

IPCOM L シリーズ 認証機能

Authentication Functionality of the IPCOM L Series

北井彦久 *
Hikohisa Kitai

中村美樹 *
Yoshiki Nakamura

* ソフト・アプライアンスグループ アプライアンス事業部 第一開発部

企業における情報セキュリティ対策の一つである内部ウイルス感染からのシステム保護のため、ネットワークの入口での保護セキュリティ技術として、ネットワーク利用者を接続時に認証する技術について、当社と富士通で共同開発している IPCOM L シリーズを中心に説明し、連携する Systemwalker Desktop Inspection^{※1)} や Safeauthor についても言及する。

With focus on the IPCOM L series that was jointly developed by PFU and Fujitsu Limited, this paper describes the technology of network user authentication at the time of connection. This technology serves as a security protection technique at the network entrance that protects the system against virus infection from inside, which is one of the targets of information security measures for corporations. References are also made to Systemwalker Desktop Inspection and Safeauthor that operate in conjunction with the IPCOM L series.

1 まえがき

ネットワークは企業のビジネスに必要不可欠な存在である一方で、ネットワークを経由した外部からの不正アクセスやウイルス感染パソコンの持ち込みによる大規模ウイルス感染が社会問題にまで及んでいる。ネットワークセキュリティは、業務の妨害・機会損失などの直接的な被害だけでなく、顧客情報の漏洩などで企業の信用が失墜するなど、企業経営の危機管理対象として重要な対策となっている。

このような背景から各企業では、ファイアウォールの設置やサーバ・パソコンへのセキュリティパッチの適用などの対策が取られてきているが、ウイルス・セキュリティホールの発見から対応までの間に被害が拡大するケースが増えてきており、これまでの対策だけでは企業システムを守る事が困難となってきた。

企業ネットワークでの深刻なセキュリティ問題は、アクセス LAN に持ち込み PC を接続した場合に、一気にバックボーンネットワークを経由しネットワーク全体にウイルスや攻撃が蔓延することである。そのため、企業ネットワークにおけるセキュリティ対策として、エ

ンドポイントセキュリティが大切である。ここで言うエンドポイントセキュリティとは、表-1に示すように基本対策の他3つの対策レベルで構成され、エンドポイント(クライアント等が接続されるシステムの末端)で守るセキュリティ対策である。

基本対策は、PC 自体への対策としてのパーソナルファイアウォールや暗号化である。レベル1は、ネットワークにつながると最初に必ず認証サーバに行かせるしくみである。認証サーバで確実な認証を行い、クリアした PC だけをネットワークに接続させる。レベル2は、対策チェックサーバを導入して、PC に必要なセキュリ

表-1 エンドポイントセキュリティ対策

区分	対 策 内 容
基本対策	パーソナルファイアウォールや暗号化を PC に施す
レベル1	ネットワークに接続する際にユーザー認証を行う
レベル2	セキュリティチェックにより不適格な PC を排除する
レベル3	資産管理ソフトウェアによりセキュリティパッチやウイルスパターンファイルの更新を強制適用する

ティパッチが適用されているかどうか、ウイルスパターンファイルは最新かなどをチェックして、不適格な PC は排除し、検疫ネットワークへと強制的に誘導する。そこで自分で必要なサイトへ行きセキュリティパッチやウイルスパターンファイルの更新を行う。レベル 3 は、対策チェックサーバで不適格と見なされた場合、自動で最新の状態になるようファイルの更新を行う。

これらのエンドポイントセキュリティ対策を実現するため、当社と富士通で共同開発した IPCOM L シリーズ (図 - 1) は、第 1 ステップとして 2006 年 1 月から Web 認証による不正 PC の接続制限機能を、第 2 ステップとして 2006 年 7 月から IEEE802.1X 認証による不正 PC の接続制限機能を出荷開始した。さらに、当社開発の認証・検疫機能に加え、富士通独自の IDP ((Intrusion Detection and Prevention : 侵入検知・防御) 機能、未知のワーム対策やアプリケーションレベルの遮断機能を統合することで、1 台でイントラネットのセキュリティ課題を解決する。

本稿では、当社開発の IPCOM L シリーズの認証機能に焦点をあて、開発目的と特長、利用事例などを紹介する。

2 開発目的

現在の企業ネットワークでは、エンドポイントセキュリティが重要であることは認識されているが、実際に内部セグメントのセキュリティ確保のために、図 - 2 のように端末認証 (IEEE802.1X 認証) 機能付のスイ

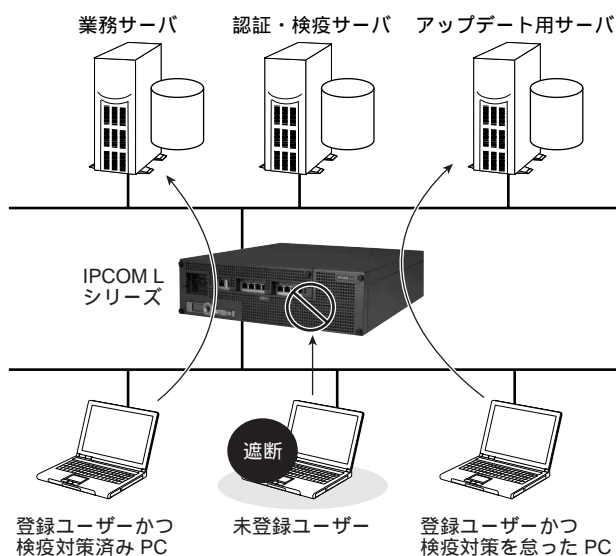


図 1 IPCOM L シリーズ
(Fig.1-IPCOM L series)

チを全体に展開することには経済的な問題がある。

この点を考慮して、IPCOM L シリーズでは、ユーザー毎の認証を安価に実現することを狙いとした二つの導入方法 (Web 認証, IEEE802.1X 認証) を提案する。

(1) Web 認証

Web 認証方式は、Web ブラウザを用いて端末が定められた VLAN に接続できるかどうかの認証を行う機能である。端末へのエージェント配布やインストールが不要のため、各端末に要する運用コストを低く抑えることができる。

(2) IEEE802.1X 認証

IEEE802.1X 認証方式は、ネットワーク機器によるユーザー認証の IEEE 規格である EAP 認証プロトコルを利用し、EAP 上位で動作する各種 EAP 認証方式により認証を行う機能である。IEEE802.1X 認証は一つの物理ポートに一つの認証端末が前提であるが、複数認証端末に対応したマルチサブリカント機能を実現した。この機能によりポートの配下に HUB 等を接続できるため、IPCOM L シリーズの設置を、図 - 3 のように内部セグメントとバックボーン LAN との境界に位置することが可能である。

上記 2 方式は、IPCOM L シリーズを利用すること

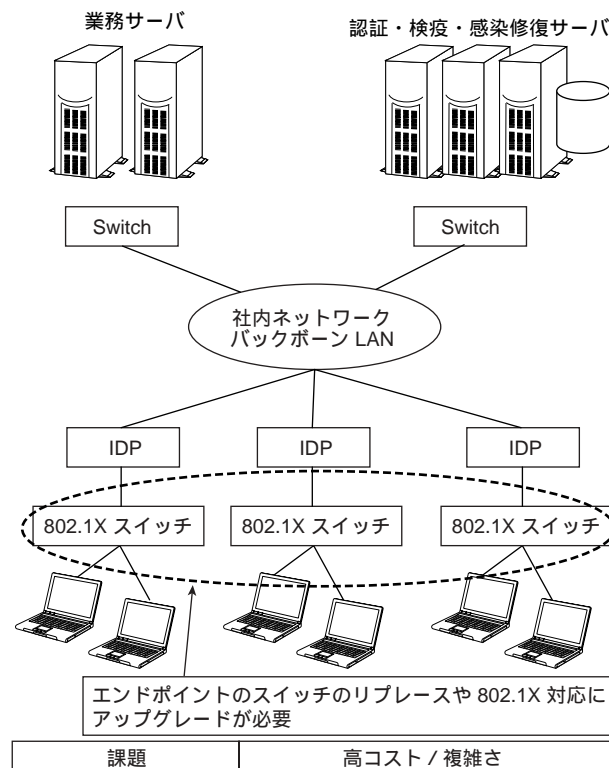


図 2 従来方式
(Fig.2-Conventional method)

る．認証 VLAN は，ユーザー認証と動的 VLAN を組み合わせた技術であり，認証の結果によって，動的にユーザーを特定の VLAN に割り当て，VLAN 間の通信を制御する設定が可能である．

該当 VLAN に対し，ネットワーク管理者があらかじめセキュリティ・ポリシーを設定することにより，図-6のようにユーザーは社内内のどこからアクセスしても，アクセス権限を持つサーバやネットワークを自由に利用することができ，高いモビリティが実現できる．

(4) 検疫サーバ連携による PC セキュリティチェック

IPCOM L シリーズでは認証機能の拡張として，図-7のように検疫サーバ (Systemwalker Desktop Inspection) と連携した検疫ネットワークを構築することができる．検疫ネットワークとは，PC のセキュリティ監査を行い，不合格の PC を隔離するネットワークシステムである．

不合格の PC に対しては，アクセス制限や警告通知をすることができる．IPCOM L シリーズでは，セキュリティ監査に基づくアクセス制御やユーザー名に基づくアクセス制御を行う．

3.2 機能詳細

3.2.1 Web 認証と URL リダイレクト機能

IPCOM L シリーズで Web 認証を行うには，エンドユーザーが認証操作を意識する必要がある．エンドユーザーは，PC 起動後に，必ず Web ブラウザを起動して，自動的に表示される認証画面で認証を行わなければ

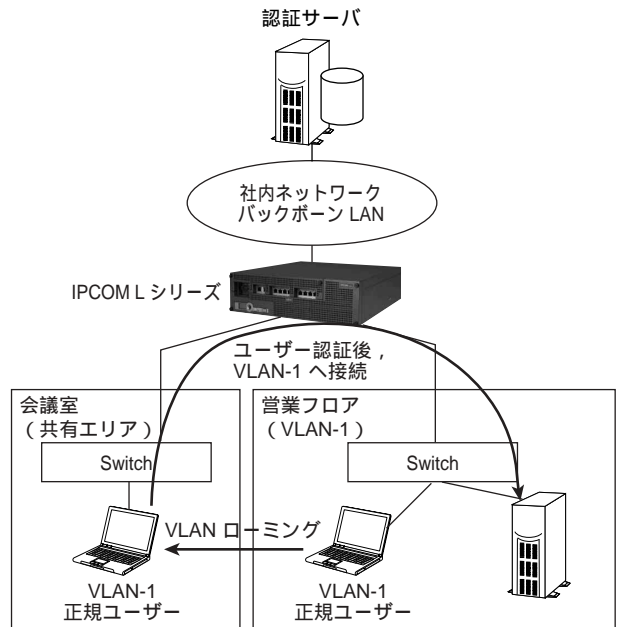
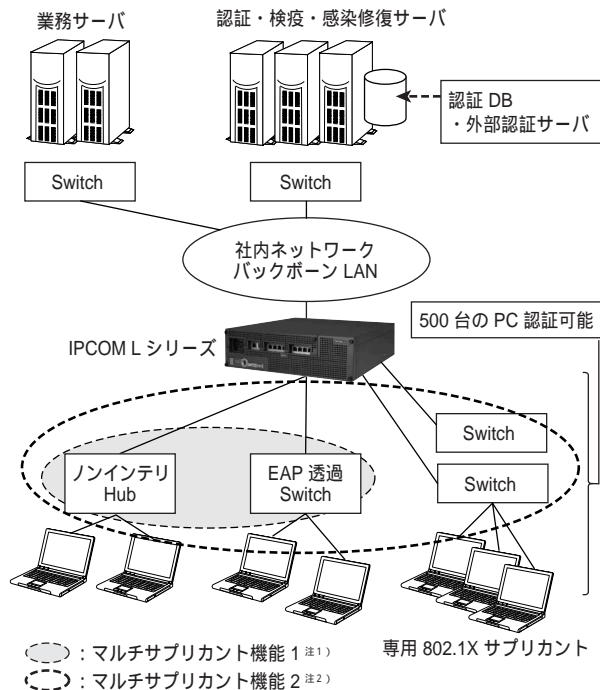


図 6 認証 VLAN (Fig.6-Authentication VLAN)



注 1) 一つの認証スイッチポート配下に複数のエンドユーザーを収容できる．IPCOM L シリーズ配下は EAP 透過なスイッチかノンインテリな Hub.
 注 2) IPCOM L シリーズ配下が EAP 透過な装置以外でも，複数エンドユーザーに対応できる．サブリカントとして，検疫サーバ添付の専用サブリカントを利用する．

図 5 IEEE802.1X 認証 (Fig.5-IEEE802.1X authentication)

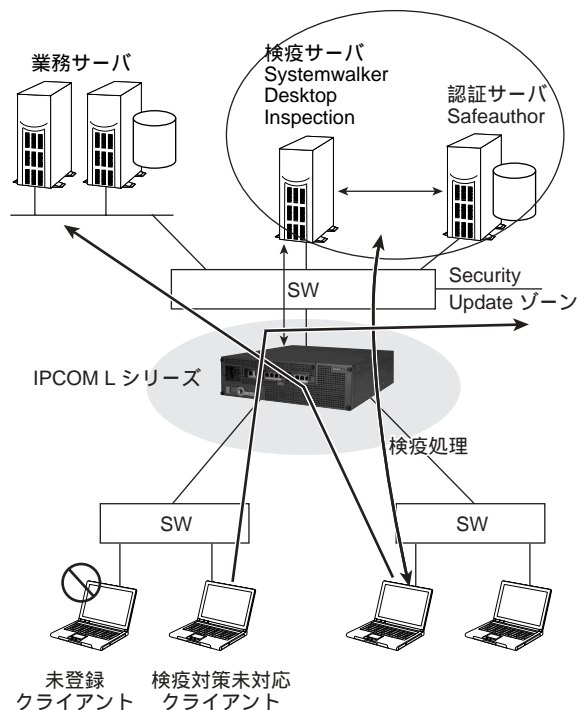


図 7 検疫連携 (Fig.7-Linkage with inspection)

ならない。認証画面では HTTPS を使用することで、ユーザー ID、パスワードなどの盗聴を防止できる。

認証画面は、HTTP/HTTPS アクセス時に自動的に表示されるため、特定の URL にアクセスする必要はない。この自動表示を実現するため、図 - 8 に示す認証シーケンスを実行する。IPCOM L シリーズは、本シーケンスにて Web アクセスに対して別の URL にアクセスし直す URL リダイレクト機能を実装した。

3.2.2 IEEE802.1X 認証とマルチサブリカント

IEEE802.1X 認証は、一つの物理ポートに一つの認証端末が前提であるが、IPCOM L シリーズでは複数端末を認証できるようにマルチサブリカント対応した。ただし、標準的なサブリカントは、IEEE802.1d 準拠の標準的なスイッチで、EAPOL フレームに利用するマルチキャスト宛先をフレーム中継できない。そのため、IEEE802.1X 認証はエンドポイントでの運用となり、内部セグメントとバックボーン LAN との境界に位置する IPCOM L シリーズで利用するためには、標準的なスイッチをノンインテリジェント HUB か、EAP 透過なスイッチに置き換える必要があった。

従来の構成を変更せず、容易な導入を実現するため、802.1X サブリカントと IPCOM L シリーズで独自拡張したマルチサブリカント機能を実現した。図 - 9 に示すように IPCOM L シリーズと 802.1X サブリカント間で、独自のユニキャスト MAC アドレスを用意することで、標準的なスイッチを置き換えることなく、EAPOL フレーム中継を可能にした。

また、標準的な IEEE802.1X 認証はポート VLAN

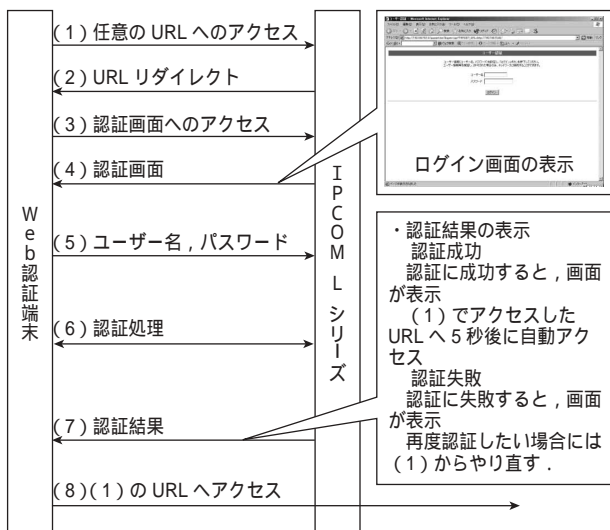


図 8 URL リダイレクト (Fig.8-URL redirection)

を利用しているが、IPCOM L シリーズではタグ VLAN もサポートすることで柔軟なネットワーク設計を可能とした。

3.2.3 認証 VLAN とアクセス制御

IPCOM L シリーズは認証ユーザーに基づいたグループ単位でアクセス制御を行う。具体的には、図 - 10 の (1) 認証サーバ連携にあるように、各ユーザーのユーザーロール^{注2)}を認証サーバの Filter-ID に設定し IPCOM L シリーズでユーザーロール毎のフィルタ設定 (class-map) を行う。また、検疫サーバ連携している場合は、図 - 10 の (2) 検疫サーバ連携にあるように、検疫サーバにユーザーロールを設定し IPCOM L シリーズでユーザーロール毎のフィルタ設定 (class-map) を行う。

3.2.4 検疫サーバ連携とバイオ認証

IEEE802.1X 認証で利用する専用サブリカントは、図 - 11 に示すような構成で SMARTACCESS/Premium と連携することで、バイオ認証装置 (Secure Login Box) を利用した指紋認証、Felica

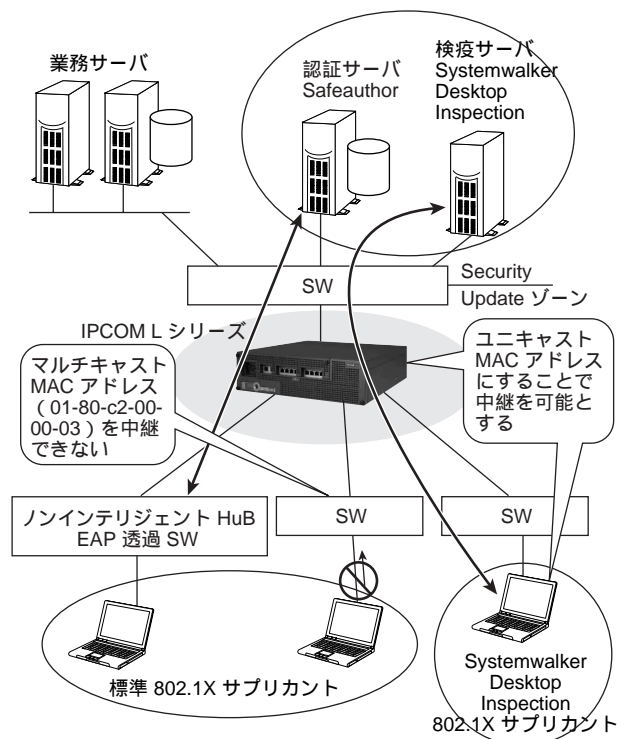


図 9 マルチサブリカント (Fig.9-Multiple-suppllicant feature)

注 2) ユーザーロールとは、定義された共通の役割や権限が付与された抽象的な概念である。認証されたユーザー (または、ユーザーグループ) とアクセス制御ルールなどを論理的に結合する役割を果たす。

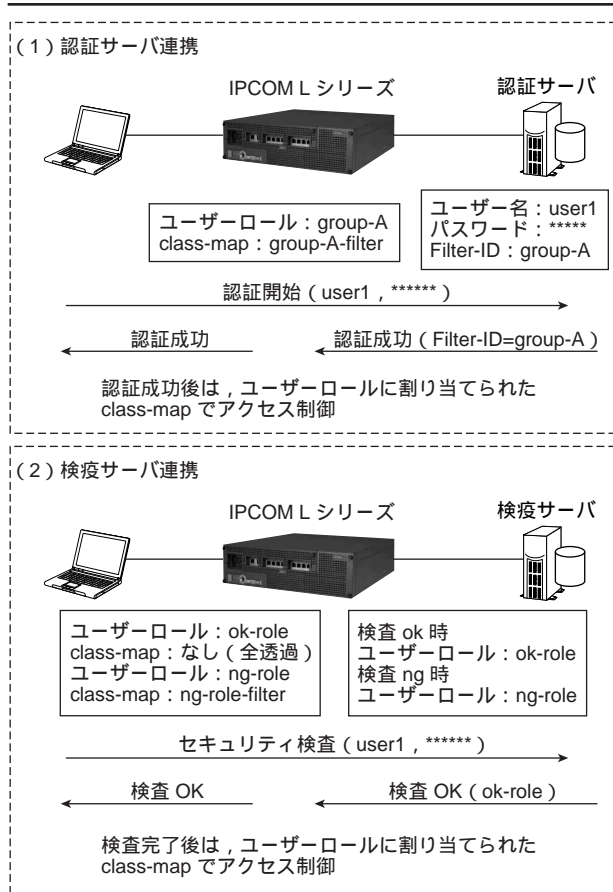


図 10 アクセス制御
(Fig.10-Access control)

カードやスマートカード内のログイン情報を内蔵したセキュリティデバイスを利用した認証に対応する。さらに、ログオン情報を指紋認証で代行することでシングルサインオンを実現する。

4 利用事例

既存ネットワークへの追加設置によりシンプルな導入を可能とする IPCOM L シリーズによるシステム構築例として、以降に既存ネットワークへの追加構築の二つの運用シーンを紹介する。

4.1 Web 認証方式による構築例

(1) 要件と対策

想定する企業ネットワークとして、一般社員と派遣社員、見学者に VLAN ゾーンを分け、それぞれに異なるアクセス制御を設定、全体に不正 PC は接続禁止する例を挙げる。

要件としては、右記を想定する。

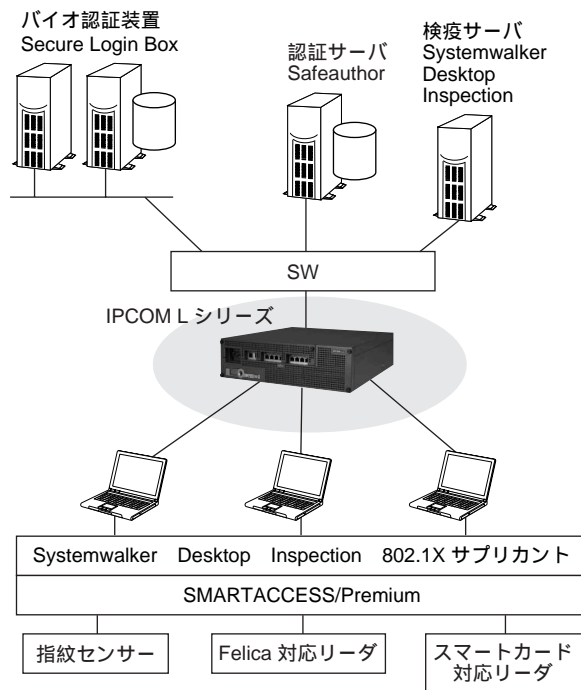


図 11 バイオ認証
(Fig.11-Bio-authentication)

- 1) ソフトウェア配布したくない
- 2) アカウントを集中管理したい
- 3) セキュリティポリシーを満たしていない PC は接続させたくない

この要件に対しての対策として、以下を組み合わせる。

- 1) Web 認証方式を採用
- 2) 外部認証サーバとして Safeauthor を採用
- 3) 検査サーバとして Systemwalker Desktop Inspection を採用

(2) 構築例

対策に従い、図 - 12 の構成を作成する。運用手順は、以下の通りである。

クライアントが Web ブラウザを使用し HTTP/HTTPS の接続要求を行った時、IPCOM L シリーズがその接続要求を認証・検査サーバへリダイレクトし強制的に認証 Web 画面を表示する。認証・検査サーバは、認証プロセスでユーザーの接続要求を許可して構わないのかを認証サーバに問い合わせる。

検査プロセスでクライアントの Windows^{注3)}セ

注3) Windows は、米国 Microsoft Corporation の米国およびその他の国における登録商標である。

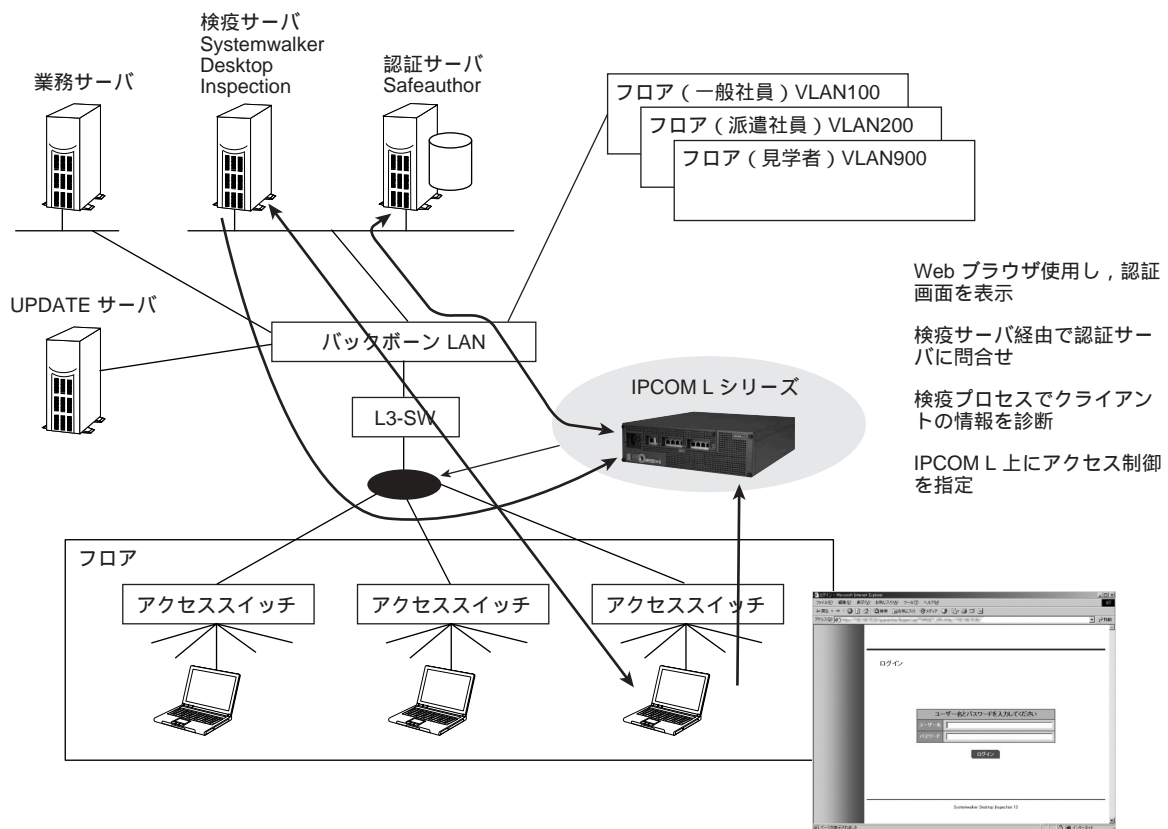


図 12 Web 認証方式による構築例
(Fig.12-Example of development based on the Web authentication method)

セキュリティパッチの適用状況，ウイルス対策ソフトのパターン更新状況を確認する．

認証・検疫プロセスが成功した場合，認証・検疫サーバは IPCOM L シリーズに対してメッセージを送信してそのユーザーがネットワーク上の資源全体もしくは一部に接続することを許可（図では業務サーバ）する．

検疫プロセスだけ NG の場合は，必要のあるサーバだけに接続することを許可（例えば UPDATE 用のサーバのみ）する．

4.2 IEEE802.1X 認証方式による構築例

(1) 要件と対策

想定する企業ネットワークは，4.1 節と同様とする．要件としては，以下を想定する．

- 1) Web 操作等を意識せずに運用したい
- 2) アカウントを集中管理したい
- 3) セキュリティポリシーを満たしていない PC は接続させたくない

この要件に対する対策として，右記を組み合わせる．

- 1) IEEE802.1X 認証方式を採用
- 2) 外部認証サーバとして Safeauthor を採用
- 3) 検疫サーバとして Systemwalker Desktop Inspection を採用

(2) 構築例

対策に従い，図 - 13 の構成を作成する．運用手順は，以下の通りである．

クライアントがネットワークに 802.1X 認証により接続要求を行う（サブリカント自動接続）．

IPCOM L シリーズがその接続要求を受け，EAP 認証プロセスでユーザーの接続要求を許可して構わないのかを認証サーバに問い合わせる．

EAP 認証中に検疫プロセスでクライアントの Windows セキュリティパッチの適用状況，ウイルス対策ソフトのパターン更新状況を確認する．

認証・検疫プロセスが成功した場合，認証・検疫サーバは IPCOM L シリーズに対してメッセージを送信してそのユーザーがネットワーク上の資源全体もしくは一部に接続することを許可（図では業務サーバ）する．

検疫プロセスだけ NG の場合は，必要のあるサ

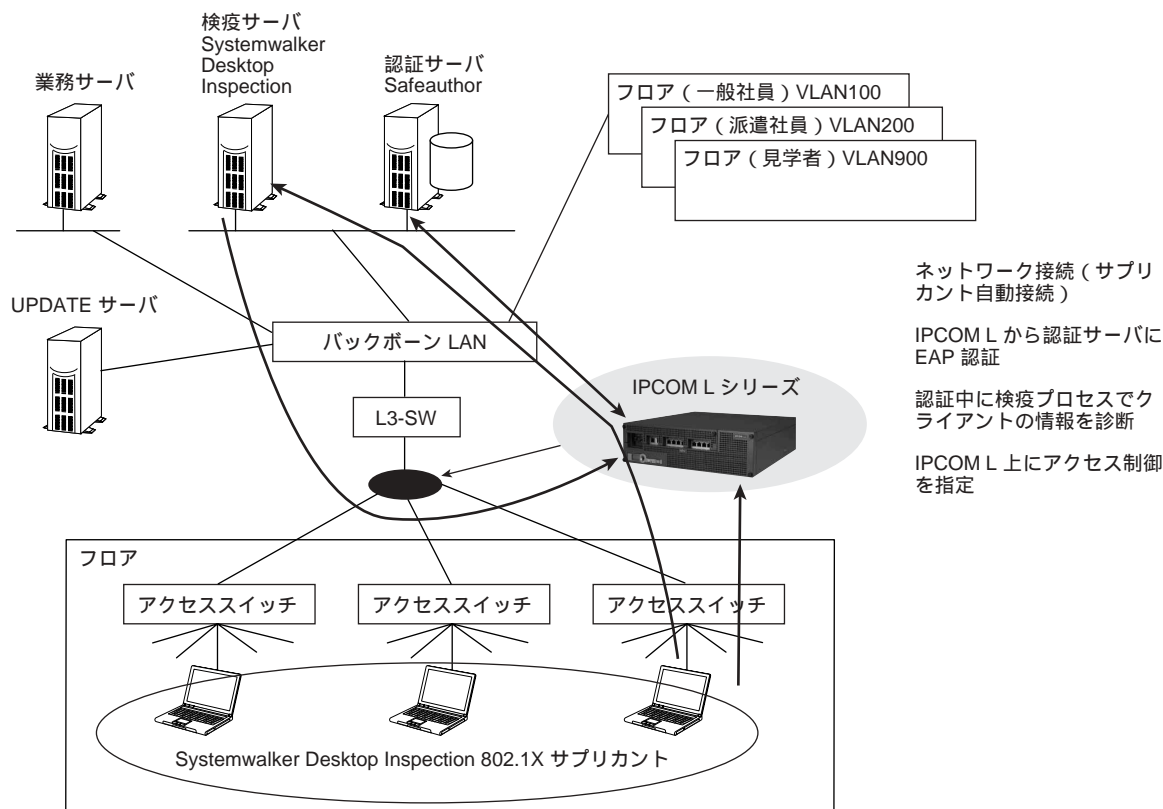


図 13 IEEE802.1 認証方式による構築例
 (Fig.13-Example of development based on the IEEE802.1X authentication method)

サーバだけに接続することを許可 (例えば UPDATE 用のサーバのみ) する。

5 むすび

エンドポイントセキュリティ対応装置として IPCOM L シリーズは認証・検疫機能を提供した。また、他社機に比較した優位性を掲げるために、各種 RADIUS サーバへの対応や認証タイプの拡大などを実現している。

今後、低価格なスイッチにも同等機能が搭載され、

価格・クライアント数から見た適用領域が狭まることが見込まれるため、クライアント数の拡大を主体に、以下の取り組みを進めていく。

- (1) 認証クライアント数の拡大
- (2) 拠点向け製品として、センターアクセス不可時のサーバ代替機能である、RADIUS サーバ / DHCP サーバ / DNS サーバの実装

参考文献

- 参 1) 富士通 Systemwalker Desktop Inspection 紹介ページ
http://systemwalker.fujitsu.com/jp/desktop_inspection/