2004年2月24日
大域ディペンダブル情報基盤 シンポジウム

人間・社会と調和した ディペンダブル情報セキュリティ技術

今井秀樹　松浦幹太
(東京大学
生産技術研究所)

構成

1. はじめに --- 情報セキュリティの立場から「超ディペンダブル」を目指すために
2. 三つのアプローチとその概要
   - 人間的要素
   - システム構築技術と事後解決技術
   - 社会的要素
3. まとめ

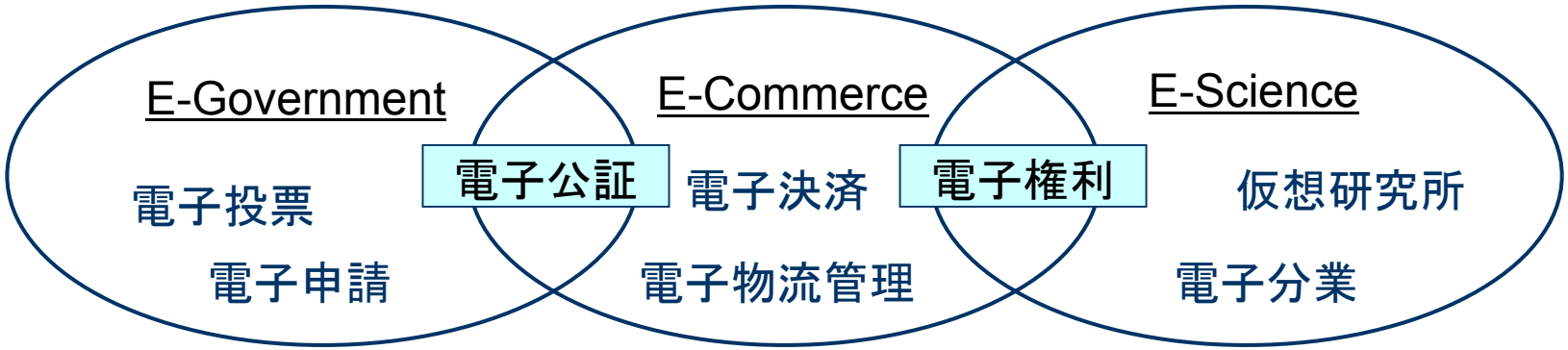
1．はじめに

はじめに --- 情報セキュリティの立場から「超ディペンダブル」を目指すために

- テーマ名：「ヒューマンクリプトに基づく超ディペンダブル暗号系」
- 概要：　人とコンピュータシステムをセキュリティの面から総合的に最適化するヒューマンクリプトの手法によって、安心感を飛躍的に高めた暗号系を構築する。人の立場から見た安全性の検証可能性を重視し、ディペンダビリティのブレークスルーを達成する。

情報セキュリティの概観と電子社会

- “E-Something”の類型



支える情報セキュリティ技術

共に支える
社会制度
（法・制度・
施策・監査・
保険など）

セキュアプロトコル　暗号インフラ　鍵管理
アクセス制御　侵入検知
耐タンパー　個人認証　暗号　電子透かし

システム技術
要素技術

ヒューマンクリプトの立場

- 狭義には、人とコンピュータやネットワークとの関わりの部分における暗号技術
- 広義には、それと密接に関連したプロトコルも含めた情報セキュリティ技術全般
- つまり、人とコンピュータネットワークを情報セキュリティの面から総合的に最適化するアプローチ

- 本研究では、社会的側面にまで拡張
- 「評価」「実証」を重視

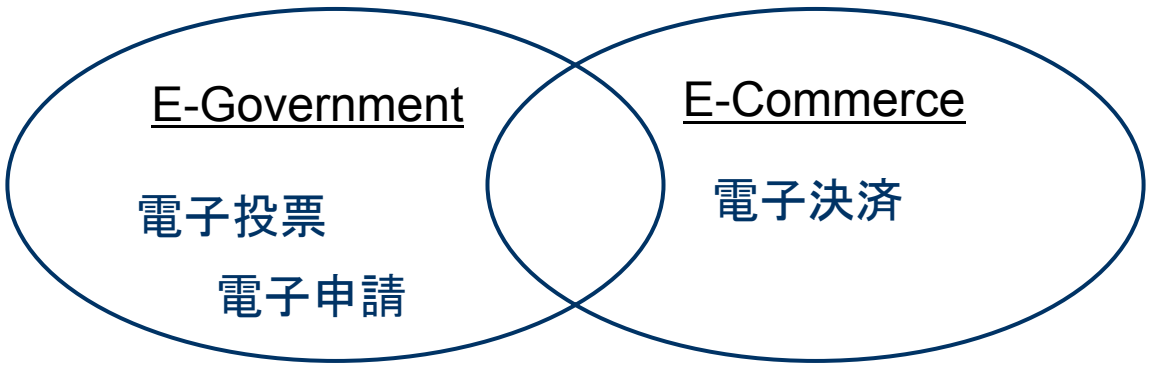
2. 三つのアプローチとその概要

三つのアプローチ（←排他的ではない）

- 人間的要素（と直接関わる技術）
  - 狭義のヒューマンクリプト
- システム構築技術と事後解決技術
  - 広義のヒューマンクリプト
- 社会的要素
  - ソーシャルクリプト

2.1 人間的要素(と直接関わる技術)

- 厳しい条件の中で安全性評価を追究
  - “Pretty Simple” and yet “Provably-Secure” PAKE(Password-Authenticated Key Exchange)
  - PAKEの発展： 限られたリソースのもとでのグループ鍵共有
- 人間的要素の積極的な利用
  - バイオメトリックスによる暗号鍵生成と更新
  - 対面取引に限定した場合の秘密鍵漏洩対策



支える情報セキュリティ技術

セキュアプロトコル　暗号インフラ　鍵管理

耐タンパー　個人認証　暗号

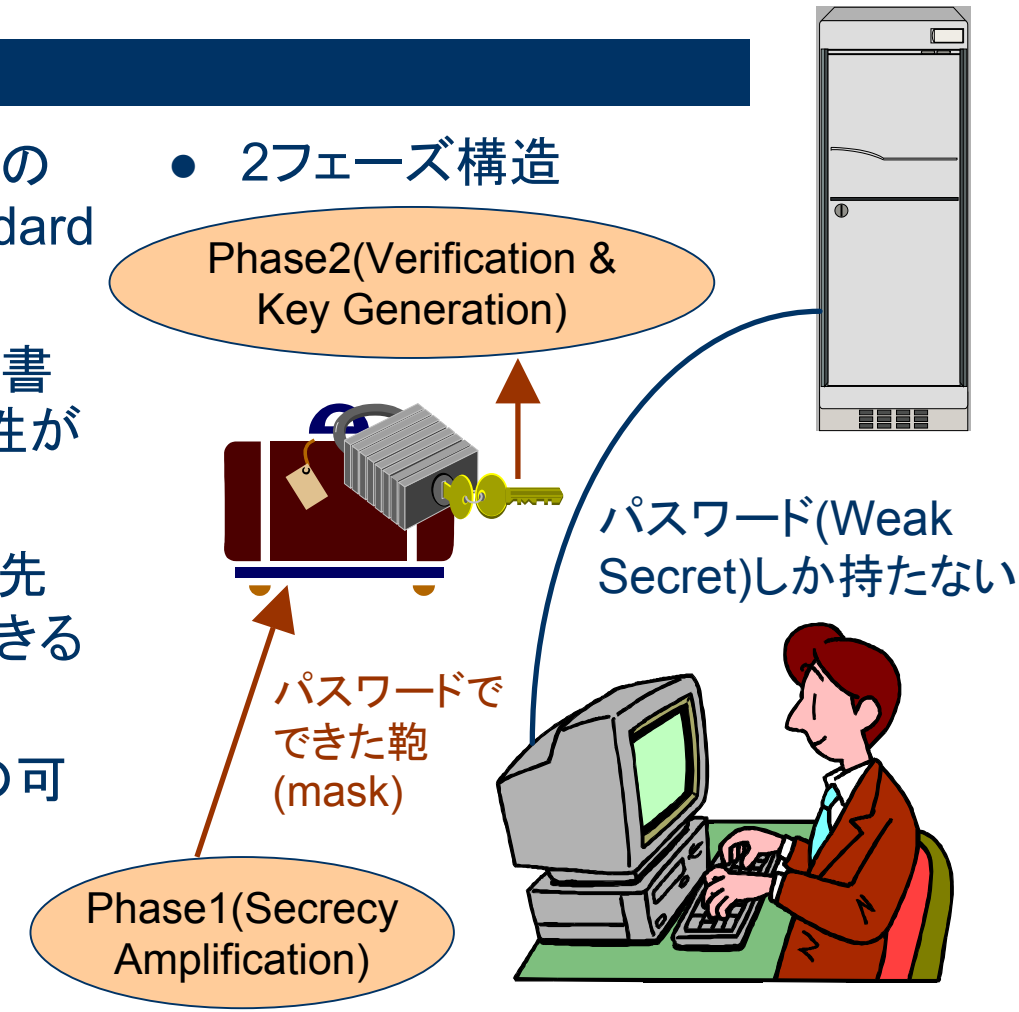
システム技術

要素技術

証明可能安全性をもつPAKEの概要

- オンラインプロトコルとしての暗号学的安全性は、Standard Modelで証明可能。
- オフラインの脅威である辞書攻撃対策のsaltingとも相性がよい。
- 公開鍵基盤がなくても、出先の計算機で暗号通信ができるようになる。
- 計算負荷も軽い（サーバの可用性などにも貢献）。

- 2フェーズ構造



A View on “PKC or PAKE?”

- 長期的な見方も含めると:

	Would survive the attacks over quantum computers	No need to hold and manage public keys	Security proof under standard model
PKC	○	×	×
PAKE	×	○	○

公開鍵基盤(PKI)

（暗号通信）受信者Bの公開鍵で暗号化して送信

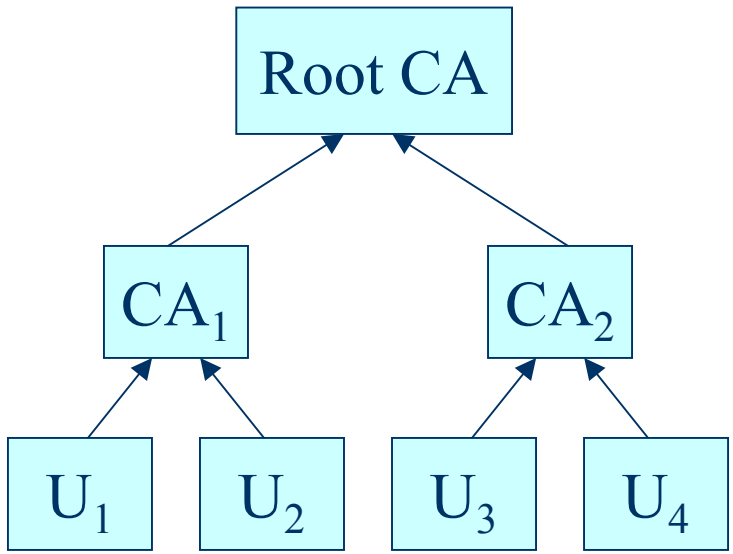
→Bは自身の秘密鍵で復号

（電子署名）署名者Bは秘密鍵を用いて認証子を生成

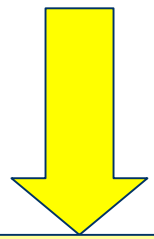
→検証者はBの公開鍵を用いて検証

- 実際には、公開鍵が確かに所望のエンティティのものであるかどうか、かつ、有効な使われ方かどうか（有効期間内かどうか等）をチェックしなければならない。

- 認証機関CAが発行するお墨付き（公開鍵証明書）とブラックリスト(CRL)でチェック。



- 秘密鍵漏洩の問題（実装バグ, 内部不正, サイドチャネル攻撃, etc）
- その無効化周知に遅延がある問題
- そもそも「いつ気づくのか」という問題

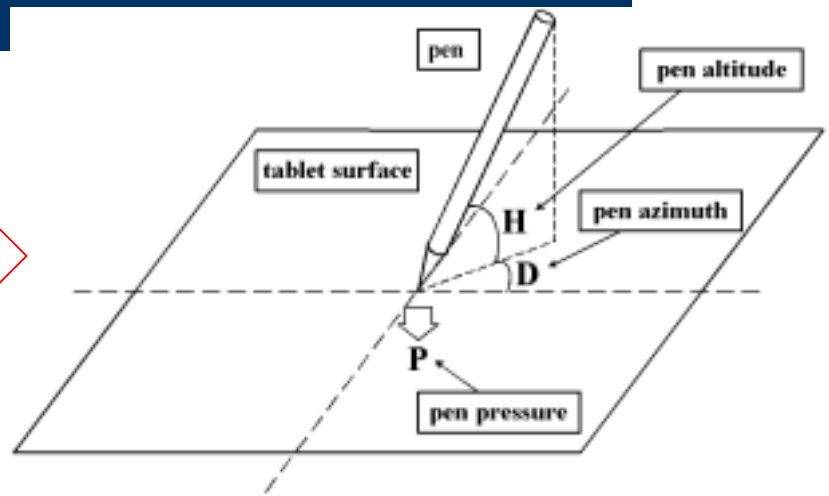


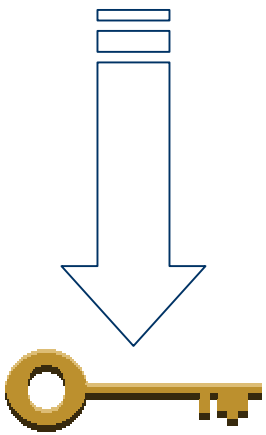
「『PKI and/or Biometrics』でよいだろう」で済むほど単純ではない

バイオメトリックスの利用

- バイオメトリクス情報を単純に秘密鍵として利用するのは，それが漏洩したときにシステム全体が脆弱になるので，好ましくない
- その代わりに，秘密鍵を所有者のバイオメトリクス情報を利用して更新する
  - 本人以外は，秘密鍵の更新が困難
  - バイオメトリクス情報が漏洩する最悪の場合でも，以前に暗号化したものが解読されることがない（Forward Security）

想定する環境





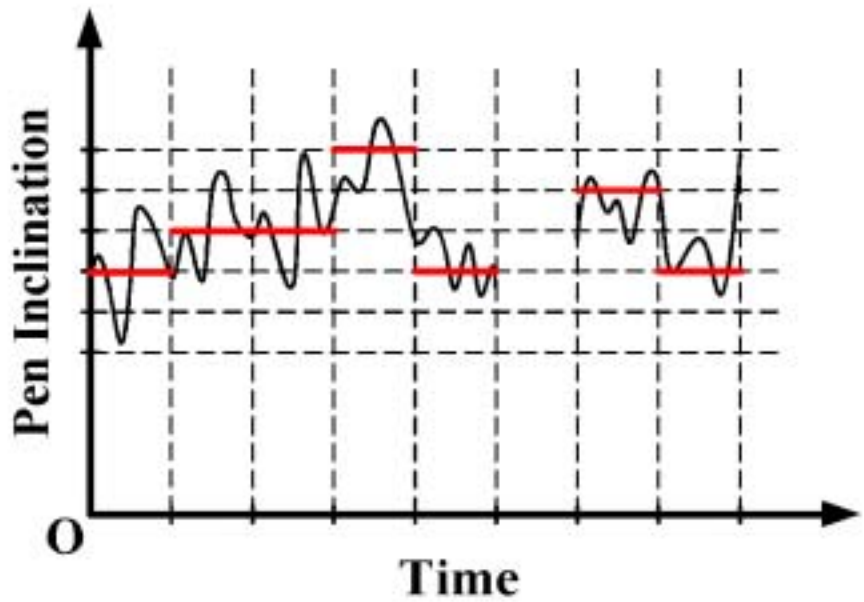
0110010101111010100010010010100001010010101101001011010010101001010101110100100101010101010111

ビット列生成過程例(傾き)

<時間軸上>
各ストローク時間を量子化
複数区間に分離

<傾き軸上>
各区間の代表値を量子化
筆圧0の区間は無視

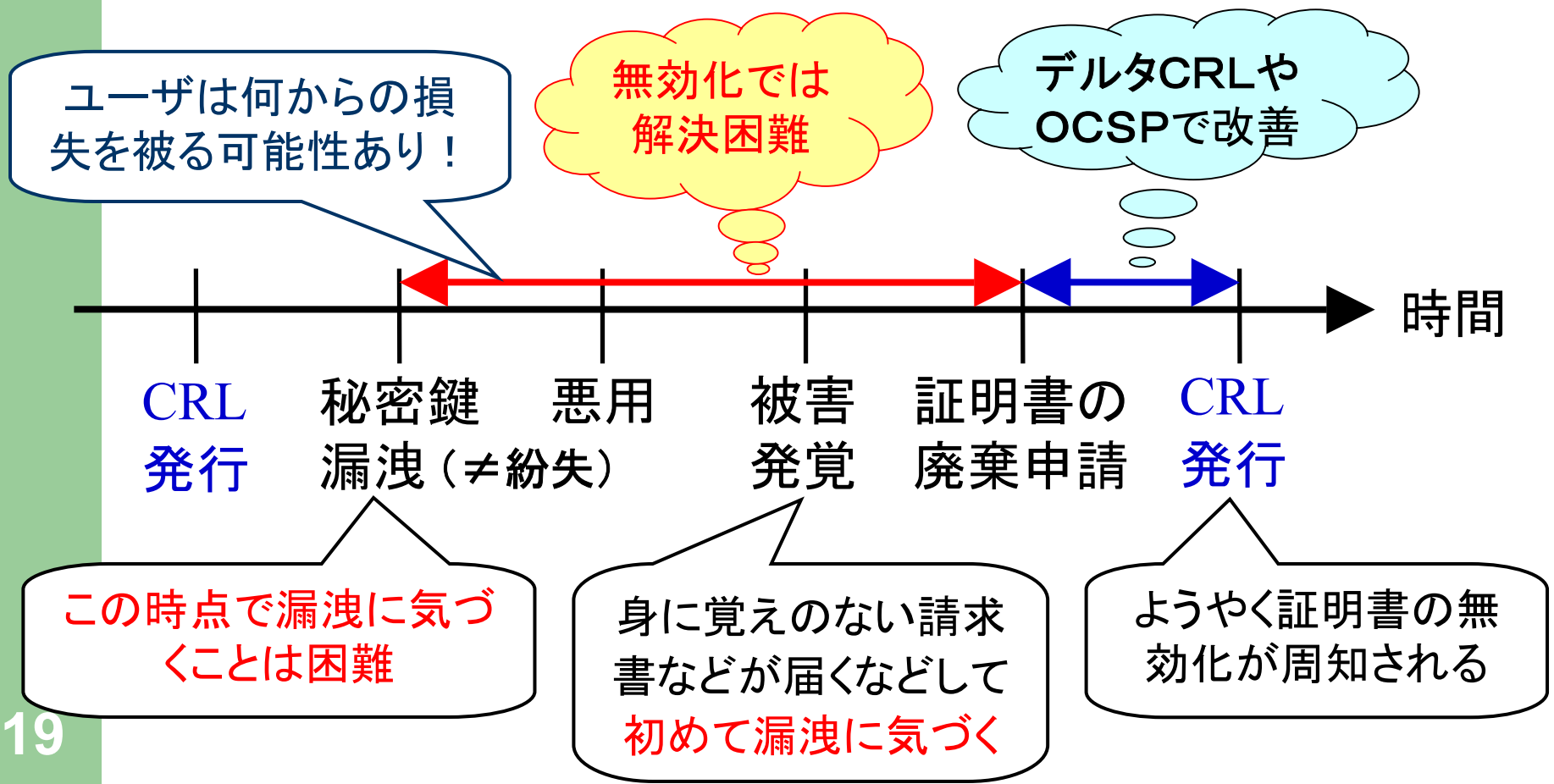
<量子化>
最近接の切りの良い値に近似



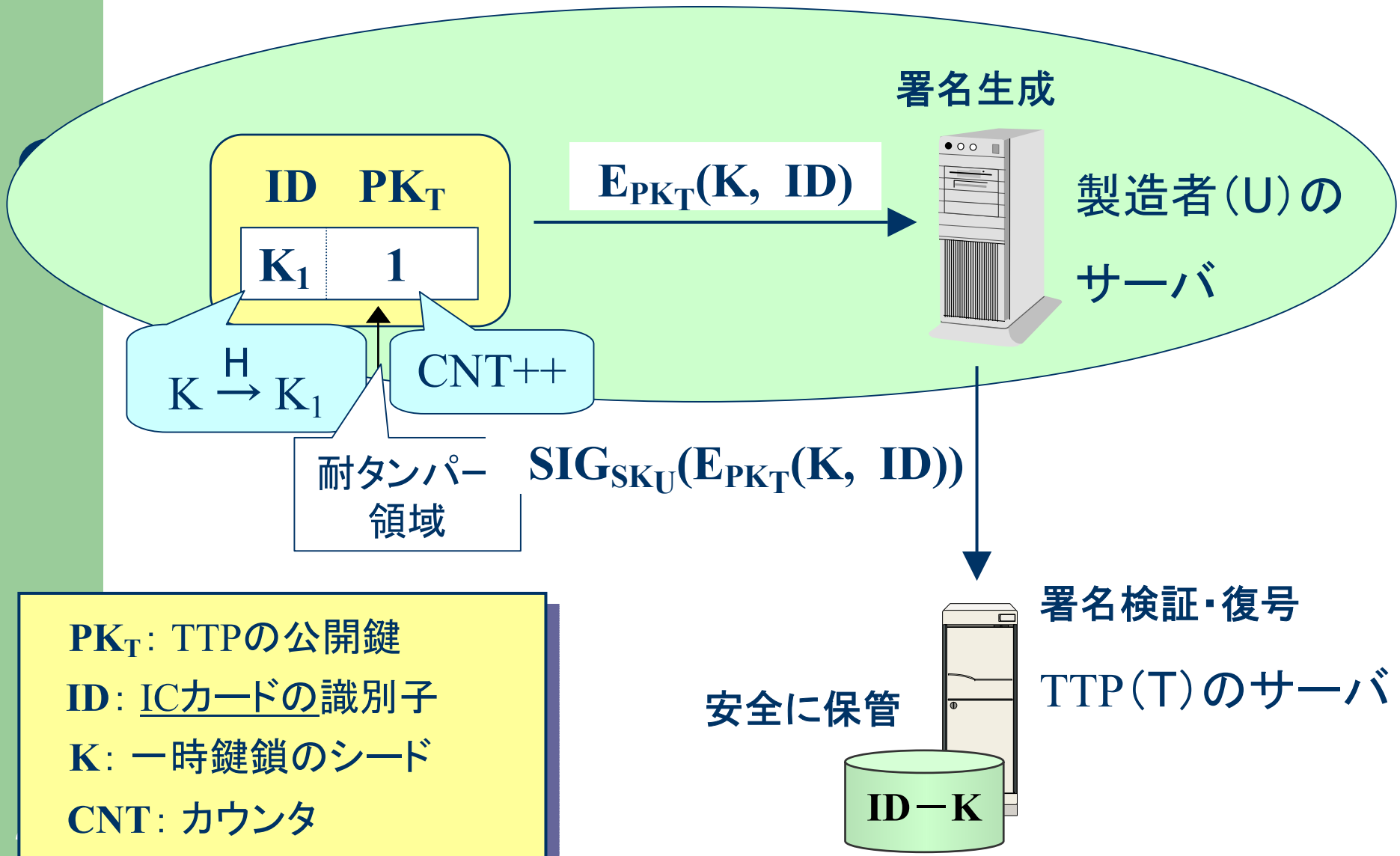
開発した方式の評価

- バイオメトリックス秘密鍵 K_{bio} が漏洩しない場合、ユーザの秘密鍵がある閾値以上漏洩しない限り、すべての暗号文が解読されることはない。
- たとえ K_{bio} が漏洩したとしても、ユーザの秘密鍵が漏洩しない間は、暗号文が解読されることはない。
- K_{bio} が漏洩し、さらにある期間(t=i)のユーザの秘密鍵が漏洩しても、それ以前の暗号文(t<i)が解読されることはない。

証明書廃棄におけるタイムラグの問題

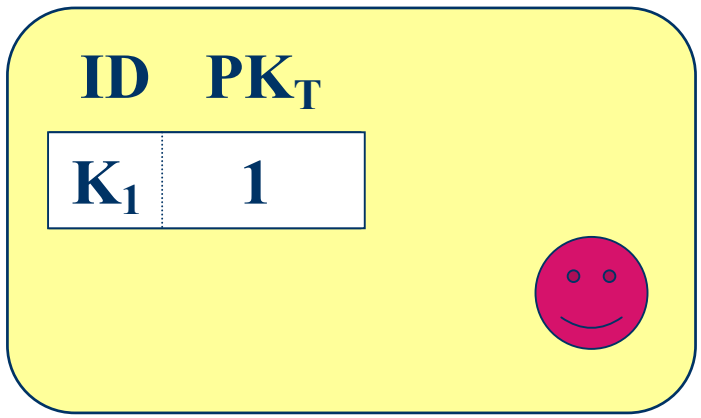


ICの製造過程



PK$_T$: TTPの公開鍵
ID: ICカードの識別子
K: 一時鍵鎖のシード
CNT: カウンタ

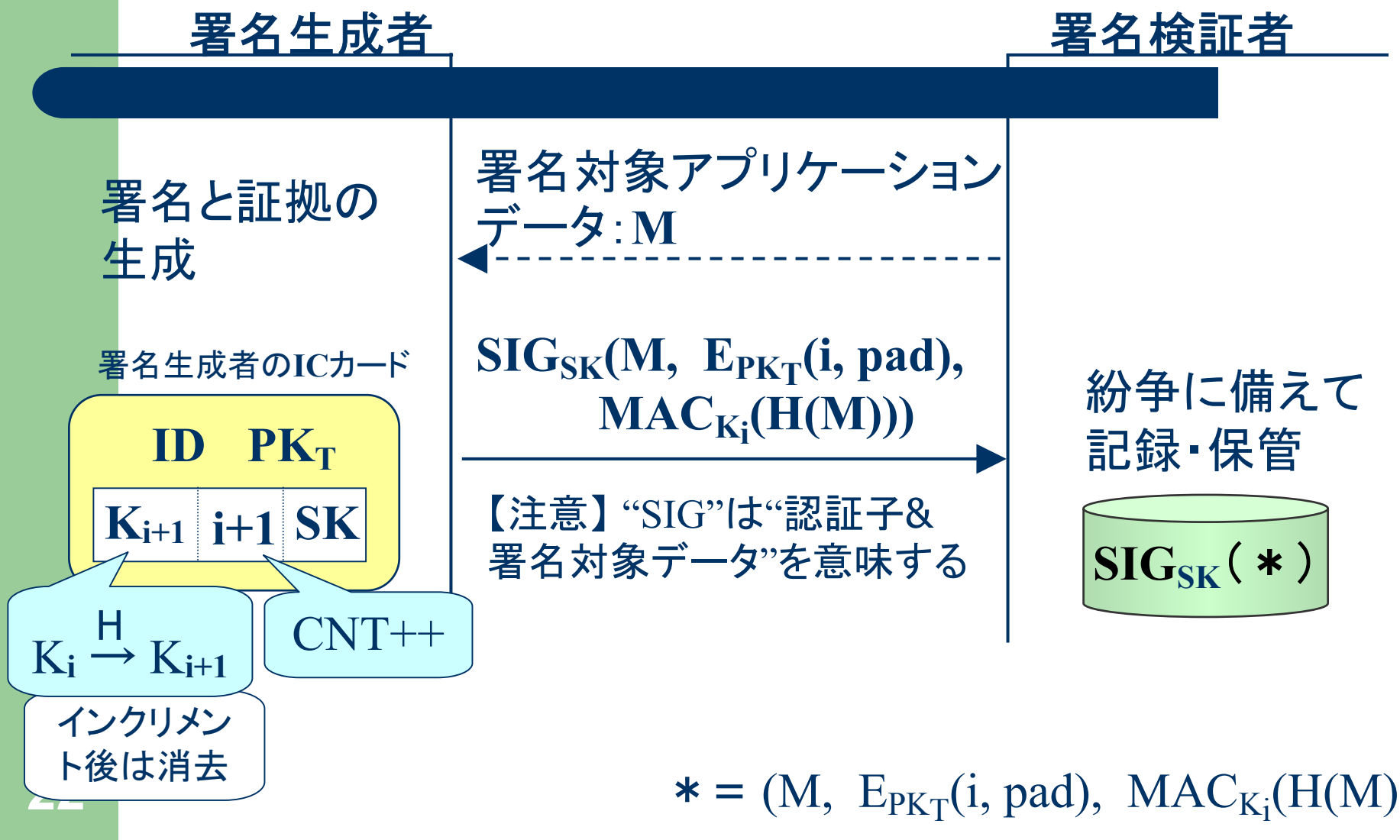
ICカードの発行過程



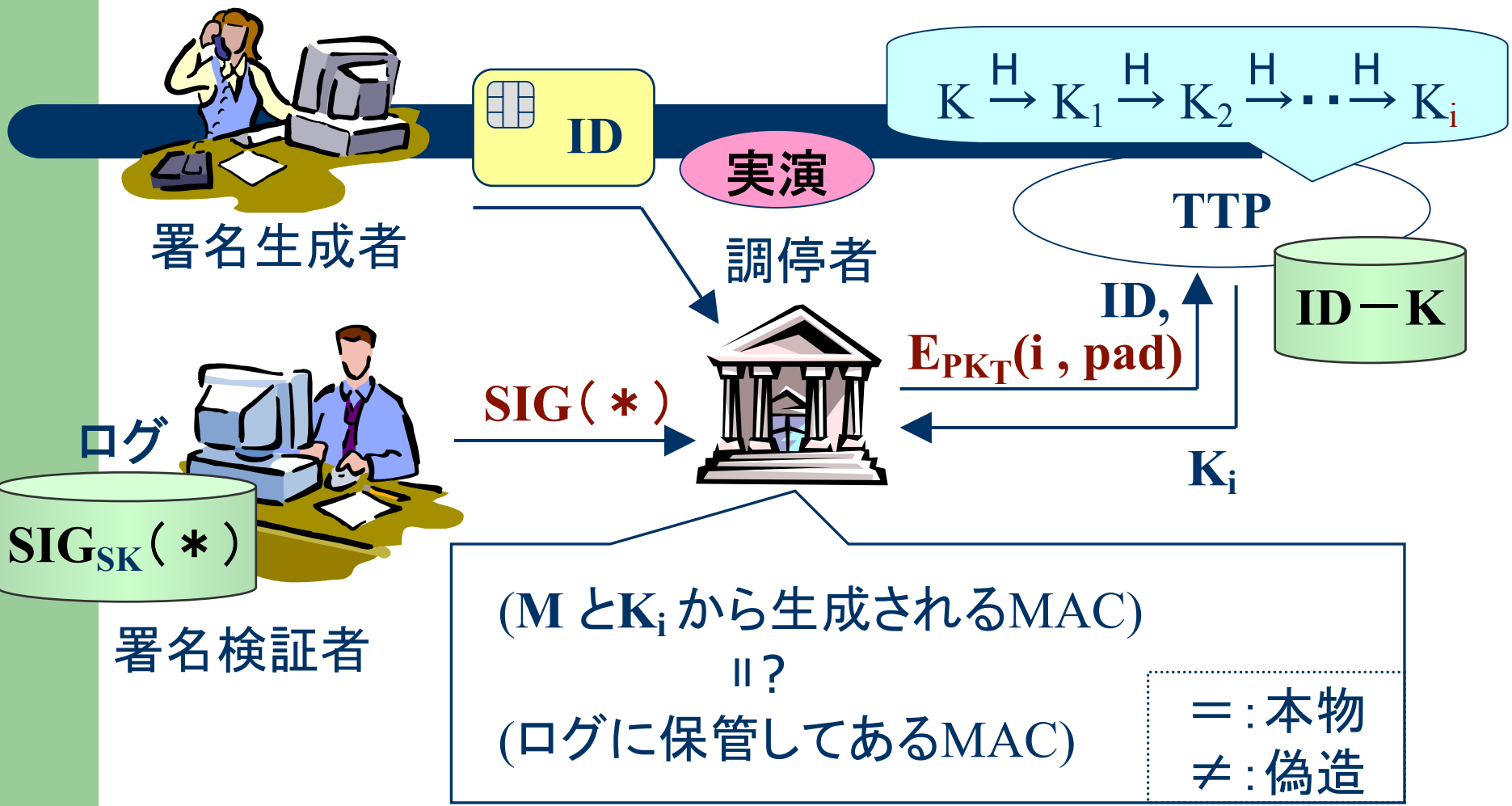
- 対面取引でとりわけ威力を発揮するBiometricsを利用
- 製造過程と分離することで、ある種の内部不正に対処

署名生成時に何を添えるか

（CNT= i のとき）



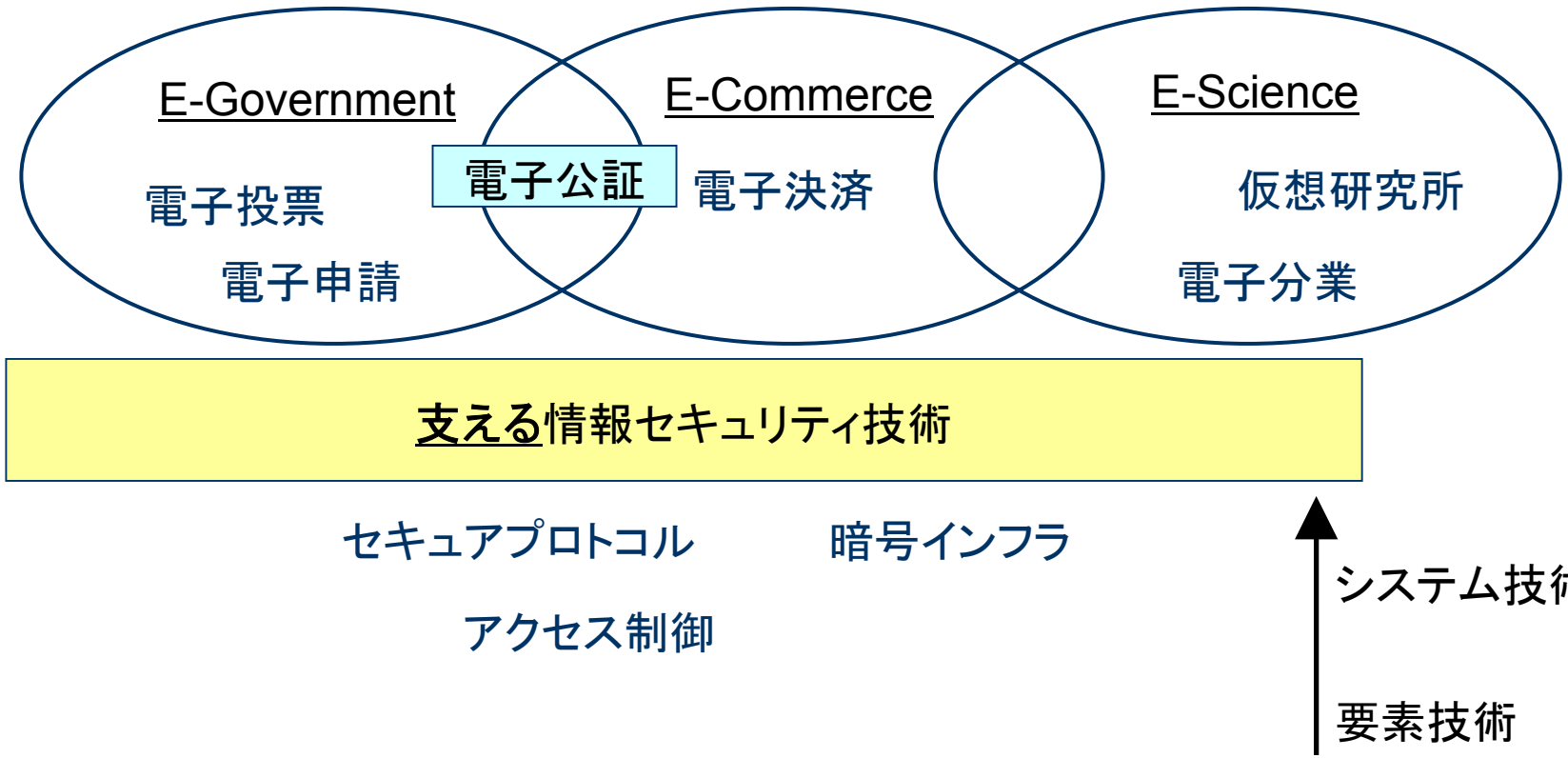
調停プロトコル



＊＝ (M, E_{PK_T}(i, pad), MAC_{K_i}(H(M)))

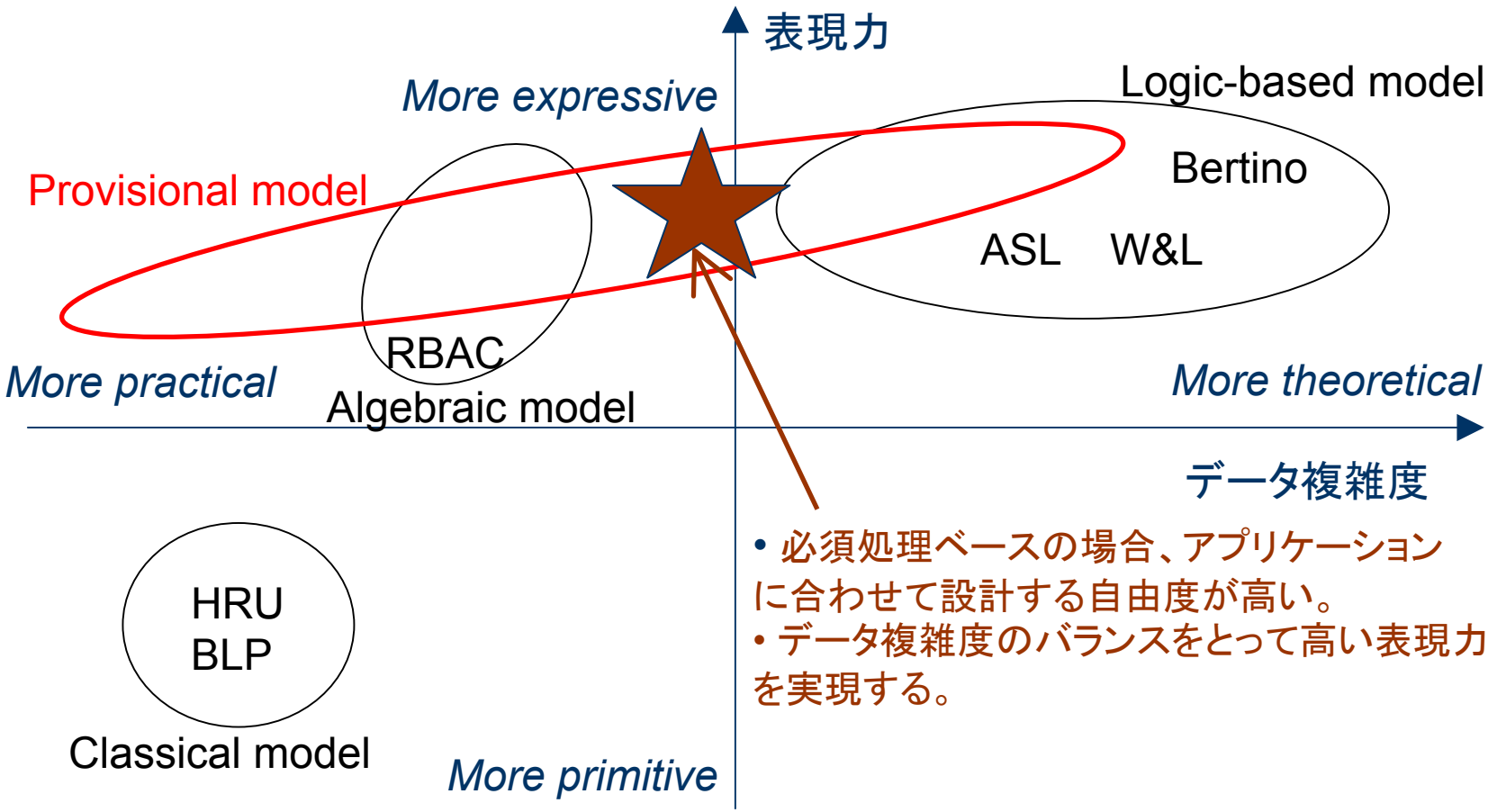
2.2 システム構築技術と事後解決技術

- 「確実な」システム構築
  - PBLP(Provision-Based Linking Process)及びそのE-Scienceへの応用
- 心理的に安心感を与える技術
  - 超高精細な電子時刻印
  - プライバシーを保護したトラストメトリックス

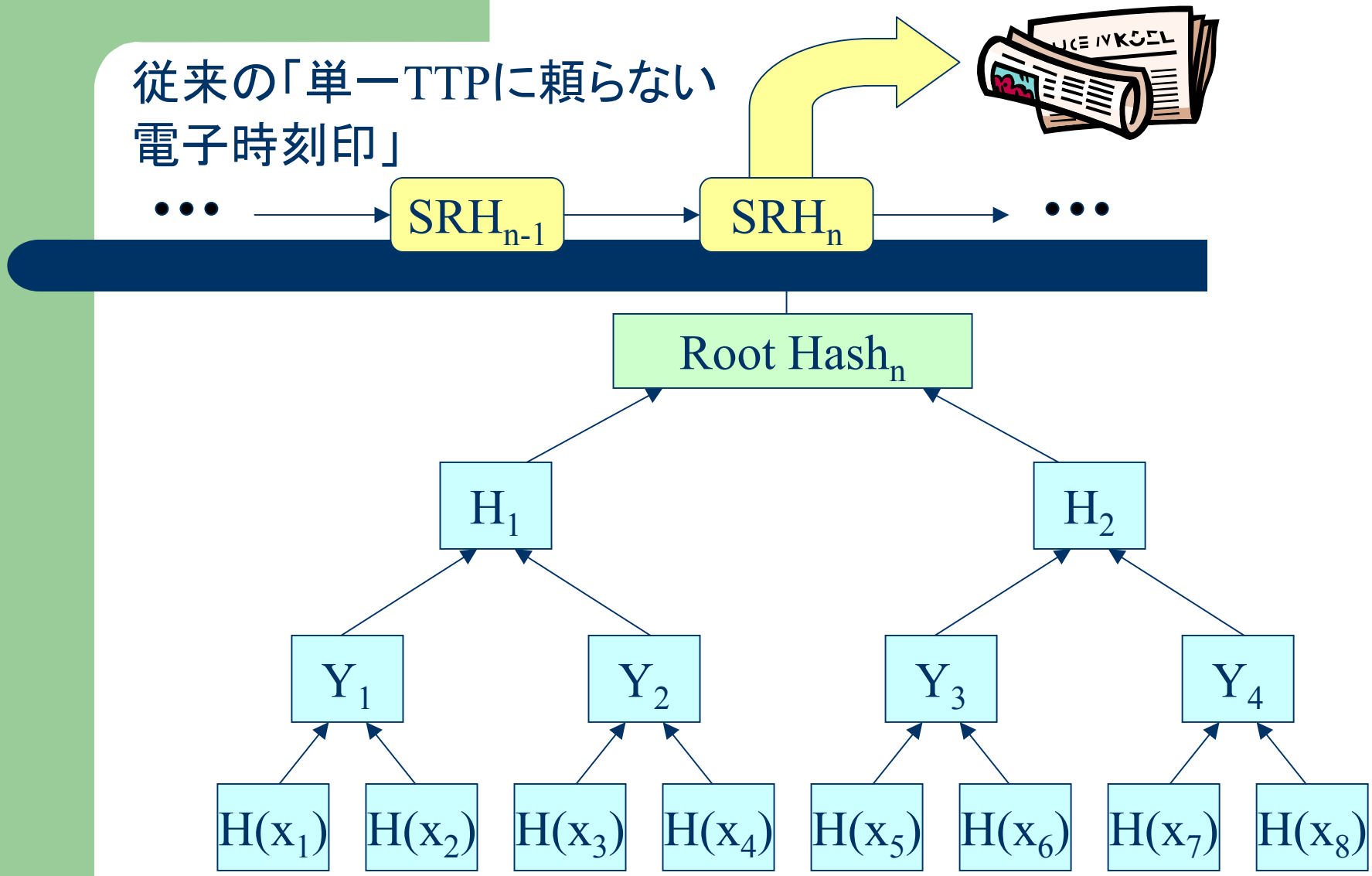

E-Government
電子投票
電子申請
電子公証
E-Commerce
電子決済
E-Science
仮想研究所
電子分業
支える情報セキュリティ技術
セキュアプロトコル
暗号インフラ
アクセス制御
システム技術
要素技術

PBLP（必須処理付きリンキングプロセス）

- （例）「ユーザAは、仮想研究所のサーバで保管されているデータBを書き換えて構わないが、書き換えた直後に**必ず**自身の秘密鍵で電子署名を施し、かつ、実行時刻のタイムスタンプを押さなければならない。」
- 評価： Provisional Action Propertyなどを満足するアクセス制御規則(ACPI: Access Control Policy Information)を設計


表現力
More expressive
Logic-based model
Provisional model
Bertino
ASL
W&L
RBAC
Algebraic model
More practical
More theoretical
データ複雑度
HRU
BLP
Classical model
More primitive
• 必須処理ベースの場合、アプリケーションに合わせて設計する自由度が高い。
• データ複雑度のバランスをとって高い表現力を実現する。

従来の「単一TTPに頼らない電子時刻印」



$Y_1=H(H(x_1), H(x_2))$

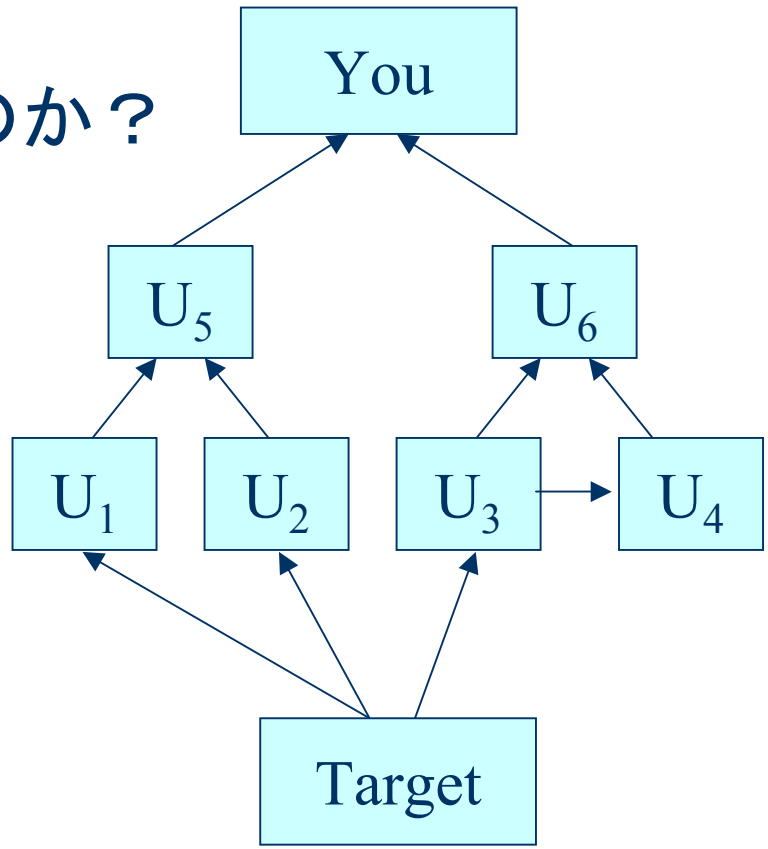
限界は安全性よりもむしろ精度

- 暗号学的な安全性の論拠は従来法と同一
- 新聞ではせいぜい半日単位の精度
- 我々のアイデア： ディジタルTV放送を利用して「電子公表」 → 秒のオーダーへ
- 物理的な証拠との整合性をより詳細に調べることができる → 総合的に見て安全性向上

もう一つのPKI

- Web of trust
- 結局どの程度信頼できるのか？

→ Trust Metrics

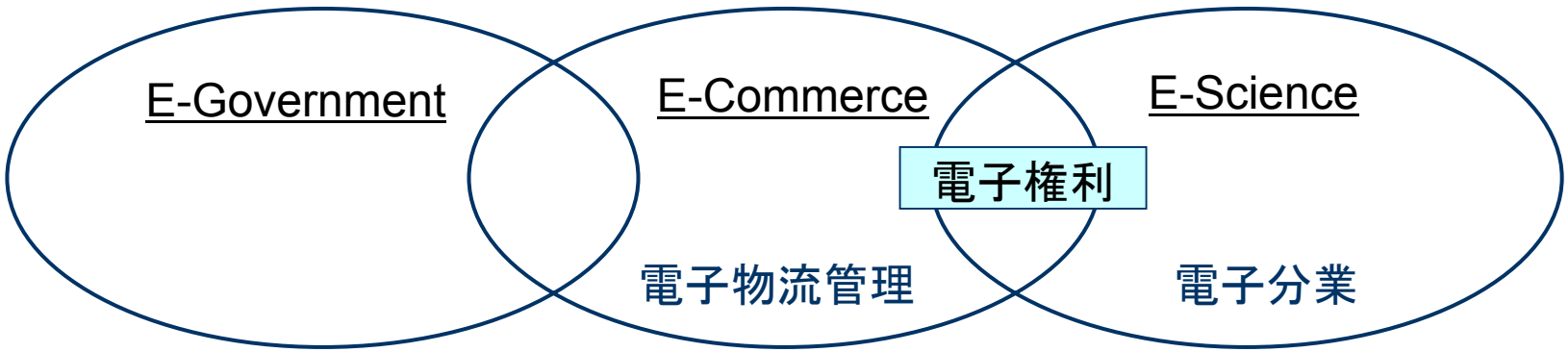


頑健さとプライバシー保護の両立

- 各矢印（枝）に2つのパラメータを割り当てる：
  - Direct trust: そのエンティティIDと鍵のバインドの信頼性を表現
  - Recommendation trust: そのエンティティの判断能力の信頼性を表現
- 「人が人に誤った判断をさせる攻撃」に対する頑健さを向上させる。
- 判断結果の匿名性
  - 暗号学的に、閾値を導入した評価
  - 匿名性が確保されることの二次的効果： 遠慮がなくなることで、より正確な判断結果が出回る可能性

2.3 社会的要素

- 情報セキュリティの技術革新基盤
  - 産学連携分析
- 脅威の予見と周知
  - 現実は、管理者も含めて「侵入検知システム」
  - 「スローな」侵入検知と管理者へのフィードバック
  - 情報提供は社会の役割
- 流通システム
  - 「軽い電子タグ」のセキュリティ
  - プライバシー保護も事業者の社会的責任(CSR: Corporate Social Responsibility)
  - モデル化等のフレームワークは終了。現在開発中。



支える情報セキュリティ技術

共に支える
社会制度
（法・制度・
施策・監査・
保険など）

暗号インフラ　鍵管理

侵入検知

電子透かし

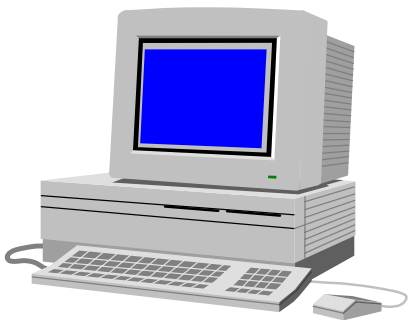
システム技術

要素技術

迅速な技術革新の重要性 → 文献計量分析と特許調査で産学連携分析

- 一部の攻撃者が最新の技術や情報に追随。
- 一方で、ユーザは・・・

一部の攻撃者

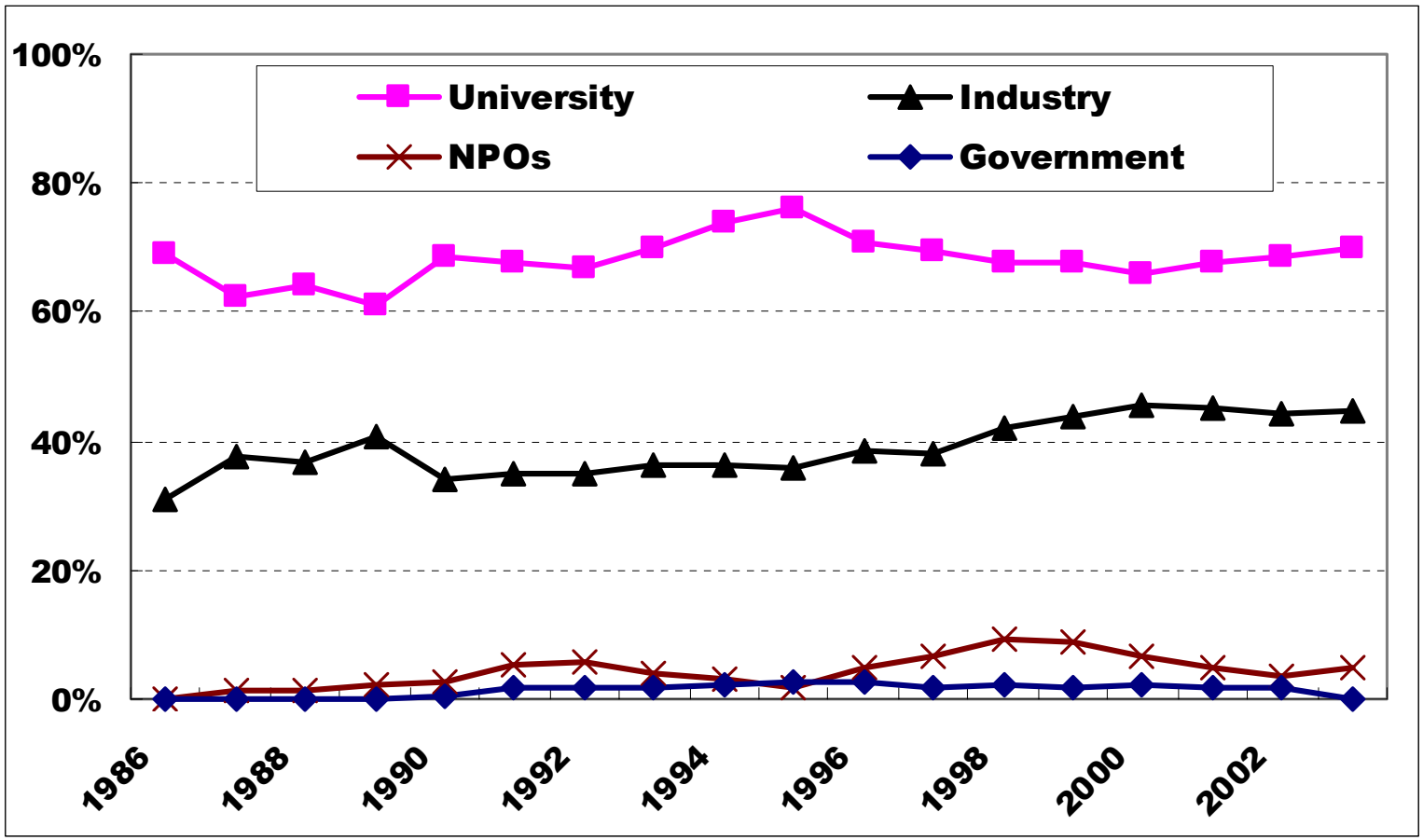


普及レベル

何故いつまでたっても・・・

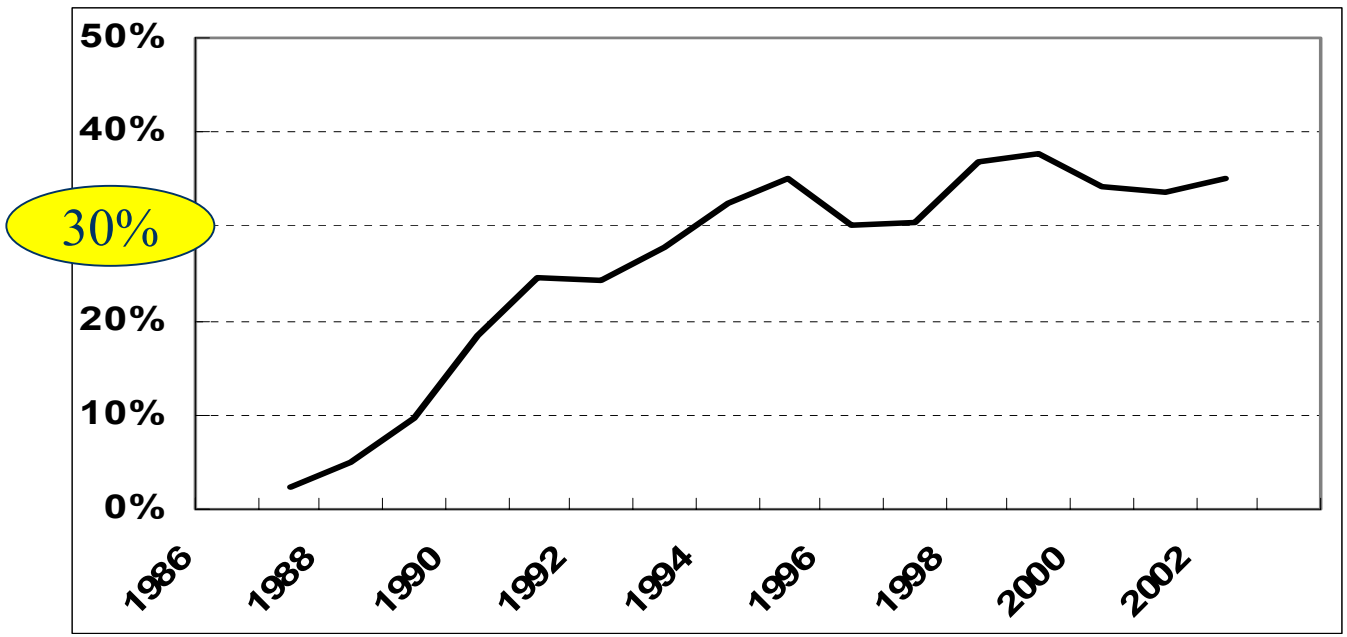
Share of papers, 1986 – 2003

→ No major change occurs



Share of industry cross-sector coauthored papers (Moving average of 3 years), 1986-2003

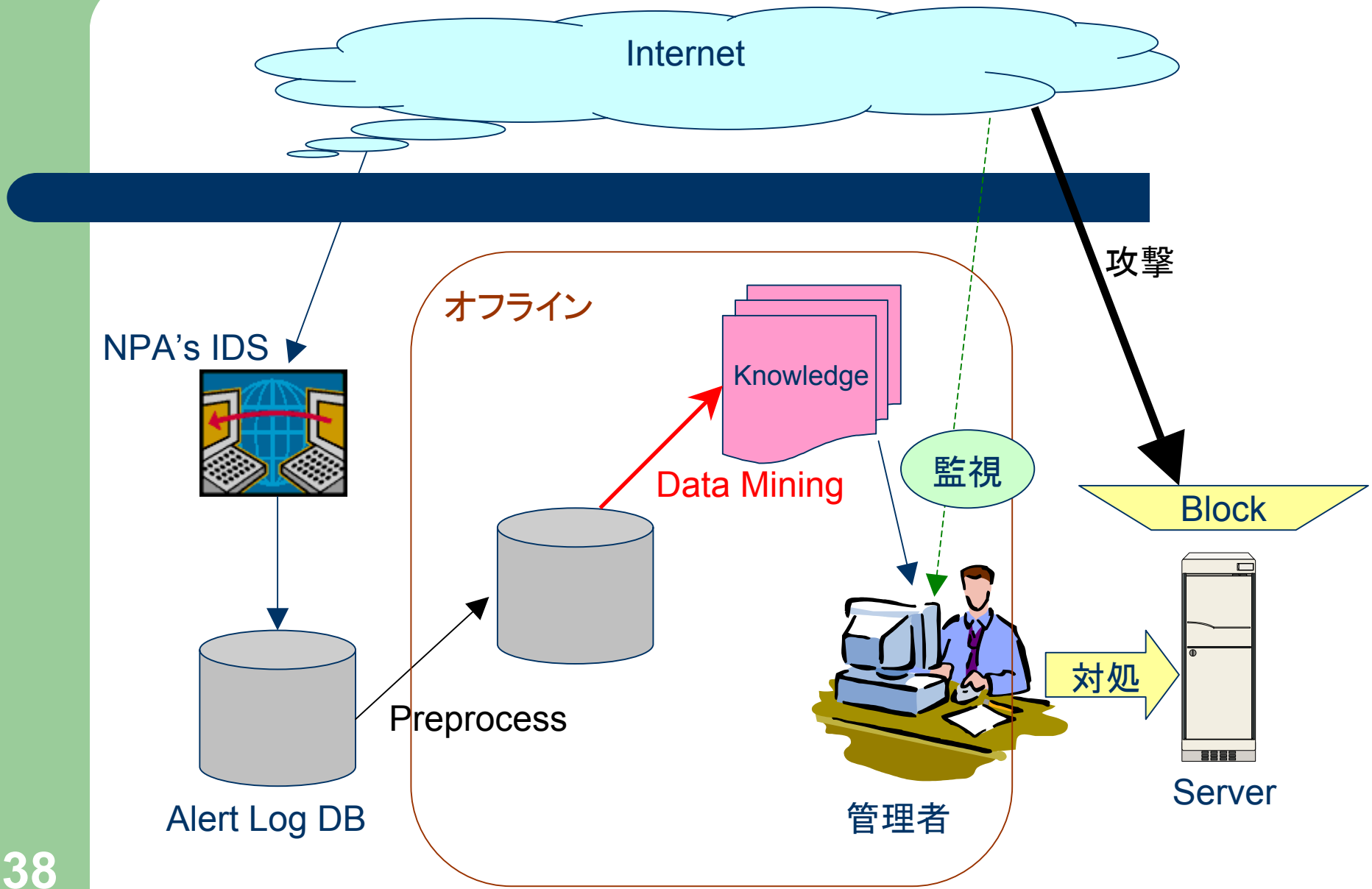
- Share of cross-sectoral coauthored papers in industry sector
  - 電気：54%、機械：78% (1995年調査)
- *Lower level compared to the other fields*



IDS警告ログの分析

- 段階を踏む攻撃は多岐にわたっている。
- たとえ兆候を察知しても、対処を自動化するとそれ自体がセキュリティホールになる恐れがある。

警告ログを分析し、その結果を
管理者に周知させる


Internet
攻撃
オフライン
NPA’s IDS
Knowledge
Data Mining
監視
Block
Preprocess
対処
Alert Log DB
管理者
Server

分析の実際

- Preprocessで ((Date), Source domain, Detection place, Attack name) を抽出。
- 自身では未知（未体験）でも、社会としては既知の（スローな）攻撃や傾向が存在する。
- 驚くほどスローなものも存在することや、地域性を実証。

危険だが知っていれば
対処可能な攻撃

- Examples from USA

Date	detected in	Attack
01.24.	Tokyo	SA
01.24.	Tokyo	PA
	…	
10.14.	Tokyo	PA
10.14.	Tokyo	CC
10.14.	Tokyo	OF
	…	

3. まとめ

超ディペンダビリティを達成するためには広い視野が必要

- 三つのアプローチ（人間的要素、システム構築と事後解決、社会的要素）で超ディペンダブル暗号系を構築：　明確な定義から評価・実証まで（検証可能性や新しい視点の導入を重視）
- ヒューマンクリプトを実践
- ソーシャルクリプトを開拓
- その中で総合力のある若手研究者を育成

長期的な基礎研究との融合

- 積み重ねの重要性：
  - 本研究では、随所で、当研究グループが長く取り組んできた暗号理論（とくに評価モデル）を駆使。