第5章 電子署名/ハッシュ関数の基礎知識 

# ブロックチェーンで使われる暗号技術入門

小暮 淳

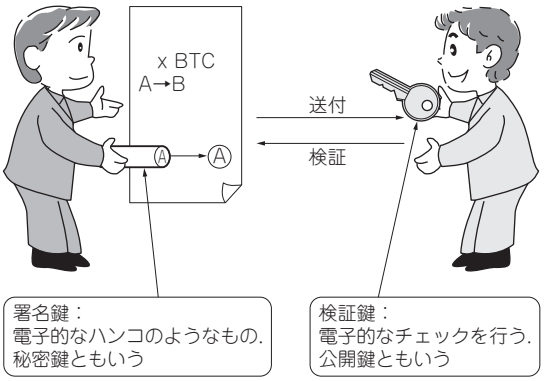


**図1　公開鍵型電子署名･･･秘密鍵を文書に署名する署名鍵として，公開鍵を電子署名を検証する検証鍵として利用する**

本稿では，ブロックチェーンで用いられる暗号技術に関して解説します．今やブロックチェーンにはさまざまな種類のものがありますが，もともとはビットコインの実現に用いられた技術の呼称です．そのため，ここでは元祖であるビットコインに用いられる暗号技術を主な対象とします．

ブロックチェーン上で取引する際には，暗号技術の中身を知らなくても取引可能ではありますが，その原理や用いられる意義を理解することによって，セキュリティ上注意すべき点が明確になり，より安心・安全に取引を行うことができるでしょう[注1]．

## ブロックチェーンで使われる暗号技術①…電子署名

### ● 公開鍵型を利用する

電子署名の目的は，データの真正性を保証することです．公開鍵型電子署名の場合，秘密鍵を文書に署名する署名鍵として，公開鍵を電子署名を検証する検証鍵として使います．

ビットコインの場合，所有するビットコインを次の所有者に対して送るというトランザクションが，「確かにそのビットコインの所有者，即ち署名鍵（秘密鍵）の所有者が意図するものであることを保証」します（**図1**）．

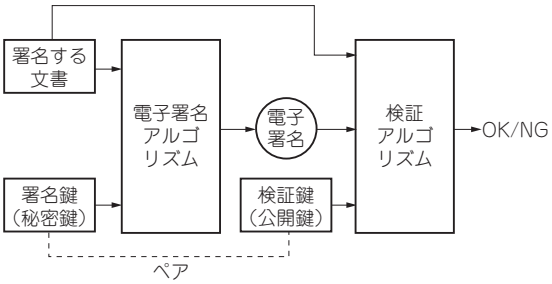


**図2　電子署名のフレームワーク**

電子署名は，署名鍵を知っている人にしか作ることのできないデータを，署名するデータに対して作ることによって，署名されたデータは署名鍵を知っている人が意図したものであり，かつ改変されていないことを保証できるようになります．

電子署名の検証は署名鍵に対応する検証鍵（公開鍵）によって行うことができます．検証鍵は公開してよいものであるため，誰でも電子署名の正しさを検証できます．電子署名のフレームワークを**図2**に示します．

### ● Satoshi Nakamoto論文の要件を満たす

ビットコインで実際に用いられている電子署名アルゴリズムはECDSA（Elliptic Curve Digital Signature Algorithm：楕円曲線電子署名アルゴリズム）というものです．

実はブロックチェーン（ビットコイン）の生みの親である「Satoshi Nakamoto論文（第4章）」には楕円曲線電子署名は登場しません．「電子コインを電子署名のチェーンにより定義する．コインの所有者は，次の人に前トランザクションと次の所有者の公開鍵のハッシュに電子署名することによりコインを送り，これらをコインの最後に追加する」と書かれているだけです．

注1：セキュリティに絶対はないため，本稿が暗号通貨取引の安全性を保証することはないことに気をつけてください．