

研究報告 2019-CSEC-087

※Windowsの方は[Ctrl]キーを, Macの方は[option]キーを押しながらリンク先をクリックしてください.

12月3日(火)

■Session 1

- (1) [格子問題に基づく Semi-Adaptive 安全な内積暗号](#)
宮澤 智輝, 佐藤 慎悟, 四方 順司
- (2) [アルゴリズム変換型プロキシ再暗号化を用いたオンラインストレージシステムの実装・評価](#)
岡部 大地, 柳 宏之, 木村 隼人, 鈴木 達也, 石橋 拓哉, 渡邊 英伸, 大東 俊博
- (3) [ビットコインにおけるデジタル署名の乱数分析](#)
坂間 潤一郎, 金岡 晃
- (4) [ロボットオペレーティングシステムの対応 OS による暗号通信における性能評価](#)
亘理 克好, 大久保 隆夫
- (9) [ユーザの利用環境に応じたポリシーを設定可能なパスワードマネージャ](#)
松本 大輝, 鈴木 達也, 木村 隼人, 大東 俊博

■Session 2 (企画セッション)

12月4日(水)

■Session 3

- (5) [既存の Web アプリケーションへの適用性を考慮したプリミティブな Trusted Types による Client-Side XSS 防御手法の提案](#)
山崎 勇二, 垣内 正年, 新井 イスマイル, 藤川 和利
- (6) [ブラウザと TLS によるアンチフィンガープリンティングツールの性能評価](#)
中村 綾花, 大久保 隆夫
- (7) [画像処理ベースのプログラム識別を目的としたプログラムの挙動の可視化に関する検討](#)
石川 亮太, 小林 良太郎, 加藤 雅彦, 嶋田 創
- (8) [拡張視覚復号秘密分散法の QR コードへの適用](#)
大川 直也, 栃窪 孝也

■Session 4 (企画セッション)

■ Session 5

(10) [共用 DNS 権威サーバの脆弱性](#)

鈴木 常彦

(11) [A survey on the status of measures against IP fragmentation attacks on DNS](#)

Kenya Ota, Tsunehiko Suzuki

(12) [TDC による遅延時間の高時間分解能観測に基づく CAN メッセージの送信元識別手法](#)

大平 修慈, Kibrom Araya Desta, 新井 イスマイル, 藤川 和利

(13) [サイバー攻撃解析共有プラットフォームを用いた悪性サイトの継続的観測](#)

藤井 翔太, 佐藤 隆行, 青木 翔, 津田 侑, 岡野 友輔, 川口 信隆, 重本 倫宏, 寺田 真敏