社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2006－DSM－40 (12)
2006／3／29

階層型VPNにおける他ドメインの証明書を用いたユーザ単位のアクセス制御

土居 正行† 岡山 聖彦†† 山井 成良†† 石橋 勇人††† 安部 広多††† 松浦 敏雄†††

† 岡山大学大学院自然科学研究科
†† 岡山大学総合情報基盤センター
††† 大阪市立大学大学院創造都市研究科

あらまし 階層型VPNにおいて，各VPNゲートウェイでの効率的なアカウント管理を実現するため，証明書を利用したアクセス制御手法が提案されている．しかし，従来手法では組織全体を一つの認証局(CA)が管理することを前提としているため，利用者の多い大規模組織では，CA管理者にかかる負担が大きいという問題がある．本論文では，この問題を解決するため，CAの分散配置を前提としたアクセス制御手法を提案する．提案手法では，CAを設置しないドメイン(CA未設置ドメイン)が存在することを考慮し，CAを設置しているドメインの証明書にCA未設置ドメインのユーザ名を別名として登録する．CA未設置ドメインのVPNゲートウェイは証明書に登録された別名を利用することにより，アカウント登録を行うことなくユーザ単位のアクセス制御が可能となる．

An Access Control Method on a Per-User Basis with Certificates Issued by Other Domains in Hierarchical VPNs

Masayuki Doi† Kiyohiko Okayama†† Nariyoshi Yamai††
Hayato Ishibashi††† Kota Abe††† Toshio Matsuura†††

† Graduate School of Natural Science and Technology, Okayama University
†† Information Technology Center, Okayama University
††† Graduate School of Creative Cities, Osaka City University

Abstract In order to realize efficient account management in hierarchical VPNs, an access control method with certificates has been proposed. However, since this method assumes centralized CA(Certification Authority) which manages all users in an organization, administrative cost of the CA is considerably high if this method is applied to large scale organizations which have many users. To solve this problem, we propose an access control method which assumes distributed CAs environment. In the proposed method, in order to deal with VPN domains which have no CAs, a user name of a VPN domain which has no CA is registered to the optional field of the user's certificate issued by another domain as an "alternative name". By using alternative names of certificates, VPN gateways of VPN domains which have no CAs are able to perform access control on a per-user basis without registration of user accounts.

1 はじめに

近年，インターネットの発展にともない，通信のセキュリティに対する要求が高まっている．特に，インターネットを介して組織内のネットワークにアクセスする場合，セキュリティの確保は必須である．このような場合に使用される技術の 1 つとして，仮想プライベートネットワーク (Virtual Private Network，以下，VPN という) が注目されている．VPN は，仮想的なリンク (以下，VPN リンク) を設けることにより，VPN リンク両端のホストあるいはネットワークが直接接続されているように見せる技術であり，認証と暗号化通信技術を組み合わせることにより，通信の安全性を確保することが可能である．VPN には様々な実現方法があるが，ホスト-ホスト間で VPN リンクを構成するものと，ホスト-ネットワーク間またはネットワーク-ネットワーク間で VPN リンクを構成するものに分けられる．前者は VPN を利用するアプリケーションクライアントとサーバの双方に VPN のためのソフトウェアを組み込まなければならないのに対し，後者の多くはアプリケーションサーバへの組み込みを必要としないので，本論文では後者の VPN 実現方法を対象とする．

VPN では，同一のアクセスポリシ (認証の有無や認証方法，アクセスの可否などのアクセス制御の設定) を持つ範囲を VPN ドメインと呼び，VPN ドメインの境界を跨る通信を制御する VPN ゲートウェイ (以下，VGW) を設置する．このとき，組織内のアクセスポリシが一様であれば組織全体が 1 つの VPN ドメインとなるが，組織内部においても，ある部署の情報を他部署から守りたいという要求がある場合，部署毎に VPN ドメインが形成され，VPN ドメインは組織の内部構成と同様に階層的に構成されることになる．このような構成の VPN を階層型 VPN(図 1) という．階層型 VPN では，組織外にあるクライアントが組織内の VPN ドメインにアクセスするには，最も外側の VPN ドメインから目的の VPN ドメインに向かって 1 つずつ VGW を辿る必要がある．

階層型 VPN に対応できる既存のアクセス方式としては，SOCKS5 の多段プロキシ機構を利用する方式 [1] や仮想パス方式 [2] がある．これらのアクセス方式では，パスワード認証や Kerberos 認証 [3] を利用してユーザを認証した上で，アクセスの可否を決定する．しかし，認証に使用するアカウント情報は各 VGW で独自に管理されるため，各 VGW においてアカウントを登録する必要があり，共同研究などの理由で組織外ユーザを一時的にアクセスさせたい場合，各 VGW でのアカウント管理作業が煩雑になる．これに対し，証明書を利用したアクセス制御手法 [4](以下，従来手法) では，組織全体に 1 つの認証局 (Certification Authority，以下 CA) を設置し，CA の発行した証明書を利用して認証を行う．他組織のユーザに対しては，他組織で発行された証明書の利用や自組織ユーザの発行する証明書を紹介状として利用することにより，各 VGW へのアカウント登録を不要としている．しかし，ユーザの多い大規模組織では，CA の管理者は膨大なアカウント情報を管理しなければならず，管理の負担が大きくなるという問題がある．

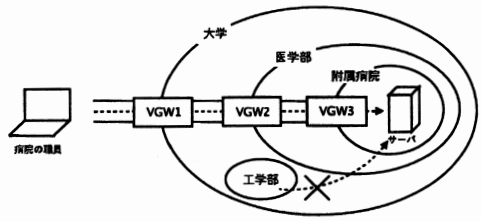

図 1: 階層型 VPN の例

この問題を解決するため，本論文では，CA の分散配置を前提とした，証明書によるユーザ単位のアクセス制御手法を提案する．提案手法では，CA を配置しない VPN ドメイン (以下，CA 未設置ドメイン) が存在することを考慮し，証明書のオプションフィールドを利用して，CA が設置されている VPN ドメイン (以下，CA 設置ドメイン) の証明書に CA 未設置ドメインのユーザ名 (以下，別名) を登録する．CA 未設置ドメインの VGW は，証明書の別名を取り出して利用することにより，CA 設置ドメインの証明書を利用した認証とユーザ単位のアクセス制御を行うことができる．別名の証明書への登録時には，別名と共にディジタル署名を付加することで，CA 設置ドメインでのユーザ名 (以下，本名) と別名の対応を保証している．

以下，従来手法の問題点を考察した後，提案手法の概要について述べ，その有効性を確かめるために実施した性能評価実験について述べる．なお，文献 [2] のアクセス方式と同様に，本論文においても，原則として VPN ドメインを DNS のドメインと一致させることを前提とする．以下，特に明記しない限り，ドメインという用語は VPN ドメインとそれに対応する DNS ドメインの両方を指すものとする．

2 従来のアクセス制御手法と問題点

従来手法では，CA を組織に 1 つ配置し，その CA が組織内の全ユーザに証明書を発行する．自組織のユーザが組織外からアクセスする際には，通過する各 VGW に自己の証明書を提出し，VGW は証明書を用いてユーザを認証すればよいため，個別にアカウント情報を持つ必要がない．

一方，従来手法の他組織のユーザへの対応方法は二つある．一つめは，VGW が信頼する CA リストに自組織の CA だけでなく他組織の CA も加え，他組織のユーザであっても，CA リストに登録されている CA が発行した証明書を持っていればアクセスを許可するという方法である．二つめは，自組織のユーザに証明書発行権限を与え，自組織のユーザが発行した証明書を持っていれば，他組織のユーザであってもアクセスを許可するという方法である．いずれの方法についても，他組織のユーザを一時的に組織内にアクセスさせる際に，各 VGW でのアカウント登録や削除といった作業は不要である．

従来手法では，上述した認証結果に基づいてユーザごとのアクセス制御を行うため，各ドメインにポリシサーバを設置する．ポリシサーバは，ユーザをグループ化するためのグループデータベースと，グループ情報に基づいてアクセスの可否などを決定するためのポリシデータベースを持つ．グループデータベースは図 2 のようなツリー構造を持ち，組織内ツリーはユーザ名，組織外ツリーは他組織の CA の名前をラベルとするノードを持つ，グループデータベースの検索は証明書の所有者名や発行者名に基づいて行い，マッチしたノードの属性値がそのユーザの所属するグループとなる．一方，ポリシデータベースも図 3 のようなツリー構造を持っており，各ノードはアクセスを許可するグループ名を属性として持つ．ポリシデータベースの検索はアクセス先サーバの FQDN(Fully Qualified Domain Name) に基づいて行い，最長一致したノードの属性に基づいてアクセスの可否を決定する．このように，従来手法では，ユーザを複数のグループにまとめた上で，グループ単位での効率的なアクセス制御を実現している．

しかし，従来手法では組織内でのアカウント管理の省力化のため，1 つの CA が組織全体をカバーするネットワークを想定している．すなわち，その CA が組織の全ユーザのアカウント情報を管理することになる．このため，各 VGW においてアカウント登録を行うことなく，ユーザ単位のアクセス制御を行うことができるという利点があるが，多数のユーザが存在する大規模組織では，CA の管理者は膨大なアカウント情報を管理しなければならず，管理の負担が大きくなるという問題がある．また，大規模な組織では，アカウント情報が部署毎に管理されている場合もあり，このような組織に対しては従来手法が適用できないことも考えられる．

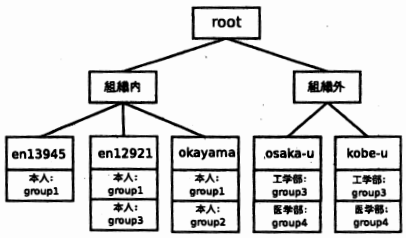

図 2: グループデータベースの例

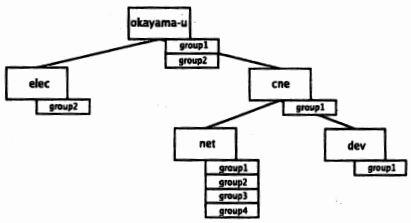

図 3: ポリシデータベースの例

3 他ドメインの証明書を利用したユーザ単位のアクセス制御

3.1 前提とするネットワーク

2 章で述べた CA の管理コストを分散するため，本論文では，各ドメインに CA を配置することを前提とする．但し，管理者の技術レベルやコストなどの理由により，すべてのドメインで CA を運用管理できるとは限らないため，CA 未設置ドメインが存在することを考慮する必要がある．この場合，CA 設置ドメインでは，そのドメインの CA の発行した証明書を利用して認証を行えばよいが，CA 未設置ドメインでは証明書が利用できない．そこで，CA 未設置ドメインでも証明書を利用したアクセス制御を行うために，CA 設置ドメインの証明書を利用して，CA 未設置ドメインにおいて認証を行う方法を検討する．

なお，アカウント情報が部署ごとに独自管理されている環境を考慮し，同一ユーザに対するユーザ名がドメインごとに異なってもよいものとする．

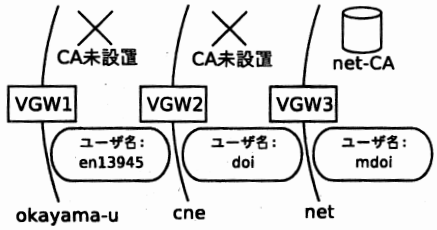

図 4: CA の分散配置の例

3.2 他ドメインの証明書の利用

図 4 のように net ドメインのみに CA が配置され，okayama-u ドメインと net ドメインには CA が配置されていないネットワークを考える．net ドメインのユーザ mdoi は，okayama-u ドメインでは en13945，cne ドメインでは doi というユーザ名を持つものとする．mdoi が組織外から net ドメイン内の情報にアクセスする場合，VGW1〜3 を順に辿る必要がある．mdoi は net ドメインの CA(net-CA) から発行された証明書を持っているが，okayama-u 及び cne ドメインではユーザ en13945 及び doi に対応する証明書を発行できないので，そのままでは VGW1 及び VGW2 で認証を行うことができない．

そこで，CA 設置ドメインでのユーザ名を本名，CA 未設置ドメインでのユーザ名を別名とし，別名を CA 設置ドメインの証明書に記述するものとする．具体的には，net-CA の発行する証明書に，証明書の所有者が okayama-u ドメインでは en13945，cne ドメインでは doi であることを示す情報を記述する．そして，認証の際，各 VGW が自ドメインに対応するユーザ名を取り出してユーザの識別を行う．これにより，CA 未設置ドメインにおいても証明書を利用した認証とユーザ単位のアクセス制御をおこなうことができる．以下，別名の証明書への登録方法と，本名と別名の対応を保証する方法について述べる．

3.2.1 証明書の拡張

証明書には，基本的なフィールド (所有者の情報や発行者の情報等) の他に，オプションフィールドが設けられている．オプションフィールドの一つに，証明書の所有者の別名や電子メールアドレスなどを格納するための Subject Alternative Name Extension フィールド (以下，別名フィールド) がある．提案手法では，別名フィールドに CA 未設置ドメインのユーザ名とドメイン名の組を記述し，CA 未設置ドメインの VGW における認証時にその情報を利用する．別名フィールドには複数のユーザ名

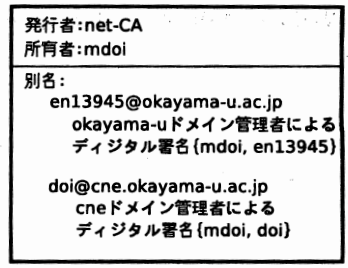

図 5: 別名を付加した証明書の例

が記述できるので，ドメイン名の部分を参照すればドメインの別名なのかが判別できる．別名を付加した証明書の例を図 5 に示す．別名は，メールアドレスのように"ユーザ名@ドメイン名"という形式を用いる．図中のディジタル署名 (以下，署名という) については 3.2.2 節で述べる．

3.2.2 別名の正当性の保証

CA が証明書を作成する際に，別名のみを登録するだけでは本名と別名の対応が保証されない．そこで，CA 未設置ドメインの管理者が別名と本名に対する署名を発行し，CA 設置ドメインの管理者は本名を確認してから証明書に別名と署名を埋め込むものとする．これにより，CA 未設置ドメインの VGW は，認証の際に署名を利用して別名と本名の正当性を検証することができる．例えば，図 4 において net ドメインでは mdoi というユーザが okayama-u ドメインでは en13945 という別名を利用する場合，ユーザは okayama-u ドメインの管理者に mdoi と en13945 という文字列に対する署名を要求する．すると，okayama-u ドメインの管理者は，mdoi というユーザが，そのドメインでは en13945 であるということを確認した上でユーザに署名を発行する．ユーザは同様の手順で cne ドメインにも署名の発行を要求し，mdoi と cne ドメインでの別名である doi という文字列に対する署名を得る．各ドメインでの署名を受け取ったユーザは署名を別名と共に net-CA に提出し，これら付加した証明書の発行を受ける．

このような証明書をあらかじめ作成することにより，okayama-u および cne ドメインの VGW では，ユーザが送信した証明書から，証明書に記載された本名と，自ドメインに対応する別名および署名を利用することにより，別名の正当性を確認することが可能となる．

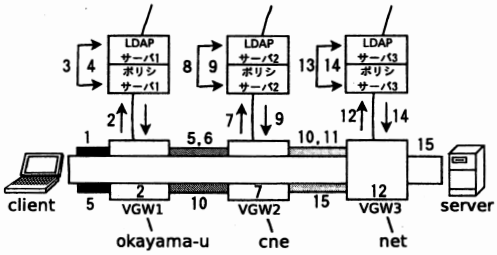

図 6: 別名認証の動作例

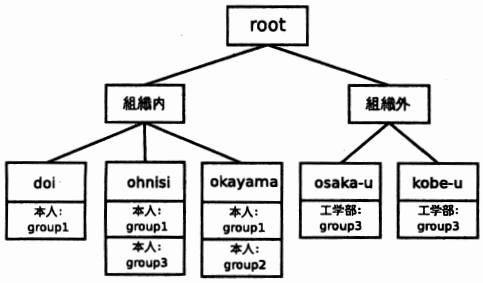

図 7: LDAP サーバ 2 のグループデータベース

3.3 動作例

図 6 のようなドメイン構成を例に，提案手法の VPN リンク確立手順を示す．各ドメインにおけるユーザ名は図 4 のようになっているものとする．図 6 において，LDAP サーバ 1〜3 のグループデータベースはそれぞれ図 2，図 7，図 8，ポリシサーバ 1〜3 のポリシデータベースはそれぞれ図 3 のように設定されているものとする．このとき，図 4 の net-CA から発行された証明書を持つユーザ mdoi が，あらかじめ別名として en13945 および doi を証明書に登録している場合，アクセス手順は以下のようになる．

1. クライアントは VGW1 とコネクションを確立し，VGW1 に証明書を送信する．
2. VGW1 は別名フィールドを読み込み，証明書所有者の自ドメインにおける別名を検索する．別名 en13945 を発見すると付加された署名を用いて正当性を検証した後，それを取り出してポリシサーバ 1 へ送信する．
3. ポリシサーバ 1 は LDAP サーバ 1 のグループデータベースから取得したユーザ名 en13945 のグループ名を検索し，本人属性の属性値 group1 を取得する．
4. ポリシサーバ 1 は LDAP サーバ 1 のポリシデータベースを検索し，目的のサーバの FQDN に

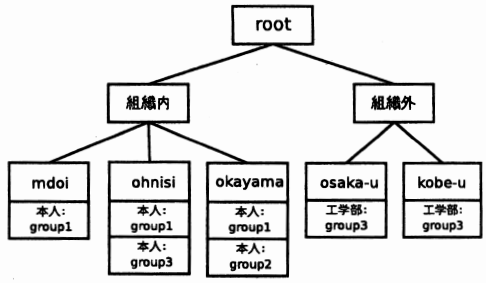

図 8: LDAP サーバ 3 のグループデータベース

最長一致するノード net に取得したグループ group1 があるので，VGW1 にアクセス可能であることを伝える．

5. VGW1 はクライアント-VGW1 間の VPN リンクを確立し，次に VGW2 とコネクションを確立する．
6. クライアントは VGW2 とコネクションを確立し，VGW2 に証明書を送信する．
7. VGW2 は別名フィールドを読み込み，証明書所有者の自ドメインにおける別名を検索する．別名 doi を発見すると付加された署名を用いて正当性を検証した後，それを取り出してポリシサーバ 2 へ送信する．
8. ポリシサーバ 2 は LDAP サーバ 2 のグループデータベースから，取得したユーザ名 doi のグループ名を検索し，本人属性の属性値 group1 を取得する．
9. ポリシサーバ 2 は LDAP サーバ 2 のポリシデータベースを検索し，目的のサーバの FQDN に最長一致するノード net に取得したグループ group1 があるので VGW2 にアクセス可能であることを伝える．
10. VGW2 は VGW1-VGW2 間の VPN リンクを確立し，次に VGW3 とコネクションを確立する．
11. クライアントは VGW3 とコネクションを確立し，VGW3 に証明書を送信する．
12. VGW3 は自組織の CA が発行した証明書なので，証明書の所有者名 mdoi を取得し，それをポリシサーバ 3 へ送信する．
13. ポリシサーバ 3 は LDAP サーバ 3 のグループデータベースから取得したユーザ名 mdoi のグループ名を検索し，本人属性の属性値 group1 を取得する．

表 1: 実験結果

コネクション確立時間 [ms]		
認証無し	従来手法	提案手法
186	1131	1137

14. ポリシサーバ3はLDAPサーバ3のポリシデータベースを検索し，目的のサーバのFQDNに最長一致するノードnetに取得したグループgroup1があるのでVGW3にアクセス可能であることを伝える．
15. VGW3はVGW2-VGW3間のVPNリンクを確立し，次に目的のサーバとコネクションを確立する．

4 性能評価実験

提案手法において，CA未設置ドメインのVGWでは，従来手法における証明書の検証処理だけでなく，証明書に記載された別名と署名の検証処理が加わることになる．そこで，提案手法が従来手法に対してどのくらいの時間がかかるかを調べるために，クライアントが目的のサーバに対してVPNリンクを確立するまでの時間を計測する性能評価実験を行った．

実験ネットワークの構成は図6と同様であり，各ドメインにVGW，DNS，LDAPサーバ，ポリシサーバを配置している．なお，各ホストは学内ネットワークを利用し，100Mbpsのリンクにより接続した．

実験は，組織外のechoクライアントが組織内の最も内側にあるechoサーバに対してVPNリンクを確立する際，各VGWでの認証方法として認証無し，従来手法による認証，提案手法による認証の3通りを行った．別名を利用した認証の実験では，CA設置ドメインとCA未設置ドメインを図4のように設定し，VGW1，VGW2において別名による認証を行い，VGW3では本名による認証を行った．それぞれの認証方法でコネクションの確立を100回ずつ行い，その平均値を算出した．

実験結果を表1に示す．表1より，提案手法と従来手法の差は6msであり，okayama-uおよびcneドメインのVGWにおける別名の検証時間に相当するため，VGWあたりのオーバヘッド増加は3msであると言える．今回の実験における階層数は3であるが，階層数の増加に伴ってCA未設置ドメインが増えた場合，別名検証によるオーバヘッドも増加することが予想される．しかし，提案手法によるオーバヘッドは全体の処理に対して非常に小さいため，実用上問題ないと考えられる．また，認証無しの場合と比べると，提案手法及び従来手法はコネクション確立時間が大きい．その理由として，提案手法および従来手法では，ユーザの提出する証明書が同じであっても，各VGWで独立して証明書の検証を行っていることが挙げられる．従って，あるVGWにおける証明書の検証結果を他のVGWと共有するようにすれば，証明書の検証にかかるオーバヘッドの改善が期待できる．

5 おわりに

本論文では，階層型VPNにおける従来のアクセス制御手法の問題点を考察し，これを解決するための，他ドメインの証明書を利用したアクセス制御手法を提案した．CA設置ドメインの証明書にあらかじめCA未設置ドメインの別名を登録することにより，CA未設置ドメインでも別名を用いたユーザ単位のアクセス制御が可能となる．さらに，従来手法のVGWを拡張して提案手法を実装し，これを用いた性能評価実験を行うことにより，提案手法が実用上問題ないことを確認した．

今後の課題としては，コネクション確立時間を短縮するため，証明書の検証結果をVGW間で共有する仕組みなどを検討する予定である．

謝辞

本研究の一部は，総務省・戦略的情報通信研究開発推進制度 (特定領域重点型研究開発プログラム，課題番号 041108001) の補助を受けている．ここに記して感謝の意を表する．

参考文献

[1] NEC: *SOCKS Home Page*, http://www.socks.nec.com/index.html

[2] 岡山聖彦，山井成良，金出地友治，石橋勇人，安倍広多，松浦敏雄: “階層型VPNのためのLDAPサーバを用いた経路制御手法”, 情報処理学会論文誌, vol.45, no.01, pp.46–55 (2004-01).

[3] J,Linn.:The Kerberos Version 5 GSS-API Mechanism, RFC 1964(1996)

[4] 大西宇泰，岡山聖彦，山井成良，石橋勇人，松浦敏雄：“階層型VPNにおける証明書を利用したアクセス制御手法”, 情報処理学会研究報告, 2004-DSM-34, pp.25–30 (2004-07).