

(19) 日本国特許庁 (JP)

(12) 特 許 公 報 (B2)

(11) 特許番号

特許第4927361号
(P4927361)

(45) 発行日 平成24年5月9日 (2012.5.9)

(24) 登録日 平成24年2月17日 (2012.2.17)

(51) Int.Cl.	F I
G06F 21/20 (2006.01)	G06F 21/20 131A
H04L 12/66 (2006.01)	G06F 21/20 133
H04L 9/32 (2006.01)	H04L 12/66 B
	H04L 9/00 675Z

請求項の数 17 (全 14 頁)

(21) 出願番号	特願2005-232768 (P2005-232768)	(73) 特許権者	500310339
(22) 出願日	平成17年8月11日 (2005.8.11)		アバイア インコーポレーテッド
(65) 公開番号	特開2006-53923 (P2006-53923A)		アメリカ合衆国、07920 ニュージャ
(43) 公開日	平成18年2月23日 (2006.2.23)		ーシー、バスキング リッジ、マウント
審査請求日	平成18年11月30日 (2006.11.30)		エアリー ロード 211
(31) 優先権主張番号	10/915,330	(74) 代理人	100094112
(32) 優先日	平成16年8月11日 (2004.8.11)		弁理士 岡部 譲
(33) 優先権主張国	米国 (US)	(74) 代理人	100064447
			弁理士 岡部 正夫
		(74) 代理人	100085176
			弁理士 加藤 伸晃
		(74) 代理人	100106703
			弁理士 産形 和央
		(74) 代理人	100096943
			弁理士 白井 伸一

最終頁に続く

(54) 【発明の名称】 ネットワーク・アクセスを制御するシステムおよび方法

(57) 【特許請求の範囲】

【請求項 1】

ネットワーク・アクセスを制御するシステムであって、

第1の事業体の業務管理下で、少なくとも1つの装置に接続されるセキュリティ機器と、
第2の事業体の業務管理下の、ユーザ端末によりアクセスされる製品接続プラットフォーム及び該ユーザ端末とを含み、1つの信頼関係が、該第1の事業体と該第2の事業体の各々の身元を表す証明書又は公的鍵／私的鍵を取り交わすことで、該第1の事業体と該第2の事業体との間で確立され、該第2の事業体が該第1の事業体にユーザの身元証明情報を送った後にのみ、該第1の事業体は、該ユーザ端末のユーザが該第1の事業体の複数の装置のうちの1つにアクセスすることを可能とすることができ、

該第2の事業体の該ユーザ端末の該ユーザによる、該第1の事業体の該装置へのアクセスの認証は、該信頼関係に基づいて、該第2の事業体の該製品接続プラットフォームの判断にゆだねられ、

該第2の事業体の該製品接続プラットフォームが該ユーザを認証し、該第1の事業体にユーザの身元証明情報を送った後に、該第1の事業体でローカルな認証データベースに対してこのリモート・ユーザの身元をチェックする代わりに、該第1の事業体の該セキュリティ機器は、該第1の事業体と該第2の事業体との間で該信頼関係が確立されているか否かを判定するために該証明書又は公的鍵／私的鍵を使用して該第2の事業体の身元をチ

10

20

ェックすることで、到来する接続が既知の信頼されたシステムから由来することを確認し、そして、該ユーザの身元証明情報に基づいて、該ユーザの身元及び関連する役割をチェックし、該関連する役割が特定の役割に適合する場合には、該第1の事業体の該セキュリティ機器は、該第2の事業体の該ユーザ端末の該ユーザによる該第1の事業体の装置へのアクセスを許可するネットワーク・アクセスを制御するシステム

【請求項2】

該セキュリティ機器と該製品接続プラットフォームとが互いに隔てられ、安全なネットワーク接続により接続可能であり、アクセスが許可された場合、該ユーザが該安全な接続を介して該装置にアクセスする、請求項1に記載のネットワーク・アクセスを制御するシステム。

10

【請求項3】

該セキュリティ機器が、該第2の事業体の身元を確認するために与えられる認証情報を確認し、権限委任要求ドキュメントをポリシー・サーバに送る第1のSOCKSサーバと、該第1の事業体によって定義されたアクセス規則を、該権限委任要求ドキュメントによって与えられる情報に適用するポリシー・サーバ、及び該第1のSOCKSサーバによって提供されたすべての情報を記憶する製品アクセス監査ログとを含む、請求項1に記載のネットワーク・アクセスを制御するシステム。

【請求項4】

該製品接続プラットフォームが、該第1の事業体の該セキュリティ機器内の該第1のSOCKSサーバとの安全な接続を確立し、該第2の事業体の認証情報、ユーザの身元証明情報、アクセスされる装置、及び機能する障害チケットを含むすべての関連する情報を含む該権限委任要求ドキュメントを送る第2のSOCKSサーバを含む、請求項1に記載のネットワーク・アクセスを制御するシステム。

20

【請求項5】

該第2の事業体の該ユーザを認証する認証サーバと障害チケットを発行する障害管理システムとが該製品接続プラットフォームに接続された、請求項1に記載のネットワーク・アクセスを制御するシステム。

【請求項6】

該製品接続プラットフォームが、障害チケット番号、該装置の認識票及び該ユーザの役割を含む、アクセス要求を発行する、請求項1に記載のネットワーク・アクセスを制御するシステム。

30

【請求項7】

該第1の事業体と該第2の事業体とが同じである、請求項1に記載のネットワーク・アクセスを制御するシステム。

【請求項8】

該ポリシー・サーバが、該装置へのアクセスがリアルタイムの権限委任を必要とすることを指定する、請求項3に記載のネットワーク・アクセスを制御するシステム。

【請求項9】

ネットワーク・アクセスを制御するシステムであって、

第1の事業体の業務管理下で、複数の装置に接続されるセキュリティ機器と、

40

第2の事業体の業務管理下の、ユーザ端末とを含み、

1つの信頼関係が、該第1の事業体と該第2の事業体の各々の身元を表す証明書又は公的鍵／私的鍵を取り交わすことで、該第1の事業体と該第2の事業体との間で確立され、該第2の事業体が該第1の事業体にユーザの身元証明情報送った後にのみ、該第1の事業体は、該第2の事業体のユーザが該第1の事業体の該複数の装置のうちの1つにアクセスすることを可能とすることができ、

該第2の事業体のユーザ端末のユーザによる、該第1の事業体の該装置へのアクセスの認証が、該信頼関係に基づいて、該第2の事業体の該ユーザ端末の判断にゆだねられ、

該第2の事業体の製品接続プラットフォームが該ユーザを認証し、該第1の事業体にユーザの身元証明情報を送った後に、該第1の事業体でローカルな認証データベースに対し

50

て個々のリモート・ユーザの身元をチェックする代わりに、該第1の事業体の該セキュリティ機器は、該第1の事業体と該第2の事業体との間で該信頼関係が確立されているか否かを判定するために該証明書又は公的鍵／私的鍵を使用して該第2の事業体の身元をチェックすることで、到来する接続が既知の信頼されたシステムから由来することを確認し、該ユーザの身元証明情報に基づいて、該ユーザの身元及び関連する役割をチェックし、該関連する役割が特定の役割に適合する場合には、該第1の事業体の該セキュリティ機器は、該第2の事業体の該ユーザ端末の該ユーザによる該第1の事業体の装置へのアクセスを許可するネットワーク・アクセスを制御するシステム。

【請求項10】

該ユーザ端末が該セキュリティ機器と通信するためのSOCKSソフトウェアを備える、請求項9に記載のネットワーク・アクセスを制御するシステム。

10

【請求項11】

該セキュリティ機器が、第1のSOCKSサーバと、ポリシー・サーバ及び製品アクセス監査ログを含む、請求項9に記載のネットワーク・アクセスを制御するシステム。

【請求項12】

該ユーザ端末が、障害チケット番号、該装置の認識票及び該ユーザの役割を含む、アクセス要求を発行する、請求項9に記載のネットワーク・アクセスを制御するシステム。

【請求項13】

該ポリシー・サーバが、該装置へのアクセスがリアルタイムの権限委任を必要とすることを指定する、請求項11に記載のネットワーク・アクセスを制御するシステム。

20

【請求項14】

ネットワーク・アクセスを制御する方法であって、

第1の事業体と第2の事業体の各々の身元を表す証明書又は公的鍵／私的鍵を取り交わすことで、該第1の事業体と該第2の事業体の間に1つの信頼関係を確立するステップと

、
ユーザ端末を該第2の事業体の制御下に置くステップと、

該第2の事業体の製品接続プラットフォームで該ユーザ端末のユーザの身元を認証するステップと、

該第2の事業体のユーザが該第1の事業体の装置へのアクセスを要求するステップと、

該第1の事業体でローカルな認証データベースに対して個々のリモート・ユーザの身元をチェックする代わりに、該第1の事業体と該第2の事業体との間で該信頼関係が確立されているか否かを判定するために該証明書又は公的鍵／私的鍵を使用して、該第1の事業体のセキュリティ機器において、該第2の事業体の身元をチェックすることで、到来する接続が既知の信頼されたシステムから由来することを確認するステップと、

30

該第1の事業体で該ユーザの身元を保証する情報をチェックすることで、該ユーザが該第1の事業体の装置にアクセスすることを禁止されていないことを確認するステップと、

該第1の事業体の装置への該第2の事業体のユーザによるアクセスを提供するステップからなるネットワーク・アクセスを制御する方法。

【請求項15】

該第1の事業体のセキュリティ機器に、アクセス要求を生成して送信するステップをさらに含む、請求項14に記載のネットワーク・アクセスを制御する方法。

40

【請求項16】

SOCKSサーバに安全なネットワーク接続のアクセス要求を送信するステップをさらに含む、請求項14に記載のネットワーク・アクセスを制御する方法。

【請求項17】

リアルタイム・ベースで認証を許可するステップをさらに含む、請求項14に記載のネットワーク・アクセスを制御する方法。

【発明の詳細な説明】

【技術分野】

50

【0001】

本発明は、ネットワーク・アクセスを制御するシステムおよび方法に関する。

【背景技術】

【0002】

近年、様々な規模の公的機関や私企業が、遠距離通信システム、情報システムおよび日常のビジネス業務用の作業インフラストラクチャとして機能するその他の製品の大規模アレイを、ますます備えてきている。

【0003】

しかしながらそれらの製品、システムおよびサービスのプロバイダは、彼らの顧客のシステムおよび装置の試験を行い、アップグレードし、かつ維持するために、アクセスと認証図式の統合に関する課題を抱えてきた。特にこれらのプロバイダおよびサービス会社は、彼らの顧客により用いられる多数のリモート・アクセスの要求と異なるリモート・アクセスおよび権限委任パッケージに応じることは困難であることが判ってきた。さらに、顧客の拡張されたユーザ・ベースにより用いられる、製品やシステムへのリモート・アクセスを必要とする、全ての第三者機関の技術者、ビジネス・パートナーおよびアウト・ソースを管理することは、コストと資源に関わる課題である。

10

【0004】

企業の顧客は一般的に、確認し、制御し、ユーザにログするための、彼らのサイトに配置された認証／権限委任／管理（AAA）サーバを有する。

AAAサーバは、

20

- ・ 認証：ユーザの特定および認識の処理、
- ・ 権限委任：あるユーザができることの決定、
- ・ 管理：あるユーザがしていることおよびしてきたことの記録動作、

を提供する。

【0005】

図1は、代表的な顧客ネットワーク環境での、従来の認証／権限委任／管理（AAA）サーバ50を示す。図1はまた、顧客VPNゲートウェイ51および製品52、53（例えば、PBX）を示す。

【0006】

サービス・プロバイダ技術者によるアクセスは、インターネットを経由してアクセス装置40により実行される。従来、ユーザの認証を要求する顧客は、サービス・プロバイダの技術者に、彼らの仮想プライベート・ネットワーク（VPN）クライアント（図示せず）および保証IDのような彼らのハード・トークンの使用を要求する。数人のサービス技術者しか有さないサービス・プロバイダにとって、これは実行可能なオプションである。しかしながら、数百または数千の技術者を有するプロバイダにとっては、これは殆ど不可能である。

30

【0007】

・ 各々のサービス技術者は、全ての顧客のVPNクライアントを彼らのPC上にインストールする必要がある。VPNクライアントは一般的にPCのTCP/IPスタックを変更するので、サービス・プロバイダのPCはもはや適切には機能しない。

40

【0008】

・ 各々のサービス技術者は、全てのサービスを受けている顧客の数百またはできれば数千のハード・トークンを管理する必要がある。これは、プロバイダと顧客の双方にとって管理不能になる。顧客がこの可能性について尋ねられると、彼らはよりよい解決法が必要であることに同意する。

【0009】

・ 認証の前に、サービス・プロバイダが障害チケットまたは作業チケットを公表するように、との要望はない。

【0010】

RSAセキュリティ社およびイオンネットワーク社のような、ハードおよびソフトのト

50

ークン・ベースのリモート・アクセス制御の解決法を提供する、多数の会社がある。この解決法は、彼ら自身の装置にアクセスする単一の会社に関しては、うまく動作する。外注のまたは第三者の保守の局面においては、これは、顧客のアクセス制御システムに設定され、個々のハードまたはソフトのトークンを割り当てられた、全てが第三者の技術者であることを含む、完全な拡張された技術者の力を必要とする。外部の保守会社にとって、各々の顧客に対する各々の技術者用のハード・トークン装置と連絡を絶やさないとの要望は、コストと保守の重大な問題である。

【0011】

パーメオ技術社 (Permeo Technologies, Inc.) のような会社は、認証とリモート・アクセス制御の解決法の装置に、ターンキィ・デスクトップを提案する。この解決法は、彼ら自身の装置にアクセスする単一の会社については、うまく動作する。これは、全てのリモート・ユーザが全く同じソフトウェアのセットを購入して用いることと、顧客のアクセス制御システムに設定された、全てが第三者の技術者であることを含む、完全に拡張された技術者の力を必要とする。全ての顧客が選択したターンキィの解決法に必要とされる、全ての種々の構成およびソフトウェアを個々の技術者に提供することは実現可能でないで、これは第三者管理会社とコストにとっては重荷である。

【0012】

リバティ・アライアンスおよびセキュリティ・アサーション・マークアップ (ダッシュ抜き) 言語 (SAML) 機関は、ウェブ・ベースのビジネス作業用の、信用ベースの身元確認および認証交換標準を開発中である。この標準化の努力は、ウェブ・ベースのビジネス取引およびその用途に、完全に焦点を当てている。リモート・メンテナンス監視およびサポートのためのプロトコルおよびそのアクセス要求は、アプリケーションへのウェブ・ベースのアクセスを遙かに超えている。

【0013】

ソックス (SOCKS) インターネット・コメント要請 (RFC1928、3089、1929) は、プロキシ・サービスを用いるネットワーク装置へのアクセスを確立する、プロトコルを提供する。プロキシ・サービスは、プロキシの背後の装置に対し、アクセスと権限委任制御を実施することができる。現在の標準は、クライアントのアプリケーションとプロキシの協定に基づいて、追加の権限委任モデルが設定されることを可能にするために、一般セキュリティ・サービス・アプリケーション・プログラミング・インターフェイス (GSSAPI) へのサポートと同様に、ユーザIDおよびパスワード・ベースの権限委任制御の使用をカバーする。

【0014】

これらについてのさらなる情報は、以下に記載されている：

・ ネットグリティ役割管理：

<http://www.netegrity.com/news/webseminararchive/rolesarchive.html>

・ パーメオ社 (Permeo Technologies, Inc.) 外向けアクセス：
<http://www.permeo.com/outboundaccess.htm>

・ イオン・ネットワーク・セキュア・リモート・アクセス：
<http://www.ion-networks.com/prisms.shtml>

上記の問題が与えられた時に前進するために必要なものは、三つのAAA機能を分離して、認証はサービス・プロバイダのサイトで、ユーザの身元確認とそれに関連する役割はアクセスが要求された時に顧客のサイトにパスする手段である。認証と管理は、その後顧客のサイトで実行される。

【発明の開示】

【発明が解決しようとする課題】

【0015】

本発明は、主たる目的として、背景技術のシステムおよびアプローチを改良すること、

10

20

30

40

50

および背景技術のシステムに関連する欠点を解決することを有する。

【0016】

ここに提案される解決法は、二つの会社の間の外用の信頼関係に基づく、認証モデルを含むためのSOCKSトンネリングの概念を拡張することである。この信頼関係は、証明書を用いて実装される。

【0017】

SOCKSトンネリングは、SOCKSクライアント・アプリケーションの代わりに、あるSOCKSサーバがある装置へのプロキシ接続を確立するために、他のSOCKSサーバに接触することである。SOCKSトンネリングに対しては、現在のところインターネット標準は存在しない。

10

【0018】

権限委任モデルは、会社Aがそれ自身の従業員を認証するために会社Bを信用するような、二つの会社の間の予め確立された信頼関係に基づいている。会社Aは、会社Bから隔てられたリモート・ユーザを認証することを企図していない。その代わりに会社Aは、会社Bの従業員によりなされた任意のリモート・アクセス要求を権限委任する。この権限委任は、そのリモート・アクセス要求の一部として安全なチャンネルを通して送信された、身元情報のセットに基づいている。

【0019】

作業においては二つの会社は、それらの会社の身元を表す、証明書または公的／私的鍵の組を最初に交換する。証明書は、リモート・アクセス要求がなされた場合に、各々の会社の身元を確立するために用いられる。それはまた、その要求を作成したリモート・ユーザの身元を交換するために、安全な通信機構を確立するためにも用いられる。

20

【0020】

本発明の他の目的およびさらなる適用範囲は、以下に与えられる詳細な説明から明らかになるであろう。しかしながら、本発明の望ましい実施形態を示す一方で、詳細な説明および特定の実施例は一例としてのみ与えられるので、この詳細な説明から本発明の精神と範囲内の種々の変形および修正が当業者には自明であることが、理解されなければならない。

【0021】

本発明は、以下に示される詳細な記述と、一例としてのみ添付された本発明の限定ではない図面により、さらに完全に理解されるであろう。

30

【課題を解決するための手段】

【0022】

本発明は、従来のシステムおよびアプローチとは全く異なる、権限委任モデルを提供する。

この権限委任モデルは、会社A（例えば顧客）が会社B（例えばサービス・プロバイダ）に、会社Bのシステムが全ての関係する従業員の身元証明を会社Aに送った後にのみ、会社Aの装置の一つにアクセスする権限を会社Aが委任するようにされた、二つの会社の間の予め確立された信頼関係に基づいている。

【0023】

40

顧客Aは、図2に示される工程を実装することにより、二つの会社の間の信頼関係を最初に確立する。当該二つの会社の間に信頼関係が一度確立されると、会社Bによるリモート・アクセスができるようになる。

【発明を実施するための最良の形態】

【0024】

図3(a)に示されるように会社Aの環境は、SOCKSサーバ5、ポリシー・サーバ6および製品アクセス監査証跡装置7からなる、ローカル・ゲートウェイSSG10を含む。製品8（例えばPBX）は、ローカル・ゲートウェイSSG10に接続されている。

【0025】

会社Bのシステムは、SOCKSサーバ4、AAAシステム2および障害チケット・シ

50

システム 1 を備える、製品接続システム 3 を含む。

作業において二つの会社は、各々の会社の身元を表す、証明書または公的鍵／私的鍵の組を最初に取り交わす。証明書は、到来する要請が信頼されるシステムに由来することを確認するために用いられる。この取り交わしは、図 3 (a) に示される会社 A と B の環境について、また図 3 (b) に示されるメッセージのシーケンスについて図示される。再確認すると、会社 A は音声 P B X スイッチのような、リモートでサービス可能なある製品のユーザであり、会社 B はこのシステムのサービス・プロバイダである。ローカルな認証データ・ベースに対し個々のリモート・ユーザの身元をチェックする代わりに、到来する接続が既知で信頼されるシステムに由来することを確認するために、ローカル・ゲートウェイ S S G 1 0 は会社の証明書または保証書をチェックする。個々のユーザの情報は、ローカル・ゲートウェイ S S G 1 0 により検査できる暗号化されたパケットの一部として送信され、個々のユーザの身元と他の関連する情報は S S G 1 0 により記録される。

10

【 0 0 2 6 】

ここで図 3 (b) を参照すると、会社 B の技術者 (ユーザ) が会社 A のネットワーク上の製品 8 に接続しようと企てる場合、以下の工程が発生する。

工程 1 : 会社 B の技術者は、端末 4 0 を経由して障害チケット・システム 1 にログインする。

工程 2 : 技術者は、会社 B の A A A サービス 2 により認証される。

工程 3 : 技術者は、障害チケット・システム 1 からサービスするチケットを選択する。

工程 4 : 会社 B の技術者は、チケット内で参照される製品 8 への接続を要求する。

20

工程 5 : 障害チケット・システム 1 は、製品接続システム 3 をコールし、接続を要求する。

工程 6 : 製品接続システム 3 は、その技術者が当該の接続を許可されるべき適宜の権限委任を有するかどうかを決定するために、会社 B の A A A システム (2) にコンタクトする。

工程 7 : 権限委任が許可されたと仮定すると、製品接続システム 3 は会社 B の S O C K S サーバ 4 にコンタクトし、会社 A のリモート製品 8 への接続を要求する。技術者の身元と障害チケット番号が、製品 8 の特定情報と共に S O C K S サーバ 4 に送信される。

工程 8 : 会社 B の S O C K S サーバ 4 は、ローカル・ゲートウェイ S S G 1 0 内で稼働中の、会社 A の S O C K S サーバ 5 との安全な接続を生成し、会社 B の保証書、技術者の身元、アクセスされる製品および作業される障害チケットを含む全ての関連する情報を包含する、権限委任要求ドキュメント 9 を送信する。

30

工程 9 : 会社 A の S O C K S サーバ 5 は、会社 B の任意の身元を有効にするために供給される保証書を有効にする。

工程 1 0 : 会社 A の S O C K S サーバ 5 は、処理のためにこれまたローカル・ゲートウェイ S S G 1 0 で稼働中の、ポリシー・サーバ 6 にアクセス要求ドキュメントを送信する。

工程 1 1 : ポリシー・サーバ 6 は、顧客が定義した任意のアクセス規則を、アクセス要求ドキュメント 9 の名前 (name?) で供給される情報に適用する。ポリシー・サーバ 6 は、特定の顧客の従業員による現場でのリアルタイムの権限委任を必要とする、特定の装置へのアクセスを指定する。ローカル・ゲートウェイ S S G 1 0 は次に、その製品にアクセスするための権限委任を承認するために、これらの特定の顧客の従業員を通知する、顧客のインスタント・メッセージ・サーバ 1 1 にアクセスする。S S G 1 0 は、リアルタイムの権限委任のために、顧客の従業員に特定のアクセス属性 (故障チケット番号、製品の説明書、会社および従業員がアクセスする製品) を表す。一人またはそれ以上の顧客の従業員は、アクセスを「許可」または「拒否」することができる。顧客の従業員の誰かが、顧客が指定した時間内に「拒否」と言った場合は、アクセスは拒否される。拒否の理由は、顧客のインスタント・メッセージ・クライアントを用いて提供されることができる。顧客の従業員全員が「許可」と言った場合には、アクセスは許可される。所望のアクセス・ポリシーを提供するために、他のセキュリティ・パラメータがプログラムされてもよい

40

50

。

【0027】

本発明は以上に記述したような、リアルタイム警報のインスタント・メッセージの型式に限定されない。リアルタイムの権限委任への代替案の解決法は、標準の番号パッドを備えるディスプレイ電話14を用いて顧客と交信する、SIP（セッション起動プロトコル）サーバ13（図3（a）に示される）を用いる。ここでSSGのポリシー・サーバ6は、例えばサービス・プロバイダの技術者名、故障チケット情報および／またはアクセスを要求する装置を表すために、顧客のディスプレイ電話14をコールし、次にアクセス情報を送る。顧客は、許可のために「1」を、拒否のために「2」を押す。SSG10は管理する装置毎に、顧客がプログラムしたアクセス・ポリシーを記憶している。

10

【0028】

供給元のアクセスを許可するために顧客が用いる装置は、電話またはインスタント・メッセージ・サービスに限定されない。電話のような無線装置、パーソナル・デジタル・アシスタント、ブラック・ベリー（<http://www.blackberry.com>）装置、任意のローカルまたはリモート通信クライアントが、本発明に含まれる。

【0029】

工程12：SOCKSサーバ5は、SSG10に配置された会社Aの監査ログ7に、全ての情報を記録する。

工程13：権限委任が許可されたと仮定すると、SOCKSサーバ5は製品8への接続を公開する。その後制御は、技術者に戻される。SOCKSサーバ5は、ローカル装置にアドレスするために必要な、ネットワーク・アドレス変換を実行する。

20

【0030】

認証機能と処理

認証機能は、顧客のサイトとはリモートに配置された、サービス・プロバイダのサービス配送プラットフォームと、顧客の構内またはその近くに配置された、ローカル・ゲートウェイ／セキュリティ機器SSGの、二つの個別のプラットフォームの相互作用により提供される。SSGは、サービス・プロバイダではなく、顧客により制御され、監視される。

。

【0031】

サービス・プロバイダは、サービス技術者の顧客のサイトへの任意のアクセスが許可される前に、サービス技術者が認証されることを保証しなければならない。この認証処理は、また各々の個々の技術者にサービスする「役割」を割り当てる。ある役割は、顧客の装置またはシステムの特定の一部に、サービスを提供するための個々のサービス技術者の「免許」と考えられることができる。

30

【0032】

例えば生成された障害チケットの結果としてアクセスが必要になると、最初にアクセス要求が顧客とは隔たったセキュリティ機器（SSG）と交渉される。

アクセス要求は、以下のような属性を含む。

- ・サービス会社名
- ・技術者名、役割、アドレス
- ・技術者の管理者名、アドレスおよび電話番号
- ・アクセスされる製品
- ・障害チケット番号
- ・要求された現場での承認
- ・それらのネットワークに、サービス・プロバイダへのアクセス許可を与えた現場の担当の、電話番号、インスタント・メッセージ名またはIPアドレス

40

【0033】

- ・サービス・プロバイダの社内処理ID

SSGは顧客により、特定の役割を有する技術者が彼らの装置およびネットワークにアクセスできるようにされている。サービス技術者によるアクセス要求は、SSGに安全に

50

送られ、SSG内に記憶されたアクセス・ポリシーと比較される。役割が適合すると、ユーザの身元およびアクセス要求内のその他全ての情報がSSGの監査ログに記憶される。アクセス要求はまた、ネットワーク・マネジメント・システム、またはそれらにリアルタイムのアクセス通知を与えるシスログ・サーバに、SSGにより送信されることができる。以上に記述したように、アクセスはユーザの身元ではなく役割に対して与えられるが、ユーザの身元も説明責任のために同様に記録される。

【0034】

認証機能および処理はまた、顧客が身元パケット内の他の情報について規則を構築できるようにしてもよい。例えば、特定のサービス技術者（または他のユーザ）が彼らのネットワークにアクセスできないようにする、顧客が「名前による拒否」ができる規則を作ることができる。これは、特定のサービス技術者またはユーザについての、顧客の過去の経験の結果であってもよい。この機能を提供するためには、サービス会社BはSSGに全ての彼らの技術者名を送信する必要はない。むしろSSGは、製品へのアクセスの通常処理中に、身元パケットで通過した名前を記憶する。この自動的な名前リストの作成は、除外リストの基礎となる。SSG監査ログを裁判解析に用いて、顧客は除外すべき人物を決定する。顧客は次に、その名前を除外リストにコピーする。その人物が次にどんな製品にアクセスしようとしても、SSGはその人物によるどんな製品へのアクセスも拒否する。SSGはまた、拒否の理由を記述したSOCKS接続要求内の拒否メッセージを、会社BのSOCKSサーバに返送する。

【0035】

このようにして、認証機能は顧客が定義した権限委任チェックを許可する。

さらに認証機能は、「要求された現場での承認」権限委任モデルを可能にすることができる。例えばある顧客は、彼らのサイトに接続するのに先だって、サービス・プロバイダがリアルタイムのアクセス許可を得ることを必要とするかもしれない。このエントリーは、顧客のサイトのSSGにパスされる。SSGセキュリティ・ポリシーは、外部の通知サービス（以前に記述）を経由して、その技術者（名前による）がその製品にアクセスすることを許可するのに先立って、顧客の権限委任を求めるインスタント・メッセージ、ビーパまたはEメールのようなメッセージを送信する。SSGは、顧客がそのアクセスを許可するか否か決定できるように、サポートするアクセス情報を提供する。顧客の代理人がSSGに承認を一度与えると、そのサービス技術者によるアクセスが許可される。SSGは後刻の顧客の監査のために、全ての許可および拒否されたアクセス要求を記録する。これは、あるベンダによりなされたアクセスが結果として、他の顧客のサーバにサービス停止やセキュリティ攻撃を起こした場合に重要である。この記録は、それを引き起こしたベンダ、技術者またはベンダの自動化ツールを指定することを助ける。

【0036】

権限委任機能と処理

権限委任は、ユーザのアクセスが割り当てられたリソースにのみであることを保証する処理である。これは、通常、認証段階の後で行われる。

【0037】

最初に、VPNクライアントについての簡潔な記述が提供される。VPN接続処理では、あるネットワークまたはIPアドレスにのみアクセスするように、VPNクライアントが顧客のVPNサーバによりリモートで作成される。リモートPCのIPパラメーターが、リモートネットワーク上のリソースにアクセスして使用するために、変更される。全ての実際的な目的のために、リモートPCはそのPCのローカルLAN上のリソースにはアクセスできない。そのPCは、論理的には顧客のネットワーク上に存在する。

【0038】

LAN接続へのVPNクライアントの代わりにLAN-LAN接続が用いられた場合、二つの異なるIPネットワークへの橋渡しのために、ネットワーク・アドレス変換（NAT）が必要になるのでこれは重要である。顧客のAAAサーバが許可された本当のIPアドレスを含む場合、アクセスがなされる前に、SSGはAAAサーバからそれらを回収し

、次にそれらをサービス・プロバイダの内部アドレスにマップする必要がある。

この処理を簡便化するために、SSGはネットワーク・アドレス変換(NAT)と権限委任および管理機能の双方を実行する。

【0039】

管理機能および処理

管理は、全ての認証および権限委任工程が完了した後に、SSG内で実行される。

その顧客が管理に用いられる外部AAAサーバ(例えば、ポート1813を用いる、リモート認証ダイヤル・イン・ユーザ・サーバ(RADIUS)システム)を有する場合は、SSGは顧客のサーバにアクセス要求/結果を記録することができる。これは、一つのサーバ内の全てのアクセス要求の監査を可能にする。

10

【0040】

自動化リモート・アクセス・システム

以上に記述された処理は、サービス技術者により起動される。代替案としてシステムは、一般的に診断コンピュータにより起動される、自動化リモート・アクセスを提供するために用いられてもよい。

【0041】

自動化システム・リモート・アクセスの際のメッセージ・フローは、以下の例外を除き、リモート技術者によるアクセスと同様である。会社Bの各々の自動化システムはそれ自身の固有の身元を有し、この身元はサービス・プロバイダのシステムにより確認され、次に顧客のシステムに提供される。SSGに送信された身元は技術者のそれではなく、診断コンピュータのそれなので、これは非常に重要である。障害チケット・システム1にアクセスする代わりに、自動化システム・リモート・アクセス・アプリケーションは、適切なチケット情報を供給する製品接続システム3に直接アクセスする。

20

【0042】

ローカル技術者によるアクセス

ローカル技術者によるアクセスの際の、システムの構成要素の間のメッセージ・フローは、図4(a)の矢印により示されている。図4(b)は、リモート技術者のアクセスの際の、工程のフロー・チャートを提供する。

【0043】

会社Bの技術者によるローカル・アクセスの事前要件は、その技術者のPCがSOCKS化されていなければならないことである。SOCKSソフトウェアは、会社AのSSG1により管理されている製品への全てのトラフィックを、SOCKSサーバ2にリダイレクトするようにされていなければならない。SOCKS化されたクライアントとSOCKSサーバの間のプロトコルは、SSGへの安全なローカル・アクセスを維持するために、SSLを用いて暗号化されている

30

関連する工程は、以下を含んでいる：

工程1：ローカル技術者が、ローカルSSG1上で稼働中のSOCKSサーバ2に接続する。

工程2：SOCKSサーバ2は、顧客のAAAサーバ4に対して技術者の情報を認証する。

40

工程3：技術者は、ローカル・ネットワーク・アドレスを用いて製品5への接続を生成しようとする。

工程4：SOCKSサーバ2は、製品5にアクセスするための権限委任を求めて顧客のAAAサーバ4をチェックする。

工程5：SOCKSサーバ2は、SSG1のローカル監査ログ3内の接続要求を記録する。

工程6：SOCKSサーバ2は、製品5への接続を開放し、会社Aのローカル技術者に制御を戻す。

【0044】

以上に記述した本発明は、従来技術の審判アプローチの問題への、安全で統合された解

50

決法を提供する。この解決法の利点は、以下を含む：

サービス・プロバイダが、顧客のアクセス制御システムに全ての第三者の技術者の身元を維持することは、もはや不必要である。

各々の第三者の保守、監視または支援ベンダのそれぞれが、各々の全ての顧客が彼らの装置にアクセスするために要求する、ソフトウェアまたはハード・トークンを有することは不必要である。

【0045】

安全、監査手続および立法を充足するために必要な情報は、サービス会社とその装置を用いる顧客の双方により安全な方法で維持される。

【0046】

サービス・プロバイダまたは顧客のどちらかによる甚大な作業を必要とすることなく、非常に個別的なアクセス制御規則の構築が可能となる。交換される身元情報は、リモートの保守、監視または支援の顧客が彼ら自身の装置にアクセスするための個別的で詳細なアクセス制御記録を、サービス・プロバイダに重荷を負わずことなく構築できるようにするのに充分である。

【0047】

他の固有の利点は、以下を含む：

- ・権限委任はサービス・プロバイダのサイトではなく、むしろ顧客のサイトで起こる。
- ・顧客のサイトへのIPアクセスを可能にする、障害／作業チケットが最初に生成されなければならない。サービス・プロバイダのサイトに配置されたSSGは、顧客のサイトへの直接のIPアクセスを妨げる。要求された情報が提供されない場合、アクセスは拒否される。これは、サービス・プロバイダの身元、サービス・プロバイダの技術者の身元および作業される障害チケットを含む。技術者の会社、技術者の身元（または自動化エキスパート・システムの身元）、役割、チケット番号および／または製品IPアドレスおよび「要求された現場での承認」が、権限委任要求ドキュメントを用いて、現場のゲートウェイSSGに安全に送信される。

- ・顧客は現場でのアクセス制御を保持し、その制御のためにサービス・プロバイダを信用する必要がない。

- ・顧客は：

- i. アクセスが許可された時間

- ii. 彼らの製品にアクセスする、許可された技術者の役割

- iii. アクセスが許可された製品

- iv. 彼らの製品へのアクセスが許可されなかった人物（おそらく過去の経験から）および

- v. 「要求された現場での承認」を与えることを許可された人物

など、所望のアクセス制御規則を有するオンサイト・ゲートウェイを予めプログラムする能力を有する。

- ・この解決法はまた、取引を記録する場所として、顧客のAAAデータ・ベースとの統合を可能にする。認証は、サービス・プロバイダのAAAシステムにより実行される。権限委任は、現場のゲートウェイ（SSG）により実行される。管理（記録）は、SSGまたは顧客のAAAサーバにより、オプションとして実行される。

- ・顧客の技術者は、SSGを通してローカルの製品に接続するために、標準SOCKSクライアントを用いることができる。SSGは、製品にアクセスするための単一のゲートウェイになる。

- ・この解決法は、顧客が現有するB2B接続を用いることができる。それは、サービス・プロバイダに個別のVPN／フレーム・リレー接続を必要とさせない。

【0048】

本発明は以上のように記述されたが、これが多様な方法で変形されることが自明であろう。そのような変形は本発明の精神と範囲から逸脱していると見なしてはならず、当業者に自明な全てのそのような変形が、添付の請求項の範囲内に含まれることが企図されてい

10

20

30

40

50

る。

【図面の簡単な説明】

【0049】

【図1】顧客のネットワーク環境の代表例としての、従来技術の認証／権限委任／管理（AAA）サーバを示す図である。

【図2】二つの会社の間の信頼関係の確立に際して起こる、マニュアルの工程のフロー・チャートである。

【図3（a）】顧客のネットワーク環境の代表例としての、本発明の認証／権限委任／管理（AAA）システムを示す図である。

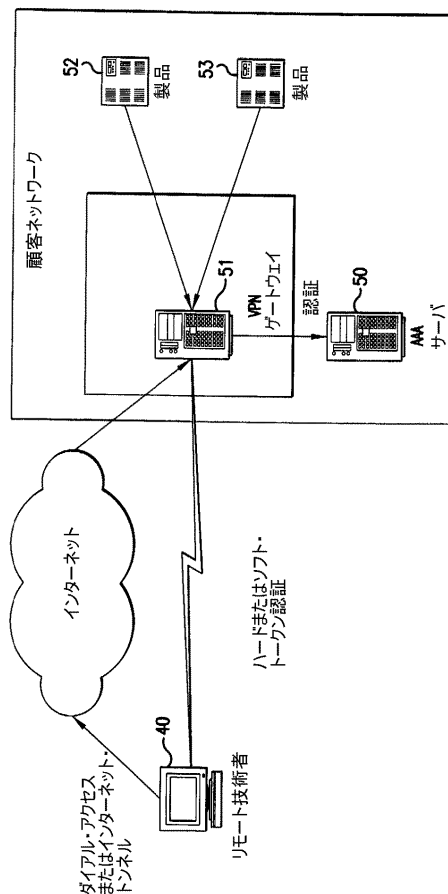
【図3（b）】本発明の主たる利用に関わる工程を強調した、シーケンス図である。

10

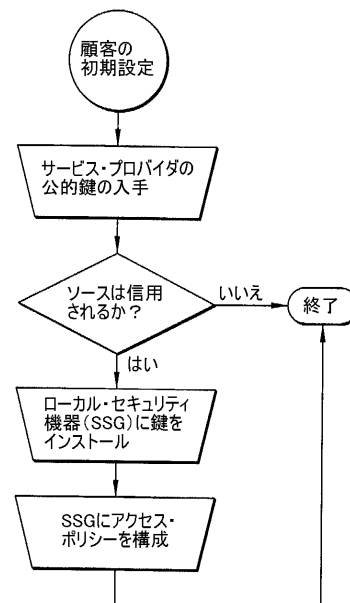
【図4（a）】顧客サイトにいる、サービス技術者用の処理を示す図である。

【図4（b）】本発明の変形に関わる工程を強調した、シーケンス図である。

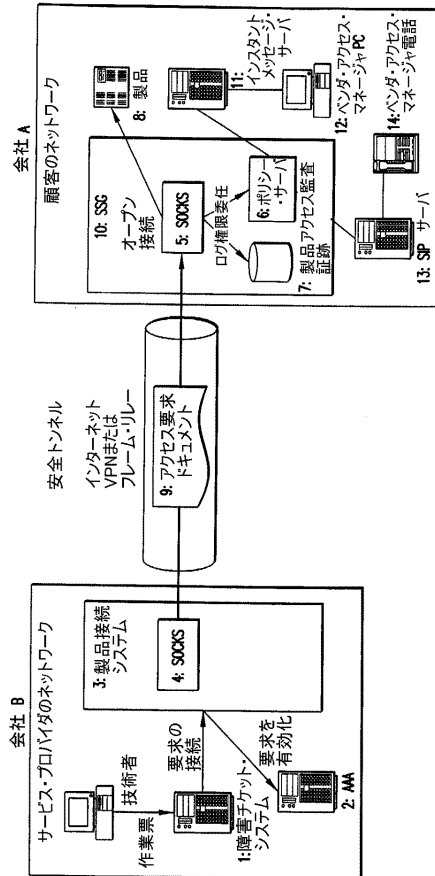
【図1】



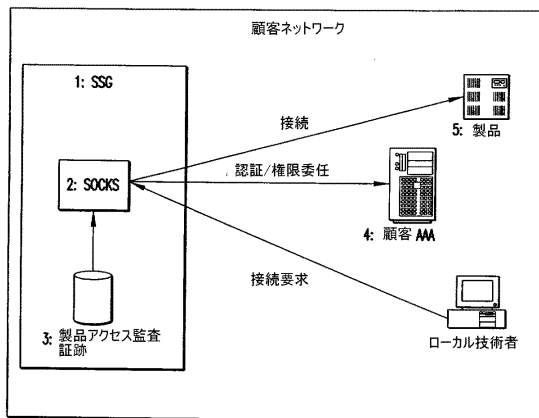
【図2】



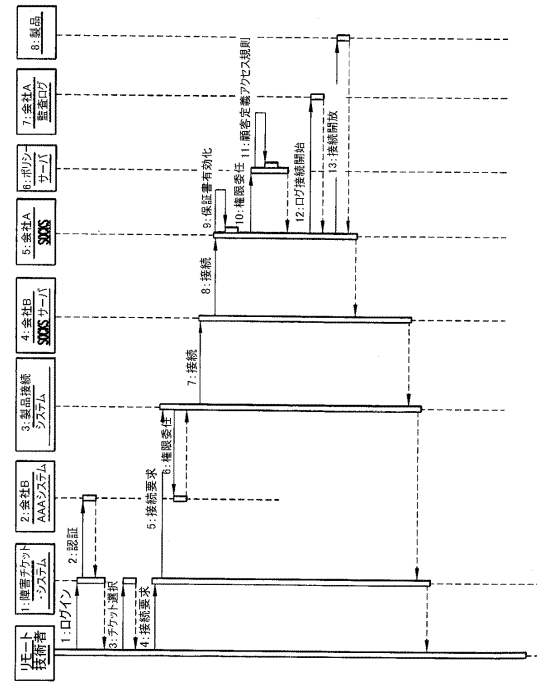
【図 3 (a)】



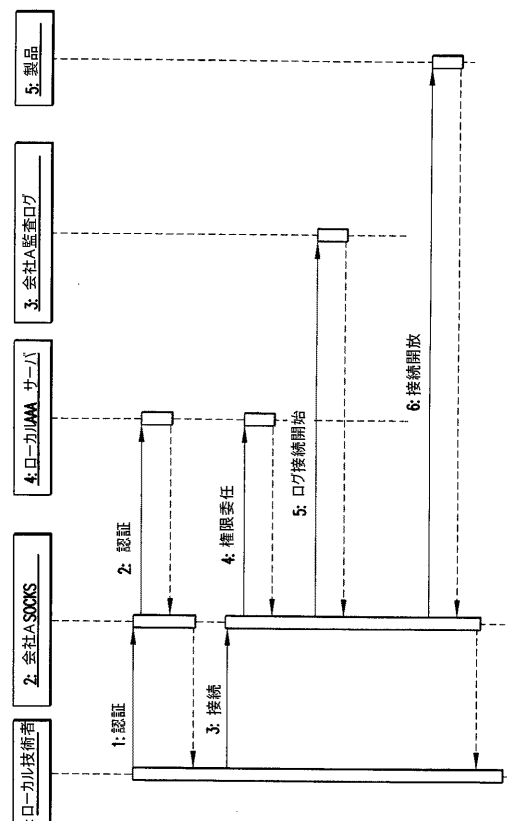
【図 4 (a)】



【図 3 (b)】



【図 4 (b)】



フロントページの続き

- (74)代理人 100101498
弁理士 越智 隆夫
- (74)代理人 100096688
弁理士 本宮 照久
- (74)代理人 100104352
弁理士 朝日 伸光
- (74)代理人 100128657
弁理士 三山 勝巳
- (72)発明者 メーロン オデル クリモンズ ザ セカンド
アメリカ合衆国 75019 テキサス, コペル, ウッドハースト ドライヴ 459
- (72)発明者 サブラタ マズンダー
アメリカ合衆国 07746 ニュージャージー, マールボロ, ケープ メイ ドライヴ 18
- (72)発明者 ロバート アール. シーベル
アメリカ合衆国 08758 ニュージャージー, ウェアータウン, ライトハウス ドライヴ 154
- (72)発明者 ティーケイ スリニヴァス
アメリカ合衆国 07731 ニュージャージー, ハウエル, リバティー コート 11
- (72)発明者 スリラン チテュア ヴィスワナサン
アメリカ合衆国 80234 コロラド, ウェストミンスター, ワン ハンドレット アンド シ
ックスティーンズ アヴェニュー ナンバー 27, 1490 ダブリュ

審査官 田中 慎太郎

- (56)参考文献 特開2001-186186 (JP, A)
及川晴生, ブロードバンドで専用線を作ろう ADSL+VPNを成功させるコツ, NETWORK MAGAZINE, 日本, 株式会社アスキー, 2002年12月 1日, 第7巻第12号, p.145-167
横山哲也, あなたのNTの使い方は間違っている!? NTドメイン、超・整理法., ASCII network PRO, 日本, 株式会社アスキー, 1999年12月 1日, 第4巻第12号, p.162-167

- (58)調査した分野(Int.Cl., DB名)
G06F 21/20
H04L 9/32
H04L 12/66