平成 24 年度 技術士第二次試験 模擬答案用紙

受験番号	
問題番号	Ⅰ－2－2

技術部門	部門
選択科目	
専門とする事項	

※

○受験番号，問題番号，技術部門，選択科目及び専門とする事項の欄は必ず記入すること。
○解答欄の記入は，1マスにつき1文字とすること。（英数字及び図表を除く。）

（1）IDS／IPSについて

IDSは「侵入検知システム」、IPSは「侵入防御システム」の意味である。IDS／IPSは、コンピュータやネットワークに対する不正行為を検出するシステムだが、検出後に防御措置を取るのがIPS、防御措置を取らないのがIDSである。

（2）IDS／IPSの分類

不正検出：あらかじめ登録されたシグネチャと呼ばれる侵入手口のパターンとマッチングさせ、不正行為を検出する手法で、既知の侵入手口を使った攻撃のみ検出することができる。

異常検出：通常とは異なる振る舞いを検出する方法で、未知の手法による攻撃も発見することができる。

（3）IDS／IPSの導入型

ホスト型：OSの監査機能と連携して不正侵入を検知する。保護したいPCにインストールし、ログやファイルの改ざんの監視を行う。インストールされたホスト自身に対する攻撃以外は検出できない。

ネットワーク型：ミラーポートからパケットのコピーをキャプチャする「プロミスキャスモード」や、ネットワークに挿入する「インラインモード」により、接続しているネットワークセグメントの全てのトラフィックを監視する。具体的には、ネットワーク上を流れるパケットを収集し、そのプロトコルヘッダやデータを解析し、不正を検出する。

●裏面は使用しないで下さい。　●裏面に記載された解答は無効とします。　24字×25字