(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6201614号
(P6201614)
(45)発行日　平成29年9月27日(2017.9.27)　(24)登録日　平成29年9月8日(2017.9.8)

(51)Int.Cl.　F I
H04L 12/70 (2013.01)　H04L 12/70 100Z

請求項の数 6　(全 27 頁)

(21)出願番号　特願2013-214198(P2013-214198)
(22)出願日　平成25年10月11日(2013.10.11)
(65)公開番号　特開2015-76863(P2015-76863A)
(43)公開日　平成27年4月20日(2015.4.20)
審査請求日　平成28年6月6日(2016.6.6)

(73)特許権者　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　100074099
弁理士　大菅　義之
(74)代理人　100133570
弁理士　▲徳▼永　民雄
(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　藤嶌　由紀
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

最終頁に続く

(54)【発明の名称】ログ分析装置、方法およびプログラム

(57)【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を受けた期間と、前記期間内における前記攻撃を受けた回数との間の関係についての、前記複数の被攻撃先通信装置の間での相関の高さを示す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前記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、前記検知時刻および前記検知時間を含む前記攻撃を受けた期間内における前記攻撃を受けた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前記相関係数を有する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を受けた期間と、前記期間内における前記攻撃を受けた回数との間の関係についての、前記複数の被攻撃先通信装置の間での相関の高さを示す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を受けた期間と、前記期間内における前記攻撃を受けた回数との間の関係についての、前記複数の被攻撃先通信装置の間での相関の高さを示す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。
【発明の詳細な説明】
【技術分野】
【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。
【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。

【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。

【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）やファイアーウォール（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。

【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、ファイアー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。

【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
【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。

【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、攻撃を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を受けた期間と、当該期間内における攻撃を受けた回数との間の関係についての、複数の被攻撃先通信装置の間での相関の高さを示す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、当該期間において攻撃元通信装置が同一である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。

【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。

【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。

【図１１】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１２】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１３】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。

【図１４】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。

【図１５】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。

【図１６】最大クリーク法の概略を説明するための図である。

【図１７】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１８Ａ】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である。

【図１８Ｂ】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である。

【図１８Ｃ】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

す図である。
【図１９】コンピュータの構成の例を示す図である。
【図２０】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】
【００１６】
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。
【００１７】
＜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（ＩＤ）、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。
【００１８】
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。
【００１９】
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。
【００２０】
「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。
【００２１】
「Ｖｉｃｔｉｍ」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（ＩＤＳ）、侵入防止システム（ＩＰＳ）等がブルートフォース攻撃を検知した時刻である。
【００２２】
「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。
「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、ファイアー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。

【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。
【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。
【００３１】
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、グループ化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。

【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。

【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。

【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）h_2は１１月１日４時に、通信装置（Ｖｉｃｔｉｍ）v_1、v_2、v_3、v_4、v_5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）h_2は１１月１日４時１分に、通信装置（Ｖｉｃｔｉｍ）v_1、v_2、v_3、v_4、v_5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）h_2は１１月１日４時２分には、通信装置（Ｖｉｃｔｉｍ）v_1、v_2、v_3、v_4、v_5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）h_3は１１月１日４時３分に、通信装置（Ｖｉｃｔｉｍ）v_6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。

【００４９】

図６に示されている例では、攻撃元（Ｈａｃｋｅｒ）h_2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）v_1、v_2、v_3、v_4、v_5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）h_3から通信装置（Ｖｉｃｔｉｍ）v_6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。

【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。

【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。
【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。
【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、
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と組み合わされて、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。
【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。

【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。

【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。

【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。

【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。

【００７１】

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。

【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。

【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。

【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（Ｖｉ

ｃｔｉｍ）へのログイン試行があたっときに、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。

【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。

【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。

【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。

【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。

【００８４】

＜＜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。

【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。

【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）、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」、「２．２２．３３．４４」、「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グイン試行回数、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グ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～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_i、検知時刻をt_iとして、

【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として、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ＤＢ１０４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が辺で結ばれることによって表現される。

【０１１５】

図１８Ａ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１８Ａ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。

【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に対応する頂点が一つのクリークを構成する。また、ｖｉｃｔｉｍ１０とｖｉｃｔｉｍ１３とｖｉｃｔｉｍ１４に対応する頂点が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。

【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。

【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。

【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】

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

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。

【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。

【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、ＣＰＵ２０２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。

【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。ＣＰＵ２０２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、ＣＰＵ２０２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。
【０１３４】
ハードディスク装置２０８は、ＣＰＵ２０２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。ＣＰＵ２０２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ＣＰＵ２０２に送付する。
【０１３６】
表示装置２１２は例えば液晶ディスプレイであり、ＣＰＵ２０２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で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ラムやデータの読み出しを行う装置である。ＣＰＵ２０２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ＣＰＵ２０２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、ＣＰＵ２０２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ＣＰＵ２０２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一である場合には、処理はＳ１１０に進む。また、判定の結果が“Ｎｏ”、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一ではない場合には、処理は終了する。

【０１４７】

Ｓ１１０でブルートフォース攻撃分析部１０２（出力部１０２６）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（Ｖｉｃｔｉｍ）の候補を、相関が高い被攻撃先通信装置（Ｖｉｃｔｉｍ）として認定し、要対策通信装置リスト１５０に登録する。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。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。

【０１４８】

また、Ｓ１１０でインターフェース部１０６は、相関が高い被攻撃先通信装置（Ｖｉｃｔｉｍ）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。

【０１４９】

また、Ｓ１１０でインターフェース部１０６は、相関が高い被攻撃先通信装置（Ｖｉｃｔｉｍ）に関する情報をログ分析装置１００に送る。この相関が高い被攻撃先通信装置（Ｖｉｃｔｉｍ）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。

【０１５０】

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。

【０１５１】

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、

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、

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、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１１）

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させる、付記９または１０に記載のプログラム。

（付記１２）

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１１のいずれか１項に記載のプログラム。

【符号の説明】

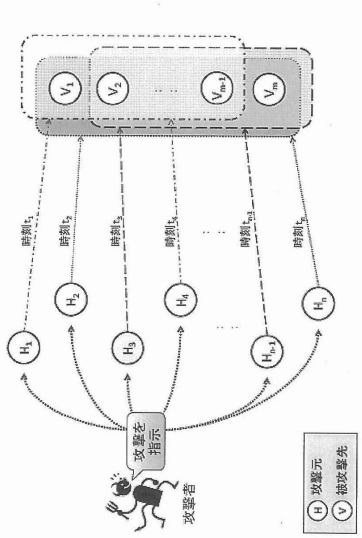
【０１５２】

１０　システム
１００　ログ分析装置
１０２　ブルートフォース攻撃分析部
１０４　分析設定データベース（ＤＢ）
１０６　インターフェース部
１００２　相関係数計算部
１００４　抽出部（通信装置（Ｖｉｃｔｉｍ）群選択部）

１００６　出力部
１１０　侵入検知システム（ＩＤＳ）
１１２　攻撃探知部
１１４　ＩＤＳログデータベース（ＤＢ）
１１６　攻撃対策部
１１８　要対策通信装置ＩＰアドレスデータベース（ＤＢ）
１２０　ネットワーク
１３０　通信装置群
１４０　ＩＤＳログ
１５０　要対策通信装置リスト

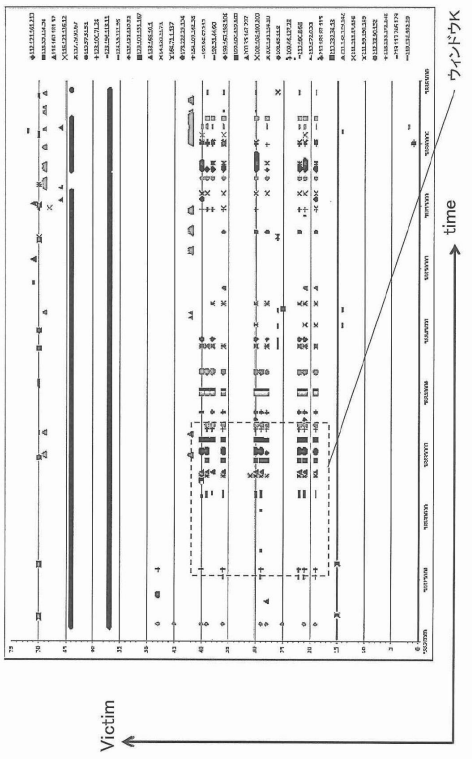
【図１】

ブルートフォース攻撃の例の概略を説明する図

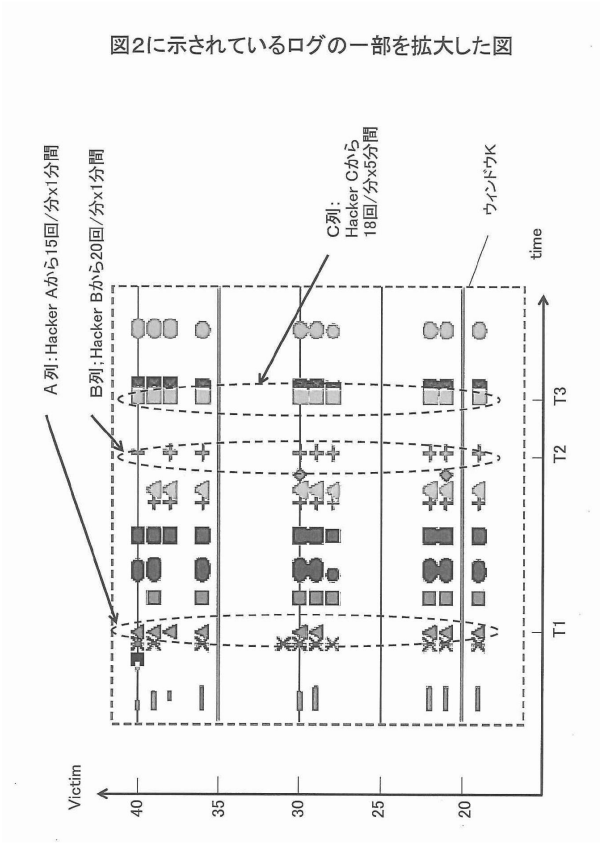


【図２】

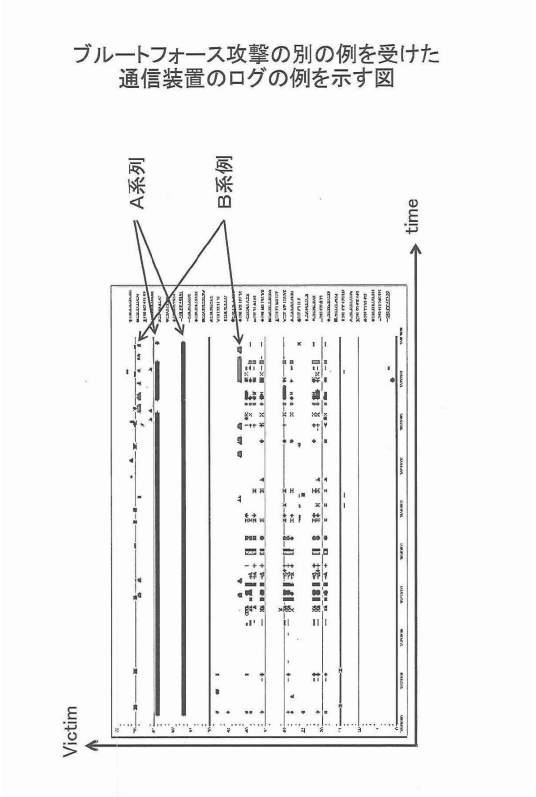
ブルートフォース攻撃の一例を
受けた通信装置のログの例を示す図



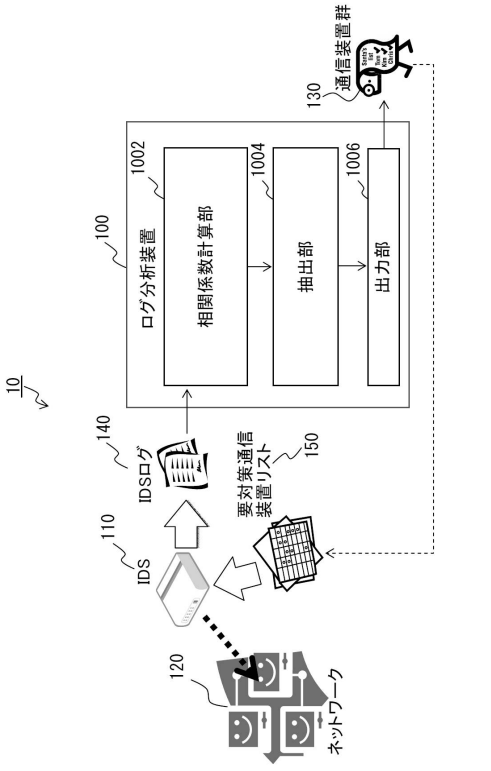
【図３】



【図４】



【図５】



【図６】

ログ分析装置の出力の例を示す図

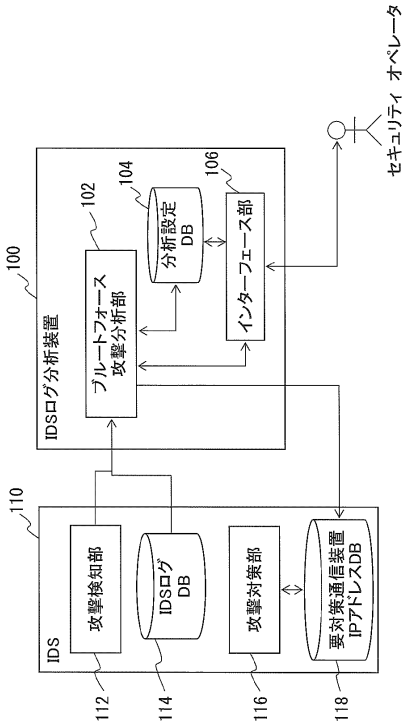
今後も攻撃を受ける可能性
がある通信装置(Victim)群

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										

相関が高いデータ列

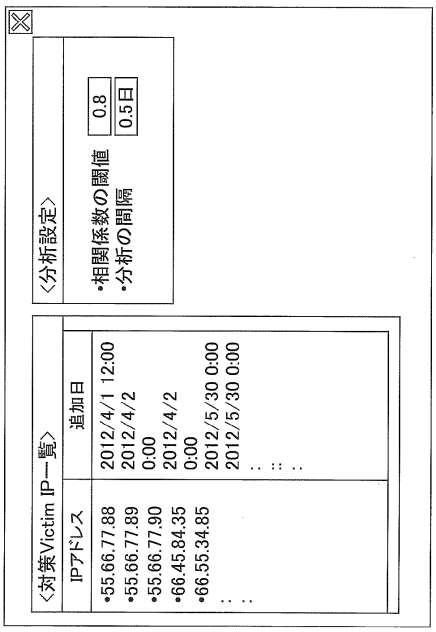
【図７】

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



【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
:	:	:	:	:

【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
相関係数の閾値	0.8
分析の間隔	0.5day

【図１１】

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１２】

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１３】

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１４】

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

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１５】

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

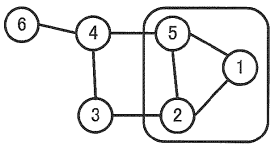
Port = 22	被攻撃先通信装置(Victim)				
Hacker	time	11.22.33.4	2.22.33.4	3.22.33.4	4.22.33.4	5.22.33.4
55.66.77.8	2013/11/1 0:00	30	0	0	0	0
:	:					
11.22.33.4	2013/11/1 4:00	12	12	12	0	0
11.22.33.4	2013/11/1 4:01	10	9	9	0	0
11.22.33.4	2013/11/1 4:02	3	4	4	0	0
5.5.6.6	2013/11/1 4:03	0	0	0	100	0
:	:					
4.3.2.1	2013/11/1					

相関が高い被攻撃先通信装置(Victim)

11.22.33.44から同じ回数・同じ時刻で攻撃を受けていた

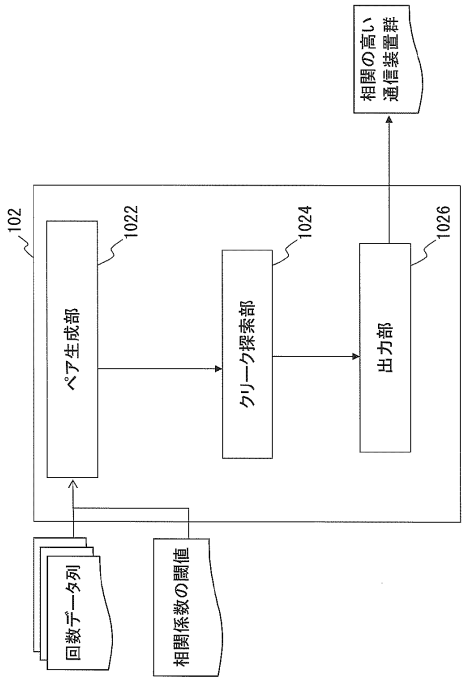
【図１６】

最大クリーク法の概略を説明するための図



【図１７】

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１８Ａ】

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１８Ｂ】

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)

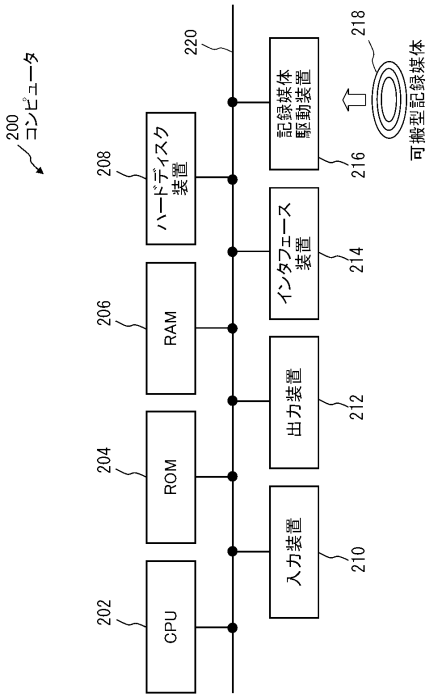
【図１８Ｃ】

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)

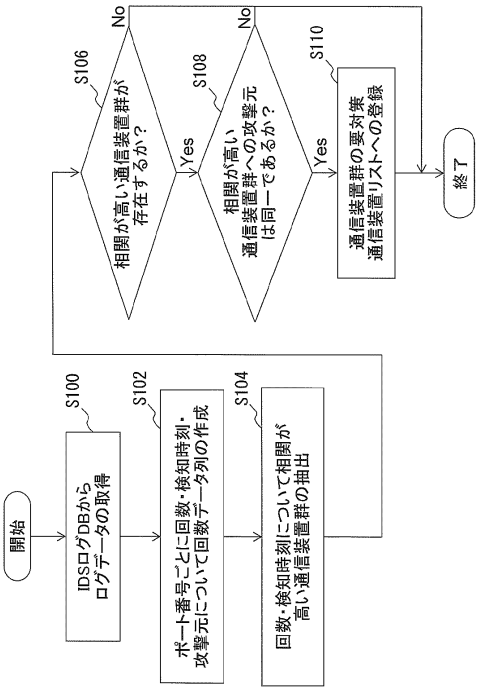
【図１９】

コンピュータの構成の例を示す図



【図２０】

ログ分析処理の流れを示す図



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

審査官　宮島　郁美

(56)参考文献　国際公開第２０１３／０１９１９８（WO，Ａ１）
米国特許出願公開第２０１１／０１８５４１９（ＵＳ，Ａ１）
特開２００５－０３８１１６（ＪＰ，Ａ）
国際公開第２００７／０５５２２２（WO，Ａ１）
特開２００６－３１９６３３（ＪＰ，Ａ）
国際公開第２０１３／０３６２６９（WO，Ａ１）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ１２／００－１２／２８，１２／４４－１２／９５５
Ｇ０６Ｆ１３／００