堀部政男情報法研究会 共通番号制度と国民ID時代に向けた
プライバシー・個人情報保護法制のあり方 ＜課題と提言＞
第4回シンポジウム
2011年3月26日

パネル討論 論旨

独立行政法人産業技術総合研究所
情報セキュリティ研究センター
高木浩光

WGの議論を拝見して外野から

- 内閣官房
  - 「社会保障・税に関わる番号制度及び国民ID制度」における
    「個人情報保護の仕組みに関する事項」のWG
    「両制度で共通する事項のうち技術に係る事項」のWG
    http://www.cas.go.jp/jp/seisaku/jouhouwg/
- 「個人情報保護WG」（傍聴可）（法WG）
  - 第1回 2月7日
  - 第2回 2月23日
  - 第3回 3月18日
- 「情報連携基盤技術WG」（傍聴不可）（技術WG）
  - 第1回 2月4日
  - 第2回 3月4日
  - 第3回 3月23日

法WGに尋ねたい点

- 法WGの内容から
  - (1)「番号の告知を求めてはならない」が後退した件
  - (2)「番号の告知を求めてはならない」を根拠づける法的理念
- 技術WGの内容から
  - (3)「情報連携基盤」を全データが通過する方式は許されるか
  - (4)「情報連携基盤」の運営主体となる省が「情報保有機関X」を兼ねてよいか
  - (5)「対照テーブルによる管理を行わない」はナンセンスでは
  - (6) 2つのIDを持たない原則がマイポータルの設計で一人歩き
- 総論
  - (7) 技術WGと法WGの連携ができていない
  - (8) 拙速では

(1)「告知を求めてはならない」が後退

- 法WG第2回の資料3「骨格案」では
  - 「何人も正当な理由なく上記利用目的以外の用に供する目的で、番号の告知を求めてはならないこととしてはどうか」
- 法WG第3回の資料3「概要座長私案」では
  - 「何人も不当な目的で番号の告知を求めてはならないこととすることが考えられる」
- 住民基本台帳法では住民票コードの告知を求めることを明確に禁止してきた（間接罰）
- 「不当な目的で」とは？
  - 例：レンタル店が会員登録時に身分証として共通番号の書かれた税と社会保障カードの提示を求める行為は、不当な目的か？

どうしてこうなった?

- 背景となる案
  - 番号制度のICカードが配布される
  - ICカードを身分証として使えるようにする案
  - ICカードには券面に共通番号を印刷する案（「見える番号」）
- こういうことですか?
  - レンタル店等で、身分証としてICカードが提示されたとき、身分証の写しをとる際に、共通番号まで記録してしまう
  - それを避けよとするのは運用上無理がある
  - したがって、「正当な理由なく利用目的以外の用に供する目的で、番号の告知を求めてはならない」は現実的でない
  - だから、「不当な目的で」に緩めざるを得なくなった（?）
- 本末転倒であり受け入れ難い
  - 対案：ベルギーのIDカードでは裏面に「番号」が書かれている？ http://en.wikipedia.org/wiki/Belgian_national_identity_card

- 住民基本台帳法 第30条の43
  - （…）以外の者は、何人も、自己と同一の世帯に属する者以外の者（…）に対し、当該第三者又は当該第三者以外の者に係る住民票に記載された住民票コードを告知することを求めてはならない。
  - 2 市町村長等以外の者は、何人も、その者が業として行う行為に関し、その者に対し売買、貸借、雇用その他の契約（…）の申込みをしようとする第三者若しくは申込みをする第三者又はその者と契約の締結をした第三者に対し、当該第三者又は当該第三者以外の者に係る住民票に記載された住民票コードを告知することを求めてはならない。
  - 3 市町村長等以外の者は、何人も、業として、住民票コードの記録されたデータベース（…）であつて、当該住民票コードの記録されたデータベースに記録された情報が他に提供されることが予定されているものを構成してはならない。
  - 4 都道府県知事は、前二項の規定に違反する行為が行われた場合において、当該行為をした者が更に反復してこれらの規定に違反する行為をするおそれがあると認めるときは、当該行為をした者に対し、当該行為を中止することを勧告し、又は当該行為が中止されることを確保するために必要な措置を講ずることを勧告することができる。
  - 5 都道府県知事は、前項の規定による勧告を受けた者がその勧告に従わないときは、都道府県の審議会の意見を聴いて、その者に対し、期限を定めて、当該勧告に従うべきことを命ずることができる。（罰則：命令に違反した者は、一年以下の懲役又は五十万円以下の罰金）

(2)「番号の告知…」の法的理念

- 私の意見
  - 住民基本台帳法と同様に、番号の本来の目的以外での使用を抑制できるよう、「告知を求めてはならない」等とすべき
- しかし
  - どんな脅威を回避するためにそうするのか
  - 唯一無二の番号を全国民が持つことが保障されることによって生ずる目的外の利用、トラッキング、不当な差別への使用などの懸念
  - 法WG第2回の資料1「 税・社会保障に関わる番号制度に対する国民の懸念」にこの脅威が想定されていない!!
    - データセキュリティ（漏洩リスク）のことしか検討されていない
- 法的理念がない
  - 番号の告知云々は、個人情報保護法から導かれる？
  - データプライバシーという基礎概念を欠いているのでは？

資料1－①

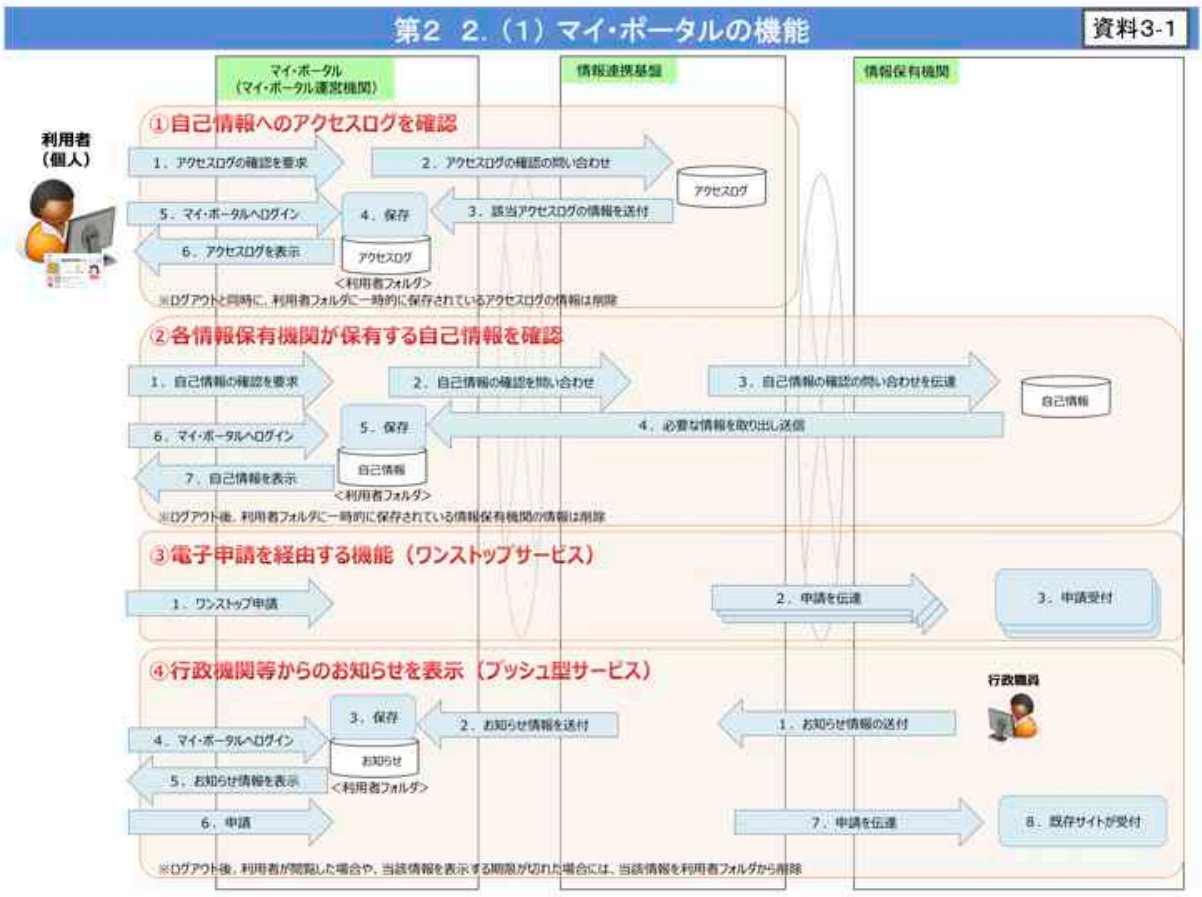
税・社会保障に関わる番号制度に対する国民の懸念

	具体的な懸念		関連する主な事件	具体策
国（行政）に対する懸念	国家による国民の監視・監督についての懸念	○国民の勤務先や家族の状況、各種納税・社会保険料支払いに関する情報、社会保障給付に関する情報、各種経済取引活動・消費活動に関する情報、更に制度設計によっては消費の嗜好が国家により一元管理されるのではないか。	○防衛庁の海幕三等海佐が個人の発意により、情報公開請求者についての個人情報を付加した開示請求者リストを作成した事案（2002年）	○自己情報へのアクセス記録の確認 ○第三者機関 ○目的外利用・提供の制限等 ○罰則の強化 ○プライバシーに対する影響評価
	不適正行為についての懸念	○正当な理由がないにもかかわらず、保有する番号及び個人情報を第三者に提供してしまうのではないか。 ○コンピュータウィルスやハッキングの被害による情報の漏えいがありえるのではないか。	○経産省の元職員が個人情報を含むデータをUSBメモリに記録して持ち出し、紛失した事案（2006年） ○京都府宇治市の住民基本台帳を利用したシステム開発に従事した再々委託先従業員が、21万人分の台帳データを名簿業者に売却した事案（1999年） ○神奈川県教育委員会のシステム開発を担当した再々委託先従業員のパソコンより、同県立高校生徒の個人情報約11万人分がインターネットのファイル交換ソフトを通じて漏えいした事案（2008年）	
		○行政機関による個人情報の改ざん・虚偽の記録がありえるのではないか。	○社会保険庁職員が恒常的に年金記録等の改ざんを行った事案（2007年）	
		○行政機関がその職務の用以外の用に供する目的でファイル又はデータベースを作成するのではないか。	○防衛省鹿児島地方協力本部の所長が、隊員出身地カードデータをCD-Rに無断複製し、不動産会社役員に売却した事案（2009年）	
	目的外利用についての懸念	○本人が知らぬ間に目的外で利用されるのではないか。	○社会保険庁職員が私用目的で年金加入者の年金納付記録を閲覧した事案（2004年）	
一般個人・企業に対する懸念	不適正行為についての懸念	○第三者の成りすましによる番号及び個人情報の不正取得行為がありえるのではないか。	○東京都等において偽造運転免許証による住民基本台帳カードの詐取が発生した事案（2010年）	
		○民間事業者による情報漏えいがありえるのではないか。 ○コンピュータウィルスやハッキングの被害による情報の漏えいがありえるのではないか。	○A企業の社員が約1万人分の社員の個人情報ファイルを記録したUSBメモリを入れた鞄を帰宅途中に紛失した事案（2005年） ○B企業の元契約社員がB企業のサーバーに不正アクセスし、約450万人分の顧客データを漏えいさせた事案（2004年） ○C企業の元社員が個人情報約860万件分を不正に持ち出し、インターネット通販詐欺グループに売却した事案（2007年） ○医療センターの個人情報約26万人分がインターネットのファイル交換ソフトを通じて漏えいした事案（2006年）	
		○民間利用者による個人情報の改ざん・虚偽の記録がありえるのではないか。	○訪問介護事業所が訪問介護記録を作成し、不正に介護報酬を請求した事案（2011年）	
	目的外利用についての懸念	○本人が知らぬ間に目的外で利用されるのではないか。	○金融機関が個人の信用情報を本人の同意を得ずに、与信審査目的以外の目的で第三者に提供した事案（2005年）	

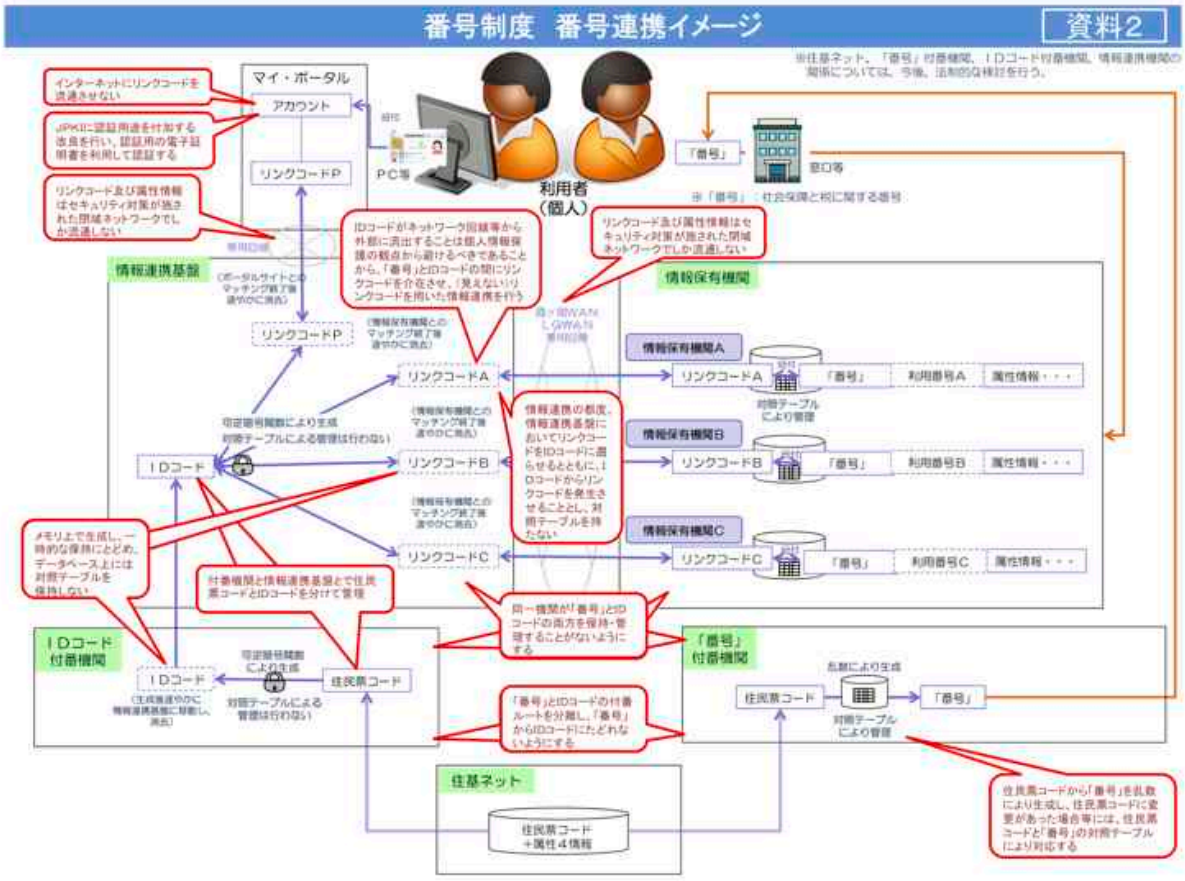
法WG第2回資料1より

(3)「情報連携基盤」を全データが通過?

- 技術WGで示された「情報連携基盤」案
  - 認証連携方式は示されたが、データの転送方式が明確でない
  - 技術WG第3回資料3-1「マイ・ポータルの機能」の図からすると、すべての情報が「情報連携基盤」を通るようにも見える（ゲートウェイ方式？）
- 違憲性を払拭しきれないのでは？
  - 「情報連携基盤」を全データが通過する
  - 記録・保管しなければ合憲なのか、それとも、記録・保管可能であるかぎり違憲なのか
- 他の技術実現的方式がある
  - 「情報連携基盤」は認証連携のみ行い、データは「情報保有機関」に接続して直接得る方式
  - 世界的今日的に言って普通はそのような プロトコルに設計するもの



技術WG第3回資料3-1より



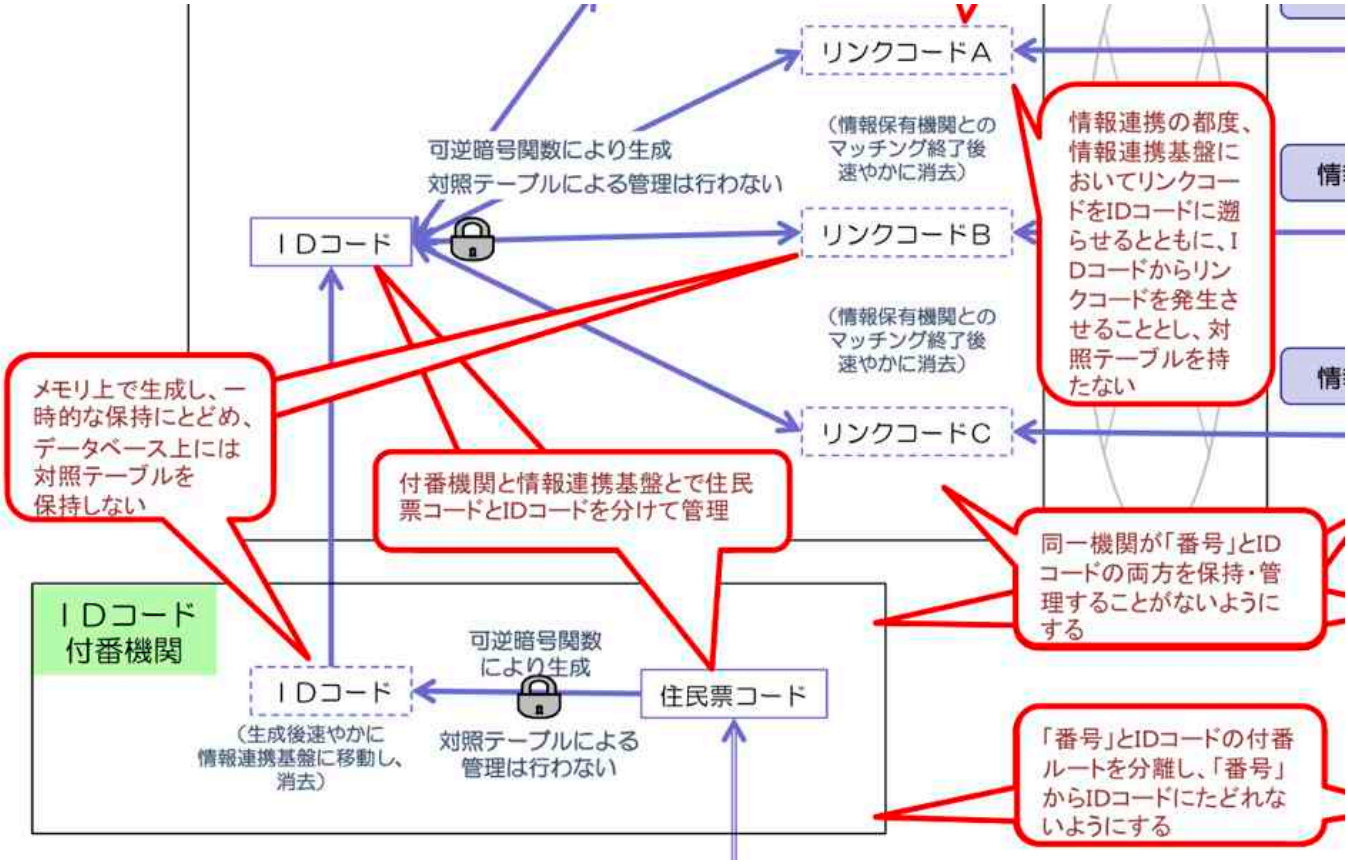
技術WG第2回資料2より

(4)「情報連携基盤」の運営主体

- 「情報連携基盤」の運営主体の案は総務省
- 総務省は別途「情報保有機関X」として参加し得る
- 同じ主体が両方を兼ねることの是非をどう考えるか

(5)「対照テーブル管理は行わない」？

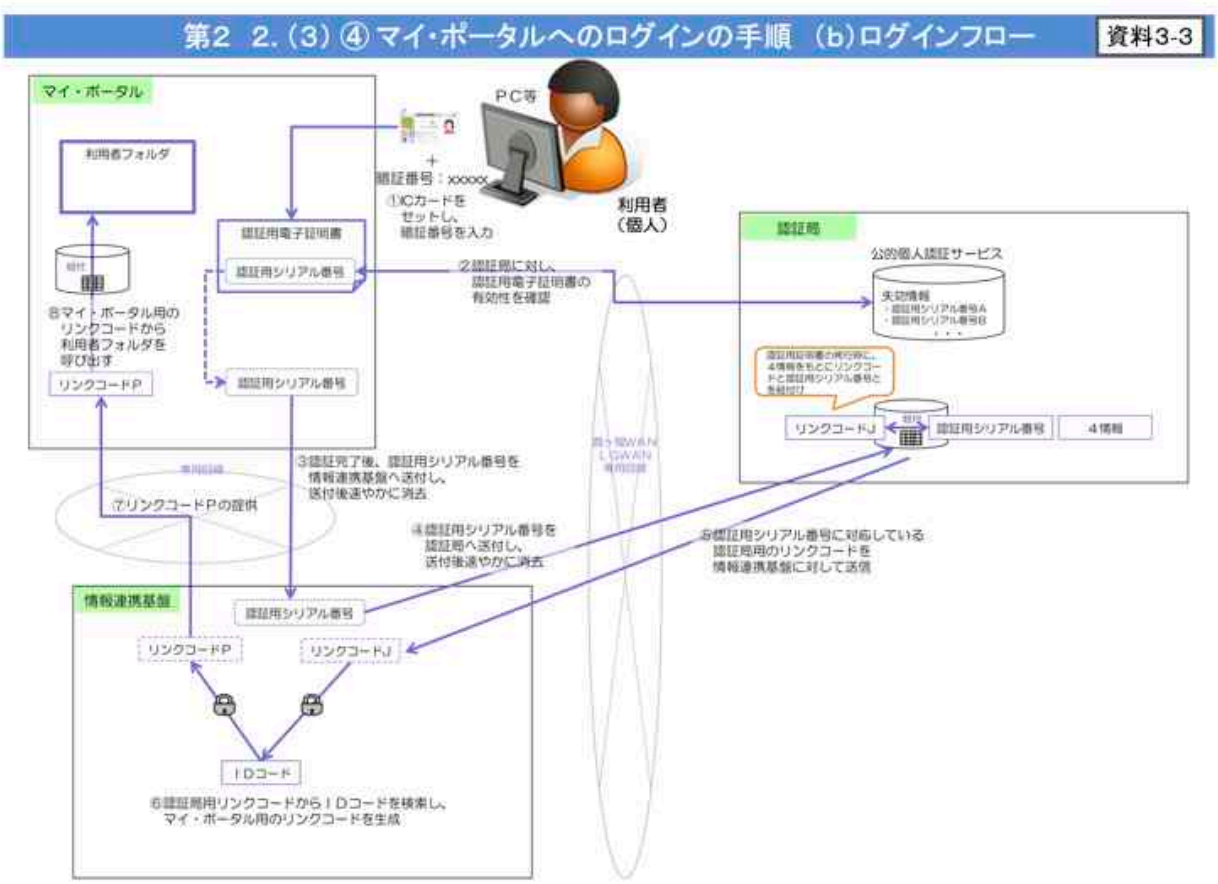
- 技術WG第2回資料2「番号制度 番号連携イメージ」
  - 「対照テーブルによる管理は行わない」「可逆暗号関数により生成」という記述がそこかしこに見られる
- 「対照テーブルによる管理を行わない」のはなぜ？
  - 違憲性を避けているつもりなのか？
  - 「2つのIDを紐付けて保管してはいけない」という原則がある？
- ナンセンスですよ
  - 「可逆暗号関数により生成」であれば、対照テーブルを持つのとまったく同じこと
  - 法的に何か違いがあるのですか？（法WGからの要求ですか？）
- デメリットが存在
  - 暗号関数は危殆化し得る（対照テーブルは危殆化しないのに）



技術WG第2回資料2より

(6) 2つのIDを持たない原則が一人歩き

- 技術WG第3回資料3-3「マイ・ポータルへのログインの手順 (b)」
  - 類い稀なる珍妙プロトコルになっている
  - 「認証用電子証明書」の「認証用シリアル番号」（Common Name）から「情報連携基盤」が「認証局」に「リンクコードJ」を求め、「リンクコードJ」から「IDコード」を介して「リンクコードP」を算出し、「リンクコードP」をポータルに返す
  - ナンセンス極まりない!!!!!!!
- どうしてそうなった？
  - 「2つのIDを持たない原則」のため、「リンクコードP」と「認証用シリアル番号」をポータルが紐付け保管が許されない（と勘違いしている？）
- 誤解に基づく設計
  - リンクコードPと認証用シリアル番号は共にポータル専用なので、紐付けてかまわないし、そうするのが当然の設計
  - 逆に、認証用シリアル番号を他サイトでも使う想定なら、それ自体が問題



技術WG第3回資料3-3より

総論

- (7) 技術WGと法WGの連携ができていない
  - 技術WGは、ナンセンスな法的要求を勝手に想定して検討
    - 最大限に法律面に配慮したつもりで無用な技術方式の設計を邁進
  - 法WGは、技術的代替方式の存在を知らないまま検討
    - 技術方式の選択に法律面が影響することの自覚が足りない

- (8) 拙速では
  - このまま内部からの異論が検討されることなく決定されるなら、私は、アプリケーションセキュリティとデータプライバシー技術専門の立場から、外野からの批判を開始せざるを得ない。