

自動車サービス連携の セキュリティアーキテクチャの提案

南山大学

数理情報学部情報通信学科

2008MI011 朝倉知也

2008MI079 岩井 大

指導教員:青山 幹雄

シナリオ

1. 研究背景と提案
2. HTTPS(SSL)通信の実装
3. 車載サービスブローカのセキュリティ
4. 目次案予定
5. 今後の課題とスケジュール

1.研究背景と提案

背景

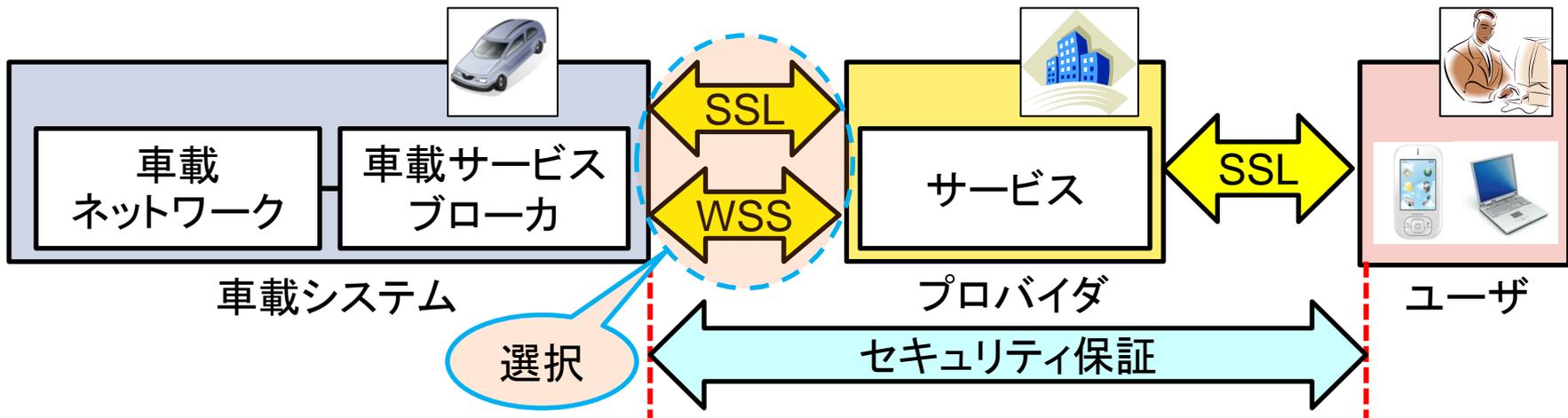
自動車ネットワークサービスの多様化
⇒ SOAに基づくアーキテクチャが提案

問題点

- ✓ 外部システムとユーザ間のプロトコル/インタフェースの定義が必要
- ✓ 通信セキュリティの保証が必要

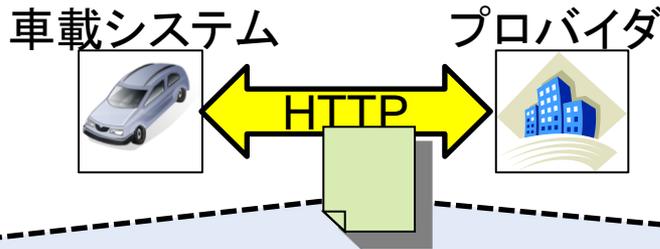
提案

- ✓ SOAに基づくアーキテクチャを拡張, End-to-Endでセキュリティを保証
- ✓ サービスの要求するサービスレベルに対し適切なセキュリティを選択
⇒ SSL/WS-Securityを用いて実現



2.HTTPS(SSL)通信の実装

HTTP通信



レスポンスのキャプチャ

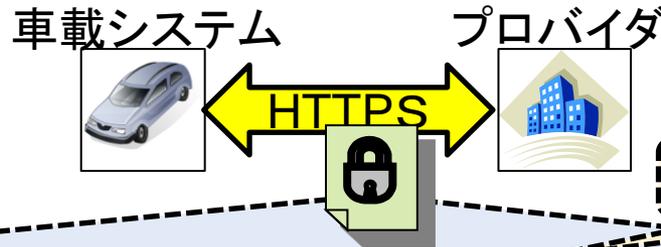
```

HTTP/1.1 200 OK
Date: Sat, 19 Nov 2011 03:25:55 GMT
MIME-Version: 1.0
Server: The Knopflerfish HTTP Server
Connection: Close
Content-Type: application/xml;charset=UTF-8
<ns:getStateResponse xmlns:ns="getStateService.OSGi_01_bundle/ResTEST"><return>str01</return></ns:getStateResponse>
  
```

ヘッダ

ボディ

HTTPS(SSL)通信

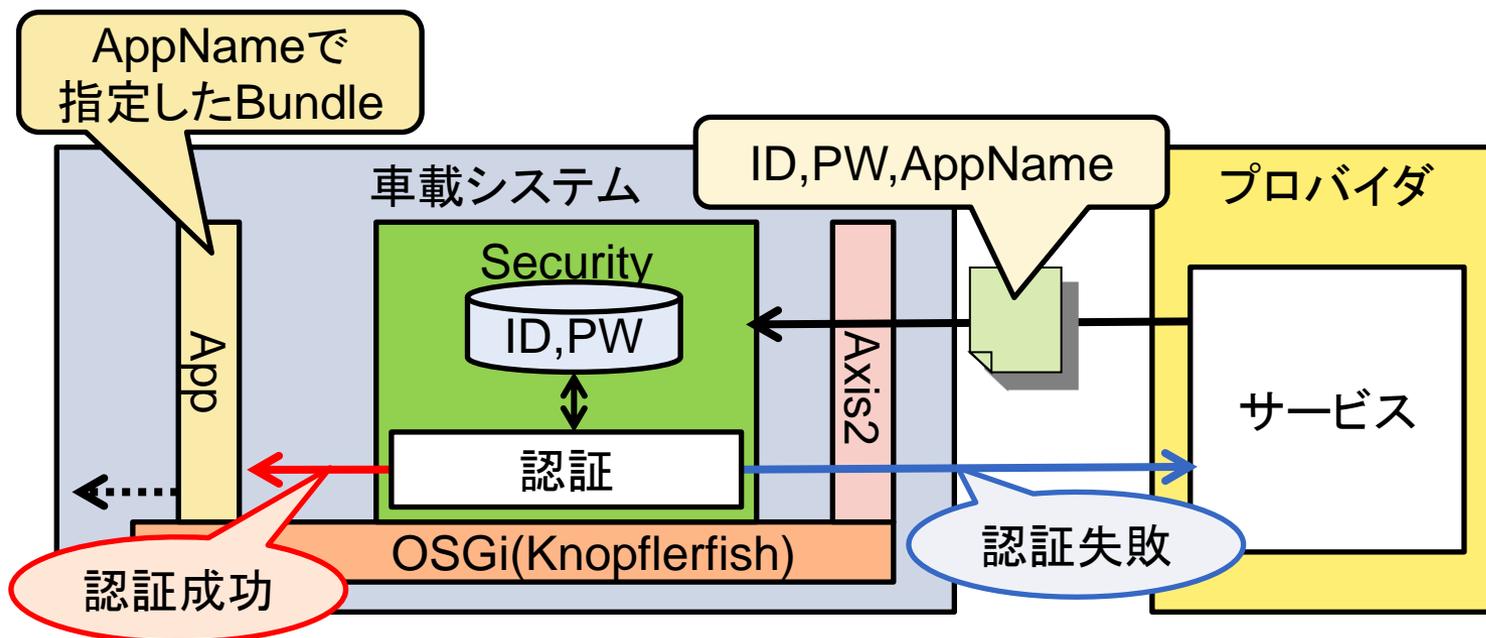


レスポンスのキャプチャ

```

T...ラM... NX%鯉燻鮑↓尊□ヒヒ□Pイキ観角↑5 NX%ソモ 璿ルオ妹 オ3n*フ豫爰 兎8□ | □ ヲ〜 {1 x0□t0□n1J A↑ンセ0 - *□□
  | 0÷10 - L U - !! 1 US10 - L U □ !! 1 CA140* - L U □ . !! □ San Jose1 0!! - L U □ !! Knopflerfish1#0! - L U □ !! → Certificate
Administration1 0!! - L U □ !! KF Developer0 1 040811085006Z 480122132518Z0+10 - L U □ - !! 1 US10
- L U □ !! 1 CA140* - L U □ . !! □ San Jose1 0!! - L U □ !! Knopflerfish1#0! - L U □ !! → Certificate Administration1 0!! - L U □ !! KF
Developer0 ◆0 - *□□ | L "0♂1 =カS+ J- 宋睭0□オJ、 | aフ*#ヶケヨソ議砭。Nムラレ→□o□。ケh#!! - hrヨ膠コシv→ - カモb# %N;{WG"ミへ□廖ヒ
E□「ヨ・Ty□+ 騎ウ攜a@ D餒□煮kマ□□(□笑dノメ□セ「ヤ」@C1 L 0 - *□□ | L =ウb^ヌIq7F| 饅ド'S□ナJ暁9M□ iソク エ「カ;# L → 6-ハ
鑰r登 鷲9|3□t 「溢v; ;T - 7! %*h□原(□E□) - 所L□ " (敘(9 給マ□Q'萄'体bU+ Y□□モ□レ[.a□Eレ"n□ | L ヲ L mアエリ喚 X覽ヤ□□ニ
□レ↑□%弱」r□ L 子!!儂jw'ホ*hd <□□□レ7□一1sP □Xスギイ「7在キセ・実6 □□ろ訣1%轟蝨嗜穩 □□ワホ決鋤h}k%U□^mPム□□ル94□HnX↑
ハレMムカ#A#俾□□|= (L - ヲウ - リシ□2イ*4J□Zwauルム瘡^◀ p冀S□□□X□&cm| gキ枹マチ5冽°i鞞'ヤ、□1SB鞞J9- 赴ッhu□ L □Jwiiiン謐 t宰ホ血ハ
<□オING 柰DaiMn'>cA↑ P+ □ネ9□ □アJ□ワ□Mア(y2□□□ - =4外□チ^5B剪?柄ア嬾驕8PッホS0]s腔Q Qサウ9サメy| = 証□鞞登部kYd|ウハDッd9ア
_ L L ↑ 4梓:□□カ□jgix S□
  
```

3.車載サービスブローカのセキュリティ(1/2)



Security Bundle(SB)

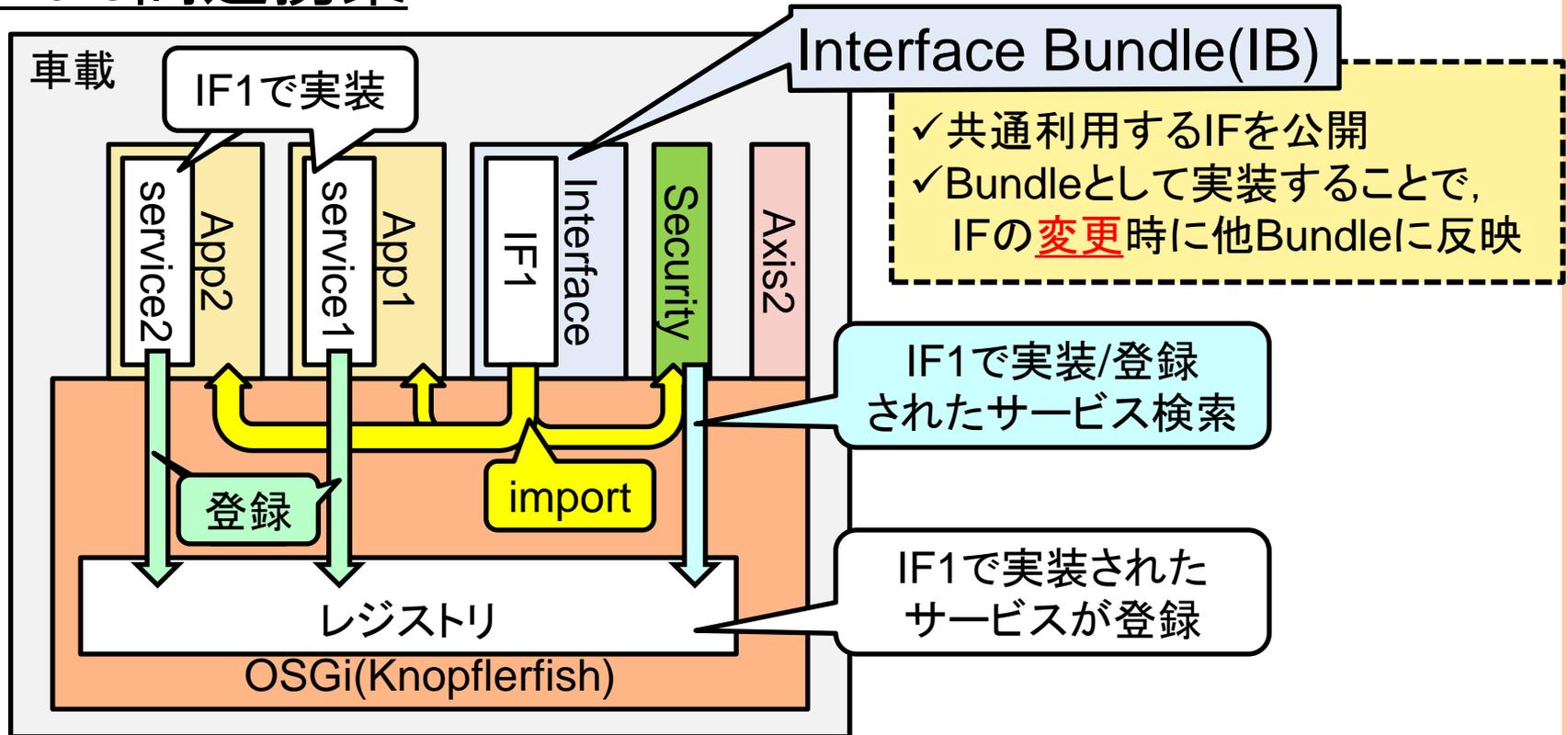
1. プロバイダは(ID,PW,AppName)を送信
2. 保持しているID,PWと比較, 認証
3. 認証成功の場合: AppNameで指定したBundleと連携
認証失敗の場合: プロバイダに認証失敗を通知

実装課題

SBとApp Bundle(AB)は 1:n となる

- ⇒ Bundle間連携では呼び出すBundleのインタフェースをインポートする
- ⇒ AB追加の度, SBのManifestを書き換える必要がある

Bundle間連携案



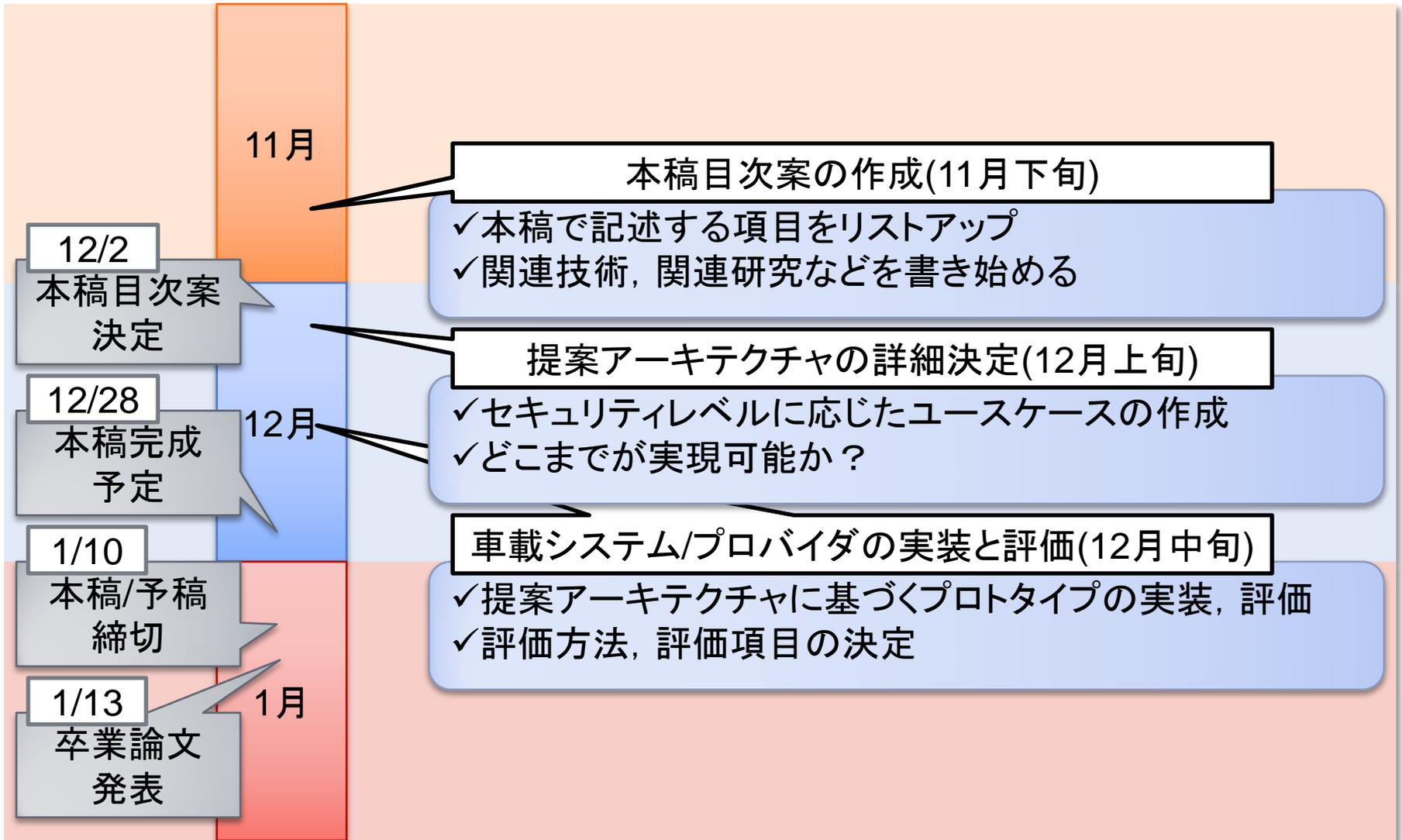
連携案の課題と解決法

- ✓ SBはStart時に検索を行う為, AB追加後に更新が必要
⇒ SBがAB追加を認識し更新する, 又はABのStartでSBを更新する機能を実装
- ✓ インタフェースの追加時にSBの変更が必要
⇒ 数種類のインタフェースをIBで作成, 公開

4.本稿目次案予定

- 1 はじめに
 - 1.1 研究の背景
 - 1.2 研究の目的
 - 1.3 本稿の構成
- 2 自動車ネットワークサービスの現状と課題
 - 2.1 自動車ネットワークサービスとは
 - 2.2 自動車ネットワークサービスの現状
 - 2.3 研究課題
- 3 利用技術
 - 3.1 SOA技術(WSDL,UDDI,SOAP,REST)
 - 3.2 セキュリティ(SSL,WS-Security)
- 4 車載ネットワークについて
 - 4.1 車載ネットワーク
 - 4.2 テレマティクスサービス
- 5 関連研究
 - 5.1 OSGi(概要,ライフサイクル,Bundle間連携)
 - 5.2 SOA適用アーキテクチャ
 - 5.3 自動車サービスのセキュリティ
- 6 アプローチ
- 7 アーキテクチャの提案
 - 7.1 車載サービスブローカーアーキテクチャ
 - 7.2 外部システムとの連携
 - 7.3 実装するセキュリティ機能
- 8 プロトタイプの実装
- 9 プロトタイプに基づく評価
- 10 考察
- 11 今後の課題
- 12 まとめ
- 13 参考文献
- 付録 ソースコード

5. 今後の課題とスケジュール





自動車サービス連携の セキュリティアーキテクチャの提案 END

南山大学

数理情報学部情報通信学科

2008MI011 朝倉知也

2008MI079 岩井 大

指導教員:青山 幹雄