

# 『毎日の情報 I』 ～毎日配信企画～

No.030

データのセキュリティを確保するために情報通信技術は重要な役割を果たしています。その中でも **A 共通鍵暗号方式と公開鍵暗号方式** は、データの機密性と完全性を保つための主要な手段です。

共通鍵暗号方式は、送信者と受信者が同じ秘密鍵を共有し、それを用いてデータを暗号化および復号化する方法です。しかし、この方法では鍵の配布が課題となります。これに対して、公開鍵暗号方式は、公開鍵と秘密鍵の2つの鍵を使用します。[ ① ] はデータを暗号化し、[ ② ] はそれを復号化します。これにより、公開鍵を公開しても安全な通信が可能となります。

さらに、デジタル署名は公開鍵暗号を利用して、データの [ ③ ] と認証を実現します。これらの暗号化技術は、デジタル化が進む現代社会において、個人情報や企業情報を保護する重要なツールとなっています。

しかし、暗号化技術だけでは情報セキュリティを十分に保証することは難しいです。ネットワークセキュリティ、アプリケーションセキュリティ、物理的なセキュリティなども組み合わせて行う必要があります。また、定期的なセキュリティ教育やシステムのアップデートも重要な役割を果たします。

問1 空欄 [ ① ] から [ ③ ] に当てはまる言葉をそれぞれ答えなさい。

問2 下線部 A について、デジタル署名が果たす役割とその重要性について述べる文章を一つ選びなさい。

- ① デジタル署名は、情報の送信者がその情報を改ざんされないように保護するための手段です。これにより、受信者は送信者が実際に送った情報であることを確認できます。
- ② デジタル署名は、情報の送信者が秘密鍵で暗号化し、受信者が公開鍵で復号化することで、情報の安全性を確保します。
- ③ デジタル署名は、情報の送信者がその情報の機密性を保つための手段です。これにより、受信者は情報の内容が公開されることなく安全に受信できます。
- ④ デジタル署名は、情報の送信者がその情報の完全性を保証するための手段です。これにより、受信者は情報が途中で改ざんされていないことを確認できます。
- ⑤ デジタル署名は、情報の送信者がその情報を第三者に知られることなく、安全に受信者に送ることができる手段です。