(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
2020年3月12日(12.03.2020)

WIPO | PCT

(10) 国際公開番号
WO 2020/050355 A1

(51) 国際特許分類:
G06F 21/57 (2013.01)

(21) 国際出願番号： PCT/JP2019/034930

(22) 国際出願日： 2019年9月5日(05.09.2019)

(25) 国際出願の言語： 日本語

(26) 国際公開の言語： 日本語

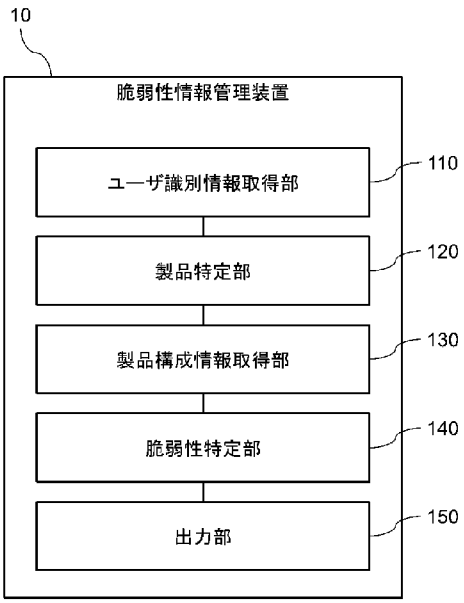
(30) 優先権データ：
特願 2018-166076 2018年9月5日(05.09.2018) JP

(71) 出願人: ＮＥＣソリューションイノベータ株式会社 (**NEC SOLUTION INNOVATORS, LTD.**) [JP/JP]; 〒1368627 東京都江東区新木場一丁目１８番７号 Tokyo (JP).

(72) 発明者: 水野 史博 (**MIZUNO Fumihiro**); 〒1368627 東京都江東区新木場一丁目１８番７号 ＮＥＣソリューションイノベータ株式会社内 Tokyo (JP). 杉山 和義 (**SUGIYAMA Kazuyoshi**); 〒1368627 東京都江東区新木場一丁目１８番７号 ＮＥＣソリューションイノベータ株式会社内 Tokyo (JP). 中貝 順一 (**NAKAGAI Junichi**); 〒1368627 東京都江東区新木場一丁目１８番７号 ＮＥＣソリューションイノベータ株式会社内 Tokyo (JP). 村上 正一 (**MURAKAMI Shouichi**); 〒1368627 東京都江東区新木場一丁目１８番７号 ＮＥＣソリューションイノベータ株式会社内 Tokyo (JP). 小柳 亘 (**KOYANAGI Wataru**); 〒1368627 東京都江東区新木場一丁目１８番７号 ＮＥＣソリュ

(54) **Title:** VULNERABILITY INFORMATION MANAGEMENT DEVICE, VULNERABILITY INFORMATION MANAGEMENT METHOD, AND PROGRAM

(54) 発明の名称： 脆弱性情報管理装置、脆弱性情報管理方法、およびプログラム



10 Vulnerability information management device
110 User identification information acquisition unit
120 Product specification unit
130 Product composition information acquisition unit
140 Vulnerability specification unit
150 Output unit

(57) **Abstract:** A vulnerability information management device (10) is provided with: a user identification information acquisition unit (110) for acquiring user identification information; a product specification unit (120) for specifying one or more products associated with the acquired user identification information; a product composition information acquisition unit (130) for acquiring, for each of one or more specified products, product composition information that indicates the constituent elements of the product; a vulnerability specification unit (140) for referring to a vulnerability information storage means that stores vulnerability information pertaining to each of elements that can be the constituent elements of a product and specifying a constituent element having vulnerability from among the constituent elements corresponding to the acquired product composition information; and an output unit (150) for associating information that indicates the

WO 2020/050355 A1

［続葉有］

ーションイノベータ株式会社内 Tokyo (JP). 谷川 智彦(**TANIKAWA Tomohiko**); 〒1368627 東京都江東区新木場一丁目１８番７号 ＮＥＣソリューションイノベータ株式会社内 Tokyo (JP).

(74) 代理人:速水 進治(**HAYAMI Shinji**); 〒1410031 東京都品川区西五反田７丁目９番２号 ＫＤＸ五反田ビル９階 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, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, 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, ST, 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, 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:

一 国際調査報告（条約第21条(3)）

constituent element having vulnerability with information that indicates a product including the constituent element, and outputting the information to a user terminal.

(57) 要約：脆弱性情報管理装置（１０）は、ユーザ識別情報を取得するユーザ識別情報取得部（１１０）と、取得されたユーザ識別情報に関連付けられた、１以上の製品を特定する製品特定部（１２０）と、特定された１以上の製品それぞれについて、製品の構成要素を示す製品構成情報を取得する製品構成情報取得部（１３０）と、製品の構成要素となり得る要素それぞれの脆弱性情報を要素別に記憶する脆弱性情報記憶手段を参照して、取得された製品構成情報に対応する構成要素の中から、脆弱性を有する構成要素を特定する脆弱性特定部（１４０）と、脆弱性を有する構成要素を示す情報を、当該構成要素を含む製品を示す情報と関連付けてユーザ端末に出力する出力部（１５０）と、を備える。

明　細　書

発明の名称 ：

脆弱性情報管理装置、脆弱性情報管理方法、およびプログラム

技術分野

[0001]　本発明は、製品に潜む脆弱性を管理する技術に関する。

背景技術

[0002]　世の中で流通している製品について、その製品の製造者が意図しない脆弱性が後に発見され、悪用されることがある。ある製品に脆弱性が見つかった場合、その製品の製造者やユーザは、適切な対処を行う必要がある。

[0003]　脆弱性を管理する技術の一例が、下記特許文献１乃至５に開示されている。特に、下記特許文献１には、対象とする装置にインストールされているソフトウエアと、そのソフトウエアのバージョンやサービスパックの適用状況等を含む構成情報を取得し、その構成情報を基に脆弱性を検索し、脆弱性が見つかった場合には適切な対策を実行する技術が開示されている。

先行技術文献

特許文献

[0004] 特許文献1：特開２０１４－１３０５０２号公報

特許文献2：国際公開第２０１３／０３５１８１号

特許文献3：特開２０１０－０６７２１６号公報

特許文献4：特開２０１７－１７４３７８号公報

特許文献5：特開２０１５－１１４８３３号公報

発明の概要

発明が解決しようとする課題

[0005]　１つの製品は、基本的に、様々な要素（ハードウエア部品やソフトウエア部品）を組み合わせて構成されている。１つの製品を構成する各要素（以下、「構成要素」とも表記）のいずれかが脆弱性を有している場合、製品として脆弱性の影響を受けることになる。ユーザが扱う製品のどの部分にどのよ

うな脆弱性が存在しているかを知りたいというニーズがある。

[0006] 本発明は、上記の課題に鑑みてなされたものである。本発明の目的の一つは、ユーザが扱う製品のどの部分にどのような脆弱性があるかを容易に把握する技術を提供することである。

課題を解決するための手段

[0007] 本発明の脆弱性情報管理装置は、

ユーザ識別情報を取得するユーザ識別情報取得手段と、

取得された前記ユーザ識別情報に関連付けられた、１以上の製品を特定する製品特定手段と、

特定された前記１以上の製品それぞれについて、製品の構成要素を示す製品構成情報を取得する製品構成情報取得手段と、

製品の構成要素となり得る要素それぞれの脆弱性情報を要素別に記憶する脆弱性情報記憶手段を参照して、取得された前記製品構成情報に対応する構成要素の中から、脆弱性を有する構成要素を特定する脆弱性特定手段と、

前記脆弱性を有する構成要素を示す情報を、当該構成要素を含む製品を示す情報と関連付けてユーザ端末に出力する出力手段と、

を備える。

[0008] 本発明の脆弱性情報管理方法は、

コンピュータが、

ユーザ識別情報を取得し、

取得された前記ユーザ識別情報に関連付けられた、１以上の製品を特定し、

特定された前記１以上の製品それぞれについて、製品の構成要素を示す製品構成情報を取得し、

製品の構成要素となり得る要素それぞれの脆弱性情報を要素別に記憶する脆弱性情報記憶手段を参照して、取得された前記製品構成情報に対応する構成要素の中から、脆弱性を有する構成要素を特定し、

前記脆弱性を有する構成要素を示す情報を、当該構成要素を含む製品を示

す情報と関連付けてユーザ端末に出力する、

ことを含む。

[0009] 本発明のプログラムは、コンピュータに、上述の脆弱性情報管理方法を実行させる。

発明の効果

[0010] 本発明によれば、ユーザが扱う製品のどの部分にどのような脆弱性があるかを容易に確認または検索することができる。

図面の簡単な説明

[0011] 上述した目的、およびその他の目的、特徴および利点は、以下に述べる好適な実施の形態、およびそれに付随する以下の図面によってさらに明らかになる。

[0012] [図1]本発明に係る脆弱性情報管理装置が行う処理を概念的に示す図である。

[図2]第１実施形態における脆弱性情報管理装置の機能構成を例示する図である。

[図3]本発明に係る脆弱性情報管理装置のハードウエア構成を例示するブロック図である。

[図4]第１実施形態の脆弱性情報管理装置により実行される処理の流れを例示するフローチャートである。

[図5]第１実施形態における製品構成情報記憶部に記憶される情報を例示する図である。

[図6]第１実施形態における製品構成情報記憶部に情報を登録する流れを例示する図である。

[図7]第１実施形態における脆弱性情報記憶部に記憶される脆弱性情報の一例を示す図である。

[図8]第１実施形態における出力部による出力の一例を示す図である。

[図9]第１実施形態における出力部による出力の他の一例を示す図である。

[図10]第１実施形態における出力部による出力の他の一例を示す図である。

[図11]第１実施形態における出力部による出力の他の一例を示す図である。

[図12]第１実施形態における出力部による出力の他の一例を示す図である。

[図13]第２実施形態における脆弱性情報管理装置の機能構成を例示する図である。

[図14]第２実施形態の脆弱性情報管理装置により実行される処理の流れを例示するフローチャートである。

[図15]第２実施形態における脆弱性情報管理装置により提供されるサービスのトップ画面を例示する図である。

[図16]第２実施形態において脆弱性を検索するための画面の一例を示す図である。

[図17]第３実施形態における脆弱性情報管理装置の機能構成を例示する図である。

[図18]第３実施形態においてユーザ毎に保管される対処計画情報の一例を示す図である。

[図19]第４実施形態における脆弱性情報管理装置の機能構成を例示する図である。

[図20]第４実施形態におけるグループ識別情報記憶部に記憶される情報の一例を示す図である。

[図21]第４実施形態における製品構成情報記憶部に記憶される情報を例示する図である。

発明を実施するための形態

[0013] 以下、本発明の実施形態について、図面を用いて説明する。尚、すべての図面において、同様な構成要素には同様の符号を付し、適宜説明を省略する。また、特に説明する場合を除き、各ブロック図において、各ブロックは、ハードウエア単位の構成ではなく、機能単位の構成を表している。

[0014] ［概要］

本発明に係る脆弱性情報管理装置１０は、製品の脆弱性を管理する作業を支援するサービスをユーザに提供する。以下、図１を用いて、本発明に係る脆弱性情報管理装置１０が行う処理の概要について説明する。図１は、本発

明に係る脆弱性情報管理装置１０が行う処理を概念的に示す図である。

[0015] まず、脆弱性情報管理装置１０は、脆弱性情報管理装置１０により提供されるサービスのユーザを一意に識別する情報（ユーザ識別情報）を取得する。脆弱性情報管理装置１０は、例えば図１に示されるように、ユーザ端末３０と通信して、ユーザ端末３０に入力されたユーザ識別情報を取得することができる。また、脆弱性情報管理装置１０は、予め設定された処理実行スケジュールに従って、脆弱性情報管理装置１０のメモリやストレージデバイスといった記憶領域（図示せず）に予め記憶されたユーザ識別情報を読み出してもよい。

[0016] そして、脆弱性情報管理装置１０は、製品構成情報記憶部２２に記憶されている製品構成情報（製品の構成要素を製品別に示す情報）の中から、取得したユーザ識別情報に紐付く製品構成情報を取得する。ここで、製品構成情報記憶部２２に記憶される製品構成情報は、ユーザにより登録される。例えば、ユーザは、管理対象の製品に含まれる構成要素（ハードウエアやソフトウエア）の情報を、ユーザ端末３０を介して、脆弱性情報管理装置１０に入力する。この場合、脆弱性情報管理装置１０は、ユーザにより入力された製品の構成要素に関する情報（製品構成情報）を、そのユーザを識別するユーザ識別情報と関連づけて製品構成情報記憶部２２に記憶する。

[0017] そして、脆弱性情報管理装置１０は、製品構成情報記憶部２２から取得した製品構成情報と、脆弱性情報記憶部２０に記憶されている既知の脆弱性情報とを用いて、脆弱性を有する構成要素を検出する（脆弱性検出処理）。ここで、脆弱性情報記憶部２０に記憶される脆弱性情報は、脆弱性情報収集装置４０からインポートされる。脆弱性情報収集装置４０は、製品の構成要素となり得る要素（ハードウエア部品やソフトウエアプログラム等）の脆弱性に関する情報を、ネットワーク上の情報源５０から収集し、データベース（脆弱性情報記憶部４１０）に蓄積している。情報源５０は、脆弱性に関する情報を有するネットワーク上の任意のノードである。情報源５０は、例えば公的機関やベンダなどにより運営される。情報源５０の具体例としては、Ｊ

ＶＮ（Japan Vulnerability Notes）、ＮＶＤ（National Vulnerability Database）、ＯＳＶＤＢ（Open Source Vulnerability Database）などが挙げられる。また、情報源５０としては、発見された脆弱性に関連する、ＰｏＣ（Proof of Concept）やエクスプロイト・コードの情報を公開するノードが含まれ得る。

[0018] そして、脆弱性情報管理装置１０は、脆弱性検出処理の結果（脆弱性を有する構成要素を示す情報およびその構成要素を含む製品を示す情報）を、ユーザ端末３０に出力する。

[0019] ＜作用・効果＞

上述した脆弱性情報管理装置１０の動作により、脆弱性を有する構成要素を示す情報およびその構成要素を含む製品を示す情報がユーザ端末３０に出力される。ユーザは、脆弱性情報管理装置１０から出力された情報をユーザ端末３０上で確認することにより、どの製品のどの部分にどのような脆弱性があるかを容易に把握することができる。

[0020] ＜機能構成例＞

図２は、第１実施形態における脆弱性情報管理装置１０の機能構成を例示する図である。図２に示されるように、本実施形態の脆弱性情報管理装置１０は、ユーザ識別情報取得部１１０、製品特定部１２０、製品構成情報取得部１３０、脆弱性特定部１４０、および出力部１５０を有する。

[0021] ユーザ識別情報取得部１１０は、ユーザ識別情報を取得する。ユーザ識別情報は、本実施形態の脆弱性情報管理装置１０によって提供されるサービスを利用するユーザ毎に割り当てられる。ユーザ識別情報は、例えば、任意の数字や文字を組み合わせたＩＤ（Identifier）などである。

[0022] 製品特定部１２０は、ユーザ識別情報取得部１１０により取得されたユーザ識別情報に関連付けられた、１以上の製品を特定する。ユーザ識別情報と製品に関する情報とは、例えば、予めユーザからの入力により関連付けられている。

[0023] 製品構成情報取得部１３０は、製品特定部１２０により特定された１以上

の製品それぞれについて、製品構成情報を取得する。製品構成情報は、製品に含まれる構成要素（ハードウエアやソフトウエア）を示す情報である。

[0024] 脆弱性特定部１４０は、脆弱性情報記憶部２０を参照して、製品構成情報取得部１３０により取得された製品構成情報に対応する構成要素の中から、脆弱性を有する構成要素を特定する。上述したように、脆弱性情報記憶部２０は、製品の構成要素となり得る要素（ハードウエアやソフトウエア）それぞれの脆弱性情報をネットワーク上の情報源５０から収集し、要素別に記憶している。

[0025] 出力部１５０は、脆弱性特定部１４０により特定された脆弱性を有する構成要素を示す情報を、当該構成要素を含む製品を示す情報と関連付けてユーザ端末３０に出力する。

[0026] 〔ハードウエア構成例〕

脆弱性情報管理装置１０の各機能構成部は、各機能構成部を実現するハードウエア（例：ハードワイヤードされた電子回路など）で実現されてもよいし、ハードウエアとソフトウエアとの組み合わせ（例：電子回路とそれを制御するプログラムの組み合わせなど）で実現されてもよい。以下、脆弱性情報管理装置１０の各機能構成部がハードウエアとソフトウエアとの組み合わせで実現される場合について、さらに説明する。

[0027] 図３は、脆弱性情報管理装置１０のハードウエア構成を例示するブロック図である。脆弱性情報管理装置１０は、バス１０１０、プロセッサ１０２０、メモリ１０３０、ストレージデバイス１０４０、入出力インタフェース１０５０、及びネットワークインタフェース１０６０を有する。

[0028] バス１０１０は、プロセッサ１０２０、メモリ１０３０、ストレージデバイス１０４０、入出力インタフェース１０５０、及びネットワークインタフェース１０６０が、相互にデータを送受信するためのデータ伝送路である。ただし、プロセッサ１０２０などを互いに接続する方法は、バス接続に限定されない。

[0029] プロセッサ１０２０は、ＣＰＵ（Central Processing Unit）やＧＰＵ（G

raphics Processing Unit）などで実現されるプロセッサである。

[0030] メモリ１０３０は、ＲＡＭ（Random Access Memory）などで実現される主記憶装置である。

[0031] ストレージデバイス１０４０は、ＨＤＤ（Hard Disk Drive）、ＳＳＤ（Solid State Drive）、メモリカード、又はＲＯＭ（Read Only Memory）などで実現される補助記憶装置である。ストレージデバイス１０４０は、脆弱性情報管理装置１０の各機能（ユーザ識別情報取得部１１０、製品特定部１２０、製品構成情報取得部１３０、脆弱性特定部１４０、出力部１５０など）を実現するプログラムモジュールを記憶している。プロセッサ１０２０がこれら各プログラムモジュールをメモリ１０３０上に読み込んで実行することで、各プログラムモジュールに対応する各機能が実現される。

[0032] 入出力インタフェース１０５０は、脆弱性情報管理装置１０と各種入出力デバイスとを接続するためのインタフェースである。入出力インタフェース１０５０には、キーボードやマウスといった入力装置、スピーカーやディスプレイといった出力装置などが接続され得る。

[0033] ネットワークインタフェース１０６０は、脆弱性情報管理装置１０をネットワークに接続するためのインタフェースである。このネットワークは、例えばＬＡＮ（Local Area Network）やＷＡＮ（Wide Area Network）である。ネットワークインタフェース１０６０がネットワークに接続する方法は、無線接続であってもよいし、有線接続であってもよい。脆弱性情報管理装置１０は、ネットワークインタフェース１０６０を介して、ユーザ端末３０や脆弱性情報収集装置４０といった、ネットワーク上の外部装置と通信することができる。

[0034] なお、図３はあくまで例示であり、脆弱性情報管理装置１０のハードウエア構成は図３に例示される構成に限定されない。例えば、脆弱性情報管理装置１０は、脆弱性情報収集装置４０の機能（情報源５０から脆弱性情報を収集する機能）を更に備えていてもよい。

[0035] ＜処理の流れ＞

図４は、第１実施形態の脆弱性情報管理装置１０により実行される処理の流れを例示するフローチャートである。以下、図４のフローチャートに沿って、第１実施形態の脆弱性情報管理装置１０により実行される処理の流れを説明する。

[0036] まず、ユーザ識別情報取得部１１０は、ユーザ識別情報を取得する（Ｓ１０２）。例えば、脆弱性情報管理装置１０は、ユーザ端末３０と通信して、ユーザ端末３０に入力されたユーザ識別情報を取得することができる。また、脆弱性情報管理装置１０は、予め設定された処理実行スケジュールに従って、脆弱性情報管理装置１０のメモリ１０３０やストレージデバイス１０４０といった記憶領域に予め記憶されたユーザ識別情報を読み出してもよい。

[0037] そして、製品特定部１２０は、Ｓ１０２の処理で取得されたユーザ識別情報に基づいて、１以上の製品を特定する（Ｓ１０４）。製品特定部１２０は、例えば、製品構成情報記憶部２２に記憶されている情報（例：図５）を参照して、１以上の製品を特定することができる。

[0038] 図５は、製品構成情報記憶部２２に記憶される情報を例示する図である。製品構成情報記憶部２２は、製品構成情報を含む製品に関する情報をユーザ識別情報と関連付けて記憶している。図５の例において、各レコードは、「ユーザＩＤ」、「製品ＩＤ」、および「製品構成情報」という３つのカラムを含んで構成されている。「ユーザＩＤ」は、脆弱性情報管理装置１０が提供するサービスのユーザを一意に識別するための情報（ユーザ識別情報）である。「製品ＩＤ」は製品を識別するための情報である。「製品ＩＤ」は、例えば、製品構成情報が登録される際に、脆弱性情報管理装置１０によって自動的に割り当てられる。「製品構成情報」は、ユーザからの入力を基に生成される、製品の構成要素に関する情報である。各製品の製品構成情報は、ユーザＩＤと関連付けて記憶されている。

[0039] 図５の例において、「製品構成情報」のカラムは、「要素ＩＤ」、「要素名」、および「階層構造情報」を含んでいる。「要素ＩＤ」は、製品に含まれる構成要素を識別するための情報である。「要素ＩＤ」は、例えば、製品

構成情報が登録される際に、脆弱性情報管理装置１０によって自動的に割り当てられる。「要素名」は、構成要素（ハードウエア部品やソフトウエアといった最終製品を構成する部品）の名称を示す情報である。「バージョン情報」は、当該構成要素のバージョンを示す情報である。「階層構造情報」は、製品に含まれる構成要素の階層構造を示す情報である、図５に例示される階層構造情報において、階層構造は、各製品をトップノードとして、「／（スラッシュ）」を使って表現されている。例えば、要素ＩＤ「Ｅ００１」の階層構造情報は「／Ｅ００１」である。これは、構成要素「部品Ａ１」がトップノード直下の第１階層に位置することを示している。また例えば、要素ＩＤ「Ｅ００５」の階層構造情報は「／Ｅ００１／Ｅ００３／Ｅ００５」である。これは、構成要素「部品Ａ１」がトップノード直下の第１階層に位置し、構成要素「電子部品１」が構成要素「部品Ａ１」の下位ノードとして第２階層に位置し、構成要素「ＸＸＸ＃１」が構成要素「電子部品１」の下位ノードとして第３階層に位置することを示している。また例えば、要素ＩＤ「Ｅ００８」の階層構造情報は「／／／Ｅ００８」である。これは、構成要素「ＸＸＸ＃４」が、第１および第２階層を省略して、第３階層に位置することを示している。

[0040] なお、図５に例示されるような情報は、例えば、図６に示すように登録される。図６は、製品構成情報記憶部２２に情報を登録する流れを例示する図である。まず、ユーザは、ユーザ端末３０を使って、脆弱性情報管理装置１０が提供するサービスにログインする（図中（１））。このログイン時に、ユーザ端末３０に入力されたユーザを一意に識別するためのユーザＩＤといった情報が、上述のユーザ識別情報として取得される。そして、ユーザは、ユーザ端末３０を使って、自身が管理したい製品と、その製品に含まれる構成要素に関する情報を入力する（図中（２））。ここで、ユーザは、製品に含まれる構成要素の階層構造を示す情報を更に入力してもよい。脆弱性情報管理装置１０は、ユーザにより入力された情報を製品構成情報として、先に取得したユーザ識別情報に紐付けて製品構成情報記憶部２２に登録する（図

中（３））。

[0041] 図５に例示される情報を用いる場合、製品特定部１２０は、Ｓ１０２の処理で取得されたユーザ識別情報を用いて、当該取得されたユーザ識別情報と同一のユーザ識別情報を有するレコードを特定することができる。レコードが特定できた時点で、製品特定部１２０は、１以上の製品を特定できたことになる。

[0042] 図４に戻り、製品構成情報取得部１３０は、Ｓ１０４の処理で特定された１以上の製品それぞれについて、製品構成情報を取得する（Ｓ１０６）。上述の具体例で言えば、製品構成情報取得部１３０は、製品特定部１２０により特定されたレコードの中から、「製品構成情報」のカラムに格納されている情報（要素ＩＤ、要素名、階層構造情報など）を取得することができる。

[0043] そして、脆弱性特定部１４０は、脆弱性検出処理を実行する（Ｓ１０８）。具体的には、脆弱性特定部１４０は、Ｓ１０６の処理で取得された製品別の構成要素情報と、脆弱性情報記憶部２０に記憶された脆弱性情報（例：図７）とを用いて、脆弱性を有する製品およびその脆弱性を実際に有する構成要素を特定することができる。

[0044] 図７は、脆弱性情報記憶部２０に記憶される脆弱性情報の一例を示す図である。脆弱性情報記憶部２０は、製品の構成要素となり得る要素の脆弱性に関する情報を要素毎に記憶している。図７の例において、各レコードは、「脆弱性情報ＩＤ」、「脆弱性情報」、および「影響を受ける要素」という３つのカラムを含んで構成されている。「脆弱性情報ＩＤ」は、脆弱性に関する情報を一意に識別するための情報である。「脆弱性情報」は、例えば脆弱性の危険度、確認方法や対処方法などの、脆弱性の詳細を示す情報である。「影響を受ける要素」は、同じレコードの中で定義されている脆弱性の影響を受ける要素を示す情報である。図７の例において、「影響を受ける要素」のカラムは、「要素名」および「バージョン情報」を含んでいる。脆弱性特定部１４０は、製品構成情報記憶部２２の「要素名」および「バージョン情報」を使って脆弱性情報記憶部２０を検索することにより、製品構成情報記

憶部２２に記憶されている各構成要素に存在する脆弱性に関する情報を特定することができる。

[0045] 脆弱性特定部１４０は、Ｓ１０６の処理で取得した製品構成情報の「要素名」および「バージョン情報」を検索キーとして用いて、脆弱性情報記憶部２０に記憶されている脆弱性情報を検索する。検索キーに対応する脆弱性情報が見つかった場合、脆弱性特定部１４０は、その検索キーに対応する構成要素を「脆弱性を有する構成要素」と特定することができる。また、脆弱性特定部１４０は、「脆弱性を有する構成要素」として特定された構成要素を有する製品を「脆弱性を有する製品」として特定することができる。

[0046] そして、脆弱性特定部１４０は、Ｓ１０４の処理で特定された１以上の製品について、Ｓ１０８の脆弱性検出処理で脆弱性を有する構成要素が検出された否かを判定する（Ｓ１１０）。脆弱性検出処理で脆弱性を有する構成要素が検出された場合（Ｓ１１０：ＹＥＳ）、脆弱性を有する構成要素を示す情報およびその構成要素を含む製品を示す情報を出力部１５０に通知する。出力部１５０は、脆弱性特定部１４０からの通知に基づいて、脆弱性を有する構成要素を示す情報を、その構成要素を含む製品を示す情報と関連付けてユーザ端末３０に出力する（Ｓ１１２）。

[0047] Ｓ１０６の処理で取得した製品構成情報が、製品に含まれる構成要素の階層構造を示す情報を有している場合、出力部１５０は、その製品構成情報（階層構造を示す情報）に基づいて、図８に例示されるような画面をユーザ端末３０に出力することができる。図８は、出力部１５０による出力の一例を示す図である。図８には、製品に含まれる構成要素の階層構造をツリー形式で示す情報ｉ１を含む画面が例示されている。また、出力部１５０は、脆弱性を有する構成要素を、その他の構成要素と区別可能に表示する画面を出力することができる。例えば、出力部１５０は、図８の符号ｈで示すように、脆弱性を有する構成要素を強調表示してもよい。ユーザは、図８に例示される画面を確認することによって、複数の構成要素からなる製品について、脆弱性を有する構成要素を一目で把握することができる。また、図８に例示さ

れるような画面において、１つの製品を構成する多数の構成要素が、ツリーの上位に行くほど汎化される。その結果、ツリーの上位を見ることによって、脆弱性情報を保有する対象物を容易に把握することが可能となる。

[0048] なお、図８に例示される画面はあくまで一例であり、出力部１５０による出力は図８の例に限定されない。例えば、出力部１５０は、図９または図１０に示されるような画面を出力してもよい。図９および図１０は、出力部１５０による出力の他の一例を示す図である。図９の例では、出力部１５０は、製品に含まれる構成要素の階層構造を示す情報として、リスト形式の情報ｉ２を表示している。また、図１０の例では、出力部１５０は、製品に含まれる構成要素の階層構造を示す情報として、製品に含まれる構成要素の階層構造を別のツリー形式で示す情報ｉ３を表示している。図９および図１０に例示されるような画面によっても、ユーザは、複数の構成要素からなる製品について、脆弱性を有する構成要素を一目で把握することができる。

[0049] また、ある構成要素の下位の階層に位置する別の構成要素に脆弱性が存在する場合、上位の階層の構成要素もその脆弱性の影響を受けることになる。そこで、脆弱性特定部１４０は、階層構造において、脆弱性を有する構成要素の上位階層に位置する他の構成要素（以下、「上位構成要素」と表記）を特定し、出力部１５０は、特定された上位構成要素を示す情報を、ユーザ端末３０に更に出力してもよい（例：図１１）。図１１は、出力部１５０による出力の他の一例を示す図である。図１１の例では、脆弱性特定部１４０は、構成要素「電子部品２」および構成要素「部品Ａ２」を、脆弱性を有する構成要素「ＸＸＸ＃２」の上位構成要素として特定している。具体的には、脆弱性特定部１４０は、図５に例示されるような、構成要素「ＸＸＸ＃２」の階層構造情報「Ｅ００２／Ｅ００４／Ｅ００６」に基づいて、要素ＩＤ「Ｅ００２」および要素ＩＤ「Ｅ００４」の構成要素、すなわち、構成要素「部品Ａ２」および構成要素「電子部品２」を、構成要素「ＸＸＸ＃２」の上位構成要素として特定することができる。そして、出力部１５０は、脆弱性特定部１４０により特定された上位構成要素を示す情報ｉ４を表示すること

ができる。このようにすることで、ユーザは、脆弱性の影響を受ける範囲（構成要素群）を一目で把握することができる。

[0050] また、出力部１５０は、脆弱性を有する構成要素を示す情報を出力する際、その構成要素が有する脆弱性に関する情報を、ユーザ端末３０に更に出力してもよい（例：図１２）。図１２は、出力部１５０による出力の他の一例を示す図である。図１２の例では、出力部１５０は、構成要素の脆弱性に関する情報ｉ５を出力している。

[0051] 出力部１５０は、構成要素の脆弱性に関する情報ｉ５を出力する際、例えば、製品に含まれる構成要素の階層構造を示す情報ｉ１において、構成要素のいずれかを選択する入力を受け付ける。具体的な例として、出力部１５０は、脆弱性を有する構成要素に関する領域にポインタＰを重ねる操作や、脆弱性を有する構成要素に関する領域にポインタＰを重ねた上でマウスやキーボードの所定のボタンを押下する操作を、ユーザの入力操作として受け付ける。そして、出力部１５０は、受け付けた入力により選択された構成要素の脆弱性に関する情報ｉ５を、ユーザ端末３０に出力する。このようにすることで、ユーザは、製品に含まれる構成要素がどのような脆弱性を有しているかを容易に確認することができる。

[0052] ［第２実施形態］

本実施形態は、以下の点において、上述の第１実施形態と異なる。

[0053] ＜機能構成例＞

図１３は、第２実施形態における脆弱性情報管理装置１０の機能構成を例示する図である。図１３に示されるように、本実施形態の脆弱性情報管理装置１０は、ユーザ識別情報取得部１１０、製品特定部１２０、製品構成情報取得部１３０、脆弱性特定部１４０、出力部１５０、および、入力受付部１６０を少なくとも有する。

[0054] 本実施形態において、入力受付部１６０は、脆弱性を指定する入力を受け付ける。例えば、入力受付部１６０は、ユーザ端末３０を介して、複数の脆弱性の中から特定の脆弱性を指定する入力を受け付ける。また、本実施形態

の脆弱性特定部１４０は、入力受付部１６０が受け付けた入力に基づいて、その入力よって指定される脆弱性を有する構成要素を、製品構成情報取得部１３０が取得した製品構成情報に対応する構成要素の中から特定する。また、出力部１５０は、入力受付部１６０が受け付けた入力により指定される脆弱性を有する構成要素として特定された構成要素を示す情報を、ユーザ端末３０に更に出力する。

[0055] ＜処理の流れ＞

図１４は、第２実施形態の脆弱性情報管理装置１０により実行される処理の流れを例示するフローチャートである。以下、図１４のフローチャートに沿って、第２実施形態の脆弱性情報管理装置１０により実行される処理の流れを説明する。

[0056] 入力受付部１６０は、脆弱性を指定する入力を受け付ける（Ｓ２０２）。入力受付部１６０は、例えば、図１５に例示されるような画面を介して、脆弱性を指定する入力を受け付けることができる。

[0057] 図１５は、脆弱性情報管理装置１０により提供されるサービスのトップ画面を例示する図である。例えば、脆弱性情報管理装置１０により提供されるサービスを利用するためにユーザがログイン動作を行った場合、図１５に例示されるような画面がユーザ端末３０に出力される。具体的には、脆弱性特定部１４０は、あるユーザのログイン動作に応じて、第１実施形態で説明したように、製品構成情報記憶部２２の中からそのユーザに関する製品構成情報を取得する。そして、脆弱性特定部１４０は、取得した製品構成情報と脆弱性情報記憶部２０に記憶されている脆弱性情報とを突き合わせることによって、そのユーザの製品に関係のある脆弱性を特定する。ここで、脆弱性特定部１４０は、特定した脆弱性と、その脆弱性を有する構成要素との対応関係を示す情報をメモリ１０３０などに記憶することができる。そして、出力部１５０は、ユーザの製品に関係のある脆弱性を示す情報ｉ６を含む画面を、ユーザ端末３０に出力することができる。ユーザは、ユーザ端末３０の入力装置を使って、図１５に例示されるような画面上で、脆弱性を指定するこ

とができる。また、ユーザは、脆弱性を検索する画面（図１６）を介して、脆弱性を指定する入力操作を行ってもよい。図１６は、脆弱性を検索するための画面の一例を示す図である。

[0058] 図１４に戻り、Ｓ２０２の処理で入力受付部１６０が脆弱性を指定する入力を受け付けると、脆弱性特定部１４０は、当該入力によって指定される脆弱性を有する構成要素を特定する（Ｓ２０４）。例えば、脆弱性特定部１４０は、ユーザのログイン動作時にメモリ１０３０などに記憶しておいた、そのユーザの製品に関係のある脆弱性と、その脆弱性を有する構成要素との対応関係を示す情報を用いて、Ｓ２０２の入力で指定された脆弱性を有する構成要素を特定できる。

[0059] そして、出力部１５０は、Ｓ２０４の処理で特定された構成要素を示す情報を、ユーザ端末３０に出力する（Ｓ２０６）。例えば、出力部１５０は、図８乃至図１０に例示されるように、指定された脆弱性を有する構成要素を強調表示するような出力を行うことができる。

[0060] 以上、本実施形態では、脆弱性を指定するユーザ入力に応じて、当該脆弱性を有する構成要素を示す情報がユーザ端末３０に出力される。本実施形態の構成により、ユーザは、指定した脆弱性がそのユーザに関係のある製品のどの構成要素に存在しているかを容易に確認することができる。

[0061] ［第３実施形態］

本実施形態は、以下の点において、上述の第１実施形態と異なる。

[0062] ＜機能構成例＞

図１７は、第３実施形態における脆弱性情報管理装置１０の機能構成を例示する図である。図１７に示されるように、本実施形態の脆弱性情報管理装置１０は、対処計画情報取得部１７０および通知部１８０を更に有する。

[0063] 対処計画情報取得部１７０は、製品（製品に含まれる構成要素）に関して見つかった脆弱性への対処計画を示す情報（対処計画情報）を取得する。ここで「対処計画」は、脆弱性に対して取り得る対処の完了予定日や進捗状態（「未確認」、「調査中」、「対処済み」、「該当なし」等）を含む。ユー

ザは、例えば、図８乃至図１０に例示されるような画面において、そのユーザに関係する製品の脆弱性の情報を確認した後、その脆弱性に対する対処スケジュールや対処の進捗状態を示す対処計画情報を、ユーザ端末３０を介して入力することができる。対処計画情報取得部１７０は、ユーザの入力に応じて取得された対処計画情報を、そのユーザを識別する情報と対応付けて、メモリ１０３０やストレージデバイス１０４０などの記憶領域に記憶する（例：図１８）。図１８は、ユーザ毎に保管される対処計画情報の一例を示す図である。図１８では、各ユーザを一意に識別するユーザ識別情報と対応付けて、対処計画情報を記憶するテーブルが例示されている。

[0064] 通知部１８０は、対処計画情報取得部１７０により取得された対処計画情報に基づいて、脆弱性への対処についてのリマインド情報をユーザに通知する。

[0065] 一例として、通知部１８０は、対処計画における進捗状態別の件数を示す情報を、ユーザ端末３０に通知することができる。具体的には、通知部１８０は、図１８に示すような情報を参照して、ユーザ毎の対処計画情報を取得する。そして、通知部１８０は、対処計画情報の進捗状態の値に基づいて、進捗状態別のレコードを特定し、その件数または各レコードに登録された内容を示す情報等をユーザ端末３０に送信する。他の一例として、通知部１８０は、対処計画情報の完了予定日を過ぎても対処が完了していない脆弱性の件数を示す情報を、ユーザ端末３０に通知することができる。具体的には、通知部１８０は、図１８に示すような情報を参照して、ユーザ毎の対処計画情報を取得する。そして、通知部１８０は、対処計画情報の完了予定日の値および進捗状態の値に基づいて、完了予定日を過ぎても対処が完了していない脆弱性のレコードを特定し、その件数または各レコードに登録された内容を示す情報等をユーザ端末３０に送信する。

[0066] なお、図示しないが、ユーザ識別情報（ユーザＩＤ）とユーザ端末３０のアドレス情報との対応関係を示す情報が、例えばストレージデバイス１０４０に予め登録されている。通知部１８０は、ユーザＩＤを基に取得されるユ

ーザ端末３０のアドレス情報を用いて、先に例示したような通知を行うことができる。

[0067] 以上、本実施形態では、ユーザが入力した脆弱性対処情報に基づいて、ユーザ端末３０にリマインド情報が出力される。そして、このリマインド情報によって、ユーザに脆弱性への対処を促すことができる。

[0068] ［第４実施形態］

本実施形態は、以下の点において、上述の第１実施形態と異なる。

[0069] ＜機能構成例＞

図１９は、第４実施形態における脆弱性情報管理装置１０の機能構成を例示する図である。本実施形態の製品特定部１２０は、ユーザ識別情報取得部１１０により取得されたユーザ識別情報に紐付けられたグループ識別情報を取得する。ここで、グループ識別情報は、製品が属するグループ（例えば、プロジェクト）を示す情報である。グループ識別情報は、グループ識別情報記憶部２４に記憶されている（例：図２０）。図２０は、グループ識別情報記憶部２４に記憶される情報の一例を示す図である。図２０に例示されるように、グループ識別情報記憶部２４は、各ユーザのユーザ識別情報（ユーザＩＤ）と紐付けて、グループ識別情報（グループＩＤ）を記憶している。更に、本実施形態の製品特定部１２０は、取得されたグループ識別情報を用いて、１以上の製品を特定する。例えば、本実施形態において、製品構成情報記憶部２２は、図２１に例示されるような情報を記憶している。図２１は、第４実施形態の製品構成情報記憶部２２に記憶される情報を例示する図である。本実施形態の製品構成情報記憶部２２は、ユーザＩＤの代わりに、グループＩＤに関連づけて、製品の情報を記憶している。製品特定部１２０は、ユーザ識別情報を基に取得したグループ識別情報を使い、第１実施形態と同様に、１以上の製品を特定することができる。１以上の製品が特定する処理以外については、上述の各実施形態と同様である。

[0070] 以上、本実施形態では、ユーザ識別情報と製品構成情報（１以上の製品の情報）とが、各製品が属するグループ（例えば、プロジェクト）を示すグル

ープ識別情報を介して紐付けられている。本実施形態の構成により、製品構成情報をユーザ毎に記憶する必要がなくなるため、システムで保持する情報の更新および管理が容易になる。また、システム全体のハードウエア資源を節約する効果も見込める。

[0071] 以上、図面を参照して本発明の実施形態について述べたが、これらは本発明の例示であり、上記以外の様々な構成を採用することもできる。

[0072] また、上述の説明で用いた複数のフローチャートでは、複数の工程（処理）が順番に記載されているが、各実施形態で実行される工程の実行順序は、その記載の順番に制限されない。各実施形態では、図示される工程の順番を内容的に支障のない範囲で変更することができる。また、上述の各実施形態は、内容が相反しない範囲で組み合わせることができる。

[0073] 上記の実施形態の一部または全部は、以下の付記のようにも記載されうるが、以下に限られない。

１．

ユーザ識別情報を取得するユーザ識別情報取得手段と、

取得された前記ユーザ識別情報に関連付けられた、１以上の製品を特定する製品特定手段と、

特定された前記１以上の製品それぞれについて、製品の構成要素を示す製品構成情報を取得する製品構成情報取得手段と、

製品の構成要素となり得る要素それぞれの脆弱性情報を要素別に記憶する脆弱性情報記憶手段を参照して、取得された前記製品構成情報に対応する構成要素の中から、脆弱性を有する構成要素を特定する脆弱性特定手段と、

前記脆弱性を有する構成要素を示す情報を、当該構成要素を含む製品を示す情報と関連付けてユーザ端末に出力する出力手段と、

を備える脆弱性情報管理装置。

２．

前記出力手段は、前記脆弱性を有する構成要素として特定された構成要素に関する脆弱性情報を、前記ユーザ端末に更に出力する、

１．に記載の脆弱性情報管理装置。

３．

前記製品構成情報は、製品に含まれる構成要素の階層構造を示す情報を更に有しており、

前記出力手段は、前記取得された製品構成情報に基づいて、製品に含まれる構成要素の階層構造を示す情報を、前記ユーザ端末に更に出力する、

１．または２．に記載の脆弱性情報管理装置。

４．

前記脆弱性特定手段は、前記階層構造において、前記脆弱性を有する構成要素の上位に位置する上位構成要素を更に特定し、

前記出力手段は、前記上位構成要素を示す情報を、前記ユーザ端末に更に出力する、

３．に記載の脆弱性情報管理装置。

５．

前記出力手段は、

前記階層構造を示す情報において構成要素のいずれかを選択する入力を受け付け、

前記入力により選択された構成要素に関する脆弱性情報を、前記ユーザ端末に更に出力する、

３．または４．に記載の脆弱性情報管理装置。

６．

脆弱性を指定する入力を受け付ける入力受付手段を更に備え、

前記脆弱性特定手段は、前記脆弱性情報記憶手段を参照して、前記取得された製品構成情報に対応する構成要素の中から、前記入力により指定された脆弱性を有する構成要素を特定し、

前記出力手段は、前記入力により指定された脆弱性を有する構成要素を示す情報を、前記ユーザ端末に出力する、

１．から５．のいずれか１つに記載の脆弱性情報管理装置。

７．

製品に関して見つかった脆弱性への対処計画を示す対処計画情報を取得する対処計画情報取得手段と、

前記対処計画情報が示す対処計画に基づいて、脆弱性への対処についてのリマインド情報をユーザに通知する通知手段と、を更に備える、

１．から６．のいずれか１つに記載の脆弱性情報管理装置。

８．

前記製品特定手段は、

製品が属するグループを示すグループ識別情報を各ユーザのユーザ識別情報と紐付けて記憶するグループ識別情報記憶手段を参照して、前記取得されたユーザ識別情報に紐付けられたグループ識別情報を取得し、

製品の情報をグループ識別情報別に対応付けて記憶する製品情報記憶手段を参照して、取得された前記グループ識別情報に紐付けられた１以上の製品を特定する、

１．から７．のいずれか１つに記載の脆弱性情報管理装置。

９．

コンピュータが、

ユーザ識別情報を取得し、

取得された前記ユーザ識別情報に関連付けられた、１以上の製品を特定し、

特定された前記１以上の製品それぞれについて、製品の構成要素を示す製品構成情報を取得し、

製品の構成要素となり得る要素それぞれの脆弱性情報を要素別に記憶する脆弱性情報記憶手段を参照して、取得された前記製品構成情報に対応する構成要素の中から、脆弱性を有する構成要素を特定し、

前記脆弱性を有する構成要素を示す情報を、当該構成要素を含む製品を示す情報と関連付けてユーザ端末に出力する、

ことを含む脆弱性情報管理方法。

１０．

前記コンピュータが、前記脆弱性を有する構成要素として特定された構成要素に関する脆弱性情報を、前記ユーザ端末に更に出力する、

ことを含む９．に記載の脆弱性情報管理方法。

１１．

前記製品構成情報は、製品に含まれる構成要素の階層構造を示す情報を更に有しており、

前記コンピュータが、前記取得された製品構成情報に基づいて、製品に含まれる構成要素の階層構造を示す情報を、前記ユーザ端末に更に出力する、

ことを含む９．または１０．に記載の脆弱性情報管理方法。

１２．

前記コンピュータが、

前記階層構造において、前記脆弱性を有する構成要素の上位に位置する上位構成要素を更に特定し、

前記上位構成要素を示す情報を、前記ユーザ端末に更に出力する、

ことを含む１１．に記載の脆弱性情報管理方法。

１３．

前記コンピュータが、

前記階層構造を示す情報において構成要素のいずれかを選択する入力を受け付け、

前記入力により選択された構成要素に関する脆弱性情報を、前記ユーザ端末に更に出力する、

ことを含む１１．または１２．に記載の脆弱性情報管理方法。

１４．

前記コンピュータが、

脆弱性を指定する入力を受け付け、

前記脆弱性情報記憶手段を参照して、前記取得された製品構成情報に対応する構成要素の中から、前記入力により指定された脆弱性を有する構成要

素を特定し、

前記入力により指定された脆弱性を有する構成要素を示す情報を、前記ユーザ端末に出力する、

ことを含む９．から１３．のいずれか１つに記載の脆弱性情報管理方法。

１５．

前記コンピュータが、

製品に関して見つかった脆弱性への対処計画を示す対処計画情報を取得し、

前記対処計画情報が示す対処計画に基づいて、脆弱性への対処についてのリマインド情報をユーザに通知する、

ことを更に含む９．から１４．のいずれか１つに記載の脆弱性情報管理方法。

１６．

前記コンピュータが、

製品が属するグループを示すグループ識別情報を各ユーザのユーザ識別情報と紐付けて記憶するグループ識別情報記憶手段を参照して、前記取得されたユーザ識別情報に紐付けられたグループ識別情報を取得し、

製品の情報をグループ識別情報別に対応付けて記憶する製品情報記憶手段を参照して、取得された前記グループ識別情報に紐付けられた１以上の製品を特定する、

ことを含む９．から１５．のいずれか１つに記載の脆弱性情報管理方法。

１７．

コンピュータに、９．から１６．のいずれか１つに記載の脆弱性情報管理方法を実行させるプログラム。

[0074] この出願は、２０１８年９月５日に出願された日本出願特願２０１８－１６６０７６号を基礎とする優先権を主張し、その開示の全てをここに取り込む。

請求の範囲

[請求項1] ユーザ識別情報を取得するユーザ識別情報取得手段と、

取得された前記ユーザ識別情報に関連付けられた、１以上の製品を特定する製品特定手段と、

特定された前記１以上の製品それぞれについて、製品の構成要素を示す製品構成情報を取得する製品構成情報取得手段と、

製品の構成要素となり得る要素それぞれの脆弱性情報を要素別に記憶する脆弱性情報記憶手段を参照して、取得された前記製品構成情報に対応する構成要素の中から、脆弱性を有する構成要素を特定する脆弱性特定手段と、

前記脆弱性を有する構成要素を示す情報を、当該構成要素を含む製品を示す情報と関連付けてユーザ端末に出力する出力手段と、

を備える脆弱性情報管理装置。

[請求項2] 前記出力手段は、前記脆弱性を有する構成要素として特定された構成要素に関する脆弱性情報を、前記ユーザ端末に更に出力する、

請求項１に記載の脆弱性情報管理装置。

[請求項3] 前記製品構成情報は、製品に含まれる構成要素の階層構造を示す情報を更に有しており、

前記出力手段は、前記取得された製品構成情報に基づいて、製品に含まれる構成要素の階層構造を示す情報を、前記ユーザ端末に更に出力する、

請求項１または２に記載の脆弱性情報管理装置。

[請求項4] 前記脆弱性特定手段は、前記階層構造において、前記脆弱性を有する構成要素の上位に位置する上位構成要素を更に特定し、

前記出力手段は、前記上位構成要素を示す情報を、前記ユーザ端末に更に出力する、

請求項３に記載の脆弱性情報管理装置。

[請求項5] 前記出力手段は、

前記階層構造を示す情報において構成要素のいずれかを選択する入力を受け付け、

前記入力により選択された構成要素に関する脆弱性情報を、前記ユーザ端末に更に出力する、

請求項３または４に記載の脆弱性情報管理装置。

[請求項6] 脆弱性を指定する入力を受け付ける入力受付手段を更に備え、

前記脆弱性特定手段は、前記脆弱性情報記憶手段を参照して、前記取得された製品構成情報に対応する構成要素の中から、前記入力により指定された脆弱性を有する構成要素を特定し、

前記出力手段は、前記入力により指定された脆弱性を有する構成要素を示す情報を、前記ユーザ端末に出力する、

請求項１から５のいずれか１項に記載の脆弱性情報管理装置。

[請求項7] 製品に関して見つかった脆弱性への対処計画を示す対処計画情報を取得する対処計画情報取得手段と、

前記対処計画情報が示す対処計画に基づいて、脆弱性への対処についてのリマインド情報をユーザに通知する通知手段と、を更に備える、

請求項１から６のいずれか１項に記載の脆弱性情報管理装置。

[請求項8] 前記製品特定手段は、

製品が属するグループを示すグループ識別情報を各ユーザのユーザ識別情報と紐付けて記憶するグループ識別情報記憶手段を参照して、前記取得されたユーザ識別情報に紐付けられたグループ識別情報を取得し、

製品の情報をグループ識別情報別に対応付けて記憶する製品情報記憶手段を参照して、取得された前記グループ識別情報に紐付けられた１以上の製品を特定する、

請求項１から７のいずれか１項に記載の脆弱性情報管理装置。

[請求項9] コンピュータが、

ユーザ識別情報を取得し、

取得された前記ユーザ識別情報に関連付けられた、１以上の製品を特定し、

特定された前記１以上の製品それぞれについて、製品の構成要素を示す製品構成情報を取得し、

製品の構成要素となり得る要素それぞれの脆弱性情報を要素別に記憶する脆弱性情報記憶手段を参照して、取得された前記製品構成情報に対応する構成要素の中から、脆弱性を有する構成要素を特定し、

前記脆弱性を有する構成要素を示す情報を、当該構成要素を含む製品を示す情報と関連付けてユーザ端末に出力する、

ことを含む脆弱性情報管理方法。

[請求項10] 前記コンピュータが、前記脆弱性を有する構成要素として特定された構成要素に関する脆弱性情報を、前記ユーザ端末に更に出力する、

ことを含む請求項９に記載の脆弱性情報管理方法。

[請求項11] 前記製品構成情報は、製品に含まれる構成要素の階層構造を示す情報を更に有しており、

前記コンピュータが、前記取得された製品構成情報に基づいて、製品に含まれる構成要素の階層構造を示す情報を、前記ユーザ端末に更に出力する、

ことを含む請求項９または１０に記載の脆弱性情報管理方法。

[請求項12] 前記コンピュータが、

前記階層構造において、前記脆弱性を有する構成要素の上位に位置する上位構成要素を更に特定し、

前記上位構成要素を示す情報を、前記ユーザ端末に更に出力する、

ことを含む請求項１１に記載の脆弱性情報管理方法。

[請求項13] 前記コンピュータが、

前記階層構造を示す情報において構成要素のいずれかを選択する

入力を受け付け、

前記入力により選択された構成要素に関する脆弱性情報を、前記ユーザ端末に更に出力する、

ことを含む請求項１１または１２に記載の脆弱性情報管理方法。

[請求項14] 前記コンピュータが、

脆弱性を指定する入力を受け付け、

前記脆弱性情報記憶手段を参照して、前記取得された製品構成情報に対応する構成要素の中から、前記入力により指定された脆弱性を有する構成要素を特定し、

前記入力により指定された脆弱性を有する構成要素を示す情報を、前記ユーザ端末に出力する、

ことを含む請求項９から１３のいずれか１項に記載の脆弱性情報管理方法。

[請求項15] 前記コンピュータが、

製品に関して見つかった脆弱性への対処計画を示す対処計画情報を取得し、

前記対処計画情報が示す対処計画に基づいて、脆弱性への対処についてのリマインド情報をユーザに通知する、

ことを更に含む請求項９から１４のいずれか１項に記載の脆弱性情報管理方法。

[請求項16] 前記コンピュータが、

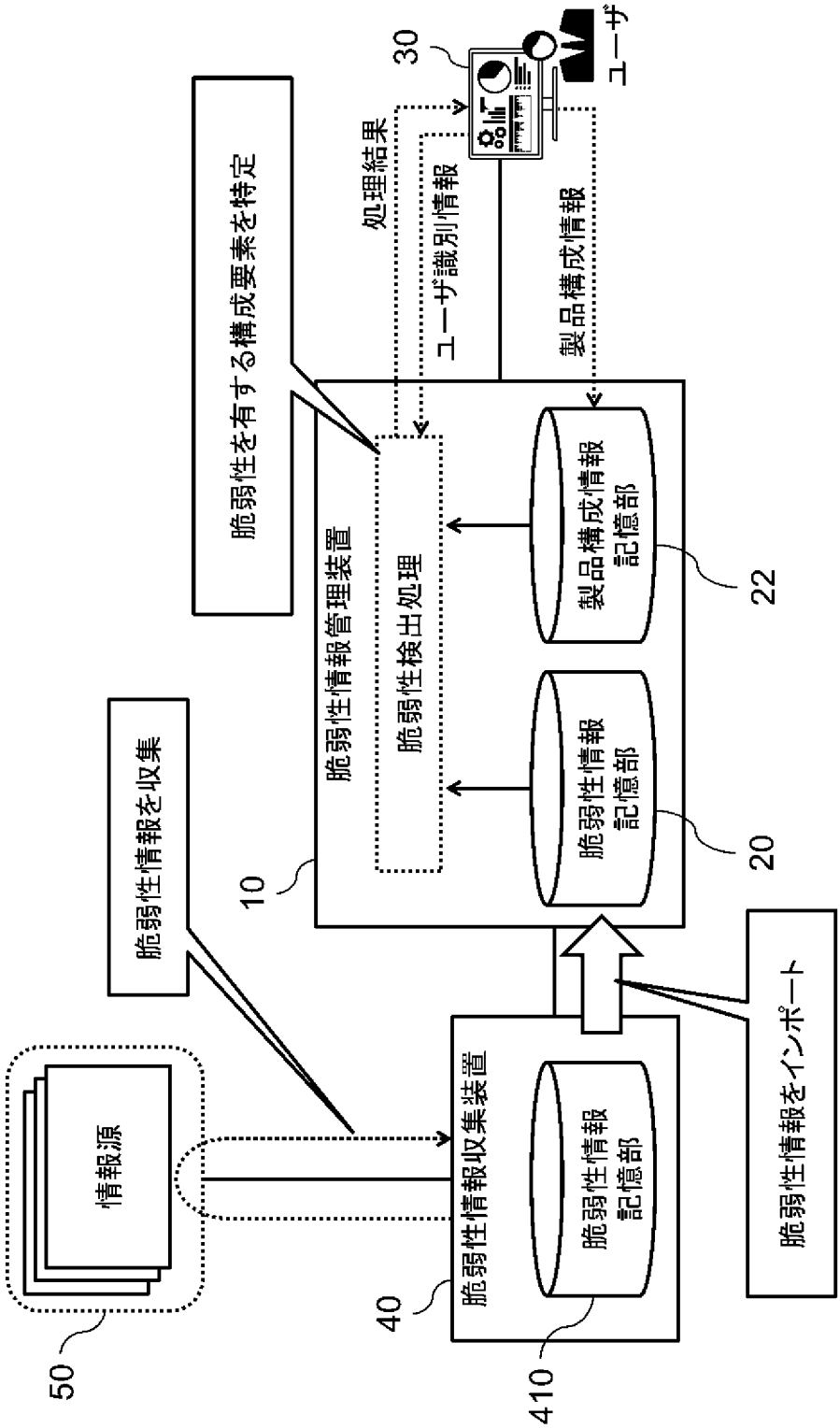
製品が属するグループを示すグループ識別情報を各ユーザのユーザ識別情報と紐付けて記憶するグループ識別情報記憶手段を参照して、前記取得されたユーザ識別情報に紐付けられたグループ識別情報を取得し、

製品の情報をグループ識別情報別に対応付けて記憶する製品情報記憶手段を参照して、取得された前記グループ識別情報に紐付けられた１以上の製品を特定する、

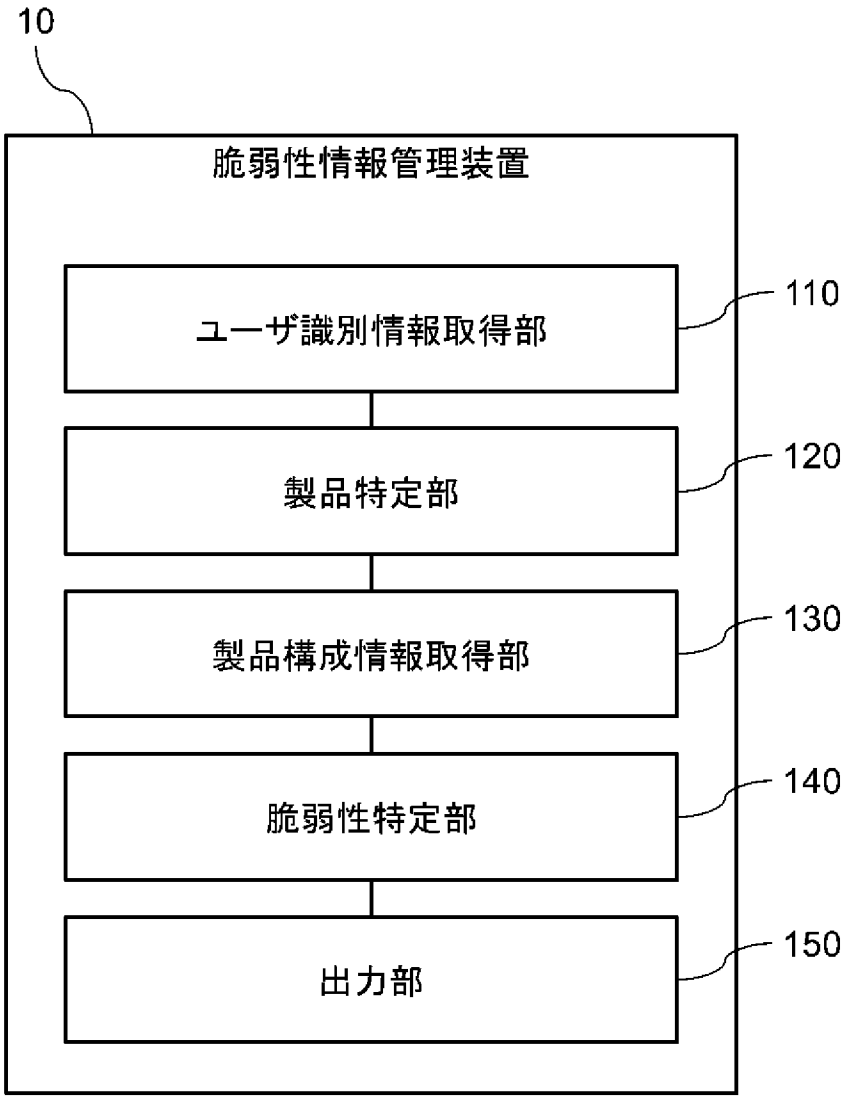
ことを含む請求項９から１５のいずれか１項に記載の脆弱性情報管理方法。

[請求項17] コンピュータに、請求項９から１６のいずれか１項に記載の脆弱性情報管理方法を実行させるプログラム。

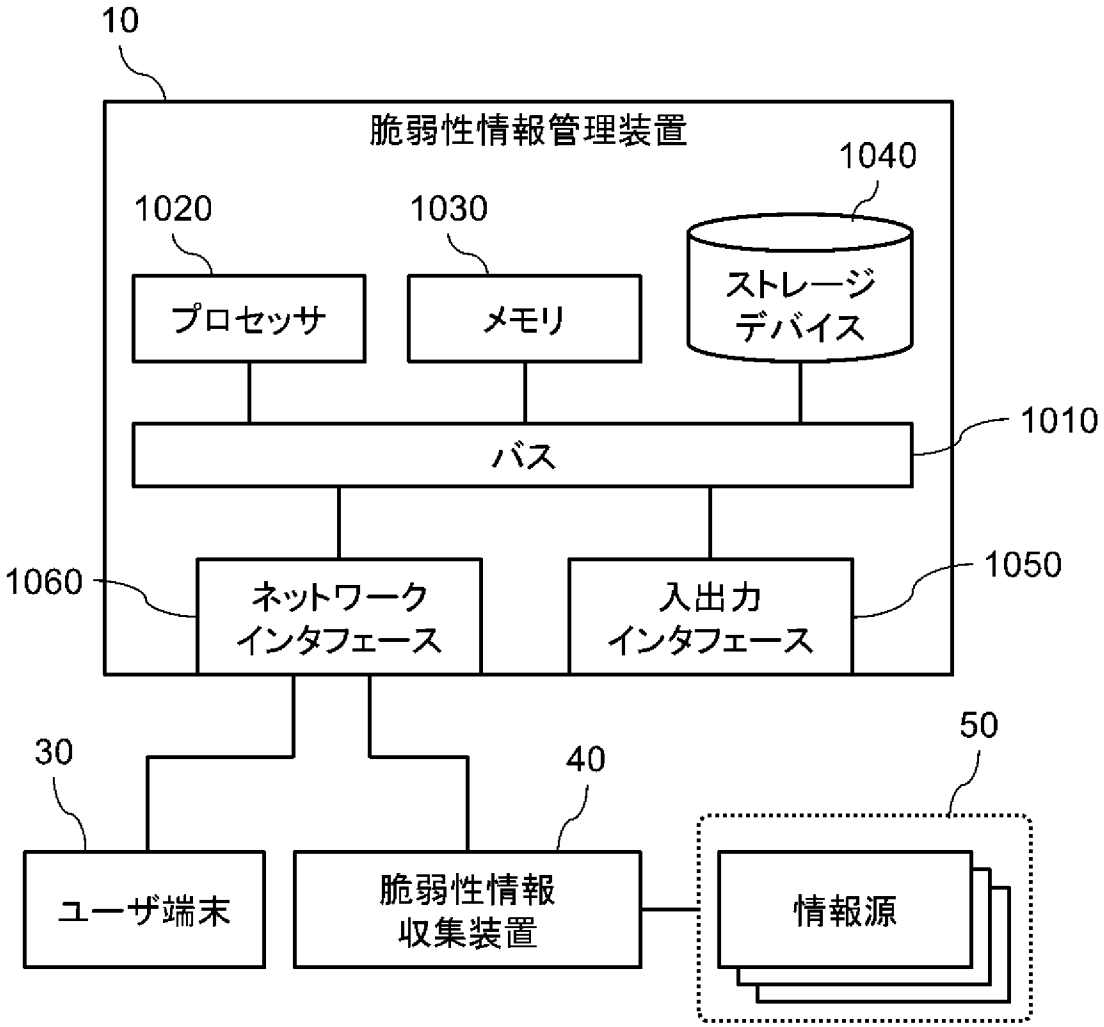
[図1]


脆弱性を有する構成要素を特定
脆弱性情報を収集
情報源
50
脆弱性情報収集装置
40
脆弱性情報
記憶部
410
脆弱性情報をインポート
脆弱性情報管理装置
10
脆弱性検出処理
脆弱性情報
記憶部
20
製品構成情報
記憶部
22
処理結果
ユーザ識別情報
製品構成情報
30
ユーザ

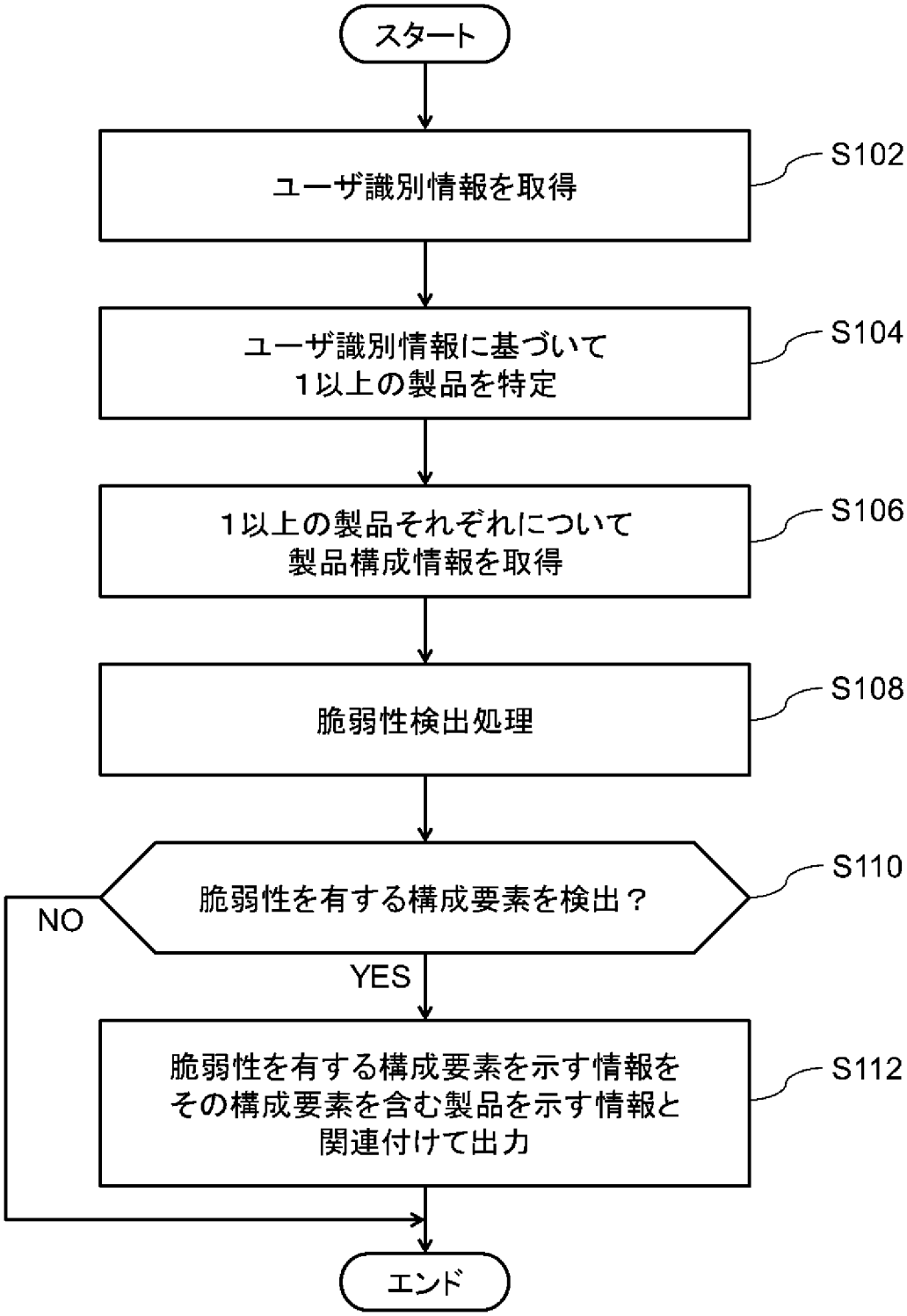
[図2]


10
脆弱性情報管理装置
ユーザ識別情報取得部
110
製品特定部
120
製品構成情報取得部
130
脆弱性特定部
140
出力部
150

[図3]


10
脆弱性情報管理装置
1040
1020
1030
プロセッサ
メモリ
ストレージ
デバイス
1010
バス
1060
ネットワーク
インタフェース
入出力
インタフェース
1050
30
40
50
ユーザ端末
脆弱性情報
収集装置
情報源

[図4]

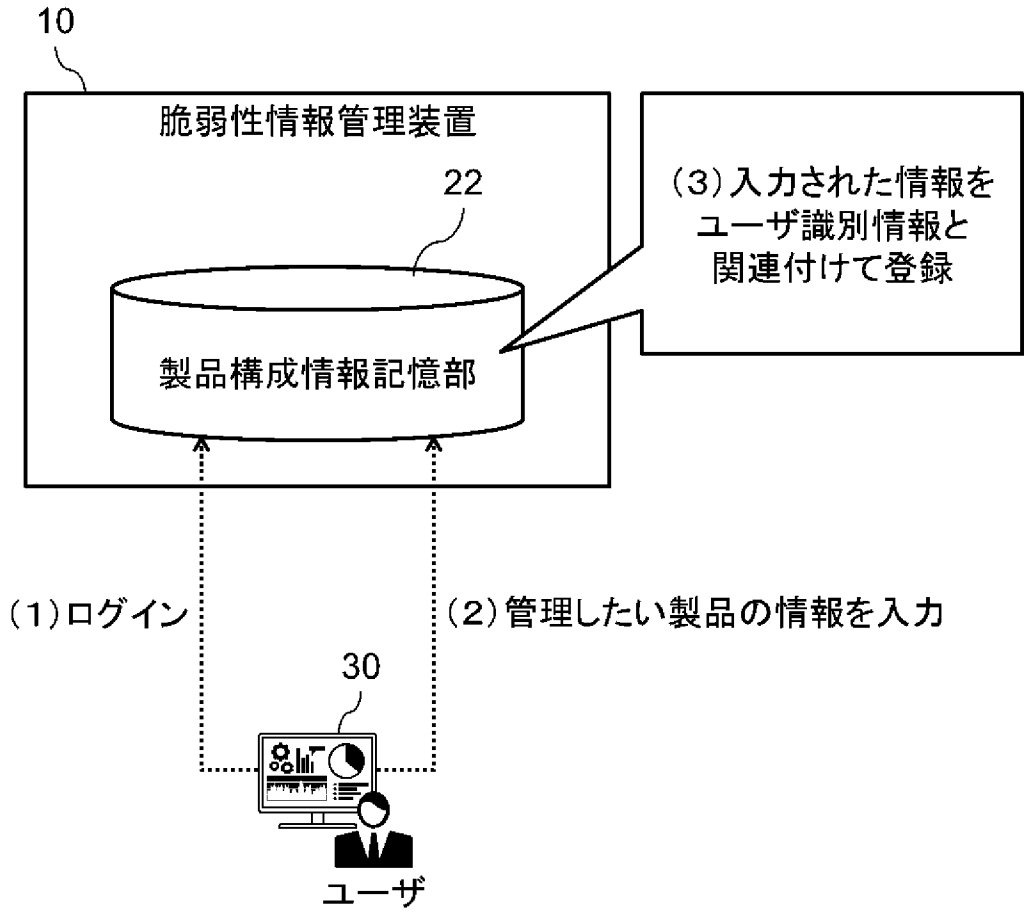

スタート
ユーザ識別情報を取得
S102
ユーザ識別情報に基づいて
1以上の製品を特定
S104
1以上の製品それぞれについて
製品構成情報を取得
S106
脆弱性検出処理
S108
脆弱性を有する構成要素を検出？
S110
NO
YES
脆弱性を有する構成要素を示す情報を
その構成要素を含む製品を示す情報と
関連付けて出力
S112
エンド

[図5]

22

ユーザID	製品ID	製品構成情報				
		要素ID	要素名	バージョン情報	階層構造情報	…
U001	PD001（製品A）	E001	部品A1	1.5	/E001	
		E002	部品A2	1.0	/E002	
		E003	電子部品1	1.5	/E001/E003	
		E004	電子部品2	1.0	/E002/E004	
		E005	XXX#1	1.5	/E001/E003/E005	
		E006	XXX#2	1.0	/E002/E004/E006	
		E007	XXX#3	1.0	/E002/E004/E007	
		E008	XXX#4	2.0	///E008	
	PD002（製品B）	E009	部品B1	1.5	/E009	
		E010	部品B2	1.2	/E010	
		E011	電子部品3	1.0	/E010/E011	
		E012	電子部品4	1.0	/E010/E012	
		E013	XXX#5	1.2	/E009//E013	
		E014	XXX#6	2.0	/E009//E014	
		E015	XXX#7	2.2	/E010/E011/E015	
		E016	XXX#8	1.0	/E010/E012/E016	
		E017	XXX#9	1.5	/E010/E012/E017	
	…	…	…	…	…	
…	…					

[図6]

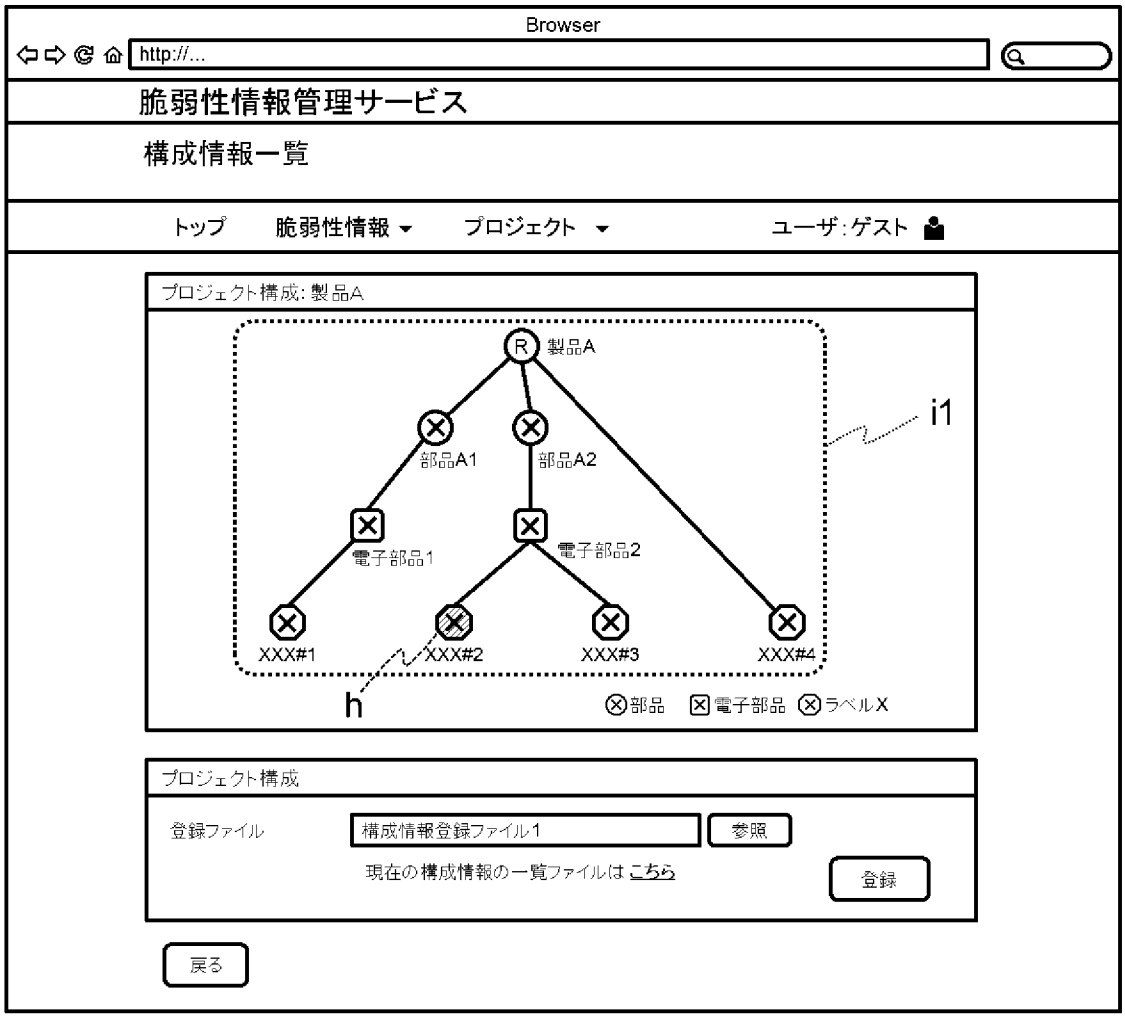

10
脆弱性情報管理装置
22
製品構成情報記憶部
(3)入力された情報を
ユーザ識別情報と
関連付けて登録
(1)ログイン
(2)管理したい製品の情報を入力
30
ユーザ

[図7]

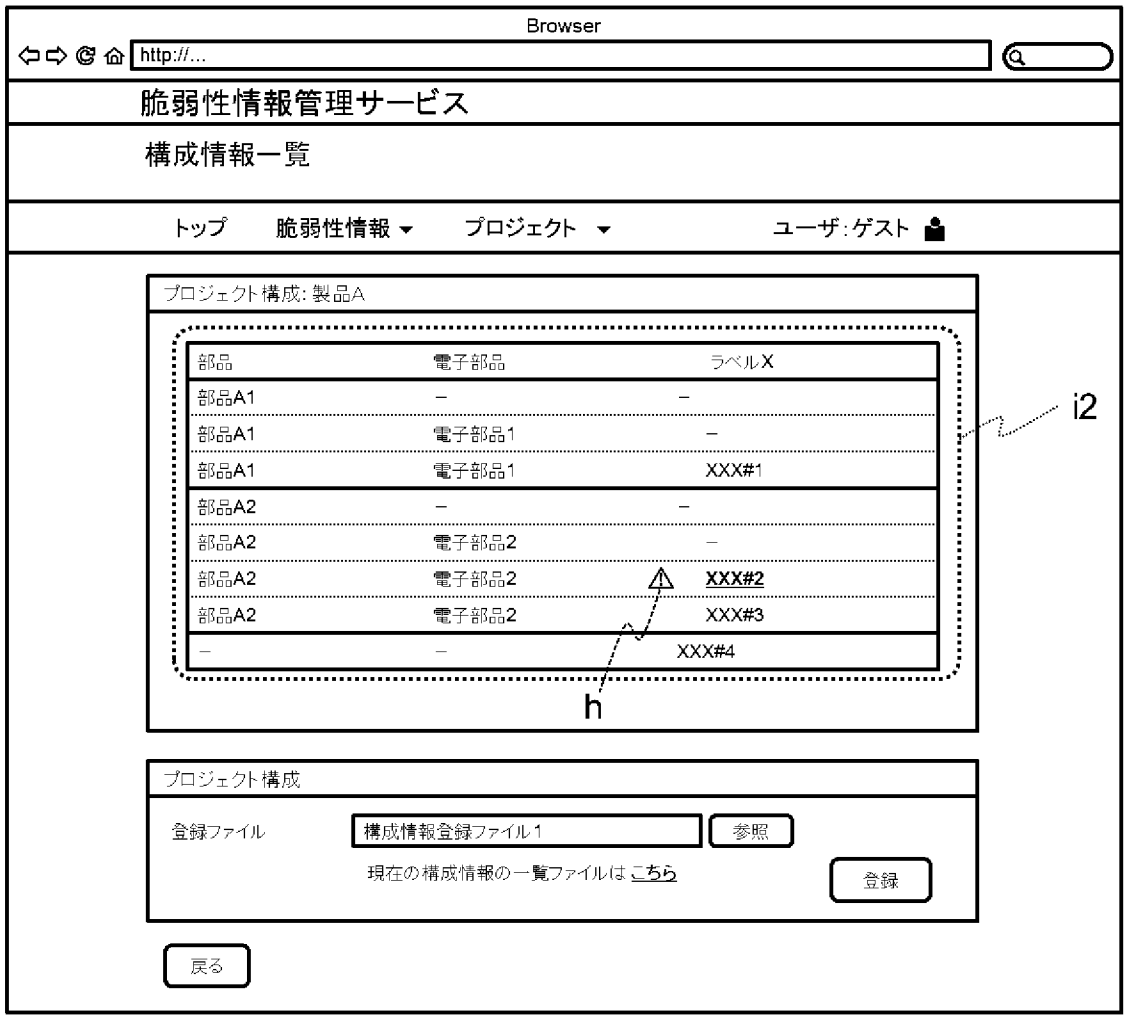
20

脆弱性情報ID	脆弱性情報	影響を受ける要素	
		要素名	バージョン情報
V001	・脆弱性の詳細:・・・ ・危険度:Critical ・確認方法:・・・ ・対処方法:・・・ ⋮	XXX#1	1.2以前
		XXX#2	1.0
		XXX#5	2.0以前
V002	・脆弱性の詳細:・・・ ・危険度:Low ・確認方法:・・・ ・対処方法:・・・ ⋮	部品B2	1.0
V003	・脆弱性の詳細:・・・ ・危険度:High ・確認方法:・・・ ・対処方法:・・・ ⋮	電子部品3	1.5以前
⋮	⋮	⋮	⋮

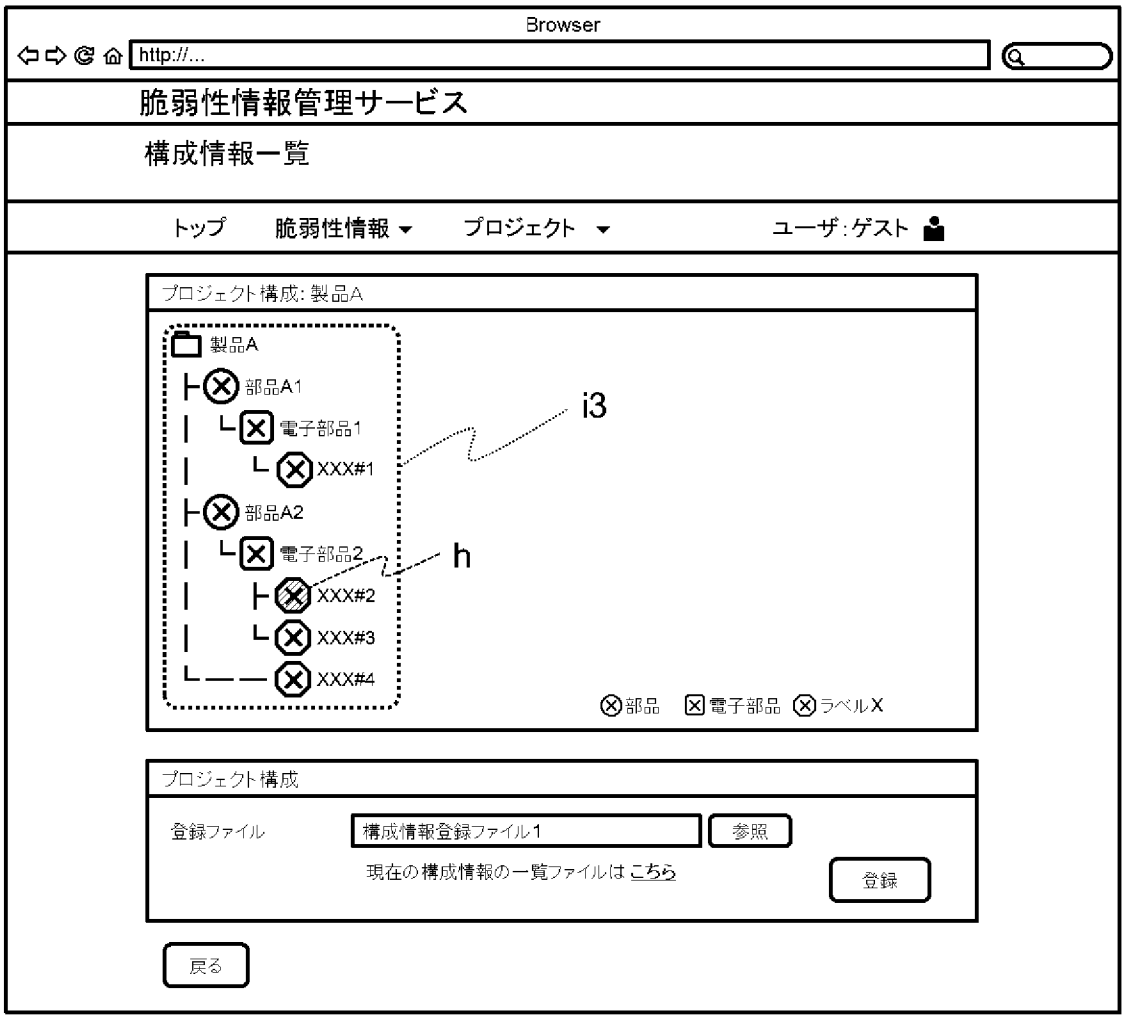
[図8]


Browser
http://...
脆弱性情報管理サービス
構成情報一覧
トップ
脆弱性情報
プロジェクト
ユーザ:ゲスト
プロジェクト構成:製品A
R
製品A
部品A1
部品A2
電子部品1
電子部品2
XXX#1
XXX#2
XXX#3
XXX#4
i1
h
部品
電子部品
ラベルX
プロジェクト構成
登録ファイル
構成情報登録ファイル1
参照
現在の構成情報の一覧ファイルは こちら
登録
戻る

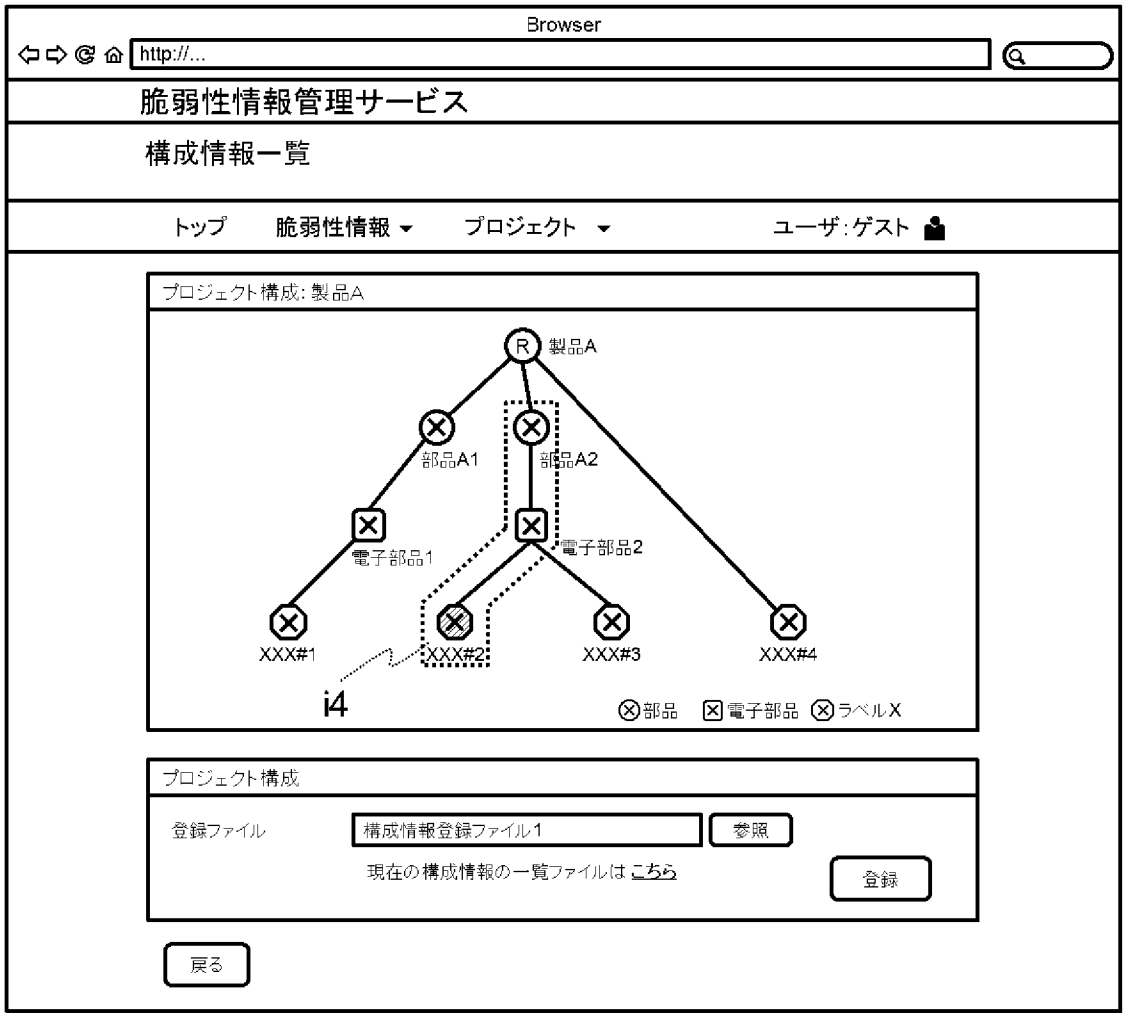
[図9]


Browser
http://...
脆弱性情報管理サービス
構成情報一覧
トップ
脆弱性情報
プロジェクト
ユーザ:ゲスト
プロジェクト構成: 製品A
部品
電子部品
ラベルX
部品A1 – –
部品A1 電子部品1 –
部品A1 電子部品1 XXX#1
部品A2 – –
部品A2 電子部品2 –
部品A2 電子部品2 XXX#2
部品A2 電子部品2 XXX#3
– – XXX#4
i2
h
プロジェクト構成
登録ファイル
構成情報登録ファイル1
参照
現在の構成情報の一覧ファイルは こちら
登録
戻る

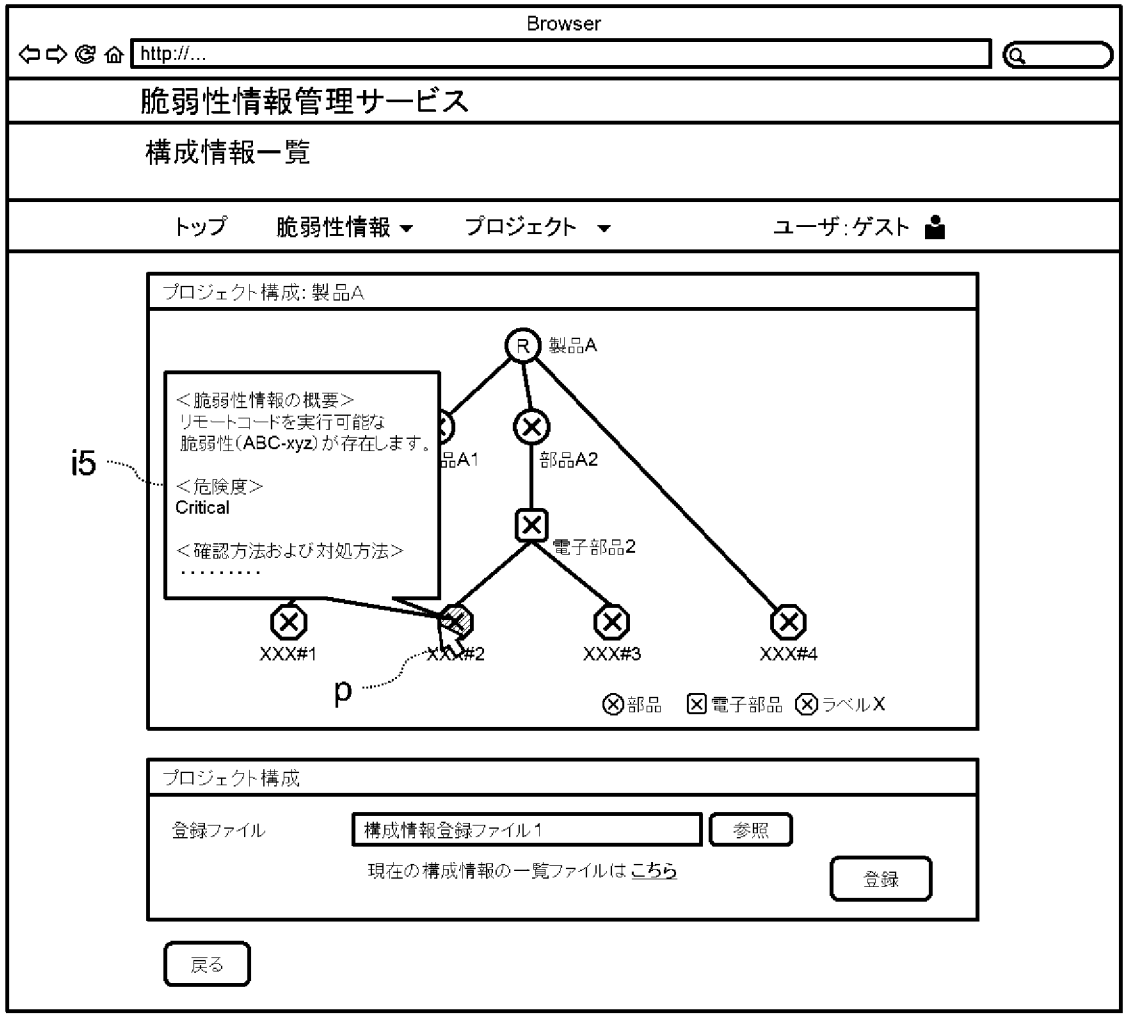
[図10]


Browser
http://...
脆弱性情報管理サービス
構成情報一覧
トップ
脆弱性情報
プロジェクト
ユーザ:ゲスト
プロジェクト構成:製品A
製品A
部品A1
電子部品1
XXX#1
部品A2
電子部品2
XXX#2
XXX#3
XXX#4
i3
h
部品
電子部品
ラベルX
プロジェクト構成
登録ファイル
構成情報登録ファイル1
参照
現在の構成情報の一覧ファイルは こちら
登録
戻る

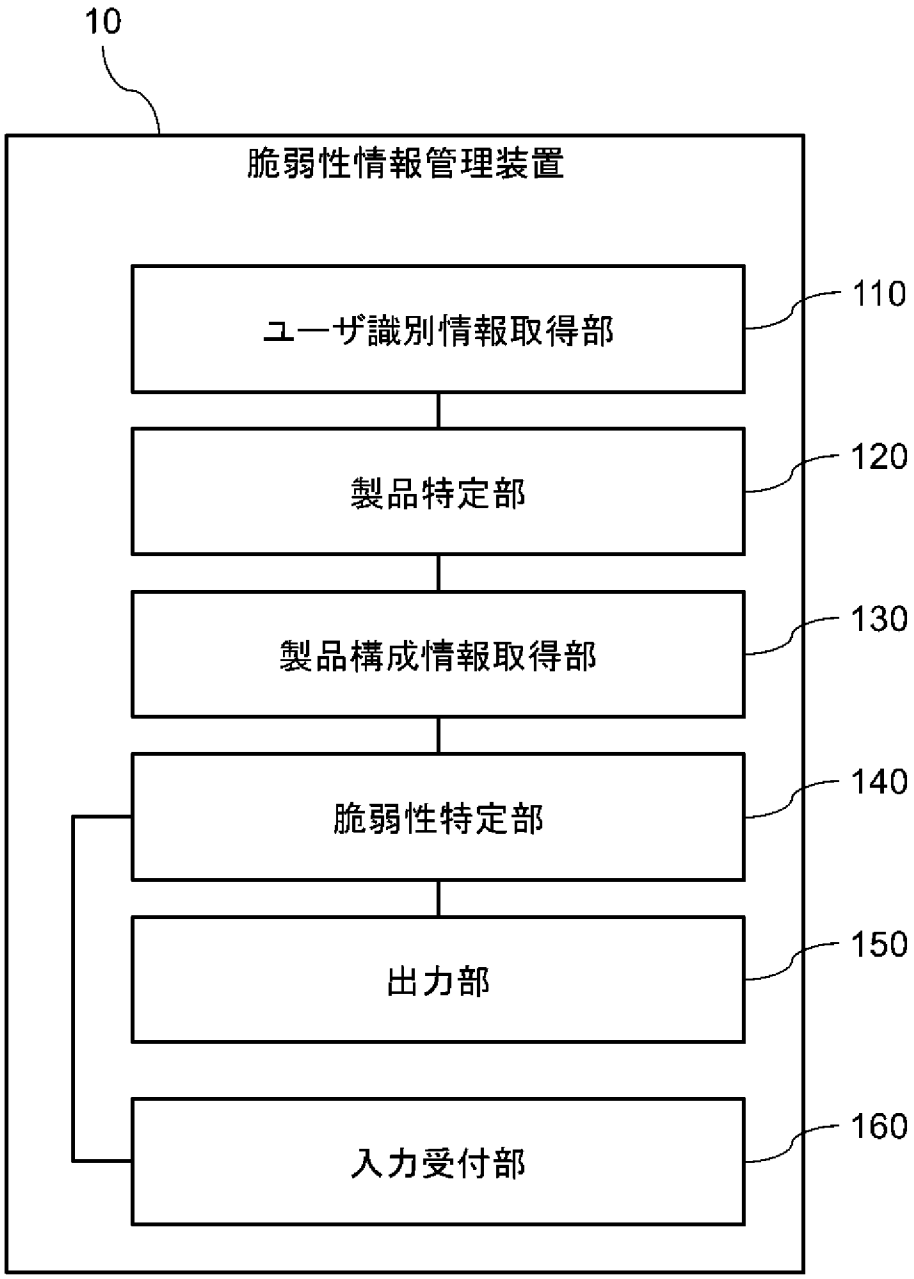
[図11]


Browser
http://...
脆弱性情報管理サービス
構成情報一覧
トップ
脆弱性情報
プロジェクト
ユーザ:ゲスト
プロジェクト構成:製品A
R
製品A
部品A1
部品A2
電子部品1
電子部品2
XXX#1
XXX#2
XXX#3
XXX#4
i4
部品
電子部品
ラベルX
プロジェクト構成
登録ファイル
構成情報登録ファイル1
参照
現在の構成情報の一覧ファイルは こちら
登録
戻る

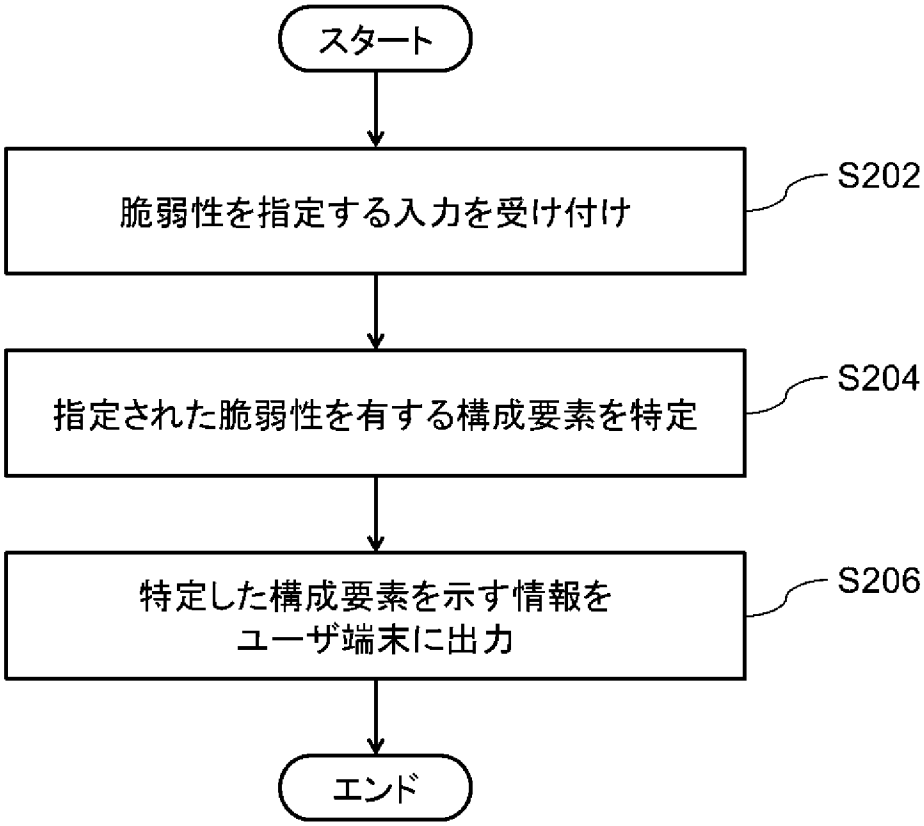
[図12]


Browser
http://...
脆弱性情報管理サービス
構成情報一覧
トップ
脆弱性情報
プロジェクト
ユーザ:ゲスト
プロジェクト構成: 製品A
製品A
＜脆弱性情報の概要＞
リモートコードを実行可能な
脆弱性(ABC-xyz)が存在します。
＜危険度＞
Critical
＜確認方法および対処方法＞
・・・・・・・・・
i5
品A1
部品A2
電子部品2
XXX#1
XXX#2
XXX#3
XXX#4
p
部品
電子部品
ラベルX
プロジェクト構成
登録ファイル
構成情報登録ファイル1
参照
現在の構成情報の一覧ファイルは こちら
登録
戻る

[図13]


10
脆弱性情報管理装置
ユーザ識別情報取得部
110
製品特定部
120
製品構成情報取得部
130
脆弱性特定部
140
出力部
150
入力受付部
160

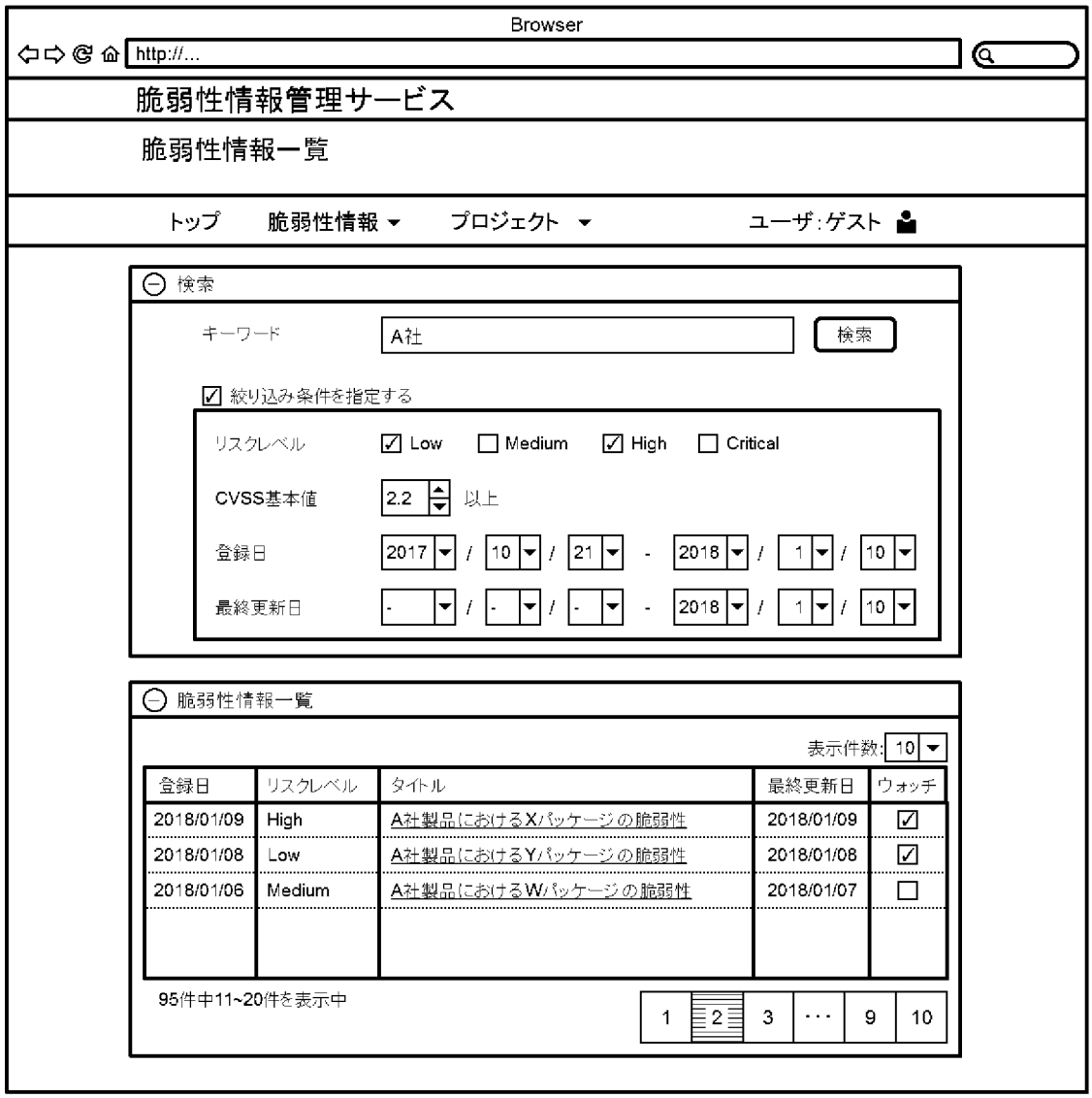
[図14]


スタート
脆弱性を指定する入力を受け付け
S202
指定された脆弱性を有する構成要素を特定
S204
特定した構成要素を示す情報を
ユーザ端末に出力
S206
エンド

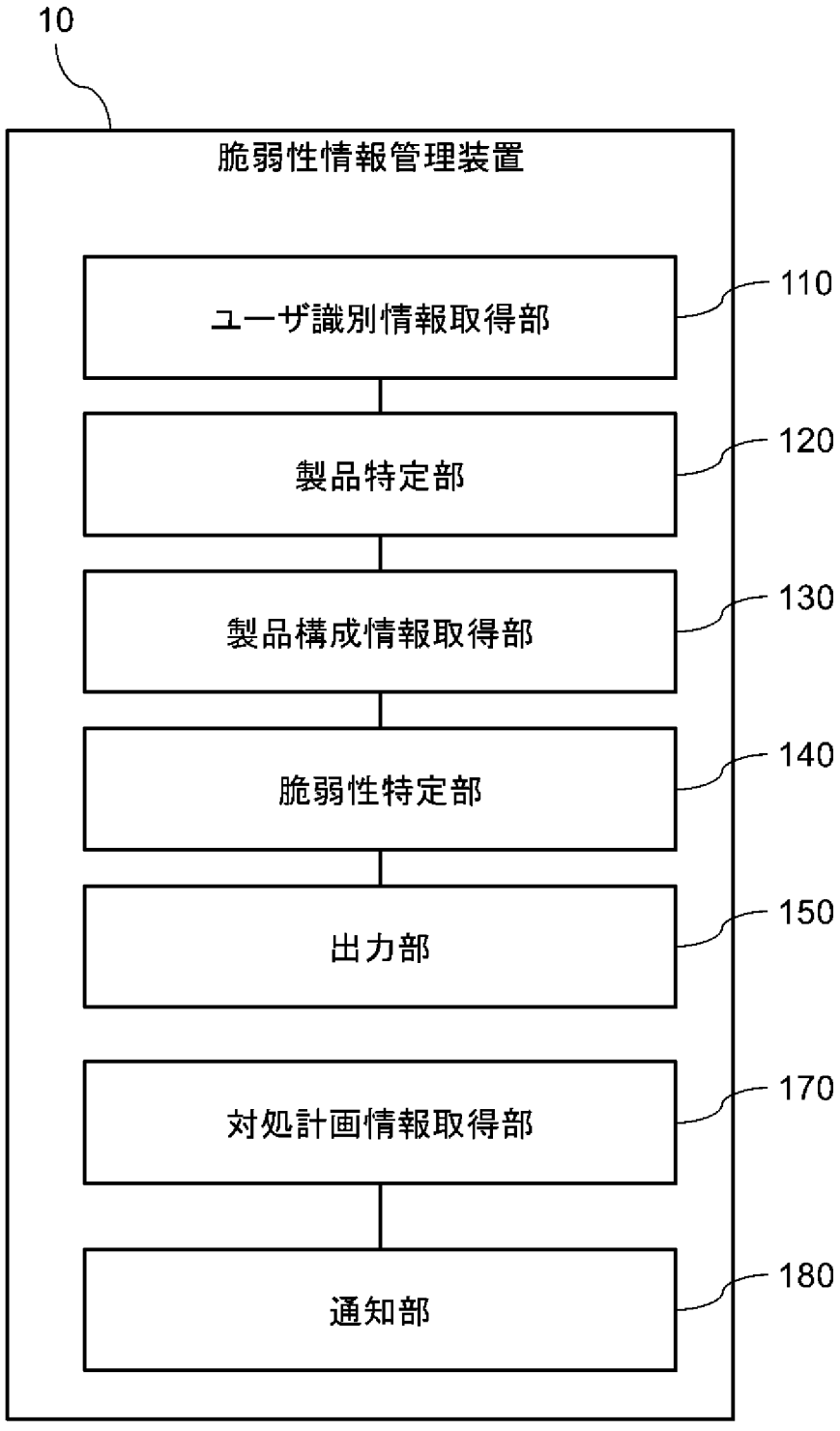
[図15]


Browser
http://...
脆弱性情報管理サービス
トップページ
トップ
脆弱性情報
プロジェクト
ユーザ:ゲスト
i6
新着脆弱性情報一覧
表示件数: 10
登録日 リスクレベル タイトル 最終更新日
2018/01/09 High A社製品におけるXパッケージの脆弱性 2018/01/09
2018/01/08 Low A社製品におけるYパッケージの脆弱性 2018/01/08
2018/01/07 Critical B社製ソフトウェアZにおけるリモートコード実行の脆弱性 2018/01/09
95件中11~20件を表示中
1 2 3 ・・・ 9 10
ウォッチ一覧
表示件数: 20
登録日 リスクレベル タイトル 最終更新日
2018/01/07 Critical B社製ソフトウェアZにおけるリモートコード実行の脆弱性 2018/01/09
2018/01/08 Low A社製品におけるYパッケージの脆弱性 2018/01/08
2018/01/09 High A社製品におけるXパッケージの脆弱性 2018/01/09
12件中1~12件を表示中
1

[図16]


Browser
http://...
脆弱性情報管理サービス
脆弱性情報一覧
トップ
脆弱性情報
プロジェクト
ユーザ:ゲスト
検索
キーワード
A社
検索
絞り込み条件を指定する
リスクレベル
Low
Medium
High
Critical
CVSS基本値
2.2
以上
登録日
2017 / 10 / 21 - 2018 / 1 / 10
最終更新日
- / - / - - 2018 / 1 / 10
脆弱性情報一覧
表示件数: 10
登録日
リスクレベル
タイトル
最終更新日
ウォッチ
2018/01/09
High
A社製品におけるXパッケージの脆弱性
2018/01/09
2018/01/08
Low
A社製品におけるYパッケージの脆弱性
2018/01/08
2018/01/06
Medium
A社製品におけるWパッケージの脆弱性
2018/01/07
95件中11~20件を表示中
1
2
3
・・・
9
10

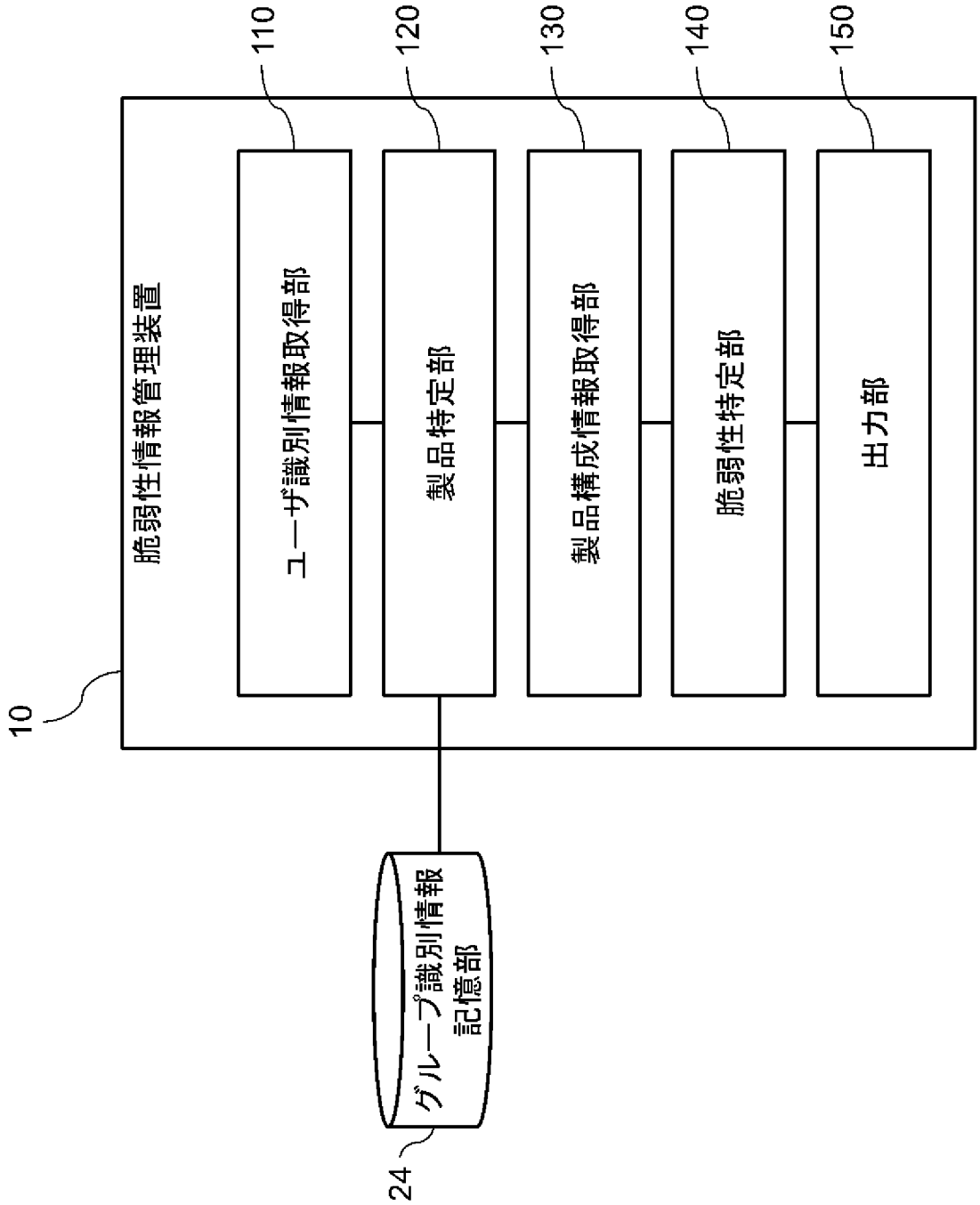
[図17]


10
脆弱性情報管理装置
ユーザ識別情報取得部
110
製品特定部
120
製品構成情報取得部
130
脆弱性特定部
140
出力部
150
対処計画情報取得部
170
通知部
180

[図18]

ユーザID	対処計画情報
U001	・脆弱性ID：V001 ・完了予定日：YYYY/MM/DD ・進捗状態：調査中 ⋮
	・脆弱性ID：V002 ・完了予定日：YYYY/MM/DD ・進捗状態：未確認 ⋮
U002	・脆弱性ID：V003 ・完了予定日：YYYY/MM/DD ・進捗状態：対処済（完了日：YYYY/MM/DD） ⋮
	・脆弱性ID：V004 ・完了予定日：YYYY/MM/DD ・進捗状態：未確認 ⋮
⋮	⋮

[図19]


10
脆弱性情報管理装置
110
ユーザ識別情報取得部
120
製品特定部
130
製品構成情報取得部
140
脆弱性特定部
150
出力部
24
グループ識別情報
記憶部

[図20]

24

グループID	ユーザID
G001	U001,U002,...
G002	U101,U102,...
⋮	⋮

[図21]

22

グループID	製品ID	製品構成情報				
		要素ID	要素名	バージョン情報	階層構造情報	…
G001	PD001（製品A）	E001	部品A1	1.5	/E001	
		E002	部品A2	1.0	/E002	
		E003	電子部品1	1.5	/E001/E003	
		E004	電子部品2	1.0	/E002/E004	
		E005	XXX#1	1.5	/E001/E003/E005	
		E006	XXX#2	1.0	/E002/E004/E006	
		E007	XXX#3	1.0	/E002/E004/E007	
		E008	XXX#4	2.0	///E008	
		E009	部品B1	1.5	/E009	
	PD002（製品B）	E010	部品B2	1.2	/E010	
		E011	電子部品3	1.0	/E010/E011	
		E012	電子部品4	1.0	/E010/E012	
		E013	XXX#5	1.2	/E009//E013	
		E014	XXX#6	2.0	/E009//E014	
		E015	XXX#7	2.2	/E010/E011/E015	
		E016	XXX#8	1.0	/E010/E012/E016	
		E017	XXX#9	1.5	/E010/E012/E017	
	…	…	…	…	…	
…	…					

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/034930

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl. G06F21/57(2013.01)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)
Int.Cl. G06F21/57

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Published examined utility model applications of Japan	1922-1996
Published unexamined utility model applications of Japan	1971-2019
Registered utility model specifications of Japan	1996-2019
Published registered utility model applications of Japan	1994-2019

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.
X	JP 2009-015570 A (NIPPON TELEGRAPH AND TELEPHONE CORP.) 22 January 2009, paragraphs [0025]-[0045],	1, 2, 7, 9, 10, 15, 17
Y	[0084]-[0093] (Family: none)	6, 14
A		3-5, 8, 11-13, 16
Y	JP 2007-058514 A (MITSUBISHI ELECTRIC CORP.) 08 March 2007, paragraphs [0046]-[0052] (Family: none)	6, 14

☒ 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
15 November 2019 (15.11.2019)	26 November 2019 (26.11.2019)

Name and mailing address of the ISA/	Authorized officer
Japan Patent Office 3-4-3, Kasumigaseki, Chiyoda-ku, Tokyo 100-8915, Japan	Telephone No.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2019/034930

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP 2016-091402 A (HITACHI, LTD.) 23 May 2016 (Family: none)	1-17
A	JP 2008-197877 A (NEC CORP.) 28 August 2008 (Family: none)	1-17
A	JP 2003-108521 A (TOSHIBA CORP.) 11 April 2003 (Family: none)	1-17

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２０１９／０３４９３０

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Int.Cl.　G06F21/57(2013.01)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.　G06F21/57

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	１９７１－２０１９年
日本国実用新案登録公報	１９９６－２０１９年
日本国登録実用新案公報	１９９４－２０１９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
X	JP 2009-015570 A（日本電信電話株式会社）2009.01.22, 段落２５－４５，８４－９３（ファミリーなし）	1,2,7,9,10,15,17
Y		6,14
A		3-5,8,11-13,16
Y	JP 2007-058514 A（三菱電機株式会社）2007.03.08, 段落４６－５２（ファミリーなし）	6,14

☑　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
１５．１１．２０１９	２６．１１．２０１９

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）　５Ｓ　５３８０
和平　悠希
電話番号　０３－３５８１－１１０１　内線　３５４６

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 2016-091402 A（株式会社日立製作所）2016.05.23,（ファミリーなし）	1-17
A	JP 2008-197877 A（日本電気株式会社）2008.08.28,（ファミリーなし）	1-17
A	JP 2003-108521 A（株式会社東芝）2003.04.11,（ファミリーなし）	1-17