様式Ｆ－１９

科学研究費助成事業（学術研究助成基金助成金）研究成果報告書

平成２５年５月２３日現在

機関番号：１３９０３
研究種目：若手研究（B）
研究期間：2011～2012
課題番号：２３７０００７４
研究課題名（和文）　需要家主導でプライバシー制御するスマートグリッドの情報提供に関する研究
研究課題名（英文）　Study on Customer Controllable Information Sharing for Smart Grid

研究代表者
白石　善明（SHIRAISHI YOSHIAKI）
名古屋工業大学・工学研究科・准教授
研究者番号：７０３５１５６７

研究成果の概要（和文）：次世代送電網（スマートグリッド）では、需要家（電気の最終利用者）のプライバシーに関わる情報である家庭内での活動の詳細なタイムライン（電力消費履歴）が収集され、電力産業以外の様々な組織に使用される。需要家が安心してプライバシー情報を提供するために、需要家主導で開示先の制御ができ、セキュアに情報を流通させる技術の開発は、スマートグリッドを社会的基盤システムにしていく上で必要不可欠である。本研究では、このような情報流通基盤をタイムラインを保管する主体の導入により実現することを目指し、需要家とサービス利用者の間の情報流通を安心して行える要素技術の開発を行った。

研究成果の概要（英文）：Customer's timeline, history of power consumption, is collected and widely used by service providers in Smart Grid. One of important issues is to provide secure information sharing platform in order that Smart Grid becomes social infrastructure system. This research proposes the three components for secure information sharing; a threshold cryptography-based cloud storage, a fair exchange protocol, and an order-stamping protocol.

交付決定額

（金額単位：円）

	直接経費	間接経費	合　計
交付決定額	2,400,000	720,000	3,120,000

研究分野：総合領域
科研費の分科・細目：情報学・計算機システム・ネットワーク
キーワード：ネットワーク，スマートグリッド，プライバシー保護，情報流通，アクセス制御

１．研究開始当初の背景

スマートグリッドを推進する理由の一つに省エネがある。エネルギー利用効率の向上を目指す例として、現在は工場やビルのような大口の需要家に対してのみ行われていたデマンドレスポンスを、スマートメータ（情報通信・制御機能を備えた電力メータ）を家庭などの小口の需要家に設置することで実施できるようにすることが、スマートグリッドの構想に含められている。

このようなスマートグリッドの標準化に向けた枠組みがアメリカ国立標準技術研究所（NIST）により示されている。その中で、セキュリティとプライバシーの確保は重要な課題として挙げられている。

例として挙げたデマンドレスポンスのための基本データは需要家の電力消費履歴（タイムライン）となる。デマンドレスポンスのような小口の需要家の協力を得る必要があるサービスのためには、需要家がスマートメータを介して安心してスマートグリッドに接続できる環境を用意しなければならない。具体的には、需要家が安心して一次情報を提供するためには、配電などのサービス提供者に情報を預ける際に、需要家の意思（ポリシー）を反映した一次あるいは二次情報として

利用されるようなプライバシー制御ができる情報流通基盤の確立が必要である。

２．研究の目的

本研究では、このような情報流通基盤をタイムラインを保管する主体の導入により実現することを目指し、需要家とサービス利用者の間の情報流通を安心して行える要素技術の開発を行う。データ（タイムライン）保管者を導入した際のデータ提供時の懸念事項は、(1)データ保管者の目的外の閲覧、(2)第三者によるデータの不正な入手、(3)データの不正な二次利用であり、これらを解消するシステムを実現するための情報提供方式を開発する。

３．研究の方法

本研究では、(1)データ保管者はデータの閲覧ができない、(2)開示許可のない者はデータを利用できない、(3)利用許可のない者に対するデータの二次利用の防止あるいは抑止がなされる、以上の３つの要件を満たすデータ提供方式を実装するための要素技術を開発する。(1)および(2)については、Cryptographic Cloud Storage の構成により、(3)についてはデータの確実な受け渡しと適切なログ保管により満たすことを考える。

４．研究成果

情報流通基盤としてある種のクラウドストレージサービスを利用する際、サービス利用者にとってはサービス提供者の不正なデータの閲覧が懸念される。これを解消するために、データをサービス利用者側で暗号化し、復号に必要な鍵をグループ内のサービス利用者に開示してデータを共有する Cryptographic Cloud Storage という考え方がある。

Cryptographic Cloud Storage の研究では、データの機密性（サービス提供者であってもデータを閲覧できないこと）を保つために属性ベース暗号や ID ベース暗号が用いられているが、これらの暗号方式は PKG（Private Key Generator）という、サービス利用者の属性や ID に対応する秘密鍵を生成する主体が必要になる。サービス提供者が PKG を運営すると復号権限が集中し，サービス利用者にとっての懸念は解消しない。

本研究では、サービス利用者以外のデータを復号する能力を持つ組織を用意する代わりに、サービス提供者を（1）サービス利用者と結託しない、（2）プロトコル通りに動作すると信頼することで、データの機密性を保つデータ共有方式を考える。この仮定の下で、具体的には、秘密鍵を(2,n)閾値秘密分散し、サービス提供者とサービス利用者の二者で、公開鍵で暗号化した共通鍵暗号化の鍵であるデータ復号鍵を(2,n)閾値復号してデータを共有するクラウドサービスを考える。分散情報生成プロトコルで秘密鍵に対する分散情報を配付し、シェアの再分散でグループの構成の変化に対応すると、秘密鍵を共有せずにデータの共有・グループの構成を変更でき、暗号化をやりなおすコストが生じない。

このような(2,n)閾値復号による Cryptographic Cloud Storage をスマートグリッドに対応づけると、需要家は暗号化するクラウドサービス利用者に、配電などのスマートグリッドのサービス提供者は復号するクラウドサービス利用者となる。本研究では、クラウドを介した(2,n)閾値復号によるデータ共有サービスにおいて、復号権限を委譲する手法を提案した。提案手法は、サービス利用者が単独で復号権限を委譲でき、権限を委譲したいサービス利用者との事前通信や、他のサービス利用者との通信が不要である。権限を委譲しても部分復号鍵が漏れない、登録した条件を満たしていない場合はデータを復号できないことを確認している。この手法により、要件の(1)データ保管者はデータの閲覧ができないことを満たしつつ、要件の(2)開示許可のない者はデータを利用できない、すなわち需要家により復号権限が委譲されたスマートグリッドのサービス提供者のみがデータを利用できることになる。

要件の(3)利用許可のない者に対するデータの二次利用の防止あるいは抑止がなされることに対して、まず、配達証明付きデータ送受信について検討した。

スマートグリッドのタイムラインはパーソナル情報に該当する。パーソナル情報とは個人情報保護法の対象である個人情報には限定しない、個人に属する電子的情報全般を指すものである。蓄積されたパーソナル情報を企業がパーソナライゼーションサービスやマーケティングに活用しようとする動きがある。その一方でパーソナル情報を扱う企業には情報漏洩による訴訟リスクがあり、パーソナル情報を活用するサービスの阻害要因となっている。パーソナル情報のさらなる活用のためには訴訟リスクの低減が課題としてあげられている。パーソナル情報の漏洩を完全になくすことは難しいため、企業は情報漏洩が起こってしまった場合の対策も求められる。

個人情報漏洩事件による賠償額の算定には、情報漏洩による被害額だけでなく企業が個人情報保護法に則った情報の取り扱いをしていたかが重要な判断要素になると考えられる。個人情報保護法の事業者が対応する必要がある項目の一つに安全管理があり、個人情報の適切な管理が要求されている。つまり、情報を適切に管理していたことを第三者に示すことが訴訟リスクの低減につながる

ことから、そのようなところを情報技術で支援することを考える。例えば、情報漏洩により訴訟を起こされた場合に、裁判で不利にならないような証拠を残すような技術的な対策をとるということである。そのような対策の要素技術として配達証明に本研究では注目する。パーソナル情報の受け渡しをする際に配達証明を発行することで、誰から誰へパーソナル情報が渡ったのか記録され、パーソナル情報の移動経路の把握が迅速かつ容易にできるようになる。

配達証明は送信データと受領書の公平な交換によって実現される。ここでの公平な交換とは「お互いに目的の物を手に入れるか、どちらも手に入らない」ことを保証した交換である。お互いが見えないネットワーク上でデータの公平な交換を実現することは容易ではない。

公平な交換を実現するためのアプローチは大きく二つに分けられる。一つは段階的秘密交換と呼ばれ、データを 1 ビットずつ交換していくことで、プロトコルが中断されても、両者の持つ情報の差が高々1 ビットに過ぎないようにするものである。

もう一方のアプローチは、どちらかがプロトコルを不正に中断しても正しく交換が完了することを保証するものである。このアプローチでは送信者と受信者の他に、信頼出来る第三者（Trusted Third Party: TTP）が仲介者として交換に参加する。すべての交換に必ず参加する On-line TTP を用いたプロトコルでは､データの送受信処理が TTP に集中し、通信のボトルネックが発生するなど交換の効率が悪くなる。ほとんどの交換において不正は起きないと見込まれることから、通常は交換に参加せず、不正が起きたときのみ交換に参加する Off-line TTP を用いた Optimistic 型と呼ばれるプロトコルが提案されている。

公平な交換を扱っている既存の論文をもとに、本研究では配達証明付きデータ送受信プロトコルの要件を以下のものとした。

公平性：利用者は自身だけが目的のものを得るようにプロトコルを中断または不正することができない。プロトコルの終了時には、利用者がどちらも目的の物を入手しているか、どちらも入手していない状態である。

秘匿性：送信者と受信者を除いた仲介者を含む第三者がデータの内容を読むことができない。

単一性：プロトコル中で行われた操作はプロトコルの適切な終了のために取り消されない。

TTP 不可視性：プロトコル終了時の結果から TTP が交換に参加したかどうかがわからない。

これまでに多くの公開鍵基盤（Public Key Infrastructure：PKI）ベースの公開鍵暗号（Public Key Encryption：PKE）を用いた公平な交換プロトコルが提案されている。PKI を用いた方式では通信相手の公開鍵証明書が必要である。スマートグリッドあるいは一般のクラウドサービスなどの多くの利用者がいるサービスの場合、公開鍵証明書の管理コストがサービス事業者にとって大きな負担となるため、公開鍵証明書の管理コストを減らすことが課題としてあげられる。そこで本研究では、任意の ID 情報を公開鍵とする ID ベース暗号・ID ベース署名を用いて公開鍵証明書不要な Optimistic 型の配達証明付きデータ送受信プロトコルを提案している。提案方式は Off-line TTP を用いた Optimistic 型の配達証明プロトコルのうちで、最も少ない 3 回の通信でプロトコルを終了することができる。提案方式の安全性は利用した ID ベース暗号方式の IND-ID-CCA 安全、ID ベース署名方式の EUF-ID-CMA 安全と用いる共通鍵暗号が擬似ランダム置換族である仮定のもとで、公平性、秘匿性、単一性、TTP 不可視性の要件を満たすことを示している。

要件の(3)利用許可のない者に対するデータの二次利用の防止あるいは抑止がなされることに対して、次に、データの存在証明について検討した。

データの存在を証明する技術に時刻認証がある。信頼できる第三者機関である時刻認証局（TSA：Time-Stamping Authority）がクライアントから時刻認証対象データのハッシュ値を受け取り、信頼できる時刻情報とともに署名し、タイムスタンプを作成する。タイムスタンプを TSA の公開鍵で検証することで、データが当該時刻以前に存在していたことが証明される。しかし、データが破棄されれば、その存在を証明できないので、ログなどの複数のデータが時系列順に全て揃っていることの証明は時刻認証ではできない。

例えば、データ A、B、C があるとし、それぞれ､A には 10:00､B には 11:00､C には 12:00 のタイムスタンプが付されているとする。このとき、タイムスタンプは互いに独立なので、B を失ったとしてもそのことを検知することはできない。また、A、B、C 以外にも 10:30 のデータがあるかもしれないが、それを確認することはできない。このように、タイムスタンプだけでは A より後に B、B より後に C ということは分かるが、A の次に B、B の次に C ということは分からない。本研究では、A より後に B があることを A ≺ B と表し、この関係を“前後関係”と呼ぶこととする。また、A の次に B があることを A→B と表し、この関係を“順序関係”と呼ぶこととする。

このように、時刻認証ではデータの前後関係は分かるが、順序関係までは確認できない。

データの順序関係を確認することを考えたとき、単純な実現方法として、データに通し番号を割り当てることが考えられる。既に、セキュリティチップ TPM に実装されている改ざん・偽造検知可能で単調増加する Monotonic Counter の個数を仮想的に増やせる Virtual Monotonic Counter が提案されている。このカウンターの出力する値を端末内での通し番号として利用すれば、データの順序関係を証明できる。しかし、出力されたカウンター値は各 TPM 固有のものになるので、異なる端末でデータに付されたカウンター値をそのまま比較できない。

本研究では、ある比較可能な範囲で異なる端末で付されたデータの前後関係を判定できる Virtual Monotonic Counter の階層型接続による順序認証方式を提案している。

提案方式を構成するエンティティは次の 5 つである。

[Privacy CA] TCG が定めたプロトコルに従い、下位端末と上位端末が TPM を搭載していることを確認し、TPM が所持する公開鍵ペア AIK の公開鍵証明書 AIKCert を発行する。

[端末認証者（TAA: Terminal Authentication Authority）] 端末を特定するための識別情報と AIK の公開鍵を含む AIKCert を紐付けて保持する。AIK による署名の検証により、どの端末に搭載された TPM が生成した署名か知ることができる。

[下位端末（Lower Terminal）] TPM 搭載端末であり、後述する上位端末に接続する VMC_{lower} をもつ。上位端末への VMC_{lower} の接続の要求、順序認証、上位端末への順序交差を要求するローカル順序認証者（LOC: Local Order Certifier）と LOC に順序認証／順序交差を要求する Client から構成される。事前に Privacy CA から AIKCert の発行を受け、TAA に端末の識別情報とともに登録しておく。

[上位端末（Upper Terminal）] TPM 搭載端末であり、下位端末の VMC_{lower} を階層的に接続する VMC_{upper} をもつ。LOC の要求に応じて、VMC_{upper} と VMC_{lower} の接続、順序交差を行うグローバル順序認証者（GOC: Global Order Certifier）から構成される。事前に Privacy CA から AIKCert の発行を受けておく。

[検証者（Verifier）] 上位端末が出力した CrossCert を用いて、異なる端末で出力された二つの OrderCert の前後関係を比較する。

提案方式は、順序認証開始処理 Initializing、順序認証処理 OrderStamping、順序交差処理 OrderCrossing、データの前後関係を比較する前後関係比較処理 Comparing の 4 つの処理から構成される。Initializing 実行後、下位端末は OrderStamping、OrderCrossing からデータの順序関係を保証していき、任意のタイミングで Comparing を実行する。

各下位端末が VMC を用いてデータの順序関係を独立して保証する“順序認証”と順序認証により作成される OrderCert を信頼できる上位端末が持つ単一の VMC が出力する CrossCert で順序付ける“順序交差”を行う。OrderCert が端末内でのデータの順序を、CrossCert が端末を超えての OrderCert の順序を保証することで、異なる端末で順序認証されたデータの前後関係を調べることができる。提案方式は、署名とハッシュ関数が安全であれば、削除、交換、置換、挿入をする攻撃を検知できること示した。

５．主な発表論文等

〔学会発表〕（計 3 件）

1．掛井将平，毛利公美，白石善明，野口亮司,“TPM を用いた Virtual Monotonic Counter の階層型接続による順序認証方式”，2013 年暗号と情報セキュリティシンポジウム，3A3-3，2013 年 1 月 24 日.

2．宮嵜仁志，毛利公美，土井洋，白石善明，“機密データと公開データを公平に交換するための公開鍵証明書不要な配達証明付きデータ送受信方式”，第 10 回情報学ワークショップ，pp.99-104，2012 年 12 月 8 日.

3．長澤悠貴，毛利公美，福田洋治，廣友雅徳，白石善明，“(2,n)閾値復号によるデータ共有の復号権限委譲”，2012 年電子情報通信学会総合大会，AS-2-5，pp.S-25-S-26，2012 年 3 月 22 日.

６．研究組織

(1)研究代表者
白石　善明（SHIRAISHI　YOSHIAKI）
名古屋工業大学・工学研究科・准教授
研究者番号：７０３５１５６７

(2)研究分担者
なし

(3)連携研究者
なし