情報セキュリティマネジメント試験合格講座 02

- 不正のメカニズム

1. 脅威（Threat）
   リスクを発生させる要因、情報資産に損失を与える要因。結果的に組織が保有する情報資産に対して害を与える可能性があるもの。脆弱性とともに情報セキュリティリスクを構成する要素のひとつ。

2. 物理的脅威
   ハードウェアが破損したり処理を妨害されたりする脅威。地震、落雷、火災、停電、故障、ネットワークの障害など。

3. 技術的脅威
   コンピュータに対するプログラムが介在する脅威。セキュリティホール、改ざん、マルウェア、クロスサイトスクリプティング、DoS 攻撃、危殆化など。

4. 人的脅威
   人間の行為が直接関係する脅威。操作のミス、意図的な漏えい、過失、失念、紛失、ソーシャルエンジニアリングなど。

5. 脆弱性（Vulnerability）
   攻撃によって悪用される可能性がある弱点。脅威の原因になる可能性がある弱点。

6. 人為的脆弱性
   コンピュータやソフトウェアに関する脆弱性に対し、セキュリティ環境の未整備や情報の管理体制が実践されていない状態。施設内への侵入による盗難や破損、会話からの情報漏洩などがある。

7. ソーシャルエンジニアリング
   技術的な手段ではなく、人間の心理的な弱点や行動の特性などを利用して機密情報を入手する方法。

8. 不正のトライアングル
   不正行為を行う条件のことで、機会、動機、正当化の 3 つが揃った状態。

   ✓ 機会
   例えば「自分がシステムの管理者である」や「他の誰にも見られていない」など、行為を実行できる状態。

   ✓ 動機
   例えば「お金に困っている」や「相手に個人的な恨みがある」など、不正を働こうとする理由がある心理状態。

   ✓ 正当化
   例えば「どうせ使っていないものだから（なくなっても困らないだろうと考える）」や「卑怯なやり方で儲けた金だから（盗んでも罪悪感が少ない）」など、不正行為を正当だと思うことができる状態。

9. 故意犯
   自己の行為が社会的に許されないことを認識しながら不正行為をすることや実行する者。

10. 確信犯
    自己の行為が正しいと信じ込んで不正行為をすることや実行する者。なお、「悪いことだと分かっていながらする行為」という意味で使うのは誤用である。

11. 愉快犯
    個人や社会集団を混乱やパニックに陥れる様な行為を行い、その反応を楽しむことを目的とした行動や犯人。

12. 詐欺犯
    他人をだまして損害を与えようとする行動や犯人。アカウントを乗っ取り、友人などを装って、電子マネーの購入などを持ちかける事件が多発している。

13. サイバー攻撃（Cyber Attack、Cyber Terrorism）
コンピュータシステムやインターネットなどを利用して、不正侵入を行い、データの詐取、破壊、改ざんなどを行なったり、標的のシステムを機能不全に陥らせたりする攻撃。

14. クラッキング（Cracking）
システムへの不正侵入、破壊や改ざんなど、コンピュータを不正に利用すること。

15. スクリプトキディ（Script Kiddie）
自分ではマルウェアの作成能力がないが、他者が作ったプログラムを悪用して、第三者に被害を与えるクラッカーの俗称。

16. ファイル共有ソフト
インターネットで不特定多数の利用者とファイルをやり取りすることができるソフトウェアの総称。専用のプロトコルで通信を行うことで、専用のネットワークを構成することで、ネットワークに接続された不特定多数の端末同士でファイルのやりとりを行う仕組みを提供する。

17. マルウェア （Malware）
コンピュータウイルス、ワーム、トロイの木馬、スパイウェアなどの不正かつ有害な動作を行う意図で作成された「悪意のある」ソフトウェアの総称。

18. ワーム（Warm）
インターネットなどのネットワークを介して、自分自身の複製を電子メールに添付して勝手に送信したり、ネットワーク上のほかのコンピュータに自分自身をコピーしたりして、自己増殖するプログラム。

19. トロイの木馬
ある特定の期日や条件を満たしたときに、データファイルを破壊するなど不正な機能が働くプログラム。

20. スパイウェア
利用者の意図に反してインストールされ、利用者の個人情報やアクセス履歴などの情報を収集するプログラム。

21. ランサムウェア（Ransom Ware）
感染すると勝手にファイルやデータの暗号化などを行って、正常にデータにアクセスできないようにし、元に戻すための代金を利用者に要求するソフトウェア。

22. ボット
多数の PC に感染して、ネットワークを通じた指示に従って PC を不正に操作することで一斉攻撃などの動作を行うプログラム。

23. ボットハーダー（Bot Herder）
遠隔地から制御できるネットワークであるボットネットを操作する者のこと。ボットネットを構成する遠隔制御されるボットを「家畜」として操り、その牧場の「番人、牧夫」という意味。

24. ルートキット（Rootkit）
攻撃者が PC への侵入後に利用するために、ログの消去やバックドアなどの攻撃ツールをパッケージ化して隠しておく仕組み。

25. バックドア
侵入を受けたサーバに設けられた、不正侵入を行うための通信経路。

26. ハクティビズム（Hacktivism）
思想的な意思の表明や政治目的の実現のためにハッキングを手段として利用する行為や考え方。積極行動主義という意味のアクティビズム（Activism）と、不正侵入という意味のハック（Hack）を組み合わせた新語。

27. キーロガー
キーボード入力を記録する仕組みを利用者の PC で動作させ、この記録を入手する行為や実行するソフトウェア。

〔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/