様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

令和　２ 年　 ５ 月 ２５ 日現在

機関番号：３２６１２
研究種目：基盤研究(C)（一般）
研究期間：2017～2019
課題番号：１７Ｋ０６４４０

研究課題名（和文）IoTにおける安全なWebインタフェースおよび高効率なデータ配信方式に関する研究

研究課題名（英文）Research on Secure Web Interface and Efficient Data Distribution on IoT

研究代表者
笹瀬　巌（Sasase, Iwao）

慶應義塾大学・理工学部（矢上）・教授

研究者番号：００１８７１３９

交付決定額（研究期間全体）：（直接経費）　　3,700,000円

研究成果の概要（和文）：Web インタフェースにおける高いセキュリティとプライバシーを確保するため，SSL サーバ証明書の認証レベルに着目した悪性 Android アプリ検知手法，色相を利用した自動的に検知範囲を拡大可能なフィッシングサイト検知法，宛先までのホップ数解析によるTracerouteを用いた検知手法，良性と悪性の特徴出現の比率と比率差を考慮したAndroidにおけるICCに着目したマルウエア検出法を提案した．
また,効率的なデータ配信方式として，経路構築法RPLがセンサの観測データを収集する経路を作成する際に，同時にネットワーク構造を収集することで省電力化を実現するコード配布方式を提案した．

研究成果の学術的意義や社会的意義
偽造サイトや SNS 上の不正アカウントを用いたWebインタフェースセキュリティ方式や，効率的なデータ配信方式を提案し，その研究成果は,複数のユーザが各々の目的に応じたアプリケーションを，Webインタフェース経由でIoT 機器へアクセスする際の，Webインタフェースのセキュリティの確保，および，IoT 機器への効率的な配信において有効であり,社会的意義は高い．

研究成果の概要（英文）：In order to achieve high security and privacy on Web interface, we proposed Android malware detection scheme based on level of SSL server certificatehue signature auto update system for visual similarity-based phishing detection with tolerance to zero-Day attack, traffic feature-based botnet detection scheme emphasizing the importance of long patterns, and effective feature selection scheme for Android ICC-based malware detection using the gap of the appearance ratio.
We also proposed RPL-based tree construction scheme for target specific code dissemination in wireless sensors networks as an effective data distribution scheme.

研究分野：IoTにおけるデータ配信とセキュリティ

キーワード：Internet of Things　データ配信　セキュリティ　Webインターフェース　偽造サイト　不正アカウント　コード配布

様　式　Ｃ－１９、Ｆ－１９－１、Ｚ－１９、ＣＫ－１９（共通）

１．研究開始当初の背景

様々なデバイスをネットワークへ接続することで情報の収集を自動化する IoT (Internet of Things) は，患者の健康管理，商品の品質管理などのアプリケーションを実現する基盤技術であり，異なる複数の目的のアプリケーションを扱える汎用性，省電力性，セキュリティ・プライバシが求められる．しかし，様々なアプリケーションが混在する環境における効率的なアプリケーションデータの配信方法 および IoT 機器を操作する Web インタフェースのセキュリティ・プライバシに関する検討は十分ではない．そこで，
本研究では，IoT における省電力かつ汎用性の高いデータ配信方式，および，高いセキュ リティ・プライバシを満たす Web インタフェースについて検討を行う．

２．研究の目的

センサに代表される様々なデバイスをネットワークへ接続することで情報の収集を自動化する IoT が急速に普及している．従来，多くの IoT 機器は特定の目的に特化したものが使用されていた．しかし，近年，複数 のユーザが各々の目的に応じたアプリケーションを，Web インタフェース経由でインストールして使用する汎用性の高い IoT 機器が注目されている．このような環境では，ユーザが IoT 機器へアクセスするための Web インタフェースのセキュリティ・プライバシの確保およびユーザのアプリケーション を IoT 機器へ効率的に配信する方法が重要となる．しかし，偽造サイトや SNS 上の不正アカウントを用いた Web インタフェース上の攻撃や，それに伴うユーザの位置情報などのプライバシ情報の流出は深刻な問題となっている．また，従来の IoT 機器へのデータ配信方法は，単一ユーザを想定しており，複数のユーザによる同時利用時には，信頼性が低下する問題がある．そこで，本研究では，Web インタフェースのセキュリティの確保と，効率的なデータ配信方式について検討する．本研究における具体的な課題と研究目的を，以下に示す．

(1) Web インタフェースにおけるセキュリティの確保および偽造サイト検出方式

Web インタフェースにおけるセキュリティの課題として，パケットを暗号化する悪性 Android アプリの検知，ボットネットの検出，新種の DDoS 攻撃である Target Link Flooding Attack の検知，マルウエアの検出などがあげられる．また，偽造サイトの検出法として，主にブラックリストによってユーザからのアクセスを防止する方法が取られているが，ブラックリストに登録されていない偽造サイトにはアクセス可能となってしまう．検索エンジンの検索結果を利用する方式も取れているが，検索エンジンの提供する検索 API 等は高額であり，汎用性に乏しい．そこで，偽造サイト検出するための専用データベースを用意し，検索エンジンを用いないことに加え，過去の偽造サイトの情報を用いて検出し，同時に標的サイトも特定する方式を提案する．

(2) 効率的なデータ配信方式

無線センサネットワークを用いたデータの配信においては，複数のアプリケーションの同時配信時には特定の経路に負荷が集中して配信の信頼性が低下する問題がある．そこで，ネットワークの殆どのセンサはアプリケーションのインストール対象ではないことに注目し，複数のアプリケーションが，これらセンサを用いて，複数経路を容易に構築できる並列配信を行うことにより，遅延と中継回数を従来と同程度に保ちつつ，少ない変更で信頼性の改善ができる方式を提案する．

３．研究の方法

提案方式の有効性を明らかにするために，理論解析および Contiki OS のシミュレータ Cooja，Python，機械学習等を用いたシミュレーションを行うとともに，無線 LAN，Bluetooth，RFID などを用いた実機実験も行う．提案方式の理論解析・計算機シミュレーションプログラムの作成などに関しては，本研究課題のサブテーマに密接に関わる研究を行っている研究代表者の研究室に所属する大学院・学部学生と共に研究を推進する．研究成果は速やかに国内研究会や国際会議で発表し，内外の研究者との討論を積極的に行い，研究レベルと内容を充実させ，学術論文誌への投稿を行う．

４．研究成果

Web インタフェースセキュリティの確保，および，効率的なデータ配信に関して，論文誌 8 件、国際会議論文 10 件，研究会 12 件の学術的成果をあげ，国際的にも高い評価を得た．具体的な研究成果を，以下に示す．

(1) 経路構築法 RPL がセンサの観測データを収集する経路を作成する際に，同時にネットワーク構造を収集することで省電力化を実現するコード配布方式

バグの修正などを目的としたアップデートコードの配信において，一部のセンサのみを配信対象とした電力効率の良い方式が課題となっている．従来方式は，可能な限り多くの配布対象を含む少数の経路を用いることで省電力化を実現しているが，経路特定のために，多数の制御メッセージを用いてネットワーク全体の構造を把握する必要があり，配布対象のセンサが少ない状況下では，オーバーヘッドが増大する問題があった．本論文では，経路構築法 RPL が，センサの観測データを収集する経路を作成する際に，同時に，ネットワーク構造を収集することで省電力化を実現する，コード配布方式を提案した．事前にネットワーク構造を収集することにより，配布対象のセンサのリストの送信のみで，省電力な経路を特定することが可能となり，制御メッセージに起因した消費電力の削減が可能となる．シミュレーション結果より，提案方式は，従来方式と比べ最大 50%の送信回数の削減が可能であることを示した．

(2) SSL サーバ証明書の認証レベルに着目した悪性 Android アプリ検知手法

パケットを暗号化する悪性 Android アプリを検知するために，SSL サーバ証明書の認証レベルに着目した悪性 Android アプリ検知手法を提案した．信頼性の高い証明書を取得するためには，厳正な審査が必要であるため，攻撃者は多くの場合，パケットを暗号化するために信頼性の低い証明書を用いる傾向にある．したがって，攻撃者のサーバは，信頼性の低いサーバになる傾向があるため，SSL サーバ証明書を基にした特徴を検知に用いる．さらに，より正確な特徴を取得するために，悪性アプリは悪性の動作に関連する権限を必ず要求することから，アプリが要求する権限を基にした重みを導入する．実データを用いた特性評価により，提案方式は 92.7% の正解率を達成でき，暗号化されたパケットおよび従来方式が検知できない 89 個の悪性アプリに対応可能であることを示した．

(3) トラヒックにおいて，長いパターンの特徴ベクトルを強調してボットネットの検出能力を高める方式

ボットネットを検出する方法として，通信シーケンスを用いる方法が有望視されている．なぜなら，通信シーケンスはプログラムによって制御されるため，通信シーケンスでは特別な長いパターンを生じやすいという特徴を有するからである．これまで，通信シーケンスを n-gram によって短く分割してトークン化し，トークン化したパターンの出現数を特徴ベクトルとして利用する方式が提案されている．しかしながら，従来法では，特徴ベクトルを，n の値に関係なく，すべてのパターンの出現回数の合計値によって正規化するため，n が大きい場合の出現回数は n が小さい場合の出現回数より少なくなり，結果として，正規化された長いパターンの特徴ベクトルは非常に小さな値となる．この欠点を克服するために，本論文では，トラヒックにおいて，長いパターンの特徴ベクトルを強調してボットネットの検出能力を高める方式を提案した． １つ目のアイデアとして，すべてのパターンの出現回数の合計値ではなく，各 n の出現回数の合計値でそれぞれ正規化することを提案し，特徴ベクトルのバランスをよりとれるようにする．２つ目のアイデアとして，各 n において特徴ベクトルのランク付けを行い，ランクに従って特徴を重み付けすることにより，より長いパターンがより強調されるようにする．実際のデータセットを用いて，コンピュータシミュレーションにより特性評価を行った結果，提案方式は，従来法に比べて，ボットネット検出をより有効に検出できることを示した．

(4) 色相を利用して自動的に検知範囲を拡大可能なフィッシングサイト検知法

増加し続けるフィッシングサイト（PWS: Phishing Website）の亜種を検知するために，検知範囲を拡大することは，重要な課題である．この課題に対処するため，本論文では，色相を利用して自動的に検知範囲を拡大可能なフィッシングサイト検知法を提案した．PWS は標的サイトおよび他の亜種を元に作られ，それらの間では類似した色相が用いられるため，色相の類似する亜種を追跡することで多くの亜種を網羅的に検知できると考えられる．この考えに基づき，提案方式は，データベースに登録されている検知済み PWS と似た色相を持つサイトを登録済みの PWS の亜種として検知し，データベースに追加することで，検知範囲を拡大する．また，既知の PWS の色相と類似した色相を持つ正規サイトが誤検知されるのを抑制するため，色相情報の中でも使用される色の組み合わせが正規サイトと PWS の間で異なることを利用する．シミュレーションにより，提案方式は，検知された PWS の増加に伴い検知性能を向上させることが可能であることを示した．

(5) 宛先までのホップ数解析による Traceroute を用いた検知手法

近年，新種の DDoS 攻撃である Target Link Flooding Attack の検知が急務である．この

攻撃は，特定のリンクを輻輳させることで標的のネットワークをインターネットから孤立させることが可能である．また，標的が直接攻撃されているわけではないため，従来のDDoS 攻撃への対策が講じにくいという特徴がある．Target Link Flooding Attack への対策として，攻撃の予兆を検知することができる Traceroute を用いた手法が注目されている．この方式は，Traceroute の急激な増加を観測した場合には攻撃を検知できるが，攻撃者が Traceroute の送信レートを下げた場合には，検知不可能である．そこで，本論文では，宛先までのホップ数解析による Traceroute を用いた検知手法を提案した.正規の Traceroute が分散するのに対し，攻撃者の Traceroute は特定のホップ数内に集中するということに着目し，Traceroute をホップ数毎に分けることにより，変化が強調され，従来では捉えることができなかった攻撃を検知することが可能になる．コンピュータシミュレーションにより，提案手法が従来手法よりも優れていることを示した．

(6) 良性と悪性の特徴出現の比率と比率差を考慮した Android におけるＩＣＣに着目したマルウエア検出法

近年，Android の悪性アプリが横行している．多くの検知方式が存在する中，Inter-Component Communication (ICC)に着目した方式が注目されている．この方式では，Correlation-based Feature Selection (CFS)により特徴を選択してから機械学習を行うが，CFS は相互特徴間で相関の強い特徴を除くため，検知に有用な特徴まで除去しうるという問題が存在する．本論文では，これに対応するため，特徴の良性と悪性での出現率の比率に基づいて，一方に頻出する有用な特徴を選択し，さらに，比率だけでは適切な特徴選択が不可能な場合もあるため，出現率の差も用いることで対応する方式を提案し，実データセットを用いたシミュレーションにより，提案方式の有効性を示した．

(7) 車々間通信における通信範囲の重複を用いた偽装車両密度情報の検知手法

車々間通信において，隣接車両から送信される偽装情報を検知することは重要である．従来手法は偽造情報を周辺の車両密度を用いて検知しているが，周辺車両から受信した車両密度を正しく検証することができない．本論文では，車々間通信における通信範囲の重複を用いた偽装車両密度情報の検知手法を提案した．車両は隣接車両周辺の車両数を受信した車両密度を用いて計算することができるため，自身の通信範囲外に多くの車両が存在する場合，受信した車両密度が嘘であると検知できる．コンピュータシミュレーションによって，提案手法が従来手法の検知率を向上できることを示した．

(8) 大学図書館における IoT デバイスを活用した利用状況把握の取り組みに関する研究

大学図書館では，貸出ログや入館ログといった利用データを用いて，図書館利用者の行動やニーズを分析し，サービス改善に繋げることは従来までも行われてきたが，それらのデータからでは，施設の空席情報や滞在時間，館内での利用者の行動など，可視化できていない部分も多い．本論文では，種々の IoT (Internet of Things) デバイスを用いて，慶應義塾大学理工学メディアセンター(図書館)における利用状況把握の実証実験を行い，利用者の資料探索行動に焦点を当て，BLE (Bluetooth Low Energy) ビーコンと専用スマートフォンを活用した資料探索時の行動，移動軌跡を推定する手法について検討した．また、MAC アドレスがランダム化されていたとしても，Probe request のメッセージヘッダ内の特徴が変化しないことに着目し，MAC アドレスがランダム化された Wi-Fi 無線端末の，同定のための非匿名化手法を提案した．なお．これまで，MAC アドレスのランダム化された正解ラベル付きのデータセットは存在していないため，慶應義塾大学理工学部メディアセンター利用者の協力を得て，21 台分のスマートフォンをモニタと近接させることで，同一端末からのメッセージを受信し，ラベル付けすることでデータセットを構築した． このデータセットに教師あり学習手法の Random Forest を用いて，重要度の高い特徴量の分析および識別精度を評価した．

(9) NDN において，ユーザのコンテンツ取得傾向に基づく信頼値により攻撃者の行動を制限する方式

NDN (Named Data Networking)において，ユーザのコンテンツ取得傾向に基づく信頼値により攻撃者の行動を制限する方式を提案した．提案方式は，ルータでコンテンツの正当性を認証する方式において懸念される verification attack の対策手法である．verification attack 下では，攻撃者はルータに未認証コンテンツを大量に要求し，そのコンテンツがルータのキャッシュに挿入された後，すぐにそれらのコンテンツを要求することで，ルータの認証を集中させる．攻撃者が 1 回目の要求の際に，大量に未認証コンテンツを要求することに着目し，ルータのキャッシュに存在しないコンテンツへのアクセス間隔が極端に短くなった場合，攻撃が発生したと判断し，全ユーザの要求を一時的に制限する．しかし，この場合，攻撃者の特定が不可能であり，正規

ユーザの要求にも制限がかかる．そこで，本論文では，正規ユーザがキャッシュにある複数の未認証コンテンツを短時間で大量に要求することは稀であるのに対して，攻撃者はそれらを連続して大量に要求することに着目し，キャッシュ内の未認証コンテンツを，連続して大量に要求するユーザの信頼値のみを下げることで，攻撃者を特定し，攻撃者の要求にのみ制限をかけることが可能となる方式を提案した．特性評価の結果，提案手法は，verification attack を未然に検知し，攻撃者の特定および攻撃者の要求のみを制限することが可能であることを示した．

(10)遅延耐性ネットワークにおける通信　履歴を用いた効率的なフラッディング攻撃緩和手法

遅延耐性ネットワーク（DTN: Delay Tolerant Networks）は，エンドツーエンドの接続を必要としない次世代型通信プロトコルとして注目を集めている．しかしながら，DTN 上においてフラッディング攻撃が行われた場合，DTN の通信特性により攻撃の発見が遅れ，被害がより増大する．本論文では，通信履歴を用いて，効率的に DTN におけるフラッディング攻撃を緩和する手法を提案した．通信ノード同士の理論的接触確率を用いることで，低電力で攻撃を緩和することが可能となる．計算機シミュレーションにより，従来法に比べて，攻撃検知精度を保ちつつ，25%の省電力化を達成できることを示した．

(11)受信信号強度と位相と RF タグの読み取り回数を特徴量とした機械学習を用いたディープショッピングデータの取得方法

商用 RF タグとリーダ及びアンテナを用い，受信信号強度と位相と RF タグの読み取り回数を特徴量とした機械学習を用いたディープショッピングデータの取得方法を提案した．機械学習と読み取り回数と位相を特徴量に用いることで，受信信号強度の変動量がより正確に検知が可能となり特性改善が図れることを，実験によって示した．

５．主な発表論文等

〔雑誌論文〕　計8件（うち査読付論文　7件／うち国際共著　1件／うちオープンアクセス　0件）

１．著者名 豊田健太郎，五十嵐由美子，今井星香，笹瀬巌	４．巻 69巻3号
２．論文標題 大学図書館におけるIoTデバイスを活用した利用状況把握の取り組み	５．発行年 2019年
３．雑誌名 情報の科学と技術	６．最初と最後の頁 117～120
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 無
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Kyohei Osuge, Hiroya Kato, Shuichiro Haruta and Iwao Sasase	４．巻 E102-D, No.6
２．論文標題 An effective feature selection scheme for Android ICC-based malware detection using the gap of the appearance ratio	５．発行年 2019年
３．雑誌名 IEICE Trans. on Communications	６．最初と最後の頁 1136～1144
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2018EDP7301	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Masashi Yoshida, Hiromu Asahina, Shuichiro Haruta and Iwao Sasase,	４．巻 Vol.8, No.5
２．論文標題 A false density information attack detection scheme using overlap of communication range in VANET	５．発行年 2019年
３．雑誌名 IEICE Communications Express	６．最初と最後の頁 135～140
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

１．著者名 Hiromu Asahina, Kei Sakuma, Shuichiro Haruta, Hiroya Kato and Iwao Sasase	４．巻 Vol.8, No.7
２．論文標題 Traceroute-based target link flooding attack detection scheme by analyzing hop count to the destination	５．発行年 2019年
３．雑誌名 IEICE Communications Express	６．最初と最後の頁 251～256
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Shuichiro Haruta, Hiromu Asahina, Fumitaka Yanazaki and Iwao Sasase	4．巻 E102-D, No.12
2．論文標題 Traceroute-based target link flooding attack detection scheme by analyzing hop count to the destination	5．発行年 2019年
3．雑誌名 IEICE Trans. on Information and Systems	6．最初と最後の頁 2461～2471
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transinf.2019EDP7079	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Yichen An, Shuichiro Haruta, Sanghun Choi and Iwao Sasase	4．巻 Vo.9, No.1
2．論文標題 Traffic feature-based botnet detection scheme emphasizing the importance of long patterns	5．発行年 2019年
3．雑誌名 IEICE Communications Express	6．最初と最後の頁 7～12
掲載論文のDOI（デジタルオブジェクト識別子） なし	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Hiroya Kato, Shuichiro Haruta and Iwao Sasase	4．巻 E103-D. No.2
2．論文標題 Android malware detection scheme based on level of SSL server certificate	5．発行年 2020年
3．雑誌名 IEICE Trans. on Information and Systems	6．最初と最後の頁 379～389
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transcom.2019EDP7119	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 －

1．著者名 Hiromu Asahina, Kentaroh Toyoda, P. Takis Mathiopoulos, Iwao Sasase and Hisao Yamamoto	4．巻 E103-B, No.3
2．論文標題 RPL-based tree construction scheme for target specific code dissemination in wireless sensors networks	5．発行年 2020年
3．雑誌名 IEICE Transactions on Communications	6．最初と最後の頁 190～199
掲載論文のDOI（デジタルオブジェクト識別子） 10.1587/transcom.2019EBP3066	査読の有無 有
オープンアクセス オープンアクセスではない、又はオープンアクセスが困難	国際共著 該当する

〔学会発表〕　計22件（うち招待講演　0件／うち国際学会　10件）

1．発表者名
Shinichiro Aita, Hiromu Asahina, Kentaroh Toyoda and Iwao Sasase

2．発表標題
RFID-based deep shopping data acquisition scheme with multiple feature extraction

3．学会等名
IEICE Information and Communication technology Forum 2018（国際学会）

4．発表年
2018年

1．発表者名
Kyohei Osuge, Hiroya Kato and Iwao Sasase

2．発表標題
Feature selection scheme for Android ICC-related features based on the gap of the appearance ratio

3．学会等名
IEICE Information and Communication technology Forum 2018（国際学会）

4．発表年
2018年

1．発表者名
Masashi Yoshida, Hiromu Asahina, Shuichiro Haruta and Iwao Sasase

2．発表標題
A false information attack detection scheme using density of vehicles and overlap of communication range in VANET

3．学会等名
IEICE Information and Communication technology Forum 2018（国際学会）

4．発表年
2018年

1．発表者名
Hiromu Asahina, Kentaroh Toyoda, Iwao Sasase, P. Takis Mathiopoulos and Hisao Yamamoto

2．発表標題
An efficient code dissemination tree construction algorithm using data collection tree in WSNs

3．学会等名
Workshop on Smart City based on Ambient Intelligence（国際学会）

4．発表年
2018年

１．発表者名
Hiromu Asahina, Kentaroh Toyoda, Iwao Sasase, P. Takis Mathiopoulos and Hisao Yamamoto

２．発表標題
An energy efficient target specific code dissemination scheme with forwarder selection algorithm

３．学会等名
The 2018 IEEE 29th Annual International Symposium on Personal, Indoor and Mobile Radio Communications（国際学会）

４．発表年
2018年

１．発表者名
Keisuke Arai, Shuichiro Haruta, Hiromu Asahina and Iwao Sasase

２．発表標題
Encounter record reduction scheme based on theoretical contact probability for flooding attack mitigation in DTN

３．学会等名
The 2018 24th Asia-Pacific Conference on Communications（国際学会）

４．発表年
2018年

１．発表者名
Hiromu Asahina, Kentaroh Toyoda, Iwao Sasase, P.Takis Mathiopoulos and Hisao Yamamoto

２．発表標題
An energy efficient target epecific code dissemination scheme with RPL-based forwarder selection algorithm,

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2018年

１．発表者名
Keisuke Arai, Shuichiro Haruta, Hiromu Asahina and Iwao Sasase

２．発表標題
Encounter record reduction scheme based on theoretical contact probability for flooding attack mitigation in DTN

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2018年

１．発表者名
大菅恭平，加藤広野，春田秀一郎，笹瀬巌

２．発表標題
AndroidのICCに関する特徴の出現率の差異に基づいた特徴選択方式

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2018年

１．発表者名
吉田匡志，朝比奈啓，春田秀一郎，笹瀬 巌

２．発表標題
車々間通信における通信範囲の重複を用いた 偽装車両密度情報の検知手法

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2018年

１．発表者名
豊田健太郎，五十嵐由美子，今井星香，笹瀬巌

２．発表標題
図書・雑誌検索実験から得られた大学図書館ユーザ行動調査

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2018年

１．発表者名
朝比奈啓，豊田健太郎，笹瀬巌

２．発表標題
Wi-Fiフレームデータを用いた大学図書館における滞在時間の推定手法

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2018年

１．発表者名
中野紘典，加藤広野，春田秀一郎，吉田匡志，笹瀬巌

２．発表標題
NDNにおいてユーザのコンテンツ取得傾向に基づく信頼値により攻撃者の行動を制限する方式

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2019年

１．発表者名
春田秀一郎，山崎史貴，朝比奈啓，笹瀬巌

２．発表標題
色相を利用して自動的に検知範囲を拡大可能なフィッシングサイト検知法

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2019年

１．発表者名
加藤広野，春田秀一郎，笹瀬巌

２．発表標題
SSLサーバ証明書の認証レベルに着目した悪性Androidアプリ検知手法

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2019年

１．発表者名
後藤隆星，朝比奈啓，豊田健太郎，笹瀬巌

２．発表標題
図書館内におけるBLEビーコンを用いた動線分析のための座標近似手法

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2019年

１．発表者名
古屋優希，朝比奈啓，豊田健太郎，笹瀬巌

２．発表標題
MACアドレスがランダム化されたWi-Fi無線端末の同定のための非匿名化手法の検討

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2019年

１．発表者名
Yichen An, Shuichiro Haruta, Sanghun Choi and Iwao Sasase

２．発表標題
Traffic feature-based botnet detection scheme emphasizing the importance of long patterns

３．学会等名
電子情報通信学会通信方式研究会

４．発表年
2019年

１．発表者名
Yichen An, Shuichiro Haruta, Sanghun Choi and Iwao Sasase

２．発表標題
Traffic feature-based botnet detection scheme emphasizing the importance of long patterns

３．学会等名
2019 IEICE Information and Communication Technology Forum（国際学会）

４．発表年
2019年

１．発表者名
Hironori Nakano, Hiroya Kato, Shuichiro Haruta, Masashi Yoshida and Iwao Sasase

２．発表標題
Trust-based verify- cation attack prevention scheme using tendency of contents request on NDN

３．学会等名
The 2019 25th Asia-Pacific Conference on Communications（国際学会）

４．発表年
2019年

１．発表者名
Shuichiro Haruta, Fumitaka Yamazaki, Hiromu Asahina and Iwao Sasase

２．発表標題
A novel visual similarity-based phishing detection scheme using hue information with auto updating database

３．学会等名
The 2019 25th Asia-Pacific Conference on Communications（国際学会）

４．発表年
2019年

１．発表者名
Hiroya Kato, Shuichiro Haruta and Iwao Sasase

２．発表標題
Android malware detection scheme based on level of SSL server certificate

３．学会等名
IEEE Global Communications Conference 2019（国際学会）

４．発表年
2019年

〔図書〕　計0件

〔産業財産権〕

〔その他〕
慶應義塾大学理工学部情報工学科笹瀬研究室
www.sasase.ics.keio.ac.jp

６．研究組織

	氏名 （ローマ字氏名） （研究者番号）	所属研究機関・部局・職 （機関番号）	備考