

【特許請求の範囲】**【請求項 1】**

攻撃元通信装置から攻撃を受ける複数の被攻撃先通信装置をネットワーク機器から収集したログに基いて分類するログ分析装置であって、

前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した検知時刻および前記検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する相関係数を前記ログに基いて計算する相関係数計算部と、

前記相関係数が所定の閾値以上であり、かつ、前記期間において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出する抽出部と、

を含むログ分析装置。

10

【請求項 2】

前記攻撃は断続的に複数の期間にわたり行われ、前記検知時刻は複数であり、前記複数の期間の各々はそれぞれ異なる前記複数の検知時刻の一つを含み、

前記相関係数計算部は、前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した前記複数の検知時刻および前記複数の期間の各々における前記攻撃の回数に関する相関係数を前記ログに基いて計算し、

前記抽出部は、前記相関係数が所定の閾値以上であり、かつ、前記期間の各々において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出する、請求項 1 に記載のログ分析装置。

20

【請求項 3】

前記抽出部は、前記複数の被攻撃先通信装置が受けた前記攻撃の前記検知時刻および前記検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する情報に対応した頂点と、前記所定の閾値以上の相関係数を有する前記複数の被攻撃先通信装置のうちの 2 つに対応する頂点間に付与した辺を含むグラフから、クリークを抽出することによって前記高相関通信装置群を抽出する、請求項 1 または 2 に記載のログ分析装置。

【請求項 4】

前記攻撃はブルートフォース攻撃であり、前記攻撃はログイン試行である請求項 1 乃至 3 のいずれか 1 項に記載のログ分析装置。

【請求項 5】

攻撃元通信装置から攻撃を受ける複数の被攻撃先通信装置をネットワーク機器から収集したログに基いて分類するログ分析方法であって、

前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した検知時刻および前記検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する相関係数を前記ログに基いて計算することと、

前記相関係数が所定の閾値以上であり、かつ、前記期間において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出することと、

を含むログ分析方法。

30

【請求項 6】

コンピュータに、攻撃元通信装置から攻撃を受ける複数の被攻撃先通信装置をネットワーク機器から収集したログに基いて分類させるプログラムであって、

前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した検知時刻および前記検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する相関係数を前記ログに基いて計算し、

前記相関係数が所定の閾値以上であり、かつ、前記期間において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出、

する処理を前記コンピュータに実行させるプログラム。

40

【発明の詳細な説明】**【技術分野】**

50

【0001】

本発明は、ログ分析装置、方法およびプログラムに関するものである。

【背景技術】

【0002】

近年、ネットワーク上でのサイバー攻撃が活発化している。例として、攻撃者がホストプロバイダの「admin」などの監視者ユーザ名に対するブルートフォース攻撃を実施し、パスワードを搾取するものがある。そして、サイバー攻撃の活発化に伴って、被害も深刻化している。このようなサイバー攻撃では、攻撃を受けた通信装置を管理するプロバイダは、攻撃元のIPアドレスを特定し、そのアドレスからの通信を遮断する防御策を取ることで対応する。

10

【0003】

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)と呼ばれるセキュリティ装置が知られている。一般にIDSでは、ネットワーク上を流れるパケットがサーバー攻撃などの特異事象のパターンであるか否かを判定し、特異事象のパターンである場合は、ログに記録する。パケットがサーバー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いて判定したりする。

【0004】

また、侵入検知システムのようなセキュリティ装置を含むセキュリティ対策システムであって、セキュリティ装置が収集したログのパターン分析を行うなど、セキュリティ装置の運用を支援するマネージドセキュリティサービス(Managed Security System、MMS)が知られている。

20

【0005】

さらに、侵入検知システムから出力されるログを分析するために、ログ分析装置が知られている。

【0006】

ログ分析装置の一例では、まず、過去のある期間に記録されたイベントの到着間隔または継続時間を示す時間値に関する分布を生成し、生成した分布の平均値および標準偏差に基いて理論統計分布を生成する。次に、分析対象の所定期間に記録されたイベントの時間値に関する分布と、理論統計分布との相関を表す相関係数を算出し、相関係数の値が所定値以下の場合に分析対象のイベントが特異であると判断する。

30

【0007】

また、別のログ分析装置では、まず、ネットワークに設置されている侵入検知システム(IDS)やファイアウォール(FW)等のセキュリティ装置が検出したイベント情報を度数化した統計情報と、その統計情報を周波数分解して得られる周波数成分情報とを得て、その周波数成分に基いてインシデントの発生傾向を判断する。このような構成を採用することによって、ネットワーク上で発生した1つあるいは複数の攻撃を記録したセキュリティ装置のログに対し、効率的に特徴づけを行い、その中の特異な変化を検出することで、複雑なインシデントを検出することができる。ここで、インシデントとは、コンピュータセキュリティに関連したイベントのことを指す。

40

【0008】

さらに別のログ分析装置では、まず、ログ中から分析に用いるパラメータを抽出し、そのパラメータに属するイベントの数に基いてネットワークの異常度に関する異常値を算出する。次に、その異常値に関する所定の条件が満たされた場合に所定の事象が発生する条件付確率を算出することで未来のイベント数の推移を客観的に予測する、たとえば、所定の事象が発生する条件付確率を算出する。パラメータとしては、侵入検知システム、ルータ、ファイアウォールなどのネットワーク機器から出力されるログに記録されている、Attack Signature、Source/Destination PortおよびSource/Destination IDなどが挙げられる。異常値として

50

は、比率分析における比率や、確率分析における上側稀率、下側稀率が挙げられる。

【0009】

このようなログ分析装置では、特に、攻撃の回数たとえば、毎分100回などと多く、同じ攻撃パターン、たとえば攻撃元も攻撃先も毎回変わらないような攻撃が繰り返し発生しているような場合には、攻撃を検知することができる。ここで攻撃元、攻撃先はそれぞれ、攻撃元IPアドレス、攻撃先IPアドレスで指定され得る。

【先行技術文献】

【非特許文献】

【0010】

【特許文献1】特開2005-236862号公報

10

【特許文献2】特開2006-319633号公報

【特許文献3】特開2005-196675号公報

【発明の概要】

【発明が解決しようとする課題】

【0011】

近年、ブルートフォース攻撃の攻撃者は、複数の攻撃先に対して、断続的に攻撃元を変えて攻撃をしたり、攻撃開始から終了まで単一の攻撃元から行うログイン試行などの攻撃の回数を少なくしたりと、侵入検知システム(Intrusion Detection System、IDS)などのセキュリティ装置からの検出を回避するための手段を採用している。そのため、このような攻撃の攻撃元を特定するには長い期間にわたりセキュリティ装置のログを分析しないといけないという問題がある。

20

【0012】

よって、一つの側面として、本発明は、ログに基づいて、複数の通信装置の中から、効率よく攻撃対象となる通信装置を抽出することを目的とする。

【課題を解決するための手段】

【0013】

攻撃元通信装置から攻撃を受ける複数の被攻撃先通信装置をネットワーク機器から収集したログに基いて分類するログ分析装置が提供される。ログ分析装置は、複数の被攻撃先通信装置の組み合わせに対して、攻撃を前記ネットワーク機器が検知した検知時刻および検知時間を含む攻撃が行われた期間における攻撃の回数に関する相関係数をログに基いて計算する相関係数計算部と、相関係数が所定の閾値以上であり、かつ、期間において攻撃元通信装置が同一である複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出する抽出部と、を含むことを特徴とする。

30

【発明の効果】

【0014】

ログに基づいて、複数の通信装置の中から、効率よく攻撃対象となる通信装置を抽出することができる。

【図面の簡単な説明】

【0015】

【図1】ブルートフォース攻撃の例の概略を説明する図である。

40

【図2】ブルートフォース攻撃の一例を受けた通信装置のログの例を示す図である。

【図3】図2に示されているログの一部を拡大した図である。

【図4】ブルートフォース攻撃の別の例を受けた通信装置のログの例を示す図である。

【図5】ログ分析装置を含むシステムの概略を説明する図である。

【図6】ログ分析装置の出力の例を示す図である。

【図7】侵入検知システムとログ分析装置の機能ブロック図の例を示す図である。

【図8】ログ分析装置のインターフェース部の出力画面の例を示す図である。

【図9】侵入検知システムのIDSログデータベースに格納されるデータの例を示す図である。

【図10】ログ分析装置の分析設定データベースに格納されるデータの例を示す図である

50

。

【図 1 1】侵入検知システムの要対策通信装置 IP アドレスデータベースに格納されるデータの例を示す図である。

【図 1 2】ログ分析装置が侵入検知システムの IDS ログデータベースから受け取るログデータの例を示す図である。

【図 1 3】ブルートフォース攻撃分析部で作成されるポート番号ごとの攻撃元 (H a c k e r)、攻撃回数、検知時刻 (t i m e)、被攻撃先 (被攻撃先通信装置 (V i c t i m)) についてのデータの示す回数データ列の例を示す図である。

【図 1 4】ブルートフォース攻撃分析部で関連の高い通信装置を抽出する様子の例を示す図である。

10

【図 1 5】ブルートフォース攻撃分析部で関連の高い通信装置を抽出する様子の例を示す図である。

【図 1 6】最大クリーク法の概略を説明するための図である。

【図 1 7】最大クリーク法を用いるブルートフォース攻撃分析部の機能ブロック図の例を示す図である。

【図 1 8 A】図 1 7 に示されているブルートフォース攻撃分析部のペア生成部の出力の例を示す図である。

【図 1 8 B】図 1 7 に示されているブルートフォース攻撃分析部のクリーク探索部の出力の例を示す図である。

【図 1 8 C】図 1 7 に示されているブルートフォース攻撃分析部の出力部の出力の例を示す図である。

20

【図 1 9】コンピュータの構成の例を示す図である。

【図 2 0】ログ分析処理の流れを示す図である。

【発明を実施するための形態】

【 0 0 1 6 】

以下、図面を参照して、まず、概略について説明し、その後、実施形態のログ分析装置、方法およびプログラムについて説明する。

【 0 0 1 7 】

< 概略 >

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。攻撃を効率的に実施するために、辞書に収集されている単語を候補として探す辞書攻撃や、システムに初期設定される値を使うといった手段も存在する。さらに、ブルートフォース攻撃には、あるシステムから漏洩したと考えられる大量の識別子 (I D)、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得る。

30

【 0 0 1 8 】

以下では、次のような用語を用いる。

「攻撃元」とは、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し、発信元の IP アドレスを意味することもある。

【 0 0 1 9 】

ここで、「IP アドレス」とは、通信の送受信を行う通信装置を識別するための番号である。

40

【 0 0 2 0 】

「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し、攻撃を受ける通信装置の IP アドレスを意味することもある。

【 0 0 2 1 】

「 V i c t i m 」とは、被攻撃先のことである。

「検知時刻」とは、侵入検知システム (I D S)、侵入防止システム (I P S) 等がブルートフォース攻撃を検知した時刻である。

【 0 0 2 2 】

「ログイン試行回数」とは、ある検知時刻を含むある連続的期間において、攻撃元から

50

被攻撃先へログイン試行のブルートフォース攻撃が検知された回数であり得る。たとえば、ある時刻から5分間にわたり、ある被攻撃先がある攻撃元から攻撃を受けた場合、その5分間の攻撃の総数でも良い。また、このログイン試行回数は、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。たとえば、1分間あたりのログイン試行の回数であっても良い。たとえば、ある時刻から5分間にわたり、ある被攻撃先がある攻撃元から攻撃を受けた場合、1分あたりの攻撃の回数の平均であっても良い。また、5分間を1分の攻撃が5回行われたとしても良い。この場合、ログイン試行回数は、1分ごとの平均であってもよい。

【0023】

また、「ログイン試行回数」を単に攻撃の回数と呼ぶこともある。

10

「ポート番号」とは、攻撃が検知された被攻撃先の通信装置のポート番号である。

【0024】

侵入検知システム (IDS) は、ブルートフォース攻撃を検知したり、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したりといった対策のために用いられる。一般に、IDSは、攻撃元IPアドレスを特定する機能を有する。IDSで攻撃元IPアドレスが特定されれば、ユーザはそのアドレスからの通信を遮断するなどして防御を行う。

【0025】

侵入防止システム (IPS) は異常を通知するだけでなく、ファイアウォールと連動して通信を遮断するなどのネットワーク防御を自動で行う機能を持つ。

20

【0026】

図1はブルートフォース攻撃の例の概略を説明する図である。

図1に示されているブルートフォース攻撃では、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攻撃が行われる。

【0027】

図1では、たとえば、時刻 t_1 では、攻撃元 H_1 から被攻撃先 V_1 、 V_2 、...、 V_{m-1} 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。時刻 t_3 では、攻撃元 H_3 から被攻撃先 V_2 、...、 V_m へブルートフォース攻撃を行い、時刻 t_4 では、攻撃元 H_4 から被攻撃先 V_1 、 V_2 、...、 V_{m-1} へブルートフォース攻撃を行う。時刻 t_{n-1} では、攻撃元 H_{n-1} から被攻撃先 V_2 、...、 V_m へブルートフォース攻撃を行い、時刻 t_n では、攻撃元 H_n 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。

30

【0028】

図2は、ブルートフォース攻撃の一例を受けた通信装置のログの例を示す図であり、図3は図2に示されているログの一部を拡大した図である。

【0029】

図2のウィンドウKとして示されている部分に、図1のようなブルートフォース攻撃を見ることができる。

【0030】

たとえば、図3に示されているように、時刻 T_1 で通信装置 (Victim) の番号が、18、21-22、29、30、36、38-40の通信装置は、Hacker A (攻撃元) から毎分15回のログイン試行を1分間にわたり行うというブルートフォース攻撃 (A列) を受けている。また、時刻 T_2 で通信装置 (Victim) の番号が、18、21、22、28-30、36、38、40の通信装置はHacker B (攻撃元) から毎分20回のログイン試行を1分間にわたり行うというブルートフォース攻撃 (B列) を受けている。また、時刻 T_3 から5分間にわたり通信装置 (Victim) の番号が、18、21-22、28-30、36、38-40の通信装置は、Hacker C (攻撃元) から毎分18回のログイン試行を行うというブルートフォース攻撃 (C列) を受けている。

40

【0031】

50

このように、図 2、3 に示されているログは、攻撃を受ける期間によって異なる攻撃元から特定の被攻撃先群へ向けて繰り返しブルートフォース攻撃が行われていることを示している。攻撃を受けた通信装置のログを検証すると、このようなブルートフォース攻撃は、攻撃元、被攻撃先、ログイン試行回数、攻撃検知時刻について、次のような特徴を有している。

【0032】

攻撃元については、攻撃元は攻撃のたびに異なる。「攻撃元が攻撃のたびに異なる」という意味は、攻撃を受ける側から見ると、複数の被攻撃先に対して断続的に攻撃元を変えて攻撃が行われる、という意味であり得る。

【0033】

被攻撃先については、特定の被攻撃先群が複数の攻撃元から比較的長期間継続して攻撃を受ける。被攻撃先群の中には、被攻撃先群中の他の通信装置が攻撃を受けたものの、攻撃を受けないものも存在する。途中から攻撃を受けるようになり新たに被攻撃先群に加わる被攻撃先や、逆に途中から攻撃を受けなくなった被攻撃先や、また一定の期間のみ攻撃を受ける被攻撃先も存在し得る。

【0034】

ログイン試行回数は、比較的少ない。たとえば、分析対象とするログ全体のログイン試行回数の平均が72回程度のときに、平均18回程度という場合もある。

【0035】

攻撃検知時刻は、ある一つの攻撃元から被攻撃先群に対してほぼ同時刻において攻撃が検知される。しかし、被攻撃先によっては、時間的に連続して攻撃が検知されるものもあれば、そうでない被攻撃先も存在する。

【0036】

このように、図 1 - 3 に示されているログのウィンドウ K に含まれるブルートフォース攻撃は次のような特徴を有する。

(C1) 複数の被攻撃先が、ほぼ同時刻に、同じログイン試行回数の攻撃を受ける、

(C2) 攻撃元は攻撃のたびに異なる、

(C3) 侵入検知システム (IDS) や侵入防止システム (IPS) からの検知を回避するために、少ないログイン試行回数でブルートフォース攻撃を行う。

【0037】

上記の特徴は、図 2 に示されているようなブルートフォース攻撃が有する特徴とは異なっている。

【0038】

図 4 は、ブルートフォース攻撃の別の例を受けた通信装置のログの例を示す図である。

図 4 には、攻撃元 A から特定の被攻撃先がブルートフォース攻撃を受け (A 系列)、別の攻撃元 B から別の被攻撃先がブルートフォース攻撃を受ける (B 系列) 様子が示されている。図 4 に示されているようなブルートフォース攻撃では、攻撃元が特定されれば、その攻撃元からの通信を遮断することで、攻撃を防御することができる。しかしながら、図 1 - 3 に示されているようなブルートフォース攻撃に対策を施すとしても、このような攻撃を受ける通信装置をグループ化し、被攻撃先群 (Victim 群) として特定する必要がある。

【0039】

図 5 は、グループ化装置を含むシステムの概略を説明する図である。

システム 10 は、侵入検知システム (IDS) 110 と、侵入検知システム (IDS) 110 から提供される IDS ログを分析し、攻撃を受ける通信装置をグループ化し、攻撃先群 (Victim 群) として特定するログ分析装置 100 を含んでいる。ログ分析装置 100 は、IDS ログ分析装置と呼ばれることもある。

【0040】

侵入検知システム (IDS) 110 は、ネットワーク 120 に接続され、グループ化装置 100 に IDS ログ 140 を提供する。

10

20

30

40

50

【0041】

ログ分析装置100は、相関係数計算部1002、抽出部(通信装置(Victim)群選択部)1004、および出力部1006を含む。

【0042】

相関係数計算部1002は、IDSログ140に基づいて、攻撃元(Hacker)、攻撃回数、検知時刻の3つについて、複数の被攻撃先(Victim)の相関係数を計算する。

【0043】

抽出部1004は、相関係数の高い通信装置(Victim)を抽出し、攻撃先群(Victim群)として特定する。

10

【0044】

出力部1006は、抽出部1004で特定された通信装置(Victim)は、要対策通信装置リスト150に登録し、侵入検知システム(IDS)110に送る。

【0045】

要対策通信装置リスト150を受けた侵入検知システム(IDS)110は、リスト150に登録されている通信装置に対し、ログイン試行に対する監視を強めるなどの対策を行う。

【0046】

また、抽出部1004は、相関係数が所定の閾値以上であり、かつ、期間の各々において前記攻撃元通信装置が同一である複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出する。

20

【0047】

図6は、ログ分析装置の出力の例を示す図である。

図6に示されている表には、攻撃元(Hacker)、検知時刻、被攻撃先とログイン試行回数が含まれている。

【0048】

たとえば、攻撃元(Hacker)h₂は11月1日4時に、通信装置(Victim)v₁、v₂、v₃、v₄、v₅に対し12回のログイン試行を行うブルートフォース攻撃を仕掛けている。攻撃元(Hacker)h₂は11月1日4時1分に、通信装置(Victim)v₁、v₂、v₃、v₄、v₅に対し9回から10回(v₁に対してのみ10回でその他に対しては9回)のログイン試行を行うブルートフォース攻撃を仕掛けている。攻撃元(Hacker)h₂は11月1日4時2分には、通信装置(Victim)v₁、v₂、v₃、v₄、v₅に対し3回から4回(v₁に対してのみ3回でその他に対しては4回)のログイン試行を行うブルートフォース攻撃を仕掛けている。また、攻撃元(Hacker)h₃は11月1日4時3分に、通信装置(Victim)v₆に対して、100回のログイン試行を行うブルートフォース攻撃を仕掛けている。

30

【0049】

図6に示されている例では、攻撃元(Hacker)h₂からの攻撃は、図1-3に示されているようなブルートフォース攻撃であり、攻撃元(Hacker)h₃からの攻撃は図4に示されているようなブルートフォース攻撃である。よって、通信装置(Victim)v₁、v₂、v₃、v₄、v₅が、複数の攻撃先に対して断続的に攻撃元を変えて攻撃をするブルートフォース攻撃を受ける可能性が高い通信装置(Victim)群として特定されている。また、攻撃元(Hacker)h₃から通信装置(Victim)v₆に対する攻撃は、図1-3に示されているようなブルートフォース攻撃ではない。

40

【0050】

このようにログ分析装置100は、攻撃元通信装置から攻撃を受ける複数の被攻撃先通信装置を侵入検知システム(IDS)110等のネットワーク機器から収集したログに基づいて分類する。

【0051】

ログ分析装置100の相関係数計算部1002は、複数の被攻撃先通信装置の組み合わ

50

せに対して、攻撃を侵入検知システム（IDS）110等のネットワーク機器が検知した検知時刻および検知時間を含む攻撃が行われた期間における攻撃の回数に関する相関係数をログに基いて計算しても良い。

【0052】

ログ分析装置100の抽出部1004は通信装置（Victim）群選択部1004や高相関通信装置群選択部1004と呼ばれることもある。

【0053】

抽出部1004は、相関係数が所定の閾値以上であり、かつ、ある期間において攻撃元通信装置が同一である複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出しても良い。

10

【0054】

出力部1006は、高相関通信装置群に関する情報を侵入検知システム（IDS）110等のネットワーク機器に出力しても良い。高相関通信装置群に関する情報を受けた侵入検知システム（IDS）110等のネットワーク機器は、高相関通信装置群のIPアドレスに向けてのアクセスを重点的に監視し、攻撃に備えることができる。

【0055】

ここで、攻撃は断続的に複数の期間にわたり行われ、検知時刻は複数であり、複数の期間の各々はそれぞれ異なる前記複数の検知時刻の一つを含んでも良い。この場合、相関係数計算部1002は、複数の被攻撃先通信装置の組み合わせに対して、攻撃を侵入検知システム（IDS）110等のネットワーク機器が検知した複数の検知時刻および複数の期間の各々における前記攻撃の回数に関する相関係数を前記ログに基いて計算しても良い。

20

【0056】

抽出部1004は、複数の被攻撃先通信装置が受けた攻撃の検知時刻および検知時間を含む攻撃が行われた期間における攻撃の回数に関する情報に対応した頂点と、所定の閾値以上の相関係数を有する複数の被攻撃先通信装置のうち2つに対応する頂点間に付与した辺を含むグラフから、クリークを抽出することによって高相関通信装置群を抽出しても良い。このように抽出部1004は、最大クリーク法等のグラフ理論における手法を用いても良い。

【0057】

また、ログ分析装置100は、ログから、ブルートフォース攻撃を受けた通信装置のみを対象として通信装置の分類（グループ化）を行っても良い。

30

【0058】

上記のような構成を採用することによって、

（E1）長期間にわたりログを収集せずとも、将来攻撃を受ける可能性が高い通信装置（Victim）群を特定することができる、

（E2）特定された通信装置（Victim）群を重点的に監視することで、ブルートフォース攻撃に対する対策を促すことができる、

（E3）要対策通信装置リスト150を適宜更新することができるので、被攻撃先群の変化を追跡することができる、たとえば、ある時刻から要対策通信装置リスト150に載らなくなった通信装置があるとすれば、攻撃者が何らかの理由でその通信装置を攻撃先から外した、攻撃が成功してブルートフォース攻撃を行う必要がなくなったなどの変化を推測することができる、

40

などの効果を奏する。

【0059】

< 侵入検知システム（IDS）とログ分析装置 >

図7は侵入検知システム（IDS）110とログ分析装置100の機能ブロック図の例を示す図である。

【0060】

図7に示されているログ分析装置100は、侵入検知システム（IDS）110と組み合わせられて、上記の（C1）～（C3）のような特徴を有するようなブルートフォース攻

50

撃に対応するため、このような攻撃を受ける通信装置をグループ化するログ分析装置である。そして、上記(E1)～(E3)のような効果を得ることができる。

【0061】

図7では、ログ分析装置100は、侵入検知システム(IDS)110とは別の外の装置である。しなしながら、ログ分析装置100は、侵入検知システム(IDS)110の中に組み込まれてもよい。

【0062】

侵入検知システム(IDS)110は、攻撃探知部112、IDSログデータベース(DB)114、攻撃対策部116、および要対策通信装置(Victim)IPアドレスデータベース(DB)118を含む。

10

【0063】

侵入検知システム(IDS)110の攻撃探知部112は、たとえば、図5に示されているようにネットワーク120に接続され、ネットワーク120を流れる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ログ分析装置100に向けて発行する。

【0064】

侵入検知システム(IDS)110のIDSログデータベース(DB)114は、攻撃探知部112によって検知され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格納する。

【0065】

図9は侵入検知システム(IDS)110のIDSログデータベース(DB)114に格納されるデータの例を示す図である。

20

【0066】

図9に示されているように、IDSログデータベース(DB)114に格納されるデータには、攻撃元(Hacker)、被攻撃先(Victim)、検知時刻、ログイン試行回数(攻撃回数)、被攻撃先のポート(Port)が含まれている。

【0067】

たとえば図9に示されているデータからは、IPアドレスが「11.22.33.44」の攻撃元(Hacker)のから、IPアドレスが「55.66.77.88」の被攻撃先(Victim)のポート番号(Port)「22」に対し、検知時刻「2013年4月1日0時0分」にログイン試行回数30回のブルートフォース攻撃が行われたことが分かる。

30

【0068】

ログ分析装置100は、侵入検知システム(IDS)110のIDSログデータベース(DB)114に格納されるデータに基づいて、ブルートフォース攻撃の攻撃元と考えられる通信装置のIPアドレスを要対策通信装置(Victim)IPアドレスとして特定する。具体的には、ログ分析装置100は、IDSログデータベース(DB)114に格納されるデータに基づいて、攻撃元(Hacker)、攻撃回数、検知時刻の3つについて、複数の被攻撃先(Victim)の相関係数を計算する。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ても良い。そして、相関係数の高い通信装置(Victim)を抽出し、通信装置群(Victim群)として特定する。これらの通信装置群を被攻撃先群と呼ぶこともある。

40

【0069】

図8は、ログ分析装置の出力画面の例を示す図である。

図8に示されているように、ブルートフォース攻撃の攻撃元の候補であるIPアドレスが、そのIPアドレスが攻撃元と認定された日時(追加日)と共に表示される。

【0070】

図8の例では、IPアドレス「55.66.77.88」は「2013年4月1日12時0分」に攻撃元の候補と認定されたことが表示される。

【0071】

50

図 8 の例において、「<分析設定>」の欄は、攻撃先群（Victim群）を特定する際の相関係数の閾値、分析に使用したログデータの期間を含んでいる。

【0072】

侵入検知システム（IDS）110の要対策通信装置（Victim）IPアドレスデータベース（DB）118には、ログ分析装置100において特定された要対策通信装置（Victim）IPアドレスが、そのIPアドレスが攻撃元の候補と認定された日時（追加日）と共に格納されている。

【0073】

図 11 は、侵入検知システム 110 の要対策通信装置（Victim）IP アドレスデータベース（DB）118 に格納されるデータの例を示す図である。要対策通信装置（Victim）IP アドレスデータベース（DB）118 に格納されるデータは、図 5 に示されている要対策通信装置リスト 150 に対応する。

10

【0074】

図 11 の例では要対策通信装置（Victim）IP アドレスデータベース（DB）118 には、たとえば、IP アドレス「55.66.77.88」は「2013年4月1日12時0分」に攻撃元と認定されたことを示すデータが格納されている。

【0075】

侵入検知システム（IDS）110の攻撃対策部116は、要対策通信装置（Victim）IPアドレスデータベース（DB）118に格納されているリストに含まれる攻撃元からの通信に対する対策を行う。たとえば攻撃対策部116は、要対策通信装置（Victim）からログイン試行があたったときに、アラート（警報）を発しても良い。また、攻撃対策部116は、要対策通信装置（Victim）からの通信を遮断しても良い。

20

【0076】

ログ分析装置100は、ブルートフォース攻撃分析部102、分析設定データベース（DB）104、インターフェース部106を含む。

【0077】

ログ分析装置100のブルートフォース攻撃分析部102は、図5の相関係数計算部1002と抽出部1004の機能を合わせた機能を有している。すなわち、侵入検知システム（IDS）110のIDSログデータベース（DB）114に格納されるデータに基づいて、ブルートフォース攻撃の攻撃元と考えられる通信装置のIPアドレスを要対策通信装置（Victim）IPアドレスとして特定する。具体的には、ログ分析装置100は、IDSログデータベース（DB）114に格納されるデータに基づいて、攻撃元（Hacker）、攻撃回数、検知時刻の3つについて、複数の被攻撃先（Victim）の相関係数を計算する。攻撃回数、検知時刻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ても良い。そして、相関係数の高い通信装置（Victim）を抽出し、被攻撃先群（Victim群、通信装置群）として特定する。

30

【0078】

ログ分析装置100の分析設定データベース（DB）104は、ブルートフォース攻撃分析部102で相関係数と計算し、相関係数の高い通信装置（Victim）を抽出し、被攻撃先群（Victim群）として特定する際のパラメータが格納されている。

40

【0079】

図 10 は、ログ分析装置 100 の分析設定データベース 104 に格納されるデータの例を示す図である。

【0080】

図 10 に示されているように、分析設定データベース 104 に格納されるデータは、被攻撃先群（Victim群）を特定する際の相関係数の閾値、分析に使用したログデータの期間（分析の間隔）を含んでいる。図 10 の例では、相関係数の閾値は 0.8、分析の間隔は 0.5 日である。

【0081】

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

50

t_i として、

【数 1】

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

として定義しても良い。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 分間あたりのログイン試行回数であっても良い。 10

【0082】

ログ分析装置 100 のインターフェース部 106 は、ブルートフォース攻撃分析部 102 で特定されたブルートフォース攻撃の被攻撃先に関する情報を表示する。インターフェース部 106 の出力の例は、図 8 に示されている。分析設定データベース 104 に格納されるデータは、図 8 に示されているインターフェース部 106 の出力の例では、「<分析設定>」の欄の出力に用いられる。

【0083】

またログ分析装置 100 のインターフェース部 106 は、ブルートフォース攻撃分析部 102 で特定されたブルートフォース攻撃の被攻撃先に関する情報をログ分析装置 100 に送る。このブルートフォース攻撃の被攻撃先に関する情報は、図 5 に示されている要対策通信装置リスト 150 に対応する。要対策通信装置リスト 150 に含まれる情報は、侵入検知システム (IDS) 110 の要対策通信装置 (Victim) IP アドレスデータベース (DB) 118 に格納される。 20

【0084】

<<ブルートフォース攻撃分析部の機能>>

ここで、ログ分析装置 100 のブルートフォース攻撃分析部 102 の機能について説明する。

【0085】

ログ分析装置 100 のブルートフォース攻撃分析部 102 では、まず、ログ分析装置 100 の IDS ログデータベース (DB) 114 に格納されるデータを取得する。そして、そのデータに基づいて、攻撃元 (Hacker)、被攻撃先 (Victim)、検知時刻、ログイン試行回数 (攻撃回数)、被攻撃先のポート (Port) に関する回数データ列を作成する。 30

【0086】

図 12 は、侵入検知システム 110 の IDS ログデータベース 114 から受け取るログデータの例を示す図である。図 12 は図 9 と同様であり、IDS ログデータベース (DB) 114 に格納されるデータには、攻撃元 (Hacker)、被攻撃先 (Victim)、検知時刻、ログイン試行回数 (攻撃回数)、被攻撃先のポート (Port) が含まれている。 40

【0087】

たとえば図 12 に示されているデータからは、IP アドレスが「11.22.33.44」の攻撃元 (Hacker) のから、IP アドレスが「55.66.77.88」の被攻撃先 (Victim) のポート番号 (Port) 「22」に対し、検知時刻「2013 年 4 月 1 日 0 時 0 分」にログイン試行回数 30 回のブルートフォース攻撃が行われたことが分かる。

【0088】

次に、ログ分析装置 100 のブルートフォース攻撃分析部 102 は、図 12 に示されているデータから、ポートごとに、どの攻撃元 (Hacker) から、いつ (time)、 50

どの被攻撃先（被攻撃先通信装置（Victim））にブルートフォース攻撃があったか、に関する情報を含む回数データに書き直す。

【0089】

図13は、ブルートフォース攻撃分析部で作成されるポート番号ごとの攻撃元（Hacker）、攻撃回数、検知時刻（time）、被攻撃先（被攻撃先通信装置（Victim））についてのデータの示す回数データ列の例を示す図である。

【0090】

たとえば図13に示されている回数データ列の例からは、IPアドレス「11.22.33.44」の攻撃元から、検知時刻「2013年11月1日4時0分」に、IPアドレス、「11.22.33.44」、「2.22.33.44」、「3.22.33.44」、「4.22.33.44」、「5.22.33.44」を有する被攻撃先にログイン試行回数12回のブルートフォース攻撃が行われたことが分かる。また、IPアドレス「11.22.33.44」の攻撃元は、検知時刻「2013年11月1日4時1分」に、IPアドレス、「11.22.33.44」、「2.22.33.44」、「3.22.33.44」、「4.22.33.44」、「5.22.33.44」を有する被攻撃先にログイン試行回数9回または10回のブルートフォース攻撃を行い、検知時刻「2013年11月1日4時2分」には、同じ被攻撃先に対して、ログイン試行回数3回または4回のブルートフォース攻撃を行っている。

【0091】

次に、ログ分析装置100のブルートフォース攻撃分析部102は、試行回数、検知時刻、攻撃元（Hacker）について相関が高い通信装置（Victim）群を抽出する。これは、複数の攻撃先に対して複数の異なる攻撃元からブルートフォース攻撃をしたり、攻撃開始から終了まで単一の攻撃元から行うログイン試行などのブルートフォース攻撃の回数が少ないようなブルートフォース攻撃が有する特徴、すなわち、

（C1）複数の被攻撃先が、ほぼ同時刻に、同じログイン試行回数の攻撃を受ける、

（C2）攻撃元は攻撃のたびに異なる、

（C3）侵入検知システム（IDS）や侵入防止システム（IPS）からの検知を回避するために、少ないログイン試行回数でブルートフォース攻撃を行う、

のうち、特徴（C1）を利用している。試行回数、検知時刻について相関が高い通信装置（Victim）群を抽出する際には、最大クリーク法を用いることができる。

【0092】

図14は、ブルートフォース攻撃分析部1024で相関の高い通信装置を抽出する様子の例を示す図である。

【0093】

たとえば図14に示されている回数データ列の例では、「11.22.33.44」、「2.22.33.44」、「3.22.33.44」の3つのIPアドレスを有する通信装置が、検知時刻「2013年11月1日4時0分」、「2013年11月1日4時1分」、「2013年11月1日4時2分」に、ログイン試行回数12回、ログイン試行回数9～10回、ログイン試行回数3～4回のブルートフォース攻撃を受けている。

【0094】

そして、ブルートフォース攻撃分析部102は、「11.22.33.44」、「2.22.33.44」、「3.22.33.44」の3つのIPアドレスを有する通信装置を、相関が高い被攻撃先通信装置（Victim）の候補として選ぶ。

【0095】

図15は、ブルートフォース攻撃分析部で相関の高い通信装置を抽出する様子の例を示す図である。IPアドレス「11.22.33.44」、「2.22.33.44」、「3.22.33.44」を有する通信装置が受けたブルートフォース攻撃の攻撃元はいずれもIPアドレス「11.22.33.44」を有する通信装置である。

【0096】

よって、ブルートフォース攻撃分析部102は、「11.22.33.44」、「2.

10

20

30

40

50

「22.33.44」、 $\{3.22.33.44\}$ の3つのIPアドレスを有する通信装置を、相関が高い被攻撃先通信装置 (Victim) として出力する。

【0097】

このようにして、試行回数、検知時刻、攻撃元 (Hacker) について相関が高い通信装置 (Victim) 群を抽出することができる。

【0098】

ここで、最大クリーク法を用いた、試行回数、検知時刻について相関が高い通信装置 (Victim) 群の抽出について説明する。

【0099】

最大クリーク問題とは、無向グラフ中の部分グラフの中の完全グラフでサイズが最大のものを選び出す組み合わせ最適化問題の一種である。

【0100】

まず用語をいくつか定義する。

「クリーク」とは、完全グラフを誘導する頂点集合である。完全グラフとは任意の2つの頂点の間に辺が存在するグラフである。

【0101】

「最大クリーク」とは、グラフ中で頂点数が最大のクリークである。

最大クリーク法は、グラフ中のクリークの中で最大のものを見付ける方法である。アルゴリズムの一つは、まず、候補節点集合を探す。「候補節点集合」とは、ある時点で保持しているクリークに付け加えても、またクリークとなるような頂点の集合である。そして、候補節点集合中の頂点をクリークに追加し、頂点数が1つだけ増加したクリークを作る。この操作を出来る限り繰り返すことにより、最大クリークを見付ける。

【0102】

図16は最大クリーク法の概略を説明するための図である。

図16に示されているグラフは、1から6で指定される6つの頂点を含んでいる。頂点1は、頂点2、5と、頂点2は、頂点1、3、5と、頂点3は頂点2、4と、頂点4は頂点3、5、6と、頂点5は頂点1、2、4と辺によって結ばれている。

【0103】

図16に示されているグラフでは、頂点1、2、5によって構成されるクリークが最大クリークである。

【0104】

最大クリーク法を、相関係数の高い通信装置 (Victim) を抽出し、攻撃先群 (Victim群) として特定する問題に適用するには、各頂点には、ブルートフォース攻撃を受けた通信装置 (Victim) を割り当てる。さらに、各頂点には、その通信装置 (Victim) が受けたブルートフォース攻撃のロゲイン試行回数、検知時刻、攻撃元 (Hacker) に関するデータを対応させる。

【0105】

頂点間を辺で結ぶか否かは、その通信装置 (Victim) が受けたブルートフォース攻撃の回数、検知時刻の2つに関する相関を計算し、所定の閾値以上であれば2つの頂点を辺で結ぶ。ブルートフォース攻撃の回数は、単位時間あたりのロゲイン試行回数であっても良い。単位時間は1分であり得る。

【0106】

たとえば、通信装置 v_i が割り当てられた頂点 i ($i = 1 \sim n$) の相関係数を求めるには次のような方法がある。

【0107】

たとえば、通信装置 v_1 が割り当てられた頂点1と通信装置 v_2 が割り当てられた頂点2の相関係数 R_2 を計算し、閾値以上であるか否かによって頂点1と2を辺で結ぶか否かを決定しても良い。

【0108】

相関係数 R_2 は、通信装置 v_i ($i = 1, 2$) 受けたブルートフォース攻撃の回数を x

10

20

30

40

50

i 、検知時刻を t_i とし、

【数 2】

$$R_2 = \frac{\sum_{i=1}^2 (x_i - x_{av})(t_i - t_{av})}{\sqrt{\sum_{i=1}^2 (x_i - x_{av})} \sqrt{\sum_{i=1}^2 (t_i - t_{av})}}$$

と定義してもよい。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。

【0109】

または、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、ブルートフォース攻撃の回数 x_i の差と、検知時刻 t_i についての差が共に、所定の範囲内にあるときに、通信装置 v_i が割り当てられた頂点間を辺で結んでも良い。

【0110】

図 17 は、最大クリーク法を用いるブルートフォース攻撃分析部 102 の機能ブロック図の例を示す図である。

【0111】

図 17 に示されているブルートフォース攻撃分析部 102 は、ペア生成部 1022、クリーク探索部 1024、および出力部 1026 を含んでいる。

【0112】

ブルートフォース攻撃分析部 102 のペア生成部 1022 では、相関の高い、すなわち相関係数が閾値以上である通信装置 (Victim) のペアを作る。相関係数の閾値は、分析設定 DB 104 に格納されているものを用いても良い。

【0113】

まずブルートフォース攻撃分析部 102 のペア生成部 1022 は、ログ分析装置 100 の IDS ログデータベース (DB) 114 に格納されるデータを取得する。次に、ペア生成部 1022 は、取得したデータに基づいて、攻撃元 (Hacker)、被攻撃先 (Victim)、検知時刻、ログイン試行回数 (攻撃回数)、被攻撃先のポート (Port) に関する回数データ列を作成する。そして、ペア生成部 1022 は、検知時刻、ログイン試行回数 (攻撃回数) について相関の高い通信装置 (Victim) のペアを作る。

【0114】

通信装置 (Victim) 同士のペアは、グラフではそれぞれが割り当てられた頂点間を辺で結ばれることによって表現される。

【0115】

図 18 A は、図 17 に示されているブルートフォース攻撃分析部のペア生成部 1022 の出力の例を示す図である。

【0116】

図 18 A の例では、victim1 で指定される通信装置と victim2 で指定される通信装置がペアを形成する。また、victim10 で指定される通信装置は、victim13 および victim14 で指定される通信装置とペアを形成する。さらに、victim13 で指定される通信装置と victim14 で指定される通信装置がペアを形成する。

【0117】

これをグラフ化すると次のようなグラフになる。まず、victim1 が割り当てられる頂点と、victim2 が割り当てられる頂点の間は辺で結ばれており、victim10 が割り当てられる頂点と、victim13 が割り当てられる頂点と、victim14 が割り当てられる頂点は完全グラフを形成する。

10

20

30

40

50

【0118】

ブルートフォース攻撃分析部102のクリーク探索部1024は、ペア生成部1022で形成された通信装置(Victim)同士のペアを表現するグラフから、クリークを構成する頂点を見付ける。ブルートフォース攻撃分析部102のクリーク探索部1024は、最大クリークを構成する頂点を見付けても良い。

【0119】

図18Bは、図17に示されているブルートフォース攻撃分析部102のクリーク探索部1024の出力の例を示す図である。

【0120】

ペア生成部1022の結果を用いると、上の例では、victim1、2、10、13、14に対応する頂点を含むグラフ中で、クリークを構成する頂点は、victim1とvictim2に対応する頂点の一つのクリークを構成する。また、victim10とvictim13とvictim14に対応する頂点の一つのクリークを構成する。最大クリークを構成する頂点を見付ける場合は、victim10とvictim13とvictim14に対応する頂点から構成されるクリークが、最大クリークである。

10

【0121】

そしてクリーク探索部1024は、クリークを構成する頂点に対応する通信装置群を、相関が高い被攻撃先通信装置(Victim)の候補とする。

【0122】

ブルートフォース攻撃分析部102の出力部1026は、クリーク探索部1024で選ばれた相関が高い被攻撃先通信装置(Victim)の候補が受けたブルートフォース攻撃の攻撃元が同一かどうかを判定し、同一であれば相関が高い被攻撃先通信装置(Victim)群として認定する。相関が高い被攻撃先通信装置(Victim)群は、高相関通信装置群と呼ばれることもある。

20

【0123】

図18Cは、図17に示されているブルートフォース攻撃分析部102の出力部1026の出力の例を示す図である。

【0124】

victim1とvictim2で指定される通信装置を含む通信装置(Victim)群(victim1、victim2)と、victim10、victim13、victim14で指定される通信装置を含む通信装置(Victim)群(victim10、victim13、victim14)が、相関が高い被攻撃先通信装置(Victim)群として出力される。

30

【0125】

別の方法として、ブルートフォース攻撃分析部102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、相関係数 R を、

【数3】

$$R = \frac{\sum_{i=1}^n (x_i - x_{av})(t_i - t_{av})}{\sqrt{\sum_{i=1}^n (x_i - x_{av})^2} \sqrt{\sum_{i=1}^n (t_i - t_{av})^2}}$$

40

と定義し、相関係数 R が所定の閾値以上となるような通信装置 v_i の組み合わせを探しても良い。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。

【0126】

図17のブルートフォース攻撃分析部102のペア生成部1022とクリーク探索部1024は、図5の相関係数計算部1002と抽出部1004に対応する。

50

【0127】

図17のブルートフォース攻撃分析部102の出力部1026は、図5の出力部1006に対応する。

【0128】

上記のような構成を採用することによって、ログ分析装置100は、複数の攻撃先に対して断続的に攻撃元を変えて攻撃をするブルートフォース攻撃を受ける通信装置を特定し、その攻撃に対する対策を取るために、短い期間のセキュリティ装置のログの分析によって、このような攻撃を受ける通信装置を特定することができる。

【0129】

図19は実施形態のログ分析装置100の構成の例を示す図である。ログ分析装置100と侵入検知システム110が一体となって構成される場合には、両者を含む装置の構成の例でもある。

10

【0130】

このコンピュータ200は、Central Processing Unit (CPU) 202、Read Only Memory (ROM) 204、及びRandom Access Memory (RAM) 206を備えている。コンピュータ500は、さらに、ハードディスク装置208、入力装置210、表示装置212、インターフェース装置214、及び記録媒体駆動装置216を備えている。なお、これらの構成要素はバスライン220を介して接続されており、CPU 202の管理の下で各種のデータを相互に授受することができる。

20

【0131】

Central Processing Unit (CPU) 202は、このコンピュータ200全体の動作を制御する演算処理装置であり、コンピュータ200の制御処理部として機能する。

【0132】

Read Only Memory (ROM) 204は、所定の基本制御プログラムが予め記録されている読み出し専用半導体メモリである。CPU 202は、この基本制御プログラムをコンピュータ100の起動時に読み出して実行することにより、このコンピュータ200の各構成要素の動作制御が可能になる。

【0133】

Random Access Memory (RAM) 206は、CPU 202が各種の制御プログラムを実行する際に、必要に応じて作業用記憶領域として使用する、随時書き込み読み出し可能な半導体メモリである。

30

【0134】

ハードディスク装置208は、CPU 202によって実行される各種の制御プログラムや各種のデータを記憶しておく記憶装置である。MPU 502は、ハードディスク装置208に記憶されている所定の制御プログラムを読み出して実行することにより、後述する各種の制御処理を行えるようになる。

【0135】

入力装置210は、例えばマウス装置やキーボード装置であり、情報処理装置のユーザにより操作されると、その操作内容に対応付けられている各種情報の入力を取得し、取得した入力情報をCPU 202に送付する。

40

【0136】

表示装置212は例えば液晶ディスプレイであり、CPU 202から送付される表示データに応じて各種のテキストや画像を表示する。

【0137】

インターフェース装置214は、このコンピュータ200に接続される各種機器との間の各種情報の授受の管理を行う。

【0138】

記録媒体駆動装置216は、可搬型記録媒体218に記録されている各種の制御プログ

50

ラムやデータの読み出しを行う装置である。CPU 202は、可搬型記録媒体 218に記録されている所定の制御プログラムを、記録媒体駆動装置 216を介して読み出して実行することによって、後述する各種の制御処理を行うようにすることもできる。なお、可搬型記録媒体 218としては、例えばUSB (Universal Serial Bus)規格のコネクタが備えられているフラッシュメモリ、CD-ROM (Compact Disc Read Only Memory)、DVD-ROM (Digital Versatile Disc Read Only Memory)などがある。

【0139】

このようなコンピュータ 200を用いてログ分析装置またはログ分析装置を含む侵入検知システムを構成するには、例えば、上述の各処理部における処理をCPU 202に行わせるための制御プログラムを作成する。作成された制御プログラムはハードディスク装置 208若しくは可搬型記録媒体 218に予め格納しておく。そして、CPU 202に所定の指示を与えてこの制御プログラムを読み出させて実行させる。こうすることで、ログ分析装置またはログ分析装置を含む侵入検知システムが備えている機能がCPU 202により提供される。

【0140】

<ログ分析処理>

図20は、ログ分析処理の流れを示す図である。

【0141】

また、ログ分析装置が図19に示されているような汎用コンピュータ 200である場合には、下記の説明は、そのような処理を行う制御プログラムを定義する。すなわち、以下では、下記に説明する処理を汎用コンピュータに行わせる制御プログラムの説明でもある。

【0142】

処理が開始されるとS100で、ログ分析装置100のブルートフォース攻撃分析部102(ペア生成部1022)は、ログ分析装置100のIDSログデータベース(DB)114に格納されるデータを取得する。

【0143】

次にS102でログ分析装置100のブルートフォース攻撃分析部102(ペア生成部1022)は、S100で取得したデータに基づいて、攻撃元(Hacker)、被攻撃先(Victim)、検知時刻、ログイン試行回数(攻撃回数)、被攻撃先のポート(Port)に関する回数データ列を作成する。

【0144】

次にS104でログ分析装置100のブルートフォース攻撃分析部102(クリーク探索部1024)は、S102で形成された通信装置(Victim)同士のペアを表現するグラフから、頂点間の相関係数を計算する。

【0145】

次のS106でブルートフォース攻撃分析部102(出力部1026)は、S104で計算された相関係数を用いて、クリークが構成されるかどうかを判定し、相関が高い通信装置(Victim)群が存在するかどうかを判定する。クリークが構成されるかどうかを判定する際、頂点間の相関係数が分析設定DB104に格納されている相関係数の閾値より大きいかどうかに基づいて判定しても良い。この判定の結果が“Yes”、すなわち、相関が高い通信装置(Victim)群が存在する場合には、処理はS108に進む。また、判定の結果が“No”、すなわち、相関が高い通信装置(Victim)群が存在しない場合には、処理は終了する。

【0146】

S108でブルートフォース攻撃分析部102(出力部1026)は、S106で選ばれた相関が高い被攻撃先通信装置(Victim)の候補が受けたブルートフォース攻撃の攻撃元が同一かどうかを判定する。この判定の結果が“Yes”、すなわち、相関が高い被攻撃先通信装置(Victim)の候補が受けたブルートフォース攻撃の攻撃元が同

10

20

30

40

50

一である場合には、処理はS 1 1 0に進む。また、判定の結果が“ N o ”、すなわち、相関が高い被攻撃先通信装置（ V i c t i m ）の候補が受けたブルートフォース攻撃の攻撃元が同一ではない場合には、処理は終了する。

【 0 1 4 7 】

S 1 1 0でブルートフォース攻撃分析部 1 0 2（出力部 1 0 2 6）は、同一の攻撃元からのブルートフォース攻撃を受けた相関が高い被攻撃先通信装置（ V i c t i m ）の候補を、相関が高い被攻撃先通信装置（ V i c t i m ）として認定し、要対策通信装置リスト 1 5 0に登録する。要対策通信装置リスト 1 5 0に含まれる情報は、侵入検知システム（ I D S ） 1 1 0の要対策通信装置（ V i c t i m ） I P アドレスデータベース（ D B ） 1 1 8に格納される。相関が高い被攻撃先通信装置（ V i c t i m ）群は、高相関通信装置群と呼ばれることもある。

10

【 0 1 4 8 】

また、 S 1 1 0でインターフェース部 1 0 6は、相関が高い被攻撃先通信装置（ V i c t i m ）をディスプレイ等に表示しても良い。図 8 はそのような表示の例である。

【 0 1 4 9 】

また、 S 1 1 0でインターフェース部 1 0 6は、相関が高い被攻撃先通信装置（ V i c t i m ）に関する情報をログ分析装置 1 0 0に送る。この相関が高い被攻撃先通信装置（ V i c t i m ）に関する情報は、図 5 に示されている要対策通信装置リスト 1 5 0に対応する。

20

【 0 1 5 0 】

上記のような処理によって、複数の攻撃先に対して断続的に攻撃元を変えて攻撃をするブルートフォース攻撃を受ける通信装置を特定し、その攻撃に対する対策を取るために、短い期間のセキュリティ装置のログの分析によって、このような攻撃を受ける通信装置を特定することができる。

【 0 1 5 1 】

以上の実施形態に関し、さらに以下の付記を開示する。

（付記 1）

攻撃元通信装置から攻撃を受ける複数の被攻撃先通信装置をネットワーク機器から収集したログに基いて分類するログ分析装置であって、

前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した検知時刻および前記検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する相関係数を前記ログに基いて計算する相関係数計算部と、

30

前記相関係数が所定の閾値以上であり、かつ、前記期間において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出する抽出部と、
を含むログ分析装置。

（付記 2）

前記攻撃は断続的に複数の期間にわたり行われ、前記検知時刻は複数であり、前記複数の期間の各々はそれぞれ異なる前記複数の検知時刻の一つを含み、

前記相関係数計算部は、前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した前記複数の検知時刻および前記複数の期間の各々における前記攻撃の回数に関する相関係数を前記ログに基いて計算し、

40

前記抽出部は、前記相関係数が所定の閾値以上であり、かつ、前記期間の各々において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出する、付記 1 に記載のログ分析装置。

（付記 3）

前記抽出部は、前記複数の被攻撃先通信装置が受けた前記攻撃の前記検知時刻および前記検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する情報に対応した頂点と、前記所定の閾値以上の相関係数を有する前記複数の被攻撃先通信装置のうちの 2 つに対応する頂点間に付与した辺を含むグラフから、クリークを抽出することによって

50

前記高相関通信装置群を抽出する、付記 1 または 2 に記載のログ分析装置。

(付記 4)

前記攻撃はブルートフォース攻撃であり、前記攻撃はログイン試行である付記 1 乃至 3 のいずれか 1 項に記載のログ分析装置。

(付記 5)

攻撃元通信装置から攻撃を受ける複数の被攻撃先通信装置をネットワーク機器から収集したログに基いて分類するログ分析方法であって、

前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した検知時刻および前記検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する相関係数を前記ログに基いて計算することと、

前記相関係数が所定の閾値以上であり、かつ、前記期間において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出することと、

を含むログ分析方法。

(付記 6)

前記攻撃は断続的に複数の期間にわたり行われ、前記検知時刻は複数であり、前記複数の期間の各々はそれぞれ異なる前記複数の検知時刻の一つを含み、

前記相関係数を計算することは、前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した前記複数の検知時刻および前記複数の期間の各々における前記攻撃の回数に関する相関係数を前記ログに基いて計算し、

前記高相関通信装置群を抽出することは、前記相関係数が所定の閾値以上であり、かつ、前記期間の各々において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出する、付記 5 に記載のログ分析方法。

(付記 7)

前記高相関通信装置群を抽出することは、前記複数の被攻撃先通信装置が受けた前記攻撃の前記検知時刻および前記検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する情報に対応した頂点と、前記所定の閾値以上の相関係数を有する前記複数の被攻撃先通信装置のうち 2 つに対応する頂点間に付与した辺を含むグラフから、クリークを抽出することによって前記高相関通信装置群を抽出する、付記 5 または 6 に記載のログ分析方法。

(付記 8)

前記攻撃はブルートフォース攻撃であり、前記攻撃はログイン試行である付記 5 乃至 7 のいずれか 1 項に記載のログ分析方法。

(付記 9)

コンピュータに、攻撃元通信装置から攻撃を受ける複数の被攻撃先通信装置をネットワーク機器から収集したログに基いて分類させるプログラムであって、

前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した検知時刻および前記検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する相関係数を前記ログに基いて計算し、

前記相関係数が所定の閾値以上であり、かつ、前記期間において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出する処理を前記コンピュータに実行させるプログラム。

(付記 10)

前記攻撃は断続的に複数の期間にわたり行われ、前記検知時刻は複数であり、前記複数の期間の各々はそれぞれ異なる前記複数の検知時刻の一つを含み、

前記相関係数を計算することは、前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した前記複数の検知時刻および前記複数の期間の各々における前記攻撃の回数に関する相関係数を前記ログに基いて計算し、

前記高相関通信装置群を抽出することは、前記相関係数が所定の閾値以上であり、かつ、前記期間の各々において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置

10

20

30

40

50

の組み合わせを高相関通信装置群として抽出させる、付記 9 に記載のプログラム。

(付記 1 1)

前記高相関通信装置群を抽出することは、前記複数の被攻撃先通信装置が受けた前記攻撃の前記検知時刻および前記検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する情報に対応した頂点と、前記所定の閾値以上の相関係数を有する前記複数の被攻撃先通信装置のうち 2 つに対応する頂点間に付与した辺を含むグラフから、クリークを抽出することによって前記高相関通信装置群を抽出させる、付記 9 または 1 0 に記載のプログラム。

(付記 1 2)

前記攻撃はブルートフォース攻撃であり、前記攻撃はログイン試行である付記 9 乃至 1 1 のいずれか 1 項に記載のプログラム。

10

【符号の説明】

【 0 1 5 2 】

1 0 システム

1 0 0 ログ分析装置

1 0 2 ブルートフォース攻撃分析部

1 0 4 分析設定データベース (D B)

1 0 6 インターフェース部

1 0 0 2 相関係数計算部

1 0 0 4 抽出部 (通信装置 (V i c t i m) 群選択部)

20

1 0 0 6 出力部

1 1 0 侵入検知システム (I D S)

1 1 2 攻撃探知部

1 1 4 I D S ログデータベース (D B)

1 1 6 攻撃対策部

1 1 8 要対策通信装置 I P アドレスデータベース (D B)

1 2 0 ネットワーク

1 3 0 通信装置群

1 4 0 I D S ログ

1 5 0 要対策通信装置リスト

30

【 図 6 】

ログ分析装置の出力の例を示す図

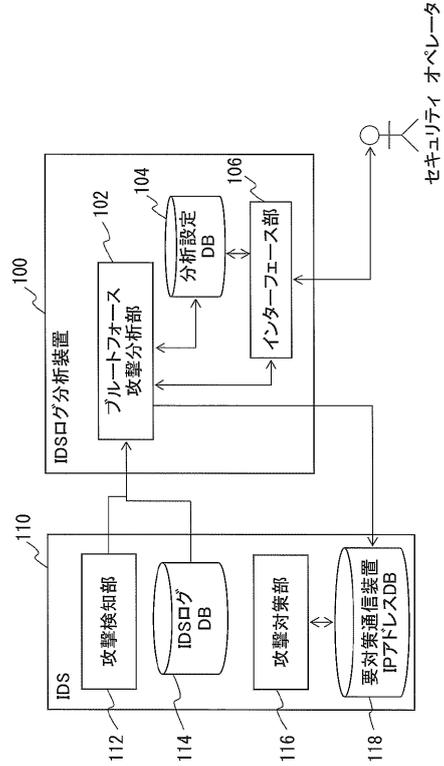
Hacker	time	v1	v2	v3	v4	v5	v6	v7	v8	v9	v10
h1	11/1 0:01										
..
h2	11/1 4:00	12	12	12	12	12	0	0	0	0	0
h2	11/1 4:01	10	9	9	9	9	0	0	0	0	0
h2	11/1 4:02	3	4	4	4	4	0	0	0	0	0
h3	11/1 4:03	0	0	0	0	0	100	0	0	0	0
..
h4	11/1 11:59										

今後攻撃を受ける可能性
がある通信装置 (Victim) 群

相関が高いデータ列

【 図 7 】

侵入検知システムとログ分析装置の
機能ブロック図の例を示す図



【 図 8 】

ログ分析装置のインターフェース部の
出力画面の例を示す図

＜分析設定＞

*相関係数の閾値
*分析の間隔

0.8
0.5日

＜対策Victim IP一覧＞

IPアドレス	追加日
*55.66.77.88	2012/4/1 12:00
*55.66.77.89	2012/4/2 0:00
*55.66.77.90	2012/4/2 0:00
*66.45.84.35	2012/5/30 0:00
*66.55.34.85	2012/5/30 0:00
..	..

【 図 9 】

侵入検知システムのIDSログデータベースに
格納されるデータの例を示す図

IDSログDB

Hacker	Victim	検知時刻	攻撃回	Port
11.22.33.4	55.66.77.8	2013/4/1	30	22
11.22.33.4	55.66.77.8	2013/4/2	100	338
..

【 図 10 】

ログ分析装置の分析設定データベースに
格納されるデータの例を示す図

分析設定DB

項目	設定値
相関係数の閾	0.8
分析の間隔	0.5day

【 図 1 1 】

侵入検知システムの要対策通信装置
IPアドレスデータベースに格納されるデータの
例を示す図

要対策通信装置IPアドレスDB

IPアドレス	ポート	追加日
55.66.77.8	22	2012/4/1
55.66.77.8	22	2012/4/2 0:00
:	:	:

【 図 1 2 】

ログ分析装置が侵入検知システムの
IDSログデータベースから受け取るログデータの例を示す図

Hacker	被攻撃先通信装置 (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 1 3 】

ブルートフォース攻撃分析部で作成されるポート番号ごとの
攻撃元(Hacker)、攻撃回数、検知時刻(time)、
被攻撃先(被攻撃先通信装置(Victm))についての
データの示す回数データ列の例を示す図

Port = 22		被攻撃先通信装置 (Victim)					
Hacker	time	11.22.33.44	2.22.33.44	3.22.33.44	4.22.33.44	5.22.33.44	
55.66.77.88	2013/11/1 0:00	30	0	0	0	0	
11.22.33.44	2013/11/1 4:00	12	12	12	12	12	
11.22.33.44	2013/11/1 4:01	10	9	9	9	9	
11.22.33.44	2013/11/1 4:02	3	4	4	4	4	
5.5.6.6	2013/11/1 4:03	0	0	0	0	0	
4.3.2.1	2013/11/1 11:59						

【 図 1 4 】

ブルートフォース攻撃分析部で関連の
高い通信装置を抽出する様子の例を示す図

Port = 22		被攻撃先通信装置 (Victim)					
Hacker	time	11.22.33.44	2.22.33.44	3.22.33.44	4.22.33.44	5.22.33.44	
55.66.77.88	2013/11/1 0:00	30	0	0	0	0	
11.22.33.44	2013/11/1 4:00	12	12	12	12	12	
11.22.33.44	2013/11/1 4:01	10	9	9	9	9	
11.22.33.44	2013/11/1 4:02	3	4	4	4	4	
5.5.6.6	2013/11/1 4:03	0	0	0	0	0	
4.3.2.1	2013/11/1 11:59						

相関が高い被攻撃先通信装置 (Victim) の候補

【 図 1 5 】

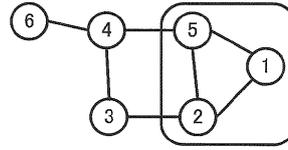
ブルートフォース攻撃分析部で関連の
高い通信装置を抽出する様子の例を示す図

Port = 22		被攻撃先通信装置 (Victim)									
Hacker	time	11.22.33.4	2.22.33.4	3.22.33.4	4.22.33.4	5.22.33.4	6.22.33.4	7.22.33.4	8.22.33.4	9.22.33.4	10.22.33.4
55.66.77.8	2013/11/1 0:00:30	0	0	0	0	0	0	0	0	0	0
11.22.33.4	2013/11/1 4:00:12	12	12	12	12	12	12	12	12	12	12
11.22.33.4	2013/11/1 4:01:10	9	9	9	9	9	9	9	9	9	9
11.22.33.4	2013/11/1 4:02:13	4	4	4	4	4	4	4	4	4	4
5.5.6.6	2013/11/1 4:03:0	0	0	0	0	0	0	0	0	0	0
4.3.2.1	2013/11/1										

11.22.33.44から同じ回数・同じ時刻で攻撃を受けていた
相関が高い被攻撃先通信装置 (Victim)

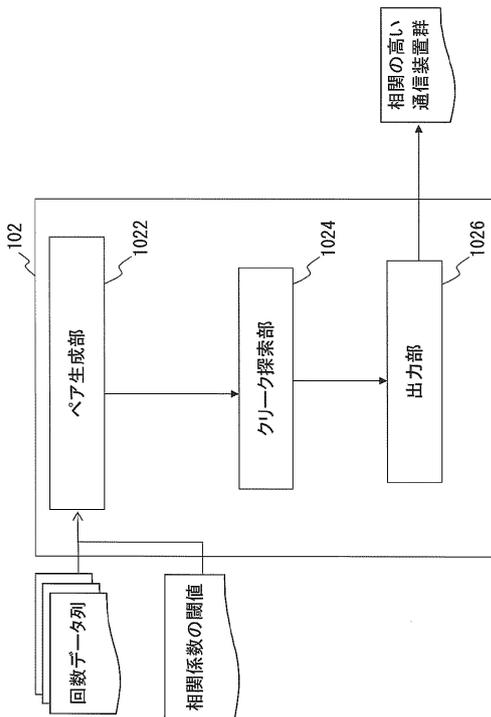
【 図 1 6 】

最大クリーク法の概略を説明するための図



【 図 1 7 】

最大クリーク法を用いるブルートフォース攻撃分析部の
機能ブロック図の例を示す図



【 図 1 8 A 】

図17に示されているブルートフォース攻撃分析部の
ペア生成部の出力の例を示す図

Victimのペア (victim1,victim2) (victim10,victim13) (victim10,victim14) (victim13,victim14)

【 図 1 8 B 】

図17に示されているブルートフォース攻撃分析部の
クリーク探索部の出力の例を示す図

クリークの頂点 (victim1,victim2) (victim10,victim13,victim14)
--

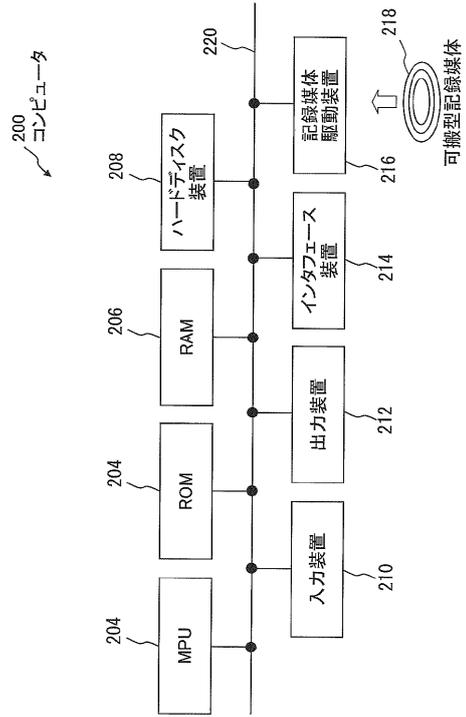
【 図 1 8 C 】

図17に示されているブルートフォース攻撃分析部の出力部の出力の例を示す図

	相関が高い被攻撃先通信装置 (Victim) 群 (victim1,victim2) (victim10, victim13,victim14)
--	--

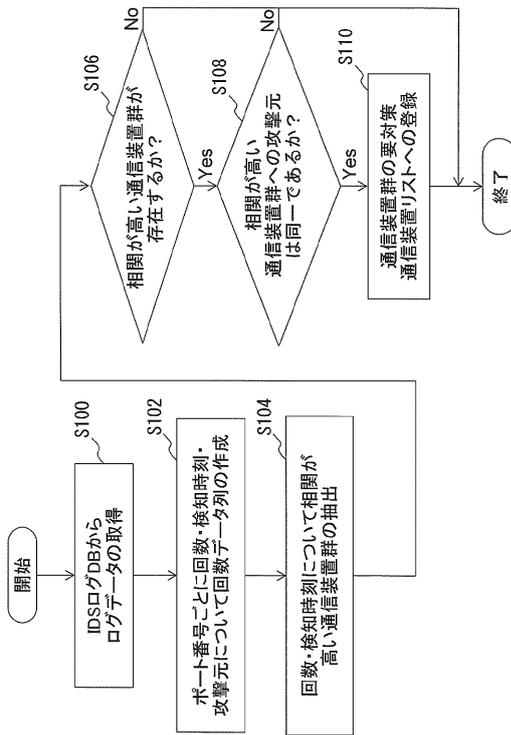
【 図 1 9 】

コンピュータの構成の例を示す図



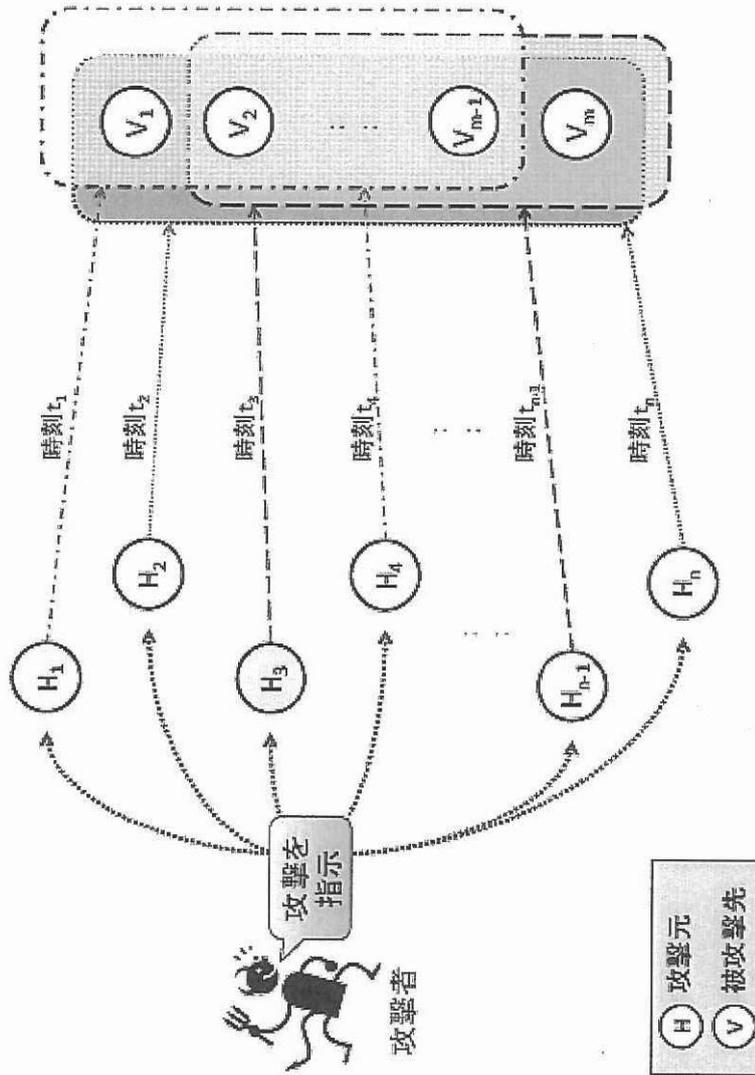
【 図 2 0 】

ログ分析処理の流れを示す図



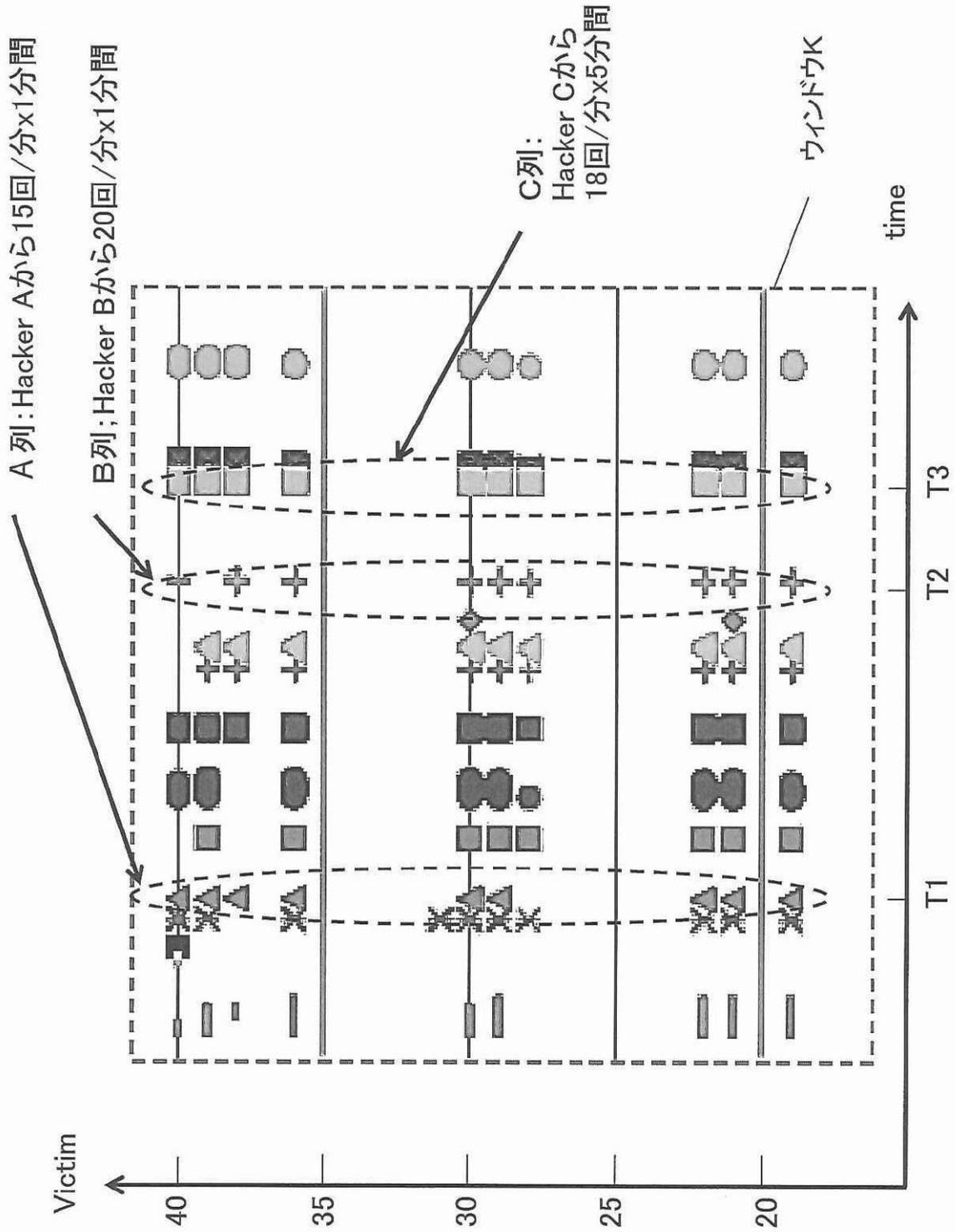
【 図 1 】

ブルートフォース攻撃の例の概略を説明する図



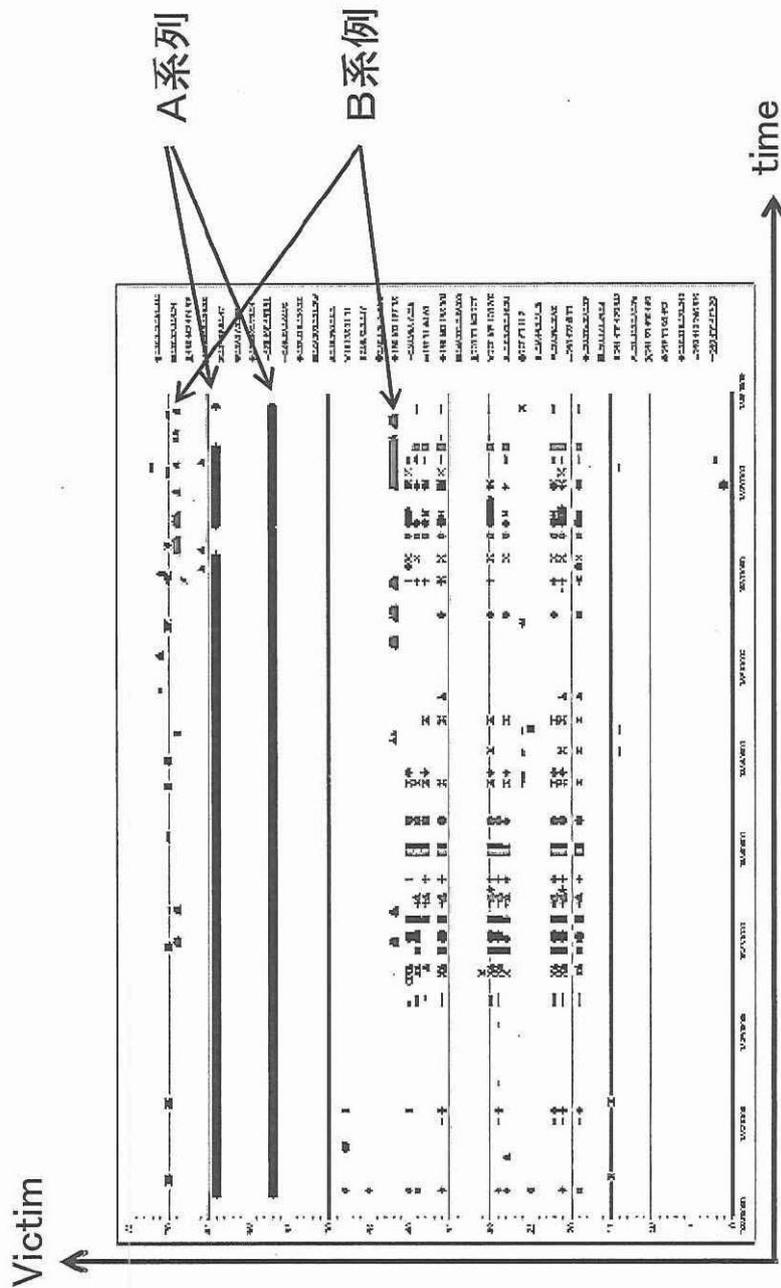
【 図 3 】

図2に示されているログの一部を拡大した図



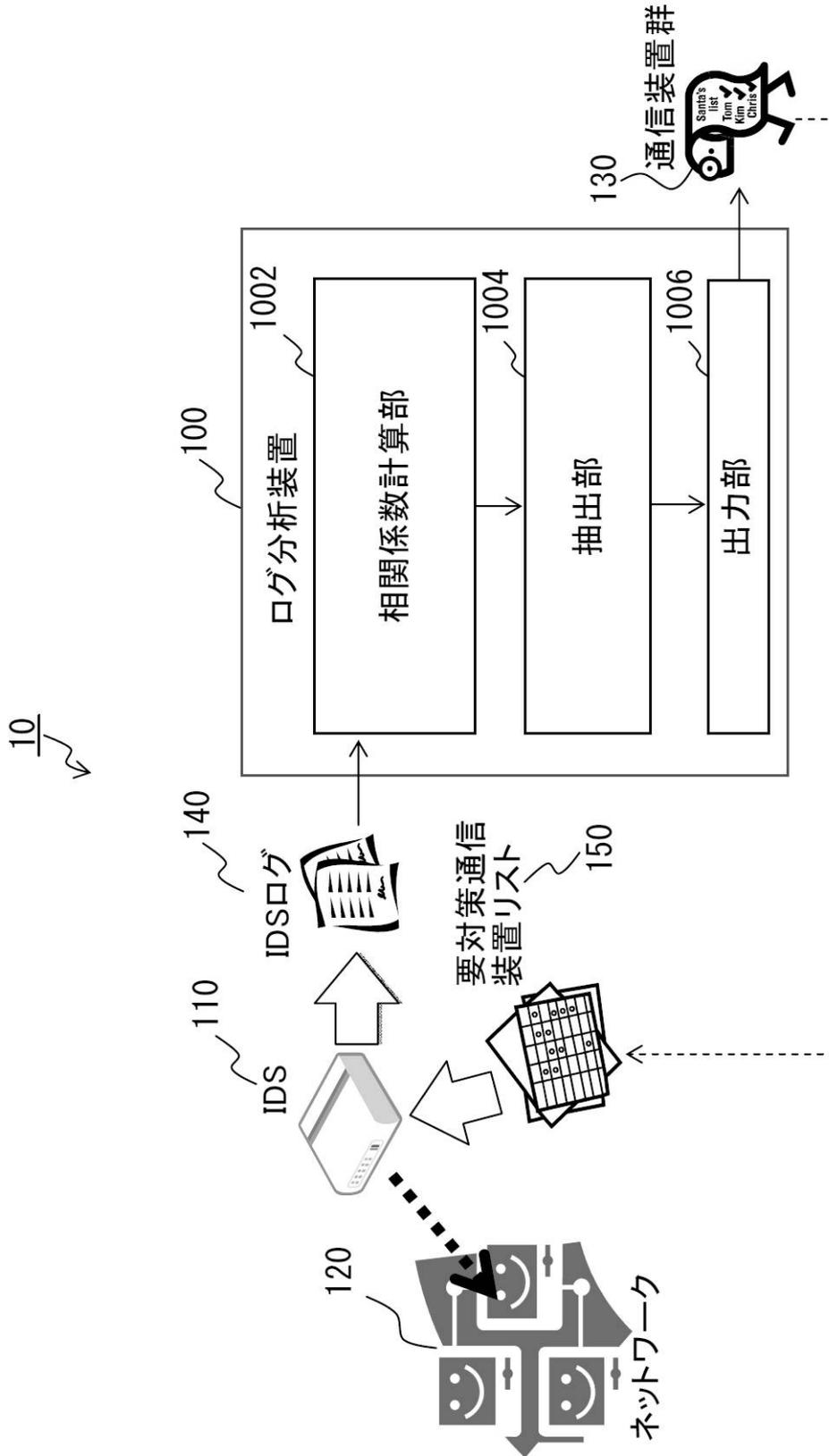
【 図 4 】

ブルートフォース攻撃の別の例を受けた通信装置のログの例を示す図



【図5】

ログ分析装置を含むシステムの概略を説明する図



【 手続補正書 】

【 提出日 】平成26年9月5日(2014.9.5)

【 手続補正 1 】

【補正対象書類名】特許請求の範囲

【補正対象項目名】全文

【補正方法】変更

【補正の内容】

【特許請求の範囲】

【請求項 1】

攻撃元通信装置から攻撃を受ける複数の被攻撃先通信装置をネットワーク機器から収集したログに基いて分類するログ分析装置であって、

前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した検知時刻および検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する相関係数を前記ログに基いて計算する相関係数計算部と、

前記相関係数が所定の閾値以上であり、かつ、前記期間において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出する抽出部と、

を含むログ分析装置。

【請求項 2】

前記攻撃は断続的に複数の期間にわたり行われ、前記検知時刻は複数であり、前記複数の期間の各々はそれぞれ異なる前記複数の検知時刻の一つを含み、

前記相関係数計算部は、前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した前記複数の検知時刻および前記複数の期間の各々における前記攻撃の回数に関する相関係数を前記ログに基いて計算し、

前記抽出部は、前記相関係数が所定の閾値以上であり、かつ、前記期間の各々において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出する、請求項 1 に記載のログ分析装置。

【請求項 3】

前記抽出部は、前記複数の被攻撃先通信装置が受けた前記攻撃の前記検知時刻および前記検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する情報に対応した頂点と、前記所定の閾値以上の相関係数を有する前記複数の被攻撃先通信装置のうちの 2 つに対応する頂点間に付与した辺を含むグラフから、クリークを抽出することによって前記高相関通信装置群を抽出する、請求項 1 または 2 に記載のログ分析装置。

【請求項 4】

前記攻撃はブルートフォース攻撃であり、前記攻撃はログイン試行である請求項 1 乃至 3 のいずれか 1 項に記載のログ分析装置。

【請求項 5】

攻撃元通信装置から攻撃を受ける複数の被攻撃先通信装置をネットワーク機器から収集したログに基いて分類するログ分析方法であって、

前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した検知時刻および検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する相関係数を前記ログに基いて計算することと、

前記相関係数が所定の閾値以上であり、かつ、前記期間において前記攻撃元通信装置が同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出することと、

を含むログ分析方法。

【請求項 6】

コンピュータに、攻撃元通信装置から攻撃を受ける複数の被攻撃先通信装置をネットワーク機器から収集したログに基いて分類させるプログラムであって、

前記複数の被攻撃先通信装置の組み合わせに対して、前記攻撃を前記ネットワーク機器が検知した検知時刻および検知時間を含む前記攻撃が行われた期間における前記攻撃の回数に関する相関係数を前記ログに基いて計算し、

前記相関係数が所定の閾値以上であり、かつ、前記期間において前記攻撃元通信装置が

同一である前記複数の被攻撃先通信装置の組み合わせを高相関通信装置群として抽出、する処理を前記コンピュータに実行させるプログラム。

【手続補正2】

【補正対象書類名】明細書

【補正対象項目名】0008

【補正方法】変更

【補正の内容】

【0008】

さらに別のログ分析装置では、まず、ログ中から分析に用いるパラメータを抽出し、そのパラメータに属するイベントの数に基づいてネットワークの異常度に関する異常値を算出する。次に、その異常値に関する所定の条件が満たされた場合に所定の事象が発生する条件付確率を算出することで未来のイベント数の推移を客観的に予測する、たとえば、所定の事象が発生する条件付確率を算出する。パラメータとしては、侵入検知システム、ルータ、ファイアウォールなどのネットワーク機器から出力されるログに記録されている、Attack Signature、Source/Destination PortおよびSource/Destination IDなどが挙げられる。異常値としては、比率分析における比率や、確率分析における上側稀率、下側稀率が挙げられる。

【手続補正3】

【補正対象書類名】明細書

【補正対象項目名】0039

【補正方法】変更

【補正の内容】

【0039】

図5は、グループ化装置を含むシステムの概略を説明する図である。

システム10は、侵入検知システム(IDS)110と、侵入検知システム(IDS)110から提供されるIDSログを分析し、攻撃を受ける通信装置をグループ化し、攻撃先群(Victim群)として特定するログ分析装置100を含んでいる。ログ分析装置100は、グループ化装置と呼ばれることもある。

【手続補正4】

【補正対象書類名】明細書

【補正対象項目名】0068

【補正方法】変更

【補正の内容】

【0068】

ログ分析装置100は、侵入検知システム(IDS)110のIDSログデータベース(DB)114に格納されるデータに基づいて、ブルートフォース攻撃の攻撃先と考えられる通信装置のIPアドレスを要対策通信装置(Victim)IPアドレスとして特定する。具体的には、ログ分析装置100は、IDSログデータベース(DB)114に格納されるデータに基づいて、攻撃元(Hacker)、攻撃回数、検知時刻の3つについて、複数の被攻撃先(Victim)の相関係数を計算する。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ても良い。そして、相関係数の高い通信装置(Victim)を抽出し、通信装置群(Victim群)として特定する。これらの通信装置群を被攻撃先群と呼ぶこともある。

【手続補正5】

【補正対象書類名】明細書

【補正対象項目名】0069

【補正方法】変更

【補正の内容】

【0069】

図8は、ログ分析装置の出力画面の例を示す図である。

図 8 に示されているように、ブルートフォース攻撃の攻撃先の候補である IP アドレスが、その IP アドレスが攻撃先と認定された日時（追加日）と共に表示される。

【手続補正 6】

【補正対象書類名】明細書

【補正対象項目名】0070

【補正方法】変更

【補正の内容】

【0070】

図 8 の例では、IP アドレス「55.66.77.88」は「2013年4月1日12時0分」に攻撃先の候補と認定されたことが表示される。

【手続補正 7】

【補正対象書類名】明細書

【補正対象項目名】0072

【補正方法】変更

【補正の内容】

【0072】

侵入検知システム（IDS）110の要対策通信装置（Victim）IPアドレスデータベース（DB）118には、ログ分析装置100において特定された要対策通信装置（Victim）IPアドレスが、その IP アドレスが攻撃先の候補と認定された日時（追加日）と共に格納されている。

【手続補正 8】

【補正対象書類名】明細書

【補正対象項目名】0074

【補正方法】変更

【補正の内容】

【0074】

図 11 の例では要対策通信装置（Victim）IPアドレスデータベース（DB）118には、たとえば、IP アドレス「55.66.77.88」は「2013年4月1日12時0分」に攻撃先と認定されたことを示すデータが格納されている。

【手続補正 9】

【補正対象書類名】明細書

【補正対象項目名】0075

【補正方法】変更

【補正の内容】

【0075】

侵入検知システム（IDS）110の攻撃対策部116は、要対策通信装置（Victim）IPアドレスデータベース（DB）118に格納されているリストに含まれる攻撃元からの通信に対する対策を行う。たとえば攻撃対策部116は、要対策通信装置（Victim）へのログイン試行があたったときに、アラート（警報）を発しても良い。また、攻撃対策部116は、要対策通信装置（Victim）への通信を遮断しても良い。

【手続補正 10】

【補正対象書類名】明細書

【補正対象項目名】0077

【補正方法】変更

【補正の内容】

【0077】

ログ分析装置100のブルートフォース攻撃分析部102は、図5の相関係数計算部1002と抽出部1004の機能を合わせた機能を有している。すなわち、侵入検知システム（IDS）110のIDSログデータベース（DB）114に格納されるデータに基づいて、ブルートフォース攻撃の攻撃先と考えられる通信装置の IP アドレスを要対策通信

装置 (Victim) IPアドレスとして特定する。具体的には、ログ分析装置 100 は、IDSログデータベース (DB) 114 に格納されるデータに基づいて、攻撃元 (Hacker)、攻撃回数、検知時刻の3つについて、複数の被攻撃先 (Victim) の相関係数を計算する。攻撃回数、検知時刻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ても良い。そして、相関係数の高い通信装置 (Victim) を抽出し、被攻撃先群 (Victim群、通信装置群) として特定する。

【手続補正 11】

【補正対象書類名】明細書

【補正対象項目名】0078

【補正方法】変更

【補正の内容】

【0078】

ログ分析装置 100 の分析設定データベース (DB) 104 は、ブルートフォース攻撃分析部 102 で相関係数を計算し、相関係数の高い通信装置 (Victim) を抽出し、被攻撃先群 (Victim群) として特定する際のパラメータが格納されている。

【手続補正 12】

【補正対象書類名】明細書

【補正対象項目名】0134

【補正方法】変更

【補正の内容】

【0134】

ハードディスク装置 208 は、CPU 202 によって実行される各種の制御プログラムや各種のデータを記憶しておく記憶装置である。CPU 202 は、ハードディスク装置 208 に記憶されている所定の制御プログラムを読み出して実行することにより、後述する各種の制御処理を行えるようになる。

【手続補正 13】

【補正対象書類名】図面

【補正対象項目名】図 9

【補正方法】変更

【補正の内容】

【図 9】

侵入検知システムのIDSログデータベースに格納されるデータの例を示す図

IDSログDB

Hacker	Victim	検知時刻	攻撃回数	Port
11.22.33.4	55.66.77.8	2013/4/1	30	22
11.22.33.4	55.66.77.8	2013/4/2	100	338
:	:	:	:	:

【手続補正 14】

【補正対象書類名】図面

【補正対象項目名】図 10

【補正方法】変更

【補正の内容】

【図 1 0】

ログ分析装置の分析設定データベースに 格納されるデータの例を示す図

分析設定DB

項目	設定値
相関係数の閾値	0.8
分析の間隔	0.5day

【手続補正 1 5】

【補正対象書類名】図面

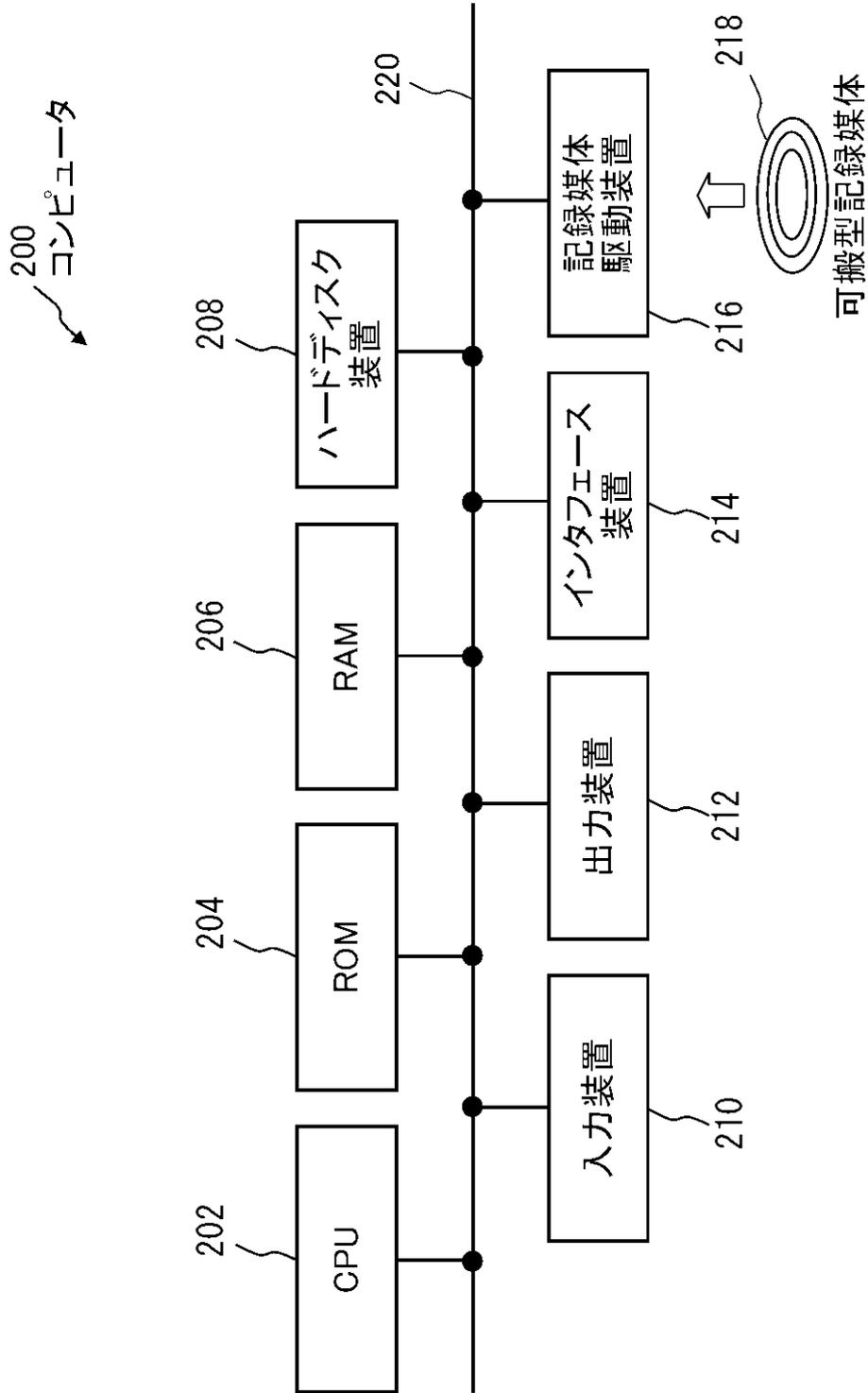
【補正対象項目名】図 1 9

【補正方法】変更

【補正の内容】

【図19】

コンピュータの構成の例を示す図



フロントページの続き

(72)発明者 武仲 正彦

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) 5K030 GA15 JA10 LE16 MA06 MB09 MC07