(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2021-144639
(P2021-144639A)
(43)公開日　令和3年9月24日(2021.9.24)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/57	(2013.01)	G06F	21/57	370	5K033
H04L 12/46	(2006.01)	H04L	12/46	M	

審査請求 未請求　請求項の数 9　ＯＬ　（全 26 頁）

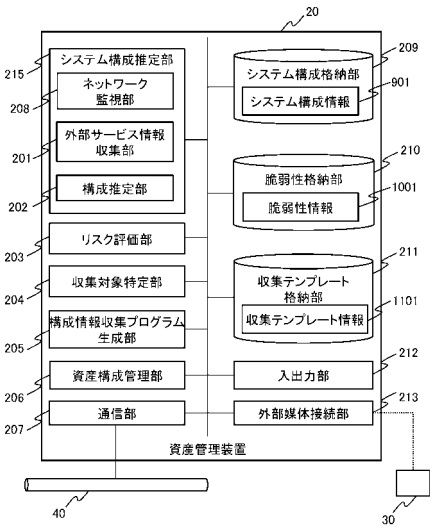
(21)出願番号　特願2020-44679(P2020-44679)
(22)出願日　令和2年3月13日(2020.3.13)

(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　110000176
一色国際特許業務法人
(72)発明者　内山　宏樹
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　亀田　貴之
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

Ｆターム(参考)　5K033 BA02　BA08　DA01　DA06　DB12　DB20　EA07

(54)【発明の名称】資産情報管理システム、及び資産情報管理方法

(57)【要約】　（修正有）
【課題】制御システムに対する影響を抑えつつ、制御システムの安定制御に必要な資産情報を取得する。
【解決手段】資産情報管理システムにおいて、資産管理装置２０は、所定の制御を行う制御装置を複数備えて構成されている制御システムの通信状態の情報を取得し、取得した通信状態の情報に基づき制御システムの構成を推定するシステム構成推定部と、制御装置に関する脆弱性情報及び推定した制御システムの構成に基づき、制御装置のそれぞれの制御上のリスクを推定するリスク評価部と、制御上のリスクが所定の条件を満たす制御装置である収集対象装置を特定する収集対象特定部と、特定した収集対象装置が管理する資産の構成の情報を取得する資産構成管理部と、を備える。
【選択図】図２



【特許請求の範囲】
【請求項１】
プロセッサ及びメモリを有すると共に、
所定の制御を行う制御装置を複数備えて構成されている制御システムの通信状態の情報を取得し、取得した通信状態の情報に基づき前記制御システムの構成を推定するシステム構成推定部と、
前記制御装置に関する脆弱性情報、及び前記推定した制御システムの構成に基づき、前記制御装置のそれぞれの制御上のリスクを推定するリスク評価部と、
前記制御上のリスクが所定の条件を満たす制御装置である収集対象装置を特定する収集対象特定部と、
前記特定した収集対象装置が管理する資産の構成の情報を取得する資産構成管理部と
を備える資産情報管理システム。
【請求項２】
前記特定した収集対象装置の情報に基づき、当該収集対象装置の資産の構成の情報を取得するための所定のプログラムを生成する構成情報収集プログラム生成部をさらに備え、
前記資産構成管理部は、前記生成したプログラムに基づき、前記資産の構成の情報を取得する、
請求項１に記載の資産情報管理システム。
【請求項３】
前記リスク評価部は、前記制御システムの構成の過去の推定時から所定時までの時間の長さに応じて、前記制御装置のそれぞれの制御上のリスクの大きさを推定する、
請求項１に記載の資産情報管理システム。
【請求項４】
前記リスク評価部は、前記脆弱性情報の設定時から所定時までの時間の長さに応じて、前記制御装置のそれぞれの制御上のリスクの大きさを推定する、
請求項１に記載の資産情報管理システム。
【請求項５】
前記構成情報収集プログラム生成部は、前記生成したプログラムを所定の記憶装置に記憶し、
前記収集対象装置は、前記記憶されたプログラムを実行し、当該収集対象装置が管理する前記資産の構成の情報を前記記憶装置に記憶するプログラム実行部を備え、
前記資産構成管理部は、前記記憶された資産の構成の情報を、前記記憶装置から取得する、
請求項２に記載の資産情報管理システム。
【請求項６】
前記プログラム実行部は、前記プログラムが前記収集対象装置で実行されたか否かを判定し、前記プログラムが前記収集対象装置で実行されたと判定した場合にのみ、当該収集対象装置が管理する資産の構成の情報を前記記憶装置に記憶する、
請求項５に記載の資産情報管理システム。
【請求項７】
前記推定した前記制御システムの構成の情報、及び、前記取得した収集対象装置が管理する資産の構成の情報のうち少なくともいずれかを出力する入出力部を備える、
請求項１に記載の資産情報管理システム。
【請求項８】
前記収集対象特定部は、前記所定の条件として、前記リスクに基づく前記収集対象装置の候補としての優先順位の情報を設定し、
前記入出力部は、前記収集対象装置の構成の情報と共に、前記優先順位の情報を出力する、
請求項１に記載の資産情報管理システム。
【請求項９】

プロセッサ及びメモリを有する情報処理装置が、
所定の制御を行う制御装置を複数備えて構成されている制御システムの通信状態の情報を取得し、取得した通信状態の情報に基づき前記制御システムの構成を推定するシステム構成推定処理と、
前記制御装置に関する脆弱性情報、及び前記推定した制御システムの構成に基づき、前記制御装置のそれぞれの制御上のリスクを推定するリスク評価処理と、
前記制御上のリスクが所定の条件を満たす制御装置である収集対象装置を特定する収集対象特定処理と、
前記特定した収集対象装置が管理する資産の構成の情報を取得する資産構成管理処理と
を実行する、資産情報管理方法。

【発明の詳細な説明】
【技術分野】
【０００１】
本発明は、資産情報管理システム、及び資産情報管理方法に関する。
【背景技術】
【０００２】
電力、鉄道、水道、ガスといった社会インフラや自動車で利用されるような、様々な装置（例えば、バルブ、アクチュエータ）の制御を行う制御システムは、各装置を制御することで、これらを予め設定されている圧力や温度に保っている。
【０００３】
このような制御を実現するために、通常、制御システムにおいては、コントローラ等の組込み装置が、装置のセンサの情報を定期的に取得して装置の状態を確認し、この情報を他のコントローラやサーバ等に通知し、その結果に基づき制御装置が必要に応じて装置の制御を行っている。この場合、制御システムでは周期的な通信が発生し、その通信データをもとに各処理及び制御が行われていることが通例である。
【０００４】
従来、このような制御システムは、専用のＯＳ又は専用のプロトコルを利用しており、また、インターネット等の外部ネットワークからアクセスできない領域に孤立した状態で設置されていた。そのため、いわゆるコンピュータウィルスやＤｏＳ攻撃といったサイバー攻撃からは無縁であると考えられてきた。
【０００５】
しかしながら、近年、コスト削減のために汎用ＯＳ及び汎用プロトコルを制御システムに利用するケースが増加しており、また、処理効率向上のための汎用的な情報システムとの連携も進んできている。また、制御システムをターゲットとしたコンピュータウィルスも広まりつつある。このような状況から、制御システムにおいても、一般的な情報システムと同様のレベルで、制御システム内の装置又は機器に関連する脆弱性情報を収集し、脆弱性の悪用を防止するといった、より適切な対処が求められている。
【０００６】
具体的には、制御システム内に存在する資産情報（ＯＳ情報やソフトウェア情報）を収集し、日々公開される脆弱性情報と突合せ、パッチを適用するなどといった事前の対処が必要である。しかしながら、多種多様な制御を継続的に行わなければならない制御システムはその性質上、資産情報の収集のために新たなソフトウェアを導入するといった構成変更が複雑となりかつ難しいという問題がある。
【０００７】
この点、なるべく構成変更を行わずに資産情報を収集する方法としては、ネットワークを流れる通信パケットを監視し、内部構成に変更が発生したと考えられる場合には、機器に対して、個別に通信パケットを送信することで資産情報を収集する技術が提案されている（例えば、特許文献１参照）。
【先行技術文献】
【特許文献】

【０００８】
【特許文献１】特開２００９－３０２６２５号公報
【発明の概要】
【発明が解決しようとする課題】
【０００９】
しかしながら、制御システムは各機器のＣＰＵ負荷やネットワークの使用帯域が予めシステム構築時に定められており、その設定値から外れてしまうとネットワークに大きく影響する可能性が高まる。これにより制御システムの動作に影響が生じ、業務に支障をきたすおそれがある。特許文献１のような従来技術では、資産情報の収集のためにネットワークに多くの通信が発生するため、制御システムの動作状況によってはネットワーク及び負荷が上昇し、業務に支障が生じてしまう可能性があった。
【００１０】
本発明はこのような現状に鑑みてなされたものであり、その目的は、制御システムに対する影響を抑えつつ、制御システムの安定制御に必要な資産情報を取得することが可能な資産情報管理システム及び資産情報管理方法を提供することにある。
【課題を解決するための手段】
【００１１】
前記した課題を解決するための本発明の一つは、プロセッサ及びメモリを有すると共に、所定の制御を行う制御装置を複数備えて構成されている制御システムの通信状態の情報を取得し、取得した通信状態の情報に基づき前記制御システムの構成を推定するシステム構成推定部と、前記制御装置に関する脆弱性情報、及び前記推定した制御システムの構成に基づき、前記制御装置のそれぞれの制御上のリスクを推定するリスク評価部と、前記制御上のリスクが所定の条件を満たす制御装置である収集対象装置を特定する収集対象特定部と、前記特定した収集対象装置が管理する資産の構成の情報を取得する資産構成管理部とを備える資産情報管理システム、とする。
【００１２】
前記した課題を解決するための本発明の他の一つは、プロセッサ及びメモリを有する情報処理装置が、所定の制御を行う制御装置を複数備えて構成されている制御システムの通信状態の情報を取得し、取得した通信状態の情報に基づき前記制御システムの構成を推定するシステム構成推定処理と、前記制御装置に関する脆弱性情報、及び前記推定した制御システムの構成に基づき、前記制御装置のそれぞれの制御上のリスクを推定するリスク評価処理と、前記制御上のリスクが所定の条件を満たす制御装置である収集対象装置を特定する収集対象特定処理と、前記特定した収集対象装置が管理する資産の構成の情報を取得する資産構成管理処理とを実行する、資産情報管理方法、とする。
【発明の効果】
【００１３】
本発明によれば、制御システムに対する影響を抑えつつ、制御システムの安定制御に必要な資産情報を取得することができる。
【００１４】
上記した以外の課題、構成及び効果は、以下の実施形態の説明により明らかにされる。
【図面の簡単な説明】
【００１５】
【図１】第１実施形態に係る資産情報管理システムが備える構成及び機能の一例を説明する図である。
【図２】第１実施形態に係る資産管理装置が備える機能の一例を説明する図である。
【図３】脆弱性情報のデータ構成の一例を示す図である。
【図４】収集テンプレート情報のデータ構成の一例を示す図である。
【図５】制御装置及び資産管理装置のハードウェア構成の一例を示す図である。
【図６】外部記憶媒体のハードウェア構成の一例を示す図である。
【図７】第１実施形態に係る資産情報管理システムにおいて行われる処理の概要を説明す

るフロー図である。
【図８】外部サービス情報収集処理の一例を説明するフロー図である。
【図９】外部サービス情報収集コマンドの一例を示す図である。
【図１０】システム構成情報のデータ構成の一例を示す図である。
【図１１】システム構成表示画面の一例を示す図である。
【図１２】構成情報収集プログラム生成処理の一例を説明するフロー図である。
【図１３】優先順位表示画面の一例を示す図である。
【図１４】構成情報収集プログラムの一例を示す図である。
【図１５】構成情報収集プログラム実行処理の一例を説明するフロー図である。
【図１６】構成情報の一例を示す図である。
【図１７】資産情報更新処理の一例を説明するフロー図である。
【図１８】第２実施形態に係る資産情報管理システムの構成及び機能の一例を説明する図である。
【図１９】第２実施形態に係る内部構成情報自動収集処理の一例を説明するフロー図である。
【発明を実施するための形態】
【００１６】
以下、本発明の各実施形態について図面を参照しつつ説明する。
【００１７】
［第１実施形態］
＜システム構成＞
図１は、第１実施形態に係る資産情報管理システム１が備える構成及び機能の一例を説明する図である。同図に示すように、資産情報管理システム１は、複数の制御装置１０（１０（１）～１０（ｎ））及びその制御対象の装置７０（７０（１）～７０（ｎ））を含む制御システム５０と、資産管理装置２０と、資産管理装置２０及び各制御装置１０に接続可能な外部記憶媒体３０とを含んで構成されている。なお、以下では、制御装置１０及び装置７０を機器と総称することがある。
【００１８】
なお、制御システム５０は、例えば、電力、鉄道、水道、ガスといった社会インフラシステム又は自動車製造工場等において設けられる様々な装置７０を制御する情報処理システムである。
【００１９】
資産情報管理システム１は、制御システム５０による安定的ないしセキュアな制御を維持するため、制御システム５０を構成する各制御装置１０の内部構成の情報を収集するプログラムである構成情報収集プログラム（詳細は後述）に基づき、必要な制御装置１０からその内部構成の情報を収集する。これにより、作業員等のユーザは、各制御装置１０に対して必要な措置を講ずることができる。
【００２０】
なお、内部構成とは、本実施形態では、制御装置１０で動作しているＯＳ（Operating System）、及びその他のソフトウェア等（ミドルウェア、アプリケーション等）の情報資産の構成をいうものとする。
【００２１】
制御装置１０は、装置７０の動作を制御する情報処理装置である。制御装置１０（１０（１）～１０（ｎ））は、例えば、装置７０（７０（１）～７０（ｎ））に設けられているセンサ等（不図示）から取得した圧力又は温度等の属性情報を所定のタイミング（時間間隔等）にて取得しつつ、装置７０を制御する。
【００２２】
資産管理装置２０は、構成情報収集プログラムを制御装置１０に実行させ、その実行結果に基づき、制御装置１０の内部構成の情報を取得する情報処理装置である。
【００２３】

なお、資産管理装置２０と制御装置１０の間、及び、制御装置１０間は、ＬＡＮ（Local Area Network）、ＷＡＮ（Wide Area Network）、インターネット、専用線等の有線又は無線のネットワーク４０によって通信可能に接続される。

【００２４】

次に、資産情報管理システム１における各情報処理装置の機能について説明する。

【００２５】

＜機能＞

図１に示すように、制御装置１０は、装置７０の制御を行う制御処理部１０１（１０１（１）～１０１（ｎ））と、装置７０又は他の制御装置１０等に提供している機能（以下、外部サービスという。例えば、外部に公開している通信サービス。Ｔｅｌｎｅｔ等。）を管理する外部サービス管理部１０２（１０２（１）～１０２（ｎ））と、自身に接続された外部記憶媒体３０とデータの送受信を行う外部媒体接続部１０３（１０３（１）～１０３（ｎ））と、当該制御装置１０の内部構成の情報を管理する内部構成管理部１０４（１０４（１）～１０４（ｎ））と、他の情報処理装置と通信を行う通信部１０５（１０５（１）～１０５（ｎ））と、各種のプログラムを実行するプログラム実行部１０６（１０６（１）～１０６（ｎ））とを含む各機能部を備える。

【００２６】

外部記憶媒体３０は、ＳＤカード又はＵＳＢメモリ等の、可搬性の記憶装置である。外部記憶媒体３０は、資産管理装置２０が生成した構成情報収集プログラム１２０１を記憶する構成情報収集プログラム格納部３０１と、各制御装置１０から収集した内部構成の情報（構成情報１３０１）を記憶する構成格納部３０２と、自身に接続された制御装置１０又は資産管理装置２０とデータの送受信を行う接続部３０３とを含む各機能部を有する。

【００２７】

資産情報管理システム１におけるユーザは、外部記憶媒体３０を持参してこれを資産管理装置２０又は各制御装置１０に接続する。

【００２８】

次に、図２は、第１実施形態に係る資産管理装置２０が備える機能の一例を説明する図である。同図に示すように、資産管理装置２０は、システム構成推定部２１５、リスク評価部２０３、収集対象特定部２０４、構成情報収集プログラム生成部２０５、資産構成管理部２０６、通信部２０７、システム構成情報９０１（後述）を記憶するシステム構成格納部２０９、脆弱性情報１００１（後述）を記憶する脆弱性格納部２１０、収集テンプレート情報１１０１（後述）を記憶する収集テンプレート格納部２１１、入出力部２１２、及び外部媒体接続部２１３の各機能部を備える。

【００２９】

まず、システム構成推定部２１５は、所定の制御を行う制御装置１０を複数備えて構成されている制御システム５０の通信状態の情報を取得し、取得した通信状態の情報に基づき制御システム５０の構成を推定する。

【００３０】

具体的には、システム構成推定部２１５は、ネットワーク監視部２０８、外部サービス情報収集部２０１、及び構成推定部２０２を備える。

【００３１】

ネットワーク監視部２０８は、ネットワーク４０の負荷の状況を監視する。外部サービス情報収集部２０１は、ネットワーク４０の負荷の状況に応じて、制御装置１０から外部サービスの情報を収集する。構成推定部２０２は、外部サービスの情報に基づき、制御システム５０の構成を推定する。

【００３２】

次に、リスク評価部２０３は、制御装置１０に関する脆弱性情報、及びシステム構成推定部２１５が推定した制御システム５０の構成に基づき、制御装置１０のそれぞれの制御上のリスク（例えば、セキュリティ上のリスク）を推定する。

【００３３】

具体的には、例えば、リスク評価部２０３は、制御システム５０の構成の過去の推定時から所定時（本実施形態では現在時とするが、他の所定のタイミングでよい）までの時間の長さに応じて、制御装置１０のそれぞれの制御上のリスクの大きさを推定する。

【００３４】

また、例えば、リスク評価部２０３は、脆弱性情報１００１の設定時から所定時（本実施形態では現在時とするが、他の所定のタイミングでよい）までの時間の長さに応じて、制御装置１０のそれぞれの制御上のリスクの大きさを推定する。

【００３５】

ここで、脆弱性情報１００１について説明する。

【００３６】

（脆弱性情報）

図３は、脆弱性情報１００１のデータ構成の一例を示す図である。脆弱性情報１００１は、制御装置１０が記憶しているＯＳ又はソフトウェアが有している脆弱性（例えば、制御上、セキュリティ上の脆弱性）に関する情報である。脆弱性情報１００１は、例えば、資産情報管理システム１の外部のネットワークから、資産管理装置２０に自動的に又はユーザの指定したタイミングで提供される。

【００３７】

具体的には、脆弱性情報１００１は、脆弱性が発見された制御装置１０におけるＯＳ又はソフトウェア等である脆弱性対象１００２と、脆弱性対象１００２に係る情報が公開された日時である公開日時１００３と、脆弱性対象１００２に係る脆弱性の危険度１００４とを含むレコードを１つ以上有するデータベースである。

【００３８】

なお、脆弱性情報１００１の構成要素はここで説明したものに限定されるものではない。また、脆弱性情報１００１における各情報の登録順序もここで説明した順序に限定されない。

【００３９】

次に、図２に示すように、収集対象特定部２０４は、制御上のリスクが所定の条件を満たす制御装置１０である収集対象装置を特定する。

【００４０】

具体的には、収集対象特定部２０４は、所定の条件として、リスクに基づく収集対象装置の候補としての優先順位の情報を設定する。

【００４１】

構成情報収集プログラム生成部２０５は、収集対象特定部２０４が特定した収集対象装置の情報に基づき、当該収集対象装置の資産の構成の情報（内部構成の情報）を取得するための所定のプログラム（すなわち、構成情報収集プログラム）を生成する。

【００４２】

なお、本実施形態では、構成情報収集プログラム生成部２０５は、構成情報収集プログラム生成部２０５が生成したプログラムを所定の記憶装置（外部記憶媒体３０）に記憶する。そして、収集対象装置は、記憶されたプログラムを実行し、当該収集対象装置が管理する資産の構成の情報をその記憶装置に記憶する（プログラム実行部１０６）。

【００４３】

なお、プログラム実行部１０６は、プログラム（構成情報収集プログラム）が収集対象自身の収集対象装置で実行されたか否かを判定し、プログラムがその収集対象装置で実行されたと判定した場合にのみ、当該収集対象装置が管理する資産の構成の情報を記憶装置（外部記憶媒体３０）に記憶する

資産構成管理部２０６は、収集対象特定部２０４が特定した収集対象装置が管理する資産の構成の情報を取得する。すなわち、資産構成管理部は、構成情報収集プログラム生成部２０５が生成したプログラムに基づき、資産の構成の情報を取得する。

【００４４】

本実施形態では、前記資産構成管理部２０６は、構成情報収集プログラム生成部２０５

で記憶された資産の構成の情報を、記憶装置（外部記憶媒体３０）から取得する。
【００４５】
次に、通信部２０７は、ネットワーク４０を介して制御装置１０とデータの送受信を行う。
【００４６】
システム構成格納部２０９は、システム構成推定部２１５が推定した制御システム５０の構成をシステム構成情報９０１として記憶し、資産構成管理部２０６が取得した資産の構成の情報（構成情報１３０１）を記憶する。
【００４７】
脆弱性格納部２１０は、脆弱性情報１００１を記憶する。
【００４８】
収集テンプレート格納部２１１は、内部構成の情報の収集手順や収集対象を記憶した情報である収集テンプレート情報１１０１を格納する。
【００４９】
ここで、収集テンプレート情報１１０１について説明する。
【００５０】
（収集テンプレート情報）
図４は、収集テンプレート情報１１０１のデータ構成の一例を示す図である。収集テンプレート情報１１０１は、制御装置１０で動作するＯＳのＯＳ情報１１０２と、ＯＳ情報１１０２に係るＯＳに対応した構成情報収集スクリプト１１０３とを含んで構成されているレコードを少なくとも１以上有するデータベースである。
【００５１】
構成情報収集スクリプト１１０３は、制御装置１０の内部構成の情報を収集するプログラム等である。構成情報収集スクリプト１１０３は、例えば、内部構成の情報を収集するために参照すべきデータの場所及び参照方法を記述したプログラムである。構成情報収集スクリプト１１０３の内容は、ＯＳごとに異なる。
【００５２】
なお、収集テンプレート情報１１０１の構成要素はここで説明したものに限定されるものではなく、少なくともここで説明した要素が含まれていればよい。また、収集テンプレート情報１１０１の構成要素の順序はここで説明したものに限定されるものではない。
【００５３】
次に、図２に示すように、入出力部２１２は、資産管理装置２０へのユーザ入力を受け付け、また、ユーザに提示する情報の表示を行う。
【００５４】
具体的には、例えば、入出力部２１２は、システム構成推定部２１５が推定した制御システム５０の構成の情報、及び、収集対象特定部２０４が取得した収集対象装置が管理する資産の構成の情報のうち少なくともいずれかを出力する。また、入出力部２１２は、収集対象装置の構成の情報と共に、優先順位の情報を出力する。
【００５５】
次に、外部媒体接続部２１３は、接続された外部記憶媒体３０とデータの送受信を行う。
【００５６】
ここで、図５は、制御装置１０及び資産管理装置２０のハードウェア構成の一例を示す図である。これらの情報処理装置は、ＣＰＵ１４と、ＲＡＭ（Random Access Memory）、ＲＯＭ（Read Only Memory）等のメモリ１５と、ＨＤＤ（Hard Disk Drive）、ＳＳＤ（Solid State Drive）等の記憶装置１３と、キーボード又はタッチパネル等とモニタ又はディスプレイ等とからなる入出力装置１１と、他の情報処理装置と通信を行う通信装置１１とを備え、これらがバスなどの内部通信線１６により接続される。
【００５７】
制御装置１０及び資産管理装置２０の各機能部の機能は、ＣＰＵ１４が、メモリ１５又

は記憶装置１３に記憶されている、各機能を実現する所定のプログラムを読み出すことにより実現される。なお、各プログラムは、制御装置１０及び資産管理装置２０が読み取り可能な記録媒体にあらかじめ記録されていてもよいし、記憶媒体又は通信媒体（ネットワークまたはネットワークを伝搬する搬送波）を介して、必要なときに導入されてもよい。

【００５８】

次に、図６は、外部記憶媒体３０のハードウェア構成の一例を示す図である。外部記憶媒体３０は、データの入出力（接続）を行う入出力装置３１と、フラッシュメモリ等の記憶装置３２とを備え、これらがバスなどの内部通信線３３で接続される。

【００５９】

次に、資産情報管理システム１において行われる処理について説明する。

【００６０】

＜処理の概要＞

図７は、第１実施形態に係る資産情報管理システム１において行われる処理の概要を説明するフロー図である。

【００６１】

まず、資産管理装置２０は、所定のタイミングにて、制御システム５０の構成を収集する外部サービス情報収集処理を実行する（Ｓ１）。そして、資産管理装置２０は、外部サービス情報収集処理の結果に基づき、構成情報収集プログラム１２０１を生成して外部記憶媒体３０に記憶する構成情報収集プログラム生成処理を実行する（Ｓ３）。

【００６２】

他方、制御装置１０は、外部記憶媒体３０に記憶されている構成情報収集プログラム１２０１を実行してその出力情報（構成情報１３０１）を外部記憶媒体３０に記憶する構成情報収集プログラム実行処理を実行する（Ｓ５）。

【００６３】

資産管理装置２０は、外部記憶媒体３０に記憶された構成情報１３０１を取得する資産情報更新処理を実行する（Ｓ７）。

【００６４】

その後、ユーザは、資産管理装置２０の構成情報１３０１に基づき、必要に応じて、制御装置１０に対して、その内部構成の変更に関する処理（例えば、制御装置１０の資産（ＯＳ、各種ソフトウェア等）の脆弱性を解消するためのアップデート）を実行させる。

【００６５】

以下、これらの処理の詳細を説明する。

【００６６】

＜外部サービス情報収集処理＞

図８は、外部サービス情報収集処理の一例を説明するフロー図である。外部サービス情報収集処理は、例えば、資産情報管理システム１の起動後、所定のタイミング（例えば、所定の時間間隔、所定の時刻、又はユーザにより指定されたタイミング）で実行される。

【００６７】

まず、資産管理装置２０のネットワーク監視部２０８は、ネットワーク４０の現在の状態（ネットワーク４０の負荷の状況）を示す情報を取得する（Ｓ４０１）。具体的には、例えば、ネットワーク監視部２０８は、ネットワーク４０の通信状態を監視することで（例えば、所定のパケットをネットワーク４０に送信することでレスポンスデータを取得する）、ネットワーク４０における単位時間あたりの通信パケットの数又はデータサイズ、又はネットワーク４０で使用されている帯域の情報等を生成する。

【００６８】

ネットワーク監視部２０８は、Ｓ４０１で取得した情報に基づき、ネットワーク４０の負荷が高いか否かを判定する（Ｓ４０２）。具体的には、例えば、ネットワーク監視部２０８は、Ｓ４０１で取得したパケット数もしくはデータサイズが所定の閾値以上であるか否か、又は、使用されている帯域が所定の閾値以上であるか否か等を判定する。

【００６９】
ネットワーク４０の負荷が高い場合は（Ｓ４０２：規定以上）、現時点ではネットワーク４０の負荷が高く外部サービス情報を取得するには適さないため、ネットワーク監視部２０８は、Ｓ４０１の処理を繰り返す。
【００７０】
他方、ネットワーク４０の負荷が高くない場合は（Ｓ４０２：規定未満）、資源管理装置２０の外部サービス情報収集部２０１は、外部サービスの情報を取得する対象となる制御装置１０を特定する（Ｓ４０３）。
【００７１】
具体的には、例えば、外部サービス情報収集部２０１は、全ての制御装置１０を特定してもよいし、制御装置１０の一部（例えば、そのＩＤ番号が所定範囲にある制御装置１０）を取得してもよい。
【００７２】
外部サービス情報収集部２０１は、Ｓ４０３で特定した制御装置１０から外部サービス情報を取得するためのプログラムである外部サービス情報収集コマンド８０１を生成する（Ｓ４０４）。
【００７３】
（外部サービス情報収集コマンド）
ここで、図９は、外部サービス情報収集コマンド８０１の一例を示す図である。外部サービス情報収集コマンド８０１は、外部サービス情報を取得する対象の制御装置１０を特定する情報（本実施形態ではＩＰアドレスとする）である収集対象機器アドレス８０２と、収集対象機器アドレス８０２が示す制御装置１０との通信に用いられるプロトコル（例えば、ＴＣＰ：Transmission Control Protocol、ＵＤＰ：User Datagram Protocol）の情報であるプロトコル８０３と、収集対象機器アドレス８０２が示す制御装置１０との通信に使用されるポート番号８０４と、情報収集用データ８０５とを含む。
【００７４】
情報収集用データ８０５は、例えば、プロトコル８０３及びポート番号８０４に対応するデータである。このデータを制御装置１０に送信すると、当該制御装置１０はこれに対応する所定のレスポンスデータを返信するので、当該制御装置１０で動作しているＯＳ及び、当該制御装置１０が外部の装置に提供している外部サービスを、特別な機能を設けることなく識別することができる。
【００７５】
なお、外部サービス情報収集コマンド８０１の構成要素はここで説明したものに限定されず、少なくとも収集対象機器アドレス８０２、プロトコル８０３、及びポート番号８０４が含まれていればよい。情報収集用データ８０５は必須の要素ではない。また、外部サービス情報収集コマンド８０１の構成要素の格納順序はここで説明した順序に限定されない。
【００７６】
また、本実施形態では、外部サービス情報収集コマンド８０１は、制御装置１０ごとに生成するものとするが、Ｓ４０３で特定した全制御装置１０に対する１つのコマンドとして生成してもよい。
【００７７】
次に、図８のＳ４０５に示すように、外部サービス情報収集部２０１は、Ｓ４０３で特定した各制御装置１０に対して、Ｓ４０４で生成した外部サービス情報収集コマンド８０１を送信する。すると、外部サービス情報収集コマンド８０１を受信した各制御装置１０の通信部１０５は、予め設けられている所定の機能に基づき、所定のレスポンス４０２（例えば、制御装置１０のＩＤ、ＩＰアドレスを含む情報）を生成し（Ｓ４０５）、生成したレスポンス４０２を資産管理装置２０に送信する。
【００７８】
資産管理装置２０の外部サービス情報収集部２０１は、Ｓ４０４で生成した外部サービ

ス情報収集コマンド８０１を全て送信したか否かを確認する（Ｓ４０６）。送信していない外部サービス情報収集コマンド８０１がある場合はこれを送信し（Ｓ４０６：未完了）、外部サービス情報収集コマンド８０１を全て送信した場合は（Ｓ４０６：完了）、外部サービス情報収集部２０１は、以下の処理を行う。

【００７９】

すなわち、外部サービス情報収集部２０１は、各制御装置１０から受信したレスポンス４０２に基づき、制御システム５０の構成を推定する（Ｓ４０７）。

【００８０】

具体的には、例えば、外部サービス情報収集部２０１は、受信した各レスポンス４０２に基づき、各制御装置１０の異常の有無、各レスポンス４０２の送信元である各制御装置１０の間の接続関係、各制御装置１０で動作しているＯＳ、各制御装置１０が提供している外部サービス等を推定する。

【００８１】

システム構成格納部２０９は、Ｓ４０７で推定した結果をシステム構成情報９０１として記憶する（Ｓ４０８）。

【００８２】

（システム構成情報）

図１０は、システム構成情報９０１のデータ構成の一例を示す図である。システム構成情報９０１は、制御装置１０の識別子である機器識別子９０２と、機器識別子９０２に係る制御装置１０における内部構成９０７の情報を取得した日時である収集日時９０３と、機器識別子９０２に係る制御装置１０を特定する情報であるＩＰアドレス９０４と、機器識別子９０２に係る制御装置１０で動作しているＯＳの情報であるＯＳ情報９０５（例えば、ＯＳによって異なるＩ／Ｏポートの空き番号の情報）と、機器識別子９０２に係る制御装置１０が提供している外部サービスを特定する情報である外部サービス９０６と、機器識別子９０２に係る制御装置１０における内部構成９０７とを含むレコードを１以上有するデータベースである。なお、最初のＳ４０の実行時点では、内部構成９０７は空情報としてもよい。

【００８３】

外部サービス９０６及び内部構成９０７には、装置又は機器の構成に応じて、複数の外部サービス又は構成の情報が含まれる場合がある。

【００８４】

なお、システム構成情報９０１の構成要素はここで説明したものに限定されるものではなく、少なくともここで説明した要素が含まれていればよい。また、システム構成情報９０１の構成要素の格納順序はここで説明した順序に限定されるものではない。

【００８５】

次に、図８のＳ４０９に示すように、入出力部２１２は、Ｓ４０７で生成したシステム構成情報９０１の内容を示すシステム構成表示画面を表示する。以上で外部サービス情報収集処理は終了する。

【００８６】

（システム構成表示画面）

図１１は、システム構成表示画面１４０１の一例を示す図である。システム構成表示画面１４０１は、ＩＰアドレスの情報に基づき資産管理装置２０及び各制御装置１０の間の接続関係（接続の有無等）を示したシステム構成図１４０２と、各制御装置１０の構成を示した詳細構成一覧１４０３とを備える。

【００８７】

詳細構成一覧１４０３は、制御装置１０を特定する情報である機器情報１４０４、機器情報１４０４に係る制御装置１０の内部構成の情報の取得日時１４０５、機器情報１４０４に係る制御装置１０のＩＰアドレス１４０６、機器情報１４０４に係る制御装置１０で動作しているＯＳ１４０７、機器情報１４０４に係る制御装置１０が提供している外部サービス１４０８、及び、機器情報１４０４に係る制御装置１０における内部構成１４０９

の各情報が、各制御装置１０（機器）について一覧表示される。なお、内部構成１４０９は、Ｓ４０８の最初の実行時点では非表示となる。

【００８８】

なお、システム構成表示画面１４０１の構成要素はここで説明したものに限定されるものではなく、少なくとも上記の要素が含まれていればよい。また、システム構成表示画面１４０１の構成要素の表示順序はここで説明したものに限定されるものではない。

【００８９】

＜構成情報収集プログラム生成処理＞

図１２は、構成情報収集プログラム生成処理の一例を説明するフロー図である。なお、この処理は、外部サービス情報収集処理の実行後、所定のタイミング（例えば、所定の時間間隔、所定の時刻、又はユーザにより指定されたタイミング）で実行される。また、この処理の開始に際して、ユーザは、外部記憶媒体３０を資産管理装置２０に接続する。

【００９０】

まず、資産管理装置２０の構成情報収集プログラム生成部２０５は、外部サービス情報収集処理でシステム構成格納部２０９に格納したシステム構成情報９０１を取得する（Ｓ５０１）。

【００９１】

また、構成情報収集プログラム生成部２０５は、脆弱性格納部２１０に格納されている脆弱性情報１００１を取得する（Ｓ５０２）。

【００９２】

リスク評価部２０３は、Ｓ５０１で取得したシステム構成情報９０１と、Ｓ５０２で取得した脆弱性情報１００１とに基づき、制御システム５０における各制御装置１０の現在のリスクを評価する（Ｓ５０３）。

【００９３】

具体的には、例えば、リスク評価部２０３は、システム構成情報９０１が示す各制御装置１０の構成と、脆弱性情報１００１の脆弱性対象１００２が示すＯＳ及び外部サービスとを比較し、脆弱性を有しているＯＳ及び外部サービスの数を各制御装置１０について特定し、この数が大きいほどリスクが高い制御装置１０であると評価する（または、この数が一定値以上の制御装置１０はリスクが高いと評価する）。また、例えば、リスク評価部２０３は、各制御装置１０のハードウェアの情報を取得することによりそれらのリスクを評価してもよい。

【００９４】

そして、同じリスク評価であった制御装置１０間については、リスク評価部２０３は、例えば、脆弱性情報１００１の公開日時１００３から現在日時との時間差（経過時間）を算出することで、脆弱性の情報が古い制御装置１０ほどリスクが高いと評価する（または、脆弱性の情報が一定時以前であればその制御装置１０のリスクは高いと評価する）。

【００９５】

収集対象特定部２０４は、Ｓ５０３で評価したリスクに基づき、各制御装置１０の優先順位（構成情報１３０１を取得する優先順位）を算出する（Ｓ５０４）。

【００９６】

具体的には、例えば、収集対象特定部２０４は、リスクが大きい制御装置１０ほどその優先順位を高くする。また、収集対象特定部２０４は、同じリスクの制御装置１０間については、脆弱性情報１００１の危険度１００４が高く又は公開日時１００３が一定時期以前のＯＳ又は外部モジュールを有する制御装置１０の優先順位を高くする。

【００９７】

なお、収集対象特定部２０４は、同じリスクの制御装置１０間については、その物理的位置に応じて優先順位を設定してもよい（例えば、資産管理装置２０との距離が近い制御装置１０ほど優先順位が高い）。これにより、ユーザの作業負担を調整することができる。

【００９８】

入出力部２１２は、Ｓ５０４で算出した優先順位の情報を、優先順位表示画面１５０１に表示する（Ｓ５０５）。

【００９９】

（優先順位表示画面）

図１３は、優先順位表示画面１５０１の一例を示す図である。優先順位表示画面１５０１は、ＩＰアドレスの情報に基づき資産管理装置２０及び各制御装置１０の間の接続関係を示したシステム構成図１５０２と、各制御装置１０の優先順位の情報を示した優先順位詳細一覧１５０３とを備える。

【０１００】

優先順位詳細一覧１５０３には、制御装置１０を特定する機器情報１５０５、機器情報１５０５に係る制御装置１０の優先順位１５０４、機器情報１５０５に係る制御装置１０のリスクの大きさ１５０６、及び、リスクの大きさ１５０６の算定根拠１５０７の各情報が一覧表示される。同図の例では、算定根拠１５０７には、１ヶ月以内に脆弱性が公開されている点又は、前回の内部構成の情報の収集日時から半年以上経過している点などが示されている。

【０１０１】

優先順位表示画面１５０１の構成要素はここで説明した項目に限定されるものではなく、少なくともここで説明した要素が含まれていればよい。また、優先順位表示画面１５０１の構成要素の表示順序はここで説明した順序に限定されるものではない。

【０１０２】

ユーザは、この優先順位表示画面１５０１を確認しつつ、どの制御装置１０のリスクが高いかを検討することができる。

【０１０３】

次に、図１２のＳ５０６に示すように、構成情報収集プログラム生成部２０５は、収集テンプレート格納部２１１から収集テンプレート情報１１０１を取得し、この取得した収集テンプレート情報１１０１に基づき、構成情報収集プログラム１０２１を生成する。

【０１０４】

具体的には、例えば、まず、構成情報収集プログラム生成部２０５は、ユーザから、優先順位表示画面１５０１に対する入力を受け付けることにより、優先順位表示画面１５０１に表示されている制御装置１０から収集対象装置を特定する。なお、構成情報収集プログラム生成部２０５は、所定の優先順位を有する各制御装置１０（例えば、最優先順位から所定順位までの制御装置１０）を、収集対象装置として自動的に特定してもよい。

【０１０５】

そして、構成情報収集プログラム生成部２０５は、特定した収集対象装置で動作しているＯＳを全て特定する。そして、構成情報収集プログラム生成部２０５は、特定した各ＯＳに対応する構成情報収集スクリプト１１０３を、収集テンプレート情報１１０１からそれぞれ取得する。構成情報収集プログラム生成部２０５は、取得した各構成情報収集スクリプト１１０３に対して、各収集対象装置のＩＰアドレス（システム構成情報９０１から取得）を対応付けて記憶することにより、構成情報収集プログラム１２０１を生成する。

【０１０６】

なお、構成情報収集プログラム生成部２０５は、収集テンプレート情報１１０１を用いずに独自に構成情報収集プログラム１２０１を生成してもよい。また、構成情報収集プログラム生成部２０５は、収集対象装置の情報を含むテンプレートを用いて、構成情報収集プログラム１２０１を生成してもよい。

【０１０７】

（構成情報収集プログラム）

図１４は、構成情報収集プログラム１２０１の一例を示す図である。構成情報収集プログラム１２０１は、収集対象装置のＩＰアドレス１２０２と、収集対象装置の内部構成の情報を収集するためのプログラムである構成情報収集スクリプト１２０３と、構成情報収集スクリプト１２０３が実行されたか否かを示す情報（実行フラグ）である実行有無フラ

グ１２０４とを含む。
【０１０８】
なお、実行有無フラグ１２０４は、収集対象装置に対して構成情報収集スクリプト１２０３を実行したか否かを示すフラグであり、実行した場合には「実行済」、未実行の場合は「未実行」の情報が設定される。
【０１０９】
なお、構成情報収集プログラム１２０１は、収集対象装置ごとに生成してもよいし、全ての収集対象装置に関するプログラムをひとつにまとめたプログラムとしてもよい。
【０１１０】
構成情報収集プログラム１２０１の構成要素はここで説明したものに限定されるものではなく、少なくともここで説明した要素が含まれていればよい。また、構成情報収集プログラム１２０１の構成要素の格納順序はここで説明した順序に限定されるものではない。
【０１１１】
次に、図１２に示すように、外部媒体接続部２１３は、外部記憶媒体３０に対して、接続確認コマンド５０１を送信する。外部記憶媒体３０の接続部３０３は、接続確認コマンド５０１を受信すると、接続状態を示すレスポンス５０２を生成し、生成したレスポンス５０２を資産管理装置２０に送信する。
【０１１２】
資産管理装置２０の外部媒体接続部２１３は、レスポンス５０２を確認する（Ｓ５０７）。
【０１１３】
レスポンス５０２が接続失敗を示している場合（又はレスポンス５０２を受信していない場合）は（Ｓ５０７：接続失敗）、外部媒体接続部２１３は構成情報収集プログラム生成処理を終了する（Ｓ５０８）。他方、レスポンス５０２が接続成功を示している場合には（Ｓ５０７：接続成功）、構成情報収集プログラム生成部２０５は、Ｓ５０６で生成した構成情報収集プログラム１２０１を外部記憶媒体３０に送信する。
【０１１４】
外部記憶媒体３０の構成情報収集プログラム格納部３０１は、受信した構成情報収集プログラム１２０１を記憶する（Ｓ５０９）。そして、外部記憶媒体３０の接続部３０３は、所定のレスポンス５０４を資産管理装置２０に送信する。
【０１１５】
次に、構成情報収集プログラム生成部２０５は、受信したレスポンス５０４を確認する（Ｓ５１０）。構成情報収集プログラム生成部２０５は、受信したレスポンス５０４に基づき、構成情報収集プログラム１２０１の記憶が失敗したと判断した場合には、再度、構成情報収集プログラム１２０１を送信する（Ｓ５１０：格納失敗）。一方、構成情報収集プログラム生成部２０５は、構成情報収集プログラム１２０１の記憶が成功したと判断した場合には、構成情報収集プログラム生成処理を終了する（Ｓ５１０：格納成功）。
【０１１６】
なお、所定回数以上、構成情報収集プログラム１２０１の記憶が失敗した場合には、外部記憶媒体３０の空き容量がない、外部記憶媒体３０が書き込み不能状態になっているといった状況が考えられるため、構成情報収集プログラム生成部２０５は、このような場合にも、構成情報収集プログラム格納処理を終了するようにしてもよい。
【０１１７】
＜構成情報収集プログラム実行処理＞
図１５は、構成情報収集プログラム実行処理の一例を説明するフロー図である。なお、この処理は、構成情報収集プログラム生成処理の実行後、所定のタイミング（例えば、所定の時間間隔、所定の時刻、又はユーザにより制御装置１０に対して指定されたタイミング）で実行される。
【０１１８】
なお、この処理の開始に際して、ユーザは、外部記憶媒体３０を収集対象装置である制

御装置１０に接続する。ここでは、制御装置１０（１）～（ｎ）のうち制御装置１０（ｘ）が収集対象装置である場合を説明する。

【０１１９】

まず、制御装置１０（ｘ）の外部媒体接続部１０３（ｘ）は、外部記憶媒体３０に対して、接続確認コマンド６０１を送信する。外部記憶媒体３０の接続部３０３は、接続確認コマンド６０１を受信すると、接続状態を示すレスポンス６０２を制御装置１０（ｘ）に送信する。なお、資産管理装置２０からの指示によって外部媒体接続部１０３（ｘ）が接続確認コマンド６０１を送信するようにしてもよい。

【０１２０】

その後、制御装置１０（ｘ）の外部媒体接続部１０３（ｘ）は、レスポンス６０２を確認する（Ｓ６０１）。外部記憶媒体３０との接続に失敗していると判断した場合（又はレスポンス６０２を受信していない場合）には（Ｓ６０１：接続失敗）、外部媒体接続部１０３（ｘ）は構成情報収集プログラム実行処理を終了する（Ｓ６０２）。一方、外部記憶媒体３０との接続に成功していると判断した場合には（Ｓ６０１：接続成功）、外部媒体接続部１０３（ｘ）は、構成情報収集プログラム１２０１の取得を外部記憶媒体３０に要求する取得コマンド６０３を外部記憶媒体３０に送信する。

【０１２１】

外部記憶媒体３０の構成情報収集プログラム格納部３０１は、取得コマンド６０３の受信に応じて構成情報収集プログラム１２０１を取得する（Ｓ６０３）。接続部３０３は、この構成情報収集プログラム１２０１を制御装置１０（ｘ）に送信する。

【０１２２】

制御装置１０（ｘ）のプログラム実行部１０６（ｘ）は、受信した構成情報収集プログラム１２０１を実行する（Ｓ６０４）。なお、プログラム実行部１０６（ｘ）は、構成情報収集プログラム１２０１を受信した後に自動的にこれを実行してもよいし、ユーザ入力に基づき実行してもよい。

【０１２３】

構成情報収集プログラム１２０１の実行後、プログラム実行部１０６（ｘ）は、当該構成情報収集プログラム１２０１が自身の制御装置１０（ｘ）に対応したプログラムであるか否かを確認する（Ｓ６０５）。具体的には、例えば、プログラム実行部１０６（ｘ）は、構成情報収集プログラム１２０１の収集対象ＩＰアドレス１２０２又は構成情報収集スクリプト１２０３に登録されている制御装置１０の情報を確認する。

【０１２４】

構成情報収集プログラム１２０１が自身に対応したプログラムでなかった場合には（Ｓ６０５：不一致）、接続先の制御装置１０に誤りがあるため、プログラム実行部１０６（ｘ）は、構成情報収集プログラム実行処理は終了する（Ｓ６０６）。

【０１２５】

一方、構成情報収集プログラム１２０１が自身に対応したプログラムであった場合には（Ｓ６０５：一致）、プログラム実行部１０６（ｘ）は、構成情報収集プログラム１２０１（収集テンプレート情報１１０１）に従って、所定の機能に基づき、制御装置１０（ｘ）の内部構成の情報を収集する（Ｓ６０７）。そして、プログラム実行部１０６（ｘ）は、構成情報収集プログラム１２０１の実行有無フラグ１２０４を「実行済」に設定する（構成情報収集プログラム１２０１を更新する）（Ｓ６０８）。

【０１２６】

制御装置１０（ｘ）の外部媒体接続部１０３（ｘ）は、Ｓ６０７で収集した内部構成の情報と、Ｓ６０８で更新した構成情報収集プログラム１２０１とを、外部記憶媒体３０に送信する。

【０１２７】

外部記憶媒体３０の構成格納部３０２は、制御装置１０（ｘ）から受信した内部構成の情報を構成情報１３０１として記憶する（Ｓ６０９）。また、外部記憶媒体３０の構成情報収集プログラム格納部３０１は、制御装置１０（ｘ）から受信した構成情報収集プログ

ラム１２０１を記憶する（Ｓ６１０）。以上で構成情報収集プログラム実行処理は終了する。

【０１２８】

なお、収集対象装置が複数ある場合、各収集対象装置に関して、以上の構成情報収集プログラム実行処理が実行される。

【０１２９】

ここで、構成情報について説明する。

【０１３０】

（構成情報）

図１６は、構成情報１３０１の一例を示す図である。構成情報１３０１は、制御システム５０における制御装置１０（機器）の識別子１３０２と、内部構成の情報１３０６の収集日時１３０３と、識別子１３０２に係る制御装置１０を特定する情報であるＩＰアドレス１３０４と、識別子１３０２に係る制御装置１０で動作しているＯＳ情報１３０５と、識別子１３０２に係る制御装置１０における内部構成の情報１３０６とを含む。

【０１３１】

なお、構成情報１３０１の構成要素はここで説明したものに限定されるものではなく、また、その各情報の格納順序もここで説明した順序に限定されるものではない。

【０１３２】

＜資産情報更新処理＞

図１７は、資産情報更新処理の一例を説明するフロー図である。なお、この処理は、構成情報収集プログラム実行処理の実行後、所定のタイミング（例えば、所定の時間間隔、所定の時刻、又はユーザにより指定されたタイミング）で実行される。なお、この処理の開始に際して、ユーザは、外部記憶媒体３０を資産管理装置２０に接続する。

【０１３３】

まず、資産管理装置２０の外部媒体接続部２１３は、外部記憶媒体３０に、接続確認コマンド７０１を送信する。外部記憶媒体３０の接続部３０３は、接続確認コマンド７０１を受信すると、資産管理装置２０との接続状態を示すレスポンス７０２を資産管理装置２０に送信する。

【０１３４】

その後、資産管理装置２０の外部媒体接続部２１３は、レスポンス７０２を確認する（Ｓ７０１）。レスポンス７０２が接続失敗を示している場合（又はレスポンス７０２を受信していない場合）は（Ｓ７０１：接続失敗）、外部媒体接続部２１３は、資産情報更新処理を終了する（Ｓ７０２）。

【０１３５】

レスポンス７０２が接続成功を示している場合は（Ｓ７０１：接続成功）、資産構成管理部２０６は、構成情報収集プログラム１２０１の取得を要求する構成情報収集プログラム取得コマンド７０３を送信する。

【０１３６】

外部記憶媒体３０の構成情報収集プログラム格納部３０１は、構成情報収集プログラム取得コマンド７０３の受信に応じて、構成情報収集プログラム１２０１を取得する（Ｓ７０３）。接続部３０３は、この構成情報収集プログラム１２０１を資産管理装置２０に送信する。

【０１３７】

資産管理装置２０の資産構成管理部２０６は、外部記憶媒体３０から受信した構成情報収集プログラム１２０１の実行有無フラグ１２０４を確認する。実行有無フラグ１２０４が「実行済」になっていることを確認後、資産構成管理部２０６は、構成情報収集プログラム１２０１の収集対象ＩＰアドレス１２０２の内容を抽出する（Ｓ７０４）。

【０１３８】

そして、資産構成管理部２０６は、この抽出したＩＰアドレスに係る制御装置１０の内部構成の情報の取得を要求するためのコマンドである構成情報取得コマンド７０５を、外

部記憶媒体３０に送信する。
【０１３９】
外部記憶媒体３０の構成格納部３０２は、構成情報取得コマンド７０５の受信に応じて、構成情報取得コマンド７０５が示す制御装置１０に係る構成情報１３０１を取得する（Ｓ７０５）。外部記憶媒体３０の接続部３０３は、取得した構成情報１３０１を資産管理装置２０に送信する。
【０１４０】
資産管理装置２０の資産構成管理部２０６は、このシステム構成情報９０１を取得する（Ｓ７０６）。そして、システム構成格納部２０９は、取得したシステム構成情報９０１を、外部記憶媒体３０から受信した構成情報１３０１で更新する（Ｓ７０７）。
【０１４１】
具体的には、例えば、資産構成管理部２０６は、システム構成情報９０１のうち、受信した構成情報１３０１の機器識別子１３０２に対応する機器識別子９０２のレコードにおいて、システム構成情報９０１の収集日時９０３で構成情報１３０１の収集日時１３０３を更新し、システム構成情報９０１のＩＰアドレス９０４で構成情報１３０１のＩＰアドレス１３０４を更新し、システム構成情報９０１のＯＳ情報９０５で構成情報１３０１のＯＳ情報１３０５を更新し、システム構成情報９０１の内部構成９０７で構成情報１３０１の内部構成の情報１３０６を更新する（対応する情報がなかった場合は追加する）。
【０１４２】
システム構成格納部２０９は、Ｓ７０７で更新したシステム構成情報９０１を記憶し、資産情報更新処理を終了する（Ｓ７０８）。
【０１４３】
その後、ユーザは、構成情報１３０１（内部構成の情報）を確認することにより、特に制御上の問題がある制御装置１０を確定し、この制御装置１０に対して適切な対応を取る。例えば、所定のネットワークから、ＯＳ又は外部サービス等のソフトウェアに関する更新プログラムを取得して制御装置１０にインストールする、制御装置１０を停止する、他の制御装置１０と交換する、その他制御システム５０の構成を変更する等の対応が考えられる。
【０１４４】
なお、以上の対応は、資産管理装置１０が、更新した構成情報９０１に基づき自動的に行ってもよい。
【０１４５】
以上のように、本実施形態の資産情報管理システム１は、制御システム５０の通信状態の情報に基づき制御システム５０の構成を推定し、脆弱性情報１００１及び、推定した制御システム５０の構成に基づき、制御装置１０のそれぞれの制御上のリスクを推定し、所定の条件（優先順位）の制御上のリスクを有する制御装置１０（収集対象装置）を特定し、その収集対象装置が管理する資産の構成の情報を取得する。
【０１４６】
すなわち、ネットワーク４０の通信状態の情報に基づき制御システム５０の構成を推定し、この推定結果に基づき、リスクを有する制御装置１０のみを資産情報の収集対象としている。これにより、制御システム５０内の資産情報を、制御システム５０内の制御装置１０やネットワーク４０に対して大きな負荷をかけることなく収集することができる。そして、制御装置１０のリスクに応じて、必要な資産情報のみを効率よく収集することができる。
【０１４７】
このように、本実施形態の資産情報管理システム１によれば、制御システムに対する影響を抑えつつ、制御システムの安定制御に必要な資産情報を取得することができる。
【０１４８】
［第２実施形態］
第１実施形態では、構成情報収集プログラム１２０１が外部記憶媒体３０に記憶され、

各制御装置１０が外部記憶媒体３０から構成情報収集プログラム１２０１を読み出して実行する形態である。

【０１４９】

これに対して、本実施形態は、外部記憶媒体３０を用いることなく、各制御装置１０が構成情報収集プログラム１２０１をそれぞれ実行する形態である。

【０１５０】

＜構成及び機能＞

図１８は、第２実施形態に係る資産情報管理システム１の構成及び機能の一例を説明する図である。第１実施形態と同様の構成には同一の符号を付している。以下、第１実施形態と異なる点を中心に説明する。

【０１５１】

本実施形態に係る資産情報管理システム１は、資産管理装置２０と、複数の制御装置１０及び制御対象の装置７０を含む制御システム５０とを含んで構成されており、これらはネットワーク４０により通信可能に接続されている。すなわち、資産情報管理システム１は、第１実施形態と異なり外部記憶媒体３０を有しない。

【０１５２】

また、制御装置１０は、第１実施形態と異なり、外部媒体接続部１０３を有しない。資産管理装置２０も、第１実施形態と異なり、外部媒体接続部２１３を有しない。

【０１５３】

制御装置１０及び資産管理装置２０のハードウェア構成は第１実施形態と同様である。

【０１５４】

次に、資産情報管理システム１が行う処理について説明する。

【０１５５】

本実施形態では、資産情報管理システム１は、資産管理装置２０が構成情報収集プログラム１２０１を直接各制御装置１０に送信し、各制御装置１０がその内部構成の情報を収集し、資産管理装置２０がその内部構成の情報を直接受信する処理（以下、内部構成情報自動収集処理という）を行う。

【０１５６】

具体的には、まず、第１実施形態と同様に外部サービス情報取得処理が行われ、その後、内部構成情報自動収集処理が行われる。

【０１５７】

＜内部構成情報自動収集処理＞

図１９は、第２実施形態に係る内部構成情報自動収集処理の一例を説明するフロー図である。なお、この処理は、例えば、外部サービス情報取得処理の終了後、所定のタイミング（例えば、所定の時間間隔、所定の時刻、又はユーザにより指定されたタイミング）で実行される。

【０１５８】

まず、資産管理装置２０のシステム構成格納部２０９は、第１実施形態のＳ５０１と同様に、外部サービス情報取得処理で生成されたシステム構成情報９０１を取得する（Ｓ１７０１）。また、脆弱性格納部２１０は、第１実施形態のＳ５０２と同様に、脆弱性情報１００１を取得する（Ｓ１７０２）。

【０１５９】

資産管理装置２０のリスク評価部２０３は、第１実施形態のＳ５０３と同様に、Ｓ１７０１で取得したシステム構成情報９０１とＳ１７０２で取得した脆弱性情報１００とに基づき、各制御装置１０のリスクを算出する（Ｓ１７０３）。そして、収集対象特定部２０４は、第１実施形態のＳ５０４と同様に、Ｓ１７０３で算出したリスクに基づき、各制御装置１０の優先順位を算出し（Ｓ１７０４）、第１実施形態のＳ５０５と同様に、収集優先順位画面を表示する（Ｓ１７０５）。

【０１６０】

次に、資産管理装置２０の収集対象特定部２０４は、第１実施形態のＳ５０６と同様に

収集対象装置を特定し、構成情報収集プログラム生成部２０５は、第１実施形態のＳ５０６と同様に、特定した各収集対象装置について、収集テンプレート情報１１０１から、対応する構成情報収集スクリプト１１０３を取得し、取得した各構成情報収集スクリプト１１０３に基づき、各構成情報収集プログラム１２０１を生成する（Ｓ１７０６）。なお、ここでは、収集対象装置が制御装置１０（ｘ）であったものとする。

【０１６１】

すると、本実施形態では、資産管理装置２０の通信部２０７は、生成した構成情報収集プログラム１２０１を制御装置１０（ｘ）に送信する。そして、制御装置１０（ｘ）のプログラム実行部１０６（ｘ）は、第１実施形態のＳ６０４と同様に、所定の機能により、受信した構成情報収集プログラム１２０１を実行する（Ｓ１７０７）。

【０１６２】

プログラム実行部１０６（ｘ）は、第１実施形態のＳ６０５と同様に、構成情報収集プログラム１２０１を実行した制御装置１０が、構成情報収集プログラム１２０１で定義されている制御装置１０と一致しているか否かを判定する（Ｓ１７０８）。

【０１６３】

両者が一致していない場合は（Ｓ１７０８：不一致）、送信先の制御装置１０に誤りがあるとして、プログラム実行部１０６（ｘ）は、内部構成情報自動収集処理を終了する（Ｓ１７０９）。

【０１６４】

他方、両者が一致した場合は（Ｓ１７０８：一致）、プログラム実行部１０６（ｘ）は、第１実施形態のＳ６０７と同様に、構成情報収集プログラム１２０１に含まれている構成情報収集スクリプト１２０３に従って、制御装置１０（ｘ）の内部構成の情報を収集する（Ｓ１７１０）。

【０１６５】

第１実施形態のＳ６０８と同様に、プログラム実行部１０６（ｘ）は、構成情報収集プログラム１２０１に含まれている実行有無フラグ１２０４を「実行済」に更新する（Ｓ１７１１）。通信部１０５（ｘ）は、Ｓ１７１０で収集した内部構成の情報である構成情報１３０１と、Ｓ１７１１で更新した構成情報収集プログラム１２０１とを、資産管理装置２０に送信する。

【０１６６】

資産管理装置２０の資産構成管理部２０６は、第１実施形態のＳ７０４と同様に、制御装置１０（ｘ）から受信した構成情報収集プログラム１２０１に含まれる実行有無フラグ１２０４を確認することで、構成情報収集プログラム１２０１が実行されたか否かを判定する（Ｓ１７１２）。その結果、未実行と判定した場合には、資産構成管理部２０６は、再度、構成情報収集プログラム１２０１を制御装置１０（ｘ）に送信する（Ｓ１７１２：未実行）。

【０１６７】

他方、実行済と判定した場合には（Ｓ１７１２：実行済）、資産構成管理部２０６は、第１実施形態のＳ７０６と同様に、システム構成情報９０１を取得する（Ｓ１７１３）。

【０１６８】

そして、システム構成格納部２０９は、第１実施形態のＳ７０７と同様に、Ｓ１７１３で取得したシステム構成情報９０１を、制御装置１０（ｘ）から受信した構成情報１３０１で更新する（Ｓ１７１４）。

【０１６９】

また、システム構成格納部２０９は、第１実施形態のＳ７０８と同様に、Ｓ１７１４で更新したシステム構成情報９０１を記憶し、処理を終了する（Ｓ１７１５）。

【０１７０】

以上のように、本実施形態の資産情報管理システム１によれば、資産管理装置２０が、外部記憶媒体３０を介さずに、構成情報収集プログラム１２０１を制御装置１０に提供することができる。これにより、制御装置１０及び装置７０が多数存在する場合であっても

、迅速に資産の情報を更新することができる。

【０１７１】

本発明は上記の各実施形態に限定されるものではなく、様々な変形例が含まれる。例えば、上記した実施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。例えば、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。

【０１７２】

例えば、制御装置１０の資産管理装置２０の機能を含ませてもよく、資産管理装置２０の機能の一部を制御装置１０に含ませてもよい。また、制御装置１０及び資産管理装置２０の間の通信を、他の装置を経由して行ってもよい。

【０１７３】

また、本実施形態でデータベース形式の情報として示したデータについては、他の任意のデータ形式であってよい。

【０１７４】

また、本実施形態では、ネットワーク４０の負荷の状況を調べるためにパケット数、帯域の情報等を使用するものとしたが、通信量を示す他の情報を使用してもよい。

【０１７５】

また、本実施形態では、収集テンプレート情報１１０１及び構成情報収集スクリプトはＯＳ等のソフトウェアに依存するとしたが、制御装置１０や装置７０のハードウェアに依存する場合は、これらのハードウェアに応じた情報又はプログラムとしてもよい。

【０１７６】

また、本実施形態では、制御装置１０（装置７０）のリスクは、脆弱性を有するＯＳ又は外部サービスの有無又は数、脆弱性の危険度、前回の内部構成の情報の収集日時からの経過時間などから算出するものとしたが、その他のソフトウェアの情報、ハードウェアの仕様又は構成等の他の要素を利用して算出してもよい。

【０１７７】

また、本実施形態では、制御装置１０（装置７０）の優先順位の算出方法として、算出したリスクの大きさや、制御装置１０の物理的位置による算出方法を説明したが、ハードウェアの仕様又は構成等の他の要素を用いて算出してもよい。

【０１７８】

また、本実施形態では、構成情報収集プログラム等を格納する主体としてＵＳＢメモリ等の外部記憶媒体３０を使用するものとしたが、クラウド等の、資産情報管理システム１外の他の情報処理システムを使用してもよい。

【０１７９】

また、本実施形態では、収集対象装置を特定するための条件として、リスクの高さに基づく優先順位、日時、装置の物理的な位置を設定したが、他の条件（例えば、収集対象装置の最大台数）を設定してもよい。

【０１８０】

また、本実施形態では、内部構成の情報は、ＯＳ及びその他のソフトウェアの構成の情報であるとしたが、他の情報（例えば、各装置のハードウェアの情報、ネットワーク４０に関する情報、各装置の管理情報）を加えても、又は他の情報と置き換えてもよい。

【０１８１】

以上の本明細書の記載により、少なくとも次のことが明らかにされる。すなわち、各実施形態の資産情報管理システムは、前記特定した収集対象装置の情報に基づき、当該収集対象装置の資産の構成の情報を取得するための所定のプログラムを生成する構成情報収集プログラム生成部をさらに備え、前記資産構成管理部は、前記生成したプログラムに基づき、前記資産の構成の情報を取得する、としてもよい。

【０１８２】

このように、収集対象装置の資産の構成の情報を取得するための構成情報収集プログラムを生成し、このプログラムに基づき資産の構成の情報を取得することで、各収集対象装

置が多種多様の構成を有する場合であっても、それらの資産の構成の情報を確実に取得することができる。

【０１８３】

また、各実施形態の資産情報管理システムにおいて、前記リスク評価部は、前記制御システムの構成の過去の推定時から所定時までの時間の長さに応じて、前記制御装置のそれぞれの制御上のリスクの大きさを推定する、としてもよい。

【０１８４】

このように、制御システム５０の構成の過去の推定時から現在までの時間の長さに応じて制御装置１０の制御上のリスクの大きさを推定することで、例えば、長くその構成がチェックされていない制御装置１０についてはリスクが高いとする等、制御装置１０に対して、その現状に応じた適切なリスク評価をすることができる。

【０１８５】

また、各実施形態の資産情報管理システムにおいて、前記リスク評価部は、前記脆弱性情報の設定時から所定時までの時間の長さに応じて、前記制御装置のそれぞれの制御上のリスクの大きさを推定する、としてもよい。

【０１８６】

このように、脆弱性情報１００１の設定時から現在までの時間の長さに応じて制御装置１０の制御上のリスクの大きさを推定することで、例えば、長くその構成が更新されていない制御装置１０についてはリスクが高いとする等、制御装置１０に対して、その更新履歴に基づく適切なリスク評価をすることができる。

【０１８７】

また、各実施形態の資産情報管理システムにおいては、前記構成情報収集プログラム生成部は、前記生成したプログラムを所定の記憶装置に記憶し、前記収集対象装置は、前記記憶されたプログラムを実行し、当該収集対象装置が管理する前記資産の構成の情報を前記記憶装置に記憶するプログラム実行部を備え、前記資産構成管理部は、前記記憶された資産の構成の情報を、前記記憶装置から取得する、としてもよい。

【０１８８】

このように、構成情報収集プログラム１２０１を外部記憶媒体３０等の記憶装置に記憶し、収集対象装置が、その構成情報収集プログラム１２０１を実行して資産の構成の情報を得、資産管理装置がその資産の構成の情報を記憶装置から取得することで、構成情報収集プログラム１２０１を容易に管理することができる。例えば、ユーザは、構成情報収集プログラム１２０１を記憶可能な外部記憶媒体３０等を用いることで、様々な場所に設置されている、収集対象装置の制御装置１０（装置７０）からの情報収集及びその構成の更新を容易に行うことができる。

【０１８９】

また、各実施形態の資産情報管理システムにおいては、前記プログラム実行部は、前記プログラムが前記収集対象装置で実行されたか否かを判定し、前記プログラムが前記収集対象装置で実行されたと判定した場合にのみ、当該収集対象装置が管理する資産の構成の情報を前記記憶装置に記憶する、としてもよい。

【０１９０】

このように、構成収集プログラムが収集対象装置で実行されたと判定した場合にのみ、その資産の構成の情報を記憶装置に記憶することで、記憶装置に、誤った制御装置１０における資産の構成の情報が記憶されることを防ぐことができる。

【０１９１】

また、各実施形態の資産情報管理システムにおいては、前記推定した前記制御システムの構成の情報、及び、前記取得した収集対象装置が管理する資産の構成の情報のうち少なくともいずれかを出力する入出力部を備える、としてもよい。

【０１９２】

このように、制御システム５０の構成の情報、又は、収集対象装置が管理する資産の構成の情報を表示することで、ユーザは、制御システム５０の現状、及び制御システム５０

において制御上重要な制御装置１０の情報を知ることができる。

【０１９３】

また、各実施形態の資産情報管理システムにおいては、前記収集対象特定部は、前記所定の条件として、前記リスクに基づく前記収集対象装置の候補としての優先順位の情報を設定し、前記入出力部は、前記収集対象装置の構成の情報と共に、前記優先順位の情報を出力する、としてもよい。

【０１９４】

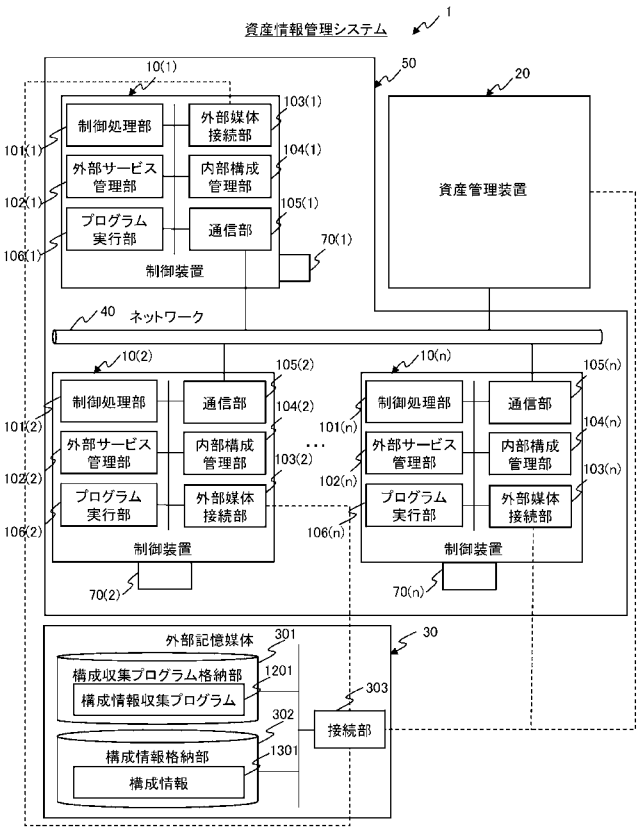
このように、収集対象装置の決定に関してリスクに基づく優先順位の条件を設定しておき、収集対象装置の構成の情報と共に、その優先順位の情報を出力するようにすることで、制御システム５０による制御における各制御装置１０の重要性についてより詳細な情報を得ることができる。

【符号の説明】

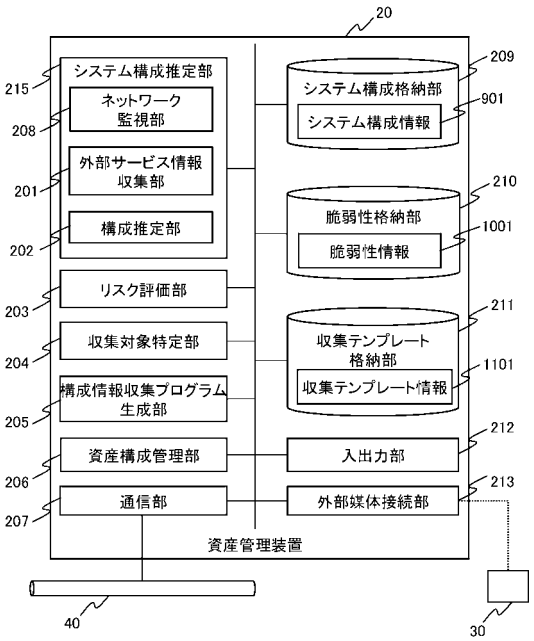
【０１９５】

１　資産情報管理システム、１０　制御装置、７０　装置、２０　資産管理装置、３０　外部記憶媒体、５０　制御システム、２１５　システム構成推定部、２０３　リスク評価部、２０４　収集対象特定部、２０６　資産構成管理部、１００１　脆弱性情報

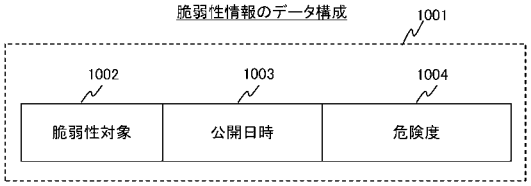
【図１】



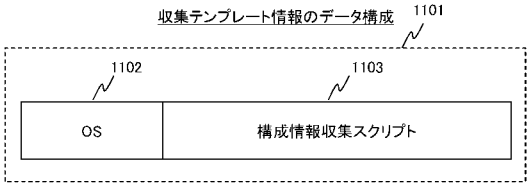
【図２】



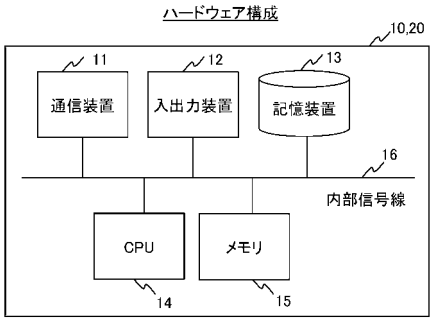
【図３】



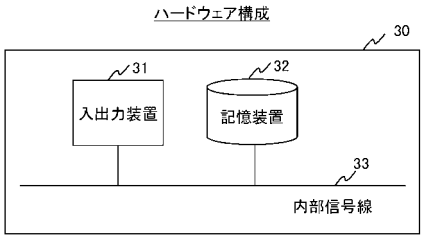
【図４】



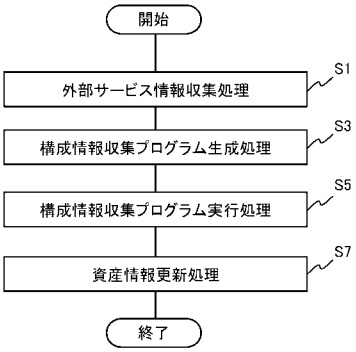
【図５】



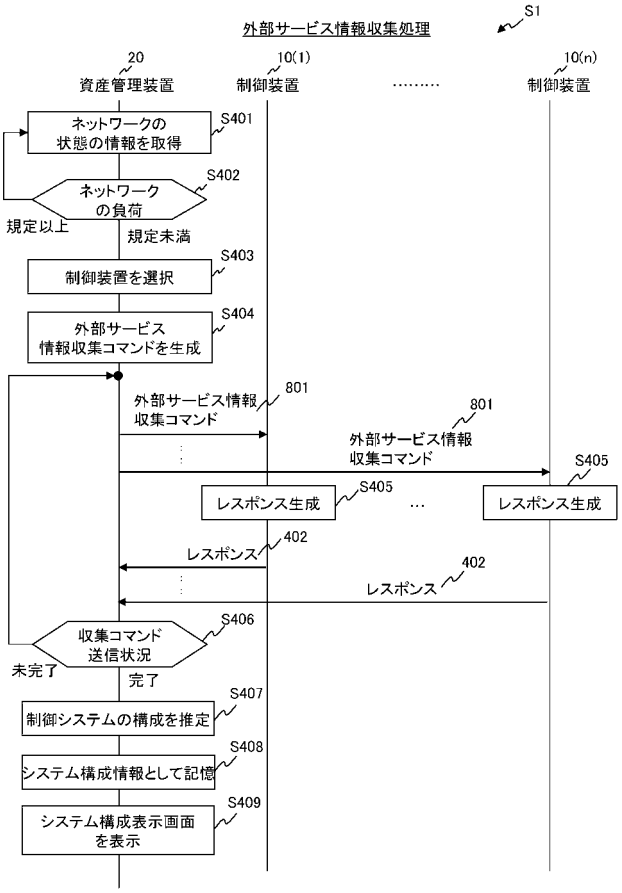
【図６】



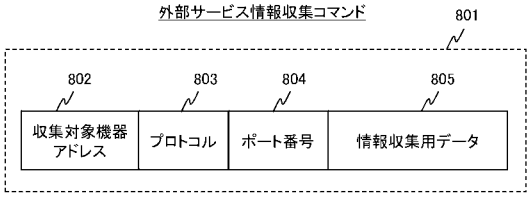
【図７】



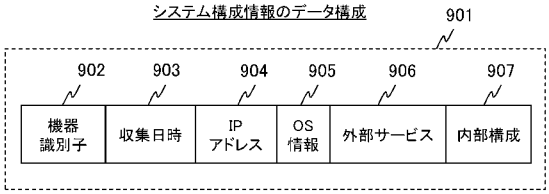
【図８】



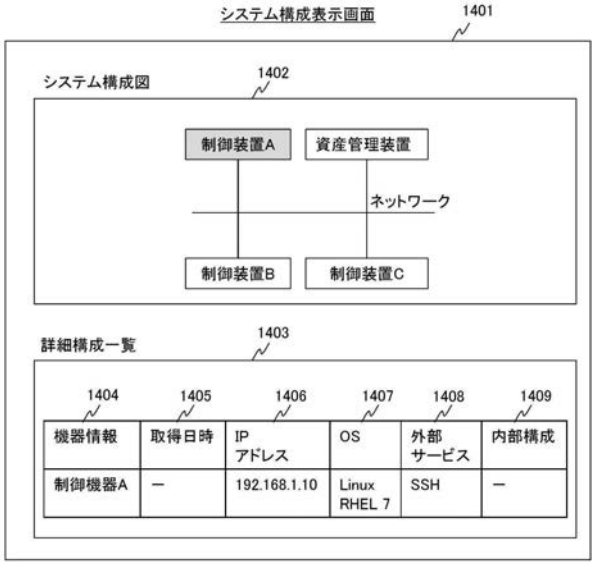
【図９】



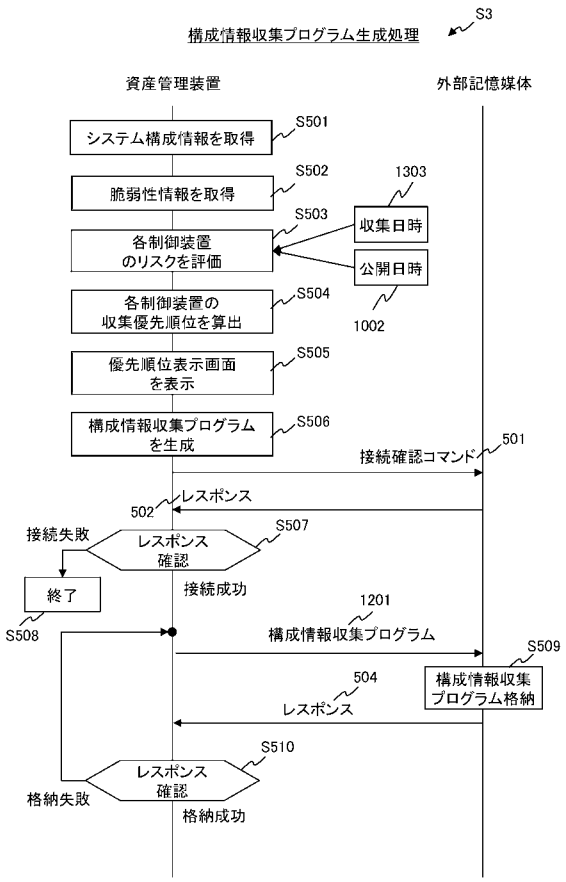
【図１０】



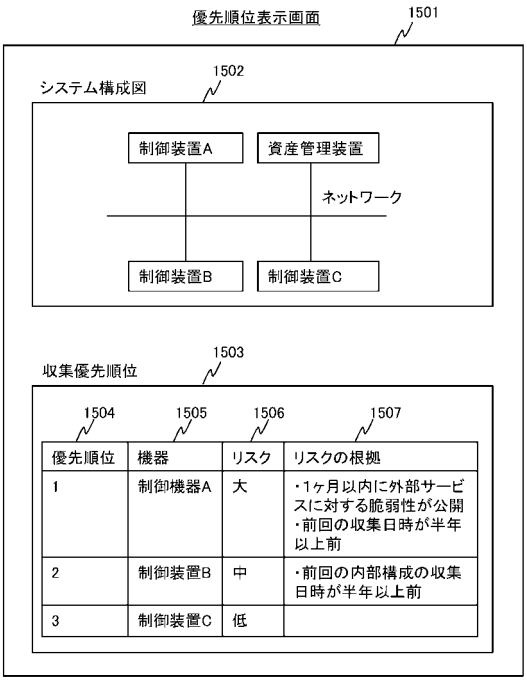
【図１１】



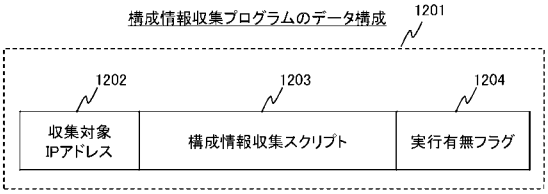
【図１２】



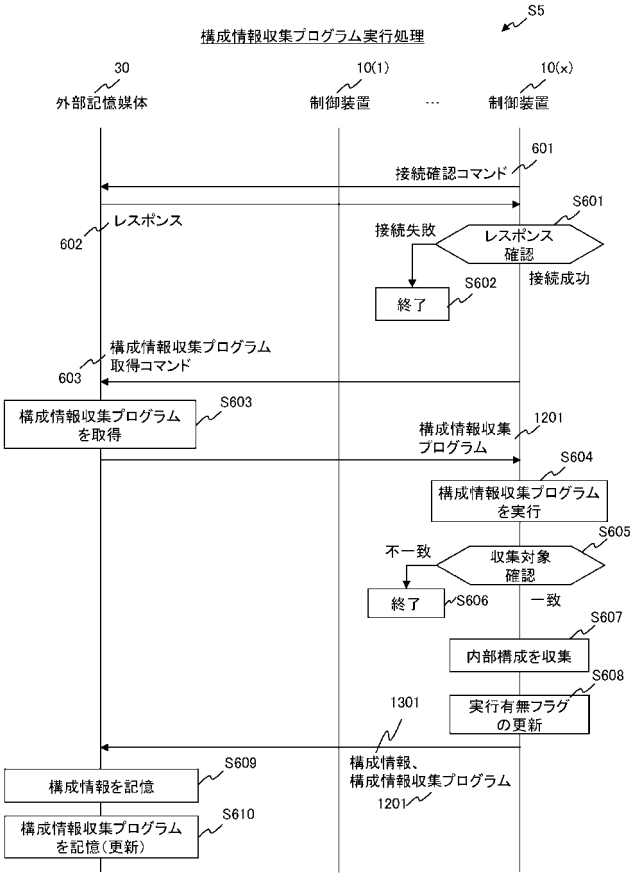
【図１３】



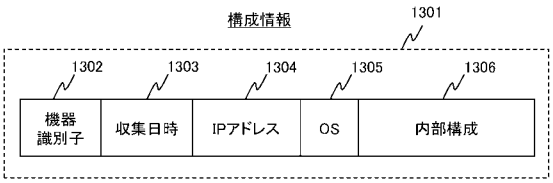
【図１４】



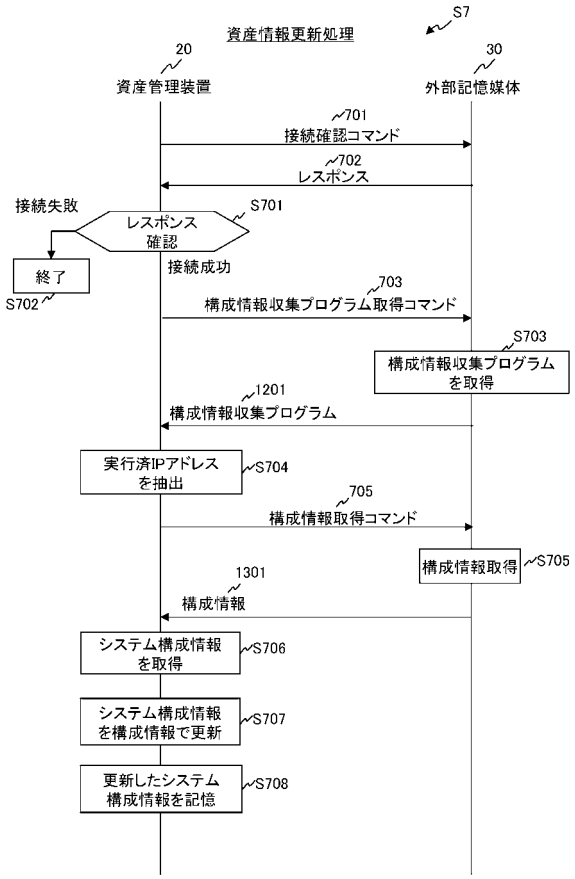
【図１５】



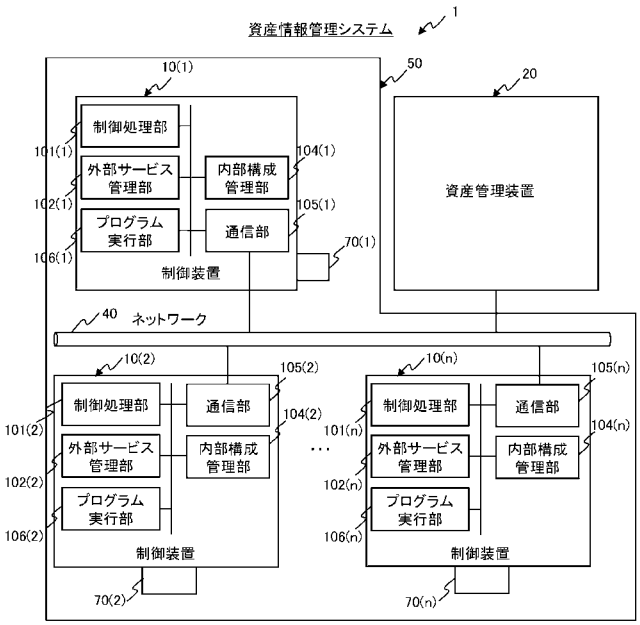
【図１６】



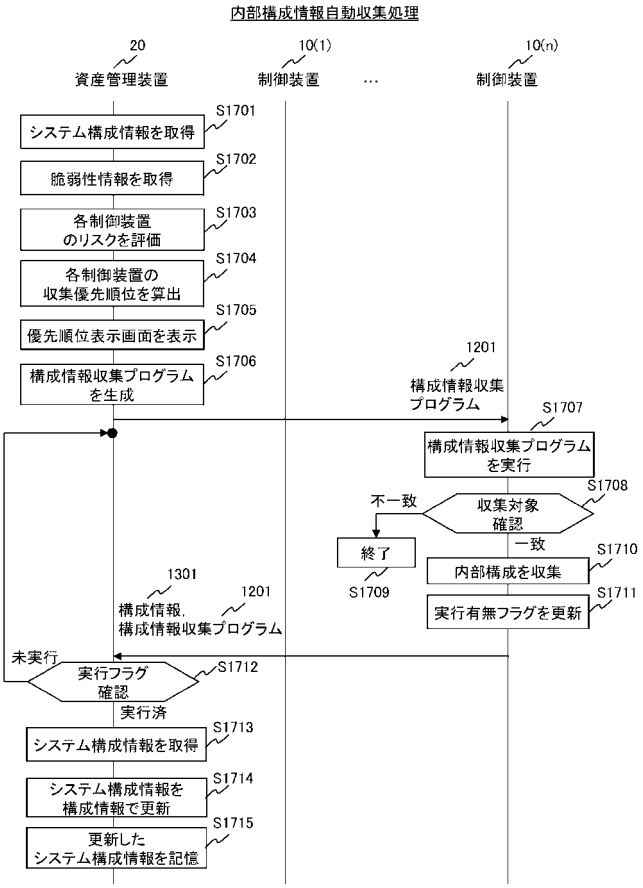
【図１７】



【図１８】


資産情報管理システム
1
10(1)
50
20
制御処理部
101(1)
外部サービス管理部
102(1)
プログラム実行部
106(1)
内部構成管理部
104(1)
通信部
105(1)
70(1)
制御装置
資産管理装置
40
ネットワーク
10(2)
105(2)
制御処理部
通信部
101(2)
外部サービス管理部
104(2)
内部構成管理部
102(2)
プログラム実行部
106(2)
制御装置
70(2)
10(n)
105(n)
制御処理部
通信部
101(n)
外部サービス管理部
104(n)
内部構成管理部
102(n)
プログラム実行部
106(n)
制御装置
70(n)

【図１９】


内部構成情報自動収集処理
20
資産管理装置
10(1)
制御装置
…
10(n)
制御装置
S1701
システム構成情報を取得
S1702
脆弱性情報を取得
S1703
各制御装置のリスクを評価
S1704
各制御装置の収集優先順位を算出
S1705
優先順位表示画面を表示
S1706
構成情報収集プログラムを生成
1201
構成情報収集プログラム
S1707
構成情報収集プログラムを実行
S1708
収集対象確認
不一致
終了
S1709
一致
S1710
内部構成を収集
S1711
実行有無フラグを更新
1301
構成情報，
1201
構成情報収集プログラム
未実行
S1712
実行フラグ確認
実行済
S1713
システム構成情報を取得
S1714
システム構成情報を構成情報で更新
S1715
更新したシステム構成情報を記憶