松浦研究室

暗号と情報セキュリティ

情報・エレクトロニクス系部門

情報理工学系研究科 電子情報学専攻
http://kmlab.iis.u-tokyo.ac.jp/

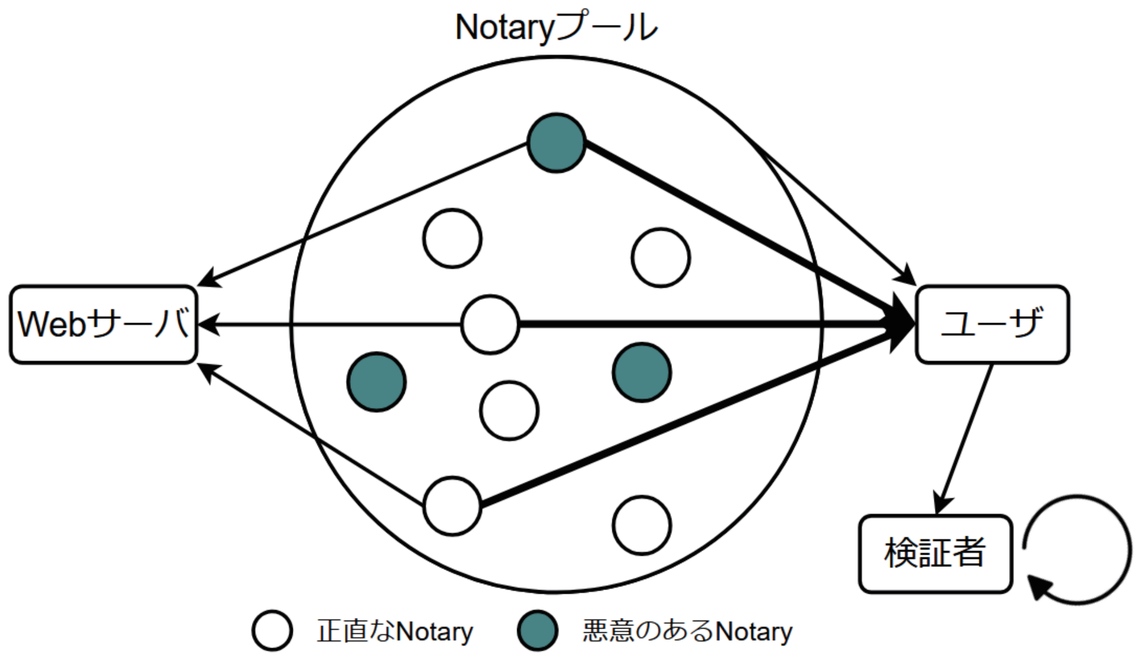
誰もが不安なく情報をやり取りできる社会システム構築への技術的貢献を目標とし、
暗号技術、情報セキュリティ、ネットワークプロトコルといった基盤技術、その技術革新、
実用時の問題などの研究に取り組んでいます。

Webの情報を「信頼できる証明」に
～Web通信をVCとして保存・提示し、分散Notary＋報酬設計で改ざん耐性を向上～

経費精算や証明手続きでは、Web画面のスクリーンショット提出が求められることがあります。しかしスクショは加工が容易で、受け取る側が「本当にそのWebサイトから得た情報か」を機械的に確認しにくいのが現状の課題です。Webサービスが最初から来歴証明を提供していない場合も多く、受け手側で“来歴”を示す仕組みが必要になります。そこで本研究では、Webで見た情報をスクリーンショットではなく、あとから第三者が機械的に確かめられる「信頼できる証明」として残し、必要なときに提示できる仕組みを研究しています。

新しい仕組みを詳しく解説

提案手法では、公証役（Notary）がユーザとWebサーバの間でTLS通信を中継し、中身を見ずに通信記録へ署名して「取得後に改ざんされていない」ことを担保します。署名つき記録は“検証可能な証明書（VC）”として保存・提示でき、サーバ改修も不要です。さらに単一Notaryへの依存を避けるため複数Notaryで署名し、担保や違反時の没収など“ズルが割に合わない”設計により、同じ安心感をより少ない人数・コストで実現できる可能性を示します。



この研究がどう活きるか

カード明細による立替精算、大学サイトの在籍確認、銀行残高の提示などで、スクリーンショットの代わりに“検証可能な証明”を提出できるようになります。提出先は証明に付いた署名を手がかりに、取得元や改ざんの有無を機械的に確認でき、こうした形式が広がることで確認手順の標準化や自動化につながることが期待されます。