情報処理学会論文誌 Vol. 49 No. 7 2440–2455 (July 2008)

次世代プライバシ保護サービスのコンセプト提案

谷本茂明[†1] 廣田啓一[†1] 山本太郎[†1]
千田浩司[†1] 畑島隆[†1]
高橋克巳[†1] 金井敦[†2]

ユビキタス環境下での安心・安全なIT社会の構築に向け，技術と社会科学の両面を考慮したセキュリティ対策は重要な課題である．その課題の1つとしてプライバシ情報の収集や扱いに関する問題があるが，現状では，プライバシ情報は保護されるべき対象として議論されている場合が多い．しかしながら，たとえば複数人の判断によって本人情報開示をコントロールできる匿名性管理技術や，各消費者の消費行動を暗号化したまま統計分析を行う秘匿関数計算技術等，暗号応用技術の高度化によりプライバシ情報を安全に活用することが技術的に可能になってきている．本論文では，プライバシ保護技術に対する新たなパラダイムとして，プライバシ情報の保護と活用を両立させる次世代プライバシ保護技術のコンセプトについて業界動向調査や企業に対するアンケート調査および最新の暗号応用技術をもとに提案するものである．

Proposal for a Concept of Next-generation Privacy-protection Services

Shigeaki Tanimoto,[†1] Keiichi Hirota,[†1]
Taro Yamamoto,[†1] Koji Chida,[†1]
Takashi Hatashima,[†1] Katsumi Takahashi[†1]
and Atsushi Kanai[†2]

Security application technology which considers both technology and social informatics is an important aspect of the construction of a safe and secure IT society in a ubiquitous computing environment. Privacy protection is one of the problems, but the technology that defends personal information is of primary concern in the current state. On the other hand, there is a Secure function evaluation that is effectively utilizable with cipher technology while protecting privacy. This paper describes the concept of services using next-generation privacy protection technology, which reconciles protection and practical use of privacy information in a new paradigm.

1. はじめに

近年，光によるブロードバンド化の進展に象徴されるように，インターネットサービスがこれまで以上に身近にまた安価に使用できる環境が整ってきている．さらに，広域イーサネットや無線LANサービス等によるNWサービスの多様化が進んできており，いつでもどこでも容易にインターネット環境が利用できる，いわゆるユビキタス環境での利用が本格化している．さらに，アドホックNWやセンサNW等の実用化検討も進んでおり，ユーザの周辺にITが「溶け込んだ」環境として，ユビキタスに続く次世代IT環境であるアンビエント環境[1)]へと進化しつつある．

一方，昨今いろいろなメディア上で，インターネット上におけるコンピュータウィルスや不正アクセス等による被害に関する報告がなされており，セキュリティ対策は社会問題としても重要な課題である．総務省が2004年に作成した「u-Japan（ユビキタスネット・ジャパン）政策」で掲げた100の課題でも重要な課題として取り上げられており，特に，プライバシ保護技術は，この中でも一番に取り上げられている[2)]．我々は，このような背景の下，安心・安全なIT社会の構築に向け，技術と社会科学の両面から総合的にセキュリティ応用技術の研究を進めており，暗号応用技術を基にしたプライバシ保護技術・サービスに関する検討を行っている．平成17年4月に個人情報保護法が施行されたことにともない，プライバシ保護に関する研究が進んでいる[3)–7)]．これらは，主に個人情報をいかに守るか，というプライバシ情報（個人情報保護法によって保護される「個人情報」や私的かつ広く開示したくない情報であるところのセンシティブな情報）の保護を主体に検討がなされている．ところで，一般に，セキュリティと利便性はトレードオフの関係にあるといわれている．これは，プライバシ保護技術においても同様である．すなわち，個人情報を守ることが最も重要であり，利便性等に関しては補完的な位置づけにあるといえる．

しかしながら，たとえば文献8)では，守りの情報セキュリティから攻めの情報セキュリティへの認識の転換を推進すべき，また，文献9)ではプライバシ情報に関して「侵害されてはならないと一元的に保護すべき対象」から「条件に応じてその開示をコントロールす

†1 NTT 情報流通プラットフォーム研究所
NTT Information Sharing Platform Laboratories, NTT Corporation
†2 法政大学理工学部
Faculty of Science and Engineering, Hosei University

ることで様々なベネフィットを獲得する」考え方への進化を提唱する等，プライバシ情報の保護と活用を両立させる試案も報告されてきている．このような考え方は業界動向や技術動向にも見受けられる．2 章で詳しく述べるが，プライバシ保護に関する業界動向としては PRIME[10]（Privacy and Identity Management for Europe）や P3P[11]（Platform for Privacy Preferences）等が知られ，技術動向としては PET（Privacy Enhanced Technology）の総称で，文献 12) に詳しい．筆者らにおいても，PET の一手法として匿名性管理技術[13),14)]や秘匿関数計算技術[15)]を提案している．また，2004 年度からスタートした科学技術振興調整費重要課題型研究の「セキュリティ情報の分析と共有システムの開発」プロジェクト[16)]では，プライバシ保護とセキュリティの確保を両立させるための情報の隔離・匿名化技術，漏洩に強い認証技術等が検討課題となっていることも興味深い[6),7)]．これらの事例，動向等が示すように，プライバシ情報を単に保護するだけでなく活用しようという動きが出てきているが，まだ萌芽的な状況であり，体系的に整理，方向づけしたものはいまだ見られない．

本論文では，これらの背景の下，プライバシ情報を保護しつつ，様々な観点からプライバシ情報を保護するだけでなく新たに活用する点を次世代と定義し，そのコンセプトについて具体的に整理し，提案するものである．以降，2 章で，プライバシ情報の保護と活用に関する様々な視点からの現状把握および分析を行う．すなわち 2.1 節で，プライバシ保護サービスに関する先駆的な業界の動向を中心に概観し，2.2 節において最新の技術動向であるプライバシ強化技術の総称である PET について述べた後，筆者らの関連研究を紹介する．3 章では，市場動向を把握する観点からプライバシ情報を比較的多く保有している企業に対し，プライバシ保護に関する現状調査と将来動向に関するアンケート調査を行った結果を示す．4 章では 2 章と 3 章における現状のプライバシ情報に関する技術動向や業界動向の調査・分析結果をふまえ，新たにプライバシ情報の保護と活用を両立させる次世代プライバシ保護技術のコンセプト提案を行い，5 章において定性的な評価等により，提案コンセプトの実現可能性に関する考察結果について述べる．最後に 6 章で本論文のまとめと今後の課題について示す．

2. 現状把握・分析

2.1 業界動向

2.1.1 PRIME（PRivacy and Identity Management for Europe）

PRIME は，複数の国（ベルギー，フランス，ドイツ，イタリア，オランダ，スイス，イギリス，アメリカ）や組織にまたがる教育および公共セクタの 20 以上のパートナからなる共同研究プロジェクトである．PRIME では身元情報管理における問題の大きさを把握し，その解決法を見い出すための基本的な研究が行われており，その目的はプライバシ保護機能を備えた身元管理システムの開発である．一般に個人情報の収集と利用は，インターネットでの電子取引が促進される中，増加の一途をたどっている．このような取引において個人情報の交換が必要となるが，現実世界では，人々は社会生活を通じて各自の個人情報を交換する場合にどの程度情報を開示すればよいか判断するのは比較的容易であるが，オンライン上でこれを判断するのはかなり難しい．たとえば，医療健康，金融，ショッピング嗜好等のデータの誤用は個人のプライバシに大きな影響を与える可能性がある．PRIME では，個人がこれらの「部分的な身元情報」を自ら管理でき，取引に必要な最小限の情報だけを開示するのに利用できる安全な手段を検討している．これまでに，e ラーニングや，航空会社および空港における乗客処理等を含むいくつかのシナリオのプロトタイプが現在開発されている．今後，ポリシの編集やテスト環境構築用の API としてすでに公開されている JRC Policy Workbench[17)] のような OSS として公開される予定である．

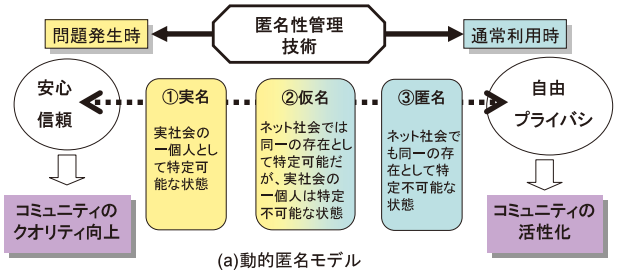
2.1.2 P3P（Platform for Privacy Preferences）

P3P は，ウェブサイトのプライバシポリシを，ユーザのソフトウェアが自動的に読み取り，容易に理解できる標準的なフォーマットで公開できるという機能を開発することを目的としている．P3P を利用するウェブサイトはそこで収集される情報の内容やその利用法について自動的にユーザに通知し，P3P 機能を備えたブラウザのユーザはそのウェブサイトにどのような内容の情報を開示するかを判断できる．これまでに，1.0 仕様を 2000 年に公開しているが，P3P Working Group（WG）では 1.1 仕様を 2006 年 11 月に公開した後，活動を停止している．また，Internet Explorer や Firefox 等の主要なブラウザによる P3P サポートは限定的である．

2.2 技術動向

2.2.1 PET（Privacy Enhanced Technology）

PET[12)] は，暗号ソフトやデータベースシステムにおけるデータの取扱いやネットワークへのアクセス方法等定められたポリシやこれらをコントロールするソフトウェア，ツール等を指している．PET を導入することで，個人情報流出等のリスクを回避することが可能となるが，PET の導入によって万全なプライバシ情報保護が可能となるわけではない．たとえば，運用面としてデータを扱うユーザのセキュリティに対する意識や組織等の体制，ポリシ等の考慮も必要である．PET の例としては，種々の暗号化技術やバイオメトリックス，



(a)動的匿名モデル

対象		ネット社会の人格	
		特定	非特定
実社会の人間	特定	①実名	
	非特定	②仮名	③匿名

(b)実社会とのマッピング

図 1　匿名性管理技術
Fig. 1　Function of anonymity management.

データベースにおける ID 管理，匿名化技術等である．

2.2.2　筆者らの PET に対する取組み

筆者らは PET の一手法として次のような技術提案を行っている．

(1) 匿名性管理技術[13),14)]

匿名性管理技術は加入者の ID（Identity Document: 実名，仮名，匿名）を通常時は匿名や仮名の状態とすることで発信者の積極的な参加を促進し，何か問題が生じた際には匿名性を剥奪する，すなわち，ふだんは匿名や仮名により加入者のプライバシを保護し，問題が発生した場合は匿名を剥奪できる機構を提供することにより発信者の自己抑制を促し，違法・有害情報等の発信を削減する技術である．**図 1** にその概要を，**図 2** に加入者の ID が場面（①通常時，②問題発生時）によってどのように遷移するかに関しての概要について示す．

図 2 の実名追跡者（群）とは，仮名利用者の実名を特定できる権限者である．暗号応用技術の 1 つである閾値暗号（一定数以上の復号者の協力がないと復号できない暗号）[18)] により，一定数以上の権限者が合意協力しない限り実名を特定できないようにすることが可能である．仮名追跡者（群）についても同様である．このように合意形成を必ず必要とすることにより，少数の不正な権限者による利用者のプライバシ侵害や過失による個人情報漏洩を防ぐことができる．

また，筆者らは上記の技術について，ユーザ行動実験（実験室実験）により主に利用者側

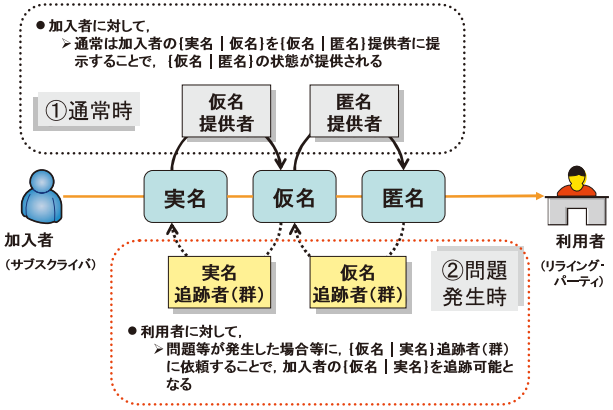


図 2　ID の遷移イメージ
Fig. 2　Process of changing ID (Identity Document).

の観点からのサービス受容性を評価した[19)]．具体的には，匿名性に由来する誹謗中傷等の問題が多発している電子掲示板に着目し，掲示板上でのユーザの振舞いについてモデル化を行い，被験者実験を行った．すなわち，複数の被験者に対し，匿名性管理技術を模擬した擬似電子掲示板による掲示板利用時の環境を再現し，記事の閲覧や投稿といった行動を行ってもらった．このときの評価パラメータとして，匿名・仮名・管理者の有無といった点が，ユーザの掲示板利用に対してどのような影響を及ぼすか，すなわち，ユーザの行動と意識に関する実験を行った．その結果，管理者がいる匿名掲示板での行動は，管理者の存在を意識して投稿を判断したという結果が得られ，管理者の存在により投稿時の抑制効果があることが実験結果から得られた．このように，匿名性管理技術により，サービス提供者が適切な管理を行うことを前提に，プライバシを保護しつつかつユーザ側においても荒らしや誹謗中傷のような行動を抑止しうることの可能性を確認することができた．

(2) 秘匿関数計算技術（文献 20) 等）

秘匿関数計算技術（Secure function evaluation）は，プライバシ情報の漏洩を技術的に防止し，安全な利用を可能とする技術である．秘匿関数計算技術により，ユーザ i がプライバシ情報 x_i を保持し，企業等の組織が x_i から $z = f(x_1, \ldots, x_n)$ を求める場合において，z から x_i を求めることが困難であるようなプライバシ情報を扱った安全な計算が実現できるようになる．たとえば f が平均値や検定といった統計関数であれば，一般に演算結果から個人のプライバシが侵害されることはないため，強力な情報漏洩対策，プライバシ保護手

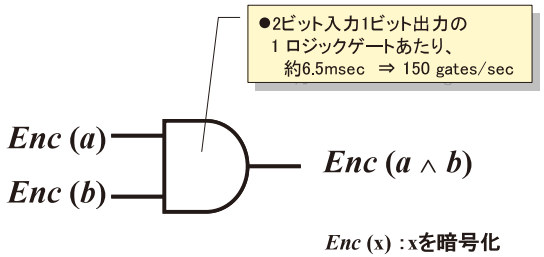


図 3　基本ロジックゲート
Fig. 3　Basic logic gate.

段となりえる．

上述の秘匿関数計算技術は，一般に演算を行うたびにすべてのユーザ（の所有する端末）が演算に参加する必要があるため，特に多数のユーザのプライバシ情報を用いた演算（国民全体を対象としたオンラインアンケート等）は実現が難しい．そこで各ユーザは複数存在する代理人のいずれかに処理を委託し，演算時には当該すべてまたは一定数以上の代理人が演算に参加することで秘匿関数計算を実現する手法が提案されている（たとえば文献 15)）．このような委託型の秘匿関数計算では，すべてまたは一定数以上の代理人が不正に結託しない限りは個人のプライバシ情報を知られず，したがって自身が選択した代理人に対してもプライバシ情報を知られなくすることが可能である．

文献 15) では秘匿関数計算の実装評価により一定の実用レベルを示した．文献 15) によれば，代理人の総数（＝分散数）を 2 としたとき，**図 3** に示すような 2 ビット入力 1 ビット出力の 1 ロジックゲートあたりで，約 6.5 msec（150 gates/sec，各代理人の計算環境：Intel Xeon 2.8 GHz × 4 台構成）を要する．これはたとえば，10,000 人のアンケートで，4 問中 3 問以上 Yes（2 択）と答えた人の総数を得る場合，約 7 分半で集計が可能となる．また，同様に，64 ビット共通鍵暗号 DES の暗号文を復号せずにデータ検索する場合，1 ブロックあたり約 1 分かかる．これは，約 1 日で 10 KB 程度の暗号データを復号せずに検索可能ということになる．

3.　プライバシ保護に関する企業意識調査

3.1　調査の概要

3.1.1　調査の背景と目的

1 章で述べたように，情報通信環境のユビキタス化・アンビエント化により生活の利便性が著しく向上してきている．その結果，個人に関連する多種多様なプライバシ情報が取得，蓄積されている．このようにプライバシ情報が多量に保有されている状況では，これらの情報が適切に利用されている範囲においてはサービス等の利便性や満足度が向上するが，一方で個々人のプライバシ情報が侵害される脅威が増大しているといえる．プライバシ情報の適切な活用を実現するためには，保有するプライバシ情報を保護するために種々の対応を導入する必要がある．これらの対応は人的・制度的なもの，情報技術的なもの等多様なものが考えられる．ここでは，今後，プライバシ情報の活用と保護が実現される社会を目指すにあたり，企業等におけるプライバシ情報管理が，現状および今後どのように変化していくかについて，アンケート等による調査・分析を行った結果について示す．

表 1　調査票の配布状況および回収率
Table 1　Distribution situation of questionnaire and its rate of collection.

業種	配布数	回収数	回収率
①情報通信	125票	10票	8.0%
②教育	125票	17票	13.6%
③流通	125票	14票	11.2%
④医療	125票	19票	15.2%
⑤金融	125票	9票	7.2%
⑥行政	125票	13票	10.4%
⑦その他	250票	22票	8.8%
合計	1000票	104票	10.4%

3.1.2　調査の方法

(1) 調査対象企業

3.1.1 項で示すように，本調査では，プライバシ情報の保護と活用の両立に向け，現状および今後の分析として，企業等における保有プライバシ情報，特に重要となる顧客のプライバシ情報に関する保護対策の現状の満足度や，プライバシ保護技術に関する今後の導入意向等についてのアンケート調査を行った．調査票は，**表 1** に示すとおり，プライバシ情報を比較的多く保有していると思われる教育・医療・行政等の業種に対し計 1,000 票配布し，約 10%の回収率が得られた．アンケート内容自体が**表 2**，**表 3** に示すように，回答を得難いものなので低い回答率であることは想定していたが，母集団の状況を分析するための参考情報としては十分なものと考えられる．また，回答企業は，プライバシ問題に意識の高い企

表 2　現状把握のための分析対象項目
Table 2　Assessment of company status regarding privacy protection service.

カテゴリ	問番号	設問内容（把握すべき事項）
保有情報	問1	保有するプライバシ情報の種類
	問2	保有するプライバシ情報の形態(紙か電子か)
	各業種	業種特異的に保有するプライバシ情報の種類
保護対策	問4	設置する役職・組織
	問5	プライバシ情報の管理体制
	問6	外部機関による認証状況
	問7	その他の人的・制度的な対応
	問8	情報技術的な対応の実施状況
	問9	投資額
対策満足度	問8	情報技術的な対応に関する満足度
	問8付	情報技術的な対応に関する不満理由

表 3　中長期的な将来の動向予測項目
Table 3　Medium-to-long term future trend prediction item.

カテゴリ		問番号	設問内容（把握すべき事項）
共通項目	保有情報	問3	プライバシ情報の保管方法の変化
	保護対策	問10	今後の投資額（「近い将来動向」においても利用しうる）
業種別項目	保有情報	各業種	今後保有する可能性のあるプライバシ情報（自由回答）
		各業種	深掘テーマ(※)に関する実施状況・意向
		各業種	深掘テーマにおいて実施あるいは予定している個別用途
	保護対策	各業種	深掘りテーマ実施に当たり想定される問題点
		各業種	有効であると想定される対策
		各業種	影響を与えると考えられる法制度・ガイドライン

※深堀りテーマ
①情報通信：CGMの活用，②教育：高機能学生証の活用，③流通：コンテキストマーケティングの活用，
④医療：医療サービスに対する通信ネットワークの活用，⑤金融：顧客向け生体認証の活用，
⑥行政：申請・届出オンラインサービスの活用

業群であると思われることから，これら企業の意見はプライバシ問題を議論する材料としての価値が十分であると思われる．業種別の回答率についても表 1 に示すように極端に高い，あるいは低いものがないことからアンケート配布先のサンプリングの方法も妥当だったといえ，これらのことから，市場全体の状況を反映する参考情報になりうると考えられる．

(2) アンケート項目とその目的

本調査におけるアンケート項目は表 2 および表 3 のように構成した．表 2 は，現状把握を目的とした調査項目であり，「保有する情報」，「情報保護のための対策」，「対策の満足度」等について把握するものである．表 3 は中長期的な将来動向予測を主眼としたもので，業種間共通項目と業種別項目により構成している．

3.2　調 査 結 果

3.2.1　現状把握項目からの主な結果

(1) 保有するプライバシ情報

図 4 (a) の調査結果に示すように，現状，保有するプライバシ情報に関しては，基本的な情報（氏名，住所，電話番号等）に関するものが圧倒的に多いが，マルチメディア情報（監視カメラの録画映像，コールセンタの音声等）についても保有事例が存在する．また，同図 (b) より，保有媒体に関しては，紙・電子の両者で保有しつつも，電子媒体の割合の方が多いとする割合が多い．

(2) 人的・制度的な保護対策

図 5 (a) に示すように，プライバシ情報に関する制度的な管理方法では，ポリシを策定するとする割合が最も高い．同図 (b) に示す管理体制では，全社統一的な管理組織を設置するよりも，担当部署ごとでの管理の実施が一般的である．また，同図 (c) に示すように，第三者認証を受けている割合は 3 割程度である．その中では，プライバシーマークの取得割合が比較的高い．

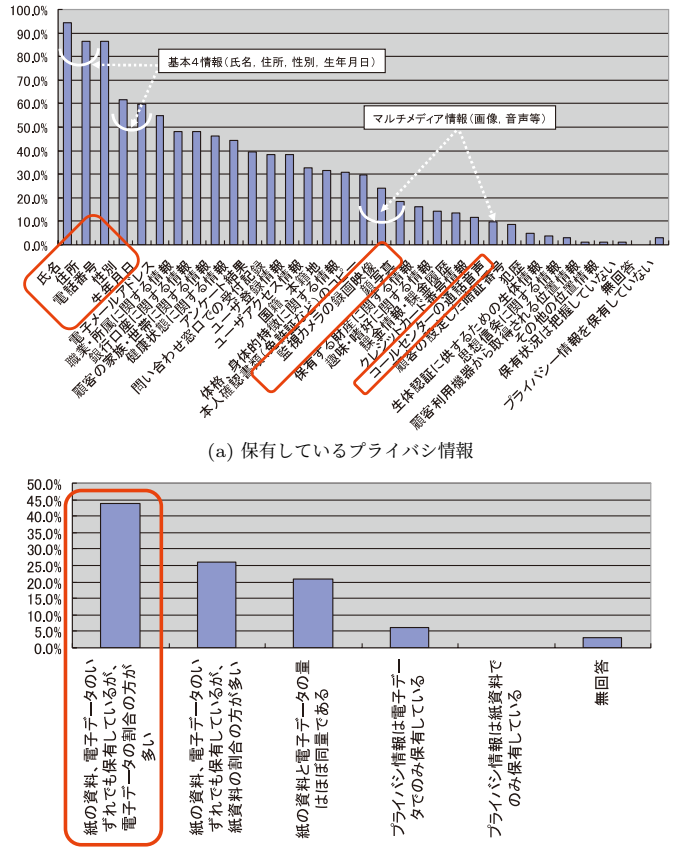
(3) 技術的な保護対策

技術的対策では，**図 6** に示すように，媒体の適切廃棄，バックアップメディアの厳重保管等情報漏洩に直結する要素をあげる割合が高い．一方，導入率が比較的高いにもかかわらず満足度が低い項目としては費用的な面から通信の暗号化，また機能の不十分な点から，送信メールのフィルタリングがあげられている．

3.2.2　中長期的な動向予測項目からの主な結果

(1) プライバシ保護を促進させる契機

図 7 (a) に示すように，プライバシ情報保護を促進させる契機としては法制度制定の影響が最も大きい．次いで，システム投資額の増加等投資予算的な事項をあげる割合が多い．自社でのインシデント発生が影響を及ぼすとする割合は，全体で見た場合には比較的低い．しかし，同図 (b) に示すように，投資積極群のみに注目した場合，その割合は投資積極群以外に比べ著しく高い状況がうかがわれる．



(a) 保有しているプライバシ情報

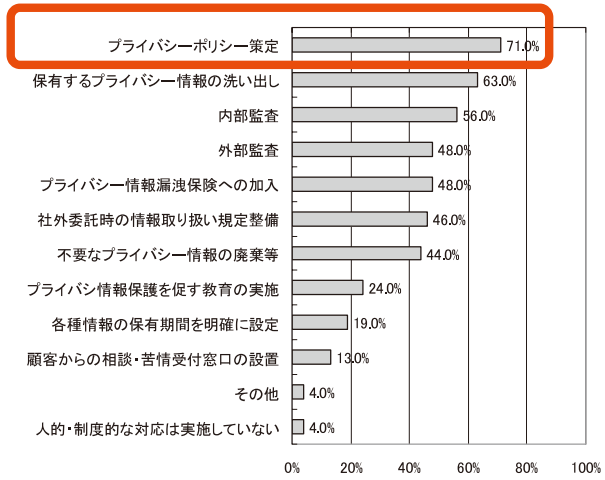
(b) 保有媒体に関して

図 4　保有するプライバシ情報の調査結果

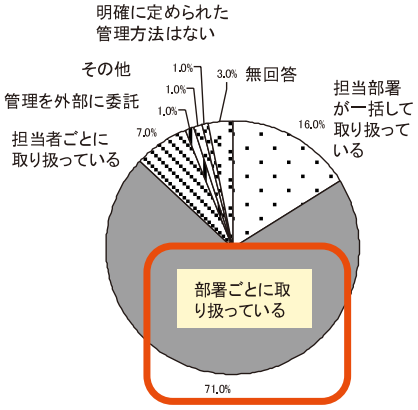
Fig. 4　Questionnaire survey result of the possessed privacy information.

(2) 監視カメラ録画映像の保護対策

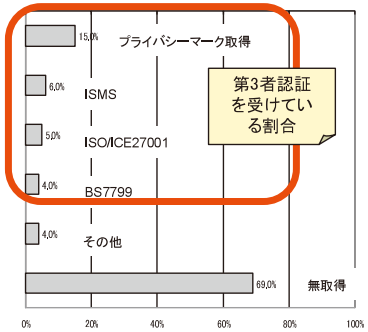
監視カメラ録画映像の保護については，**図 8** に示すように「必要ではあると思うが，現状，対策の予定はない」が約半数を占め，それほど意識が高くない現状がうかがわれるが，「行政」,「金融」,「教育」においては，それぞれ 10〜20%程度が,「必要であり，今後対策予定である」としている．



(a) プライバシ情報保護のための人的・制度的対応



(b) プライバシ情報の管理体裁



(c) 第三者機関による評価・認証の取得状況

図 5　人的・制度的な保護対策

Fig. 5　Questionnaire survey result about human activity and policies in privacy protection.

3.2.3　中長期的な動向予測項目からの主な課題

u-Japan [2] 等を参考に，業種別に今後想定される課題を深掘りする観点より個別に調査を行った（表 3．深堀テーマ）．ここでは，特に，特徴的な結果が得られた情報通信業と流通

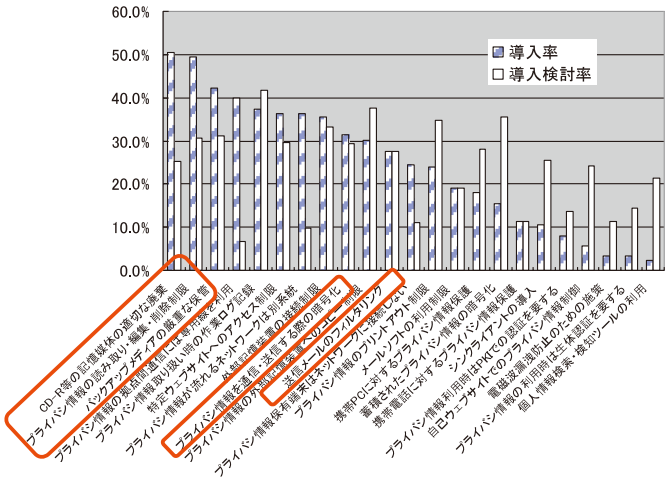


図 6　技術的な保護対策

Fig. 6　Questionnaire survey result about technical methods of privacy protection.

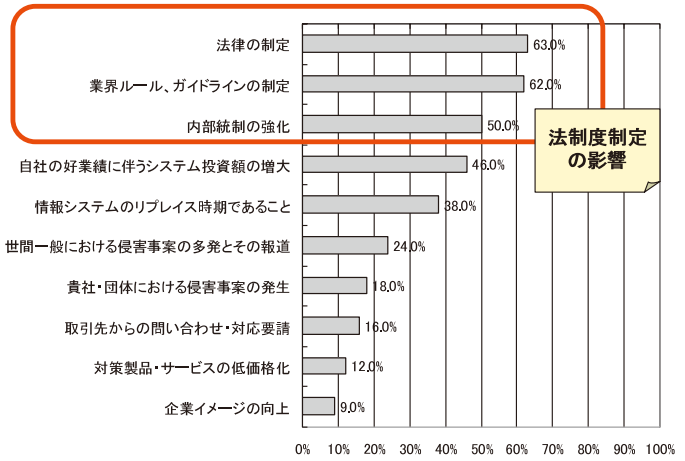
業の結果を示す．

(1) 情報通信業（深堀テーマ：CGM の活用）における調査結果

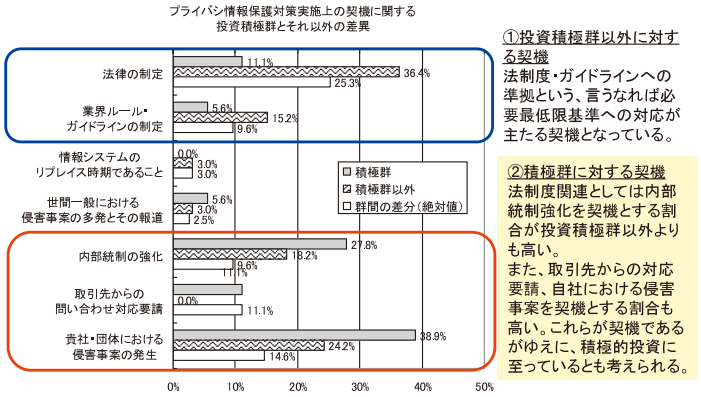
図 9 に示すように，電子掲示板や blog，SNS 等，今後の CGM（Consumer Generated Media）サービスの提供にともない想定される問題点としては「誹謗中傷」をあげる割合が最も高い．次いで，「悪意なきユーザによる，意図せずに行われるプライバシの開示」や「第三者に関するプライバシ情報の意図せぬ公開」といった項目が高く，「悪意あるユーザによる他者プライバシ情報の開示」に比べ不作為によるプライバシ情報漏洩を懸念する意識が高い状況がうかがえる．

(2) 流通業（深堀テーマ：コンテキストマーケティングの活用）における調査結果

図 10 に示すように，まず今後保有情報が増加するとする割合が 8 割に達する．特に，急増するとする割合も 2 割強存在しており，プライバシ情報に依拠したマーケティングの重要性が増すことを示唆している．ここでの情報の種類としては，現状は購買履歴に関する情報が多く，今後は購買に至る前段階としての，消費者が関心を示した商品に関する情報等を取得する事例も増加すると考えられる．顧客情報の増加にともない予想される問題点としては，情報漏洩および情報死蔵をあげる割合が高く，負担としては人的・金銭的なものよりも技術的なものをあげる割合が高い．



(a) プライバシ保護を促進させる契機



(b) プライバシ保護を促進させる契機（投資積極群とそれ以外との差異）

図 7　プライバシ保護を促進させる契機

Fig. 7　Questionnaire survey result of trigger events that promote privacy protection.

3.3　主な分析結果

3.3.1　現状把握項目に関する主な分析結果

ここでは，企業の保有するプライバシ情報の調査結果を中心に分析した結果について示す．企業の保有する主なプライバシ情報は，氏名・住所等であり，これらはテキストベース

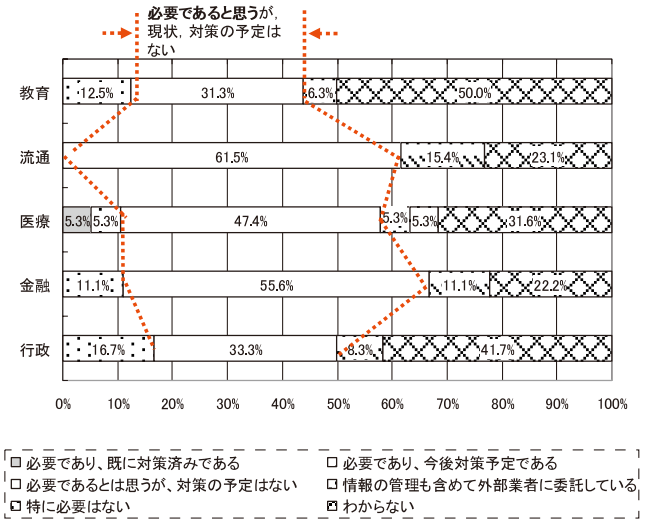


図 8　監視カメラ映像の保護対策
Fig. 8　Questionnaire survey result about usage of security camera.

で保存されている場合がほとんどである．今回の調査結果より，これらに加えてマルチメディアベースのプライバシ情報が顕在化してきていることが分かる．一般的には，監視カメラの録画映像や，コールセンタにおける応対の録音音声等が該当する．また，医療現場では検査データが画像映像形式であることもあるため，それらの情報を医師間，あるいは医師・患者間において電子的に共有するという状況が，今後増大すると考えられている．

そのほか，電子マネーの普及等を受け，種々のサービスと決済関連情報を結び付けようとする傾向が見られ，その結果，金融や流通に限らない，情報通信業界や教育機関においても決済関連の情報を保有する事業者が増加することも予想される．

3.3.2　中長期的な動向予測項目に関する分析結果

監視カメラ録画映像に関する保護対策に関する分析結果を示す．3.3.2 項 (2) でも示したように，現状は，監視カメラ録画映像に対する保護は，「必要性は認識されているが，現状，対策の予定はない」という回答が多く見られたが，3.2.1 項 (1) の保有プライバシ情報において，監視カメラの録画映像の保有事例があること，また，利用用途として，たとえば東京メトロによる顔認証実験の事例[21] が報告されていること，さらには，アンビエント化[1] に

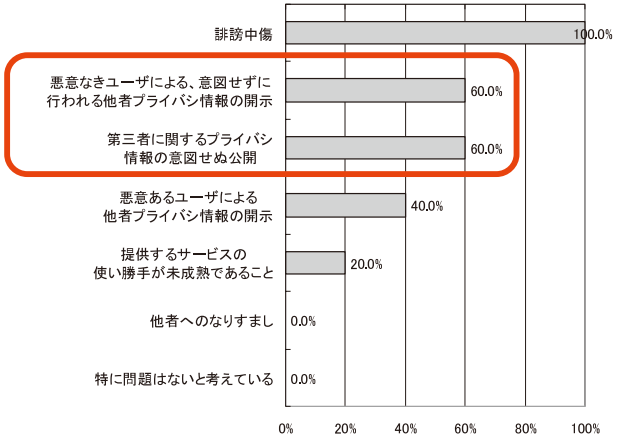


図 9　CGM サービスの提供にともない想定される問題点
Fig. 9　Questionnaire survey result about assumed problem caused by CGM servicing.

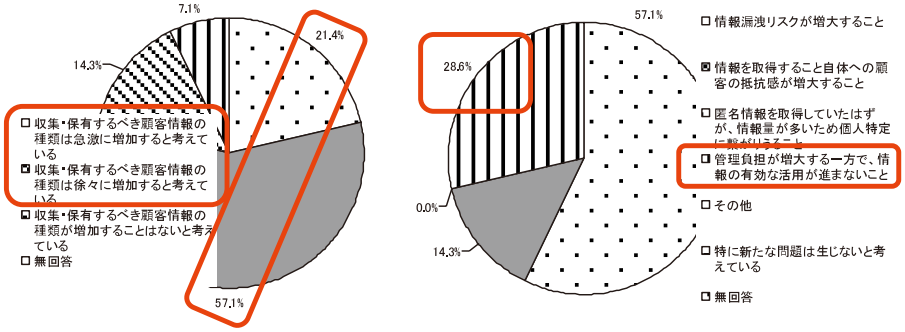


図 10　流通業界における調査結果
Fig. 10　Questionnaire survey result of context marketing field.

より，いろいろなセンサと監視カメラとの組合せが考えられること等から，今後，監視カメラに関するプライバシ保護対策はますます必須になってくると思われる．

3.3.3　中長期的な動向予測項目からの課題に関する分析結果

3.2.3 項 (1) の情報通信業（深堀テーマ：CGM の活用）における調査結果からは，悪意なきユーザによる不作為の情報漏洩を懸念する声があげられている点，3.2.3 項 (2) の流通

業（深堀テーマ：コンテキストマーケティングの活用）からは，保有情報が増加する一方で有効活用できず死蔵させてしまう恐れがあげられている点が特に興味深いものであり，今後，検討する必要性が高い課題と考えられる．

4. 次世代プライバシ保護サービスのコンセプト提案

4.1 提案の背景

2 章で示したように，現状のプライバシ保護技術においては，プライバシ情報保護を中心とする要素技術やシステムの検討が進んでいる．また，3 章で示した企業意識の調査結果からは，保有プライバシ情報のマルチメディア化や，新たな課題である不作為の情報漏洩，保有情報の有効活用等があげられている．ここでは，このような背景において，多様な観点による次世代プライバシ保護サービスのコンセプト創出をねらいとして，以下に示す 3 つの観点，すなわち，質的側面，量的側面，付加価値創造を基にしたコンセプト提案を行う（**表 4**）．

表 4 は，3 つの観点（質的側面，量的側面，付加価値創造）から次世代プライバシ保護サービスのコンセプトを提案するものであり，今後，このコンセプト案をサービスとして具現化することにより，プライバシ情報を保護しつつ，さらに不作為の情報漏洩や匿名性とモラル面との両立といった社会的課題の解消やマルチメディア化等による適用領域の拡大，プライバシ情報の活用といった新たなサービスの創出を可能とするものである．

表 4　多様な観点に基づくコンセプト案
Table 4　Conceptual proposal based on various viewpoints.

<table>
<tr><td rowspan="2"></td><td rowspan="2">現状</td><td colspan="2">次世代</td></tr>
<tr><td>拡張項目</td><td>コンセプト</td></tr>
<tr><td>(1)質的側面</td><td>自分だけ
保護</td><td>相手の状況も
考慮</td><td>CGMプライバシ：
→プライバシとモラルとの両立、倫理面考慮</td></tr>
<tr><td rowspan="2">(2)量的側面</td><td>テキスト
データ</td><td>マルチメディア化
（音声、映像）</td><td rowspan="2">マルチメディア＆
アンビエントプライバシ：
→マルチメディア化，アンビエント化による適用領域，利便性の拡大</td></tr>
<tr><td>RFID</td><td>センサ</td></tr>
<tr><td>(3)付加価値
創造</td><td>プライバシ情報は
保護のみ</td><td>プライバシ情報を
保護しつつ積極的
に活用</td><td>バリューアッドプライバシ：
→プライバシ情報活用</td></tr>
</table>

4.2 3 つのコンセプト提案

4.2.1 CGM プライバシ（プライバシとモラルの両立，倫理面の考慮）

プライバシ保護された IT 環境下では，一般に自由な発言等が促進されるが，反面，節度を持った行動も要求される．CGM プライバシでは，匿名性管理技術等の暗号応用技術を用いて，ある程度の抑止力を有することにより，プライバシを保護しつつモラルを遵守することを可能とする．これは，自分のプライバシ情報だけを守る，という観点から，匿名性による弊害，たとえば，掲示板等における荒らしや誹謗中傷の問題を解消する必要性，すなわち，自分だけでなく相手の立場も尊重する，といったプライバシ保護とモラル遵守の両立を可能とするものである．

4.2.2 マルチメディア&アンビエントプライバシ（マルチメディア化，アンビエント化による適用領域，利便性の拡大）

3.2.1 項 (1) に示す音声や映像といった保有プライバシ情報のマルチメディア化や，RFID からセンサ技術等によるアンビエント環境の進展にともない，今後，保護すべきプライバシ情報の範囲は拡大する傾向にある．マルチメディア&アンビエントプライバシでは，暗号応用技術を駆使することにより，音声や画像情報等のマルチメディア化，RFID からセンサといったアンビエント化により，今後，量的に拡大するプライバシ情報を適切に保護するとともにこれらを活用し，次世代プライバシ保護サービスとしての適用領域と利便性の拡大を図るものである．

4.2.3 バリューアッドプライバシ（プライバシ情報活用）

従来の守るためのプライバシ保護技術に加え，さらなる活用を図るためのコンセプトである．すなわち，バリューアッドプライバシでは，プライバシ情報を守るだけでなく，秘匿関数計算技術等の高度な暗号応用技術を利用し積極的に活用する観点から新たな技術・サービスの創出を可能とするものである．

4.2.4 ま と め

本論文で提案する提案コンセプトの位置づけを，現状のプライバシ保護サービスと比較した結果として**図 11** に示す．すなわち，次世代プライバシ保護技術のサービスコンセプトは，現状のプライバシ保護技術を包含しつつ，質的向上（プライバシとモラルの両立：CGM プライバシ），量的拡大（マルチメディア化＋アンビエント化：マルチメディア&アンビエントプライバシ），さらに付加価値創造（プライバシ情報の積極活用：バリューアッドプライバシ）を可能とし，現状のプライバシ保護サービスの有する安心・安全に加え，利便性も兼ね備えた IT 社会の実現を可能とするものである．

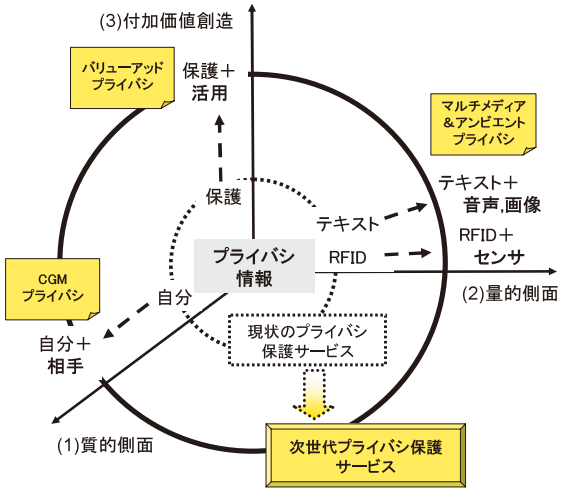


図 11　提案コンセプトの位置づけ
Fig. 11　Overview of proposal concept.

5. 評　　価

ここでは，提案コンセプトの評価として，5.1 節で 3 つのコンセプトに対してそれぞれ既存サービス・技術との比較を行い，その有効性を示すとともに，その実現のために必要となる技術等を明らかにし，5.2 節で，具体的なサービス例を示すことにより，本コンセプト提案に対するフィージビリティ評価について示す．

5.1　既存サービスとの比較

図 11 に示したように，本論文で提案する次世代プライバシ保護サービスのコンセプトは，従来のサービスに比べ，プライバシ情報を保護しつつ，質的向上，量的拡大，付加価値創造をねらいとするものである．

以下に，これらの観点より既存技術・サービスと比較した結果について示す．

5.1.1　質的な観点

(1) 既存サービス

現在，電子掲示板に代表されるユーザ参加型サービス，いわゆる CGM サービスにおいて課題となっている「影」の部分，すなわち匿名性による荒らしや誹謗中傷といった負の部分が顕在化している[19]．既存のサービスにおいてもこれらの課題への対処が検討されており，たとえば，編集スタッフにより掲載管理を行うことにより掲示板が “荒れない” ことを特徴とする掲示板「goo ニュース畑」の提供が開始されているが[22]，CGM サービスの特徴であるユーザ参加型という観点では，管理面にも編集者に加えユーザも参加可能とする形態が望まれることから，今後さらなる検討が必要と思われる．

(2) CGM プライバシ

CGM プライバシは，2.2.2 項 (1) で述べた暗号応用技術の 1 つである匿名性管理技術[13]を利用することにより，これら「影」の部分を抑止しうることが可能である．掲示板サービスに適用する場合として考えると，ふだんは匿名や仮名により加入者のプライバシを保護し，問題が発生した場合は匿名を剥奪できる機構を提供することにより発信者の自己抑制を促し，違法・有害情報等の発信を削減することが可能になる．

一方，問題が発生した場合の匿名剥奪機構に関しては，前述の閾値暗号技術[18]を用いる．すなわち，一定数以上の権限者（たとえば，編集者に加えてユーザにもその権限を与える）が合意しない限り，匿名を剥奪できなくする．これにより，ユーザも管理に参加することが可能となり CGM サービス受容性の向上が見込めるとともに，あわせて少数の不正な権限者によるプライバシ侵害や過失等の不作為による個人情報漏洩を防ぐことも可能となる．

5.1.2　量的な観点

(1) マルチメディア化の観点

(a) 既存技術・サービス

一般にプライバシ保護技術としては，個人情報漏洩対策と匿名性の維持対策があげられる[6),7),23)]．個人情報漏洩対策では，PC 等に保管されている個人情報が，管理対象外に出て行くのを防ぐ技術である．具体的には，メールでの個人情報流出の防止機能等のオンラインによるファイル流失の防止機能や入退室管理等のオフラインでのファイル流出防止機能，さらには，PC 上の個人情報検索ツールによる個人情報管理機能等が代表的である．匿名性の維持対策は，個人の匿名性を維持するための技術であり，暗号技術を用いた匿名署名技術や秘密分散技術等がある．これらは，いずれも主に PC 等に保管されているテキスト情報を対象としている．

(b) マルチメディアプライバシ

マルチメディアプライバシでは，3 章の調査結果でも示したように，(a) のこれまでのプライバシ保護技術が対象としているテキスト情報に加え，監視カメラの映像記録情報やコールセンタにおける音声記録情報等のいわゆるマルチメディア情報をプライバシ保護の対象と

して検討する必要が出てきている．これまでに，先駆的な研究として，画像情報に関するプライバシ保護に関しては，画像の抽象化（モザイク，ぼかし等）[24),25)] 等の対処策が，音声情報に関するプライバシ保護では，音質変換や音声モーフィング[26)] を利用した対処策の検討が進められており，今後，実用化に向けた検討が期待されている．

(2) アンビエント化の観点

(a) 既存技術・サービス

ユビキタスの観点からは，RFID（Radio Frequency IDentification）に関するプライバシ保護技術が代表的である．RFID におけるプライバシ保護では，RFID 自体に書かれるコンテンツに加えて位置情報に関するプライバシに留意する必要がある点が特徴である．既存技術として，RFID に蓄積する情報を PC 等であらかじめ暗号化しておき，これを RFID に書き込む可変秘匿 ID 方式[27)] 等が提案されている．

(b) アンビエントプライバシ

1 章で示したように，今後，ユビキタスに続くアンビエント環境では，RFID に加え，さらなるプライバシ情報の拡張として，たとえばセンサに関するプライバシ保護が必要となる．センサに関するプライバシ保護に関しては，広義には，赤外線センサから RFID のようなタグ，そしてカメラやマイクもその範疇に入ることから，多様な検討が必要となる．たとえば，(a) に記したように，RFID では，位置情報に関するプライバシ保護の検討が必要となり，また，監視カメラやマイク等によるプライバシ保護では，前述のマルチメディアプライバシの観点による検討が必要である．今後，これら多様な観点の検討を行うとともに，これらを組み合わせることにより，アンビエント化における新たなプライバシ保護技術やサービスの創出が期待できる．

5.1.3　付加価値創造

(1) 既存技術・サービス

これまでに述べたように，既存のプライバシ保護サービスは，プライバシ情報を保護するためのものであり[6),7)]，プライバシを保護しつつ活用する，といった検討はこれまであまりなされていない．先駆的な研究として Privacy-Preserving Data Mining（PPDM：プライバシを保護したデータマイニング）[28)] がある．PPDM のアプローチの 1 つとして，秘密計算プロトコルを適用し，個人の属性情報を暗号化したまま各種の統計情報や属性間の相関関係等の有益な知識を獲得しようとする手法があるが，研究面が中心であり，実用面に関しての検討はこれからである．

(2) バリューアッドプライバシ

文献 9) や，今年度より開始された経産省の情報大航海プロジェクトの基盤共通技術開発の 1 つに Privacy-Preserving Data Mining が課題として公募されたように[29)]，実用化に向けた検討が加速されている．バリューアッドプライバシでは，これらの技術を研究面から実用化に向けブラッシュアップさせるとともに，その適用領域を統計計算だけでなくより汎用的な適用領域の検討を行うことにより，さらなるサービス拡充が見込める．具体的には，2.2.2 項 (2) で示した秘匿関数計算技術[15)] は任意の計算に適用可能であるが，まだ汎用的な応用に供するには，特に性能面のブラッシュアップが必要である．

5.1.4　ま　と　め

これらの検討結果を，**図 12** および**表 5** にまとめて示す．本論文で提案する次世代プライバシ保護サービスのコンセプトに関して，5.1.1 項から 5.1.3 項で述べたように，個々の要素技術やサービスに関するフィージビリティは十分あるといえるが，今後，これらの要素技術やサービスのブラッシュアップや組合せ等の検討を加速することにより，提案する 3 つの観点（質的向上，量的拡大，付加価値創造）からのコンセプトに基づく新たなプライバシ保護サービスの創出が期待できる．

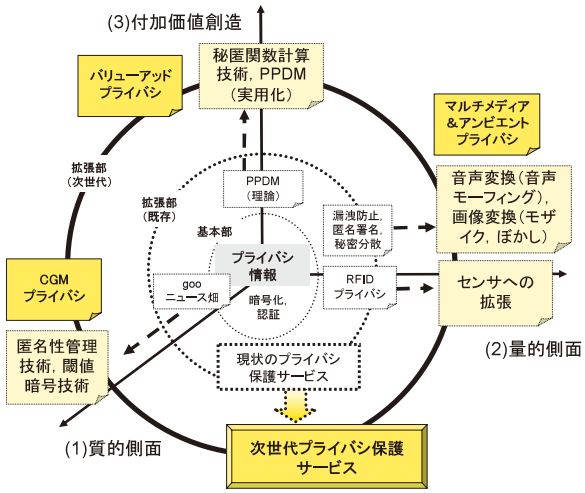


図 12　従来技術との比較
Fig. 12　Comparison with existing technology.

表 5　従来技術との比較評価結果
Table 5　Evaluation result of comparison with existing technology.

		現状のプライバシ保護サービス		次世代プライバシ保護サービス		
		主な技術・サービス	評価	コンセプト	実現のために必要となる主な技術・課題	評価
基本	プライバシ情報保護	暗号化，認証	−	同左		−
拡張	質的な観点	gooニュース畑	△ 編集者による管理	CGM プライバシ	匿名性管理技術，閾値暗号技術	○ CGMへの適用
拡張	量的な観点	漏洩防止，匿名署名，秘密分散	△ テキスト	マルチメディア&アンビエントプライバシ	画像変換（モザイク，ぼかし），音質変換（音声モーフィング）	○ 音声，画像も対応
拡張	量的な観点	RFID プライバシ保護技術	○	マルチメディア&アンビエントプライバシ	センサへの拡張によるアンビエントプライバシ保護技術	○ センサ等への拡張
拡張	付加価値創造の観点	Privacy Preserving Data Mining（研究）	△ 研究主体	バリューアッドプライバシ	秘匿関数計算技術，Privacy Preserving Data Mining（実用化）	○ プライバシ情報活用の実現
総合評価		△ プライバシ保護が主体		◎ 従来のプライバシ保護サービスに比べ，多様な観点からのサービス拡張が期待できる		

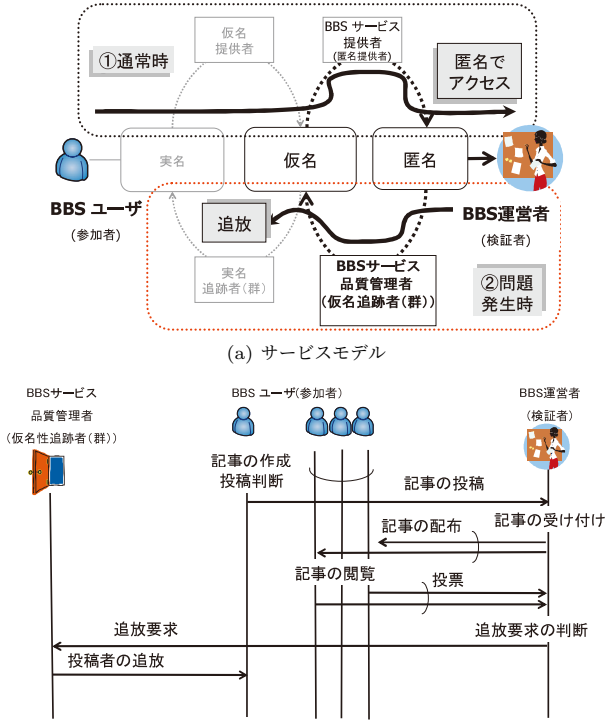
5.2　フィージビリティ評価

ここでは，提案サービスコンセプトのフィージビリティ評価として，具体的なサービス例を示すことにより，本提案コンセプトの有効性について考察する．

5.2.1　CGM プライバシ

CGM プライバシのコンセプトからは，匿名性管理技術をベースに，ID 管理を核とした次世代 BBS（掲示板）サービスの例を示す[18]．5.1.1 項 (1) に示したように，現在，編集スタッフにより掲載管理を行い掲示板が “荒れない” ことを特徴とする掲示板「goo ニュース畑」の提供が開始されている[22]．これに対し，次世代 BBS（掲示板）サービスでは，編集者に加え BBS のユーザも参加して “荒れない” 掲示板とすることが特徴である．以下，**図 13** に示す本サービスのサービスモデルおよびシーケンスを用いて説明する．

次世代 BBS サービスでは，同図 (a) に示すように，参加者である BBS ユーザは，通常時，匿名の状態で検証者である BBS 運営者へアクセスし，その BBS へ投稿を行うことができるが，何か問題のある記事を投稿した場合には，同図 (b) に示すように，BBS ユーザの投票結果と BBS 運営者との合議による追放判断を行い，その結果，追放と判断がなされた場合は，BBS サービス品質管理者に追放要求を発出する．これにより，BBS サービス品質管理者（仮名追跡者（群））の仮名追跡が行われ，その記事を投稿した匿名の BBS ユーザの仮名を明らかにし，BBS からの追放や投稿不可等の罰則を与えることとする．この結果，BBS サービスの品質を維持し，安心・安全な BBS を提供することが可能となる．



(a) サービスモデル

(b) サービスシーケンス

図 13　次世代 BBS サービス
Fig. 13　Next-generation BBS service.

5.2.2　マルチメディア&アンビエントプライバシ

マルチメディア化の観点からは，画像に関するサービスについて紹介する．アンビエントの観点からは，センサをネットワーク化する際に想定されるアドホック NW においてプライバシ保護に対応したサービス例を示す．

(1) 画像プライバシ

画像に関するプライバシ保護は，これまでにプライバシ上，不都合な部分（顔等）に自動

的にモザイクやマスクをかける手法が検討されてきている．馬場口は，これらを具現化したシステムとして PriSurv システム（Privacy Protected Video Surveillance System）を提案している[24),25)]．このシステムは，プライバシ保護のための各種映像画像処理，プライバシポリシ記述，コンテンツ流通におけるセキュリティ等の技術を確立することにより安心感のある映像サーベイランス（video surveillance）の実現を図るものである．PriSurv システムは，情報獲得（センサ），情報流通（ネットワーク），情報表示（インタフェース）に関し，プライバシとセキュリティをトータルに考えている点が特徴である．あらかじめプライバシポリシにより観察者と被写体の間でどのレベルまで視覚情報を開示するかを取り決め，開示情報を動的に，たとえば被写体の状況に応じて変化させつつ映像を生成表示する点が特徴である．この例が示すように，今後，画像に関してもポリシをうまく取り決めることにより，プライバシを保護しつつ映像を楽しめるサービスの提供が見込める．

(2) アドホック NW プライバシ

ここでは，アンビエントプライバシの一具現化形態として，アドホック NW を例にしたプライバシ保護サービスに関して示す．

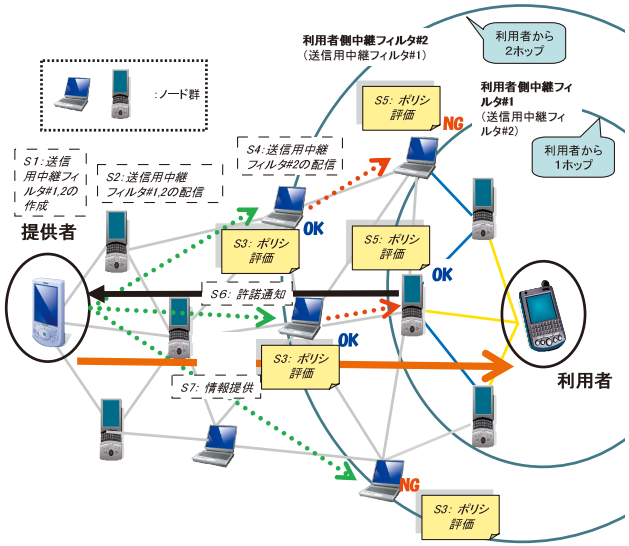
図 14 (a) に示すアドホックネットワークにおいて，直接の知り合いでなくても，ある条件を満たす者同士で，情報やデータの交換等のコミュニケーションを安全に行うことを可能とするために，情報提供者と利用者間のポリシマッチングを（環境等の変化に追従しつつ），第三者である複数の中継ノードが行うことで公平さを保証する双方向マルチフィルタリング技術[30)] によって実現し，情報提供者と利用者双方に対し安心なネットワークサービスを提供しようとするものである．一般にアドホックネットワークでは，通信相手を発見するために，主に適用者側または利用者側の一方にフィルタを設置していたのに対し，本提案サービスにおける双方向マルチフィルタリング技術により，同図 (b) に示すように，提供者と利用者双方の意向を複数の第三者ノード（中継ノード）が汲み取ってマッチング（同図 (b) の S3, S5：提供者と利用者のフィルタリング条件がマッチングする場合のみ通過させる）を行うことが特徴である．

5.2.3　バリューアッドプライバシ

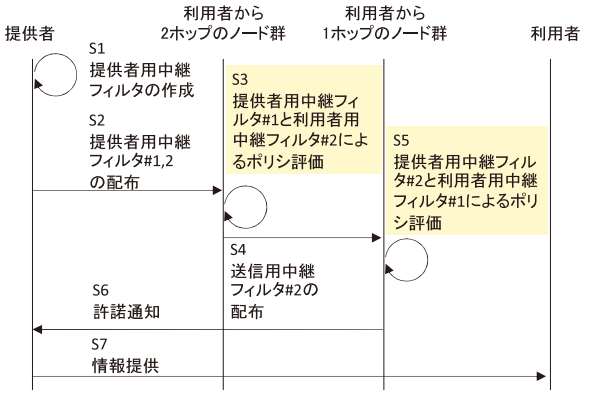
バリューアッドプライバシでは，秘匿関数計算技術をベースに以下のサービスが新たに考えられる．

(1) プライバシ保護アンケート

従来，アンケート情報を外部に依頼して集計を行う必要がある場合，個人を特定できないようにデータを加工してから外部依頼を行うということが一般に行われている．しかし，



(a) アドホックネットワークモデル



(b) サービスシーケンス

図 14　双方向マルチフィルタリング
Fig. 14　Bidirectional multi-filtering.

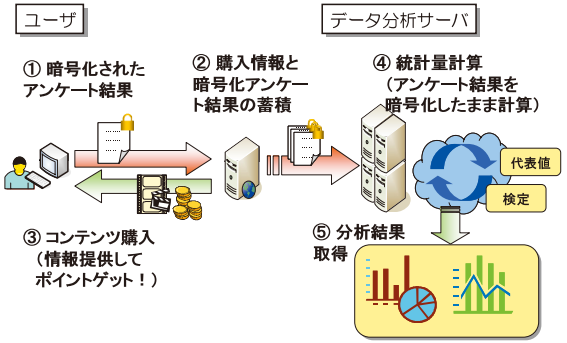


図 15　プライバシ保護アンケート
Fig. 15　Privacy-protection questionnaire.

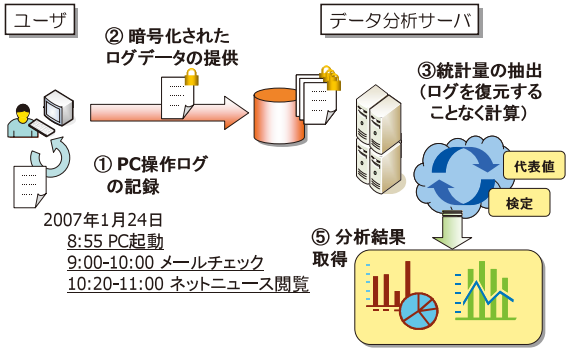


図 16　プライバシ保護履歴収集
Fig. 16　Privacy-protection log collection.

この方法では，データの加工に手間がかかるうえ，そうした加工が行われたために集計者の希望する統計処理が行えないケースが生じてしまうことも想定される．さらに個人情報保護法の施行により，アンケート等の取扱いにも，さらなる慎重さが求められるようになってきている．

これに対し，秘匿関数計算技術を用いると，**図 15** に示すように，アンケート結果を回答者が暗号化したままで任意の演算が行えるため，個々のアンケート情報を漏らすことなく，集計者に統計処理を行わせて，その結果だけを提示する，プライバシ保護アンケートが実現可能になる．

(2) プライバシ保護履歴収集

ここでは，(1) で示したプライバシ保護アンケートのようにユーザが意識的に情報提供するのではなく，パソコン等の操作履歴を自動収集する場合においても有効となることを示す．**図 16** に示すように，各ユーザ端末が，ユーザの端末操作履歴を定期的にオフラインで暗号化し，その後当該暗号文を自動的にサーバ送信し，サーバ側で秘匿関数計算を実行して一般ユーザの端末操作に関する傾向を見る．事業者側はマーケティング等に活用可能な統計情報を得ることができる．これにより，たとえば，ユーザは暗号化したプライバシ情報との引き換えにポイント等のインセンティブを享受できる可能性も想定される．

(3) プライバシ保護データ検索

プライバシ保護データ検索は，暗号化されたメッセージやデータセットを復元することなく文字検索を行うサービスである．たとえば通信内容やファイルデータを暗号化したままブラックリストワードの有無のみ検閲することにより，検閲者はユーザのプライバシを侵害することなくブラックリスト照合を行うことが可能となる．

5.3　ま　と　め

以上，本論文で提案する次世代プライバシ保護サービスのコンセプトは，現状のプライバシ保護サービスに加え，質的向上の観点（モラルの向上：CGM プライバシ），量的拡大の観点（マルチメディア，アンビエント化：マルチメディア&アンビエントプライバシ），さらには付加価値創造としての観点（プライバシ情報の活用：バリューアッドプライバシ），の 3 つの観点に基づき新たなサービス創出をねらいとするものである．本提案コンセプトにより，従来のプライバシ保護サービスによる安心・安全の提供に加え，さらなる適用領域の拡大，利便性の提供をプラスした IT 社会の実現が可能になると考えられる．

6. む　す　び

本論文では，今後のユビキタス環境の進展，特に RFID やセンサ NW の一般化にともなうアンビエント化に向けてますます重要性が高まっているプライバシ保護の問題に対して，最新の暗号応用技術をベースに新たなパラダイムとして，質的向上，量的拡大，付加価値創造を実現する次世代プライバシ保護サービスに関するコンセプトを提案した．すなわち，従来のプライバシ保護技術・サービスが，主にプライバシ情報を保護する技術・サービスであったのに対し，次世代プライバシ保護サービスのコンセプトとして，プライバシ保護とモラル向上の両立（質的向上：CGM プライバシ），マルチメディア化やアンビエント化にと

もなうプライバシ情報の増加（量的拡大：マルチメディア&アンビエントプライバシ），プライバシ保護と活用の両立（付加価値創造：バリューアッドプライバシ）を実現可能とするコンセプトを提案し，これらに関して，既存技術やサービスとの比較による定性的評価および具体的なサービスイメージを用いたフィージビリティ評価により提案コンセプトの有効性を明らかにした．

今後の課題としては，本コンセプト提案のベースとなっている匿名性管理技術や秘匿計算技術等の暗号応用技術の改良とともに，具体的な実サービスへの展開に向けた検討，すなわち性能面や運用面の検討を加速させる．また，実用化を想定したサービス受容性の検討や，個人情報保護法の見直し[31),32)]等，今後の法制度面等の社会科学的な側面からの検討も重要な課題であることから，これらの検討もあわせて行う予定である．以上の検討をふまえ，今後の安心・安全な情報化社会の実現に寄与しうる次世代プライバシ保護サービス創出のために，さらにコンセプトの内容を具体化していく予定である．

謝辞　本研究を進めるにあたり，研究当初の構想段階からご指導・ご協力いただいた塩野入理氏，諸橋玄武氏，佐藤亮太氏に感謝いたします．また，アンケート結果を実証的に示すこと等，有益なコメントをいただいた査読者の皆様に感謝いたします．

参 考 文 献

1) http://www.hitachi-hri.com/handshaking/back/vol_15/img/HS15-Report.pdf
2) http://www.soumu.go.jp/s-news/2004/pdf/041217_7_bt2_10.pdf
3) 新保：ユビキタスメディアの利用とプライバシー保護の限界，情報処理学会研究報告，2006-CVM-152(11), pp.77–84 (2006).
4) 本村，橋本，井上，金田：ネットワーク上での情報統合に対するプライバシー保護，情報処理学会論文誌，Vol.41, No.11, pp.2985–3000 (2000).
5) 萬代：情報処理とプライバシ保護，情報処理，Vol.22, No.9, pp.872–883 (1981).
6) 岡本：プライバシ保護のための要素技術の動向，情報処理，Vol.48, No.7, pp.744–749 (2007).
7) 小松：プライバシ保護のためのアーキテクチャ，情報処理，Vol.48, No.7, pp.737–743 (2007).
8) 影井：情報セキュリティ—守りから攻めへの変革の時，ビジネスコミュニケーション，Vol.44, No.8 (2007).
9) http://www.yano.co.jp/prs/page_overview.html
10) https://www.prime-project.eu/about/
11) http://www.w3.org/P3P/
12) Ministry of Interior and Kingdom Relations, Netherland: Privacy-Enhancing Technologies White Paper for Decision Makers (Dec. 2004).
13) 千田，小宮，林：匿名性確保と不正者追跡の両立が可能な通信方式，情報処理学会論文誌，Vol.45, No.8, pp.1873–1880 (2004).
14) 谷口，千田，塩野入，金井：分散アイデンティティエスクローにおける匿名性/仮名性/本人性の管理に関する考察，信学技報，SITE2005-53, pp.7–12 (Feb. 2006).
15) Chida, K., Yamamoto, G., Suzuki, K., Uchiyama, S., Taniguchi, N., Shionoiri, O. and Kanai, A.: Non-optimistic secure circuit evaluation based on ElGamal encryption and its applications, *IEICE Trans. Fundamentals*, Vol.E90-A, pp.128–138 (2007).
16) 徳田：情報セキュリティの研究開発の動向，情報処理，Vol.48, No.7, pp.693–698 (2007).
17) http://sourceforge.net/projects/jrc-policy-api
18) Pedersen, T.P.: A threshold cryptosystem without a trusted party, Advance in Cryptology-EUROCRYPT'91, LNCS 47, pp.522–526, Spring-Verlag (1991).
19) 佐藤，廣田，山本，谷本，塩野入，金井：分散アイデンティティエスクローを想定した電子掲示板におけるユーザ行動に関する研究，Vol.2007, No.71, 2007-CSEC-038 (2007).
20) Yao, A.C.: How to generate and exchange secrets, *Proc. FOCS'86*, pp.162–167, IEEE Press (1986).
21) http://www.mlit.go.jp/tetudo/kiki_top.html
22) http://help.goo.ne.jp/info/detail/1038/
23) 笠原，佐々木：著作権・個人情報保護と暗号技術，IPSJ Magazine, Vol.45, No.11, pp.1153–1156 (2004).
24) 馬場口：プライバシーを考慮した映像サーベイランス，情報処理，Vol.48, No.1, pp.30–36 (2007).
25) 馬場口：安心な映像サーベイランスのためのプライバシー保護処理，2007-CVIM-157(12) (2007).
26) 高橋，大西，森勢，坂野，河原：音声モーフィングのための母音スペクトル間区分線形写像の自動設計手法，FIT2007，E-041 (2007).
27) 木下，星野，小室，藤村，大久保：ローコスト RFID プライバシ保護方法，情報処理学会論文誌，Vol.45, No.8, pp.2007–2021 (2004).
28) 菊池：データマイニングと個人情報保護，FIT2004 (2004).
29) http://www.igvpj.jp/pdf/igvpj_outline.pdf
30) 山本，谷本：アドホックネットワークにおけるマルチフィルタリング，DICOMO2007, pp.33–40 (2007).
31) http://www5.cao.go.jp/seikatsu/kojin/20060228moshiawase.pdf
32) http://www5.cao.go.jp/seikatsu/kojin/gaidorainkentou.html

(平成 19 年 10 月 10 日受付)
(平成 20 年 4 月 8 日採録)

谷本　茂明（正会員）

1982 年徳島大学工学部電気工学科卒業．1984 年徳島大学大学院工学研究科電気工学専攻修了．同年日本電信電話公社入社．入社以来，主にプライベートネットワークシステムにおける研究開発に従事．現在，NTT 情報流通プラットフォーム研究所セキュリティ社会科学グループ主幹研究員．情報セキュリティ，プライバシ保護等の研究に従事．電子情報通信学会，IEEE 各会員．博士（工学）．国立情報学研究所客員教授．

廣田　啓一（正会員）

1995 年三重大学工学部情報工学科卒業．1997 年三重大学大学院工学研究科情報工学専攻修士課程修了．同年日本電信電話株式会社入社．現在，NTT 情報流通プラットフォーム研究所セキュリティ社会科学グループ研究主任．自然言語処理，権利流通，コミュニティ研究等を背景とした情報セキュリティ技術，特にプライバシ保護技術の研究開発に従事．

山本　太郎（正会員）

1992 年北海道大学工学部情報工学科卒業．1994 年北海道大学大学院工学研究科情報工学専攻修士課程修了．同年日本電信電話株式会社入社後，データベース研究部門にて，医療情報システム等向けのアクセス制御システムの研究開発等に従事．現在，NTT 情報流通プラットフォーム研究所セキュリティ社会科学グループ研究主任．主に社会科学的アプローチからのプライバシ保護活用技術の研究に従事．

千田　浩司（正会員）

1998 年早稲田大学理工学部情報学科卒業．2000 年早稲田大学大学院理工学研究科数理科学専攻修士課程修了．同年日本電信電話株式会社入社．現在，NTT 情報流通プラットフォーム研究所セキュリティ社会科学グループ所属．主に，暗号理論に基づくプライバシ保護強化技術の研究に従事．博士（工学）．2004 年より情報処理学会コンピュータセキュリティ研究会（CSEC）運営委員．電子情報通信学会会員．電子情報通信学会 SCIS2000 論文賞受賞．

畑島　　隆（正会員）

1993 年名古屋大学工学部情報工学科卒業．1995 年名古屋大学大学院工学研究科博士前記課程修了．同年日本電信電話株式会社入社．入社以来，インターネット上のネットコンテンツに対する利用者の関心度を計量する手法やサーチエンジンにおける表示順位決定方式の研究，情報配送システムにおける効果的な配送方式やサービス連携プラットフォームの研究開発に従事．現在，NTT 情報流通プラットフォーム研究所セキュリティ社会科学グループ研究主任．情報システムのセキュリティに対する社会科学的アプローチによる研究に従事．本会 1997 年度第 54 回全国大会優秀賞受賞．

高橋　克巳（正会員）

1988 年東京工業大学理学部数学科卒業．2006 年東京大学大学院情報理工学系研究科電子情報学専攻博士後期課程修了．1988 年日本電信電話株式会社入社．現在，NTT 情報流通プラットフォーム研究所セキュリティ社会科学グループリーダ．情報セキュリティ，プライバシ保護，情報検索，データマイニング，地理情報処理等の研究に従事．本会 1999 年度論文賞受賞．博士（情報理工学）．

金井　　敦（正会員）

1980 年東北大学工学部通信工学科卒業．1982 年東北大学大学院工学研究科情報工学科博士前期課程修了．同年日本電信電話公社入社．以来，クロスコンパイラ，ソフトウェア開発プロセス，ソフトウェア設計技法，ソフトウェア開発環境，超高速 Web 検索技術，ネットワークコミュニティ，情報セキュリティの研究開発に従事．2008 年 4 月より，法政大学理工学部応用情報工学科教授．博士（情報科学）．電子情報通信学会，IEEE 各会員．