# 研究報告 2020-CSEC-90

※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．

## 7 月 20 日（月）

■SITE/BioX

(1) 欧州 SATORI プロジェクトにおける研究開発倫理ガイドライン開発(2)－共通フレームワークと CEN 標準案－
大谷 卓史，大澤 博隆，神崎 宣次，久木田 水生，西條 玲奈

(2) データ保護に関する国際政策動向調査報告～ 欧州における顔認識規制に関する一考察 ～
加藤 尚徳，鈴木 正朝，村上 陽亮

(3) 深層学習を用いた可視光虹彩認証のための特徴抽出器の開発
本田 哲也，高野 博史

(4) 知覚できない視覚刺激を用いた個人認証－ウェーブレット変換と機械学習による識別性能の改善－
三宅 崇弘，金城 希望，中西 功

■ISEC(1)

(5) 分散機械学習手法を用いたビッグデータシステムのプライバシー保護
陳 昭衡，面 和成

(6) ブロックチェーン技術の分散性による無停止メカニズムのリスク分析(2)
田口 渉，面 和成

(7) 指数ブラインディングされた Sliding Window 法を用いた CRT-RSA に対するサイドチャネル攻撃に関する検討
大澤 創紀，上野 嶺，本間 尚文

■CSEC(1)

(8) 対象スレッドの違いによるマルウェア検知精度の比較
梶原 友希，鄭 俊俊，毛利 公一

(9) Windows におけるハッシュ値の伝播によるスレッドインジェクション機能を持つマルウェアの特定手法
田中 大樹，川古谷 裕平，岩村 誠，鄭 俊俊，毛利 公一

(10) 詐欺メール対策の試作
今橋 泰則

■企画セッション；パネルディスカッション
(11)With/Post COVID-19 時代における セキュリティサマーサミットの在り方

■ISEC(2)
(12) Sum of Even-Mansour 擬似ランダム関数に対する量子攻撃
品川 和生, 岩田 哲

(13) 効率的なタグ生成を用いた署名サイズの小さい格子ベース署名方式と実装評価
梶田 海成, 大竹 剛, 小川 一人, 縫田 光司, 高木 剛

(14) ストカスティック演算を用いた確率的準同型暗号の構成に関する検討
小関 隆介, 上野 嶺, 本間 尚文

■CSEC(2)
(15)スペクトル領域上の雑音摂動法における雑音抑圧手法
黄 緒平, 川島 龍太

(16)脆弱性データベースを使用した脅威分析－トピックモデル分析による攻撃事例と大規模脆弱性 DB の突合手法の複数事例への適用－
小柳 洋貴, 寳木 和夫, 三科 雄介, 梅澤 克之

**7 月 21 日（火）**

■HWS
(17) ラッチを用いた物理乱数生成器の乱数の性能評価
鳥居 直哉, 大前 Kevin 秀明

(18) 直線型バスにおける不正機器検出
福田 國統, 安永 貴仁, 礒山 芳一, 朝夷名 巧, 畑 洋一

(19) LiDAR-based SLAM における姿勢推定のための ICP アルゴリズムに対する敵対的スキャン生成攻撃
吉田 康太, 藤野 毅

(20) 車載通信向けメッセージ認証コードに対するサイドチャネル解析
永戸 謙成, ヴィッレ ウリマウル, 上野 嶺, 遠山 毅, 小熊 寿, 本間 尚文

■CSEC(3)
(21)リンクデコレーションおよび CNAME クローキングによるクッキー共有のリスク分析
高田 雄太, 伊藤 大貴, 熊谷 裕志, 神薗 雅紀

(22)Web アプリケーションを安全にする新しいフレームワークの機能
久保田 康平, 小出 洋

■ICSS
(23) 準同型性を有する定数出力局所性を持つコミットメント方式
宮地 秀至, 宮地 充子

■SPT/CSEC(4)
(24) 侵入検知に向けたシステム内悪性活動の紐付け及び可視化手法の検討
末次 信貴, 橋本 正樹, 大窪 巳祐

(25) Android アプリケーションにおける暗号 API 利用動向の基礎調査
河合 惇丞, 金岡 晃

(26) 自律的なセキュリティ行動変容ステージモデルの定義とユーザ要因の影響分析
佐野 絢音, 澤谷 雪子, 山田 明, 窪田 歩

■企画セッション:招待講演
(27) 本人に伝えるプライバシー・ポリシー ～ISO/IEC 29184 より～
崎村 夏彦

■ISEC(3)
(28) 送・受信者間での鍵交換が不要な共通鍵暗号のための鍵共有方式
鈴木 伸治, 佐々木 浩二, 吉村 孝広, 吉村 賢哉, 辻 敏雄, 山澤 昌夫, 五太子 政史, 辻井 重男

(29) 任意の BLS 曲線の最終べきの hard part について
白勢 政明, 南條 由紀

(30) 安全かつ軽量な楕円曲線 LR スカラー倍算
キン ヨウアン, 宮地 充子