社会保障分野における安全で利便性の高い情報連携が地域住民にもたらす効果に関する検証成果について

～社会保障カード(仮称)の制度設計に向けた実証事業　～

各実証成果のまとめと今後の方向性について

平成22年8月31日

日本システムサイエンス株式会社

各コンソーシアムの主な実証サービス

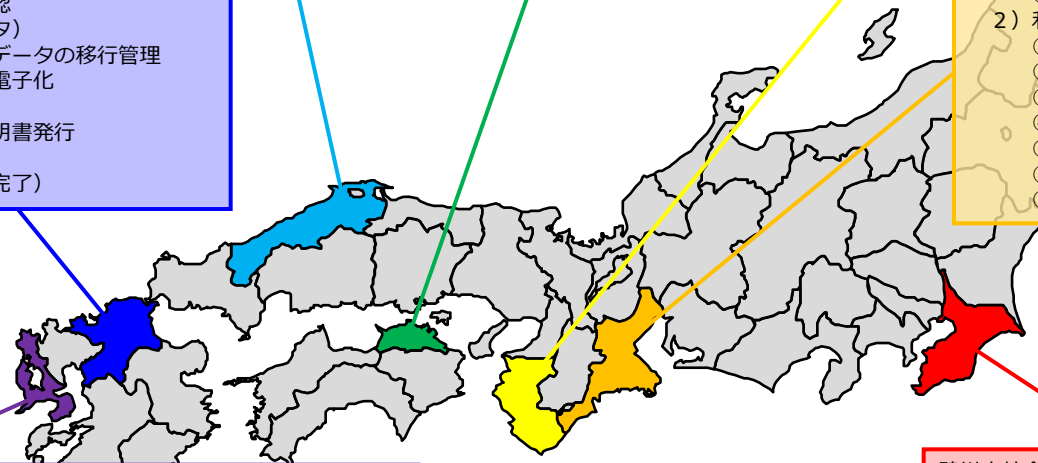
いずも医療カード利用推進コンソーシアム
1）医療機関向けサービス
①医療保険の資格確認
②健康診断結果
③診察予約
④診療情報
2）利用者向けサービス
①年金情報（実証ではダミーデータ）
②健康診断結果
③診察予約
④診療情報

かがわSSCコンソーシアム
1）医療機関向けサービス
①医療保険の資格確認
②かがわ遠隔医療ネットワークへの接続
2）利用者向けサービス
①医療保険の被保険者証の資格確認
②年金情報（実証ではダミーデータ）
③医療費通知情報
④健康診断結果
⑤PHRへの接続

わかやま安心医療・社会保障カードコンソーシアム
1）医療機関向けサービス
①医療保険の資格確認
②共通診察券
③健康情報管理 （体重・歩数・血圧・体温）
④診療情報
2）利用者向けサービス
①医療保険の被保険者証の資格確認
②介護保険の被保険者証の資格確認
③年金情報（実証ではダミーデータ）
④健康情報管理 （体重・歩数・血圧・体温）
⑤共通診察券
⑥診療情報

福岡経済情報基盤コンソーシアム
1）主な医療機関向けサービス
①医療保険の資格確認
②緊急時の医療情報
2）主な利用者向けサービス
①医療保険の被保険者証の資格確認
②年金情報（実証ではダミーデータ）
③乳幼児育児検診データ関連各種データの移行管理
④母子手帳の電子化出生手続等の電子化
⑤役所関係からのお知らせ
⑥住民票等のオンライン申請、証明書発行
⑦引越し時の住民情報の移行
（引越し先で転入・転出手続き完了）

日立製作所・名張市社会保障カード(仮称)実証コンソーシアム
1）医療機関向けサービス
①医療保険の資格確認
2）利用者向けサービス
①医療保険の被保険者証の資格確認
②年金情報（実証ではダミーデータ）
③健康診断結果
④医療費通知情報
⑤保健指導情報
⑥予防接種情報閲覧
⑦名張市からのお知らせ



おおむら社会保障カード（仮称）コンソーシアム
1）医療機関向けサービス
①医療保険の資格確認
2）小中学生サービス
①身体測定、体力測定、予防注射接種記録、出欠席の記録の閲覧
3）利用者向けサービス
①医療保険の被保険者証の資格確認
②年金情報（実証ではダミーデータ）
③健康診断結果
④医療費通知情報

鴨川市社会保障カード実証事業コンソーシアム
1）鴨川市役所
①亀田健保脱退者の鴨川市役所市民生活課での確認
2）医療機関向けサービス
①医療保険の資格確認
3）利用者向けサービス
①医療保険の被保険者証の資格確認
②年金情報（実証ではダミーデータ）
③健康診断結果
④医療費通知情報
⑤診療情報

まとめの内容

実証事業の狙い

- 情報基盤としてあるべき姿を整理・検証する
- 便利で安心安全なものと利用者に実感してもらう
- 制度・運用面等での課題を抽出する
- 発展的活用のモデルを探る

サービスとしての実証課題

- 便利で安心安全なサービスの提供
- 資格証としてのあるべき姿
- 公共サービスとしての発展的な活用モデル

技術としての実証課題

- 情報連携基盤としてのあるべき姿
- シングルサインオンによるサイト間連携
- セキュリティに関する安全性の検証

情報連携基盤の主な要件

- 給付調整やサービスの発展的な活用のために
- 利用者本人による情報のコントロールで
- ICカードのセキュア・チップに本人識別情報を格納して

今後の展開イメージ

制度・運用面での課題と今後の進め方

便利で安心安全なサービスの提供は

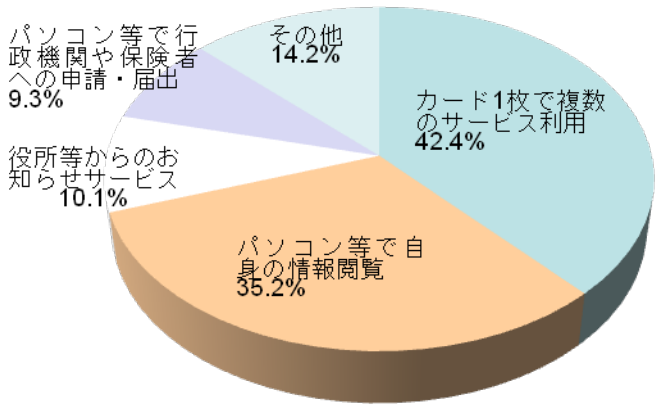
● ワンストップサービスや社会保障関連のサービスの利便性がアピールできました。

医療保険者や年金保険者などの異なる団体が提供する社会保障関連の情報を1枚のカードで安全に閲覧できることに興味を持っていただいた方の多くに便利さをアピールできました。実証事業以後の継続的な利用に関する意向もほとんどの方が利用したいとの意向を示されています。

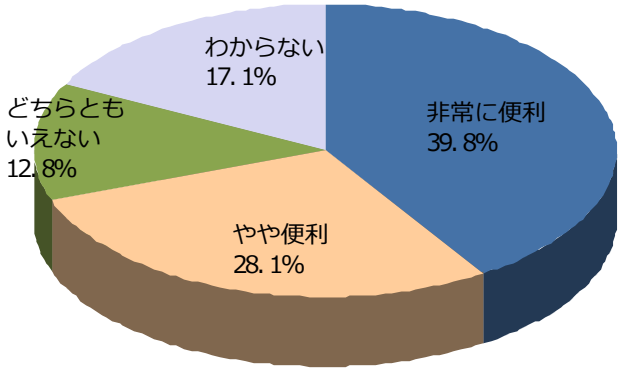
● サービスを継続して利用したいという意向が多いという結果が得られました。

プライバシー保護やセキュリティ対策については、イベントや説明会等での説明では十分に理解していただけていない結果となりました。しかし、継続利用したい意向が多いことから、利便性を優先してもよい程度の安全性は確保されていると感じていただけていると推測できる結果になっています。

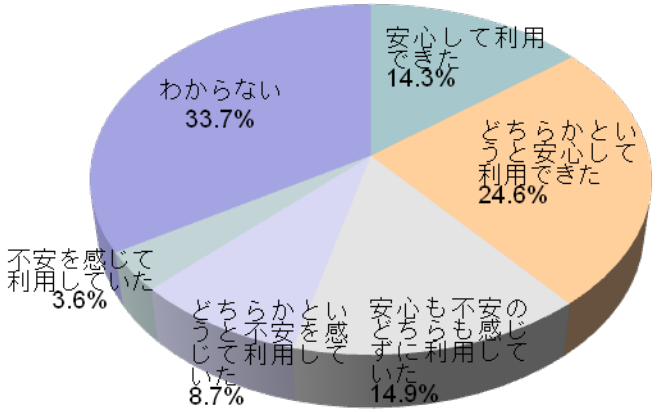
参加の動機 (N=1652)



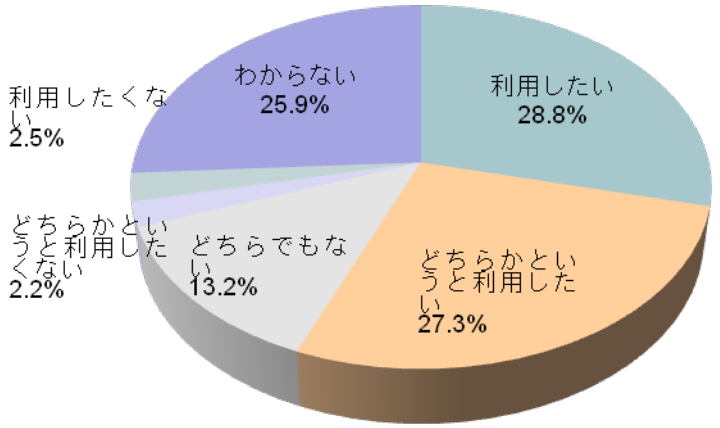
ワンストップサービスの利便性 (N=1689)



プライバシーの保護に関する安心感 (N=1652)



サービスの継続利用 (N=1650)



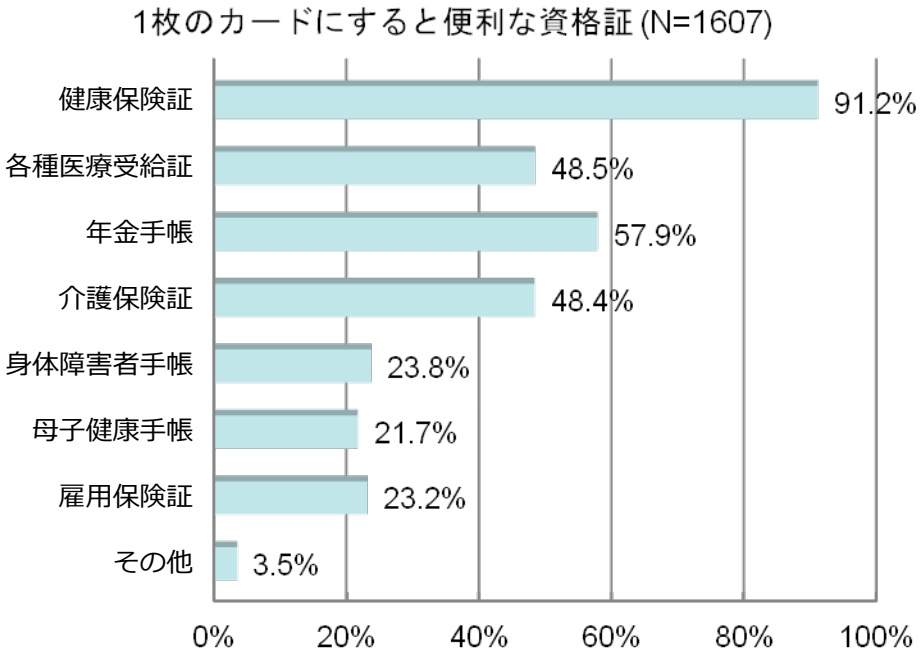
資格証としてのあるべき姿

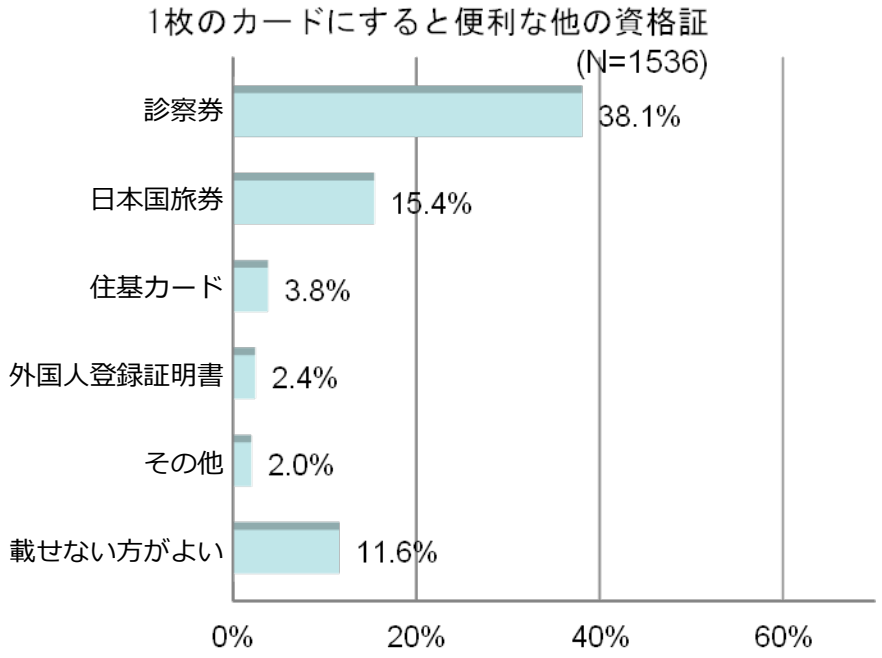
●医療・年金・介護に関わる社会保障サービスは、1枚のカードでサービスが受けられるようにすべきと考えます。

1枚のカードに集約したいサービスとしては、健康保険証、年金手帳、介護保険証、各種医療受給証の要望が多くなっています。年代別に見てみると、普段の生活において資格証を利用する人が身近にいる人や必要性が高い年代の人以外の要望が少なくない傾向があります。このため、社会保障関連のサービスに関して、1枚のカードでサービスを受けることに関する要望は総じて高いものと考えられます。

●その他の資格証については、関係の深い診察券についての要望が高くなっています。

他の資格証を載せない方がいいと積極的に答えた方を含め、社会保障に関わるカードに他の分野の機能を載せたいという積極的な要望はないと考えられます。しかし、医療に関わる診察券は、他の分野の資格証よりは要望も高く、医療機関で共通に使える診察券は発展的な活用モデルとしても要望が高くなっており、社会保障に関係するものの集約に関する潜在的な要望があると考えられます。





公共サービスとしての発展的な活用モデル

●社会保障関連の情報閲覧は、年金情報、健診情報などの要望があります。

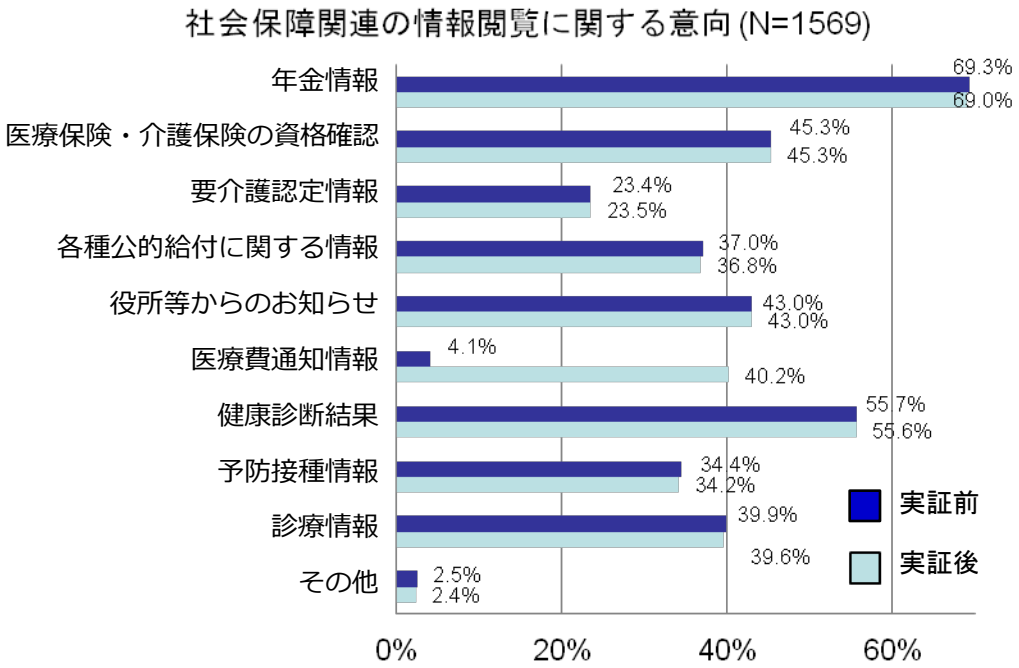
社会保障関連の情報閲覧については、期待通りの内容だったと考えられるため、ほとんどのサービスで実証の前後で利用意向に差がありませんでした。継続利用に関する意向も強いため、社会保障関連の情報閲覧に関する潜在的な要望は高いものがあると考えられます。

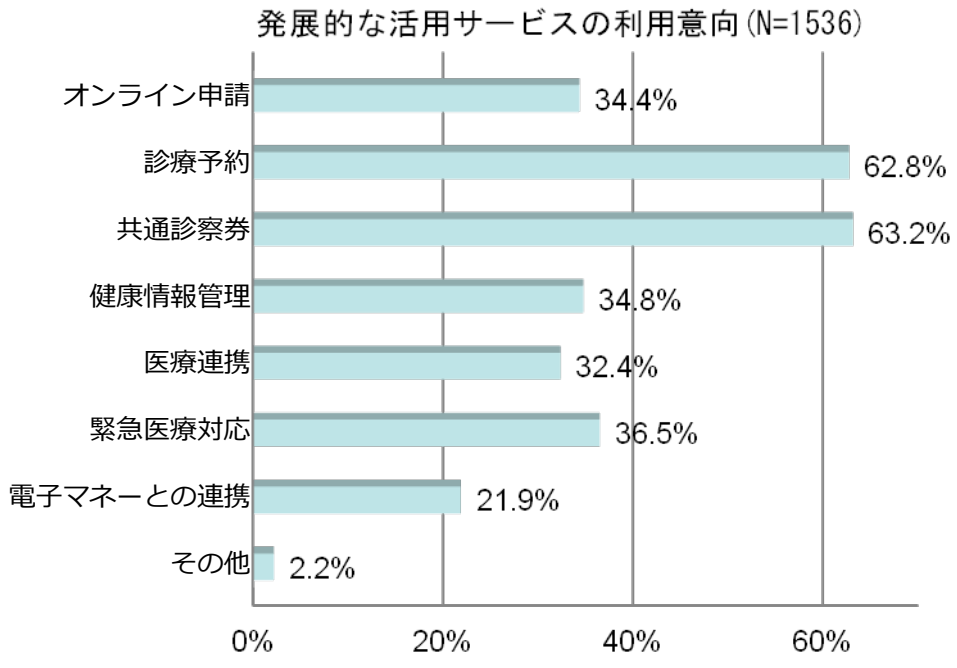
●発展的な活用として、診療予約や共通診察券など医療関連が有望です。

発展的な活用として、診察予約、共通診察券、オンライン申請など、情報連携基盤の目指す能動的な用途に関する強い要望があります。また、地域での健康情報管理、医療連携や救急医療対応など、必要な時に適切な医療が受けられる仕組みや、そうならないための健康増進に関わる活用に関する利用意向も強く出ています。

●医療費通知については、実証で正確に内容が理解できたため要望が伸びています。

医療費通知については、税務申告や健康管理等の応用に関するメリットについて実証事業の中で理解できたため、意向が増大したと考えられます。このように実証的なアプローチ、またはプロトタイピングで仮想的な利用環境で利用者の理解を深めながら利用要望が調査できると、正確な状況分析に基づいた展開計画の立案ができると考えられます。

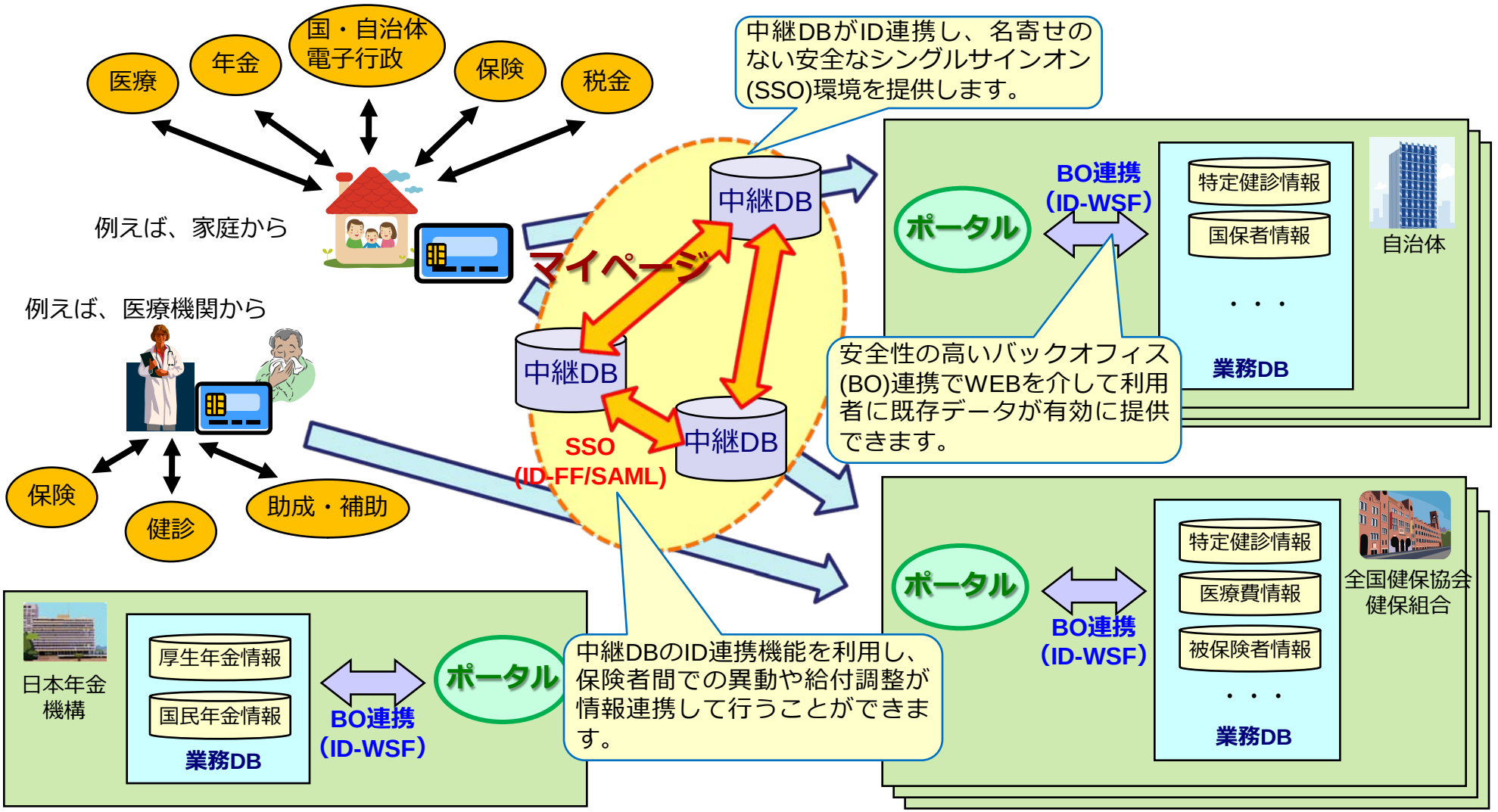




情報連携基盤のあるべき姿

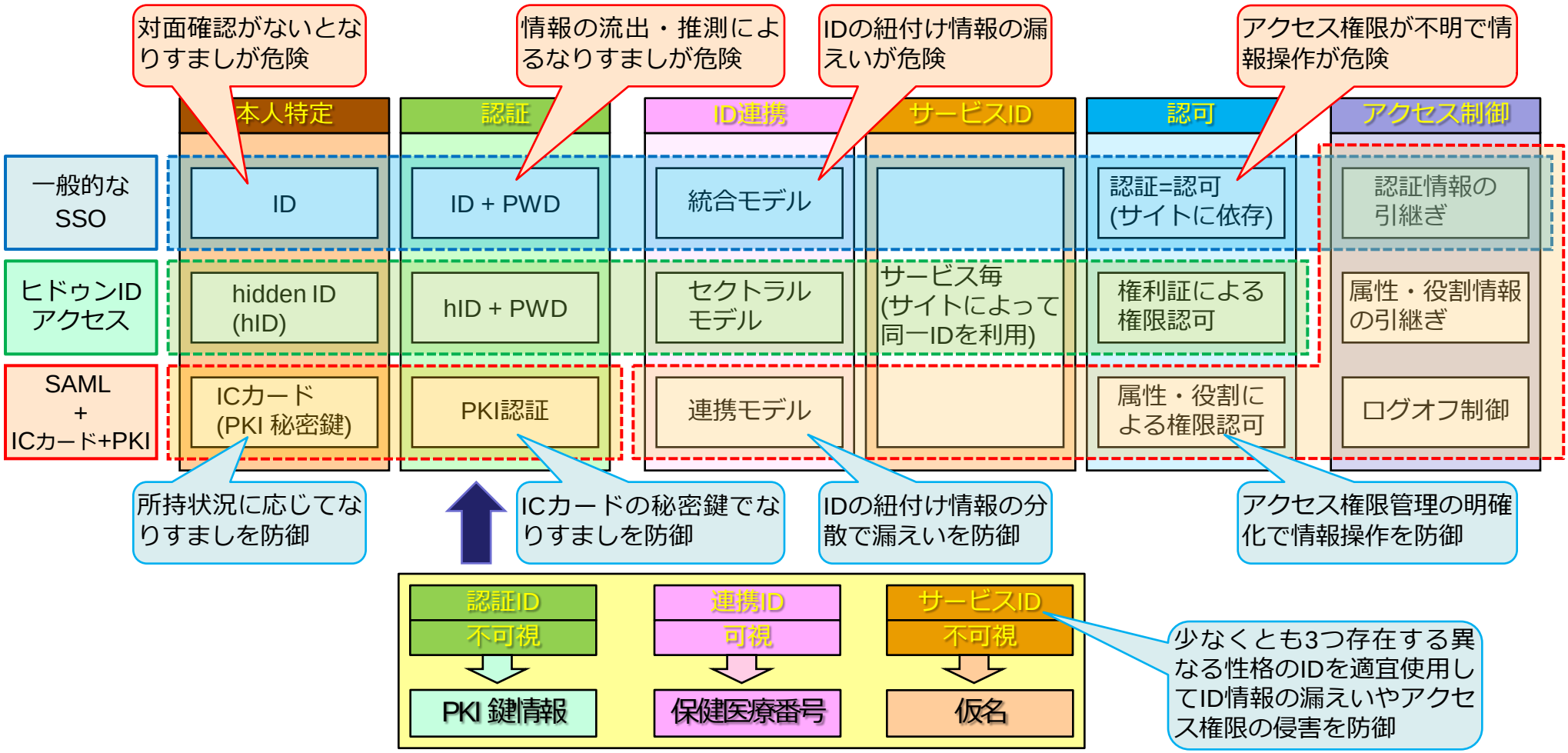
プライバシー保護の観点から
中継DBでセキュリティ対策

- ICカードを用いて他人によるなりすましの防止
- 情報の分散管理で情報漏洩の危険を抑制
- 本人によるアクセス履歴の確認で不正アクセスを抑止



シングルサインオン(SSO)によるサイト間連携

- **ヒドゥンIDアクセス方式やSAML2.0に基づいてサイト間連携を実現しました。**
  一般的なSSOが持っている本人確認、認証、ID連携、認可に関わるリスクに関して対策がなされた手法でセキュリティに関する問題がないことを検証しました。
- **ICカードと公開鍵基盤(PKI)を用いて安全な認証環境を実現しました。**
  PKIの秘密鍵をICカードのセキュアな部分に格納し、暗号化を使った認証を行うことによって本人を認証しました。ICカードの紛失や盗難に対する失効手続きを準備して所有者の実在性やなりすましを検査しました。



セキュリティに関する安全性の検証

運用について各種セキュリティ・ポリシーの策定

- CP/CPS
- 個人情報保護方針
- 運用手順書　　..等

構築についてセキュリティ評価のチェックシートの策定

- 全体のセキュリティ
  関係する拠点での通信ポリシーの確認
- 外部接続のチャネル・セキュリティ
  利用者やサービスに関連した法人間の通信に関するセキュリティ基準
- 拠点のチャネルセキュリティ
  通信設備が置かれた拠点のネットワーク構成、情報やサーバの配置などのセキュリティ基準
- オブジェクト・セキュリティ
  WEBシステムやサイト間連携のセキュリティ基準
- リモート保守サービスの利用
  外部にリモート保守を委託する場合のセキュリティ基準

- データの利用やマルチサイト連携など、全国的な運用に当たっては下記のような事項についてセキュリティ基準を統一的なものにすべきと考えます。
  - セキュリティ基準の精度を保証
  - 監査の厳密さを保証
  - 新しい技術や脅威に対応
- 国としてセキュリティ基準を維持・監査するための第三者機関を設置すべきと考えます。

  情報連携基盤は、複数の法人組織を相互に接続して業務に関する要求や応答のメッセージを交換します。このような複合システムは、一部のセキュリティ対策が弱い組織に合わせてセキュリティ強度が落ちることがあります。これを防ぐには、本実証事業で実施したようなセキュリティに関する安全性を担保する基準を明確にするとともに、これが常に維持されていることを監査できる体制の構築が必要になります。このため、このようなセキュリティ基準の維持・監査を客観的に行う第三者機関が必要と考えます。

ポリシー遵守と監査の結果

- チェックシートによるセルフチェックでは、実証システムにおいて運用上問題ないレベルのセキュリティ基準は達成できてると考えています。
- 各地域でサービスの実現のために接続された既存のシステムのセキュリティレベルと本実証のセキュリティ基準の整合を取るため、各地域の運用などにかなりの影響が出たと考えています。

給付調整やサービスの発展的な活用のために

保健医療番号を導入すべきと考えます。

できるようになること

- 医療保険者と介護保険者の間の制度間での給付調整
- バックオフィス連携による制度内異動に関わる情報の通知 (無保険状態の回避)
- 年金からの介護保険料等の源泉徴収

医療保険に関するメリット

利用者	手続き漏れの防止と手続きの簡素化
保険者	各種通知等のコスト、医療費請求の過誤調整事務の削減
医療機関	資格未確認による未収金の低減
自治体	本人の特定に関する事務負担の軽減

健診情報閲覧に関するメリット

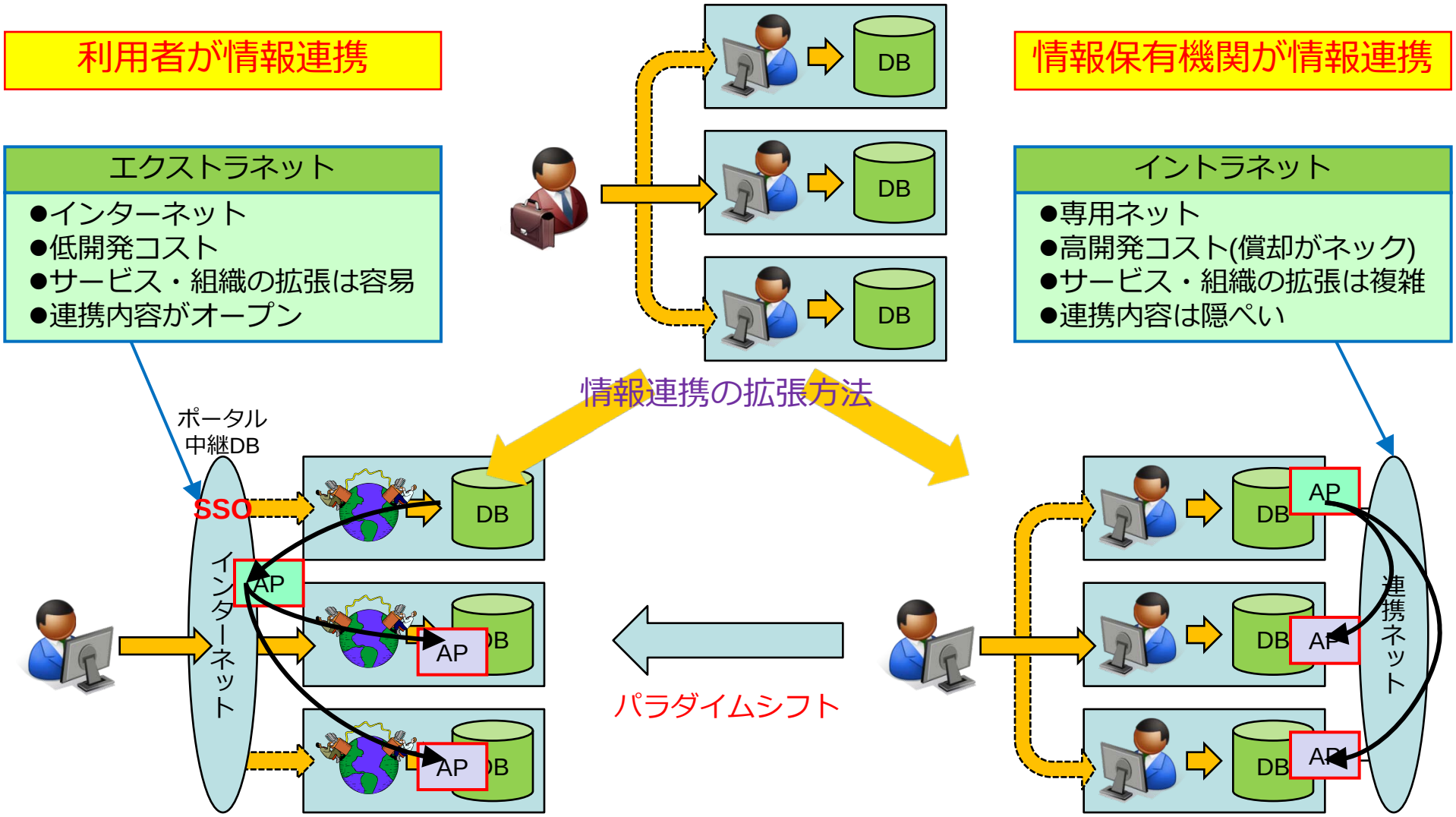
利用者	生活習慣の改善による健康増進
保険者	保険者内で異動があった場合の健康情報の一元的管理

社会保障と密接な関係のある共通診察券や診療予約などの医療系の発展的な活用モデルを社会保障サービスの一つとして取り込むことができます。さらに、医療情報や健診情報の共有が医療機関や地域を超えてできるようになります。これにより、利用者の利便性がさらに増すことが期待され、システム全体の利用率を向上させることができます。

利用者本人による情報のコントロールで

●情報の流れの可視化と既存リソースの流用ができるように実装方法を検討すべきです。

ポータルを活用して制度間での連携を実現することにより、制度毎の組織を単位としてオブジェクト指向のシステム設計や開発ができるようになります。また、これによって開発がポータルなどの一部の連携機能や接続I/Fに絞られるため、開発コストを抑制することができます。



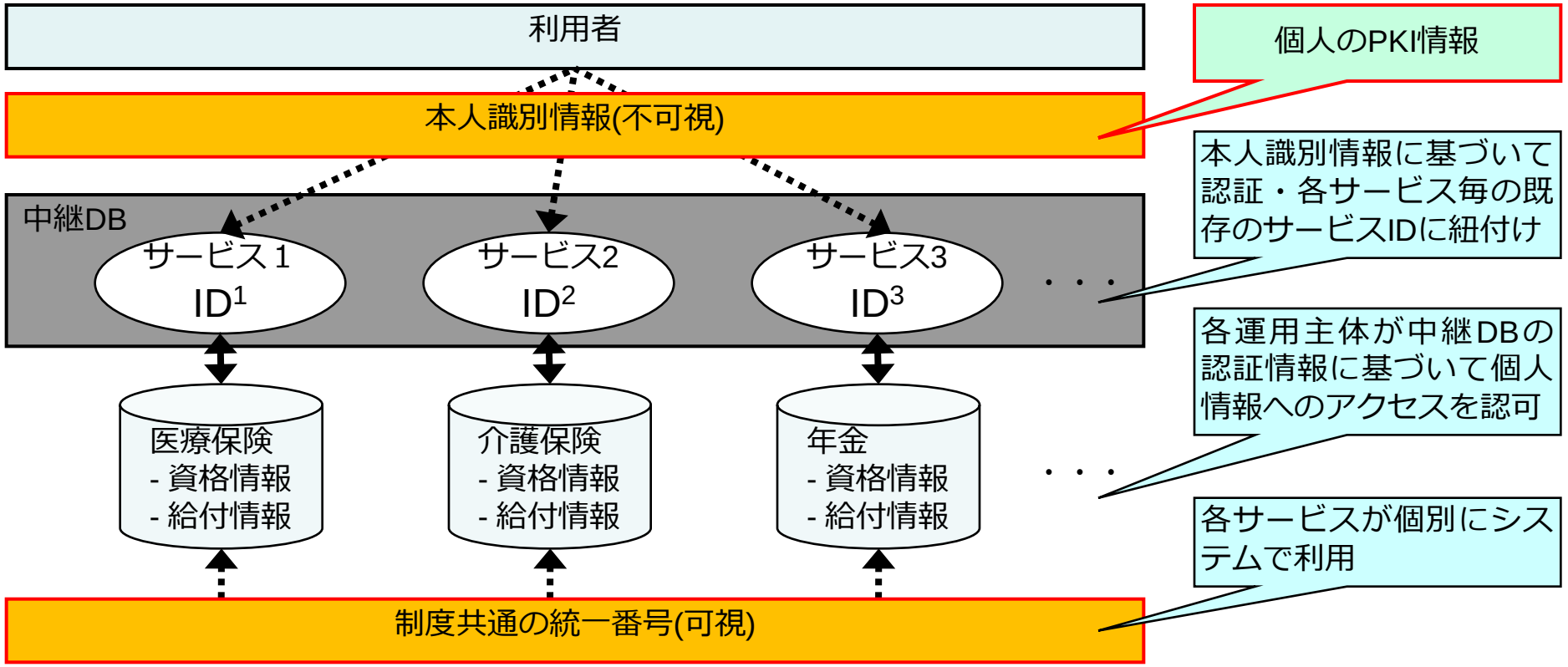
ICカードのセキュア・チップに本人識別情報を格納して

- 情報の紐付けに用いる券面表記が必要な制度共通の番号と認証に用いる本人識別情報を分離して用途に応じて使い分けてリスクを軽減するべきと考えます。

  制度共通の統一番号は、医療機関や自治体、医療保険者、介護保険者、年金保険者等の運用を考えると、カードやカルテ等への「表記が可能」という要件があります。しかし、本人識別情報が表記可能な場合、中継DBへの攻撃によって発生する個人情報の漏えいリスクが増大することに関する問題が指摘されています。

- ICカードと公開鍵基盤(PKI)を用いて厳重な個人情報の保護を図れる仕組みとすべきと考えます。

  ICカードのセキュアな部分でPKIの秘密鍵を発生させて隠ぺいし、この本人も知らない情報を用いて暗号化を使った認証を行います。ICカードの紛失や盗難に対する失効手続きが準備され、所有者の実在性やなりすましが確認できるため、現時点では電子的に最も安全な方式と考えられます。このため、公的個人認証の電子証明書及びその格納媒体である住基カードを活用することは、費用対効果の観点から有用と考えます。



今後の展開イメージ

●ICカードを用いて本人による情報コントロールを実現します。

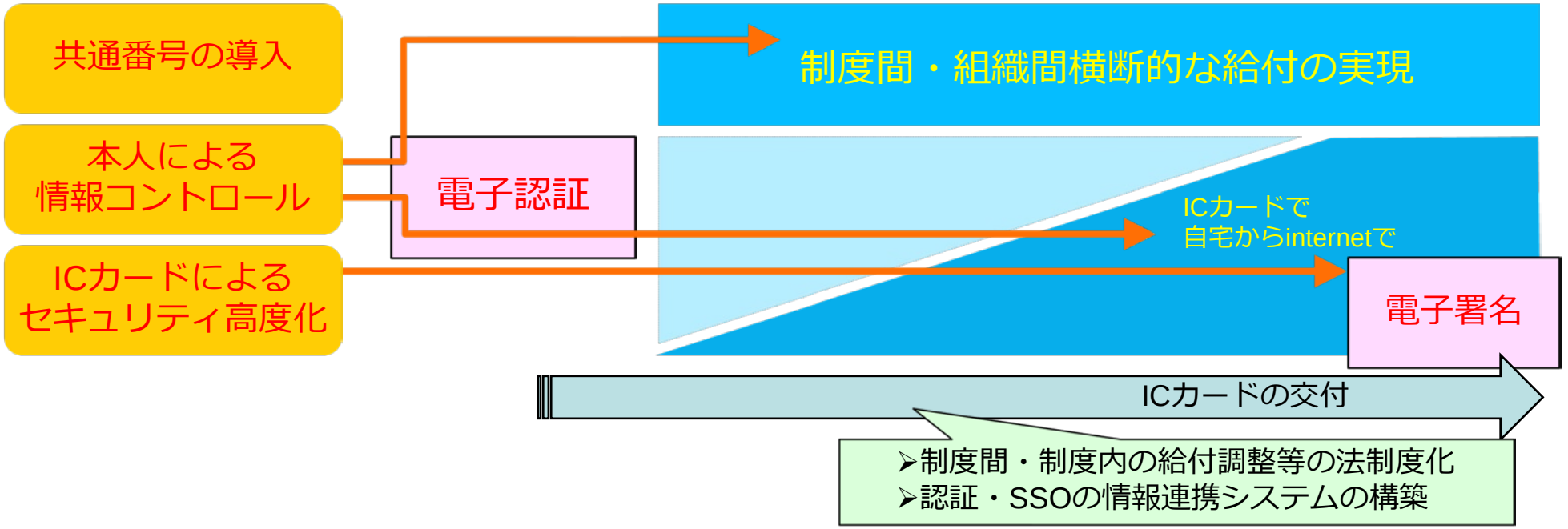
PKI技術をICカードと組合せることによって電子的に本人特定や偽造対策を可能にし、これをキーにして情報の保存や利用を情報の持ち主である本人自身によって行えるようにします。これによって、情報へのアクセスについて本人がモニタできるようになると同時にシステムの管理状況を監査することができるようになります。また、電子署名を利用した電子申請など、情報の能動的な活用が可能になります。

●情報連携基盤を早期に整備して保険者間での事務負担を軽減します。

旧制度と新制度の混在による業務負荷の増大を抑えるため、保健医療番号による資格確認サイトはすべての医療機関や保険者が利用できるように施策を打ちます。このため、医療・年金・介護それぞれの保険者と紐付けるため、社会保障及び保健医療番号に関する台帳を整備してデータベース化します。年金・介護など制度毎に開始時期を決めて情報連携を制度・組織の組み合わせで実施していきます。

●移行期間における業務の負担を軽減しつつ、速やかな移行ができるようにします。

ICカードの配布は、耐用年数や発行に関わるリソースやコストの平準化に配慮して順次行っていく必要があると考えらます。このため、ICカードと既存の健康保険証等が併用される移行期間が発生し、この期間には各保険者や医療機関などの関係する機関に日常の業務を二つの社会インフラに沿って運用していただく問題があります。また、この移行期間が長引くことは国民のメリットにも反します。このため、移行期間における関係各機関の運用に関わる負担を軽減するよう努力しつつ、速やかに移行できるようにします。



制度・運用面での課題と今後の進め方

本実証事業で抽出された主な課題

●サービス
- 自治体負担の福祉・公費等に関する資格確認の実現
- 事業体にある既存のDBとの接続とサービス連携
- 既存の医療ネットを含めた医療連携基盤の整備
- 自治体独自のサービス拡張に対する自由度
- 利便性を高める民間サービスとの連携

●制度設計
- 個人情報保護を考慮した関連法制度の準備
- 地域間での異動が可能なカードの活用
- 多様なアクセス端末の提供
- 民を活用した情報連携基盤の整備
- 異動・給付調整等の組織間での情報連携方法
- 社会保障制度に関する教育の充実
- 周産期・死亡等に関わる運用方法
- 自治体を活用した多様なサービスの提供

●情報連携基盤技術
- 第三者認証機関を活用した認証リソースの共有
- 関連機関への機器等リソースの早期配備
  - SSOに向けた環境整備
  - バックオフィス連携済みの機関との連携方式

今後やっていくべきこと

●サービス基盤の形成

本実証事業でできなかった「実データを利用した安全性や利便性のさらなる検証」

●制度の整備

抽出された制度設計に関わる課題に基づいた社会保障の給付実現に向けた法制度の整備

●情報連携基盤の構築準備

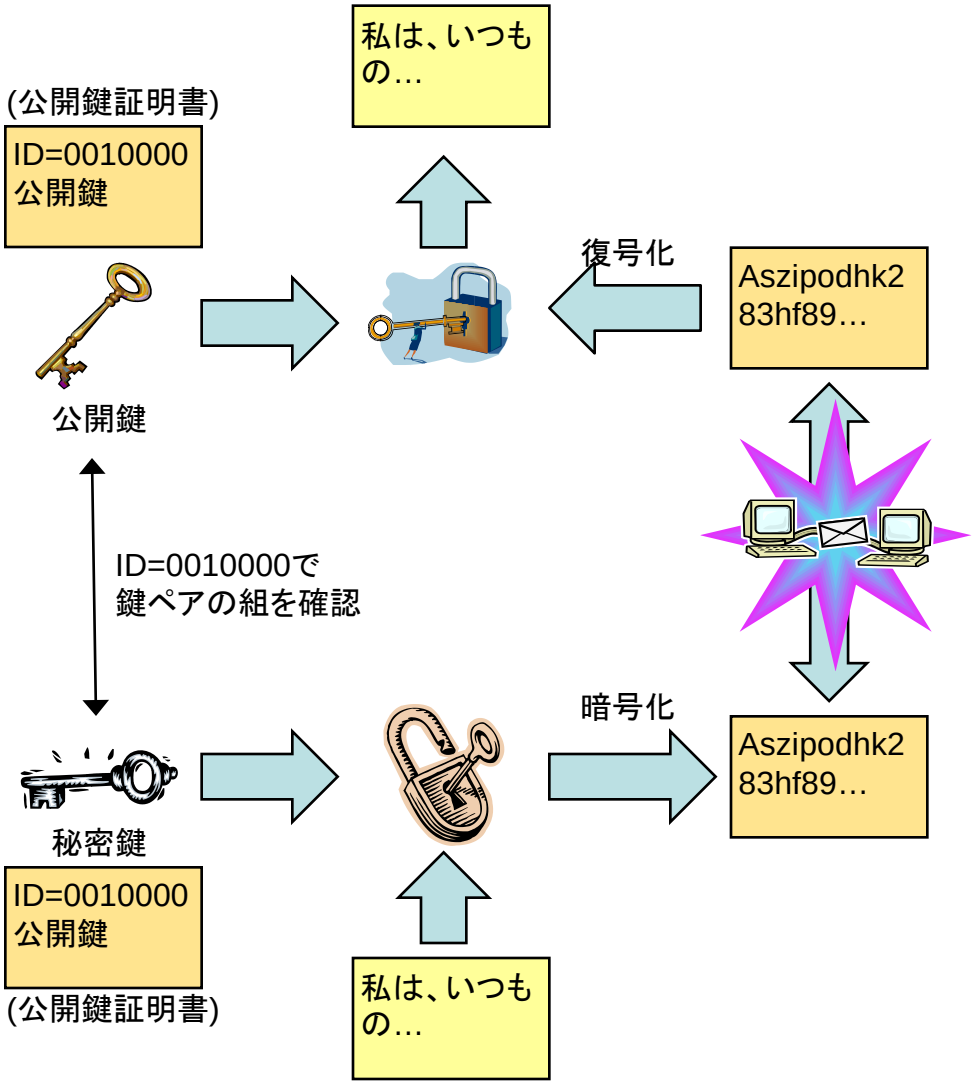
情報連携基盤の基盤となる社会保障に関する台帳の整備や統一技術仕様の整備

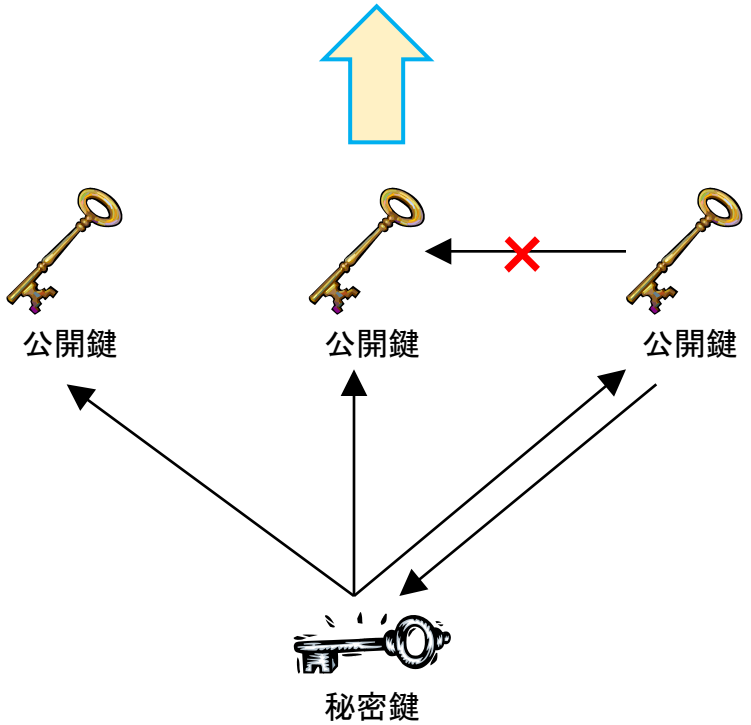
(参考資料 1)

安全な公開鍵基盤(PKI)認証

この暗号化の仕組みを使って認証

- 秘密鍵をICカード上のチップ内で生成して外に出さずに隠ぺいする。所有者本人も知らない認証情報を生成できます。
- 紛失・盗難等によるクレジットカードのように失効手続きができます。
- 物理媒体なので紛失・盗難に気付きやすい。また、よく使う発展的サービスがあるほど気づくサイクルが早くなります。





- 公開鍵と秘密鍵のペアでしか暗号化・復号化ができません。
- 公開鍵を配った人とだけ暗号化通信や認証ができます。
- 秘密鍵を持っている人から公開鍵を持っている人には暗号化して同報ができます。
- 公開鍵を持っている人から秘密鍵を持っている人には個別通信しかできません。

(参考資料 2)

実証事業におけるセキュリティ評価のためのチェックシート

検討項目		ガイドライン	セキュリティ対策状況の判定	
大中項目	小項目	該当項目	対策内容	判定基準
1 全体のセキュリティ				
1 通信ポリシーの管理	1 接続相手の確認	6.11 B-1 6.11 B-3	自治体、保険者、医療機関、保守会社等の社会保障サービスに関わるサービスプロバイダが本「チェックシート」の各項目について、技術的な対処、システム設定による対処及び運用による対処の総合的な対策が判定基準を満たしている。	自治体、保険者、医療機関、保守会社等の社会保障サービスに関わる、すべてのサービスプロバイダが本「チェックシート」の判定基準を満たしてサービスが提供されていることを示すエビデンスを保管・管理している。
	2 接続先拠点との通信に関する合意	6.5 B-5	一般人や異なる法人と通信を行う場合は接続相手の確認を行った上で相手に応じた接続に関する合意を文書で交わしている。	文書によるサービス内容・運用形態の確認と合意がされている。 合意された内容に沿ったVPN通信の設定や運用がなされていることを確認している。
2 外部接続のチャネル・セキュリティ				
1 個人からのアクセス	1 アクセス回線	6.5 B-1 B-2 B-3 6.11 B-1 6.11 B-2 6.11 B-3 6.11 C-1 6.11 C-2 8.1.3 D-1①	個人のアクセス回線としてインターネットを想定し、本人認証する場合及び個人情報や重要な情報を伝送する場合には暗号化などの安全対策がされている。	認証情報や個人情報を伝送する場合、アクセスプロトコルとして以下のいずれかの方式が採用されている。 ・SSL 3.0と同等またはそれ以上の安全性のある方式 ・TLS 1.0と同等またはそれ以上の安全性のある方式
				暗号化アルゴリズムとして以下のいずれかを採用している。 ・3DES-CBC ・AES128-CBC ・3DES-CBCと同等またはそれ以上の安全性のある方式
				認証アルゴリズムとして以下のいずれかを採用している。 ・HMAC-SHA1 ・SHA256 ・HMAC-SHA1と同等またはそれ以上の安全性のある方式
				鍵長(DHグループ)として以下のいずれかを採用している。 ・Group2（1024ビット） ・Group14（2048ビット）
2 法人間のVPN接続	1 アクセス回線	6.11 B-3	IP-VPN、広域イーサネット、専用線、ISDN等の通信会社が提供する専有型通信サービスを利用するか、オープンネットワークのような共有型通信サービスを利用している。	(1) 通信会社またはサービス・プロバイダが提供する以下の回線 ・IP-VPN ・広域イーサネット ・専用線 ・ISDN (2) 2-2項の認証・暗号化通信要件を満たした下記の回線 ・インターネットVPN ・情報スーパーハイウェイ ・閉域網
			異なる法人間を接続する場合は、必ず接続セッション毎に認証した上で接続する。	通信会社またはサービスプロバイダから配布された以下の情報に基づいて認証している。 ・秘密鍵と公開鍵証明書 ・自動鍵配送機能によってセッション毎に割り当てられた共通鍵 ・IDとワンタイムパスワード
	2 認証・暗号化通信	6.5 B-1 B-2 B-3 6.11 B-1 6.11 B-2 6.11 B-3 6.11 C-1 6.11 C-2 8.1.3 D-1①	IKEを用いて認証及び通信モードを決定して鍵交換を行っている。	通信モードとして以下のいずれかを採用している。 ・メインモード ・アグレッシブモード
				暗号化アルゴリズムとして以下のいずれかを採用している。 ・3DES-CBC ・AES128-CBC ・3DES-CBCと同等またはそれ以上の安全性のある方式
				認証アルゴリズムとして以下のいずれかを採用している。 ・HMAC-SHA1 ・SHA256 ・HMAC-SHA1と同等またはそれ以上の安全性のある方式
				鍵長(DHグループ)として以下のいずれかを採用している。 ・Group2（1024ビット） ・Group14（2048ビット）

(参考資料 3)

出生・交付時における運用フローの検討例