慶應 SFC 学会（A）研究成果発表（学会発表）

慶應義塾大学　環境情報学部四年　赤間滉星
慶應義塾大学大学院　政策・メディア研究科修士課程一年　牧野青希

1　発表概要

我々は、イタリア・トレントで開催された国際会議　第２８回 ACM SACMAT に参加し、ポスター発表を行った。以下の表に発表の概要を示す。

名前	内容
タイトル	Poster: Non-repudiable Secure Logging System for the Web.
発表形式	ポスター発表
学会	Proceedings of the 28th ACM Symposium on Access Control Models and Technologies. 2023.
参加期間	2023 年 6 月 7 日〜6 月 9 日 (CEST)
原稿の URL	https://dl.acm.org/doi/abs/10.1145/3589608.3595080

2　研究概要

Web サービスを提供するサービサーとそのユーザの間での紛争を解決するためには、一方による「事実の否認」または「虚偽の主張」を退けられる、「否認不能な証拠」が重要である。

「否認不能な証拠」が重要となるケースの例として、チャージバック詐欺（ユーザによる契約の否認）、架空請求（サービサーによる架空の主張）などが挙げられる。そのような紛争では、注文や請求の「否認不能な証拠」が存在することで、不正を働いたユーザまたはサービサーの主張を退けることができる。

我々の研究では、Web サービスにおいて「否認不能な証拠」を生み出すために Web リクエスト・レスポンスを TEE (Trusted Execution Environment) でセキュアに記録する、ロギングシステムを提案する。

ロガーは、既存の Web サービスに対して小さな変更で適用でき、またユーザ側の環境は一切の変更なしに使用できる。

他にも、安全なログを生成するための技術的な課題が３つ存在する。まず、先行研究では Web 特有の多様な通信経路を想定しきれていない。Web ではサービス自身が保有しない外部リソースを頻繁に取得するが、サービサーがここに悪意のあるデータを挿入する恐れがある。

このため、レスポンスを返却する前に Web コンテンツを改変することで、外部リソースのアクセスにロガーを経由させる工夫を施した。

次に、サービスの管理するユーザ認証（ログイン）機能では、サービスがデータベース内の認証情報を悪用してユーザになりすますおそれがある。提案手法では、ロガーが認証機能を提供することで、このなりすましの脅威を防ぐ。

最後に、提案手法のロガーが適切に設定されていることを、ユーザが簡単に確認できる必要がある。本来これには専用のソフトウェアを用いてロガーの情報を検証する必要があるが、ユーザ全員にこのソフトウェアの使用を強制するのは非現実的である。そこで、第三者によって事前に検証されたロガーに対し特別なドメイン名を与えることで、ブラウザ画面を目視するのみでの簡単な確認を可能にした。

3　発表成果

発表を行なった国際学会は、情報技術におけるアクセスコントロール、認可をテーマとしている。このため、ポスター発表中の参加者との議論では認可に関するコメント・質問が多くあった。特にユーザ認証機能については、専門家からのコメントを受けて認可に関する考慮が不足していることがわかった。

ほかにも、問題意識には共感を得られたものの、提案手法の実現性を疑問視するコメントがあった。具体的には、特殊なハードウェア TEE の中で、我々が主張するような大規模なプログラムが動作できるのかを懸念していた。加えて、サービスへのアクセスすべてのログは膨大なデータ量となり得ることから、パフォーマンスおよび実用性の面で課題があるのではないかとの指摘を受けた。

4　今後の展望

発表者からのコメントを受け、特にアイデアの実現性を示すための実装物が必要である。このため今後の展望として、提案手法に含まれる 2 つのエンティティ「Logger」「Trusted Third Party」、および提案手法の適用先となるサービスのサンプルを実装する。また、そのプログラムを TEE 上で動作させ、パフォーマンスの面で実用に耐えうるかを試験・評価する。

評価の結果十分な実用性があると判断できれば、その成果および全体の貢献をまとめて学会発表することを見据えている。

5　研究成果の活用

提案した手法は、一般の Web サービスで活用することができる。必要なハードウェア TEE はパブリッククラウドサービスによってもサポートされているため、サービスの運用者はすぐに使用を開始できる。

提案手法を適用したサービスは安全なログを取得できるため、悪意あるユーザの虚偽の主張を退けることができ、チャージバック詐欺等の紛争の解決が容易になる。またユーザ視点でも、ロガーが適用されたサービスはドメイン名から簡単に判別できるため、安心してサービスを利用できる。