

(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2007-235730
(P2007-235730A)

(43) 公開日 平成19年9月13日(2007.9.13)

(51) Int. Cl. F I テーマコード(参考)
H04L 12/66 (2006.01) H04L 12/66 B 5K030

審査請求 未請求 請求項の数 7 O L (全 18 頁)

<p>(21) 出願番号 特願2006-56577 (P2006-56577)</p> <p>(22) 出願日 平成18年3月2日(2006.3.2)</p> <p>(出願人による申告) 国等の委託研究の成果に係る特許出願(平成17年度、総務省、「認証機能を具備するサービスプラットフォーム技術」委託研究、産業活力再生特別措置法第30条の適用を受けるもの)</p>	<p>(71) 出願人 399035766 エヌ・ティ・ティ・コミュニケーションズ株式会社 東京都千代田区内幸町一丁目1番6号</p> <p>(74) 代理人 100083806 弁理士 三好 秀和</p> <p>(74) 代理人 100095500 弁理士 伊藤 正和</p> <p>(74) 代理人 100101247 弁理士 高橋 俊一</p> <p>(74) 代理人 100098327 弁理士 高松 俊雄</p>
--	---

最終頁に続く

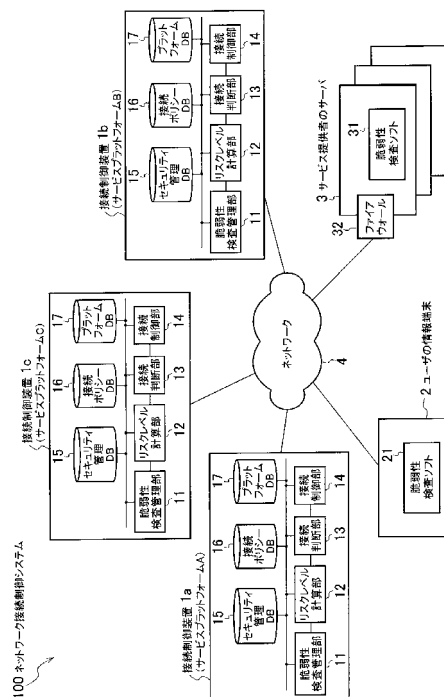
(54) 【発明の名称】 ネットワーク接続制御システム、ネットワーク接続制御方法、およびネットワーク接続制御プログラム

(57) 【要約】

【課題】 セキュリティレベルの低いユーザの情報端末あるいはサービス提供者のサーバがネットワークに接続することによる被害の発生を防止する。

【解決手段】 複数の接続制御装置 1 a - 1 c をユーザの情報端末 2 およびサービス提供者のサーバ 3 にネットワーク 4 を介して接続可能に設け、各接続制御装置 1 a - 1 c における脆弱性検査管理部 1 1 により情報端末 2 およびサーバ 3 のそれぞれの脆弱性を管理し、リスクレベル計算部 1 2 により情報端末 2 およびサーバ 3 について脆弱性レベルに基づくリスクレベルを計算し、接続判断部 1 3 により、情報端末 2 が接続しようとするサーバ 3 を管理する接続制御装置 1 b から、サーバ 3 への接続に必要な接続ポリシーを示す第 2 閾値を取得して、計算したリスクレベルと取得した第 2 閾値とを比較して情報端末 2 によるサーバ 3 への接続の可否を判断する。

【選択図】 図 1



【特許請求の範囲】

【請求項 1】

ユーザの情報端末およびサービス提供者のサーバに対してネットワークを介して接続可能な複数の接続制御装置を備えたネットワーク接続制御システムであって、

各接続制御装置は、

当該接続制御装置への接続に必要な接続ポリシーを示す第 1 閾値および前記サーバへの接続に必要な接続ポリシーを示す第 2 閾値を記憶しておくデータベースと、

前記情報端末からは当該情報端末の脆弱性レベルを示す情報を受信し、前記サーバからは当該サーバの脆弱性レベルを示す情報を受信して、前記情報端末および前記サーバのそれぞれの ID と脆弱性レベルとを関連付けてデータベースに記憶させる脆弱性管理手段と

10

、
前記情報端末および前記サーバのそれぞれについて、前記データベースから読み出した脆弱性レベルに基づいてリスクレベルを計算してメモリに記憶させるリスクレベル計算手段と、

前記メモリからリスクレベルを読み出すとともに前記データベースから第 1 閾値を読み出し、前記情報端末および前記サーバのそれぞれについてリスクレベルと第 1 閾値とを比較して当該接続制御装置への接続の可否を判断する接続判断手段と、

前記情報端末が接続しようとするサーバが当該接続制御装置による管理下において接続の許可されたサーバである場合には前記データベースから第 2 閾値を取得し、当該接続制御装置による管理下でないサーバの場合には当該サーバの接続が許可された他の接続制御装置へアクセスして当該サーバへの接続に必要な接続ポリシーを示す第 2 閾値を取得し、前記情報端末のリスクレベルと取得した第 2 閾値とを比較して前記情報端末による当該サーバへの接続の可否を判断する接続判断手段と、

20

を有することを特徴とするネットワーク接続制御システム。

【請求項 2】

前記情報端末および前記サーバは、

正、副の二つの接続制御装置に関する情報を記憶しておく記憶手段と、

正の接続制御装置への接続に際して応答がなかった場合に、副の接続制御装置への接続に切り替える接続切替手段と、

をそれぞれ有することを特徴とする請求項 1 記載のネットワーク接続制御システム。

30

【請求項 3】

前記正、副の二つの接続制御装置は、

前記情報端末および前記サーバによる接続制御装置への接続の許可状態を示す情報と、前記情報端末による前記サーバへの接続に必要な接続ポリシーを示す第 2 閾値とを共有する共有手段をそれぞれ有することを特徴とする請求項 2 記載のネットワーク接続制御システム。

【請求項 4】

前記接続制御装置は、前記情報端末による接続が許可されたサーバに対して、この接続許可の制御を行う接続制御手段を有することを特徴とする請求項 1 乃至 3 のいずれかに記載のネットワーク接続制御システム。

40

【請求項 5】

前記リスクレベル計算手段は、脆弱性レベルとその脆弱性レベルの状態で経過した経過時間との積について脆弱性の数の分だけ総和をとることよりリスクレベルを計算することを特徴とする請求項 1 乃至 4 のいずれかに記載のネットワーク接続制御システム。

【請求項 6】

ユーザの情報端末およびサービス提供者のサーバに対してネットワークを介して接続可能な複数の接続制御装置を用いて行うネットワーク接続制御方法であって、

各接続制御装置により、

当該接続制御装置への接続に必要な接続ポリシーを示す第 1 閾値および前記サーバへの接続に必要な接続ポリシーを示す第 2 閾値をデータベースに記憶させるステップと、

50

前記情報端末からは当該情報端末の脆弱性レベルを示す情報を受信し、前記サーバからは当該サーバの脆弱性レベルを示す情報を受信して、前記情報端末および前記サーバのそれぞれのIDと脆弱性レベルとを関連付けてデータベースに記憶させるステップと、

前記情報端末および前記サーバのそれぞれについて、前記データベースから読み出した脆弱性レベルに基づいてリスクレベルを計算してメモリに記憶させるステップと、

前記メモリからリスクレベルを読み出すとともに前記データベースから第1閾値を読み出し、前記情報端末および前記サーバのそれぞれについてリスクレベルと第1閾値とを比較して当該接続制御装置への接続の可否を判断するステップと、

前記情報端末が接続しようとするサーバが当該接続制御装置による管理下において接続の許可されたサーバである場合には前記データベースから第2閾値を取得し、当該接続制御装置による管理下でないサーバの場合には当該サーバの接続が許可された他の接続制御装置へアクセスして当該サーバへの接続に必要な接続ポリシーを示す第2閾値を取得し、前記情報端末のリスクレベルと取得した第2閾値とを比較して前記情報端末による当該サーバへの接続の可否を判断するステップと、

を有することを特徴とするネットワーク接続制御方法。

【請求項7】

ユーザの情報端末およびサービス提供者のサーバに対してネットワークを介して接続可能な複数の接続制御装置のそれぞれに実行させる接続制御プログラムであって、

当該接続制御装置への接続に必要な接続ポリシーを示す第1閾値および前記サーバへの接続に必要な接続ポリシーを示す第2閾値をデータベースに記憶させる処理と、

前記情報端末からは当該情報端末の脆弱性レベルを示す情報を受信し、前記サーバからは当該サーバの脆弱性レベルを示す情報を受信して、前記情報端末および前記サーバのそれぞれのIDと脆弱性レベルとを関連付けてデータベースに記憶させる処理と、

前記情報端末および前記サーバのそれぞれについて、前記データベースから読み出した脆弱性レベルに基づいてリスクレベルを計算してメモリに記憶させる処理と、

前記メモリからリスクレベルを読み出すとともに前記データベースから第1閾値を読み出し、前記情報端末および前記サーバのそれぞれについてリスクレベルと第1閾値とを比較して当該接続制御装置への接続の可否を判断する処理と、

前記情報端末が接続しようとするサーバが当該接続制御装置による管理下において接続の許可されたサーバである場合には前記データベースから第2閾値を取得し、当該接続制御装置による管理下でないサーバの場合には当該サーバの接続が許可された他の接続制御装置へアクセスして当該サーバへの接続に必要な接続ポリシーを示す第2閾値を取得し、前記情報端末のリスクレベルと取得した第2閾値とを比較して前記情報端末による当該サーバへの接続の可否を判断する処理と、

を実行させることを特徴とするネットワーク接続制御プログラム。

【発明の詳細な説明】

【技術分野】

【0001】

本発明は、ユーザの情報端末あるいはサービス提供者のサーバについて各々のセキュリティの状態に応じてネットワークへの接続を制御する技術に関する。

【背景技術】

【0002】

従来より、社内等を対象にした狭域ネットワークにおいては、サーバによりクライアント端末のセキュリティ状態を診断し、ネットワーク全体としてセキュリティ状態を管理するシステムが利用されている（例えば特許文献1参照）。

【0003】

一方、インターネット等による広域ネットワークを利用する場合には、各ユーザはパソコン等の情報端末のセキュリティ状態を自分で把握し対処している。具体的には、各ユーザは、脆弱性検査用のソフトウェア、ウィルス対策用のソフトウェア、不正侵入防止用のパーソナルファイアウォール等を情報端末にインストールし、これらのソフトを用いてセ

10

20

30

40

50

キュリティ状態を管理している。尚、その他、本願に関連する技術としては特許文献 2 , 3 に記載のものが知られている。

【特許文献 1】特開 2004 - 289260 号公報

【特許文献 2】特開 2004 - 220120 号公報

【特許文献 3】特開 2004 - 234378 号公報

【発明の開示】

【発明が解決しようとする課題】

【0004】

しかしながら、近年のインターネットの急速な普及に伴ってユーザの裾野が広がる中で、全てのユーザがセキュリティ管理に精通しているわけではないため、全てのユーザが日々発生する新しい脆弱性に対応し、対処することは困難である。 10

【0005】

また、インターネットを通じてユーザに対して何らかのサービスを提供しようとするサービス提供者においても、サーバ等のセキュリティ管理を自分でやっているため、同様の問題があり、さらにはユーザの情報端末のセキュリティ状態に応じて接続の可否を判断することはできてきない。

【0006】

このため、サービス提供者にとっては、自己のサーバにセキュリティの低い情報端末がアクセスしてきた場合には、第三者による不正アクセスや、なりすましといった被害を受けるおそれがある。また、ユーザにとっても、自己の情報端末がアクセスしたサービス提供者のサーバのセキュリティが低い場合には、やはり第三者による不正アクセスや通信異常といった被害を受けるおそれがある。 20

【0007】

本発明は、上記に鑑みてなされたものであり、その課題とするところは、セキュリティレベルの低いユーザの情報端末あるいはサービス提供者のサーバがネットワークに接続することによる被害の発生を防止することにある。

【課題を解決するための手段】

【0008】

第 1 の本発明に係るネットワーク接続制御システムは、ユーザの情報端末およびサービス提供者のサーバに対してネットワークを介して接続可能な複数の接続制御装置を備えたネットワーク接続制御システムであって、各接続制御装置は、当該接続制御装置への接続に必要な接続ポリシーを示す第 1 閾値および前記サーバへの接続に必要な接続ポリシーを示す第 2 閾値を記憶しておくデータベースと、前記情報端末からは当該情報端末の脆弱性レベルを示す情報を受信し、前記サーバからは当該サーバの脆弱性レベルを示す情報を受信して、前記情報端末および前記サーバのそれぞれの ID と脆弱性レベルとを関連付けてデータベースに記憶させる脆弱性管理手段と、前記情報端末および前記サーバのそれぞれについて、前記データベースから読み出した脆弱性レベルに基づいてリスクレベルを計算してメモリに記憶させるリスクレベル計算手段と、前記メモリからリスクレベルを読み出すとともに前記データベースから第 1 閾値を読み出し、前記情報端末および前記サーバのそれぞれについてリスクレベルと第 1 閾値とを比較して当該接続制御装置への接続の可否を判断する接続判断手段と、前記情報端末が接続しようとするサーバが当該接続制御装置による管理下において接続の許可されたサーバである場合には前記データベースから第 2 閾値を取得し、当該接続制御装置による管理下でないサーバの場合には当該サーバの接続が許可された他の接続制御装置へアクセスして当該サーバへの接続に必要な接続ポリシーを示す第 2 閾値を取得し、前記情報端末のリスクレベルと取得した第 2 閾値とを比較して前記情報端末による当該サーバへの接続の可否を判断する接続判断手段と、を有することを特徴とする。 40

【0009】

本発明にあつては、ユーザの情報端末とサービス提供者のサーバのそれぞれについて、脆弱性レベルに基づいてリスクレベルを計算し、このリスクレベルと第 1 閾値とを比較し 50

て接続制御装置への接続の可否を判断することで、リスクレベルが第1閾値による条件を満たさない情報端末あるいはサーバについては接続制御装置への接続を拒否し、セキュリティレベルの低い情報端末あるいはサーバが接続されることによる被害の発生を防止する。

【0010】

また、ユーザの情報端末のリスクレベルと第2閾値とを比較して情報端末によるサーバへの接続の可否を判断することで、リスクレベルが第2閾値の条件を満たさない情報端末についてはサーバへの接続を拒否し、セキュリティレベルの低い情報端末がサーバに接続した場合に起こり得る不正アクセスやなりすましといった被害の発生を防止する。

【0011】

さらに、複数の接続制御装置を設け、情報端末が接続しようとするサーバが、その情報端末が接続中の接続制御装置による管理下でないサーバの場合には、当該接続制御装置によりそのサーバの接続が許可された他の接続制御装置へアクセスして当該サーバへの接続に必要な接続ポリシーを示す第2閾値を取得し、これを用いて情報端末のサーバへの接続の可否を判断することで、ユーザの情報端末は、接続中の接続制御装置以外の接続制御装置が管理するサーバによるサービスの提供を受けることができる。

【0012】

上記ネットワーク接続制御システムは、前記情報端末および前記サーバが、正、副の二つの接続制御装置に関する情報を記憶しておく記憶手段と、正の接続制御装置への接続に際して応答がなかった場合に、副の接続制御装置への接続に切り替える接続切替手段と、

10

20

【0013】

本発明にあつては、情報端末およびサーバが、正、副の二つの接続制御装置に関する情報を記憶しておき、正の接続制御装置への接続に際して応答がなかった場合に、副の接続制御装置への接続に切り替えることで、情報端末あるいはサーバの接続先である接続制御装置に故障等が発生した場合でも、他の接続制御装置へ接続することができる。

【0014】

上記ネットワーク接続制御システムは、前記正、副の二つの接続制御装置が、前記情報端末および前記サーバによる前記接続制御装置への接続の許可状態を示す情報と、前記情報端末による前記サーバへの接続に必要な接続ポリシーを示す第2閾値とを共有する共有手段をそれぞれ有することを特徴とする。

30

【0015】

本発明にあつては、正、副の二つの接続制御装置が、情報端末およびサーバによる接続制御装置への接続の許可状態を示す情報と、情報端末によるサーバへの接続に必要な接続ポリシーを示す第2閾値とを共有することで、副の接続制御装置においても、接続判断手段によって、情報端末が接続しようとするサーバが当該接続制御装置によって接続が許可されたサーバである場合にはデータベースから第2閾値を取得し、当該接続制御装置による管理下でないサーバの場合には当該サーバの接続が許可された他の接続制御装置へアクセスして当該サーバへの接続に必要な接続ポリシーを示す第2閾値を取得することが可能になり、情報端末はサービス提供者のサーバへ接続して、サービスの提供を受けることができる。

40

【0016】

上記ネットワーク接続制御システムは、前記各接続制御装置は、情報端末による接続が許可されたサーバに対して、この接続許可の制御を行う接続制御手段を有することを特徴とする。

【0017】

本発明にあつては、接続制御装置からサーバに対して情報端末による接続許可の制御を行うことで、情報端末がサーバに対して確実に接続できるようにする。

【0018】

上記ネットワーク接続制御システムは、前記リスクレベル計算手段が、脆弱性レベルと

50

その脆弱性レベルのまま経過した経過時間との積について脆弱性の数の分だけ総和をとることよりリスクレベルを計算することを特徴とする。

【0019】

本発明にあっては、脆弱性の大きい状態が長く続く程、セキュリティレベルが低いといえることから、脆弱性レベルと経過時間との積の総和をもってリスクレベルを定義することで、接続可否の判断をより正確なものにする。

【0020】

第2の本発明に係るネットワーク接続制御方法は、ユーザの情報端末およびサービス提供者のサーバに対してネットワークを介して接続可能な複数の接続制御装置を用いて行うネットワーク接続制御方法であって、各接続制御装置により、当該接続制御装置への接続に必要な接続ポリシーを示す第1閾値および前記サーバへの接続に必要な接続ポリシーを示す第2閾値をデータベースに記憶させるステップと、前記情報端末からは当該情報端末の脆弱性レベルを示す情報を受信し、前記サーバからは当該サーバの脆弱性レベルを示す情報を受信して、前記情報端末および前記サーバのそれぞれのIDと脆弱性レベルとを関連付けてデータベースに記憶させるステップと、前記情報端末および前記サーバのそれぞれについて、前記データベースから読み出した脆弱性レベルに基づいてリスクレベルを計算してメモリに記憶させるステップと、前記メモリからリスクレベルを読み出すとともに前記データベースから第1閾値を読み出し、前記情報端末および前記サーバのそれぞれについてリスクレベルと第1閾値とを比較して当該接続制御装置への接続の可否を判断するステップと、前記情報端末が接続しようとするサーバが当該接続制御装置による管理下において接続の許可されたサーバである場合には前記データベースから第2閾値を取得し、当該接続制御装置による管理下でないサーバの場合には当該サーバの接続が許可された他の接続制御装置へアクセスして当該サーバへの接続に必要な接続ポリシーを示す第2閾値を取得し、前記情報端末のリスクレベルと取得した第2閾値とを比較して前記情報端末による当該サーバへの接続の可否を判断するステップと、を有することを特徴とする。

10

20

【0021】

第3の本発明に係るネットワーク接続制御プログラムは、ユーザの情報端末およびサービス提供者のサーバに対してネットワークを介して接続可能な複数の接続制御装置のそれぞれに実行させる接続制御プログラムであって、当該接続制御装置への接続に必要な接続ポリシーを示す第1閾値および前記サーバへの接続に必要な接続ポリシーを示す第2閾値をデータベースに記憶させる処理と、前記情報端末からは当該情報端末の脆弱性レベルを示す情報を受信し、前記サーバからは当該サーバの脆弱性レベルを示す情報を受信して、前記情報端末および前記サーバのそれぞれのIDと脆弱性レベルとを関連付けてデータベースに記憶させる処理と、前記情報端末および前記サーバのそれぞれについて、前記データベースから読み出した脆弱性レベルに基づいてリスクレベルを計算してメモリに記憶させる処理と、前記メモリからリスクレベルを読み出すとともに前記データベースから第1閾値を読み出し、前記情報端末および前記サーバのそれぞれについてリスクレベルと第1閾値とを比較して当該接続制御装置への接続の可否を判断する処理と、前記情報端末が接続しようとするサーバが当該接続制御装置による管理下において接続の許可されたサーバである場合には前記データベースから第2閾値を取得し、当該接続制御装置による管理下でないサーバの場合には当該サーバの接続が許可された他の接続制御装置へアクセスして当該サーバへの接続に必要な接続ポリシーを示す第2閾値を取得し、前記情報端末のリスクレベルと取得した第2閾値とを比較して前記情報端末による当該サーバへの接続の可否を判断する処理と、を実行させることを特徴とする。

30

40

【発明の効果】

【0022】

本発明によれば、セキュリティレベルの低いユーザの情報端末あるいはサービス提供者のサーバがネットワークに接続することによる被害の発生を防止することができる。

【0023】

また、本発明によれば、セキュリティレベルの低い情報端末がサーバに接続した場合に

50

起こり得る不正アクセスやなりすましといった被害の発生を防止することができる。

【0024】

さらに、本発明によれば、ユーザの情報端末は、接続中の接続制御装置以外の接続制御装置が管理するサーバによるサービスの提供を受けることができる。

【発明を実施するための最良の形態】

【0025】

以下、本発明の最良の形態について図面を用いて説明する。

【0026】

図1は、本実施の形態におけるネットワーク接続制御システムの構成を示すブロック図である。ネットワーク接続制御システム100は、ユーザの情報端末2およびサービス提供者のサーバ3に対してネットワーク4を介して接続可能な複数の接続制御装置1a-1cを備えた構成である。各接続制御装置1a-1cにはコンピュータシステムが用いられる。各接続制御装置1a-1cは、それぞれ別個の運営者によって運営されるものであり、ここではサービスプラットフォームA-Cと適宜呼ぶものとする。

10

【0027】

同図に示すように、各接続制御装置1a-1cは、脆弱性検査管理部11、リスクレベル計算部12、接続判断部13、接続制御部14、セキュリティ管理データベース15、接続ポリシーデータベース16、プラットフォームデータベース17を有しており、各部の処理は、接続制御装置1にインストールされたプログラムによって実行される。各処理の詳細については後述する。

20

【0028】

ユーザの情報端末2は、パーソナルコンピュータや携帯端末等に相当する。情報端末2には情報端末2の脆弱性を検査するための脆弱性検査ソフト21が予めインストールされている。

【0029】

サービス提供者のサーバ3もコンピュータシステムによって構成される。サーバ3には脆弱性検査ソフト31がインストールされている。また、サーバ3は、情報端末2との接続の可否を制御するためのファイアウォール32がインストールされており、ファイアウォール32によって許可された情報端末2に対してネットワーク4を介して情報提供等のサービスを行う機能を備えている。

30

【0030】

ネットワーク4は、インターネットに代表される広域ネットワークである。なお、同図においては、説明の便宜上、情報端末2およびサーバ3を1つずつ示しているが、情報端末2とサーバ3がそれぞれ複数ある場合にも本システムは適用可能である。

【0031】

次に、各接続制御装置1a-1cの各部における処理について説明する。

【0032】

脆弱性検査管理部11は、情報端末2から情報端末2の脆弱性レベルを示す情報を受信するとともに、サーバ3からサーバ3の脆弱性レベルを示す情報を受信し、情報端末2およびサーバ3のそれぞれについて脆弱性レベルを関連付けてセキュリティ管理データベース15に記憶させる。1つの情報端末2あるいはサーバ3において複数の脆弱性がある場合には、脆弱性毎にそれぞれ登録する。この登録においては、セキュリティ管理データベース15で管理されている脆弱性管理テーブル、脆弱性マスタテーブルを用いる。

40

【0033】

脆弱性管理テーブルは、図2に示すように、情報端末ID・サーバID、脆弱性ID、発見日時、対処日時の対応関係を管理するためのものである。脆弱性マスタテーブルは、図3に示すように、脆弱性ID、脆弱性名称、脆弱性レベルの対応関係を管理するためのものである。この脆弱性マスタテーブルでは、脆弱性レベルは、セキュリティが強いほど低く、セキュリティが弱いほど高くなるように定義されている。これらのテーブルを用いることで、情報端末2あるいはサーバ3が送信する脆弱性情報に含ませる情報として、脆

50

弱性レベルそのものを用いた場合にも、これに代えて脆弱性IDを用いた場合にも対応可能となる。

【0034】

リスクレベル計算部12は、セキュリティ管理データベース15から脆弱性レベルを読み出し、情報端末2およびサーバ3のそれぞれについて脆弱性レベルに基づいてリスクレベルを計算して内部のメモリに記憶させる。計算手法の詳細については後述する。

【0035】

接続ポリシーデータベース16は、自己の接続制御装置1への接続に必要な接続ポリシーを示す第1閾値、および情報端末2からサーバ3への接続に必要な接続ポリシーを示す第2閾値を予め記憶している。具体的には、接続ポリシーデータベース16は、第1閾値管理テーブルと第2閾値管理テーブルを記憶している。第1閾値管理テーブルは、図4に示すように、情報端末2とサーバ3のそれぞれについて接続ポリシーと第1閾値とを対応させたものである。第2閾値管理テーブルは、図5に示すように、接続ポリシーと第2閾値とを対応させたものである。ここで、第1閾値に対応する接続ポリシーとは、接続制御装置1の運営者が、情報端末2あるいはサーバ3に対して接続制御装置1への接続を許可できるレベルの方針のことをいい、第2閾値に対応する接続ポリシーとは、サービス提供者が、情報端末2に対して自己のサーバ3への接続を許可できるレベルの方針のことをいう。

10

【0036】

また、接続ポリシーデータベース16は、接続ポリシー管理テーブルを予め記憶している。接続ポリシー管理テーブルは、図6に示すように、サービスID、接続ポリシー、サービスURL、ファイアウォールアドレス、サービスプロトコルを対応付けて管理するためのものである。サービスIDは、サービスを特定するためのIDである。接続ポリシーは、そのサービスを提供するサービス提供者が情報端末に対する接続許可レベルとして設定する項目であり、第2閾値に対応する。サービスURLは、そのサービスを提供するための情報が格納されている格納先を指定するためのアドレスである。ファイアウォールアドレスは、そのサービスを提供するサーバ3におけるファイアウォール32のアドレスであり、サービスプロトコルは、そのサービスの提供に際して通信に用いられるプロトコルである。

20

【0037】

接続判断部13は、リスクレベル計算部12が計算したリスクレベルをメモリから読み出すとともに、接続ポリシーデータベース16から第1閾値を読み出し、情報端末2およびサーバ3のそれぞれについてリスクレベルと第1閾値とを比較して接続制御装置1への接続の可否を判断する。

30

【0038】

接続制御部14は、接続制御装置1への接続の可否の結果を情報端末2あるいはサーバ3へ通知するとともに、接続が許可された情報端末2あるいはサーバ3の接続制御装置1への接続の制御を行う。そして、接続制御装置1に接続してきた情報端末2あるいはサーバ3については、図7に示す接続状態管理テーブルに情報端末IDあるいはサーバIDと接続日時を登録する。この接続状態管理テーブルは、セキュリティ管理データベース15に記憶しておく。

40

【0039】

また、接続判断部13は、情報端末2のリスクレベルをメモリから読み出すとともに、情報端末2が接続しようとするサーバ3が当該接続制御装置1による管理下において接続が許可されたサーバの場合には接続ポリシーデータベース16から第2閾値を取得し、管理下でないサーバの場合には当該サーバ3の接続が許可された他の接続制御装置へアクセスして当該サーバ3への接続に必要な接続ポリシーを示す第2閾値を取得し、情報端末2のリスクレベルと取得した第2閾値とを比較して情報端末2の当該サーバ3への接続の可否を判断する。

【0040】

50

この後、接続制御部 14 は、サーバ 3 への接続の可否の結果を情報端末 2 へ通知するとともに、サーバ 3 に対しては接続が許可された情報端末 2 の接続を認めるように指示を出す。

【0041】

ここで、接続制御装置 1 の接続判断部 13 が他の接続制御装置を特定できるように、プラットフォームデータベース 17 には、図 8 に示すような、各接続制御装置（サービスプラットフォーム）についてドメイン名称と接続先 IP アドレスとを対応付けたサービスプラットフォーム管理テーブルを記憶させておく。

【0042】

また、情報端末 2 およびサーバ 3 は、正、副の 2 つの接続制御装置に関する情報を記憶しておく記憶装置をそれぞれ備えており、正の接続制御装置への接続に際して応答がなかった場合に、副の接続制御装置への接続に切り替える機能をそれぞれ備えている。

10

【0043】

正、副の接続制御装置は、相手の接続制御装置が管理する情報端末 2 およびサーバ 3 について自己でも管理できるように、情報端末 2 およびサーバ 3 による接続制御装置 1 への接続の許可状態を示す情報としての接続状態管理テーブルと、情報端末 2 によるサーバ 3 への接続に必要な接続ポリシーを示す情報としての接続ポリシー管理テーブルとを共有するようになっている。共有の仕方としては、これらのテーブルを記憶したデータベースそのものを正、副の接続制御装置でマウントすることで実際に共有してもよいし、これらのテーブルの内容を定期的に交換するようによい。

20

【0044】

次に、本ネットワーク接続制御システム 100 における全体的な処理の流れを示しながら、各部の処理についてより詳細に説明する。本処理は、(1) 情報端末 2 およびサーバ 3 における脆弱性の検査、(2) 情報端末 2 およびサーバ 3 による接続制御装置 1 への接続、(3) 情報端末 2 によるサーバ 3 への接続、の 3 段階を有する。以下、順に説明する。

【0045】

[脆弱性の検査]

まず、情報端末 2 およびサーバ 3 における脆弱性検査の処理について説明する。情報端末 2 およびサーバ 3 では、それぞれの脆弱性検査ソフトを実行することにより、脆弱性のレベルを示す情報を生成する。脆弱性のレベルを示す情報は、脆弱性レベルそのものを示すものでもよいし、後述するように脆弱性 ID であってもよい。情報端末 2 およびサーバ 3 では、この脆弱性のレベルを示す情報、脆弱性の発見日時、対処日時を含む脆弱性情報を記憶しておく。

30

【0046】

この脆弱性検査の処理について図 9 のシーケンス図を用いて説明する。同図では、サービスプラットフォーム A（接続制御装置 1a）がユーザの情報端末 2 による接続を管理し、サービスプラットフォーム B（接続制御装置 1b）がサービス提供者のサーバ 3 による接続を管理するものとする。

【0047】

情報端末 2 における脆弱性検査ソフト 21 は、随時または定期的に起動する（ステップ 1：図においては「S1」と示す。以下同じ）。脆弱性検査ソフト 21 は、検査パターンの確認のためサービスプラットフォーム A（接続制御装置 1a）にアクセスする。

40

【0048】

サービスプラットフォーム A では、情報端末 2 に記憶されている検査パターン情報と最新の検査パターン情報とを比較する（ステップ 2）。両者に相違がある場合には、検査パターンの更新が必要である旨を情報端末 2 に応答し、両者に相違がない場合には、更新は必要ない旨を情報端末 2 に応答する。

【0049】

情報端末 2 の脆弱性検査ソフト 21 は、更新が必要な場合には、検査パターンの更新を

50

サービスプラットフォーム A に要求する (ステップ 3)。サービスプラットフォーム A はその要求に応じて最新の検査パターンを情報端末 2 へ送信する (ステップ 4)。情報端末 2 では、この最新の検査パターンを適用する (ステップ 5)

そして、脆弱性検査ソフト 2 1 は、最新の検査パターンを用いて情報端末 2 における脆弱性の検査を行い、脆弱性のレベルを示す情報、脆弱性の発見日時、対処日時を脆弱性検査結果情報として保存する (ステップ 6, 7)。

【0050】

図 9 においては、情報端末 2 における脆弱性検査の処理を示したが、サーバ 3 においても同様の処理を行う。

【0051】

[接続制御装置への接続]

次に、情報端末 2 およびサーバ 3 が接続制御装置 1 へ接続する際の処理について図 10 のシーケンス図を用いて説明する。なお、同図においても情報端末 2 を対象に示しているが、サーバ 3 でも同様の処理を行う。

【0052】

サービスプラットフォームに接続しようとする情報端末 2 あるいはサーバ 3 は、そのサービスプラットフォームに対して脆弱性検査結果情報を含む接続要求を送信する (ステップ 11)。この接続要求には、脆弱性情報の他、情報端末識別用の情報端末 ID あるいはサーバ識別用のサーバ ID が含まれる。

【0053】

接続要求を受けたサービスプラットフォーム A では、脆弱性検査管理部 1 1 により、情報端末 2 あるいはサーバ 3 のそれぞれについて脆弱性レベルを関連付けてセキュリティ管理データベース 1 5 の脆弱性管理テーブルに登録する (ステップ 12)。

【0054】

続いて、リスクレベル計算部 1 2 により、情報端末 2 あるいはサーバ 3 について、リスクレベルを計算する (ステップ 13)。この計算では、まず脆弱性管理テーブルと脆弱性マスタテーブルを用いて、情報端末 2 あるいはサーバ 3 についての脆弱性レベルを読み出すとともに、その脆弱性レベルに対応する発見日時と対処日時を読み出す。そして、発見日時と対処日時の差分を取ることにより、その脆弱性レベルの状態が放置されたまま経過した経過時間を算出する。また、対処がなされておらず、対処日時に関する情報がない場合には、現在日時を取得し、発見日時と現在日時の差分をとることにより経過時間を算出する。脆弱性レベルの高い状態が長時間に渡って放置されている場合には、リスクレベルが高いと考えられるので、リスクレベル計算部 1 2 では、次式 (1) に従ってリスクレベル RL を計算する。

【0055】

$$RL = (\text{脆弱性レベル} \times \text{経過時間}) \quad (1)$$

ここで、積分記号 \int は、1 つの情報端末 2 あるいはサーバ 3 に複数の脆弱性がある場合に、その情報端末 2 あるいはサーバ 3 におけるそれぞれのリスクレベルの合計を求めることを意味する。

【0056】

式 (1) を用いた計算に際しては、脆弱性レベルについては、例えば「高」は 10 ポイント、「中」は 5 ポイント、「低」は 1 ポイントなどと決めておき、経過時間については、例えば 3 日未満は 0.1 ポイント、3 日以上 1 週間未満は 0.5 ポイント、1 週間以上 1 ヶ月未満は 0.8 ポイント、1 ヶ月以上は 1.0 ポイントなどと決めておくようにする。

【0057】

続いて、接続判断部 1 3 により、接続ポリシーデータベース 1 6 に記憶されている第 1 閾値管理テーブルを用いて、サービスプラットフォーム A への接続の可否判断を行う (ステップ 14)。接続判断部 1 3 は、情報端末 2 について接続可否の判断をするときには、情報端末 2 に対応する第 1 閾値を第 1 閾値管理テーブルから読み出し、サーバ 3 について

10

20

30

40

50

接続可否の判断をするときには、サーバ3に対応する第1閾値を第1閾値管理テーブルから読み出す。そして、接続判断部13は、リスクレベル計算部12が計算したリスクレベルRLと読み出した第1閾値とを比較して、接続の条件を満たす場合には接続許可と判断し、条件を満たさない場合には接続拒否と判断する。そして、接続判断部13は、接続を許可した情報端末2あるいはサーバ3について、それぞれのIDと接続日時とを対応させて接続状態管理テーブルへ登録する(ステップ15)。以後、接続制御部14は、接続を許可した情報端末2あるいはサーバ3に対しては接続を許可する制御を行う。

【0058】

続いて、接続制御部14は、情報端末2あるいはサーバ3に対して接続可否の判定結果を送信する(ステップ16)。接続拒否の場合には、この結果に対策方法の情報も含めるものとする。 10

【0059】

情報端末2では、脆弱性検査ソフト21により、接続可否の結果を受信し(ステップ17)、接続拒否の場合には、その対策方法を画面に表示する(ステップ18)。

【0060】

一方で、情報端末2あるいはサーバ3が接続しようとした正のサービスプラットフォームが故障等により応答しない場合には次のように処理する。まず、ステップ11の処理において、情報端末2あるいはサーバ3は、予め登録されている副のサービスプラットフォームへの接続に切り替える。切り替えのタイミングは、例えば、正のサービスプラットフォームが数回の接続要求に対して応答しなかった場合に切り替えるものとする。 20

【0061】

続いて、ステップ12において、副のサービスプラットフォームでは、正のサービスプラットフォームと共有している情報端末2のIPアドレスを用いて、情報端末2から脆弱性検査結果を直接収集し、脆弱性管理テーブルに登録する。以降は、上記ステップ13~18と同様に処理する。

【0062】

[情報端末によるサーバへの接続]

次に、サービスプラットフォームへの接続が許可された情報端末2とサーバ3との間での接続処理について図11、図12のシーケンス図を用いて説明する。図11、図12においても、サービスプラットフォームA(接続制御装置1a)がユーザの情報端末2による接続を管理し、サービスプラットフォームB(接続制御装置1b)がサービス提供者のサーバ3による接続を管理するものとする。 30

【0063】

まず、情報端末2は、サービスの提供を受けようとするサーバ3への接続を要求する旨を示すサービス接続要求をサービスプラットフォームAに対して送信する(ステップ21)。このサービス接続要求には、サービス毎に割り振られるサービスIDまたはサービスURIが含まれる。

【0064】

このサービス接続要求を受信したサービスプラットフォームAは、接続判断部13により、その要求を解析する(ステップ22)。ここでは、まず、プラットフォームデータベース17を検索して(ステップ23)、情報端末2が接続しようとするサーバ3の所属するプラットフォームを特定する(ステップ24)。 40

【0065】

そして、接続先のサーバが、サービスプラットフォームAの管理下において既に接続が許可されたサーバである場合には、接続ポリシーデータベース16からこのサーバに対応する接続ポリシーを示す第2閾値を取得する。一方、接続先のサーバが、サービスプラットフォームAによる管理下でないサーバの場合には、そのサーバの接続が許可されている他のサービスプラットフォームBへアクセスする。このアクセスでは、情報端末2およびサーバ3のそれぞれのIPアドレスを送信する。すなわち、情報端末2の脆弱性検査結果についてはサービスプラットフォームBへは送らないものとし、またサーバ3へも送られ 50

ることがないようにする。そして、サービスプラットフォーム B から、サーバ 3 への接続に必要な接続ポリシーを示す第 2 閾値を取得する（ステップ 25）。

【0066】

また、サービスプラットフォーム A では、リスクレベル計算部 12 により情報端末 2 のリスクレベルを計算し、メモリに記憶させておく（ステップ 26）。

【0067】

続いて、接続判断部 13 により、メモリから読み出した情報端末のリスクレベルと先に取得した第 2 閾値とを比較して情報端末 2 のサーバ 3 への接続の可否を判定する。

【0068】

この判定結果が接続拒否の場合には、接続制御部 14 は、その判定結果を対策方法の情報も含めて情報端末 2 へ送信する。情報端末 2 では、脆弱性検査ソフト 21 により、接続可否の判定結果を受信し（ステップ 28）、接続拒否の場合には、その対策方法を画面に表示する（ステップ 29）。

10

【0069】

一方、判定結果が接続許可の場合には、接続制御部 14 は、サーバ 3 による接続を管理するサービスプラットフォーム B に対して、サーバ 3 のファイアウォール 32 を制御する要求を送信する（ステップ 30）。サービスプラットフォーム B では、ファイアウォール 32 の設定変更をサーバ 3 へ送信し（ステップ 31）、サーバ 3 では、情報端末 2 による接続を許可するように、ファイアウォール 32 の動作を制御するためのアクセスリストを変更する（ステップ 32, 33）。

20

【0070】

この後、サービスプラットフォーム B では、サーバ 3 から応答完了の通知を受け、接続制御部 14 により、サービスプラットフォーム B においてもアクセスリストを変更する（ステップ 34）。サービスプラットフォーム A では、ユーザの情報端末 2 に対して許可通知を送信する（ステップ 35）。情報端末 2 では、サーバ 3 への接続処理を開始する（ステップ 36）。サーバ 3 は、情報端末 2 に対してネットワーク 4 を介したサービスの提供を開始する。

【0071】

このときの情報端末 2 とサーバ 3 間の通信では、情報端末 2 がネットワーク 4 を介してサーバ 3 と直接通信するようにしてもよいし、サービスプラットフォーム A, B を介して通信するようにしてもよい。また、情報端末 2 とサーバ 3 間での通信をリダイレクトによって行うようにしてもよいし、情報端末 2 に対して何らかのトークンを配布するようにしてもよい。

30

【0072】

なお、上記の各ステップ 21 ~ 36 は、情報端末 2 あるいはサーバ 3 が副のサービスプラットフォームに接続した場合も同様に行う。これを実現するために、正、副のサービスプラットフォームでは、情報端末 2 およびサーバ 3 によるサービスプラットフォームへの接続の許可状態を示す情報と、情報端末 2 によるサーバ 3 への接続に必要な接続ポリシーを示す第 2 閾値とを共有しておく。これにより、副のサービスプラットフォームにおいても、接続判断部 13 によって、情報端末 2 が接続しようとするサーバ 3 が当該サービスプラットフォームによって接続が許可されたサーバである場合には接続ポリシーデータベースから第 2 閾値を取得し、当該サービスプラットフォームによる管理下でないサーバの場合には当該サーバの接続が許可された他のサービスプラットフォームへアクセスして当該サーバへの接続に必要な接続ポリシーを示す第 2 閾値を取得することを可能にする。

40

【0073】

以上、説明したように、本実施の形態によれば、ユーザの情報端末 2 とサービス提供者のサーバ 3 のそれぞれについて、脆弱性レベルに基づいてリスクレベルを計算し、このリスクレベルと接続制御装置 1 への接続に必要な接続ポリシーを示す第 1 閾値とを比較して接続制御装置 1 への接続の可否を判断することで、リスクレベルが第 1 閾値による条件を満たさない情報端末 2 あるいはサーバ 3 については接続制御装置 1 への接続を拒否する。

50

これにより、セキュリティレベルの低い情報端末 2 あるいはサーバ 3 が接続されることによる被害の発生を防止することができる。

【0074】

本実施の形態によれば、サービス提供者のサーバ 3 への接続に必要な接続ポリシーを示す第 2 閾値を接続制御装置 1 に登録しておき、ユーザの情報端末 2 のリスクレベルと第 2 閾値とを比較してサーバ 3 への接続の可否を判断することで、リスクレベルが第 2 閾値の条件を満たさない情報端末 2 についてはサーバ 3 への接続を拒否する。これにより、セキュリティレベルの低い情報端末 2 がサーバ 3 に接続した場合に起こり得る不正アクセスやなりすましといった被害を防止することができる。

【0075】

本実施の形態によれば、複数の接続制御装置 1 a - 1 c を設け、情報端末 2 が接続しようとするサーバ 3 が、その情報端末 2 が接続中の接続制御装置 1 a による管理下にない場合には、接続制御装置 1 a によりそのサーバ 3 の接続が許可された他の接続制御装置 1 b へアクセスしてサーバ 3 への接続に必要な接続ポリシーを示す第 2 閾値を取得し、これを用いて情報端末 2 のサーバ 3 への接続の可否を判断することで、ユーザの情報端末 2 は、接続中の接続制御装置 1 a 以外の接続制御装置 1 b が管理するサーバ 3 によるサービスの提供を受けることができる。また、サービス提供者側で情報端末 2 からの接続の可否を判断することを不要にできる。

【0076】

本実施の形態によれば、情報端末 2 およびサーバ 3 において、正、副の二つの接続制御装置に関する情報を記憶しておき、正の接続制御装置への接続に際して応答がなかった場合に、副の接続制御装置への接続に切り替えることで、接続先である接続制御装置に故障等が発生した場合でも、情報端末 2、サーバ 3 は、他の接続制御装置へ接続することができる。

【0077】

本実施の形態によれば、正、副の二つの接続制御装置が、情報端末 2 およびサーバ 3 による接続制御装置への接続の許可状態を示す情報と、情報端末 2 によるサーバ 3 への接続に必要な接続ポリシーを示す第 2 閾値とを共有することで、副の接続制御装置においても、接続判断部 1 3 によって、情報端末 2 が接続しようとするサーバ 3 が当該接続制御装置による管理下にあつて接続が許可されたサーバである場合には接続ポリシーデータベース 1 6 から第 2 閾値を取得し、当該接続制御装置による管理下にないサーバの場合には当該サーバの接続が許可された他の接続制御装置へアクセスして当該サーバへの接続に必要な接続ポリシーを示す第 2 閾値を取得することが可能になり、情報端末 2 はサービス提供者のサーバ 3 へ接続して、サービスの提供を受けることができる。

【0078】

本実施の形態によれば、脆弱性レベルの大きい状態が長く続く程、セキュリティレベルが低いということができることから、脆弱性レベルと経過時間との積の総和をもってリスクレベルを定義することで、接続可否の判断をより正確にすることができる。なお、リスクレベルについて精度が要求されない場合には、脆弱性レベルと経過時間との積に代えて、脆弱性レベルそのものを用いても良い。

【0079】

本実施の形態によれば、接続先のサーバが接続制御装置 1 a による管理下にないサーバの場合に、そのサーバの接続が許可されている他の接続制御装置 1 b へアクセスする際に、必要最小限の情報、すなわち情報端末 2 およびサーバ 3 のそれぞれの IP アドレスを送信することで、情報端末 2 の脆弱性検査結果については他の接続制御装置 1 b やサーバ 3 へ送られることがないので、情報端末 2 のセキュリティ状態に関わる情報の漏洩を防止することができる。

【図面の簡単な説明】

【0080】

【図 1】一実施の形態におけるネットワーク接続制御システムの構成を示すブロック図で

10

20

30

40

50

ある。

【図 2】脆弱性管理テーブルを示す図である。

【図 3】脆弱性マスタテーブルを示す図である。

【図 4】第 1 閾値管理テーブルを示す図である。

【図 5】第 2 閾値管理テーブルを示す図である。

【図 6】接続ポリシー管理テーブルを示す図である。

【図 7】接続状態管理テーブルを示す図である。

【図 8】サービスプラットフォーム管理テーブルを示す図である。

【図 9】情報端末において脆弱性を検査する際の処理の流れを示すシーケンス図である。

【図 10】情報端末が接続制御装置へ接続する際の処理の流れを示すシーケンス図である 10

。

【図 11】情報端末がサーバへ接続する際の処理の流れを示すシーケンス図である。

【図 12】情報端末がサーバへ接続する際の処理の流れの続きを示すシーケンス図である

。

【符号の説明】

【0081】

1 a - 1 c ... 接続制御装置 (サービスプラットフォーム)

2 ... ユーザの情報端末

3 ... サービス提供者のサーバ

4 ... ネットワーク 20

1 1 ... 脆弱性検査管理部

1 2 ... リスクレベル計算部

1 3 ... 接続判断部

1 4 ... 接続制御部

1 5 ... セキュリティ管理データベース

1 6 ... 接続ポリシーデータベース

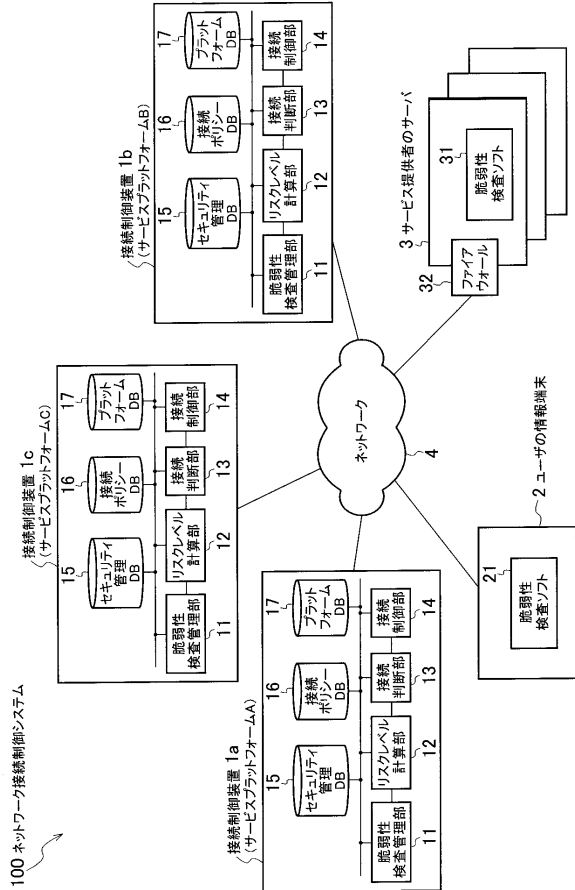
1 7 ... プラットフォームデータベース

2 1 , 3 1 ... 脆弱性検査ソフト

3 2 ... ファイアウォール

1 0 0 ... ネットワーク接続制御システム 30

【 図 1 】



【 図 2 】

情報端末ID・サーバID	脆弱性ID	発見日時	対処日時
A001	5	2005/2/21 13:00	2005/2/25 10:00
A001	6	2005/2/23 18:00	
...			
A004	6	2005/2/10 10:00	2005/2/25 10:00
...			

【 図 3 】

脆弱性ID	脆弱性名称	脆弱性レベル
1	No-AntiVirus-Software-Installed	中
2	Password-Never-Expires	低
3	MDAC-Buffer-Overflow	高
...		

【 図 4 】

	接続ポリシー	第1閾値
情報端末	B	----
サーバ	A	----

【 図 6 】

サービスID	接続ポリシー	サービスURI	ファイアウォールアドレス	サービスプロトコル
1	B	https://www....	10.0.10.20	HTTPS
2	C	ftp://ftp....	10.0.10.20	FTP
:				
4	D	http://www....	192.168.0.20	HTTP
:				

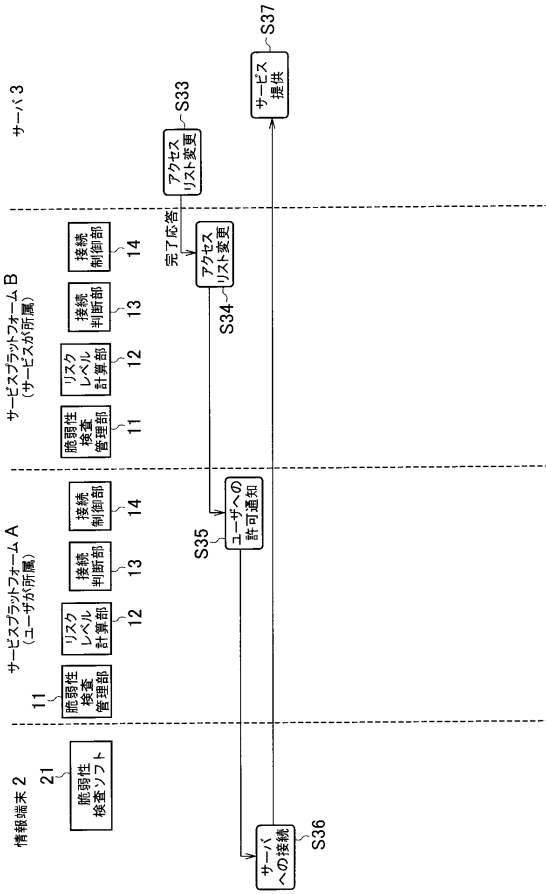
【 図 5 】

接続ポリシー	第2閾値
A	----
B	----
C	----
D	----
----	----

【 図 7 】

情報端末ID・サーバID	接続日時
18	2005/2/21 13:00
104	2005/2/21 13:00
:	
10	2005/2/21 13:00
:	

【図 12】



フロントページの続き

(72)発明者 細木 正司

東京都千代田区内幸町一丁目1番6号 エヌ・ティ・ティ・コミュニケーションズ株式会社内

Fターム(参考) 5K030 GA15 HA08 HC01 HD03 JT02 LC13 LD20 MA01 MA04