

# システムセキュリティ 【学習のポイント】

## ■1 様々なシステムセキュリティ脅威の区別

権限の昇格やウイルス、ワームといったシステムに対する脅威に関する問題が出題されます。また、昨今の事情を反映して、アドウェアやボットネットなど、新たな脅威についても学習する必要があります。

## ■2 システムハードウェアや周辺機器に関連したセキュリティリスクの識別

システムハードウェアの中でも、情報セキュリティに関わる機器や機能に関する問題が出題されます。また、BIOSやUSBデバイスといった幅広い機能、機器に対しても、それぞれのリスクを学習する必要があります。

## ■3 ワークステーションやサーバのセキュリティ確保、およびOSのセキュリティ対策

ワークステーションやサーバに対するセキュリティ対策として、OSのセキュリティ対策を具体的に確認する問題が出題されます。そのため、サービスパックやパッチ適用だけでなく、セキュリティテンプレートやグループポリシーなどを学習する必要があります。

## ■4 アプリケーションセキュリティ構築の方法

アプリケーションに関連するセキュリティ上のリスクに関する問題が出題されます。以下に挙げるアプリケーションについて、それぞれのリスクや防御方法などを学習する必要があります。

- Active X
- Java
- スクリプト
- ブラウザ
- バッファオーバーフロー
- Cookie
- SMTPオープンリレー
- インスタントメッセージング
- P2P
- 入力検証
- クロスサイトスクリプティング(XSS)

# 問題

## 問題

1

あるユーザーが管理者権限を奪取するために、他人のアカウントを利用して不正アクセスする行為は、次のうちどれですか。

- A バッファオーバーフロー
- B 多重ログイン
- C ID詐称
- D ID Key Synchronize

## 問題

2

プログラムを媒介して、自分自身をコピーし、そのプログラム実行時に他のコンピュータやファイルに感染範囲を拡大させるのは、次のうちどれですか。

- A トロイの木馬
- B バックドア
- C ロジック爆弾
- D ウイルス

## 問題

3

メモリ上に常駐し、感染以前のファイルサイズや更新日付を表示して、自身を隠べいしようとするウイルスは、次のうちどれですか。

- A マルチパーティー (multiparty)
- B ステルス (stealth)
- C ミューテーション (mutation)
- D ポリモーフィック (polymorphic)

## 問題

4

媒介となるファイルを必要とせずに感染を広げるウイルスは、次のうちどれですか。

- A マクロウイルス
- B トロイの木馬
- C ロジック爆弾
- D ワーム

## 問題

5

便利なツールを装ってインストールさせ、ユーザーの見えないところで気づかぬうちに、好ましくない動作をするものは、次のうちどれですか。

- A トロイの木馬
- B ウイルス
- C ワーム
- D ActiveX

# 解答・解説

## 問題

1

◆解答 C

◆解説

不正アクセスに関連する事件簿を見ていると、アクセスした証拠を限りなく減らすために、他人のアカウントを利用する事例が後を絶ちません。これらの行為はID詐称もしくはIDなりすましと呼ばれています。

バッファオーバーフローは、具体的に管理者権限を奪取するための手法の一つです。

多重ログインは、同一のIDを使用してシステムに複数のログインを行うことで、オンラインバンキングなどでは禁止されています。また、電子掲示板のような一人のユーザーに1アカウントしか発行しないサーバの場合、複数アカウントを取得して別人になりますことも行われますが、管理者権限の奪取が目的ではないために設問の答えとしては適切ではありません。

ID Key Synchronizeは造語です。

## 問題

2

◆解答 D

◆解説

プログラムファイルやデータファイルに感染し、その感染ファイル実行時に発病するものはウイルスです。不正なプログラムはすべてウイルスであると考え「**広義のウイルス**」では、ワームやトロイの木馬も含まれます。しかし、「**狭義のウイルス**」では、ウイルスは必ず「**感染機能**」「**潜伏機能**」「**発病機能**」の一つ以上の機能を有しており、ウイルスが感染する対象(寄生媒体)が必要となります。

トロイの木馬は、ユーザーにとって表面上は無害なプログラムであっても、知らぬ間に情報を抜き取られたりするなど、悪意ある行為をする不正プログラムですが、他のファイルに自分自身をコピーする能力はありません。バックドアは、アタッカーが攻略したサーバなどに再侵入する際に、同じ攻撃手順などを使用せずにアクセスするための裏口です。攻撃手順を何度も繰り返すことがなくなるため、侵入されたシステムの管理者などに発見される可能性を下げるためにバックドアが使用されます。他のファイルへの感染活動は行いません。ロジック爆弾は、ある一定条件を満たしたとき、特定の処理を行ったときに攻撃者に都合のよい処理を実施するようなプログラムのことです。

## 問題

3

◆解答 B

◆解説

ウイルス対策ソフトは、ウイルスを検知する仕組みとして、ディスクに読み書きされるデータや、メモリ上で読み書きされるデータなどを、定義ファイルと呼ばれるウイルスパターンと照合して、一致した場合にウイルスだと判定します。ステルス型のウイルスは、これらのウイルス対策ソフトの検知から逃れるために、ディスクやメモリ上に展開されるデータをランダムに配置したり、ランダムに配置するデータなどを暗号化することによって、一部分のデータを参照しただけではウイルスと判定できないようにします。ミューテーション型ウイルスの場合も自身を暗号化することでウイルス対策ソフトからの検知を逃れようとしませんが、ミューテーション型ウイルスの場合は暗号化されていることが判別できる状態で保存されるのとは異なり、ステルス型ウイルスの場合は暗号化されていることも偽装するなど、ウイルスの存在自体を隠ぺいしようとしています。ポリモーフィック型ウイルスはミューテーション型ウイルスと同義です。マルチパーティーは、複数のベンダーの製品やプログラムなどを組み合わせて構成するシステムの通称です。そのため、選択肢Bが正解となります。

## 問題

4

◆解答 D

◆解説

マクロウイルスは、Microsoft社のExcelやWordファイルなどに寄生し、そのマクロ機能を利用して自己増殖や破壊活動を行うウイルスです。マクロ機能を有効にしている場合、ファイルを開いた時点で感染してしまいます。トロイの木馬は、無害であるプログラムを装い、実行することによって破壊活動などを行う不正プログラムです。ロジック爆弾は、作成者が仕込んだある条件を満たすことにより、活動を開始する不正プログラムです。たとえば、アクセス回数が一定数になるなどの条件によって活動を開始します。ワームはネットワークを経由して自身を複製するプログラムですが、ウイルスと異なり、媒介とするファイルは必要ありません。ワームは、たとえばシステムのセキュリティホールを悪用してコンピュータに侵入し、ネットワーク上の別のコンピュータなどへ攻撃して感染範囲を拡大させていきます。

## 問題

5

◆解答 A

◆解説

トロイの木馬は、一見、有益なツールと見せかけて侵入してきます。実際に有益なツールとしての働きをしながら、裏側で動作しているものもあります。

最近では有益なツールに見せかけて侵入するという手口よりも、ユーザーが気づかない間に情報が盗み出されたり、意図しない操作が実行されたりするなどのツールを指す場合もあり、定義自体があいまいになってきています。

ちなみにトロイの木馬という呼び名は、トロイ戦争の際にギリシア軍が巨大な木馬の中に潜み、トロイ軍の城内に潜入したことに由来しています。

ウイルスやワームは、トロイの木馬と異なり、感染機能や自己伝染機能を有するのが特徴です。ActiveXはMicrosoft社が開発した、Web上でコンポーネントをやり取りする技術の総称です。