工学院大学
KOGAKUIN UNIVERSITY

Linux Conference 2006

SELinuxを用いたビジネス・プロセスベースの強制アクセス制御による権限管理方法

工学院大学大学院
工学研究科情報学専攻

岡上 智也

発表日　2006/06/01

1. はじめに

- 企業情報システムは、ビジネスの効率化・低コスト化と情報の信頼性・説明責任を果たす必要がある
  - 情報の信頼性と説明責任
    - 今までは紙で情報の信頼性を確保し、電子情報で効率化やコストダウンを実現していた
    - これからは紙が無くなり、電子情報のみで情報の信頼性を確保しなければならない
    - 日本版SOXなどのコンプライアンスのために、情報の信頼性を確保出来ていたことを事後的に第三者に説明できなければならない

企業情報システムの要件と既存技術

- 迅速に柔軟なサービスを開発する
  例： Web Service（WS）
- 利便性とセキュリティを両立する
  例： Single Sign On（SSO）
- 情報の信頼性・説明責任をサポートする
  例： 強制アクセス制御、最小特権
- 効率のよい開発を可能にするサービスプラットフォームを提供する
  例： .NET、 J2EE、 SELinux

モチベーション

- これらの例の技術の単純な組み合わせで目的の達成は可能か？
- そうでないとしたらどんな課題があるのか？
- 要件をすべて満たす方式の基本アーキテクチャとはどんなものか？
- それを実行できるプラットフォームの構成法は？

コミットメント

Ⅰ．目的達成を困難にする課題を明らかにする

Ⅱ．要件を全て満たす方式の基本アーキテクチャのひとつを提案

Ⅲ．SELinuxをベースとしたプラットフォーム

Ⅰ．目的達成を困難にする3つの課題

(1) ビジネスの変化への対応により最小特権が困難

- 権限下方硬直性の問題

(2) ビジネスの変化に伴う更新すべき情報の散らばり

- 記述局所化の問題

(3) ポリシーに基づく宣言的なアクセス制御の記述困難性

- 宣言的アクセス制御の問題

II．要件を全て満たす方式の基本アーキテクチャ

(1) アクセス制御の主体として、ユーザIDに基づく役割に加えて
ビジネス・プロセスの状態に基づく役割を追加

(2) ビジネス・プロセスの実行エンジンにSSOの
Delegation機能を付与

(3) SELinuxの強制アクセス制御とインパーソネーション機能を活用

III．SELinuxをベースとしたプラットフォーム

（1）強制アクセス制御環境において3つの最小特権を実現する機能

サービスアカウントへの権限の制限
- TE

コードアクセスセキュリティ
- ドメイン遷移

インパーソネーション
- setcon/setforkcon

工学院大学
KOGAKUIN UNIVERSITY

Agenda

1. はじめに
2. 関連技術説明
3. 目標達成を困難にする課題
4. 提案方法の基本アーキテクチャ
5. SELinuxベースのプラットフォーム
6. 提案方法の評価
7. まとめ

2. 関連技術説明

2-1. 迅速な柔軟なサービスを開発する技術

2-2. 利便性とセキュリティを両立する技術

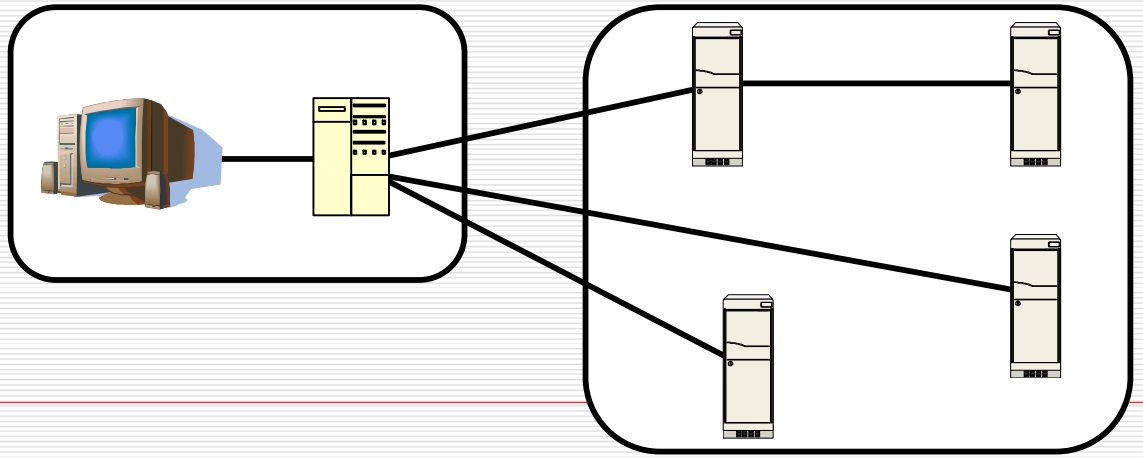
2-3. 情報の信頼性・説明責任をサポートする技術

2-4. 効率のよい開発を可能にするサービス
プラットフォーム

2-1. 迅速に柔軟なサービスを開発する技術

Web Service（WS）

- Web上のアプリケーションを自由に組み合わせ、柔軟にシステムを構築することができる
- システムに必要な機能を一から作る必要がなく、その機能を提供しているアプリケーションを組み入れるだけでよい



2-1. 迅速に柔軟なサービスを開発する技術(つづき)

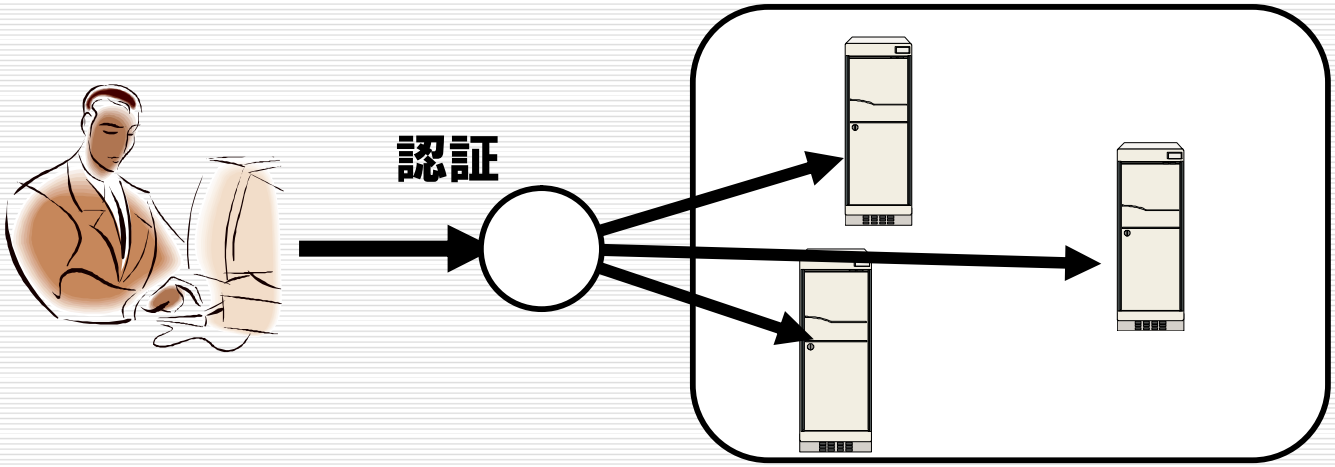
□ ビジネス・プロセス記述(WS-BPEL)

- Web上のアプリケーションとのサービス連携をワークフローとして記述することができる
- 複数のWSの実行を自動化することができる
- 失敗した処理など信頼性に関する記述ができる

2-2. 利便性とセキュリティを両立する技術

Single Sign On（SSO）

- 一回の認証をすることで、その後許可されているアプリケーションなどのサービスを、認証なしで利用することができる
- 他のアプリケーションでは権限情報を使ってセキュリティを確保



認証なしで利用可能

Delegation

- プリンシパルな主体から処理を受けているサービスが他のサービスを使うために、権限の追加や変更を行うことができる機能

2-3. 情報の信頼性・説明責任をサポートする技術

□ ポリシーによる宣言的強制アクセス制御

- セキュリティ管理者が決めたポリシーが強制されており、ユーザはポリシー以外のことができない
- ポリシーの記述により抽象レベルでのアクセス制御記述が行える
- ポリシーで記述されているため、どういうルールの下でシステムが機能していたのかを検証することが容易に行うことができる

2-3. 情報の信頼性・説明責任をサポートする技術（つづき）

□ 最小特権

- サーバアカウントへの権限の制限
  - 全権のアカウント権限からサービスアカウント権限へ制限をし、サービスが必要となる権限だけを与える
- コードアクセスセキュリティ
  - 保護されたデータにアクセスする場合に、信頼されたコードを経由してのみアクセスすることができるようにする
- インパーソネーション
  - サービス側にリクエストが来たときに、サーバ側ではリクエスト元である主体の許されている権限に偽装して処理を行う

工学院大学
KOGAKUIN UNIVERSITY

2-4. 効率のよい開発を可能にする サービスプラットフォーム

- .NET 、 J2EE
  - WSを前提としている分散型サービスのプラットフォームであり、WSで必要となる機能を備える
  - XMLデータフォーマット、HTTP通信など用いることによりOSに依存しないWS環境を開発することができる
  - 柔軟性、拡張性、信頼性を確保するための機能を備えている

2-4. 効率のよい開発を可能にするサービスプラットフォーム(つづき)

SELinux (Security-Enhanced Linux)

- 強制アクセス制御
- TE、RBACのアクセス制御技術をサポートしている
- カーネルレベルでの実装となっているため、様々なログを取得することができる
- 宣言的な強制アクセス制御記述の定義により、第三者への説明責任を果たしやすい

3. 目的達成を困難にする課題

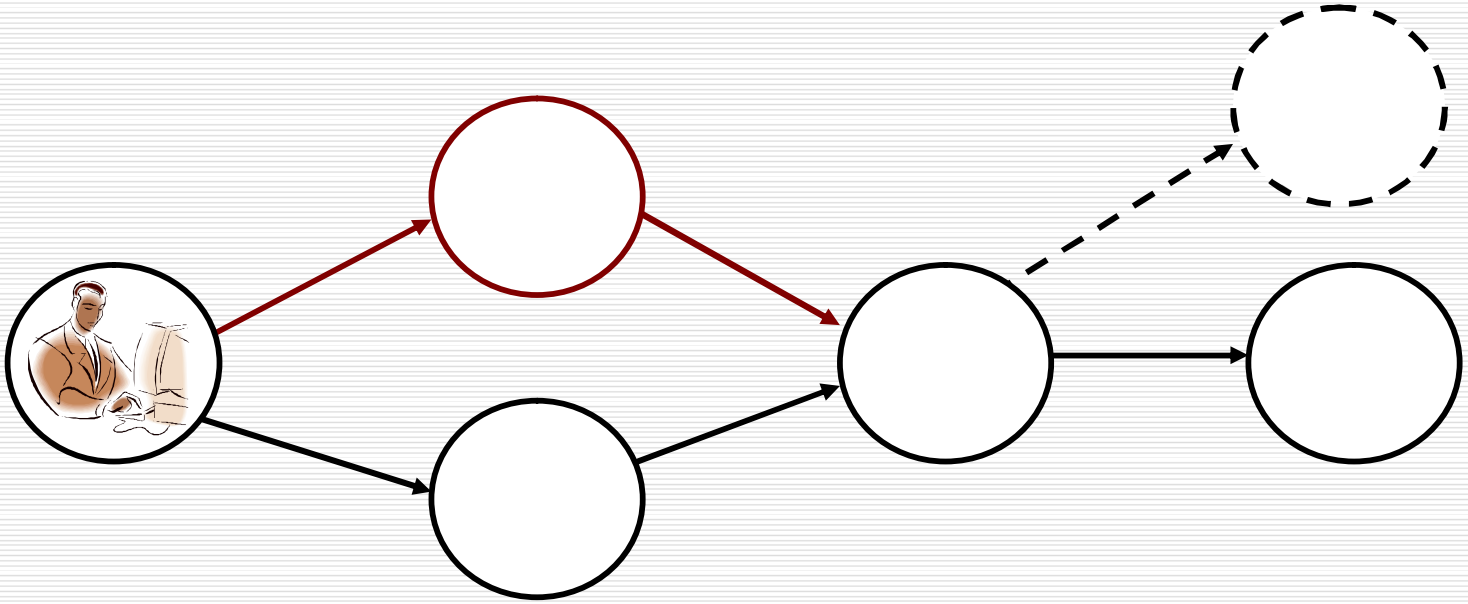
3-1. 権限下方硬直性の問題

3-2. 記述局所性の問題

3-3. 宣言的アクセス制御記述の困難性

3-1. 権限下方硬直性の問題

- ビジネスが変わることによるビジネス・プロセスやプリンシパルな主体に基づくロールの変化



3-1. 権限下方硬直性の問題(つづき)

□ 権限の増加

- 各アプリケーションが関係するACLにおいて権限の増加を行うだけでよい
- システムへの影響は少ない
- 比較的容易

□ 権限の減少

- 何が必要な権限で何が必要でない権限なのかが分かりづらい
- システムへの影響が大きい(支障が発生する危険)
- 困難

3-2. 記述局所化の問題

- ビジネス・プロセスやプリンシパルに基づくロールの変化によるシステムへの影響
  - BPやロールの変更に伴って、様々な場所で変更を行わなければならない
    - ACLやプログラムコード

少ない変更でもその影響が波及していく

3-3. 宣言的強制アクセス制御記述の困難性

- 説明責任のためのポリシーに基づく宣言的強制アクセス制御記述の必要性
  - 記述を行う場所が集中している
  - WSの配置後でもポリシーを追加することができる
  - アプリケーションに踏み入らないポリシー記述
  - 第三者から検証しやすい

3-3. 宣言的アクセス制御記述の困難性（つづき）

- 現状では各アプリケーションにおいて手続き的アクセス制御記述を行っている
  - J2EEではコードの中で権限の増加や減少を行えてしまう（検証外の所でアクセス制御が行われる）
  - 記述の複雑さ
  - 記述を行う場所が分散している
  - 第三者から検証しづらい

4. 提案方式の基本アーキテクチャ

4-1. ビジネス・プロセスに基づく役割

4-2. WSのアーキテクチャとDelegation機能

4-3. SELinuxの強制アクセス制御と
インパーソネーション機能

4-1. ビジネス・プロセスに基づく役割

□ プリンシパルな主体

■ 従来のWSの方式

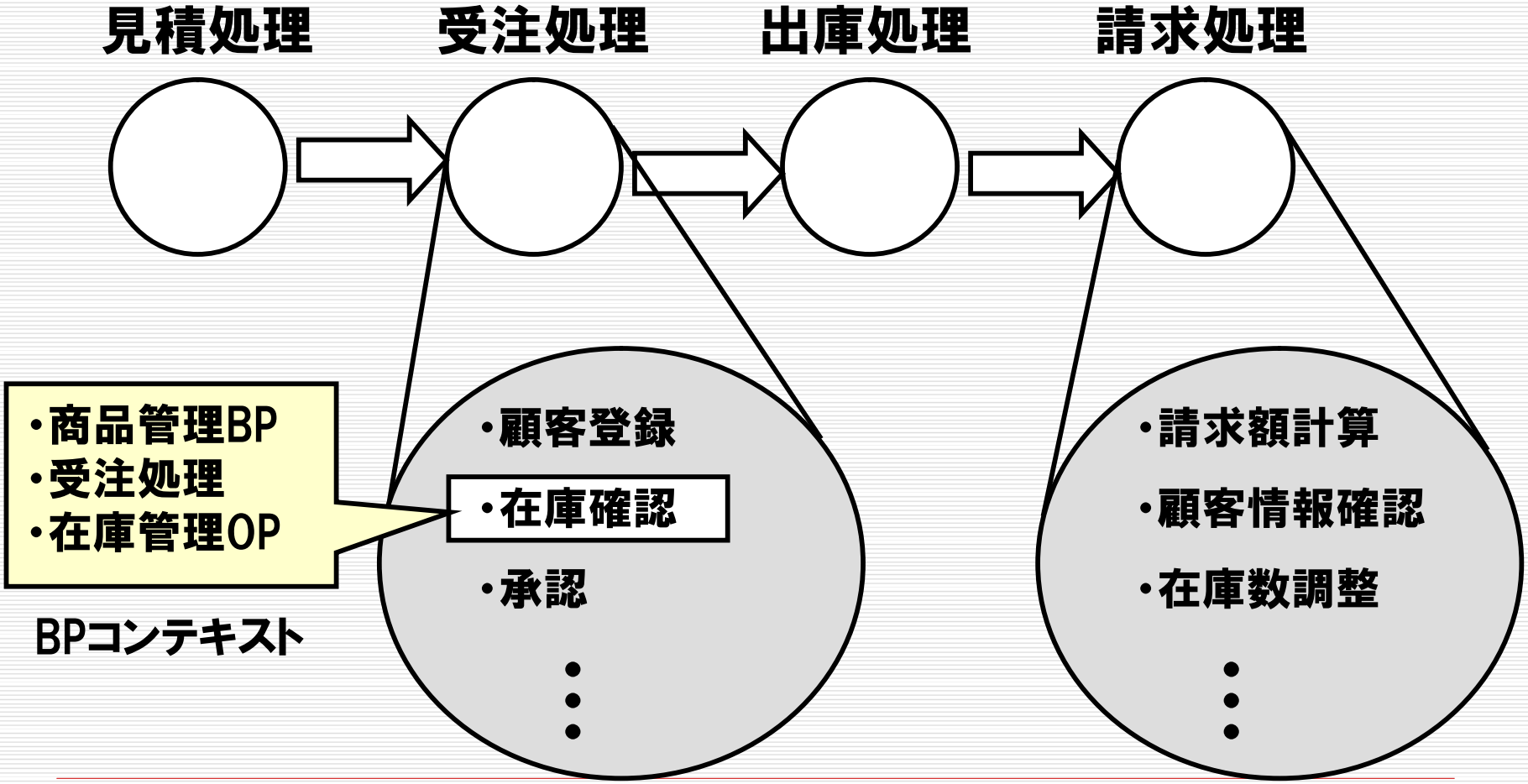
SSOにより付与されるユーザIDやその役割(ロール)に基づく
プリンシパルな主体

■ 提案方式

SSOによるプリンシパルな主体とビジネス・プロセスの位置や
オペレーションを記述したビジネス・プロセスコンテキストを
組み合わせた新しいプリンシパルな主体

BPの位置やオペレーション毎に異なる権限を割り当てることができる

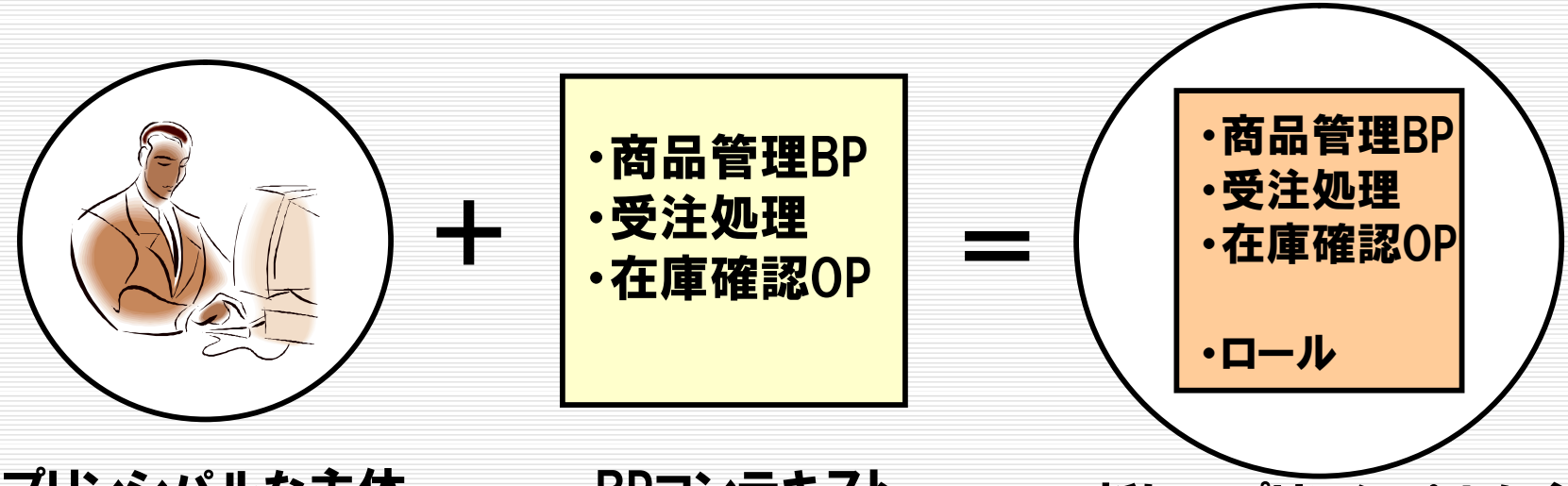
4-1. ビジネス・プロセスに基づく役割（つづき）



商品管理ビジネス・プロセスのコンテキスト

□ ビジネス・プロセスに基づく役割

－ BPセキュリティコンテキストを生成



プリンシパルな主体
（IDとロール）

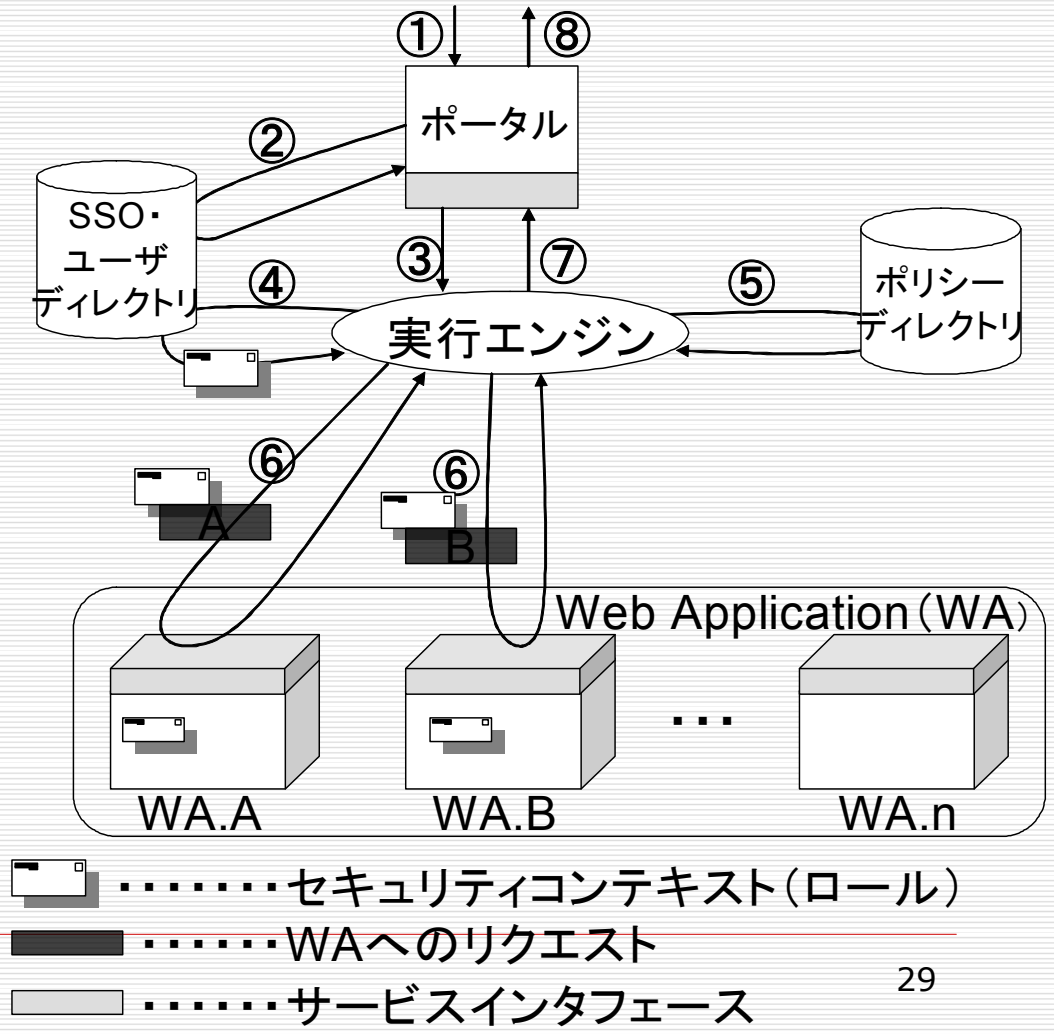
BPコンテキスト

新しいプリンシパルな主体
（BPセキュリティコンテキスト）

章2の図1

4-2. WSの実行エンジンにおけるDelegation機能

- 既存のSSOを行うWSの処理フロー
  - 実行エンジンはセキュリティコンテキストを変更することなくプロキシとして動作
  - セキュリティコンテキストの変更は不可



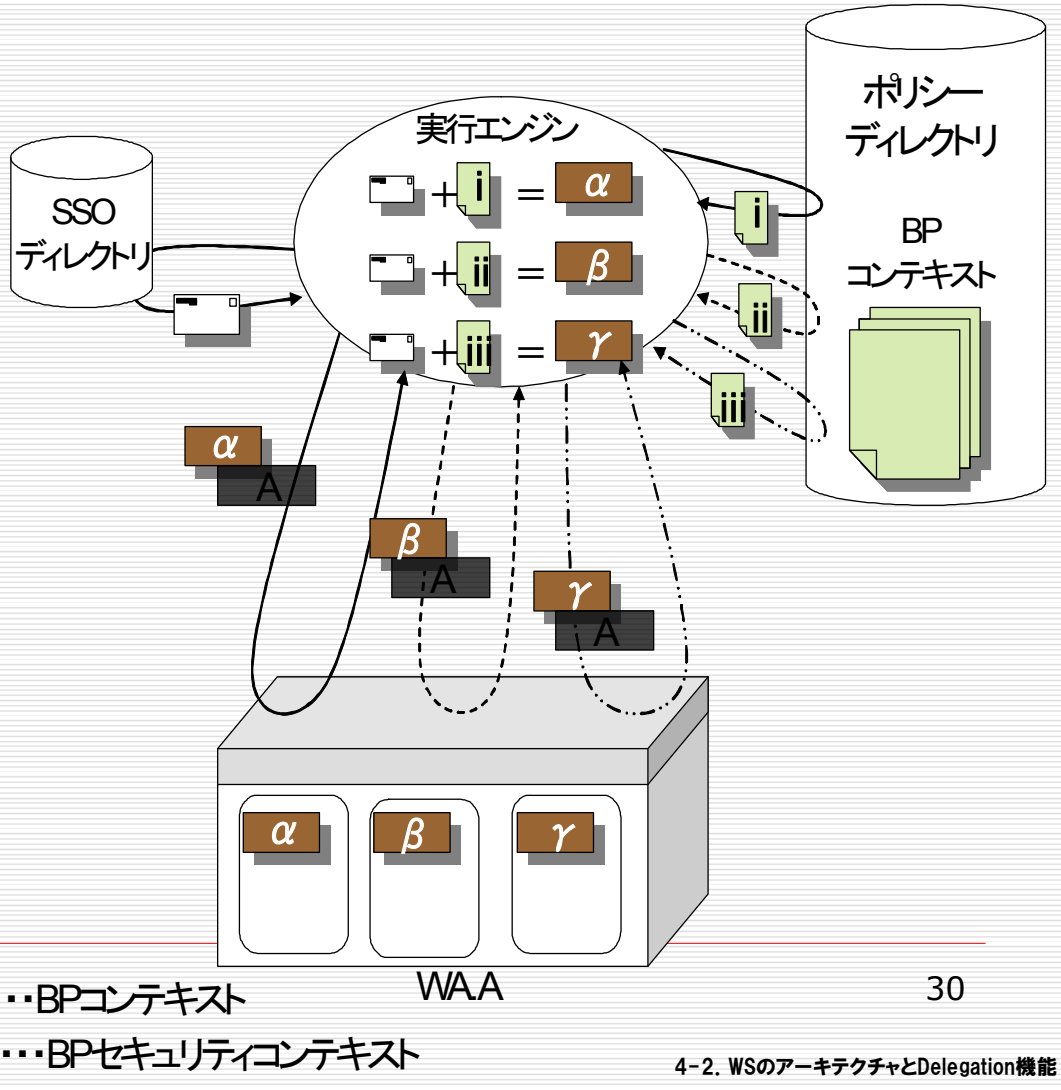
4-2. WSの実行エンジンにおけるDelegation機能(つづき)

章3の図4

Delegation機能の付与

- 実行エンジンはプリンシパルベースのセキュリティコンテキストにBPコンテキストを結び付け、BPに基づくロールを新しく生成するロールを結びつける

  Delegation機能を追加



4-3. SELinuxの強制アクセス制御とインパーソネーション機能

- アプリケーションのプラットフォームとしてSELinuxを用いる
  - ポリシーに基づく宣言的な強制アクセス制御
  - 各アプリケーションでは、リクエスト毎にセキュリティコンテキストでインパーソネーションを行う
    - setconやsetforkconによる強制アクセス制御環境でのインパーソネーション

setforkcon・・・Linux Conference2004においてフェルナンド・バスケス氏によって発表されたSELinuxの拡張機能

節4．3の評価

5．SELinuxベースのプラットフォーム

□ SELinuxにおける3つの最小特権を実現する機能

- サーバアカウントへの権限の制限
  - TE（Type Enforcement）

    TEを使って必要な権限のみを割り当てるようにする
- コードアクセスセキュリティ
  - ドメイン遷移

    ドメイン遷移を使い、信頼コードをエントリ・ポイントとした信頼コード経由の保護データへのアクセスを行う
- インパーソネーション
  - setcon / setforkcon

    setconとコンストレインの緩和によって、プロセスレベルでの偽装を行う

6. 提案方式の評価

□ 定義した4つの要件で評価

- 迅速に柔軟なサービスを開発
- 利便性とセキュリティを両立
- 情報の信頼性・説明責任をサポート
- 効率のよい開発を可能にするサービスプラットフォーム

次の3点において改善があった

□ 権限下方硬直性の緩和

- インパーソネーションを用いることにより、プリンシパルな主体の権限を変えることなく、リクエスト毎の権限の減少を行うことができる(プリンシパルな主体に対するACLはそのまま)

□ BPに基づくロールへの記述局所化

- ビジネス・プロセスの変更が生じた場合、BPセキュリティコンテキストの追加や削除、それに対応するアプリケーションのACLのエントリへの追加や削除だけで済む

□ 宣言的強制アクセス制御記述のサポート

- SELinuxを用いることにより、宣言的なアクセス制御記述を行うことができ、検証しやすく説明責任を果たしやすい

7. まとめ

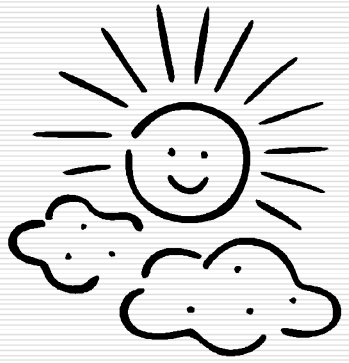
- 企業情報システムの要件を定義し、要件達成における3つの課題を明らかにした
- 本研究では、ビジネス・プロセスに基づく新しい役割を用いた権限管理の方法を提案した
- SELinuxの権限管理機能を用いた、強制アクセス制御環境での最小特権の機能について述べた
- 本方式により3つの課題の緩和を実現することができた

□ 残された課題

- SElinuxのsetconによるインパーソネーションは
  プロセスレベルでしか扱うことができない
  （スレッドレベルでのインパーソネーションが必要）
- .NETやJ2EEのインパーソネーションとSELinux機能の
  シームレスな連携の実現
- 必要なBPELなどへの仕様拡張方法
- 拡張したBPELを扱える実行エンジンの構築

おわり

ご清聴ありがとうございました



発表　2006/06/01