(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6530495号
(P6530495)
(45)発行日　令和1年6月12日(2019.6.12)　(24)登録日　令和1年5月24日(2019.5.24)

(51)Int.Cl.　F I
G06F 21/55 (2013.01)　G06F 21/55
G06F 21/12 (2013.01)　G06F 21/12　３１０

請求項の数 16　(全 22 頁)

(21)出願番号　特願2017-539368 (P2017-539368)
(86)(22)出願日　平成28年1月19日 (2016.1.19)
(65)公表番号　特表2018-503197 (P2018-503197A)
(43)公表日　平成30年2月1日 (2018.2.1)
(86)国際出願番号　PCT/US2016/013942
(87)国際公開番号　WO2016/118517
(87)国際公開日　平成28年7月28日 (2016.7.28)
審査請求日　平成31年1月21日 (2019.1.21)
(31)優先権主張番号　14/827,230
(32)優先日　平成27年8月14日 (2015.8.14)
(33)優先権主張国　米国 (US)
(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　米国 (US)

早期審査対象出願

(73)特許権者　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　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
(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

審査官　宮司　卓佳

最終頁に続く

(54)【発明の名称】セッションセキュリティ分割およびアプリケーションプロファイラ

(57)【特許請求の範囲】
【請求項１】
リソースへの不正アクセスに対してセキュアにするためのコンピュータ実施方法であって、
第１のアプリケーションに対応する複数のアプリケーションセッションの持続時間をモニタして、セッション持続時間データを生成することと、
前記セッション持続時間データに基づいて、前記第１のアプリケーションに関するセキュリティをセキュリティ階層に分割する第１の複数のセキュリティタイムリミットを決定することと、
第１のクライアントと前記第１のアプリケーションとの間で確立された第１のアプリケーションセッションを検出することと、
前記第１のクライアントと前記第１のアプリケーションとの間で確立された前記第１のアプリケーションセッションの持続時間をモニタすることと、
前記第１のアプリケーションセッションの前記持続時間が前記第１の複数のセキュリティタイムリミットのセキュリティタイムリミットに到達したことに応答して、前記第１のアプリケーションセッションに対して１つまたは複数の第１のセキュリティアクションを実行することと、
前記第１のアプリケーションセッションの前記持続時間が前記第１の複数のセキュリティタイムリミットの別のセキュリティタイムリミットに到達したことに応答して、前記第１のアプリケーションセッションに対して１つまたは複数の第２のセキュリティアクショ

ンを実行することと
を含み、
前記第１のセキュリティアクションまたは前記第２のセキュリティアクションのうちの１つは、前記第１のアプリケーションセッションを第１のホストデバイスから第２のホストデバイスに移動させることによって、前記第１のアプリケーションセッションを前記第１のホストデバイスに関連付けられた他のアプリケーションセッションから分離することを含む、
方法。
【請求項２】
第２のクライアントと前記第１のホストデバイスの第２のアプリケーションとの間で確立された第２のアプリケーションセッションを検出することであって、前記第２のアプリケーションは、前記アプリケーションに関するセキュリティをセキュリティ階層に分割する第２の複数のセキュリティタイムリミットと関連付けられる、ことと、
前記第２のクライアントと前記第２のアプリケーションとの間で確立された前記第２のアプリケーションセッションの持続時間をモニタすることと、
前記第２のアプリケーションセッションの前記持続時間が前記第２の複数のセキュリティタイムリミットのセキュリティタイムリミットに到達したことに応答して、前記第２のアプリケーションセッションに対して前記１つまたは複数の第１のセキュリティアクションを実行することと、
前記第２のアプリケーションセッションの前記持続時間が前記第２の複数のセキュリティタイムリミットの別のセキュリティタイムリミットに到達したことに応答して、前記第２のアプリケーションセッションに対して前記１つまたは複数の第２のセキュリティアクションを実行することと
をさらに含む、請求項１に記載の方法。
【請求項３】
前記第１のセキュリティアクションまたは前記第２のセキュリティアクションのうちの１つは、ＩＰルックアップ、ディープパケットインスペクション、不正な形式のパケット検出、またはハニーポットセキュリティセンサの有効化のうちの１つを含む、請求項１に記載の方法。
【請求項４】
前記第１のセッションは、開放型システム間相互接続（ＯＳＩ）セッション層のセッションである、請求項１に記載の方法。
【請求項５】
リソースへの不正アクセスに対してセキュアにする命令を格納する非一時的なコンピュータ可読記憶媒体であって、前記命令は、少なくとも１つのプロセッサによって実行されると、
第１のアプリケーションに対応する複数のアプリケーションセッションの持続時間をモニタして、セッション持続時間データを生成することと、
前記セッション持続時間データに基づいて、前記第１のアプリケーションに関するセキュリティをセキュリティ階層に分割する第１の複数のセキュリティタイムリミットを決定することと、
第１のクライアントと前記第１のアプリケーションとの間で確立された第１のアプリケーションセッションを検出することと、
前記第１のクライアントと前記第１のアプリケーションとの間で確立された前記第１のアプリケーションセッションの持続時間をモニタすることと、
前記第１のアプリケーションセッションの前記持続時間が前記第１の複数のセキュリティタイムリミットのセキュリティタイムリミットに到達したことに応答して、前記第１のアプリケーションセッションに対して１つまたは複数の第１のセキュリティアクションを実行することと、
前記第１のアプリケーションセッションの前記持続時間が前記第１の複数のセキュリテ

ィタイムリミットの別のセキュリティタイムリミットに到達したことに応答して、前記第１のアプリケーションセッションに対して１つまたは複数の第２のセキュリティアクションを実行することと
の工程を前記少なくとも１つのプロセッサに行わせ、
前記第１のセキュリティアクションまたは前記第２のセキュリティアクションのうちの１つは、前記第１のアプリケーションセッションを第１のホストデバイスから第２のホストデバイスに移動させることによって、前記第１のアプリケーションセッションを前記第１のホストデバイスに関連付けられた他のアプリケーションセッションから分離することを含む、
非一時的なコンピュータ可読記憶媒体。

【請求項６】
前記工程は、
第２のクライアントと前記第１のホストデバイスの第２のアプリケーションとの間で確立された第２のアプリケーションセッションを検出することであって、前記第２のアプリケーションは、前記アプリケーションに関するセキュリティをセキュリティ階層に分割する第２の複数のセキュリティタイムリミットと関連付けられる、ことと、
前記第２のクライアントと前記第２のアプリケーションとの間で確立された前記第２のアプリケーションセッションの持続時間をモニタすることと、
前記第２のアプリケーションセッションの前記持続時間が前記第２の複数のセキュリティタイムリミットのセキュリティタイムリミットに到達したことに応答して、前記第２のアプリケーションセッションに対して前記１つまたは複数の第１のセキュリティアクションを実行することと、
前記第２のアプリケーションセッションの前記持続時間が前記第２の複数のセキュリティタイムリミットの別のセキュリティタイムリミットに到達したことに応答して、前記第２のアプリケーションセッションに対して前記１つまたは複数の第２のセキュリティアクションを実行することと
をさらに含む、請求項５に記載の非一時的なコンピュータ可読記憶媒体。

【請求項７】
前記第１のセキュリティアクションまたは前記第２のセキュリティアクションのうちの１つは、ＩＰルックアップ、ディープパケットインスペクション、不正な形式のパケット検出、またはハニーポットセキュリティセンサの有効化のうちの１つを含む、請求項５に記載の非一時的なコンピュータ可読記憶媒体。

【請求項８】
前記第１のセッションは、開放型システム間相互接続（ＯＳＩ）セッション層のセッションである、請求項５に記載の非一時的なコンピュータ可読記憶媒体。

【請求項９】
リソースへの不正アクセスに対してセキュアにするためのコンピュータ実施方法であって、
第１のアプリケーションに対応するセッションに対して確立された複数の接続の持続時間をモニタして、接続持続時間データを生成することと、
前記接続持続時間データに基づいて、前記第１のアプリケーションに関するセキュリティをセキュリティ階層に分割する第１の複数のセキュリティタイムリミットを決定することと、
第１のクライアントと前記第１のアプリケーションとの間の第１のセッションに対して確立された第１の接続を検出することと、
前記第１のクライアントと前記第１のアプリケーションとの間で確立された前記第１の接続の持続時間をモニタすることと、
前記第１の接続の前記持続時間が前記第１のアプリケーションに関連付けられた前記第１の複数のセキュリティタイムリミットのセキュリティタイムリミットに到達したことに応答して、前記第１の接続に対して１つまたは複数の第１のセキュリティアクションを実

行することと、
前記第１の接続の前記持続時間が前記第１の複数のセキュリティタイムリミットの別のセキュリティタイムリミットに到達したことに応答して、前記第１の接続に対して１つまたは複数の第２のセキュリティアクションを実行することと
を含み、
前記第１のセキュリティアクションまたは前記第２のセキュリティアクションのうちの１つは、前記第１の接続を第１のホストデバイスから第２のホストデバイスに移動させることによって、前記第１の接続を前記第１のホストデバイスに関連付けられた他の接続から分離することを含む、
を含む、方法。
【請求項１０】
第２のクライアントと前記第１のホストデバイスの第２のアプリケーションとの間の第２のセッションに対して確立された第２の接続を検出することであって、前記第２のアプリケーションは、前記第２のアプリケーションに関するセキュリティをセキュリティ階層に分割する第２の複数のセキュリティタイムリミットに関連付けられることと、
前記第２の接続の持続時間をモニタすることと、
前記第２の接続の前記持続時間が前記第２の複数のセキュリティタイムリミットのセキュリティタイムリミットに到達したことに応答して、前記第２の接続に対して前記１つまたは複数の第１のセキュリティアクションを実行することと、
前記第２の接続の前記持続時間が前記第２の複数のセキュリティタイムリミットの別のセキュリティタイムリミットに到達したことに応答して、前記第２の接続に対して前記１つまたは複数の第２のセキュリティアクションを実行することと
をさらに含む、請求項９に記載の方法。
【請求項１１】
前記第１のセキュリティアクションまたは前記第２のセキュリティアクションのうちの１つは、ＩＰルックアップ、ディープパケットインスペクション、不正な形式のパケット検出、またはハニーポットセキュリティセンサの有効化を含む、請求項９に記載の方法。
【請求項１２】
前記第１の接続はＴＣＰ接続である、請求項９に記載の方法。
【請求項１３】
リソースへの不正アクセスに対してセキュアにする命令を格納する非一時的なコンピュータ可読記憶媒体であって、前記命令は、少なくとも１つのプロセッサによって実行されると、
第１のアプリケーションに対応するセッションに対して確立された複数の接続の持続時間をモニタして、接続持続時間データを生成することと、
前記接続持続時間データに基づいて、前記第１のアプリケーションに関するセキュリティをセキュリティ階層に分割する第１の複数のセキュリティタイムリミットを決定することと、
第１のクライアントと前記第１のアプリケーションとの間の第１のセッションに対して確立された第１の接続を検出することと、
前記第１のクライアントと前記第１のアプリケーションとの間で確立された前記第１の接続の持続時間をモニタすることと、
前記第１の接続の前記持続時間が前記第１のアプリケーションに関連付けられた前記第１の複数のセキュリティタイムリミットのセキュリティタイムリミットに到達したことに応答して、前記第１の接続に対して１つまたは複数の第１のセキュリティアクションを実行することと、
前記第１の接続の前記持続時間が前記第１の複数のセキュリティタイムリミットの別のセキュリティタイムリミットに到達したことに応答して、前記第１の接続に対して１つまたは複数の第２のセキュリティアクションを実行することと
の工程を前記少なくとも１つのプロセッサに行わせ、

前記第１のセキュリティアクションまたは前記第２のセキュリティアクションのうちの１つは、前記第１の接続を第１のホストデバイスから第２のホストデバイスに移動させることによって、前記第１の接続を前記第１のホストデバイスに関連付けられた他の接続から分離することを含む、

非一時的なコンピュータ可読記憶媒体。

【請求項１４】

前記工程は、

第２のクライアントと前記第１のホストデバイスの第２のアプリケーションとの間の第２のセッションに対して確立された第２の接続を検出することであって、前記第２のアプリケーションは、前記第２のアプリケーションに関するセキュリティをセキュリティ階層に分割する第２の複数のセキュリティタイムリミットに関連付けられることと、

前記第２の接続の持続時間をモニタすることと、

前記第２の接続の前記持続時間が前記第２の複数のセキュリティタイムリミットのセキュリティタイムリミットに到達したことに応答して、前記第２の接続に対して前記１つまたは複数の第１のセキュリティアクションを実行することと、

前記第２の接続の前記持続時間が前記第２の複数のセキュリティタイムリミットの別のセキュリティタイムリミットに到達したことに応答して、前記第２の接続に対して前記１つまたは複数の第２のセキュリティアクションを実行することと

をさらに含む、請求項１３に記載の非一時的なコンピュータ可読記憶媒体。

【請求項１５】

前記第１のセキュリティアクションまたは前記第２のセキュリティアクションのうちの１つは、ＩＰルックアップ、ディープパケットインスペクション、不正な形式のパケット検出、またはハニーポットセキュリティセンサの有効化を含む、請求項１３に記載の非一時的なコンピュータ可読記憶媒体。

【請求項１６】

前記第１の接続はＴＣＰ接続である、請求項１３に記載の非一時的なコンピュータ可読記憶媒体。

【発明の詳細な説明】

【技術分野】

【０００１】

１．発明の技術分野

本開示は、リソースへの不正アクセスに対するコンピュータセキュリティに関し、より具体的には、アプリケーションをプロファイルすることおよびそれらのアプリケーションのセッションおよび接続をセキュリティ階層に分割することに関する。

【０００２】

（関連特許の相互参照）

本出願は、２０１５年１月２０日に出願された米国特許仮出願第６２／１０５，６８５号明細書の優先権を主張し、その開示内容は、その全体が参照により組み込まれる。

【背景技術】

【０００３】

２．発明の技術分野

ネットワーク通信において、ファイヤーウォールおよび侵入検知防止システムを含む、ソフトウェアおよびハードウェアの多くのセキュリティ形式がある。しかしそれらの形式はすべて、規則が正しく適用されなければ、不正アクセスの機会を開くことになるという１つの核心問題に対して欠陥がある。インターネットにさらされると、アプリケーションをホストしているサーバへのリモートアクセスを可能にし得る、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多数のバグを有する。

【０００４】

既存のファイヤーウォールは、パケットインスペクションをサポートする。インスペクションは、ファイヤーウォールの設定に適用される規則に基づいており、アプリケーショ

ンスタックに伝送する能力がなく、そしてアプリケーションスタックがセキュリティスタックに伝送する能力に制限があるため、能動学習に制限がある。ファイヤーウォールは通常、ホストに接続する度に膨大なオーバーヘッドを生成し、および適用される規則が多すぎると、スケールに問題が生じる可能性があるため、規則の数の削減に努める。

【発明の概要】

【課題を解決するための手段】

【０００５】

本開示の実施形態は、ハッカーがセキュアなリソースへの不正アクセスの取得を防止する、ハッカーに対するオンラインセキュリティを提供する知的方法を含む。一実施形態において、リソースへの不正アクセスに対するセキュリティの方法が開示されている。第１のクライアントと第１のホストデバイスの第１のアプリケーションとの間で確立された第１のアプリケーションセッションが検出される。第１のアプリケーションは、第１のアプリケーションのセキュリティをセキュリティ階層に分割する第１の複数のセキュリティタイムリミットと関連付けられる。第１のクライアントと第１のアプリケーションとの間で確立された第１のアプリケーションセッションの持続時間がモニタされる。１つまたは複数の第１のセキュリティアクションは、第１の複数のセキュリティタイムリミットのうちの或るセキュリティタイムリミットに到達する第１のアプリケーションセッションの持続時間に応答して第１のアプリケーションセッションに対して実行される。１つまたは複数の第２のセキュリティアクションは、第１の複数のセキュリティタイムリミットのうちの別のセキュリティタイムリミットに到達する第１のアプリケーションセッションの持続時間に応答して第１のアプリケーションセッションに対して実行される。

【０００６】

一実施形態において、セキュリティタイムリミットは、機械学習プロセスを通じて確立される。そのプロセスは、第１のセッション持続時間データを作成する第１のアプリケーションに対応する複数の前のアプリケーションセッションの持続時間をモニタすることを含むことができる。第１の複数のセキュリティタイムリミットはその後、複数の前のアプリケーションセッションの第１のセッション持続時間データに基づいて判定される。

【０００７】

一実施形態において、方法はさらに、第２のクライアントと少なくとも１つのサーバの第２のアプリケーションとの間で確立された第２のアプリケーションセッションを検出することであって、第２のアプリケーションが、第２のアプリケーションのセキュリティをセキュリティ階層に分割する第２の複数のセキュリティタイムリミットと関連付けられることと、第２のクライアントと第２のアプリケーションとの間で確立された第２のアプリケーションセッションの持続時間をモニタすることと、複数のセキュリティタイムリミットのうちの或るセキュリティタイムリミットに到達する第２のアプリケーションセッションの持続時間に応答して第２のアプリケーションセッションに対する１つまたは複数の第１のセキュリティアクションを実行することと、複数のセキュリティタイムリミットのうちの別のセキュリティタイムリミットに到達する第２のアプリケーションセッションの持続時間に応答して第２のアプリケーションセッションに対する１つまたは複数の第２のセキュリティアクションを実行することを備える。

【０００８】

一実施形態において、第１のセキュリティアクションまたは第２のセキュリティアクションのうちの１つは、ＩＰルックアップ、ディープパケットインスペクション、不正な形式のパケット検出、またはハニーポットセキュリティセンサの有効化のうちの１つを含む。一実施形態において、第１のセキュリティアクションまたは第２のセキュリティアクションのうちの１つは、第１のアプリケーションセッションを少なくとも１つのホストデバイスと関連付けられた他のアプリケーションセッションから分離することを含む。第１のアプリケーションセッションを分離することは、第１のアプリケーションセッションを第２のホストデバイスに移動することを備えることができる。第１のアプリケーションセッションを分離することはまた、第１のホストデバイス上の第１のアプリケーションセッシ

ョンを維持すること、および他のアプリケーションセッションが第１のホストデバイスと確立されることを防止することも備えることができる。

【０００９】

一実施形態において、オンラインセキュリティの方法はまた、アプリケーションセッションに確立される接続に適用することもできる。他の実施形態は、命令を格納する非一時的なコンピュータ可読媒体を含む。命令は、少なくとも１つのプロセッサがリソースへの不正アクセスを防止するオペレーションを実施することにより実行可能である。

【図面の簡単な説明】

【００１０】

【図１】実施形態にかかる、セッション／接続分割を有するネットワーク化された通信システムのブロック図である。

【図２】実施形態にかかる、異なるセキュリティ階層に分割されたアプリケーションセッション／接続の図である。

【図３】実施形態にかかる、異なるセキュリティ階層に分割された異なるアプリケーションのアプリケーションセッション／接続の図である。

【図４】実施形態にかかる、アプリケーションセッション／接続の分離を示す図である。

【図５】別の実施形態にかかる、アプリケーションセッション／接続の分離を示す図である。

【図６】実施形態にかかる、図１からのセッション／接続マネージャモジュールのブロック図である。

【図７】実施形態にかかる、アプリケーションのセッション／接続をプロファイルし、タイムリミットを学習するための方法のフローチャートである。

【図８】実施形態にかかる、セッション／接続分割セキュリティのための方法のフローチャートである。

【図９】実施形態にかかる、コンピュータ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】

【００１１】

本開示のいくつかの実施形態についてこれより詳細に言及し、それらの例を添付図面で示す。なるべく同種の参照番号を図面に使用して、同種の機能性を示し得ることに留意されたい。本開示の実施形態を示す図面は、説明のみを目的にする。本明細書に示した構造および方法の代替的実施形態を本明細書に記載の開示原理、または予想される(touted)利益から逸脱しない範囲で用いてもよいという以下の説明から当業者には容易に理解されよう。

【００１２】

セキュアリングオンラインアプリケーションの特徴は、機械レベルのセキュリティの学習に基づき、セキュリティシステムが平均的アプリケーションセッションフローをプロファイルすることを可能にする。平均的アプリケーションセッションフローは、マルチ段階のトリガリングセッションのトリガリングポイントを変更することができる。セッションの継続が長いほど、セッションが危険にさらされるリスクがますます高くなる。本開示の実施形態は、セッションをプロファイルして、時間または状態に応じて、異常なパケットフローのセッションを分析することまたは制御された分析セキュリティサンドボックスの再生のためのパケットフローを複製することなどにより、セキュリティアクションを開始する。

【００１３】

本開示の実施形態は、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止するおよび進行中の任意のデータセットへのアクセスを防止するためにアプリケーションをプロファイルするセキュリティシステムプラットフォームのコンポーネントに関する。本開示の実施形態はまた、アプリケーションおよびネットワークで発見されたさまざまなアプリケーションセッションを単一のセッション内のセキュリティ階層／セグメントに分

割して、経時的にセキュリティ階層／セグメントごとのセキュリティレベルを強化する。より詳細には、本開示の実施形態は、より高いセキュリティソリューションのセキュリティレベルをエスカレートすることを用いて権限のないリソースへのアクセスを防止することができる。本開示の実施形態はまた、接続をセキュリティ階層に分割して、経時的にセキュリティ階層ごとのセキュリティレベルを強化することもできる。

【００１４】

図１は、実施形態にかかる、セッション接続分割セキュリティを有するネットワーク化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、ネットワーク１１０、ルータ１１５、ファイヤーウォール１２０、ロードバランサ１２５、フロントエンドサーバ１３０、バックエンドサーバ１３５、およびデータベース１４０などのコンピュータデバイスは、ネットワーク１１０経由でクライアント１０５によってアクセスされるデータセンターを形成することができる。説明を容易にするために２つのクライアント１０５と２つのフロントエンドサーバ１３０のみを図１に示している。他の実施形態において、より多い数のクライアントデバイス１０５およびフロントエンドサーバ１３０になることもある。

【００１５】

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タデバイスになり得る。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フェースを通じ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、ユーザがアプリケーションセッションおよび、フロントエンドサーバ１３０によってホストされたさまざまなアプリケーションとの接続を確立することによって制御される。

【００１６】

フロントエンドサーバ１３０は、１つ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タデバイスであり、オペレーティングシステムを実行する。サーバ１３０は、いくつかのソフトウェアアプリケーション１５０をホストし、また本明細書ではホストデバイスと呼ぶこともできる。例えば、アプリケーション１５０は、クレジットカード支払いアプリケーション１５０Ａ、ウェブサイト１５０Ｂ、およびオンラインバンキングアプリケーション１５０Ｃをホストすることができる。アプリケーション１５０をホストするホストデバイスの他の例は、汎用家電、電話機、タブレット、飛行機の飛行管制システムなどであってよい。

【００１７】

クライアントデバイス１０５は、ネットワーク１１０、ルータ１１５、ファイヤーウォール、およびロードバランサ１２５経由でアプリケーション１５０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とサーバ１５０のソケット間の双方向通信チャネルとして使用される。接続は、或る時点でハンドシェイクを使用するまたは時にはハンドシェイクプロセスを使用しないなどにより確立され、そして後の時点で終了する。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むことができる。接続例のうちの１つのタイプは、開放型システム間相互接続（ＯＳＩ）モデルのトランスポート層の下の伝送制御プロトコル（ＴＣＰ）接続である。

【００１８】

クライアントデバイス１０５はまた、接続Ｃ１－Ｃ６を介してアプリケーション１５０のアプリケーションセッションＳ１－Ｓ６も確立する。アプリケーションセッションは、所与のアプリケーションの２以上の通信エンティティ間の対話型情報交換である。アプリケーションセッションは、或る時点で確立され、そして後の時点で終了する。アプリケーションセッション中、情報を要求するまたは要求に応答する１つまたは複数のメッセージは、セッションのために確立された接続を介して各方向に送信され得る。セッションの状態（例えば、ログイン、ログアウト、アイドル、アップロード、ダウンロード、探索、既存データの操作または更新、データの破壊または除去、アラームのトリガ、タイムカウン

タ状態、鍵適合、鍵変更、リスク因子の状態）は、フロントエンドサーバ１３０Ａまたはクライアントデバイス１０５のいずれかによって維持され得る。一実施形態において、アプリケーションセッションは、トランスポート層の上にあるＯＳＩセッション層のセッションである。セッションの例は、とりわけＨＴＴＰセッション、ＦＴＰセッション、およびＳＭＴＰセッションになり得る。

【００１９】

一例として、ユーザがクライアントデバイス１０５Ａにクレジットカードを通すと、クレジットカード認証セッション（例えば、Ｓ１、Ｓ２）が開始され、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１５０Ａ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１５０Ａは、クライアントデバイス１０５Ａと通信してクレジットカード番号を取得し、クライアントデバイス１０５Ａから入金する。クレジットカード支払いアプリケーション１５０Ａは次に、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があるかどうかを判定するためにバックエンドサーバ１３５経由でデータベース１４０にアクセスする。クレジットカード支払いアプリケーション１５０Ａは次に、クライアントデバイス１０５Ａに肯定／否定応答を提供する。接続およびセッションは次に、応答をクライアントデバイス１０５Ａに提供した後に終了する。

【００２０】

別の例では、ユーザがＵＲＬをクライアント１０５Ｂのブラウザに入力すると、ウェブフォームセッション（例えば、Ｓ３、Ｓ４）が開始される。クライアントデバイス１０５Ｂは、ウェブサイト１５０Ｂとセッションを確立する。フロントエンドサーバ１３０Ａ（即ち、ウェブサーバ）は、複数のセッションを処理することができる。フロントエンドサーバ１３０Ａは、セッションごとのタイムカウンタで開始する。ユーザは、セッションが閉じる前にフォームに記入する時間量ｘを有する。異なるフロントエンドサーバ１３０Ｂは、ウェブフォームデータに記入するのに時間を要するため、最初のセッションからフォーム提出（submission）を処理することができる。

【００２１】

さらなる例では、ユーザがクライアントデバイス１０５Ｂのモバイルバンキングアプリケーションを開くと、オンラインバンキングセッション（例えば、Ｓ５、Ｓ６）が開始されて、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１５０Ｃと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１５０Ｃは、クライアントデバイス１０５Ｃと通信してクライアントデバイス１０５Ｃから認証情報を取得する。ひとたび認証されると、クライアントデバイス１０５Ｃは、口座残高を要求し、預金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。バンキングアプリケーション１５０Ｃは、これらの要求を処理するバックエンドサーバ１３５経由でデータベース１４０に格納された口座情報にアクセスすることができる。

【００２２】

バックエンドサーバ１３５は、データベース１４０に格納されたデータへのアクセスを提供する。アプリケーション１５０のいずれもバックエンドサーバ１３５にデータを要求することができ、バックエンドサーバはその後、データベース１４０からデータを読み出してデータをアプリケーション１５０に提供する。バックエンドサーバ１３５の例にＳＱＬサーバがある。ハッカーは、ハッキングしたセッションまたは接続を通じてデータベース１４０のデータにアクセスしようと試みることが多く、セッション／接続マネージャモジュール１５２は、ハッカーがデータに上手くアクセスする前にこれらのハッキングされたセッションおよび接続を検出しようと試みる。ハッキングされたセッションの場合、ハッカーは、セッションのタイムラインを延長し、そこからリスク因子が増加し、セッション／接続マネージャモジュール１５２は、セキュリティを強化してアラートをトリガすることができる。

【００２３】

セッション／接続マネージャモジュール１５２は、ハッキングされたセッション／接続

に対するセキュリティを提供する。各セッション／接続に対し、セッション／接続マネージャモジュール１５２は、セキュリティ階層がトリガされる異なる時間にセッション／接続を分割する。セッション／接続が時間によってセキュリティ階層に分割されるように強制することにより、異なるアクションは、単一のセッション／接続の分割階層に基づいてトリガされる。各階層では、セッション／接続マネージャモジュール１５２は、１つまたは複数のセキュリティアクションをセッション／接続に適用する。一実施形態において、セキュリティアクションは、処理装置（例えば、プロセッサまたはコントローラまたはカスタムアプリケーション特定集積回路）上でセキュリティアクションのソフトウェアプログラムコードを実行することによってセッション／接続に対して適用される。

【００２４】

セキュリティアクションは、セッションからのデータを分析することによってハッカーを検出するまたはハッカーがハッキングを上手く完了することを防止するように設計されたアクションになり得る。セキュリティアクションの例は、ＩＰルックアップ、ハニーポットセンサの起動、セッション／接続の分離、ディープパケットインスペクション、セッション／接続の包含、セキュリティ警告、セッション／接続のトレース、セッション／接続の記録、機械学習をセッション／接続に適用すること、およびセッション／接続の完全制御／警告および終了を含むことができる。先のセキュリティ階層は、異なる規則を含む場合があり、誤検出(false positives)を削減するセキュリティアクションがほとんどもしくは全くないように構成される可能性がある一方、後のセキュリティ階層は、よりリソースに集中したセキュリティアクションを含む場合がある。後のセキュリティ階層では、セッション／接続マネージャモジュール１５２は、ルータ１１５、ファイヤーウォール１２０またはロードバランサ１２５などの他のデバイスに、ハイリスクのセキュリティセッション／接続を通知することができ、他のデバイスがセキュリティアクションをセッション／接続に適用するようにさせる。

【００２５】

セッション／接続マネージャモジュール１５２は、セッション／接続の持続時間をモニタし、そしてひとたびセッション／接続持続時間が或るセキュリティタイムリミットに到達すると、セキュリティをあるセキュリティ階層から次のセキュリティ階層に進展させる。通常のほとんどのセッション／接続は、セキュリティタイムリミットに到達する前に完了することが期待される。ハッキングされたセッション／接続のみがセキュリティタイムリミットを超えることが期待される。よりリソースに集中したセキュリティアクションは従って、セッションがハッキングされるリスクがより高いセッション／接続のみに適用される。その結果、セキュリティ階層の経時的な増加は、ハッカーに対するハイレベルのセキュリティをさらに維持しながら、セッションの特定の時間期間内でセキュリティ階層を系統的に増加させることによってフロントエンドサーバ１３０の、プロセッサおよびメモリなどのコンピュータハードウェアの計算負荷を削減することによってフロントエンドサーバ１３０の機能性を改善する技術的優位性を有する。

【００２６】

異なる時間間隔に異なるセキュリティアクションを有することはまた、ツールが通常のセッションとハッキングされたセッションがどうであるかを理解し、それに応じてセッションの状態を終了し、追跡し、トレースし、記録し、エスカレートし、分析することを可能にする。さらに、接続およびセッションは、最終的にハッカーが出ていくまたは追い出すことに基づいてセッションの最後に終了する。ハッカーが戻ると、ハッカーの以前のハッキングの企てによってプロファイルされた或るフィンガープリントデータを使用して、ハッカーを識別し、そしてシステムが、どのようにハッカーがホストまたはバックエンドシステムへの自分のアクセス権をエスカレートしようとしているかを学習しながら、記録をトリガするまたはより多くのセキュリティセンサを適用する、リスクレベルを直ちにエスカレートすることができる。ひとたび接続されたセッション状態が除去される／終了すると、機械学習は、発見されたセキュリティホール(hole)を自己修正して、セッションを終了してハッカーの侵入を防ぐことができる。

【００２７】
セキュリティタイムリミットは、アプリケーション１５０の各タイプで異なってもよい。一実施形態において、セッション／接続マネージャモジュール１５２は、機械学習プロセスを経て各アプリケーションに別個にセキュリティタイムリミットを判定する。学習プロセスは、アプリケーションの以前のセッション／接続持続時間をモニタし、セッション／接続持続時間からセッション／接続持続時間データを作成し、セッション／接続持続時間データを、アプリケーションセキュリティプロファイルデータベース１５４のアプリケーションセキュリティプロファイルに格納する。アプリケーションのセッション／接続のセキュリティタイムリミットは次に、結果的に各アプリケーション１５０が最適にテイラードされたセキュリティタイムリミットとなる、アプリケーションのアプリケーションセキュリティプロファイルのセッション／接続持続時間データから判定される。他の実施形態において、ハッキングされたセッションタイムリミットを、ユーザのリスク因子および設定に応じてさらなる機械学習のために延長することができる。

【００２８】
ネットワーク１１０は、クライアント１０５とルータ１１５との間の通信経路を表す。ネットワーク１１０は、有線ネットワーク、無線ネットワーク、または有線ネットワークと無線ネットワークの組み合わせを含むことができる。ネットワーク１１０は、ネットワーク１１０とファイヤーウォール１２０との間のデータパケットを経路指定するネットワーキングデバイスである。ファイヤーウォール１２０は、データトラフィックをフィルタにかけて、或るデータパケットがファイヤーウォールの規則に合わなければ、それらのデータパケットを遮断することができる。ロードバランサ１２５は、アプリケーショントラフィックを多数のサーバ１３０に分散する。

【００２９】
一実施形態において、セッション／接続マネージャモジュール１５２は、ソフトウェア命令、ハードウェア論理、またはソフトウェアとハードウェアの組み合わせとして実装されてもよい。一実施形態において、セッション／接続マネージャモジュール１５２は、ルータ１１５、ファイヤーウォール１２０、ロードバランサ１２５、またはバックエンドサーバ１３５など、システムのどこでも配置され得る。他の実施形態において、セッション／接続マネージャモジュール１５２の機能は、いくつかのコンピュータデバイスに分散され得る。

【００３０】
次に図２について、実施形態にかかる、アプリケーションセッションまたは接続が異なるセキュリティ階層に分割された図を示している。図２のセッション／接続は、４つのセキュリティ階層：セキュリティ階層Ａ２０２、セキュリティ階層Ｂ２０４、セキュリティ階層Ｃ２０６、およびセキュリティ階層Ｄ２０８に分割される。各セキュリティ階層は、セッション／接続の長さが増加する時にセッション／接続に適用される上位レベルのセキュリティを表す。各連続したセキュリティ階層は、異なるセキュリティタイムリミットに到達するアプリケーションセッション／接続の持続時間によってトリガされる。各セキュリティ階層は、固有のセキュリティアクションが行われる、いくつかのセキュリティ段階（即ち、セキュリティサブ階層）を含む。一般的に言えば、セッション／接続の状態は、異なる段階を有し、強化されたセッション／接続のセキュリティが増加し、セキュリティアクションが時間の経過とともに適用される。

【００３１】
セキュリティ階層Ａ２０２は、９秒の長さである。セキュリティ階層Ａ２０２中、最小数のセキュリティアクション（例えば、セキュリティアクションが無いまたはセキュリティアクションがほとんど無い）がセッション／接続に適用される。セキュリティアクションは一般的に、通常のほとんどのアプリケーションセッション／接続が、セキュリティ階層Ａ２０２が終わる前に完了することが期待される理由で、セキュリティ階層Ａ２０２中に必要ない。

【００３２】

ひとたびセッション／接続がセキュリティ階層Ａの９秒のタイムリミットに到達すると、セキュリティレベルは、セキュリティ階層Ａ２０２からセキュリティ階層Ｂ２０４に強化される。セキュリティ階層Ｂ２０４は、９秒の長さであり、セキュリティ階層Ｂ２０４中に基本セキュリティアクションがアプリケーションセッション／接続に適用される。例えば、セキュリティ階層Ｂの段階４中、クライアントデバイス１０５のＩＰアドレスを検索して、そのアドレスが疑わしいアドレスであるかどうかを判定することができる。ＩＰアドレスは、そのアドレスが或る国に由来するかどうかまたはＩＰアドレスがプロキシサーバであるかどうか疑わしい場合もあり、あるいは所定の因子分析の結果、そのＩＰが疑わしいというフラグが立つ。ＩＰアドレスが疑わしい場合、セキュリティレベルは、直ちにセキュリティ階層Ｃ２０６に引き上げられる間、セキュリティ段階５と６のいずれのセキュリティアクションも省かれる。

【００３３】

別の例として、セキュリティ階層Ｂの段階５中、ハニーポットセキュリティセンサを起動することができる。ハニーポットセキュリティセンサは、偽造データおよび非実データを包含するファイルフォルダに添付される。偽造データのフォルダは、フォルダのファイルがアクセスされるまたはフォルダが開かれると、セキュリティアラートを作成するセキュリティセンサをフォルダに添付させることができる。例えば、ディレクトリ構造は、フォルダ“／ｈｏｍｅ／ｕｓｅｒ１／”“／ｈｏｍｅ／ｕｓｅｒ２／”“／ｈｏｍｅ／ｕｓｅｒ３／”を含むことができる。実データは、“／ｈｏｍｅ／ｕｓｅｒ３／”のみに格納されるが、“／ｈｏｍｅ／ｕｓｅｒ１／”や“／ｈｏｍｅ／ｕｓｅｒ２／”ディレクトリには格納されない。ディレクトリツリーにアクセスするハッカーは、どのディレクトリが実データを包含するかおよびどのディレクトリが偽造データを含むか知らない。従って、ハッカーは、セッション／接続中にハニーポットフォルダを恐らく開き、ハニーポットセキュリティセンサをトリガする。

【００３４】

ひとたびセッション／接続がセキュリティ階層Ｂ２０４の９秒のタイムリミット（即ち、セッション／接続の開始から１８秒のタイムリミット）に到達すると、セキュリティレベルは、セキュリティ階層Ｂ２０４からセキュリティ階層Ｃ２０６に強化される。セキュリティ階層Ｃ２０６は、９秒の長さであり、中間のセキュリティアクションは、セキュリティ階層Ｃ２０６中にアプリケーションセッション／接続に適用される。例えば、セキュリティ階層Ｃ２０６の段階７中、アプリケーションセッション／接続を他のアプリケーションセッションから分離することができる。セッション／接続の分離は、後に図４および図５を参照して説明される。

【００３５】

別の例として、セキュリティ階層Ｃ２０６の段階８中、ディープパケットインスペクションは、データパケットが疑わしいかどうかを判定するためにアプリケーションセッション／接続のデータパケットで行われる。データパケットは、それらのデータパケットがプロトコル異常、ＳＱＬインジェクション、または不正な形式のパケットを含むと判定されるかどうか疑われる。

【００３６】

別の例として、セキュリティ階層Ｃ２０６の段階９中、他のネットワーキングデバイス（例えば、ルータ１１５、ファイヤーウォール１２０またはロードバランサ１２５）は、ハイリスクセッションが通知される。他のネットワーキングデバイスは次に、ハイリスクセッションのデータのデバイス自身の分析を開始して、この情報をセッション／接続マネージャモジュール１５２に戻す。

【００３７】

ひとたびセッション／接続がセキュリティ階層Ｃ２０６の９秒のタイムリミット（即ち、セッション／接続の開始から２７秒のタイムリミット）に到達すると、セキュリティレベルは、セキュリティ階層Ｃ２０６からセキュリティ階層Ｄ２０８に強化される。セキュリティ階層Ｃ２０６は、９秒の長さであり、進展したセキュリティアクションは、セキュ

リティ階層Ｄ２０８中にアプリケーションセッション／接続に適用される。例えば、セキュリティ階層Ｃ２０６の段階１０中、実データへのアクセスを遮断して偽造データへのアクセスのみを許可する、アプリケーションセッション／接続を包含することができる。セキュリティ階層２０６の段階１１中、警告、トレースおよび記録を行うことができる。警告は、電子メールまたはＳＭＳテキストなど、潜在的にハッキングされたセッションをネットワーキング管理者に通知することを伴う。トレースは、ファイルディレクトリがアプリケーションセッション中にアクセスされた順序など、アプリケーションセッション中に行われるアクションのフローをトレースすることを伴う。記録は、さらなる調査のための第三者ツールによる後のオフライン分析のトレース中に獲得されるデータを格納することを伴う。セッション／接続を段階１２の最後で終了することもできる。

【００３８】

セキュリティ階層および段階はすべて、図２の同じ持続時間を有するように示されている。他の実施形態において、セキュリティ階層および段階は、異なる持続時間を有することができる。図２において、数個のセキュリティ階層の数個のセキュリティアクションしか示されていないが、図２に示した他のセキュリティアクションを他のセキュリティ段階中に行うこともできる。さらに、セキュリティアクションは、異なる順序で、図２に示した段階とは異なるセキュリティ段階中に適用されてもよい。

【００３９】

さらに、セキュリティを時間によってセキュリティ階層に分割することは、必ずしもセッション／接続マネージャモジュール１５２が常に高いセキュリティを実行することを防止することではない。セキュリティ規則の異なるセットは単純に、異なるセキュリティ階層２０２、２０４、２０６および２０８中に適用されてよい。これは、誤検出を防止する一方、さらにコンピュータリソースが、典型的にはハッキングされてないセッション／接続よりも長く続く、ハッキングされたセッション／接続に重点が置かれることも可能にする。例えば、セキュリティ階層Ｂ２０４はまた、ＩＰルックアップインジケータが疑わしいＩＰである場合にのみ、ディープパケットインスペクションを適用する規則のセットを含むことができる。

【００４０】

図３は、実施形態にかかる、異なるセキュリティ階層に分割された異なるアプリケーションのアプリケーションセッション／接続の図を示している。セキュリティ階層の長さは、アプリケーションのタイプに応じて異なる。クレジットカード処理アプリケーション１５０Ａの場合、セキュリティ階層は、９秒の長さであり、各セキュリティ段階は、３秒の長さである。ウェブアプリケーション１５０Ｂの場合、セキュリティ階層は、９０秒の長さであり、各セキュリティ段階は、３０秒の長さである。オンラインバンキングアプリケーション１５０Ｃの場合、セキュリティ階層は、９分の長さであり、各セキュリティ段階は、３分の長さである。

【００４１】

クレジットカードの例について、普通に機能するクレジットカード処理アプリケーション１５０Ａは通常、５－１０秒以内でトランザクションを処理し、５－１０秒で承認されたまたは拒否されたクレジット回答を与える。本開示の実施形態は、平均のクレジットカードトランザクションのアプリケーション１５０Ａをプロファイルして、平均のクレジットカードトランザクション時間からシステムの時間ベースのセッション／接続タイムリミットを算定する。

【００４２】

セキュリティ階層で行われるセキュリティアクションは、アプリケーションに関係なくアプリケーションにわたって同じにすることができる。例えば、ＩＰルックアップは、３つのすべてのアプリケーションのセキュリティ階層中に発生させることができる。

【００４３】

図４は、実施形態にかかる、アプリケーションセッションの分離を示す図である。図５は、別の実施形態にかかる、アプリケーションセッションの分離を示す図である。図４と

図５の両方は、図２の段階７からのセッション／接続分離セキュリティアクションを示す。

【００４４】

図４のセッション／接続分離は、元のサーバのハイリスクセンサ／接続を維持することによりおよびサーバ１３０Ａと確立した他のセッション／接続を完了させる一方、任意の新しいセッション／接続がそのサーバ１３０Ａのアプリケーション１５０と確立されることを防止することにより発生する。最初に、アプリケーション１５０と確立された６つのセッションＳ１－Ｓ６、および対応する接続Ｃ１－Ｃ６がある。次にセッションＳ３が通常でない長さの時間期間開いていて、分離しなければならないことを判定する。セッションＳ３を分離するために、セッションＳ１、Ｓ２、Ｓ４、Ｓ５およびＳ６は、完了することを許可される。しかしながら、どの新しいセッションもサーバ１３０Ａと確立されることを許可されない。最終的に、セッションＳ３は、サーバ１３０Ａのアプリケーション１５０と確立される唯一のセッションであり、それによりセッションＳ３および接続Ｃ３を分離する。

【００４５】

あるいは、ハイリスクセッションＳ３を分離するために、他方のセッション（Ｓ１、Ｓ２、Ｓ４、Ｓ５、Ｓ６）は、フロントエンドサーバ１３０Ａから別のフロントエンドサーバ１３０Ｂに移動されて、より高いリスクセッションＳ３または接続によって危険にさらされるデータを保護するようにできる。より高いリスクのセッション時間は、通常許可される時間を超えて延長し、さらにセキュリティアクションは、セッション対して行われる：そのアクションの分析が処理され、パケットが記録され、より深化したモニタリングを開始し、起きたことまたは起きていたことをトレースして追跡するために完全なソースデータを用いて終了する。動的アクセス制御リスト（ＡＣＬ）は、より高いリスクのセッションＳ３が任意のタイプの広範な探索、走査またはより大規模なデータセットのダウンロードを行うことを遮断するために導入される。データベース１４０への接続もセッションのリスク因子に応じてすべて除去されるまたは限定され得る。セッションＳ３と関連付けられたＩＰアドレスも記録することができ、クライアント１０５は、再接続を強制される場合もある。セッションＳ３が確立される第２の時間のセッション／接続マネージャモジュール１５２は、ハッカーのセッションＳ３のアクティビティを記録する完全な記録モードである。ハッカーのセッションＳ３はまた、ハッカーが実際には有していない時にデータを見つけたと思わせるように騙すために偽データを示すように操作されることもできる。バックエンドデータベース１４０はまた、本物にするまたは偽造データベースに置き換えることもできる。

【００４６】

図５のセッション／接続分離は、サーバ間のセッション／接続を移動することによって発生する。最初に、６つのセッションＳ１－Ｓ６およびフロントエンドサーバ１３０Ａのアプリケーション１５０と確立された対応する接続Ｃ１－Ｃ６がある。次にセッションＳ３が通常でない長さの時間期間開いていて、分離しなければならないことを判定する。セッションＳ３を分離するために、セッションＳ３および接続Ｃ３は、フロントエンドサーバＡ１３０Ａから異なるフロントエンドサーバＢ１３０Ｂに移動される。残りのセッションＳ１、Ｓ２、Ｓ４、Ｓ５およびＳ６と接続Ｃ１、Ｃ２、Ｃ４、Ｃ５およびＣ６は、影響を受けず、フロントエンドサーバ１３０Ａに存続する。

【００４７】

図５に示すように、セッションに時間に応じて、セッションＳ３および接続Ｃ３の状態は、セッションホップまたはミラーリング(mirror)を行うことによって別のサーバＢ１３０Ｂに移動され得る。アップストリームデバイス（例えば、ルータ１１５、ファイヤーウォール１２０、ロードバランサ１２５）もまた、その移動を通知される。これによりユーザのセッション／接続を切断するまたはユーザが完全状態の移動が起きたことを検出することをせずに完全なセッション／接続の移行が可能になる。ハッカーがこの例ではフロントエンドサーバ１３０Ａに接続されていて、サーバ１３０Ａを危険にさらすリモートスク

リプトをアップロードしたならば、セッション／接続ホップは、以前のサーバ１３０Ａのアプリケーションビットを変更されたままにして、ハッカーのセッション／接続が機能することが防止されるまたは防止される可能性がある。セッション／接続ホップまたはフェイルオーバーは、ホップに基づいてアラートの作成を開始することができ、さらに状態変更のマルチレベルも有する。

【００４８】

さらに、フロントエンドサーバＢ１３０Ｂは、専用セキュリティサーバであってもよい。専用セキュリティサーバは、リアルタイムですべてのセッション／接続パケットを記録する能力を含み、上記のように、ハッカーがどのようにシステムに入り込むかを分析するためにパケットの再生を可能にする。

【００４９】

図６は、実施形態にかかる、図１からのセッション／接続マネージャモジュール１５２のブロック図である。セッション／接続マネージャモジュール１５２は、セッション／接続モニタリングモジュール６０５、アプリケーションプロファイラモジュール６１０、セキュリティレベル進展モジュール６１５、セキュリティアクションモジュール６２０およびタイムリミット判定モジュール６２５を含む。一実施形態において、各モジュールは、コンピュータ可読媒体に格納されたソフトウェア命令として実装される。

【００５０】

セッション／接続モニタリングモジュール６０５は、アプリケーション１５０またはネットワークトラフィックをモニタするか、または新しいアプリケーションセッション／接続がクライアント１０５のいずれかとアプリケーション１５０のいずれかとの間で確立された時に検出する。ひとたび新しいアプリケーションセッション／接続が検出されると、セッション／接続モニタリングモジュール６０５は、セッションの持続時間を示すセッション／接続のセッション／接続カウンタを維持する。別個のセッション／接続カウンタは、セッション／接続の持続時間を別個に追跡できるように、セッション／接続ごとに維持される。任意の所与の時間に、セッション／接続モニタリングモジュール６０５は、複数のアプリケーション１５０の複数のセッション／接続をモニタリングすることができる。セッション／接続モニタリングモジュール６０５はまた、アプリケーションセッション／接続が確立されるアプリケーション１５０のタイプを特定することもできる。

【００５１】

アプリケーションプロファイラモジュール６１０は、セッション／接続の時間期間を獲得して、アプリケーションセキュリティプロファイル１５４のセッション／接続持続時間データを作成するための学習プロセスを実装する。一実施形態において、アプリケーションプロファイラモジュール６１０は、アプリケーション１５０のセッション／接続のセッション／接続持続時間を獲得する。アプリケーション１５０のセッション／接続持続時間データを作成するためにセッション／接続持続時間が処理される。セッション／接続持続時間データの例は、（１）アプリケーションセッション／接続の最短観察持続時間、（２）アプリケーションセッション／接続の最長観察持続時間、（３）アプリケーションセッション／接続の平均観察持続時間、（４）アプリケーションセッション／接続の実持続時間、およびその他の関連する持続時間データを含む。セッション／接続持続時間データは次に、アプリケーション１５０のアプリケーションセキュリティプロファイルに格納される。異なるアプリケーション１５０プロセスは、各アプリケーション１５０がそれ自身の固有のアプリケーションセキュリティプロファイルを有するように反復される。

【００５２】

アプリケーションプロファイラモジュール６１０はまた、セッション／接続がハッキングされたと見なされるか否か、セッション／接続持続時間と関連するアプリケーションセキュリティプロファイルにどれが格納されたかを示すハッキング状態情報を獲得することもできる。セッション／接続は、ハッキング例えば、ハッカーがシステム内のハニーポットをトリガしているかどうかまたは他のセキュリティがトリガしたかどうかを考慮する。

【００５３】

タイムリミット判定モジュール６２５は、アプリケーションセキュリティプロファイルのセッション／接続持続時間データにアクセスして、セキュリティタイムリミットがあるセキュリティ階層と次のセキュリティ階層に分離されていることを判定するためにデータを使用する。アプリケーションのセキュリティタイムリミットは、そのアプリケーションのみのセッション／接続持続時間データから得られる。従って、アプリケーションＡ１５０Ａのセキュリティタイムリミット、アプリケーションＢ１５０Ｂのセキュリティタイムリミット、アプリケーションＣ１５０Ｃのセキュリティタイムリミットは、すべて異なる。

【００５４】

セキュリティタイムリミットは、所定の数式を使用して以前に獲得されたセッション／接続持続時間データから得ることができる。セッションのセキュリティタイムリミットは、セッション持続時間データから計算され、そして接続のセキュリティタイムリミットは、接続持続時間データから計算される。例えば、アプリケーションのセッションのセキュリティタイムリミットは、アプリケーションのセッションの平均持続時間の倍数（例えば、２×、６×、８×、１０×）として計算され得る。別の例として、アプリケーションのセッションのタイムリミットは、アプリケーションのセッションの最長観察セッション持続時間の倍数（例えば、１×、２×、３×、４×）として計算され得る。アプリケーション１５０の各タイプは従って、その特定のアプリケーションのセッション／接続特性を最適に反映するセキュリティタイムリミットを有する。

【００５５】

タイムリミット判定モジュール６２０はまた、同様のプロセスを使用してあるセキュリティ段階と別のセキュリティ段階に分離するタイムリミットを判定することもできる。ハッキング状態情報をさらに使用して、通常のセッション／持続時間の持続時間がハッキングされたセッション／接続とどのように異なるかを学習することができ、今度はそれがセキュリティタイムリミットの設定に使用される。

【００５６】

セキュリティレベル進展モジュール２１０は、あるセキュリティ階層から別のセキュリティ階層への進展を制御する。所与のセッションでは、セキュリティレベル進展モジュール２１０は、セッション／接続持続時間をそのセッションに確立されたタイムリミットと比較する。ひとたび比較が、セッション／接続持続時間が対応するタイムリミットに到達したことを示すと、セキュリティレベル進展モジュール２１０は、セキュリティ階層を上位のセキュリティ階層に進展させる。

【００５７】

一実施形態において、アプリケーションセッション／接続の持続時間は、アプリケーションセッションの開始から測定される全体の持続時間である。セキュリティ階層ごとにタイムリミットもまた、アプリケーションセッションの開始から測定される。別の実施形態において、アプリケーションセッション／接続の持続時間は、単一のセキュリティ階層内のアプリケーションセッション／接続の持続時間を表す部分的持続時間になり得る。タイムリミットはまた、個々のセキュリティ階層の最大タイムリミットにもなり得る。

【００５８】

セキュリティアクションモジュール６２０は、フロントエンドサーバ１３０、バックエンドサーバ１３５およびデータベース１４０を悪意のセッションによるハッキングに対してセキュアにするさまざまなセキュリティアクションを実行するまたは開始する。以前に説明したように、セキュリティアクションの例は、ＩＰルックアップ、ハニーポットセンサの起動、セッション／接続の分離、ディープパケットインスペクション、セッションの包含、セキュリティ警告、セッション／接続のトレースおよびセッション／接続の記録である。異なるセキュリティアクションは、各セキュリティ階層において行われ、そしてタイムリミットに到達するセッション／接続の持続時間によってトリガされる。いくつかの実施形態において、セキュリティアクションのうちの１つまたは複数を暗号化されたセッションデータに行うことができる。

【００５９】
一実施形態において、セキュリティアクションモジュール６２０は、セキュリティ開始要求をアップストリームまたはダウンストリームデバイスに送信することによってセキュリティアクションを開始することができ、それにより他のデバイスにセキュリティアクションを実行させる。例えば、ルータ１１５、ファイヤーウォール１２０、ロードバランサ１２５、またはバックエンドサーバ１３５は、セキュリティアクションモジュール６２０によって起動される、セキュリティアクションを行う機能性を含むことができる。セキュリティアクションモジュール６２０はまた、セキュリティアクションの結果、他のデバイスから通信を受信することもできる。
【００６０】
図７は、実施形態にかかる、アプリケーションセッションをプロファイルする方法のフローチャートである。フローチャートは、セッション／接続マネージャモジュール１５２のオペレーションを表すことができる。いくつかの実施形態において、フローチャートのステップは、図に示した順序とは異なる順序で行われてもよい。
【００６１】
ステップ７０２において、アプリケーションのアプリケーションセッション／接続が検出される。ステップ７０４において、セッション／接続の持続時間がモニタされて獲得される。ステップ７０６において、セッション／接続持続時間データは、獲得されたセッション／接続持続時間から作成される。セッション／接続持続時間データは、アプリケーションと関連するアプリケーションセキュリティプロファイルに格納される。ステップ７０８において、ひとたび十分なセッション／接続持続時間データが以前に確立されたセッション／接続に使用可能になれば、セキュリティプロファイルは、アクセスされて、セキュリティタイムリミットは、セキュリティプロファイルのセッション／接続持続時間データから判定される。セキュリティタイムリミットは、或るセキュリティ階層と別のセキュリティ階層との時間境界を示す。
【００６２】
図７のプロセスは、異なるアプリケーション（例えば、１５０Ａ、１５０Ｂ、１５０Ｃ）がアプリケーションセキュリティプロファイルの大規模セットおよびアプリケーションのセキュリティを、セキュリティリスクの強化されるレベルを表す異なるセキュリティ階層に分割するアプリケーションごとの異なるセキュリティタイムリミットを作成するために数回反復される。
【００６３】
図８は、実施形態にかかる、セッション／接続分割セキュリティのための方法のフローチャートである。フローチャートは、典型的には図７のフローチャートの後に発生するセッション／接続マネージャモジュール１５２のオペレーションを表すことができる。いくつかの実施形態において、フローチャートのステップは、図に示した順序とは異なる順序で行われてもよい。
【００６４】
ステップ８０５において、クライアント１０５とアプリケーション１５０との間で確立されたアプリケーションセッション／接続が検出される。ステップ８１０において、アプリケーションセッション／接続に対応するアプリケーション１５０が特定される。ステップ８２５において、アプリケーションセッション／接続の持続時間がモニタされる。ステップ８３０において、アプリケーションセッション／接続のセキュリティレベルは、アプリケーションセッション／接続の持続時間がそのアプリケーションに判定されたセキュリティタイムリミットに到達する時に経時的に強化される。ステップ８３０において、いくつかのサブステップ８４０－８７０に分割され得る。
【００６５】
ステップ８４０において、セキュリティは最初に、セキュリティ階層Ａ２０２など、最低のセキュリティ階層に設定される。最低のセキュリティ階層Ａ２０２中、セキュリティ規則の最小セットによって定義された最小数のセキュリティアクションが行われる。

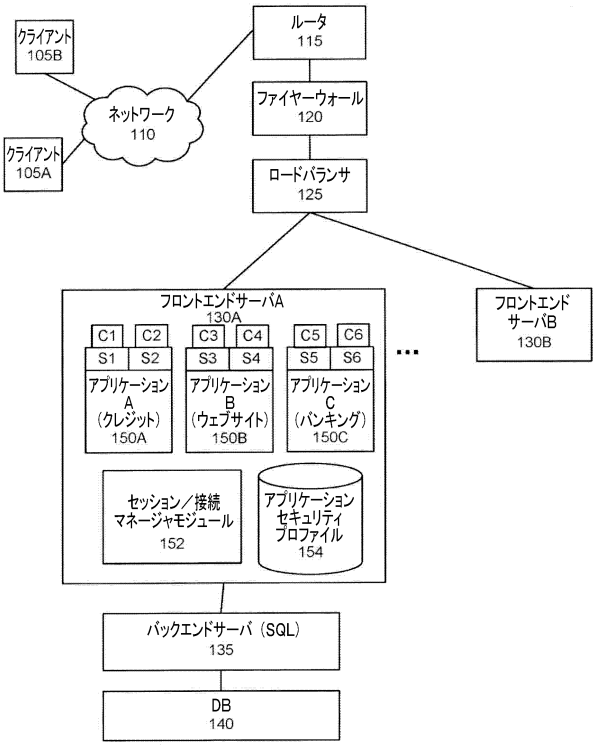
【００６６】
ステップ８４５において、セッション／接続持続時間は、最初のセキュリティタイムリミットと比較される。ステップ８５０において、セッション／接続持続時間が最初のセキュリティタイムリミットに到達したならば、セキュリティは、セキュリティ階層Ｂ２０４に強化される。セキュリティ階層Ｂ２０４中、基本セキュリティ規則によって定義された基本セキュリティアクションがトリガされて、アプリケーションセッション／接続に適用される。基本セキュリティアクションは、アプリケーションセッション／接続に対する基本セキュリティアクションを実行することによって適用される。
【００６７】
ステップ８５５において、セッション／接続持続時間は、基本セキュリティタイムリミットと比較される。ステップ８６０において、セッション／接続持続時間が基本セキュリティタイムリミットに到達したならば、セキュリティは、セキュリティ階層Ｃ２０６に強化される。セキュリティ階層Ｃ２０６中、中間セキュリティ規則によって定義された中間セキュリティアクションがトリガされて、アプリケーションセッション／接続に適用される。中間データセキュリティアクションは、アプリケーションセッション／接続に対して基本中間データセキュリティアクションを実行することによって適用される。
【００６８】
ステップ８６５において、セッション／接続持続時間は、中間セキュリティタイムリミットと比較される。ステップ８７０において、セッション／接続持続時間が中間セキュリティタイムリミットに到達したならば、セキュリティは、セキュリティ階層Ｄ２０８に強化される。セキュリティ階層Ｃ２０８中、進展したセキュリティ規則のセットによって定義された進展したセキュリティアクションがトリガされて、アプリケーションセッション／接続に適用される。進展したセキュリティアクションは、アプリケーションセッション／接続に対する進展したセキュリティアクションを実行することによって適用される。
【００６９】
図８に示したプロセスは、クライアント１０５のいずれかとアプリケーション１５０Ａ、１５０Ｂまたは１５０Ｃのいずれかとの間で確立されたアプリケーションセッション／接続ごとに反復され、それにより各アプリケーション１５０Ａ、１５０Ｂまたは１５０Ｃにテイラードされる、ハッカーに対する時間ベースのセキュリティを提供する。
【００７０】
本開示の実施形態は、以下の利点を有することができる。アプリケーションセッション／接続をプロファイルすることによってより良いセキュリティ決定を行う知識を増やす。アプリケーションセッション／接続をセキュリティ階層に相関させることは、より正しく判断できる(enlightened)セキュリティおよび意思決定に基づくことを可能にできる。相関したデータの分析の強化によってタイムリーな応答および完全なネットワークが危険にさらされる前にイシュー(issue)を封じ込めることが可能になる。データセンターのすべてのデバイスとのセキュリティ統合のためのアプリケーションをプロファイルすることは、ネットワークにおけるハッカー制御の阻止(containing)を改善する。時間段階のセッション／接続は、新しいレベルのセキュリティ分析を開く。より深化した分析は、ハッカーがプラットフォームにアクセスするために自分達のハッキングを何度も繰り返さなければならないように行うことができる。システムがハッキングされればますます、アプリケーション、プラグ接続され得るＯＳまたはプロトコルのホールをセンサが捕捉する機会が増える。
【００７１】
図９は、実施形態にかかる、ルータ１１５、ファイヤーウォール１２０、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、またはバックエンドサーバ１３５など、コンピュータ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、コンピュータデバイスは、プロセッサ９０２、メモリ９０３、ストレージモジュール９０４、入力モジュール（例えば、キーボード、マウスその他）９０６、ディスプレイモジュール９０７および通信インタフェース９０５、バス９０１を通

じてデータおよび制御信号を互いに交換すること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９０４は、１つまたは複数の非一時的なコンピュータ可読ストレージ媒体（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）として実装されて、本明細書に記載のセキュリティ特徴を実装するメモリ９０３と一体のプロセッサ９０２によって実行されるソフトウェア命令９４０（例えば、モジュール）を格納する。ソフトウェア命令の例は、ソフトウェアコードまたはプログラムコードになり得る。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もまた、プロセッサ９０２上で実行するストレージモジュール９０４に格納されてよい。

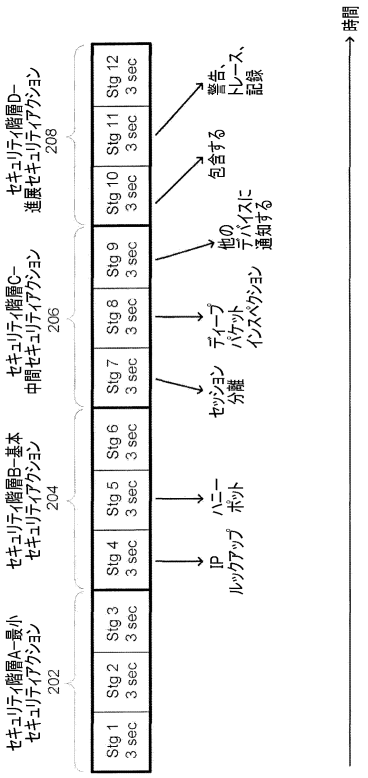
【００７２】

本開示を読んだ後、当業者は、セッション／接続分割セキュリティの付加的な代替設計をさらに認識することができる。従って、本開示の特定の実施形態およびアプリケーションが説明されているが、開示が本明細書に開示された正確な構造およびコンポーネントに限定されないことを理解されたい。当業者には明らかであろうさまざまな修正、変更および変形形態は、添付の特許請求の範囲で定義された本開示の精神および範囲から逸脱しない範囲で本明細書の本開示の方法および装置の配置、オペレーションおよび詳細に対して行われてもよい。

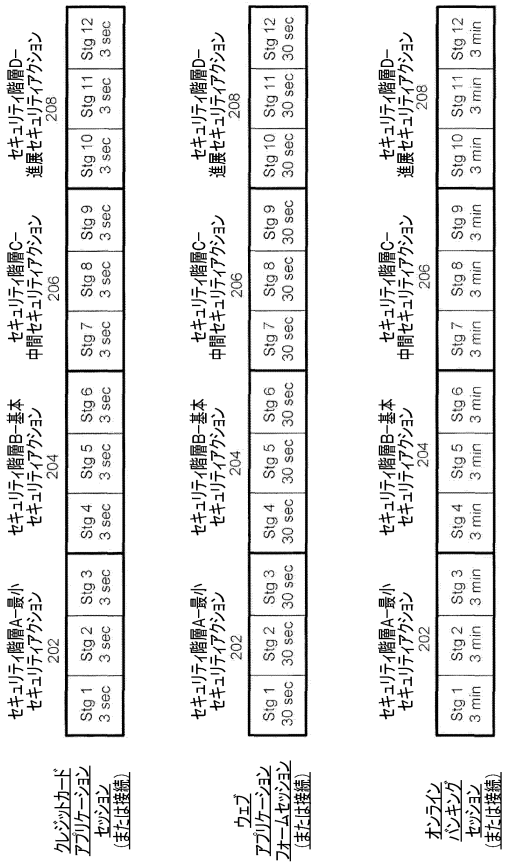
【図１】



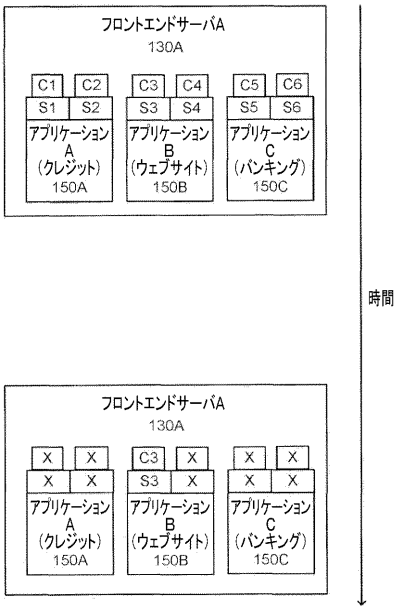
【図２】



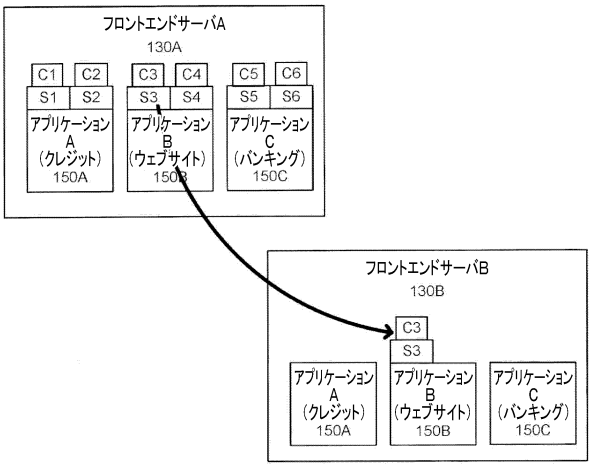
【図３】


セキュリティ階層A–最小セキュリティアクション 202
セキュリティ階層B–基本セキュリティアクション 204
セキュリティ階層C–中間セキュリティアクション 206
セキュリティ階層D–進展セキュリティアクション 208
Stg 1 3 sec
Stg 2 3 sec
Stg 3 3 sec
Stg 4 3 sec
Stg 5 3 sec
Stg 6 3 sec
Stg 7 3 sec
Stg 8 3 sec
Stg 9 3 sec
Stg 10 3 sec
Stg 11 3 sec
Stg 12 3 sec
クレジットカードアプリケーションセッション（または接続）
Stg 1 30 sec
Stg 2 30 sec
Stg 3 30 sec
Stg 4 30 sec
Stg 5 30 sec
Stg 6 30 sec
Stg 7 30 sec
Stg 8 30 sec
Stg 9 30 sec
Stg 10 30 sec
Stg 11 30 sec
Stg 12 30 sec
ウェブアプリケーションフォームセッション（または接続）
Stg 1 3 min
Stg 2 3 min
Stg 3 3 min
Stg 4 3 min
Stg 5 3 min
Stg 6 3 min
Stg 7 3 min
Stg 8 3 min
Stg 9 3 min
Stg 10 3 min
Stg 11 3 min
Stg 12 3 min
オンラインバンキングセッション（または接続）

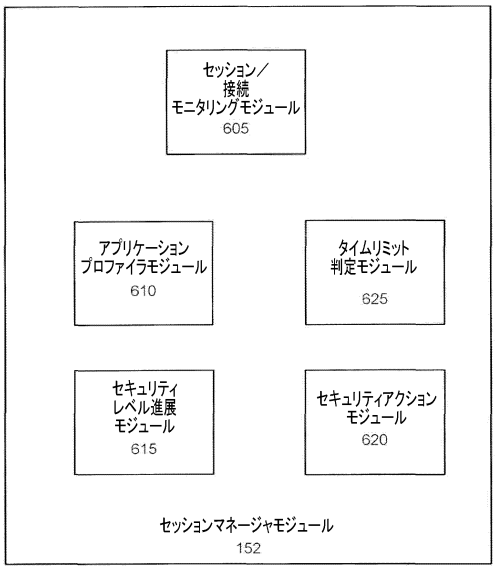
【図４】


フロントエンドサーバA
130A
C1 C2 C3 C4 C5 C6
S1 S2 S3 S4 S5 S6
アプリケーションA（クレジット）150A
アプリケーションB（ウェブサイト）150B
アプリケーションC（バンキング）150C
時間
フロントエンドサーバA
130A
X X C3 X X X
X X S3 X X X
アプリケーションA（クレジット）150A
アプリケーションB（ウェブサイト）150B
アプリケーションC（バンキング）150C

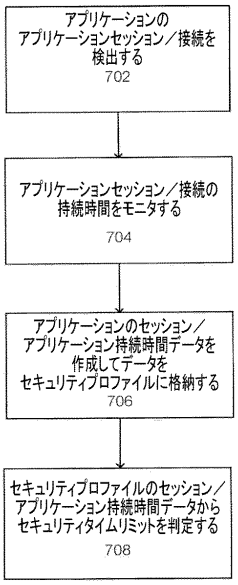
【図５】


フロントエンドサーバA
130A
C1 C2 C3 C4 C5 C6
S1 S2 S3 S4 S5 S6
アプリケーションA（クレジット）150A
アプリケーションB（ウェブサイト）150B
アプリケーションC（バンキング）150C
フロントエンドサーバB
130B
C3
S3
アプリケーションA（クレジット）150A
アプリケーションB（ウェブサイト）150B
アプリケーションC（バンキング）150C

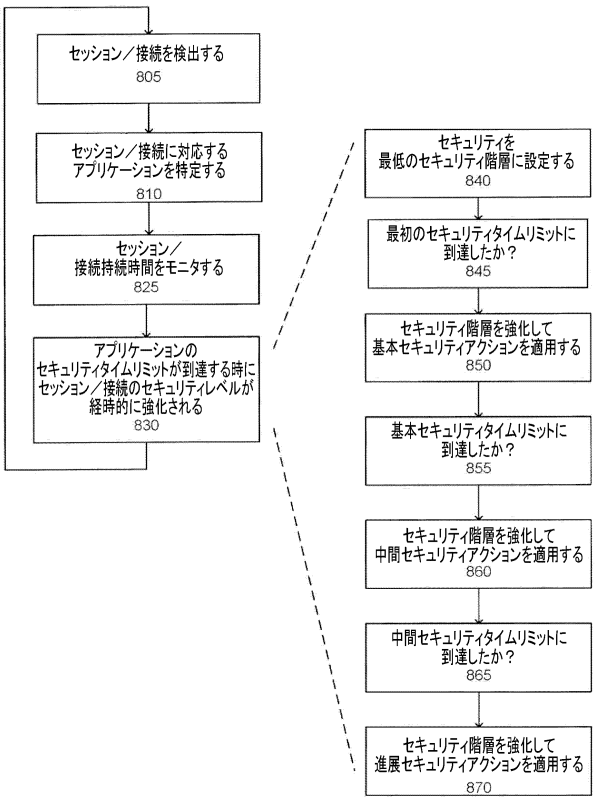
【図６】


セッション／接続モニタリングモジュール 605
アプリケーションプロファイラモジュール 610
タイムリミット判定モジュール 625
セキュリティレベル進展モジュール 615
セキュリティアクションモジュール 620
セッションマネージャモジュール 152

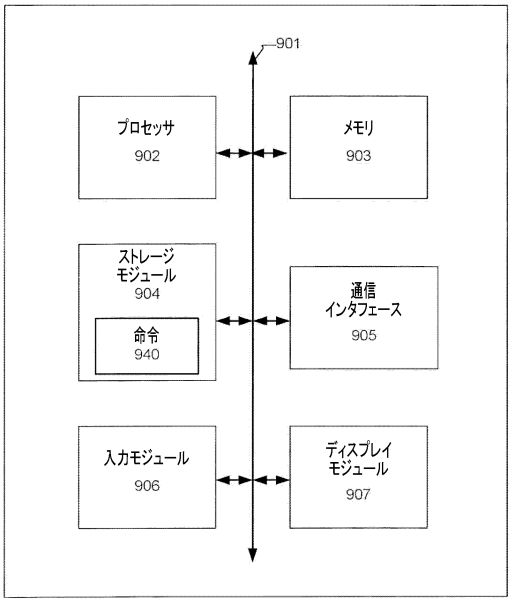
【図７】


アプリケーションの
アプリケーションセッション／接続を
検出する
702
アプリケーションセッション／接続の
持続時間をモニタする
704
アプリケーションのセッション／
アプリケーション持続時間データを
作成してデータを
セキュリティプロファイルに格納する
706
セキュリティプロファイルのセッション／
アプリケーション持続時間データから
セキュリティタイムリミットを判定する
708

【図８】


セッション／接続を検出する
805
セッション／接続に対応する
アプリケーションを特定する
810
セッション／
接続持続時間をモニタする
825
アプリケーションの
セキュリティタイムリミットが到達する時に
セッション／接続のセキュリティレベルが
経時的に強化される
830
セキュリティを
最低のセキュリティ階層に設定する
840
最初のセキュリティタイムリミットに
到達したか？
845
セキュリティ階層を強化して
基本セキュリティアクションを適用する
850
基本セキュリティタイムリミットに
到達したか？
855
セキュリティ階層を強化して
中間セキュリティアクションを適用する
860
中間セキュリティタイムリミットに
到達したか？
865
セキュリティ階層を強化して
進展セキュリティアクションを適用する
870

【図９】


901
プロセッサ
902
メモリ
903
ストレージ
モジュール
904
命令
940
通信
インタフェース
905
入力モジュール
906
ディスプレイ
モジュール
907

フロントページの続き

(56)参考文献 特開２００７－１７２０９３（ＪＰ，Ａ）
特開２０１０－２４４５１５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５５
Ｇ０６Ｆ　２１／１２