プライバシ保護のための要素技術の動向

8

岡本栄司 筑波大学

近年，情報社会の進展が目覚しいが，それとともに情報に対する脅威も高まっている．情報漏洩もその 1 つであり，プライバシ確保は一般ユーザの大きな関心の 1 つである．そこで，科学技術振興調整費「セキュリティ情報の分析と共有システムの開発」において，大学や企業等，複数の研究機関が，プライバシ関連技術の研究を平成 16 年度から 18 年度に渡って行ってきた．ここではその活動を解説する．なお，本稿は本特集「7. プライバシ保護のためのアーキテクチャ」とペアをなすものである．プライバシ保護全体像を受けて，ここでは，プライバシ保護のための要素技術を解説する．

プライバシ保護技術の必要性と対策

最近，プライバシ保護の必要性が叫ばれているが，その大きな原因に人とモノ，および情報の ID 化が急激な勢いで進んできたことがあげられる．実際，住民基本台帳ネットワーク（住基ネット）の住民票コードにより各人に ID 番号が付与されネットワークが稼働しており，また，無線タグによりあらゆる商品に ID が付与されようとしている．さらには，コンテンツにも ID が埋め込まれつつある．

しかしながら，原則的に ID は公開情報であるため，コンピュータやネットワークの進歩により，経済活動に関連して収集され，データベース化されることが予想される．それに伴い，ID や電子化文書を悪用することも可能となっている．実際，技術的には，あらゆる情報が，すべての人々に，瞬時に共有可能となりつつある．このため，ID 化された個人の情報ばかりでなく，個人そのものの所在などまで不特定の人に知られるというプライバシの問題が生じたり，悪評を立てられることになる．

また，ID の改ざんや盗んだ ID を悪用する可能性も出てくる．現にこのような ID の盗用（ID Theft）は，米国で大きな社会問題になっており，確実性の高い個人認証が必要となっている．同様に，モノに対しては ID 耐偽造化が求められる．

社会は人・モノ・情報が中心となって動いているが，その電子化においては，「プライバシを保ちながら真正なユーザが信頼できる情報を扱える」ことが，安心・安全で快適な社会の実現に繋がる．本研究はこれを実現するための情報セキュリティ対策技術に焦点をあて，その確立を目指して研究を進めたものである．

システムの全体像を図 -1 に示すが，これは文献 6）の図 -7 に，必要となるサブテーマを示したものである．以下，これらのサブテーマごとに説明する．

匿名署名技術

本研究においては，さまざまな重要情報をセキュアでプライバシを守ったかたちで利用できるシステムで必要な，匿名署名やグループ署名等に関する要件の抽出と，機能・性能・安全性に関する分類，これらの署名方式を実現するためのアルゴリズムの調査研究等を行った．また，最小構成のシステムを構築し，モジュールレベルでの性能面を中心とした評価等を行った．具体的には，ペアリングと呼ばれる双線形写像関数を用いたグループ署名ライブラリのプロトタイプを作成し，モジュールレベルの評価を行った．担当は筑波大学，情報セキュリティ大学院大学，NEC であった．

■匿名署名技術についての成果

匿名署名やグループ署名等に関する要件の抽出，分類，実現方式の比較調査を行った．匿名性を有する署名は，ブラインド署名，グループ署名，1-out-of-n 署名，リング署名等があるが，まず，これらの各方式について，署名長，署名生成と検証の速度等を中心に特徴を明らかにした．表 -1 に代表的な匿名性を有する署名方式の特徴を示す．表 -1 の特徴は方式の概念提案時のもので，現時点では多少改良されているものもある．

この結果を受け，署名時に他のエンティティとの通信

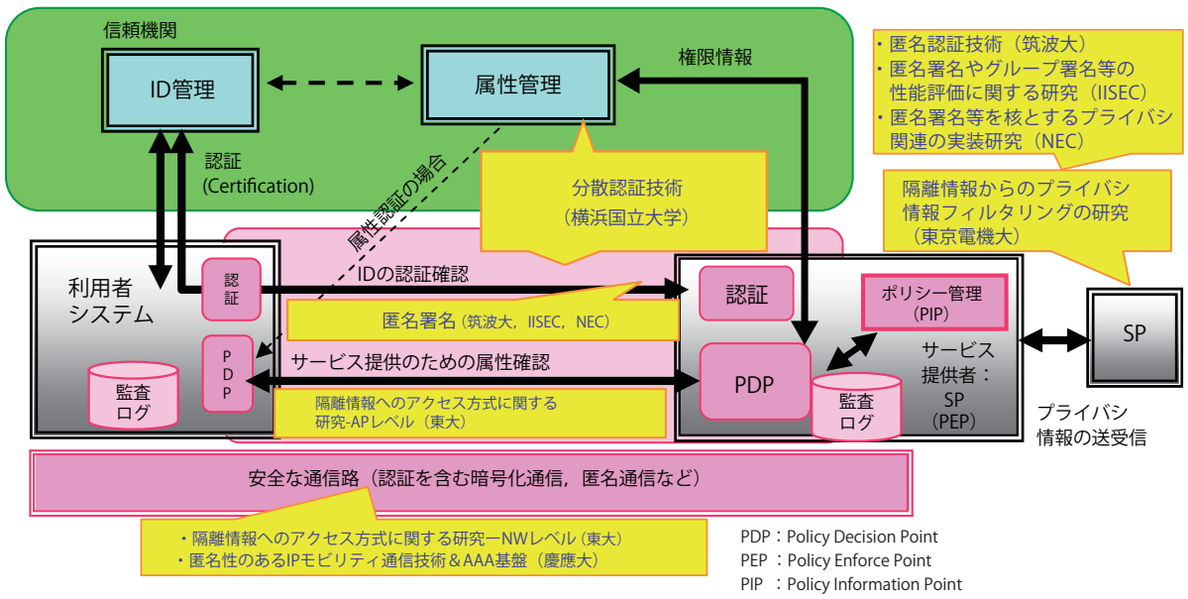

図-1　プライバシ保護システムのコンポーネント関連と各機関における研究テーマ

方式	署名長	登録等の事前処理	署名時通信	速度	
				署名	検証
ブラインド署名	短	ほぼ不要	必要	速い	速い
グループ署名	やや長	必要	不要	やや遅い	やや遅い
1-out-of-n 署名	n に比例	ほぼ不要	不要	n に比例	n に比例
リング署名	n に比例	不要	不要	n に比例	n に比例

表-1　匿名性を有する署名の特徴

が不要であり，署名長を短くできるグループ署名に対象を絞り，Bellare らによりなされたグループ署名のモデルと安全性の形式化を中心に，安全性等の要件抽出を行った．

この調査結果を踏まえ，重要情報をセキュアでプライバシを守ったかたちで利用できるシステムについての研究も行った．特に署名者が複数である署名の機能拡張等について研究を進め，

- 署名順序検証可能な ID ベースの多重署名の提案
- 閾値付き署名（k-out-of-n 署名，“just” k-out-of-n 署名）
- 追跡可能型署名（detective 署名，traceable 署名）の提案
- 匿名性を重視した暗号系（オブリビアス署名，遠隔地支援型暗号通信）の提案
- 通信相手の匿名性を管理できるペアリング型鍵共有方式

などの成果を得た．

■ソフトウェア試作

本研究では，実装研究と基盤ソフトウェア試作も目標の 1 つである．得られた成果物は以下の通りである．

①標数 p の楕円曲線ライブラリ・ペアリングライブラリおよび標数 3 の楕円曲線ライブラリ・ペアリングライブラリを用いたグループ署名ライブラリ（東京電機大学の匿名内部告発システム（改良型墨塗り署名技術）の実装へ提供）

② XML 形式上でセキュリティ情報を送受信する SAML（Security Assertion Markup Language）を利用したユーザアシスタント機能（横浜国立大学の分散認証技術の実装へ提供）

本稿では①について解説する．詳細は文献 1）を参照されたい．

調査・検討の結果，今回の実装のターゲットとして，署名長を短くできることからペアリングを用いるグループ署名方式（Boneh らの Short Group Signature）を選んだ．

匿名性を有する署名としてグループ署名ライブラリを作成する場合，処理性能，安全性，今後の拡張などを考慮したインタフェースの設計について検討を進める必要がある．ライブラリの構成は下位層から順に体演算ライブラリ，楕円曲線ライブラリ，ペアリングライブラリから構成されており，グループ署名ライブラリの利用者には内部ライブラリ群の存在を意識させないアーキテクチャを策定し実装している．下位ライブラリのパラメタ

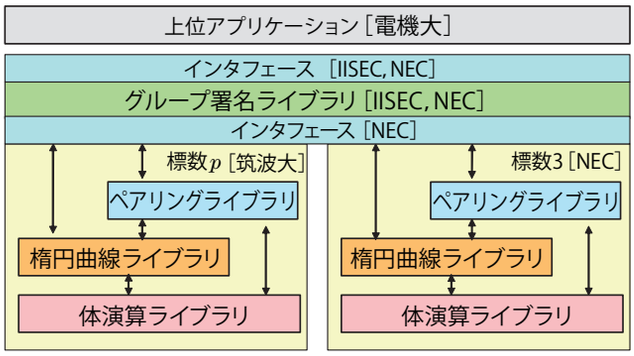

図 -2 グループ署名ライブラリ全体像

についても処理性能と安全性を評価しつつ，実装対象となるパラメタを決定した．本ライブラリ実装ではライブラリ初期化の関数を用意し，ライブラリハンドルを用いることでグループ署名，正確には下位のペアリングライブラリを定めるパラメタを利用者側で選択可能となるようにした．下位ライブラリのうちのペアリングライブラリについては，標数p（大きな素数）の有限体上の楕円曲線上の Tate ペアリングに工夫を加え高速化したものと，標数 3 の有限体上の「η ペアリング」を選び実装した．図 -2 にグループ署名ライブラリの全体像を示す．

このグループ署名ライブラリは内部で使用する楕円曲線ライブラリやペアリングライブラリを完全に包含しており，これらが変更された場合でもグループ署名ライブラリのインタフェースへ影響を与えないアーキテクチャを採用して実装を行っている．したがって下位（ペアリング）ライブラリの拡張等にも柔軟に対応するものができたと考えている．

このライブラリについては，現実的な環境でモジュールレベルの性能評価を行うとともに，東京電機大学が研究している匿名内部告発システムの一部として組み込むことで，インタフェースが妥当であること，システムとして利用する場合も実用上問題ない処理性能であることを検証した．

今後の発展としては，より高速な楕円曲線ライブラリの採用や他のグループ署名アルゴリズムの採用によるライブラリの活用範囲の拡大等が考えられる．また，本研究にて試作したグループ署名ライブラリを公開することなどで，他の研究機関等における匿名性を有するアプリケーションの試作と評価などに寄与したい．

情報隔離技術

プライバシ情報を含めた内部情報の漏洩や不要な外部情報の流入をフィルタリングすることにより情報を隔離する技術がテーマである．担当は東京電機大学であった．本プロジェクトでは電子メールシステムをターゲットとし，電子メールにおける情報隔離技術の実現を目指した．主な研究成果として

①暗号化メールにおける個人情報チェックシステム
②ワンタイムメールシステムの提案
③情報漏洩データベースの提案
④公益情報者保護システムの提案と開発

があるが本稿では①についての解説をする．詳細は文献 2) を参照されたい．

■暗号化メールにおける個人情報チェックシステム

近年増加しつつある個人情報等のプライバシ情報の漏洩の経路の 1 つとして，電子メールがある．一方，メール内容の機密性保持のために暗号化メールが普及しつつある．暗号化メールではメール内容が暗号化されているためチェックすることができないという性質があり，暗号化メールにより機密性を保持しようとするとプライバシ情報漏洩を防ぐことが難しくなるという問題がある．そこで，暗号化によりセキュリティを確保しつつ，プライバシ情報が漏洩することを防止することができる，効率的なフィルタリング技術とそれを用いたメールシステムを提案することを目標とした．

まず，基本となる個人情報の不正送出を防止する不正情報チェックシステムを開発した．チェックシステムの基本的な流れは以下の通りである．メールサーバに搭載されたチェックシステムでは社員のメールチェックを行い，不正がないと判断されればメール受信者へメールが送信される．しかし，個人情報の不正送出が疑われるメールを検出した場合，メールの送出を止め上司に転送し，上司の判断を仰ぐ．上司はそのメール内容が不正送出かどうかの確認を行い，外部への送信の可否を決定する（図 -3）．

この方式では，チェックの結果，問題がなければ S/MIME などの従来方式に戻すことができるので，一般の人は従来と同じメールプログラムの利用が可能であるというメリットがある．本システムの有効性を確認するため，プログラムを開発し，実験を行った．

チェックシステムのチェックでは，強い暗号による暗号化メールを乱数性判定により通常メールと効率的に区別することができた．また，処理速度については，クライアントのアリスからメールクライアントを用いて，メールを送信して処理時間を計測したところ，各機能を含むシステム全体の処理時間が 0.92 秒であった．これより，メール 1 通あたり，約 0.9 秒の遅延が発生することになるが，ある程度の遅延を許容するメールの性質から送受信の障害にはなりにくいと考えられる．

乱数性を持たない弱い暗号に対してはスパムメールフ

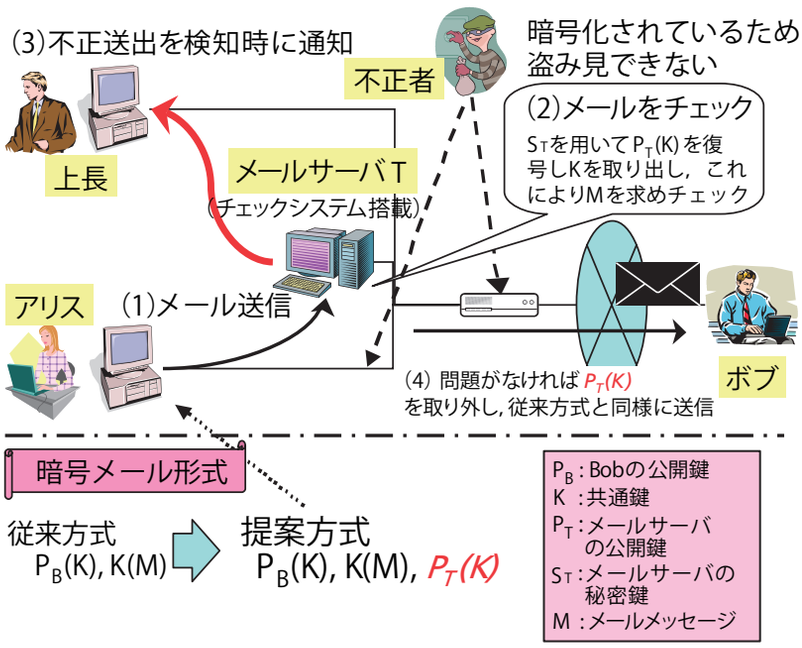

図 -3　個人情報チェックシステム

ィルタリングソフトを用いた弱暗号チェック方式を提案した．さらに開発と実験評価を行い，弱暗号を検出するフィルタリング方式としての有効性と効率を確認した．

これらのチェック機能を実現したフィルタリングプログラムを不正情報チェックシステムに組み入れ「個人情報不正送出チェックシステム」を構築し，実験評価を行った．「暗号化によりセキュリティを確保しつつ，プライバシ情報が漏洩することを防止する」という目的に対して一定の達成を見たと考える．

分散認証技術

電子媒体を利用したサービスの増加・多様化に伴い，ユーザの属性を確認するための属性認証技術や，ユーザのプライバシ保護の需要が高まっている．本研究では，ユーザがすべての個人情報を手元に集めるのではなく，秘密分散方式を利用して個人情報を分散管理する分散属性認証方式を提案し，考察した．担当は横浜国立大学であった．

分散属性認証方式は，従来の属性認証方式のモデルとは異なり，秘密分散を利用してユーザの属性情報を分散した分散属性情報，ユーザの ID を組にして複数の機関に登録しておき，ユーザが選択した属性の種類に対応する分散属性情報を示す分散属性証明書（SAC：Shared Attribute Authority）を一定数の機関が仮 ID をもとに発行する属性認証方式である．仮 ID は，サービス提供者がユーザに対して，ユーザのサービス要求ごとに発行する値である．ユーザは，一定の数だけ分散属性証明書を集めて匿名属性証明書（AAC：Anonymous Attribute Certificate）としてサービス提供者に示す．仮 ID を利用して，分散属性証明書や匿名属性証明書の利用先を分散属性証明書発行機関に隠したままとし，利用をワンタイムに限るための工夫をしている．

分散属性認証方式の特徴は，属性情報を管理する機関からの属性情報の漏洩に対する耐性，ユーザが選択した属性だけを示すことができる機能，そして証明書に示した属性以外のサービスを何回利用したかといった情報も含めたユーザのサービス利用情報を必要以上に流出させない機能を同時に持つプライバシ保護機能と，従来の属性認証方式では考察されていなかったサービスを利用するユーザと属性証明書を提示しているユーザが同じであることまでを要求するサービス不正利用防止機能を持つことである．また，分散属性認証方式がプライバシ保護機能と不正利用防止機能を持つことを一般的なセキュリティ技術であるディジタル署名技術などの要素技術の安全性に帰着させて証明できる．単純に秘密分散を利用したデータベースとディジタル署名などの技術を組み合わせただけでは，これらの機能を持つことを証明できない．

本方式は，以下のようにまとめられる．詳細は文献 3）を参照されたい．

- 複数の分散属性認証機関を設け，秘密分散技術により分散属性情報を分散して管理
- サービス利用に求められる属性情報の組を利用者が選択して，複数の分散属性認証機関へのアクセスを通じ，ワンタイムの匿名属性証明書を作成し，サービス提供者に提示．サービス提供者が確認して利用者にサービスが提供される．
- 衝突困難なハッシュ関数，安全な（k, n）秘密分散方式，安全なディジタル署名方式，安全な暗号化方式（これらの要素技術は特殊なものでなく一般的な技術でよい）の利用を前提として，求められる安全性（関連付け困難性，偽造困難性，なりすまし困難性）が証明できるプロトコルを実現．
- SAML，XML 署名，(2, n) 閾値法，SSL 等を用い，Java プログラムとして実装し実証．Internet 環境で実験．

分散属性認証方式は，一般のセキュリティ技術で構成でき，ユーザのニーズに柔軟に対応する属性認証方式で

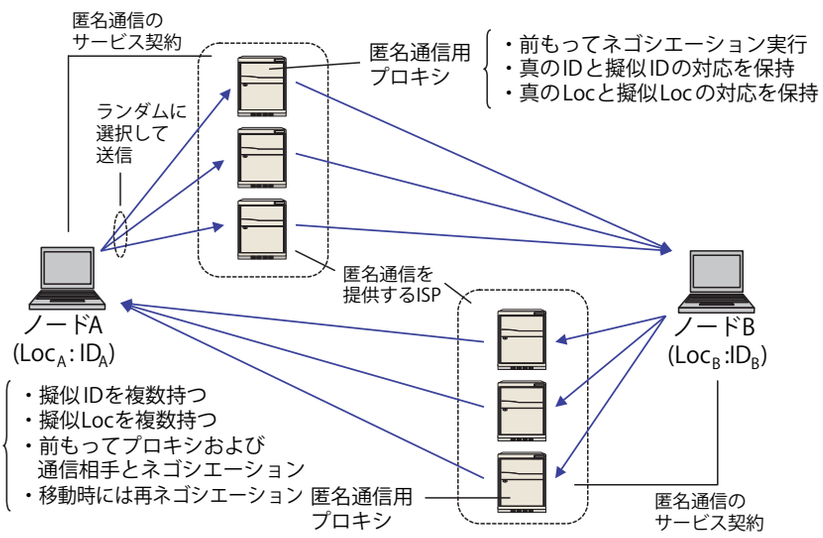

図 -4 SLIN6 の概要

ある．具体的なネットワーク利用サービスへの応用が開拓できれば有効ではないかと期待する．

匿名性のある IP モビリティ通信技術

本研究の目的は，現実のインターネットにおいて実用に耐える匿名性のある IP モビリティプロトコルを開発することである．担当は慶應義塾大学であった．

インターネットにおいて移動しながら通信を行う際，本来は移動ノードの認証，権限委譲，課金情報収集（Authentication, Authorization, and Accounting，AAA 機能）が必要となるが，現状では移動体通信プロトコルと AAA 機能との連携が図られていない．また，現在の移動体通信プロトコルでは通信路の監視などにより，どのノード同士が通信しているかということを知られたり，移動ノードの位置追跡をされてしまう．上記の問題点を解決するため本研究では 2 つの目標を立てた．1 つは匿名性のある IP モビリティ通信プロトコルを設計・実装すること，もう 1 つはモビリティを考慮したマルチドメイン環境における AAA 基盤を構築することである．研究成果として，第 1 の目標については IPv6 上での移動通信プロトコルである LIN6（Location Independent Networking for IPv6）を基盤とした SLIN6（Stealth LIN6）を開発・実装し，基本性能を測定した．第 2 の目標については，調査の結果マルチドメインに適した AAA プロトコルとして IETF（Internet Engineering Task Force）で標準化が行われているプロトコルである Diameter, PANA（Protocol for carrying Authentication for Network Access），EAP（Extensible Authentication Protocol）の組合せが最適であると判断し，これらのプロトコルを組み合わせた最初の汎用的な AAA 基盤を構築した．本稿では匿名性のある IP モビリティ通信技術についての解説を行う．詳細は文献 4）を参照されたい．

SLIN6 の開発

インターネットのモビリティ環境においては IP ヘッダの暗号化ができないため，IP ヘッダを盗聴することにより送受信者の識別や移動ノードの移動軌跡の追跡が可能となってしまう．匿名性を持つ IPv6 モビリティプロトコルである SLIN6 では，図 -4 に示すように通信するノードはそれぞれ匿名通信を提供するサービスプロバイダと契約し，匿名通信プロキシを介して通信する．たとえばノード A は複数の匿名通信プロキシをランダムに選択して送信する．その際，IP ヘッダに格納される始点アドレスや終点アドレスには擬似 ID や擬似 Locator を使用することにより，盗聴者が IP ヘッダを盗聴しても送受信ノードの特定は不可能であり，またノードが移動した際も移動の軌跡を追跡することは不可能となる．

SLIN6 は IPv6 でのノードモビリティプロトコルである LIN6 をもとに設計した．LIN6 はノードの ID と Locator を分離するアーキテクチャに基づく LIN6 アドレスを導入している．LIN6 アドレスにおいては，パケット転送中に Locator 部分を書き換えても問題ない．SLIN6 はこの性質を利用して擬似 ID や擬似 Locator の使用を可能にしている．また，SLIN6 では通信に先立って空いているノードや使用する匿名通信用プロキシ間で使用する擬似 ID や擬似 Locator をネゴシエーションする必要がある．ネゴシエーションに使用されるパケットについては，盗聴されてはいけない情報に関しては暗号化している．

本研究では SLIN6 を FreeBSD 上に実装した．実装はカーネル部分の改良とユーザスペースにおけるデーモンプロセスからなる．FreeBSD 上に実装した SLIN6 について，実験ネットワークにおいて目的とする匿名性が得られているかを検証し，また通信のオーバーヘッドを測定した．匿名性の検証については，実験ネットワーク上で SLIN6 におけるネゴシエーションパケットおよびデータ通信パケットを盗聴し，送受信者のノード ID およびノード Locator の真の組合せが得られないことを確認した．通信のオーバーヘッドに関しては，通常の IPv6 と比較した SLIN6 の送信処理時間は +12.5%，受信処理時間は +44.7% となった．しかし実際の値はマイクロ秒の単位であり，インターネットにおける RTT（Round

Trip Time）に比較すると十分小さいものであることが分かった．また SLIN6 は通信開始前に匿名通信用プロキシや通信相手とネゴシエーションを行う必要があり，この処理には，IPv6 における重複アドレス検出処理のため，秒単位の時間がかかることが分かった．

隔離情報へのアクセス方式に関する研究

本研究では，通信レイヤにおける匿名通信技術およびアプリケーションレイヤにおける匿名認証技術を開発し，統合することでユーザの個人情報等を保護したまま必要な認証サービスを利用する，いわゆる隔離情報へのアクセス方式の構築を行った．担当は東京大学であった．詳細は文献 5)を参照されたい．

匿名通信技術とは，送・受信者の匿名性を保ったまま通信を行う技術であり，電子投票や内部告発，匿名相談システム等がその応用例としてあげられる．アドホックネットワークに代表されるような動的なネットワーク上でなんらかの双方向通信を行う際，送信時に利用した経路を返信時では利用できないケースは当然考慮されるべきであるが，とりわけ，返信時にその返信先を知ることができない匿名通信においては，これはそう単純な問題ではない．特に匿名医療相談など，返信までのタイムラグが大きいアプリケーションほどそのような問題に陥る可能性は高い．しかしながらこうした点について従来の匿名通信方式では十分に考慮されているとは言い難い．そこで本研究では主な既存方式の特徴や問題点とその原因を整理した上で，新たに高いデータ可用性を有した方式を提案し，またこれら提案方式を含め種々の組合せについて匿名性，データの可用性，および操作のコストという観点からの比較検証を行った．

これまで提案されてきた匿名技術において最も高い匿名性を有していた通信方式はオニオンルーティング方式であり，ルーティングテーブルの多重暗号化およびルートの選択により送受信者のリンク情報を秘匿する手法が用いられていた．しかしながら，各中継ノードの公開鍵により多重暗号化されている情報を他の中継ノードが確認することができないことは，ノードの消滅などが起こりやすい動的ネットワークにおいては深刻なデータ可用性の低さの原因となっている．そこで本研究においては，安全に上位の匿名認証プロトコルと組み合わせた匿名アプリケーションを実現すべく，オニオンルーティング手法に匹敵する匿名性を有しながらも，可用性の高い方式の実現を目標とした．また同時に，匿名アプリケーションの使用時の動作等を非有識者に対しても分かりやすく表現するようなプロトタイプの作成を目指した．

その結果，現実的に考え得る結託者のノード支配率の範囲においてほとんどオニオンルーティング方式の匿名性を低めることなく，飛躍的に可用性を高めることに成功した．我々の提案方式では従来の主流なやり方であったルーティングテーブルの多重暗号化を使用せず，代わりに各中継ノード用の公開鍵で暗号化された単暗号化ブロックを用いてルーティングを行うことにより，ネットワークトポロジの動的な変化により中継の順序，あるいはノード自体が入れ替わったとしてもより柔軟に対応できる（可用性の向上）．しかも，従来方式の中で最良の匿名性を有するオニオンルーティング方式と比較しても，現実的なネットワーク環境(パラメータ)において，ほとんど匿名性を劣化させることなく構築できることを示すことができた．また GUI を用いて，匿名通信路上で動く匿名アプリケーションのプロトタイプも作成した．

おわりに

科学技術振興調整費による各研究機関の取り組みを述べることにより，プライバシ保護システムにおける要素技術を説明してきた．これらはシステムの要素となるものであるが，各々独立して利用することもできるようになっており，たとえばライブラリ化も行われている．

最後に，プライバシ関連技術の研究に参加して研究推進したメンバには，労力を惜しまず協力していただき感謝する．特に，小松・側高 (NEC)，土井 (情報セキュリティ大)，岡本(健)・金山(筑波大)，佐々木・斉藤(東京電機大)，松本・四方 (横国大)，寺岡 (慶大)，田村・繁富(東大，現産総研)の各氏には深謝する．

参考文献

1) 側高幸治，松田誠一，土井　洋，岡本　健，小松文子，岡本栄司：匿名署名を実現するための Pairing を用いたグループ署名ライブラリの実装，DICOMO'07 (2007).
2) 安　健司，赤羽泰彦，尾崎将巳，瀬本浩治，佐々木良一：暗号メールにおける個人情報不正送出チェックシステムの評価，情報処理学会論文誌，Vol.46, No.8, pp.1976-1983 (Aug. 2005).
3) 松本　勉，四方順司，堀　正義，大野一樹，塩田明弘：分散属性認証方式の実装と評価，情報処理学会 2006 年コンピュータセキュリティシンポジウム論文集，CSS 2006 (Oct. 2006).
4) 市川隆浩，坂野あゆみ，寺岡文男：Stealth-LIN6：匿名性のある IPv6 モビリティ通信，情報処理学会コンピュータセキュリティ研究会 (Mar. 2006).
5) 田村　仁，古原和邦，今井秀樹：動的ネットワークにおける双方向匿名通信路構築手法の提案，情報処理学会論文誌，シームレスコンピューティングとその応用技術・特集号，Vol. 48, No.2, pp.494-504 (Feb. 2007).
6) 小松文子：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 (July 2007).

（平成 19 年 5 月 29 日受付）

岡本栄司（正会員）okamoto@risk.tsukuba.ac.jp

1973 年東工大・工・電子卒業．1978 年同大学院博士課程修了．工学博士．同年日本電気入社．その後，北陸先端大，東邦大を経て 2002 年より筑波大教授，現在に至る．情報セキュリティの教育・研究に従事．1990 年電子情報通信学会論文賞，1993 年本会 Best Author 賞受賞．本会フェロー．