平成２８年度 共同利用研究報告書

平成 ２８ 年 １２ 月 ２ 日

九州大学 マス・フォア・インダストリ研究所長 殿

所属・職名　長崎県立大学情報システム学部情報セキュリティ学科・准教授
提案者氏名（ふりがな）　穴田 啓晃（あなだ ひろあき）

下記の通り共同研究の報告をいたします.　　記

	※整理番号	20160005		
1.研究計画題目	ネットワークストレージのディペンダビリティ，ユーザビリティとセキュリティに対する秘密分散法の応用とその数学モデリング			
2.種別（○で囲む）	a. 研究集会Ⅰ　b. 研究集会Ⅱ　c.短期共同研究　d.短期研究員			
3.研究代表者	氏名（ふりがな）	穴田啓晃（あなだ ひろあき）		
	所属部局名	長崎県立大学 情報システム学部情報セキュリティ学科	職名	准教授
	連絡先			
	e-mail		TEL	
4.研究実施期間	平成 28 年 9 月 5 日（月曜日）～平成 28 年 9 月 7 日（水曜日）			

5.参加者数・参加者リスト（＊別紙「共同利用研究報告書作成上の注意」参照）
(a,b は参加者数のみ記入し, 集会参加者リストを添付. c.の非公開プログラム参加者と d.は参加者リストに記入. c.は公開プログラムを含めた全参加者数を記入し，公開プログラム参加者リストを添付.）

参加者数：　４９　人

参加者リスト（a,b は記入不要，c.は非公開プログラム参加者，d.は共同研究参加者を記入）

氏名（ふりがな）	所属	職名	氏名（ふりがな）	所属	職名
－	－	－	－	－	－

6.本研究で得られた成果の概要

秘密分散技術は，震災などの災害によるデータ消失，また不正アクセスによるデータ漏えいの両リスクに対する解決策として産業界で盛んに研究開発されている．本研究集会はこの傾向を反映したためか，参加者数 49 名と想定以上の関心を集めた．産学官別内訳は，産から 11 名，学から 33 名，官から 5 名であった．学からは九大の教員・学生が多かった．この影響を差し引くと，およそ三つの業界の方々から満遍なく参加頂けた．また，賞味丸二日の開催期間に対しやや多めの参加者数であり，結果として，講演・聴講を通じて活発に期待以上に交流頂くことが出来た．14 名の外国籍の方々に参加頂けたため国際会議として意見交換・交流できた点も，成果と考えている．

また，研究内容の観点から，本研究集会で実施された講演を次の三つのカテゴリに分類することができる．

カテゴリA.　秘密分散技術，秘密計算

カテゴリB.　秘密分散適用・実装，ﾈｯﾄﾜｰｸ符号化，ﾈｯﾄﾜｰｸｽﾄﾚｰｼﾞｾｷｭﾘﾃｨ

カテゴリC.　A，B についてのパネルディスカッション

カテゴリ A は 8 件，カテゴリ B は 5 件，カテゴリ C は 1 件の講演を，各々トップレベルの研究開発者から頂くことが出来た．より詳細については成果報告書に示す．

（以上）

2016 年 12 月 2 日

2016 年九州大学マス・フォア・インダストリ研究所共同利用研究集会(I)

“Secret Sharing for Dependability, Usability and Security of Network Storage and Its Mathematical Modeling”

（ネットワークストレージのディペンダビリティ，ユーザビリティとセキュリティに対する秘密分散法の応用とその数学モデリング）

成果報告書

組織委員

長崎県立大学・准教授	穴田啓晃（代表者）
東京工業大学・特任准教授	モロゾフ・キリル
㈱インターネットイニシアティブ・シニアエキスパート	須賀祐治
公益財団法人九州先端科学技術研究所・研究員	奥村伸也
公益財団法人九州先端科学技術研究所・研究室長	櫻井幸一

本報告書は，2016 年の共同利用研究集会(I)て採択頂いた上記表題の研究集会を開催して得られた成果を簡潔に報告することを目的とする．

はじめに，参加者についての成果を説明する．本研究集会は 49 名の参加者があった．参加人数の内訳を，国内外（国籍）別および産学官別で図 1 に示す．本研究集会は，外国籍の参加者が 14 名（29%）であった（図 1，左）．国際研究集会として交流できたものと考えている．また，産からは 11 名（23%），学からは 33 名（67%），官からは 5 名（10%）であった（図 1，右）．学からの参加者が約 3 分の 2 であったが，これは九州大学の教員・学生が多かったためである．この影響を差し引くと，産学官からおよそ満遍なく参加頂けたと考えている．

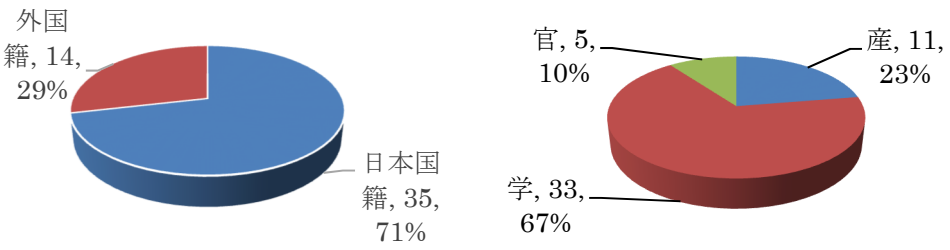

図 1　外国籍・日本国籍別（左）および産学官別（右）参加人数内訳．

次に，研究内容の成果について説明する．実施された講演は次の三つのカテゴリに分類される．

カテゴリA. 秘密分散技術，秘密計算

カテゴリB. 秘密分散適用・実装，ﾈｯﾄﾜｰｸ符号化，ﾈｯﾄﾜｰｸｽﾄﾚｰｼﾞｾｷｭﾘﾃｨ

カテゴリC. A，B についてのパネルディスカッション

次ページ表 1 は上記カテゴリ別の実施講演一覧を示す．カテゴリ A は 8 件（計 250 分），カテゴリ B は 7 件（計 230 分），そしてカテゴリ C は 1 件（計 45 分）であった．このことから，本研究集会の研究題目「ネットワークストレージのディペンダビリティ，ユーザビリティとセキュリティに対する秘密分散法の応用とその数学モデリング」に対して，件数および時間共に，賞味丸 2 日間の開催期間に対し十分な量の講演を頂けたと考えている．また，質の面では，表 1 に示されている講演者は業績の点で，産学官からのトップレベルの研究開発者である．なお，カテゴリ C のパネルディスカッションについては，聴講者も巻き込んだディスカッションが見られた．このパネルディスカッションの動画については“Youtube”を利用し，参加者に配信した．

また，講演者の予算元について触れる．本研究集会では，九州大学マス・フォア・インダストリ研究所から本研究集会へ支給頂いた予算を用い，表 1 における A1，A2，A4，A7，A8，B2，B4，B5 の研究者を招へいすることができた．ここに深謝申し上げる．

総括として，本研究集会では，講演 15 件，パネルディスカッション 1 件について，交流するのに想定（40 名）以上の方々（49 名）に参加頂き，結果として講演・聴講を通じて活発に交流頂くことが出来た．国内外のより多くの講演者・参加者が集まる研究集会を次年度も企画したい．なお，本研究集会が参加者に与えた影響については，九州大学マス・フォア・インダストリ研究所により例年行われる《講演者のその後の関連論文数アンケート》に現れることを期待したい．

（以上）

表 1　カテゴリ別の実施講演一覧

A.　秘密分散技術，秘密計算		
A1	Satoshi OBANA	Hosei University
	“Cheating Detectable Secret Sharing Scheme Supporting Finite Fields of Characteristic Two”	
A2	Hiroshi DOI	Institute of Information Security
	“Fast ({1,k},n) Hierarchical Secret Sharing Schemes”	
A3	Jon-Lark KIM	Sogang University
	“Secret sharing schemes based on additive codes”	
A4	Arkadii SLINKO	The University of Auckland
	“Classification of Ideal Secret Sharing Schemes with Weighted Access Structures”	
A5	Partha Sarathi ROY	Kyushu University
	“On The Robustness of Secret Sharing Schemes”	
A6	Rui XU	KDDI R&D Laboratories, Inc.
	“Secret Sharing against Cheaters”	
A7	Toshinori ARAKI	NEC Corporation
	“High-Throughput Secure Computation using bit slicing”	
A8	Yuji SUGA	Internet Initiative Japan Inc.
	“XOR-based (2, 2^m) threshold schemes”	
B.　秘密分散技術適用・実装，ネットワーク符号化，ネットワークストレージセキュリティ		
B1	Yvo DESMEDT	The University of Texas at Dallas
	“Applications of Secret Sharing: Beyond Storage Service”	
B2	Ryo KIKUCHI	NTT CORPORATION
	“SHSS: "Super High-speed (or, Sugoku Hayai) Secret Sharing" library for object storage systems”	
B3	Rocki H. OZAKI	Real Technology Inc.
	“Unequal Secret Sharing Scheme - a proposal”	
B4	Keiichi IWAMURA	Tokyo University of Science
	“Integration of IoT and big data security by using asymmetric secret sharing scheme”	
B5	Yuichi KOMANO	TOSHIBA CORPORATION
	“Toward Highly Secure Metering Data Management in the Smart Grid”	
B6	Chi CHENG	Kyushu University
	“Homomorphic authentication schemes for network coding”	
B7	Patrick P. C. LEE	The Chinese University of Hong Kong
	“Unifying Reliability, Security, and Deduplication in Cloud Storage”	
C.　PANEL DISCUSSION Moderator: Kirill MOROZOV, IMI, Kyushu Univ.		
C1	Panelists: Yvo DESMEDT, Jon-Lark KIM, Patrick P. C. LEE, Rocki H. Ozaki, Satoshi OBANA	
	“Secret Sharing in Real-Life Distributed Systems: Perspectives and Challenges”	