研究報告 2019-SPT-34

※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 23 日(火)

■A-1:ISEC(1) [9:55-12:00]

(1) 脆弱性情報を利用したゼロデイ攻撃対策システムにおける構成情報収集機能の実装及び脆弱性評価機能の設計
楠目 幹，喜田 弘司，最所 圭三

(2) 擬似的な標的型攻撃の実行に向けた攻撃シナリオ生成方式のアプローチ
高橋 佑典，島 成佳，内藤 厚典，田辺 瑠偉，吉岡 克成

(3) ブロックチェーンネットワークにおけるハニーポット設置に向けた悪意あるユーザのプロファイリング
原　和希，佐藤 哲平，今村 光良，面 和成

(4) 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
田口 渉，今村 光良，面 和成

(5) ビットコインにおけるユーザへの信頼性付与の手法
鈴木 明日香，佐藤 哲平，面 和成

■B-1:CSEC(1) [9:55-12:00]

(6) 金融サービスにおける機械学習システムの適切な活用について：セキュリティと品質に焦点を当てて
清藤 武暢，宇根 正志

(7) 対象者の人数と人間関係に制約のない移動履歴と SNS アカウントの照合
大岡 拓斗，松本 瞬，市野 将嗣，緑川 耀一，吉井 英樹，吉浦 裕

(8) マルウェア対策のための研究用データセット～MWS Datasets 2019～
荒木 粧子，笠間 貴弘，押場 博光，千葉 大紀，畑田 充弘，寺田 真敏

(9) 擬似 C&C サーバを用いた IoT マルウェア駆除手法の検討
三須 剛史，高田 一樹

(10) 観測ロケット MOMO3 号機による小型衛星・小型ロケット用セキュア通信方式の基礎実験
吉田 真紀，森岡 澄夫，尾花 賢

■D-1:BioX [9:55-11:35]

(11) PRNU ノイズに基づく画像クラスタリングにおける類似度計算手法の評価
内田 麻衣，富岡 洋一

(12) 出生 24 時間以内の新生児指紋撮像用 2,400ppi 指紋撮像機の開発
幸田 芳紀，高橋 愛，伊藤 康一，青木 孝文

(13) 手のひら伝搬信号の二階差分位相スペクトルを用いた個人識別
藤田 航平，石本 雄也，中西 功

(14) 顔検出防止技術の評価実験
江藤 一樹，脇 一史，森 駿文，菊池 浩明

■A-2:ISEC [13:10-15:15]

(15) 適応的安全でより効率的な格子鍵失効機能付き ID ベース暗号の構成

高安 敦
(16) クラウドセンシング向け失効可能グループ署名における匿名性の強化
中澤 勇人, 中西 透
(17) ドキュメントにおけるプライバシとリスク評価ツールの試作
三本 知明, 清本 晋作, 北村 光司, 宮地 充子
(18) 剰余逆元計算の新しい量子アルゴリズムと楕円曲線離散対数問題への応用
鞍馬 遼, 國廣 昇
(19) Attribute Based Group Signatures for Revoeable Members
Maharage Nisansala Sevwandi Perera, Toru Nakamura, Masayuki Hashimoto, Hiroyuki Yokoyama

■B-2:HWS(1) [13:10-15:15]
(20) ガロア体算術に基づく暗号ハードウェアの形式的トロイフリー性検証
伊東 燦, 上野 嶺, 本間 尚文
(21) IC チップレベル消費電流シミュレーションによる暗号モジュールのサイドチャネル漏洩評価
安田 一樹, 門田 和樹, 月岡 暉裕, 三浦 典之, 永田 真
(22) 動的電力制御によるサイドチャネル対策の検討
請園 智玲
(23) パイプライン型剰余乗算器を用いたペアリング計算 FPGA のサイドチャネルセキュリティ評価
山﨑 満文, 坂本 純一, 奥秋 陽太, 松本 勉
(24) パイプライン型剰余乗算器を用いたペアリング暗号の FPGA 実装-集約署名の場合-
奥秋 陽太, 坂本 純一, 藤本 大介, 松本 勉

■D-2:SITE(1) [13:10-14:50]
(25) 部分的なパスワードの忘却に対応するパスワードリマインドシステムの提案と実装
細田 涼太, 稲葉 宏幸
(26) 破滅的忘却を軽減するニューラルネットワークを用いたスパムフィルタの提案
川原 秀一, Lu Chen, 稲葉 宏幸
(27) フレーム間のパーシステントホモロジーの差異を用いた動画像電子透かし
木村 崇也, 稲葉 宏幸
(28) ホログラフィと視覚復号型秘密分散法を利用した三次元画像暗号化の検討
高澤 匠, 鈴木 一弘, 髙田 直樹

■招待講演 [15:30-16:30]
(29) 重大インシデントの原因分析の経験から 技術面を中心に
高木 浩光

■全体企画セッション(1) [16:30-17:30]
(30) トップカンファレンス採録への道
山田 明, 笠間 貴弘, 渡邊 卓弥

■全体企画セッション(2) [17:30-18:00]
(31) サイバーセキュリティ研究の倫理的配慮のためのチェックリスト
秋山 満昭, 島岡 政基

7 月 24 日(水)

■A-3:ISEC(3) [9:05-10:45]
(32) SecureHID:USB インタフェースのセキュリティ
ゲッテ ヤン, 矢内 直人, 森 達哉

(33) A Performance Analysis of Supersingular Isogeny Diffie-Hellman with Several Classes of the Quadratic Extension Fields
Yuki Nakajo, Masaaki Shirase, Takuya Kusaka, Yasuyuki Nogami
(34) Generic Even-Mansour Construction Based on Group Actions
Hector Hougaard, Chen-Mou Cheng, Atsuko Miyaji

■B-3:HWS(2) [9:05-10:45]
(35) ダブルレーザー照射装置を用いた TVC に対する命令置換フォールト攻撃
鈴木 朋郎, 坂本 純一, 松本 勉
(36) ASIC 実装した Ring-OscillatorPUF への電磁界解析攻撃
汐﨑 充, 藤野 毅
(37) 電磁的情報漏えいを強制的に誘発する照射周波数推定法に関する基礎検討
鍛治 秀伍, 衣川 昌宏, 藤本 大介, 林 優一
(38) 複数の受光素子を用いたパルス方式測距 LIDAR の計測セキュリティ
末廣 達也, 一ノ瀬 竜矢, 櫻澤 聡, 吉田 直樹, 松本 勉

■C-3:SITE(2) [9:30-10:45]
(39) Boid 的アノーテーションと Labeled-LDA による家族的類似の推論規則生成 -推論攻撃分析と covert channel 攻撃分析を統合する機械学習的アプローチ-
紅林 宏祐, 森住 哲也, 木下 宏揚
(40) OODA ループの「暗黙の誘導制御」に関する一考察～フィッシングサイトへの対抗策～
瀧川 雄一, 辰己 丈夫
(41) 脆弱性評価と修復プロセスを取り入れたサーバ構築演習
鈴木 大助

■A-4:CSEC(2) [10:55-12:35]
(42) n<2k-1 において計算結果の正当性を検証可能な秘密分散を用いた秘匿計算
落合 将吾, 岩村 惠市
(43) ブロックチェーンを用いた IoT システム向け証明サービス基盤の提案
大久保 隆夫, 田嶋 健, 上原 敏幸, 牧野 進二

(44) ブロックチェーンを用いた公正なオンラインゲームの構成手法
佐古 健太郎, 森 達哉, 松尾 真一郎

(45) Ethereum ブロックチェーンで綿菓子を巻く方法～ERC725 フレームワークを用いて e-KYC-e を実現する～
須賀 祐治

■B-4:EMM/ICSS[10:55-12:35]
(46) マルウェア検知システムにおけるブロックチエーンベースのマルウエア情報共有手法の検討
藤 竜成, 臼崎 翔太郎, 油田 健太郎, 山場 久昭, 片山 徹郎, 朴 美娘, 白鳥 則郎, 岡崎 直宣
(47) 能動的攻撃観測環境における端末の自動駆動システム
安田 真悟, 金谷 延幸, 津田 侑, 太田 悟史, 三浦 良介, 井上 大介
(48) 規範的影響による同調行動を考慮した違法コンテンツの利用抑制の検討
山口 央貴, 河野 和宏
(49) システムチップ依存の音響歪みに基づく録音機器識別
西村 明

■C-4:SITE(3)[10:55-12:10]

(50) 必ずしも完全に分有されないロゴスと言語ゲームをつなぐ確率的存在者-セキュリティモデルの限界と人工知能の可能性-
森住 哲也
(51) いわゆる AI に関する国際規制動向調査報告～OECD による AI 原則の分析～
加藤 尚徳, 鈴木 正朝, 板倉 陽一郎, 村上 陽亮
(52) 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(1)－背景と概要－
大谷 卓史, 大澤 博隆, 久木田 水生, 西條 玲奈

■A-5:ISEC(4)[13:45-15:50]
(53) 究極の本人確認のための 3 層構造公開鍵暗号の提案－マイナンバー･STR の秘密鍵への埋め込みとその利用に向けて－
辻井 重男, 才所 敏明, 山澤 昌夫, 四方 光, 佐々木 浩二, 鈴木 伸治
(54) 楕円曲線に基づく匿名公開鍵証明書
大石 和臣
(55) 鍵更新機能付き共通鍵型検索可能暗号の一実現方式
松崎 なつめ, 穴田 啓晃
(56) 第 9 回バル=イラン大学冬季暗号学スクール参加報告
穴田 啓晃
(57) ポチュバルの 3 値論理による Garbled Circuit
林 隼輔, 佐々木 太良, 藤岡 淳

■B-5:HWS(3)[13:45-15:50]
(58) 高位設計フローにベイズ最適化法を応用した設計空間探索
中山 亮平, 粟野 皓光, 池田 誠
(59) 乗法的オフセットに基づく高効率 AES ハードウェアアーキテクチャの設計
上野 嶺, 森岡 澄夫, 三浦 典之, 松田 航平, 永田 真, Shivam Bhasin, Yves Mathieu, Tarik Graba, Jean-Luc Danger, 本間 尚文
(60) 準同型性を有する Paillier アルゴリズムに向けた高性能プロセッサの設計
蔡 純, 粟野 皓光, 池田 誠
(61) センサデバイスの非理想特性を利用した固有性抽出法
チィボ コンスタンロッヅ, 永田 真, 三浦 典之
(62) USB 機器の電圧変化による個体識別の可能性
外山 拓, 坂本 純一, 吉田 直樹, 松本 勉

■C-5:SPT[13:45-15:50]
(63)メールにおける誘導手口の推定手法に関する検討
山本 匠, Bret Harsham, Ye Wang, 西川 弘毅, 上原 航汰, Chiori Hori, 岩崎 亜衣子, 河内 清人, 西垣 正勝
(64)新聞報道される情報漏えい事故の属性分析
新原 功一, 池上 和輝, 菊池 浩明

(65)セキュリティやプライバシーに関する SoK 論文やサーベイ論文を SoK する
金岡 晃
(66)情報セキュリティに関連するガイドラインの Doc2Vec を用いた文書内容の可視化手法の提案とその評価
尾崎 敏司