早稲田大学大学院 基幹理工学研究科

博士論文審査報告書

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

2020 年 2 月

今日インターネット上で提供されるサービスは百花繚乱である。これらの様々なサービスを活用する際に、個々のユーザのプライバシーを保護する手段の確立は、きわめて重要な問題である。プライバシーを保護するための法制度として、国内では「個人情報の保護に関する法律」（通称、「個人情報保護法」）の改正が進められている。欧州では「EU 一般データ保護規則」（GDPR）が 2018 年 5 月に施行され、米国カリフォルニア州では「カリフォルニア消費者プライバシー法」（CCPA）が 2020 年 1 月に施行された。これらは消費者のプライバシー情報を扱う事業者に対する法的規制を定めたものであり、一定の効果をあげることが期待されている。

消費者のプライバシー保護に関する法制度の整備が進む一方で、技術的な面に目を向けると、システムが具備するアクセス制御機能によって保護しているはずのプライバシー情報が、思わぬ脆弱性とそれを狙う攻撃により、漏洩してしまうリスクが存在する。例えば個人情報データをオペレーティング・システムの機能を用いて保護している場合に、CPU アーキテクチャに固有な脆弱性を狙ったタイミング攻撃（例えば Spectre や Meltdown など）を適用することにより、データが第三者に漏洩し得る脅威が知られている。このように、事業者が法制度を遵守したとしても、技術的にはプライバシー保護が万全ではない状況が遍在している。

本論文では、上述したタイミング攻撃の事例のように、本来プライバシー保護メカニズムが動作することを期待している構成要素とは独立した、別の要素から情報が漏洩するリスクを称して、「**レイヤーを越えたプライバシー脅威**」と表現している。これはソフトウェアを用いて保護している情報が人間に対するソーシャルエンジニアリングを介して漏洩するようなケース、あるいはウェブブラウザのセキュリティメカニズムで保護している情報がネットワーク層での往復遅延計測を介して漏洩するようなケースなどを含んでおり、概念としては広範な対象を指し示すものである。

以上の背景に基づき、本論文では**レイヤーを越えたプライバシー脅威**の具体的な事例として、(1)スマートフォンに搭載されたセンサーによって計測される加速度や磁場等の物理量から個人の位置情報を推定する問題、(2)インターネットにおけるクライアント・サーバ通信における往復遅延の計測値から、訪問者のソーシャルメディアアカウント情報を推定する問題、および(3)モバイルアプリがアクセスするプライバシー情報が、ユーザ向け説明文書に含まれているか否かを判断する問題に取り組む。(1)は物理層のデータを、(2)はネットワーク層のデータを、そして(3)はアプリケーション層で提供される自然言語データを対象とし、それぞれがプライバシー情報とどのように相関を持ち、データ漏えいのリスクにつながるかを実験的アプローチにより明らかにしている。また、(1)と(2)は潜在的なリスク評価と対策技術の提案を目的としているのに対し、(3)は現在のモバイルアプリマーケットにおける実態調査と対策方法の確立を目的としている。

本論文は 5 章から構成される。以下では各章の概要を述べ、それぞれに評価を加える。

第 1 章「Introduction」では、本研究の背景と目的、ならびに以降の章構成に沿って、成果の概要を示している。

第 2 章「Sensor-based user location tracking」では、スマートフォン等のモバイル端末

を対象とし、端末で動作するアプリケーションが計測可能な物理量（加速度、磁気強度、角速度）から、端末所有者の位置情報を秘密裏に推定する攻撃のリスク評価に取り組んでいる。主要なアイディアは列車等の公共交通機関の乗降状態をセンサー読み取り値から機械学習によって推定し、得られた乗降状態を時刻表、路線図と突合することにより、端末所有者の移動経路を推定することである。ユーザ実験により、リスクが現実的であること、および本質的な対策としてセンサー読み取り粒度の制限の必要性を明らかにしている。

第 3 章「Web-channel attack to identify social account of a visitor」では、ブラウザ上で動作するスクリプトを用いてネットワーク上の往復遅延情報を解析することにより、ウェブサイトを訪問した人物が持つソーシャルウェブサービスのアカウント情報が推定されてしまうプライバシー脅威を評価している。鍵となるアイディアはソーシャルウェブサービス上のユーザブロック機能を利用することにより、対象となるユーザに対して外部から付与可能な一意の ID を割り当て可能であること、およびブロック状態を往復遅延計測によって推定することにある。実験の結果、現在インターネット上で広く利用されている 12 のソーシャルウェブサービスでアカウント推定が可能であることを示した。さらにこれらのサービス事業者と連携し、実サービスにおいて有効な対策方法の実装と運用を実現したことを報告している。

第 4 章「Analyzing the inconsistency between behaviors and descriptions of mobile apps」では、モバイルアプリケーションがアクセスするプライバシーセンシティブなデータ（例えば電話帳や位置情報など）と、開発者が当該アプリケーションの動作を説明した文書の齟齬に着目した研究をしている。すなわち、説明文書にはアプリケーションがアクセスするプライバシーデータに関する記述があることを期待するが、実際にはそうなっていないケースがある。本論文では 20 万に及ぶ大規模なアプリケーションと説明文書の分析により、そうした齟齬が多々あること、およびその要因分析結果を報告している。また、アプリケーション開発者、サードパーティライブラリ開発者、モバイルアプリマーケット運用者等のステークホルダーに対し、そのような齟齬に基づくプライバシー脅威を抑制するためのガイドラインを提示している。

第 5 章「Conclusion」では、本論文を総括し、将来的な研究課題を提示している。

以上を要するに、本論文はシステムに内在する様々なサイドチャネルを通じたプライバシー情報の漏洩を「レイヤーを越えたプライバシー脅威」として定式化し、具体的な対象として物理層、ネットワーク層、そしてアプリケーション層におけるデータ漏えい攻撃の問題に取り組んだ。それぞれのテーマにおいてリスクを低減するための有効な対策方法を開発した。提案した対策方法の一部は巨大 IT 企業が提供する自社サービスに適用され、広く実用に供している。本論文が開拓した研究テーマは将来のサービスにおけるプライバシー脅威を低減するための礎となるものであり、学術・産業の発展に寄与するところが大である。よって、本論文は博士（工学）早稲田大学の学位論文として価値あるものと認める。

2020 年 2 月

審査委員

主査	早稲田大学教授	博士（情報科学）（早稲田大学）	森　達哉
	早稲田大学教授	博士（情報科学）（早稲田大学）	鷲崎　弘宜
	早稲田大学教授	博士（工学）（北海道大学）	内田　真人
	横浜国立大学准教授	博士（工学）（横浜国立大学）	吉岡　克成