(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2007-165990
(P2007-165990A)
(43)公開日　平成19年6月28日(2007.6.28)

(51)Int.Cl.	F I	テーマコード（参考）
H04L 12/56 (2006.01)	H04L 12/56 400Z	5K030

審査請求 未請求　請求項の数 15　ＯＬ　（全 15 頁）

(21)出願番号　特願2005-356190 (P2005-356190)
(22)出願日　平成17年12月9日 (2005.12.9)

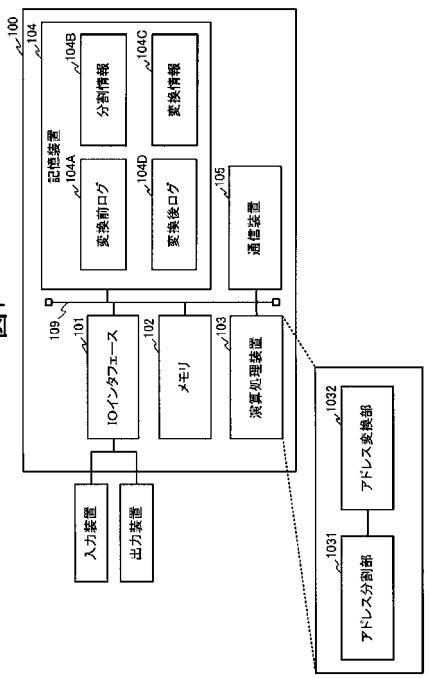
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000198
特許業務法人湘洋内外特許事務所
(72)発明者　大河内　一弥
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内
(72)発明者　森田　豊久
神奈川県川崎市麻生区王禅寺１０９９番地
株式会社日立製作所システム開発研究所内

最終頁に続く

(54)【発明の名称】ＩＰアドレス変換方法及び情報処理装置

(57)【要約】
【課題】アクセスログデータを第三者に提供する場合におけるセキュリティの向上を図る。
【解決手段】アドレス管理装置１００の記憶装置１０４には、変換対象アドレスのブロック内のデータが取り得る数値とその変換後の数値とを１対１に対応付けた変換情報１０４Ｃが格納されている。アドレス変換部１０３２は、変換対象ＩＰアドレス内に定めた各ブロック内のデータが示す数値に対応付けられた変換後数値を変換情報１０４Ｃから読み出す。そして、変換対象アドレス内の各ブロック内のデータを、当該読み出した変換後数値に基づき変換する。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
ＩＰアドレスを、当該ＩＰアドレスとは異なる値のアドレスに変換する情報処理装置であって、
予め定められたビット数のデータの変域内のデータが示す第１の数値に第２の数値を１対１に対応付ける変換情報が格納された記憶手段と、
前記ＩＰアドレスに定めた、前記ビット数のデータが示す数値のデータを含むブロックごとに、当該ブロック内のデータが示す数値に相当する前記第１の数値に対応付けられた前記第２の数値を前記変換情報から読み出し、当該ブロック内のデータを、当該読み出した第２の数値に基づき変換する演算処理手段と
を備えることを特徴とする情報処理装置。
【請求項２】
請求項１記載の情報処理装置であって、
前記演算処理手段は、アクセスログデータに含まれる、アクセス元マシンのＩＰアドレスを、前記変換対象のＩＰアドレスとして読み出し、前記アクセス元マシンのＩＰアドレスに代えて前記変換後のＩＰアドレスを含む前記アクセスログデータを出力する、
ことを特徴とする情報処理装置。
【請求項３】
請求項２記載の情報処理装置であって、
前記演算処理手段は、
前記アクセスログデータを収集するマシンのＩＰアドレスのネットワークアドレス部とホストアドレス部との境界に相当する位置を、前記ブロックの境界として設定する、
ことを特徴とする情報処理装置。
【請求項４】
請求項１、２及び３のうちのいずれか１項に記載の情報処理装置であって、
前記演算処理手段は、
前記各ブロック内のデータを、当該ブロックに関して読み出した前記第２の数値と予め定めた関係を有する、前記変域外の第３の数値のデータに変換する、
ことを特徴とする情報処理装置。
【請求項５】
請求項１、２、３及び４のうちのいずれか１項に記載の情報処理装置であって、
前記ブロックの境界位置の指定を受け付ける入力受付手段を備え、
前記演算処理手段は、前記指定された境界位置を境界として、前記ＩＰアドレスに前記ブロックを設定する、
ことを特徴とする情報処理装置。
【請求項６】
ＩＰアドレスの変換処理を情報処理装置に実行させるプログラムであって、
前記情報処理装置は、
予め定められたビット数のデータの変域内のデータが示す第１の数値に第２の数値を対応付ける変換情報が格納された記憶手段と、
演算処理手段と、
を備え、
当該プログラムは、
前記演算処理手段に、前記ＩＰアドレスに定めた、前記ビット数のデータが示す数値のデータを含むブロックごとに、当該ブロック内のデータが示す数値に相当する前記第１の数値に対応付けられた前記第２の数値を前記変換情報から読み出させる第１の処理と、
前記演算処理手段に、前記各ブロック内のデータを、当該ブロックについて読み出した第２の数値に基づき変換させる第２の処理と、
を含むことを特徴とするプログラム。
【請求項７】

請求項６記載のプログラムであって、
前記演算処理手段に、アクセスログデータに含まれる、アクセス元マシンのＩＰアドレスを、前記変換対象のＩＰアドレスとして読み出させる処理と、
前記演算処理手段に、前記アクセス元マシンのＩＰアドレスに代えて、前記第２の処理による変換後のＩＰアドレスを含む前記アクセスログデータを出力させる処理と、
を含むことを特徴とするプログラム。
【請求項８】
請求項７記載のプログラムであって、
前記第１の処理において、前記演算処理手段に、前記アクセスログデータを収集するマシンのＩＰアドレスのネットワークアドレス部とホストアドレス部との境界に相当する位置を、前記ブロックの境界として設定させる、
ことを特徴とするプログラム。
【請求項９】
請求項６、７及び８のうちのいずれか１項に記載のプログラムであって、
前記第２の処理において、前記演算処理手段に、前記各ブロック内のデータを、当該ブロックに関して読み出した前記第２の数値と予め定めた関係を有する、前記変域外の第３の数値のデータに変換させる、
ことを特徴とするプログラム。
【請求項１０】
請求項６、７、８及び９のうちのいずれか１項に記載のプログラムであって、
前記情報処理装置は入力受付手段を備え、
当該プログラムは、
前記ブロックの境界位置の指定を前記入力受付手段に受け付けさせる処理を含み、
前記第１の処理において、前記演算処理手段に、前記入力受付手段が指定を受け付けた境界位置に基づき、前記ＩＰアドレスに前記ブロックを設定させる、
ことを特徴とするプログラム。
【請求項１１】
ＩＰアドレスの変換処理を情報処理装置に実行させるＩＰアドレス変換方法であって、
前記情報処理装置は、
予め定められたビット数のデータの変域内のデータが示す第１の数値に第２の数値を対応付ける変換情報が格納された記憶手段と、
演算処理手段と、
を備え、
当該ＩＰアドレス変換方法は、
前記演算処理手段が、前記ＩＰアドレスに定めた、前記ビット数のデータが示す数値のデータを含むブロックごとに、当該ブロック内のデータが示す数値に相当する前記第１の数値に対応付けられた前記第２の数値を前記変換情報から読み出す第１の処理と、
前記演算処理手段が、前記各ブロック内のデータを、当該ブロックについて読み出した第２の数値に基づき変換する第２の処理と、
を含むことを特徴とするＩＰアドレス変換方法。
【請求項１２】
請求項１１記載のＩＰアドレス変換方法であって、
前記演算処理手段が、アクセスログデータに含まれる、アクセス元マシンのＩＰアドレスを、前記変換対象のＩＰアドレスとして読み出す処理と、
前記演算処理手段が、前記アクセス元マシンのＩＰアドレスに代えて、前記第２の処理による変換後のＩＰアドレスを含む前記アクセスログデータを出力する処理と、
を含むことを特徴とするＩＰアドレス変換方法。
【請求項１３】
請求項１２記載のＩＰアドレス変換方法であって、
前記第１の処理において、前記演算処理手段が、前記アクセスログデータを収集するマ

シンのＩＰアドレスのネットワークアドレス部とホストアドレス部との境界に相当する位置を、前記ブロックの境界として設定する、
ことを特徴とするＩＰアドレス変換方法。
【請求項１４】
請求項１１、１２及び１３のうちのいずれか１項に記載のＩＰアドレス変換方法であって、
前記第２の処理において、前記演算処理手段が、前記各ブロック内のデータを、当該ブロックに関して読み出した前記第２の数値と予め定めた関係を有する、前記変域外の第３の数値のデータに変換させる、
ことを特徴とするＩＰアドレス変換方法。
【請求項１５】
請求項１１、１２、１３及び１４のうちのいずれか１項に記載のＩＰアドレス変換方法であって、
前記情報処理装置は入力受付手段を備え、
当該ＩＰアドレス変換方法は、
前記入力受付手段が前記ブロックの境界位置の指定を受け付ける処理をさらに含み、
前記第１の処理において、前記演算処理手段は、前記入力受付手段が指定を受け付けた境界位置に基づき、前記ＩＰアドレスに前記ブロックを設定する、
ことを特徴とするＩＰアドレス変換方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワーク上のシステムが収集するアクセスログデータの管理技術に係り、特に、アクセスログデータに含まれるアクセス元マシンのＩＰアドレスを変換する情報処理に関する。
【背景技術】
【０００２】
コンピュータウィルス対策として、ルータ、ファイアウォール等に残されたアクセスログデータの分析が行われている。例えば、非特許文献１には、ネットワーク上のファイアウォールからアクセスログデータを収集する分散型侵入検知システムが記載されている。さらに、非特許文献１には、この分散型侵入検知システムが収集したアクセスログデータの解析により得られた情報が公開されている。例えば、攻撃者のトップ１０のＩＰアドレス及びホスト名のリストが公表されている。
【０００３】
【非特許文献１】”Distributed Intrusion Detection System”、[online]、インターネット<URL:http://www.dShield.org/>
【発明の開示】
【発明が解決しようとする課題】
【０００４】
一般に、アクセスログデータ収集マシンへのアクセスは、それと同じサブネットワーク内のマシンからのものが多い。このため、アクセスログデータが大量に収集されると、アクセスログデータ収集マシンが存在するサブネットワークが、それらのアクセスログデータから推測される可能性がある。このような情報は、セキュリティ向上の観点から秘匿されることが好ましい。例えば、コンピュータウィルス、ワームは、感染マシンとネットワーク的に近いマシンにさらに感染する可能性があるため、サブネットワークが第三者に推測されることは好ましくない。
【０００５】
そこで、本発明は、アクセスログデータを第三者に提供する場合におけるセキュリティの向上を図ることを目的とする。
【課題を解決するための手段】

【０００６】
本発明の一態様によれば、
ＩＰアドレスを、当該ＩＰアドレスとは異なる値のアドレスに変換する情報処理装置であって、
予め定められたビット数のデータの変域内のデータが示す第１の数値に第２の数値を１対１に対応付ける変換情報が格納された記憶手段と、
前記ＩＰアドレスに定めた、前記ビット数のデータが示す数値のデータを含むブロックごとに、当該ブロック内のデータが示す数値に相当する前記第１の数値に対応付けられた前記第２の数値を前記変換情報から読み出し、当該ブロック内のデータを、当該読み出した第２の数値に基づき変換する演算処理手段と
を備えることを特徴とする情報処理装置を提供する。
【発明の効果】
【０００７】
本発明によれば、アクセスログデータを第三者に提供する場合におけるセキュリティの向上を図ることができる。
【発明を実施するための最良の形態】
【０００８】
以下、添付の図面を参照しながら、本発明に係る実施形態について説明する。
【０００９】
まず、本実施の形態に係る情報処理装置（以下、アドレス管理装置）の構成について説明する。
【００１０】
図１に示すように、本実施の形態に係るアドレス管理装置１００は、入力装置及び出力装置が接続される入出力インタフェース１０１、メモリ１０２、各種プログラム等が格納された記憶装置１０４、記憶装置１０４からメモリ１０２上にロードしたプログラムを実行する演算処理装置１０３、記憶媒体からのデータ読み出し等を制御するドライブ（不図示）、ネットワークを介した通信を制御する通信装置１０５、これらを相互に接続するバス１０９、等を有している。
【００１１】
記憶装置１０４には、後述のアドレス管理処理が定義されたアドレス管理プログラム（不図示）が格納されている。このアドレス管理プログラムは、例えば、ドライブを介して記憶媒体から記憶装置１０４にインストールされてもよいし、ネットワークを介して記憶装置１０４にインストールされてもよい。
【００１２】
また、記憶装置１０４には、アドレス管理プログラムの他、アドレス管理プログラムにより参照等される以下の情報１０４Ａ～１０４Ｄが格納される。
【００１３】
アクセスログファイル（変換前ログファイル）１０４Ａには、図３に示すように、アクセスログ収集マシン（ルータ、ファイアウォール、侵入検知システム（ＩＤＳ）、ゲートウェイ、サーバ等）により収集されたアクセスログデータ１０４ａが記述されている。各アクセスログデータには、アクセス元マシンのＩＰアドレス１０４ａ１、アクセス時刻１０４ａ２、使用プロトコル１０４ａ３、アクセスを受け付けたポートの番号１０４ａ４、等が含まれる。なお、各アクセスログデータ内のＩＰアドレスが、後述のアドレス管理処理における変換対象アドレスとなる。
【００１４】
分割情報１０４Ｂには、図５に示すように、変換対象アドレスに含まれるブロック数１０４ｂ１、変換対象アドレスのブロック間の境界位置を表す分割位置情報１０４ｂ２が含まれている。ここでは、分割位置情報１０４ｂ２として、先頭ビットからの各境界位置までのオフセット値（１０進数表記にした変換対象アドレスの先頭ビットから各ブロックの末尾ビットまでのビット数）が格納される。なお、図５には、一例として、１０進数表記

とした変換対象アドレスが３箇所の境界位置（８ビット目、１６ビット目、３２ビット目）で８ビットの４ブロックに分割される場合の分割情報を示してある。

【００１５】

変換情報１０４Ｃには、図６に示すように、変換対象アドレスのブロック内のデータが取り得る数値（変換前ブロック値）とその変換後の数値（変換後ブロック値）との対応情報１０４ｃ１～１０４ｃｎが格納されている。すなわち、変換情報１０４Ｃは、変換前ブロック値に変換後ブロック値を一対一に対応付けたテーブルになっている。この変換情報１０４Ｃにしたがって変換対象アドレス内の各ブロックのデータを変換すれば、変換対象アドレスは、元のブロックとは異なる値を示すブロックで構成されるアドレスに変換される。

【００１６】

なお、ここでは、変換対象アドレスのすべてのブロックの変換に用いられる共通の変換情報１０４Ｃを示したが、変換対象アドレスのブロックごとに、異なる変換情報が準備されてもよい。

【００１７】

公開用のアクセスログファイル（変換後ログファイル）１０４Ｄには、図７に示すように、変換前ログファイル１０４Ａの各アクセスログデータ１０４ａから得られた公開用ログデータ１０４ｄが格納される。各公開用ログデータ１０４ｄには、対応するアクセスログデータ内の変換対象アドレスの各ブロックの変換により得られた公開用アドレス１０４ｄ１、対応アクセスログデータ内のデータ（アクセス時刻１０４ａ２、使用プロトコル１０４ａ３、ポート番号１０４ａ４）と同じデータ１０４ｄ２～１０４ｄ４が含まれている。なお、これら公開用ログデータは、後述のアドレス管理処理により生成される。

【００１８】

そして、演算処理装置１０３は、アドレス管理プログラムの実行により、以下の機能構成部を実現する。すなわち、分割情報１０４Ｂを生成するアドレス分割部１０３１、分割情報１０４Ｂ及び変換情報１０４Ｃにしたがって変換対象アドレス内の各ブロックをそれぞれ変換するアドレス変換部１０３２、を実現する。

【００１９】

これらの機能構成部の機能により公開用ログデータ生成処理が実現する。つぎに、図２により、この公開用ログデータ生成処理について説明する。ここでは、３２ビットのＩＰｖ４アドレスを含むアクセスログデータ１０４ａが記述された変換前ログファイル１０４Ａが、以下の処理の開始前に記憶装置１０４に読み込まれることとする。

【００２０】

ユーザが入力装置から所定のコマンドを入力すると、アドレス分割部１０３１は、このコマンドに応じて、記憶装置１０４内の分割情報１０４Ｂを参照し、この分割情報１０４Ｂに基づき分割情報設定画面を生成して、それを出力装置に表示する。

【００２１】

この分割情報設定画面には、変換対象アドレスのビット列に対応するボックス列と、設定完了指示を受け付けるＯＫボタンと、が配置されている。ここでは、変換対象アドレスが３２ビットのＩＰｖ４アドレスであるため、分割情報設定画面４０１上には、図４に示すように、３２個のボックスの列４０２及びＯＫボタン４０４が表示される。なお、本実施の形態においては、３２ビットのＩＰｖ４アドレスを変換対象アドレスとしているが、１２８ビットのＩＰｖ６アドレスを変換対象アドレスとする場合には、上分割情報設定画面上のボックス数を１２８個とすればよい。

【００２２】

ここで、ユーザが、入力装置を用いて、隣り合うボックスの間をマウスカーソル４０５で指示すると、この指示位置に、ブロック間の境界位置を示すスライダー４０３が配置される。これにより、ユーザは、変換対象アドレスにブロック間の境界位置を設定することができる。

【００２３】

その後、ユーザがＯＫボタン４０４を指示すると、アドレス分割部１０３１は、分割情報設定画面上の設定内容に基づき分割情報１０４Ｂを生成し、この分割情報１０４Ｂを記憶装置１０４に保存する（Ｓ２０１）。ここで生成される分割位置情報１０４Ｂには、分割情報設定画面上のスライダー４０３の数よりも１大きい数値がブロック数情報１０４ｂ１として、ボックス列４０２の先頭ボックスから各スライダー４０３までのボックス数が分割位置情報１０４ｂ２として格納されている。

【００２４】

その後、ユーザは、入力装置を用いて、ブロック値と変換後のブロック値とを１対１に対応付けたテーブルを作成し、これを変換情報１０４Ｃとして記憶装置１０４に格納する（Ｓ２０２）。なお、ここでは、ユーザが変換情報を入力しているが、アドレス管理装置１００が変換情報を自動的に生成されるようにしてもよい。例えば、アドレス変換部１０３２が、分割位置情報１０４ｂ２から求まるサイズのブロックがとり得る各値（変更前ブロック値）に対して、時刻等をシードに発生させた乱数（変更後ブロック値）を１対１に対応付けることによって変更情報を自動生成するようにしてもよい。このようにすれば、外部からの変換情報の入力を不要とすることができる。また、外部からの変換情報の入力を要しないため、変換情報の秘匿性をより向上させることができる。

【００２５】

このようにして分割情報１０４Ｂ及び変換情報１０４Ｃが準備されたら、アドレス分割部１０３１は、その旨をアドレス変換部１０３２に通知する。これにより、以下の処理（Ｓ２０３～Ｓ２０９）が開始される。

【００２６】

アドレス変換部１０３２は、記憶装置１０４の変換対象ログファイル１０４Ａを参照し、変換前ログファイル１０４Ａ内のすべてのアクセスログデータの変換が終了したか否かチェックする（Ｓ２０３）。

【００２７】

このとき、変換前ログファイル１０４Ａ内のすべてのアクセスログデータの変換が終了していれば、アドレス変換部１０３２は、記憶装置１０４から変換後ログファイル１０４Ｄ内のすべての公開用ログデータを読み出し、それらを、例えば通信装置１０５から外部システムに出力する（Ｓ２０７）。

【００２８】

一方、変換前ログファイル１０４Ａ内に未変換のアクセスログデータが残っていれば、アドレス変換部１０３２は、１レコードの未変換のアクセスログデータを、変換対象ログデータとして変換対象ログファイル１０４Ａから読み込み、この変換対象ログデータ内のＩＰアドレス１０４ａ１を変換対象アドレスとして読み出す（Ｓ２０４）。

【００２９】

その後、アドレス変換部１０３２は、記憶装置１０４内の分割情報１０４Ｂ及び変換情報１０４Ｃに基づき変換対象アドレスを公開用アドレスに変換し、変換対象ログデータに対応する公開用ログデータを生成する（Ｓ２０５）。具体的には、以下の通りである。

【００３０】

アドレス変換部１０３２は、記憶装置１０４から変換情報１０４Ｃを読み出して、各対応情報内の変換前ブロック値及び変換後ブロック値と、変換対象アドレスと、を２進数表記に変換する。

【００３１】

その後、アドレス変換部１０３２は、記憶装置１０４から分割情報１０４Ｂを読み出し、この分割情報１０４Ｂ内の分割位置情報１０４ｂ２が示す位置を境界として複数のブロックを２進数表記の変換対象アドレスから切り出す。例えば、分割情報１０４Ｂの分割位置情報１０４ｂ２が８ビットおきの３箇所の境界位置（８ビット目、１６ビット目、３２ビット目）を示している場合には、アドレス先頭から８ビット目までの第１ブロック、９ビット目から１６ビット目までの第２ブロック、１７ビット目から３２ビット目までの第３ブロック、３３ビット目からアドレス末尾までの第４ブロックが抽出される。また、分

割情報１０４Ｂの分割位置情報１０４ｂ２が１箇所の境界位置（１６ビット目）だけを示している場合には、アドレス先頭から１６ビット目までの第１ブロック、１６ビット目からアドレス末尾までの第４ブロックが抽出される。

【００３２】

アドレス変換部１０３２は、このとき抽出した各ブロックのブロック値に合致する２進表記の変換前ブロック値を変換情報１０４Ｃで検索し、この検索により得られた変換前ブロック値に対応付けられた２進表記の変換後ブロック値を読み出す。さらに、アドレス変換部１０３２は、それらの２進数表記の変換後ブロック値を、変換対象アドレス内におけるブロックの順番にしたがって連結する。これにより、２進数表記の公開用アドレスが生成される。

【００３３】

例えば、２進数表記の変換対象アドレスから１６ビットの２ブロックが抽出された場合、まず、上位１６ビットの第１ブロック及び下位１６ビットの第２ブロックの各ブロック値が、二進数表記の変換情報（０～６５５３５の各値に対応する２進数表記の変換前ブロック値に２進数表記の変換後ブロック値を１対１に対応付けるテーブル）にしたがってそれぞれ変換される。これらの２進数表記の変換後ブロック値が連結され、その結果、２進数表記の公開用アドレスが得られる。

【００３４】

その後、アドレス変換部１０３２は、２進数表記の公開用アドレスを、アドレス先頭から８ビットずつ１０進数表記に変換し、それらの間をピリオドで区切る。本実施の形態においては、このようにして得られた１０進数表記のアドレスを公開用アドレスとして用いるが、この１０進数表記のアドレス内の４つの数字（ピリオドで間を仕切られた４つの数字）を、所定の演算によって、通常のＩＰアドレス内の数字がとり得ない数値範囲の数字に変換したものを公開用アドレスとして用いてもよい。一般に、１０進数表記のＩＰアドレスは、０から２５５の数値範囲の４つの数字で構成される。したがって、例えば、上述のようにして得られた１０進数表記のアドレス内の４つの数字にそれぞれに２５６を加算したものを公開用アドレスとして用いてもよい。このようにすることによって、公開用アドレスは、ＩＰアドレスを構成する数字としてはあり得ない４つの数字で構成される。このため、公開用アドレスと実際のＩＰアドレスとを容易に識別することができるため、公開用アドレスと実際のＩＰアドレスとの混同が防止される。また、公開用アドレスを扱うユーザは、一見して、その公開用アドレスが真のＩＰアドレスでないことを識別することができるため、安心感を得ることができる。

【００３５】

さて、公開用アドレスが得られると、アドレス変換部１０３２は、Ｓ２０４で読み出したアクセスログデータからＩＰアドレス１０４ａ１以外のデータ１０４ａ２～１０４ａ４を取り出し、これらのデータと１０進数表記の公開用アドレスとを含む公開用ログデータを生成する。

【００３６】

そして、アドレス変換部１０３２は、このようなアドレス変換処理（Ｓ２０５）により生成した公開用ログデータを、記憶装置１０４上の変換後ログファイル１０４Ｄに追加レコード１０４ｄとして記述する（Ｓ２０６）。その後、アドレス変換部１０３２は、Ｓ２０３に処理を戻す。

【００３７】

以上の公開用ログデータ生成処理によれば、アクセス元マシンのＩＰアドレスが、元の値とは異なる値に変換されてから、公開用ログデータに格納されるため、公開用ログデータが第三者に公開されても、第三者による、アクセス元マシンの実際のＩＰアドレスの特定を防止することができる。このため、アクセスログデータ収集マシンが存在するサブネットワークに関する情報の漏洩を防止することができる。すなわち、ログデータを第三者に提供する場合におけるセキュリティの向上を図ることができる。

【００３８】

また、ログデータの提供を受けた第三者によるアクセス元マシンの特定を防止することができるため、例えば、どのユーザがどのようなサイトにアクセスしたかといった個人情報を秘匿することができる。すなわち、アクセス元マシンのユーザのプライバシー保護を強化することができる。

【００３９】

したがって、第三者へのログデータの公開による不利益が少なくなるため、ログデータの提供を必要とする、第三者の提供する有用なサービスの利用を促進することができる。つぎに、そのようなサービスについて説明する。ここでは、アドレス管理装置１００のユーザに提供されるログデータ分析サービスを例に挙げる。

【００４０】

図８に示すように、アドレス管理装置１００と、アドレス管理装置１００の出力する公開用ログデータの入力先となる分析装置８００とが、ネットワーク８１０を介して接続されている。

【００４１】

分析装置８００は、入力装置及び出力装置が接続された入出力インタフェース８０１、ネットワーク８１０を介した通信を制御する通信装置８０５、プログラムがインストールされた記憶装置８０２、メモリ８０４、記憶装置８０２からメモリ８０４にロードした分析プログラムを実行する演算処理装置８０３、これらを接続するバス等、を有している。

【００４２】

そして、演算処理装置８０３は、分析プログラムの実行によって、ログデータ分析処理を実行する分析部８０３１を実現する。この分析部８０３１の機能により、図９に示すフローチャートにしたがって、アドレス管理装置のユーザにログデータ分析サービスが提供される。

【００４３】

Ｓ２０８でアドレス管理装置１００が出力した公開用ログデータを通信装置８０５が受け付けると、分析部８０３１は、その公開用ログデータを記憶装置８０２に保存する（Ｓ９０１）。

【００４４】

その後、分析部８０３１は、記憶装置８０２上の公開用ログデータに基づき通常の分析処理（集計、統計等）を実行する（Ｓ９０２）。これにより、例えば、公開用ログデータのなかから、不正アクセス等の可能性を示す公開用ログデータを抽出する。

【００４５】

さらに、分析部８０３１は、抽出した公開用ログデータから公開用アドレス１０４ｄ１を読み出し、その公開用アドレスを含む報告メッセージを、通信装置８０５を介して、アドレス管理装置１００に返信する（Ｓ９０３）。このとき、さらに、分析部８０３１が、分析の結果得られた情報のうち、ＩＰアドレスを秘匿しても開示可能な情報（例えば、アクセスの多い時間帯、アクセスの多いポート番号等）を公開するようにしてもよい。

【００４６】

アドレス管理装置１００においては、分析装置８００からの報告メッセージを通信装置１０５が受け付けると、アドレス変換部１０３２が、その報告メッセージから公開用アドレスを取り出し、分割情報１０４Ｄ及び２進数表記の変換情報１０４Ｃに基づき、この公開用アドレスから、アクセス元マシンの実際のＩＰアドレスを復元する（Ｓ９０４）。具体的には、以下のアドレス逆変換処理を実行する。

【００４７】

アドレス変換部１０３２は、公開用アドレスを２進数表記に変換し、その２進数表記の公開用アドレスから、分割情報１０４Ｄの分割位置情報１０４ｄ２に基づきブロックを抽出する。その後、アドレス変換部１０３２は、各ブロックの値に合致する変換後ブロック値を２進数表記の変換情報１０４Ｃで検索し、その結果得られた変換後ブロック値に対応付けられた変換前ブロック値を変換情報１０４Ｃから取り出す。さらに、アドレス変換部１０３２は、これにより得られた変換前ブロック値を、変換後アドレス内におけるブロッ

クの順番にしたがって連結する。これにより、アクセス元マシンの２進数表記のＩＰアドレスが得られる。その後、この２真数表記のＩＰアドレスを、アドレス先頭から８ビットずつ、１０進数表記に変換する。これにより、アドレス管理装置１００では、不正なアクセスを行なった可能性のあるマシンのＩＰアドレスを特定することができる。

【００４８】

このように、アクセス元マシンの真のＩＰアドレスを秘匿したまま、ログデータの分析（不正アクセスの疑いがあるマシンの特定等）を外部システムに依頼することができる。変換後アドレスからアクセス元マシンの実際のＩＰアドレスを外部システム側で特定することは困難であるため、たとえ大量のログデータが外部システムに提供されたとしても、アクセスログデータ収集マシンが存在するサブネットワークに関する情報を外部システム側で推測することは困難である。また、変換後アドレスからではアクセス元マシンの特定は困難であるから、アクセス元マシンのユーザに関する情報が外部システム側に漏洩することを防止することができる。

【００４９】

したがって、セキュリティの維持及びアクセス元マシンのユーザのプライバシー保護を図りつつ、分析委託サービス等の外部サービスを利用することが可能となる。

【００５０】

図８には、１台の分析装置８００に公開用ログデータを提供するアドレス管理装置が１台だけの場合を示したが、もちろん、ネットワーク８１０上には、図１０に示すように、１台の分析装置８００に公開用ログデータを提供するアドレス管理装置１００が複数存在していてもよい。この場合、分析装置８００は、いずれかのアドレス管理装置から公開用ログデータを受け付けると、上述の処理（図９のＳ９０２～Ｓ９０３）を実行し、得られた報告メッセージを公開用ログデータ送信元に返信すればよい。これにより、複数のアドレス管理装置１００が１台の分析装置８００を共用することができる。

【００５１】

以上においては、変換対象アドレス内のすべての境界位置をユーザが設定しているが、一部またはすべての境界位置が自動的に設定されるようにしてもよい。例えば、アドレス管理装置１００が、アクセスログデータ収集マシンのオペレーティングシステムからサブネットマスクを取得し、このサブネットマスクから求まる、ＩＰアドレスのネットワークアドレス部（上位ビット）とホストアドレス部（下位ビット）との境界位置をブロック間境界位置として設定するようにしてもよい。また、ネットワークアドレス部とホストＩＤ部との境界位置の他、さらに、ユーザから指定された位置もブロック間境界位置として設定されるようにしてもよい。

【００５２】

このようにすれば、アクセスログデータ収集マシンと同じサブネットに属しているすべてのマシンのＩＰアドレスは、変換後も、ネットワークアドレス部に相当する上位ビットのデータの値が互いに共通する。すなわち、アクセスログデータ収集マシンと同一サブネット上のマシンであれば、そのＩＰアドレスは、アクセスログデータ収集マシンと近い位置にあることを示すアドレスに変換される。

【００５３】

このため、変換後の公開用アドレスは、アクセスログデータ収集マシンと同じサブネット内のマシン（すなわち、アクセスログデータ収集マシンに近いマシン）のものなのか、外部ネットワークのマシンのものなのかを識別可能である。したがって、例えば、ウィルス、ワーム等の感染データが発見された場合、それが、イントラネット内のウィルスまたはワームの感染データなのか、外部ネットワークのマシンからの感染データなのかを変換後の公開用アドレスから識別することができる。

【００５４】

また、以上においては、公開用ログデータ生成処理の開始前に変換前ログファイル１０４Ａが読み込まれ、この変換前ログファイル１０４Ａに記述されたすべてのログデータ１０４ａから公開用ログデータ１０４ｄが生成されているが、アクセスイベントが発生する

ごとに、新たなアクセスログデータからリアルタイムに公開用ログデータが生成されるようにしてもよい。すなわち、必ずしも、オフラインで大量のアクセスログデータのＩＰアドレスを一度に公開用アドレスに変換する必要はなく、アクセスログデータ収集マシンが新たなアクセスログデータを生成するごとに、アドレス管理装置１００が、その新たなアクセスログデータのＩＰアドレスをリアルタイムに公開用アドレスに変換するようにしてもよい。

【００５５】

このようにするには、前述の場合（図２参照）と異なり、ネットワーク上のアクセスログデータ収集マシンからのアクセスログレコードを通信装置１０５が受け付けると、アドレス変換部１０３２が、このアクセスログデータを変換対象ログデータとして上述のアドレス変換処理（Ｓ２０５と同様な処理）を実行し、その結果得られた公開用ログデータを、通信装置１０５から外部システム宛に出力するようにすればよい。

【００５６】

これにより、外部システムは、アクセスログデータ収集マシンでアクセスイベントが発生するごとに、公開用ログデータをリアルタイムに受け付けることができる。したがって、後段の外部システムは、アクセスログデータ収集マシンでアクセスが発生すると直ちに、このアクセスに関係するアクション（例えばログデータの統計等の解析処理）をとることが可能となる。

【００５７】

ところで、以上においては、アドレス管理装置１００は変換情報１０４Ｃを外部に提供しないが、アドレス管理装置１００が、ログデータの提供先に変換情報１０４Ｃを提供するようにしてもよい。例えば、ログデータの提供先が分析装置である場合を例に挙げて説明する。

【００５８】

図１１に示すように、この場合における分析装置１１００は、前述の分析装置８００と同様なハードウエア構成を有している。ただし、分析プログラムの実行によって演算処理装置が実現する機能構成が、前述の分析装置８００とは異なっている。すなわち、この場合の分析装置１１００においては、分析プログラムの実行によって、分析部１１０１に加えて、アドレス変換部１１０２を実現する。

【００５９】

このような機能構成により実現される分析処理のフローチャートを図１２に示す。ここでは、分析装置に公開用ログデータ等を提供するアドレス管理装置が複数存在する場合を例に挙げる。

【００６０】

この場合には、各アドレス管理装置１００が、Ｓ２０７において、公開用ログデータに加えて２進数表記の変換情報１０４Ｃも分析装置１１００宛てに出力する。分析装置１１００においては、いずれかのアドレス管理装置からの公開用ログデータ及び変換情報１０４Ｃを通信装置が受け付けると、分析部１１０１が、それらの公開用ログデータ及び変換情報１０４Ｃを記憶装置に保存する（Ｓ１２０１）。ここで、公開用ログデータ及び変更情報は、いずれのアドレス管理装置からのデータであるかを識別可能なファイル名のファイルに格納される。

【００６１】

分析部１１０１は、すべてのアドレス管理装置からの公開用ログデータ等の受付が終了したか否かを判断する（Ｓ１２０２）。その結果、いずれかのアドレス管理装置から公開用ログデータ等を受け付けていなければ、分析部１１０１は、そのアドレス管理装置からの公開用ログデータ等の入力を待機する（Ｓ１２０１）。

【００６２】

一方、すべてのアドレス管理装置から公開ログデータ等を受け付けていれば、アドレス変換部１１０２は、アドレス管理装置ごとに、公開用ログデータ内の公開用アドレス及び変換情報を記憶装置から読み出し、前述のアドレス逆変換処理（図９のＳ９０４）と同様

の処理によって、その変換情報に基づき、その公開用アドレスを真のＩＰアドレスに変換する（Ｓ１２０３）。そして、アドレス変換部１１０２は、記憶装置上の公開用ログデータ内の公開用アドレスを実際のＩＰアドレスで上書きする。

【００６３】

その後、分析部１１０１は、すべてのアドレス管理装置の公開用ログデータをすべてマージしてから、通常の分析処理を実行する（Ｓ１２０４）。これにより、複数のサイトの公開用ログデータのなかから、不正アクセス等を示す可能性のある公開用ログデータを抽出し、アクセス元マシンを実際のＩＰアドレスによって特定することができる。

【００６４】

分析の結果、不正なアクセス元マシンのＩＰアドレスが判明すれば、アドレス変換部１１０２が、そのＩＰアドレスを含む公開用ログデータに対応付けられたすべての変換情報を記憶装置から読み出し、各変換情報を用いて、上述のアドレス変換処理（図２のＳ２０５）と同様な処理を実行する。これにより、不正なアクセス元マシンのＩＰアドレスを、対応する公開用ログデータの各送信元（アドレス管理装置）の公開用アドレスに変換する（Ｓ１２０５）。そして、分析部１１０１は、このとき得られた公開用アドレスを含む報告メッセージを、対応する公開ログデータの送信元に、通信装置を介して返信する（Ｓ１２０６）。

【００６５】

このような分析処理によれば、複数のサイトで収集された大量のログデータに基づいて不審なアクセス元マシンを特定することができる。このため、各アドレス管理装置側では、自サイトのログデータだけなく、他のサイトのログデータも対象とした総合的な分析により不審と判断されたアクセス元マシン、すなわち、より信頼性の高い判断によって不審とされたアクセス元マシンを認識することができる。

【図面の簡単な説明】

【００６６】

【図１】本発明の実施形態に係る情報処理装置の概略ハードウエア構成図である。

【図２】本発明の実施の形態に係る公開用ログデータ生成処理のフローチャートである。

【図３】図１の変換前ログファイル内のデータ記述例を示した図である。

【図４】本発明の実施の形態に係る分割情報設定画面内のレイアウト例を示した図である。

【図５】図１の分割情報に含まれるデータを説明するための図である

【図６】図１の変換情報のデータ構造を概念的に示した図である。

【図７】図１の変換後ログファイル内のデータ記述例を示した図である。

【図８】本発明の実施の形態に係るアドレス管理装置と、その出力を受け付ける分析装置とを含むネットワークシステム構成図である。

【図９】図８のシステムにおいて、本実施の形態に係るアドレス管理装置のユーザに提供されるログデータ解析サービスのフローチャートである。

【図１０】本発明の実施の形態に係る、複数のアドレス管理装置と、その出力を受け付ける分析装置とを含むネットワークシステム構成図である。

【図１１】本発明の実施の形態に係る他の分析装置の構成を示した図である。

【図１２】図１１のシステムにおいて、本実施の形態に係るアドレス管理装置のユーザに提供されるログデータ解析サービスのフローチャートである。

【符号の説明】

【００６７】

１００…アドレス管理装置、１０３１…アドレス分割部、１０３２…アレス変換部、８００,１１００…分析装置、８０３１,１１０１…分析部、１１０２…アドレス変換部

【図１】

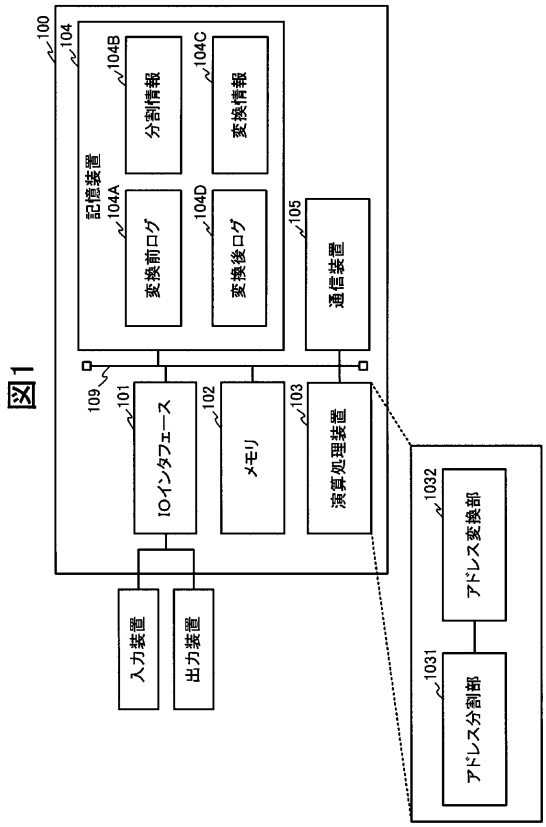
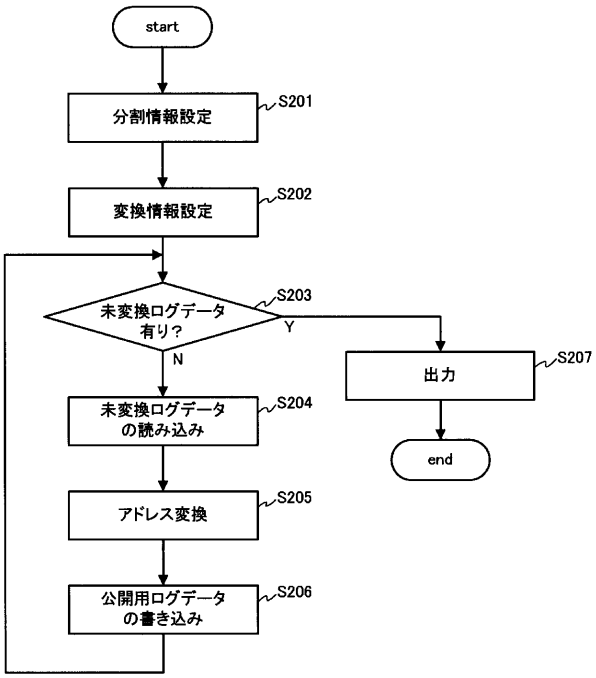


図1

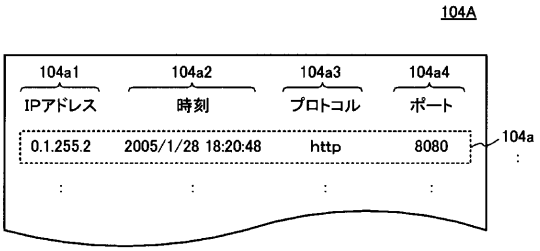
【図２】

図2



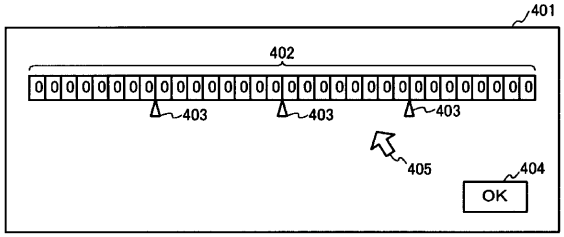
【図３】

図3



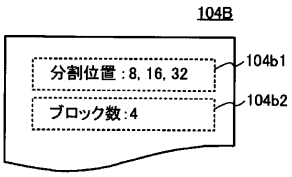
【図４】

図4



【図５】

図5



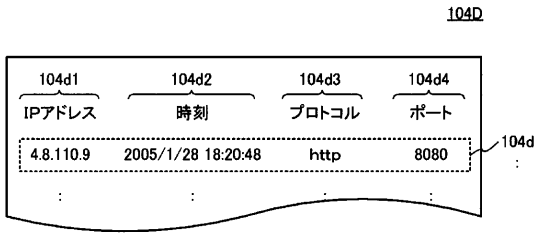
【図６】

図6

変換前ブロック値	変換後ブロック値	
0	4	104c1
1	8	104c2
2	9	104c3
255	110	104cn

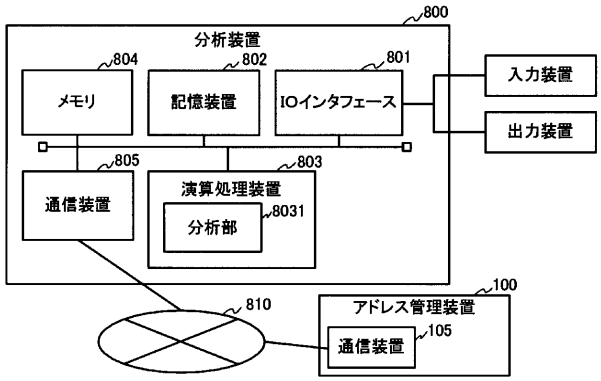
【図７】

図7



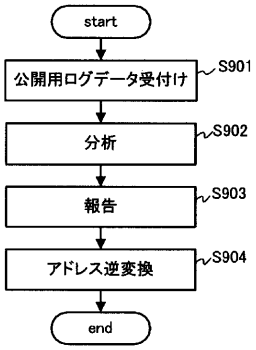
【図８】

図8



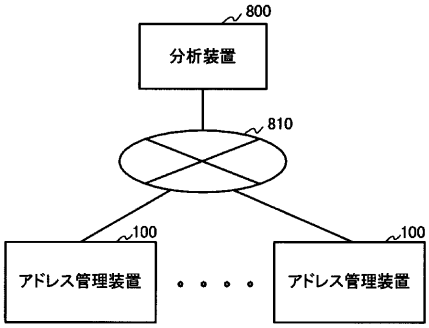
【図９】

図9



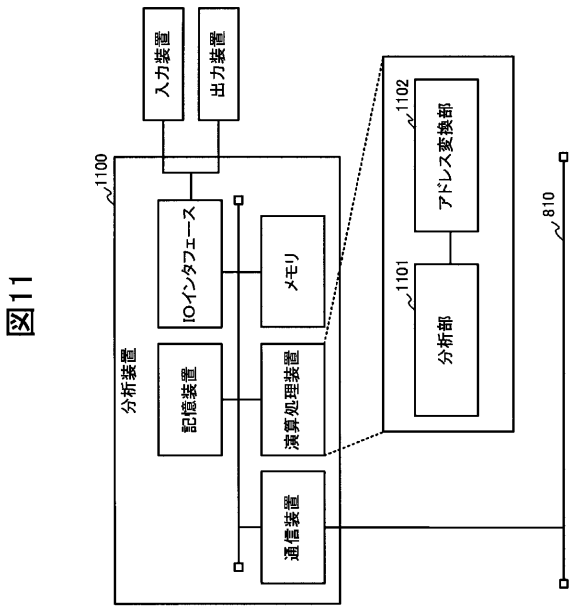
【図１０】

図10



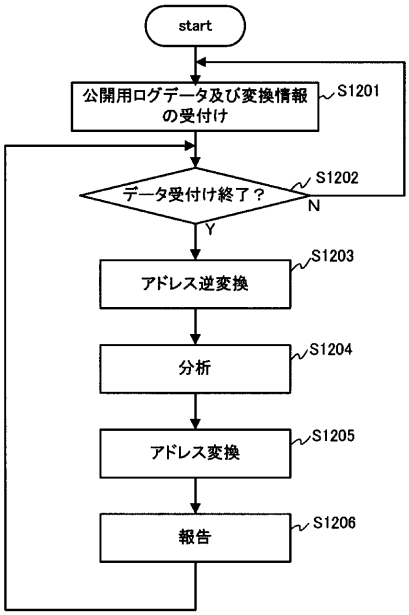
【図１１】

図11



【図１２】

図12



フロントページの続き

(72)発明者　仲小路　博史
神奈川県川崎市麻生区王禅寺１０９９番地　株式会社日立製作所システム開発研究所内

Ｆターム(参考) 5K030 GA15 HA08 HB06 HD03 JA10 KA02 LC13 MA01 MC08