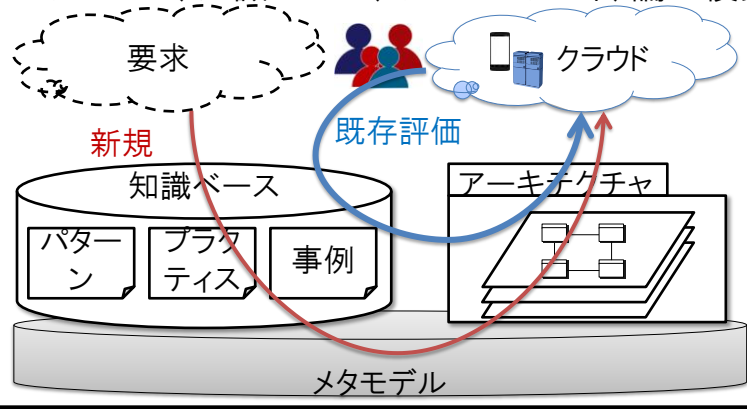
SSR平成27年度成果報告会@NII、2016年6月1日

# クラウドサービスの開発運用においてセキュリティとプライバシ を扱うためのメタモデルと応用

早稲田大学グローバルソフトウェアエンジニアリング研究所
鷲崎 弘宜
http://www.washi.cs.waseda.ac.jp/
washizaki@waseda.jp @Hiro_Washi

## 要約: クラウドサービスのためのセキュリティ＆プライバシメタモデルと応用

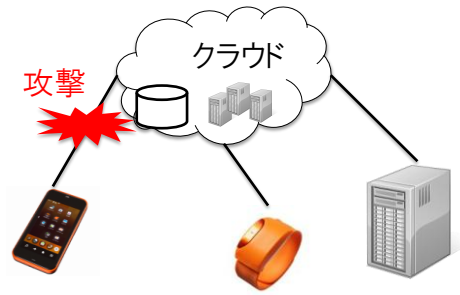
- 産学＋国際連携
  - 鷲崎(早大)、大久保(情セ大)、小形(信大)、海谷(神大)、櫨山(学芸大)、吉岡(NII)、鹿糠・近藤(日立製作所)、加藤(東芝)、鎌倉(とめ研究所)、Fernandez(FAU)、Guéhéneuc・Khomh(Poly Montreal)
- 成果: メタモデル、知識ベース、ケーススタディ、論文複数



# 背景: クラウドサービスとS&P

- 集中管理、外的要因の変化や増大、多様な接続・環境
  - 攻撃やデータ漏洩等のセキュリティ(S)＆プライバシ(P)リスクの増大

⇒ 例や知見の活用によるS&Pの効率的・効果的組み入れ
  - 課題1: 多様な知識の一貫した扱い
  - 課題2: クラウドレイヤの扱い

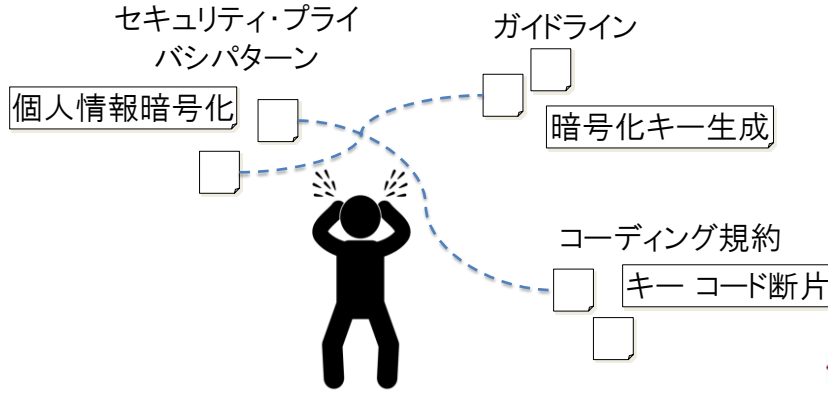



3

# 課題1: 多様な知識の一貫した扱い

- 成功例やS&P専門家の知見記述あり: パターン、ガイドライン、プラクティス、規約など
- 独立定義、比較検討や一貫した適用・組み合わせ困難

⇒ 例や知識群を一貫して扱う基盤の必要性

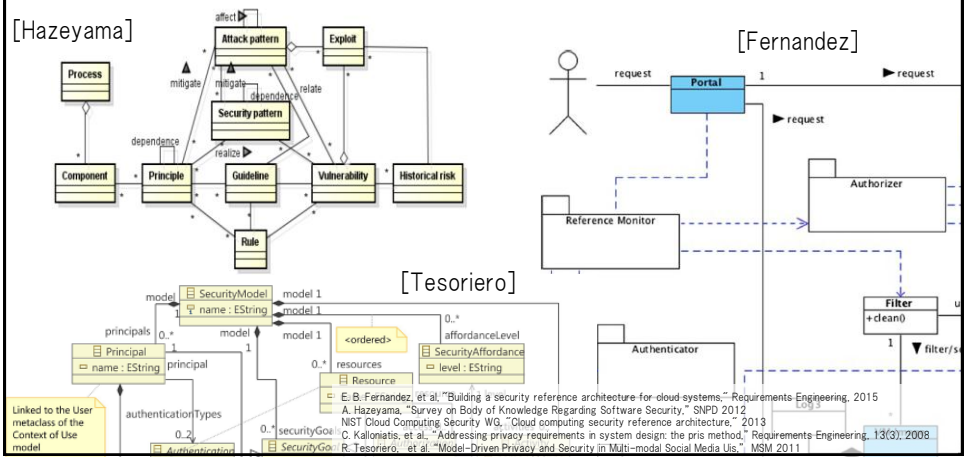



4

# 「基盤」候補

- 汎用のセキュリティ&プライバシメタモデル [Kalloniatis, REJ'08][Tesoriero, MSM'11][Hazeyama, SNPD'12][吉岡, SES'14]
- クラウド セキュリティメタモデル [NIST, 13][Fernandez, REJ'15]

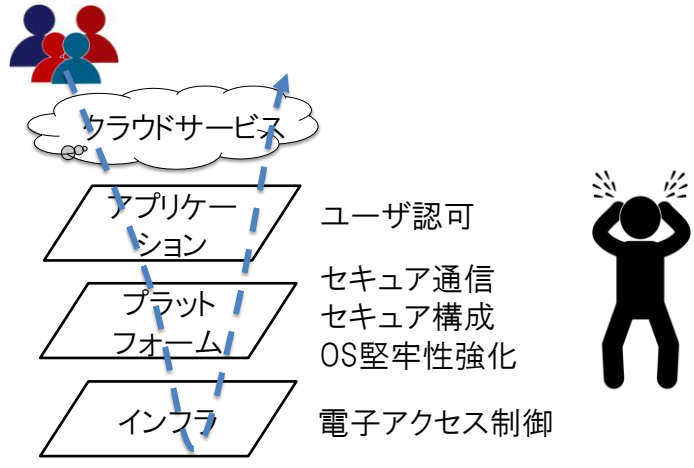
⇒ 非統一、クラウドレイヤや独立・依存部分 不明瞭




# 課題2: クラウドレイヤの扱い

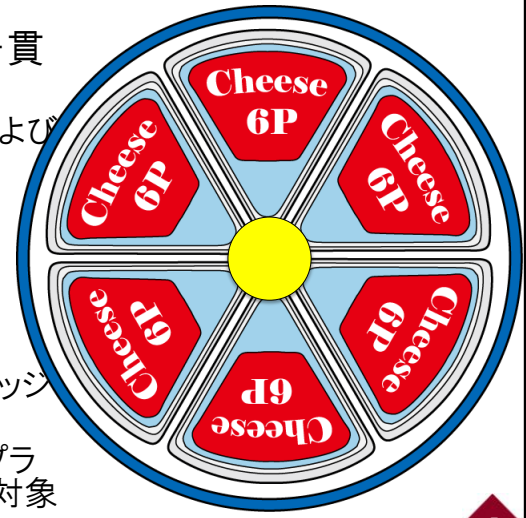
- レイヤを超えたデータとサービスの処理に伴うセキュリティ＆プライバシの扱い

⇒ レイヤを扱えるメタモデルの必要性



# 成果: 階層化クラウドS&Pメタモデル「6+1 Pieces」

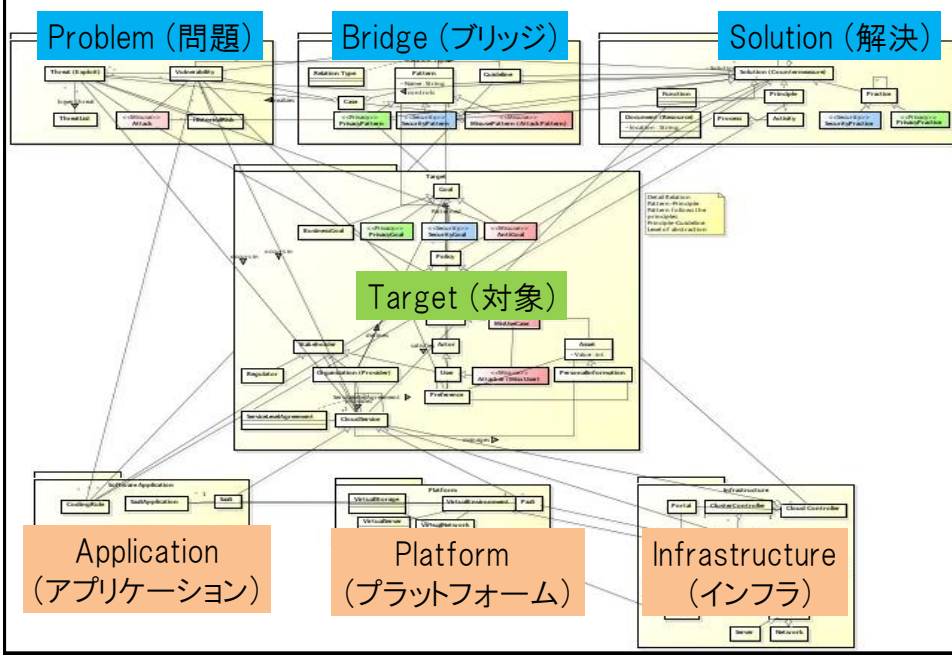
- 課題1: 多様な知識の一貫した扱い
  - 既存メタモデルの統合および拡張
- 課題2: クラウドレイヤ
  - 依存部と独立部分離
  - レイヤの明確な扱い
- 想定プロセス
  - 検討: 対象→問題→ブリッジ→解決
  - 実現: アプリケーション/プラットフォーム/インフラ →対象



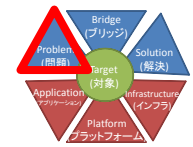

画像 http://illpop.com/png_foodhtm/cheese_a29.htm

7

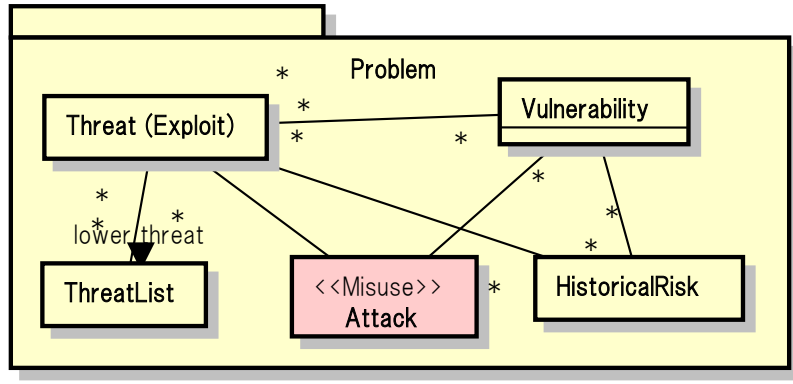
# 「6+1 Pieces」全体像



# Problem 問題

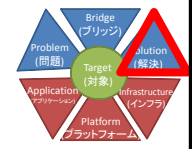



- セキュリティ＆プライバシ上の問題の共通概念
- クラウド独立

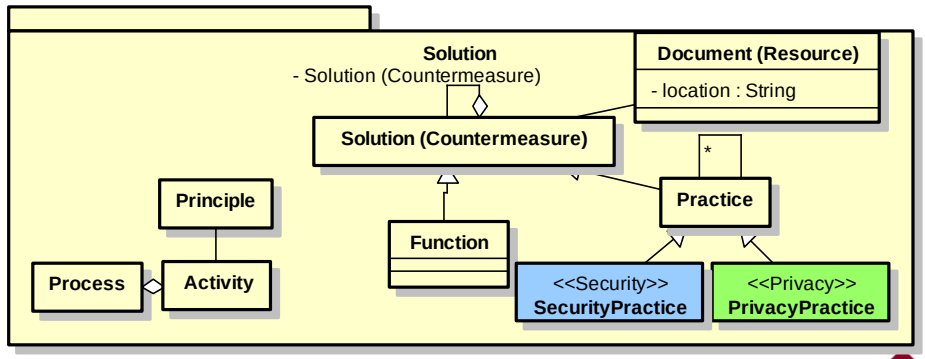



9

# Solution 解決

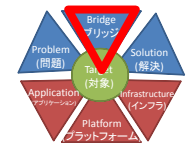



- セキュリティ＆プライバシ上の解決の共通概念
- クラウド独立

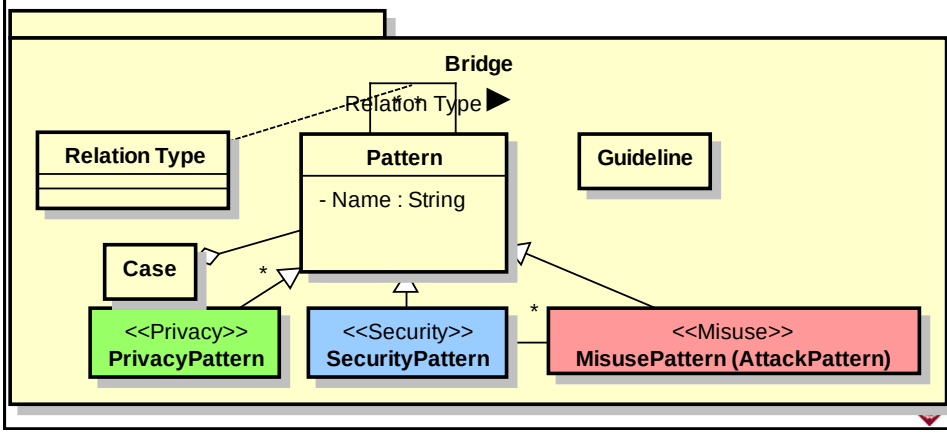



10

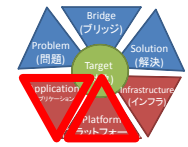
# Bridge ブリッジ



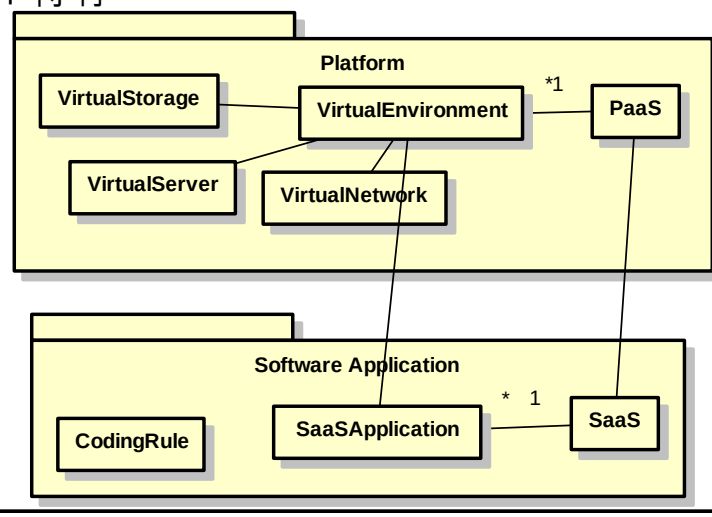

- 問題 - 解決の関係上の概念
- クラウド独立



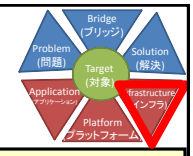

# プラットフォーム、アプリケーション



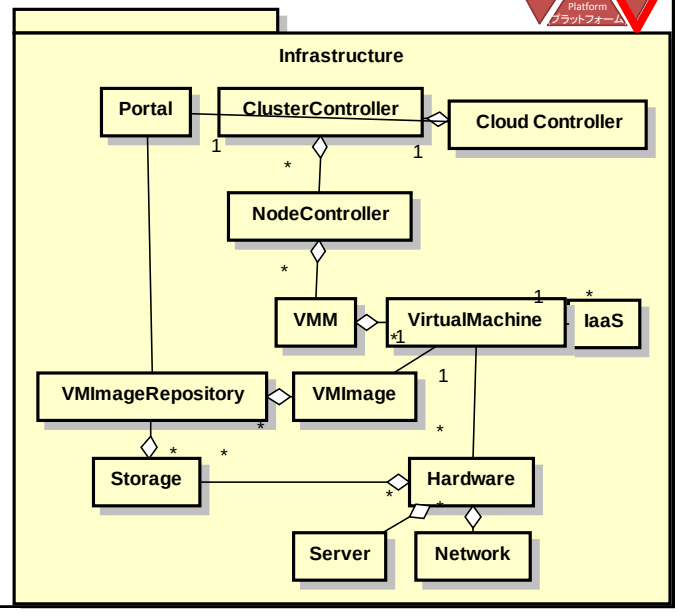

- プラットフォーム、アプリケーションレイヤの共通概念
- クラウド特有

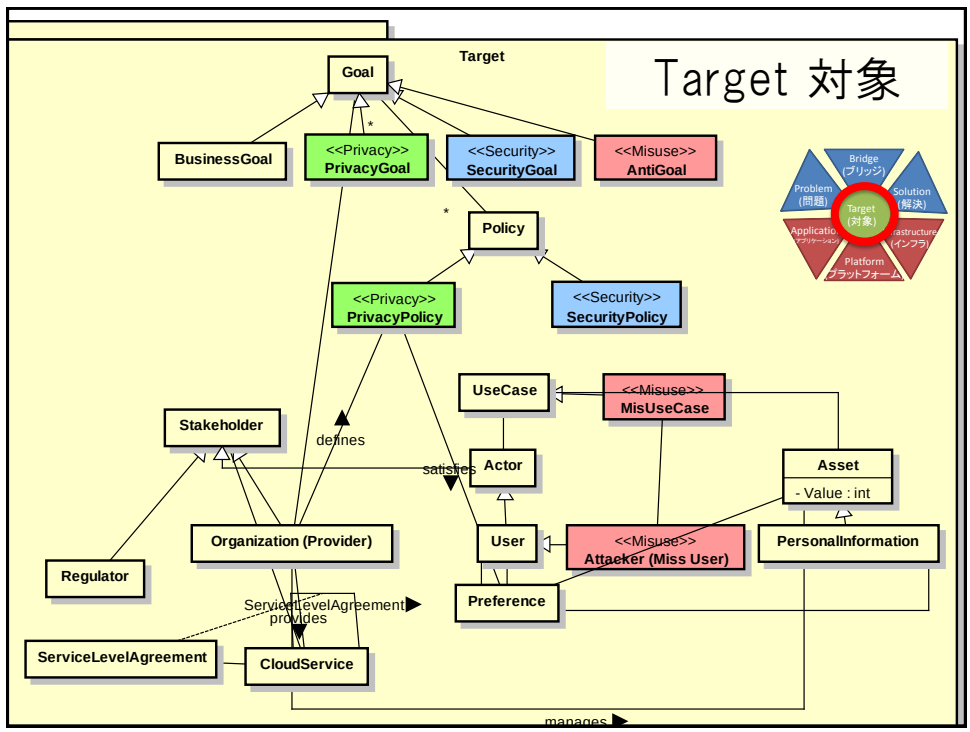


# Infrastructure インフラ




- インフラレイヤの共通概念
- クラウド特有



# メタモデルの応用と実証実験

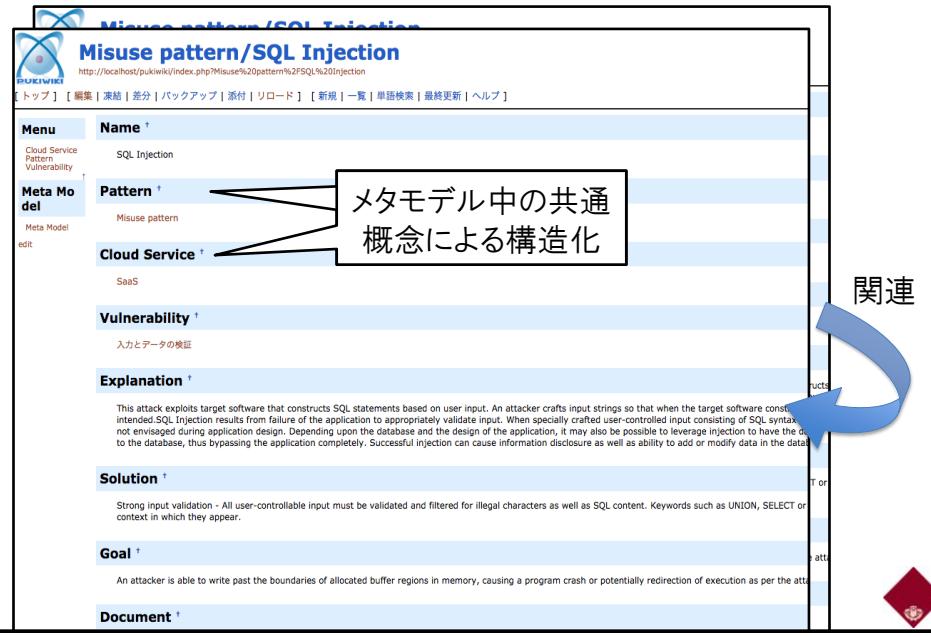
a. 知識の整理とベース構築（課題1）
- Wikiベース 知識ベース･初期案
- プライバシ技術研究サーベイ

b. 知識の一貫した表現･組み合わせ（課題1）
- 各種パターン、知識の表現･組み合わせ
- 起こりうる攻撃や脅威、それへの対策

c. クラウドサービス設計への知識適用（課題2）
- 保険クラウドサービスのアーキテクチャモデリング
- アシュアランスケースによる記述の試行

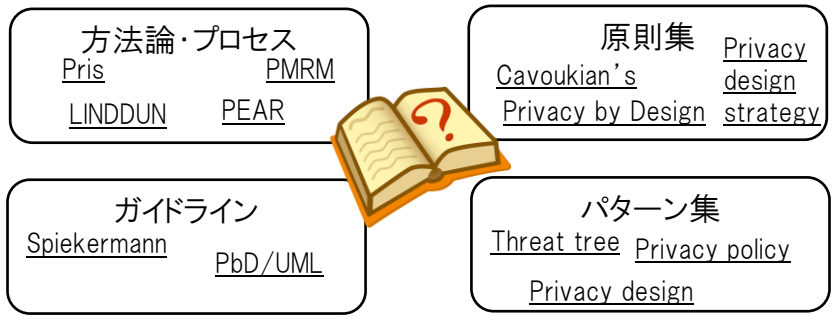


# a. Wikiベース 知識ベース･初期案



# a. プライバシ技術研究サーベイ

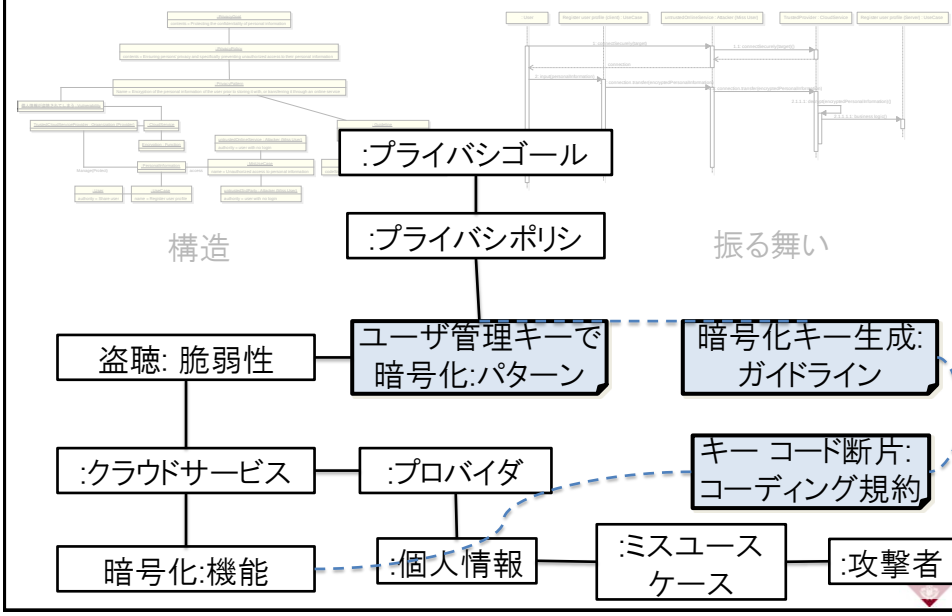
- 整理の大枠決定への活用
  - 4方法論・プロセス、3原則集、2ガイドライン、10パターン集
- 個々の知識整理への活用



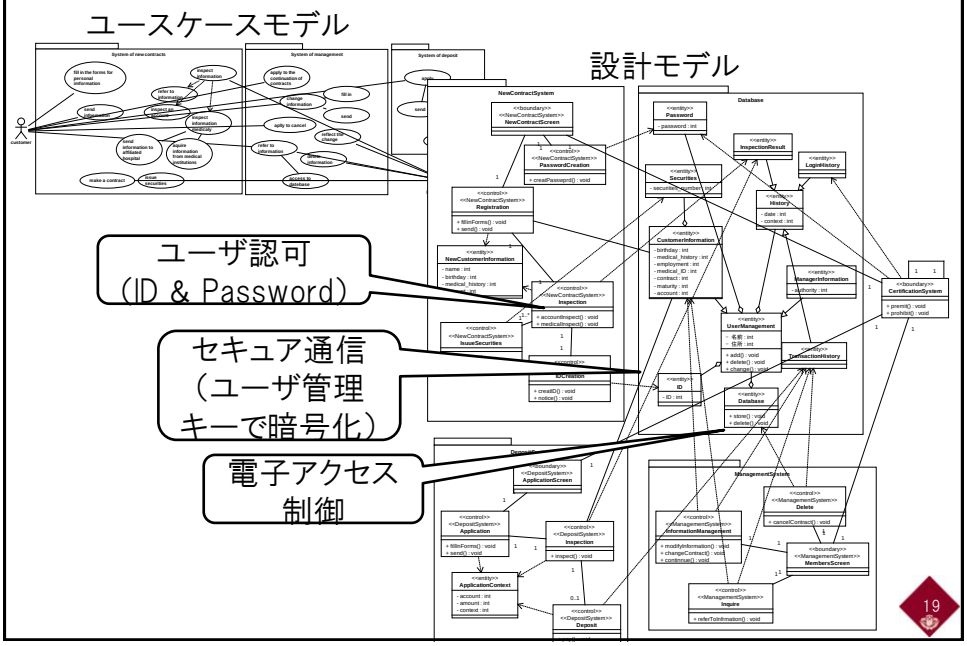

櫨山淳雄, 鷲崎弘宜, 吉岡信和, 海谷治彦, 大久保隆夫, "プライバシーを考慮したソフトウェア開発技術の文献に基づく動向調査", 人工知能学会 知識流通ネットワーク研究会, 2016

17

# b. 知識の一貫した表現・組み合わせ

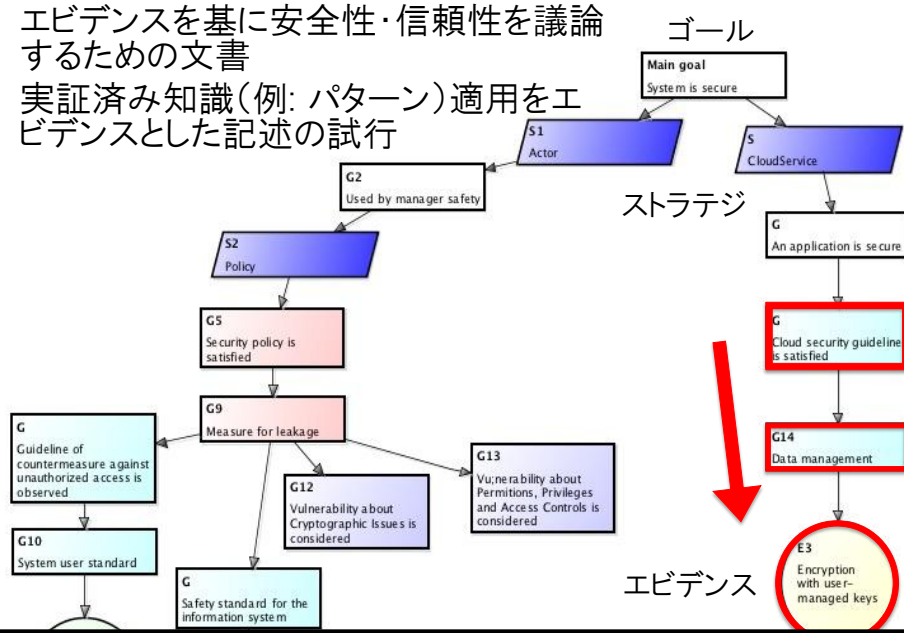


# c. 保険クラウドサービスのモデリング



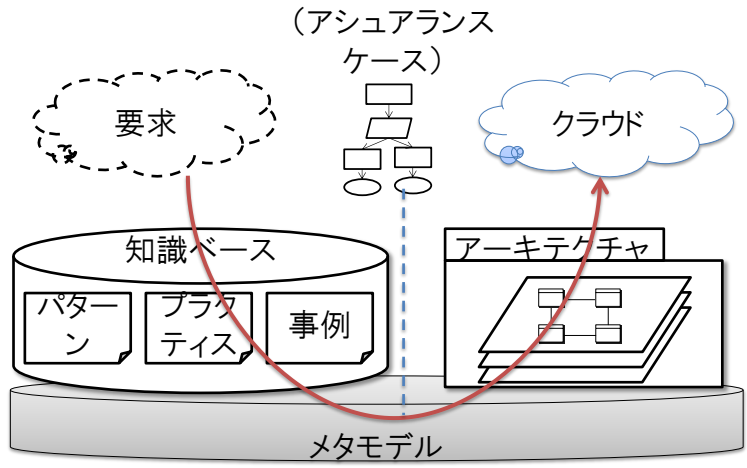

# c. アシュアランスケースによる記録の試行

- エビデンスを基に安全性・信頼性を議論するための文書
- 実証済み知識（例: パターン）適用をエビデンスとした記述の試行



# まとめ

- クラウドサービスのセキュリティとプライバシ を扱うメタモデルの実現: 多様な知識＋クラウドレイヤ
- 応用実証: 知識整理とベース構築、一貫表現、設計適用

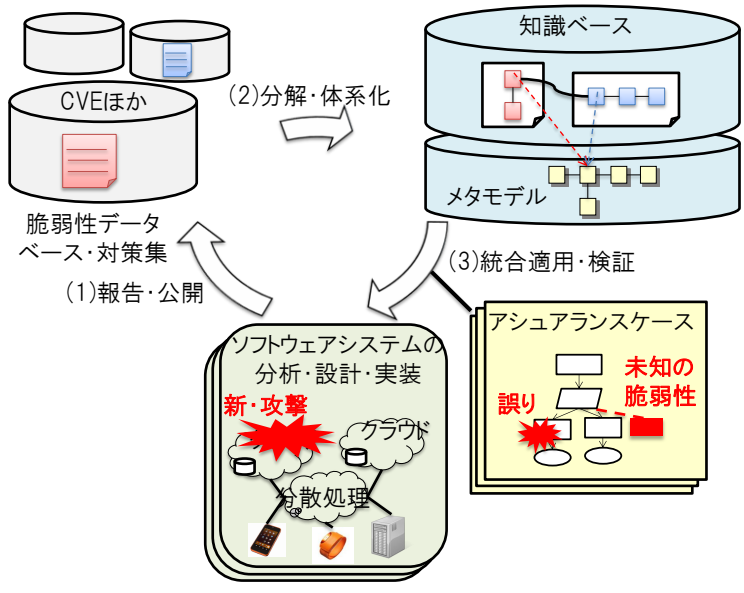



21

# 2015年度 実績

- 論文、発表
  - 鷲崎ほか、“クラウドサービスの開発と運用においてセキュリティとプライバシを扱うためのメタモデル”、コンピュータセキュリティシンポジウム2015
  - H. Washizaki, et al. “A Metamodel for Security and Privacy Knowledge in Cloud Services,” 3rd Int’l Workshop on Patterns Promotion and Anti-patterns Prevention, 2016
  - H. Washizaki, “A Metamodel for Security and Privacy Knowledge in Cloud Services,” SSE Workshop, March 22-23, 2016
  - H. Washizaki, et al. “A Metamodel for Security and Privacy Knowledge in Cloud Services,” 12th IEEE World Congress on Services, Poster Paper, 2016
  - 櫨山, 鷲崎ほか, “プライバシーを考慮したソフトウェア開発技術の文献に基づく動向調査”, 人工知能学会 知識流通ネットワーク研究会, 2016
  - E. B. Fernandez, N. Yoshioka, H. Washizaki, et al., “Modeling and Security in Cloud Ecosystems,” Future Internet, 8(2), 2016
- 国際連携: Security and Privacy Workshop at NII, Mar 22-23

# 展望:メタモデルに基づくエコシステムの実現へ



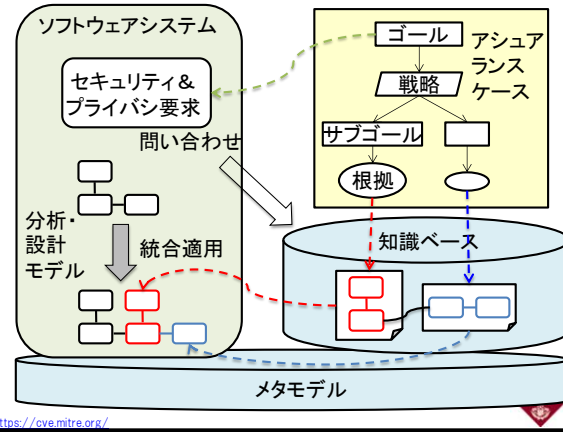



# 展望(つづき)

- (1) 既存エコシステム、脆弱性・対策公開等の調査
- (2) 脆弱性や対策報告から共通部分を知識としてメタモデル上で半自動整理、グラフ構造の知識ベース
- (3) 知識群を組み合わせた新開発および既存拡張をモデルベース＋アシュアランスケースで支援

CVE-2016-2000

HPE Asset Manager 9.40, 9.41, and 9.50 and Asset Manager CloudSystem Chargeback 9.40 allow remote attackers to execute arbitrary commands via a crafted serialized Java object, *related to the Apache Commons Collections (ACC) library*.




[CVE] The MITRE Corporation, "Common Vulnerabilities and Exposures", https://cve.mitre.org/