Ｏｐｅｎｇａｔｅ とＰＫＩ の連携

藤澤 優　（佐賀大学大学院　工学系研究科）
大谷 誠　（佐賀大学　総合情報基盤センター）
渡辺 健次（佐賀大学理　理工学部）

発表 の 流れ

1. 研究の背景 ･目的
2. Opengateについて
3. Opengate-PKIのシステム構成
4. Opengate-PKIの利用

研究 の 背景

パスワードによる認証

PKI

ディジタル証明書による認証

研究 の 目的

UPKI (University PKI)

大学間連携のための全国共同電子認証基盤

証明書認証

＋

Opengate

パスワード認証

Ｏｐｅｎｇａｔｅ－Ｐ

Ｏｐｅｎｇａｔｅとは（1）

特定多数が多様な端末を接続利用する

ネットワーク環境のための

ネットワーク利用者認証ゲートウェイシステム

http://www.cc.saga-u.ac.jp/opengate/

佐賀大学全域で2001年より運用

Ｏｐｅｎｇａｔｅ とは ⑵

背景

- 公開端末 ･利用者端末などの利用要求
- ネットワーク利用時の トラブルの発生
- 学外ネットワークへの接続を制限
- 公開端末 ･情報コンセントへの適切な認証

目的

- 公開端末 ･利用者端末でのネットワーク利用認証
- トラブル時の個人特定

Ｏｐｅｎｇａｔｅ の機能

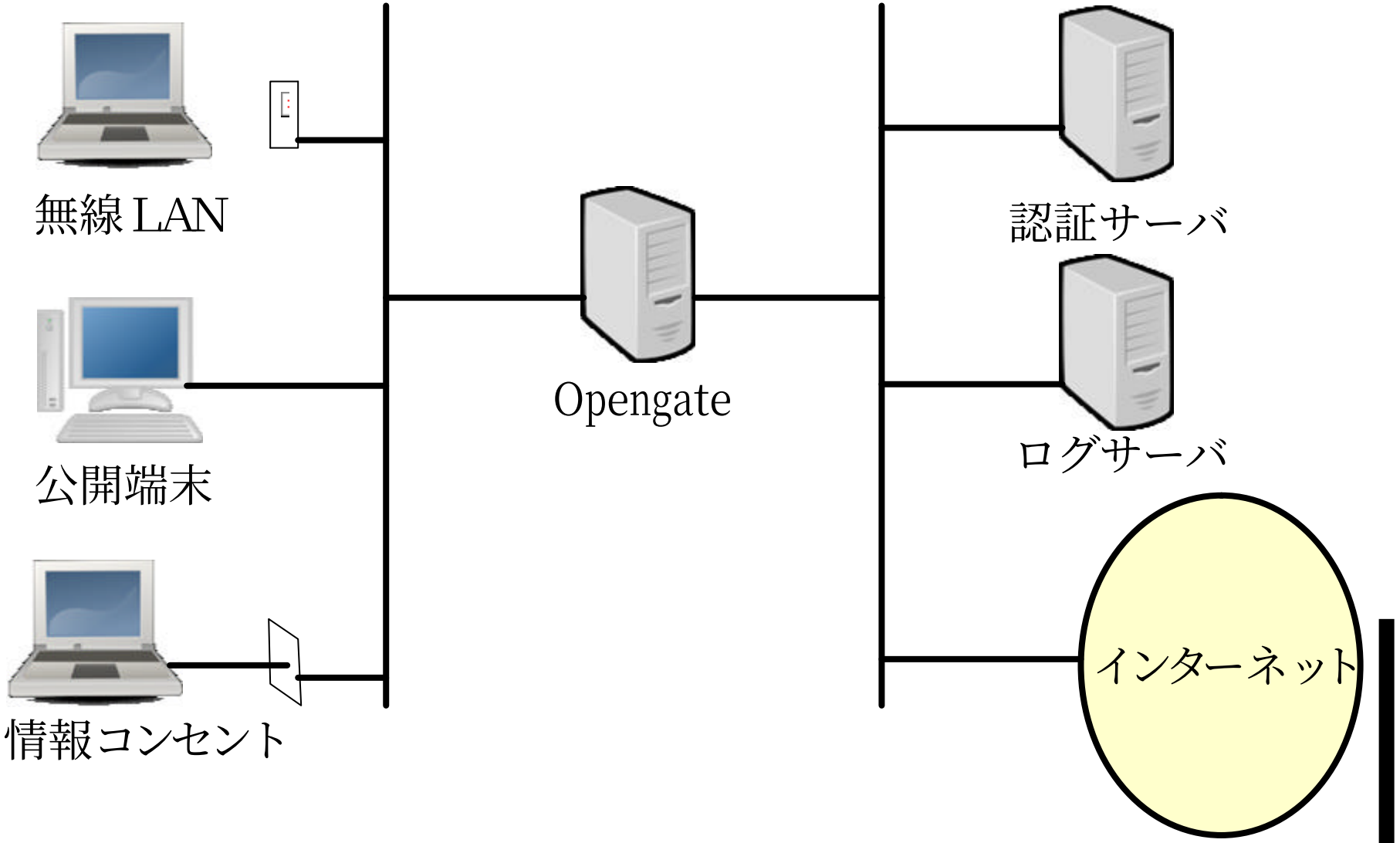
- ネットワーク利用者認証
  - 有資格者へのネットワーク解放
- ネットワーク利用終了検知
  - HTTP Keep-Alive(JavaScript)、JavaApplet
- ネットワーク利用記録
  - ネットワークの利用状況把握

Ｏｐｅｎｇａｔｅの特徴

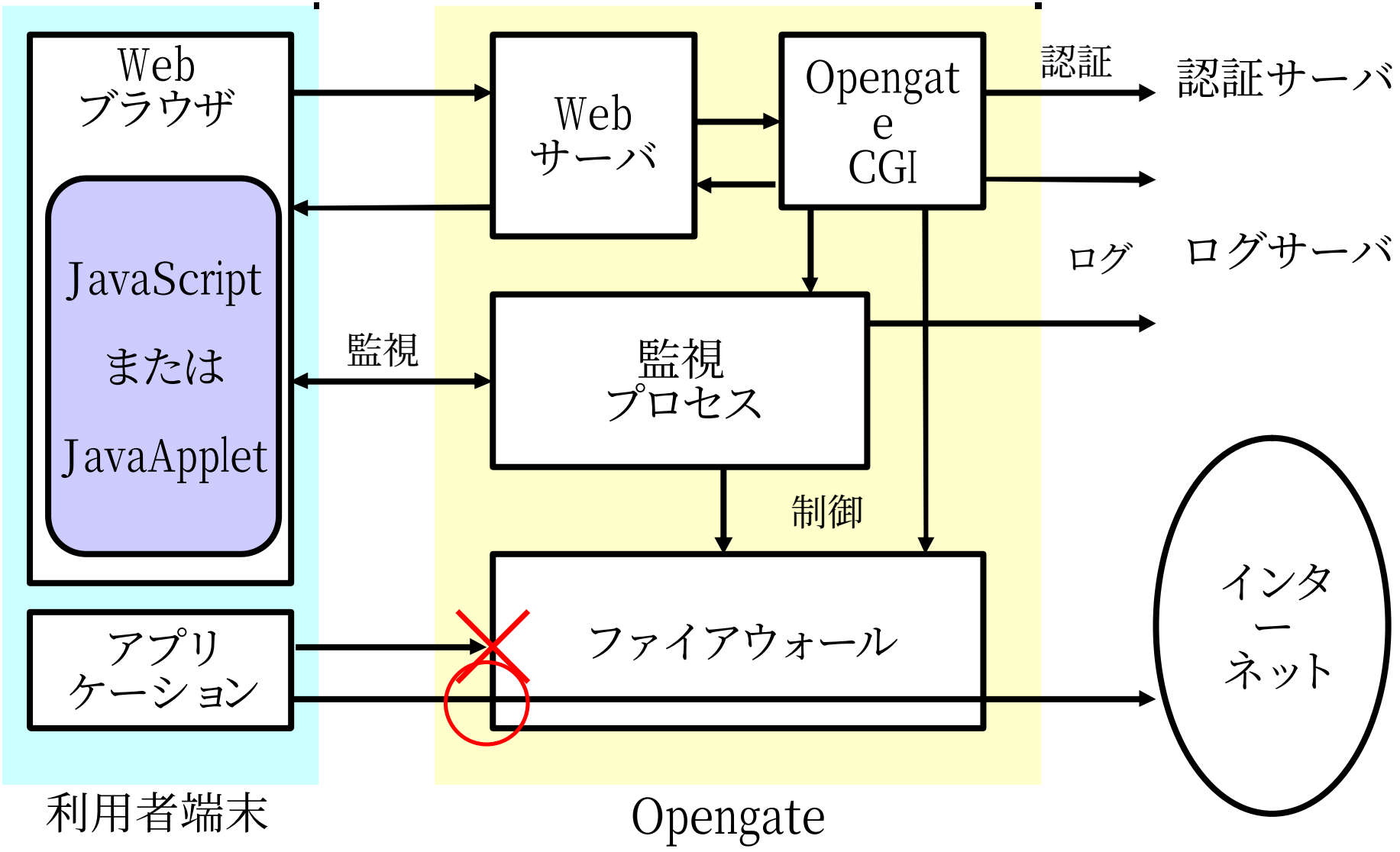
- ネットワーク環境(無線・有線)によらず動作
- GUIとしてWebブラウザを利用
- クライアントには付加ソフトが不要
- IPv4/IPv6の通信に対応

Ｏｐｅｎｇａｔｅ利用 の 流れ

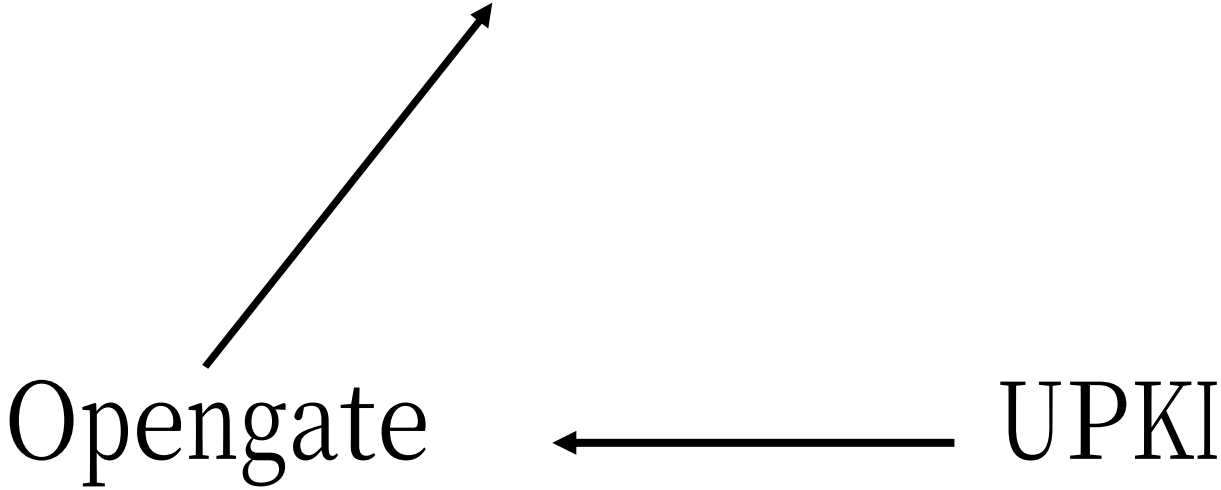
Ｏｐｅｎｇａｔｅ のシステム構



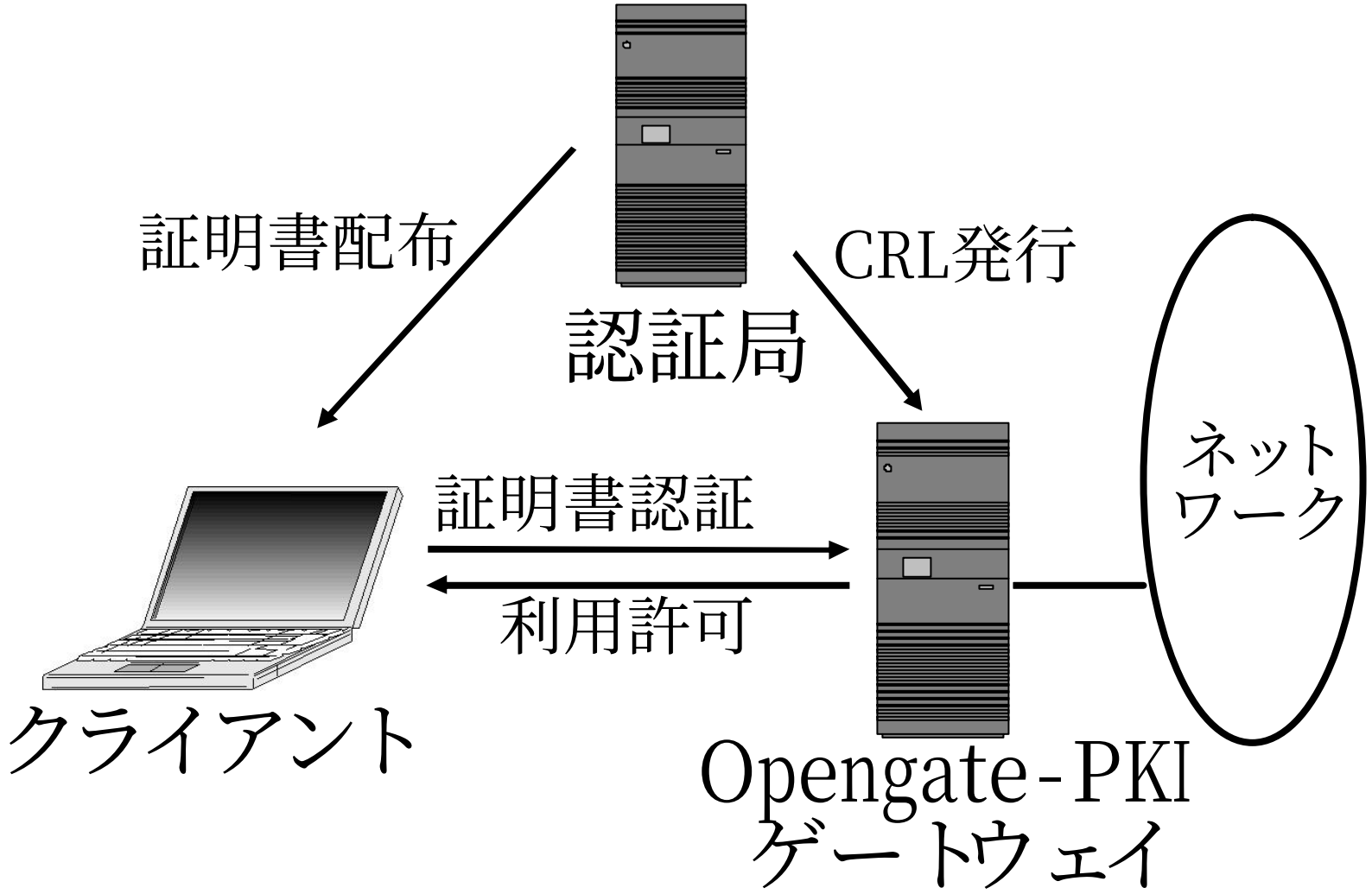
Ｏｐｅｎｇａｔｅ のソフトウェア



Opengate-PKI



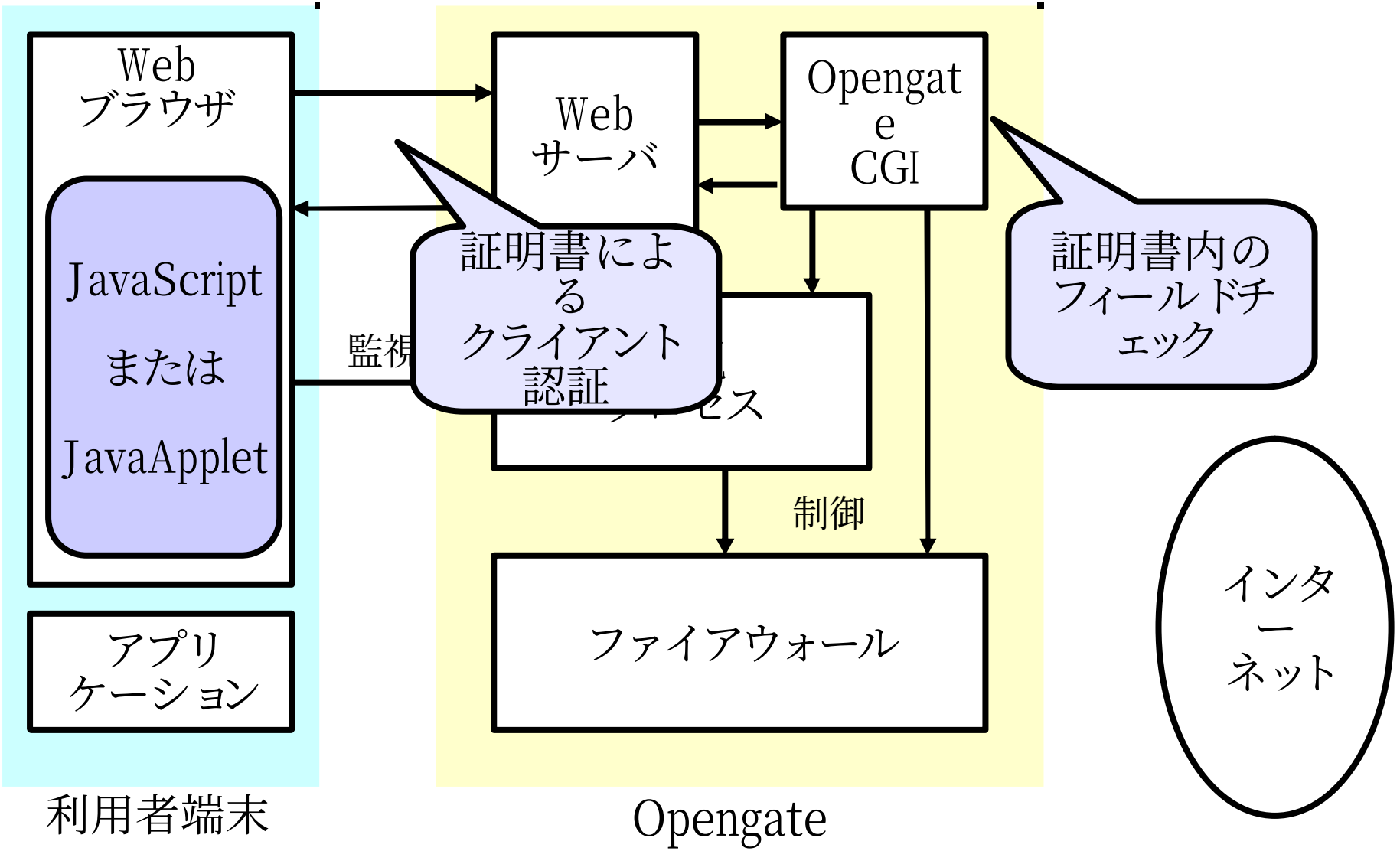
Ｏｐｅｎｇａｔｅ－ＰＫＩのシ



Ｏｐｅｎｇａｔｅからの変更点

1. ブラウザからの証明書の提出
2. Apacheによる証明書の確認
3. サーバプログラムで証明書取得
4. サーバプログラムでの証明書の確認

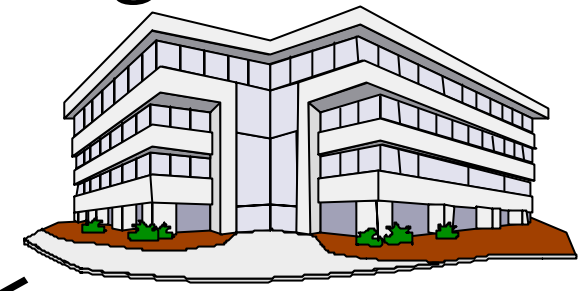
Ｏｐｅｎｇａｔｅからの変更点



Ｏｐｅｎｇａｔｅ－ＰＫＩのソフト

Opengate-PKI ゲートウェイ	
OS	FreeBSD
ファイアウォールソフト	ipfw,ip6fw
Webサーバ	Apache2.2以上
開発言語	C言語
クライアント	
Webブラウザ	証明書の認証に対応が必要 (IE6,7、Firefox、Operaなど)
認証局	
証明書・CRL発行	OpenSSL

Ｏｐｅｎｇａｔｅ－ＰＫＩの利



認証局

取得

証明書

インポート

Webページアクセス

認証
完了ページ

証明書提出

ネット
ワーク

ユーザ

ブラウザ

ゲート
ウェイ

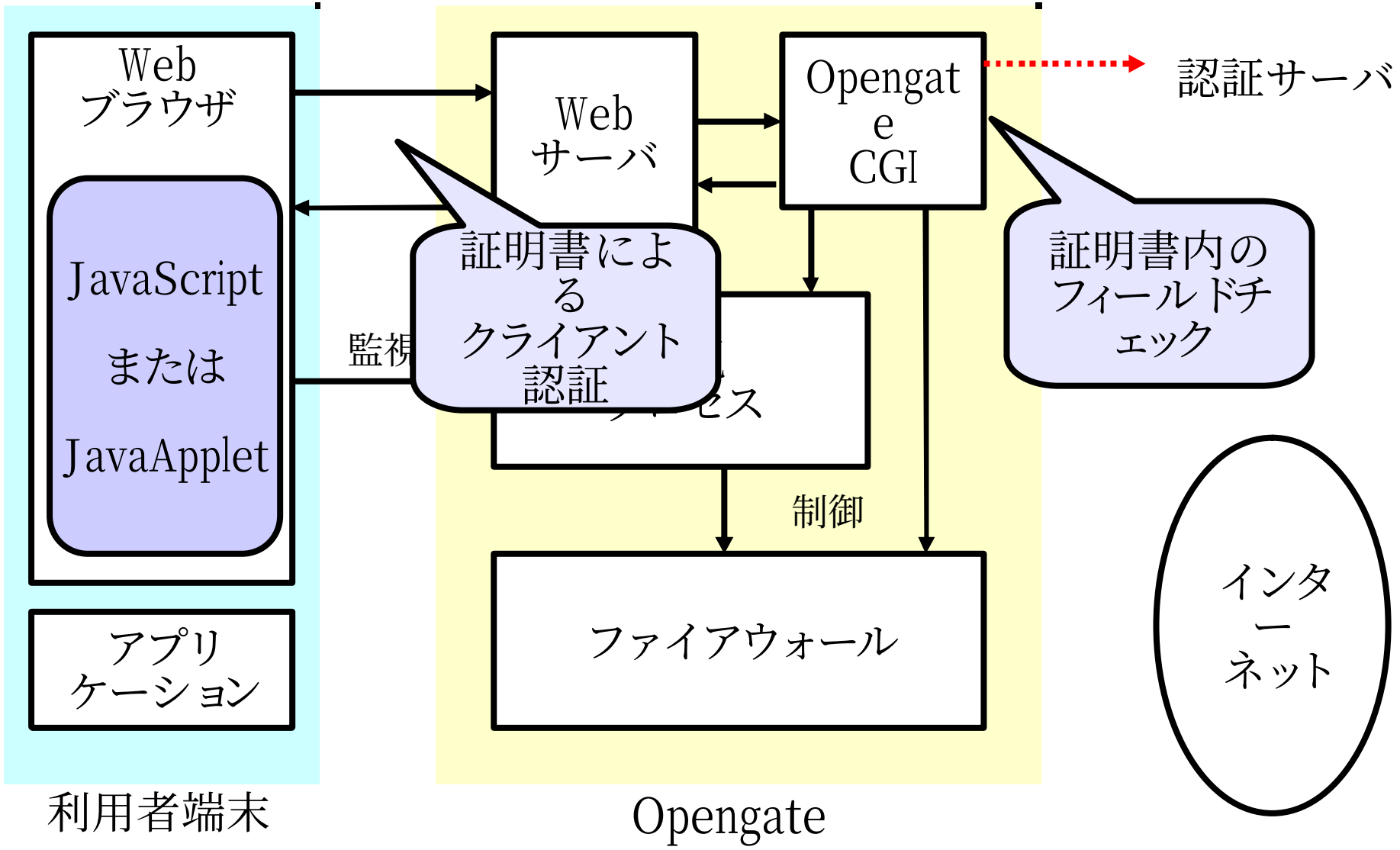
Ｏｐｅｎｇａｔｅ－ＰＫＩの

まとめ と今後 の 課題

ディジタル証明書による認証が可能な
Opengate-PKIを開発

- 認証サーバの分離
- 運用実験
- 証明書の自動認識、自動認証
- UPKIとの連携　(ICカードによる認証)

Ｏｐｅｎｇａｔｅからの変更点

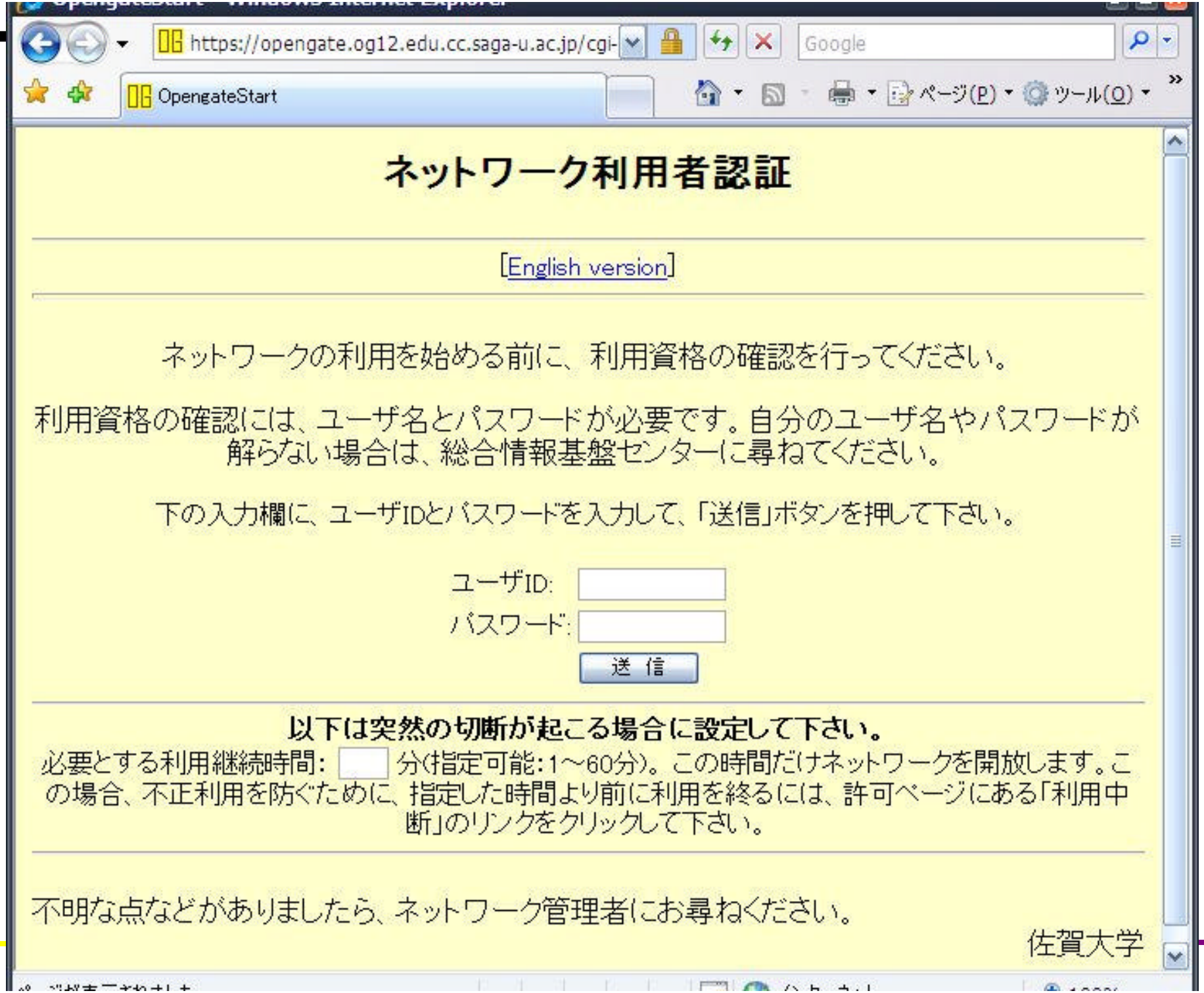


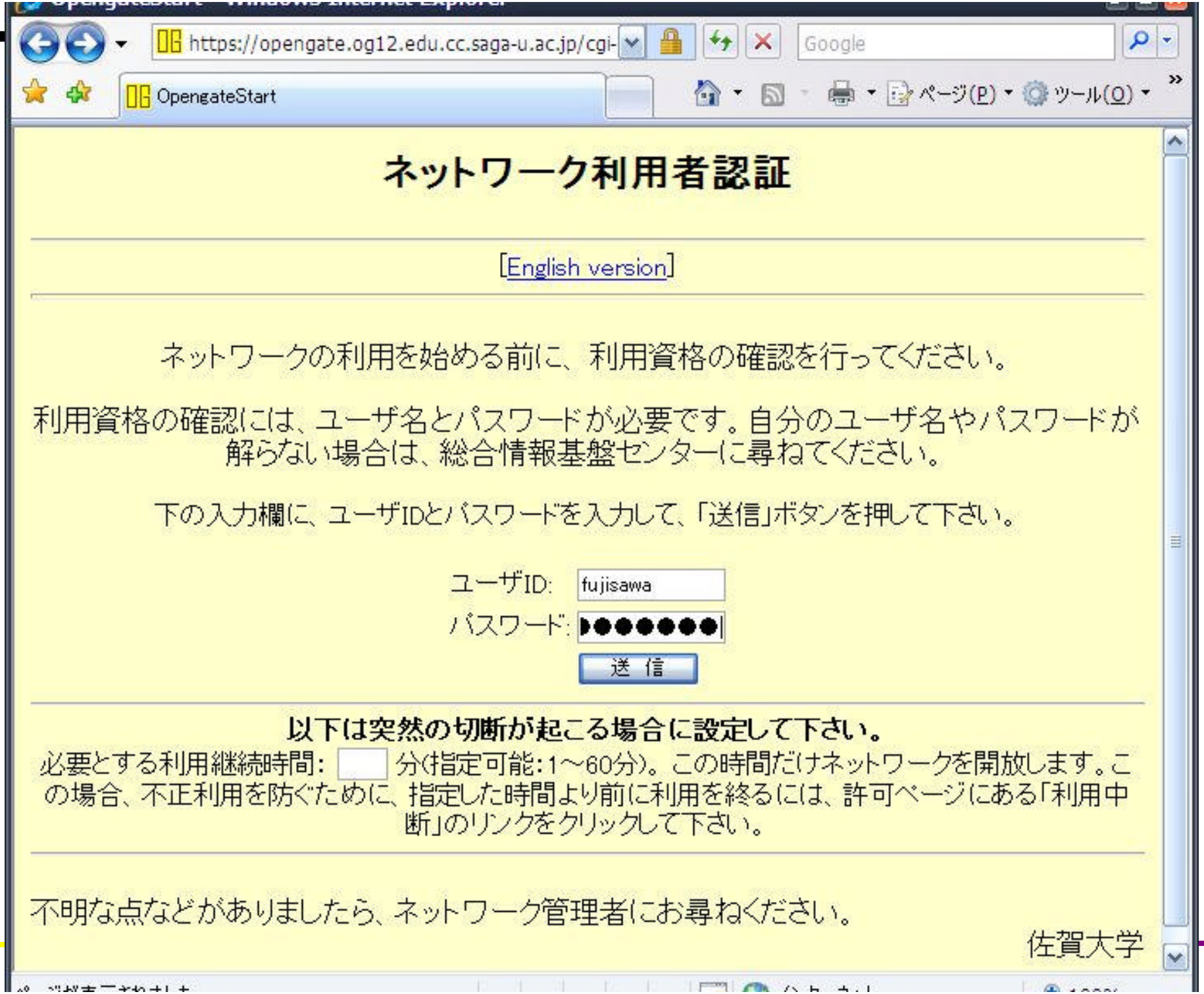
Opengate公式ページ

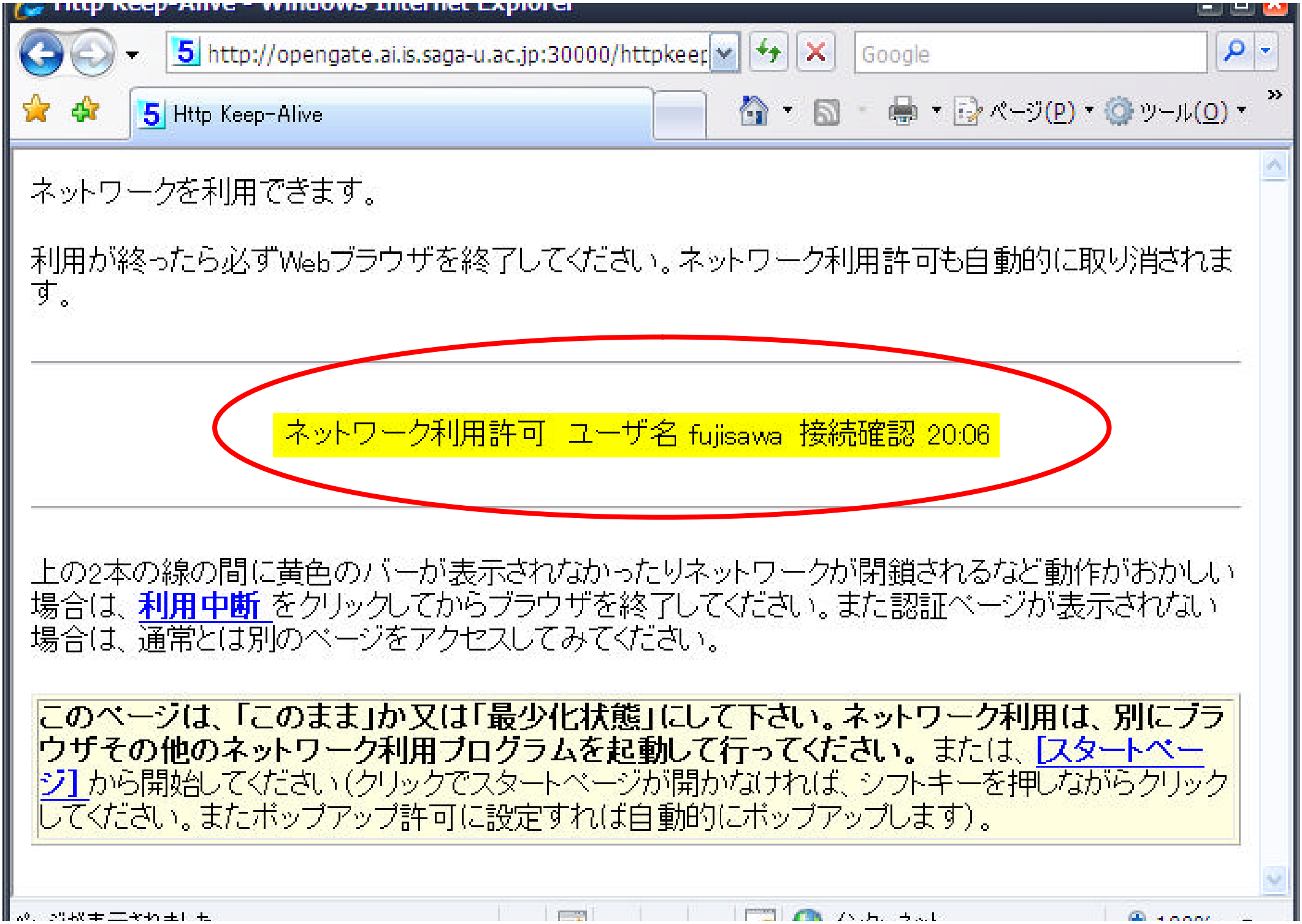
http://www.cc.saga-u.ac.jp/opengate/

Ｏｐｅｎｇａｔｅ利用 の 流れ

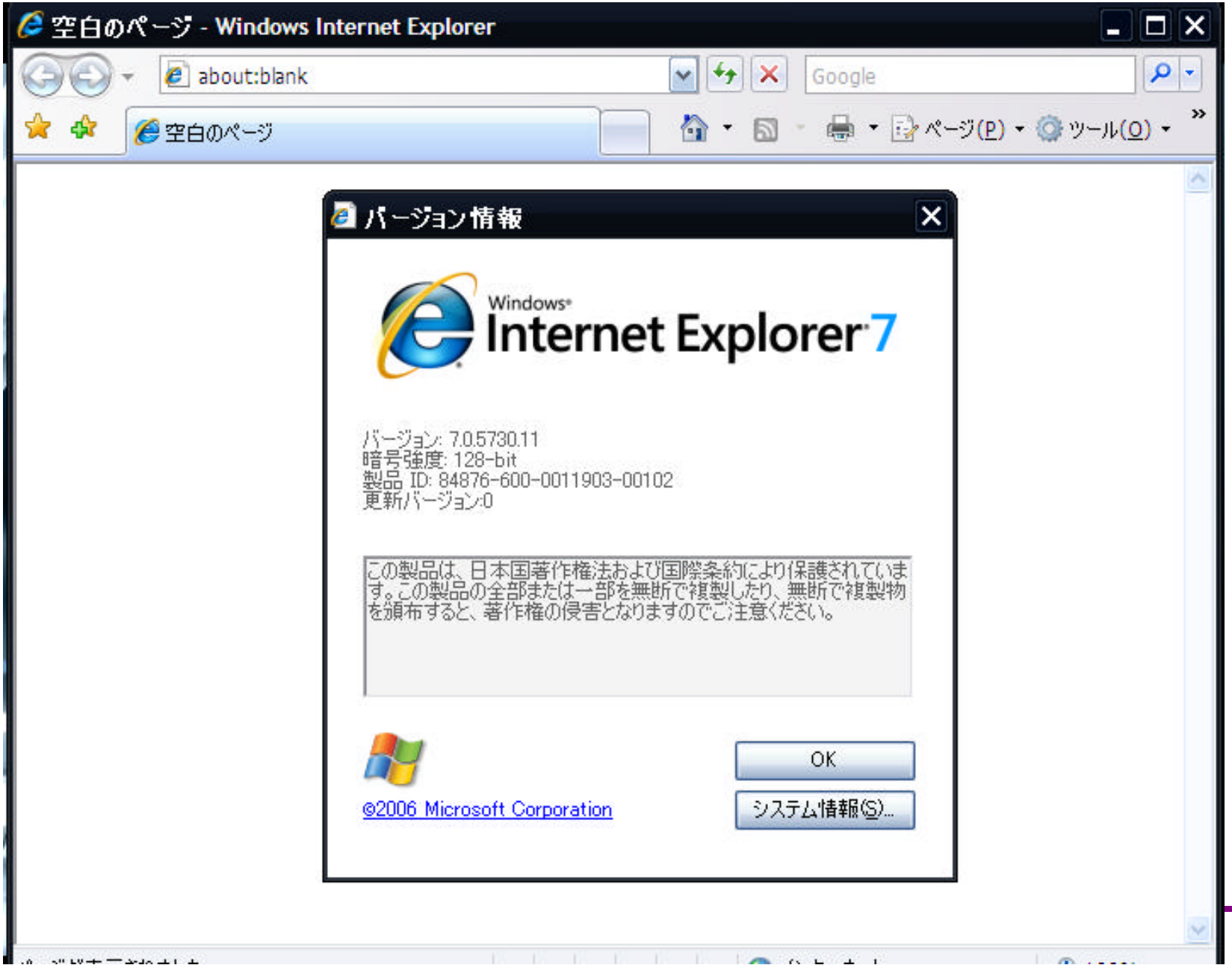
任意アドレスへアクセス


https://opengate.og12.edu.cc.saga-u.ac.jp/cgi-
Google
OpengateStart
ページ(P)
ツール(O)
ネットワーク利用者認証
[English version]
ネットワークの利用を始める前に、利用資格の確認を行ってください。
利用資格の確認には、ユーザ名とパスワードが必要です。自分のユーザ名やパスワードが解らない場合は、総合情報基盤センターに尋ねてください。
下の入力欄に、ユーザIDとパスワードを入力して、「送信」ボタンを押して下さい。
ユーザID:
パスワード:
送 信
以下は突然の切断が起こる場合に設定して下さい。
必要とする利用継続時間: 分(指定可能:1～60分)。この時間だけネットワークを開放します。この場合、不正利用を防ぐために、指定した時間より前に利用を終るには、許可ページにある「利用中断」のリンクをクリックして下さい。
不明な点などがありましたら、ネットワーク管理者にお尋ねください。
佐賀大学


https://opengate.og12.edu.cc.saga-u.ac.jp/cgi-
Google
OpengateStart
ページ(P)
ツール(O)
ネットワーク利用者認証
[English version]
ネットワークの利用を始める前に、利用資格の確認を行ってください。
利用資格の確認には、ユーザ名とパスワードが必要です。自分のユーザ名やパスワードが解らない場合は、総合情報基盤センターに尋ねてください。
下の入力欄に、ユーザIDとパスワードを入力して、「送信」ボタンを押して下さい。
ユーザID:
fujisawa
パスワード:
送 信
以下は突然の切断が起こる場合に設定して下さい。
必要とする利用継続時間: 分(指定可能:1～60分)。この時間だけネットワークを開放します。この場合、不正利用を防ぐために、指定した時間より前に利用を終るには、許可ページにある「利用中断」のリンクをクリックして下さい。
不明な点などがありましたら、ネットワーク管理者にお尋ねください。
佐賀大学


http://opengate.ai.is.saga-u.ac.jp:30000/httpkeep
Google
Http Keep-Alive
ページ(P)
ツール(O)
ネットワークを利用できます。
利用が終ったら必ずWebブラウザを終了してください。ネットワーク利用許可も自動的に取り消されます。
ネットワーク利用許可　ユーザ名 fujisawa　接続確認 20:06
上の2本の線の間に黄色のバーが表示されなかったりネットワークが閉鎖されるなど動作がおかしい場合は、利用中断 をクリックしてからブラウザを終了してください。また認証ページが表示されない場合は、通常とは別のページをアクセスしてみてください。
このページは、「このまま」か又は「最少化状態」にして下さい。ネットワーク利用は、別にブラウザその他のネットワーク利用プログラムを起動して行ってください。または、[スタートページ] から開始してください（クリックでスタートページが開かなければ、シフトキーを押しながらクリックしてください。またポップアップ許可に設定すれば自動的にポップアップします）。

Ｏｐｅｎｇａｔｅ－ＰＫＩの

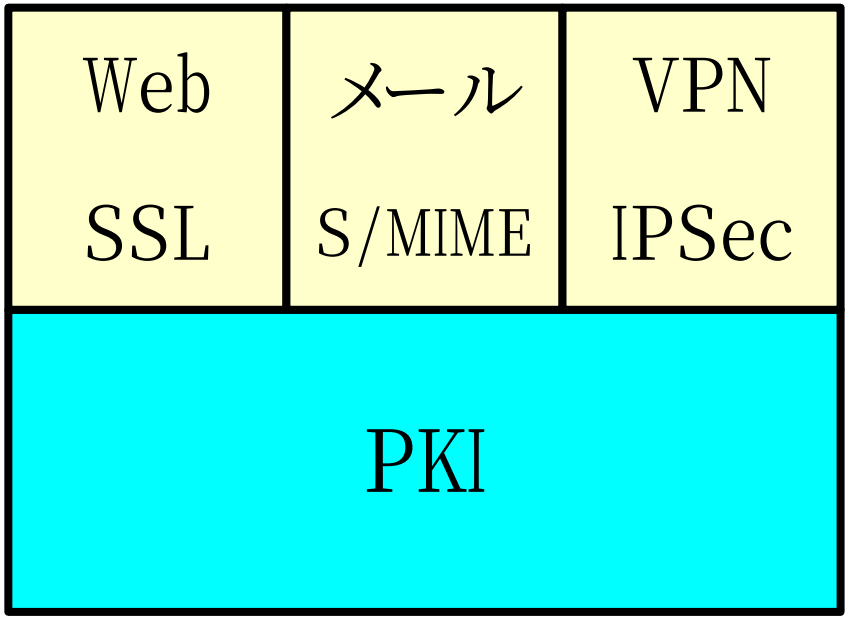


ＰＫＩとは

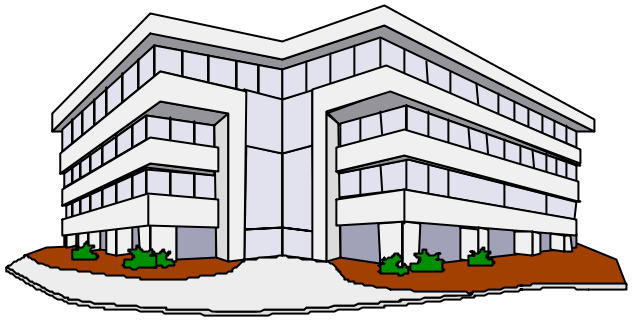
PKI (Public Key Infrastructure)

公開鍵暗号技術を利用した技術基盤

- 認証
- 暗号化
- 否認防止



ディジタル証明書 による認証



認証局

1.配布

3.確認

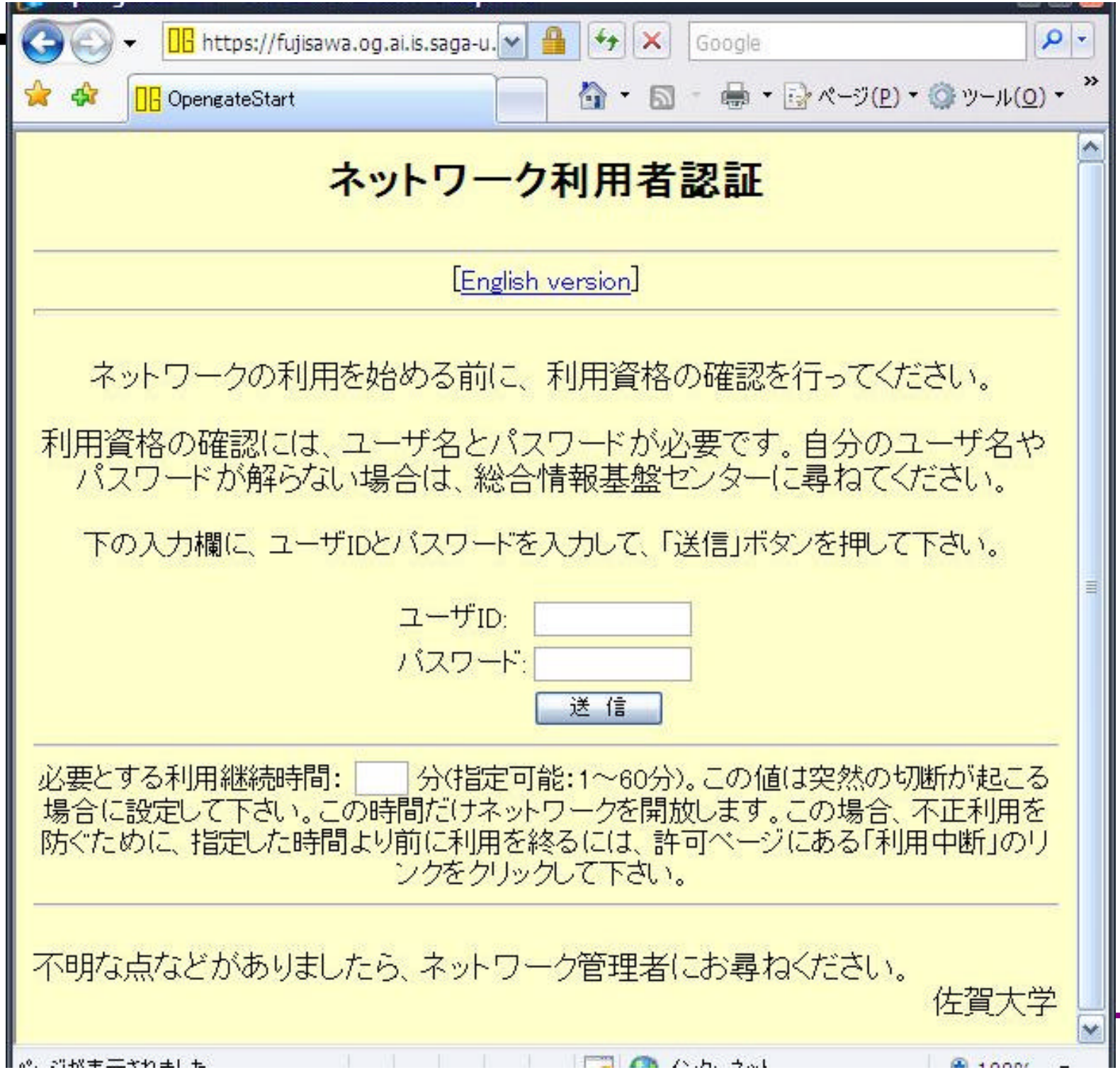
Aであると確認

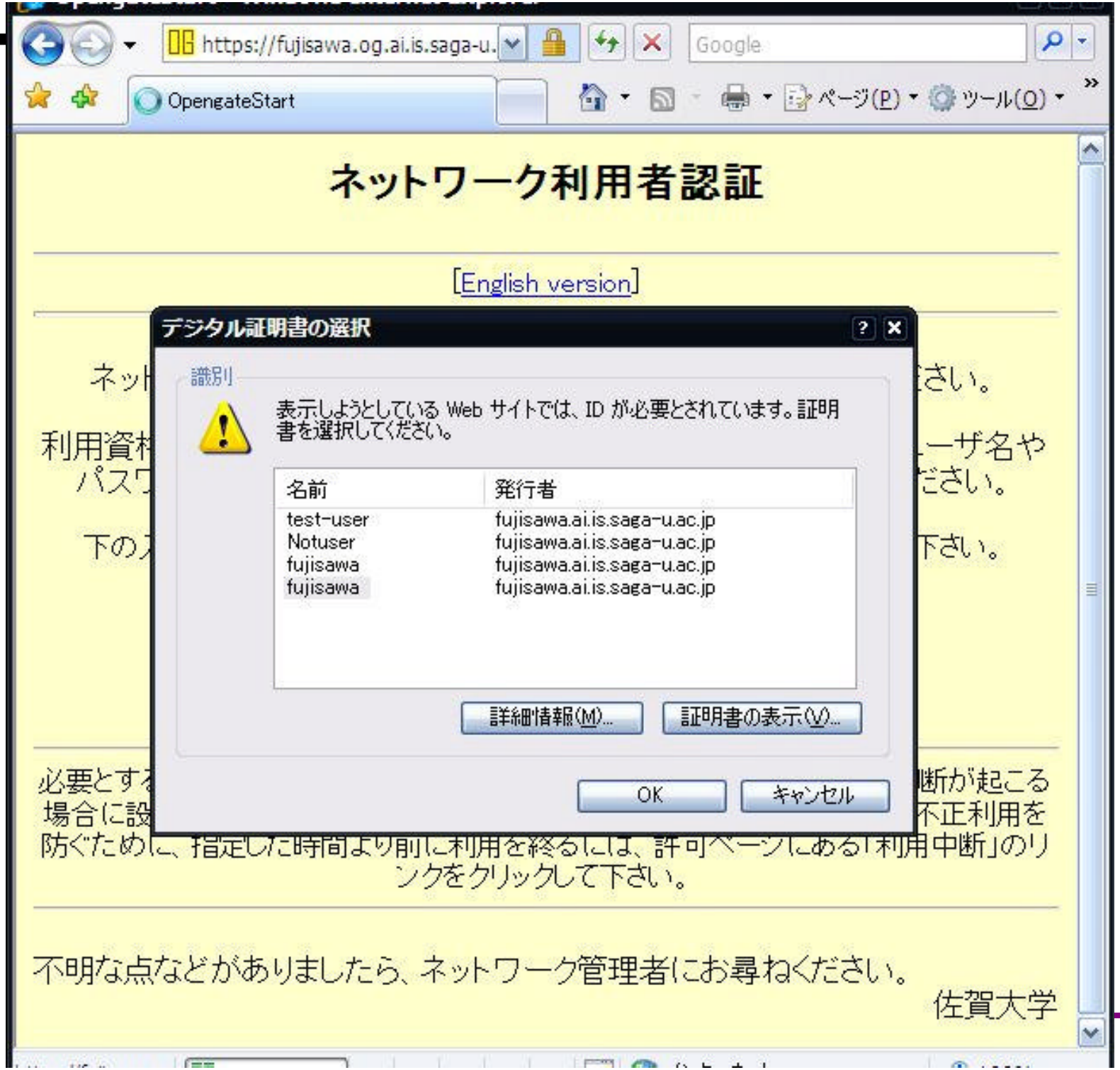
Aの
証明書

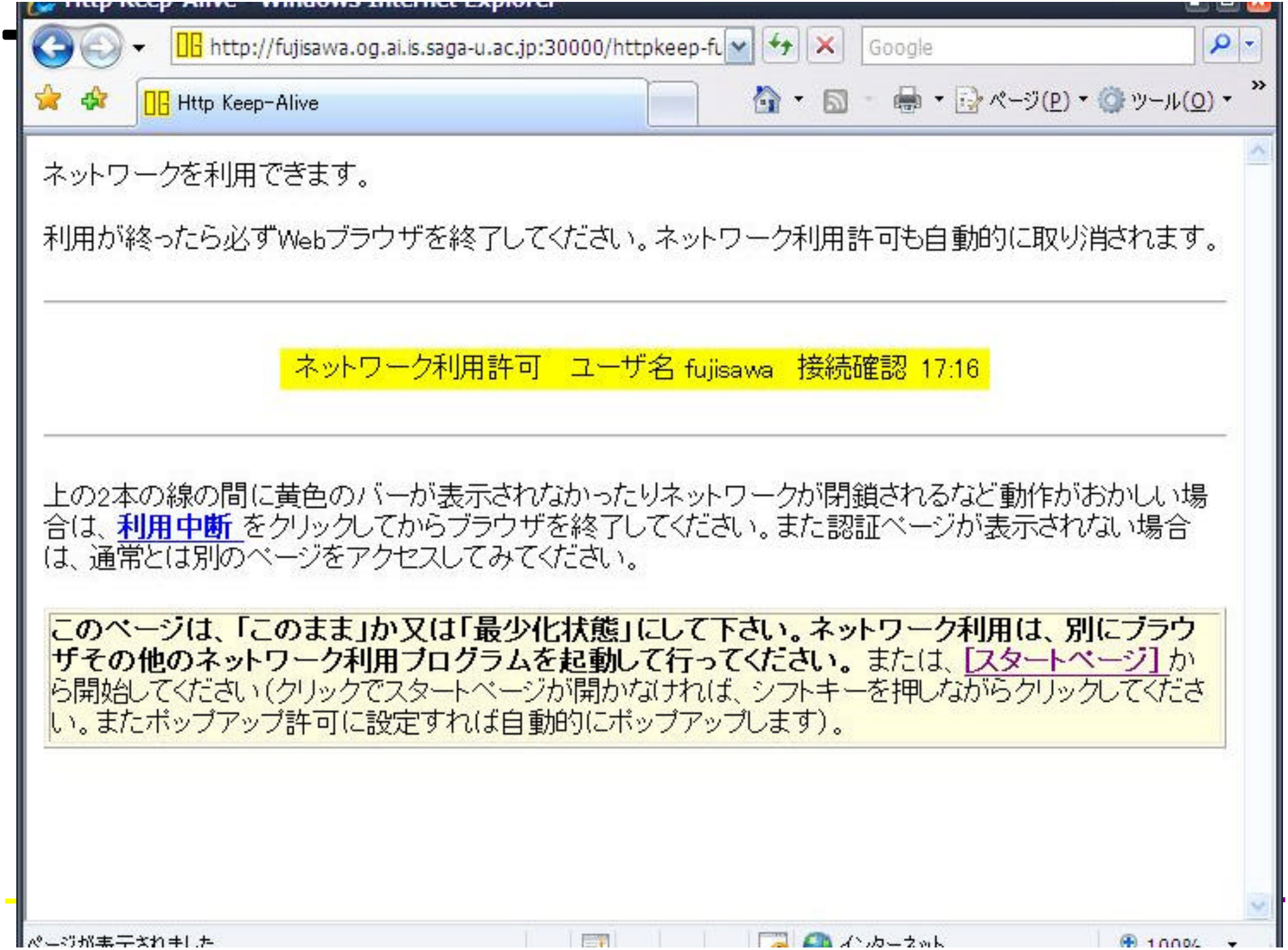
2送信

A

B


https://fujisawa.og.ai.is.saga-u.
Google
OpengateStart
ページ(P)
ツール(O)
ネットワーク利用者認証
[English version]
ネットワークの利用を始める前に、利用資格の確認を行ってください。
利用資格の確認には、ユーザ名とパスワードが必要です。自分のユーザ名やパスワードが解らない場合は、総合情報基盤センターに尋ねてください。
下の入力欄に、ユーザIDとパスワードを入力して、「送信」ボタンを押して下さい。
ユーザID:
パスワード:
送 信
必要とする利用継続時間: 分(指定可能:1～60分)。この値は突然の切断が起こる場合に設定して下さい。この時間だけネットワークを開放します。この場合、不正利用を防ぐために、指定した時間より前に利用を終るには、許可ページにある「利用中断」のリンクをクリックして下さい。
不明な点などがありましたら、ネットワーク管理者にお尋ねください。
佐賀大学


https://fujisawa.og.ai.is.saga-u.
Google
OpengateStart
ページ(P)
ツール(O)
ネットワーク利用者認証
[English version]
デジタル証明書の選択
識別
表示しようとしている Web サイトでは、ID が必要とされています。証明書を選択してください。
名前
発行者
test-user
fujisawa.ai.is.saga-u.ac.jp
Notuser
fujisawa.ai.is.saga-u.ac.jp
fujisawa
fujisawa.ai.is.saga-u.ac.jp
fujisawa
fujisawa.ai.is.saga-u.ac.jp
詳細情報(M)...
証明書の表示(V)...
OK
キャンセル
ンクをクリックして下さい。
不明な点などがありましたら、ネットワーク管理者にお尋ねください。
佐賀大学

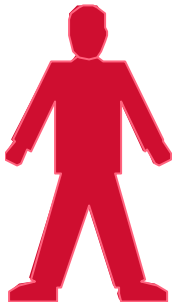

http://fujisawa.og.ai.is.saga-u.ac.jp:30000/httpkeep-fu
Google
Http Keep-Alive
ページ(P)
ツール(O)
ネットワークを利用できます。
利用が終ったら必ずWebブラウザを終了してください。ネットワーク利用許可も自動的に取り消されます。
ネットワーク利用許可　ユーザ名 fujisawa　接続確認 17:16
上の2本の線の間に黄色のバーが表示されなかったりネットワークが閉鎖されるなど動作がおかしい場合は、利用中断 をクリックしてからブラウザを終了してください。また認証ページが表示されない場合は、通常とは別のページをアクセスしてみてください。
このページは、「このまま」か又は「最少化状態」にして下さい。ネットワーク利用は、別にブラウザその他のネットワーク利用プログラムを起動して行ってください。 または、[スタートページ] から開始してください（クリックでスタートページが開かなければ、シフトキーを押しながらクリックしてください。またポップアップ許可に設定すれば自動的にポップアップします）。
インターネット
100%

公開鍵暗号方式

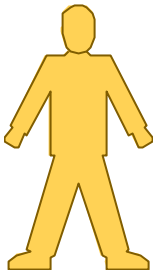
- 秘密鍵と公開鍵の一対の鍵
- 秘密鍵は鍵生成者のみが持つ
- 公開鍵は配付される

データ の 暗号化

公開鍵暗号方式



A



B

メッセージ

メッセージ

暗号文

送信

暗号文

復号

暗号化

Aの秘密鍵

Aの公開鍵

取得

Aの公開鍵

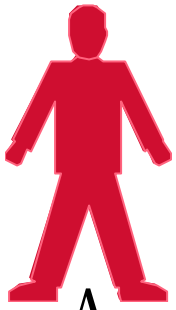
ディジタル署名

- 現実のサインと同様
- 秘密鍵を用い署名
- 公開鍵で確認

本人 の 確認

データ の 完全性 の 保証

ディジタル署名



A

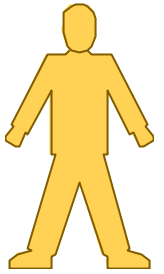
メッセージ

署名

送信

メッセージ

署名



B

暗号化
（署名）

Bの秘密鍵

復号
（署名検証）

Bの公開鍵

取得

Bの公開鍵

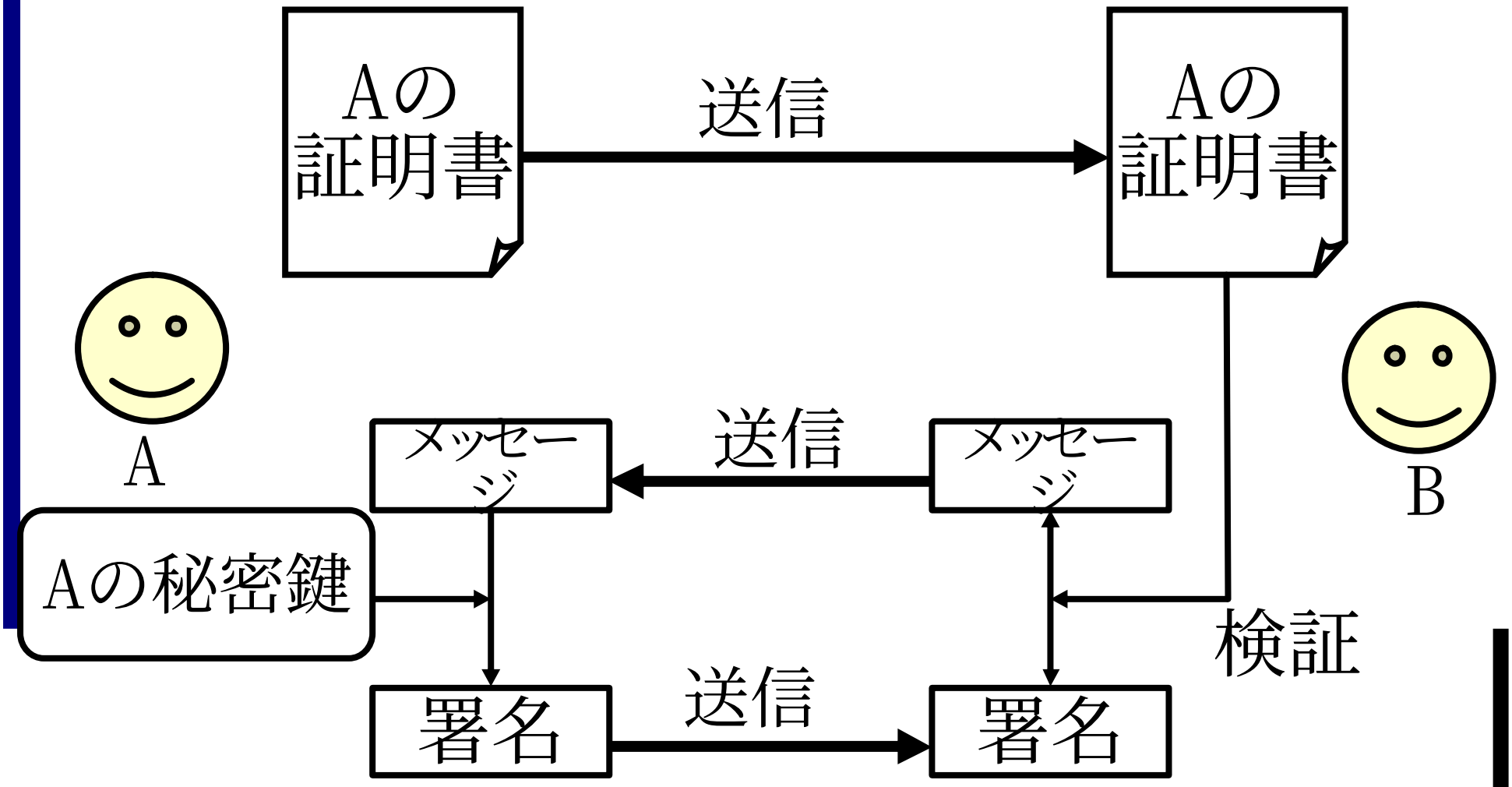
認証局

- 公開鍵の作成者を確認
- なりすましを防止
- 公開鍵の作成者に証明書を配付
- 証明書に認証局の署名

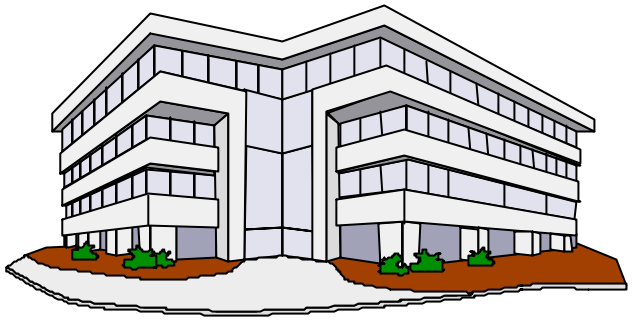
Ｏｐｅｎｇａｔｅ－ＰＫＩ運用

1. 管理者
   - 利用者を手渡しなどで確実に本人確認
   - 証明書と秘密鍵はPKCS#12形式で配付
   - 証明書の失効を素早く反映
2. 利用者
   - 秘密鍵の盗難による危険性を認識
   - 秘密鍵はブラウザの機能などで保護
   - 秘密鍵の盗難、紛失を管理者に報告

ＰＫＩによる認証



ディジタル証明書 による認証



認証局

取得

認証局の署名

1.配布

3確認

署名確認

認証局の証明書

Aであると確認

Aの証明書

2送信

A

B

ＵＰＫＩ

UPKI共通仕様ドラフト版（2007年1月30日）

- キャンパスPKI　CP/CPSガイドライン（初版）
- キャンパスPKI　調達仕様ガイドライン（初版）

⇩

将来の連携性確保、
構築コスト削減の観点を含めた
学内PKIの構築の指針

証明書 の 確認

1. Apacheによる確認

証明書内の署名を確認

信頼できる認証局から
発行されている証明書であることを確認

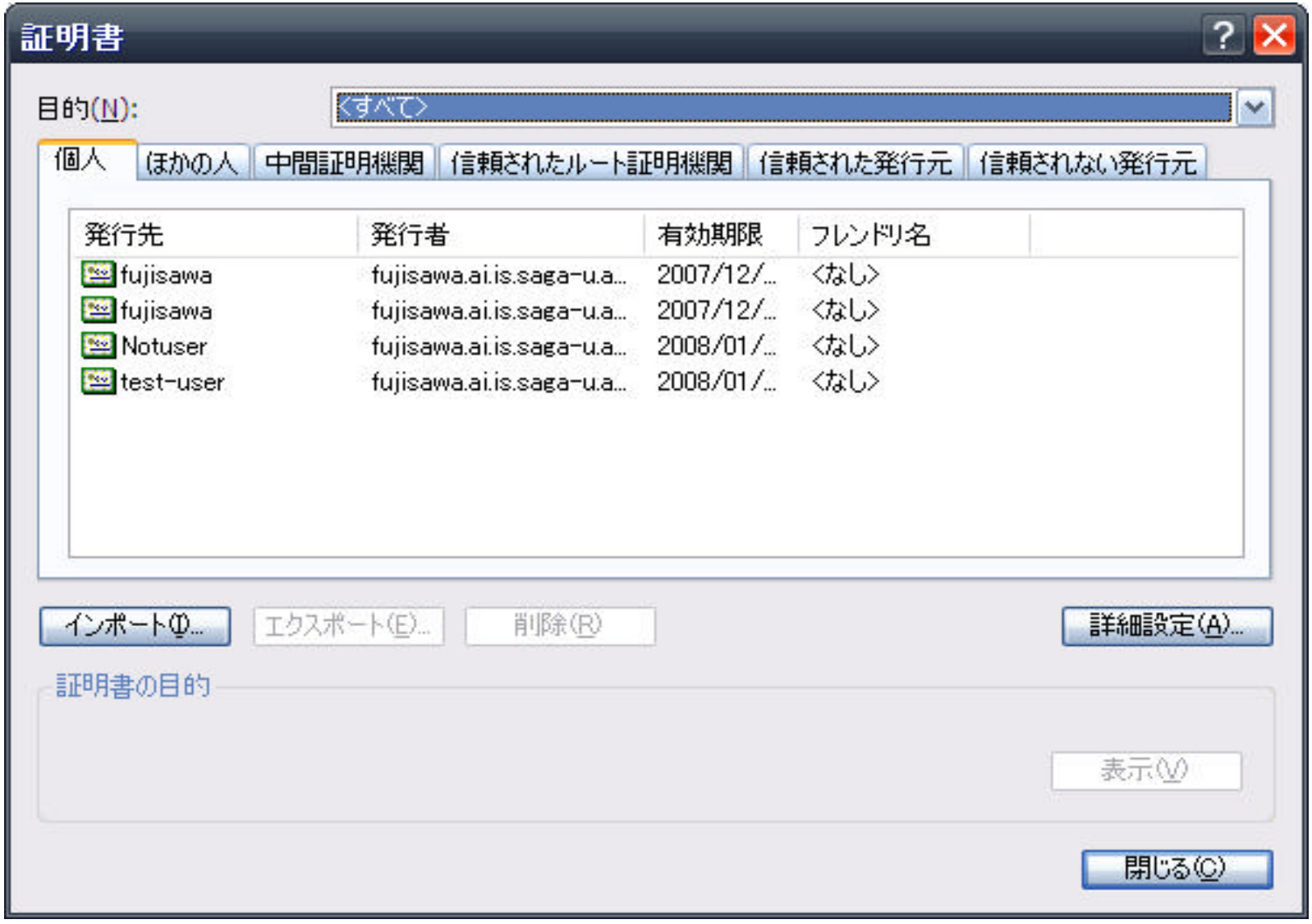
2. サーバプログラムによる確認

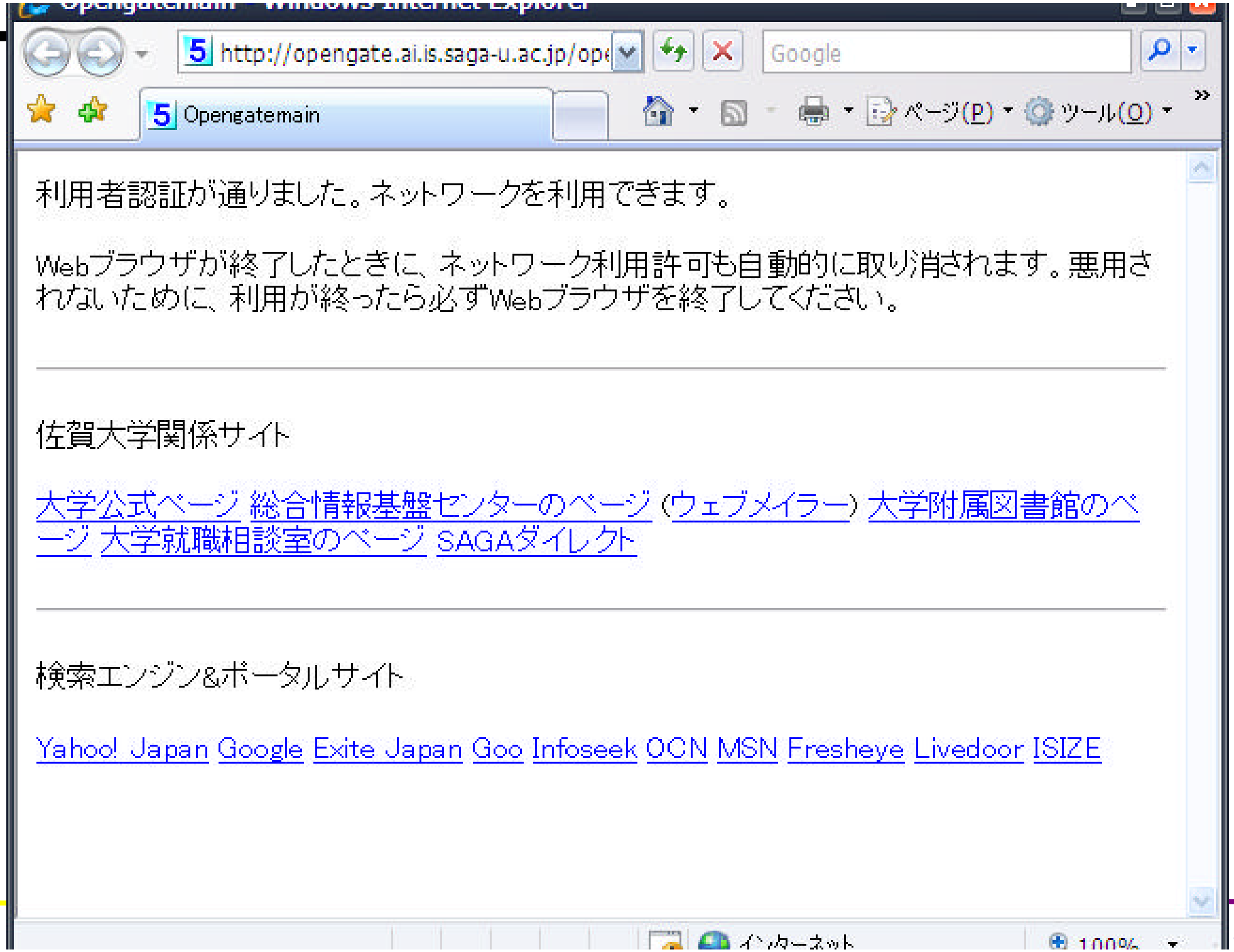
証明書内のユーザ情報を確認

利用者ユーザを確認

Ｏｐｅｎｇａｔｅ－ＰＫＩの利

1. 認証局から証明書を取得
2. ブラウザに証明書をインポート
3. ブラウザからWebページアクセス
4. 認証ページで証明書提出
5. 認証完了後、ネットワーク利用可能


証明書
目的(N):
<すべて>
個人
ほかの人
中間証明機関
信頼されたルート証明機関
信頼された発行元
信頼されない発行元
発行先
発行者
有効期限
フレンドリ名
fujisawa
fujisawa.ai.is.saga-u.a...
2007/12/...
<なし>
fujisawa
fujisawa.ai.is.saga-u.a...
2007/12/...
<なし>
Notuser
fujisawa.ai.is.saga-u.a...
2008/01/...
<なし>
test-user
fujisawa.ai.is.saga-u.a...
2008/01/...
<なし>
インポート(I)...
エクスポート(E)...
削除(R)
詳細設定(A)...
証明書の目的
表示(V)
閉じる(C)


http://opengate.ai.is.saga-u.ac.jp/ope
Google
Opengatemain
ページ(P)
ツール(O)
利用者認証が通りました。ネットワークを利用できます。
Webブラウザが終了したときに、ネットワーク利用許可も自動的に取り消されます。悪用されないために、利用が終ったら必ずWebブラウザを終了してください。
佐賀大学関係サイト
大学公式ページ 総合情報基盤センターのページ (ウェブメイラー) 大学附属図書館のページ 大学就職相談室のページ SAGAダイレクト
検索エンジン&ポータルサイト
Yahoo! Japan Google Exite Japan Goo Infoseek OCN MSN Fresheye Livedoor ISIZE
インターネット
100%