(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2015-225500
(P2015-225500A)
(43)公開日　平成27年12月14日(2015.12.14)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/55	(2013.01)	G06F	21/00	155A	5K201
H04M 3/42	(2006.01)	H04M	3/42	A	
G06F 21/31	(2013.01)	G06F	21/20	131A	

審査請求 未請求　請求項の数 4　OL　（全 19 頁）

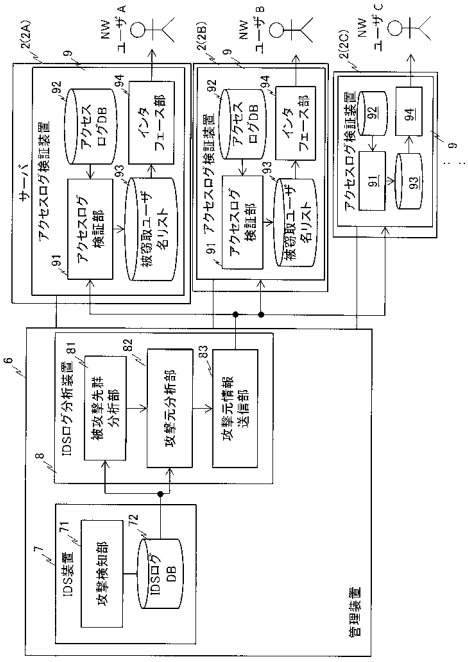
(21)出願番号　特願2014-109914 (P2014-109914)
(22)出願日　平成26年5月28日 (2014.5.28)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100113608
弁理士　平川　明
(74)代理人　100105407
弁理士　高田　大輔
(72)発明者　本多　聡美
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　鳥居　悟
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Fターム(参考)　5K201 AA09 BC27 CB01 CB06 CB16 CC03 DC04 EC06 FA04

(54)【発明の名称】認証用情報の窃取検知方法、認証用情報の窃取検知装置、及びプログラム

(57)【要約】
【課題】ログイン要求元の情報を手掛かりにアクセスログから認証用情報が窃取されたことを検知可能とする。
【解決手段】ログイン成功により所定サービスをユーザに提供する通信装置に関して、ユーザがログインに用いる認証用情報の窃取を情報処理装置が検知する方法であって、情報処理装置が、ログイン要求元の情報と、ログイン要求元がログインに際して通信装置に提示した認証用情報と、当該認証用情報を用いたログインの成否を示す情報とを含むログイン要求毎のレコードを記憶し、通信装置に対する攻撃元の情報を通信装置が存するネットワークの管理装置から受信し、攻撃元の情報と一致するログイン要求元の情報を含むレコードにログインの成功を示す情報が記憶されているときに当該レコード中の認証用情報が攻撃元に窃取されたと判定し、窃取されたと判定した認証用情報を出力することを含む。
【選択図】図４



【特許請求の範囲】
【請求項１】
ログイン成功により所定サービスをユーザに提供する通信装置に関して、ユーザがログインに用いる認証用情報の窃取を情報処理装置が検知する方法であって、
前記情報処理装置が、ログイン要求元の情報と、ログイン要求元がログインに際して前記通信装置に提示した認証用情報と、当該認証用情報を用いたログインの成否を示す情報とを含むログイン要求毎のレコードを記憶し、
前記情報処理装置が、前記通信装置に対する攻撃元の情報を前記通信装置が存するネットワークの管理装置から受信し、
前記情報処理装置が、前記攻撃元の情報と一致する前記ログイン要求元の情報を含むレコードにログインの成功を示す情報が記憶されているときに当該レコード中の認証用情報が前記攻撃元に窃取されたと判定し、
前記攻撃元に窃取されたと判定した認証用情報を出力する
ことを含む認証用情報の窃取検知方法。
【請求項２】
前記情報処理装置は、或る攻撃元が或る時刻で前記通信装置を含む被攻撃先群に実質的に同数と認め得る回数の攻撃を行ったことを示す情報が前記管理装置で得られているときに前記或る攻撃元の情報を受信する
請求項１に記載の認証用情報の窃取検知方法。
【請求項３】
ログイン成功により所定サービスをユーザに提供する通信装置に関して、ユーザがログインに用いる認証用情報の窃取を検知する装置であって、
ログイン要求元の情報と、ログイン要求元がログインに際して前記通信装置に提示した認証用情報と、当該認証用情報を用いたログインの成否を示す情報とを含むログイン要求毎のレコードを記憶する記憶装置と、
前記通信装置に対する攻撃元の情報を前記通信装置が存するネットワークの管理装置から受信する受信装置と、
前記攻撃元の情報と一致する前記ログイン要求元の情報を含むレコードにログインの成功を示す情報が記憶されているときに当該レコード中の認証用情報が前記攻撃元に窃取されたと判定する制御装置と、
前記攻撃元に窃取されたと判定した認証用情報を出力する出力装置と
を含む認証用情報の窃取検知装置。
【請求項４】
ログイン成功により所定サービスをユーザに提供する通信装置に関して、ユーザがログインに用いる認証用情報の窃取を検知する処理をコンピュータに実行させるプログラムであって、
ログイン要求元の情報と、ログイン要求元がログインに際して前記通信装置に提示した認証用情報と、当該認証用情報を用いたログインの成否を示す情報とを含むログイン要求毎のレコードを記憶するステップと、
前記通信装置に対する攻撃元の情報を前記通信装置が存するネットワークの管理装置から受信するステップと、
前記攻撃元の情報と一致する前記ログイン要求元の情報を含むレコードにログインの成功を示す情報が記憶されているときに当該レコード中の認証用情報が前記攻撃元に窃取されたと判定するステップと、
前記攻撃元に窃取されたと判定した認証用情報を出力するステップと
をコンピュータに実行させるプログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本開示は、認証用情報の窃取検知方法、認証用情報の窃取検知装置、及びプログラムに

関する。
【背景技術】
【０００２】
従来、ネットワーク管理者（ＮＷ管理者）が管理するネットワークに接続された通信装置（例えば、サーバ）をユーザ（ネットワークユーザ（ＮＷユーザ）と称する）に貸与することが行われている。ＮＷユーザは、貸与された通信装置を用いてエンドユーザに対し所定のサービス（Ｗｅｂサービス、メールサービス、クラウドサービス等）を提供する。
【０００３】
典型的には、ネットワークサービスプロバイダ（ＮＳＰ）がＮＷ管理者として管理するネットワーク上のサーバを企業や学校のような各種の団体或いは個人であるＮＷユーザに貸与する「レンタルサーバ」がある。ＮＷユーザは、貸与されたサーバを用いてＷｅｂサイト（Ｗｅｂサービス）やメールサービス等を運営する。エンドユーザは、各種の団体の所属員であったり、そのような制限のない一般であったりする。
【０００４】
各エンドユーザは、サービスの利用に当たり、予め登録した認証用情報（典型的には、エンドユーザ名及びパスワード）を用いてＮＷユーザのシステムにログインする。エンドユーザのログイン記録（アクセスログ）は、例えば、サービスを提供するサーバにて記録される。アクセスログは、各ＮＷユーザによって管理されるため、ＮＷ管理者はアクセスログにアクセスすることはできない。
【０００５】
近年、エンドユーザの認証用情報がサイバー攻撃により窃取され、攻撃者がエンドユーザになりすましてシステムに不正ログインする事象が発生している。このため、ＮＷユーザからは、エンドユーザ保護の観点で、認証用情報（特にエンドユーザ名）が窃取されていないか否かを知りたいとの要望がある。
【先行技術文献】
【特許文献】
【０００６】
【特許文献１】特開２００８－２２７９３１号公報
【特許文献２】特開２００４－２２０３７３号公報
【特許文献３】特開２０１０－２３９３９２号公報
【特許文献４】特開２００５－２３４７２９号公報
【特許文献５】特開２００５－３３２１５２号公報
【特許文献６】特開２０１２－２１２３５４号公報
【発明の概要】
【発明が解決しようとする課題】
【０００７】
しかしながら、ＮＷユーザは、サービスへのアクセスログの内容から認証用情報の窃取を判定することは困難であった。これは以下の理由による。典型的なアクセスログは、ログイン要求元（エンドユーザ）のＩＰアドレス（送信元ＩＰアドレス）と、ログインに用いたエンドユーザ名及びパスワードと、ログインの成否とを１つのレコードとして記録する。
【０００８】
エンドユーザ名及びパスワードが窃取されている場合、ログインが不正か否かを判定するレコード中の情報要素はＩＰアドレスとなる。しかしながら、エンドユーザのＩＰアドレスは、通常、Dynamic Host Configuration Protocol（ＤＨＣＰ）サーバによって貸し出されるものであるので、必ずしも同じＩＰアドレスとはならない。また、エンドユーザが、複数の端末を使い分けたり、ログインを試行する場所を変えたりすることなどによっても、ログイン要求元のＩＰアドレスは異なる結果となる。
従って、アクセスログ中の或るレコードが窃取されたエンドユーザ名及びパスワードを用いた不正ログインのレコードであったとしても、ＮＷユーザは当該レコードのＩＰアドレ

スから当該ログインが不正ログインか否かを判断することができなかった。
【０００９】
本発明の１つの側面では、ログイン要求元の情報を手掛かりにアクセスログを用いて認証用情報が窃取されたことを検知可能な技術を提供することを目的とする。
【課題を解決するための手段】
【００１０】
１つの側面は、ログイン成功により所定サービスをユーザに提供する通信装置に関して、ユーザがログインに用いる認証用情報の窃取を情報処理装置が検知する方法であって、
前記情報処理装置が、ログイン要求元の情報と、ログイン要求元がログインに際して前記通信装置に提示した認証用情報と、当該認証用情報を用いたログインの成否を示す情報とを含むログイン要求毎のレコードを記憶し、
前記情報処理装置が、前記通信装置に対する攻撃元の情報を前記通信装置が存するネットワークの管理装置から受信し、
前記情報処理装置が、前記攻撃元の情報と一致する前記ログイン要求元の情報を含むレコードにログインの成功を示す情報が記憶されているときに当該レコード中の認証用情報が前記攻撃元に窃取されたと判定し、
前記攻撃元に窃取されたと判定した認証用情報を出力する
ことを含む認証用情報の窃取検知方法である。
【発明の効果】
【００１１】
１つの側面では、ログイン要求元の情報を手掛かりにアクセスログを用いて認証用情報が窃取されたことを検知することが可能となる。
【図面の簡単な説明】
【００１２】
【図１】図１は、実施形態に係る認証用情報の窃取検知方法が適用されるネットワークシステムの一例を示す図である。
【図２】図２は、認証用情報の窃取検知方法の説明図である。
【図３】図３は、サーバ及び管理装置のそれぞれに適用可能な情報処理装置（コンピュータ）の構成例を示す図である。
【図４】図４は、ＩＤＳ装置及びＩＤＳログ分析装置、並びにアクセスログ検証装置の機能的な構成を模式的に示す図である。
【図５】図５は、ＩＤＳログＤＢのデータ構造例を示す図である。
【図６】図６は、被攻撃先群分析部における処理の説明図である。
【図７】図７は、アクセスログＤＢのデータ構造例を示す図である。
【図８】図８は、アクセスログ検証部の動作例を示すフローチャートである。
【図９】図９は、アクセスログ検証部の処理の説明図である。
【図１０】図１０は、被窃取ユーザ名リストのデータ構造例を示す図である。
【図１１】図１１は、インタフェース部が出力する表示画面の例を示す。
【発明を実施するための形態】
【００１３】
以下、図面を参照して本発明の実施形態について説明する。実施形態の構成は例示であり、本発明は、実施形態の構成に限定されない。
【００１４】
＜システム構成例＞
図１は、本実施形態に係るネットワーク管理方法（認証用情報の窃取検知方法）が適用されるネットワークシステムの一例を示す図である。図２は、認証用情報の窃取検知方法の説明図である。
【００１５】
図１において、ネットワーク１は、ネットワーク管理者（ＮＷ管理者）によって管理されるネットワークである。ネットワーク１は、例えば、通信装置がInternet Protocol（

ＩＰ）パケット（以下単に「パケット」と表記）を用いてデータを送受信するＩＰ網である。例えば、ネットワーク１は、ネットワークサービスプロバイダ（ＮＳＰ）によって管理されるプロバイダ網である。但し、ＮＷ管理者は、ＮＳＰに制限されない。

【００１６】

ネットワーク１には、複数の通信装置が接続されている。図１では、複数の通信装置の一例として、サーバ装置（以下単に「サーバ」と表記）２Ａ，２Ｂ及び２Ｃがネットワーク１内に存在している。以下の説明において、サーバ２Ａ，２Ｂ，２Ｃを区別しない場合には、サーバ２と表記する。

【００１７】

各サーバ２Ａ，２Ｂ，２Ｃのそれぞれは、ＮＷ管理者からネットワークユーザ（ＮＷユーザ）に貸与されている。例えば、サーバ２Ａは、企業であるＮＷユーザＡに貸与されている。サーバ２Ｂは、大学であるＮＷユーザＢに貸与されている。サーバ２Ｃは、或る団体であるＮＷユーザＣに貸与されている。但し、ＮＷユーザは、企業、学校、企業や学校以外の団体、個人のいずれであっても良い。

【００１８】

各ＮＷユーザＡ，Ｂ，Ｃのそれぞれは、貸与されたサーバ２を用いて、エンドユーザに向けたネットワークサービスを提供する。サーバ２Ａ，サーバ２Ｂ，サーバ２Ｃのそれぞれは、各ＮＷユーザＡ，Ｂ，Ｃのサービス提供システムとして動作する。例えば、各サーバ２Ａ，２Ｂ，２Ｃは、各ＮＷユーザＡ，Ｂ，Ｃがそれぞれ運営するＷｅｂサイトを提供するＷｅｂサービス提供システムとして動作する。エンドユーザは、「ユーザ」の一例である。

【００１９】

サーバ２Ａで運営されるＷｅｂサイトに係るサービス提供システム（「システムＡ」と称する）は、企業の所属員である複数の（ｎ人（ｎは正の整数）の）エンドユーザによって利用される。システムＡの各エンドユーザは、自身が使用する端末３を用いてサーバ２Ａ（システムＡ）にアクセスし、Ｗｅｂサイトの閲覧を通じて、テキスト、画像、サウンド，ビデオのような様々な情報の提供を受けることができる。

【００２０】

サーバ２Ｂで運営されるＷｅｂサイトに係るサービス提供システム（「システムＢ」と称する）は、大学の学生や職員である複数の（ｎ人の）エンドユーザによって利用される。システムＢの各エンドユーザは、自身が使用する端末３を用いてサーバ２Ｂ（システムＢ）にアクセスし、Ｗｅｂサイトを閲覧することができる。

【００２１】

サーバ２Ｃで運営されるＷｅｂサイトに係るサービス提供システム（「システムＣ」と称する）は、団体の所属員である複数の（ｎ人の）エンドユーザによって利用される。システムＣの各エンドユーザは、自身が使用する端末３を用いてサーバ２Ｃ（システムＣ）にアクセスし、Ｗｅｂサイトを閲覧することができる。

【００２２】

ＮＷユーザが提供するネットワークサービスは、Ｗｅｂサイト以外のメール，クラウドのような様々なサービスを含み、提供されるサービスの内容に制限はない。但し、各エンドユーザは、サービス利用に当たり、予め登録された認証用情報（本実施形態ではエンドユーザ名及びパスワード）を用いてシステムにログインする。

【００２３】

サービス提供システムとして動作する各サーバ２Ａ，２Ｂ，２Ｃのそれぞれは、エンドユーザが端末３を用いて当該システムへのログインを試行した記録をアクセスログとして記憶する。すなわち、サーバ２Ａは、システムＡへのアクセスログを記憶し、サーバ２Ｂは、システムＢへのアクセスログを記憶し、サーバ２Ｃは、システムＣへのアクセスログを記憶する。各アクセスログは、少なくとも、アクセス者（ログイン要求元）のＩＰアドレス，認証用情報（エンドユーザ名及びパスワード），ログインの成否を示す情報を含む１以上のレコードを記憶する。エンドユーザ名は、「ユーザ識別子」、「ユーザＩＤ」の

一例である。
【００２４】
ネットワーク１は、外部ネットワーク（外部ＮＷ）４と接続されている。外部ネットワーク４は、例えば、インターネット（公衆網），イントラネットに代表されるＩＰ網である。ネットワーク１に接続された端末３は、パケットの送受信によって、外部ネットワーク４に接続された端末との間で通信を行うことができる。
【００２５】
各サーバ２Ａ，２Ｂ，２Ｃのそれぞれは、外部ネットワーク４に接続された攻撃者の端末５からパケットを用いたサイバー攻撃（図１において破線矢印で示す）を受ける虞がある。このため、ＮＷ管理者は、ネットワーク１と外部ネットワーク４との間に、ネットワーク管理装置（以下「管理装置」と表記する）６を設けている。管理装置６は、外部ネットワーク４からネットワーク１へ入るパケットの経路上に設置されている。
【００２６】
管理装置６は、サイバー攻撃の監視のための侵入検知システム（Intrusion Detection System（ＩＤＳ）装置７（図２参照）と呼ばれるセキュリティ装置を含む。ＩＤＳ装置７は、外部ネットワーク４からネットワーク１に入る複数のパケットがサーバ攻撃などの特異事象のパターンを示すか否かを判定する。
【００２７】
複数のパケットが特異事象のパターンを示す場合には、ＩＤＳ装置７はログ（ＩＤＳログ）への記録を行う。ＩＤＳ装置７は、パケットがサーバ攻撃などの特異事象のパターンであるか否かを判定する際には、予め登録してある特異事象のパターンと合致するかに基いて判定したり、過去のパターンとの比較に基づいて判定したりする。
【００２８】
管理装置６は、更に、ＩＤＳ装置７から出力されるログを分析するＩＤＳログ分析装置８（以下「分析装置８」と表記する）を含んでいる（図２参照）。分析装置８は、ＩＤＳ装置から出力されたＩＤＳログの解析を行い、攻撃目的でサーバ２へアクセスしたＩＰアドレス（以下、「攻撃元ＩＰ」と表記することもある）を出力する（図２＜１＞）。出力された攻撃元ＩＰは、攻撃対象となったサーバ２へ送信される。
【００２９】
サーバ２（各サーバ２Ａ，２Ｂ，２Ｃ：図２ではサーバ２Ａを例示）は、アクセスログ検証装置９（以下「検証装置９」と表記する）を含んでいる（図２参照）。検証装置９は、管理装置６の分析装置８から攻撃元ＩＰを受け取ると、アクセスログを参照し、攻撃元ＩＰによるログインが成功していたか否かを判定する（図２＜２＞）。
【００３０】
すなわち、検証装置９は、ログイン要求元のＩＰアドレスが攻撃元ＩＰであり（すなわち、ログイン要求元情報と攻撃元情報とが一致し）、且つログイン成功の情報を含むレコードがアクセスログに記憶されているか否かを判定する。このとき、該当するレコードがアクセスログから発見された場合（図２＜２＞，ＹＥＳ）には、検証装置９は以下の処理を行う。すなわち、検証装置９は、当該レコード中のエンドユーザ名を「被窃取ユーザ名」と判断する（図２＜３＞）。「被窃取ユーザ名」とは、攻撃者によって窃取されたエンドユーザ名を示す。
【００３１】
検証装置９は、被窃取ユーザ名を出力する（図２＜４＞）。被窃取ユーザ名は、例えばリストに登録される。ＮＷユーザＡは、リストの参照によって被窃取ユーザ名を知ると、当該被窃取ユーザ名でのログインを拒絶するようにシステムＡの設定を変更することができる。また、ＮＷユーザＡは、被窃取ユーザ名を有するエンドユーザに対し、エンドユーザ名の変更を依頼することができる。このとき、ＮＷユーザＡは、パスワードの変更も依頼し得る。
【００３２】
＜情報処理装置の構成例＞

図３は、サーバ２及び管理装置６のそれぞれに適用可能な情報処理装置（コンピュータ）の構成例を示す図である。図３において、情報処理装置１０は、バスＢを介して接続されたCentral Processing Unit（ＣＰＵ）１１と、メモリ（主記憶装置）１２と、補助記憶装置１３と、通信インタフェース（通信ＩＦ）１４と、入出力装置１５とを含む。ＣＰＵ１１は、「プロセッサ」、或いは「制御装置」の一例である。

【００３３】

メモリ１２は、不揮発性記憶媒体と、揮発性記憶媒体とを含む。不揮発性記憶媒体は、例えば、Read Only Memory（ＲＯＭ）である、揮発性記憶媒体は、例えば、Random Access Memory（ＲＡＭ）である。メモリ１２は、ＣＰＵ１１の作業領域として使用される。

【００３４】

補助記憶装置１３は、例えば、ハードディスク，Solid State Drive（ＳＳＤ），Electrically Erasable Programmable Read-Only Memory（ＥＥＰＲＯＭ），フラッシュメモリなどの少なくとも１つである。補助記憶装置１３は、ＣＰＵ１１によって実行されるプログラムや、プログラムの実行に際して使用されるデータを記憶する。メモリ１２，補助記憶装置１３のそれぞれは、「記憶装置」、「記憶媒体」の一例である。

【００３５】

通信ＩＦ１４は、通信に係る信号変換、プロトコル変換を司る装置である。通信ＩＦ１４として、例えば、ネットワークカード、或いはネットワークインタフェースカード（ＮＩＣ）と呼ばれる通信インタフェース装置が適用される。通信ＩＦ１４は、「送信装置」、「受信装置」の一例である。

【００３６】

入出力装置１５は、入力装置と出力装置とを含む。入力装置は、キー，ボタン，マウス等のポインティングデバイス，タッチパネルなどの少なくとも１つを含み、情報の入力に使用される。出力装置は、例えばディスプレイ装置（表示装置）であり、情報の表示に使用される。入出力装置１５は、マイクロフォンのような音声入力装置、スピーカのような音声出力装置を含むこともある。

【００３７】

ＣＰＵ１１は、補助記憶装置１３に記憶されたプログラムをメモリ１２にロードして実行する。これによって、情報処理装置１０は、管理装置６として動作したり、サーバ２として動作したりすることができる。

【００３８】

＜機能的構成＞

図４は、管理装置６に備えられたＩＤＳ装置７及びＩＤＳログの分析装置８、並びにサーバ２（各サーバ２Ａ，２Ｂ，２Ｃ）に備えられた検証装置９の機能的な構成を模式的に示す図である。

【００３９】

＜＜管理装置＞＞

ＩＤＳ装置７は、攻撃検知部７１と、ＩＤＳログデータベース（ＩＤＳログＤＢ）７２とを含む。分析装置８は、被攻撃先群分析部８１と、攻撃元分析部８２と、攻撃元情報送信部８３とを含む。

【００４０】

管理装置６として動作する情報処理装置１０のＣＰＵ１１は、プログラムを実行することによって、攻撃検知部７１，被攻撃先群分析部８１，攻撃元分析部８２，及び攻撃元情報送信部８３として動作する。ＩＤＳログＤＢ７２は、管理装置６として動作する情報処理装置１０の補助記憶装置１３，或いはメモリ１２に記憶される。

【００４１】

[ＩＤＳ装置]

ＩＤＳ装置７は、サイバー攻撃の監視のための侵入検知システム（ＩＤＳ）を運用する装置である。ＩＤＳ装置７は、一例として、攻撃元からのブルートフォース攻撃を検知する。ブルートフォース攻撃とは、考えられる全ての鍵をリストアップすることで暗号文の

復号を試みる攻撃である。効率的な攻撃の実施のために、辞書に収集されている単語を候補として検索する辞書攻撃や、システムに初期設定される値を用いた攻撃も存在する。ブルートフォース攻撃には、或るシステムから漏洩したと考えられる大量の識別子（ＩＤ）及びパスワードを別のシステムへのログインに使用する攻撃も含まれる。

【００４２】

ＩＤＳ装置７は、ブルートフォース攻撃を検知し、特定のＩＰアドレスを有する通信装置に向けてのアクセスを重点的に監視するような対策のために用いられる。ＩＤＳ装置７は、攻撃元のＩＰアドレスを特定する機能を有する。ＩＤＳで特定された攻撃元ＩＰに対し、管理装置６は、当該攻撃元ＩＰからの通信を遮断するなどの防御を行い得る。

【００４３】

ＩＤＳ装置７の攻撃検知部７１は、外部ネットワーク４からネットワーク１へ流れるパケットのうち、ブルートフォース攻撃に関わるパケットを検知し、異常を知らせるイベントを分析装置８向けに発行する。攻撃検知部７１は、検知したブルートフォース攻撃に関わるパケットに関する情報をＩＤＳログＤＢ７２に格納する。

【００４４】

図５は、ＩＤＳログＤＢ７２のデータ構造例を示す図である。図５において、ＩＤＳログＤＢ７２は、１以上のレコードで形成されるテーブルを有している。１つのレコードは、“Hacker(ハッカー)”，“Victim(ビクティム)”，“検知時刻”，“攻撃回数”，“Port（ポート番号）”を情報要素として含んでいる。

【００４５】

“Hacker”は、「攻撃元」を示す。攻撃元とは、サーバ２を用いて提供されるシステムに対して攻撃（本実施形態ではブルートフォース攻撃）を仕掛ける通信の発信元の通信装置を指す。本実施形態では、攻撃元は発信元のＩＰアドレスで特定される。

【００４６】

“Victim”は、「被攻撃先」を示す。被攻撃先とは、ブルートフォース攻撃を受ける通信装置を指す。本実施形態では、被攻撃先は、攻撃される通信装置（サーバ２）に割り当てられたＩＰアドレスで特定される。

【００４７】

“検知時刻”は、侵入検知システム（ＩＤＳ）がブルートフォース攻撃を検知した時刻を示す。“攻撃回数”は、攻撃元がログインを試行した回数を示す。攻撃回数は「ログイン試行回数」とも呼ばれる。攻撃回数は、或る検知時刻を含む或る連続的期間において、攻撃元から被攻撃先へログインを試行するブルートフォース攻撃が検知された回数であり得る。ブルートフォース攻撃は、未知のエンドユーザ名及びパスワードを窃取するために、当てずっぽうのエンドユーザ名及びパスワードでのログインを繰り返し試行するためである。

【００４８】

例えば、或る時刻から５分間に亘って、或る被攻撃先が攻撃元から攻撃を受けた場合、当該５分間における攻撃の総数を攻撃回数としても良い。攻撃回数は、単位時間当たりのブルートフォース攻撃が検知された回数であっても良い。或いは、或る時間帯（例えば５分）における単位時間（例えば１分）あたりの攻撃回数の平均であっても良い。

【００４９】

“Port”は、攻撃が検知された被攻撃先の通信装置（サーバ２）のポート番号である。攻撃検知部７１は、例えば、外部ネットワーク４からネットワーク１へ流れるパケットの送信元ＩＰアドレス及び宛先ＩＰアドレスを参照し、或る送信元から或る宛先へのパケットの送信パターンがブルートフォース攻撃のパターンに合致する場合に、ＩＤＳログＤＢ７２にレコードを書き込む。

【００５０】

図５に示すレコードの内容からは、以下のことが分かる。例えば、図５に示すテーブルの１番目（上側）のレコードは、以下を示している。すなわち、ＩＰアドレス“11.22.33.44”の攻撃元から、ＩＰアドレス“55.66.77.88”の被攻撃先のポート番号“22”に対し

ブルートフォース攻撃が行われている。ブルートフォース攻撃の検知時刻は「２０１３年４月１日０時０分」であり、攻撃回数は３０回である。

【００５１】

[分析装置]

図４に戻って、分析装置８の被攻撃先群分析部（分析部）８１は、ＩＤＳログＤＢ７２に格納されたデータ（ＩＤＳログ：図５）に基づいて、ブルートフォース攻撃の被攻撃先と考えられる通信装置のＩＰアドレスを特定する。本実施形態では、攻撃を受けたサーバ２のＩＰアドレスが被攻撃先のＩＰアドレスとして特定される。

【００５２】

被攻撃先群分析部８１は、例えば、周期的にＩＤＳログを取得して分析を開始することができる。或いは、被攻撃先群分析部８１は、ＩＤＳ装置７で発行されたイベント受信を契機として分析を開始することができる。

【００５３】

具体的には、被攻撃先群分析部８１は、ＩＤＳログＤＢ７２に格納されたデータ（ＩＤＳログ）に基づいて、攻撃回数及び検知時刻について、複数の被攻撃先（Victim）の相関係数を計算する。

【００５４】

攻撃回数及び検知時刻のそれぞれに関する相関係数の計算方法としては、たとえば、最大クリーク法を用いることができる。そして、相関係数の高い通信装置（Victim）を選択し、被攻撃先群（Victim群、通信装置群）として特定する。被攻撃先群分析部８１が参照する記憶領域（補助記憶装置１３又はメモリ１２の記憶領域）には、分析設定ＤＢ（図示せず）が記憶されている。分析設定ＤＢには、被攻撃先群を特定するための相関係数の閾値と、分析に使用したＩＤＳログデータの期間（分析の間隔）とを少なくとも含む。被攻撃先群分析部８１は、分析の間隔に合致するデータをＩＤＳログから得て、相関係数の計算結果が閾値を超える被攻撃先を選択（特定）する。

【００５５】

例えば、相関係数Ｒは、通信装置v_iが受けたブルートフォース攻撃の回数をx_i、検知時刻をt_iとして、以下の式で定義することができる。

【００５６】

【数１】

$$R = \frac{\sum_{i=1}^{n}(x_i - x_{av})(t_i - t_{av})}{\sqrt{\sum_{i=1}^{n}(x_i - x_{av})}\sqrt{\sum_{i=1}^{n}(t_i - t_{av})}}$$

ここで、x_{av}はブルートフォース攻撃の回数x_iの平均、t_{av}は検知時刻t_iの平均である。ブルートフォース攻撃の回数は、１分間あたりの攻撃回数であっても良い。

【００５７】

図６は、被攻撃先群分析部８１における処理の説明図である。ブルートフォース攻撃は、或る攻撃元から複数の被攻撃先（被攻撃先群）へ向けて行われることがある。また、ブルートフォース攻撃は、検知時刻によって毎回異なる攻撃元から特定の複数の被攻撃先群へ向けて行われることがある。例えば、或る時刻t_1では、攻撃元H_1から被攻撃先V_1、V_2、…、V_m（mは正の整数）へブルートフォース攻撃を行い、時刻t_2では、攻撃元H_2から被攻撃先V_1、V_2、…、V_mへブルートフォース攻撃を行うことがある。

【００５８】

上記のように、被攻撃先群に対するブルートフォース攻撃が行われる場合、或る１つの攻撃元から、ほぼ同時刻に、ほぼ同じ回数だけ複数の被攻撃先に対して攻撃が行われた形跡がＩＤＳログに残る。

【００５９】
被攻撃先群分析部８１は、複数の通信装置に関して、或る送信元ＩＰアドレスからのアクセス時刻（検知時刻）及びログイン試行回数（攻撃回数）の相関係数を計算する。被攻撃先群分析部８１は、検知時刻及び攻撃回数の相関係数が閾値以上又は閾値を上回るときに、当該或る送信元ＩＰアドレスを攻撃元ＩＰとして特定し、複数の通信装置を被攻撃先群として特定する。
【００６０】
図６に示す例において、例えば、検知時刻“10/1 0:01”において、ＩＰアドレスH_1（H_i（ｉは正の整数））からＩＰアドレスV_1，V_2，V_3に対してそれぞれ５０回のログイン試行回数が記録されている。このように、被攻撃先群分析部８１は、或るＩＰアドレスから、ほぼ同時刻で、ほぼ同じ回数のログイン試行回数が認められた複数のＩＰアドレス（V_1，V_2，V_3）が、被攻撃先群のＩＰアドレスとして特定する。また、被攻撃先群分析部８１は、ログインを試行したＩＰアドレス（H_1）を攻撃元ＩＰとして特定する。
【００６１】
図６に示す例では、被攻撃先群分析部８１は、上述した処理によって、ＩＰアドレスH_1，H_2，及びH_3のそれぞれを攻撃元ＩＰとして特定する。これに対し、ＩＰアドレスH_4の検知時刻では、ＩＰアドレスV_2及びV_3に対するログイン試行回数（攻撃回数）は記録されていない。このため、ＩＰアドレスH_4は、攻撃元ＩＰとして特定されない。
【００６２】
各ＩＰアドレスV_1，V_2，V_3が、サーバ２Ａ，２Ｂ，２Ｃのそれぞれのアドレスであると仮定すると、被攻撃先群分析部８１は、被攻撃先群であるサーバ２Ａ，２Ｂ，２Ｃに対する攻撃元ＩＰを特定することができる。
【００６３】
分析装置８の攻撃元分析部（分析部）８２は、ＩＤＳログＤＢ７２からＩＤＳログの情報を得るとともに、被攻撃先群分析部８１から被攻撃先群の情報を得る。攻撃元分析部８２は、各被攻撃先のＩＰアドレス（Victim）を含むレコードをＩＤＳログから特定し、特定したレコード中の攻撃先（Hacker）のＩＰアドレスを攻撃元ＩＰとして特定する。
【００６４】
攻撃元情報送信部（送信部）８３は、被攻撃先群のＩＰアドレスへ向けて、攻撃元ＩＰを含む攻撃元情報を送信する処理を行う。すなわち、攻撃元情報送信部８３は、攻撃元情報を含むパケットを生成する。このとき、パケットの宛先ＩＰアドレスには、被攻撃先のＩＰアドレスが設定される。
【００６５】
管理装置６として動作する情報処理装置１０の通信ＩＦ１４は、パケットを被攻撃先（サーバ２）へ向けて送信する。これによって、被攻撃先群であるサーバ２Ａ，２Ｂ，２Ｃのそれぞれに対し、攻撃元情報（攻撃元ＩＰ）が受信される。
【００６６】
攻撃元情報の送信は、攻撃元情報が得られたことを契機として開始されるようにしても良い。或いは、攻撃元情報が補助記憶装置１３又はメモリ１２の所定の記憶領域に記憶され、検証装置９からの要求に応じて攻撃元情報送信部８３が送信処理を実行するようにしても良い。
【００６７】
＜＜サーバ＞＞
図４に示すように、サーバ２が備える検証装置９は、アクセスログ検証部（検証部）９１と、アクセスログＤＢ９２と、被窃取ユーザ名リスト（リスト）９３と、インタフェース部９４とを含む。サーバ２として動作する情報処理装置１０のＣＰＵ１１は、プログラムを実行することによって、アクセスログ検証部９１として動作する。サーバ２は、「通信装置」の一例であり、検証装置９は、「情報処理装置」の一例である。
【００６８】

アクセスログＤＢ９２及び被窃取ユーザ名リスト９３は、サーバ２として動作する情報処理装置１０の補助記憶装置１３又はメモリ１２に記憶される。サーバ２の入出力装置１５に含まれる出力装置（ディスプレイ装置）は、インタフェース部９４として動作する。

【００６９】

サーバ２として動作する情報処理装置１０のＣＰＵ１１は、補助記憶装置１３に記憶されたプログラムを実行することによって、Ｗｅｂサービスの提供システムとして動作する。すなわち、サーバ２は、Ｗｅｂクライアントであるエンドユーザの端末３にＷｅｂページの情報を提供するＷｅｂサーバとして動作する。サーバ２がＷｅｂサーバとして動作するためのプログラム及びデータは、予め補助記憶装置１３に記憶されている。

【００７０】

ＣＰＵ１１は、エンドユーザの端末３からサーバ２へ送信されたＷｅｂサイトへのログイン要求を通信ＩＦ１４を介して受信する。すると、ＣＰＵ１１は、ログイン画面のＷｅｂページの情報を補助記憶装置１３から読み出し、端末３へ送信する。Ｗｅｂページの情報は、予め補助記憶装置１３に記憶されている。

【００７１】

端末３を用いるエンドユーザは、ログイン画面を用いて、認証用情報（認証コードともいう）、すなわちエンドユーザ名及びパスワードを入力する。認証用情報は、端末３からサーバ２の通信ＩＦ１４で受信され、ＣＰＵ１１に渡される。

【００７２】

ＣＰＵ１１は、補助記憶装置１３に予め記憶された認証用情報を用いて認証用情報が正当か否かを判定する。認証用情報が正当であれば、ＣＰＵ１１は、ログイン“ＯＫ（Ｙｅｓ）”と判定し、次のＷｅｂページの情報を端末３へ送信する処理を行う。これに対し、認証用情報が不正であれば、ＣＰＵ１１は、ログイン“ＮＧ（Ｎｏ）”と判定し、エラーメッセージを端末３へ送る処理を行う。

【００７３】

認証用情報が不正の場合として、例えば、エンドユーザ名が認証用情報として登録されていない場合や、パスワードが認証用情報として登録されたパスワードに一致しない場合が挙げられる。

【００７４】

ＣＰＵ１１は、認証の成否（すなわち、ログインの成否）を含むレコードをアクセスログＤＢ９２に記憶する。このとき、レコードに含まれる情報要素（パラメータ）として、少なくとも、ログイン要求の送信元の通信装置のＩＰアドレスと、認証用情報（エンドユーザ名及びパスワード）と、ログインの成否を示す情報とが含まれる。

【００７５】

図７は、アクセスログＤＢ９２のデータ構造例を示す図である。アクセスログＤＢ９２は、上記したように、ログイン要求元のＩＰアドレスと、エンドユーザ名と、パスワードと、ログインの成功／失敗（Ｙｅｓ／Ｎｏ）を示す情報とを含む１以上のレコードを記憶する。ログイン要求元のＩＰアドレスは、「ログイン要求元の情報」の一例である。

【００７６】

ＣＰＵ１１は、アクセスログＤＢ９２へのレコード登録を、ログイン要求に基づく認証処理を実行する毎に行う。このようなアクセスログＤＢ９２のレコード（ログ）には、正当なエンドユーザの端末３からのログイン要求に対する結果のログと、ブルートフォース攻撃による攻撃元の端末５からのログイン要求に対する結果のログとが含まれ得る。

【００７７】

図８は、アクセスログ検証部９１（ＣＰＵ１１）の動作（処理）例を示すフローチャートである。図８に示す処理は、例えば、周期的又は定期的に実行される。或いは、図８に示す処理は、周期的又は定期的に攻撃元情報の受信（到着）をチェックし、攻撃元情報が到着している場合に開始されるようにしても良い。或いは、図８に示す処理は、攻撃元情報の受信を契機として開始されるようにしても良い。

【００７８】

図８において、アクセスログ検証部９１は、アクセスログＤＢ９２からログデータ（各レコード）を取得する（０１）。続いて、アクセスログ検証部９１は、分析装置８から攻撃元情報（攻撃元ＩＰ）を取得する（０２）。図８の例では、以下を仮定している。すなわち、アクセスログ検証部９１（サーバ２）が分析装置８（管理装置６）へ攻撃元情報の提供要求のメッセージを送信する。提供要求を受信した分析装置８（攻撃元情報送信部８３）は、提供要求に応じて攻撃元情報を提供要求の送信元のサーバ２へ送る。

【００７９】

次に、アクセスログ検証部９１は、ログデータから攻撃元ＩＰが含まれるレコードを抽出する（０３）。次に、アクセスログ検証部９１は、抽出されたレコード中にログイン成功を示す情報を含んだレコードが存在するか否かを判定する（０４）。

【００８０】

このとき、該当するレコードが存在しない場合（０４，Ｎｏ）には、図８の処理が終了する。これに対し、該当するレコードが存在する場合（０４，Ｙｅｓ）には、アクセスログ検証部９１は、当該レコードに含まれるエンドユーザ名を被窃取ユーザ名リスト９３に登録する（０５）。その後、図８の処理が終了する。

【００８１】

なお、図８における０１の処理と０２の処理とは逆でも良い。また、０３以降の処理は、図８の例では、複数の攻撃元ＩＰが得られた場合において、各攻撃元ＩＰに関して並列に実行される。但し、各攻撃元ＩＰに関して０３～０５の処理が繰り返し実行されるようにしても良い。

【００８２】

図９は、アクセスログ検証部９１の処理の説明図である。図９では、図９に示す内容のアクセスログに関して、攻撃元ＩＰとしてH_1，H_2及びH_3が得られた様子が図示されている。アクセスログ検証部９１は、攻撃元ＩＰ“H_1”，“H_2”を含むレコードを抽出する。このとき、上から２番目のレコード（「レコード２」と称する）と上から３番目のレコード（「レコード３」と称する）とが抽出される。

【００８３】

アクセスログ検証部９１は、レコード２及びレコード３のそれぞれにおける“ログイン成功／失敗”の情報（ステータス）を参照する。このとき、レコード２及びレコード３のそれぞれのステータスは“Ｙｅｓ（ログイン成功）”を示す。このため、アクセスログ検証部９１は、レコード２及びレコード３中の認証用情報が攻撃元に窃取されたと判定する。レコード２の認証用情報は、エンドユーザ名“Alice”及びパスワード“1234”であり、レコード３の認証用情報は、エンドユーザ名“Bob”及びパスワード“aaaa”である。アクセスログ検証部９１は、レコード２及びレコード３の各エンドユーザ名（“Alice”及び“Bob”）を被窃取ユーザ名リスト９３に登録する。

【００８４】

図１０は、被窃取ユーザ名リスト９３（以下、「リスト９３」と表記）のデータ構造例を示す図である。図１０に示すように、リスト９３は、窃取されたと判定された（推定された）エンドユーザ名と、追加日（追加日時）とを含む１以上のレコードを記憶する。リスト９３には、さらにパスワードが記憶されるようにしても良い。

【００８５】

インタフェース部９４は、アクセスログ検証部９１によって特定された被攻撃先に関する情報を表示する。図１１は、インタフェース部９４（入出力装置１５に含まれるディスプレイ装置）が出力する表示画面の例を示す。図１１に示すように、インタフェース部９４は、一例として、被窃取ユーザ名リスト９３の登録内容を表示画面に表示する。サーバ２（例えばサーバ２Ａ）を利用するＮＷユーザＡは、表示画面を参照することで、エンドユーザ名“Alice”及び“Bob”が攻撃元に窃取されたことを知ることができる。

【００８６】

上述したように、攻撃元情報（攻撃元ＩＰ）は、被攻撃先群として特定された各サーバ２Ａ，２Ｂ，２Ｃにおける検証装置９のそれぞれに送信される。従って、各サーバ２の検

証装置９が上記した処理を行う。これにより、ＮＷユーザＡだけでなく、サーバ２Ｂを利用するＮＷユーザＢ，サーバ２Ｃを利用するＮＷユーザＣも、対応する被窃取ユーザ名リスト９３を参照することで、攻撃元に窃取されたエンドユーザ名を知ることができる。

【００８７】

ＮＷユーザＡは、例えば、エンドユーザ名“Alice”及び“Bob”を用いたログインがパスワードの如何に拘わらず拒絶されるようにシステムＡの設定変更を行う。このような設定変更は、マニュアルで実施することができる。或いは、所定のアルゴリズム（プログラム）を用いて、例えば、被窃取ユーザ名リスト９３にエンドユーザ名が追加されたことを契機として自動的に実行されるようにすることもできる。これによって、攻撃元による不正ログイン（なりすまし）を回避することが可能となる。

【００８８】

また、ＮＷユーザＡは、“Alice”及び“Bob”をそれぞれ有するエンドユーザに対し、エンドユーザ名の変更を依頼する。エンドユーザ名の変更によって、攻撃元のなりすましが不可能となる。また、窃取されたエンドユーザ名でのログインが拒絶される設定となっている場合には、エンドユーザ名変更によって、正規のエンドユーザがシステムＡにログイン可能な環境を得ることができる。変更依頼は、メール，郵送等適宜の手法を用いてエンドユーザに与えられる。

【００８９】

＜実施形態の作用効果＞

実施形態によれば、検証装置９がアクセスログ及び攻撃元ＩＰを用いて認証用情報（エンドユーザ名）が窃取されたことを検知し、被窃取ユーザ名リスト９３に登録する。ＮＷユーザは、出力された被窃取ユーザ名リスト９３を参照して、窃取に対する対策を採ることができる。

【００９０】

サーバ２（検証装置９）は、ＮＷ管理者の運用する管理装置６（ＩＤＳ装置７及び分析装置８）によって得られた攻撃元情報（攻撃元ＩＰ）を受信することで、既存のアクセスログを用いて窃取を検知することができる。このため、ＮＷユーザがアクセスログから認証用情報の窃取を知るための導入コストが小さくて済む。

【００９１】

また、本実施形態による攻撃元ＩＰの特定方法によれば、比較的短い期間で得られたＩＤＳログを用いて攻撃元ＩＰを特定することができる。このため、既存のレピュテーションサービスのように、アクセスログ中のＩＰアドレスが悪性か否かを判断するための十分な評価材料を得るために、長い期間のアクセスログを要するという欠点がない。

【００９２】

また、本実施形態による攻撃元ＩＰの特定方法では、管理装置６で或る時刻で通信装置（サーバ２）を含む被攻撃先群に実質的に同数と認め得る回数の攻撃（ログイン試行）を行ったＩＰアドレスが検証装置９に供給する攻撃元ＩＰとして特定される。このため、比較的少ない攻撃回数（ログイン試行回数）であっても、攻撃元ＩＰを特定することができる。

【００９３】

このため、例えば、大量のログイン試行失敗の後に１回ログインに成功した記録がアクセスログにあるという特徴を不正ログイン成功と判断するような構成に比べて、大量のログイン試行失敗を要しない点で、攻撃元ＩＰ特定が容易化される。

【００９４】

さらに、例えば、ＩＰアドレスとエンドユーザ名とを紐づけ、普段と異なるＩＰアドレスでログイン成功した場合に、当該ログインが不正ログインであると判断する手法がある。このような手法では、エンドユーザが複数の端末３を使い分ける場合に不正ログインを誤検知する可能性がある。また、１つのエンドユーザ名を複数人で共有する場合にも誤検知が発生し得る。

【００９５】

本実施形態による攻撃元ＩＰの特定方法では、攻撃元ＩＰとして特定する条件が満たされる限り、複数のＩＰアドレスのそれぞれが攻撃元ＩＰとして検知される。よって、上記紐づけによる手法で生じる欠点（誤検知）は発生しない。また、本実兄対の攻撃元ＩＰの特定手法では、複数のＩＰアドレスを用いたブルートフォース攻撃に対して、それぞれの攻撃元ＩＰを検知することができる。

【００９６】

＜変形例＞

本実施形態では、ＩＤＳ装置７及び分析装置８を用い、図６を用いて説明した手法で攻撃元ＩＰを特定する。但し、当該攻撃元ＩＰの特定方法は例示である。すなわち、検証装置９に供給（受信）される攻撃元ＩＰ（攻撃元情報）の特定方法は、実施形態で説明した手法に限定されない。すなわち、既存のＩＤＳを用いたブルートフォース攻撃の攻撃元ＩＰの特定方法を含むあらゆる攻撃元ＩＰの特定方法を適用可能である。このため、攻撃元ＩＰの特定のために被攻撃先群が特定されることは必須要件ではなく、単一の通信装置（サーバ）に対する攻撃元ＩＰが検知される手法が適用されても良い。

【００９７】

また、本実施形態では、攻撃元情報としてＩＰアドレスが使用される。このため、攻撃元の通信装置に依存しない管理を行うことができ、また、ログイン要求元（送信元）のＩＰアドレスを記録する既存のアクセスログとの対応（紐づけ）が容易である。但し、攻撃元情報がＩＰアドレスであることは必須条件ではなく、アクセスログにて攻撃元情報と一致するログイン要求元情報が特定される限り、ＩＰアドレス以外の情報を攻撃元情報として適用しても良い。アクセスログに記録されるログイン要求元の情報も、送信元ＩＰアドレスに限られない。

【００９８】

また、本実施形態では、ＩＤＳ装置７と分析装置８とが一つの情報処理装置１０（管理装置６）上で動作する例について説明している。但し、ＩＤＳ装置７と分析装置８とが個別の情報処理装置上で動作し、情報処理装置間の通信によりＩＤＳ装置７で得られたＩＤＳログが分析装置８へ送信されるようにしても良い。

【００９９】

また、本実施形態では、「情報処理装置」の一例である検証装置９が「通信装置」の一例であるサーバ２に含まれている例を示している。当該構成に代えて、検証装置９がサーバ２と通信可能なサーバ２から独立した情報処理装置に実装されるようにしても良い。この場合、既存のサーバ（サービス提供システム）について、アクセスログを検証装置９に供給する構成を追加するだけで良く、サーバに対する改変度合いを小さくすることができる。また、Ｗｅｂサーバとして動作する情報処理装置とアクセスログＤＢを記憶する情報処理装置とが別の装置であっても良い。

【０１００】

上述した実施形態は、以下の付記を開示する。以下の付記は適宜組み合わせることが可能である。

（付記１）　ログイン成功により所定サービスをユーザに提供する通信装置に関して、ユーザがログインに用いる認証用情報の窃取を情報処理装置が検知する方法であって、

前記情報処理装置が、ログイン要求元の情報と、ログイン要求元がログインに際して前記通信装置に提示した認証用情報と、当該認証用情報を用いたログインの成否を示す情報とを含むログイン要求毎のレコードを記憶し、

前記情報処理装置が、前記通信装置に対する攻撃元の情報を前記通信装置が存するネットワークの管理装置から受信し、

前記情報処理装置が、前記攻撃元の情報と一致する前記ログイン要求元の情報を含むレコードにログインの成功を示す情報が記憶されているときに当該レコード中の認証用情報が前記攻撃元に窃取されたと判定し、

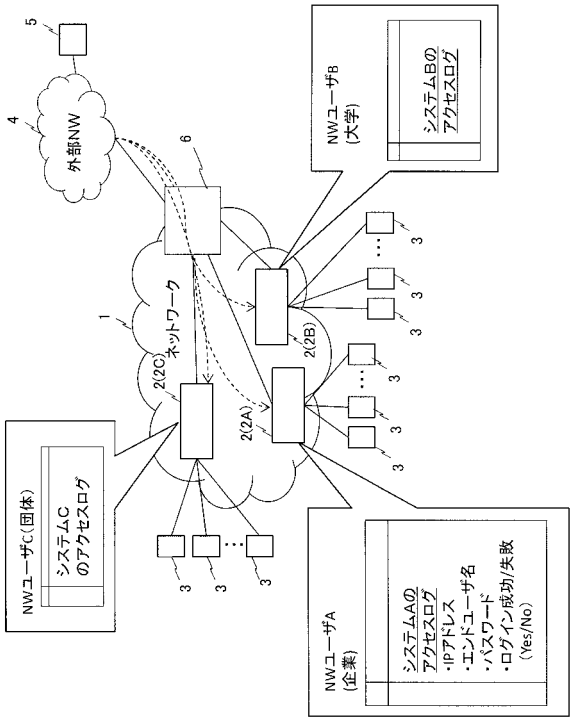
窃取されたと判定した認証用情報を出力する

ことを含む認証用情報の窃取検知方法。（１）

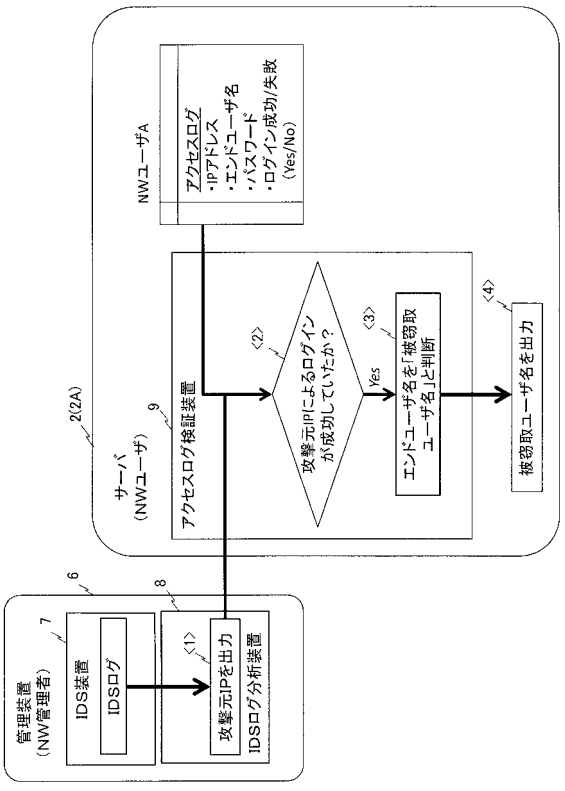
【０１０１】
（付記２）　前記情報処理装置は、或る攻撃元が或る時刻で前記通信装置を含む被攻撃先群に実質的に同数と認め得る回数の攻撃を行ったことを示す情報が前記管理装置で得られたときにおける前記或る攻撃元の情報を受信する
付記１に記載の認証用情報の窃取検知方法。（２）
【０１０２】
（付記３）　前記情報処理装置は、或る攻撃元からの攻撃の検知時刻及び攻撃回数のそれぞれの相関係数が閾値以上である被攻撃先群の１つが前記通信装置であることを検知した前記管理装置から前記或る攻撃元の情報を受信する
付記１に記載の認証用情報の窃取検知方法。
【０１０３】
（付記４）　前記攻撃元の情報及び前記ログイン要求元の情報がＩＰアドレスである
付記１から３のいずれか１項に記載の認証用情報の窃取検知方法。
【０１０４】
（付記５）　前記認証用情報は、ユーザ識別子を含む
付記１から４のいずれか１項に記載の認証用情報の窃取検知方法。
【０１０５】
（付記６）　ログイン成功により所定サービスをユーザに提供する通信装置に関して、ユーザがログインに用いる認証用情報の窃取を検知する認証用情報窃取検知装置であって、
ログイン要求元の情報と、ログイン要求元がログインに際して前記通信装置に提示した認証用情報と、当該認証用情報を用いたログインの成否を示す情報とを含むログイン要求毎のレコードを記憶する記憶装置と、
前記情報処理装置が、前記通信装置に対する攻撃元の情報を前記通信装置が存するネットワークの管理装置から受信する受信装置と、
前記情報処理装置が、前記攻撃元の情報と一致する前記ログイン要求元の情報を含むレコードにログインの成功を示す情報が記憶されているときに当該レコード中の認証用情報が前記攻撃元に窃取されたと判定する判定部と、
窃取されたと判定した認証用情報を出力する出力装置と、
を含む認証用情報の窃取検知装置。（３）
【０１０６】
（付記７）　ログイン成功により所定サービスをユーザに提供する通信装置（図４の２）に関して、ユーザがログインに用いる認証用情報（エンドユーザ名）の窃取を検知する処理をコンピュータに実行させるプログラムであって、
ログイン要求元の情報と、ログイン要求元がログインに際して前記通信装置に提示した認証用情報と、当該認証用情報を用いたログインの成否を示す情報とを含むログイン要求毎のレコードを記憶するステップと、
前記通信装置に対する攻撃元の情報を前記通信装置が存するネットワークの管理装置から受信するステップと、
前記攻撃元の情報と一致する前記ログイン要求元の情報を含むレコードにログインの成功を示す情報が記憶されているときに当該レコード中の認証用情報が前記攻撃元に窃取されたと判定するステップと、
前記攻撃元に窃取されたと判定した認証用情報を出力するステップと
をコンピュータに実行させるプログラム。
【符号の説明】
【０１０７】
１・・・ネットワーク
２・・・サーバ
３，５・・・端末
４・・・外部ネットワーク

６・・・ネットワーク管理装置
７・・・ＩＤＳ装置
８・・・ＩＤＳログ分析装置
９・・・アクセスログ検証装置
１０・・・情報処理装置
１１・・・ＣＰＵ
１２・・・メモリ
１３・・・補助記憶装置
１４・・・通信インタフェース
１５・・・入出力装置

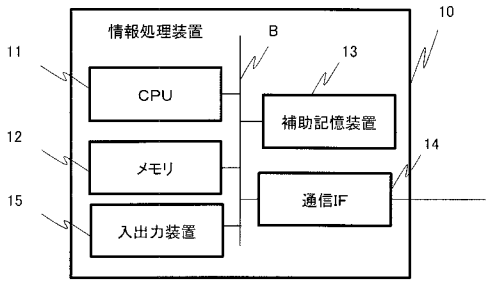
【図１】



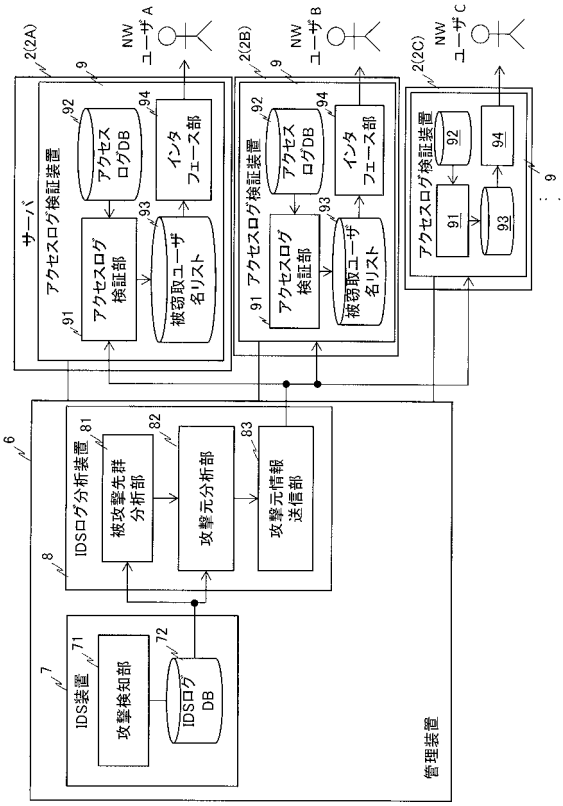
【図２】



【図３】



【図４】

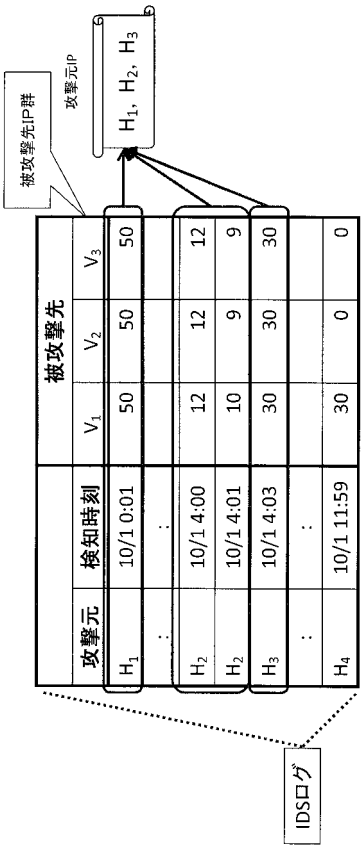


【図５】

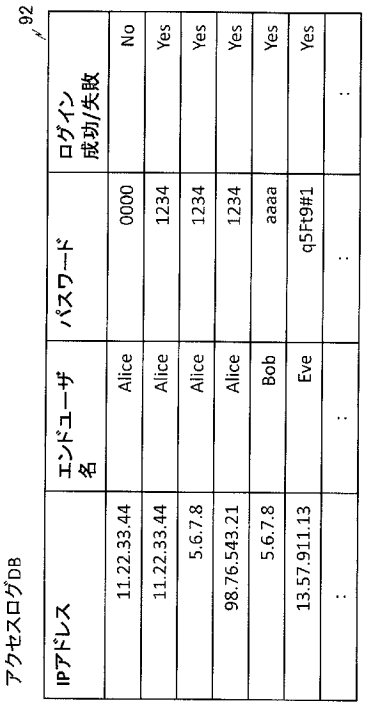
IDSログDB

Hacker	Victim	検知時刻	攻撃回数	Port
11.22.33.44	55.66.77.88	2013/4/1 0:00	30	22
11.22.33.45	55.66.77.88	2013/4/2 0:01	100	3389
:	:	:	:	:

【図６】



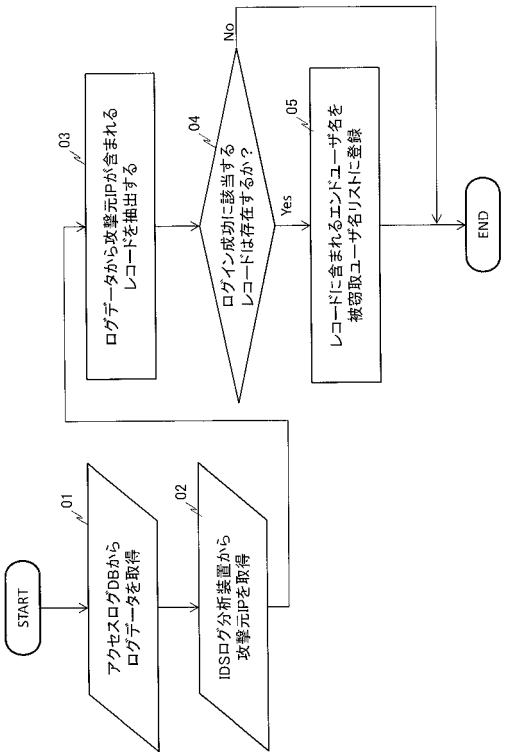
【図７】



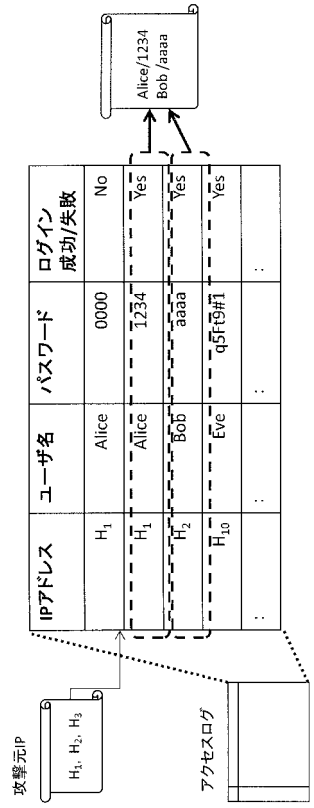
アクセスログDB 92

IPアドレス	エンドユーザ名	パスワード	ログイン成功/失敗
11.22.33.44	Alice	0000	No
11.22.33.44	Alice	1234	Yes
5.6.7.8	Alice	1234	Yes
98.76.543.21	Alice	1234	Yes
5.6.7.8	Bob	aaaa	Yes
13.57.911.13	Eve	q5Ft9#1	Yes
:	:	:	:

【図８】



【図９】



【図１０】

被窃取ユーザ名リスト 93

エンドユーザ名	追加日
Alice	2012/11/1 12:00
Bob	2012/11/2 0:00
:	:

【図１１】