研究報告 2021-SPT-43

※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（月）

■PWS 企画セッション [9:10-10:15]
〇新たなターゲティング広告におけるプライバシーの課題-FLoC と Unified ID-
寺田 眞治

〇PWSCUP2021 について
PWS2021 実行委員会 Cup ワーキングループ

■CSEC 一般講演 1 [10:30-11:45]
(1) マルウェア検知に対するバックドアポイズニング攻撃の対策としてのオートエンコーダの定量的評価
松本 悠希，成定 真太郎，披田野 清良，内林 俊洋，菅沼 拓夫，樋地 正浩

(2) IoT 機器の WebUI を模したハニーポットの自動生成フレームワーク
山本 萌花，掛井 将平，齋藤 彰一

(3) コンピュータセキュリティシンポジウム CSS2020 開催報告～オンライン化を支えたシステムと UX～
白石 善明，掛井 将平，瀧田 愼，磯部 光平，田宮 寛人，毛利 公美，箕浦 翔悟，冨田 裕涼，古本 啓祐，廣友 雅徳，福田 洋治，池上 雅人，甲斐 博，曽根 直人，森井 昌克

■ISEC 一般講演 1 [10:30-11:45]
(4) Android OS におけるプロセスが占有する仮想メモリに着目した閲覧 WEB サイト特定手法
岡崎 竜也，加藤 広野，春田 秀一郎，笹瀬 巌

(5) MAC アドレス重複環境下におけるアドレス解決プロトコルの不成功を利用した悪性アクセスポイント検知手法
五十嵐 幸佑，加藤 広野，笹瀬 巌

(6) SVM を用いた制御システムに対する偽装命令攻撃の検知
原田 雄基，布田 裕一，岡崎 裕之

■HWS 一般講演 1 [13:30-14:45]
(7) RNS 表現におけるペアリング計算に適した BEEA の逆元計算高速化の検討
森本 康太，藤本 大介，大須賀 彩希，川村 信一，照屋 唯紀，林 優一

(8) BLS12-381 曲線上ペアリング暗号の省メモリ実装
安西 陸，坂本 純一，宋 子豪，吉田 直樹，松本 勉

(9) 並列化 Quotient Pipelining モンゴメリ乗算に基づくFp2 乗算器データパスの設計とその同種写像暗号への応用に関する検討
上野 嶺, 本間 尚文

■SITE シンポジウム 1 [13:30-14:50]
(10) データサイエンスの ELSI
村上 祐子

(11) 数理・データサイエンス・AI リテラシー講座「心得」における情報セキュリティ
辰己 丈夫

(12) データサイエンスの法と倫理規制
加藤 尚徳

■CSEC 一般講演 2 [15:00-16:15]
(13)ビットコイン利用者の特定・追跡の仕組みに関する考察(2)
才所 敏明, 辻井 重男, 櫻井 幸一

(14)サーバ台数 n<2k-1 において実数演算可能な秘匿計算法の提案
納所 勇之介, 岩村 恵市, 稲村 勝樹

(15)n<2k-1 において malicious な攻撃者に対しても安全な秘密分散を用いた秘匿計算の高速化
工藤 凌也, 岩村 恵市, 稲村 勝樹

■SITE シンポジウム 2 [15:00-15:50]
(16) 人工知能の倫理とその教育
久木田 水生

(17) [招待講演]データサイエンスの実践と法・倫理―アバターコミュニティアプリを一例として―
森下 壮一郎

■SITE シンポジウム 3 [16:00-16:30]
ディスカッション

■SPT 一般講演 1 [16:55-18:10]
(18)セキュリティインシデント対応の組織およびプロセスのシミュレーションによる検討手法の提案と評価
粕淵 卓, 稗方 和夫

(19)パスワード構成ポリシー自動取得技術の開発:Web 上認証サイトのパスワード構成ポリシー表示方法に関する大規模調査

藤田 真浩, 山中 忠和, 松田 規, 金岡 晃

(20) アプリのトラッキング許可に対するダークパターン調査
坂本 一仁

■ISEC 一般講演 2 [16:55-17:45]
(21) 認証鍵交換方式 FSXY におけるハイブリッド安全性の検証
川口 武瑠, 鈴木 誠十郎, 藤岡 淳, 佐々木 太良

(22) Somewhat 準同型暗号に基づく生体テンプレート保護システムの評価
田宮 寛人, 一色 寿幸, 森 健吾, 尾花 賢, 大木 哲史

7 月 20 日(火)

■SPT 一般講演 2 [9:00-10:15]
(23) Windows Update に関するユーザの行動傾向と環境・心理学的要因の関係の調査
河田 真由子, 古川 和快, 角尾 幸保

(24) 個人特性を活用したデータ流通に向けた一貫性選好に関する検討
大橋 盛徳, 藤村 滋, 土屋 志高, 中平 篤

(25) ユーザブルセキュリティ研究における満足度評価の実態調査
金岡 晃

■ISEC 一般講演 3 [9:00-10:15]
(26) 鍵紛失時における非常ボタン式資産退避手法の実用化に関する考察
松崎 なつめ, 喜多 義弘

(27) Dogecoin ネットワークの特徴とセキュリティリスクの考察
今村 光良, 面 和成

(28) NFT の信頼性にみるセキュリティリスクの考察
木村 圭吾, 今村 光良, 面 和成

■CSEC 一般講演 3/BioX 一般講演 1 [10:30-12:10]
(29) サーバレスアプリケーションにおけるデータの変化に伴う機密度再計算手法の提案
田村 悠, 磯部 義明

(30) Black-box Adversarial Attack による顔認証へのなりすまし可能性に関する検討
ヴォゴックコイ グエン, 寺田 崇倫, 西垣 正勝, 大木 哲史

■EMM 一般講演 1/ICSS 一般講演 1 [10:30-12:10]
(31) Minecraft を活用した AI リテラシー学習ツールの開発

岸本 彗佳, 河野 和宏

(32) ハイブリッド乗法的秘密分散
吉田 真紀

(33) Twitter で収集された Android アプリのアクセシビリティサービスの利用率と API Level の分析
市岡 秀一, 三村 隆夫, 中嶋 淳, 山内 利宏

(34) ID/Password 設定に不備のある IoT 機器におけるマルウェア感染可能性の大規模調査
村上 洸介, 笠間 貴弘, 井上 大介

■招待講演 [13:10-14:10]
(35)IoT におけるサイバー攻撃の最新動向～IoT マルウェアの多様化～
田辺 瑠偉

■HWS 一般講演 2 [14:25-15:15]
(36) マスキング対策された暗号ハードウェアへの深層学習を用いたサイドチャネル解析
小嶋 健太, 伊東 燦, 上野 嶺, 本間 尚文

(37) ハードウェア実装された未対策 AES および RSM-AES に対する深層学習サイドチャネル攻撃
福田 悠太, 吉田 康太, 橋本 尚志, 藤野 毅

■ISEC 一般講演 4 [14:25-15:15]
(38) ForkSkinny に対する MILP を用いた差分パス探索
岡崎 雅哉, 佐々木 悠, 岩田 哲 br>
(39) 暗号ハッシュ関数を利用した仮想通貨採掘の時間分散に対する計算機実験評価
池辺 慶, 櫻井 幸一

■HWS 一般講演 3 [15:30-16:45]
(40) PUF を信頼の基点とした RISC-V TEE 環境の実装
吉田 康太, 須崎 有康, 藤野 毅

(41) CMOS イメージセンサを利用した物理乱数生成器の性能評価
龍野 隼人, 大山 達哉, 白畑 正芳, 大倉 俊介, 藤野 毅

(42) リングオシレータ型真性乱数生成器の実装と評価(2)
皆川 隆一, 大前 ケヴィン秀明, 林 光太郎, 鳥居 直哉

■SITE 一般講演 1 [15:30-17:10]
(43) DCT ブロックに適応的にゲインを乗じる周波数領域利用型ステガノグラフィの検討
大沼 海仁, 宮田 純子

(44) トランスクリエーションを利用したプログラミング教育方法の開発－トランスクリエーションスケールの創造と活用－
森田 正大

(45) 意思決定支援としての研究倫理－AoIR 倫理ガイドラインの原則と倫理分析－
大谷 卓史, 壁谷 彰慶, 西條 玲奈, 神崎 宣次, 大澤 博隆, 久木田 水生

(46) いわゆる AI に関する国際規制動向調査報告～欧州委員会による AI 規則提案の分析 2～
加藤 尚徳, 鈴木 正朝, 板倉 陽一郎, 村上 陽亮, 花原 克年