(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-102479
(P2004-102479A)
(43)公開日　平成16年4月2日(2004.4.2)

(51)Int.Cl.[7]	F I	テーマコード（参考）
G06F 15/00	G06F 15/00 330A	5B085

審査請求 未請求　請求項の数 4　ＯＬ　（全 9 頁）

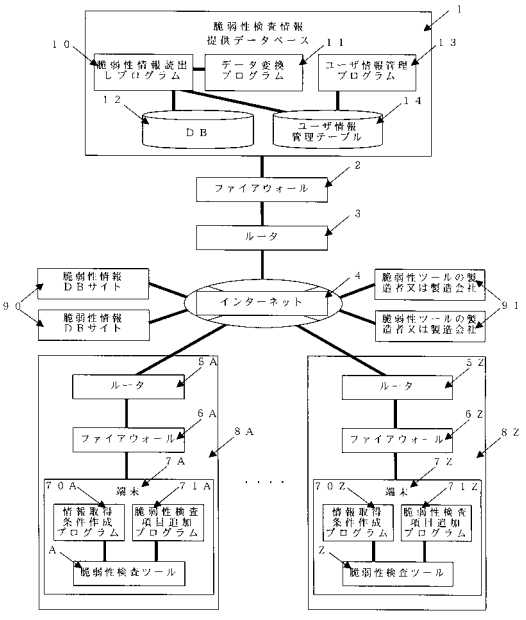
(21)出願番号　特願2002-261039(P2002-261039)
(22)出願日　平成14年9月6日(2002.9.6)

(71)出願人　000233055
日立ソフトウエアエンジニアリング株式会社
神奈川県横浜市鶴見区末広町一丁目１番４３
(74)代理人　100096954
弁理士　矢島　保夫
(72)発明者　杉山　雅樹
神奈川県横浜市中区尾上町６丁目８１番地　日立ソフトウエアエンジニアリング株式会社内
(72)発明者　丑屋　幸男
神奈川県横浜市中区尾上町６丁目８１番地　日立ソフトウエアエンジニアリング株式会社内

Ｆターム(参考)　5B085 AA08 AC16 BG01 BG04 BG07

(54)【発明の名称】脆弱性検査情報提供システム及び脆弱性検査情報提供方法

(57)【要約】
【課題】情報通信ネットワーク及びシステムに対する脆弱性検査を、常に最新の脆弱性情報に基づいた脆弱性検査項目により、簡易に実施できるようにすることを目的とする。
【解決手段】脆弱性検査情報提供システムには、多種類ある脆弱性検査ツールの脆弱性検査情報項目の情報をすべて包含する脆弱性検査情報をその登録日時とともに格納したデータベースを設ける。ユーザシステムは、一定時間間隔で脆弱性検査情報提供データベースに対して読出し条件情報を送る。読出し条件情報を受けた脆弱性検査情報提供データベースは、前回脆弱性情報を取得した日時以降に登録された脆弱性検査情報をデータベースから読出し、そのユーザシステムの脆弱性検査ツールの種類に応じた形式変換を行ってユーザシステムに送る。ユーザシステムは、前記変換後の脆弱性検査情報を新たに追加すべき脆弱性検査情報として脆弱性検査ツールに追加設定する。
【選択図】　図１



【特許請求の範囲】
【請求項１】
ユーザシステムにインストールされている脆弱性検査ツールに対してネットワークを介して脆弱性検査情報を提供する脆弱性検査情報提供システムであって、
多種類ある脆弱性検査ツールの脆弱性検査情報項目の情報をすべて包含する脆弱性検査情報を格納したデータベースと、
前記ユーザシステムから所定の情報が送信されたとき、当該ユーザシステムに現在反映されていない脆弱性検査情報を、前記データベースから読出す手段と、
読出した脆弱性検査情報を、前記ユーザシステムの脆弱性検査ツールの種類に応じた形式に変換する手段と、
変換後の脆弱性検査情報を、新たに追加すべき脆弱性検査情報として前記ユーザシステムに送信する手段と
を備えたことを特徴とする脆弱性検査情報提供システム。
【請求項２】
ユーザシステムにインストールされている脆弱性検査ツールに対してネットワークを介して脆弱性検査情報を提供する脆弱性検査情報提供システムであって、
多種類ある脆弱性検査ツールの脆弱性検査情報項目の情報をすべて包含する脆弱性検査情報を、その登録日時とともに、格納したデータベースと、
前記ユーザシステムから、前回脆弱性情報を取得した日時を含む所定の情報が送信されたとき、前記データベースから、前回脆弱性情報を取得した日時以降に登録された脆弱性検査情報を読出す手段と、
読出した脆弱性検査情報を、前記ユーザシステムの脆弱性検査ツールの種類に応じた形式に変換する手段と、
変換後の脆弱性検査情報を、新たに追加すべき脆弱性検査情報として前記ユーザシステムに送信する手段と
を備えたことを特徴とする脆弱性検査情報提供システム。
【請求項３】
脆弱性検査ツールがインストールされているユーザシステムと、該脆弱性検査ツールに対して脆弱性検査情報を配布する脆弱性検査情報提供データベースとをネットワークに接続した脆弱性検査情報配布システムであって、
前記ユーザシステムは、
一定の時間間隔で、前記脆弱性検査情報提供データベースに対して、所定の情報を送信する手段と、
前記脆弱性検査情報提供データベースから脆弱性検査情報が送信されてきたとき、その脆弱性検査情報を、前記脆弱性検査ツールが保持する脆弱性検査情報に追加設定する手段とを備え、
前記脆弱性検査情報提供データベースは、
多種類ある脆弱性検査ツールの脆弱性検査情報項目の情報をすべて包含する脆弱性検査情報を格納したデータベースと、
前記ユーザシステムから前記所定の情報が送信されてきたとき、当該ユーザシステムに現在反映されていない脆弱性検査情報を、前記データベースから読出す手段と、
読出した脆弱性検査情報を、前記ユーザシステムの脆弱性検査ツールの種類に応じた形式に変換する手段と、
変換後の脆弱性検査情報を、新たに追加すべき脆弱性検査情報として前記ユーザシステムに送信する手段と
を備えたことを特徴とする脆弱性検査情報配布システム。
【請求項４】
ユーザシステムにインストールされている脆弱性検査ツールに対してネットワークを介して脆弱性検査情報を提供する脆弱性検査情報提供方法であって、
ユーザシステムから一定の時間間隔で、脆弱性検査情報提供データベースに対して所定の

情報を送信するステップと、
脆弱性検査情報提供データベースにて前記所定の情報を受信したとき、当該ユーザシステムに現在反映されていない脆弱性検査情報を、多種類ある脆弱性検査ツールの脆弱性検査情報項目の情報をすべて包含する脆弱性検査情報を格納したデータベースから、読出すステップと、
読出した脆弱性検査情報を、前記ユーザシステムの脆弱性検査ツールの種類に応じた形式に変換するステップと、
変換後の脆弱性検査情報を、新たに追加すべき脆弱性検査情報として前記ユーザシステムに送信するステップと、
脆弱性検査情報提供データベースから脆弱性検査情報が送信されてきたとき、その脆弱性検査情報を、前記脆弱性検査ツールが保持する脆弱性検査情報に追加設定するステップとを備えたことを特徴とする脆弱性検査情報提供方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、情報通信ネットワーク及びシステムの脆弱性を検査するための情報提供システム及び情報提供方法に関する。
【０００２】
【従来の技術】
近年、経済、防衛等のあらゆる重要基盤分野は、高度に情報化され、情報通信ネットワーク及びシステムへの依存度が急速に高まっている。それに伴い、インターネット等の外部ネットワーク等から行われる情報通信ネットワーク及びシステムに対する不正アクセスの問題が顕在化してきている。
【０００３】
そこで、このような問題に対し、情報通信ネットワーク及びシステムのセキュリティ水準を維持・向上するため、情報通信ネットワーク及びシステムのセキュリティホールや設定等の脆弱性有無を検査するいわゆる脆弱性検査が従来から実施されている。
【０００４】
脆弱性検査を定期的に実施することで、情報通信ネットワーク及びシステムのセキュリティ上の問題点を検証・評価でき、セキュリティ水準を維持・向上することが可能となるが、脆弱性検査の性質上、実施する脆弱性検査項目及びその内容を常に最新にすることが理想となる。
【０００５】
脆弱性検査を実施するための公知の技術として、脆弱性検査ツールが存在する。脆弱性検査ツールは、情報通信ネットワーク及びシステムに対する脆弱性検査を簡易に実施できるツールである。
【０００６】
また、脆弱性検査で利用する最新の脆弱性情報を提供する手法として、例えば、下記の特許文献１に記載のものが知られている。この文献に記載の技術は、情報通信ネットワーク及びシステムのセキュリティ水準を維持・向上するための脆弱性に関する情報（改善策含む）を提供する手法に関するものである。
【０００７】
【特許文献１】特開２００２－１２３４９４
【０００８】
【発明が解決しようとする課題】
しかしながら、公知の技術である脆弱性検査ツールは、脆弱性検査項目及びその内容を最新化するために、脆弱性検査ツールの製造者又は製造会社等から定期的に提供されるパターンファイル（最新の脆弱性情報に基づき追加する脆弱性検査項目の情報）をインストールする必要があり、その提供間隔は１ヶ月程度が通常であるため、常に最新の脆弱性情報に基づいた状態で検査することができず、対処・対策が遅れるという問題がある。

【０００９】
この問題を解消するため、ユーザが自ら脆弱性検査項目を新たに追加できる機能を有する脆弱性検査ツールも存在するが、そのようなツールでは、ユーザ自らが、最新の脆弱性情報を入手・整理し、その情報を脆弱性検査ツールの脆弱性検査項目として設定する必要がある。そのため、ユーザ自身がセキュリティに関する高度な知識・ノウハウを有する必要があり、ユーザの作業負担も増大するという問題がある。
【００１０】
また、特許文献１に記載の技術は、脆弱性に関する情報（改善策含む）を提供するのみであり、脆弱性検査を実施するためには、提供される脆弱性情報に基づいて、ユーザ自身がその脆弱性検査のための項目・内容を抽出・規定する必要がある。そのため、ユーザ自身がセキュリティに関する高度な知識・ノウハウを有する必要があり、ユーザの作業負担も増大するという問題がある。
【００１１】
本発明の目的は、情報通信ネットワーク及びシステムに対する脆弱性検査を、常に最新の脆弱性情報に基づいた脆弱性検査項目により、簡易に実施できるようにすることにある。これにより、脆弱性検査結果に基づいた速やかな対処・対策が可能となる。
【００１２】
【課題を解決するための手段】
上記目的を達成するため、請求項１に係る発明は、ユーザシステムにインストールされている脆弱性検査ツールに対してネットワークを介して脆弱性検査情報を提供する脆弱性検査情報提供システムであって、多種類ある脆弱性検査ツールの脆弱性検査情報項目の情報をすべて包含する脆弱性検査情報を格納したデータベースと、前記ユーザシステムから所定の情報が送信されたとき、当該ユーザシステムに現在反映されていない脆弱性検査情報を、前記データベースから読出す手段と、読出した脆弱性検査情報を、前記ユーザシステムの脆弱性検査ツールの種類に応じた形式に変換する手段と、変換後の脆弱性検査情報を、新たに追加すべき脆弱性検査情報として前記ユーザシステムに送信する手段とを備えたことを特徴とする。
【００１３】
請求項２に係る発明は、ユーザシステムにインストールされている脆弱性検査ツールに対してネットワークを介して脆弱性検査情報を提供する脆弱性検査情報提供システムであって、多種類ある脆弱性検査ツールの脆弱性検査情報項目の情報をすべて包含する脆弱性検査情報を、その登録日時とともに、格納したデータベースと、前記ユーザシステムから、前回脆弱性情報を取得した日時を含む所定の情報が送信されたとき、前記データベースから、前回脆弱性情報を取得した日時以降に登録された脆弱性検査情報を読出す手段と、読出した脆弱性検査情報を、前記ユーザシステムの脆弱性検査ツールの種類に応じた形式に変換する手段と、変換後の脆弱性検査情報を、新たに追加すべき脆弱性検査情報として前記ユーザシステムに送信する手段とを備えたことを特徴とする。
【００１４】
請求項３に係る発明は、脆弱性検査ツールがインストールされているユーザシステムと、該脆弱性検査ツールに対して脆弱性検査情報を配布する脆弱性検査情報提供データベースとをネットワークに接続した脆弱性検査情報配布システムであって、前記ユーザシステムは、一定の時間間隔で、前記脆弱性検査情報提供データベースに対して、所定の情報を送信する手段と、前記脆弱性検査情報提供データベースから脆弱性検査情報が送信されてきたとき、その脆弱性検査情報を、前記脆弱性検査ツールが保持する脆弱性検査情報に追加設定する手段とを備え、前記脆弱性検査情報提供データベースは、多種類ある脆弱性検査ツールの脆弱性検査情報項目の情報をすべて包含する脆弱性検査情報を格納したデータベースと、前記ユーザシステムから前記所定の情報が送信されてきたとき、当該ユーザシステムに現在反映されていない脆弱性検査情報を、前記データベースから読出す手段と、読出した脆弱性検査情報を、前記ユーザシステムの脆弱性検査ツールの種類に応じた形式に変換する手段と、変換後の脆弱性検査情報を、新たに追加すべき脆弱性検査情報として前

記ユーザシステムに送信する手段とを備えたことを特徴とする。
【００１５】
請求項４に係る発明は、ユーザシステムにインストールされている脆弱性検査ツールに対してネットワークを介して脆弱性検査情報を提供する脆弱性検査情報提供方法であって、ユーザシステムから一定の時間間隔で、脆弱性検査情報提供データベースに対して所定の情報を送信するステップと、脆弱性検査情報提供データベースにて前記所定の情報を受信したとき、当該ユーザシステムに現在反映されていない脆弱性検査情報を、多種類ある脆弱性検査ツールの脆弱性検査情報項目の情報をすべて包含する脆弱性検査情報を格納したデータベースから、読出すステップと、読出した脆弱性検査情報を、前記ユーザシステムの脆弱性検査ツールの種類に応じた形式に変換するステップと、変換後の脆弱性検査情報を、新たに追加すべき脆弱性検査情報として前記ユーザシステムに送信するステップと、脆弱性検査情報提供データベースから脆弱性検査情報が送信されてきたとき、その脆弱性検査情報を、前記脆弱性検査ツールが保持する脆弱性検査情報に追加設定するステップとを備えたことを特徴とする。
【００１６】
【発明の実施の形態】
以下、本発明を実施する場合の一形態を、図面を参照して具体的に説明する。
【００１７】
図１は、本発明の実施の一形態である脆弱性検査情報提供システムの構成を示すブロック図である。
【００１８】
同図において、８Ａから８Ｚは、それぞれ、脆弱性検査情報提供システムを利用する各ユーザが運用・管理する情報通信ネットワーク及びシステムであり、インターネット４に接続されている。情報通信ネットワーク及びシステム（８Ａから８Ｚ）は、インターネット４に接続されたルータ（５Ａから５Ｚ）と、ルータ（５Ａから５Ｚ）に接続されたファイアウォール（６Ａから６Ｚ）と、ファイアウォール（６Ａから６Ｚ）に接続された端末（７Ａから７Ｚ）を含む。端末（７Ａから７Ｚ）は、ユーザが自ら脆弱性検査項目を新たに追加できる機能及びインターフェースを有する脆弱性検査ツール（ＡからＺ）と、情報取得条件作成プログラム（７０Ａから７０Ｚ）と、脆弱性検査項目追加プログラム（７１Ａから７１Ｚ）を含む。脆弱性検査ツール（ＡからＺ）は、それぞれ種類が異なるもの（例えば、別々のベンダから提供されているツール）でよい。
【００１９】
脆弱性検査情報提供システムは、インターネット４に接続されたルータ３と、ルータ３に接続されたファイアウォール２と、ファイアウォール２に接続された脆弱性検査情報提供データベース１を含む。脆弱性検査情報提供システムは、ユーザが運用・管理する情報通信ネットワーク及びシステム（８Ａから８Ｚ）の脆弱性検査ツール（ＡからＺ）が導入された端末（７Ａから７Ｚ）に対して脆弱性検査に係る情報を提供する。脆弱性検査情報提供データベース１は、最新の脆弱性情報（対処・対策情報含む）を蓄積・管理するデータベース（ＤＢ）１２と、脆弱性情報読出しプログラム１０と、データ変換プログラム１１を含む。また、脆弱性検査情報提供データベース１は、脆弱性検査情報提供システムを利用するユーザを管理するため、ユーザ情報管理プログラム１３とユーザ情報管理テーブル１４を含む。
【００２０】
本実施の形態において、脆弱性検査情報提供データベース１のＤＢ１２には、常に最新の脆弱性情報が予め格納される。この脆弱性情報は、インターネット上で公開されている脆弱性情報ＤＢサイト９０や、脆弱性検査ツールの製造者、又は製造会社９１より入手する最新の情報に基づいて作成されたものであり、ＤＢ１２に蓄積される。
【００２１】
図２に、ＤＢ１２に格納される情報形式の例を示す。ＤＢ１２の脆弱性情報は、多種類の脆弱性検査ツール（ＡからＺ）の脆弱性検査項目として形式変換可能な情報形式で格納さ

れる。すなわち、ＤＢ１２に格納される情報形式１２Ｆには、各種の脆弱性検査ツール（ＡからＺ）に脆弱性検査項目を追加設定するために必要な情報形式（ＡＦからＺＦ）がすべて包含されている。そして、ＤＢ１２に格納されている情報形式１２Ｆから、各種の脆弱性検査ツール（ＡからＺ）の脆弱性検査項目を追加設定するために必要な情報形式（ＡＦからＺＦ）へ、形式変換することができるようになっている。

【００２２】

脆弱性情報読出しプログラム１０及びデータ変換プログラム１１は、ＤＢ１２に格納される情報形式１２Ｆから、各脆弱性検査ツールに脆弱性検査項目として追加設定するために必要な情報形式（ＡＦからＺＦ）に形式変換するため、ＤＢ１２から脆弱性情報を読出し、適切な形式へデータ変換するプログラムである。これらのプログラムは、脆弱性検査ツールの種類毎に作成するものとする。

【００２３】

以下、脆弱性検査情報提供システムを利用するユーザの登録・管理方法と、利用ユーザに対する課金方法を説明する。

【００２４】

まず最初に、脆弱性検査情報提供システムを利用するユーザは、脆弱性検査情報提供システムの管理者に対して、事前に利用申請書（ユーザ名等のユーザ情報）を提出し、利用年会費を入金する。脆弱性検査情報提供システムの管理者は、利用申請書及び利用年会費の入金を確認し、利用申請書の内容と金額が妥当であった場合、脆弱性検査情報提供データベース１のユーザ情報管理プログラム１３に対して利用申請書に記載されたユーザ情報を入力する。ユーザ情報管理プログラム１３は、入力されたユーザ情報にユーザＩＤを付与して、ユーザ登録情報（ユーザ情報とユーザＩＤと登録年月日）をユーザ情報管理テーブル１４に登録する。

【００２５】

続いて、脆弱性検査情報提供システムの管理者は、脆弱性検査情報提供システムの利用申請ユーザに対して、ユーザ情報管理テーブル１４に登録されたユーザＩＤと端末側にインストールする情報取得条件作成プログラム（７０Ａから７０Ｚ）と脆弱性検査項目追加プログラム（７１Ａから７１Ｚ）を提供する。そして、脆弱性検査情報提供システムの利用申請ユーザは、提供されたユーザＩＤとユーザが所有する脆弱性検査ツールの名称を入力して、情報取得条件作成プログラム（７０Ａから７０Ｚ）と脆弱性検査項目追加プログラム（７１Ａから７１Ｚ）をインストールする。

【００２６】

以上により、利用申請したユーザは、登録年月日より例えば１年間、脆弱性検査情報提供システムを利用することが可能となる。なお、脆弱性検査情報提供データベース１のユーザ情報管理プログラム１３は、ユーザ情報管理テーブル１４に登録されたユーザ登録情報の登録年月日を日々自動でチェックし、登録年月日より１年間経過した場合、該当するユーザ登録情報を削除する。これにより、ユーザの脆弱性検査情報提供システムの利用を１年間に制限することが可能となる。

【００２７】

なお、１年を超え継続して脆弱性検査情報提供システムを利用したいユーザは、ユーザ情報管理テーブル１４のユーザ登録情報が削除される前に、脆弱性検査情報提供システムの管理者に対して利用申請書（利用者が所有するユーザＩＤを含むユーザ情報）を提出し、利用年会費を入金するものとする。脆弱性検査情報提供システムの管理者は、脆弱性検査情報提供データベース１のユーザ情報管理プログラム１３に対して、利用申請書に記載されたユーザＩＤを入力し、ユーザ情報管理テーブル１４の中の該当するユーザ登録情報の登録年月日を１年後の日付に更新する。これにより、更に１年間の該当ユーザによる脆弱性検査情報提供システム利用が可能となる。

【００２８】

次に、図１及び図２と、図３に示されたフローチャートを参照して、ユーザが運用・管理する情報通信ネットワーク及びシステム（８Ａから８Ｚ）の端末（７Ａから７Ｚ）の脆弱

性検査ツール（ＡからＺ）に対し、自動的に最新の脆弱性情報に基づいた脆弱性検査項目を追加設定する方法について、情報通信ネットワーク及びシステム８Ａを例にして説明する。

【００２９】

まず最初に、ユーザが運用・管理する情報通信ネットワーク及びシステム８Ａの脆弱性検査ツールＡが導入された端末７Ａ上で動作する情報取得条件作成プログラム７０Ａにより、一定の時間間隔で自動的に、脆弱性検査情報提供データベース１に対し読出し条件情報（端末７Ａに導入された脆弱性検査ツールＡの名称と、前回脆弱性検査情報提供データベース１のＤＢ１２から脆弱性情報を取得した日時と、ユーザＩＤとを含む）を送信する（ステップＳ１）。

【００３０】

その読出し条件情報を受信した脆弱性検査情報提供データベース１では、脆弱性情報読出しプログラム１０により、当該読出し条件情報（ユーザＩＤ）をキーにして、ユーザ情報管理テーブル１４からユーザ登録情報を読出し、当該ユーザが脆弱性検査情報提供システムを利用可能かどうか確認する（ステップＳ２）。

【００３１】

更に、脆弱性情報読出しプログラム１０により、当該読出し条件情報（端末７Ａに導入された脆弱性検査ツールＡの名称と、前回ＤＢ１２から脆弱性情報を取得した日時）をキーにして、端末７Ａの脆弱性検査ツールＡの脆弱性検査項目に現在反映されていない脆弱性情報をＤＢ１２から読出す（ステップＳ３）。具体的に言うと、ＤＢ１２の脆弱性情報の中から、脆弱性検査ツールＡに脆弱性検査項目を追加設定するために必要な情報ＡＦ（検査項目名、脅威情報（種別、対象製品、脅威内容、侵入コード、侵入コード実行による応答判別、情報公開日時、情報源）、対策情報、登録日時）を、前回ＤＢ１２から脆弱性情報を取得した日時より後に登録された脆弱性情報を対象にして抽出し、その全情報の読出しを行う。ここでは脆弱性検査ツールＡの名称をキーとしてＤＢ１２から脆弱性情報を読出しているが、これは脆弱性検査ツールの名称からその種類を特定し、その種類に応じた脆弱性情報を読出しているものである。したがって、脆弱性検査ツールの名称の代わりに、その種類が特定できる他の情報を用いてもよい。

【００３２】

ステップＳ３に続いて、脆弱性検査情報提供データベース１上で動作するデータ変換プログラム１１により、読出した脆弱性情報を、端末７Ａの脆弱性検査ツールＡに脆弱性検査項目として追加設定するのに適切な形式（脆弱性検査ツールの種類により異なる）へデータ変換し、その形式変換したデータを端末７Ａへ返信する（ステップＳ４）。例えば、前述した脆弱性検査ツールＡに脆弱性検査項目を追加設定するためにＤＢ１２より読出した情報に対し、脅威情報の侵入コードと侵入コード実行による応答判別とを侵入コードとして結合し、また、対策情報の対策１から対策Ｎとして整理された各項目の情報を１つのプレーンテキストの情報へ結合する、というようにデータの形式変換を行い、その形式変換したデータを端末７Ａへ返信する。

【００３３】

ステップＳ４に続いて、脆弱性検査ツールＡが導入された端末７Ａ上で動作する脆弱性検査項目追加プログラム７１Ａにより、脆弱性検査情報提供データベース１から返信されたデータを脆弱性検査ツールＡが有する脆弱性検査項目を新たに追加できる機能のインターフェースに渡すことで、脆弱性検査項目を追加する（ステップＳ５）。

【００３４】

なお、ステップＳ１からステップＳ５までの処理は全て自動的に実施される。

【００３５】

上記実施の形態では、端末側から一定の時間間隔でデータベース側に読出し条件を送ることにより、自動的に最新の脆弱性検査情報を入手するようにしたが、逆にデータベース側から端末側に対してアクションを起こすことにより、最新の脆弱性検査情報を端末側に配布するようにしてもよい。また、一定時間間隔で処理を行うのでなく、端末側からのユー

ザの指示あるいはデータベース側からの管理者の指示を契機として、上記の処理を行うようにしてもよい。

【００３６】

さらに、上記実施の形態では、ＤＢ１２の脆弱性検査情報には登録日時を付け、端末側から送る読出し条件情報には前回ＤＢ１２から脆弱性検査情報を取得した日時を含め、これらの日時を比較して、現在脆弱性検査ツールに反映されていない脆弱性検査情報をＤＢ１２から抽出したが、日時で比較する方式には限らない。日時の代わりに、ＤＢ１２内のどの脆弱性検査情報まで反映されているかが分かる情報を用いればよい。例えば、ＤＢ１２に登録された順に脆弱性検査情報に番号を付け、どの番号まで脆弱性検査ツールに反映されているかを管理する方式でもよい。

【００３７】

【発明の効果】

以上説明したように、本発明によれば、日々追加・更新される最新の脆弱性情報を自動的にユーザの脆弱性検査ツールの種類に応じた形式で取得し、脆弱性検査項目として脆弱性検査ツールに設定することができる。これにより、情報通信ネットワーク及びシステムに対する脆弱性検査を常に最新の脆弱性情報に基づいた脆弱性検査項目により実施可能となり、その検査結果に基づいた速やかなセキュリティ対処・対策が可能となる。また、最新の脆弱性情報に基づいた脆弱性検査項目が自動的に脆弱性検査ツールに設定されるため、ユーザ自らが、最新の脆弱性情報を入手・整理し、その情報を脆弱性検査ツールの脆弱性検査項目に設定するというユーザの作業負担も軽減でき、ユーザ自身がセキュリティに関する高度な知識・ノウハウを有していなくても、簡易に脆弱性検査が実施できる。更に、最新の脆弱性情報に基づいた脆弱性検査をユーザが所有する脆弱性検査ツールの種類に依存することなく実施できる。

【図面の簡単な説明】

【図１】本発明の実施の一形態の脆弱性検査情報提供システムの構成を示すブロック図である。

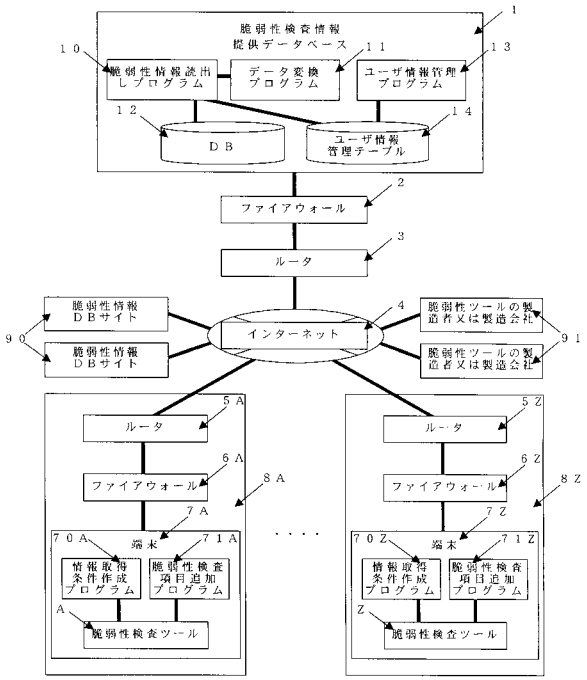
【図２】脆弱性情報を蓄積・管理するデータベース（ＤＢ）に格納される脆弱性情報の形式の例である。

【図３】本発明の実施の一形態の脆弱性検査情報提供方法を示すフローチャートである。

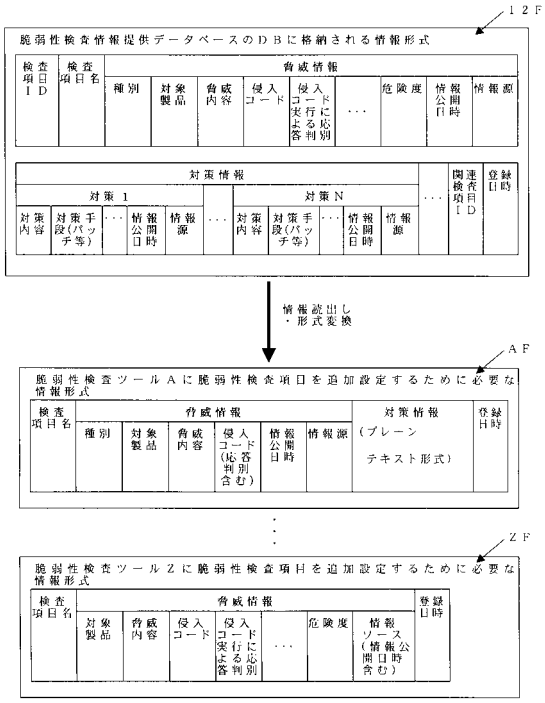
【符号の説明】

１　脆弱性検査情報提供データベース
２、６Ａ、６Ｚ　ファイアウォール
３、５Ａ、５Ｚ　ルータ
４　インターネット
７Ａ、７Ｚ　端末
８Ａ、８Ｚ　情報通信ネットワーク及びシステム
１０　脆弱性情報読出しプログラム
１１　データ変換プログラム
１２　脆弱性情報を蓄積・管理するデータベース（ＤＢ）
１２Ｆ　脆弱性検査情報提供データベースのＤＢに格納される情報形式
１３　ユーザ情報管理プログラム
１４　ユーザ情報管理テーブル
７０Ａ、７０Ｚ　情報取得条件作成プログラム
７１Ａ、７１Ｚ　脆弱性検査項目追加プログラム
９０　脆弱性情報ＤＢサイト
９１　脆弱性検査ツールの製造者、又は製造会社
Ａ、Ｚ　脆弱性検査ツール
ＡＦ　脆弱性検査ツールＡに脆弱性検査項目を追加設定するために必要な情報形式
ＺＦ　脆弱性検査ツールＺに脆弱性検査項目を追加設定するために必要な情報形式

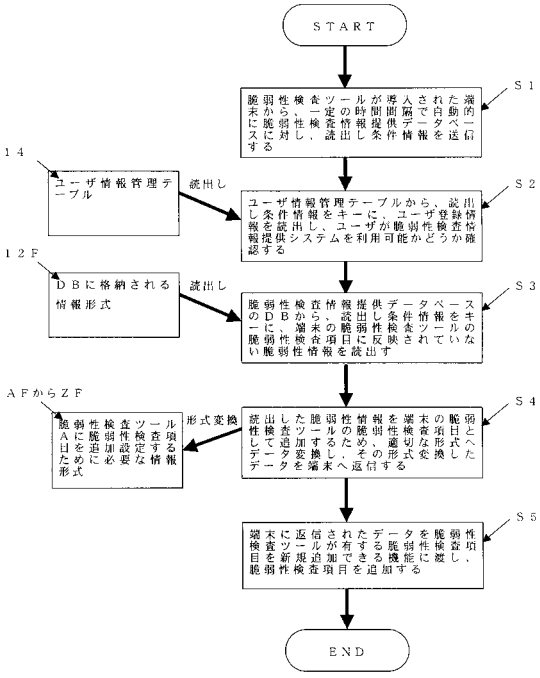
【図１】


1
脆弱性検査情報
提供データベース
10
脆弱性情報読出
しプログラム
11
データ変換
プログラム
13
ユーザ情報管理
プログラム
12
DB
14
ユーザ情報
管理テーブル
2
ファイアウォール
3
ルータ
脆弱性情報
DBサイト
90
脆弱性情報
DBサイト
4
インターネット
脆弱性ツールの製
造者又は製造会社
脆弱性ツールの製
造者又は製造会社
91
5A
ルータ
6A
ファイアウォール
8A
7A
端末
70A
71A
情報取得
条件作成
プログラム
脆弱性検査
項目追加
プログラム
A
脆弱性検査ツール
5Z
ルータ
6Z
ファイアウォール
8Z
7Z
端末
70Z
71Z
情報取得
条件作成
プログラム
脆弱性検査
項目追加
プログラム
Z
脆弱性検査ツール

【図２】


12F
脆弱性検査情報提供データベースのＤＢに格納される情報形式
検査項目ID
検査項目名
脅威情報
種別
対象製品
脅威内容
侵入コード
侵入コード実行に応答する判別
...
危険度
情報開時公開日時
情報源
対策情報
対策１
対策N
対策内容
対策手段(パッチ等)
...
情報開時公開日時
情報源
対策内容
対策手段(パッチ等)
...
情報開時公開日時
情報源
...
関連検査項目ID
登録時
情報読出し
・形式変換
AF
脆弱性検査ツールＡに脆弱性検査項目を追加設定するために必要な情報形式
検査項目名
脅威情報
種別
対象製品
脅威内容
侵入コード(応答判別含む)
情報開時公開日時
情報源
対策情報
(プレーンテキスト形式)
登録時
ZF
脆弱性検査ツールＺに脆弱性検査項目を追加設定するために必要な情報形式
検査項目名
脅威情報
対象製品
脅威内容
侵入コード
侵入コード実行に応答する判別
...
危険度
情報ソース(情報公開日時含む)
登録時

【図３】


START
S1
脆弱性検査ツールが導入された端末から、一定の時間間隔で自動的に脆弱性検査情報提供データベースに対し、読出し条件情報を送信する
14
ユーザ情報管理テーブル
読出し
S2
ユーザ情報管理テーブルから、読出し条件情報をキーに、ユーザ登録情報を読出し、ユーザが脆弱性検査情報提供システムを利用可能かどうか確認する
12F
ＤＢに格納される情報形式
読出し
S3
脆弱性検査情報提供データベースのＤＢから、読出し条件情報をキーに、端末の脆弱性検査ツールに反映されていない脆弱性情報を読出す
AFからZF
脆弱性検査ツールＡに脆弱性検査項目を追加するために必要な情報形式
形式変換
S4
読出した脆弱性情報を端末の脆弱性検査ツールで検査可能な形式に変換し、その形式変換したデータを端末へ返信する
S5
端末に返信されたデータを脆弱性検査ツールが有する脆弱性検査機能に適用し、新規追加できる脆弱性検査項目を追加する
END