情報セキュリティマネジメント試験合格講座 04

- 情報セキュリティ技術

1. CRYPTREC（Cryptography Research and Evaluation Committees、クリプトレック）
   電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するプロジェクト。総務省と経済産業省が共同で運営する暗号技術検討会などで構成される。

2. CRYPTREC 暗号リスト
   暗号技術検討会及び関連委員会によって安全性及び実装性能が確認された暗号技術のうち、市場における利用実績が十分であるか今後の普及が見込まれると判断され、当該技術の利用を推奨する暗号技術のリスト。

3. 共通鍵暗号方式
   暗号化と復号で同じ鍵を使用する暗号方式。代表的なアルゴリズムに、DES、IDES、次世代の暗号方式として AES がある。

4. DES（Data Encryption Standard）
   1970 年代に規格化された共通鍵暗号方式のひとつで、米国の旧国家暗号規格である。

5. Triple DES
   共通鍵暗号方式のひとつ。暗号化、復号、暗号化と 3 つの鍵を変えながら、DES を三回繰り返すことで強度を高めた暗号アルゴリズム。

6. IDEA（International Data Encryption Algorithm）
   1991 年に開発された共通鍵暗号方式のひとつ。データを 64 ビット単位に区切って、128 ビットの鍵を用いて処理するブロック暗号方式である。

7. AES（Advanced Encryption Standard）
   米国の次世代暗号方式としてアメリカ国立標準技術研究所（NIST、National Institute of Standards and Technology）によって規格された共通鍵暗号方式。DES の鍵長が 56 ビットなのに対し、最大 256 ビットの鍵長を利用する。

8. 公開鍵暗号方式(Public key cryptosystem)
暗号化と復号で別の鍵を使用する暗号方式。代表的なアルゴリズムに RSA がある。暗号化鍵と暗号化アルゴリズムは公開するが、復号鍵は秘密にしなければならない。

9. RSA(Rivest Shamir Adleman)
公開鍵暗号のひとつ。桁数が大きい数の素因数分解が困難であることを利用している。1983 年に米国の特許を取得しているが、特許期間満了に伴って現在は誰でも自由に使用できるようになった。

10. S/MIME(Secure/Multipurpose Internet Mail Extensions)
電子メールを暗号化するために使用される方式。公開鍵暗号標準 PKCS(Public Key Cryptography Standards)に従って暗号化やディジタル署名などを行うことで、通信の機密性と完全性を高めることができる。

11. ハイブリッド暗号方式
公開鍵暗号方式における鍵管理の利便性と、共通鍵暗号方式の速い処理速度を組み合わせた方式。公開暗号方式を利用して通信をしようとする当事者が共通鍵を共有する。共通鍵を共有した後は、その鍵を使って暗号化通信を行う。

12. PGP(Pretty Good Privacy)
ファイルや電子メールの暗号化ツール。信用の輪(Web of Trust)という考え方に基づいて安全性や信頼性を担保している。暗号化アルゴリズムとして RSA と IDEA が用いられている。

13. 信用の輪(Web of Trust)
信頼し合う者同士が互いの公開鍵に自ら署名し合う事によって、互いの信用度を維持し、更に複数の者がこれを行うことで、直接署名の交換をしていない者同士でも、信頼している第三者を介することによって相手の信用度を維持できるというものである。この時の相手までの信頼関係のことを信用パス(Trust Path) という。

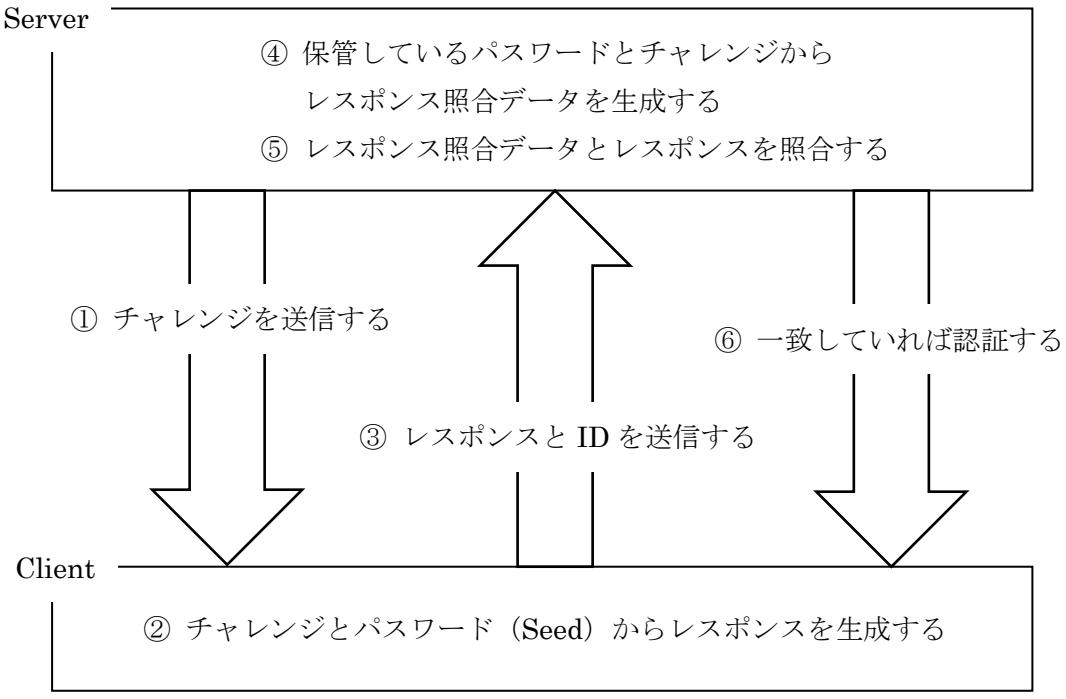
14. ハッシュ関数(Hash Function)
任意の長さのデータを入力すると、一定のハッシュ値(メッセージダイジェスト)を生成する関数。

15. SHA（Secure Hash Algorithm）-256
ハッシュ関数のひとつ。32 ビットのワード長から計算される。ソフトウェアパッケージの認証や、メッセージ署名標準として利用されている。

16. ディジタル署名（Digital Signature）
公開鍵暗号方式の技術を使ってディジタル文書の正当性を保証する署名鍵検証鍵。受信者はハッシュ関数を用いてメッセージからハッシュ符号を生成し、送信者の公開鍵で復号したハッシュ値と比較し、送信者の正当性と改ざんがないことを確認できる。

17. MAC（Message Authentication Code、メッセージ認証符号）
比較する出力値（MAC 値）を生成する際に、元データに加えて送信者と受信者のみが持つ共通鍵を加えることで、データとハッシュ値の改ざんを検知する仕組み。メッセージ認証完全性符号（MAIC、Message Authentication and Integrity Code）とも呼ばれる。

18. チャレンジレスポンス認証（Challenge And Response Authentication）
ワンタイムパスワードによる認証方法のひとつ。サーバから送られてきたランダムなデータであるチャレンジと利用者が入力したパスワードをクライアント側で演算し、その結果を送信することで、パスワードの直接の通信を避ける認証方法。



19. S/KEY 方式
ワンタイムパスワードによる認証方法のひとつ。サーバはクライアントから送られた使い捨てパスワードを演算し、サーバで記憶している前回の使い捨てパスワードと比較することによってクライアントを認証する。

20. PAP(Password Authentication Protocol)
利用者の認証を行う通信プロトコルのひとつ。クライアントが ID とパスワードを送信して、サーバが認証するかどうかを応答する仕組み。パスワードを平文のまま送信するのでセキュリティ対策が必要。

21. CHAP(Challenge Handshake Authentication Protocol)
PPP(Point to Point Protocol)で利用できる認証プロトコルで、チャレンジレスポンス方式で認証を受ける方式。

22. PPTP(Point to Point Tunneling Protocol)
PPP パケットを IP データグラム(インターネットデータグラム、基本転送単位)でカプセル化して VPN(Virtual Private Network、仮想プライベートネットワーク)を作り出す技術。

23. タイムスタンプ(時刻認証)
日時、日付、時刻などを示す文字列。「信頼できるタイムスタンプ」とは、時刻認証局(TSA、Time Stamp Authority)が発行する時刻情報を含んだ電子文書を指す。

24. 危殆化(きたいか)(Compromise)
技術の進歩によって計算性能が著しく向上し、非常に複雑な計算が可能になり、従来の暗号技術などの安全性が相対的に低下してくる状況のこと。

〔問題集〕
- ✓ 石川敢也(共著)「情報セキュリティマネジメント要点整理＆予想問題集」 翔泳社
- ✓ 情報セキュリティマネジメント試験合格講座 http://rakupass.com/security/