(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第6463661号
(P6463661)
(45)発行日　平成31年2月6日(2019.2.6)　(24)登録日　平成31年1月11日(2019.1.11)

(51)Int.Cl.　F I
H04L 12/70 (2013.01)　H04L 12/70 100Z

請求項の数 14　(全 35 頁)

(21)出願番号　特願2015-187715(P2015-187715)
(22)出願日　平成27年9月25日(2015.9.25)
(65)公開番号　特開2017-63336(P2017-63336A)
(43)公開日　平成29年3月30日(2017.3.30)
審査請求日　平成29年11月17日(2017.11.17)

(73)特許権者　000233491
株式会社日立システムズ
東京都品川区大崎一丁目２番１号
(74)代理人　110000176
一色国際特許業務法人
(72)発明者　来間　一郎
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　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　吉田　智仁
東京都品川区大崎一丁目２番１号　株式会社日立システムズ内

最終頁に続く

(54)【発明の名称】ネットワーク制御装置、及びネットワーク制御方法

(57)【特許請求の範囲】
【請求項１】
機能の異なるネットワーク機器を含んで構成されるネットワークを制御する装置であって、
前記ネットワーク機器の機能に関する情報であるネットワーク機器情報を記憶するネットワーク機器情報記憶部と、
前記ネットワークにおいて発生したインシデントに対する対処方針に関する情報である対処方針情報を記憶する対処方針情報記憶部と、
前記ネットワーク機器情報及び前記対処方針情報に基づき、前記インシデントに対処するための前記ネットワーク機器の設定に関する情報である設定情報を一つ以上生成する対処設定情報生成部と、
を備え、
前記対処設定情報生成部は、前記設定情報の生成に際し、発生したインシデントに関する情報であるインシデント情報を前記対処方針と対応づけることにより、前記インシデントに対する対処の方法に関する情報である対処方法を一つ以上生成し、
前記対処方法は、前記ネットワーク機器間で送受信されるパケットの送信元と受信先を特定する情報を含み、
前記対処設定情報生成部は、前記設定情報の生成に際し、前記送信元から前記受信先に至る経路である対処経路を一つ以上探索し、
前記対処方針は、前記ネットワークを流れるパケットに加える更新処理を指定する情報

を含み、
前記対処設定情報生成部は、前記設定情報の生成に際し、前記対処経路上の前記ネットワーク機器への前記更新処理の割り当てである対処処理配置を、前記ネットワーク機器情報に基づき可能な割り当て方の組み合わせを探索して一つ以上生成し、
前記対処方針情報は、前記対処処理配置と前記対処経路との対応を示す情報、前記対処経路と前記対処方法との対応を示す情報、前記対処方針と前記対処方法との対応を示す情報、及び前記インシデントに対する対処の目的を示す情報である対処目的と前記対処方針との対応を示す情報を含み、
前記対処設定情報生成部は、前記対処目的ごとに対応する前記対処処理配置を選択することにより生成される情報である対処候補を一つ以上生成する、
ネットワーク制御装置。
【請求項２】
請求項１に記載のネットワーク制御装置であって、
前記対処方針は、前記ネットワークを流れるパケットに加える更新処理を指定する情報を含み、
前記対処設定情報生成部は、前記設定情報の生成に際し、前記更新処理と前記ネットワーク機器情報とを対照することにより前記対処候補を実現可能か否かを判定する
ネットワーク制御装置。
【請求項３】
請求項１に記載のネットワーク制御装置であって、
前記対処方針の夫々について設定された優先度を記憶し、
前記対処設定情報生成部は、前記優先度に基づき前記対処候補の優先度を求める
ネットワーク制御装置。
【請求項４】
請求項３に記載のネットワーク制御装置であって、
前記対処方針の夫々ついて一つ以上の評価項目と前記評価項目の夫々の優先度を記憶し、
前記対処設定情報生成部は、前記評価項目の夫々の前記優先度に基づき前記対処候補の前記優先度を算出する
ネットワーク制御装置。
【請求項５】
請求項１に記載のネットワーク制御装置であって、
前記対処設定情報生成部は、前記対処目的の夫々について優先度を記憶し、前記優先度に基づき前記対処候補の優先度を求める
ネットワーク制御装置。
【請求項６】
請求項１に記載のネットワーク制御装置であって、
前記対処処理配置の夫々について優先度の算出手順を記憶し、
前記対処設定情報生成部は、前記算出手順に従い前記対処処理配置の夫々の優先度を求め、求めた前記優先度に基づき前記対処候補の優先度を求める
ネットワーク制御装置。
【請求項７】
請求項１に記載のネットワーク制御装置であって、
前記対処方針の夫々について設定された優先度である対処方針評価スコアを記憶し、
前記対処目的の夫々について設定された優先度である対処目的評価スコアを記憶し、
前記対処処理配置の夫々について設定された優先度である対処処理配置評価スコアを記憶し、
前記対処設定情報生成部は、前記対処方針評価スコア、対処目的評価スコア、及び対処処理配置評価スコアに基づき、前記対処候補の優先度である対処候補評価スコアを求める、

ネットワーク制御装置。
【請求項８】
機能の異なるネットワーク機器を含んで構成されるネットワークを制御するネットワーク制御装置が、
前記ネットワーク機器の機能に関する情報であるネットワーク機器情報を記憶する処理と、
前記ネットワークにおいて発生したインシデントに対する対処方針に関する情報である対処方針情報を記憶する処理と、
前記ネットワーク機器情報及び前記対処方針情報に基づき、前記インシデントに対処するための前記ネットワーク機器の設定に関する情報である設定情報を一つ以上生成する処理と、
前記設定情報の生成に際し、発生したインシデントに関する情報であるインシデント情報を前記対処方針と対応づけることにより、前記インシデントに対する対処の方法に関する情報である対処方法を一つ以上生成する処理と、
前記設定情報の生成に際し、前記ネットワーク機器間で送受信されるパケットの送信元から受信先に至る経路である対処経路を一つ以上探索する処理と、
前記設定情報の生成に際し、前記ネットワークを流れるパケットに加える更新処理の前記対処経路上の前記ネットワーク機器への割り当てである対処処理配置を、前記ネットワーク機器情報に基づき可能な割り当て方の組み合わせを探索して一つ以上生成する処理と、
前記対処方針情報として、前記対処処理配置と前記対処経路との対応を示す情報、前記対処経路と前記対処方法との対応を示す情報、前記対処方針と前記対処方法との対応を示す情報、及び前記インシデントに対する対処の目的を示す情報である対処目的と前記対処方針との対応を示す情報を記憶する処理と、
前記対処目的ごとに対応する前記対処処理配置を選択することにより生成される情報である対処候補を一つ以上生成する処理と、
を実行する、
ネットワーク制御方法。
【請求項９】
請求項８に記載のネットワーク制御方法であって、
前記対処方針は、前記ネットワークを流れるパケットに加える更新処理を指定する情報を含み、
前記ネットワーク制御装置が、前記設定情報の生成に際し、前記更新処理と前記ネットワーク機器情報とを対照することにより前記対処候補を実現可能か否かを判定する処理
を更に実行する、ネットワーク制御方法。
【請求項１０】
請求項８に記載のネットワーク制御方法であって、
前記ネットワーク制御装置が、
前記対処方針の夫々について設定された優先度を記憶する処理と、
前記優先度に基づき前記対処候補の優先度を求める処理と、
を更に実行する、ネットワーク制御方法。
【請求項１１】
請求項１０に記載のネットワーク制御方法であって、
前記ネットワーク制御装置が、
前記対処方針の夫々ついて一つ以上の評価項目と前記評価項目の夫々の優先度を記憶する処理と、
前記評価項目の夫々の前記優先度に基づき前記対処候補の前記優先度を算出する処理と、
を更に実行する、ネットワーク制御方法。
【請求項１２】

請求項８に記載のネットワーク制御方法であって、
前記ネットワーク制御装置が、前記対処目的の夫々について優先度を記憶し、前記優先度に基づき前記対処候補の優先度を求める処理
を更に実行する、ネットワーク制御方法。
【請求項１３】
請求項８に記載のネットワーク制御方法であって、
前記対処処理配置の夫々について優先度の算出手順を記憶し、
前記ネットワーク制御装置が、前記算出手順に従い前記対処処理配置の夫々の優先度を求め、求めた前記優先度に基づき前記対処候補の優先度を求める処理
を更に実行する、ネットワーク制御方法。
【請求項１４】
請求項８に記載のネットワーク制御方法であって、
前記ネットワーク制御装置が、
前記対処方針の夫々について設定された優先度である対処方針評価スコアを記憶する処理と、
前記対処目的の夫々について設定された優先度である対処目的評価スコアを記憶する処理と、
前記対処処理配置の夫々について設定された優先度である対処処理配置評価スコアを記憶する処理と、
前記対処方針評価スコア、対処目的評価スコア、及び対処処理配置評価スコアに基づき、前記対処候補の優先度である対処候補評価スコアを求める処理と、
を更に実行する、ネットワーク制御方法。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワーク制御装置、及びネットワーク制御方法に関する。
【背景技術】
【０００２】
特許文献１には、「ＶＬＡＮ機能を有するレイヤー２スイッチを備えたネットワークを対象として検疫処理を行う検疫装置であって、前記レイヤー２スイッチの特定のポートに、ＶＬＡＮ機能を有していない集線装置を介して、１台の端末が接続されている場合に、前記集線装置への新たな端末の接続を検出する、端末検出部と、前記新たな端末の接続が検出された場合に、前記特定のポートをトランクポートに設定し、更に、前記特定のポートに、設定されたタグが付加されたイーサーネット（登録商標）フレームのみを転送する第１のＶＬＡＮ、及び前記タグが付加されていないイーサーネット（登録商標）フレームのみを転送する第２のＶＬＡＮを設定する、スイッチ制御部と、を備えている。」と記載されている。
【先行技術文献】
【特許文献】
【０００３】
【特許文献１】特開２０１２－０８０２１６号公報
【発明の概要】
【発明が解決しようとする課題】
【０００４】
情報通信機器の普及に伴い、サイバー攻撃の多様化／複雑化が進んでいる。とくに標的型攻撃と呼ばれるタイプの攻撃は、従来の愉快犯的な無差別攻撃と異なり明確な目的を持ち、特定の個人や組織を標的として情報の窃取や改竄等を行う。昨今、政府機関や企業等を対象とした標的型攻撃による被害が実際に発生しており、社会問題となっている。
【０００５】
標的型攻撃の一例を以下に述べる。攻撃者は、まずメールへの添付やＷｅｂサイトから

のダウンロード等の手法を利用し、標的となるクライアント端末にマルウェアを侵入させる。クライアント端末に侵入したマルウェアは、当該クライアント端末が接続するネットワークの調査、攻撃者が用意した外部Ｃ＆Ｃ（Command and Control）サーバからの新たなマルウェアのダウンロードによる攻撃機能の補強等の各種の動作を行う。そして攻撃者は、最終的にマルウェアを介して標的とする情報や資産性の高い情報にアクセスし、窃取や改竄等を行う。

【０００６】

こうした標的型攻撃に対しては、例えば、「ネットワーク上でのマルウェアの活動を検知し対処する」、「マルウェアが機密情報を外部に送信するのを防ぐ」といった複数のセキュリティ対策を組み合わせた多重防御が有効とされている。上記のような対策を施し、ネットワークにマルウェアが侵入し活動している兆候をインシデントとして検知した場合、ネットワークに設けられた防御システムは、例えば、次のように対処する。

【０００７】

まず上記防御システムは、証拠保全や他の装置へ攻撃を防ぐこと等を目的として、マルウェアに感染している可能性のある端末を本番系のネットワークから切り離して調査環境に置き、当該端末を調査する。調査によりマルウェアを特定すると、上記防御システムは、マルウェアの活動履歴を取得するとともに感染端末からマルウェアを除去し、マルウェアの活動内容を出力する。マルウェアの存在を知った管理者は、クリーンな端末をネットワークに再接続する等の対応をとる。

【０００８】

ここでこうした対処を迅速かつ効率的に行うためには、予めインシデントの状況に応じた対処方針を用意しておき、対処方針に基づく隔離及び調査に必要な通信経路の設定をネットワークの制御により一括して行うことが有効である。尚、上記対処方針には、例えば、マルウェア感染端末とネットワーク内の他の機器との全ての通信の遮断、マルウェア感染端末とネットワーク内の他の機器との一部の通信の遮断、マルウェア感染端末を遠隔から詳細に調査するためのログイン経路の確立、マルウェア感染端末が送受信するパケットの取得経路の確立、マルウェア感染端末の挙動を観察するためのダミーサーバへの通信経路の確立等がある。

【０００９】

但し、ネットワークを構成している機器の種類は様々であるため、その機能や配置形態によっては上記のような対処を全て実施できるとは限らない。例えば、リピータハブのような従来（レガシー）タイプの機器は、ＡＣＬ（Access Control List）による各種制御機能やＶＬＡＮ（Virtual Local Area Network）等の機能を備えていない。また昨今、注目されているＳＤＮ（Software-Defined Networking）技術に対応したネットワーク機器は、従来のネットワーク機器よりも柔軟にパケット制御方法を設定することが可能であり、従来のネットワーク機器では実現できない高度な対処も可能になる。但し現状ではＳＤＮ対応機器は高価であり導入実績も少なく、当面は従来タイプのネットワーク機器とＳＤＮ対応機器とが混在する状態が続くと考えられ、こうした混在環境でのインシデントに対する効率的な対処方法が重要になると考えられる。

【００１０】

ここで上記特許文献１には、機能が異なる複数のネットワーク機器が混在する環境でのインシデントの対処方法について記載されている。具体的には、レイヤー２スイッチのポートに、ＶＬＡＮ機能を有していない集線装置を介して、複数の端末が接続された場合に、各端末に対して個別に検疫を実行する検疫システムについて記載されている。上記検疫システムは、ＶＬＡＮ機能を持たないネットワーク機器が接続されているレイヤー２スイッチのポートをトランクポートにすることで、端末が送受信するパケットをＬ２レイヤーで識別可能にする。但しこの手法では、ＶＬＡＮタグが付加されたパケットを送受信する機能を端末が備えている必要がある。また未検疫の端末がＶＬＡＮタグ付きのパケットを解析もしくは送受信する機能を備えていた場合、完全な隔離が達成できない可能性がある。

【００１１】
本発明はこうした背景に鑑みてなされたもので、機能の異なる複数のネットワーク機器を含んで構成されるネットワークシステムにおいて、発生したインシデントに対して効率よく対処することが可能な、ネットワーク制御装置、及びネットワーク制御方法を提供することを目的としている。
【課題を解決するための手段】
【００１２】
上記目的を達成するための本発明のうちの一つは、機能の異なるネットワーク機器を含んで構成されるネットワークを制御する装置であって、前記ネットワーク機器の機能に関する情報であるネットワーク機器情報を記憶するネットワーク機器情報記憶部と、前記ネットワークにおいて発生したインシデントに対する対処方針に関する情報である対処方針情報を記憶する対処方針情報記憶部と、前記ネットワーク機器情報及び前記対処方針情報に基づき、前記インシデントに対処するための前記ネットワーク機器の設定に関する情報である設定情報を一つ以上生成する対処設定情報生成部と、を備え、前記対処設定情報生成部は、前記設定情報の生成に際し、発生したインシデントに関する情報であるインシデント情報を前記対処方針と対応づけることにより、前記インシデントに対する対処の方法に関する情報である対処方法を一つ以上生成し、前記対処方法は、前記ネットワーク機器間で送受信されるパケットの送信元と受信先を特定する情報を含み、前記対処設定情報生成部は、前記設定情報の生成に際し、前記送信元から前記受信先に至る経路である対処経路を一つ以上探索し、前記対処方針は、前記ネットワークを流れるパケットに加える更新処理を指定する情報を含み、前記対処設定情報生成部は、前記設定情報の生成に際し、前記対処経路上の前記ネットワーク機器への前記更新処理の割り当てである対処処理配置を、前記ネットワーク機器情報に基づき可能な割り当て方の組み合わせを探索して一つ以上生成し、前記対処方針情報は、前記対処処理配置と前記対処経路との対応を示す情報、前記対処経路と前記対処方法との対応を示す情報、前記対処方針と前記対処方法との対応を示す情報、及び前記インシデントに対する対処の目的を示す情報である対処目的と前記対処方針との対応を示す情報を含み、前記対処設定情報生成部は、前記対処目的ごとに対応する前記対処処理配置を選択することにより生成される情報である対処候補を一つ以上生成する。
【００１３】
その他、本願が開示する課題、及びその解決方法は、発明を実施するための形態の欄、及び図面により明らかにされる。
【発明の効果】
【００１４】
本発明によれば、機能の異なる複数のネットワーク機器を含んで構成されるネットワークシステムにおいて、発生したインシデントに対して効率よく対処することが可能になる。
【図面の簡単な説明】
【００１５】
【図１】一実施形態として示すネットワークシステム１の構成を示す図である。
【図２】ネットワーク制御装置１１１のハードウェア構成の一例を示す図である。
【図３】ネットワーク制御装置１１１が備える機能、及びネットワーク制御装置１１１が記憶するデータを示す図である。
【図４】ネットワーク機器情報管理テーブル４００の一例である。
【図５】トポロジ情報テーブル５００の一例である。
【図６】ネットワーク変数テーブル６００の一例である
【図７】機能マスタテーブル７００の一例である。
【図８】機能対応テーブル８００の一例である。
【図９】機能割り当てテーブル９００の一例である。
【図１０】リソース情報テーブル１０００の一例である。

【図１１】対処目的テーブル１１００の一例である。
【図１２】対処方針テーブル１２００の一例である。
【図１３】対処変数テーブル１３００の一例である。
【図１４】対処方針評価項目テーブル１４００の一例である。
【図１５】処理配置評価項目テーブル１５００の一例である。
【図１６】インシデントテーブル１６００の一例である。
【図１７】対処方法テーブル１７００の一例である。
【図１８】対処経路テーブル１８００の一例である。
【図１９】対処処理配置テーブル１９００の一例である。
【図２０】対処候補テーブル２０００の一例である。
【図２１】ネットワーク情報設定画面２１００の一例である。
【図２２】対処設定画面２２００の一例である。
【図２３】対処設定画面２２００の一例である。
【図２４】評価項目設定画面２４００の一例である。
【図２５】評価項目設定画面２４００の一例である。
【図２６】対処候補設定画面２６００の一例である。
【図２７】情報取得設定処理Ｓ２７００を説明するフローチャートである。
【図２８】インシデント検知時処理Ｓ２８００を説明するフローチャートである。
【図２９】対処設定情報生成処理Ｓ２８０２の詳細を説明するフローチャートである。
【図３０】インシデント情報取得／登録処理Ｓ２９０１の詳細を説明するフローチャートである。
【図３１】対処方法生成処理Ｓ２９０２の詳細を説明するフローチャートである。
【図３２】対処経路生成処理Ｓ２９０３の詳細を説明するフローチャートである。
【図３３】対処処理配置生成処理Ｓ２９０４の詳細を説明するフローチャートである。
【図３４】対処候補生成処理Ｓ２９０５の詳細を説明するフローチャートである。
【図３５】対処候補判定処理Ｓ２９０６の詳細を説明するフローチャートである。
【図３６】対処候補評価スコア算出処理Ｓ２９０７の詳細を説明するフローチャートである。

【発明を実施するための形態】

【００１６】

以下、図面を参照しつつ実施形態について説明する。尚、以下の説明において、同一又は類似の構成について同一の符号を付すことにより重複した説明を省略することがある。また「ネットワークスイッチ」のことを「スイッチ」と略記する。

【００１７】

＜システム構成＞

図１に実施形態として説明するネットワークシステム１の概略的な構成を示している。同図に示すように、ネットワークシステム１は、サービス系ネットワーク５１、管理系ネットワーク５２、サービス系ネットワーク５１に接続するネットワーク機器（スイッチ１５１～１５５、リピータハブ１５６、端末１６１～１６２、サーバ装置１６３、調査端末１６４、ダミーサーバ１６５、及びキャプチャサーバ１６６）、管理系ネットワーク５２に接続する、ネットワーク制御装置１１１、トポロジアナライザ１１２、及びインシデント検知装置１１３を含む。

【００１８】

サービス系ネットワーク５１は、管理系ネットワーク５２に接続するネットワーク制御装置１１１による制御対象となるネットワークであり、例えば、ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）、インターネット（Internet）等である。以下、サービス系ネットワーク５１はＩＰネットワークであるとして説明する。

【００１９】

上記ネットワーク機器のうち、スイッチ１５１～１５５は、例えば、レイヤー２スイッチ、レイヤー３スイッチ、ルータ、ＳＤＮスイッチ（SDN:Software-Defined Networking

）等であり、いずれもネットワーク制御装置１１１からの監視や制御が可能なインテリジェントな機能（情報処理装置としての機能）を備える。スイッチ１５１は、ルータとしても機能し、サービス系ネットワーク５１をインターネット１９１に接続する。端末１６１～１６２、サーバ装置１６３、調査端末１６４、ダミーサーバ１６５、及びキャプチャサーバ１６６は、いずれも情報処理装置（コンピュータ）を用いて構成される。尚、以下では、端末１６１を、マルウェアの感染が予想される端末であるとして説明する。

【００２０】

尚、同図に示したサービス系ネットワーク５１の構成は一例であり、サービス系ネットワーク５１を構成するネットワーク機器の種類や数は同図に示すものに限られない。ネットワーク機器は、インターネット１９１を介して接続される機器であってもよい。またネットワーク機器はハードウェアとして構成されたものに限られず、例えば、ＳＤＮに対応したネットワーク機器のように仮想的に実現されるものであってもよい。

【００２１】

管理系ネットワーク５２は、サービス系ネットワーク５１の管理に用いられるネットワークであり、例えば、ＬＡＮである。尚、同図に示した管理系ネットワーク５２の構成は一例であり、管理系ネットワーク５２を構成する機器の種類や数は同図に示すものに限られない。ネットワーク制御装置１１１、トポロジアナライザ１１２、及びインシデント検知装置１１３は、いずれも情報処理装置（コンピュータ）を用いて構成される。これらは夫々が独立したハードウェアによって実現されるものであってもよいし、これらの２つ以上が共通のハードウェアによって実現されるものであってもよい。以下、管理系ネットワーク５２はＩＰネットワークであるとして説明する。

【００２２】

ネットワーク制御装置１１１は、管理系ネットワーク５２を介して、ネットワーク機器に関する情報の取得やネットワーク機器の動作の設定を行う。ネットワーク制御装置１１１は、サービス系ネットワーク５１においてマルウェア等を用いたサイバー攻撃によるインシデントが発生した際、管理系ネットワーク５２を介して、当該インシデントに関する情報（以下、インシデント情報と称する。）やサービス系ネットワーク５１におけるネットワーク機器の接続に関する情報（以下、トポロジ情報と称する。）を取得する。ネットワーク制御装置１１１は、サービス系ネットワーク５１を構成するネットワーク機器の設定を行うことで、特定の端末が行う通信を制御する。

【００２３】

ネットワーク制御装置１１１は、ネットワークシステム１の管理者等（以下、ユーザと称する。）によって予め設定された対処方針、及び予め取得したネットワーク情報を参照し、インシデントに対する対処方法の候補（以下、対処候補と称する。）を複数生成し、生成した各対処候補について、夫々の望ましさを評価し、評価した結果を提示する。ネットワークシステム１は、提示した対処候補からユーザが選択した対処候補に基づき、ネットワーク機器の設定を行う。

【００２４】

インシデント検知装置１１３は、サービス系ネットワーク５１においてセキュリティに関するインシデントが発生すると、管理系ネットワーク５２を介して、サービス系ネットワーク５１を構成するネットワーク機器からインシデント情報を取得し、取得したインシデント情報を管理系ネットワーク５２を介してネットワーク制御装置１１１に通知する。

【００２５】

トポロジアナライザ１１２は、管理系ネットワーク５２を介して、サービス系ネットワーク５１を構成するネットワーク機器からトポロジ情報を取得し、取得したトポロジ情報を管理系ネットワーク５２を介してネットワーク制御装置１１１に通知する。

【００２６】

図２にネットワーク制御装置１１１のハードウェア構成の一例を示す。同図に示すように、ネットワーク制御装置１１１は、プロセッサ２０１、主記憶装置２０２、補助記憶装置２０３、入力装置２０４、出力装置２０５、及び通信装置２０６を備える。これらは図

示しないバス等の通信手段を介して通信可能に接続されている。

【００２７】

プロセッサ２０１は、例えば、ＣＰＵ（Central Processing Unit）やＭＰＵ（Micro Processing Unit）を用いて構成される。主記憶装置２０２は、揮発性もしくは不揮発性の記憶素子を用いて構成された、プログラムやデータを記憶する装置であり、例えば、ＲＯＭ（Read Only Memory）、ＲＡＭ（Random Access Memory）、ＮＶＲＡＭ（Non Volatile RAM）等である。プロセッサ２０１及び主記憶装置２０２は情報処理装置を構成する。補助記憶装置２０３は、例えば、ＳＳＤ（Solid State Drive）、ハードディスクドライブ、光学式記憶装置、記録媒体の読取／書込装置等である。補助記憶装置２０３に記憶されているプログラムやデータは主記憶装置２０２に随時ロードされる。

【００２８】

入力装置２０４は、ユーザから情報を取得するユーザインタフェースであり、例えば、キーボード、マウス、タッチパネル、操作ボタン、カードリーダ、音声入力装置等である。出力装置２０５は、ユーザに情報を提供するユーザインタフェースであり、例えば、ＬＣＤ（Liquid Crystal Display）、グラフィックカード、音声出力装置（アンプ、スピーカ等）、印字／印刷装置等である。通信装置２０６は、管理系ネットワーク５２に接続する他の機器と通信する有線方式又は無線方式の通信インタフェースであり、例えば、ＮＩＣ（Network Interface Card）、無線通信モジュール等を用いて構成される。

【００２９】

図３にネットワーク制御装置１１１が備える機能、及びネットワーク制御装置１１１が記憶するデータを示している。同図に示すように、ネットワーク制御装置１１１は、表示／操作部１２１、ネットワーク機器情報取得部１２２、インシデント情報取得部１２３、対処設定情報生成部１２４、及びネットワーク機器設定部１２５の各機能を備える。これらの機能は、ネットワーク制御装置１１１のハードウェアによって、もしくは、ネットワーク制御装置１１１のプロセッサ２０１が、主記憶装置２０２（又は補助記憶装置２０３）に記憶されているプログラムを読み出して実行することにより実現される。

【００３０】

同図に示すように、ネットワーク制御装置１１１は、ネットワーク機器情報１３１、対処方針情報１３２、及びインシデント情報１３３の各データを記憶する。これらのデータは、例えば、ネットワーク制御装置１１１（もしくはこれに通信可能に接続された情報処理装置）において動作するＤＢＭＳ（Data Base Management System）によって管理されるデータベースのテーブルとして管理される。

【００３１】

上記機能のうち、表示／操作部１２１は、例えば、サービス系ネットワーク５１の構成情報やインシデントへの対処方針等の情報をユーザが入力／設定するためのユーザインタフェースや、前述した対処候補をユーザに提示し選択を促すためのユーザインタフェースを提供する。

【００３２】

ネットワーク機器情報取得部１２２は、管理系ネットワーク５２を介して、サービス系ネットワーク５１に接続するネットワーク機器が備える機能に関する情報（以下、ネットワーク機器情報と称する。）を取得する。ネットワーク機器情報には、例えば、スイッチ１５１～１５６に関する情報、端末１６１～１６２に関する情報、サーバ装置１６３に関する情報、調査端末１６４に関する情報、ダミーサーバ１６５に関する情報、キャプチャサーバ１６６に関する情報等がある。

【００３３】

インシデント情報取得部１２３は、前述したインシデント情報をインシデント検知装置１１３等を介してサービス系ネットワーク５１から取得する。

【００３４】

対処設定情報生成部１２４は、ネットワーク機器情報取得部１２２やインシデント情報取得部１２３が取得した情報に基づき、サービス系ネットワーク５１において発生したイ

ンシデントに対する対処候補を生成し、生成した対処候補の夫々について望ましさを評価する。

【００３５】

ネットワーク機器設定部１２５は、対処設定情報生成部１２４が生成した対処候補に基づき、サービス系ネットワーク５１を構成しているネットワーク機器に対して、それらのネットワーク機器に対処候補に対応した動作をさせるための情報（以下、設定情報と称する。）を送信する。

【００３６】

ネットワーク制御装置１１１が管理する上記データのうち、ネットワーク機器情報１３１は、サービス系ネットワーク５１を構成しているネットワーク機器の情報（ネットワーク機器を特定する情報、ネットワーク機器の構成に関する情報、ネットワーク機器が備える機能に関する情報、ネットワーク機器間の接続関係を示す情報等。）を含む。対処方針情報１３２は、サービス系ネットワーク５１において発生したインシデントに対する対処方法を決定するために用いる情報を含む。インシデント情報１３３は、サービス系ネットワーク５１において発生したインシデントに関する情報を含む。

【００３７】

＝＝＝データ構成＝＝＝

ネットワーク制御装置１１１が管理（記憶）する、ネットワーク機器情報１３１、対処方針情報１３２、及びインシデント情報１３３について詳細に説明する。

【００３８】

以下では、ネットワーク機器情報１３１の例として、ネットワーク機器情報管理テーブル４００、トポロジ情報テーブル５００、ネットワーク変数テーブル６００、機能マスタテーブル７００、機能対応テーブル８００、機能割り当てテーブル９００、及びリソース情報テーブル１０００を示す。

【００３９】

また対処方針情報１３２の例として、対処目的テーブル１１００、対処方針テーブル１２００、対処変数テーブル１３００、対処方針評価項目テーブル１４００、及び処理配置評価項目テーブル１５００を示す。

【００４０】

またインシデント情報１３３の例として、インシデントテーブル１６００、対処方法テーブル１７００、対処経路テーブル１８００、対処処理配置テーブル１９００、及び対処候補テーブル２０００を示す。

【００４１】

＜ネットワーク機器情報＞

【００４２】

図４は、ネットワーク機器情報１３１の一つとして示すネットワーク機器情報管理テーブル４００の一例である。ネットワーク機器情報管理テーブル４００には、ネットワーク制御装置１１１が、管理系ネットワーク５２を介して制御可能なネットワーク機器に関する情報が管理される。同図に示すように、ネットワーク機器情報管理テーブル４００は、ネットワーク機器ＩＤ４０１、管理アドレス４０２、型番４０３、及びタイプ４０４の各項目を有する一つ以上のレコードで構成される。ネットワーク機器情報管理テーブル４００のレコードの数は、ネットワーク制御装置１１１が制御対象とするネットワーク機器の数に応じて増減する。

【００４３】

上記項目のうち、ネットワーク機器ＩＤ４０１には、ネットワーク機器の識別子（以下、ネットワーク機器ＩＤと称する。）が設定される。管理アドレス４０２には、管理系ネットワーク５２において当該ネットワーク機器に付与されているネットワークアドレス（本例ではＩＰアドレス）が設定される。型番４０３には、当該ネットワーク機器の型番４０３が設定される。タイプ４０４には、当該ネットワーク機器の種類を示す情報（以下、タイプと称する。）が設定される。本実施形態では、同図では、レイヤー２スイッチ等の

レガシータイプのスイッチには上記タイプとして「Legacy」が、ＳＤＮに対応したスイッチには上記タイプとして「SDN」が、夫々設定されている。

【００４４】

図５は、ネットワーク機器情報１３１の一つとして示すトポロジ情報テーブル５００の一例である。トポロジ情報テーブル５００には、ネットワーク機器情報管理テーブル４００の各ネットワーク機器の、サービス系ネットワーク５１における接続関係を示す情報（以下、トポロジ情報と称する。）が管理される。同図に示すように、トポロジ情報テーブル５００は、トポロジＩＤ５０１、ネットワーク機器ＩＤ５０２、インタフェース５０３、対向ネットワーク機器ＩＤ５０４、対向インタフェース５０５、ＳＴＰ状態５０６、通信速度５０７、及び所属ＬＡＮ５０８の各項目からなる一つ以上のレコードで構成される。トポロジ情報テーブル５００のレコード数は、ネットワーク機器間のリンクの数に応じて増減する。

【００４５】

上記項目のうち、トポロジＩＤ５０１には、ネットワーク機器の接続関係（組み合わせ）ごとに付与される識別子（以下、トポロジＩＤと称する。）が設定される。ネットワーク機器ＩＤ５０２には、ネットワーク機器ＩＤが設定される。インタフェース５０３には、当該ネットワーク機器が備える通信インタフェース（例えば、ポート）を特定する情報が設定される。対向ネットワーク機器ＩＤ５０４には、当該ネットワーク機器と接続するネットワーク機器（以下、対向ネットワーク機器と称する。）のネットワーク機器ＩＤが設定される。対向インタフェース５０５には、対向スイッチの通信インタフェース（例えば、ポート）を特定する情報が設定される。ＳＴＰ状態５０６（STP: Spanning Tree Protocol）には、当該ネットワーク機器と対向ネットワーク機器とが現在、通信可能な状態にあるか否かを示す情報が設定される。通信速度５０７には、当該ネットワーク機器と対向ネットワーク機器との間の通信速度５０７の理論値を示す情報が設定される。所属ＬＡＮ５０８には、当該ネットワーク機器が所属しているネットワーク（例えば、ＶＬＡＮ機能やルーティング機能によって分轄された個々のネットワーク）の識別子が設定される。

【００４６】

図６は、ネットワーク機器情報１３１の一つとして示すネットワーク変数テーブル６００の一例である。ネットワーク変数テーブル６００には、ネットワーク制御装置１１１が、サービス系ネットワーク５１の監視や制御に用いる変数や変数に代入されている値が管理される。同図に示すように、ネットワーク変数テーブル６００は、変数名６０１、値６０２、説明６０３の各項目を有する一つ以上のレコードで構成される。ネットワーク変数テーブル６００のレコード数は、ネットワーク制御装置１１１が取り扱う変数の数に応じて増減する。

【００４７】

上記項目のうち、変数名６０１には、変数ごとに付与される識別子（例えば、変数名）が設定される。値６０２には、当該変数に現在代入されている値が設定される。説明６０３には、当該変数に関する情報（当該変数の説明等）が設定される。

【００４８】

図７は、ネットワーク機器情報１３１の一つとして示す機能マスタテーブル７００の一例である。機能マスタテーブル７００には、サービス系ネットワーク５１を構成するネットワーク機器が備える機能を抽象化して表現した情報が管理される。同図に示すように、機能マスタテーブル７００は、機能ＩＤ７０１、サブＩＤ７０２、入力条件７０３、更新処理７０４、出力７０５、及び設定用スクリプトＵＲＩ７０６の各項目を有する一つ以上のレコードで構成される。機能マスタテーブル７００の一つのレコードは抽象化して表現された一つの機能に対応している。

【００４９】

上記項目のうち、機能ＩＤ７０１には、ネットワーク機器が備える機能ごとに付与される識別子（以下、機能ＩＤと称する。）が設定される。サブＩＤ７０２には、複数の機能が連携して動作する場合に、連携して動作する機能群を区別するための識別子（以下、サ

ブＩＤと称する。）が設定される。入力条件７０３には、当該機能の処理対象となるパケットの条件を示す情報が設定される（当該条件を満たすパケットが当該機能の処理の対象となる。）。更新処理７０４には、当該機能の処理対象となるパケットに対して行われる処理（当該パケットに加えられる更新処理）を示す情報が設定される。出力７０５には、当該機能の処理対象となるパケットの出力先となる通信インタフェース（例えば、ポート）を示す情報が設定される。設定用スクリプトＵＲＩ７０６には、当該機能をネットワーク機器に設定するためのコマンドを生成するスクリプトの所在を示す情報（本例では、ＵＲＩ（Uniform Resource Identifier））が設定される。

【００５０】

図８は、ネットワーク機器情報１３１の一つとして示す機能対応テーブル８００の一例である。機能対応テーブル８００には、サービス系ネットワーク５１を構成するネットワーク機器と、各ネットワーク機器が備える機能とを対応付けた情報が管理される。同図に示すように、機能対応テーブル８００は、ネットワーク機器ＩＤ８０１と機能ＩＤ８０２の各項目を有する一つ以上のレコードで構成される。上記項目のうち、ネットワーク機器ＩＤ８０１には前述したネットワーク機器ＩＤが、機能ＩＤ８０２には前述した機能ＩＤが、夫々設定される。

【００５１】

図９は、ネットワーク機器情報１３１の一つとして示す機能割り当てテーブル９００の一例である。機能割り当てテーブル９００には、サービス系ネットワーク５１を構成するネットワーク機器に現在設定されている（割り当てられている）機能を示す情報が管理される。同図に示すように、機能割り当てテーブル９００は、ネットワーク機器ＩＤ９０１、機能ＩＤ９０２、及び変数９０３の各項目からなる一つ以上のレコードで構成される。機能割り当てテーブル９００のレコード数は、ネットワーク機器に現在設定されている機能の数に伴い増減する。

【００５２】

上記項目のうち、ネットワーク機器ＩＤ９０１には前述したネットワーク機器ＩＤが設定される。機能ＩＤ９０２には当該スイッチに割り当てられている機能の前述した機能ＩＤが設定される。変数９０３には当該機能に関する変数に現在代入されている値を示す情報が設定される。

【００５３】

図１０は、ネットワーク機器情報１３１の一つとして示すリソース情報テーブル１０００の一例である。リソース情報テーブル１０００には、サービス系ネットワーク５１における資源（リソース）の割り当てに関する情報（以下、リソース情報と称する。）が管理される。同図に示すように、リソース情報テーブル１０００は、リソースＩＤ１００１、リソース種別１００２、範囲１００３、及び使用状態１００４の各項目からなる一つ以上のレコードで構成される。リソース情報テーブル１０００のレコード数は、サービス系ネットワーク５１における資源（リソース）の変化に伴い増減する。

【００５４】

上記項目のうち、リソースＩＤ１００１には、リソースの識別子（以下、リソースＩＤと称する。）が設定される。リソース種別１００２には、当該リソースの種別を示す情報（以下、リソース種別と称する。）が設定される。範囲１００３には、当該リソースの割り当て可能な範囲を示す情報が設定される。使用状態１００４には、当該リソースが現在、使用中であるか否かを示す情報が設定される。

【００５５】

＜対処方針情報＞

【００５６】

図１１は、対処方針情報１３２の一つとして示す対処目的テーブル１１００の一例である。対処目的テーブル１１００は、サービス系ネットワーク５１において発生したインシデントに対する対処の目的を示す情報（以下、対処目的と称する。）が管理される。同図に示すように、対処目的テーブル１１００は、対処目的ＩＤ１１０１、説明１１０２、及

び対処目的評価スコア１１０３の各項目からなる一つ以上のレコードで構成される。

【００５７】

上記項目のうち、対処目的ＩＤ１１０１には、対処目的ごとに付与される識別子（以下、対処目的ＩＤと称する。）が設定される。説明１１０２には、当該対処目的に関する情報（対処目的の説明等）が設定される。対処目的評価スコア１１０３には、当該対処目的の重要度を示す値（以下、対処目的評価スコアと称する。）が設定される。

【００５８】

図１２は、対処方針情報１３２の一つとして示す対処方針テーブル１２００の一例である。対処方針テーブル１２００は、サービス系ネットワーク５１において発生したインシデントに対して、ネットワークの設定変更等の具体的な対処方法を決定する際の雛形となる情報（以下、対処方針と称する。）が管理されるテーブルである。同図に示すように、対処方針テーブル１２００は、対処方針ＩＤ１２０１、識別条件１２０２、終点１２０３、更新処理１２０４、対処目的ＩＤ１２０５、対処方針評価項目１２０６、及び簡易メモ１２０７の各項目からなる一つ以上のレコードで構成される。対処方針テーブル１２００のレコード数は、設定する対処方針の数に伴い増減する。

【００５９】

上記項目のうち、対処方針ＩＤ１２０１には、対処方針ごとに付与される識別子（以下、対処方針ＩＤと称する。）が設定される。識別条件１２０２には、当該対処方針の処理対象とするパケットを識別する条件を示す情報が設定される。終点１２０３には、当該対処方針の処理対象となるパケットの最終的な転送先を示す情報が設定される。更新処理１２０４には、当該対処方針が適用される際に当該対処方針の処理対象となるパケットに対して行われる処理（更新処理等）を示す情報が設定される。対処目的ＩＤ１２０５には、当該対処方針に対応づけられる対処目的を示す情報が設定される。対処方針評価項目１２０６には、当該対処方針とその望ましさを評価するための項目（以下、対処方針評価項目と称する。）との対応を示す情報が設定される。簡易メモ１２０７には、当該対処方針に関する情報（当該対処方針の説明等）が設定される。

【００６０】

図１３は、対処方針情報１３２の一つとして示す対処変数テーブル１３００の一例である。対処変数テーブル１３００には、対処方針に関する処理で使用する変数（以下、対処変数と称する。）に代入する値が管理される。同図に示すように、対処変数テーブル１３００は、変数名１３０１、アドレス１３０２、接続インタフェース１３０３、及び説明１３０４の各項目からなる一つ以上のレコードで構成される。対処変数テーブル１３００のレコード数は、設定する対処変数の数に伴い増減する。

【００６１】

上記項目のうち、変数名１３０１には、対処変数の識別子（例えば、変数名）が設定される。アドレス１３０２には、当該変数に設定される情報（本例ではＩＰアドレス）が設定される。接続インタフェース１３０３には、当該変数に設定される情報（本例ではトポロジＩＤ５０１）が設定される。説明１３０４には、当該変数に関する情報（例えば、当該変数の用途の説明等）を示す情報が設定される。

【００６２】

図１４は、対処方針情報１３２の一つとして示す対処方針評価項目テーブル１４００の一例である。対処方針評価項目テーブル１４００には、前述した対処方針評価項目に関する情報が管理される。同図に示すように、対処方針評価項目テーブル１４００は、対処方針評価項目ＩＤ１４０１、説明１４０２、及び対処方針評価スコア１４０３の各項目からなる一つ以上のレコードで構成される。対処方針評価項目テーブル１４００のレコード数は、設定する対処方針評価項目の数に伴い増減する。

【００６３】

上記項目のうち、対処方針評価項目ＩＤ１４０１には、対処方針の評価項目の識別子（以下、評価項目ＩＤと称する。）が設定される。説明１４０２は、当該評価項目に関する情報（例えば、当該評価項目の説明情報等）が設定される。対処方針評価スコア１４０３

には、当該対処方針の望ましさを定量化した値（以下、対処方針評価スコアと称する。）が設定される。

【００６４】

図１５は、対処方針情報１３２の一つとして示す処理配置評価項目テーブル１５００の一例である。処理配置評価項目テーブル１５００には、後述する対処処理配置に対してその望ましさの算出に用いる項目（以下、処理配置評価項目と称する。）が管理される。同図に示すように、処理配置評価項目テーブル１５００は、処理配置評価項目ＩＤ１５０１、説明１５０２、算出用スクリプトＵＲＩ１５０３、及び処理配置評価重み１５０４の各項目からなる一つ以上のレコードで構成される。処理配置評価項目テーブル１５００のレコード数は、設定する処理配置評価項目の数に伴い増減する。

【００６５】

上記項目のうち、処理配置評価項目ＩＤ１５０１には、処理配置評価項目ごとに付与される識別子（以下、処理配置評価項目ＩＤと称する。）が設定される。説明１５０２には、当該処理配置評価項目の内容を示す情報が設定される。算出用スクリプトＵＲＩ１５０３には、処理配置評価項目についての評価値（以下、処理配置評価項目評価値と称する。）を算出するためのスクリプトの所在（本例ではＵＲＩ）が設定される。処理配置評価重み１５０４には、算出された上記処理配置評価項目評価値に対して重み付けをするための係数が設定される。

【００６６】

＜インシデント情報＞

図１６は、インシデント情報１３３の一つとして示すインシデントテーブル１６００の一例である。インシデントテーブル１６００には、サービス系ネットワーク５１において発生したインシデントに関する情報が管理される。同図に示すように、インシデントテーブル１６００は、インシデントＩＤ１６０１、対象端末ＩＤ１６０２、接続インタフェース１６０３、及び状況１６０４の各項目からなる一つ以上のレコードで構成される。インシデントテーブル１６００のレコード数は、現在管理中のインシデント数に伴い増減する。

【００６７】

上記項目のうち、インシデントＩＤ１６０１には、インシデントごとに付与される識別子（以下、インシデントＩＤと称する。）が設定される。対象端末アドレス１６０２には、対処の対象となる端末（本例では端末１６１）を特定する情報（本例では端末１６１のＩＰアドレス）が設定される。接続インタフェース１６０３には、当該対象端末１６１から最も少ないホップ数で到達するネットワーク機器（例えば、スイッチ１５１～１５５）の通信インタフェース（例えば、ポート）を特定する情報が設定される。状況１６０４には、当該インシデントの対処の状況を示す情報が設定される。

【００６８】

図１７は、インシデント情報１３３の一つとして示す対処方法テーブル１７００の一例である。対処方法テーブル１７００には、対処方針をインシデントに対応づけて具体化した情報（以下、対処方法と称する。）が管理される。同図に示すように、対処方法テーブル１７００は、対処方法ＩＤ１７０１，インシデントＩＤ１７０２、及び対処方針ＩＤ１７０３の各項目からなる一つ以上のレコードで構成される。対処方法テーブル１７００のレコード数は、管理中のインシデントの数に伴い増減する。

【００６９】

上記項目のうち、対処方法ＩＤ１７０１には、対処方法の識別子（以下、対処方法ＩＤと称する。）が設定される。インシデントＩＤ１７０２には、当該対処方法に対応づけられたインシデントのインシデントＩＤが設定される。対処方針ＩＤ１７０３には、当該対処方法に対応づけられた対処方針の対処方針ＩＤが設定される。

【００７０】

図１８は、インシデント情報１３３の一つとして示す対処経路テーブル１８００の一例である。対処経路テーブル１８００には、対処方法を実現するためのサービス系ネットワ

ーク５１における具体的な経路(以下、対処経路と称する。）を示す情報が管理される。同図に示すように、対処経路テーブル１８００は、対処経路ＩＤ１８０１、対処方法ＩＤ１８０２、及び制御経路１８０３の各項目からなる一つ以上のレコードで構成される。対処経路テーブル１８００のレコード数は、管理中の対処方法の数に伴い増減する。

【００７１】

上記項目のうち、対処経路ＩＤ１８０１には、対処経路ごとに付与される識別子（以下、対処経路ＩＤと称する。）が設定される。対処方法ＩＤ１８０２には、当該対処経路に対応する対処方法の対処方法ＩＤが設定される。制御経路１８０３には、対処経路を、サービス系ネットワーク５１におけるネットワーク機器（ネットワーク機器ＩＤ）のリスト（組み合わせ）として表現した情報が設定される。

【００７２】

図１９は、インシデント情報１３３の一つとして示す対処処理配置テーブル１９００の一例である。対処処理配置テーブル１９００には、各対処経路に対し、対応する対処方法に指定されているパケットの更新処理のネットワーク機器への具体的な割り当てを示す情報（以下、対処処理配置と称する。）が管理される。同図に示すように、対処処理配置テーブル１９００は、対処処理配置ＩＤ１９０１、対処経路ＩＤ１９０２、更新処理配置１９０３、及び処理機能設定１９０４の各項目からなる一つ以上のレコードで構成される。対処処理配置テーブル１９００のレコード数は、管理中の対処経路の数に伴い増減する。

【００７３】

上記項目のうち、対処処理配置ＩＤ１９０１には、対処処理配置の識別子（以下、対処処理配置ＩＤと称する。）が設定される。対処経路ＩＤ１９０２には、当該対処処理配置に対応づけられている対処経路の対処経路ＩＤが設定される。更新処理配置１９０３は、パケットの更新処理の割り当てを示す情報が設定される。処理機能設定１９０４には、上記割り当ての可否についての判定結果や上記更新処理の具体的な設定値等の情報が設定される。

【００７４】

図２０は、インシデント情報１３３の一つとして示す対処候補テーブル２０００の一例である。対処候補テーブル２０００には、対処目的を具体化する対処処理配置の組み合わせ（前述した対処候補に相当）が管理される。同図に示すように、対処候補テーブル２０００は、対処候補ＩＤ２００１、目的／対処処理配置対応２００２、及び対処候補評価スコア２００３の各項目からなる一つ以上のレコードで構成される。対処候補テーブル２０００のレコード数は、対処目的テーブル１１００、インシデントテーブル１６００、及び対処処理配置テーブル１９００のうちの少なくともいずれかのレコードの数の増減に伴い増減する。

【００７５】

上記項目のうち、対処候補ＩＤ２００１には、対処候補ごとに付与される識別子（以下、対処候補ＩＤと称する。）が設定される。目的／対処処理配置対応２００２には、対処目的と対処処理配置とを対応づけた情報が設定される。対処候補評価スコア２００３には、目的／対処処理配置対応２００２に基づき算出される、当該対処候補の望ましさを示す値（以下、対処候補評価スコアと称する。）が設定される。

【００７６】

＝＝＝ユーザインタフェース＝＝＝

続いて、表示／操作部１２１が提供するユーザインタフェースの例を示す。

【００７７】

図２１は、表示／操作部１２１が提供するユーザインタフェースの一つとして示すネットワーク情報設定画面２１００の一例である。ユーザは、ネットワーク情報設定画面２１００を利用して、サービス系ネットワーク５１に関する情報をネットワーク機器情報１３１としてネットワーク制御装置１１１に設定することができる。

【００７８】

同図に示すように、ネットワーク情報設定画面２１００には、タブ２１４０、プレビュ

ー画面２１１０、ネットワーク機器一覧２１２０、及びネットワーク機器情報編集欄２１３０が設けられている。

【００７９】

このうちタブ２１４０は、出力装置２０５に表示させる画面の切り替えに用いられる。ユーザは、タブ２１４０の一つを選択することにより、当該ネットワーク情報設定画面２１００や後述する対処設定画面２２００、評価項目設定画面２４００、及び対処候補設定画面２６００のいずれかを出力装置２０５に表示させることができる。

【００８０】

プレビュー画面２１１０には、ネットワーク制御装置１１１が、ネットワーク機器情報管理テーブル４００及びトポロジ情報テーブル５００に基づき生成するサービス系ネットワーク５１の構成図が表示される。

【００８１】

ネットワーク機器一覧２１２０には、ネットワーク機器情報管理テーブル４００の内容が表示される。ユーザは、ネットワーク機器一覧２１２０からネットワーク機器を選択することができる。ネットワーク機器情報編集欄２１３０には、ネットワーク機器一覧２１２０から選択されたネットワーク機器に関する詳細が表示される。

【００８２】

ネットワーク制御装置１１１は、ユーザが更新ボタン２１２１を選択すると、管理系ネットワーク５２に接続しているネットワーク機器やトポロジアナライザ１１２等からネットワーク機器情報を取得する。ネットワーク制御装置１１１は、取得したネットワーク機器情報を、ネットワーク機器情報１３１として記憶する。またネットワーク制御装置１１１は、取得したネットワーク機器情報に基づき、当該ネットワーク情報設定画面２１００の表示内容を更新する。尚、ユーザは編集ボタン２１２２を選択することで、ネットワーク機器情報編集欄２１３０に表示されている内容を編集（ネットワーク機器情報１３１を編集）することもできる。

【００８３】

図２２及び図２３は、表示／操作部１２１が提供するユーザインタフェースの一つとして示す対処設定画面２２００の一例である。ユーザは、この対処設定画面２２００を利用して、対処方針や対処目的に関する情報を入力し、対処方針情報１３２として設定することができる。これらの図に示すように、対処設定画面２２００には、前述したタブ２１４０、対象選択欄２２１０、対処一覧２２２０、及び対処編集欄２２３０が設けられている。

【００８４】

このうち対象選択欄２２１０にはプルダウンメニュー２２１１が設けられている。ユーザは、プルダウンメニュー２２１１を利用して、閲覧や編集の対象を選択することができる。

【００８５】

図２２は、ユーザがプルダウンメニュー２２１１を操作して「対処方針」を選択した場合に相当する。同図に示すように、対処一覧２２２０には、対処方針テーブル１２００の内容が表示されている。対処一覧２２２０から対処方針の一つが選択されると、選択された対処方針に対応する対処方針テーブル１２００の内容が対処編集欄２２３０に表示される。ユーザは対処編集欄２２３０の内容を編集することで対処方針テーブル１２００の内容を更新することができる。

【００８６】

図２３は、プルダウンメニュー２２１１を操作して「対処目的」を選択した場合に相当する。同図に示すように、対処一覧２２２０には、対処目的テーブル１１００の内容が表示されている。対処一覧２２２０から対処目的の一つが選択されると、選択された対処目的に対応する対処目的テーブル１１００の内容が対処編集欄２２３０に表示される。ユーザは対処編集欄２２３０の内容を編集することで対処目的テーブル１１００の内容を更新することができる。

【００８７】
図２４及び図２５は、表示／操作部１２１が提供するユーザインタフェースの一つとして示す評価項目設定画面２４００の一例である。ユーザは、この評価項目設定画面２４００を利用して、評価項目に関する情報を対処方針情報１３２として設定することができる。これらの図に示すように、評価項目設定画面２４００には、前述したタブ２１４０、対象評価項目選択欄２４１０、評価項目一覧２４２０、及び評価項目編集欄２４３０が設けられている。
【００８８】
このうち対象評価項目選択欄２４１０にはプルダウンメニュー２４１１が設けられている。ユーザは、プルダウンメニュー２４１１を利用して、閲覧や編集の対象を選択することができる。
【００８９】
図２４は、ユーザがプルダウンメニュー２４１１を操作して「対処方針」を選択した場合に相当する。この場合、評価項目一覧２４２０には、対処方針評価項目テーブル１４００の内容が表示される。ユーザが評価項目一覧２４２０から評価項目を一つ選択し、編集ボタン２４２１を選択すると、選択した評価項目の内容が評価項目編集欄２４３０に表示される。ユーザは、評価項目編集欄２４３０の内容を編集することで対処方針評価項目テーブル１４００の内容を更新することができる。またユーザは、新規作成ボタン２４２２を選択することで、対処方針評価項目テーブル１４００に新規のレコードを追加することができる。ユーザは、削除ボタン２４２３を選択することで、対処方針評価項目テーブル１４００の任意のレコードを削除することができる。
【００９０】
図２５は、ユーザがプルダウンメニュー２４１１を操作して「対処処理配置」を選択した場合に相当する。この場合、評価項目一覧２４２０には、処理配置評価項目テーブル１５００の内容が表示される。ユーザが評価項目一覧２４２０から処理配置評価項目を一つ選択し、編集ボタン２４２１を選択すると、選択した処理配置評価項目の内容が評価項目編集欄２４３０に表示される。ユーザは、評価項目編集欄２４３０の内容を編集することで処理配置評価項目テーブル１５００の内容を更新することができる。またユーザは、新規作成ボタン２４２２を選択することで、処理配置評価項目テーブル１５００に新規のレコードを追加することができる。ユーザは、削除ボタン２４２３を選択することで、処理配置評価項目テーブル１５００の任意のレコードを削除することができる。
【００９１】
図２６は、表示／操作部１２１が提供するユーザインタフェースの一つとして示す対処候補設定画面２６００の一例である。ユーザは、この対処候補設定画面２６００を利用して、インシデントの対処に用いる対処候補を選択する。
【００９２】
同図に示すように、対処候補設定画面２６００には、対象インシデント選択欄２６１０、対処候補選択欄２６２０、対処目的・処理配置選択欄２６３０、及びプレビュー画面２６４０が設けられている。
【００９３】
対象インシデント選択欄２６１０にはプルダウンメニュー２６１１が設けられている。ユーザは、プルダウンメニュー２６１１を利用して、インシデントテーブル１６００のインシデントの一つを選択することができる。
【００９４】
対処候補選択欄２６２０には、対処候補テーブル２０００から取得される、対象インシデント選択欄２６１０にて選択されたインシデントに対応づけられている対処候補の一覧が表示される。ユーザは、表示されている対処候補の中から、インシデントの対処に用いる対処候補を選択することができる。
【００９５】
対処候補が選択されると、対処目的・処理配置選択欄２６３０には対処候補テーブル２

０００の目的／対処処理配置対応２００２の一覧が表示される。ユーザが対処目的・処理配置の組み合わせの一つを選択すると、上記選択した組み合わせに対応する対処処理配置の詳細を示した図がプレビュー画面２６４０に表示される。

【００９６】

尚、以上では、ユーザインタフェースとしてＧＵＩ（Graphical User Interface）によるものを例示したが、これに限定されず、ユーザインタフェースは、例えば、ＣＬＩ（Command Line Interface）を利用するものやファイルのアップロードやダウンロードを利用するものであってもよい。

【００９７】

＝＝＝処理例＝＝＝

続いて、以上に説明した構成からなるネットワークシステム１において行われる処理について説明する。

【００９８】

図２７は、ネットワーク機器情報１３１や対処方針情報１３２の設定に関してネットワーク制御装置１１１が行う処理（以下、情報取得設定処理Ｓ２７００と称する。）を説明するフローチャートである。以下、同図とともに情報取得設定処理Ｓ２７００について説明する。

【００９９】

ネットワーク制御装置１１１のネットワーク機器情報取得部１２２は、トポロジアナライザ１１２等を介して、サービス系ネットワーク５１を構成しているネットワーク機器からネットワーク情報を取得し、取得した情報をネットワーク機器情報１３１として記憶する（Ｓ２７０１）。当該処理は、例えば、予め設定されたタイミング行ってもよいし、ユーザの操作指示等に応じて任意のタイミングで行ってもよい。

【０１００】

ユーザは、表示／操作部１２１を介して、前述したネットワーク機器情報及びインシデント情報をネットワーク制御装置１１１に入力する（Ｓ２７１１）。ネットワーク制御装置１１１は、入力された上記情報を、夫々、ネットワーク機器情報１３１、対処方針情報１３２として記憶する（Ｓ２７１２）。ユーザは、表示／操作部１２１を介して、ネットワーク機器情報１３１及び対処方針情報１３２を参照することができる。

【０１０１】

図２８は、ネットワーク制御装置１１１が、サービス系ネットワーク５１において発生したインシデントを検知した場合に行う処理（以下、インシデント検知時処理Ｓ２８００と称する。）を説明するフローチャートである。以下、同図とともにインシデント検知時処理Ｓ２８００について説明する。

【０１０２】

同図に示すように、ネットワーク制御装置１１１のインシデント情報取得部１２３は、インシデント検知装置１１３を介してインシデント情報を取得し、取得したインシデント情報を対処設定情報生成部１２４に送信する（Ｓ２８０１）。

【０１０３】

続いて、ネットワーク制御装置１１１の対処設定情報生成部１２４は、インシデント情報取得部１２３から受信したインシデント情報をインシデント情報１３３として記憶する。また対処設定情報生成部１２４は、ネットワーク機器情報１３１及び対処方針情報１３２に基づき、発生したインシデントに対する対処方法、対処経路、及び対処処理配置を生成し、生成した対処方法、対処経路、及び対処処理配置に基づき対処候補を生成する。また対処設定情報生成部１２４は、生成した対処候補の夫々について対処候補評価スコアを算出し、算出した対処候補及び対処候補評価スコアを表示／操作部１２１に送信する（Ｓ２８０２）。以下、当該処理を対処設定情報生成処理Ｓ２８０２と称する。

【０１０４】

表示／操作部１２１は、対処設定情報生成部１２４から受信した対処候補及び対処候補評価スコアを出力装置２０５に出力（表示）してユーザに提示する（Ｓ２８０３）。

【０１０５】
ユーザは、表示／操作部１２１が提供するユーザインタフェースを介して対処候補を選択する（Ｓ２８０４）。表示／操作部１２１は、ユーザが選択した対処候補を対処設定情報生成部１２４に送信する（Ｓ２８０５）。
【０１０６】
対処設定情報生成部１２４は、表示／操作部１２１から受信した対処候補に基づき、選択する対処候補を決定し、インシデント情報１３３を更新する（Ｓ２８０６）。また対処設定情報生成部１２４は、採用した対処候補に基づきネットワーク機器の設定を変更するよう、ネットワーク機器設定部１２５に指示を送信する（Ｓ２８０７）。ネットワーク機器設定部１２５は、指示に応じてネットワーク機器情報１３１を更新する（Ｓ２８０８）。
【０１０７】
ネットワーク機器設定部１２５は、対処設定情報生成部１２４から受信した指示に応じて、各スイッチ１５１～１５５に設定変更指示を送信する（Ｓ２８０８）。
【０１０８】
図２９は、図２８の対処設定情報生成処理Ｓ２８０２の詳細を説明するフローチャートである。以下、同図とともに対処設定情報生成処理Ｓ２８０２について説明する。
【０１０９】
まずネットワーク制御装置１１１の対処設定情報生成部１２４は、インシデント情報取得部１２３からインシデント情報を取得し、取得したインシデント情報をインシデント情報１３３として記憶する。以下、この処理をインシデント情報取得／登録処理Ｓ２９０１と称する。対処設定情報生成部１２４は、上記インシデント情報として、例えば、端末１６１のネットワークアドレス（ＩＰアドレス）や端末１６１が接続されているネットワーク機器の通信インタフェース（例えば、スイッチ１５３が備えるポートの識別子）を取得する。
【０１１０】
続いて、対処設定情報生成部１２４は、対処方針テーブル１２００を参照し、インシデント情報取得／登録処理Ｓ２９０１で取得したインシデント情報に対処方針を対応させることにより対処方法を生成し、生成した対処方法を対処方法テーブル１７００に記憶する。以下、この処理を対処方法生成処理Ｓ２９０２と称する。対処設定情報生成部１２４は、対処方針テーブル１２００の対処方針における変数に、上記インシデント情報から取得される具体的な値を代入することにより対処方針を具体化して対処方法を生成する。
【０１１１】
このように対処設定情報生成部１２４は、インシデント情報に基づき対処方針を具体化して対処方法を生成するので、発生したインシデントに対処するための対処方針に沿った対処方法を自動的に生成することができる。
【０１１２】
続いて、対処設定情報生成部１２４は、対処設定情報生成部１２４が生成した対処方法について対処経路を生成し、生成した対処経路を対処経路テーブル１８００に記憶する。以下、この処理を対処経路生成処理Ｓ２９０３と称する。対処設定情報生成部１２４は、例えば、対処方法に指定されているパケットの送信元と受信先に基づき、パケットが送信元から受信先に至る途中経路のバリエーションを探索して複数の経路を生成し、生成した経路を対処経路とする。
【０１１３】
このように対処設定情報生成部１２４は、対処方法に基づき途中経路のバリエーションを探索して複数の対処経路を生成するので、対処方法に対応する対処経路を自動的に生成することができる。
【０１１４】
続いて、対処設定情報生成部１２４は、生成した対処経路の夫々について更新処理配置１９０３を複数生成し、生成した更新処理配置１９０３を対処処理配置テーブル１９００

に記憶する。以下、この処理を対処処理配置生成処理Ｓ２９０４と称する。対処設定情報生成部１２４は、例えば、対処経路上のネットワーク機器の、対処方針に指定されている更新処理（パケットに加える更新処理）の割り当てを、ネットワーク機器情報１３１に基づき可能な組み合わせを探索して複数生成し、生成した組み合わせを対処処理配置とする。

【０１１５】

このように対処設定情報生成部１２４は、更新処理のネットワーク機器への割り当てを、ネットワーク機器情報１３１に基づき可能な組み合わせを探索することにより生成するので、ネットワークを構成する個々のネットワーク機器が備える機能を考慮しつつ更新処理のネットワーク機器への割り当てを生成することができる。

【０１１６】

続いて、対処設定情報生成部１２４は、対処処理配置テーブル１９００を参照し、対処目的ごとに対処処理配置を選択して対処候補を複数生成し、生成した対処候補を対処候補テーブル２０００に記憶する。以下、この処理を対処候補生成処理Ｓ２９０５と称する。対処設定情報生成部１２４は、例えば、対処目的の夫々について、対応する対処方針の一つから生成された対処処理配置の一つを選択し、対処目的の夫々について対処処理配置の組み合わせを探索して複数生成し、対処候補とする。

【０１１７】

このように対処設定情報生成部１２４は、対処目的の夫々について対処処理配置の組み合わせ方を探索して対処候補を生成するので、対処目的と対処処理配置とを組合せた形で対処候補をユーザに提示することができる。

【０１１８】

続いて、対処設定情報生成部１２４は、生成した対処候補の夫々について実現可能性を判定して対処候補テーブル２０００を更新する。以下、この処理を対処候補判定処理Ｓ２９０６と称する。対処設定情報生成部１２４は、例えば、対処処理配置及びその生成元の対処方法に指定されているパケットの制御方法と、ネットワーク機器情報１３１から取得されるネットワーク機器が備える機能とを対照（比較）することによりパケットの制御方法が実現可能か否かを判定し、対処候補の実現可能性を判定する。

【０１１９】

このように対処設定情報生成部１２４は、対処候補の夫々について、サービス系ネットワーク５１を構成している個々のネットワーク機器が備える機能を考慮して対処候補の実現可能性を判定するので、現状のネットワーク機器の構成に則して対処候補の実現可能性を判定することができる。

【０１２０】

続いて、対処設定情報生成部１２４は、生成した対処候補の夫々について対処候補評価スコアを算出して対処候補テーブル２０００を更新する。以下、この処理を対処候補評価スコア算出処理Ｓ２９０７と称する。対処設定情報生成部１２４は、例えば、対処処理配置の生成元の対処方針に設定されている対処方針評価スコア１４０３、対処方針に対応する対処目的に設定されている対処目的評価スコア１１０３、及び対処処理配置から求められる評価スコア（後述の対処処理配置評価スコア）に基づき、対処候補の優先度である対処候補評価スコアを求める。

【０１２１】

このように対処設定情報生成部１２４は、各対処方針の優先度（対処方針評価スコア１４０３）、各対処目的の優先度（対処目的評価スコア１１０３）、及び各対処処理配置の優先度（対処処理配置評価スコア）に基づき、対処候補の優先度を求めるので、対処方針、対処目的、及び対処処理配置の夫々の優先度を考慮した形で対処候補の優先度をユーザに提示することができる。

【０１２２】

続いて、対処設定情報生成部１２４は、対処候補を対処候補評価スコア２００３でソートし、表示／操作部１２１に出力する（Ｓ２９０８）。

【０１２３】
図３０は、図２９に示したインシデント情報取得／登録処理Ｓ２９０１の詳細を説明するフローチャートである。以下、同図とともにインシデント情報取得／登録処理Ｓ２９０１について説明する。以下では、マルウェアの感染が予想される端末１６１（以下、隔離対象端末とも称する。）が関係するインシデントが発生した場合を例として説明する。
【０１２４】
対処設定情報生成部１２４は、発生したインシデントの情報をインシデント検知装置１１３から取得する（Ｓ３００１）。上記インシデント情報は、例えば、端末１６１のＩＰアドレスや端末１６１に関する他の情報を含む。
【０１２５】
続いて、対処設定情報生成部１２４は、インシデントテーブル１６００に新規のレコードを追加し、追加したレコードの内容を設定する。例えば、対処設定情報生成部１２４は、インシデントＩＤ１６０１に未使用のＩＤを、対象端末アドレス１６０２に端末１６１のＩＰアドレスを、夫々設定する（Ｓ３００２）。対処設定情報生成部１２４が必要に応じて端末１６１のＩＰアドレス以外の情報をさらにインシデントテーブル１６００に設定してもよい。
【０１２６】
続いて、対処設定情報生成部１２４は、端末１６１のトポロジ情報テーブル５００のネットワーク機器ＩＤ５０２及び所属ＬＡＮ５０８と、ネットワーク変数テーブル６００の変数名６０１及び値６０２を参照し、各スイッチが接続しているＬＡＮのＩＰアドレス帯を取得する。続いて、トポロジアナライザ１１２に、取得したＩＰアドレス帯のＩＰアドレスとＭＡＣアドレスとを対応付けた情報を要求し、端末１６１のＩＰアドレスに対応づけられているＭＡＣアドレスを取得する（Ｓ３００３）。
【０１２７】
続いて、対処設定情報生成部１２４は、取得したＩＰアドレス帯と端末１６１のＩＰアドレスとを比較し、端末１６１が所属するＬＡＮに接続されているスイッチ（スイッチ１５１～１５５）の一覧を取得する。対処設定情報生成部１２４は、取得した各スイッチ（スイッチ１５１～１５５）に対し、トポロジアナライザ１１２を介して指示を送信し、各スイッチ（スイッチに１５１～１５５）に保存されているＭＡＣアドレステーブルを取得する。そして対処設定情報生成部１２４は、ＭＡＣアドレステーブル及びトポロジ情報テーブル５００を参照し、端末１６１のＭＡＣアドレスを送信元とするパケットが入力された通信インタフェース（例えば、ポート）の一覧を取得する（Ｓ３００４）。
【０１２８】
続いて、対処設定情報生成部１２４は、インタフェースの一覧の中で、トポロジ情報テーブル５００において対向インタフェース５０５が登録されていないインタフェースを特定し、特定したインタフェースを端末１６１から最小のホップ数で接続されているインタフェースであるとみなして、インシデントテーブル１６００の接続インタフェース１６０３に設定する（Ｓ３００５）。
【０１２９】
続いて、対処設定情報生成部１２４は、追加したインシデントテーブル１６００のレコードの状況１６０４に「未対処」を設定する（Ｓ３００６）。
【０１３０】
図３１は、図２９に示した対処方法生成処理Ｓ２９０２の詳細を説明するフローチャートである。以下、同図とともに対処方法生成処理Ｓ２９０２について説明する。
【０１３１】
対処設定情報生成部１２４は、対処方針テーブル１２００及びインシデントテーブル１６００を参照し、対処方針テーブル１２００から対処方針の一覧を、インシデントテーブル１６００からインシデントの一覧を、夫々取得する。対処設定情報生成部１２４は、対処方法テーブル１７００に、取得したインシデントの一覧の夫々について取得した対処方針の一覧を対応づけたレコードを新規に生成する。対処設定情報生成部１２４は、生成し

た各レコードの対処方法ＩＤ１７０１には未使用の対処方法ＩＤを、インシデントＩＤ１７０２にはインシデントＩＤを、対処方針ＩＤ１７０３には対処方針ＩＤを、夫々設定する（Ｓ３１０１～Ｓ３１０３）。

【０１３２】

図３２は、図２９に示した対処経路生成処理Ｓ２９０３の詳細を説明するフローチャートである。以下、同図とともに対処経路生成処理Ｓ２９０３について説明する。

【０１３３】

同図に示すように、対処設定情報生成部１２４は、ネットワーク機器情報管理テーブル４００からネットワーク機器の一覧を、トポロジ情報テーブル５００からインタフェースの一覧を、夫々取得する。続いて、対処設定情報生成部１２４は、取得したインタフェース一覧の夫々について、ＳＴＰ状態５０６に基づき、現在通信可能な状態にあるインタフェースを選出する（Ｓ３２０１）。

【０１３４】

続いて、対処設定情報生成部１２４は、対処方法テーブル１７００から対処方法の一覧を取得し、取得した対処方法の夫々について、以下のＳ３２０２～Ｓ３２０５の処理を実行する。

【０１３５】

対処設定情報生成部１２４は、対処方法（対処方法ＩＤ１７０１）に対処方針ＩＤ１７０３を介して対処方針テーブル１２００に対応付けられている対処方針の識別条件１２０２、終点１２０３、及び更新処理１２０４の各変数に対応する値を、ネットワーク変数テーブル６００、リソース情報テーブル１０００、及び対処変数テーブル１３００から取得する。続いて、対処設定情報生成部１２４は、各対処方法（対処方法ＩＤ１７０１）にインシデントＩＤ１７０２を介して対応付けられているインシデントに、インシデントテーブル１６００の接続インタフェース１６０３を介して対応付けられているインタフェースを「始点」として取得する。また対処設定情報生成部１２４は、各対処方法（対処方法ＩＤ１７０１）に対応づけられている対処方針ＩＤ１７０３に、対処方針の終点１２０３を介して対応付けられた変数に、対処変数の接続インタフェース１６０３を介して対応付けられたインタフェースを終点として取得する。そして対処設定情報生成部１２４は、上記始点から上記終点に至る経路を生成（前述した通信可能な状態にあるインタフェースとして識別したインタフェースのみを経由する経路）を生成し、生成した経路を制御経路とする（Ｓ３２０３）。尚、経路の選び方により、制御経路は複数になりうる。経路の生成は任意のアルゴリズムを用いて行うことができる。

【０１３６】

続いて、対処設定情報生成部１２４は、対処経路テーブル１８００に、生成した制御経路１８０３の夫々に対応するレコードを新規に追加し、追加したレコードに内容を設定する（対処経路ＩＤ１８０１には未使用のＩＤを、対処方法ＩＤ１８０２には対応する対処方法を、制御経路１８０３には生成した制御経路を設定する。）（Ｓ３２０４）。

【０１３７】

図３３は、図２９に示した対処処理配置生成処理Ｓ２９０４の詳細を説明するフローチャートである。以下、同図とともに対処処理配置生成処理Ｓ２９０４について説明する。

【０１３８】

同図に示すように、対処設定情報生成部１２４は、対処経路テーブル１８００に設定されている各対処経路について、以下のＳ３３０１～Ｓ３３０４の処理を実行する。

【０１３９】

まず対処設定情報生成部１２４は、各対処経路に対し、対処経路テーブル１８００の対処方法ＩＤ１８０２、及び対処方法テーブル１７００の対処方針ＩＤ１７０３を参照し、対応する対処方針テーブル１２００の更新処理１２０４を取得する。そして対処設定情報生成部１２４は、取得した更新処理１２０４を、対処経路上に存在するネットワーク機器に割り当て、対処処理配置テーブル１９００の更新処理配置１９０３の内容を生成する（Ｓ３３０２）。尚、対処経路上に存在するネットワーク機器の割り当て方を変更すること

で、生成される更新処理配置１９０３は複数になりうる。上記割り当てには任意のアルゴリズムを用いて行うことができる。

【０１４０】

対処設定情報生成部１２４は、対処処理配置テーブル１９００に、生成した更新処理配置ごとに新規レコードを追加する。そして対処設定情報生成部１２４は、生成したレコードの対処処理配置ＩＤ１９０１には未使用の対処処理配置ＩＤを、対処経路ＩＤ１９０２には対応する対処経路の対処経路ＩＤを、夫々設定する（Ｓ３３０３）。尚、この段階では処理機能設定１９０４は未設定の状態である。

【０１４１】

図３４は、図２９に示した対処候補生成処理Ｓ２９０５の詳細を説明するフローチャートである。以下、同図とともに対処候補生成処理Ｓ２９０５について説明する。

【０１４２】

対処設定情報生成部１２４は、対処処理配置テーブル１９００から対処処理配置１９０１に対応する対処経路ＩＤ１９０２を取得し、対処経路テーブル１８００から対処経路ＩＤ１９０２に対応する対処方法１８０２を取得し、対処方法テーブル１７００から上記対処方法に対応する対処方針１７０３を取得し、対処方針テーブル１２００から上記対処方針に対応する対処目的１２０５を取得する。そして対処設定情報生成部１２４は、対処目的テーブル１１００に格納されている各対処目的と対処処理配置の組み合わせを目的／対処処理配置対応２００２とした新規レコードを対処候補テーブル２０００に追加する（Ｓ３４０１）。尚、この段階では、対処候補ＩＤ２００１は未使用の値を設定し、対処候補評価スコア２００３は未設定の状態である。

【０１４３】

図３５は、図２９に示した対処候補判定処理Ｓ２９０６の詳細を説明するフローチャートである。以下、同図とともに対処候補判定処理Ｓ２９０６について説明する。

【０１４４】

同図に示すように、対処設定情報生成部１２４は、対処処理配置テーブル１９００を参照し、各対処処理配置に対して以下のＳ３５０１～Ｓ３５０６の処理を繰り返し実行する。

【０１４５】

まず対処設定情報生成部１２４は、対処経路テーブル１８００を参照し、対処処理配置に対応する対処経路を取得する。そして対処設定情報生成部１２４は、対処経路上の各ネットワーク機器について以下の処理を行う。

【０１４６】

まず対処設定情報生成部１２４は、対処方法テーブル１７００を参照し、対処経路に対応する対処方法を取得し、対処方針テーブル１２００を参照して上記対処方法に対応する対処方針を取得し、対処変数テーブル１３００、リソース情報テーブル１０００、及びネットワーク変数テーブル６００を参照して変数の値を取得し、取得した上記対処方針の変数に代入する。また対処設定情報生成部１２４は、取得した上記対処方針の識別条件１２０２、上記対処処理配置の更新処理配置１９０３、上記対処経路及びトポロジ情報テーブル５００から取得されるパケットの入力元の通信インタフェース（例えば、ポート）及び出力先の通信インタフェース、の組み合わせを取得し、取得した組み合わせを各ネットワーク機器でのパケットの処理とする（Ｓ３５０２）。

【０１４７】

続いて、対処設定情報生成部１２４は、機能マスタテーブル７００を参照して上記パケット処理に対応する入力条件７０３、更新処理７０４、及び出力７０５の組み合わせを選択し、機能対応テーブル８００を参照してネットワーク機器に機能が対応付けられているか否かを判定する（Ｓ３５０３）。対処設定情報生成部１２４が、対処経路上の全てのネットワーク機器に対して機能が対応付けられていると判定した場合(Ｓ３５０３：ＹＥＳ）、処理はＳ３５０４に進む。上記以外の場合（Ｓ３５０３：ＮＯ）、処理はＳ３５０５に進む。

【０１４８】
Ｓ３５０４では、対処設定情報生成部１２４は、Ｓ３５０３で取得した各ネットワーク機器でのパケットに対する更新処理を実現する機能を、ネットワーク機器ＩＤ４０１、機能ＩＤ７０１、及び変数の具体値、の組み合わせにより表現し、対処処理配置テーブル１９００の処理機能設定１９０４に設定する（Ｓ３５０４）。
【０１４９】
Ｓ３５０５では、対処設定情報生成部１２４は、処理機能設定１９０４の値に「Impossible」を設定する。
【０１５０】
続いて、対処設定情報生成部１２４は、各対処候補について以下のＳ３５０７～Ｓ３５１０の処理を繰り返し実行する。
【０１５１】
まず対処設定情報生成部１２４は、対処処理配置テーブル１９００を参照し、対処候補テーブル２０００の目的／対処処理配置対応２００２の各値に対応する処理機能設定１９０４を取得する。対処設定情報生成部１２４は、取得した処理機能設定１９０４の夫々に対し、競合する設定の有無を判定する。例えば、同じ入力条件に対して違う処理を行う設定が同一のネットワーク機器に対して設定されている場合、対処設定情報生成部１２４は設定が競合していると判定する。また対処設定情報生成部１２４は、機能割り当てテーブル９００を参照し、既存のネットワーク機器の設定との競合の有無を判定する（Ｓ３５０８）。対処設定情報生成部１２４が競合がないと判定した場合（Ｓ３５０８：ない）、処理はＳ３５１０へ進み、次の対処候補について同様の処理を行う。対処設定情報生成部１２４が競合があると判定した場合（Ｓ３５０８：ある）、処理はＳ３５０９に進む。
【０１５２】
Ｓ３５０９では、対処設定情報生成部１２４は、対処候補テーブル２０００の対処候補評価スコア２００３に「Impossible」を設定する（Ｓ３５０９）。
【０１５３】
図３６は、図２９に示した対処候補評価スコア算出処理Ｓ２９０７の詳細を説明するフローチャートである。以下、同図とともに対処候補評価スコア算出処理Ｓ２９０７について説明する。
【０１５４】
同図に示すように、対処設定情報生成部１２４は、対処候補テーブル２０００を参照し、各対処候補について以下のＳ３６０１～Ｓ３６０８の処理を繰り返し実行する。
【０１５５】
対処設定情報生成部１２４は、対処候補評価スコア２００３を参照し、値が「Impossible」であるか否かを判定する（Ｓ３６０２）。対処設定情報生成部１２４が、対処候補評価スコア２００３が「Impossible」であると判定した場合（Ｓ３６０２：ＮＯ）、処理はＳ３６０８に進み、次の対処候補に対して処理を続行する。対処設定情報生成部１２４が、対処候補評価スコア２００３が「Impossible」でないと判定した場合（Ｓ３６０２：ＹＥＳ）、処理はＳ３６０３に進む。
【０１５６】
Ｓ３６０３では、対処設定情報生成部１２４は、目的／対処処理配置対応２００２を参照し、目的と対処処理配置の組み合わせの夫々について、以下の処理を繰り返し実行する。
【０１５７】
まず対処設定情報生成部１２４は、対処処理配置の処理機能設定１９０４を参照し、値が「Impossible」であるか否かを判定する（Ｓ３６０４）。対処設定情報生成部１２４が、処理機能設定１９０４が「Impossible」であると判定した場合（Ｓ３６０４：ＮＯ）、処理はＳ３６０６へ進み、次の目的と対処処理配置の組み合わせに対して処理を続行する。対処設定情報生成部１２４が、処理機能設定１９０４が「Impossible」でないと判定した場合（Ｓ３６０４：ＹＥＳ）、処理はＳ３６０５へ進む。

【０１５８】
Ｓ３６０５では、対処設定情報生成部１２４は、対処目的テーブル１１００を参照し、上記目的に対応する対処目的評価スコア１１０３の値を取得する。そして対処設定情報生成部１２４は、対処処理配置テーブル１９００を参照して上記対処処理配置に対応する対処経路を取得し、取得した対処経路に対応する対処方法を対処経路テーブル１８００から取得し、取得した対処方法に対応する対処方針を対処方法テーブル１７００から取得し、取得した対処方針に対応する対処方針評価項目を対処方針テーブル１２００から取得し、取得した対処方針評価項目の夫々に対応する対処方針評価スコアを対処方針評価項目テーブル１４００から取得し、取得した対処方針評価スコアの合計を算出する。続いて、対処設定情報生成部１２４は、算出用のスクリプトを処理配置評価項目テーブル１５００から取得し、上記対処処理配置を各スクリプトに与えて実行し、出力された値の合計を算出することで、対処処理配置評価スコアを取得する。そして対処設定情報生成部１２４は、上記対処目的評価スコア、上記対処方針評価スコア、上記対処処理配置評価スコアの積を算出し、算出した値を対処候補テーブル２０００の目的／対処処理配置対応２００２の夫々の評価スコアとする。
【０１５９】
Ｓ３６０７では、対処設定情報生成部１２４は、上記目的／対処処理配置対応２００２の夫々の評価スコアを合計し、合計した値を対処候補テーブル２０００の対処候補評価スコア２００３に設定する。
【０１６０】
尚、以上では、評価スコアの算出方法として積と和を用いたが、評価スコアは任意の方法（関数等）を用いて算出してよい。
【０１６１】
以上に説明したように、本実施形態のネットワーク制御装置１１１は、ネットワーク機器情報１３１及び対処方針情報１３２に基づき、発生したインシデントに対処するための設定情報を生成するので、サービス系ネットワーク５１を構成している個々のネットワーク機器が備える機能を考慮しつつ対処方針に則した形で設定情報を生成することができる。そのため、ネットワーク制御装置１１１は、サービス系ネットワーク５１に新たな機器や機能を追加することなく、発生したインシデントに対して効率よく適切に対処することができる。
【０１６２】
以上、本発明者によってなされた発明を実施の形態に基づき具体的に説明したが、本発明は上記の実施の形態に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。例えば、上記の実施の形態は本発明を分かりやすく説明するために詳細に説明したものであり、必ずしも説明した全ての構成を備えるものに限定されるものではない。また上記実施形態の構成の一部について、他の構成の追加・削除・置換をすることが可能である。
【０１６３】
また上記の各構成、機能、処理部、処理手段等は、それらの一部または全部を、例えば、集積回路で設計する等によりハードウェアで実現してもよい。また、上記の各構成、機能等は、プロセッサがそれぞれの機能を実現するプログラムを解釈し、実行することによりソフトウェアで実現してもよい。各機能を実現するプログラム、テーブル、ファイル等の情報は、メモリやハードディスク、ＳＳＤ（Solid State Drive）等の記録装置、またはＩＣカード、ＳＤカード、ＤＶＤ等の記録媒体に置くことができる。
【０１６４】
また上記の各図において、制御線や情報線は説明上必要と考えられるものを示しており、必ずしも実装上の全ての制御線や情報線を示しているとは限らない。実際にはほとんど全ての構成が相互に接続されていると考えてもよい。
【０１６５】
例えば、以上に説明した実施形態では、対処設定情報生成部１２４が対処候補評価スコ

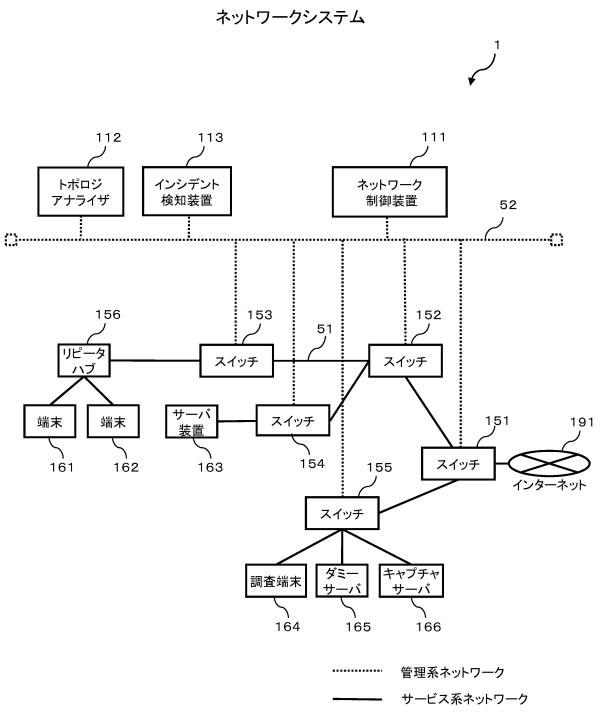
ア２００３を算出した後（図２８の対処設定情報生成処理Ｓ２８０２）、ユーザが表示／操作部１２１を介して対処候補の一覧を参照し（Ｓ２８０３）、適用する対処候補を選択しているが（Ｓ２８０４）、対処設定情報生成部１２４が対処候補評価スコア２００３を算出した後、対処候補評価スコア２００３が最大のものを選択し、これを適用するまでの処理を自動的に行うようにしてもよい。この場合、例えば、図２８のＳ２８０３で結果を表示／操作部１２１に出力する代わりに対処設定情報生成部１２４が対処候補評価スコア２００３が最大のものを選択し、その後はＳ２８０６に進むようにする。このようにすることで、インシデントが多発した場合にユーザの業務負荷を緩和することができる。またインシデントに対して迅速に対処することができる。

【符号の説明】

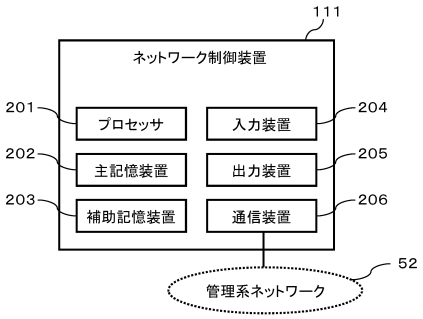
【０１６６】

１　ネットワークシステム、５１　サービス系ネットワーク、５２　管理系ネットワーク、１１１　ネットワーク制御装置、１１２　トポロジアナライザ、１１３　インシデント検知装置、１２１　表示／操作部、１２２　ネットワーク機器情報取得部、１２３　インシデント情報取得部、１２４　対処設定情報生成部、１２５　ネットワーク機器設定部、１３１　ネットワーク機器情報、１３２　対処方針情報、１３３　インシデント情報、１５１～１５５　スイッチ、１６１，１６２　端末、４００　ネットワーク機器情報管理テーブル、５００　トポロジ情報テーブル、６００　ネットワーク変数テーブル、７００　機能マスタテーブル、８００　機能対応テーブル、９００　機能割り当てテーブル、１０００　リソース情報テーブル、１１００　対処目的テーブル、１２００　対処方針テーブル、１３００　対処変数テーブル、１４００　対処方針評価項目テーブル、１５００　処理配置評価項目テーブル、１６００　インシデントテーブル、１７００　対処方法テーブル、１８００　対処経路テーブル、１９００　対処処理配置テーブル、２０００　対処候補テーブル、２１００　ネットワーク情報設定画面、２２００　対処設定画面、２４００　評価項目設定画面、２６００　対処候補設定画面、１１０３　対処目的評価スコア、１４０３　対処方針評価スコア、２００３　対処候補評価スコア

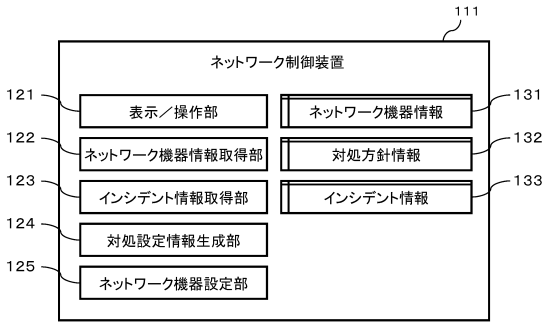
【図１】



【図２】



【図３】



【図４】

ネットワーク機器情報131

ネットワーク機器情報管理テーブル400

401 ネットワーク機器ID	402 管理アドレス	403 型番	404 タイプ
Sw31(152)	192.168.1.131	C35	Legacy
Sw32(151)	192.168.1.132	P32	SDN
Sw21(153)	192.168.1.121	C29	Legacy
Sw22(154)	192.168.1.122	P32	SDN
Sw23(155)	192.168.1.123	C29	Legacy
:	:	:	:

【図５】

ネットワーク機器情報131

トポロジ情報テーブル500

501 トポロジID	502 ネットワーク機器ID	503 インタフェース	504 対向ネットワーク機器ID	505 対向インタフェース	506 STP状態	507 通信速度	508 所属LAN
IF1	Sw31	Gi 0/1	Sw32	Gi 0/1	Forward	10G	Lan2
IF2	Sw31	Gi 0/2	Sw21	Gi 0/1	Forward	1G	Lan1
IF3	Sw32	Gi 0/2	Sw22	Gi 0/1	Forward	1G	Lan3
IF4	Sw31	Gi 0/3	Sw23	Gi 0/1	Forward	1G	Lan4
IF5	Sw32	Gi 0/1	Sw31	Gi 0/1	Forward	10G	Lan2
IF6	Sw21	Gi 0/1	Sw31	Gi 0/2	Forward	1G	Lan1
IF7	Sw22	Gi 0/1	Sw32	Gi 0/2	Forward	1G	Lan3
IF8	Sw23	Gi 0/1	Sw31	Gi 0/3	Forward	1G	Lan4
IF9	Sw21	Gi 0/2	−	−	Forward	1G	Lan1
IF10	Sw22	Gi 0/2	−	−	Forward	1G	Lan3
IF11	Sw22	Gi 0/3	−	−	Forward	1G	Lan3
IF12	Sw22	Gi 0/4	−	−	Forward	1G	Lan3
IF13	Sw23	Gi 0/2	−	−	Forward	1G	Lan4
:	:	:	:	:	:	:	:

【図６】

ネットワーク機器情報131

ネットワーク変数テーブル600

601 変数名	602 値	603 説明
Lan1	10.0.1.0/24	LAN
Lan2	10.0.2.0/24	LAN
Lan3	10.0.3.0/24	LAN
Lan4	10.0.4.0/24	LAN
:	:	:

【図７】

ネットワーク機器情報131

機能マスタテーブル700

701 機能ID	702 サブID	703 入力条件	704 更新処理	705 出力	706 設定用スクリプトURI
Fnc1	1	If(x)	UpdateVid(a)	If(y)	/etc/fnc/fnc1.py
Fnc2	1	if(x)	PushVid(a)	if(y)	/etc/fnc/fnc2-1.py
Fnc2	2	if(y)	PopVid()	if(x)	/etc/fnc/fnc2-2.py
Fnc3	1	if(x) and IpDst(a)	UpdateIpDst(a)	if(y)	/etc/fnc/fnc3.py
Fnc4	1	−	DefaultL2SW ()	−	/etc/fnc/fnc4.py
Fnc5	1	−	DefaultL3SW()	−	/etc/fnc/fnc5.py
:	:	:	:	:	:

【図８】

ネットワーク機器情報131

機能対応テーブル800

801 ネットワーク機器ID	802 機能ID
Sw21	Fnc4
Sw32	Fnc5
Sw23	Fnc4
Sw31	Fnc1
Sw31	Fnc2
Sw31	Fnc3
Sw31	Fnc4
Sw31	Fnc5
Sw22	Fnc1
Sw22	Fnc2
Sw22	Fnc3
Sw22	Fnc4
Sw22	Fnc5
:	:

【図９】

ネットワーク機器情報131

機能割り当てテーブル900

901 ネットワーク機器ID	902 機能ID	903 変数
Sw21	Fnc4	−
Sw23	Fnc4	−
Sw32	Fnc5	−
Sw31	Fnc5	−
Sw31	Fnc1	X=1, a=100, y=1
Sw22	Fnc4	−
:	:	:

【図１０】

ネットワーク機器情報131

リソース情報テーブル1000

1001 リソースID	1002 リソース種別	1003 範囲	1004 使用状態
Rsc/ip1	IPアドレス	10.0.1.0/24	使用中
Rsc/ip2	IPアドレス	10.0.2.0/24	使用中
Rsc/ip3	IPアドレス	10.0.3.0/24	使用中
Rsc/ip4	IPアドレス	10.0.4.0/24	使用中
Rsc/ip5	IPアドレス	10.0.5.0/24	未使用
Rsc/vid100	VLAN ID	100	未使用
⋮	⋮	⋮	⋮

【図１１】

対処方針情報132

対処目的テーブル1100

1101 対処目的ID	1102 説明	1103 対処目的評価スコア
Obj1	感染端末を隔離	1.0
Obj2	感染端末周辺の端末のサーバへの通信許可	0.3
Obj3	調査端末から感染端末への通信の許可	0.6
Obj4	ダミーサーバへの通信誘導	0.1
Obj5	パケットキャプチャ	0.6
:	:	:

【図１２】

対処方針情報132

対処方針テーブル1200

1201 対処方針ID	1202 識別条件	1203 終点	1204 更新処理	1205 対処目的ID	1206 対処方針評価項目	1207 簡易メモ
Pcy1	Ip.if==targetCnt.if	−	SetVid(isolateLan)	Obj1	P/E1, P/E11	ポートごとの隔離
Pcy2	Ip.src==targetCnt.ip	−	SetVid(isolateLan)	Obj1	P/E1, P/E4, P/E11,	IP指定しての隔離
Pcy3	Ip.if==targetCnt.if && Ip.src!=targetCnt.ip && Ip.dst==sv.ip	sv	UpdateVid(serviceLan)	Obj2	P/E4, P/E15	周辺端末からサーバへの通信を通常LANへ
Pcy4	Ip.src==invCnt.ip	targetCnt	None	Obj3	P/E5	調査端末から感染端末への通信許可
Pcy5	Ip.src==targetCnt.ip && ip.dst==sv.ip	dummySv	UpdateIpDst(dummySv.ip)	Obj4	P/E6, P/E9, P/E12	感染端末からダミーサーバへ通信誘導
Pcy6	Ip.if==targetCnt.if	capSv	UpdateIpDst(capSv.ip)	Obj5	P/E14, P/E16	感染端末からの通信キャプチャ(宛先IP変更)
Pcy7	Ip.if==targetCnt.if	capSv	None	Obj5	P/E16	感染端末の通信キャプチャ(IP変更なし)
:	:	:	:	:	:	:

【図１３】

対処方針情報132

対処変数テーブル1300

1301 変数名	1302 アドレス	1303 接続インタフェース	1304 説明
Sv	10.0.4.51	IF13	通信を許可するサーバ
invCnt	10.0.3.101	IF10	調査端末
dummySv	10.0.3.102	IF11	ダミーサーバ
capSv	10.0.3.103	IF12	キャプチャサーバ
:	:	:	:

【図１４】

対処方針情報132

対処方針評価項目テーブル1400

1401 対処方針評価項目ID	1402 説明	1403 対処方針評価スコア
P/E1	感染端末の隔離が可能	1.0
P/E2	感染端末から一部の通常系サーバへ通信可能	0.2
P/E3	感染端末の周辺端末が通常系へ通信可能	0.8
P/E4	感染端末の周辺端末が一部の通常系サーバへ通信可能	0.6
P/E5	調査端末から感染端末へ接続可能	1.0
P/E6	感染端末からダミーサーバへ接続可能	0.4
P/E7	感染端末のIP変更が必要	−0.9
P/E8	ネットワークのIP変更が必要	−0.9
P/E9	切り替え時に通信途絶発生	−0.1
P/E10	新規IPアドレス使用が必要	−0.5
P/E11	新規VLANID使用が必要	−0.2
P/E12	宛先IP変更が必要	−0.1
P/E13	送信元IP変更が必要	−0.1
P/E14	キャプチャパケットのIP変更が必要	−0.4
P/E15	VLANIDの変更が必要	−0.1
P/E16	感染端末のパケットキャプチャが可能	0.8
:	:	:

【図１５】

対処方針情報132

処理配置評価項目テーブル1500

1501 処理配置評価項目ID	1502 説明	1503 算出用スクリプトURI	1404 処理配置評価重み
F/E1	ホップ数	/etc/eval/eval1.py	0.9
F/E2	レイテンシ	/etc/eval/eval2.py	0.4
F/E3	通常通信への影響	/etc/eval/eval3.py	0.9
F/E4	使用帯域	/etc/eval/eval4.py	0.9
F/E5	スイッチへの負荷集中	/etc/eval/eval5.py	0.5
:	:	:	:

【図１６】

インシデント情報133

インシデントテーブル1600

1601 インシデントID	1602 対象端末アドレス	1603 接続インタフェース	1604 状況
Inc1	10.0.0.101	IF9	未対処
Inc2	10.0.0.102	IF9	対処済
:	:	:	:

【図１７】

インシデント情報133

対処方法テーブル1700

1701 対処方法ID	1702 インシデントID	1703 対処方針ID
Res1	Inc1	Pcy1
Res2	Inc1	Pcy2
Res3	Inc1	Pcy3
Res4	Inc1	Pcy4
Res5	Inc1	Pcy5
Res6	Inc1	Pcy6
Res7	Inc1	Pcy7
:	:	:

【図１８】

インシデント情報133

対処経路テーブル1800

1801 対処経路ID	1802 対処方法ID	1803 制御経路
Rou1	Res1	Sw21
Rou2	Res1	Sw21, Sw31
Rou3	Res1	Sw21, Sw31,Sw32
Rou4	Res2	Sw21
Rou5	Res2	Sw21, Sw31
Rou6	Res2	Sw21, Sw31,Sw32
Rou7	Res3	Sw21, Sw31, Sw23
Rou8	Res3	Sw21, Sw31, Sw32, Sw31, Sw23
Rou9	Res3	Sw21, Sw31, Sw32, Sw22, Sw32, Sw31, Sw23
Rou10	Res4	Sw23, Sw32, Sw31, Sw21
Rou11	Res4	Sw23, Sw32, Sw31, Sw23, Sw31, Sw21
Rou12	Res5	Sw21, Sw31, Sw32, Sw23
Rou13	Res5	Sw21, Sw31, Sw23, Sw31, Sw32, Sw22
Rou14	Res6	Sw21, Sw31, Sw32, Sw23
Rou15	Res6	Sw21, Sw31, Sw23, Sw31, Sw32, Sw22
:	:	:

【図１９】

インシデント情報133

対処処理配置テーブル1900

1901 対処処理配置ID	1902 対処経路ID	1903 更新処理配置	1904 処理機能設定
Arg71	Rou7	Sw21: UpdateIpDst(serviceLan)	Impossible
Arg72	Rou7	Sw31: UpdateIpDst(serviceLan)	Impossible
Arg73	Rou7	Sw23: UpdateIpDst(serviceLan)	Impossible
Arg81	Rou8	Sw21: UpdateIpDst(serviceLan)	Impossible
Arg82	Rou8	Sw31(1): UpdateIpDst(serviceLan)	Impossible
Arg83	Rou8	Sw32: UpdateIpDst(serviceLan)	(Sw32, Fnc1, [x:1, a:100, y:1])
Arg84	Rou8	Sw31(2): UpdateIpDst(serviceLan)	Impossible
Arg85	Rou8	Sw23: UpdateIpDst(serviceLan)	Impossible
Arg91	Rou9	Sw21: UpdateIpDst(serviceLan)	Impossible
Arg92	Rou9	Sw31(1): UpdateIpDst(serviceLan)	Impossible
Arg93	Rou9	Sw32(1): UpdateIpDst(serviceLan)	(Sw32, Fnc1, [x:1, a:100, y:2])
Arg94	Rou9	Sw22: UpdateIpDst(serviceLan)	(Sw22, Fnc1, [x:1, a:100, y:1])
Arg95	Rou9	Sw32(2): UpdateIpDst(serviceLan)	(Sw32, Fnc1, [x:2, a:100, y:1])
Arg96	Rou9	Sw31(2): UpdateIpDst(serviceLan)	Impossible
Arg97	Rou9	Sw23: UpdateIpDst(serviceLan)	Impossible
:	:	:	:

【図２０】

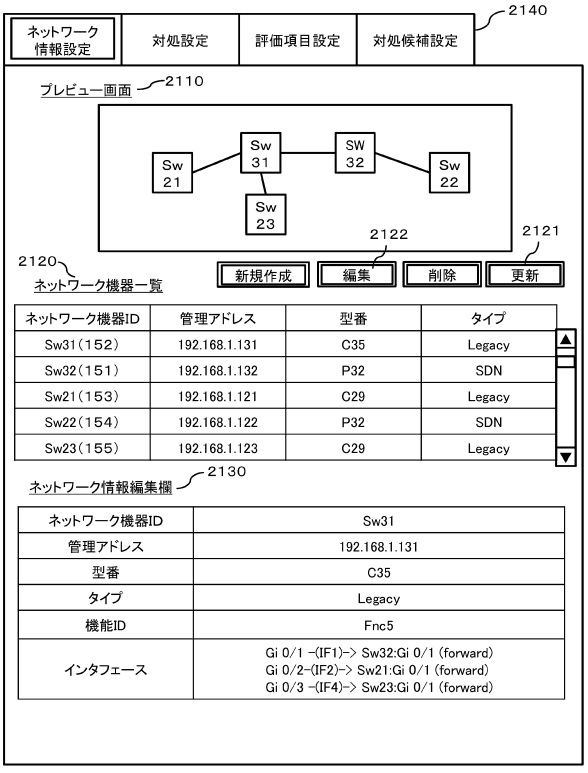
インシデント情報133

対処候補テーブル2000

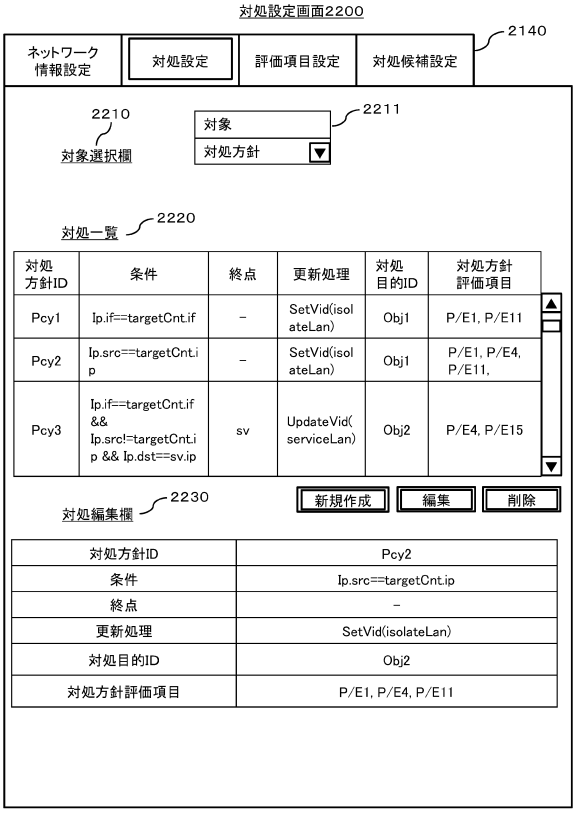
2001 対処候補ID	2002 目的・対処処理配置対応	2003 対処候補評価スコア
Opt1	Obj1: Arg11 Obj2: Arg72 Obj3: Arg101 Obj4: Arg141 Obj5: Arg191	3.7
Opt2	Obj1: Arg11 Obj2: Arg83 Obj3: Arg101 Obj4: Arg141 Obj5: Arg191	4.5
Opt3	Obj1: Arg11 Obj2: Arg95 Obj3: Arg101 Obj4: Arg141 Obj5: Arg191	4.3
:	:	:

【図２１】

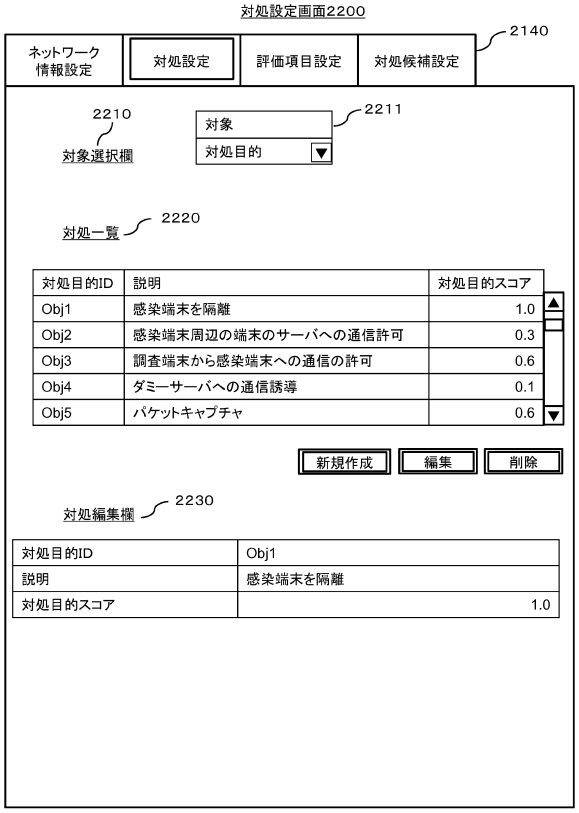
ネットワーク情報設定画面2100



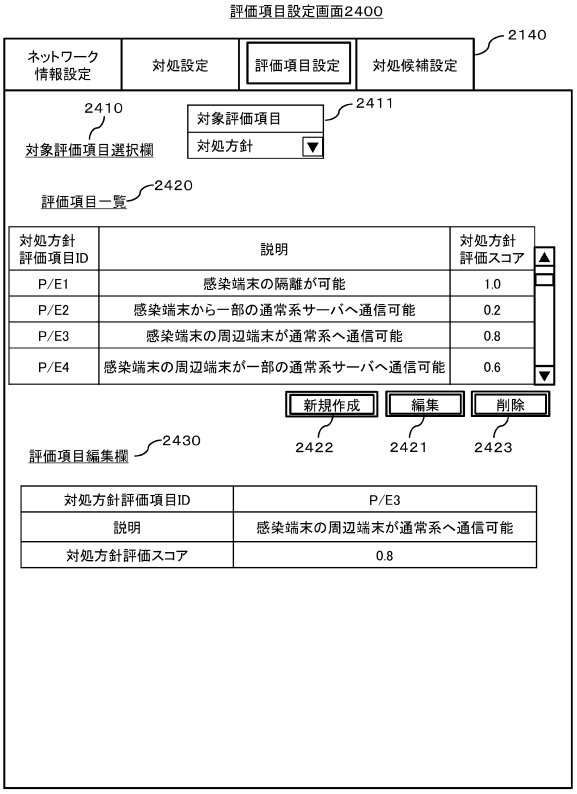
【図２２】



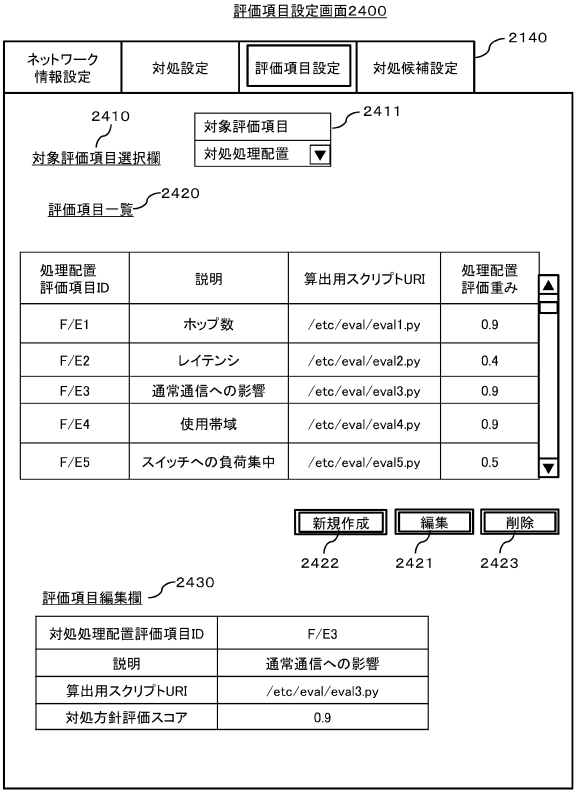
【図２３】



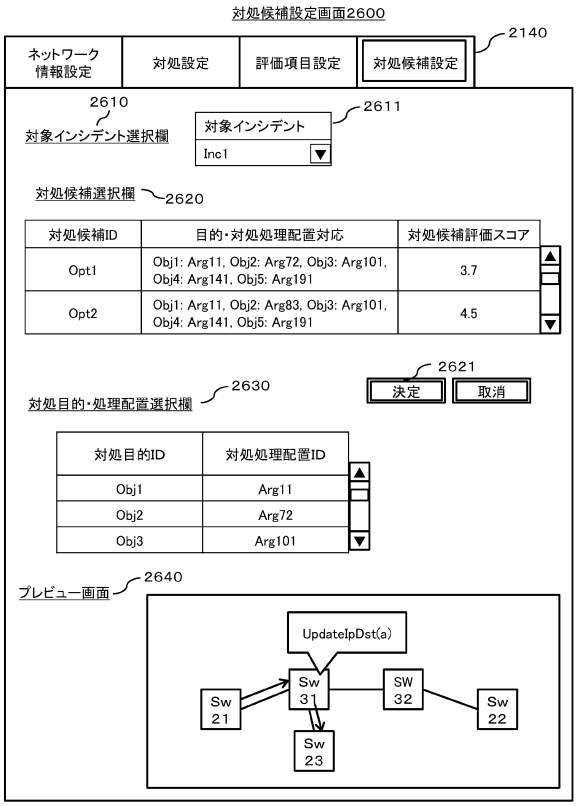
【図２４】



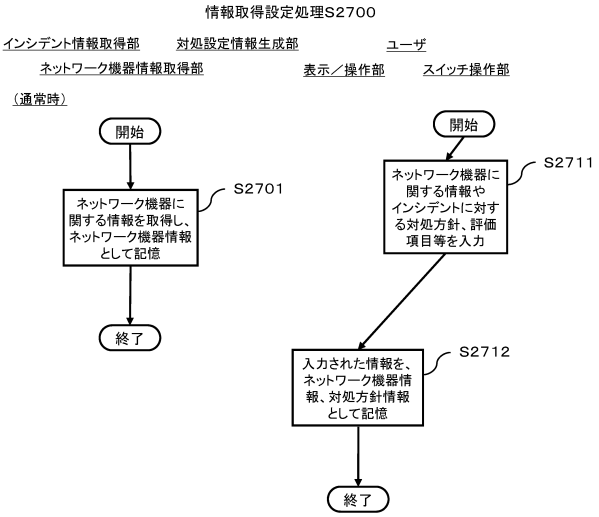
【図２５】



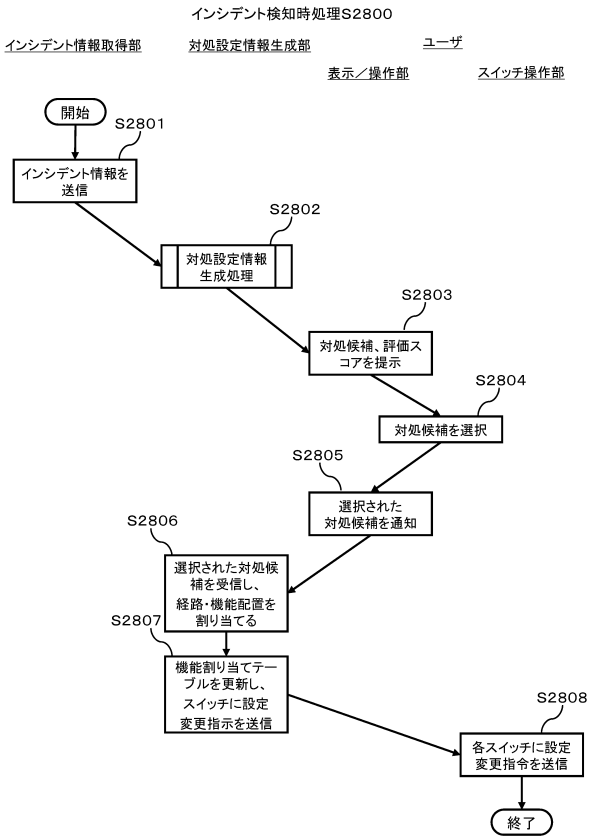
【図２６】



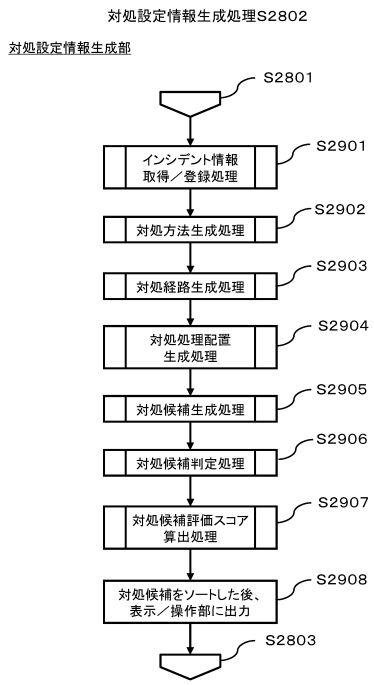
【図２７】



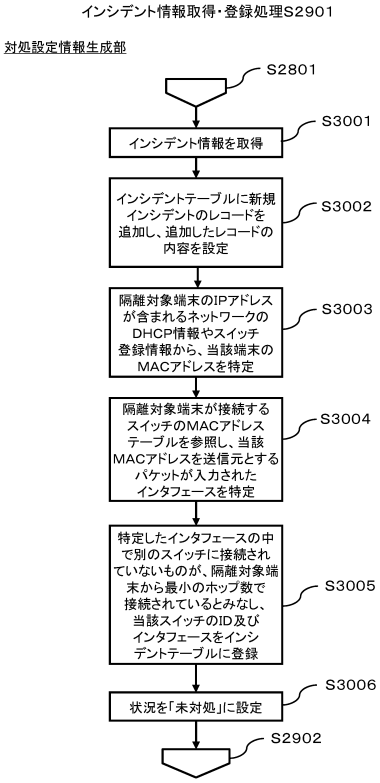
【図２８】



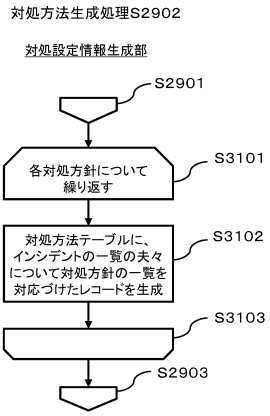
【図２９】



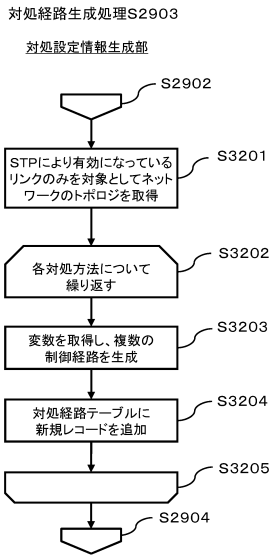
【図３０】



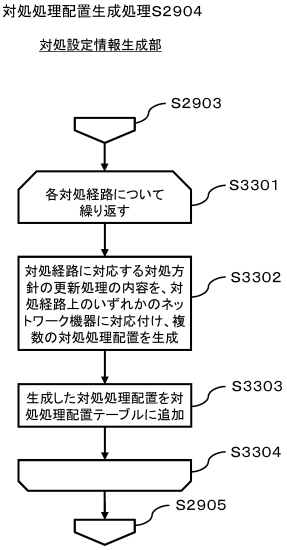
【図３１】



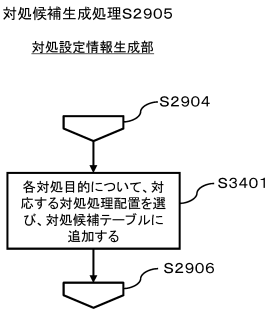
【図３２】



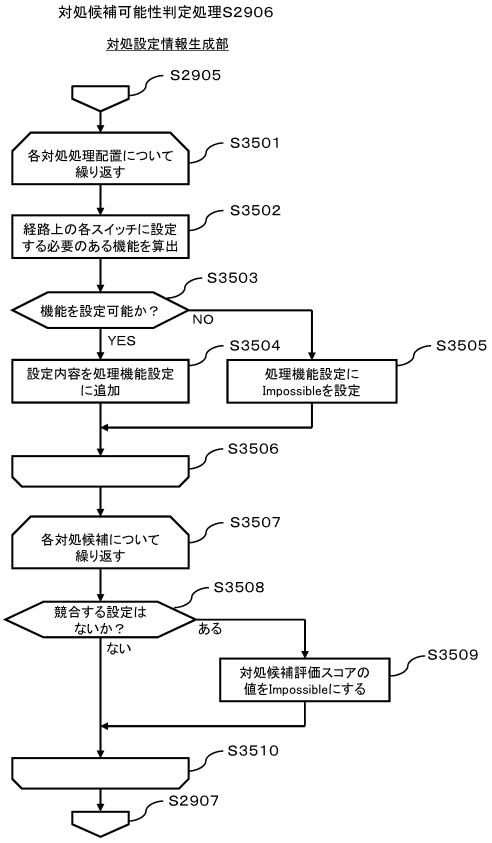
【図３３】



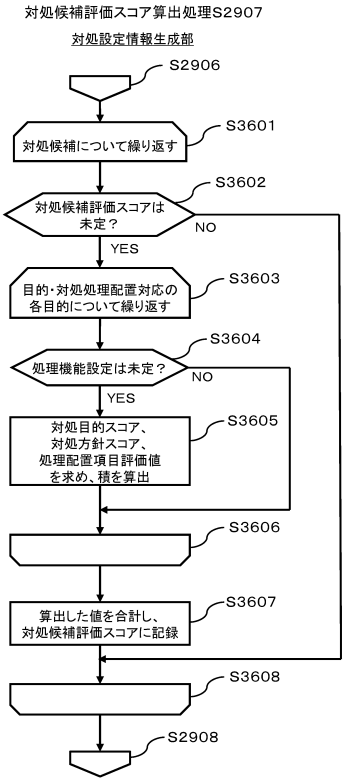
【図３４】


対処候補生成処理S2905
対処設定情報生成部
S2904
各対処目的について、対応する対処処理配置を選び、対処候補テーブルに追加する
S3401
S2906

【図３５】


対処候補可能性判定処理S2906
対処設定情報生成部
S2905
各対処処理配置について繰り返す
S3501
経路上の各スイッチに設定する必要のある機能を算出
S3502
機能を設定可能か？
S3503
NO
YES
設定内容を処理機能設定に追加
S3504
処理機能設定にImpossibleを設定
S3505
S3506
各対処候補について繰り返す
S3507
競合する設定はないか？
S3508
ある
ない
対処候補評価スコアの値をImpossibleにする
S3509
S3510
S2907

【図３６】


対処候補評価スコア算出処理S2907
対処設定情報生成部
S2906
対処候補について繰り返す
S3601
対処候補評価スコアは未定？
S3602
NO
YES
目的・対処処理配置対応の各目的について繰り返す
S3603
処理機能設定は未定？
S3604
NO
YES
対処目的スコア、対処方針スコア、処理配置項目評価値を求め、積を算出
S3605
S3606
算出した値を合計し、対処候補評価スコアに記録
S3607
S3608
S2908

フロントページの続き

(72)発明者　木城　武康
東京都品川区大崎一丁目２番１号　株式会社日立システムズ内

審査官　森田　充功

(56)参考文献　特開２００７－１２９５４７（ＪＰ，Ａ）
特開２００８－０８３７５１（ＪＰ，Ａ）
特開２００９－０１０４３８（ＪＰ，Ａ）
特開２０１３－０４６３２２（ＪＰ，Ａ）
特開２００６－２４６１２２（ＪＰ，Ａ）
特開２０１６－０９２７６３（ＪＰ，Ａ）
特開２０１５－２１９８５９（ＪＰ，Ａ）
来間　一郎　他，マルウェア調査のためのＳＤＮによるネットワーク切替え手法，情報処理学会論文誌（ジャーナル）［ｏｎｌｉｎｅ］，情報処理学会，２０１５年　9月１５日，第56巻，第9号，p.1706～1715
来間　一郎　他，ＳＤＮによるマルウェア調査のためのネットワーク切り替え手法，電子情報通信学会技術研究報告，２０１４年　6月２６日，第114巻,第118号，p.117～124
栗田　享佳　他，富士通の実践知に基づくセキュリティ対策技術，ＦＵＪＩＴＳＵ，富士通株式会社，２０１５年　1月　1日，第66巻,第1号，p.93～99

(58)調査した分野(Int.Cl.，ＤＢ名)
Ｈ０４Ｌ　　１２／７０