(19)日本国特許庁(JP)　(12)特　許　公　報(B2)　(11)特許番号
特許第3860420号
(P3860420)
(45)発行日　平成18年12月20日(2006.12.20)　(24)登録日　平成18年9月29日(2006.9.29)

(51)Int.Cl.		F I		
H04L 29/08	(2006.01)	H04L	13/00	307A
H04L 12/22	(2006.01)	H04L	12/22	
H04L 29/14	(2006.01)	H04L	13/00	315Z

請求項の数 2　(全 30 頁)

(21)出願番号　特願2001-4772(P2001-4772)
(22)出願日　平成13年1月12日(2001.1.12)
(65)公開番号　特開2002-208986(P2002-208986A)
(43)公開日　平成14年7月26日(2002.7.26)
審査請求日　平成15年12月18日(2003.12.18)

(73)特許権者　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　100089244
弁理士　遠山　勉
(74)代理人　100090516
弁理士　松倉　秀実
(72)発明者　野田　敏達
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　小村　昌弘
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】通信装置

(57)【特許請求の範囲】
【請求項１】
ネットワークを利用し電子的に情報を送信または受信する通信装置であり、
ネットワークにアクセスする通信部と、
通信を制御する制御部と、
送受信される情報の種類と問い合わせる相手装置の安全性に関連する情報の項目との関係を管理する情報項目管理部とを備え、
前記制御部は、送受信する情報の種類に応じて、前記情報項目管理部から相手装置の安全性に関連する情報の項目を選択し、情報の送受信の相手である相手装置に係る相手装置の安全性に関連する情報を当該相手装置に問い合わせ、その相手装置の安全性が所定の程度に確保されているか否かに基づいて、それ以降の送受信を行うか否かを判断する通信装置。
【請求項２】
前記制御部は、前記入手した相手装置の安全性に関連する情報を検証するテストパケットを前記通信部から相手装置に対して送信し、そのテストパケットへのレスポンスが妥当か否かを判定することにより相手装置を検証する請求項１記載の通信装置。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
本発明は、情報通信のセキュリティに関するものである。

【０００２】
【従来の技術】
従来からネットワークを利用し電子的に情報を交換する際、通信相手を確認するための認証が行われている。また、通信相手を照会し、その信頼性を確認するための与信サービス等が提供されている。また、通信経路の安全化を図るための暗号技術などが利用されている。
【０００３】
さらに、システムの安全性を確認するためのチェックサービスやハッキングサービスも提供されている。これは、例えば、確認対象のシステムに対して試みにハッキングするサービスである。
【０００４】
しかし、従来は、システムがその通信相手の安全性を確認する方法は提供されていなかった。このため、通信相手が認証され、あるいは通信経路の安全性が保証されても、相手相手にセキュリティホールがある場合があった。そして、その通信相手から第三者に情報が漏洩するおそれがあった。また、その通信相手を通じて第三者がなりすましをするおそれがあった。そのようなおそれのため、特定の相手システムとの情報交換が自由に行えない場合があった。
【０００５】
【発明が解決しようとする課題】
本発明はこのような従来の技術の問題点に鑑みてなされたものである。すなわち、本発明の課題は、通信相手の安全性を確認した上で通信する技術を提供することにある。
【０００６】
【課題を解決するための手段】
本発明は前記課題を解決するために、以下の手段を採用した。すなわち、本発明は、ネットワークを利用し電子的に情報を送信または受信する通信装置（Ａ）であり、
ネットワークにアクセスする通信部（７）と、通信を制御する制御部（２）とを備え、
上記制御部（２）は、情報の送受信の相手である相手装置（Ｂ）のシステム情報を当該相手装置（Ｂ）に問い合わせ、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断するものである。
【０００７】
好ましくは、上記システム情報には、相手装置（Ｂ）の安全性に関連する情報が含まれており、
上記制御部（２）は、相手装置（Ｂ）の安全性が所定の程度に確保されているか否かを判断してもよい。
【０００８】
好ましくは、上記制御部（２）は、相手装置（Ｂ）の安全性が所定の程度に確保されていないと判断したときに、その事実または理由を相手装置（Ｂ）に通知してもよい。
【０００９】
好ましくは、この通信装置（Ａ）は、送受信される情報の種類と問い合わせるシステム情報の項目との関係を管理する情報項目管理部（５）をさらに備え、
上記制御部（２）は、送受信する情報の種類に応じて、前記情報項目管理部（５）からシステム情報の項目を選択し、相手装置（Ｂ）に問い合わせてもよい。
【００１０】
好ましくは、この制御部（２）は、入手済みのシステム情報を管理する入手情報管理部（５）をさらに備え、
上記制御部（２）は、前記入手情報管理部（５）を参照し、その入手済みのシステム情報が相手装置（Ｂ）において更新されているか否かを問い合わせ、更新されたシステム情報と未入手のシステム情報とを入手するようにしてもよい。
【００１１】
好ましくは、上記入手情報管理部（５）は、システム情報の項目ごとにその情報を入手し

た日時を管理し、
上記制御部（２）は、入手済みのシステム情報の項目にその入手日時を付加して相手装置（Ｂ）に問い合わせてもよい。
【００１２】
好ましくは、上記制御部（２）は、相手装置（Ｂ）から入手したシステム情報に基づき相手装置（Ｂ）を検証してもよい。
【００１３】
好ましくは、上記制御部（２）は、入手したシステム情報を検証するテストパケットを通信部から相手装置（Ｂ）に対して送信し、そのテストパケットへのレスポンスが妥当か否かを判定することにより相手装置（Ｂ）を検証してもよい。
【００１４】
また、本発明は、送信元装置（Ａ）から相手装置（Ｂ）に電子的な情報の送信または受信を行うときに、送信元装置（Ａ）の処理を代行する通信装置（２２）であり、
ネットワークにアクセスする通信部（７）と、通信を制御する制御部（２）とを備え、
上記通信部（７）は、送信元装置（Ａ）からの指令を受信し、
制御部（２）は、その指令にしたがい、相手装置（Ｂ１、Ｂ２）に係るシステム情報を当該相手装置（Ｂ１、Ｂ２）に問い合わせ、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断するものでもよい。
【００１５】
好ましくは、この制御部（２）は、上記相手装置（Ｂ１、Ｂ２）に代えて、相手装置（Ｂ１、Ｂ２）の処理を代行する代理装置（２４）に相手装置（Ｂ１、Ｂ２）に係るシステム情報を問い合わせるものでもよい。
【００１６】
また、本発明は、ネットワークを利用し電子的に情報を送信または受信する通信装置（Ｂ）であり、
ネットワークにアクセスする通信部（７）と、通信を制御する制御部（２）と、情報管理部（５）とを備え、
上記通信部（７）は、相手装置（Ａ）から当該通信装置（Ｂ）に係るシステム情報の問い合わせを受信し、
情報管理部（５）は、問い合わせの対象となるシステム情報を管理し、
制御部（２）は、問い合わせに応じて前記情報管理部（５）のシステム情報を検索し、通信部（７）から返答するものでもよい。
【００１７】
好ましくは、上記制御部（２）は、返答済みのシステム情報のうちの更新されたシステム情報および未返答のシステム情報を返答するものでもよい。
【００１８】
好ましくは、上記通信装置（Ｂ）は、システム情報を更新した日時を管理する更新履歴管理部（５）をさらに備え、
上記通信部（７）は、今回の問い合わせとその問い合わせに対する前回の返答日時とを受信し、
上記制御部（２）は、前回の返答日時と更新した日時とを比較し、前回の返答日時以降に更新されたシステム情報を返答してもよい。
【００１９】
好ましくは、上記通信装置（Ｂ）は、送信元装置（Ａ）、その送信元装置（Ａ）が問い合わせたシステム情報の項目およびその問い合わせに対する返答日時を管理する返答履歴管理部（５）と、
システム情報を更新した日時を管理する更新履歴管理部（５）とをさらに備え、
上記制御部（２）は、送信元装置（Ａ）から問い合わせがあったときに、その問い合わせに対する返答日時とシステム情報を更新した日時と比較し、前回の返答日時の後に、更新されたシステム情報を返答してもよい。

【００２０】
好ましくは、上記制御部（２）は、問い合わせに対してシステム情報の返答可否を判断し、返答不可と判断されたシステム情報を返答しないようにしてもよい。
【００２１】
好ましくは、上記通信装置（Ｂ）は、システム管理者の判断を促す入出力部（６）をさらに備え、
上記制御部（２）は、問い合わせに対してシステム情報の返答可否を判断し、返答可否を決定できないシステム情報について、上記入出力部（６）を通じて、システム管理者に返答可否の判断を促してもよい。
【００２２】
好ましくは、上記通信装置（Ｂ）は、システム管理者の判断を促す入出力部（６）をさらに備え、
上記制御部（２）は、問い合わせに対しシステム情報の返答可否を判断し、返答不可と判定されたシステム情報を返答をせず、返答可否を決定できないシステム情報についてシステム管理者に返答可否の判断を促してもよい。
【００２３】
好ましくは、上記通信装置（Ｂ）は、送信元装置（Ａ）の属性に係る情報を管理する送信元管理部（５）をさらに備え、
上記制御部（２）は、上記送信元管理部（５）を検索し、その送信元装置（Ａ）に応じてシステム情報の返答可否を判断し、返答不可と判断されたシステム情報を返答しないようにしてもよい。
【００２４】
好ましくは、上記通信装置（Ｂ）は、システム管理者の判断を促す入出力部（６）をさらに備え、
上記制御部（２）は、上記送信元管理部（５）を検索し、その送信元装置（Ａ）に応じてシステム情報の返答可否を判断し、その送信元装置（Ａ）に対して返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促してもよい。
【００２５】
好ましくは、上記通信装置（Ｂ）は、送信元装置（Ａ）の属性に係る情報を管理する送信元管理部（５）と、
システム管理者の判断を促す入出力部（６）とをさらに備え、
上記制御部（２）は、前記送信元管理部（５）を検索し、その送信元装置（Ａ）に応じてシステム情報の返答可否を判断し、返答不可と判断されたシステム情報は返答をせず、返答可否を決定できないシステム情報についてはシステム管理者に返答可否の判断を促すようにしてもよい。
【００２６】
また、本発明は、送信元装置（Ａ）から相手装置（Ｂ）へのシステム情報の問い合わせに対する返答を代行する通信装置（２４）であり、
ネットワークにアクセスする通信部（７）と、通信を制御する制御部（２）と、情報管理部（５Ｃ）とを備え、
上記通信部（７）は、送信元装置（Ａ）からの相手装置（Ｂ）に係るシステム情報の問い合わせを受信し、
上記情報管理部（５Ｃ）は、相手装置（Ｂ）に係る問い合わせの対象となるシステム情報を管理し、
上記制御部（２）は、問い合わせに応じて情報管理部（５Ｃ）のシステム情報を検索し、相手装置（Ｂ）に代わって通信部から返答するものでもよい。
【００２７】
好ましくは、上記通信部（７）は、送信元装置（Ａ）に代えて、送信元装置（Ａ）の処理を代行する代理装置（２２）からシステム情報の問い合わせを受信し、その代理装置に返答するようにしてもよい。

【００２８】
また、本発明は、ネットワークを利用し電子的に情報を送信または受信する通信方法であり、
情報の送受信の相手である相手装置（Ｂ）に係るシステム情報を当該相手装置（Ｂ）に問い合わせるステップ（Ｓ１）と、
そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する判断ステップ（Ｓ３、Ｓ５）とを有するものでもよい。
【００２９】
また、本発明は、送信元装置（Ａ）から相手装置（Ｂ１、Ｂ２）に電子的な情報の送信または受信を行うときに、送信元装置（Ａ）の処理を代行する通信方法であり、
送信元装置（Ａ）からの指令を受信するステップ（Ｓ１００）と、
その指令にしたがい、相手装置（Ｂ１、Ｂ２）に係るシステム情報を当該相手装置（Ｂ１、Ｂ２）に問い合わせる問い合わせステップ（Ｓ１０１）と、
そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断するステップ（Ｓ１０３、Ｓ１０５）とを有するものでもよい。
【００３０】
また、本発明は、ネットワークを利用し電子的に情報を送信または受信させる通信方法であり、
送信元装置（Ａ）からシステム情報の問い合わせを受信する受信ステップ（Ｓ１）と、
問い合わせに対するシステム情報を検索するステップ（Ｓ２２、Ｓ２３）と、
そのシステム情報を返答する返答ステップ（Ｓ２８）とを有するものでもよい。
【００３１】
また、本発明は、送信元装置（Ａ）から相手装置（Ｂ１、Ｂ２）へのシステム情報の問い合わせに対する返答を代行する通信方法であり、
送信元装置（Ａ）からの相手装置（Ｂ１、Ｂ２）に係るシステム情報の問い合わせを受信する受信ステップ（Ｓ１０１）と、
問い合わせに応じて、相手装置（Ｂ１、Ｂ２）に係るシステム情報を検索するステップ（Ｓ１０２）と、
相手装置（Ｂ１、Ｂ２）に代わって通信部から返答するステップ（Ｓ１０２）とを有するものでもよい。
【００３２】
また、本発明は、コンピュータに以上の機能を実現させるプログラムをコンピュータ読み取り可能な記録媒体に記録したものでもよい。
【００３３】
以上述べたように、本発明によれば、通信相手のセキュリティレベルをチェックできるようになり、情報交換をする際の、通信相手を通じた情報の漏洩やなりすましによる不正アクセスの危険が軽減される。さらにこのようなシステム情報の管理をデータベースを利用して自動化することにより、管理者の負担が軽減される。
【００３４】
【発明の実施の形態】
以下、図面を参照して本発明の実施の形態を説明する。
【００３５】
《第１実施形態》
本発明の第１実施形態を図１から図１１の図面に基いて説明する。
【００３６】
図１は、セキュリティレベルの確認を行う情報システムの構成図であり、図２は、図１に示した問い合わせ項目管理データベースのデータ構造を示す図であり、図３は、問い合わせ側のシステムが一度入手したデータを管理する入手データ管理データベースのデータ構造を示す図であり、図４は、図１に示した返答側のシステムが問い合わせに対する返答の可否を判断するための返答可否データベースのデータ構造を示す図であり、図５は、返答

側のシステムが返答するセキュリティデータを管理するセキュリティデータ管理データベースのデータ構造を示す図であり、図６は問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャートであり、図７は、図６に示したセキュリティデータの問い合わせ処理の詳細を示すフローチャートであり、図８は、図６に示したセキュリティデータの返答処理の詳細を示すフローチャートであり、図９は、図６に示したセキュリティ判定処理の詳細を示すフローチャートであり、図１０は、第１実施形態の変形例における返答履歴管理データベースのデータ構造を示す図であり、図１１は、第１実施形態の変形例における情報を過去に提供した日時と変更した日時を確認する処理示す図である。

【００３７】

＜システム構成＞

図１は、システム間の情報授受に際して、セキュリティレベルの確認を行う情報システムの構成図である。この情報システムは、情報を提供するシステムＡと、情報の提供を受けるシステムＢと、管理者端末１２および１３とから構成される。

【００３８】

システムＡは、例えば、パーソナルコンピュータにより構成される。システムＡは、情報提供に際して、提供先のセキュリティレベルを判定するため、予め情報提供先（これを情報入手側ともいう）にセキュリティデータを問い合わせる。このような問い合わせを行うシステムを問い合わせ側システムと呼ぶ。

【００３９】

一方、情報の提供を受けるシステムＢは、この問い合わせに返答する。本実施形態では、このようなシステムを返答側システムと呼ぶ。このシステムＢも、例えば、パーソナルコンピュータにより構成される。

【００４０】

また、システムＢは、情報受信後に、受信した情報が信用できるか否かを判断するため、システムＡにセキュリティデータを問い合わせる。したがって、システムＢは問い合わせ側システムとしても機能する。

【００４１】

また、このとき、システムＡは、その問い合わせに返答する。したがって、システムＡは、返答側システムとしても機能する。

【００４２】

システムＡおよびシステムＢは、各々管理者端末１２および１３に接続されている。そして、システムＡにおいて判断できない問題は、管理者端末１２に転送される。また、システムＢにおいて判断できない問題は、管理者端末１３に転送される。このような問題は、各管理者の判断に委ねられる。

【００４３】

図１のように、システムＡは、システムＡの各構成要素を制御する中央制御部２と、情報処理のためのアプリケーションプログラムから構成され情報処理を実行する情報処理部３と、情報入手側のセキュリティレベルを判定するセキュリティデータチェック部４と、各種の情報を提供するデータベース５と、管理者端末１２との通信を行う入出力部６と、ネットワークにアクセスし、情報提供先のシステムＢ等と通信するネットワークインターフェース７とを有している。

【００４４】

中央制御部２は、いわゆるＣＰＵであり、各種のプログラムを実行し、システムＡの機能を提供する。

【００４５】

情報処理部３は、不図示のメモリ上にロードされ、中央制御部２で実行される各種のアプリケーションプログラムである。これらのアプリケーションプログラムには、例えば、システムＢとの通信を実行するプログラム等が含まれる。

【００４６】

セキュリティデータチェック部４は、情報処理部３から情報を提供される提供先、例えば

、システムＢにセキュリティデータを問い合わせ、そのセキュリティレベルを判定する。
【００４７】
データベース５は、問い合わせ項目管理データベースおよび入手データ管理データベースを含んでいる。これらのデータベースは、システムＡが問い合わせ側システムとして機能するときに使用される。
【００４８】
問い合わせ項目管理データベースは、セキュリティデータチェック部４が返答側システムに問い合わせるセキュリティデータの項目を管理する。また、入手データ管理データベースは、過去に返答側システムから返答されたセキュリティデータを管理する。
【００４９】
さらに、データベース５は、返答可否データベースおよびセキュリティデータ管理データベースを含んでいる。これらのデータベースは、システムＡが返答側システムとして機能するときに参照される。
【００５０】
返答可否データベースは、問い合わせ側システムから問い合わせのあったセキュリティデータ等を問い合わせ側システムに返答することの可否を判定するために使用される。
【００５１】
また、セキュリティデータ管理データベースは、システムＡ自身のセキュリティデータを管理する。このデータベースでは、問い合わせへの返答対象となる情報が管理される。
【００５２】
入出力部６は、中央制御部２からの指令により管理者端末１２との通信を実行する。ネットワークインターフェース７は、中央制御部２からの指令によりシステムＢ等と通信する。
【００５３】
システムＢの構成は、システムＡの構成と同様である。そこで、システムＢの構成については、説明を省略する。
【００５４】
＜データ構造＞
図２に問い合わせ項目管理データベースのデータ構造を示す。システム間の情報授受において、情報提供元のシステム（問い合わせ側システムに該当）は、情報を提供する前に、このデータベースを参照し、その情報入手側のシステム（返答側システムに相当）に問い合わせる項目を決定する。
【００５５】
また、情報の提供を受けたシステム（問い合わせ側システムに該当）は、情報を入手後、その情報が信用できるか否かを判定するために、このデータベースを参照し、情報提供側のシステム（返答側システムに相当）に問い合わせる項目を決定する。
【００５６】
問い合わせ項目管理データベースは、テーブル形式で構成される。このテーブルの各行は、授受される情報の種類と必要なセキュリティデータ項目のフィールドを有している。
【００５７】
授受される情報の種類には、例えば、”１０００万円未満の取引”、”１０００万円以上の取引”、”関係者外秘情報”、”情報Ａ”等のように、授受される情報の区分が記述される。
【００５８】
一方、必要なセキュリティデータ項目には、例えば、”ＯＳ”、”パスワード暗号化”、”ログ監査”、”項目Ａ”、”開いているポート”、”ウィルス対策”等が列記される。
【００５９】
ここで、”ＯＳ”とは、ＯＳの種類を問い合わせることの指定である。また、”パスワード暗号化”とは、パスワード暗号化機能の有無を問い合わせることの指定である。
【００６０】

”ログ監査”とは、蓄積された通信ログを監査する監査機能の有無や監査の頻度を問い合わせることの指定である。”開いているポート”とは、受信したデータを処理するアプリケーション層プロトコルが設定されているポート番号を問い合わせることの指定である。

【００６１】

図２では、”１０００万円未満の取引”の行には、”ＯＳ”および”パスワード暗号化”が必要なセキュリティデータの項目として指定されている。この場合、問い合わせ側システムは、１０００万円未満の取引に関する情報を提供する場合、その情報提供先にＯＳの種類、およびパスワード暗号化機能の有無を問い合わせる。

【００６２】

図３に入手データ管理データベースのデータ構造を示す。このテーブルは、問い合わせ側システムが返答側システムから入手したセキュリティデータを管理するために使用される。

【００６３】

この入手データ管理データベースは、テーブル形式で構成される。このテーブルの各行は、返答側システム、項目、入手日時、入手セキュリティデータの各フィールドを有している。

【００６４】

返答側システムは、入手データを返答したシステムを一意に特定する情報である。これは、例えば、ネットワーク上のホスト名である。ホスト名の代わりに、ＩＰ（Internet Protocol）アドレスやＭＡＣ（Media Access Control）アドレスを用いてシステムを記述してもよい。

【００６５】

項目は、入手したセキュリティデータの種類である。これは、例えば、”ＯＳ”、”開いているポート”、”ログ監査頻度”、”項目Ａ”、”パスワード暗号化”等である。

【００６６】

入手日時は、その情報を入手した年月日と時刻である。入手セキュリティデータには、入手されたデータを記述する。例えば、項目”ＯＳ”に対して、Windows NT SP5（Windows NTは、米国マイクロソフト社の商標である）が記録される。また、項目”開いているポート”に対して７、２３、８０等が記録される。また、項目”ログ監査頻度”に対して、１回／１日が指定される。

【００６７】

図４に、返答可否データベースのデータ構造を示す。このデータベースは、返答側システムにおいて、問い合わせに対する返答の可否を判断するために使用される。この返答可否データベースは、テーブル形式で構成される。

【００６８】

このテーブルの各行は、問い合わせ側システム、項目、および判断の各フィールドを有している。

【００６９】

問い合わせ側システムは、問い合わせ側のシステムを一意に特定する情報である。また、項目は、問い合わせの対象であるセキュリティデータの種類である。判断には、返答の可否が記述される。

【００７０】

図４では、例えば、システムＡからの項目”ＯＳ”に対する問い合わせに対して、×、すなわち、返答不可であることが指定されている。また、システムＡからの項目”開いているポート”に対する問い合わせに対して○、すなわち、返答可が指定されている。

【００７１】

また、システムＣからの項目”ＯＳ”に対する問い合わせに対して、△、すなわち、判断不可が指定されている。この場合、返答側システム、例えばシステムＢは、管理者端末１３に返答可否の判断を問い合わせて、管理者の指示を受けることになる。

【００７２】

図５にセキュリティデータ管理データベースのデータ構造を示す。このデータベースは、返答側システムが、セキュリティデータを管理するために使用される。返答側システムは、問い合わせ側システムからの問い合わせに対して、このデータベースを参照して返答する。

【００７３】

セキュリティデータ管理データベースは、テーブル形式で構成される。このテーブルの各行は、項目、セキュリティデータおよび更新日時の各フィールドを有している。

【００７４】

これらのうち、項目およびセキュリティデータは、図３に示した入手データ管理データベースの項目および入手セキュリティデータと同様であるので、その説明を省略する。

【００７５】

また、更新日時は、各セキュリティデータの更新日時である。図５では、例えば、この返答側システムのＯＳが２０００年１月１３日１１時０分に更新され、Windows NT SP5になったことが分かる。また、”開いているポート”が２０００年３月３１日１２時２４分に７、２３、８０に設定されたことが分かる。

【００７６】

＜作用と効果＞

図６に、情報提供側であるシステムＡと情報入手側であるシステムＢとの通信手順を示す。図６では、システムＡがシステムＢに情報を提供する前に、システムＢのセキュリティを検証する。そのセキュリティが充分であると確認された場合、システムＡがシステムＢに情報を提供する。

【００７７】

一方、システムＢは、逆にシステムＡのセキュリティを検証することで、入手した情報が信用できるか否かを確認する。

【００７８】

図６では、まず、システムＡがシステムＢにセキュリティデータを問い合わせる（Ｓ１）。すると、システムＢが対応するセキュリティデータを返答する（Ｓ２）。

【００７９】

次に、システムＡは、セキュリティ判定処理を実行する（Ｓ３）。すなわち、システムＡは、返答されたセキュリティデータを基に、システムＢのセキュリティが充分か否かを判定する。システムＢのセキュリティが充分でない場合（Ｓ３でＮＧの場合）、システムＡは、処理を終了する。

【００８０】

一方、セキュリティが充分である場合（Ｓ３でＯＫの場合）、システムＡは、入手したセキュリティデータを検証するためのテストパケットを送信する（Ｓ４）。そして、テストパケットに対するレスポンスにより、セキュリティデータが正しいか否かを判断する（Ｓ５）。

【００８１】

これは、例えば、入手したセキュリティデータの項目が”開いているポート”であり、入手したデータが７、２３、８０の場合、そのポート番号のパケットを送信し、応答が返るか確認する処理である。また、そのポート番号以外のパケットに対して応答がないことを確認してもよい。

【００８２】

また、相手システムのＯＳの種類の入手するアプリケーションとして、例えば、nmapが知られている。nmapは、インターネット上のホームページ、http://www.insecure.org/nmap/index.htmlで解説されている。nmapは、例えば、相手システムに対して、telnetやftpのようなアプリケーション層に接続されるポートにパケットを送信し、そのシステムにログインする前に返送されるバナーを収集する。そのような手順により、nmapは、相手システムのＯＳの種類を入手する。そのようなバナーには、ＯＳの種類やバージョンが含まれるからである。

【００８３】
また、パスワードの暗号化の有無、ログ監査の頻度等に関しては、システムの監査を行う第三者機関に問い合わせる。情報の提供側システムと提供先システムは、自身の監査を行う第三者機関を互いに相手に通知しておけばよい。
【００８４】
以上のようなテストパケット確認の結果、セキュリティデータが正しくなかった場合、システムＡは、処理を終了する。一方、セキュリティデータが正しいことが確認された場合、システムＡは、情報提供を行う（Ｓ６）。これは、例えば、取引情報の送信、関係者外秘情報の送信、特定の情報の送信等である。
【００８５】
その結果、システムＢは、その情報を入手する（Ｓ７）。次に、システムＢは、システムＡにセキュリティデータを問い合わせる（Ｓ８）。入手した情報が信用できるか否かを確認するためである。
【００８６】
これに対して、システムＡは、セキュリティデータを返答する（Ｓ９）。すると、システムＢは、入手したセキュリティデータによりシステムＡのセキュリティを確認するため、セキュリティ判定処理を実行する（ＳＡ）。
【００８７】
その結果、システムＡのセキュリティが不充分な場合（ＳＡの処理結果がＮＧの場合）、システムＢは処理を終了する。一方、システムＡのセキュリティが充分な場合（ＳＡの処理結果がＯＫの場合）、セキュリティデータを検証するためのテストパケットをシステムＡに送信する（ＳＢ）。そして、システムＢは、セキュリティデータが正しいか否かを確認する（ＳＣ）。ＳＢおよびＳＣの処理は、システムＡにおけるＳ４－Ｓ５の処理と同様である。
【００８８】
ＳＣの判定における確認の結果、システムＡのセキュリティデータが正しくなかった場合、システムＢは、処理を終了する。一方、システムＡのセキュリティデータが正しことを確認できた場合、システムＢは提供されたセキュリティデータを信用し、利用する。
【００８９】
図７に、セキュリティデータの問い合わせ処理（図６のＳ１またはＳ８）の詳細を示す。いま、図７では、システムＡからシステムＢに問い合わせる場合（図６のＳ１の処理）を仮定する。
【００９０】
まず、問い合わせ側のシステムＡは、問い合わせ項目管理データベースを参照し、送受信する情報内容に応じて問い合わせるセキュリティデータの項目を決定する（Ｓ１１）。
【００９１】
次に、システムＡは、問い合わせるセキュリティデータの項目が入手データ管理データベースに登録されているか否かを判定する（Ｓ１２）。入手データ管理データベースには、過去に問い合わせられたセキュリティデータの項目がそのセキュリティデータの入手日時とともに記録されている。
【００９２】
そして、システムＡは、入手データ管理データベースに登録されている項目については、その項目に対応するデータが変更されているか否かをシステムＢに問い合わせる（Ｓ１３）。この問い合わせは、その問い合わせ項目に前回データを入手した日時（時間データ）を付して行う。
【００９３】
一方、入手データ管理データベースに登録されていない項目については、システムＡは、そのままシステムＢに問い合わせる（Ｓ１４）。以上は、システムＡからシステムＢに問い合わせる場合（図６のＳ１の処理）を仮定して説明したが、システムＢからシステムＡに問い合わせる場合（図６のＳ８の処理）も同様である。

【００９４】
図８に、セキュリティデータ返答処理（図６のＳ２またはＳ９の処理）の詳細を示す。図８では、システムＢからシステムＡにセキュリティデータを返答する場合（図６のＳ２の処理）を仮定して説明する。
【００９５】
まず、システムＢは、問い合わせ元のシステムをチェックし、問い合わせ元がシステムＡであることを認識する（Ｓ２１）。次に、システムＢは、問い合わせ項目をチェックする（Ｓ２２）。
【００９６】
次に、システムＢは、返答可否データベースを参照し（Ｓ２３）、問い合わせ元と問い合わせ項目との組み合わせが返答可能なものか否かを判定する（Ｓ２４）。そして、その問い合わせ元と問い合わせ項目とが、返答可否データベースにおいて”返答してよい”と規定されている場合、システムＢは、セキュリティデータ管理データベースを参照し、問い合わせの対象となっている項目のセキュリティデータを参照する（Ｓ２６）。
【００９７】
次に、過去においてセキュリティデータが提供された日時がその問い合わせに付加されている場合、システムＢは、過去に提供された日時とそのセキュリティデータがシステムＢで変更された日時とを確認する（Ｓ２７）。
【００９８】
そして、そのセキュリティデータが過去に提供されていないか（初めて提供されるデータか）、または、過去に提供されたデータでその後変更されたものである場合、システムＢはそのセキュリティデータを返答する（Ｓ２８）。
【００９９】
一方、そのセキュリティデータが過去にシステムＡに提供された後、変更されていない場合、システムＢはシステムＡに変更なしという返答を行う（Ｓ２９）。
【０１００】
また、Ｓ２４の判定で、その問い合わせ元と問い合わせ項目とが、返答可否データベースにおいて”返答してはいけない”と規定されている場合、システムＢは、問い合わせ対象のセキュリティデータを返答できないとシステムＡに返答する（Ｓ２Ａ）。
【０１０１】
また、Ｓ２４の判定で、その問い合わせ元と問い合わせ項目とが、返答可否データベースにおいて返答の”可否を判断できない”と規定されている場合、システムＢは、管理者端末１３に返答可否を問い合わせるメッセージを送信し、管理者の指令を求める（Ｓ２５）。
【０１０２】
管理者からの指令が”返答してよい”というものである場合、システムＢは、Ｓ２６以下の処理により、システムＡに返答する。一方、管理者からの指令が”返答してはいけない”というものである場合、システムＢは、システムＡに返答できないと返答する（Ｓ２Ａ）。
【０１０３】
図９に、セキュリティ判定処理（図６のＳＡの処理）の詳細を示す。図９では、システムＡから入手した情報をシステムＢが判定する場合について説明する。
【０１０４】
まず、システムＢは、システムＡからのセキュリティデータの項目に関する返答内容をチェックする（ＳＡ１）。次に、システムＢは、入手データ管理データベースに返答内容と入手日時を登録する（ＳＡ２）。
【０１０５】
次に、システムＢは、返答内容に問題がないか否かを判定する（ＳＡ３）。これは、返答内容からシステムＡのセキュリティレベルを判定する処理である。返答内容に問題がない場合（ＳＡ３の処理結果が”問題ない”の場合）、システムＢは、システムＡのセキュリ

ティレベルが充分である（ＯＫ）と判定する（ＳＡ５）。
【０１０６】
また、返答内容に問題がある場合（ＳＡ３の処理結果が”問題あり”の場合）、システムＢは、セキュリティレベルが不充分である事実および理由を相手（システムＡ）に通知する（ＳＡ６）。これにより、システムＢは、本処理結果をＮＧと判定する。
【０１０７】
また、返答内容に問題があるか否かが分からない場合（ＳＡ３の処理結果が”分からない”の場合）、システムＢは、管理者端末１３にシステムＡのセキュリティレベルの判断を求めるメッセージを送信し、管理者の判断を求める（ＳＡ４）。
【０１０８】
管理者の判断が”問題ない”の場合、システムＢは、システムＡのキュリティレベルが充分である（ＯＫ）と判定する（ＳＡ５）。一方、管理者の判断が”問題あり”の場合、システムＢは、セキュリティレベルが不充分である事実および理由を相手（システムＡ）に通知する（ＳＡ６）。これにより、システムＢは、本処理結果をＮＧと判定する。
【０１０９】
以上述べたように、本実施形態の情報システムによれば、情報の送受信の相手である相手システムのセキュリティデータを当該相手システムに問い合わせる。そして、各システムは、そのセキュリティデータに基づいて、それ以降の送受信を行うか否かを判断する。その結果、相手システムのセキュリティレベルが不充分な状態での通信の継続を回避できる。
【０１１０】
また、本情報システムによれば、返答側のシステムのセキュリティレベルが不充分であると判断された場合、問い合わせ側のシステムは、その事実および理由を返答側のシステムに通知する。これにより、返答側システムシステムは、自身のセキュリティ上の欠陥を認識できる。
【０１１１】
また、本情報システムによれば、授受される情報に応じて必要なセキュリティ項目が問い合わせ項目管理データベースに定義される。これにより、各システムは、授受される情報に応じて適切な問い合わせ項目を決定できる。
【０１１２】
また、本情報システムによれば、上記返答側システムは、問い合わせ側システムからの問い合わせに対して返答するセキュリティデータを管理するセキュリティデータ管理データベースを有している。これにより、返答側システムは、返答すべきセキュリティデータを一元的に管理できる。
【０１１３】
また、本情報システムによれば、返答側システムは、問い合わせに対する返答の可否を判断する返答可否データベースを有している。これにより、返答側のシステムは、問い合わせに返答すべきか否か、またはその判断できないかを、問い合わせ側システムと問い合わせ内容の関係から導くことができる。
【０１１４】
また、本実施形態では、問い合わせ側システムは、返答側システムから入手したセキュリティデータを管理する入手データ管理データベースを有している。これにより、問い合わせ側システムは、過去に問い合わせたセキュリティデータについては、入手日時を付加して返答側システムに問い合わせることができる。
【０１１５】
また、返答側サブシステムは、上記セキュリティデータ管理データベースに各セキュリティデータの更新日時を有している。その結果、返答側システムは、問い合わせのあったセキュリティデータうち、更新があったセキュリティデータ、また、初めて問い合わせのあったセキュリティデータに限定して返答することができる。
【０１１６】

また、本情報システムによれば、返答側システム、例えばシステムＢは、管理者端末１３に接続され、問い合わせに対する返答の可否を判断できない場合、返答可否の判断を求めるメッセージを管理者端末１３に送信することができる。したがって、返答可否の判断が困難な問題については、その判断を管理者に委ねることができ、判断の難易に応じて柔軟な対応ができる。

【０１１７】

また、本実施形態では、セキュリティデータを問い合わせたシステム、例えばシステムＢは、そのセキュリティデータから相手システムのセキュリティが充分か否かを判断できない場合、その判断を求めるメッセージを管理者端末１３に送信することができる。したがって、セキュリティレベルの良否の判断が困難な場合においては、その判断を管理者に委ねることができ、判断の難易に応じて柔軟な対応ができる。

【０１１８】

また、返答可否の判断が困難な問題以外については、上記データベースの検索結果に基づいてシステムが処理する。このため、管理者の負担を軽減することができる。

【０１１９】

＜変形例＞

上記実施形態では、問い合わせ側システム、例えば、システムＡがセキュリティデータを問い合わせる際、入手データ管理データベースを参照し、過去に問い合わせた日時をその問い合わせに付加した。

【０１２０】

しかし、本発明の実施は、このような構成や作用に限定されない。例えば、返答側システム、例えば、システムＢにおいて過去に返答した内容を記録する返答履歴管理データベースを有し、セキュリティデータ管理データベースの変更履歴と比較して、変更のあったセキュリティデータを返答するようにしてもよい。

【０１２１】

図１０に返答履歴管理データベースのデータ構造を示す。このデータベースの構造は、図３に示した入手データ管理データベースと同様である。この返答履歴管理データベースは、テーブル形式で構成される。このテーブルの各行は、問い合わせ側システム、項目、返答日時、返答セキュリティデータの各フィールドを有している。

【０１２２】

問い合わせ側システムは、セキュリティデータを問い合わせたシステムを一意に特定する情報である。項目は、返答されたセキュリティデータの種類である。返答日時は、その情報を返答した年月日と時刻である。返答セキュリティデータには、返答されたデータを記述する。

【０１２３】

図１１に、この返答履歴管理データベースを用いて、過去に返答をした日時（過去に提供した日時）と変更した日時を確認する処理（図８のＳ２７に代わる処理）を示す。

【０１２４】

問い合わせを受信した返答側システム、例えばシステムＢは、返答履歴管理データベースを参照し（Ｓ２７１）、その問い合わせにすでに返答済みであるか否かを判定する（Ｓ２７２）。その問い合わせに対してセキュリティデータが、その問い合わせ側システムに返答済みでない場合、システムＢは、Ｓ２８の処理（図８）に制御を進める。これにより、問い合わせのあったセキュリティデータが返答される。

【０１２５】

一方、その問い合わせ側システムに対してセキュリティデータが返答済みである場合、システムＢは、セキュリティデータ管理データベース（図５）の更新日時を参照する（Ｓ２７３）。そして、その更新日時を返答履歴データベースの返答日時と比較する（Ｓ２７４）。

【０１２６】

更新日時が返答日時より後である場合、システムＢは、Ｓ２８の処理（図８）に制御を進

める。これにより、問い合わせのあったセキュリティデータが返答される。
【０１２７】
また、更新日時が返答日時より後でない場合、システムＢは、Ｓ２９の処理（図８）に制御を進める。これにより、変更なしという返答が問い合わせ側システムに送信される。
【０１２８】
《第２実施形態》
図１２から図１７を参照して本発明の第２実施形態を説明する。図１２は、第２実施形態に係る情報システムのシステム構成図であり、図１３は、図１２に示した返答側代理指定データベース２３のデータ構成を示す図であり、図１４および図１５は、第２実施形態における問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャートであり、図１６および図１７は、第２実施形態の変形例に係る情報システムのシステム構成図である。
【０１２９】
上記第１実施形態では、情報提供に際して、提供先のシステムＢのセキュリティレベルを判定し、セキュリティに問題がないシステムＢに対して情報を提供するシステムＡについて説明した。
【０１３０】
また、その場合に情報の提供を受けたシステムＢがその情報が信用できるか否かをシステムＡのセキュリティレベルを判定することによって確認する処理についても説明した。
【０１３１】
上記のような相手システムのセキュリティを判定するため、システムＡは、システムＢに対して必要なセキュリティデータを問い合わせた。また、システムＢも、入手した情報が信用できるか否かを確認するために、システムＡのセキュリティデータを問い合わせた。
【０１３２】
本実施形態では、このようなセキュリティデータの問い合わせまたは返答を代理システムを通じて授受する例について説明する。他の構成および作用は第１実施形態と同様である。そこで、同一の構成については、同一の符号を付してその説明を省略する。また、必要に応じて図１から図１１の図面を参照する。
【０１３３】
＜システム構成＞
図１２に本実施形態における情報システムのシステム構成図を示す。この情報システムは、問い合わせ側のシステムＡと、問い合わせ側代理システム２２と、返答側代理システム２４と、返答側のシステムＢ１、Ｂ２等から構成される。
【０１３４】
システムＡは、システムＢ１、Ｂ２等に情報を提供する際、提供する情報の種類を問い合わせ側代理システム２２に通知する。ここで、システムＡを代理する問い合わせ側代理システム２２は、問い合わせ側代理指定ファイル２１に定義されている。
【０１３５】
すると、問い合わせ側代理システム２２は、問い合わせ項目管理データベース５Ａを参照し、第１実施形態の場合におけるシステムＡと同様、情報提供先のシステム（システムＢ１、Ｂ２等）に問い合わせるセキュリティデータの項目を決定する。
【０１３６】
次に、問い合わせ側代理システム２２は、問い合わせるセキュリティデータの項目が入手データ管理データベース５Ｂに格納されているか否かを検索する。そのセキュリティデータの項目が入手データ管理データベース５Ｂに格納されている場合、そのセキュリティデータの入手日時を検索する。そして、問い合わせ側代理システム２２は、その日時を付して問い合わせを行う。
【０１３７】
また、このとき、問い合わせ側代理システム２２は、直接システムＢ１、Ｂ２等に問い合わせることをせず、返答側代理システム２４に問い合わせる。Ｂ１、Ｂ２等の返答側代理

システム２４は、返答側代理指定データベース２３に定義されている。
【０１３８】
すると、返答側代理システム２４は、問い合わせの対象であるシステムＢ１、Ｂ２等に代わって、そのセキュリティデータを問い合わせ側代理システム２２に返答する。このとき、返答側代理システム２４の処理は、第１実施形態におけるシステムＢと同様である。
【０１３９】
すなわち、返答側代理システム２４は、問い合わせ対象のシステムごとに構成されたセキュリティデータ管理データベース５Ｃおよび問い合わせ可否データベース５Ｄを参照し、問い合わせ側のシステムＡに対して返答可とされているセキュリティデータを返答する。
【０１４０】
返答されたセキュリティデータを受信した問い合わせ側代理システム２２は、返答されてセキュリティデータを入手データ管理データベース５Ｂに格納する。さらに、問い合わせ側代理システム２２は、そのセキュリティが充分か否かを判定し、システムＡに返答する。
【０１４１】
＜データ構成＞
図１３に返答側代理指定データベース２３の構成を示す。このデータベースは、テーブル形式で構成される。この表の各行は、返答側システムおよび返答側代理システムの各フィールドを有している。
【０１４２】
この返答側システムのフィールドには、返答側システムをユニークに識別する情報が指定される。また、返答側代理システムのフィールドには、返答側代理システムをユニークに識別する情報が指定される。
【０１４３】
図１３では、例えば、返答側システムＢ１、およびＢ２の返答側代理システムとして、各々Ｄ１が指定されている。また、返答側システムＢ３の返答側代理システムとして、各々Ｄ２が指定されている。このように、返答側代理システムは、複数の返答側システムの代理となってよい。
【０１４４】
そのため、図１２に示した、セキュリティデータ管理データベース５Ｃおよび応答可否データベース５Ｄは、代理される返答側のシステムＢ１、Ｂ２ごとにデータを保持する。
【０１４５】
図１２に示した問い合わせ側代理指定ファイル２１には、自身（例えば、システムＡの）問い合わせ側代理システムを識別する情報が少なくとも１つ定義される。これは、例えば、問い合わせ側代理システム２２のホスト名、ＩＰアドレス、ＭＡＣアドレス等である。
【０１４６】
＜作用と効果＞
図１４および図１５に、本実施形態における問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャートを示す。なお、図１４および図１５において、問い合わせ側代理システムＶ、Ｘとは、図１２における問い合わせ側代理システム２２と同様の機能を提供するシステムである。また、図１４および図１５において、返答側代理システムＷ、Ｙとは、図１２における返答側代理システム２４と同様の作用をするシステムである。
【０１４７】
図１４のフローチャートは、情報を提供するシステムＡが問い合わせ側代理システムＶおよび返答側代理システムＷにより、情報の提供先であるシステムＢに関するセキュリティレベルを判定する処理を示している。
【０１４８】
この処理では、システムＡは、情報提供先のシステムＢと提供する情報の種類とを添付し、問い合わせ側代理システムＶにセキュリティデータの問い合わせを依頼する（Ｓ１００

）。
【０１４９】
すると、問い合わせ側代理システムＶは、セキュリティデータの問い合わせ処理を実行する（Ｓ１０１）。この処理は、第１実施形態に示したＳ１の処理とほぼ同様である。ただし、問い合わせ側代理システムＶは、応答側代理指定データベース２３に定義された返答側代理システムＷに問い合わせを発信する。
【０１５０】
すると、返答側代理システムＷは、問い合わせの対象であるシステムＢにおけるセキュリティデータを返答する（Ｓ１０２）。この処理は、図６に示したＳ２の処理と同様である。
【０１５１】
すると、問い合わせ側代理システムＶは、セキュリティ判定処理（Ｓ１０３）およびセキュリティデータを検証するためのテストパケットの送信を実行する（Ｓ１０４）。
【０１５２】
次に、問い合わせ側代理システムＶは、テストパケットに対する応答からセキュリティデータが正しいか否かを判定する（Ｓ１０５）。セキュリティデータが正しい場合、問い合わせ側代理システムＶは、その旨をシステムＡに回答する。その結果、システムＡは、システムＢに情報提供をする（Ｓ１０６）。
【０１５３】
図１５は、入手した情報が信用できるか否かを、問い合わせ側代理システムＸおよび返答側代理システムＹによってシステムＢが判定する処理を示すフローチャートである。
【０１５４】
システムＢは、入手した情報の種類と入手先を添付してセキュリティデータの問い合わせを問い合わせ側代理システムＸに依頼する（Ｓ１０Ｅ）。すると、問い合わせ側代理システムＸは、セキュリティデータの問い合わせ処理を実行する（Ｓ１０８）。すると、返答側代理システムＹは、問い合わせ対象のセキュリティデータを返答する（Ｓ１０９）。
【０１５５】
これに対して、問い合わせ側代理システムＸは、セキュリティ判定処理（Ｓ１０Ａ）を実行し、さらに、セキュリティデータを検証するためのテストパケットを送信する（Ｓ１０Ｂ）。そのレスポンスに基づき、問い合わせ側代理システムＸは、セキュリティデータが正しいか否かを判断する（Ｓ１０Ｃ）。
【０１５６】
そして、セキュリティデータが正しい場合、システムＢは、入手した情報を信用できるものとし、その後の処理を続ける（Ｓ１０Ｄ）。
【０１５７】
以上述べたように、本実施形態では、問い合わせ側のシステムＡに代えて、問い合わせ側代理システムＶがセキュリティデータの問い合わせの代理を行う。また、返答側のシステムＢ等に代えて、返答側代理システムＷがセキュリティデータを返答する。また、システムＢは、問い合わせ側代理システムＸおよび返答側代理システムＹを通じて、入手した情報が信用できるか否かを判断する。
【０１５８】
そのため、セキュリティデータの授受が問い合わせ側代理システムＶ（Ｘ）と返答側代理システムＷ（Ｙ）との間に集約される。その結果、セキュリティデータを授受する際のトラフィックが低減される。また、返答側のシステムＢ（またはＡ）等は、個々の問い合わせに返答する手間を省略することができ、本来のアプリケーションの実行効率を向上できる。
【０１５９】
＜変形例＞
上記実施形態では、図１６に示したように、問い合わせ項目管理データベース５Ａは、問い合わせ側代理システム２２から参照された。しかし、これに代えて、例えば、問い合わ

せを行うシステムＡが直接問い合わせ項目管理データベース５Ａを参照し、問い合わせを行うセキュリティデータの項目を決定してもよい。そして、システムＡが問い合わせ側代理システム２２に対してその項目の問い合わせを行うように依頼すればよい。

【０１６０】

また、上記実施形態では、問い合わせ側代理システム２２は、セキュリティデータの問い合わせを代理した。しかし、これに加えて、問い合わせ側代理システム２２は、システムＡからシステムＢ１、Ｂ２等への情報提供をも代行するようにしてもよい。

【０１６１】

上記実施形態では、問い合わせ側のシステムＡの代わりに問い合わせ側代理システム２２を設け、返答側のシステムＢ１、Ｂ２等の代わりに返答側代理システム２４を設けた。

【０１６２】

しかし、本発明の実施は、このような構成には限定されない。例えば、返答側代理システム２４を設けず、問い合わせ側代理システム２２だけを設けてもよい。図１６は、そのような情報システムのシステム構成図である。このシステムでは、上記実施形態と同様、問い合わせ側のシステムＡから問い合わせ側代理システム２２に問い合わせが依頼される。しかし、問い合わせ側代理システム２２は、直接返答側システムＢ１、Ｂ２等に問い合わせを送信する。

【０１６３】

また、例えば、問い合わせ側代理システム２２等を設けず、返答側代理システム２４だけを設けてもよい。図１７にそのような構成の例を示す。この構成では、問い合わせ側のシステムＡは、返答側代理指定データベース２３を参照し、返答側代理システム２４に問い合わせを行う。

【０１６４】

《コンピュータ読み取り可能な記録媒体》

上記実施の形態におけるシステムＡ、Ｂ、問い合わせ側代理システムＶ、Ｘまたは返答側代理システムＷ、Ｙの機能をコンピュータに実現させるプログラムをコンピュータ読み取り可能な記録媒体に記録することができる。そして、コンピュータに、この記録媒体のプログラムを読み込ませて実行させることにより、上記実施の形態に示したシステムＡ、Ｂ、問い合わせ側代理システムＶ、Ｘまたは返答側代理システムＷ、Ｙとして機能させることができる。

【０１６５】

ここで、コンピュータ読み取り可能な記録媒体とは、データやプログラム等の情報を電気的、磁気的、光学的、機械的、または化学的作用によって蓄積し、コンピュータから読み取ることができる記録媒体をいう。このような記録媒体のうちコンピュータから取り外し可能なものとしては、例えばフロッピーディスク、光磁気ディスク、CD-ROM、CD-R/W、DVD、DAT、８mmテープ、メモリカード等がある。

【０１６６】

また、コンピュータに固定された記録媒体としてハードディスクやＲＯＭ（リードオンリーメモリ）等がある。

【０１６７】

《搬送波に具現化されたデータ通信信号》

また、上記プログラムをコンピュータのハードディスクやメモリに格納し、通信媒体を通じて他のコンピュータに配布することができる。この場合、プログラムは、搬送波によって具現化されたデータ通信信号として、通信媒体を伝送される。そして、その配布を受けたコンピュータを上記実施の形態に示したシステムＡ、Ｂ、問い合わせ側代理システムＶ、Ｘまたは返答側代理システムＷ、Ｙとして機能させることができる。

【０１６８】

ここで通信媒体としては、有線通信媒体、例えば、同軸ケーブルおよびツイストペアケーブルを含む金属ケーブル類、光通信ケーブル等、または、無線通信媒体例えば、衛星通信、地上波無線通信等のいずれでもよい。

【０１６９】
また、搬送波は、データ通信信号を変調するための電磁波または光である。ただし、搬送波は、直流信号でもよい。この場合、データ通信信号は、搬送波がないベースバンド波形になる。したがって、搬送波に具現化されたデータ通信信号は、変調されたブロードバンド信号と変調されていないベースバンド信号（電圧０の直流信号を搬送波とした場合に相当）のいずれでもよい。
【０１７０】
《その他》
更に、本実施の形態は以下の発明を開示する。
【０１７１】
（付記１）　ネットワークを利用し電子的に情報を送信または受信する通信装置であり、ネットワークにアクセスする通信部と、通信を制御する制御部とを備え、
前記制御部は、情報の送受信の相手である相手装置に係るシステム情報を当該相手装置に問い合わせ、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する通信装置。（１）
（付記２）　前記システム情報には、相手装置の安全性に関連する情報が含まれており、前記制御部は、相手装置の安全性が所定の程度に確保されているか否かに基づき、前記送受信を行うか否かを判断する付記１記載の通信装置。（２）
（付記３）　前記制御部は、相手装置の安全性が所定の程度に確保されていないと判断したときに、その事実または理由を相手装置に通知する付記２記載の通信装置。
【０１７２】
（付記４）　送受信される情報の種類と問い合わせるシステム情報の項目との関係を管理する情報項目管理部をさらに備え、
前記制御部は、送受信する情報の種類に応じて、前記情報項目管理部からシステム情報の項目を選択し、相手装置に問い合わせる付記１または２記載の通信装置。
【０１７３】
（付記５）　入手済みのシステム情報を管理する入手情報管理部をさらに備え、
前記制御部は、前記入手情報管理部を参照し、その入手済みのシステム情報が相手装置において更新されているか否かを問い合わせ、更新されたシステム情報と未入手のシステム情報とを入手する付記１または２記載の通信装置。
【０１７４】
（付記６）　前記入手情報管理部は、システム情報の項目ごとにそのシステム情報を入手した日時を管理し、
前記制御部は、入手済みのシステム情報の項目にその入手日時を付加して相手装置に問い合わせる付記５記載の通信装置。
【０１７５】
（付記７）　前記制御部は、相手装置から入手したシステム情報に基づき相手装置を検証する付記１記載の通信装置。（３）
（付記８）　前記制御部は、前記入手したシステム情報を検証するテストパケットを前記通信部から相手装置に対して送信し、そのテストパケットへのレスポンスが妥当か否かを判定することにより相手装置を検証する付記７記載の通信装置。（４）
（付記９）　送信元装置から相手装置に電子的な情報の送信または受信を行うときに、送信元装置の処理を代行する通信装置であり、
ネットワークにアクセスする通信部と、通信を制御する制御部とを備え、
前記通信部は、送信元装置からの指令を受信し、
前記制御部は、その指令にしたがい、前記相手装置に係るシステム情報を当該相手装置に問い合わせ、そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する通信装置。（５）
（付記１０）　前記制御部は、前記相手装置に代えて、相手装置の処理を代行する代理装置に前記相手装置に係るシステム情報を問い合わせる付記９記載の通信装置。

【０１７６】
（付記１１）　ネットワークを利用し電子的に情報を送信または受信する通信装置であり、
ネットワークにアクセスする通信部と、通信を制御する制御部と、情報管理部とを備え、
前記通信部は、送信元装置から当該通信装置に係るシステム情報の問い合わせを受信し、
前記情報管理部は、問い合わせの対象となるシステム情報を管理し、
前記制御部は、問い合わせに応じて前記情報管理部のシステム情報を検索し、前記通信部から返答する通信装置。（６）
（付記１２）　前記制御部は、返答済みのシステム情報のうちの更新されたシステム情報および未返答のシステム情報を返答する付記１１記載の通信装置。
【０１７７】
（付記１３）　システム情報を更新した日時を管理する更新履歴管理部をさらに備え、
前記通信部は、今回の問い合わせとその問い合わせに対する前回の返答日時とを受信し、
前記制御部は、前回の返答日時と更新した日時とを比較し、前回の返答日時以降に更新されたシステム情報を返答する付記１１記載の通信装置。
【０１７８】
（付記１４）　送信元装置、その送信元装置が問い合わせたシステム情報の項目およびその問い合わせに対する返答日時を管理する返答履歴管理部と、
システム情報を更新した日時を管理する更新履歴管理部とをさらに備え、
前記制御部は、送信元装置から問い合わせがあったときに、その問い合わせに対する前回の返答日時とシステム情報を更新した日時と比較し、前回の返答日時の後に、更新されたシステム情報を返答する付記１１記載の通信装置。
【０１７９】
（付記１５）　前記制御部は、問い合わせに対してシステム情報の返答可否を判断し、返答不可と判断されたシステム情報を返答しない付記１１記載の通信装置。
【０１８０】
（付記１６）　システム管理者の判断を促す入出力部をさらに備え、
前記制御部は、問い合わせに対してシステム情報の返答可否を判断し、返答可否を決定できないシステム情報について、前記入出力部を通じて、システム管理者に返答可否の判断を促す付記１１記載の通信装置。
【０１８１】
（付記１７）　システム管理者の判断を促す入出力部をさらに備え、
前記制御部は、問い合わせに対しシステム情報の返答可否を判断し、返答不可と判定されたシステム情報を返答をせず、返答可否を決定できないシステム情報についてシステム管理者に返答可否の判断を促す付記１１記載の通信装置。
【０１８２】
（付記１８）　送信元装置の属性に係る情報を管理する送信元管理部をさらに備え、
前記制御部は、前記送信元管理部を検索し、その送信元装置に応じてシステム情報の返答可否を判断し、返答不可と判断されたシステム情報を返答しない付記１１記載の通信装置。（７）
（付記１９）　システム管理者の判断を促す入出力部をさらに備え、
前記制御部は、前記送信元管理部を検索し、その送信元装置に応じてシステム情報の返答可否を判断し、その送信元装置に対して返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促す付記１８記載の通信装置。
【０１８３】
（付記２０）　送信元装置の属性に係る情報を管理する送信元管理部と、
システム管理者の判断を促す入出力部とをさらに備え、
前記制御部は、前記送信元管理部を検索し、その送信元装置に応じてシステム情報の返答可否を判断し、返答不可と判断されたシステム情報は返答をせず、返答可否を決定できないシステム情報についてはシステム管理者に返答可否の判断を促す付記１１記載の通信装

置。
【０１８４】
（付記２１）　送信元装置から相手装置へのシステム情報の問い合わせに対する返答を代行する通信装置であり、
ネットワークにアクセスする通信部と、通信を制御する制御部と、情報管理部とを備え、
前記通信部は、送信元装置から相手装置に係るシステム情報の問い合わせを受信し、
前記情報管理部は、前記相手装置に係るシステム情報を管理し、
前記制御部は、問い合わせに応じて前記情報管理部のシステム情報を検索し、前記相手装置に代わって前記通信部から返答する通信装置。（８）
（付記２２）　前記通信部は、前記送信元装置に代えて、送信元装置の処理を代行する代理装置からシステム情報の問い合わせを受信し、その代理装置に返答する付記２１記載の通信装置。
【０１８５】
（付記２３）　ネットワークを利用し電子的に情報を送信または受信する通信方法であり、
情報の送受信の相手である相手装置に係るシステム情報を当該相手装置に問い合わせるステップと、
そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する判断ステップとを有する通信方法。（９）
（付記２４）　前記システム情報には、相手装置の安全性に関連する情報が含まれており、
前記判断ステップでは、相手装置の安全性が所定の程度に確保されているか否かに基づき、前記送受信を行うか否かが判断される付記２３記載の通信方法。
【０１８６】
（付記２５）　前記判断ステップにおいて、相手装置の安全性が所定の程度に確保されていないと判断されたときに、その事実または理由を相手装置に通知するステップをさらに有する付記２４記載の通信方法。
【０１８７】
（付記２６）　送受信する情報の種類に応じて、問い合わせるシステム情報の項目を選択するステップをさらに有する付記２３または２４記載の通信方法。
【０１８８】
（付記２７）　入手済みのシステム情報を管理する入手情報管理部を参照する参照ステップと、
その入手済みのシステム情報が相手装置において更新されているか否かを問い合わせる問い合わせステップと、
更新されたシステム情報および未入手のシステム情報を入手するステップとをさらに有する付記２３または２４記載の通信方法。
【０１８９】
（付記２８）　前記入手情報管理部は、システム情報の項目ごとにその情報を入手した日時を管理しており、
前記参照ステップでは、システム情報の項目ごとの入手日時が参照され、
前記問い合わせステップでは、その入手日時が付加されてシステム情報の項目が問い合わせられる付記２７記載の通信方法。
【０１９０】
（付記２９）　相手装置から返答されたシステム情報に基づき相手装置を検証する検証ステップをさらに有する付記２３記載の通信方法。
【０１９１】
（付記３０）　前記入手したシステム情報を検証するテストパケットを前記相手装置に対して送信するステップをさらに有し、
前記検証ステップでは、そのテストパケットへのレスポンスに基づき相手装置が検証され

る付記２９記載の通信方法。
【０１９２】
（付記３１）　送信元装置から相手装置に電子的な情報の送信または受信を行うときに、送信元装置の処理を代行する通信方法であり、
前記送信元装置からの指令を受信するステップと、
その指令にしたがい、前記相手装置に係るシステム情報を当該相手装置に問い合わせる問い合わせステップと、
そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断するステップとを有する通信方法。
【０１９３】
（付記３２）　前記問い合わせステップでは、前記相手装置に代えて、相手装置の処理を代行する代理装置に対して相手装置に係るシステム情報が問い合わせられる付記３１記載の通信方法。
【０１９４】
（付記３３）　ネットワークを利用し電子的に情報を送信または受信する通信方法であり、
送信元装置からシステム情報の問い合わせを受信する受信ステップと、
問い合わせに対するシステム情報を検索するステップと、
そのシステム情報を返答する返答ステップとを有する通信方法。
【０１９５】
（付記３４）　前記返答ステップでは、返答済みのシステム情報のうちの更新されたシステム情報および未返答のシステム情報が返答される付記３３記載の通信方法。
【０１９６】
（付記３５）　システム情報を更新した日時を管理する更新履歴管理部を参照するステップと、
前回の問い合わせに対する返答日時とシステム情報を更新した日時とを比較するステップとを有し、
前記受信ステップでは、問い合わせとともに前回の問い合わせに対する返答日時を受信し、
前記返答ステップでは、その返答日時以降に更新されたシステム情報が返答される付記３３記載の通信方法。
【０１９７】
（付記３６）　送信元装置、その送信元装置が問い合わせたシステム情報の項目およびその問い合わせに対する返答日時を管理する返答履歴管理部を参照するステップと、
送信元装置から問い合わせがあったときに、前回の返答日時とシステム情報を更新した日時とを比較するステップとをさらに有し、
前記返答ステップでは、前回の返答日時の後に、更新されたシステム情報が返答される付記３３記載の通信方法。
【０１９８】
（付記３７）　問い合わせに対しシステム情報の返答可否を判断するステップをさらに有し、返答不可と判断されたシステム情報が返答されない付記３３記載の通信方法。
【０１９９】
（付記３８）　返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促すステップをさらに有する付記３７記載の通信方法。
【０２００】
（付記３９）　送信元装置の属性に係る情報を管理する送信元管理部を検索するステップと、
前記送信元装置に応じて返答可否を判断するステップとを有する付記３３記載の通信方法。
【０２０１】

（付記４０）　前記送信元装置に対して返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促すステップをさらに有する付記３９記載の通信方法。

【０２０２】

（付記４１）　送信元装置から相手装置へのシステム情報の問い合わせに対する返答を代行する通信方法であり、

前記送信元装置からの相手装置に係るシステム情報の問い合わせを受信する受信ステップと、

問い合わせに応じて、前記相手装置に係るシステム情報を検索するステップと、

前記相手装置に代わって通信部から返答するステップとを有する通信方法。

【０２０３】

（付記４２）　前記受信ステップでは、前記送信元装置に代えて、送信元装置の処理を代行する代理装置からシステム情報の問い合わせが受信される付記４１記載の通信方法。

【０２０４】

（付記４３）　コンピュータに、ネットワークを利用し電子的に情報を送信または受信するさせるプログラムであり、

情報の送受信の相手である相手装置に係るシステム情報を当該相手装置に問い合わせるステップと、

そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断する判断ステップとを有するプログラムを記録したコンピュータ読み取り可能な記録媒体。（１０）

（付記４４）　前記システム情報には、相手装置の安全性に関連する情報が含まれており、

前記判断ステップでは、相手装置の安全性が所定の程度に確保されているか否かに基づき、前記送受信を行うか否かが判断される付記４３記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０２０５】

（付記４５）　前記判断ステップにおいて、相手装置の安全性が所定の程度に確保されていないと判断されたときに、その事実または理由を相手装置に通知するステップをさらに有する付記４４記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０２０６】

（付記４６）　送受信する情報の種類に応じて、問い合わせるシステム情報の項目を選択するステップをさらに有する付記４３または４４記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０２０７】

（付記４７）　入手済みのシステム情報を管理する入手情報管理部を参照する参照ステップと、

その入手済みのシステム情報が相手装置において更新されているか否かを問い合わせる問い合わせステップと、

更新されたシステム情報および未入手のシステム情報を入手するステップとをさらに有する付記４３または４４記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０２０８】

（付記４８）　前記入手情報管理部は、システム情報の項目ごとにその情報を入手した日時を管理しており、

前記参照ステップでは、システム情報の項目ごとの入手日時が参照され、

前記問い合わせステップでは、その入手日時が付加されてシステム情報の項目が問い合わせられる付記４７記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０２０９】

（付記４９）　相手装置から返答されたシステム情報に基づき相手装置を検証する検証ステップをさらに有する付記４３記載のプログラムを記録したコンピュータ読み取り可能な

記録媒体。
【０２１０】
（付記５０）　前記入手したシステム情報を検証するテストパケットを前記相手装置に対して送信するステップをさらに有し、
前記検証ステップでは、そのテストパケットへのレスポンスに基づき相手装置が検証される付記４９記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【０２１１】
（付記５１）　コンピュータに、送信元装置から相手装置に電子的な情報の送信または受信を行うときに、送信元装置の処理を代行させるプログラムであり、
前記送信元装置からの指令を受信するステップと、
その指令にしたがい、前記相手装置に係るシステム情報を当該相手装置に問い合わせる問い合わせステップと、
そのシステム情報に基づいて、それ以降の送受信を行うか否かを判断するステップとを有するプログラムを記録したコンピュータ読み取り可能な記録媒体。
【０２１２】
（付記５２）　前記問い合わせステップでは、前記相手装置に代えて、相手装置の処理を代行する代理装置に対して相手装置に係るシステム情報が問い合わせられる付記５１記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【０２１３】
（付記５３）　コンピュータに、ネットワークを利用し電子的に情報を送信または受信させるプログラムであり、
送信元装置からシステム情報の問い合わせを受信する受信ステップと、
問い合わせに対するシステム情報を検索するステップと、
そのシステム情報を返答する返答ステップとを有するプログラムを記録したコンピュータ読み取り可能な記録媒体。
【０２１４】
（付記５４）　前記返答ステップでは、返答済みのシステム情報のうちの更新されたシステム情報および未返答のシステム情報が返答される付記５３記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【０２１５】
（付記５５）　システム情報を更新した日時を管理する更新履歴管理部を参照するステップと、
前回の問い合わせに対する返答日時とシステム情報を更新した日時とを比較するステップとを有し、
前記受信ステップでは、問い合わせとともに前回の問い合わせに対する返答日時を受信し、
前記返答ステップでは、その返答日時以降に更新されたシステム情報が返答される付記５３記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【０２１６】
（付記５６）　送信元装置、その送信元装置が問い合わせたシステム情報の項目およびその問い合わせに対する返答日時を管理する返答履歴管理部を参照するステップと、
送信元装置から問い合わせがあったときに、前回の返答日時とシステム情報を更新した日時とを比較するステップとをさらに有し、
前記返答ステップでは、前回の返答日時の後に、更新されたシステム情報が返答される付記５３記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【０２１７】
（付記５７）　問い合わせに対しシステム情報の返答可否を判断するステップをさらに有し、返答不可と判断されたシステム情報が返答されない付記５３記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。
【０２１８】

（付記５８）　返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促すステップをさらに有する付記５７記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０２１９】

（付記５９）　送信元装置の属性に係る情報を管理する送信元管理部を検索するステップと、

前記送信元装置に応じて返答可否を判断するステップとを有する付記５３記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０２２０】

（付記６０）　前記送信元装置に対して返答可否を決定できないシステム情報について、システム管理者に返答可否の判断を促すステップをさらに有する付記５９記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０２２１】

（付記６１）　コンピュータに、送信元装置から相手装置へのシステム情報の問い合わせに対する返答を代行させるプログラムであり、

前記送信元装置からの相手装置に係るシステム情報の問い合わせを受信する受信ステップと、

問い合わせに応じて、前記相手装置に係るシステム情報を検索するステップと、

前記相手装置に代わって通信部から返答するステップとを有するプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０２２２】

（付記６２）　前記受信ステップでは、前記送信元装置に代えて、送信元装置の処理を代行する代理装置からシステム情報の問い合わせが受信される付記６１記載のプログラムを記録したコンピュータ読み取り可能な記録媒体。

【０２２３】

【発明の効果】

以上説明したように、本発明によれば、通信相手の安全性を確認した上で通信することができる。

【図面の簡単な説明】

【図１】　本発明の第１実施形態におけるセキュリティレベルの確認を行う情報システムの構成図

【図２】　問い合わせ項目管理データベースのデータ構造を示す図

【図３】　入手データ管理データベースのデータ構造を示す図

【図４】　返答可否データベースのデータ構造を示す図

【図５】　セキュリティデータ管理データベースのデータ構造を示す図

【図６】　問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャート

【図７】　セキュリティデータの問い合わせ処理の詳細を示すフローチャート

【図８】　セキュリティデータの返答処理の詳細を示すフローチャート

【図９】　セキュリティ判定処理の詳細を示すフローチャート

【図１０】第１実施形態の変形例における返答履歴管理データベースのデータ構造を示す図

【図１１】第１実施形態の変形例における情報を過去に提供した日時と変更した日時を確認する処理示す図

【図１２】第２実施形態に係る情報システムのシステム構成図

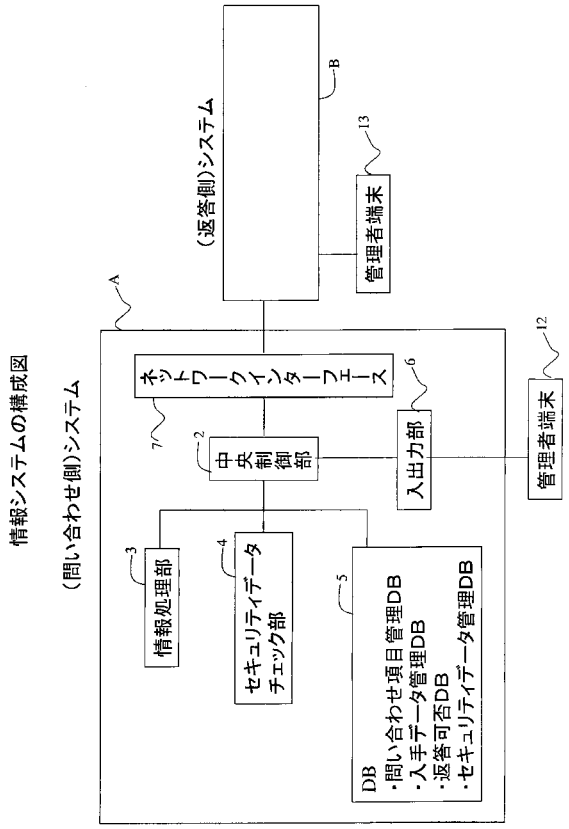
【図１３】返答側代理指定データベース２３のデータ構成を示す図

【図１４】第２実施形態における問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャート（１）

【図１５】第２実施形態における問い合わせ側のシステムと返答側のシステムとの通信手順を示すフローチャート（２）

【図１６】第２実施形態の変形例に係る情報システムのシステム構成図（１）
【図１７】第２実施形態の変形例に係る情報システムのシステム構成図（２）
【符号の説明】
Ａ、Ｂ　システム
２　中央制御部
３　情報処理部
４　セキュリティデータチェック部
５　データベース
６　入出力部
７　ネットワークインターフェース
１２、１３　管理者端末
２１　問い合わせ側代理指定ファイル
２２、Ｖ、Ｘ　問い合わせ側代理システム
２３　返答側代理指定データベース
２４、Ｗ、Ｙ　返答側代理システム

【図１】



【図２】

問い合わせ項目管理データベース

授受される情報の種類	必要なセキュリティデータ項目
1000万円未満の取引き 1000万円以上の取引き 関係者外秘情報 情報A	OS，パスワード暗号化 OS，パスワード暗号化，ログ監査，項目A OS，開いているポート，ウィルス対策，ログ監査 開いているポート，パスワード暗号化，項目A

【図３】

入手データ管理データベース

返答側システム	項目	入手日時	入手セキュリティデータ
システムB	OS	2000.9.14 09:00	Windows NT SP5
システムB	開いているポート	1999.11.9 17:32	7, 23, 80
システムB	ログ監査頻度	2000.9.17 01:04	1回／1日
システムB	項目A	2000.4.4	データA
システムC	OS	1999.1.25 03:57	Linux 2.2.8
システムC	パスワード暗号化	2000.10.5 14:24	している

【図４】

返答可否データベース

問い合わせ側システム	項目	判断
システムA	OS	×
システムA	開いているポート	○
システムA	ウィルス対策	○
システムA	ログ監査頻度	○
システムA	パスワード暗号化	○
システムA	項目A	×
システムC	OS	△
システムC	開いているポート	○
システムC	ウィルス対策	×
システムC	ログ監査頻度	○
システムC	パスワード暗号化	○
システムA	項目A	×

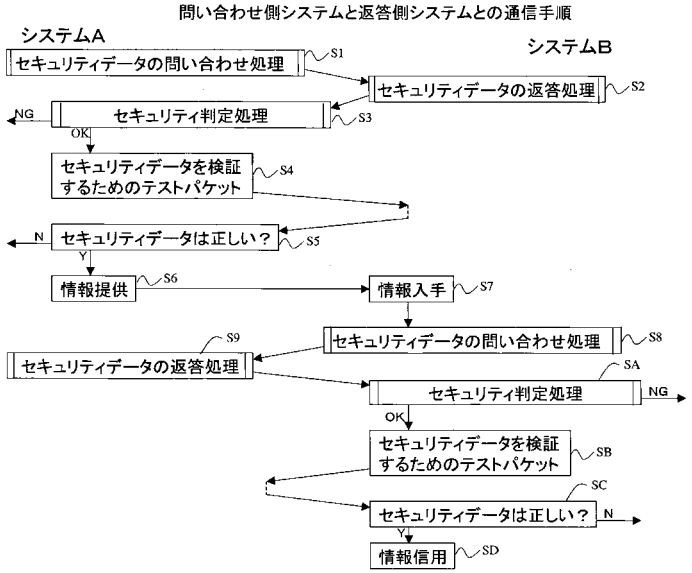
○：返答してよい
×：返答してはいけない
△：返答可否の判断不可

【図５】

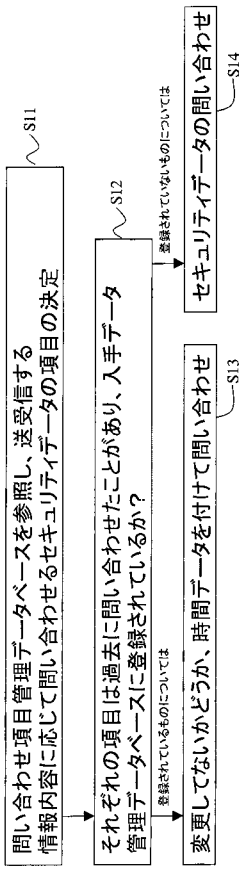
セキュリティデータ管理データベース

項目	セキュリティデータ	更新日時
OS	Windows NT SP5	2000.1.13 11:00
開いているポート	7, 23, 80	2000.3.31 12:24
ウィルス対策	Norton Anti Virus	2000.2.24 15:28
ログ監査頻度	1回／1日	1996.12.6 07:32
パスワード暗号化	している	1998.9.14 14:12
項目A	データA	1999.12.4 09:07

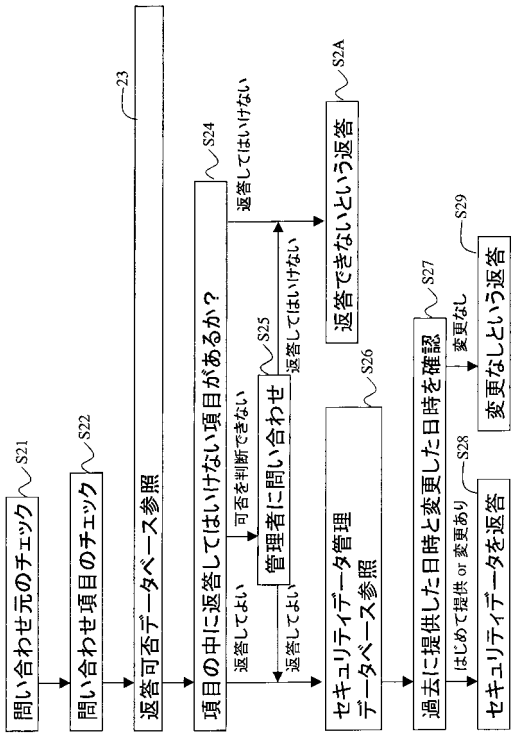
【図６】



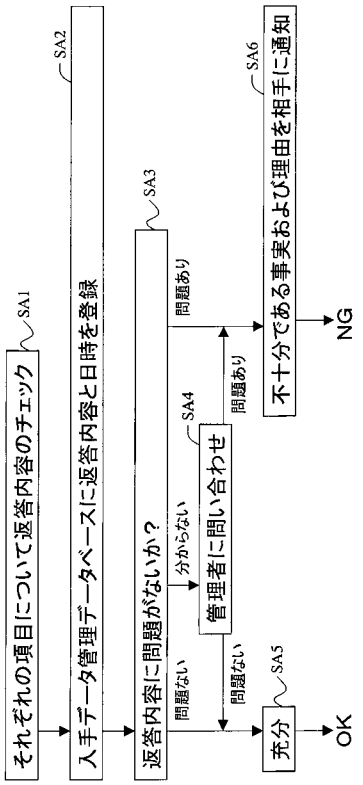
【図７】



【図８】



【図９】



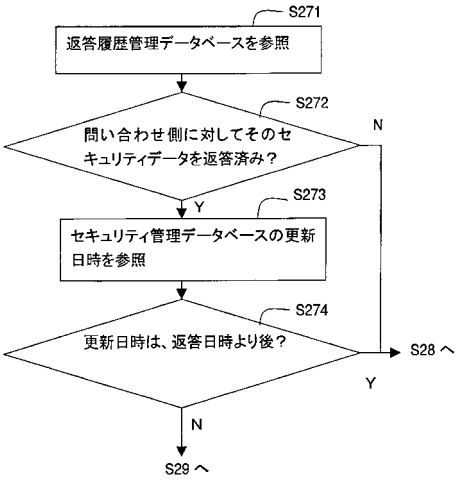
【図１０】

返答履歴管理データベース

問い合わせ側システム	項目	返答日時	返答セキュリティデータ
システムA	OS	2000.9.14 09:00	Windows NT SP5
システムA	開いているポート	1999.11.9 17:32	7, 23, 80
システムA	ログ監視頻度	2000.9.17 01:04	1回／1日
システムA	項目A	2000.4.4	データA
システムC	OS	1999.1.25 03:57	Linux 2.2.8
システムC	パスワード暗号化	2000.10.5 14:24	している

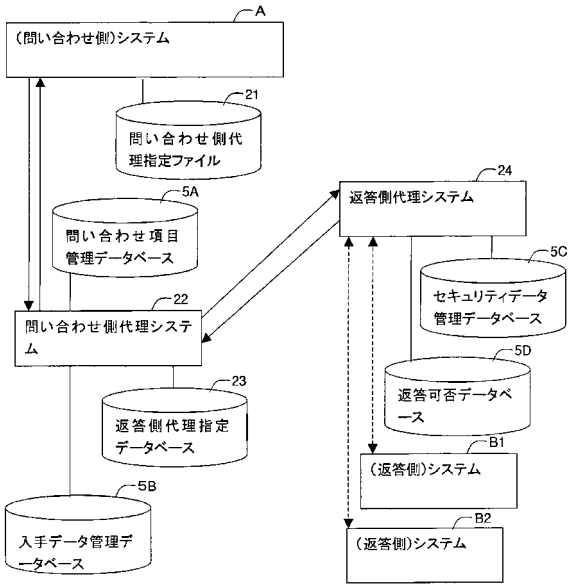
【図１１】

過去に提供をした日時と変更した日時を確認する処理(変形例)



【図１２】

第2実施形態に係る情報システムのシステム構成図

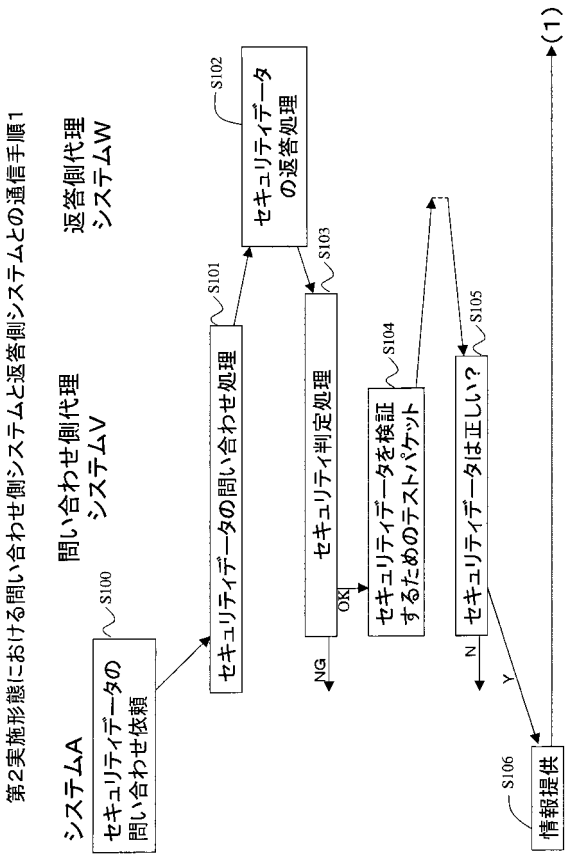


【図１３】

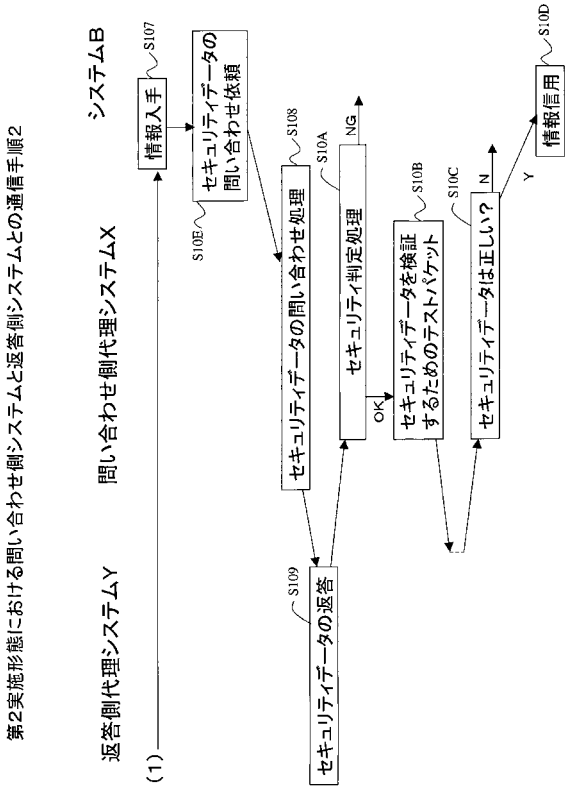
返答側代理指定データベース

返答側システム	返答側代理システム
B1	D1
B2	D1
B3	D2
:	

【図１４】

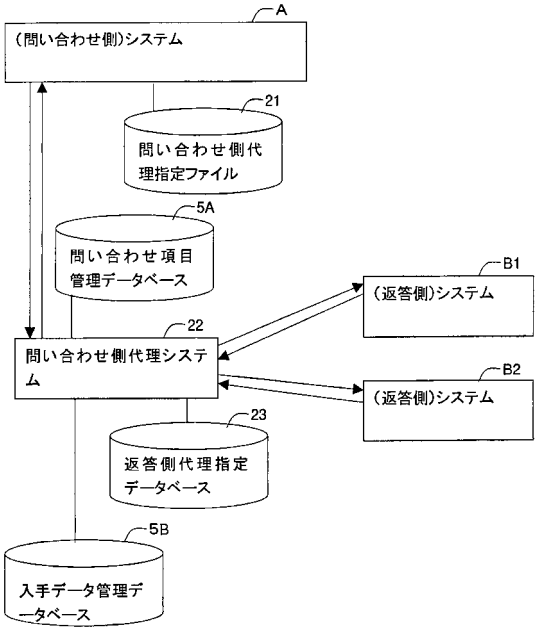


【図１５】



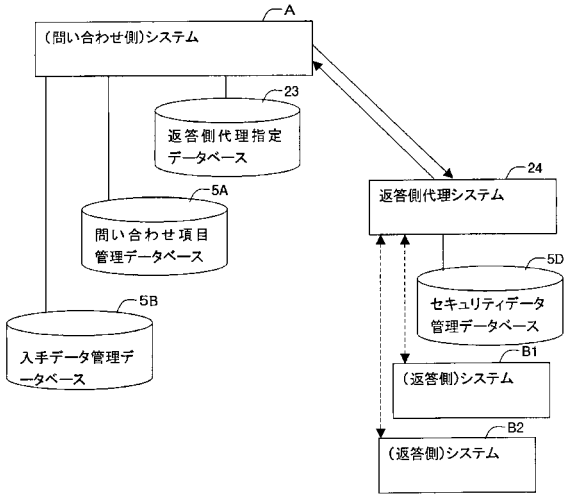
【図１６】

第2実施形態の変形例に係る情報システムのシステム構成図



【図１７】

第2実施形態の変形例に係る情報システムのシステム構成図



フロントページの続き

(72)発明者　黒田　康嗣
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　小谷　誠剛
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

審査官　阿部　弘

(56)参考文献　特開平０９－２００３４５（ＪＰ，Ａ）
特開２０００－２８７０２０（ＪＰ，Ａ）
特開平０４－２７７８５５（ＪＰ，Ａ）
特開昭６４－０４１５４０（ＪＰ，Ａ）
特開平０８－１８６６０１（ＪＰ，Ａ）
特開平１０－１６４１４５（ＪＰ，Ａ）

(58)調査した分野(Int.Cl.，ＤＢ名)
H04L 29/08
H04L 12/22
H04L 29/14