イントロダクション2

全てのモノがネットワークにつながる今…
ますます重要に

情報社会を縁の下で支える！セキュリティの要「暗号技術」

野上 保之

図1
さまざまなデータや価値の流通（データ・チェーン）は便利な反面，危険性もあるので暗号技術などで守る必要がある

暗号技術は，古代から情報を守る方法として発達してきました．現代社会において，あらゆるものがネットワークでつながり便利になった一方で，情報セキュリティという観点では，課題は多層化，複雑化しています．本稿では，情報社会のセキュリティにおいて考えるべき点と，セキュリティを守る暗号技術の役割を説明します．

高度に情報化された便利な現代社会を安心して過ごしたい

● 情報システムは社会インフラやビジネス・モデルの根幹

現代社会において，情報セキュリティを取り巻く課題は多層化，複雑化しています．近年，スマートフォンなどのデバイス，車，家電，銀行などが高度に連結し，巨大なデータ・チェーン（データ・価値の流通）を構成し，社会インフラやビジネス・モデルの根幹をなしています．

● 便利な反面，セキュリティは複雑化

このような相互接続性は利便性と効率性を飛躍的に向上させる一方で，セキュリティの維持，連携が極めて困難になっています（図1）．

特に異なる業界や行政分野（例えばスマート・シティにおける交通，医療，エネルギー管理）のAPI連携では，標準化の不足や認証基準の差異がセキュリティ・ホールを生み出しやすくなっています．また，今後，ロボットや自動運転車，IoTデバイス同士が自律的に連携，交渉する世界では，これらの課題（特に対策実装の困難性）はさらに深刻化することが予測されます．このような高度に連結された社会では，会社や組織など単一システムの単位ではなく，データ流通全体を俯瞰して価値を守る視点，ならびにAPI経由の通信経路の末端での認証，認可セキュリティの確保が重要です．

まとめると，次のような課題が挙げられます．

- 通信経路上にあるサーバ，デバイスなどの各要素が提供，取得するデータの正当性，完全性，機密性を保証する難しさ
- 一部のノードやデバイスの脆弱性が，連鎖的にネットワーク全体のリスクへ拡大する構造的な脆弱性
- API連携の動的，多様化により，認証・認可の管理が複雑化し，統一したセキュリティ・ポリシを適用することが困難
- データの流通経路の可視性が低く，リアルタイムのモニタリングや追跡が難しいため，インシデントの検知や対応が遅れるリスク

このような状況に加えて，ハッカーなど攻撃者側の