(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2006-500657

(P2006-500657A)

(43)公表日　平成18年1月5日(2006.1.5)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B017
G06F 21/24	(2006.01)	G06F	12/14	530D	5B285
H04L 9/08	(2006.01)	G06F	12/14	540A	5J104
		G06F	12/14	540P	
		G06F	12/14	560B	

審査請求 未請求　予備審査請求 未請求　（全 25 頁）　最終頁に続く

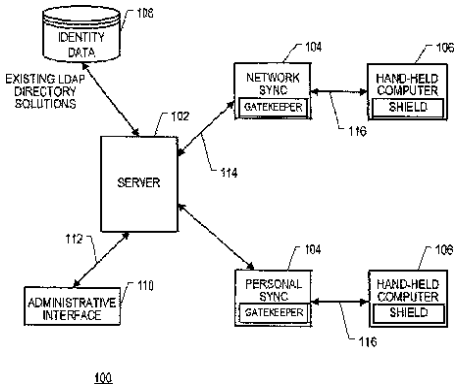
(21)出願番号　特願2004-537963 (P2004-537963)
(86)(22)出願日　平成15年9月19日 (2003.9.19)
(85)翻訳文提出日　平成17年3月23日 (2005.3.23)
(86)国際出願番号　PCT/US2003/029347
(87)国際公開番号　WO2004/028070
(87)国際公開日　平成16年4月1日 (2004.4.1)
(31)優先権主張番号　10/252,212
(32)優先日　平成14年9月23日 (2002.9.23)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　10/252,225
(32)優先日　平成14年9月23日 (2002.9.23)
(33)優先権主張国　米国 (US)
(31)優先権主張番号　10/252,213
(32)優先日　平成14年9月23日 (2002.9.23)
(33)優先権主張国　米国 (US)

(71)出願人　505105763
クレダント　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　テキサス州　７５００１　アディソン　ダラス　パークウェイ　１５３０５　スイート　１０１０
(74)代理人　100082005
弁理士　熊倉　禎男
(74)代理人　100067013
弁理士　大塚　文昭
(74)代理人　100074228
弁理士　今城　俊夫
(74)代理人　100086771
弁理士　西島　孝喜

最終頁に続く

(54)【発明の名称】セキュリティポリシーの維持及び配信をサポートするためのサーバー、コンピュータメモリ、及び方法

(57)【要約】
無線ネットワークアクセスノードに接続されるサーバー上に配置されたサーバーモジュールは、開放されている。サーバーモジュールは、複数の無線デバイスのためのユーザー情報を収容するデータベースを含む。データベース内の各エレメントは、許可された少なくとも1つの無線デバイスに帰するものであり、次のグループ、すなわち(i)無線接続性許可、(ii)許可された無線デバイスの識別情報、及び(iii)許可されたネットワークアクセスノードの情報、からの少なくとも1つの形式のデータファイルを含む。



【特許請求の範囲】
【請求項１】
複数の無線デバイスのユーザー情報を収容するデータベース、
を備え、前記データベースの各要素が、許可された少なくとも1つの無線デバイスに依るものであり、かつ、(i)無線接続許可、(ii)許可された無線デバイスの識別情報、及び、(iii)許可されたネットワークアクセスノードの情報、で構成されるグループからの少なくとも1つの形式のデータファイルを収容する、
ことを特徴とする、無線ネットワークアクセスノードに接続されたサーバーに配置されたサーバーモジュール。
【請求項２】
モバイルコンピューティングデバイスのセキュリティ機能との接続に使用する複数の動作鍵、及び、
前記複数の動作鍵を暗号化するルート鍵、
を備えることを特徴とするコンピューターメモリ。
【請求項３】
モバイルコンピューティングデバイスにおいてセキュリティポリシーを施行する方法であって、
前記モバイルコンピューティングデバイスにおいて、少なくとも1つのデバイス使用制限を含むポリシーを受け取るステップと、
前記モバイルコンピューティングデバイスのユーザーが、前記使用制限によって排除された使用に関与することを禁止することにより、前記モバイルコンピューティングデバイスにおいて、前記ポリシーを施行するステップと、
を含むことを特徴とする方法。
【請求項４】
モバイルコンピューティングデバイスのユーザーからパスワードを受け取るステップ、
非線形関数を適用することにより、前記パスワードからセキュリティコードを引き出すステップ、及び、
前記パスワードを暗号鍵として使用して、前記セキュリティコードを暗号化するステップ、
を含むことを特徴とするセキュリティ方法。
【請求項５】
モバイルコンピューティングデバイスに、サーバー上のソフトウェアアプリケーションへのアクセスを選択的に提供する方法であって、
前記ソフトウェアアプリケーションにアクセスする要求を、前記モバイルコンピューティングデバイスから受け取るステップ、及び、
前記コンピューティングデバイスが、インストール済みのセキュリティプログラムを持っているかどうかを調べることにより、前記ソフトウェアアプリケーションへのアクセスを許可するかどうかを定めるステップ、
を含むことを特徴とする方法。
【請求項６】
サーバー及びクライアントモジュールで共有される共有暗号鍵を提供し、
前記共有暗号鍵を使って、前記クライアント上のデータを暗号化し、
パスワードを受け取ることにより、前記クライアントが常駐するモバイルコンピューティングデバイスのユーザーを認証し、
前記パスワードを使って、前記共有鍵を復号化し、
更新されたポリシー及び鍵材料を復号化するために、前記共有鍵を使用し、かつ、
前記モバイルコンピューティングデバイスにあるポリシー及び鍵材料を、前記更新及び復号化されたポリシー及び鍵材料で置き換える
ステップを含むことを特徴とする、ポリシー及び鍵材料を更新する方法。
【請求項７】

無線デバイス上に配置されたクライアントモジュール、
同期をとる間、前記クライアントモジュールに選択的に繋がれるネットワークモジュール、及び、
前記ネットワークモジュールに繋がれたサーバーモジュール、
を備え、前記クライアントモジュールが、前記ネットワークモジュール及び前記サーバーモジュールから独立した無線コンピューティングデバイスの使用を認証するようにされたことを特徴とする無線セキュリティシステム。
【請求項８】
ネットワークモジュールからモバイルコンピューティングデバイスにセキュリティソフトウェアアプリケーションをインストールする方法であって、
サーバーから伝達されたセキュリティポリシー及び鍵材料を含むネットワークモジュールを提供し、
前記モバイルデバイスが前記ネットワークモジュールと同期をとっている間、前記モバイルセキュリティデバイスへのセキュリティソフトウェアプログラムのインストールを開始し、
ワンタイムパスワードを要求し、
前記モバイルコンピューティングデバイスにおいて、前記ワンタイムパスワードを受け取り、かつ、
前記鍵材料と関連付けられるルート鍵を復号化するために、前記ワンタイムパスワードを使用する
ステップを含むことを特徴とする方法。
【請求項９】
サーバーからモバイルコンピューティングデバイスへセキュリティポリシー情報を配信する方法であって、
前記サーバーとゲートキーパーの間の接続を認証し、
ポリシーパッケージを前記ゲートキーパーに送り、
前記モバイルコンピューティングデバイスと前記ゲートキーパーの間のデータ同期をとることを開始し、
前記モバイルコンピューティングデバイスを認証し、かつ、
前記ゲートキーパーから前記モバイルコンピューティングデバイスに前記ポリシーパッケージを送る
ステップを含むことを特徴とする方法。
【請求項１０】
無線デバイス上に配置されたクライアントモジュールであって、
前記無線デバイスが伝達することのできる許可されたデバイスのリストを含むポリシーデータベース、
を備えることを特徴とするクライアントモジュール。
【請求項１１】
無線デバイス上に配置されたクライアントモジュールであって、
前記無線デバイスについての少なくとも2つのユーザープロファイルを収容するポリシーデータベース、
を備えることを特徴とするクライアントモジュール。
【請求項１２】
無線接続許可に関する規則を含むポリシーデータベース、及び、
前記ポリシーデータベースのルールを施行する知的エージェント、
を備えることを特徴とする、無線デバイス上に配置されたクライアントモジュール。
【請求項１３】
無線デバイスに配置されたクライアントモジュールであって、
ポリシーデータベース、及び、
前記無線デバイスの許可されない使用を監視するように構成された、前記ポリシーデー

タベースに応答するエージェント、
を備えることを特徴とするクライアントモジュール。
【請求項１４】
(i)複数のプロファイルデータ、(ii)接続許可、(iii)許可された無線デバイスの識別情報、及び(iv)許可されたネットワークアクセスノードの情報、から成るグループからの少なくとも1つの形式のデータファイルを含むポリシーデータベース、
前記ポリシーデータベースのルールを施行する知的エージェント、及び、
無線接続の履歴情報を収容するアクティビティログ
を備えることを特徴とする、無線デバイスに配置されたクライアントモジュール。
【請求項１５】
許可された無線デバイスのリストを含むポリシーデータベース、及び、
前記ポリシーデータベースのルールを施行するエージェント、
を備えることを特徴とする、無線ネットワークアクセスノードに配置されたネットワークモジュール。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、セキュリティポリシーの配信及び施行のシステム及び方法に関するものである。
【背景技術】
【０００２】
企業環境における、携帯情報端末(PDA)のようなモバイルデバイスの使用は、来たる3～3年にわたって、大幅に成長することが予測される。これらのスマートデバイスは、数に加えて、多様性、及び性能も増大している。これらのデバイスは、計量モビリティ、利便性、及び、電子メール、カレンダー、アドレス帖、及び他のドキュメントのような情報への瞬時アクセスを提供する機能性の固有の調和を提供する。多くの企業は、プラットフォームをミッションクリティカルなツールに変換するモバイルデバイスのための、及び、企業の機密データの責任のための特別なアプリケーションを開発している、又は導入した。
【０００３】
結果として、モバイルデバイスは、ビジネス通信における不可欠なツールとなった。これらのデバイスの使用は、業界の専門家により急速に成長することが予想される。
【０００４】
モバイルコンピューティングデバイスの普及及び能力、及び、無線接続性の増大する利用可能性は、人々がどのようにコンピュータを使用し、データにアクセスするかということにおけるパラダイムシフトを表している。これらのデバイスの現在の使用及び多様性は、企業のIT基盤の一貫性に、多くの方法で影響与えている。これらのデバイスは、複数の、セキュアでない、監視するのが困難な過渡的な方法で、企業ネットワークに接続する。シリアル又はUSBの線を使って、デバイスをラップトップ又はデスクトップと同期させるのに、架台を使用する。モデム、及び、有線又は無線ネットワークを使用する。セルラー電話はPDAと集束して、高度なセルラーアクセスポイントの拡大するネットワーク内の企業データにアクセスすることのできる新世代のデバイスを提供する。最終的に、これらのデバイスはかなりのストレージを持つので、これらのデバイスの接続及び切断モードにおけるコンピューティング能力及び動作、セキュリティ管理、及び制御は、重大な課題のままである。
【０００５】
特に、失われた又は盗まれた場合には、モバイルデバイスは、企業内の「門戸開放」を提供する。殆どの企業のデータベース、ネットワークファイル、及びアプリケーションのためのパスワード及びアクセスコードを含む様々な機密情報が、これらのデバイスに常駐し得る。これらポケットサイズのデバイスは、21世紀の「パスワードのステッキ-ノート」となった。無線の「常にオン状態」の世界では、これらのデバイスは、1日に、多数の

未知のアドホックなネットワークに入り、かつ、存在することができる。産業取引展示会、サイバーカフェ、又は業界ネットワーキング環境において、企業データは特に、許可されないアクセスにさらされる。

【０００６】

これらのデバイスは、ビジネス機密情報のための大きな移動式レポジトリとなった。モバイルの専門家は、財務結果、新規事業計画、個人情報、クライアント記録、又は特定用途向け情報のようなラップトップからの独自の企業情報を、頻繁に同期させる、又はコピーする。モバイルデバイスの大きなメモリ容量、及び、アフターマーケットのメモリカードの急落する価格は、より、ユーザーが彼らのデバイスに付加情報を格納するようにさせる。

【０００７】

これらのデバイスの新しく出てきた企業の使用及び能力は、企業スケールのモバイルセキュリティソリューションに対する固有の課題を作る。モバイルデバイスは、しばしば切断モードで動作するので、オンポリシーポリシーの施行が必要とされる。

【０００８】

企業内に入っているモバイルデバイスの数、及び、セキュリティ要求の複雑さは、企業の管理及び企業セキュリティをモバイルデバイスに施行させる能力への要求を増大している。多くの情報技術(IT)部門は、多くの非法人の出すデバイスが、現在どのように従業員に使用されているかを知らない。これらのデバイスを、企業データにアクセスすることから制限するためのツールを、彼らは全く持っていない。ただ単に設置された現在のIT部門は、新しく出現したモバイルデバイスのコンピューティング標準に対応する能力を備えていない。

【０００９】

従って、モバイルデバイスに対してセキュリティポリシーを与えるシステム及び方法の改善の必要性がある。

【００１０】

(要約)

特定の実施形態では、無線ネットワークアクセスノードに接続されるサーバー上に配置されたサーバーモジュールは、開放されている。サーバーモジュールは、複数の無線デバイスのためのユーザー情報を収容するデータベースを含む。データベース内の各エレメントは、許可された少なくとも1つの無線デバイスに帰するものであり、次のグループ、すなわち(i)無線接続性許可、(ii)許可された無線デバイスの識別情報、及び(iii)許可されたネットワークアクセスノードの情報、からの少なくとも1つの形式のデータファイルを含む。

【００１１】

もう1つの実施形態では、コンピュータメモリが開放される。コンピュータメモリは、モバイルコンピューティングデバイスのセキュリティ機能との接続に使用するための複数の動作鍵、及び、ルート鍵を含む。ルート鍵は、その複数の動作鍵を暗号化する。

【００１２】

もう1つの実施形態では、モバイルコンピューティングデバイスにおいてセキュリティポリシーを施行する方法を提供する。その方法は、モバイルコンピューティングデバイスにおいてポリシーを受け取ること、及び、モバイルコンピューティングデバイスのユーザーが使用制限によって排除された使用に従事することを禁止することにより、モバイルコンピューティングデバイスにおいてそのポリシーを施行することを含む。このポリシーは、少なくとも1つのデバイス使用制限を含む。

【００１３】

もう1つの実施形態では、セキュリティ方法を提供する。このセキュリティ方法は、モバイルコンピューティングデバイスのユーザーからパスワードを受け取り、非線形関数を適用することにより、そのパスワードからセキュリティコードを導き出し、かつ、そのパスワードを暗号鍵として使用して、そのセキュリティコードを暗号化することを含む。

【００１４】
もう1つの実施形態では、サーバー上のソフトウェアアプリケーションへのアクセスをモバイルコンピューティングデバイスに選択的に与える方法を、提供する。この方法は、モバイルコンピューティングデバイスからソフトウェアアプリケーションにアクセスしたいという要求を受け取り、かつ、そのモバイルコンピューティングデバイスがインストールされたセキュリティプログラムを持っているかどうかを調べることにより、ソフトウェアアプリケーションへのアクセスを許可するかどうかを決定することを含む。
【００１５】
更なる実施形態では、ポリシー及び鍵材料を更新する方法を提供する。この方法は、サーバー及びクライアントモジュールで共有される共有暗号鍵を提供し、その共有暗号鍵を使ってクライアント上のデータを暗号化し、クライアントがモバイルコンピューティングデバイスに常駐している場合、パスワードを受け取ることにより、モバイルコンピューティングデバイスのユーザーを認証し、そのパスワードを使って共有鍵を復号化し、更新されたポリシー及び鍵材料を復号化するために、その共有鍵を使用し、かつ、モバイルコンピューティングデバイスにおけるポリシー及び鍵材料を、更新され、復号化されたポリシー及び鍵材料で置き換えることを含む。
【００１６】
異なる図面における同じ参照記号の使用は、同様又は同一のものを示す。
【００１７】
(本図面の詳細な説明)
図1を参照すると、企業セキュリティ管理において使用するためのシステム100が開示されている。システム100は、サーバー102、ゲートキーパー104、及び、クライアントデバイスモジュール106を含む。セキュリティ機能を提供するために使用されるクライアントデバイスモジュール106はまた、シールドとも呼ばれる。システム100は、様々なモバイルオペレーティングシステム、アプリケーション、及びデバイスのための包括的な企業セキュリティ管理ソフトウェアプラットフォームである。システム100は、組織がモバイルデバイスを容易にかつ低コストでセキュリティ保護し、管理することを可能にする。サーバー102は、既存のセキュリティポリシー管理システムと一体化し、管理者が既存のセキュリティポリシーを拡張させることにより、新しいモバイルセキュリティポリシーを集約的に作ること、及び、それらをモバイルデバイスの様々な集団に配信することを可能にする。サーバー102及びゲートキーパー104は一緒に動作して、これらのセキュリティポリシーを特定のモバイルデバイスに自動的かつセキュアに展開させる。シールド106は、分散セキュリティポリシーを実施及び施行し、モバイルデバイスへのアクセスを制御し、データセキュリティを提供するモバイルデバイス上の信頼できるコンピューティング環境である。
【００１８】
サーバー102は、モバイルセキュリティポリシーの集約的作成及び管理を提供するウェブベースのアプリケーションサーバーとして実装することができる。サーバー102は、Java、XML、及び他の高度なウェブ技術のような業界標準を使って、意識して移植性、拡張性、及び、保守性を持って実装されることが望ましい。容易な制御及びアクセシビリティを提供するため、サーバー102に接続されたローカルネットワーク上の如何なるワークステーション又はPCによる役割及びアクセスの単純な委任を可能にするセキュアなブラウザインターフェースを通して、サーバー102との管理インターフェースが提供される。
【００１９】
既存の識別情報データベース108のような既存の企業セキュリティ基盤とサーバー102を一体化するために、統合LDAPディレクトリ(CLD)技術を使用することができる。既存のポリシー及び識別情報管理システムは、ディレクトリリソースとのリアルタイムインターフェースを通して一体化される。サーバー102内の層は、外部LDAPサービスの統合化表示を提供し、ポリシーの継承及びオーバーライディングを通して、これらのサービスを提供する。結果として、データをコピーすることなく、かつ、既存の企業セキュリティシステム

のデータスキーマを変えることなく、ディレクトリ108のような既存の識別情報ディレクトリを使用することができる。

【００２０】

ゲートキーパー104、及びそれに続くモバイルデバイス106に送られたデータは、セキュリティ機能から引き出され、かつ、セキュアソケットレイヤー(SSL)とデータ暗号化の組み合わせを通して保護される。モバイルセキュリティポリシーは、管理インターフェース110を使って形成され、この管理インターフェース110は、インターフェース112を介してサーバー102に繋がれて、統合ディレクトリ(例えば、LDAP)内にポリシーをセットし、拡張する。ポリシーがセットされると、ポリシーパッケージが、機能内で各ユーザーについて生成され、特定のユーザーの暗号鍵で暗号化され、かつ、ターゲットのモバイルデバイス106上でのインストールためにゲートキーパー104に転送される。ポリシーパッケージの暗号化は、システムセキュリティの主柱を形成する。さらに、セキュアインターフェース114にわたるサーバー102とゲートキーパー104の間の更なるプライバシー及び認証のために、SSL通信を使用する。システム100は、強固なセキュリティ管理のために設計されて、切断されたデバイスの集中管理、ポリシーの自動版数管理及び配信、機能ベースのポリシー作成及び管理、既存の機能レポジトリ及びセキュリティ基盤とのシームレスな統合、委任されたセキュリティ管理、管理義務の分離、デバイスの検査ログの自動検索、統合、変更、及び通知、及び、モバイルデバイス管理を含む多くの高度なセキュリティ機能を提供する。

【００２１】

ゲートキーパー104は、HotSync、ActiveSync、及びScoutSyncのような既存のサードパーティの同期システム上に仮想セキュリティ層を形成するセキュリティ管理ソフトウェアエージェントとして実装することができる。ゲートキーパー104の機能は、サーバー102からポリシーパッケージを受け取り、そのパッケージをターゲットのモバイルデバイス106上にインストールすることである。ゲートキーパー104は、ローカル及びネットワークの同期をサポートするように、2つのモードで動作する。ローカルモードでは、実行可能なゲートキーパー104は、デスクトップ及びラップトップコンピュータ上で動作し、個人同期ツールの一番上にセキュリティ層を形成する。ネットワークモードでは、実行可能なゲートキーパー104は、企業サーバー上で動作し、ネットワーク同期アプリケーションの一番上にセキュリティ層を形成する。ゲートキーパー104を導入するとき、個人情報端末(PDA)のようなモバイルデバイス106は、サードパーティのデータ同期ツールを起動することが可能になる前に、認証し、かつ同期をとる許可を要求することが求められる。さらに、ゲートキーパー104は、特定のPDA上でのモバイルシールドの自動インストール、アプリケーション構成、更新及びパッチ管理、モバイルデバイス構成の管理、同期アプリケーションの監視、管理、及びそれへの制御アクセス、及び、デバイスポリシー、許可、及び構成の配信に備える。

【００２２】

モバイルデバイスアプリケーション、すなわちシールド106は、モバイルデバイスオペレーティングシステムの一番上のソフトウェア層として動作する高信頼コンピューティング環境として実装することができる。セキュリティポリシーを、双方向認証プロセスを使って、ゲートキーパー104から受け取る。データを暗号化し、デバイスのアクセス、デバイス周辺装置、及び、デバイスのソフトウェア及びハードウェア動作を監視及び制御するために、ポリシーは、モバイルデバイスにおいてエージェントソフトウェアによって使用される。モバイルデバイスの高信頼環境のアプローチは、接続又は切断のいずれかのオンデバイスポリシーの施行、必須のアクセス制御、セキュアな回復を持つデータ暗号化、必須の同期認証、アプリケーションの制御されたアクセス及び使用、赤外線(IR)、コンパクトフラッシュ(CF)、ユニバーサルシリアルバス(USB)、セキュアデジタル(SD)のハードウェアポートの制御、個人及びビジネスの複数のプロファイル、及び、セキュアな検査ログを含む多くのセキュリティ機能を提供する。シールドソフトウェアを受け入れることのできるサンプルデバイスは、Palm、Handspring、Sonyで作成される個人用デバイス、Compaq

のiPaq、及びHPのJornada500シリーズを含む。

【００２３】

まとめると、システム100の3つの全ての主要コンポーネントは、ユーザーの体験を大いに抑止することなく、セキュアなモバイル環境を可能にするように、実質的にシームレスに、かつユーザーに透過に相互作用する。サーバー102は、外部LDAP識別情報及びポリシーのデータを実質的に統合して、既存のセキュリティ基盤に組み込む。サーバー102上の管理ツールは、ポリシーパッケージを自動的に形成し、各モバイルデバイス106に配信することを可能にする。ゲートキーパー104は、同期を監視し、ターゲットにされたデバイス上にシールドソフトウェア及びポリシーパッケージをインストールする。最終的に、シールドは、モバイルオペレーティングシステム上にセキュリティレイヤーを形成することにより、高信頼コンピューティング環境を形成して、サーバー102から発生したポリシーを施行する。完全なシステム100は、包括的な企業スケールのモバイルセキュリティ管理システムを形成する。

【００２４】

システム100は、外部システムに組み込むコンポーネントを含む。大きな顧客ベースをサポートするために、各コンポーネントにおいて、複数のプラットフォームがサポートされる。以下のサンプルリストは、統合における例証となるデバイス及びソフトウェアプラットフォームを特定する。サーバー102では、windows2000オペレーティングシステム、MSアクティブディレクトリシステム(ADS)のLDAP、CriticalPath、又はiPlanet flat files、及び、エクスプローラ バージョン5.0+ ブラウザである。ゲートキーパー104では、互換性のあるオペレーティングシステムは、Win98、WinNT4.0、Win2000、WinXPを含み、互換性のあるデータ同期ソフトウェアは、HotSync、ActiveSync バージョン3.1+、Win2000のサーバーオペレーティングシステム、及びScoutSync バージョン3.5+のネットワーク同期を含む。シールドでは、サポートされるオペレーティングシステムは、PocketPC2000、PocketPC2002、及び、device OS バージョン3.5+を含む。

【００２５】

サーバー102は、拡張性サーバー及び機能の移植性を提供する連合ウェブサービスのような企業スケールのサーバー技術、保守性及び速度を提供するモデル表示コントローラ(MVC)ウェブインターフェース技術、及び、互換性を提供し、既存のセキュリティ基盤におけるインストール及び管理コストを低減する統合LDAPディレクトリ(CLD)技術を使って構成される。

【００２６】

サーバー102のアーキテクチャは、図2に示すように、ウェブサービスパラダイムを通して一体化される。このパラダイムは、企業ウェブアプリケーションを開発及び統合するための業界認定の最良の手法である。ウェブサービスパラダイムは、柔軟で、付加機能を可能にし、かつ、負荷平衡化及び付加サーバーを通したスケールの増大と同様にサーバーの置き換えを可能にするプロセスの疎結合アーキテクチャである。

【００２７】

ウェブサービス手法の核心は、結合するインターフェースを通して、サービスを公表、又は宣言する能力にある。図2を参照すると、アクセス制御、検査ログ、及びセキュリティポリシー管理のようなサーバー102の重要な機能の多くは、個々のJava「アプリケーション」として実装され、かつ、サービスとして内部のローカルエリアネットワーク(LAN)に宣言又は公表される。これらの「アプリケーション」は、ウェブサービスとして動作する。各サービスは、共有サーバー上で、別々のサーバー上で、又は、より少ないサーバー上で組み合わせて、プロセス又はスレッドとして実行することができる。単一のサーバー上、又はサーバー群上でサービスの複数のスレッドを実行することにより、拡張性及び負荷平衡化を実現する。保守は、サーバー間でサービスを移動させる能力、及び、サーバーを動的に置き換える能力をサポートすることにより、単純化される。

【００２８】

図2の連合するウェブサービスは、内部宣言されたサービスを統合し、ハイパーテキス

ト転送プロトコル(HTTP)インターフェースを通して外部ユーザーに対応するサービスを提供するプロキシ形式のサービスである。連合ウェブサービスは、外部ユーザーへの機能を代理することにより、内部サービスを統合する。サービスのロケーションは、拡張マーク付け言語(XML)でフォーマットされたサービステーブル、又は構成ファイル内で視程される。サービス管理は、連合サービス手法の利点である。拡張性のあるサーバー及びサービス群にサービスを提供するために、単一のURLのみを維持する必要がある。連合するサービスは、負荷平衡化を実行するために動的にアプリケーションコールを送る能力を持つ。連合するサービスの拡張性は、複数の連合するサービスサーバー、及び、シスコのLocalDirectorルーターのような標準の負荷平衡化ルーターを使って実現される。

【００２９】

連合するサービス及び外部ユーザーは、業界標準スクリプティングプロトコルの拡張マーク付け言語(XML)、及びシンプルオブジェクトアクセスプロトコル(SOAP)を通して一体化することができる。XMLが、ウェブページにおけるHTMLと同様なマーク付け言語である一方で、SOAPは、XMLで書かれた構造又は分で構成される。ウェブサービスで、XMLは、データを表すアルファベットである一方で、SOAPは、リモート関数コールと同様なサービスコールを定義する文法である。特に、XMLは、サービス間で移植可能なデータ表現を可能にするタグ付けされたマークアップ言語を提供する。SOAPは、コールする順序、パラメータ構造、及び結果変数を定義する業界標準のXMLタグ構造である。これらのプロトコルは、ウェブのユビキタスなHTTP通信チャネル全体にわたってサポートされる。

【００３０】

結果として、XML/SOAPは、ゲートキーパー104のような外部アプリケーションが、単一の連合ウェブサービスのURLとしてサービスを要求すること、実際のウェブサービスに結果をプロキシすること、及び、結果をゲートキーパー104に返すことを可能にする。ゲートキーパー104のプライバシー及び認証は、HTTPの代わりに標準HTTPSプロトコルを使用することによるSSLサービスを使って実現することができる。

【００３１】

管理インターフェース112は、軽量HTTP又はウェブインターフェースの使用を通じて提供される。この構成の利点は、LAN内の任意の場所からのアクセスの幅広い利用可能性、SSLプロトコルを通してのセキュアな使用法、加えて、認証及びアクセス制御を通じた責任の単純委任及び責務の分離を含む。

【００３２】

管理者コンソールのグラフィカルユーザーインターフェース(GUI)を実装するために、サーバー102は、MVCプログラミングモデルという業界認定の最良手法を使用する。モデル表示コントローラ(MVC)は、リモート関数コールを提供する方法であるという点で、ウェブサービスと似ている。MVCは、リソースを管理するように、統合するウェブサービスを強化する。しかしながら、MVCは、ウェブページ表示及びGUIを提供するために、サービスの結果を図式的に表す付加能力を提供する。

【００３３】

MVCは、ウェブページから関数を呼び出すためのCGIの最新の進化である。CGI手法は、表示するためにHTTPデータをブラウザに返すために、無数のprintln()コールを使用した。サーブレットは、特定のタスクを実行し、GUI機能を持たないサーバー側のJavaアプリケーションである。サーブレットは、JSPがHTML書式付けを管理する間のフローを管理ために使用された。MVCモデルは、サーブレットを、論理(又は、モデル)サーブレットと制御サーブレットとに分けて、頭字語MVCという結果になる。

【００３４】

サーバー102は、GUIを実装するためにMVCを使用する。表示コンポーネントは、GUIをフォーマットし、ブラウザに表示するために使用される。JSP及びHTMLは、この表示コンポーネントを実装するために使用される。コントローラコンポーネントは、制御フローを連結、委任、及び管理するために使用され、連合ウェブサービスでHTTPSを使って、Javaサーブレットコントローラで実装することができる。最終的に、コントローラは、作業をサ

ーバー102内の適切なモデルに委任する。このモデルは、サーブレットとしてJavaで実装することができる。このモデルは、ポリシーの設定、LDAP内に格納された機能へのアクセス、及び配信のためのポリシーパッケージの形成を制御するために使用される。演算及びロジックを含むGUI全体は、MVCフレームワークによって制御及び管理される。このフレームワークは手早く実装され、かつ、容易に変更、拡張、及び維持される。

【００３５】

モバイルセキュリティ管理システムの情報システム総合コストの単純化及び低減が、システム100の設計における目標である。インストールの課題及びコストは、既存の識別情報データ管理システムとの融合である。LDAPは、認証及び許可システムをサポートするための識別情報及びセキュリティポリシーを格納するために一般的に使用されるデータディレクトリ構造である。顧客が、LDAP機能ベースポリシーシステムを作成し、そのシステムを社内のすべてのユーザーに定着させるために時間及び労力をつぎ込んだ後、既存のLDAPレポジトリを再使用したいというのは、理解できる。さらに、顧客は、如何なるデータベーススキーマを変更することによってもシステムの整合性を損なうことなく、未来のセキュリティシステムが既存のLDAPレポジトリを使用することを望むこともある。

【００３６】

サーバー102は、この融合課題に対処するために、統合LDAPディレクトリ(CLD)技術を使用する。サーバー102は、LDAPレポジトリの連合表示を提供するために、階層化手法を使用し、外部及び内部LDAPシステムの上に仮想の層を置く。図3は、この手法を示している。

【００３７】

その連合は、3つの層で動作する。最下層302は、データ格納フォーマットに固有ものであり、その格納表現を移植可能なフォーマットに変換するアダプタ層である。中間層304は、最上位のクライアント要求を各レポジトリの背景に変形するオンザフライマッピングを実行し、連合表現という結果になるコアディレクトリエンジンである。最上位層306は、ディレクトリエンジンの結果を正規のLDAPフォーマットに変換するフロントエンドリスナである。その結果は、異なる顧客の識別情報データの蓄積を単純化されたサーバーインストールのための統一表示に統合するための有力な方法である。

【００３８】

アクセス制御サービスは、管理者ログイン、及びゲートキーパー104の通信における認証を提供する。このサービスは、システム及びデータアクセスに制御を提供するために、識別情報及び許可のLDAPディレクトリに接続する。管理者は、JSPを持つブラウザで表示されたログイン画面を通して、認証される。JSPは、連合サービスのサーブレットインターフェースを通して、ユーザー名及びパスワードを伴う認証を要求する。その要求は、完全のため、アクセス制御サービスにプロキシされる。認証は、CLDを通してLDAPバージョン3の動作で行うことができ、また代わりに、秘密鍵暗号化形式の認証システムを使って行うこともできる。

【００３９】

ゲートキーパー104は、SSLサーバー証明書、及び領域認証を使って認証される。SSL接続は、サーバー102とゲートキーパー104の間の通信を提供するように作成される。最初に、サーバー102が、SSL証明書認証を通してゲートキーパー104に認証される。次に、SSLチャネルが、秘話性のために構築される。最後に、(領域認証につき)ユーザー名/パスワードのペアが、連合サービスを通して、認証のためにアクセス制御サービスに送られる。ユーザー名及びパスワードの一致の成功は、サーバー102に対するゲートキーパー104の認証を提供する。

【００４０】

ポリシーサービスは、ポリシーファイルの作成と同様に、機能ベースのポリシーの管理を提供する。ポリシー管理サービスは、管理コンソールに提供され、機能(又は、グループ)及び個々のユーザーの双方についてのポリシー値の定義を可能にする。ポリシーがユーザーの集団に対して定められると、管理者は、そのポリシーを発行するように選択する

ことができる。この発行のプロセスは、セキュアなポリシーファイルを形成し、そのポリシーファイルを個々のシールドアプリケーション106に送りつける行為である。ポリシー管理のスクリーンショットの例を図4に示す。

【００４１】

システム100は、シールド106における暗号化動作のためのパスワード鍵を生成及び保管する重要な管理サービスを提供する。業界標準X9.17のような技術を使って、対称暗号鍵を生成する。モバイルデバイス上のデータを保護するために、対称鍵を使用する。これらのデータ暗号鍵は、各モバイルデバイスについて一意に生成され、サーバー102及びシールド106の双方上に格納されて、管理者介入を伴うセキュアなデータ復元を可能にすると同時に、データ保護を可能にする。非対称又は公開/秘密鍵のペアが楕円曲線暗号(ECC)鍵アルゴリズムで作成され、ポリシーファイルを暗号化し、ログファイルを検査するために使用される。各デバイスに対して、及び、ポリシーファイル及び検査ログに対して個々に、別個の鍵のペアが生成される。鍵のペアは、管理者介入を通したセキュアなデータ復元のために、サーバー102上に格納される。検査ログ秘密鍵はシールド106上に格納されて、検査ログ情報を暗号化して、デバイスの移動をサポートする。ポリシーファイル公開鍵は、シールド106上に格納されて、ソフトウェアが認証、及び、暗号化されたポリシーファイルからポリシー項目を抽出することを可能にする。もう一方の鍵は、サーバー102上で使用されて、検査ログファイルを復号化し、デバイスをサポートするポリシーファイルを暗号化する。

【００４２】

ポリシーファイルは、単一のデータパッケージに集約され、XMLでフォーマットされたポリシー項目の集合である。ポリシーファイルは、セキュリティの構築及び施行のため、サーバー102からモバイルデバイスに転送される。ポリシーファイルは、実際には、定義されたポリシーの各カテゴリについて1つの主索引ファイル及びその他から成る多数のファイルである。各カテゴリファイルは、シールド106の許可及び挙動を定義する一連のポリシーを含む。カテゴリ、鍵、及び、値の名前の3つの項目が、各ポリシーを定義する。鍵は、ゼロ以上の名前/値のペアを、それと関連付けることができる。

【００４３】

サーバー102は、ECC非対称暗号化でポリシーファイルを暗号化し、そのファイルをモバイルデバイスに転送する。個々のモバイルデバイスのポリシー管理に対応する鍵のペアが、サーバー102で作成及び管理される。秘密鍵は、サーバー102上に格納され、ポリシーファイルを暗号化するために使用される。公開鍵は、シールドアプリケーション106によって、モバイルデバイス上に格納される。ポリシーファイルは、認証が行われた後、同期をとる間、モバイルデバイスに転送される。シールドに格納された公開鍵は、ポリシーファイルを開くために使用される。公開鍵は、セキュアな手法で、シールドアプリケーションに送られる。このポリシーファイル管理の方法は、特定のシールド配置への秘密転送を提供し、ポリシー認証及び管理を提供し、かつ、一貫したポリシー施行を可能にするように改竄に耐性がある。

【００４４】

ポリシーデータは、以下のカテゴリ、すなわち、I/O、ストレージ、アプリケーション、及び認証、に分類される。

10

許可ポリシー

名前	ID (カテゴリ)	値	形式	読み取り専用	影響
IR_Enable	I/O	True/False	Boolean	True	Palm:Excgange Manager, IR Library CE:
TCPIP_Enable	I/O	True/False	Boolean	True	Palm:Network, INet Library CE:
NetBios_Enable	I/O	True/False	Boolean	True	Palm:N/A CE:
SyncAuthenticated_Required	I/O	True/False	Boolean	True	Palm: CE:
VolumeMount_Enable	Storage	True/False	Boolean	True	Palm:DB, VFS Manager(File system mounting) CE:
DateBook_Enable	Applications	True/False	Boolean	True	Palm:DateBook CE:Calendar
AddressBook_Enable	Applications	True/False	Boolean	True	Palm:AddressBook CE:Contacts
Todo_Enable	Applications	True/False	Boolean	True	Palm:Todo CE:Tsks
Memo_Enable	Applications	True/False	Boolean	True	Palm:Memo CE:Notes
Expense_Enable	Applications	True/False	Boolean	True	Palm:Expense CE:Money
Mail_Enable	Applications	True/False	Boolean	True	Palm:Mail CE:Inbox
Prefs_Enable	Applications	True/False	Boolean	True	Palm:Prefs CE:Settings
Security_Enable	Applications	True/False	Boolean	True	Palm:Security CE:N/A
FileExplorer_Enable	Applications	True/False	Boolean	True	Palm:N/A CE:File Explorer
Internet Explorer_Enable	Applications	True/False	Boolean	True	Palm:N/A CE:Internet Explorer
PocketWord_Enable	Applications	True/False	Boolean	True	Palm:N/A CE:Pocket Word
PocketExcel_Enable	Applications	True/False	Boolean	True	Palm:N/A CE:Pocket Excel
WindowsMedia_Enable	Applications	True/False	Boolean	True	Palm:N/A CE:WindowsMedia
Reader_Enable	Applications	True/False	Boolean	True	Palm:N/A CE:MS Reader

ルールポリシー

名前	ID (カテゴリ)	値	形式	読み取り専用	説明
PINEnable	認証	True/Flase	Boolean	True	パスワード階層構造内に、PIN認証を含むかどうか
PasswordEnable	認証	True/Flase	Boolean	True	パスワード階層構造内に、パスワード認証を含むかどうか
PassPhrase Enable	認証	True/Flase	Boolean	True	パスワード階層構造内に、パスフレーズ認証を含むかどうか
ManAuthEnable	認証	True/Flase	Boolean	True	パスワード階層構造内に、PIN認証を含むかどうか
PasswordNum Chars	認証	8-16 characters	Number	True	
Password AlpasRequired	認証	True/Flase	Boolean	True	
Password Numeric Required	認証	True/Flase	Boolean	True	
PasswordSpecial Required	認証	True/Flase	Boolean	True	
Password UpperCase Required	認証	True/Flase	Boolean	True	
PassPhrase NumChats	認証	16-32 characters	Number	True	
NumPINAttemps	認証	1-4	Number	True	
NumPassword Attemps	認証	1-4	Number	True	
NumPassPhrase Attemps	認証	1-4	Number	True	
NumManAuth Attemps	認証	1-4	Number	True	
UserSession Timeout	認証	1-120分	Number	True	ユーザーが再認証しなければならない時までの休止時間
PowerOff TimeoutEnable	認証	True/Flase	Boolean	True	デバイスをオフにした後、ユーザーが再認証することを要求する
AuthDataExpires	認証	1-365日	Number	True	ユーザーが認証情報をリセットしなければならない時までの時間

【００４５】
システム100はまた、ログ収集サービスを提供する。ログ収集において定義された各イベントは、登録された対応するポリシーを持つ。これは、管理者が、どのイベントを検査ログに書き込むかを制御することを可能にする。
【００４６】
ログファイルは、シールドソフトウェア106で生成されたイベントの記録である。シールド106は、最初に、ファイルをローカルに格納する。同期をとる間、ログファイルは、自動的に、ゲートキーパー104を通してサーバー102に転送される。同期がとれた後、シールド106は新規ファイルを初期化する。サーバー102は、連結されたログを形成するように、新たなログを直前の同期のとれたログの最後に追加する。顧客又はサードパーティ通知ツールを使用することを可能にするために、ログへのサーバーアクセスが、開放型データベース接続機能(ODBC)インターフェースを通して提供される。
【００４７】
ログファイルは、楕円アルゴリズム非対称暗号化による改竄から、ローカルに保護される。個々のモバイルデバイスのオンデバイス検査ログに対応する鍵のペアが、サーバー102で作成、及び管理される。公開鍵はサーバー上に格納され、同期のとれた後、検査ログを開くために使用される。秘密鍵は、シールドアプリケーション106によってモバイルデバイス上に格納され、イベントログに新たなイベント記録を追加するために使用される。初期値又は根は、同期をとる間、セキュアモードで、サーバー102からモバイルデバイスに転送される。記録が検査ログに追加されるとき、暗号化プロセスを通して根が更新される。これは、イベント記録プロセスを通して、暗号化スレッドを形成する。さらに、サーバーからのタイムスタンプは、ファイルを初期化するために使用される。ファイル内の周期イベントと組み合わされる最初のタイムスタンプは、モバイルデバイスクロックの監視が、時間改竄を防ぐことを可能にする。このオンデバイス検査ログ収集の方法は、サーバーで容易に維持されるセキュアかつプライベートな検査ログを提供し、時間とログ収集の順番とのギャップを検出し、かつ、強健なオンデバイス監視システムを提供するように改竄に耐性がある。
【００４８】
図5を参照すると、ゲートキーパー104における例示の機能図が開示されている。ゲートキーパー104は、永続ネットワーク502、サーバーインターフェース504、クライアントインターフェース506、暗号化モジュール508、検査モジュール510、同期プラグインモジュール512、及び認証モジュール514を含む。ゲートキーパー104は、インターフェース114を越えて、HTTPS及びXMLを使ってサーバー102と通信し、かつ、SKID3及びXMLのようなもので、同期インターフェース116を介してモバイルデバイス106と通信する。
【００４９】
図6を参照すると、代表的なモバイルデバイス上のシールドアプリケーション106における例示のブロック図が示されている。シールドアプリケーション106は、通信モジュール602、ストレージ領域604、ユーザーインターフェース606、暗号化モジュール608、検査及びログモジュール610、ポリシールールエンジン612、及びシステムインターフェース614を含む。
【００５０】
通信モジュール602は、ゲートキーパーのような外部システムと通信する。通信モジュールは、ゲートキーパー104から、アプリケーションデータ、個人情報データ(PIM)、新しい鍵の材料、及び、ポリシーデータを受け取る。アプリケーションデータ及びPIMデータは、汎用デバイスストレージ604に格納される。この汎用ストレージは、暗号化モジュール608で暗号化されることができる。新しい鍵の材料は、暗号化モジュール608で復号化され、608の中の鍵データ記憶装置内に格納される。ポリシーデータは、暗号化モジュール608で復号化され、ルールエンジン記憶装置612内に格納される。
【００５１】

ユーザーインターフェースモジュール606は、ユーザーを認証し、デバイスをロック解除するために、デバイスユーザーと通信する。ユーザーインターフェースは、PIN(個人識別番号)、パスワードのような複数のデータのいずれかを検索し、質問に答え、かつ、呼掛けに応答することができる。暗号化モジュール608内のデータを検索されたデータで復号化することによって、認証が試される。復号化が成功したとき、認証が承認される。同様な認証試験は、検索された情報をハッシュし、その情報を暗号化モジュール608内に格納されたデータと比較することができる。ユーザーインターフェース606はまた、同期をとっている最中、又は、デバイスがロックされた、のような警告を表示する。

【００５２】

検査ログモジュール610は、認証試行の成功又は失敗のようなシステムイベントデータを、610の暗号化されたログの記憶装置内に格納する。イベントは、暗号化モジュール608で暗号化され、通信モジュール602によりゲートキーパー104に転送される。

【００５３】

ルールエンジン612は、その記憶装置内のポリシーデータに基づく認証を提供する。ポリシーは、ゲートキーパー104に接続している間、通信モジュール602から検索され、接続されている又は切断されている何れかの間、常にそのポリシーを施行する。ポリシーデータは、暗号化された形で、通信モジュール602によってゲートキーパー104から検索される。暗号化モジュール608は、612の中のポリシーデータ記憶装置上に記憶する前に、データを暗号化する。ルールエンジンは、複数のモジュールから許可要求を受け取り、その中に格納されたポリシーに基づく許可で応答する。ポリシーエンジンは、ユーザーの行為が否認された、又は許可されないイベントが生じた場合には、デバイスをロックするようにユーザーインターフェース606に信号を送ることができる。

【００５４】

ルールエンジン612は、どのデバイスとどの通信モジュール602が通信できるかを施行する。ポリシーデータベースは、通信することのできるデバイスのリスト、通信することのできないデバイスのリスト、又は、デバイスを認証するために使用することのできる暗号化モジュール608内に格納された鍵のリストを収容することができる。外部デバイスが、通信するのを許可されたデバイスのリスト内に含まれる場合には、ルールエンジン612は、その外部デバイスと通信するよう、通信モジュール602に許可を与える。外部デバイスが、通信するのを許可されないデバイスのリスト内に含まれる場合には、ルールエンジンは、その外部デバイスと通信するための通信モジュール602への許可を否認する。ポリシーデータベース内に複数の鍵がリストされる場合には、ルールエンジンは、認証を判断するために、暗号化モジュール608に、外部デバイスで呼掛け応答を実行するよう要求する。認証が成功した場合には、ルールエンジン612は、外部デバイスと通信する許可を通信モジュール602に与えることができる。さもなければ、ルールエンジンは、外部デバイスと通信する通信モジュール602への許可を否認することができる。

【００５５】

ルールエンジン612及びユーザーインターフェース606は、個人又はビジネスモードを施行することができる。ユーザーインターフェース606は、個人モード又はビジネスモードのいずれかでユーザーを認証することができる。モードは、ユーザーインターフェースから検索された、ユーザーがどちらのモードを要求しているかを示すデータから定められる。ルールエンジンは、各モードで何の行為を実行することができるかを許可する。さらに、ルールエンジンは、汎用データ記憶装置604内のどのデータ項目をユーザーインターフェース606によって表示することができるか許可し、複数のモジュールによってアクセスされ、かつ、通信モジュール602によって転送されることができる。

【００５６】

システムインターフェース614は、遮断されたイベントを使って、OSイベントハンドラ630のような外部イベントハンドラと通信し、かつ、システムコールを遮断することにより、OS632のような外部オペレーティングシステムと通信する。システムインターフェース614は、システムコール及びイベントを遮断し、ポリシーエンジン612から許可を要求し、

かつシステムコール又はイベントを是認又は否認することにより、システムコール及びイベントを許可する。

【００５７】

図7を参照すると、セキュリティソフトウェアをサーバー102からモバイルコンピューティングデバイスに配信する方法を示している。最初に702において、ネットワークスクリプト、ポリシー、及び鍵の材料を含むゲートキーパーソフトウェア104が、サーバー102からデスクトップコンピュータ又は他の適切なゲートキーパープラットフォームにインストールされる。704において、モバイルコンピューティングデバイスが、データ同期イベントの間ゲートキーパー104に接続しているとき、シールドソフトウェアアプリケーション106、すなわち、モバイルコンピューティングデバイスにおけるセキュリティソフトウェアが、ゲートキーパー104からモバイルコンピューティングデバイスにインストールされる。706において、ゲートキーパー104は、ワンタイムパスワードをサーバー102から要求する。708において、サーバー102は、ワンタイムパスワードをモバイルコンピューティングデバイスのユーザーに電子メールで送る。次に、モバイルコンピューティングデバイスは、セキュリティシールドアプリケーションのインストールを完了するために、ワンタイムパスワードを使用することができる。

【００５８】

この時点で、710において、鍵パックのためのルート鍵が、ワンタイムパスワードを使って復号化され、ユーザーが新しいパスワード、個人識別番号(PIN)、及びパスフレーズ、及び任意で、ユーザーの母親の旧姓又はペットの名前のようなその他のユーザー識別情報を入力するアクセスを可能にする。次に712において、新しいパスワード、PIN、フレーズ、及び、鍵の質問に対するユーザーの答えを含む上記ユーザー情報の項目の各々を使って、ルート鍵が暗号化される。モバイルコンピューティングデバイスのユーザーにセキュリティ動作を起動させる上記プロセスは、ユーザー情報の登録を促すように指示画面を提供することによって、というようにユーザーインターフェースソフトウェアを使って遂行することができる。

【００５９】

図8を参照すると、新規の又は変更されたセキュリティポリシー情報をモバイルデバイスに配信する方法を示している。802において、ポリシーの変更又は新しいポリシーが、サーバー102に接続された管理者によって加えられ、管理者の要求に応じて、サーバー102は新しいポリシーパッケージを作成する。ポリシーパッケージは、新しい又は変更されたポリシーを含む。804において、新しいポリシーパッケージをモバイルコンピューティングデバイスに配信するために、サーバー102は、ゲートキーパー104との通信を認証し、認証の成功時には、そのポリシーパッケージをゲートキーパー104に送る。

【００６０】

デバイスとゲートキーパーの間の認証は、共有鍵を認証を定めるための共有秘密鍵として使用する相互呼掛け応答アルゴリズムを使って、実装することができる。このプロセスは、デバイス又はゲートキーパーのいずれかで開始することのできる二段階の呼掛け応答である。デバイスが呼掛けを開始する例を考えなさい。乱数がデバイスで計算され、呼掛けとしてゲートキーパーに送られる。ゲートキーパー及びデバイスは、並行して、かつ秘密に、予想される応答を算出する。共有鍵及び呼掛け値の任意の一方向関数によって、応答を計算することができる。例えば、鍵を呼掛けの最後に追加し、メッセージダイジェストの計算のために、MD5のようなハッシュアルゴリズムに入力することができる。ゲートキーパーは、算出された応答を返すことにより、デバイスに応答する。応答が予測された値と一致する場合には、相互呼掛け応答の第一のステップ又は段階が正常に完了し、ゲートキーパーが戻り試行のための乱数を計算する。次のステップは、逆方向の機能の場合を除いて、第一のステップを繰り返す。ゲートキーパーは、乱数を用いてデバイスに呼びかける。各々が、予測される応答をプライベートに算出する。デバイスは、応答として、計算された値を返す。それらの値が一致した場合には、第二段階を通過する。どちらかの段階が失敗した場合には、全プロセスが失敗に終わる。成功するためには、両方のステップ

を通過しなければならない。

【００６１】

806において、ゲートキーパー104は、ポリシーパッケージを受け取り、モバイルコンピューティングデバイスとの次の同期通信を待つ。808において、モバイルコンピューティングデバイスが、データの同期をとるのを開始したとき、ゲートキーパー104は、モバイルコンピューティングデバイスを認証する。810において、モバイルコンピューティングデバイスの認証成功時に、ゲートキーパー104は、モバイルコンピューティングデバイスにポリシーパッケージを送り付ける。次に、812において、モバイルコンピューティングデバイスはポリシーを復号化し、新しい又は変更されたセキュリティポリシーを起動させる。サーバー102からのゲートキーパー104の認証、又は、ゲートキーパー104からのモバイルコンピューティングデバイスの認証のいずれかが失敗した場合には、更新されたポリシーパッケージは配信されず、管理者に通知され得る。

【００６２】

図9を参照すると、モバイルコンピューティングデバイスがポリシーの更新を要求する方法を示している。この方法では、902において、モバイルコンピューティングデバイスが、ゲートキーパー104と同期をとることを開始する。904において、モバイルコンピューティングデバイスとゲートキーパー104との間の接続、及び、ゲートキーパー104とサーバー102との間の接続が認証される。認証が成功した後、906において、ゲートキーパー104が、新しいポリシーがないかサーバー102を調べる。908において、サーバー102は、新しく、かつ更新されたポリシーに基づいてポリシーパッケージを作成し、そのポリシーパッケージをゲートキーパー104に送る。910において、ゲートキーパー104は、新しい及び/又は更新されたポリシーを、モバイルコンピューティングデバイス上にインストールする。912において、モバイルコンピューティングデバイスでは、セキュリティアプリケーション(すなわち、シールドアプリケーション106)がポリシーパッケージを復号化し、モバイルコンピューティングデバイス上で、新しい又は更新されたポリシーを起動させる。

【００６３】

図10を参照すると、鍵の材料、及び、セキュリティアプリケーションに備えるための鍵の材料の使用が示されている。ソフトウェアフィールド1004、日付フィールド1006、所有者フィールド1008、長さフィールド1010、鍵ID1012、及び巡回冗長検査フィールド1014を含む複数のフィールドを持つ鍵の例1002が示されている。また、ルート鍵1016も示されている。ルート鍵1016は、ユーザーのPIN1018、パスワード1020、フレーズ1022、及び呼掛け1024(すなわち、鍵の質問に対する応答)を使って暗号化される。次に、ルート鍵1016が、鍵リングと呼ばれる一連の動作鍵1036を暗号化するために使用される。動作鍵1036は、データ鍵1038、ポリシー鍵1040、ログ鍵1042、ゲートキーパー認証要素1044、更新鍵1046、及び、ハートビートログ鍵1048を含む。データ鍵1038は、モバイルコンピューティングデバイス内のロック解除データストレージ1054にリンクされる。公開鍵1040は、ポリシー1050にアクセスするために使用され、ログ鍵1042は、モバイルデバイスのユーザー行為の履歴を追跡するログファイル1052にアクセスするために使用される。

【００６４】

ログ鍵は、公開鍵暗号アルゴリズムを用いて、データを、モバイルデバイスのユーザー行為の履歴を追跡するイベントログに暗号化するために使用される公開鍵である。

【００６５】

ゲートキーパー認証鍵は、呼掛け応答アルゴリズムでデバイスがその識別情報をゲートキーパーで証明するために使用される。その鍵は、呼掛けに対する応答を算出するために、共有秘密鍵として使用される。ハートビート鍵は、デバイスとサーバーの間の認証のために、ゲートキーパー認証鍵と同じように使用される。デバイスとサーバーの間の呼掛け及び応答は、デバイスを監視するために、ハートビートとして使用される。

【００６６】

ポリシー鍵を使って暗号化されるポリシーパック1056、及び、ルート鍵1016を使って暗号化された鍵材料パック1058を含むポリシーパッケージもまた示されている。ポリシーパ

ッケージは、ゲートキーパー104を介してサーバー102からモバイルコンピューティングデバイス106に送り付けることができる、又は、ゲートキーパー104を介してモバイルコンピューティングデバイスからサーバー102に送り付けることができる。このポリシーパッケージを配信する方法は、図8及び9を参照して、上で説明した。

【００６７】

上述で開示した内容は、例証として考えられるものであり、後に付けた特許請求の範囲は、本発明の技術的範囲内に入るような全ての変更及び他の実施形態を含むことを意図される。従って、法で許される最大限で、本発明の技術的範囲は、以下の特許請求の範囲及びその均等物の最も許容し得る解釈で定められるものであり、前述の詳細な説明で制限、又は限定されるものではない。

【図面の簡単な説明】

【００６８】

【図１】セキュリティポリシーの配信、及び、モバイルデバイスの管理を提供するのに使用するシステムの実施形態のブロック図である。

【図２】図1のシステム内のサーバーの実施形態のブロック図である。

【図３】図2のサーバー内のソフトウェア層を示す一般的な図である。

【図４】図2のサーバーで使用する管理用ユーザーインターフェースの画面の、説明のための一場面である。

【図５】図1のゲートキーパー内の機能要素を示すブロック図である。

【図６】図1のシステムのシールドアプリケーション内の要素を示すブロック図である。

【図７】モバイルデバイスへのシールドセキュリティアプリケーションのインストールを示すフローチャートである。

【図８】ポリシー情報を更新し、その更新されたポリシー情報をモバイルデバイスに配信する方法を示すフローチャートである。

【図９】ポリシー情報を更新し、その更新されたポリシー情報をモバイルデバイスに配信するもう1つの方法を示すフローチャートである。

【図１０】鍵材料、及び、ポリシー情報の暗号化で使用する特定の鍵フィールドのフォーマットを示す図である。

【図１】

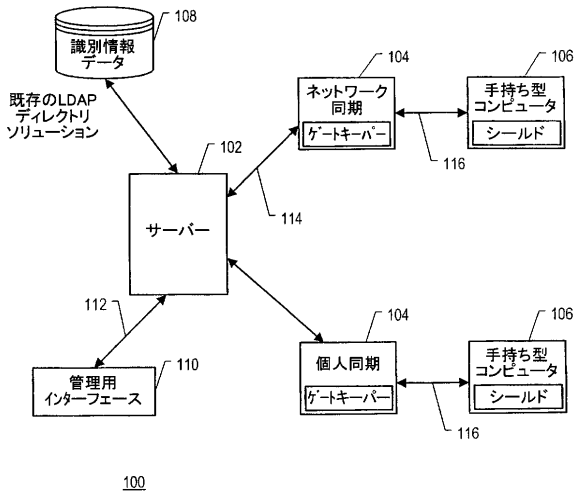


FIG. 1

【図２】

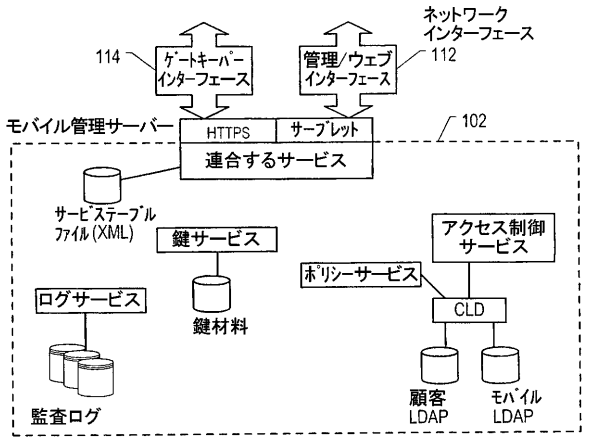


FIG. 2

【図３】

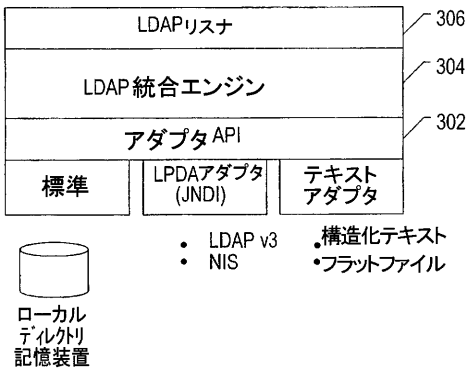


FIG. 3

【図４】

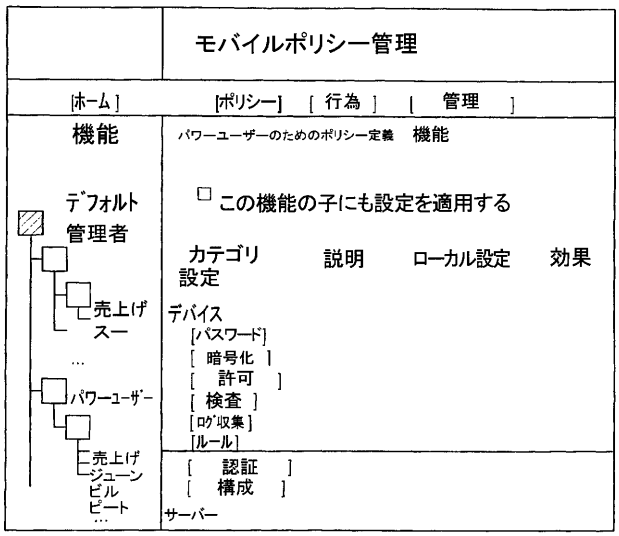


FIG. 4

【図５】

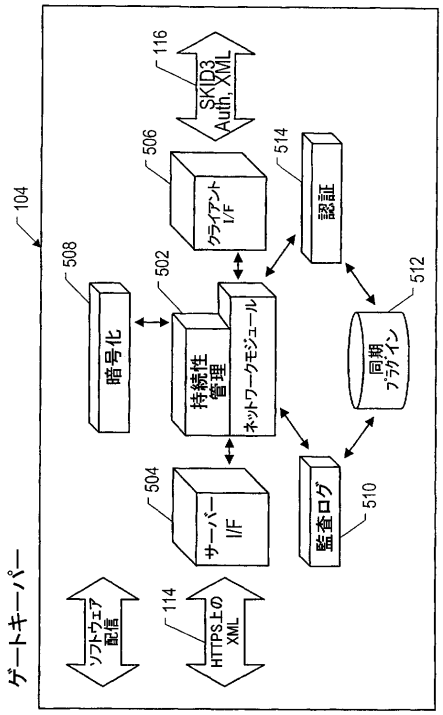


FIG. 5

【図６】

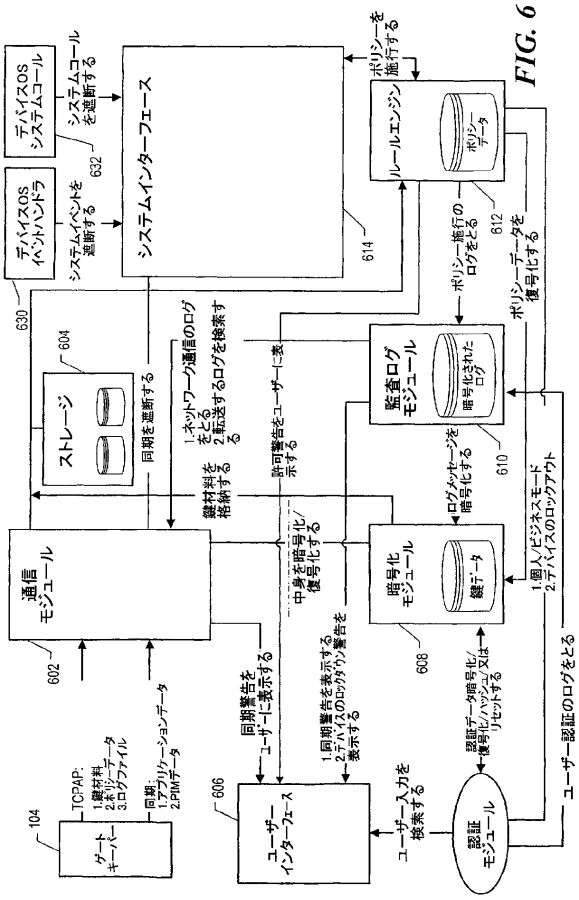


FIG. 6

【図７】

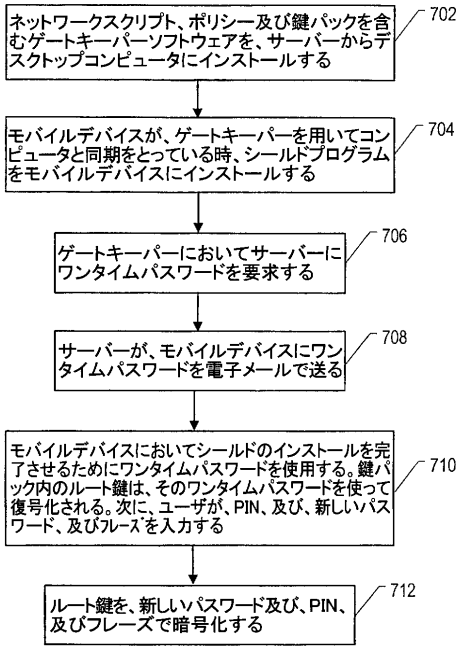


FIG. 7

【図８】

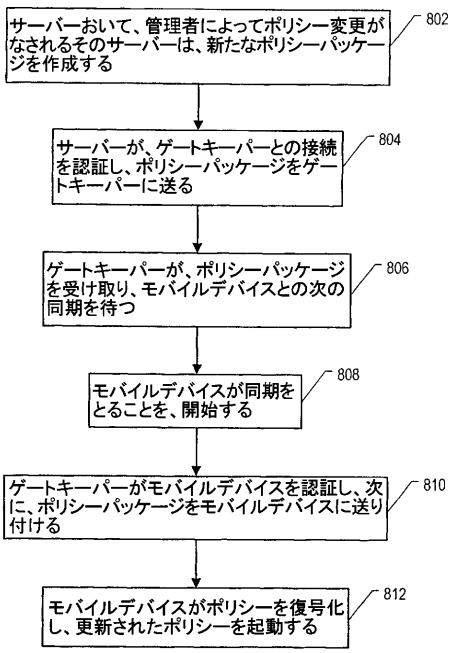


FIG. 8

【図９】

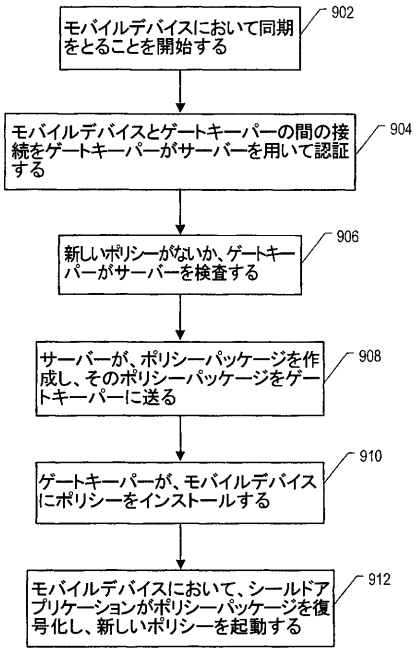


FIG. 9

【図１０】

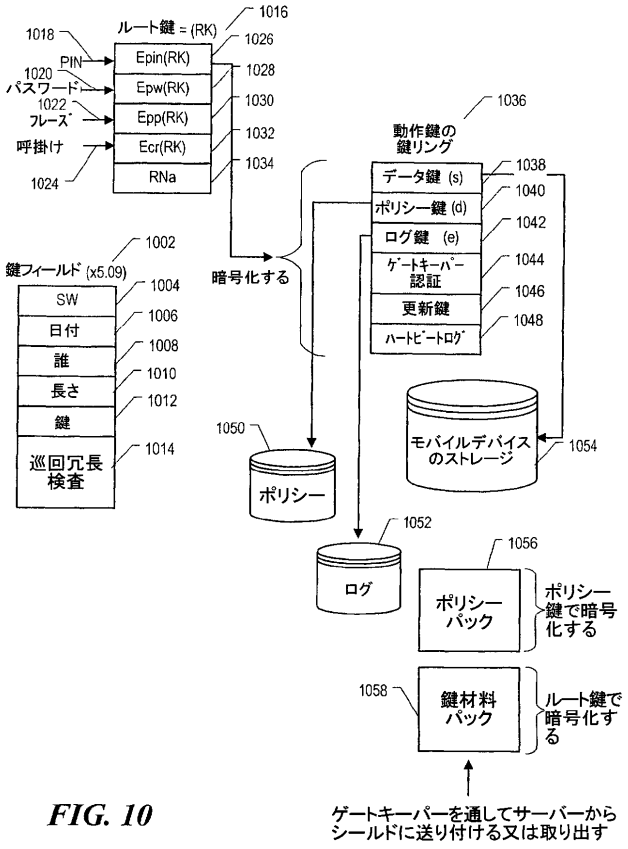


FIG. 10

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/29347

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : H04L 9/00, 9/32
US CL : 713/150, 200-202; 380/255, 270, 277, 278, 279, 281, 283, 284
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. : 713/150, 200-202; 380/255, 270, 277, 278, 279, 281, 283, 284

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)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6,236,852 B1 (VEERASAMY et al) 22 May 2001, see abstract, col. 2, lines 4-36, col. 5, lines 14-40, col. 8, lines 19-55, col. 9, lines 23-46, col. 11, lines 5-11	1,3,5,9-15
X	US 5,850,444 A (RUNE) 15 December 1998, see abstract, col. 3, lines 12-50, col. 4, lines 16-38, col. 5, lines 54-61	2,8
X	US 6,178,506 B1 (QUICK, JR.) 23 January 2001, see col. 2, lines 46-60, col. 4, line 45-col. 5, line 8, col. 6, lines 11-40	4,6

☐ 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
04 December 2003 (04.12.2003)

Date of mailing of the international search report
23 DEC 2003

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
Ayaz Sheikh

Telephone No. 703-305-3900

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

INTERNATIONAL SEARCH REPORT

PCT/US03/29347

Continuation of B. FIELDS SEARCHED Item 3:
BRS TEXT SEARCH (files: USPAT, DERWENT, JPO, EPO, IBM TDB, US PGPUB)

search terms: wireless, cell, cellular, policy, root, key, encrypt, encrypting, password, authentic, authenticate, authentication, authenticating, authenticated, authorize, authorizing, authorization, authorized

フロントページの続き

(51)Int.Cl.	FI		テーマコード（参考）
	Ｈ０４Ｌ 9/00	６０１Ａ	
	Ｈ０４Ｌ 9/00	６０１Ｅ	

(31)優先権主張番号 10/252,211
(32)優先日 平成14年9月23日(2002.9.23)
(33)優先権主張国 米国(US)

(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

（特許庁注：以下のものは登録商標）
ＪＡＶＡ
コンパクトフラッシュ
ＷＩＮＤＯＷＳ

(72)発明者 マン ドゥウェイン アール
アメリカ合衆国 テキサス州 ７５０１３ アレン デル リオ コート ４０１
(72)発明者 ハード ロバート ダブリュー
アメリカ合衆国 テキサス州 ７５０２５ プラノ ウルフ コート ３３２１
(72)発明者 バーチェット クリストファー ディー
アメリカ合衆国 テキサス州 ７５０５６ ルイスヴィル サー ランスロット サークル １０１９
(72)発明者 ゴードン イアン アール
カナダ ケイ１エス ２エス２ オンタリオ オタワ メルガンド アベニュー ３２

Ｆターム(参考) 5B017 AA03 BA05 BA07 CA05 CA16
5B285 AA01 BA01 BA03 BA08 CA32 CA42 CA43 CB02 CB47 CB62
CB72 CB76 CB95
5J104 AA16 EA17 EA18 PA01 PA07