L-009

バイオメトリクス認証を用いたManaged VLANサービス

Managed VLAN service using biometrics authentication

吉井 英樹† 明石 正則† 村上 誠† 山口 英子† 芦萱 吉喜†
Hideki Yoshii Masanori Akashi Makoto Murakami Eiko Yamaguchi Yoshiki Ashikaya

1. まえがき

近年，ワームやウィルスによるネットワークの被害，顧客情報の流出といった情報漏洩が社会問題となってきている．これらの原因として，企業ネットワークにおけるLAN内部のセキュリティ対策の甘さが指摘されている．

これを解決するために，LAN側が，ユーザや端末を認証し，かつ端末のセキュリティ対策状況に応じてレイヤ2レベルでネットワークアクセスを制御するManaged VLANサービスが考案されている[1,2]．

また，より高い認証レベルを求めて，バイオメトリクスの利用が広がりつつある．これは，入退室などの物理的なセキュリティレベルを上げるためだけでなく，PCログオンやWebベースのサービスへのログオン[3]といったネットワーク上でのセキュリティレベルの向上のためにも利用されている．このバイオメトリクス認証では，モダリティ間，及び方式間の互換性の問題が，普及阻害の一因となっている．この問題を解決するために，OASIS(The Organization for the Advancement of Structured Information Standards)において，XML (eXtensible Markup Language)を用いたバイオメトリクスの共通データ形式としてXCBF(XML Common Biometric Format)が標準化された[4]．

本論文では，このXCBFを用い，バイオメトリクス認証のネットワーク利用をより容易にするバイオメトリクス認証ゲートウェイ（GW）を提案する．さらに，Managed VLANが提供する認証，及びバイオメトリクス認証といった複数の認証手段を用意し，その認証レベルに応じたVLANを割り当てることでネットワークアクセスを制御するという，よりセキュアなネットワーク利用を実現する方法を提案する．

本論文は，2章において，Managed VLANサービスについて，3章において，バイオメトリクス認証GWについて，4章において，バイオメトリクス認証を用いたManaged VLANサービスについて述べる．まとめと今後は5章で述べる．

2. Managed VLANサービス

2.1. サービス要件

Managed VLANサービスのサービス要件を以下に示す．

① ネットワーク管理者が許可していないユーザのネットワークアクセス，及び端末からのネットワークアクセスの拒否
② 適切なセキュリティ対策が施されていない端末からのネットワークアクセスの拒否
③ 管理者がリアルタイムにユーザ端末のネットワークアクセスを制御
④ LANに接続されているユーザ端末の監視
⑤ 広域LAN上での利用

†日本テレコム株式会社

2.2. サービス概要

Managed VLANサービスはIEEE802.1xの利用を前提にしており，Managed VLANサービス=802.1x+αであると言える．このαは大きくふたつの機能からなる．ひとつは，“端末のセキュリティ対策状況に応じた認証機能”であり，もうひとつは，“ユーザ端末の状態に応じてVLAN環境を制御する機能”である．

2.2.1. 端末のセキュリティ対策状況に応じた認証

IEEE802.1xは，LAN内のユーザ認証の方式を定めた規格である．このIEEE802.1xについては，現在，様々な拡張がなされているが，一般に行われているウィルス対策を用いた認証について言及されていない．そのため，サービス要件②を実現するには，別途対策が必要である．そこで，Managed VLANサービスでは，LAN内に少なくとも2つのVLAN(セキュリティ対策用，業務用)を作成し802.1x認証後，まずセキュリティ対策用VLANを割り当て，その後，セキュリティ対策状況を確認し，十分な対策が施されている端末のみ業務用VLANを割り当てるというシステムを開発した[1]．

2.2.2. ユーザ端末の状況に応じたVLAN制御

現在，ウィルス感染端末の業務用ネットワークからの除去，及び隔離にあたって，ネットワーク管理者は非常に大きな労力をかけている．例えば，ウィルスに感染したと思われる端末のIPアドレスを発見した場合，現状ではそのIPアドレスをWeb等でアナウンスし，該当する端末のケーブルを抜く，端末をシャットダウンするといったことが行われている．すなわち，即座にその端末のネットワーク利用を停止する，制限するといったことは行われていない．

Managed VLANでは，不正端末の発見後，即座に該当端末の除去，及び隔離を実現している[2]．ここで，除去とは，該当端末が使用しているスイッチポートのシャットダウン，隔離とは，該当端末が使用しているスイッチポートのVLAN IDの変更を言う．このダイナミックな端末除去，及び隔離を実現するために，Managed VLANでは，現在LANに接続中のユーザID，端末ID(MACアドレス)，ネットワークID(IPアドレス)，VLANID，接続先スイッチ情報(IPアドレス，ポート番号)を，802.1x対応Radiusサーバ やDHCP(Dynamic Host Configuration Protocol)サーバのログ情報，及びL2デバイスのMIB(Management Information Base)情報等から収集し，管理する．これらの情報を基に，ウィルス感染端末の発見時には，ウィルスに感染したIPアドレス等から，該当するスイッチのポートをコントロールすることが可能となる．(無線の場合は，スイッチをアクセスポイントに，ポートをひとつの無線セッションに置き換える．)

3. バイオメトリクス認証ゲートウェイ

バイオメトリクス認証は，顔や指紋などの生体情報を用いて本人確認をするものである[5]．生体情報は，記憶や所有物のように忘却や紛失の心配がなく，偽造が困難で本人との結びつきがより強いことなどから，バイオメトリクス認証はセキュリティと利便性の両面から近年特に注目されている．殊に，9.11 を機に米国を中心にして起こった国境警備強化の動き，空き巣犯罪や金融機関でのなりすまし犯罪の急増，企業による個人情報漏洩事件の多発などによって，我々の生活の身近なところでバイオメトリクス認証システムが導入されてきている．

3.1. バイオメトリクス認証のシステムモデル

バイオメトリクス認証システムは，その照合処理をどこで行うかによって，クライアント認証モデルとサーバ認証モデルに大別できる．

クライアント認証モデルは，生体情報を IC カードや PC 内などのクライアント側で管理し，照合処理もクライアント側で行う．このモデルでは，生体情報の管理をユーザ個人が行うため，システム側のデータ管理負荷が軽減され，サーバ側のコストを低減できるメリットがある．

サーバ認証モデルは，生体情報をサーバ側のデータベースで集中管理し，照合処理もサーバ側で行う．このモデルでは，クライアントには生体情報を取得するセンサさえあれば良く，利用端末や場所を選ばないメリットがある．そのため，いつでも，どこでも，ネットワークにアクセスしてさまざまなサービスを享受するユビキタス環境での利用には，サーバ認証モデルの方が適している．

3.2. 共通データ形式(XCBF)

バイオメトリクス認証は，顔，指紋，虹彩，音声，サインといったモダリティの多様性とともに，同一モダリティであっても，その照合アルゴリズムが開発元によって異なるため，異なる方式間でのデータの互換性はもちろん，データ形式の互換性も無いのが現状である．そのため，複数のモダリティや方式を扱うシステムを構築する際に，生体情報を統一的に扱うことができず，それぞれに応じた個別の開発が必要となるため，非常に効率が悪くシステムが複雑化するという問題がある．そのため，システムインタフェースの統一は重要である．このような問題を解決するために，OASIS において標準化された共通データ形式が XCBF である．

3.3. バイオメトリクス認証ゲートウェイモデル

我々は，XCBF を用いた顔と指紋によるバイオメトリクス認証システムを開発した．図 1にそのシステム構成図を示す．図中，認証 GW はバイオメトリクス認証 GW，認証サーバは顔，及び指紋を用いたバイオメトリクス認証を実施するサーバを表し，認証 DB はユーザ毎に登録された生体情報を保存している．

本システムでは，モダリティ間，及び方式間の互換性の問題を解決し，バイオメトリクス認証のネットワーク利用をより容易にするために，前述のサーバ認証モデルにおいて，クライアントとバイオメトリクス認証サーバの間にバイオメトリクス認証 GW を設けたシステムモデルを採用している．

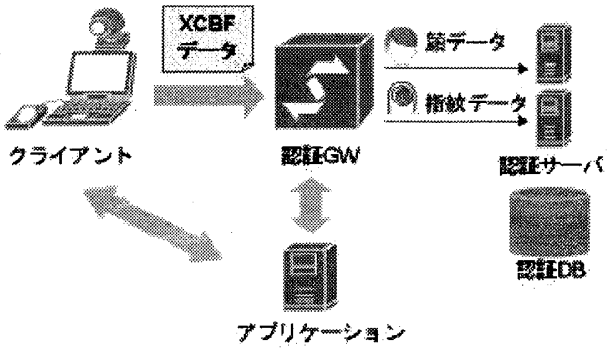

図 1 バイオメトリクス認証 GW モデル

クライアントで取得した生体情報は XCBF 化され，バイオメトリクス認証 GW に送信される．バイオメトリクス認証 GW は，受信した XCBF データを解析し，生体情報に対応した照合エンジンをもつバイオメトリクス認証サーバにデータを送信する．バイオメトリクス認証サーバでは，受信した生体情報をデータベースに登録されているそれと照合して認証を行い，その結果をバイオメトリクス認証 GW に送信する．認証結果が OK であればアプリケーションが提供され，NG であればアクセスは拒否される．

本システムのように，共通データ形式（XCBF）とバイオメトリクス認証 GW モデルを採用することによって，

- モダリティや方式の異なるデータであっても統一的なデータハンドリングが可能であり，マルチバイオメトリクス認証システムの構築が容易になる
- システムの拡張や機能変更が容易になる
- クライアントはバイオメトリクス認証サーバの位置を意識しなくてもよい
- アプリケーションとの連携が一元的にできる

などの効果がある．また，バイオメトリクス認証 GW は，生体情報のデータ形式を XCBF から方式依存の形式に変換することが可能である．そのため，バイオメトリクス認証 GW モデルの採用によって，既存のバイオメトリクス認証システムに変更を加えることなく，他のシステムに組み込むことが可能になる．実際，今回のシステムで利用している顔認証サーバ，及び指紋認証サーバは，XCBF 非対応であるが，バイオメトリクス認証 GW でデータ形式の変換を行うことによって本システムに取り込むことを可能にした．このように，バイオメトリクス認証 GW は，データ形式の差異を吸収する役割も果たす．

これらの効果により，バイオメトリクスを用いた個人認証サービスを提供しようとする事業者にとっては，サービス提供が非常に容易になる．例えば，個人認証サービス提供事業者は，バイオメトリクス認証 GW のみを自社データセンタで管理し，認証サーバはそれを提供する各ベンダの管理下におくことが可能になる．そして，新規に別のモダリティや方式の認証サービスを追加する際にも，その認証処理を提供するベンダの認証サーバに接続するだけでよい．

なお，バイオメトリクス認証 GW は，生体情報のデータそのものには一切関知しない．そのため，クライアントからバイオメトリクス認証 GW に送信される生体情報が，生

データであっても特徴点抽出処理などを施した加工データであっても良い．どのような状態のデータが送受信されるかは，クライアントとバイオメトリクス認証サーバの間でのみ理解できれば良い問題である．

3.4. バイオメトリクス認証 GW の構成

図 2にバイオメトリクス認証 GW システムのコンポーネント図を示す．図中，色付きの部分が今回開発した部分である．

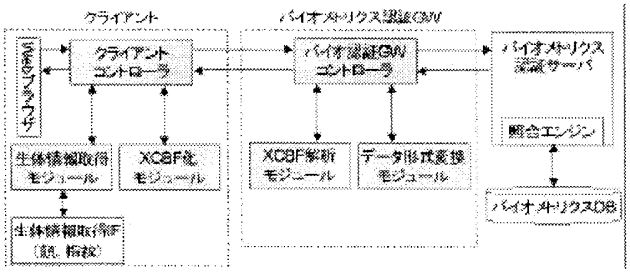

図 2 コンポーネント図

各モジュールの機能は以下に示す通りである．

【クライアント】

- クライアントコントローラ：Web ブラウザからの認証要求を受け，クライアントでの処理全体を司る．
- 生体情報取得モジュール：クライアントコントローラからの依頼を受け，既存の生体情報取得 IF を介して顔または指紋の生体情報を取得する．
- XCBF 化モジュール：生体情報取得モジュールが取得した顔または指紋の生体情報を XCBF 化する．

【バイオメトリクス認証 GW】

- バイオメトリクス認証 GW コントローラ：クライアントからの認証要求を受け，バイオメトリクス認証 GW での処理全体を司る．
- XCBF 解析モジュール：受信した XCBF データを解析し，モダリティ情報などから，このデータを送信すべきバイオメトリクス認証サーバを決定する．
- データ形式変換モジュール：受信した XCBF データを，送信先のバイオメトリクス認証サーバに合ったデータ形式に変換する．

4. バイオメトリクス認証を用いた Managed VLAN サービス

IEEE802.1x では，基本的に一人のユーザに一つのアクセスポリシーが割り当てられている．例えば，IEEE802.1x を拡張したダイナミックな VLAN 割り当てにしても，ユーザ認証の成功時，VLAN を割り当てるといった程度で，その後ユーザのネットワーク利用に応じて異なる VLAN を割り当てるといったことは考慮されていない．しかし，企業ユーザにおいては，例えば，インターネット利用 LAN と業務用 LAN を全く別網で構築する，顧客 DB へアクセス可能な LAN を業務用 LAN から切り離すといったことがなされており，これは一人のユーザに複数のアクセスポリシーを割り当てている事例と言える．このような事例は，物理的に異なるネットワーク利用を，セキュリティレベルを保った上で，一つのネットワーク上で提供し，ユーザの利便性を向上させることの必要性を示している．すなわち，一つのネットワーク上で，一人のユーザに複数のアクセスポリシーを割り当て，それを柔軟に管理可能とすることが標榜されている．

このような一つのネットワーク上で，一人のユーザに複数のアクセスポリシーを設定する場合，その異なるアクセスポリシー間では，異なる認証レベルを与えることが望ましいと考えられる．そこで，Managed VLAN サービスにおいては，セキュリティ対策を確認し，業務用 VLAN にログインしたユーザ，及び端末が，その後，異なるセキュリティレベルの VLAN にログインする際に，バイオメトリクス認証を利用することを提案する．

この提案する仕組みを利用することにより，端末，及びユーザの認証レベルに応じて，物理的に一つのネットワークを仮想的に複数のネットワークに動的に分離することが可能となる．そのため，ネットワーク敷設のコストが大幅に削減できるとともに，ネットワークの構成変更が柔軟にできるという大きなメリットがある．

4.1. 認証レベルとネットワークアクセス

図 3に認証レベルとネットワークアクセス(VLAN)の関係を示す．端末をネットワークに接続した場合は，まず，IEEE802.1x 認証を行う．この認証をパスすれば，セキュリティ対策用 VLAN を，パスできなかった端末は，Guest VLAN を割り当てる．続いて，このセキュリティ対策用 VLAN 上で端末のセキュリティ対策状況をチェックし，業務用 VLAN を割り当てる．この業務用 VLAN 作業中，より高いセキュリティレベルを必要とする作業を行う場合は，バイオメトリクス認証に基づいて，High Security VLAN を割り当てる．

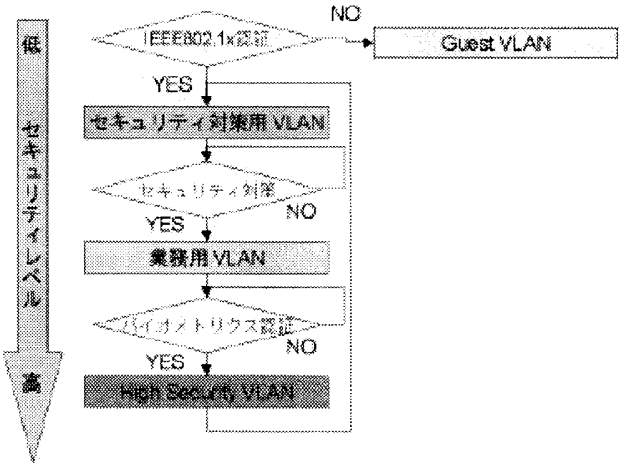

図 3 認証レベルとネットワークアクセス

4.2. サービスアーキテクチャ

図 4にバイオメトリクス認証を用いた Managed VLAN サービスのシステム構成を示す．まず，LAN 内に少なくとも 4 つの VLAN(管理用 VLAN，セキュリティ対策用 VLAN，業務用 VLAN，High Security VLAN)を用意する．図中，IEEE802.1x 認証に失敗したユーザが割り当てられる Guest VLAN は省略している．

Managed VLAN サービスにより，業務用 VLAN を割り当てられているユーザが，より高いセキュリティレベルのネ

ットワークアクセスを必要とするとき(例えば，顧客 DB へのアクセス)，バイオメトリクス認証サーバで承認された場合のみ，High Security VLAN へのアクセスを許可される．

High Security VLAN から戻るときは，セキュリティ対策用 VLAN に入り，セキュリティ対策チェック後，業務用 VLAN に戻るものとする．

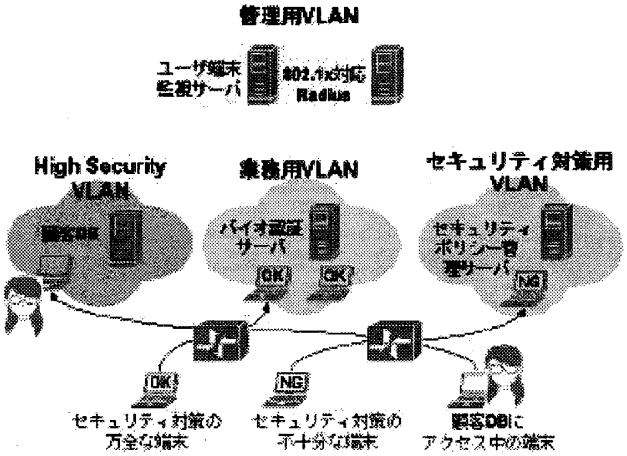

図 4 バイオメトリクス認証を用いた Managed VLAN システム構成

4.3. プロトタイプの実装

図 3に示した認証レベルに応じたネットワークアクセスフローを実現するプロトタイプを開発した．そのネットワーク構成を図 5に示す．図中，VLAN1 は管理用，VLAN2 はセキュリティ対策用，VLAN3 は業務用，そして VLAN 4 は High Security 用とした．

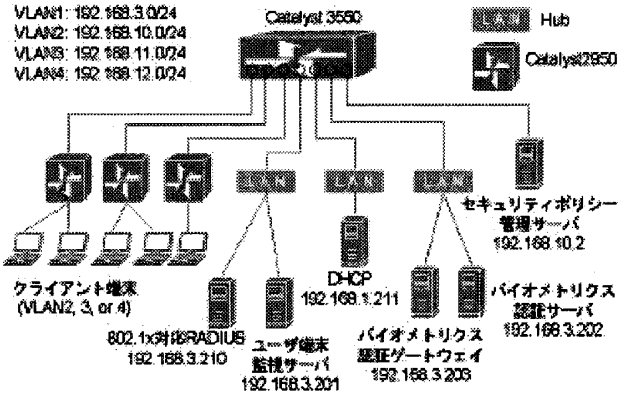

図 5 ネットワーク構成

利用した機器等は以下の通りである．

- 802.1x対応スイッチ：Cisco catalyst 2950 (IOS C2950 software v12.1(20)Enhanced Image，及び Standard Image)
- L3 スイッチ：Cisco catalyst 3550
- 802.1x 対応 RADIUS：Cisco Secure ACS (Access Control Server) v3.1
- DHCP (Dynamic Host Configuration Protocol)サーバ：Microsoft 2003 Server 付属のもの
- バイオメトリクス認証サーバ：富士通サポートアンドサービス社の SF2000 にオムロン社の顔照合エンジンと指紋照合エンジンを搭載したもの
- セキュリティポリシー管理サーバ：NRI Secure Technologies 社の Secure Cube[6]
- クライアント端末：Windows2000，及び XP professional
- バイオメトリクス認証端末：オムロン社製の指紋認証装置，顔認証ソフトウェア，及び PC カメラをインストールした Windows2000 professional

ユーザ端末監視サーバ，及びバイオメトリクス認証 GW は Java を用いて実装した．利用した Java パッケージは以下の通りである．

- J2SE 1.4 SDK
- J2EE 1.4 SDK
- JDMK (Java Dynamic Management Kit) 5.0
- JWSDP (Java Web Service Developer Pack) 1.3

5. まとめと今後

本論文では，まず，XCBF を用いたバイオメトリクス認証 GW モデルを提案し，その有効性を述べた．さらに，このバイオメトリクス認証 GW と Managed VLAN サービスを組み合わせることで，より安全で，利便性の高いネットワーク利用を実現する手法を示し，そのプロトタイプを作成し，図 3に示した認証レベルに応じてネットワークアクセスを制御する仕組みを実現した．

今後は，本サービスの広域 LAN 上での展開を予定している．また，今回，セキュリティポリシー管理サーバーユーザ端末監視サーバ間，及びバイオメトリクス認証サーバーユーザ端末監視サーバ間のメッセージ交換に XML を用いたが，そのメッセージ，及びトランスポートプロトコルにセキュリティ対策を施していない．このメッセージのセキュリティ対策を考慮する必要がある．

謝辞

本研究を進めるにあたってご助言をいただいた日本テレコム株式会社情報通信研究所各位に対して，特に米田研究所副所長，並びに次世代網システム部笠部長に対して，厚く御礼申し上げる．

参考文献

[1] 村上誠, 吉井英樹, "Managed VLAN サービスに関する一検討", 2004 年電子情報通信学会総合大会 B-16-15.
[2] 吉井英樹, 村上誠, "ユーザ端末の状態に応じて VLAN 環境を管理するシステムに関する検討", 2004 年電子情報通信学会総合大会 B-14-21.
[3] Hirokazu Ishimatsu, et al, "Prototype Demonstration of On-Demand/Scheduled Wavelength Path Service", OFC 2003, ThR2, 2003.
[4] http://www.oasis-open.org/
[5] 明石正則 監修, 神鋼リサーチ 編著, "トコトンやさしいバイオメトリクスの本", 日刊工業新聞社, ISBN4-526-05246-9, 2004 年 3 月.
[6] http://www.nri-secure.co.jp/