

ネットワーク利用者認証システム OpengateとIPv6・Shibboleth ～佐賀大学のネットワーク～

渡辺健次
佐賀大学

watanabe@is.saga-u.ac.jp



Opengateの歴史

- 1999年、開発開始
- 2000年、試験運用開始
- 2001年、全学で運用開始
- 2006年、IPv6対応版
- 2008年、全学でIPv6版運用開始
- 2009年、Shibboleth対応版
- 2010年、全学でShibboleth対応版運用開始
- 2011年、OpengateM

2012年2月11日

オープンソースカンファレンス2012 in Oita



目次

- 無線LANの展開(1999年頃)
- ネットワーク利用者認証システムOpengate
- OpengateとIPv6
- OpengateとShibboleth
- なぜ自ら開発するのか？
- Opengateの今後
- まとめ

2012年2月11日

オープンソースカンファレンス2012 in Oita



無線LANの展開(1999年頃)

- ノートPCを自由に接続可能な情報コンセントや無線LAN環境の準備
- 利用者の認証
 - 大学の関係者だけが使えるように
- 利用者の記録
 - 何か起きたときにトレースできるように

2012年2月11日

オープンソースカンファレンス2012 in Oita



大学の実体は

- 多種多様なハードウェア、ソフトウェア
 - 各自が好きなPCを購入、使い続ける
 - ソフトもさまざま (IE、Firefox、Opera、Safari・・・)
- 利用者
 - 教員は「個性的」
 - 学生は(最初は)初心者
- 管理者は人手不足で過負荷
 - 新たな仕事が発生しないように
- システム更新が難しい
 - 学内LANの更新は10年に1回程度

2012年2月11日

オープンソースカンファレンス2012 in Oita



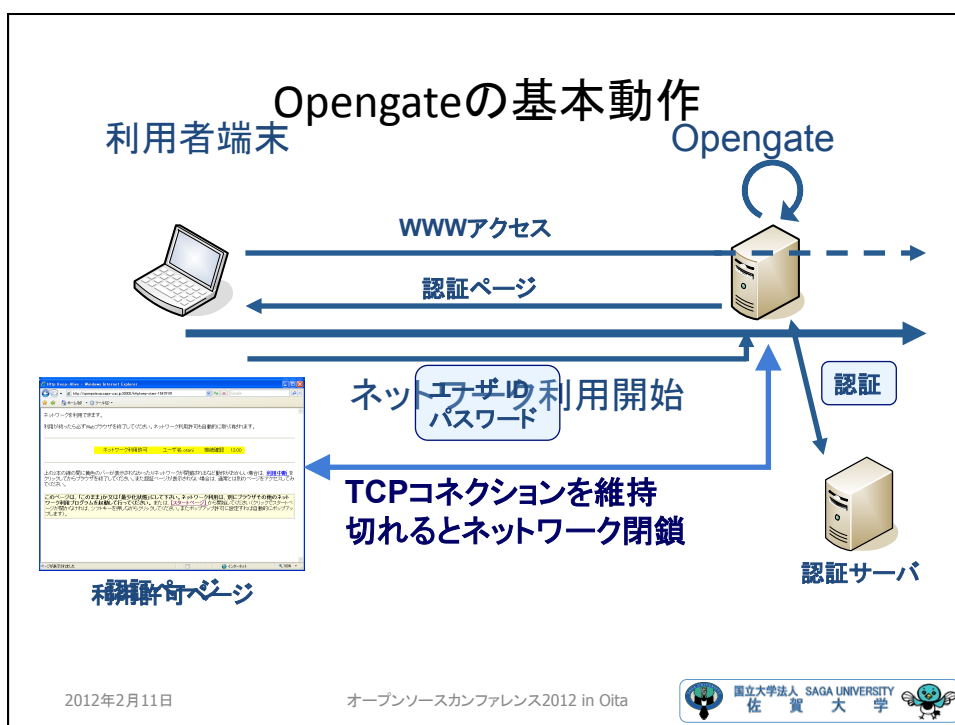
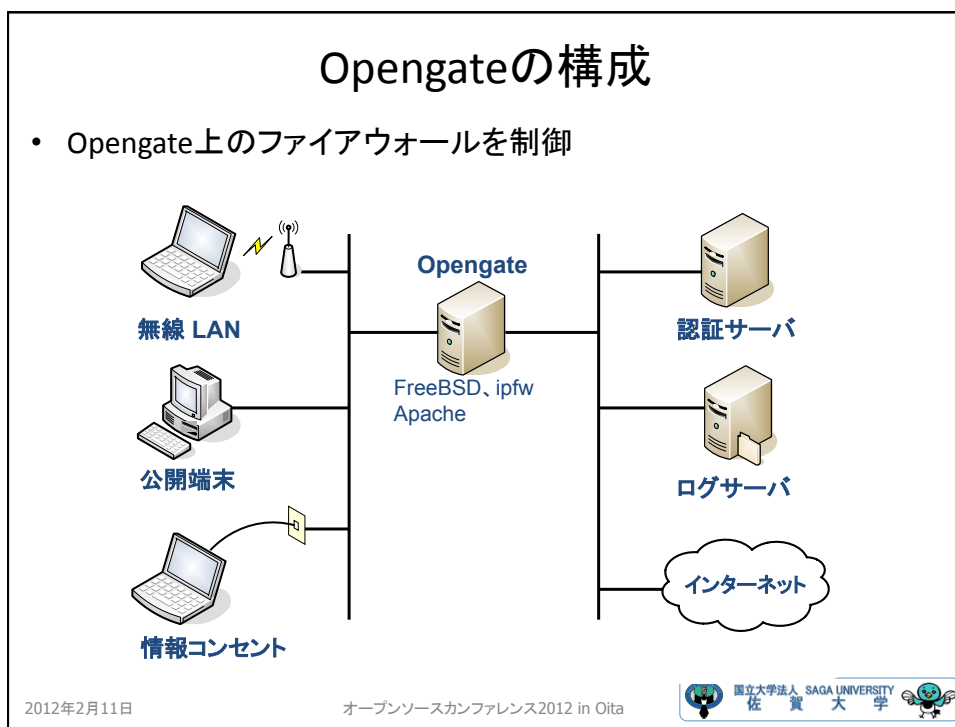
ネットワーク利用者認証システム Opengate

- 利用が容易
 - 任意URLへのアクセスで認証ページが表示
 - ブラウザを閉じると利用終了
 - 利用申請不要・・・事前登録などの手間が不要
- 多様な環境に適用
 - 無線/有線、公開端末/持参端末
 - Windows/Mac/Linux・・・ブラウザがあれば良い
 - IE、FireFox、Safari・・・普通のブラウザで良い
- 導入が容易
 - 既存認証サーバ利用可 (POP(S), LDAP(S), FTP, RADIUS, PAM)
 - 既存ネットワーク環境に導入容易

2012年2月11日

オープンソースカンファレンス2012 in Oita





端末用LAN(2001～2010)

- 持ち込みPC専用のLANを整備
 - 情報コンセント(約730口)
 - ほぼ全教室(各2口)、図書館、学生居室等
 - 無線LANアクセスポイント(約90箇所)
 - ほとんどの教室から利用可能な位置、図書館等
 - 各学部の教授会の部屋から整備
- 利用資格保有者
 - 教職員約1500人
 - 学生約7500人
 - 学外者(一時利用者)

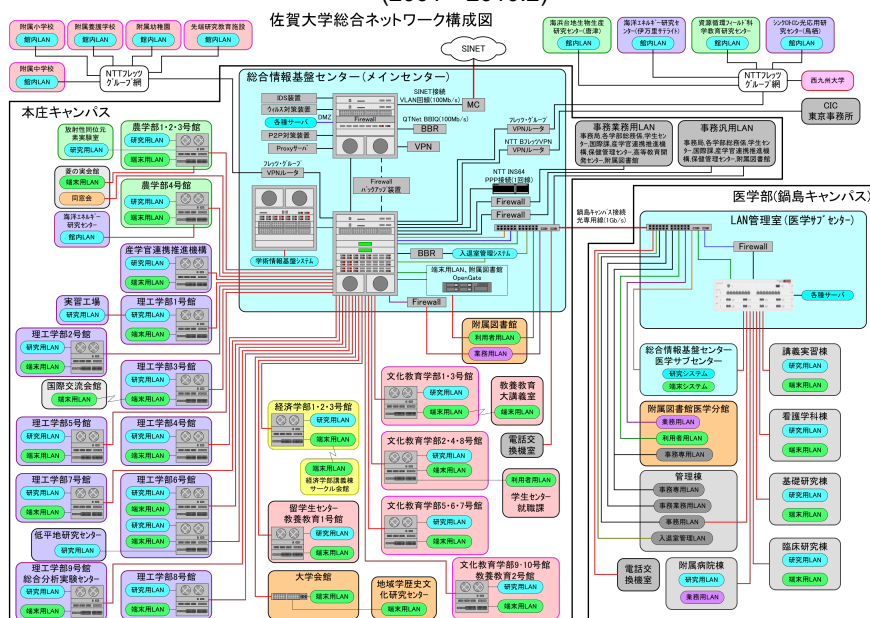
2012年2月11日

オープンソースカンファレンス2012 in Oita



(2001～2010.2)

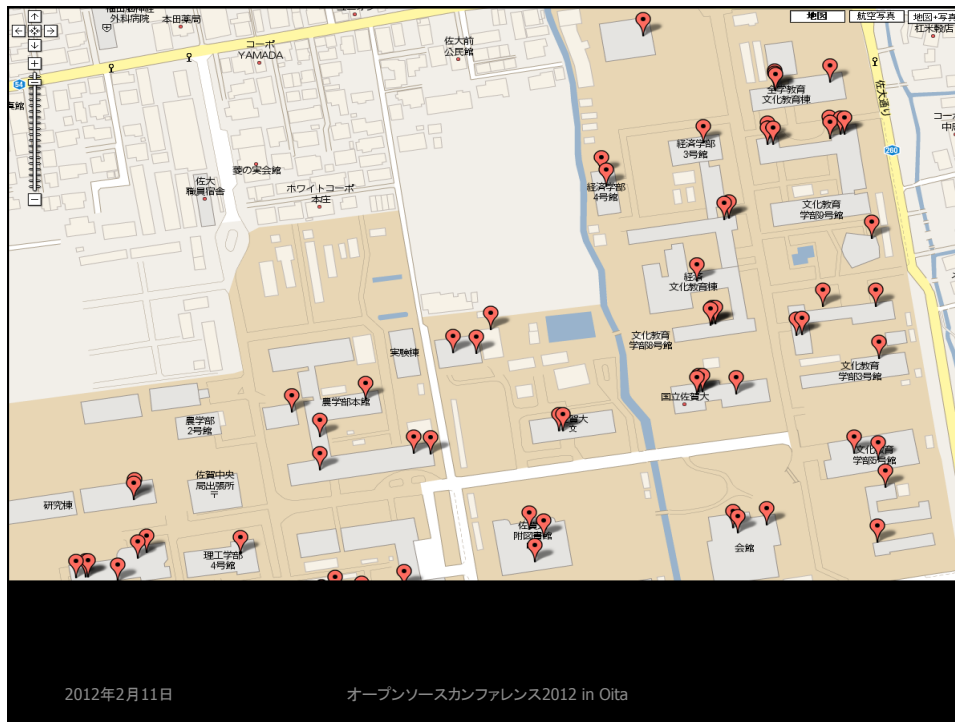
佐賀大学総合ネットワーク構成図



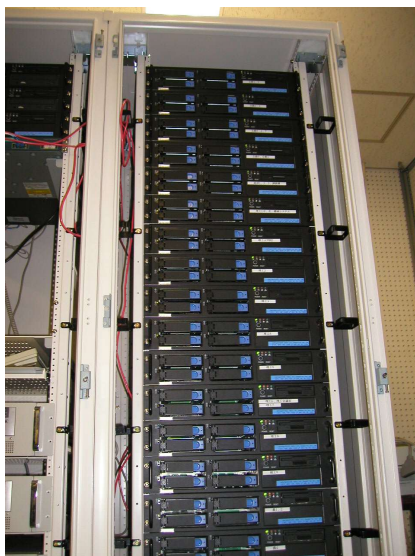
2012年2月11日

オープンソースカンファレンス2012 in Oita





ハードウェア (2001～2010.2)



- Pentium III 1GHz
- 1建物に1台程度
合計22台
- ディスクレスで運用
 - PXE boot

佐賀大学来訪者用ネットワーク利用申込書

ユーザID: ユーザ名が記されている

受付年月日: 年 月 日

利用期間: 年 月 日 ~ 年 月 日

申込者住所:
(or 所属組織名)

申込者電話番号:

申込者氏名(自署):

佐賀大学来訪者用ネットワーク利用許可書

ユーザID ユーザ名とパスワードが
パスワード 記されている

無線LAN SSID ogwap ☆☆ (☆の部分は数字またはなし)

このユーザID及びパスワードの申込利用期間中有効です。

● 利用上の注意事項
以下のことに注意してください。

ー 禁止事項

1. 申請者以外の利用
2. 営利目的の利用
3. 犯罪・反社会的目的の利用
4. 人権侵害・著作権侵害など他人の権利を侵害する利用
5. 悪戯など公序良俗に反する利用
6. 他人に物的・精神的被害を与える利用
7. システムに正常な運用を妨げる利用

適切でない行為があった場合には、利用の停止、その他の処分を行うことがあります。

また、佐賀大学キャンパス情報ネットワーク利用倫理規程
(<http://www.cc.saga-u.ac.jp/outline/rules.htm>) に従ってください。

記載された個人情報、本システムの運用・管理以外の目的には使用しません。

学外者(一時利用者)用申請書

申請者が記入

ここで切り取り、下半分を渡す
上半分は大学で保管

学会や研究会を開催するとき
とても便利！


国立大学法人 SAGA UNIVERSITY
佐賀大学


2012年2月11日
オープンソースカンファレンス2012 in Oita

OpengateとIPv6

- 背景
 - ー 1997年からIPv6に取り組んでいた
 - ー KAMEから始めてDVTS+JGNで遠隔授業
 - ー 工業高校でIPv6
- デュアルスタックの普及(2004頃)
 - ー Windows、MacOS、各種UNIX
- 端末用LANをIPv6対応に
 - ー OpengateのIPv6対応

2012年2月11日

オープンソースカンファレンス2012 in Oita



OpengateのIPv6対応

- ひとつの端末がIPv6とIPv4両方を使う
 - 利用者端末のIPv4/IPv6両方のアドレスを取得
 - 認証後はIPv4/IPv6両方の通信を可能にする
 - 利用終了時はIPv4/IPv6両方を閉鎖する
- 複数のIPv6アドレスを持つ
 - 認証時に取得したIPv6アドレスとは異なるアドレスを使うことがある
 - 認証時に用いられなかったIPv6アドレスを知る

2012年2月11日

オープンソースカンファレンス2012 in Oita



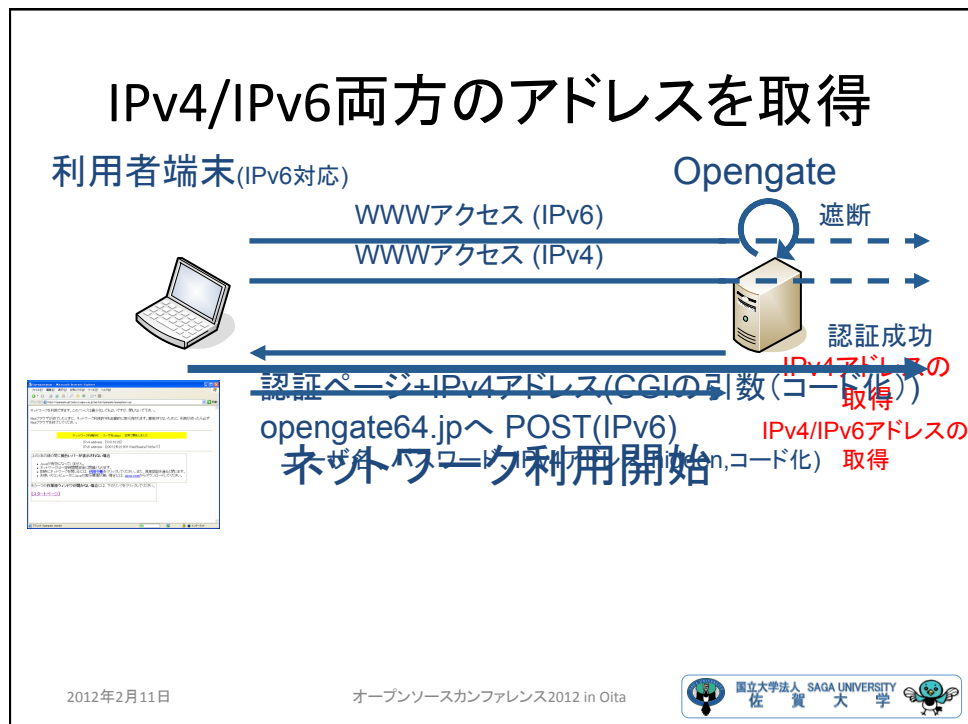
IPv4/IPv6両方のアドレスを取得

- Opengate をIPv4/IPv6で設定
 - DHCP (IPv4)、RA (IPv6)
- IPv4/IPv6アドレスの両方をDNSに登録
 - opengate64.jpに対してAとAAAAを登録
- Webブラウザの挙動
 - 相手がIPv6なら先にIPv6を試して失敗したらIPv4

2012年2月11日

オープンソースカンファレンス2012 in Oita





複数のIPv6アドレスを持つ

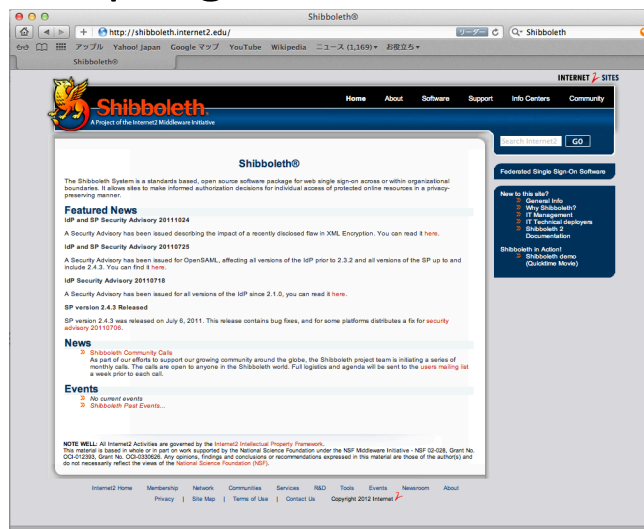
- どのような場合に？
 - マルチホーム
 - Windowsの匿名アドレス
- 認証時に用いられなかったIPv6アドレス
 - NDP (Neighbor Discovery Protocol) エントリを監視
 - MACアドレスに対応するIPv6アドレス
 - 新たなIPv6アドレスを発見したら通信路を解放

2012年2月11日

オープンソースカンファレンス2012 in Oita



OpengateとShibboleth

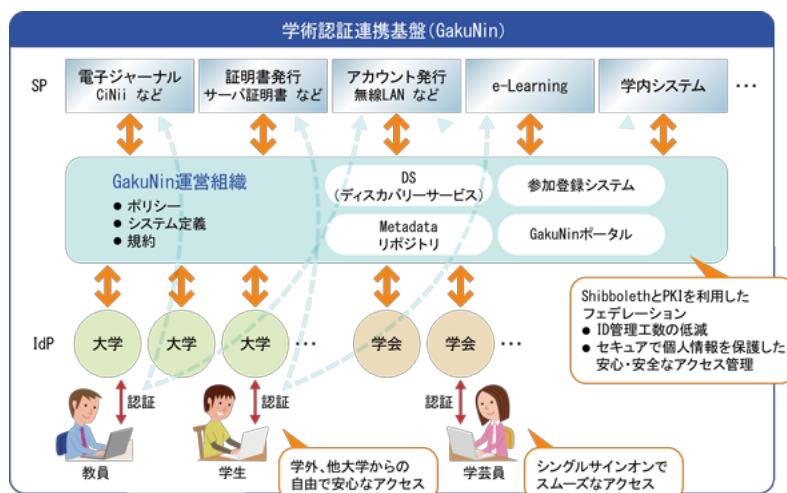


2012年2月11日

オープンソースカンファレンス2012 in Oita



国立情報学研究所「学認」



<http://www.gakunin.jp/docs/fed> より引用

2012年2月11日

オープンソースカンファレンス2012 in Oita

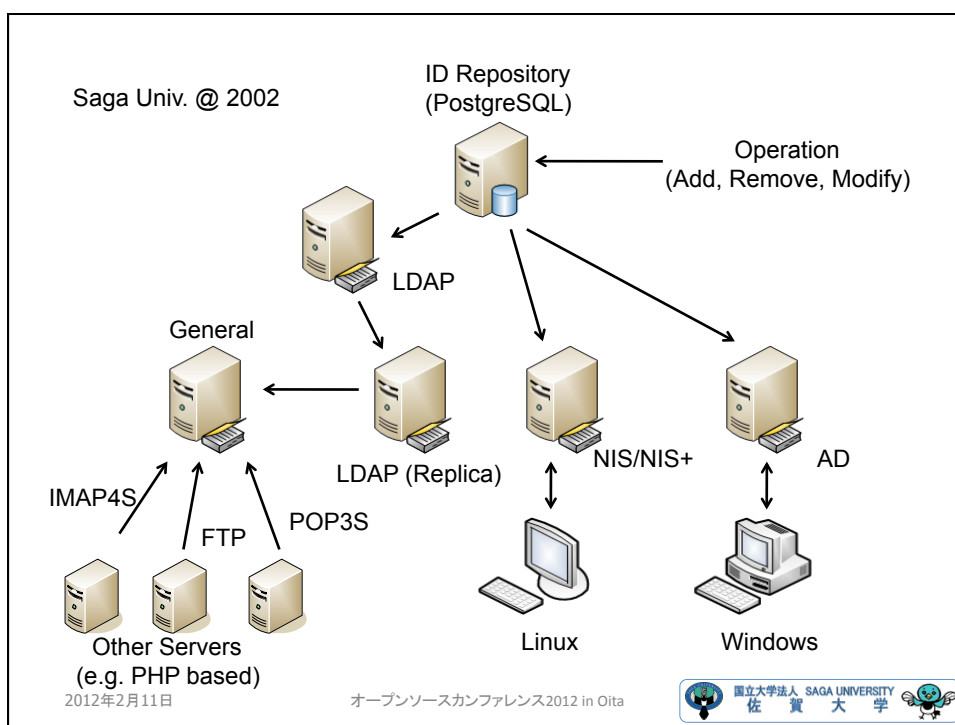


シングルサインオンの必要性

- Webベースシステムの増加
 - 教務システム
 - オンラインシラバス
 - e-Learning（佐賀大学ネット授業ではMoodle）
 - Opengate
- 統合認証システム
 - ユーザIDとパスワードを一括管理
 - 同じユーザIDとパスワードを何度も入力
- Opengateが定着している！
 - Shibbolethに対応させよう

2012年2月11日

オープンソースカンファレンス2012 in Oita



2012年2月11日

オープンソースカンファレンス2012 in Oita



Shibboleth

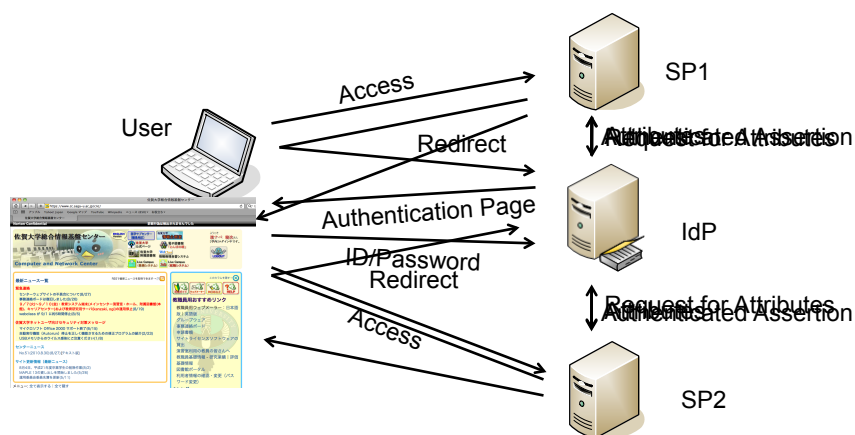
- IdP (Identity Provider)
 - 認証サーバ
 - 認証機能、SPに対して属性情報を提供
- SP (Service Provider)
 - 認証付Webアプリケーション
 - simpleSAMLphp, Apache with mod_shibboleth
- DS (Discovery Service)
 - IdP のセレクト

2012年2月11日

オープンソースカンファレンス2012 in Oita



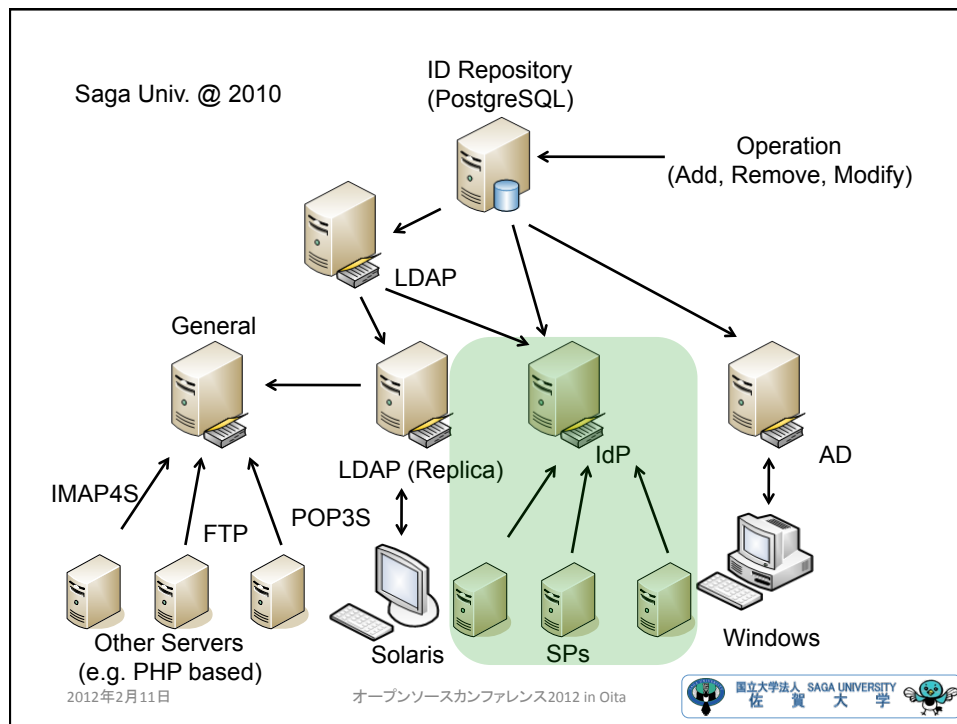
Work Flow of Shibboleth



2012年2月11日

オープンソースカンファレンス2012 in Oita

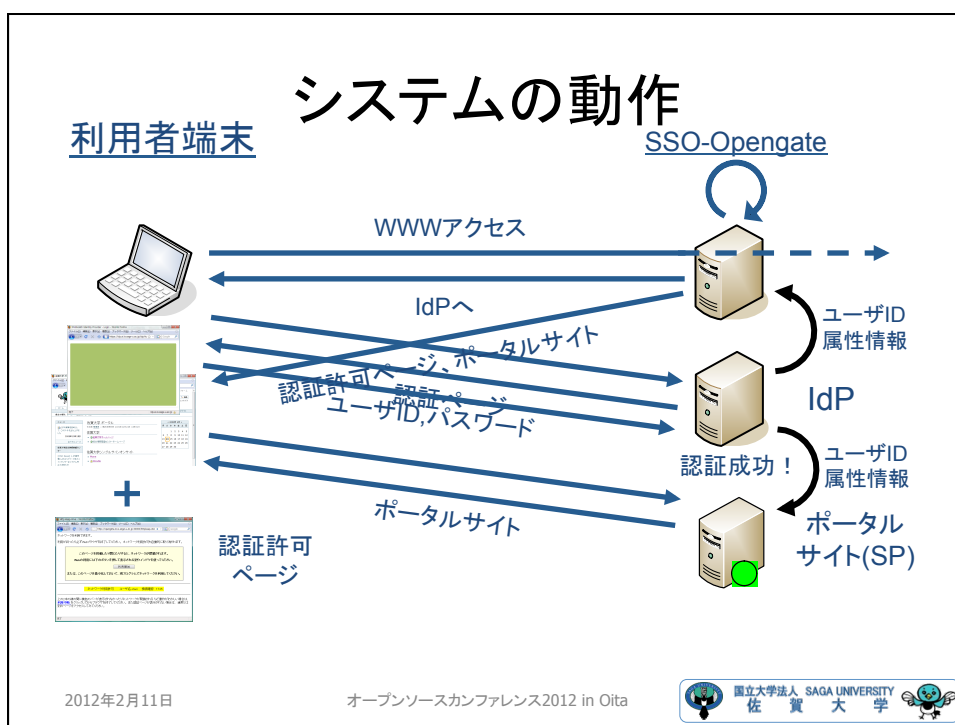
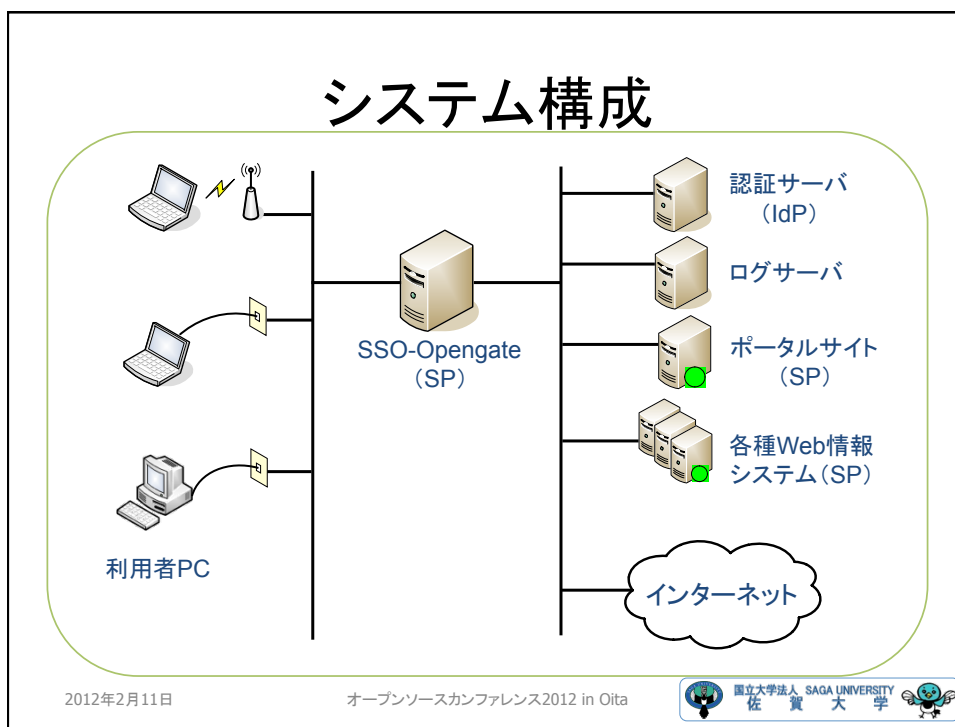




SSO-Opengate

- Web利用時に強制的に認証ページを表示
- 認証に成功すると許可(利用監視)ページの表示
- 認証を行ったブラウザを閉じるまでネットワークが利用可

基本動作は、Opengateと同じ
Shibboleth 的にはSPになる



SSOに対応したサービス

- SSO-Opengate
- 図書館ポータル
- 図書館蔵書検索
- 教職員グループウェア
- 教務ポータル、教務システム
- 佐賀大学e-Learningシステム
- 総合情報基盤センターホームページ
- ユーザパスワード変更
- 研究業績データベース
- 教職員基礎情報データベース
- 教員評価報告様式
- WWWSSO

2012年2月11日

オープンソースカンファレンス2012 in Oita



来学者用の無線LAN

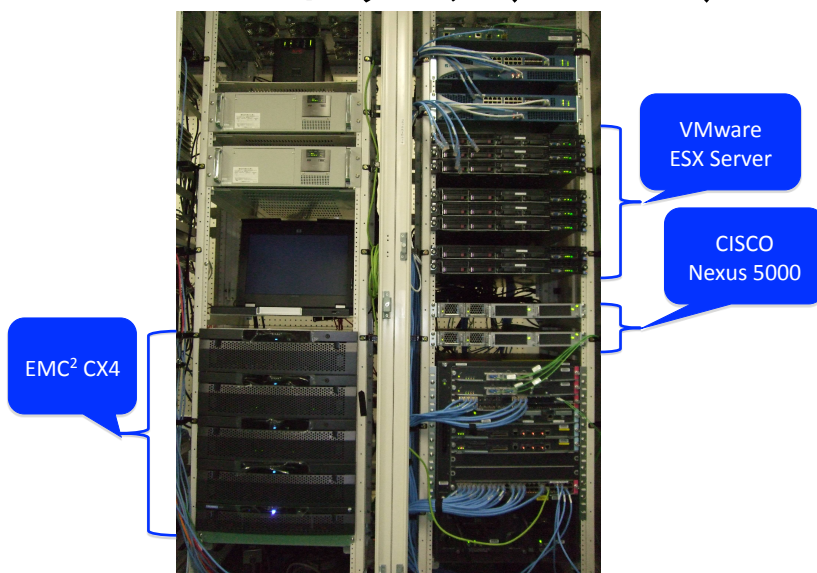
- ゲスト用のSSID
- ブラウザを起動するとDSが表示される
- 「学認」参加機関は自分のIdPで認証可能
- 佐賀大学に来られれば体験可能！

2012年2月11日

オープンソースカンファレンス2012 in Oita



ハードウェア(2010～)



2012年2月11日

オープンソースカンファレンス2012 in Oita



物理マシン1台で運用

HN-CN1-VCN01 ~ vSphere Client

ファイル (E) 編集 (E) 表示 (W) インベントリ (N) 管理 (A) プラグイン (P) ヘルプ (H)

ホーム インベントリ ホストおよびクラスター 検索 インベントリ

hn-cn1-esx03.net.cc.saga-u.ac.jp VMware ESX, 4.0.0, 208167

はじめに サマリ 仮想マシン フォーマット 構成 タスクおよびイベント アラーム 権限 マップ ストレージ ビュー Hardware Status

名前、状態または ゲスト OS に次の内容を含む: クリア

名前	状態	ステータス	使用領域	ホスト CPU - MHz	ホスト メモリ - MB	ゲスト メモリ - %	メモ	アラーム	アクション
Opengate01	パワーオン	標準	34.00 GB	278	2087	19	Opengate (文化教育学部/教養教育)	有効	
Opengate02	パワーオン	標準	34.00 GB	75	1676	15	Opengate (経済学部)	有効	
Opengate03	パワーオン	標準	38.13 GB	861	1821	30	Opengate (理工学部)	有効	
Opengate04	パワーオン	標準	34.00 GB	227	1747	43	Opengate (農学部)	有効	
Opengate05	パワーオン	標準	34.00 GB	227	2083	16	Opengate (医学部)	有効	
Opengate06	パワーオン	標準	34.00 GB	177	1597	9	Opengate (運動施設)	有効	
Opengate07	パワーオン	標準	34.00 GB	75	1226	11	Opengate (その他施設)	有効	
Opengate08	パワーオン	標準	34.00 GB	101	1150	5	Opengate (事務局)	有効	
Opengate09	パワーオン	標準	37.74 GB	151	1687	12	Opengate (学芸)	有効	
Opengate10	パワーオン	標準	34.00 GB	75	1775	13	Opengate (図書館)	有効	

タスク アラーム Administrator

2012年2月11日

オープンソースカンファレンス2012 in Oita



SSO-Opengateの物理構成

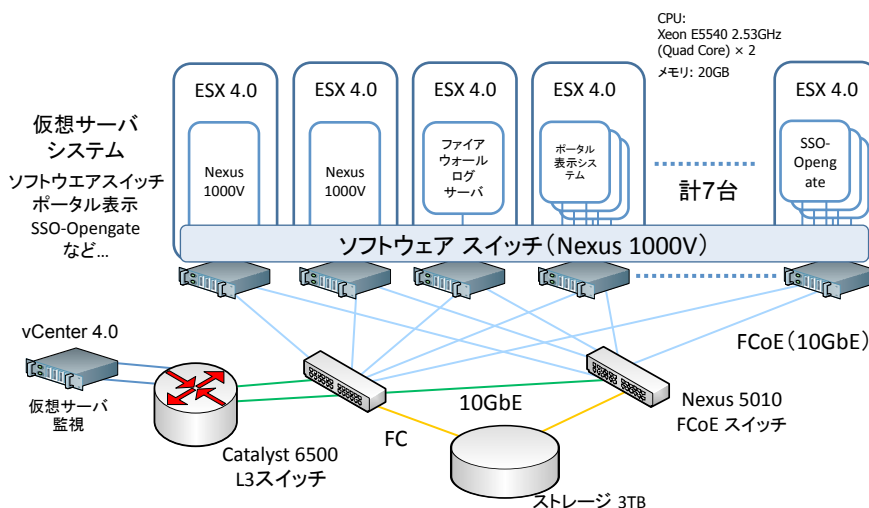
- SSO対応に合わせ、システムを仮想化
 - 組織毎に1台のSSO-Opengateが稼働(現在10台)
- 仮想システム(VMware ESX) 上で動作
 - ESX サーバ ×7 台 (1台でSSO-Opengateが複数動作)
 - OS: VMware ESX 4.0 Enterprise Plus
 - CPU: Xeon E5540 2.53GHz Quad Core ×2
 - Memory: 20GB
 - Guest OS: FreeBSD 6.4-RELEASE
 - SSO-Opengate (従来システムの仮想化 + SSO)

2012年2月11日

オープンソースカンファレンス2012 in Oita



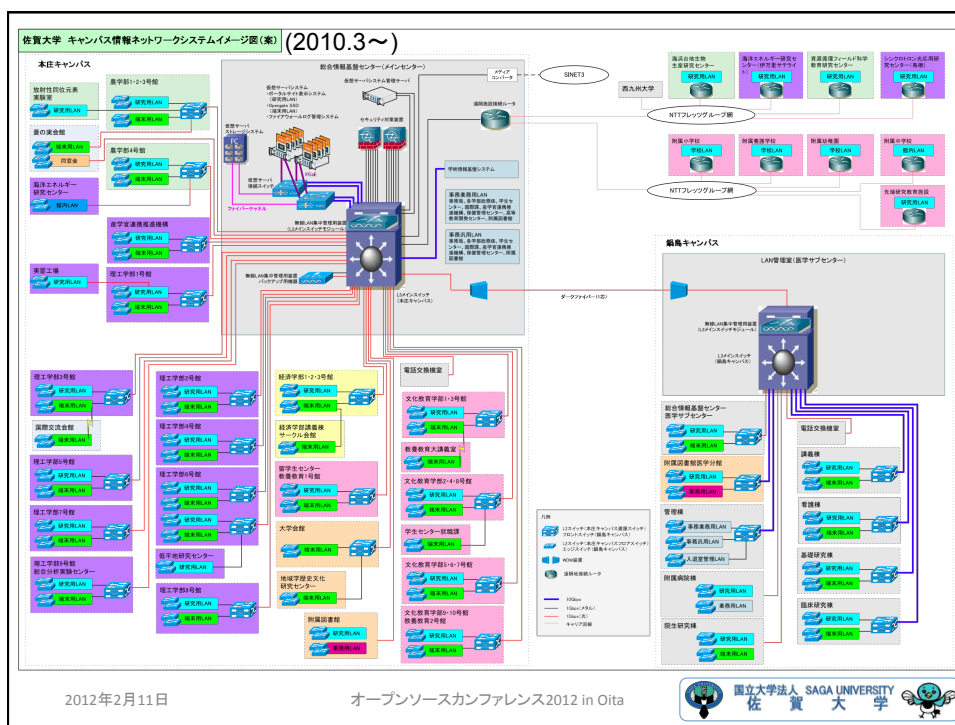
VMware を用いた仮想システム イメージ図



2012年2月11日

オープンソースカンファレンス2012 in Oita





なぜ自ら開発するのか？

- 新しい技術を速やかに取り入れることができる
 - IPv6
 - Shibboleth
- 大学のミッション
 - 研究
 - 教育
- 大学の評価

今やアプライアンスも多い



2012年2月11日

オープンソースカンファレンス2012 in Oita

査読付論文

- 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、渡辺義明、渡辺健次、江藤博文、只木進一、情報処理学会論文誌、Vol.42、No.12、pp.2802-2809(2001.12)
- 利用者移動端末に対応した大規模ネットワークのOpengateによる構築と運用、只木進一、江藤博文、渡辺健次、渡辺義明、情報処理学会論文誌、Vol.46、No.4、pp.922-929(2005.4)
- 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、大谷誠、江口勝彦、渡辺健次、情報処理学会論文誌、Vol.47、No.4、pp.1146-1156(2006.4)
- 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)
- シングルサインオンに対応したネットワーク利用者認証システムの開発、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. 51、No. 3、pp. 1031 – 1039 (2010.3)

2012年2月11日

オープンソースカンファレンス2012 in Oita



教育

- 2010年度の卒業論文、修士論文
 - Opengateへの補助認証システムの導入
 - 認証ゲートウェイの仮想化
 - Opengateの管理者用システム開発
 - Opengateと連動した無線LAN利用者監視システムの開発
- 講義「情報ネットワーク」(渡辺健次担当)
 - 講義の総括にOpengateの仕組みを説明

2012年2月11日

オープンソースカンファレンス2012 in Oita



大学の評価

8-1-② 大学において編成された教育課程の遂行に必要なICT環境が整備され、有効に活用されているか。

総合情報基盤センターによる情報化支援、機能的管理・運用により、学内の各建物及びキャンパス間のネットワークシステムを構築し、ほぼすべての教室・自習スペースに無線LAN局（約300機）及び情報コンセント（約980口）を設置し、当該大学独自開発の「Opengate」（ネットワーク利用認証システム）等を介して、学生・教職員がパソコンをインターネット接続できる環境を提供している。また、全学的に学生用パソコンを設置し、情報処理教育、専門教育、履修登録、文献蔵書検索など、授業・自習に活用している。附属図書館にも無線LAN局及び情報コンセントを設置し、学生・教職員がパソコンをインターネット接続できる環境を整備している。総合情報基盤センターに設置されたパソコン（325台）は、授業以外の時間帯には、学生の自主的な学習活動に利用でき、大学院学生のセンター相談員を配置して利用支援を行っている。

2012年2月11日

認証評価(学位授与機構)

オープンソースカンファレンス2012 in Oita



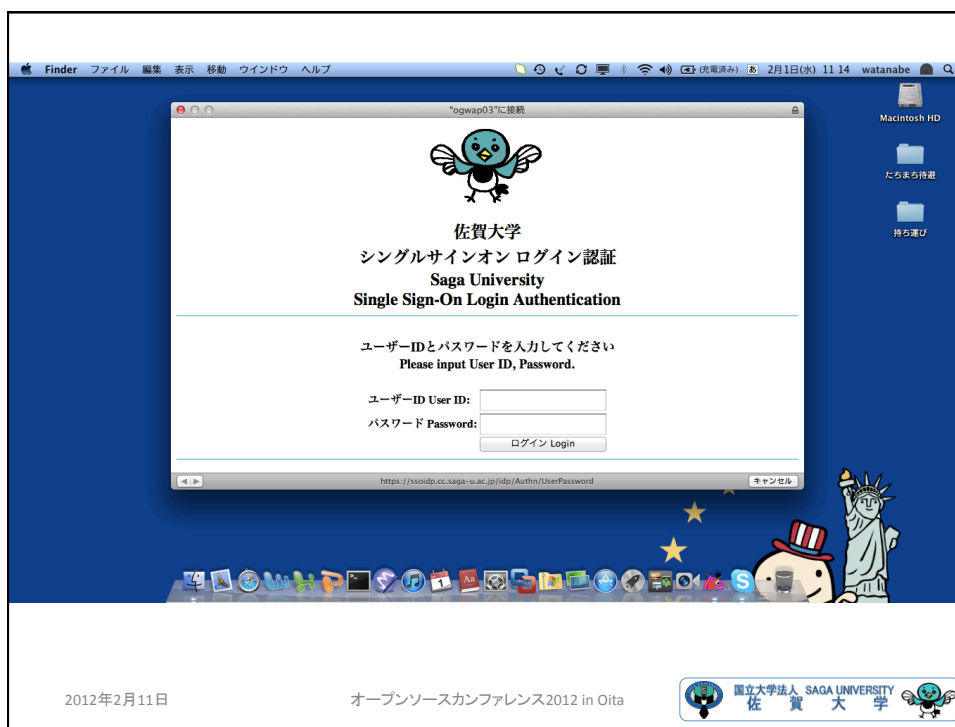
Opengateの今後

- スマートフォンの増加
 - － 節電モードで無線インタフェースがOFFになる
 - － TCPが切れてOpengateが通信路を閉鎖してしまう
- MacOS LION
 - － iOSと同じような認証ウィンドウ
 - － 認証後、認証ウィンドウは閉じてしまう
 - － TCPが切れてOpengateが通信路を閉鎖してしまう

2012年2月11日

オープンソースカンファレンス2012 in Oita





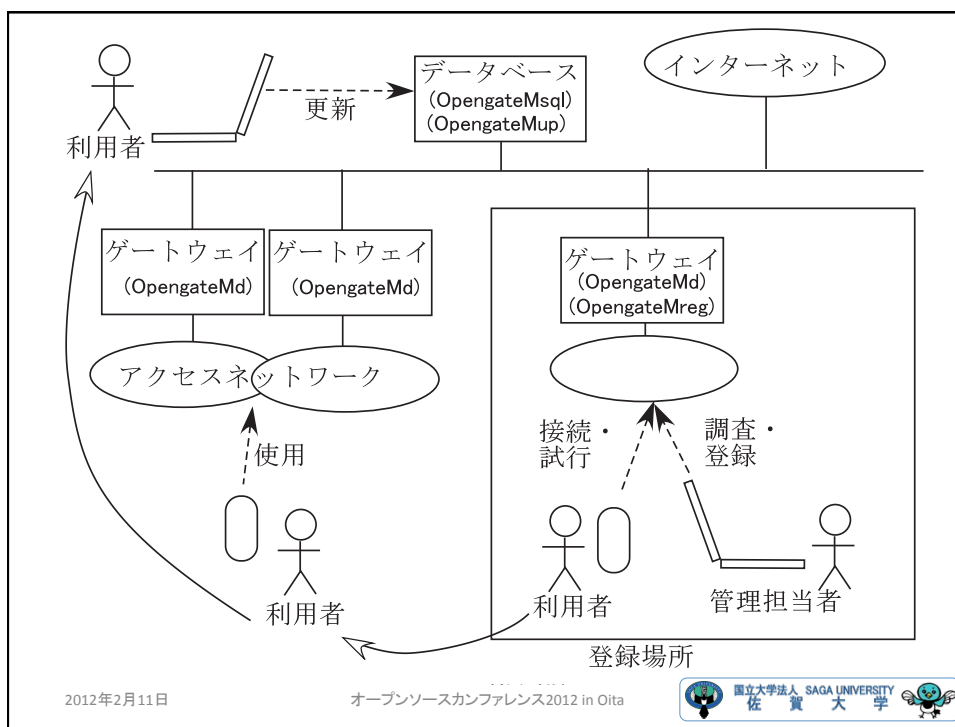
OpengateM

- MACアドレス登録方式
 - 事前にユーザIDとMACアドレスを登録
- 利用
 - 利用者が使用を開始すると、デーモンがMACアドレスを確認して、ファイアウォールに通過ルールを挿入
 - 一定時間ネットワーク利用が無いと、デーモンがファイアウォールから通過ルールを削除
- 更新
 - 一定期間経つと利用期限が切れる。警告メールが届く。
 - 利用者はWebにより更新処理を行う

2012年2月11日

オープンソースカンファレンス2012 in Oita



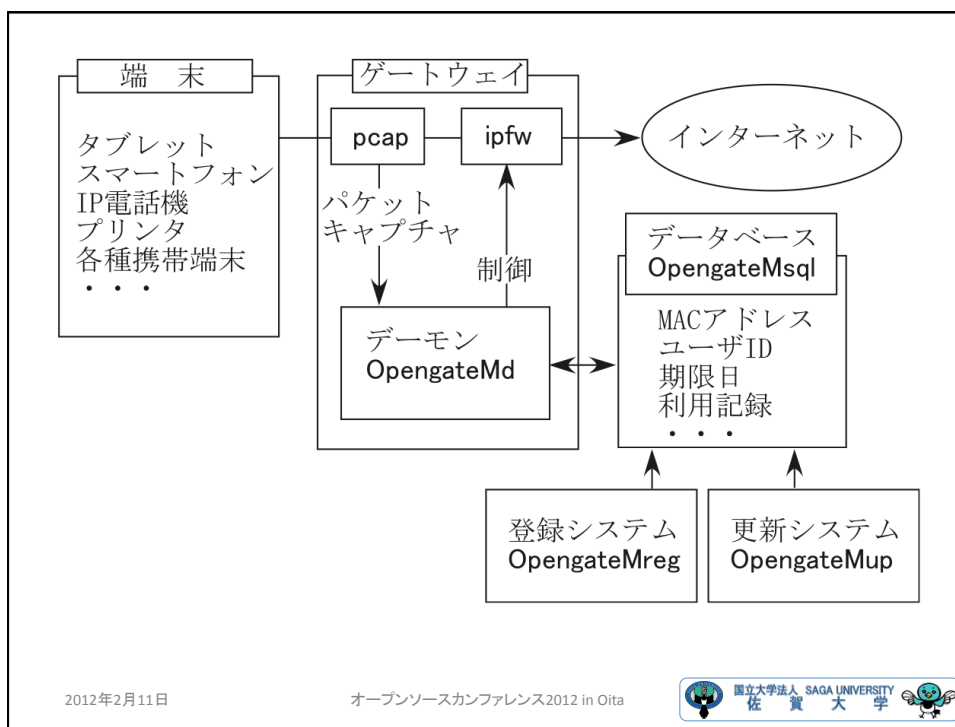


インタフェース

2012年2月11日

オープンソースカンファレンス2012 in Oita

国立大学法人 SAGA UNIVERSITY
佐賀大学



OpengateMを IOT研究会で発表します

- 渡辺義明、大谷誠、江藤博文、只木進一、渡辺健次: “Opengateを補完するMACアドレス認証システム OpengateM”, 情報処理学会インターネットと運用技術研究会(IOT研究会), 北海道大学, 2012.3.15-16.

2012年2月11日

オープンソースカンファレンス2012 in Oita



まとめ

- 自己紹介
- 無線LANの展開(1999年頃)
- ネットワーク利用者認証システムOpengate
- OpengateとIPv6
- OpengateとShibboleth
- なぜ自ら開発するのか？
- Opengateの今後

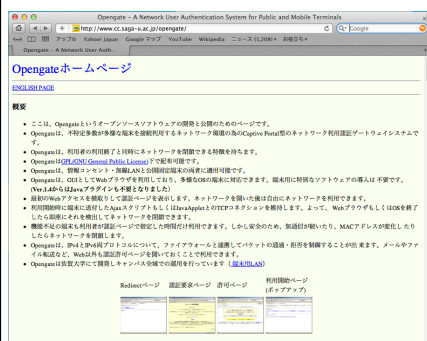
2012年2月11日

オープンソースカンファレンス2012 in Oita



詳しくは

- Opengateホームページ
 – <http://www.cc.saga-u.ac.jp/opengate/>
 – ソースコードあります



2012年2月11日

オープンソースカンファレンス2012 in Oita

