Vol.2010-IOT-9 No.5
2010/5/13

仮想環境によるSSO対応Opengateの構築とその運用

大谷 誠[†1] 江藤博文[†1] 渡辺健次[†2]
只木進一[†1] 渡辺義明[†2]

佐賀大学では，ネットワークの利用者認証と利用記録を行うためのゲートウェイシステム Opengate を開発し，学内において運用を行っている．この Opengate を Shibboleth によるシングルサインオン認証に対応させ，2010 年 3 月より全学において運用を開始した．

このようなシステムを全学規模で運用するためには，多数のサーバを準備し統合的に管理・運用をしていく必要がある．多数のサーバを用いるシステムの冗長性確保とコスト削減には，仮想化技術が有用であり，本システムの実現においても仮想化技術 (VMware) を用いた．本稿では，仮想環境による SSO 対応 Opengate の構築とその運用について述べる．

Operation of SSO-Opengate Using virtual machine

Makoto Otani,[†1] Hirofumi Eto,[†1] Kenzi Watanabe,[†2]
Shin-ichi Tadaki[†1] and Yoshiaki Watanabe[†2]

We have developed and distributed a network user authentication system “Opengate”. It has been operated in Saga University. We developed Opengate corresponding to single sign-on authentication by “Shibboleth”, and this has been working for controlling the open network in the campus since March 2010.

Many systems are needed in order to realize this system at the university. To reduction of this cost, the system management by the virtual machine technology is useful, and such technology (VMware) is used for this system. This paper describes operation of SSO-Opengate which used the virtual machine.

1. はじめに

近年，大学などにおいて情報提供や各種情報サービスを目的とした Web を用いる多種多様な情報システムが運用されるようになってきた．このような Web 情報システムは用途ごとに構築される場合が多く，通常は利用者が用途に応じてそれぞれの情報システムにアクセスする必要がある．そこで，各システムを利用しやすいようにポータルサイトにまとめるといった，利便性を向上させる取り組み[1]も行われている．

一方，多くの大学においてネットワーク利用者認証および記録機能を備えた，個人所有のノート PC などを接続可能な情報コンセント，無線 LAN などの設置が行われている．このような認証の仕組みを実現するシステムの 1 つとして Web ブラウザを使ったネットワーク利用者認証システムがある．佐賀大学では，このような認証システムとして Opengate[2,3]を全学的に整備しており，学内ネットワークを利用するための認証として利用されている．このような Web によるネットワーク利用者認証システムと，Web による情報システムがシングルサインオン認証に対応すれば，最初にネットワーク利用者認証を行うだけで，Web 情報システムを再認証なしに利用することが可能となり，利用者の利便性が向上すると考えられる．

そこで我々は，シングルサインオン認証に対応した Opengate (以下，SSO-Opengate) の開発を行い 2009 年より試験運用を行ってきた．そして，2010 年 3 月より全学規模で運用を開始した．この SSO-Opengate は，Shibboleth によるシングルサインオン認証に対応しており，ネットワーク利用者認証を行うだけで，Shibboleth に対応した Web 情報システムにおいて再認証が必要がなくなる．

このようなシングルサインオンの認証サービスを全学規模運用していくためには，多数のサーバを準備し，統合的に管理・運用を行っていく必要がある．佐賀大学では，これまでディスクレスによるネットワークブートが可能な機器を複数台用い，マスターサーバによって設定等を一元管理することで，管理コストを抑えつつ，ネットワークの認証サービスを提供してきた[4]．しかし，この方法では 1 台のサーバを構築するために，それに対応する物理サーバをそれぞれ 1 台準備する必要があった．このような多数のサーバを構築する際の冗長性確保と運用コスト削減において，近年，仮想化技術が注目されている．そこで SSO-Opengate

†1 佐賀大学 総合情報基盤センター
Computer and Network Center, Saga University
†2 佐賀大学 工学系研究科
Faculty of Science and Engineering, Saga University

による新たなサービスの実現において，VMware による仮想化技術を用いた．

2. 背　　景

2.1 Opengate の概要

我々は，ネットワーク利用者認証システムとして Opengate を開発・改良し，2001 年より全学規模で運用を行ってきた．Opengate では利用者が Web ブラウザを起動し，任意のページにアクセスする際の通信を奪い取り，認証ページを表示する．認証ページを用いて利用者認証を行うことでファイアウォールが開き，IPv4/IPv6 ネットワークの利用が可能となる．

認証後は，ログイン状況を表示するとともに，同時に利用案内のページが表示される．Opengate は，認証を行った Web ブラウザのウィンドウの閉鎖をネットワーク利用終了と判断し，ファイアウォールを閉鎖する．Opengate では，認証で得られた利用者の情報，端末情報，利用開始・終了時刻を記録する．

佐賀大学では現在，学内のほぼ全ての教室や図書館などにおいて，有線および無線による Opengate の使用が可能である．会議室や研究室にもサービスを提供し，学生だけでなく教員も利用している．また，利用申請を行ってもらうことで，来訪者の利用も可能である．

2.2 Opengate におけるシングルサインオン認証の必要性

利用者認証基盤として，佐賀大学では総合情報基盤センターの統合認証システム[5]を用いている．この統合認証システムは 2003 年に導入され，Opengate を含む学内の情報システムにそれぞれ認証情報を提供している．各情報システムでは，総合情報基盤センターの共通のユーザ ID とパスワードで認証が行われており，統合認証システムは学内の認証基盤として位置づけられている．

利用者は持ち込み PC などを学内ネットワークに接続し，各種 Web 情報システムを利用する場合は，まずはネットワーク利用者認証システムである Opengate により認証を行うこととなる．その後に，教務・財務システム，e ラーニング，Web メールなど，各種 Web 情報システムで個別に認証し，それぞれのサービスを受けることになる．

そのため，たとえ統合認証システムにより各 Web 情報システムを同じユーザ ID とパスワードで利用可能であったとしても，利用者認証が何度も行う必要があり，利用者にとっては不便である．よって，ネットワーク利用者認証システムと Web 情報システムがそれぞれシングルサインオン認証に対応し，各種 Web 情報システムのログインの手間を省くことができれば利便性が大幅に向上すると考えられる．

そこで，Opengate を Shibboleth によるシングルサインオン認証に対応させた SSO-Opengate を開発し，実際に 2010 年 3 月より学内において運用を開始した．

3. SSO-Opengate

3.1 シングルサインオン認証

SSO-Opengate におけるシングルサインオン認証の実現に，Shibboleth を利用した[6]．Shibboleth は，Internet2 の教育機関向けプロジェクトである MACE (Middleware Architecture Committee for Education) で開発された SAML ベース (OpenSAML) の認証システムである．

Shibboleth は，利用者の認証と利用者の属性情報を提供する IdP (Identity Provider)，IdP からの属性情報によりサービスを提供する SP (Service Provider)，IdP が複数存在する場合に，IdP のリストを提供する DS (Discovery Service) で構成される．IdP,SP,DS として動作させるためのソフトウェアは，Internet2 から公開され，このソフトウェアと Web サービスを連携させることにより，シングルサインオン認証の実現が可能となる．

SSO-Opengate では，ネットワーク利用時に認証を利用者に求めるが，SSO-Opengate 自体は，IdP として動作するわけではない．SSO-Opengate は，別途準備された IdP よりネットワーク利用者の属性情報の提供を受け，その属性情報をもとにネットワーク利用を許可するサービスとなる．よって，Shibboleth に対応しサービスを提供する他の Web 情報システムと同様に，SP として動作している．

3.2 SSO-Opengate のシステム構成

SSO-Opengate は，従来の Opengate と同様に利用者端末のネットワークとの間に，ゲートウェイとなるよう設置し，そこを通過する IPv4/IPv6 パケットをファイアウォールで制御することによってネットワーク認証を行うシステムである．利用者の認証は，シングルサイン認証を行うために別途準備された IdP を用いる．**図 1** にシステムの構成を示す．

SSO-Opengate は，Web サーバから CGI として起動され，利用者のインターネット利用のためのファイアウォールの制御を行う．SSO-Opengate は，FreeBSD 上で構築されており，ファイアウォールの制御には ipfw，Web サーバには Apache を用いて実現した．IdP および，SSO-Opengate のソフトウェア構成を**表 1** に示す．

SSO-Opengate については，VMware による仮想環境上で動作している．これについては，第 4 章において述べる．

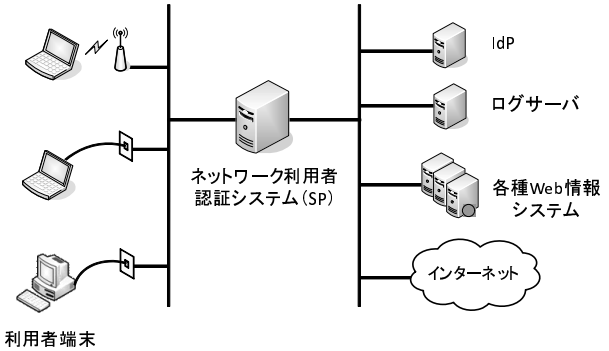

図 1 システム構成
Fig. 1 System architecture.

表 1 ソフトウェア構成
Table 1 Software architecture.

IdP	OS	Solaris 10
	シングルサインオン	Shibboleth IdP 2.1.2
	Web サーバ	Apache 2.2.14
SSO-Opengate	OS	FreeBSD 6.4-RELEASE
	シングルサインオン	Shibboleth SP 2.1
	Web サーバ	Apache 2.2.14
	ファイアウォール	ipfw (OS 付属)

3.3 SSO-Opengate の利用手順

SSO-Opengate が動作している環境で，インターネットを利用する手順を以下に示す．

(1) 利用者が Web ブラウザを用いて任意の URL へアクセスを行うと，通信が奪い取られ，ユーザ ID とパスワードを要求する認証ページが送られてくる*1．
(2) 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する．
(3) 認証に成功すると，認証が成功したことを示す認証許可ページが表示されるとともに，認証後に表示するように設定されているサイトが別ウィンドウ (ブラウザの設定によっては，別タブ) で表示される．
(4) ネットワークの利用を終了する際には，認証許可ページを閉じる．これによりインターネットへの通信路が閉鎖され，(1) の状態に戻る．

*1 来訪者へのサービスとして DS を用いている場合は，まず DS による IdP 選択の画面が現れるので，利用する IdP を選択する

SSO-Opengate では，自分自身ではなく IdP を経由して認証を行うが，利用者の操作は変わらないため，従来の Opengate 利用していた利用者に対しては，特に利用指導を行うことなく，この SSO-Opengate を導入することができる．佐賀大学においても特に新たな利用指導なしに，従来の Opengate から SSO-Opengate への切り替えを行ったが，トラブルも発生せずスムーズに移行が可能であった．

3.4 認証フェデレーションによる来訪者への提供

SSO-Opengate は，複数の IdP を利用する必要がある場合でも，Shibboleth の DS を用いて IdP の選択を行い，認証を行うことが可能である．これにより，他大学などで構築された IdP を用いて認証連携することで，来訪者がネットワークを別途申請なしに利用することも可能である．

佐賀大学では現在，学術認証フェデレーション（学認: Gakunin[7]) 参加者用に，無線接続で利用できる SSO-Opengate ネットワーク (アクセスポイント数:300 弱) を準備しており，「学認」の参加者であれば，学内の多くの場所で申請なしに SSO-Opengate によるネットワークの利用が可能である．

4. 仮想システムを用いた SSO-Opengate の構築

4.1 SSO-Opengate の仮想化

SSO-Opengate は，ゲートウェイとして動作することが想定されているため，通常のネットワークにおいて機能しているルーティング装置の役割も，このシステムが担うことになる．従って，本システムは，安定なサービス提供とともに適切な負荷分散と冗長性を確保するためにも，1 つのサーバとしてではなく複数のサーバとして導入し，これらを一括して管理・運用していくことが望ましいと考えられる．

従来の Opengate は，複数のサーバ (20 台前後) で構成していた．この複数のサーバには，ディスクレスによるネットワークブートが可能な機器を用いていた．また，ネットワークブートのために必要となるマスターサーバ上で設定等を一元管理することで，管理コストを抑えていた[4]．しかしながら，この方法では 1 台のサーバを構築するために，それに対応する物理サーバをそれぞれ 1 台準備する必要があった．ディスクレスであるため，障害の発生率も低く，これまで安定して運用してきたが，2001 年より同一筐体で運用を続けており，低スペック (CPU: Pentium III 1GHz , Memory: 512MB) であるため，これを用いて SSO-Opengate の安定運用を行うのは難しい．そこで，SSO-Opengate の運用を始めるに

図 2 仮想システムによる SSO-Opengate の運用
Fig. 2 Operation of SSO-Opengate by virtual machine.

あたり，新たな運用環境を構築する必要があった．

我々は近年急速に普及してきた仮想化システムに注目し，SSO-Opengate の運用に用いた．実際に使用した仮想化システムは，VMware (vSphere 4.0) である．仮想化システムにおいて SSO-Opengate が利用する FreeBSD OS を標準的にサポートするものは少ないが，vSphere 4.0 は FreeBSD もサポート対象の OS であり，SSO-Opengate の安定運用が期待できる．

vSphere 4.0 では仮想化 OS(ハイパーバイザ) として ESX が用いられるが，この ESX を動作させる物理サーバとして，以下のスペックのサーバを 7 台準備した．

- CPU: Xeon E5540 2.53GHz (Quad Core) × 2
- Memory: 20GB
- CNA (Converged Network Adapter): 2 ポート
- Ethernet: 10/100/1000BASE-T 2 ポート

また，これら 7 台の ESX サーバを一元的に管理するために必要な vCenter Server を動作させるサーバとして，同一スペックのサーバをもう 1 台準備した (**図 2**).

4.2 仮想環境での SSO-Opengate の構築手順

vSphere 4.0 では，vCenter Server 上で一度作成した仮想サーバのクローンを簡単に作成することができる．そこで，SSO-Opengate を複数台構築するにあたり，雛形となるマスターサーバを 1 台構築し，そのクローンを作成することで SSO-Opengate を運用するサーバを複数台構築することとした．以下に，その構築手順を示す．

(1) 仮想サーバの設定を行う vSphere Client を用いて，vCenter Server に接続する．これ以降の作業は，基本的に vSphere Client を用いて行う．

(2) 各 SSO-Opengate の雛形となるマスターサーバを構築するため，新規マシンの作成を行い，その新規マシンに FreeBSD6.4 のインストールを行う．
ここで，仮想マシンの各リソースを以下のように設定した．
  - CPU: 1CPU(クロック数は動的割り当て)
  - Memory: 2GB
  - HDD: 32GB
  - Ethernet: 10/100/1000BASE-T 3 ポート (WAN,LAN, ログ出力用)

(3) SSO-Opengate に必要な各種ソフトウェア (表 1 等) のインストールを行い，基本設定を行う．

(4) ゲスト OS と vSphere との連携を行うことで仮想システムの効果的な利用を可能とする，VMware Tools のインストールを行う．SSO-Opengate の運用においては，電源異常が発生した際に，UPS 装置と連携し SSO-Opengate を正常にシャットダウンさせるために，この VMware Tools を利用する．

(5) 以上で，SSO-Opengate の雛形となるマスターサーバが完成となる．このマスターサーバからクローンを作成し，複数台の SSO-Opengate を作成する．クローンの作成後は，各サーバ毎の個別設定 (ネットワーク設定,SSL サーバ証明書設定等) を行い，新規設定でサーバを起動する．

クローンの作成後，個別の設定を行う際には，クローンとして作成した仮想サーバを一度起動する必要がある．しかしながらこの起動した仮想サーバは，雛形として作成したマスターサーバと全く同じ設定であるため，そのまま起動すると，ネットワーク等の設定が重複しトラブルが発生する場合がある．そこで，クローンにより作成した仮想サーバの初回起動時には，各 NIC がネットワークに接続しないように設定を変更 (**図 3** の「パワーオン時に接続」のチェックをオフ) した後に，サーバを起動し，各種設定変更を行う必要がある．ネットワークに関する設定の詳細は，第 4.3 節にて説明する．

現在は，上記の ESX サーバ 1 台上で SSO-Opengate を 8 台ほど仮想に動作させ，学内にサービス提供している．この 8 台はそれぞれ，文化教育学部・教養教育, 経済学部, 理工

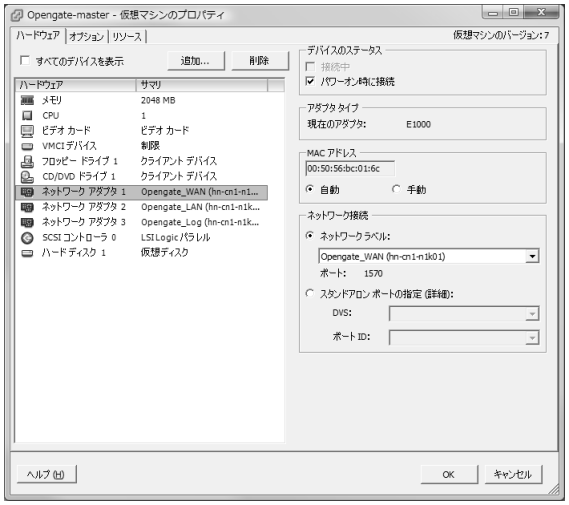

図 3 仮想サーバの設定画面
Fig. 3 Setting screen of virtual server.

学部, 農学部, 医学部, 遠隔施設, その他組織,「学認」参加者用である．従来の Opengate では，先に述べたように 20 台前後の物理サーバでサービスの提供を行っていた．仮想システムにおいては，処理能力の向上もあり仮想サーバ 8 台でサービスを提供しているが，これまで問題なく動作している．

運用開始が 3 月 (春休み) であったため，授業開講時と比べ利用者は少なめ (同時利用者数:最大 200 人前後) であるが，この規模でも各サーバの CPU・メモリの利用率はかなり低く (**図 4**)，授業開講時に利用者が大幅に増えたとしても十分耐えられると思われる．もしサーバの台数を増やす必要性が生じた場合にも，先に述べたようにサーバの複製も容易で，柔軟に対応することが可能である．

4.3 ネットワークの仮想化

SSO-Opengate は，先にも述べたようにゲートウェイとして動作する．よって，この SSO-Opengate 自体がルータとしても動作することでネットワークが構築される．現在，主に持ち込み PC を想定した SSO-Opengate が運用されるネットワークだけでなく，その他のネットワークに対してもポータルサイトなどを表示することを想定した場合，数十台のルータ (SSO-Opengate) を仮想システムを用いて構築していくこととなる．

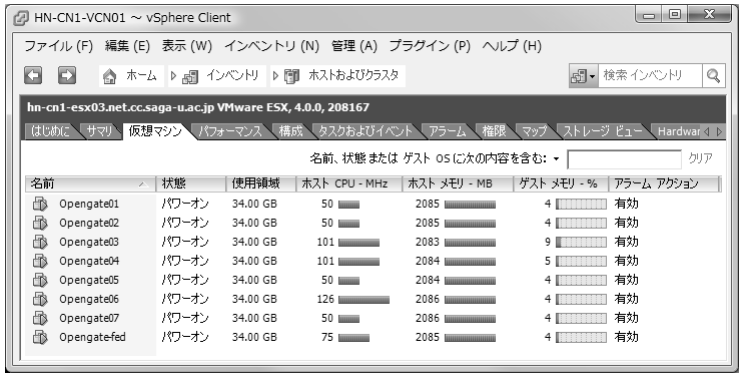

図 4 仮想サーバの状態確認画面
Fig. 4 Status screen of virtual server.

よって，ネットワーク自体の冗長性や柔軟性，帯域の確保が重要な課題となる．このような要件を満たし，かつ既存のネットワークから柔軟に移行を行うことを想定すると，仮想サーバを用いてネットワークを構成する場合においても，ネットワークの設定が既存の物理ネットワーク機器 (L2 スイッチ) と同様に行えることが望ましい．

そこで，仮想サーバ全体のネットワークの統合的な管理を実現し，かつ物理ネットワーク機器 (L2 スイッチ) と同様に設定可能となる仮想ソフトウェアスイッチ (Nexus 1000V[8]) もあわせて導入した．Nexus 1000V は，Cisco Nexus スイッチをソフトウェアとして実装するものである．このソフトウェアは，仮想 OS を管理するハイパーバイザ (ESX) に統合され，仮想マシン対応のネットワークサービスを提供する．以下に，Nexus1000V の設定例を示す．

Nexus1000V 設定例

```
n1000v(config)# port-profile type vethernet Opengate_WAN
n1000v(config)# vmware port-group
n1000v(config)# switchport mode access
n1000v(config)# switchport access vlan 100
n1000v(config)# no shutdown
n1000v(config)# state enabled
```

Nexus1000V 特有の設定が含まれているものの，物理的な Cisco スイッチと同様に設定が可能であり，上記のような設定を行うと，仮想サーバの設定画面上 (図 3) でネットワークラベルとして指定が可能となり，指定後にネットワークの利用が可能となる．

この Nexus 1000V を導入したことにより，運用するサーバの台数が増えてもネットワークに関するケーブリングが新たに発生せず，かつ従来の物理スイッチと同様に，ネットワークを管理 (SNMP の利用, ポートミラーリング等) することが可能であるため，移行も非常にスムーズに行えた．また，vSphere の機能として仮想サーバについての様々なデータを統合的に把握することが可能となり (図 4 など)，管理コストの軽減にも繋がった．

5. Web 情報システムのシングルサインオン認証対応

SSO-Opengate が導入されたネットワークにおいては，ネットワークの利用者認証の際に，ポータルサイトなどを表示し，そこで Web 情報システムへのリンクを提示することによって，各システムの利用を促すことが可能である．Web 情報システムの利便性を向上するためには，先に述べたようにそれぞれの Web 情報システムをシングルサインオン認証に対応させていく必要がある．

現在，佐賀大学においてシングルサインオン認証に対応 (または予定) する主なサービスは以下の通りである．

- SSO-Opengate
- 総合情報基盤センターポータルサイト
- 図書館ポータルサイト
- 教職員グループウェア
- 統合認証パスワード変更
- 佐賀大学 e-Learning システム (試験運用中)
- 教務ポータル・教務システム (2010 年 7 月〜)

多くの Web 情報システムがシングルサインオン認証に対応しつつあるが，これ以外のシステムも学内に多く存在する．また，大学では次々の新しい Web 情報システムが発生するため，情報システムをシングルサインオン対応とするための手順の整理や支援体制の構築が今後重要になると思われる．

6. ま と め

佐賀大学ではネットワーク利用者認証システム Opengate を全学的に整備している．この Opengate は，主に持ち込み PC を学内ネットワークに接続する際の最初の認証になる．この Opengate の認証と Web による情報システムが，ともにシングルサインオン認証に対応すれば，最初にネットワーク利用者認証を行うだけで，Web 情報システムを再認証なしに利用することが可能となり，利用者の利便性が向上する．

そこでシングルサインオン認証に対応した SSO-Opengate の開発を行い，2010 年 3 月より全学規模で運用を開始した．また，この SSO-Opengate を構築・運用するにあたり，VMware による仮想化技術を用いた．これにより冗長性確保と運用コストの削減とともに，従来システムからの移行負荷も軽減することができた．

参 考 文 献

1) 名古屋大学ポータルによる情報サービスの統合と課題, 梶田将司, 内藤久資, 平野靖, 瀬川午直, 小尻智子, 間瀬健二, 情報処理学会研究報告, 2007-DSM-046, pp.1-6 (2007)
2) HTTP コネクションの監視により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円滑な導入, 大谷誠, 江藤博文, 渡辺健次, 只木進一, 渡辺義明, 情報処理学会論文誌, Vol.50, No.3, pp.1032-1042 (2009)
3) Opengate とシングルサインオン, 江藤博文, 大谷誠, 渡辺健次, 只木進一, 情報処理学会研究報告, 2009-IOT-4, pp.259-264 (2009)
4) 公開端末及び利用者移動端末の認証システムとそのディスクレスマシンによる運用, 只木進一，江藤博文，渡辺健次，渡辺義明，学術情報処理研究, No.5, pp.15-20 (2001)
5) 江藤博文, 渡辺健次, 只木進一, 渡辺義明, 大学における情報基盤整備の中核となる統合認証システム, 分散システム/インターネット運用技術シンポジウム,2003
6) Shibboleth,http://shibboleth.internet2.edu/
7) UPKI イニシアティブ 学術認証フェデレーション（学認：Gakunin), https://upki-portal.nii.ac.jp/SSO
8) Cisco Nexus 1000V, http://www.cisco.com/web/JP/product/hs/switches/nexus1000/