

(19)日本国特許庁(JP)

(12)公開特許公報(A)

(11)公開番号
特開2024-136161
(P2024-136161A)

(43)公開日 令和6年10月4日(2024.10.4)

(51)国際特許分類
G 0 6 F 21/55 (2013.01)

F I
G 0 6 F 21/55

審査請求 未請求 請求項の数 14 O L (全23頁)

(21)出願番号	特願2023-47167(P2023-47167)	(71)出願人	000005108
(22)出願日	令和5年3月23日(2023.3.23)		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	110000176
			弁理士法人一色国際特許事務所
		(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	山岸 伶
			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	重本 倫宏
			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	佐藤 隆行

最終頁に続く

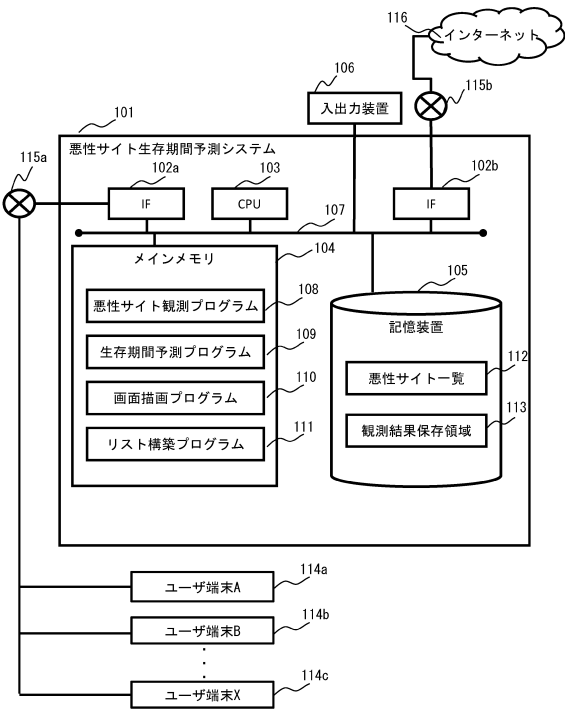
(54)【発明の名称】 悪性サイト生存期間予測システム及び悪性サイト生存期間予測方法

(57)【要約】

【課題】悪性サイトの生存期間を予測することにより、遮断リストや監視リストの構築に係る業務コストや属人性を低減可能とする。

【解決手段】悪性サイト生存期間予測システム101において、ネットワーク116にアクセスする通信装置115と、各悪性サイトの情報を保持する記憶装置101と、各悪性サイトにおける所定事象を観測し、悪性サイトにおける前記事象に関する傾向と当該悪性サイトの生存期間との間の関係性を規定した判定ルールに、観測結果を適用して生存期間を予測し、生存期間に応じて悪性サイトを選択し遮断リスト又は監視リストを生成する演算装置104を含む構成とする。

【選択図】図1



【特許請求の範囲】

【請求項 1】

ネットワークにアクセスする通信装置と、

前記ネットワークにおける各悪性サイトの情報を保持する記憶装置と、

前記各悪性サイトのそれぞれにアクセスし、当該悪性サイトにおける所定事象を観測する処理と、悪性サイトにおける前記事象に関する傾向と当該悪性サイトの生存期間との間の関係性を規定した判定ルールに、前記観測の結果を適用して当該悪性サイトの生存期間を予測する処理と、前記生存期間に応じて前記各悪性サイトのうち所定のものを選択し、遮断リスト又は監視リストを生成する処理を実行する演算装置と、

を備えることを特徴とする悪性サイト生存期間予測システム。

10

【請求項 2】

前記演算装置は、

前記観測の結果、前記予測の結果、及び前記遮断リスト又は前記監視リストの少なくともいずれかを、所定装置に出力する処理をさらに実行するものである、

ことを特徴とする請求項 1 に記載の悪性サイト生存期間予測システム。

【請求項 3】

前記演算装置は、

前記観測の結果に加えて、前記悪性サイトに関して前記ネットワークにて公開されている外部情報を前記判定ルールに適用して前記生存期間を予測するものである、

ことを特徴とする請求項 2 に記載の悪性サイト生存期間予測システム。

20

【請求項 4】

前記演算装置は、

前記観測の結果および前記外部情報に基づき、前記悪性サイトの役割を含む性質を推定し、当該推定の結果も前記判定ルールに適用して前記生存期間の予測を行うものである、

ことを特徴とする請求項 3 に記載の悪性サイト生存期間予測システム。

【請求項 5】

前記演算装置は、

前記観測の結果および前記外部情報を所定のアルゴリズムに適用し、前記悪性サイトに紐づく攻撃グループ又はマルウェアを予測し、当該予測の結果も前記判定ルールに適用することで、前記生存期間の予測を行うものである、

ことを特徴とする請求項 4 に記載の悪性サイト生存期間予測システム。

30

【請求項 6】

前記演算装置は、

前記生存期間の予測結果が示す、前記悪性サイトの役割に応じて監視又は遮断の対象となるリストを生成するものである、

ことを特徴とする請求項 5 に記載の悪性サイト生存期間予測システム。

【請求項 7】

前記演算装置は、

前記予測した生存期間と、悪性サイトの遮断又は観測に関して対処しうるリソース性能とに基づき、前記遮断リスト又は前記監視リストを最大化する処理をさらに実行するものである、

ことを特徴とする請求項 6 に記載の悪性サイト生存期間予測システム。

40

【請求項 8】

情報処理装置が、

ネットワークにアクセスする通信装置と、前記ネットワークにおける各悪性サイトの情報を保持する記憶装置を備えて、

前記各悪性サイトのそれぞれにアクセスし、当該悪性サイトにおける所定事象を観測する処理と、悪性サイトにおける前記事象に関する傾向と当該悪性サイトの生存期間との間の関係性を規定した判定ルールに、前記観測の結果を適用して当該悪性サイトの生存期間を予測する処理と、前記生存期間に応じて前記各悪性サイトのうち所定のものを選択し、

50

遮断リスト又は監視リストを生成する処理を実行する、
ことを特徴とする悪性サイト生存期間予測方法。

【請求項 9】

前記情報処理装置が、
前記観測の結果、前記予測の結果、及び前記遮断リスト又は前記監視リストの少なくともいずれかを、所定装置に出力する処理をさらに実行する、
ことを特徴とする請求項 8 に記載の悪性サイト生存期間予測方法。

【請求項 10】

前記情報処理装置が、
前記観測の結果に加えて、前記悪性サイトに関して前記ネットワークにて公開されている外部情報を前記判定ルールに適用して前記生存期間を予測する、
ことを特徴とする請求項 9 に記載の悪性サイト生存期間予測方法。 10

【請求項 11】

前記情報処理装置が、
前記観測の結果および前記外部情報に基づき、前記悪性サイトの役割を含む性質を推定し、当該推定の結果も前記判定ルールに適用して前記生存期間の予測を行う、
ことを特徴とする請求項 10 に記載の悪性サイト生存期間予測方法。

【請求項 12】

前記情報処理装置が、
前記観測の結果および前記外部情報を所定のアルゴリズムに適用し、前記悪性サイトに紐づく攻撃グループ又はマルウェアを予測し、当該予測の結果も前記判定ルールに適用することで、前記生存期間の予測を行う、
ことを特徴とする請求項 11 に記載の悪性サイト生存期間予測方法。 20

【請求項 13】

前記情報処理装置が、
前記生存期間の予測結果が示す、前記悪性サイトの役割に応じて監視又は遮断の対象となるリストを生成するものである、
ことを特徴とする請求項 12 に記載の悪性サイト生存期間予測方法。

【請求項 14】

前記情報処理装置が、
前記予測した生存期間と、悪性サイトの遮断又は観測に関して対処しうるリソース性能とに基づき、前記遮断リスト又は前記監視リストを最大化する処理をさらに実行する、
ことを特徴とする請求項 13 に記載の悪性サイト生存期間予測方法。 30

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、悪性サイト生存期間予測システム及び悪性サイト生存期間予測方法に関するものである。

【背景技術】

【0002】

悪性サイトの遮断は被害の抑制に有効である。また、そうした悪性サイトを定期的に観測することは、攻撃の解明や攻撃兆候の検出に有用である。

このため、悪性サイトの遮断リストの提供サービスや監視サービスが存在する。また、悪性サイトへの通信を遮断する手法として、遮断リストを活用した通信制御がある。これは、フォワードプロキシ等の層に実装されており、事前に通信を遮断したい悪性サイトを登録しておき、同リストに一致した通信を検知した際に、当該通信を遮断することにより被害を抑制するものである。

【0003】

こうした悪性サイトに対応する従来技術としては、例えば、未知の悪性サイトへのアクセスを検出可能とすると共に該検出にかかる負担を軽減する技術（特許文献 1 参照）など 50

が提案されている。

【0004】

この技術は、観測装置と、前記観測装置と通信回線で接続される解析装置とを有する監視システムであり、前記観測装置は、ユーザによるWebページへのアクセスに関する情報を収集するデータ観測部と、前記データ観測部で収集された情報を前記解析装置へ送信する送信部と、を備え、前記解析装置は、前記観測装置から送信された情報を受信する受信部と、前記受信部で受信された情報に基づいて特定のページ遷移方法の検出を行い、前記特定のページ遷移方法の検出結果に基づいて前記Webページへのアクセスからダウンロードされたコンテンツの悪性を判断する解析部と、前記解析部により悪性が疑われると判断されたコンテンツだけを解析の対象に決定する

10

解析対象決定部と、を備えた監視システムにかかるものである。

【先行技術文献】

【特許文献】

【0005】

【特許文献1】特開2016-45887号公報

【非特許文献】

【0006】

【非特許文献1】Nappa, A., Xu, Z., Rafique, M.Z., Caballero, J., and Gu, G.: CyberProbe: Towards Internet-Scale Active Detection of Malicious Servers, Proc. 2014 Network and Distributed System Security Symposium (NDSS2014), pp.1-15(2014). <https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiGmd-D0tD8AhXbZt4KHUyqCQoQFnoECAUQAQ&url=https%3A%2F%2Fflirias.kuleuven.be%2Fretrieve%2F384185&usg=AOvVaw3rKJj5MlZX684yxfDdtlzk>

20

【非特許文献2】Soska, K. and Christin, N.: Automatically detecting vulnerable websites before they turn malicious, Proc. the 23rd USENIX conference on Security Symposium (SEC2014), pp. 625-640 (2014).<https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/soska>

30

【発明の概要】

【発明が解決しようとする課題】

【0007】

ところが、悪性サイトの数は無数に存在し、かつ日々増加する。そのため、その全てを遮断や観測を行うことは非現実的である。

そこで、その時点での状態等々を基に、より優先度が高いものに絞って遮断リストや監視リストを構築することが必要であるが、そうした作業は実施コストが大きく、属人性も高い。

【0008】

従来技術においては、WEBサイトを監視し、そこでのページ遷移情報等から悪性サイト検出する手法が存在する。しかしながら、遮断／観測の対象となる悪性サイトの棚卸／選定に寄与する、生存期間に関する情報の提供は提案されていない。

40

【0009】

また他にも、観測によって活性状態にある悪性サイトを検出する手法も存在する。しかし、悪性サイトの性質や生存期間に関する情報を提供することはスコープ外である。

【0010】

つまり、上述のように、悪性サイトの監視に焦点を当てた従来技術は多く存在するものの、遮断／観測の対象とする悪性サイトの棚卸／選定を目的とした技術は提案されていない状況にある。よって、既に述べた遮断リストや監視リストの構築に係る業務コストの大きさや属人性の高さの解決には至っていない。

【0011】

50

そこで本発明の目的は、悪性サイトの生存期間を予測することにより、遮断リストや監視リストの構築に係る業務コストや属人性を低減可能とする技術を提供することにある。

【課題を解決するための手段】

【0012】

上記課題を解決する本発明の悪性サイト生存期間予測システムは、ネットワークにアクセスする通信装置と、前記ネットワークにおける各悪性サイトの情報を保持する記憶装置と、前記各悪性サイトのそれぞれにアクセスし、当該悪性サイトにおける所定事象を観測する処理と、悪性サイトにおける前記事象に関する傾向と当該悪性サイトの生存期間との間の関係性を規定した判定ルールに、前記観測の結果を適用して当該悪性サイトの生存期間を予測する処理と、前記生存期間に応じて前記各悪性サイトのうち所定のものを選択し、遮断リスト又は監視リストを生成する処理を実行する演算装置と、を備えることを特徴とする。

10

また、本発明の悪性サイト生存期間予測方法は、情報処理装置が、ネットワークにアクセスする通信装置と、前記ネットワークにおける各悪性サイトの情報を保持する記憶装置を備えて、前記各悪性サイトのそれぞれにアクセスし、当該悪性サイトにおける所定事象を観測する処理と、悪性サイトにおける前記事象に関する傾向と当該悪性サイトの生存期間との間の関係性を規定した判定ルールに、前記観測の結果を適用して当該悪性サイトの生存期間を予測する処理と、前記生存期間に応じて前記各悪性サイトのうち所定のものを選択し、遮断リスト又は監視リストを生成する処理を実行する、ことを特徴とするとする。

20

【発明の効果】

【0013】

本発明によれば、悪性サイトの生存期間を予測することにより、遮断リストや監視リストの構築に係る業務コストや属人性を低減可能となる。

【図面の簡単な説明】

【0014】

【図1】本発明の実施例1に係る悪性サイト生存期間予測システムの構成例を示した図である。

【図2】本発明の実施例1に係る悪性サイト一覧の一例を示す図である。

【図3】本発明の実施例1に係る観測結果保存領域の一例を示す図である。

30

【図4】本発明の実施例1に係る全体処理フローを示す図である。

【図5】本発明の実施例1に係る悪性サイト観測の処理フローを示す図である。

【図6】本発明の実施例1に係る生存期間予測の処理フローを示す図である。

【図7】本発明の実施例1に係る画面描写の処理フローを示す図である。

【図8】本発明の実施例1に係る画面の一例を示す図である。

【図9】本発明の実施例1に係るリスト構築の処理フローを示す図である。

【図10】本発明の実施例2に係る悪性サイト生存期間予測システムの構成例を示した図である。

【図11】本発明の実施例2に係る観測間隔策定の処理フローを示す図である。

【図12】本発明の実施例2に係る性質予測の処理フローを示す図である。

40

【図13】本発明の実施例2に係るバックグラウンド予測の処理フローを示す図である。

【図14】本発明の実施例3に係る悪性サイト生存期間予測システムの構成例を示した図である。

【発明を実施するための形態】

【0015】

以下、本発明の実施例を、図面を用いて説明する。ただし、本発明は以下に示す実施例の記載内容に限定して解釈されるものではない。本発明の思想ないし趣旨から逸脱しない範囲で、その具体的構成を変更し得ることは当業者であれば容易に理解される。

以下に説明する発明の構成において、同一又は類似する構成又は機能には同一の符号を付し、重複する説明は省略する。

50

【0016】

本明細書等における「第1」、「第2」、「第3」等の表記は、構成要素を識別するために付するものであり、必ずしも、数又は順序を限定するものではない。

【0017】

図面等において示す各構成の位置、大きさ、形状、及び範囲等は、発明の理解を容易にするため、実際の位置、大きさ、形状、及び範囲等を表していない場合がある。したがって、本発明では、図面等に開示された位置、大きさ、形状、及び範囲等に限定されない。

[実施例1]

実施例1では、オンプレミスで悪性サイトの生存期間を予測することにより、遮断リストや監視リストの構築に係る業務コストや属人性の低減を図る場合の悪性サイト生存期間予測システムの処理について示す。

<ネットワーク構成>

以下に本発明の実施形態について図面を用いて詳細に説明する。図1は、本実施例における悪性サイト生存期間予測システム101を含むネットワーク構成図である。

【0018】

図1に示す悪性サイト生存期間予測システム101は、悪性サイトの生存期間を予測することにより、遮断リストや監視リストの構築に係る業務コストや属人性を低減可能とするコンピュータシステムである。

【0019】

実施例1に係る悪性サイト生存期間予測システム101は、ユーザが操作するユーザ端末114と、インターネット116及びネットワーク115を介して接続される。よって、ユーザ端末114を含めて悪性サイト生存期間予測システムと捉えるとしてもよい。

【0020】

悪性サイト生存期間予測システム101は、CPU (Central Processing Unit) 103と、メインメモリ104と、記憶装置105と、IF (インタフェース) 102と、入出力装置106と、これらの各装置を接続する通信路107と、を備えている。

【0021】

このうち、IF 102は、ユーザ端末114など他装置と通信を行なうための通信装置である。

【0022】

また、CPU (Central Processing Unit) 103は、メインメモリ104に格納された悪性サイト観測プログラム108を実行することにより、悪性サイトの観測を、また、生存期間予測プログラム109を実行することにより、接続先の生存期間の予測を、また、画面描写プログラム110を実行することにより、上述の各プログラムによる処理結果 (観測の結果、悪性度や対処優先度等の情報) の出力を、また、リスト構築プログラム111を実行することにより、悪性サイトの遮断および観測のリスト生成の各機能を実装することとなる。

【0023】

また、メインメモリ104は、上述のCPU 103が処理を実行するために必要なデータを格納する揮発性記憶素子で構成されたものである。

【0024】

また、記憶装置105は、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不揮発性記憶素子で構成されたものである。

【0025】

また、入出力装置106は、キーボード、ディスプレイなどの入出力を行う装置である。

【0026】

10

20

30

40

50

また、通信路 107 は、これらの各装置を接続するバスやケーブルなどの情報伝達媒体である。

【0027】

なお、上述の記憶装置 105 には、悪性サイトを管理する悪性サイト一覧 112、及び観測結果を保存する観測結果保存領域 113 が格納されている。

【0028】

上記の各プログラムやデータは、あらかじめメインメモリ 104 または記憶装置 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、または IF 102 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】

なお、図 1 で説明した、悪性サイト生存期間予測システムの構成は、一例であって、これに限定されない。

<データ構造例>

続いて、本実施形態の悪性サイト生存期間予測システム 101 が用いる各種情報について説明する。図 2 は、悪性サイト一覧 112 の一例を示す図である。

【0030】

図 2 に示すように、悪性サイト一覧 112 は、例えば、接続先 ID 201 と、接続先 202 と、観測スパン 203 と、観測日時 204 と、予測生存期間 205 とを含んで構成される。

【0031】

このうち接続先 ID 201 は、観測対象の接続先を一意に識別するための識別情報を格納するフィールドである。実施例 1 の接続先 ID 201 には数字が識別情報として格納される。

【0032】

また、接続先 202 は、観測対象の接続先の URL を格納するフィールドである。例えば、接続先 ID 201 が「0」のエントリに対応する接続先は、「search.example.com/」であることを表す。

【0033】

また、観測スパン 203 は、該接続先を観測する頻度を表す。例えば、接続先 ID 201 が「0」のエントリについては、4 時間ごとに観測を試みることを表す。

【0034】

また、観測日時 204 は、該接続先を観測した日時を表す。例えば、接続先 ID 201 が「0」のエントリのうち、直近の観測は、2023 年 01 月 01 日の 04 時 00 分 00 秒に行ったことを表す。本発明は、観測日時 204 に格納される時刻のデータ形式に限定されない。Unixtime 等、時刻が判別できるデータ形式であれば、どのようなデータ形式を用いてもよい。

【0035】

また、予測生存期間 205 は、該接続先（の悪性サイト）について予測した生存期間を表す。例えば、接続先 ID 201 が「0」について、最新の「2023 年 01 月 01 日の 04 時 00 分 00 秒」に観測した結果を用いて、その時点からの生存期間の予測結果を表す。

【0036】

なお、図 2 で説明した、悪性サイト一覧は、一例であって、これに限定されない。

【0037】

図 3 は、観測結果保存領域 113 の一例を示す図である。図 3 に示すように、観測結果保存領域 113 は、例えば、接続先 ID 301 と、接続先 302 と、観測日時 303 と、ステータスコード 304 と、コンテンツ 305 とを含んで構成される。

【0038】

10

20

30

40

50

このうち接続先ID301は、観測対象の接続先を一意に識別するための識別情報を格納するフィールドである。実施例1の接続先ID301には数字が識別情報として格納される。

【0039】

また、接続先302は、観測対象の接続先のURLを格納するフィールドである。例えば、接続先ID301が「0」のエントリに対応する接続先は、「search.example.com/」であることを表す。

【0040】

また、観測日時303は、該接続先を観測した日時を表す。例えば、接続先ID301が「0」のエントリのうち、直近の観測は、「2023年01月01日の04時00分00秒」に行ったことを表す。本発明は、観測日時303に格納される時刻のデータ形式に限定されない。Unixtime等、時刻が判別できるデータ形式であれば、どのようなデータ形式を用いてもよい。

【0041】

また、ステータスコード304は、観測時の該接続先のステータスコードを格納するフィールドである。例えば、接続先ID301が「0」の接続先を「2023年01月01日の04時00分00秒」に観測した際のステータスコードが「200」であったことを表す。なお、ステータスコードは、HTTPのレスポンスとして接続先のサーバが応答してくるコードであって、情報レスポンス、成功レスポンス、リダイレクトメッセージ、クライアントエラーレスポンス、及びサーバーエラーレスポンスといった種類のものが存在する。

【0042】

また、コンテンツ305は、観測時に該接続先から得られたコンテンツを格納するフィールドである。例えば、接続先ID301が「0」の接続先を「2023年01月01日の04時00分00秒」に観測した際に得られたコンテンツが「1.exe」であったことを表す。なお、観測結果として格納する情報は、これに限定されない。

【0043】

なお、図3で説明した、観測結果保存領域は、一例であって、これに限定されない。
<フロー例：全体フロー>

以下、本実施形態における悪性サイト生存期間予測方法の実際手順について図に基づき説明する。以下で説明する悪性サイト生存期間予測方法に対応する各種動作は、悪性サイト生存期間予測システム101がメモリ等に読み出して実行するプログラムによって実現される。そして、このプログラムは、以下に説明される各種の動作を行うためのコードから構成されている。

【0044】

図4は、実施例1における悪性サイト生存期間予測方法のフロー例を示す図であり、具体的には、悪性サイト生存期間予測システム101が実行する処理の概要を説明するフローチャートである。

【0045】

ここで、悪性サイト生存期間予測システム101は、周期的に、以下で説明する処理を実行する（ステップ401）。

【0046】

まず、悪性サイト生存期間予測システム101は、悪性サイトの観測を行う（ステップ402）。この悪性サイト観測に関する詳細フローは、図5を用いて後述するものとする。

【0047】

次に、悪性サイト生存期間予測システム101は、ステップ402による観測結果を用いて、該悪性サイトの生存期間予測する（ステップ403）。この生存期間予測の詳細フローは、図6を用いて後述するものとする。

【0048】

悪性サイト生存期間予測システム101は、全悪性サイトに対して上記処理を実施し、フローを終了する。

【0049】

なお、図4で説明した、悪性サイト生存期間予測システムの処理フローは、一例であって、これに限定されない。

<フロー例：悪性サイト観測>

図5は、実施例1の接続先悪性度判定システム101が実行する悪性サイト観測処理（上述のステップ402）の一例を説明するフローチャートである。

【0050】

CPU103によって実行される悪性サイト観測プログラム108は、例えば、ユーザー端末114から実行指示を受け付けた場合、以下で説明する処理を開始する。

【0051】

悪性サイト観測プログラム108は、悪性サイト一覧112から観測対象の接続先の一覧を取得する（ステップ501）。ここでは、接続先ID201から構成されるエントリを含む一覧が取得されるものとする。

【0052】

次に、悪性サイト観測プログラム108は、悪性サイト一覧112の接続先IDを意味する変数*i*に初期値0を設定する（ステップ502）。

【0053】

次に、悪性サイト観測プログラム108は、接続先IDが*i*の接続先について処理を開始する（ステップ503）。

【0054】

次に、悪性サイト観測プログラム108は、悪性サイト一覧112の直近のエントリにおける観測日時204と観測スパン203を参照し、該接続先の最終観測日時からプログラム実行までの経過時間を算出することにより、接続先が観測スパンに到達しているか判定する（ステップ504）。

【0055】

この判定の結果、該接続先が観測スパンに到達していなかった場合（ステップ504：No）、悪性サイト観測プログラム108は、該接続先に関する処理を終了し、ステップ507へ進む。

【0056】

一方、上述の判定の結果、該接続先が観測スパンに到達していた場合（ステップ504：Yes）、悪性サイト観測プログラム108は、ステップ505へ進む。

【0057】

次に、悪性サイト観測プログラム108は、該接続先について、観測を実施する（ステップ505）。この観測に際しては、例えば、ブラウザを用いて該接続先にアクセスし、その応答結果を取得する。応答結果の一例としては、既に述べたステータスコードを想定できる。

【0058】

次に、悪性サイト観測プログラム108は、上述のステップ505で得た観測結果を、観測結果保存領域113における該接続先の接続先IDに対応するエントリへ保存する（ステップ506）。

【0059】

次に、悪性サイト観測プログラム108は、変数*i*に1を加算し、ステップ508へ進む（ステップ507）。

【0060】

次に、悪性サイト観測プログラム108は、変数*i*と、悪性サイト一覧112を参照することによって得ることのできる接続先数とを比較する。

【0061】

10

20

30

40

50

この比較の結果、変数 i が接続先数に満たない場合（ステップ 508：No）、悪性サイト観測プログラム 108 は、ステップ 503 に戻る。

【0062】

他方、上述の比較の結果、変数 i が接続先数を上回っていた場合（ステップ 508：Yes）、悪性サイト観測プログラム 108 は、処理を終了する（ステップ 508）。

【0063】

なお、図 5 で説明した、悪性サイト観測処理の方法は、一例であって、これに限定されない。

<フロー例：生存期間予測>

図 6 は、実施例 1 の接続先悪性度判定システム 101 が実行する生存期間予測処理の一例を説明するフローチャートである。

【0064】

CPU 103 によって実行される生存期間予測プログラム 109 は、ユーザ端末 114 から実行指示を受け付けた場合、以下で説明する処理を開始する。

【0065】

生存期間予測プログラム 109 は、悪性サイト一覧 112 から観測対象の接続先の一覧を取得する（ステップ 601）。ここでは、接続先 ID 201 から構成されるエントリを含む一覧が取得されるものとする。

【0066】

次に、生存期間予測プログラム 109 は、悪性サイト一覧 112 の接続先 ID を意味する変数 i に初期値 0 を設定する（ステップ 602）。

【0067】

次に、生存期間予測プログラム 109 は、接続先 ID が i の接続先について処理を開始する（ステップ 603）。

【0068】

次に、生存期間予測プログラム 109 は、観測結果保存領域 113 を参照し、該接続先について、前回の予測時から追加の観測結果があるか確認する（ステップ 604）。

【0069】

この際、追加の観測結果がなかった場合（ステップ 604：No）、生存期間予測プログラム 109 は、該接続先に関する処理を終了し、ステップ 608 へ進む。

【0070】

一方、追加の観測結果があった場合（ステップ 604：Yes）、生存期間予測プログラム 109 は、ステップ 605 へ進む。

【0071】

次に、生存期間予測プログラム 109 は、該接続先に係る外部情報を取得する（ステップ 605）。外部情報としては、例えば、WHOIS 情報、DNS 情報、証明書情報等を取得する。

【0072】

次に、生存期間予測プログラム 109 は、観測結果保存領域 113 から得た観測結果やステップ 605 で得た外部情報を、所定の判定ルール（例：悪性サイトにおける所定の事象に関する傾向と当該悪性サイトの生存期間との間の関係性を機械学習したエンジンなど）に適用して該接続先の生存期間を予測する（ステップ 606）。

【0073】

なお、上述の事象とは、悪性サイトからの応答であるステータスコードの種類、当該悪性サイトの役割、WHOIS 情報の外部情報、など様々なものを採用しうる。

【0074】

次に、生存期間予測プログラム 109 は、ステップ 606 で得た生存期間の予測結果を悪性サイト一覧 112 における該接続先の接続先 ID に対応するエントリの、予測生存期間 205 へ保存する（ステップ 607）。

【0075】

10

20

30

40

50

次に、生存期間予測プログラム 109 は、変数 i に 1 を加算し、ステップ 609 へ進む（ステップ 608）。

【0076】

次に、生存期間予測プログラム 109 は、変数 i と、悪性サイト一覧 112 を参照することによって得ることのできる接続先数とを比較する（ステップ 609）。

【0077】

上述の比較の結果、変数 i が接続先数に満たない場合（ステップ 609：No）、生存期間予測プログラム 109 は、ステップ 603 に戻る。

【0078】

また、上述の比較の結果、変数 i が接続先数を上回っていた場合（ステップ 609：Yes）、生存期間予測プログラム 109 は、処理を終了する（ステップ 609）。

【0079】

なお、図 6 で説明した、生存期間予測処理の方法は、一例であって、これに限定されない。例えば、上記の例で述べた以外の情報を用いて接続先の生存期間を予測しても良い。さらに、予測した該接続先の性質に基づいて観測スパンを変動させてもよい。例えば、短期間で性質を変え得るものは短い間隔で観測し、生存期間は長いが期間中に性質を変えないものは長い間隔で観測する等の方策が挙げられる。

<フロー例：画面描写>

悪性サイト生存期間予測システム 101 は、図 4 で説明した処理とは別に、ユーザに対して各種情報を表示するための画面描写処理を実行する。図 7 は、実施例 1 の悪性サイト生存期間予測システム 101 が実行する画面描写処理の一例を説明するフローチャートである。

【0080】

CPU 103 によって実行される画面描写プログラム 110 は、ユーザ端末 114 から実行指示を受け付けた場合、以下で説明する処理を開始する。

【0081】

画面描写プログラム 110 は、悪性サイト一覧 112 から観測対象の接続先の一覧を取得する（ステップ 701）。ここでは、接続先 ID 201 から構成されるエントリを含む一覧が取得されるものとする。

【0082】

画面描写プログラム 110 は、観測結果保存領域 113 から接続先の観測結果を取得する（ステップ 702）。ここでは、接続先 ID 301 から構成されるエントリを含む一覧が取得されるものとする。

【0083】

画面描写プログラム 110 は、描画対象の接続先に関する情報を画面データに生成し、これをユーザ端末 114 に配信して表示させ（ステップ 703）、処理を終了する。

【0084】

なお、図 7 で説明した、画面描写の方法は、一例であって、これに限定されない。

【0085】

図 8 は、実施例 1 の悪性サイト生存期間予測システム 101 における画面描写プログラム 110 が生成し、ユーザ端末 114 で表示させた悪性サイト生存期間予測結果描写画面 800 の一例である。

【0086】

図 8 における画面 800 は、悪性サイト概要 801 と、予測生存期間 802 と、観測結果 803 と、を含む。

【0087】

このうち悪性サイト概要 801 は、描写対象の接続先に関する基本的な情報を示すものとなる。例えば、接続先 ID、接続先、観測スパン、観測日時、及び予測生存期間といった情報が含まれる。

【0088】

10

20

30

40

50

また、予測生存期間 802 は、該接続先について生存期間を予測した結果である。

【0089】

また、観測結果 803 は、描写対象の接続先を観測した結であって、例えば、接続先 ID、接続先、観測日時、ステータスコード、コンテンツ、及び形式といった情報が含まれる。

【0090】

上述のコンテンツは、悪性サイトがダウンロード可能に提供しているファイルや、ステータスコードを含む画面データなどを想定しうる。

【0091】

上述のように、該接続先について、その予測生存期間を中心に表示することによって、分析者をはじめとしたユーザに対して、監視リストや遮断リストを作成するに際の支援効果が期待される。

10

【0092】

なお、今回は実施例 1 に係る各プログラムの実行結果を基に描写画面を例示したが、一例であって、これに限定されない。例えば、接続先に関連するものであれば、どのような情報をどのような形式で描写しても良い。

<フロー例：遮断リスト提供>

悪性サイト生存期間予測システム 101 は、図 4 で説明した処理とは別に、リスト構築処理を実行する。図 9 は、実施例 1 の悪性サイト生存期間予測システム 101 が実行する遮断リスト提供処理の一例を説明するフローチャートである。

20

【0093】

CPU 103 によって実行されるリスト構築プログラム 111 は、ユーザ端末 114 からの実行指示を受け付けた場合、以下で説明する処理を開始する。

【0094】

リスト構築プログラム 111 は、利用者のユーザ端末 114 から、リストの上限数の指定を受け付ける（ステップ 901）。

【0095】

リスト構築プログラム 111 は、悪性サイト一覧 112 から悪性サイトの情報を取得する（ステップ 902）。

【0096】

また、リスト構築プログラム 111 は、予測生存期間が長い順に、悪性サイト一覧 112 から、ステップ 901 で受け付けた上限数まで悪性サイトを抽出する（ステップ 903）。

30

【0097】

リスト構築プログラム 111 は、ステップ 903 で抽出した悪性サイト群を、遮断リストとして出力し（ステップ 904）、処理を終了する。この際、他の機器、例えば実際に通信を遮断する役割を担うネットワーク機器と IF 102 を介して連携する形が考えられる。

【0098】

なお、図 9 で説明した、リスト構築処理の方法は、一例であって、これに限定されない。例えば、予測生存期間だけでなく、該接続先の悪性度等の別の要素を考慮してリストを構築してもよい。

40

【0099】

また、リストの利用先を考慮してリストを作成してもよい。例えば、悪性サイトを監視するには可能な限り多種の監視結果を得たいため、監視リストとしては、コンテンツを次々と変更するような悪性サイトを優先的にリストに加える等の方策が考えられる。加えて、上記の例ではリストの上限数はユーザが入力したが、予測した生存期間等を活用し、遮断リストの容量や観測システムの観測可能数のようなリソースを考慮した上で、遮断リストの遮断性能や監視リストの監視可能性を最大化する機能を具備してもよい。

【0100】

50

悪性サイトの遮断や観測は有用な一方で、悪性サイトの数は無数に存在し、かつ日々増加するため、その全てを遮断や観測することは非現実的である。このため、その時点での状態等々を基に、より優先度が高いものに絞って遮断リストや監視リストを構築することが必要であり、実施コストが大きく属人性も高いという課題があった。

【0101】

実施例1によれば、悪性サイト生存期間予測システム101は、悪性サイトの生存期間を予測するとともに、その結果を用いて遮断リストや監視リストを自動で構築する。これにより、遮断リストや監視リストの構築に係る業務コストや属人性を低減することが期待される。

[実施例2]

実施例2では、悪性サイトの観測や解析に係る支援機能を具備し、より高度かつ省力的な分析を可能にする悪性サイト生存期間予測システムの処理について示す。以下、実施例1との差異を中心に実施例2について説明する。

【0102】

図10は、本発明の実施例2に係る悪性サイト生存期間予測システム1001の構成例を示す図である。実施例2の計算機システムの構成は実施例1と同一である。また、実施例2の悪性サイト生存期間予測システムのハードウェア構成は実施例1と同一である。

【0103】

実施例2のプログラム構成として、実施例1のものに加えて、観測間隔策定プログラム1012、性質予測プログラム1013、バックグラウンド予測プログラム1014を有する。また、実施例2の悪性サイト観測プログラム1008、生存期間予測プログラム1009、画面描画プログラム1010、リスト構築プログラム1011の処理は、実施例1と同一である。

【0104】

実施例2のデータ構造は実施例1と同一である。

【0105】

なお、図10で説明した、実施例2に係る悪性サイト生存期間予測システムの構成は、一例であって、これに限定されない。

<フロー例：観測間隔策定>

図11は、実施例2の接続先悪性度判定システム1001が実行する観測間隔策定処理の一例を説明するフローチャートである。

【0106】

CPU1003によって実行される観測間隔策定プログラム1012は、ユーザ端末114から実行指示を受け付けた場合、以下で説明する処理を開始する。

【0107】

観測間隔策定プログラム1012は、悪性サイト一覧1015から観測対象の接続先の一覧を取得する（ステップ1101）。ここでは、接続先IDから構成されるエントリを含む一覧が取得されるものとする。

【0108】

次に、観測間隔策定プログラム1012は、悪性サイト一覧1015の接続先IDを意味する変数*i*に初期値0を設定する（ステップ1102）。

【0109】

次に、観測間隔策定プログラム1012は、接続先IDが*i*の接続先について処理を開始する（ステップ1103）。

【0110】

次に、観測間隔策定プログラム1012は、観測結果保存領域1016を参照し、該接続先について、観測結果や外部情報の各項目に変化があるか確認する（ステップ1104）。

【0111】

上述の確認の結果、変化があった場合（ステップ1104：Yes）、観測間隔策定プ

10

20

30

40

50

プログラム 1012 は、該接続先に関する処理を終了し、ステップ 1107 へ進む。

【0112】

一方、上述の確認の結果、変化がなかった場合（ステップ 1104：No）、観測間隔策定プログラム 1012 は、ステップ 1105 へ進む。

【0113】

次に、観測間隔策定プログラム 1012 は、該接続先の観測スパンを、例えば、デフォルト値よりも一定割合で長大化させる（ステップ 1105）。

【0114】

次に、観測間隔策定プログラム 1012 は、ステップ 1105 で長大化した観測スパンを悪性サイト一覧 1015 へ反映する（ステップ 1106）。

【0115】

次に、観測間隔策定プログラム 1012 は、変数 i に 1 を加算し、ステップ 1108 へ進む（ステップ 1107）。

【0116】

次に、観測間隔策定プログラム 1012 は、変数 i と、悪性サイト一覧 1015 を参照することによって得ることのできる接続先数とを比較する（ステップ 1108）。

【0117】

ここで、変数 i が接続先数に満たない場合（ステップ 1108：No）、観測間隔策定プログラム 1012 は、ステップ 1103 に戻る。

【0118】

一方、変数 i が接続先数を上回っていた場合（ステップ 1108：Yes）、観測間隔策定プログラム 1012 は、処理を終了する。

【0119】

なお、図 11 で説明した、観測間隔策定処理の方法は、一例であって、これに限定されない。例えば、観測結果や外部情報に変化があった場合に観測スパンを短縮してもよい。
＜フロー例：性質予測＞

図 12 は、実施例 1 の接続先悪性度判定システム 1001 が実行する性質予測処理の一例を説明するフローチャートである。

【0120】

CPU 1003 によって実行される性質予測プログラム 1013 は、ユーザ端末 114 から実行指示を受け付けた場合、以下で説明する処理を開始する。

【0121】

性質予測プログラム 1013 は、悪性サイト一覧 1015 から観測対象の接続先の一覧を取得する（ステップ 1201）。ここでは、接続先 ID から構成されるエントリを含む一覧が取得されるものとする。

【0122】

次に、性質予測プログラム 1013 は、悪性サイト一覧 1015 の接続先 ID を意味する変数 i に初期値 0 を設定する（ステップ 1202）。

【0123】

次に、性質予測プログラム 1013 は、接続先 ID が i の接続先について処理を開始する（ステップ 1203）。

【0124】

次に、性質予測プログラム 1013 は、観測結果保存領域 1016 を参照し、該接続先について、前回の予測時から追加の観測結果があるか確認する（ステップ 1204）。

【0125】

この確認の結果、追加の観測結果がなかった場合（ステップ 1204：No）、性質予測プログラム 1013 は、該接続先に関する処理を終了し、ステップ 1207 へ進む。

【0126】

一方、上述の確認の結果、追加の観測結果があった場合（ステップ 1204：Yes）、生存期間予測プログラム 1013 は、ステップ 1205 へ進む。

10

20

30

40

50

【0127】

次に、性質予測プログラム1013は、該接続先に係る外部情報を取得する（ステップ1205）。こうした外部情報としては、例えば、WHOIS情報、DNS情報、証明書情報等を取得する。

【0128】

次に、性質予測プログラム1013は、ここまでで得ている観測結果やステップ1205で取得した外部情報などを、所定の判定ルールに適用して該接続先の性質を予測する（ステップ1206）。ここでの性質は、例えば、短期間で次々にコンテンツが変わるサイト、終了まで性質を変えないサイト、等のようなものを指す。また、上述の判定ルールは、観測結果や外部情報が含む各事項の値と、悪性サイトの性質との感の関係性について機械学習で得た判定エンジンといったものを、一例として想定できる。

10

【0129】

次に、性質予測プログラム1013は、変数*i*に1を加算し、ステップ1108へ進む（ステップ1207）。

【0130】

次に、性質予測プログラム1013は、変数*i*と、悪性サイト一覧1015を参照することによって得ることのできる接続先数とを比較する（ステップ1208）。

【0131】

上述の比較の結果、変数*i*が接続先数に満たない場合（ステップ1208：No）、性質予測プログラム1013は、ステップ1203に戻る。

20

【0132】

一方、上述の確認の結果、変数*i*が接続先数を上回っていた場合（ステップ1208：Yes）、性質予測プログラム1013は、処理を終了する（ステップ1208）。

【0133】

なお、図12で説明した、性質予測処理の方法は、一例であって、これに限定されない。

<フロー例：バックグラウンド予測>

図13は、実施例1の接続先悪性度判定システム1001が実行するバックグラウンド予測処理の一例を説明するフローチャートである。

【0134】

CPU1003によって実行されるバックグラウンド予測プログラム1014は、ユーザ端末114から実行指示を受け付けた場合、以下で説明する処理を開始する。

30

【0135】

バックグラウンド予測プログラム1014は、悪性サイト一覧1015から観測対象の接続先の一覧を取得する（ステップ1301）。ここでは、接続先IDから構成されるエントリを含む一覧が取得されるものとする。

【0136】

次に、バックグラウンド予測プログラム1014は、悪性サイト一覧1015の接続先IDを意味する変数*i*に初期値0を設定する（ステップ1302）。

【0137】

次に、バックグラウンド予測プログラム1014は、接続先IDが*i*の接続先について処理を開始する（ステップ1303）。

40

【0138】

次に、バックグラウンド予測プログラム1014は、観測結果保存領域1016を参照し、該接続先について、前回の予測時から追加の観測結果があるか確認する（ステップ1304）。

【0139】

上述の確認の結果、追加の観測結果がなかった場合（ステップ1304：No）、バックグラウンド予測プログラム1014は、該接続先に関する処理を終了し、ステップ1307へ進む。

50

【0140】

一方、上述の確認の結果、追加の観測結果があった場合（ステップ1304：Yes）、バックグラウンド予測プログラム1014は、ステップ1305へ進む。

【0141】

次に、バックグラウンド予測プログラム1014は、該接続先に係る外部情報を取得する（ステップ1305）。なお、外部情報としては、例えば、WHOIS情報、DNS情報、証明書情報等を取得するものとする。

【0142】

次に、バックグラウンド予測プログラム1014は、ここまでで得ている観測結果や、ステップ1305で取得した外部情報などを用いて、該接続先のバックグラウンドを予測する（ステップ1306）。ここでのバックグラウンドは、例えば、該接続先に紐づく攻撃グループやマルウェアを指す。

【0143】

次に、バックグラウンド予測プログラム1014は、変数*i*に1を加算し、ステップ1108へ進む（ステップ1307）。

【0144】

次に、バックグラウンド予測プログラム1014は、変数*i*と、悪性サイト一覧1015を参照することによって得ることのできる接続先数とを比較する（ステップ1308）。

【0145】

上述の比較の結果、変数*i*が接続先数に満たない場合（ステップ1308：No）、バックグラウンド予測プログラム1014は、ステップ1303に戻る。

【0146】

一方、変数*i*が接続先数を上回っていた場合（ステップ1308：Yes）、バックグラウンド予測プログラム1014は処理を終了する（ステップ1308）。

【0147】

なお、図13で説明した、バックグラウンド予測処理の方法は、一例であって、これに限定されない。

【0148】

実施例2によれば、悪性サイト生存期間予測システム1001は、実施例1と同様の悪性サイト生存期間予測機能に加えての支援機能として、観測間隔策定機能、性質予測機能、バックグラウンド予測機能を具備する。これにより、悪性サイト生存期間予測やこれに係るリスト構築について、より高度かつ省力的な実施を可能にする。

[実施例3]

実施例3では、オンプレミスでの悪性サイト生存期間予測に加えて、ネットワーク経由で判定結果を外部に共有することにより、クラウドでのサービス提供を可能にする悪性サイト生存期間予測システムの処理について示す。以下、実施例1との差異を中心に実施例2について説明する。

【0149】

図14は、本発明の実施例3に係る悪性サイト生存期間予測システム1401の構成例を示す図である。実施例3の計算機システムの構成は実施例1と同一である。

【0150】

実施例3における悪性サイト生存期間予測システム1401のハードウェア構成は、実施例2の構成に加えて、外部ユーザ端末1420を含みうる。

【0151】

実施例3においては、各プログラムは、ネットワーク内のユーザ端末1417だけでなく、外部ユーザ端末1420からの要求に応じて処理を実行し、その結果をインターネット1419を介して外部ユーザ端末1420へ返却する。これにより、クラウドでのサービス提供を可能にする。

【0152】

実施例 3 のプログラムは実施例 2 と同一である。また、実施例 3 の悪性サイト観測プログラム 1 4 0 8、生存期間予測プログラム 1 4 0 9、画面描画プログラム 1 4 1 0、リスト構築プログラム 1 4 1 1、観測間隔策定プログラム 1 4 1 2、性質予測プログラム 1 4 1 3、バックグラウンド予測プログラム 1 4 1 4 が実行する処理は、実施例 2 と同一である。また、実施例 3 のデータ構造は実施例 2 と同一である。

【0 1 5 3】

なお、図 1 4 で説明した、実施例 3 に係る悪性サイト生存期間予測システム 1 4 0 1 の構成は、一例であって、これに限定されない。

【0 1 5 4】

実施例 3 によれば、悪性サイト生存期間予測システム 1 4 0 1 は、実施例 1 や実施例 2 と同様に、オンプレミスで内部ユーザに対して悪性サイトの生存期間予測機能を提供しつつ、外部ユーザに対しても同様の情報をインターネット 1 4 1 9 を介して提供しうる。これにより、クラウドでのサービス提供が可能となる。

【0 1 5 5】

以上、本発明を実施するための最良の形態などについて具体的に説明したが、本発明はこれに限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能である。

【0 1 5 6】

こうした本実施形態によれば、悪性サイトの生存期間を予測することにより、遮断リストや監視リストの構築に係る業務コストや属人性を低減可能となる。

【0 1 5 7】

本明細書の記載により、少なくとも次のことが明らかにされる。すなわち、本実施形態の悪性サイト生存期間予測システムにおいて、前記演算装置は、前記観測の結果、前記予測の結果、及び前記遮断リスト又は前記監視リストの少なくともいずれかを、所定装置に出力する処理をさらに実行するものである、としてもよい。

【0 1 5 8】

これによれば、悪性サイトへの対処を行う担当者等が、生存期間を含む、悪性サイトに関する種々の情報を効率良く認識可能となり、その対処の適時性も高まることとなる。

【0 1 5 9】

また、本実施形態の悪性サイト生存期間予測システムにおいて、前記演算装置は、前記観測の結果に加えて、前記悪性サイトに関して前記ネットワークにて公開されている外部情報を前記判定ルールに適用して前記生存期間を予測するものである、としてもよい。

【0 1 6 0】

これによれば、WHOIS 情報や DNS 情報といった、悪性サイトを運用しているドメインや国、所有者といった様々な情報も、生存期間の予測アルゴリズムに適用することが可能となり、生存期間の予測精度が効果的に高まることとなる。

【0 1 6 1】

また、本実施形態の悪性サイト生存期間予測システムにおいて、前記演算装置は、前記観測の結果および前記外部情報に基づき、前記悪性サイトの役割を含む性質を推定し、当該推定の結果も前記判定ルールに適用して前記生存期間の予測を行うものである、としてもよい。

【0 1 6 2】

これによれば、マルウェア配布を担うサイトやそうしたマルウェアへの指示を一定期間に亘って行う管理・指令のためのサイトといった役割ごとに、生存期間が異なりやすいといった傾向を的確に踏まえた上で、生存期間の予測を精度良く行うことが可能となる。

【0 1 6 3】

また、本実施形態の悪性サイト生存期間予測システムにおいて、前記演算装置は、前記観測の結果および前記外部情報を所定のアルゴリズムに適用し、前記悪性サイトに紐づく攻撃グループ又はマルウェアを予測し、当該予測の結果も前記判定ルールに適用することで、前記生存期間の予測を行うものである、としてもよい。

【0 1 6 4】

これによれば、悪性サイトの運用元や所属する国、ターゲットとしているシステム、サービス、或いは使用されやすいマルウェアなどの過去傾向等を踏まえて、当該悪性サイトの攻撃グループ、使用マルウェアを予測し、これに応じて生存期間の予測精度をさらに高めることが期待出来る。

【0165】

また、本実施形態の悪性サイト生存期間予測システムにおいて、前記演算装置は、前記生存期間の予測結果が示す、前記悪性サイトの役割に応じて監視又は遮断の対象となるリストを生成するものである、としてもよい。

【0166】

これによれば、例えば、マルウェア配布の役割を担うサイトは迅速な遮断が望ましく、また、マルウェア配布役のサイトへの指示を担うサイトは継続的な監視が望ましい、といった根拠を踏まえ、精度良くリストを生成可能となる。

【0167】

また、本実施形態の悪性サイト生存期間予測システムにおいて、前記演算装置は、前記予測した生存期間と、悪性サイトの遮断又は観測に関して対処しうるリソース性能とに基づき、前記遮断リスト又は前記監視リストを最大化する処理をさらに実行するものである、としてもよい。

【0168】

これによれば、遮断リストや監視リストの維持、管理等に用意できるリソースの範囲内で、当該リストを効率的に生成し、その後に利活用する状況を生み出せる。

【0169】

また、本実施形態の悪性サイト生存期間予測方法において、前記情報処理装置が、前記観測の結果、前記予測の結果、及び前記遮断リスト又は前記監視リストの少なくともいずれかを、所定装置に出力する処理をさらに実行する、としてもよい。

【0170】

また、本実施形態の悪性サイト生存期間予測方法において、前記情報処理装置が、前記観測の結果に加えて、前記悪性サイトに関して前記ネットワークにて公開されている外部情報を前記判定ルールに適用して前記生存期間を予測する、としてもよい。

【0171】

また、本実施形態の悪性サイト生存期間予測方法において、前記情報処理装置が、前記観測の結果および前記外部情報に基づき、前記悪性サイトの役割を含む性質を推定し、当該推定の結果も前記判定ルールに適用して前記生存期間の予測を行う、としてもよい。

【0172】

また、本実施形態の悪性サイト生存期間予測方法において、前記情報処理装置が、前記観測の結果および前記外部情報を所定のアルゴリズムに適用し、前記悪性サイトに紐づく攻撃グループ又はマルウェアを予測し、当該予測の結果も前記判定ルールに適用することで、前記生存期間の予測を行う、としてもよい。

【0173】

また、本実施形態の悪性サイト生存期間予測方法において、前記情報処理装置が、前記生存期間の予測結果が示す、前記悪性サイトの役割に応じて監視又は遮断の対象となるリストを生成するものである、としてもよい。

【0174】

また、本実施形態の悪性サイト生存期間予測方法において、前記情報処理装置が、前記予測した生存期間と、悪性サイトの遮断又は観測に関して対処しうるリソース性能とに基づき、前記遮断リスト又は前記監視リストを最大化する処理をさらに実行する、としてもよい。

【符号の説明】

【0175】

101 悪性サイト生存期間予測システム

102 IF（通信装置）

10

20

30

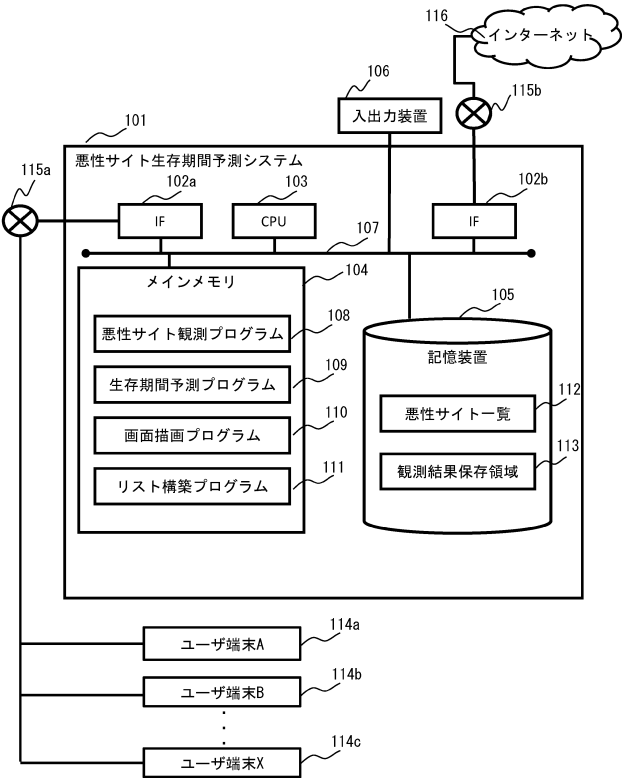
40

50

- 103CPU（演算装置）
- 104メインメモリ
- 105記憶装置
- 106入出力装置
- 107通信路
- 108悪性サイト観測プログラム
- 109生存期間予測プログラム
- 110画面描写プログラム
- 111リスト構築プログラム
- 112悪性サイト一覧
- 113観測結果保存領域
- 114ユーザ端末
- 115ネットワーク
- 116インターネット

【図面】

【図1】



【図2】

悪性サイト一覧				
201 接続先ID	202 接続先	203 観測スパン	204 観測日時	205 予測生存期間
0	search.example.com/	4時間	2023-01-01 04:00:00	120時間
			2023-01-01 00:00:00	
1	192.0.2.1/c2	30分	2023-01-01 04:00:00	48時間
			2023-01-01 03:30:00	
			2023-01-01 03:00:00	
2	example.com/hoge	2時間	2023-01-01 04:00:00	24時間
...				

10

20

30

40

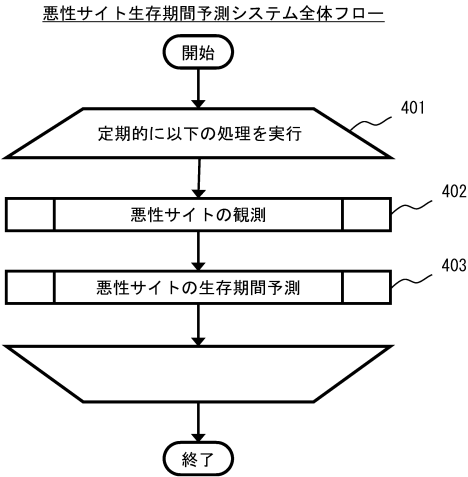
50

【図 3】

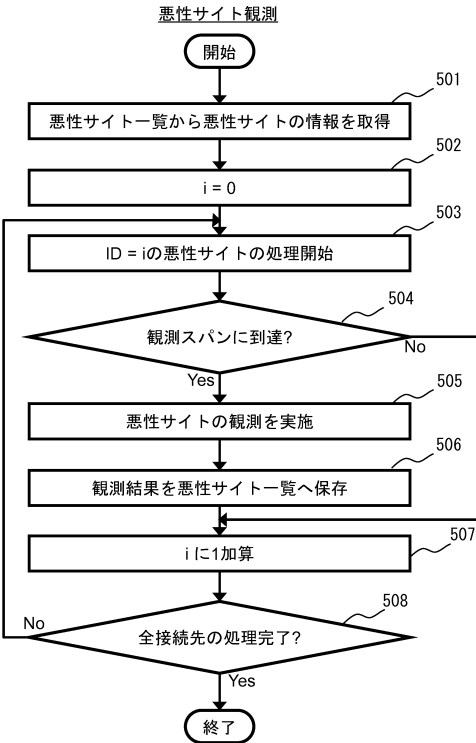
観測結果保存領域

301 接続先 ID	302 接続先	303 観測日時	304 ステータスコード	305 コンテンツ
0	search.example.com /	2023-01-01 04:00:00	200	1.exe
		2023-01-01 00:00:00	404	404.html
1	192.0.2.1/c2	2023-01-01 04:00:00	200	2.exe
		2023-01-01 03:30:00	200	2.exe
		2023-01-01 03:00:00	200	2.exe
2	example.com/hoge	2023-01-01 04:00:00	404	404.html
...				

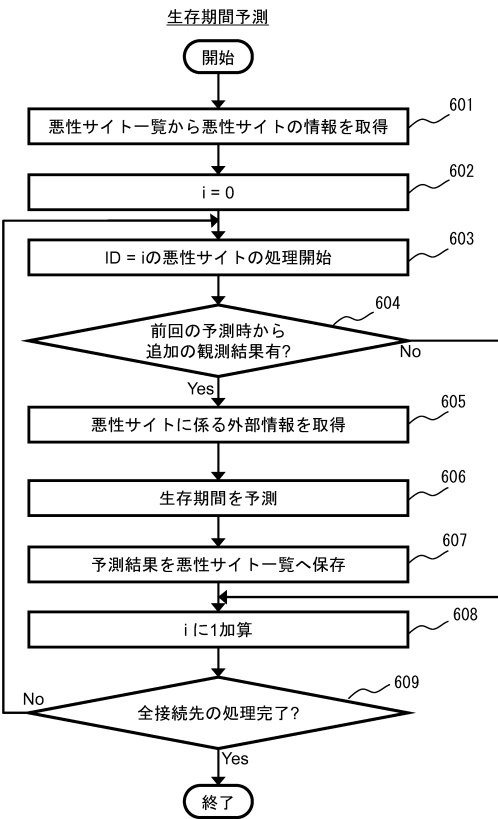
【図 4】



【図 5】



【図 6】



10

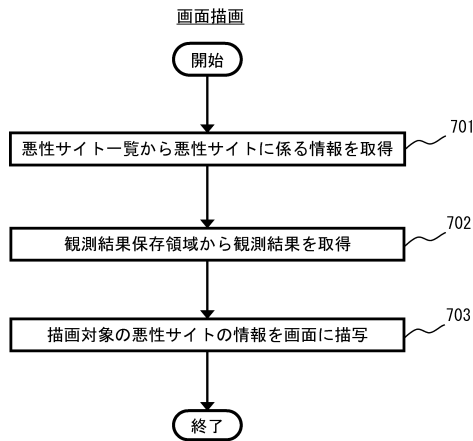
20

30

40

50

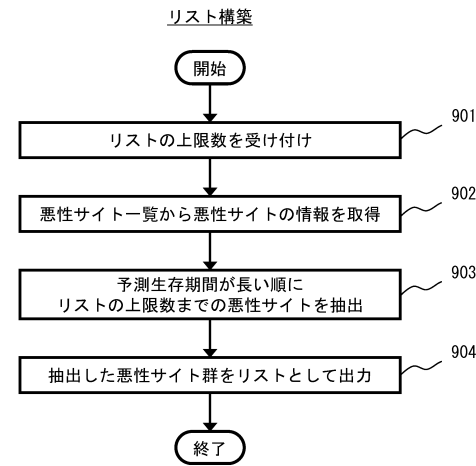
【図 7】



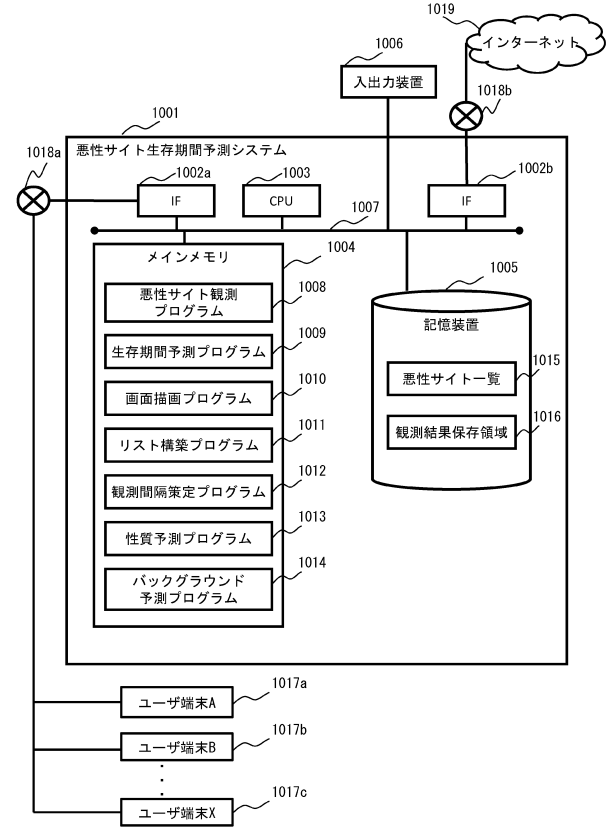
【図 8】



【図 9】



【図 10】



10

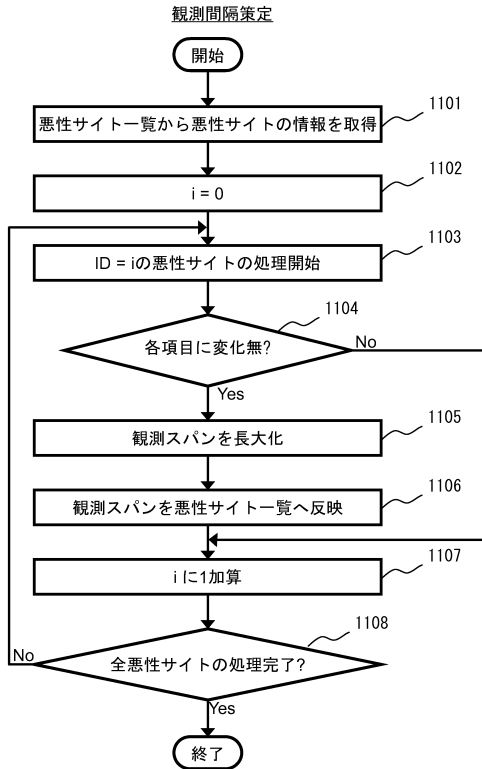
20

30

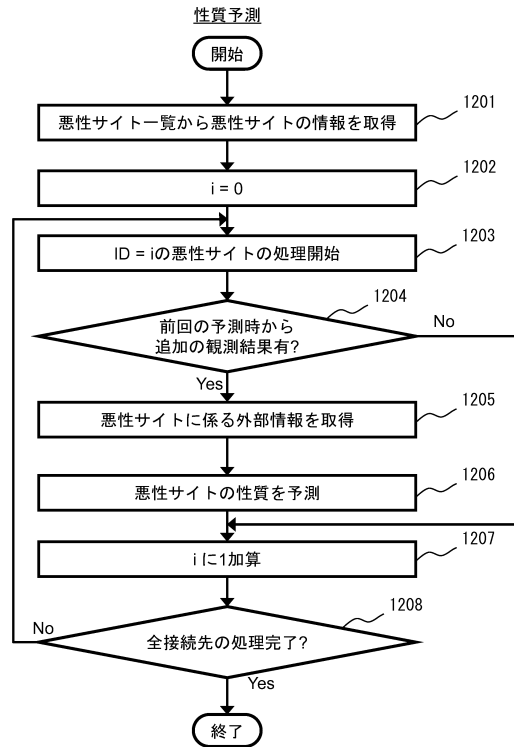
40

50

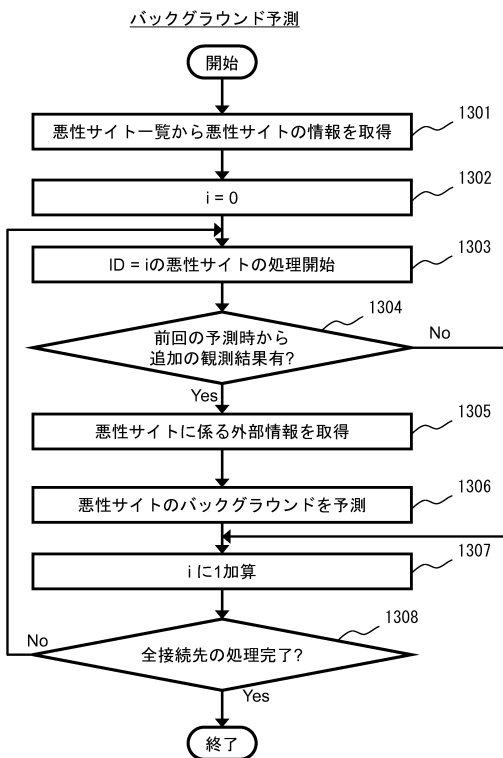
【図 1 1】



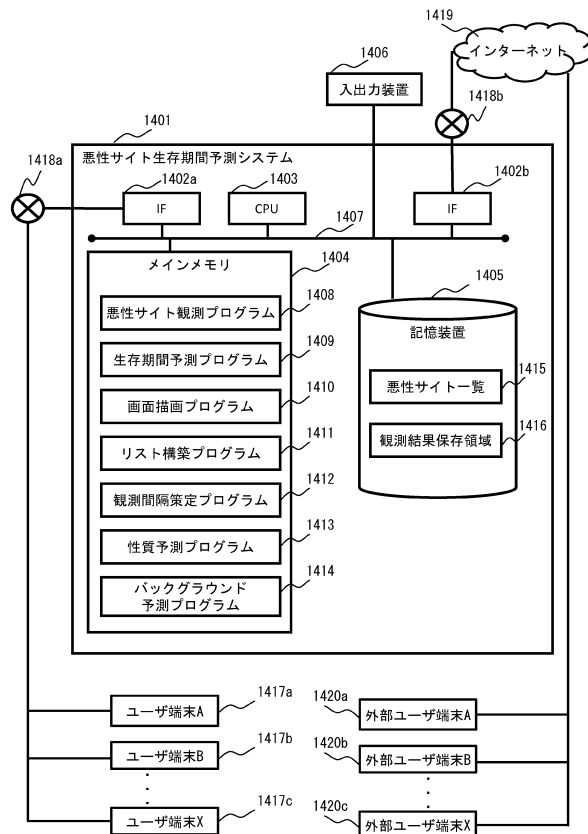
【図 1 2】



【図 1 3】



【図 1 4】



10

20

30

40

50

フロントページの続き

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