(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2012-48556
(P2012-48556A)
(43)公開日　平成24年3月8日(2012.3.8)

(51)Int.Cl.		F I			テーマコード（参考）
G06F 21/20	(2006.01)	G06F	15/00	330A	5B276
G06F 21/22	(2006.01)	G06F	9/06	660Z	5B285

審査請求 有　請求項の数 5　ＯＬ　（全 9 頁）

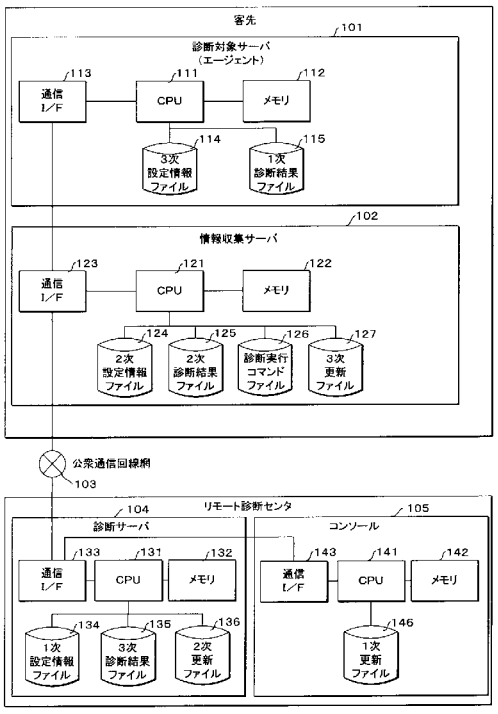
(21)出願番号　特願2010-190956 (P2010-190956)
(22)出願日　平成22年8月27日 (2010.8.27)

(71)出願人　302061130
東芝ＩＴサービス株式会社
東京都港区芝浦四丁目９番２５号
(74)代理人　110000235
特許業務法人　天城国際特許事務所
(72)発明者　大谷　武良
東京都港区芝浦四丁目９番２５号　東芝ＩＴサービス株式会社内
(72)発明者　小西　正志
東京都港区芝浦四丁目９番２５号　東芝ＩＴサービス株式会社内

Ｆターム(参考)　5B276 FD00
5B285 AA06　BA03　CA32　CA36

(54)【発明の名称】リモートセキュリティ診断システム

(57)【要約】
【課題】コンピュータが遠隔地にある場合にはオペレータが監視対象のコンピュータのある場所まで出向かなければならず、人手、時間、工数がかかるという問題点を解決する。
【解決手段】セキュリティを診断するエージェントを備える診断対象サーバと、このエージェントにセキュリティ診断の指示を行い、エージェントから受信したセキュリティの診断データを、インターネットを介して送信する情報収集サーバと、情報収集サーバから受信した診断データを解析する診断サーバと、を備える。
【選択図】図１



【特許請求の範囲】
【請求項１】
セキュリティを診断するエージェントを備える診断対象サーバと、
前記エージェントに前記診断対象サーバのセキュリティ診断を行うための指示を送信し、前記セキュリティ診断の結果である診断データを、公衆通信回線網を介して送信する情報収集サーバと、
前記情報収集サーバから受信した診断データを解析する診断サーバと、
を備えるリモートセキュリティ診断システム。
【請求項２】
前記診断サーバは、
前記情報収集サーバと通信を確立するとき、前記情報収集サーバからのアクセスを待ち、情報収集サーバからのアクセスがあった後に通信を確立する請求項１記載のリモートセキュリティ診断システム。
【請求項３】
前記情報収集サーバが、
更新情報を、前記公衆通信回線網を介して前記診断サーバからダウンロードし、
前記診断対象サーバが、
前記情報収集サーバが前記診断サーバからダウンロードした更新情報を前記情報収集サーバからダウンロードする更新処理を行う請求項２記載のリモートセキュリティ診断システム。
【請求項４】
前記診断サーバは、
前記診断データを解析して異常を判定したとき、前記情報収集サーバが前記更新処理を行うのを待機する請求項３記載のリモートセキュリティ診断システム。
【請求項５】
前記診断サーバは、
前記診断データの解析結果をメール送信する請求項４記載のリモートセキュリティ診断システム。
【発明の詳細な説明】
【技術分野】
【０００１】
本発明の実施形態は、監視すべきサーバ乃至コンピュータのセキュリティを遠隔監視するリモートセキュリティ診断システムに関する。
【背景技術】
【０００２】
サーバやクライアント等のコンピュータはオペレーションシステム、ウイルス対策プログラムなどのソフトウエアの陳腐化や、簡素なパスワード、容易に類推できるアカウント名などのソフトウエアの設定などにより、いわゆるセキュリティが低下することがある。
【０００３】
このセキュリティの低下の診断は人手に頼ることは工数の面や見落としが発生する危険性から問題がある。
【０００４】
そこで、セキュリティの低下を診断するエージェントを監視対象のサーバ、クライアントに常駐させ、このエージェントの診断結果を収集することによりセキュリティを監視する技術が提案されている。
【先行技術文献】
【特許文献】
【０００５】
【特許文献１】特開２００３－２４２１１２号公報
【発明の概要】

【発明が解決しようとする課題】
【０００６】
しかし、上述の技術によってはコンピュータが遠隔地にある場合にはオペレータが監視対象のコンピュータのある場所まで出向かなければならず、人手、時間、工数がかかるという問題点がある。
【課題を解決するための手段】
【０００７】
上記の課題を解決するために、本発明の一実施形態はセキュリティを診断するエージェントを備える診断対象サーバと、エージェントに診断対象サーバのセキュリティ診断を行うための指示を送信し、セキュリティ診断の結果である診断データを、公衆通信回線網を介して送信する情報収集サーバと、情報収集サーバから受信した診断データを解析する診断サーバと、を備えるリモートセキュリティ診断システムを提供する。
【図面の簡単な説明】
【０００８】
【図１】リモートセキュリティ診断システムの構成を表す図である。
【図２】１次設定情報ファイル、２次設定情報ファイル、３次設定情報ファイル、１次更新ファイル、２次更新ファイル、及び３次更新ファイルのファイル構造を示す図である。
【図３】診断実行コマンドファイルのデータ構造を示す図である。
【図４】１次診断結果ファイル、２次診断結果ファイル、及び３次診断結果ファイルのファイル構造を示す図である。
【図５】診断対象サーバ、情報収集サーバ、診断サーバ、及びコンソールの情報更新動作を示すフローチャートである。
【図６】診断サーバ、情報収集サーバ、診断サーバ、及びコンソールのセキュリティ診断動作を示すフローチャートである。
【発明を実施するための形態】
【０００９】
以下、本発明によるリモートセキュリティ診断システムの一実施形態について、図面を用いて詳細に説明する。
【００１０】
リモートセキュリティ診断システムは、セキュリティを診断するエージェントを備える診断対象サーバと、エージェントに診断対象サーバのセキュリティ診断を行うための指示を送信し、セキュリティ診断の結果である診断データを、公衆通信回線網を介して送信する情報収集サーバと、情報収集サーバから受信した診断データを解析する診断サーバと、を備える。
【００１１】
図１は、本実施形態のリモートセキュリティ診断システムの構成を表す図である。図１に示すように、リモートセキュリティ診断システムは、遠隔地である客先に設置される診断対象サーバ／クライアント（以下、単に診断対象サーバ１０１と呼ぶ。）、客先に設置され、診断対象サーバ１０１に接続される情報収集サーバ１０２と、客先とは別の場所にあるリモート診断センタに設置され、この情報収集サーバ１０２とインターネットなどの公衆通信回線網１０３を介して接続される診断サーバ１０４及びコンソール１０５と、を備える。
【００１２】
診断対象サーバ１０１は、演算装置であるＣＰＵ１１１と、記憶装置であるメモリ１１２と、通信インターフェース（以下、インターフェースをＩ／Ｆと略す。）１１３と、診断対象サーバ１０１の現在の設定情報を格納する３次設定情報ファイルと、セキュリティの診断結果を格納する１次診断結果ファイル１１５と、を備える。
【００１３】
診断対象サーバ１０１は、診断対象サーバ１０１のセキュリティを診断する常駐プログラムであるエージェントを備える。

【００１４】
情報収集サーバ１０２は、演算装置であるＣＰＵ１２１と、記憶装置であるメモリ１２２と、通信Ｉ／Ｆ１２３と、情報収集サーバ１０２の現在の設定情報を格納する２次情報設定ファイル１２４と、セキュリティ診断の結果を格納する２次診断結果ファイル１２５と、診断対象サーバ１０１のエージェントに与える診断コマンドを格納する診断実行コマンドファイル１２６と、更新情報を格納する３次更新ファイル１２７と、を備える。診断対象サーバ１０１は、情報収集サーバ１０２と通信Ｉ／Ｆ１１３を介して接続される。
【００１５】
情報収集サーバ１０２は、エージェントに診断対象サーバ１０１のセキュリティ診断を指示し、エージェントから送信される診断データを収集する。情報収集サーバ１０２は、収集した診断情報を、公衆通信回線網１０３を介してリモート診断センタの診断サーバ１０４に一括して送信する。
【００１６】
エージェントがセキュリティの診断を行う場合、情報収集サーバ１０２からの指示が必要となる。ここで、診断サーバ１０４が直接エージェントにセキュリティ診断を行う旨の指示を出すようにシステムを構成すると、診断対象サーバ１０１に対して外部からのアクセスを許すこととなり、セキュリティが低下する。従って、診断対象サーバ１０１のセキュリティ維持のために情報収集サーバ１０２が必要となる。
【００１７】
診断サーバ１０４は、演算装置であるＣＰＵ１３１と、記憶装置であるメモリ１３２と、診断情報サーバ１０４の現在の設定情報を格納する１次設定情報ファイル１３４と、セキュリティ診断の結果を格納する３次診断結果ファイル１３５と、更新情報を格納する２次更新ファイル１３６と、を備える。診断サーバ１０４は、情報収集サーバ１０２と通信Ｉ／Ｆ１３３を介して接続される。
【００１８】
診断サーバ１０４は、通信の確立に際しては情報収集サーバ１０２に最初にアクセスしない。診断サーバ１０４は情報収集サーバ１０２からのアクセスを待ち、情報収集サーバ１０２からのアクセスがあった後に通信を確立する。
【００１９】
従って、情報収集サーバ１０２は診断サーバ１０４のアクセスを制限する設定を行う必要がない。
【００２０】
コンソール１０５は、演算装置であるＣＰＵ１４１と、記憶装置であるメモリ１４２と、通信Ｉ／Ｆ１４３と、更新情報を格納する１次更新ファイルと、を備える。診断サーバ１０４は、コンソール１０５と通信Ｉ／Ｆ１４３を介して接続される。
【００２１】
図２は、１次設定情報ファイル１３４、２次設定情報ファイル１２４、３次設定情報ファイル１１４、１次更新ファイル１４６、２次更新ファイル１３６、及び３次更新ファイル１２７のファイル構造を示す図である。１次設定情報ファイル１３４、２次設定情報ファイル１２４、３次設定情報ファイル１１４、１次更新ファイル１４６、２次更新ファイル１３６、及び３次更新ファイル１２７は同じファイル構成をとる。
【００２２】
図２に示すように、１次設定情報ファイル１３４、２次設定情報ファイル１２４、３次設定情報ファイル１１４、１次更新ファイル１４６、２次更新ファイル１３６、及び３次更新ファイル１２７は、診断ツールのバージョンと、セキュリティ診断用のエージェントのバージョンであるエージェント診断エンジンバージョンと、エージェントファイルのバージョンであるエージェントアップグレードファイルバージョンと、エージェント管理のための子マネージャファイルのバージョンを示すエージェント管理用子マネージャバージョンと、親マネージャとの通信サービスに使用されるプログラムのバージョンを示す親マネージャ通信用子マネージャバージョンと、親マネージャアクセスＩＤと、アクセスＩＤ

パスワードと、子マネージャコマンドクリアと、エージェント管理サービスリセットと、を格納する。

【００２３】

図３は、診断実行コマンドファイル１２６のデータ構造を示す図である。図３に示すように、診断実行コマンドファイル１２６は、診断コマンドに一意に割り当てられる診断コマンドＩＤと、診断開始予定時刻と、診断開始日時と、診断完了日時と、診断するエージェントの数と、を格納する。

【００２４】

図４は、１次診断結果ファイル１１５、２次診断結果ファイル１２５、及び３次診断結果ファイル１３５のファイル構造を示す図である。

【００２５】

図４に示すように、１次診断結果ファイル１１５、２次診断結果ファイル１２５、及び３次診断結果ファイル１３５は、診断対象機器ＩＤと、診断実施日時と、診断コマンドＩＤと、診断対象機器のオペレーションシステム名である診断対象機器ＯＳと、診断対象機器に適用されているオペレーションシステムのサービスパックバージョンである適用サービスパックと、診断対象機器に適用されているオペレーションシステムの適用パッチＮｏ．と、診断結果であるセキュリティレベルと、を格納する。

【００２６】

図５は、診断対象サーバ１０１、情報収集サーバ１０２、診断サーバ１０４、及びコンソール１０５の情報更新動作を示すフローチャートである。

【００２７】

診断対象サーバ１０１は診断の基準を定期的に更新する必要がある。診断の基準が陳腐化するとセキュリティの診断を誤ることがあるからである。

【００２８】

図５に示すように、ステップ２０１において、診断サーバ１０４はコンソール１０５の１次更新ファイル１４６と診断サーバ１０４の１次設定情報ファイル１３４とを比較する。

【００２９】

ステップ２０２において、診断サーバ１０４は、１次更新ファイル１４６と１次設定情報ファイル１３４との比較結果から更新情報があるかを判定する。診断サーバ１０４は、更新情報がある場合ステップ２０３に進み、ない場合処理を終了する。

【００３０】

ステップ２０３において、診断サーバ１０４はコンソール１０５から更新情報をダウンロードする。

【００３１】

ステップ２０４において、診断サーバ１０４はダウンロードした更新情報により２次更新情報ファイル１３６を更新する。

【００３２】

ステップ２０５において、診断サーバ１０４は更新した情報に基づいて１次情報設定ファイル１３４を更新する。

【００３３】

ステップ２０６において、情報収集サーバ１０２は情報収集サーバ１０２の２次設定情報ファイル１２４と診断サーバ１０４の２次更新ファイル１３６とを比較する。

【００３４】

ステップ２０７において、情報収集サーバ１０２は、２次設定情報ファイル１２４と２次更新ファイル１３６との比較結果から更新情報があるかを判定する。情報収集サーバ１０２は、更新情報がある場合ステップ２０８に進み、ない場合処理を終了する。

【００３５】

ステップ２０８において、情報収集サーバ１０２は診断サーバ１０４から更新情報をダウンロードする。

【００３６】
ステップ２０９において、情報収集サーバ１０２はダウンロードした更新情報により３次更新情報ファイル１２７を更新する。
【００３７】
ステップ２１０において、情報収集サーバ１０２は更新した情報に基づいて２次情報設定ファイル１２４を更新する。
【００３８】
ステップ２１１において、診断対象サーバ１０１は診断対象サーバ１０１の３次設定情報ファイル１１４と情報収集サーバ１０２の３次更新ファイル１２７とを比較する。
【００３９】
ステップ２１２において、診断対象サーバ１０１は、３次設定情報ファイル１１４と３次更新ファイル１２７との比較結果から更新情報があるかを判定する。診断対象サーバ１０１は、更新情報がある場合ステップ２１３に進み、ない場合処理を終了する。
【００４０】
ステップ２１３において、診断対象サーバ１０１は情報収集サーバ１０２から更新情報をダウンロードする。
【００４１】
ステップ２１４において、診断対象サーバ１０１はダウンロードした更新情報により３次設定ファイル１１４を更新する。
【００４２】
以上に述べた情報更新動作において、通信確立の際に診断サーバ１０４は情報収集サーバ１０２に最初にアクセスせず、情報収集サーバ１０２は診断対象サーバ１０１に最初にアクセスしない。
【００４３】
従って、診断対象サーバ１０１のセキュリティの設定を変更することなしに、通常のインターネット通信により診断対象サーバ１０１は更新情報をダウンロードすることが可能となる。
【００４４】
図６は、診断対象サーバ１０１、情報収集サーバ１０２、診断サーバ１０４、及びコンソール１０５のセキュリティ診断動作を示すフローチャートである。
【００４５】
図６に示すように、ステップ３０１において情報収集サーバ１０２は診断内容を診断実行コマンドファイル１２６から取得する。
【００４６】
ステップ３０２において、情報収集サーバ１０２はセキュリティ診断の開始を指示するコマンドを診断対象サーバ１０１に送信する。
【００４７】
ステップ３０３において、診断対象サーバ１０１は診断開始のコマンドを受信すると、エージェントにより事前に定義された３次設定情報ファイル１１４の内容に従い診断対象サーバ１０１のセキュリティの診断を実施し、結果を１次診断結果ファイル１１５に格納する。
【００４８】
診断対象サーバ１０１がエージェントにより行う診断は例えば次のような項目が挙げられる。
【００４９】
すなわち、診断項目はセキュリティパッチの適用状態、パスワードの強さ、アカウント設定状態、ログインの設定状態、ネットワークの設定状態、監査ログ記録の設定状態、スタートアップの設定状態、等である。
【００５０】
ステップ３０４において、診断対象サーバ１０１はエージェントにより１次診断結果フ

ファイル１１５に格納した診断結果である診断データを情報収集サーバ１０２に送信する。情報収集サーバ１０２は受信した診断データを２次診断結果ファイル１２５に格納する。

【００５１】

ステップ３０５において、情報収集サーバ１０２は診断サーバ１０４に２次診断結果ファイル１２５に格納された診断データを送信する。

【００５２】

ステップ３０６において、診断サーバ１０４は受信した診断データを３次診断結果ファイル１３５に格納する。

【００５３】

ステップ３０７において、コンソール１０５は３次診断結果ファイル１３５に格納された診断データを解析する。

【００５４】

ステップ３０８において、コンソール１０５は報告用のレポートを、診断データを基に作成する。

【００５５】

ステップ３０９において、コンソール１０５は作成したレポートを顧客にメール送信する。

【００５６】

以上に述べたセキュリティ診断動作において、通信確立の際に診断サーバ１０４は情報収集サーバ１０２に最初にアクセスせず、情報収集サーバ１０２は診断対象サーバ１０１に最初にアクセスしない。

【００５７】

従って、診断対象サーバ１０１のセキュリティの設定を変更することなしに、通常のインターネット通信により診断対象サーバ１０１は診断データを送信することが可能となる。よって、診断対象サーバ１０１に第三者が公衆通信回線網１０３を介してアクセスすることは生じえず、高いセキュリティを確保しつつリモートによるセキュリティ診断が可能となる。

【００５８】

以上述べたように、本実施形態のリモートセキュリティ診断システムは、セキュリティを診断するエージェントを備える診断対象サーバ１０１と、このエージェントにセキュリティ診断の指示を行い、エージェントから受信したセキュリティの診断データを、インターネットを介して送信する情報収集サーバ１０２と、情報収集サーバ１０２から受信した診断データを解析する診断サーバ１０４と、を備える。

【００５９】

従って、診断対象サーバ１０１のセキュリティを低下させずに遠隔地から診断対象サーバ１０１のセキュリティ診断が可能となるという効果がある。

【００６０】

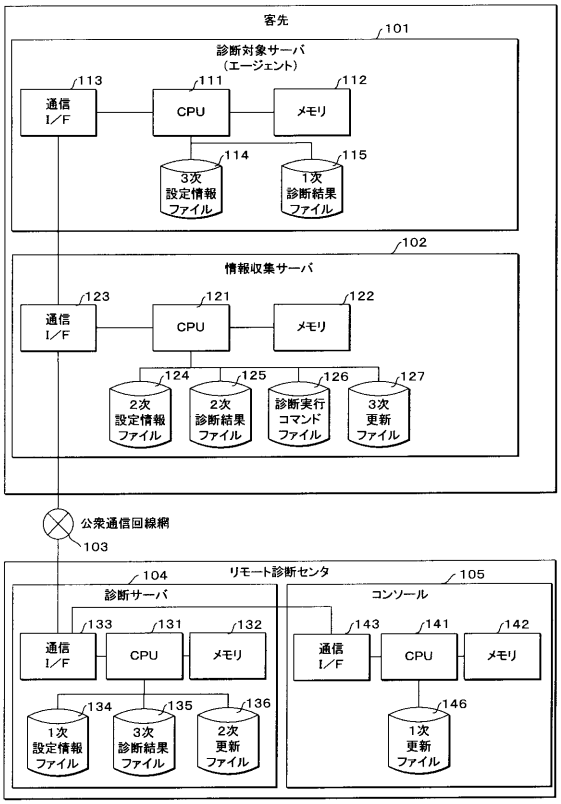
本発明のいくつかの実施形態を説明したが、これらの実施形態は、例として提示したものであり、発明の範囲を限定することは意図していない。これら実施形態は、その他の様々な形態で実施されることが可能であり、発明の要旨を逸脱しない範囲で、種々の省略、置き換え、変更を行うことができる。これら実施形態やその変形は、発明の範囲や要旨に含まれると同様に、特許請求の範囲に記載された発明とその均等の範囲に含まれるものである。

【符号の説明】

【００６１】

１０１：診断対象サーバ、
１０２：情報収集サーバ、
１０３：公衆通信回線網、
１０４：診断サーバ。

【図１】



【図２】

診断ツールバージョン
エージェント診断エンジンバージョン
エージェントアップグレードファイルバージョン
エージェント管理用子マネージャバージョン
親マネージャ通信用子マネージャバージョン
親マネージャアクセスID
アクセスIDパスワード
子マネージャコマンドクリア
エージェント管理サービスリセット

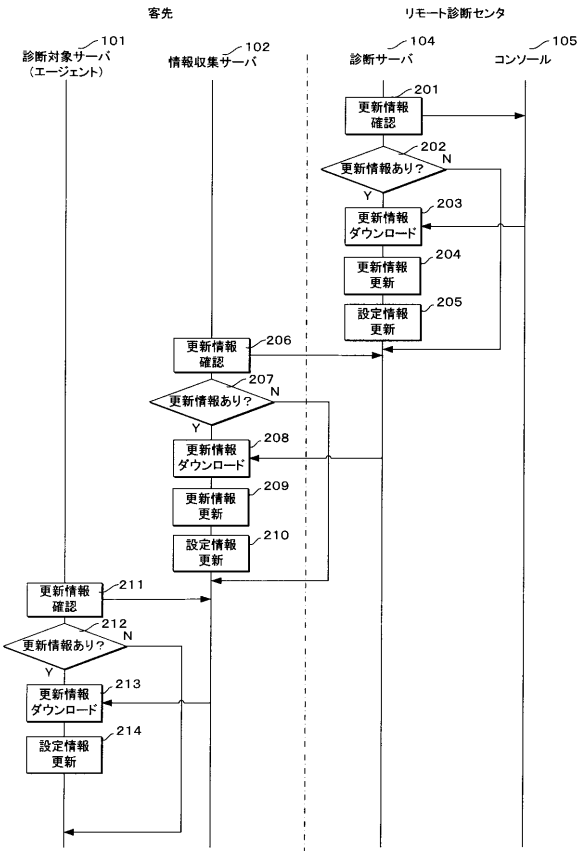
【図３】

診断コマンドID
診断開始予定日時
診断開始日時
診断完了日時
診断するエージェントの数

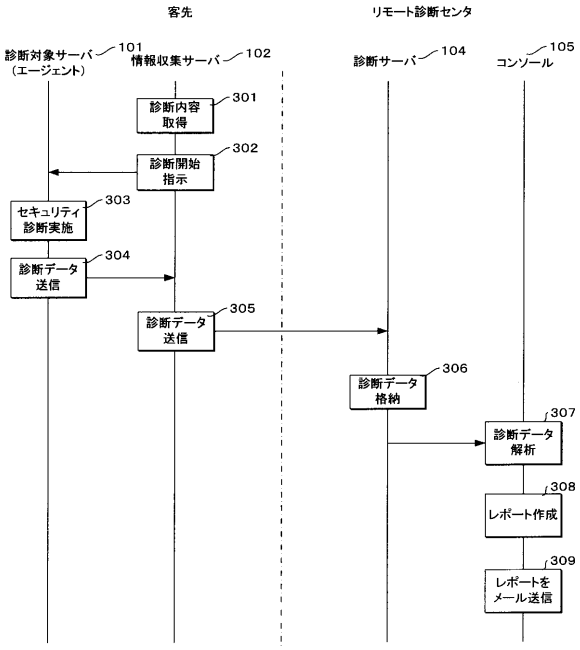
【図４】

診断対象機器ID
診断実施日時
診断コマンドID
診断対象機器OS
適用サービスパック
適用パッチNo.
セキュリティレベル

【図５】



【図６】


客先
リモート診断センタ
診断対象サーバ（エージェント）
101
情報収集サーバ
102
診断サーバ
104
コンソール
105
診断内容取得
301
診断開始指示
302
セキュリティ診断実施
303
診断データ送信
304
診断データ送信
305
診断データ格納
306
診断データ解析
307
レポート作成
308
レポートをメール送信
309