(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6138367号
(P6138367)
(45)発行日　平成29年5月31日(2017.5.31)　(24)登録日　平成29年5月12日(2017.5.12)

(51)Int.Cl.　F I
G06Q 10/00 (2012.01)　G06Q 10/00 ZIT

請求項の数 4 (全 8 頁)

(21)出願番号　特願2016-524945(P2016-524945)
(86)(22)出願日　平成26年6月3日(2014.6.3)
(86)国際出願番号　PCT/JP2014/002955
(87)国際公開番号　WO2015/186155
(87)国際公開日　平成27年12月10日(2015.12.10)
審査請求日　平成28年3月31日(2016.3.31)

(73)特許権者　000006013
三菱電機株式会社
東京都千代田区丸の内二丁目７番３号
(74)代理人　100099461
弁理士　溝井　章司
(74)代理人　100176728
弁理士　北村　慎吾
(72)発明者　松田　規
日本国東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　平野　貴人
日本国東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

最終頁に続く

(54)【発明の名称】ログ分析装置、及びログ分析方法

(57)【特許請求の範囲】
【請求項１】
物理的な施設管理機器のログである物理系ログとユーザの操作により情報処理を実行する情報機器のログである情報系ログとを収集するログ収集部と、
前記物理系ログと前記情報系ログとの時間間隔の頻度分布を計算し、この頻度分布を前記情報機器が正常な状態で計算した頻度分布と比較して前記情報機器の異常を検知するログ分析部と
を備えたログ分析装置。
【請求項２】
前記ログ収集部が収集した前記物理系ログと前記情報系ログとを格納するログデータベースを備え、
前記ログ分析部は、前記ログデータベースから第１の期間と第２の期間に発生した前記物理系ログと前記情報系ログとを抽出し、前記第１の期間の前記物理系ログと前記情報系ログとの時間間隔の第１の頻度分布と、前記第２の期間の前記物理系ログと前記情報系ログとの時間間隔の第２の頻度分布との時間軸方向のずれτを計算し、このずれτが、前記情報機器が正常な状態で計算した前記第１の頻度分布と前記第２の頻度分布との時間軸方向のずれＴより大きい場合に前記情報機器の異常を検知する請求項１記載のログ分析装置。
【請求項３】
前記ログ分析部が前記情報機器の異常を検知した場合、警告を生成して管理者に通知する

アラート生成部を備えた請求項１または請求項２記載のログ分析装置。
【請求項４】
ログを分析して情報機器の異常を検知するログ分析装置のログ分析方法であって、
ログ収集部が、物理的な施設管理機器のログである物理系ログとユーザの操作により情報処理を実行する情報機器のログである情報系ログとを収集するログ収集ステップと、
ログ分析部が、前記物理系ログと前記情報系ログとの時間間隔の頻度分布を計算し、この頻度分布を前記情報機器が正常な状態で計算した頻度分布と比較して前記情報機器の異常を検知するログ分析ステップと
を備えたログ分析方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、マルウェア感染の検知や組織内部の不正行為の発見を行なうログ分析装置に関する。
【背景技術】
【０００２】
従来の物理系・情報系統合ログ分析装置は、ビルの入退室に関するログ（物理系ログ）と、ＰＣの操作履歴やプロキシなどのＷｅｂアクセス履歴のログ（情報系ログ）を、統合して分析することで、不正利用を検知していた。例えば、ある社員Ａが居室から退室したログが出力された後に、ファイルサーバ上の機密情報の読み込みのログが出力されていた場合、他人が社員Ａになりすまして機密情報を盗み見ていた可能性を検知することができる（例えば、特許文献１）。
【０００３】
また、利用者の操作が事前に設定された許容範囲からずれているときに異常を検知する仕組みも提案されている。企業内では様々な業務を行なっている人がいるため、全員を包括するような許容範囲を設定してしまうと、異常が起こっても検知できなくなってしまうという課題に対して、個人の業務の傾向を掴んで許容範囲をいくつかのパターンから選択することで、異常の検知可能性を向上させている（例えば、特許文献２）。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００７－２３３６６１号公報
【特許文献２】特開２０１０－２１１２５７号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
従来の物理系・情報系統合ログ分析装置は、実際のイベントを時系列に並べて社員の行動を把握することができていたが、具体的にどのようなルールでどのような不正を検知するかまでは開示されていなかった（例えば、特許文献１）。
【０００６】
一般的には、物理系と情報系のログを統合分析することで、居室から退室して再度入室するまでの間に行なわれた操作のログを監視することで不正を見つけることができると言われているが、例えば、社員が自席を離席して居室から退室する間に行なわれる不正の検知方法は知られていない。
【０００７】
また、利用者の操作が、事前に設定された許容範囲からずれているときに異常を検知する仕組みの場合、人間の操作時間や操作間隔などは、時期や急ぎ度合いなどによって多少なりともずれが生ずることから、異常検知のためのしきい値（許容範囲）を大きな値とする必要がある。そのため、例えば、人が操作をやめたら活動を中止するようなマルウェアに感染した場合、その感染を検知することは非常に困難であった（例えば、特許文献２）

。
【０００８】
この発明は上記のような問題点を解決するためになされたもので、人が操作をやめたら活動を中止するようなマルウェアに感染した場合でも、その感染を検知する可能性を向上させることを目的とする。
【課題を解決するための手段】
【０００９】
上記で述べた課題を解決するため、本発明のログ分析装置は、物理的な施設管理機器のログである物理系ログとユーザの操作により情報処理を実行する情報機器のログである情報系ログとを収集するログ収集部と、前記物理系ログと前記情報系ログとの時間間隔の頻度分布を計算し、この頻度分布を前記情報機器が正常な状態で計算した頻度分布と比較して前記情報機器の異常を検知するログ分析部とを備える。
【００１０】
また、本発明のログ分析方法は、ログを分析して情報機器の異常を検知するログ分析装置のログ分析方法であって、ログ収集部が、物理的な施設管理機器のログである物理系ログとユーザの操作により情報処理を実行する情報機器のログである情報系ログとを収集するログ収集ステップと、ログ分析部が、前記物理系ログと前記情報系ログとの時間間隔の頻度分布を計算し、この頻度分布を前記情報機器が正常な状態で計算した頻度分布と比較して前記情報機器の異常を検知するログ分析ステップとを備える。
【発明の効果】
【００１１】
本発明によれば、物理系ログと情報系ログを統合分析し、かつ、過去のログ間隔と、現在のログ間隔とを比較して、そのずれを分析することにより、従来のように退室している時に行なわれた不正だけでなく、退室前の異常に関しても検知することができるという効果がある。
【図面の簡単な説明】
【００１２】
【図１】実施の形態１に係るログ分析装置の一構成例を示す構成図である。
【図２】物理系ログの一つである入退室ログの一例を示す図である。
【図３】情報系ログの一つであるファイルサーバのアクセスログの一例を示す図である。
【図４】実施の形態１に係るログ分析装置のログ分析処理の流れを示すフローチャートである。
【図５】ログ分析結果のグラフ化の一例を示す図である。
【発明を実施するための形態】
【００１３】
実施の形態１.
図１は、実施の形態１に係るログ分析装置の一構成例を示す構成図である。
図１において、居室１００は、普段、ユーザが端末１０１を用いて業務を行なう場所である。居室１００は、セキュリティゲート制御装置１０２によって制御されたセキュリティゲート１０３を通してのみ、入退室ができるものとする。また、入退室できるユーザも制限されているものとする。端末１０１は、居室１００の中に設置され、ユーザが情報処理業務を行なうために設置された機器であり、信号入出力部１０４、演算部１０５、メモリ１０６を内蔵している。また、端末１０１には、ユーザが端末に入出力するためのデバイスの基本構成として、キーボード１０７、マウス１０８、モニタ１０９が接続されている。
【００１４】
また、端末１０１はネットワーク１１０に接続されており、ネットワーク１１０を通じて、ネットワーク１１０に接続された他の機器と通信を行なうことができる。ネットワーク１１０に接続された他の機器とは、例えば、ファイルサーバ１１１、認証サーバ１１２、メールサーバ１１３、プロキシ１１４、ファイアウォール１１５などがある。また、イ

ンターネット１１６上のサーバとの通信には、メールサーバ１１３を介したメールの送受信、プロキシ１１４を介したＷｅｂ通信、ＦＴＰ（Ｆｉｌｅ　Ｔｒａｎｃｅｆｅｒ　Ｐｒｏｔｏｃｏｌ）などがある。

【００１５】

ログ分析装置１１７は、ファイルサーバ１１１や認証サーバ１１２と同様、組織内部のネットワーク１１０に接続されているものとする。ログ分析装置１１７は、ログ収集部１１８により、ネットワークに接続された端末１０１のログや、ファイルサーバ１１１、認証サーバ１１２、メールサーバ１１３、プロキシ１１４、ファイアウォール１１５といった情報処理に関わる機器に加え、セキュリティゲート制御装置１０２のような、例えば居室１００へのユーザの入室や退室といった物理的な施設管理に関わるログも収集し、ログデータベース１１９に蓄積しているものとする。ログ分析部１２０は、ログデータベース１１９に蓄積されたログを、キーワードを基にした検索、ログの集計などの統計的な分析、予め定められたルールに一致するかどうかに基づいた分析などを行なう。ログ分析部１２０で、セキュリティ侵害や故障など、管理者に通知して対処が必要な事象が検知された場合には、アラート生成部１２１によってアラート（警告）が生成され、管理者に通知される。

【００１６】

次に、ログデータベース１１９に保管されるログについて説明する。

図２は、物理系ログの一つである入退室ログの一例を示す図である。

図３は、情報系ログの一つであるファイルサーバのアクセスログの一例を示す図である。

【００１７】

始めに、図２について説明する。これは、物理系ログの一つである入退室ログである。入退室ログは、例えば、日付、時刻、ユーザＩＤ、イベントから構成される。日付は入退室を行なった日付、時刻は入退室を行なった時刻、ユーザＩＤは入退室を行なった社員のＩＤ、イベントは入室や退室などの事象を表す。図２の例では、２０１４年４月１日１２時２分２０秒にユーザＡが退室した、というような入退室の履歴がログとして保管される。

【００１８】

次に、図３について説明する。これは、情報系ログの一つであるファイルサーバのアクセスログである。アクセスログは、例えば、日付、時刻、ユーザＩＤ、ファイル、操作から構成される。日付はファイル操作を行なった日付、時刻はファイル操作を行なった時刻、ユーザＩＤはファイル操作を行なった社員のＩＤ、ファイルはアクセスされたファイル名、操作はファイルに対して何を行なったかという操作、を表す。図３の例では、２０１４年４月１日１２時２分０秒にユーザＡが「提案書．ｄｏｃ」というファイルの読み込みを行なった、というようなファイルアクセスの履歴がログとして保管される。

【００１９】

次に、ログ分析装置の動作について説明する。

図４は、実施の形態１に係るログ分析装置のログ分析処理の流れを示すフローチャートである。

【００２０】

始めに、ステップＳ１０１において、ログ分析部１２０は、ログデータベース１１９に保管してある物理系ログと情報系ログから、分析対象とするログを抽出する。例えば、ユーザＡが退室する間際のファイル読み込みについて分析を行ないたい場合、図２で示した入退室ログからはユーザＡの退室イベントに関するログを抽出し、図３で示したファイルアクセスログからはユーザＡによる読み込み操作が行なわれたログを抽出する。

【００２１】

次に、ステップＳ１０２において、ログ分析部１２０は、ステップＳ１０１により抽出したログから、期間ごとに、分析に必要なログレコード同士の時間間隔を計算し、発生頻度ごとにグラフ化するなどの統計処理を行なう。例えば、ユーザＡが退室直前にファイル

読み込みを行なった場合を見つけ、その時間間隔を計測する場合、図２と図３で示したログの突き合わせを行ない、２０１４年４月１日１２時２分２０秒の退室直前のファイルアクセスは１２時２分０秒であることを見つけ、時間間隔２０秒であることがわかる。これを全ての退室イベントについて実施し、更に月ごとなどでグラフ化を行なう。その結果が、図５の（ａ）や（ｂ）のグラフである。

【００２２】

次に、ステップＳ１０３において、ログ分析部１２０は、ステップＳ１０２で統計処理した結果のグラフを比較して、両者のずれを検証する。例えば、図５（ｃ）に記載のように、両者のグラフを重ねて時間軸方向のずれτを計算する。これは、例えば（ａ）のグラフを固定した状態で、（ｂ）のグラフを時間軸方向に少しずらしてみて、（ａ）のグラフとの差が最小になるような時間軸のずれτを探す。このずれτを探す方法としては、下記の数１に示すように、単純に２乗距離が最小になるずれτを見つける方法などがある。

【００２３】

【数１】

$$\tau : \min \Sigma (a(t) - b(t+\tau))^2$$

【００２４】

次に、ステップＳ１０４において、ログ分析部１２０は、ステップＳ１０３で計算したずれτがしきい値Ｔよりも大きいか否かを検証する。このしきい値Ｔは、マルウェアに感染していない正常時におけるずれτの値から、事前に決定したパラメータである。このしきい値Ｔよりも、人間が操作をやめてからマルウェアが活動を停止するまでの時間、すなわちステップＳ１０３で計算したずれτが大きい場合、異常を検知することができる。異常を検知した場合は、ステップＳ１０５に処理が進み、異常を検知しなかった場合は、処理が終了する。

【００２５】

最後に、ステップＳ４０５において、アラート生成部１２１は、ステップＳ１０４で異常を検知した場合、管理者に対して警告を提示する。

【００２６】

以上のように、本実施の形態１の発明では、物理系ログと情報系ログを統合分析し、かつ、過去のログ間隔と、現在のログ間隔とを比較して、そのずれを分析することにより、従来のように退室している時に行なわれた不正だけでなく、退室前の異常に関しても検知することができる。例えば、マルウェアに感染した場合など、ログ間隔に数百ミリ秒や数秒のずれが生ずることが予想されるが、そのずれを検知することによって、マルウェア感染の検知や内部不正の発見を行なうことができる。

【００２７】

また、本発明は、期間ごとにログ間隔の統計をとった後に、統計量のずれの算出を行なっているため、個々のログ間隔のばらつきの影響を受けにくい。一般には、人の操作の間隔は数秒や十数秒といった単位でずれることが予想される。そのため、個々のログ間隔を見てずれを評価する場合は、大きなしきい値Ｔを使って判定を行なう必要が生ずる。しかし、本発明は、個々のログ間隔で評価するのではなく、全体的な分布傾向のずれを使って分析するため、小さなしきい値Ｔを使って異常の検知が可能となり、マルウェア感染などの異常を検知できる可能性が向上する。

【００２８】

なお、ステップＳ１０３では、分布のずれの評価尺度として、一般的に使われる２乗距離を使ったが、例えば、頻度のピークのずれを使っても良いし、アースムーバー距離等の別の距離を使ってずれを判定してもよい。また、カルバック・ライブラー情報量やジェンセン・シャノン情報量などを使って、分布のずれを評価してもよい。

【００２９】

また、ステップＳ１０１やステップＳ１０２では、ファイル読み込み操作について分析

する例を示したが、ファイル書き込みやＷｅｂアクセスなどの操作を使ってログ間隔を分析しても良い。また、特定の操作に限定して分析する必要もなく、退室前に行なわれた何らかの操作を元にログ間隔を算出してもよい。

【００３０】

また、本実施の形態１では、情報系ログとしてファイルアクセスのログを用いたが、Ｗｅｂアクセスのログや、メール送受信のログや、認証のログや、ＰＣ（端末）操作のログなど、どのようなログを使って分析してもよい。

【００３１】

また、本実施の形態１では、入退室のログのうち退室イベントに関するログを使った分析を示したが、入室に関するイベントを使ってログ分析を行なっても良い。これは例えば、ＰＣ（端末）が置かれた居室から、居室に隣接して設置されている実験室に移動した場合、実験室の入室イベントを検知することで端末操作をやめていることが判別できるからである。

【００３２】

また、本実施の形態１では、物理系ログとして入退室のログを用いたが、ＰＣ（端末）を操作していないことが分かれば良いので、例えば、監視カメラによる離席やＰＣ（端末）操作終了の検知ログ、ＲＦ－ＩＤなどのセンサを用いた離席やＰＣ（端末）操作終了の検知ログ、照明のＯｎ／Ｏｆｆの検知ログなど、どのようなログを使って分析してもよい。

【００３３】

また、ステップＳ１０２では、ログを月単位で集計する例を示したが、月単位に制約する必要はなく、週単位や日単位などで集計を行なっても良い。本発明は、集計する単位には依存しない。

【００３４】

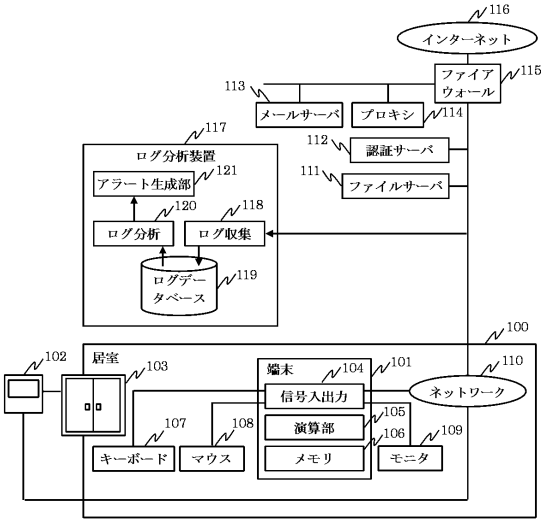
また、ステップＳ１０２では、ログが秒単位で出力されていたので秒単位で頻度グラフを作ることを暗に想定していたが、秒単位ではなく２秒単位や５秒単位や１分単位などに丸めてグラフを作るようにしてもよい。

【符号の説明】

【００３５】

１００　居室、１０１　端末、１０２　セキュリティゲート制御装置、１０３　セキュリティゲート、１０４　信号入出力部、１０５　演算部、１０６　メモリ、１０７　キーボード、１０８　マウス、１０９　モニタ、１１０　ネットワーク、１１１　ファイルサーバ、１１２　認証サーバ、１１３　メールサーバ、１１４　プロキシ、１１５　ファイアウォール、１１６　インターネット、１１７　ログ分析装置、１１８　ログ収集部、１１９　ログデータベース、１２０　ログ分析部、１２１　アラート生成部。

【図１】



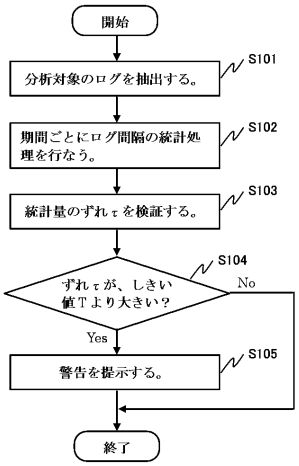
【図２】

日付	時刻	ユーザ ID	イベント
2014/4/1	12:02:20	ユーザ A	退室
2014/4/1	12:55:30	ユーザ A	入室
2014/4/1	14:57:00	ユーザ A	退室
2014/4/1	16:34:15	ユーザ A	入室

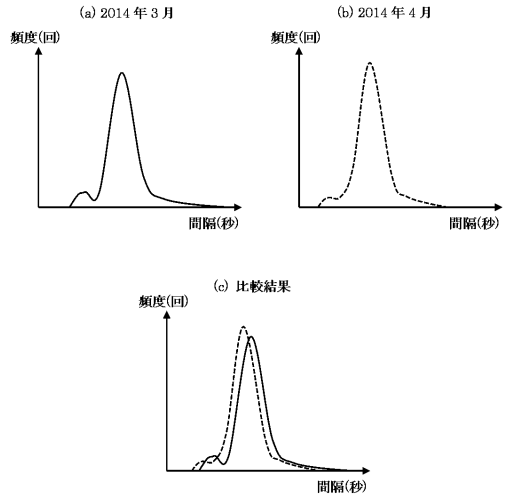
【図３】

日付	時刻	ユーザ ID	ファイル	操作
2014/4/1	12:02:00	ユーザ A	提案書.doc	読み込み
2014/4/1	12:55:45	ユーザ A	提案書.doc	読み込み
2014/4/1	14:56:45	ユーザ A	提案書.doc	書き込み
2014/4/1	16:34:30	ユーザ A	提案書.doc	読み込み

【図４】



【図５】



フロントページの続き

(72)発明者　北澤　繁樹
日本国東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内
(72)発明者　米田　健
日本国東京都千代田区丸の内二丁目７番３号　三菱電機株式会社内

審査官　大野　朋也

(56)参考文献　特開２００７－２３３６６１（ＪＰ，Ａ）
特開２００５－２３６８６３（ＪＰ，Ａ）
ログの一元管理でセキュリティリスクを統合管理　内部統制向けのセキュリティ対策を支援，保存版　ＰＲ別冊　セキュリティ総覧２００７　情報資産を守る製品選びの決定版，日本，日経ＢＰ社，２００７年　7月１９日，p.39

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｇ０６Ｑ　１０／００－９９／００