早稲田大学大学院 基幹理工学研究科

博 士 論 文 概 要

論 文 題 目

Beyond the Layers: Identifying Novel Privacy Threats for Internet Users

レイヤーを越えて：インターネットユーザに対する
未知なるプライバシー脅威の特定

申 請 者

渡邉	卓弥
Takuya	WATANABE

情報理工・情報通信専攻 ネットワークシステム研究

2019 年 12 月

スマートフォンおよびInternet of Things (IoT)の普及にともない，2018年，インターネットに接続されるデバイスの数は220億に達した．これは，インターネットを通じて世界に公開し得るユーザデータが拡大したことを意味する．デバイスに保持されるユーザデータの中には，ユーザの身元情報や位置情報，カメラの映像，音声といったプライバシー情報が含まれており，インターネットデバイスの隆盛は，利便性と引き換えにプライバシーデータが漏洩するリスクを高めているという現状がある．こうしたプライバシーリスクの深刻化を受けて，プライバシーを保護するための取り組みは世界的な潮流となった．サイバーセキュリティ分野では，サーバやクライアントのログから攻撃の痕跡を解析し，ユーザのプライバシーを保護する技術に関する研究がなされてきた．また技術的アプローチに加え，法的アプローチによるプライバシー保護のための取り組みも活発化している．米国における California Consumer Privacy Act (CCPA)や欧州における General Data Protection Regulation (GDPR) はその一例であり，我が国においても，2020年に個人情報保護法が改正され，広告や機械学習のユースケースにおいてユーザのプライバシーを保護するための条項追加が予定されている．

こうした取り組みにも関わらず，残念ながらインターネットユーザが晒されているプライバシーの脅威は激化の一途を辿っている．たとえば，攻撃者がアプリケーションのセキュリティのホール，いわゆる脆弱性を悪用する攻撃は未だ健在である．2018年に，世界最大のソーシャルネットワークサービスであるFacebookは，あるユーザに対して別のユーザのアクセストークンが付与されるバグにより，5,000万人のユーザ情報が漏洩したことを明らかにした．さらに，最新の攻撃者の行動は，もはやコンピュータシステムの内部に留まらない．サイドチャネル攻撃は，コンピュータシステムが物理空間に対して漏洩するデータを測定することにより，間接的にシステム内に保管された機密情報を推定するアプローチである．Hornらは，CPUに対するタイミング攻撃であるMeltdownおよびSpectreの2つの脆弱性によって，1995年以降のリリースされた大半のCPUにデータ漏洩の潜在的なリスクがあることを示した．また，フィッシング攻撃は，恐怖心や好奇心といった人間の心理的な弱点を悪用する．カスペルスキーが実施した調査によれば，2019年の4月から6月にかけた3ヶ月の間に約1億3,000万件のフィッシング攻撃が検出された．これらの例のように，最先端のサイバー攻撃は，コンピュータシステムの内部に留まらず，ソフトウェア，ハードウェア，人間の認知といった様々な「レイヤー」にまたがっている．ユーザのプライバシーを保護するためには，さまざまなレイヤーにおける情報漏洩の経路を特定した上で，対策のためレイヤーに応じた制御機構の追加を検討する必要がある．

この博士論文では，以下に述べる3つのコンピュータシステム外部のリソースを悪用するプライバシー脅威に着目する．

(1) 物理空間におけるサイドチャネルの悪用：スマートフォンおよびIoTデバイスには，現実世界での体験とリンクしたリッチなユーザエクスペリエンスを提供するための物理センサが備わっている．これらのセンサは，物理空間における加速度や磁場といった物理量を計測する．こうした計測データは，デバイスを所有するユーザの実空間での行動を反映しているため，ユーザのプライバシーを侵害する可能性がある．物理センサへのアクセスは，一般的にパーミッションのような機構で制限されていない．

(2) ネットワークにおけるサイドチャネルの悪用：通信回線の広帯域，高品質化が進み，ネットワーク遅延等の通信品質は主としてサーバの状態によって左右されるようになった．したがって，攻撃者はネットワーク往復遅延を監視することにより，遠隔サーバで実行されているアプリケーションの状態を推定することが可能である．さらに複数のアプリケーション状態を組み合わせることで，より詳細なユーザデータを推定できる場合がある．現状では，ランダマイゼーションなどによって処理時

間を意図的に隠匿するような対策はほとんど普及していない.

(3) ユーザ認知の悪用：ユーザは，自身の認知や期待に基づいて，コンピュータシステムにどのような操作を加えるか決定する．特に，アプリケーションの動作を説明する説明文のようなメタデータは,ユーザがアプリケーションをインストールするかどうかを判断するための有用な情報源である．一方でユーザは，ときに説明文に欺かれ,期待に反してプライバシーデータにアクセスするようなアプリケーションをインストールする．アプリマーケットでは，ユーザに適切に理解させるための説明文のガイドラインは設けられていない.

本論文の目的は，コンピュータシステム外に存在する，様々なレイヤーのリソースを悪用することで，現代のインターネットユーザに広く影響を与え得るプライバシー脅威を特定し，その対策技術を明らかにすることである． 2 章と 3 章では新しい攻撃を構築する概念的アプローチによって潜在的な脅威を示し,4 章では大規模なデータ分析によって市場において脅威がどの程度存在するかを明らかにする.

本論文の主要な貢献は，インターネットユーザのプライバシーを保護するために必要なガイドラインを示すことで，研究コミュニティと開発者に有益な知見をもたらしたことである．具体的には，センサデバイス，Web サービス，アプリマーケットを安全に設計するための方法に関する重要な指針を提供した．本論文のもう一つの貢献は，実存するサービスに対して実現可能な対策を示し，実装・運用に導いたことである．本論文で示された新しい脅威に対する対策は，世界的なサービスプロバイダやブラウザベンダとの協力を経て，実サービスを保護する技術として採用された．影響を受けるサービス・ブラウザのユーザ数は数億人にのぼり，本研究の成果によって多数のユーザのプライバシーを堅牢に保護することができた.

論文の構成を以下に示す.

1 章「Introduction」では，本研究の背景と，成果のもたらした貢献を示す.

2 章「Sensor-based user location tracking」では，ユーザの行動を収集する物理センサのデータが,ユーザの実際の位置情報を漏洩することを実証する．具体的には，スマートデバイスを携帯して鉄道で移動する人物の位置情報を追跡する新たなサイドチャネル攻撃の実現可能性を検証する．一般にモバイルアプリは GPS 等によって位置情報を取得するために，ユーザの許可を必要とする．一方，加速度，磁力，角速度等を計測するハードウェアセンサにアクセスする際は許可を必要としない．本章の狙いは，ハードウェアセンサの情報のみを用いて人物の位置を推定する脅威の実現性評価と対策技術の確立である．まず，センサデータに対し教師あり機械学習を適用することで，標的の行動を歩行中，走行車両内，その他の 3 種に分類する．次に，時系列順に並んだ行動推定の結果から，列車の出発時刻と到着時刻のシーケンスを抽出する．最後に，得られた時刻シーケンスを鉄道の時刻表と路線図に照合し，標的の移動経路を特定する．上記のシステムを実装し，ユーザ実験によって集めたセンサデータと，172 の鉄道会社，9,090 の駅を対象にシミュレーションを行った結果，本攻撃による脅威が現実的であることを示し，有効な対策について検討した.

3 章「Web side-channel attack to identify social account of a visitor」では，ユーザと Web サーバ間のネットワーク通信の所要時間を攻撃者が観察した際に，ユーザの ID が漏洩する脅威を評価する．脅威モデルは，攻撃者のウェブサイトに訪問したユーザのソーシャルアカウントを特定することである．攻撃の骨子となるのは，ソーシャルウェブサービスにおいて，各ユーザが閲覧できるコンテンツを制御するユーザブロックの特性を悪用することである．攻撃者は事前にアカウントを用意し，サービス上のユーザに対してブロック/非ブロックの状態を任意に設定できる．これを複数組み合わせることで一意のビット列を形成し，大量のユーザに割り当てる．その後ウェブサイトに訪問したユーザに対して，タイミング攻撃によって各アカウントからブロックされているか否かを推定し，ビット列を復元してソーシャルアカウントと紐付け

る．検証の結果，SNS，ゲーム，オークションなど著名な 12 サービスでアカウントを特定可能であることが明らかとなった．フィールド実験では，最短 4 秒程度という所要時間の下，100%の精度で攻撃が成功することを示した．最後に，実現可能な対策を紹介し，サービス事業者と連携して実現に至った対策について説明する．

4 章「Analyzing the inconsistency between behaviors and descriptions of mobile apps」では，ユーザのアプリに対する期待に反して，プライバシーデータにアクセスするアプリの解析を行う．ユーザのアプリに対する期待を作り出す情報源としてアプリストア上で公開されたアプリの動作を記述した説明文に着目し，説明文がプライバシーデータへのアクセスについて言及していない理由を解明する．そのために，静的コード解析とテキスト分類を組み合わせたフレームワークを開発し，ACODE (Analyzing COde and DEscription)と名付けた．ACODE を用いて，大規模なアプリを対象とした実態調査を行う．テキスト分類では教師データを必要としない方法を用いるため，スケーラブルな分類を実施することができる．公式とサードパーティの Android アプリマーケットから収集した 21 万個のアプリの分析によって，説明文とプライバシーデータアクセスとの間に生じる齟齬の原因を 4 つ解明した．不要なパーミッション利用を行うアプリ自動生成サービス，類似のコードを用いて大量にアプリを公開する開発者の存在，説明文で言及されにくい副次的な機能の存在，プライバシーデータにアクセスするサードパーティのライブラリの 4 つである．これらの調査結果は，アプリ配信プラットフォームにおけるユーザ，開発者，マーケッターのプライバシー意識を向上させるために有益である．

最後に 5 章「Conclusions」では，レイヤーを越えたインターネットユーザに対するプライバシー脅威を特定するために，上記で述べた位置情報追跡攻撃の実証，ソーシャルアカウント特定攻撃の実証，および説明文とアプリの解析によって得られた成果についてまとめる．

日夜，進化を遂げる攻防の舞台はもはやサイバー空間に留まらず，物理空間や人間の認知といったさまざまなレイヤーに及んでいる．こうした状況下では，コンピュータシステムを対象とした従来の防御手段だけでユーザプライバシーの安全を保つことはもはや困難である．本研究は，レイヤーを超えた新たな攻撃を示すことで見落とされていたプライバシー漏洩チャネルに光を当てるとともに，実態調査によって攻撃の実際のインパクトを明らかにした．

今後の研究の方向性を以下に 3 つ示す．まず，本研究で提案した対策は，単一の攻撃からプライバシー情報を保護するだけの機構ではなく，その攻撃原理から派生する数多くの脅威を無力化できるという点で汎用性を有するものである．しかしながら，レイヤーをまたがった脅威は他にも潜在していると考えられ，これらすべてを特定することは現時点で容易ではない．本研究で取り扱わなかったものの，攻撃者にとって有望と考えられる物理空間情報として，光量や消費電力などが考えられる．これらを含めたより広範な攻撃経路の調査が今後の研究方向性の一つである．もう一つの方向性として，「攻撃研究の効果測定」が挙げられる．本論文で特定されたプライバシー脅威は，対策やガイドラインを示した上で詳細を外部に公開した．この活動は，攻撃者が独占的に脆弱性情報を保有している状態を防ぐことができる点において有益であるが，一方で我々が公開した情報が今後の脆弱性発見のためのヒントを与えるリスクがある．そのようなリスクを評価するには現時点では実証データが不足している．攻撃研究の発表と実際のサイバー攻撃発生の関係性を定量的に調査することを，2 つ目の今後の研究方向性とする．最後に，本論文の 2 章と 3 章で示された攻撃手法は，ウェブサービスやモバイルアプリの事業者が一定の制約下でユーザをプロファイリングできるという実用的な側面がある． 本研究の成果を発展させ，マーケティングおよびサービス機能の向上のために，ユーザの同意を得た上でプライバシーを侵害することなくユーザ属性や位置情報を推定する手法を確立することを 3 つ目の今後の研究方向性とする．

早稲田大学　博士（工学）　学位申請　研究業績書

氏 名　　渡邉 卓弥 印

（2019 年　12 月　現在）

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
査読付き論文誌	1. Takuya Watanabe, Mitsuaki Akiyama, Fumihiro Kanei, Eitaro Shioji, Yuta Takata, Bo Sun, Yuta Ishii, Toshiki Shibahara, Takeshi Yagi, and Tatsuya Mori, “Study on the Vulnerabilities of Free and Paid Mobile Apps Associated with Software Library,” IEICE Transactions on Information and Systems, vol.E103-D, no.2, to appear, February 2020. 2. Takuya Watanabe, Eitaro Shioji, Mitsuaki Akiyama, Keito Sasaoka, Takeshi Yagi, and Tatsuya Mori, “Follow Your Silhouette: Identifying the Social Account of Website Visitors through User-Blocking Side Channel,” IEICE Transactions on Information and Systems, vol.E103-D, no.2, to appear, February 2020. 3. Takuya Watanabe, Mitsuaki Akiyama, Tetsuya Sakai, Hironori Washizaki, and Tatsuya Mori, “Understanding the Inconsistency between Behaviors and Descriptions of Mobile Apps,” IEICE Transactions on Information and Systems, vol.E101-D, no.11, pp.2584- 2599, November 2018. 4. Takuya Watanabe, Mitsuaki Akiyama, and Tatsuya Mori, “Tracking the Human Mobility Using Mobile Device Sensors,” IEICE Transactions on Information and Systems, vol.E100-D, no.8, pp.1680- 1690, August 2017. 5. Bo Sun, Xiapu Luo, Mitsuaki Akiyama, Takuya Watanabe, and Tatsuya Mori, “PADetective: A Systematic Approach to Automate Detection of Promotional Attackers in Mobile App Store,” Journal of Information Processing, vol.26, pp.212-223, January 2018. 6. Yuta Ishii, Takuya Watanabe, Mitsuaki Akiyama, and Tatsuya Mori, “APList of Research Achievements Praiser: A Large Scale Analysis of Android Clone App,” IEICE Transactions on Information and Systems, vol.E100-D, no.8, pp.1703- 1713, August 2017.
査読付き国際会議	1. Takuya Watanabe, Eitaro Shioji, Mitsuaki Akiyama, and Tatsuya Mori, “Melting Pot of Origins: Compromising the Intermediary Web Services that Rehost Websites,” Proceedings of the Network and Distributed System Security Symposium (NDSS 2020), to appear, February 2020. 2. Takuya Watanabe, Eitaro Shioji, Mitsuaki Akiyama, Keito Sasaoka, Takeshi Yagi, and Tatsuya Mori, “User Blocking Considered Harmful? An Attacker-controllable Side Channel to Identify Social Accounts,” Proceedings of IEEE European Symposium on Security and Privacy (EuroS&P 2018), pp.323- 337, April 2018. 3. Takuya Watanabe, Mitsuaki Akiyama, Fumihiro Kanei, Eitaro Shioji, Yuta Takata, Bo Sun, Yuta Ishii, Toshiki Shibahara, Takeshi Yagi, and Tatsuya Mori, “Understanding the Origins of Mobile App Vulnerabilities: A Largescale Measurement Study of Free and Paid Apps,” Proceedings of International Conference on Mining Software Repositories (MSR 2017), pp.14- 24, May 2017. 4. Takuya Watanabe, Mitsuaki Akiyama, and Tatsuya Mori, “RouteDetector: Sensor-based Positioning System That Exploits Spatio-Temporal Regularity of Human Mobility,” Proceedings of USENIX Workshop on Offensive Technologies (WOOT 15), pp.1- 11, August 2015.

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
	5. Takuya Watanabe, Mitsuaki Akiyama, Tetsuya Sakai, Hironori Washizaki, and Tatsuya Mori, “Understanding the Inconsistencies between Text Descriptions and the Use of Privacy-sensitive Resources of Mobile Apps,” Proceedings of Symposium On Usable Privacy and Security (SOUPS 2015), pp.241- 255, July 2015. 6. Ayako Akiyama Hasegawa, Takuya Watanabe, Eitaro Shioji, and Mitsuaki Akiyama, “I Know What You Did Last Login: Inconsistent Messages Tell ExistenceofaTarget’s Account to Insiders,”Proceedings of Annual Computer Security Applications Conference (ACSAC 2019), to appear, December 2019. 7. Asuka Nakajima, Takuya Watanabe, Eitaro Shioji, Mitsuaki Akiyama, and 136 MaverickWoo, “APilotStudyonConsumerIoTDeviceVulnerabilityDisclosure and Patch Release in Japan and the United States,” Proceedings of ACM ASIA Conference on Information, Computer and Communications Security (ASIACCS 2019), pp.485- 492, July 2019. 8. Keika Mori, Takuya Watanabe, Yunao Zhou, Ayako Hasegawa, Mitsuaki Akiyama, and Tatsuya Mori, “Comparative Analysis of Three Language Spheres: Are Linguistic and Cultural Differences Reflected in Password Selection Habits?,” Proceedings of Proceedings of the 4th IEEE European Workshop on Usable Security (EuroUSEC 2019), pp.159- 171, June 2019. 9. Tatsuhiko Yasumatsu, Takuya Watanabe, FumihiroKanei, EitaroShioji, Mitsuaki Akiyama, and Tatsuya Mori, “Understanding the Responsiveness of Mobile App Developers to Software Library Updates,” Proceedings of ACM Conference on Data and Application Security and Privacy (CODASPY2019), pp.13- 24, March 2019. 10. Yuta Ishii, Takuya Watanabe, Fumihiro Kanei, Yuta Takata, Eitaro Shioji, Mitsuaki Akiyama, Takeshi Yagi, Bo Sun,and Tatsuya Mori„ “Understanding the Security Management of Global Third-Party Android Marketplaces,” Proceedings of International Workshop on App Market Analytics (WAMA 2017), pp.12- 18, September 2017. 11. Bo Sun, Xiapu Luo, Mitsuaki Akiyama, Takuya Watanabe, and Tatsuya Mori , “Characterizing Promotional Attacks in Mobile App Store,” Proceedings of International Conference on Applications and Techniques in Information Security (ATIS2017), pp.113- 127, July 2017, **Best Paper Award**. 12. Yuta Ishii, Takuya Watanabe, Mitsuaki Akiyama, and Tatsuya Mori„ “Clone or Relative?: Understanding the Origins of Similar Android Apps,” Proceedings of ACM International Workshop on Security And Privacy Analytics (IWSPA 2016), pp.25- 32, March 2016.
ポスター	1. Takuya Watanabe and Tatsuya Mori, “Understanding the Consistency Between Words and Actions for Android Apps,” ACM ASIA Conference on Information, Computer and Communications Security (ASIACCS 2014), Poster Session, June 2014, **Best Poster Award**. 2. Atsuko Natatsuka, Ryo Iijima, Takuya Watanabe, Mitsuaki Akiyama, Tetsuya Sakai,and Tatsuya Mori, “A First Look at the Privacy Risks of VoiceAssistant Apps,” ACM Conference on Computer and Communications Security (CCS 2019), Poster Session, November 2019.

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
	3. Bo Sun, Takuya Watanabe, Mitsuaki Akiyama, and Tatsuya Mori, “Seeing is Believing? The Analysis of Unusual Ratings and Reviews on Android App Store,” International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2015), Poster Session, November 2015. 4. Yuta Ishii, Takuya Watanabe, Mitsuaki Akiyama, and Tatsuya Mori, “Understanding the Origins of Similar Android Apps,” International Symposium on Research in Attacks, Intrusions and Defenses (RAID 2015), Poster Session, November 2015.
口頭発表	1. Takuya Watanabe, “[Invited Talk] トップカンファレンス採録への道 ,” セキュリティサマーサミット 2019, July 2019. 2. Takuya Watanabe, “[Refereed Talk] I Block You Because I Love You: Social Account Identification Attack Against a Website Visitor,” Black Hat Europe, December 2018. 3. Takuya Watanabe, “[Invited Talk] Silhouette: Controlling Side Channel to Identify Social Account of Website Visitor,” International Workshop on Security (IWSEC 2018), September 2018. 4. Takuya Watanabe, “[InvitedTalk]Understanding the Inconsistencies between Text Descriptions and the Use of Privacy-sensitive Resources of Mobile Apps,” Workshop on Psychological Factors of Cybersecurity, April 2017. 5. Takuya Watanabe, “[Invited Talk] ACODE: Analyzing the Inconsistencies between User Expectations and the Developer Intentions of Mobile Apps,” International Workshop on Security (IWSEC 2015) , August 2015.
その他	1. 渡邉卓弥 , “ 新たなプライバシ脅威「 Silhouette 」の発見と対策への取り組み ,” NTT 技術ジャーナル Vol. 31 No. 2, pp.15-18, February 2019. 2. Takuya Watanabe, “Discovery of Silhouette- a New Threat to Privacy- and Our Efforts to Counter It,” NTT Technical Review, Vol. 17 No. 3, pp.11-15, March 2019. 3. 渡邉卓弥, 塩治榮太朗, 秋山満昭, 笹岡京斗, 八木毅, 森達哉 , “ ユーザブロック機能の光と陰 : ソーシャルアカウントを特定するサイドチャネルの 構成 ,” コンピュータセキュリティシンポジウム 2017 論文集 , pp.858- 865, October 2017, **情報処理学会 CSS 最優秀論文賞 , 山下記念研究賞** . 4. 渡邉卓弥, 秋山満昭, 森達哉 , “RouteDetector: 9 軸センサ情報を用いた位置情報追跡攻撃 ,” コンピュータセキュリティシンポジウム 2015 論文集 , pp.1127-1134, October 2015, **情報処理学会 PWS 優秀論文賞** . 5. 渡邉卓弥, 秋山満昭, 森達哉 , “Android アプリの説明文とプライバシー情報アクセスの相関分析 ,” コンピュータセキュリティシンポジウム 2014 論 文集 , pp.590 - 597, October 2014, **情報処理学会 CSS 学生論文賞 , MWS 学生論文賞** . 6. 渡邉卓弥, 森達哉, 酒井哲也 , “ カメラを秘密裏に濫用する Android アプリの検出 ,” 電子情報通信学会技術研究報告 (信学技報) Vol. 113 No. 502, pp.119124, March 2014.

早稲田大学　博士（工学）　学位申請　研究業績書

種 類 別	題名、　発表・発行掲載誌名、　発表・発行年月、　連名者（申請者含む）
	7. 刀塚敦子，飯島涼，渡邉卓弥，秋山満昭，酒井哲也，森達哉，“Voice Assistant アプリの大規模実態調査，” コンピュータセキュリティシンポジウム 2019 論文集，pp.618- 625, October 2019, **情報処理学会 CSS 最優秀論文賞**． 8. 櫻井悠次，渡邉卓弥，奥田哲矢，秋山満昭，森達哉，“ サーバ証明書解析によるフィッシングサイトの発見手法，” コンピュータセキュリティシンポジウ ム 2019 論文集，pp.910- 917, October 2019, **情報処理学会 CSS 学生論文賞**． 9. 森啓華，長谷川 彩子，渡邉卓弥，笹崎寿貴，秋山満昭，森達哉，“ パスワード生成アシスト技術の有効性評価 ： 異なる言語圏のユーザを対象とした追試研究，” コンピュータセキュリティシンポジウム 2019 論文集，pp.214- 221, October 2019, **情報処理学会 UWS 論文賞**． 10. 長谷川彩子，渡邉卓弥，塩治榮太朗，秋山満昭，“ ログイン関連画面に潜む脅威：センシティブサービスにおけるアカウント所有の特定，” コンピュータセキュリティシンポジウム 2019 論文集，pp.704- 711, October 2019. 11. 高田雄太，渡邉卓弥，中野弘樹，波戸邦夫，秋山満昭，“Web プッシュ通知の悪用に関する実態調査，” 研究報告コンピュータセキュリティ (CSEC) Vol. 2018 No. 17, pp.1- 8, December 2018, **情報処理学会 CSEC 優秀研究賞**． 12. 櫻井悠次，奥田哲矢，秋山満昭，渡邉卓弥，高田雄太，須賀祐治，森達哉，“Web サイトのセキュリティ・センサス，” コンピュータセキュリティシンポジウム 2018 論文集, pp.77- 84, October 2018. 13. 安松達彦, 金井文宏, 渡邉卓弥, 塩治榮太朗, 秋山満昭, 森達哉，“ モバイルアプリ開発者による脆弱性対応の実態調査，” コンピュータセキュリティシンポジウム 2017 論文集，pp.644- 651, October 2017, **情報処理学会 MWS 学生論文賞**． 14. 石井悠太, 渡邉卓弥, 秋山満昭, 森達哉，“Android クローンアプリの大規模分析，” コンピュータセキュリティシンポジウム 2015 論文集，pp.207- 214, October 2015, **情報処理学会 MWS 学生論文賞**． 15. 孫博, 渡邉卓弥, 秋山満昭, 森達哉，“Android アプリストアにおける不自然なレーティング・レビューの解析，” コンピュータセキュリティシンポジウム 2015 論文集，pp.655- 662, October 2015. 16. 石井悠太, 渡邉卓弥, 秋山満昭, 森達哉，“ 正規アプリに類似した Android アプリの実態解明，” 研究報告コンピュータセキュリティ (CSEC) Vol. 2014 No. 94, pp.187- 192, March 2015, **電子情報通信学会 情報通信システムセキュリティ研究賞**