16－4 情報ネットワーク【選択科目Ⅱ】

Ⅱ　次の２問題（Ⅱ－１，Ⅱ－２）について解答せよ。（問題ごとに答案用紙を替えること。）

Ⅱ－１　次の４設問（Ⅱ－１－１～Ⅱ－１－４）のうち２設問を選び解答せよ。（設問ごとに答案用紙を替えて**解答設問番号**を明記し，それぞれ１枚以内にまとめよ。）

Ⅱ－１－１　ホームページが改ざんされたため，その手口を調べたところ，HTTP PUTメソッドを悪用した手法であることが判明した。改ざんの手法を具体的に説明し，再発防止のための対策を述べよ。

Ⅱ－１－２　IPバージョン６のヘッダフォーマットの特徴をIPバージョン４と比較して解説せよ。

Ⅱ－１－３　データセンター内のネットワークに関する，ToR（Top of Rack）とEoR（End of Raw）について概説し，それらの必要性と，それぞれの得失を述べよ。

Ⅱ－１－４　ネットワークの経路を調査するツールとしてtracerouteコマンド（あるいはtracertコマンド）がある。これらのツールがTCP/IPネットワークのどのような仕組みを使って機能しているか説明せよ。

Ⅱ－２　次の２設問（Ⅱ－２－１，Ⅱ－２－２）のうち１設問を選び解答せよ。（**解答設問番号**を明記し，答案用紙２枚以内にまとめよ。）

Ⅱ－２－１　ネットワークに接続された機器間で行われる通信を意味するM2M（Machine to Machine）は様々な分野での利用が期待されている。これについて以下の問いに答えよ。

（１）M2Mで発生するトラフィックの特徴を説明し，M2Mのトラフィックを運ぶネットワーク側で技術的に配慮すべき事項を挙げよ。

（２）M2Mにおける情報交換用プロトコルとしてHTTPを用いる場合の長所と短所を挙げ，現在検討されている代替案について知るところを述べよ。

Ⅱ－２－２　デジタルフォレンジック手法を用いて情報セキュリティ侵害の調査・分析を行う際に，ネットワークやサーバ，パソコンにあるデータやログといった電磁的記録を証拠として保全する作業を行う。証拠の保全や取扱いに関して，以下の問いに答えよ。

（１）保全の対象となり得る電磁的記録を３種類挙げよ。

（２）（１）で挙げた電磁的記録を保全する順番を示し，その理由を説明せよ。

（３）証拠保全において考慮すべき技術的事項と配慮すべき非技術的事項を１つずつ挙げ，具体例を示しながら説明せよ。

16－4 情報ネットワーク【選択科目Ⅲ】

Ⅲ　次の２問題（Ⅲ－１，Ⅲ－２）のうち１問題を選び解答せよ。（**解答問題番号**を明記し，答案用紙３枚以内にまとめよ。）

Ⅲ－１　Ａ社は全国に拠点を持つ中堅企業である。Ａ社の情報システムは，本社内のサーバ室に設置された200台の物理サーバで稼働し，その保守と運用は本社の情報システム部が担当している。事業継続性の確保，サーバ設備の老朽化，情報システム部員の高齢化などの課題を踏まえ，Ａ社の経営陣は情報システム部へ，Ｂ社が提供するIaaS（Infrastructure As A Service）へ全サーバを移行する検討を指示した。１年間の移行期間を経てサーバ室を廃止する前提である。この状況に関して，以下の問いに答えよ。

（１）移行する主なネットワーク基盤を挙げ，それぞれについて移行の概要を述べよ。

（２）移行後のネットワーク基盤の運用を想定し，Ａ社，Ｂ社とそれ以外のステークホルダにおける，運用体制とそれぞれの役割を述べよ。

（３）（１），（２）に関する技術的課題や留意点を３つ挙げ，それぞれについて，複数の解決案を述べよ。

Ⅲ－２　Ａ社ではサイバー攻撃や情報漏洩等の情報セキュリティインシデントの調査を少なくとも１年前まで遡って行えるようにするために，社内ネットワークとインターネットとの間の通信に関するログを適切に記録・保管することになった。プロキシサーバ及びファイアウォールの１日当たりのログのサイズを計測したところ，プロキシサーバでは約２Ｇバイトのログが生成され，ファイアウォールでは警告等の異常系ログのみを記録するように設定した場合は約１Ｇバイト，正常系ログも記録するように設定した場合は約４Ｇバイトのログが生成されることがわかった。Ａ社での検討に関して，以下の問いに答えよ。

（１）通信に関するログ以外で調査に有用なデータを少なくとも１つ例示し，有用性を説明せよ。

（２）プロキシサーバとファイアウォールのログ，及び（１）で挙げたデータの適切な記録・保管の方針について検討し，それを実現するためのログ等の設定要件とサーバ等の機器やネットワークに対する要件を示せ。

（３）これらのログ等を用いて情報セキュリティインシデントの早期発見を行えるようにするために，どのような手法やツールを導入すべきか提案せよ。

16－4 情報ネットワーク【選択科目Ⅲ】

Ⅲ　次の２問題（Ⅲ－１，Ⅲ－２）のうち１問題を選び解答せよ。（**解答問題番号**を明記し，答案用紙３枚以内にまとめよ。）

Ⅲ－１　Ａ社は全国に拠点を持つ中堅企業である。Ａ社の情報システムは，本社内のサーバ室に設置された200台の物理サーバで稼働し，その保守と運用は本社の情報システム部が担当している。事業継続性の確保，サーバ設備の老朽化，情報システム部員の高齢化などの課題を踏まえ，Ａ社の経営陣は情報システム部へ，Ｂ社が提供するIaaS（Infrastructure As A Service）へ全サーバを移行する検討を指示した。１年間の移行期間を経てサーバ室を廃止する前提である。この状況に関して，以下の問いに答えよ。

（１）移行する主なネットワーク基盤を挙げ，それぞれについて移行の概要を述べよ。

（２）移行後のネットワーク基盤の運用を想定し，Ａ社，Ｂ社とそれ以外のステークホルダにおける，運用体制とそれぞれの役割を述べよ。

（３）（１），（２）に関する技術的課題や留意点を３つ挙げ，それぞれについて，複数の解決案を述べよ。

Ⅲ－２　Ａ社ではサイバー攻撃や情報漏洩等の情報セキュリティインシデントの調査を少なくとも１年前まで遡って行えるようにするために，社内ネットワークとインターネットとの間の通信に関するログを適切に記録・保管することになった。プロキシサーバ及びファイアウォールの１日当たりのログのサイズを計測したところ，プロキシサーバでは約２Ｇバイトのログが生成され，ファイアウォールでは警告等の異常系ログのみを記録するように設定した場合は約１Ｇバイト，正常系ログも記録するように設定した場合は約４Ｇバイトのログが生成されることがわかった。Ａ社での検討に関して，以下の問いに答えよ。

（１）通信に関するログ以外で調査に有用なデータを少なくとも１つ例示し，有用性を説明せよ。

（２）プロキシサーバとファイアウォールのログ，及び（１）で挙げたデータの適切な記録・保管の方針について検討し，それを実現するためのログ等の設定要件とサーバ等の機器やネットワークに対する要件を示せ。

（３）これらのログ等を用いて情報セキュリティインシデントの早期発見を行えるようにするために，どのような手法やツールを導入すべきか提案せよ。