セキュリティ総論 D レポート No.5

慶應義塾大学 理工学部物理学科 61908697 佐々木良輔

電子署名と電子認証

電子署名は電子データに付与されるもので, データの作成者の確認や改ざん検出などに用いられる技術である. 対して電子認証は通信において相手が本人であることを認証するために用いられる技術である. 2021 年現在において, 電子署名と電子認証は共に公開鍵認証を用いた技術である.

電子署名

上で述べた通り, 電子署名は文章などの電子データに付与されるもので, インターネットでデータを送信する際にデータの改ざん検出を行うための技術である. 電子署名は公開鍵暗号と電子証明を用いた技術であり, 電子署名による文章の改ざん検知は以下の手順で行われる.

1. 送信する文書をハッシュ化する
2. ハッシュ値を秘密鍵で暗号化する
3. 送信者は文書, 暗号文, 公開鍵, 電子証明書を送信する
4. 受信者は暗号文を公開鍵で復号し, ハッシュ値を得る
5. 上で得たハッシュ値と文章から得られたハッシュ値を比較する
6. 同時に電子証明書の有効性を確認し, 公開鍵が正当なものであることを確認する
7. 電子証明書が有効で, なおかつハッシュ値が一致したとき, 文章が正当なものであることがわかる

マイナンバー制度においては電子署名に用いる公開鍵, 秘密鍵および電子証明書が署名用電子証明書として RFID タグであるマイナンバーカードに記録されており, これを用いることで完全性を担保した通信ができる. 現在ではマイナンバー制度による電子署名で確定申告などの書類申請を行うことができる.[1]

電子認証

上で述べた通り, 電子認証は通信において相手が本人であることを確認うするために用いられる技術である. 電子認証は電子署名と同様に公開鍵暗号と電子証明を用いた技術であり, 電子認証は以下の手順で行われる.

1. 受信者が送信者に向けて任意のデータ (乱数) を送信する
2. 送信者は秘密鍵で乱数を暗号化する
3. 送信者は乱数, 暗号文, 公開鍵, 電子証明書を送信する
4. 受信者は暗号文を公開鍵で復号し, 乱数を得る
5. 上で得た乱数と送付された乱数を比較する
6. 同時に電子証明書の有効性を確認し, 公開鍵が正当なものであることを確認する
7. 電子証明書が有効で, なおかつ乱数が一致したとき, 電子認証は成功する.

このように電子認証において文章のハッシュ値を乱数とすることで電子認証を行うことができる. マイナンバー制度においては電子署名と同様に公開鍵, 秘密鍵, 及び電子証明書が利用者証明用電子証明書としてマイナンバーカードに記録されており, これを用いることで電子認証を行える. 現在ではマイナポータルへのログインなどで用いられている.

参考文献

[1] 総務省. マイナンバー制度とマイナンバーカード. https://www.soumu.go.jp/kojinbango_card/03.html. (Accessed on 12/29/2021).