(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2019-92106
(P2019-92106A)
(43)公開日　令和1年6月13日(2019.6.13)

(51)Int.Cl.		F I			テーマコード（参考）
H04L 12/70	(2013.01)	H04L	12/70	100Z	5K030
H04L 12/28	(2006.01)	H04L	12/28	200M	5K033
G06F 21/55	(2013.01)	G06F	21/55		

審査請求 未請求　請求項の数 5　ＯＬ　（全 20 頁）

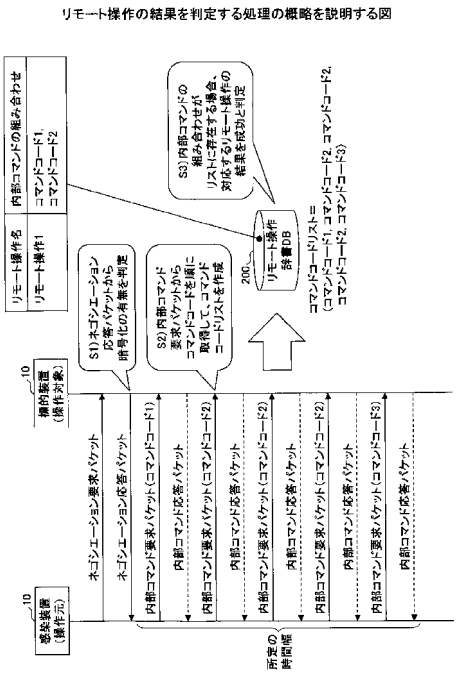
(21)出願番号　特願2017-220985 (P2017-220985)
(22)出願日　平成29年11月16日 (2017.11.16)

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号
(74)代理人　100107766
弁理士　伊東　忠重
(74)代理人　100070150
弁理士　伊東　忠彦
(72)発明者　藤嶌　由紀
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内
(72)発明者　森永　正信
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54)【発明の名称】ネットワーク監視装置、ネットワーク監視方法及びネットワーク監視プログラム

(57)【要約】
【課題】暗号化されたリモート操作の成否を判定する
【解決手段】リモート操作を実現する１以上のコマンドを実行させるための暗号化された実行要求パケットのヘッダから、前記コマンドを示すコマンドコードを取得する取得部と、リモート操作と、１以上のコマンドコードの組み合わせとが対応付けられた記憶部を参照して、前記取得部が取得したコマンドコードのリストに含まれる前記組み合わせが存在するか否かを判定する第１の判定部と、前記第１の判定部により前記組み合わせが存在すると判定された場合、該組み合わせに対応付けられているリモート操作が成功したと判定する第２の判定部と、を有することを特徴とするネットワーク監視装置が提供される。
【選択図】図３



【特許請求の範囲】
【請求項１】
リモート操作を実現する１以上のコマンドを実行させるための暗号化された実行要求パケットのヘッダから、前記コマンドを示すコマンドコードを取得する取得部と、
リモート操作と、１以上のコマンドコードの組み合わせとが対応付けられた記憶部を参照して、前記取得部が取得したコマンドコードのリストに含まれる前記組み合わせが存在するか否かを判定する第１の判定部と、
前記第１の判定部により前記組み合わせが存在すると判定された場合、該組み合わせに対応付けられているリモート操作が成功したと判定する第２の判定部と、
を有することを特徴とするネットワーク監視装置。
【請求項２】
前記取得部は、
前記リモート操作の操作元の装置と、操作対象の装置との間でネゴシエーションが行われてから所定の時間以内に送受信された前記実行要求パケットのヘッダから、前記コマンドコードを取得し、
前記第２の判定部は、
前記所定の時間以内に、前記第１の判定部により前記組み合わせが存在すると判定されなかった場合、リモート操作が失敗したと判定する、ことを特徴とする請求項１に記載のネットワーク監視装置。
【請求項３】
前記ネゴシエーションの応答を示す応答パケットから、前記実行要求パケットが暗号化されるか否かを判定する第３の判定部を有し、
前記取得部は、
前記第３の判定部により前記実行要求パケットが暗号化されると判定された場合、暗号化された前記実行要求パケットのヘッダから、前記コマンドコードを取得する、ことを特徴とする請求項２に記載のネットワーク監視装置。
【請求項４】
リモート操作を実現する１以上のコマンドを実行させるための暗号化された実行要求パケットのヘッダから、前記コマンドを示すコマンドコードを取得し、
リモート操作と、１以上のコマンドコードの組み合わせとが対応付けられた記憶部を参照して、取得したコマンドコードのリストに含まれる前記組み合わせが存在するか否かを判定し、
前記組み合わせが存在すると判定された場合、該組み合わせに対応付けられているリモート操作が成功したと判定する、
処理をコンピュータが実行することを特徴とするネットワーク監視方法。
【請求項５】
リモート操作を実現する１以上のコマンドを実行させるための暗号化された実行要求パケットのヘッダから、前記コマンドを示すコマンドコードを取得し、
リモート操作と、１以上のコマンドコードの組み合わせとが対応付けられた記憶部を参照して、取得したコマンドコードのリストに含まれる前記組み合わせが存在するか否かを判定し、
前記組み合わせが存在すると判定された場合、該組み合わせに対応付けられているリモート操作が成功したと判定する、
処理をコンピュータに実行させることを特徴とするネットワーク監視プログラム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、ネットワーク監視装置、ネットワーク監視方法及びネットワーク監視プログラムに関する。
【背景技術】

【０００２】
サイバー攻撃の一形態として、マルウェアに感染したコンピュータが、標的であるコンピュータをリモート操作することがある。例えば、マルウェアに感染したコンピュータは、不正に窃取した正規のアカウントを用いて、標的であるコンピュータに対してリモート操作を行う。このようなサイバー攻撃を受けた際には、サイバー攻撃に対する対処内容や優先順位を決めるために、リモート操作の成否（成功又は失敗）を特定することが求められる。
【０００３】
これに対して、リモート操作の要求パケットに対する複数の応答パケットのうちの先頭のパケット又は最後のパケットの特定位置に格納されているステータス値を取得することで、リモート操作の成否を特定する技術が知られている。
【先行技術文献】
【特許文献】
【０００４】
【特許文献１】特開２００５－２１６２９１号公報
【特許文献２】特開２０００－１１２８４７号公報
【特許文献３】特開２００６－１９５９８４号公報
【特許文献４】特開２０１０－１５５１３号公報
【発明の概要】
【発明が解決しようとする課題】
【０００５】
ここで、あるコンピュータが他のコンピュータをリモート操作する場合には、操作元のコンピュータと、操作対象のコンピュータとの間で、通信方式や暗号化の有無等を取り決めるためのネゴシエーションが行われる。ネゴシエーションにより通信の暗号化が取り決められると、以降の通信では、要求パケットや応答パケットのデータ部が暗号化される。
【０００６】
したがって、この場合、応答パケットの特定位置に格納されているステータス値からリモート操作の成否を特定することができない。
【０００７】
１つの側面では、本発明は、暗号化されたリモート操作の成否を判定することを目的とする。
【課題を解決するための手段】
【０００８】
１つの態様では、リモート操作を実現する１以上のコマンドを実行させるための暗号化された実行要求パケットのヘッダから、前記コマンドを示すコマンドコードを取得する取得部と、リモート操作と、１以上のコマンドコードの組み合わせとが対応付けられた記憶部を参照して、前記取得部が取得したコマンドコードのリストに含まれる前記組み合わせが存在するか否かを判定する第１の判定部と、前記第１の判定部により前記組み合わせが存在すると判定された場合、該組み合わせに対応付けられているリモート操作が成功したと判定する第２の判定部と、を有することを特徴とする。
【発明の効果】
【０００９】
暗号化されたリモート操作の成否を判定することができる。
【図面の簡単な説明】
【００１０】
【図１】本実施形態に係るネットワーク監視装置が含まれるシステムの全体構成の一例を示す図である。
【図２】本実施形態に係るネットワーク監視装置のハードウェア構成の一例を示す図である。
【図３】リモート操作の結果を判定する処理の概略を説明する図である。

【図４】本実施形態に係るネットワーク監視装置の機能構成の一例を示す図である。
【図５】リモート操作辞書ＤＢの一例を示す図である。
【図６】本実施形態に係るネットワーク監視装置が実行する全体処理の一例を示すフローチャートである。
【図７】ネゴシエーションの判定処理の一例を示すフローチャートである。
【図８】リモート操作判定用情報の一例を示す図である。
【図９】リモート操作の判定処理の一例を示すフローチャートである。
【図１０】コマンドコードが追加されたリモート操作判定用情報の一例を示す図である。
【図１１】リモート操作結果情報の一例を示す図である。
【発明を実施するための形態】
【００１１】
以下、本発明の実施形態について添付の図面を参照しながら説明する。
【００１２】
（全体構成）
まず、本実施形態に係るネットワーク監視装置３０が含まれるシステムの全体構成について、図１を参照しながら説明する。図１は、本実施形態に係るネットワーク監視装置３０が含まれるシステムの全体構成の一例を示す図である。
【００１３】
図１に示すように、例えば会社や団体等の組織のイントラネット等であるシステム環境Ｅには、複数の情報処理装置１０と、収集装置２０と、ネットワーク監視装置３０と、ファイアウォール４０とが含まれる。また、複数の情報処理装置１０と、収集装置２０と、ネットワーク監視装置３０と、ファイアウォール４０とは、例えばＬＡＮ（Local Area Network）等のネットワークＮを介して通信可能に接続されている。
【００１４】
システム環境Ｅにおけるネットワークは、ファイアウォール４０を介してインターネットと接続している。
【００１５】
複数の情報処理装置１０は、例えばサーバ装置やクライアント端末である。サーバ装置は、任意の機能を提供するサーバであり、例えば、ドメイン管理サーバ、Ｗｅｂサーバ、ファイルサーバ、Ｗｉｎｄｏｗｓ（登録商標）サーバ、Ｓａｍｂａサーバ等が挙げられる。クライアント端末は、任意の端末であり、例えばデスクトップＰＣ、ノート型ＰＣ、タブレット端末等が挙げられる。
【００１６】
ここで、クライアント端末は、サーバ装置が提供する機能を利用することもあれば、クライアント端末同士で処理の連携やデータ共有、各種機能の提供等を行うこともあるものとする。また、サーバ装置が他のサーバ装置と処理の連携等を行うこともあるものとする。すなわち、情報処理装置１０同士は、所定の条件の下で、任意にリモート操作を行うことがあるものとする。このようなリモート操作を行うために、複数の情報処理装置１０の間では、例えばＳＭＢ（Server Message Block）やＲＰＣ（Remote Procedure Call）が用いられる。ＳＭＢやＲＰＣは、リモート操作を行うためのアプリケーション層のプロトコルの一例である。
【００１７】
収集装置２０は、パケットの複製（ミラーリング）機能を有するネットワーク・スイッチやタップ等である。収集装置２０は、複数の情報処理装置１０間のリモート操作に関するパケットを収集する。そして、収集装置２０は、収集したパケットをネットワーク監視装置３０に転送する。
【００１８】
ネットワーク監視装置３０は、例えばＲＡＴ（Remote Administration Tool又はRemote Access Tool）等の標的型攻撃を行うマルウェアに感染した情報処理装置１０が他の情報処理装置１０に行ったリモート操作の成否を判定するコンピュータである。

【００１９】
ＲＡＴ等の標的型攻撃を行うマルウェアは、例えば、標的型メールや不正サイト等を介して、システム環境Ｅ内の情報処理装置１０に送り込まれる。このようなマルウェアに情報処理装置１０が感染した場合、当該情報処理装置１０は、例えば、システム環境Ｅの外にあるＣ＆Ｃ（Command and Control）サーバ５０の指示を受けて、他の情報処理装置１０に対して不正なリモート操作を行う。以降では、ＲＡＴ等の標的型攻撃を行うマルウェアに感染した情報処理装置１０を「感染装置１０」、感染装置１０から不正なリモート操作が行われる情報処理装置１０を「標的装置１０」と表す。なお、マルウェアに感染した情報処理装置１０の検知は従来技術を用いて行うことができる。
【００２０】
感染装置１０による不正なリモート操作としては、例えば、標的装置１０に対して様々なスキャンを行って、顧客情報等の機密情報を収集した上で、攻撃者のＰＣ等に転送する操作が挙げられる。また、例えば、マルウェアの感染を拡大させるために、マルウェアの複製を標的装置１０に送り込む操作が挙げられる。これら以外にも、例えば、標的装置１０に格納されている情報を改ざんや削除する操作等も挙げられる。
【００２１】
ここで、リモート操作は、一般に、１以上のコマンドが実行されることにより実現される。例えば、マルウェアを標的装置１０に送り込むための操作では、標的装置１０の感染対象のファイルをオープンするためのコマンドと、マルウェアを所定のバイト単位でファイルに書き込むための１以上のコマンドと、ファイルをクローズするためのコマンドとが実行されることにより実現される。以降では、リモート操作を実現する１以上のコマンドそれぞれを「内部コマンド」と表す。
【００２２】
したがって、リモート操作は、１以上の内部コマンドの実行をそれぞれ要求するためのパケット（以降では、「内部コマンド要求パケット」と表す。）が感染装置１０から標的装置１０に送信されることで行われる。
【００２３】
ネットワーク監視装置３０は、ネットワーク監視プログラム１００と、リモート操作辞書ＤＢ２００とを有する。ネットワーク監視プログラム１００は、リモート操作が成功する場合における特徴的な内部コマンドの組み合わせに関する情報が格納されたリモート操作辞書ＤＢ２００を参照して、暗号化されている内部コマンド要求パケットからリモート操作の成否を判定する。
【００２４】
特徴的な内部コマンドの組み合わせとは、リモート操作が成功する場合には少なくとも実行される内部コマンドの組み合わせのことである。例えば、リモート操作が「ファイルの書込み」操作である場合、当該操作は、ファイルをオープンするためのコマンドと、データを所定のバイト単位でファイルに書き込むための１以上のコマンドと、ファイルをクローズするためのコマンドとが実行される。このとき、「ファイルの書込み」操作が成功する場合、ファイルをオープンするためのコマンドと、データを所定のバイト単位でファイルに書き込むための１以上のコマンドとが少なくとも実行される。したがって、「ファイルの書込み」操作が成功する場合における特徴的な内部コマンドの組み合わせには、ファイルをオープンするためのコマンドと、データを所定のバイト単位でファイルに書き込むためのコマンドとの組み合わせが挙げられる。
【００２５】
感染装置１０から標的装置１０へのリモート操作の成否が判定されることで、例えばシステム環境Ｅのセキュリティ管理者等は、不正なリモート操作に対する対処内容やその優先順位を決める際の参考にすることができる。例えば、感染装置１０から標的装置１０へマルウェアを送り込むための操作が成功している場合、感染の拡大を防止するために、感染装置１０をネットワークから隔離する等の対処を行うことができる。
【００２６】

なお、図１示すシステムの構成は一例であって、他の構成であっても良い。例えば、収集装置２０とネットワーク監視装置３０とが一体で構成されていても良い。

【００２７】

（ハードウェア構成）

次に、本実施形態に係るネットワーク監視装置３０のハードウェア構成について、図２を参照しながら説明する。図２は、本実施形態に係るネットワーク監視装置３０のハードウェア構成の一例を示す図である。

【００２８】

図２に示すように、本実施形態に係るネットワーク監視装置３０は、入力装置１１と、表示装置１２と、外部Ｉ／Ｆ１３と、通信Ｉ／Ｆ１４とを有する。また、本実施形態に係るネットワーク監視装置３０は、ＲＯＭ（Read Only Memory）１５と、ＲＡＭ（Random Access Memory）１６と、ＣＰＵ（Central Processing Unit）１７と、補助記憶装置１８とを有する。これら各ハードウェアは、それぞれがバス１９で相互に接続されている。

【００２９】

入力装置１１は、例えばキーボードやマウス、タッチパネル等であり、ネットワーク監視装置３０に各種の操作信号を入力するのに用いられる。表示装置１２は、例えばディスプレイ等であり、ネットワーク監視装置３０による各種の処理結果を表示する。なお、ネットワーク監視装置３０は、入力装置１１及び表示装置１２の少なくとも一方を有していなくても良い。

【００３０】

外部Ｉ／Ｆ１３は、外部装置とのインタフェースである。外部装置には、記録媒体１３ａ等がある。ネットワーク監視装置３０は、外部Ｉ／Ｆ１３を介して、記録媒体１３ａの読み取りや書き込みを行うことができる。

【００３１】

記録媒体１３ａには、例えば、ＳＤメモリカード(SD memory card）やＵＳＢ（Universal Serial Bus）メモリ、ＣＤ（Compact Disk）、ＤＶＤ（Digital Versatile Disk）等がある。

【００３２】

通信Ｉ／Ｆ１４は、ネットワーク監視装置３０がネットワークに接続するためのインタフェースである。ネットワーク監視装置３０は、通信Ｉ／Ｆ１４を介して、収集装置２０から転送されたパケットを受信することができる。

【００３３】

ＲＯＭ１５は、電源を切ってもデータを保持することができる不揮発性の半導体メモリである。ＲＡＭ１６は、プログラムやデータを一時保持する揮発性の半導体メモリである。ＣＰＵ１７は、例えば補助記憶装置１８やＲＯＭ１５等からプログラムやデータをＲＡＭ１６上に読み出して、各種処理を実行する演算装置である。

【００３４】

補助記憶装置１８は、例えばＨＤＤ（Hard Disk Drive）やＳＳＤ（Solid State Drive）等であり、プログラムやデータを格納している不揮発性のメモリである。補助記憶装置１８には、例えば、基本ソフトウェアであるＯＳ（Operating System）や各種アプリケーションプログラム、ネットワーク監視プログラム１００等が格納される。

【００３５】

本実施形態に係るネットワーク監視装置３０は、図２に示すハードウェア構成を有することにより、後述する各種処理が実現される。

【００３６】

（処理の概略）

次に、感染装置１０から標的装置１０へのリモート操作の結果をネットワーク監視装置３０が判定する処理の概要について、図３を参照しながら説明する。図３は、リモート操作の結果を判定する処理の概略を説明する図である。なお、図３における各種パケット（

例えば、ネゴシエーション要求パケット、ネゴシエーション応答パケット、内部コマンド要求パケット及び内部コマンド応答パケット等）は、収集装置２０からネットワーク監視装置３０へ転送される。

【００３７】

Ｓ１）感染装置１０と標的装置１０との間では、リモート操作に先立ってネゴシエーションが行われる。すなわち、感染装置１０は、操作対象である標的装置１０に対してネゴシエーション要求パケットを送信する。一方で、標的装置１０は、ネゴシエーション要求パケットを受信すると、操作元の感染装置１０に対してネゴシエーション応答パケットを送信する。ネゴシエーション応答パケットには、感染装置１０と標的装置１０との間で用いられる通信方式や通信が暗号化される場合における暗号化方式等が含まれる。

【００３８】

そこで、ネットワーク監視装置３０は、ネゴシエーション応答パケットから暗号化の有無を判定する。例えば、ネゴシエーション応答パケットに暗号化方式が含まれる場合には、通信が暗号化されると判定される。一方で、ネゴシエーション応答パケットに暗号化方式が含まれない場合は、通信が暗号化されないと判定される。なお、暗号化の有無は、例えば、ＯＳやリモート操作の種類等に応じて決定される。

【００３９】

通信が暗号化されると判定された場合は、ネゴシエーション以降に送受信される内部コマンド要求パケット及び内部コマンド応答パケットのデータ部が所定の暗号化方式で暗号化される。以降では、通信が暗号化されると判定されたものとする。

【００４０】

Ｓ２）感染装置１０と標的装置１０との間では、リモート操作に応じた１以上の内部コマンド要求パケットと、当該内部コマンド要求に対する内部コマンド応答パケットとが送受信される。ここで、感染装置１０から標的装置１０に送信される内部コマンド要求パケットのヘッダ部は、暗号化されない。

【００４１】

そこで、ネットワーク監視装置３０は、所定の時間幅における内部コマンド要求パケットのヘッダ部に含まれるコマンドコードを順に取得して、コマンドコードリストを作成する。コマンドコードとは、コマンドを識別する識別情報であり、例えば、コマンド名やコマンドＩＤ等が挙げられる。

【００４２】

例えば、「コマンドコード１」が含まれる内部コマンド要求パケットと、「コマンドコード２」が含まれる３つの内部コマンド要求パケットと、「コマンドコード３」が含まれる内部コマンド要求パケットとが感染装置１０から標的装置１０に送信されたものとする。この場合、コマンドコードリスト「コマンドコード１，コマンドコード２，コマンドコード２，コマンドコード２，コマンドコード３」が作成される。

【００４３】

なお、所定の時間幅は、例えば、１つのリモート操作に要すると想定される時間幅であり、セキュリティ管理者等により予め設定される。

【００４４】

Ｓ３）ネットワーク監視装置３０は、リモート操作辞書ＤＢ２００に格納されている内部コマンドの組み合わせのうち、上記のＳ２で作成されたコマンドコードリストに含まれる内部コマンドの組み合わせが存在するか否かを判定する。そして、ネットワーク監視装置３０は、コマンドコードリストに含まれる内部コマンドの組み合わせが存在すると判定した場合、当該組み合わせに対応するリモート操作名のリモート操作が成功したものと判定する。

【００４５】

例えば、リモート操作名「リモート操作１」と、内部コマンドの組み合わせ「コマンドコード１，コマンドコード２」とが対応付けられてリモート操作辞書ＤＢ２００に格納されているものとする。この場合、「コマンドコード１」及び「コマンドコード２」は、こ

の順で、コマンドコードリスト「コマンドコード１，コマンドコード２，コマンドコード２，コマンドコード２，コマンドコード３」に含まれる。したがって、ネットワーク監視装置３０は、当該内部コマンドの組み合わせに対応付けられているリモート操作名「リモート操作１」のリモート操作が成功したものと判定する。

【００４６】

以上のように、本実施形態に係るネットワーク監視装置３０は、リモート操作を行うための内部コマンド要求パケットのヘッダ部からコマンドコードを取得することで、コマンドコードリストを作成する。そして、本実施形態に係るネットワーク監視装置３０は、リモート操作に含まれる特徴的なコマンドのコマンドコードの組み合わせがコマンドコードリストの中に含まれる場合に、当該リモート操作を成功したものと判定する。これにより、本実施形態に係るネットワーク監視装置３０は、感染装置１０と標的装置１０との間のリモート操作に関する通信が暗号化されている場合であっても、リモート操作の成否を特定することができるようになる。

【００４７】

なお、上記のＳ１で通信が暗号化されないと判定された場合、内部コマンド要求パケット及び内部コマンド応答パケットのデータ部は暗号化されない。したがって、この場合、従来技術を用いて、例えば、最初の内部コマンド応答パケット又は最後の内部コマンド応答パケットの特定位置に格納されているステータス値からリモート操作の成否を判定すれば良い。

【００４８】

（機能構成）

次に、本実施形態に係るネットワーク監視装置３０の機能構成について、図４を参照しながら説明する。図４は、本実施形態に係るネットワーク監視装置３０の機能構成の一例を示す図である。

【００４９】

図４に示すように、本実施形態に係るネットワーク監視装置３０は、受信部１０１と、パケット判定部１０２と、ネゴシエーション判定処理部１０３と、リモート操作判定処理部１０４とを有する。これら各機能部は、ネットワーク監視プログラム１００がＣＰＵ１７に実行させる処理により実現される。

【００５０】

また、本実施形態に係るネットワーク監視装置３０は、リモート操作辞書ＤＢ２００を有する。当該ＤＢは、例えば補助記憶装置１８を用いて実現可能である。なお、当該ＤＢは、ネットワーク監視装置３０とネットワークを介して接続される記憶装置等を用いて実現されていても良い。

【００５１】

受信部１０１は、収集装置２０から転送された各種パケット（例えば、ネゴシエーション要求パケット、ネゴシエーション応答パケット、内部コマンド要求パケット及び内部コマンド応答パケット等）を受信する。

【００５２】

パケット判定部１０２は、受信部１０１が受信したパケットがネゴシエーション応答パケットであるか否かを判定する。また、パケット判定部１０２は、受信部１０１が受信したパケットが内部コマンド要求パケットであるか否かを判定する。

【００５３】

ネゴシエーション判定処理部１０３は、パケット判定部１０２がネゴシエーション応答パケットを受信したと判定した場合、リモート操作に関する通信の暗号化有無の判定や空のコマンドコードリストの作成等の処理を行う。ここで、ネゴシエーション判定処理部１０３は、取得部１１１と、暗号化判定部１１２と、判定用情報作成部１１３とを有する。

【００５４】

取得部１１１は、受信部１０１が受信したネゴシエーション応答パケットから所定の情報（例えば、時刻、送信元ＩＰ（Internet Protocol）アドレス、送信元ポート番号、宛

先ＩＰアドレス、宛先ポート番号、暗号化方式等）を取得する。
【００５５】
第３の判定部の一例として、暗号化判定部１１２は、ネゴシエーション以降の通信（すなわち、内部コマンド要求パケット及び内部コマンド応答パケット）の暗号化有無を判定する。
【００５６】
判定用情報作成部１１３は、暗号化判定部１１２によりネゴシエーション以降の通信が暗号化されると判定された場合、空のコマンドコードリストが含まれるリモート操作判定用情報１０００を作成する。リモート操作判定用情報１０００の詳細については後述する。
【００５７】
リモート操作判定処理部１０４は、パケット判定部１０２が内部コマンド要求パケットを受信したと判定した場合、リモート操作の成否を判定するための処理を行う。ここで、リモート操作判定処理部１０４は、取得部１２１と、リスト追加部１２２と、時間判定部１２３と、結果判定部１２４と、結果作成部１２５とを有する。
【００５８】
取得部１２１は、受信部１０１が受信した内部コマンド要求パケットのヘッダ部から所定の情報（例えば、時刻、送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス、宛先ポート番号、コマンドコード等）を取得する。
【００５９】
リスト追加部１２２は、取得部１２１が取得したコマンドコードを、リモート操作判定用情報１０００のコマンドコードリストに追加する。
【００６０】
時間判定部１２３は、受信部１０１が受信した内部コマンド要求パケットが、ネゴシエーションから所定の時間幅以内であるか否かを判定する。
【００６１】
第１の判定部の一例として、結果判定部１２４は、時間判定部１２３が所定の時間幅以内であると判定した場合、リモート操作辞書ＤＢ２００を参照して、コマンドコードリストに含まれる内部コマンドの組み合わせが存在するか否かを判定する。
【００６２】
第２の判定部の一例として、結果作成部１２５は、結果判定部１２４がコマンドコードリストに含まれる内部コマンドの組み合わせが存在すると判定した場合、当該内部コマンドの組み合わせに対応するリモート操作が成功したことを示すリモート操作結果情報２０００を作成する。一方で、結果作成部１２５は、時間判定部１２３が所定の時間幅以内でないと判定した場合、リモート操作が失敗したことを示すリモート操作結果情報２０００を作成する。
【００６３】
なお、結果作成部１２５により作成されたリモート操作結果情報２０００は、例えば、補助記憶装置１８等における所定の記憶領域に記憶される。
【００６４】
リモート操作辞書ＤＢ２００は、リモート操作毎に、当該リモート操作が成功する場合における特徴的な内部コマンドの組み合わせに関する情報が格納されている。ここで、リモート操作辞書ＤＢ２００について、図５を参照しながら説明する。図５は、リモート操作辞書ＤＢ２００の一例を示す図である。
【００６５】
図５に示すように、リモート操作辞書ＤＢ２００では、リモート操作名と、内部コマンドの組み合わせとが対応付けられている。
【００６６】
例えば、リモート操作名「リモート操作１」には、内部コマンドの組み合わせ「コマンドコード１，コマンドコード２」が対応付けられている。これは、リモート操作名「リモ

ート操作１」のリモート操作が成功する場合には、少なくとも「コマンドコード１」の内部コマンドと、「コマンドコード２」の内部コマンドとが、この順に実行されることを示している。

【００６７】

同様に、例えば、リモート操作名「リモート操作２」には、内部コマンドの組み合わせ「コマンドコード６，コマンドコード８，コマンドコード１０」が対応付けられている。これは、リモート操作名「リモート操作２」のリモート操作が成功する場合には、少なくとも「コマンドコード６」の内部コマンドと、「コマンドコード８」の内部コマンドと、「コマンドコード１０」の内部コマンドとが、この順に実行されることを示している。

【００６８】

なお、図５に示す例では、リモート操作名と、内部コマンドの組み合わせとが対応付けられているが、例えば、リモート操作ＩＤ等のリモート操作を識別する識別情報と、内部コマンドの組み合わせとが対応付けられていても良い。

【００６９】

（全体処理）

次に、本実施形態に係るネットワーク監視装置３０が実行する全体処理について、図６を参照しながら説明する。図６は、本実施形態に係るネットワーク監視装置３０が実行する全体処理の一例を示すフローチャートである。以降で説明する全体処理は、収集装置２０からパケットが転送される度に実行される。

【００７０】

まず、受信部１０１は、収集装置２０から転送されたパケットを受信する（ステップＳ１０１）。

【００７１】

次に、パケット判定部１０２は、受信部１０１が受信したパケットがネゴシエーション応答パケットであるか否かを判定する（ステップＳ１０２）。

【００７２】

ステップＳ１０２において、受信部１０１により受信されたパケットがネゴシエーション応答パケットであると判定された場合、ネゴシエーション判定処理部１０３は、ネゴシエーション判定処理を行う（ステップＳ１０３）。ネゴシエーション判定処理では、リモート操作に関する通信の暗号化有無の判定やリモート操作判定用情報１０００の作成等が行われる。ネゴシエーション判定処理の詳細については後述する。

【００７３】

ステップＳ１０２において、受信部１０１により受信されたパケットがネゴシエーション応答パケットでないと判定された場合、パケット判定部１０２は、当該パケットが内部コマンド要求パケットであるか否かを判定する（ステップＳ１０４）。

【００７４】

ステップＳ１０４において、受信部１０１により受信されたパケットが内部コマンド要求パケットであると判定された場合、リモート操作判定処理部１０４は、リモート操作の判定処理を行う（ステップＳ１０５）。リモート操作の判定処理では、リモート操作の成否が判定される。リモート操作の判定処理の詳細については後述する。

【００７５】

なお、ステップＳ１０４において、受信部１０１により受信されたパケットが内部コマンド要求パケットでないと判定された場合、ネットワーク監視装置３０は、処理を終了する。

【００７６】

（ネゴシエーションの判定処理）

次に、図６のステップＳ１０３におけるネゴシエーションの判定処理の詳細について、図７を参照しながら説明する。図７は、ネゴシエーションの判定処理の一例を示すフローチャートである。

【００７７】

まず、ネゴシエーション判定処理部１０３の取得部１１１は、受信部１０１が受信したネゴシエーション応答パケットから所定の情報を取得する（ステップＳ２０１）。取得部１１１により取得される所定の情報としては、例えば、時刻、送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス、宛先ポート番号、及び暗号化方式等が挙げられる。

【００７８】

次に、ネゴシエーション判定処理部１０３の暗号化判定部１１２は、ネゴシエーション以降の通信の暗号化有無を判定する（ステップＳ２０２）。暗号化判定部１１２は、例えば、取得部１１１により何等かの暗号化方式がネゴシエーション応答パケットから取得された場合に、ネゴシエーション以降の通信が暗号化されると判定すれば良い。一方で、暗号化判定部１１２は、例えば、取得部１１１により暗号化方式がネゴシエーション応答パケットから取得されなかった場合（又は暗号化方式としてＮＵＬＬ値等が取得された場合）に、ネゴシエーション以降の通信は暗号化されないと判定すれば良い。

【００７９】

ステップＳ２０２において、ネゴシエーション以降の通信が暗号化されると判定された場合、ネゴシエーション判定処理部１０３の判定用情報作成部１１３は、空のコマンドコードリストが含まれるリモート操作判定用情報１０００を作成する（ステップＳ２０３）。

【００８０】

ここで、判定用情報作成部１１３により作成されるリモート操作判定用情報１０００について、図８を参照しながら説明する。図８は、リモート操作判定用情報１０００の一例を示す図である。

【００８１】

図８に示すように、リモート操作判定用情報１０００には、時刻と、送信元ＩＰアドレスと、宛先ＩＰアドレスと、宛先ポート番号と、暗号化方式と、コマンドコードリストとが含まれる。

【００８２】

判定用情報作成部１１３により作成されたリモート操作判定用情報１０００の時刻、送信元ＩＰアドレス、宛先ＩＰアドレス、宛先ポート番号及び暗号化方式には、上記のステップＳ２０１で取得部１１１により取得された情報が設定される。また、判定用情報作成部１１３により作成されたリモート操作判定用情報１０００のコマンドコードリストには、例えばＮＵＬＬ値が設定される。すなわち、判定用情報作成部１１３により作成されたリモート操作判定用情報１０００には、空のコマンドコードリストが含まれる。

【００８３】

このように、判定用情報作成部１１３は、空のコマンドコードリストが含まれるリモート操作判定用情報１０００を作成する。判定用情報作成部１１３により作成されたリモート操作判定用情報１０００は、例えば、ＲＡＭ１６や補助記憶装置１８等における所定の記憶領域に記憶される。

【００８４】

なお、ステップＳ２０２において、ネゴシエーション以降の通信が暗号化されないと判定された場合、ネゴシエーション判定処理部１０３は、処理を終了する。この場合、内部コマンド応答パケットのデータ部は暗号化されないため、従来技術を用いて、例えば、最初の内部コマンド応答パケット又は最後の内部コマンド応答パケットの特定位置に格納されているステータス値からリモート操作の成否を判定すれば良い。

【００８５】

（リモート操作の判定処理）

次に、図６のステップＳ１０５におけるリモート操作の判定処理の詳細について、図９を参照しながら説明する。図９は、リモート操作の判定処理の一例を示すフローチャートである。

【００８６】

まず、リモート操作判定処理部１０４の取得部１２１は、受信部１０１が受信した内部

コマンド要求パケットのヘッダ部から所定の情報を取得する（ステップＳ３０１）。取得部１２１により取得される所定の情報としては、例えば、時刻、送信元ＩＰアドレス、送信元ポート番号、宛先ＩＰアドレス、宛先ポート番号、及びコマンドコード等が挙げられる。

【００８７】

次に、リモート操作判定処理部１０４のリスト追加部１２２は、該当のリモート操作判定用情報１０００があるか否かを判定する（ステップＳ３０２）。すなわち、リスト追加部１２２は、取得部１２１により取得された送信元ＩＰアドレスと、送信元ポート番号と、宛先ＩＰアドレスと、宛先ポート番号とが含まれるリモート操作判定用情報１０００が存在するか否かを判定する。

【００８８】

ステップＳ３０２において、該当のリモート操作判定用情報１０００があると判定された場合、リスト追加部１２２は、当該リモート操作判定用情報１０００のコマンドコードリストに対して、取得部１２１が取得したコマンドコードを追加する（ステップＳ３０３）。

【００８９】

ここで、コマンドコードリストにコマンドコードが追加されたリモート操作判定用情報１０００を図１０に示す。図１０に示す例では、リモート操作判定用情報１０００のコマンドコードリストに「コマンドコード１」、「コマンドコード２」、及び「コマンドコード２」等が追加されている。このように、リスト追加部１２２は、該当のリモート操作判定用情報１０００のコマンドコードリストに、取得部１２１により取得されたコマンドコードを順に追加する。

【００９０】

次に、リモート操作判定処理部１０４の時間判定部１２３は、受信部１０１が受信した内部コマンド要求パケットが、ネゴシエーションから所定の時間幅以内であるか否かを判定する（ステップＳ３０４）。すなわち、時間判定部１２３は、取得部１２１により取得された時刻が、該当のリモート操作判定用情報１０００に含まれる時刻から所定の時間幅以内であるか否かを判定する。

【００９１】

ステップＳ３０４において、所定の時間幅以内であると判定された場合、リモート操作判定処理部１０４の結果判定部１２４は、コマンドコードリストに含まれる内部コマンドの組み合わせがリモート操作辞書ＤＢ２００に存在するか否かを判定する（ステップＳ３０５）。すなわち、結果判定部１２４は、リモート操作辞書ＤＢ２００に格納されている内部コマンドの組み合わせの中に、順序を保ったまま、該当のリモート操作判定用情報１０００のコマンドコードリストに含まれるものが存在するか否かを判定する。

【００９２】

例えば、当該リモート操作判定用情報１０００のコマンドコードリストが「コマンドコード１」、「コマンドコード２」、「コマンドコード２」であったとする。この場合、図５に示すリモート操作辞書ＤＢ２００に格納されている内部コマンドの組み合わせ「コマンドコード１，コマンドコード２」がこの順にコマンドコードリストに含まれる。したがって、この場合、結果判定部１２４は、コマンドコードリストに含まれる内部コマンドの組み合わせがリモート操作辞書ＤＢ２００に存在すると判定する。

【００９３】

また、例えば、当該リモート操作判定用情報１０００のコマンドコードリストが「コマンドコード６」、「コマンドコード７」、「コマンドコード８」、「コマンドコード９」、「コマンドコード１０」であったとする。この場合、図５に示すリモート操作辞書ＤＢ２００に格納されている内部コマンドの組み合わせ「コマンドコード６，コマンドコード８，コマンドコード１０」がこの順にコマンドコードリストに含まれる。したがって、この場合、結果判定部１２４は、コマンドコードリストに含まれる内部コマンドの組み合わせがリモート操作辞書ＤＢ２００に存在すると判定する。

【００９４】
ステップＳ３０５において、コマンドコードリストに含まれる内部コマンドの組み合わせが存在すると判定された場合、リモート操作判定処理部１０４の結果作成部１２５は、当該内部コマンドの組み合わせに対応するリモート操作が成功したことを示すリモート操作結果情報２０００を作成する（ステップＳ３０６）。
【００９５】
例えば、内部コマンドの組み合わせ「コマンドコード１，コマンドコード２」がコマンドコードに含まれると判定されたものとする。この場合、結果作成部１２５は、当該内部コマンドの組み合わせに対応するリモート操作名「リモート操作１」のリモート操作が成功したことを示すリモート操作結果情報２０００を作成する。
【００９６】
また、例えば、内部コマンドの組み合わせ「コマンドコード６，コマンドコード８，コマンドコード１０」がコマンドコードに含まれると判定されたものとする。この場合、結果作成部１２５は、当該内部コマンドの組み合わせに対応するリモート操作名「リモート操作２」のリモート操作が成功したことを示すリモート操作結果情報２０００を作成する。
【００９７】
ここで、リモート操作が成功したことを示すリモート操作結果情報２０００を図１１（ａ）に示す。図１１（ａ）に示すように、リモート操作が成功したことを示すリモート操作結果情報２０００には、時刻と、送信元ＩＰアドレスと、宛先ＩＰアドレスと、宛先ポート番号と、リモート操作名と、リモート操作結果とが含まれる。
【００９８】
リモート操作が成功したことを示すリモート操作結果情報２０００の時刻、送信元ＩＰアドレス、宛先ＩＰアドレス、及び宛先ポート番号には、リモート操作判定用情報１０００と同様の情報が設定される。また、リモート操作が成功したことを示すリモート操作結果情報２０００のリモート操作名には、コマンドコードリストに含まれると判定された内部コマンドの組み合わせに対応するリモート操作名が設定される。当該リモート操作名は、リモート操作辞書ＤＢ２００から取得される。更に、リモート操作が成功したことを示すリモート操作結果情報２０００のリモート操作結果には、「成功」が設定される。
【００９９】
このように、結果作成部１２５は、リモート操作名と、当該リモート操作が成功したことを示す結果とが含まれるリモート操作結果情報２０００を作成する。結果作成部１２５により作成されたリモート操作結果情報２０００は、例えば、補助記憶装置１８等における所定の記憶領域に記憶される。
【０１００】
一方で、ステップＳ３０４において、所定の時間幅以内でないと判定された場合、リモート操作判定処理部１０４の結果作成部１２５は、リモート操作が失敗したことを示すリモート操作結果情報２０００を作成する（ステップＳ３０７）。
【０１０１】
ここで、リモート操作が失敗したことを示すリモート操作結果情報２０００を図１１（ｂ）に示す。図１１（ｂ）に示すように、リモート操作が失敗したことを示すリモート操作結果情報２０００には、時刻と、送信元ＩＰアドレスと、宛先ＩＰアドレスと、宛先ポート番号と、リモート操作名と、リモート操作結果と、コマンドコードリストとが含まれる。なお、リモート操作名を特定できない場合、リモート操作が失敗したことを示すリモート操作結果情報２０００には、リモート操作名は含まれない。一方で、リモート操作名を特定できた場合には、リモート操作名が含まれる。
【０１０２】
リモート操作が失敗したことを示すリモート操作結果情報２０００の時刻、送信元ＩＰアドレス、宛先ＩＰアドレス、及び宛先ポート番号には、リモート操作判定用情報１０００と同様の情報が設定される。また、リモート操作が失敗したことを示すリモート操作結

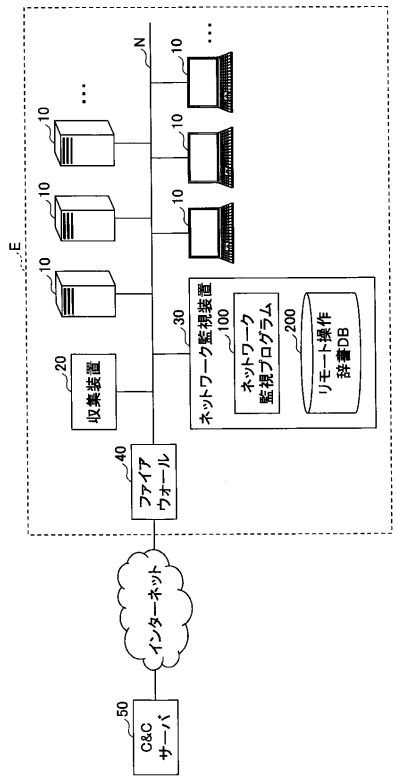
果情報２０００のリモート操作結果には、「失敗」が設定される。
【０１０３】
更に、リモート操作が失敗したことを示すリモート操作結果情報２０００のコマンドコードリストには、リモート操作判定用情報１０００と同様の情報が設定される。リモート操作が失敗したことを示すリモート操作結果情報２０００にコマンドコードリストが含まれることで、例えばシステム環境Ｅのセキュリティ管理者等は、失敗したリモート操作について、どこまでのコマンドが実行されたのかを知ることができる。
【０１０４】
このように、結果作成部１２５は、リモート操作が失敗したことを示す結果と、当該リモート操作で実行されるコマンドのリストとが含まれるリモート操作結果情報２０００を作成する。結果作成部１２５により作成されたリモート操作結果情報２０００は、例えば、補助記憶装置１８等における所定の記憶領域に記憶される。
【０１０５】
なお、ステップＳ３０２において、該当のリモート操作判定用情報１０００がないと判定された場合、リモート操作判定処理部１０４は、処理を終了する。同様に、ステップＳ３０５において、コマンドコードリストに含まれる内部コマンドの組み合わせがリモート操作辞書ＤＢ２００に存在しないと判定された場合、リモート操作判定処理部１０４は、処理を終了する。
【０１０６】
（まとめ）
以上のように、本実施形態に係るネットワーク監視装置３０は、感染装置１０と標的装置１０との間のネゴシエーションから通信の暗号化の有無を判定する。また、本実施形態に係るネットワーク監視装置３０は、通信が暗号化されている場合、リモート操作で実行されるコマンドの要求パケットのヘッダ部から順にコマンドコードを取得する。そして、本実施形態に係るネットワーク監視装置３０は、取得したコマンドコードの組み合わせがリモート操作辞書ＤＢ２００に格納されている場合に、当該組み合わせに対応するリモート操作が成功したものと判定する。
【０１０７】
これにより、本実施形態に係るネットワーク監視装置３０は、通信が暗号化されている場合であっても、感染装置１０が標的装置１０に行ったリモート操作の成否を特定することができる。
【０１０８】
リモート操作の成否を知ることで、例えばシステム環境Ｅのセキュリティ管理者等は、感染装置１０から標的装置１０への不正なリモート操作に対する対処内容やその優先順位を決める際の参考にすることができる。
【０１０９】
なお、図１１（ａ）及び図１１（ｂ）に示すリモート操作結果情報２０００には、例えば、標的装置１０へのリモート操作に用いられたアカウント名や感染装置１０が当該リモート操作に用いたサービス名、操作対象のファイル名等の情報が含まれていても良い。これにより、例えばシステム環境Ｅのセキュリティ管理者等は、これらのアカウント名やサービス名、ファイル名等の情報を参考して、不正なリモート操作に対する対処内容やその優先順位を決めることができるようになる。
【０１１０】
以上、本発明の実施形態について詳述したが、本発明は斯かる特定の実施形態に限定されるものではなく、特許請求の範囲に記載された本発明の要旨の範囲内において、種々の変形・変更が可能である。
【０１１１】
以上の説明に関し、更に以下の項を開示する。
（付記１）
リモート操作を実現する１以上のコマンドを実行させるための暗号化された実行要求パ

ケットのヘッダから、前記コマンドを示すコマンドコードを取得する取得部と、
リモート操作と、１以上のコマンドコードの組み合わせとが対応付けられた記憶部を参照して、前記取得部が取得したコマンドコードのリストに含まれる前記組み合わせが存在するか否かを判定する第１の判定部と、
前記第１の判定部により前記組み合わせが存在すると判定された場合、該組み合わせに対応付けられているリモート操作が成功したと判定する第２の判定部と、
を有することを特徴とするネットワーク監視装置。
（付記２）
前記取得部は、
前記リモート操作の操作元の装置と、操作対象の装置との間でネゴシエーションが行われてから所定の時間以内に送受信された前記実行要求パケットのヘッダから、前記コマンドコードを取得し、
前記第２の判定部は、
前記所定の時間以内に、前記第１の判定部により前記組み合わせが存在すると判定されなかった場合、リモート操作が失敗したと判定する、ことを特徴とする付記１に記載のネットワーク監視装置。
（付記３）
前記ネゴシエーションの応答を示す応答パケットから、前記実行要求パケットが暗号化されるか否かを判定する第３の判定部を有し、
前記取得部は、
前記第３の判定部により前記実行要求パケットが暗号化されると判定された場合、暗号化された前記実行要求パケットのヘッダから、前記コマンドコードを取得する、ことを特徴とする付記２に記載のネットワーク監視装置。
（付記４）
リモート操作を実現する１以上のコマンドを実行させるための暗号化された実行要求パケットのヘッダから、前記コマンドを示すコマンドコードを取得し、
リモート操作と、１以上のコマンドコードの組み合わせとが対応付けられた記憶部を参照して、取得したコマンドコードのリストに含まれる前記組み合わせが存在するか否かを判定し、
前記組み合わせが存在すると判定された場合、該組み合わせに対応付けられているリモート操作が成功したと判定する、
処理をコンピュータが実行することを特徴とするネットワーク監視方法。
（付記５）
前記リモート操作の操作元の装置と、操作対象の装置との間でネゴシエーションが行われてから所定の時間以内に送受信された前記実行要求パケットのヘッダから、前記コマンドコードを取得し、
前記所定の時間以内に、前記組み合わせが存在すると判定されなかった場合、リモート操作が失敗したと判定する、ことを特徴とする付記４に記載のネットワーク監視方法。
（付記６）
前記ネゴシエーションの応答を示す応答パケットから、前記実行要求パケットが暗号化されるか否かを判定し、
前記実行要求パケットが暗号化されると判定された場合、暗号化された前記実行要求パケットのヘッダから、前記コマンドコードを取得する、ことを特徴とする付記５に記載のネットワーク監視方法。
（付記７）
リモート操作を実現する１以上のコマンドを実行させるための暗号化された実行要求パケットのヘッダから、前記コマンドを示すコマンドコードを取得し、
リモート操作と、１以上のコマンドコードの組み合わせとが対応付けられた記憶部を参照して、取得したコマンドコードのリストに含まれる前記組み合わせが存在するか否かを判定し、

前記組み合わせが存在すると判定された場合、該組み合わせに対応付けられているリモート操作が成功したと判定する、
処理をコンピュータに実行させることを特徴とするネットワーク監視プログラム。
（付記８）
前記リモート操作の操作元の装置と、操作対象の装置との間でネゴシエーションが行われてから所定の時間以内に送受信された前記実行要求パケットのヘッダから、前記コマンドコードを取得し、
前記所定の時間以内に、前記組み合わせが存在すると判定されなかった場合、リモート操作が失敗したと判定する、ことを特徴とする付記７に記載のネットワーク監視プログラム。
（付記９）
前記ネゴシエーションの応答を示す応答パケットから、前記実行要求パケットが暗号化されるか否かを判定し、
前記実行要求パケットが暗号化されると判定された場合、暗号化された前記実行要求パケットのヘッダから、前記コマンドコードを取得する、ことを特徴とする付記８に記載のネットワーク監視プログラム。
【符号の説明】
【０１１２】
１０　情報処理装置
２０　収集装置
３０　ネットワーク監視装置
４０　ファイアウォール
５０　Ｃ＆Ｃサーバ
１００　ネットワーク監視プログラム
１０１　受信部
１０２　パケット判定部
１０３　ネゴシエーション判定処理部
１０４　リモート操作判定処理部
１１１　取得部
１１２　暗号化判定部
１１３　判定用情報作成部
１２１　取得部
１２２　リスト追加部
１２３　時間判定部
１２４　結果判定部
１２５　結果作成部
２００　リモート操作辞書ＤＢ
１０００　リモート操作判定用情報
２０００　リモート操作結果情報

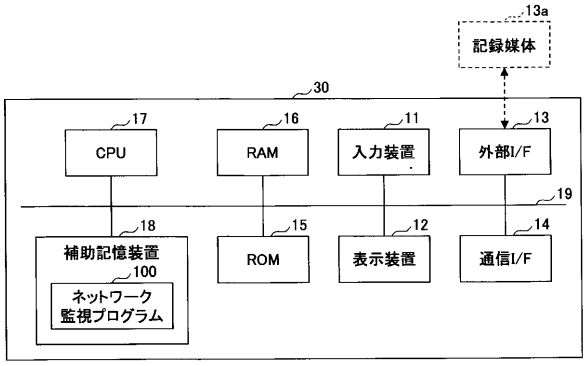
【図１】

本実施形態に係る
ネットワーク監視装置が含まれるシステムの全体構成の一例を示す図



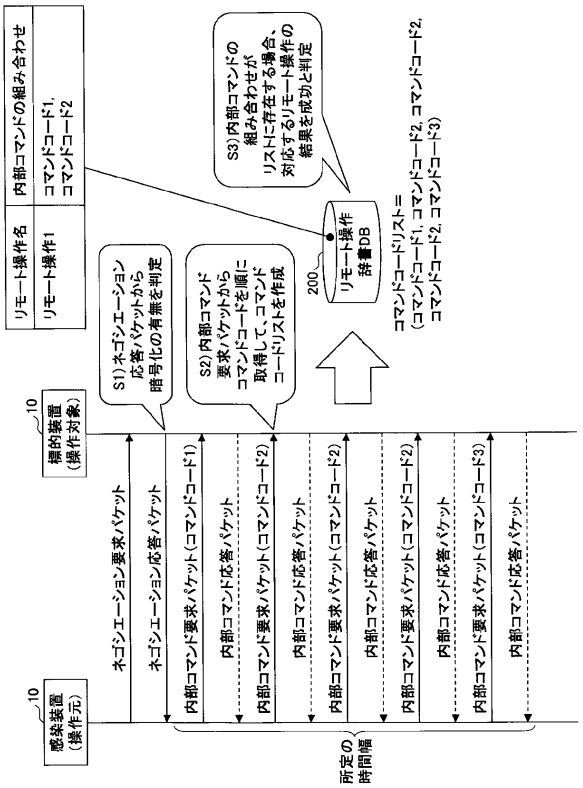
【図２】

本実施形態に係るネットワーク監視装置のハードウェア構成の一例を示す図



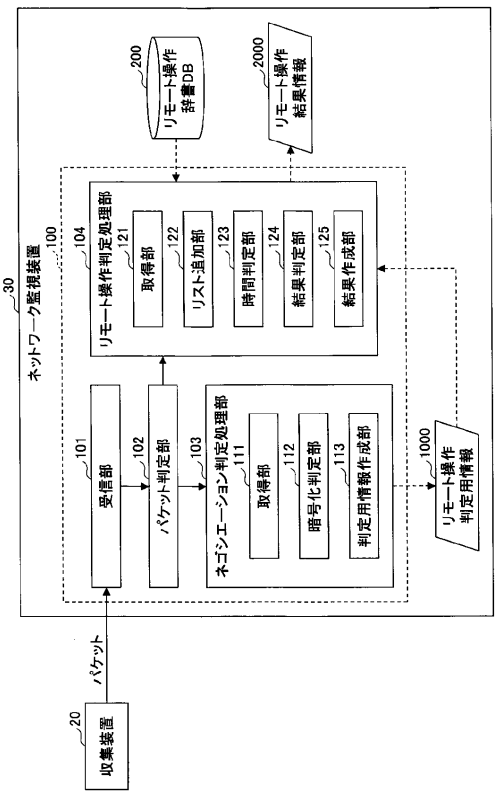
【図３】

リモート操作の結果を判定する処理の概略を説明する図



【図４】

本実施形態に係るネットワーク監視装置の機能構成の一例を示す図



【図５】

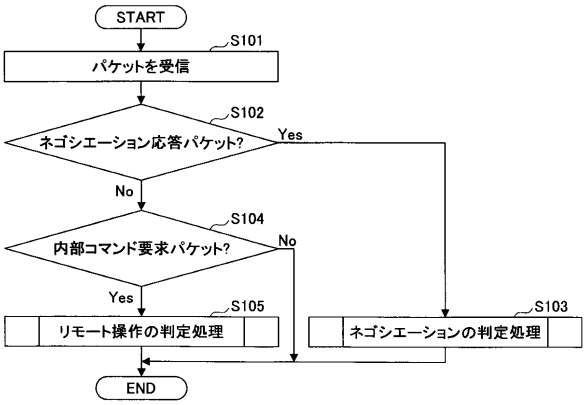
リモート操作辞書DBの一例を示す図

200

リモート操作名	内部コマンドの組み合わせ
リモート操作1	コマンドコード1, コマンドコード2
リモート操作2	コマンドコード6, コマンドコード8, コマンドコード10
リモート操作3	コマンドコード11, コマンドコード12
…	…

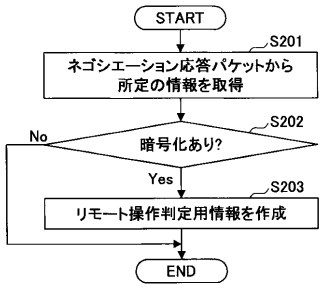
【図６】

本実施形態に係る
ネットワーク監視装置が実行する全体処理の一例を示すフローチャート



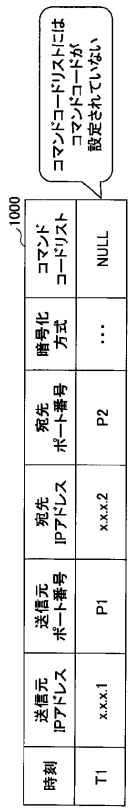
【図７】

ネゴシエーションの判定処理の一例を示すフローチャート



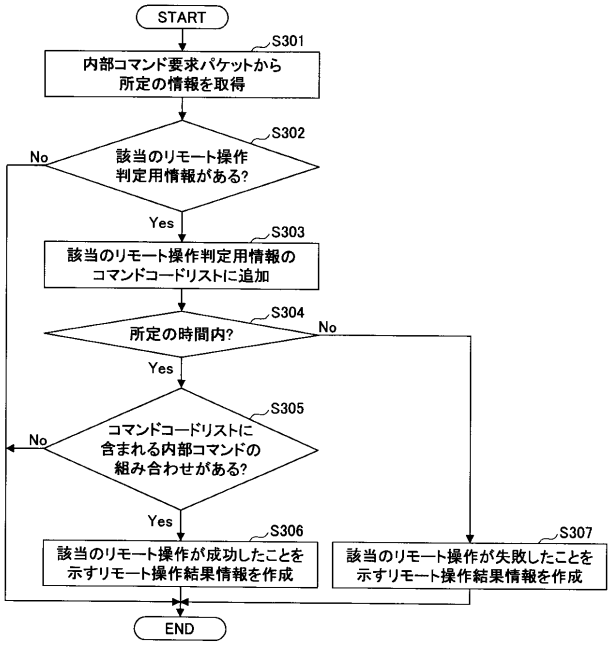
【図８】

リモート操作判定用情報の一例を示す図



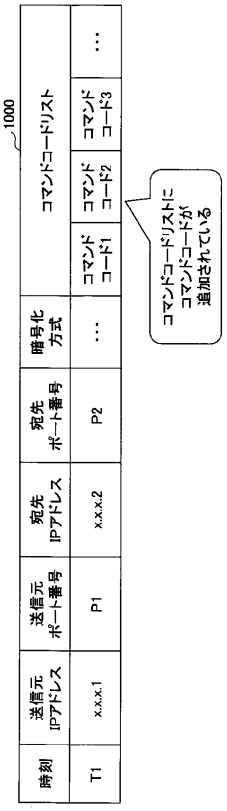
【図９】

リモート操作の判定処理の一例を示すフローチャート



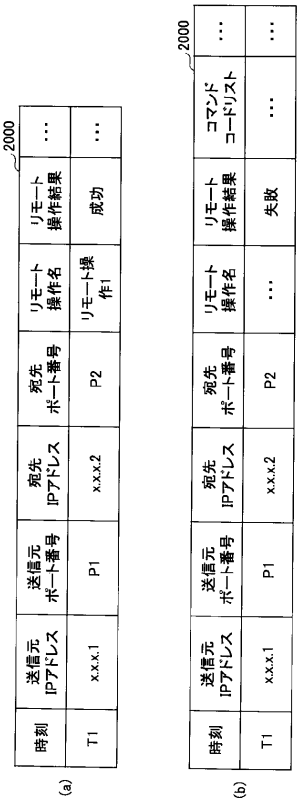
【図１０】

コマンドコードが追加されたリモート操作判定用情報の一例を示す図



【図１１】

リモート操作結果情報の一例を示す図



フロントページの続き

(72)発明者　古川　和快
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

Ｆターム(参考) 5K030 GA15 HA08 HC13 HD06 JA10 KX30 LC13 LD19 MC09
5K033 AA08 CC02 DA01 DA06 DB18 DB20 EA07