先端科学技術研究科　修士論文要旨

所属研究室 (主指導教員)	サイバーレジリエンス構成学 (門林　雄基 (教授))		
学籍番号	2311062	提出日	令和 7年 1月 20日
学生氏名	大岡　冬偉		
論文題目	安全な自動組織認証に向けた期限付き VC トークンを活用する拡張 ACME プロトコル		

要旨

公開鍵基盤では認証局 (CA) が Web サーバに対して TLS サーバ証明書を発行し, インターネット上での安全な通信を実現している. Web ブラウザは TLS サーバ証明書により, 通信相手である Web サーバーを確実に識別できる. ただし, TLS サーバ証明書の有効期限切れは Web サイトの可用性を損なう問題が存在した. この問題に対処するため, ACME プロトコルが確立され, 証明書発行プロセスの自動化が実現された. 現在, 自動化できていない証明書として Organization Validation (OV) 証明書があり, OV 証明書の発行には, 組織の登記情報や法的文書の確認, 電話による実在確認など, 自動化が困難な組織認証処理が含まれる. そこで本研究では, ACME プロトコルを拡張し, Verifiable Credentials (VC) を利用した組織認証の自動化を提案する. VC は身分証明や学歴証明などのデータが信頼できる機関によって保証される検証可能な資格情報である. しかし, 一度発行された VC を使いまわして組織認証を行えば, 不正に認証を迂回される危険がある. 提案プロトコルでは, 短い有効期限の VC を組織認証開始以降に取得させることで, VC の使いまわしを制限し, 不正利用を防ぐ. また, 組織認証に用いる VC にはプライバシー性の高いデータが含まれるので, プライバシーを保護する必要がある. しかし, プライバシー保護手法を適用した VC の検証処理には DoS 攻撃脆弱性が発生する可能性がある. 評価実験により, 提案プロトコルが認証情報の悪用や無効な VC の不正利用を阻止しつつ, 有意な遅延を生じないこと, プライバシー保護手法を適用した上で DoS 攻撃に対して安全であることを示す.