(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2024-108352
(P2024-108352A)
(43)公開日　令和6年8月13日(2024.8.13)

(51)Int.Cl.		F I		テーマコード（参考）
G06F 21/50	*(2013.01)*	G06F 21/50		

審査請求 未請求　請求項の数 7　ＯＬ　（全 17 頁）

(21)出願番号　特願2023-12665(P2023-12665)
(22)出願日　令和5年1月31日(2023.1.31)

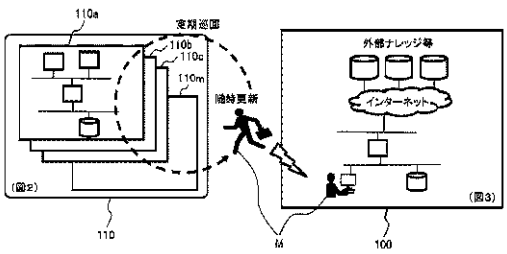
(71)出願人　000005108
株式会社日立製作所
東京都千代田区丸の内一丁目６番６号
(74)代理人　110000350
ポレール弁理士法人
(72)発明者　磯部　義明
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　永島　秀康
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内
(72)発明者　谷口　一水
東京都千代田区丸の内一丁目６番６号　株式会社日立製作所内

最終頁に続く

(54)【発明の名称】セキュリティ維持管理支援システム並びにセキュリティ維持管理支援方法

(57)【要約】
【課題】回線接続のない環境下にある多数の管理対象システムに対し、新規脅威情報に対するセキュリティ対策（検知および業務影響を考慮した対処）を支援し得るセキュリティ維持管理支援システムを提供する。
【解決手段】セキュリティ維持対象のシステムにおけるシステム構成情報と、セキュリティインシデントを検知するログ情報源の情報と、セキュリティ対処可能な箇所の対処策とその業務影響の情報とを管理情報として記憶するデータベースと計算機装置を備え、計算機装置は、新規脅威情報を入手する第１の手段と、新規脅威情報とシステム構成情報から当該新規脅威情報に該当するシステムを抽出する第２の手段と、抽出したシステムのシステム構成情報とログ情報源に適合した検知ルール情報を生成する第３の手段と、当該検知ルールが検知した際の対処策情報を生成する第４の手段と、当該対処策による業務影響の情報を生成する第５の手段を備える、ことを特徴とするセキュリティ維持管理支援システム。
【選択図】図１

図 1



【特許請求の範囲】
【請求項１】
セキュリティ維持対象のシステムにおけるシステム構成情報と、セキュリティインシデントを検知するログ情報源の情報と、セキュリティ対処可能な箇所の対処策とその業務影響の情報とを管理情報として記憶するデータベースと計算機装置を備え、
計算機装置は、新規脅威情報を入手する第１の手段と、前記新規脅威情報と前記システム構成情報から当該新規脅威情報に該当する前記システムを抽出する第２の手段と、抽出した前記システムのシステム構成情報とログ情報源に適合した検知ルールの情報を生成する第３の手段と、当該検知ルールが検知した際の前記対処策の情報を生成する第４の手段と、当該対処策による前記業務影響の情報を生成する第５の手段を備える、ことを特徴とするセキュリティ維持管理支援システム。
【請求項２】
請求項１に記載のセキュリティ維持管理支援システムであって、
対処策の生成および業務影響の情報の生成に際し、事前に整理された対象システムにおいて取りうる対処策とシステムのアプリケーションの影響範囲、影響内容を利用して、当該検知ルールが検知した際の対処策とその業務影響を出力することを特徴とするセキュリティ維持管理支援システム。
【請求項３】
請求項１に記載のセキュリティ維持管理支援システムであって、
前記検知ルールの生成および対処策の生成の際に、ログ発生個所毎に分類し、分類ごとにスクリプトとパラメータを整備し、検知ルールと対処策を生成することを特徴とするセキュリティ維持管理支援システム。
【請求項４】
請求項１に記載のセキュリティ維持管理支援システムであって、
前記検知ルールの生成の生成の際に、脅威情報が分類された脅威識別子とその検知ルール対応表を使って、脅威と検知ルールのデータ源と対象システムの持つログ種別を対応させて、生成する検知ルールを特定することを特徴とするセキュリティ維持管理支援システム。
【請求項５】
請求項１に記載のセキュリティ維持管理支援システムであって、
前記セキュリティ維持対象のシステムと前記計算機装置は、回線接続されておらず、前記セキュリティ維持対象のシステムで収集した前記管理情報が前記計算機装置の前記データベースに記憶されていることを特徴とするセキュリティ維持管理支援システム。
【請求項６】
セキュリティ維持対象のシステムにおけるシステム構成情報と、セキュリティインシデントを検知するログ情報源の情報と、セキュリティ対処可能な箇所の対処策とその業務影響の情報とを管理情報として記憶するデータベースと計算機装置を備え、
前記計算機装置を用いて、新規脅威情報を入手し、前記新規脅威情報と前記システム構成情報から当該新規脅威情報に該当する前記システムを抽出し、抽出した前記システムのシステム構成情報とログ情報源に適合した検知ルールの情報を生成し、当該検知ルールが検知した際の前記対処策の情報を生成し、当該対処策による前記業務影響の情報を生成することを特徴とするセキュリティ維持管理支援方法。
【請求項７】
請求項６に記載のセキュリティ維持管理支援方法であって、
前記セキュリティ維持対象のシステムと前記計算機装置は、回線接続されておらず、前記セキュリティ維持対象のシステムで収集した前記管理情報が前記計算機装置の前記データベースに記憶されていることを特徴とするセキュリティ維持管理支援方法。
【発明の詳細な説明】
【技術分野】
【０００１】

本発明は、情報通信技術を利用したＩＴシステムおよび制御システムにおけるセキュリティ対処を維持管理する業務を支援するセキュリティ維持管理支援システム並びにセキュリティ維持管理支援方法に関する。

【背景技術】

【０００２】

本技術分野の背景技術として、特許文献１に記載の技術がある。特許文献１には、ネットワーク内で発生した攻撃に対するセキュリティ対処案を設計するセキュリティ対処案設計装置であって、攻撃に対するセキュリティ対処案を作成するための対処テンプレートを記憶する対処テンプレート記憶部と、攻撃を検知する攻撃検知装置から、攻撃の検知情報を受信する受信部と、前記対処テンプレート記憶部から、前記検知情報に対応する複数の対処テンプレートを抽出し、当該抽出された複数の対処テンプレート及び前記検知情報に基づいて、前記検知情報からセキュリティ対処案の実行範囲を割り出すことによって複数のセキュリティ対処案を作成し、ネットワーク内の機器情報及びトポロジ情報を参照して、当該作成された複数のセキュリティ対処案の中から実施可能なセキュリティ対処案を抽出する対処案作成部と、前記抽出されたセキュリティ対処案を出力する対処案出力部と、を有することを特徴とする技術が記載されている。

【先行技術文献】

【特許文献】

【０００３】

【特許文献１】特許６６４９２９６号

【発明の概要】

【発明が解決しようとする課題】

【０００４】

回線の接続がない、あるいは、回線の容量が十分でない、あるいは回線の接続が許されない等の理由でネットワークを介したセキュリティ維持管理ができない環境においても、サイバー攻撃への脅威が高まっており、適切にセキュリティの維持管理を行う必要がある。

【０００５】

しかし、特許文献１は、ネットワーク環境下でのセキュリティ対処に留まっており、本発明の課題とする、ローカル環境下の管理対象システムの可用性を保持するセキュリティ対策を維持することは困難であった。

【０００６】

そこで、本発明の目的とするところは、回線接続のない環境下にある多数の管理対象システムに対し、新規脅威情報に対するセキュリティ対策（検知および業務影響を考慮した対処）を支援し得るセキュリティ維持管理支援システムを提供することにある。

【課題を解決するための手段】

【０００７】

以上のことから本発明においては、「セキュリティ維持対象のシステムにおけるシステム構成情報と、セキュリティインシデントを検知するログ情報源の情報と、セキュリティ対処可能な箇所の対処策とその業務影響の情報とを管理情報として記憶するデータベースと計算機装置を備え、計算機装置は、新規脅威情報を入手する第１の手段と、新規脅威情報とシステム構成情報から当該新規脅威情報に該当するシステムを抽出する第２の手段と、抽出したシステムのシステム構成情報とログ情報源に適合した検知ルール情報を生成する第３の手段と、当該検知ルールが検知した際の対処策情報を生成する第４の手段と、当該対処策による業務影響の情報を生成する第５の手段を備える、ことを特徴とするセキュリティ維持管理支援システム」としたものである。

【０００８】

また本発明においては、「セキュリティ維持対象のシステムにおけるシステム構成情報と、セキュリティインシデントを検知するログ情報源の情報と、セキュリティ対処可能な箇所の対処策とその業務影響の情報とを管理情報として記憶するデータベースと計算機装

置を備え、計算機装置を用いて、新規脅威情報を入手し、新規脅威情報とシステム構成情報から当該新規脅威情報に該当するシステムを抽出し、抽出したシステムのシステム構成情報とログ情報源に適合した検知ルール情報を生成し、当該検知ルールが検知した際の対処策情報を生成し、当該対処策による業務影響の情報を生成することを特徴とするセキュリティ維持管理支援方法」としたものである。

【発明の効果】

【０００９】

本発明によれば、回線接続のない環境下にある多数の管理対象システムに対し、新規脅威情報に対するセキュリティ対策（検知および業務影響を考慮した対処）を支援することができる。

【図面の簡単な説明】

【００１０】

【図１】本発明の実施例１に係るセキュリティ維持管理支援システムの全体構成例を示す図。

【図２】管理対象システムの構成例を示す図。

【図３】維持管理支援システムの構成例を示す図。

【図４】セキュリティ維持管理支援機能で実施する概略の処理フロー例を示す図。

【図５】新規脅威に対する脅威判定機能のアルゴリズムフロー例を示す図。

【図６】検知ルール生成機能のアルゴリズムフロー例を示す図。

【図７】対処策生成機能のアルゴリズムフロー例を示す図。

【図８】対処影響算定機能のアルゴリズムフロー例を示す図。

【図９】維持管理支援システムの管理データベースのデータモデルのうち、プラットフォーム部分を詳細化したデータモデル例を示す図。

【図１０】維持管理支援システムの管理データベースのデータモデルのうち、機能部分を詳細化したデータモデル例を示す図。

【図１１】維持管理支援システムの管理データベースのデータモデルのうち、セキュリティ対策部分を詳細化したデータモデル例を示す図。

【図１２】対処場所ごとの対処策を一覧としたデータ例を示す図。

【図１３】各対処策の業務影響の範囲、業務影響内容について、示した内容分類表例を示す図。

【図１４】ＡＴＴ＆ＣＫテクニックと検知ルールの種別の対応表の一部例を示す図。

【図１５】検知ルール種別ごとの検知ルールパラメータの対応表の一部例を示す図。

【図１６】図４の概略処理により生成されるデータ一覧の例を示す図。

【図１７】セキュリティ維持管理支援システムの脅威起点からの画面例を示す図。

【図１８】セキュリティ維持管理支援システムのシステム起点からの画面例を示す図。

【発明を実施するための形態】

【００１１】

以下、図面を用いて本発明の実施例について説明する。なお、実施例により、本発明が限定されるものではない。

【実施例１】

【００１２】

本実施例では、管理対象システムのセキュリティ維持管理のため、管理対象システムのシステム情報、業務情報、セキュリティ対策情報を対応づけて管理し、新規の脅威情報に対して、インシデント検知ルールおよび検知後の対処策、対処策の業務影響を算出・用意することで、各管理対象システムでのセキュリティ対策の更新を支援し、インシデント発生時の対処支援を行う例を説明する。

【００１３】

最初に本発明の実施例１に係るセキュリティ維持管理支援システムの全体構成例について、図１を参照して説明する。

【００１４】

図１に示す本発明の実施例１に係るセキュリティ維持管理支援システム１００は、ローカルに多数ある管理対象システム１１０のセキュリティ維持管理を支援する。

【００１５】

セキュリティ維持担当者Ｍは、複数ある管理対象システム１１０（１１０ａ、１１０ｂ・・・１１０ｍ）を定期的に巡回し、新規脅威に対するセキュリティ対策を反映する業務を行う。このための支援機能をセキュリティ維持管理システム１００が提供する。

【００１６】

図２は、管理対象システム１１０の構成例を示す図である。なおこの場合に、管理対象システム１１０は、回線接続のない環境下にあるシステムであることを前提としている。ここでは、複数の管理対象システム１１０（１１０ａ、１１０ｂ・・・１１０ｍ）の中から、１１０ａの構成例を示している。その他の管理対象システム１１０の構成も同様の構成のものであることから、以下の説明では特に必要がない限り１１０ａを代表例として説明する。

【００１７】

管理対象システム１１０ａは、管理対象部１１１と、バス１１５を介して管理対象部１１１に接続される管理部から構成されており、管理部は管理対象部１１１からのセキュリティアラートやセキュリティログを収集・管理するＳＩＥＭ（Ｓｅｃｕｒｉｔｙ Ｉｎｆｏｒｍａｔｉｏｎ ａｎｄ Ｅｖｅｎｔ Ｍａｎａｇｅｍｅｎｔ）１１２、ＳＩＥＭ１１２からのインシデント検知を受けて、自動対処を支援する自動対処支援装置１１３、管理対象部１１１から管理情報を収集し、セキュリティ検知・対処情報の更新を行う管理情報収集・セキュリティ更新装置１１４から構成されている。

【００１８】

管理対象部１１１は、複数のＩＴ機器や制御機器で構成されるとともに、セキュリティ対策も組み込まれており、セキュリティ対策からのアラートやログがＳＩＥＭ１１２に転送・集約管理される。ＳＩＥＭ１１２は、管理対象部１１１から集約されたアラートやログからインシデントを検知し、自動対処支援装置１１３に通知する。自動対処支援装置１１３は、通知された情報から、事前に定められた対処策を検索し、対処策の影響を評価し、評価により選択された対処策を管理対象システムに適用する。

【００１９】

管理情報収集・セキュリティ更新装置１１４は、定期巡回するセキュリティ維持担当者Ｍにより、新規脅威に対する検知ルールや検知の際の対処策やその影響など、自動対処支援装置１１３が自動対処に必要な情報を更新するとともに、管理対象システムのセキュリティ対策のパラメータや対策情報（シグネチャなど）を更新する。また、管理対象システムのセキュリティを維持するために必要な情報収集も実施する。

【００２０】

この実施例で収集する情報は、システム構成情報（各機器が構成する汎用ソフトウェア情報、ネットワーク情報）、ネットワークトポロジ情報（セグメントやゾーン）、ネットワークセグメント（ゾーン）間の接続情報（ＦＷ設定など）、セキュリティ対策情報（ＩＤＳ／ＩＰＳ（Ｉｎｔｒｕｓｉｏｎ Ｄｅｔｅｃｔｉｏｎ Ｓｙｓｔｅｍ／ Ｉｎｔｒｕｓｉｏｎ Ｐｒｅｖｅｎｔｉｏｎ Ｓｙｓｔｅｍ）、ウィルスワクチン、ホストベースＩＤＳ、ネットワーク異常検知など、各機器が担当する業務（機能）および前提関連業務およびその接続種別である。

【００２１】

また、本実施例で想定している更新するセキュリティ情報は、セキュリティ対策のパラメータや対策情報（シグネチャなど）、ＳＩＥＭ１１２の検知ルール、上記検知ルールが検知した際の対処策、上記対処策を適用した際の管理対象システムへの影響である。

【００２２】

図３は、図１における維持管理支援システム１００の構成例を示す図である。維持管理支援システム１００は、ローカルの複数の管理対象システム１１０（１１０ａ、１１０ｂ・・・１１０ｍ）のセキュリティ管理および保守を支援するセキュリティ維持管理支援装

置１０７、ローカルな管理対象システムの情報を管理するローカルシステム管理データベースＤＢ１、インターネット等を介して接続された外部セキュリティナレッジ等１０６からナレッジ情報を収集し、構造化して管理するナレッジ収集管理装置１０２、セキュリティ維持担当者Ｍが操作し、ローカルの管理対象システム１１０の管理情報を登録・更新するための端末１０３、セキュリティ対処策の業務影響の有無を評価する管理対象システムのテスト環境設備１０４から構成される。

【００２３】

セキュリティ維持担当者Ｍは、端末１０３を用いて、ローカルの管理対象システム１１０から収集したシステム管理情報をローカルシステム管理データベースＤＢ１に登録・更新する。このローカル管理データベースＤＢ１に登録された情報に基づき、セキュリティ維持管理装置１０７は、ナレッジ情報収集管理装置１０２が収集する新規脅威に対し、必要なセキュリティ対策および検知ルール、対処策、その業務影響などを自動的に算出し、更新すべき情報として、管理データベースＤＢ１に登録管理する。

【００２４】

さらに、複数の管理対象システム１１０を巡回するセキュリティ維持担当者Ｍは、前回更新以降に明らかとなった新規脅威に対する更新情報を管理データベースＤＢ１から呼び出し、ローカルの管理対象システムの更新端末１１４により、更新情報を更新し、セキュリティ維持を行う。

【００２５】

以下、セキュリティ維持管理支援装置１００におけるセキュリティ更新情報の自動生成機能について、説明する。図４にセキュリティ維持管理支援装置１００で実施する概略の処理フローの例を示す。

【００２６】

図４のフローにおける最初のステップＳ４００は新規脅威受信機能であり、ナレッジ収集管理装置１０２によりセキュリティ維持管理支援装置１０７が新規脅威を受信したことをトリガーにして図４の以下の処理フローを開始する。あるいは、セキュリティ維持管理支援装置１０７よりナレッジ収集管理装置１０２に新規脅威の有無を問合せ、新規脅威があり、そのその新規重視を入手したことをトリガーにして図４の以下の処理フローを開始する。

【００２７】

ステップＳ４０５は、脅威判定機能であり、ローカルシステム管理データベースＤＢ１を参照してすべての管理対象システム１１０において、当該脅威が存在するか判定する。この詳細を図５により後述する。

【００２８】

ステップＳ４１０は、判定処理機能であり、脅威が存在する管理対象システムがあり、かつ、以下のステップＳ４１５～４２５を未処理の管理対象システム１１０がある場合（ｙｅｓ）、管理対象システム１１０の管理ＩＤ順に特定し、ステップＳ４１５に進む。以下のステップＳ４１５～Ｓ４２５を未処理の管理対象システム１１０がない場合（ｎｏ）は、ステップＳ４５０に進み、一連の処理が完了したので処理ステップを完了する。

【００２９】

ステップＳ４１５は検知ルール生成機能であり、特定された管理対象システム１１０について、当該脅威の検知ルールを生成する。この詳細を図６により後述する。

【００３０】

ステップＳ４２０は、対処策生成機能であり、ステップＳ４１５にて生成された検知ルールが検知された場合の対処策を生成する。この詳細を図７により後述する。

【００３１】

ステップＳ４２５は、対処影響判定機能であり、ステップＳ４２０にて生成された対処策の業務影響を評価する。この詳細を図８により後述する。終了後はステップＳ４１０に戻り、繰り返し処理を実行する。

【００３２】

次に、図４の全体フローの各部処理の詳細について、図５から図８を用いて説明する。まず、図５により新規脅威が管理対象システム１１０の脅威となるか判定するステップＳ４０５の脅威判定機能の詳細アルゴリズムフローを説明する。

【００３３】

脅威判定機能の詳細アルゴリズムフローは、図４の脅威判定機能Ｓ４０５として実行される。このため、ステップＳ４００により、新規脅威情報を受信、あるいは、入手することで、開始する。

【００３４】

ステップＳ４０５ａでは、新規脅威情報に脅威の対象となるソフトウェアが明示されているか確認し、明示されていれば、ステップＳ４０５ｂに進む。

【００３５】

ステップＳ４０５ｅでは、ステップＳ４０５ａと並列に、新規脅威情報に、脅威が使う脆弱性を識別する脆弱性識別情報ＣＶＥが明示されているか確認し、明示されていれば、ステップＳ４０５ｆに進む。

【００３６】

ステップＳ４０５ｂでは、脅威の対象となるソフトウェアをソフトウェア識別名ＣＰＥに変換する。この際、ソフトウェアとソフトウェア識別名ＣＰＥとの対応テーブルなどを利用して変換し、処理後はＳ４０５ｃに進む。

【００３７】

ステップＳ４０５ｆでは、脆弱性識別情報ＣＶＥより、脅威の影響があるソフトウェアのソフトウェア識別名ＣＰＥを脆弱性情報リポジトリ（ＮＶＤ（Ｎａｔｉｏｎａｌ Ｖｕｌｎｅｒａｂｉｌｉｔｙ Ｄａｔａｂａｓｅ）やＪＶＮ（Ｊａｐａｎ Ｖｕｌｎｅｒａｂｉｌｉｔｙ Ｎｏｔｅｓ）データベースＤＢ２の情報から入手し、処理後はステップＳ４０５ｃに進む。

【００３８】

ステップＳ４０５ｃでは、管理対象システム１１０の管理データベースＤＢ１を脆弱性識別情報ＣＰＥで検索し、管理対象システム１１０に脅威が及ぶソフトウェアや脆弱性を持つか確認し、処理後はＳ４０５ｄに進む。

【００３９】

ステップＳ４０５ｄでは、ステップＳ４０５ｃの結果、新規脅威の対象となる管理対象システムのリストを得、処理後は図６のステップＳ４１５に進む。

【００４０】

次に図６を用いて、検知ルール生成機能Ｓ４１５の詳細アルゴリズムフローを説明する。なお図６の処理は、図５のステップＳ４０５ｄより引き継ぐが、図５のステップＳ４０５ｄで得た新規脅威の対象となる管理対象システムのリストがあり、かつ、以下のローがすべてのリストの管理対象システムで処理済みでない場合、以下に続き、そうでない場合、処理を終了する。

【００４１】

図６のステップＳ４１５ａでは、新規脅威情報のＡＴＴ＆ＣＫ脅威識別子に基づき、脅威識別子と検知識別子のマッピングテーブルから、対応する検知識別子を導出し、ステップＳ４１５ｂに進む。

【００４２】

ステップＳ４１５ｂでは、検知識別子ごとに複数の検知ルールパターン（データ源、データ要素）のうち、該当管理対象システム１１０のＳＩＥＭ１１２が収集しているデータ源のログに該当する検知対象ログを複数選定する。

【００４３】

ステップＳ４１５ｃでは、管理データベースＤＢ１を参照して検知ルールパターンのデータ源毎、データ要素毎に従い、システム毎の検知ルールテンプレートをあてはめ、ルールを適用する。ここでデータ源としては、ネットワーク、ファイル操作、コマンド、プロセスが想定され、このためルール生成は、これらデータ源別に行われる。

【００４４】
ステップＳ４１５ｄでは、データ源がネットワークの場合の検知ルール生成を行う。具体的には、通信コンテンツを対象とする場合は、コンテンツ向けに侵害の痕跡ＩＯＣ（Ｉｎｄｉｃａｔｏｒｓ　ｏｆ　Ｃｏｍｐｒｏｍｉｓｅ）を適用する。通信トラフィックの場合は、通信トラフィックに侵害の痕跡ＩＯＣを適用する。トラフィックの場合は、通信元、通信先のＩＰアドレス、ポートの情報に対して、管理対象システムのアウトバウンド、インバウンドの通信方向、および、通信元、通信先ＩＰアドレス範囲（ＣＩＤＲ（Ｃｌａｓｓｌｅｓｓ　Ｉｎｔｅｒ－Ｄｏｍａｉｎ　Ｒｏｕｔｉｎｇ）情報）を検知ルールテンプレートに当てはめて、適用する。その後は、図７のステップＳ４２０ａに進む。
【００４５】
ステップＳ４１５ｅでは、データ源がファイル操作の場合の検知ルール生成を行う。検知の対象となる操作、対象ファイル、対象ディレクトリをパラメータとして、検知ルールの生成をテンプレートに基づいて行う。その後は、図７のステップＳ４２０ｂに進む。
【００４６】
ステップＳ４１５ｆでは、データ源がコマンド操作の場合の検知ルール生成を行う。検知の対象となる操作、対象となるコマンドをパラメータとして、テンプレートに当てはめて適用し、検知ルールを生成する。その後は、図７のステップＳ４２０ｃに進む。
【００４７】
ステップＳ４１５ｇでは、検知ルールがプロセスの場合の検知ルール生成を行う。検知の対象となるプロセス、対象となる動作をパラメータとして、テンプレートに当てはめて適用し、検知ルールを生成する。その後は、図７のステップＳ４２０ｄに進む。
【００４８】
次に図７を用いて、対処策生成機能のアルゴリズムフローを説明する。ここでは図６のデータ源種別に応じた検知ルール生成に応じて、次に当該データ源種別に応じた対処策生成処理を実施する。
【００４９】
ステップＳ４２０ａでは、図６のステップＳ４１５ｄにおけるネットワークの場合の検知ルール生成に続き、ネットワークの検知ルールに対する対応策を生成する。対応策生成は、検知ルールの種別に対し、ログデータ源の機器による検知通信の遮断あるいは、脅威対象の機器への通信の遮断を対処策として生成し、その後ステップＳ４２０ｅに進む。例えばファイアウォールＦＷについてＩＰ／Ｐｏｒｔを遮断することに関して、具体的には例えばＩＰＳについてシグネチャを遮断する。
【００５０】
ステップＳ４２０ｂでは、図６のステップＳ４１５ｅにおけるファイル操作の場合の検知ルール生成に続き、ファイル操作の検知ルールに対する対応策を生成する。対応策生成は、検知ルールのパラメータに対し、当該ファイルの検知動作の権限の制御（操作拒否）を対処策として生成し、その後ステップＳ４２０ｅに進む。ＯＳ権限の制御として、例えばＯＳの再起動／停止を決定し、或はＶＭやコンテナの切り戻しを行う。
【００５１】
ステップＳ４２０ｃでは、図６のステップＳ４１５ｆにおけるコマンド操作の場合の検知ルール生成に続き、コマンド操作の検知ルールに対する対処策を生成する。対処策生成は、検知ルールのパラメータに対し、当該コマンドの検知動作の権限の制御（コマンド実行の拒否）を対処策として生成し、その後ステップＳ４２０ｅに進む。ＯＳ権限の制御として、例えばＯＳの再起動／停止を決定する。
【００５２】
ステップＳ４２０ｄでは、図６のステップＳ４１５ｇにおけるプロセスの場合の検知ルール生成に続き、プロセスの検知ルールに対する対処策を生成する。対処策生成は、検知ルールのパラメータに対し、当該プロセスの停止、プロセスの実行ファイルの権限の制御（実行の拒否）を対処策として、生成し、その後ステップＳ４２０ｅに進む。プロセスの停止、プロセスの実行ファイルの権限の制御としては、例えばＯＳのプロセス停止、再起

動または権限制御、停止を行う。

【００５３】

ステップＳ４２０ｅでは生成した検知ルール・対処策を該当の管理システムの検知ルール・対処策として、登録し、その後図８のステップＳ４２５へ進む。

【００５４】

次に図８を用いて、対処影響算定機能Ｓ４２５の詳細アルゴリズムフローを説明する。図８の最初のステップＳ４２５ａでは、ステップＳ４２０で取得した対処策案に対して、直接の影響範囲、想定影響を検索する。当該機器の機能の前提となる通信（ポート）、ファイル権限、コマンド権限、前提プロセスなどを検索により特定し、影響の有無を特定する。

【００５５】

ステップＳ４２５ｂでは、間接の影響範囲、想定影響を明確化する。影響のある機能の利用が前提となる他の機能を特定し、特定した他の機能とステートフルな連携であれば、直接影響と同等の影響、ステートレスな連携であれば、連携機能のみの影響として抽出する。

【００５６】

ステップＳ４２５ｃでは、算定した対処案の影響を、管理データベースＤＢ１に登録する。これらのフローを、導出したすべての対処案に対し実施し、管理データベースＤＢ１に登録する。

【００５７】

次に図９～図１１を用いて、維持管理支援システムのデータベースのデータモデルについて説明する。図９はプラットフォーム名部分を詳細化したデータモデル１、図１０は機能名部分を詳細化したデータモデル２、図１１はセキュリティ対策名部分を詳細化したデータモデル３の例を示してる。

【００５８】

図９～図１１の維持管理支援システムにおける管理データベースＤＢ１の主要項目は以下のようである。

データ９００（管理対象システムＩＤ）：管理対象システムを一意に特定する識別子

データ９１０（管理対象システム名）：管理対象システムの名前

データ９２０（システム種別）：管理対象システムの種別（管理対象システムの機能特徴による分類。例えば、Ｗｅｂシステム、組立ラインシステムなど）

データ９３０（その他情報）：管理対象システムについての管理情報。例えば、管理者や連絡先、所在地、営業担当など）

データ９４０（プラットフォーム名）：管理システムにある計算機ＰＦの名前（共用計算機、特定業務専用機など）

データ９６０（機能名）：管理対象システムの持つ機能（ＩＣＴを利用した）の名称。

データ９８０（管理対象システムのセキュリティ対策名）：管理対象システムのセキュリティ対策の名称

図９のプラットフォーム名部分を詳細化したデータモデル１についての項目は以下のとおりである。

データ９４１（プラットフォーム名９４０のタイプ）：プラットフォームのタイプ。例えば、フィジカルマシン（ＰＭ）／仮想マシン（ＶＭ）／コンテナ（ＣＭ）。

データ９４２（プラットフォーム名９４０のハードウェア）：プラットフォームが搭載されているハードウェア機種名および形式番号

データ９４３（プラットフォーム名９４０のＯＳ）：プラットフォームに稼働させているＯＳ

データ９４４（プラットフォーム９４０に搭載されるソフトウェア情報）：パッケージソフト構成（含むＫＶＭ等の仮想化ソフトやＤｏｃｋｅｒ等のコンテナソフト）やそのＣＰＥ情報

データ９４５（プラットフォーム９４０のＮＩＣ情報）：すべてのネットワークアダプタ

のＭＡＣアドレスやＩＰアドレス）
データ９４６（プラットフォーム９４０の脆弱性）：プラットフォームが持つ脆弱性（ＣＶＥ他）
データ９４７（プラットフォーム９４０で取りうる対処策）：プラットフォームで取りうる対処策
データ９５０（プラットフォーム９４０で取りうる対処策９４７の業務影響）：前述９４７の対処策での業務影響
図１０の機能名部分を詳細化したデータモデル２についての項目は以下のとおりである。
データ１０１０（機能９６０との連携機能）：機能９６０が連携する他の（管理対象システム内の）機能
データ１０１１（上記連携機能１０１０の連接状況）：連携機能の本機能９６０との連接状況がステートレスかステートフルかを示す。
データ１０２０（機能９６０の役割）：各機能の役割
データ１０３０（機能９６０のベースシステム）：機能が搭載されいているベース（プラットフォーム）システム（専用ハード、仮想マシンＶＭ、コンテナＣＭ、共用ハード）
データ１０４０（機能９６０が使うＮＩＣ情報）：例えば、ＶＬＡＮ　ｔａｇ、ＩＰアドレス、ＭＡＣ
データ１０５０（機能９６０が載っているＯＳ）：機能を実行しているＯＳ
データ１０６０（機能９６０を実行するためのソフトウェアおよびそのＣＰＥ）：機能を実行するためのソフトウェア（汎用ミドルウェアやライブラリ）、あるいは、そのＣＰＥ情報
データ１０７０（機能９６０が提供するサービス）：ＡＰＩ名やＵＲＬ、利用ポート
データ１０８０（機能９６０が持つ脆弱性）：機能のＯＳやソフトウェアが持つ脆弱性（ＣＶＥ他）
データ１０９０（機能９６０にて取りうる対処策）：機能で取りうる対処策
データ１０９１（機能９６０に取りうる対処策１０９０の業務影響）：上記対処策策１０９０での業務影響
図１１のセキュリティ対策名部分を詳細化したデータモデル３についての項目は以下のとおりである。
データ１１１０（セキュリティ対策９８０のベースシステム）：セキュリティ対策の装備機器（ＰＦあるいは専用ハード、専用アプライアンス）
データ１１２０（セキュリティ対策９８０が使うＮＩＣ情報）：例えば、ＶＬＡＮ　ｔａｇ、ＩＰアドレス、ＭＡＣ
データ１１３０（セキュリティ対策９８０が載っているＯＳ）：セキュリティ対策を実行しているＯＳ
データ１１４０（セキュリティ対策９８０を実行するためのソフトウェアおよびそのＣＰＥ）：セキュリティ対策を実行するためのソフトウェア（汎用ミドルウェアやライブラリ）、あるいは、そのＣＰＥ情報
データ１１５０（セキュリティ対策９８０に適用している検知ルールあるいはシグネチャ、設定情報）：セキュリティ対策９８０が装備している検知ルールあるいはシグネチャ、設定情報など
データ１１５１（上記検知ルール等１１５０の対処策）：セキュリティ対策で可能な対処策
データ１１６１（上記対処策１１５１を適用した際の業務影響）：上記対応策での業務影響
次に図１２を用いて、各対処場所における取りうる対処策とその業務影響の情報の例について説明する。図１２の縦方向には、対処場所Ｄ１１の例として、機能を実装したＯＳでの対応Ｄ１１ａ、ＰＦでの対応Ｄ１１ｂ、ＮＷ（Ｓｗｉｔｃｈ）での対応Ｄ１１ｃ、ＥＰ（ＨＩＤＳ）での対応Ｄ１１ｄ、ＩＤＳ／Ｐでの対応Ｄ１１ｅを示している。また、横

方向には、対処場所Ｄ１１、対処策Ｄ１２、検知データ群Ｄ１３、実施パラメータＤ１４の例を示している。

【００５９】

また図１２には、対処策Ｄ１２として、機能で取りうる対処策１０９０（図１０）、プラットフォームで取りうる対処策９４７（図９）、セキュリティ対策で取りうる対処策１１５１（図１１）の例を示している。

【００６０】

機能が取りうる対処策１０９０（図１０）として、プロセスの停止／再起動、ポートフィルタリング、ＩＰフィルタリング、ファイル削除、ファイル権限の変更などが考えられる。それぞれ、検知ルールの適用データ源Ｄ１３により、対処の実施パラメータＤ１４が抽出され適用される。

【００６１】

検知ルールデータ源Ｄ１３は、プロセス（ＯＳの通信ログ：ｉｐｔａｂｌｅｓの出力等を含む）、ファイル（ファイルアクセスログ：ａｕｄｉｔの出力ログ等を含む）、ＮＷ（ネットワークＳｗｉｔｃｈのログ）、セキュリティ対策（ホストベース侵入検知ＨＩＤＳやエンドポイントプロテクションＥＰ：ウィルスワクチン含む、ネットワークベース侵入検知／防止ＩＤＳ／ＩＤＰのログから実施パラメータを抽出し、対処策を適用できるようスクリプトなど用意する。

【００６２】

図１３に上記対処策（１０９０、９４７、１１５１）の業務影響９５０、１０９１、１１６１の内容の例を示す。

【００６３】

機能が取りうる対処策１０９０やプラットフォームが取りうる対処策９４７、セキュリティ対策機能が取りうる対処策１１５１によって、影響範囲が異なり、また対処策によっても影響範囲が異なる。このため、当該対処策による影響範囲をあらかじめ明らかにする。さらに、その影響内容種別についても、機能停止、サービス停止、再起動、副系切り替え、応答遅延、影響なしをそのパラメータ（再起動時間、遅延時間、応答劣化率等）と合わせて、明確化されて定義される。

【００６４】

図１２と図１３はデータモデル（図９－１１）とは別に定義しておき、処理フローにおいて、対処策の生成（図７）、業務影響の判定（図８：８１０）に利用される。

【００６５】

図１４は、脅威情報の脅威テクニック種別の識別子と検知ルールの分類を示す。新規脅威情報にて分類された脅威テクニック種別を起点に検知ルールを生成するログデータ源と検知対象のデータ内容を確定するため、この表を用いる。

【００６６】

図１５に検知ルールの生成のための表を示す。図１４のログデータ源とコンテンツに基づき、ログデータに対する検知ルールを生成する。具体的には脅威のある端末への通信に対して、特定のポートの通信を検知したり、通信データのコンテンツに関わる文字列の合致により検知を行ったり、脅威のある端末の特定のファイルへのアクセスや書き込みを検知したり、特定のコマンドの実行を検知したり、プロセスの起動等を検知したり、通信プロセスの受信を検知する検知ルールの生成を行う。

【００６７】

図１６に検知ルール毎に生成した情報を示す。図４の処理の結果、図１６が生成される。この生成のために、図１２～図１５のデータがあらかじめ、対象システムごとに整備されており、このデータを利用して、セキュリティインシデントが検知された際の取りうる対処策とその業務影響を整備することで、各システムが稼働している現場において、セキュリティ専門家が不在な状況でも適切な対処を選択することが可能となる。

【００６８】

図１７にセキュリティ維持管理支援システムの脅威起点の画面例を示す。脅威起点の画

面委は、脅威一覧が表示され、一覧で指定された脅威情報を表示するとともに、脅威が対象となるシステムを一覧表示できる。当該一覧から指定されたシステム向けに生成された検知ルールの一覧と、当該一覧で指定された検知ルールの説明と対処策の一覧と、当該対処策の一覧で指定された対処策の説明と対処策の業務影響が表示でき、生成結果を確認できる。

【００６９】

図１８にセキュリティ維持管理支援システムのシステム起点の画面例を示す。システム起点の画面にはシステム一覧から指定されたシステムに特定された脅威情報の一覧が紐づけて表示でき、さらに当該一覧に指定した脅威の説明が表示でき、さらに当該指定した脅威についてのシステムでの検知ルール一覧と、当該一覧から指定された検知ルールの説明とその対処策一覧と、当該一覧から指定された対処策の説明とその対処策の業務影響が表示できる。

【００７０】

また、対象脅威についてのセキュリティ維持管理情報を脅威情報一覧より指定でき、当該指定された脅威について、システムに反映するためにセキュリティ維持管理情報をタウンロードして出力し、対象システムのセキュリティ維持情報として、反映することができる。

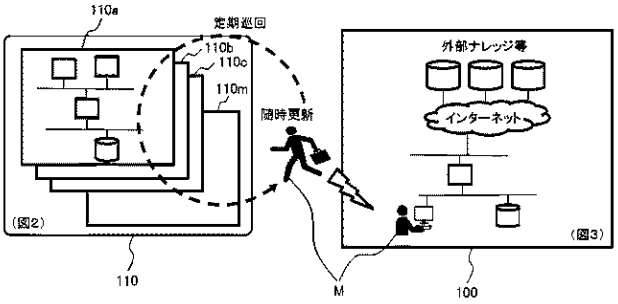
【符号の説明】

【００７１】

１００：セキュリティ維持管理支援システム
１０２：ナレッジ収集管理装置
１０３：端末
１０４：テスト環境設備
１０６：外部セキュリティナレッジ等
１０７：セキュリティ維持管理支援装置
１１０（１１０ａ、１１０ｂ・・・１１０ｍ）：管理対象システム
１１１：管理対象部
１１２：ＳＩＥＭ
１１３：自動対処支援装置
１１４管理情報収集・セキュリティ更新装置
１１５：バス
ＤＢ１：ローカルシステム管理データベース
Ｍ：セキュリティ維持担当者

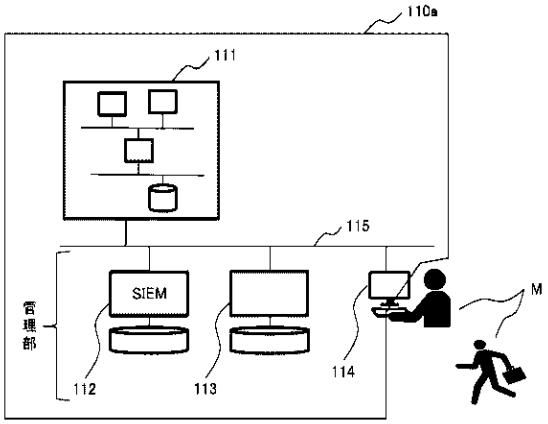
【図１】

図 1



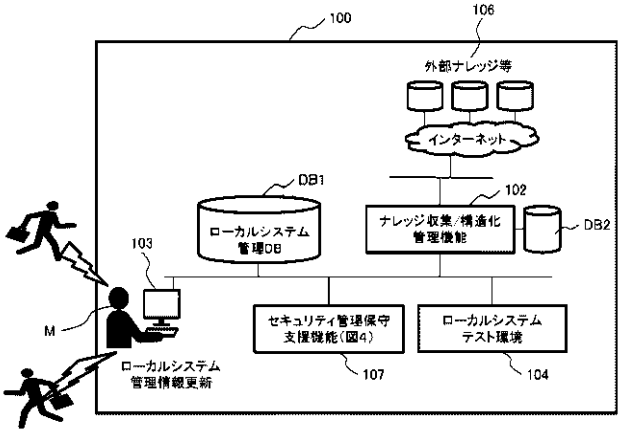
【図２】

図 2



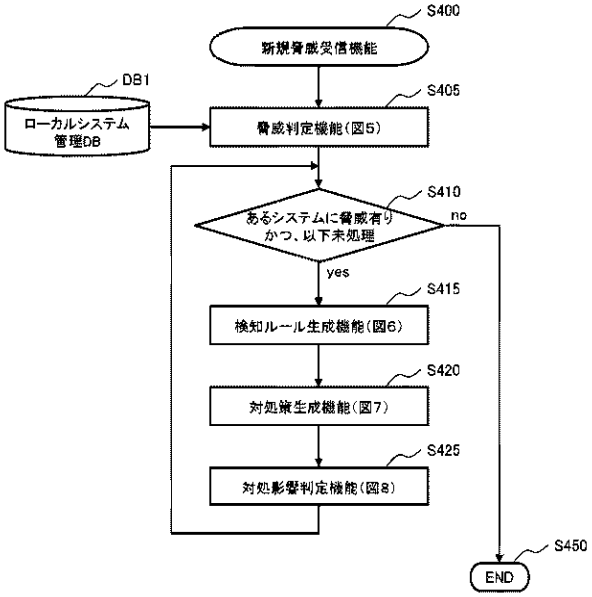
【図３】

図 3



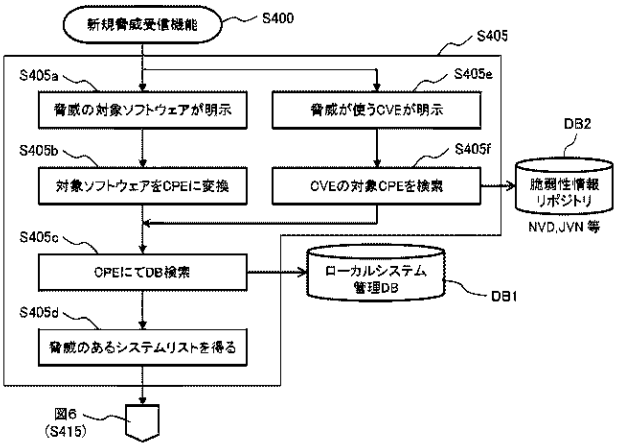
【図４】

図 4



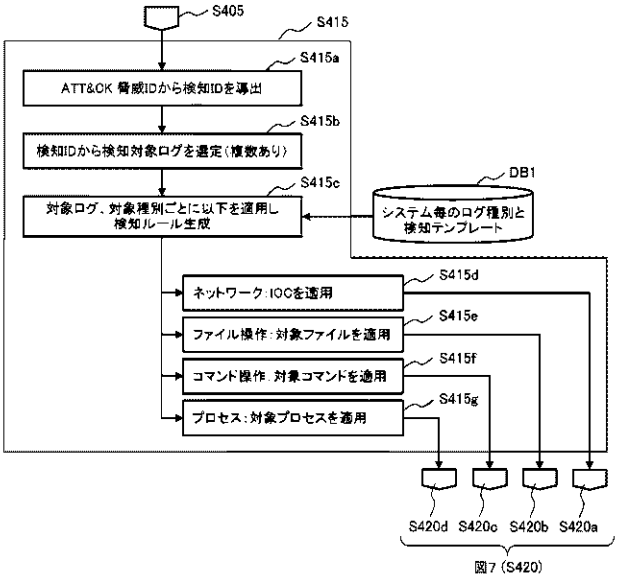
【図５】

図 5



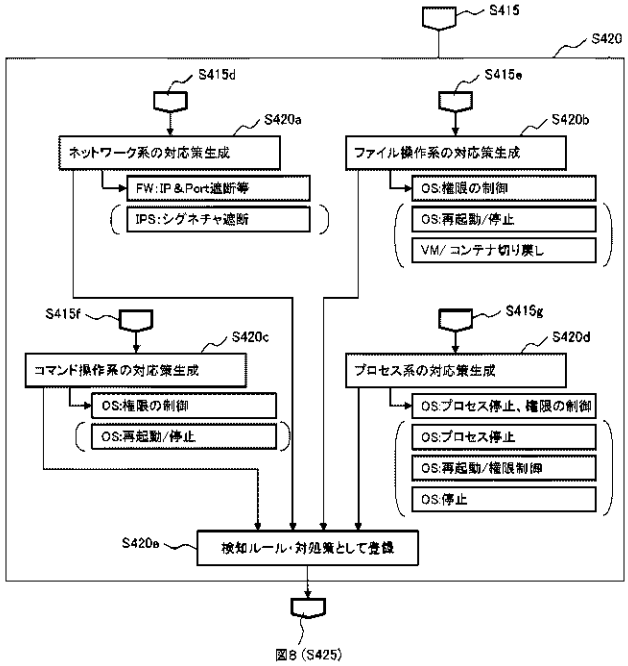
【図６】

図 6



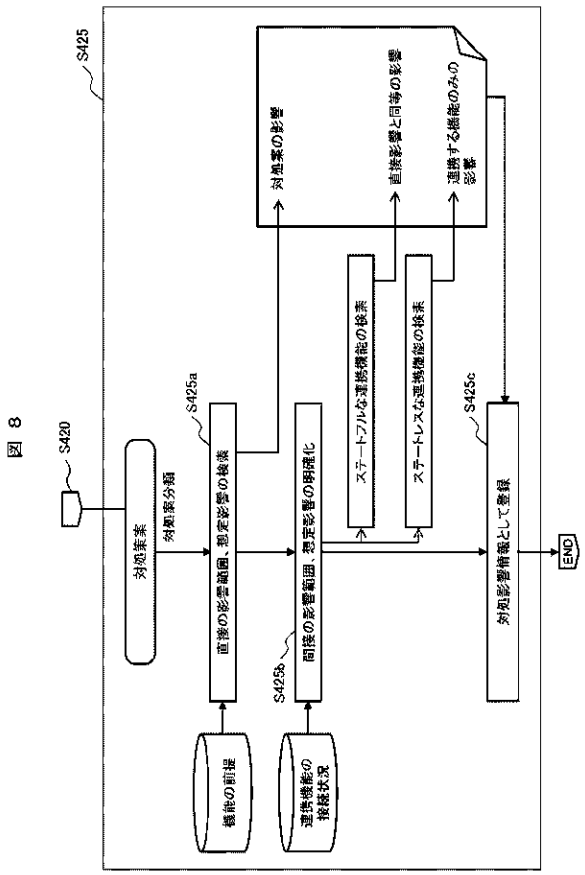
【図７】

図 7



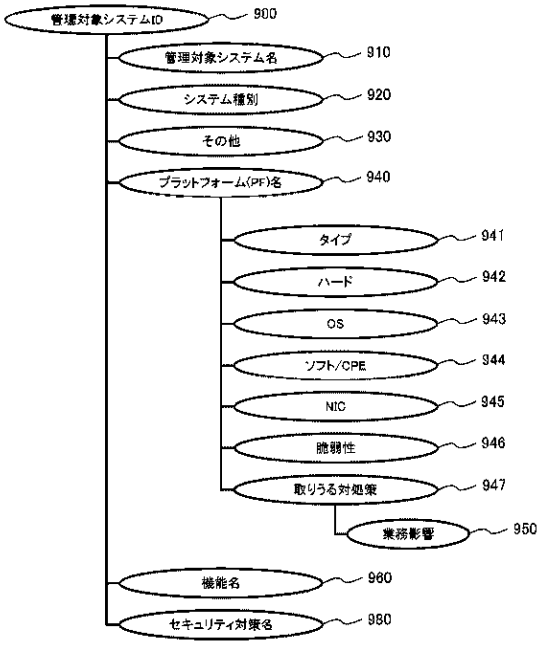
【図８】

図 8



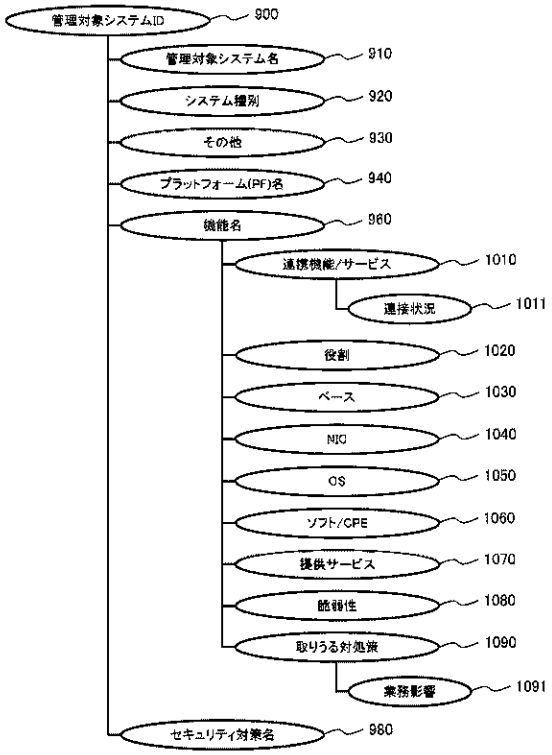
【図９】

図 9



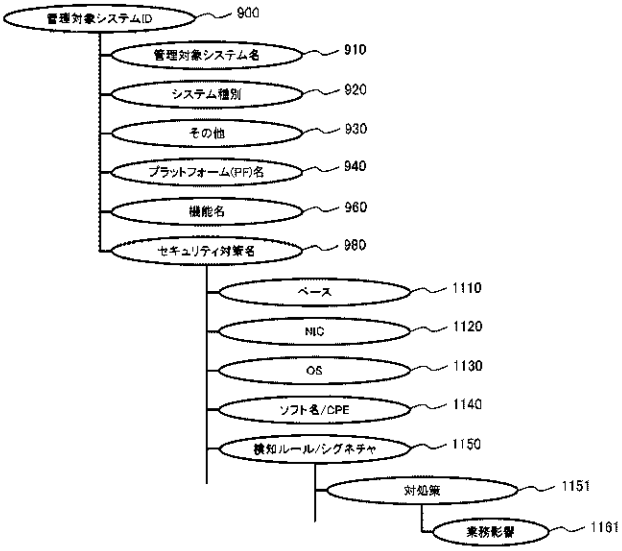
【図１０】

図 10



【図１１】

図 11



【図１２】

図 12

	D11 対処場所	D12 対処策		D13 検知データ源	D14 実施パラメータ
D11a	機能を実装したOSでの対応	プロセスの停止/再起動		プロセス	対象OSのIP、プロセスID
		iptablesによるポートフィルタ設定		プロセス	対象OSのIP、ポートID
		iptablesによる通信先フィルタ設定	1090	プロセス	対象OSのIP、通信先IP
		ファイルの削除		ファイル	対象OSのIP、ファイル名
		ファイルの権限変更		ファイル	対象OSのIP、ファイル名
D11b	PFでの対応	コンテナOSの停止/再起動		プロセス	対象コンテナのIP、コンテナID
		仮想VMの停止/再起動	947	プロセス	対象VMのIP、VM名
		PFのOSの停止/再起動		プロセス	対象PFOSのIP(ホスト名)
		NWブリッジの設定変更(IP/ポートフィルタリング)		プロセス	対象PFOSと対象コンテナのIP
D11c	NW(Switch)での対応	あて先毎のフィルタIP設定		NW	あて先IP
		あて先毎のフィルタポート設定		NW	あて先ポートID
		該当マシンの隔離/バックアップ切り替え	1151	NW	隔離IP
D11d	EP(HIDS)での対応	検疫		EP	ファイル名
		改ざんファイルのバックアップとのリプレース		ファイル	対象ファイル名、バックアップファイル名
D11e	IDS/IPでの対応	アプリレベルのフィルタリング(例:AP通信のID)		NW-AP	フィルタリングするAPP通信特徴
		フィルタリングシグネチャの追加		NW-AP	シグネチャ

【図１３】

図 13

	対応策種別	影響範囲	影響内容
1090	機能が動くOSで取る対処策	影響機能/影響サービス	下表のどれか
947	プラットフォームが取る対処策	影響PF/影響機能/影響サービス	
1151	セキュリティ対策機能が取る対処策	影響PF/影響機能/影響サービス	

影響内容種別	パラメータ	説明	影響時間
機能停止	---	該当の機能停止	根本対策まで復帰なし
サービス停止	---	機能は継続	同上
再起動	再起動時間	機能復帰までの時間	単位は秒
副系切替	遅延時間	応答遅延する時間	単位は秒
応答遅延	応答劣化率	レスポンス低下率	単位はパーセント
影響なし	ー	ー	ー

【図１４】

図 14

Technique		ID	Data Source	Data Component
T1190	Exploit Public-Facing Application	DS0015	Application Log	Application Log Content
		DS0029	Network Traffic	Network Traffic Content
T1100	Web Shell	DS0015	Application Log	Application Log Content
		DS0022	File	File Creation
				File Modification
		DS0029	Network Traffic	Network Traffic Content
				Network Traffic Flow
		DS0009	Process	Process Creation
T1215	Kernel Modules and Extensions	DS0017	Command	Command Execution

【図１５】

図 15

#	ログデータ源		説明	パラメータ	
1	ネットワーク	IP層	IP/Port、通信向きに関する検知ルール	IP/Port、向き	
		AP層	APレイヤの通信内容に関する検知ルール	Web	URL/Method
				AP	通信パタン(文字列)
2	ファイル		ファイル操作に関する検知ルール	ファイル名	
3	プロセス		プロセスに関する検知ルール	プロセス名	
			通信プロセスに関するIP/Port、通信向きに関する検知ルール	IP/Port、向き	
4	コマンド		コマンドに関する検知ルール	コマンド名	

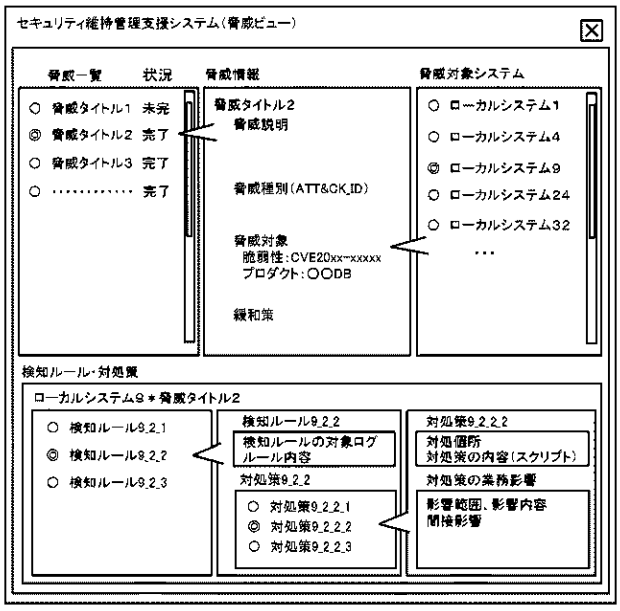
【図１６】

図 16

#	項目	説明
1601	検知ルールID	検知ルール識別子
1602	検知ルール種別	検知ルールの種別(NW、ファイル、コマンド、プロセス)
1603	検知ルール	検知ルールの内容
1604	検知ルールの対象脅威識別子	検知対象の脅威ID。ATT&CKテクニカルID等で識別
1605	検知ルールの対象脅威明	検知対象の脅威名。脅威の説明
1606	検知ルールの脅威の対象脆弱性	検知対象の脅威が使う脆弱性の識別子。CVE等で識別
1611	検知ルールの対処策ID	検知ルールが検知した際の対処策
1612	対処策	対処策の内容(検知ルールのパラメータを利用)
1621	対処策の業務影響	影響範囲と影響内容

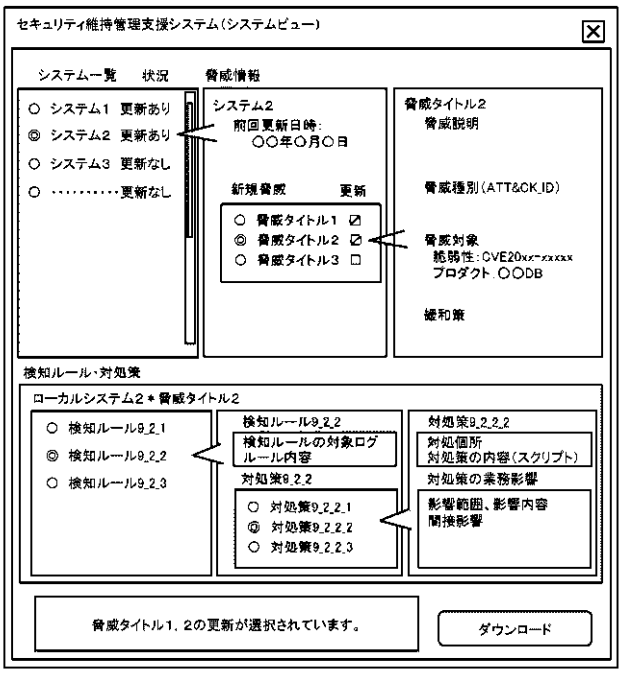
【図１７】

図 17



【図１８】

図 18



フロントページの続き

(72)発明者　橋本　孝紀
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