SINET＆学認 クラウド利用説明会
「 学認参加大学における活用事例の紹介」

Proxyを用いた Web アクセス制御の シングルサインオンの実現

佐藤聡
筑波大学

背景

- ネットワーク認証
  - 認証に基づいて アクセスの権限を付与
  - アクセス制限の単位
    - アクセス対象のIPアドレス，プロトコル

- キヨスク端末におけるアクセス制限

  例） 非認証状態でも，特定のURLはアクセスさせたい

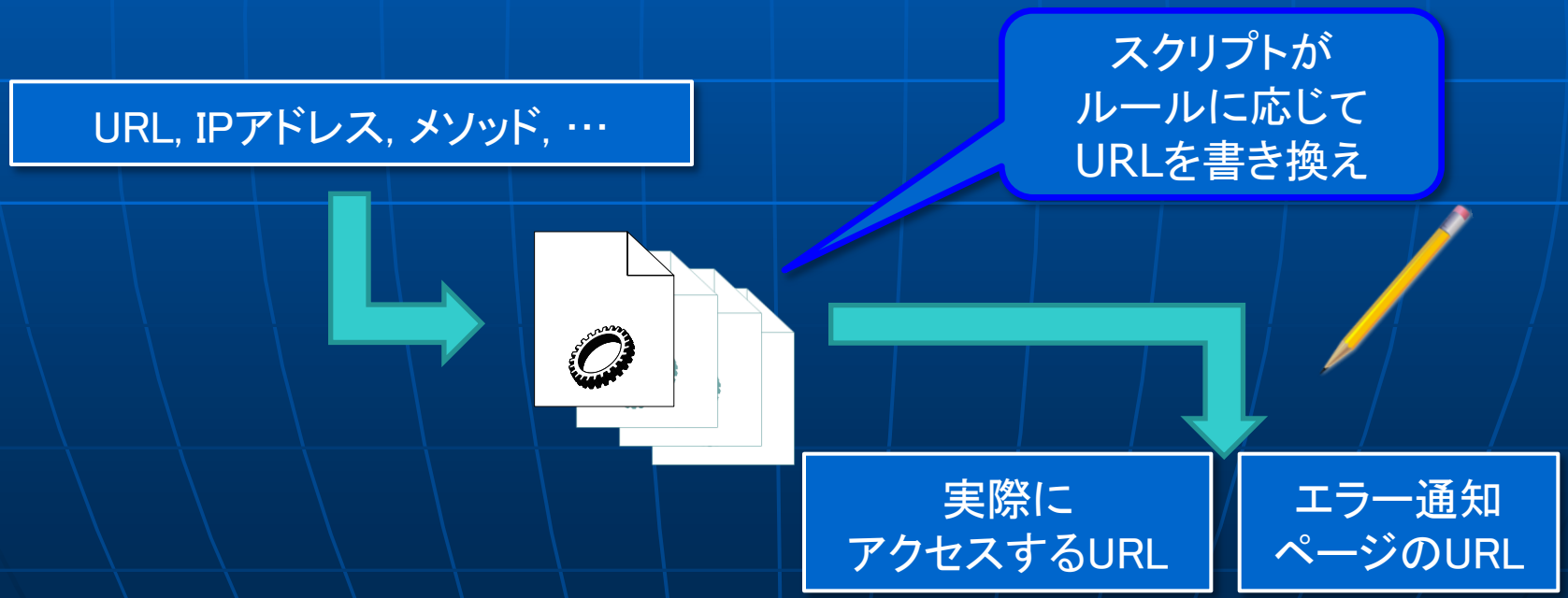
提案システム

- キオスク端末に対象としたWebアクセス制御を対象としたシングルサインオンシステム
- 端末からのHTTP通信をWeb Proxyで制御
  - 利用者の属性に応じてルールを設定
  - 一時的アカウントが不要に
- HTTPリクエストの内容に応じた柔軟なアクセス制御ルール

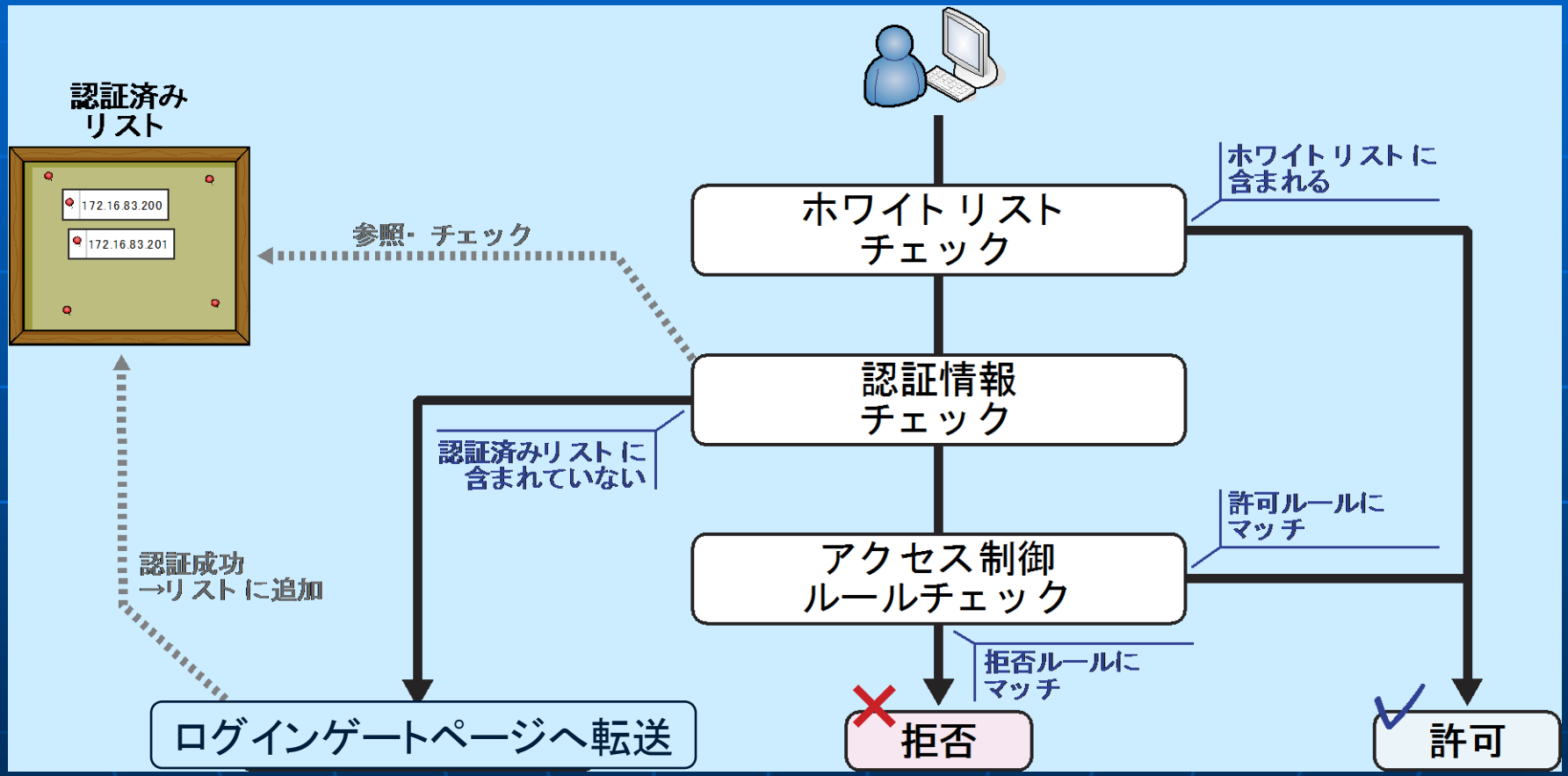
- 2010月3月,2011年10月の情報処理学会IOT研究会にて発表

アクセス制御の実現

- URLの書き換えでアクセス制御
- Web ProxyとしてSquidを使用
  - url_rewrite_programを利用



url_rewrite_programの概要



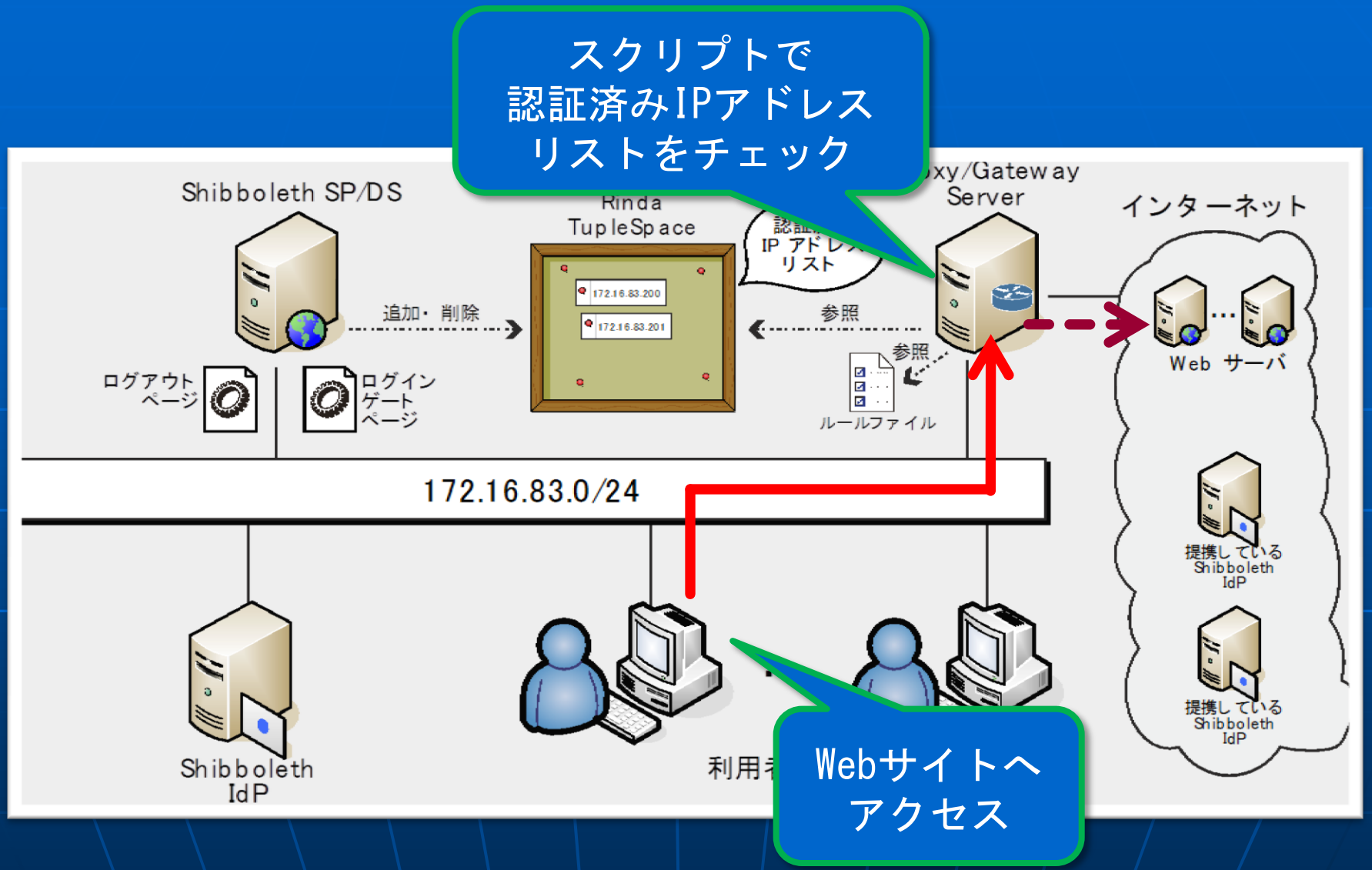
ホワイトリスト

- 認証なしでアクセス可能なリスト
  - 蔵書検索
  - 大学のWebサイト
  - 検索サイト　など
  - 認証に利用するIdP(認証サーバ)

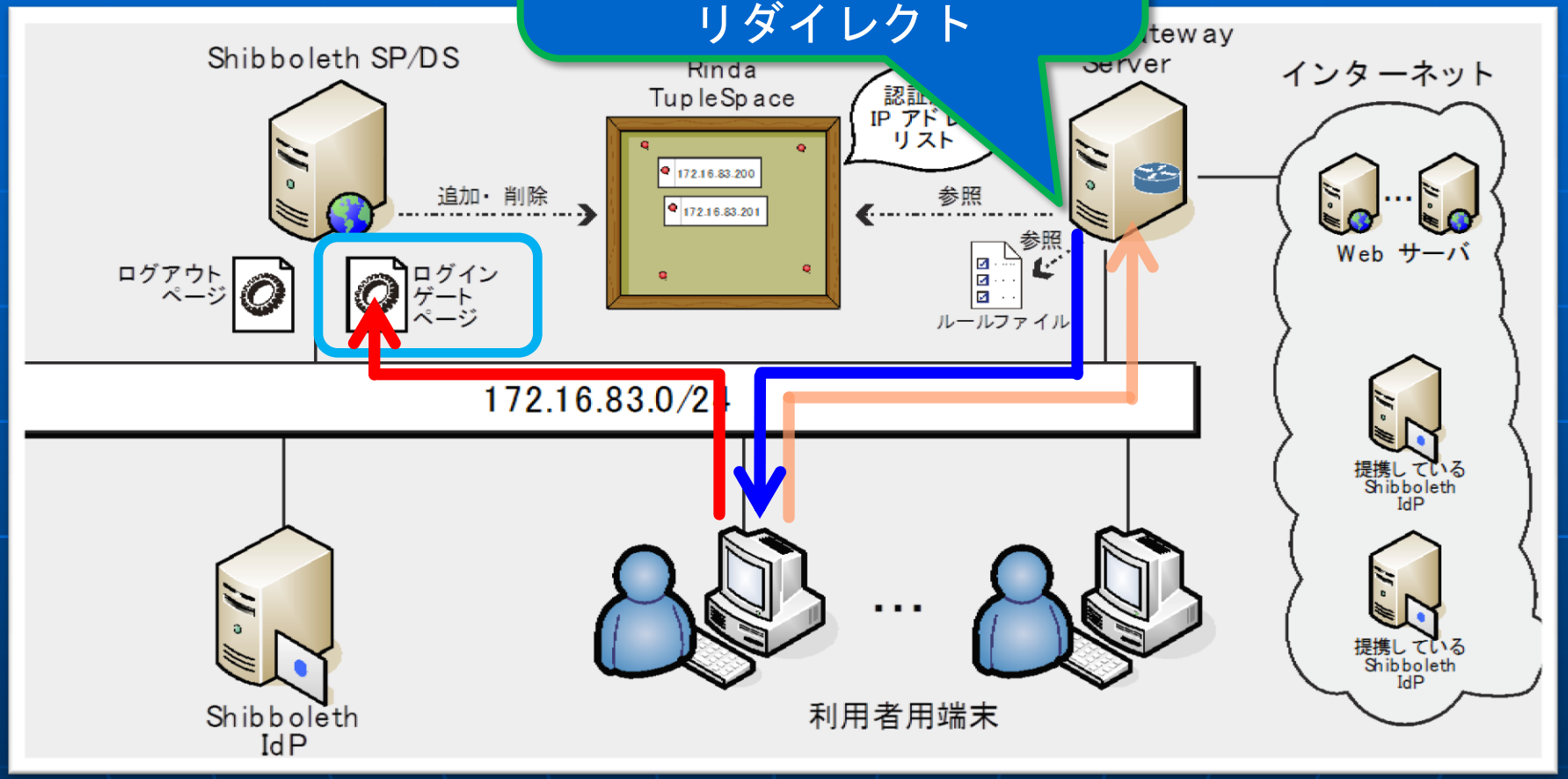
ログインゲートページ

- Shibboleth SP (Service Provider)のCGIプログラムとして動作
- Shibboleth認証を要求
- IPアドレス，Shibboleth属性を認証済みIPアドレスリストに登録
  - Proxyサーバはこのリストをもとにアクセス制御ルールを設定
- ログアウトページも用意

システム構成と処理の流れ

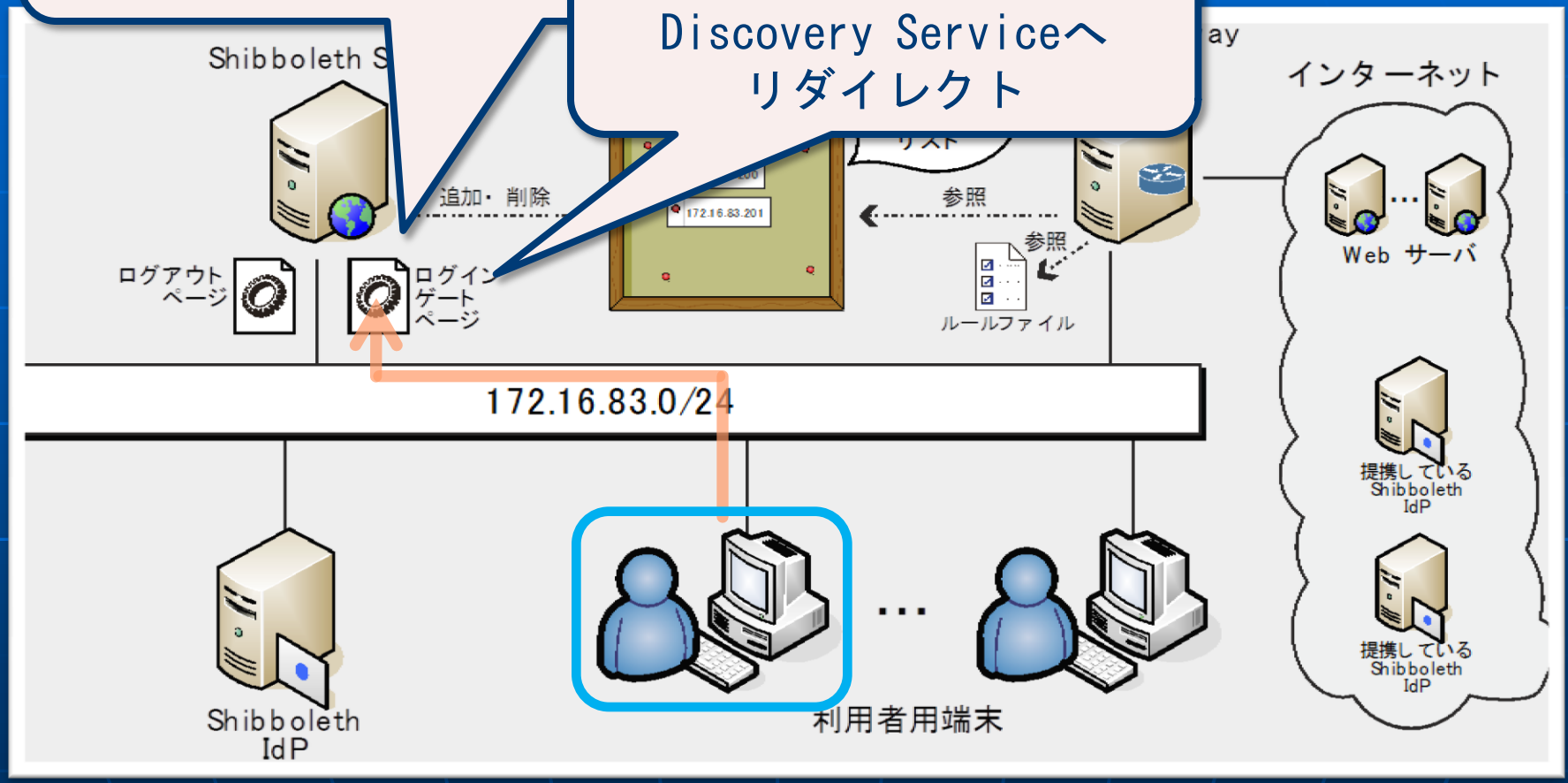

スクリプトで
認証済みIPアドレス
リストをチェック
Shibboleth SP/DS
Rinda
TupleSpace
xy/Gateway
Server
インターネット
追加・削除
参照
参照
172.16.83.200
172.16.83.201
ログアウト
ページ
ログイン
ゲート
ページ
ルールファイル
Web サーバ
172.16.83.0/24
提携している
Shibboleth
IdP
提携している
Shibboleth
IdP
Shibboleth
IdP
Webサイトへ
アクセス

リストにIPアドレスが
載っていないので
ログインゲートページへ
リダイレクト



Shibboleth SPとして動作
認証情報をチェック
(Cookie)

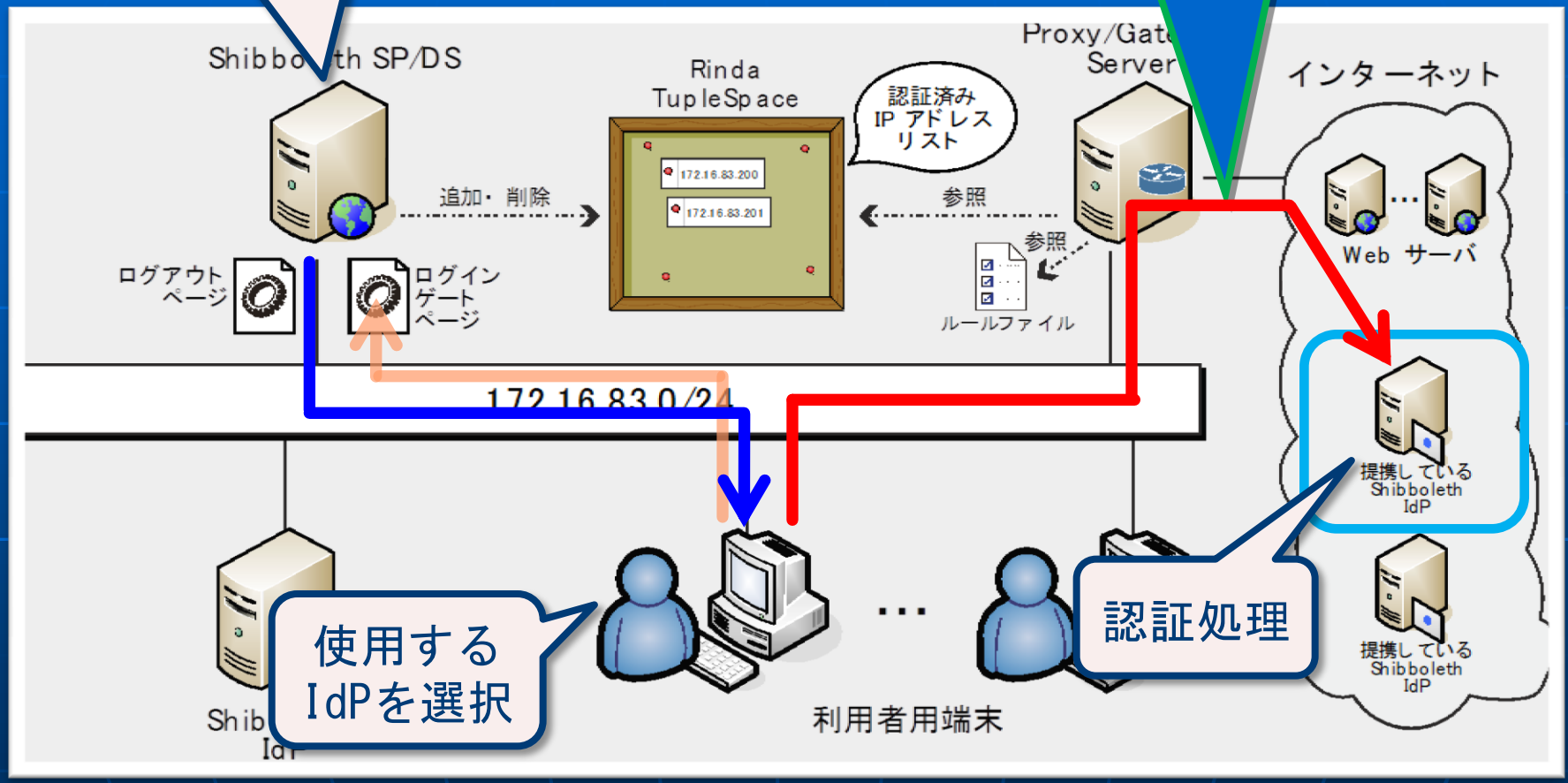
認証情報がなければ
Discovery Serviceへ
リダイレクト



※Shibbolethの標準動作

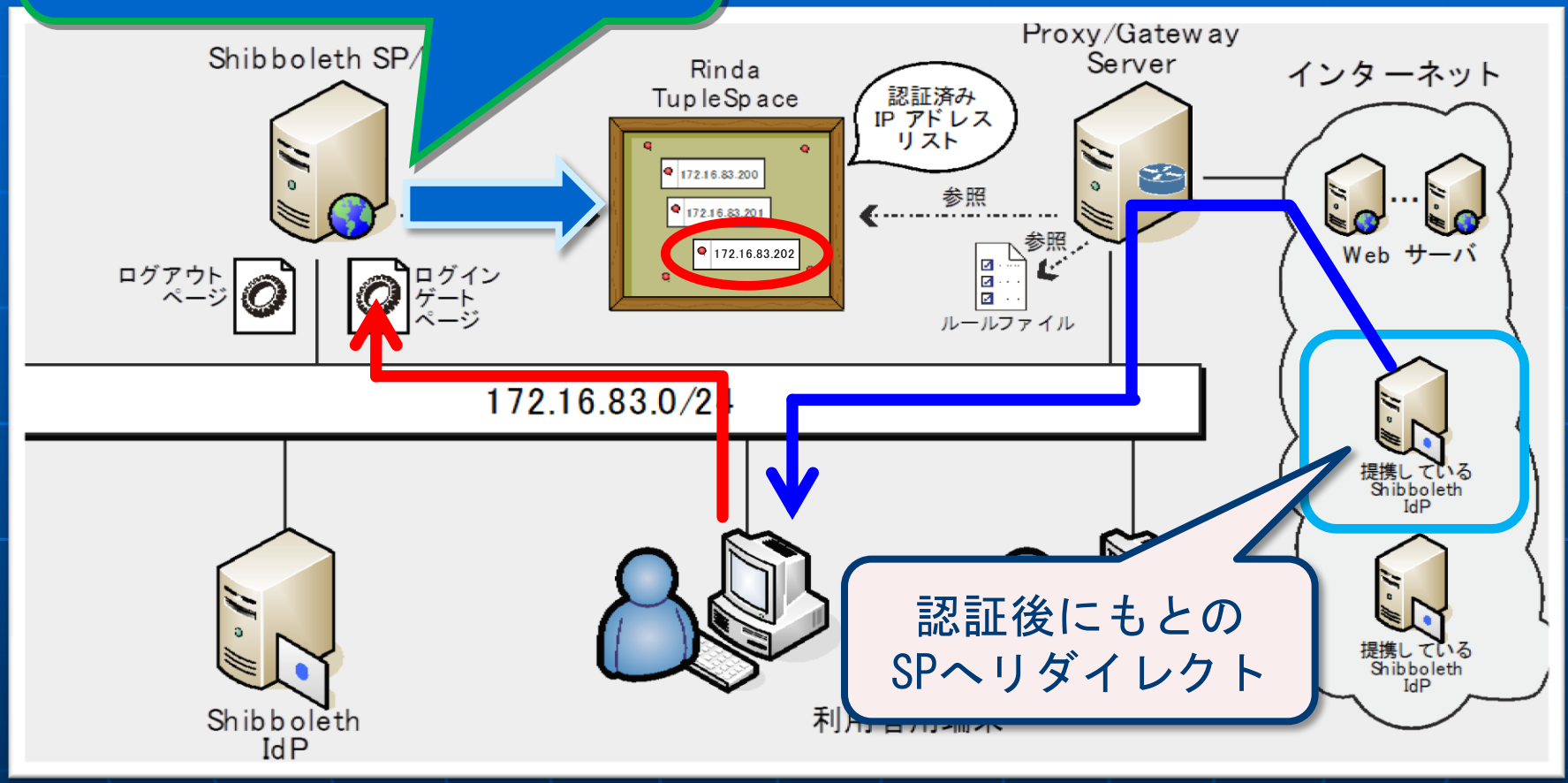
選択されたIdPへ
リダイレクト

IdPとの通信は
ホワイトリストで
許可されている

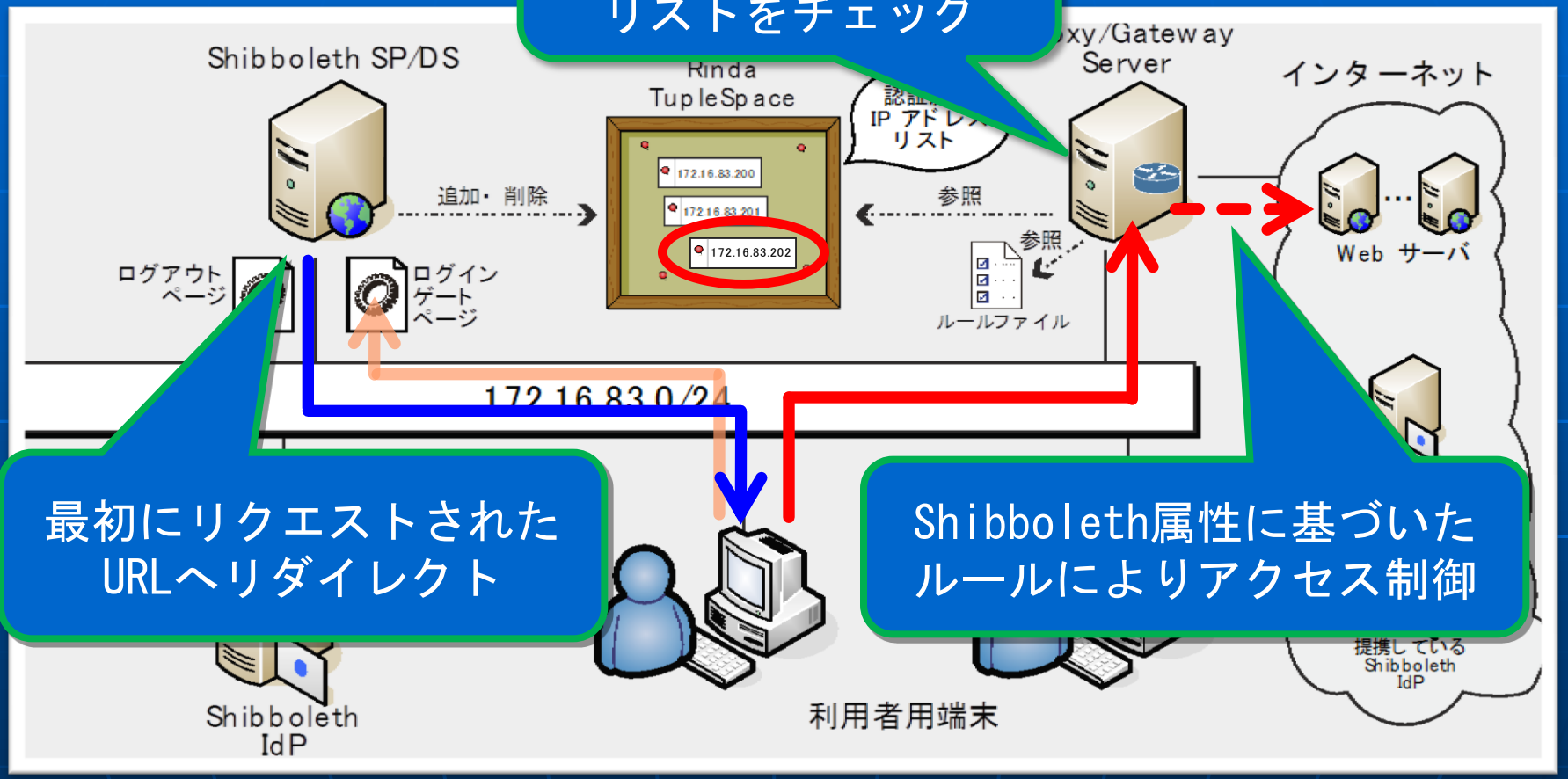


※Shibbolethの標準動作

Shibboleth 属性をチェック
認証済みリストに登録



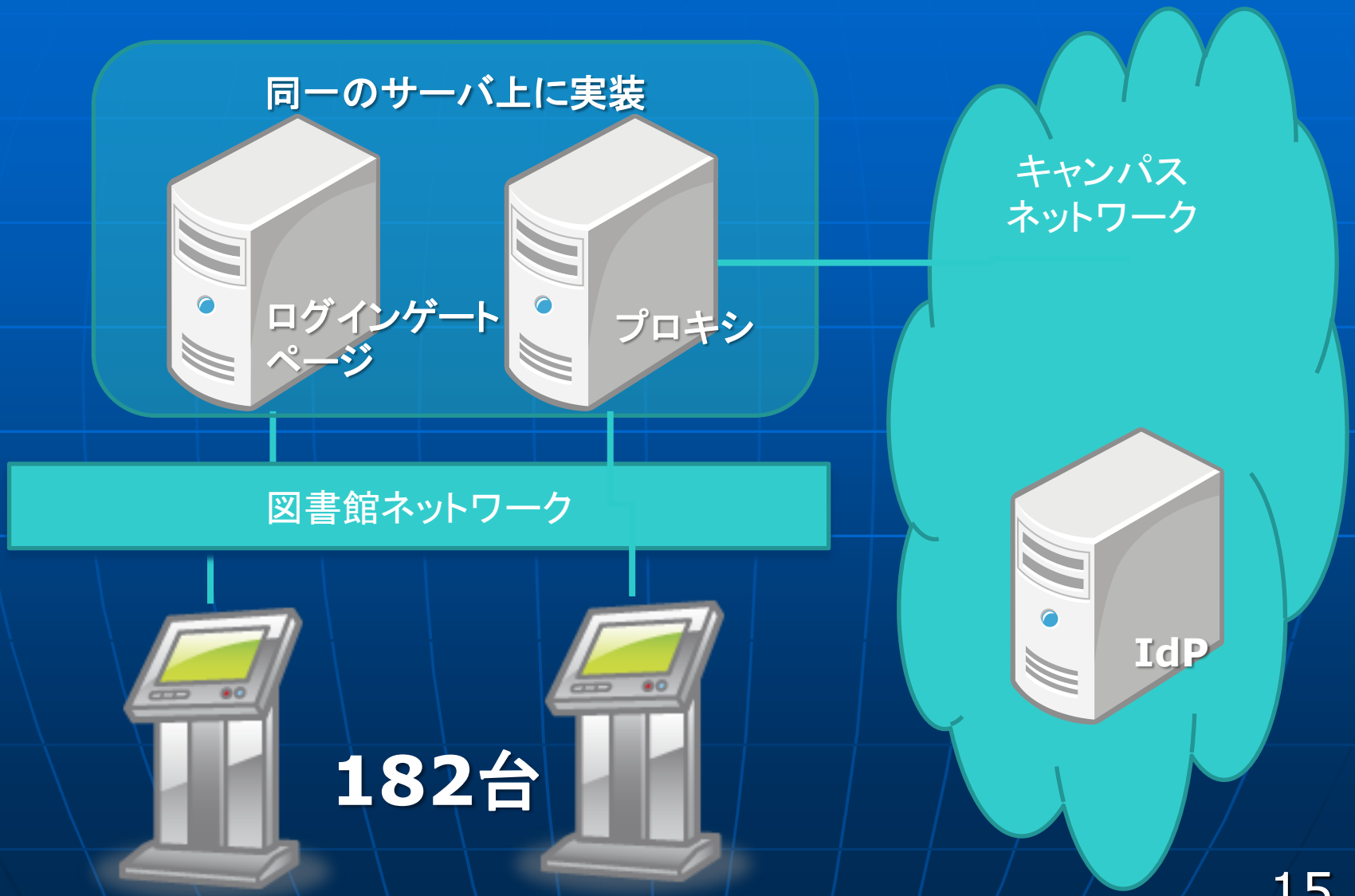
※Shibbolethの標準動作


スクリプトで
認証済みIPアドレス
リストをチェック
Shibboleth SP/DS
Rinda
TupleSpace
172.16.83.200
172.16.83.201
172.16.83.202
追加・削除
参照
参照
ルールファイル
ログアウト
ページ
ログイン
ゲート
ページ
Server
インターネット
Web サーバ
172.16.83.0/24
最初にリクエストされた
URLへリダイレクト
Shibboleth属性に基づいた
ルールによりアクセス制御
Shibboleth
IdP
利用者用端末

キオスク端末の管理方法

- Windows系　OS
- グループ･ポリシによる一括管理
  - 利用者による設定変更の禁止
  - ソフトウェアのインストール，アンインストールの禁止
  - ブラウザ以外のソフトウェアの削除
    - 蔵書検索のためにブラウザは必須

実装


同一のサーバ上に実装
ログインゲートページ
プロキシ
キャンパスネットワーク
図書館ネットワーク
IdP
182台

ログアウト処理の実現方法

- 利用者の能動的な処理
  - ブラウザを起動・終了と連携
    - プライバシー保護の観点から起動・終了すべき
    - ブラウザが起動する際にログアウト処理を実施
- 利用者のし忘れの対策
  - スクリーンセーバーと連携
  - サイネージとしても利用可能
  - グループ・ポリシにより一括インストール可能

スクリーンセーバによるログアウト処理の実現方法

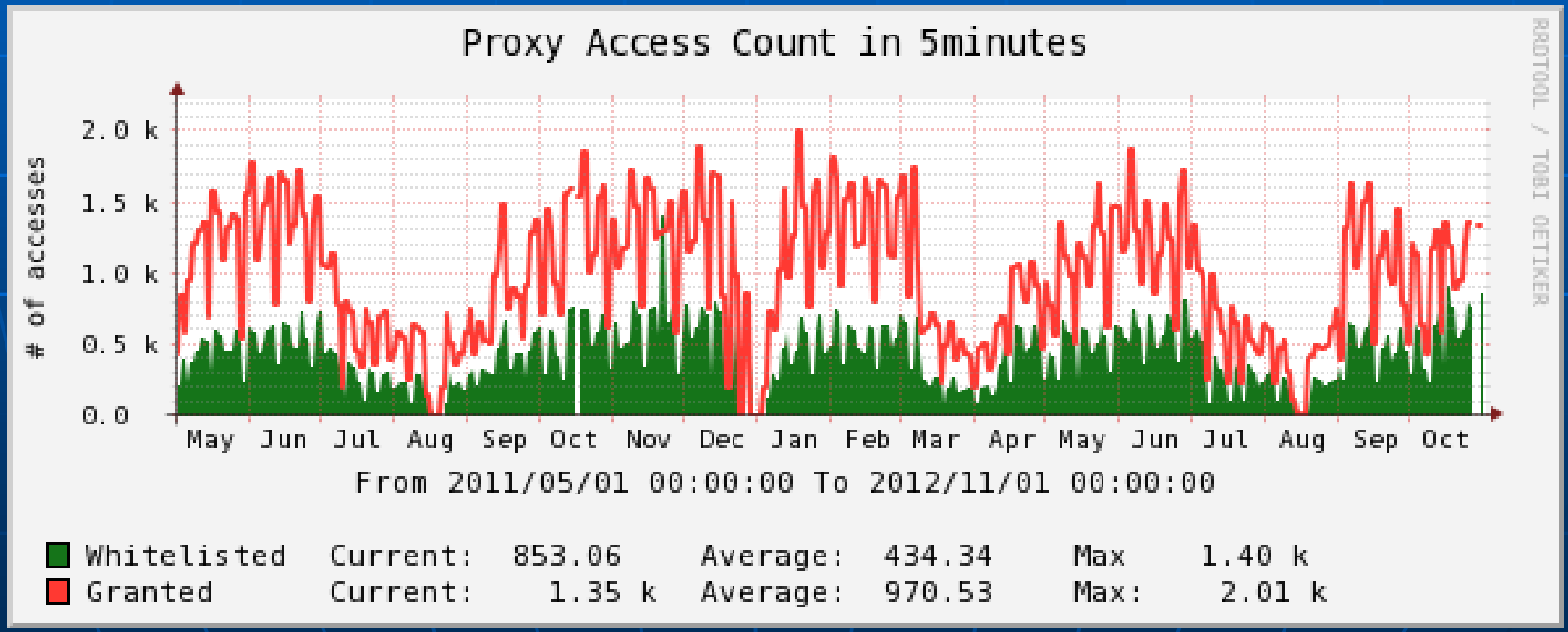
- ブラウザが起動している場合
  1. 指定された時間の間，利用者への注意喚起メッセージを表示
  2. ブラウザを強制的に終了
  3. ログアウト処理を実施
  4. 指定されたスクリーンセーバを実行
- ブラウザが起動していない場合
  1. ログアウト処理を実施
  2. 指定されたスクリーンセーバを実行

Webアクセス制御ルール

- ホワイトリスト
  - 約500行
  - IPアドレスリストでは記載しきれないものも記載可能
- 利用者の属性によるルールの切り替え
  - UIDのコード体系に着目した実装

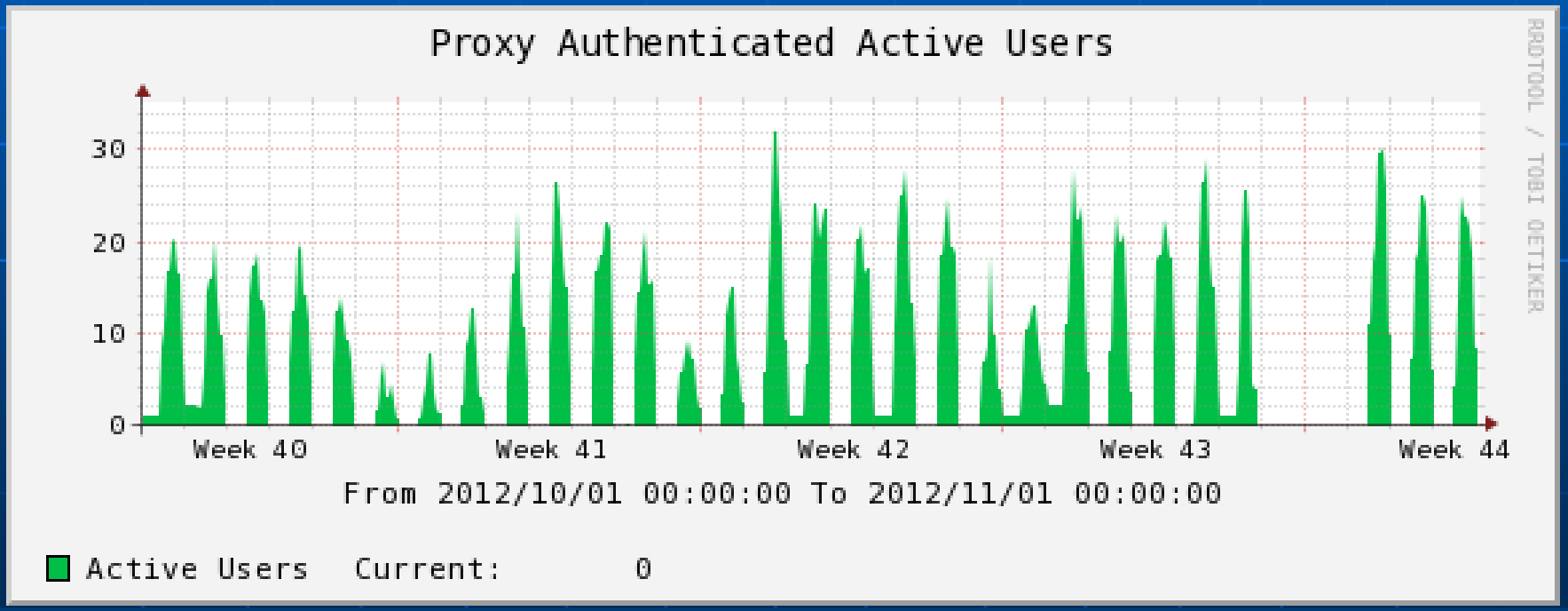
アクセス数

- 赤：認証が必要なULR　緑：ホワイトリストで許可されたURL
- 2011/05/01～2012/10/31



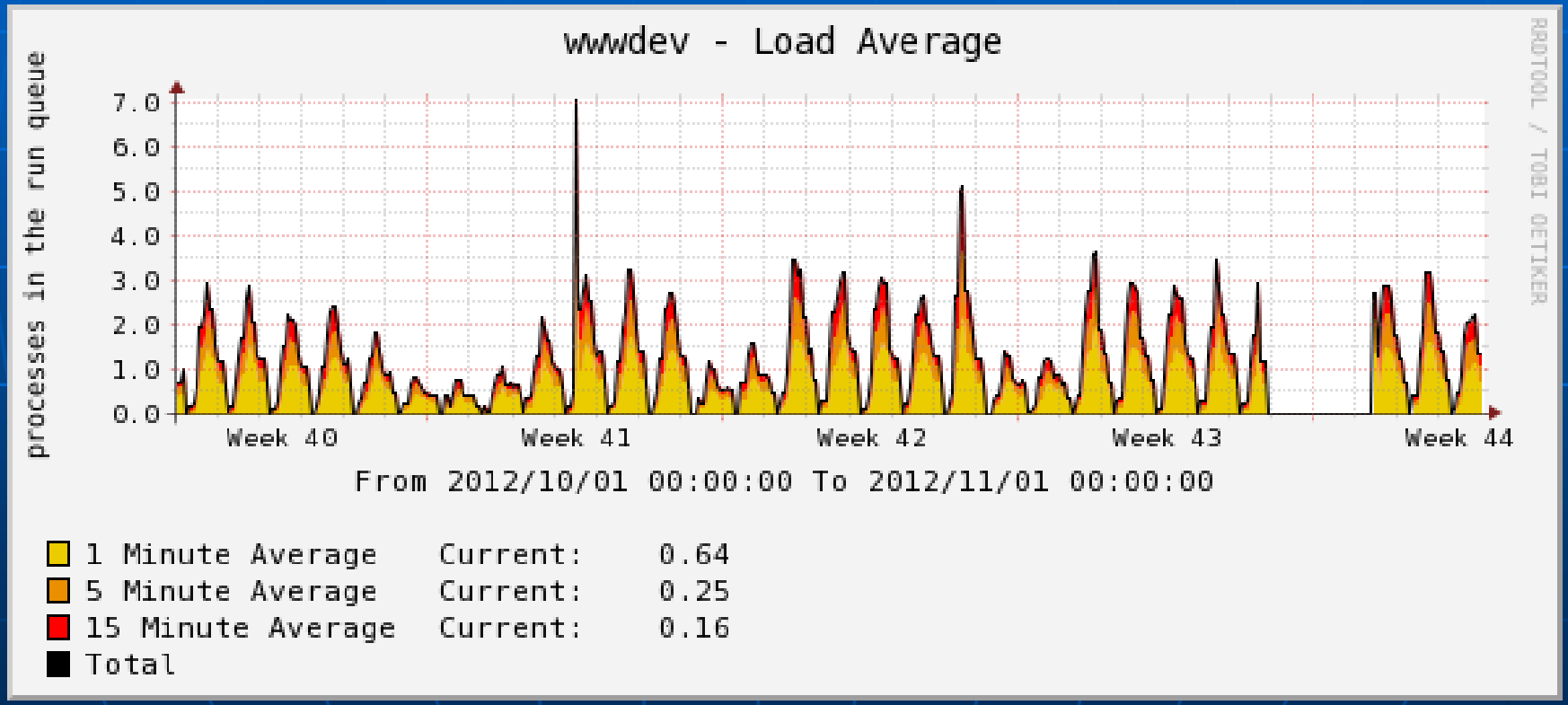
ユーザ数(月)

- 2012/10/01～2012/10/31



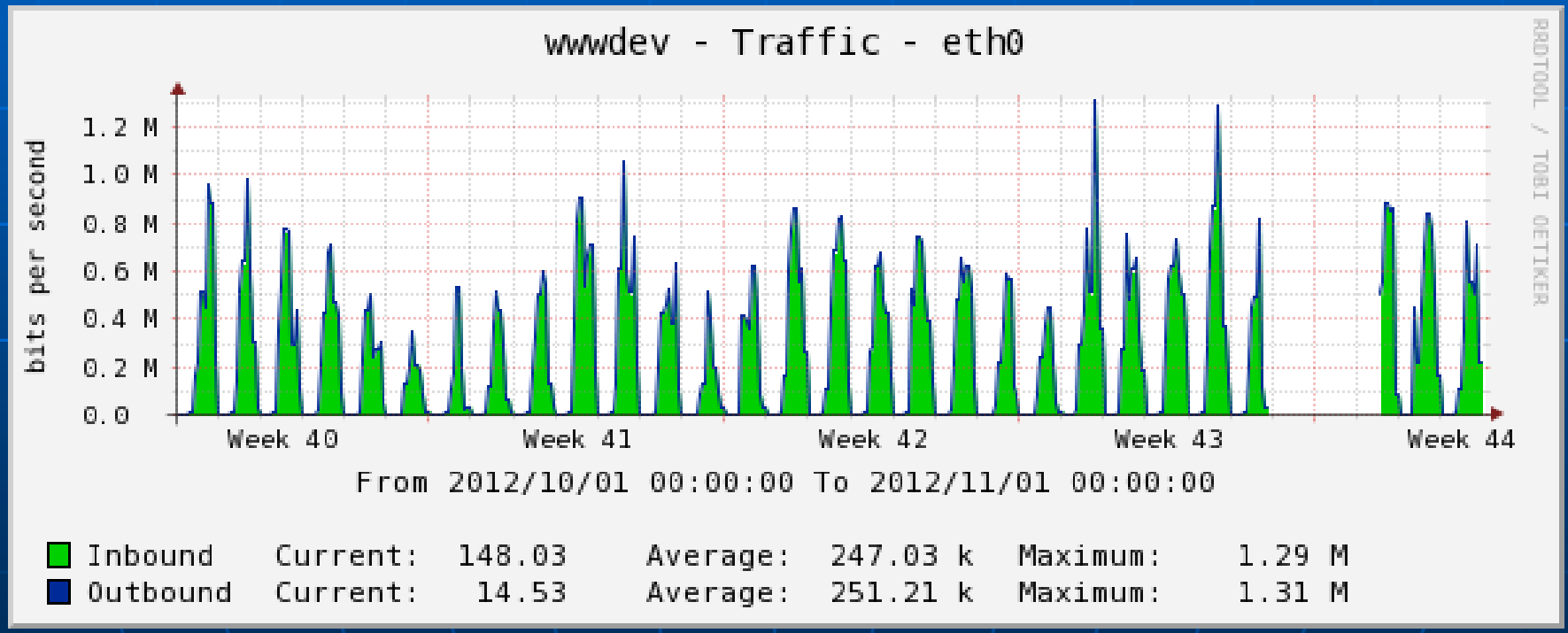
CPU ロード(月)

- 2012/10/01～2012/10/31



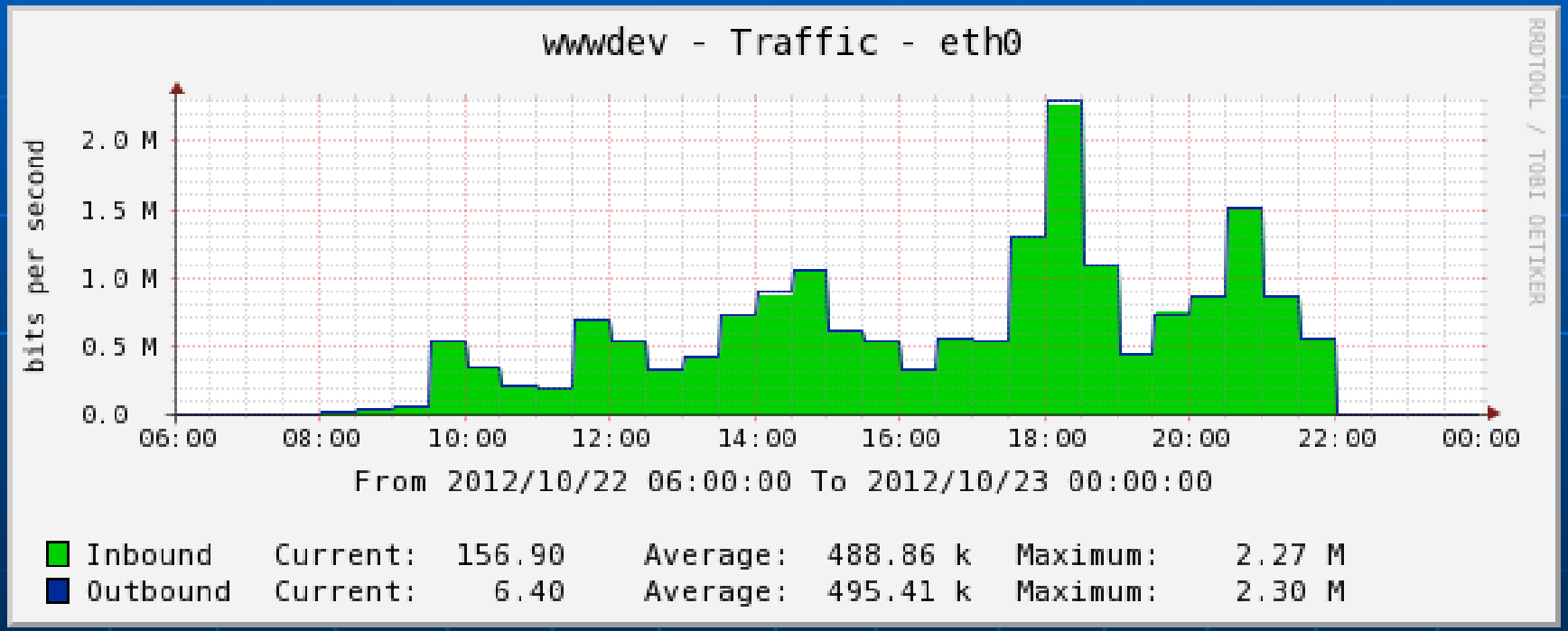
トラフィック(月)

- 2012/10/01～2012/10/31

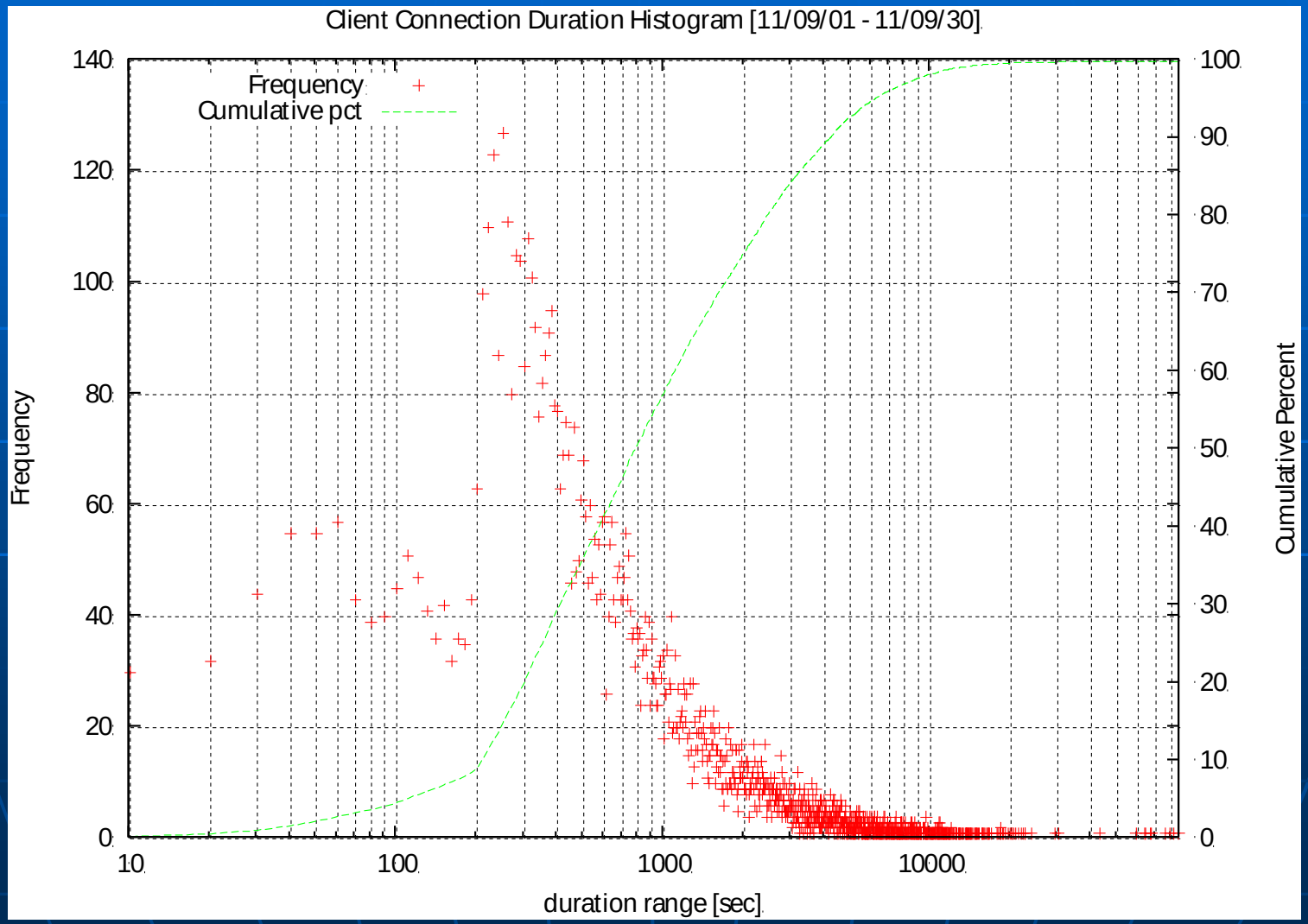


トラフィック(日)

- 2012/10/22 06:00～ 23:59



利用時間


Client Connection Duration Histogram [11/09/01 - 11/09/30]
Frequency
Cumulative pct
Frequency
Cumulative Percent
duration range [sec]
0
20
40
60
80
100
120
140
0
10
20
30
40
50
60
70
80
90
100
10
100
1000
10000

利用時間

- 200 秒から300 秒で利用を終了している
- 約60% の利用者は1000 秒以内に利用を終了
- 約73% の利用者は2000 秒以内に利用を終了
- 約83% の利用者は3000 秒(50 分) 以内
- 約90% の利用者は3600 秒(60 分) 以内

その他

- ログインゲートページをOauthのアプリケーションとして実装
  - 例）Facebook上にアカウントがあれば利用可能
- 複数の認証システムの利用可能

今後の課題

- 様々な環境での適用可能性の検証
  - 透過的Proxy
    - 持ち込みPCセグメントでの利用
  - セキュアProxy
    - ゲスト用の無線LANでの応用

まとめ

- Webアクセス制御を対象としたシングルサインオンシステム
  - 筑波大学の附属図書館のキオスク端末を対象にして実運用を行った報告
- スクリーンセーバを活用したログアウト忘れに対する対策方法の提案