資料5

ユビキタスネット社会のプラットフォーム技術

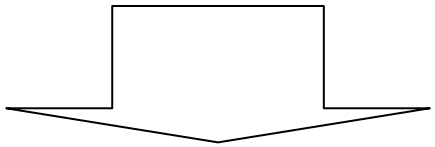
2005年5月25日

NTT情報流通プラットフォーム研究所

ユビキタスネット社会に向けて

情報通信市場におけるお客様ニーズ： 多様化･複合化

1．より高速で双方向性を活かしたブロードバンドサービス
2．固定通信と移動通信の連携により“いつでもどこでも
　何でもつながる”ユビキタスサービス
3．多彩なコンテンツやアプリケーションを“安心･簡単･便利”に利用できる
　ブロードバンドポータルやグローバルなワンストップサービス



展開の方向

安心･安全で便利なブロードバンド･ユビキタスサービスの発展

ＮＴＴ中期経営戦略（主にプラットフォームに関連した具体的な取り組み）

１．固定通信と移動通信の融合などを実現する ブロードバンド・ユビキタスサービスの開発・普及

－固定・移動連携ＦＭＣによるＰＣ、ＴＶ、携帯電話や情報家電等から簡単に利用可能な**ユビキタスサービスを提供**
－臨場感のあるリアルタイムな双方向映像通信サービスを提供
－モバイルにも対応した総合的な**ポータルサービスを提供**

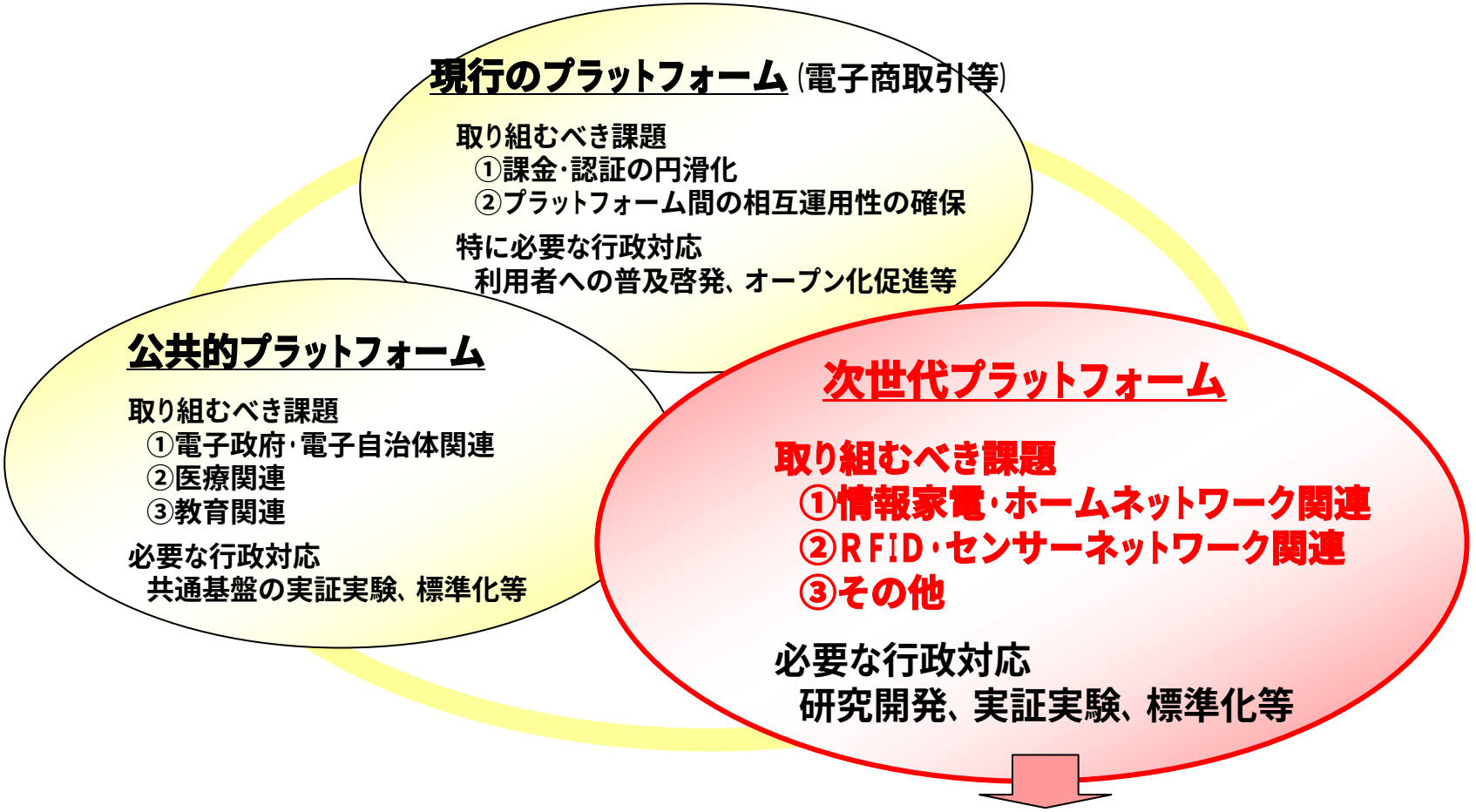
２．高品質・柔軟でセキュリティを担保する 次世代ネットワークの構築

－**ネットワークの安全性**やサイバーテロ**への対応**
－ネット上の不正取引や**プライバシーの侵害**、風評の流布など、ネットの悪用**に対する防御**
－不正トラヒックの流入の防止など品質や**セキュリティの確保**

本研究会で対象とするプラットフォーム分野

第3回「研究会の今後の方向性について」資料3pから抜粋

今後検討すべき3つのプラットフォーム分野



NTTで取り組むプラットフォーム関連技術を紹介

NTTのプラットフォーム関連技術の紹介

次世代プラットフォームの取り組むべき課題

①情報家電・ホームネットワーク関連

1. セキュアゲートウェイ技術

②RFID・センサーネットワーク関連

2. RFIDセキュリティ関連技術

③その他

3. 位置情報関連技術

4. 電子利用権技術

(参考) IDコマース基盤 ((株)NTTデータ他の取り組み)

1．1　セキュアゲートウェイ技術の背景

現状認識　ホームネットワーク（ＰＣ程度）＋ブロードバンドルータ

・光、IP電話対応などで、ホームNWと大容量回線間にブロードバンドルータ設置
　ホームNWに接続されている機器はＰＣ程度
・簡易なファイアウォール機能などはあるものの高度なセキュリティ設定は困難

将来像　ホームネットワーク（多種多様な家電機器）＋**セキリティ機能をもったホームゲートウェイ**

・ＰＣなどに加え、ＴＶなどのＡＶ機器、ホームセキュリティ機器（監視カメラ等）がホームNWに接続
・外出先からでも自由に自宅の家電機器を利用
・セキュリティ脅威（不正侵入、ウィルス、ＤＤｏＳ、など）が増大

技術課題（安心・安全に向けた問題認識）

・セキュアゲートウェイによる**セキュリティ脅威**（不正侵入、ウィルス、ＤＤｏＳ、など）**に対する対策**

1．2　セキュアゲートウェイ技術の特徴

ホームゲートウェイ（HGW）へのセキュリティ機能追加で、外から家電機器を安全・簡単に利用

課題（現状）

FW設定の簡易化
→ 一般ユーザには設定が困難

セキュリティと利便性の両立
→ 特定ポートを常時開
→ 又は登録アドレスからの通信に限定

既存機器・NWでそのまま利用可
☆家電機器へ追加機能なし
☆IPv4（NAT）環境でも利用可能
☆外出先の機器はWebブラウザ機能でOK

解決する技術

①Zero-Configuration

②Dynamic Firewall

利用シーン

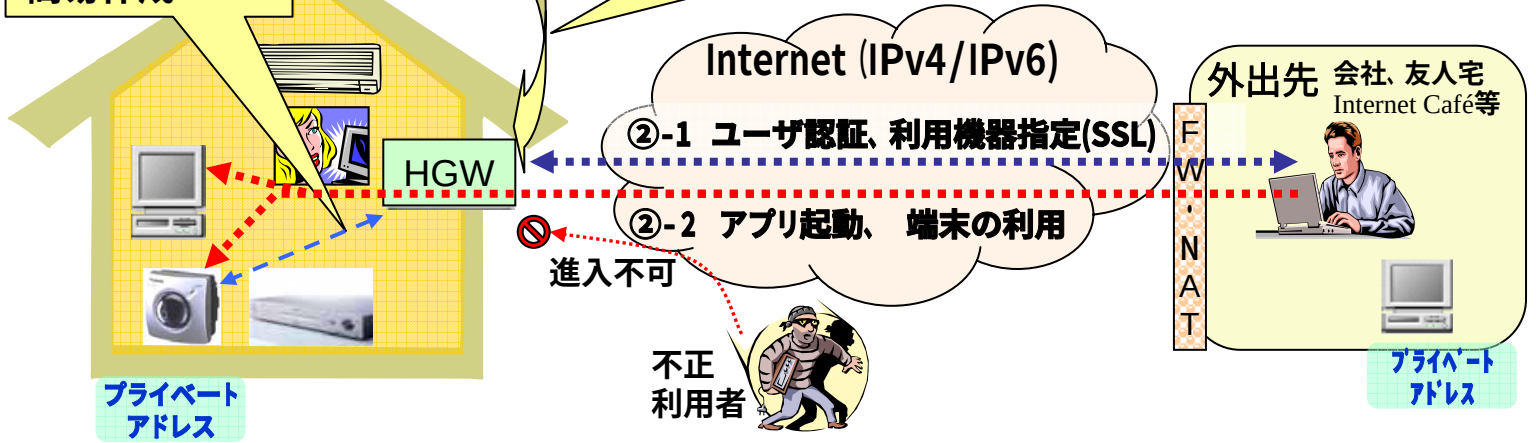
家電機器の新規追加時

外出先からのアクセス時

家電機器設定&アクセスポリシ簡易作成

ユーザ・端末毎アクセスポリシ

ユーザ認証の有効期間内のみそのアドレス発の通信を許可



1．3 セキュアゲートウェイサービスイメージ

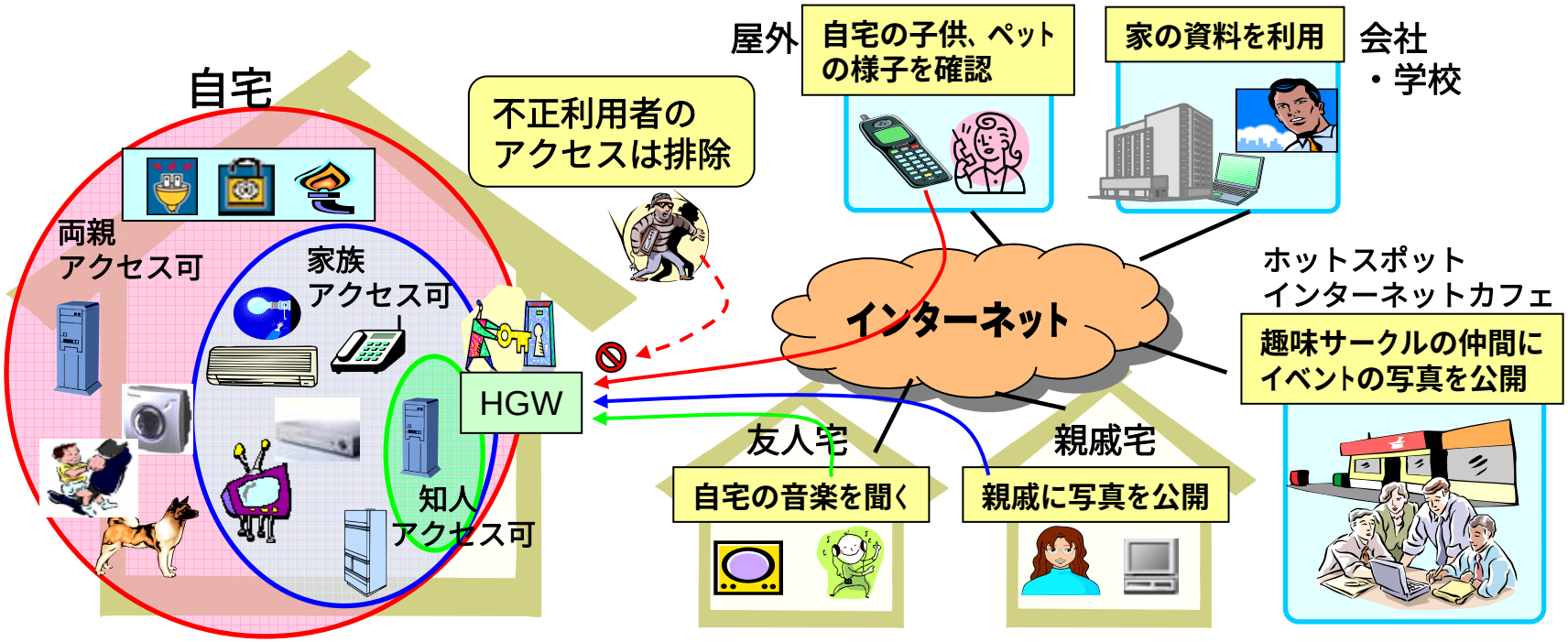
端末、場所を限定することなく、安全･簡単に外出先から家庭内機器を制御することを可能にするサービス

自動に設定！

誰でも、簡単に、新しい機器のセキュリティ設定が可能

簡単に利用！

利用端末、場所を選ばず**簡単、安全に自宅のコンテンツ、機器を利用**



1．4　セキュアゲートウェイ技術からの提言

プラットフォーム化に向けた今後の課題

- 汎用ＯＳ利用、複数ベンダ開発に伴うオープン化に向けた**ＯＳ、ハードウェアの安全性、信頼性の向上**
- （遠隔）サービス機能追加時の安全性、**サービス相互の協調性の担保**
- ビジネス化推進中であるが、更なるプラットフォームの発展のためには、専門知識を有しない　個人のエンパワーメント向上のため、以下の課題検討も必要

- **ユーザへの適切な情報提供（脆弱性情報、わかり易い安全性の表示）**
  - ユーザに対するセキュリティ関連情報の開示（脆弱性情報と対応策）と取扱体制の確立。購入に際して安全性が容易にわかる表示
- **サービスの責任分担と安全基準**
  - ウィルス、DDoSなど様々な攻撃への対応に向け、ネットワーク、HGW、各家電等ホームネットワークの構成要素についてセキュリティの観点からのアーキテクチャ検討
- **安全な機器購入のための業界全体での認定制度、安全体制つくり**
  - ＨＧＷの高機能化が進展した際にも対応可能な、簡易なセキュリティレベルの機能要件と保証要件の認定、相互接続環境の提供

2．1　RFIDセキュリティ関連技術の背景

現状認識　利用分野は限定的でセキュリティ対策も不十分

・流通・物品管理分野では個別適用が中心。セキュリティに関するプラットフォームレベルでの検討・対策は不十分
・ユビキタス分野（商品購入後のRFID利活用、個人識別への活用など）での適用例は少ない
- 魅力的なアプリケーション模索状態
- プライバシ問題に対する懸念が大きい

将来像　あらゆるモノにRFIDタグが着く

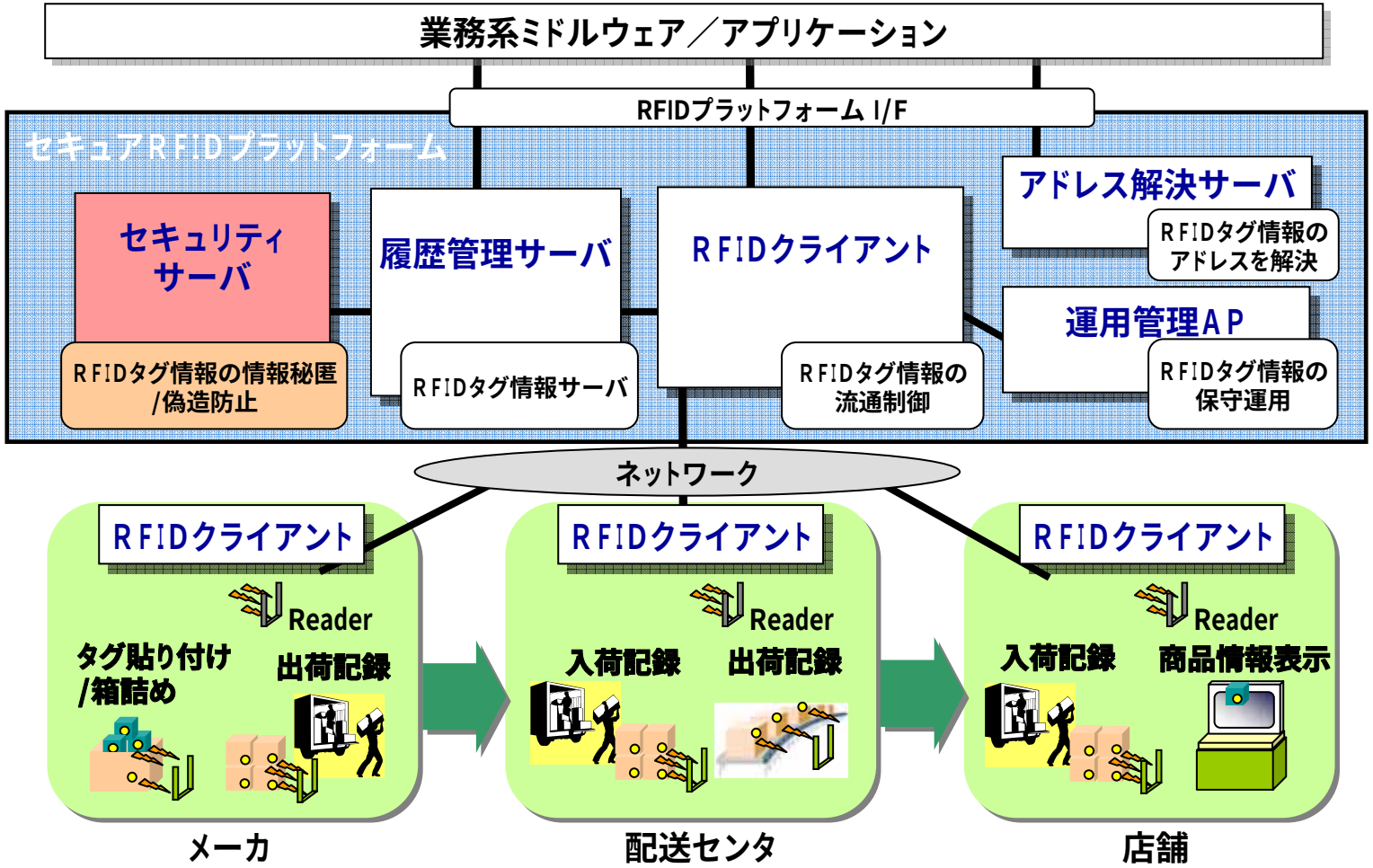
流通・物品管理分野および将来のユビキタス分野における安全・安心なRFIDサービスの実現

技術課題（安心・安全に向けた問題認識）

・RFIDプラットフォームのセキュリティ高度化（情報秘匿、偽造防止など）
・RFIDプライバシ問題の解決

2．2 セキュアRFIDプラットフォームの特徴

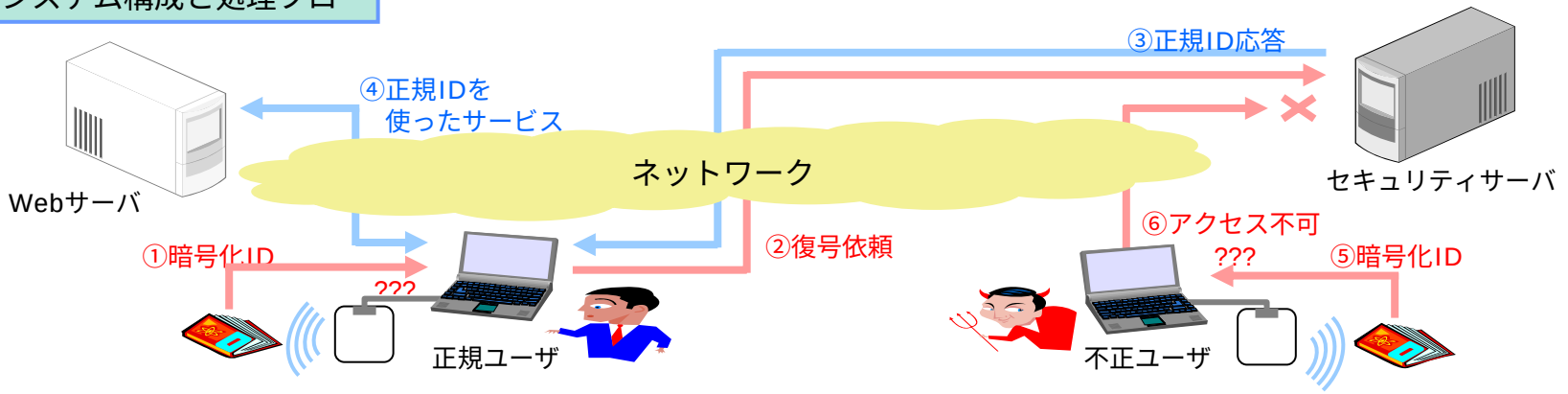
アプリケーションの開発効率や再利用性に優れた機能／性能を有するサービス基盤を構築し、その上でRFIDタグ情報の情報秘匿/偽造防止を**セキュリティサーバ**で実現



2．3　RFIDプライバシ保護技術の特徴

RFIDタグによる所持品情報の盗み見やユニークIDの追跡･名寄せなどのRFIDプライバシ脅威に対して、IDの秘匿化などにより、プライバシの保護を実現

システム構成と処理フロー



RFIDプライバシ保護方式1

①可変秘匿ID方式「コストを最優先させた方式」

- ●外部コンピュータでIDを再暗号化＆再格納
- ●定期的なIDの変更（毎送信毎ではない）
- ●メモリのみ搭載するため非常に低コスト

ID（EPCの例）

Ver	製造者ｺｰﾄﾞ	商品ｺｰﾄﾞ	ｼﾘｱﾙ番号

①暗号化など

1&(H)I#090djewIEJEU$J”) “HJUI

外部コンピュータ

1&(H)I#090djewIEJEU$J”)928#” (“HJUI

④再秘匿化(再暗号化など)

jferJIE#u9frennzl)(KD#IDN#URH#OJ

②格納　秘匿ID　③読込　⑤再格納

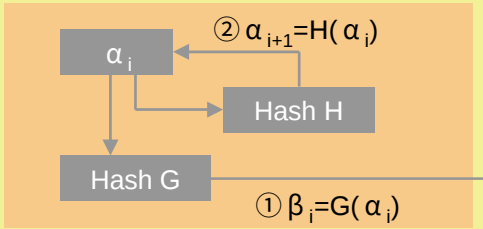
RFIDタグ

RFIDプライバシ保護方式2

②Hash-chain方式「安全性とコストを優先した方式」

- ●タグ内部でIDを再暗号化（Hash演算）
- ●送信毎にIDが変更されるため安全
- ●Hash演算回路のみを搭載するため比較的低コスト

RFIDタグ



α：仮ID（毎回ハッシュ演算更新される）

3．1　位置情報関連技術の背景

現状認識

・位置測位技術
- 広域：ＧＰＳ、携帯電話、ＰＨＳなど
- 狭域：アクティブＲＦＩＤタグ、パッシブＲＦＩＤタグ、音など

・位置情報活用サービス・技術
- 広域：カーナビゲーション、迷子探索、緊急救助などプラットフォームレベルでの活用が促進
- 狭域：物品管理、行動監視、マーケティングなどに利用
  個別ソリューションが中心でプラットフォーム化に至っていない

将来像

人、乗り物、物品などの位置を検出し、それに基づくさまざまなサービスに活用

ＮＴＴにおける位置情報活用システムの研究事例紹介

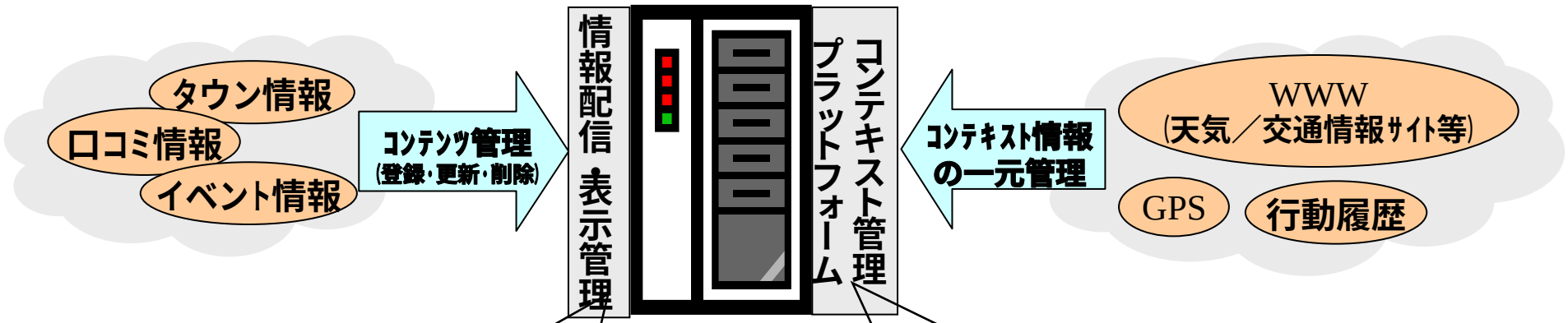
（広域レベルでの新しいアプリケーションの創出）
・携帯電話を利用したコンテキストアウェアネス配信システム
（狭域レベルでの新しいアプリケーションの創出）
・ＲＦＩＤタグの位置情報を利用した映像システム

3．2　コンテキストアウェアネス配信システム

ケータイに**タイミングよく情報を配信できるシステム**

3．3　コンテキストアウェアネス技術の特徴

利用者のコンテキスト（位置、天候、情報閲覧履歴などの状況）を把握し、**コンテキストにあわせた情報配信**を可能とする技術



＜研究所技術の特長点＞

コンテキストにあわせた情報表示

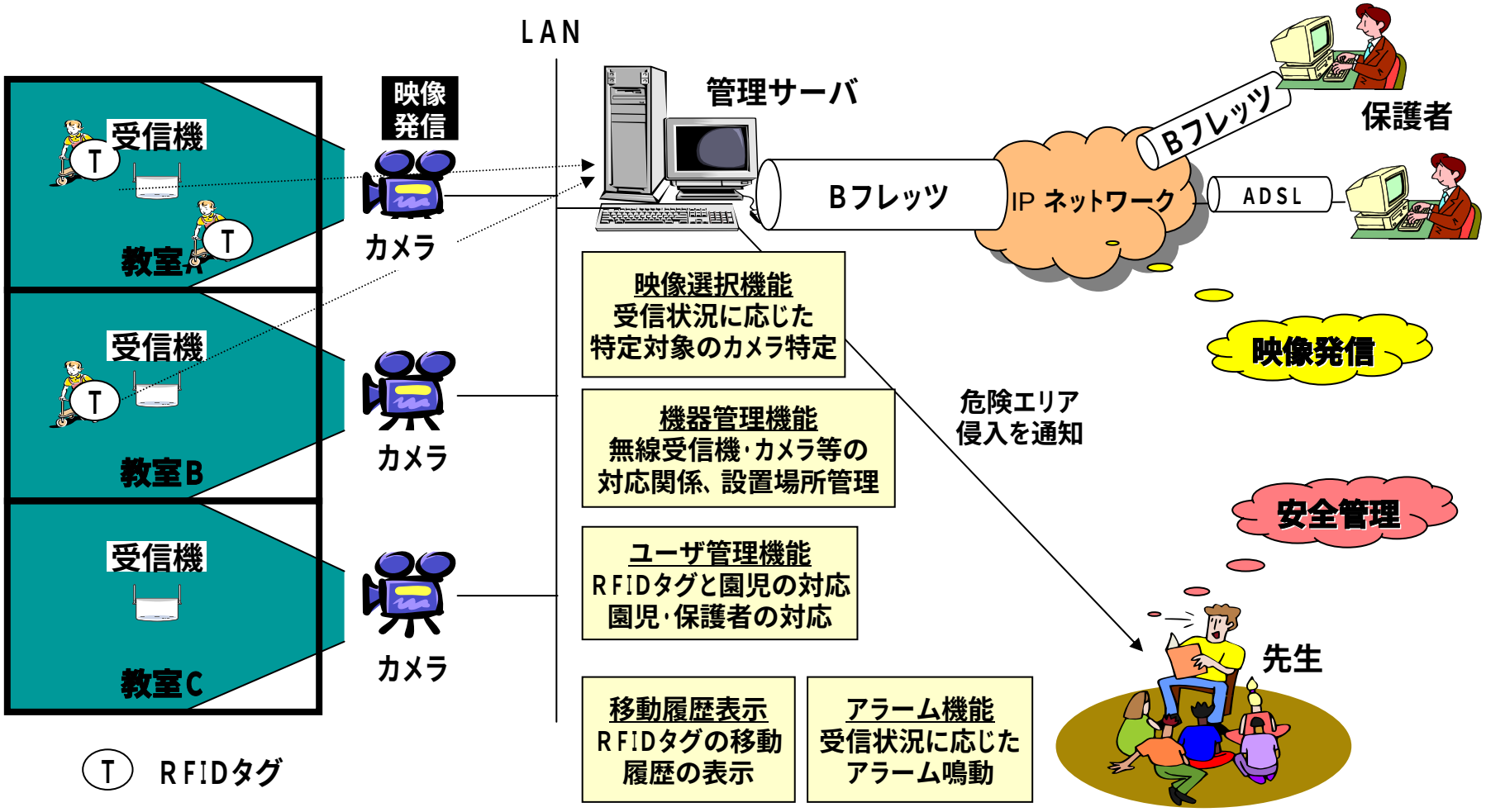
携帯電話の画面に、**状況に適した情報へのポータル**を表示、一度表示した情報を**状況変化にあわせて消去**することも可能

コンテキスト情報に関する処理を共通化したプラットフォームを実現

“お店付近にいる”、“お店から遠ざかる”といった**利用者状況の時系列変化を把握**

3．4　RFIDタグの位置情報を利用した映像システム

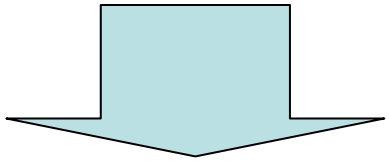
RFIDタグとカメラとの連携により、RFIDタグを所持する個人･個体を指定して、そのカメラ映像をネットワーク経由で受信できるシステム



3．5　プラットフォーム化に向けた今後の課題

RFIDセキュリティ関連技術、位置情報関連技術からの課題

・ユビキタスサービス分野におけるアプリケーションの創出・検証
・社会受容性（サービス魅力、プライバシ問題、倫理上の課題など）の検証
・技術実効性（安全性、スケーラビリティなど）の実環境での検証
・広域・公衆化（幼稚園内→街など）に伴う 技術課題（RFIDプライバシ保護技術、追跡能力、スケーラビリティ）の解決
・プラットフォーム要件の明確化



ユビキタスネット社会のプラットフォーム要件を明確化するためにも、いくつかのアプリケーションに適用するアクティビティを推進

4．1　電子利用権技術の背景

現状認識　　電子チケット流通

・改ざんや複製を防止する機能を付加することで、物理的に流通しているチケット（コンサートチケットや電車定期券など）が電子的に安全に流通可能
・電子チケットを保有する人が権利を行使

将来像　　**権利流通**

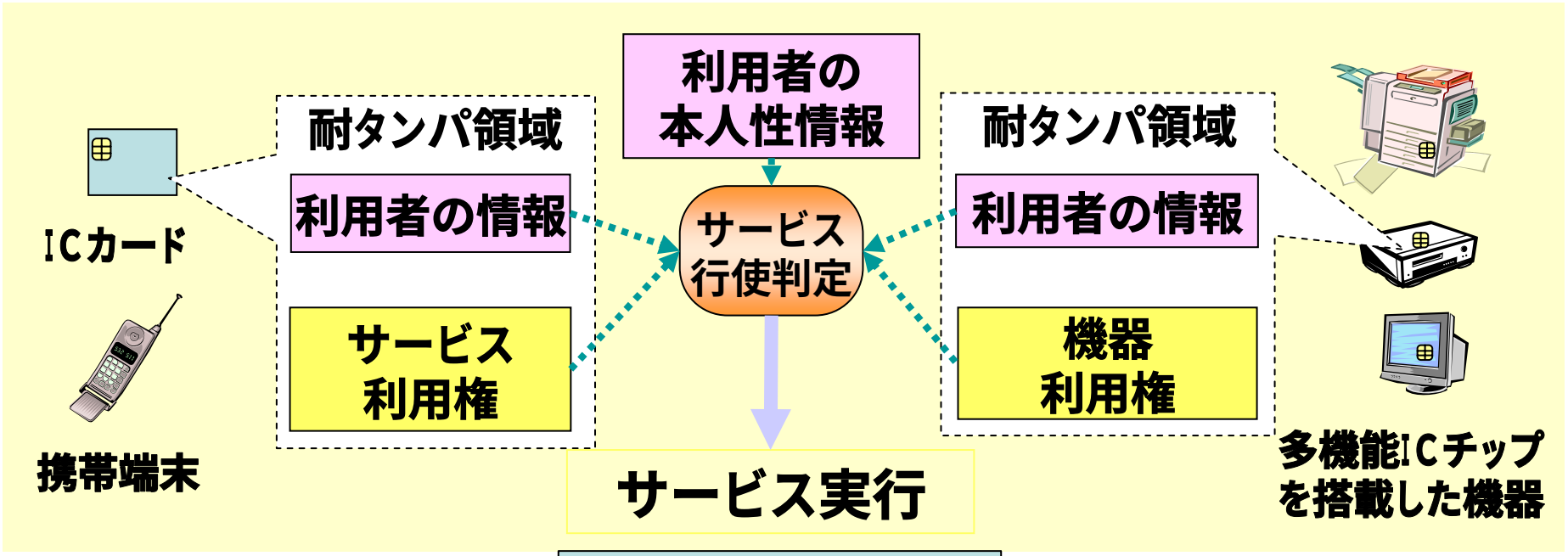
・改ざんや複製を防止する機能に加え、本人性や属性によって権利行使の制御が付加され、権利保有者の権利行使を保障
・異なるポリシーを持つ複数の主体間の合意条件変更に動的に追従
・インターネット上の権利流通では**利用権**の取り扱いが極めて重要
ディジタルコンテンツ、会員権、リモートメンテナンス、学校施設の利用管理などを統合的に扱う**利用権管理フレームワーク**が必要

技術課題（安心・安全に向けた問題認識）

・第三者が電子チケットを入手すると悪用可能

4．2　電子利用権のサービスイメージ

必要な**利用権（サービス利用権、機器利用権）、本人性確認**によりサービスを享受



適用サービス例

コンテンツ利用権流通サービス　　**リモートメンテナンスサービス**

公共施設（学校）アクセス管理サービス

4．3　電子利用権技術の特徴

異なるポリシーを持つ複数の主体間の合意条件の変更に動的に追従できるアクセス管理方式

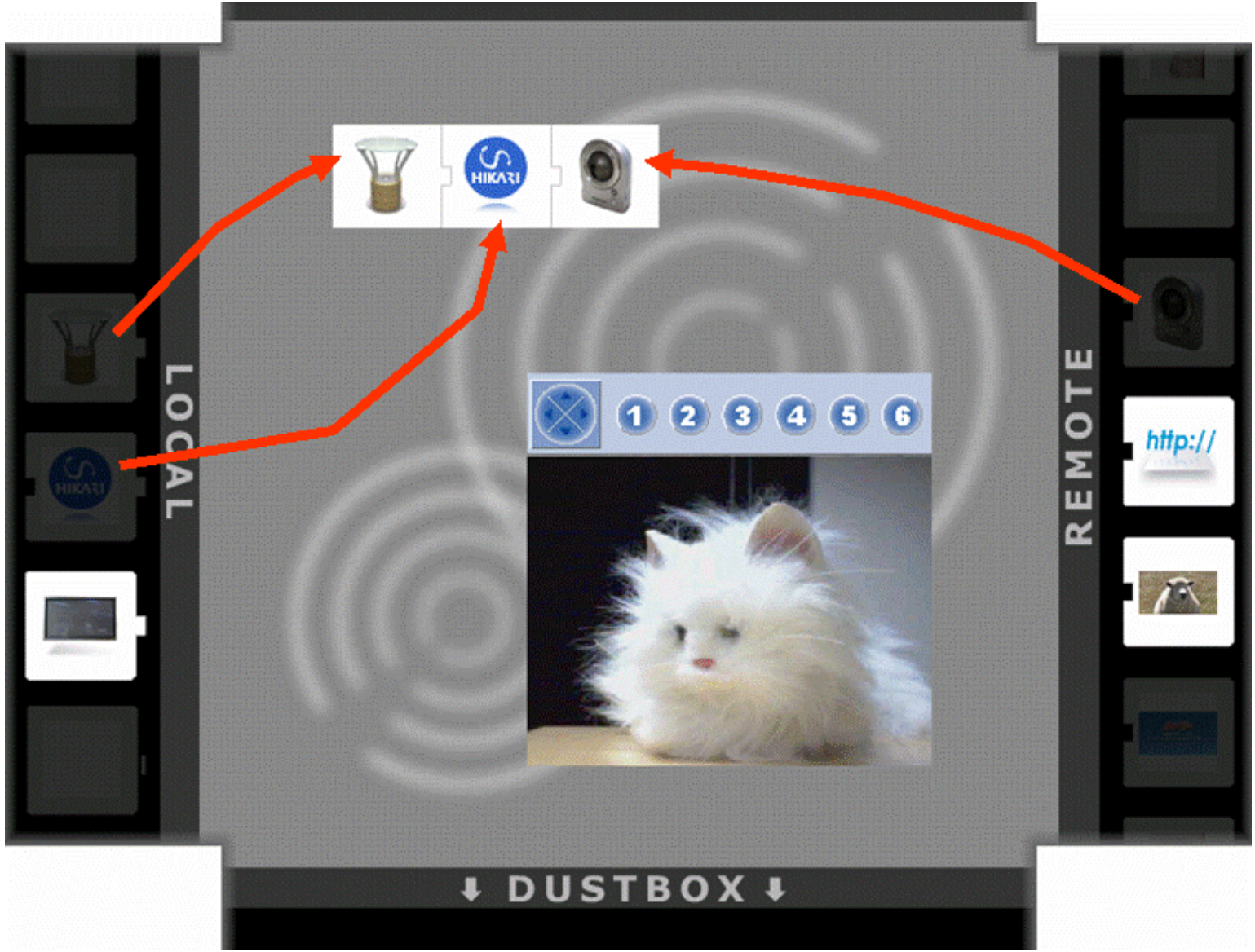
- 適用対象例：リモートメンテナンス
  - 保守者は、オフィス機器メーカと保守用APの利用に関して合意を取得し、かつ、顧客とメンテナンスのための被保守機器の利用に関して合意を取得する必要がある。

- リモートでかつ、それぞれの主体間の合意条件の変更に動的に追従できるアクセス管理方式が必要　→　利用権管理技術
  - 人、機器、アプリケーションの相互認証による信頼基盤
  - サービス単位に独立した合意条件記述
  - 上記信頼基盤の上で複数の合意条件判定結果の組み合わせよる機器アクセス

リモートメンテナンスの例

4．4　電子利用権システム(1)

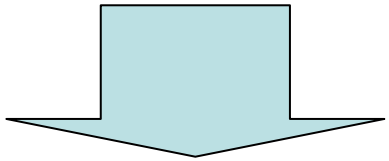
4．4　電子利用権システム(2)



4．5　プラットフォーム化に向けた今後の課題

電子利用権プラットフォームの課題

・いくつかのアプリケーションを想定して技術開発を進めているが、未だビジネス化が不明。権利流通の発展にはキラーアプリケーションが必要。
・本人性認証のための個人情報の利用に対する社会受容性を検証。



アプリケーション需要喚起、プラットフォーム機能の検証を目的として、いくつかのアプリケーションに適用するアクティビティを推進

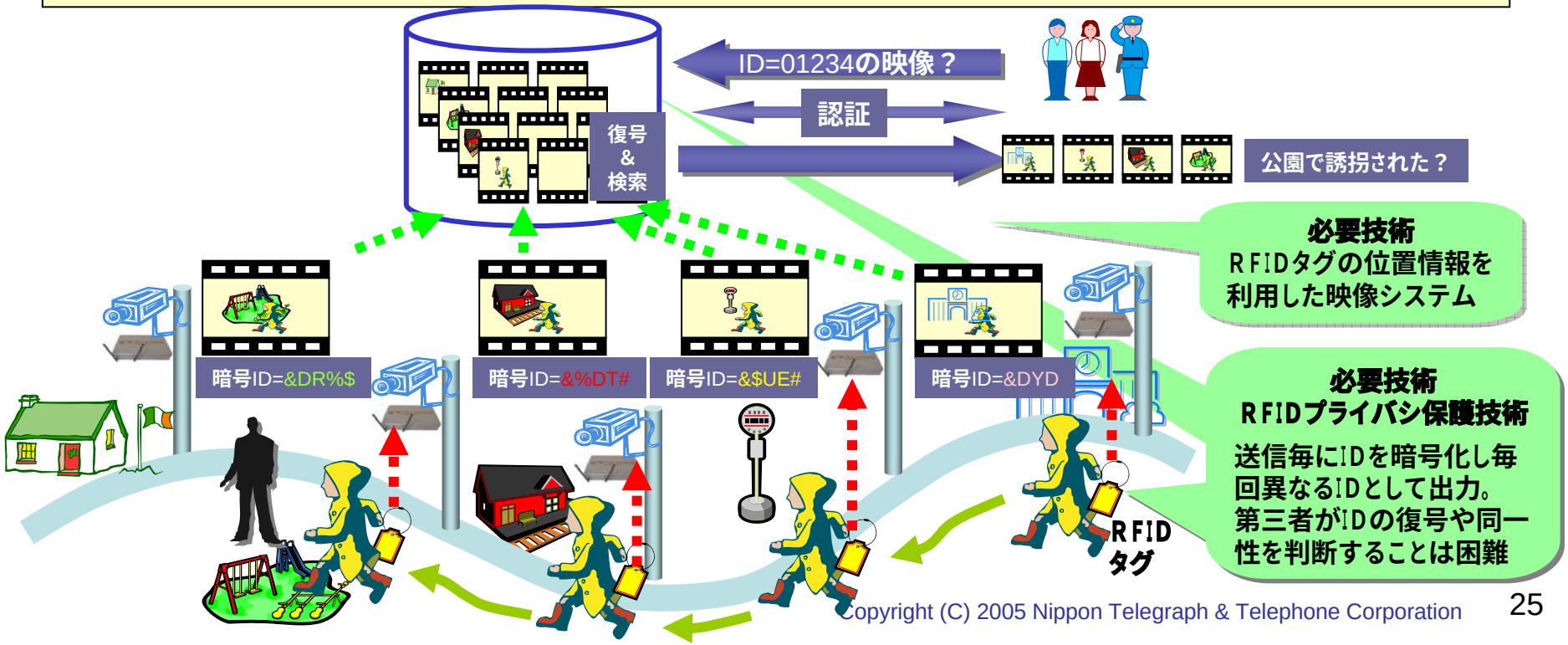
5．1　実験事例提案

- ユビキタスネット社会のプラットフォーム要件を明確化するために、応用事例をプロモートするアクティビティが必要
- 有効なアクティビティとして、学校などの公共施設の安心･安全に関わるタイムリな社会問題を捉え、実証実験による社会受容性、安心･安全なプラットフォームの検証
  - 通学路への適用実験
  - 学校の出入り管理への適用実験

但し、実験前に社会受容性、即ち実験の是非を議論する必要がある

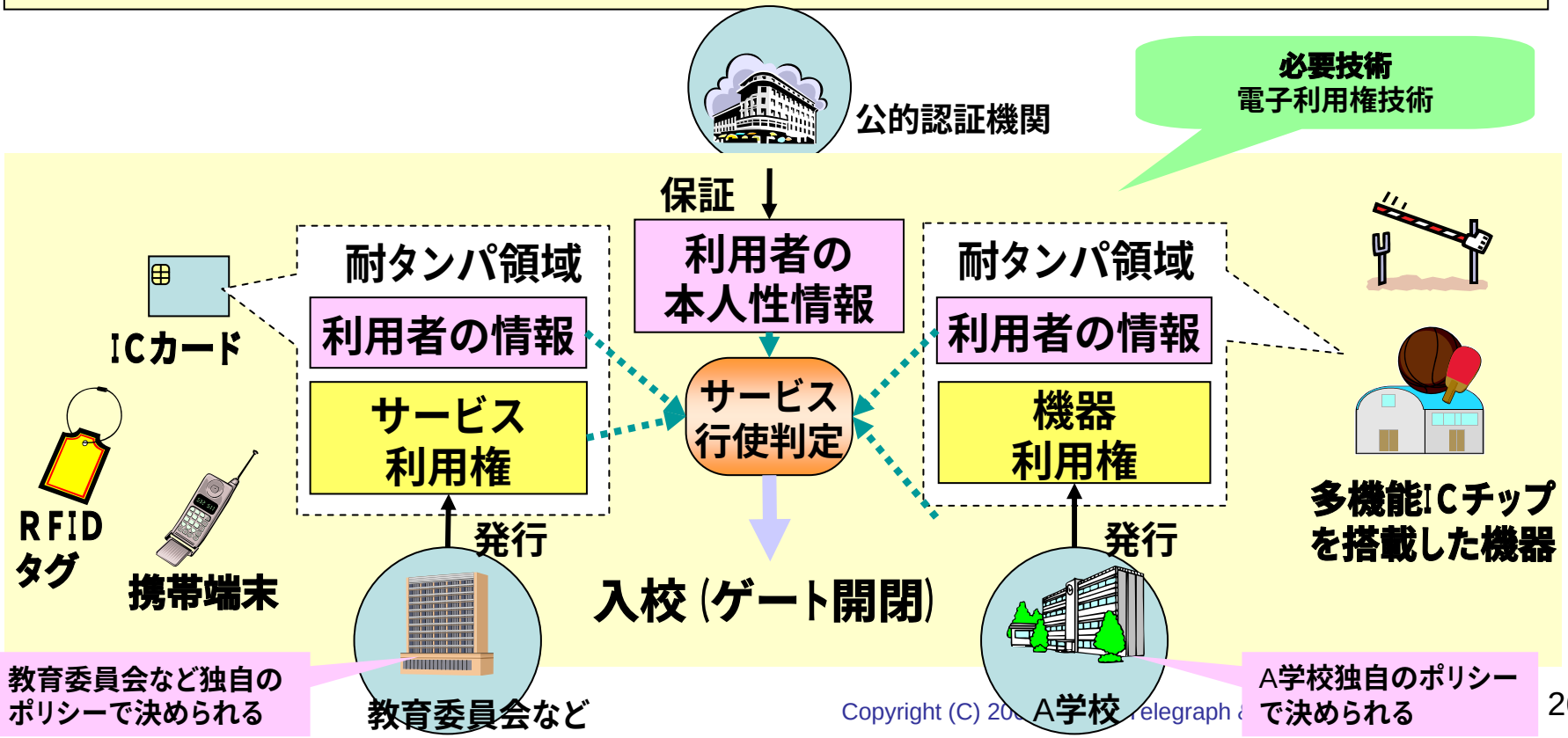
5．2　実証実験例（RFID関連技術の学校への適用例）

【目的】　児童の誘拐犯罪などの社会問題に対して、有事の際などに個人の行動履歴を確認
【実験イメージ】
・街中に監視カメラとアクティブタグリーダを配置し、子供はアクティブタグを所持
・子供が監視カメラの近くを通ると、監視カメラは映像データと（そのメタデータとして）IDを合わせて蓄積
・有事の際には家族や裁判所など妥当性が認められる開示要請に基づきIDをキーとして効率的に履歴映像を検索し追跡
【実証内容】
・社会受容性（サービス、プライバシへの懸念、倫理上の課題など）の検証
・技術的実効性（追跡能力、プライバシ保護技術のスケーラビリティなど）の検証
注：実験とはいえ、プライバシ問題など社会問題の可能性を考慮し、実証実験そのものの実施是非を事前に十分検討する必要がある



5．3　電子利用権の実証実験例（学校への適用例）

【目的】　学校への不審者の侵入などの社会問題に対して、不審者の侵入を回避
【実験イメージ】
・学校に入校したい人（生徒や業者や父兄など）は、インターネットなどを通して「サービス利用権」を取得
・学校は、安全に関する条件などを「機器利用権」として学校のゲートに設定
・学校のゲートは、本人性情報とサービス利用権/機器利用権の複数の合意条件が一致した場合開閉
【実証内容】
・利用者の本人性を保証するための個人情報の適用検証
・社会受容性（サービス、プライバシへの懸念など）の検証



(参考) IDコマース基盤

課題

ユビキタスネットワーク社会の到来により、生活者や企業が利便性の高いサービスが享受できるが、現状のままでは、様々なシステム間や機器間の連携に問題が生じて、利便性の高いユビキタスサービスが提供できなくなる怖れがある

1. **機器間連携とセキュリティの課題**
   ITシステムと外部（ユーザー、モノなど）との接点が増加・多様化し、セキュリティ面でのリスクが増大
2. **ID連携の課題**
   企業や業界が違うと、同じモノに対して異なるID情報を付与している場合があるため、個別のシステムごとに、ID情報を相互に流通させるシステムを構築しなければならない
3. **システム連携の課題**
   現状では、既存の業務システムとID情報システム間の連携が進んでいないため、サービス提供に限界がある

解決方法

「IDコマース基盤」で解決

モノや人に付されたIDをキーにして、情報の安全な流通を総合的に管理し、多くのITシステムや機器を連携することで様々なユビキタスサービスの提供を実現する

(参考) IDコマース基盤の構成

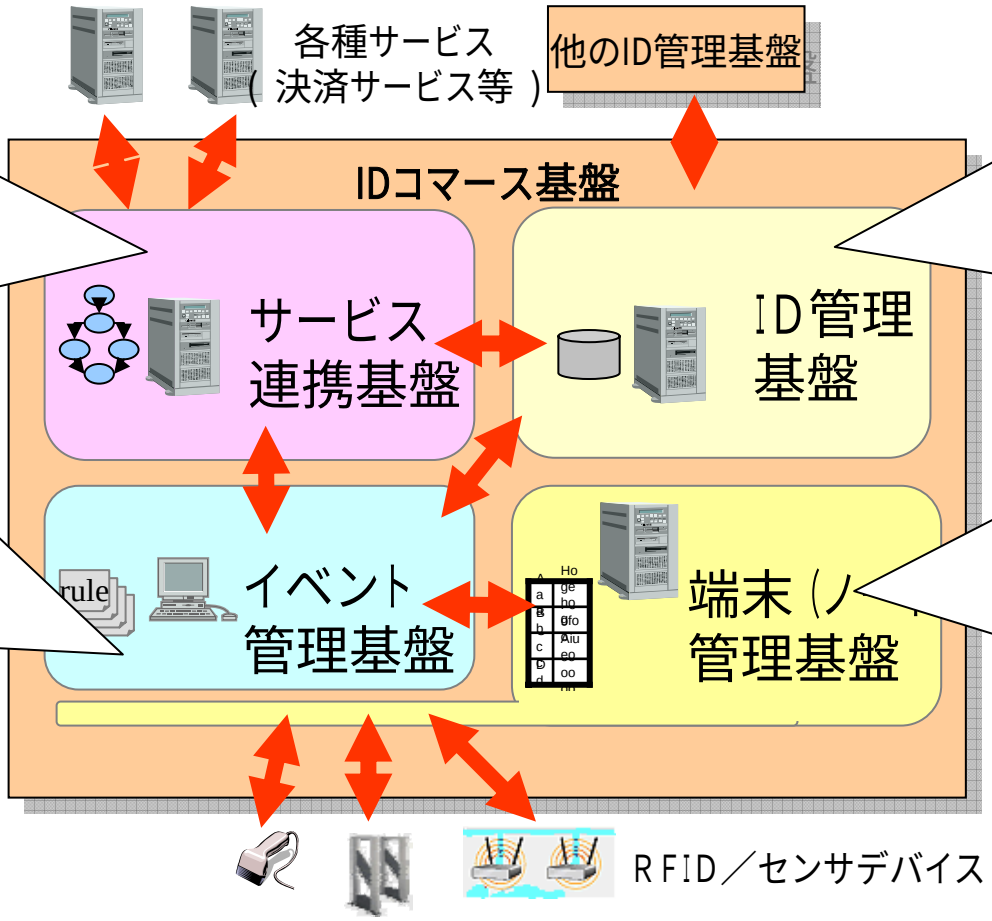
サービス連携、ID管理、イベント管理、端末(ノード)管理の4つの基盤から構成

システム連携の課題を解決

業務アプリケーションと既存システムとの連携を通じて、サービス統合を実現する
サービス連携基盤

機器間連携の課題を解決

モノの状態や情報、状況に基づく処理をIDと共にイベントとして集約、依頼などを実現する
イベント管理基盤



ID連携の課題を解決

IDに紐付く情報の保存や登録を管理し、異なるID情報の相互連携を実現する
ID管理基盤

機器間連携とセキュリティの課題を解決

RFID端末やセンサ端末の認証、登録を通じて、端末間のセキュアな接続を実現する
端末(ノード)管理基盤