問1　ネットワークの更改に関する次の記述を読んで，設問1～3に答えよ。

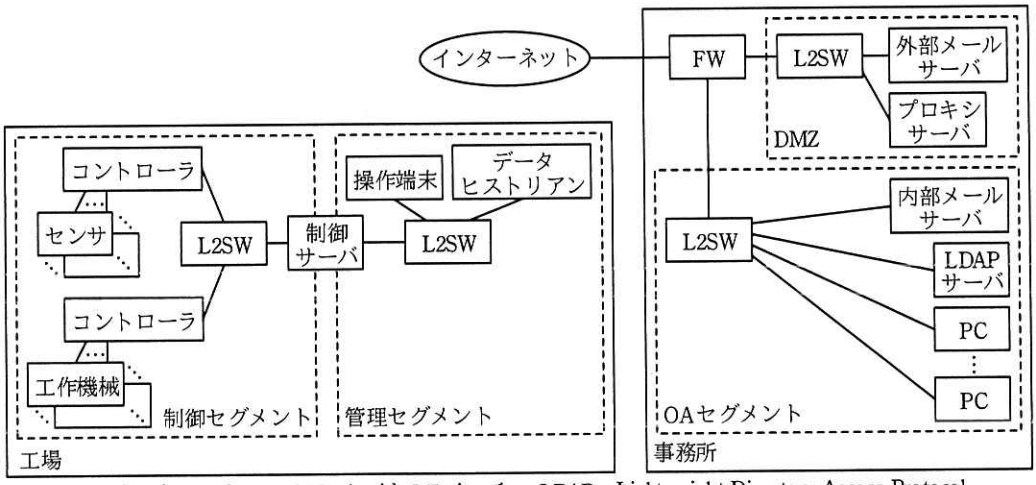
〔現状のネットワーク〕

A社は，精密機械部品を製造する中小企業であり，敷地内に事務所と工場がある。事務所には電子メール（以下，メールという）送受信やビジネス資料作成などのためのOAセグメントと，社外との通信を行うDMZが設置されている。工場には工作機械やセンサを制御するための制御セグメントと，制御サーバと操作端末のアクセスログ（以下，ログデータという）や制御セグメントからの測定データを管理するための管理セグメントが設置されている。

センサや工作機械を制御するコントローラの通信は制御セグメントに閉じた設計としているので，事務所と工場の間は，ネットワークで接続されていない。また制御セグメントと管理セグメントの間には，制御サーバが設置されているがルーティングは行わない。

操作端末は，制御サーバを介してコントローラに対し設定値やコマンドを送出する。コントローラは，常に測定データを制御サーバに送信する。制御サーバは，収集した測定データを，1日1回データヒストリアンに送る。データヒストリアンは，ログデータ及び測定データを蓄積する。

A社ネットワークの構成を，図1に示す。



FW：ファイアウォール　L2SW：レイヤ2スイッチ　LDAP：Lightweight Directory Access Protocol

図1　A社ネットワークの構成（抜粋）

ログデータの転送は，イベント通知を転送する標準規格（RFC 5424）の［ a ］プロトコルを利用している。データヒストリアンに蓄積された測定データとログデータは，ファイル共有プロトコルで操作端末に共有され，社員が USB メモリを用いて OA セグメント内の PC に 1 週間に 1 回複製する。

制御サーバ，操作端末及びデータヒストリアンのソフトウェア更新は，必要の都度，OA セグメントの PC でインターネットからダウンロードしたソフトウェア更新ファイルを，USB メモリを用いて操作端末に複製した上で実施される。

A 社の社員は，PC でメールの閲覧やインターネットアクセスを行う。OA セグメントからインターネットへの通信は DMZ 経由としており，DMZ には社外とのメールを中継する外部メールサーバと，OA セグメントからインターネットへの Web 通信を中継するプロキシサーバがある。DMZ にはグローバル IP アドレスが，OA セグメントにはプライベート IP アドレスがそれぞれ用いられている。

社員のメールボックスをもつ内部メールサーバと，プロキシサーバは，ユーザ認証のために LDAP サーバを参照する。プロキシサーバのユーザ認証には，Base64 でエンコードする Basic 認証方式と，MD5 や SHA-256 でハッシュ化する［ b ］認証方式があるが，A 社では後者の方式を採用している。また，プロキシサーバは，HTTP の［ c ］メソッドでトンネリング通信を提供し，トンネリング通信に利用する通信ポートを 443 に限定する。

〔ネットワークの更改方針〕

A 社では，USB メモリ紛失によるデータ漏えいの防止，測定データのリアルタイムの可視化，及び過去の測定データの蓄積のために，USB メモリの利用を廃止し，工場と事務所をネットワークで接続することにした。A 社技術部の B さんが指示された内容を次に示す。

(a) データヒストリアンにあるログデータを PC にファイル送信できるようにする。また PC にダウンロードしたソフトウェア更新ファイルを操作端末にファイル送信できるようにする。

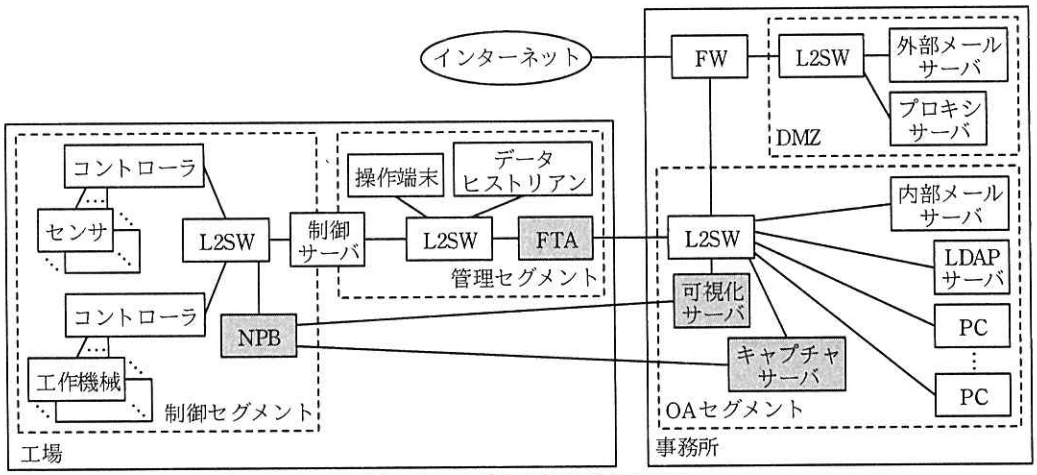
(b) 測定データの統計処理を行い時系列グラフとして可視化するサーバと，長期間の測定データを加工せずそのまま蓄積するサーバを OA セグメントに設置する。

(c) セキュリティ維持のために，工場の制御セグメント及び管理セグメントと，事

務所の OA セグメントとの間はルーティングを行わない。

B さんは，工場のネットワークを設計したベンダに実現方式を相談した。指示 (a) と (c) については，ファイル転送アプライアンス（以下，FTA という）がベンダから提案された。指示 (b) と (c) については，ネットワークパケットブローカ（以下，NPB という），可視化サーバ，キャプチャサーバがベンダから提案された。

B さんがベンダから提案を受けた，A 社ネットワークの構成を，図 2 に示す。



注記　網掛け部分は，ネットワーク更改によって追加される箇所を示す。

図 2　ベンダが提案した A 社ネットワークの構成（抜粋）

〔管理セグメントと OA セグメント間のファイルの受渡し〕

FTA は，分離された二つのネットワークでルーティングすることなくファイルの受渡しができるアプライアンスである。ファイルの送信者は，①FTA に Web ブラウザを使ってログインし，受信者を指定してファイルをアップロードする。ファイルの受信者は，FTA に Web ブラウザを使ってログインし，自身が受信者として指定されたファイルだけをダウンロードできる。

FTA の機能を使い，ファイルの受渡しの際に上長承認手続を必須にする。上長への承認依頼，受信者へのファイルアップロード通知は，FTA が自動的にメールを送信して通知する。承認は設定された上長だけが行うことができる。

B さんが検討した FTA の利用時の流れを，表 1 に示す。

表1　FTAの利用時の流れ

項番	概要	説明
1	アップロード	送信者は，FTA に HTTPS（HTTP over TLS）でアクセスし，PC 又は操作端末から FTA にファイルをアップロードする。
2	承認依頼	上長宛ての承認依頼メールが，FTA から内部メールサーバに自動送信される。
3	承認	上長は，PC でメールを確認後，FTA に HTTPS でアクセスし，ファイルの中身を確認した上で承認する。
4	ファイル アップロード通知	受信者宛てのファイルアップロード通知メールが，FTA から内部メールサーバに自動送信される。
5	ダウンロード	受信者は，PC でメールを確認後，FTA に HTTPS でアクセスし，ファイルを PC 又は操作端末にダウンロードする。

②指示(c)のとおり，FTA には静的経路や経路制御プロトコルの設定は行わない。

③FTAは，認証及び認可に必要な情報について，既存のサーバを参照する。

Bさんは，ベンダからFTAを借りて想定どおりに動作をすることを確認した。

〔測定データの可視化〕

NPB は事前に入力ポート，出力ポートを設定し，入力したパケットを複数の出力ポートに複製する装置である。NPB ではフィルタリングを設定して，複製するパケットを絞り込むことができる。可視化サーバは複製されたパケット（以下，ミラーパケットという）を受信して統計処理を行い，時系列グラフによって可視化をすることができる。キャプチャサーバは大容量のストレージをもち，ミラーパケットをそのまま長期間保存することができ，必要時にファイルに書き出すことができる。

Bさんは，NPBの動作の詳細についてベンダに確認した。Bさんとベンダの会話を次に示す。

Bさん：L2SWとNPBの転送方式は，何が違うのですか。

ベンダ：L2SW の転送方式では，受信したイーサネットフレームのヘッダにある送信元 MAC アドレスと L2SW の入力ポートを MAC アドレステーブルに追加します。フレームを転送するときは，宛先 MAC アドレスが MAC アドレステーブルに学習済みかどうかを確認した上で，学習済みの場合には学習されているポートに転送します。宛先 MAC アドレスが学習されていない場合は

[d] します。

これに対して NPB の転送方式では，入力ポートと出力ポートの組合せを事前に定義して通信路を設定します。今回のA社の構成では，一つの入力ポートに対して出力ポートを二つ設定し，パケットの複製を行っています。

NPBの入力は，L2SWからのミラーポートと接続する方法と，ネットワークタップと接続する方法の二つがあります。ネットワークタップは，既存の配線にインラインで接続し，パケットを NPB に複製する装置です。今回検討したネットワークタップを使う方法では，送信側，受信側，それぞれの配線でパケットを複製するので，NPBの入力ポートは2ポート必要です。④今回採用する方法では，想定トラフィック量が少ないので既存のL2SWのミラーポートを用います。NPB につながるケーブルは全て 1000BASE-SX です。

B さんは，ベンダへの確認結果を基に A 社における NPB による測定データの送信について整理した。その内容を次に示す。

・可視化サーバとキャプチャサーバを OA セグメントに設置する。
・コントローラは，更改前と同様に測定データを制御サーバに常時送信する。
・⑤制御セグメントに設置されている L2SW の特定ポートにミラー設定を行い，L2SW の該当ポートの送信側，受信側，双方のパケットを複製して NPB に送信させる。
・NPB は受信したミラーパケットを必要なパケットだけにフィルタリングした後に再度複製し，⑥可視化サーバとキャプチャサーバに送信する。

B さんは，FTA，NPB によるネットワーク接続方式を上司に説明し，承認を得た。

設問1　〔現状のネットワーク〕について，(1)，(2) に答えよ。

(1) 本文中の [a] ～ [c] に入れる適切な字句を答えよ。

(2) 外部からアクセスできるサーバを FW によって独立した DMZ に設置すると，OA セグメントに設置するのに比べて，どのようなセキュリティリスクが軽減されるか。40 字以内で答えよ。

設問２　〔管理セグメントと OA セグメント間のファイルの受渡し〕について，(1)～(3) に答えよ。

(1) 本文中の下線①について，利用者の認証を既存のサーバで一元的に管理する場合，どのサーバから認証情報を取得するのが良いか。図 2 中の字句を用いて答えよ。

(2) 本文中の下線②について，FTA にアクセスできるのはどのセグメントか。図 2 中の字句を用いて全て答えよ。

(3) 本文中の下線③について，FTA において認証と認可はそれぞれ何をするために使われるか。違いが分かるようにそれぞれ 25 字以内で述べよ。

設問３　〔測定データの可視化〕について，(1)～(5) に答えよ。

(1) 本文中の［　d　］に入れる適切な字句を答えよ。

(2) 本文中の下線④について，L2SW からミラーパケットで NPB にデータを入力する場合，ネットワークタップを用いて NPB にデータを入力する方式と比べて，性能面でどのような制約が生じるか。40 字以内で述べよ。

(3) 本文中の下線⑤について，1 ポートだけからミラーパケットを取得する設定にする場合には，どの装置が接続されているポートからミラーパケットを取得するように設定する必要があるか。図 2 中の字句を用いて答えよ。

(4) 本文中の下線⑥について，サーバでミラーパケットを受信するためにはサーバのインタフェースを何というモードに設定する必要があるか答えよ。また，このモードを設定することによって，設定しない場合と比べどのようなフレームを受信できるようになるか。30 字以内で答えよ。

(5) キャプチャサーバに流れるミラーパケットが平均 100 k ビット／秒であるとき，1,000 日間のミラーパケットを保存するのに必要なディスク容量は何 G バイトになるか。ここで，1 k ビット／秒は 10^3 ビット／秒，1 G バイトは 10^9 バイトとする。ミラーパケットは無圧縮で保存するものとし，ミラーパケット以外のメタデータの大きさは無視するものとする。