(19)日本国特許庁(JP)

(12)特許公報(B2)

(11)特許番号
特許第7409978号
(P7409978)

(45)発行日　令和6年1月9日(2024.1.9)

(24)登録日　令和5年12月25日(2023.12.25)

(51)国際特許分類
Ｇ０６Ｆ　21/57　(2013.01)

ＦＩ
Ｇ０６Ｆ　21/57　３７０

請求項の数　6　（全30頁）

(21)出願番号　特願2020-107261(P2020-107261)
(22)出願日　令和2年6月22日(2020.6.22)
(65)公開番号　特開2022-2057(P2022-2057A)
(43)公開日　令和4年1月6日(2022.1.6)
審査請求日　令和5年2月9日(2023.2.9)

(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　110002365
弁理士法人サンネクスト国際特許事務所
(72)発明者　笹 晋也
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　太田原 千秋
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　内山 宏樹
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　小林 秀和

最終頁に続く

(54)【発明の名称】　リスク評価システムおよびリスク評価方法

(57)【特許請求の範囲】

【請求項１】

攻撃の対象と前記攻撃によるセキュリティへの影響の有無とに係る情報を含む１つ以上のセキュリティ情報から得られる、前記攻撃の対象に対する前記攻撃の発生状況を示す攻撃発生状況情報と、所定のシステムにおける前記攻撃の対象となり得る資産を示す資産情報とを対応付け、前記資産に対する前記攻撃のリスクを示すリスク値を算出する算出部と、

前記算出部により算出されたリスク値を出力する出力部と、

複数の期間の各々に対応する攻撃発生状況情報を記憶する記憶部と、

前記複数の期間の任意の期間の攻撃発生状況情報をもとに、所定の期間における前記資産に対する前記攻撃の発生状況を予測する予測部と、

を備え、

前記算出部は、前記予測部により予測された前記所定の期間における前記攻撃の発生状況と前記資産情報とを対応付け、前記所定の期間における前記資産に対する前記攻撃のリスクを示す予測値を算出し、

前記出力部は、前記算出部により算出された予測値を出力する、

リスク評価システム。

【請求項２】

前記算出部により算出されたリスク値を記憶する記憶部を備え、

前記出力部は、前記記憶部に記憶されている最新のリスク値を含む所定の期間のリスク値を表示する、

請求項１に記載のリスク評価システム。
【請求項３】
前記セキュリティ情報は、自然言語で記述され、
外部の情報源から前記セキュリティ情報を収集する収集部と、
前記セキュリティ情報に対して自然言語処理を行って統計処理可能な形式に変換して前処理済セキュリティ情報にする処理を行う処理部と、
前記前処理済セキュリティ情報をもとに前記攻撃発生状況情報を生成する生成部と、を備える、
請求項１に記載のリスク評価システム。
【請求項４】
前記セキュリティ情報には、前記攻撃の種類に係る情報が含まれ、
前記セキュリティ情報から、前記攻撃の種類ごとに、前記攻撃の対象への前記攻撃の発生状況を示す攻撃発生状況情報を生成する生成部を備え、
前記算出部は、前記攻撃の種類ごとに、前記攻撃発生状況情報と前記資産情報とを対応付け、前記リスク値を算出する、
請求項１に記載のリスク評価システム。
【請求項５】
前記セキュリティ情報は、前記攻撃の対象の脆弱性の種類に係る情報を含む脆弱性情報であり、
前記脆弱性情報から前記脆弱性の種類ごとに前記脆弱性の個数を集計し、集計した結果と前記脆弱性の種類と前記攻撃との関連度を示す情報とをもとに、所定の期間における前記資産に対する前記攻撃の発生状況を予測する予測部を備える、
請求項１に記載のリスク評価システム。
【請求項６】
算出部が、攻撃の対象と前記攻撃によるセキュリティへの影響の有無とに係る情報を含む１つ以上のセキュリティ情報から得られる、前記攻撃の対象に対する前記攻撃の発生状況を示す攻撃発生状況情報と、所定のシステムにおける前記攻撃の対象となり得る資産を示す資産情報とを対応付け、前記資産に対する前記攻撃のリスクを示すリスク値を算出することと、
出力部が、前記算出部により算出されたリスク値を出力することと、
記憶部が、複数の期間の各々に対応する攻撃発生状況情報を記憶することと、
予測部が、前記複数の期間の任意の期間の攻撃発生状況情報をもとに、所定の期間における前記資産に対する前記攻撃の発生状況を予測することと、
を含み、
前記算出部は、前記予測部により予測された前記所定の期間における前記攻撃の発生状況と前記資産情報とを対応付け、前記所定の期間における前記資産に対する前記攻撃のリスクを示す予測値を算出し、
前記出力部は、前記算出部により算出された予測値を出力する、
リスク評価方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、概して、リスクの評価に関する。
【背景技術】
【０００２】
システムをセキュアに保つためには、サイバー攻撃の発生、脆弱性の存在等を検知して対処するだけでなく、将来的なリスクに対する予防を行う必要がある。しかしながら、例えば、脆弱性検知システムは、既知の脆弱性と資産とをマッチングさせるため、既に発見された脆弱性への対策に利用することしかできない。同様に、侵入検知システムは、既に発生しているサイバー攻撃を検知することは可能であるが、将来起こり得る攻撃に対する

予防に利用することはできない。
【０００３】
近年、あるマルウェアが特定のＯＳ（Operating System）の脆弱性を利用してシステムを次々に攻撃する等、共通の特徴を有するシステムに対する攻撃が連続して発生する事例が確認されている。このことから、攻撃の発生の傾向等を把握することにより、システムへの将来的なリスクを予測して将来的な脅威に対処できる可能性がある。
【０００４】
これに関し、ソーシャルネットワーキングサービス（ＳＮＳ）、通常の方法ではアクセスができないＷｅｂコンテンツであるダークウェブ等の情報源からセキュリティ情報を収集し、攻撃手法、攻撃者、脆弱性等が言及されている回数の時間変化を出力する技術が開示されている（非特許文献１参照）。
【先行技術文献】
【非特許文献】
【０００５】
【文献】Zane Pokorny, “ The Threat Intelligence Handbook ”,CyberEdge Group, LLC, 2019
【発明の概要】
【発明が解決しようとする課題】
【０００６】
しかしながら、非特許文献１に記載の技術では、対象システムに対する将来的なリスクを評価するためには、攻撃手法、攻撃者、脆弱性等のトレンドと対象システムの資産とを突き合わせる作業を別途行う必要がある。
【０００７】
本発明は、以上の点を考慮してなされたもので、資産に対する攻撃のリスクを評価し得るリスク評価システム等を提案しようとするものである。
【課題を解決するための手段】
【０００８】
かかる課題を解決するため本発明においては、攻撃の対象と前記攻撃によるセキュリティへの影響の有無とに係る情報を含む１つ以上のセキュリティ情報から得られる、前記攻撃の対象に対する前記攻撃の発生状況を示す攻撃発生状況情報と、所定のシステムにおける前記攻撃の対象となり得る資産を示す資産情報とを対応付け、前記資産に対する前記攻撃のリスクを示すリスク値を算出する算出部と、前記算出部により算出されたリスク値を出力する出力部と、を設けるようにした。
【０００９】
上記構成では、例えば、ニュース記事、セキュリティレポート等のセキュリティ情報から得られた攻撃発生状況情報と資産情報とを対応付けてリスク値を算出することで、資産に対する攻撃のリスクを自動的に評価することができる。上記構成によれば、例えば、クライアントは、現在のリスク値をもとに、資産に対する将来的な攻撃への対策を行うことができるようになる。
【発明の効果】
【００１０】
本発明によれば、資産に対する攻撃のリスクを評価することができる。
【図面の簡単な説明】
【００１１】
【図１】第１の実施の形態によるリスク評価システムの一例を示す図である。
【図２】第１の実施の形態によるサーバ装置の物理構成の一例を示す図である。
【図３】第１の実施の形態によるサーバ装置の機能的な構成の一例を示す図である。
【図４】第１の実施の形態によるクライアント装置の物理構成の一例を示す図である。
【図５】第１の実施の形態によるクライアント装置の機能的な構成の一例を示す図である。
【図６】第１の実施の形態によるセキュリティ情報源設定画面の一例を示す図である。

【図７】第１の実施の形態による資産情報入力画面の一例を示す図である。
【図８】第１の実施の形態によるリスク分析結果出力画面の一例を示す図である。
【図９】第１の実施の形態によるセキュリティ情報の一例を示す図である。
【図１０】第１の実施の形態によるセキュリティ情報源設定情報の一例を示す図である。
【図１１】第１の実施の形態による前処理済セキュリティ情報の一例を示す図である。
【図１２】第１の実施の形態による攻撃発生状況情報の一例を示す図である。
【図１３】第１の実施の形態による資産情報の一例を示す図である。
【図１４】第１の実施の形態によるリスク分析結果の一例を示す図である。
【図１５】第１の実施の形態によるリスク評価システムの処理の一例を示す図である。
【図１６】第１の実施の形態によるリスク評価システムの処理の一例を示す図である。
【図１７】第１の実施の形態によるサーバ装置の処理の一例を示す図である。
【図１８】第１の実施の形態によるサーバ装置の処理の一例を示す図である。
【図１９】第１の実施の形態によるサーバ装置の処理の一例を示す図である。
【図２０】第１の実施の形態によるサーバ装置の処理の一例を示す図である。
【図２１】第１の実施の形態によるサーバ装置の処理の一例を示す図である。
【図２２】第１の実施の形態によるクライアント装置の処理の一例を示す図である。
【図２３】第１の実施の形態によるクライアント装置の処理の一例を示す図である。
【図２４】第１の実施の形態によるクライアント装置の処理の一例を示す図である。
【図２５】第２の実施の形態による脆弱性脅威対応関係情報の一例を示す図である。
【発明を実施するための形態】
【００１２】
（１）第１の実施の形態
以下、本発明の一実施の形態を詳述する。本実施の形態では、資産に対する将来的な攻撃に対して事前に対策をとるための技術に関して説明する。ただし、本発明は、実施の形態に限定されるものではない。
【００１３】
本実施の形態に係るリスク評価システムは、サーバ装置とクライアント装置との２つの装置を含んで構成される。本リスク評価システムでは、サーバ装置が外部情報源からセキュリティ情報を収集し、攻撃発生状況を分析した結果である攻撃発生状況情報をクライアント装置に送信する。クライアント装置には、対象システムの資産情報が格納されており、クライアント装置は、サーバ装置から配信された攻撃発生状況情報と資産情報とを突き合わせることにより、資産に対する現在および将来のリスクを評価して出力する。
【００１４】
上記構成により、攻撃発生状況をもとに資産に対する攻撃のリスクを自動的に評価することができ、将来的な攻撃に対して事前に対策を行うことが可能になる。
【００１５】
セキュリティ情報は、インターネット（例えば、ニュースサイト、セキュリティベンダ）等から収集した、セキュリティに関する情報である。セキュリティは、攻撃（脅威）から資産を守ることを意味する。セキュリティの要素については、機密性、完全性、および可用性を例に挙げて説明する。資産は、ハードウェア、ソフトウェア、データ、ネットワークのいずれであってもよい。以下では、主に、ソフトウェアを例に挙げて説明する。
【００１６】
次に、本発明の実施の形態を図面に基づいて説明する。
【００１７】
図1は、リスク評価システム１００の一例を示す図である。リスク評価システム１００は、サーバ装置１１０およびクライアント装置１２０を備える。サーバ装置１１０は、通信ネットワーク１０１を介してクライアント装置１２０と接続されている。また、サーバ装置１１０は、通信ネットワーク１０２を介して外部セキュリティ情報源１３０と接続されている。
【００１８】

サーバ装置１１０は、セキュリティ情報源設定部１１１、セキュリティ情報収集部１１２、セキュリティ情報前処理部１１３、攻撃発生状況分析部１１４、および攻撃発生状況予測部１１５を備える。また、サーバ装置１１０は、セキュリティ情報源設定情報１１６、前処理済セキュリティ情報１１７、および攻撃発生状況情報１１８を備える。

【００１９】

クライアント装置１２０は、資産情報入力部１２１、リスク分析部１２２、およびリスク分析結果出力部１２３を備える。また、クライアント装置１２０は、資産情報１２４およびリスク分析結果１２５を備える。

【００２０】

サーバ装置１１０およびクライアント装置１２０の構成の詳細、および他の装置との通信の詳細については、後述する。

【００２１】

図２は、サーバ装置１１０の物理構成の一例を示す図である。サーバ装置１１０は、装置本体２１０と入出力装置２２０とを含んで構成される。装置本体２１０は、ＣＰＵ２１１、メモリ２１２、外部記憶装置２１３、インタフェース２１４、インタフェース２１５、およびバス２１６を備えている。

【００２２】

ＣＰＵ２１１は、処理を実行するための演算装置である。メモリ２１２は、ＣＰＵ２１１で実行する命令のセットがプログラムとして記述されたデータを含む記憶媒体である。メモリ２１２には、分析予測プログラム２１７が読み込まれている。分析予測プログラム２１７がＣＰＵ２１１で実行されることによって、各機能部が具現化される。分析予測プログラム２１７の動作については後述する。外部記憶装置２１３は、ＨＤＤ（Hard Disk Drive）等の記憶媒体から構成される。外部記憶装置２１３は、セキュリティ情報源設定情報１１６、前処理済セキュリティ情報１１７、および攻撃発生状況情報１１８等を記憶する。これらの情報の具体的な内容については後述する。

【００２３】

インタフェース２１４は、サーバ装置１１０を通信ネットワーク１０１と接続するための通信装置である。ＬＡＮ（Local Area Network）カード等の通信機器がこれに対応する。インタフェース２１４は、ＩＦと記述することがある。インタフェース２１５は、サーバ装置１１０を通信ネットワーク１０２と接続するための通信装置である。ＬＡＮカード等の通信機器がこれに対応する。バス２１６は、ＣＰＵ２１１、メモリ２１２、外部記憶装置２１３、インタフェース２１４、インタフェース２１５、および入出力装置２２０を接続する。入出力装置２２０は、サーバ装置１１０に対して、サービス管理者によるデータの入力、およびサーバ装置１１０内のデータの出力を行うための装置である。入出力装置の一例としては、キーボード、マウス、ディスプレイ、スピーカ等がある。具体的な入出力については後述する。

【００２４】

図３は、サーバ装置１１０の機能的な構成の一例を示す図である。ＣＰＵ２１１は、セキュリティ情報源設定部１１１、セキュリティ情報収集部１１２、セキュリティ情報前処理部１１３、攻撃発生状況分析部１１４、および攻撃発生状況予測部１１５に係る処理を行う。これらの機能部の各機能は、ＣＰＵ２１１による、分析予測プログラム２１７の実行によって具現化される。

【００２５】

セキュリティ情報源設定部１１１は、外部セキュリティ情報源１３０として用いるウェブサイトのＵＲＬ（Uniform Resource Locator）の入力を受け付け、セキュリティ情報源設定情報１１６として記憶する。セキュリティ情報収集部１１２は、セキュリティ情報源設定情報１１６に含まれているＵＲＬを持つ外部セキュリティ情報源１３０からセキュリティ情報を取得し、セキュリティ情報前処理部１１３に送信する。セキュリティ情報前処理部１１３は、セキュリティ情報収集部１１２より受信したセキュリティ情報を解析し、攻撃発生日、攻撃対象、脅威分類、セキュリティへの影響の有無を抽出し、前処理済セ

キュリティ情報１１７として記憶する。
【００２６】
攻撃発生状況分析部１１４は、前処理済セキュリティ情報１１７に含まれている前処理済セキュリティ情報および攻撃発生状況情報１１８に含まれている過去の攻撃発生状況情報を取得し、現在までの攻撃発生状況を分析し、攻撃発生状況情報１１８を更新する。攻撃発生状況予測部１１５は、攻撃発生状況情報１１８に含まれている現在までの攻撃発生状況情報を取得し、取得した攻撃発生状況情報をもとに将来の攻撃発生状況を予測し、攻撃発生状況情報１１８に記憶する。
【００２７】
サーバ装置１１０は、上記の機能に加えて、例えば、ＯＳ、デバイスドライバ、ファイルシステム、ＤＢＭＳ（DataBase Management System）等の機能を更に備えていてもよい。なお、サーバ装置１１０の１つの機能は、複数の機能に分けられていてもよいし、複数の機能は、１つの機能にまとめられていてもよい。また、サーバ装置１１０の機能の一部は、別の機能として設けられてもよいし、他の機能に含められていてもよい。また、サーバ装置１１０の機能の一部は、サーバ装置１１０と通信可能な他のコンピュータにより実現されてもよい。
【００２８】
図４は、クライアント装置１２０の物理構成の一例を示す図である。クライアント装置１２０は、装置本体４１０と入出力装置４２０とを含んで構成される。装置本体４１０は、ＣＰＵ４１１、メモリ４１２、外部記憶装置４１３、インタフェース４１４、およびバス４１５を備えている。
【００２９】
ＣＰＵ４１１は、処理を実行するための演算装置である。メモリ４１２は、ＣＰＵ４１１で実行する命令のセットがプログラムとして記述されたデータを含む記憶媒体である。メモリ４１２には、リスク分析プログラム４１６が読み込まれている。リスク分析プログラム４１６がＣＰＵ４１１で実行されることによって、各機能部が具現化される。リスク分析プログラム４１６の動作については後述する。外部記憶装置４１３は、ＨＤＤ等の記憶媒体から構成される。外部記憶装置４１３は、資産情報１２４、リスク分析結果１２５を記憶する。これらの情報の具体的な内容については後述する。
【００３０】
インタフェース４１４は、クライアント装置１２０を通信ネットワーク１０１と接続するための通信装置である。ＬＡＮカード等の通信機器がこれに対応する。バス４１５は、ＣＰＵ４１１、メモリ４１２、外部記憶装置４１３、インタフェース４１４、および入出力装置４２０を接続する。入出力装置４２０は、クライアント装置１２０に対して、クライアントによるデータの入力、およびクライアント装置１２０内のデータの出力を行うための装置である。入出力装置の一例としては、キーボード、マウス、ディスプレイ、スピーカ等がある。具体的な入出力については後述する。
【００３１】
図５は、クライアント装置１２０の機能的な構成の一例を示す図である。ＣＰＵ４１１は、資産情報入力部１２１、リスク分析部１２２、リスク分析結果出力部１２３に係る処理を行う。これらの機能部の各機能は、ＣＰＵ４１１による、リスク分析プログラム４１６の実行によって具現化される。
【００３２】
資産情報入力部１２１は、対象システム内の資産の資産情報の入力を受け付け、資産情報１２４として記憶する。リスク分析部１２２は、攻撃発生状況情報１１８に含まれている攻撃発生状況情報および資産情報１２４に含まれている資産情報を取得し、資産に対するリスクを分析し、リスク値の時間変化として出力し、リスク分析結果１２５を更新する。リスク分析結果出力部１２３は、リスク分析結果１２５に含まれているリスク分析結果を取得し、リスク値およびその時間変化を表すグラフを画面上に表示する。
【００３３】

クライアント装置１２０は、上記の機能に加えて、例えば、ＯＳ、デバイスドライバ、ファイルシステム、ＤＢＭＳ等の機能を更に備えていてもよい。なお、クライアント装置１２０の１つの機能は、複数の機能に分けられていてもよいし、複数の機能は、１つの機能にまとめられていてもよい。また、クライアント装置１２０の機能の一部は、別の機能として設けられてもよいし、他の機能に含められていてもよい。また、クライアント装置１２０の機能の一部は、クライアント装置１２０と通信可能な他のコンピュータにより実現されてもよい。

【００３４】

図６は、セキュリティ情報源設定画面６００の一例を示す図である。セキュリティ情報源ＵＲＬ入力欄６０１には、サービス管理者は、外部セキュリティ情報源１３０として利用するウェブサイトのＵＲＬ（セキュリティ情報源ＵＲＬ）を入力する。サービス管理者が削除ボタン６１１を押下する場合、対応するセキュリティ情報源ＵＲＬが削除される。サービス管理者が登録ボタン６１２を押下する場合、セキュリティ情報源設定部１１１は、入力されているセキュリティ情報源ＵＲＬをセキュリティ情報源設定情報１１６に格納する。

【００３５】

図７は、資産情報入力画面７００の一例を示す図である。資産入力欄７０１には、クライアントは、対象システム内に存在する資産の資産名を入力する。例えば、資産がＯＳ、アプリケーションといったソフトウェアである場合は、ソフトウェア名等、ソフトウェアを特定できる識別情報が入力され、資産がパソコン、産業用のコンピュータといったハードウェアである場合は、ハードウェアのモデル番号等、ハードウェアを特定できる識別情報が入力される。

【００３６】

なりすまし対策状況入力欄７０２において、クライアントが選択ボタン７１２を押下する場合、なりすましに対する対策が資産に施されていることを意味する選択肢「○」と、なりすましに対する対策が資産に施されていないことを意味する選択肢「×」とが画面上に表示される。クライアントが選択肢「○」または選択肢「×」を選択することにより、「○」または「×」が入力される。改ざん対策状況入力欄７０３において、クライアントが選択ボタン７１３を押下する場合、改ざんに対する対策が資産に施されていることを意味する選択肢「○」と、改ざんに対する対策が資産に施されていないことを意味する選択肢「×」とが画面上に表示される。クライアントが選択肢「○」または選択肢「×」を選択することにより、「○」または「×」が入力される。

【００３７】

否認対策状況入力欄７０４において、クライアントが選択ボタン７１４を押下する場合、否認に対する対策が資産に施されていることを意味する選択肢「○」と、否認に対する対策が資産に施されていないことを意味する選択肢「×」とが画面上に表示される。クライアントが選択肢「○」または選択肢「×」を選択することにより、「○」または「×」が入力される。情報漏洩対策状況入力欄７０５において、クライアントが選択ボタン７１５を押下する場合、情報漏洩に対する対策が資産に施されていることを意味する選択肢「○」と、情報漏洩に対する対策が資産に施されていないことを意味する選択肢「×」とが画面上に表示される。クライアントが選択肢「○」または選択肢「×」を選択することにより、「○」または「×」が入力される。

【００３８】

ＤｏＳ（Denial of Service）対策状況入力欄７０６において、クライアントが選択ボタン７１６を押下する場合、ＤｏＳに対する対策が資産に施されていることを意味する選択肢「○」と、ＤｏＳに対する対策が資産に施されていないことを意味する選択肢「×」とが画面上に表示される。クライアントが選択肢「○」または選択肢「×」を選択することにより、「○」または「×」が入力される。特権昇格対策状況入力欄７０７において、クライアントが選択ボタン７１７を押下する場合、特権昇格に対する対策が資産に施されていることを意味する選択肢「○」と、特権昇格に対する対策が資産に施されていないこ

とを意味する選択肢「×」とが画面上に表示される。クライアントが選択肢「○」または選択肢「×」を選択することにより、「○」または「×」が入力される。

【００３９】

Ｃ重要度入力欄７０８において、クライアントは、資産に要求される機密性の度合いを数値で入力する。本実施の形態では、クライアントは、例えば、予め定められている基準に従って、下限を「０」、上限を「１」とした数値をＣ重要度入力欄７０８に入力する。Ｉ重要度入力欄７０９において、クライアントは、資産に要求される完全性の度合いを数値で入力する。本実施の形態では、クライアントは、例えば、予め定められている基準に従って、下限を「０」、上限を「１」とした数値をＩ重要度入力欄７０９に入力する。Ａ重要度入力欄７１０において、クライアントは、資産に要求される可用性の度合いを数値で入力する。本実施の形態では、クライアントは、例えば、予め定められている基準に従って、下限を「０」、上限を「１」とした数値をＡ重要度入力欄７１０に入力する。

【００４０】

クライアントが登録ボタン７１８を押下した場合、資産情報入力部１２１は、入力されている情報を資産情報１２４として記憶する。

【００４１】

図８は、リスク分析結果出力画面８００の一例を示す図である。リスク分析結果出力画面８００に表示される表のそれぞれの行は、対象システム内に存在する資産、脅威分類の組に対応する。

【００４２】

資産名表示欄８０１は、対象システム内に存在する資産の資産名を表示する。クライアントが並び替えボタン８１１を押下する場合、レコードが資産名順に並び替えられる。脅威分類表示欄８０２は、なりすまし、改ざん、否認、情報漏洩、ＤｏＳ、特権昇格のいずれかの脅威分類を表示する。クライアントが並び替えボタン８１２を押下する場合、レコードが脅威分類順に並び替えられる。前回のリスク値表示欄８０３は、リスク分析部１２２が出力した、１つ前の分析期間のリスク値を表示する。クライアントが並び替えボタン８１３を押下する場合、レコードが１つ前の分析期間のリスク値順に並び替えられる。

【００４３】

今回のリスク値表示欄８０４は、リスク分析部１２２が出力した、最新の分析期間のリスク値を表示する。クライアントが並び替えボタン８１４を押下する場合、レコードが最新の分析期間のリスク値順に並び替えられる。リスク予測値表示欄８０５は、リスク分析部１２２が出力した、将来（所定の期間、例えば、最新の分析期間後の１週間）のリスク値の予測値を表示する。クライアントが並び替えボタン８１５を押下する場合、レコードが将来のリスク値の予測値順に並び替えられる。対策状況表示欄８０６は、各資産に各脅威分類の脅威に対する対策が施されている場合「○」、施されていない場合「×」を出力する。クライアントが並び替えボタン８１６を押下する場合、レコードが対策状況に応じて並び替えられる。

【００４４】

前回のリスク値表示欄８０３、今回のリスク値表示欄８０４、リスク予測値表示欄８０５においては、資産が要対策資産に分類されている場合、フィールドをハイライト表示する。要対策資産凡例８２１は、要対策資産のハイライト表示の凡例である。要対策資産凡例８２１によれば、クライアントは、対策が必要な資産を容易に認識することができる。

【００４５】

要対策資産とは、脅威に対する対策の必要性がある資産である。要対策資産は、例えば、脅威に対する対策が施されていない資産であって、かつ、今回のリスク値が「７０」以上となる資産、前回のリスク値より今回のリスク値が「１０」以上高い資産、直近３か月続けてリスク値が「７０」以上である資産等である。

【００４６】

例えば、各資産における各脅威についての今回のリスク値が表示されることによって、クライアントは、現時点でリスクが高い資産の脅威から順に対策を行うことができるよう

になる。また、例えば、各資産における各脅威について、今回のリスク値と前回のリスク値が表示されることによって、クライアントは、今回のリスク値が前回のリスク値から急激に上がっている脅威に対する対策を優先して行うことができるようになる。また、例えば、各資産における各脅威についてのリスク値の予測値が表示されることによって、クライアントは、将来的にリスクが高い資産の脅威から順に対策を行うことができるようになる。

【００４７】

リスク値グラフ８３１は、リスク分析結果１２５のデータをもとに、例えば、２か月前から１週間後までのリスク値の変化を、資産、脅威分類ごとに表示する。例えば、脅威に対する対策が施されていない資産であって、今回のリスク値が「７０」以上である資産を要対策資産であると判断するルールが設定されている場合、リスク値グラフ８３１のリスク値が「７０」以上の部分に色を付けて要対策資産であることを強調してもよい。付言するならば、リスク値グラフ８３１では、各分析期間は、全て１週間として示されているが、後述するように、データが所定の件数集まるまでの期間となり、１週間に限られない。

【００４８】

図９は、セキュリティ情報収集部１１２がセキュリティ情報前処理部１１３に送信する新規セキュリティ情報（未だ収集されていないセキュリティ情報）の一例を示す図である。

【００４９】

「取得日時」フィールド９０１には、セキュリティ情報収集部１１２が外部セキュリティ情報源１３０よりセキュリティ情報を取得した日時が格納される。「セキュリティ情報源ＵＲＬ」フィールド９０２には、セキュリティ情報を取得したセキュリティ情報源ＵＲＬが格納される。「タイトル」フィールド９０３には、セキュリティ情報のタイトルが格納される。例えば、セキュリティ情報がＲＳＳ（Really Simple Syndication / Rich Site Summary）形式で配信されている場合、ｔｉｔｌｅ要素として含まれている文字列が該当する。「説明」フィールド９０４には、セキュリティ情報の本文が格納される。例えば、セキュリティ情報がＲＳＳ形式で配信されている場合、ｄｅｓｃｒｉｐｔｉｏｎ要素として含まれている文字列が該当する。

【００５０】

図１０は、セキュリティ情報源設定情報１１６の一例を示す図である。「セキュリティ情報源ＵＲＬ」フィールド１００１には、サービス管理者がセキュリティ情報源設定画面６００において設定した、利用するセキュリティ情報源ＵＲＬが格納される。利用する外部セキュリティ情報源１３０としては、ニュースサイト、セキュリティベンダのサイト等が用いられる。

【００５１】

図１１は、前処理済セキュリティ情報１１７の一例を示す図である。「攻撃発生日」フィールド１１０１には、セキュリティ情報前処理部１１３がセキュリティ情報を解析することにより得られた、攻撃の発生日が格納される。「攻撃対象」フィールド１１０２には、セキュリティ情報前処理部１１３がセキュリティ情報を解析することにより得られた、攻撃対象が格納される。「脅威分類」フィールド１１０３には、セキュリティ情報前処理部１１３がセキュリティ情報を解析することにより得られた、脅威分類が格納される。

【００５２】

「Ｃ影響」フィールド１１０４には、セキュリティ情報前処理部１１３がセキュリティ情報を解析した結果、機密性へ影響する攻撃であると判断された場合「１」が、影響しない攻撃であると判断された場合「０」が格納される。「Ｉ影響」フィールド１１０５には、セキュリティ情報前処理部１１３がセキュリティ情報を解析した結果、完全性へ影響する攻撃であると判断された場合「１」が、影響しない攻撃であると判断された場合「０」が格納される。「Ａ影響」フィールド１１０６には、セキュリティ情報前処理部１１３がセキュリティ情報を解析した結果、可用性へ影響する攻撃であると判断された場合「１」が、影響しない攻撃であると判断された場合「０」が格納される。「新規」フィールド１１０７には、攻撃発生状況分析部１１４が各レコードを未使用である場合「１」が、既に

使用した場合「０」が格納される。

【００５３】

図１２は、攻撃発生状況情報１１８の一例を示す図である。攻撃発生状況分析部１１４は、現在までの攻撃発生状況を分析期間ごとに出力する。攻撃発生状況予測部１１５は、将来の攻撃発生状況を分析期間ごとに出力する。分析期間の長さは変化し得るものとし、攻撃発生状況分析部１１４および攻撃発生状況予測部１１５が分析期間を決定するアルゴリズムについては後述する。

【００５４】

「期間開始日」フィールド１２０１には、攻撃発生状況分析部１１４または攻撃発生状況予測部１１５が出力した攻撃発生状況の分析期間の開始日が格納される。「期間終了日」フィールド１２０２には、攻撃発生状況分析部１１４または攻撃発生状況予測部１１５が出力した攻撃発生状況の分析期間の終了日が格納される。

【００５５】

「予測」フィールド１２０３には、レコードが攻撃発生状況分析部１１４より出力されたものである場合「０」が、攻撃発生状況予測部１１５より出力されたものである場合、「１」が格納される。「変更あり」フィールド１２０４には、レコードが攻撃発生状況分析部１１４または攻撃発生状況予測部１１５により変更または追加された場合、「１」が格納される。リスク分析部１２２がレコードを取得する際、「変更あり」フィールド１２０４の値は、「０」に変更される。「攻撃対象」フィールド１２０５には、攻撃発生状況分析部１１４または攻撃発生状況予測部１１５が出力した攻撃発生状況の攻撃対象が格納される。「脅威分類」フィールド１２０６には、攻撃発生状況分析部１１４または攻撃発生状況予測部１１５が出力した攻撃発生状況の脅威分類が格納される。

【００５６】

「Ｃ影響頻度」フィールド１２０７は、攻撃発生状況分析部１１４または攻撃発生状況予測部１１５が出力した攻撃発生状況のＣ影響頻度が格納される。「Ｉ影響頻度」フィールド１２０８は、攻撃発生状況分析部１１４または攻撃発生状況予測部１１５が出力した攻撃発生状況のＩ影響頻度が格納される。「Ａ影響頻度」フィールド１２０９は、攻撃発生状況分析部１１４または攻撃発生状況予測部１１５が出力した攻撃発生状況のＡ影響頻度が格納される。

【００５７】

図１３は、資産情報１２４の一例を示す図である。各レコードが１つの資産に対応する。「資産」フィールド１３０１には、クライアントが資産情報入力画面７００において入力した資産名が格納される。「なりすまし対策状況」フィールド１３０２には、クライアントが資産情報入力画面７００おいて入力したなりすまし対策状況が格納される。「改ざん対策状況」フィールド１３０３には、クライアントが資産情報入力画面７００において入力した改ざん対策状況が格納される。「否認対策状況」フィールド１３０４には、クライアントが資産情報入力画面７００において入力した否認対策状況が格納される。

【００５８】

「情報漏洩対策状況」フィールド１３０５には、クライアントが資産情報入力画面７００において入力した情報漏洩対策状況が格納される。「ＤｏＳ対策状況」フィールド１３０６には、クライアントが資産情報入力画面７００において入力したＤｏＳ対策状況が格納される。「特権昇格対策状況」フィールド１３０７には、クライアントが資産情報入力画面７００において入力した特権昇格対策状況が格納される。

【００５９】

「Ｃ重要度」フィールド１３０８には、クライアントが資産情報入力画面７００において入力したＣ重要度が格納される。「Ｉ重要度」フィールド１３０９には、クライアントが資産情報入力画面７００において入力したＩ重要度が格納される。「Ａ重要度」フィールド１３１０には、クライアントが資産情報入力画面７００において入力したＡ重要度が格納される。

【００６０】

図１４は、リスク分析結果１２５の一例を示す図である。リスク分析部１２２は、分析期間、資産、脅威分類ごとのリスク値を出力する。

【００６１】

「期間開始日」フィールド１４０１には、リスク分析部１２２より出力されたリスク分析結果の分析期間の開始日が格納される。「期間終了日」フィールド１４０２には、リスク分析部１２２より出力されたリスク分析結果の分析期間の終了日が格納される。「資産」フィールド１４０３には、リスク分析部１２２より出力されたリスク分析結果の資産名が格納される。「脅威分類」フィールド１４０４には、リスク分析部１２２より出力されたリスク分析結果の脅威分類が格納される。

【００６２】

「リスク値」フィールド１４０５には、リスク分析部１２２より出力されたリスク分析結果のリスク値が格納される。「対策状況」フィールド１４０６には、リスク分析部１２２より出力されたリスク分析結果において、資産が各脅威分類の脅威に対して対策されている場合「１」、対策されていない場合「０」が格納される。「予測」フィールド１４０７には、リスク分析部１２２より出力されたリスク値が予測値である場合「１」、予測値でない場合「０」が格納される。

【００６３】

図１５は、セキュリティ情報収集部１１２およびセキュリティ情報前処理部１１３の動作の一例の概要を示すシーケンス図である。各部の詳細な処理については後述する。

【００６４】

セキュリティ情報収集部１１２は、例えば、１時間ごとにセキュリティ情報源設定情報１１６を参照し、セキュリティ情報源設定情報として、利用するセキュリティ情報源ＵＲＬを取得する（１５０１）。次に、セキュリティ情報収集部１１２は、取得したセキュリティ情報源ＵＲＬの外部セキュリティ情報源１３０に新規セキュリティ情報を問い合わせる（１５０２）。次に、セキュリティ情報収集部１１２は、外部セキュリティ情報源１３０から応答された新規セキュリティ情報を受信する（１５０３）。次に、セキュリティ情報収集部１１２は、受信した新規セキュリティ情報をセキュリティ情報前処理部１１３に送信する（１５０４）。

【００６５】

セキュリティ情報前処理部１１３は、受信した新規セキュリティ情報を統計処理可能な形式に変換する（１５０５）。次に、セキュリティ情報前処理部１１３は、変換した情報を前処理済セキュリティ情報として前処理済セキュリティ情報１１７に格納する（１５０６）。

【００６６】

図１６は、攻撃発生状況分析部１１４、攻撃発生状況予測部１１５、およびリスク分析部１２２の処理の一例の概要を示すシーケンス図である。各部の詳細な処理については後述する。

【００６７】

攻撃発生状況分析部１１４は、例えば、１日ごとに前処理済セキュリティ情報１１７を参照し、前処理済セキュリティ情報を取得する（１６０１）。次に、攻撃発生状況分析部１１４は、新規前処理済セキュリティ情報、つまり「新規」フィールド１１０７が「１」であるような前処理済セキュリティ情報が、予め定められた件数、例えば、１００件以上存在するか否かを判定する（１６０２）。新規前処理済セキュリティ情報が予め定められた件数以上存在しない場合、攻撃発生状況分析部１１４は、処理を行わない。新規前処理済セキュリティ情報が予め定められた件数以上存在する場合、攻撃発生状況分析部１１４は、それらの前処理済セキュリティ情報の「新規」フィールド１１０７を「０」に更新する（１６０３）。

【００６８】

次に、攻撃発生状況分析部１１４は、攻撃発生状況情報１１８にアクセスし、必要な過去の攻撃発生状況を参照する（１６０４）。次に、攻撃発生状況分析部１１４は、前処理

済セキュリティ情報について、分析期間、脅威分類、攻撃対象ごとに、セキュリティそれぞれに影響を与える攻撃の頻度をカウントする（１６０５）。次に、攻撃発生状況分析部１１４は、カウントした情報を攻撃発生状況として攻撃発生状況情報１１８に格納する（１６０６）。この際、攻撃発生状況分析部１１４は、「変更あり」フィールド１２０４の値を「１」に設定する。また、攻撃発生状況分析部１１４は、攻撃発生状況情報１１８において「予測」フィールド１２０３の値が「１」であるレコードを削除する。次に、攻撃発生状況分析部１１４は、攻撃発生状況更新通知を攻撃発生状況予測部１１５に送信する（１６０７）。

【００６９】

攻撃発生状況予測部１１５は、攻撃発生状況更新通知を受信すると、攻撃発生状況情報１１８にアクセスし、現在までの攻撃発生状況を取得する（１６０８）。次に、攻撃発生状況予測部１１５は、予め定められたアルゴリズムに従い、現在までの攻撃発生状況をもとに将来の攻撃発生状況を予測する（１６０９）。攻撃発生状況予測部１１５は、予測した攻撃発生状況を攻撃発生状況情報１１８に格納する（１６１０）。次に、攻撃発生状況予測部１１５は、攻撃発生状況更新通知をリスク分析部１２２に送信する（１６１１）。

【００７０】

リスク分析部１２２は、攻撃発生状況更新通知を受信すると、資産情報１２４を参照し資産情報を取得する（１６１２）。次に、リスク分析部１２２は、攻撃発生状況情報１１８を参照し、「変更あり」フィールド１２０４の値が「１」であるようなレコードを取得する（１６１３）。次に、リスク分析部１２２は、攻撃発生状況情報１１８から取得したレコードの「変更あり」フィールド１２０４の値を「０」に更新する（１６１４）。

【００７１】

次に、リスク分析部１２２は、リスク分析を行う（１６１５）。より具体的には、リスク分析部１２２は、攻撃発生状況の「攻撃対象」フィールド１２０５と資産情報の「資産」フィールド１３０１とを突き合わせ、予め定義された算出式に従い、分析期間、資産、脅威分類ごとのリスク値を出力する。次に、リスク分析部１２２は、リスク分析結果１２５を更新する（１６１６）。より具体的には、リスク分析部１２２は、「予測」フィールド１４０７が「１」であるレコードを削除した上で、分析期間、資産、脅威分類ごとのリスク値をリスク分析結果としてリスク分析結果１２５に格納する。この際、リスク分析部１２２は、格納するレコードの「変更あり」フィールド１２０４の値を「１」に設定する。

【００７２】

図１７は、セキュリティ情報源設定部１１１の処理の一例を示すフローチャートである。セキュリティ情報源設定部１１１は、サービス管理者がセキュリティ情報源設定画面６００にアクセスすると、セキュリティ情報源設定情報１１６を参照し、現在のセキュリティ情報源設定情報、すなわち全てのレコードの「セキュリティ情報源ＵＲＬ」フィールド１００１の値を取得する（１７０１）。

【００７３】

次に、セキュリティ情報源設定部１１１は、セキュリティ情報源設定画面６００を表示する（１７０２）。より具体的には、セキュリティ情報源設定部１１１は、取得したセキュリティ情報源ＵＲＬの一覧をセキュリティ情報源ＵＲＬ入力欄６０１に表示する。次に、セキュリティ情報源設定部１１１は、セキュリティ情報源設定情報を受け付ける（１７０３）。例えば、サービス管理者がセキュリティ情報源ＵＲＬ入力欄６０１を更新して登録ボタン６１２を押下すると、セキュリティ情報源設定部１１１は、入力されたセキュリティ情報源ＵＲＬの一覧を取得する。次に、セキュリティ情報源設定部１１１は、取得したセキュリティ情報源ＵＲＬの一覧と一致するように、セキュリティ情報源設定情報１１６の「セキュリティ情報源ＵＲＬ」フィールド１００１を更新する（１７０４）。

【００７４】

図１８は、セキュリティ情報収集部１１２の処理の一例を示すフローチャートである。セキュリティ情報収集部１１２には、予めセキュリティ情報を収集する頻度（例えば、１時間ごと）が設定されているものとする。セキュリティ情報収集部１１２は、その設定に

従い、一定時間ごとにセキュリティ情報源設定情報１１６を参照し、全ての「セキュリティ情報源ＵＲＬ」フィールド１００１の値を取得する（１８０１）。

【００７５】

セキュリティ情報収集部１１２は、取得したそれぞれのセキュリティ情報源ＵＲＬに対し、処理１８０２、処理１８０３、および処理１８０４の処理を行う。セキュリティ情報収集部１１２は、セキュリティ情報源ＵＲＬの外部セキュリティ情報源１３０に新規セキュリティ情報を問い合わせる（１８０２）。次に、セキュリティ情報収集部１１２は、外部セキュリティ情報源１３０より応答される新規セキュリティ情報を受信する（１８０３）。

【００７６】

新規セキュリティ情報としては、例えば、ニュースサイト、セキュリティベンダ等から配信されるＲＳＳ形式のドキュメント（ニュース記事、セキュリティレポート等）を利用する。この場合、ニュースサイト、セキュリティベンダ等から受信するファイルの中には、ｔｉｔｌｅ要素としてドキュメントのタイトルが含まれ、ｄｅｓｃｒｉｐｔｉｏｎ要素としてドキュメントの本文が含まれている。セキュリティ情報収集部１１２は、図９に示すとおり、「取得日時」フィールド９０１に新規セキュリティ情報の取得日時、「セキュリティ情報源ＵＲＬ」フィールド９０２にセキュリティ情報源ＵＲＬ、「タイトル」フィールド９０３にドキュメントのタイトル、「説明」フィールド９０４にドキュメントの本文を格納し、セキュリティ情報前処理部１１３に送信する（１８０４）。

【００７７】

図１９は、セキュリティ情報前処理部１１３の処理の一例を示すフローチャートである。セキュリティ情報前処理部１１３は、セキュリティ情報収集部１１２より新規セキュリティ情報を受信する（１９０１）。

【００７８】

セキュリティ情報前処理部１１３は、各新規セキュリティ情報について、「タイトル」フィールド９０３に含まれているドキュメントのタイトルと、「説明」フィールド９０４に含まれているドキュメントの本文とに対して自然言語処理を行う。これにより、ドキュメント内で言及されているサイバー攻撃について、攻撃発生日、攻撃対象、脅威分類、セキュリティへの影響の有無を特定する（１９０２）。ここで、脅威分類としては、なりすまし、改ざん、否認、情報漏洩、ＤｏＳ、特権昇格からなるＳＴＲＩＤＥを利用することができる。

【００７９】

例えば、セキュリティレポートが、取得日時が「２０２０／１／６　１４：２２：４２」、タイトルが「Ｘ社へのサイバー攻撃が発生」、本文が「１／５にＸ社へのサイバー攻撃が発生し、顧客情報が流出したことが判明した。この攻撃は、ソフトウェアＡの脆弱性を利用したものと見られ・・・」であったとする。当該セキュリティレポートについて、セキュリティ情報前処理部１１３は、攻撃発生日を「２０２０／１／５」、攻撃対象を「ソフトウェアＡ」、脅威分類を「情報漏洩」、機密性への影響を「あり」、完全性への影響を「なし」、可用性への影響を「なし」と判断する。

【００８０】

セキュリティ情報前処理部１１３は、前処理済セキュリティ情報１１７を更新する（１９０３）。より具体的には、セキュリティ情報前処理部１１３は、このように抽出した攻撃発生日、攻撃対象、脅威分類、セキュリティへの影響を、それぞれ「攻撃発生日」フィールド１１０１、「攻撃対象」フィールド１１０２、「脅威分類」フィールド１１０３、「Ｃ影響」フィールド１１０４、「Ｉ影響」フィールド１１０５、「Ａ影響」フィールド１１０６に格納する。この際、「Ｃ影響」フィールド１１０４、「Ｉ影響」フィールド１１０５、「Ａ影響」フィールド１１０６については、セキュリティ情報前処理部１１３は、「あり」を「１」、「なし」を「０」として格納する。また、セキュリティ情報前処理部１１３は、「新規」フィールド１１０７については「１」とする。

【００８１】

図２０は、攻撃発生状況分析部１１４の処理の一例を示すフローチャートである。攻撃発生状況分析部１１４には、予め動作を行う頻度（例えば、１日ごと）が設定されているものとする。攻撃発生状況分析部１１４は、その設定に従い、一定時間ごとに前処理済セキュリティ情報１１７を参照し、前処理済セキュリティ情報を取得する（２００１）。

【００８２】

次に、攻撃発生状況分析部１１４は、新規前処理済セキュリティ情報、つまり「新規」フィールド１１０７が「１」であるような前処理済セキュリティ情報が、予め設定された件数、例えば１００件以上存在するか否かを判定する（２００２）。新規前処理済セキュリティ情報が予め定められた件数以上存在しない場合、攻撃発生状況分析部１１４は、処理を行わない。新規前処理済セキュリティ情報が予め定められた件数以上存在する場合、攻撃発生状況分析部１１４は、前処理済セキュリティ情報１１７において、それらの前処理済セキュリティ情報の「新規」フィールド１１０７の値を「０」に変更する（２００３）。

【００８３】

次に、攻撃発生状況分析部１１４は、攻撃発生状況情報１１８を参照し、新規前処理済セキュリティ情報の攻撃発生日をもとに、必要なレコードを取得する（２００４）。より具体的には、攻撃発生状況分析部１１４は、ある新規前処理済セキュリティ情報の攻撃発生日が「２０１９／１２／２５」であった場合、攻撃発生状況情報１１８のレコードのうち、「期間開始日」フィールド１２０１の日付が２０１９／１２／２５以前であり、かつ「期間終了日」フィールド１２０２の日付が２０１９／１２／２５以降であるようなものを取得する。この処理を全ての新規前処理済セキュリティ情報について行う。

【００８４】

次に、攻撃発生状況分析部１１４は、新規前処理済セキュリティ情報および過去の攻撃発生状況をもとに、分析期間、攻撃対象、脅威分類ごとに、セキュリティそれぞれに影響を与える攻撃の頻度をカウントする（２００５）。図中およびこれ以降の文章中、セキュリティそれぞれに影響を与える攻撃の頻度をＣＩＡ影響頻度と記すことがある。

【００８５】

次に、攻撃発生状況分析部１１４は、分析期間、攻撃対象、脅威分類ごとのＣＩＡ影響頻度を、現在までの攻撃発生状況として攻撃発生状況情報１１８に格納する（２００６）。

【００８６】

例えば、新規前処理済セキュリティ情報の中に以下のレコードが存在した場合を考える。

「攻撃発生日：２０１９／１２／２９、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響：１、Ｉ影響：０、Ａ影響：０、新規：１」

「攻撃発生日：２０１９／１２／３０、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響：１、Ｉ影響：０、Ａ影響：１、新規：１」

「攻撃発生日：２０１９／１２／３０、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響：１、Ｉ影響：０、Ａ影響：０、新規：１」

「攻撃発生日：２０１９／１２／３１、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響：１、Ｉ影響：０、Ａ影響：１、新規：１」

【００８７】

また、攻撃発生状況の中に以下のレコードが存在したとする。

「期間開始日：２０１９／１２／２５、期間終了日：２０１９／１２／３１、予測：０、変更あり：０、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響頻度：３、Ｉ影響頻度：０、Ａ影響頻度：１」

【００８８】

この場合、新規前処理済セキュリティ情報のうち、攻撃発生日が２０１９／１２／２５以降２０１９／１２／３１以前であり、攻撃対象がソフトウェアＡであり、かつ脅威分類が特権昇格であるレコードについて、Ｃ影響が「１」であるものが４個、Ｉ影響が「１」であるものが０個、Ａ影響が「１」であるものが２個存在する。処理２００５において、攻撃発生状況分析部１１４は、これらの値を期間開始日が２０１９／１２／２５、期間終

了日が２０１９／１２／３１、攻撃対象がソフトウェアＡ、脅威分類が特権昇格である攻撃発生状況のレコードの中の、Ｃ影響頻度、Ｉ影響頻度、Ａ影響頻度の値に加え、新しいＣ影響頻度、Ｉ影響頻度、Ａ影響頻度とする。この例では、新しいＣ影響頻度は、３＋４＝７、新しいＩ影響頻度は、０＋０＝０、新しいＡ影響頻度は、１＋２＝３と計算される。処理２００６において、攻撃発生状況分析部１１４は、Ｃ影響頻度、Ｉ影響頻度、Ａ影響頻度をこれらの新しい値に変更し、更に「変更あり」フィールド１２０４の値を「１」に変更する。

【００８９】

この例において、攻撃発生状況のレコードは、以下のものに変更される。

「期間開始日：２０１９／１２／２５、期間終了日：２０１９／１２／３１、予測：０、変更あり：１、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響頻度：７、Ｉ影響頻度：０、Ａ影響頻度：３」

【００９０】

一方、新規前処理済セキュリティ情報の「攻撃発生日」が、攻撃発生状況情報１１８の「期間終了日」フィールド１２０２の中で最新の日付よりも新しい場合、処理２００５では新たに分析期間を設定した上でＣＩＡ影響頻度をカウントする。

【００９１】

例えば、攻撃発生状況分析部が２０２０／１／７に動作しており、新規前処理済セキュリティ情報の中に以下のレコードが存在する場合を考える。

「攻撃発生日：２０２０／１／２、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響：１、Ｉ影響：０、Ａ影響：０、新規：１」

「攻撃発生日：２０２０／１／２、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響：１、Ｉ影響：０、Ａ影響：０、新規：１」

「攻撃発生日：２０２０／１／３、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響：１、Ｉ影響：０、Ａ影響：０、新規：１」

「攻撃発生日：２０２０／１／４、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響：１、Ｉ影響：１、Ａ影響：０、新規：１」

「攻撃発生日：２０２０／１／５、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響：１、Ｉ影響：０、Ａ影響：０、新規：１」

【００９２】

更に、セキュリティ情報ＤＢの「期間終了日」フィールド１２０２の中で最新の日付が２０１９／１２／３１であるとする。

【００９３】

この場合、攻撃発生状況分析部１１４は、「期間終了日」フィールド１２０２の中で最新の日付の１日後、すなわち２０２０／１／１から、攻撃発生状況分析部１１４が動作している現在の日付、すなわち２０２０／１／７までの期間について、ＣＩＡ影響頻度をカウントする。この例では、新規前処理済セキュリティ情報のうち、期間開始日が２０２０／１／１以降２０２０／１／７以前であり、攻撃対象がソフトウェアＡであり、かつ脅威分類が特権昇格であるレコードについて、Ｃ影響が「１」であるものが５個、Ｉ影響が「１」であるものが１個、Ａ影響が「１」であるものが０個存在する。

【００９４】

攻撃発生状況分析部１１４は、処理２００６において、これらの値をそれぞれＣ影響頻度、Ｉ影響頻度、Ａ影響頻度とした以下のレコードを攻撃発生状況情報１１８に追加する。

「期間開始日：２０２０／１／１、期間終了日：２０２０／１／７、予測：０、変更あり：１、攻撃対象：ソフトウェアＡ、脅威分類：特権昇格、Ｃ影響頻度：５、Ｉ影響頻度：１、Ａ影響頻度：０」

【００９５】

次に、攻撃発生状況分析部１１４は、攻撃発生状況情報１１８において「予測」フィールド１２０３の値が「１」であるレコードを全て削除する（２００７）。次に、攻撃発生状況分析部１１４は、攻撃発生状況更新通知を攻撃発生状況予測部１１５に送信する（２

００８）。

【００９６】

図２１は、攻撃発生状況予測部１１５の処理の一例を示すフローチャートである。まず、攻撃発生状況予測部１１５は、攻撃発生状況分析部１１４より攻撃発生状況更新通知を受信する（２１０１）。次に、攻撃発生状況予測部１１５は、攻撃発生状況情報１１８を参照し、必要なレコードを取得する（２１０２）。必要なレコードは、処理２１０３の処理により異なるが、以下では、前回のＣＩＡ影響頻度と今回のＣＩＡ影響頻度とを結んだ直線上の将来の日時の値を将来（予測の期間）のＣＩＡ影響頻度とする方式を例に挙げて説明することから、各攻撃対象、各脅威分類について、分析期間が最新のレコードと２番目に新しいレコードとを用いるケースを例示する。

【００９７】

次に、攻撃発生状況予測部１１５は、予め定められた方式に基づき、攻撃発生状況情報１１８から取得したレコードをもとに、将来の攻撃発生状況を予測する（２１０３）。例えば、ある攻撃対象、脅威分類について、分析期間が最新のレコード（期間開始日ｓ、期間終了日ｅ）のＣ影響頻度をｎ［Ｃ］、分析期間が２番目に新しいレコード（期間開始日ｓ’、期間終了日ｅ’）のＣ影響頻度をｎ［Ｃ］’とする。このとき、期間開始日がｓ”＝ｅ＋１、期間終了日がｅ”＝ｓ”＋７であるような分析期間のＣ影響頻度ｎ［Ｃ］”を下記の予測式に従って予測する。なお、ここでは、今後１週間を予測すると仮定しているが、つまり予測の期間を固定としているが、前回の期間、今回の期間等に応じて予測の期間を変更してもよい。

【００９８】

【数１】

$$n[\mathrm{C}]'' = n[\mathrm{C}] + \frac{s'' + e'' - s - e}{s + e - s' - e'}(n[\mathrm{C}] - n[C]')$$

【００９９】

ただし、この予測式に従って算出した値が「０」以下である場合、ｎ［Ｃ］”＝０とする。Ｉ影響頻度、Ａ影響頻度についても同様に予測し、この処理を全ての攻撃対象、全ての脅威分類について繰り返す。なお、Ｃ影響頻度、Ｉ影響頻度、Ａ影響頻度の予測式は、上記に限定されるものではない。その他の予測式としては、例えば、過去のリスク値の変化のパターンを解析し、リスク値がこのくらい増えているときには、次はこれくらい変化するといったデータを集めて適用した予測式であってもよい。

【０１００】

次に、攻撃発生状況予測部１１５は、処理２１０３において予測したＣＩＡ影響頻度を、攻撃発生状況情報１１８に追加する（２１０４）。この際、攻撃発生状況予測部１１５は、「予測」フィールド１２０３の値を「１」、「変更あり」フィールド１２０４の値を「１」とする。次に、攻撃発生状況予測部１１５は、攻撃発生状況更新通知をリスク分析部１２２に送信する（２１０５）。

【０１０１】

図２２は、資産情報入力部１２１の処理の一例を示すフローチャートである。資産情報入力部１２１は、クライアントが資産情報入力画面７００にアクセスすると、資産情報１２４を参照し、現在の資産情報として全てのレコードを取得する（２２０１）。次に、資産情報入力部１２１は、資産情報入力画面７００を表示する（２２０２）。より具体的には、資産情報入力部１２１は、取得した現在の資産情報を資産入力欄７０１、なりすまし対策状況入力欄７０２、改ざん対策状況入力欄７０３、否認対策状況入力欄７０４、情報漏洩対策状況入力欄７０５、ＤｏＳ対策状況入力欄７０６、特権昇格対策状況入力欄７０７、Ｃ重要度入力欄７０８、Ｉ重要度入力欄７０９、Ａ重要度入力欄７１０に表示する。

【０１０２】

次に、資産情報入力部１２１は、資産情報を受け付ける（２２０３）。より具体的には

、資産情報入力部１２１は、クライアントが資産入力欄７０１、なりすまし対策状況入力欄７０２、改ざん対策状況入力欄７０３、否認対策状況入力欄７０４、情報漏洩対策状況入力欄７０５、ＤｏＳ対策状況入力欄７０６、特権昇格対策状況入力欄７０７、Ｃ重要度入力欄７０８、Ｉ重要度入力欄７０９、Ａ重要度入力欄７１０を更新して登録ボタン７１８を押下すると、資産情報入力部１２１は、入力された資産情報を取得する。次に、資産情報入力部１２１は、取得した資産情報と一致するように、資産情報１２４を更新する（２２０４）。

【０１０３】

図２３は、リスク分析部１２２の処理の一例を示すフローチャートである。リスク分析部１２２は、攻撃発生状況予測部１１５より攻撃発生状況更新通知を受信する（２３０１）。次に、リスク分析部１２２は、資産情報１２４を参照し、全てのレコードを取得する（２３０２）。次に、リスク分析部１２２は、攻撃発生状況情報１１８を参照し、「変更あり」フィールド１２０４の値が「１」であるレコードを取得する（２３０３）。次に、リスク分析部１２２は、取得したレコードの「変更あり」フィールド１２０４の値を「０」に変更する（２３０４）。

【０１０４】

次に、リスク分析部１２２は、取得した攻撃発生状況に含まれる全ての分析期間、攻撃対象、脅威分類の組み合わせについて、予め定義された算出式に従ってリスク値を算出する（２３０５）。より具体的には、リスク分析部１２２は、取得した資産情報に含まれるＣ重要度、Ｉ重要度、Ａ重要度の値と、取得した攻撃発生状況に含まれるＣ影響頻度、Ｉ影響頻度、Ａ影響頻度の値とを用いてリスク値を算出する。

【０１０５】

まず、リスク分析部１２２は、攻撃発生状況情報１１８から取得した各レコードについて、Ｃ影響頻度ｎ［Ｃ］、Ｉ影響頻度ｎ［ｉ］、Ａ影響頻度ｎ［Ａ］を下記の算出式に従ってＣ影響度ｉ［Ｃ］、Ｉ影響度ｉ［ｉ］、Ａ影響度ｉ［Ａ］に変換する。

【０１０６】

【数２】

$$i[\mathrm{C}] = 1 - e^{-n[\mathrm{C}]},\quad i[\mathrm{I}] = 1 - e^{-n[\mathrm{I}]},\quad i[A] = 1 - e^{-n[\mathrm{A}]}$$

【０１０７】

ここでｅは、自然対数の底であり、この変換によりｉ［Ｃ］、ｉ［Ｉ］、ｉ［Ａ］は、「０」以上「１」未満の値になる。次に、分析期間、攻撃対象、脅威分類の組み合わせについて、攻撃対象である資産のＣ重要度ｒ［Ｃ］、Ｉ重要度ｒ［Ｉ］、Ａ重要度ｒ［Ａ］を先ほど取得した資産情報から取り出し、リスク値Ｒを下記の算出式に従って算出する。

【０１０８】

【数３】

$$R = 100(1 - (1 - r[\mathrm{C}]i[\mathrm{C}])(1 - r[\mathrm{I}]i[\mathrm{I}])(1 - r[\mathrm{A}]i[\mathrm{A}]))$$

【０１０９】

上記の算出式によれば、各資産における各脅威のリスクを、同一の基準の下で定量的に評価することができる。なお、リスク値の算出式は、上記に限定されるものではない。評価項目としては、ＣＩＡの全てを用いてもよいし、ＣＩといったように任意の２つを用いてもよいし、Ｃのみといったように任意の１つを用いてもよいし、これらに他の評価項目を組み合わせてもよい。

【０１１０】

次に、リスク分析部１２２は、リスク分析結果１２５において「予測」フィールド１４

０７の値が「１」であるようなレコードを削除する（２３０６）。
【０１１１】
次に、リスク分析部１２２は、分析期間、資産、脅威分類ごとのリスク値、対策状況をリスク分析結果としてリスク分析結果１２５に格納する（２３０７）。このとき、分析期間、資産、脅威分類が全て一致するレコードがリスク分析結果１２５に既にある場合、そのレコードを更新する。ここで、「期間開始日」フィールド１４０１、「期間終了日」フィールド１４０２、「資産」フィールド１４０３、「脅威分類」フィールド１４０４には、取得した攻撃発生状況に含まれる、対応するレコードの期間開始日、期間終了日、攻撃対象、脅威分類を格納する。「リスク値」フィールド１４０５には、処理２３０５において算出したリスク値を格納する。「対策状況」フィールド１４０６には、取得した資産情報に含まれる、当該資産の脅威分類に対する対策状況を格納する。ただし、既にあるリスク分析結果１２５のレコードを更新する場合、「対策状況」フィールド１４０６については、元の値のまま変更しないものとする。「予測」フィールド１４０７には、取得した攻撃発生状況に含まれる、対応するレコードの「予測」フィールドの値を格納する。
【０１１２】
処理２３０７では、リスク分析部１２２は、リスク分析結果１２５において、ある分析期間のレコードが一部の資産、脅威分類の組み合わせについてのみ存在する場合、レコードが存在しない資産、脅威分類の組み合わせについてレコードを追加するものとする。このとき、追加しようとするレコードと分析期間が同じレコードの「予測」フィールド１４０７が「０」である場合、リスク分析部１２２は、追加するレコードでは「リスク値：０、予測：０」とする。一方、追加しようとするレコードと分析期間が同じレコードの「予測」フィールド１４０７が「１」である場合、リスク分析部１２２は、追加するレコードでは「リスク値：Ｎｏｎｅ、予測：１」とする。
【０１１３】
例えば、リスク分析結果１２５に「期間開始日：２０２０／１／１、期間終了日：２０２０／１／７、資産：ソフトウェアＡ、脅威分類：なりすまし、予測：０」であるレコードが存在する一方、「期間開始日：２０２０／１／１、期間終了日：２０２０／１／７、資産：ソフトウェアＢ、脅威分類：なりすまし」であるレコードが存在せず、資産情報においてソフトウェアＢのなりすまし対策状況が「○」である場合、レコード「期間開始日：２０２０／１／１、期間終了日：２０２０／１／７、資産：ソフトウェアＢ、脅威分類：なりすまし、リスク値：０、対策状況：○、予測：０」を追加する。別の例として、リスク分析結果１２５に「期間開始日：２０２０／１／８、期間終了日：２０２０／１／１５、資産：ＯＳ　Ｃ、脅威分類：なりすまし、予測：１」であるレコードが存在する一方、「期間開始日：２０２０／１／８、期間終了日：２０２０／１／１５、資産：ソフトウェアＡ、脅威分類：否認」であるレコードが存在せず、資産情報においてソフトウェアＡの否認対策状況が「×」である場合、レコード「期間開始日：２０２０／１／８、期間終了日：２０２０／１／１５、資産：ソフトウェアＡ、脅威分類：否認、リスク値：Ｎｏｎｅ、対策状況：×、予測：１」を追加する。
【０１１４】
図２４は、リスク分析結果出力部１２３の処理の一例を示すフローチャートである。クライアントがリスク分析結果出力画面８００にアクセスすると、リスク分析結果出力部１２３は、リスク分析結果１２５を参照し、リスク分析結果出力画面８００に表示する期間のレコードを取得する（２４０１）。リスク分析結果出力画面８００に表示する期間については、リスク分析結果出力部１２３に事前に設定されているものとする。
【０１１５】
次に、リスク分析結果出力部１２３は、取得した各レコードについて、要対策資産への該当および非該当を判定する（２４０２）。判定条件（ルール）については、事前に設定されているものとする。判定条件としては、例えば、「リスク値が「７０」以上であるものを要対策資産とする」という条件を用いることができる。
【０１１６】

次に、リスク分析結果出力部１２３は、リスク分析結果および要対策資産への該当または非該当をリスク分析結果出力画面８００に表示する（２４０３）。これにより、リスク分析結果出力画面８００を閲覧したクライアントが優先して対処すべき資産および脅威が明確になる。

【０１１７】

（２）第２の実施の形態

本実施の形態は、攻撃発生状況予測部１１５において、過去の攻撃発生状況をもとに将来の攻撃発生状況を予測する代わりに、脆弱性情報をもとに将来の攻撃発生状況を予測するものである。脆弱性の種類によって、どのような攻撃に利用され易いかが違ってくるので、本実施の形態に係るリスク評価システム１００では、脆弱性の種類を加味してＣＩＡ影響頻度を推定し、その推定の結果を用いて将来のリスクを予測する。脆弱性情報は、セキュリティ情報の一例である。脆弱性情報は、例えば、「ＯＳに情報漏洩を発生し得る脆弱性が発見された」といった情報である。

【０１１８】

本実施の形態において、第１の実施の形態からの主な変更点を以下に示す。例えば、新たな機能部として脆弱性情報収集部が追加され、新たな情報として脆弱性情報および脆弱性脅威対応関係情報が追加される。なお、第１の実施の形態と同じ構成については同じ符号を用いてその説明を省略する。

【０１１９】

脆弱性情報収集部は、予め定められた情報源（例えば、インターネット上）より定期的に脆弱性情報を収集する。収集する脆弱性情報としては、少なくとも脆弱性情報の公表日、脆弱性が存在する製品の名称、脆弱性分類の情報を含むものとする。脆弱性情報収集部は、収集した脆弱性情報を記憶する。

【０１２０】

図２５は、脆弱性脅威対応関係情報の一例を示す図である。脆弱性脅威対応関係情報は、脆弱性分類と脅威分類との対応関係を記憶している情報である。

【０１２１】

「脆弱性分類」フィールド２５０１には、不適切な認証、ＳＱＬインジェクション等の脆弱性分類が格納される。「脅威分類」フィールド２５０２には、なりすまし、改ざん、否認、情報漏洩等の脅威分類が格納される。「影響するセキュリティ要素」フィールド２５０３には、影響するセキュリティ要素（本例では、機密性を示す「Ｃ」、完全性を示す「Ｉ」、可用性を示す「Ａ」の何れか）が格納される。「関連度」フィールド２５０４には、脆弱性分類と脅威分類と影響するセキュリティ要素との関連度が「０」以上「１」以下の値として格納される。関連度の値は、事前に手動で設定されていてもよく、または、別の機能部によって自動的に設定されてもよい。以下、脆弱性分類ｖ、脅威分類ｔ、セキュリティ要素ａの間の関連度をｃ［ｖ，ｔ，ａ］と記す。

【０１２２】

次に、攻撃発生状況予測部１１５の処理が図２１より以下の通り変更される。まず、処理２１０２において、攻撃発生状況予測部１１５は、脆弱性情報を参照し、一定期間（例えば、直近１週間）に公表された脆弱性情報を取得する。次に、処理２１０３において、攻撃発生状況予測部１１５は、以下の通り脆弱性情報をもとに将来の攻撃発生状況を予測する。

【０１２３】

はじめに、攻撃発生状況予測部１１５は、取得した脆弱性情報について、製品、脆弱性分類ごとに個数を集計する。ここで、製品ｐに存在する脆弱性分類ｖの脆弱性の個数をｍ［ｐ，ｖ］とする。次に、下記の算出式に従って、製品ｐ、脆弱性分類ｖ、セキュリティ要素ａに対する所定の期間（例えば、今後１週間）のＣＩＡ影響頻度ｎ［ｐ，ｔ，ａ］を算出する。

【０１２４】

【数４】

$$n[p,t,a] = \sum_{v} m[p,v]c[v,t,a]$$

【０１２５】
攻撃発生状況予測部１１５は、このように算出したＣＩＡ影響頻度を攻撃発生状況情報１１８に格納する。この際、攻撃発生状況予測部１１５は、「期間開始日」フィールド１２０１には、攻撃発生状況予測が動作している日の翌日の日付、「期間終了日」フィールド１２０２には、攻撃発生状況予測が動作している日の１週間後の日付、「予測」フィールド１２０３には、「１」、「変更あり」フィールド１２０４は「１」を格納する。
【０１２６】
（３）付記
上述の実施の形態には、例えば、以下のような内容が含まれる。
【０１２７】
上述の実施の形態においては、本発明をリスク評価システムに適用するようにした場合について述べたが、本発明はこれに限らず、この他種々のシステム、装置、方法、プログラムに広く適用することができる。
【０１２８】
また、上述の実施の形態において、脅威分類を複数設ける場合について説明したが、本発明は、これに限られない。例えば、脅威分類が１種類（例えば、特定の攻撃）設けられる構成であってもよい。付言するならば、脅威分類は、設けられなくてもよい。
【０１２９】
また、上述の実施の形態において、各テーブルの構成は一例であり、１つのテーブルは、２以上のテーブルに分割されてもよいし、２以上のテーブルの全部または一部が１つのテーブルであってもよい。
【０１３０】
また、上述の実施の形態において、図示および説明した画面は、一例であり、受け付ける情報が同じであるならば、どのようなデザインであってもよい。
【０１３１】
また、上述の実施の形態において、情報の出力は、ディスプレイへの表示に限るものではない。情報の出力は、スピーカによる音声出力であってもよいし、ファイルへの出力であってもよいし、印刷装置による紙媒体等への印刷であってもよいし、プロジェクタによるスクリーン等への投影であってもよいし、記憶装置への記憶であってもよいし、その他の態様であってもよい。
【０１３２】
また、上記の説明において、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）等の記憶装置、または、ＩＣカード、ＳＤカード、ＤＶＤ等の記録媒体に置くことができる。
【０１３３】
上述した実施の形態は、例えば、以下の特徴的な構成を有する。
【０１３４】
リスク評価システム（例えば、リスク評価システム１００）は、攻撃（例えば、なりすまし、改ざん、否認、情報漏洩、ＤｏＳ、特権昇格等）の対象（例えば、攻撃対象）と上記攻撃によるセキュリティへの影響の有無（例えば、機密性へ影響する攻撃の有無、完全性へ影響する攻撃の有無、可用性へ影響する攻撃の有無）とに係る情報を含む１つ以上のセキュリティ情報（例えば、図９参照）から得られる、上記攻撃の対象に対する上記攻撃の発生状況（例えば、ＣＩＡ影響頻度）を示す攻撃発生状況情報（例えば、攻撃発生状況情報１１８）と、所定のシステム（例えば、対象システム）における上記攻撃の対象となり得る資産（ソフトウェア、ハードウェア、データ、ネットワーク等）を示す資産情報（例えば、資産情報１２４）とを対応付け、上記資産に対する上記攻撃のリスクを示すリス

ク値を算出する算出部（例えば、リスク分析部１２２、クライアント装置１２０、回路）と、上記算出部により算出されたリスク値を出力する出力部（例えば、リスク分析結果出力部１２３、クライアント装置１２０、回路）と、を備える。

【０１３５】

上記構成では、例えば、ニュース記事、セキュリティレポート等のセキュリティ情報から得られた攻撃発生状況情報と資産情報とを対応付けてリスク値を算出することで、資産に対する攻撃のリスクを自動的に評価することができる。上記構成によれば、例えば、クライアントは、現在のリスク値をもとに、資産に対する将来的な攻撃への対策を行うことができるようになる。

【０１３６】

上記リスク評価システムは、複数の期間の各々に対応する攻撃発生状況情報（例えば、図１２参照）を記憶する記憶部（例えば、外部記憶装置２１３、サーバ装置１１０、サーバ装置１１０とは異なる他のコンピュータ）と、上記複数の期間の任意の期間の攻撃発生状況情報をもとに、所定の期間（例えば、最新の分析期間から１週間）における上記資産に対する上記攻撃の発生状況を予測する予測部（例えば、攻撃発生状況予測部１１５、サーバ装置１１０、回路）と、を備え、上記算出部は、上記予測部により予測された上記所定の期間における上記攻撃の発生状況と上記資産情報とを対応付け、上記所定の期間における上記資産に対する上記攻撃のリスクを示す予測値を算出し（例えば、図２３参照）、上記出力部は、上記算出部により算出された予測値を出力する（例えば、図８参照）。

【０１３７】

上記構成では、現在までの攻撃の発生状況をもとに予測値が出力されるので、クライアントは、例えば、将来のリスクが高い脅威に対する対策を優先して行うことができるようになる。

【０１３８】

上記リスク評価システムは、上記算出部により算出されたリスク値を記憶する記憶部（例えば、外部記憶装置４１３、クライアント装置１２０、クライアント装置１２０とは異なる他のコンピュータ）を備え、上記出力部は、上記記憶部に記憶されている最新のリスク値を含む所定の期間のリスク値を表示する（図８参照）。

【０１３９】

上記構成では、現在のリスク値と過去のリスク値とが表示されるので、例えば、クライアントは、リスク値の変動をもとに、将来的な攻撃への対策を行うことができるようになる。

【０１４０】

上記セキュリティ情報は、自然言語で記述され、上記リスク評価システムは、外部の情報源から上記セキュリティ情報を収集する収集部（例えば、セキュリティ情報収集部１１２、サーバ装置１１０、回路）と、上記セキュリティ情報に対して自然言語処理を行って統計処理可能な形式に変換して前処理済セキュリティ情報にする処理を行う処理部（例えば、セキュリティ情報前処理部１１３、サーバ装置１１０、回路）と、上記前処理済セキュリティ情報をもとに上記攻撃発生状況情報を生成する生成部（例えば、発生状況分析部１１４、サーバ装置１１０、回路）と、を備える（例えば、図１８、図１９を参照）。

【０１４１】

上記セキュリティ情報には、上記攻撃の種類（例えば、脅威分類）に係る情報が含まれ、上記リスク評価システムは、上記セキュリティ情報から、上記攻撃の種類ごとに、上記攻撃の対象への上記攻撃の発生状況を示す攻撃発生状況情報を生成する生成部（例えば、発生状況分析部１１４、サーバ装置１１０、回路）を備え、上記算出部は、上記攻撃の種類ごとに、上記攻撃発生状況情報と上記資産情報とを対応付け、上記リスク値を算出する（例えば、図２３参照）。

【０１４２】

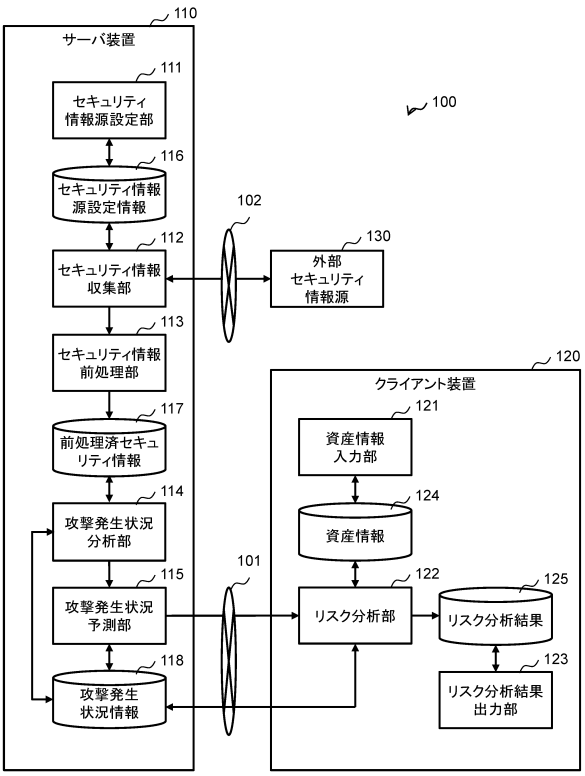
上記構成では、攻撃の種類ごとにリスク値が算出されるので、例えば、クライアントは、攻撃の種類ごとに、資産に対する将来的な攻撃への対策を行うことができるようになる。

【０１４３】
上記セキュリティ情報は、上記攻撃の対象の脆弱性の種類（例えば、脆弱性分類）に係る情報を含む脆弱性情報であり、上記脆弱性情報から上記脆弱性の種類ごとに上記脆弱性の個数を集計し、集計した結果と上記脆弱性の種類と上記攻撃との関連度を示す情報（例えば、脆弱性脅威対応関係情報、図２５参照）とをもとに、所定の期間における上記資産に対する上記攻撃の発生状況を予測する予測部（例えば、攻撃発生状況予測部１１５、サーバ装置１１０、回路）を備える。
【０１４４】
上記構成によれば、脆弱性情報をもとに将来の攻撃の発生状況を予測できるようになる。
【０１４５】
なお、本発明は、上記した実施の形態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、上記した実施の形態は、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、必ずしも説明した全ての構成を備えるものに限定されるものではない。また、ある実施の形態の構成の一部を他の実施の形態の構成に置き換えることが可能であり、また、ある実施の形態の構成に他の実施の形態の構成を加えることも可能である。また、各実施の形態の構成の一部について、他の構成の追加、削除、置換等をすることが可能である。また、上記の各構成、機能、処理部、処理手段等は、それらの一部または全部を、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等の記録装置、または、ＩＣカード、ＳＤカード、ＤＶＤ等の記録媒体に置くことができる。
【符号の説明】
【０１４６】
１００……リスク評価システム。

【図面】

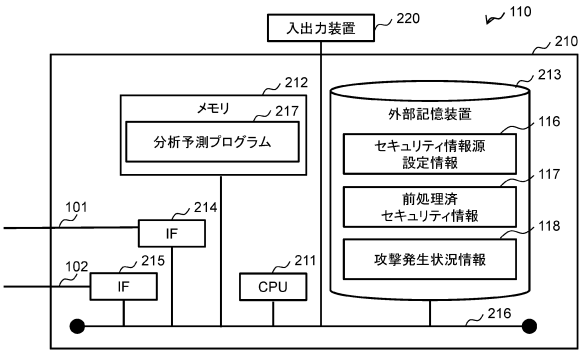
【図１】

図 1



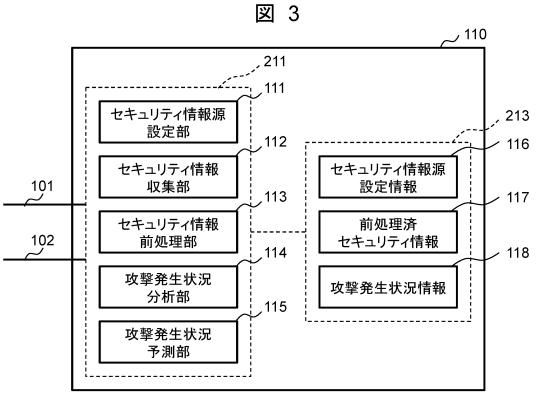
【図２】

図 2



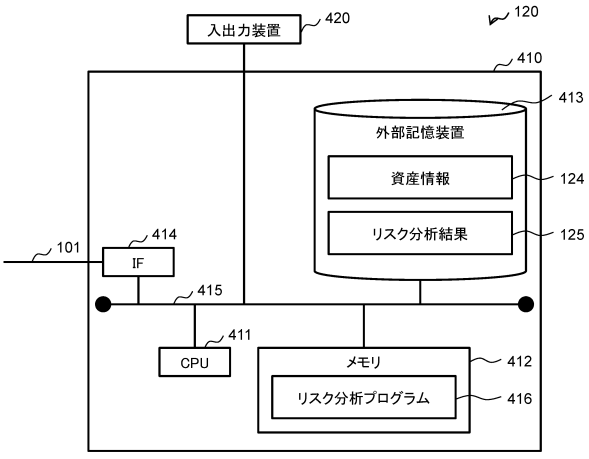
【図３】

図 3



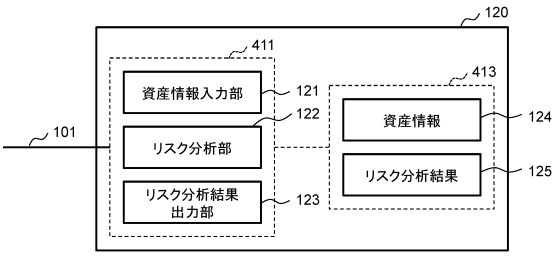
【図４】

図 4



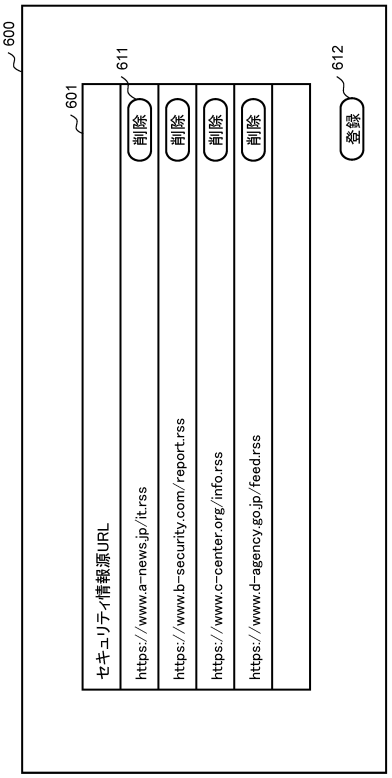
【図５】

図 5



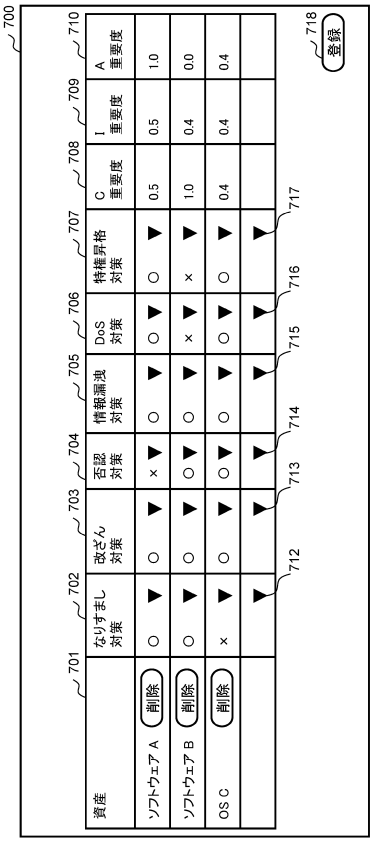
【図６】

図 6



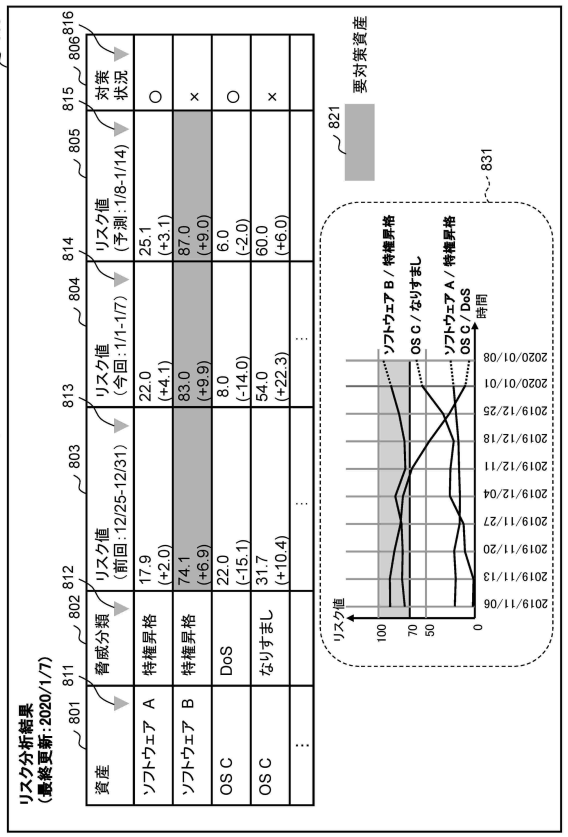
【図７】

図 7



【図８】

図 8



【図９】

図 9

901 取得日時	902 セキュリティ情報源URL	903 タイトル	904 説明
2020/1/6 14:22:42	https://www.a-news.jp/it.rss	X社へのサイバー攻撃が発生	1/5にX社へのサイバー攻撃が発生し、顧客情報が流出したことが判明した。この攻撃はソフトウェアAの脆弱性を利用したものと見られ…
2020/1/7 09:31:11	https://www.b-security.com/report.rss	サイバー攻撃によりサービスYが停止	1/6 10:00-14:00にかけてサービスNが停止した。これは、サーバーが使用しているOS Cの脆弱性を利用したDoS攻撃と見られ…この攻撃による顧客情報流出は無いと考えられる。…

【図１０】

図 10

1001 セキュリティ情報源URL
https://www.a-news.jp/it.rss
https://www.b-security.com/report.rss
https://www.c-center.org/info.rss
https://www.d-agency.go.jp/feed.rss
…

【図１１】

図 11

1101 攻撃発生日	1102 攻撃対象	1103 脅威分類	1104 C影響	1105 I影響	1106 A影響	1107 新規
…	…	…	…	…	…	…
2019/12/29	ソフトウェアA	特権昇格	1	0	0	1
2019/12/30	ソフトウェアA	特権昇格	1	0	1	1
2019/12/30	ソフトウェアA	特権昇格	1	0	0	1
2019/12/31	ソフトウェアA	特権昇格	1	0	1	1
2020/1/1	ソフトウェアA	情報漏洩	1	0	0	1
2020/1/2	ソフトウェアA	特権昇格	1	0	0	1
2020/1/2	ソフトウェアA	特権昇格	1	0	0	1
2020/1/2	OS C	DoS	0	0	1	1
2020/1/3	ソフトウェアA	特権昇格	1	0	0	1
2020/1/4	ソフトウェアA	情報漏洩	1	0	0	1
2020/1/4	ソフトウェアA	特権昇格	1	1	0	1
2020/1/5	ソフトウェアA	特権昇格	1	0	0	1
2020/1/5	ソフトウェアA	情報漏洩	1	0	0	1
2020/1/6	OS C	DoS	0	0	1	1
…	…	…	…	…	…	…

【図１２】

図 12

1201 期間開始日	1202 期間終了日	1203 予測	1204 変更あり	1205 攻撃対象	1206 脅威分類	1207 C影響頻度	1208 I影響頻度	1209 A影響頻度
2020/1/8	2020/1/14	1	1	ソフトウェアA	特権昇格	5	1	0
2020/1/8	2020/1/14	1	1	ソフトウェアB	特権昇格	8	7	7
2020/1/8	2020/1/14	1	1	OS C	DoS	0	0	1
2020/1/8	2020/1/14	1	1	OS C	なりすまし	4	4	0
2020/1/1	2020/1/7	0	1	ソフトウェアA	特権昇格	5	1	0
2020/1/1	2020/1/7	0	1	ソフトウェアA	情報漏洩	2	0	0
2020/1/1	2020/1/7	0	1	ソフトウェアB	特権昇格	8	7	7
2020/1/1	2020/1/7	0	1	OS C	DoS	0	0	1
2020/1/1	2020/1/7	0	1	OS C	なりすまし	4	4	0
2019/12/25	2019/12/31	0	1	ソフトウェアA	特権昇格	7	0	3
…	…	…	…	…	…	…	…	…

【図１３】

図 13

1301 資産	1302 なりすまし対策状況	1303 改ざん対策状況	1304 否認対策状況	1305 情報漏洩対策状況	1306 DoS対策状況	1307 特権昇格対策状況	1308 C重要度	1309 I重要度	1310 A重要度
ソフトウェアA	○	○	×	○	○	○	0.5	0.5	1.0
ソフトウェアB	○	○	○	○	×	×	1.0	0.4	0.0
OS C	×	○	○	○	○	○	0.4	0.4	0.4
…	…	…	…	…	…	…	…	…	…

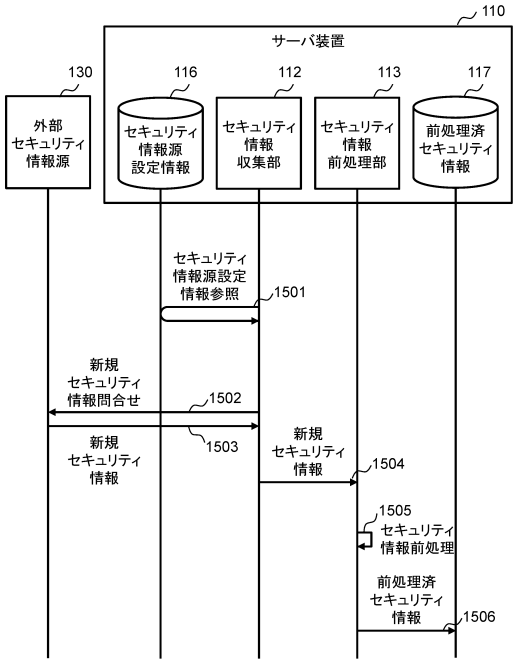
【図１４】

図 14

1401 期間開始日	1402 期間終了日	1403 資産	1404 脅威分類	1405 リスク値	1406 対策状況	1407 予測
…	…	…	…	…	…	…
2020/1/8	2020/1/14	OS C	なりすまし	60.0	0	1
2020/1/1	2020/1/7	ソフトウェアA	特権昇格	22.0	1	0
2020/1/1	2020/1/7	ソフトウェアB	特権昇格	83.0	0	0
2020/1/1	2020/1/7	OS C	DoS	8.0	1	0
2020/1/1	2020/1/7	OS C	なりすまし	54.0	0	0
2019/12/25	2019/12/31	ソフトウェアA	特権昇格	17.9	1	0
…	…	…	…	…	…	…

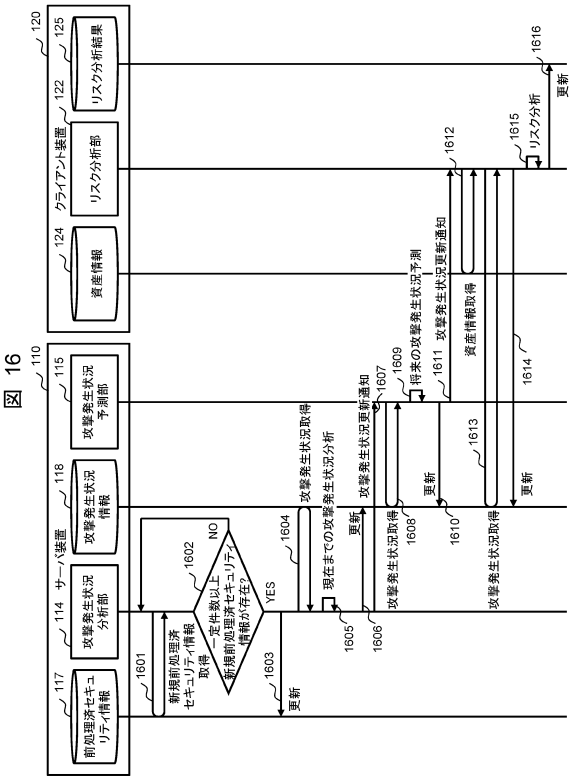
【図１５】

図 15



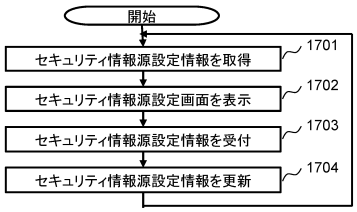
【図１６】

図 16



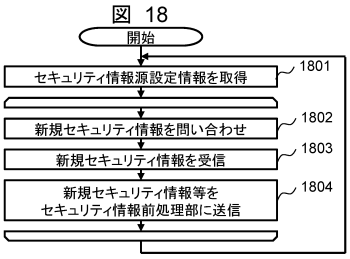
【図１７】

図 17



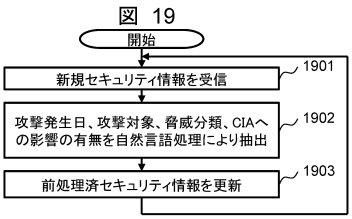
【図１８】

図 18



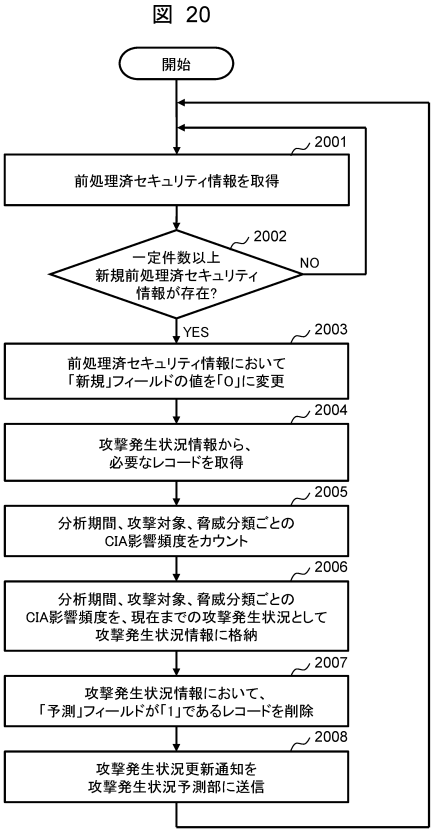
【図１９】

図 19



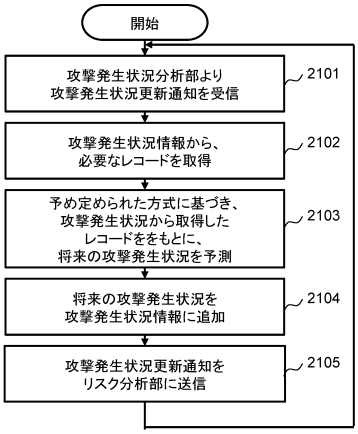
【図２０】

図 20



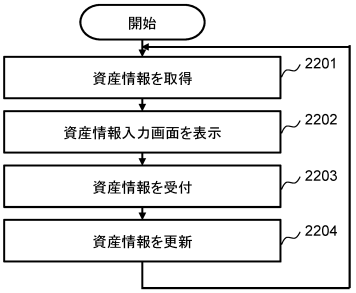
【図２１】

図 21



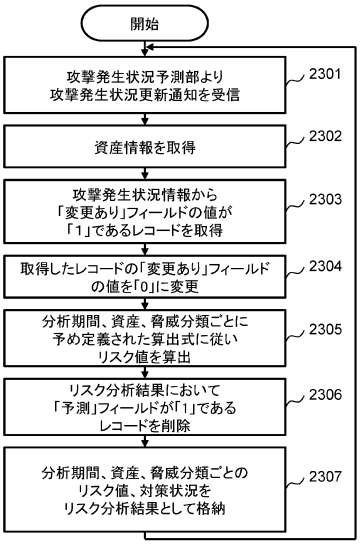
【図２２】

図 22



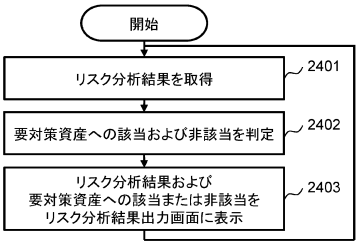
【図２３】

図 23



【図２４】

図 24



【図２５】

図 25

2501 脆弱性分類	2502 脅威分類	2503 影響するセキュリティ要素	2504 関連度
SQLインジェクション	なりすまし	C	1.0
SQLインジェクション	なりすまし	I	1.0
SQLインジェクション	なりすまし	A	0.0
SQLインジェクション	改ざん	C	0.0
SQLインジェクション	改ざん	I	1.0
SQLインジェクション	改ざん	A	0.0
SQLインジェクション	否認	C	0.0
SQLインジェクション	否認	I	0.5
SQLインジェクション	否認	A	0.0
SQLインジェクション	情報漏洩	C	1.0
SQLインジェクション	情報漏洩	I	0.0
SQLインジェクション	情報漏洩	A	0.0
…	…	…	…
不適切な認証	なりすまし	C	1.0
不適切な認証	なりすまし	I	1.0
不適切な認証	なりすまし	A	1.0
不適切な認証	改ざん	C	0.0
不適切な認証	改ざん	I	1.0
不適切な認証	改ざん	A	0.0
…	…	…	…

フロントページの続き

(56)参考文献　特開２０１５－１９１３９０（ＪＰ，Ａ）
特開２００９－２８９１３７（ＪＰ，Ａ）
特開２００３－１０８５２１（ＪＰ，Ａ）
特開２０１９－１４４９７０（ＪＰ，Ａ）
米国特許出願公開第２０１８／０１５０６３９（ＵＳ，Ａ１）

(58)調査した分野　(Int.Cl.，ＤＢ名)
Ｇ０６Ｆ　２１／５７