UPKI イニシアティブ サーバ証明書の認証ネットワークへの導入

Installation to the Authentication Network of UPKI Initiative Server Certificate

大谷 誠 †, 江藤 博文 †, 渡辺 健次 ‡, 只木 進一 †, 渡辺 義明 ‡

Makoto Otani†, Hirofumi Eto†, Kenzi Watanabe‡, Shin-ichi Tadaki†, Yoshiaki Watanabe‡

otani@cc.saga-u.ac.jp, etoh@cc.saga-u.ac.jp, watanabe@is.saga-u.ac.jp
tadaki@cc.saga-u.ac.jp, watanaby@is.saga-u.ac.jp

佐賀大学 総合情報基盤センター †
佐賀大学 理工学部 ‡
Computer and Network Center, Saga University†
Faculty of Science and Engineering, Saga University‡

概要

佐賀大学では，利用者端末や公開端末からのネットワーク利用を認証・記録する Opengate を開発・公開し，学内において 2001 年より運用を行っている．この Opengate は IPv4/v6 の両通信に対応しており，これまで学内の一部で IPv6 の試験運用を行っていたが，2008 年 8 月より全学で IPv6 ネットワークのサービスを開始した．

Opengate では，Web ブラウザを用いて利用者認証を提供する．この認証の際に，Web ブラウザのドメイン名に対する名前解決の挙動を利用することで，利用者端末の IPv4/v6 アドレス情報を取得する．8 月からの運用では，この名前解決に使用するドメイン名で UPKI イニシアティブの発行する SSL 証明書を導入した．

本稿では，Opengate における利用者端末の IP アドレス情報の取得と，UPKI イニシアティブの SSL 証明書の導入について報告する．

キーワード

認証ネットワーク，UPKI，IPv6，Opengate，ネットワーク運用

1 はじめに

コンピュータを利用した情報処理や，インターネットによる情報収集は，大学における研究教育で，もはや必要不可欠な技術となっている．専門教育においても様々な形でコンピュータやインターネットを利用するようになっており，学生の個人所有の PC を大学のネットワークに接続し利用することも一般的になりつつある．

しかし，大学のネットワークは，大学における研究教育を支援することを目的として構築され，原則として大学の構成員が利用資格を有するものである．従って，自由に利用できることを目的として設置される公開端末や利用者の移動端末を接続する情報コンセント，無線 LAN においても，利用資格を有する者のみを利用可能とする仕組みが必要となる．

佐賀大学では，利用者端末や公開端末からのネットワーク利用を認証・記録する “Opengate” を開発・公開し，2001 年より学内においてディスクレ

スで運用を行ってきた [1]．2005 年には IPv6 にも対応し，学内において試験運用を行ってきた [2]．

この Opengate は，Web ブラウザにより利用者認証を行う．この認証の際に，Web ブラウザのドメイン名に対する名前解決の挙動を利用することで，利用者端末の IPv4/v6 アドレス情報を取得し，その利用者端末に対する通信路を開放する．

2005 年から試験運用を行うとともに改良を加え，2008 年 8 月より全学で IPv6 ネットワークサービスの運用を開始した．この運用では，名前解決に使用するドメイン名で，UPKI イニシアティブの発行する SSL 証明書を使用し，利用者の入力情報の暗号化等を行っている．

本稿では，Opengate における利用者端末の IP アドレス情報の取得と，UPKI イニシアティブの SSL 証明書の導入について報告する．

2 Opengate ついて

2.1 Opengate の概要

Opengate は，特定多数の利用者が多様な端末を接続するネットワーク環境において，利用者認証と利用記録を行うことができるシステムである．この Opengate は，利用者認証に Web ブラウザを用いるため，特別な申請やソフトウェアの準備なしに，利用者端末等をインターネットに接続することができる．

Opengate のシステム構成例を図 1 に示す．

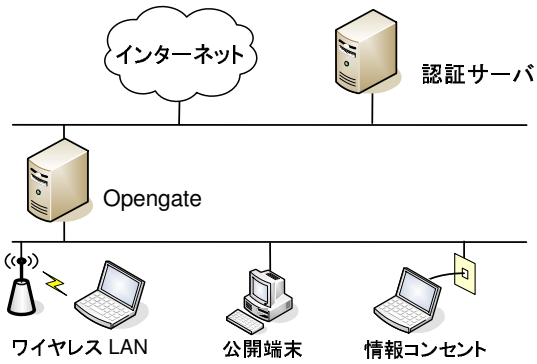

図- 1: Opengate のシステム構成例

利用者が，始めに Web サイトを閲覧しようとする際に，Opengate はその通信を奪い取り，代わりに認証ページを利用者に提供する．利用者は，この認証ページにユーザ ID とパスワードを入力し，認証サーバを利用した認証に成功すると，ネットワークの利用が可能となる．この際に，Web ブラウザで SSL が利用可能であれば，利用者の入力情報は暗号化され，Opengate に送信される．

Opengate では，ファイアウォールの設定によって任意の通信プロトコルを常時開放・常時閉鎖・認証後開放に選択制御できる．

Opengate の認証インタフェースと認証後の表示をそれぞれ，図 2，図 3 に示す．

図- 2: 認証インタフェース

図- 3: 認証後の表示

2.2 利用終了の検知

認証終了後，Web ブラウザ上で JavaScript が実行され，Opengate の監視プロセスと非同期通信を行う．この際の HTTP コネクションを HTTP Keep-Alive と遅延応答によって，長期間維持し，この HTTP コネクションの切断を検知することで，ネットワークの利用終了と判断する [3]．

ただし，HTTP コネクションの維持によって，利用者端末の存在が確認できたとしても，必ずしも利用者がネットワークを利用しているとは限らない．そこで利用者端末から送信されたパケット数を監視し，設定時間内にパケットの通過が確認できない場合も利用終了と判断し，通信路を閉鎖する．

3 利用者端末の IP アドレスの取得

Opengate では，認証後に利用者端末が利用する IP アドレスに対する通信路を，ファイアウォールによって開放する．特に IPv4/v6 デュアルネットワークでは，利用者は，IPv4/IPv6 の通信を意識せずに併用するため，利用者端末が利用する IPv4/v6 アドレスを把握し，統合的に管理する．

利用者認証の際に Web ブラウザのドメイン名に対する名前解決の挙動を利用することで，Opengate は利用者端末の IPv4/v6 アドレス情報を把握し，その利用者端末に対する通信路を開放する．以下に，利用者端末のアドレス情報の流れを示す．

(1) 利用者端末が IPv6 通信に対応し，かつ最初にアクセスした任意の Web サーバも IPv6 通信に対応していた場合は，通常多くの Web ブラウザは，最初の通信を IPv6 で行う．しかし，通信路をファイアウォールで閉鎖しているため，IPv6 HTTP リクエストは遮断される．

(2) Web ブラウザは，同じ Web サーバに IPv4 HTTP リクエストを送信する．ここで Opengate は，ファイアウォールの転送機能を用いて HTTP リクエストを自身の Web サーバへ転送する．

(3) 上記の (2) における転送は，必ず IPv4 通信によって行われる．この際に，利用者端末の IPv4 アドレスを環境変数 “REMOTE_ADDR” より取得する．取得した IPv4 アドレスを URL の引数に付加し，認証を行うページ (CGI) に，クライアントプル機能 (html の meta タグ: http-equiv=”Refresh”) を使って転送する．

(4) 認証ページに，利用者 ID とパスワードを入力すると，これと一緒に hidden タグによってページに埋め込んだ利用者端末の IPv4 アドレスを Opengate の CGI へ送信 (POST) する．この際，送信先の Opengate CGI の URL に，IPv4/v6 両アドレスを持つ FQDN(以下，FQDN_64) の URL を指定する．

(5) Opengate CGI において，URL が FQDN_64 で指定されているので，IPv6 アドレスに対して HTTP 通信が行われる．こで Opengate は，環境変数 “REMOTE_ADDR” より利用者端末の IPv6 アドレスを取得する．IPv4 アドレスは，認証データとあわせて POST されているため，これより取得する．

最初の Web サイトのアクセスが IPv4 で行われた場合，従来手法と同様に上記の (1) の手順が省略され，後は同様である．

利用者端末が IPv6 に対応していない場合も同様に (1) の手順が省略される．また，(5) の手順の POST が IPv4 によって行われるため，ここで利用者端末の IPv4 アドレスが再度取得される．

以上の利用者端末のアドレス取得の流れを，図 4 に示す．

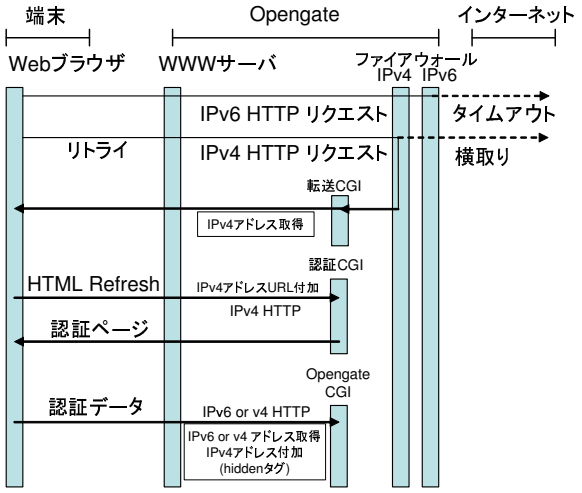

図- 4: 利用者端末のアドレス取得の流れ

試験運用を開始した当初，認証ページを表示する際に，IPv4 アドレスのみを持つドメイン名 (以下，FQDN_4) を準備し，そのドメイン名に一度，ブラウザのクライアントプル機能を用いて転送することによって，利用者端末の IPv4 アドレスを把握していた．このため，FQDN_4 を，FQDN_64 とは別に準備する必要があった．また，SSL による暗号化を行う際には，この FQDN_4 の為の SSL 証明書も別途必要であった [2].

佐賀大学では Opengate を全学規模で運営しており，Opengate のサーバ台数は 20 数台にも及ぶ．このように複数台の Opengate を運営するといった場合に，従来手法ではドメイン名や SSL 証明書の管理コストがとても大きくなってしまう．よって別途ドメイン名を準備する必要のない現行の方法に改良した [4].

3.1 複数の IPv6 アドレスの取得

IPv6 では，利用者端末が複数の IPv6 アドレスを利用する場合があるため，認証時に使用された IPv6 アドレスに対する通信のみを，ファイアウォールで開放しただけでは，十分ではない．そこで，通信状況を監視する際，近隣探索プロトコルである NDP(Neighbor Discovery Protocol) エントリの一覧から得られるアドレス情報と MAC アドレスも監視している．NDP エントリの一覧に，利用者端末の MAC アドレスに対応する IPv6 アドレスが新たに追加された場合は，その IPv6 アドレスに対しても通信路を開放する．ただし，これは利用者端末が Opengate の直下に接続された場合にのみ機能する．

4 SSL サーバ証明書の導入

佐賀大学では，2001 年より全学で Opengate を行っている．従来の Opengate は，IPv4 のみのサービスであったため，通信路の開放には利用者端末の IPv4 アドレスのみを取得すればよかった．そこで，環境変数 “REMOTE_ADDR” から IPv4 アドレスを取得し，ブラウザのドメイン名に対する挙動を使用していなかった．よって，Opengate に利用する URL にもドメイン名を利用せずに，IPv4 アドレスを使用していた．

ユーザ ID やパスワードの入力を行う Web ページでは，HTTPS による暗号化を行っていたが，ここで利用していた SSL のサーバ証明書は IPv4 アドレスによる自己署名証明書であった．よって，セキュリティ上の問題があった．また，近年自己署名証明書検出時の Web ブラウザの警告表示等が強化されつつあるため，この警告等が利用の妨げにもなっていた．

そこで，全学で IPv6 のサービスを開始するにあたり，UPKI イニシアティブの発行する SSL サーバ証明書の取得し，Opengate に導入を行った．

4.1 UPKI イニシアティブ

UPKI イニシアティブは，最先端学術情報基盤 (サイバー・サイエンス・インフラストチャ: CSI) を実現するために構築中である大学間連携のための全国大学共同電子認証基盤構築事業 (UPKI: University Public Key Infrastructure) の仕様や利用方法について，広く情報公開する目的で設立された組織である [5].

4.2 サーバ証明書プロジェクト

この UPKI イニシアティブのプロジェクトの一つに「サーバ証明書発行・導入における啓発・評価研究プロジェクト (サーバ証明書 PJ)」がある．このプロジェクトでは，大学等へのサーバ証明書の普及や学術機関の Web サーバ信頼性向上，サーバ証明書の導入・運用ノウハウの共有を目的として，参加者の Web サーバに対してサーバ証明書の無償配布を行っている．

このプロジェクトには，学術情報ネットワーク (SINET) に加入する大学等であれば無償で参加できる．2008 年 8 月 1 日現在で，71 の機関が参加している．佐賀大学においても，Opengate 等でのサーバ証明書の利用を目的として参加した．

プロジェクトに参加するには，代表となる「機関責任者」と，サーバ証明書発行に関する事務手続きを行う「登録担当者」を決め，機関責任者がドメインの所有や，登録担当者の本人性・実在性を確認した後，書面にて参加申請を行う．申請後，機関責任者の本人性・実在性等の確認が行われた後に，参加手続きが完了する．

4.3 Opengate へのサーバ証明書の導入

佐賀大学では Opengate を全学規模で安定かつ低運用コストでサービスを行うために，若干の設定だけが異なる 22 台のサーバをディスクレスで運用する仕組みを導入している．ディスクレスではあるものの，各 Opengate は異なるハードウェアで構成されている．このような Web サーバの場合，サーバ証明書としてワイルドカード証明書を導入するのが一つの方法である．

しかし，UPKI イニシアティブのサーバ証明書プロジェクトでは，ワイルドカード証明書を発行していない．サーバの冗長化を目的とした同一 FQDN のサーバに対して証明書の発行は行っているが，これは，各サーバ毎に個別の CSR(Certificate Signing Request) を作成する必要がある．Opengate では，各 Opengate 毎に個別の FQDN とし，ぞれぞれの FQDN について CSR を作成した．

サーバ証明書プロジェクトにおけるサーバ証明書の申請は，Excel ファイルによって行われる．登録担当者が，Web サーバの運用を行う「加入者」の本人性・実在性を確認するとともに，ドメインの実在性とサーバの管理権限等の確認を行う．この確認のち，加入者から提出された CSR 情報を Excel に記入し，メールにてプロジェクトに申請する．この

メールには，プロジェクトから発行されたS/MIME証明書により電子署名を行う必要がある．

全学で運用しているOpengateは22台であり，各OpengateのCSRを個別に作成し，一度に申請を行った．ただし，すべてのOpengate情報を一括してExcelファイルに記述できなかったため，2つのファイルに分けて記述し，申請を行った．発行された証明書は，プロジェクトの中間CA証明書とともに，Webサーバに設定する必要があるが，導入マニュアルなども整備されており，導入も容易であった．

5　全学での運用

Opengateの利用対象者は，佐賀大学の構成員である学生 (約7,500人)，教職員 (約1,500名) および学外利用者である．開講期間には月平均で約2〜3万回の利用があり，多い時には，約240人前後が同時に利用している．

2008年8月より，全学のOpengateでIPv6ネットワーク (SINET3) のサービスの運用を開始した．移行の際には，ディスクレス環境の再起動などによる10分程度のサービス停止が必要であったが，停止を事前にアナウンスしていたこともあり，円滑に移行作業を行うことができた．

IPv6対応のOpengateは，利用者端末のIPアドレスの取得方法が，従来のものと異なるものの，インタフェースやその利用方法は，従来のOpengateと同じになるよう開発している．このため，移行に伴う新たな利用指導も特に必要としなかった．また，Opengate環境下で利用される多くのWebブラウザで，導入したSSLサーバ証明書の正常な動作が確認できた．

IPv6対応のOpengateを導入後，2週間の利用者は779人 (教員148人，学生614人，学外利用者17人) で，利用回数は，のべ6,981回であった．開講期間ではないため，学生の利用は通常より少なめであったが，利用者の多く学生であった．また，IPv6対応端末の接続は，のべ1,196回 (17.13%) であった．IPv6対応端末のうち，Windows Vistaが918回 (76.76%) であり，利用の多くが標準でIPv6が利用可能なVista OSであった．

6　まとめ

大学のネットワークは，大学における研究教育を支援することを目的として構築され，原則として大学の構成員が利用資格を有するものである．従って，自由に利用できることを目的として設置される公開端末や利用者の移動者端末を接続する情報コンセントにおいても，利用資格を有する者のみが利用できる仕組みが必要である．

また，近年，大学などの教育・研究機関において，IPv6ネットワークの導入が進んでいる．よって将来，IPv6ネットワークの利用者に対して，公開端末や情報コンセントを提供するためには，IPv4/v6の通信を統合的に制御可能とする利用者認証システムが必要となる．

佐賀大学では，利用者端末や公開端末からのネットワーク利用を認証・記録するOpengateを開発・公開し，学内において運用を行っている．このOpengateはIPv4/v6の両通信に対応しており，2008年8月からは全学でIPv6ネットワークのサービスを開始した．

Opengateでは，Webブラウザのドメイン名に対する名前解決の挙動を利用することで，利用者端末のIPv4/v6アドレス情報を取得する．今回は，この名前解決に使用するドメイン名でUPKIイニシアティブの発行するSSL証明書を取得し，導入した．

参考文献

[1] 渡辺義明, 渡辺健次, 江藤博文, 只木進一 : 利用と管理が容易で適用範囲が広い利用者認証ゲートウェイシステムの開発, 情報処理学会論文誌, Vol.42, No.12 pp.2802-2809 (2001)

[2] 大谷誠, 江口勝彦, 渡辺健次 : IPv4/IPv6デュアルスタックネットワークに対応したネットワーク利用者認証システムの開発, 情報処理学会論文誌, Vol. 47, No. 4, pp.1146-1157 (2006)

[3] 大谷 誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明: “HTTPコネクションの維持による利用終了検知を行うネットワーク利用者認証システムの開発とその運用”, 学術情報処理研究, No. 11, p.87-p.91 (2007)

[4] 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明: “ネットワーク利用者認証システム Opengate の改良と運用について”, 学術情報処理研究, No. 10 (2006)

[5] UPKIイニシアティブ ホームページ
https://upki-portal.nii.ac.jp/