7-4　機密レベルに応じた暗号化ファイル共有システムとその応用

王　立華　林　卓也　早稲田篤志　野島　良　盛合志帆

本稿では、セキュリティ基盤研究室が NICT 独自の再暗号化技術を用いて開発した汎用的な暗号ストレージシステム「PRINCESS」と、その応用例として開発した自動車情報共有システムを紹介する。PRINCESS では、外部のプロキシサーバを介して、データを暗号化したまま、組織内外の人と安全に機密レベルに応じた共有が可能であり、クラウド環境におけるプライバシーを保護した情報共有などへの応用が期待される。

1　まえがき

近年、クラウドストレージサービスが普及しているが、現在の多くのクラウドストレージシステムでは、データが暗号化されずにそのままストレージサーバにアップロードされることが多く、サイバー攻撃や管理会社の運用ミス等で保管データの情報が漏えいする危険性がある。さらに、データをどのメンバに共有するかにより共有ポリシー（機密レベル）の設定が可能であることが望まれる。これらの問題を解決するためには、保管データの暗号化は有効な手段である。しかしながら、従来の公開鍵暗号技術（例えば、RSA 暗号）では、ユーザ A の公開鍵で暗号化されたファイルは、ユーザ A の秘密鍵でしか復号できないため、暗号化ファイルを複数のメンバで共有するためには、共有メンバの人数分だけ暗号化処理が必要になるという課題があった。一方、共通鍵暗号（例えば、AES）によって共有メンバ全員に同じ鍵を用いて暗号化する場合は、一括で暗号化することが可能であるため、公開鍵暗号で実現した場合の問題点は解決できる。しかし、安全性を確保するために毎回異なる鍵を使わなければならないため、鍵共有や管理の課題が残る。このような課題に対するひとつの解決策として、セキュリティ基盤研究室では、PRINCESS（Proxy Re-encryption with INd-Cca security in Encrypted file Storage System：代理再暗号化技術を活用した IND-CCA 安全な暗号化ファイルストレージシステム）[1][2] を開発した。PRINCESS は NICT 独自の技術である「代理復号と代理再暗号化の 2 機能を実現する ID ベース暗号（IBPdr〈IBE with functions of Proxy decryption and Proxy re-encryption〉）」[3][4] を用いて、利用者のプライバシーや機密情報の取り扱いに配慮した暗号化ファイル共有システムである。PRINCESS には以下の特徴がある。

■ID ベース暗号（以下、IBE）による組織管理や、現行ストレージシステムからの移行の容易さ
■「高」「中」「低」の 3 つの機密レベル設定による組織内外との柔軟な情報共有
■委託した権限の無効化機能による柔軟なプロジェクト・ユーザ管理

PRINCESS は汎用的な情報共有システムとして、災害時早期復旧向けの医療データのバックアップなど様々な応用が考えられる。本稿では、ひとつの応用例として、PRINCESS に基づいて開発した自動車情報共有システム [5][6] を紹介する。このシステムでは、GPS から取得した車両の位置情報や車速、エンジン回転数などの CAN（Controller Area Network）情報を柔軟に共有できる。これにより、プライバシー保護に配慮した自動車情報共有サービスを実現することが可能になる。

2　PRINCESS

2.1　PRINCESS に使われる暗号技術

IBE：「IBE」とは公開鍵暗号の一種であり、その特徴はユーザの公開鍵として一意な ID（例えば利用者のメールアドレスなど）を用いる点が挙げられる。そのため、ユーザにとっての利便性が高い暗号方式である。1984 年に Shamir により最初の IBE[7] が提案されて以来、安全性証明可能な様々な方式が提案されてきた [8][9]。IBE システムでは、ID に対する秘密鍵は、ユーザ自身が発行する従来の公開鍵暗号システムと違い、信頼できる鍵生成センター（Private Key Generator: PKG、例えば組織の情報管理部門）により発行される。

代理復号：「代理復号」とは、本来正規の受信者のみが復号可能な暗号文を、事前に依頼した代理人によっても復号可能な機能をもつ暗号方式であり、1997 年に Mambo らが代理復号機能付き暗号方式 [10] とし

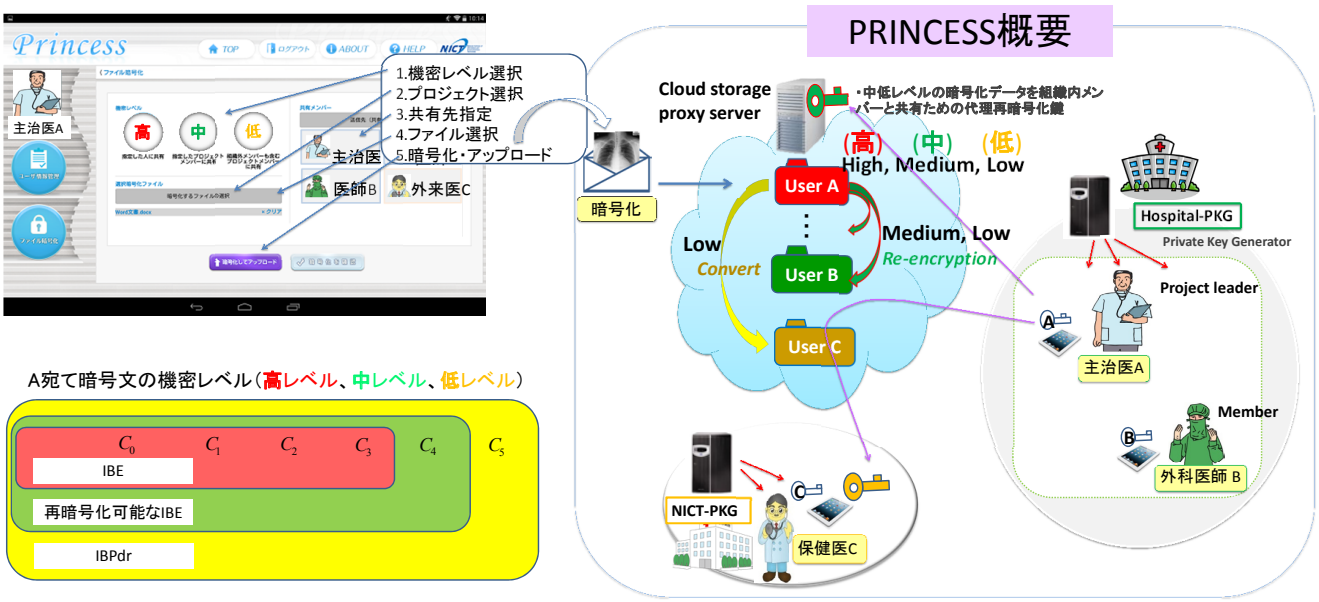


図 1　PRINCESS 概要

て提案した。このとき正規の受信者は代理人に自分の秘密鍵を渡すのではなく、「代理復号鍵」を渡し、代理人はこの代理復号鍵を使って暗号文を復号することができる。

代理再暗号： Blaze らにより提案された「代理再暗号」[11] は、受信者であるユーザ A が他のユーザ B への再暗号化鍵をプロキシサーバに渡し、プロキシサーバはその鍵を使って A あてに暗号化されたデータを復号することなく B あての暗号化データに変換可能な機能である。その後 B は「自分の秘密鍵」を使って変換後の暗号文を復号する。この再暗号化鍵は A 宛の暗号文も、B あてに変換された暗号文も復号することはできないという特徴がある。したがって、代理再暗号は（A の）データを、（プロキシサーバを経て）暗号化したまま（B と）共有可能な暗号技術となる。代理再暗号を拡張した方式としては、暗号文を再暗号化できる暗号文と再暗号化できない暗号文の 2 つの機密レベルに分けることが可能な方式 [12][13] がある。

我々は双線形写像を用いて、上記 3 つの暗号技術を組み合わせた代理復号機能を有する暗号方式で作られた暗号文を、代理再暗号化により別のユーザ宛の暗号文へ変換することができる ID ベース暗号方式 IBPdr を提案した。この方式は暗号文を 3 つの機密レベルに分けられるという特徴があるため、より柔軟なデータ共有が可能である [3][4]。

Hybrid 暗号： 公開鍵暗号と共通鍵暗号を組み合わせた暗号化方式で、公開鍵暗号によって共通鍵暗号の鍵を配送し、その鍵によってデータ本体の暗号化を行なう方式である。PRINCESS ではデータを共通鍵暗号方式 AES で暗号化し、その AES の鍵を IBPdr で暗号化、暗号化されたデータファイルと共にサーバに保存している。

2.2　全体像・特徴

PRINCESS では、共有先の範囲によって暗号文の機密レベルを「高」・「中」・「低」の 3 つに分類する。特定のメンバとのみ共有できる暗号文を「高」レベル、組織内のメンバと共有できる暗号文を「中」レベル、外部連携者を含むメンバと共有できる暗号文を「低」レベルと定義する。「高」・「中」・「低」レベルの暗号文は、それぞれ IBE、再暗号化可能な IBE、IBPdr で暗号化され、図 1 左下のような包含構造となっており、機密レベルがより低い暗号文は機密レベルがより高い暗号文への変換が可能であるが、逆の変換を行うことはできない。

本システムは複数の組織とプロキシサーバで構成され、各組織は鍵生成センターとその組織に所属するユーザを持ち、以下のステップで動作する。

（1）システムの準備　各鍵生成センター（例えば、図 1 の Hospital-PKG、NICT-PKG）で自組織の情報システムにおける公開パラメータを作成し、組織内職員の秘密鍵（SK_{id}）を発行、必要に応じて職員間の再暗号化鍵シード（$rk^{(0)}_{A\to B}$）を作成する。そして、公開パラメータ（$params$）を組織内外に公開し、プロキシサーバに送信する。また、マスターキー（msk）を PKG 内に安全に保管する。

$$Hospital\ -PKG:$$
$$params = (G_1, G_2, p, e, g, g_1 = g^{\alpha_{HOS}}, g_2, \{w_i\}_0^{2l}, H, H_2)$$
$$msk = g_2^{\alpha_{HOS}}$$
$$SK_A = (d_{A0}, d_{A1}) = (g_2^{\alpha_{HOS}} H(HOS \| A)^{u_A}, g^{u_A})$$
$$SK_B = (d_{B0}, d_{B1}) = (g_2^{\alpha_{HOS}} H(HOS \| B)^{u_B}, g^{u_B})$$
$$rk_{A\to B}^{(0)} = \left(\frac{H(HOS \| A)}{H(HOS \| B)}\right)^{u_B}$$

$$NICT-PKG:$$
$$params = (G_1, G_2, p, e, g, g_1 = g^{\alpha_{NICT}}, g_2, \{w_i\}_0^{2l}, H, H_2)$$
$$msk = g_2^{\alpha_{NICT}}$$
$$SK_A = (d_{C0}, d_{C1}) = (g_2^{\alpha_{NICT}} H(NICT \| C)^{u_C}, g^{u_C})$$

ここで、*params* 内の G_1 と G_2 は位数 p を持つ乗法群、$e: G_1 \times G_1 \to G_2$ となる双線形写像、g は G_1 の任意の生成元とし、g_2 と $\{w_i\}, i = 0,...,2l$ は G_1 の任意の元であり、w_i は Waters ハッシュ関数 $H: \{0,1\}^{2l} \to G_1$ の入力であり（詳細は [4][9] を参照）、H_2 はハッシュ関数 $H_2: \{0,1\}^* \to G_2$ である。

(2) 共有グループの作成　データを共有するグループは、ユーザであれば誰でも作成できる。グループ作成者はリーダーとなる。例えば、病院の医師であるユーザ A が同じ所属の医師であるユーザ B と企業等の保健医師であるユーザ C と検診のプロジェクト *job* を遂行するためにグループを作成する場合、A はリーダーとしてプロキシサーバにログインし、プロジェクトを作成する。そして、再暗号化鍵 $(rk_{A\to B}; ck)$ と代理復号鍵 (pdk) をそれぞれプロキシサーバと C へ配布し*1、共用データ $(Y(\tau))$ をプロキシサーバへ定期的に配信する。

Re-encryption/convert key
$$(rk_{A\to B}; ck) = (rk^{(1)}, rk^{(2)}; ck) = \left(\gamma \cdot H(HOS \| A)^{d_\gamma} rk_{A\to B}^{(0)}, g^{d_\gamma}; d_{A1}\right)$$

Proxy decryption key *pdk*
$$pdk_1^{(job)} = \gamma \cdot d_{A0} H(job \| A)^{d_{job}},$$
$$pdk_2^{(job)} = g^{d_{job}}$$

Proxy Common data
$$y_1(\tau) = \gamma^{-1} H(\tau \| A)^{d_\tau}, \quad y_2(\tau) = g^{d_\tau}$$

ここで、γ は G_2 からとる乱数、$d_\gamma, d_{job}, d_\tau$ は Z_p からとる乱数であり、リーダーの端末で安全に保管する。

(3) 柔軟な情報共有の実現　データ送信者は機密レベルを設定し、リーダー A 宛てに機密レベルに応じて暗号化、生成された暗号文 $(Enc_K^{AES}(file), Enc_A^{IBPdr}(K))$ をプロキシサーバにアップロードし、A あてのフォルダに保存する。

$$Enc_A^{IBPdr}(K) = (C_0, C_1, C_2, C_3, C_4, C_5)$$
$$= (K \oplus H_2(\sigma), \sigma \cdot \hat{e}(g_1, g_2)^r, g^r,$$
$$H(HOS \| A)^r, H(\tau \| A)^r, H(job \| A)^r)$$

プロキシサーバにより機密レベルのチェックが行われ、組織内ユーザ B へは「中」・「低」レベルのデータ再暗号化（Re-encryption）を行い B のフォルダに、組織外ユーザ C へは「低」レベルのデータ変換（Convert）を行い C のフォルダにそれぞれ分配する。

プロキシサーバ

Re-encryption
$$C_1' = C_1 \cdot \left(\frac{\hat{e}(C_4, y_2(\tau))\hat{e}(C_3, rk_{A\to B}^{(2)})}{\hat{e}(C_2, y_1(\tau) \cdot rk_{A\to B}^{(1)})}\right)$$

Convert
$$C_1'' = C_1 \cdot \frac{\hat{e}(C_3, ck)\hat{e}(C_4, y_2(\tau))}{\hat{e}(C_2, y_1(\tau))}$$

最後に、A、B、C それぞれがデータをダウンロードし、端末で A と B は復号処理（*Dec*）を、C は代理復号処理（*PDec*）を行う。

クライアント

Dec (Leader)
$$\sigma = C_1 \cdot \frac{\hat{e}(C_3, d_{A1})}{\hat{e}(C_2, d_{A0})}$$

Dec (Member)
$$\sigma = C_1' \cdot \frac{\hat{e}(C_3, d_{B1})}{\hat{e}(C_2, d_{B0})}$$

PDec (External member)
$$\sigma = C_1'' \cdot \frac{\hat{e}(C_5, pdk_2)}{\hat{e}(C_2, pdk_1)}$$

$$K = C_0 \oplus H(\sigma)$$
$$file = Dec_K^{AES}(C^*, K)$$

Remark: リーダーは委託された代理復号・再暗号化処理の権限の無効化（Revocation）をする際、γ の値を再設定し、再度ステップ (2) を行う。つまり、PRINCESS ではユーザは誰でもリーダーとしてプロジェクトを立ち上げ、メンバの追加・削除することができ、さらに、プロジェクトを削除して終了させることもできるという柔軟性がある。ここで述べているプロジェクトの削除とメンバの削除は単に削除するメンバをメンバリストから削除するという意味だけではなく、それに加えて、既にサーバに保存した削除メンバに関係する再暗号化鍵、代理復号鍵を無効化できることも意味している。これは IBPdr が、委譲した代理復号・再暗号化権限を無効化（Revocation）することができる [1] ためである。したがって、プロジェクトとメンバだけではなく、クラウドストレージサービスも必要がなくなったときに終了させる事ができる。

*1　代理復号鍵を配布するとき、C の ID を使って pdk を暗号化してからプロキシサーバ経由で行う。

2.3　性能評価

本システムの実用性や性能などを評価するために試作及び実装評価を行った。実験機材として、プロキシサーバとして Intel Core i7 3770（3.4 GHz〈64 bit〉Memory 32 GB）のサーバ 1 台、クライアント用タブレット端末として SONY Xperia Z2（Android 4.4）を利用した。IBPdr ライブラリ 内で使用するハッシュ関数として Waters ハッシュ関数 [10] を実装し、双線形写像の演算に PBC Library（https://crypto.stanford.edu/pbc/）を用いた、（詳細は [1][2] を参照）。計測結果を表 1 にまとめる。

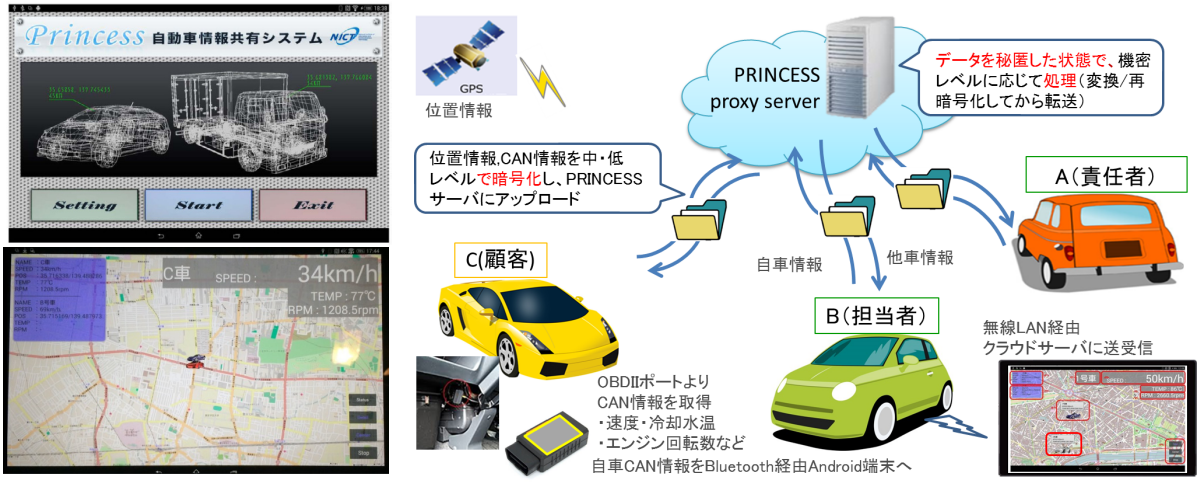
表 1 中、“Level check” はプロキシサーバの機密レベルチェック、“Re-encryption or Convert” は「中」・「低」レベルのデータへの再暗号化処理と「低」レベル暗号文への変換処理、“Encryption” はユーザが情報をアップロードする際に行う暗号化処理、“Decryption” はユーザがダウンロードした後に行う復号処理また代理復号処理、“Update proxy Common Data” はリーダーが行う共用データ $Y(\tau)$ の作成、“Revocation” はユーザ削除に伴う再暗号化用鍵の再生成、代理復号鍵の再作成などの一連の処理の所要時間（単位：ミリ秒）を示している。

表 1　計測時間（ミリ秒）

PRINCESSプロキシサーバ（PC）	
Level check	11.81
Re-encryption or Convert	4.61
クライアント任意のユーザ(Android device)	
Encryption	51.26
Decryption	22.58
クライアントグループリーダー(Android device)	
Update proxy Common Data	3.61
Revocation	47.72

3　自動車情報共有システムへの応用

今後、全ての物がインターネットに接続される（IoT：Internet of Things）社会がやってくると予測されている。自動車についても例外ではなく、10 億台を超える自動車がインターネットに接続される可能性がある。その自動車から得られる膨大なデータを、クラウド（例えば、ITS クラウドセンター）に集約させることができれば、新たなビッグデータサービスを創出することも可能であると予想される。例えば、外部からの自動車のメンテナンス、ECU（Engine Control Unit）のアップデートはその好例である。さらには、GPS 情報、各種センサ情報などをクラウドに集約させれば、通常時のみならず、震災時、緊急時の道路の



	A車	B車	C車
位置情報	中	低	低/中
車速	中	低	低/中
冷却水温	中	中	低/中
エンジン回転数	中	中	低/中

A、B車の端末では			C車の端末では		
A情報	B情報	C情報	A情報	B情報	C情報
表示	表示	表示	非表示	表示	表示
表示	表示	表示	非表示	表示	表示
表示	表示	表示	非表示	非表示	表示
表示	表示	表示	非表示	非表示	表示

図 2　PRINCESS 自動車情報共有システム（デモ）

状況把握にも役立つと考えられる。一方、自動車から得られるデータには、プライバシー情報が含まれていると考えられるため、通信データの盗聴やクラウドサーバからの情報漏洩を防ぐ機構が必要となる。プライバシー情報として位置情報はその代表例であるが、スピード、エンジン回転数などにも、運転手の運転特性が如実に表れてしまう [14]。更には、自動車に生体認証を組み込む動きもあるため、自動車から得られるデータには、プライバシーに関わる機微な情報が今後も多く含まれていくと予想される。これらのデータをクラウドに集約させることを考えると、必要な範囲以上のデータを流出させないように、データの機密性を重視していかなければならない。

本節では、この様なニーズを背景に、PRINCESS を基に開発した自動車情報共有システム（以降「PRINCESS 自動車情報共有システム」と呼ぶ）[5][6] を紹介する。

3.1　システムの概要

PRINCESS 自動車情報共有システムでは、車の位置情報や CAN 情報を暗号化状態で共有し、それぞれの情報の共有先の範囲を柔軟に設定できる。以下のシナリオを例に、システムの概要を述べる。

ディーラーで修理した C 車を試走中、ディーラーの責任者 A と担当者 B が対応する場合を考える（図 2）。A はディーラーの責任者として、C 車の位置情報や CAN 情報を把握しなければいけないが、A 自身の車情報を顧客 C に提供する必要は無い。一方、担当者 B は C 車が不具合を起こして B 車が現場へ向かう際に、B 車の位置情報や車速情報を顧客 C に伝えることができれば、顧客 C に対して安心感を与えることができると思われる。図 2 の左下の表の様に機密レベルを設定することによってこのデータ共有をまとめると、図 2 の右下の表になる。これを実現するために、PRINCESS 自動車情報共有システムでは以下のようにデータの共有を行う。

① C は A あてに暗号化した自車情報をプロキシサーバへアップロードする。
② A は A から B への再暗号化鍵をプロキシサーバへ配布。

これにより、B は C の車情報を閲覧できる。

③ B は A あてに暗号化した自車情報をプロキシサーバへアップロードする。
④ A は C あてに、一時的に使用できる代理復号鍵を配布する。

これにより、C は B の車の位置情報を閲覧できる。

デモとして、PRINCESS 自動車情報共有システムを端末 SONY Xperia Z2（Android　4.4）に実装し、実際に走行中の車からリアルタイムで GPS から取得した位置情報と、OBD Ⅱポート経由で所得した車速、冷却水温、エンジン回転数などの CAN 情報を PRINCESS 自動車情報共有システムで共有するテストを行った。

3.2　PRINCESS 自動車システムの応用展開

上記は、ディーラーと顧客というシナリオであったが、その他、様々なシナリオへの活用も可能である。

友人とのドライブ： 運転中の位置情報や渋滞情報を友人と共有することで、集合時間や場所を柔軟に調整できる。

運輸会社の業務管理： 社内で位置情報や CAN 情報を集約・共有し、配車などの業務管理や車のメンテナンスに利用できる。

自動車盗難防止： 車から自分の携帯電話等へ機密レベル「低」で暗号化した位置情報を送信することで、盗難を確認でき、また、その情報を警察と共有することで盗難車の発見の手助けが可能となる。

自動車保険への安全運転証明： CAN 情報などを含めた車の情報を機密レベル「低」で暗号化し、プロキシサーバにアップロードしておき、必要なときに、保険会社などに提供する。メンバの無効化機能により、見積り時のみ一定期間だけ情報共有を行うといった、柔軟な共有が可能である。

4　今後の展望・課題

PRINCESS は汎用的な暗号化ファイル共有ストレージシステムとして、医療データや自動車情報の共有システム、ソーシャルビッグデータの利活用など、様々な応用が可能である。これらの情報は多分にプライバシー情報を含んでいるため、データ保護対策が不十分なクラウドストレージサービスを利用するにはセキュリティ上の不安がある。PRINCESS はこのようなプライバシー問題の解決のみならず、BCP（Business Continuity Planning：事業継続計画）の観点からも有用なシステムと考えられ、今後、PRINCESS 及び PRINCESS 自動車情報共有システムが様々な分野で活用されるよう、実用化に向けた活動にも取り組んで行く。

謝辞

システム仕様の検討や事務手続きのサポート等で多大な貢献を頂いた、NICT セキュリティ基盤研究室黒川貴司技術員と金森祥子技術員に感謝する。

【参考文献】

1 王立華，早稲田篤志，野島良，盛合志帆，“PRINCESS: プロキシ再暗号化技術を活用したセキュアなストレージシステム，” SCIS2014, Jan. 2014.
2 L. Wang, T. Hayashi, S. Kanamori, A. Waseda, R. Nojima, and S. Moriai, “POSTER: PRINCESS: A Secure Cloud File Storage System for Managing Data with Hierarchical Levels of Sensitivity”, In: CCS2015, pp.1684–1686, ACM 2015.
3 王立華，“二機能付き ID ベース暗号化方法及び暗号システム，” 特許第 5298394 号．
4 L. Wang, L. Wang, M. Mambo, and E. Okamoto, “Identity-Based Proxy Cryptosystems with Revocability and Hierarchical Confidentialities,” IEICE, E95-A(1), pp.70–88, 2012.
5 王立華，野島良，盛合志帆，“PRINCESS を利用したセキュアな自動車情報共有システム，” SCIS2015, Jan. 2015.
6 L. Wang, R. Nojima, and S. Moriai, “A Secure Automobile Information Sharing System,” In: AsiaCCS-IoTPTS2015, pp.19–26, ACM 2015.
7 A. Shamir, “Identity-based cryptosystems and signature schemes,” In: CRYPTO 1984, LNCS 196, pp.47–53, Springer 1985.
8 D. Boneh and X. Boyen, “Efficient Selective Identity-Based Encryption Without Random Oracles,” J.Cryptology 24(4), pp.659–693, 2011.
9 B. Waters, “Efficient Identity-Based Encryption Without Random Oracles,” In: EUROCRYPT 2005 LNCS 3494, pp.114–127, 2005.
10 M. Mambo and E. Okamoto, “Proxy cryptosystem: Delegation of the power to decrypt ciphertexts,” IEICE, E80-A(1), pp.54–63, 1997.
11 M. Blaze, G. Bleumer, and M. Strauss, “Divertible protocols and atomic proxy cryptography,” In: EUROCRYPT 1998, LNCS 1403, pp.127–144, Springer 1998.
12 B. Libert and D. Vergnaud, “Unidirectional Chosen-Ciphertext Secure Proxy Re-encryption,” In: PKC 2008, LNCS 4939, pp.360–379, Springer, 2008.
13 R. Hayashi, T. Matsushita, T. Yoshida, Y. Fujii, and K. Okada, “Unforgeability of Re-Encryption Keys against Collusion Attack in Proxy Re-Encryption,” In: IWSEC 2011, LNCS 7038, pp.210–229, 2011.
14 早稲田篤志，野島良，“車々間通信におけるプライバシ漏洩の実証実験，” CSS2015.

王　立華　（おう　りつか）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（工学）
暗号プロトコル設計と安全性評価

林　卓也　（はやし　たくや）
サイバーセキュリティ研究所
セキュリティ基盤研究室
研究員
博士（機能数理学）
暗号解析、高速実装

早稲田篤志　（わせだ　あつし）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（情報科学）
情報セキュリティ

野島　良　（のじま　りょう）
サイバーセキュリティ研究所
セキュリティ基盤研究室
主任研究員
博士（工学）
暗号理論、暗号プロトコル、情報セキュリティ、
プライバシー、セキュリティ

盛合志帆　（もりあい　しほ）
サイバーセキュリティ研究所
セキュリティ基盤研究室
室長
博士（工学）
暗号技術、セキュリティ評価、
プライバシ保護技術