(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6829615号
(P6829615)
(45)発行日　令和3年2月10日(2021.2.10)　(24)登録日　令和3年1月26日(2021.1.26)

(51)Int.Cl.　F I
H04L 12/28 (2006.01)　H04L 12/28　2OOM

請求項の数 15　(全 24 頁)

(21)出願番号　特願2017-15790(P2017-15790)
(22)出願日　平成29年1月31日(2017.1.31)
(65)公開番号　特開2018-125669(P2018-125669A)
(43)公開日　平成30年8月9日(2018.8.9)
審査請求日　令和2年1月7日(2020.1.7)

(73)特許権者　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　110001678
特許業務法人藤央特許事務所
(72)発明者　竹内　理
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　春名　高明
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内

審査官　平井　嗣人

最終頁に続く

(54)【発明の名称】送信パケットを監視する装置

(57)【特許請求の範囲】
【請求項１】
ネットワークアドレスによって定義されるセキュリティ境界内に位置するパケット送信元から送信されるパケットを、監視する装置であって、
プロセッサと、
前記プロセッサが実行するプログラムを格納するメモリと、を含み、
前記プロセッサは、
前記パケット送信元から送信されたパケットの宛先ネットワークアドレスの前記セキュリティ境界に対する位置を、前記セキュリティ境界上のネットワークアドレスと前記セキュリティ境界内のネットワークアドレスとを管理する管理情報に基づいて、特定し、
前記宛先ネットワークアドレスが前記セキュリティ境界外のアドレスであるパケットを破棄し、
前記宛先ネットワークアドレスが前記セキュリティ境界上のネットワークアドレスであるパケットに対して監視処理を実行する、装置。
【請求項２】
請求項１に記載の装置であって、
前記プロセッサは、前記宛先ネットワークアドレスが前記セキュリティ境界内のネットワークアドレスであるパケットを、前記監視処理を実行することなく転送する、装置。
【請求項３】
請求項１に記載の装置であって、

前記プロセッサは、前記監視処理において、パケットの種別に基づくフィルタリング、及び、パケットのログ記録の少なくとも一方を実行する、装置。
【請求項４】
請求項２に記載の装置であって、
前記パケット送信元は、前記装置で実行されているプログラムである、装置。
【請求項５】
請求項２に記載の装置であって、
ネットワークを介して、前記パケット送信元である計算機から送信されたパケットを受信する、装置。
【請求項６】
請求項１に記載の装置であって、
前記パケット送信元である計算機から送信されたパケットのうち、ゲートウェイ計算機において選択された、前記宛先ネットワークアドレスが前記セキュリティ境界上のネットワークアドレスのパケット及び前記セキュリティ境界外のネットワークアドレスのパケットを受信する、装置。
【請求項７】
請求項１に記載の装置であって、
前記プロセッサは、
前記宛先ネットワークアドレスが前記セキュリティ境界上のネットワークアドレスであり、かつ、予め設定されたセキュリティ境界内の記憶領域からのデータであることを示すマークを含むパケットに対して、前記監視処理を実行し、
前記宛先ネットワークアドレスが前記セキュリティ境界上のネットワークアドレスであり、かつ、前記予め設定されたセキュリティ境界内の記憶領域からのデータであることを示すマークを含まないパケットを、前記監視処理を実行することなく転送する、装置。
【請求項８】
請求項７に記載の装置であって、
前記プロセッサは、宛先アドレスがシールド境界内のＩＰアドレスである送信パケットに前記マークを含める、装置。
【請求項９】
ネットワークアドレスによって定義されるセキュリティ境界内に位置し、所定のパケットを送信するパケット送信元計算機と、
前記パケット送信元計算機からの前記所定のパケットを受信するパケット受信計算機と、
前記パケット送信元計算機及び前記パケット受信計算機の一方から送信されるパケットを監視する監視部と、を含み、
前記監視部は、
前記パケット送信元計算機及び前記パケット受信計算機の前記一方から送信されたパケットの宛先ネットワークアドレスの前記セキュリティ境界に対する位置を、前記セキュリティ境界上のネットワークアドレスと前記セキュリティ境界内のネットワークアドレスとを管理する管理情報に基づいて特定し、
前記宛先ネットワークアドレスが前記セキュリティ境界外のアドレスであるパケットを破棄し、
前記宛先ネットワークアドレスが前記セキュリティ境界上のネットワークアドレスであるパケットに対して監視処理を実行する、システム。
【請求項１０】
請求項９に記載のシステムであって、
前記監視部は、前記宛先ネットワークアドレスが前記セキュリティ境界内のネットワークアドレスであるパケットを、前記監視処理を実行することなく転送する、システム。
【請求項１１】
請求項１０に記載のシステムであって、

前記パケット受信計算機は、前記監視部を含み、
前記監視部は、前記パケット受信計算機から送信されるパケットを監視し、
前記パケット送信元計算機は、第２監視部を含み、
前記第２監視部は、
前記管理情報に基づいて、前記パケット送信元計算機から送信されるパケットの宛先ネットワークアドレスと前記セキュリティ境界との関係を特定し、
前記宛先ネットワークアドレスが前記セキュリティ境界外のアドレスであるパケットを破棄し、
前記宛先ネットワークアドレスが前記セキュリティ境界上のネットワークアドレスであるパケットに対して監視処理を実行し、
前記宛先ネットワークアドレスが前記セキュリティ境界内のネットワークアドレスであるパケットを、前記監視処理を実行することなく転送する、システム。
【請求項１２】
請求項９に記載のシステムであって、
前記セキュリティ境界内の第１ゲートウェイ計算機と第２ゲートウェイ計算機とをさらに含み、
前記第１ゲートウェイ計算機は転送部と前記監視部とを含み、
前記第２ゲートウェイ計算機は第２転送部と第２監視部とを含み、
前記転送部は、前記パケット受信計算機から送信されたパケットのうち、ネットワークアドレスが前記第２ゲートウェイ計算機と異なるパケットを選択して、前記監視部に送信し、
前記第２転送部は、前記パケット送信元計算機から送信されたパケットのうち、ネットワークアドレスが前記第１ゲートウェイ計算機と異なるパケットを選択して、前記第２監視部に送信し、
前記第２監視部は、
前記管理情報に基づいて、前記パケット送信元計算機から送信されるパケットの宛先ネットワークアドレスと前記セキュリティ境界との関係を特定し、
前記宛先ネットワークアドレスが前記セキュリティ境界外のアドレスであるパケットを破棄し、
前記宛先ネットワークアドレスが前記セキュリティ境界上のネットワークアドレスであるパケットに対して監視処理を実行する、システム。
【請求項１３】
請求項９に記載のシステムであって、
前記パケット送信元計算機及び前記パケット受信計算機の前記一方から送信されたパケットを転送するゲートウェイ計算機と、
前記監視部を含む監視計算機と、をさらに含み、
前記ゲートウェイ計算機は、前記パケット送信元計算機及び前記パケット受信計算機の前記一方からのパケットのうち、前記宛先ネットワークアドレスが前記セキュリティ境界上のネットワークアドレスのパケット及び前記セキュリティ境界外のネットワークアドレスのパケットを選択して、前記監視計算機に転送する、システム。
【請求項１４】
ネットワークアドレスによって定義されるセキュリティ境界内に位置するパケット送信元から送信されるパケットを、監視する方法であって、
前記パケット送信元から送信されたパケットの宛先ネットワークアドレスの前記セキュリティ境界に対する位置を、前記セキュリティ境界上のネットワークアドレスと前記セキュリティ境界内のネットワークアドレスとを管理する管理情報を参照して特定し、
前記宛先ネットワークアドレスが前記セキュリティ境界外のアドレスであるパケットを破棄し、
前記宛先ネットワークアドレスが前記セキュリティ境界上のネットワークアドレスであるパケットに対して監視処理を実行する、ことを含む方法。

【請求項１５】
請求項１４に記載の方法であって、
さらに、前記宛先ネットワークアドレスが前記セキュリティ境界内のネットワークアドレスであるパケットを、前記監視処理を実行することなく転送する、ことを含む方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、送信パケットを監視する技術に関する。
【背景技術】
【０００２】
本開示の背景技術として、特開２０００－３４９８５１号公報が知られている。特開２０００－３４９８５１号公報は、各ネットワークに属する端末間の通信を行うパケット転送装置において、セッションに対応したセキュリティ制御及び優先制御を可能にする技術を開示する。具体的には、「ルーティング処理、フィルタリング処理、及び優先制御処理を実行する主処理部から出力されたパケットがセッション開設条件に適合するか否かを判定し、該パケットについて適合判定した時、そのパケット情報を保持し、該パケット情報に基づいて同一セッションに属する後続のパケットを、該主処理部をバイパスして送出する。」ことを開示する（要約）。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０００－３４９８５１号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
例えば、エッジコンピューティング型分析／監視は、データ分析者がいない顧客の拠点に、分析プログラムを配信する。拠点の管理者（顧客管理者）に分析プログラムを持ち出されないセキュリティ機能が必要であるため、分析プログラムは暗号化される。顧客管理者は、分析プログラムの出力内容を確認できない。データ分析者は、例えば、顧客管理者が不在のデータセンタにおいて、分析プログラムの分析結果の解析作業を実施する。
【０００５】
上記例のように、顧客が管理できないアプリケーションプログラムが顧客の拠点において実行されている場合、上記アプリケーションプログラムに拠点内の機密データを外部に持ち出されないための、セキュリティ機能（情報漏洩監視機能）が要求される。さらに、情報漏洩監視のための処理負荷を低減することが望まれる。
【課題を解決するための手段】
【０００６】
本発明の代表的な一例は、ネットワークアドレスによって定義されるセキュリティ境界内に位置するパケット送信元から送信されるパケットを、監視する装置であって、プロセッサと、前記プロセッサが実行するプログラムを格納するメモリと、を含み、前記プロセッサは、前記パケット送信元から送信されたパケットの宛先ネットワークアドレスの前記セキュリティ境界に対する位置を、前記セキュリティ境界上のネットワークアドレスと前記セキュリティ境界内のネットワークアドレスとを管理する管理情報に基づいて、特定し、前記宛先ネットワークアドレスが前記セキュリティ境界外のアドレスであるパケットを破棄し、前記宛先ネットワークアドレスが前記セキュリティ境界上のネットワークアドレスであるパケットに対して監視処理を実行する。
【発明の効果】
【０００７】
本発明の一態様によれば、情報漏洩監視のための処理負荷を低減できる。
【図面の簡単な説明】

【０００８】
【図１Ａ】実施例１のシステムの構成例を示す。
【図１Ｂ】一般的な計算機構成を示す。
【図２Ａ】シールド内計算機ＩＰアドレスリストの構成例を示す。
【図２Ｂ】シールド境界計算機ＩＰアドレスリストの構成例を示す。
【図２Ｃ】フィルタポリシの構成例を示す。
【図３】パケットの構成例を示す。
【図４】分析結果確認部及びデータ分析部の処理のフローチャートを示す。
【図５】配信元計算機及び配信先計算機における、ネットワークＩ／Ｏ記録＆フィルタ部による監視処理を含むフローチャートを示す。
【図６】フィルタポリシに基づく処理の詳細のフローチャートを示す。
【図７】実施例２のシステムの構成例を示す。
【図８】転送制御テーブルの構成例を示す。
【図９】ゲートウェイ計算機ＩＰアドレス／ＭＡＣアドレスリストの構成例を示す。
【図１０】転送制御テーブルを作成するフローチャートを示す。
【図１１】配信元計算機及び配信先計算機における処理のフローチャートを示す。
【図１２】スイッチ装置Ａ、スイッチ装置Ｂの処理のフローチャートを示す。
【図１３】ゲートウェイ計算機Ａ／ゲートウェイ計算機Ｂにおけるパケット転送部の処理のフローチャートを示す。
【図１４】ゲートウェイ計算機Ａ／ゲートウェイ計算機ＢにおけるネットワークＩ／Ｏ記録＆フィルタ部の処理のフローチャートを示す。
【図１５】実施例３のシステムの構成例を示す。
【図１６】フィルタ計算機ＩＰアドレス／ＭＡＣアドレスリストの構成例を示す。
【図１７】転送制御テーブルを作成するフローチャートを示す。
【図１８】ゲートウェイ計算機Ａにおけるパケット転送部の処理のフローチャートを示す。
【図１９】実施例４のシステムの構成例を示す。
【図２０】ｔａｉｎｔ領域リストの構成例を示す。
【図２１】ｔａｉｎｔ　ｂｉｔｍａｐの構成例を示す。
【図２２】ｔａｉｎｔ領域追跡部による処理のフローチャートを示す。
【図２３】配信先計算機及び配信元計算機それぞれにおける処理のフローチャートを示す。
【図２４】ネットワークＩ／Ｏ記録＆フィルタ部による受信パケットの処理のフローチャートを示す。
【図２５】ネットワークＩ／Ｏ記録＆フィルタ部による送信パケットの処理のフローチャートを示す。
【発明を実施するための形態】
【０００９】
以下、添付図面を参照して本発明の実施形態を説明する。本実施形態は本発明を実現するための一例に過ぎず、本発明の技術的範囲を限定するものではないことに注意すべきである。
【実施例１】
【００１０】
本実施例は、分析プログラムの配信元計算機及び配信先計算機において、ネットワークＩ／Ｏ記録＆フィルタプログラムを実行する。本実施例において、分析プログラム及び分析結果確認プログラムは、それぞれ、配信先計算機及び配信元計算機において、仮想マシンにおいて実行される。Ｈｙｐｅｒｖｉｓｏｒ及びネットワークＩ／Ｏ記録＆フィルタプログラムは、ホストＯＳ上で動作する。
【００１１】
配信先計算機に実行されるネットワークＩ／Ｏ記録＆フィルタプログラムは、分析プロ

グラムが発行するＩ／Ｏ（機密データ漏洩）を監視する。分析プログラム及び仮想マシンは、それぞれパケットの送信元である。配信元計算機に実行されるネットワークＩ／Ｏ記録＆フィルタプログラムは、分析結果確認プログラムが発行するＩ／Ｏ（機密データ漏洩）を監視する。分析結果確認プログラム及び仮想マシンは、それぞれパケットの送信元である。

【００１２】

顧客管理者は、ネットワークにおけるセキュリティ境界（データシールド）を予め定義する。データシールド内においては、機密データを含むデータの移動が許可されている。データシールド境界のノード及びデータシールド内のノードが管理情報において管理される。本例において、データシールドは、これらノードにより定義される。以下に説明する例において、データシールドは、ネットワークアドレスの一例であるＩＰアドレスにより定義される。

【００１３】

例えば、配信先計算機、配信元計算機、分析プログラムが分析するデータを格納する拠点データベースは、データシールド内の計算機である。後述する例において、プロキシサーバがデータシールド境界の計算機として定義される。

【００１４】

ネットワークＩ／Ｏ記録＆フィルタプログラムは、監視対処プログラムから送信されるパケットを、送信先ノードのデータシールドにおける位置に基づいて、フィルタリングする。パケットは、ネットワークを転送されるデータユニットであって、任意の通信プロトコルレイヤのデータユニットである。

【００１５】

以下に説明する例において、ネットワークＩ／Ｏ記録＆フィルタプログラムは、データシールド外のノード（ＩＰアドレス）を宛先とするパケットをブロック（破棄）する。これにより、データ漏洩監視のための負荷を低減し、データシールド外へ転送されるパケットを、データシールド境界のノードを経由させる。

【００１６】

ネットワークＩ／Ｏ記録＆フィルタプログラムは、データシールド境界のノード（ＩＰアドレス）を宛先とするパケットを選択して、監視処理を実行する。監視処理は、フィルタリング及び／又はログ記録を行う。データシールド内のノード（ＩＰアドレス）を宛先とするパケットは、監視処理を行うことなく転送される。これにより、データ漏洩監視のための分析の負荷を低減する。

【００１７】

ネットワークＩ／Ｏ記録＆フィルタプログラムは、データシールド境界上のＩＰアドレスを経由したネットワークＩ／Ｏに対して、予め設定されているフィルタポリシ従ってフィルタリングを実行する。フィルタポリシは、例えば、プロキシサーバを介したｗｒｉｔｅ＝ｈｔｔｐのパケットにおいて、所定サイズ以上のＰＵＴを禁止する。

【００１８】

ネットワークＩ／Ｏ記録＆フィルタプログラムは、データシールド境界上のＩＰアドレスを宛先とするパケットのログを記録する。例えば、ネットワークＩ／Ｏ記録＆フィルタプログラムは、全てのパケットのログを記録する、又は、フィルタポリシに応じて選択した一部のパケットのログを記録する。なお、ネットワークＩ／Ｏ記録＆フィルタプログラムは、データシールド境界上ノードを宛先とするパケットのフィルタリングとログ記録の一方のみを実行してもよい。

【００１９】

以下に説明する例において、配信元計算機は、外部デバイスＩ／Ｏ記録＆フィルタプログラムを実行する。外部デバイスＩ／Ｏ記録＆フィルタプログラムは、分析結果確認プログラムから外部記憶デバイス、例えば、ハードディスクドライブ（ＨＤＤ）やＵＳＢフラッシュドライブへのデータ漏洩を監視する。配信先計算機も、外部デバイスＩ／Ｏ記録＆フィルタプログラムを実行し、分析プログラムから外部記憶デバイスへのデータ漏洩を監

視してもよい。

【００２０】

図１Ａは、本実施例のシステムの構成例を示す。図１Ａにおいて、同一の機能を有する異なる構成要素は、同一の符号を付されることがある。データ分析プログラムの配信元計算機１１１と配信先計算機１１２とは、ネットワーク１０４を介して接続されている。図１Ａの例において、ネットワークは、ＶＰＮ（Ｖｉｒｔｕａｌ　Ｐｒｉｖａｔｅ　Ｎｅｔｗｏｒｋ）である。配信元計算機１１１はデータセンタ１０１に設置され、配信先計算機１１２はデータセンタ１０１とは異なる拠点に設置されている。

【００２１】

配信元計算機１１１及び配信先計算機１１２は、ＶＰＮ１０４又は他のネットワークを介して、Ｉ／Ｏログデータベース（ＤＢ）１２１及び構成ＤＢ１２２にアクセスする。Ｉ／Ｏログデータベース（ＤＢ）１２１及び構成ＤＢ１２２は、それぞれ、例えば、データセンタ１０１又は拠点１０２に設置されたサーバ計算機に格納される。拠点ＤＢ１２３は、拠点１０２内の、例えばサーバ計算機に格納され、配信先計算機１１２からアクセスされる。

【００２２】

プロキシサーバ１１３及び１１４は、それぞれ、データセンタ１０１及び拠点１０２内に設置されている。プロキシサーバ１１３及び１１４は、他の計算機と外部ネットワーク（インターネット１０３）との間のデータ通信を仲介する。

【００２３】

ネットワークにおけるセキュリティ境界であるデータシールド１３１が、システムにおいて予め定義されている。データシールド１３１内においては、機密データを含むデータの移動が許可されている。データシールド１３１は、システム内のノードにより定義される。

【００２４】

具体的には、データシールド内のノード及びデータシールドの境界ノードにより定義される。図１Ａの例において、プロキシサーバ１１３、１１４は境界ノードであり、外部記憶デバイス１２５を除く他のノードが、シールド内ノードである。計算機は、ノードの一例である。

【００２５】

配信先計算機１１２は、データ分析部１４３、Ｈｙｐｅｒｖｉｓｏｒ１４５、ネットワークＩ／Ｏ記録＆フィルタ部１４７、ホストＯＳ１４８を含む。データ分析部１４３は、ＮＩＣ（Ｎｅｔｗｏｒｋ　Ｉｎｔｅｒｆａｃｅ　Ｃａｒｄ）を介して拠点ＤＢ１２３内の拠点データ１５５を取得して、分析する。

【００２６】

データ分析部１４３は、プロセッサが、Ｈｙｐｅｒｖｉｓｏｒ１４５でデータ分析プログラムを実行することで実現される。データ分析部１４３の分析結果は、Ｈｙｐｅｒｖｉｓｏｒ１４５を介して、ネットワークＩ／Ｏ記録＆フィルタ部１４７に送信される。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、プロセッサが、ホストＯＳ１４８上で、ネットワークＩ／Ｏ記録＆フィルタプログラムを実行することで実現される。

【００２７】

後述するように、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、データ分析部１４３のネットワークＩ／Ｏを監視する監視部である。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、構成ＤＢ１２２に格納されている情報を参照して、データ分析部１４３からのパケットのフィルタリング及びログ記録を実行する。

【００２８】

構成ＤＢ１２２は、シールド内計算機ＩＰアドレスリスト１５２、シールド境界計算機ＩＰアドレスリスト１５３、及びフィルタポリシ１５４を格納している。構成ＤＢ１２２の情報は、顧客管理者により予め構成される。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、データ分析部１４３のＩ／Ｏログの情報を、Ｉ／ＯログＤＢ１２１のＩ／Ｏログ１

５１に格納する。Ｉ／Ｏログ１５１は、顧客管理者によりチェックされる。
【００２９】
分析結果は、さらに、ネットワークＩ／Ｏ記録＆フィルタ部１４７から、ＮＩＣ、ＶＰＮ１０４を介して、配信元計算機１１１に転送される。配信先計算機１１２は分析結果を示すパケットの送信元計算機であり、配信元計算機１１１はそのパケットの受信計算機である。
【００３０】
配信元計算機１１１は、分析結果確認部１４１、Ｈｙｐｅｒｖｉｓｏｒ１４５、外部デバイスＩ／Ｏ記録部１４６、ネットワークＩ／Ｏ記録＆フィルタ部１４７、ホストＯＳ１４８を含む。配信元計算機１１１において、分析結果は、ＮＩＣ及びホストＯＳ１４８を介して、ネットワークＩ／Ｏ記録＆フィルタ部１４７に送信される。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、プロセッサが、ホストＯＳ１４８上でネットワークＩ／Ｏ記録＆フィルタプログラムを実行することで実現される。
【００３１】
ネットワークＩ／Ｏ記録＆フィルタ部１４７は、分析結果確認部１４１のネットワークＩ／Ｏを監視する監視部である。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、構成ＤＢ１２２に格納されている情報を事前に読み出し保持する。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、構成情報を参照して、分析結果確認部１４１からのパケットのフィルタリング及びログ記録を実行する。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、分析結果確認部１４１のＩ／Ｏログの情報を、Ｉ／ＯログＤＢ１２１におけるＩ／Ｏログ１５１に格納する。
【００３２】
分析結果確認部１４１は、分析結果を、ネットワークＩ／Ｏ記録＆フィルタ部１４７から、Ｈｙｐｅｒｖｉｓｏｒ１４５を介して、受信する。分析結果確認部１４１は、データ分析者が使用するユーザ端末に送信する。分析結果は、例えば、配信元計算機１１１の補助記憶に格納される。分析結果確認部１４１は、プロセッサが、Ｈｙｐｅｒｖｉｓｏｒ１４５でデータ分析プログラムを実行することで実現される。
【００３３】
外部デバイスＩ／Ｏ記録部１４６は、分析結果確認部１４１の外部記憶デバイス１２５とのＩ／Ｏを監視し、そのログを記録する。ログは、Ｉ／Ｏログ１５１に格納される。外部デバイスＩ／Ｏ記録部１４６は、プロセッサが、ホストＯＳ１４８上で外部デバイスＩ／Ｏ記録プログラムを実行することで実現される。
【００３４】
図１Ｂは、一般的な計算機構成を示す。配信元計算機１１１、配信先計算機１１２、プロキシサーバ１１３、１１４、ＤＢ１２１、１２２、１２３を格納する計算機、及びプロキシサーバ１１３、１１４は、例えば、図１Ｂに示すハードウェア構成を有する。
【００３５】
計算機１２は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）２２３と、ＣＰＵ２２３が処理を実行するために必要なデータ（プログラムを含む）を格納するための主記憶２２４と、大量のデータを記憶する容量を持つハードディスクやフラッシュメモリなどの補助記憶２２５を含む。
【００３６】
計算機１２は、さらに、他装置と通信を行なうためのＩＦ（インタフェイス）２２２と、これらの各装置を接続する通信路２２７と、を含む。プロセッサであるＣＰＵ２２３は、主記憶２２４に格納されたプログラムを実行することで所定の機能を実現する機能部として動作する。
【００３７】
補助記憶２２５は、ＣＰＵ２２３が使用するデータ（情報）を格納する。プログラムやデータは、あらかじめ主記憶２２４または非一時的記憶媒体を含む補助記憶２２５に格納されていてもよいし、必要な時に、ＩＦ２２２を介して他の装置から、インストール（ロ

ード）されてもよい。主記憶２２４及び補助記憶２２５は、個別に又は一体でメモリを構成する。計算機１２は、さらに、キーボード、ディスプレイなどの入出力を行うための入出力デバイス２２６を含んでもよい。なお、機能部の一部は、ＣＰＵ２２３と異なる専用回路で実現されてもよい。

【００３８】

データシールド１３１は、構成ＤＢ１２２の情報により管理（定義）されている。具体的には、データシールド１３１の境界計算機及び内部計算機の情報が、構成ＤＢ１２２に格納される。

【００３９】

図２Ａは、シールド内計算機ＩＰアドレスリスト１５２の構成例を示す。シールド内計算機ＩＰアドレスリスト１５２はデータシールド内の計算機のＩＰアドレスを示す。図２Ｂは、シールド境界計算機ＩＰアドレスリスト１５３の構成例を示す。シールド境界計算機ＩＰアドレスリスト１５３は、データシールド１３１の境界の計算機のＩＰアドレスを示す。

【００４０】

図２Ｃは、フィルタポリシ１５４の構成例を示す。フィルタポリシ１５４は、ネットワークＩ／Ｏ記録＆フィルタ部１４７により参照され、パケットに応じて実行すべき動作（）を示す。具体的には、フィルタポリシ１５４は、プロトコルカラム２０３、ｒｅａｄカラム２０４、ｗｒｉｔｅカラム２０５、及びａｃｔｉｏｎカラム２０６を有する。

【００４１】

ｒｅａｄカラム２０４及びｗｒｉｔｅカラム２０５は、それぞれ、ｒｅａｄパケット及びｗｒｉｔｅパケットを監視することなく転送することが許可されているか禁止されているか示す。ａｃｔｉｏｎ２０６は、禁止されているパケットに対する処理を示す。「禁止」されているパケットに対して、例えば、破棄、ログ記録、破棄及びログ記録、の処理が実行される。

【００４２】

図３は、パケットの構成例を示す。パケットは、Ｅｔｈｅｒｎｅｔ（登録商標）ヘッダ３０１、ＩＰヘッダ３０２、ＴＣＰヘッダ３０３、Ｌ７ヘッダ３０４及びＬ７データフィールド３０５を含む。Ｅｔｈｅｒｎｅｔヘッダ３０１は、宛先ＭＡＣアドレスフィールド３０６を含む。ＩＰヘッダ３０２は、送信元ＩＰアドレスフィールド３０７及び宛先ＩＰアドレスフィールド３０８を含む。ＴＣＰヘッダ３０３は、シーケンス番号フィールド３０９を含む。

【００４３】

図４は、分析結果確認部１４１及びデータ分析部１４３の処理のフローチャートを示す。分析結果確認部１４１は、分析部１４３（分析プログラム）を配信先計算機１１２のＨｙｐｅｒｖｉｓｏｒ１４５上で起動する（４０２）。分析部１４３は、拠点データ１５５にアクセスし、データ分析処理を実行する（４０３）。分析部１４３は、分析結果確認部１４１にデータ分析結果を送信する（４０４）。分析結果確認部１４１は、データ分析者の端末からの要求に応じて、データ分析結果をデータ分析者の端末において表示する（４０５）。

【００４４】

データ分析結果は、配信先計算機１１２において、Ｈｙｐｅｒｖｉｓｏｒ１４５、ネットワークＩ／Ｏ記録＆フィルタ部１４７、ホストＯＳ１４８を介して、配信元計算機１１１に転送される。配信元計算機１１１において、データ分析結果は、ホストＯＳ１４８、ネットワークＩ／Ｏ記録＆フィルタ部１４７、Ｈｙｐｅｒｖｉｓｏｒ１４５を介して、分析結果確認部１４１に転送される。

【００４５】

図５は、配信元計算機１１１及び配信先計算機１１２における、ネットワークＩ／Ｏ記録＆フィルタ部１４７による処理を含むフローチャートを示す。分析部１４３又は分析結果確認部１４１は、Ｈｙｐｅｒｖｉｓｏｒ１４５にＩ／Ｏ要求を発行する（５０１）。Ｈ

ｙｐｅｒｖｉｓｏｒ１４５は、Ｉ／Ｏ要求が、ネットワークＩ／Ｏ要求（ネットワークを介したＩ／Ｏ要求）であるか判定する（５０２）。

【００４６】

図１Ａの例においては、分析結果確認部１４１からのＩ／Ｏ要求は、ネットワークＩ／Ｏ要求ではなく、外部デバイスへのＩ／Ｏ要求であり得る。発行されたＩ／Ｏ要求がネットワークＩ／Ｏ要求ではない場合（５０２：他）、Ｈｙｐｅｒｖｉｓｏｒ１４５は、Ｉ／Ｏ要求をホストＯＳ１４８へのＩ／Ｏ要求に変換し、外部デバイスＩ／Ｏ記録部１４６に送信する（５０５）。外部デバイスＩ／Ｏ記録部１４６は、Ｉ／ＯログをＩ／ＯログＤＢ１２１に出力し（５０６）、Ｉ／Ｏ要求をホストＯＳ１４８に転送する。

【００４７】

発行されたＩ／Ｏ要求がネットワークＩ／Ｏ要求である場合（５０２：ネットワークＩ／Ｏ）、Ｈｙｐｅｒｖｉｓｏｒ１４５は、Ｉ／Ｏ要求をホストＯＳ１４８へのＩ／Ｏ要求に変換し、ネットワークＩ／Ｏ記録＆フィルタ部１４７に送信する（５０３）。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、Ｉ／Ｏ要求に含まれるパケットのＩＰヘッダ３０２における宛先ＩＰアドレスフィールド３０８を参照し、宛先ＩＰアドレスを特定する（５０４）。

【００４８】

ネットワークＩ／Ｏ記録＆フィルタ部１４７は、シールド内計算機ＩＰアドレスリスト１５２及びシールド境界計算機ＩＰアドレスリスト１５３を参照し、パケットの宛先ＩＰアドレスが、データシールド１３１に対して、どこに存在するか判定する（５０７）。

【００４９】

宛先ＩＰアドレスがシールド内ＩＰアドレスである場合、つまり、宛先ＩＰアドレスがシールド内計算機ＩＰアドレスリスト１５２に含まれる場合（５０７：シールド内ＩＰアドレス）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、フィルタリング及びログ記録（監視処理）を実行することなく、Ｉ／Ｏ要求をホストＯＳ１４８に転送する（５０８）。

【００５０】

宛先ＩＰアドレスがシールド外ＩＰアドレスである場合、つまり、宛先ＩＰアドレスがシールド内計算機ＩＰアドレスリスト１５２及びシールド境界計算機ＩＰアドレスリスト１５３に含まれない場合（５０７：他）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、Ｉ／Ｏ要求を破棄する（５１１）。

【００５１】

宛先ＩＰアドレスがシールド境界ＩＰアドレスである場合、つまり、宛先ＩＰアドレスがシールド境界計算機ＩＰアドレスリスト１５３に含まれる場合（５０７：シールド境界ＩＰアドレス）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、ＴＣＰヘッダ３０３のシーケンス番号（フィールド３０９内）に基づき、パケットを再構成した（５０９）後、フィルタポリシ１５４に基づきＩ／Ｏ要求（パケット）を処理する（監視処理）（５１０）。

【００５２】

図６は、フィルタポリシ１５４に基づく処理（５１０）の詳細のフローチャートを示す。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、Ｌ７ヘッダ３０４を解析して、使用されているプロトコルと、ｒｅａｄ／ｗｒｉｔｅ種別を判定する（６０１）。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、パケットが該当するエントリを、フィルタポリシ１５４においてを検索する（６０２）。

【００５３】

パケットが該当するエントリがフィルタポリシ１５４に存在しない場合（６０３：ＮＯ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、Ｉ／ＯログをＩ／ＯログＤＢ１２１に出力し（６１０）、当該パケットを破棄する（６１１）。

【００５４】

パケットが該当するエントリがフィルタポリシ１５４に存在する場合（６０３：ＹＥＳ

）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、当該パケットが、ホストＯＳ１４８からの送信が許可されているか判定する（６０４）。具体的には、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、該当エントリのｒｅａｄカラム２０４とｗｒｉｔｅカラム２０５の内の該当カラムが、「許可」を示すか判定する。

【００５５】

当該パケットが「許可」されている場合（６０４：ＹＥＳ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、Ｉ／Ｏログを出力することなく、Ｉ／Ｏ要求をホストＯＳ１４８に転送する（６０５）。

【００５６】

当該パケットが「禁止」されている場合（６０４：ＮＯ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、当該エントリのａｃｔｉｏｎカラム２０６の値が、「ｌｏｇ」を含むか判定する（６０６）。「ｌｏｇ」が含まれている場合（６０６：ＹＥＳ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、Ｉ／ＯログをＩ／ＯログＤＢ１２１に出力する（６０７）。

【００５７】

さらに、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、当該エントリのａｃｔｉｏｎカラム２０６の値が、「ｄｉｓｃａｒｄ」を含むか判定する（６０８）。「ｄｉｓｃａｒｄ」が含まれてない場合（６０８：ＮＯ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、Ｉ／Ｏ要求をホストＯＳ１４８に転送する（６０５）。「ｄｉｓｃａｒｄ」が含まれている場合（６０８：ＹＥＳ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、当該パケットを破棄する（６０９）。

【００５８】

上述のように本実施例の監視処理は、フィルタポリシに従い、パケットの種別（プロトコル種別及びｒｅａｄ／ｗｒｉｔｅ種別）に基づき、パケットの破棄／転送を決定し（フィルタリング）及びログ記録の有無を決定する。

【００５９】

以上のように、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、宛先ＩＰアドレスのデータシールド１３１に対する位置に基づき一部のパケットのみを選択して、ログ記録及びフィルタリング（監視処理）を実行する。これにより、情報漏洩のための処理負荷を低減できる。パケットの送信元（データ分析結果確認プログラム又は分析プログラム）と同一計算機においてネットワークＩ／Ｏ記録＆フィルタ部１４７が動作することで、他のハードウェア資源を使用することなく効率的にパケットを監視することができる。

【実施例２】

【００６０】

以下において、実施例２を説明する。主に、実施例１との差異を説明する。本実施例において、配信元計算機又は配信先計算機からのパケットは、ゲートウェイ計算機に転送される。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、ゲートウェイ計算機において、パケットのフィルタリング及びログ記録を実行する。これにより、配信元計算機及び配信先計算機の負荷を低減できる。また、複数の配信先計算機又は複数の配信元計算機のパケットを１台のゲートウェイ計算機において監視することができる。

【００６１】

図７は、本実施例のシステムの構成例を示す。実施例１の構成に加えて、スイッチ装置Ａ２１１、ゲートウェイ計算機Ａ２１３が、データセンタ１０１において追加され、スイッチ装置Ｂ２１２、ゲートウェイ計算機Ｂ２１４が、拠点１０２において追加されている。これら装置は、データシールド１３１内に配置されている。

【００６２】

配信先計算機１１２は、スイッチ装置Ｂ２１２を介して、ゲートウェイ計算機Ｂ２１４に接続されている。図７は１台の配信先計算機を示すが、複数の配信先計算機がゲートウェイ計算機Ｂ２１４に接続されてもよい。配信元計算機１１１は、スイッチ装置Ａ２１１を介して、ゲートウェイ計算機Ａ２１３に接続されている。図７は１台の配信元計算機を

示すが、複数の配信元計算機がゲートウェイ計算機Ａ２１３に接続されてもよい。
【００６３】
ゲートウェイ計算機Ａ２１３、ゲートウェイ計算機Ｂ２１４は、ＶＰＮ１０４を介して接続されている。配信元計算機１１１及び配信先計算機１１２は、それぞれ、ゲートウェイ計算機Ａ２１３及びゲートウェイ計算機Ｂ２１４を介して、プロキシサーバ１１３及び１１４に接続されている。
【００６４】
ゲートウェイ計算機Ａ２１３、ゲートウェイ計算機Ｂ２１４は、それぞれ、転送制御テーブル２５２、パケット転送部２４２、ネットワークＩ／Ｏ記録＆フィルタ部１４７を含む。ゲートウェイ計算機Ａ２１３、ゲートウェイ計算機Ｂ２１４は、それぞれ、はＮＩＣを介して他装置（ネットワーク）に接続されているに接続されている。パケット転送部２４２は、プロセッサがプログラムを実行することで実現される。
【００６５】
スイッチ装置Ａ２１１、スイッチ装置Ｂ２１２は、それぞれ、パケット検査部２４１を含む。スイッチ装置Ａ２１１、スイッチ装置Ｂ２１２は、それぞれ、はＮＩＣを介して他装置（ネットワーク）に接続されているに接続されている。パケット検査部２４１は、例えば、プロセッサがプログラムを実行することにより実現される。
【００６６】
本実施例において、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、配信元計算機１１１及び配信先計算機１１２に代えて、ゲートウェイ計算機Ａ２１３及びゲートウェイ計算機Ｂ２１４に実装されている。構成ＤＢ１２２は、実施例１の情報に加え、ゲートウェイ計算機ＩＰ／ＭＡＣアドレスリスト２５１を格納している。
【００６７】
図８は、転送制御テーブル２５２の構成例を示す。転送制御テーブル２５２は、パケットの宛先アドレスと転送先アドレスとを関連付ける。転送制御テーブル２５２は、宛先ＩＰアドレスカラム１００１、転送先ＩＰアドレスカラム１００２、及び転送先ＭＡＣアドレスカラム１００３を有する。
【００６８】
図９は、ゲートウェイ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１の構成例を示す。ゲートウェイ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１は、ゲートウェイ計算機のアドレスを管理する。ゲートウェイ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１は、ＩＰアドレスカラム１１０１及びＭＡＣアドレスカラム１１０２を有する。各エントリは、ゲートウェイ計算機のＩＰアドレスとＭＡＣアドレスとを示す。ゲートウェイ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１は、顧客管理者により予め設定される。
【００６９】
図１０は、転送制御テーブル２５２を作成するフローチャートを示す。ゲートウェイ計算機Ａ２１３、ゲートウェイ計算機Ｂ２１４は、それぞれ、シールド内計算機ＩＰアドレスリスト１５２に記載されている宛先ＩＰアドレス用の転送制御テーブルエントリを作成する（１２０１）。ゲートウェイ計算機Ａ２１３、ゲートウェイ計算機Ｂ２１４は、それぞれ、転送先ＩＰアドレスカラム１００２、転送先ＭＡＣアドレスカラム１００３にゲートウェイ計算機のＩＰアドレス及びＭＡＣアドレスを設定する（１２０２）。
【００７０】
図１１は、配信元計算機１１１及び配信先計算機１１２における処理のフローチャートを示す。ステップ８０１から８０５は、それぞれ、図５のステップ５０１から５０３、５０５、５０６に対応する。配信元計算機１１１及び配信先計算機１１２にネットワークＩ／Ｏ記録＆フィルタ部１４７が実装されていないため、図５のフローチャートにおけるそのステップは省略されている。
【００７１】
図１２は、スイッチ装置Ａ２１１、スイッチ装置Ｂ２１２の処理のフローチャートを示

す。パケット検査部２４１は、受信したパケットの宛先ＭＡＣアドレスを特定する（９０１）。パケット検査部２４１は、受信したパケットのＥｔｈｅｒｎｅｔヘッダ３０１における宛先ＭＡＣアドレスフィールド３０６を参照する。

【００７２】

パケット検査部２４１は、ゲートウェイ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１を参照し、宛先ＭＡＣアドレスが、ゲートウェイ計算機のＭＡＣアドレスか判定する（９０２）。パケット検査部２４１は、ゲートウェイ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１を、事前に構成ＤＢ１２２から読み込み、保持している。

【００７３】

宛先ＭＡＣアドレスが、ゲートウェイ計算機のＭＡＣアドレスである場合（９０２：ＹＥＳ）、スイッチ装置Ａ２１１／スイッチ装置Ｂ２１２は、当該パケットをゲートウェイ計算機に転送する（９０３）。宛先ＭＡＣアドレスが、ゲートウェイ計算機のＭＡＣアドレスではない場合（９０２：ＮＯ）、パケット検査部２４１は、当該パケットを破棄する（９０４）。

【００７４】

図１２の処理により、スイッチ装置Ａ２１１上で動作するパケット検査部２４１は、配信元計算機１１１からゲートウェイ計算機Ａ２１３を介して送信されるＩＰパケット以外のパケットをブロック（破棄）する。スイッチ装置Ｂ２１２上で動作するパケット検査部２１１は、配信先計算機１１２からゲートウェイ計算機Ｂ２１４を介して送信されるＩＰパケット以外のパケットをブロック（破棄）する。これにより、配信元計算機１１１及び配信先計算機１１２からの全てネットワークパケットは、ゲートウェイ計算機を通過する。

【００７５】

図１３は、ゲートウェイ計算機Ａ２１３／ゲートウェイ計算機Ｂ２１４におけるパケット転送部２４２の処理のフローチャートを示す。パケット転送部２４２は、スイッチ装置からパケットを受信すると、当該パケットの宛先ＩＰアドレスを特定する（１３０１）。パケット転送部２４２は、受信パケットのＩＰヘッダ３０２における宛先ＩＰアドレスフィールド３０８を参照する。

【００７６】

パケット転送部２４２は、転送制御テーブル２５２を参照し、該当エントリの転送先ＭＡＣアドレスを取得する（１３０２）。パケット転送部２４２は、当該パケットのＥｔｈｅｒｎｅｔヘッダ３０１の宛先ＭＡＣアドレスフィールド３０６に、上記転送先ＭＡＣアドレスを設定する（１３０３）。

【００７７】

パケット転送部２４２は、ゲートウェイ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１を参照し、転送先ＭＡＣアドレスがゲートウェイ計算機のアドレスであるか判定する（１３０４）。転送先ＭＡＣアドレスがゲートウェイ計算機である場合（１３０４：ゲートウェイ計算機）、パケット転送部２４２は、転送先に当該パケットを転送する（１３０５）。転送先ＭＡＣアドレスがゲートウェイ計算機でない場合（１３０４：他）、パケット転送部２４２は、当該パケットをネットワークＩ／Ｏ記録＆フィルタ部１４７に送信する（１３０６）。

【００７８】

図１３の処理により、ネットワークＩ／Ｏ記録装置＆フィルタ部１４７が処理するパケットを、データシールド境界を含む外部宛パケットのみに制限できる。パケット転送部２４２は、他方のゲートウェイ計算機から受信したパケットを、宛先ＩＰアドレスに従って転送する。

【００７９】

図１４は、ゲートウェイ計算機Ａ２１３／ゲートウェイ計算機Ｂ２１４におけるネットワークＩ／Ｏ記録＆フィルタ部１４７の処理のフローチャートを示す。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、パケット転送部２４２から受信したパケットのＩＰヘッダ

３０２における宛先ＩＰアドレスフィールド３０８を参照し、宛先ＩＰアドレスを特定する（１４０１）。

【００８０】

ネットワークＩ／Ｏ記録＆フィルタ部１４７は、シールド境界計算機ＩＰアドレスリスト１５３を参照し、パケットの宛先ＩＰアドレスが、シールド境界のアドレスであるか判定する（１４０２）。

【００８１】

宛先ＩＰアドレスがシールド外ＩＰアドレスである場合、つまり、宛先ＩＰアドレスがシールド境界計算機ＩＰアドレスリスト１５３に含まれない場合（１４０２：他）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、当該パケットを破棄する（１４０５）。

【００８２】

宛先ＩＰアドレスがシールド境界ＩＰアドレスである場合、つまり、宛先ＩＰアドレスがシールド境界計算機ＩＰアドレスリスト１５３に含まれる場合（１４０２：シールド境界ＩＰアドレス）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、ＴＣＰヘッダ３０３のシーケンス番号（フィールド３０９内）に基づき、パケットを再構成する（１４０３）。

【００８３】

ネットワークＩ／Ｏ記録＆フィルタ部１４７は、フィルタポリシ１５４及びＬ７ヘッダ３０４に基づき、パケットを処理する（１４０４）。ステップ１４０４は、図６を参照した説明のように、パケットフィルタリング及び不ログ記録を実行する。廃棄されないパケットは、プロキシサーバに転送される。

【実施例３】

【００８４】

以下において、実施例３を説明する。主に、実施例２との差異を説明する。本実施例において、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、ゲートウェイ計算機とは異なるフィルタ計算機に実装される。ゲートウェイ計算機や配信元／配信先計算機と異なる計算機に実装することで、それら計算機の負荷を低減できる。また。既存のネットワークシステムに用意にネットワークＩ／Ｏ記録＆フィルタ部１４７を組み込むことができる。

【００８５】

図１５は、本実施例のシステムの構成例を示す。実施例２の構成と比較して、拠点１０２のゲートウェイ計算機Ｂ２１４、スイッチ装置Ｂ２１２及びプロキシサーバ１１４が省略されている。フィルタ計算機１５１１がデータセンタ１０１において追加されている。

【００８６】

配信元計算機１１１は、スイッチ装置Ａ２１１を介して、ゲートウェイ計算機Ａ２１３に接続されている。ゲートウェイ計算機Ａ２１３とスイッチ装置Ｂ２１２とは、ＶＰＮ１０４を介して接続されている。配信先計算機１１２は、スイッチ装置Ｂ２１２を介して、ゲートウェイ計算機Ａ２１３に接続されている。フィルタ計算機１５１１は、ゲートウェイ計算機Ａ２１３及びプロキシサーバ１１３に接続されている。

【００８７】

ネットワークＩ／Ｏ記録＆フィルタ部１４７は、ゲートウェイ計算機に代えて、フィルタ計算機１５１１に実装されている。フィルタ計算機１５１１は、ＮＩＣを介して他装置に接続される。構成ＤＢ１２２は、実施例２の情報に加え、フィルタ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１を格納している。フィルタ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１は、顧客管理者により予め設定されている。

【００８８】

図１６は、フィルタ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１の構成例を示す。フィルタ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１は、フィルタ計算機１５１１のアドレスを管理する。フィルタ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１は、ＩＰアドレスカラム１６０１及びＭＡＣアドレスカラム１６０２を有する。

【００８９】

図１７は、転送制御テーブル２５２を作成するフローチャートを示す。ゲートウェイ計算機Ａ２１３は、シールド内計算機ＩＰアドレスリスト１５２に記載されている宛先ＩＰアドレス用の転送制御テーブルエントリを作成し、転送先ＩＰアドレスカラム１００２及び転送先ＭＡＣアドレスカラム１００３に、シールド内計算機のＩＰアドレス及びＭＡＣアドレスをそれぞれ設定する（１７０１）。

【００９０】

ゲートウェイ計算機Ａ２１３は、ｄｅｆａｕｌｔ用の転送制御テーブルエントリを作成し、転送先ＩＰアドレスカラム１００２及び転送先ＭＡＣアドレスカラム１００３に、フィルタ計算機１５１１のＩＰアドレス及びＭＡＣアドレスをそれぞれ設定する（１７０２）。

【００９１】

スイッチ装置Ａ２１１のパケット検査部２４１は、構成ＤＢ１１２から、ゲートウェイ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１を読み込み、配信元計算機１１１からゲートウェイ計算機Ａ２１３を介して転送されるＩＰパケット以外のパケットをブロック（破棄）する。

【００９２】

スイッチ装置Ｂ２１２のパケット検査部２４１は、構成ＤＢ１１２から、ゲートウェイ計算機ＩＰアドレス／ＭＡＣアドレスリスト２５１を読み込み、配信先計算機１１２からゲートウェイ計算機Ａ２１３を介して転送されるＩＰパケット以外のパケットをブロック（破棄）する。これにより、配信元計算機１１１及び配信先計算機１１２からの全ての生存パケットは、ゲートウェイ計算機Ａ２１３を通過する。

【００９３】

図１８は、ゲートウェイ計算機Ａ２１３におけるパケット転送部２４２の処理のフローチャートを示す。パケット転送部２４２は、パケットを受信すると、当該パケットの宛先ＩＰアドレスを特定する（１８０１）。パケット転送部２４２は、受信パケットのＩＰヘッダ３０２における宛先ＩＰアドレスフィールド３０８を参照する。

【００９４】

パケット転送部２４２は、転送制御テーブル２５２において、受信パケットのＩＰアドレスを検索する。合致するＩＰアドレスが存在する場合、パケット転送部２４２は、対応するＭＡＣアドレスを取得し（１８０２）、当該パケットのＥｔｈｅｒｎｅｔヘッダの宛先ＭＡＣアドレスフィールドに、上記転送先ＭＡＣアドレスを設定する（１８０３）。

【００９５】

合致するＩＰアドレスが存在しない場合、パケット転送部２４２は、ｄｅｆａｕｌｔのエントリから、フィルタ計算機１５１１のＭＡＣアドレスを取得し（１８０２）、当該パケットのＥｔｈｅｒｎｅｔヘッダの宛先ＭＡＣアドレスフィールドに、フィルタ計算機１５１１のＭＡＣアドレスを設定する（１８０３）。これにより、データシールド１３１の外部（シールド境界計算機を介して又は介さず）に向かうパケットのみがフィルタ計算機１５１１に転送され、フィルタ計算機１５１１の負荷を低減できる。

【００９６】

パケット転送部２４２は、設定したＭＡＣアドレスに対してパケットを転送する（１８０４）。フィルタ計算機１５１１のネットワークＩ／Ｏ記録＆フィルタ部１４７は、実施例２の図１４に示すフローチャートが示すようにパケットのフィルタリング及びログ記録を実行する。

【００９７】

なお、本例は一つのゲートウェイ計算機を示すが、実施例２のように、複数のゲートウェイ計算機に異なるフィルタ計算機が接続されてもよい。一つのフィルタ計算機が複数のゲートウェイ計算機に接続されてもよい。

【実施例４】

【００９８】

以下において、実施例４を説明する。主に、実施例１との差異を説明する。顧客管理者

は、機密情報を含むデータ領域（ｔａｉｎｔ領域）を予め設定する。ネットワークＩ／Ｏ記録＆フィルタ部は、ｔａｉｎｔ領域からのデータの転送を監視し、他の領域からのデータは監視対象から除外される。ネットワークＩ／Ｏ記録＆フィルタ部は、ｔａｉｎｔ領域からデータが読み出されると、ｔａｉｎｔ領域追跡部に追跡指示を発行する。

【００９９】

ｔａｉｎｔ領域追跡部は、データ分析部／データ分析結果確認部のメモリアクセスを追跡し、ｔａｉｎｔ領域から読み出されたデータの伝播を解析する。これにより、分析部／分析結果確認部からの情報漏洩を効率的に監視できる。

【０１００】

図１９は、本実施例のシステムの構成例を示す。実施例１の構成に加え、配信元計算機１１１及び配信先計算機１１２において、ｔａｉｎｔ領域追跡部１９４１が実装されている。ｔａｉｎｔ領域追跡部１９４１は、ｔａｉｎｔ　ｂｉｔｍａｐ１９５２を含む。ｔａｉｎｔ領域追跡部１９４１は、ＣＰＵ２２３がｔａｉｎｔ領域追跡プログラムを実行することにより実現される。構成ＤＢ１２２は、ｔａｉｎｔ領域リスト１９５１を格納する。

【０１０１】

図２０は、ｔａｉｎｔ領域リスト１９５１の構成例を示す。ｔａｉｎｔ領域リスト１９５１は、ストレージのｔａｉｎｔ領域を管理する。ｔａｉｎｔ領域リスト１９５１は、ストレージＩＰアドレスカラム２００１、開始セクタ番号カラム２００２、終了セクタ番号カラム２００３を有する。

【０１０２】

図２１は、ｔａｉｎｔ　ｂｉｔｍａｐ１９５２の構成例を示す。ｔａｉｎｔ　ｂｉｔｍａｐ１９５２は、メモリにおける領域（の格納データ）が、ｔａｉｎｔ領域（の格納データ）であるかを示す。ｔａｉｎｔ　ｂｉｔｍａｐ１９５２は、ページアドレスカラム２１０１及びｔａｉｎｔ有無ビットカラム２１０２を有する。ページは、メモリにおける管理単位領域である。

【０１０３】

図２２は、ｔａｉｎｔ領域追跡部１９４１による処理のフローチャートを示す。ｔａｉｎｔ領域追跡部１９４１は、ｔａｉｎｔ領域受信通知をネットワークＩ／Ｏ記録＆フィルタ部１４７から受信する（２２０１）。ｔａｉｎｔ領域追跡部１９４１は、当該メモリ領域をｔａｉｎｔ領域として登録するようｔａｉｎｔ　ｂｉｔｍａｐ１９５２を更新する（２２０２）。ｔａｉｎｔ領域追跡部１９４１は、Ｈｙｐｅｒｖｉｓｏｒ１４５経由で、分析部１４３／分析結果確認部１４１にパケット受信を通知する（２２０３）。

【０１０４】

図２３は、配信先計算機１１２及び配信元計算機１１１それぞれにおける処理のフローチャートを示す。分析部１４３／分析結果確認部１４１は、Ｈｙｐｅｒｖｉｓｏｒ１４５に命令実行要求を発行する（２３０１）。Ｈｙｐｅｒｖｉｓｏｒ１４５は、ｔａｉｎｔ領域追跡部１９４１に命令実行通知を発行する（２３０２）。

【０１０５】

ｔａｉｎｔ領域追跡部１９４１は、命令解析を実行する（２３０３）。ｔａｉｎｔ領域から読んだデータのメモリｗｒｉｔｅ発生している場合（２３０４：ＹＥＳ）、ｔａｉｎｔ領域追跡部１９４１は、当該メモリ領域をｔａｉｎｔ領域として登録するよう、ｔａｉｎｔ　ｂｉｔｍａｐ１９５２を更新する（２３０５）。これにより、ｔａｉｎｔ領域を追跡できる。ｔａｉｎｔ領域から読んだデータのメモリｗｒｉｔｅ発生していない場合（２３０４：ＮＯ）、ステップ２３０５はスキップされる。

【０１０６】

ｔａｉｎｔ領域以外から読んだデータのメモリｗｒｉｔｅ発生している場合（２３０６：ＹＥＳ）、ｔａｉｎｔ領域追跡部１９４１は、当該メモリ領域をｔａｉｎｔ領域から削除するようｔａｉｎｔ　ｂｉｔｍａｐ１９５２を更新する（２３０７）。ｔａｉｎｔ領域以外から読んだデータのメモリｗｒｉｔｅ発生していない場合（２３０６：ＮＯ）、ステップ２３０７はスキップされる。

【０１０７】
ｔａｉｎｔ領域追跡部１９４１は、Ｈｙｐｅｒｖｉｓｏｒ１４５に再開要求を発行し、Ｈｙｐｅｒｖｉｓｏｒ１４５は、分析部１４３／分析結果確認部１４１を再開する（２３０８）。
【０１０８】
図２４は、ネットワークＩ／Ｏ記録＆フィルタ部１４７による受信パケットの処理のフローチャートを示す。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、ＮＩＣ経由でパケットを受信する（２４０１）。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、受信したパケットが、ストレージＩ／Ｏによるパケットであるか判定する（２４０２）。パケットの送信元ＩＰアドレスフィールド３０７の値と一致するＩＰアドレスがｔａｉｎｔ領域リスト１９５１に存在する場合、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、受信したパケットが、ストレージＩ／Ｏによるパケットであると判定する。
【０１０９】
パケットが、ストレージＩ／Ｏによるパケットである場合（２４０２：ＹＥＳ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、パケットにおいてデータが読み出されたセクタを同定し、ｔａｉｎｔ領域リスト１９５１を参照して、当該セクタがｔａｉｎｔ領域であるか判定する（２４０３）。
【０１１０】
当該セクタがｔａｉｎｔ領域である場合（２４０３：ＹＥＳ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、受信メモリ領域をｔａｉｎｔ領域に登録するよう、ｔａｉｎｔ領域追跡部１９４１にｔａｉｎｔ領域受信通知を発行する（２４０４）。これにより、ｔａｉｎｔ領域が追跡される。当該セクタがｔａｉｎｔ領域でない場合（２４０３：他）、ステップ２４０４はスキップされる。
【０１１１】
パケットが、ストレージＩ／Ｏによるパケットではない場合（２４０２：ＮＯ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、受信パケットのＩＰヘッダ３０２がｔａｉｎｔマークを含むか判定する（２４０５）。
【０１１２】
ＩＰヘッダ３０２がｔａｉｎｔマークを含む場合（２４０５：ＹＥＳ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、受信メモリ領域をｔａｉｎｔ領域に登録するよう、ｔａｉｎｔ領域追跡部１９４１にｔａｉｎｔ領域受信通知を発行する（２４０６）。ｔａｉｎｔマークにより、ノード間でｔａｉｎｔ領域のデータを追跡できる。ＩＰヘッダ３０２がｔａｉｎｔマークを含まない場合（２４０５：ＮＯ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、Ｈｙｐｅｒｖｉｓｏｒ１４５経由で、分析部１４３／分析結果確認部１４１にパケット受信を通知する（２４０７）。
【０１１３】
図２５は、ネットワークＩ／Ｏ記録＆フィルタ部１４７による送信パケットの処理のフローチャートを示す。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、ｔａｉｎｔ領域追跡部１９４１よりｔａｉｎｔ領域送信通知を受信する（２５０１）。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、ｔａｉｎｔ領域のデータについて以下のステップを実行する。
【０１１４】
ネットワークＩ／Ｏ記録＆フィルタ部１４７は、当該パケットのＩＰヘッダ３０２の宛先ＩＰアドレスフィールド３０８を参照し、宛先ＩＰアドレスを特定する（２５０２）。宛先がシールド境界計算機である場合、つまり、宛先ＩＰアドレスがシールド境界計算機ＩＰアドレスリスト１５３に存在する場合（２５０３：シールド境界サーバ）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、フィルタポリシ１５４及びパケット種別に基づいて、パケットを処理する（２５０４）。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、読みされたデータのファイル情報を復元し、Ｉ／Ｏログに含める。
【０１１５】

宛先がシールド内計算機である場合、つまり、宛先ＩＰアドレスがシールド内計算機ＩＰアドレスリスト１５２に存在する場合（２５０３：シールド内計算機）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、当該パケットのＩＰヘッダ３０２にｔａｉｎｔマークを設定してＮＩＣ経由で送信する（２５０５）。

【０１１６】

宛先が、シールド境界外アドレスである、つまり、シールド境界計算機でも、シールド境界内計算機でもない場合（２５０３：他）、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、当該パケットを破棄する（２５０６）。

【０１１７】

上述のように、ネットワークＩ／Ｏ記録＆フィルタ部１４７は、宛先がシールド内計算機であり、かつ、ｔａｉｎｔ領域からのネットワークパケット（ネットワークＩ／Ｏ）を検出すると、当該ネットワークパケットにｔａｉｎｔマークを設定する。また。ネットワークＩ／Ｏ記録＆フィルタ部１４７は、ｔａｉｎｔマークが設定されたネットワークパケット受信を検出すると、ｔａｉｎｔ領域追跡部にｔａｉｎｔ領域受信通知（追跡指示）を発行する。これにより、ｔａｉｎｔ領域追跡処理が、他ノードに承継される。

【０１１８】

ネットワークＩ／Ｏ記録＆フィルタ部１４７は、宛先がシールド境界計算機であり、かつ、ｔａｉｎｔ領域からのネットワークパケット（ネットワークＩ／Ｏ）を検出すると、パケットに対するフィルタリング及びログ記録（監視処理）を実行する。ｔａｉｎｔ領域からシールド境界計算機へのネットワークＩ／Ｏ以外のパケットの解析及びログ出力が不要であり、負荷を低減することができる。

【０１１９】

なお、本発明は上記した実施例に限定されるものではなく、様々な変形例が含まれる。例えば、上記した実施例は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明したすべての構成を備えるものに限定されるものではない。また、ある実施例の構成の一部を他の実施例の構成に置き換えることが可能であり、また、ある実施例の構成に他の実施例の構成を加えることも可能である。また、各実施例の構成の一部について、他の構成の追加・削除・置換をすることが可能である。

【０１２０】

また、上記の各構成・機能・処理部等は、それらの一部又は全部を、例えば集積回路で設計する等によりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロセッサがそれぞれの機能を実現するプログラムを解釈し、実行することによりソフトウェアで実現してもよい。各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリや、ハードディスク、ＳＳＤ（Ｓｏｌｉｄ　Ｓｔａｔｅ　Ｄｒｉｖｅ）等の記録装置、または、ＩＣカード、ＳＤカード等の記録媒体に置くことができる。

【０１２１】

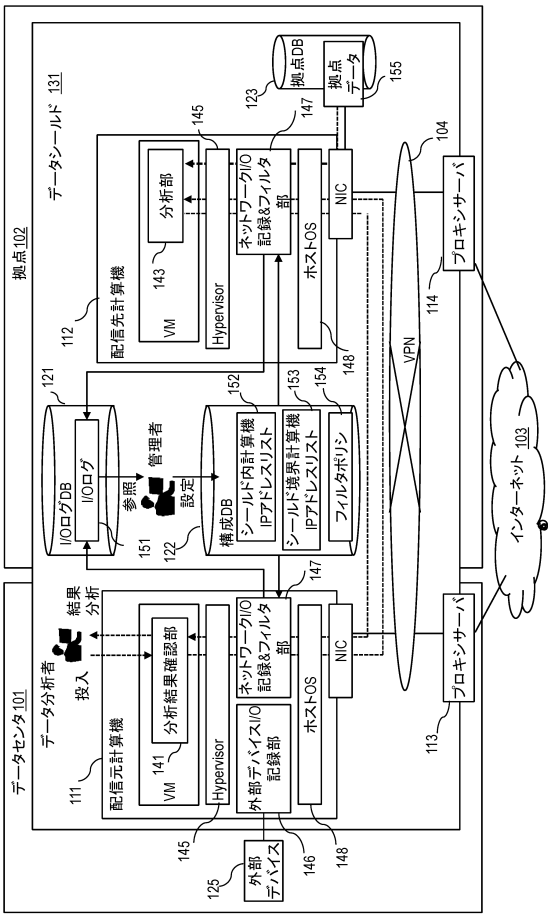
また、制御線や情報線は説明上必要と考えられるものを示しており、製品上必ずしもすべての制御線や情報線を示しているとは限らない。実際には殆どすべての構成が相互に接続されていると考えてもよい。

【符号の説明】

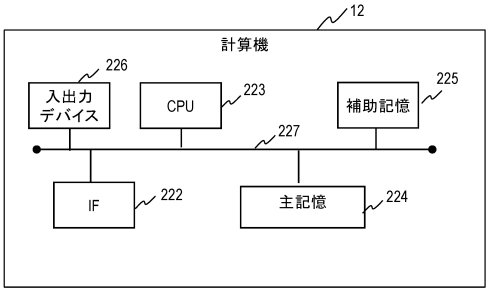
【０１２２】

１０１　データセンタ、１０２　拠点、１０３　インターネット、１０４　ネットワーク、１１１　配信元計算機、１１２　配信先計算機、１１３、１１４　プロキシサーバ、１２５　外部記憶デバイス、１３１　データシールド、１４１　分析結果確認部、１４３　分析部、１４６　外部デバイスＩ／Ｏ記録部、１４７　ネットワークＩ／Ｏ記録＆フィルタ部、１５１　Ｉ／Ｏログ、１５２　シールド内計算機ＩＰアドレスリスト、１５３　シールド境界計算機ＩＰアドレスリスト、１５４　フィルタポリシ、１５５　拠点データ、２１１、２１２　スイッチ装置、２１３、２１４　ゲートウェイ計算機、２２３　ＣＰＵ、２２４　主記憶、２２５　補助記憶、２２６　入出力デバイス、２４１　パケット検査部、２４２　パケット転送部、１５１１　フィルタ計算機

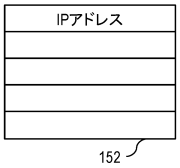
【図１Ａ】



【図１Ｂ】

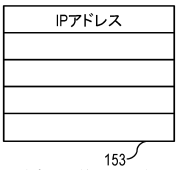


【図２Ａ】



シールド内計算機IPアドレスリスト

【図２Ｂ】



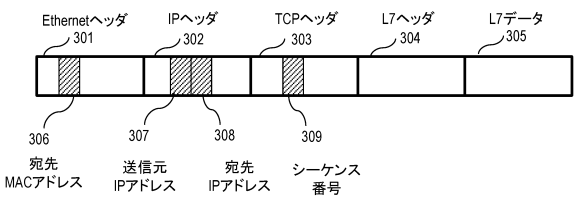
シールド境界計算機IPアドレスリスト

【図２Ｃ】

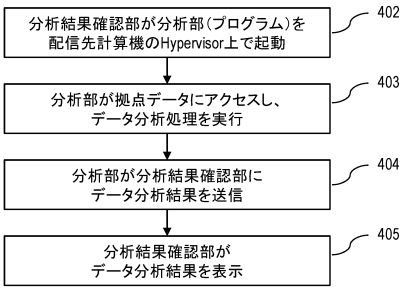
203 プロトコル	204 read	205 write	206 action
CIFS	許可	禁止	discard
FTP	禁止	禁止	log
SMTP	許可	許可	nop
HTTP	許可	禁止	discard+log
…	…	…	…

フィルタポリシ 154

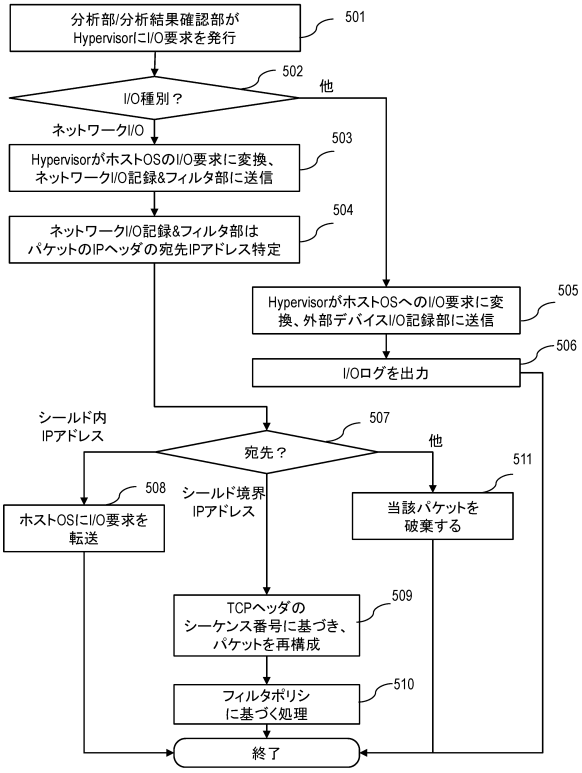
【図３】



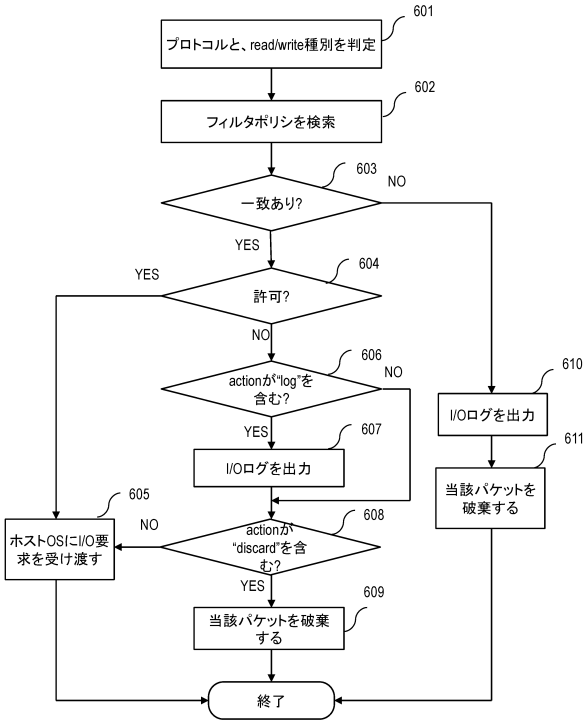
【図４】



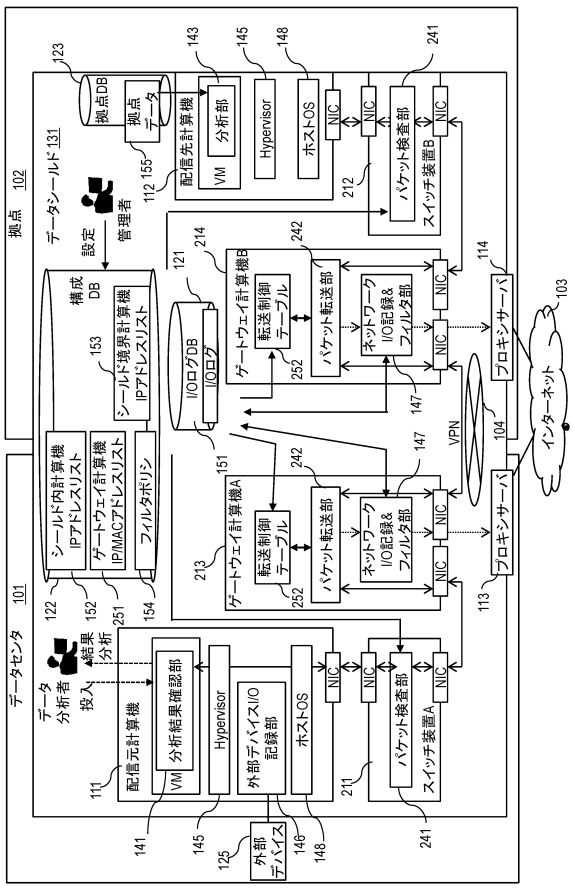
【図５】



【図６】



【図７】



【図８】

1001 宛先IPアドレス	1002 転送先IPアドレス	1003 転送先MACアドレス
1.2.3.4	3.4.5.6	00:11:22:33:44:55
2.3.4.5	3.4.5.7	11:22:33:44:55
default	3.4.5.8	22:33:44:55:66

転送制御テーブル 252

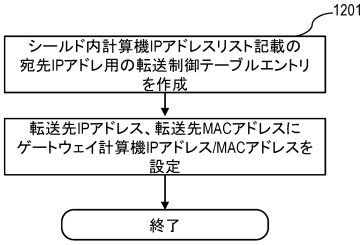
【図９】

1101 IPアドレス	1102 MACアドレス

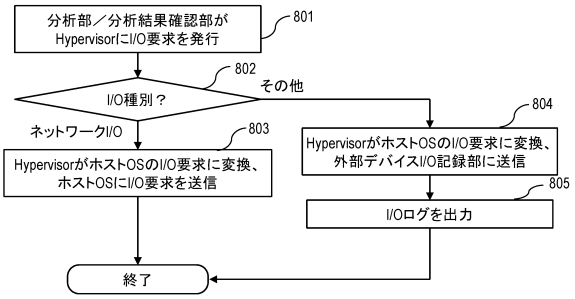
251

ゲートウェイ計算機IPアドレス/MACアドレスリスト

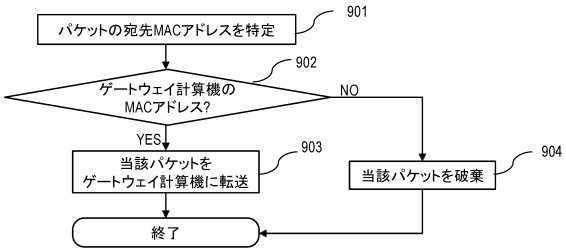
【図１０】



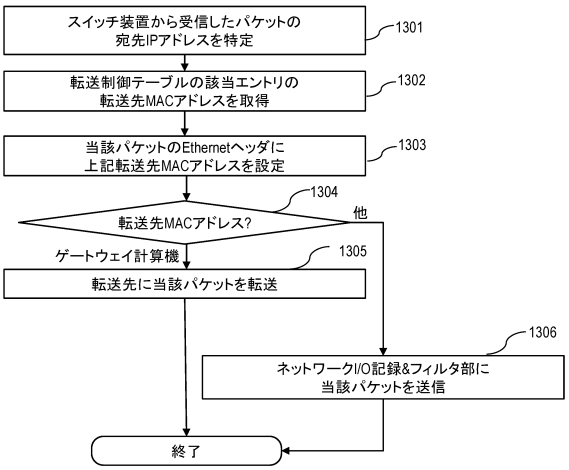
【図１１】



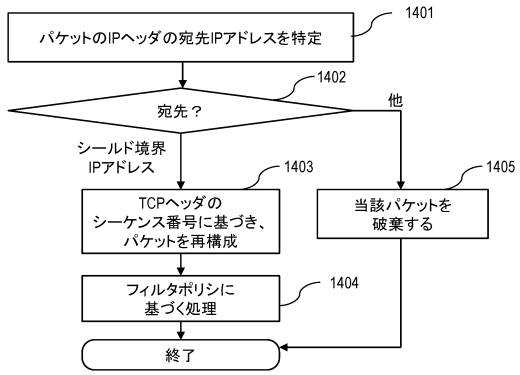
【図１２】



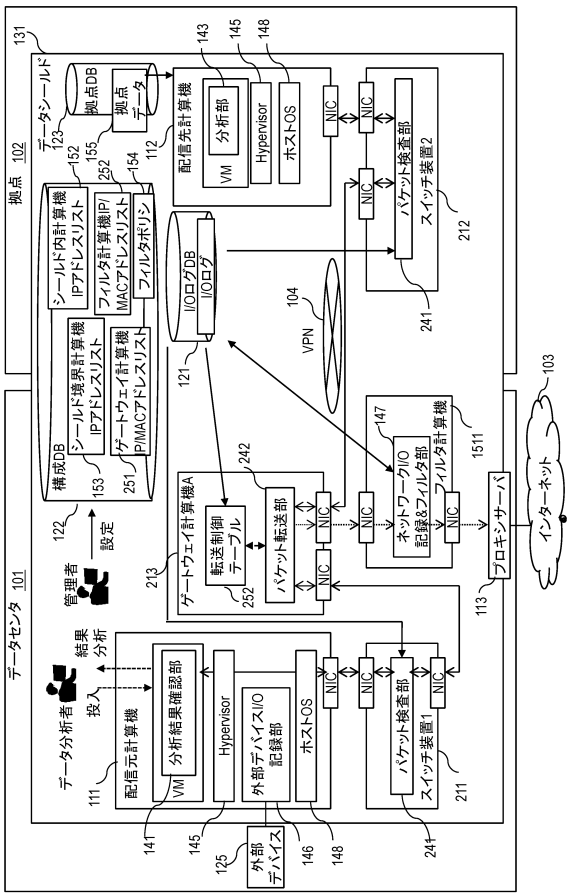
【図１３】



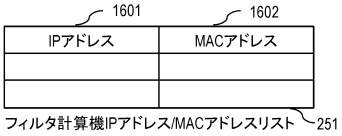
【図１４】



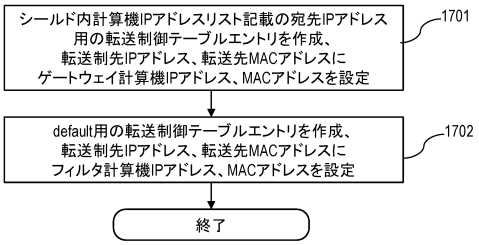
【図１５】



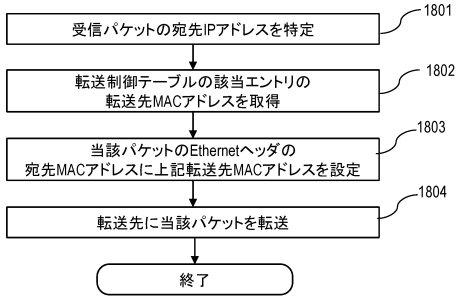
【図１６】



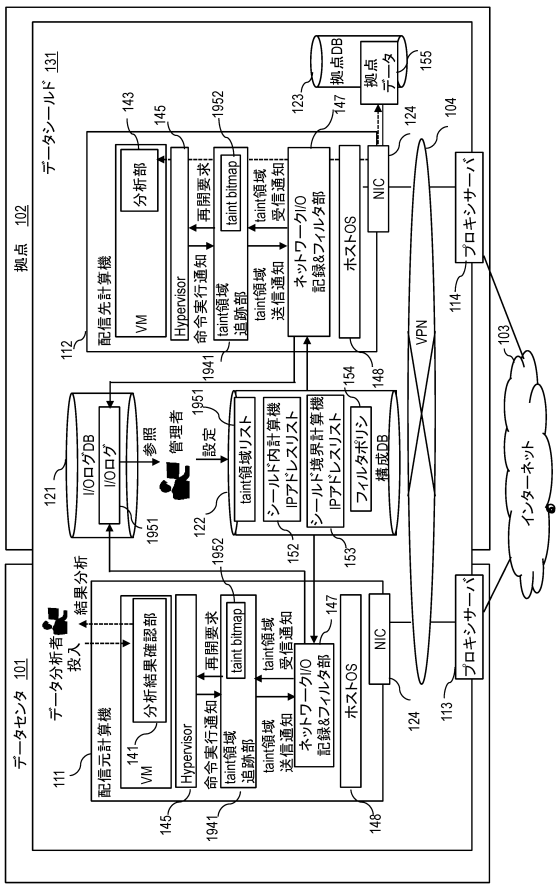
【図１７】



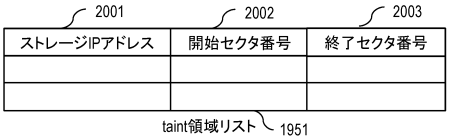
【図１８】



【図１９】

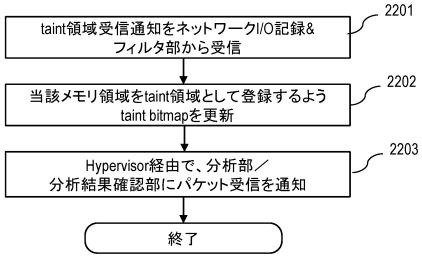


【図２０】

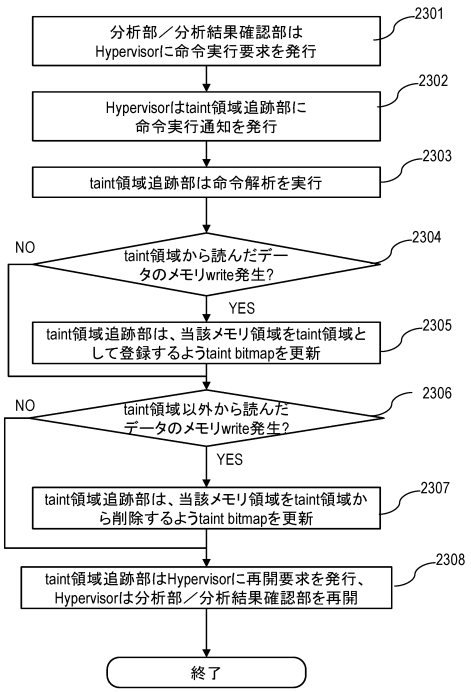


【図２１】

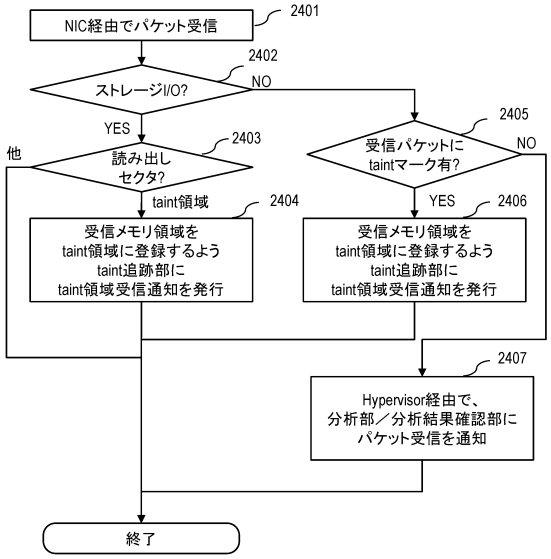
【図２２】



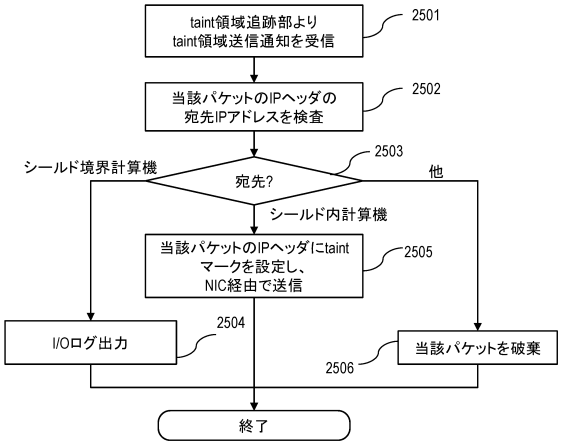
【図２３】



【図２４】


NIC経由でパケット受信
2401
ストレージI/O?
2402
NO
YES
読み出し
セクタ?
2403
他
taint領域
受信メモリ領域を
taint領域に登録するよう
taint追跡部に
taint領域受信通知を発行
2404
受信パケットに
taintマーク有?
2405
NO
YES
2406
受信メモリ領域を
taint領域に登録するよう
taint追跡部に
taint領域受信通知を発行
Hypervisor経由で、
分析部／分析結果確認部に
パケット受信を通知
2407
終了

【図２５】


taint領域追跡部より
taint領域送信通知を受信
2501
当該パケットのIPヘッダの
宛先IPアドレスを検査
2502
シールド境界計算機
宛先?
2503
他
シールド内計算機
当該パケットのIPヘッダにtaint
マークを設定し、
NIC経由で送信
2505
I/Oログ出力
2504
当該パケットを破棄
2506
終了

フロントページの続き

(56)参考文献 特開２００７－０９６６６６（ＪＰ，Ａ）
特開２０１４－０２７６０２（ＪＰ，Ａ）
特開２００７－１０４５０９（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　１２／２８
Ｈ０４Ｌ　１２／６６
Ｈ０４Ｌ　１２／７０