

# Web Application のための Single Sign On と Authorization 環境

– Central Authentication and Authorization Service –

内藤 久資 (Hisashi NAITO)

naito@math.nagoya-u.ac.jp

名古屋大学多元数理科学研究科

**and**

名古屋大学情報連携統括本部情報戦略室



- 共同研究者：  
梶田将司氏 †, 平野靖氏 ‡, 小尻智子氏 ‡, 間瀬健二氏 †  
† (名古屋大学情報連携基盤センター  
名古屋大学情報連携統括本部情報戦略室)  
‡ (名古屋大学情報連携基盤センター)
- 研究協力者：  
小村道明氏, 福山貴幸氏  
(株式会社エミットジャパン)



# Plan of Talk

- CAS と CAS<sup>2</sup> の簡単な解説
- CAS の認証メカニズムと CAS<sup>2</sup> の権限管理メカニズム
- CAS<sup>2</sup> と「名古屋大学ポータル」
- CAS<sup>2</sup> と CSI 計画
- まとめ

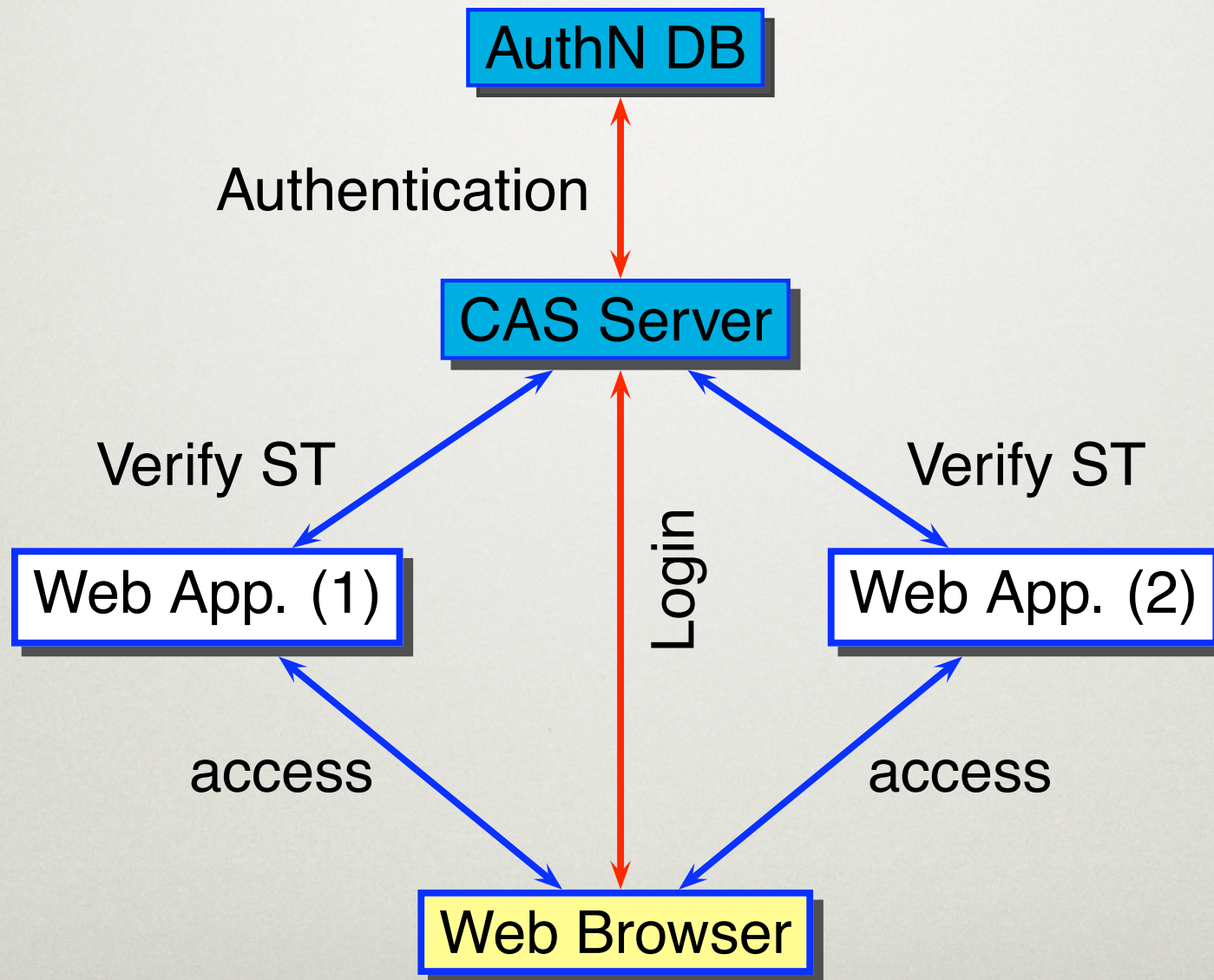


# What is CAS

- CAS (Central Authentication Service)
  - Web Applications に対する Single Sign On Infrastructure
  - Yale University で開発された Open Source Software  
現在は JA-SIG の Official Project
  - Single Sign On 環境を極めて簡単に実現できる
  - Current Version: 3.0.5-final  
<http://www.ja-sig.org/products/cas/>



# SSO Infrastructure using CAS





# What is CAS2

- CAS<sup>2</sup> (Central Authentication & Authorization Service)

- CAS<sup>2</sup> = CAS + アクセス権管理機構

- 複数の Application に対して, 個別にアクセス権を管理

- WHO

- 各 Application に対するユーザのアクセス権限

- WHEN

- 各 Application に対するアクセス時間帯制限

- WHERE

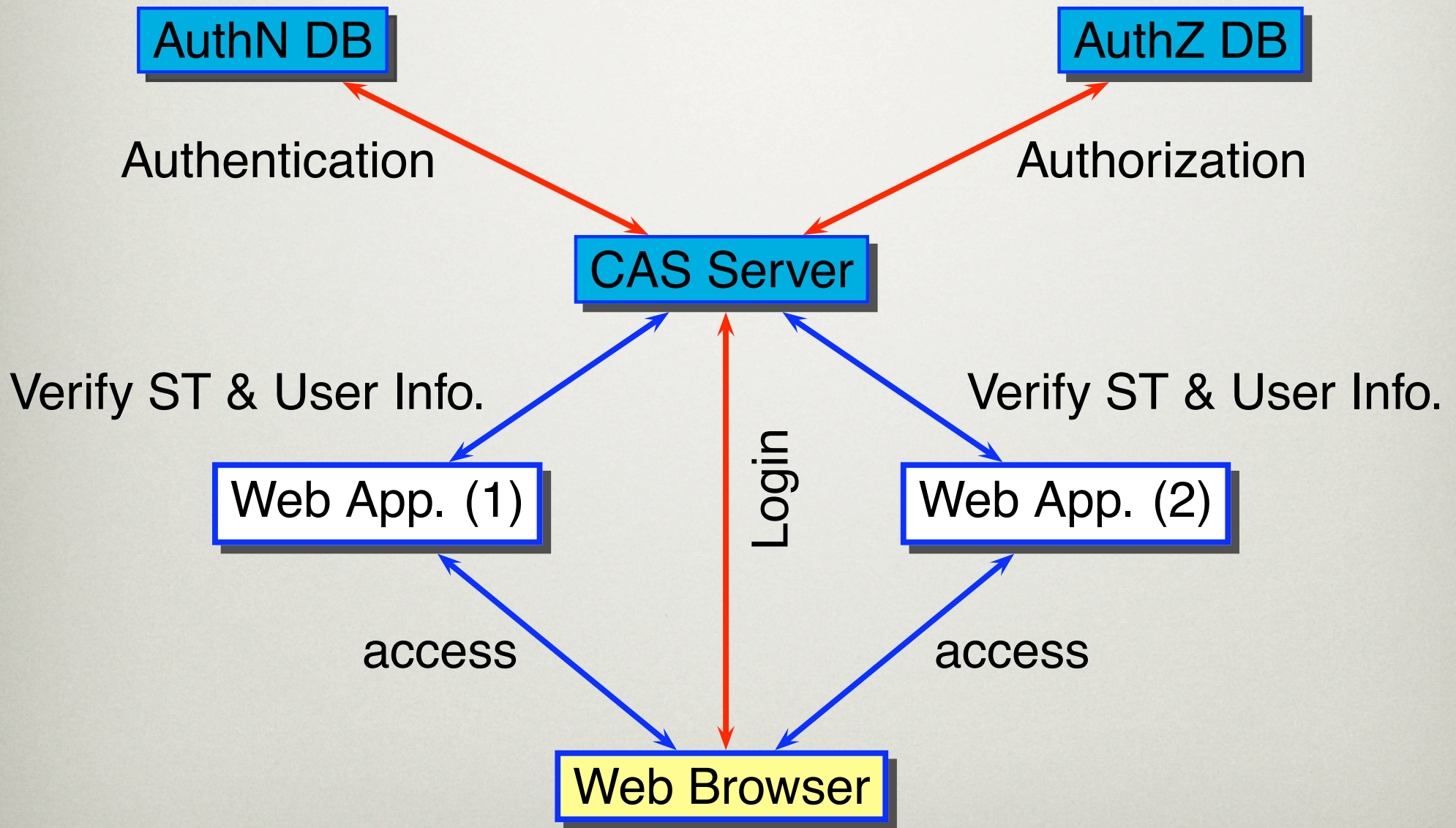
- 各 Application に対するアクセス元による制限

- HOW

- 各 Application に対して, Login ユーザのセキュリティレベルによる制限



# SSO and Authorization Infrastructure using CAS





# Mechanism of CAS and CAS2

## ● Ticket Granting Cookie (TGC)

- 「Browser が TGC を持っていること」  
= 「Browser は 認証済である」

## ● Service Ticket (ST)

- Web Application へのアクセスのための One Time Ticket
- Authorization Information を含んでいる
- 「有効な ST を持っていること」  
= 「アクセスは Authorized されている」



# Authorization Mechanism of CAS2

- 権限管理のためのデータベース (CAS-ACL)
  - Access Permission Lists:
    - WHAT**      どの Web Application に対して？
    - WHO**        だれが (User Information) ？
    - WHEN**      いつ (Access Time) ？
    - WHERE**     どこから (Client Information) ？
    - HOW**        どのようにして (Login Method) ？
- **ST** は CAS-ACL のどのエントリに一致しているかの情報を持っている



## Example of CAS-ACL

**dn:** `cn=entry1,ou=portal,ou=cas,o=nagoyaUniv`

**cas-service:** `https://app.*\.mynu\.jp/.*`

**cas-allow:** `(&(uid=naito)(date>=20051010)  
(date<=20051110)(IP=133.6.130.0/24))`

**cas-attributes:** `uid,mailAddress,FullName`

**cas-security-level:** `X509`



## Example of CAS-ACL

- URL が `https://app.*\.mynu\.jp/.*` に一致したとき：
  - `uid` is `naito`
  - Access 日時が **2005/10/10** から **2005/11/10** の間
  - Client IP が **133.6.130.0/24** にマッチ
  - Login Method が クライアント証明書を利用このときに限りアクセスが許可される
- CAS Server は Web Application に対して `uid,mailAddress,FullName` を送化する



# CAS2 in Nagoya University Portal

- 以下の Application 群の SSO & Access Control
  - 名古屋大学ポータル
  - 新教務システム（履修登録・成績入力）
    - 約 10000 人の学生と, 約 2000 人の教員
  - 研究者統合データベース
    - 約 2000 人の教員
  - Web CT
  - ...



## UPKI and CAS2

- PKI を利用したセキュアな Application へのアクセスの実現
  - 統一認証基盤の下で, **セキュアにしたい** Application のみに PKI を利用できる
- 近日中に「公開版 CAS<sup>2</sup>」を Open Source で公開予定
  - 誰でも容易に SSO とアクセス管理を実現可能



# Summary

- CAS<sup>2</sup> を使えば...
  - SSO 環境を容易に構築可能
  - 統一的なアクセス権限管理環境を容易に構築可能
- CAS<sup>2</sup> はセキュア :
  - Web Application はユーザ認証情報を一切受け取らない
  - Web Application はユーザDBにはアクセスしない
- CAS<sup>2</sup> は余分なものを必要としない :
  - tomcat
  - 通信路暗号化のための SSL
  - Web Application を CAS<sup>2</sup> 化することが容易 :  
CAS client module を組み込むことだけ



## Bibliograph

- 内藤久資, 梶田将司, 小尻智子, 平野靖, 間瀬健二,  
大学における統一認証基盤としての CAS とその拡張,  
情報処理学会論文誌, Vol. 47, No 4, 1127-1135, (2006)
- 内藤久資, 梶田将司,  
Central Authentication and Authorization Service  
–Web Application のための新しい認証システムの試み–,  
京都大学数理解析研究所講究録, Vol. 1446,  
「電子情報交換に関する最近の話題」, 14-39, (2005)
- JA-SIG, <http://www.ja-sig.org/products/cas/>



**END**