研究報告 2022-CSEC-98

※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 19 日（火）

■シンポジウム：「倫理綱領をアップデートする：2 学会倫理綱領改訂とその普及協力」[09：00-11：30]

■HWS1（トラック 1）「13:00-14:40」
(1) 耐量子鍵カプセル化メカニズムに対する多クラス分類ニューラルネットワークを用いたサイドチャネル攻撃の検討
田中 裕太郎，上野 嶺，草川 恵太，伊東 燦，高橋 順子，本間 尚文

(2) 深層学習を用いた非プロファイル型サイドチャネル解析の再考
今福 健太郎，川村 信一，野﨑 華恵，坂本,純一，大須賀　彩希

(3) サイドチャネル攻撃対策を適用した TERO-based TRNG の乱数性評価
大須賀 彩希，藤本 大介，林 優一，川村 信一

(4) 線形漏洩モデルに基づく高 SNR の選択平文セットを用いた相関電力解析結果予測の検討
日室 雅貴，五百旗頭 健吾，豊田 啓孝

■HWS2（トラック 1）[14:50-16:05]
(5) Intel SGX の ECDSA Attestation における検証についての課題とその改善に向けた考察
矢川 嵩，須崎 有康，照屋 唯紀，大原 一真，阿部 洋丈

(6) Reed-Muller 符号を使用した Fuzzy Extractor に対する差分電力解析による PUF レスポンスの窃取
渡辺 壮柾，福田 悠太，大山 達哉，吉田 康太，藤野 毅

(7) 無線技術を介してユーザの資格と位置を自動認証するシステムのセキュリティ
橘 和樹，坂本 純一，松本 勉

■HWS3（トラック 1）[16:15-17:30]
(8) 電磁リレーへの静磁界攻撃とその対策に関する検討
大和田 拓実，橘 樹，松本 勉

(9) 距離偽装攻撃の LiDAR とステレオカメラによる検出
久保 中，深津 勇貴，吉田 直樹，松本 勉

(10)レーザー検知機能付き暗号回路のダブルスポットレーザーによるセキュリティ評価
近野 真生, 吉田 直樹, 坂本 純一, 林 俊吾, 松本 勉

■CSEC1(トラック 2) [13:00-14:40]
(11)IoT マルウェアを無害化するための情報抽出における NCD による分類の検証
岩本 一樹

(12)IoT デバイス上の差分プライバシー強化手法の提案と評価
田口 魁人, 櫻井 幸一, 飯田 全広

(13)Android アプリケーションの例外処理によるリークの制約の演算
大西 導徳, 稲吉 弘樹, 掛井 将平, 齋藤 彰一

(14)ランサムウェアに対する CPU 命令実行抑止機構の提案と評価
榎本 秀平, 葛野 弘樹, 山田 浩史, 白石 善明, 森井 昌克

■CSEC2(トラック 2) [14:50-16:05]
(15)準パススルー型ハイパーバイザーを用いた差分メモリダンプ機構の評価
牧原 京佑, 平野 学, 小林 良太郎

(16)MITRE ATT&CK を用いたログ選 6 定におけるフォレンジック適正の向上に向けた初期検討
中川 桃李, 妙中 雄三, 門林 雄基

■CSEC3(トラック 2)[16:15-17:30]
(17)C2 サーバを対象とした脅威持続把握のための公開情報の再考
堀井 大雄, 藤井 翔太, 青木 翔, 佐藤 隆行, 寺田 真敏

(18)ランダムカット 1 回の 6 枚 XOR プロトコルの不可能性について
芳賀 陸雄, 林 優一, 宮原 大輝, 水木 敬明

(19)勾配情報変化量を利用した SVM ベースのマルウェア検知を標的にする中毒攻撃データの検知
嶋田 創, 蘇 思遠, 長谷川 皓一, 山口 由紀子

■招待講演 [9:00-10:00]
(20)音響法科学と録音属性推定
西村 明

7 月 20 日(水)

■BioX (トラック 1)[10:15-11:55]
(21)超音波による誘発脳波を用いた個人識別-特徴融合における関連性の検討-
石川 裕太, 向井 宏太朗, 中西 功

(22)超音波による誘発脳波を用いた個人識別-電極間相互特徴の導入-
向井 宏太朗, 中西 功

(23) スマートデバイスの継続認証における生体モダリティに関する一検討
渡邊 友花, 山崎 恭

(24)知覚できない振動刺激による誘発脳波を用いた個人識別-脳波スペクトル含有率への正規化導入-
小林 裕季, 中島 宏智, 中西 功

■SITE(トラック 1)[13:00-14:15]
(25)SNS を経由するクレジットカード不正利用のモデル化と抑止方法の検討
趙 智賢, 長田 繁幸

(26)欧州標準化機構における CWA(CEN Workshop Agreement)とはどのような文書か
大谷 卓史

(27)日本法における特許出願の非公開制度の概要
小池 誠

■ICSS (トラック 1)[14:25-15:15]
(28)サイバー犯罪エコノミーを把握するための暗号資産分析システムの提案
森 博志, 熊谷 裕志, インミン パパ, 高田 雄太, 古川 凌也, 櫻井 悠次, 神薗 雅紀

(29)スマートコントラクト上で実行可能な分散型擬似乱数生成手法名
佐古 健太郎, 松尾 真一郎, 森 達哉

■ISEC (トラック 1) [15:25-17:05]
(30)3 次ツイストを持つペアリングフレンドリ曲線における効率的な疎乗算アルゴリズム
林田 大輝, 早坂 健一郎, 照屋 唯紀

(31)CCA 安全性及び復号鍵漏洩耐性を持つ複数の鍵生成局を用いた鍵失効機能付き ID ベース暗号
鈴木 裕大, 藤岡 淳, 佐々木 太良, 永井 彰

(32)ブラウザフィンガープリンティングにおけるプライバシーを考慮した Web サイト利用者の識別・追跡

塚崎 崇至, 布田 裕一, 鈴木 智道, 岡崎 裕之

(33)LWE 仮定に基づく適応的 CCA 安全な平文一致確認可能 ID ベース暗号の効率的な構成
浅野 京一, 江村 恵太, 高安 敦

■CSEC4(トラック 2) [10:15-11:30]
(34)骨格情報を用いた 1 対多掌紋認証の N 位認証率向上に関する基礎検討
芹澤 歩弥, 吉平 瑞穂, 野崎 真之介, 中原 正隆, 馬場 昭, 窪田 歩, 三宅 優, 大木 哲史, 西垣 正勝

(35)利用者教育・訓練から考える組織体制／セキュリティ文化の構築
内田 勝也

(36)個人情報保護システム要件一覧抽出ツールの実現
藤田 真浩, 山中 忠和, 松田 規, 吉村 礼子, 堀込 光, 伊藤 聡志, 菊池 浩明

■SPT(トラック 2) [13:00-13:50]
(37)セキュリティインシデント対応プロセスの改善を動機づけするプロセスシミュレーションを用いたワークショップ手法の提案と評価
粕淵 卓, 稗方 和夫

(38)パスワード強度評価システムの追試と追試研究実施時に得た知見
小沼 悠, 金岡 晃

■PWS 企画セッション(トラック 2)[14:25-15:30]