MELT up フォーラム

組織間機密通信のための組織暗号の研究開発と社会的利用

開催趣旨

20世紀までの通信・放送は、通信の秘密を基本理念とする個人通信と、公序良俗という価値観に基ずく公共放送の2分野であった。21世紀に入ると、SNSが急速に普及してきた。今後は、この3者に加えて、企業、自治体、医療機関など多様な組織間での、電子化された文書による通信が、文書の電子化・ビッグデータ化の進展、クラウド環境の広がり、及び、マイナンバーの導入などに伴って、広がるものと予想される。従って、これからの通信・放送分野は、個人通信、組織通信、SNS、公共放送の4つに類型化されるものと考えられる。

比較的自由な個人通信と異なり、組織通信の場合は、伝達情報の正確性、迅速性・緊急性、証拠性、機密性、個人情報保護、法的整合性、論理的無矛盾性、多言語性などへの配慮が求められる場合が少なくない。

組織通信における、これ等の理念の内、機密性、証拠性を支える基本技術は暗号であり、自治体の有する個人情報・企業の機密情報の限定的送出や、再暗号化、秘匿検索・推論などの暗号化状態処理を含む暗号技術（以下組織暗号と総称する）は、クラウド環境の広がりなどの中で、不可欠となっている。

1990年代、「暗号は軍事外交以外に、情報社会でも有用なのかということから社会的関心を集めたが、暗号が認証・署名や秘匿の基盤技術として生活を支えるるようになると、新技術の宿命として、暗号への人々の関心は薄れていった。

最近、第2次大戦において、エニグマ（ナチスドイツの暗号）を解読して、連合国を勝利に導いた、悲劇の天才、アラン・チューリングを主人公にした映画「イミテーション・ゲーム」が話題を呼んでいる。チューリング時代の古典暗号の解読も鍵管理の不完全さがきっかけになる場合が多かったが、この点は、現在も通じる課題である。暗号がセキュリティの基本技術として、話題になり始めたころ、大蔵省（現在財務省）のある局長から「素数は、そんなに沢山あるのですか」という玄人裸足の質問を受けたことがある。それ程関心を集めた暗号も、現在は、情報システム技術者ですら「素数の使い回し」という初歩的なミスを冒しているという状況である。我々暗号技術者は、再度、暗号に対する社会的関心を高めることに智慧とエネルギーを注ぐ必要があると痛感している。

本フォーラムは、中央大学研究開発機構が、国立研究開発法人情報通信研究機構から委託を受けている「組織間機密通信のための公開鍵システムの研究開発―クラウド環境における機密情報・パーソナルデータの保護と利用の両立に向けて―」の研究活動の一環として行うものであり、これまでの本委託研究成果を含め、産学官の関連研究動向について広く討議することにより、今後の組織暗号の研究開発と社会的活用に資することを目的として開催するものである。

実行委員会

委員長	辻井重男	**幹事**	五太子政史
副委員長	山口　浩	〃	藤田　亮
幹事長	才所敏明	**事務局**	堂上一男

主催　　中央大学研究開発機構

後援　　NICT 国立研究開発法人情報通信研究機構
四国情報通信懇談会

協賛　　電子情報通信学会
日本セキュリティ・マネジメント学会
一般財団法人マルチメディア振興センター
一般財団法人放送セキュリティセンター
NPO デジタル・フォレンジック研究会
NPO中央コリドー情報通信研究所
NPO ASP・Saas・クラウド コンソーシアム
MCPC モバイルコンピューティング推進コンソーシアム

参加申込先　　https://c-faculty.chuo-u.ac.jp/~tsujii/application.html

❖開催日	6月15日（月）
❖時間	18:00 ～ 20:00
❖会場	中央大学後楽園キャンパス 3号館 3階　3300号室 キャンパスマップ URL http://www.chuo-u.ac.jp/campusmap/kourakuen/pdf/kourakuen_01.pdf?1431493225541
❖参加費	無料

（五十音順・敬称略）

プログラム	**パネル討論　組織間機密通信のための公開鍵暗号理論の最前線と将来展望**	
司会	辻井重男	中央大学研究開発機構 機構教授
パネリスト	**円分整数と暗号**	
	有田正剛	情報セキュリティ大学院大学情報セキュリティ研究科 教授
	共通鍵暗号系の最新の話題	
	岩田　哲	名古屋大学大学院工学研究科 准教授
	群構造維持暗号系とその応用	
	大久保美也子	国立研究開発法人情報通信研究機構 ネットワークセキュリティ研究所 主任研究員
	(Batch) Fully Homomorphic Encryotin over Integers for Non-Binary Message Spaces	
	黒澤　馨	茨城大学 工学部情報工学科 教授
	高機能暗号と防御者革命	
	松浦幹太	東京大学生産技術研究所 情報・エレクトロニクス系部門 教授
	ナップザック暗号について	
	村上恭通	大阪電気通信大学情報通信工学部 准教授

❖開催日	6月17日（水）
❖時間	18：00～20：00
❖会場	中央大学後楽園キャンパス 3号館 3階 3300号室 会場案内図URL http://www.chuo-u.ac.jp/campusmap/kourakuen/pdf/kourakuen_01.pdf?1431493225541
❖参加費	無料

（五十音順・敬称略）

プログラム	**パネル討論　組織間機密通信のための暗号化状態処理の研究と実用化の動向**	
司会	盛合志帆	国立研究開発法人情報通信研究機構 ネットワークセキュリティ研究所 セキュリティ基盤研究室 室長
	東芝における再暗号化技術の研究と実用化	
パネリスト	秋山浩一郎	株式会社東芝 研究開発センター コンピュータアーキテクチャ・セキュリティラボラトリー 研究主幹
	NECにける暗号化状態処理の研究	
	佐古和恵	日本電気株式会社 クラウドシステム研究所 技術主幹
	情報利活用のための暗号技術と日立の取組み	
	佐藤尚宜	株式会社日立製作所 研究開発グループ システムイノベーションセンタ 主任研究員
	準同型暗号の応用と実適用における課題 ―富士通研究所のプライバシー保護技術	
	下山武司	株式会社富士通研究所 知識情報処理研究所 データプライバシー保護プロジェクト 研究主幹
	ユーザー安心のための暗号化状態処理	
	松崎なつめ	パナソニック株式会社 先端研究本部 知能研究室 主幹研究員
	マルチキー完全準同型暗号と組織間機密通信	
	満保雅浩	金沢大学 理工研究域　電子情報学系 教授

❖開催日	6月19日（金）
❖時間	10:00～17:OO
❖会場	中央大学駿河台記念館 610号室 会場案内図URL http://www.chuo-u.ac.jp/access/surugadai/
❖参加費	無料

プログラム　　（敬称略）

10:00	総合司会	才所敏明	中央大学研究開発機構 専任研究員
10:05－10:40	講演	**A. 組織通信の理念・価値観と情報セキュリティ概念の高度化 B. エニグマ暗号解読で母国イギリスを救った悲劇の天才 —映画 イミテーションゲームの主人公 アラン・チューリングの業績—**	
		辻井重男	実行委員長 中央大学研究開発機構 機構教授
10:40－12:00	講演・鼎談	**組織通信におかるマイナンバーの導入を巡って**	
	司会	宮崎　緑	千葉商科大学国際教養学部長 教授
	講演	**自治体における個人情報の保護と活用**	
		井堀幹夫	東京大学高齢社会総合研究機構　特別研究員
	講演	**特定個人情報保護と産業界の動向**	
		手塚　悟	東京工科大学教授　特定個人情報保護委員会委員
	鼎談	司会：宮崎 緑　　井堀幹夫　手塚　悟	
12:00－13:00	昼食		
13:00－14:00	特別講演	**(Authenticated) Key Exchanges from (Ring) Learning with Errors**	
		Jintai Ding, Professor of Department of Mathematical Sciences, University of Cincinnati	
14:00－15:10	**中央大学研究開発機構におけるNICT委託研究活動 —組織暗号と自治体における実証実験状況—**		
14:10－14:10	司会	山口　浩	中央大学研究開発機構 機構教授
14:10－14:20	発表者	五太子政史	中央大学研究開発機構 機構准教授
14:20－14:30		藤田　亮	中央大学研究開発機構 機構助教
14:30－14:40		山口　浩	中央大学研究開発機構 機構教授
14:40－14:50		只木孝太郎	中部大学工学部 教授
		組織暗号の実証実験	
14:50－15:05		才所敏明	中央大学研究開発機構 専任研究員
15:05－15:10	Q&A		
15:10-15:30	休憩		

15:30－16:10	講演	**病院・医療施設等の組織間通信における医療情報の保護と活用**

		山本隆一	東京大学大学院医学系研究科特任准教授 一般財団法人医療情報システム開発センター 理事長
16:10－17:00	講演	**組織間機密通信と多変数公開鍵暗号**	
	1	**【九州大学における研究活動の紹介】 SCOPE「多変数多項式システムを用いた 安全な暗号技術の研究」の活動**	
		安田貴徳	(財)九州先端科学技術研究所 情報セキュリティ研究室 研究員
	2	**中央大学における研究活動の紹介 多変数公開鍵暗号の組織間機密通信への応用**	
		五太子政史	中央大学研究開発機構 機構准教授

❖開催日	開催日	6月20日（土）
❖時間	時間	10:00～17:00
❖会場	会場	中央大学後楽園キャンパス 5号館 5233号室 会場案内図URL http://www.chuo-u.ac.jp/campusmap/kourakuen/pdf/kourakuen_01.pdf?1431493225541
❖参加費	無料	

	総合司会	山口　浩	副委員長 中央大学研究開発機構 機構教授
10:00－11:00	講演	**組織間機密通信における属性暗号・関数暗号と再暗号化**	
		関数型暗号について	
		岡本龍明	NTTセキュアプラットフォーム研究所 岡本特別研究室長
		高安全な関数型代理人再暗号化	
		高島克幸	三菱電機株式会社 情報技術総合研究所 松井暗号プロジェクトグループ 主席技師長
11:00－11:40	講演	**ペアリングの着想とその後の組織間機密通信への応用 ―その背景にあったもの―**	
		笠原正雄	中央大学研究開発機構 機構教授
		境　隆一	大阪電気通信大学金融経済学部 准教授
11:40－12:20	講演	**組織暗号のための楕円暗号の性能と安全性の両立に向けて**	
		趙　晋輝	中央大学 理工学研究科 教授
		飯島　努	株式会社光電製作所 特機技術部研究課 研究員
12:20－13:20	昼食		
13:20－13:50	講演	**各国政府の暗号政策動向 ―組織間機密通信を中心として―**	
		神田雅透	IPA 独立行政法人情報処理推進機構 セキュリティセンター 研究員 NTTセキュアプラットフォーム研究所 セキュアアーキテクチャプロジェクト主任研究員
13:50－14:30	講演	**国際標準化動向について―組織間機密通信を中心として―**	
		宮地充子	北陸先端科学技術大学院大学 教授
14:30－14:50	休憩		
			（五十音順・敬称略）
14:50－16:50	パネル討論会	**クラウド環境における組織暗号機密通信のための 暗号化状態処理を廻って**	
	司会	森井昌克	神戸大大学大学院工学研究科 教授

		クラウド環境における暗号化状態での「情報共有」と「代理計算」に関する	
	パネリスト	王　立華	国立研究開発法人情報通信研究機構 ネットワーク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
		クラウド環境における暗号化状態処理を廻って	
		尾形わかは	東京工業大学大学院情報理工学研究科 教授
		情報理論的安全性の立場からの研究の取り組み	
		四方順司	横浜国立大学大学院環境情報研究院 社会環境と情報部門 准教授
		須賀祐治	株式会社インターネットイニシアティブ サービスオペレーション本部 セキュリティ情報統括室 シニアエンジニア
		代理人再暗号化に要求される性質、特に、non-transferability	
		田中圭介	東京工業大学大学院情報理工学研究科 准教授
		花岡悟一郎	国立研究開発法人産業技術総合研究所 セキュアシステム研究部門 次世代暗号研究グループ 研究グループ長
16:50－17:00	閉会挨拶	山口　浩	副委員長 中央大学研究開発機構 機構教授