(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2014-501955
(P2014-501955A)
(43)公表日　平成26年1月23日(2014.1.23)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/62	(2013.01)	G06F	21/24	165A
G06F 21/30	(2013.01)	G06F	21/20	130
G06F 21/86	(2013.01)	G06F	21/06	186
G06F 21/74	(2013.01)	G06F	21/02	174

審査請求 未請求　予備審査請求 未請求　（全 21 頁）

(21)出願番号　特願2013-537679 (P2013-537679)
(86)(22)出願日　平成23年10月11日 (2011.10.11)
(85)翻訳文提出日　平成25年7月4日 (2013.7.4)
(86)国際出願番号　PCT/US2011/055705
(87)国際公開番号　WO2012/060979
(87)国際公開日　平成24年5月10日 (2012.5.10)
(31)優先権主張番号　12/939,702
(32)優先日　平成22年11月4日 (2010.11.4)
(33)優先権主張国　米国 (US)

(71)出願人　509213484
シルバー　スプリング　ネットワークス　インコーポレイテッド
ＳＩＬＶＥＲ　ＳＰＲＩＮＧ　ＮＥＴＷＯＲＫＳ，　ＩＮＣ．
アメリカ合衆国、カリフォルニア州　９４０６３、レッドウッド　シティ、ブロードウェイ　ストリート　５５５
(74)代理人　100076428
弁理士　大塚　康徳
(74)代理人　100112508
弁理士　高柳　司郎
(74)代理人　100115071
弁理士　大塚　康弘

最終頁に続く

(54)【発明の名称】公益事業用途向けの物理的にセキュリティ保護された認可

(57)【要約】
全体的なセキュリティを公益事業管理システムに提供するために、システムの構成要素に対して発行される重要なコマンド・制御メッセージは、セキュリティ保護された権限により明示的に承認される。明示的な承認により、要求された動作を認証し、メッセージにおいて示された特定の動作の実行を認可する。アクセス制御と関連付けられる公益事業管理及び制御システムの重要な構成要素は、物理的にセキュリティ保護された環境に配置される。この手法を用いる場合、ネットワーク動作を承認する役割を担うこれらのサブシステムをバンカすることのみが必要となる。他の管理モジュールは、バンカの外側に配置されてもよく、それにより、これらのサブシステムをバンカ及び非バンカされた構成要素に区分する必要性を回避する。非バンカされたサブシステムの各々の重要な構成要素へのアクセスは、バンカされた承認システムを介して制御される。

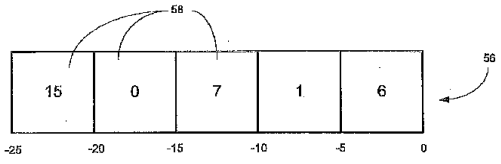

Fig. 5

【特許請求の範囲】
【請求項１】
公益事業用途向けのためのデータセンタであって、
物理的にセキュリティ保護された環境と、
少なくともいくつかが前記データセンタの外側の場所から公益事業の動作に関係する機能を実行するリモート要求を受信するインタフェースを有する前記公益事業の前記動作と関連付けられた１つ以上のアプリケーションプログラムを実行するように構成された前記物理的にセキュリティ保護された環境の外部の少なくとも１つのサーバと、
前記物理的にセキュリティ保護された環境内に配置され且つ秘密鍵を格納するハードウェアセキュリティモジュールと、
前記アプリケーションプログラムに向けられたリモート要求を受信し且つ前記秘密鍵に従って署名される認可された要求を提供するように構成された前記物理的にセキュリティ保護された環境内に配置された認可エンジンと、
前記アプリケーションプログラムと関連付けられたビジネス論理に従って前記リモート要求を処理し且つ前記要求が前記認可エンジンにより認可されることを選択的に可能にするように構成された前記物理的にセキュリティ保護された環境内に配置されたポリシーモジュールと、
を備えることを特徴とするデータセンタ。
【請求項２】
前記データセンタにおいて受信され且つ前記アプリケーションプログラムに対して意図されるリモート要求を受信し、且つ前記受信した要求を前記ポリシーモジュールに転送するように動作する前記物理的にセキュリティ保護された環境内に配置された前記インタフェースに対するプロキシを更に備えることを特徴とする請求項１記載のデータセンタ。
【請求項３】
前記アプリケーションプログラムは、前記アプリケーションプログラムにより受信されるリモート要求を前記ポリシーモジュールに転送するように構成されることを特徴とする請求項１記載のデータセンタ。
【請求項４】
前記ポリシーモジュールは、所定の期間内に発行される電力を切断するコマンドを含むリモート要求の数が限界値を超えるかを判定し、且つ当該要求の数が前記限界値を超える場合に前記コマンドが実行されるのを阻止するように構成されることを特徴とする請求項１記載のデータセンタ。
【請求項５】
前記ポリシーモジュールは、電力を切断及び再接続するコマンドを含む一連のリモート要求が同一の顧客と関連付けられるかを判定し、且つ一連のリモート要求がそのような条件を満たす場合に前記コマンドが実行されるのを阻止するように構成されることを特徴とする請求項１記載のデータセンタ。
【請求項６】
前記ポリシーモジュールは、電力を切断及び再接続するコマンドを含むリモート要求が顧客の現在の状況に一致しないかを判定し、且つリモート要求が一致しない場合に前記コマンドが実行されるのを阻止するように構成されることを特徴とする請求項１記載のデータセンタ。
【請求項７】
前記ポリシーモジュールは、リモート要求が認証されたソースから受信されるかを判定し、且つ前記ソースが認証されてない場合に前記要求が処理されるのを阻止するように構成されることを特徴とする請求項１記載のデータセンタ。
【請求項８】
前記ポリシーモジュールは、動作を実行するリモート要求がそのような動作を要求する許可を有するアプリケーションから受信されるかを判定し、且つ前記要求側のアプリケーションがそのような許可を有さない場合に前記要求が処理されるのを阻止するように構成

されることを特徴とする請求項１記載のデータセンタ。
【請求項９】
前記ポリシーモジュールは、前記物理的にセキュリティ保護された環境内から入力されたコマンドにより再設定可能であることを特徴とする請求項１記載のデータセンタ。
【請求項１０】
公益事業制御及び通信ネットワークであって、
複数のエンドポイントノードと、
認証の関連証明書を有する物理的にセキュリティ保護された環境、
少なくともいくつかが前記データセンタの外側の場所から公益事業の動作に関係する機能を実行するリモート要求を受信するインタフェースを有する前記公益事業の前記動作と関連付けられた１つ以上のアプリケーションプログラムを実行するように構成された少なくとも１つのサーバ、
前記物理的にセキュリティ保護された環境内に配置され且つ暗号鍵を格納するハードウェアセキュリティモジュール、及び
前記アプリケーションプログラムに向けられたリモート要求を受信し且つ前記暗号鍵に従って署名される認可された要求を提供するように構成された前記物理的にセキュリティ保護された環境内に配置された認可エンジンを含むデータセンタと、
前記エンドポイントノードが前記データセンタに配置された前記アプリケーションプログラムと通信する少なくとも１つのアクセスポイントと、
前記データセンタにおいて前記物理的にセキュリティ保護された環境のセキュリティが危険にさらされているという表示に応答して、セキュリティが危険にさらされる前記物理的にセキュリティ保護された環境と関連付けられた前記証明書が無効であることを示す証明書撤回リストを構成するコマンドをアクセスポイントに対して発行し、且つアクセスポイントから前記証明書撤回リストをロードするコマンドを前記エンドポイントノードに対して発行するサーバと、
を備えることを特徴とするネットワーク。
【請求項１１】
前記サーバは、データセンタにおける前記物理的にセキュリティ保護された環境の前記セキュリティが危険にさらされているという表示に応答して、物理的にセキュリティ保護された環境が危険にさらされている前記データセンタから発信される通信を無視するコマンドを前記アクセスポイントに対して更に発行することを特徴とする請求項１０記載のネットワーク。
【請求項１２】
前記エンドポイントノードは、受信したコマンドが前記暗号鍵と関連付けられた公開鍵を使用して認可されるかを判定するように構成されることを特徴とする請求項１０記載のネットワーク。
【請求項１３】
公益事業ネットワークの装置を制御する方法であって、
前記公益事業ネットワークの装置により実行される動作に対するコマンドを生成することと、
前記コマンドをハードウェアセキュリティモジュールに転送することと、
前記ハードウェアセキュリティモジュール内において、
前記サービスが実行されると、前記コマンドの受信者が実行することを許可されるコマンドとして前記コマンドを認証することを可能にする前記コマンドに対して暗号サービスを実行する機能、
規定された期間に前記ハードウェアセキュリティモジュールにより実行された暗号サービスの数をカウントする機能、及び
前記規定された期間内に実行された暗号サービスの前記カウント数が閾値限界を超える場合、受信したコマンドに対する更なる暗号サービスの実行を終了する機能を実行することと、

前記暗号サービスが実行されると、前記動作を実行する前記コマンドを前記公益事業ネットワークの装置に送信することと、
を備えることを特徴とする方法。
【請求項１４】
暗号サービスの数の前記カウントは、前記規定された期間のスライディングタイムウィンドウ上で実行されることを特徴とする請求項１３記載の方法。
【請求項１５】
暗号サービスの数の前記カウントは、各々がそれぞれ異なる時間の長さ及び閾値限界と関連付けられる複数のスライディングタイムウィンドウに対して実行されることを特徴とする請求項１４記載の方法。
【請求項１６】
前記暗号サービスは前記コマンドの暗号化であることを特徴とする請求項１３記載の方法。
【請求項１７】
前記暗号サービスは前記コマンドに署名することであることを特徴とする請求項１３記載の方法。
【請求項１８】
暗号サービスの前記カウント数が前記閾値限界を下回る所定の値に到達する場合に警告を生成するステップを更に備えることを特徴とする請求項１３記載の方法。
【請求項１９】
前記ハードウェアセキュリティモジュールは複数のスロットを含み、前記機能は前記スロットのうちの１つにおいて実行されることを特徴とする請求項１３記載の方法。
【請求項２０】
前記機能は、それぞれの異なる閾値限界を使用して第２のスロットにおいて更に実行されることを特徴とする請求項１９記載の方法。
【請求項２１】
前記装置は、受信したコマンドが前記暗号サービスと関連付けられた公開鍵を使用して認可されるかを判定するように構成されることを特徴とする請求項１３記載の方法。
【請求項２２】
公益事業ネットワークの装置を制御する方法であって、
前記公益事業ネットワークの装置により実行される動作に対するコマンドを生成することと、
前記生成されたコマンドが許可を必要とするかを判定することと、
前記生成されたコマンドが許可を必要とする場合に前記コマンドを許可サーバに転送することと、
前記許可サーバ内において、（i）前記許可が有効である期間、（ii）実行される前記動作及び（iii）前記動作を実行する前記装置を規定する許可を生成することと、
前記許可を含むデータパケットを前記公益事業ネットワークの装置に送信することと、
前記装置において前記データパケットを受信すると、前記規定された動作が許可を必要とするか、且つ許可を必要とする場合に前記許可が現在有効であるかを判定することと、
前記許可が現在有効である場合に前記規定された動作を実行することと、
を備えることを特徴とする方法。
【請求項２３】
前記許可は、前記許可が有効になる時を示す開始値と、前記許可が前記開始値から有効なままである時間の長さを示す継続時間値とを含むことを特徴とする請求項２２記載の方法。
【請求項２４】
前記許可は、前記動作を実行する前記装置の表示を含む第１のフィールドと、前記第１のフィールドについての形式を示す第２のフィールドとを含むことを特徴とする請求項２２記載の方法。

【請求項２５】
前記第１のフィールドに含まれた前記表示は、前記装置のＭＡＣアドレスを含むことを特徴とする請求項２４記載の方法。
【請求項２６】
前記形式はＤＥＲオクテット列型であることを特徴とする請求項２４記載の方法。
【請求項２７】
前記許可は、前記許可サーバと関連付けられた鍵を用いて署名され、前記装置は、前記許可の前記署名を検証することを特徴とする請求項２２記載の方法。
【請求項２８】
前記許可サーバは、ハードウェアセキュリティモジュール内で実現されることを特徴とする請求項２２記載の方法。
【請求項２９】
前記ハードウェアセキュリティモジュールは、
規定された期間に前記ハードウェアセキュリティモジュールにより生成された許可の数をカウントする機能と、
前記規定された期間内に生成された許可の前記カウント数が閾値限界を超える場合、受信したコマンドに対する更なる許可の前記生成を終了する機能とを実行することを特徴とする請求項２８記載の方法。
【請求項３０】
生成された許可の数の前記カウントは、前記規定された期間のスライディングタイムウィンドウ上で実行されることを特徴とする請求項２９記載の方法。
【請求項３１】
生成された許可の数の前記カウントは、各々がそれぞれ異なる時間の長さ及び閾値限界と関連付けられる複数のスライディングタイムウィンドウに対して実行されることを特徴とする請求項３０記載の方法。
【請求項３２】
公益事業ネットワークに対する認証システムであって、
前記公益事業ネットワークの装置により実行される動作に対するコマンドを受信し、且つ（ｉ）許可が有効である期間、（ｉｉ）実行される前記動作及び（ｉｉｉ）前記動作を実行する前記装置を規定する前記許可を生成するように構成された許可サーバと、
前記許可を含むデータパケットを前記公益事業ネットワークの装置に送信するように構成された通信インタフェースと、
を備えることを特徴とする認証システム。
【請求項３３】
前記許可は、前記許可が有効になる時を示す開始値と、前記許可が前記開始値から有効なままである時間の長さを示す継続時間値とを含むことを特徴とする請求項３２記載の認証システム。
【請求項３４】
前記許可サーバはハードウェアセキュリティモジュールにおいて実現されることを特徴とする請求項３２記載の認証システム。
【請求項３５】
前記ハードウェアセキュリティモジュールは、
規定された期間に前記ハードウェアセキュリティモジュールにより生成された許可の数をカウントする機能と、
前記規定された期間内に生成された許可の前記カウント数が閾値限界を超える場合、受信したコマンドに対する更なる許可の前記生成を終了する機能とを実行するように構成されることを特徴とする請求項３４記載の認証システム。
【請求項３６】
生成された許可の数の前記カウントは、前記規定された期間のスライディングタイムウィンドウ上で実行されることを特徴とする請求項３５記載の認証システム。

【請求項３７】
生成された許可の数の前記カウントは、各々がそれぞれ異なる時間の長さ及び閾値限界と関連付けられる複数のスライディングタイムウィンドウに対して実行されることを特徴とする請求項３６記載の認証システム。
【請求項３８】
前記許可サーバが収容される物理的にセキュリティ保護された環境を更に含むことを特徴とする請求項３２記載の認証システム。
【請求項３９】
公益事業ネットワークであって、
前記公益事業ネットワークの装置により実行される動作に対するコマンドを受信し、且つ（i）許可が有効である期間、（ii）実行される前記動作及び（iii）前記動作を実行する前記装置を規定する前記許可を生成するように構成された許可サーバと、
前記許可を含むデータパケットを前記公益事業ネットワークを介して送信するように構成された通信インタフェースと、
データパケットを受信する前記公益事業ネットワークに接続された複数の装置であり、前記装置の各々が、
受信したデータパケットにおいて規定された動作が許可を必要とするかを判定し、
許可を必要とする場合に前記許可が現在有効であるかを判定し、且つ
前記許可が現在有効である場合に前記規定された動作を実行するように構成される複数の装置と、
を備えることを特徴とする公益事業ネットワーク。
【請求項４０】
前記許可は、前記許可が有効になる時を示す開始値と、前記許可が前記開始値から有効なままである時間の長さを示す継続時間値とを含むことを特徴とする請求項３９記載の公益事業ネットワーク。
【請求項４１】
前記許可サーバは、鍵を使用して前記許可に署名するように構成され、前記装置は、前記許可の前記署名を検証するように構成されることを特徴とする請求項３９記載の公益事業ネットワーク。
【請求項４２】
前記許可サーバは、ハードウェアセキュリティモジュールにおいて実現されることを特徴とする請求項３９記載の公益事業ネットワーク。
【請求項４３】
前記ハードウェアセキュリティモジュールは、
規定された期間に前記ハードウェアセキュリティモジュールにより生成された許可の数をカウントする機能と、
前記規定された期間内に生成された許可の前記カウント数が閾値限界を超える場合、受信したコマンドに対する更なる許可の前記生成を終了する機能とを実行するように構成されることを特徴とする請求項４２記載の公益事業ネットワーク。
【請求項４４】
生成された許可の数の前記カウントは、前記規定された期間のスライディングタイムウィンドウ上で実行されることを特徴とする請求項４３記載の公益事業ネットワーク。
【請求項４５】
生成された許可の数の前記カウントは、各々がそれぞれ異なる時間の長さ及び閾値限界と関連付けられる複数のスライディングタイムウィンドウに対して実行されることを特徴とする請求項４４記載の公益事業ネットワーク。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、公益事業会社と関連付けられた動作の管理及び制御に関し、特にそのような

動作を管理及び制御するシステムのセキュリティに関する。

【背景技術】

【０００２】

公益事業会社は、その動作を管理及び制御する多数の関連ソフトウェアモジュールを起動する物理サーバ上で実行する複雑で高度に相互接続されたシステムを有する。図１は、電力及び場合によっては例えばガス、水等の他の製品を顧客に供給する公益事業会社に対する一般的な管理及び制御システムにおいて見られる可能性のある構成要素のうちのいくつかを示す概略ブロック図である。システムのバックオフィス１０は、公益事業の種々の動作と関連付けられた多くの個々のサブシステム、例えば顧客情報システム（ＣＩＳ）１２と、顧客関連モジュール（ＣＲＭ）１４と、停止管理システム（ＯＭＳ）１６と、ＧＰＳ情報システム１８と、請求書作成システム２０と、グリッド安定モジュール２２と、ユーザインタフェース２４とを含む。図１には示されないが、更なる機能モジュールがバックオフィス１０に存在してよい。これらのサブシステムのうちのいくつかは、供給されている製品に対して配電網の装置と通信し、且つこれらの装置と関連付けられた動作をリモート制御する機能を有してもよい。例えばバックオフィスサーバは、顧客の建物に配置された個々のメータ２６と通信して請求書作成のための消費データを取得し、且つ公益事業会社により提供される１つ以上の製品の供給元に対して顧客を選択的に切断又は再接続するようにメータに指令してもよい。バックオフィスサーバから個々のメータへの他のコマンドは、顧客からのエネルギーの流出を受け入れるコマンドを含んでもよい。

【０００３】

図１の例において、メータは、ネットワークへの及びネットワークからの出口を提供するアクセスポイント３２を有するローカルエリアネットワーク３０によりバックオフィスと通信するエンドポイントノードを構成する。一実施形態において、ローカルエリアネットワークは無線メッシュネットワークであってよい。アクセスポイント３２は、ワイドエリアネットワーク３４又は専用の通信リンクにより、バックオフィス１０においてサーバと通信する。

【０００４】

この種のシステムにおいて、考慮すべき１つの問題は、それぞれ、顧客が建物を引き払うか又は支払いを滞納する場合、あるいは新しい顧客が建物を手に入れる場合に発生する可能性のあるリモート切断及び再接続をセキュリティ保護して管理することである。リモートで切断及び／又は再接続するように故意に且つ／あるいは誤って発行されたコマンドは、配電グリッドを不安定にする潜在性を有するだろう。無認可の再接続は、結果として配電された電力の盗難ともなりうる。そのような可能性を制限するために、コマンド・制御動作がそのような動作を実行する認可を受けているエンティティによってのみセキュリティ保護されて行われることを保証する努力がなされなければならない。しかし、一般的な公益事業のバックオフィスが種々の相互接続されたシステムから構成されるため、セキュリティ保護されたアクセスの実行は困難になる。公益事業内の多くの異なるグループは、全て又は一部のソフトウェアシステムへのアクセスが必要であり、これにより個々のサブシステムへの論理的及び／又は物理的なアクセスを制限する機能は複雑になる。

【０００５】

この問題に対する１つの可能な解決策は、以下においてバンカ（bunker）と呼ばれる物理的にセキュリティ保護された環境内にある特定のシステム又はそのようなシステムの一部を配置することである。バンカの例には、密室等のアクセスが制限された部屋又はコンテナ及び保護されたシステムの周囲のタンパ防止シェル又はエンクロージャが含まれる。バンカは、システム又はシステムの保護された部分が実行しているハードウェア装置への物理的アクセスを厳しく制限する。また、バンカ内のシステムは、非常に限定された論理的なアクセスをエクスポートする。しかし、この解決策は、より融通性のあるアクセスをそれを必要とするユーザに提供するためにバンカ内に配置されるべき部分及びバンカの外側に配置してもよい部分を判定するように公益事業ソフトウェアシステムをリファクタリングするのは困難であるという困難な問題を依然として提示する。

【発明の概要】
【０００６】
全体的なセキュリティを公益事業管理システムに提供するために、システムの構成要素に対して発行される重要なコマンド・制御メッセージは、セキュリティ保護された権限により明示的に承認される必要がある。明示的な承認により、要求された動作を認証し、メッセージにおいて示された特定の動作の実行を認可する。アクセス制御と関連付けられる公益事業管理及び制御システムの重要な構成要素は、物理的にセキュリティ保護された環境に配置される。この手法を用いる場合、例えばバンカによりネットワーク動作を承認する役割を担うこれらのサブシステムを物理的にセキュリティ保護することのみが必要となる。換言すると、例えばＣＩＳ、ＣＲＭ、ＯＭＳ、請求書作成等の殆どの管理モジュールは、バンカの外側に配置されてもよく、それにより、これらのサブシステムをバンカ及び非バンカされた構成要素に区分する必要性を回避する。非バンカされたサブシステムの各々の重要な構成要素へのアクセスは、バンカされた承認システムを介して制御される。
【図面の簡単な説明】
【０００７】
【図１】図１は、公益事業管理及び制御システムを示す概略ブロック図である。
【図２】図２は、バンカされた構成要素を有する公益事業バックオフィスシステムを示すブロック図である。
【図３】図３は、メッセージがメータに送出される際のデータの流れを概略的に示すブロック図である。
【図４】図４は、ハードウェアセキュリティモジュールの構成を示すブロック図である。
【図５】図５は、スライディングウィンドウ上で暗号動作をカウントする多段バッファを示すブロック図である。
【図６】図６は、コマンドに対する許可を発行するシステム及び手順の一例を示す図である。
【図７】図７は、許可ペイロードの例示的な形式を示すブロック図である。
【図８】図８は、多数のデータセンタにおいて実現された公益事業制御及び管理システムを示すブロック図である。
【発明を実施するための形態】
【０００８】
本発明が基づいている原理を理解しやすくするために、以下において、配電システムにおけるリモート接続及び切断コマンドのセキュリティ保護された制御を参照して本発明を説明する。しかし、そのような例がこれらの原理の唯一の実際的な応用例ではないことが理解されるだろう。これらの原理は、不適当に又は誤って発行された場合にはシステムを大きく混乱又は損傷させる潜在性を有する可能性のあるあらゆる種類の重要なコマンドと併せて採用される。同様に、これらの原理は、適切な動作が常に必須であるシステムの重要な構成要素に送出された全てのコマンド・制御メッセージと組み合わせて使用可能である。
【０００９】
図２は、本発明の概念が実現されるデータセンタ４０の一例を示す。従来のように、データセンタは、種々のアプリケーション１２、１４、１６が実行される多くの物理サーバを含む。いくつかの代表的なアプリケーションのみを図示するが、より多くのそのようなアプリケーションがデータセンタ内で実現可能であることが理解されるだろう。逆に、アプリケーションのうちのいずれか２つ以上により実行された機能は、単一の包括的なプログラムに組み込まれてもよい。
【００１０】
補強壁を有する密室等の制限された物理的アクセスを有する物理バンカ４２もデータセンタ内に配置される。別の例として、バンカは、ロックされることに加えあるいはその代わりに、セキュリティカメラ、動作検出器等を使用して厳密に観察又は保護される領域であってもよい。更に別の例として、バンカは物理的に配電されてもよく、セキュリティ関

係は配電された部分の間で確立されている。更に別の例として、バンカは、例えばセキュリティ保護して実行しているソフトウェア及び／又はファームウェアを使用して論理的にセキュリティ保護されてもよく、その機能性は、自己破壊的な包装等の物理的タンパリングからセキュリティ保護される。バンカは、部屋である必要はないが、例えば物理的にセキュリティ保護されたボックスであってもよい。

【００１１】

関連ハードウェアセキュリティモジュール４４を有する１つ以上の更なるサーバ装置は、認可、認証及び課金等のセキュリティ関連動作を実行するソフトウェアモジュールを有する認可エンジン４６を実現するためにバンカ内に配置される。ハードウェアセキュリティモジュールは、秘密鍵又は他の共通鍵をセキュリティ保護して含む。ハードウェアセキュリティモジュールは、秘密鍵にリンクされる公開証明書を更に含んでもよい。ハードウェアセキュリティモジュールは、暗号動作を実行するために、楕円曲線暗号法等の強固なあるセキュリティアルゴリズム又は別の高度にセキュリティ保護された暗号方式を使用することが好ましい。本明細書において説明するアプリケーションに対して適切なハードウェアセキュリティモジュールの一例は、Ｕｔｉｍａｃｏ　Ｓａｆｅｗａｒｅ　ＡＧからのハードウェアセキュリティモジュールのＳａｆｅＧｕａｒｄ　ＣｒｙｐｔｏＳｅｒｖｅｒラインである。

【００１２】

バンカへのセキュリティ保護されたアクセス及びバンカ内に配置されたサーバ装置は、指紋検出、物理的な鍵又はトークン及び／あるいはパスワード保護等のバイオセンサ技術を用いて実行可能である。一実現例において、階層的な階層セキュリティシステムは、保護を最大限にするように採用される。セキュリティの１つの層が障害を起こす場合、例えばパスワードが偶発的に暴露又は盗難される場合、システム全体の物理的なセキュリティを維持するために、鍵又はトークンが作動させたデッドボルトロック等の高水準のセキュリティ機構が起動される。

【００１３】

非バンカされたバックオフィスアプリケーション１２～１６からのある特定の種類のコマンドは、個別に認証されない限り実行されないように制限される。例えば、リモート切断及び再接続のコマンドは、配電グリッドの安定の深刻な中断を引き起こすという潜在性のために、これらの制限されたコマンドのうちの１つの分類である。これらの種類の動作に関係するセキュリティを強化するために、それらを実行するアプリケーションは、バンカ４２内のコンソールから発生するか、あるいはバンカ４２内から発行された許可により認証される場合にのみのそのように実行するコマンドを受け入れてもよい。従って、これらのコマンドを発行する権限を有し且つバンカにアクセスするために必要な手段、例えばパスワード、鍵、指紋等を処理する人員だけがアプリケーションに対して制限されたコマンドを発行できる。

【００１４】

コマンドを生成させる動作が開始されると、その動作は、認可エンジン４６により署名又は認証されて、バンカ４２の外部の適切なアプリケーションと関連付けられたアプリケーションプログラミングインタフェース（ＡＰＩ）に転送されてもよい。例えばコマンドは、ハードウェアセキュリティモジュール４４内に格納された秘密鍵により署名されてもよい。署名されたコマンドは、外部のアプリケーション、例えばアプリケーション１２～１６のうちの１つ又はメータ２６のうちの１つにおいて実行するアプリケーションにおいて受信されると、アプリケーションがアクセスした公開鍵により検証される。コマンドは、バンカ内から発生したものとして検証されると、外部のアプリケーションにより実行される。

【００１５】

状況によっては、リモート切断コマンドを発行するエンティティがバンカ内に物理的に存在しているのは実際的ではないだろう。しかし、そのようなコマンドのリモート生成が支持される場合、そのようなコマンドは、認可されたエンティティになりすましているユ

ーザにより故意に発行される可能性がある。そのようなことが発生する可能性を制限するために、本発明に従って、ポリシーモジュール４８はバンカ内で実現される。ポリシーモジュールは、図２に示されるように、別個のソフトウェアコンポーネント又はファームウェアコンポーネントであってもよく、あるいは以下において説明されるように、ハードウェアセキュリティモジュールに論理的に組み込まれてもよい。ポリシーモジュール４８は、例えばバンカ内部から入力されたコマンドにより、セキュリティ保護して再設定又は再プログラムされてもよい。このモジュールは、要求された動作を検査するビジネス論理を含み、その実行が許可されるかを判定する。例えば、配電グリッドの安定を中断しうる再接続コマンドは、順番に又は相対的なタイミングで発行される場合、ポリシーにより阻止されて署名のために認可エンジンに渡されない。また、ある特定の条件が検出される場合、ポリシーフラグがオンにされ、コマンドを発行するエンティティの切断等の適切な措置がとられる。これらの条件は、例えば以下のものを含みうる。

【００１６】

１．配電グリッドからユーザを故意に切断することを意図する多くのリモート切断コマンドは、一度に、例えば所定の時間間隔内に発行される。

【００１７】

２．同一の顧客と関連付けられる一連の繰返しの接続及び切断のコマンド又は例えばまだ電力グリッドに接続していないユーザに対して切断コマンドを発行する顧客の現在の状況に一致しないコマンド等のコマンドは、疑わしい順序で発行される。

【００１８】

３．要求側のアプリケーションは、必要な信用証明書を提供できないか、あるいは認証されない。

【００１９】

４．要求側のアプリケーションは、ある特定の動作を発行する許可を有する承認されたアプリケーションの集合の間にはない。

【００２０】

５．実際の電力負荷及び予想された電力要求に基づいている配電網の状態。

【００２１】

この機能性を実現するために、バンカは、バンカの外部にあるアプリケーションのアプリケーションプログラミングインタフェース（ＡＰＩ）に対するプロキシ５０を含んでもよい。動作中、これらの「外部の」アプリケーションのうちの１つに対するＡＰＩへの呼び出しが行われる場合、その呼び出しはバンカ内のプロキシ５０に向けられる。プロキシは、要求を認可することが必要とされてもよいポリシーモジュール４８において公益事業ビジネス論理を調査し、適切なビジネス論理により署名された要求を有する。その後要求は、署名のために認可エンジン４６に渡される。認可されると、プロキシは、バンカの外部にある呼び出されたアプリケーションに対して正常なＡＰＩを呼び出し、認可された呼び出しに沿って通過する。

【００２２】

別の一実現例において、バンカ４２はプロキシを含まなくてもよい。この場合、要求は、外部のアプリケーションのＡＰＩに対して直接行われてもよい。その結果、外部のアプリケーションは、要求された動作が署名を必要とすると判定する場合にバンカ内で認可エンジンを呼び出す。デフォルトとして、全ての要求は、認可のためにバンカに渡され、外部のアプリケーションによるあらゆる判定の必要性を回避してもよい。バンカに提供された要求は、最初にポリシーモジュールによりチェック及び署名され、次に認可エンジン４６に渡される。要求が認可されると、呼び出されたアプリケーションは要求に基づいて動作する。

【００２３】

バンカ４２に含まれたハードウェアセキュリティモジュール４４は、２つのレベルで動作可能である。メータ２６において実行される動作と併せて、以下において例を説明する。動作の第１のレベルにおいて、公益事業会社は、バックオフィス１０におけるアプリケ

ーションとメータ２６との間の全ての通信又はネットワーク３０の他のあらゆる構成要素が暗号化及び署名されなければならないというポリシーを設けてもよい。このポリシーの実現例を図３の例に示す。この例において、メータ管理アプリケーション５２は、メータ２６のうちの１つ以上に送出するコマンド等のメッセージを有する。メッセージの適切な暗号化及び署名を実行する要求と共に、このメッセージは、アプリケーションのメータコマンド及びインタフェースモジュール５４において構成され、バンカ４２のハードウェアセキュリティモジュール４４に転送される。ポリシーモジュール４８は、要求が認可されたソースから発生したことを確認するように最初にチェックしてもよい。そのような場合、ポリシーモジュール４８は、ハードウェアセキュリティモジュールに沿って渡される。ハードウェアセキュリティモジュール４４は、アプリケーションと関連付けられた適切なキーを使用して、メッセージに対して要求された動作を実行し、暗号化及び署名されたデータを返送する。その後、メータ管理アプリケーションのコマンド及びインタフェースモジュール５４は、暗号化及び署名されたメッセージを組み込むデータパケットを作成し、ネットワーク３０を介してそれをメータに送信する。

【００２４】

アプリケーション５２によりネットワーク３０においてノードから受信したメッセージについては、それらは、復号化されるために最初にハードウェアセキュリティモジュールに転送される。更にモジュール４８は、受信したメッセージの送出者の信憑性及びデータの整合性のあらゆる適切な検証を実行できる。その後、検証及び復号化されたメッセージはアプリケーション５２に返送される。

【００２５】

リモート接続及び切断等の重要な動作については、ハードウェアセキュリティモジュールは、そのような動作に対する速度を制限するように第２のレベルで動作可能である。図４は、ハードウェアセキュリティモジュールの内部構成の一例を示す。モジュールは多くのスロットで構成される。各スロットは、例えば署名、暗号化、復号化等の暗号サービスを実行するために、秘密鍵、証明書、共有鍵及びアクセス特権の集合を含む。種々のスロットは、種々のセキュリティコンテキストと関連付けられ、それぞれのコンテキストに関係する鍵、証明書及び他の情報を含む。秘密鍵を用いてそれに署名する等のハードウェアセキュリティモジュールを用いてコマンドに対して暗号サービスを実行することにより、関連公開鍵を使用してコマンドのソースを認証するノード２６等のコマンドを受信できる。ポリシーモジュール４８は、要求されたコマンドを１つ以上の暗号サービスのためにハードウェアセキュリティモジュールに対して提示できるかを最初に判定する。

【００２６】

各スロットは、例えばコマンドライン管理ツールにより１つ以上の速度制限で所望のビジネス論理を実行するように選択的に構成可能である。スロットを構成するコマンドの一例は以下の通りである。

【００２７】

ＨＳＭ＿ｃｏｎｆｉｇｕｒｅ　ｓｌｏｔ＝２＝ｒａｔｅ－ｎａｍｅ＝”ｒａｔｅ１”ｗｉｎｄｏｗ＝２４ｈ　ｃｏｕｎｔ＝１００００

そのようなコマンドは、２４時間のスライディングウィンドウ毎に１０，０００個の暗号動作の最大速度制限でスロット２を構成する。この割り当てられた数を上回る暗号動作が先行する２４時間内に発生する場合、スロットは、全ての更なる暗号動作を停止する。その後、管理者は、リセットコマンドを送出することでスロットをリセットすることが必要となる。

【００２８】

スロットは、以下の通り２つ以上の速度で構成可能である。

【００２９】

ＨＳＭ＿ｃｏｎｆｉｇｕｒｅ　ｓｌｏｔ＝２＝ｒａｔｅ－ｎａｍｅ＝”ｒａｔｅ１”ｗｉｎｄｏｗ＝２４ｈ　ｃｏｕｎｔ＝４００００

ＨＳＭ＿ｃｏｎｆｉｇｕｒｅ　ｓｌｏｔ＝２＝ｒａｔｅ－ｎａｍｅ＝”ｒａｔｅ２”

ｗｉｎｄｏｗ＝６０ｍ　ｃｏｕｎｔ＝２０００
これらの２つのコマンドは、１つが２４時間のスライディングウィンドウ上の４０，０００個の暗号動作に対するもので、別が６０分間のスライディングウィンドウ上の２０００個の暗号動作に対するものである２つの速度制限ウィンドウを用いてスロット２を構成する。

【００３０】
スロットが速度制限で構成される場合、スロットにおいて実行された全ての暗号動作は、スライディングウィンドウ上で割り当てられた制限に対してカウントされる。先に挙げられた例において、過去２４時間に４０，０００個を上回る暗号動作又は最後の６０分に２０００個を上回る暗号動作がある場合、スロットは、更なる暗号動作のいずれも停止する。

【００３１】
一実施形態において、閾値の侵害に対する課金は５分刻みで実行可能である。図５は、スロットが２５分間のスライディングウィンドウにおいて８００個の暗号動作の制限で構成されている一例を示す。スライディングウィンドウは、多段バッファ５６として実現可能である。示されたバッファは、各々が５分間の時間間隔を表す５つの段階５８を含む。各段階は、対応する時間間隔の間にスロットにより実行された暗号動作のカウント数を含む。以下の表は、所定の時点でバッファに含まれたデータのスナップショットを提供する。

【００３２】
【表１】

段階	時間フレーム	カウント
1	－25分～－20分	15
2	－20分～－15分	0
3	－15分～－10分	7
4	－10分～－5分	1
5	－5分～0分	6

【００３３】
この場合は１５＋０＋７＋１＋６＝２９である全てのカウントの合計が閾値を超える場合、スロットは、管理上リセットされるまで全ての更なる暗号動作を停止する。警告機構は、動作が停止される時間の前に管理人に通知するように実現可能である。例えば、カウントの合計が速度制限の８０％を超える時に第１の警告が生成されてもよく、カウントの合計が制限の９０％に到達する場合に第２の警告が生成されてもよい。

【００３４】
この場合は段階５である最後の間隔と関連付けられた段階は、新しい暗号動作の各々の実行カウントを維持する。５分間の間隔の各々の最後に、格納されたカウントは次に以前の段階にシフトされる。最新の段階は、ゼロにリセットされ、次の５分間の間隔の間にもう一度新しく暗号動作をカウントし始める。

【００３５】
各スロットが自身の速度制限で選択的に構成可能であるため、ビジネス論理の実現例において柔軟性が与えられる。例えば以下において説明するように、ある特定の重要なコマンドは、実行可能になる前に、以下において「許可」と呼ばれる明示的な種類の認証を要求してもよい。これらのコマンドは、許可手順を実行するスロットと関連付けられるセキュリティコンテキストにマッピングされ、且つ特に厳しい速度制限を有してもよい。他の種類のコマンドは、異なるセキュリティコンテキストにマッピングされ、且つより厳しくない速度制限を有する異なるスロットを介して暗号化及び／又は署名されてもよい。

【００３６】
リモート切断及び再接続のコマンド等の重要なコマンドについては、各々が受信側のノ

ードにおいて認証されなければならない多数の関係者による承認等のより高いレベルのセキュリティが適切だろう。しかし、ネットワーク効率の観点から、より高いレベルのセキュリティは、コマンドが向けられるノードがコマンドを実行するために１度接続されるだけでよい場合に望ましい。本発明の一態様において、これらの目的は、ノードがコマンドを認証できるように要求された全ての情報を提供する許可システムにより実現可能である。本質的に、メータに対する切断コマンド等のアプリケーションに送出される全ての重要なコマンドは、許可を伴うことを要求されてもよい。上述したように、種々のコマンドは種々のセキュリティコンテキストにマッピング可能である。コマンドがアプリケーションにより自動的に又はユーザインタフェースを介して発行される場合、発行側のアプリケーションはコマンドのセキュリティコンテキストをチェックする。暗号化が要求される場合、コマンドは、そのような動作のためにハードウェアセキュリティモジュールの適切なスロットに転送される。セキュリティコンテキストが許可を必要とすると判定される場合、コマンドは、許可を発行するバンカの許可サーバに転送される。一実施形態において、許可サーバの機能は、ハードウェアセキュリティモジュールにおいてスロットにより実現可能である。

【００３７】

配電グリッドから建物を切断するコマンドを参照して、許可を発行する構成及び手順の一例を図６に示す。この例において、課金システム等のバックオフィス１０におけるビジネスモジュールのうちの１つは、口座と関連付けられた建物への切断コマンドをメータ管理アプリケーション５２に対して発行する。このコマンドを受信すると、メータ管理アプリケーションは、特定の時間に切断動作をスケジュールしてもよく、次に、メッセージをセキュリティ保護されたリンクを介して負荷マネージャモジュール５９に送出し、コマンドを発行する許可を要求する。負荷マネージャは、バンカ４２内に配置されるビジネス論理の構成要素であり、配電グリッドへの負荷変動が有害となる可能性があるかを判定する。この例において、負荷マネージャは許可サーバの一実現例として機能する。負荷マネージャは、要求された変動が有害となる可能性があると判定される場合に要求を拒否するか、例えば非常に多くの要求が現在未処理である場合にある期間の間要求を延期するか、あるいは要求を承認できる。負荷マネージャに対する要求は、コマンドの実行を完了するために必要なターゲットノード、スケジュールされた動作時間及び時間ウィンドウのサイズ等の情報を含んでもよい。

【００３８】

要求が承認される場合、負荷マネージャは、コマンドが向けられるノードにより認識可能な許可を作成する。許可は、メータ管理アプリケーション５２に返送される前に、負荷マネージャと関連付けられた鍵を用いて署名される。示された例において、許可サーバ、すなわち負荷マネージャ５９は、ハードウェアセキュリティモジュール４４から離間される。従って、この場合、許可は、負荷マネージャの秘密鍵を用いて署名されるハードウェアセキュリティモジュールに送出される。その後、署名された許可は、メータ管理アプリケーション５２に転送される負荷マネージャに返送される。

【００３９】

署名された許可を受信すると、メータ管理アプリケーションは、署名された許可と共に、切断される建物と関連付けられるノード２６に認可されたコマンドを送出する。次にノードは、負荷マネージャの信用証明書を介して、例えば許可からの証明書のチェーンに後続することにより、配電グリッドに対するシステムオペレータと関連付けられたルート権限に対する許可を検証する。ノードは、許可内の時間値が現在時刻に一致することを更に検証する。全ての情報が正確であり且つ検証される場合、ノードは、コマンドを実行し、コマンドの完了を示す署名されたレシートをメータ管理アプリケーション５２に送出する。レシートのコピーは、未処理の要求を追跡し続けられるように負荷マネージャ５９に送出されてもよい。

【００４０】

メータ管理アプリケーション５２は、異なる制御エンティティ、すなわちメータ管理ア

プリケーション及び負荷マネージャにより発行されるコマンドに対する２つの独立した認可を提供するために、ノードに送出されるパケットのペイロードに更に署名できる。双方の形式の認可は、ノードがコマンドを実行する前にノードにより検証される必要がある。この例において、負荷マネージャ等の許可サーバは、ノード２６と直接通信するために必要とされる信用証明書を処理しない。許可サーバは、認可されたコマンドを実行するために、この場合はメータ管理アプリケーション５２である別の制御エンティティに信用証明書を提供する。

【００４１】

コマンドを承認するかを判定するビジネス論理は、相対的に単純であってよく、例えば、所定の数の切断動作の最初のバーストが許可されるリーキーバケットアルゴリズムであってよく、単位時間当たりより少ない数の動作が後続する。この場合、負荷マネージャの機能は、上述した速度制御を使用してハードウェアセキュリティモジュールのスロット内で実現されてもよい。別のより複雑なアルゴリズムは、配電網の状態に基づいていてよく、例えば電力要求の予想に基づいて実際の電力負荷を追跡し且つ判定を行う。この後者の実施形態は、ハードウェアセキュリティモジュールの外側で、図６に示されたように、例えば専用の物理システム、仮想化されたサーバ又は共有システム上のアプリケーション内で実行されてもよい。

【００４２】

リモート切断及び再接続に加え、他の種類のコマンドは、規定された期間にわたり消費量を減少する顧客の建物に向けられる負荷制限コマンド等の許可を有するように要求される。また、システムにおける特定の種類の装置のセキュリティ保護された動作が配電自動化構成要素等のシステムの安定に対して重要である場合、その装置に対して発行された全てのコマンドは、許可を有するように要求されてもよい。バックオフィスモジュールは、そのような装置に対してコマンドを発行する場合は常に、必要な許可を得るために許可サーバにコマンドを転送する。

【００４３】

メッセージのペイロード内に含まれる許可に対する例示的な形式を図７に示す。許可ペイロードの第１のフィールド６０は、開始時間、すなわち許可が有効になる時間を示す。許可ペイロードを含むメッセージがノードにおいて受信される場合、ノードは開始時間を現在時刻と比較する。開始時間が現在時刻＋５分等の所定の増分より遅い場合、ノードは、無効なものとして許可を拒否する。

【００４４】

許可ペイロードの第２のフィールド６２は、許可が有効なままである間の継続時間ウィンドウを示す。このフィールドは、開始時間を超えると許可が有効である５分間のブロック等の所定の時間間隔の数を示す値である。ノードの現在時刻が許可開始時間＋所定の間隔とウィンドウ値との積より大きい場合、許可は無効なものとして拒否される。例えば、開始時間が１：００：００であり、ウィンドウ値が２であり且つ現在時刻が１：１２：３８である場合、許可は期限が切れているものとして拒否される。

【００４５】

許可ペイロードの次のフィールド６４は、実行が許可される動作を示す。例えばこのフィールドは、電力切断動作又は電力再接続動作を示す値を含んでもよい。多数の動作は単一の許可と関連付けられる。ターゲットの種類のフィールド６６は、後続するターゲットフィールド６８に対する形式を示す。ターゲットフィールド６８は、すなわち許可された動作を実行するノード又は装置を指定する。例えばターゲットは、ノードのＭＡＣアドレスであってよい。ターゲットの種類のフィールド６６は、ＤＥＲオクテット列型等のこのアドレスが表現される形式を示す。

【００４６】

セキュリティを更に向上するために、切断又は再接続のコマンドが一度に１つのメータに対してのみ発行可能であるという制約が課されてもよい。許可を発行する前に、負荷マネージャは、装置に対するターゲットアドレスが単一の装置と関連付けられ、且つグルー

プ又はブロードキャストのアドレスではないことを保証するようにチェックしてもよい。

【００４７】
許可ペイロードは、示された動作に対して特権を有する証明書と関連付けられた秘密鍵により署名される。許可ペイロードを含むデータパケットを受信すると、ノードは、示された動作が許可を必要とするかを確認するように最初にチェックする。許可が必要とされる場合、ノードは、許可に署名するために使用された証明書及び秘密鍵が要求された動作を実行するために必要な特権を有することを確認する。確認が肯定的である場合、ノードは、示された証明書の対応する秘密鍵により署名されているものとして、署名された許可の信憑性を検証する。次にノードは、ターゲット指定がノード自体を識別することを検証する。最後にノードは、現在時刻に対する開始時間及びウィンドウ値を調査し、許可の期限が切れていないことを確認する。
【００４８】
全ての検証チェックが成功した場合、動作が実行され、成功した実行を確認するために応答が返送される。検証ステップのうちのいずれかが失敗する場合、許可は拒絶され、エラーメッセージが返送される。データパケットにおける全ての動作が完了しているかあるいはエラーメッセージが返送されるとすぐ、許可は破棄されてそれ以上保持されない。
【００４９】
バンカへのアクセスが危険にさらされる場合には、適切な形式の救済措置が実現されてもよい。１つのそのような解決策は、バンカと関連付けられる論理的又は物理的な非常ボタンを提供することである。この非常ボタンは、非常ボタンと関連付けられたバンカが危険にさらされ且つもはや信用されるべきではないことを管理システムに通知するように起動可能である（例えば、物理ボタンを押下又はユーザインタフェース要素を起動するユーザ、あるいは自動的に適切な判定を行う論理により）。例えば、危険にさらされたバンカにより署名されるリモート切断サービスに対するいかなる要求も無視されるべきではない。
【００５０】
非常ボタンは種々の方法で実現可能である。適切な例には、無線又は有線の通信システムを介して送出される制御信号、ローカル又はワイドエリアネットワークに接続される従業員のデスク等の適切な場所における物理的なプッシュボタン、並びに／あるいはオーディオコマンド機能及び無線接続性を有するウェアラブルデバイスが含まれる。
【００５１】
図８は、非常ボタンの機能性が実現可能であるシステムの一例を示す。この例において、公益事業管理及び制御システムは、２つのデータセンタ７０及び７２内に収容される。例えば各データセンタは、冗長のために種々の管理及び制御サブシステムの完全なインスタンスを含んでもよい。各データセンタは、それぞれ「バンカ１」及び「バンカ２」とラベル付けされた関連バンカを含む。各バンカは、ルートが認識されている権限にある証明書チェーンを含む証明書を有する。２つのバンカに対する証明書は互いに異なる。
【００５２】
アクセスポイント３２及びエンドポイントノード２６等の制御ネットワークにおける各ノードは、証明書撤回リストを格納及びインストールする機能を有する。アクセスポイント３２は、ソースアドレスをフィルタリングする機能を更に有する。
【００５３】
例示的な動作は、バンカ１へのアクセスが危険にさらされている状況を説明する。バンカ１と関連付けられた非常ボタンが起動され、その結果得られる非常信号は、非常ボタン機能を実現するバンカ２のサーバに送出される。この非常信号は、それが送出される装置の認証の適切な表示を含む。例えばこの非常信号は、装置と関連付けられた署名を含んでもよく、あるいは所定のアルゴリズムに従って生成されたハッシュ値を伴ってもよい。認証された非常信号を受信すると、バンカ２のサーバは、データセンタ７０から発信されるパケットをドロップするように全てのアクセスポイント３２に命令するファイアウォール

ルールを全てのアクセスポイント３２に対して設定するコマンドを発行する。バンカ２のサーバは、バンカ１と関連付けられた証明書が有効ではないことを示す全てのアクセスポイント上の証明書撤回リストを構成するコマンドを更に発行する。バンカ２のサーバは、アクセスポイントから証明書撤回リストを再ロードするように全てのエンドポイントノードに命令するメッセージを全てのエンドポイントノードに更に送出する。

【００５４】

データセンタ７０からパケットをドロップするようにアクセスポイント上のファイアウォールフィルタを構成することにより、潜在的な攻撃者は、証明書撤回リストを全てのエンドポイントノードに伝播できるような十分な期間、減速されてもよい。潜在的な違反が発生した後にバンカ１を回復するために、新しい証明書がインストールされなければならず、その証明書との新しい関連付けが行われて、制御ネットワークにおいて全てのノードに伝播される。

【００５５】

要約すると、開示された本発明は、公益事業会社により提供された製品の供給と関連付けられた故意の又は不適切な動作の危険性を低下させる種々のセキュリティ機能を提供する。公益事業配電網の安定を中断する潜在性を有する重要なコマンドは、そのようなコマンドの認証、署名及び暗号化のためにハードウェアセキュリティモジュールを使用することと組み合わせて、バックオフィス管理システムの影響されやすい構成要素へのアクセスを制限する物理バンカの機構を介してセキュリティ保護される。許可に基づく認可フレームワークは、特に重要なコマンドに対して細粒レベルのセキュリティを提供する。ハードウェアセキュリティモジュールは、コマンドが実行される速度を制限し、且つ不適当なコマンドのシーケンスを発行しようという試みを更に妨害するように更に構成される。

【００５６】

開示された概要はその趣旨又は必須の特徴から逸脱せずに他の特定の形式において実施可能であることは、当業者により理解されるだろう。本発明で開示された実施形態は、限定するものではなく例示するものとして全ての点において考慮される。本発明の範囲は、上述の説明ではなく添付の特許請求の範囲により示され、添付の特許請求の範囲の意味及び等価の範囲内の全ての変更は、特許請求の範囲に含まれることを意図する。

【図１】

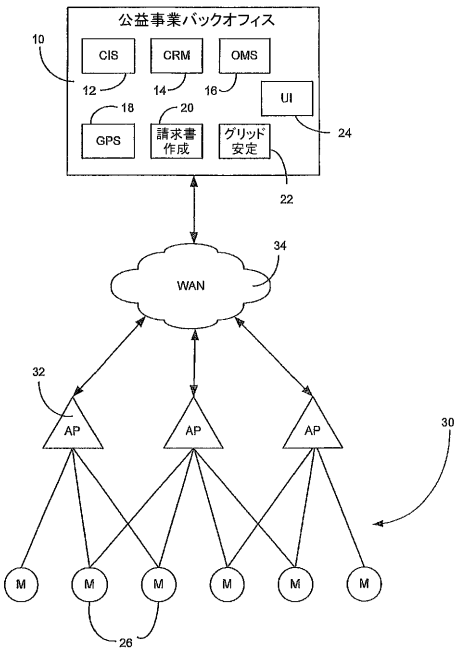

Fig. 1

【図２】

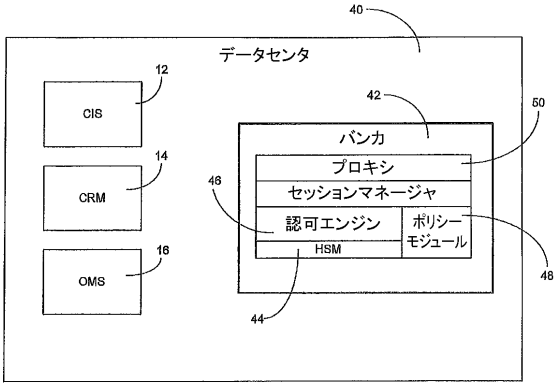

Fig. 2

【図３】

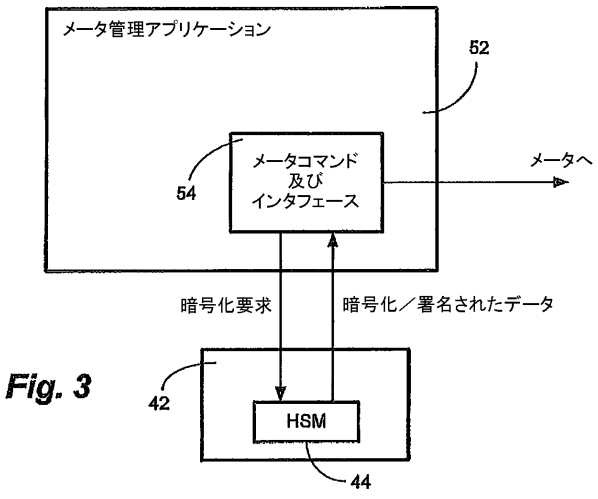

Fig. 3

【図４】

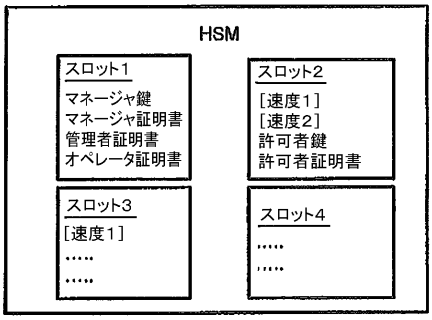

Fig. 4

【図５】

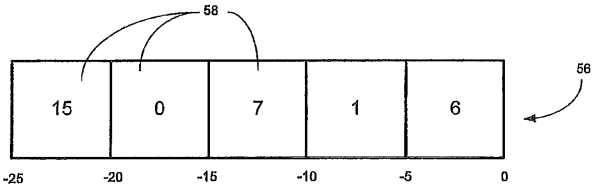

Fig. 5

【図６】

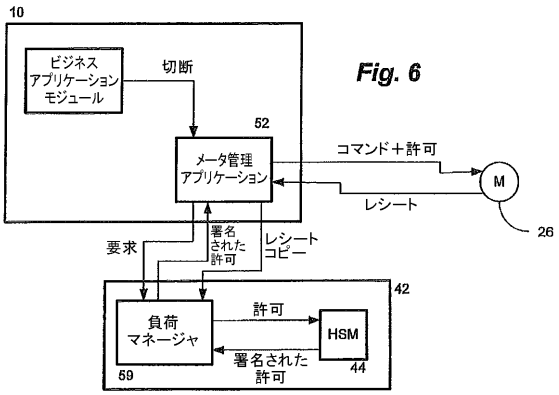

Fig. 6

【図７】

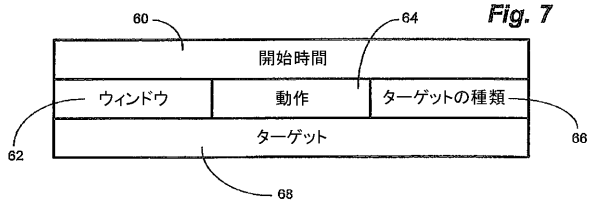

Fig. 7

【図８】

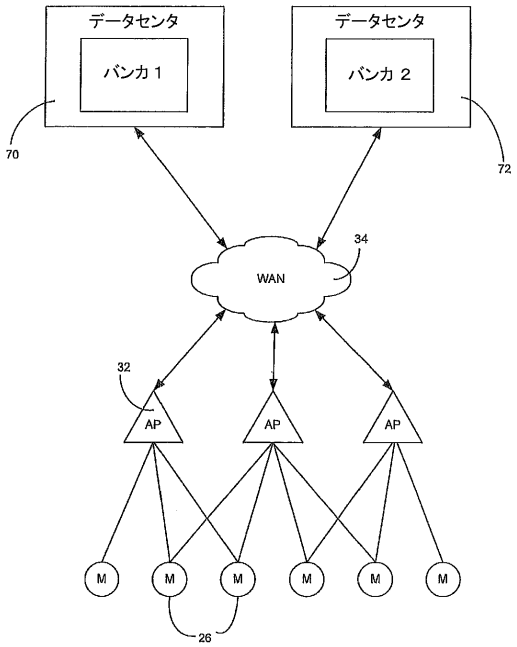

Fig. 8

【国際調査報告】

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2011/055705

A. CLASSIFICATION OF SUBJECT MATTER

G06F 21/20(2006.01)i, G06F 21/22(2006.01)i, H04L 9/32(2006.01)i

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)

G06F 21/20; G06K 5/00; G06F 7/00; G06F 12/14; H04L 9/32; G06F 21/00; G06Q 20/00

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

Korean utility models and applications for utility models
Japanese utility models and applications for utility models

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

eKOMPASS(KIPO internal) &
Keywords:(cyptographic*,encryption*,authenticat*,confirm*,monitor*,supervis*,securing*,guard*,safe*,protocol*,securit*,confident*,key* secrecy* privacy*)+(application*

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 2010-0044433 A1 (WANKMUELLER JOHN R. et al.) 25 February 2010 See abstract, claims 14-16	1-45
A	US 2010-0275016 A1 (ZIMMER VINCENT J. et al.) 28 October 2010 See abstract, claims 33,35,37,40,43,44,49 and figure 2	1-45
A	US 2008-0222714 A1 (WAHL MARK FREDERICK) 11 September 2008 See abstract, claims 1,4,11,13 and figure 1	1-45
A	US 7770789 B2 (ODER, II JOHN DAVID et al.) 10 August 2010 See abstract, claims 1,12	1-45

☐ 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 but 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 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	Date of mailing of the international search report
17 APRIL 2012 (17.04.2012)	**18 APRIL 2012 (18.04.2012)**

Name and mailing address of the ISA/KR	Authorized officer
Korean Intellectual Property Office Government Complex-Daejeon, 189 Cheongsa-ro, Seo-gu, Daejeon 302-701, Republic of Korea Facsimile No. 82-42-472-7140	UHM, In Kwon Telephone No. 82-42-481-5712

Form PCT/ISA/210 (second sheet) (July 2009)

INTERNATIONAL SEARCH REPORT
Information on patent family members

International application No.
PCT/US2011/055705

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2010-0044433 A1	25.02.2010	None	
US 2010-0275016 A1	28.10.2010	CN 101036096 A0	12.09.2007
		CN 101036096 B	17.11.2010
		EP 1805572 A2	11.07.2007
		JP 2008-517400 A	22.05.2008
		JP 2008-517400 T	22.05.2008
		TW I314684A	11.09.2009
		US 2006-0085652 A1	20.04.2006
		US 7711965 B2	04.05.2010
		WO 2006-044710 A2	27.04.2006
		WO 2006-044710 A3	10.08.2006
		WO 2006-044710 A3	27.04.2006
US 2008-0222714 A1	11.09.2008	None	
US 7770789 B2	10.08.2010	CA 2688762 A1	27.11.2008
		EP 2156397 A1	24.02.2010
		US 2008-0283590 A1	20.11.2008
		US 2008-0283591 A1	20.11.2008
		US 2008-0283592 A1	20.11.2008
		US 2011-0125597 A1	26.05.2011
		US 7841523 B2	30.11.2010
		US 7891563 B2	22.02.2011
		WO 2008-144555 A1	27.11.2008

Form PCT/ISA/210 (patent family annex) (July 2009)

フロントページの続き

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

(74)代理人 100116894
弁理士 木村 秀二
(74)代理人 100130409
弁理士 下山 治
(72)発明者 ヴァスワニ, ラジ
アメリカ合衆国 カリフォルニア州 ９４０２８, ポートラ ヴァレー, トリニティ レーン １９０
(72)発明者 ヤン, ウィルソン チェン ユー
アメリカ合衆国 カリフォルニア州 ９５００８, キャンベル, マントン コート １６５１
(72)発明者 サイバート, クリスティーナ
アメリカ合衆国 カリフォルニア州 ９４０４３, マウンテン ヴュー, ジャクソン ストリート ８７５
(72)発明者 ボルヤード, ネルソン ブルース
アメリカ合衆国 カリフォルニア州 ９５０３５, ミルピタス, ペスカデロ コート ２７３
(72)発明者 ダム, ベンジャミン エヌ.
アメリカ合衆国 カリフォルニア州 ９４００２, ベルモント, スイート ビー, オールド カントリー ロード ７３１
(72)発明者 セントジョーンズ, マイケル シー.
アメリカ合衆国 メリーランド州 ２０８７４, ジャーマンタウン, ブロムフィールド ロード １３９３９