プロローグ

パスワード認証を例に…
暗号なしの場合から公開鍵暗号まで

認証のしくみから見る暗号技術の役割

荒木 俊輔

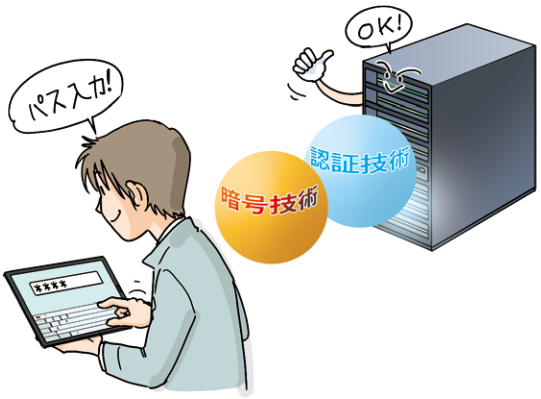

図1　認証システムは暗号によって守られている

現在では，非常に多くの人がネットワークに接続されたノートPCやスマートフォンなどの携帯デバイスを持ち，さまざまなサービスを受けるために，認証を経ています．例えば，最も基本的な認証手法の1つであるパスワード認証では，入力されたIDとパスワードを，事前に保存しておいた情報と照らし合わせて一致することを確認しています．

一見そこには，それ以上の技術が存在しないようにも思えますが，実は，情報セキュリティ技術が利用されています（**図1**）．例えば，攻撃者からIDやパスワード情報を守るため，システム側に保存してるパスワード・データを暗号化したり，通信中の盗聴を防ぐために，通信前にIDやパスワード情報を暗号化したりしています．

本稿では，認証と，情報セキュリティ技術，特に暗号技術が密接に関係していることを，パスワード認証を事例として取り上げ，解説します．

認証とは…
自分が自分であることを証明すること

認証とは端的に言えば，自分が自分であることを他者に示すことです．そこでは何かしらの自分についての情報が必要となります．イメージしやすいように日常生活での認証から説明します．

● 日常生活における認証

証明書などの書類を申請，受領する際，本人が窓口に出向く場合でも，本人であることを窓口の人に示すには，第三者の力を借りる必要があります．その際に，運転免許証などの身分証明書が要求されます．運転免許証は，各都道府県の公安委員会により発行されます．2者間において共通して信頼できる第三者が保証する運転免許証によって，他者に自分が自分であることを証明できています．

● 情報セキュリティでの認証

よく行われる認証として，パスワード認証があります．事前にサービス提供者側にパスワードを登録しておき，認証時にIDとパスワードを入力し，サービス提供者側で検証が行われます．事前に両者で秘密の情報を共有することにより，他者との識別ができています．また，ノートPCやスマートフォン，スマート・ロックなどで，指紋で認証され，他者と識別する技術もあります．さまざまな認証方法がありますが，これらは，その実施形態により，SYK，SYH，SYAの3つに分けられます（**表1**）．

パスワード認証の基本構成
（暗号なしの場合）

以降，最も身近な認証であるパスワード認証を暗号利用度順に説明していきます．なお，説明の容易化のために，単純化して説明しています．実際の実装とは異なりますので，注意してください．

● 認証のためには利用者とシステム側が秘密の文字列の共有が必要

パスワード認証では，認証のために，利用者とシステム側が秘密の文字列を共有する必要があります．例えば，PCのセットアップ時に，利用者自身がユーザIDとパスワード（10文字程度の英数文字列）を登録します．これは，利用者のみがその環境を利用できるよ