情報セキュリティマネジメント試験合格講座 05

- 利用者認証技術

1. ワンタイムパスワード(One Time Password)
   認証を行う度に毎回異なる使い捨てのパスワードを使用する認証方式。

2. PIN(Personal Identification Number)
   利用者とシステムとの間で共有している個人を識別するための暗証番号。

3. 多要素認証
   利用者が知っていたり、持っていたりする情報を、複数の要素を使用して認証を行う方式。例えば「トークンを持っていて、パスワードを知っている」など。

4. シングルサインオン(Single Sign On)
   一度の認証で、許可されている複数のサーバやアプリケーションなどを利用できる仕組み。

   ✓ HTTP Cookie 方式
   認証済みの利用者の情報を HTTP cookie で識別してシングルサインオンを可能にする認証方式。

   ✓ リバースプロキシ方式
   利用者認証においてパスワードの代わりにディジタル証明書でシングルサインオンを可能にする認証方式。

   ✓ SAML(Security Assertion Markup Language)方式
   認証情報を安全にやりとりするための XML である SAML を使って複数のドメイン間でシングルサインオンを可能にする認証方式。

5. CAPTCHA
   人間には読み取ることが可能でも、プログラムでは読み取ることが難しいという差異を利用して、ゆがめたり一部を隠したりした画像から文字を判読させ入力させることで、人間以外による自動入力を排除する技術。

6. パスワードリマインダ
   パスワードを忘れたユーザのため、あらかじめ登録された利用者のメールアドレス宛てにパスワード再登録用ページへアクセスできる URL を送信するなどの仕組み。

7. バイオメトリクス認証（Biometrics Authentication）
   生体認証。指の指紋、皮膚の隆線、血管、瞳の虹彩など、身体の特徴によって個人を識別する方法と、サインをするときなど決まった動作や行動の特徴などによって個人を識別する方法がある。

8. 静脈パターン認証（Vein Authentication）
   生体認証のひとつ。掌や指先の静脈パターンで本人確認を行う認証方式。

9. 虹彩認証（Iris Recognition）
   生体認証のひとつ。角膜と水晶体の間にある薄い膜の皺によって本人確認を行う認証方式。成人には虹彩の経年変化がないので、認証デバイスでのパターン更新がほとんど不要である。

10. FRR(False Rejection Rate)
    本人拒否率。本人であるにもかかわらず、誤って本人ではないと判断される確率。

11. FAR（False Acceptance Rate）
    他人受入率。他人であるにもかかわらず、誤って本人であると判断される確率。FRR と FAR の関係はトレードオフであり、FRR を減少させると FAR は増大し、FRR を減少させると FAR は増大する。

12. PKI（Public Key Infrastructure、公開鍵基盤）
    所有者と公開鍵の対応付けをするのに必要なポリシや技術の集合によって実現される基盤。

13. ディジタル証明書
    公開鍵の証明書。SSL/TLS プロトコルにおいて通信データの暗号化のための鍵交換や通信相手の認証に利用されている。

14. SSL/TLS（Secure Socket Layer/Transport Layer Security）
通信データの暗号化のための鍵交換や通信相手の認証にディジタル証明書を用いてデータを安全に送受信する仕組み。

15. ルート証明書
ディジタル証明書を発行する認証局が、自ら署名して発行する証明書。受信した証明書が正当なものかどうかを確認するため、SSL/TLS などで暗号通信を利用できる Web ブラウザに組み込まれている。

16. サーバ証明書
ディジタル証明書を発行する認証局が発行する証明書で、Web サイトの身元の照会や通信の暗号化に使われる。

17. クライアント証明書
個人や組織が身元の証明を行うための公開鍵の証明書。クライアントとサーバが通信する場合にクライアントを照会するために提示する。

18. CRL（Certificate Revocation List）
有効期間内に効力を無くしたディジタル証明書を集めた証明書失効リスト。

19. VA（Validation Authority）
ディジタル証明書の失効リスト（CRL）を集中管理して、証明書の有効性をチェックする証明書有効性検証局。

20. OCSP(Online Certificate Status Protocol)
ディジタル証明書が失効しているかどうかをオンラインでリアルタイムに確認するために、鍵の漏えい、破棄申請の状況をリアルタイムに反映するプロトコル。

21. RADIUS（Remote Authentication Dial In User Service）
無線 LAN や VPN 接続などで利用され、利用者を認証するためのシステム。

22. ディレクトリサービス
ネットワーク上にある ID、パスワード、属性情報、設定情報、ファイル、プリンタなどの資源を一元管理して、検索したり提供したりできるようにした仕組み。

23. LDAP(Lightweight Directory Access Protocol)
ネットワーク上にある情報を管理するディレクトリデータベースへアクセスするためのプロトコル。

24. EAP(Extensible Authentication Protocol)
PPP の認証機能を強化したユーザ認証のプロトコル。

- ✓ EAP-TLS(Transport Layer Security)
ディジタル証明書を使った TLS による相互認証を行う方式。

- ✓ EAP-TTLS(Tunneled TLS)
TLS による認証の後に TLS のトンネル(パケットのカプセル)内でサプリカント(認証を要求するクライアント側の機器やソフトウェア)を認証する方式。

- ✓ EAP-MD5(Message Digest Algorithm 5)
ハッシュ関数 MD5 を用いたチャレンジレスポンス方式によってパスワードを暗号化して、サプリカントの認証を行う方式。サーバの認証は行わない。

25. ライブネット
組織に割り当てられている IP アドレスのうちコンピュータで使用されている IP アドレス空間。

26. ダークネット
インターネット上で到達可能、かつ、未使用の IP アドレス空間。

27. 深層 Web(ディープ Web)
通常の検索エンジンが収集することができないインターネットの情報である。「インビジブル Web」とも呼ばれる。

〔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/