＝日本学術振興会産学協力研究委員会＝
インターネット技術第163委員会
JSPS 163rd Committee on Internet Technology
第21回インターネット技術第163委員会研究会 -ITRC meet21-

大阪大学　事務基幹系システムへのThinClient導入について

＝Sun Rayによるスマートカードログオン事例紹介 ＝

2007年05月31日

長岡亨+, 下條真司+, 米村直樹++, 斉藤圭吾+++

+ 大阪大学
++ サン･マイクロシステムズ
+++ 日本ベリサイン

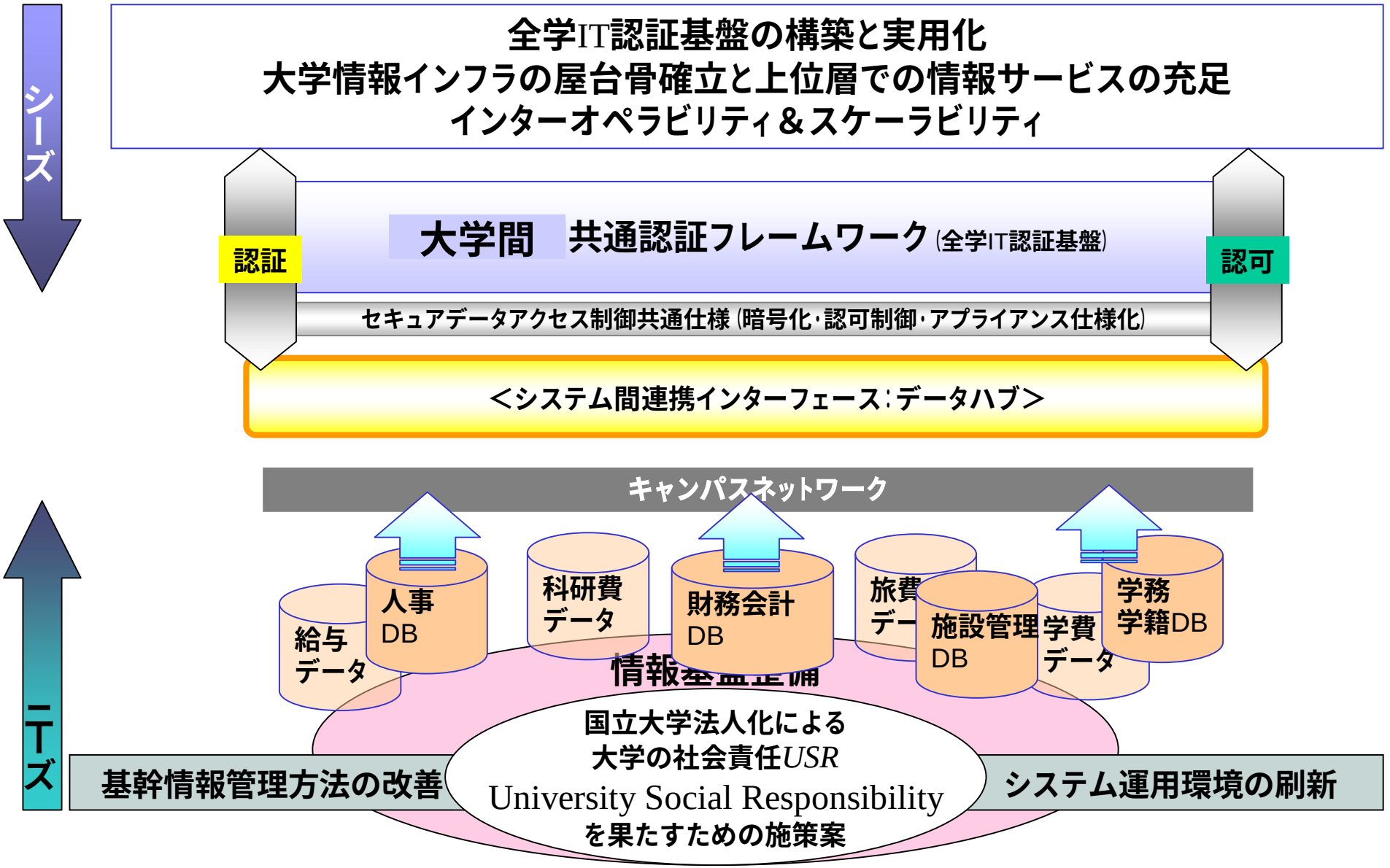
要約

概要：
本学では、情報漏洩防止などのセキュリティ強化のため、ThinClientを用 いた事務基幹系システムの導入整備を戦略的に取り組んでいる。
ThinClientの利用に際しては、電子証明書による個人認証を必須とし、ICカードによるスマートカードログオンで実現した。また、全学IT認証基盤（PKI/SSO)システムの運用を本年度より本格的にスタートさせており、全学主要システム間のSSO連携に対応するS.B.C.(Server Base Computing)試行開発にも取り組んできた。
本稿では、これら導入の経緯及び、当該システムについての実装等に関して紹介するものである。

本日の内容

1. はじめに
2. 大阪大学におけるThinClient導入実績状況
3. スマートカードログオンとは
4. Sun RayのICカード利用によるログイン
5. 大阪大学ThinClientのスマートカードログオンについて
6. 全学ActiveDirectoryの設計と導入について
7. スマートカードログオンからSSOへの連携について

はじめに


シーズ
全学IT認証基盤の構築と実用化
大学情報インフラの屋台骨確立と上位層での情報サービスの充足
インターオペラビリティ＆スケーラビリティ
認証
大学間 共通認証フレームワーク (全学IT認証基盤)
認可
セキュアデータアクセス制御共通仕様 (暗号化・認可制御・アプライアンス仕様化)
＜システム間連携インターフェース：データハブ＞
キャンパスネットワーク
人事 DB
給与 データ
科研費 データ
財務会計 DB
旅費 デー
施設管理 DB
学費 データ
学務 学籍DB
情報基盤整備
国立大学法人化による
大学の社会責任USR
University Social Responsibility
を果たすための施策案
ニーズ
基幹情報管理方法の改善
システム運用環境の刷新

実証のねらい

ICカードを認証トークンとし、**電子証明書による個人認証を用いた（必須とした）**全学規模の
ThinClient実行環境の構築（技術的視点とミッションクリティカルな業務への適用性評価）

**いつでも・どこでも・欲しい情報に
安全に手が届く大学基幹系システム
の基盤環境の実現**

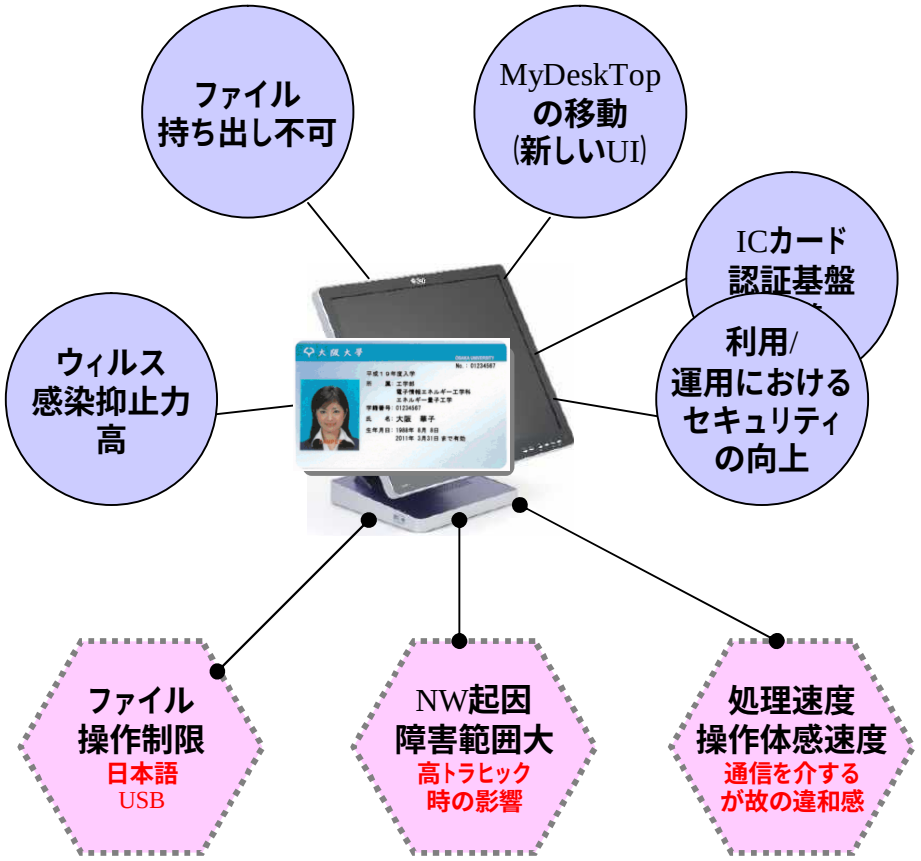
キャンパス内ユビキタス的な、新しい情報アクセス環境のリファレンスモデルの提示

○大学運営組織側が期待する効果

**大学情報を外部媒体を介して
持ち出せない/させない**

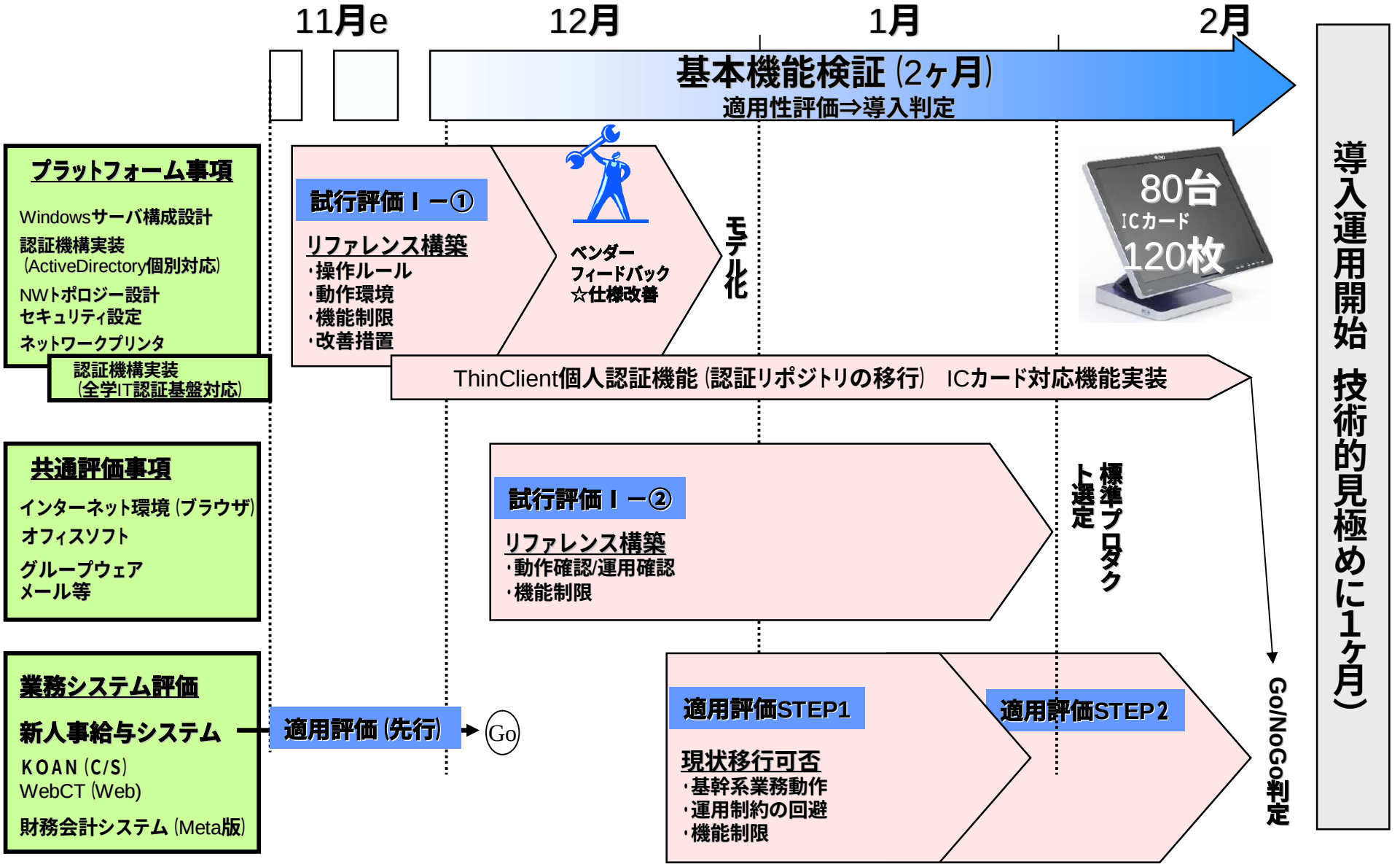
ウィルスを持ち込ませない
（ネットワークからも、人為的操作からも）

センター一元運用監視・管理
（全学均一なセキュリティレベルの保持）

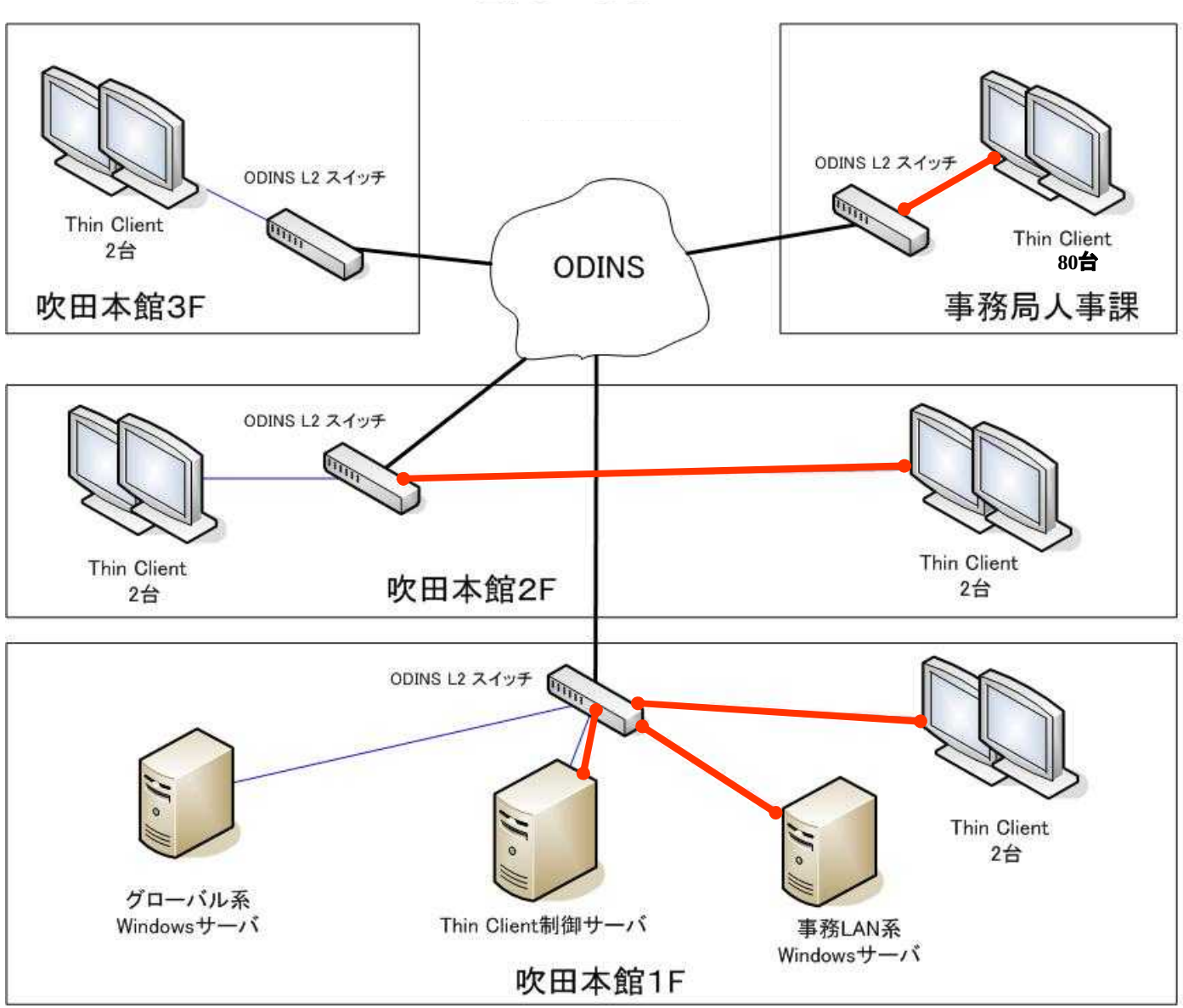


できること／できないこと（トレードオフの評価）

大阪大学におけるThinClient導入実績状況（1／2）



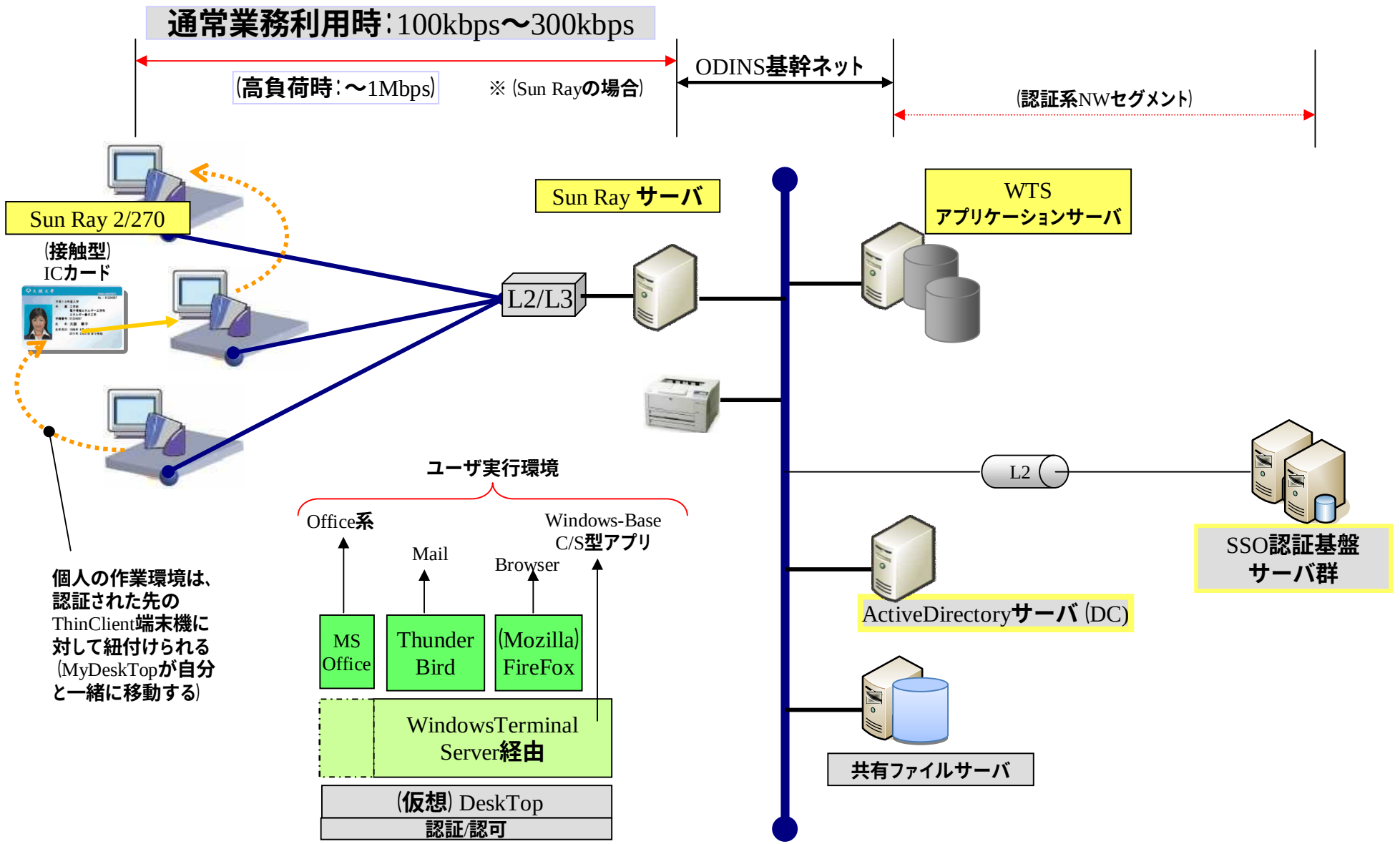
大阪大学におけるThinClient導入実績状況（2／2）



●ThinClient**端末**
Sun Ray 270 / 2
(Sun Ray Server Software)
●**認証ソリューション**
日本VeriSign
Kerberos-Smartcard-Logon

●IT/SSO**認証基盤**SYS
Sun Java System
- Identity Manager
Sun Java System
- Access Manager

Sun Ray導入のイメージ

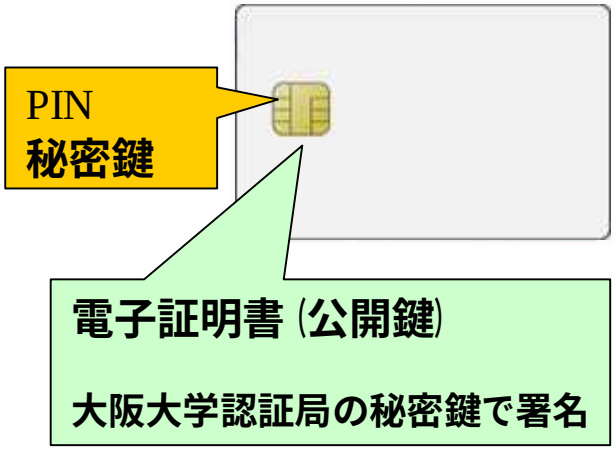


スマートカードログオン‥概略

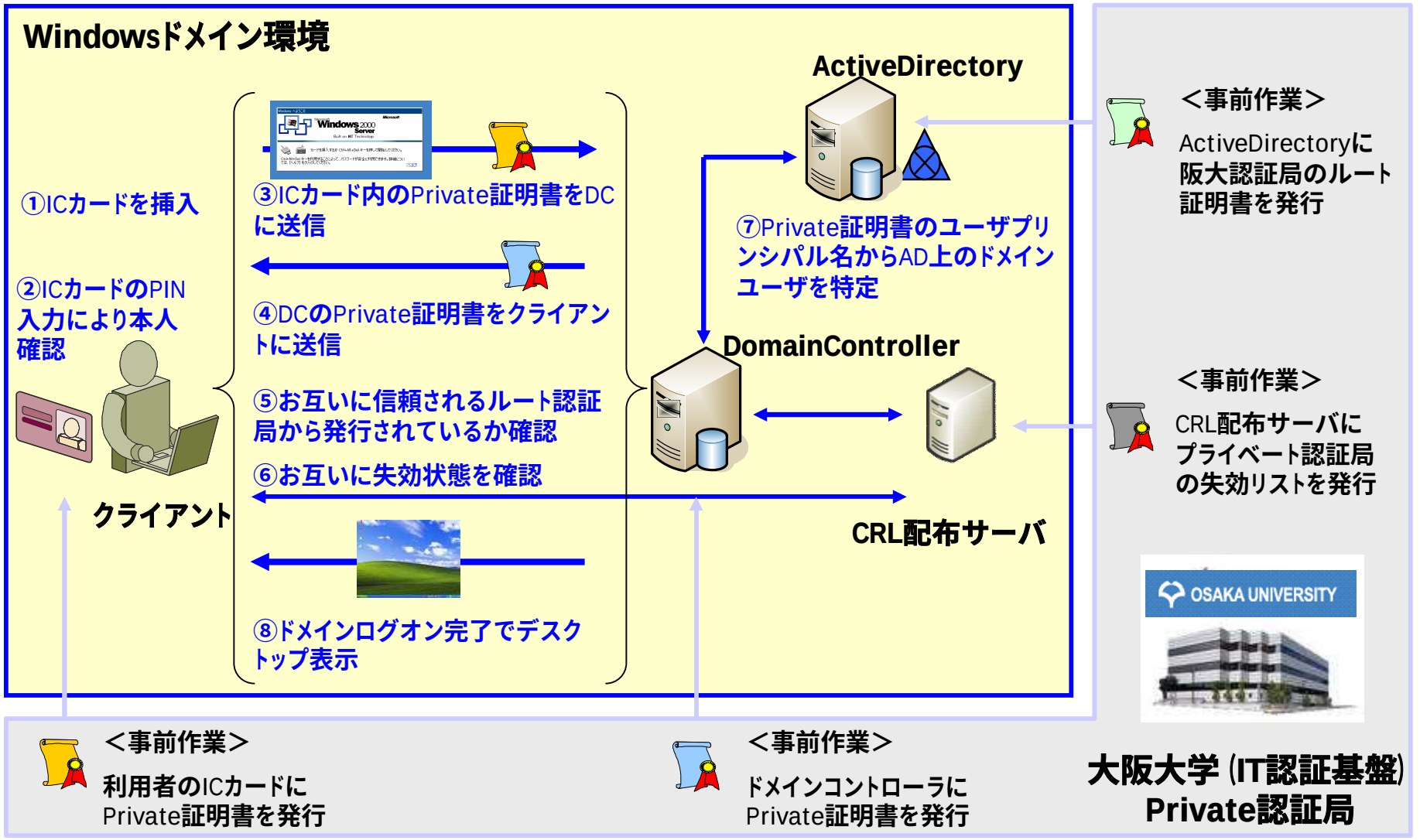
- **概要**
  - ICカードを利用した**Windowsドメイン**へのログオン認証
  - PKIの概念を導入した強固な認証が可能
  - スマートカードログオンに対応した電子証明書が必要

ROLE

- **利用者**
  - パソコンに接続されたICカードリーダにICカードを挿入
  - 本人確認のためICカードのPIN入力
- **システム管理者**
  - ログオン認証の種類を設定
    - ID／パスワード認証と併用
    - スマートカードログオン認証必須
  - ICカードを抜いたときの振る舞いを設定
    - コンピュータのロック
    - ログアウト

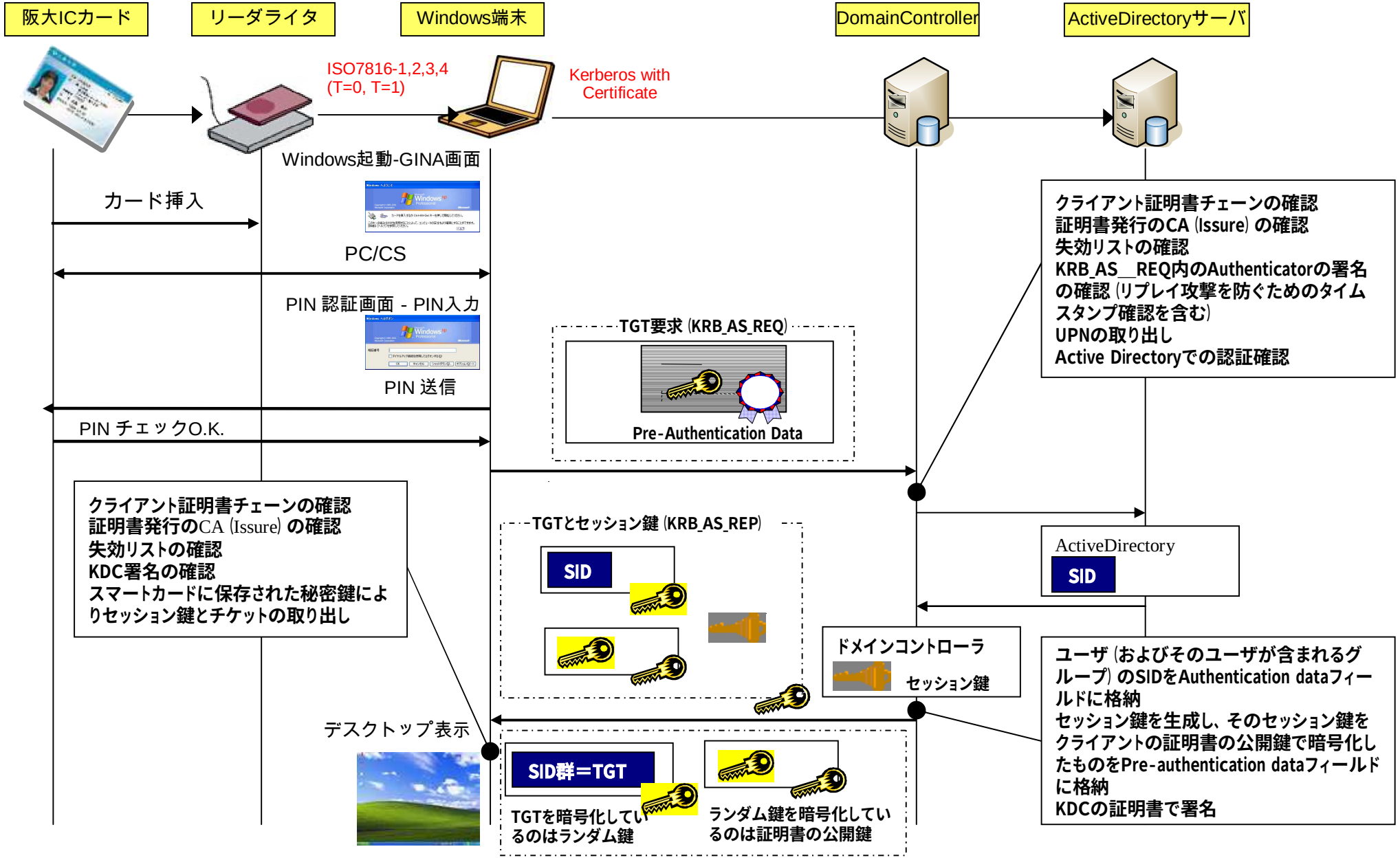


スマートカードログオンとは・・



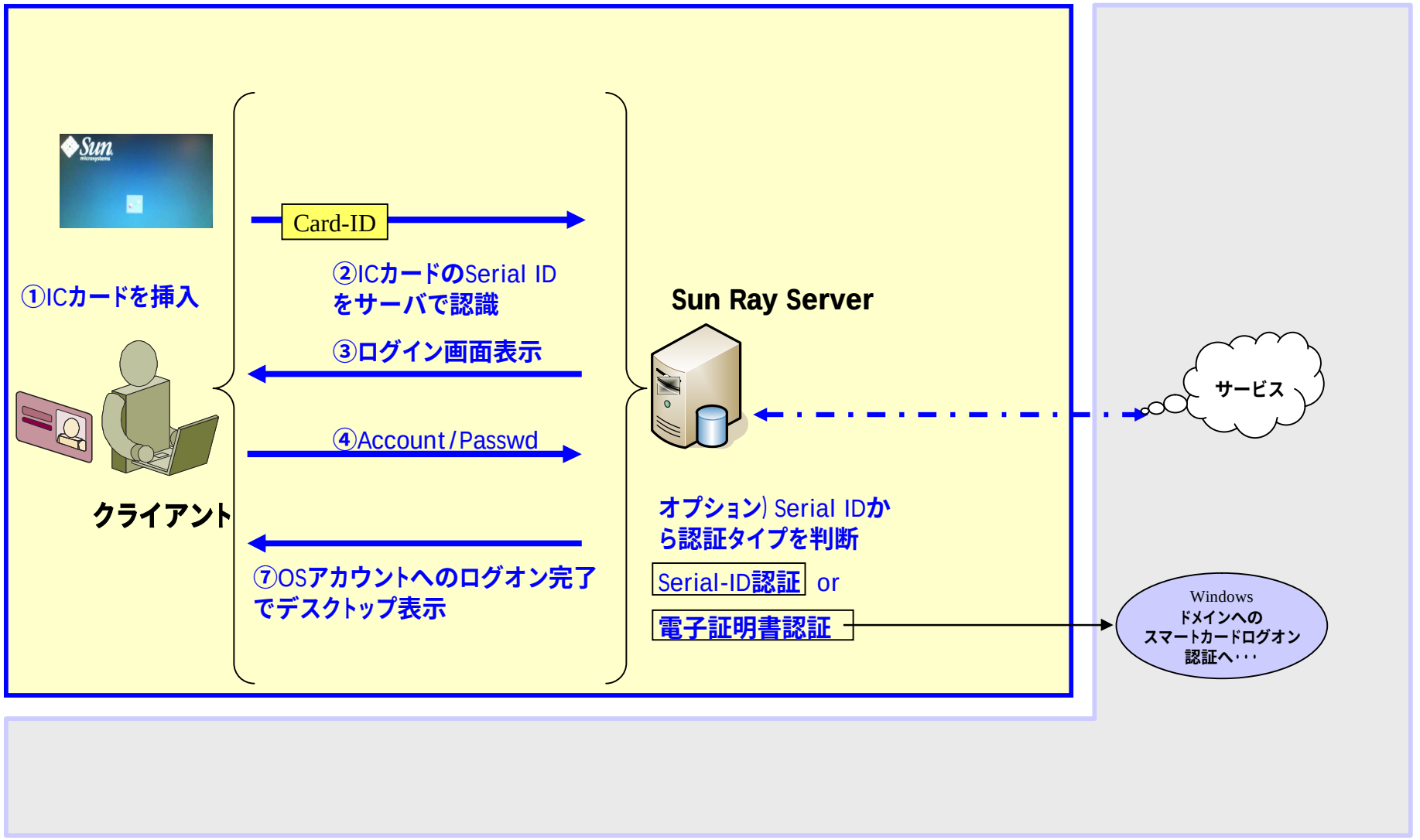
Kerberos Smartcard Logon (with Certificate)

参考) Windowsドメインのスマートカードログオン：プロダクト仕様

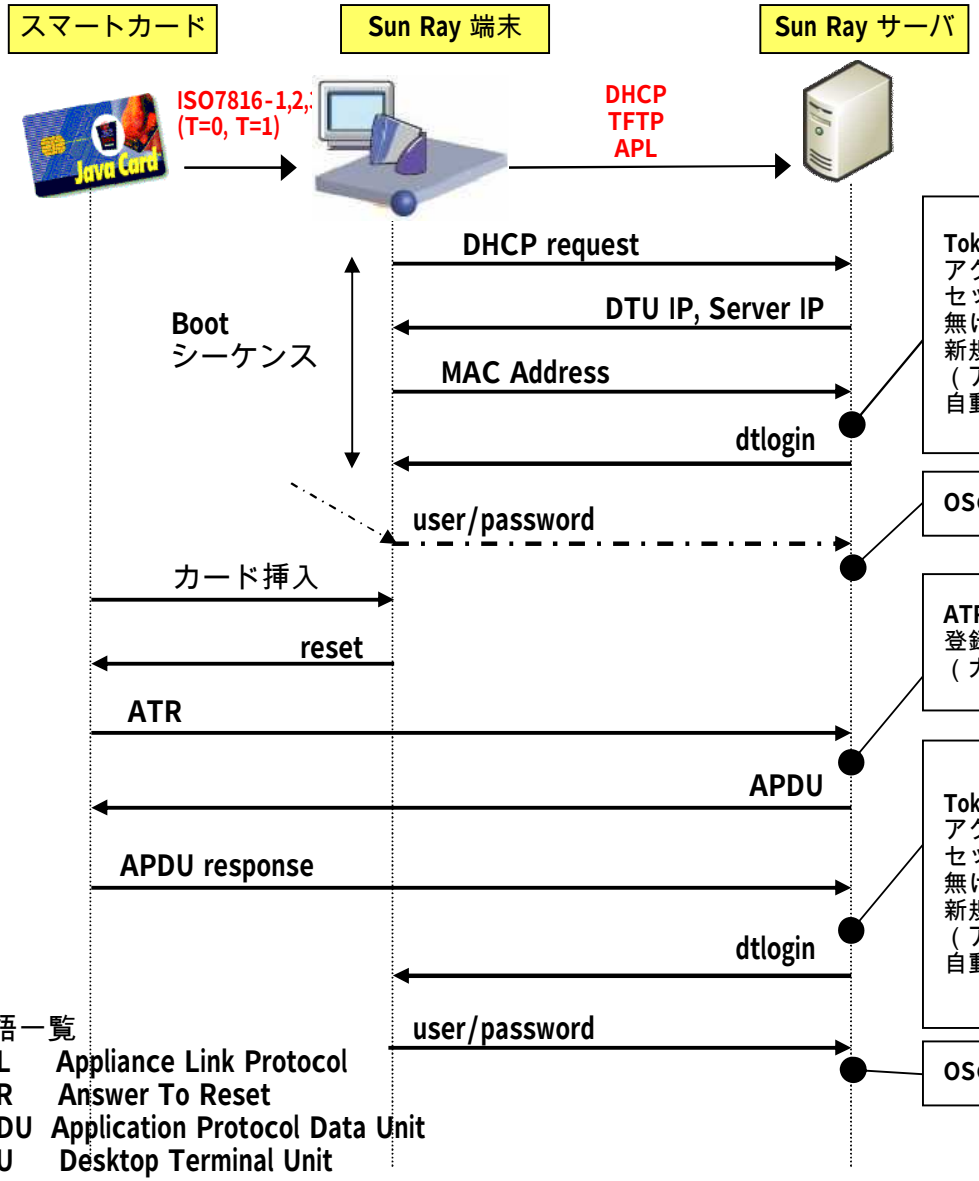


Sun RayのICカード利用によるログイン

Solaris OSへの認証手続き



参考) Sun RayのICカード利用ログインのプロダクト仕様



Sun Ray のスマートカードによる認証には２段階ある。

●STEP1

:カードのタイプ･シリアルIDに対する認証　（カードがアクセス可能か）

●STEP2

:Sun Ray サーバOSに対するログイン認証（ユーザ、パスワードは正当な組合せか）

TokenID (pseudo.MACADDRESS) のアクセス権限をチェック
アクセス許可の場合 TokenIDに対するセッションを検索
セッションが既にある場合そのサーバにリダイレクトしセッションを再開
無ければ負荷の低いサーバにリダイレクトしセッションを生成
新規セッションの場合は口グイン画面を表示
（アクセス制御モードの場合は、専用ユーザで
自動口グインして指定されたアプリケーションを起動）

OSのユーザアカウント機構(LDAP, NIS, /etc/shadow 等)で認証

ATRからカードタイプが登録されているか検索
登録済みの場合、カードタイプに応じた APDU等を発行
（カードによっては APDUにてカードタイプを特定する場合もあり）

TokenID (cardType.cardID) のアクセス権限をチェック
アクセス許可の場合 TokenIDに対するセッションを検索
セッションが既にある場合そのサーバにリダイレクトしセッションを再開
無ければ負荷の低いサーバにリダイレクトしセッションを生成
新規セッションの場合は口グイン画面を表示
（アクセス制御モードの場合は、専用ユーザで
自動口グインして指定されたアプリケーションを起動）

OSのユーザアカウント機構(LDAP, NIS, /etc/shadow 等)で認証

略語一覧

APL　Appliance Link Protocol
ATR　Answer To Reset
APDU　Application Protocol Data Unit
DTU　Desktop Terminal Unit

 # 主要なシーケンス及びパターンのみを抜粋

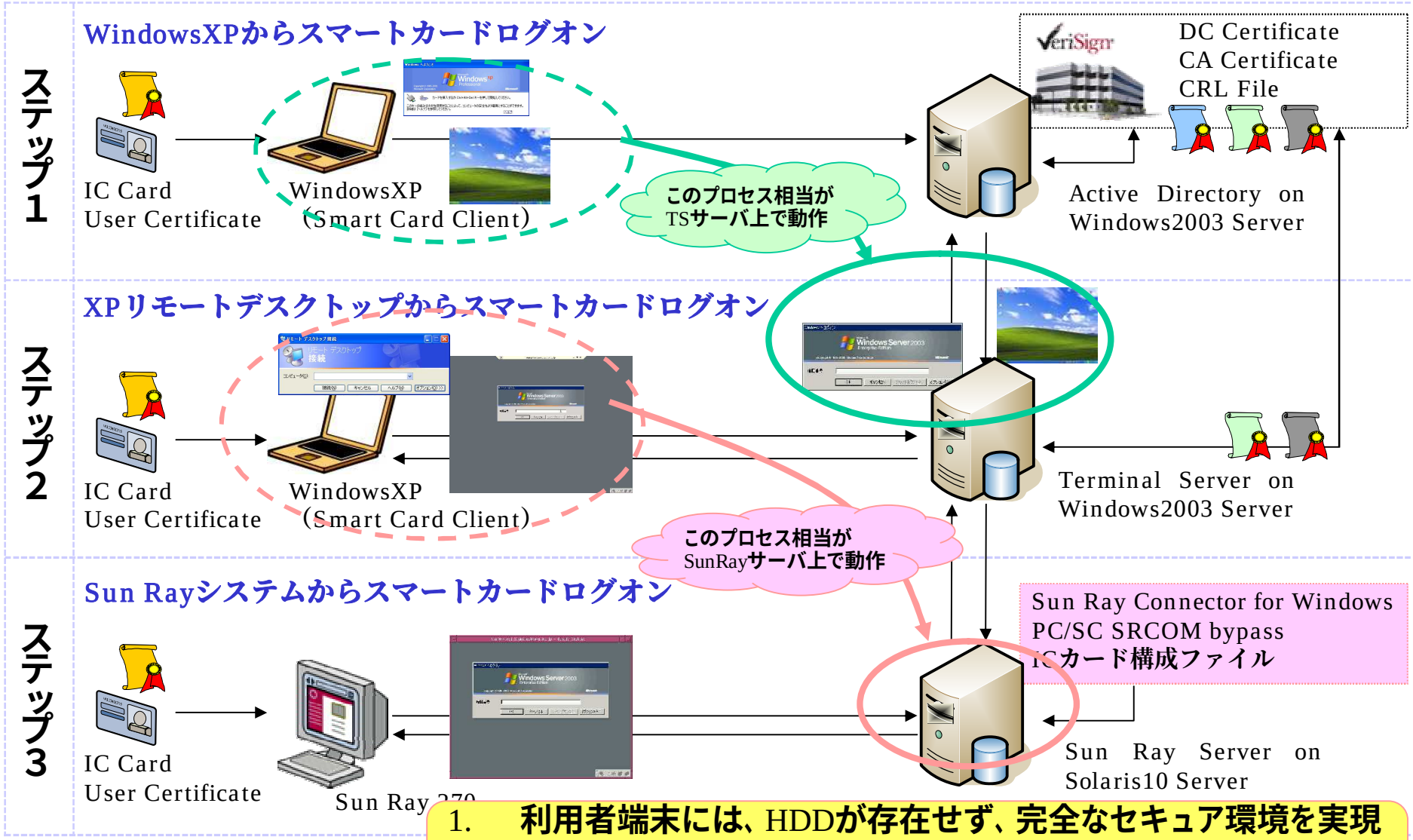
大阪大学ThinClientのスマートカードログオンについて

- 方針
  - 本人認証に全学IT認証基盤システムの利用者証明書とICカードを利用
  - 事務基幹系システムの移行においては、既存のクラサバシステムの環境を維持
  - シンクライアントシステムには、Sun Microsystems のSun Rayを採用
  - スマートカードログオン対応ICカードと、電子証明書には、VeriSignのマネージドPKIサービスを採用

- 検証
  - 事前準備：Sun Ray Serverと、Sun Rayクライアントの手配
  - ステップ1：Windowsネイティブのスマートカードログオン環境準備
  - ステップ2：上記にターミナルサービスを追加しスマートカードログオンを実施
  - ステップ3：上記にSun Rayシステムを組み合わせてスマートカードログオンを実施

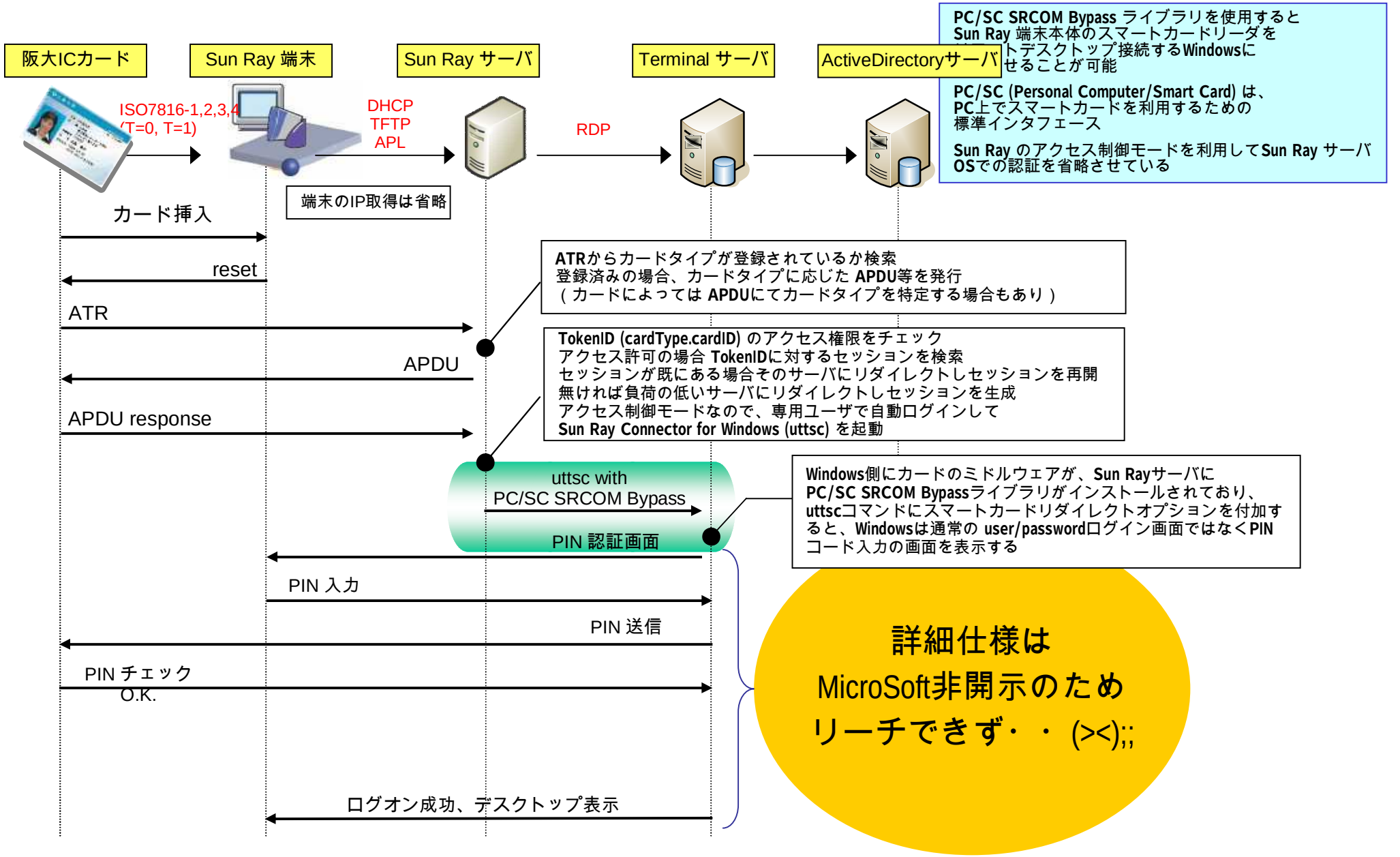
- 構築
  - 大阪大学が事務用端末としてSun Rayシンクライアントを採用
  - （全学IT認証基盤と連携したシングル・サインオンも実現）
  - http://jp.sun.com/company/Press/release/2007/0312.html

検証：スマートカードログオン導入ステップ

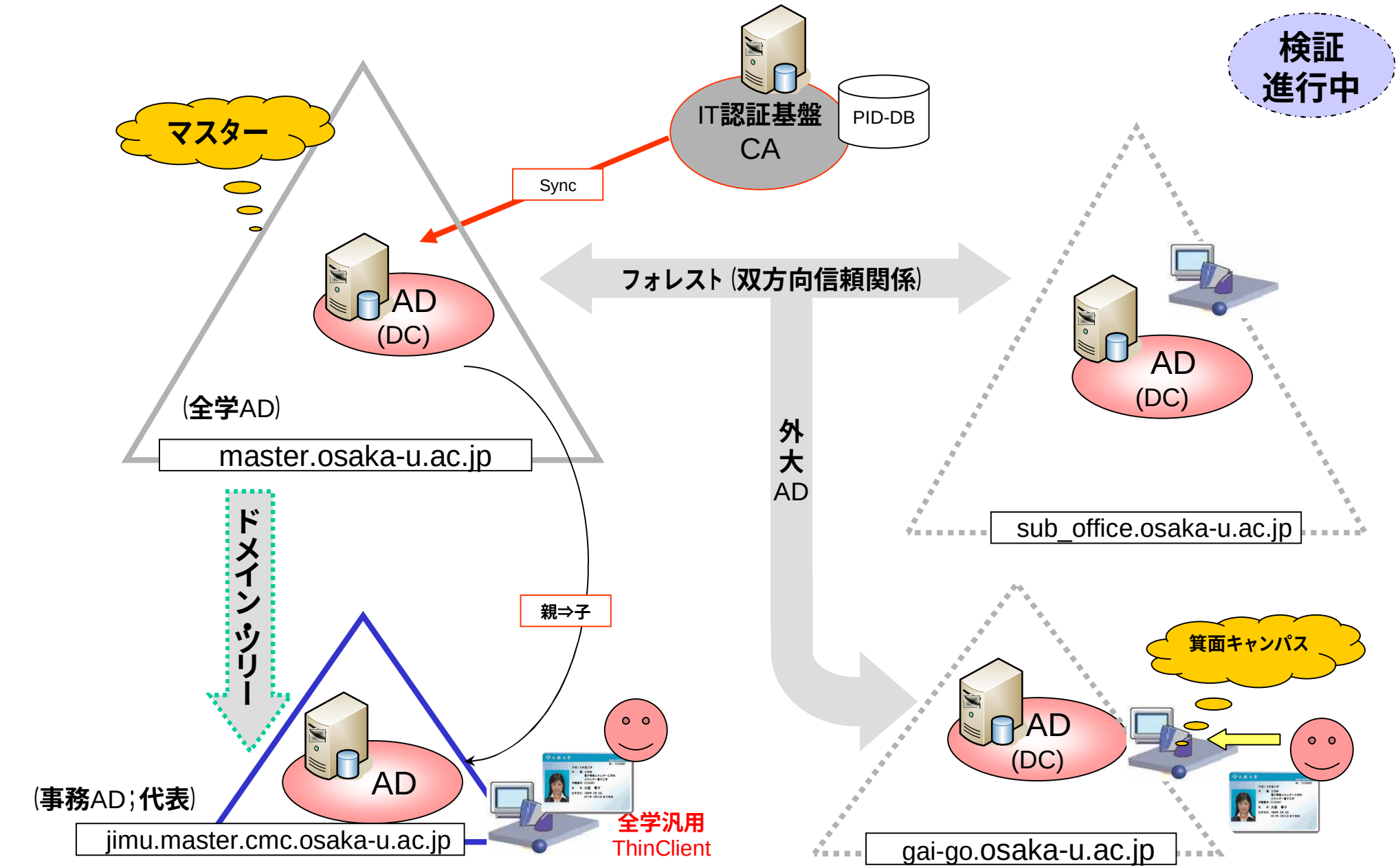


1. **利用者端末には、HDDが存在せず、完全なセキュア環境を実現**
2. **ICカード（電子証明書）と、PIN入力の2要素で本人認証を実現**
3. **Sun Rayシステム（Solarisベース）と、Windows環境を統合**

参考）処理シーケンス概略

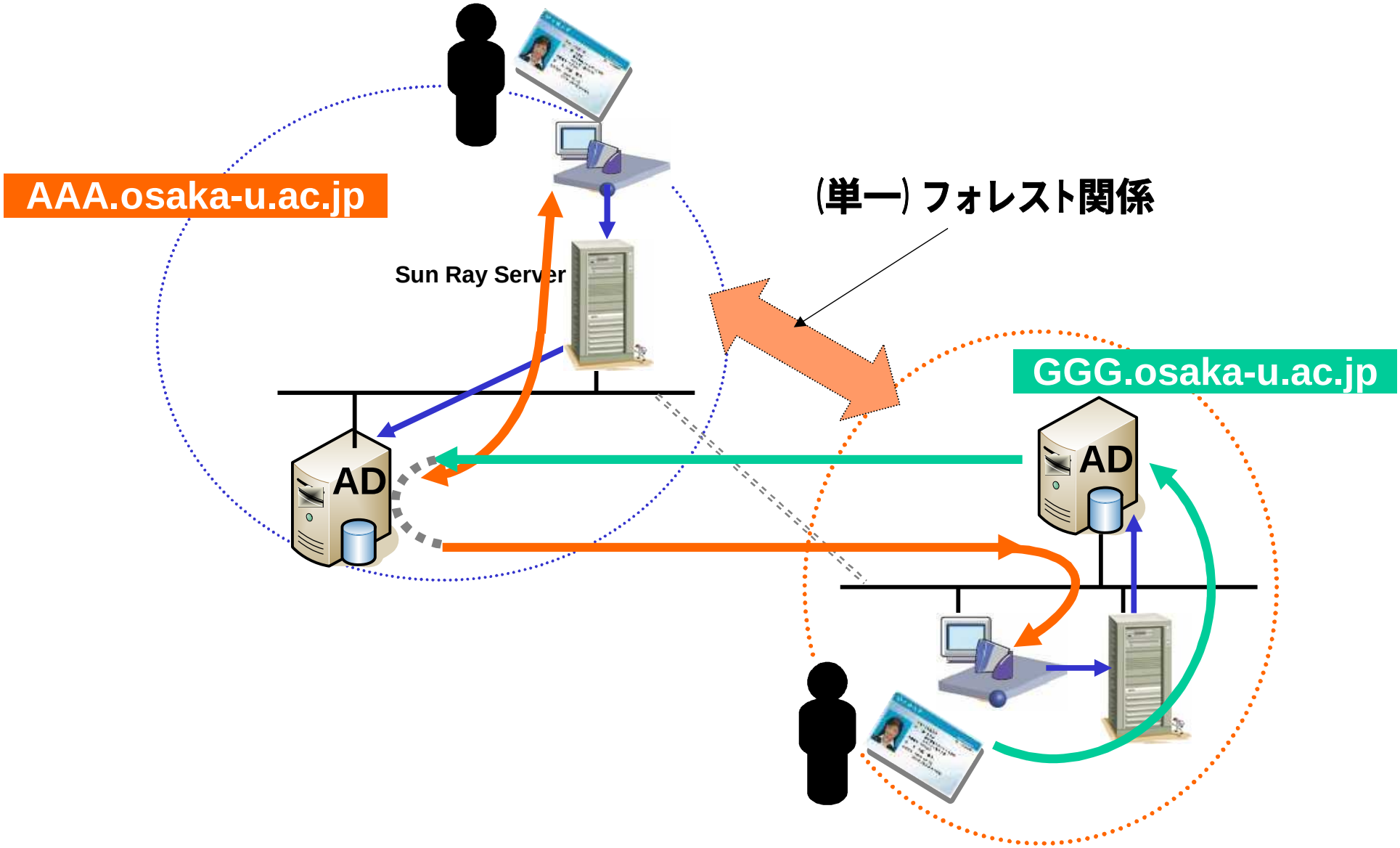


全学ActiveDirectoryの設計と導入について

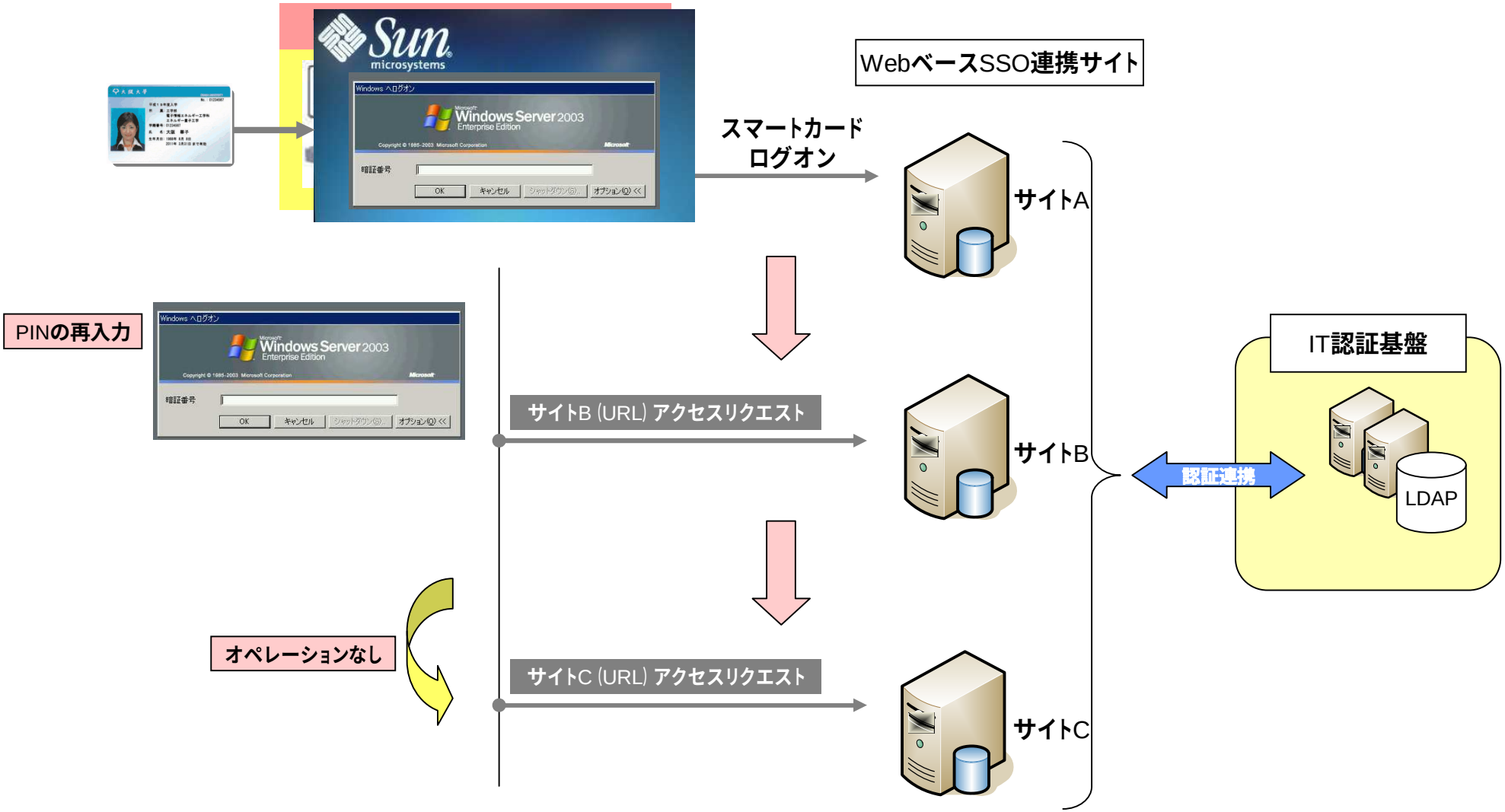


ドメイン間のモビリティについて（継続検証中）

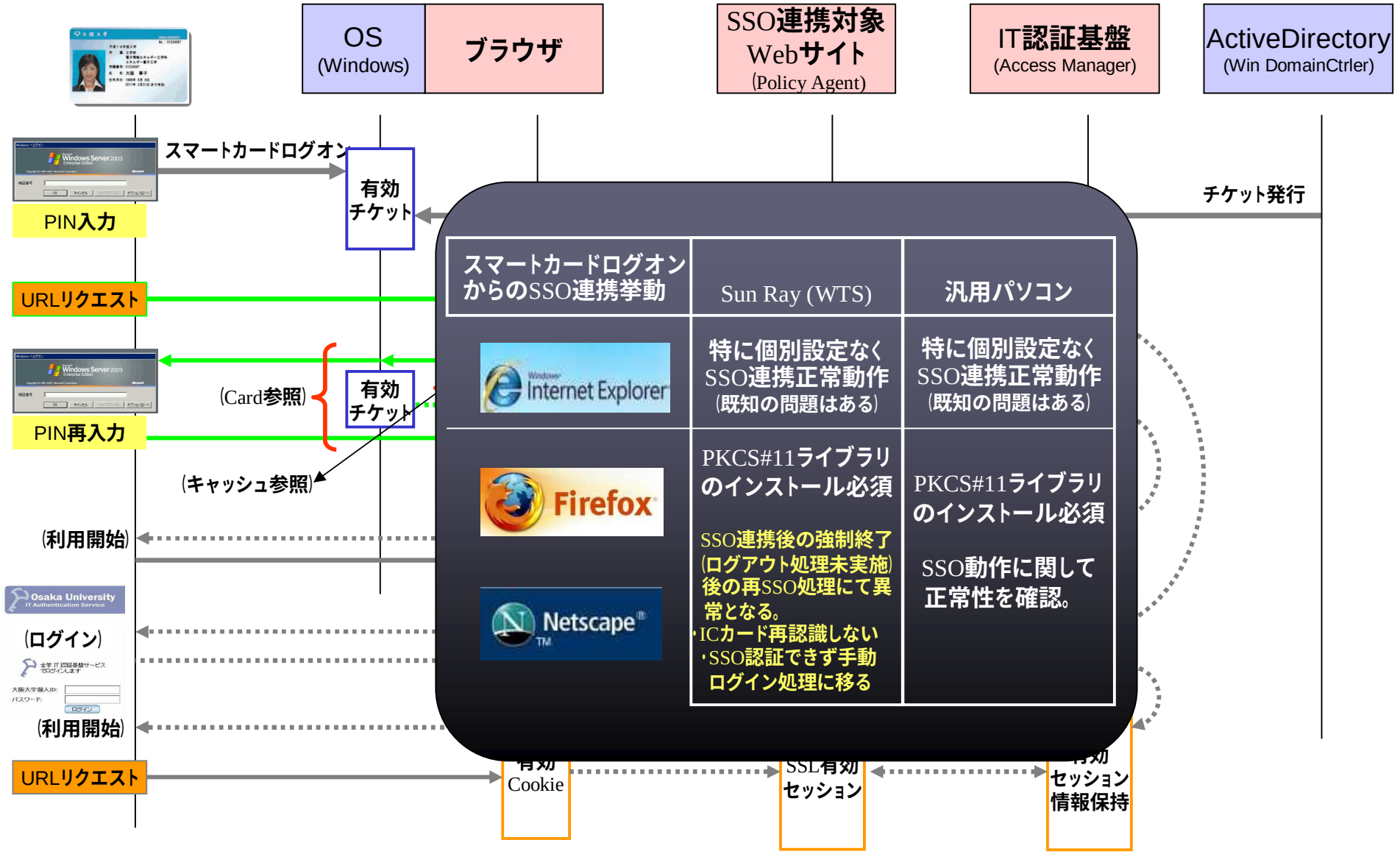
ICカードに書き込んであるドメイン=AAA.osaka-u.ac.jp　の場合



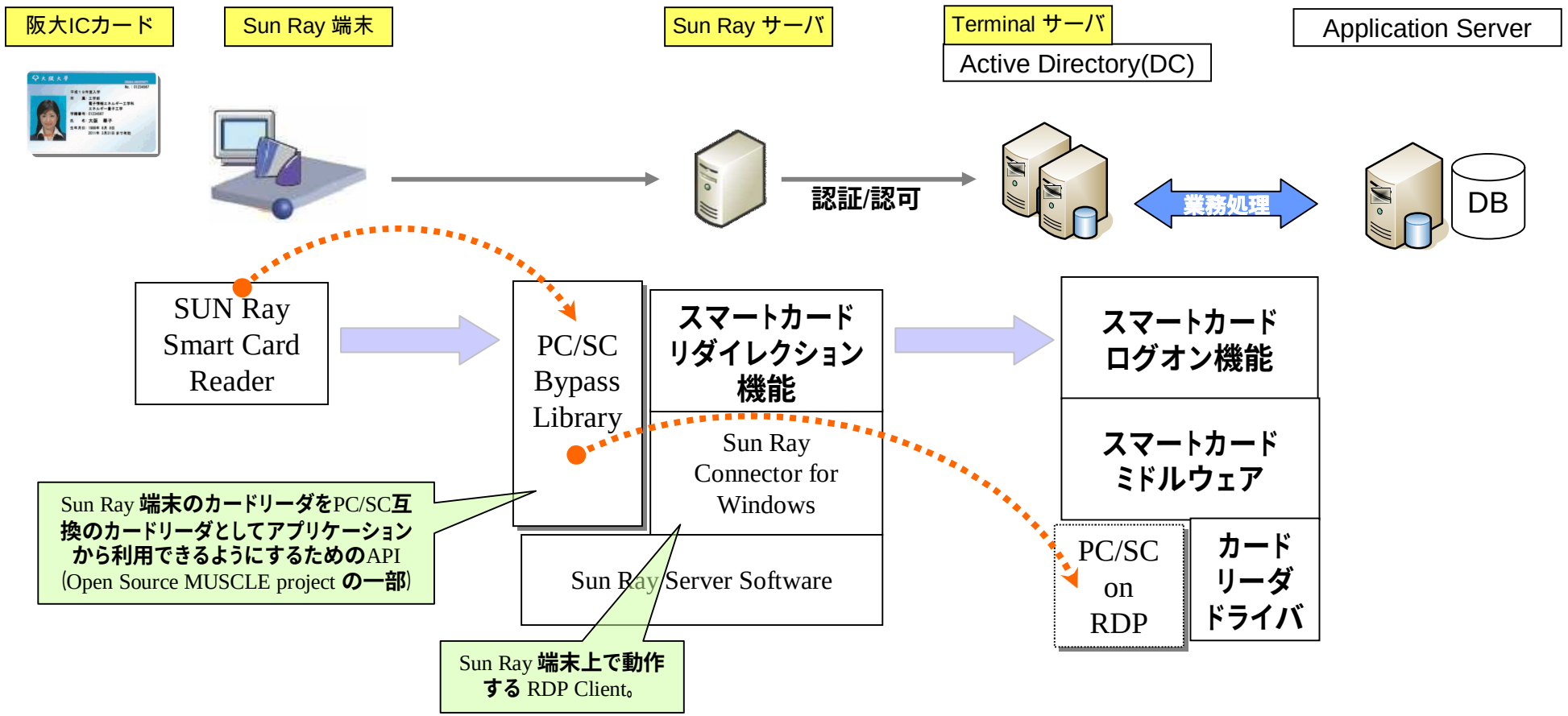
SSOオペレーションイメージ：実装差異／動作環境差異



参考）SSOオペレーションイメージ：ブラウザ実装差異／動作の差異

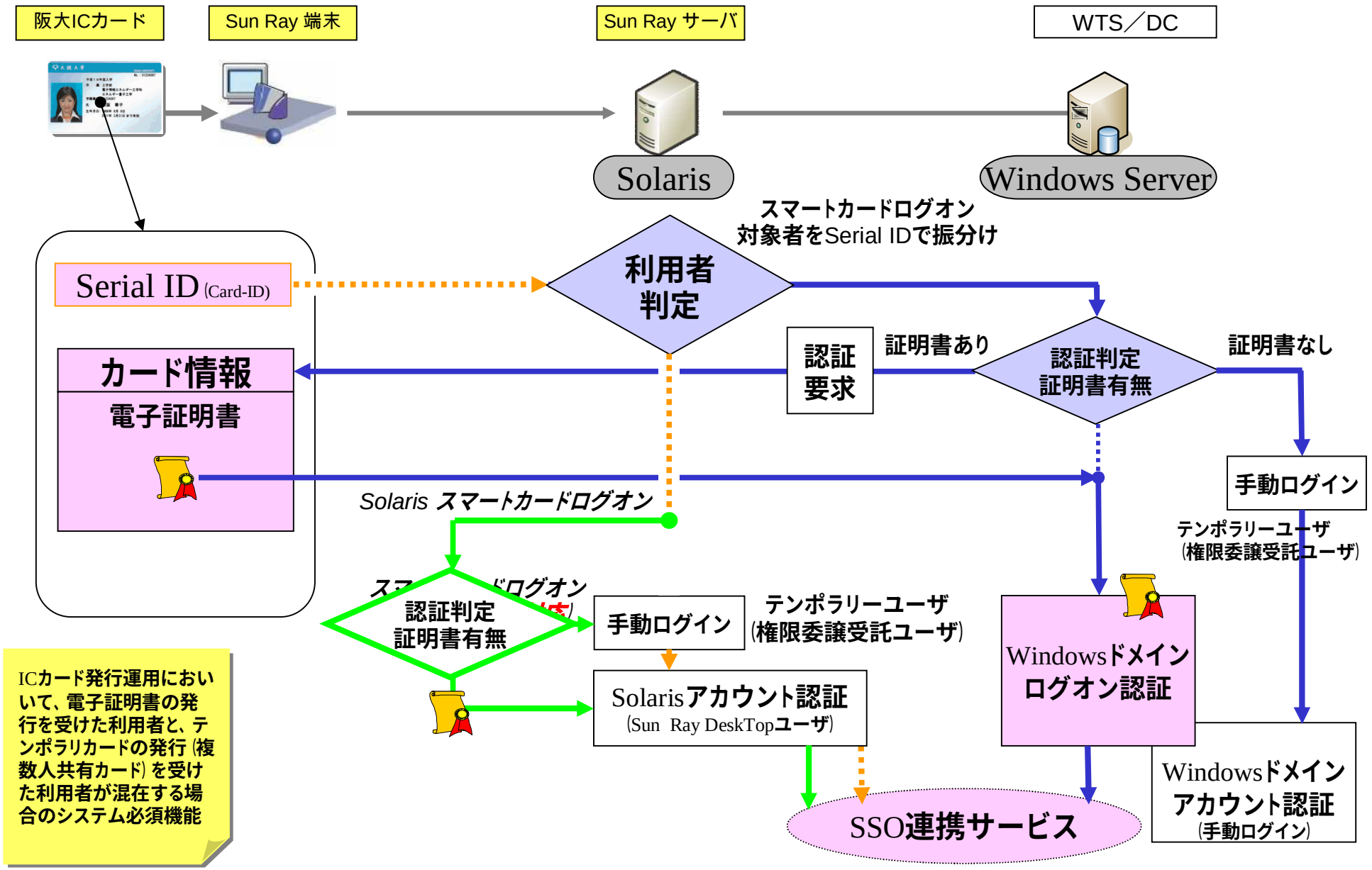


ノウハウ1) Sun RayとWTS(DC)の連携実装について



Sun Ray サーバにて、PC/SC Bypass libraryとSun Ray Connector for Windows のスマートカードリダイレクション機能を適用し、Windows Terminal Server 上のアプリケーションから Sun Ray 端末のカードリーダにアクセス、ICカードに格納されたクライアント証明書などの情報を読み取り、ログイン認証やブラウザ・メーラ等でのクライアント認証及び電子署名、暗号化等の実行環境を実現。

ノウハウ2) ICカードによる認証振り分け



ノウハウ3) WTS (Windows Terminal Server) 環境における不具合 …. (><);;

リエントラント実装対応になっていないアプリケーションでも、利用は避けられない

ThinClient環境の適用により多くの場合、WTS環境をRDPで利用する（1:n）。Office系パッケージを含め、Winパソコンベースのパッケージソフトは、通常インストールでは動作しないと思うべき。従ってSBC導入（取組み）決定は慎重に決断する必要が（入念な動作確認が）・・・ある。　さらにOwn-risk・・

＜見つけだした策＞

●アプリケーションの インストールディレクトリに対して、Authenticated_Userにフルコントロール を与えることで正常動作させることができることを発見（セキュリティ運用面では暫定措置としての域でしかない）。

●ただしインストールディレクトリ内で競合が発生する場合、コンピュータ名ごとにインストールディレクトリを複数用意し使い分けて利用する策は有効。

●*iniファイルのＰＡＴＨが素直なインストールでは通らない場合には、
HKEY_LOCAL_MACHINE¥SOFTWARE¥Microsoft¥Windows NT¥CurrentVersion¥Terminal Server¥Compatibility¥Applications 配下にレジストリ値を手動で追加する事で正常動作できる。

WTSダウン多発：SBCたるがゆえに業務アプリケーションの全停止回避の為に重要

重要パッチ情報

http://support.microsoft.com/kb/924806/ja

文書番号：９２４８００６
最終更新日：２００７／２／１
リビジョン：１．０
「クライアントがｓｅｒｖｉｃｅ ｐａｃｋ１でＷｉｎｄｏｗｓ Ｓｅｒｖｅｒ2003を実行しているサーバーでターミナルサービスセッションからログオフすると、停止エラーメッセージ：「０ｘ０００００ＡＢ >> （session_has_valid_pool_on_exit）を停止する」

今のところの評価) S.B.C.導入とスマートカードログオンに対しての評価

1. 利便性のUP

実行環境の高速化が図れる：アプリケーション起動時の高速化、処理そのものが体感的に高速

→一人に割り振る事が可能なリソースが大きいので、プログラム の起動時間も短く、レスポンスよく高速に動作するようでその点では利用者満足度UP。

→S.B.C の場合は通常サーバを起動しっぱなしであり、ユーザが帰宅する際もログアウトせずカードを抜くだけという運用なので、通常のPCに比べて、起動・終了・ログオン・ログアウトの時間も削減できている。

2. ADと認証基盤との間でのアカウント情報の自動同期の仕組み

→WindowsドメインにログインするためのAD**認証情報と、認証マスタデータに相当する認証基盤の認証情報を動的に同期更新する方法を至急確立する必要がある**(LDAP**から抽出できれば**)。

(案)

1. Sun Java System Identity Manager **より事務**AD **に必要なデータを直接同期**
2. **事務**AD **を廃止して全学**AD **を使用する**
3. **全学**AD **と事務**AD **間で何らかの同期を行う**

3. 全学ネットワークのトポロジ構成に密接に影響をうけるThinClient構成設計

→現行 Sun Ray**はDHCPで運用しており、**DHCP**サーバの論理位置やアドレス管理範囲が大きく影響する。**

選択肢として、Sun Ray **だけの** Private Network **を組む(遠隔地には** VLAN **で伸ばして)こと も考慮したが、大阪大学では** PC **のネットワークとの混在が避けられなかったので** Sun Ray **だけの** Private Network **を組まない構成で運用。**

※*SunRay次期バージョンでは DHCP だけではなく static IP アドレス での運用も実装予定らしい・・・*
http://www.sun.com/software/sunray/features_beta.jsp

参考）電子証明書による認証スキーム

- Kerberos認証ではKDC（キー配付センター：Key Distribution Center）が認証を実施
- Windows環境において、KDCはドメインコントローラー（DC）に相当
- ドメインコントローラにはドメインコントローラの電子証明書が必要
- 相互に信頼の連鎖を確認できることが必要
  - ICカード内の利用者証明書の有効期間を検証
  - 利用者証明書の信頼チェーン確認
  - 利用者証明書の発行元のCA（Issure）証明書の有効期間を検証
  - 各証明書の失効情報の確認
  - KRB_AS_REQ内のAuthenticatorの署名検証
    - リプレイ攻撃を防ぐためのタイムスタンプ確認を含む
  - 利用者証明書からUPN名の取り出し
  - Active Directoryでアカウント認証を実施
- 相互に行う失効情報の確認では、電子証明書のCDP（crlDistributionPoint）に記載されているURIを参照してCRLファイルを入手
- 相互にCRLファイルを有効期間中はキャッシュ。

以上

著者：長岡亨+,下條真司+
共著：米村直樹++，斉藤圭吾+++
+ 大阪大学 、++ サン・マイクロシステムズ、+++ 日本ベリサイン