社団法人　電子情報通信学会
THE INSTITUTE OF ELECTRONICS,
INFORMATION AND COMMUNICATION ENGINEERS

信学技報
IEICE Technical Report
SITE2011-28(2011-12)

電子行政における個人情報の保護と利用の両立を図る情報連携システムに関する研究　―第１報

辻井 重男† 山口 浩† 五太子政史† 角尾 幸保‡ 井堀 幹夫‡† 山本 拓真‡‡

†中央大学研究開発機構 〒105-0123 東京都文京区春日 1-2-3
‡NEC 情報・メディアプロセッシング研究所 〒211-8666 神奈川県川崎市中原区下沼部 1753
‡†東京大学高齢社会総合研究機構 〒277-8589 千葉県柏市柏の葉 5－1－5 第 2 総合研究棟 209
‡‡株式会社カナミックネットワーク 〒141-0031 東京都品川区西五反田 8-1-14 最勝ビル
E-mail: gotaishi@tamacc.chuo-u.ac.jp

あらまし 先ず，電子行政を，精神構造，社会システム，技術システムの 3 階層として捉え，各々の階層について概説した後，現在，内閣官房を中心に政府で検討が進められている情報連携基盤について技術システムの立場から考察する．情報連携基盤は，認証機能，番号機能，情報連携機能の 3 機能を有するが，認証機能については，公的個人認証などの実績があるので，これらを利用すれば良く，番号機能については，個人情報保護を中心に政府で議論が深められている．しかし，情報連携機能については，考察が進んでいないように見受けられる．情報連携基盤の大きな目的は，個人情報を最大限保護しつつ，これを国民のために活用することにある．本論文では，暗号技術などの利用により，個人情報の保護と活用の間の矛盾を可能な限り超克し得る技術システムの構成法を提案する．

キーワード 電子行政，個人情報，プライバシー，医療・介護，公開鍵暗号，Pailler 暗号，RSA 暗号，PPDM，クラウドコンピューティング，意味検索，情報連携基盤

On Electronic Government System for Overcoming Contradiction between Protection and Utilization of Personal Information and Privacy －Part 1－

Shigeo TSUJII† Hiroshi YAMAGUCHI† Masahito GOTAISHI†

Mikio IHORI‡ Yukiyasu TSUNOO‡† Takuma YAMAMOTO‡‡

†Faculty of Engineering, First University 1-2-3 Yamada, Minato-ku, Tokyo, 105-0123 Japan
‡Information and Media Processing Laboratories, NEC Corporation
1753 Shimonumabe, Nakahara-ku, Kawasaki, Kanagawa, 211-8666 Japan
‡†Institute of Gerontology, University of Tokyo 7-3-1 Hongo, Bunkyo, Tokyo, 113-8656 Japan
‡‡Kanamic Network Co. Ltd. Saisho Bldg., 8-1-14 Nishi-Gotanda, Shinagawa, Tokyo, Japan, 141-0031
E-mail: gotaishi@tamacc.chuo-u.ac.jp

Abstract First the concept of 3 layers of electronic government is proposed. 3 layers are mental, social system, and technological system layers. In this paper, electronic government system to overcome contradiction between protection and utilization of personal information and privacy is proposed based on public key encryption, privacy preserving data mining and private information retrieval.

Keyword electronic government, personal information, privacy protection, Pailler cryptosystem, RSA cryptosystem, privacy preserving data mining, private information retrieval

1. 電子行政の現状と研究の目的

日本の電子行政(電子政府・自治体)の遅れは，国民にとって不幸なことであり，国家の衰退につながりかねない．望ましい電子行政の姿は：

1. 個人情報が保護された環境の中で，
2. 国民一人一人が，自宅にいながら，行政機関に蓄積されている自己情報を簡単に確認し，必要な行政サービスをプッシュ型で受けることが出来，
3. 行政は，国民の全てに対して，そして産業界などの民間組織に対しても，公平な行政サービスを効率よく展開できる

というものである．

このような観点から見ると，プライバシー保護に関して寛容な韓国は可なり進んでいて，2010 年の世界各国の電子行政の進展度に対する国連の評価では，世界 1 位であるのに対し，日本は 17 位である．

歴史や文化の相違もあり，一概に比較は出来ないが，最大多数の幸福・最小不幸社会の実現のために，電子行政の全体最適化と総合的デザインが急がれる．

日本の電子行政の遅れの要因は多岐にわたり複雑であるが，

1. プライバシー保護が観念的に先行し，
2. 煩雑で分り難い行政手続きのため，納税，年金，福祉，介護・医療，災害等の面で，多くの国民に，年金情報のミス，不透明性や不公平性などのしわ寄せが来ていることに対する理解が不十分であった

ことが大きな要因として挙げられる．

個々の行政手続きは電子化されていても，例えば，介護者の多くは，ある介護サービスの処理が終わると紙にプリントして，次のサービスに渡し，そこで再びデータ入力しなければならないというような非効率さにより，要介護者に向かい合う時間が少ないという悩みを抱えている．ある自治体で，電子化によるサービス連携を試みたところ，要介護者に向かい合う時間とパソコンに向かう時間の比率が逆転したそうである．

このような状況を打破し，電子行政を進展させるために，精神構造面，法制度面，技術面などからの多面的・総合的な改革と検討が必要である．本研究は，韓国などと異なり，プライバシー・イデオロギーが浸透している我が国において，技術面から，個人情報の活用と保護の矛盾相克を可能な限り止揚する手法とシステムを開発し，電子行政に発展に寄与することを目指すものである．

本研究では，現在，内閣官房を中心に構想が固められつつある情報連携基盤の枠組みを前提として，国税庁や年金機構などの中央諸官庁，及び，多くの地方公共団体(自治体)や医療機関などの情報保有機関が有する個人情報を保護しつつ活用するための技術システムを開発することを目的とする．

情報連携基盤は，認証機能，番号機能，情報連携機能の 3 つの機能を有する．認証機能については，公的個人認証の実績があり，また，番号機能に関しては，内閣官房を中心に鋭意検討されているが，諸官庁，自治体などの情報保有機関との情報連携機能に関しての検討は進んでいないように見受けられる．

本研究では，電子行政を精神構造，社会システム，技術システムの 3 階層からなるシステムとして概観した後，情報連携機能を対象として，自治体や医療機関関係者などとの討議を通じて得られた知見を基に，現実的場面を想定しつつ，独自技術を開発し，社会的実装に適したシステム構成を提案する．

2. 電子行政の 3 階層―精神構造・社会システム・技術システム

国民のための行政を進めるには、図 1 に示すように、個人情報の保護と合わせて、年金、災害時対応、医療・介護などの面で不利益を被る国民を極小化しなければならない。そのためには、データ処理の正確性の向上と効率化を進め、自己情報の本人への迅速な提供が可能な電子行政システムを構築しなければならない。

電子行政システムは図 2 に示すように、精神構造、社会システム、技術システムの 3 階層として捉えることが出来る。精神構造は、各国の歴史と文化により異なるが、日本の場合、第 2 次大戦中の影響も遠因となって、プライバシー・イデオロギーが支配的な精神構造が長く続き、電子行政を積極的に推進する機運が盛り上がらなかった。中央官庁や自治体による個人情報の管理は確かに大きな課題ではあるが、上に述べたように、電子行政の遅れにより、年金、災害時対応、医療・介護などの面で国民にしわ寄せが来ないようにしなければならない。このような意味で、電子行政はリアリズムに立脚すべきである[1]。

プライバシー・イデオロギーの面からのみの電子行政論議は、太平洋戦争時における多くの文化人達の議論を連想させる。昭和 17 年 7 月に開催された、歴史に残る座談会「近代の超克」には、河上徹太郎、小林秀雄，亀井勝一郎，西谷啓治，竹内好など、当時の著名な思想家や文化人が一堂に会したが、この座談会を中心に当時の多くの論客達が、英米と日本の間の一桁以上の経済力格差という現実を認識せずに精神論を展開しているように見受けられる[3]。大哲学者、西田幾多郎も、太平洋戦争の始まる前年の昭和 15 年、ある論説で「自己矛盾的同一的世界の形成原理を見出すことによって世界に貢献しなければならない。そのことが皇道の発揮と言うことであり、八紘一宇の真の意義でなければならない。」と述べている。戦争の正義と言う議論はさておくとして、現状認識を無視したイデオロギー先行は、多くの人々の不幸を招く一因となったことを忘れてはならない。

電子行政に話を戻せば、プライバシー・イデオロギーのみを絶対視して、年金、医療・介護、災害、生活保護などの現実認識を欠くことは国民にとって不幸である。とは言え、公務員などによるプライバシー侵害は、国民にとって不快であるのみでなく、金銭面などでの実害を招く恐れもあるので、次に述べるように、法制度や技術の立場から、十分な対策を要することは勿論である。

電子行政の推進には、第 2 層の法制度、行政システムや官民連携などの改革が必要である。電子手続などの制度を変えずに、電子署名などの技術を導入しても、電子行政を進めたことにはならない。例えば、公的個人認証は、現在、電子署名にのみ利用に制限されているが、国民が随時、自己情報をマイ・ポータルから確認できるように、広く認証用途にも利用できるように改正すべきである。また、信用度の高

い民間への用途にも拡大すべきであろう。民間用には、電子署名法が施行されているが、このように官と民にわかれて電子証明に関する法律が定められている国は珍しいようである。

社会システム層に関しては、多くの抜本的課題があるが、本研究の対象ではないので、これ以上述べることは差し控える。

電子行政の効率化、正確性の向上、及び、個人情報の保護と活用の矛盾の超克には第3層の技術システムが大きな役割を果す。その概要を3に述べる。

3. 情報連携機能

電子行政の技術システムは，図3，図4に示すように情報連携基盤を中心に構成される．太枠内は，次の通り本研究で開発する独自技術である．

1. 異種データベース結合技術の開発
2. 個人情報を保護しつつ活用するための暗号技術の開発
3. 個人情報を保護しながら，問い合わせ，検索，及び問題解決の可能なシステムの開発
4. 組織暗号による秘匿情報の伝送・アクセス方式の開発

を行う．以下，それらの概要を述べる（図 5，6，7，8 参照）．

1. 行政サービス毎に異なるデータベース規格をコーディネイトして，バック・オフイス連携を図り，行政の効率を上げるための開発:
   NEC ソフト(株)が開発を進めてきたデータコーディネータの構成を図5に示す．これを基盤として，今後展開される情報保有機関のサービスに個人情報保護機能を盛り込んだ方式を開発する．
2. 個人情報を保護しつつ活用するための暗号技術の開発:
   個人情報を暗号化したまま，あるいは秘密分散したまま，加算，乗算などを行う研究を進める．これは，PPDM(Privacy Preserving Data Mining)と呼ばれる手法である．
   その目的は，下記の通りである:
   (1) 暗号化せず，平文のまま，匿名で処理を行った場合，いくつかの属性から，本人が特定できてしまう危険性を防ぐため．
   (2) クラウドの普及に伴う，預託される情報の全文が暗号化されている環境に対して，平文に戻さず，計算処理を行うため．
   (3) 統計処理などを行った後，限られた個人に対して，必要な，あるいは有益な情報をフィードバックする必要が生じる場合に対応するため．
   暗号化状態のまま，乗算及び加算を行う暗号としては完全準同型暗号が提案されているが，現在のところ，乗算に制限があり非現実的な処理量を要する．

   本研究では，電子行政の現実的要請に照らし，また，クラウドコンピューティング環境を想定して，個人情報保有機関，個人情報活用機関，及び，計算受託システムと言う3つのセンターの役割・機能分担を定めた上で，Pailler 暗号，及び RSA 暗号などの暗号方式や秘密分散処理，あるいはマルチパーティ・プロトコル等を状況に応じて利用し，個人情報を保護したままで，加算・乗算を行い，統計値などを算出する手法を開発している．その構成例を図 7，図 8 に示す．
3. 上記の連携されたデータベースに対して，個人情報を保護しながら，問合せ，検索，及び問題解決の可能なシステムの開発 [7][8][9][10]
   (1) 自治体や医療機関などへ完全な匿名でクレームや意見などが寄せられた場合，回答を返すことが出来ない．このような場合，氏名は記入して貰った上で，回答者には投書者の匿名性を確保しながら，意見交換を行い，有益な結論や知見が得られることが望ましい．
   (2) データベースへの検索において，個人情報や組織情報の保護などの観点から「誰が」を，あるいは「何を検索しているか」を秘密にしたい場合も少なくない．
   (3) 検索内容に関しては，単なるキーワード検索に止まらず，自然言語によるコンテクスト，文脈依存型検索への要求も増加している． このような要請に対して，我々が 10 年来， 共同研究を進めてきた米国 California 大学の Sheu 教授らと共同で，個人情報や機密情報を保護しながら，意味検索を行うシステムを開発する．

4. 組織暗号による秘匿情報の伝送方式の開発

例えば，ある自治体から，ある医療介護ネットワークへ，文書をデータで秘密に伝送する場合，自治体側では，文書のどの部分を医療介護ネットワークの誰に読ませれば良いかは判断できない場合が多い．このような場合，現状では，自治体はケアマネージャー宛に文書を送り，ケアマネージャーが，一旦，暗号文を復号して平文に戻して，「この部分は A 介護士に，これは B ホームヘルパーに・・・」と判断して，再び，それぞれ暗号化して，必要な部分を復号することになる．しかし，それでは，平文に戻す手間と情報漏洩の可能性が増えることが懸念される．こうした課題解決のため，我々は，組織暗号という概念を提案してきた[4][5][6]．組織暗号は，我々が長年，開発してきた多変数公開鍵を利用して階層的復号を行う方式である．

組織暗号に類似と誤解されやすい暗号として，属性暗号・関数暗号が知られている．属性暗号の代表例は放送暗号であるが，これは，放送局が，多くの視聴者に対して，視聴料を払っているかいないかを把握していて，視聴料を払っている視聴者に対してのみ，復号鍵を渡すような場合

に使用される暗号である. つまり, 暗号文の送信者が, 受信者の復号資格などを論理的に記述できる場合に適用される暗号である. これに対して, 例えば, 医療介護の現場などでは, 非介護者の状況も日々変化したり, 介護者も日ごとに変わったりして, 非定常的で, 臨機応変な対応が求められる.

組織暗号は, このような場合に対処するための公開鍵暗号である[4].

5. むすび

以上の通り, 本研究では, 独自に開発しつつある個人情報保護を前提とした暗号技術, 意味検索技術など構成要素を, 情報連携基盤・情報保有機関に組み込んで電子行政の進展に寄与することを目的とするものである. 匿名ベース意味問い合わせ/ソリューション提供方式, 及び組織暗号の詳細については紙面の都合で省略したが, 続報で報告する予定である.

情報連携基盤・情報保有機関における個人情報の保護と活用の両立は, 21 世紀の国家基盤であり, 本研究は緒に就いたばかりであるが, 今後, 諸賢のご意見・ご批判を仰ぎつつ, その構成に貢献したいと考えている.

謝辞

本研究開発は, 経済産業省「企業・個人の情報セキュリティ対策促進事業(新世代情報セキュリティ研究開発事業)」からの研究受託に基づいて行うものである. 関係各位に感謝する.

文　献

[1] 辻井重男, "創立 50 周年記念特集:情報処理技術の未来地図　7. 電子行政・総合科学・現代社会と教養・人材育成-情報セキュリティ視点からの起承転結-, " 情報処理, vol.51, no.5, pp.500-503, may 2010.

[2] 山口浩, 只木孝太郎, 辻井重男, 土居範久, "医療・介護ネットワークにおける個人情報の保護と活用の両立に関する考察, " 信学技報, vol. 110, no. 429, SITE2010-52, pp. 33-38, 2011.

[3] 河上徹太郎, 竹内好, 他, 近代の超克, 富山房百科文庫, 冨山房, 東京, 1979.

[4] 辻井重男, 五太子政史, "相補型 STS－MPKC 方式による組織対応型公開鍵暗号の提案," 2010 年 暗号と情報セキュリティシンポジウム 3A2-2, 2011.

[5] 五太子政史, 辻井重男, "相補型 MPKC 役割交代型署名の提案," vol.110, no.443, pp.383-388, 日本電子情報通信学会 2011.

[6] 五太子政史, 辻井重男, "多変数公開鍵暗号による署名方式 Hidden Pair of Bijection 第二報 ～ セキュリティの検討 ～" vol.111, no. 285, pp.55-60, 日本電子情報通信学会, 2011.

[7] H. Yamaguchi, P. Sheu, S. Tsujii and N. Doi, "Semantic PIR" Annual Conference of the Society for Design and Process Science (SDPS 2011)

[8] A. Kitazawa, X. Zhang, X.F. Yao, P.C-Y Sheu, H. Yamaguchi, "A Query Optimization Model for Object Relational Databases," Annual Conference of the Society for Design and Process Science (SDPS2011)

[9] A. Kitazawa, X. Zhang, X. F. Yao, P.C-Y Sheu, H. Yamaguchi, "A Query Optimization Model for Object Relational Databases," Annual Conference of the Society for Design and Process Science (SDPS 2011)

[10] G. G. Zhang, C. Z. Xu, P. Sheu,and H. Yamaguchi, "Parallel Processing of Rule Networks," Annual Conference of the Society for Design and Process Science (SDPS2011)

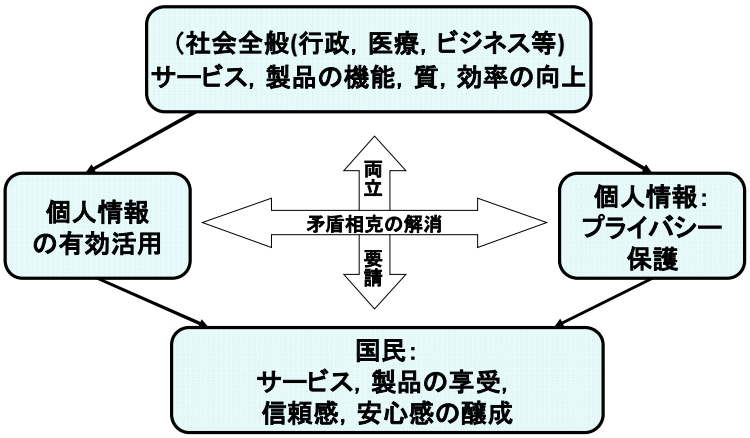


図1: 個人情報のプライバシー保護, 有効活用という相矛盾する要件克服による社会性の向上

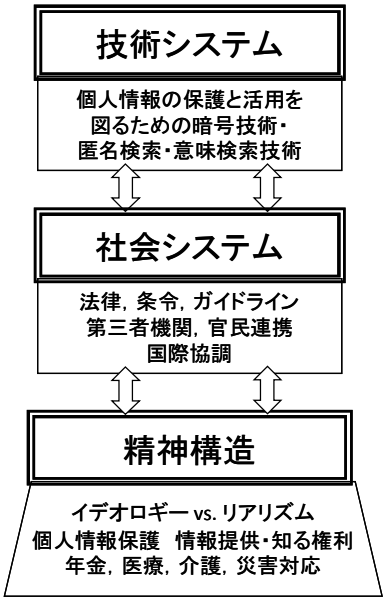


図2: 電子行政システムの階層

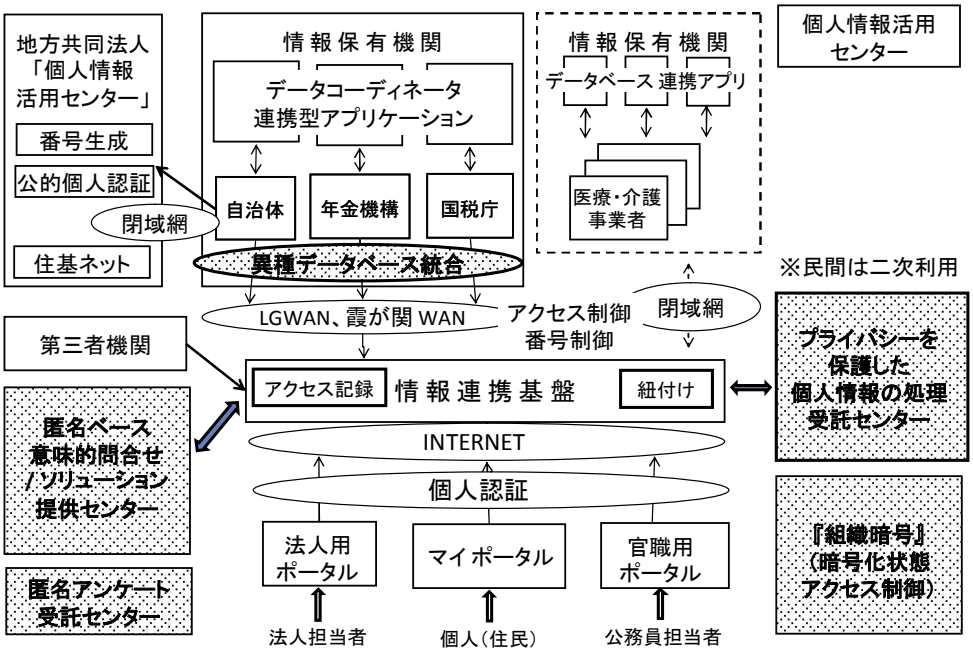


図3: 個人情報の保護と利用の両立を図る情報連携システム

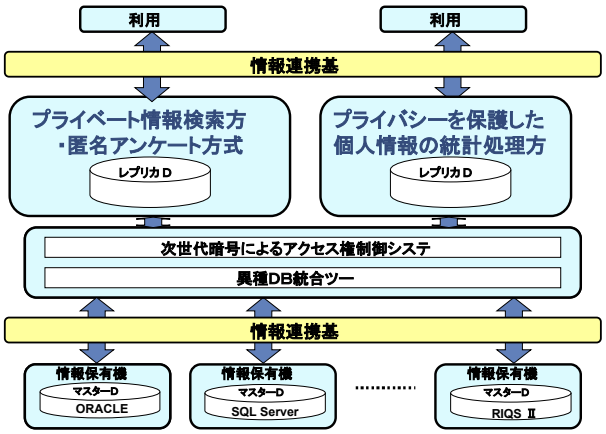
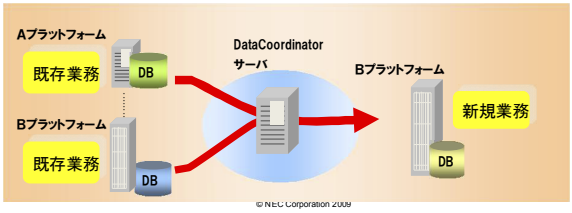


図4: 情報連携基盤との関連

複数システムのDBを統合



製品適用のメリット
文字コード，列属性，データ形式などが異なるDBをプログラム作成無しで論理的にデータ統合可能

図5: 異種データベースの統合

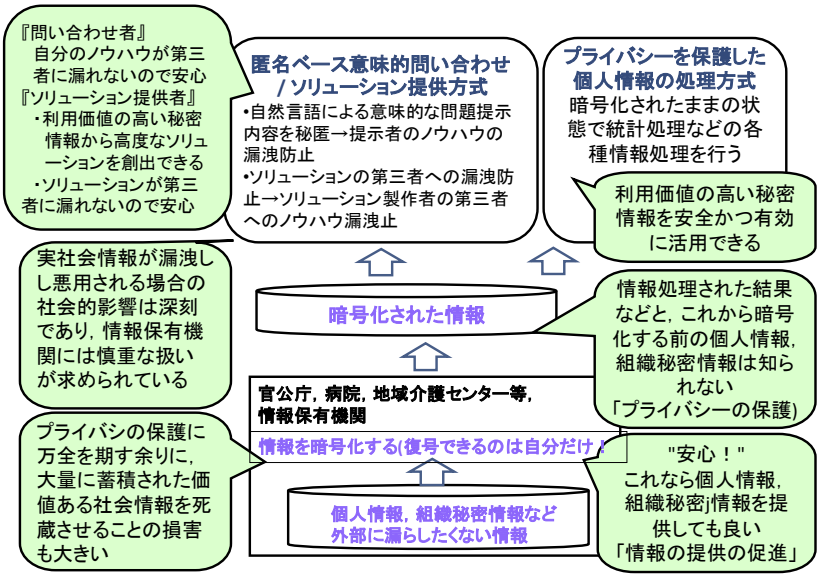


図6: 暗号化された状態の秘密情報処理におけるプライバシーを保護しつつ，社会に有用な情報活用に貢献する方式

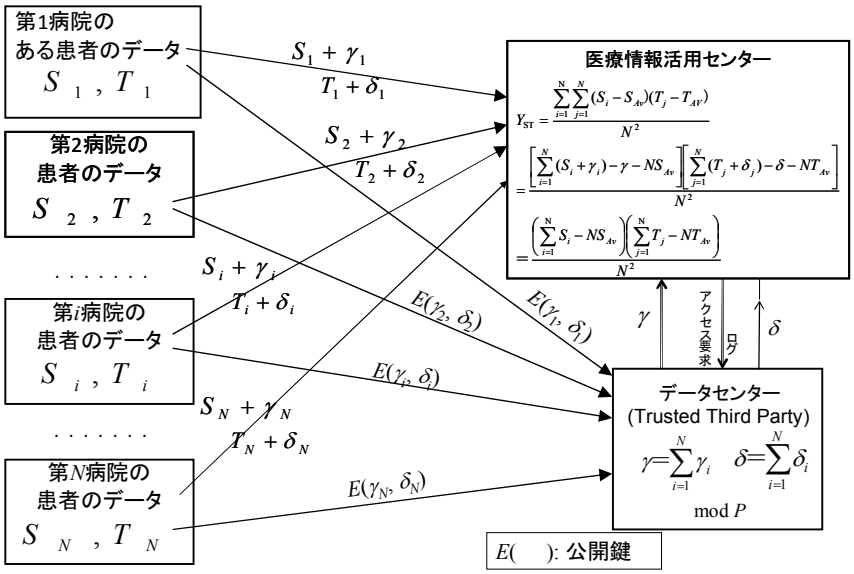


図7: クラウド対応型　暗号化状態処理の構成(1B)
（患者の個人データを秘匿したまま、異なる医療データ間の相関値を求める方法）
（例えば中性脂肪と善玉コレステロール値の相関）

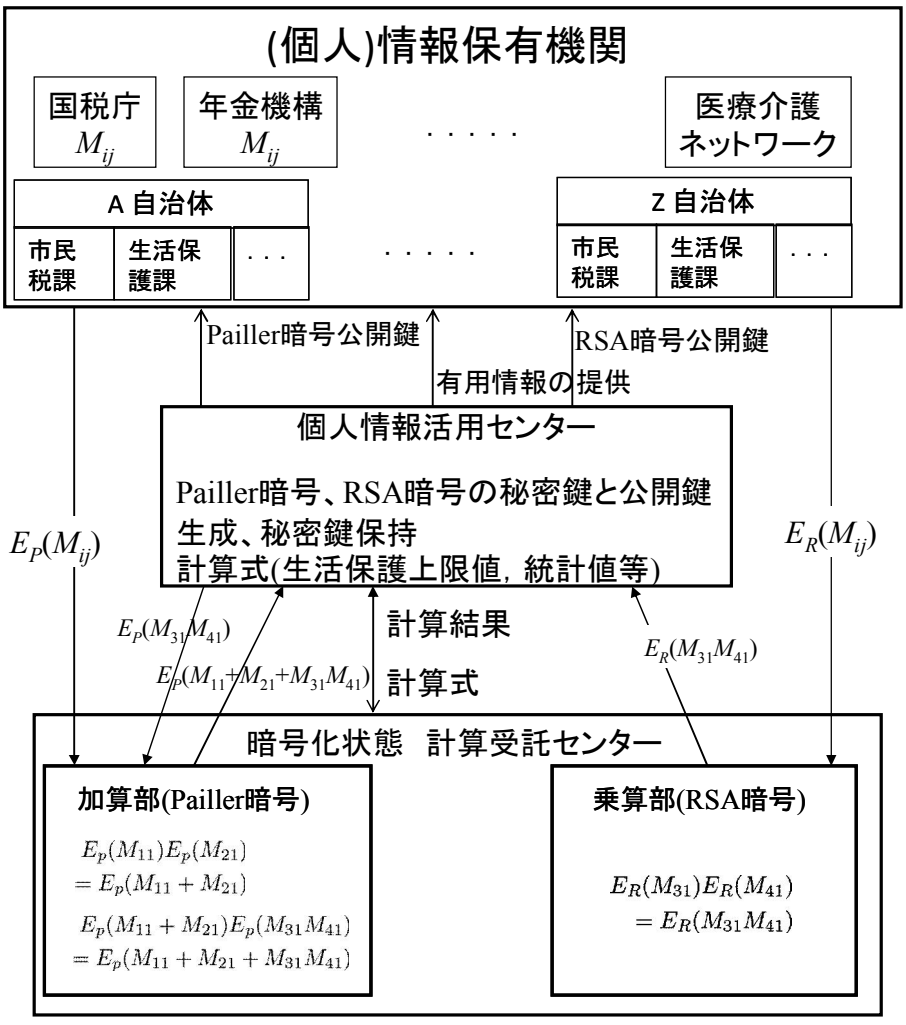


図8: クラウド対応型暗号化状態処理の構成-2
(Pailler暗号とRSA暗号の強調)