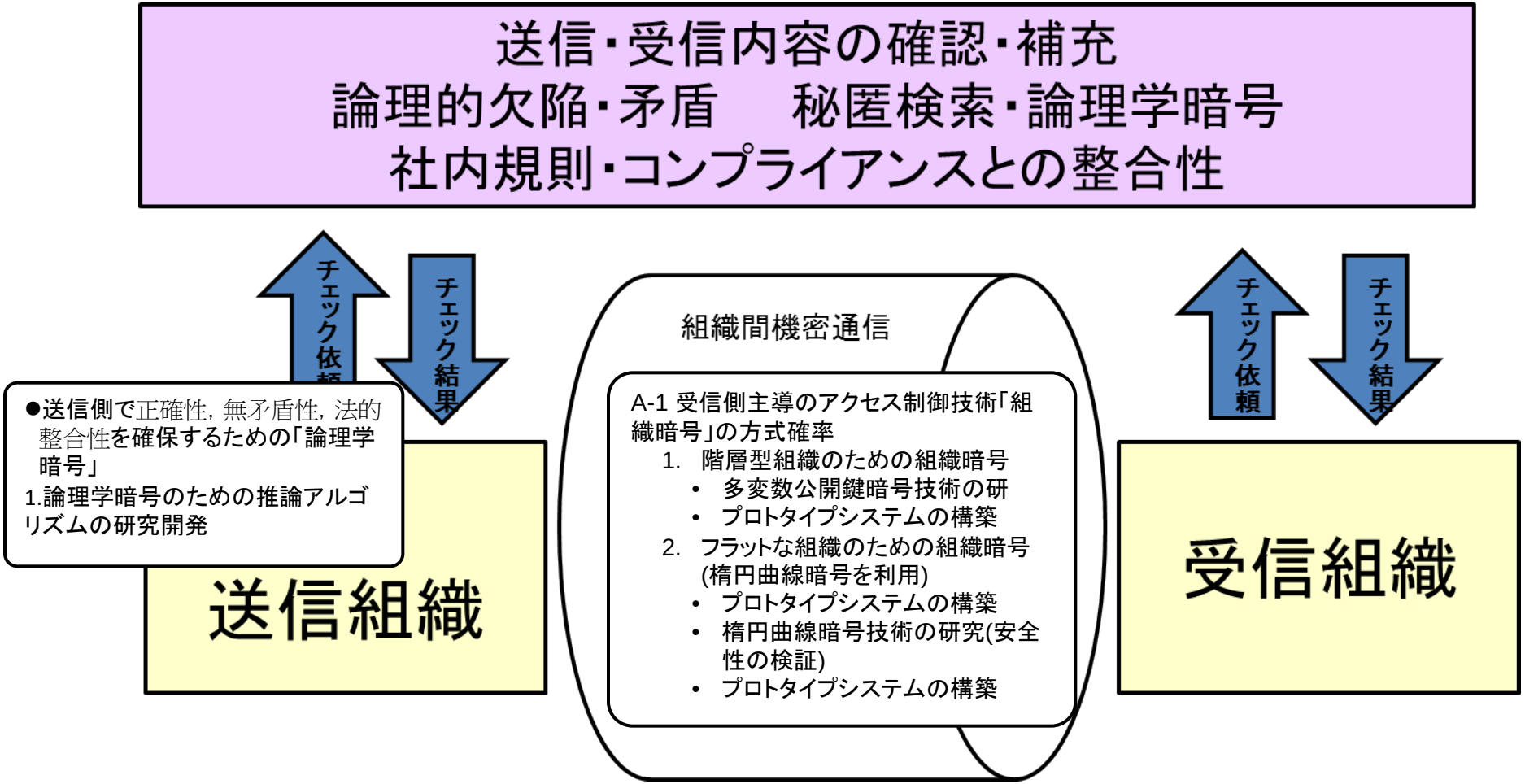
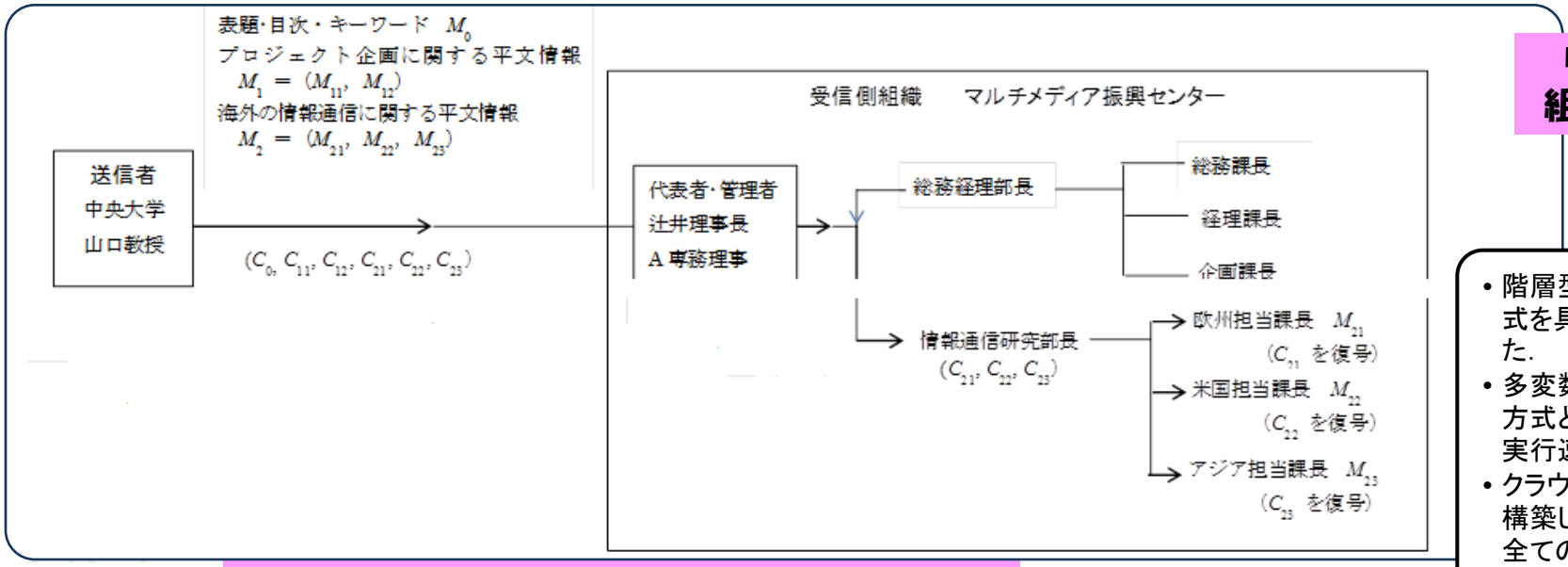
平成25年度「組織間機密通信のための公開鍵システム」の研究開発目標・成果と今後の研究計画

1. 実施機関・研究開発期間・研究開発費
   実施機関：中央大学
   研究開発期間：平成25～27年度
   研究開発費：　156百万円　(平成25年度55百万円)

2. 研究開発の目標
   組織の機密情報やパーソナルデータの活用と保護の両立を図ること

3. 研究開発の成果





「階層型組織向け組織暗号の実用化

- 階層型組織のための組織暗号方式を具体化し，機能仕様を作製した．
- 多変数公開鍵暗号技術を用いた方式とし，プロトタイプシステムで実行速度などの性能を確認した．
- クラウド上で実行するシステムを構築し，ブラウザ上でユーザーが全ての操作を行えるユーザーインターフェースを作製した．

「フラット型組織向け組織暗号の実用化

表題・目次・キーワード（M_0）
個人情報保護に関する
相談情報　M_1
プライバシーマークに関する
相談情報　M_2

送信者
中央大学
山口教授*

$(C_0, C_{11}, C_{12}, C_{13}, C_{21}, C_{22})$
楕円エルガマル暗号
$(rP, C_0, G_1, G_2, G_3, C_{21}, C_{22})$
$= (rP, M_0 + rQ_{11}, M_{11} + rQ_{11}, M_{12} + rQ_{12}, M_{13} + rQ_{13}, M_{21} + rQ_{21}, M_{22} + rQ_{22}) \bmod q$

$Q_{ij} = S_{ij} M_{ij}$
S_{ij} は文書 M_{ij}（受信担当者ではなく）に対応する秘密鍵

受信側組織　放送セキュリティセンター

代表者・管理者
辻井理事長
B 専務理事
D 総務部長

代表者・管理者は各担当者への復号用秘密鍵 S_{ij} は別途配布する

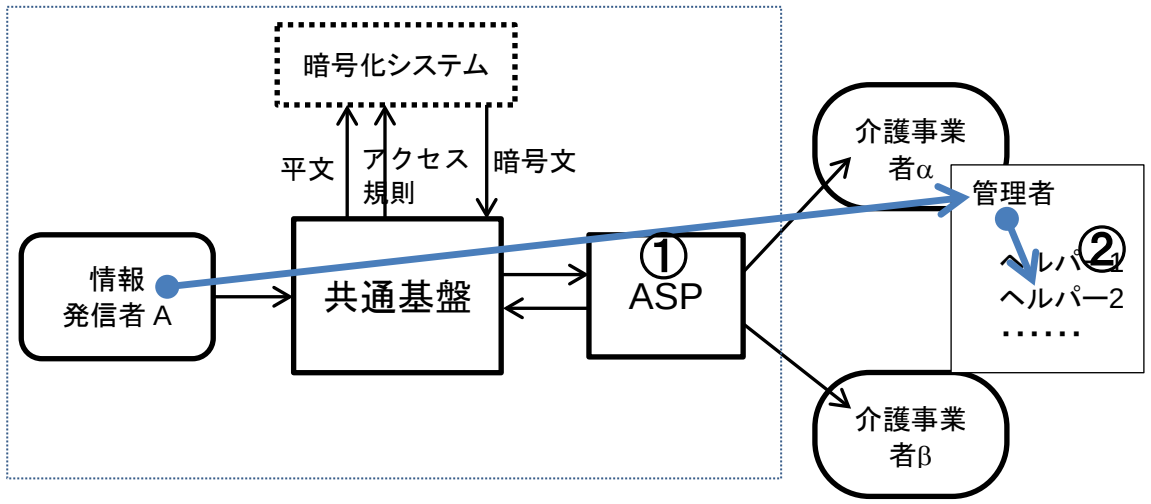
- 個人情報保護相談員 H_1
- 個人情報保護相談員 H_2
- 個人情報保護相談員 H_3
- 個人情報保護相談員 H_4
- プライバシーマーク相談員 T_1
- プライバシーマーク相談員 T_2
- プライバシーマーク相談員 T_3
- プライバシーマーク相談員 T_4

代表者・管理者は、各相談員の当日の適性や勤務状況（多忙さや健康状態等）を見て担当を定める。

* 山口教授は、放送セキュリティセンターが個人情報保護、及び、プライバシーマークに関する相談を受け付けていることは知っているが、どのような相談員がいるか等、組織内の状況は知らない。

- フラット型組織のための組織暗号方式を具体化し，機能仕様を作製した．
- 楕円曲線暗号技術を用いた方式とし，プロトタイプシステムで実行速度などの性能を確認した．
- ユーザーのコンピュータにインストールして動作させるシステムを構築し，ユーザーが操作をうためのユーザーインターフェース，及びインストーラを作製した．

総務省の「医療・介護業務向け情報共有基盤」への組織暗号の実用化



●「在宅医療・介護分野における情報連携基盤の開発及び活用の実証に関する請負事業」の中で，組織間通信でのアクセス制御を行うセキュリティ部分を提供：

① 送信者は情報を暗号化し，送信情報に関するサマリーをメタデータとして提供

② 各ノード内で組織構造と役割分担に応じて，受信者主導で情報へのアクセス許可(復号の権利)を与える組織暗号システム(階層型)

4．これまで得られた成果（特許出願や論文発表等） **※成果数は累計件数と（ ）内の当該年度件数です。**

	国内出願	外国出願	研究論文	その他研究発表	プレスリリース	展示会	標準化提案
組織間機密通信のための公開鍵システムの研究開発	0 （0）	0 （0）	0 （0）	8 （8）	6 （6）	0 （0）	0 （0）

5．研究成果発表等について

（1）

Melt-upフォーラム　講演会
http://c-faculty.chuo-u.ac.jp/~tsujii/_userdata/2013meltup.pdf
2014年9月13日(金)，14日（土）
情報セキュリティと情報の有効活用に関して，暗号とセキュリティ技術，及び法制度の観点からの講演，及び，主に医療・介護のICTによる質向上とセキュリティに関して討論会を行った．

（2）

Melt-up フォーラム「日本の情報通信産業の盛衰から再生へ」
http://c-faculty.chuo-u.ac.jp/~tsujii/lecture.html
2014年2月24日，3月4，5日　於 中央大学後楽園キャンパス／中央大学駿河台記念館
フォーラム概要：日本の電子産業の移り変わり，国際標準化戦略の成功事例などに関する講演，及び，次代を担う人材の育成の方向性や企業のICTネットワーク活用のあり方，及び災害時のコミュニケーション方法などに関して各界を代表する有識者の間でパネルディスカッションや討論会を行った．
本研究で提案している組織通信・組織暗号の概念は、国際会議などで度々、招待講演を依頼され、高い評価を得ているが、国内でも社会的関心を高める必要があることを痛感し、「放送・通信の４類型化と情報セキュリティ概念の高度化、及び組織通信・組織暗号の重要性」について、辻井が講演した。

6. 今後の研究開発計画

組織通信概念の確立と情報セキュリティ概念の高度化へ向けての考察を深める。
20世紀までの通信は、主として、通信の秘密という価値観に基づいた個人間の通信が主であった。今後、OCBM、即ち、Open data, Cloud, Big data, My number の普及とともに、企業、自治体や医療・介護システム等の間でやり取りされる電子文書が膨大になることは必然である。これに伴って、送信文書の機密性、正確性、論理的無矛盾性や法的整合性を、紙文書時代に比べて、短時間で確認した上で送信すること、また、受信側では、機密性や個人情報保護の観点から、必要とされる情報のみを、担当者のみに配布すること等が要請される。
このような観点から、組織通信概念の確立と情報セキュリティ概念の高度化へ向けての考察を深める。

具体的には、下記のようなテーマを中心に研究開発を推進する。

1）平成25年度に開発した組織暗号は、既に、総務省の請負事業
「在宅医療・介護分野における情報連携基盤の開発及び活用の実証」に実装されつつあるが、平成26・7年度は、その全国的展開にあわせて、組織構造の多様性を考慮した柔軟性のある組織暗号の研究開発を続け、わが国の情報連携基盤における個人情報の保護と活用の両立に貢献する。
2）クラウドの利用における情報秘匿を保障しつつ、組織通信の送信文書の論理性の向上を目指して、平成25年度に着想した論理学暗号の研究を発展させる。
3）平成25年度に論文発表した、自治体や病院等が保管する個人情報の内、必要最小限のリストのみを抽出して送信する手法に関して、その効率化を進め、実装を進める。