KDDI R&D LABS

オープン環境における プログラム保護技術の研究開発

田中俊昭、三宅優、清本晋作、仲野有登
（KDDI研究所）

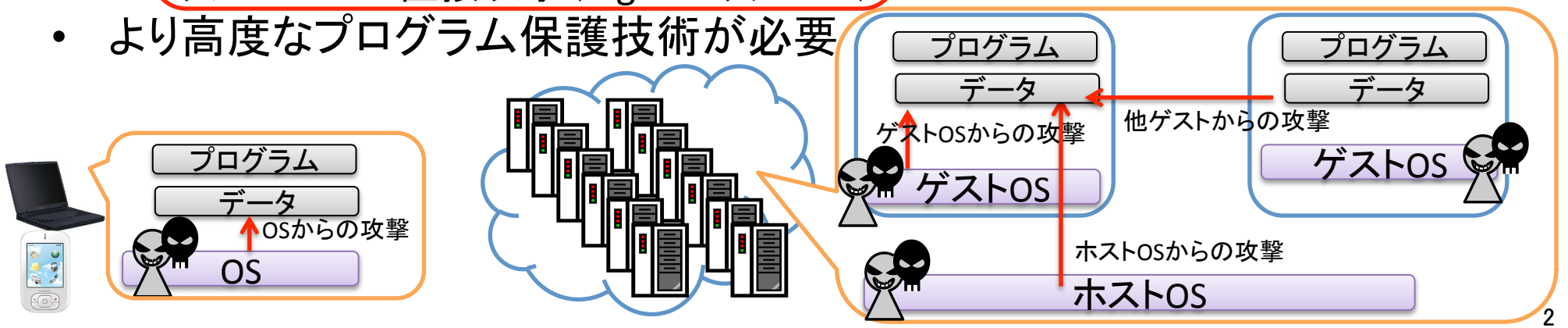
2013.10.1

KDDI R&D LABS

背景

- オープン環境の普及
  - クラウド、スマートフォン、組み込み系システム
- 詳細な仕様が公開
  - 脆弱性も公開
  - 利用者・攻撃者による操作可能範囲の拡大
- 特に以下の脅威に注意が必要
  - 他のゲストOSからの攻撃
  - 実行環境に仕込まれたマルウェア
  - クラウド内の内部不正者の可能性
  - リソースへの直接攻撃（e.g.メモリダンプ）
- より高度なプログラム保護技術が必要

実行環境が安全とは限らず
データと処理の安全性が保証
できない

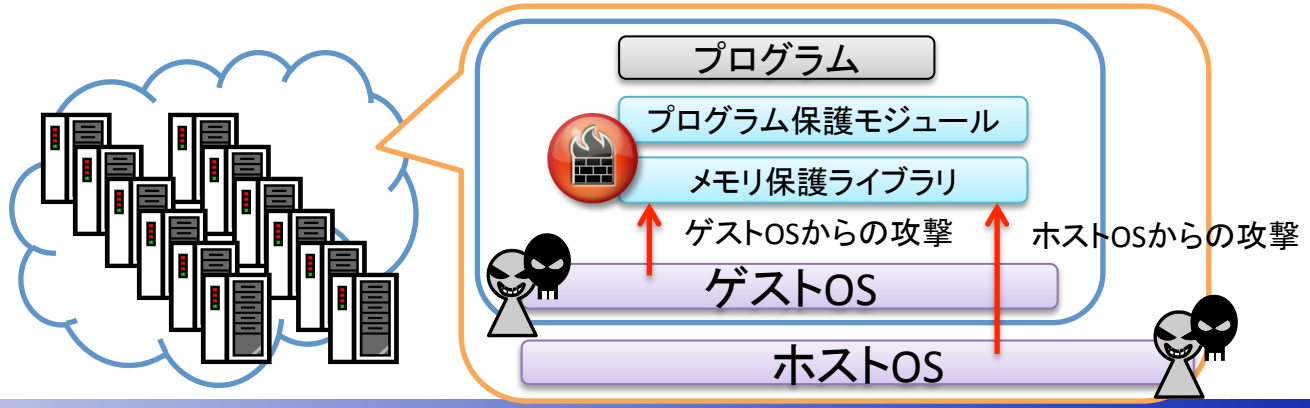


研究開発の目的

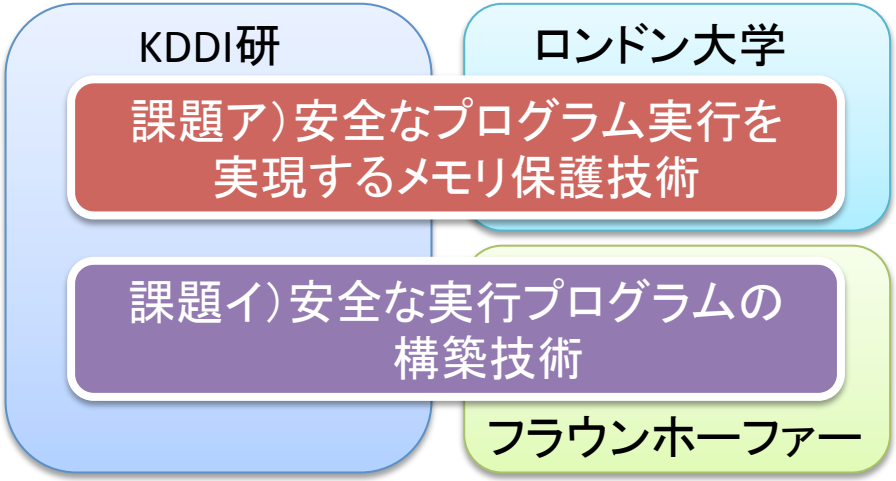
ソフトウェアによるプログラム保護技術を確立

- ハードウェアに依存しない対策
- 低コストで様々な環境に適用可能な対策
- 新たな脅威に対する機能追加の容易さ

- 課題ア）安全なプログラム実行を実現するメモリ保護技術
  - プログラム保護のための新たな要素技術（メモリダンプ等への対策）
- 課題イ）安全な実行プログラムの構築技術
  - メモリ保護を基に安全な環境を構築



研究開発体制

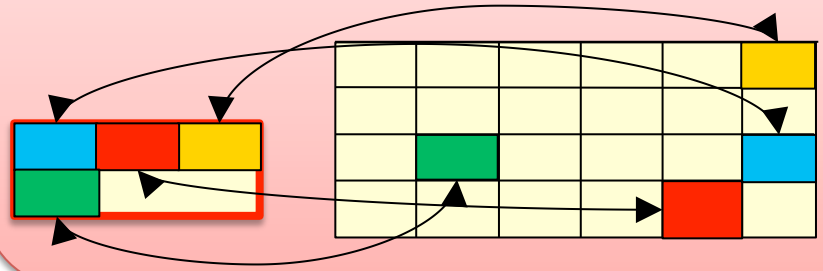


- 日本
  - KDDI研究所
    - 両課題の方式検討、プロトタイプ実装、安全性評価
- 欧州
  - ロンドン大学ロイヤルホロウェイ校（自己資金）
    - 課題ア）に関する方式検討、安全性評価
  - フラウンホーファーSIT研究所（FP7 SecFutur）
    - 課題イ）に関する方式検討、安全性評価

KDDI R&D LABS

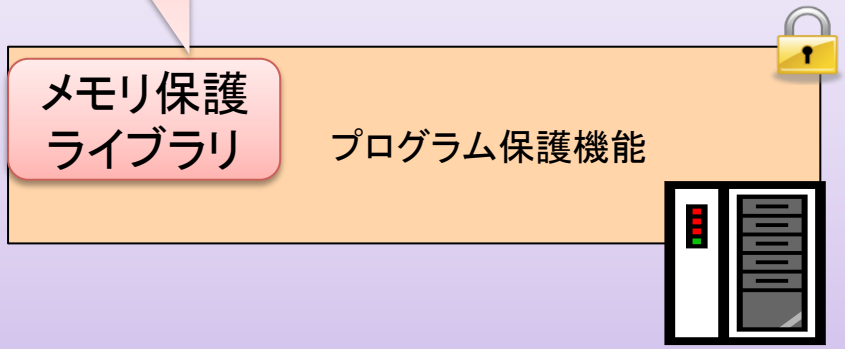
研究開発概要

課題ア）安全なプログラム実行を実現するメモリ保護技術



- 実用的なメモリ保護技術の確立
- 保護手法のライブラリ化
- Linux環境での性能評価

課題イ）安全な実行プログラムの構築技術

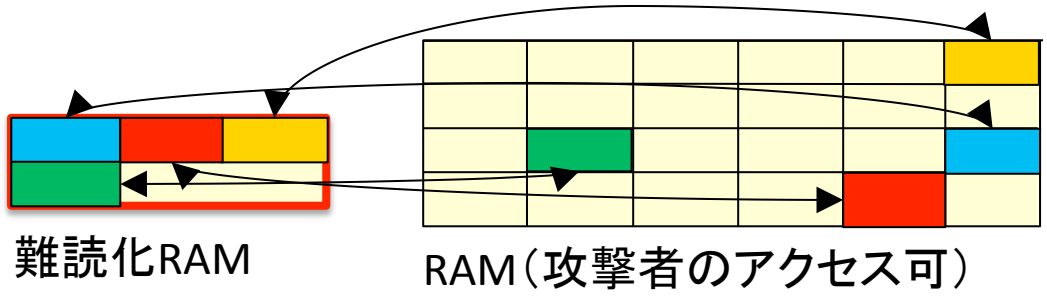


- 課題アとの組合せによる耐タンパ機能の実現とそれを基にしたプログラム保護技術の確立
- クラウド上での実装評価

KDDI R&D LABS

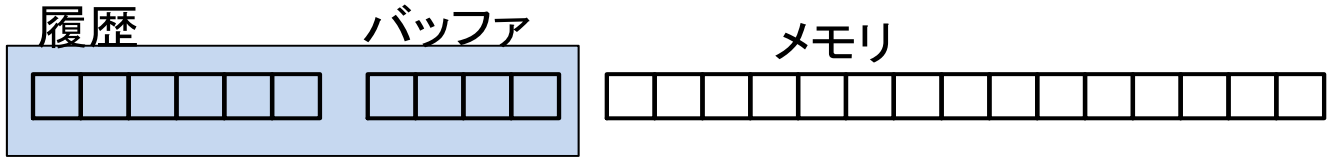
課題ア）安全なプログラム実行を実現するメモリ保護技術

- 目標
  - メモリ保護手法の確立
  - 理論オーバーヘッドを5倍以内
- 成果
  - 難読化RAMと疑似アクセスによるメモリ保護手法を確立
    - 難読化手法を応用して小規模なセキュアRAMを構築
    - 安全性確保のためのダミーアクセスの追加
      - 理論オーバーヘッド5倍以内を達成
    - フラグを用いた高速化
      - 既存のメモリ保護方式（Stefanovら）に比べ約8倍高速な処理を実現
  - 攻撃者のモデル化による安全性の定量評価
    - 同評価を用いた安全性指標の提示



KDDI R&D LABS

提案手法概要



- 難読化手法を利用して安全なRAMを構成
  - アクセスするデータを一旦難読化RAMにコピーする
- 同一データに対する複数回のアクセスを保護
  - ダミーデータ、ダミーアクセスの追加
  - ランダムなダミーアクセスに加え、履歴を参照したダミーアクセスを追加
- 常に二つのデータ(r,p)をコピー
  - 一つは履歴から、もう一つはランダムに選択

KDDI R&D LABS

安全性評価

定義：δ-長ε-安全性

ブロック‘a’に対する2回のアクセスの間隔がδ以下のとき、攻撃者が2回のアクセスを正しく推定できる確率が高々εであるとき、δ-長ε-安全性と定義する

2048 (128×16)バイトのバッファがあったとき
δ=100であれば攻撃者がアクセスを正しく推定できる確率は $\epsilon \leq 1.06 \times 10^{-3}$

KDDI R&D LABS

実装の課題と効率化

- ストレージ利用の効率化
  - 1ブロックに複数のデータを保持
- フラグによるバッファ内のデータを高速検索
  - データ検索のためのスキャンをフラグによって削減
- 難読化によってバッファ・履歴を保護
  - 全データに対してアクセスするよりも効率的、同程度の安全性を確保

KDDI R&D LABS

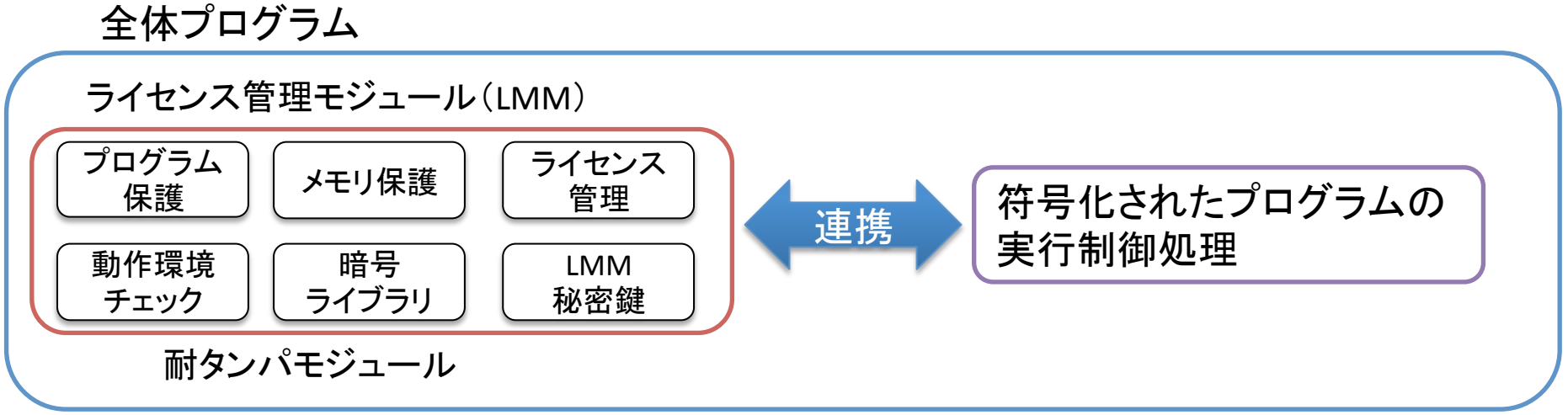
性能評価

- 1MByteのデータ書込みに必要な時間を計測
  - 保護なしの単純書き込み
  - 提案手法
  - 既存方式
- 測定環境
  - Ubuntu12.04, Intel Core i7 3720QM, RAM 16GB

	時間 [s]
保護なし	0.000092
提案方式	0.13
既存方式	1.03

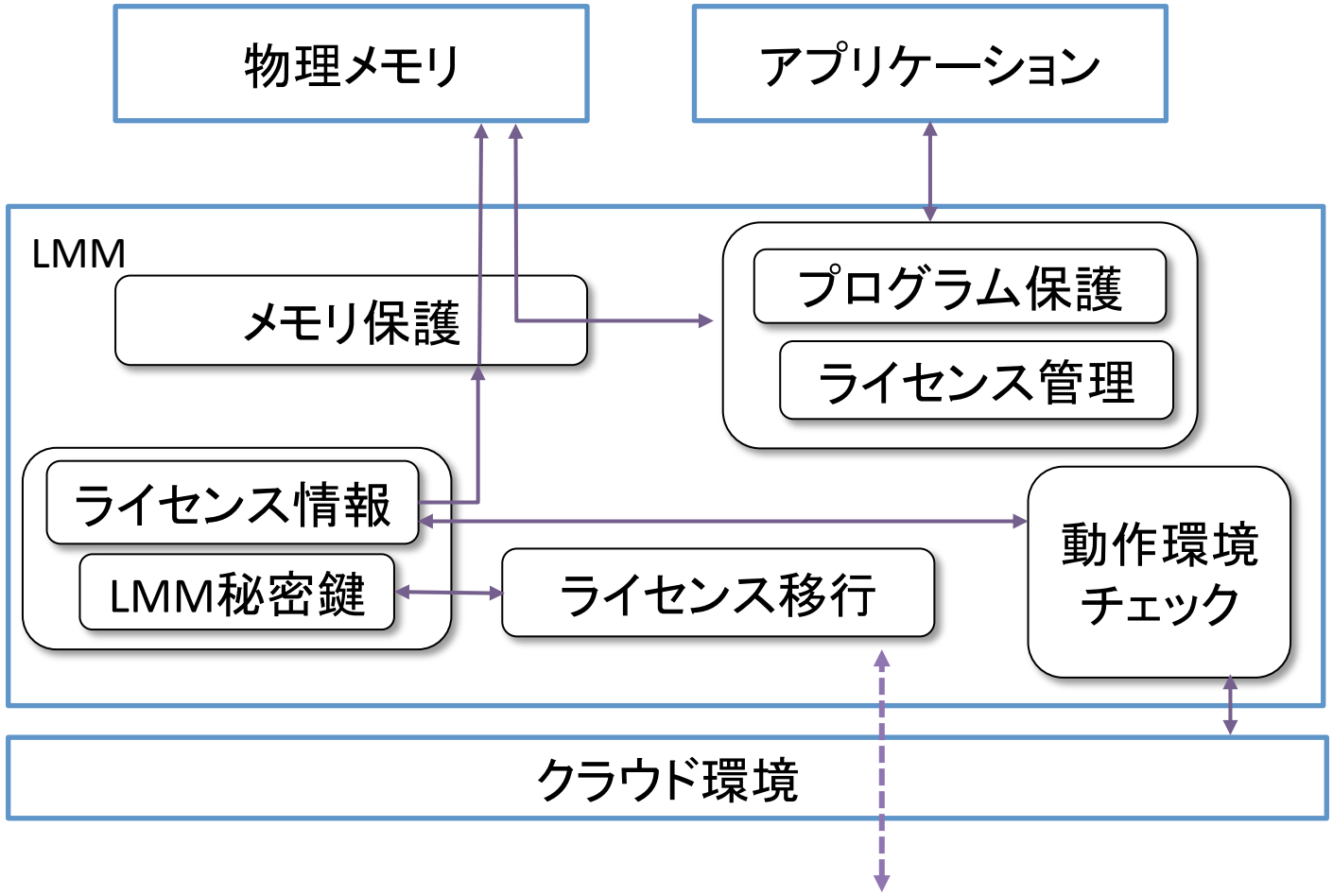
課題イ）安全な実行プログラムの構築技術

- 目標
  - 課題アをもとにプログラム保護手法の確立
- 成果
  - 変数を符号化することでプログラムを保護する手法、並びに、課題アを基に構成した耐タンパモジュール上でその復号処理を安全に実行する手法を確立
  - クラウド上のライセンス管理を例にとり、上記のプログラム保護技術を実証
    - セキュリティ要件を抽出・安全性評価の実施
    - プログラム保護技術の最適化により、約40msecでプログラム保護機能を実現可能



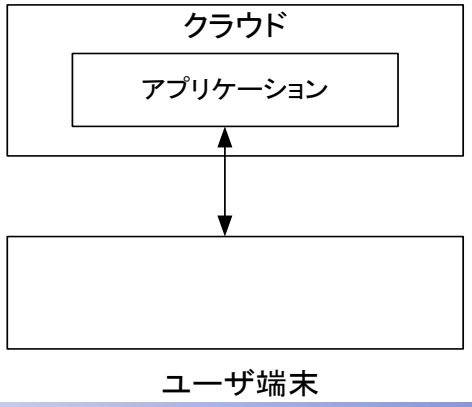
KDDI R&D LABS

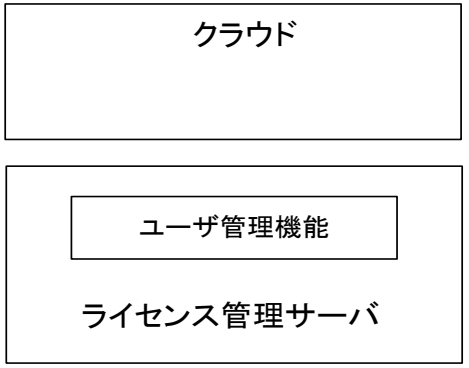
ライセンス管理モジュール



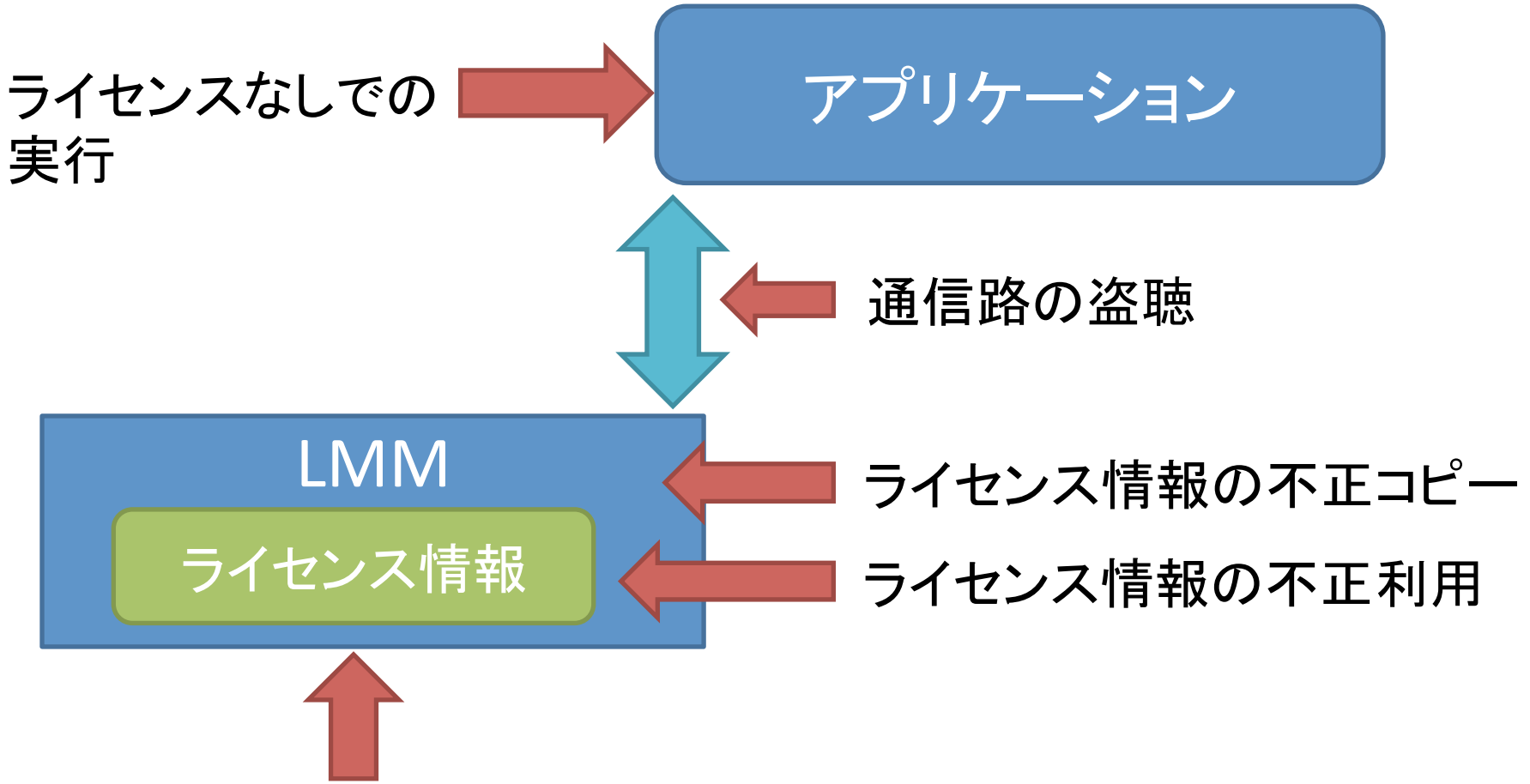
利用モデル

- モデルA
  - LMMをユーザ端末に保管
- モデルB
  - LMMをユーザ端末とアプリケーションを実行するクラウドに保存、アプリケーション実行時にライセンス情報のみクラウドに移行
- モデルC
  - LMMをアプリケーションを実行するクラウドとは別のクラウドサーバで保管
- モデルD
  - モデルBとCの組み合わせ





LMMに対する脅威(概要)



KDDI R&D LABS

LMMに対する脅威

全モデルにおいて、想定される脅威と脅威に対する評価の実施

想定される脅威		攻撃者	ターゲット	モデル			
				A	B	C	D
ライセンスなしでの実行		ユーザ 内部不正者	プログラム (クラウド上)	✓	✓	✓	✓
ライセンスの不正利用		ユーザ 内部不正者	LMM		✓	✓	✓
ライセンスの漏洩	端末から	ユーザ	LMM	✓	✓		
	クラウドから	ユーザ 内部不正者	LMM		✓	✓	✓
通信に対する攻撃		ユーザ 内部不正者 第3者	通信データ	✓	✓	✓	✓
ライセンスの不正コピー	端末から	ユーザ	LMM	✓	✓		
	クラウドから	ユーザ 内部不正者	LMM		✓	✓	✓

KDDI R&D LABS

安全性検証

- ライセンスなしの実行
  - 安全性はアプリケーションバインディングに依存
- ライセンス情報の不正利用
  - LMMによるユーザ認証で防止
- ライセンス情報の盗難
  - 安全な保存領域・メモリ保護によって防止
- 通信路の盗聴
  - 安全な移譲プロトコルによって防止
  - リモートのライセンス確認時には安全な通信路が必要
- ライセンス情報の不正コピー
  - LMMによって保護される

KDDI R&D LABS

性能評価結果

- 各機能の実行に必要な時間をPC上・クラウド上で計測
- 測定環境
  - PC: CentOS 6.3, Intel Core i7 3720QM, 8GB
  - クラウド: Amazon EC2, Xeon 2.66GHz

機能	処理時間[ms]	
	PC	クラウド
ライセンス読み込み	43	42
ライセンス検証	37	37
ローカル環境検証	36	36
ライセンス移譲（AKEは除く）	83	156

KDDI R&D LABS

今後の研究開発・成果展開

- 課題ア）安全なプログラム実行を実現するメモリ保護技術
  - 安全性の検証（PCやスマートフォンでの安全性評価）
  - 既存/新規セキュリティ技術との組み合わせによる安全性・効率性向上
  - PC、スマートフォン、クラウドサーバなどの安全性強化技術として展開
- 課題イ）安全な実行プログラムの構築技術
  - 他のアプリケーションへの応用
  - 高度なライセンス形態（e.g.グループライセンス）への対応
  - ライセンス移譲可能なクラウド向けライセンス管理手法の展開

KDDI R&D LABS

成果のまとめ

- 課題ア）安全なプログラム実行を実現するメモリ保護技術
  - メモリアクセスパターン技術の確立
  - 理論オーバーヘッド5倍の達成
  - 関連特許出願（記憶装置、アクセスパターンの秘匿方法およびプログラム、特願2013040592、日本、2013年3月1日）
  - 国際会議への投稿を検討中
- 課題イ）安全な実行プログラムの構築技術
  - プログラム保護技術によるセキュアなプログラム実行方式を実装評価
  - 課題アと組み合わせたシステムの構築、現実的な処理時間で実現可能
  - 関連特許出願（ライセンス管理システム、方法及びモジュール、特願2013060475、日本、2013年3月22日）
  - 国際会議投稿（LMM: A Common Component for Software License Management on Cloud, SECRYPT2013、発表済み）

	平成24年度	合　計	当初目標
国際会議投稿	2件	2件*	2件
申請特許数	2件	2件	2件

*:1件は発表済み

KDDI R&D LABS

ありがとうございました