(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2020-201979
(P2020-201979A)
(43)公開日　令和2年12月17日(2020.12.17)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/57	(2013.01)	G06F	21/57	
G06F 21/62	(2013.01)	G06F	21/62	

審査請求 有　請求項の数 20　ＯＬ　（全 23 頁）

(21)出願番号　特願2020-140219 (P2020-140219)
(22)出願日　令和2年8月21日 (2020.8.21)
(62)分割の表示　特願2019-119791 (P2019-119791)の分割
原出願日　平成28年1月19日 (2016.1.19)
(31)優先権主張番号　62/105,685
(32)優先日　平成27年1月20日 (2015.1.20)
(33)優先権主張国・地域又は機関　米国 (US)
(31)優先権主張番号　14/857,775
(32)優先日　平成27年9月17日 (2015.9.17)
(33)優先権主張国・地域又は機関　米国 (US)

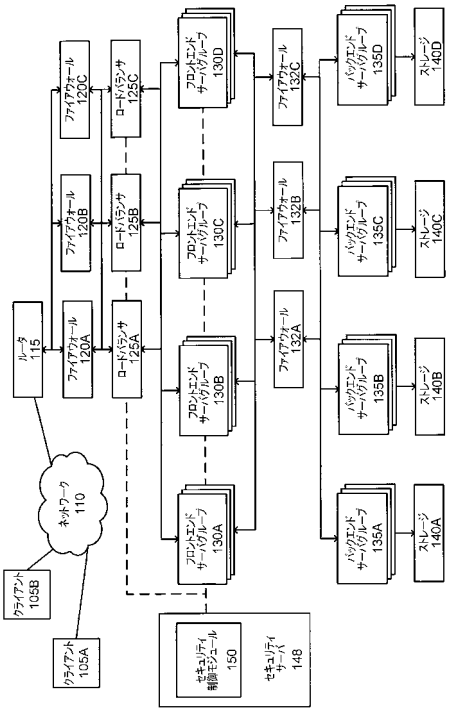
（特許庁注：以下のものは登録商標）

(71)出願人　517255773
サイエンプティブ　テクノロジーズ　インコーポレイテッド
アメリカ合衆国　９８２９０　ワシントン州　スノホミッシュ　シダー　アベニュー　１１０　スイート　１０３
(74)代理人　110001243
特許業務法人　谷・阿部特許事務所
(72)発明者　ロバート　パイク
アメリカ合衆国　９８０７７　ワシントン州　ウッディンビル　２２　ウェイ　ノー　スイースト　１８４３３　エンゾー　インコーポレイテッド内

最終頁に続く

(54)【発明の名称】ローリングセキュリティプラットフォーム

(57)【要約】
【課題】１または複数のサーバの第１のサーバグループおよび１または複数のサーバの第２のサーバグループなど、複数のサーバグループを含むシステムのためのローリングセキュリティの方法を提供する。
【解決手段】方法は、１または複数のサーバの第１のサーバグループの再構築を反復的に開始するステップを含む。方法は、また、１または複数のサーバの第２のサーバグループの再構築を反復的に開始するステップを含む。１または複数のサーバの第１のサーバグループの再構築は、１または複数のサーバの第２のサーバグループの再構築から時間的にずらされる。サーバは、物理サーバまたは仮想マシンであってよい。ローリングセキュリティは、ソフトウェアコンテナ、データセンタ内のコンピューティングデバイス、およびデータセンタ外のコンピューティングデバイスに適用されてもよい。
【選択図】図１Ａ



【特許請求の範囲】
【請求項１】
ローリングタイミング情報を生成するためのコンピュータによって実行される方法であって
第１のサーバグループ上で第１の複数のアプリケーションセッションを監視し、第２のサーバグループ上で第２の複数のアプリケーションセッションを監視するステップと、
前記第１の複数のセッションを監視することに基づいて、前記第１の複数のセッションの間の第１の複数の持続時間を判定し、前記第２の複数のセッションを監視することに基づいて、前記第２の複数のセッションの間の第２の複数の持続時間を判定するステップと、
前記第１の複数の持続時間に基づいて、前記第１のサーバグループに対する第１の再構築間隔を判定するステップと、
前記第２の複数の持続時間に基づいて、前記第２のサーバグループに対する第２の再構築間隔を判定するステップと、
前記第１の再構築間隔に基づいて、前記第１のサーバグループに対する再構築タイミングを示すローリングタイミング情報を生成し、前記第２の再構築間隔に基づいて、前記第２のサーバグループに対する再構築タイミングを示すローリングタイミング情報を生成するステップであって、前記第１のサーバグループおよび前記第２のサーバグループに対する前記再構築タイミングは、時間的にずらされる、ステップと、
前記ローリングタイミング情報に基づいて、前記第１のサーバグループを再構築させ、前記第２のサーバグループを再構築させるステップと、
を備えたことを特徴とする方法。
【請求項２】
前記第１のサーバグループに対する前記第１の再構築間隔を判定するステップは、
前記第１の複数のアプリケーションセッションの前記第１の複数の持続時間に基づいて、統計的尺度を計算することと、
前記統計的尺度に乗数を加えることによって、前記第１の再構築間隔を判定することと、
を含むことを特徴とする請求項１に記載の方法。
【請求項３】
前記統計的尺度は、平均持続時間および最大持続時間のうちの１つであることを特徴とする請求項２に記載の方法。
【請求項４】
前記第１のサーバグループを再構築させるステップは、前記第１のサーバグループに通常動作モードからシャットダウン準備モードに入らせることを含むことを特徴とする請求項１に記載の方法。
【請求項５】
前記ローリングタイミング情報を生成するステップは、前記通常動作モードの最大持続時間を生成することを含むことを特徴とする請求項４に記載の方法。
【請求項６】
前記第１のサーバグループにシャットダウン準備モードに入らせることは、１つまたは複数のロードバランサにシャットダウン準備開始コマンドを送信することを含み、前記シャットダウン準備開始コマンドは、前記第１のサーバグループの識別子を含むことを特徴とする請求項４に記載の方法。
【請求項７】
前記ローリングタイミング情報を生成するステップは、前記第１のサーバグループに対する第１のエントリを生成することを含み、前記第１のエントリは、通常動作の間の時間、シャットダウン準備モードの間の時間、および再構築モードの間の時間を含むことを特徴とする請求項１に記載の方法。
【請求項８】

前記第１のサーバグループを再構築させ、前記第２のサーバグループを再構築させるステップは、前記第２のサーバグループの再構築を開始する前に、前記第１のサーバグループが再構築されたと判定することを含むことを特徴とする請求項１に記載の方法。
【請求項９】
命令を記憶した非一時的コンピュータ可読媒体であって、前記命令は、１つまたは複数のプロセッサによって実行されるとき、
第１のサーバグループ上で第１の複数のアプリケーションセッションを監視し、第２のサーバグループ上で第２の複数のアプリケーションセッションを監視することと、
前記第１の複数のセッションを監視することに基づいて、前記第１の複数のセッションの間の第１の複数の持続時間を判定し、前記第２の複数のセッションを監視することに基づいて、前記第２の複数のセッションの間の第２の複数の持続時間を判定することと、
前記第１の複数の持続時間に基づいて、前記第１のサーバグループに対する第１の再構築間隔を判定することと、
前記第２の複数の持続時間に基づいて、前記第２のサーバグループに対する第２の再構築間隔を判定することと、
前記第１の再構築間隔に基づいて、前記第１のサーバグループに対する再構築タイミングを示すローリングタイミング情報を生成し、前記第２の再構築間隔に基づいて、前記第２のサーバグループに対する再構築タイミングを示すローリングタイミング情報を生成することであって、前記第１のサーバグループおよび前記第２のサーバグループに対する前記再構築タイミングは、時間的にずらされる、ことと、
前記ローリングタイミング情報に基づいて、前記第１のサーバグループを再構築させ、前記第２のサーバグループを再構築させることと、
を前記１つまたは複数のプロセッサに行わせることを特徴とする非一時的コンピュータ可読媒体。
【請求項１０】
前記第１のサーバグループに対する前記第１の再構築間隔を判定することを前記１つまたは複数のプロセッサに行わせる前記命令は、
前記第１の複数のアプリケーションセッションの前記第１の複数の持続時間に基づいて、統計的尺度を計算することと、
前記統計的尺度に乗数を加えることによって、前記第１の再構築間隔を判定することと、
を前記１つまたは複数のプロセッサに行わせる命令を更に含むことを特徴とする請求項９に記載の非一時的コンピュータ可読媒体。
【請求項１１】
前記統計的尺度は、平均持続時間および最大持続時間のうちの１つであることを特徴とする請求項１０に記載の非一時的コンピュータ可読媒体。
【請求項１２】
前記第１のサーバグループを再構築させることを前記１つまたは複数のプロセッサに行わせる前記命令は、前記第１のサーバグループに通常動作モードからシャットダウン準備モードに入らせることを前記１つまたは複数のプロセッサに行わせる命令を更に含むことを特徴とする請求項９に記載の非一時的コンピュータ可読媒体。
【請求項１３】
前記ローリングタイミング情報を生成することを前記１つまたは複数のプロセッサに行わせる前記命令は、前記通常動作モードの最大持続時間を生成することを前記１つまたは複数のプロセッサに行わせる命令を更に含むことを特徴とする請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項１４】
前記第１のサーバグループにシャットダウン準備モードに入らせることを前記１つまたは複数のプロセッサに行わせる前記命令は、１つまたは複数のロードバランサにシャットダウン準備開始コマンドを送信することを前記１つまたは複数のプロセッサに行わせる命

令を更に含み、前記シャットダウン準備開始コマンドは、前記第１のサーバグループの識別子を含むことを特徴とする請求項１２に記載の非一時的コンピュータ可読媒体。
【請求項１５】
前記ローリングタイミング情報を生成することを前記１つまたは複数のプロセッサに行わせる前記命令は、前記第１のサーバグループに対する第１のエントリを生成することを前記１つまたは複数のプロセッサに行わせる命令を更に含み、前記第１のエントリは、通常動作の間の時間、シャットダウン準備モードの間の時間、および再構築モードの間の時間を含むことを特徴とする請求項９に記載の非一時的コンピュータ可読媒体。
【請求項１６】
前記第１のサーバグループを再構築させ、前記第２のサーバグループを再構築させることを前記１つまたは複数のプロセッサに行わせる前記命令は、前記第２のサーバグループの再構築を開始する前に、前記第１のサーバグループが再構築されたと判定することを前記１つまたは複数のプロセッサに行わせる命令を更に含むことを特徴とする請求項９に記載の非一時的コンピュータ可読媒体。
【請求項１７】
ローリングタイミング情報を生成するシステムであって、
サーバの第１のサーバグループと、
サーバの第２のサーバグループであって、前記第１のサーバグループおよび第２のサーバグループにおける各々のサーバは、オペレーティングシステムおよびユーザセッションをサポートするアプリケーションを含む、サーバの第２のサーバグループと、 命令を記憶した非一時的コンピュータ可読媒体であって、前記命令は、１つまたは複数のプロセッサによって実行されるとき、
第１のサーバグループ上で第１の複数のアプリケーションセッションを監視し、第２のサーバグループ上で第２の複数のアプリケーションセッションを監視することと、
前記第１の複数のセッションを監視することに基づいて、前記第１の複数のセッションの間の第１の複数の持続時間を判定し、前記第２の複数のセッションを監視することに基づいて、前記第２の複数のセッションの間の第２の複数の持続時間を判定することと、
前記第１の複数の持続時間に基づいて、前記第１のサーバグループに対する第１の再構築間隔を判定することと、
前記第２の複数の持続時間に基づいて、前記第２のサーバグループに対する第２の再構築間隔を判定することと、
前記第１の再構築間隔に基づいて、前記第１のサーバグループに対する再構築タイミングを示すローリングタイミング情報を生成し、前記第２の再構築間隔に基づいて、前記第２のサーバグループに対する再構築タイミングを示すローリングタイミング情報を生成することであって、前記第１のサーバグループおよび前記第２のサーバグループに対する前記再構築タイミングは、時間的にずらされる、ことと、
前記ローリングタイミング情報に基づいて、前記第１のサーバグループを再構築させ、前記第２のサーバグループを再構築させることと、
を前記１つまたは複数のプロセッサに行わせる、非一時的コンピュータ可読媒体と、
を備えたことを特徴とするシステム。
【請求項１８】
前記第１のサーバグループに対する前記第１の再構築間隔を判定することを前記１つまたは複数のプロセッサに行わせる前記命令は、
前記第１の複数のアプリケーションセッションの前記第１の複数の持続時間に基づいて、統計的尺度を計算することと、
前記統計的尺度に乗数を加えることによって、前記第１の再構築間隔を判定することと、
を前記１つまたは複数のプロセッサに行わせることを特徴とする請求項１７に記載のシステム。
【請求項１９】

前記統計的尺度は、平均持続時間および最大持続時間のうちの１つであることを特徴とする請求項１８に記載のシステム。
【請求項２０】
前記第１のサーバグループを再構築させることを前記１つまたは複数のプロセッサに行わせる前記命令は、前記第１のサーバグループに通常動作モードからシャットダウン準備モードに入らせることを前記１つまたは複数のプロセッサに行わせることを特徴とする請求項１７に記載のシステム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、リソースへの無権限アクセスに対するコンピュータセキュリティに関し、より詳細には、向上されたセキュリティのためのローリングセキュリティプラットフォームに関する。
【０００２】
本出願は、２０１５年１月２０日に出願された米国仮特許出願第６２／１０５６８５号、および２０１５年９月１７日に出願された米国特許出願第１４／８５７７７５号に基づく優先権を主張し、それらの内容は、全体的に参照することによって組み込まれる。
【背景技術】
【０００３】
ネットワーク通信においては、ファイアウォールおよび侵入検知防御システムを含む、多くの形態のソフトウェアおよびハードウェアセキュリティが、存在する。
【発明の概要】
【発明が解決しようとする課題】
【０００４】
しかし、それらはどれも、ルールが正確に適用されない場合、それらが無権限アクセスに機会を開くことができるという、１つの核心的な問題に関して欠点がある。今日のオペレーティングシステムおよびアプリケーションも、インターネットにさらされた場合、アプリケーションをホストするサーバへのリモートアクセスを可能にすることができる、多くのバグを有する。
【課題を解決するための手段】
【０００５】
本開示の実施形態は、ハッカーに対抗するオンラインセキュリティを提供する合理的な方法およびシステムを含む。一実施形態においては、ローリングセキュリティのためのシステムが、開示される。システムは、サーバの第１のサーバグループと、サーバの第２のサーバグループとを備える。第１のサーバグループおよび第２のサーバグループ内の各サーバは、オペレーティングシステムと、ユーザセッションをサポートするアプリケーションとを含む、ソフトウェアを含む。非一時的コンピュータ可読媒体は、少なくとも１つのプロセッサによって実行されたときに、少なくとも１つのプロセッサに、第１のサーバグループのための再構築タイミングおよび第２のサーバグループのための再構築タイミングを示すローリングタイミング情報にアクセスすることを行わせる命令を記憶する。第１のサーバグループのための再構築タイミングは、第２のサーバグループの再構築タイミングから時間的にずらされる。命令は、また、プロセッサに、第１のサーバグループのための再構築タイミングに従って、サーバの第１のサーバグループの各サーバのソフトウェアの再構築を定期的に開始することを行わせる。命令は、また、プロセッサに、第２のサーバグループのための第２の再構築タイミングに従って、サーバの第２のサーバグループ内の各サーバのソフトウェアの再構築を定期的に開始することを行わせる。サーバの第１のサーバグループの再構築は、サーバの第２のサーバグループの再構築から時間的にずらされる。
【０００６】
一実施形態においては、複数のサーバグループを含むシステムのためのローリングセキ

ュリティの方法が、開示される。方法は、１または複数のサーバの第１のサーバグループの再構築を反復的に開始するステップを含む。方法は、また、１または複数のサーバの第２のサーバグループの再構築を反復的に開始するステップを含む。１または複数のサーバの第１のサーバグループの再構築は、１または複数のサーバの第２のサーバグループの再構築から時間的にずらされる。

【０００７】

一実施形態においては、第１および第２のグループ内のサーバの各々は、定期的など、反復的に再構築されるソフトウェアを含む。再構築されるソフトウェアは、オペレーティングシステム、アプリケーション、および他のソフトウェアを含むことができる。一実施形態においては、第１および第２のサーバグループ内のサーバの各々は、それぞれのファームウェアを含む。第１のサーバグループの再構築を反復的に開始することは、第１のサーバグループの各サーバ内のそれぞれのファームウェアの再構築を開始することを含む。第２のサーバグループの再構築を反復的に開始することは、第２のサーバグループの各サーバ内のそれぞれのファームウェアの再構築を開始することを含む。

【０００８】

一実施形態においては、第１および第２のサーバグループ内のサーバの各々は、それぞれのパスワードを含む。方法は、また、第１のサーバグループを再構築するときに、第１のサーバグループ内の各サーバのパスワード変更を反復的に開始するステップと、第２のサーバグループを再構築するときに、第２のサーバグループ内の各サーバのパスワード変更を反復的に開始するステップとを含む。

【０００９】

一実施形態においては、方法は、第１のサーバグループおよび第２のサーバグループを再構築するための再構築タイミングを示すローリングタイミング情報にアクセスするステップを含む。第１のサーバグループおよび第２のサーバグループは、ローリングタイミング情報に従って、反復的に再構築される。加えて、第１のサーバグループおよび第２のサーバグループ内のサーバの各々は、それぞれのアプリケーションをホストし、アプリケーションのためのユーザセッションをサポートし、方法は、それぞれのアプリケーションのためのユーザセッションの持続時間を監視するステップと、ユーザセッションの監視された持続時間に基づいて、第１のサーバグループおよび第２のサーバグループのための再構築タイミングを示すローリングタイミング情報を生成するステップとをさらに含む。

【００１０】

一実施形態においては、反復的に再構築される第１のサーバグループおよび第２のサーバグループ内のサーバは、物理サーバである。一実施形態においては、反復的に再構築される第１のサーバグループおよび第２のサーバグループ内のサーバは、仮想マシンである。

【００１１】

一実施形態においては、システムは、第１のサーバグループと第２のサーバグループとの間のネットワークトラフィックを平衡させるための、１または複数のロードバランサをさらに備える。方法は、また、第１のサーバグループの各再構築に先立って、第１のサーバグループのシャットダウン準備モードを反復的に開始するステップであって、ロードバランサは、第１のサーバグループがシャットダウン準備モードにある間、第１のサーバグループのアプリケーションとの新しいセッションが確立されることを防止する、ステップを含む。方法は、また、第２のサーバグループの各再構築に先立って、第２のサーバグループのシャットダウン準備モードを反復的に開始するステップであって、ロードバランサは、第２のサーバグループがシャットダウン準備モードにある間、第２のサーバグループのアプリケーションとの新しいセッションが確立されることを防止する、ステップを含む。

【００１２】

他の実施形態は、命令を記憶する非一時的コンピュータ可読媒体を含む。命令は、少なくとも１つのプロセッサによって実行可能であって、少なくとも１つのプロセッサに、ロ

ーリングセキュリティの方法を実行することを行わせる。他の実施形態は、ローリングセキュリティを、ソフトウェアコンテナに適用してよい。他の実施形態は、ローリングセキュリティを、データセンタ内のネットワーク接続されたコンピューティングデバイス、またはデータセンタ外のコンピューティングデバイスに適用してよい。

【図面の簡単な説明】

【００１３】

【図１Ａ】実施形態による、ローリングセキュリティのためのセキュリティ保護されたデータセンタのコンポーネントを有する、ネットワーク接続された通信システムのブロック図である。

【図１Ｂ】別の実施形態による、ローリングセキュリティのためのセキュリティ保護されたデータセンタのコンポーネントを有する、ネットワーク接続された通信システムのブロック図である。

【図１Ｃ】さらなる実施形態による、ローリングセキュリティのためのセキュリティ保護されたデータセンタのコンポーネントを有する、ネットワーク接続された通信システムのブロック図である。

【図２Ａ】実施形態による、図１Ａのフロントエンドサーバのブロック図である。

【図２Ｂ】実施形態による、仮想マシンを有するサーバのブロック図である。

【図２Ｃ】実施形態による、ソフトウェアコンテナを有するサーバのブロック図である。

【図３】実施形態による、ローリングサーバグループの図である。

【図４】実施形態による、セキュリティ制御モジュールのブロック図である。

【図５】実施形態による、ローリングセキュリティの方法についてのフローチャートである。

【図６】コンピューティングデバイスのハードウェアアーキテクチャを示す図である。

【発明を実施するための形態】

【００１４】

例が添付の図において説明されている、本開示のいくつかの実施形態に対する言及を、これから詳細に行う。使用可能であればどこででも、類似または同様の参照番号を、図において使用してよく、類似または同様の機能を指し示してよいことに留意されたい。図は、もっぱら説明の目的で、本開示の実施形態を描写している。当業者は、本明細書で説明される開示の本質または得られる便益から逸脱することなく、本明細書で説明される構造および方法の代替的実施形態が使用されてよいことを、以下の説明から容易に認識するであろう。

【００１５】

本開示は、ハッカーがバックエンドデータセットにアクセスすることを防御する、および任意のデータセットへの進行中のアクセスを防御する、システムプラットフォームに関する。より詳細には、本発明は、より高度なセキュリティソリューションのために、無権限リソースへのエスカレートするアクセスを止めることができる。

【００１６】

一実施形態においては、データセンタのためのセキュリティプラットフォームが、開示される。セキュリティプラットフォームは、時間の特定の測定基準に基づいたローリング方式で、自らを継続的および反復的に再構築する。ローリングセキュリティは、時間の短い期間のうちにサーバソフトウェアを自動的に置き換えて、オペレーティングシステムまたはアプリケーションにおいて見出されるいかなる構成またはホールも完全に一掃し、それによって、いかなるサーバへのアクセスも時間の短い期間に制限する。例えば、この時間は、１０秒ほどの短さ、または数時間ほどの長さとすることができる。一実施形態においては、標準的な構成は、再構築どうしの間をデフォルトで１０分とする。ハッカーは、ハッキングを知り、バックエンドにおけるアーキテクチャがどのようなものかを解明し、サーバに不正侵入し、さらなるアクセスのためにルートキットをインストールしようと試みるのに、そのようなほんの短い間しか有さない。したがって、サーバの置き換えが非常に頻繁に生じるので、ハッカーがハッキングを完了しようと試みることは、無意味である

。ハッカーが、パスワードまたは公開鍵基盤（ＰＫＩ）鍵を発見する時までには、オペレーティングシステム（ＯＳ）は、新しいパスワードおよび鍵とともに、置き換えられようとしている。

【００１７】

システムは、限定することなく、時間の短い期間内に、ＯＳ、アプリケーション、コンテンツ、データ、およびキャッシュを含む、デバイス上のソフトウェアスタック全体を置き換えることができる。システムは、本物のユーザおよびハッカーユーザの両方を途切れなく管理するために、ネットワーク内の複数のデバイス（例えば、ロードバランサ、ファイアウォールなど）と完全に統合されることができる。他の実施形態においては、セッションカウント、接続カウント、一意的センサトリガ、および他のセキュリティ表示が、再構築をトリガするために使用されることができる。他の実施形態においては、セッションは、絶縁された環境内に動的に含められることができ、セッションの時間は、絶縁された環境内において実行されているハッキングを調べるために、拡張されることができる。

【００１８】

システムは、動的にアプリケーション平均セッションカウンタおよび時間を調べ、再構築タイミングを動的に調整することができ、またはより厳格なセキュリティポリシを可能にするために、手動構成を有することができる。システムは、任意の単一のセッションがフロントエンドアプリケーションおよびデータセットに接続されることができる時間を制限して、いかなるシステムに対する長期間リモートアクセスを防止する。

【００１９】

図１Ａは、実施形態による、ローリングセキュリティのためのセキュリティ保護されたデータセンタのコンポーネントを有する、ネットワーク接続された通信システムのブロック図である。システムは、いくつかのクライアントデバイス１０５と、ネットワーク１１０と、ルータ１１５と、フロントエンドファイアウォール１２０Ａ～Ｃと、ロードバランサ１２５Ａ～Ｃと、フロントエンドサーバグループ１３０Ａ～Ｄと、バックエンドファイアウォールまたはロードバランサ１３２Ａ～Ｃと、バックエンドサーバグループ１３５Ａ～Ｄと、ストレージシステム１４０Ａ～Ｄと、セキュリティサーバ１４８とを含む。ルータ、ファイアウォール１２０、ロードバランサ１２５、フロントエンドサーバ１３０、ファイアウォール１３２、バックエンドサーバ１３５、およびストレージシステム１４０は、データセンタのコンポーネントであってよい。図１Ａにおいては、限られた数のデバイスだけが示されているが、他の実施形態においては、より多数のデバイス（例えば、５つ以上のフロントエンドサーバグループ）が、存在してよい。

【００２０】

クライアントデバイス１０５は、とりわけ、スマートフォン、タブレットコンピュータ、ラップトップコンピュータ、およびデスクトップコンピュータなどの、コンピューティングデバイスとすることができる。ユーザは、タッチスクリーンまたはマウスおよびキーボードなどの、インターフェースを通して、クライアントデバイス１０５のソフトウェアと対話する。クライアントデバイス１０５は、ユーザによって制御されて、フロントエンドサーバグループ１３０によってホストされる様々なアプリケーションとのアプリケーションセッションおよび接続を確立する。

【００２１】

ルータ１１５は、ネットワーク１１０とデータセンタ内の残りのコンポーネントとの間のネットワークトラフィックをルーティングする。フロントエンドファイアウォール１２０は、適用されるルールセットを使用して、着信および発信ネットワークトラフィックを制御する、ハードウェアベースのファイアウォールデバイスである。ファイアウォールは、データセンタの内部ネットワークと外部ネットワーク１１０との間に、障壁を確立する。ロードバランサ１２５は、多数のフロントエンドサーバグループ１３０の間にネットワークトラフィックを分散させる。ロードバランサは、いずれか１つの特定のフロントエンドサーバグループ１３０にかかる負担を減らすことによって、アプリケーションの能力および信頼性を向上させる。

【００２２】
各フロントエンドサーバグループ１３０は、いくつかの物理フロントエンドサーバを含む。サーバは、１または複数のプロセッサを含むことができるサーバクラスのコンピューティングデバイスであり、オペレーティングシステムを実行する。サーバは、いくつかのソフトウェアアプリケーションをホストする。クライアント１０５は、フロントエンドサーバによってホストされるアプリケーションとのネットワーキング接続およびアプリケーションセッションを確立することができる。セキュリティ目的で、各サーバグループは、ある時間が満了した後、ローリングされること（すなわち、サーバグループを再構築することによって）ができ、サーバグループは、時間差方式で、ローリングされることができる。サーバグループが、ローリングされたときでさえも、アプリケーションが、依然として、クライアントデバイス１０５に利用可能であるように、同じアプリケーションのコピーが、複数のサーバグループ１３０によってホストされる。一実施形態においては、全部で９つのフロントエンドサーバグループ１３０が、存在し、各フロントエンドサーバグループ１３０は、数千のフロントエンドサーバを含む。
【００２３】
バックエンドファイアウォール１３２は、適用されるルールセットを使用して、フロントエンドサーバグループ１３０とバックエンドサーバグループ１３５との間のトラフィックを制御する、ハードウェアベースのファイアウォールデバイスまたは仮想ファイアウォールである。各バックエンドサーバグループ１３５は、１または複数のバックエンドサーバを含む。バックエンドサーバは、ストレージシステム１４０内に記憶されたデータへのアクセスを可能にする。バックエンドサーバは、フロントエンドサーバグループ１３０によってホストされるアプリケーションによって要求されると、ストレージシステム１４０にデータを記憶し、ストレージシステム１４０からデータを取り出す。バックエンドサーバの例は、ＳＱＬデータベースへのアクセスを提供するＳＱＬサーバである。
【００２４】
セキュリティサーバ１４８は、フロントエンドサーバグループ１３０のローリング動作を調整する、セキュリティ制御モジュール１５０を含む。具体的には、セキュリティ制御モジュール１５０は、定期的な時間差のある間隔で、フロントエンドサーバグループ１３０の再構築を反復的に開始する。サーバの再構築は、サーバのハードドライブイメージを公知の好ましい置き換えイメージで置き換えることによって、オペレーティングシステム（ＯＳ）、アプリケーション、コンテンツ、およびキャッシュを含む、サーバのソフトウェアスタック全体を置き換えることを含むことができる。サーバの再構築は、サーバのファームウェアを置き換えることを含むこともできる。再構築は、これらの動作に加えて、他の動作を含んでもよい。再構築どうしの間の時間は、１０秒ほどの短さ、または数時間ほどの長さとすることができる。他の実施形態においては、標準的な再構築時間は、デフォルトで１０分である。
【００２５】
定期的および頻繁にサーバを反復的に再構築することは、ハッカーにハッキングを短い時間（例えば、５秒未満）のうちに完了することを強いるが、応答時間およびアップロード時間は、通常、より長い時間を必要とするので、それは、ほぼ不可能である。例えば、ＤＮＳサーバの場合、ＤＮＳサーバは、新しいＯＳおよびＤＮＳデータベースキャッシュを用いて、１０秒おきに再構築されることができる。この状況においては、ハッカーは、プロトコルをハッキングし、キャッシュスプーフィングによって偽データをアップロードするための時間を有さない。ハッカーによってアップロードされたいずれの悪意あるコードも、また、排除される。サーバに結び付けられたあらゆるものが、置き換えられ、外部からリモートでＯＳに働きかけることを不可能にする。同時に、標準的なカスタマ要求のために必要とされるすべてのコンテンツは、正しく供給される。これは、今日のソフトウェアにおいて見出されるいかなるホールも完璧に解決する。
【００２６】
セキュリティ制御モジュール１５０は、また、各フロントエンドサーバグループ（例え

ば、１３０Ａ）の再構築を、他のフロントエンドサーバグループ（例えば、１３０Ｂ）に関して、時間的にずらすことによって、ローリングベースで再構築を開始する。各フロントエンドサーバグループ１３０は、サーバグループ１３０がいつオンラインになり、トラフィックに対するサービスを開始するかについての時間差手法を生成して、異なる時刻にユーザセッションに対するサービスを開始する。セッションがそこから開始し、終了するプロセスは、すべて、単一のサーバ、またはサーバのグループ１３０内で生じる。これは、グループ内における簡単なロードバランシングを可能にするばかりでなく、セッションの終了がグループ内で生じることも可能にする。サーバグループ１３０内のサーバは、それらのＯＳを同時に置き換えるが、その間に、他のサーバグループ１３０が、ちょうどオンラインになっており、新しいユーザセッションに対するサービスを行っている。サーバグループ１３０を再構築するためのタイムフレームは、サーバグループ１３０内のアプリケーションの機能性に応じて、多様なものとすることができる。

【００２７】

セキュリティ制御モジュール１５０は、また、ロードバランサ１２５と通信し、ロードバランサ１２５が、新しいＯＳインストールのためにシャットダウンされているサーバグループを知り、それによって、ロードバランサ１２５が、オンラインであるサーバグループ１３０だけにネットワークトラフィックを分配することを可能にするようにする。セキュリティ制御モジュール１５０は、サーバグループ１３０がいつシャットダウンのための準備を開始するかを示すための情報を、ロードバランサ１２５に送信することができる。それに応答して、ロードバランサ１２５は、サーバグループ１３０をオフラインにし、サーバグループ１３０との新しい接続が確立されることを防止する。サーバグループ１３０が、ひとたび再構築されると、セキュリティ制御モジュール１５０は、サーバグループ１３０が新しい接続を受け入れる準備を整えたことを示す情報を、ロードバランサ１２５に送信することができる。それに応答して、ロードバランサ１２５は、サーバグループ１３０をオンラインに戻し、サーバグループ１３０との新しい接続が確立されることを可能にする。

【００２８】

セキュリティ制御モジュール１５０は、サーバグループ１３０を再構築するとき、サーバグループ１３０のパスワードを変更することもできる。頻繁なパスワード変更は、サーバ上でパスワード攻撃を行うことを不可能にする。

【００２９】

セキュリティ制御モジュール１５０は、ソフトウェア、ハードウェアとして、またはハードウェアおよびソフトウェアの組み合わせとして、実施されることができる。他の実施形態においては、セキュリティ制御モジュール１５０は、セキュリティサーバ１４８以外のデータセンタの１または複数のコンポーネントにわたって分散させることができる。

【００３０】

図１Ｂは、別の実施形態による、ローリングセキュリティのためのセキュリティ保護されたデータセンタのコンポーネントを有する、ネットワーク接続された通信システムのブロック図である。図１Ｂは、今度は、フロントエンド仮想マシン（ＶＭ）グループ１６０と、ハイパーバイザ１９０とを含むということを除いて、図１Ａに類似している。各ＶＭグループ１６０は、１または複数のＶＭを含む。ＶＭは、コンピュータサーバのエミュレーションなど、コンピュータシステムのエミュレーションである。各ＶＭは、自らの仮想ディスクに接続されてよい。ＶＭは、本明細書では、仮想サーバと呼ばれることがある。

【００３１】

ハイパーバイザ１９０は、ＶＭグループ１６０を生成し、管理する。各ハイパーバイザ１９０は、自らの物理フロントエンドサーバ１５９上に配置されてよく、同じ物理フロントエンドサーバ上に配置されたＶＭのグループ１６０を制御してもよい。例えば、ハイパーバイザ１９０ＡおよびＶＭグループ１６０Ａは、単一の物理サーバ１５９Ａ上に配置される。

【００３２】

この実施形態においては、セキュリティ制御モジュール１５０は、フロントエンドＶＭグループ１６０（すなわち、仮想サーバグループ）の再構築を定期的に開始することによって、ネットワーク接続された通信システムにローリングセキュリティを提供する。ＶＭグループ１６０が再構築されているときであってさえも、アプリケーションが常にオンラインであるように、複数のＶＭグループ１６０が同じアプリケーションのコピーをホストする。ＶＭの再構築は、ＶＭの状態を元の公知の好ましい状態に回復することを含むことができる。再構築は、以下でより詳細に説明される。

【００３３】

それ以外は、セキュリティ制御モジュール１５０の動作は、図１Ａに関連して説明されたものと同じである。一実施形態においては、ネットワーク接続された通信システムは、定期的な時間差ベースで再構築される、物理サーバグループおよび仮想サーバグループの両方を含んでよい。

【００３４】

図１Ｃは、さらなる実施形態による、ローリングセキュリティのためのセキュリティ保護されたデータセンタのコンポーネントを有する、ネットワーク接続された通信システムのブロック図である。図１Ｃは、今度は、サーバ１５９上に配置された、コンテナグループ９６０と、コンテナエンジン９９０とを含むということを除いて、図１Ｂに類似している。

【００３５】

各コンテナグループ９６０は、オペレーティングシステムレベルの仮想化のために使用される、１または複数のソフトウェアコンテナを含む。ソフトウェアコンテナは、単一のパッケージ内にバンドリングされた、アプリケーション、それの従属物、ライブラリ、およびバイナリを含む。ソフトウェアコンテナは、同じサーバ１５９上の他のソフトウェアコンテナと、オペレーティングシステム（図示されず）を共用する。ソフトウェアコンテナは、オペレーションシステムのカーネル内でインスタンス化され、アプリケーションのインスタンスを仮想化する。ソフトウェアコンテナは、リソースのブロック内に入れられるアプリケーションまたはサービスの迅速な生成を可能にする。コンテナは、コアＯＳからのコアライブラリファイルを共用することができるので、コンテナの配備は、高速である。ソフトウェアコンテナは、コンテナエンジン９９０によって管理される。一実施形態においては、ソフトウェアコンテナ９６０は、ＤＯＣＫＥＲコンテナであり、またはオープンコンテナプロジェクト規格に準拠している。

【００３６】

この実施形態においては、セキュリティ制御モジュール１５０は、コンテナグループ９６０の再構築をローリングベースで定期的に開始することによって、ネットワーク接続された通信システムにローリングセキュリティを提供する。コンテナグループ９６０のいくつかが再構築されているときであってさえも、アプリケーションが常にオンラインであるように、同じアプリケーションのコピーが、複数のコンテナグループ９６０内に含まれる。コンテナは、コンテナを公知の好ましい状態に回復することによって、再構築されることができる。再構築は、以下でより詳細に説明される。それ以外は、セキュリティ制御モジュール１５０の動作は、図１Ａおよび図１Ｂに関連して説明されたものと同じである。一実施形態においては、コンテナの再構築は、物理サーバおよび仮想マシンを再構築するよりも効率的であることができる。例えば、コンテナは、～３０秒で回復され、配備されることができる。対照的に、サーバおよび仮想マシンの再構築は、はるかに長くかかることができる。コンテナのローリングは、物理サーバおよびＶＭのローリングよりも容易であることができるが、それらは、共用されるコアＯＳファイルの使用に起因する、より高いリスクを有する。ハイパーバイザアーキテクチャも、リスクを有するが、ＯＳは、各ＶＭに占有されるので、そのことが、コンテナプラットフォームと比較して、リスクを低減させる。物理サーバをローリングするときは、ハッカーは、サーバハイジャックを行うのに、サーバのＢＩＯＳレベル制御を有する必要があり、またはハッカーは、リモート管理ツールアクセスを必要とするので、リスクは、やはりより低い。

【００３７】
本明細書の説明は、主として物理サーバまたは仮想マシンのローリングに重点が置かれることがある。しかしながら、本明細書で説明されるローリングセキュリティの原理は、物理サーバ、仮想マシン、またはコンテナのローリングに適用可能である。
【００３８】
図２Ａは、実施形態による、フロントエンドサーバ２００のブロック図である。フロントエンドサーバ２００は、図１Ａのフロントエンドサーバグループ１３０に属するフロントエンドサーバを表してよい。フロントエンドサーバ２００は、いくつかのソフトウェアアプリケーション２５０Ａ～Ｃと、ＯＳ１５２と、ファームウェア１５４と、フロントエンドセキュリティモジュール１５６とを含む。ＯＳ１５２の例は、とりわけ、ＬＩＮＵＸおよびＭＩＣＲＯＳＯＦＴ　ＷＩＮＤＯＷＳ（登録商標）を含む。アプリケーション２５０は、ＯＳ１５２の上で実行される。ファームウェア１５４は、プログラム可能なメモリチップ内に記憶されたソフトウェアを含む。
【００３９】
クライアントデバイス１０５は、アプリケーション２５０とのネットワーキング接続Ｃ１～Ｃ６を確立することができる。接続は、クライアントデバイス１０５におけるソケットとサーバ２００との間の双方向通信チャネルとして使用される。接続は、ハンドシェイクプロセスを使用して、ある時点において確立され、その後、後の時点において終了される。接続は、プロトコルによって定義されるいくつかの状態を含んでよい。接続の例は、開放型システム間相互接続（ＯＳＩ）モデルのトランスポートレイヤの伝送制御プロトコル（ＴＣＰ）接続である。
【００４０】
クライアントデバイス１０５は、また、接続Ｃ１～Ｃ６上において、アプリケーション２５０とのアプリケーションユーザセッションＳ１～Ｓ６を確立する。ユーザセッションは、与えられたアプリケーションのための２つ以上の通信エンティティ間の対話的な情報交換である。ユーザセッションは、ある時点において確立され、その後、後の時点において終了される。ユーザセッションの間、１または複数のメッセージが、セッションのために確立された接続上において、各方向に送信されてよい。一実施形態においては、アプリケーションセッションは、トランスポートレイヤの上位に存在するＯＳＩセッションレイヤのセッションである。
【００４１】
一例においては、クレジットカード認証セッション（例えば、Ｓ１、Ｓ２）は、ユーザが、クライアントデバイス１０５Ａにおいて、クレジットカードをリーダに通したときに、開始されることができ、クライアントデバイス１０５Ａは、クレジットカード支払いアプリケーション２５０Ａとの接続およびセッションを確立する。クレジットカード支払いアプリケーション２５０Ａは、クライアントデバイス１０５Ａと通信して、クライアントデバイス１０５Ａからクレジットカード番号および請求金額を獲得する。クレジットカード支払いアプリケーション２５０は、その後、バックエンドサーバ１３５を介して、データベース１４０にアクセスし、クレジットカード番号が、支払いを処理するのに十分な信用を有するかどうかを決定する。クレジットカード支払いアプリケーション２５０は、その後、はい／いいえ応答をクライアントデバイス１０５Ａに提供する。接続およびセッションは、その後、応答をクライアントデバイス１０５Ａに提供した後、終了される。
【００４２】
別の例においては、ウェブフォームセッション（例えば、Ｓ３、Ｓ４）は、ユーザが、クライアント１０５Ｂにおいて、ＵＲＬをブラウザに入力したときに、開始されることができる。クライアントデバイス１０５Ｂは、ウェブサイト２５０Ｂとのセッションを確立する。クライアントデバイス１０５Ｂは、ウェブサイト２５０Ｂとのセッションを確立する。サーバ２００は、複数のセッションを処理していてよい。サーバ２００は、セッション毎に時間カウンタを開始する。ユーザは、セッションが閉じる前に、フォームに記入するためのｘの時間を有する。ウェブフォームデータを記入するのにかかる時間のため、異

なるサーバが、最初のセッションからのフォーム提出を処理してよい。

【００４３】

さらなる例においては、オンラインバンキングセッション（例えば、Ｓ５、Ｓ６）は、ユーザが、クライアントデバイス１０５Ｂにおいて、モバイルバンキングアプリケーションを開いたときに、開始されることができ、クライアントデバイス１０５Ｂは、オンラインバンキングアプリケーション２５０Ｃとの接続およびセッションを確立する。オンラインバンキングアプリケーション２５０Ｃは、クライアントデバイス１０５Ｂと通信して、クライアントデバイス１０５Ｂから認証情報を獲得する。ひとたび認証されると、クライアントデバイス１０５Ｂは、勘定残高を要求し、預金のための小切手のコピーをアップロードし、他のバンキング要求を行うことができる。バンキングアプリケーション２５０Ｃは、バックエンドサーバ１３５を介して、データベース１４０内に記憶された勘定情報にアクセスして、これらの要求を処理することができる。接続およびセッションは、セッションの最後に、最終的に終了される。

【００４４】

フロントエンドセキュリティモジュール１５６は、セキュリティ制御モジュール１５０と通信して、ローリングセキュリティを実施するためのセキュリティ情報を送信および受信することができる。セキュリティモジュール１５６は、フロントエンドサーバ２００の再構築を開始するためのコマンドを受信することができる。コマンドは、再構築のためのテンプレートとして使用されるべき、公知の好ましいマスタソフトウェアイメージである、ゴールデンイメージの名前を含むことができる。セキュリティモジュール１５６は、その後、コマンドに従って、ＯＳ１５２、アプリケーション、および／またはファームウェア１５４の置き換えなどを行うことによって、フロントエンドサーバ２００を再構築する。ＯＳ１５２、アプリケーション２５０、および／またはファームウェア１５４は、サーバ２００上の既存のソフトウェアをゴールデンイメージで上書きすること、サーバ２００上の既存のソフトウェアを削除し、ゴールデンイメージから新しいソフトウェアをサーバ２００上にコピーすることなどによって、置き換えられることができる。ゴールデンイメージは、サーバ２００内のディスク上にローカルに、またはネットワーク上の他の場所に記憶されることができる。

【００４５】

変化する再構築時刻を用いる異なる再構築技法が、使用されることができる。一実施形態においては、単一のゴールデンイメージが、複数のサーバ２００を再構築するために、使用されることができる。ゴールデンイメージからのデータが、フロントエンドサーバ２００上にコピーされることができ、その後、ＯＳ１５２またはアプリケーション２５０を構成するために、後処理構成が、各フロントエンドサーバ２００上で実行される。例えば、サーバのための一意名およびサーバのためのＩＰアドレスを確立するために、異なるスクリプトが、各フロントエンドサーバ２００上で実行されてよい。一実施形態においては、各フロントエンドサーバ２００に固有および一意の複数のゴールデンイメージが、存在してよい。ゴールデンイメージからのデータは、後処理構成の必要なしに、それぞれのサーバ上にコピーされることができ、そのことが、短縮再構築時刻を短縮する。

【００４６】

別の実施形態においては、データ差分技法が、フロントエンドサーバ２００を再構築するために使用される。具体的には、フロントエンドサーバ２００のソフトウェアのデータブロックまたはファイルは、ゴールデンイメージのデータブロックまたはファイルと比較されることができる。異なるデータブロックまたはファイルだけが、ゴールデンイメージから回復される。ブロックまたはファイルベースの差分を利用することによって、ローカルディスク、リモートＳＡＮディスク、ＮＡＳディスクを介した、事前構成されたＯＳおよびアプリケーション構成の迅速な配備が、可能である。他の再構築技法が可能であってよく、依然として、本開示の範囲内に包含されることに留意されたい。

【００４７】

一実施形態においては、再構築が標準的な予期された構成であること、および状態が良

好な知られた構成であることを検証するために、様々なハッシュもしくは暗号化モデル、またはブロック状態比較が、再構築されたソフトウェアイメージに適用されることができる。例えば、再構築ソフトウェアは、再構築が予期された通りに実行されたことを検証するために、ハッシュ値を計算され、その後、ゴールデンイメージのハッシュと比較されることができる。

【００４８】

一実施形態においては、フロントエンドセキュリティモジュール１５６は、改ざんに対する防御のために、再構築の間、フロントエンドサーバ２００をロックダウンセキュリティモードに置く。再構築の間、フロントエンドセキュリティモジュール１５６は、セキュリティサーバ１４８のセキュリティ制御モジュール１５０との通信以外の、何らかのポートへのいかなるトラフィックもブロックするパーミッションを有する、それの内部ファイアウォールアクセス制御リスト（ＡＣＬ）を設定してよい。ＡＣＬは、ネットワークポートを使用することを許可された特定のエンティティを伴う、ネットワークポートのリストとすることができる。他のサードパーティアプリケーションは、コンプライアンスの状態の検証のために、必要に応じて、アクセスを与えられてもよい。

【００４９】

セキュリティモジュール１５６は、また、ＯＳ１５２のパスワードを変更するためのコマンドを受信し、その後、コマンドに従って、パスワードを置き換えることができる。一実施形態においては、セキュリティ情報は、インテリジェントなプラットフォーム管理インターフェース（ＩＰＭＩ）を介して伝達される。

【００５０】

図２Ｂは、実施形態による、ＶＭ２０４を用いるフロントエンドサーバ２０２のブロック図である。フロントエンドサーバ２０２は、図１Ｂに属するフロントエンドサーバ１５９を表してよい。フロントエンドサーバ２０２は、いくつかのＶＭ２０４と、ハイパーバイザ２０８と、ＯＳ１５２と、フロントエンドセキュリティモジュール１５６Ａとを含む。各ＶＭは、仮想化ＯＳ２０６と、アプリケーション２５０とを含む。

【００５１】

フロントエンドセキュリティモジュール１５６Ａは、フロントエンドモジュール１５６に類似しているが、今度は、ＶＭ２０４を再構築するためのコマンドに応答して、ＶＭを再構築する。ＶＭ２０４の再構築は、図２Ａに関して説明された再構築に類似しており、やはり、ＶＭ２０４を生成するために、ＶＭ２０４のゴールデンイメージを利用すること、データ差分を利用すること、および／またはＶＭ２０４を再構築した後、再構築検証を実行することができる。

【００５２】

図２Ｃは、実施形態による、コンテナ２９２を用いるフロントエンドサーバ２９０のブロック図である。フロントエンドサーバ２９０は、図１Ｃに属するフロントエンドサーバ１５９を表してよい。フロントエンドサーバ２９０は、いくつかのコンテナ２９２と、コンテナエンジン２９４と、ＯＳ１５２と、フロントエンドセキュリティモジュール１５６Ｂとを含む。各コンテナは、仮想化アプリケーション２５０を含む。

【００５３】

フロントエンドセキュリティモジュール１５６Ｂは、フロントエンドモジュール１５６に類似しているが、今度は、コンテナ２９２を再構築するためのコマンドに応答して、ローリングベースでコンテナ２９２を再構築する。コンテナ２９２の再構築は、図２Ａに関して説明された再構築に類似しており、やはり、コンテナ２９２を生成するために、コンテナ２９２のゴールデンイメージを利用すること、データ差分を利用すること、および／またはコンテナ２９２を再構築した後、再構築検証を実行することができる。

【００５４】

図３は、実施形態による、ローリングサーバグループの図である。４つのサーバグループ１３０Ａ～１３０Ｄのローリング動作が、図３に示されている。他の実施形態においては、図３に示されるローリング動作は、ＶＭグループ１６０およびソフトウェアコンテナ

グループ９６０のローリングにも適用可能である。
【００５５】
各サーバグループ１３０は、異なるローリングセキュリティモード、すなわち、（１）通常動作モード、（２）シャットダウン準備モード、および（３）再構築モードで動作する。通常動作モードの間、サーバグループ１３０は、新しいユーザセッションおよび接続を受け入れ、それらにサービスを行う。シャットダウン準備モードの間、サーバグループ１３０は、新しいセッションおよび接続を受け入れない。既存のセッションおよび接続は、終了することを許可される。一実施形態においては、ロードバランサ１２５は、特定のサーバグループ１３０が、シャットダウン準備モードに入ろうとしており、新しいセッションおよび接続を受け入れていないことを通知されてよい。ロードバランサ１２５は、新しいセッションおよび接続が行われることができる実行可能なサーバグループ１３０から、サーバグループ１３０を削除することによって応答する。再構築モードの間、サーバグループ１３０は、サービスから除外され、サーバグループ１３０のソフトウェアを置き換えることによって再構築される。モードは、６０秒おきなど、定期的に反復される。
【００５６】
サーバグループ１３０は、異なるサーバグループの再構築が異なる時刻に開始されるように、ローリング方式で動作させられる。例えば、サーバグループ１３０Ａは、１：００：５０に再構築され、サーバグループ１３０Ｂは、１：０１：００に再構築され、サーバグループ１３０Ｃは、１：０１：１０に再構築され、サーバグループ１３０Ｄは、１：０１：２０に再構築される。再構築時刻は、互いに１０秒だけずらされている。再構築時刻をずらすことは、サーバグループ１３０によってホストされるアプリケーションのために、新しい接続およびユーザセッションを受け入れるための、サービス中であり利用可能なサーバグループ１３０が、常に少なくとも１つ存在することを保証する。言い換えると、通常動作モードにあるサーバグループ１３０が、常に少なくとも１つ存在する。
【００５７】
一実施形態においては、ハッカーの存在を示すセキュリティ条件がトリガされた場合、サーバグループ１３０についてのシャットダウン準備モードは、延期されてよい。セキュリティ条件は、例えば、セッションが、疑わしいＩＰと関連付けられる場合、またはあまりにも長くセッションを開いたままにしてある場合、トリガされてよい。その状況においては、セキュリティ制御モジュール１５０は、ハッカーのアクションをより良く理解するために、セッションの高度な分析、セッションの封じ込め、およびセッションの記録を実施してよい。あるいは、セキュリティ条件がトリガされた場合、セキュリティモジュール１５０は、ハッキングされたセッションが検出されたハッキングされたサーバを、サーバグループ１３０から取り除いてよい。その後、サーバグループ１３０のローリングが中断されないように、新しいサーバが、ハッキングされたサーバの代わりに、ホットスワップされる。
【００５８】
図４は、実施形態による、セキュリティ制御モジュール１３０のブロック図である。セキュリティ制御モジュール１３０は、通信モジュール４０５と、ローリングタイミングモジュール４１０と、ローリング制御モジュール４１５と、パスワード変更モジュール４２０とを含む。他の実施形態においては、セキュリティ制御モジュール１３０は、図４に示されていない追加のモジュールを有してよい。
【００５９】
ローリングタイミングモジュール４１０は、（本明細書では一括して「ローリングエンティティグループ」と呼ばれる）物理サーバグループ１３０、ＶＭグループ１６０、またはコンテナグループ９６０が、通常動作モード、シャットダウン準備モード、および再構築モードなどの異なるモードにいつ入るべきかについてのずらされたタイミングを示す、ローリングタイミング情報を維持する。タイミング情報は、ローリングエンティティグループと、各ローリングエンティティグループがいつ異なるモードに入るべきかについての特定の時刻とのリストを含む、タイミングスケジュールの形式を取ってよい。以下の表は

、タイミングスケジュールの例である。

【００６０】

【表１】

ｻｰﾊﾞｸﾞﾙｰﾌﾟ	モード：通常動作	モード：シャットダウン準備	モード：再構築
1	1:00:00 1:01:00 …	1:00:30 1:01:30 …	1:00:50 1:01:50 …
2	1:00:10 1:01:10 …	1:00:40 1:01:40 ..	1:01:00 1:02:00 …
3	1:00:20 1:01:20 …	1:00:50 1:01:50 ..	1:01:10 1:02:10 …
4	1:00:30 1:01:30 …	1:01:00 1:02:00 …	1:01:20 1:02:20 …

【００６１】

表の第１列は、サーバグループを識別する。第２列は、サーバグループがいつ通常動作モードに入るべきかについての開始時刻を識別する。第３列は、サーバグループがいつシャットダウン準備モードに入るべきかを識別する。第４列は、再構築プロセスがいつ開始すべきかを識別する。

【００６２】

他の実施形態においては、タイミング情報は、タイミングスケジュールの代わりに、最大時間限界の形式を取ってよい。例えば、タイミング情報は、ローリングエンティティグループの最大稼働時間、通常動作モードの最大持続時間、シャットダウン準備モードの最大持続時間、および／または再構築モードの最大持続時間を含んでよい。タイミング情報は、ローリングエンティティグループどうしの間のずらされた遅れの長さを記述する情報を含んでもよい。

【００６３】

ローリングモードのためのローリングタイミング情報は、ユーザによって手動で設定されてよい。別の実施形態においては、タイミング情報は、サーバ上における以前のアプリケーションセッションまたは接続の持続時間を監視し、監視された持続時間を含むアプリケーションプロファイルを生成することによって、機械学習されてよい。持続時間の統計的尺度（例えば、平均持続時間、最大持続時間）が、監視された持続時間から決定されることができる。統計的尺度は、その後、各ローリングモードの最大持続時間を決定するために、乗数倍される（例えば、８×、１０×）。その結果、再構築どうしの間の時間は、ローリングエンティティグループが再構築される前に、新しいユーザセッションおよび接続が確立され、完了するのに十分なものとなる。例えば、ユーザセッションが、６秒の長

さになる傾向にある場合、この値は、８倍されて、定期的な再構築どうしの間に４８秒の持続時間をもたらしてよく、それは、セッション持続時間よりもはるかに長い。

【００６４】

ローリング制御モジュール４１５は、上で説明されたローリングタイミングスケジュールまたは最大時間限界などのローリングタイミング情報に従って、ローリングエンティティグループのローリング動作を制御する。ローリング制御モジュール４１５は、ローリングタイミング情報を使用して、サーバグループがいるべきローリングモードを決定する。ローリング制御モジュール４１５は、その後、図３に示されたようなローリング方式でローリングエンティティグループを動作させる制御コマンドを、通信モジュール４０５を介して、ロードバランサ１２５およびローリングエンティティグループに送信する。ローリングエンティティグループが、制御されたずらされた時刻にローリングされることを保証するために、各ローリングエンティティグループに対するコマンドは、他のローリングエンティティグループに対するコマンドに関して、時間的にずらされてよい。

【００６５】

通常動作モードを開始するために、ローリング制御モジュール４１５は、通常動作開始コマンドをロードバランサ１２５に送信してよい。コマンドは、特定のローリングエンティティグループを識別し、そのローリングエンティティグループのための通常動作モードが開始すべきであることも示す。ロードバランサ１２５は、識別されたローリングエンティティグループとのセッションおよび接続が確立されることを可能にすることによって、コマンドに応答する。一実施形態においては、通常動作開始コマンドは、通常動作が開始される適切なローリングエンティティグループに送信されてもよい。

【００６６】

シャットダウン準備モードを開始するために、ローリング制御モジュール４１５は、シャットダウン準備開始コマンドをロードバランサ１２５に送信してよい。コマンドは、特定のローリングエンティティグループを識別し、そのローリングエンティティグループのためのシャットダウン準備モードが開始すべきであることも示す。ロードバランサ１２５は、識別されたローリングエンティティグループとのいかなる新しいセッションおよび接続も確立されないようにすることによって、コマンドに応答する。ローリングエンティティグループの既存のセッションおよび接続は、完了することを許可される。一実施形態においては、シャットダウン準備開始コマンドは、ローリングエンティティグループのための適切なサーバに送信されてもよい。

【００６７】

再構築を開始するために、ローリング制御モジュール４１５は、再構築開始コマンドを、再構築されるべきローリングエンティティグループと関連付けられた適切なフロントエンドサーバに送信してよい。コマンドは、再構築のために使用されるべき、公知の好ましいソフトウェアイメージの名前を含むことができる。それに応じて、ローリングエンティティグループは、公知の好ましいソフトウェアイメージを用いて再構築されることができる。再構築がひとたび完了されると、ローリング制御モジュール４１５は、適切なフロントエンドサーバから再構築確認情報を受信してもよい。

【００６８】

加えて、再構築に先立って、ローリング制御モジュール４１５は、データを、ローリングエンティティグループから別個のストレージドライブにコピーすることができる。データの変更について監視し、他のサーバにわたる大域的な比較のための変更のインライン分析を行うために、機械学習が、使用されることができる。これは、エンティティがオンラインであった間に、ハッカーによってＯＳ、アプリケーション、またはファイルに対して行われた、すべての変更の理解を可能にする。再構築状態およびタイミングを学習する機械は、重要であるが、より高度な学習を可能にするための、ハッキングされた状況を制圧する再構築状態の遅れは、ローリング制御モジュール４１５を介して管理されるシステム制御の一部でもある。ローリング制御モジュール４１５は、ハッカーの能力を知り、新しい攻撃についてより多く知るための、より多くのデータの学習および収集を意図して、ハ

ッカーにサービスし続けるために、ローカルサーバグループ、ルータ１１５、およびファイアウォール１２０と通信することもできる。

【００６９】

パスワード変更モジュール４２０は、サーバグループ１３０のためのパスワード変更を開始する。パスワードは、とりわけ、ＯＳ、データベース、またはアプリケーションパスワードとすることができる。パスワードは、ローリングタイミング情報によって示されるように、再構築毎に変更されることができ、または特定のタイムスタンプで（すなわち、ある間隔で）再構築されることができる。パスワード変更の頻度は、ローリングエンティティグループ再構築の頻度と同じであること、または異なることができる。一実施形態においては、パスワード変更モジュール４２０は、新しいパスワードを生成し、そのパスワードをサーバに送信することによって、パスワード変更を開始することができる。別の実施形態においては、パスワード変更モジュール４２０は、パスワード変更コマンドをサーバに送信することによって、パスワード変更を開始することができる。サーバは、その後、コマンドに応答して、新しいパスワードを生成する。数々のアルゴリズムのうちのいずれかが、パスワードを生成するために使用されることができる。一実施形態においては、タイムスタンプは、パスワードを生成するために使用される要素の１つである。

【００７０】

通信モジュール４０５は、ネットワーク接続された通信システムにおいて、サーバ、ロードバランサ１２５、および他のデバイスと通信する。通信モジュール４０５は、ローリングする時間差方式でローリングエンティティグループを動作させるローリングセキュリティコマンドを送信してよい。通信モジュール４０５は、ローリングエンティティグループにおいてパスワード変更を開始するコマンドを送信してよい。通信モジュール４０５は、ネットワーク接続された通信システムにおいて、デバイスから他のタイプの情報を受信してもよい。

【００７１】

図５は、実施形態による、ローリングセキュリティの方法についてのフローチャートである。ステップ５０５において、ローリングエンティティグループによってホストされるアプリケーションのための以前の接続またはユーザセッションが、監視される。持続時間が、アプリケーションプロファイル内に記憶される。十分な情報がひとたび収集されると、異なるローリングエンティティグループがいつ再構築されるべきかについてのずらされたタイミングなど、ローリングエンティティグループの異なるローリングセキュリティモードについてのずらされたタイミングを記述する、ローリングタイミング情報を生成するために、以前の接続またはユーザセッションについての持続時間が、使用される。

【００７２】

ステップ５１０において、セキュリティ制御モジュール１５０は、ローリングタイミング情報によって指定されるタイミングで、第１のローリングエンティティグループの通常動作を開始する。ステップ５１２において、セキュリティ制御モジュール１５０は、ローリングタイミング情報によって指定されるタイミングで、ローリングエンティティグループのシャットダウン準備モードを開始する。ステップ５１４において、セキュリティ制御モジュール１５０は、ローリングタイミング情報によって指定されるタイミングで、第１のローリングエンティティグループの再構築を開始する。加えて、セキュリティ制御モジュール１５０は、同時に、第１のローリングエンティティグループのパスワード変更を開始する。ステップ５１０～ステップ５１４は、定期的な間隔などで、継続的に反復する。

【００７３】

ステップ５２０において、セキュリティ制御モジュール１５０は、ローリングタイミング情報によって指定されるタイミングで、第２のローリングエンティティグループの通常動作を開始する。ステップ５２２において、セキュリティ制御モジュール１５０は、ローリングタイミング情報によって指定されるタイミングで、第２のローリングエンティティグループのシャットダウン準備モードを開始する。ステップ５２４において、セキュリティ制御モジュール１５０は、ローリングタイミング情報によって指定されるタイミングで

、第２のローリングエンティティグループの再構築を開始する。加えて、セキュリティ制御モジュール１５０は、同時に、第２のローリングエンティティグループのパスワード変更を開始する。ステップ５２０～ステップ５２４は、定期的な間隔などで、継続的に反復する。

【００７４】

他のローリングエンティティグループが、ステップ５１０～ステップ５１４およびステップ５２０～ステップ５２４と類似の方式で、制御されてもよい。加えて、各ローリングエンティティグループについて、再構築、通常動作モード、およびシャットダウン準備モードの開始は、他のローリングエンティティグループに関して、時間的にずらされる。セキュリティモードの時間差は、図３に示されるローリングセキュリティをもたらす。

【００７５】

図６は、一実施形態による、ファイアウォール１２０、ルータ１１５、ロードバランサ１２５、クライアントデバイス１０５、フロントエンドサーバ１３０もしくは１５９、バックエンドサーバ１３５、またはセキュリティサーバ１４８などの、コンピューティングデバイスのハードウェアアーキテクチャを示している。一実施形態においては、コンピューティングデバイスは、バス６０１を通して互いにデータおよび制御信号を交換する、プロセッサ６０２、メモリ６０３、ストレージモジュール６０４、入力モジュール（例えば、キーボードおよびマウスなど）６０６、ディスプレイモジュール６０７、ならびに通信インターフェース６０５などのコンポーネントを含む、コンピュータである。ストレージモジュール６０４は、１または複数の非一時的コンピュータ可読記憶媒体（例えば、ハードディスクまたはソリッドステートドライブ）として実施され、本明細書で説明されるローリングセキュリティ機能を実施するために、メモリ６０３と連携して、プロセッサ６０２によって実行されるソフトウェア命令６４０（例えば、モジュール）を記憶する。オペレーティングシステムソフトウェアおよび他のアプリケーションソフトウェアは、プロセッサ６０２上で動作するために、ストレージモジュール６０４内に記憶されてもよい。

【００７６】

本明細書で説明されるローリングセキュリティは、フロントエンドサーバ１３０、仮想マシン１６０、およびコンテナ９６０だけに限定されない。他の実施形態においては、ローリングセキュリティは、ファイアウォール１２０、ロードバランサ１２５、スイッチ、バックエンドサーバ１３５、およびバックエンドストレージ１４０などの、データセンタ内のコンピューティングシステムの他のグループを定期的に再構築するために使用されることができる。加えて、本明細書で説明されるモジュールの機能は、単一のモジュール内に組み合わされてよく、または追加のモジュール間で分散されてよい。

【００７７】

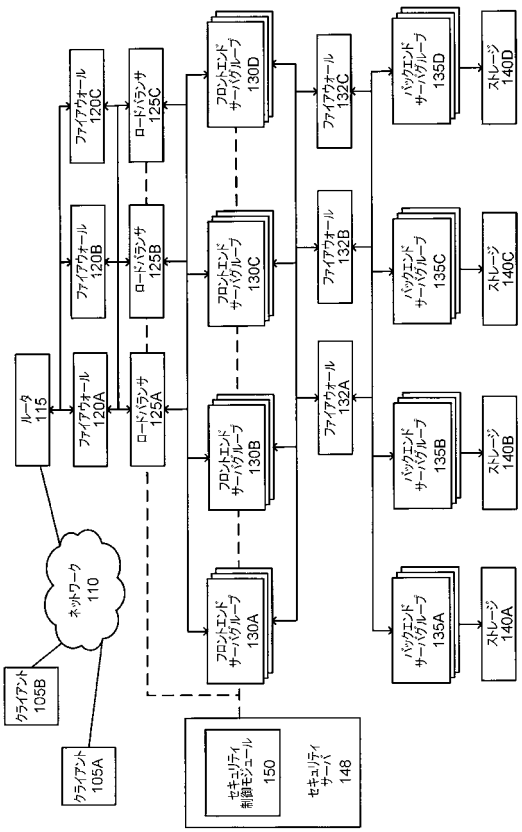
他の実施形態においては、本明細書で説明されるローリングセキュリティは、一般的なソフトウェア機能性を提供する、データセンタ外のコンピューティングシステムの他のグループに適用されてよい。コンピューティングシステムは、デスクトップ、ラップトップ、ｉパッド、ｉフォン、ならびに乗物（自動車、列車、飛行機）内のコンピューティングシステム、および発電所、発電機内のコンピューティングシステムなどとすることができる。飛行機の例においては、飛行機は、いくつかの並列フライト制御システムを含んでよく、それらの各々は、飛行機に対するフライト制御を提供することができる。時間差ベースのフライト制御システムのローリングは、少なくとも１つのフライト制御システムが常にオンラインであることを保証しながら、フライト制御システムがハッキングされることを防御することができる。

【００７８】

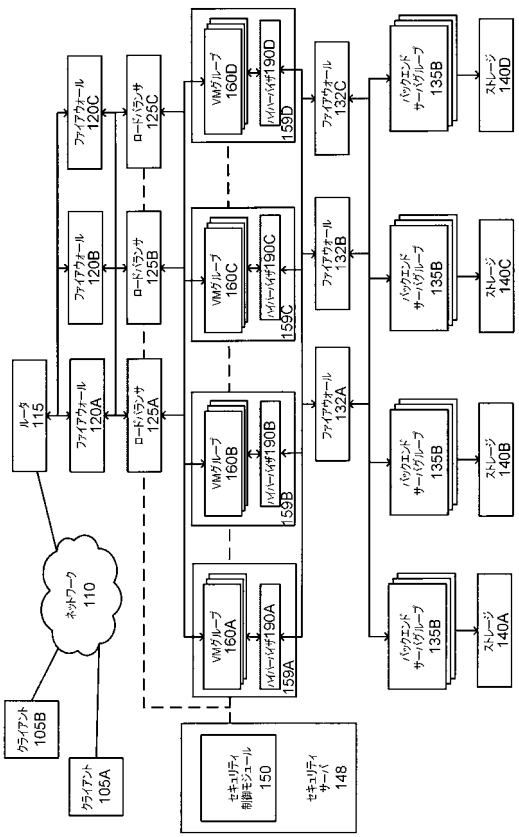
本開示を読むことで、当業者は、ローリングセキュリティのためのさらなる追加の代替的設計を理解することができる。したがって、本開示の特定の実施形態および適用が示され、説明されたが、本開示は、本明細書で開示された通りの構成およびコンポーネントに限定されないことが理解されるべきである。当業者に明らかであり得る様々な修正、変化、および変形が、添付の特許請求の範囲において定義される本開示の主旨および範囲から

逸脱することなく、本明細書の本開示の方法および装置の配置、動作、および細部に施されてよい。

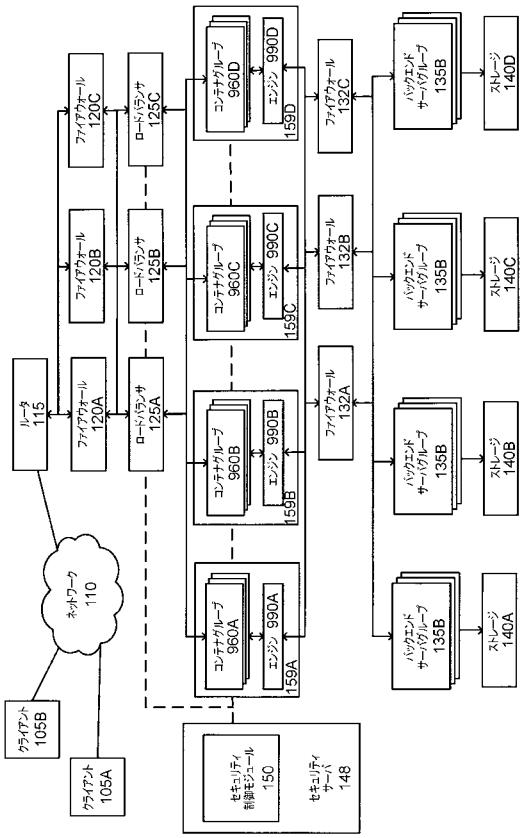
【図１Ａ】



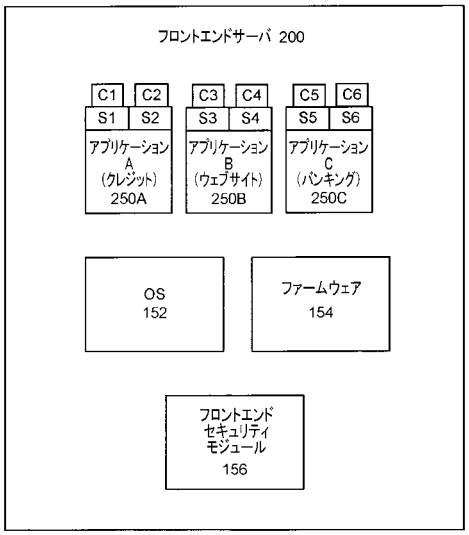
【図１Ｂ】



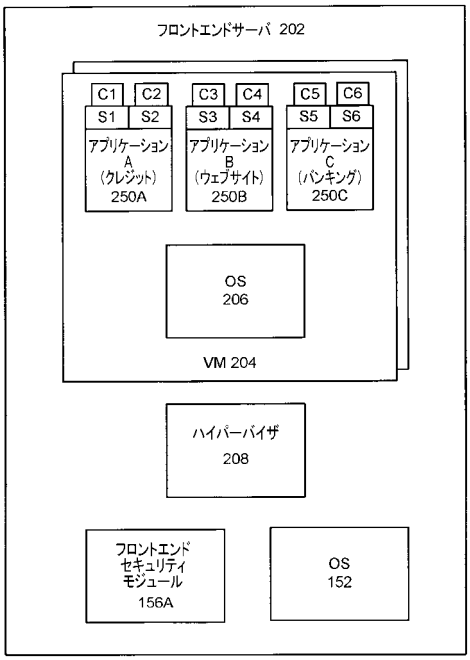
【図１Ｃ】



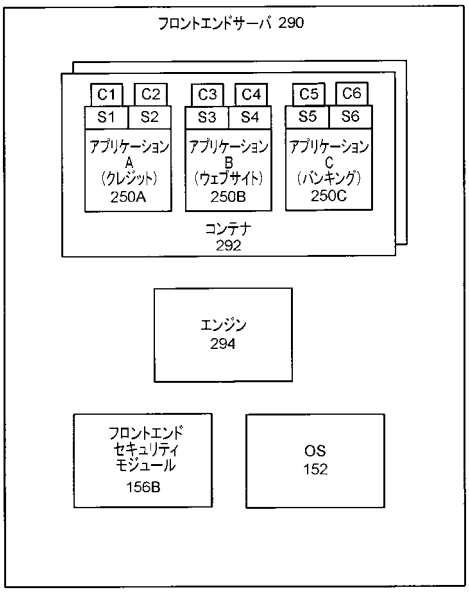
【図２Ａ】



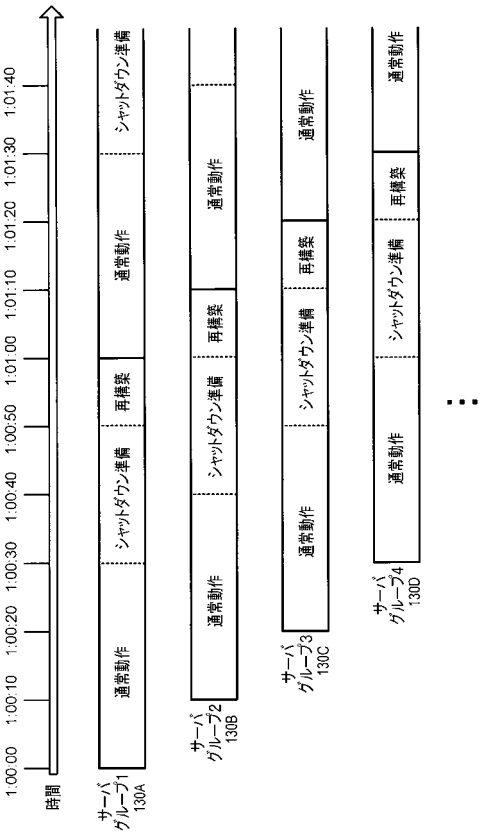
【図２Ｂ】



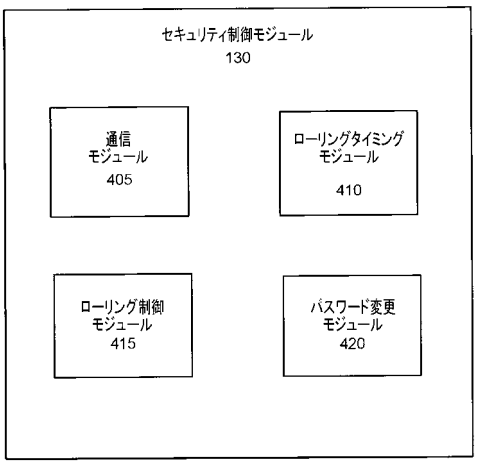
【図２Ｃ】



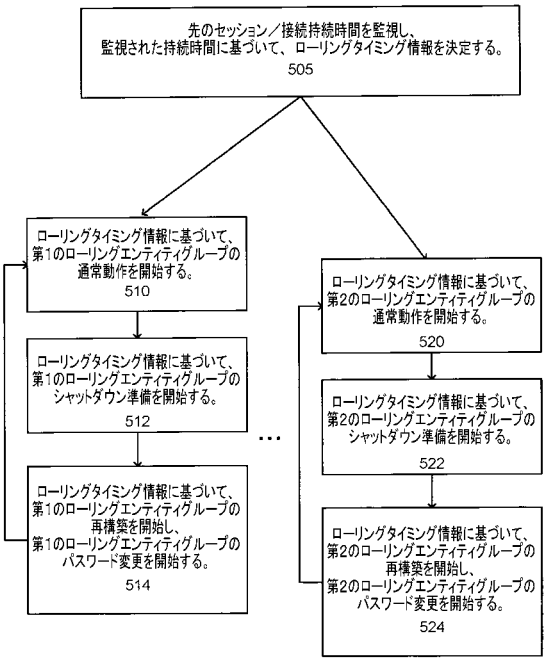
【図３】


1:00:00
1:00:10
1:00:20
1:00:30
1:00:40
1:00:50
1:01:00
1:01:10
1:01:20
1:01:30
1:01:40
時間
サーバグループ1 130A
通常動作
シャットダウン準備
再構築
通常動作
サーバグループ2 130B
通常動作
シャットダウン準備
再構築
通常動作
サーバグループ3 130C
通常動作
シャットダウン準備
再構築
通常動作
サーバグループ4 130D
通常動作
シャットダウン準備
再構築
通常動作
...

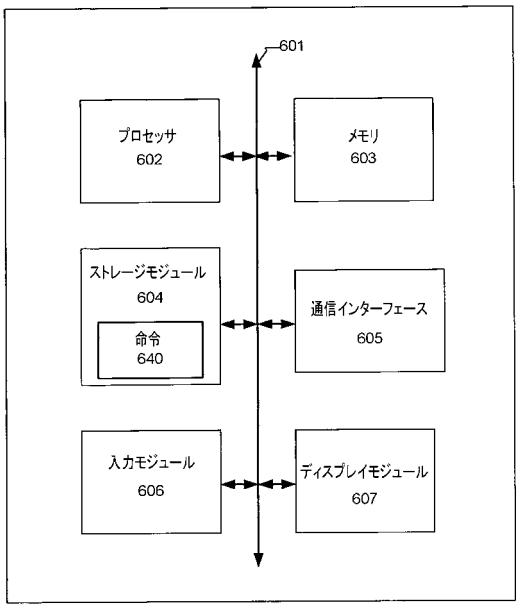
【図４】


セキュリティ制御モジュール
130
通信
モジュール
405
ローリングタイミング
モジュール
410
ローリング制御
モジュール
415
パスワード変更
モジュール
420

【図５】


先のセッション／接続持続時間を監視し、
監視された持続時間に基づいて、ローリングタイミング情報を決定する。
505
ローリングタイミング情報に基づいて、
第1のローリングエンティティグループの
通常動作を開始する。
510
ローリングタイミング情報に基づいて、
第1のローリングエンティティグループの
シャットダウン準備を開始する。
512
ローリングタイミング情報に基づいて、
第1のローリングエンティティグループの
再構築を開始し、
第1のローリングエンティティグループの
パスワード変更を開始する。
514
...
ローリングタイミング情報に基づいて、
第2のローリングエンティティグループの
通常動作を開始する。
520
ローリングタイミング情報に基づいて、
第2のローリングエンティティグループの
シャットダウン準備を開始する。
522
ローリングタイミング情報に基づいて、
第2のローリングエンティティグループの
再構築を開始し、
第2のローリングエンティティグループの
パスワード変更を開始する。
524

【図６】


601
プロセッサ
602
メモリ
603
ストレージモジュール
604
命令
640
通信インターフェース
605
入力モジュール
606
ディスプレイモジュール
607

フロントページの続き

１．Ｌｉｎｕｘ