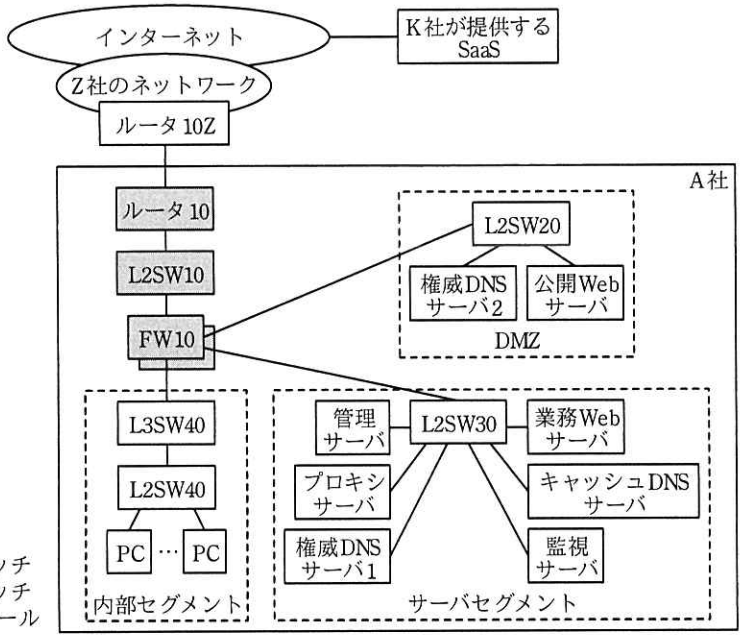
問2　インターネット接続環境の更改に関する次の記述を読んで，設問1～4に答えよ。

物品販売を主な事業とするA社は，近年，ネット通販に力を入れている。A社は，K社が提供するSaaSを利用して，顧客との電子メールやビジネスチャット，ファイル共有などを行っている。A社のシステム部では，老朽化に伴うA社インターネット接続環境の新しい機器への交換とインターネット接続の冗長化の検討を進めている。システム部門のB課長は，Cさんをインターネット接続環境の更改の担当者として任命した。

A社は，専用線を利用して，インターネットサービスプロバイダであるZ社を経由して，インターネットに接続している。現在のA社ネットワーク環境を図1に示す。



注記1　FWはクラスタ構成であり，物理的に2台のFWが論理的に1台のFWとして動作している。
注記2　□は，交換対象機器を示す。

図1　現在のA社ネットワーク環境（抜粋）

現在のA社ネットワーク環境の概要は次のとおりである。

・FWは，ステートフルパケットインスペクション機能をもつ。FWは，A社で必要な通信を許可し，必要のない通信を拒否している。

・FW は，許可又は拒否した情報を含む通信ログデータを管理サーバに SYSLOG で送信している。
・プロキシサーバは，従業員が利用する PC からインターネット向けの HTTP 通信及び HTTPS 通信をそれぞれ中継し，通信ログデータを管理サーバに SYSLOG で送信している。
・K 社が提供する SaaS との通信は全て HTTPS 通信である。
・管理サーバには，A 社のルータ，FW，L2SW 及び L3SW（以下，A 社 NW 機器という）から SNMP を用いて収集した通信量などの統計データ，FW とプロキシサーバの通信ログデータが保存されている。
・管理サーバは，通信ログデータを基に FW とプロキシサーバの通信ログ分析レポートを作成している。
・監視サーバは，A 社 NW 機器及びサーバを死活監視している。
・キャッシュ DNS サーバは，PC やサーバセグメントのサーバからの名前解決の問合せ要求に対して，他の DNS サーバへ問い合わせた結果，得られた情報を応答する。
・権威 DNS サーバ 1 は，A 社内の PC やサーバセグメントのサーバのホスト名などを管理し，名前解決の問合せ要求に対して PC やサーバセグメントのサーバなどに関する情報を応答する。
・サーバセグメントには，プライベート IP アドレスを付与している。
・サーバセグメントからインターネットに接続する際に，FW で NAPT による IP アドレスとポート番号の変換が行われる。
・内部セグメントには，プライベート IP アドレスを付与している。
・権威 DNS サーバ 2 は，A 社内の公開 Web サーバのホスト名などを管理し，名前解決の問合せ要求に対して公開 Web サーバなどに関する情報を応答する。
・DMZ には，グローバル IP アドレスを付与している。
・ルータ 10Z には，A 社が割当てを受けているグローバル IP アドレスの静的経路設定がされており，これを基に Z 社内部のルータに経路情報の広告を行っている。
・ルータ 10，FW10 及び L3SW40 の経路制御は静的経路制御を利用している。

C さんは，インターネット接続環境の更改の検討を進めるに当たり，まず，インタ

ーネット接続環境の利用状況を調査することにした。

〔インターネット接続環境の利用状況の調査〕

管理サーバは，SNMP を用いて，5 分ごとに A 社 NW 機器の情報を収集している。A 社 NW 機器のインタフェースの情報は，インタフェースに関する MIB によって取得できる。そのうち，インタフェースの通信量に関する MIB の説明を表 1 に示す。

表 1　インタフェースの通信量に関する MIB の説明（抜粋）

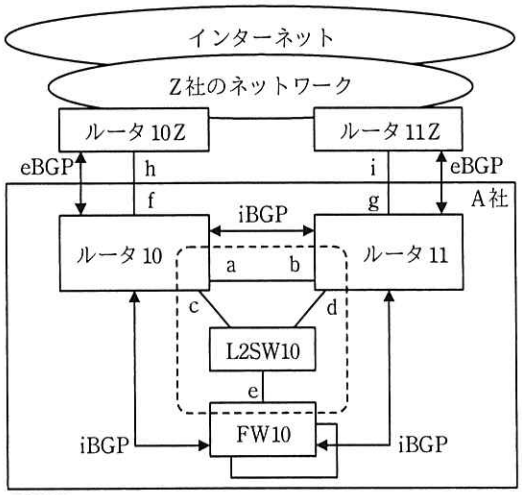
MIB の種類	説明
ifInOctets	インタフェースで受信したパケットの総オクテット数（32 ビットカウンタ）
ifOutOctets	インタフェースで送信したパケットの総オクテット数（32 ビットカウンタ）
ifHCInOctets	インタフェースで受信したパケットの総オクテット数（64 ビットカウンタ）
ifHCOutOctets	インタフェースで送信したパケットの総オクテット数（64 ビットカウンタ）

例えば，ifInOctets はカウンタ値で，電源投入によって機器が起動すると初期値の 0 から加算が開始され，インタフェースでパケットを受信した際にそのパケットのオクテット数が加算される。機器は，管理サーバから SNMP で問合せを受けると，その時点のカウンタ値を応答する。①管理サーバは，5 分ごとに SNMP でカウンタ値を取得し，単位時間当たりの通信量を計算し，統計データとして保存している。単位時間当たりの通信量の単位はビット／秒である。②カウンタ値が上限値を超える場合，初期値に戻って（以下，カウンタラップという）再びカウンタ値が加算される。通信量が多いとカウンタラップが頻繁に起きることから，インタフェースの通信量の情報を取得する場合には，32 ビットカウンタではなく，64 ビットカウンタを利用することが推奨されている。管理サーバに保存された統計データは，単位時間当たりの通信量の推移を示すトラフィックグラフとして参照できる。

統計データから，過去に何度か利用が増え，インターネットに接続する専用線に輻輳（ふくそう）が起きていたことが判明したので，専用線を増速する必要があると C さんは考えた。また，統計データと通信ログ分析レポートから交換対象機器の通信量や負荷の状態を確認した結果，ルータ 10 及び L2SW10 は同等性能の後継機種に交換し，FW10 は性能が向上した上位機種に交換すればよいと C さんは考えた。

〔インターネット接続の冗長化検討〕

C さんは，インターネット接続の冗長化方法について Z 社に提案を求めた。Z 社の提案は，動的経路制御の一つである BGP を用いた構成であった。Z 社の提案した構成を図 2 に示す。



各機器に付与されているアドレス一覧

機器名	インタフェース	IPアドレス/ネットマスク
ルータ10Z	h	α.β.γ.1/30
ルータ11Z	i	α.β.γ.5/30
ルータ10	a	α.β.γ.13/30
	c	α.β.γ.17/29
	f	α.β.γ.2/30
	ループバック	α.β.γ.8/32
ルータ11	b	α.β.γ.14/30
	d	α.β.γ.18/29
	g	α.β.γ.6/30
	ループバック	α.β.γ.9/32
FW10	e	α.β.γ.19/29

[- - -]：OSPFエリア
注記1　L2SWは冗長構成であるが，図では省略している。
注記2　a～iは，各機器の物理インタフェースを示す。
注記3　FWはクラスタ構成であり，物理的に2台のFWが論理的に1台のFWとして動作している。
注記4　表中のIPアドレスは，グローバルIPアドレスである。
注記5　◀――▶は，BGPピアを示す。

図 2　Z 社の提案した構成（抜粋）

Z 社の提案した構成の概要は次のとおりである。

・ルータ 10 側の専用線を増速する。また，新たに専用線を敷設して Z 社に接続する。新たに敷設する専用線を終端する機器として，ルータ 11 とルータ 11Z を設置する。ルータ 11 側の専用線の契約帯域幅は，ルータ 10 側の専用線と同じにする。

・平常時はルータ 10 側の専用線を利用し，障害などでルータ 10 側が利用できない場合は，ルータ 11 側を利用するように経路制御を行う。

・ルータ 10 とルータ 11 にはループバックインタフェースを作成し，これらに IP アドレスを設定する。

・a～e の各物理インタフェース及びループバックインタフェースでは，OSPF エリアを構成する。

・③ルータ 10 とルータ 11 はループバックインタフェースに設定した IP アドレスを利用し，FW10 は e に設定した IP アドレスを利用して，互いに iBGP のピアリングを行う。④ iBGP のピアリングでは，経路情報を広告する際に，BGP パスアトリビュートの一つである NEXT_HOP の IP アドレスを，自身の IP アドレスに書き換える設定を行う。

・ルータ 10 とルータ 10Z の間，及びルータ 11 とルータ 11Z の間では，eBGP のピアリングを行う。ピアリングには，f と h，及び g と i に設定した IP アドレスを利用する。

・eBGP のピアリングでは，A 社側はプライベート AS 番号である 64512 を，Z 社側はグローバル AS 番号である 64496 を利用する。

C さんは，Z 社の提案を受け，BGP の標準仕様について調査を行った。

BGP では，それぞれの経路情報に，パスアトリビュートの情報が付加される。BGP パスアトリビュートの一覧を表 2 に示す。

表 2　BGP パスアトリビュートの一覧（抜粋）

タイプコード	パスアトリビュート
2	AS_PATH
3	NEXT_HOP
4	MULTI_EXIT_DISC
5	LOCAL_PREF

AS_PATH は，経路情報がどの AS を経由してきたのかを示す AS 番号の並びである。eBGP ピアにおいて，隣接する AS に経路情報を広告する際に，AS_PATH に自身の AS 番号を追加する。また，⑤隣接する AS から経路情報を受信する際に，自身の AS 番号が含まれている場合はその経路情報を破棄する。

NEXT_HOP は，宛先ネットワークアドレスへのネクストホップの IP アドレスを示す。ネクストホップの IP アドレスは，ルータがパケットを転送する宛先を示す。eBGP ピアに経路情報を広告する際には，NEXT_HOP を自身の IP アドレスに書き換えて送信する。iBGP ピアに経路情報を広告する際には，NEXT_HOP を書き換えず，そのまま送信する。

MULTI_EXIT_DISC（以下，MED という）は，eBGP ピアに対して通知する，自身の AS 内に存在する宛先ネットワークアドレスの優先度である。MED はメトリックとも呼ばれる。

LOCAL_PREF は，iBGP ピアに対して通知する，外部の AS に存在する宛先ネットワークアドレスの優先度である。

BGP では，ピアリングで受信した経路情報を BGP テーブルとして構成する。この BGP テーブルに存在する，同じ宛先ネットワークアドレスの経路情報の中から，最適経路を一つだけ選択し，ルータのルーティングテーブルに反映する。A 社で利用している機器の最適経路選択アルゴリズムの仕様を表 3 に示す。

表 3　最適経路選択アルゴリズムの仕様

評価順	説明
1	LOCAL_PREF の値が最も大きい経路情報を選択する。
2	AS_PATH の長さが最も［　ア　］経路情報を選択する。
3	ORIGIN の値で IGP，EGP，Incomplete の順で選択する。
4	MED の値が最も［　イ　］経路情報を選択する。
5	eBGP ピアで受信した経路情報，iBGP ピアで受信した経路情報の順で選択する。
6	NEXT_HOP が最も近い経路情報を選択する。
7	ルータ ID が最も小さい経路情報を選択する。
8	ピアリングに使用する IP アドレスが最も小さい経路情報を選択する。

最適経路の選択は，表 3 中の評価順に行われる。例えば，同じ宛先ネットワークアドレスの経路情報が二つあった場合には，最初に，LOCAL_PREF の値を評価し，値に違いがあれば最も大きい値をもつ経路情報を選択し，評価を終了する。値に違いがなければ，次の AS_PATH の長さの評価に進む。

なお，ルータのルーティングテーブルに最適経路を反映するためには，NEXT_HOP の IP アドレスに対応する経路情報が，ルータのルーティングテーブルに存在し，ルータがパケット転送できる状態にある必要がある。

C さんは，以上の調査結果を基に Z 社の提案した構成を確認した。C さんと Z 社の担当者との会話は，次のとおりである。

C さん：専用線の経路制御はどのように行いますか。

担当者：今回は，LOCAL_PREF を利用して，図 2 中の各ルータ及び FW のパケット送信を制御します。ルータ 10Z とルータ 11Z が経路情報を受信した際に，LOCAL_PREF の値をそれぞれ設定し，Z 社内部の機器に経路情報の広告を行います。ルータ 10 とルータ 11 が経路情報を受信した際も同様に，LOCAL_PREF の値をそれぞれ設定し，A 社内部の機器に経路情報の広告を行ってください。

C さん：BGP で広告する経路情報はどのようなものですか。

担当者：ルータ 10Z とルータ 11Z はデフォルトルートの経路情報の広告を行います。ルータ 10 とルータ 11 は A 社が割当てを受けているグローバル IP アドレスの経路情報の広告を行ってください。平常時の FW10 の BGP テーブルは表 4 のように，ルーティングテーブルは表 5 のようになるはずです。

表 4　FW10 の BGP テーブル（抜粋）

宛先ネットワークアドレス	AS_PATH	MED	LOCAL_PREF	NEXT_HOP
0.0.0.0/0	64496	0	200	ウ
0.0.0.0/0	64496	0	100	エ

表 5　FW10 のルーティングテーブル（抜粋）

宛先ネットワークアドレス	ネクストホップ	インタフェース
0.0.0.0/0	$\alpha.\beta.\gamma.8$	e
$\alpha.\beta.\gamma.8/32$	オ	e
$\alpha.\beta.\gamma.9/32$	カ	e

C さん：分かりました。リンクダウンしないにもかかわらず，通信ができなくなるような専用線の障害時は，どのような動作になりますか。

担当者：BGP では，［　キ　］メッセージを定期的に送信します。専用線の障害時には，ルータが［　キ　］メッセージを受信しなくなることによって，ピアリングが切断され，AS 内の各機器の経路情報が更新されます。

C さん：分かりました。

担当者：ところで，⑥BGP の標準仕様ではトラフィックを分散する経路制御はできません。BGP マルチパスと呼ばれる技術を使うことで，平常時からルータ 10 側，ルータ 11 側両方の専用線を使って，トラフィックを分散する経路制御ができますがいかがですか。教えていただいた，今回利用を検討されている機器はどれも BGP マルチパスをサポートしています。BGP マルチパスを有効にすると，BGP テーブル内の LOCAL_PREF や AS_PATH，MED の値は同じで，NEXT_HOP だけが異なる複数の経路情報を，同時にルーティングテーブルに反映します。その結果，ECMP（Equal-Cost Multi-Path）によってトラフィックを分散することができます。

C さん：いいですね。では，BGP マルチパスを利用したいと思います。

担当者：承知しました。各機器の設定例を後ほどお渡ししますので参考にしてください。

C さん：ありがとうございます。

〔インターネット接続の冗長化手順〕

C さんは，冗長化作業中にインターネット利用に対する影響が最小限となる，インターネット接続の冗長化手順の検討を行った。C さんが検討した冗長化手順を表 6 に示す。

表 6　C さんが検討した冗長化手順

手順	作業対象機器	作業内容
手順 1	ルータ 11Z，ルータ 11	機器の設置
手順 2	ルータ 11Z，ルータ 11，ルータ 10，L2SW10	ケーブルの接続
手順 3	ルータ 11Z，ルータ 11，ルータ 10，L2SW10	物理インタフェースの設定，IP アドレスの設定及び疎通の確認
手順 4	ルータ 10，ルータ 11	ク
手順 5	ルータ 10，ルータ 11，FW10	ケ
手順 6	ルータ 10，ルータ 11，FW10	コ
手順 7	ルータ 10，ルータ 11，ルータ 10Z，ルータ 11Z	サ
手順 8	シ	静的経路の削除
手順 9	ルータ 10，L2SW10，FW10	後継機種又は上位機種に交換

手順 1，2 では，新たに導入する機器の設置及びケーブルの接続を行い，物理構成

を完成する。手順 3 では，作業対象機器の物理インタフェースの設定及び IP アドレスの設定を行い，機器間で疎通の確認を行う。疎通の確認では，ping を用いて，パケットロスが観測されないことを確認する。手順 4～7 で，BGP や OSPF を順次設定する。続いて，手順 8 を実施する。⑦A 社からインターネットへ向かう通信については，手順 8 の静的経路の削除が行われた時点で，動的経路による制御に切替えが行われ，冗長化が完成する。最後に，手順 9 では，インターネット利用に対する影響が最小限になるように機器を操作しながら，作業対象機器をあらかじめ設定を投入しておいた後継機種又は上位機種に交換する。例えば，ルータ 10 の交換に当たっては，⑧通信がルータ 10 を経由しないようにルータ 10 に対して操作を行った後に交換作業を実施する。

C さんは，これまでの検討結果をインターネット接続環境の更改案としてまとめ，B 課長に報告した。B 課長は，専用線に輻輳が発生していたこと，及び監視サーバで検知できなかったことを問題視した。想定外のネットワーク利用などによって突発的に発生した通信や輻輳を迅速に検知できるように，単位時間当たりの通信量の監視（以下，トラフィック監視という）について，C さんに検討するよう指示した。

〔トラフィック監視の導入〕

監視サーバの死活監視は，監視対象に対して，1 回につき ICMP のエコー要求を 3 パケット送信し，エコー応答を受信するかどうかを確認する。1 分おきに連続して 5 回，一つもエコー応答を受信しなかった場合に，アラートとして検知する。エコー要求のタイムアウト値は 1 秒である。C さんは，⑨専用線の輻輳を検知するために，監視サーバの監視対象として，ルータ 10Z とルータ 11Z を追加することを考えたが，問題があるため見送った。

そこで，C さんは，通信量のしきい値を定義し，上限値を上回ったり，下限値を下回ったりするとアラートとして検知する監視（以下，しきい値監視という）の利用を検討した。通信を均等に分散できると仮定すると，インターネット接続の冗長化導入によって利用できる帯域幅は専用線 2 回線分になる。どちらかの専用線に障害が発生すると，利用できる帯域幅は専用線 1 回線分になる。C さんは，どちらかの専用線に障害が発生した状況において，専用線に流れるトラフィックの輻輳の発生を避けるためには，平常時から，それぞれの専用線で利用できる帯域幅の

［　ス　］%を単位時間当たりの通信量の上限値としてしきい値監視すればよいと考えた。このしきい値監視でアラートを検知すると，トラフィック増の原因を調査して，必要であれば専用線の契約帯域幅の増速を検討する。

次に，C さんは，想定外のネットワーク利用などによって単位時間当たりの通信量が突発的に増えたり，A 社 NW 機器の故障などによって単位時間当たりの通信量が突発的に減ったりすること（以下，トラフィック異常という）を検知する監視の利用を検討した。C さんは機械学習を利用した監視（以下，機械学習監視という）の製品を調査した。

C さんが調査した製品は，過去に収集した時系列の実測値を用いて，傾向変動や周期性から近い将来の値を予測し，異常を検知することができる。例えば，単位時間当たりの通信量について，その予測値と新たに収集した実測値を基に，トラフィック異常を検知することができる。

C さんは，管理サーバに保存されている単位時間当たりの通信量の統計データを用いて，機械学習監視製品の試験導入を行った。C さんは，これまで検知できなかったトラフィック異常が検知できることを確認した。さらに，⑩管理サーバに保存されている，統計データとは別のデータについても，機械学習監視製品を用いて監視することで，トラフィック異常とは別の異常が検知できることを確認した。複数のデータを組み合わせて，機械学習監視製品を用いて監視することで，ネットワーク環境の状況を素早く，かつ，詳細に把握できることが分かった。

C さんは，機械学習監視製品の試験結果についてまとめ，B 課長に報告を行い，インターネット接続環境の更改に併せて，管理サーバにしきい値監視と機械学習監視製品を導入することが決まった。

その後，A 社では，C さんがまとめたインターネット接続環境の更改案を基に設備更改が実施され，また，しきい値監視と機械学習監視製品が導入された。

設問 1　〔インターネット接続環境の利用状況の調査〕について，(1)～(3) に答えよ。

(1) 本文中の下線①について，取得時刻 t におけるカウンタ値を X_t，取得時刻 t の 5 分前の時刻 t−1 におけるカウンタ値を X_{t-1} としたとき，t−1 と t の間における単位時間当たりの通信量（ビット／秒）を算出する計算式を答えよ。

ここで，1オクテットは8ビットとし，t−1とtの間でカウンタラップは発生していないものとする。

(2) 本文中の下線①について，利用状況の調査を目的として，単位時間当たりの通信量（ビット／秒）を求める際に時間平均することによる問題点を 35 字以内で述べよ。

(3) 本文中の下線②について，32 ビットカウンタでカウンタラップが発生した際に，通信量を正しく計算するためには，カウンタ値をどのように補正すればよいか。解答群の中から選び，記号で答えよ。ここで，取得時刻 t におけるカウンタ値を X_t，取得時刻 t の 5 分前の時刻 t−1 におけるカウンタ値を X_{t-1}，t−1 と t の間でカウンタラップが 1 回発生したとする。

解答群

ア　X_t を X_t+2^{32} に補正する。　　イ　X_t を $X_t+2^{32}-1$ に補正する。

ウ　X_{t-1} を $X_{t-1}+2^{32}$ に補正する。　　エ　X_{t-1} を $X_{t-1}+2^{32}-1$ に補正する。

設問2　〔インターネット接続の冗長化検討〕について，(1)〜(5)に答えよ。

(1) 本文中の下線③について，図 2 中のルータ 10 やルータ 11 にはループバックインタフェースを作成し，iBGP のピアリングにループバックインタフェースに設定した IP アドレスを利用するのはなぜか。FW10 とのインタフェースの数の違いに着目し，60 字以内で述べよ。

(2) FW10 のルーティングテーブルを表 7 に示す。本文中の下線④について，書き換える設定を行わない場合に，FW10 のルーティングテーブルに追加で必要になる情報はどのような内容か。表 5 を参考に，表 7 中の［ a ］，［ b ］に入れる適切な字句を答えよ。

表 7　FW10 のルーティングテーブル（抜粋）

宛先ネットワークアドレス	ネクストホップ	インタフェース
a	（設問のため省略）	e
b	（設問のため省略）	e

(3) 本文中の下線⑤について，経路情報を破棄する目的を 20 字以内で述べよ。

(4) 本文及び表 3〜5 中の［ ア ］〜［ キ ］に入れる適切な字句を答え

よ。

(5) 本文中の下線⑥について，BGP の標準仕様とはどのような内容か。本文中の字句を用いて 50 字以内で述べよ。

設問３　〔インターネット接続の冗長化手順〕について，(1)～(4) に答えよ。

(1) 表 6 中の［　ク　］～［　サ　］に入れる適切な字句を解答群の中から選び，記号で答えよ。

解答群

ア　eBGP の導入　　イ　iBGP の導入　　ウ　OSPF の導入

エ　ループバックインタフェースの作成と IP アドレスの設定

(2) 表 6 中の［　シ　］に入れる適切な機器名を，図 2 中の機器名で全て答えよ。

(3) 本文中の下線⑦について，静的経路の削除が行われた時点で，動的経路による制御に切替えが行われる理由を 40 字以内で述べよ。

(4) 本文中の下線⑧について，ルータ 10 に対して行う操作はどのような内容か。操作の内容を 20 字以内で述べよ。

設問４　〔トラフィック監視の導入〕について，(1)～(3) に答えよ。

(1) 本文中の下線⑨について，問題点を二つ挙げ，それぞれ 30 字以内で述べよ。

(2) 本文中の［　ス　］に入れる適切な数値を答えよ。

(3) 本文中の下線⑩について，統計データとは別のデータにはどのようなデータがあるか。本文中の字句を用いて 25 字以内で答えよ。また，そのデータを，機械学習監視製品を用いて監視することによって，どのようなトラフィック異常とは別の異常を検知できるようになるか。検知内容を 40 字以内で述べよ。