(19)日本国特許庁(JP)　(12)公表特許公報(A)　(11)特許出願公表番号
特表2006-506749
(P2006-506749A)
(43)公表日　平成18年2月23日(2006.2.23)

(51)Int.Cl.		F I			テーマコード（参考）
G06Q 50/00	(2006.01)	G06F	17/60	132	5B285
G06Q 10/00	(2006.01)	G06F	17/60	172	
G06F 21/20	(2006.01)	G06F	17/60	512	
		G06F	15/00	330A	

審査請求 未請求　予備審査請求 有　（全 26 頁）

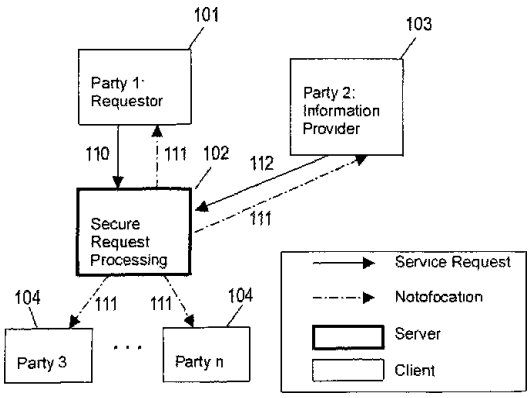
(21)出願番号　特願2004-555286 (P2004-555286)
(86)(22)出願日　平成15年8月18日 (2003.8.18)
(85)翻訳文提出日　平成17年7月12日 (2005.7.12)
(86)国際出願番号　PCT/US2003/025720
(87)国際公開番号　WO2004/049101
(87)国際公開日　平成16年6月10日 (2004.6.10)
(31)優先権主張番号　10/065,802
(32)優先日　平成14年11月20日 (2002.11.20)
(33)優先権主張国　米国 (US)

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレーション
ＩＮＴＥＲＮＡＴＩＯＮＡＬ　ＢＵＳＩＮＥＳＳ　ＭＡＳＣＨＩＮＥＳ　ＣＯＲＰＯＲＡＴＩＯＮ
アメリカ合衆国１０５０４　ニューヨーク州　アーモンク　ニュー　オーチャード　ロード
(74)代理人　100086243
弁理士　坂口　博
(74)代理人　100091568
弁理士　市位　嘉宏
(74)代理人　100108501
弁理士　上野　剛史

最終頁に続く

(54)【発明の名称】機密データの保護処理のための方法及び装置

(57)【要約】
機密データの保護処理のための装置は、保護ネットワーク・チャネルを通じて依頼者から処理のための要求を受信するネットワーク・サーバと、機密データを外部から監視することも改ざんすることもできない方法で処理するための保護計算環境と、当事者が合意した契約に基づいて要求の処理を制御する契約エンジンとを含む。契約エンジンは、要求を司る契約を選択する要求ハンドラを含み、当事者が要求をサーバに送信することができるかどうか、及び、該要求が該契約に適合するかどうかを検査する。タスク処理ユニットが、契約に定められた通りに一連の処理ステップを実施し、当初は要求内に含めて送信された情報を含む処理状態を利用して、拡張するようにする。レスポンダは、契約に定められた通りに処理状態の一部を選択し、保護ネットワーク・チャネルを通じて該契約に定められた当事者に送信される応答メッセージを生成する。



【特許請求の範囲】
【請求項１】
多数当事者電子サービスのためのコンピュータ・ベースの方法であって、
サービス・プロバイダと、クライアントと、少なくとも１つの他の当事者との間のサービスを司るための少なくとも１つの契約を、コンピュータ・システムに実装し、
クライアントからの第１の要求を、前記サービス・プロバイダで受信し、
前記サービス・プロバイダから少なくとも１つの他の当事者の１つにデータ要求を送信し、
少なくとも１つの他の当事者の前記１つからのデータ応答を、保護計算環境において前記サービス・プロバイダで受信し、
前記第１の要求と前記データ応答との間に一致が存在するかどうかを、前記契約に従って判断し、
前記判断ステップにより一致する結果が得られた場合には、前記一致の通知を前記少なくとも１つの他の当事者に提供する、
ステップを含む方法。
【請求項２】
前記判断ステップで判断したときに一致が存在しない場合であっても、前記通知を提供するステップをさらに含む、請求項１に記載の方法。
【請求項３】
前記通知を提供する前記ステップが、ダミー・メッセージを前記少なくとも１つの他の当事者に提供するステップを含む、請求項２に記載の方法。
【請求項４】
前記第１の要求が処理されたことを前記クライアントに通知するステップをさらに含む、請求項１に記載の方法。
【請求項５】
前記少なくとも１つの契約を実装する前記ステップが、前記サービス・プロバイダと、前記クライアントと、前記少なくとも１つの他の当事者との間のサービスを司るあらゆる契約に対して契約ＩＤを割り当てるステップを含む、請求項１に記載の方法。
【請求項６】
保護計算環境内の契約エンジンにおいて先のステップを実行するステップをさらに含む、請求項１に記載の方法。
【請求項７】
通信ネットワークに結合された複数の契約エンジンを提供するステップをさらに含む、請求項６に記載の方法。
【請求項８】
前記判断ステップが、暗号化コプロセッサにおいて判断を行うステップからなる、請求項１に記載の方法。
【請求項９】
多数当事者電子サービスのためのコンピュータ・ベースの方法であって、
サービス・プロバイダと、クライアントと、少なくとも１つの他の当事者との間のサービスを司るための少なくとも１つの契約を、コンピュータ・システムに実装し、
前記クライアントからの第１の要求と、少なくとも１つの他の当事者の１つからのデータ応答との間に一致が存在するかどうかを、前記契約に従って判断し、
前記判断ステップにより一致する結果が得られた場合には、前記一致の通知を前記少なくとも１つの他の当事者に提供する、
ステップを含む方法。
【請求項１０】
前記判断ステップで判断したときに一致が存在しない場合であっても、前記通知を提供するステップをさらに含む、請求項９に記載の方法。
【請求項１１】

前記通知を提供する前記ステップが、ダミー・メッセージを前記少なくとも１つの他の当事者に提供するステップを含む、請求項１０に記載の方法。

【請求項１２】

前記第１の要求が処理されたことを前記クライアントに通知するステップをさらに含む、請求項９に記載の方法。

【請求項１３】

前記少なくとも１つの契約を実装する前記ステップが、前記サービス・プロバイダと、前記クライアントと、前記少なくとも１つの他の当事者との間のサービスを司るあらゆる契約に対して契約ＩＤを割り当てるステップを含む、請求項９に記載の方法。

【請求項１４】

照合識別サービスを管理するためのコンピュータ・ベースの方法であって、

サービス・プロバイダと、クライアントと、少なくとも１つの他の当事者との間の照合識別サービスを司るための、契約ＩＤを有する少なくとも１つの契約を、コンピュータ・システムに実装し、前記クライアントからの第１の要求と、少なくとも１つの他の当事者の１つからのデータ応答との間に一致が存在するかどうかを、前記契約ＩＤに従って判断し、

前記判断ステップにより一致する結果が得られた場合には、前記一致の通知を前記少なくとも１つの他の当事者に提供する、

ステップを含む方法。

【請求項１５】

前記判断ステップで判断したときに一致が存在しない場合であっても、前記通知を提供するステップをさらに含む、請求項１４に記載の方法。

【請求項１６】

前記通知を提供する前記ステップが、ダミー・メッセージを前記少なくとも１つの他の当事者に提供するステップを含む、請求項１５に記載の方法。

【請求項１７】

前記第１の要求が処理されたことを前記クライアントに通知するステップをさらに含む、請求項１４に記載の方法。

【請求項１８】

多数当事者電子サービスのための装置であって、

サービス・プロバイダと、クライアントと、少なくとも１つの他の当事者との間のサービスを司るための少なくとも１つの契約を保持して履行し、前記クライアントからの第１の要求と、少なくとも１つの他の当事者の１つからのデータ応答との間に一致が存在するかどうかを、前記少なくとも１つの契約に従って判断するように作動する少なくとも１つのホスト・コンピュータを備え、

前記判断により一致する結果が得られた場合には、前記少なくとも１つのホスト・コンピュータが、前記少なくとも１つの他の当事者に通知を提供するようにさらに作動する装置。

【請求項１９】

前記少なくとも１つのホスト・コンピュータが、前記判断により一致する結果が得られない場合であっても、前記少なくとも１つの他の当事者に前記通知を提供するようにさらに作動する、請求項１８に記載の装置。

【請求項２０】

前記少なくとも１つのホスト・コンピュータが、ダミー・メッセージを前記少なくとも１つの他の当事者に提供するようにさらに作動する、請求項１９に記載の装置。

【請求項２１】

前記少なくとも１つのホスト・コンピュータが、前記第１の要求が処理されたことの通知を前記クライアントに提供するようにさらに作動する、請求項１８に記載の装置。

【請求項２２】

前記少なくとも１つのホスト・コンピュータが、

機密データを処理するための保護計算環境と、
前記保護計算環境及びネットワークとの間でメッセージを送受信するためのネットワーク・ハンドラと、
前記保護計算環境内部から送られてくるデータベース要求を処理し、保護されたデータベースから前記契約及び個人情報データを含む情報を取得するストレージ・ハンドラと、
を備える、請求項１８に記載の装置。
【請求項２３】
前記少なくとも１つのホスト・コンピュータが、前記サービス・プロバイダと、前記クライアントと、前記少なくとも１つの他の当事者との間のサービスを司るあらゆる契約に対して契約ＩＤを与えるようにさらに作動する、請求項１８に記載の装置。
【請求項２４】
照合識別サービスのための装置であって、
サービス・プロバイダと、クライアントと、少なくとも１つの他の当事者との間のサービスを司るための、契約ＩＤを有する少なくとも１つの契約を保持して履行し、前記クライアントからの第１の要求と、少なくとも１つの他の当事者の１つからのデータ応答との間に一致が存在するかどうかを、前記少なくとも１つの契約に従って判断するように作動する少なくとも１つのホスト・コンピュータを備え、
前記判断により一致する結果が得られた場合には、前記少なくとも１つのホスト・コンピュータが、前記少なくとも１つの他の当事者に通知を提供するようにさらに作動する装置。
【請求項２５】
前記少なくとも１つのホスト・コンピュータが、
機密データを処理するための保護計算環境と、
前記保護計算環境及びネットワークとの間でメッセージを送受信するためのネットワーク・ハンドラと、
前記保護計算環境内部から送られてくるデータベース要求を処理し、保護されたデータベースから前記契約及び個人情報データを含む情報を取得するストレージ・ハンドラと、
を備える、請求項２４に記載の装置。
【請求項２６】
前記保護計算環境が、前記第１の要求を処理し、照合タスクを行い、前記通知としての役割を果たす応答を提供するように作動する契約エンジンを備える、請求項２５に記載の装置。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、機密データの保護処理のためのシステム及び方法に関する。より具体的には、本発明は、必ずしも相互に信頼するとは限らない当事者が、処理と自らのデータの使用とを制御することが必要なシステムに関する。
【背景技術】
【０００２】
多くのＩＴアプリケーションは、機密データ、すなわち、ＩＴシステムが秘密又は機密を保持すべきデータの処理から構成される。こうしたアプリケーションの典型的な例は、飛行機搭乗前又は雇用前の、警戒リストとの対照による個人のスクリーニングである。こうしたスクリーニングは、氏名又は他の個人データの簡単なテキストベースの照合とすることが可能であり、特に、指紋の特徴点又は人間の顔の特徴などのバイオメトリクス（非特許文献１参照）を用いて、照合した個人の身元を確認するか、又は候補者の集合の中から個人を特定することができる。
【０００３】
データをコンピュータ・ネットワークを通じて送信するか又はストレージ・メディアに格納する際に、データを暗号化し、保護するための暗号化技術が存在する（例えば、非特

許文献２参照）。しかしながら、実際の処理ステップのためには、処理の間にコンピュータ・システムがデータを解釈し、変更し、新たなデータを得ることが可能になるように、データを自由に利用できなければならない。この処理の間、データは、処理環境に侵入してデータを探し出し、変更する攻撃者に対して脆弱である。ＩＴシステムには、その処理環境に入る方法を発見した攻撃者からプログラム及びデータを保護する手段がない。

【０００４】

ＩＴシステムを侵入者から保護する１つの方法は、機密データの処理を保護計算環境に限定することである（２００１年１１月６日に付与されたＳｃｈｎｅｃｋらの特許文献１、及び、引用によりここに組み入れられる非特許文献３参照）。保護計算環境は、ＦＩＰＳ　１４０－１　Ｌｅｖｅｌ　４妥当性検査を有するＩＢＭ　４７５８　暗号化コプロセッサのような汎用コンピュータ装置である（非特許文献４参照）。保護計算環境内の計算は、外部から監視することはできない。さらに、処理又は処理データを、保護計算環境の外部から悪意を持って変更することは不可能である。保護計算環境、内部で作動しているプログラム、又は内部で処理中のデータを改ざんしようとする試みは、該環境によって検出され、その後、該環境は、該環境内部に格納された機密データを破壊するか、又は該データに永久にアクセスできないようにする。

【０００５】

保護計算環境は、外部からの攻撃に対する保護を与えることができるが、システムによって当事者の保護要求及びプライバシー要求が満たされることを、該システム自体が保証することはできない。当事者は、自らのデータが予定通りの方法で処理されるアプリケーションのプロバイダを信頼しなければならない。当事者はサービスを制御できないため、このことに対する技術的な保証は存在しない。

【０００６】

当事者は、自らが処理とデータの使用とを制御できない場合、すなわち完全に信頼に頼らなければならない場合には、データ処理タスクに参加しようとしないことが多い。

【０００７】

既存のシステムは、関与する当事者にサービスを制御させないようにするか、又は、単に当事者の数を１つに減らして問題を回避する。例えば、幾つかの航空会社は、規則に従わない乗客のデータベースを持ち、乗客をこのデータと照合することがある。この場合、必然的に自らを信頼する航空会社は、全ての役割、すなわち、サービス・プロバイダ、情報プロバイダ、スクリーナ、及び通知された当事者のすべての役割を担当する。他のデータベースの例として、法執行エージェンシ（非特許文献５参照）又は信用履歴検査がある。これらのアプリケーションは、サービス・プロバイダでもあるインフォメーション・プロバイダによって完全に制御される。スクリーナである当事者には、該スクリーナが提供する情報をサービス・プロバイダがさらにどのように用いるかを制御する方法がない。同様の例は、乗客をその乗客のＩＤ文書の写真と照合する、空港での顔認識アプリケーションである。このアプリケーションは、サービス・プロバイダでもあるスクリーナによって完全に制御される。

【０００８】

例えば２００１年のスーパーボール又は幾つかの空港で用いられる顔認識システムのような既存の監視システム（非特許文献６参照）は、大部分が閉回路システムである。これらのシステムは、バイオメトリック・データを、ローカル・データベース、又は個人が所持するスマート・カードに格納された情報と比較する問い合わせに対して、直接応答を返す。したがって、対話中の異なる当事者が用いることが可能な、より一般的なサービスについての必要性が存在する。

【０００９】

サーバに対して認められる一連の要求を契約が定めるコンピュータ・プログラムを用いて、可能な対話パターンを定めるために、Ａｓｉｔ　Ｄａｎ及びＦｒａｎｃｉｓ　Ｎｉｃｈｏｌａｓ　Ｐａｒｒに対して２０００年１１月４日に付与され、全体が引用によりここに組み入れられる特許文献２に記載されるような他のシステムが用いられてきた。これら

のシステムでは、サービス・プロバイダは、サービス契約を決定する。この契約は、有効な別の要求Ｂが要求Ａに先行することを必要とする。当事者は、こうした種類の契約を用いて処理とデータの使用とを制御することができない。

【００１０】

多くの既存システムは、保護計算環境では実行されない。この場合、処理にアクセスする攻撃者は、自由にその処理を監視し、影響を及ぼすことができる。このように、当事者が処理ステップ及びデータの取扱いについて合意したとしても、こうした無保護環境において処理が該当事者のセキュリティ要件を満たすことを保証する技術的な方法は存在しない。

【００１１】

ウェブ・サービスに構築された既存システム（非特許文献７）は、どのサービス・プロバイダを選択するかをクライアントに制御させるが、サービスの機能自体は制御させない。

【００１２】

例えば、（非特許文献８）に記載されるようなサービス・レベル合意又はサービス合意の質などの明示的な契約を用いる既存のシステムは、リソース消費又は所要時間などの、サービスの非機能的な特徴に対応するのみである。こうした手法は、当事者にサービスの機能を制御させない。

【００１３】

【特許文献１】米国特許第６，３１４，４０９号明細書
【特許文献２】米国特許第６，１４８，２９０号明細書
【特許文献３】米国特許第６，１６７，５２１号明細書
【特許文献４】米国特許第５，６５０，９４８号明細書
【非特許文献１】Ａｎｌｉ Ｊａｉｎ、Ｌｉｎ Ｈｏｎｇ、及びＳｈａｒａｔｈ Ｐａｎｋａｎｔｉ、「Ｂｉｏｍｅｔｒｉｃ ｉｄｅｎｔｉｆｉｃａｔｉｏｎ」、Ｃｏｍｍｕｎｉｃａｔｉｏｎｓ ｏｆ ｔｈｅ ＡＣＭ、４３（２）、９０－９８ページ、ＡＣＭ Ｐｒｅｓｓ、２０００年
【非特許文献２】Ｂｒｕｃｅ Ｓｃｈｎｅｉｅｒ、「Ａｐｐｌｉｅｄ Ｃｒｙｐｔｏｇｒａｐｈｙ」、Ｊｏｈｎ Ｗｉｌｅｙ＆Ｓｏｎｓ、１９９６年
【非特許文献３】Ｓｅａｎ Ｗ． Ｓｍｉｔｈ及びＤａｖｅ Ｓａｆｆｏｒｄ、「Ｐｒａｃｔｉｃａｌ Ｐｒｉｖａｔｅ Ｉｎｆｏｒｍａｔｉｏｎ Ｒｅｔｒｉｅｖａｌ ｗｉｔｈ Ｓｅｃｕｒｅ Ｃｏｐｒｏｃｅｓｓｏｒ」、ＩＢＭ Ｒｅｓｅａｒｃｈ Ｒｅｐｏｒｔ、ＲＣ２１８０６、２０００年７月
【非特許文献４】ｈｔｔｐ：／／ｗｗｗ．ｉｂｍ．ｃｏｍ／ｓｅｃｕｒｉｔｙ／ｃｒｙｐｔｏｃａｒｄｓ
【非特許文献５】Ｊａｍｅｓ Ｘ．Ｄｅｍｐｓｅｙ、「Ｏｖｅｒｖｉｅｗ ｏｆ ｃｕｒｒｅｎｔ ｃｒｉｍｉｎａｌ ｊｕｓｔｉｃｅ ｉｎｆｏｒｍａｔｉｏｎ ｓｙｓｔｅｍｓ」、Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ｔｈｅ １０ｔｈ Ｃｏｎｆｅｒｅｎｃｅ ｏｎ Ｃｏｍｐｕｔｅｒｓ，Ｆｒｅｅｄｏｍ ａｎｄ Ｐｒｉｖａｃｙ、Ｔｏｒｏｎｔ、１０１～１０６ページ、ＡＣＭ Ｐｒｅｓｓ、２０００年
【非特許文献６】Ｓｃｈｏｌｚ及びＪｏｈｎｓｏｎ、「Ｉｎｔｅｒａｃｔｉｎｇ ｗｉｔｈ ｉｄｅｎｔｉｆｉｃａｔｉｏｎ Ｔｅｃｈｎｏｌｏｇｙ：Ｃａｎ ｉｔ ｍａｋｅ ｕｓ ｍｏｒｅ ｓｅｃｕｒｅ?」、Ｃｏｎｆｅｒｅｎｃｅ ｏｎ Ｈｕｍａｎ Ｆａｃｔｏｒｓ ｉｎ Ｃｏｍｐｕｔｅｒ Ｓｙｓｔｅｍｓ、Ｍｉｎｎｅａｐｏｌｉｓ、５６４～６５６ページ、ＡＣＭ Ｐｒｅｓｓ、２００２年
【非特許文献７】Ｖａｄｉｍ Ｄｒａｌｕｋ、「Ｄｉｓｃｏｖｅｒｉｎｇ Ｗｅｂ Ｓｅｒｖｉｃｅｓ：Ａｎ Ｏｖｅｒｖｉｅｗ」、Ｐｒｏｃｅｅｄｉｎｇｓ ｏｆ ｔｈｅ Ｔｗｅｎｔｙ－ｓｅｖｅｎｔｈ Ｉｎｔｅｒｎａｔｉｏｎａｌ Ｃｏｎｆｅｒｅｎｃｅ ｏｎ Ｖｅｒｙ Ｌａｒｇｅ Ｄａｔａ Ｂａｓｅｓ、Ｒｏｍａ、Ｉｔａｌｙ、６３７ページ、Ｍｏｒｇａｎ Ｋａｕｆｍａｎｎ、２０００年

【非特許文献８】Ｄｉｎｅｓｈ　Ｖｅｒｍａ、Ｍａｎｄｉｓ　Ｂｅｉｇｉ、及びＲａｙｍｏｎｄ　Ｊｅｎｎｉｎｇｓ、「Ｐｏｌｉｃｙ　Ｂａｓｅｄ　ＳＬＡ　Ｍａｎａｇｅｍｅｎｔ　ｉｎ　Ｅｎｔｅｒｐｒｉｓｅ　Ｎｅｔｗｏｒｋｓ」、Ｌｅｃｔｕｒｅ　Ｎｏｔｅｓ　ｉｎ　Ｃｏｍｐｕｔｅｒ　Ｓｃｉｅｎｃｅ、１９９５巻、１３７～１５２ページ、Ｓｐｒｉｎｇｅｒ－Ｖｅｒｌａｇ、２００１年

【発明の開示】

【発明が解決しようとする課題】

【００１４】

本発明は、必ずしも相互に信頼するとは限らない多数当事者が機密データの処理に参加することを可能にする。当事者間の関係は、処理システムが自動的に履行することができる契約によって保護される。契約は、要求が処理される方法と、この処理において個々の当事者によって提供される情報が用いられ、開示される方法とを定める。処理は、誰も該処理を監視することも改ざんすることもできないことを保証する保護計算環境で実行されることが好ましい。

【課題を解決するための手段】

【００１５】

本発明の一実施形態においては、契約がシステムに実装される前に、すべての当事者が該契約に合意することができる。このようにして、機密データの処理のためにサービスを用いる当事者は、その処理とそのデータの使用とを完全に制御することができる。

【００１６】

本発明の別の実施形態においては、依頼者が、処理要求をサーバに送信することによってデータ処理を起動する。処理自体は、監視することも外部から改ざんすることもできない。処理の最後に、サービスは、依頼者を含むこともある、直接的又は間接的に要求の処理に関わった幾つかの又はすべての当事者に、応答メッセージを送信する。

【００１７】

本発明のさらに別の実施形態においては、サービス要求の処理は、要求の処理の間に行われることになるアクションと、これらのアクション間における情報の流れ方とを指定する契約によって定められる。サービス要求の処理に協力する当事者は、システムが契約を実行する前に、該契約に相互に合意しなければならない。

【００１８】

本発明のさらに別の実施形態においては、要求の処理に協力する当事者は、要求の処理の間に計算されるデータ項目の所有者である。データ項目の所有者は、どの処理ステップに、又は他の当事者のどれに、データ項目を開示しようとするかを正確に制御することができる。

【００１９】

本発明の他の特徴及び利点は、添付図面と併せて解釈され、本発明の原理の明細並びに例を与える以下の詳細な説明から、明らかになるであろう。

【発明を実施するための最良の形態】

【００２０】

本発明は、機密データの保護処理のための方法を以下のように定めるものである、すなわち、

ａ）機密データの処理に協力する当事者は、まず、処理を構成する機能ステップと、個々の処理ステップで用いられるべきデータ項目とについて合意する関係を構築する。

ｂ）当事者は、契約に明示された、処理とデータの使用とについての公式仕様に合意する。契約は、他の情報の中から、処理の中の個々の処理ステップと、個々の処理ステップに対する入力として用いられるべきデータ項目と、処理ステップが処理状態に与える出力とを定める。

ｃ）サービスは、契約についてのインタプリタである。契約は、システムが該契約によって定められた機能を正確に実行し、意図した通りにのみデータ項目を用いることを保証する。特に、このことは、用いられる処理及びデータ項目が、外部から監視又は改ざんでき

ないことを意味する。

【００２１】

スクリーニング・シナリオの場合には、関与する当事者は、スクリーニング・サービスを行うサービス・プロバイダと、個人を検査しようとするスクリーナと、警戒リスト・データを提供する幾つかの情報プロバイダと、審査対象の個人が警戒リスト上に発見された場合に情報を与えられるべき、法執行、空港警備、又は人的資源などの他の当事者とになるであろう。

【００２２】

情報プロバイダは警戒リスト・データを機密扱いしようとし、すなわち、該プロバイダは、該データをスクリーニングに用いることは認めるが、該リスト上の情報はシステムの外に漏らすことはない。スクリーナは、審査対象の個人が警戒リストに現れない限り、該審査対象の個人についての基本的なプライバシーを保証しようとする。特に、スクリーナは、情報プロバイダがスクリーニング要求に基づいて任意の個人を追跡することを不可能にしようとする。スクリーナ及び情報プロバイダは、一致した場合のみ法執行に通知しようとし、他の場合には、情報を漏らすことはない。いずれの当事者も、サービス・プロバイダ又は侵入者に情報を漏洩しないようにすべきである。

【００２３】

図１は、本発明の実施形態に係る参加当事者間の概略的な作業の流れを示す。一般に、すべての処理は、以下のスキームによって表される。区別された当事者である依頼者１０１が、サービス要求１１０を保護要求処理１０２に送信する。この要求の処理を司り、契約に基づいて一連の処理ステップを実行する要求処理１０２は、その契約を判断する。要求処理１０２は、サービス契約に基づいてデータを当事者１０３から受信する。個々の処理ステップのアプリケーションは、処理状態のサブセットを入力として用いる。処理ステップの出力は、処理状態を拡張するのに用いられる。入出力の仕様は、契約内に定められる。処理の初期状態は、処理を起動させる要求からの情報で構成される。該当するすべての処理ステップが実行されると、要求処理１０２は、要求の処理に関わった当事者１０１、１０３、及び１０４のための応答メッセージ１１１を生成する。当事者のためのメッセージの内容が、契約内に指定される。

【００２４】

各々の要求は、異なる依頼者を有することがある。例えば、要求１１０が図１で処理された後、当事者１０３は、依頼者の役割を引き受け、自分のサービス要求１１２を送信することができる。異なる種類のサービス要求が異なる契約を呼び出し、該契約が次に、異なるサービス機能をクライアントに提供する。

【００２５】

典型的なアプリケーションにおいては、情報プロバイダ１０３が、時折、サービス要求１１２を送信して、サービスに提供する情報を更新することになる。この種の要求を制御する契約は、情報プロバイダからの要求内のデータをどのように用いてサービス内部の情報を変えるかを指定する。他のサービス要求は、その後、更新済みの情報を用いて処理される。

【００２６】

システムは、異なる当事者が異なる契約に基づいて同時に対話することを可能にする。例えば、スクリーニングの用途においては、多数の異なるスクリーナである当事者と、多数の異なる情報プロバイダと、多数の異なる法執行エージェンシが存在することになる。システムに送信された各々の要求は、指定された契約に基づいて処理を呼び出す。契約は、どの当事者がこの要求の処理に同時使用されるかを判断する。便宜上、以下にさらに示される複合契約も定められる。

【００２７】

処理は契約によって制御され、参加する当事者は契約を制御するので、参加する当事者は、処理と自分のデータが用いられる方法とを完全に制御することになる。保護計算環境において契約を実行することにより、情報が漏洩せず、誰もデータの処理を改ざんできな

いことが保証される。

【００２８】

図２は、本発明の実施形態による契約によって定められ、制御される保護データ処理のためのシステムの全体構造のブロック図を示す。一般に、処理は、サーバ２０１がネットワーク接続２０４を通じてサービス要求２００を受信したときに開始される。要求２００は、要求ハンドラ２０５と、タスク処理２０８と、レスポンダ２０９とから構成される契約エンジン２０３によって処理される。３つの要素のすべては、処理状態２０７と連動し、契約２０６によって制御される。

【００２９】

要求ハンドラ２０５は、まず、送られてくる要求が有効で、処理に受け入れられるかどうかを検査する。要求ハンドラは、要求の内容と該要求を送信した当事者とを、この特定のサービス要求の処理を定め、制御する契約２０６に定められた情報と照合することによって、この検査を行う。

【００３０】

本発明によって説明されるシステムでは、サービス要求の処理は、契約２０６によって制御される。契約（図６を見よ）は、サービス要求の処理に協力するすべての当事者によって相互に合意される公式仕様である。契約は、サーバが要求を処理する方法と、この処理の際に情報が個々の処理ステップ間で開示され、集約される方法とを正確に定め、制御する。

契約は、

ａ）要求の処理に協力する当事者、

ｂ）要求メッセージ内に与えられるデータ項目、

ｃ）要求の処理の間に実行されなければならない個々のアクション、

ｄ）アクションを実行した結果として生成されるデータ項目、及び、これらのデータ項目の所有権、

ｅ）個々のアクションのアプリケーションを制御する作業の流れ、

ｆ）データ項目の所有者がどの処理ステップを開示しようとし、どの処理ステップを開示しようとしないかを正確に制御することを可能にする、個々のアクション間の制御されたデータの流れ、

を指定する。

公式データ・モデル、及び契約に関するさらなる詳細が、以下に与えられる。

【００３１】

送られてくるサービス要求２００の要求ハンドラ２０５による検査が失敗した場合には、該要求は拒否される。そうではなく、すべてが許容された場合には、処理は、タスク処理２０８内における要求処理の個々のタスクの処理を続ける。

【００３２】

タスク処理２０８は、２つのデータ構造を用いる。処理の根拠となる契約２０６、及び、要求処理の過程で個々の処理タスクによって作成されるデータ項目を蓄積する処理状態２０７である。図３で分かるように、処理状態２０７は、ＩｔｅｍＳｅｔ（項目セット）と呼ばれる名前／値ペアの順序付きセットである。

【００３３】

当初は、タスク処理２０８の処理状態２０７は、入力サービス要求２００によって提供されたデータ項目のみからなる。タスク処理２０８は、契約２０６を用いて、サービス要求を処理するために実行されるべき一連のタスクを判断する。タスク処理２０８はまた、処理状態のどの部分が、サービス要求の処理を含む個々のタスクに送られるべきかを契約から判断する。次いで、契約の中にも定められるタスクの結果を用いて、処理状態を拡張し、次のタスクに使用できるようにする。タスク処理は、契約を読み込むのみであるが、処理状態２０７を読み込んで、修正する。契約が指定するすべてのタスクが指定された順序で処理されると、タスク処理２０８は終了する。

【００３４】

すべてのタスクがタスク処理２０８によって処理された後、制御は、レスポンダ２０９に受け渡される。レスポンダは、主に、協力する当事者に送出される応答メッセージ２１０を生成する。応答は、処理状態から生成される。実際には、レスポンダ２０９は、タスク処理２０８と同様のものである。主な違いは、レスポンダ２０９によって実行されるタスクは、所定の意味体系を有するため、特殊なものであるということである。

【００３５】

契約２０６は、電子的な形式でコンピュータ・プログラムが解釈し、実行することができる。保護計算環境２０２で実行される場合には、契約が電子的に実行されることによって、すべてのステップが指定された順序で処理されること、及び契約が提示する通りに情報が正確に流れることが保証される。

【００３６】

保護計算環境２０２は、閉鎖されたコンピュータであるため、内部処理は外部から監視することができず、適切な許可なしでは、外部の誰も装置内部の計算又はデータを改変することはできない。こうした装置は、装置を開き、侵入し、又は探ろうとする試みを検出する。改ざんしようとするこれらの試みのいずれかが検出された場合には、保護計算環境は、内部に格納された機密データを破壊し、作動を完全に中止する。こうした保護計算環境の一例は、ＩＢＭ４７５８プログラマブル暗号化コプロセッサである。

【００３７】

保護計算環境２０２の保護機能は、コンピュータ・ネットワーク上の通信に拡張することができる。これは、２つの保護計算環境間のネットワーク通信に、標準的な暗号化技術を用いることによって達成することができる。このように保護された、チャネル２０４としても知られる通信セッションは、チャネルを通じて通信されるデータが攻撃者に読み取られないようにする。通信セッションはまた、攻撃者が、いつメッセージを改変し、自分自身のメッセージを挿入し、又は保護計算環境の１つになりすまそうとしたかを、検出することを可能にする。当然のことながら、ネットワークは信頼されておらず、すべての暗号化技術は、保護計算環境の内部に実装されなければならない。チャネルについてのさらなる詳細については、図５の記述を参照されたい。

【００３８】

本発明で説明されるシステムが保護計算環境内に実装されない場合には、様々な攻撃者に対して極めて脆弱となることに注目する必要がある。具体的には、無保護環境では、要求２００及び処理状態２０７が攻撃者からアクセス可能になるので、契約を電子的に実行しても、情報が指定されたタスクにのみ流れ、公開も改変もされないことが保証されない場合がある。

【００３９】

図３ａは、本発明の実施形態による契約の構造を統一モデリング言語（ＵＭＬ）のクラス図として示す。各々の契約（Ｃｏｎｔｒａｃｔ）３０７は、その契約をシステム内の他のすべての契約と一意的に区別する契約ＩＤ（ｃｏｎｔｒａｃｔＩＤ）を有する。契約３０７は、サービス要求を満たすことに協力するであろう１つ又はそれ以上の当事者（当事者（ｐａｒｔｉｅｓ））を指定する。個々の当事者を記述する当事者（Ｐａｒｔｙ）クラス３０１は、システム内の当事者の固有ＩＤ（ｉｄ）と、サービス要求の処理に応答してサービスがメッセージを送信できるネットワーク・アクセス・ポイントとを含む。サービス・アクセス・ポイントは、例えば、インターネット・アドレス及びポート番号、又は、ユニフォーム・リソース・ロケータ（ＵＲＬ）によって定めることができる。当事者クラスは、当事者の名前を含むこともできる。一実施形態においては、当事者のこの最小定義は、要求の保護処理には必要ないが当事者間の付加的な関係を維持するために必要な場合がある番地（ＳｔｒｅｅｔＡｄｄｒｅｓｓ）などの属性によって、さらに増加する場合がある。

【００４０】

契約３０７はさらに、処理されるべきサービス要求の到着である単一のアクション（トリガー（ｔｒｉｇｇｅｒ））を指定する。要求到着（ＲｅｑｕｅｓｔＡｒｒｉｖａｌ）ク

ラス３０４のオブジェクトは、この契約によって定められ、制御される処理を起動する、送られてくる要求を記述する。

【００４１】

契約３０７はさらにまた、要求の処理の間に実行されるゼロ又はそれ以上の処理ステップ（タスク（ｔａｓｋｓ））を指定する。タスクは、タスク（Ｔａｓｋ）オブジェクト３０５によって作成されるタスク仕様の順序付きリストとして与えられる。さらに契約は、要求の処理後にシステムが協力当事者に対して応答するのに用いるゼロ又はそれ以上の出力メッセージ（応答（ｒｅｓｐｏｎｓｅｓ））を指定する。応答は、応答仕様の順序付きリストとして与えられる。アクション（Ａｃｔｉｏｎ）３０２は、要求到着３０４と、タスク３０５と、応答（Ｒｅｓｐｏｎｓｅ）３０６との共通のアブストラクションである。各々のアクションは、名前（名前（ｎａｍｅ））と、完了後に提供されるデータ項目（項目仕様セット（ＩｔｅｍＳｐｅｃＳｅｔ））の順序付きセットの仕様（出力仕様（ｏｕｔｐｕｔＳｐｅｃ））とを有する。アクションは、単一の当事者（オーナー（ｏｗｎｅｒ））によって所有される。

【００４２】

実施することができる多数のアクションが存在する。第１のタイプのアクションは、新たなサービス要求の到着、すなわち要求到着３０４である。この場合、オーナーは、この種の要求を送信することができる依頼者、すなわち当事者を定める。要求到着アクションの出力仕様は、要求内に存在するデータ項目を記述する。各々の要求は、この要求の処理を定め、制御する契約を一意的に特定するのに用いられる契約ＩＤと呼ばれる少なくとも１つの必須項目を有する。

【００４３】

第２のタイプのアクションは、機能（Ｆｕｎｃｔｉｏｎ）３０３である。機能は、データ項目の順序付きセットを入力（入力仕様（ｉｎｐｕｔＳｐｅｃ））として取得し、データ項目の順序付きセットを出力（ｏｕｔｐｕｔＳｐｅｃ）として戻す。機能の実行は、ブール式（述部）によって制御される。ブール式は、特殊定数「真」及び「偽」と、ブール演算子「ｎｏｔ」、「ａｎｄ」、及び「ｏｒ」と、関係演算子＜、＜＝、＝、／＝、＞、＞＝と、任意定数と、図２に示される処理状態における項目名とから構成される式である。機能は、その述部が真を戻した場合のみ、実行される。

【００４４】

タスク３０５は、協力する当事者（そのオーナー）の１つによって定められ、任意の機能を実行することができる機能である。実行されることになる機能は、タスクを実装するコードを参照することによって定められる。

【００４５】

応答３０６は、タスクと同様のものであるが、応答が提供する機能は、事前に定められ、固定される。この機能は、協力当事者が変更することはできない。同様に、応答の出力仕様の項目数は１つに固定される。しかしながら、この戻りコードの名前は、自由に定めることができる。

【００４６】

図３ｂは、本発明の実施形態による項目セット（ＩｔｅｍＳｅｔ）及び項目仕様セットのＵＭＬ仕様を示す。項目仕様セット３１１は、入力仕様及び出力仕様を定めるのに用いられる。項目仕様セットは、項目仕様（ＩｔｅｍＳｐｅｃ）３１２と呼ばれるデータ項目仕様の順序付きセットを定める。データ項目仕様は、その名前（ｎａｍｅ）によってデータ項目を特定する。項目（Ｉｔｅｍ）クラス３１４によって定められるデータ項目は、名前／値のペアである。項目セット３１３は、データ項目の順序付きセットである。

【００４７】

図４Ａは、本発明の実施形態に係る、要求ハンドラ、タスク処理、及びレスポンダの処理のフローチャート図を示す。送られてくる要求は、図３で定められる項目セットとすることができる。サーバが新たなサービス要求を受信したときは、要求ハンドラはまず、ステップ４００において、要求の要素である項目セットから必須項目の契約Ｉｄを取り出す

。契約Ｉｄ項目の値によって、ステップ４０１で、要求ハンドラが、送られてくるサービス要求の処理を制御する契約を取得することが可能になる。次にステップ４０２で、要求ハンドラは、この送信者からの要求を受け入れるかどうかを検査する。要求ハンドラは、この検査のために、契約のトリガーを所有する当事者を選択し、その当事者を、チャネルの他端に存在し、該チャネルを通じて要求を受信した当事者と比較する。両方の値が同一の当事者であることを示した場合には、要求がさらに処理されることが考慮され、そうでなければ、処理は、ステップ４０３においてエラー・ハンドラを用いて終了する。

【００４８】

次の検査は、ステップ４０４において、要求が完全であるかどうか、すなわち、契約が必要とするすべての項目を該要求が提供するかどうかを判断するものである。この検査は、トリガーの出力仕様に定められたすべての名前が、要求の項目セットの中に正確に一度現れ、かつ、それらが定められた値を有することを肯定することによって実施される。項目が現れる順序は問題にはならない。要求が、トリガーの出力仕様に記述されない付加的な項目を有する場合は、エラーとはみなされない。次に続く処理ステップのいずれもこれらの項目にはアクセスできないので、該項目は、要求処理によって無視されるだけであり、損なわれることはない。エラーの場合には、要求処理は、ステップ４０３で終了する。

【００４９】

両方の検査を通った場合には、要求ハンドラは、ステップ４０５において、タスク処理のために処理状態Ｓを初期化する。初期の処理状態は、トリガー出力仕様によって名前が指定された項目をそのまま含む。

【００５０】

タスク処理は、ステップ４１０で始まる。契約の順序付きタスク・リストにはより多くのタスクが存在するが、タスク処理は、ステップ４１１において、順番に次のタスクＴを選択する。

【００５１】

ステップ４１２は、処理状態ＳにわたってＴの述部を評価する。タスクの述部は、処理状態のすべての項目にアクセスすることができる。評価されている式は、すべての当事者に対して契約から明らかであるので、当事者は、所与の述部の評価について、処理状態の項目の特定の使用に関してすでに合意したことが明らかである。述部がｆａｌｓｅを与える場合には、タスクＴは無視され、処理は、ステップ４１０において、タスクのリスト内の次のタスクを用いて続く。タスクの述部が真と評価された場合には、ステップ４１３が、新たな項目セットｓを作る。処理は、タスクＴの入力仕様の中に項目の名前を発見した場合には、処理状態Ｓの項目を新たな項目セットｓに挿入する。

【００５２】

ステップ４１４は、Ｔのタスク仕様からタスクの実装を判断し、次いで、唯一のパラメータとして新たな項目セットｓを用いて該タスクの実装を呼び出す。この呼び出しの結果は、項目セットｒである。ステップ４１５は、名前がタスクＴの出力仕様に現れるすべての項目をｒから取り出して、それらを処理状態Ｓに挿入する。ステップ４１５は、ｒからの新たな値を用いてＳの既存値をオーバーライドすることはない。同一の名前を持つ項目が既に存在する場合には、その項目も同一の値を持つはずであり、そうでなければ、契約は正当なものではない。しかしながら、タスクの述部又はそれらの実装が、２つのアクティブにされたタスクが同一の項目名について異なる値を生成しないことを保証する場合には、幾つかのタスクは、その出力仕様に同一の項目仕様を指定することができる。

【００５３】

タスクのすべてが処理されると、タスク処理ユニットは、制御をレスポンダに渡す。これは、ステップ４２０に示される。応答の処理は、タスク処理と同じ基本構造に従う。

【００５４】

未処理の応答仕様が存在するが、レスポンダは順番にそれらを処理する。ステップ４２１及び４２２における応答の取り出し及び応答の述部の評価は、タスク処理のステップ４１１及び４１２における処理と同一であり、ステップ４２３は４１３と同様である。ステ

ップ４２３において、処理状態Ｓと実際の応答Ｒの入力仕様とから新たな項目セットｓを生成した後、ステップ４２４は、応答仕様の中にＲの所有者として定められた当事者Ｐからネットワーク・アクセス・ポイントを取り出し、それを用いて、ｓを応答メッセージとしてＰに送出する。

【００５５】

各々の応答仕様についての出力仕様は、単一の要素を持つセットである。この要素の値は、ブール値であり、応答を当事者Ｐに配信するのに成功したかどうかを記述するものである。この項目の名前は、自由に定めることができる。項目は、処理状態Ｓに追加され、したがって、まだ処理されていない他の応答がアクセスすることができる。具体的には、このことによって、別の応答が成功したか失敗したかに応じて応答を送出するか、又は、他のメッセージに以前の応答の戻りコードを含ませることができる。すべての応答が処理されると、全要求処理は、ステップ４２６で無事に終了する。

【００５６】

タスク及び応答の順次処理は、簡単であるという利点があるが、必ずしも極めて効率的な処理を可能にするとは限らない。一実施形態は、アクション間の依存関係を判断することを選択し、アクションの入力仕様に与えられたすべての項目が利用可能であるときには、独立のアクションを同時に実行する。

【００５７】

図５は、本発明の実施形態に係る、ネットワークと保護されたデータベースとの統合を示す。保護計算環境５０６、ネットワーク・ハンドラ５０３、及び大容量ストレージ・ハンドラ５０５の１つ又はそれ以上と、同一のホスト・コンピュータ上の１つ又はそれ以上の保護されたローカル・データベース５０４との集合体は、サービス・セル又は単にセルとも呼ばれる。例えばＩＢＭ４７５８プログラマブル暗号化コプロセッサのような保護計算環境には、データベース又はネットワークに直接アクセスする方法がない場合がある。図５は、保護計算環境５０６内部のアプリケーション・コードが、安全にデータベース５０４及びネットワーク５０２にアクセスすることができる方法を示す。契約と、例えば警戒リストなどのすべてのデータ項目とがデータベース５０４に格納されるので、ネットワーク５０２に送信されるすべてのメッセージは、暗号化技術によって保護される。

【００５８】

ホスト・コンピュータ５０１は、保護計算環境５０６、ネットワーク・ハンドラ５０３、大容量ストレージ・ハンドラ５０５、及びデータベース５０４のホストとなる。ネットワーク・ハンドラ５０３は、ホスト・コンピュータ５０１のオペレーティング・システムに対する呼び出しを用いて、ネットワーク５０２にアクセスし、保護計算環境内部から送られてくるネットワーク要求を処理する。大容量ストレージ・ハンドラ５０５は、ＳＱＬなどの標準的なデータベース・インターフェースを用いて、データベース５０４にアクセスし、保護計算環境内部から送られてくるデータベース要求を処理する。

【００５９】

ネットワーク・ハンドラ５０３は、ネットワーク５０２との間でメッセージを送受信する。メッセージは、暗号化技術、すなわち、暗号化、認証、メッセージ要約、及びシーケンス番号を用いて保護される。これにより、監視者が、検出されずにメッセージの内容を解釈することも変更することもできないことが保証される。ネットワーク・ハンドラ５０３は、暗号化された入力メッセージをネットワーク５０２から受信し、それを保護計算環境５０６内部のチャネル・ハンドラ５０７に与える。チャネル・ハンドラ５０７は、暗号化チェックサムを検査し、シーケンス番号を取り外し、データを暗号解除する。ここで、保護計算環境５０６内部の契約エンジン５０８は、データに自由にアクセスすることができる。

【００６０】

契約エンジン５０８がネットワークを通じてメッセージを送出しようとするときは、該契約エンジンは、該メッセージを暗号化してシーケンス番号及びメッセージ要約を追加するチャネル・ハンドラ５０７に、該メッセージを送信する。次いで、チャネル・ハンドラ

５０７は、ホスト５０１上ではあるが保護計算環境５０６の外部にあるネットワーク・ハンドラ５０３に暗号化されたメッセージを送信し、該ネットワーク・ハンドラ５０３は、次に、該メッセージをネットワークに送信する。

【００６１】

契約エンジン５０８がデータベース５０４にアクセスしようとする場合には、該契約エンジンは、チャネル・ハンドラ５０７に平文の要求を送信し、該チャネル・ハンドラは、要求内のデータを暗号化して、それをホスト５０１上ではあるが保護計算環境５０６の外部にある大容量ストレージ・ハンドラ５０５に送る。大容量ストレージ・ハンドラは、データベース５０４に直接アクセスし、該データベースからの結果をカード内部のチャネル・ハンドラ５０７に戻すことができ、そこで返答は暗号解除され、契約エンジンに戻される。

【００６２】

最適化のために、契約エンジン５０８は、データベース５０４からのデータの一部を、保護計算環境５０６内部のキャッシュ５１０に格納することができる。これによって、チャネル・ハンドラ５０７と、大容量ストレージ・ハンドラ５０５と、データベース５０４とを通り、大容量ストレージ・ハンドラ５０５と、チャネル・ハンドラ５０７とを通って戻る、コストのかかる往復を避けることができる。

【００６３】

図６は、本発明の実施形態に係る、個人が厳重に警戒リストと照合される用途のための契約例を示す。図６は、個人を犯罪者の警戒リストと照合するのに用いることができる契約６０１についての例を与えるものである。テーブルに与えられた情報は、図３ＡのＵＭＬクラス図に定められた変数に対応する。この例では、契約識別番号６０２は「４７１１Ｂ５」であり、Ａ、Ｂ、Ｃと名前が付けられた関与する当事者６０３は、申込者を審査しようとする空港６０３Ａと、照合されることになる警戒リストを提供する政府機関６０３Ｂと、一致が見出されたときに通知されるべき法執行官庁６０３Ｃとである。

【００６４】

テーブルの行には、契約に定められたアクションによって作成される個々のデータ項目が記載される。データ項目の各々のブロックについて、第１列には、データ項目を作成するアクションと、このアクションの所有者と、該アクションが実施される条件とが記述される。この列は、各々の処理ステップ及び応答について、どのデータ項目が入力として渡されるかを記述する。

【００６５】

行６０４は、サービス要求を定める。欄６０５は、当事者Ａのみが要求を送信できることを示す。行６０４の第２列の欄６０６は、どのデータ項目が要求の中に存在しなければならないかを示す。行６０７は、この契約の処理タスクを定める。この例では、３つの処理ステップ、すなわち、行６０８の「１：ｎ照合」、行６０９の「バイオメトリック照合」、及び行６１０の「おとり生成」が存在する。行６０８の第２列の欄６１１は、タスク「１：ｎ照合」の出力仕様のデータ項目を定める。行６０９及び６１０の第２列の欄は、これらのタスクについての単一のデータ項目のみを持つ出力仕様を定める。行６１２は、この契約の可能な４つの応答を定める。行６１２の第１列の欄は、応答の名前と、所有者と、述部とを、すなわち、応答がどのように呼ばれるか、応答がどの当事者に送信されるか、及び応答がどの条件の下で送信されるか、を定める。行６１２の第２列の欄は、応答の出力仕様の中の個々の戻り値を定める。

【００６６】

列６０８は、タスク及び応答についての入力仕様を定める。各々のタスクについての列と、各々の応答についての列が存在する。欄の中のプラス記号（＋）は、プラス記号が現れている行によって特定されるデータ項目が、列が属するタスク又は応答の入力仕様の一部であることを示す。行ａ、列ｂのスラッシュ（／）は、行ａのデータ項目が、列ｂのタスク又は応答の入力仕様に属さないことを示す。空欄（　）は、データ項目が未計算のため、該データ項目がこの入力仕様に含まれるべきか否かを決定する意味がないことを示す

。
【００６７】
この契約例は以下のように解釈される、すなわち、処理は、契約Ｉｄと、名と、姓と、誕生日と、指紋データと、場所と、トランザクション番号とを含む、当事者Ａが送信する要求６０４によって起動される。
【００６８】
最初の処理ステップは、ＸＹＺという名前の警戒リストとの１：ｎ照合６０８である。この処理ステップは、当事者Ｂが所有し、無条件に（述部＝真）実行される。「１：ｎ照合」という名前の列は、＋記号を用いて、この処理ステップついての入力、すなわち、名と、姓と、誕生日とを定める。列６０８には、出力、すなわち、照合が成功したかどうかを示す値と、名と、姓と、誕生日と、容疑者クラスと、ファイルからの指紋データと、前科に関する情報と、反応アドバイスとが定められる。
【００６９】
次の処理ステップ６０９は、バイオメトリック照合を用いる。バイオメトリック照合は、当事者Ｃが所有し、１：ｎ照合が成功した場合にのみ実行される。入力は、実際の指紋データ、及び１：ｎ照合ステップからの指紋データである。出力は、これら２つの指紋の間の相関を示す値である。
【００７０】
次に、おとり生成処理ステップ６１０は、１：ｎ照合が成功しなかった場合に、おとりメッセージを生成する。
【００７１】
契約は、行６１２において、当事者Ｃに対する３つの代替的な応答と、当事者Ａに対する１つの応答と、当事者Ｂに対する無応答とを定める。すべての応答は、受信者が該応答を確認したか否かを示す単一の出力値を有する。応答１は、１：ｎ照合が成功し、かつ、個人の容疑者クラスが＜５の場合に、Ｃに送信される。この応答は、名と、姓と、誕生日と、場所と、バイオメトリック照合の出力とを含む。応答２は、１：ｎ照合が成功し、かつ、容疑者クラスが＞４の場合に、Ｃに送信される。この応答は、応答１と同じ欄に加えて、反応アドバイスを含む。応答３は、１：ｎ照合が失敗した場合に送信される。この応答は、おとりメッセージのみを含み、検査対象の個人に関するデータは含まない。応答４は、当事者Ａに送られる。この応答は、実際の要求と共に到着したトランザクション番号と、サービスが通知当事者Ｃにおいて成功したかどうかを示す値とを含む。
【００７２】
図６から、前科に関する情報は、この契約の下では、いかなる当事者にも開示されないことが明らかである。１：ｎ照合が失敗した場合には、個人に関する情報が送信されないことも明らかである。（おとりメッセージは、実データを含まず、単に、サービスと当事者Ｃとの間の通信を監視できる攻撃者から一致又は非一致の事実を隠すために送信される。）
【００７３】
当事者がサービス要求の処理に協力することができるようになる前に、当事者はまず、この種の要求を処理するに当たって最初に定められ、合意された基本を定め、制御する契約に合意しなければならない。すべての当事者が合意した後にのみ、この契約に基づく処理がサーバ内でアクティブにされる。アクティブにされた契約のセットは、当事者によって動的に拡張されることがある。新たな契約を導入し、アクティブにすることによって、サービスは、新たな種類の要求の処理方法を学習する。
【００７４】
契約は、データ構造、すなわち電子文書として表すことができる公式仕様と考えることができる。一実施形態においては、相互合意による契約は、すべての当事者が契約の電子署名付き複製をサーバにアップロードする方法でアクティブにされる。サーバが、すべての当事者からこうした署名付き複製を受信し、電子署名を検証し、すべての複製が実際に同一の契約を指定していることを確認した後、処理は自動的にアクティブにされる。

【００７５】
同様に、電子的に提出された契約は、いつでも、又は契約の期限が切れたときに、取り消すこともできる。当事者がそのように合意した場合には、単一の当事者が契約を取り消すことができ、契約の期限が切れた場合には、システムは、この契約が司る要求を受け付けるのを中止する。
【００７６】
依頼者が、同時に実行しようとする多数の契約を有する場合には、これらの契約をグループ化し、単一の要求に代えて実行することができる。幾つかの他の契約を束ねた契約は、複合契約と呼ばれる。複合契約の構造は、基本的な契約の構造と極めて類似する。違いは、複合契約は処理ステップ及び応答を定めるのではなく、組み合わされるべき契約のＩＤを列挙するのが好ましいことである。基本的な契約と同様に、複合契約もトリガーを有する。このトリガーの出力仕様は、この複合契約内で組み合わされるべき基本的な契約の出力仕様の結合を定める。契約エンジンは、受信した要求に関する副契約を呼び出すことによって、複合契約を処理する。
【００７７】
例えば、スクリーニングの用途においては、これは、スクリーナが、エージェンシＡからの警戒リストと照らし合わせて審査を行うための契約と、エージェンシＢからの警戒リストと照らし合わせて審査を行うための別の契約とを有することを可能にする。組み合わされた契約は、システムに対する単一の要求に代えて、両方の検索を呼び出すことになる。他の複合契約は、さらに他の組み合わせとの照合を可能にすることができる。
【００７８】
エントリー・ポイントで走査されたバイオメトリック情報は、要求内に入れて、データを処理し、該データを多数のデータベースと照合することができる１つ又はそれ以上のサーバに送信することができる。作業の流れは、審査対象の個人に関するデータをスクリーナに戻す代わりにアラームを法執行エージェンシに送信することを含めて、参加する当事者が全面的に判断する。
【００７９】
提案された処理の実装の正確さに関する公式証明は、契約エンジンと、個々の処理ステップについてのコードとの検証を必要とする。このように構築されたすべてのシステムは同一の契約エンジンを用いるため、契約エンジンの検証は、１回限りのタスクである。個々の処理ステップについてのコードは、該コードがシステムに導入されるときに検証されなければならない。個々の処理ステップについてのコードは、異なる契約が再利用することができ、それが、全体の検証作業を最小にする。
【００８０】
個々の処理ステップの名前のみを提供するのとは対照的に、個々の処理ステップのコードを契約の一部にすることによって、前述のシステムの動的な特徴をさらに向上させることができる。コードを安全にサービスにダウンロードすることを可能にする技術については、例えば、全体が引用によりここに組み入れられる（２００年１２月２６日に付与されたＳｍｉｔｈらの特許文献３）を参照されたい。処理ステップについてのコードを提供することによって、当事者がサービスの機能を動的に拡張することが可能になり、検証処理を局所的に行うことができる。
【００８１】
図１を用いて、本発明の実施形態に係る、参加当事者間における作業の流れの具体例を示す。スクリーナ１０１が、サービス要求１１０を保護要求処理１０２に送信する。この要求の処理を司り、契約に基づいて一連の処理ステップを実行する要求処理１０２は、その契約を判断する。個々の処理ステップのアプリケーションは、処理状態のサブセットを入力として用いる。処理ステップの出力は、処理状態を拡張するのに用いられる。入出力の仕様は、契約内に定められる。処理の初期状態は、処理を起動させる要求からの情報で構成される。該当するすべての処理ステップが実行されたときには、処理状態を用いて、要求の処理に関わった当事者１０１、１０３、及び１０４’のための応答メッセージ１１

１が生成される。どの当事者が通知を受け、該当事者に送信される応答にどんな情報が含まれるかもまた、契約に指定される。

【００８２】

図７は、本発明の実施形態に係る可能な分散の一例を示す。本発明のサービスは、相互接続された幾つかのサービス・セルから構成される。１つのセルは、１つ又はそれ以上の保護計算環境と、ネットワーク・ハンドラと、大容量ストレージ・ハンドラと、１つ又はそれ以上の保護されたデータベースとを含むことができる。１つの物理的位置に多数のセルを導入することができるが、図７に示されるように、２つ以上の物理的位置が存在することになる。図７に示されるように、セル８０１～８０６は、異なる場所に存在することができる。クライアントが、利用可能なセルのサブセットに接続されることがある。

【００８３】

この構成によって、十分な量のリソースが可能になり、個々の誤作動に対する複合サービスの高度な耐障害性がもたらされる。さらに、この構成は、地理的及び／又は国家的（法律的）な問題に応じて、サービス及びデータを容易に分割することができるという効果がある。

【００８４】

本発明は、より小規模なシナリオに実装することができるが、アーキテクチャは、世界規模のサービスに備えたものである。

【００８５】

図８は、本発明の実施形態に係る、異なる保護範囲を示す。暗号化コプロセッサ９０７、９１０は、サービス内（９０８、９０９、９１１）だけでなく、クライアントＡ及びＢに配置される。コプロセッサ９０７～９１１は、保護ストレージ及び通信セグメント９０１～９０６と共に物理的に配置され、それらすべては、セル外周９２０～９２４の内部に配置される。

【００８６】

したがって、すべての機密操作は、保護暗号化コプロセッサ９０７～９１１内部に閉じ込められる。データベースの内容は常に暗号化され、保全性はメッセージ要約によって確保される。セル間の通信は、暗号化され、認証され、改変及びリプレイから保護される。最終的に、セル外周９２０～９２４は、ファイアウォール及びシステムレベルのアクセス制御を用いて保護される。

【００８７】

図９は、本発明の実施形態に係るスクリーニング・シナリオを示す。まず最初は、サーバ・セル１１０３に対するスクリーナ１１０１からのスクリーニング要求１１１０で始まる。セル１１０３は、ネットワーク・ハンドラ１１０６を通じて要求を受信し、処理のために該要求をコプロセッサ１１０８に伝える。スクリーニングに用いられるべき警戒リストがこのセル内で利用可能な場合には、コプロセッサ１１０８は、個人に関する情報についてデータベース１１０９に問い合わせを行う。次いで、コプロセッサは、ネットワーク・ハンドラを用いて、法執行１１０７に通知する。この通知は、どんな場合でも送信される。一致しなかった場合には、通知には、法執行においてアラームとして表示されないおとりが含まれる。法執行１１０７の確認通知が受信された後、スクリーナ１１０１は、自分の要求が処理されたことの通知を受ける。

【００８８】

別のシナリオも同様である。この場合の主な違いは、警戒リストがスクリーナのクライアント・セル１１０３で局所的に利用できないことである。この場合には、このセルは、必要なテーブルを有するセル１１０５に要求を転送する。このセル１１０５も、法執行１１０７に通知し、転送された要求についての通知を返信し、該通知はスクリーナ１１０１に返信される。

【００８９】

図１０は、本発明による一実施形態の一般構造を示す。処理の大部分は図１０に示されるコプロセッサ内部で実施されることになるが、ＰＣＩバス１２１０及びシリアル・ポー

トは、カードがその環境と通信を行う唯一の方法であるため、本発明の一部はホスト１２０４上に実装することができる。

【００９０】

ホスト・アプリケーションは、ネットワーク・アクセス１２２４及び大容量ストレージ１２２６を提供しなければならない。ホスト・アプリケーションはまた、カード／ホスト通信のホスト部分１２２０を実装しなければならない。無保護ホスト１２０４は、ホスト／カード・インターフェース１２２０と、ネットワーク・ハンドラ１２２４と、大容量ストレージ・ハンドラ１２２６と、データベース１２２８とを含む。しかしながら、保護計算環境１２０２は、保護処理の主要部分を取り扱うために、コプロセッサ１２０６と、他のコプロセッサ１２０８とを含む。

【００９１】

図１１は、本発明の実施形態に係る機能モジュール図を示す。図１１は、異なるインターフェース及び幾つかのセル１５１０、１５１０′などから構成される基本的な要素のアーキテクチャを示す。システムに対する要求は、ユーザ・インターフェースによって生成される。異なるクライアントに対して異なるインターフェースが存在する。サービス・プロバイダは、設定インターフェースＳＰ　Ｃｏｎｆｉｇ１５７０と、サービスの請求を制御し、管理する請求インターフェース１５７１とを有する。スクリーニング当事者もまた、設定インターフェースＳＣ　Ｃｏｎｆｉｇ１５７２と、スクリーニング要求を送信するグラフィカル・ユーザ・インターフェースＳＣ　ＧＵＩとを有する。スクリーニング当事者が、自動的に要求を生成することができるＩＴシステムであるＳＣ　Ｂａｃｋｅｎｄをすでに保有している場合がある。この場合には、そのシステムをサービスに接続するために、統合コンポーネントＳＣ　ＢＥ　Ｉｎｔｅｇｒが必要である。情報プロバイダ当事者もまた、既存システムＩＰ　Ｂａｃｋｅｎｄをサービスに接続するために、種々のインターフェース１５７３、すなわち統合インターフェースＩＰ　ＢＥ　Ｉｎｔｅｇｒを必要とする。サービス設定のために、専用インターフェースＩＰ　Ｃｏｎｆｉｇが存在する。法執行もまた、設定インターフェースＬＥ　Ｃｏｎｆｉｇ１５７４と、アラーム・メッセージが表示されるグラフィカル・ユーザ・インターフェースＬＥ　Ｎｏｔｉｆ．ＧＵＩとを有する。状況に応じて、アラーム・メッセージをＬＥ　Ｎｏｔｉｆ．ＧＵＩから法執行バックエンド・システムＬＥ　Ｂａｃｋｅｎｄに転送することもできる。

【００９２】

各々のセル、すなわちセル１５１０及び他のセル１５１０′は、ホスト・アプリケーション１５２０と、１つ又はそれ以上のコプロセッサ（コプロセッサ１５４０、他のコプロセッサ）とで構成される。ホスト・アプリケーション１５２０は、インターフェースが接続されるネットワーク・ハンドラ１５２３を介して要求を受信する。ネットワーク・ハンドラ１５２３は、ホスト－カード通信コンポーネント１５２４を介して、このセル１５１０内のコプロセッサ１５４０、１５４０′の１つに要求を転送する。ホスト・アプリケーションのもう１つのコンポーネントは、ホスト－カード通信コンポーネント１５２４を介してコプロセッサ１５４０からデータベースの問い合わせを受信し、それをローカル又は遠隔データベース１５２１に配信するストレージ・ハンドラ１５２２である。コプロセッサ１５４０の内部では、ネットワーク・ハンドラ１５２３から送られてくる要求は、暗号化／暗号解除と認証とセッションとを実装し、平文の要求を要求ハンドラ１５４３に転送するネットワーク・チャネル・ハンドラ１５４１によって、処理される。要求ハンドラ１５４３は、要求の完全性及び正確性について検査し、次いで、該要求を専門のハンドラの１つに委任する。スクリーニング要求ハンドラ１５４６はスクリーニング要求を処理し、設定要求ハンドラ１５４５はサービス内部の制御構造の更新を可能にし、更新要求ハンドラ１５４４はスクリーニングに用いられる警戒リストの内容を変更することができ、セル間ハンドラ１５５０は要求を他のセル１５１０′に転送し、データを他のセルに配布するのに用いられる。セル間ハンドラ１５５０は、要求ハンドラ１５４３からネットワークの質に関するフィードバックを得て、ネットワークを通る最適経路に関して動的に学習するグローバル・セル・モデル１５４９によって制御される。大部分のハンドラは、設定ハン

ドラ１５４７によって提供される設定情報にアクセスし、かつ、ホスト上のデータベース１５２１にアクセスすることが必要であり、後者のアクセスは、次にデータベース・チャネル・ハンドラ１５４２を用いるバケット・ハンドラ１５４８によって提供される。データベース・チャネル・ハンドラ１５４２は、データベース１５２１との間を行き来するデータのすべての暗号化／暗号解除及び認証を取り扱う。

【００９３】

図１２Ａ～図１２Ｃは、本発明の他の実施形態に係る、可能な異なる設計を示す。図１２Ａから図１２Ｃまでは、単一のセルについての可能な異なる設計を示すものであり、図１２Ａは単層を、図１２Ｂは２層を、図１２Ｃは複製アプリケーション・サーバを備える２層を示す。単層の環境においては、セルは、ファイアウォール２０１１と、ホスト・アプリケーション・サーバ２０１０とを含むことになる。２層の場合には、ファイアウォール２０１１及び２０２１が用いられ、データベース・サーバ２０４０は、ホスト・アプリケーション・サーバ２０２０から分離される。図１２Ｃに示される構成は、多数のホスト・アプリケーション・サーバ２０２０を含む。

【００９４】

本発明の別の実施形態は、契約の動的な特徴を減少させることもできる。さらに極端な場合には、システムを、１つの契約か又は少数の異なる契約に完全に特化することができる。技術的には、これは、既知の契約を持つ契約エンジンの部分評価と、結果として得られるコードの最適化とによって行うことができる。これは、例えば、全体が引用によりここに組み入れられる（１９９７年７月２２日に付与されたＧａｆｔｅｒの特許文献４）の手法を用いて行うことができる。結果は、契約が明示的なデータ・オブジェクトではなく、当事者間の合意の履行がプログラム・コードに組み込まれている静的実装と等価である。こうした実施形態においては、契約の取り消し、及び新たな契約の合意には、ソフトウェアの一部を再生成又は再実装し、再インストールし、サービスを再始動することが必要である。

【００９５】

提示された実施例は、本発明についての多くの可能な使用方法を網羅するものではないことを理解すべきである。

前述の説明から、当業者であれば、本発明の本質的な特徴を容易に把握することができ、本発明の精神及び範囲から逸脱することなく、本発明を様々に変更及び修正して、様々な利用及び条件に適合させることができる。

本発明は、上述の唯一の実施形態に限定されるものではなく、あらゆる実施形態が添付の特許請求の範囲に包含されることを理解すべきである。

【図面の簡単な説明】

【００９６】

【図１】本発明の実施形態に係る参加当事者間の概略的な作業の流れを示す。

【図２】本発明の実施形態による契約によって定められ、制御される保護データ処理のためのシステムの全体構造のブロック図を示す。

【図３Ａ】本発明の実施形態による契約の構造を統一モデリング言語（ＵＭＬ）のクラス図として示す。

【図３Ｂ】本発明の実施形態による項目セット及び項目仕様セットのＵＭＬ仕様を示す。

【図４Ａ】本発明の実施形態に係る、要求ハンドラ、タスク処理、及びレスポンダの処理のフローチャート図を示す。

【図４Ｂ】本発明の実施形態に係る、提案から契約までの状態遷移図を示す。

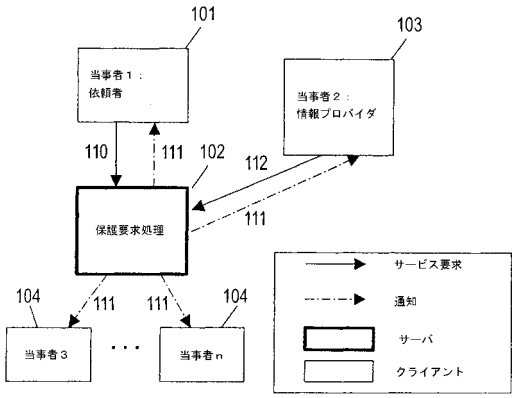
【図４Ｃ】本発明の実施形態に係る、アップロードから仕様の取消しまでの状態遷移図を示す。

【図５】本発明の実施形態に係る、ネットワークと保護されたデータベースとの統合を示す。

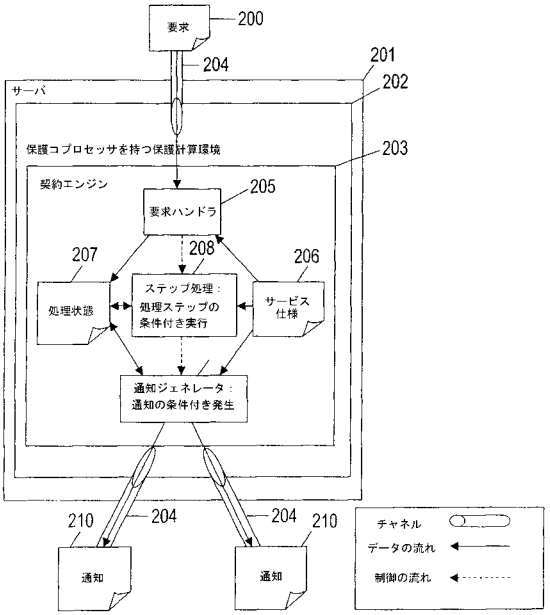
【図６】本発明の実施形態に係る、個人が厳重に警戒リストと照合されるアプリケーションのための契約例を示す。

【図７】本発明の実施形態に係る可能な分散の一例を示す。
【図８】本発明の実施形態に係る、異なる保護範囲を示す。
【図９】本発明の実施形態に係るスクリーニング・シナリオを示す。
【図１０】本発明による一実施形態の一般構造を示す。
【図１１】本発明の実施形態に係る機能モジュール図を示す。
【図１２Ａ】本発明の他の実施形態に係る、可能な異なる設計を示す。
【図１２Ｂ】本発明の他の実施形態に係る、可能な異なる設計を示す。
【図１２Ｃ】本発明の他の実施形態に係る、可能な異なる設計を示す。

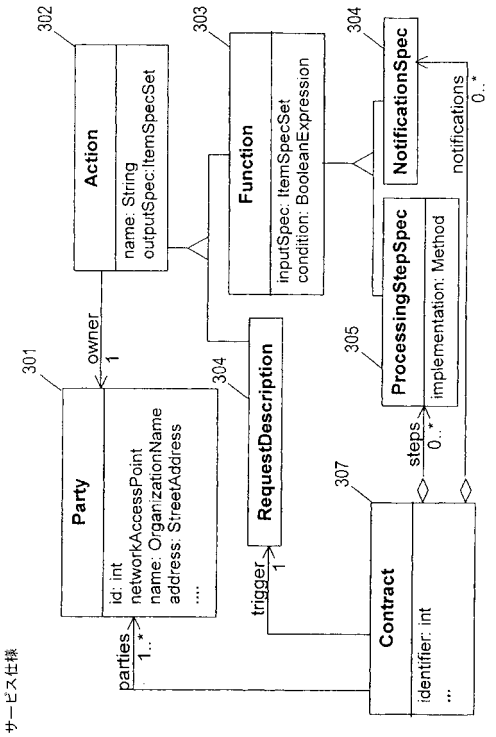
【図１】



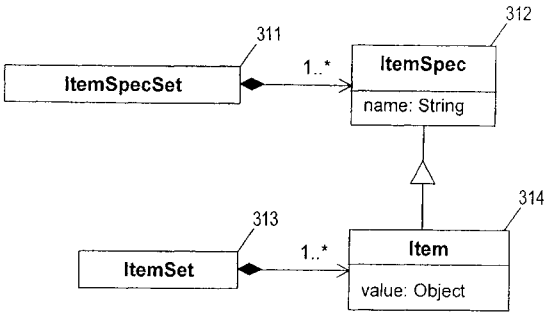
【図２】



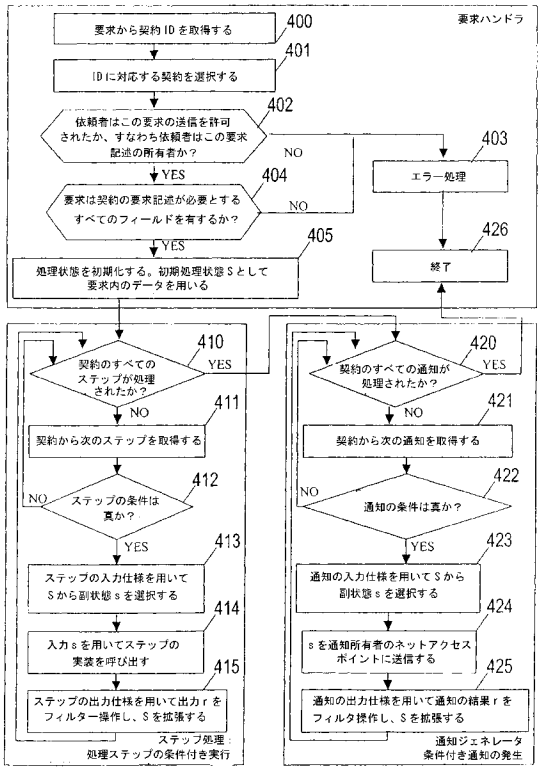
【図３Ａ】



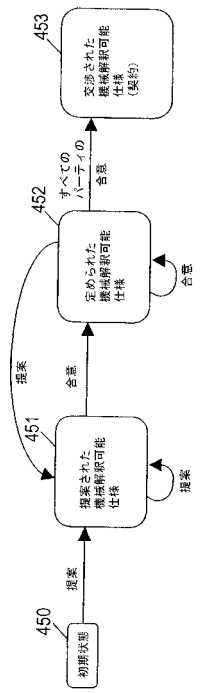
【図３Ｂ】



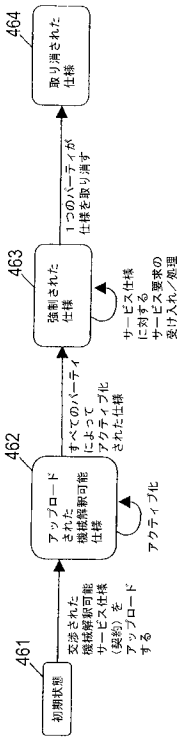
【図４Ａ】



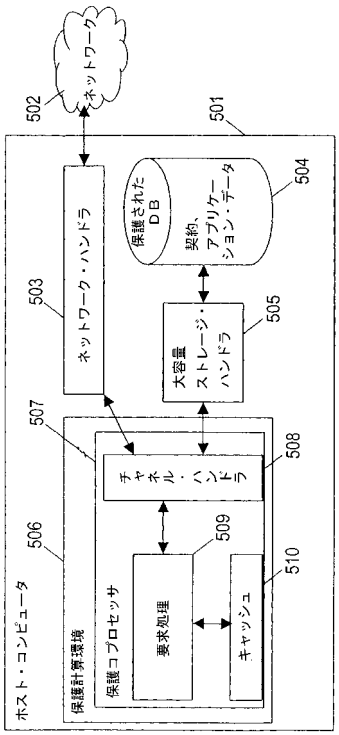
【図４Ｂ】



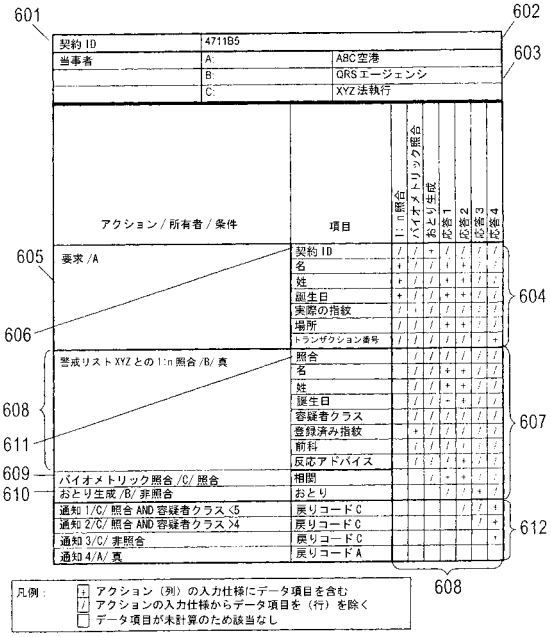
【図４Ｃ】


464
取り消された仕様
1つのパーティが仕様を取り消す
463
強制された仕様
サービス仕様に対するサービス要求の受け入れ／処理
すべてのパーティによってアクティブ化された仕様
462
アップロードされた機械解釈可能仕様
アクティブ化
交渉された機械解釈可能サービス仕様（契約）をアップロードする
461
初期状態

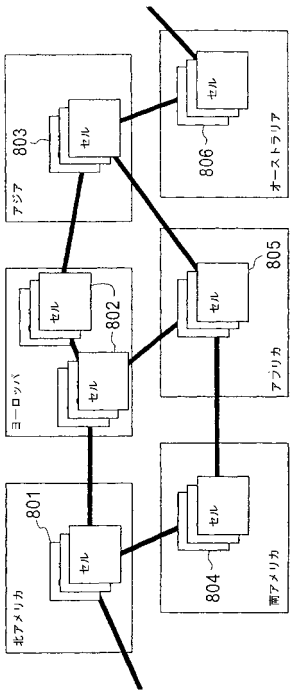
【図５】


ネットワーク
502
501
504
保護された DB
契約、アプリケーション・データ
503
ネットワーク・ハンドラ
505
大容量ストレージ・ハンドラ
507
508
チャネル・ハンドラ
506
509
510
要求処理
キャッシュ
保護計算環境
保護コプロセッサ
ホスト・コンピュータ

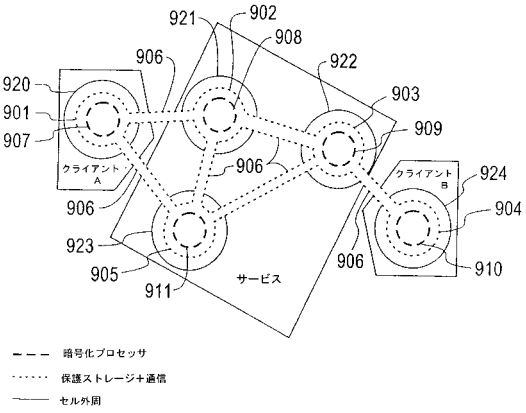
【図６】


601
602
603
契約 ID
4711B5
当事者
A:
ABC空港
B:
QRSエージェンシ
C:
XYZ法執行
アクション／所有者／条件
項目
1:n照合
バイオメトリック照合
おとり生成
応答1
応答2
応答3
応答4
605
要求 /A
契約 ID
名
姓
誕生日
実際の指紋
場所
トランザクション番号
604
606
警戒リスト XYZ との 1:n 照合 /B/ 真
照合
名
姓
誕生日
容疑者クラス
登録済み指紋
前科
反応アドバイス
607
608
611
609
610
バイオメトリック照合 /C/ 照合
相関
おとり生成 /B/ 非照合
おとり
通知 1/C/ 照合 AND 容疑者クラス <5
戻りコード C
通知 2/C/ 照合 AND 容疑者クラス >4
戻りコード C
通知 3/C/ 非照合
戻りコード C
通知 4/A/ 真
戻りコード A
612
608
凡例：
アクション（列）の入力仕様にデータ項目を含む
アクションの入力仕様からデータ項目を（行）を除く
データ項目が未計算のため該当なし

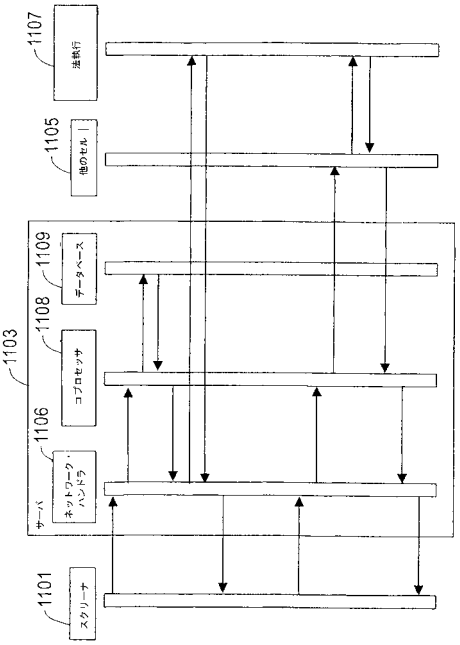
【図７】


アジア
803
セル
オーストラリア
806
セル
ヨーロッパ
802
セル
セル
アフリカ
805
セル
北アメリカ
801
セル
南アメリカ
804
セル

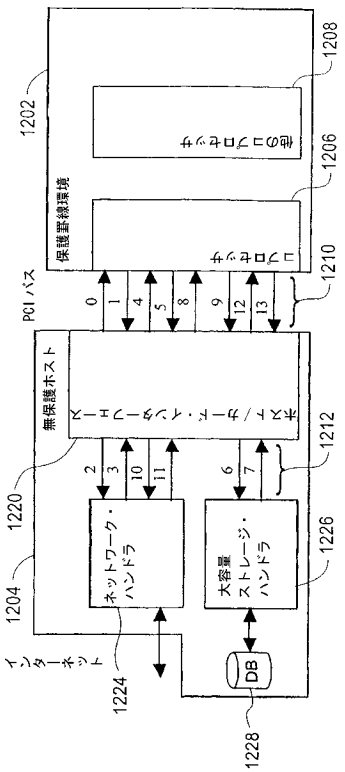
【図８】


921
902
908
906
922
920
901
907
903
909
クライアントA
906
924
クライアントB
906
904
923
905
911
サービス
906
910
暗号化プロセッサ
保護ストレージ＋通信
セル外周

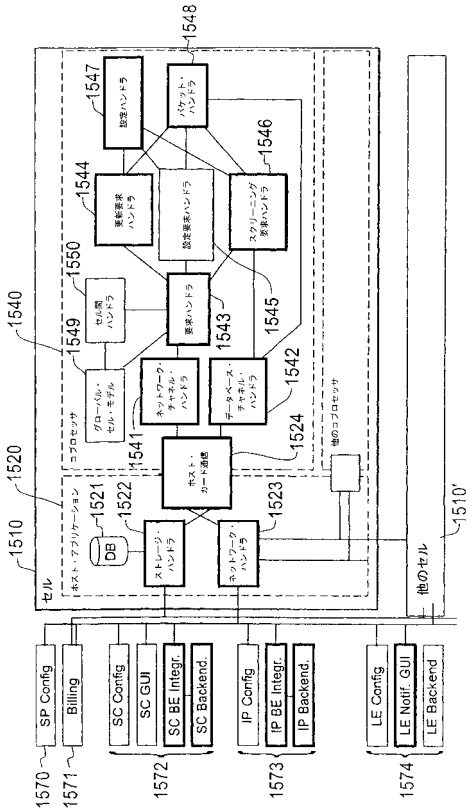
【図９】


1107
法執行
1105
他のセル
1109
データベース
1108
コプロセッサ
1103
1106
サーバ
ネットワーク・ハンドラ
1101
スクリーナ

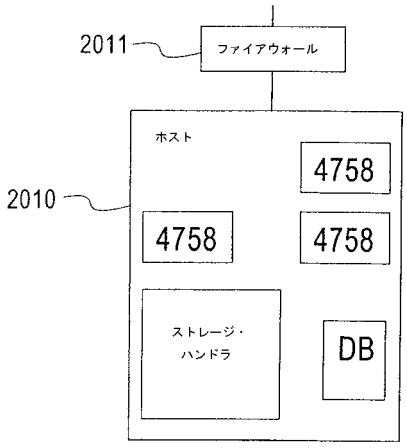
【図１０】


1208
1202
他のコプロセッサ
保護署線環境
1206
コプロセッサ
1210
PCIバス
0
1
4
5
8
9
12
13
無保護ホスト
メモリ／ホーム・ネットワーク
1212
1220
2
3
10
11
6
7
1204
ネットワーク・ハンドラ
大容量ストレージ・ハンドラ
1226
インターネット
1224
DB
1228

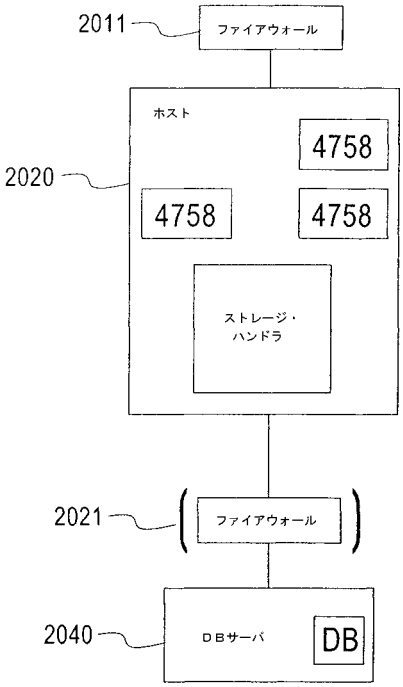
【図１１】


1548
1547
設定ハンドラ
パケット・ハンドラ
1546
1544
要求要求ハンドラ
設定要求ハンドラ
プログラミング要求ハンドラ
1550
セル間ハンドラ
1549
1543
要求ハンドラ
1545
1540
グローバル・セル・ギルド
ネットワーク・チャネル・ハンドラ
データベース・チャネル・ハンドラ
1542
他のコプロセッサ
1541
1524
ホスト・カード通信
1520
1521
1522
1523
1510
セル
ホスト・アプリケーション
DB
ストレージ・ハンドラ
ネットワーク・ハンドラ
1510'
他のセル
SP Config
Billing
SC Config
SC GUI
SC BE Integr.
SC Backend
IP Config
IP BE Integr.
IP Backend
LE Config
LE Notif. GUI
LE Backend
1570
1571
1572
1573
1574

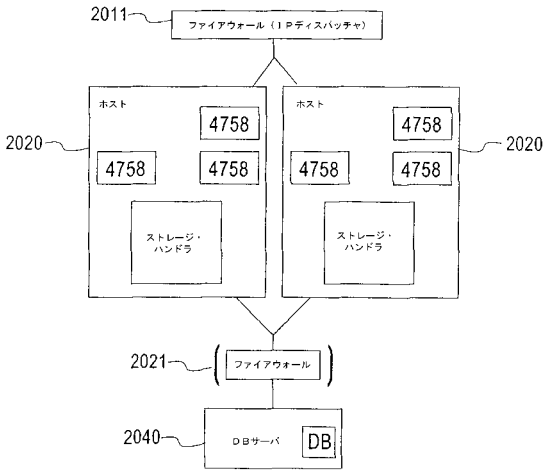
【図１２Ａ】



【図１２Ｂ】



【図１２Ｃ】



【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/25720

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : G06F 15/16
US CL : 709/201, 203, 229
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/201, 203, 229

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, E	US 6,658,568 B1 (Ginter et al.) 02 December 2003, Abstract, col. 4, line 60 - col. 13, line 51, col. 17, line 1 - col. 19, line 45, col. 21, line 27 - col. 23, line 53, col. 33, lines 5-25, col. 39, lines 36-67.	1-27

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
20 July 2004 (20.07.2004)

Date of mailing of the international search report
16 AUG 2004

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703)305-3230

Authorized officer
Le H Luu
for Michelle R. Cour

Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

フロントページの続き

(81)指定国 AP(GH,GM,KE,LS,MW,MZ,SD,SL,SZ,TZ,UG,ZM,ZW),EA(AM,AZ,BY,KG,KZ,MD,RU,TJ,TM),EP(AT,BE,BG,CH,CY,CZ,DE,DK,EE,ES,FI,FR,GB,GR,HU,IE,IT,LU,MC,NL,PT,RO,SE,SI,SK,TR),OA(BF,BJ,CF,CG,CI,CM,GA,GN,GQ,GW,ML,MR,NE,SN,TD,TG),AE,AG,AL,AM,AT,AU,AZ,BA,BB,BG,BR,BY,BZ,CA,CH,CN,CO,CR,CU,CZ,DE,DK,DM,DZ,EC,EE,ES,FI,GB,GD,GE,GH,GM,HR,HU,ID,IL,IN,IS,JP,KE,KG,KP,KR,KZ,LC,LK,LR,LS,LT,LU,LV,MA,MD,MG,MK,MN,MW,MX,MZ,NI,NO,NZ,OM,PG,PH,PL,PT,RO,RU,SC,SD,SE,SG,SK,SL,SY,TJ,TM,TN,TR,TT,TZ,UA,UG,UZ,VC,VN,YU,ZA,ZM,ZW

(72)発明者 トラップ、マルティン
ドイツ連邦共和国 ７６５３４ バーデンバーデン ブラームスシュトラーセ ８
(72)発明者 ツウィスラー、ソーニャ
ドイツ連邦共和国 ７２２５０ フロイデンシュタット マイ マンヴェーク ６

Ｆターム(参考) 5B285 AA01 AA04 BA01 BA10 CA31 CB01