研究報告 2021-CSEC-192

※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．

3 月 15 日(月)

■トラック 1 CSEC:社会分析・教育[9:00-10:20]

(1) フィッシング詐欺のビジネスプロセス分類
林 憲明，唐沢 勇輔，中村 智史，坂本 美子，柘植 悠孝，岡田 雅之，加藤 雅彦

(2) グループ会社の情報セキュリティ対策実施を左右する要因の分析
古殿 瑶子，稲葉 緑

(3) 高校生に対する効果的な情報モラル教材に関する研究
稲葉 啓太，稲葉 緑

(4) Twitter 上における大規模な情報拡散事例の分析とその考察
嶋田 里聖，田畑 唯斗，利光 能直，菊田 翼，田中 絵麻，齋藤 孝道

■トラック 2 CSEC:セキュアプロトコル [9:00-10:20]

(5) 差分プライベートな秘密計算のための暗号化された離散乱数を生成する非対話型二者間プロトコル
紀伊 真昇，市川 敦謙

(6) 6 枚のカードを用いた非コミット型 3 入力 AND プロトコル
佐々木 優，宮原 大輝，水木 敬明，曽根 秀昭

(7) 手の内だけで簡単に実行可能な Six Card Trick とカード入力後の置換に関する考察
須賀 祐治

(8) Generalization of Contact Tracing
Mathieu de Goyon，Atsuko Miyaji，Yangguang Tian

■トラック 1 CSEC:システム設計・実装 [10:30-11:50]

(9) メモリ破損脆弱性を利用した攻撃に対する Rust を用いた対策手法
千脇 貴之，橋本 正樹

(10) ブラウザフィンガープリントを用いた会員 ID 推定を提供する Web API システムの提案と構築
渡名喜 瑞稀，藤井 達也，神 章洋，利光 能直，北條 大和，齋藤 孝道

(11) Coq を用いたソフトウェアスイッチの設計と実装
斎藤 文弥，高野 祐輝，宮地 充子

(12) Rust 言語用動的メモリアロケータの検査フレームワークの提案
尾崎 純平, 高野 祐輝, 宮地 充子

■トラック 2 DPS:システム基盤技術 [10:30-11:50]
(13) 天候要素を考慮したビデオストリーミングのノイズ除去フレームワークの設計と実装
陳 明康, 孫 静涛, 佐賀 一繁, 丹生 智也, 合田 憲人

(14) 確率的暗号ベースの検索可能暗号を用いた全文検索の高速化検討
森 郁海, 平野 貴人, 中村 嘉隆, 稲村 浩

(15) DPDK の超高速通信を活用した、緩和法解析の分散処理に関する研究
伴野 隼一, 矢吹 道郎

(16) 地域を支える山間道路のセンシングデータ収集と解析に関する試み
廣森 聡仁, 塚本 幸宏, 山口 弘純, 高井 峰生, 梶田 宗吾, 東野 輝夫, 前野 誉

■トラック 1 CSEC:攻撃検知・防御 [12:50-14:10]
(17) 仮想的 BGP リンクの分類と検知手法の検討
長坂 明紀, 相田 仁

(18) TLS への Bleichenbacher's CAT 攻撃の考察および実装
嶂南 秀敏, 王 イントウ, 藤崎 英一郎

(19) 複数組織の接続傾向を用いた自律進化型防御システムの提案
西嶋 克哉, 川口 信隆, 植木 優輝, 重本 倫宏, 近藤 賢郎, 中村 修

(20) 不適切なデータセットや処理方法を用いた機械学習による XSS 攻撃検出研究の解説と精度の比較
飯野 和真, 宇田 隆哉

■トラック 2 DPS:ネットワーク基盤 [12:50-14:10]
(21) ホワイトボックススイッチを利用したネットワークサービスプロバイダ視点での機能カスタマイズを実現する VNF 基盤
田部 悠介, 近藤 賢郎, 寺岡 文男, 金子 晋丈

(22) 地理的分散環境を想定した MEC におけるオフローディング機構
稲垣 勇佑, 渡邊 大記, 安森 涼, 近藤 賢郎, 熊倉 顕, 前迫 敬介, 張 亮, 寺岡 文男

(23) NDN ベースのエッジコンピューティング環境における位置データの計算ノード選択に関する一考察
武政 淳二, 小泉 佑揮, 田上 敦士, 長谷川 亨

(24) AIS 拡張利用を目指したユーザ参加型リアルタイム風況データと航海状態の可視化に向けた提案

藤本 隆晟, 浦上 美佐子

■トラック 1 CSEC:IoT セキュリティ [14:20-15:40]

(25) IoT マルウェアの分類における画像化を用いた手法とシステムコール列を用いた手法の比較
イボット アリジャン, 大山 恵弘

(26) クロック分解能を用いた Raspberry Pi 仮想マシンの検出
鈴木 克弥, 大山 恵弘

(27) 車載エレクトロニクスへのサイバー攻撃を解析するための三層型ログ保全技術の提案
五十嵐 貴久, 松井 俊浩

(28) Intel SGX を用いたサーバーにおけるチート対策のクライアント委任手法
高橋 孝輔, 橋本 正樹

■トラック 2 DPS:無線ネットワーク [14:20-15:40]

(29) 密集無線 LAN 環境における Q 学習を用いた送信電力・信号検知閾値制御の検討
武松 未来, 坂井 渉太, 重野 寛

(30) 異種無線多重 MIMO チャネル動的構成方式における動的感度レート制御
奥本 裕介, 滝沢 泰久

(31) モバイルセンサネットワークにおける端末密度情報収集手法について
粉川 博明, 寺井 元基, 神崎 映光

(32) 開放環境無線センサネットワークにおける協調的改ざん検知と自己組織化マップを用いた不正ノード孤立化手法の提案
木村 圭希, 滝沢 泰久

■トラック 1 CSEC:暗号(1) [15:50-17:30]

(33) 解読計算量に基づく LWE 暗号の安全性に関する検討
岡 翔子, 國枝 義敏, 上原 哲太郎, 猪俣 敦夫

(34) Threshold ECDSA for securing digital assets in combination with blockchain
Zhaobo Wang, Atsuko Miyaji

(35) 耐量子暗号 *Giophantus*$^{+}$暗号における多項式の項省略による線形代数攻撃の改良
中村 友耀, 奥村 伸也, 宮地 充子

(36) 格子を用いた複数鍵線形準同型署名
小﨑 俊二, 有田 正剛

(37) Decision Ring-LWE 問題に対する部分格子攻撃の改良について
室井 謙典, 奥村 伸也, 宮地 充子

■トラック 1 DPS:協調制御 [15:50-17:10]
(38)分散台帳に従うデータ流通制御に向けたオフチェーンデータの紐づけ方式
大橋 盛徳, 藤村 滋, 中平 篤

(39)IoT データ経済流通のための価格競争が起きない価格決定手法に関する一検討
吉廣 卓哉

(40)需要分布に基づくロードプライシングにおける計算量削減手法の検討
山本 規吉, 川上 朋也

(41)天気予報による発電量予測をもとにユーザとセンサーデータのサービスレベルを合意する手法
杉本 一彦, 串田 高幸

3 月 16 日(火)

■トラック 1 CSEC:暗号通貨・ネットワーク分析 [9:00-10:20]
(42)オーバレイネットワーク情報を活用した暗号通貨追跡手法の研究
髙橋 智士, 大塚 玲

(43)ハニーポットにより観測される DRDoS 攻撃の影響評価と要因分析
新谷 夏央, 牧田 大佑, 吉岡 克成, 松本 勉

(44)Android における遷移元 Web サイトから利用者の意図しない Web サイトまでの通信内容の分析
川島 千明, 市岡 秀一, 山内 利宏

(45)不正な暗号資産のマネーフロー分析を目的とした取引タイミングに着目した可視化手法の提案
森 博志, 熊谷 裕志, インミン パパ, 高田 雄太, 鈴木 将吾, 神薗 雅紀

■トラック 2 CSEC:情報収集・分析 [9:00-10:20]
(46)準パススルー型ハイパーバイザによるメモリデータ収集機能の性能改善と評価
大森 貴通, 水野 広基, 牧原 京佑, 平野 学, 小林 良太郎

(47)Cyber Threat Intelligence の構造化による分析支援手法の提案
藤井 翔太, 川口 信隆, 重本 倫宏, 山内 利宏

(48)ユーザ操作特定のためのカーネル内でのプロセス挙動収集手法
藤枝 慶弘, 羽角 太地, 島 成佳, 安田 真悟, 鄭 俊俊, 毛利 公一

(49)ダークネットにおける大規模調査パケットを考慮したポート番号埋め込みベクトルによるスキャンパケット解析

石川 真太郎, 中藤 大暉, 班 涛, 小澤 誠一

■トラック 1 CSEC:マルウェア検知 [10:30-11:50]
(50)デコイファイルを用いた暗号化型ランサムウェアの検知とプロセス特定に関する検討
荻原 拓海, 小林 良太郎, 加藤 雅彦

(51)IoT マルウェア自動検知のための悪性コマンド列の特徴に対する概念ドリフト検出
小川 真聖, 松井 俊浩

(52)ストレージアクセスパターンを用いた機械学習によるランサムウェア判別システムの精度向上に関する考察
程田 凌羽, 平野 学, 小林 良太郎

(53)動的解析システムのネットワーク接続の有無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

■トラック 2 DPS:ネットワーク制御 [10:30-11:50]
(54)ビザンチン障害耐性を備えるキー順序保存型構造化オーバーレイネットワークの実現に向けて
寺西 裕一, 秋山 豊和, 安倍 広多

(55)オーバレイネットワークにおける帯域消費が軽微な L2 ループ検出手法の提案
野呂 正明, 高野 陽介, 小口 直樹, 阿部 俊二

(56)複数の時間間隔に基づくオーバレイネットワークにおけるルーティング効率化手法の検討
久保 達也, 川上 朋也

(57)AS グラフ構造に基づく経路情報耐性と協調防御の有効性に関する解析
明石 修

■トラック 1 CSEC:ネットワーク攻撃検知 [12:50-14:10]
(58)組織内で学習データを採取し定期的に判別器を更新する機械学習ベースの NIDS
佐藤 秀哉, 林 はるか, 小林 良太郎

(59)MQTT ブローカーのための免疫的攻撃検知の試作
岡本 剛

(60)疑似ログ生成によるアノマリ検知技術強化に関する考察
山本 匠, 岩崎 亜衣子, 小林 創, 西川 弘毅, 河内 清人, 吉村 礼子

(61)DCGAN とパーティクルフィルタを用いたネットワークトラフィック異常検出
森岡 卓哉, 青木 茂樹, 宮本 貴朗

■トラック 2 DPS:機械学習 [12:50-14:10]

(62) 分散機械学習 MicroDeep のエナジーハーベスト実装と実証実験
Gereltod Sengun, 山口 弘純, 東野 輝夫, 安本 慶一, 田上 敦士

(63) 歩行者の移動傾向を考慮した強化学習による自律移動ロボットナビゲーション
一色 春香, 天野 加奈子, 加藤 由花

(64) Auto-Encoder による異常検知手法のための実数を使用した秘密計算方法
松本 麻里, 古田 雅則

(65) 推論多重実行における GPU 資源利用効率化技術
鈴木 貴久, 田中 美帆, 豊永 慎也, 松倉 隆一

■トラック 1 CSEC :暗号(2) [14:20-15:40]
(66) CFB モードにおける IV の誤使用と計算量の低下現象について
沖津 直樹

(67) ニューラルネットワークを用いた軽量ブロック暗号 PRESENT の解析
勝田 耕作, 五十嵐 保隆, 金子 敏信

(68) General Sieve Kernel の考察および改良
長谷川 奨, 王 イントウ, 藤崎 英一郎

(69) 情報理論的に安全な完全準同型暗号に関する考察
佐藤 慎悟, 四方 順司

■トラック 2 DPS:サービス支援 [14:20-15:40]
(70) 持続可能なセキュア共生情報システムの提案とデジタル寺院・ネバーダイプロフェッサへの応用
藤田 茂, 滝 雄太郎, 白鳥 則郎

(71) 長期的な孤立運用後にサービスを統合可能なデータ管理手法
大坂 優輝, 北形 元, 長谷川 剛

(72) オントロジを活用した多様な利用者環境に適用可能な IoT サービス構成手法
和室 昂佑, 北形 元, 長谷川 剛

(73) 非集中型モデルによる動画配信プレーヤー用個人視聴データ取得・蓄積モジュールの試作
関根 大輔, 松村 欣司, 藤井 亜里砂