(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6228317号
(P6228317)
(45)発行日　平成29年11月8日(2017.11.8)　(24)登録日　平成29年10月20日(2017.10.20)

(51)Int.Cl.　F I
G06F 13/00 (2006.01)　G06F 13/00 510A

請求項の数 6 (全 11 頁)

(21)出願番号　特願2016-548233(P2016-548233)
(86)(22)出願日　平成26年12月12日(2014.12.12)
(65)公表番号　特表2017-505489(P2017-505489A)
(43)公表日　平成29年2月16日(2017.2.16)
(86)国際出願番号　PCT/KR2014/012240
(87)国際公開番号　WO2015/111842
(87)国際公開日　平成27年7月30日(2015.7.30)
審査請求日　平成28年8月18日(2016.8.18)
(31)優先権主張番号　10-2014-0007297
(32)優先日　平成26年1月21日(2014.1.21)
(33)優先権主張国　韓国(KR)

(73)特許権者　516219369
イーストセキュリティー　カンパニー　リミテッド
ＥＳＴＳＥＣＵＲＩＴＹ　ＣＯ．　ＬＴＤ．
大韓民国，１３７－８６７　ソウル，ソチョ－グ，バンポ－デロ　３（ソチョ－ドン，イーストビルディング）
３　Ｂａｎｐｏ－ｄａｅｒｏ（Ｓｅｏｃｈｏ－ｄｏｎｇ，ＥＳＴ　Ｂｕｉｌｄｉｎｇ）Ｓｅｏｃｈｏ－ｇｕ，Ｓｅｏｕｌ　１３７－８６７，Ｒｅｐｕｂｌｉｃ　ｏｆ　Ｋｏｒｅａ
(74)代理人　100121382
弁理士　山下　託嗣

最終頁に続く

(54)【発明の名称】イントラネットセキュリティシステム及びセキュリティ方法

(57)【特許請求の範囲】
【請求項１】
内部イントラネットにログインするために用いられる第１のアカウント情報と、外部システム（２０６）にログインするために用いられる第２のアカウント情報とを比較し、特定のクライアント（２０２）の前記イントラネットへのアクセスを遮断するセキュリティシステムであって、
前記クライアント（２０２）がインターネット網（２０４）を介して前記外部システム（２０６）にアクセスするとき、前記外部システム（２０６）にログインするために、前記外部システム（２０６）に伝送する前記第２のアカウント情報を抽出するアカウント情報抽出部（２２１）と、
ハッシュ関数を用いて前記アカウント情報抽出部（２２１）が抽出して伝達した前記第２のアカウント情報に対するハッシュ値を生成するハッシュ値生成部（２２２）と、
前記ハッシュ値生成部（２２２）から前記第２のアカウント情報のハッシュ値が伝達されると、前記第１のアカウント情報のハッシュ値と比較し、前記第１のアカウント情報と前記第２のアカウント情報が一致するかを確認するアカウント情報比較部（２２３）と、
前記第２のアカウント情報の抽出対象となるシステムのＵＲＬやＩＰアドレスについての情報を保存する管理対象目録ＤＢ（２２４）と、
前記第１のアカウント情報または前記第１のアカウント情報に対するハッシュ値のいずれか一つを保存するアカウント情報ＤＢ（２２５）と、
を備え、

前記イントラネットを管理するイントラネットサーバ（２１０）は、前記第１のアカウント情報と前記第２のアカウント情報が一致する場合、前記クライアント（２０２）が前記イントラネットにアクセスすることを遮断することを特徴とするイントラネットセキュリティシステム。

【請求項２】
前記第１のアカウント情報は、前記イントラネットにアクセスするためのＩＤとパスワードを含み、前記第２のアカウント情報は、前記外部システム（２０６）にアクセスするためのＩＤとパスワードを含むことを特徴とする請求項１に記載のイントラネットセキュリティシステム。
【請求項３】
前記アカウント情報抽出部（２２１）は、前記クライアント（２０２）がアクセスする前記外部システム（２０６）が、前記管理対象目録ＤＢ（２２４）に保存されたシステムであるときにのみ、前記第２のアカウント情報を抽出することを特徴とする請求項１に記載のイントラネットセキュリティシステム。
【請求項４】
内部イントラネットにログインするために用いられる第１のアカウント情報と、外部システム（２０６）にログインするために用いられる第２のアカウント情報とを比較し、特定のクライアント（２０２）の前記イントラネットへのアクセスを遮断するセキュリティ方法であって、
前記イントラネットを管理するイントラネットサーバ（２１０）が、前記クライアント（２０２）にセキュリティシステム（２２０）をインストールした後、前記第２のアカウント情報の抽出対象となるシステムのＵＲＬやＩＰアドレスについての情報と共に、前記第１のアカウント情報を前記セキュリティシステム（２２０）に伝送して保存する第１の段階と、
前記クライアント（２０２）がインターネット網（２０４）を介して前記外部システム（２０６）にアクセスするとき、前記外部システム（２０６）にログインするために、前記外部システム（２０６）に伝送する前記第２のアカウント情報を、アカウント情報抽出部（２２１）が抽出する第２の段階と、
ハッシュ値生成部（２２２）が、前記第２の段階で抽出された前記第２のアカウント情報に対するハッシュ値を生成する第３の段階と、
アカウント情報比較部（２２３）が、前記ハッシュ値生成部（２２２）から伝達された前記第２のアカウント情報のハッシュ値と、アカウント情報ＤＢ（２２５）に保存された前記第１のアカウント情報のハッシュ値とを互いに比較する第４の段階と、
前記第４の段階の比較結果、前記第１のアカウント情報と前記第２のアカウント情報が同じであれば、前記イントラネットサーバ（２１０）は、前記クライアント（２０２）が前記イントラネットサーバ（２１０）にアクセスすることを遮断する第５の段階と、
を含むことを特徴とするイントラネットセキュリティ方法。
【請求項５】
前記第１のアカウント情報は、前記イントラネットにアクセスするためのＩＤとパスワードを含み、前記第２のアカウント情報は、前記外部システム（２０６）にアクセスするためのＩＤとパスワードとを含むことを特徴とする請求項４に記載のイントラネットセキュリティ方法。
【請求項６】
前記アカウント情報抽出部（２２１）は、前記クライアント（２０２）がアクセスする前記外部システム（２０６）が、前記セキュリティシステム（２２０）に保存されたシステムであるときにのみ、前記第２のアカウント情報を抽出することを特徴とする請求項４に記載のイントラネットセキュリティ方法。
【発明の詳細な説明】
【技術分野】

【０００１】
本発明は、イントラネットセキュリティシステム及びセキュリティ方法に関し、より詳しくは、企業内部のイントラネットと外部のインターネット網に同時にアクセス可能なクライアントが、外部システムにログインするためにアカウント情報を入力した時、イントラネットのアカウント情報と同一であるかを分析し、同一である場合は、イントラネットへのアクセスを遮断するイントラネットセキュリティシステム及びセキュリティ方法に関する。
【背景技術】
【０００２】
イントラネットは、企業体、研究所、学校等の組織内部における各種業務をインターネットのような容易な方法で処理可能にしたネットワーク環境であって、限定された空間でのネットワーク環境を基盤として、ウェブのような容易なインターフェースで基幹業務を行うようにしたものである。イントラネットは、ＬＡＮ上のサーバとクライアントとの間に情報サービス、すなわち、企業内の情報通信網上において運用される。
【０００３】
イントラネットは、インターネットに適用される技術であるＴＣＰ／ＩＰ、ＨＴＴＰ、ＨＴＭＬ、ＣＧＩ等と内部のウェブシステムを活用して、企業内の情報システムを構築し、このように構築されたシステムにグループウェアを導入すると、インターネットと同一のブラウザでグループウェアを用いることができる。
【０００４】
最近、数回のハッキング事件により、多くの使用者のアカウント情報がハッカーに流出された。また、多くの人が、自分の個人的に用いる外部システムのアカウント情報と、会社で用いる社内イントラネットシステムのアカウント情報とを同時にして用いるが、これは、社内ネットワークにハッカーが侵入可能な深刻な欠陥として作用する。
【０００５】
これを防ぐために、多くの企業では、周期的に暗号を変更することを勧告してはいるが、これは、勧告であるだけで、強制する手段がないので、社員が変えなければ、意味がない。また、多くの外部サービス会社も、半強制的に周期的な暗号変更を行うようにしているが、社内アカウントの暗号を周期的に変更するように強制しても、外部サービスにおいても同一の暗号に変えてしまうので、周期的な変更だけでは、大きな意味がない。
【０００６】
このようなイントラネットの弱いセキュリティ問題を解決するために、外部インターネットと内部イントラネットにアクセスするシステムを物理的に分離する技術が開示されている。
【０００７】
図１は、従来技術によるデュアルコンピュータを概略的に示したブロック図である。
【０００８】
図１に示すように、デュアルコンピュータは、入力インターフェースであるキーボード７２とマウス７４、デュアルコンピュータ本体１００、及びディスプレイ装置３０を含む。
【０００９】
デュアルコンピュータ本体１００は、第１のメインボード１１０、第２のメインボード１６０、スイッチ部１０５、及びＵＳＢメモリポート１０７を含む。
【００１０】
第１のメインボード１１０は、イントラネット動作モードで、イントラネット網１０にアクセスされ、必要な情報を送受信し、第２のメインボード１６０は、インターネット動作モードで、インターネット網２０にアクセスされ、必要な情報を送受信する。
【００１１】
スイッチ部１０５は、デュアルコンピュータを、イントラネット動作モードとインターネット動作モードのいずれか一つを選択する動作モード遂行命令を受ける。

【００１２】
また、スイッチ部１０５は、動作モードが選択されると、キーボード７２またはマウス７４から入力された命令を、選択された動作モードに対応する第１のメインボード１１０と第２のメインボード１６０のいずれか一つに提供する。すなわち、イントラネット動作モードでは、スイッチ部１０５が、入力される命令を第１のメインボード１１０に提供し、インターネット動作モードでは、スイッチ部１０５が、入力される命令を第２のメインボード１６０に提供する。
【００１３】
ディスプレイ装置３０は、現在の動作モードに対応して、第１のメインボード１１０または第２のメインボード１６０から出力される画像データを、パネルを通じて表示する。
【００１４】
しかしながら、このような技術を適用しても、第三者が外部システムにおいて用いられるアカウント情報を獲得してしまうと、これと同一のアカウント情報でログイン可能なイントラネットに無断でアクセスして情報を流出させることができるので、根本的な問題は解決されないという限界があった。
【発明の概要】
【発明が解決しようとする課題】
【００１５】
本発明は、上記問題点に鑑みなされたものであり、その目的は、社内イントラネットを用いる全ての職員が、指定された外部システムにログインするときに用いるアカウント情報とは異なるアカウント情報でイントラネットにアクセスするように強制することにより、イントラネットのセキュリティ状態を維持可能とする、イントラネットセキュリティシステム及びセキュリティ方法を提供することにある。
【００１６】
本発明の他の目的は、外部システムに用いられるアカウント情報とイントラネットに用いられるアカウント情報を、ハッシュ値に変換して保存し、２つの情報を比較する過程でもハッシュ値を用いるようにし、これにより、アカウント情報の流出と盗用の可能性を最小化する、イントラネットセキュリティシステム及びセキュリティ方法を提供することにある。
【課題を解決するための手段】
【００１７】
上述した目的を達成するために、本発明は、内部イントラネットにログインするために用いられる第１のアカウント情報と、外部システム２０６にログインするために用いられる第２のアカウント情報とを比較し、特定のクライアント２０２の前記イントラネットへのアクセスを遮断するセキュリティシステムであって、前記クライアント２０２がインターネット網２０４を介して前記外部システム２０６にアクセスするとき、前記外部システム２０６にログインするために、前記外部システム２０６に伝送する前記第２のアカウント情報を抽出するアカウント情報抽出部２２１と、ヘッシュ関数を用いて前記アカウント情報抽出部２２１が抽出して伝達した前記第２のアカウント情報に対するハッシュ値を生成するハッシュ値生成部２２２と、前記ハッシュ値生成部２２２から前記第２のアカウント情報のハッシュ値が伝達されると、前記第１のアカウント情報のハッシュ値と比較し、前記第１のアカウント情報と前記第２のアカウント情報が一致するかを確認するアカウント情報比較部２２３と、前記第２のアカウント情報の抽出対象となるシステムのＵＲＬやＩＰアドレスについての情報を保存する管理対象目録ＤＢ２２４と、前記第１のアカウント情報または前記第１のアカウント情報に対するハッシュ値のいずれか一つを保存するアカウント情報ＤＢ２２５と、を備え、前記イントラネットを管理するイントラネットサーバ２１０は、前記第１のアカウント情報と前記第２のアカウント情報が一致する場合、前記クライアント２０２が前記イントラネットにアクセスすることを遮断することを特徴とする。
【００１８】

前記第１のアカウント情報は、前記イントラネットにアクセスするためのＩＤとパスワードを含み、前記第２のアカウント情報は、前記外部システム２０６にアクセスするためのＩＤとパスワードを含むことを特徴とする。

【００１９】

前記アカウント情報抽出部２２１は、前記クライアント２０２がアクセスする前記外部システム２０６が、前記管理対象目録ＤＢ２２４に保存されたシステムであるときにのみ、前記第２のアカウント情報を抽出することを特徴とする。

【００２０】

上述した他の目的を達成するために、本発明は、内部イントラネットにログインするために用いられる第１のアカウント情報と、外部システム２０６にログインするために用いられる第２のアカウント情報とを比較し、特定のクライアント２０２の前記イントラネットへのアクセスを遮断するセキュリティ方法であって、前記イントラネットを管理するイントラネットサーバ２１０が、前記クライアント２０２にセキュリティシステム２２０をインストールした後、前記第２のアカウント情報の抽出対象となるシステムのＵＲＬやＩＰアドレスについての情報と共に、前記第１のアカウント情報を前記セキュリティシステム２２０に伝送して保存する第１の段階と、前記クライアント２０２がインターネット網２０４を介して前記外部システム２０６にアクセスするとき、前記外部システム２０６にログインするために、前記外部システム２０６に伝送する前記第２のアカウント情報を、アカウント情報抽出部２２１が抽出する第２の段階と、ハッシュ値生成部２２２が、前記第２の段階で抽出された前記第２のアカウント情報に対するハッシュ値を生成する第３の段階と、アカウント情報比較部２２３が、前記ハッシュ値生成部２２２から伝達された前記第２のアカウント情報のハッシュ値と、アカウント情報ＤＢ２２５に保存された前記第１のアカウント情報のハッシュ値とを互いに比較する第４の段階と、前記第４の段階の比較結果、前記第１のアカウント情報と前記第２のアカウント情報が同じであれば、前記イントラネットサーバ２１０は、前記クライアント２０２が前記イントラネットサーバ２１０にアクセスすることを遮断する第５の段階と、を含むことを特徴とする。

【００２１】

前記第１のアカウント情報は、前記イントラネットにアクセスするためのＩＤとパスワードを含み、前記第２のアカウント情報は、前記外部システム２０６にアクセスするためのＩＤとパスワードを含むことを特徴とする。

【００２２】

前記アカウント情報抽出部２２１は、前記クライアント２０２がアクセスする前記外部システム２０６が、前記セキュリティシステム２２０に保存されたシステムであるときにのみ、前記第２のアカウント情報を抽出することを特徴とする。

【発明の効果】

【００２３】

本発明によれば、外部インターネットサービスシステムにおいて用いられるアカウント情報が流出しても、その職員が社内イントラネットにアクセスするために用いるアカウント情報とは異なるので、アカウント情報を取得した第三者が無断でイントラネットにアクセスすることを防止することができる。

【図面の簡単な説明】

【００２４】

【図１】従来技術によるデュアルコンピュータを概略的に示すブロック図である。

【図２】本発明の第１実施例によるセキュリティシステムの構造を示すブロック図である。

【図３】セキュリティシステムの内部構成を示すブロック図である。

【図４】セキュリティシステムの動作過程を示すフローチャートである。

【図５】外部システムが提供するログインページにおける入力領域を示す概念図である。

【図６】本発明の第２実施例によるセキュリティシステムの構造を示すブロック図である。

【発明を実施するための形態】
【００２５】
以下、添付した図面を参照して、本発明による好適な実施例について詳述する。
【００２６】
図２は、本発明の第１実施例によるセキュリティシステムの構造を示すブロック図であり、図３は、セキュリティシステムの内部構成を示すブロック図であり、図４は、セキュリティシステムの動作過程を示すフローチャートであり、図５は、外部システムが提供するログインページにおける入力領域を示す概念図である。
【００２７】
本発明の第１実施例による「イントラネットセキュリティシステム」（以下、「セキュリティシステム」という）は、外部インターネットと社内イントラネットに同時にアクセス可能なクライアント２０２にインストールされる。
【００２８】
セキュリティシステム２２０は、ハードウェア的にインストールされることもあるが、一般に、別途の物理的装置無しで、ソフトウェア的にクライアント２０２のシステムの内部にインストールされる。イントラネットサーバ２１０は、イントラネットにアクセス可能に許容されたクライアント２０２にソフトウェアを伝送し、セキュリティシステム２２０をインストールする。
【００２９】
個別のクライアント２０２は、インターネット網２０４を介して外部システム２０６にアクセスして外部サービスを用い、またはイントラネットにアクセスして社内データを呼び出すことができる。イントラネットには、外部のインターネット網２０４からの不法侵入を防止するためにファイアウォール２０８が設けられ、ファイアウォール２０８を通過してイントラネットサーバ２１０にアクセスすると、イントラネット内部に連結された各種の処理装置２１２を実行させることができる。
【００３０】
個別のＰＣやモバイル端末機で構成されるクライアント２０２が、インターネット網２０４にアクセスして外部サービスを用い、またはイントラネットにアクセスして社内情報を用いることは、従来、開示された技術と同一であるので、重複を避けるために、この部分についての詳細な説明を省略する。
【００３１】
図３は、クライアント２０２にインストールされるセキュリティシステム２２０の構成を示している。
【００３２】
セキュリティシステム２２０は、アカウント情報抽出部２２１、ハッシュ値生成部２２２、アカウント情報比較部２２３、管理対象目録ＤＢ２２４、アカウント情報ＤＢ２２５からなる。
【００３３】
アカウント情報抽出部２２１は、社員がイントラネットに連結されたクライアント２０２を用いて、インターネット網２０４に連結された外部システム２０６にアクセスし、外部システム２０６が提供するサービスを用いるためにログイン情報を伝送するとき、伝送されるログイン情報を抽出してハッシュ値生成部２２２に伝達する。
【００３４】
クライアント２０２からイントラネットサーバ２１０に伝送されるログイン情報を第１のアカウント情報と定義し、外部システム２０６に伝送されるログイン情報を第２のアカウント情報と定義する。本発明において、第２のアカウント情報は、社員が外部システム２０６にログインするために登録したアカウント情報であって、ＩＤとパスワード、名前、住民登録番号、住所等の個人情報を意味する。セキュリティシステム２２０は、外部システム２０６にアクセスしたクライアント２０２が、特定のログイン情報入力ページに第２のアカウント情報を入力するかを監視し、予め定められた形式の第２のアカウント情報

が伝送されると、これをキャプチャーする。

【００３５】

また、第１のアカウント情報は、社員がイントラネット（またはイントラネットサーバ）にログインするために登録したアカウント情報であって、第２のアカウント情報と同一でありまたは類似した情報を含む。会社や学校、研究機関等に構築されたイントラネットである場合は、固有番号や社員番号、ＩＤ、パスワード、所属部署、職責等が含まれてもよい。

【００３６】

アカウント情報抽出部２２１は、クライアント２０２から外部システム２０６に伝送される情報のうち、第２のアカウント情報を抽出し、使用者の識別情報と共に、ハッシュ値生成部２２２に伝達する。しかし、クライアント２０２がアクセスする全ての外部システム２０６のアカウント情報を抽出することは意味がなく、使用者が多くアクセスするシステムを選択して監視することが好ましい。

【００３７】

セキュリティシステム２２０には、第２のアカウント情報の抽出対象となるシステム（ウェブサイト等）の情報が保存されるところ、管理対象となるシステムのＵＲＬやＩＰアドレス等に対する情報は、管理対象目録ＤＢ２２４に保存される。イントラネットの管理者は、予め管理対象となるシステムの目録を生成して、管理対象目録ＤＢ２２４に保存し、周期的または特別なイベントが発生するごとに、管理対象の情報を追加または修正する。

【００３８】

クライアント２０２から外部システム２０６に伝送される情報のうち、どれがログインのためのアカウント情報であるかを確認するためには、入力フィールドのＩＤ値を確認しなければならない。すなわち、外部システム２０６が提供するウェブページにおいて、使用者がＩＤとパスワードを入力するとき、ブラウザに含まれたＩＤ及びパスワードの入力フィールドのＩＤ値を確認する。また、クライアント２０２から伝送された情報が当該ＩＤ値を有する入力フィールドに入力されるとき、ＩＤとパスワードを入力したものとみなし、アカウント情報の抽出が行われる。

【００３９】

図５に示すように、ブラウザが実行されたとき、ＩＤとパスワードを入力する部分（入力領域）のＩＤ値を確認して、ここが検索語を入力する箇所であるか、ログイン情報を入力する箇所であるかを把握することができる。

【００４０】

エクスプローラーやクローム、サファリ等のインターネットブラウザにおいて、入力フィールドのＩＤ値を確認して、ログインのためのアカウント情報であるかを把握することは、従来、開示された通常の技術であって、当業者にとって容易な事項であるので、詳細な説明を省略する。

【００４１】

ハッシュ値生成部２２２は、伝達された第２のアカウント情報を用いてハッシュ値を生成する。ハッシュ値は、ヘッシュ関数の結果から作られるコードであって、入力値の長さにかかわらず、一定の長さを有する値に変換されたものである。対象となる情報やファイルが修正または変更されると、出力されるハッシュ値が異なるので、情報やファイルの同一性を把握するための方法として用いられる。ハッシュ値を生成するための関数としては、ＭＤ５のように既存に公開されたアルゴリズムを用いてもよい。

【００４２】

生成した第２のアカウント情報に対するハッシュ値は、アカウント情報比較部２２３に伝達される。アカウント情報比較部２２３は、第２のアカウント情報のハッシュ値を用いて同一のハッシュ値を有する情報があるかを把握するが、このとき、アカウント情報ＤＢ２２５に保存されたファイルを用いる。

【００４３】

アカウント情報ＤＢ２２５は、ハッシュ値に変換された第１のアカウント情報を保存する。イントラネットの管理者は、特定のクライアント２０２を用いる内部使用者（社員、研究員、教授等）のイントラネットログイン情報（第１のアカウント情報）を、ヘッシュ関数を用いてハッシュ値に変換した後、アカウント情報ＤＢ２２５に保存する。第１のアカウント情報のハッシュ値は、使用者を識別可能な情報と共に保存することが好ましい。

【００４４】

アカウント情報比較部２２３は、ハッシュ値生成部２２２から使用者の識別情報と共に、第２のアカウント情報のハッシュ値が伝達されると、当該使用者の識別情報と一致する識別情報を有する第１のアカウント情報のハッシュ値を、アカウント情報ＤＢ２２５から呼び出す。また、アカウント情報比較部２２３は、特定使用者の第１のアカウント情報と第２のアカウント情報のそれぞれのハッシュ値を互いに比較し、２つの情報（第１のアカウント情報と第２のアカウント情報）が一致するかを確認する。アカウント情報比較部２２３の比較結果、第１のアカウント情報と第２のアカウント情報が同一であれば、ハッキングや第三者による盗用を防止するために、イントラネットへのアクセスを遮断する。

【００４５】

このような構成を用いてセキュリティシステム２２０が行う動作過程について、図４を参照して説明する。

【００４６】

先ず、イントラネットサーバ２１０がクライアント２０２にインストールプログラムを伝送し、セキュリティシステム２２０をインストールする（Ｓ１０２）。

【００４７】

また、イントラネットサーバ２１０は、第１のアカウント情報をセキュリティシステム２２０に伝送し、セキュリティシステム２２０は、これをアカウント情報ＤＢ２２５に保存する（Ｓ１０４）。アカウント情報ＤＢ２２５に保存される第１のアカウント情報は、一般に、ハッシュ値に変換された状態で保存されるが、単純なテキスト情報として保存した後、追って比較過程においてハッシュ値に変換してもよい。

【００４８】

また、イントラネットサーバ２１０は、アカウント情報の管理対象となるサイトの目録と情報をセキュリティシステム２２０に伝送して保存する（Ｓ１０６）。管理対象の目録と情報は、管理対象目録ＤＢ２２４に保存される。

【００４９】

セキュリティシステム２２０のインストールと、第１のアカウント情報、管理対象目録の保存が完了すると、セキュリティシステム２２０の監視が開始される（Ｓ１０８）。

【００５０】

セキュリティシステム２２０は、クライアント２０２がインターネット網２０４を介して監視対象目録に存在する外部システム２０６にアクセスするかを持続的に監視する（Ｓ１１０）。

【００５１】

クライアント２０２がアクセスしたサイトが監視対象目録にあり、使用者がＩＤとパスワード（第２のアカウント情報）を外部システム２０６に伝送した場合、アカウント情報抽出部２２１は、伝送された第２のアカウント情報（ＩＤとパスワードを含む）を抽出してハッシュ値生成部２２２に伝達する（Ｓ１１２）。

【００５２】

ハッシュ値生成部２２２は、伝達された第２のアカウント情報のハッシュ値を生成し、アカウント情報比較部２２３に伝達する（Ｓ１１４）。

【００５３】

アカウント情報比較部２２３は、ハッシュ値生成部２２２から伝達された第２のアカウント情報のハッシュ値と、アカウント情報ＤＢ２２５に保存された第１のアカウント情報のハッシュ値とを互いに比較する（Ｓ１１６、Ｓ１１８）。

【００５４】

比較の結果、第１のアカウント情報と第２のアカウント情報が異なると、第三者によるハッキングの危険が少ないものとみなし、イントラネットへのアクセスを許容する（Ｓ１２０）。

【００５５】

しかし、特定使用者の第１のアカウント情報と第２のアカウント情報が同一であれば、その使用者は、イントラネットにアクセスするためのＩＤ及びパスワードと同一であるＩＤ及びパスワードをもって外部システム２０６にアクセスするとみなされる。この場合は、外部流出による第三者のハッキングの危険があるものとみなし、当該クライアント２０２がイントラネットにアクセスすることを遮断する（Ｓ１２２）。

【００５６】

また、管理者は、遮断されたクライアント２０２の使用者に、イントラネットにアクセスするためのログイン情報（第１のアカウント情報）を変更しなければ、イントラネットにアクセスできない旨を通知する。このような通知を受け、使用者が適切な措置を取った場合は、情報が一致するか否かをもう一度確認した後、イントラネットへのアクセスを許容する。

【００５７】

図６は、本発明の第２実施例によるセキュリティシステムの構造を示すブロック図である。

【００５８】

第１実施例によるセキュリティシステム２２０は、インターネット網２０４とイントラネットにアクセスするクライアント２０２にインストールされたが、第２実施例では、セキュリティシステム２２０が、イントラネットの内部のデータ送受信を管理するイントラネットサーバ２１０にインストールされる。

【００５９】

この場合、外部システム２０６に伝送する第２のアカウント情報の抽出は、クライアント２０２が行い、抽出された第２のアカウント情報を受け、ハッシュ値の生成、第１のアカウント情報との比較、第１のアカウント情報の保存、管理対象目録の保存等を行うことは、イントラネットサーバ２１０の内部にインストールされたセキュリティシステム２２０が行うことになる。

【００６０】

必要に応じて、アカウント情報抽出部２２１と管理対象目録ＤＢ２２４は、クライアント２０２の内部に、ハッシュ値生成部２２２、アカウント情報比較部２２３、アカウント情報ＤＢ２２５は、イントラネットサーバ２１０に分けてインストールしてもよい。

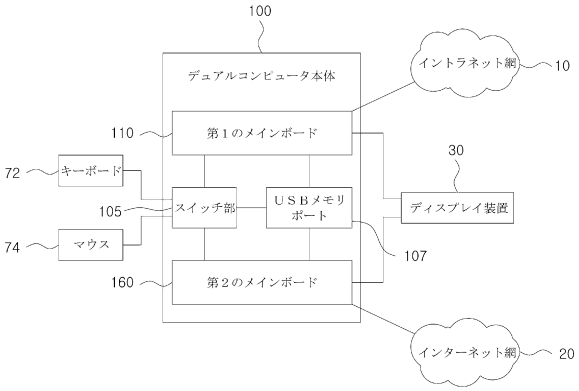
【００６１】

図６に示したセキュリティシステム２２０の構成は、図３に示したセキュリティシステム２２０の構成と同一であるので、重複する説明を省略する。

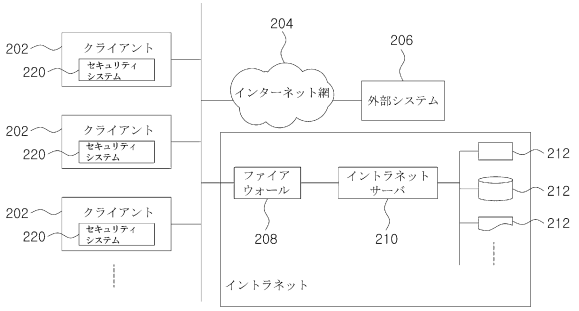
【００６２】

以上、添付した図面を参照して、本発明の好適な実施例について説明したが、上述した本発明の技術的な構成は、本発明の属する技術の分野における当業者であれば、本発明のその技術的思想や必須的特徴を変更せず、他の具体的な形態に実施され得ることが理解されるだろう。このため、上述した実施例は、全ての面において、例示的であり、限定的なものではないと理解されなければならず、本発明の範囲は、上述した詳細な説明よりも後述する特許請求の範囲により定められ、特許請求の範囲の意味及び範囲、またその等価概念から導出される全ての変更または変形された形態が、本発明の範囲に含まれるものと解釈されなければならない。

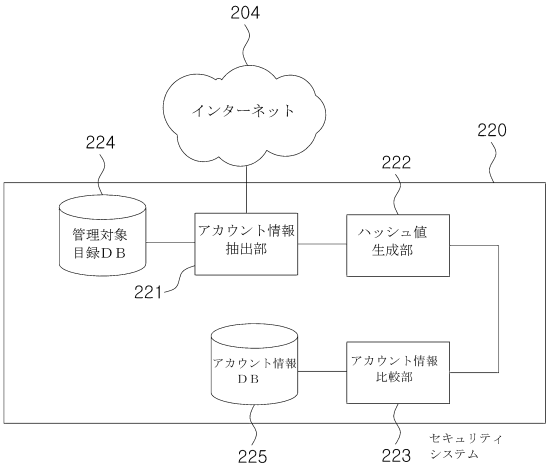
【図１】



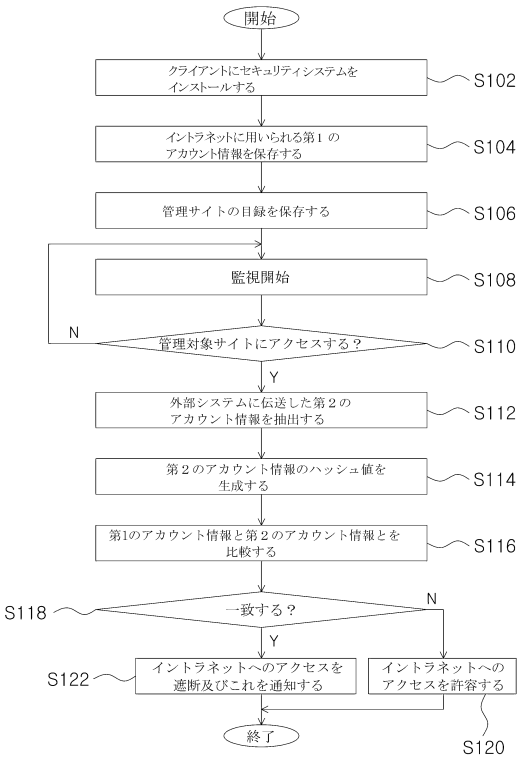
【図２】



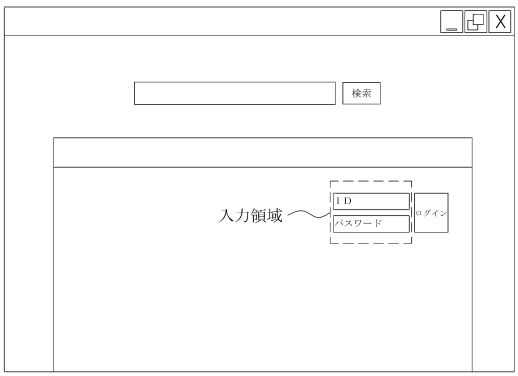
【図３】



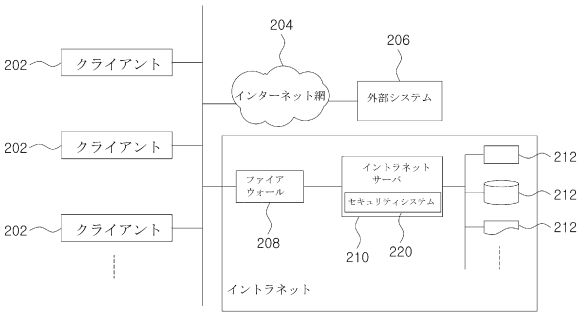
【図４】



【図５】



【図６】



フロントページの続き

(72)発明者　キム，ジュン　ソブ
大韓民国，１３４－０５３　ソウル，ガンドン－グ，ゴドク－ロ，１３０，１１１－６０１（アムサードン，プライアーパレス）
(72)発明者　ベク，ビョン　ミン
大韓民国，１４３－２２４　ソウル，グァンジン－グ，ヨンマサン－ロ　２４－ギル，１３，１－２０５（ジュンゴク－ドン，シニャン　ヴィラ）

審査官　佐々木　洋

(56)参考文献　特開２０１２－２１２２１１（ＪＰ，Ａ）
特開２０００－３２２３８０（ＪＰ，Ａ）
特開２０１１－２４２８３４（ＪＰ，Ａ）
特開２０００－００３３３４（ＪＰ，Ａ）
特開２０１５－１０３０９０（ＪＰ，Ａ）
米国特許出願公開第２０１３／０１２５２２１（ＵＳ，Ａ１）
米国特許出願公開第２０１１／０２９６００３（ＵＳ，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　１３／００