# 研究報告 2020-SPT-36

※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 2 日(月)**
＝A 会場　1 日目＝

■ICSS(1-1) [10:00-11:00]
(1)2 種類の損傷を考慮したバックアップ手法の改良
　　蓮池 大我，満保 雅浩

(2)設計モデルを用いた情報資産セキュリティ特性の推測手法
　　植田 武，清水　孝一，日夏 俊，大松,史生

(3)5 人の管理者の場合の複数割り当て法による情報比の評価
　　新間 祐太郎，栃窪 孝也

■ICSS(1-2) [11:10-12:10]
(4)Alloy Analyzer を活用した Infrastructure as Code の正当性検証
　　長谷 亮，松浦 陽平

(5)LED の個体識別における温度変化の影響
　　土屋 彩夏，藤 聡子，李 陽，崎山 一男，菅原 健

(6)ブロックチェーンを用いたログ保存システム
　　池田 貴志，廣友 雅徳，福田 洋治，毛利 公美，白石 善明

■ICSS(1-4) [13:30-14:50]
(7)ファームウェアに着目した IoT 機器のセキュリティ機能の調査
　　白石 周碁，福本 淳文，塩治 榮太朗，秋山 満昭，山内 利宏

(8)ニューラル機械翻訳モデルを用いた異なるアーキテクチャ間における類似バイナリコードの検索
　　青柳 守俊，辻 秀典，橋本 正樹

(9)AddressSanitizer を併用したデバイスドライバに対するファジングの有効性検証
　　石井 健太郎，伊沢 亮一，森井 昌克

(10)ランサムウェア感染時の復旧対策ツールの開発【続報】
　　古門 良介，池上 雅人，長谷川 智久，原田 隆史，木谷 浩，森井 昌克

■ICSS(1-6) [15:00-16:40]目
(11)IoT 機器の通信機能を起点としたバックドア検知手法の提案

依田 みなみ, 櫻庭 秀次, 山本 純一, 清 雄一, 田原 康之, 大須賀 昭彦

(12) Android 端末に対する JavaScript を用いたタイミング攻撃の検証
杉田 敬亮, 伊沢 亮一, 森井 昌克

(13) ダークネット観測における大規模スキャナの判定指標の提案
遠藤 由紀子, 森 好樹, 島村 隼平, 久保 正樹

(14) 広域スキャンとダークネット観測に基づく IoT マルウェア感染状況の分析
森下 瞬, 小川 航汰, 原 悟史, 田辺 瑠偉, 吉岡 克成, 松本 勉

(15) Mirai はあなたがスマートスピーカーに話しかけたかわかるーホームルータに侵入した攻撃者によるプライバシ侵害についてー
奥田 翔也, 玉井 達也, 藤田 彬, 吉岡 克成, 松本 勉

**3 月 3 日(火)**
＝A 会場　2 日目＝

■ICSS(2-1) [9:00-10:30]
(16) HTTP リクエストの調査と偽の User-Agent 値の識別方法の提案
井上 仁人, 橋本 正樹

(17) Web 上のリアルタイム情報を利用した WAF シグネチヤ生成の初期検討
熊崎 真仁, 長谷川 皓, 山口 由紀子, 嶋田 創

(18) 全ポート待受型の簡易 TLS ハニーポットにより観測されたサイバー攻撃の分析
牧田 大佑, 島村 隼平, 久保 正樹, 井上 大介

(19) TLS バージヨン移行と EV 証明書利用に関する局所的調査(FY20194Q)
須賀 祐治

■ICSS(2-2) [10:40-12:00]
(20) ダークウェブ上に蔓延する違法有害情報の自動分類エキスパートシステムの開発
小林 華枝, 橋本 正樹

(21) 様相 $\mu$ 計算による RNN のモデル検査
青島 達大, 碓井 利宣

(22) ニューラル機械翻訳システムに対する敵対的攻撃
坂本 岳史, 森 達哉

(23) 心電図を標的とした敵対的攻撃
小野 大河, 菅原 健, 森 達哉

■ICSS(2-4) [13:10-15:10]
(24)題名
　　氏名

■ICSS(2-5) [15:20-16:40]
(25)マルウェアの動的解析におけるログ出力が停止する現象の実態調査
　　森本 康太, 鄭 俊俊, 瀧本 栄二, 齋藤 彰一, 毛利 公一

(26)効果的な single-sided RAMBleed の提案
　　長濱 拓季, 瀧田 愼, 廣友 雅徳, 森井 昌克

(27)コンセプトドリフトに対応した脆弱性記述に基づく脆弱性特性の自動評価～トピック固有単語を用いた特徴抽出手法～
　　中川 舜太, 古本 啓祐, 白石 善明, 瀧田 愼, 毛利 公美, 森井 昌克

**3 月 2 日(月)**
＝B会場　1 日目＝

■SPT(1-1) [9:40-11:00]
(28)情報セキュリティ意識に対する楽観主義バイアスの影響分析
　　宮地 勇作, 小松 文子

(29)個人のリスク認知と情報セキュリティ対策行動
　　田﨑 来実, 小松 文子

(30)児童を対象としたパスワードに関する知識・行動の日米比較研究
　　坪根 恵, 森 啓華, 長谷川 彩子, 秋山 満昭, 森 達哉

(31)バーチャル YouTuber 技術を用いたセキュリティ教育コンテンツの作成
　　中山 実咲, 上原 哲太郎

■ICSS(1-3) [11:10-12:10]
(32)脆弱性情報の自動監視に基づく警告・初動対応自動化技術の構築
　　高橋 健志, 牛込 龍太郎, 鈴木 未央, 井上 大介

(33)セキュリティ通知における連絡先の有効性評価
　　斉藤 美織, 田辺 瑠偉, 藤田 彬, 吉岡 克成, 松本 勉

(34)コンテンツフィルタを回避する敵対的映像データ
　　大森 敬仁, 森 達哉

■ICSS(1-5) [13:30-14:50]

(35)アグリケートメッセージ認証方式の実装と評価
山岸 篤弘, 武内 良男, 竹久 達也, 西浦 英一, 鄒 家発, 今村 祐, 四方 順司, 廣瀬 勝一, 中尾 康, 石田 祐子, 今井 秀樹, 平田 康夫

(36)ハッシュチェーンアグリゲーションを用いた認証方式の拡張
平井 晨太, 双紙 正和

(37)ストリーム暗号 Salsa20/ChaCha における逆関数の特性を用いた安全性解析
松岡 勇介, 宮地 充子

(38)定数出力局所性を持つ効率的で高機能なコミットメント方式
宮地 秀至, 宮地 充子

■SPT(1-2) [15:00-16:40]
(39)ドローンにおけるセーフティ・セキュリティの統合リスク分析の試み
和田 健治, 小松 文子

(40)オストリッチ ZIP の総合的リスクアセスメント
中山 道裕, 金岡 晃

(41)フェイク情報の信じやすさと対策の基本検討
佐藤 直, 辻井 重男, 白鳥 則郎, 山口 浩, 才所 敏明, 趙 晋輝, 五太子 政史, 近藤 健, 山澤 昌夫, 山本 博資

(42)エンドユーザはフィッシングサイトを見破ることができるか？視線追跡装置と半構造化インタビューを用いたユーザ行動分析
シュウ インゴウ, 森 啓華, 櫻井 悠次, 坪根 恵, 飯島 涼, 阿曽村 一郎, 坂本 一仁, 島岡 政基, 森 達哉

(43)Brand Validation 証明書の提案および評価～Web サイトのアイデンティティ表示の改善～
奥田 哲矢, 千葉 直子, 秋山 満昭, 福永 利徳, 鈴木 亮平, 神田 雅透

**3 月 3 日(火)**
＝B会場　2 日目＝

■SPT(2-1) [9:10-10:30]
(44)半教師ありトピックモデルによるセキュリティレポートの分類の評価方法について
杉本 健太, 長田 侑樹, 瀧田 愼, 古本 啓祐, 白石 善明, 高橋 健志, 毛利 公美, 髙野 泰洋, 森井 昌克

(45)セキュリティレポートの時系列トピックモデルを用いた分析
長澤 龍成, 古本 啓祐, 瀧田 愼, 白石 善明, 高橋 健志, 毛利 公美, 髙野 泰洋, 森井 昌克

(46) Estimating Cyber Kill Chain Phases from Unstructured Technical Reports
Thin Tharaphe Thein, Yuki Ezawa, Shunta Nakagawa, Keisuke Furumoto, Yoshiaki Shiraishi, Toru Nakamura, Masayuki Hashimoto, Masami Mohri, Masakatu Morii

(47) トピックモデルとクラスタリングによるセキュリティレポートのマルチラベル分類
長田 侑樹, 瀧田 愼, 古本 啓祐, 白石 善明, 高橋 健志, 毛利 公美, 髙野 泰洋, 森井 昌克

■ICSS(2-3) [10:40-12:00]
(48) スマートコントラクトを用いた安全なセカンドプライスオークションの提案
杉谷 勇気, 宮地 充子

(49) セッション型を用いたアクセス制御システムの評価
西口 朋哉, 宮地 充子, 高野 祐輝

(50) 属性ベース暗号を用いたプライバシポリシーの実現方法とその応用
林 基, 宮地 充子

(51) ブロックチェーンを用いたユーザ中心の認可プロトコルの一実装~User-Managed Access の Hyperledger Fabric による実装~
江澤 友基, 掛井 将平, 白石 善明, 瀧田 愼, 毛利 公美, 森井 昌克

■ICSS(2-6) [15:20-16:40]
(52) 属性ベース暗号方式を用いた FIDO2 の拡張による代理認証の実現
大川 悠人, 猪俣 敦夫, 上原 哲太郎

(53) アファィン座標系に基づく安全で軽量な楕円曲線スカラー倍算
キン ヨウアン, 宮地 充子

(54) ベクトル命令による Curve25519 の高速実装
ワン チンユ, トーン ジョウ, 宮地 充子

(55) 楕円曲線に基づく匿名公開鍵証明書の実装の検討
大石 和臣