３級　技術編

問 A19　　**p56 － p57**

ある学校で，公開用の Web サーバが何者かによって不正アクセスされる事件が起きた。発見後の処理として［適切なもの］をすべて選び，チェックしなさい。

1. **ファイアウォールの設定内容の見直しを行う。**
2. **不正アクセスされたサーバをネットワークから切り離す。**
3. **不正アクセスされたサーバのハードディスクの内容には手をつけず先にフォーマットをする。**
4. **不正アクセスされたサーバのハードディスクをフォーマット後に，直近のバックアップから全内容を復元する。**
5. **JAPET（日本教育工学振興会）への届け出を行う。**

答え　1,2

解説

不正アクセスを受けた場合，発見後の対処法として

1. **ネットワークの切断**：**不正アクセスを受けたサーバをネットワークから切り離す**
2. **被害拡大の防止**：**被害が広がらないように，ネットワーク内の他のシステム管理者に不正侵入があったことを連絡し，被害にあっていないかを確認させる**
3. **被害状況の保存**：**侵入されたマシンのハードディスクのバックアップを行う**
4. **システムの復旧**：**バックアップからシステムを復旧させる**
5. **再発防止策の検討を実施**：**ファイアウォール，ルータの見直し，再発防止策を検討**
6. **関係機関への連絡**：**届け出**

1.の場合（再発防止策の検討に関連）

可能な限り原因を究明し，再発防止策を検討する（ファイアウォール，ルータの設定の見直し）

※TCP／IP で通信を行う場合は，宛先として「IP アドレス」を指定し，その通信で何をするのか（どんなサービスを受けるのか）はプロトコルによって決まる。

例） HTTP　**プロトコル** 80 **番，** POP3　**プロトコル** 110 **番　など**

2.の場合（ネットワーク切断に関連）

不正アクセスやウィルス感染などでの基本的な対処法。被害が広がらないように，ネットワーク自体を物理的にシャットアウトとしてしまう。単純かつ確実。

3,4 の場合（被害状況の保存，システムの復旧に関連）

システムのバックアップには，不正侵入者のプログラムが残っている場合が考えられるので，バックアップからシステムを復旧させるには十分な注意が必要。最初からシステムを再インストールする方法がよい。ただし，内容をすぐにフォーマットしてしまうと事後調査が困難。

5.の場合（関係機関への連絡に関連）

IPA（Information-technology Promotion Agency,Japan）

情報処理振興事業協会。政府関係機関。最新のセキュリティ情報のほか，ウィルス対策や不正アクセス対策などを掲載。ウィルスの届出や相談も受け付けている。

JPCERT/CC（JaPan Computer Emergency Response Team/Coordination Center）

コンピュータ緊急対応センター。インターネットを介した不正アクセスに関する情報を収集・公開する日本の団体。セキュリティ問題に関する啓蒙活動も行っている。