SIMを基点とした重要アプリケーションの保護技術

～あなたの取引を安全に守ります。～

BITS 2016
NIHON UNISYS GROUP BUSINESS & ICT STRATEGY FORUM

ユニシス研究会
全国カンファレンス

Foresight in sight

JUA
JAPAN UNISYS USERS ASSOCIATION

東北インフォメーション・システムズ株式会社
小関　松子
横田　勇一

目次

1. はじめに
2. スマートデバイスの普及とセキュリティ対策
3. SIM活用技術の紹介
4. 「許可証」で広がるスマートデバイスの利用
5. 今後の展望

TOINX トインクス

１．はじめに

１．はじめに　－ 会社紹介 -

会社概要

東北インフォメーション・システムズ株式会社（略称：トインクス）

宮城県**仙台市**	**東北電力** 企業グループ
取締役社長 **早坂 栄二**	**情報システム** **会社**
従業員数 **６７８名**	**６０周年**

《社名への思い》

「東北地方を拠点に総合的な情報サービスの提供を通して、経済社会に貢献していきたい」

という私たちの強い意志が込められています。

１．はじめに　－ 会社紹介 -

主な事業内容

情報システム
企画・開発・運用

電子認証サービス

データセンター

クラウドサービス

セキュリティサービス

トインクス
TOiINX
ITで、感動を、ともに。

１．はじめに　– チーム紹介 -

営業本部

- 営業部
- **営業企画部**

新規商品、サービス展開
戦略・試作・初期構築

NFCチーム

TOINX トインクス

２．スマートデバイスの普及とセキュリティ対策

２．スマートデバイスの普及とセキュリティ対策

世界的シェア №.１のAndroid

スマートフォン世界シェア80%を占めるAndroid

Androidのロゴには、ロボットのキャラクター「ドロイド君」

直感的な操作ができるタッチインターフェース

無償で、誰にでも提供されるオープンソース

↓

多種多様な端末（各メーカが端末を自由につくれる）

↓

利用の広がり　より慎重なセキュリティ対策が必要

※「Android」はGoogle Inc. の商標または登録商標です。

２．スマートデバイスの普及とセキュリティ対策

増え続けるAndroidのマルウェア被害

シェアNo.１のAndroidを狙うマルウェア

（マルウェア被害例）

- 機密情報を収集し、攻撃者に送信
- 気づかれないよう自動着信し、周りの音や会話を盗聴

マルウェア感染被害が日々増加している

※2015年 インターネットバンキング不正送金被害額 30億円　5.6%増

パターンファイルの更新やパッチの適用
対策が追いつかない状況

２．スマートデバイスの普及とセキュリティ対策

現状のセキュリティ対策とは

不正なアプリを実行させない対策が必要

既知のウイルス対策に
ブラックリスト方式

もはや、防げない

許可アプリを登録
ホワイトリスト方式

未知のウィルス対策にも

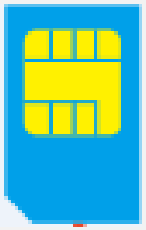
当社が考えるホワイトリスト対策・・・

国内通信キャリア管理のセキュアなSIM利用！

トインクス
TOINX

2．スマートデバイスの普及とセキュリティ対策

SIMカードとは



SIMは、携帯電話で使われている加入者を特定するためのID番号が記録されているICチップ

情報を安全に格納するメモリや、暗号ロジック回路を内蔵されているセキュアエレメント

セキュアエレメント	
ソフトウェア的特性	**ハードウェア的特性**
約束した手続きでのみ内部へアクセスできる（厳重なアクセスコントロール）	物理的に壊すと内部情報が消滅する（耐タンパー性）

2．スマートデバイスの普及とセキュリティ対策

ICチップの普及

- クレジットカード
- キャッシュカード
- マイナンバーカード
- 運転免許証

SIMカードとしてスマートデバイスに搭載

2．スマートデバイスの普及とセキュリティ対策

SIMアクセスの仕組み

① 事前に国内通信キャリアへAndroidアプリ**公開鍵証明書を申請、ハッシュ値を生成**

② 申請された公開鍵証明書の情報を**アクセス許可リストに登録**

③ Androidアプリからのアクセスを**アクセスコントロールが監視、チェック**

④ アプリの**ハッシュ値を測定**、アクセス許可リストに登録があること、改ざんがないことを確認

許可リストに登録されたアプリのみがアクセス可能

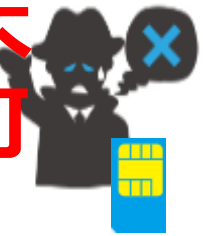
TOINX トインクス

２．スマートデバイスの普及とセキュリティ対策

まとめ：SIMの安全性について

- 許可されていないアプリ
- 改ざんされたアプリ
- 不正な経路からのアクセス

アクセス不可



- プローブを使用したアクセス
- 電子ビームによる
  ビット配列の読取

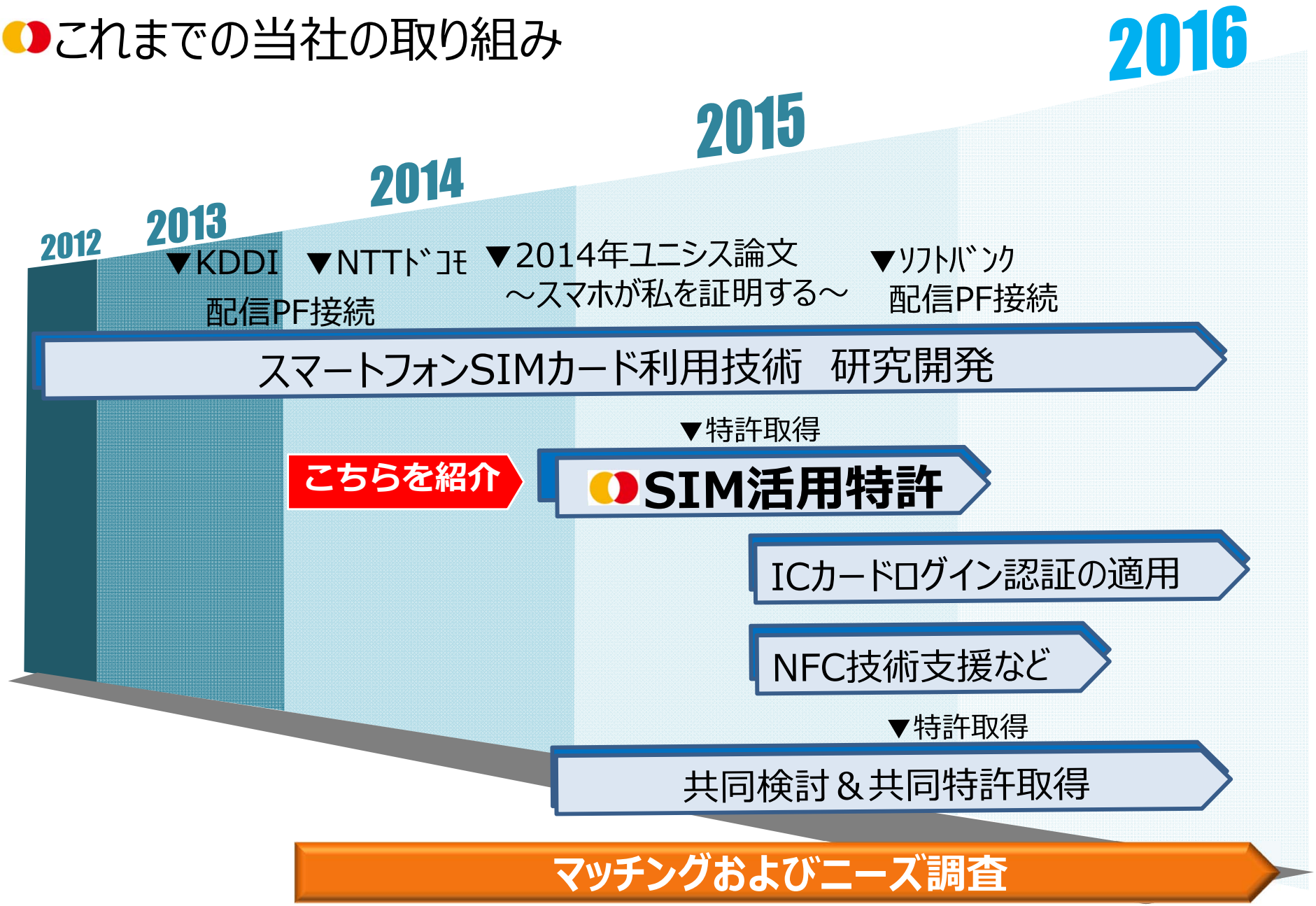
決められた手続き、許可されたアプリのみがアクセス可能

安全なSIMを利用したホワイトリスト対策が可能

3．SIM活用技術の紹介

3．SIM活用技術の紹介

これまでの当社の取り組み

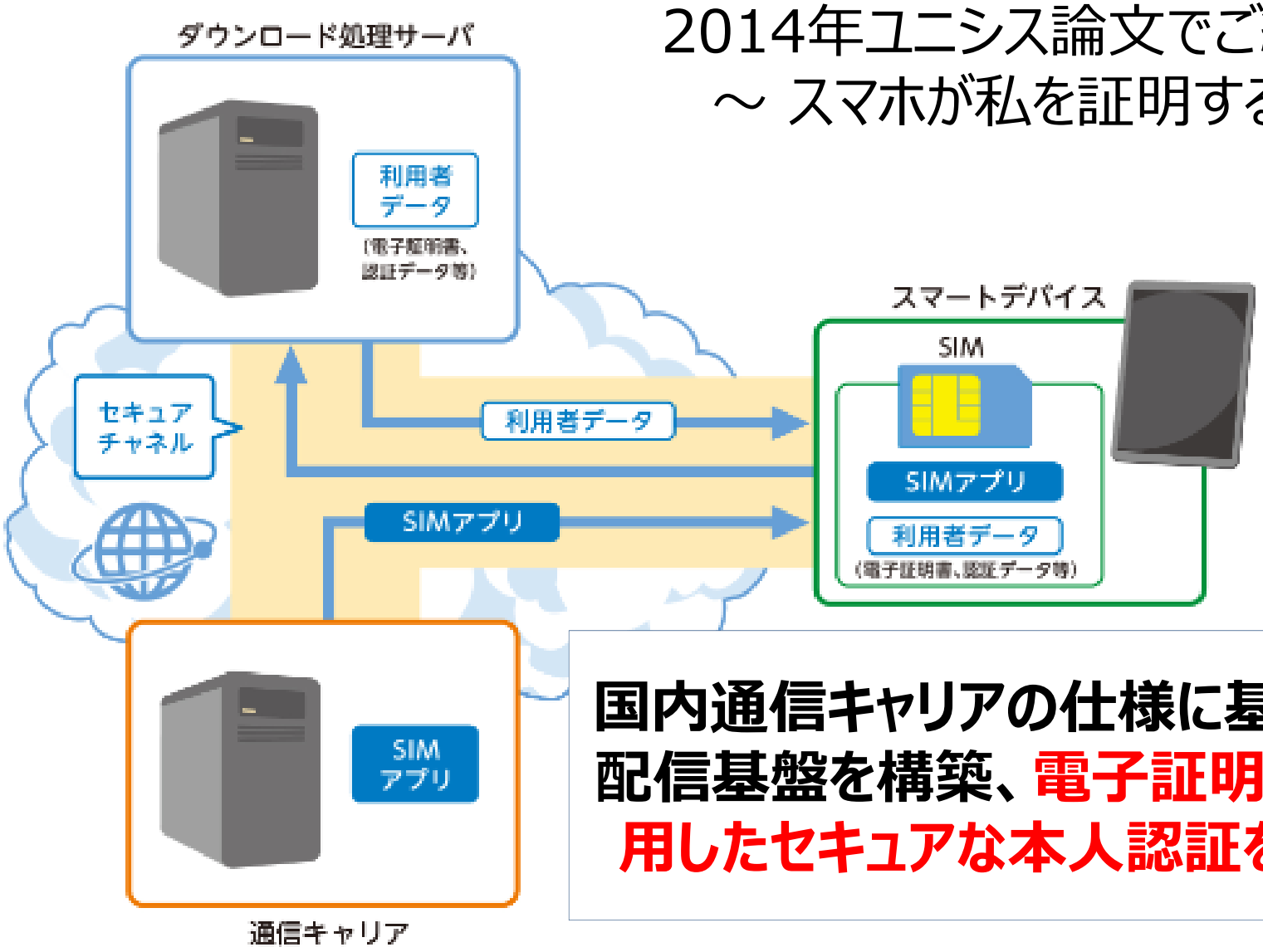


TOINX トインクス

3．SIM活用技術の紹介

配信基盤の紹介（振り返り）

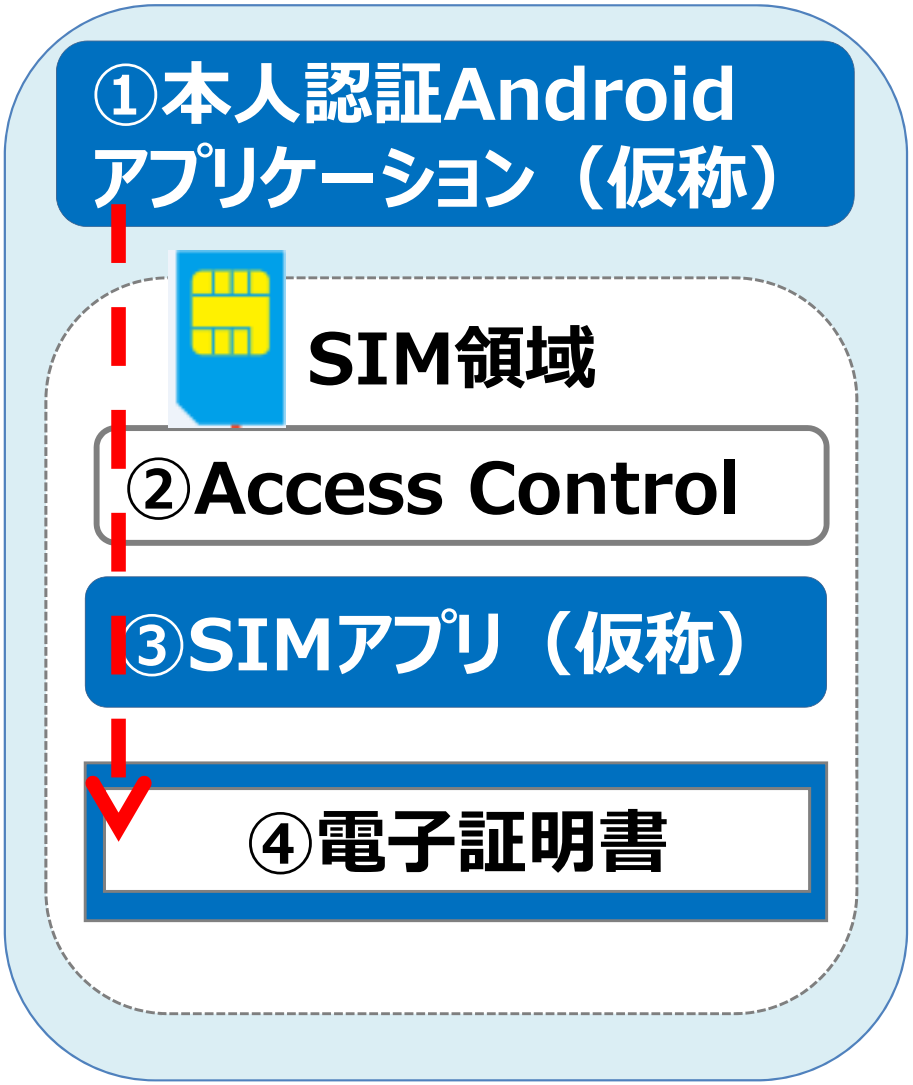
2014年ユニシス論文でご紹介
～ スマホが私を証明する ～



国内通信キャリアの仕様に基づいた配信基盤を構築、電子証明書を利用したセキュアな本人認証を実現

3．SIM活用技術の紹介

電子証明書配信サービスの仕組み（振り返り）



① 本人認証アプリより、**SIMアクセス要求**

② **アクセスコントロール**および**ハッシュ値測定**により、**SIMアクセス可否チェック**

③ SIMアプリによる**SIM内データへのアクセス処理**

④ 電子証明書データ利用

セキュアな本人認証を実現

３．SIM活用技術の紹介

- さらなる活用を目指して

求められるセキュリティ

**スマートデバイス
利用の広がり**

秘匿情報をSIMで管理する本人認証から、
さらに発展させ、**アプリケーション認証** と
SIM領域の有効活用 を実現するため、

３つの機能とSIM領域の活用方法

TOINX トインクス

3．SIM活用技術の紹介

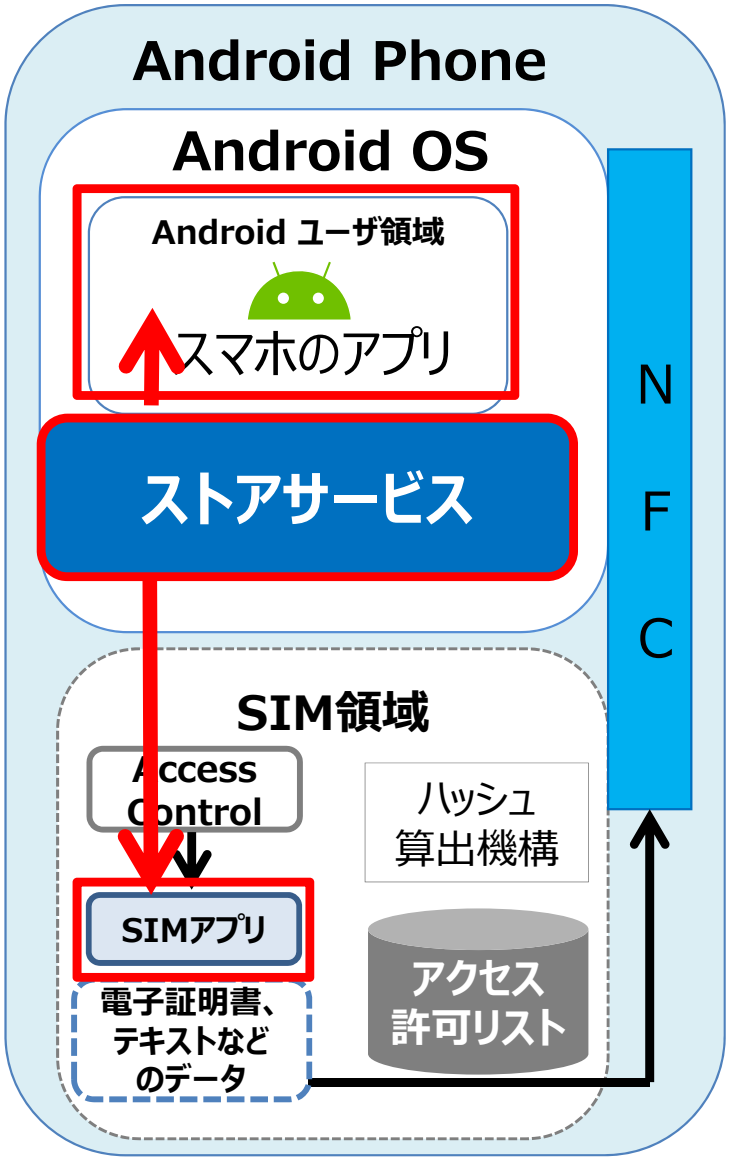
3つの機能追加

「ストアサービス（仮称）、アクセスライブラリ（仮称）、許可証データ（仮称）」の **3つの機能でアプリ認証**を実現

ストアサービス	Androidアプリケーションと SIMアプリの**仲介アプリ**
アクセスライブラリ	Androidアプリケーションがストアサービスに**アクセスするためのライブラリ**
許可証データ	SIMカード内のデータに**アクセスするための認証データ**

3．SIM活用技術の紹介

ストアサービス



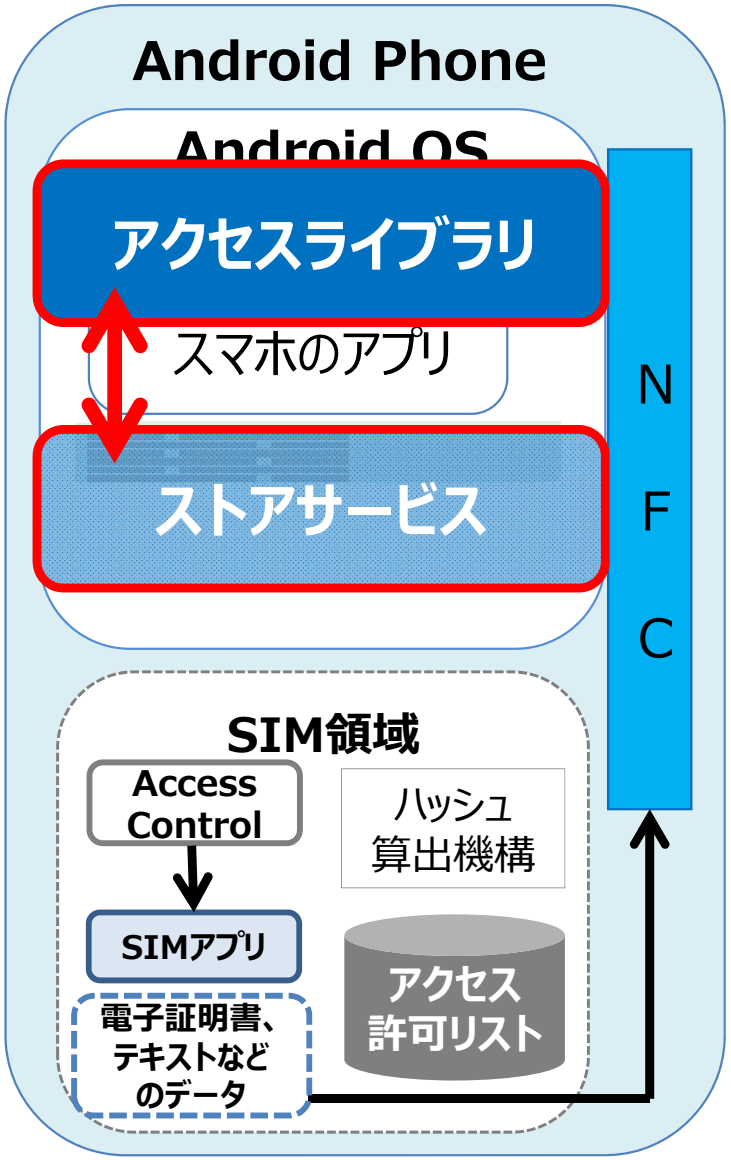
ストアサービスとは、
AndroidアプリとSIMアプリの
仲介アプリ

【ストアサービスの機能】

- 暗証番号（PIN）の入力・結果画面を表示
- 証明書ストアを提供
- 電子証明書の検証
- データの書き込み、読み込み

3．SIM活用技術の紹介

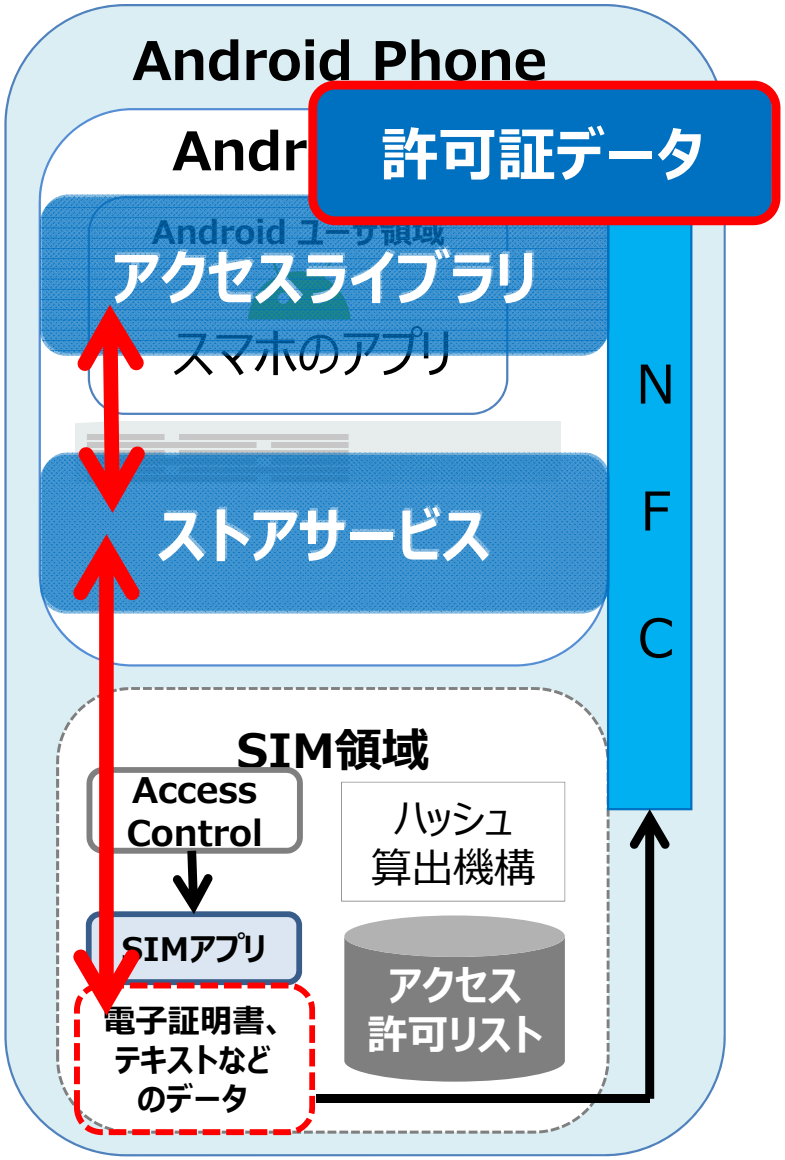
アクセスライブラリ



アクセスライブラリとは、
Androidアプリが**ストアサービスにアクセスできるようにするライブラリ**

3．SIM活用技術の紹介

許可証データ



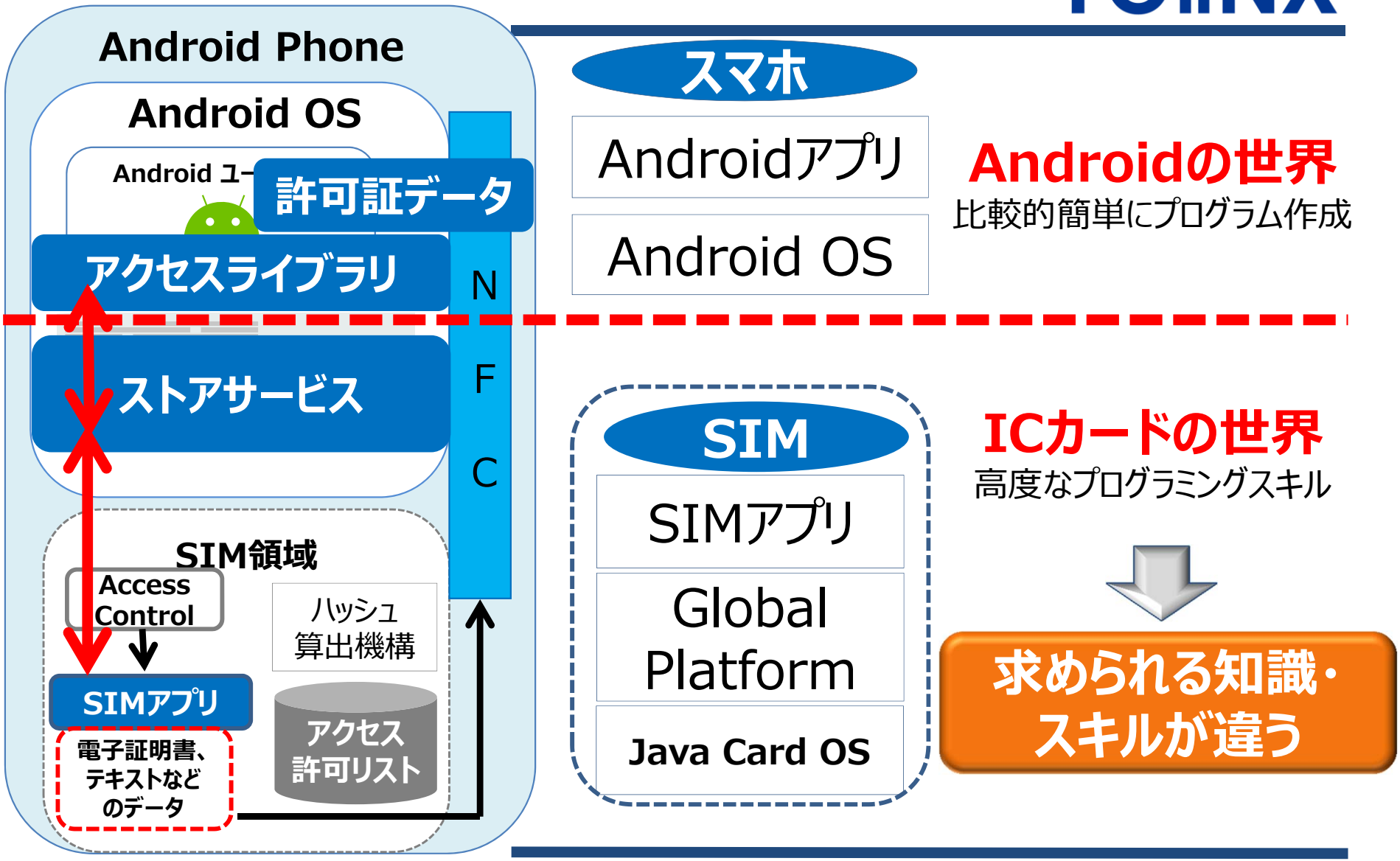
許可証データとは、
SIMカード内にあるデータに安全にアクセスするための情報を持つ
認証データ

SIMアクセス許可情報 と **データを利用するための情報**

安全にSIM内のデータへアクセス

3．SIM活用技術の紹介

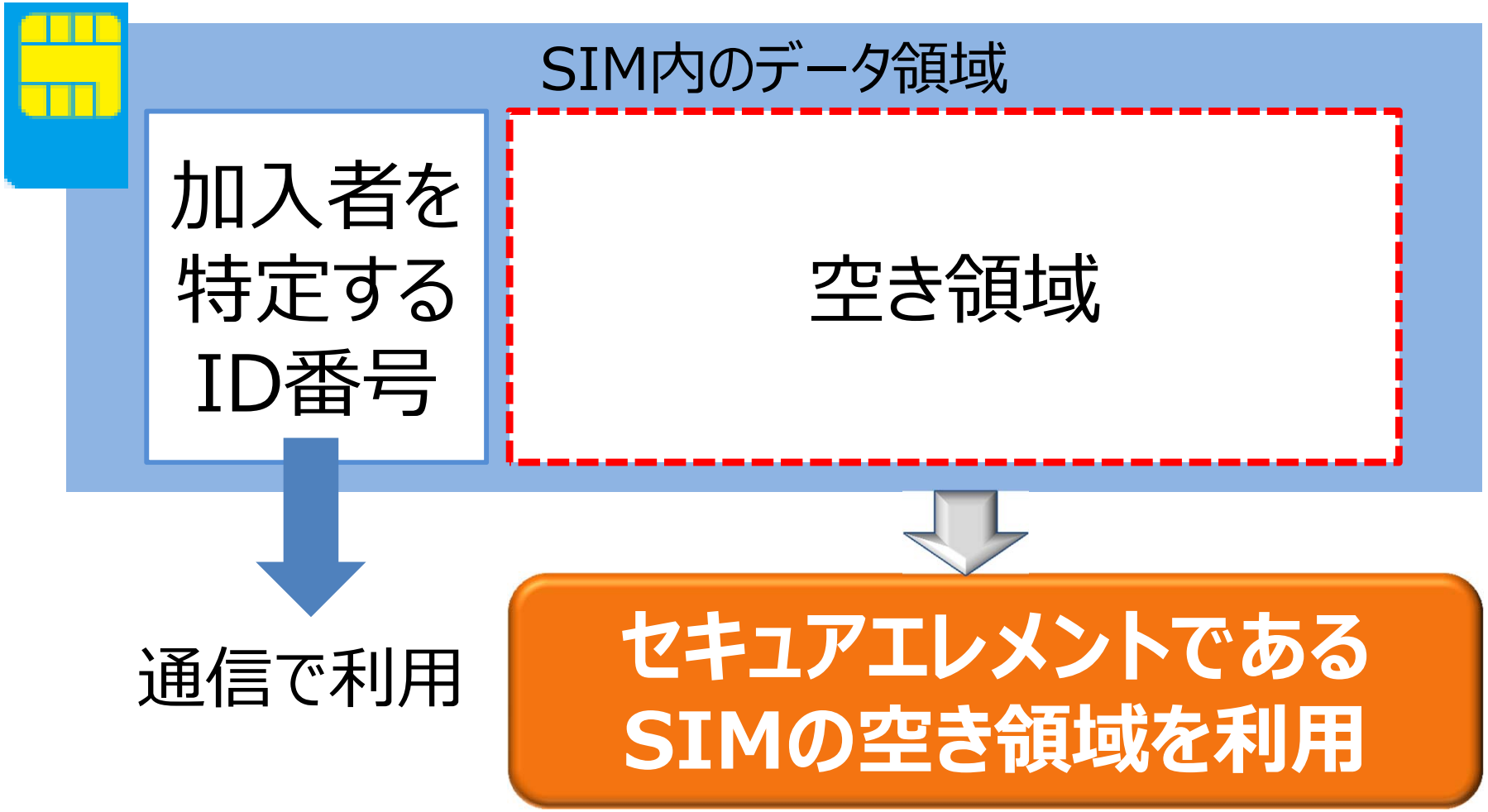
AndroidアプリとSIMアプリ



3．SIM活用技術の紹介

SIM領域の活用方法

SIM領域の有効活用を実現



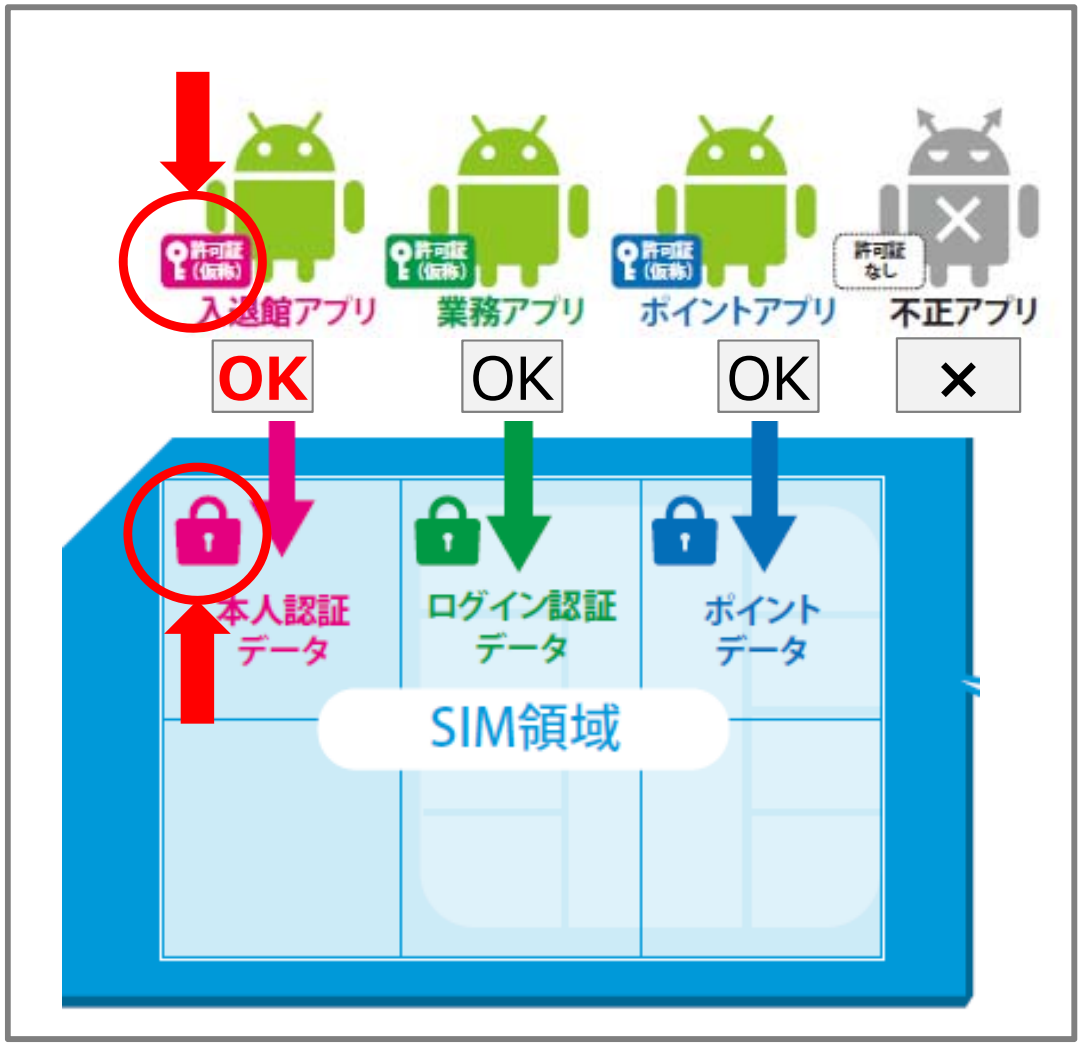
3．SIM活用技術の紹介

SIM領域のデータ利用

Androidアプリケーション単位に、データ利用が可能

3．SIM活用技術の紹介

許可証データによるアクセス管理（**許可証あり**）



許可証データと
鍵の組み合わせで
アクセス可能

**アプリごと、
データ領域ごとの
アクセス管理可能**

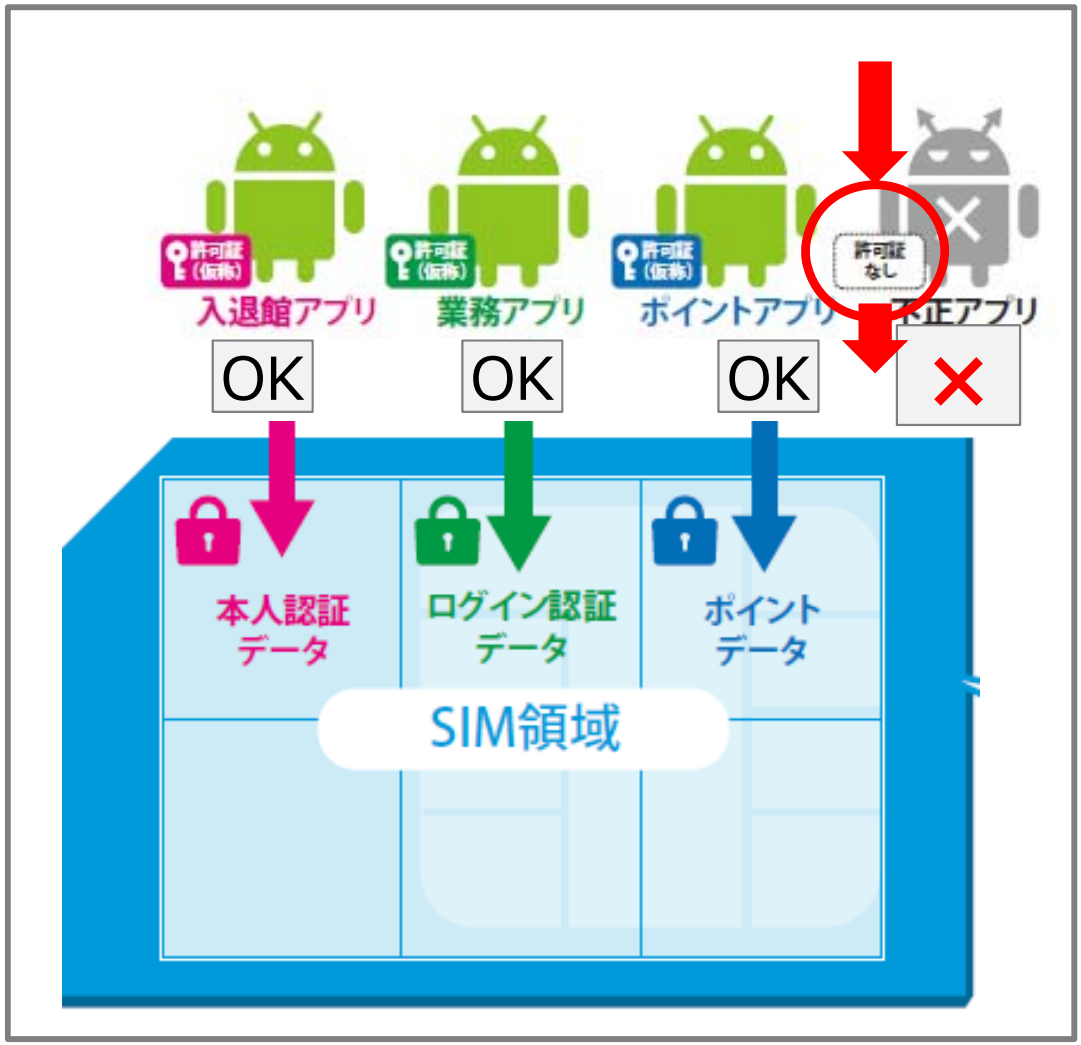
※不正アプリとは、許可証がないアプリ、改ざんされたAndroidアプリ

※「Android」はGoogle Inc. の商標または登録商標です。

トインクス TOiINX

3．SIM活用技術の紹介

許可証データによるアクセス管理（**許可証なし**）



許可証がないアプリ、改ざんアプリは、アクセス不可

不正なアプリケーションから、SIMカード内への不正アクセスを防ぐ

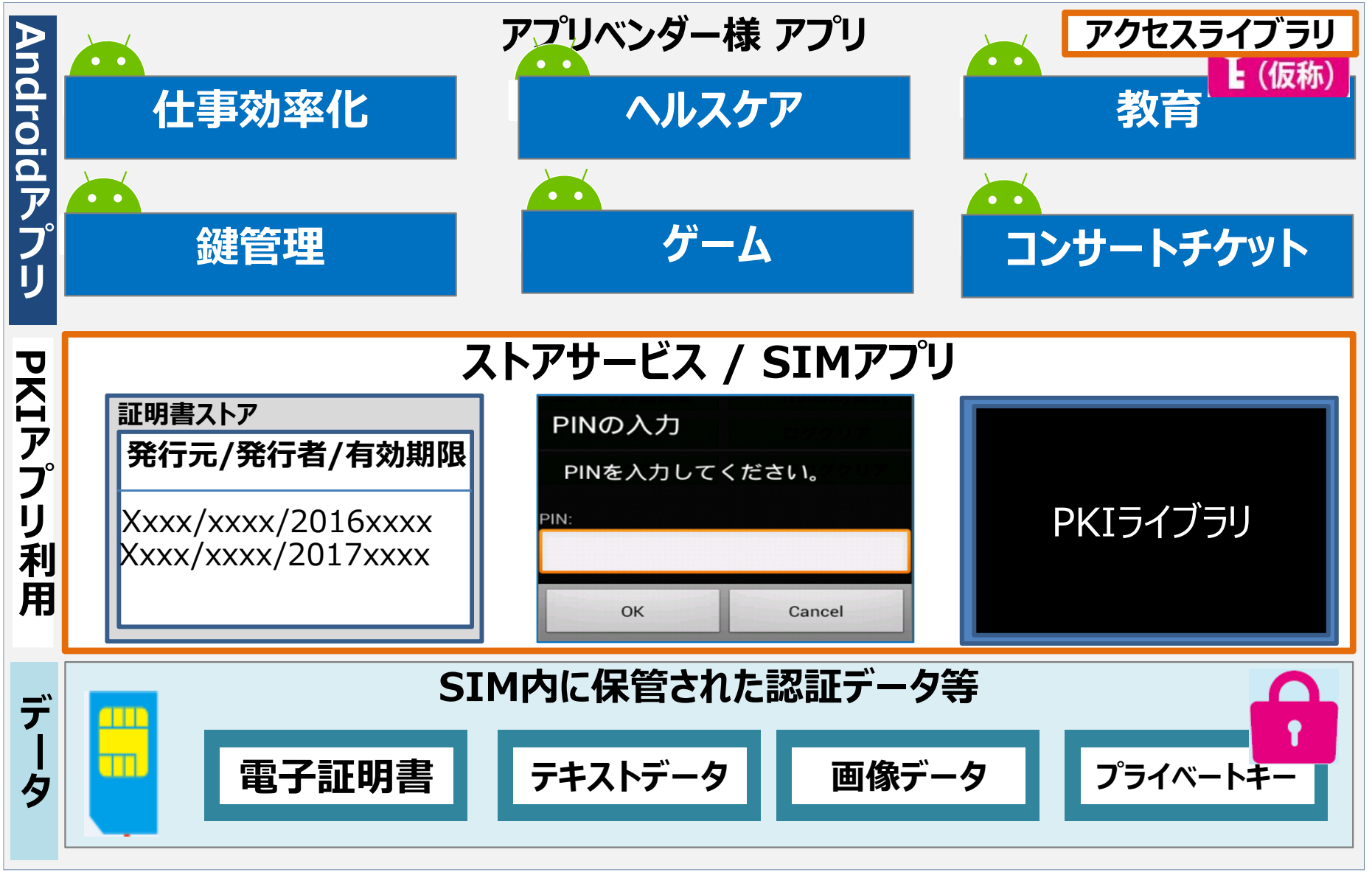
※不正アプリとは、許可証がないアプリ、改ざんされたAndroidアプリ

※「Android」はGoogle Inc. の商標または登録商標です。

TOINX トインクス

3．SIM活用技術の紹介

アプリベンダーご利用のイメージ



3．SIM活用技術の紹介

特許取得

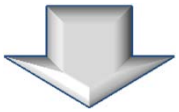
NFC対応Androidスマートデバイスの**SIM**を利用した
Androidアプリケーションのセキュリティ向上を図る技術
について特許取得（特許第5781678号）

- **アプリ認証**：許可証を利用したSIM内データアクセス制御
- **アクセス制御**：アクセスライブラリによるSIMアクセス制御
- **データ配信**：許可証データをSIMに動的に配信する制御

3．SIM活用技術の紹介

期待される効果

- ●秘匿情報を安全に保管
- ●不正アプリの対策
- ●利便性を損なわずにセキュリテイ向上



お客さまに安心してご利用いただけるサービスの提供

3．SIM活用技術の紹介

- 当社が考えたスマートデバイスのセキュリティ対策とは

アプリによる対策

デバイス設定を使った対策

ユーザ教育による対策

アプリ、スマートデバイス、利用ユーザに依存しない
新たな対応手法

NFC対応Android **SIMが持つセキュリテイ機能**に着眼し、
当社の認証・暗号化技術を組み合わせた方法を発案

～SIMを基点とした重要アプリケーションの保護技術～

TOINX トインクス

４．「許可証」で広がるスマートデバイスの利用

４．「許可証」で広がるスマートデバイスの利用

たくさんの鍵やカードをスマホ1台でスマートに！

セキュリティ
ルーム入退出

さらに安全に

取引認証

クレジット決済

身分証明書

ポイントカード

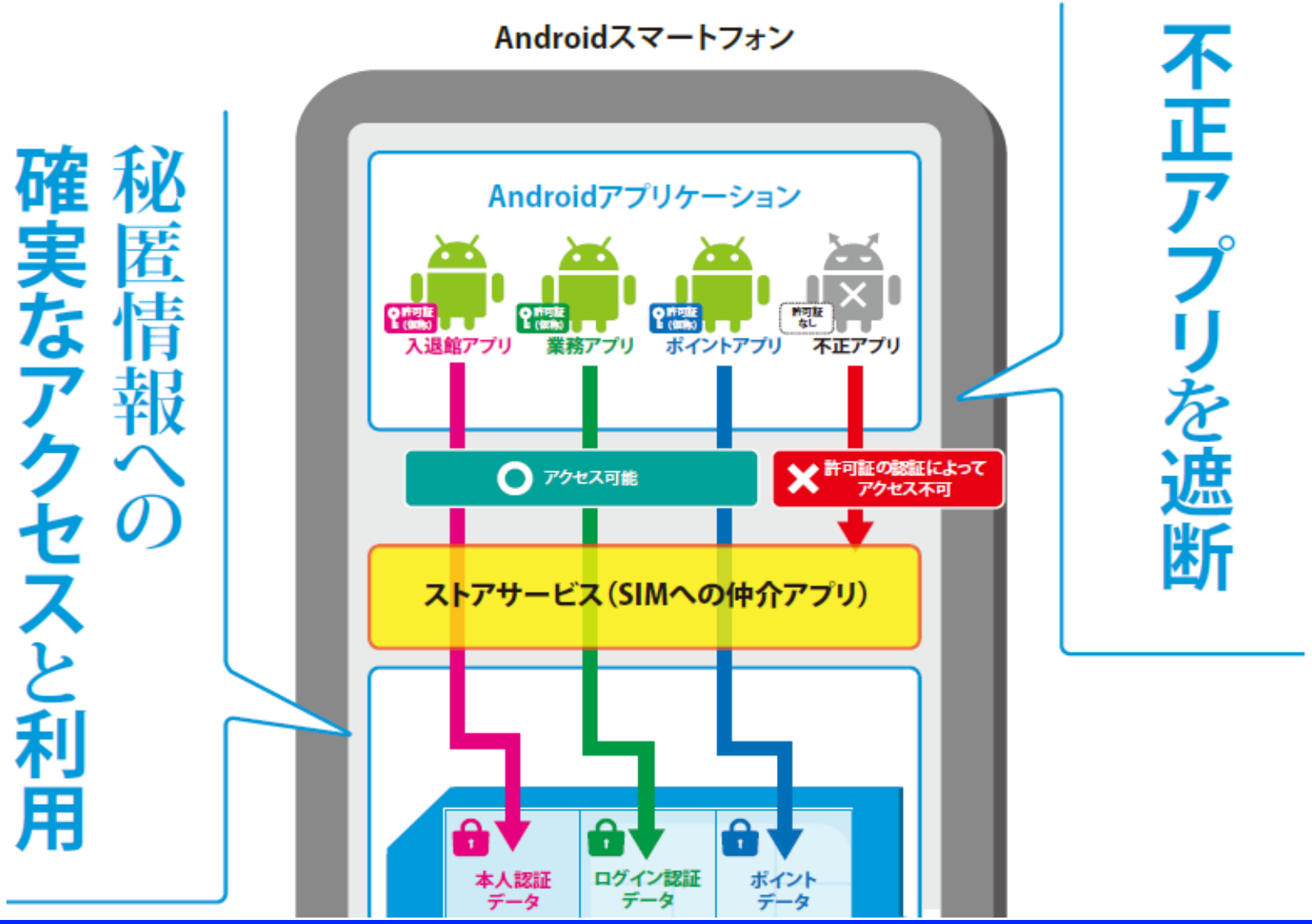
システムへの
ログイン認証

鍵

TOINX トインクス

４．「許可証」で広がるスマートデバイスの利用

不正アプリの対策に



TOINX トインクス

5. 今後の展望

5．今後の展望

- 不正な取引や情報漏洩の被害対策
- オンライン取引やモバイル・バンキングへの展開
- 鍵ベンダ、制御系ベンダ等への技術提供

つながる社会を安全に

より高いセキュリティが求められる分野へ貢献

TOINX トインクス

～ 国内の埋蔵Trust Pointは1億５千万！
スマホから広がるセキュリティ ～

TOINX トインクス

ご清聴ありがとうございました。

SIMを基点とした重要アプリケーションの保護技術
～あなたの取引を安全に守ります。～

本技術の問い合わせは、下記までご連絡ください。

東北インフォメーション・システムズ（株）
営業本部営業企画部　小関・横田
E-mail：sol_info@toinx.co.jp
電話：022-268-2821

TOINX トインクス