザから入力を受信されないとき、前記新しいユーザが認証されていない識別を前記新しいユーザのための前記エントリ内に記憶するステップと、

を含むことを特徴とする請求項 10 に記載の方法。

【請求項 14】

ユーザのそれぞれがアイデンティティ及び表示名を有するピアツーピアコラボレーションシステムにおけるエンドポイントを提供するコンピュータデバイスで動作する方法であって、

40

コンピュータデバイスのユーザ及び／又はシステム管理者からセキュリティ方針を設定する入力を受信するステップと、

第 1 のユーザの表示名の表示を含む機能を引き起こすイベントに応答して、

前記第 1 のユーザの認証レベルを判定するステップであって、前記認証レベルは、(1) 手動で認証済み、(2) 企業内で証明済み、(3) 企業間で証明済み、及び(4) 未認証を含むセットから選択された認証レベルを含み、前記証明されたレベルは、前記手動で認証済みが最高のレベルであるステップと、

前記認証レベルと前記セキュリティ方針に基づいて、前記イベントに選択的に応答するステップであって、前記セキュリティ方針は、少なくとも、許可オプションと、制限オプ

50

ションと、警告オプションとを有するステップとを含み、

前記選択的に応答するステップは、

前記セキュリティ方針オプションが許可されると判定されるときに、グラフィカルユーザインターフェース上に、前記イベントに応答する機能の実行と同時に、前記第1のユーザの表示名を表示するステップと、

前記セキュリティ方針オプションが警告されると判定され、前記認証レベルが、閾値レベルより低いか同じレベルであるときに、前記グラフィカルユーザインターフェース上に、前記機能の実行と同時に、前記第1のユーザの表示名を表示するステップであって、前記表示するステップは、前記第1のユーザの認証レベル上に警告を表示するステップを含むステップと、

10

前記セキュリティ方針オプションが制限されると判定され、前記認証レベルが、閾値レベルより低いか同じレベルであるときに、前記機能の実行が取り消されるステップとを含むことを特徴とする方法。

【請求項15】

前記セキュリティ方針を設定する入力を受信するステップは、前記コンピュータデバイスのユーザから前記セキュリティ方針の設定の入力を受信するステップを含むことを特徴とする請求項14に記載の方法。

【請求項16】

前記セキュリティ方針を設定する入力を受信するステップは、前記システム管理者から前記セキュリティ方針の設定の入力を受信するステップを含むことを特徴とする請求項14に記載の方法。

20

【請求項17】

前記イベントに選択的に応答するステップは、前記セキュリティ方針が警告されると設定され、ユーザが認証されていないか、証明されていない連絡先との通信を試みると、前記ユーザに警告を行うステップを含むことを特徴とする請求項14に記載の方法。

【請求項18】

前記イベントに選択的に応答するステップは、前記セキュリティ方針が制限されると設定され、ユーザが証明されていない連絡先との通信を試みると、ユーザが前記証明されていない連絡先との通信を行うことを防止するステップを含むことを特徴とする請求項14に記載の方法。

30

【請求項19】

前記イベントに選択的に応答するステップは、前記セキュリティ方針が許可されると設定され、ユーザが認証されていないか、証明されていない連絡先との通信を試みると、前記ユーザが認証されていないか、前記証明されていない連絡先との通信することを許容するステップを含むことを特徴とする請求項14に記載の方法。

【請求項20】

前記第1のユーザの認証レベルを判定するステップは、
連絡先の連絡先リストをコンパイルするステップと、
認証されていない連絡先を判定するために連絡先リストをチェックするステップと、
証明方針が任意の認証されていない連絡先に適用できるかどうかを判断するために、認証されていない連絡先をチェックするステップと、

40

証明方針が連絡先に適用できないときには、認証されていない及び証明されていない連絡先のリストに認証されていない連絡先を載せるステップと
を含むことを特徴とする請求項14に記載の方法。

【請求項21】

前記閾値レベルは、前記第1のユーザの表示名と同等の表示名を有する少なくとも1つの他のユーザの認証レベルに基づいて動的に判定されることを特徴とする請求項14に記載の方法。

【請求項22】

前記選択的に応答するステップは、前記認証レベル、前記セキュリティ方針、前記イベ

50

ントへの応答の性質に基づいて、前記イベントを処理するステップを含むことを特徴とする請求項 1 4 に記載の方法。

【請求項 2 3】

連絡先データストア内にエントリがない、新しいユーザからの通信を受信するとすぐに、

前記連絡先データストアに新しいユーザのエントリを作成するステップであって、前記エントリを作成するステップは、前記新しいユーザについての情報を表示するグラフィカルユーザインターフェースを表示するステップと、前記コンピュータデバイスのユーザが前記新しいユーザを認証できる入力エリアを含むステップとを含むことを特徴とする請求項 1 4 に記載の方法。

10

【請求項 2 4】

前記イベントは、前記第 1 のユーザからの通信を受信することを含むことを特徴とする請求項 1 4 に記載の方法。

【請求項 2 5】

前記イベントは、ユーザとの通信を開始するコマンドを含むユーザ入力を受信することを含むことを特徴とする請求項 1 4 に記載の方法。

【請求項 2 6】

ユーザのそれぞれがアイデンティティ及び表示名を有するピアツーピアコラボレーションシステムにおけるエンドポイントを提供するコンピュータデバイスにおいて実行されるときに、方法を実行するコンピュータ実行可能命令を記録するコンピュータ可読記録媒体であって、前記方法は、

20

コンピュータデバイスのユーザ及び／又はシステム管理者からセキュリティ方針を設定する入力を受信するステップと、

第 1 のユーザの表示名の表示を含む機能を引き起こすイベントに応答して、

前記第 1 のユーザの認証レベルを判定するステップであって、前記認証レベルは、(1) 手動で認証済み、(2) 企業内で証明済み、(3) 企業間で証明済み、及び(4) 未認証を含むセットから選択された認証レベルを含み、前記証明されたレベルは、前記手動で認証済みが最高のレベルであるステップと、

前記認証レベルと前記セキュリティ方針に基づいて、前記イベントに選択的に応答するステップであって、前記セキュリティ方針は、少なくとも許可オプションと、制限オプションと、警告オプションを有するステップとを含み、

30

前記選択的に応答するステップは、

前記セキュリティ方針オプションが許可されると判定されるときに、グラフィカルユーザインターフェース上に、前記イベントに応答する機能の実行と同時に、前記第 1 のユーザの表示名を表示するステップと、

前記セキュリティ方針オプションが警告されると判定され、前記認証レベルが、閾値レベルより低いか同じレベルであるときに、前記グラフィカルユーザインターフェース上に、前記機能の実行と同時に、前記第 1 のユーザの表示名を表示するステップであって、前記表示するステップは、前記第 1 のユーザの認証レベル上に警告を表示するステップを含むステップと、

40

前記第 1 のユーザが証明されていないと判定されると、

前記第 1 のユーザについての情報を表現するグラフィカルユーザインターフェースを表示するステップであって、前記グラフィカルユーザインターフェースは、前記第 1 のユーザを認証している前記コンピュータデバイスのユーザから入力を受信するように適用された入力エリアを含むことを特徴とする表示するステップと、

前記入力の前記第 1 のユーザを認証している前記コンピュータデバイスのユーザから受信されるとき、前記第 1 のユーザが認証された認証レベルを有すると判定され、

前記入力の前記第 1 のユーザを認証している前記コンピュータデバイスのユーザから受信されないとき、前記第 1 のユーザが認証されていない認証レベルを有すると判定され、

前記セキュリティ方針オプションが制限されると判定され、前記認証レベルが、閾値レ

50

ベルより低いか同じレベルであるときに、前記機能の実行が取り消されるステップとを含むことを特徴とするコンピュータ可読記録媒体。

【請求項 27】

ユーザのそれぞれがアイデンティティ及び表示名を有するピアツーピアコラボレーションシステムにおけるエンドポイントを提供するコンピュータデバイスにおいて実行されるときに、方法を実行するコンピュータ実行可能命令を記録するコンピュータ可読記録媒体であって、前記方法は、

前記コンピュータデバイスのユーザと異なる第1のユーザと関連付けられた機能を引き起こすように適用されたイベントに応答して、

前記第1のユーザの認証レベルを判定するステップであって、前記認証レベルは、(1) 手動で認証済み、(2) 企業内で証明済み、(3) 企業間で証明済み、及び(4) 未認証を含むセットから選択された認証レベルを含み、前記証明されたレベルは、前記手動で認証済みが最高のレベルであるステップと、

前記認証レベルと前記セキュリティ方針に基づいて、前記イベントに選択的に応答するステップであって、前記セキュリティ方針は、少なくとも許可オプションと、制限オプションと、警告オプションとを有するステップとを含み、

前記選択的に応答するステップは、

前記セキュリティ方針オプションが制限されると判定され、前記認証レベルが、閾値レベルより低いか同じレベルであるときに、前記機能の実行が取り消されるステップと

前記セキュリティ方針オプションが警告されると判定され、前記認証レベルが、閾値レベルより低いか同じレベルであるときに、前記グラフィカルユーザインターフェース上に、前記イベントに応答して前記機能を実行すると同時に、前記第1のユーザの表示名を表示するステップであって、前記表示するステップは、前記第1のユーザの認証レベル上に警告を表示するステップを含むステップと、

前記第1のユーザが証明されていないと判定されると、

前記第1のユーザについての情報を表現するグラフィカルユーザインターフェースを表示するステップであって、前記グラフィカルユーザインターフェースは、前記第1のユーザを認証している前記コンピュータデバイスのユーザから入力を受信するように適用された入力エリアを含むことを表示するステップと、

前記入力が前記第1のユーザを認証している前記コンピュータデバイスのユーザから受信されるとき、前記第1のユーザが認証された認証レベルを有すると判定されるステップと、

前記入力が前記第1のユーザを認証している前記コンピュータデバイスのユーザから受信されないとき、前記第1のユーザが認証されていない認証レベルを有すると判定されるステップと

を含むことを特徴とするコンピュータ可読記録媒体。

【請求項 28】

前記第1のユーザの前記認証レベルを判定するステップは、前記コンピュータデバイスと関連付けられたメモリ内の連絡先データストアにアクセスすることを含むことを特徴とする請求項 27 に記載のコンピュータ可読記録媒体。

【請求項 29】

前記方法は、さらに、前記イベントの前に、前記第1のユーザとの通信に応答して、前記第1のユーザを前記連絡先データベース内の前記連絡先として記録するステップを含み、前記記録するステップは、少なくとも、アイデンティティと、表示名と、前記第1のユーザの認証レベルとを記録することを含むことを特徴とする請求項 28 に記載のコンピュータ可読記録媒体。

【請求項 30】

前記第1のユーザの認証レベルを判定するステップは、

前記第1のユーザについての情報を表現するグラフィカルユーザインターフェースを表示するステップと、前記第1のユーザを認証している前記コンピュータデバイスのユ

10

20

30

40

50

ーザから入力を受信するように適用された入力エリアを含むステップと、

前記入力が、前記第1のユーザを認証している前記コンピュータデバイスのユーザから受信されるとき、前記第1のユーザが認証された認証レベルを有すると判定されるステップと

を含むことを特徴とする請求項29に記載のコンピュータ可読記録媒体。

【請求項31】

前記第1のユーザの認証レベルを判定するステップは、

ネットワーク管理者からピアツーピアコラボレーションシステムのユーザの認証レベルについての情報を受信するステップと、

前記受信された情報が、前記第1のユーザが証明されたと識別するとき、前記第1のユーザの認証レベルが証明されていると判定するステップとを含むことを特徴とする請求項29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】

【0001】

本発明は、ピアツーピアコラボレーションシステムに関し、認証関係を管理し、これらの関係を協働者に自動的に表示するための方法及び装置に関する。

【背景技術】

【0002】

政府及び他の機関は、ネットワーク化されたコンピューティングシステムのユーザとして、許可されていない開示からデータを保護する上でのセキュリティの価値を理解している。特に政府機関は、データ交換の参加者が自分の通信の相手のアイデンティティについて保証されるように、プライバシーのためにデータを暗号化し、ユーザを強力に認証するために大変な苦労を重ねてきた。更に多くの組織は、ファイアウォールの内側にあるデータに外部ユーザがアクセスするのを妨げるハードウェア障壁またはソフトウェア障壁のどちらかであるファイアウォール付きのきわめて細分化されたプライベートネットワークを実施してきた。

【0003】

この「アイランド」ネットワークセキュリティ手法の欠点は、それにより他の組織の正規のユーザとのデータの共用が複雑化するという点である。現在の組織モデル及びビジネスモデルは、ファイアウォールを越えた対話機能及びコンサルタント、作業員、及び他の提携組織の人に対する相互依存性を要求する。これらの人のすべては出現する機会及び脅威に迅速に対応するために毎日の業務の中で協調し、協働もしなければならない。今日組織の境界を越えるニーズは従来にも増して大きい。一方では強力なデータ保護と他方ではデータを共用（share）するニーズの間の——この緊張の結果が協働に対する障害を生じさせる場合がある。多くの組織は、例えば多くの場合安全ではないeメールとしてデータを送信するなど、まったくセキュリティ対策を回避している。他は単に処置を講じていない場合がある。

【0004】

多くの組織は、データアクセス許容度の問題を解決するための、誠実ではあるが場当たりの手法を講じている。選択されたプロトコルを使用する外部者によるアクセスを可能にするために、ファイアウォール内にポートを開くネットワーク管理者もいる。遠隔地に居る既知の作業員がファイアウォールの内側の特定のシステムに入る（tunnel into）ことができるようにする仮想プライベートネットワーク（VPN）を設ける他の管理者もいる。

【0005】

なお、他の組織はDMZ（「非武装地帯」）として知られるネットワーク領域内に1つまたは複数のシステムを確立する。DMZは組織のメインファイアウォールの外側にあり、組織の内部及び外部の人々がアクセスできる。例えば、ウェブサーバは多くの場合DMZ内にある。

10

20

30

40

50

【0006】

これらの解決策の1つの問題は、それらがネットワーク管理者による顕著な関与を必要とするという点である。更にいったんこれらのシステムが実現されると、管理者にはそれらを維持するという重荷が残される。これらのような解決策は管理要員に高度の責任及び信任も負わせる。このような解決策は管理上の妥協の可能性を無視し、多くの場合きわめてカスタマイズされ、十分に解説されていない。いくつかのカスタマイズされた解決策を確立する人物が組織を離れてしまうと、他の人がシステムがどのように構成されているのか分からない可能性がある。これは、さもなければ安全なネットワークのセキュリティホールにつながる可能性がある。

【0007】

これらの解決策の別の一式の問題が故障及び集中攻撃に対するそれらの脆弱性である。データのロバスト性、データ可用性、及び仲間の協働者を安全に認証する方法は安全なシステムの前提条件である。暗号保護の強度に関わりなく、情報はオンデマンドで入手可能でなければならない。

【0008】

優れたセキュリティを維持しつつもIT管理者に大きく依存することを回避するために、安全なピアツーピアコラボレーションシステムが開発されている。これらの1つが、`http://www.groove.net`に詳しく説明されている、マサチューセッツ州019015、ビバリー、カミングスセンター スィート535Q、100 (100 Cummings Center Suite 535Q, Beverly, MA 019015) のグループネットワークス社 (Groove Networks, Inc.) により開発、販売されているグループ (Groove) コラボレーションシステムである。特許文献1も参照すること。このシステムでは、協働者は「アイデンティティ」を含むアカウントを作成できる。アイデンティティはそれぞれに秘密鍵と公開鍵が付いた2つの暗号「鍵の組」である「暗号ペルソナ (cryptographic persona)」から構成されている。これらの鍵は他のアイデンティティとの安全な通信を実現するために使用される。協働者は、アイデンティティを使用すると、「共用空間 (shared space)」と呼ばれる臨時の協働場所を作成できる。共用空間は実質的には、共用される領域、つまり他の協働者がアクセスできるユーザのコンピュータメモリ内の安全なパーティションである。このような共用空間は、グループコラボレーションシステムの一部であるユーザインタフェースを使用して作成できる。共用空間は、ファイルフォルダ、または別の種類のファイル共用仕組みを作成することによってなど他の方法でも作成できるであろう。本明細書で使用される「共用空間」は、それがどのように作成されるのかには関係なくこのような共用される領域を意味する。共用空間を作成する協働者は、次に、他のメンバーに該共用空間に加わり、データ及びツールを該空間へ導入するように招待することができる。グループコラボレーションシステム (以下、グループシステム) は、それがネットワーク管理者にファイアウォール内に特別なポートを開くように要求しなくてもファイアウォールを通して通信できるように標準的なウェブ・プロトコルを使用する。更に、組織は集中管理、中継機能、統合、及びグループシステムの使用に対する制御のためにグループシステム用サーバを配備することができる。

【0009】

セキュリティを提供するために、グループシステムは192ビットの暗号を端末で使用してすべてのユーザアカウント、共用空間及びそのコンテンツを自動的に暗号化する。更に、ネットワークを介して送信される共用空間内のすべてのコンテンツと活動も暗号化され、共用空間の他のメンバーによってのみ解読できる。しかしながら、たとえすべての通信が暗号化され、完全性が保護されていても、ユーザが、彼らが通信している現実世界の人が、ユーザが自分が通信していると考えている実際の人である、及び人のままであることを容易に検証できる場合にだけ、データの起源の完全性は保証できる。

【0010】

これを行うために、グループシステムは認証と呼ばれるプロセスを使用する。このプロ

10

20

30

40

50

セスは、連絡先の「デジタル指紋」を比較することを含む。特に、グループシステムは各アイデンティティに関連付けられた一意の明白なデジタル指紋を自動的に生成する。デジタル指紋は連絡先の公開鍵から導き出され、（読みやすさのために句読点と共に）文字と数の長いランダムに見える列としてユーザに提示される。二人の人は、自分達が互いに報告している指紋に対して、彼らが互いについて見ている指紋を比較することによって互いのアイデンティティを手動で認証できる。

【0011】

例えば、第1のユーザが第2のユーザに共用空間に加わるように誘うと仮定する。該第1のユーザは自分の指紋を該第2のユーザに報告し、第2のユーザは、第2のユーザがメンバーパネルの第1のユーザの連絡先情報を開く時に表示される指紋に照らして報告された指紋をチェックする。それから、第1のユーザと第2のユーザはこの動作を繰り返し、今回は第1のユーザが第2のユーザの指紋を手動で認証する。後述されるように管理されたドメインの中で管理者により「証明」を実行することも可能である。

【特許文献1】米国特許第6,446,113号明細書

【特許文献2】William D. Tierney及びKenneth G. Mooreによって2001年10月24日に提出され、「ピアツーピアコラボレーションシステムを管理するための方法及び装置 (METHOD AND APPARATUS FOR MANAGING A PEER-TO-PEER COLLABORATION SYSTEM)」と題される同時係属中の米国特許出願第10/036,275号明細書

【非特許文献1】<http://csrc.nist.gov/encryption/aes/>

【非特許文献2】FIPS 140-2

【非特許文献3】1985年のコンピュータサイエンス (Computer Science 196)、10-18ページのT. ElGamal、暗号作成術の進歩-CRYPTO'84の会報、スプリングerverlagレクチャーノート (Springer Verlag Lecture Notes) の「公開鍵暗号システム及び離散値対数に基づいたシグナチャ方式 (A public key cryptosystem and a signature scheme based on discrete logarithms)」と題される記事

【発明の開示】

【発明が解決しようとする課題】

【0012】

しかしながら、認証手順を用いたとしても、依然として認証されていない通信が発生することはありうる。この信頼性の欠如は、ユーザが認証プロセスを実行する時間をかけず、それによりシステムをなりすまし (spoofing) 及び他の攻撃に開けてしまうために発生する。

【課題を解決するための手段】

【0013】

本発明の原理に従って、適切なユーザ対データの関連付けが、ユーザが共用空間の他のメンバーを容易に認証し、情報を暗号化することができるようにする簡略化された最小のユーザインタフェースによって（コンピュータ、PDA、ゲームコンソール、セットトップボックス、または他の電子装置などの）複数のデバイスにおいて維持される。特に、ユーザが他のユーザを認証するために時間をかけない場合にも認証された関係を自動的に構築するためのサポートが提供される。いったんこれらの関係が確立されると、それらは共用空間と関連付けられたデータに記憶される。ユーザがその共用空間に入り、その空間内の連絡先を見ると、それぞれの連絡先に独特なアイコンが付随している。これらのアイコンは瞬時にその連絡先のその認証ステータスを識別する。

【0014】

ある実施態様では、ユーザは「暗示的に」認証されてよい。例えば、第1のユーザが初めて第2のユーザと通信する時、第1のユーザが第2のユーザを手動で認証しなくても、

セキュリティシステムは依然として第1のユーザのアカウントの中の第2のユーザの連絡先情報を覚えている。その連絡先が第1のユーザのアカウントに残る限り、第1のユーザは、第2のユーザとのすべての将来の通信が同じ第2のユーザと実施されることを保証される。この暗黙の認証をサポートするためにセキュリティシステムは「名前一致解決」と呼ばれる技法を使用する。ユーザインタフェースは、類似した名称の連絡先が提示されたときにユーザに警告する機能を含んでいる。したがって、第1のユーザは、もし別のユーザが第2のユーザと同じ名前を使用することにより第2のユーザを装っているときには十分に警告される。

【0015】

別の実施態様では、名前の一致 (c o n f l i c t) は「エイリアシング (a l i a s i n g)」と呼ばれる技法で解決される。

10

【0016】

更に別の実施態様では、認証に対する一貫した手法を提供するためにセキュリティ方針を確立できる。これらの方針はユーザによって設定できる、あるいは代わりに方針は管理者によって設定できる。方針は、好ましい認証方法、あるいは必要とされる認証方法に対処する。選択された方針に基づき、コラボレーティブシステムは、ユーザが、管理者によって証明されていない人、あるいは手動で認証されていない人と通信しそうになるとユーザに警告することができる。

【0017】

更に別の実施態様では、選択された方針に基づき、コラボレーティブシステムは、連絡先のアイデンティティが管理者によって証明されていないか、あるいは手動で認証されていない限り、個人との通信を禁止できる。

20

【発明を実施するための最良の形態】**【0018】**

図1Aは、前述したグループコラボレーションシステムなどのコラボレーティブシステム100のブロック略図である。図1Aはコンピュータ、PDA、ラップトップコンピュータ、セットトップボックス、ウェブ・イネーブル携帯電話、または他の通信装置である場合がある2台の協働するデバイス102と104を示している。2台の協働装置だけが図示されているが、追加のデバイスも存在してよい。グループソフトウェアがこのようなデバイスにロードされると、それはそれぞれデバイス102と104内にデータベース112と116を作成する。これらのデータベースはそれぞれ協働者によって処理されているデータのローカルコピーを保持する。後述されるように、データベース112と116も協働するデバイス102と104のそれぞれの動作に関する情報を保持する。

30

【0019】

コラボレーティブソフトウェアは、それぞれデバイス102と104の中にトランシーバ110と114などのトランシーバも作成する。各トランシーバは、矢印106によって概略的に示されるように協働者間の「デルタ」と呼ばれるデータ変更要求の作成及び送信を担当する。通常、これらのデータ変更要求は図1Aに図示されるようにインターネット108上で送信されるが、それらはLANネットワークなどの別のネットワーク上で送信することもできるであろう。データ変更要求はシステムに協働者を追加する、及びシステムから協働者を削除する、ならびにデータコピーを同期させておくためにそれぞれの協働するデバイス内でローカルデータコピーを更新するなどの多くの目的のために使用される。

40

【0020】

図1Aは、管理ドメイン及び管理されるアイデンティティを確立するために管理要員が使用できる管理サーバ118も示している。また、通常、管理サーバ118は、矢印120と122により概略的に示されるように、インターネット108などのネットワークを介して協働するデバイスと通信する。管理サーバの動作及びドメインを作成し、管理する上でのその使用は、参照により出願が全体として本明細書に取り込まれている特許文献2に更に詳細に説明されている。

50

【0021】

前述したコラボレーティブソフトウェアを使用するために、ユーザはアカウントを確立する。このようなアカウントは、ログイン名とパスワードなどのユーザについての情報を含み、eメールアドレス及びユーザに連絡する他の方法などの追加の情報を含む場合がある。一般的には、アカウントは、アイデンティティファイル等の他のシステムに共通して見られるユーザ情報ファイルに対応する。アカウントは、コラボレーティブシステムによって維持されるデータベース112または116などのデータベースに記憶される情報を含む。このようなデータベース124は図1Bに更に詳細に図解されている。該システムデータベース124は、同様にアカウントについての特定のユーザプライベートメタデータを記憶するアカウントデータベース126を含む。ユーザが、オフィスで使用するための職業上のアイデンティティと写真や休暇の計画を共用するような目的のために家族と友人と使用するための個人用アイデンティティなどの複数のアイデンティティを持つ可能性がある。メタデータは、アカウントによって保持される1つまたは複数のアイデンティティ130及び該アイデンティティと関連付けられる秘密鍵132を含む。各アイデンティティは「アイデンティティ鍵組」と呼ばれる2つの鍵の組に関連付けられる。メタデータは更にアカウントに関連付けられた共用空間ごとに識別子134を含む。

10

【0022】

アカウントデータベース126は、アイデンティティごとの連絡先情報を記憶する連絡先記憶部136も含む。連絡先ごとの情報は個人のアイデンティティ表示名、電話番号、eメールアドレスと、職業上のアイデンティティ表示名、電話番号、eメールアドレス等を含む。連絡先情報はコラボレーティブシステムの外部のアイデンティティ間のメッセージを検証し、暗号化するために使用される公開／秘密鍵の組140の公開鍵などの何らかの公開情報も含む。連絡先情報は、連絡先の認証ステータスを示すステータスフラグを備えるメタデータ142も含む。このメタデータは連絡先の「証明書チェーン」の中の全証明書の最低有効期限も含む（連絡先は更に別の連絡先等により同様に証明される別の連絡先によって証明されてよい）。性能の理由から、コラボレーティブシステムは、一度証明書を確証してから、最低有効期限を記憶するだけである。後に、連絡先がユーザインタフェースに表示される前に、最低有効期限が確認されるが、証明書チェーンは確証し直される必要はない。この手順によりコラボレーティブシステムは証明書の満了という点で最新となることができる。

20

30

【0023】

ステータスフラグは、連絡先が未認証であるかどうか、手動で承認されたかどうか、あるいは管理者によって証明されたのかどうかを示す。後述されるように、各連絡先の認証ステータスが直ちに明らかになるように、これらのフラグにより、ユーザインタフェース上に選択されたアイコンが表示される。本発明の原理に従って、及び後述されるように、メタデータは名前及びユーザが同じ表示名を有するアイデンティティを認識し、対処できるようにする名前一致情報も含む。

【0024】

コラボレーティブシステムは、ユーザが、ユーザが協働できる個人用領域である共用空間を作成し、共用空間に加わることができるようにする。ユーザは、通常、それぞれの空間が（「メンバー」と呼ばれる）参加者の別の集合を有する複数の空間にアクセスできる。更に、各ユーザは仕事でのワークステーション、家庭でのデスクトップコンピュータ、及びモバイル使用のためのラップトップなどの複数のデバイスでいくつかの共用空間を維持できる。共用空間は、共用空間のメンバーによって寄与されるデータとツールを含み、動的である。即ち、ユーザは加わり、離れる。データは増大し、縮小する。ツールは去来する。共用空間の有効期間は束の間である（数分に過ぎない）か、あるいは共用空間は連続的に永久に持続できる。

40

【0025】

このようなコラボレーティブシステムにおいてセキュリティを維持するために、ユーザアイデンティティは認証及び暗号化の技法によりアイデンティティを使用して、現実世界

50

の人と密接に関連付けられ、それによりデータの守秘性と完全性を、それがシステムを通じて伝搬するにつれて保証する。認証は、2つの別個のステップでコラボレーティブシステムにより実行される。第1のステップでは、システムは、電子アイデンティティを、それらが表す人間のユーザと正しく関連付けることによってシステム内のユーザを認証する。いったんこれが行われると、コラボレーティブシステムは（ファイル、チャットメッセージ、キーストロークに対する修正などの）システム内の動作を電子アイデンティティに正しく関連付けることにより第2の認証を実行する。

【0026】

ユーザの自分のコンピュータアイデンティティとの初期の関連付けは、コラボレーティブソフトウェアが最初にデバイス上で構成される時に始まる。第1の構成ステップは、そのユーザを定義する属性を含むアカウント記憶部（データベース126などの暗号化されたXMLオブジェクト記憶部）を作成することである。いくつかのアカウント属性が概略XML形式で以下に一覧表示されている。

account

{identities}

identity_1

{spaces}

private signing key (for Identity 1)

private encryption key (for Identity 1)

storage master key

contact information (for Identity 1)

id-url

public key algorithms

public signing key

public encryption key

devices

relay server

status word

identity_2

{known contacts}

【0027】

このサンプルXMLファイルでは、それぞれの字下げが階層を示し、アカウントは、私的なアイデンティティと職業上のアイデンティティなどの複数のアイデンティティを含んでよい。各アイデンティティは、鍵及び連絡先情報のセットを含む独自の一意のパラメータを有している。この鍵は文書に署名するために使用される公開／秘密鍵組の一部である秘密署名鍵を含む。各連絡先は、URL、公開鍵アルゴリズム、公開署名鍵、公開暗号鍵、デバイス、連絡先によって使用される中継サーバ、及び前述されたステータスワードなどの連絡先識別情報を含む追加の情報を含む。

【0028】

アカウント記憶部を作成する構成プロセスは、ユーザに、大文字と小文字、句読点、及び数字を含み、それを推測するのが困難にする「パスフレーズ」を作成するように依頼する。このパスフレーズは、次に、同様にアカウント記憶部内の情報を暗号化するために使用される（「記憶部マスタ鍵」と総称される）個々の共用空間のための鍵を復号するために使用されるマスタ鍵を保護するために使用される。

【0029】

より具体的には、システムは、URL `http://rfc-2898.rfcindex.com/rfc-2898-27.htm` のRFC 2898、及びRSAラボラトリーズ社（RSA Laboratories, Inc.）によって維持され、`http://www.rsasecurity.com/rsalabs/pkcs/pkcs-5` に説明されている規格PKCS#5 第2版に説明されるパスワードをベースに

10

20

30

40

50

した鍵導出機能#2(PBKDF2)などのパスワードベースの鍵導出機能に対する入力としてランダムな「ソルト」(salt)値と共にパスフレーズを使用する。この機能は記憶部マスタ鍵を暗号化するアルゴリズムと共に使用するための対称鍵を作成する。この対称鍵はメモリに一時的に存在するに過ぎず、使用後はゼロにされ、絶対に電線で送信されない。別のデバイスで使用される同じパスフレーズは、PBKDF2機能に追加されたランダムなソルト値のために別の対称鍵を作成するであろう。ソルト値はパスワードが変化するたびに変化するため、パスフレーズに対するディクショナリ攻撃もPBKDF2入力にソフト値を追加することで抑止される。更に、1秒の10分の1の遅延をプロセスの中に作りこむ。この遅延は正規のログインの間にはほとんど目立たないが、それはディクショナリ攻撃の間に大きな量になり、それらを実行不可能にする。

10

【0030】

例示として、記憶部マスタ鍵を暗号化するために使用されるアルゴリズムは、高度暗号化規格アルゴリズム(AES)などのアルゴリズムとなるであろう。AESは、対称暗号化アルゴリズムのための米国で承認された規格であり、DESアルゴリズムに代わる。AESアルゴリズムは最初はラインダール(Rijndael)と呼ばれ、二人のベルギーの暗号作成者によって作成された。それは非特許文献1及び2に詳しく説明されている。記憶部マスタ鍵は他の鍵を保護するために使用される。2つの主要なマスタ鍵があり、両方ともAESアルゴリズムを用いた暗号化に使用される256ビットの対称鍵である。一方のマスタ鍵はユーザセキュリティメタデータ鍵(ユーザの私的な署名及び復号鍵)を保護し、他方のマスタ鍵はユーザの暗号鍵(共用空間データを保護する鍵)を保護する。各共用空間に記憶されるデータは、独特の(データベース単位の)192ビットの対称AES鍵により暗号化される。対応する(データベース単位の)導出された192ビットのHMAC鍵はデータベースの完全性保護を提供する。

20

【0031】

秘密鍵もアカウントにより保持されるアイデンティティと関連付けられる(アカウントは複数のアイデンティティを保持できる)。各アイデンティティは(「アイデンティティ鍵組」と呼ばれている)2つの鍵の組と関連付けられる。(1)共用空間のコンテキストの外でメッセージ(インスタントメッセージ及び共用空間招待/受諾)に署名するために使用される2048ビットの非対称RSA鍵組(RSAはRivest、Shamir、及びAdlemanの略語である――初めての実際的な公開鍵暗号システムを発明した三人の暗号作成者にちなんで。RSA公開鍵アルゴリズムは今日最も一般的に使用されている公開鍵アルゴリズムである。それは<http://www.rsasecurity.com/>に十分に説明されている)。

30

【0032】

この鍵の組は(1)ESIGNアルゴリズムを使用する空間単位の署名鍵、及び(2)(共用空間のコンテキストの外でメッセージを保護するために使用される対称鍵の)暗号化のために使用される2048ビットの非対称ElGamal鍵組を使用する空間単位の署名鍵にも署名する。ESIGNは日本で開発された特許権使用料が無料の公開鍵署名アルゴリズムである。それは現在IEEEによって標準化され、<http://info.isl.ntt.co.jp/esign/>に説明されている。ElGamalアルゴリズムは、RSA公開鍵アルゴリズムの代替策を提供する公開鍵暗号化アルゴリズムである。それは非特許文献3に詳細に説明されている。

40

【0033】

ユーザが共用空間を作成すると、コラボレーティブシステムが該空間についての情報を空間に特殊なデータベース鍵で保護されている(図1Bのデータベース144、146、及び148などの)別個の共用空間データベースに追加してから、その空間のための多様な鍵を作成する。これらの後者の鍵も共用空間セキュリティメタデータベースに追加される。後に、ユーザが共用空間を開くと、記憶部マスタ鍵が該共用空間データベースセキュリティメタデータ内に含まれる鍵を解読するために使用される。これらの後者の鍵は、記憶されている共用空間データを暗号化する192ビットの空間単位の対称鍵である

50

記憶部データベース暗号鍵を含む。この鍵は、記憶されている空間データの完全性を保護する192ビットの空間単位の対称鍵も導出する。空間は、空間のためのグループ暗号鍵を動的に導出する共用されている192ビットの対称鍵、及び「デルタ」と呼ばれる送信装置を介して電話で送信される共用空間データの完全性を保証するグループメッセージ認証(MAC)鍵である、空間のためのグループ鍵を備えている。空間グループ鍵は、後述される招待プロトコルの間に新しいメンバーに配布される。空間グループ鍵は、メンバーが空間から招かれなくなると、鍵を付け替えられる(変更される)。

【0034】

共用空間データベースはメンバーシグナチャ秘密鍵も含み、それはデルタと共用空間のコンテキストの中で送信されるデルタとメッセージに署名するためにこの空間のこのメンバーによって使用される1536ビットの非対称E S I G N鍵である。この鍵の組の公開の半分は後述される「メンバー追加」デルタプロトコルの中で送信される。全メンバーの公開鍵も共用空間データベースで維持される。共用空間データベースは、更に、共用空間内のメンバーの各組の間での組単位の鍵の確立のためにこの空間のこのメンバーにより使用される2048ビットの非対称鍵である共用空間メンバーD i f f i e - H e l l m a n秘密鍵を含む。該D i f f i e - H e l l m a nアルゴリズムは、URL <http://www.rsasecurity.com/rsalabs/pkcs/>に位置するウェブサイトのRSAラボラトリーズで入手可能なPKCS #3に詳細に説明されている。この鍵組の公開半分はユーザのアイデンティティシグナチャ秘密鍵によって署名され、後述される招待プロトコルのグループ全体に配布される。全メンバーのD i f f i e - H e l l m a n鍵の公開部分もこのデータベースに維持される。

【0035】

共用空間データベースは組単位の鍵も含む。特に、各ユーザは、2つの他の一時的な組単位の鍵を導出するために共用空間の各メンバーと独特の192ビット対称鍵を共用する。導出された鍵は、空間の中の単一のユーザをターゲットとした(デルタフェッチ要求などの)メッセージを(192ビットのAESアルゴリズムを使用して)暗号化し、(192ビットのHMAC S H A - 1ハッシュアルゴリズムを使用する。このアルゴリズムの詳細は<http://www.itl.nist.gov/fipspubs/fip180-1.htm>に位置するウェブサイトのFIPS 180-1に説明されている。)完全性保護するために使用される。空間メンバー組単位の鍵は(空間メンバーD i f f i e - H e l l m a n鍵を使用して)空間内のメンバーの各組の間でのD i f f i e - H e l l m a n鍵の一致から由来する。

【0036】

この時点で、ユーザは電子アイデンティティを作成したことになる。しかしながら、他のユーザは、認証と呼ばれるプロセスにより、作成されたばかりの電子アイデンティティが真にユーザに属していることを依然として検証しなければならない。そうでなければユーザになりすました誰かが「マンインザミドル」攻撃をしかけ、ユーザと他のユーザの両方になりすますことによりユーザと別のユーザの間のすべての通信を傍受することができるであろう。

【0037】

他のユーザを認証できる複数の方法がある。例えば、ユーザは他のユーザを手動で認証できる。別のユーザを手動で認証するためには、ユーザは他のユーザの公開鍵の「デジタル指紋」を目視で調べる。デジタル指紋はユーザの公開鍵をハッシュするために暗号的に強力なハッシュアルゴリズムを動的に使用して作成される16進文字列である。本発明と共に使用するのに適しているあるハッシュアルゴリズムが前述したS H A - 1アルゴリズムである。公開鍵の代わりにデジタル指紋が使用される理由とは、それらが、人にとって公開鍵より読み易いが同時に安全であるためである。コラボレーティブシステムがデジタル指紋を作成し、メッセージ上のシグナチャを検証するために使用するユーザの公開鍵は、同様に中央ディレクトリサーバに、あるいはローカルディレクトリサーバに記憶されているユーザの連絡先情報の中に記憶されており、該情報は他のユーザが容易に入手できる

10

20

30

40

50

。連絡先情報は、他者に送信され、彼らを共用空間に加わるように招待する「招待状」にも含まれている。招待状は更に詳しく後述される。このようにして公開鍵情報はデジタル指紋を作成するために容易に入手できる。

【0038】

手動認証は、彼らの指紋値を得るために電話呼などの帯域外手段を使用して人に連絡することを含む。特に、コラボレーションシステムは各ユーザのデジタル指紋を自動的に計算する。この指紋はそのユーザに表示できる。更に、新しい連絡先がアカウント情報に追加されると、コラボレーティブシステムはその連絡先のデジタル指紋を計算するためにこの連絡先の公開鍵情報を使用する。この後者のデジタル指紋は図2に画面場面が描かれている認証画面に表示される。ユーザは、次に、帯域外手段を使用してその連絡先に連絡し、その連絡先のデジタル指紋を要求する。それから、ユーザは要求されたデジタル指紋を認証画面に表示されたデジタル指紋と比較し、指紋が一致した場合には、「Authenticated as (として認証済み)」ボックスにチェックマークをつけることで、この連絡先が認証された旨を示す。連絡先が特定の名前で認証されることに注意する。認証のプロセスは、認証されたユーザ(M)による以下の攻撃を妨げる。つまりユーザAはユーザMを認証する。今ユーザAはMを認証アイコン付きで認証済みとして見る。認証済みのユーザMは今別のユーザBの表示名に一致するために自分の表示名を変更する。ユーザAは今Mの連絡先の隣であるがBの表示名が付いた認証アイコンを見る。このようにして、ユーザAは、事実上ユーザMと通信している時に、自分が認証済みのユーザBと通信しているように「スプーフィング」される。

10

20

【0039】

ユーザの中には「管理された」環境に属しているユーザが居る。これらの環境では、管理者は管理サーバを用いていくつかの方針態様を設定する。例えば、管理者は「ドメイン」レベルまたはグループレベルで方針を設定してよい。ドメイン単位及びグループ単位の方針管理はより大きな環境でセキュリティ制御及び操作パラメータを設定する上で柔軟性を与える。方針制御はパスフレーズ強度、特定のツールまたはソフトウェアバージョンへの制限、及び共用空間数または共用空間を作成する能力に対する制限を含む。

【0040】

管理された環境では、管理者は管理サーバを使用し、管理されたエンティティへ方針データを分散することによりデバイス及びアイデンティティを管理する。例えば、機密保護方針は組織内の(ドメインの指名された下位区分である)管理ドメインまたはグループごとに個別に設定できる。方針は、パラフレーズの構成及び期限切れのような事柄を制御する管理されたデバイスの動作、及びメンバーが複数のアカウントを作成できるか、それとも管理されていないアイデンティティを作成できるのかを設定する。ユーザを、特定のツールまたはソフトウェアバージョンのダウンロードに制限することができ、彼らを特定の出版者からの署名された構成要素だけをダウンロードするように制約することができる。したがって、管理された環境は組織全体に亘って有意義な方針を構造化する上で大きな柔軟性を提供する。

30

【0041】

ユーザが管理されたアイデンティティを有する管理された環境では、コラボレーティブシステムは、「証明機関」によって提供される証明書(署名された連絡先情報)に依存することによって自動的な認証をサポートする。例えば、グループエンタープライズマネージメントサーバ(Groove Enterprise Management Server)は証明機関として機能し、コラボレーティブソフトウェアは(ローカルに作成された公開鍵を含む)ユーザ連絡先情報を管理サーバに、それらが管理サーバによって証明できるように提示する。企業内の各管理サーバ管理ドメインは証明機関としての役割を果たす(管理サーバは複数の管理ドメイン、したがって複数の証明機関を有する)。証明機関の公開鍵はそれらの証明書と共にユーザに安全に送信される。これは、ユーザに、エンタープライズマネージメントサーバの証明機関を自分達の共通の証明機関として使用することにより彼らのドメイン内で互いを認証するための帯域内手段を与える。相互ドメイン

40

50

認証は、無関係の管理サーバドメインの公開鍵を含む相互ドメイン証明書を使用して可能にされる。管理サーバ管理者は、この機能が必要とされる場合これらの証明書を管理する。

【0042】

コラボレーティブシステムがどこに連絡先名を表示しようとも、「証明／認証アイコン」と呼ばれている認証インジケータがその認証ステータスを示す名前に先行してよい。認証インジケータは連絡先と共に、該連絡先が手動で認証されたかどうか、あるいはユーザが管理されたアイデンティティを有しており、連絡先がユーザドメインまたは相互証明されたドメインのメンバーであるかどうかを表示する。連絡先アイデンティティは、それが手動で認証されない場合、あるいは管理者によって証明されない場合は「未認証」と見なされる。付随する認証アイコン付きの連絡先アイデンティティの説明図は図3に図示されている。図3は、「Kris Jones／マーケティング／カンパニーワン（Company One）」302と名前が指定されたアイデンティティと共に、連絡先の連絡先情報の画面表示300を描いている。この画面の場面は連絡先名に先行して表示される認証アイコン304を描いている。連絡先の認証ステータスを識別する3つのさまざまな認証アイコンがある。これらのアイコンの例示的な例は図4に示されている。

10

【0043】

手動認証インジケータ400は、連絡先が手動で認証された旨を示している。ユーザが手動で認証した連絡先に加えて、このインジケータはユーザ自身のアクティブなアイデンティティ、削除されたアイデンティティ、または無効にされたアイデンティティの隣に表示されている。企業内連絡先の例示的な証明認証インジケータ402も図4に示されている。このアイコンが連絡先名の前に表示されるとき、それは連絡先が管理され、連絡先が該アイコンを見ているユーザと同じドメインに属している、あるいはユーザのドメインと相互証明されたユーザの組織内の別のドメインに属していることを示している。連絡先が証明され、手動でも認証された場合は、証明インジケータではなく、手動認証インジケータだけが表示されるであろう。第3の認証インジケータ404は、企業内連絡先のための証明インジケータである。このアイコンは、連絡先が管理され、ユーザのドメインと相互証明されるユーザの組織の外部のドメインに属していることを示している。ある実施態様では、このアイコン404は企業内認証インジケータ402からそれを明確に区別するためにカラーコード化される。

20

30

【0044】

本発明の原理に従って、コラボレーティブシステムは、「暗示認証」と呼ばれるプロセスによって認証済みの関係を自動的に構築するためのサポートを提供する。このプロセスに従って、第1のユーザがシステム内で初めて第2のユーザと通信する時、たとえ第1のユーザが第2のユーザを手動で認証しなくても、及び第2のユーザが証明されなくても、コラボレーティブシステムは第1のユーザのアカウントデータベースの中に、第2のユーザの公開鍵を含む第2のユーザの連絡先情報を依然として記憶する。その時から、システムは、第1のユーザが、第2のユーザの連絡先情報を使用するすべての将来の通信が同じ第2のユーザと行われることを保証されるように、各連絡先の公開鍵情報をチェックする。しかしながら、第2のユーザは手動で認証されていない、あるいは管理者によって証明されていないために連絡先情報の表示の第2のユーザ名の表示に認証アイコンは先行しない。

40

【0045】

前述された暗示的な認証方式で生じる1つの問題とは、アイデンティティがユーザが選択した名前と関連付けられるという点である。特に、あらゆるアイデンティティが一意であるが、ユーザが自分のアイデンティティをユーザインタフェースディスプレイで表すために選択する名称は一意である必要はない。例えば、二人がアカウントを起動し、自分達の表示名に「Janet」を入力すると仮定する。これは期せずして同じ表示名を使用する2つの一意のアイデンティティを生じさせるであろう。次に別のユーザが公開アドレスブックで「Janet」を探し、図5Aに図示されているようにそれが2度表示されてい

50

ることに気付く可能性がある。図5Aに図示されているように、両方の連絡先とも同一の表示名500と502で表示されるであろう。

【0046】

したがって、同じまたは類似した名前の2つの連絡先が混同される、あるいは詐欺師が別のユーザとの通信を開始するために正規の連絡先の名前を使用することが考えられる。この混同が発生しないことを保証するために、コラボレーティブシステムは「名前一致解決」と呼ばれるプロセスを実行する。このプロセスは、類似した名前の連絡先が提示された時にユーザに警告をするために特殊なユーザインタフェース表示アイコンを提供する。このようにして暗示的な認証が使用されると、ユーザは、あるユーザが同じ表示名を使用することにより別のユーザになりすましている場合、及びなりすましている時に警告されるだろう。

10

【0047】

特に、2つまたは3つ以上の連絡先が同等 (equivalent) の表示名を有する時、コラボレーティブシステムは、前述された認証アイコンの代わりに、図5Bに図示されるような一致する名前504、506を有する2つのアイデンティティの表示名のそれぞれの隣に、疑問符アイコン406 (図4) などの警告を表示する。コラボレーティブシステムは、2つ (または3つ以上の) 「クリーンネーム (clean name)」 が正確に一致する場合表示名を同等と見なす。クリーンネームは (1) 先行するスペースと後続のスペースを削除する、 (2) 複数の埋め込まれたスペースを圧縮する、 (3) 句読点を削除する、及び (4) すべてのテキストを小文字のUNICODE文字に変換することにより連絡先表示名から作成される。

20

【0048】

表示名を比較するプロセスは図6に示されている。特に、前述されたように、各コラボレーティブシステムアカウントは、表示名を含む連絡先とそのメタデータを維持する「連絡先記憶部」を有している。該記憶部は、ユーザの私的な連絡先リスト、共用空間のメンバーリストから得られる連絡先、及びインスタントメッセージの「To (宛て先)」フィールドと「From (送信者)」フィールドからの連絡先を含むがそれらに限られないソースから得られる連絡先を含む。

【0049】

新しい連絡先が記憶部に追加されるたびに、このプロセスはステップ600で開始し、ステップ602に進み、ここで新しい連絡先表示名が、前述されたクリーンネームを作成することによって事前に処理される。このクリーンネームはステップ604で新しい連絡先と共に記憶されるメタデータの一部として含まれる。

30

【0050】

次にクリーンネームは新しい連絡先を含む連絡先記憶部内の全連絡先についてクリーンネームと比較される。このプロセスを促進するために、クリーンネームは連絡先記憶部内の連絡先ごとにメタデータに記憶される。これらの記憶されているクリーンネームは次に新しい連絡先と比較され、名前が同等であるかどうかを判断し、名前一致リストを作成する。特にステップ606では、比較される追加のクリーンネームが連絡先記憶部に留まるかどうかを判断するために確認が行われる。追加名が留まらない場合には、名前連絡先リストは完全なものとなり、プロセスはオフページコネクタ616と618を介して、処理が後述されるように続行するステップ620に進む。

40

【0051】

代わりに、追加名がステップ606で判断されたようにまだ処理されていない場合には、プロセスはステップ608に進み、ここで次の連絡先が連絡先記憶部から取り出され、ステップ610でその連絡先のクリーンネームが新しい連絡先クリーンネームと比較される。

【0052】

ステップ612で判断されたように一致がある場合には、その連絡先はステップ614で規定されるように名前一致リストに追加される。それからプロセスはステップ606に

50

戻り、連絡先記憶部の追加の名前がまだ確認されていないかどうかを判断する。代わりに、ステップ612で一致が検出されなかった場合には、プロセスはステップ606に戻り、連絡先記憶部の追加の名前がまだ確認されていないかどうかを判断する。

【0053】

すべての連絡先名が確認されると、処理は前述されたようにステップ620へ続行する。ステップ620から642で、新しい連絡先クリーンネームと一致するクリーンネームの付いた連絡先のメタデータ内の名前一致ビットが設定されるかどうか判断される。連絡先の名前一致ビットが設定されると、連絡先表示名がコラボレーティブシステムのユーザインタフェース内のどこに、及びいつ表示されようとも、名前一致アイコンが表示される。

10

【0054】

名前一致ビットが設定されるかどうかの判断は、連絡先の認証／証明レベルの比較に基づく。前述されたように、各連絡先には以下の4つの証明レベルの1つが割り当てられる。つまり(1)手動で認証済み、(2)企業内で証明済み、(3)企業間で証明済み、及び(4)未認証。手動で認証済みが最高のレベルである。ステップ606から614で作成された名前一致リスト上の連絡先の場合、これらのレベルはステップ620から628で比較される。ステップ620では、名前一致リストが、リスト上のあらゆる連絡先が処理されていないかどうかを判断するためにチェックされる。連絡先がまだ処理されていない場合は、プロセスはリスト上の次の連絡先が処理のために選択されるステップ622に進む。ステップ614では、選択された連絡先の認証／証明レベルが、処理された連絡先の最高認証／証明レベルを保持する最高証明レベル変数と比較される。選択された連絡先の認証／証明レベルが該変数の値より高い場合には、ステップ626で、変数の値は選択された連絡先の認証／証明レベルに設定され、プロセスはステップ620に戻り、リスト上の追加の名前が処理を必要とするかどうかを判断する。

20

【0055】

ステップ624で、選択された連絡先の認証／証明レベルが最高の証明レベル変数の値より高くないと判断されると、プロセスは、選択された連絡先の認証／証明レベルが最高の証明レベル変数と比較されるステップ628に進み、選択された連絡先の認証／証明レベルが最高の証明レベル変数に等しい場合には、別の変数の値、つまり最高の一致証明レベル変数が、選択された連絡先の認証／証明レベルに設定される。プロセスは次にステップ620に戻り、一致リストの更に多くの連絡先がまだ処理されていないかどうかを判断する。代わりに、ステップ628で、選択された連絡先の認証／証明レベルが最高の証明レベル変数の値に等しくないと判断される場合、プロセスはステップ620に直接戻るだけである。

30

【0056】

最後に、一致する表示名を有する選択された連絡先と関連付けられるメタデータの名前一致ビットを設定するために、一致リスト上の一致が再び調べられる。このプロセスはステップ636から644で実行される。特に、ステップ620では、まだ処理されていない追加の名前がないと判断されると、プロセスは、オフページコネクタ632と634を介して、名前一致リストが、リスト上のあらゆる連絡先がまだ処理されていないかどうかを判断するためにチェックされるステップ636に進む。

40

【0057】

更に多くの連絡先がまだ処理されていない場合には、プロセスは、リストの次の連絡先が選択されるステップ640に進む。次に、ステップ642で、選択された連絡先の認証／承認レベルがステップ620から630で求められた最高の証明レベル変数の値と最高の一致証明変数の値と比較される。選択された連絡先の認証／証明レベルが最高の証明レベル変数の値未満である、あるいは最高の一致証明レベル変数の値に等しい場合には、プロセスは、選択された連絡先のメタデータの名前一致ビットが設定されるステップ644に進み、プロセスは追加の連絡先を処理するためにステップ636に戻る。そうでなければ、ステップ642でプロセスは追加の連絡先を処理するために直接ステップ636に戻

50

る。すべての連絡先がステップ636で決定されたように処理されると、ステップ638でプロセスは終了する。

【0058】

前述した認証／証明レベルの比較は、「名前スプーフィング」攻撃者からのサービス攻撃の拒否を緩和するために実行される。例えば、悪意のあるユーザ(M)が、表示名が本物のユーザQの表示名に一致する仮のアイデンティティQ'を作成することにより、認証済みの(あるいは相互証明された)ユーザPとQとの間の通信で混乱を生じさせようとすると仮定する。次にユーザMは、ユーザQを装ってインスタントメッセージをユーザPに送信する。連絡先QとQ'の表示名が一致するため、認証／証明レベルの比較を行わないと、ユーザPは、名前一致アイコンが連絡先QとQ'の表示名と共に表示されるのを見るであろう。ユーザPは、次に、後述されるように名前一致を解決することが必要とされるであろう。このプロセスは、Mが、すべてが本物の連絡先Qと同じ表示名を使用するアイデンティティQ'、Q'、Q'からメッセージを送信し続ける場合には再三再四繰り返されなければならないであろう。しかしながら、前述された追加の認証／証明レベルのチェックを行うことにより、コラボレーティブシステムは連絡先Q'より連絡先Qを好み、連絡先Qの表示名と関連付けられた名前一致アイコンを表示しないだろう。したがって、表示はユーザPが危険な連絡先を容易に識別できるようにする。

10

【0059】

連絡先が連絡先記憶部から削除されると必ず、ステップ600から644が、もはや存在しない名前一致を削除し、追加の認証／証明レベルチェックをもう一度行うためにその連絡先について実行される。

20

【0060】

一致アイコンにより示される名前一致を解決するために、ユーザはそれに関連付けられた一致インジケータを有する表示名を右クリックして、名前一致解決ダイアログボックスを開くことができる。この動作によりドロップダウンリストが開き、ユーザは次に該リストから「Resolve Name Conflict (名前一致を解決する)」を選択できる。

【0061】

Resolve Name Conflictのオプションを選択すると、コラボレーティブシステムは、選択された名前と同じ「クリーンネーム」の付いたユーザの連絡先記憶部内のすべての連絡先の位置を突き止め、表示する。これらの後者の連絡先は図7に図示されるようにResolve Name Conflictダイアログボックス700のリスト702に表示される。例えば、リスト702は一致する表示名「Janet」が付いた2つの前述した連絡先710と712を表示する。このリストは連絡先のステータス704(オンラインなのか、オフラインなのか)、及び連絡先のユーザに対する関係706も示す。チェックボックス708は一致する連絡先が発見されたすべての共用空間の名前を更に表示するために設けられる。リスト702内の名前の1つ(例えば、名前712)を選択すると、名前は連絡先の「vCard」に記憶された情報と共に編集ボックス714に表示される。

30

【0062】

ユーザは次に、一致する表示名を置換する「エイリアス」表示名を連絡先に割り当てるか、または(同様に、プロセスがエイリアス表示名が連絡先に割り当てられることを必要とする)連絡先を手動で認証するかのどちらかによって名前一致を解決できる。エイリアスは、ユーザがその連絡先を他の類似した名前が指定される連絡先から区別するのに役立つように連絡先に割り当てられる別の表示名に過ぎない。特に、ユーザはその上でクリックしてから、「Alias (エイリアス)」オプションまたは「Authenticate (認証)」オプションのどちらかを選択することによってResolve (解決)ドロップダウンリスト716を起動できる。

40

【0063】

Aliasオプションを選択すると、図8に図示されるAlias (エイリアス) ダイ

50

アログボックス800が表示される。このダイアログボックスには連絡先のフルネーム802が表示され、ユーザが連絡先の一意の表示名を入力してから、「OK」コマンドボタン806または「Cancel（取り消し）」コマンドボタン808のどちらかを選択することによって名前を確認できるテキストボックス804を有する。代わりに、ドロップダウンリスト716からauthenticate（認証）オプションを選択すると、図2に描かれているauthenticate（認証）ダイアログボックスが表示される。

【0064】

2つの連絡先が両方とも表示名「Janet」で存在する前述した例では、ユーザは親戚のためのエイリアス「Janet（私の姉妹）」及びビジネス上の連絡先のための別のエイリアス「Janet（私のマネージャ）」を作成することを希望する可能性がある。ユーザは、別名の付けられた（aliased）連絡先が絶対に表示名一致にならないようにそれぞれの連絡先に一意のエイリアス表示名を割り当てなければならない。後にエイリアス表示名と同じ表示名の付いた連絡先が連絡先記憶部に追加されると、新しい連絡先表示名が一致アイコンと関連付けられるが、別名が付けられ、認証された連絡先表示名は、前述した認証済み／証明済みの連絡先の優先的な処理のために、それと関連付けられた一致アイコンを有さないであろう。エイリアスがResolve Name Conflictダイアログボックス700内の連絡先のために選択されているときに、「済み」コマンドボタン718を選択するとコラボレーティブシステムは連絡先表示名を該エイリアスで置換する。エイリアス902は、次に図9に描かれているように元の表示名の代わりに連絡先リスト900に表示される。エイリアスは、エイリアス516と518を図示する図5Cに示されるように他のすべての連絡先リストにも表示される。ある実施態様では、エイリアスはユーザのアカウント内の他のすべてのデバイスで同じになるであろう。また、エイリアスは通常他のメンバーには見えないであろう。

【0065】

前述された手順を用いても、セキュリティシステムのロバスト性は確立された認証及び証明手順にユーザが準拠しているかどうか大きく依存している。システムのセキュリティを高めるためには、本発明の原理に従って、ユーザによって、あるいは管理されたアイデンティティのケースではシステム管理者によってセキュリティ方針を実現することができる。アイデンティティのためのセキュリティ方針は、コラボレーティブシステムのアイデンティティが他のアイデンティティと通信することをどのように許すのかを制御する。特に、コラボレーティブシステムは、ユーザが、彼らが管理されたアイデンティティを有しておらず、証明されたドメインの一部ではないことを意味する、管理者により証明されていない人と、あるいは手動で認証されていない人と通信しようとする時にユーザに警告することができる。

【0066】

実例としては、ユーザに警告する、あるいは個人との通信を、彼らの連絡先アイデンティティが管理者により証明されていない、または手動で認証されていない限り禁止するために、複数のオプションが提供されている。これらは、表1に述べられているオプションのようなオプションが含まれてよい。

【0067】

【表 1】

セキュリティ方針	制 限
開放	コラボレーティブシステムは、未認証または未証明のアイデンティティとの通信について警告または制限しない。
未認証の場合警告	コラボレーティブシステムはAuthenticate(認証)ダイアログボックスを表示することによって未認証のアイデンティティ(つまり、管理者によって証明されてもおらず、手動で認証されてもいない連絡先)との通信についてユーザに警告する。 このセキュリティ設定は、未認証アイデンティティとの通信を妨げないが、ユーザに続行する前にアイデンティティを手動で認証するようにプロンプトを出す。
未証明の場合拒絶	コラボレーティブシステムは、例えばユーザがそれらのアイデンティティを手動で認証していたとしてもすべての証明されていないアイデンティティと通信することを拒絶する。

10

20

【0068】

セキュリティ方針は通信活動中のコラボレーティブシステムの動作に影響を及ぼす。例えば、前述した「未認証の場合警告」方針は表 2 に示されるように活動に影響を及ぼす。表 2 が包括的ではないことに注意する。新しい連絡先と他の操作もシステムにAuthenticateダイアログを表示させることができるであろう。

30

【0069】

【表 2】

通信活動	セキュリティ動作
インスタントメッセージ及び共用空間招待状を送信する(チャットを含み、インスタントメッセージを転送する)	受取人の誰かが未認証のアイデンティティを有する場合、コラボレーティブシステムは、ユーザがこれらの受取人のアイデンティティを手動で認証するためのAuthenticateダイアログボックスを表示する。ユーザがこれらの受取人を手動で認証することを選択しない場合には、ユーザは続行する前にTo(宛て先):フィールドから彼らを削除しなければならない。
共用空間招待状を確認する	未認証アイデンティティの付いた人が共用空間招待状を受け入れ、ユーザが該招待状について「必須受諾確認」を指定した場合、コラボレーティブシステムはユーザが被招待者の受諾を確認するとAuthenticateダイアログボックスを表示する。
共用空間を開放する	共用空間メンバーの誰かが未認証アイデンティティを有する場合、コラボレーティブシステムはAuthenticateダイアログボックスを表示する。
共用空間を作成する	ユーザが共用空間を作成し、未認証アイデンティティが付いた人を招待する場合、コラボレーティブシステムはAuthenticateダイアログボックスを表示する。
共用空間をフェッチする	ユーザが未認証アイデンティティの付いたメンバーから共用空間をフェッチしようとする、コラボレーティブシステムはAuthenticateダイアログボックスを表示する。

10

20

30

【0070】

「未証明の場合拒絶」方針は表3に示されるように通信活動に影響を及ぼす(表2の場合と同様に、表3も包括的ではない)。

40

【0071】

【表 3】

通信活動	セキュリティ動作
インスタントメッセージ及び共用空間招待状を送信する	受取人の誰かが未認証のアイデンティティを有する場合、コラボレーティブシステムは、ユーザが未証明のアイデンティティと通信できないことを述べるメッセージを表示する。
共用空間招待状を確認する	未認証アイデンティティの付いた人が共用空間招待状を受け入れ、ユーザが該招待状について「必須受諾確認」を指定した場合、コラボレーティブシステムは受諾を断り、共用空間を送信しない。
共用空間を開放する	共用空間メンバーの誰かが未証明アイデンティティを有する場合、コラボレーティブシステムはユーザがこれらのメンバーとは共用空間に参加できないというメッセージを表示する。
共用空間を作成する	ユーザが共用空間を作成し、未証明のアイデンティティの付いた人を招待しようとする場合、コラボレーティブシステムはユーザがこれらの人を招待するのを妨げる。
共用空間をフェッチする	コラボレーティブシステムは、ユーザが未証明のアイデンティティの付いたメンバー(Fetch From:(からフェッチする)ドロップダウンメニューに一覧表示されていない未証明のメンバー)から共用空間をフェッチすることを許可しない。

【0072】

「未証明の場合拒絶」のセキュリティ方針が管理されているアイデンティティに適用されても、管理されているアイデンティティの付いたユーザは依然として他の連絡先アイデンティティを手動で認証できる。しかし、そのユーザは、手動で認証されたアイデンティティが更に管理者によって証明されていない場合には、手動で認証されたアイデンティティと通信できない。ユーザが、手動で認証されたに過ぎないアイデンティティと通信しようとする場合、ユーザは、「未許可の場合拒絶」方針が適用されていないアイデンティティを使用しなければならない。

【0073】

同じアカウント内の複数のアイデンティティは、各アイデンティティに割り当てられたさまざまなセキュリティ方針を有する場合がある。例えば、ユーザは「未証明の場合拒絶」のセキュリティ方針が適用された自分のオフィスに管理されたアイデンティティを有し、アイデンティティセキュリティ方針が適用されていない状態で家庭で使用するための同じアカウント内の管理されていないアイデンティティも有する可能性がある。更に、指定されたアイデンティティに関してそれぞれが別のレベルの認証を持つ複数のアイデンティティのアカウントを有することも可能である。これが発生する場合、コラボレーティブシ

システムはアカウントが指定されたアイデンティティとの最高の認証／証明関係を表示する。

【0074】

例えば、それぞれがさまざまな管理ドメインからの複数の管理されたアイデンティティの付いたアカウントがある場合に、さまざまなレベルの認証が発生することがある。このケースでは、それぞれの管理ドメインは指定されたドメインで異なる相互証明設定値を有する可能性がある。

【0075】

アイデンティティが管理されている場合、セキュリティ方針は管理サーバを使用して管理者により設定される。セキュリティ方針を特定するためには、管理者はドメインまたはグループのアイデンティティを定義してから、これらのアイデンティティを従来の様式で管理させなければならない。次に管理者はサーバでユーザインタフェースを使用し、方針を設定する。ドメインまたはグループにアイデンティティ方針を設定するために、管理者はドメイン／グループウィンドウを開き、管理ドメインまたはグループを選択してから、「方針」タブ及び「edit identity policies (アイデンティティ方針を編集する)」リンクまたは他の類似する選択機構を選択する。

【0076】

次に図10に図示されるアイデンティティ方針ページ1000が表示される。方針がドメインに対し設定されている場合にはenable policy (方針を有効にする) チェックボックス1002が表示される。ボックスにチェックマークを付けると、現在のアイデンティティ方針設定がドメインに適用されることが指定される。ボックスのチェックを解除すると、デフォルトのアイデンティティ設定値がドメインに適用されることが指定される。

【0077】

「identity may only be used on a managed device (アイデンティティは管理されているデバイスだけで使用されてよい)」チェックボックス1004は、選択されているドメインまたはグループ内の管理されているアイデンティティだけが管理されているデバイスで使用できることを指定する。このチェックボックスのチェックを解除すると、管理されているアイデンティティを、管理されているか、あるいはされていないかに関係なく任意のデバイスでできるようにする。

【0078】

「automatically publish vCard to management server directory (管理サーバディレクトリにvCardを自動的に発行する)」チェックボックス1006は、管理サーバがドメイン／グループメンバーの管理されているアイデンティティ及びvCard情報をドメインメンバーの管理サーバのローカルディレクトリに自動的に発行する必要があることを指定する。

【0079】

「prevent publishing vCard to groove.net directory (groove.netディレクトリにvCardを発行するのを妨げる)」チェックボックス1008は、管理サーバがドメイン／グループメンバーの管理されているアイデンティティ及びvCard情報をgroove.netウェブサイト上のgroove.netパブリックディレクトリに発行してはならないことを指定している。

【0080】

「backup account every (1) day(s) (maximum 7) (毎(1)日(複数の場合がある)(最大7)アカウントをバックアップする)」チェックボックス1010は、ドメインで管理されているアイデンティティについて管理サーバがどのくらい頻繁にユーザアカウントを自動的にバックアップするのかを指定する。1から7の数をテキストボックスに入力し、バックアップ間の日数を指定できる。テキストボックスを空にしておくと、この方針は無効になり、アカウントはバックアップされないであ

10

20

30

40

50

ろう。

【0081】

表示1000の次のセクションは、ピア（peer）認証方針を指定する。この方針は、管理サーバが未認証連絡先とのクライアントによる通信をどのように処理するのかを決定する。「Do not warn or restrict members about communicating with any a identities（あらゆるアイデンティティと通信することについてメンバーに警告またはメンバーを制限しない）」ラジオボタン1014を選択すると、表1に説明された「開放」方針が設定され、メンバーは、管理サーバが警告情報を生成しなくても未認証の連絡先と自由に通信できる。

10

【0082】

「Warn members before communicating with contacts that have been neither adminis tor-certified nor manually authenticated by the member（管理者に証明されていないし、メンバーによって手動で認証されてもいない連絡先と通信する前にメンバーに警告する）」ラジオボタン1016を選択すると、表1の「未認証の場合警告」方針が設定され、メンバーが未認証のユーザと通信できるが、管理サーバはこのような通信が試みられる前に前述されたように警告を発行する。

【0083】

「Only allow members to communicate with administrator-certified contacts（メンバーが管理者により証明された連絡先とだけ通信できるようにする）」ラジオボタン1018を選択すると、表1の「未証明の場合拒絶」方針が設定され、メンバーが未証明のアイデンティティと通信するのを妨げる。

20

【0084】

全ての選択がなされると、「Submit（提出）」コマンドボタン1020を選択できる。次に選択されたアイデンティティ方針が後述される管理されているオブジェクトを使用してドメイン内のデバイスに自動的に広められる。ユーザがオフラインである場合は、その方針は、彼らが次回オンラインになったときに管理オブジェクトによって更新されるだろう。

30

【0085】

更に、管理ドメインの一部ではないユーザは、図11に図示される表示画面のようなユーザインタフェース表示画面110によって独自のセキュリティ方針を設定してよい。セキュリティ方針は適切なラジオボタン1102、1104または1106を選択することによりユーザが設定（あるいは、アイデンティティが管理されているアイデンティティである場合にはレビュー）できる。アイデンティティが管理されている場合、ボタン1102、1104及び1106は、管理されているアイデンティティのセキュリティ方針が管理者によって制御されるので無効にされるだろう。アイデンティティが管理されていない場合には、ボタン1104と1106が有効化されるが、ボタン1108は、この選択が常に管理者によって制御されるため（図11に図示されるように）無効にされるだろう。

40

【0086】

ドメインセキュリティ方針は管理サーバからユーザアカウントに送信される「管理オブジェクト」によって実現される。特にセキュリティ方針は「アイデンティティ方針」オブジェクトに含まれる。このようなオブジェクトは管理サーバで作成され、作成時には対象となるユーザ（特定のアイデンティティ）を有するあるいは有さない場合がある。管理サーバが管理オブジェクトを生成した後（a）サーバがアカウントの中にオブジェクトを「投入する」または（b）アカウントに関連付けられたエンドユーザが、オブジェクトをアカウントの中に手動で注入するためにオブジェクトの表記をクリックできるかのどちらかである。アカウントの中に注入される管理オブジェクトはアカウントの内部の管理オブジ

50

ェクト記憶部（150、図1B）に記憶される。

【0087】

いずれにせよ、管理オブジェクトの注入後、アカウントの何らかのアイデンティティが（報告の目的で）オブジェクトの実際のユーザとして記されるであろう。コラボレーティブシステムが対象となるユーザをアカウントの中のアイデンティティの1つと一致させることができる場合、そのアイデンティティは管理オブジェクトと関連付けられるであろう。そうではない場合は、アカウントの所有者は、アカウントに複数のアイデンティティがある場合に1つのアイデンティティを選択できる。

【0088】

誰かが管理オブジェクトを注入するたびに、コラボレーティブシステムは（管理者要員が誰がオブジェクトを注入したのか、及び誰がオブジェクトを注入しなかったのかを突き止めることができるように）オブジェクトの実際のユーザのアイデンティティと共に管理サーバにこの事実を報告する。サーバには管理オブジェクトを取り消す能力もある。特にユーザが管理オブジェクトを要求するたびに、この事実（管理要員が、誰が実際に管理オブジェクトを使用しているのかを突き止め、必要な場合に特定のユーザについてオブジェクトを取り消すことができるように）オブジェクトの実際のユーザと共に管理サーバに報告される。

【0089】

管理オブジェクトを生成するために、選択された情報が管理サーバに提供される。サーバは次にXML文書の形式でオブジェクトを生成する。何らかの情報がオブジェクトのヘッダに含まれている。この情報は管理オブジェクトを識別する名前（大局的に一意）を含む。例えば、例示的な名前は「grooveLicense://Core/GrooveProfessional」または「grooveAccountPolicy://DataRecovery」または「grooveIdentityPolicy://.」を含む。

【0090】

管理オブジェクト情報は、オブジェクト発行者を識別する情報も含む。これは大局的に一意のURN（例えば、「urn:groove.net:」）の形を取る企業識別を含む可能性がある。管理サーバURL及び（指定されたサーバにとって一意である）管理ドメイン名を含む管理ドメインも提供される。この情報は更にオブジェクトに署名するために使用される管理ドメインの秘密鍵及び証明書、及びオプションで管理オブジェクトの対象となるユーザも含む。オプションで管理オブジェクトの本体も提供されてよい。

【0091】

一般化された管理オブジェクトを具現するXML文書のスキーマが後述される。

<!--

- optional attributes are enclosed in []
- optional attribute default values are after //
- optional elements are noted as such

-->

<g:ManagedObject

Version="0,0,0,0"

>

<g:Header

GUID="<GUID>"

NAME="<name>"

DisplayName="<display_name>"

Description="<description>"

IssuedTime="<issued_time>"

[DeviceSpecific="1|0"] //="0"

[ReplacementPolicy="\$Never|\$Always|\$IssuedTime"] //="\$Never"

10

20

30

40

50

```

    [IntendedIdentityURL=<intended_identity_URL>"] //=""
  >
  <!-- expiration is optional, default is none -->
  <g:Expiration>
    <g:TimePeriod
      Value="<value>"
      [Baseline="$IssuedTime|$InjectionTime"
//="$InjectionTime"
      [Limit="<limit>"] //="none
    />
  </g:Expiration>
  <g:Issuer
    Name="<name>"
    DisplayName="<display_name>"
  />
  <g:ManagementDomain
    Name="<name>"
    DisplayName="<display_name>"
    ServerURL="<server_URL>"
  />
</g:Header>

<!-- body is optional -->
<g:Body
  ComponentResourceURL="<component_resource_URL>"
>
  <!-- whatever data is needed by a particular type of a managed object
should be in the body element below -->
  <g:body_element>
  </g:body_element>
</g:Body>

<g:Signatures>
  <g:Signature Value="<value>"Fingerprint="<fingerprint>"/>
</g:Signatures>
</g:ManagedObject>

```

【0092】

ヘッダ部分では、GUID属性は管理オブジェクトの大局的に一意の識別子であり、それぞれの新規に生成される管理オブジェクトと共に生成される。名前属性は管理オブジェクトを識別し、前述された表示名ではない。管理オブジェクト名はURLであり、URLのスキーマ部分は管理オブジェクト型であり、残りはその特定の管理オブジェクト型に特有である。例えば、grooveLicense: // groove.net / ; Division = Core, Product = Grooveはライセンス管理オブジェクトの名称であり、「grooveLicense」部分はライセンスの管理オブジェクト型である。任意の時点で管理オブジェクト記憶部は指定された名前が付いた多くても1つの管理オブジェクトを記憶できる。

【0093】

DisplayName / Description属性は、人間が読み取り可能な管理オブジェクトの表示名 / 記述である。IssuedTime属性は管理オブジェクト発行時間を指定する。DeviceSpecific属性は、管理オブジェクトがデバイス全

体に適用できるかどうかを判断する。この属性が「1」である場合には、管理オブジェクトはデバイスに特有であり、構成要素ダウンロード方針などのデバイス全体に適用される。

【0094】

`ReplacementPolicy`属性は、既存の管理オブジェクトを同じ名前が付いた別の管理オブジェクトでいつ置換できるのかを示している。コラボレーティブシステムは、置換対象の管理オブジェクトにおける置換方針よりむしろ置換管理オブジェクト内で指定される置換方針を尊重する。この属性に考えられる値は\$`Never`—管理オブジェクトは絶対に置換できない、\$`Always`—管理オブジェクトはつ常に置換されるべきである、及び\$`IssuedTime`—管理オブジェクトは発行時刻がより最近の別の管理オブジェクトによって置換できるである。この属性のデフォルトは\$`Never`である。

10

【0095】

`IntendedIdentityURL`属性は、管理オブジェクトについて（実際のとは対照的に）対象となるアイデンティティURLを指定する。`Expiration`属性は、管理オブジェクトがいつ期限切れになり、使用できなくなるのかを定義する。期間属性は例えば30日などの有効期間について指定できる。この値は、`Baseline`属性によって指定されるベースラインに関係する。有効期間の`Baseline`属性は有効期間の開始がいつ発生するのかを指定し、以下の2つの考えられる値を有する。つまり、ベースラインが管理オブジェクト発行時刻であることを指定する\$`IssuedTime`と、ベースラインが管理オブジェクト注入時刻であることを指定する\$`InjectionTime`である。指定されない場合には値\$`InjectionTime`がデフォルトである。有効期間は、他の条件には関係なく、管理オブジェクトが期限切れになると、総合的な期限を課すことを可能にする`Limit`属性も有する場合がある。これは、ベースラインに関連しない絶対値である。

20

【0096】

発行者属性は管理オブジェクト発行者を特定する。発行者名及び表示名は指定される必要があり、名前は大局的に一意でなければならない。管理ドメイン属性は管理オブジェクトの管理ドメインを識別する。管理ドメインの名前、表示名、及びサーバURLは指定されなければならないが、この場合サーバURLが管理サーバを指し、名前がそのサーバの範囲内で一意でなくてはならない。

30

【0097】

スキーマの本体部分は、どの構成要素がこのオブジェクトの本体、及び特定のオブジェクト型によって決定される不透明なデータを含む本体要素を処理しているのかを指定する構成要素リソースURLを含む。

【0098】

前述したように、アイデンティティのセキュリティ方針はアイデンティティ方針管理オブジェクトに含まれる。このようなオブジェクトの例示的な名称は、`grooveIdentityPolicy://<GUID>`である。例示的な`ComponentResourceURL`属性は、`http://components.groove.net/Groove/Components/Root.osd?Package=net.groove.Groove.SystemComponents.GrooveAccountMgrDLL&Version=0&Factory=IdentityPolicy`である。

40

【0099】

アイデンティティ方針管理オブジェクトの本体要素の例示的なスキーマは以下に示される。このスキーマでは、`<g:Policy>`要素を除くすべての要素がオプションである。

```
<g:Policy[Flags="<flags>"][PeerAuthenticationLevel="<level>"]>
  <g:Contact>
```

50

```

<g:VCard[ChangeFlags="<vCard_change_flags>"/]>
  <g:Policies>
    <g:DirectoryListings>
      <!-- may have 0+ elements like the one below -->
      <g:DirectoryListing
        Name="<directry_name>"
        Value="<directory_listing_value>"/>
      </g:DirectoryListings>
    </g:Policies>
  </g:Contact>
  <g:Backup Interval="<interval_in_days>"/>
    [<g:Telespaces DefaultTemplateComponentResourceURL="<>"/>]
  <g:AttachmentRestriction
    AllowOnly="<true|false>"
    Size="<size_in_kb>"
    FileType="<list_file_ext>"
  />
</g:Policy>
【0100】

```

10

Flags 属性の例示的な値は、このアイデンティティがアイデンティティと関連付けられた管理ドメインからのデバイス上だけで使用できることを示す「0x1」である。PeerAuthenticationLevel 属性は、いかなる連絡先との通信時にも警告または制限が発行されないことを示す「0」を含む3つの考えられる値を有することがある。これが、例示としてデフォルトの動作となるであろう。値「1」は、システムが未認証の連絡先についてユーザに警告する必要があることを示し、値「2」は、システムが未証明の連絡先と通信するのを制限する必要があることを示している。

20

【0101】

例示としてvCard_change_flags の値は、ユーザが業種フィールドを変更できないことを示す「0x2」である。directory_name 属性は、ディレクトリがGroove.net 連絡先ディレクトリでなければならないことを指定する \$GrooveNet 及びディレクトリがアイデンティティと関連付けられた管理ドメインのための連絡先ディレクトリでなければならないことを指定する \$ManagementDomain などの複数の値を有することがある。

30

【0102】

directory_listing_value 属性の値は、連絡先リスティングが発行されるかどうかをユーザが決定することを示す「0」となる場合がある。代替値は連絡先リスティングが常に発行される必要があることを指定する「1」、及び連絡先リスティングを決して発行してはならないことを指定する「2」を含む。

【0103】

DefaultTemplateComponentResourceURL 属性の値は、共用空間テンプレートの構成要素リソースURLである。AttachmentRestriction 要素は、複数の値を有することがある属性AllowOnly を有する。これらの値は、添付リストが排除リストであり、リスト上のファイル型が許可されていないことを示す値「0」つまり「偽」を含む。代わりに、属性は、添付リストが包含リストであり、リスト上の型だけが許可されていることを示す値「1」または「真」を有することがある。size_in_kb 属性の値はキロバイト単位でファイルの最大数値サイズを指定する。list_file_ext 属性の値は、例えば、「exe」、「vb」、「dll」などの許可されているファイル拡張子の区切られたリストである。

40

【0104】

クライアントが方針オブジェクト（あるいは、通常は管理オブジェクト）を受け取ると

50

、クライアントは最初に方針オブジェクトがその管理ドメインによって署名されていることを検証する。（構成要素ダウンロードなどの）デバイス全体での方針は、デバイスの管理ドメインの公開鍵を使用して検証される。アイデンティティ全体の方針は、アイデンティティの管理ドメインの公開鍵を使用して検証される。管理オブジェクトに署名するために使用される鍵の組はユーザ証明書及び相互ドメイン証明書に署名するために使用される鍵の組とは別個である。管理ドメインは、以下の全部で4つの鍵の組を有する。つまり、（1）管理オブジェクトに署名するための鍵の組、（2）「有線での（over the wire）」クライアント／サーバ通信を保護する際に使用される鍵トランスポートの鍵の組、（3）証明書に署名するための鍵の組、及び（4）データ回復及びパスフレーズリセットのための鍵符号化のための鍵の組である。

10

【0105】

第1の管理ドメイン公開鍵はアイデンティティと管理ドメインの間の「起動プロトコル」の間にクライアントに安全に配布される。第2の公開鍵も「起動プロトコル」中に送信されるが、第1の鍵で署名された証明書の中にカプセル化されている。第3の公開鍵と第4の公開鍵は、その後、それぞれ「証明／認証」方針及び「データ回復」方針の中で送信される。これらの後者の2つの鍵は、それらが方針にパッケージ化されているため、第1の（方針署名）公開鍵と共に署名される。したがって、第1の公開鍵にアクセスできる管理者が実質的には最高の権威者である。

【0106】

アイデンティティが、セキュリティ方針が実施されている別の連絡先との通信を試みる時に実行されるプロセスは、図12Aから図12Cが共に置かれる時に形成されるフローチャートに図示されている。このプロセスはステップ1200で開始し、アイデンティティが、アイデンティティが通信を試みるすべての連絡先のリスト（「CL i s t」と呼ばれる）を作成するステップ1202に進む。方針が「未認証の場合警告」または「未証明の場合制限」に設定されているかどうかの決定がステップ1204で行われる。ステップ1204では、方針が「未認証の場合警告」または「未証明の場合制限」に設定されていると判断された場合、クライアントはCL i s tの中の連絡先の（「UnAuth L i s t」と呼ばれる）すべての未認証連絡先と未証明連絡先のリストを作成する。代わりにステップ1204では、方針が警告または制限なしに通信を可能とするために設定されていると判断された場合、プロセスは進み、ステップ1208で終了する。

20

30

【0107】

UnAuth L i s tを作成するために、クライアントはCL i s t内の連絡先のすべてを列挙し、処理する。特にプロセスは、全連絡先が処理されたかどうか判断されるステップ1206に進む。すべての連絡先が処理された場合、プロセスはステップ1208で終了し、結果として生じるUnAuth L i s tは、前述されたように実施される方針に従って通信を制御するために使用される。

【0108】

代わりに、すべての連絡先が処理されている訳ではないとステップ1206で判断されると、次にステップ1210でCL i s tの中の次の連絡先が選択される。ステップ1212では、「警告」を行うために方針が設定され、連絡先がユーザのアカウントの別のアイデンティティであるかどうか判断される。そうである場合には、連絡先はアカウントのアイデンティティの1つであり、プロセスはすべての連絡先が処理されたかどうか判断するためにステップ1206に戻るによりCL i s t連絡先の残りで続行される。代わりに、ステップ1212において、連絡先がアカウントのアイデンティティの1つではないと判断された場合には、プロセスは、方針が「警告する」ために設定され、連絡先が手動で認証されたかどうかの判断が下されるステップ1226に、オフページコネクタ1216と1222を介して進む。連絡先の手動認証ビットを調べることによって、連絡先が手動で認証されたかどうかの判断を下すことができる。連絡先がすでに認証されている場合にはプロセスはオフページコネクタ1220と1214を介してステップ1206に戻り、CL i s t上の追加の連絡先がまだ処理されていないかどうかを判断する。

40

50

【0109】

ステップ1226で連絡先がすでに認証されていなかったと判断された場合には、プロセスはIsCertifiedContact変数の値がFALSE（偽）に設定されるステップ1228に進む。プロセスはアイデンティティに関連付けられているすべての相互ドメイン証明方針を通して列挙する。特にステップ1230では、追加の相互ドメイン方針がまだ調べられていないかどうか判断される。追加の方針がまだ調べられていない場合には、ステップ1232では、次の方針が検査のために選択される。

【0110】

ステップ1234では、連絡先の管理ドメインが方針で証明されたドメインに一致するかどうか判断される。一致しない場合、プロセスはステップ1230に戻り、更に多くの方針がまだ調べられていないかどうかを判断する。ステップ1234で連絡先の管理ドメインが方針で証明されたドメインに一致すると判断されると、プロセスはオフページコネクタ1238と1246を介して、連絡先の証明書上の署名が相互証明されたドメインの公開鍵で検証され、最小証明書チェーンの有効期限が計算されるステップ1252に進む。

10

【0111】

次にステップ1254では、シグナチャが最小有効期限を検証しないのか、あるいは現在の日付が最小有効期限を越えているのかの判断が下される。そうである場合には、プロセスはオフページコネクタ1244と1236を介して、プロセスが相互ドメイン方針の残りで続行されるステップ1230に戻る。

20

【0112】

そうではない場合には、プロセスは、変数IsCertifiedContactが、連絡先が証明されていることを示すTRUEに設定されるステップ1256に進む。次に、プロセスはIsCertifiedContactの値が、連絡先が証明されていないことを示すFALSEかどうか判断されるステップ1258に進む。プロセスは、ステップ1230で判断されたようにすべての方針が調べられた後に、オフページコネクタ1240と1248を介してステップ1258にも到達する。

【0113】

連絡先がステップ1258で判断されたように証明されていない場合には、連絡先はステップ1260で未認証及び未証明連絡先リスト(UnAuthList)に追加され、プロセスはオフページコネクタ1250と1242、及びコネクタ1224と1218を介してステップ1206に戻り、すべての連絡先が処理されたかどうかを判断する。代わりに、ステップ1258で連絡先が証明されていると判断されると、プロセスはステップ1260を省略し、直接ステップ1206に進み、追加の連絡先がまだ処理されていないかどうかを判断する。

30

【0114】

すべての連絡先がステップ1206で判断されたように処理された後には、未認証連絡先リスト(UnAuthList)が選択されたセキュリティと共に使用され、未認証且つ未証明のユーザとの通信が試される場合にユーザに警告する、あるいは必要に応じて通信を制限するかのどちらかを行う。

40

【0115】

前述された実施態様のソフトウェアインプリメンテーションは、例えばディスク、CD-ROM、ROMメモリまたは固定ディスクなどのコンピュータ読み取り可能媒体などの有形媒体に固定される、またはモデムや他のインタフェースデバイスを介して媒体上にコンピュータシステムに送信可能な一連のコンピュータ命令を備えてよい。媒体は、光通信回線またはアナログ通信回線を含むがそれらに制限されない有形の媒体である場合があるか、あるいはマイクロ波技法、赤外線技法、または他の伝送技法を含むがそれらに制限されない無線技法で実現されてよい。それはインターネットであってもよい。一連のコンピュータ命令は、本発明に関してここに前述された機能性のすべてまたは一部分を具現する。当業者は、このようなコンピュータ命令が多くのコンピュータアーキテクチャまた

50

はオペレーティングシステムと使用するために多くのプログラミング言語で作成できることを理解するだろう。更に、このような命令は、半導体素子、磁気デバイス、光学素子または他のメモリ装置を含むがそれらに制限されない現在または将来の任意のメモリ技術を使用して記憶されてよい、あるいは光伝送技術、赤外線伝送技術、マイクロ波伝送技術または他の伝送技術を含むがそれらに制限されない現在または将来の任意の通信技術を使用して伝送されてよい。このようなコンピュータプログラム製品が、例えばシステムROMまたは固定ディスク上などコンピュータシステムにプレインストールされた収縮包装されたソフトウェアなどの添付の印刷文書または電子文書と共にリムーバブル媒体として配布されるか、あるいはインターネットやワールドワイドウェブなどのネットワーク上のサーバまたは電子掲示板から配布されてよいと考えられる。

10

【0116】

本発明の例示的な実施態様が開示されてきたが、本発明の精神及び範囲を逸脱することなく本発明の利点のいくつかを達成する多様な変更及び変形を加えることができることは当業者にとって明らかとなるであろう。例えば、他のインプリメンテーションにおいて、示されているものとは異なるプロトコル及び変換が実行されてよいことが適度に技術にたけた人にとって明らかになるだろう。本発明の概念に対する他の変形だけではなく特定のプロセスフロー、及び描かれているステップの順序などの他の態様も添付の請求項によってカバーされることが意図されている。

【図面の簡単な説明】**【0117】**

20

【図1】図1Aは、各コラボレーティブコンピュータがトランシーバ及びデータベースを含む例示的なコラボレーティブシステムのブロック概略図である。図1Bは、共用空間記憶部、アカウントメタデータ記憶部、及び連絡先記憶部を含むコラボレーションシステムデータベースのブロック概略図である。

【図2】図2は、連絡先を手動で認証するために使用される表示画面の画面の場面である。

【図3】図3は、詳細な連絡先情報及び認証インジケータを描く連絡先ディスプレイの画面の場面である。

【図4】図4は、連絡先認証ステータス及び表示名一致を示すために表示できる一式の例示的なアイコンを示す。

30

【図5】図5Aは、表示名一致を描く連絡先名前表示の画面の場面である。図5Bは、表示名の一致を強調表示するために名前一致アイコンの使用を描く連絡先名の表示の画面場面の一部である。図5Cは、表示名一致を解決するためのエイリアスの使用を描く連絡先名表示の画面の場面の一部である。

【図6】図6Aは、図6Bと図6Cと共に置かれた時に、連絡先表示名と共にいつ名前一致アイコンが表示されなければならないのかを決定するための例示的なプロセスのステップを示すフローチャートを形成する。図6Bは、図6Aと図6Cと共に置かれた時に、連絡先表示名と共にいつ名前一致アイコンが表示されなければならないのかを決定するための例示的なプロセスのステップを示すフローチャートを形成する。図6Cは、図6Aと図6Bと共に置かれた時に、連絡先表示名と共にいつ名前一致アイコンが表示されなければならないのかを決定するための例示的なプロセスのステップを示すフローチャートを形成する。

40

【図7】図7は、表示名の一致を解決するために使用される画面表示の画面の場面である。

【図8】図8は、エイリアスを表示名に割り当てるために使用されるダイアログボックスの画面の場面である。

【図9】図9は、表示されたエイリアス及び連絡先認証インジケータを示す連絡先名リスティングの画面の場面である。

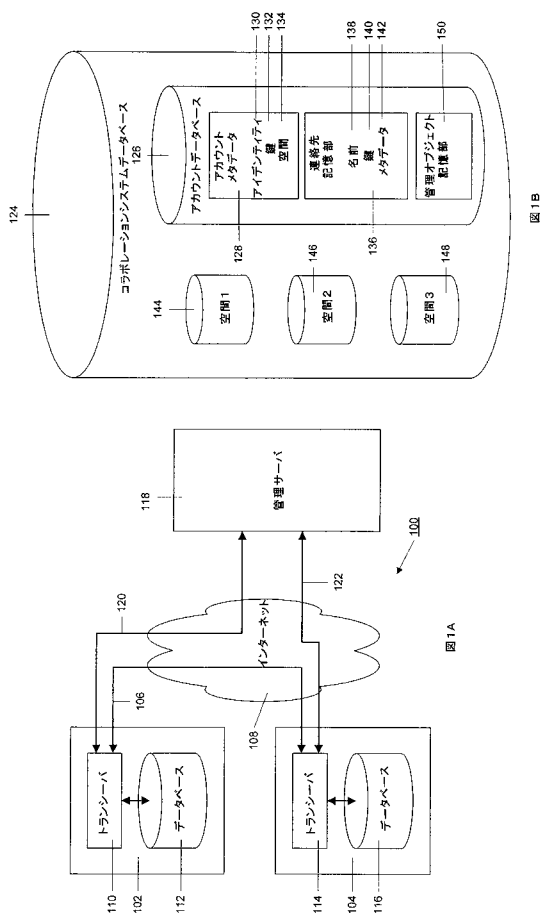
【図10】図10は、管理者が1つまたは複数のアイデンティティのためにセキュリティ方針を設定できるようにする表示画面の画面の場面である。

50

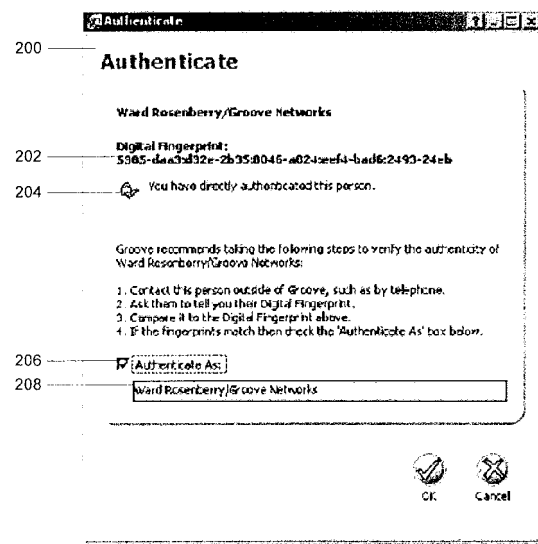
【図 1 1】図 1 1 は、ユーザがそのユーザに適用するセキュリティ方針を設定及び検討できるようにする表示画面の画面の場面である。

【図 1 2】図 1 2 A は、図 1 2 B と図 1 2 C と共に置かれた時に、認証されていなく及び証明されていない連絡先のリストをコンパイルするための例示的なプロセスのステップを示すフローチャートを形成する。図 1 2 B は、図 1 2 A と図 1 2 C と共に置かれた時に、認証されていなく及び証明されていない連絡先のリストをコンパイルするための例示的なプロセスのステップを示すフローチャートを形成する。図 1 2 C は、図 1 2 A と図 1 2 B と共に置かれた時に、認証されていなく及び証明されていない連絡先のリストをコンパイルするための例示的なプロセスのステップを示すフローチャートを形成する。

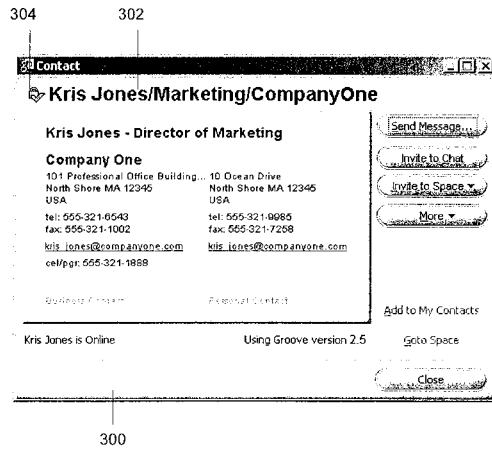
【図 1】



【図 2】



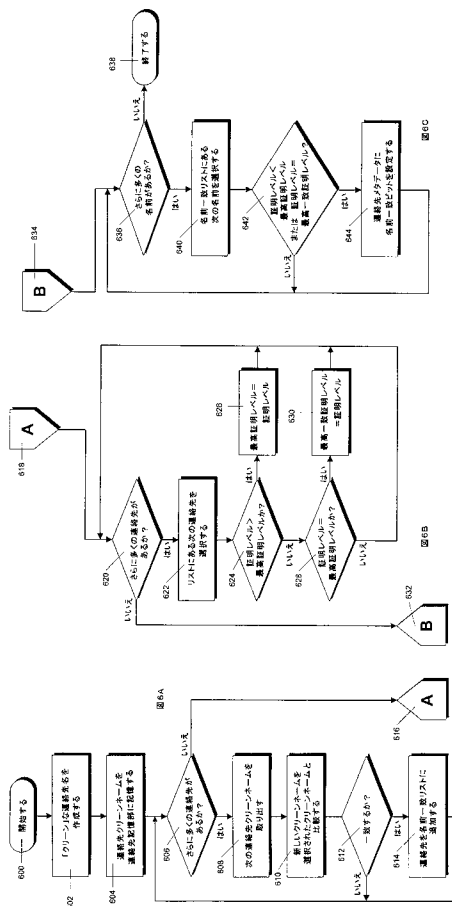
【図 3】



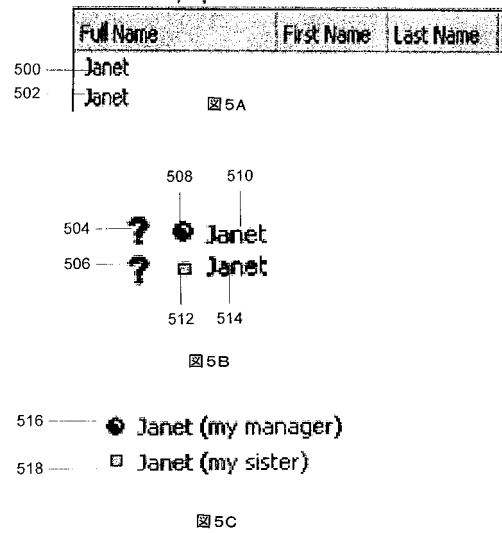
【图 4】



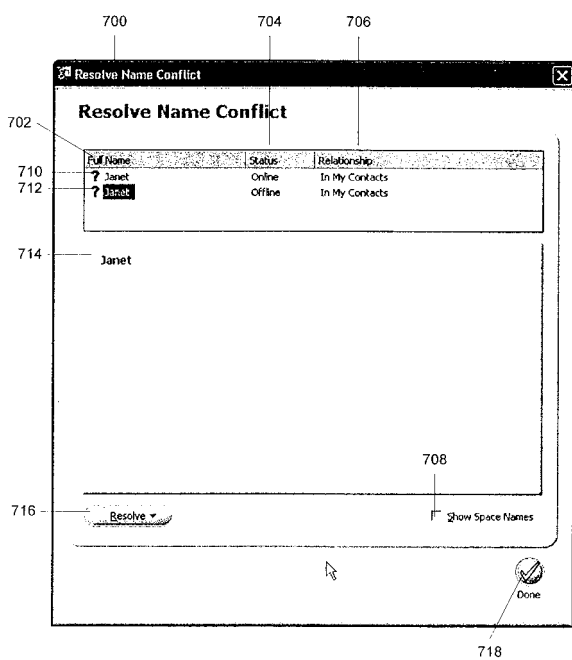
【图 6】



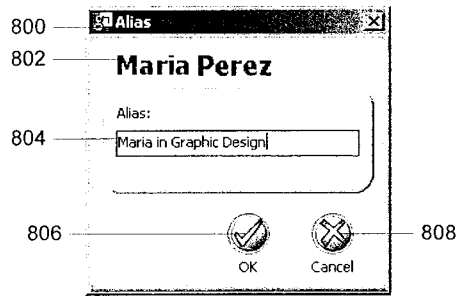
【図 5】



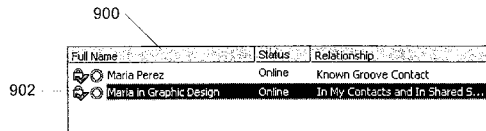
【图 7】



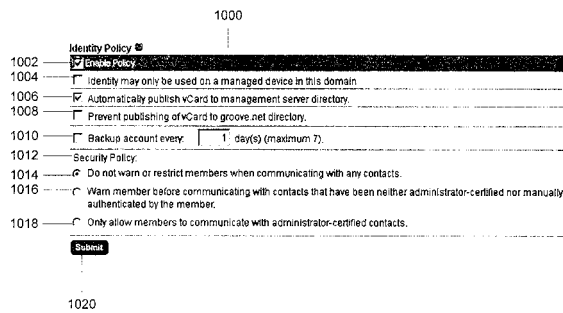
【図 8】



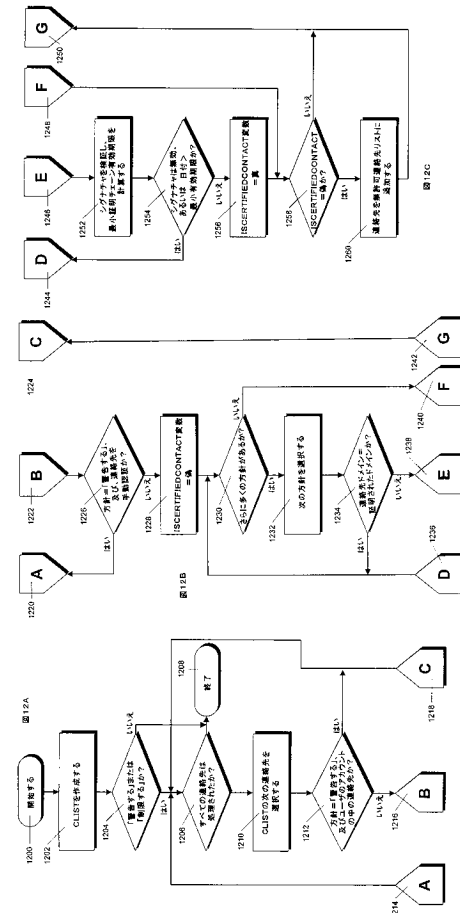
【図 9】



【図 10】



【図 12】



フロントページの続き

- (72)発明者 ジョージ・ピー・モロミサト
アメリカ合衆国 マサチューセッツ州 02140 キャンブリッジ ユニット・シー チェスター・ストリート 4
- (72)発明者 ニミシャ・アスタギリ
アメリカ合衆国 カリフォルニア州 91106 パサディナ アpartment104 サウス・ウィルソン・アヴェニュー 241
- (72)発明者 ウェイ・ダイ
アメリカ合衆国 マサチューセッツ州 01960 ピーボディ ショア・ドライブ 102
- (72)発明者 アレクセイ・エヴドキモフ
アメリカ合衆国 マサチューセッツ州 01907 スワンプスコット フランクリン・ストリート 67
- (72)発明者 マーク・コート
アメリカ合衆国 マサチューセッツ州 01913 アムスベリー ペイジ・ファーム・ロード 4
- (72)発明者 アダム・ワイス
アメリカ合衆国 マサチューセッツ州 02145 サマーヴィル #1 ローウェル・ストリート 301

審査官 田中 慎太郎

- (56)参考文献 吉田究, Groove スターターガイド 第1版, 日本, 株式会社オーム社, 2001年11月30日, 第1版第1刷, p.158-164

- (58)調査した分野(Int.Cl., DB名)
G06F 21/20
G09C 1/00