平成１９年度　秋期　テクニカルエンジニア（ネットワーク）　午後Ⅱ　解答例

問１

出題趣旨：

近年，日本においても，企業活動が適正に行われているかということを，企業自身が明らかにするための内部統制が注目されてきている。企業の活動は，コンピュータやネットワークを活用した IT 技術に支えられており，内部統制も IT 技術を活用したものにならざるを得ない。特にネットワークは，情報の受渡しのインフラを担っているので，企業活動の証拠又は履歴情報を残すというフォレンジックの観点で，重要な位置付けにある。

本問では，フォレンジックシステムを実現するに当たり，その中核となるフォレンジックサーバとネットワークをどのように構成して接続していくかを問う。

設問 1　(1) 要求を出した PC の IP アドレス

(2) アクセス元の IP アドレスはプロキシサーバのものとなり，要求を出した PC を識別できないから

(3) 内部又は社内からアクセスされたデータに絞り込めるから

設問 2　(1) ア　UDP
イ　IP-PBX
ウ　VoIP-GW
エ　標本化　又は　サンプリング　又は　シャノンの　又は　ナイキストの
オ　8

(2) RTP パケットから取得できる情報－VoIP-GW と IP 電話機の IP アドレス
SIP パケットからでないと取得できない情報－通話先電話番号と接続 IP 電話機の電話番号

(3) TOS 又はサービスタイプ

設問 3　(1)・信頼できる第三者による証明がないから
・時刻が改ざんされても分からないから

(2)①②
・転送途中で盗み見られても原本は知られない。
・転送するデータ量を削減できる。

(3)①②
・その時刻に存在していたこと
・その時刻以降に変更や改ざんが行われていないこと

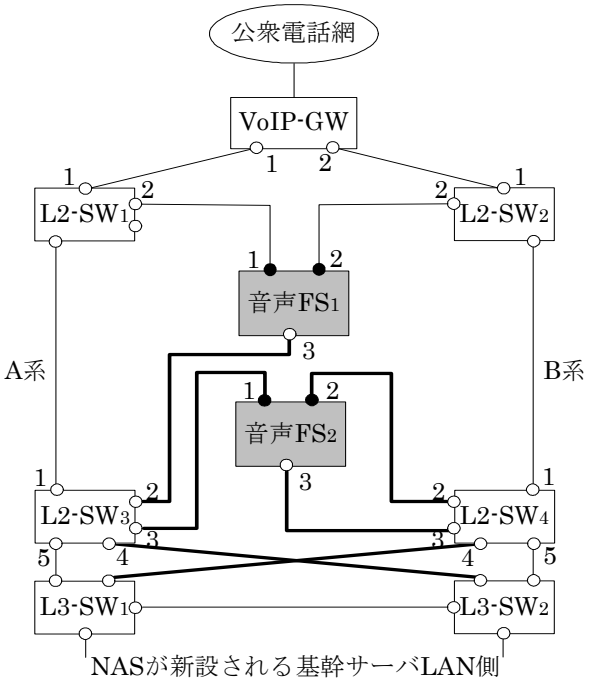
(4) ファイアウォールの設定変更が不要となる。

設問 4　(1) FS_1 から NAS に転送するデータのパケットも，FS_2 で採取するので FS_2 のデータ保存量が増大することについて，適切に記述していること（解答の要点を示す）

(2) 定められた保存期間内に削除されることを防止する。

(3) 保存するファイルのファイル名とハッシュ値を含む一覧表

設問５　(1) a－VRRP
(2) L2-SW_1の障害時に，採取した音声データをNASに送れない。
(3) 動的に通信経路を見つけることができないから
(4)



講評：
問１では，フォレンジックシステムの要件に基づく，サーバの設置方式，採取データの証拠性の確保及び障害に配慮したネットワーク接続構成について出題した。全体として，正答率は高かった。
設問 3(3)は，TST によって保証される存在証明と，完全性又は原本性について出題したが，“その時刻に存在していたこと”や“その時刻以降変更や改ざんが行われていないこと”といったタイムスタンプの時刻と，それを付与したデータの関係を明確に記述できた解答が少なかった。証拠性という観点でのタイムスタンプのもつ意味をよく理解してほしい。
設問 5(3)は，冗長な経路をもつネットワーク上で，VoIP-GW が転送用ポートを決定するための動作について出題したが，STP などの動的な経路制御が行われていないネットワークの構成ということに気付いていない解答が多かった。信頼性を高める冗長な経路をもつネットワークの動作に関して，理解を深めてほしい。

問２
出題趣旨：
IT 全般統制の一環として，ネットワークシステムの安全で安定した稼働が強く求められるようになった。対応策には，技術と人の両面からの取組がある。技術的な対応策を実施するためには，利用される技術の理解が不可欠である。
本問では，三つの技術的な対策を取り上げ，それらのシステムの機能と動作概要を記述し，記述された内容から，ネットワークエンジニアとしての経験と知識を基に，動作原理がどの程度理解できるかを問うことを主眼とした。
また，技術的な対策といえども必ずしも完全ではない。この対応は，システムの運用段階での人に依存する課題でもある。そこで，目的とする安全で安定した稼働に近づけるために，実施する技術的

な対策の限界をつかみ，人に依存する部分をどのような運用でコントロールするかを考える能力も，合わせて問う。

設問 1　a　導入作業又は構築作業　又は　インストール作業
b　ネットワークシステム運用管理規程
c　送信元 IP アドレス
d　IEEE
e　ログイン

設問 2（1）PC のハードディスクに差分データが蓄積されているので，バックアップが集中することについて，適切に記述していること（解答の要点を示す）
（2）ファイルを更新したにもかかわらず，何日間か，バックアップ時刻に社内 LAN に接続しないことについて，適切に記述していること（解答の要点を示す）

設問 3　禁止すべき通信－社内用メールサーバから中継用メールサーバへの通信
許可すべき通信－MF サーバから中継用メールサーバへの通信

設問 4（1）・DB に登録されている IP アドレスが使用された場合
・PC 情報が DB に登録された後，エージェントが削除された場合
（2）利用者が任意に変更できるから
（3）WF サーバ　又は　Web フィルタリングサーバ
（4）・WF サーバが接続されたポート
・L3-SW が接続されたポート
（5）通信を遮断すべき PC あてに，RST フラグをセットしたパケットを送る。

設問 5（1）作業 1－プロキシサーバの社内 LAN からの撤去
作業 2－USB メモリの使用制限の確認
（2）ア　中継用メールサーバ
イ　MF サーバ　又は　メールフィルタリングサーバ
ウ　遮断　又は　接続遮断
（3）デフォルトゲートウェイの IP アドレス
（4）本社のサーバを同一セグメントと判断して ARP を送出したが，ルータがプロキシ ARP で応答したので正常に通信ができたことについて，適切に記述していること（解答の要点を示す）

設問 6（1）サーバのデータをバックアップしたテープの保管を，遠隔地など災害を考慮した場所に変更することについて，適切に記述していること（解答の要点を示す）
（2）MF サーバに蓄積された不適正メールを適時にチェックし，情報漏えいの危険性がある場合，必要な処置を講じることについて，適切に記述していること（解答の要点を示す）

講評：
問 2 では，ネットワークシステムの機密性，完全性，可用性の確保を目的とした三つの技術的対策を例にとり，設計から運用までを出題した。全体として，正答率は高く期待どおりだった。
設問 4(5)は，TCP/IP 通信を妨害する基本的な方法について出題したが，的確に記述した解答は非常に少なかった。ネットワークシステムで，重要な課題になっているセキュリティ対策を考える上でも，TCP/IP の基本的な通信手順の理解が必要なので，もっと学んでほしい。
設問 5 では，導入システムの作業手順に従った導入項目の内容について出題した。(2)は，システ

ム導入時の二つの作業内容を解答させる問題で，問題文に記述された技術的なポイントを正しくつかめば解答を導き出せるが，作業2の正答率は低かった。問題文に記述された内容のポイントをつかみ，これを順序立てて整理する能力を身に付けてほしい。(4)は，ルータ経由で，エンド・ツー・エンドの通信を行うときの手順について出題したが，プロキシARPの働きがほとんど理解できていなかった。障害発生時の原因究明や，適切な対応策の立案のためには，TCP/IP通信の理解が重要である。

注：この解答例に関するメールでのご質問には、応じかねます。あしからずご了承ください。