新たな安全・簡単アイデンティティ管理体系
セキュア・アイデンティティ流通基盤

2008年4月3日

NTTコミュニケーションズ株式会社

NTTソフトウェア株式会社

序章： 海外でのセキュリティ被害の傾向

米国

NW犯罪のビジネス化・プロ化が進み、金銭的な利益を求めて、ID/認証情報への攻撃増加が止まらない

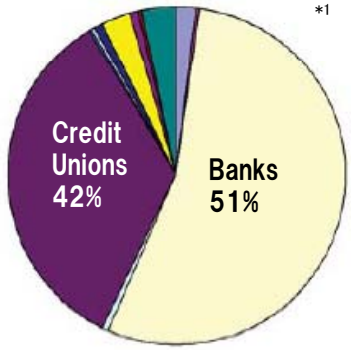
金融系認証情報がターゲット

アンダーグラウンドエコノミーサーバーで販売された商品の内訳 *2

ランク	商品	割合(%)	価格帯
1	クレジットカード	22%	$0.50–$5
2	銀行口座	21%	$30–$400
3	電子メールのパスワード	8%	$1–$350
4	メーラー	8%	$8–$10
5	電子メールアドレス	6%	$2/MB–$4/MB
6	プロキシ	6%	$0.50–$3
7	完全な個人識別情報	6%	$10–$150
8	詐欺	6%	$10／週
9	社会保障番号	3%	$5–$7
10	安全性が低下した UNIX Shell	2%	$2–$10

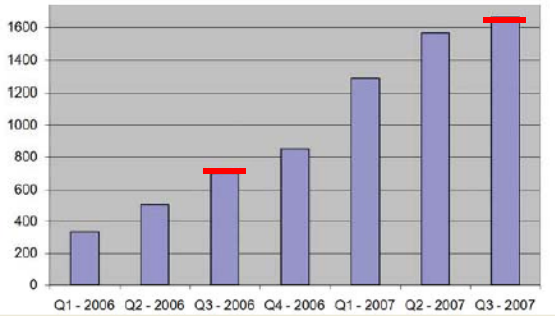
銀行・クレジット企業狙いが90%

産業別フィッシング攻撃数 *1



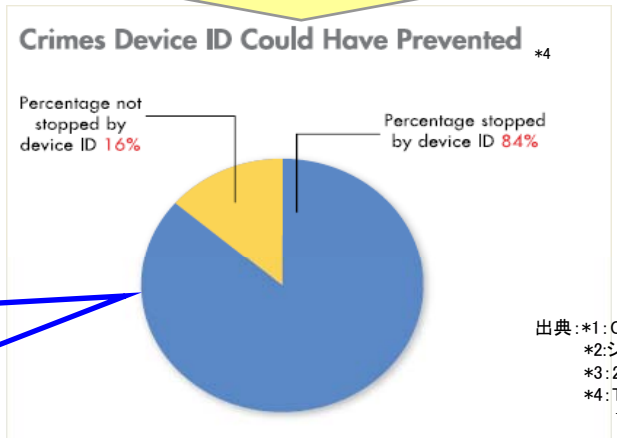
ID盗難等の脅威、昨年より200%増

フィッシング攻撃数 *1



- 06年消費者被害額 ：11億ドル
- ウィルス平均被害 ：2400ドル
  不正アクセス平均被害：150万ドル

米国企業では金銭的被害がウィルス被害額を上回る *3



ID管理を強化すれば84%防止可能

出典：*1：Cybeillance “Online Financial Fraud and Identity Theft Report” 2007.Oct
*2:シマンテック ”インターネットセキュリティ脅威レポート(20071月～2007年6月の傾向” 2007年9月
*3：2007 CSI COMPUTER CRIME
*4：TrustedStrategies “Network Attacks: Analysis of Department of Justice Prosecutions 1999–2006” 2006 Aug.

研究会での課題と施策の方向性

これまで指摘された課題

研究会まとめ（研究会資料4-6）

1. 脅威の対象となる範囲の拡大（人、物）
2. 対策の困難性の拡大（ソーシャルエンジニア攻撃、責任範囲）
3. 脅威の対象となる情報の増加（モデル、利用形態の変化）

ユビキタス社会への変化とセキュリティ（研究会資料4-6別紙）

○情報通信NW技術の高度化
- すべてにIPを利用する社会
- IP化ですべての「物」「人」がシームレスに
- 様々なID（IPv6アドレス、人、IT家電、NW機器、サービス）を、どう体系的に扱うか早急な課題

有識者ヒアリング

○NGN
- 直接到達性
- 宅内レファランスモデル

○IPv6
- 直接到達性により、ボット化の危険
- nonPC端末がネットに接続

○無線アクセス
- 端末には個人情報が集中
- 端末暗証番号の解読可能性

○情報家電
- 情報家電のPC化に伴う危険
- HGWでFWで守る or 端末機器で守る

課題に対する施策の方向性

1. 数（利用者、物、情報）の爆発的増加へ対応

- 膨大な情報が流通するend-end型IPv6によるP2P社会モデルへの対応検討
- 意味を持ったIPアドレスや様々なIDのビジネス利用の膨張と、更なる個人情報保護とのバランス議論
- あらゆる製品へのIPアドレス付与の急増や、サービスや個人属性情報に付けられる膨大なIDが流通する社会でのセキュリティ要件とICT社会モデル検討

2. 永遠のビギナーの保護

- 広がるソーシャル系脅威のセキュリティ対策(設定の自動化・容易化)
- 消費者指向に転換した産業側のあるべき施策
- リテラシの低いユーザをサポートできるICT高度化

3. 複雑化するICTに対するセキュリティモデルの確立

- 消費者保護、産業促進とのバランスを考慮した、様々な脅威に対応できるセキュリティモデルの検証
- エンドユーザに対するソーシャルエンジニアリング被害が、リアル社会のあらゆる　業界、レイヤで様々に顕在化、拡大する事への対策が必要

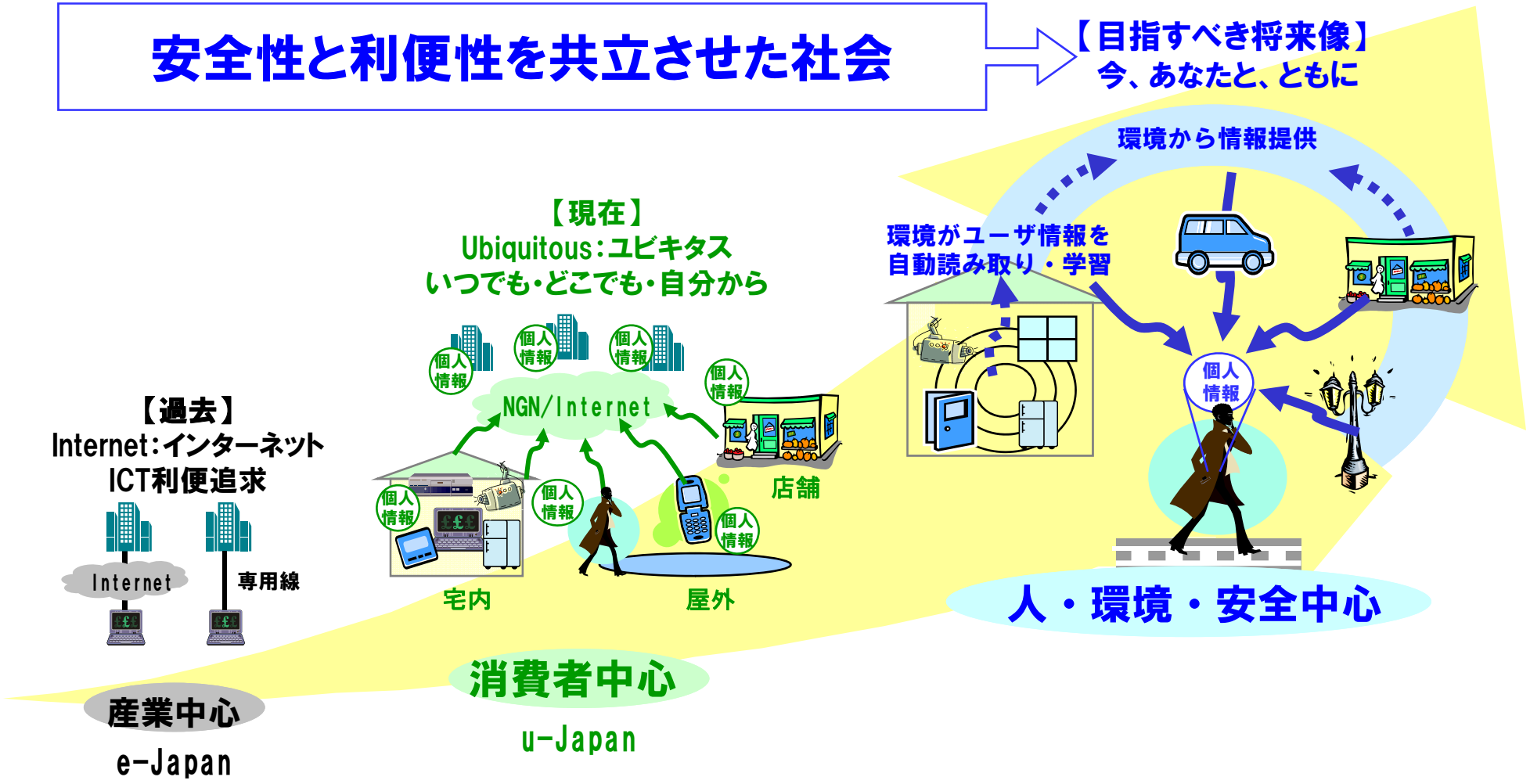
4. 産業・社会の複雑さへの施策

- 業界に複雑に絡み合うセキュリティ・コストの増加対策
- 複雑化する一方の社会における脅威への横断的対策

ICT社会の未来　－Ubiquitousの次の時代－

安全性と利便性を共立させた社会

【目指すべき将来像】
今、あなたと、ともに



垂直分散社会 接続＆単発防御	水平連携社会 マルチ利用＆マルチ防御	共生社会 双方向活用＆自動防御
～現在	現在～2010年	2010年～将来

解決すべき重要課題と対策案

【重要課題】

ユビキタスの次の時代では、個人の情報を社会システムが自動的に連携・制御するはずであるが、数（利用者、物、情報）の爆発的な増加と、それに対応する永遠のビギナーを安心・安全・快適に守る為の、アイデンティティにフォーカスした新たな基盤作りが必要である。

【対策案】

新しいｱｲﾃﾞﾝﾃｨﾃｨ管理体系

セキュア・アイデンティティ流通基盤の構築

ユーザが複雑な設定や運用を意識する事無く、ユーザアイデンティティをセキュアに流通させられる基盤を構築する

【具体例】

ユーザごとのユニークなIDと、サービスごとに利用する認証ID（ハイブリッドID）を常に一意にセキュアに生成できる方式を用いて、ユーザもサービサーも安全で簡単に利用できる仕組みの検討

【メリット】

ユーザメリット

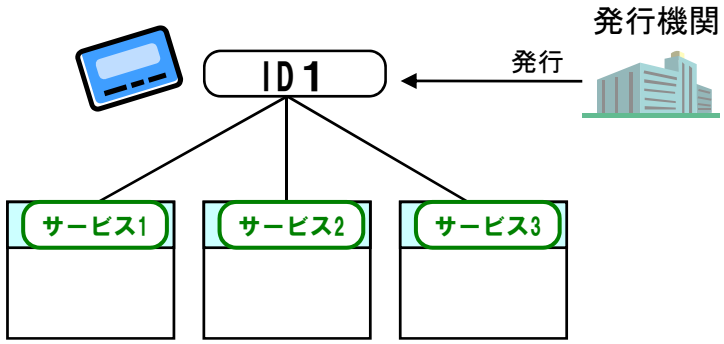
- ID、パスワードの煩わしい管理が不要
- ユーザ自身が安全で簡単にID管理ができる。

サービサーメリット

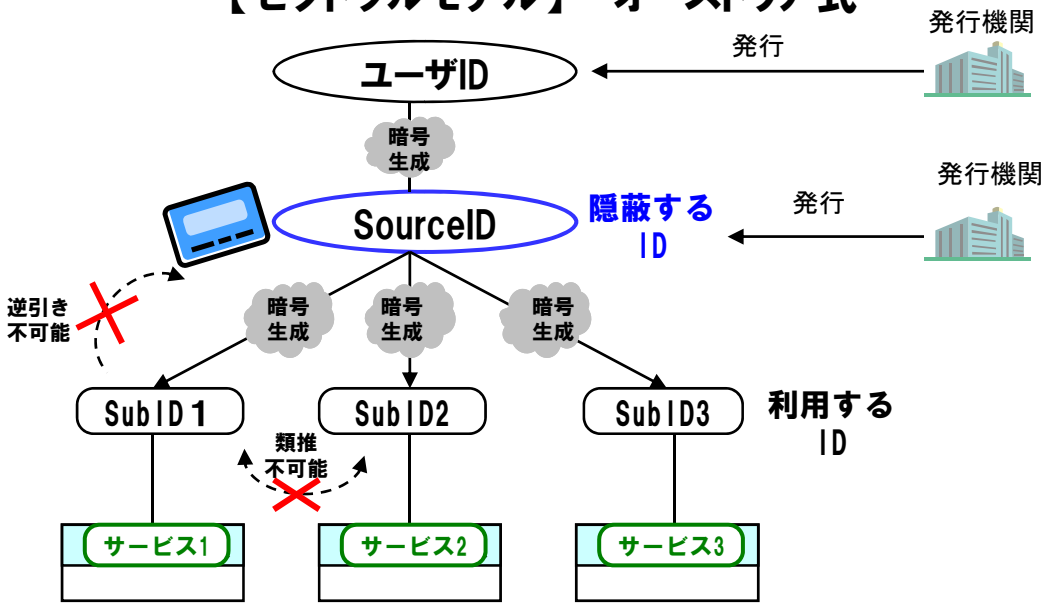
- １サービス１IDで、サービサーのID管理負担が低減
- なりすましや情報漏洩などに対する管理リスクも軽減。

海外のアイデンティティ管理例

【フラットモデル】・エストニア,デンマーク式



【セクトラルモデル】・オーストリア式

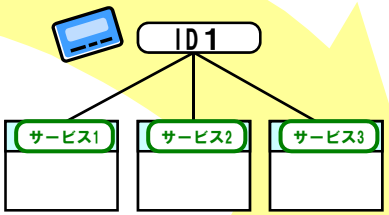


【特徴】

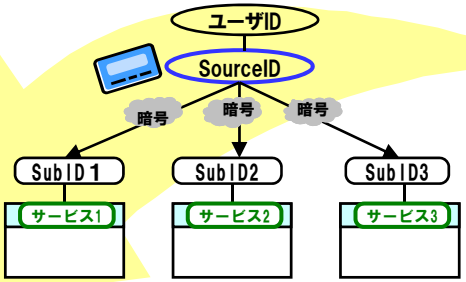
	【フラットモデル】 エストニア,デンマーク式	【セクトラルモデル】 オーストリア式
①認証モデル	ICカードモデル	ICカードモデル
②サービスごとのID発行	なし	あり（自動化）
③ID紛失時の対策	カード紛失時等はその有効性を一時停止	ID再発行不可
④暗号鍵の保護機能強化	―	未
⑤暗号危殆化	―	危殆化の危険性あり（SHA-1）

新たなアイデンティティ管理　ーセキュア･アイデンティティ流通基盤ー

【フラットモデル】



【セクトラルモデル】



セキュア・アイデンティティ流通基盤

【日本式】

安全性

暗号／ｾｷｭﾘﾃｨ強化

＋

利便性

自動化/標準化

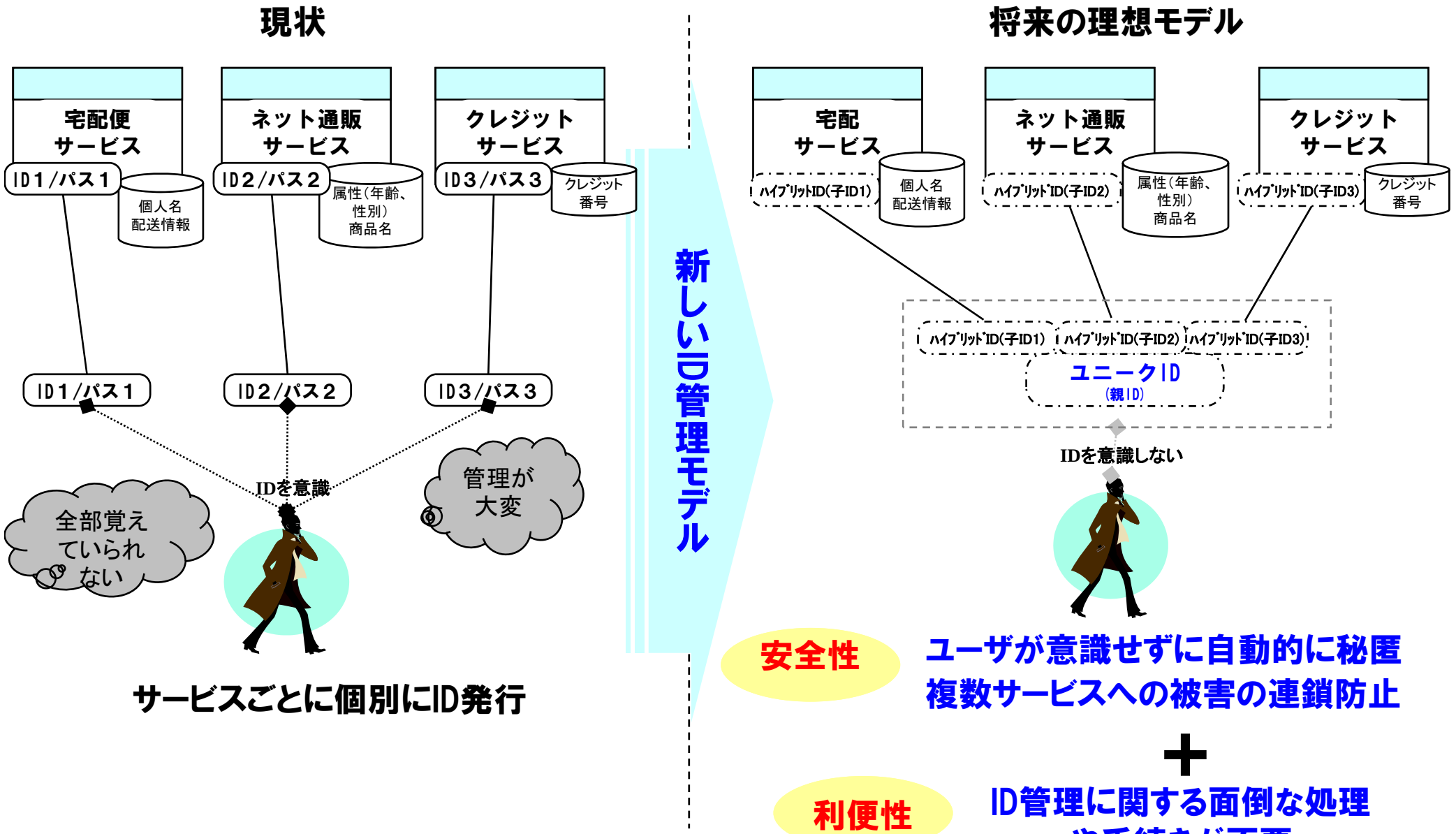
自由度

他方式との共存・融合

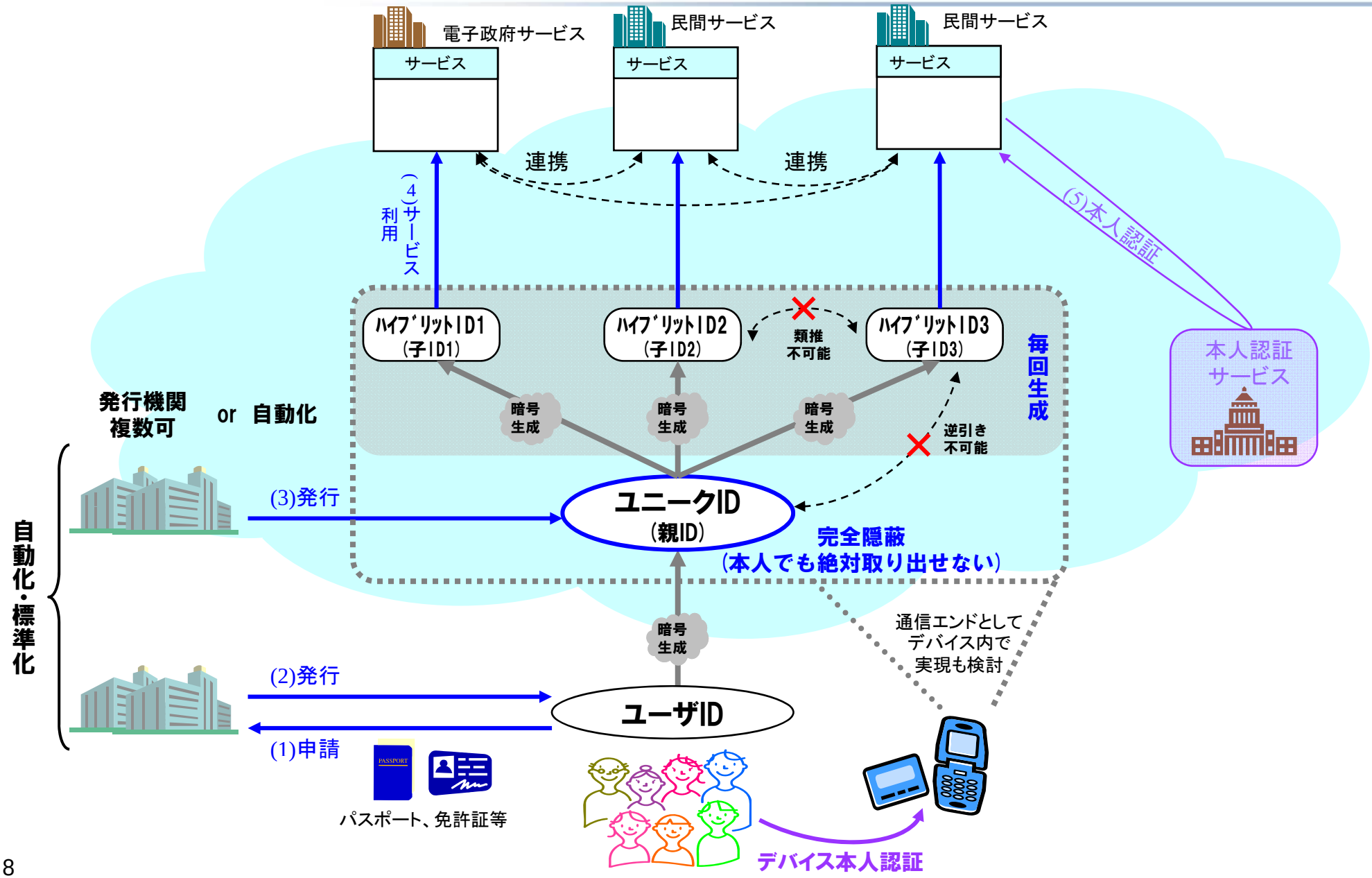
【特徴】

	【セキュア･アイデンティティ流通基盤】 ハイブリットID型
①認証	ネットワーク対応モデル （アイデンティティレイヤの標準化検討） （属性情報管理）
②ID発行	IDユニーク生成の自動化/標準化
③紛失時	IDライフサイクル化
④暗号保護	暗号鍵の完全安全化（秘密分散ｱﾙｺﾞﾘｽﾞﾑ）
⑤危殆化	暗号危殆化対策

現状のID管理と将来の理想モデルとの違い

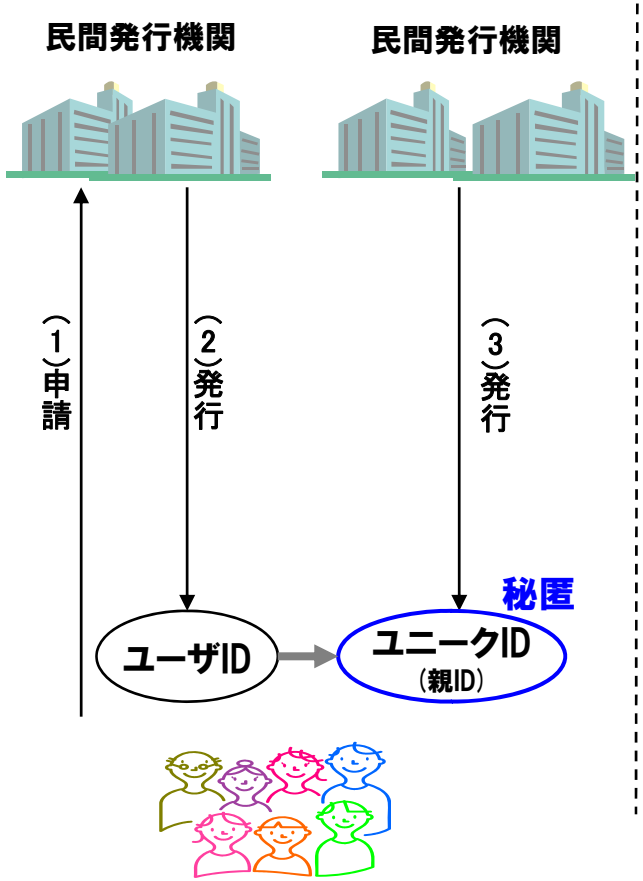


セキュア・アイデンティティ流通基盤イメージ

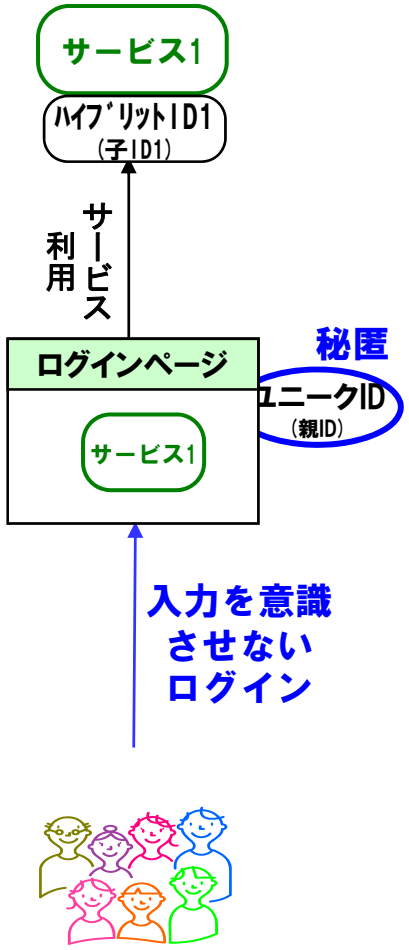


【参考】利用フロー

Step1： 発行申請



Step2： サービス利用



Step3： 複数サービス利用