ユビキタス・サービスとITS

ーセキュリティとリスク対策の課題ー

平成18年2月28日

株式会社NTTデータ
技術開発本部　副本部長

工学博士　山本修一郎

本日のアジェンダ

- ユビキタス･サービスとITS
- ユビキタス･サービスの事例
  - 歩行者･道路から車両へ
  - 車両から道路へ
- セキュリティとリスク対策の課題
- まとめ

1　ユビキタス・サービスとITS

ITSサービスとユビキタス・サービスのセキュリティ

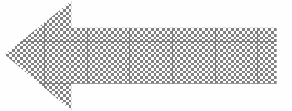
- 道路・歩行者の状況をリアルタイムに監視
- モノと情報の流れを追跡管理

- 交通状況をリアルタイムに監視
- 自動車の流れを追跡管理
- 通行料金・駐車場料金支払い

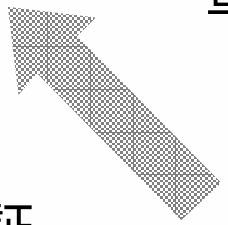
ユビキタス・サービス

ITSサービス

- 車両から道路・歩行者への情報提供



- 歩行者・道路から車両への情報提供



- 歩行者の認証
- 読取装置の認証
- 個人情報保護

- ETCタグの認証
- 車載装置の認証
- 個人情報保護

セキュリティ

2 歩行者・道路から車両へ

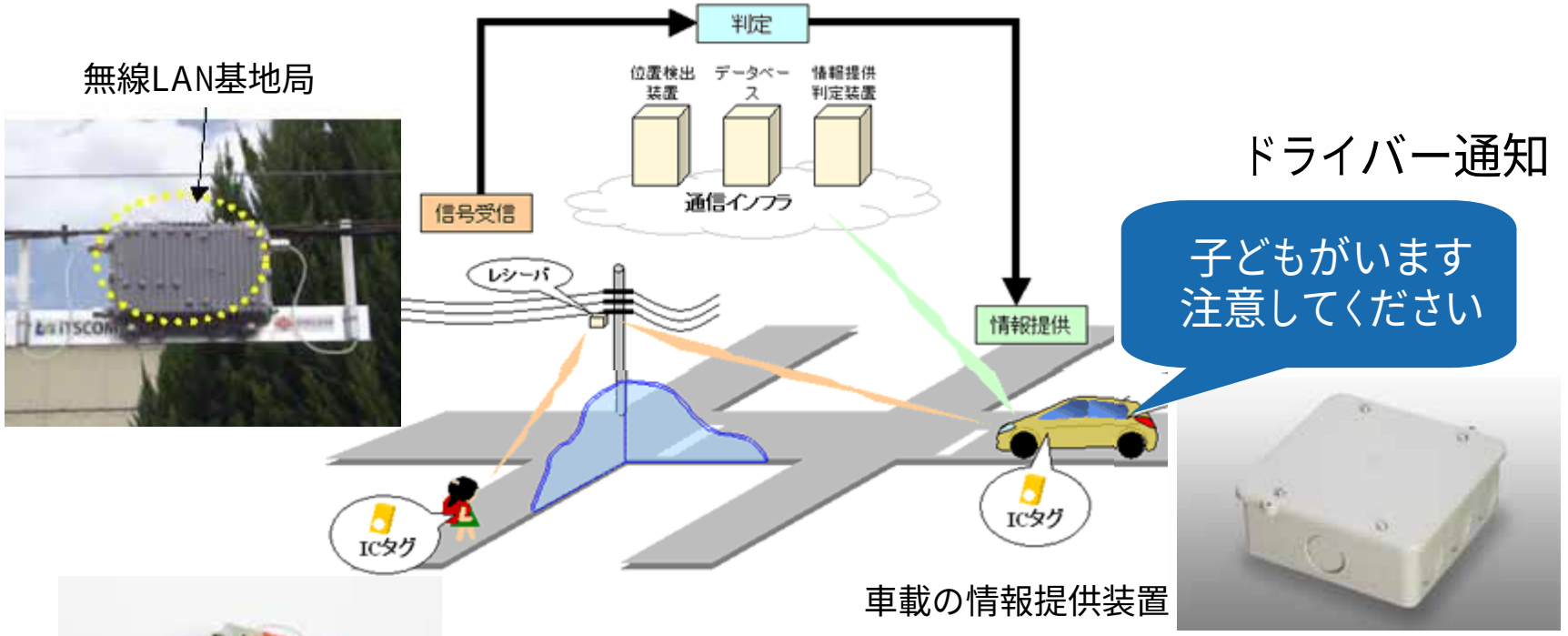
『アイセイフティ®子供見守りサービス』実験結果と今後の課題

分類		説明
実験の結果	登下校通知	■外出の多い保護者から好評
	居場所通知	■積極的な利用は少ない
	個人情報	■個人情報に関する心配は限定
今後の課題	コストの低廉化	■誰がどのコストを負担するのか ■警備員の配備も含めたサービスであれば、月額2,000 円以上でもよい ■自治体と住民との分担による負担など、複合的な形態の検討が必要
	エリア拡大とサービスの拡充	■到達距離が約30 メートルでは、通学路の多くはカバーし切れなかった ■より少ないコストでカバーエリアを拡大する技術の導入と設備コスト自体の低減が大きな課題 ■不審者情報等の情報配信を望む声も多く、自治体サービスとの連携が重要
	誤報の防止	■誤報発生件数は、53 件 ■無意識の誤報「鉄棒で遊んでいるとき」、「ランドセルの下敷きになった」 ■駆けつけ支援者の意欲低下 ■長押しするタイプのタグへの変更

(参考) http://www.tokyu-security.co.jp/kj/press_imgs/20050930_1.pdf

子ども存在情報 ドライバー通知サービス

アイセイフティ®「交通安全サービス」実験について
～子どもの存在をドライバーに知らせ、交通事故低減を目指す実験を開始～



ICタグとお守り袋

車載の情報提供装置

実施期間：2005年12月から2006年3月末(予定)

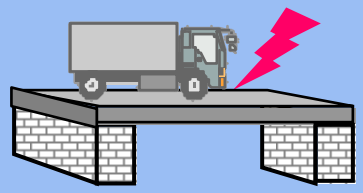
・NTTデータ：全体のコーディネートおよびシステムの開発
・日産自動車：交通安全サービスの検証
・イッツ・コミュニケーションズ：無線LAN基地局を含むネットワークインフラの提供
・トレンディ：システムの開発および実験期間中のシステム運用
・東急セキュリティ：警備サービス(地域内巡回と駆けつけ支援)の提供

3　車両から道路へ

日本の橋の現状

【橋梁の現状】
- 全橋梁の４０％が高度成長期に建設されている
- 日々のダメージが設計当時の想定を上回っている

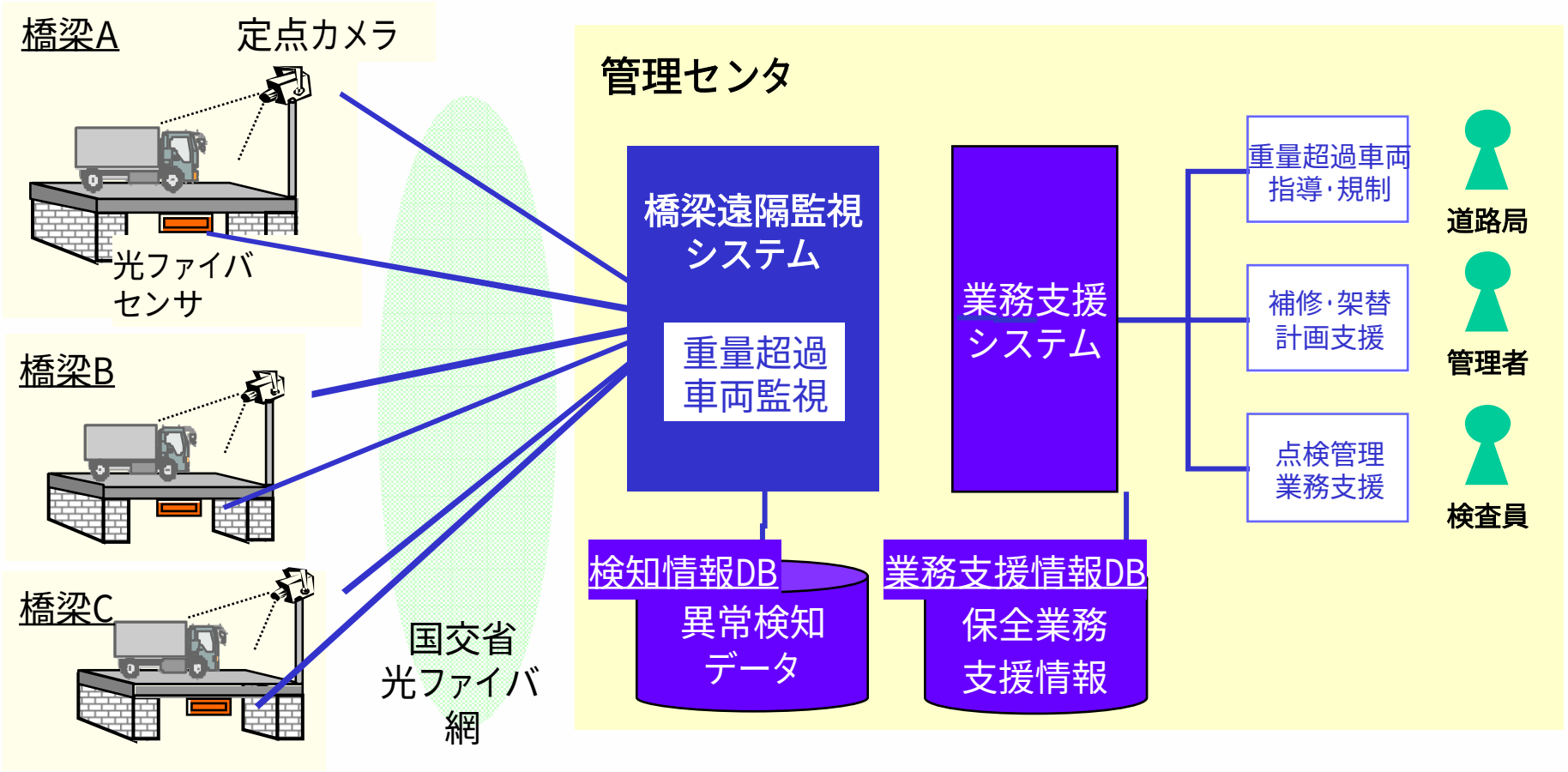
今後20年間に
橋梁の同時大量老朽化が進行



【ダメージの原因】
- 走行車両数の１％未満でしかない
  超重量車両(20トン以上) が主要な原因

NTTデータの取組：橋梁遠隔監視システム

・光ファイバセンサおよび監視映像の情報を統合した多角的モニタリングの実現
・規制や点検の対象を的確に選定するための業務支援情報を提供



3　セキュリティとリスク

ITS社会におけるセキュリティ問題

分類	問題	例
プライバシー	所持している商品に装着されたID情報から漏洩する	Aさんが車に入れているモノが何かアンテナをかざすと分かってしまう
	IDの追跡による行動追跡や本人特定される	Bさんの車に付いているIDや車の中にある所持品のIDを追跡することで、行動履歴が取得され、その結果本人特定される
セキュリティ	ID情報やメタ情報が改ざんされる	車のイモビライザーやタグのIDを別のIDに変更されてしまう
	ITSに紐付く情報が盗聴、改ざんされる	プレーヤAが設定したITS情報をプレーヤBが勝手に参照したり、変更してしまう
	RFIDが不正にコピーされる	車に偽造IDをつけて本物として流通する

米国のETC

ETCの例	概要	参考
E-ZPASS (NYState Thruway system)	フロントガラスのルームミラーに近いところに置いたカセットテープ大の「タグ」に口座情報を記録。料金所のE-ZPass Only車線を通過すると、タグの暗証が読み取られて、E-ZPass口座から通行料を自動引き落とし。東海岸8州の有料道路、橋で共通利用。空港の駐車料金の支払い。	http://www.e-zpassny.com/ http://www.driveanzen.com/
FAST LANE (Massachusetts Turnpike Authority)	E-Zpassが使えるところではFAST LANEも使える。	http://www.massturnpike.com/travel/fastlane/index.html
FasTrak	カリフォルニア州の橋の通行料を徴収。交通情報を収集しHPで公開 。	http://www.bayareafastrak.org/ http://www.511.org/fastrak/ http://traffic.511.org/

- 個人情報保護
- タグの盗難

クラッキング・システムの構成

RSAのAri Juels とJohns Hopkins大学、http://rfidanalysis.org/

構成	概要	例
スキミング	RFIDリーダでDSTタグの情報を読む	SpeedPass イモビライザ
キークラッキング	データをキークラッカーと呼ぶ特殊な装置でDSTの暗号キーを復元する。	１６台並列のFGPAで５個のDSTキーを２時間で解読 経費3500ドル
シミュレーション	DSTから復元された暗号キーを持つハードウェア装置でDSTを模倣	自動車に給油する 自動車のエンジンをかける

DST:Digital Signature Transponder,40 bit長の暗号キー

FGPA：field programmable gate array

電子タグに関するプライバシー保護ガイドライン

	ガイドライン	ポイント
1	目的	タグの有用性と消費者の利益･プライバシー保護の共通事項
2	対象範囲	電子タグ装着物品手交後に事業者が対応する規則
3	電子タグが装着されていることの表示等	装着の事実･装着箇所･の性質･情報
4	電子タグの読み取りに関する消費者の最終的な選択権の留保	電子タグ読み取りができないようにする方法について 説明･掲示･表示
5	電子タグの社会的利益等に関する情報提供	読み取りできないようにした場合、消費者利益･社会的利益が損失することについて、表示･情報提供
6	電子計算機に保存された個人情報データベース等と電子タグの情報を連係して用いる場合における取扱い	電子タグに記録された情報を用いて個人を識別できるときは、個人情報保護法としての取り扱いを受ける
7	電子タグ内に個人情報を記録する場合における情報収集及び利用の制限	利用目的の本人通知･公表 目的外利用する場合の本人同意
8	電子タグ内に個人情報を記録する場合における情報の正確性の確保	正確･最新の内容、電子タグから紐付けされる個人情報を消費者に開示･訂正、情報の消失･き損･改竄･漏えいの防止
9	情報管理者の設置	プライバシー保護情報の適正管理･苦情処理、連絡先の公表
10	消費者に対する説明及び情報提供	消費者が意思決定できるように、電子タグの理解を助ける

総務省･経済産業省：http://www.soumu.go.jp/s-news/2004/pdf/040608_4_b.pdf

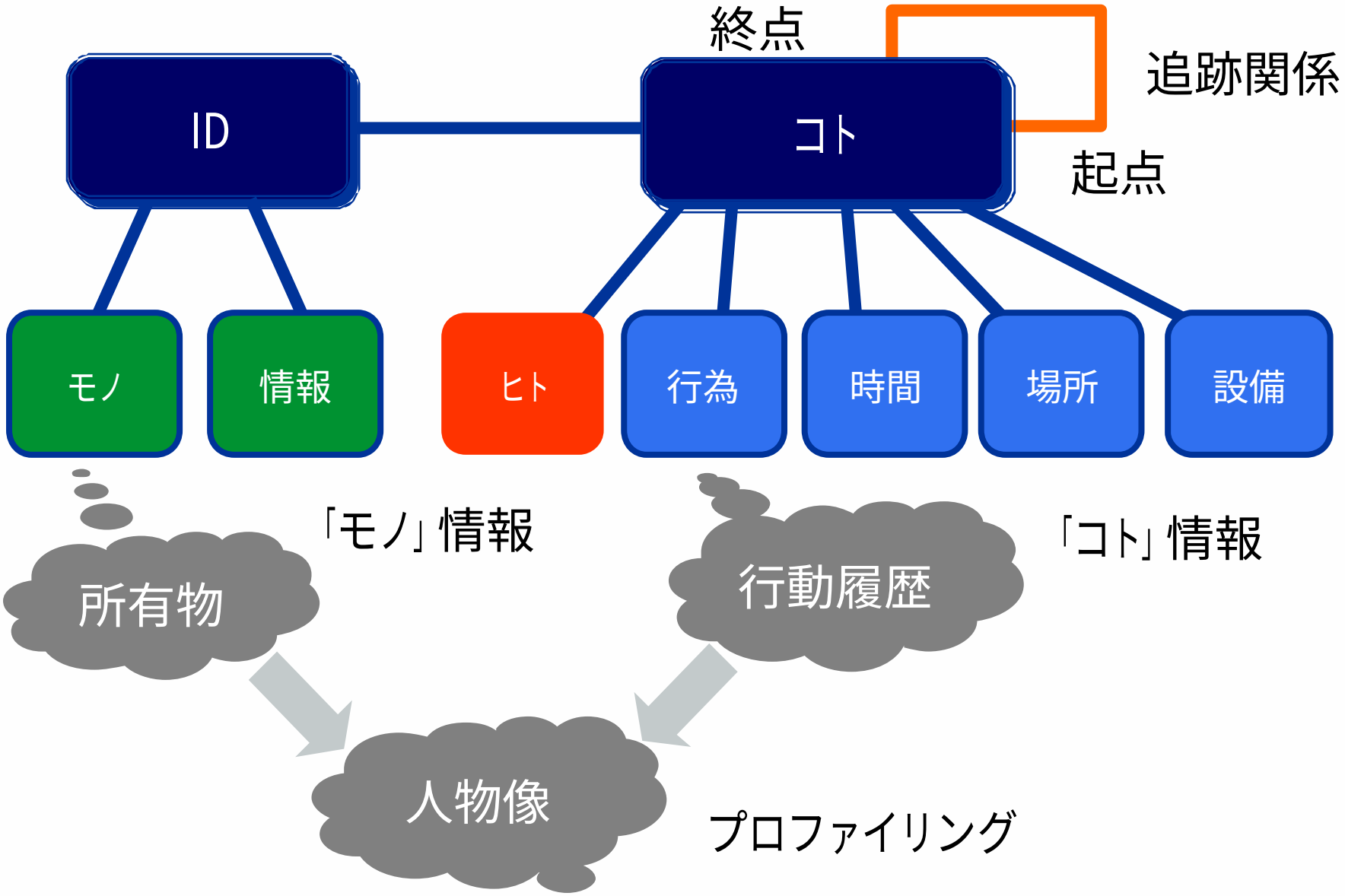
RFIDのプライバシ保護技術

方法	説明	問題点
Kill Tag	消費者への手交前にKillコマンドでタグ読取を禁止	販売後の商品情報入手が不可
Hash-lock	RFIDに鍵をかけることで情報を保護する メタID：yでロックし、ハッシュ関数y=h(x)となる鍵xを保存しておき必要なときにアンロックする	暗号処理のためのコスト増大 膨大な(x,y)の組を管理することになる リーダがハッシュ関数を認識できる
Re-Encryption	プライバシ強化装置を用いてID番号を暗号化してRFIDに書き込む	コスト増大と外部装置での暗号化による煩雑さ
Silent Tree Walking	RFIDからID情報を盗聴できないよう暗号化する	暗号処理のためのコスト増大
Blocker Tag	RFID内のID番号以外の擬似IDを発信し、正当な権限のないリーダにタグを読み取らせない	特殊なリーダのコストが大きい
Faraday cage	金属性の籠やホイルで覆い無線信号を遮断する	商品を包み込む形になるため用途限定
Active Jamming	RFIDリーダに対して妨害電波を発信する	近接するRFIDシステムへの障害
Soft Blocking	RFIDのモードを、リーダ側から変更することで、局面ごとにタグが発信する情報を変化させる	特殊なリーダのコストが大きい
DB Access Control	蓄積されたRFIDデータのDBへのアクセス制御	正規利用者による不正への対策が困難
DB Access Log Audit	RFIDデータのDBに対するアクセスログを監査し、正当な利用者の不正に対応する	不正への即時対応などが困難

参考：A. Juels, R. L. Rivest, and M. Szydlo. The Blocker Tag: Selective Blocking of RFID Tags for Consumer Privacy. In *Computer and Communications Security*, pages 103–111. ACM Press, 2003.

4　まとめ

IDで「モノの流れ」と「情報の流れ」を一致



ユビキタス・サービスが生み出す3つの価値

価値		説明	事例
協働化	モノ の協働化	モノがネットワークで直接通信することで人間が意識することなく新たな利便性を提供	車々間通信、ETC、 歩行者・道路・車両相互通信
	分散資源の協働化	分散資源（IT資源、知識、頭脳、労働力等）をネットワークを活用して協働させ、大きな資源やひとつのサービスとして活用	駆けつけサービス 交通・天候情報提供
可視化	トラッキング	対象物をネットワークを活用して位置・状態を追跡管理することで、安全、安心、効率などの価値を提供	コンテナ追跡、通過監視 移動監視、危険災害検知
	センシング	センサーによって採取したデータをネットワークを介して活用することで省力化したり、不確実性を低減	物流時の温度管理・衝撃管理、 交通監視、車両状況監視
最適化	所有から利用へのパラダイム・シフト	有形物（モノ）に対する無形物（情報）の価値が相対的に高まることで、モノを所有することの価値が薄まり、利用へ価値の移行が促進され、効率や利便性が高まる	シェアード・カー、 共同利用型センサNW ITSインフラ相互接続
	時空の短縮	様々な場所から、いつでもネットワークに接続できるようになるため、時間・場所の制約にとらわれずにサービスを享受	遠隔情報モニタリング

「IDコマース基盤」

モノや機器のIDに基づき、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

課題	管理基盤	目的
システム連携	サービス連携基盤	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
ID連携	ID管理基盤	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
機器間連携	イベント管理基盤	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
機器認証	端末（ノード）管理基盤	ID読取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

Insight for the New Paradigm

未来のしくみを、ＩＴでつくる。

株式会社ＮＴＴデータ