共同利用

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

種別	研究集会(I)
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
研究代表者	穴田 啓晃（長崎県立大学 情報セキュリティ学科・准教授）
研究実施期間	平成28年9月5日（月）～ 平成28年9月7日（水）
研究分野のキーワード	分散ストレージ，情報セキュリティ，秘密分散法，数学モデリング
目的と期待される成果	情報処理技術の急速な発展によってストレージのアウトソーシングは重要になってきている．クラウド・ストレージはこのような技術の一例である．クラウド・ストレージで，今まで機密性と信頼性はそれぞれ暗号化と誤り訂正符号を用いて達成されてきた．しかし最近は，その二つの特質を達成するため，秘密分散法を応用したシステムが活発にネットワークストレージ分野でビジネス展開されている．特に，2015 年にIBMに買収されたCleversafe社（アメリカ），IzumoBASE社（日本），TCSI社（日本）は，秘密分散法を使用したストレージサービスを提供している．秘密分散法とはデータを，冗長性を持たせた複数の断片に分割しておき，それらの断片から元の情報を再構成するという技術である． 　この技術の幅広い展開と標準化のためには，厳密な数学的モデリングが必要である．特に，理論的な研究の面では次のテーマは重要である：通信コスト対計算コスト，計算量的な安全性対情報理論的な安全性，robust性，不正者検知可能性，また，それらの性質を持つ秘密分散法のプロトコル，及びそのプロトコルの最適性．数学的観点では，秘密分散法は特に代数幾何学符号，マトロイド論，組み合わせ論の応用の一例である．情報理論とゲーム理論は秘密分散法の安全性評価の応用の一例である． 　本研究集会の目的は，他の国際会議に例の無い《秘密分散法のネットワークストレージへの応用と基礎数理固め》に特化した講演およびパネル討論を，産業界と大学（海外を含む）から研究者を集めて開催し，数理的アプローチを情報共有し，産業界のニーズを満足するための課題を明らかにすることである．成果物として，本研究集会の会議録を想定している．
組織委員(研究集会) 参加者(短期共同利用)	穴田 啓晃（長崎県立大学・准教授） 櫻井 幸一（公益財団法人九州先端科学技術研究所・研究室長） 須賀 祐治（㈱インターネットイニシアティブ・シニアエンジニア） モロゾフ キリル（東京工業大学・特任准教授） 奥村 伸也（公益財団法人九州先端科学技術研究所・研究員）
成果報告書	【Web公開】成果報告書_共20160005.pdf