(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2019-21094
(P2019-21094A)
(43)公開日　平成31年2月7日(2019.2.7)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/55	(2013.01)	G06F	21/55	
G06F 21/31	(2013.01)	G06F	21/55	320
G06F 16/00	(2019.01)	G06F	21/31	
		G06F	17/30	350C

審査請求 未請求　請求項の数 12　ＯＬ　（全 26 頁）

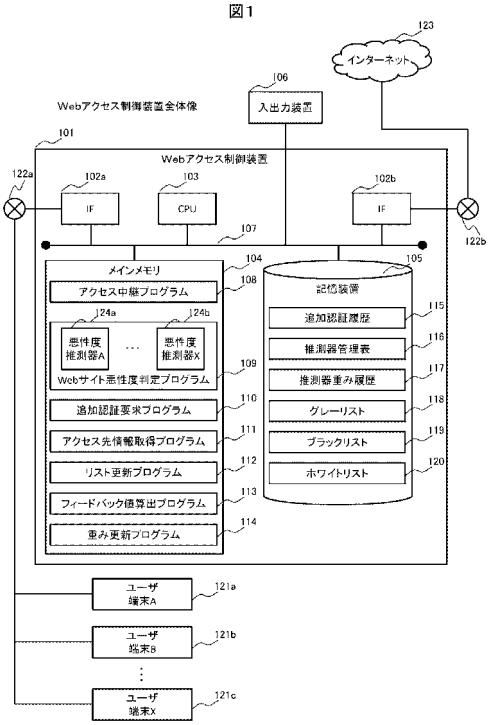
(21)出願番号　特願2017-139751 (P2017-139751)
(22)出願日　平成29年7月19日 (2017.7.19)

(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　110001689
青稜特許業務法人
(72)発明者　藤井　翔太
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　鬼頭　哲郎
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　藤井　康広
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

(54)【発明の名称】Ｗｅｂアクセス制御装置

(57)【要約】
【課題】Ｗｅｂアクセス制御装置において、Ｗｅｂサイトの悪性度を高精度で判定する。
【解決手段】重みがそれぞれ割り当てられた複数の悪性度推測器１２４ａ～１２４ｂを用いてアクセス先Ｗｅｂサイトの悪性度を所定の閾値に基づいて判定するＷｅｂサイト悪性度判定プログラム１０９と、アクセス先Ｗｅｂサイトの悪性度が所定の閾値より高いと判定した場合にユーザ端末１２１ａ～１２１ｃに対してアクセス先Ｗｅｂサイトへのアクセスの可否を決定するための追加認証を要求する追加認証要求プログラム１１０と、追加認証の結果に基づいて悪性度推測器１２４ａ～１２４ｂにそれぞれ割り当てられた重みを更新する重み更新プログラム１１４を有する。
【選択図】図１

図1



【特許請求の範囲】
【請求項１】
インターネットとユーザが操作するユーザ端末に接続されたＷｅｂアクセス制御装置であって、
重みがそれぞれ割り当てられた複数の悪性度推測器を用いて、Ｗｅｂサイト悪性度判定プログラムを実行することにより、アクセス先Ｗｅｂサイトの悪性度を所定の閾値に基づいて判定するＷｅｂサイト悪性度判定部と、
前記Ｗｅｂサイト悪性度判定部が前記アクセス先Ｗｅｂサイトの悪性度が前記所定の閾値より高いと判定した場合に、追加認証要求プログラムを実行することにより、前記ユーザ端末に対して前記アクセス先Ｗｅｂサイトへのアクセスの可否を決定するための追加認証を要求する追加認証要求部と、
前記追加認証要求部の前記追加認証の結果に基づいて、重み更新プログラムを実行することにより、前記Ｗｅｂサイト悪性度判定部の前記悪性度推測器にそれぞれ割り当てられた前記重みを更新する重み更新部と、
を有することを特徴とするＷｅｂアクセス制御装置。
【請求項２】
フィードバック値算出プログラムを実行することにより、前記Ｗｅｂサイト悪性度判定部の前記悪性度推測器にそれぞれ割り当てられた前記重みにフィードバックする値を算出するフィードバック値算出部を更に有し、
前記重み更新部は、
前記フィードバック値算出部で算出された算出値に基づいて、前記Ｗｅｂサイト悪性度判定部の前記悪性度推測器にそれぞれ割り当てられた前記重みを更新することを特徴とする請求項１に記載のＷｅｂアクセス制御装置。
【請求項３】
前記フィードバック値算出部は、
前記追加認証要求部の前記追加認証の結果に加え、前記追加認証の際に得られる付随情報を用いて、前記Ｗｅｂサイト悪性度判定部の前記悪性度推測器にそれぞれ割り当てられた前記重みへフィードバックする値を算出することを特徴とする請求項２に記載のＷｅｂアクセス制御装置。
【請求項４】
前記フィードバック値算出部は、
前記付随情報として、前記追加認証に要した時間又は前記アクセス先Ｗｅｂサイトの情報表示の有無を用いることを特徴とする請求項３に記載のＷｅｂアクセス制御装置。
【請求項５】
前記フィードバック値算出部は、
前記Ｗｅｂサイト悪性度判定部の前記悪性度推測器にそれぞれ割り当てられた前記重みの時系列の変化を用いて、前記悪性度推測器にそれぞれ割り当てられた前記重みへフィードバックする値を算出することを特徴とする請求項２に記載のＷｅｂアクセス制御装置。
【請求項６】
前記追加認証要求部は、
前記Ｗｅｂサイト悪性度判定部が前記アクセス先Ｗｅｂサイトの悪性度が前記所定の閾値より高いと判定した場合に、前記アクセス先Ｗｅｂサイトが不審サイトと判定し、前記ユーザ端末に対して前記不審サイトに関する追加情報を提供することを特徴とする請求項１に記載のＷｅｂアクセス制御装置。
【請求項７】
前記追加認証要求部は、
前記不審サイトに関する前記追加情報として、前記アクセス先Ｗｅｂサイトのサムネイル画像を用いることを特徴とする請求項６に記載のＷｅｂアクセス制御装置。
【請求項８】
前記重み更新部は、

前記Ｗｅｂサイト悪性度判定プログラムの前記悪性度推測器の推測結果と、前記追加認証要求部の前記追加認証の認証結果とを比較し、この比較結果に基づいて前記悪性度推測器にそれぞれ割り当てられた前記重みを更新することを特徴とする請求項１に記載のＷｅｂアクセス制御装置。

【請求項９】

前記重み更新部は、

前記悪性度推測器の推測結果と、前記追加認証要求部の前記認証結果との比較結果の一致率が高い前記悪性度推測器の重みを大きくすることを特徴とする請求項８に記載のＷｅｂアクセス制御装置。

【請求項１０】

前記Ｗｅｂサイト悪性度判定部の前記複数の悪性度推測器は、

第１の処理時間で前記悪性度を判定する第１のグループと、前記第１の処理時間より長い前記第２の処理時間で前記悪性度を判定する第２のグループとに階層的に分割され、

前記第１のグループに属する前記悪性度推測器で判定された悪性度に応じて、前記第２のグループに属する前記悪性度推測器で再度悪性度を判定するか否かを決定することを特徴とする請求項１に記載のＷｅｂアクセス制御装置。

【請求項１１】

前記Ｗｅｂサイト悪性度判定部は、

前記複数の悪性度推測器における推測結果を予め定めた閾値と比較し、前記悪性度推測器ごとに前記アクセス先Ｗｅｂサイトが悪性か良性かを推定し、前記悪性の数の合計数と前記良性の数の合計数との比較結果に応じて、前記アクセス先Ｗｅｂサイトの前記悪性度を判定することを特徴とする請求項１に記載のＷｅｂアクセス制御装置。

【請求項１２】

前記Ｗｅｂサイト悪性度判定部は、

前記複数の悪性度推測器の中から特定の悪性度推測器を予め決めておき、前記特定の悪性度推測器の推測結果を他の前記悪性度推測器の推測結果よりも優先させて、前記アクセス先Ｗｅｂサイトの前記悪性度を判定することを特徴とする請求項１に記載のＷｅｂアクセス制御装置。

【発明の詳細な説明】

【技術分野】

【０００１】

本発明は、Ｗｅｂアクセス制御装置に関する。

【背景技術】

【０００２】

近年、標的型攻撃に見られるように、攻撃が高度化しており、企業や国家にとって重大な脅威となっている。また、攻撃の高度化に伴い、外部からの侵入を完全に遮断することは困難になってきている。ここで、侵入された後の被害を抑制するためには、機密情報の窃取や感染拡大を目的とした外部への通信を遮断することが重要である。

【０００３】

以上のような背景から、適切に外部への通信を制御し、不審な通信は遮断する技術が求められている。これに関連する技術として、例えば、特許文献１がある。

【０００４】

特許文献１では、プロキシサーバ等のログから計算したＷｅｂサイトの悪性度に基づいて、悪性度が低いホワイトリスト、悪性度が高いブラックリスト及びいずれにも属さないグレーリストを自動的に生成する。グレーリストに含まれるＷｅｂサイトに接続する際に追加認証を要求し、追加認証に成功したときグレーリストをホワイトリストに振り分け、一定期間一度も成功しなかったときブラックリストに振り分ける。これにより、機械的にホワイトリストやブラックリストに振り分けられなかったＷｅｂサイトであっても、認証結果に応じていずれかのリストに振り分けることが可能である。

【先行技術文献】

【特許文献】
【０００５】
【特許文献１】特開２０１５－１７０２１９号公報
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかし、特許文献１では、Ｗｅｂサイトの悪性度を判定する機構の精度については考慮されていない。このため、悪性度判定機構の精度によっては、悪性度の高いＷｅｂサイトを安全と判断してしまい、アクセス時に被害を受けてしまう可能性がある。また、悪性度判定機構の精度によっては、悪性度の低いＷｅｂサイトを危険と判断してしまい、追加認証が頻発して利便性を低下してしまう可能性がある。
【０００７】
本発明の目的は、Ｗｅｂアクセス制御装置において、Ｗｅｂサイトの悪性度を高精度で判定することにある。
【課題を解決するための手段】
【０００８】
本発明の一態様のＷｅｂアクセス制御装置は、インターネットとユーザが操作するユーザ端末に接続され、重みがそれぞれ割り当てられた複数の悪性度推測器を用いて、Ｗｅｂサイト悪性度判定プログラムを実行することにより、アクセス先Ｗｅｂサイトの悪性度を所定の閾値に基づいて判定するＷｅｂサイト悪性度判定部と、前記Ｗｅｂサイト悪性度判定部が前記アクセス先Ｗｅｂサイトの悪性度が前記所定の閾値より高いと判定した場合に、追加認証要求プログラムを実行することにより、前記ユーザ端末に対して前記アクセス先Ｗｅｂサイトへのアクセスの可否を決定するための追加認証を要求する追加認証要求部と、前記追加認証要求部の前記追加認証の結果に基づいて、重み更新プログラムを実行することにより、前記Ｗｅｂサイト悪性度判定部の前記悪性度推測器にそれぞれ割り当てられた前記重みを更新する重み更新部と、を有することを特徴とする。
【発明の効果】
【０００９】
本発明の一態様によれば、Ｗｅｂアクセス制御装置において、Ｗｅｂサイトの悪性度を高精度で判定することができる。
【図面の簡単な説明】
【００１０】
【図１】実施例１のＷｅｂアクセス制御装置の構成例を示した図である。
【図２】認証情報管理表の一例を示す図である。
【図３】推測器管理表の一例を示す図である。
【図４】推測器重み履歴の一例を示す図である。
【図５】グレーリストの一例を示す図である。
【図６】ブラックリストの一例を示す図である。
【図７】ホワイトリストの一例を示す図である。
【図８】実施例１のＷｅｂアクセス制御装置の全体処理フローを示す図である。
【図９】Ｗｅｂサイト悪性度判定プログラムプログラムの処理フローを示す図である。
【図１０】リスト更新プログラムの処理フローを示す図である。
【図１１】フィードバック値算出の処理フローを示す図である。
【図１２】重み更新の処理フローを示す図である。
【図１３ａ】追加認証画面の一例を示す図である。
【図１３ｂ】追加認証画面の一例を示す図である。
【図１４】実施例２の時系列変化を考慮した重み更新の処理フローを示す図である。
【図１５】実施例３の推測器群構成を示す図であり、推測器群を階層的に並べた場合の処理例を示す図である。
【図１６】実施例４の最終予測結果算出フローの一例を示す図であり、（ａ）は推測結果

と重みの積和をとる方法、（ｂ）は多数決をとる方法、（ｃ）は特定の推測器を重用する方法をそれぞれ示す。
【図１７ａ】実施例５の低難易度の追加認証方式を用いた追加認証画面の一例を示す図である。
【図１７ｂ】実施例５の高難易度の追加認証方式を用いた追加認証画面の一例を示す図である。
【発明を実施するための形態】
【００１１】
最初に、実施形態について説明する。
実施形態では、アクセス先Ｗｅｂサイトの悪性度を判定し、悪性サイトへの通信を遮断しつつ、ユーザによるフィードバックを基に判別精度を改善する。実施形態では、それぞれに重みが付与された悪性度を判定する推測器を複数用意してアクセス先Ｗｅｂサイトの悪性度を判定し、悪性度が一定の閾値より高かった場合にはユーザに追加認証を要求する。
【００１２】
実施形態のＷｅｂアクセス制御装置は、ユーザが操作する端末と、インターネットとをネットワークを介して接続する装置であって、アクセス先Ｗｅｂサイトの悪性度をそれぞれが重み付けされた複数の機構を用いて推測するＷｅｂサイト悪性度判定プログラムと、悪性度の高いサイトへのアクセスを検出した際に、ユーザに対してその旨を伝え、ユーザの判断に基づいてアクセス可否を決定する追加認証要求プログラムを有する。
【００１３】
また、ユーザの判断やその付随情報を基にＷｅｂサイト悪性度判定プログラムにフィードバックする内容を決定するフィードバック値算出プログラムと、Ｗｅｂサイトの悪性度判定プログラムを構成する各推測器の重みを前記フィードバック値算出プログラムが算出した値に基づいて更新する重み更新プログラムとを有する。
【００１４】
実施形態によれば、Ｗｅｂサイトの悪性度を複数の推測器を用いて推測すること、及び推測結果の正否をユーザからのフィードバックによって判定することが可能である。この際、ユーザからのフィードバックを利用し、推測結果とユーザ判断の一致率が高い推測器の重みを大きくすることにより、全体の検出精度を自動的に改善する。これらの組み合わせによって、悪性サイトへの通信は遮断しつつ、不要な追加認証やブラックリストの手動での更新コストを抑制して利便性を向上する。
【００１５】
ユーザは、追加認証を要求された際にアクセス先Ｗｅｂサイトへの接続可否を判断し、問題ないと判断した場合のみ追加認証を突破してＷｅｂサイトへアクセスする。これにより、ユーザが意図しない、あるいは追加認証の存在を想定しておらず追加認証を突破できないマルウェア等による悪性サイトへのアクセスを抑制できる。
【００１６】
また、ユーザの判断とＷｅｂサイト悪性度判定プログラムが算出した結果を突合し、両者が一致したか否かによってＷｅｂサイト悪性度判定プログラムを構成する各推測器の重みを更新する。これにより、精度の高い推測器の判定を重視するようにし、全体としての悪性度判定精度が向上する。
【００１７】
また、ユーザの判断を確認する際、付随的に得られる情報を用いて判断が正しいか否か推定し、より確からしい利用者判断の結果を悪性度判定機構に反映する。これにより、誤ったユーザの判断を反映することによる悪性度判定精度の低下を抑制できる。
【００１８】
なお、以降では、サイバー攻撃に利用される悪性なＷｅｂサイトを悪性サイト、悪性サイトではないＷｅｂサイトを良性サイトと呼ぶ。
【実施例１】

【００１９】
図１を参照して、実施例１のＷｅｂアクセス制御装置の構成について説明する。
図１に示すように、実施例１のＷｅｂアクセス制御装置１０１は、ユーザが操作するユーザ端末１２１ａ～１２１ｃと、インターネット１２３とをネットワーク１２２を介して接続される。
【００２０】
Ｗｅｂアクセス制御装置１０１は、ＣＰＵ（Ｃｅｎｔｒａｌ Ｐｒｏｃｅｓｓｉｎｇ Ｕｎｉｔ）１０３と、ＣＰＵ１０３が処理を実行するために必要なデータを格納するためのメインメモリ１０４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記憶装置１０５と、他装置と通信を行なうためのＩＦ（インタフェース）１０２ａ、１０２ｂと、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装置１０６と、これらの各装置を接続する通信路１０７と、を備えたコンピュータである。なお、通信路１０７は、例えば、バスやケーブルなどの情報伝達媒体である。
【００２１】
ＣＰＵ１０３は、メインメモリ１０４に格納されたアクセス中継プログラム１０８を実行することにより不審な通信の制御を行う。また、ＣＰＵ１０３は、Ｗｅｂサイト悪性度判定プログラム１０９を実行することによりアクセス先Ｗｅｂサイトの悪性度の判定を行う。
【００２２】
また、ＣＰＵ１０３は、追加認証要求プログラム１１０を実行することによりユーザ端末１２１を操作するユーザの追加認証を行う。また、ＣＰＵ１０３は、アクセス先情報取得プログラム１１１を実行することによりアクセス先Ｗｅｂサイトの情報取得を行う。また、ＣＰＵ１０３は、リスト更新プログラム１１２を実行することによりグレーリスト１１８、ブラックリスト１１９、ホワイトリスト１２０の更新を行う。
【００２３】
また、ＣＰＵ１０３は、フィードバック値算出プログラム１１３を実行することによりＷｅｂサイト悪性度判定プログラム１０９を構成する各悪性度推測器１２４ａ～１２４ｂに割り当てられた重みへフィードバックする値の算出を行う。また、ＣＰＵ１０３は、重み更新プログラム１１４を実行することによりフィードバック値算出プログラム１１３での算出値に基づいて推測器管理表１１６に記録されているＷｅｂサイト悪性度判定プログラム１０９を構成する各悪性度推測器１２４に割り当てられた重みの更新を行う。
【００２４】
実施例１のＷｅｂアクセス制御装置１０１は、重みがそれぞれ割り当てられた複数の悪性度推測器１２４を用いて、Ｗｅｂサイト悪性度判定プログラム１０９を実行することにより、アクセス先Ｗｅｂサイトの悪性度を所定の閾値に基づいて判定するＷｅｂサイト悪性度判定部と、Ｗｅｂサイト悪性度判定部がアクセス先Ｗｅｂサイトの悪性度が所定の閾値より高いと判定した場合に、追加認証要求プログラム１１０を実行することにより、ユーザ端末１２１ａ～１２１ｃに対してアクセス先Ｗｅｂサイトへのアクセスの可否を決定するための追加認証を要求する追加認証要求部と、追加認証要求部の追加認証の結果に基づいて、重み更新プログラム１１４を実行することによりＷｅｂサイト悪性度判定部の悪性度推測器１２４にそれぞれ割り当てられた重みを更新する重み更新部を有する。
【００２５】
さらに、フィードバック値算出プログラム１１３を実行することにより、Ｗｅｂサイト悪性度判定部の悪性度推測器１２４にそれぞれ割り当てられた重みにフィードバックする値を算出するフィードバック値算出部を有する。重み更新部は、フィードバック値算出部で算出された算出値に基づいて、Ｗｅｂサイト悪性度判定部の悪性度推測器１２４にそれぞれ割り当てられた重みを更新する。
【００２６】
記憶装置１０５には、ユーザ端末１２１を操作するユーザの追加認証結果やその際の付随情報を示す追加認証履歴１１５、Ｗｅｂサイト悪性度判定プログラム１０９を構成する

悪性度推測器１２４の情報を管理する推測器管理表１１６が格納されている。
【００２７】
また、記憶装置１０５には、悪性度推測器１２４の時系列ごとの重みを管理する推測器重み履歴１１７、不審な通信先の情報を示すグレーリスト１１８、危険な通信先の情報を示すブラックリスト１１９、安全な通信先の情報を示すホワイトリスト１２０が格納されている。
【００２８】
上記の各プログラムやデータは、あらかじめメモリ１０４又は記憶装置１０５に格納されていてもよいし、必要な時に、入出力装置１０６から又はＩＦ１０２を介して他の装置から、インストール（ロード）されても良い。
【００２９】
次に、図２を参照して、追加認証履歴１１５の一例について説明する。
図２に示すように、追加認証履歴１１５は、ＩＤ２０１と、認証結果２０２と、付随情報２０３と、ユーザ識別情報２０７と、ＵＲＬ２０８とを含んで構成される。また、付随情報は、例えば、認証に要した時間２０４と、正解数２０５と、サイト情報表示有無２０６とから構成される。
【００３０】
ＩＤ２０１は、認証情報を一意に識別できる情報を表す。認証結果２０２は、ユーザが追加認証に成功したか否かを表す。例えば、認証結果２０２が「成功」の場合は、ユーザが追加認証の突破に成功したことを、認証結果２０２が「失敗」の場合は、ユーザが追加認証の突破に失敗したことを表す。
【００３１】
付随情報２０３は、ユーザが追加認証に臨んだ際に付随的に得られる情報を表す。ここでは、付随情報２０３は、認証に要した時間２０４と、正解数２０５と、サイト情報表示有無２０６とから構成されるものとして説明する。
【００３２】
認証に要した時間２０４は、ユーザに追加認証画面が提示されてから、認証が試行されるまでに要した時間を表す。例えば、追加認証画面が表示されてから認証の試行に４．３秒を要した場合、認証の成否に関わらず、「４．３」と記録される。また、あらかじめ定められた一定時間認証突破の試行がなかった場合、「ｔｉｍｅｏｕｔ」と記録される。
【００３３】
正解数２０５は、追加認証に文字列での認証を用いた場合に、全体の文字数のうち、どれだけ正解したかの数と、その正解率とを表す。例えば、認証文字列が「ａｂｃｄ」だった際、「ａｂｖｆ」と入力があったならば、全４文字中前半の２文字が正解しているため、「２（５０％）」と記録される。なお、この時間は、追加認証要求プログラム１１０において、追加認証画面を提示した時間とユーザからの追加認証文字列を受信した時間の差分によって算出される。
【００３４】
サイト情報表示有無２０６は、追加認証時にユーザが、アクセス先Ｗｅｂサイトが悪性か否か判断する材料として追加情報を要求したか否かを表す。例えば、「有」の場合は、ユーザが追加情報を要求したことを、「無」の場合には、ユーザが追加情報を要求しなかったことを表す。なお、ユーザの判断を補助するための追加情報としては、アクセス先Ｗｅｂサイトのサムネイル画像、ｗｈｏｉｓ情報、およびＤＮＳ情報等が挙げられる。
【００３５】
なお、追加認証履歴１１５の格納情報は、不審サイトへのアクセス試行があった際の追加認証時に取得され、格納されるものとする。また、今回は、付随情報として認証に要した時間２０４と、正解数２０５と、サイト情報表示有無２０６とを挙げたが、これらの情報以外に付随的に得られる情報を用いても良いものとする。
【００３６】
ユーザ識別情報２０７は、追加認証に臨んだユーザを一意に識別できる情報を表す。例

えば、ネットワーク環境において、「１２３」と識別子を付与されたユーザが認証に望んだ場合、ユーザを表す「１２３」が記録される。なお、今回はネットワークシステム上でユーザに付与された識別子を用いたが、ユーザを一意に識別できればよく、例えば、ユーザ端末のＩＰ（Ｉｎｔｅｒｎｅｔ　Ｐｒｏｔｏｃｏｌ）アドレスや、ユーザのユーザ名を用いても良い。

【００３７】

ＵＲＬ２０８は、追加認証の対象となった不審な接続先のＵＲＬを表す。例えば、「ｆｏｏ．ｃｏｍ」の場合は、ＵＲＬは、追加認証の対象となった不審な接続先であることを表す。なお、今回は、ＵＲＬを用いたが、不審な接続先を識別できれば良く、例えば、ＩＰアドレスや、ＦＱＤＮ（Ｆｕｌｌｙ　Ｑｕａｌｉｆｉｅｄ　Ｄｏｍａｉｎ　Ｎａｍｅ）を用いても良い。

【００３８】

次に、図３を参照して、推測器管理表１１６の一例について説明する。

図３に示すように、推測器管理表１１６は、ＩＤ３０１と、正解率３０２と、重み３０３と、直近の悪性度判定結果３０４とを含んで構成される。

【００３９】

ＩＤ３０１は、Ｗｅｂサイト悪性度判定プログラム１０９を構成する各悪性度推測器１２４を一意に識別できる情報を表す。正解率３０２は、これまでの各不審サイトに対する判定結果（悪性／良性）とユーザの追加認証結果（非突破／突破）の一致率を表す。例えば、「８０％」の場合は、Ｎ回の不審サイトの悪性度判定機会のうち、０．８Ｎ回分の判定結果がユーザの追加認証結果と一致していたことを表す。正解率が高い推測器ほどＷｅｂアクセス制御装置を導入した組織での悪性サイトの判別精度が高いものとして、重みを大きく付与される。各悪性度推測器１２４に付与する重みを算出する際の具体的な処理手順については、図１１を用いて後述する。

【００４０】

重み３０３は、各悪性度推測器１２４に割り当てられた重みの合計値が１になるように正規化された値を表す。例えば、「０．２」の場合は、全悪性度推測器１２４ａ～１２４ｂのうち２０％の判断権を当該悪性度推測器１２４が有することを表す。

【００４１】

直近の悪性度判定結果３０４は、直近の悪性度を判断する機会において、判定対象の悪性度をどのように判定したかを表す。例えば、「７５％」の場合は、当該悪性度推測器１２４は、判定対象が７５％の確率で悪性であると判断したことを表す。なお、今回はアクセス先Ｗｅｂサイトの不審度を表す指標として、アクセス先Ｗｅｂサイトの悪性度を用いて説明したが、アクセス先Ｗｅｂサイトの良性度等、不審度を表すことのできる指標であれば、どのような情報を用いても良い。なお、推測器管理表１１６の各情報は、管理者が必要に応じて、入力または更新しても良い。

【００４２】

次に、図４を参照して、推測器重み履歴１１７の一例について説明する。

図４に示すように、推測器重み履歴１１７は、時刻４０１と、重み４０２と、悪性度判定結果４０３と、認証結果との一致４０４とを含んで構成される。また、推測器重み履歴１１７は、Ｗｅｂサイト悪性度判定プログラム１０９を構成する悪性度推測器１２４毎に用意され、悪性度推測器１２４に関する情報を格納する。なお、図４では、図３のＩＤが０の悪性度推測器１２４に対応する悪性度重み履歴１１７を例示している。

【００４３】

時刻４０１は、悪性度推測器１２４ａ～１２４ｂが不審サイトの悪性度を判定した時間を表す。なお、図４では、年／月／日 時間：分：秒．小数秒の表記を用いているが、Ｕｎｉｘｔｉｍｅ等、時刻が判別できる情報であれば、どのような情報を用いても良い。

【００４４】

重み４０２は、当該時刻における悪性度推測器１２４の重みを表す。例えば、「０．３」の場合は、当該時刻に悪性度推測器１２４ａ～１２４ｂへ０．３の重みが付与されてい

たことを表す。
【００４５】
悪性度判定結果４０３は、当該時刻における悪性度判定対象のＷｅｂサイトに対して、悪性度推測器１２４が算出した悪性度を表す。例えば、「７５％」の場合は、当該悪性度推測器１２４は、当該時刻に判定対象が７５％の確率で悪性であると判断したことを表す。
【００４６】
認証結果との一致４０４は、当該時刻における不審サイトに対する判定結果（悪性／良性）とユーザの追加認証結果（非突破／突破）が一致したか否かを表す。例えば、「一致」の場合は、両者が一致していたことを、「不一致」の場合は、両者が一致していなかったことを表す。
【００４７】
次に、図５を参照して、グレーリスト１１８の一例について説明する。
図５に示すように、グレーリスト１１８は、ＩＤ５０１と、ＵＲＬ５０２と、認証成功ユーザ数５０３と、認証失敗ユーザ数５０４と、ユーザ毎の認証結果５０５とを含んで構成される。ＩＤ５０１は、グレーリスト１１８を一意に識別できる情報を表す。
【００４８】
ＵＲＬ５０２は、不審な接続先のＵＲＬを表す。例えば、「ｅｘａｍｐｌｅ．ｃｏｍ」の場合は、ＵＲＬは不審な接続先であることを表す。なお、今回は、ＵＲＬを用いたが、不審な接続先を識別できれば良く、例えば、ＩＰアドレスや、ＦＱＤＮを用いても良い。
【００４９】
認証成功ユーザ数５０３は、該接続先の追加認証を突破したユーザのユニーク数を表す。例えば、「２」の場合は、２人のユーザが該接続先の追加認証を突破したことを表す。なお、成功回数は、後述するユーザ毎の認証結果５０５を用いることによって算出できる。
【００５０】
認証失敗ユーザ数５０４は、接続先の追加認証を突破しなかったユーザのユニーク数を表す。例えば、「４」の場合は、４人のユーザが該接続先の追加認証を突破しなかったことを表す。なお、失敗回数は、後述するユーザ毎の認証結果５０５を用いることによって算出できる。
【００５１】
ユーザ毎の認証結果５０５は、接続先に対するユーザ毎の最新の認証結果を表す。例えば、「１２３：成功，７８９：失敗」の場合は、識別子１２３のユーザが追加認証を突破したことと識別子７８９のユーザが追加認証を突破しなかったことを表す。
【００５２】
グレーリスト１１８は、Ｗｅｂサイト悪性度判定プログラム１０９によって悪性であると判定された接続先がリスト更新プログラム１１０によって登録される。Ｗｅｂサイト悪性度判定プログラム１０９と、リスト更新プログラム１１０との具体的な処理については、図９と、図１０とを用いて後述する。なお、グレーリスト１１８の各情報は、管理者が必要に応じて、登録または更新しても良い。
【００５３】
次に、図６を参照して、ブラックリスト１１９の一例について説明する。
図６に示すように、ブラックリスト１１９は、ＩＤ６０１と、ＵＲＬ６０２とを含んで構成される。ＩＤ６０１は、ブラックリスト１１９を一意に識別できる情報を表す。
【００５４】
ＵＲＬ６０２は、悪性サイトのＵＲＬを表す。例えば、「ｂｌａｃｋ．ｃｏｍ」の場合は、ＵＲＬは悪性サイトであることを表す。なお、今回は、ＵＲＬを用いたが、悪性サイトを識別できれば良く、例えば、ＩＰアドレスや、ＦＱＤＮを用いても良い。
【００５５】
ブラックリスト１１９は、Ｗｅｂサイト悪性度判定プログラム１０９によって悪性であ

ると判定され、かつ一定数以上ユーザが認証を突破しなかった接続先がリスト更新プログラム１１０によって登録される。Ｗｅｂサイト悪性度判定プログラム１０９と、リスト更新プログラム１１０との具体的な処理については、図９と、図１０とを用いて後述する。なお、グレーリスト１１９の各情報は、管理者が必要に応じて、登録または更新しても良い。

【００５６】

次に、図７を参照して、ホワイトリスト１２０の一例について説明する。

図７に示すように、ホワイトリスト１２０は、ＩＤ７０１と、ＵＲＬ７０２を含んで構成される。ＩＤ７０１は、ホワイトリスト１２０を一意に識別できる情報を表す。ＵＲＬ７０２は、良性サイトのＵＲＬを表す。例えば、「ｗｈｉｔｅ．ｃｏｍ」の場合は、ＵＲＬは良性サイトであることを表す。なお、今回は、ＵＲＬを用いたが、悪性サイトを識別できれば良く、例えば、ＩＰアドレスや、ＦＱＤＮを用いても良い。

【００５７】

ホワイトリスト１２０は、Ｗｅｂサイト悪性度判定プログラム１０９によって悪性であると判定されたものの、一定数以上ユーザが認証を突破した接続先がリスト更新プログラム１１０によって登録される。Ｗｅｂサイト悪性度判定プログラム１０９と、リスト更新プログラム１１０との具体的な処理については、図９と、図１０とを用いて後述する。なお、ホワイトリスト１１９の各情報は、管理者が必要に応じて、登録または更新しても良い。

【００５８】

このように、実施例１のＷｅｂアクセス制御装置は、Ｗｅｂアクセス制御装置１０１のアクセス中継プログラム１０８が、端末１２１からの通信を中継する。次に、Ｗｅｂサイト悪性度判定プログラム１０９が、アクセス先Ｗｅｂサイトの悪性度を判定し、追加認証要求プログラム１１０がユーザ１２１に対して追加認証を要求する。

【００５９】

次に、アクセス先情報取得プログラム１１１が、アクセス先Ｗｅｂサイトの情報を取得し、リスト更新プログラム１１２がグレーリスト１１８、ブラックリスト１１９、およびホワイトリスト１２０を更新する。次に、フィードバック値算出プログラム１１３が、Ｗｅｂサイト悪性度判定プログラム１０９を構成する各悪性度推測器１２４に割り当てられた重みへフィードバックする値を算出する。次に、重み更新プログラム１１４が、フィードバック値算出プログラム１１３での算出値に基づいてＷｅｂサイト悪性度判定プログラム１０９を構成する各悪性度推測器１２４に割り当てられた重みを更新する。

【００６０】

以下、図８を参照して、Ｗｅｂアクセス制御装置１０１の全体処理フローについて説明する。

図８に示すように、アクセス中継プログラム１０８は、ＣＰＵ１０３により実行され、ユーザ端末１２１からの通信をＩＦ１０２ａ経由で中継する（ステップ８０１）。

【００６１】

アクセス中継プログラム１０８は、ブラックリストを参照し、アクセス先Ｗｅｂサイトがブラックリストに該当した場合はステップ８１０ａに進み、該当しなかった場合はステップ８０３に進む（ステップ８０２）。

【００６２】

アクセス中継プログラム１０８は、ホワイトリストを参照し、アクセス先Ｗｅｂサイトがホワイトリストに該当した場合はステップ８１１ａに進み、該当しなかった場合はステップ８０４に進む（ステップ８０３）。

【００６３】

Ｗｅｂサイト悪性度判定プログラム１０９は、アクセス先Ｗｅｂサイトの悪性度を算出し、ステップ８０５に進む（ステップ８０４）。なお、Ｗｅｂサイト悪性度判定プログラム１０９の悪性度算出フローについては、図９を用いて後述する。

【００６４】

アクセス中継プログラム１０８は、ステップ８０４で算出した悪性度をあらかじめ制定しておいた閾値と比較し、悪性度が閾値よりも低い場合はステップ８１１ａに進み、高い場合はステップ８０６へ進む（ステップ８０５）。追加認証要求プログラム１１０は、ユーザに追加認証を要求し、ステップ８０７へ進む（ステップ８０６）。

【００６５】

ここで、追加認証要求プログラム１１０は、ユーザへの追加認証に、ＣＡＰＴＣＨＡ（Ｃｏｍｐｌｅｔｅｌｙ Ａｕｔｏｍａｔｅｄ Ｐｕｂｌｉｃ Ｔｕｒｉｎｇ ｔｅｓｔ ｔｏ ｔｅｌｌ Ｃｏｍｐｕｔｅｒｓ ａｎｄ Ｈｕｍａｎｓ Ａｐａｒｔ）のような人間と機械を分別するような方式を利用することが考えられる。

【００６６】

これにより、マルウェアが機械的に悪性サイトへアクセスしようとした場合でも、該認証を突破することは困難であり、人間の悪性サイトへのアクセスに加え、マルウェアによる悪性サイトへのアクセスも抑制できる。なお、追加認証要求プログラム１１０の表示画面については、図１３を用いて後述する。

【００６７】

追加認証要求プログラム１１０は、ユーザがアクセスＷｅｂ先サイトの追加認証に際して追加情報を要求したか確認し、要求があった場合はステップ８０８へ、要求が無かった場合はステップ８０９へ進む（ステップ８０７）。

【００６８】

アクセス先情報取得プログラム１１１は、アクセス先のサイト情報を取得し、取得した情報をユーザ端末１１８へ表示する（ステップ８０８）。

【００６９】

追加認証要求プログラム１１０は、ユーザが追加認証に成功したか確認し、成功していた場合は８１１ｂへ、失敗していた場合は８１０ｂへ進む（ステップ８０９）。

【００７０】

アクセス中継プログラム１０８は、ユーザの当該サイトへのアクセスを拒否し、処理を終了する（ステップ８１０ａ）。アクセス中継プログラム１０８は、ユーザの当該サイトへのアクセスを許可し、処理を終了する（ステップ８１１ａ）。

【００７１】

アクセス中継プログラム１０８は、ユーザの当該サイトへのアクセスを拒否し、ステップ８１２へ進む（ステップ８１０ｂ）。アクセス中継プログラム１０８は、ユーザの当該サイトへのアクセスを許可し、ステップ８１２へ進む（ステップ８１１ｂ）。

【００７２】

アクセス中継プログラム１０８は、ユーザからの追加認証文字列を受信し、追加認証履歴１１５に、該追加認証文字列による認証結果や認証時の付随情報等の追加認証の情報を記録し、ステップ８１３へ進む（ステップ８１２）。

【００７３】

アクセス中継プログラム１０８は、ユーザの追加認証結果（認証を突破したか否か）をリスト更新プログラム１１２とフィードバック内容値プログラム１１３に通知し、各プログラムの処理であるステップ８１４と、ステップ８１５とに進む（ステップ８１３）。

【００７４】

リスト更新プログラム１１２は、追加認証履歴１１５を参照し、ユーザの追加認証結果を取得後、該情報を用いてグレーリスト１１８、ブラックリスト１１９、およびホワイトリスト１２０を更新する（ステップ８１４）。なお、リスト更新プログラム１１２の各リスト更新フローについては、図１０を用いて後述する。

【００７５】

フィードバック値算出プログラム１１３は、追加認証履歴１１５を参照し、ユーザの追加認証結果や付随情報を取得後、該情報を用いてフィードバック値を算出し、ステップ８１５へ進む（ステップ８１５）。なお、フィードバック値算出プログラム１１３のフィードバック値算出フローについては、図１１を用いて後述する。

【００７６】
重み更新プログラム１１４は、フィードバック値算出プログラム１１３が算出した値を基に推測器管理表１１６に記録されている各推測器の重みを更新し、処理を終了する（ステップ８１６）。
【００７７】
なお、ステップ８０６において、アクセス先Ｗｅｂサイトの悪性度が閾値以上の場合にユーザへ追加認証を要求しているが、ユーザの認証結果をキャッシュしておき、該ユーザが該アクセス先サイトに対する追加認証を１度でも突破していた場合、追加認証を要求せずアクセスを許可しても良い。これにより、ユーザの利便性が効率することが期待できる。
【００７８】
次に、図９を参照して、Ｗｅｂサイト悪性度判定プログラム１０９の処理フローの一例について説明する。
図９に示すように、ＣＰＵ１０３により実行され、ユーザ端末１２１の通信先のうち、ブラックリストと、ホワイトリストとに記録されていないものをアクセス中継プログラム１０８より受信すると、処理を開始する（ステップ９０１）。
【００７９】
なお、Ｗｅｂサイト悪性度判定プログラムは、それぞれが重みを持つ複数の悪性度推測器１２４から構成されており、各推測器の判断結果を統合して最終的な値を算出する。ここでの悪性度推測器１２４としては、ＵＲＬの文字列からＷｅｂサイトの悪性度を推測するもの、Ｗｅｂサイトに関する外部情報（ｗｈｏｉｓ情報やＤＮＳ情報等）からＷｅｂサイトの悪性度を推測するもの、およびＷｅｂサイトのコンテンツからＷｅｂサイトの悪性度を推測するものが考えられる。
【００８０】
Ｗｅｂサイト悪性度判定プログラム１０９は、アクセス中継プログラム１０８から受信したアクセス先Ｗｅｂサイトを各悪性度推測器１２４へ入力し、ステップ９０３へ進む（ステップ９０２）。
【００８１】
Ｗｅｂサイト悪性度判定プログラム１０９は、各悪性度推測器１２４の判定結果の受信を開始し、全ての推測器から結果を受信した後、ステップ９０４へ進む（ステップ９０３）。
【００８２】
Ｗｅｂサイト悪性度判定プログラム１０９は、ステップ９０３で受信した各推測器の判定結果を推測器管理表１１６と推測器重み履歴１１７へ記録し、ステップ９０５へ進む（ステップ９０４）。
【００８３】
Ｗｅｂサイト悪性度判定プログラム１０９は、ステップ９０３で受信した各推測器の推測結果を推測器管理表１１６を参照することによって得られる各推測器に付与された重みに掛け合わせ、その合計値を最終予測結果として算出し、処理を終了する（ステップ９０５）。なお、上述の算出手順は、以下の計算式（数１）のように示すことができる。
【００８４】
【数１】

$$\sum_{i=0}^{n} P_i \times w_i \quad (\mathrm{n}:\text{推測器の数}、\ w_n:\text{各推測器の重み}、\ P_n:\text{各推測器の推測結果})$$

【００８５】
なお、今回は上述の計算式を用いた最終予測結果の算出手順を例示したが、各推測器の予測結果に対して重みを反映させ、最終的に統合する方式であれば、どのような方式を用いても良い。また、悪性度推測器１２４の追加及び削除は可能であり、管理者が必要に応じて該悪性度推測器１２４の追加及び削除を行っても良い。

【００８６】
次に、図１０を参照して、リスト更新プログラム１１２の処理フローの一例について説明する。
図１０に示すように、ＣＰＵ１０３により実行され、ユーザ端末１２１の通信先のうち、Ｗｅｂサイト悪性度判定プログラム１０９によって、その悪性度が閾値以上と判定されたＷｅｂサイトに対するユーザの追加認証結果をアクセス中継プログラム１０８より受信すると、処理を開始する（ステップ１００１）。
【００８７】
リスト更新プログラム１１２は、グレーリスト１１８を参照し、アクセス先Ｗｅｂサイトが該グレーリストに該当した場合はステップ１００４に進み、該当しなかった場合はステップ１００３に進む（ステップ１００２）。
【００８８】
リスト更新プログラム１１２は、アクセス先Ｗｅｂサイトをグレーリスト１１８に登録し、ステップ１００４に進む（ステップ１００３）。
【００８９】
リスト更新プログラム１１２は、アクセス中継プログラム１０８より受信したユーザの追加認証結果を参照し、該追加認証結果をグレーリスト１１８に記録し、グレーリスト１１８の認証成功ユーザ数、認証失敗ユーザ数、およびユーザ毎の認証結果を更新した後、ステップ１００５に進む（ステップ１００４）。
【００９０】
リスト更新プログラム１１２は、アクセス中継プログラム１０８より受信したユーザの追加認証結果を参照し、認証に成功していた場合はステップ１００６に進み、認証に失敗していた場合はステップ１００９に進む（ステップ１００５）。
【００９１】
リスト更新プログラム１１２は、グレーリスト１１８を参照し、アクセス先Ｗｅｂサイトの累計認証成功ユーザ数が一定数を超えていた場合はステップ１００７に進み、超えていなかった場合は処理を終了する（ステップ１００６）。
【００９２】
リスト更新プログラム１１２は、アクセス先Ｗｅｂサイトをホワイトリスト１２０に登録し、ステップ１００８に進む（ステップ１００７）。
【００９３】
リスト更新プログラム１１２は、アクセス先Ｗｅｂサイトに対応する行をグレーリスト１１８から削除し、処理を終了する（ステップ１００８）。
【００９４】
リスト更新プログラム１１２は、グレーリスト１１８を参照し、アクセス先Ｗｅｂサイトの累計認証失敗ユーザ数が一定数を超えていた場合はステップ１０１０に進み、超えていなかった場合は処理を終了する（ステップ１００９）。
【００９５】
リスト更新プログラム１１２は、アクセス先Ｗｅｂサイトをブラックリスト１１９に登録し、ステップ１０１１に進む（ステップ１０１０）。
【００９６】
リスト更新プログラム１１２は、アクセス先Ｗｅｂサイトに対応する行をグレーリスト１１８から削除し、処理を終了する（ステップ１０１１）。
【００９７】
次に、図１１を参照して、フィードバック値算出プログラム１１３の処理フローについて説明する。
図１１に示すように、ＣＰＵ１０３により実行され、ユーザ端末１２１の通信先のうち、Ｗｅｂサイト悪性度判定プログラム１０９によって、その悪性度が閾値以上と判定されたアクセス先Ｗｅｂサイトに対するユーザの追加認証結果をアクセス中継プログラム１０８より受信すると、処理を開始する（ステップ１１０１）。

【００９８】
なお、今回は認証結果２０２と付随情報２０３として認証に要した時間２０４、正解数２０５、およびサイト情報表示有無２０６を用いた場合の一例を説明するが、該情報以外を用いることや同様の情報を用いた場合でも異なる処理フローで最終的な値を算出することも可能である。
【００９９】
フィードバック値算出プログラム１１３は、値の初期値１．０を設定し、ステップ１１０３に進む（ステップ１１０２）。
【０１００】
フィードバック値算出プログラム１１３は、追加認証履歴１１５の最新エントリから認証情報を取得し、ステップ１１０４に進む（ステップ１１０３）。
【０１０１】
フィードバック値算出プログラム１１３は、ステップ１１０３で取得した認証情報を参照し、認証に成功していた場合はステップ１１０９に進み、認証に失敗していた場合はステップ１１０５に進む（ステップ１１０４）。
【０１０２】
フィードバック値算出プログラム１１３は、ステップ１１０３で取得した認証情報を参照し、認証がタイムアウトしていた場合はステップ１１１２に進み、していなかった場合はステップ１１０６に進む（ステップ１１０５）。
【０１０３】
フィードバック値算出プログラム１１３は、ステップ１１０３で取得した認証情報を参照し、サイト情報の表示があった場合はステップ１１１２に進み、なかった場合はステップ１１０７に進む（ステップ１１０６）。
【０１０４】
フィードバック値算出プログラム１１３は、値を０．５倍し、ステップ１１０８に進む（ステップ１１０７）。
【０１０５】
フィードバック値算出プログラム１１３は、ステップ１１０３で取得した認証情報を参照し、値を正解数に応じて減少し、ステップ１１１２に進む（ステップ１１０８）。
【０１０６】
フィードバック値算出プログラム１１３は、ステップ１１０３で取得した認証情報を参照し、値を認証に要した時間に応じて減少し、ステップ１１１０に進む（ステップ１１０９）。
【０１０７】
フィードバック値算出プログラム１１３は、ステップ１１０３で取得した認証情報を参照し、サイト情報の表示があった場合はステップ１１１２に進み、なかった場合はステップ１１１１に進む（ステップ１１１０）。
【０１０８】
フィードバック値算出プログラム１１３は、値を０．５倍し、ステップ１１１２に進む（ステップ１１１１）。
【０１０９】
フィードバック値算出プログラム１１３は、ここまでのステップで算出した最終的な値を返却し、処理を終了する（ステップ１１１２）。
【０１１０】
本処理により、ユーザの認証結果の確からしさを数値化し、確からしさに応じてＷｅｂサイト悪性度判定プログラム１０９を構成する各推測器１２４へフィードバックを行うことが可能となる。
【０１１１】
なお、今回付随情報２０３として認証に要した時間２０４、正解数２０５、およびサイト情報表示有無２０６を用いた理由は、以下の通りである。

【０１１２】
認証に要した時間２０４は、主に人間によるアクセスとマルウェアによるアクセスを分別するために用いる。不審サイトへアクセスした際に要求する追加認証は、通常のＷｅｂアクセス時には発生せず、人間は追加認証が出た際に人間は柔軟に対応できるのに対し、追加認証を想定していないマルウェアは、これを突破できずタイムアウトになる。
【０１１３】
あるいは、近年の攻撃の高度化に伴い、追加認証を突破する機能を持つマルウェアも報告されているが、この場合は、プログラムによって人間では達成困難な入力速度で認証突破を試みると推察される。
【０１１４】
以上のように、マルウェアが認証に要する時間には、タイムアウト、あるいはきわめて短いといった特徴があり、人間による認証と分類に有用であることから、該情報を利用した。
【０１１５】
また、認証結果が成功だった場合、フィードバック値算出プログラム１１３は、ステップ１１０９において、認証に要した時間に応じてフィードバックする値を減算している。一方で、認証結果が失敗の場合は、同減算は行っていない。
【０１１６】
これは、アクセス先Ｗｅｂサイトが不審な場合でもリスクを鑑みずにアクセスしてしまうユーザを考慮したものである。セキュリティレベルの低いユーザは、アクセス先Ｗｅｂサイトが不審であると警告を受けたとしても、そのリスクを鑑みずにアクセスしてしまうことが考えられる。
【０１１７】
一方で、追加認証を突破せずにアクセスを中止した場合は、アクセス先Ｗｅｂサイトのリスクを考慮した上のものであると推察される。上述の追加認証結果の性質から、認証成功の信頼性は、認証失敗の信頼性よりも高いと推察される。
【０１１８】
以上の理由から、認証突破の場合は、認証を突破しなかった場合にはないフィードバックする値の減算を行っており、これによって、該追加認証の信頼性を反映している。
【０１１９】
正解数２０５は、主に認証失敗時、該失敗がヒューマンエラーによるものか否かを分別するために用いる。例えば、認証に失敗した際、意図したものであれば、何も入力しない、あるいは適当な文字を入力することにより、認証突破のために要求された文字列から大きく外れることが推察される。
【０１２０】
一方で、意図しないもの（ヒューマンエラー）は、突破しようとしたものの外れてしまった入力であることから、認証突破のために要求された文字列から大きくは外れないことが推察される。以上のように、認証の失敗がヒューマンエラーによるか否かは、認証突破のために要求された文字列に対する入力の正解数に現れることから、該情報を利用した。
【０１２１】
サイト情報表示有無２０６は、主にユーザの認証結果の確からしさを検証するために用いる。Ｗｅｂアクセス制御装置１０１は、前述の通り、ユーザが追加認証を要求された際にユーザの要求に応じてアクセス先Ｗｅｂサイトの情報を追加で取得・表示する機能を有する。
【０１２２】
該情報を要求したユーザは、追加情報を要求し、アクセス先Ｗｅｂサイトの性質を多角的に判断しようとするセキュリティ意識の高いユーザであることが推察されることに加え、その際の判断は追加情報を見た上のものであることから、該追加情報を見ていない判断よりも信頼性が高いと推察される。以上のように、サイト情報表示有無２０６は、ユーザの認証結果の信頼性を検証するのに有用であることから、該情報を利用した。

【０１２３】
次に、図１２を参照して、重み更新プログラム１１４の処理フローについて説明する。
図１２に示すように、ＣＰＵ１０３により実行され、フィードバック値算出プログラム１１３よりＷｅｂサイト悪性度判定プログラムを構成する各悪性度推測器１２４に反映するフィードバック値を受信すると、処理を開始する（ステップ１２０１）。
【０１２４】
重み更新プログラム１１４は、悪性度推測器１２４のＩＤを意味する変数ｉに初期値０を設定し、ステップ１２０３に進む（ステップ１２０２）。
【０１２５】
重み更新プログラム１１４は、追加認証履歴１１５と推測器管理表１１６を参照し、ＩＤが変数ｉの推測器の推測結果と認証結果を取得した後、ステップ１２０４に進む（ステップ１２０３）。
【０１２６】
重み更新プログラム１１４は、ステップ１１０３で取得したＩＤが変数ｉの推測器の推測結果と認証結果を比較し、両者が一致していた場合はステップ１２０５に進み、一致していなかった場合はステップ１２０６に進む（ステップ１２０４）。
【０１２７】
重み更新プログラム１１４は、ＩＤが変数ｉの推測器の重みをフィードバック値算出プログラム１１３より受信した値に応じて加算し、推測器管理表１１６に記録されている該推測器の重みを加算後の値に更新した後、ステップ１２０７へ進む（ステップ１２０５）。
【０１２８】
重み更新プログラム１１４は、ＩＤが変数ｉの推測器の重みをフィードバック値算出プログラム１１３より受信した値に応じて減算し、推測器管理表１１６に記録されている該推測器の重みを減算後の値に更新した後、ステップ１２０７へ進む（ステップ１２０６）。
【０１２９】
重み更新プログラム１１４は、変数ｉに１加算し、ステップ１２０３に進む（ステップ１２０７）。
【０１３０】
重み更新プログラム１１４は、変数ｉと推測器管理表１１６を参照することによって得ることのできる推測器数を比較し、変数ｉが推測器数に満たない場合はステップ１２０３に戻り、推測器数を上回っていた場合はステップ１２０９へ進む（ステップ１２０８）。
【０１３１】
重み更新プログラム１１４は、推測器の重みの合計が１になるように、推測器管理表１１６に記録されている各悪性度推測器１２４の重みを正規化し、処理を終了する（ステップ１２０９）。
【０１３２】
図１３ａ、図１３ｂを参照して、追加認証要求プログラム１１０によって表示される追加認証画面の一例について説明する。
図１３ａに示すように、アクセス先Ｗｅｂサイト悪性度判定プログラムによって閾値以上の悪性度を示したＷｅｂサイトへアクセスしようとした際、追加認証画面を表示し、画面内の追加認証を突破した場合のみ、Ｗｅｂサイトへのアクセスを許可する。追加認証画面は、アクセス先Ｗｅｂサイトが不審であるという警告文１３０１と、追加認証用の文字列表示欄１３０２と、追加認証文字列入力フォーム１３０３と、追加認証文字列送信ボタン１３０４と、追加情報要求ボタン１３０５とから構成される。
【０１３３】
ユーザは、該Ｗｅｂサイトが悪性でないと判断した場合のみ追加認証用の文字列表示欄１３０２に示された文字列を追加認証文字列入力フォーム１３０３に正しく入力し、追加認証文字列送信ボタン１３０４を押下することにより、アクセスを続行できる。また、ユ

ーザがアクセス可否の判断に窮した際には、追加情報要求ボタン１３０５を押下することにより、該判断のための追加情報を取得・表示できる。

【０１３４】

追加情報表示後の画面の一例を図１３ｂに示す。

追加情報表示後の追加認証画面は、Ｗｅｂサイト情報表示欄１３０６と、Ｗｅｂサイトサムネイル表示欄１３０７とから構成される。Ｗｅｂサイト情報表示欄１３０６には、ｗｈｏｉｓ情報やＤＮＳ情報といったアクセス先Ｗｅｂサイトに関する公開情報が表示される。Ｗｅｂサイトサムネイル表示欄１３０７には、実際に該該アクセス先Ｗｅｂサイトにアクセスした際のサムネイルが画像で表示される。ユーザはこれらの情報を基に、アクセス先Ｗｅｂサイトへのアクセス可否を判断する。

なお、実施例１の一部を変更して以下のように実施しても良い。

【０１３５】

アクセス先Ｗｅｂサイトの悪性度の最終予測結果が閾値以下であっても、ある1つ以上の推測器が高い悪性度を算出した場合は、追加認証を要求しても良い。これにより、汎用性の低さから重みが少なくなりがちな特定の悪性サイトを検出することに特化したような推測器であっても、Ｗｅｂサイト悪性度判定プログラム１１０に組み込むことが可能になり検出漏れを抑制できる。

【０１３６】

また、悪性度の値によって追加認証の難易度を上下させても良い。例えば、悪性度が相対的に低い場合はボタンのクリックのみ、高い場合はＣＡＰＴＣＨＡ認証を行うことが考えられる。これにより、良性よりのグレーなサイトに対するユーザの認証にかかる負荷を抑制できる。

【０１３７】

また、検証後のユーザの追加認証結果を正解データ（Ｇｒｏｕｎｄ Ｔｒｕｔｈ）として扱い、データが与えられる毎に逐次的に学習し、モデルを構築するオンライン学習の教師データに利用しても良い。これにより、各推測器に付与する重みの最適化だけでなく、推測器そのものの最適化も可能となる。

【実施例２】

【０１３８】

次に、図１４を参照して、実施例２のＷｅｂアクセス制御装置について説明する。

実施例２は、実施例１に係るＷｅｂアクセス制御装置１０１を含み、さらに悪性度推測器１２４に付与する重みを更新する際に、該重みの時系列変化に着目し、より適した形で重みを付与する機能を有するＷｅｂアクセス制御装置である。

【０１３９】

実施例２では、推測器の重みの時系列変化に着目し、重みの変化にこれまでと異なる傾向が見られた場合、重みの更新を保留する。例えば、潜在的に精度の高い推測器の重みは、単調増加を続け、上昇値が飽和した値へ収束することが推察されるが、ユーザの認証結果があるべきものと異なっていた場合、単調増加、あるいは一定値に収束していた重みが減少方向に向かう。この変化点を検出し、その場合重みの更新を一旦保留することにより、その重みの変動が正しいものなのか、あるいはユーザの認証ミス等によるノイズかを見極め、不適切な重みの上下を抑制でき、Ｗｅｂサイト悪性度の判定精度の低下を抑制できる。

【０１４０】

図１４は、本実施例における重み更新フローの例である。

実施例１と同一の構成要素には同一の符号を付すことによってその説明を省略し、以下では、実施例１と異なる点を中心に説明する。

【０１４１】

重み更新プログラム１１４は、図１２に示したフローに加え、重み更新時にその時系列変化に着目した処理フローを有する。具体的には、ステップ１２０４において、該推測器の推測結果と認証結果が一致したか否かを検証し、重みを加算／減算するフローに分岐し

た際に、重みの時系列変化を基に実際に重みを加算／減算するか判断するステップ１２１０とステップ１２１１を有する。以降では、ステップ１２１０とステップ１２１１の処理内容について説明する。

【０１４２】

重み更新プログラム１１４は、ＩＤが変数ｉの推測器の重みの時系列変化を該推測器に対応する推測器時系列重み管理表１１７を参照し取得する。また、仮に重みを加算した場合、重みの変化の傾向がこれまでと異なるか検証し、これまでの変化と異なる傾向が見られた場合、重み更新を保留するために、ステップ１２０７へ進む。重みの変化にこれまでと異なる傾向が見られなかった場合は、ステップ１２０５へ進む（ステップ１２１０）。

【０１４３】

重み更新プログラム１１４は、ＩＤが変数ｉの推測器の重みの時系列変化を該推測器に対応する推測器時系列重み管理表１１７を参照し取得する。また、仮に重みを減算した場合、重みの変化の傾向がこれまでと異なるか検証し、これまでの変化と異なる傾向が見られた場合、重み更新を保留するために、ステップ１２０７へ進む。重みの変化にこれまでと異なる傾向が見られなかった場合は、ステップ１２０６へ進む（ステップ１２１１）。

【実施例３】

【０１４４】

図１５を参照して、実施例３のＷｅｂアクセス制御装置について説明する。

実施例３は、実施例１に係るＷｅｂアクセス制御装置１０１を含み、さらにＷｅｂサイト悪性度判定プログラム１０９において、複数の悪性度推測器１２４を階層的に並べることによって、悪性度算出時間を効率化する機能を有する。

【０１４５】

実施例３では、複数の悪性度推測器１２４を処理時間の比較短い表層解析部分（第１のグループ）と、処理時間を要する分より高精度でＷｅｂサイトの悪性度を算出可能な詳細解析部分（第２のグループ）に階層的に分割する。これにより、明らかに良性、あるいは明らかに悪性なＷｅｂサイトに対しては、処理時間の短い表層解析部分の複数の悪性度推測器１２４のみでＷｅｂサイトの性質を判定できるため、判定に要する処理時間を短縮できる。また、表層解析部分ではＷｅｂサイトの性質を判断することが難しい場合は、詳細解析部分を用いて判断を行うため、判定精度が著しく低下することも無い。

【０１４６】

図１５は、実施例３における推測器群構成方式の一例である。なお、図１５は、実施例１におけるステップ８０４でのＷｅｂサイト悪性度判定プログラム１０９において、複数の悪性度推測器１２４を階層的に並べた場合の処理例である。Ｗｅｂサイト悪性度判定プログラム１０９以外の処理フローは実施例１と同じであるためその説明は省略し、以下では、実施例１と異なる点である階層的に複数の悪性度推測器１２４を並べた場合の推測結果導出方法を中心に説明する。

【０１４７】

Ｗｅｂサイト悪性度判定プログラム１０９は、図９に示したフローに加え、複数の悪性度推測器１２４を表層解析部分（悪性度推測器Ａ、悪性度推測器Ｂ）と詳細解析部分（悪性度推測器Ｃ、悪性度推測器Ｄ、悪性度推測器Ｅ）に分割することによる追加の悪性度計算フローを有する。具体的には、ステップ９０２において、全ての複数の悪性度推測器１２４にアクセス先Ｗｅｂサイトを入力するのではなく、表層解析部分（悪性度推測器Ａ、悪性度推測器Ｂ）にのみ入力する。その後、表層解析部分（悪性度推測器Ａ、悪性度推測器Ｂ）から推測結果（推測結果Ａ、推測結果Ｂ）を受信し、その推測結果（途中推測結果）が明らかに良性である、あるいは明らかに悪性である場合は、推測結果を最終予測結果としてステップ９０４に進む。

【０１４８】

ここでの明らかに悪性とは、例えば、悪性度が９０％以上、明らかに良性とは、例えば悪性度が１０％以下のような状態を指す。なお、具体的な数値は、この限りではない。表層解析部分（悪性度推測器Ａ、悪性度推測器Ｂ）で明らかに良性、あるいは明らかに悪性

だと判断できなかった場合は、詳細解析部分（悪性度推測器Ｃ、悪性度推測器Ｄ、悪性度推測器Ｅ）へと処理を進める。この際、詳細解析部分を構成する複数の悪性度推測器Ｃ、悪性度推測器Ｄ、悪性度推測器Ｅにアクセス先Ｗｅｂサイトを入力する。その後、推測結果（推測結果Ｃ、推測結果Ｄ、推測結果Ｅ）を受信し、該推測結果を最終予測結果とする。

【０１４９】

なお、図１５では、複数の悪性度推測器１２４を２段に分割したが、３段以上に分割しても良い。実施例３では、以上の手法によって、悪性度算出時間を効率化することを可能とする。

【実施例４】

【０１５０】

図１６を参照して、実施例４のＷｅｂアクセス制御装置について説明する。

実施例４は、実施例１に係るＷｅｂアクセス制御装置１０１を含む。さらにＷｅｂサイト悪性度判定プログラム１０９において、複数の悪性度推測器１２４から受領した悪性度を基に最終予測結果を算出する際の手法に着目し、より適した形で悪性度を算出することによってＷｅｂサイトの悪性度判定精度を向上する機能を有する。

【０１５１】

実施例４は、実施例１で示した最終予測結果算出方法（ａ）の他に、複数の悪性度推測器１２４の推測結果から多数決をとる方法（ｂ）、および実施例１の算出方法に加えて特定の場合に単体の推測器が算出した予測結果を重用する方法（ｃ）を有する。

【０１５２】

多数決をとる方法（ｂ）では、悪性度推測器Ａ、悪性度推測器Ｂ、悪性度推測器Ｃにおいて、予測結果と重みを掛け算した後に合計をとる方法（ａ）における計算処理が不要になるため処理時間を短縮できる。

【０１５３】

特定の場合に単体の推測器が算出した予測結果を重用する方法（ｃ）では、特定の性質を有するＷｅｂサイトの性質判断に特化した悪性度推測器Ｃを有効活用し全体としての推測精度を向上できる。例えば、フィッシングサイトやマルウェアダウンロードサイトのような特定の悪性サイトに特化した悪性度推測器Ｃは、よりアクセスの多い良性サイトに対しては推測精度が低く、普段の運用の中で、悪性度推測器Ｃに与えられる重みは小さくなることが考えられる。

【０１５４】

この場合には、悪性度推測器Ｃの得意とするフィッシングサイトやマルウェアダウンロードサイトへのアクセスが発生した場合でも悪性度推測器Ｃの重みが小さく、最終予測結果にほとんど反映されない。このため、最終予測結果が適切に算出できない可能性がある。そこで、上述した特定の悪性サイトに特化した悪性度推測器Ｃがアクセス先のＷｅｂサイトに対し、高い悪性度を示した場合、全体としての予測結果が良性であったとしても、悪性の恐れがあるとして利用者に追加認証を要求する。これにより、悪性サイトの見落としを抑制し、前述したような全体としての推測精度向上が可能になる。

【０１５５】

次に、図１６を参照して、実施例４における最終予測結果算出フローの一例について説明する。

なお、図１６は、実施例１におけるおよびステップ８０５でのＷｅｂサイト悪性度判定プログラム１０９において、アクセス先Ｗｅｂサイトの性質が悪性か良性か判定する際の各手法における一例である。

【０１５６】

また、左から順に、実施例１の推測結果と重みの積和をとる方法（ａ）、多数決をとる方法（ｂ）、および特定の悪性度推測器を重用する方法（ｃ）を図示している。Ｗｅｂサイト悪性度判定プログラム以外の処理フローは実施例１と同一のためその説明は省略する。以下では、実施例１と異なる方法である多数決をとる方法（ｂ）と、特定の悪性度推測

器を重用する方法（ｃ）を中心に説明する。
【０１５７】
まず、多数決をとる方法（ｂ）について説明する。
多数決をとる方法は、悪性度推測器Ａ、悪性度推測器Ｂ、悪性度推測器Ｃにおける推測結果を事前に制定していた閾値と比較し、悪性度推測器Ａ、悪性度推測器Ｂ、悪性度推測器Ｃごとにアクセス先Ｗｅｂサイトの性質が悪性か良性かを推定する。その後、悪性度推測器Ａ、悪性度推測器Ｂ、悪性度推測器Ｃから集計した性質の合計数を比較し、該合計数が最も多いものを最終予測結果として算出する。（ｂ）の例では、３つの悪性度推測器Ａ、悪性度推測器Ｂ、悪性度推測器Ｃのうち、２つが良性、１つが良性と推測しており、良性の方が多いことから、最終予測結果を良性としている。
【０１５８】
次に、特定の推測器を重用する方法（ｃ）について説明する。
特定の推測器を重用する方法では、まず重用する悪性度推測器Ｃが高い悪性度を示していないか確認する。このとき、悪性度推測器Ｃが高い値を出していた場合は、他の悪性度推測器Ａ、悪性度推測器Ｂが算出した結果に関わらず、Ｗｅｂサイトは悪性の可能性があるとして利用者に追加認証を要求する。悪性度推測器Ｃが高い値を出していなかった場合は、実施例１と同様の方法で最終予測結果を算出し、該値に応じてアクセス制御を実施する。
【０１５９】
（ｃ）の例では、３つの悪性度推測器Ａ、悪性度推測器Ｂ、悪性度推測器Ｃのうち、悪性度推測器Ｃが特定の悪性サイトに特化したものである。悪性度推測器Ｃが高い悪性度を出していることから、アクセス先Ｗｅｂサイトを悪性と判定している。なお、実施例１の計算方式だとアクセス先Ｗｅｂサイトは良性と判定される。また、重用する特定の悪性度推測器Ｃは、管理者が事前に指定しているものとし、本方法では、図３の推測器管理表１１６に各悪性度推測器について重用するか否かを表す追加項目を持つ。
【０１６０】
実施例４では、以上の手法によって、処理時間の短縮や推測精度の向上が可能となる。
【実施例５】
【０１６１】
図１７ａ及び図１７ｂを参照して、実施例５のＷｅｂアクセス制御装置について説明する。
実施例５は、実施例１に係るＷｅｂアクセス制御装置１０１を含む。さらに追加認証要求プログラム１１０において、状況に応じて追加認証方法を変更することによって、利用者の利便性を向上するとともに、悪性サイトへの誤アクセスをより高い確度で抑制する機能を有する。実施例５では、以下の３つの観点で追加認証の難易度を変更する。
【０１６２】
１つ目は、悪性度に応じた追加認証の難易度変更である。具体的には、悪性サイトへのアクセスの可能性があるとして利用者に追加認証を要求する際、Ｗｅｂサイトの悪性度を非常に高いと判断した際には、高難易度の追加認証を要求知る。一方、Ｗｅｂサイトの悪性度が閾値よりは高いものの閾値に近く悪性と判断されるものの中では相対的に低いと破断した際には、低難易度の追加認証を要求する。これにより、より悪性度の高い可能性があるＷｅｂサイトに誤アクセスする可能性を抑制し、悪性度が相対的には低いサイトにはアクセス性を向上して利便性を向上する。
【０１６３】
本方法では、悪性度が何％以上であれば非常に高いか、悪性度が何％以下であれば悪性度が相対的に低いかを表す追加の表を図１の記憶装置１０５の部分に持つ。また、各値は、事前に管理者が制定するものとする。
【０１６４】
２つ目は、グレーリストにおける情報源の信頼度に応じた追加認証の難易度変更である。グレーリストには、手動で悪性サイトらしいＷｅｂサイトを追加できるが、この際の情

報源としては、信頼性の高い組織が公開しているものから、そうでないものまでが含まれ得る。

【０１６５】

そこで、該情報源の信頼度に応じて、追加認証の難易度を変更する。信頼性の高い情報源から得られたＷｅｂサイトへのアクセスに対する追加認証には、低難易度のものを利用する。一方、そうでない情報源から得られたＷｅｂサイトへのアクセスに対する追加認証には、高難易度のものを利用する。これにより、利用者の利便性を向上するとともに、悪性サイトへの誤アクセスをより高い確度で抑制する。

【０１６６】

本方法では、図５のグレーリスト１１８に格納された各ＵＲＬについて、情報源の信頼性を、例えば、高、中及び低で表す追加項目を持つ。また、各値は、事前に管理者が制定するものとし、情報源の信頼性を表す方法は、上記の限りではない。

【０１６７】

３つ目は、特定の悪性サイトに特化した悪性度推測器が高い悪性度を示していた場合における追加認証の高難易度化である。特定の悪性サイトに特化した悪性度推測器が高い悪性度を示していた場合は、アクセスするべきでない特定の性質を持った悪性サイトである可能性が高まる。特に、悪性度推測器が高い悪性度を示し、かつ全体の推定結果としては良性サイトよりの判定であった場合は、他の悪性度推測器では検知できないような良性サイトを模した悪性サイトである可能性がある。このため、Ｗｅｂサイトへのアクセスはより遮断する必要がある。

【０１６８】

以上の理由から、利用者に要求する追加認証を高難易度のものにし、これにより、性サイトへの誤アクセスをより高い確度で抑制する。また、重用する特定の悪性度推測器は、管理者が事前に指定しているものとし、本方法では、図３の推測器管理表１１６に各悪性度推測器について重用するか否かを表す追加項目を持つ。

【０１６９】

実施例５においては、どの認証方式を利用するかを表す追加の表を図１の記憶装置１０５の部分に持つ。どの認証方式を利用するかは、事前に管理者が制定するものとする。また、実施例５では、難易度の異なる追加認証方式を実施例１に示したものの他に２つ有する。

【０１７０】

図１７ａは、低難易度の追加認証方式を用いた追加認証画面の一例を示す図である。

実施例１のように文字列を画面から読み取り入力するといったステップは無く、画面に表示された接続ボタン１７０１を押下するだけでＷｅｂサイトへのアクセスを続行できる。

【０１７１】

図１７ｂは、高難易度の追加認証方式を用いた追加認証画面の一例を示す図である。

追加認証用の計算式表示欄１７０２を備え、計算式表示欄１７０２から計算式を読み取り、計算式の計算結果を追加認証文字列入力フォーム１７０３に正しく入力し、加認証文字列送信ボタン１７０４を押下することにより、アクセスを続行できる。

【０１７２】

実施例５では、以上の方法によって、利用者の利便性を向上するとともに、悪性サイトへのアクセスをより高い確度で抑制することが可能となる。

【符号の説明】

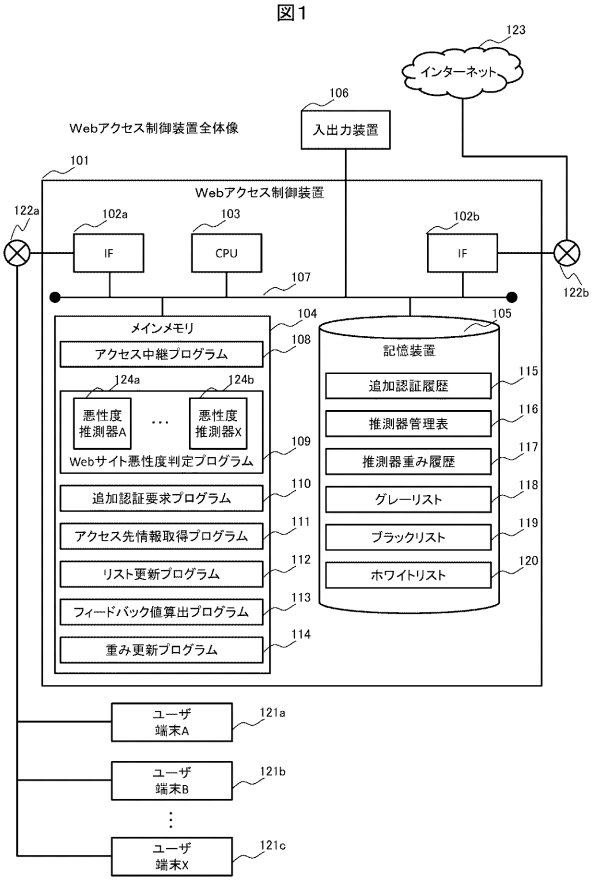
【０１７３】

１０１：Ｗｅｂアクセス制御装置
１０８：アクセス中継プログラム
１０９：Ｗｅｂサイト悪性度判定プログラム
１１０：追加認証要求プログラム
１１１：アクセス先情報取得プログラム

１１２：リスト更新プログラム
１１３：フィードバック値算出プログラム
１１４：重み更新プログラム
１１５：追加認証履歴
１１６：推測器管理表
１１７：推測器重み履歴
１１８：グレーリスト
１１９：ブラックリスト
１２０：ホワイトリスト
１２１：ユーザ端末
１２３：インターネット
１２４：悪性度推測器

【図１】

図1



【図２】

図2

追加認証履歴115

ID	認証結果	付随情報			ユーザ識別情報	URL
		認証に要した時間（s）	正解数	サイト情報表示有無		
1	成功	4.3	4 (100%)	無	123	foo.com
2	失敗	7.2	2 (50%)	有	456	bar.net
3	失敗	timeout	0 (0%)	無	789	baz.jp
…						

【図３】

図3

推測器管理表116

ID	正解率	重み	直近の悪性度判定結果
0	80%	0.4	75%
1	90%	0.5	82%
2	30%	0.05	19%
…			

【図４】

図4

推測器重み履歴117

401 時刻	402 重み	403 悪性度判定結果	404 認証結果との一致
2016/12/01 21:04:42.20	0.3	12%	一致
2016/12/01 21:04:46.30	0.4	82%	一致
2016/12/01 21:04:51.40	0.5	64%	不一致
2016/12/01 21:06:03.50	0.4	75%	不一致
...			

【図５】

図5

グレーリスト118

501 ID	502 URL	503 認証成功ユーザ数	504 認証失敗ユーザ数	505 ユーザ毎の認証結果
0	example.com	2	0	123:成功, 456:成功
1	malware.com	0	4	123:失敗, 789:失敗...
2	abc.com	4	1	456:成功, 789:成功...
3	zyz.org	1	1	123:成功, 789:失敗
...				

【図６】

図6

ブラックリスト119

601 ID	602 URL
0	black.com
1	unsafe.com
2	ng.com
...	

【図７】

図7

ホワイトリスト120

701 ID	702 URL
0	white.com
1	safe.com
2	ok.com
...	

【図８】

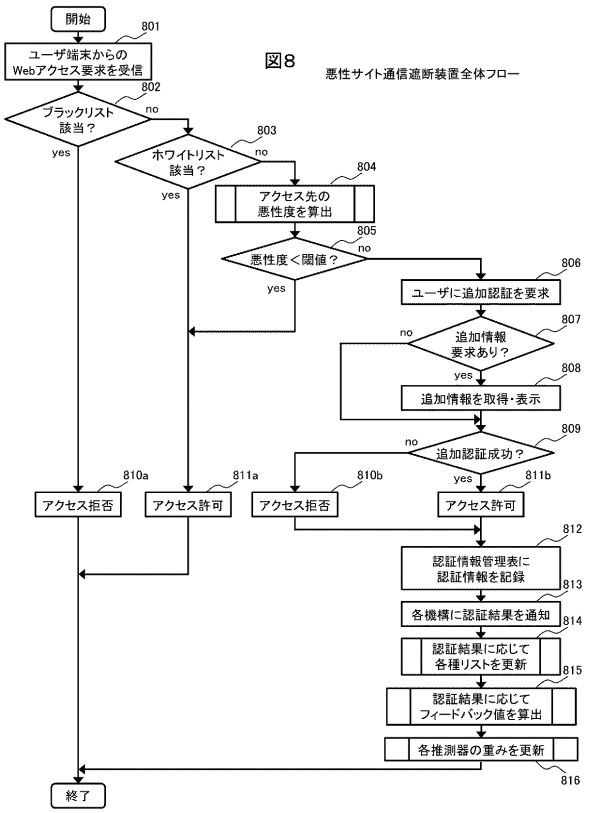
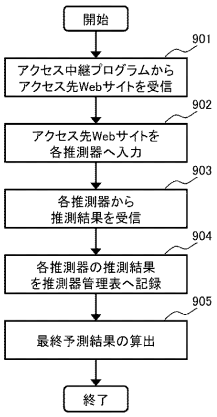


図8 悪性サイト通信遮断装置全体フロー

【図９】

図9

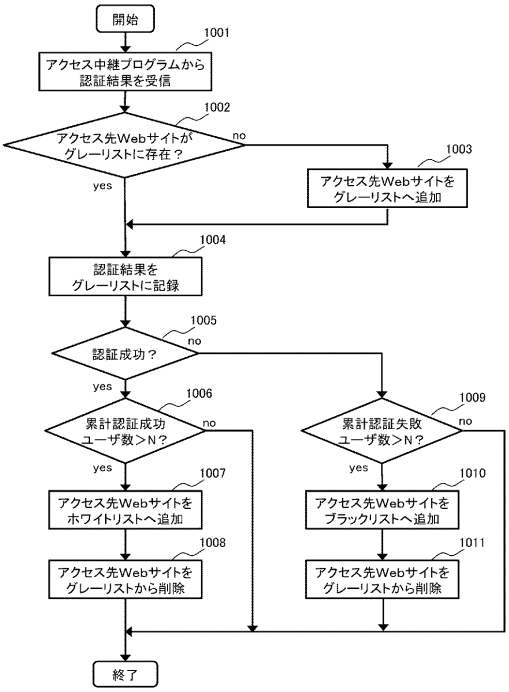
Webサイト悪性度判定フロー



【図１０】

図10

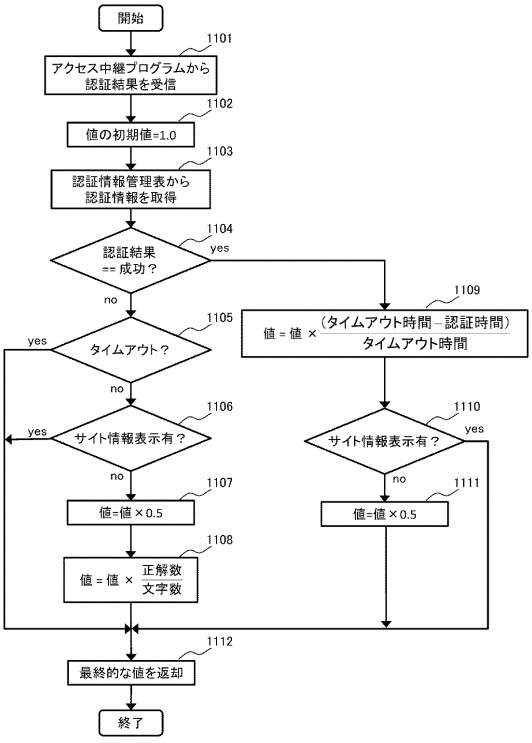
リスト更新フロー



【図１１】

図11

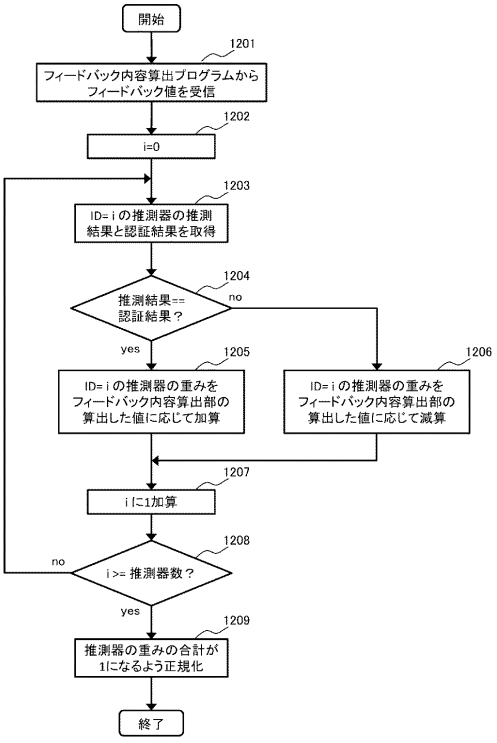
フィードバック内容算出フロー



【図１２】

図12

重み更新フロー



【図１３ａ】

図13a

追加認証画面の一例（追加情報取得前）

【図１３ｂ】

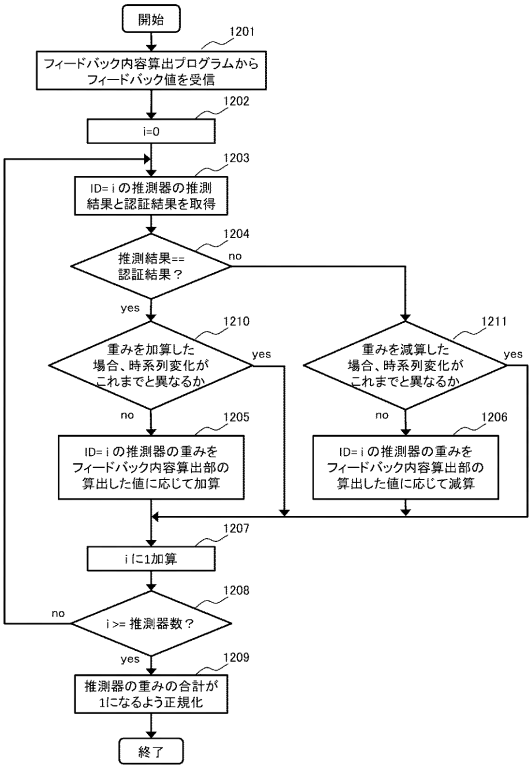
図13b

追加認証画面の一例（追加情報取得後）

【図１４】

図14

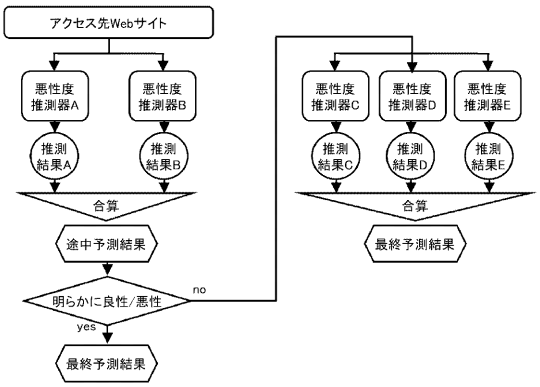
重み更新フロー（時系列変化考慮）



【図１５】

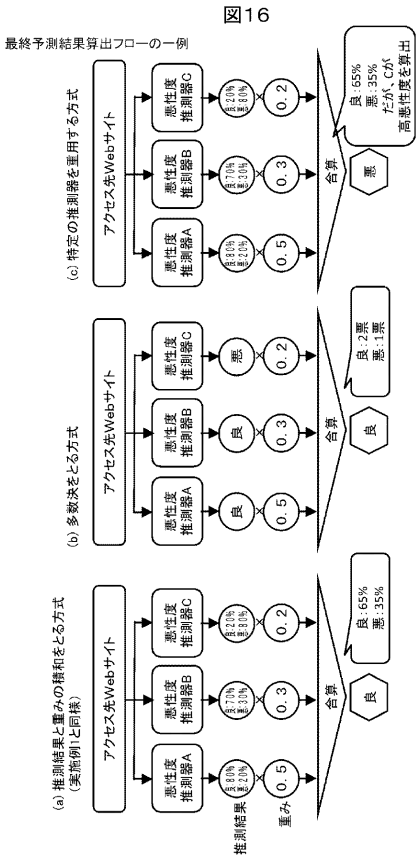
図15

推測器を階層的に並べた場合の悪性度判定例



【図１６】

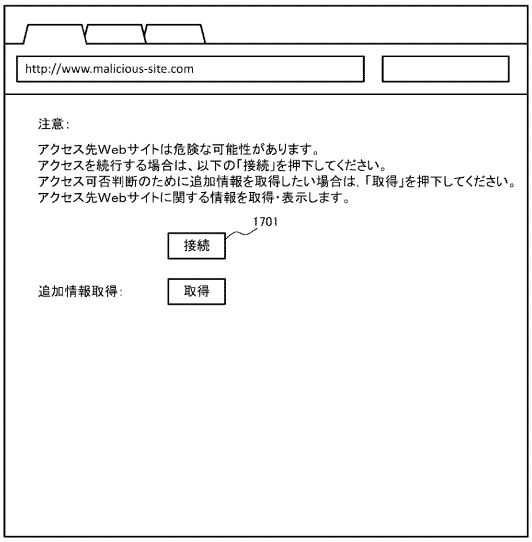
図16



【図１７ａ】

図17a

低難易度な追加認証画面の一例（追加情報取得前）



【図１７ｂ】

図17b

高難易度な追加認証画面の一例（追加情報取得前）