(12) 特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2014 年 12 月 31 日(31.12.2014)

WIPO | PCT

(10) 国際公開番号
WO 2014/208427 A1

(51) 国際特許分類:
G06F 17/30 (2006.01)

(21) 国際出願番号: PCT/JP2014/066193

(22) 国際出願日: 2014 年 6 月 18 日(18.06.2014)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願 2013-132057 2013 年 6 月 24 日(24.06.2013) JP

(71) 出願人: 日本電信電話株式会社(NIPPON TELEGRAPH AND TELEPHONE CORPORATION) [JP/JP]; 〒1008116 東京都千代田区大手町一丁目５番１号 Tokyo (JP).

(72) 発明者: 佐藤 徹(SATO, Tohru); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 岡野 靖(OKANO, Yasushi); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 朝倉 浩志(ASAKURA, Hiroshi); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP). 折原 慎吾(ORIHARA, Shingo); 〒1808585 東京都武蔵野市緑町３丁目９－１１ ＮＴＴ 知的財産センタ内 Tokyo (JP).

(74) 代理人: 酒井 宏明, 外(SAKAI, Hiroaki et al.); 〒1006020 東京都千代田区霞が関三丁目２番５号 霞が関ビルディング 酒井国際特許事務所 Tokyo (JP).

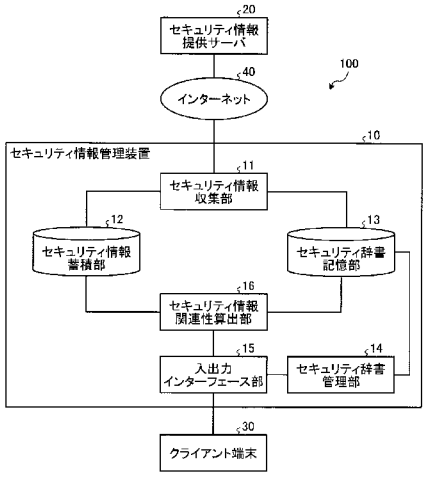
(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JP, KE, KG, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, RU, TJ, TM), ヨーロッパ (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT,

[続葉有]

(54) **Title**: SECURITY INFORMATION MANAGEMENT SYSTEM AND SECURITY INFORMATION MANAGEMENT METHOD

(54) 発明の名称 : セキュリティ情報管理システム及びセキュリティ情報管理方法



10 Security information management device
11 Security information collection unit
12 Security information accumulation unit
13 Security dictionary storage unit
14 Security dictionary management unit
15 I/O interface unit
16 Security information relation computation unit
20 Security information provision server
30 Client terminal
40 Internet

(57) **Abstract**: With a security information management device (10), security information which is information relating to security is collected. The security information management device (10) queries a security dictionary which stores keywords relating to security for each attribute, extracts the keywords from query source security information which is a source for a relation comparison with the security information, compares the extracted keywords with the keywords included in the collected security information, and computes a degree of relation between the query source security information and the security information. The security information management device (10) outputs the security information, such that the higher the computed degree of relation, the higher the priority in the output of the security information.

(57) 要約: セキュリティ情報管理装置（１０）では、セキュリティに関する情報であるセキュリティ情報を収集する。そして、セキュリティ情報管理装置（１０）は、セキュリティに関するキーワードを属性ごとに記憶するセキュリティ辞書を参照して、セキュリティ情報との関連性を比較する元となる参照元セキュリティ情報からキーワードを抽出し、該抽出されたキーワードと収集されたセキュリティ情報に含まれるキーワードとを比較して、参照元セキュリティ情報とセキュリティ情報との関連度を算出する。そして、セキュリティ情報管理装置（１０）は、算出された関連度が高いセキュリティ情報ほど優先的に出力する。

WO 2014/208427 A1

NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

添付公開書類:

— 国際調査報告（条約第 21 条(3)）

明　細　書

発明の名称 ：

セキュリティ情報管理システム及びセキュリティ情報管理方法

技術分野

[0001] 本発明は、セキュリティ情報管理システム及びセキュリティ情報管理方法に関する。

背景技術

[0002] 従来、情報システム資産を有する組織において、安定的な組織活動を継続するために、情報システム資産の管理者（以下、システム管理者と記載する）が、所属組織や管理対象の情報システム資産と関連性の高いセキュリティ情報を収集・把握し、重大な脅威が発見された場合は迅速に対応している。

[0003] このようなセキュリティ情報は、セキュリティ研究機関やセキュリティベンダ等により、インターネット上の情報提供サーバ等を通じて、新しい情報が次々に公開されている。インターネット上で公開されているセキュリティ情報としては、例えば、情報システムを構成するソフトウェアやハードウェアのセキュリティ上の欠陥と、その対策方法に関する情報等が知られている。

[0004] 例えば、セキュリティ情報を収集・提供する手法として、例えば、セキュリティ情報のうち、脆弱性情報について、インターネット上の情報提供サーバで公開されている脆弱性情報を収集する手法が知られている（特許文献１参照）。この手法では、収集した複数の脆弱性情報の参照関係等の関係性に基づく集約、集約した脆弱性情報と、システム管理者が管理する情報システム資産の関連性の判定を行うことにより、システム管理者が優先的に閲覧すべき脆弱性情報を集約して提供する。

先行技術文献

特許文献

[0005] 特許文献1：特許第４９３５３９９号公報

発明の概要

発明が解決しようとする課題

[0006] しかしながら、上述したセキュリティ情報を収集・提供する手法では、システム管理者に対して、脆弱性情報以外のセキュリティ情報について、関連性を判定し提供することができない。このため、システム管理者が参照元とする参照元セキュリティ情報と関連性の高いセキュリティ情報を、容易に収集することができない場合があるという課題があった。

[0007] 例えば、あるセキュリティ情報を参照元セキュリティ情報として、該参照元セキュリティ情報に含まれるキーワードを手掛かりに、インターネット上で提供されている検索エンジン等を用いて収集する場合、システム管理者がセキュリティに関する知識を有していないと、適切なキーワードを選択することができず、関連性の高いセキュリティ情報を収集することができない。

[0008] また、参照元セキュリティ情報に含まれるキーワードを手掛かりにインターネット上で提供されている検索エンジン等を用いて収集する際に、システム管理者がセキュリティに関する知識を有している場合であっても、検索エンジンに入力したキーワードによっては、関連性の低いセキュリティ情報や、セキュリティ情報以外の一般的な情報が、多数混在した状態で検索結果として提示され、関連性の高いセキュリティ情報を判別することに多大な労力を要する。

[0009] そこで、この発明は、参照元セキュリティ情報と関連性の高いセキュリティ情報を、容易に収集することを目的とする。

課題を解決するための手段

[0010] 上述した課題を解決し、目的を達成するため、セキュリティ情報管理システムは、セキュリティに関する情報であるセキュリティ情報を収集する収集部と、前記セキュリティに関するキーワードを属性ごとに記憶するセキュリティ辞書を参照して、前記セキュリティ情報との関連性を比較する元となる参照元セキュリティ情報からキーワードを抽出し、該抽出されたキーワードと前記収集部によって収集されたセキュリティ情報に含まれるキーワードと

を比較して、前記参照元セキュリティ情報と前記セキュリティ情報との関連度を算出する算出部と、前記算出部によって算出された関連度が高いセキュリティ情報ほど優先的に出力する出力部と、を備えたことを特徴とする。

[0011] また、セキュリティ情報管理方法は、セキュリティ情報管理装置によって実行されるセキュリティ情報管理方法であって、セキュリティに関する情報であるセキュリティ情報を収集する収集工程と、前記セキュリティに関するキーワードを属性ごとに記憶するセキュリティ辞書を参照して、前記セキュリティ情報との関連性を比較する元となる参照元セキュリティ情報からキーワードを抽出し、該抽出されたキーワードと前記収集工程によって収集されたセキュリティ情報に含まれるキーワードとを比較して、前記参照元セキュリティ情報と前記セキュリティ情報との関連度を算出する算出工程と、前記算出工程によって算出された関連度が高いセキュリティ情報ほど優先的に出力する出力工程と、を含んだことを特徴とする。

発明の効果

[0012] 本願に開示するセキュリティ情報管理システム及びセキュリティ情報管理方法は、参照元セキュリティ情報と関連性の高いセキュリティ情報を、容易に収集することが可能である。

図面の簡単な説明

[0013] [図1]図１は、第一の実施形態に係るセキュリティ情報管理システムの構成の一例を示す図である。

[図2]図２は、第一の実施形態に係るセキュリティ辞書記憶部のセキュリティ辞書によって抽出される情報の一例を示す図である。

[図3]図３は、第一の実施形態に係るセキュリティ情報蓄積部によって記憶される情報の一例を示す図である。

[図4]図４は、セキュリティ情報関連性算出部による脆弱性スコア計算処理の一例について説明する図である。

[図5]図５は、第一の実施形態に係るセキュリティ情報管理装置におけるセキュリティ情報提供処理の流れを説明するためのフローチャートである。

[図6]図６は、セキュリティ情報管理プログラムを実行するコンピュータを示す図である。

発明を実施するための形態

[0014] 以下に添付図面を参照して、この発明に係るセキュリティ情報管理システム及びセキュリティ情報管理方法の実施形態を詳細に説明する。なお、この実施形態によりこの発明が限定されるものではない。

[0015] ［第一の実施形態］

以下の実施形態では、第一の実施形態に係るセキュリティ情報管理システム及びセキュリティ情報管理方法による処理の流れを順に説明し、最後に第一の実施形態による効果を説明する。

[0016] ［システムの構成］

まず、第一の実施形態に係るセキュリティ情報管理装置が適用されるセキュリティ情報管理システム１００の構成の一例を説明する。図１は、第一の実施形態に係るセキュリティ情報管理システムの構成の一例を示す図である。図１に示すように、第一の実施形態に係るセキュリティ情報管理装置１０が適用されるセキュリティ情報管理システム１００は、セキュリティ情報管理装置１０と、セキュリティ情報提供サーバ２０と、クライアント端末３０とを有する。また、セキュリティ情報管理システム１００では、セキュリティ情報管理装置１０とセキュリティ情報提供サーバ２０とは、インターネット４０を介して接続される。また、セキュリティ情報管理装置１０は、入出力インターフェース部１５を介してクライアント端末３０と接続される。

[0017] セキュリティ情報提供サーバ２０は、セキュリティ情報を公開するサーバである。例えば、セキュリティ情報提供サーバ２０は、セキュリティ情報として、情報システムを構成するソフトウェアやハードウェアのセキュリティ上の欠陥(例えば、『脆弱性』『セキュリティホール』などと表現される場合がある）と、その対策方法に関するテキスト情報（以下、脆弱性情報とする）を公開する。

[0018] また、例えば、セキュリティ情報提供サーバ２０は、セキュリティ情報と

して、上記したセキュリティ上の欠陥の悪用技術（『PoC(Proof of Concept)』『エクスプロイト』などと表現される場合がある）と、その対策方法に関するテキスト情報を公開する。

[0019] また、例えば、セキュリティ情報提供サーバ２０は、セキュリティ情報として、上記の悪用技術を利用して作成された、第三者の情報システムに被害を与えることを目的とした、悪性プログラム（『（コンピュータ）ウイルス』『マルウェア』などと表現される場合がある）と、その対策方法に関するテキスト情報を公開する。

[0020] また、例えば、セキュリティ情報提供サーバ２０は、セキュリティ情報として、上記した悪性プログラムを利用して実行された、他組織の情報システムへの攻撃（『標的型攻撃』『APT(Advanced Persistent Threat)攻撃』『サイバー攻撃』などと表現される場合がある）のニュースや事例に関するテキスト情報を公開する。

[0021] クライアント端末３０は、システム管理者がセキュリティ情報管理システム１００を利用するために用いる、標準的なＷｅｂブラウザを搭載したＰＣ等の情報処理装置である。また、クライアント端末３０は、セキュリティ情報管理装置１０から、参照元のセキュリティ情報と関連性の高いセキュリティ情報を受信し、該セキュリティ情報を表示する。

[0022] ［セキュリティ情報管理装置の構成］

次に、図１に示したセキュリティ情報管理装置１０の構成を説明する。図１に示すように、セキュリティ情報管理装置１０は、セキュリティ情報収集部１１、セキュリティ情報蓄積部１２、セキュリティ辞書記憶部１３、セキュリティ辞書管理部１４、入出力インターフェース部１５およびセキュリティ情報関連性算出部１６を有する。

[0023] セキュリティ情報収集部１１は、セキュリティに関する情報であるセキュリティ情報を収集する。具体的には、セキュリティ情報収集部１１は、セキュリティ情報提供サーバ２０に対して、所定の時間間隔で定期的にアクセスし、セキュリティ情報を取得する。これらは、ＨＴＭＬやＰＤＦなどの一般

的なドキュメントファイルとして取得する。そして、セキュリティ情報収集部１１は、取得したファイルを、所定の形式に加工し、追加情報を付与し、セキュリティ情報蓄積部１２に格納する。なお、セキュリティ情報収集部１１は、取得したファイルを、所定の形式に加工する際は、セキュリティ辞書記憶部１３を参照する。

[0024] 例えば、セキュリティ情報収集部１１は、ドキュメントファイルのタイトルおよび本文を抽出し、セキュリティ辞書記憶部１３に記憶されたセキュリティ辞書を参照して、該タイトルおよび本文に含まれるキーワードを抽出する。セキュリティ情報収集部１１は、設定情報として、収集対象とするセキュリティ情報提供サーバ２０の「ＵＲＬリスト」と、セキュリティ情報提供サーバ２０ごとに異なるフォーマットで提供されるセキュリティ情報からシステム管理者が必要とする「タイトル」および「本文」を抽出するための「切り出し位置情報」と、セキュリティ情報提供サーバ２０に対して収集を行うタイミングを示す「時刻や間隔を示す情報」とが設定されている。セキュリティ情報収集部１１は、これらの設定情報に基づいて、動作する。なお、「切り出し位置情報」は、ＵＲＬリストごとに定義される情報である。

[0025] 例えば、セキュリティ情報収集部１１は、設定情報で指定された時刻に、ＵＲＬリストで指定されたセキュリティ情報提供サーバ２０から、セキュリティ情報が記載されたＨＴＭＬファイルやＰＤＦ等のドキュメントファイルを取得する。そして、セキュリティ情報収集部１１は、取得したファイルから、『切り出し位置情報』に基づき、当該セキュリティ情報の「タイトル」および「本文」を抽出する。

[0026] 続いて、セキュリティ情報収集部１１は、抽出した「タイトル」および「本文」に含まれるキーワードを、セキュリティ辞書との比較により抽出し、情報提供サーバのＵＲＬ、ファイルを収集した時刻、抽出した「タイトル」および「本文」、抽出したすべてのキーワードをセキュリティ情報蓄積部１２に格納する（後に、図２を用いて詳述）。その後、セキュリティ情報収集部１１は、全てのＵＲＬリストについて処理が終了するまで、上記の処理を

繰り返し行う。

[0027] セキュリティ情報蓄積部１２は、セキュリティ情報収集部１１から受信したセキュリティ情報および追加情報を保存する。また、セキュリティ情報蓄積部１２は、セキュリティ情報関連性算出部１６から要求されたセキュリティ情報を、セキュリティ情報関連性算出部１６に送信する。また、セキュリティ情報蓄積部１２では、セキュリティ情報の属性として、脆弱性の種別、製品またはサービスの種別、製品の提供者またはサービスの提供者の種別、国または組織の種別、もしくは、サイバー攻撃の種別ごとに、セキュリティに関するキーワードが登録されている。

[0028] ここで、図３の例を用いて、セキュリティ情報蓄積部１２が記憶する情報例について説明する。図３は、第一の実施形態に係るセキュリティ情報蓄積部によって記憶される情報の一例を示す図である。図３に示すように、セキュリティ情報蓄積部１２は、セキュリティ情報ごとに、セキュリティ情報収集部１１により抽出されたキーワードを、「脆弱性」、「製品／サービス」、「製品／サービス提供者」、「国／組織名」および「サイバー攻撃」のカテゴリ別に記憶する。

[0029] セキュリティ辞書記憶部１３は、セキュリティ情報の関連性を判定する際に参照する、セキュリティ分野に関するキーワードの集合を記憶する。セキュリティ辞書記憶部１３では、セキュリティに関するキーワードを属性ごとに記憶するセキュリティ辞書を記憶しており、例えば、セキュリティ情報の特徴を表すキーワードの集合として、脆弱性辞書、製品／サービス辞書、製品／サービス提供者辞書、国／組織名辞書、サイバー攻撃辞書を記憶する。

[0030] セキュリティ辞書記憶部１３は、脆弱性辞書（同義語対応含む）として、例えば、バッファオーバーフロー、クロスサイトスクリプティング等を記憶し、製品／サービス辞書（同義語対応含む）として、例えば、Windows（登録商標） 7、Windows Server 2012、Twitter（登録商標）等を記憶し、製品／サービス提供者辞書（同義語対応含む）として、例えば、Microsoft（登録商標）、Google（登録商標）等を記憶し、国／組織名辞書（同義語対応含む

）として、例えば、中国、韓国、衆議院、企業名等を記憶し、サイバー攻撃辞書（同義語対応含む）として、例えば、サイバー攻撃、標的型攻撃、標的型メール、情報漏えい、改ざん等を記憶する。

[0031] また、各辞書集合の作成例について説明する。脆弱性辞書は、脆弱性について解説している国内外のサイトに掲載されたキーワードが、専用のクローラ等によって収集され、登録される。また、製品／サービス提供者辞書は、脆弱性情報を提供している国内外のサイトに登録された製品／サービス提供者の名称をキーワードとして、専用のクローラ等によって収集され、登録される。また、製品／サービス辞書は、製品／サービス提供者が運営する製品紹介サイトに登録された、製品／サービスの名称やバージョンをキーワードとして、専用のクローラ等によって収集され、登録される。また、国／組織名辞書は、国内外の官公庁、上場企業等のリストを、専用のクローラ等によって収集され、登録される。また、サイバー攻撃辞書は、サイバー攻撃の各種手口や方法について解説している国内外のサイトに掲載されたキーワードが、専用のクローラ等によって収集され、登録される。上記に加え、システム管理者がセキュリティ辞書管理部１４より手動で登録してもよい。

[0032] ここで、図２を用いて、セキュリティ辞書記憶部１３のセキュリティ辞書によって抽出される情報の例を説明する。図２は、第一の実施形態に係るセキュリティ辞書記憶部のセキュリティ辞書によって抽出される情報の一例を示す図である。図２に例示するように、セキュリティ情報蓄積部１２は、セキュリティ情報として、「情報提供サーバ（セキュリティ情報提供サーバ２０）から取得したセキュリティ情報のファイルのＵＲＬ」、「情報提供サーバからセキュリティ情報のファイルを収集した時刻」、「タイトル」、「本文」および「キーワード」を記憶する。「タイトル」、「本文」および「キーワード」は、セキュリティ辞書記憶部１３に記憶されたセキュリティ辞書が参照され、セキュリティ情報のファイルから抽出された情報である。また、抽出したすべてのキーワードは、各セキュリティ辞書の分類に基づいて格納される。なお、一つもキーワードが抽出されなかった場合は、キーワード

に対応する「内容」は空で格納される。

[0033] セキュリティ辞書管理部１４は、辞書に含まれる、セキュリティ分野に関するキーワードについて、追加、削除を行う。例えば、セキュリティ辞書管理部１４は、システム管理者の操作指示を受け付けて、セキュリティ分野に関するキーワードについて、追加、削除を行う。

[0034] 入出力インターフェース部１５は、クライアント端末３０からの要求を受信し、要求に対する応答として、関連性判定の結果をクライアント端末３０へ送信する。具体的には、入出力インターフェース部１５は、システム管理者のクライアント端末３０から、参照元セキュリティ情報、脆弱性スコアの閾値、製品／サービススコアの閾値、製品／サービス提供者スコアの閾値、国／組織名スコアの閾値およびサイバー攻撃スコアの閾値を受け取り、セキュリティ情報関連性算出部１６へ送信する。

[0035] ここで、脆弱性スコアとは、参照元セキュリティ情報とセキュリティ情報蓄積部１２に蓄積された各セキュリティ情報を、「脆弱性辞書」を用いて比較した場合の関連性を表す数値である。製品／サービススコアとは、参照元セキュリティ情報とセキュリティ情報蓄積部１２に蓄積された各セキュリティ情報を、「製品／サービス辞書」を用いて比較した場合の関連性を表す数値である。製品／サービス提供者スコアとは、参照元セキュリティ情報とセキュリティ情報蓄積部１２に蓄積された各セキュリティ情報を、「製品／サービス提供者辞書」を用いて比較した場合の関連性を表す数値である。国／組織名スコアとは、参照元セキュリティ情報とセキュリティ情報蓄積部１２に蓄積された各セキュリティ情報を、「国／組織名辞書」を用いて比較した場合の関連性を表す数値である。サイバー攻撃スコアとは、参照元セキュリティ情報とセキュリティ情報蓄積部１２に蓄積された各セキュリティ情報を、「サイバー攻撃辞書」を用いて比較した場合の関連性を表す数値である。

[0036] また、脆弱性スコアの閾値、製品／サービススコアの閾値、製品／サービス提供者スコアの閾値、国／組織名スコアの閾値およびサイバー攻撃スコアの閾値は、参照元セキュリティ情報とセキュリティ情報蓄積部１２に蓄積さ

れた各セキュリティ情報を、上記５種のスコアに基づき関連性を判定するための指標値である。セキュリティ情報蓄積部１２に蓄積されたセキュリティ情報のうち、閾値を上回るスコアを持つセキュリティ情報を、「参照元セキュリティ情報との関連性がある」と判断する。また、各閾値は、上記５種のスコアの各々に対して、システム管理者が個別に設定する。例えば、システム管理者が、クライアント端末３０から、入出力インターフェース１５を通じて、セキュリティ情報関連性算出部１６に各閾値を送信する。

[0037] 参照元セキュリティ情報の入力には、任意のテキストを入力できるテキストボックスを表示しておき、システム管理者に入力させる機能を搭載してもよい。参照元セキュリティ情報の入力には、表示中のセキュリティ情報をワンクリックでセキュリティ情報関連性算出部１６に送信する操作を行うボタンをクライアント端末３０のブラウザ画面に表示してもよい。各閾値の入力には、スコア計算式でとりえる値を選択肢として表示しておき、システム管理者に選択させる機能を搭載してもよい。

[0038] また、各閾値の入力には、あらかじめ標準的な値を設定しておき、システム管理者からの閾値の入力がない場合は、その標準的な値を使用するようにし、システム管理者が、都度、閾値を入力する操作の負担を軽減する機能を搭載してもよい。

[0039] また、入出力インターフェース部１５は、セキュリティ情報関連性算出部１６から、スコア合計値を受け取り、参照元セキュリティ情報との関連性を表す５種のスコアの全てについて送信した閾値を超えているセキュリティ情報を、合計値が高い順にクライアント端末３０に表示する。なお、表示する際、セキュリティ情報が持つ「情報提供サーバから取得したセキュリティ情報のファイルのＵＲＬ」、「情報提供サーバからセキュリティ情報のファイルを収集した時刻」、「セキュリティ情報の『タイトル』および『本文』に含まれるキーワード」を用いたフィルタによって、表示するセキュリティ情報をさらに絞り込む機能を搭載してもよい。参照元セキュリティ情報との関連性の高いセキュリティ情報の表示後、表示された結果を、テキストファイ

ルやＰＤＦ等のドキュメントファイルの形式で外部にエクスポートする機能を搭載してもよい。

[0040] セキュリティ情報関連性算出部１６は、セキュリティに関するキーワードを属性ごとに記憶するセキュリティ辞書記憶部１３を参照して、セキュリティ情報との関連性を比較する元となる参照元セキュリティ情報からキーワードを抽出し、該抽出されたキーワードとセキュリティ情報収集部１１によって収集されたセキュリティ情報に含まれるキーワードとを比較して、参照元セキュリティ情報とセキュリティ情報との関連度を算出する。

[0041] セキュリティ情報関連性算出部１６は、入出力インターフェース部１５からの要求に基づき、セキュリティ情報蓄積部１２に格納されたセキュリティ情報を取得し、関連性判定を行う。そして、セキュリティ情報関連性算出部１６は、関連性判定の結果を入出力インターフェース部１５を介してクライアント端末３０に送信する。入出力インターフェース部１５は、セキュリティ情報関連性算出部１６によって算出された関連度が高いセキュリティ情報ほど優先的にクライアント端末３０へ出力する。

[0042] 例えば、セキュリティ情報関連性算出部１６は、設定情報として、クライアント端末３０から入出力インターフェース部１５を介して、セキュリティ情報蓄積部１２のセキュリティ情報との関連性を比較する元となる参照元セキュリティ情報、脆弱性スコアの閾値、製品／サービススコアの閾値、製品／サービス提供者スコアの閾値、国／組織名スコアの閾値およびサイバー攻撃スコアの閾値を受信する。

[0043] 以下では、セキュリティ情報関連性算出部１６による具体的な処理の流れを説明する。セキュリティ情報関連性算出部１６は、セキュリティ辞書を参照し、脆弱性の種別、製品またはサービスの種別、製品の提供者またはサービスの提供者の種別、国または組織の種別、もしくは、サイバー攻撃の種別ごとに、参照元セキュリティ情報からキーワードをそれぞれ抽出する。

[0044] そして、セキュリティ情報関連性算出部１６は、参照元セキュリティ情報から抽出したキーワードと、セキュリティ情報蓄積部１２に蓄積した各セキ

ュリティ情報の脆弱性キーワードを比較し、脆弱性スコアを計算する。具体的には、セキュリティ情報関連性算出部１６は、セキュリティ辞書を参照し、脆弱性の種別、製品またはサービスの種別、製品の提供者またはサービスの提供者の種別、国または組織の種別、もしくは、サイバー攻撃の種別ごとに、参照元セキュリティ情報からキーワードをそれぞれ抽出し、参照元セキュリティ情報から抽出されたキーワードと収集部によって収集されたセキュリティ情報に含まれるキーワードとをそれぞれ比較して、参照元セキュリティ情報とセキュリティ情報との関連度を算出する。

[0045] ここで、図４の例を用いて、セキュリティ情報関連性算出部１６による脆弱性スコア計算処理の一例について説明する。図４は、セキュリティ情報関連性算出部による脆弱性スコア計算処理の一例について説明する図である。図４に示すように、まず、セキュリティ情報関連性算出部１６は、入出力インターフェース部１５を介して、テキストおよび本文を含む参照元セキュリティ情報をクライアント端末３０から受信する。

[0046] そして、セキュリティ情報関連性算出部１６は、例えば、参照元セキュリティ情報から、脆弱性辞書に含まれるキーワードとして、「バッファオーバーフロー」を抽出する。そして、セキュリティ情報関連性算出部１６は、参照元セキュリティ情報から抽出したキーワード「バッファオーバーフロー」と、セキュリティ情報蓄積部１２に蓄積したセキュリティ情報Ａ、Ｂの脆弱性キーワードを比較し、脆弱性スコアを計算する。

[0047] 図４の例では、セキュリティ情報Ａの脆弱性キーワードが「バッファオーバーフロー」であり、参照元セキュリティ情報から抽出したキーワードと一致しているため、セキュリティ情報Ａの脆弱性スコア「ａ」と計算する。また、セキュリティ情報Ｂの脆弱性キーワードが「クロスサイトスクリプティング」であり、参照元セキュリティ情報から抽出したキーワードと一致しないため、セキュリティ情報Ｂの脆弱性スコア「ｂ」と計算する。セキュリティ情報Ａの脆弱性スコア「ａ」の方が、セキュリティ情報Ｂの脆弱性スコア「ｂ」よりも高いスコアである。例えば、一致したキーワード数に基づいて

、スコアを算出してもよい。例えば、セキュリティ情報Ａの脆弱性スコアを「１」とし、セキュリティ情報Ｂの脆弱性スコアを「０」とする。

[0048] また、商用／フリーの機械学習ライブラリを用いて、スコアを算出してもよく、それぞれ特徴ベクトル化し、特徴ベクトル間の類似度を、数値で求めることができる。この方法を用いることで、キーワードが完全一致しないような類似のキーワードを持つセキュリティ情報同士の類似度も判定が可能となる。

[0049] 続いて、セキュリティ情報関連性算出部１６は、「製品／サービス辞書」について、同様に、製品／サービススコアを計算する。そして、セキュリティ情報関連性算出部１６は、「製品／サービス提供者辞書」について、同様に、製品／サービス提供者スコアを計算する。

[0050] その後、セキュリティ情報関連性算出部１６は、「国／組織名辞書」について、同様に、国／組織名スコアを計算する。そして、セキュリティ情報関連性算出部１６は、「サイバー攻撃辞書」について、同様に、サイバー攻撃スコアを計算する。なお、各スコアについて重み付けを設定してもよい。

[0051] そして、セキュリティ情報関連性算出部１６は、スコアを合算する。そして、セキュリティ情報関連性算出部１６は、スコアの合算値が高い順に、セキュリティ情報蓄積部１２のセキュリティ情報をソートする。ただし、ソートする際、上記した５種の閾値を一つでも下回るスコアを持つセキュリティ情報は、ソートの対象から除外する。

[0052] そして、セキュリティ情報関連性算出部１６は、ソートされた順番で、セキュリティ情報を入出力インターフェース部１５に送信する。なお、処理の速度を向上するため、この際に送信されるセキュリティ情報の件数には、システム的な上限を設定してもよい。

[0053] ［セキュリティ情報管理装置による処理］

次に、図５を用いて、第一の実施形態に係るセキュリティ情報管理装置１０による処理を説明する。図５は、第一の実施形態に係るセキュリティ情報管理装置におけるセキュリティ情報提供処理の流れを説明するためのフロー

チャートである。

[0054] まず、図５を用いて、第一の実施形態に係るセキュリティ情報管理装置におけるセキュリティ情報提供処理の流れを説明する。図５に示すように、セキュリティ情報管理装置１０のセキュリティ情報関連性算出部１６は、クライアント端末３０から入出力インターフェース部１５を介して、参照元セキュリティ情報を受信すると（ステップＳ１０１）、セキュリティ情報関連性算出部１６は、参照元セキュリティ情報から、セキュリティ辞書に含まれるキーワードを抽出する（ステップＳ１０２）。

[0055] そして、セキュリティ情報関連性算出部１６は、参照元セキュリティ情報から抽出したキーワードと、セキュリティ情報蓄積部１２に蓄積した各セキュリティ情報の脆弱性キーワードを比較し、脆弱性スコアを計算する（ステップＳ１０３）。

[0056] セキュリティ情報関連性算出部１６は、「製品／サービス辞書」について、ステップＳ１０３と同様に、製品／サービススコアを計算する（ステップＳ１０４）。そして、セキュリティ情報関連性算出部１６は、「製品／サービス提供者辞書」について、ステップＳ１０３と同様に、製品／サービス提供者スコアを計算する（ステップＳ１０５）。

[0057] その後、セキュリティ情報関連性算出部１６は、「国／組織名辞書」について、ステップＳ１０３と同様に、国／組織名スコアを計算する（ステップＳ１０６）。そして、セキュリティ情報関連性算出部１６は、「サイバー攻撃辞書」について、ステップＳ１０３と同様に、サイバー攻撃スコアを計算する（ステップＳ１０７）。

[0058] そして、セキュリティ情報関連性算出部１６は、各スコアを合算する（ステップＳ１０８）。そして、セキュリティ情報関連性算出部１６は、スコアの合算値が高い順に、セキュリティ情報蓄積部１２のセキュリティ情報をソートする（ステップＳ１０９）。ただし、ソートする際、上記した５種の閾値を一つでも下回るスコアを持つセキュリティ情報は、ソートの対象から除外する。

[0059] そして、セキュリティ情報関連性算出部１６は、ソートされた順番で、セキュリティ情報を入出力インターフェース部１５に送信する（ステップＳ１１０）。

[0060] ［第一の実施形態の効果］

上述してきたように、第一の実施形態にかかるセキュリティ情報管理装置１０では、セキュリティに関する情報であるセキュリティ情報を収集する。そして、セキュリティ情報管理装置１０は、セキュリティに関するキーワードを属性ごとに記憶するセキュリティ辞書を参照して、セキュリティ情報との関連性を比較する元となる参照元セキュリティ情報からキーワードを抽出し、該抽出されたキーワードと収集されたセキュリティ情報に含まれるキーワードとを比較して、参照元セキュリティ情報とセキュリティ情報との関連度を算出する。そして、セキュリティ情報管理装置１０は、算出された関連度が高いセキュリティ情報ほど優先的に出力する。これにより、参照元セキュリティ情報と関連性の高いセキュリティ情報を、容易に出力することが可能である。

[0061] また、セキュリティ情報管理装置１０では、セキュリティ情報提供サーバ２０から、所定の時間間隔で、セキュリティ情報を含むファイル情報を収集し、該ファイル情報のタイトルおよび本文を抽出し、該タイトルおよび本文に含まれるキーワードを抽出する。セキュリティ情報管理装置１０は、抽出されたタイトルおよび本文に含まれるキーワードと、参照元セキュリティ情報から抽出されたキーワードとを比較して関連度を算出する。このため、セキュリティ情報のタイトルおよび本文に含まれるキーワードと、参照元セキュリティ情報から抽出されたキーワードとを比較して関連度を適切に算出することが可能である。

[0062] また、セキュリティ情報管理装置１０では、参照元セキュリティ情報から抽出されたキーワードと収集されたセキュリティ情報に含まれるキーワードとが一致するか否かを判定し、一致する場合には、一致しない場合よりも関連度を高く算出する。このため、関連度を容易に算出することが可能である

。

[0063] また、セキュリティ情報管理装置１０では、関連度を算出したセキュリティ情報について、関連度が高い順にソートし、ソートされた順番で、セキュリティ情報を出力する。このため、参照元セキュリティ情報と関連性の高いセキュリティ情報を分かりやすく出力することが可能である。

[0064] また、セキュリティ情報管理装置１０では、セキュリティ情報の属性として、脆弱性の種別、製品またはサービスの種別、製品の提供者またはサービスの提供者の種別、国または組織の種別、もしくは、サイバー攻撃の種別ごとに、セキュリティに関するキーワードがセキュリティ辞書に登録される。そして、セキュリティ情報管理装置１０は、セキュリティ辞書を参照し、脆弱性の種別、製品またはサービスの種別、製品の提供者またはサービスの提供者の種別、国または組織の種別、もしくは、サイバー攻撃の種別ごとに、参照元セキュリティ情報からキーワードをそれぞれ抽出する。このため、キーワードを適切に抽出することが可能である。

[0065] また、セキュリティ情報管理装置１０では、セキュリティ辞書を参照し、脆弱性の種別、製品またはサービスの種別、製品の提供者またはサービスの提供者の種別、国または組織の種別、もしくは、サイバー攻撃の種別ごとに、参照元セキュリティ情報からキーワードをそれぞれ抽出し、参照元セキュリティ情報から抽出されたキーワードと収集されたセキュリティ情報に含まれるキーワードとをそれぞれ比較して、参照元セキュリティ情報とセキュリティ情報との関連度を算出する。このため、関連度を容易に算出することが可能である。

[0066] ［システム構成等］

また、図示した各装置の各構成要素は機能概念的なものであり、必ずしも物理的に図示の如く構成されていることを要しない。すなわち、各装置の分散・統合の具体的形態は図示のものに限られず、その全部または一部を、各種の負荷や使用状況などに応じて、任意の単位で機能的または物理的に分散・統合して構成することができる。例えば、セキュリティ情報収集部１１と

セキュリティ情報関連性算出部１６とを統合してもよい。さらに、各装置にて行なわれる各処理機能は、その全部または任意の一部が、ＣＰＵおよび当該ＣＰＵにて解析実行されるプログラムにて実現され、あるいは、ワイヤードロジックによるハードウェアとして実現され得る。

[0067] また、本実施例において説明した各処理のうち、自動的におこなわれるものとして説明した処理の全部または一部を手動的に行うこともでき、あるいは、手動的におこなわれるものとして説明した処理の全部または一部を公知の方法で自動的におこなうこともできる。この他、上記文書中や図面中で示した処理手順、制御手順、具体的名称、各種のデータやパラメータを含む情報については、特記する場合を除いて任意に変更することができる。

[0068] ［プログラム］

また、上記実施形態において説明したセキュリティ情報管理装置１０が実行する処理をコンピュータが実行可能な言語で記述したプログラムを作成することもできる。例えば、第一の実施形態に係るセキュリティ情報管理装置１０が実行する処理をコンピュータが実行可能な言語で記述したセキュリティ情報管理プログラムを作成することもできる。この場合、コンピュータがセキュリティ情報管理プログラムを実行することにより、上記実施形態と同様の効果を得ることができる。さらに、かかるセキュリティ情報管理プログラムをコンピュータ読み取り可能な記録媒体に記録して、この記録媒体に記録されたセキュリティ情報管理プログラムをコンピュータに読み込ませて実行することにより上記第一の実施形態と同様の処理を実現してもよい。以下に、図１に示したセキュリティ情報管理装置１０と同様の機能を実現するセキュリティ情報管理プログラムを実行するコンピュータの一例を説明する。

[0069] 図６は、セキュリティ情報管理プログラムを実行するコンピュータ１０００を示す図である。図６に例示するように、コンピュータ１０００は、例えば、メモリ１０１０と、ＣＰＵ１０２０と、ハードディスクドライブインターフェース１０３０と、ディスクドライブインターフェース１０４０と、シリアルポートインターフェース１０５０と、ビデオアダプタ１０６０と、ネ

ットワークインターフェース１０７０とを有し、これらの各部はバス１０８０によって接続される。

[0070] メモリ１０１０は、図６に例示するように、ＲＯＭ（Read Only Memory）１０１１及びＲＡＭ１０１２を含む。ＲＯＭ１０１１は、例えば、ＢＩＯＳ（Basic Input Output System）等のブートプログラムを記憶する。ハードディスクドライブインターフェース１０３０は、図６に例示するように、ハードディスクドライブ１０３１に接続される。ディスクドライブインターフェース１０４０は、図６に例示するように、ディスクドライブ１０４１に接続される。例えば磁気ディスクや光ディスク等の着脱可能な記憶媒体が、ディスクドライブ１０４１に挿入される。シリアルポートインターフェース１０５０は、図６に例示するように、例えばマウス１０５１、キーボード１０５２に接続される。ビデオアダプタ１０６０は、図６に例示するように、例えばディスプレイ１０６１に接続される。

[0071] ここで、図６に例示するように、ハードディスクドライブ１０３１は、例えば、ＯＳ１０９１、アプリケーションプログラム１０９２、プログラムモジュール１０９３、プログラムデータ１０９４を記憶する。すなわち、上記のセキュリティ情報管理プログラムは、コンピュータ１０００によって実行される指令が記述されたプログラムモジュールとして、例えばハードディスクドライブ１０３１に記憶される。

[0072] また、上記実施形態で説明した各種データは、プログラムデータとして、例えばメモリ１０１０やハードディスクドライブ１０３１に記憶される。そして、ＣＰＵ１０２０が、メモリ１０１０やハードディスクドライブ１０３１に記憶されたプログラムモジュール１０９３やプログラムデータ１０９４を必要に応じてＲＡＭ１０１２に読み出し、各種処理手順を実行する。

[0073] なお、セキュリティ情報管理プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ハードディスクドライブ１０３１に記憶される場合に限られず、例えば着脱可能な記憶媒体に記憶され、ディスクドライブ等を介してＣＰＵ１０２０によって読み出されてもよい。あるいは

、セキュリティ情報管理プログラムに係るプログラムモジュール１０９３やプログラムデータ１０９４は、ネットワーク（ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）等）を介して接続された他のコンピュータに記憶され、ネットワークインターフェース１０７０を介してＣＰＵ１０２０によって読み出されてもよい。

符号の説明

[0074] １０　セキュリティ情報管理装置

１１　セキュリティ情報収集部

１２　セキュリティ情報蓄積部

１３　セキュリティ辞書記憶部

１４　セキュリティ辞書管理部

１５　入出力インターフェース部

１６　セキュリティ情報関連性算出部

２０　セキュリティ情報提供サーバ

３０　クライアント端末

４０　インターネット

１００　セキュリティ情報管理システム

請求の範囲

[請求項1] セキュリティに関する情報であるセキュリティ情報を収集する収集部と、

前記セキュリティに関するキーワードを属性ごとに記憶するセキュリティ辞書を参照して、前記セキュリティ情報との関連性を比較する元となる参照元セキュリティ情報からキーワードを抽出し、該抽出されたキーワードと前記収集部によって収集されたセキュリティ情報に含まれるキーワードとを比較して、前記参照元セキュリティ情報と前記セキュリティ情報との関連度を算出する算出部と、

前記算出部によって算出された関連度が高いセキュリティ情報ほど優先的に出力する出力部と、

を備えたことを特徴とするセキュリティ情報管理システム。

[請求項2] 前記収集部は、外部の装置から、所定の時間間隔で、セキュリティ情報を含むファイル情報を収集し、該ファイル情報のタイトルおよび本文を抽出し、該タイトルおよび本文に含まれるキーワードを抽出し、

前記算出部は、前記収集部によって抽出されたタイトルおよび本文に含まれるキーワードと、前記参照元セキュリティ情報から抽出されたキーワードとを比較して関連度を算出することを特徴とする請求項１に記載のセキュリティ情報管理システム。

[請求項3] 前記算出部は、前記参照元セキュリティ情報から抽出されたキーワードと前記収集部によって収集されたセキュリティ情報に含まれるキーワードとが一致するか否かを判定し、一致する場合には、一致しない場合よりも関連度を高く算出することを特徴とする請求項１に記載のセキュリティ情報管理システム。

[請求項4] 前記算出部は、前記参照元セキュリティ情報から抽出されたキーワードと前記収集部によって収集されたセキュリティ情報に含まれるキーワードとが一致するか否かを判定し、一致する場合には、一致しな

い場合よりも関連度を高く算出することを特徴とする請求項２に記載のセキュリティ情報管理システム。

[請求項5] 前記算出部は、関連度を算出したセキュリティ情報について、関連度が高い順にソートし、

前記出力部は、前記算出部によってソートされた順番で、前記セキュリティ情報を出力することを特徴とする請求項１に記載のセキュリティ情報管理システム。

[請求項6] 前記算出部は、関連度を算出したセキュリティ情報について、関連度が高い順にソートし、

前記出力部は、前記算出部によってソートされた順番で、前記セキュリティ情報を出力することを特徴とする請求項２に記載のセキュリティ情報管理システム。

[請求項7] 前記算出部は、関連度を算出したセキュリティ情報について、関連度が高い順にソートし、

前記出力部は、前記算出部によってソートされた順番で、前記セキュリティ情報を出力することを特徴とする請求項３に記載のセキュリティ情報管理システム。

[請求項8] 前記算出部は、関連度を算出したセキュリティ情報について、関連度が高い順にソートし、

前記出力部は、前記算出部によってソートされた順番で、前記セキュリティ情報を出力することを特徴とする請求項４に記載のセキュリティ情報管理システム。

[請求項9] 前記セキュリティ情報の属性として、脆弱性の種別、製品またはサービスの種別、製品の提供者またはサービスの提供者の種別、国または組織の種別、もしくは、サイバー攻撃の種別ごとに、セキュリティに関するキーワードが前記セキュリティ辞書に登録され、

前記算出部は、前記セキュリティ辞書を参照し、前記脆弱性の種別、前記製品またはサービスの種別、前記製品の提供者またはサービス

の提供者の種別、前記国または組織の種別、もしくは、前記サイバー攻撃の種別ごとに、前記参照元セキュリティ情報からキーワードをそれぞれ抽出することを特徴とする請求項１～８のいずれか一つに記載のセキュリティ情報管理システム。

[請求項10] 前記算出部は、前記セキュリティ辞書を参照し、前記脆弱性の種別、前記製品またはサービスの種別、前記製品の提供者またはサービスの提供者の種別、前記国または組織の種別、もしくは、前記サイバー攻撃の種別ごとに、前記参照元セキュリティ情報からキーワードをそれぞれ抽出し、前記参照元セキュリティ情報から抽出されたキーワードと前記収集部によって収集されたセキュリティ情報に含まれるキーワードとをそれぞれ比較して、前記参照元セキュリティ情報と前記セキュリティ情報との関連度を算出することを特徴とする請求項９に記載のセキュリティ情報管理システム。

[請求項11] 前記算出部は、前記セキュリティ辞書を参照し、前記脆弱性の種別、前記製品またはサービスの種別、前記製品の提供者またはサービスの提供者の種別、前記国または組織の種別、もしくは、前記サイバー攻撃の種別ごとに、前記参照元セキュリティ情報からキーワードをそれぞれ抽出し、前記参照元セキュリティ情報から抽出されたキーワードと前記収集部によって収集されたセキュリティ情報に含まれるキーワードとをそれぞれ比較して関連度を算出し、各関連度を合算してスコアを算出し、

前記出力部は、前記算出部によって算出されたスコアが高いセキュリティ情報ほど優先的に出力することを特徴とする請求項１０に記載のセキュリティ情報管理システム。

[請求項12] セキュリティ情報管理装置によって実行されるセキュリティ情報管理方法であって、

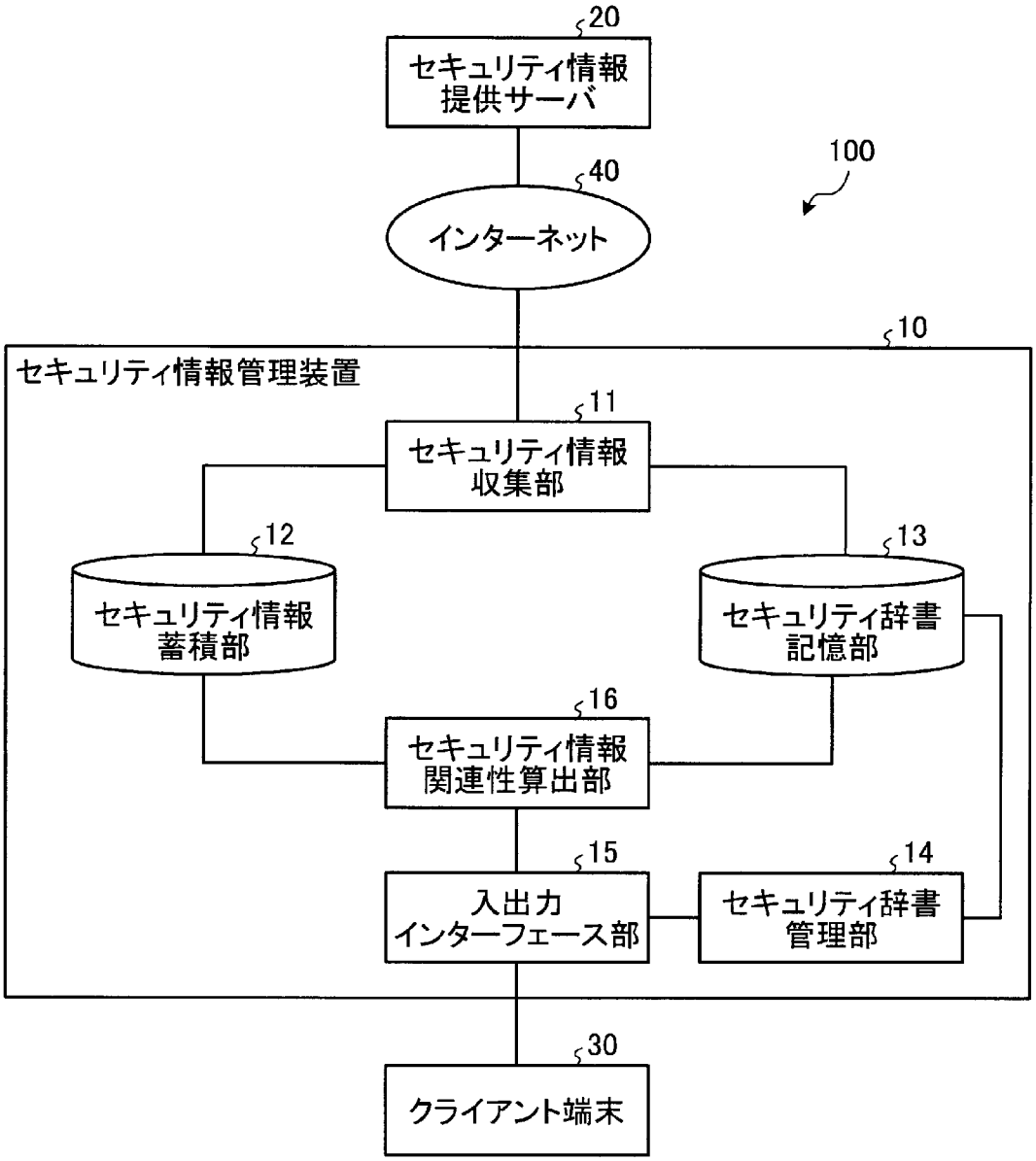
セキュリティに関する情報であるセキュリティ情報を収集する収集工程と、

前記セキュリティに関するキーワードを属性ごとに記憶するセキュリティ辞書を参照して、前記セキュリティ情報との関連性を比較する元となる参照元セキュリティ情報からキーワードを抽出し、該抽出されたキーワードと前記収集工程によって収集されたセキュリティ情報に含まれるキーワードとを比較して、前記参照元セキュリティ情報と前記セキュリティ情報との関連度を算出する算出工程と、

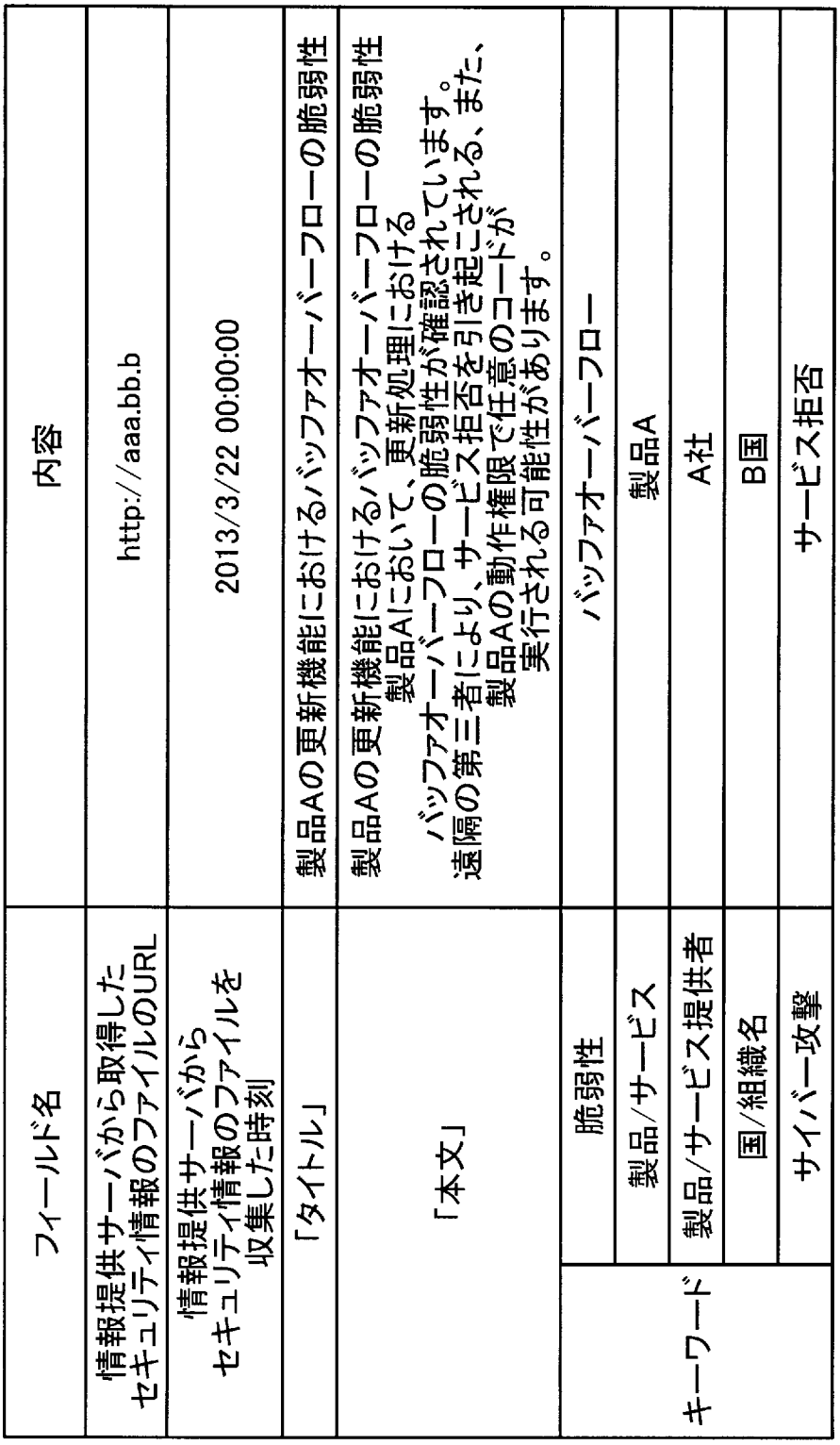
前記算出工程によって算出された関連度が高いセキュリティ情報ほど優先的に出力する出力工程と、

を含んだことを特徴とするセキュリティ情報管理方法。

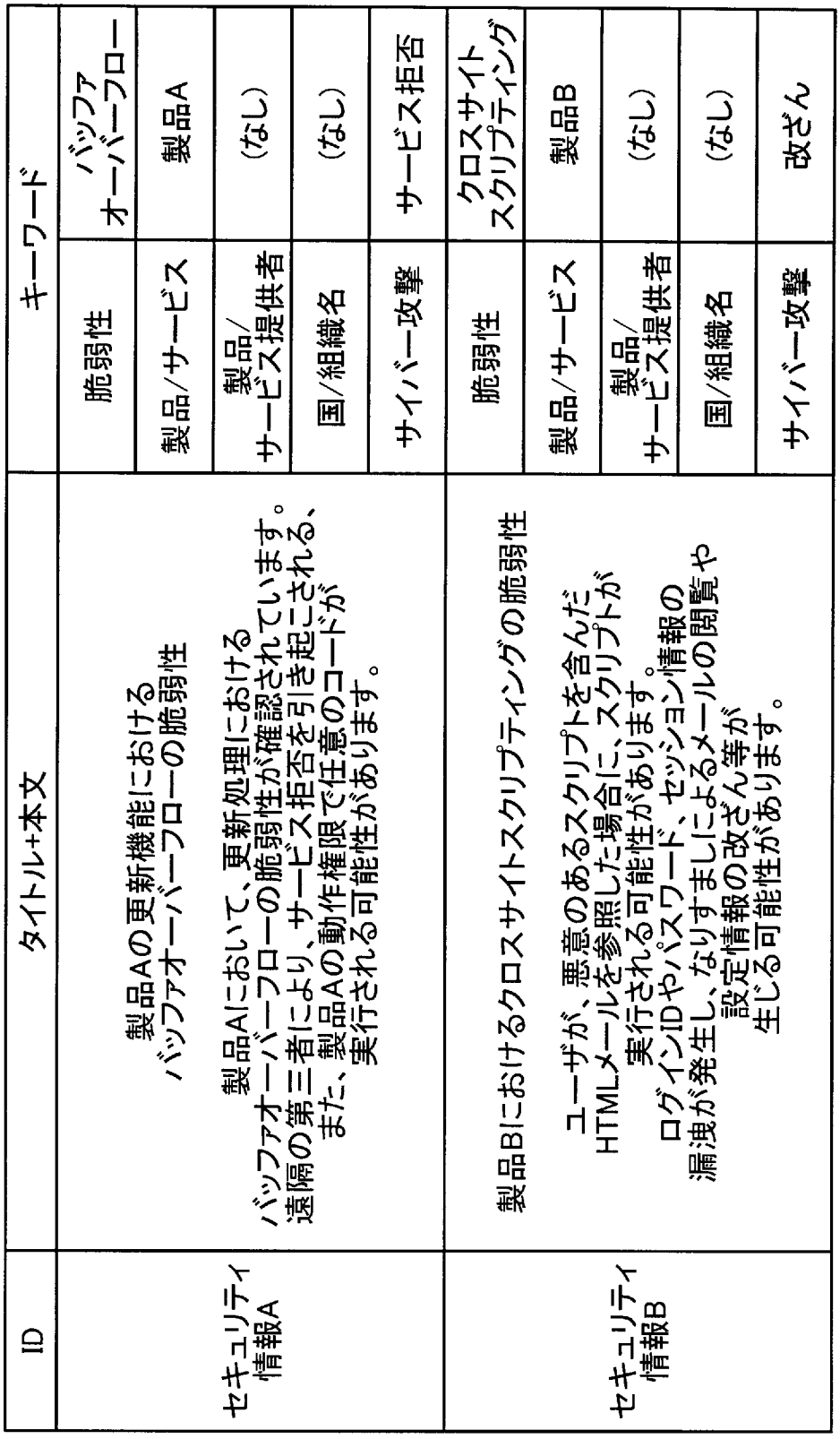
[図1]


20
セキュリティ情報
提供サーバ
100
40
インターネット
10
セキュリティ情報管理装置
11
セキュリティ情報
収集部
12
セキュリティ情報
蓄積部
13
セキュリティ辞書
記憶部
16
セキュリティ情報
関連性算出部
15
入出力
インターフェース部
14
セキュリティ辞書
管理部
30
クライアント端末

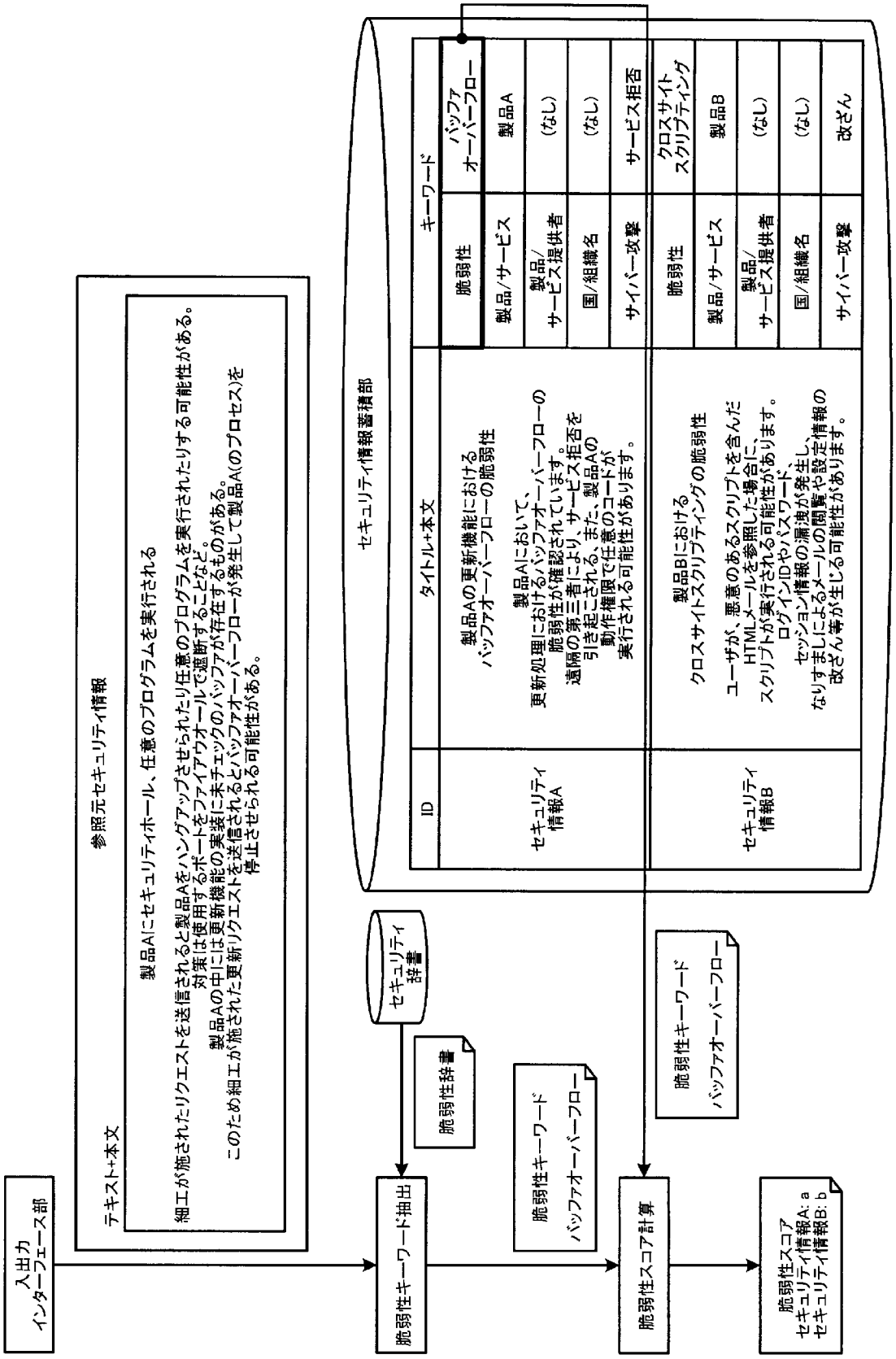
[図2]


フィールド名
内容
情報提供サーバから取得した
セキュリティ情報のファイルのURL
http://aaa.bb.b
情報提供サーバから
セキュリティ情報のファイルを
収集した時刻
2013/3/22 00:00:00
「タイトル」
製品Aの更新機能におけるバッファオーバーフローの脆弱性
「本文」
製品Aの更新機能におけるバッファオーバーフローの脆弱性
製品Aにおいて、更新処理における
バッファオーバーフローの脆弱性が確認されています。
遠隔の第三者により、サービス拒否を引き起こされる、また、
製品Aの動作権限で任意のコードが
実行される可能性があります。
キーワード
脆弱性
バッファオーバーフロー
製品/サービス
製品A
製品/サービス提供者
A社
国/組織名
B国
サイバー攻撃
サービス拒否

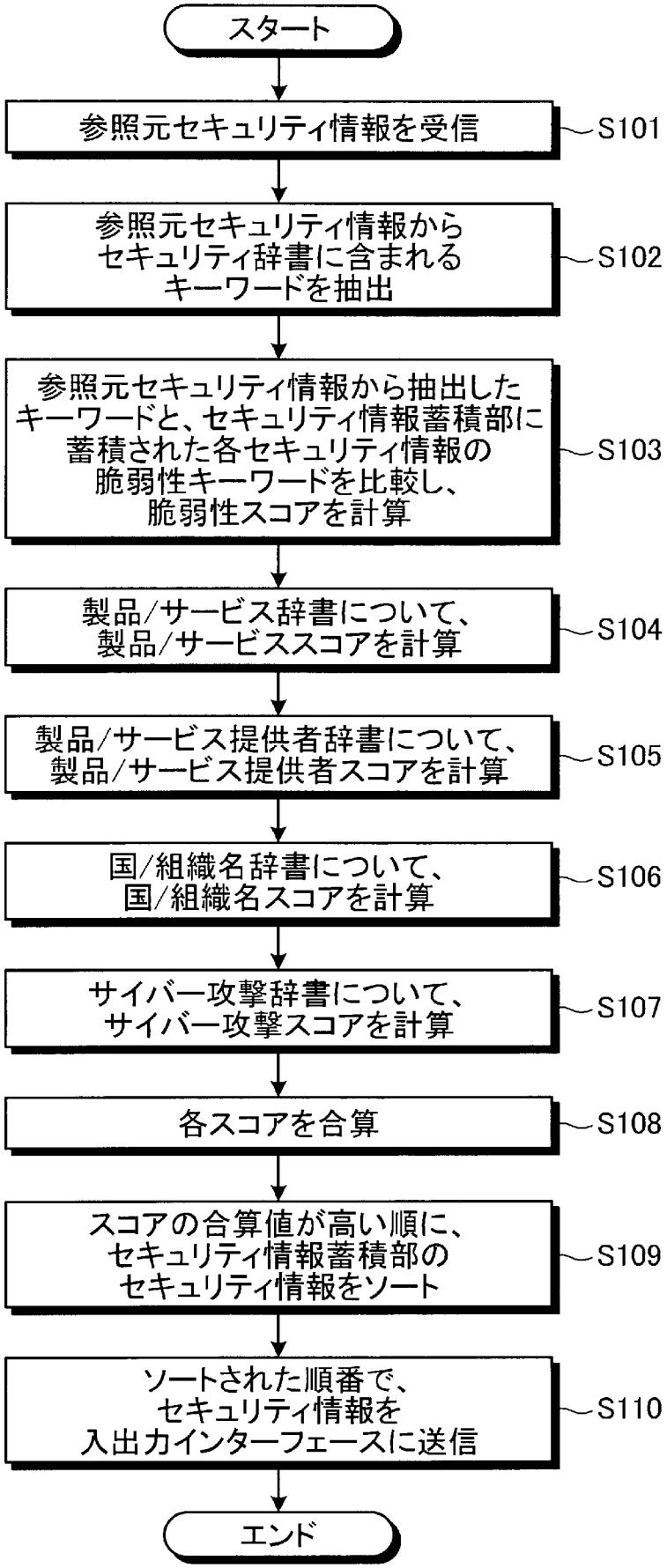
[図3]


ID
タイトル+本文
キーワード
セキュリティ情報A
製品Aの更新機能における
バッファオーバーフローの脆弱性
製品Aにおいて、更新処理における
バッファオーバーフローの脆弱性が確認されています。
遠隔の第三者により、サービス拒否を引き起こされる、
また、製品Aの動作権限で任意のコードが
実行される可能性があります。
脆弱性
バッファ
オーバーフロー
製品／サービス
製品A
製品／
サービス提供者
(なし)
国／組織名
(なし)
サイバー攻撃
サービス拒否
セキュリティ情報B
製品Bにおけるクロスサイトスクリプティングの脆弱性
ユーザが、悪意のあるスクリプトを含んだ
HTMLメールを参照した場合に、スクリプトが
実行される可能性があります。
ログインIDやパスワード、セッション情報の
漏洩が発生し、なりすましによるメールの閲覧や
設定情報の改ざん等が
生じる可能性があります。
脆弱性
クロスサイト
スクリプティング
製品／サービス
製品B
製品／
サービス提供者
(なし)
国／組織名
(なし)
サイバー攻撃
改ざん

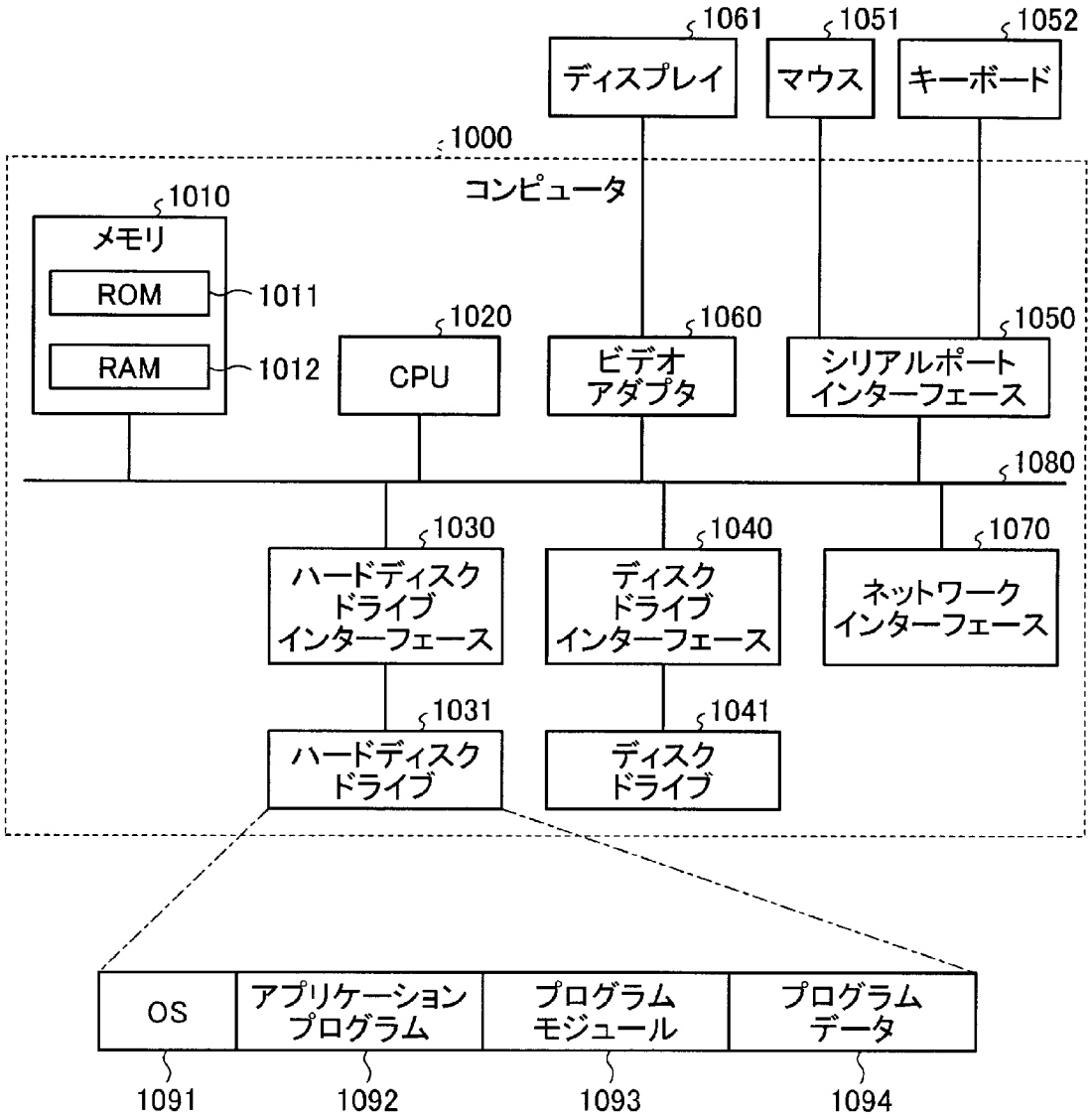
[図4]


入出力
インターフェース部
参照元セキュリティ情報
テキスト+本文
製品Aにセキュリティホール、任意のプログラムを実行される
細工が施されたリクエストを送信されると製品Aをハングアップさせられたり任意のプログラムを実行されたりする可能性がある。
対策は使用するポートをファイアウオールで遮断することなど。
製品Aの中には更新機能に未チェックのバッファが存在するものがある。
このため細工が施された更新リクエストを送信されるとバッファオーバーフローが発生して製品A(のプロセス)を
停止させられる可能性がある。
セキュリティ情報蓄積部
ID
タイトル+本文
キーワード
脆弱性
バッファオーバーフロー
セキュリティ情報A
製品Aの更新機能における
バッファオーバーフローの脆弱性
製品/サービス
製品A
製品AにおいてバッファオーバーフローのIPアドレス
更新処理における
脆弱性が確認されています。
製品/サービス提供者
(なし)
遠隔の第三者により、サービス拒否を
引き起こされる、また、製品Aの
国/組織名
(なし)
動作権限で任意のコードが
実行される可能性があります。
サイバー攻撃
サービス拒否
セキュリティ情報B
製品Bにおける
クロスサイトスクリプティングの脆弱性
脆弱性
クロスサイトスクリプティング
ユーザが、悪意のあるスクリプトを含んだ
HTMLメールを参照した場合に、
製品/サービス
製品B
スクリプトが実行される可能性があります。
ログインIDやパスワード、
製品/サービス提供者
(なし)
セッション情報の漏洩が発生し、
なりすましによるメールの閲覧や設定情報の
国/組織名
(なし)
改ざん等が生じる可能性があります。
サイバー攻撃
改ざん
セキュリティ辞書
脆弱性辞書
脆弱性キーワード抽出
脆弱性キーワード
バッファオーバーフロー
脆弱性キーワード
バッファオーバーフロー
脆弱性スコア計算
脆弱性スコア
セキュリティ情報A: a
セキュリティ情報B: b

[図5]


スタート
参照元セキュリティ情報を受信
S101
参照元セキュリティ情報から
セキュリティ辞書に含まれる
キーワードを抽出
S102
参照元セキュリティ情報から抽出した
キーワードと、セキュリティ情報蓄積部に
蓄積された各セキュリティ情報の
脆弱性キーワードを比較し、
脆弱性スコアを計算
S103
製品/サービス辞書について、
製品/サービススコアを計算
S104
製品/サービス提供者辞書について、
製品/サービス提供者スコアを計算
S105
国/組織名辞書について、
国/組織名スコアを計算
S106
サイバー攻撃辞書について、
サイバー攻撃スコアを計算
S107
各スコアを合算
S108
スコアの合算値が高い順に、
セキュリティ情報蓄積部の
セキュリティ情報をソート
S109
ソートされた順番で、
セキュリティ情報を
入出力インターフェースに送信
S110
エンド

[図6]


1061
ディスプレイ
1051
マウス
1052
キーボード
1000
コンピュータ
1010
メモリ
ROM
1011
RAM
1012
1020
CPU
1060
ビデオ
アダプタ
1050
シリアルポート
インターフェース
1080
1030
ハードディスク
ドライブ
インターフェース
1040
ディスク
ドライブ
インターフェース
1070
ネットワーク
インターフェース
1031
ハードディスク
ドライブ
1041
ディスク
ドライブ
OS
アプリケーション
プログラム
プログラム
モジュール
プログラム
データ
1091
1092
1093
1094

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2014/066193

A. CLASSIFICATION OF SUBJECT MATTER
G06F17/30(2006.01)i

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F17/30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2014
Kokai Jitsuyo Shinan Koho 1971-2014 Toroku Jitsuyo Shinan Koho 1994-2014

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2007-58514 A (Mitsubishi Electric Corp.), 08 March 2007 (08.03.2007), paragraphs [0036] to [0053], [0165] to [0191] (Family: none)	1-12
Y	JP 2012-243268 A (NEC Corp.), 10 December 2012 (10.12.2012), paragraphs [0022] to [0026], [0035] to [0036] (Family: none)	1-12
A	JP 2009-15570 A (Nippon Telegraph and Telephone Corp.), 22 January 2009 (22.01.2009), entire text; all drawings (Family: none)	1-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 July, 2014 (11.07.14)	29 July, 2014 (29.07.14)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１４／０６６１９３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F17/30(2006.01)i

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Int.Cl.　G06F17/30

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	１９２２－１９９６年
日本国公開実用新案公報	１９７１－２０１４年
日本国実用新案登録公報	１９９６－２０１４年
日本国登録実用新案公報	１９９４－２０１４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
Y	JP 2007-58514 A (三菱電機株式会社) 2007.03.08, 段落【0036】-【0053】, 【0165】-【0191】 (ファミリーなし)	1-12
Y	JP 2012-243268 A (日本電気株式会社) 2012.12.10, 段落【0022】-【0026】, 【0035】-【0036】 (ファミリーなし)	1-12

☑　Ｃ欄の続きにも文献が列挙されている。

☐　パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの

「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「Ｏ」口頭による開示、使用、展示等に言及する文献

「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
１１．０７．２０１４	２９．０７．２０１４

国際調査機関の名称及びあて先
日本国特許庁（ＩＳＡ／ＪＰ）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　５Ｍ　４６７８
久々宇　篤志
電話番号　０３－３５８１－１１０１　内線　３５９９

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求項の番号
A	JP 2009-15570 A（日本電信電話株式会社） 2009.01.22, 全文全図 (ファミリーなし)	1-12