



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

- 研究の背景と課題
- 提案アーキテクチャと今後の方針
- テレマティクスプラットフォームにおけるセキュリティ提供
- プロトタイプモデル
- プロバイダの実装
- 参考文献

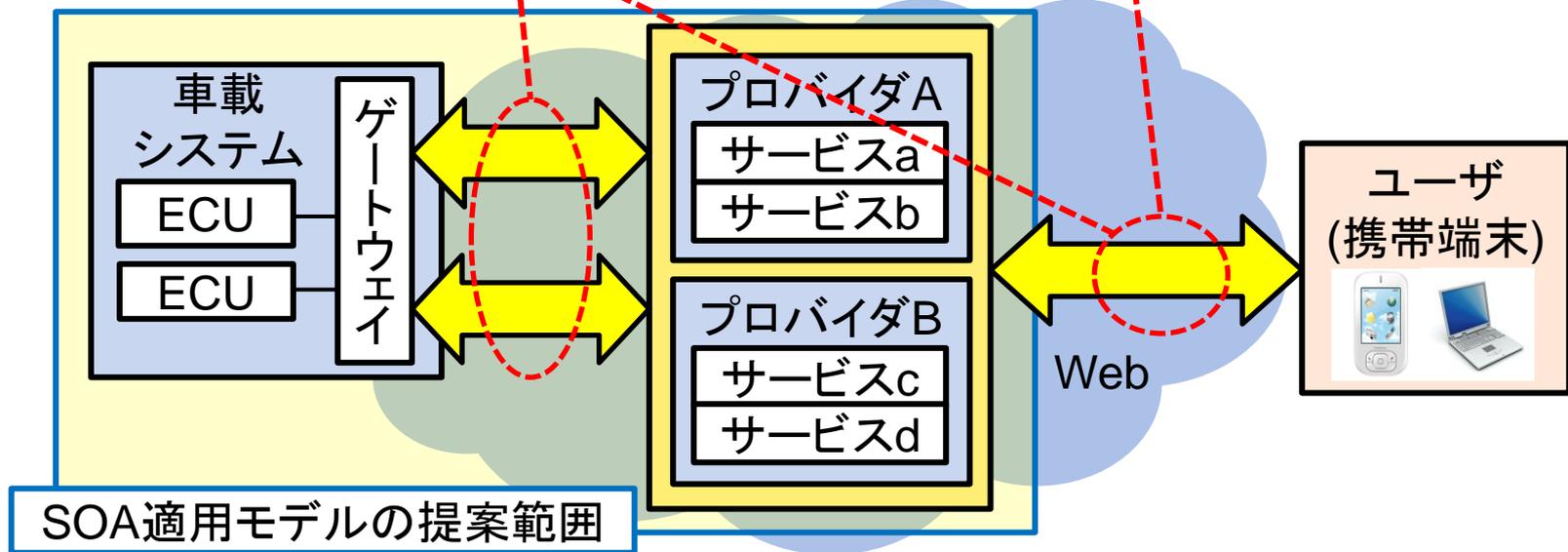
研究の背景と課題

背景

車載システムと通信技術の発達により、車外サービスが発展、多様化
 ⇒メーカーごとにプロトコル/インタフェースが固有で、他メーカーと連携が困難
 ✓ SOAを適用した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



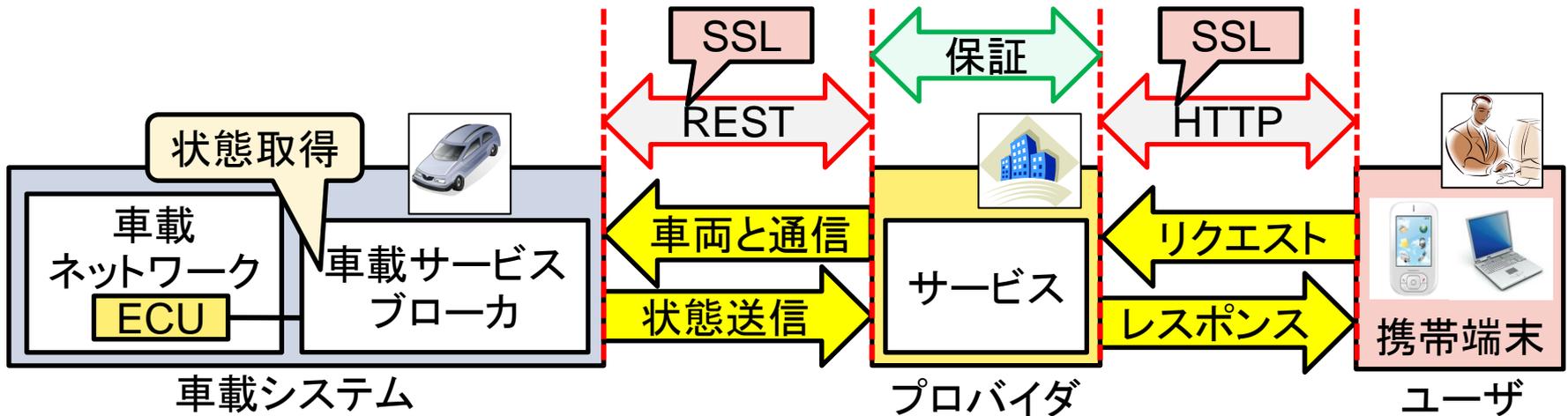
研究課題

✓ SOA適用アーキテクチャの拡張
 ✓ システム全体を一貫したセキュリティで保証

提案アーキテクチャと今後の方針

➤ SOA適用アーキテクチャを拡張

- ✓ 前提: プロバイダ自体のセキュリティは保証
- ✓ ユーザ/プロバイダ間の通信: **REST(SSL)**
- ✓ プロバイダ/車載システム間の通信: **HTTP(SSL)**

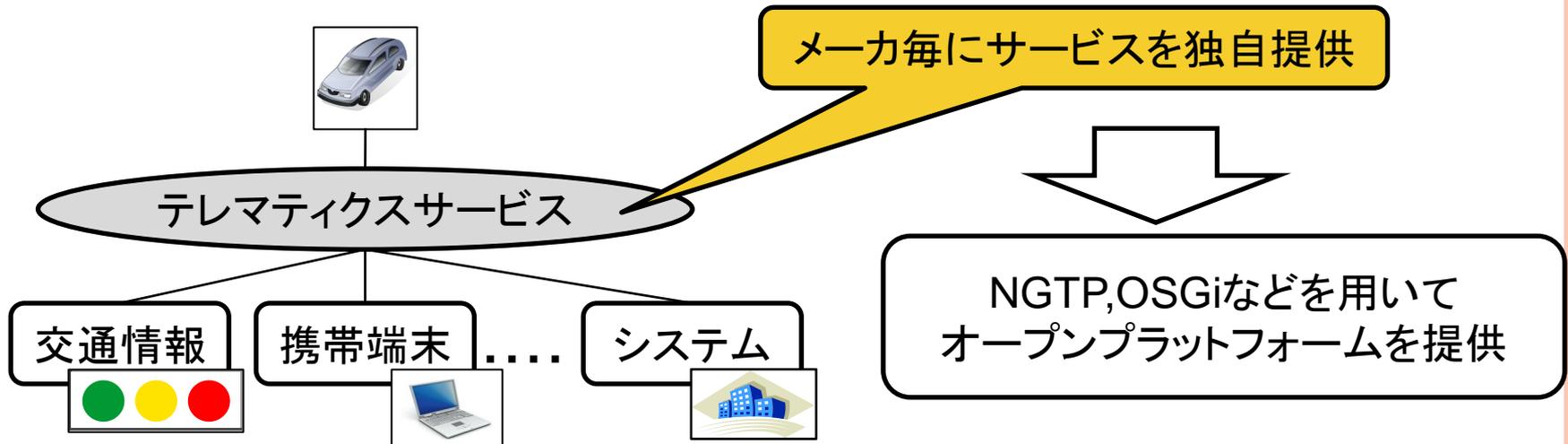


今後の方針

- ✓ 必要なセキュリティの考慮
- ✓ プロトタイプの様相明確化, 実装, 検証

テレマティクスプラットフォームにおけるセキュリティ提供

▶ テレマティクスサービス



▶ テレマティクスサービスにセキュリティを提供する際

- ✓ ネットワークを介して交換するデータの保護⇒**機密性**
 - ✓ ユーザ, サービス, システムの認証⇒**完全性**
- サービスの認証については、証明書を用いて実現できる

本研究で保証するセキュリティ機能

機密性



完全性

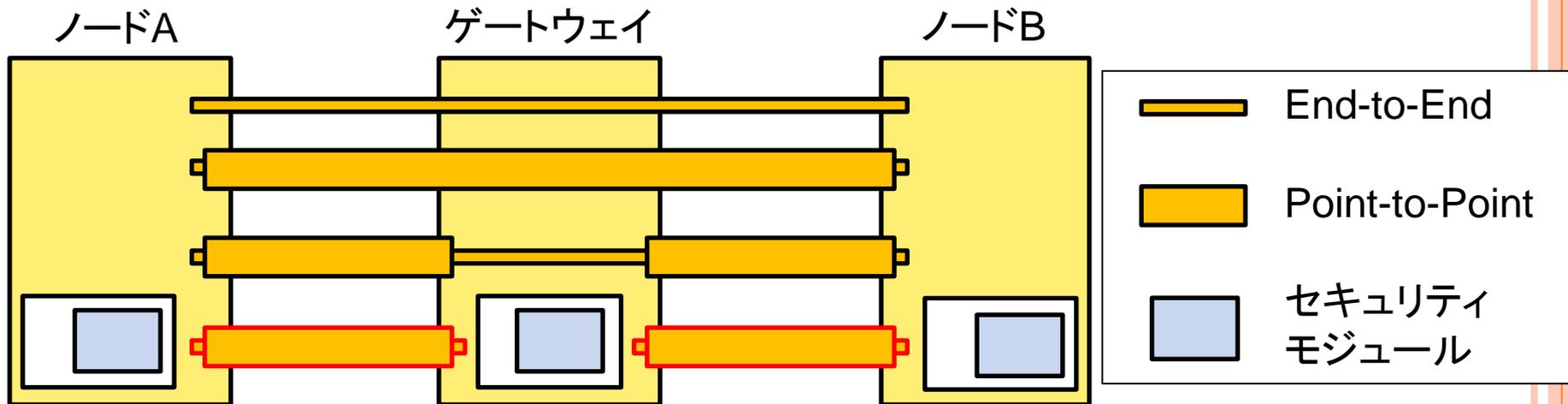
テレマティクスプラットフォームにおけるセキュリティ提供

- ▶ テレマティクスサービスではエンティティ毎にシステムの構造が異なるため、エンティティ間のセキュリティも保証する必要がある



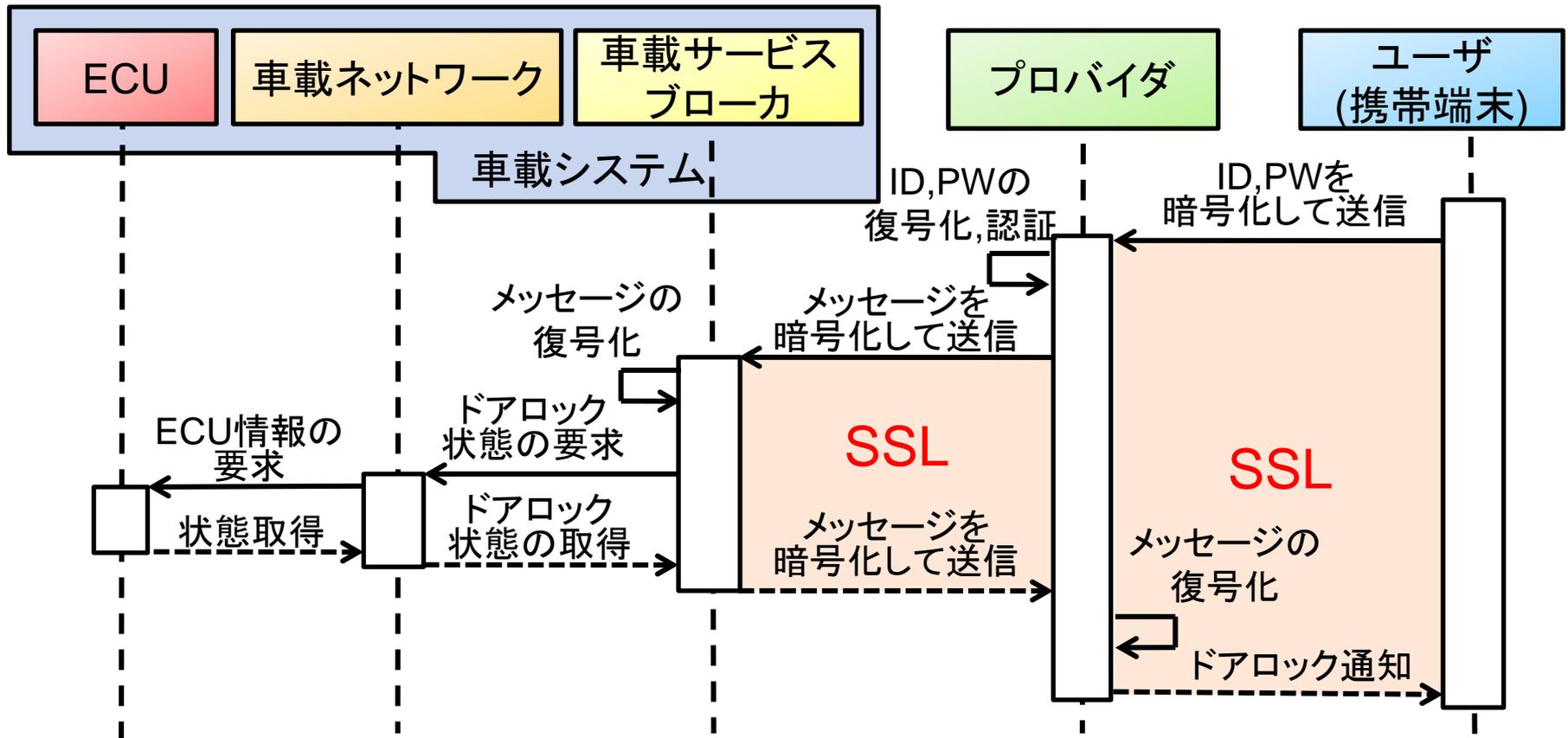
異なるエンティティ間の通信におけるセキュリティ構成

- ✓ 単純なEnd-to-End通信
- ✓ Point-to-Point通信
- ✓ 異なるPoint-to-Point通信を用いたEnd-to-End通信
- ✓ 各エンティティ間にPoint-to-Point通信



➤プロトタイプ:ドアロック確認サービス

- ✓ 現在のドアロック状況を遠隔から確認
- ✓ ユーザ~車載システムまでの通信にはSSLを用い、メッセージを暗号化
- ✓ ユーザが送信したID,PWを利用し、プロバイダはユーザ認証を実行



➤ 概要

✓ 必要機能

- Webアプリケーションとしてブラウザから実行可能
- IDとPWを用いた認証
- ユーザ, 車載システムとSSL(暗号化)通信

✓ 実装言語

- Axis2とのSSL通信は, JavaのHttpsURLConnectionクラスを用いて通信可能
⇒ Java(JSP/Servlet)で実装

✓ 実装環境

- Java(JSP/Servlet)で実装を行うWebアプリケーション
⇒ Tomcatを用い, サーバ上で動作

➤ 認証機能

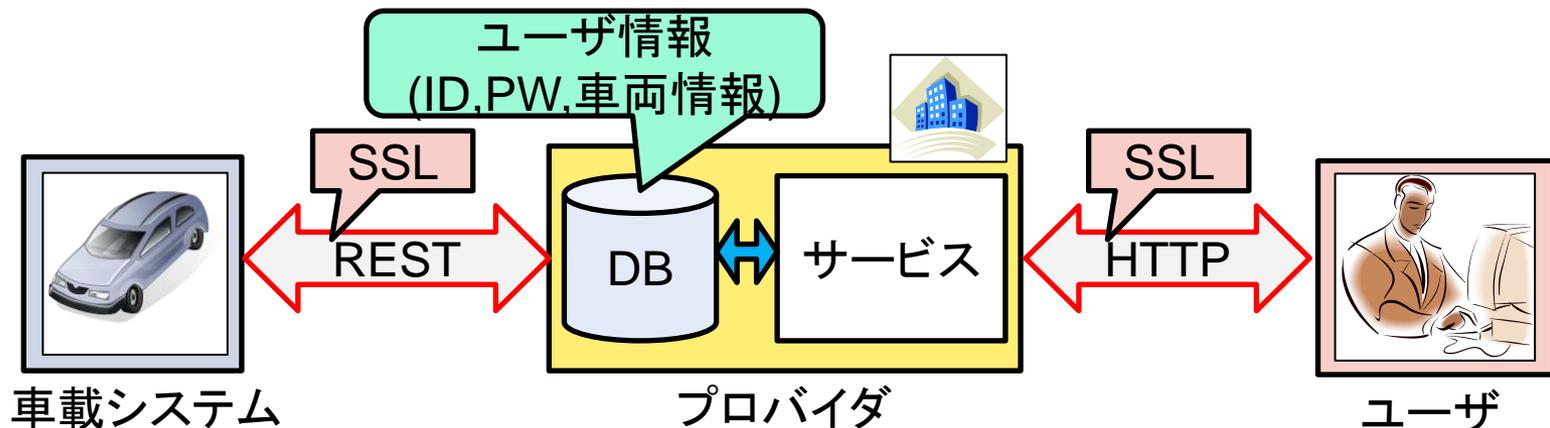
- ✓ Tomcatの認証機能では、以下のユーザ管理方法(レルム)を選択可能

方式	ユーザデータ格納場所	対象開発規模
UserDatabaseレルム	設定ファイル(tomcat-users.xml)	小規模
JDBCレルム	データベース(MySQL等)	中～大規模
JNDIレルム	ディレクトリサービス(NIS等)	中～大規模

NIS(Network Information Service): ネットワーク上にある複数台のPCでデータを共有するシステム



提案モデルでは、複数ユーザのデータ管理を行う必要がある
⇒ 管理を行いやすい**JDBCレルム**での実装を考慮



- S. Eichler 他, On Providing Security for an Open Telematics Platform.
- IT用語辞典 e-Words(<http://e-words.jp/>)
- Javaの道(<http://www.javaroad.jp/index.htm>)



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