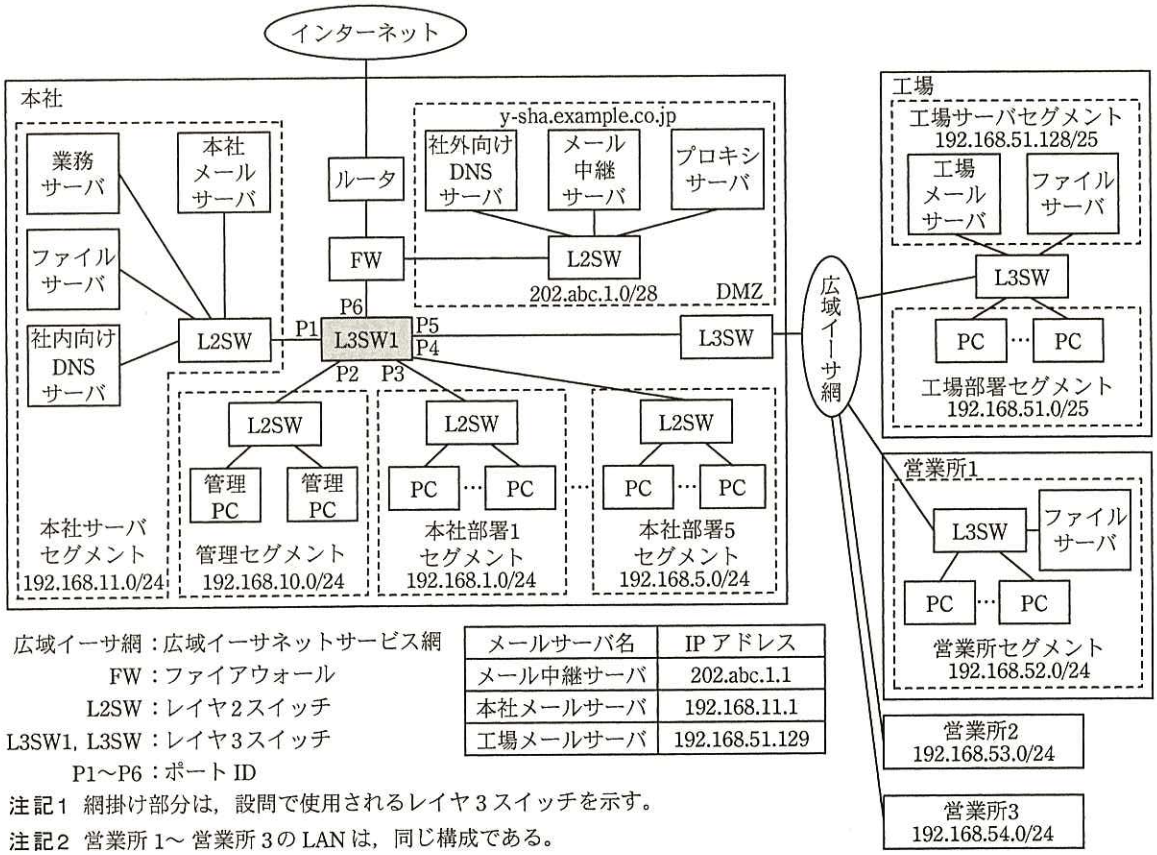
問1　標的型メール攻撃の対策に関する次の記述を読んで，設問1～5に答えよ。

Y社は，産業機械の製造会社であり，本社の他に，工場と3か所の営業所がある。Y社の先進的な技術によって製造された製品は，顧客から高い評価を受けている。この優位性を維持するために，Y社ではこれまで，知財情報，個人情報などの安全な管理に注力してきた。

Y社では，製品の設計，開発及び外注先・顧客との情報交換に，電子メール（以下，メールという）を活用している。Y社のネットワークシステム構成を，図1に示す。



広域イーサ網：広域イーサネットサービス網
FW：ファイアウォール
L2SW：レイヤ2スイッチ
L3SW1, L3SW：レイヤ3スイッチ
P1～P6：ポートID

メールサーバ名	IPアドレス
メール中継サーバ	202.abc.1.1
本社メールサーバ	192.168.11.1
工場メールサーバ	192.168.51.129

注記1　網掛け部分は，設問で使用されるレイヤ3スイッチを示す。
注記2　営業所1～営業所3のLANは，同じ構成である。
注記3　202.abc.1.0/28は，グローバルIPアドレスを示す。

図1　Y社のネットワークシステム構成

全社（本社，工場及び営業所）のネットワーク，サーバ及びPCのメンテナンスは，管理セグメントの管理PCを使用して行われている。各営業所には，当該営業所の営

業所員が使用するPCとファイルサーバが設置されている。管理PCを含む全社で使用されているPC（以下，全社のPCという）からインターネット上のWebサーバ，FTPサーバへのアクセスは，プロキシサーバを介してだけ可能である。本社と工場にはメールサーバが設置され，本社社員と営業所員は本社メールサーバで，工場社員は工場メールサーバで，メールの送受信を行っている。

メールの転送経路を，表1に示す。

表1　メールの転送経路

送信元	宛先	転送経路
本社，営業所	本社，営業所	PC → 本社メールサーバ
	工場	PC → 本社メールサーバ → 工場メールサーバ
	社外	PC → 本社メールサーバ → メール中継サーバ → 社外
工場	本社，営業所	PC → 工場メールサーバ → 本社メールサーバ
	工場	PC → 工場メールサーバ
	社外	PC → 工場メールサーバ → 本社メールサーバ → メール中継サーバ → 社外
社外	本社，営業所	社外 → メール中継サーバ → 本社メールサーバ
	工場	社外 → メール中継サーバ → 本社メールサーバ → 工場メールサーバ

最近，特定の企業，官公庁などを標的にして，その組織が保有する知財情報，個人情報などの重要な情報を窃取又は破壊する，標的型メール攻撃が増加してきた。この状況に対応するために，Y社では，標的型メール攻撃の対策を行うことにした。そこで，情報システム部のM部長は，セキュリティ担当のS主任とネットワーク担当のN主任に，対策案の検討を指示した。

S主任とN主任は，対策案の検討に先立ち，今後の進め方について打合せを行った。そのときの会話の一部を，次に示す。

S主任：標的型メール攻撃に対しては，マルウェアの侵入を防ぐ入口対策だけではなく，社内のLANに侵入したマルウェアの活動を抑えたり，活動を発見しやすくしたりする対策（以下，出口対策という）も必要になっているようだ。N主任には，ネットワークでの入口対策と出口対策を検討してもらって，私は，サーバとPCに必要なマルウェア対策と運用規程を見直すことにする。

N主任：了解した。検討後に対策案を持ち寄って，実施する対策について話し合おう。

N主任は，S主任との打合せの後，部下のJ君に，標的型メール攻撃の手法の調査と対策案の検討を指示した。

〔標的型メール攻撃の手法と対策案〕

J君は，標的型メール攻撃の手法の調査と対策案の検討を行った。

標的型メール攻撃の多くは，ソーシャルエンジニアリング手法で収集した攻撃対象者の情報を基に，（ア）攻撃対象者と関係がありそうな組織，機関及び実在の人物を装ったメールを送り付けてくる手法をとる。送り付けられたメールには，悪意のあるコード，マルウェアが埋め込まれたファイルが添付されていたり，マルウェアが仕込まれたWebサイトへのリンク先を示す［ a ］が本文に記載されていたりする。

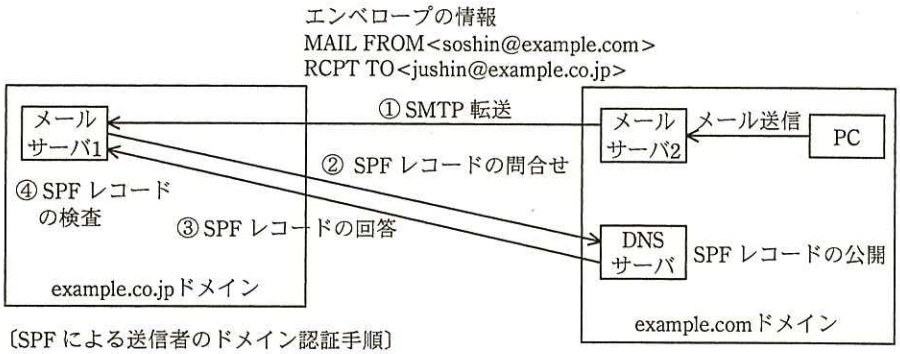
社内に侵入したマルウェアは，インターネット上の攻撃者のサーバとの通信路となるバックドアを開設して，攻撃基盤を構築することが多い。HTMLで作成されたコンテンツの送受信用プロトコルである［ b ］によってバックドアの通信が行われた場合，業務での通信との区別が困難である。マルウェアは，攻撃基盤を構築した後，システム内部への侵入を行い，拡散，重要情報の窃取，破壊などを行う。

SMTPでは，送信者が，自分自身のメールアドレスを容易に詐称することができる。しかし，送信元のMTA又はMUAが稼働するサーバ又はPCに設定されている［ c ］を書き換えることは困難である。そこで，（イ）ドメインを比較するだけでも，送信者のメールアドレスが詐称されているかどうかが，ある程度判別できる。

標的型メール攻撃の入口対策の一つとして，送信者のなりすましを検知する目的で開発された，送信ドメイン認証がある。送信ドメイン認証には，幾つかの手法があり，その中で，SPF（Sender Policy Framework）は，既存のネットワークシステムにも導入しやすい点が評価され，普及が進んでいる。

SPFでは，受信者が送信者のなりすましを検証するために，送信者のDNSの資源レコードにSPFレコードが追加されている必要がある。Y社でSPFを導入するときは，DMZの社外向けDNSサーバに，（ウ）メール中継サーバのIPアドレスを記述したSPFレコードを追加することになる。

SPFによる認証処理の概要を，図2に示す。



〔SPF による送信者のドメイン認証手順〕

① メールが，メールサーバ2からメールサーバ1に転送される。

② メールサーバ1は，エンベロープ中のメールアドレスを基に，DNS サーバにSPF レコードを問い合わせる。

③ DNSサーバから，SPF レコードが回答される。

④ メールサーバ 1 は，SPF レコードに登録されたメールサーバの IP アドレスを基に，受信したメールの正当性を検査する。不正なメールと判断したときには，受信したメールを廃棄又は隔離することができる。

図 2　SPF による認証処理の概要

J 君は，標的型メール攻撃の入口対策として，SPF を導入することを考えた。

SPF を導入しても，マルウェアの社内への侵入を完全に阻止することはできない。そこで，攻撃基盤の構築を困難にしたり，バックドアの通信を発見しやすくしたりする出口対策が重要になる。

J 君は，ネットワークにおける出口対策には，プロキシサーバでの対策と社内の LAN での対策が有効と考えた。プロキシサーバでの対策として，既設のプロキシサーバを，認証機能と，HTTPS で暗号化されたデータを復号する機能とをもつ機種に交換する。認証機能によって，マルウェアによるプロキシサーバ経由の通信を困難にさせるだけでなく，取得できるログの情報が増える。復号機能によって，SSL/TLS（以下，SSL という）通信でも，受信したデータ中に不適切な言葉や文字列などが含まれていたとき，その通信を遮断する [d] や，Web サーバからダウンロードされるファイルに対するウイルスチェックなどの，セキュリティ対策が行えるようになる。

社内の LAN での対策としては，図 1 中の L3SW1 にパケットフィルタリングを設定して，業務に不要な通信を遮断する。

J 君は，これらの検討結果を N 主任に報告した。そのときの N 主任と J 君の会話の

一部を，次に示す。

N 主任：SPF は入口対策として，容易に導入できそうだな。

J 君　：はい。機器の交換とか，新たな機器の導入は必要ありません。

N 主任：出口対策も効果がありそうだ。しかし，プロキシサーバが SSL を終端できると中間者攻撃が可能になってしまうので，復号機能の実現方法を調べてくれないか。パケットフィルタリングについては，具体的に検討してみなさい。

J 君　：分かりました。早速，調査・検討してみます。

〔プロキシサーバの復号機能の実現方法〕

まず，J 君は，プロキシサーバの復号機能の実現方法について調査した。

PC は，Web サーバとの間で SSL 通信を行うときには，プロキシサーバ宛てに connect 要求を送信する。復号機能をもたない既設のプロキシサーバの場合，受信した connect 要求に含まれる接続先サーバとの間で，指定された宛先ポート番号に対して TCP コネクションを確立する。その後，プロキシサーバは PC に connect 応答を送信して，それ以降に受信した TCP データをそのまま接続先に転送する，[e] 処理の準備が整ったことを知らせる。

復号機能をもつプロキシサーバの場合，PC からの connect 要求を受信した後の動作は，次のようになる。

復号機能をもつプロキシサーバの動作手順の概要を，図 3 に示す。

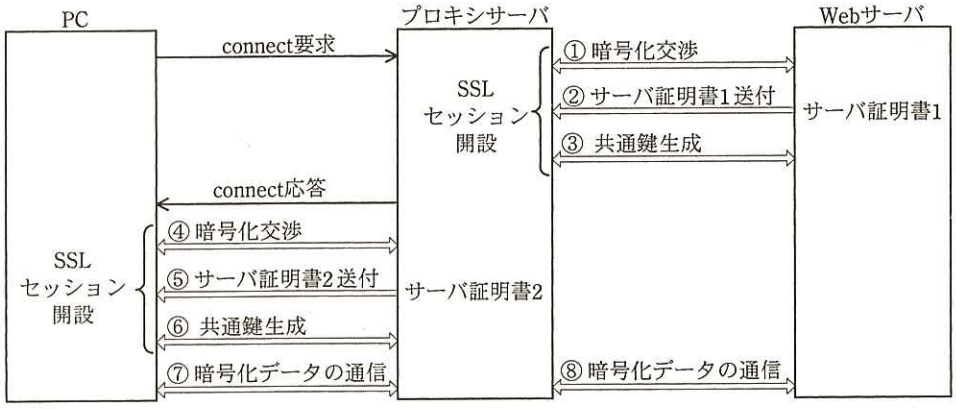


図 3　復号機能をもつプロキシサーバの動作手順の概要

図 3 に示したように，PC からの connect 要求を受信したプロキシサーバは，まず，①～③の手順で Web サーバとの間で SSL セッションを開設し，更に PC との間でも，④～⑥の手順で SSL セッションを開設する。このとき，⑤で，プロキシサーバは，サブジェクト（Subject）に含まれるコモン名（CN：Common Name）に，サーバ証明書 1 と同じ情報をもたせたサーバ証明書 2 を生成して，PC 宛てに送信する。PC はサーバ証明書 2 を検証し，認証できたときに⑥が行われ，SSL セッションが開設される。ここで，PC がサーバ証明書 2 を正当なものと判断してプロキシサーバを認証するためには，PC に，（エ）サーバ証明書 2 を検証するのに必要な情報を保有させる必要がある。

なお，仮に，図 3 中の⑤で，プロキシサーバが Web サーバから取得したサーバ証明書 1 を PC に送信した場合，PC によるプロキシサーバの認証は成功する。しかし，（オ）⑥において，プリマスタシークレット（Premaster Secret）の共有に失敗するので，このような方法で SSL セッションを開設することはできない。

調査の結果，J 君は，プロキシサーバの復号機能の実現方法を確認できたので，次のステップとして，社内の LAN におけるセグメント間のパケットフィルタリングについて検討した。

〔パケットフィルタリングの検討〕

パケットフィルタリングの検討に当たって，J 君は，業務における各サーバの利用状況を調査し，用途とアクセス元を表 2，3 にまとめた。表 2 は，DMZ で稼働しているサーバの用途とアクセス元を，表 3 は，DMZ 以外で稼働しているサーバの用途とアクセス元をまとめたものである。

表 2　DMZ で稼働しているサーバの用途とアクセス元

サーバ名	用途	アクセス元
社外向け DNS サーバ	y-sha.example.co.jp ドメインのゾーン情報の管理	社外 社内向け DNS サーバ
メール中継サーバ	社外から Y 社宛てに送信されるメールの中継 Y 社から社外宛てに送信されるメールの中継	社外 本社メールサーバ
プロキシサーバ	全社の PC による社外の Web サイトへのアクセスの代理処理	全社の PC

表3　DMZ以外で稼働しているサーバの用途とアクセス元

設置場所	サーバ名	用途	アクセス元
本社サーバセグメント	本社メールサーバ	本社社員と営業所員のメールボックスの保持	本社と営業所のPC[1)] メール中継サーバ 工場メールサーバ
	業務サーバ	全社員向けの各種業務処理サービスの提供	全社のPC
	ファイルサーバ	本社社員と営業所員向けのファイルサービスの提供	本社と営業所のPC[1)]
	社内向けDNSサーバ	全社のPC及びメールサーバからの名前解決要求への応答	全社のPC メール中継サーバ 本社メールサーバ 工場メールサーバ
工場サーバセグメント	工場メールサーバ	工場社員のメールボックスの保持	工場のPC 本社メールサーバ
	ファイルサーバ	工場社員向けのファイルサービスの提供	工場のPC
各営業所	ファイルサーバ	営業所員向けのファイルサービスの提供	当該営業所のPC

注[1)]　本社と営業所のPCは，管理PCを含んでいる。

次に，表2，3の情報を基に，マルウェアの拡散を阻止するためのパケットフィルタリングポリシを，図4にまとめた。

①PCからサーバへの業務用通信及びサーバ間の業務用通信を，表2，3どおり許可する。
②上記①に加え，業務用通信区間における疎通テストのための通信を許可する。
③管理PCについては，上記①，②の他に，他のセグメントのPC及びサーバへのリモート接続と疎通テストのための通信を許可する。
④上記①～③以外の通信を禁止する。

図4　パケットフィルタリングポリシ

その後，図4を基に，パケットフィルタリングルールを検討した。

J君が検討してまとめた，ポートA，Bに設定するパケットフィルタリングルールを，表4，5に示す。ここで，ポートA，Bは，L3SW1のP1～P6のいずれかのポートであるが，設問の関係でどのポートかは明記しない。

表4　ポートAに設定するパケットフィルタリングルール

項番	動作	送信元 IPアドレス	宛先 IPアドレス	プロトコル	送信元 ポート番号	宛先 ポート番号	TCP 制御ビット
1	許可	192.168.1.0/24	192.168.11.0/24	TCP	any	any	any
2	許可	192.168.1.0/24	192.168.11.0/24	ICMP	any	any	any
3	禁止	192.168.1.0/24	192.168.10.0/24	TCP	any	any	SYN=1 ACK=0
4	許可	192.168.1.0/24	192.168.10.0/24	TCP	any	any	any
5	許可	192.168.1.0/24	192.168.10.0/24	ICMP	any	any	any
6	許可	192.168.1.0/24	202.abc.1.0/28	TCP	any	any	any
7	許可	192.168.1.0/24	202.abc.1.0/28	ICMP	any	any	any
8	禁止	any	any	any	any	any	any

注記1　anyは，パケットフィルタリングにおいてチェックしないことを示す。
注記2　パケットフィルタリングルールは，項番の小さい順に参照され，最初に該当したルールが適用される。

表5　ポートBに設定するパケットフィルタリングルール

項番	動作	送信元 IPアドレス	宛先 IPアドレス	プロトコル	送信元 ポート番号	宛先 ポート番号	TCP 制御ビット
1	許可	192.168.10.0/24	192.168.48.0/21	TCP	any	any	any
2	許可	192.168.10.0/24	192.168.48.0/21	ICMP	any	any	any
3	許可	192.168.11.0/24	192.168.51.128/25	TCP	any	any	any
4	許可	192.168.11.0/24	192.168.51.128/25	UDP	53	any	any
（省略）							
10	禁止	202.abc.1.0/28	192.168.51.128/25	any	any	any	any
11	禁止	202.abc.1.0/28	192.168.48.0/21	TCP	any	any	SYN=1 ACK=0
12	許可	202.abc.1.0/28	192.168.48.0/21	TCP	any	any	any
13	許可	202.abc.1.0/28	192.168.48.0/21	ICMP	any	any	any
14	禁止	any	any	any	any	any	any

注記1　anyは，パケットフィルタリングにおいてチェックしないことを示す。
注記2　パケットフィルタリングルールは，項番の小さい順に参照され，最初に該当したルールが適用される。

J君は，全ての調査・検討が終了した後，プロキシサーバの復号機能の実現方法と，パケットフィルタリングルールの内容をN主任に説明した。説明を聞いたN主任は，プロキシサーバの復号機能については中間者攻撃に対して安全であることを了解した。しかし，パケットフィルタリングルールの内容については，（カ）表4にルールの漏れが一つあるので，項番1，2の間に追加するよう指示した。

〔入口対策と出口対策の実施項目〕

N主任は，J君の報告を基に対策案をまとめ，実施に移す対策（以下，実施策という）についてS主任と打合せを行った。そのときのN主任とS主任の会話を，次に示す。

N主任：ネットワークでの入口対策と出口対策の案をまとめた。入口対策としては，SPFを導入する。出口対策としては，既設のプロキシサーバを認証機能と復号機能をもつ機種に交換し，L3SW1にパケットフィルタリングを設定する。

S主任：分かった。私の方では，サーバ，PC及びFWでのマルウェア対策の実施状況について調査したところ，ウイルス対策ソフトの運用とセキュリティパッチの適用は，運用規程どおり実施されていた。また，FWでは，社内のLANからインターネットへの不必要な通信の遮断設定が適切に行われていた。しかし，不審なメールへの対応と，社内に侵入したマルウェアの活動を発見する

ためのログの検査が，適切には行われていなかった。今後，不審なメールへの対応に関する規程を定め，ログの検査方法・検査内容を見直すことにする。

N 主任：プロキシサーバの交換で，マルウェアの活動を発見しやすくなるな。

S 主任：そうだな。プロキシサーバで利用者認証を行えば，マルウェアによるバックドアの通信路の開設を困難にできるだけでなく，バックドアの通信が発見しやすくなる。セキュリティチームで，認証効果を高めるための全社の PC への対策と，プロキシサーバのログの定期的な検査を行うことにする。

N 主任：それでは，2 人の検討結果をまとめて，M 部長に提案しよう。

N 主任と S 主任は，検討結果を基に，次の 6 項目から成る標的型メール攻撃に対する実施策をまとめ，M 部長に提出した。

・図 1 のネットワークシステムに SPF を導入する。
・プロキシサーバを交換し，プロキシサーバで利用者認証を行うとともに，復号機能を利用して SSL 通信に対してもセキュリティ対策を行う。
・L3SW1 で，セグメント間のパケットフィルタリングを行う。
・プロキシサーバの認証効果を高めるために，PC の Web ブラウザの設定を変更する。
・(キ) 利用者が不審メールを発見したときの対応に関する規程を定め，運用規程に組み入れる。
・プロキシサーバのログの検査方法・検査内容を見直し，(ク) ログの検査間隔を可能な限り短縮して，定期的に検査を行う。

実施策が承認され，N 主任と S 主任は，ネットワークシステムの変更及び運用の見直しを進めることにした。

設問 1　本文中の [a] ～ [e] に入れる適切な字句を答えよ。

設問 2　〔標的型メール攻撃の手法と対策案〕について，(1) ～ (4)に答えよ。

(1) 本文中の下線（ア）のメールによって，メール送信者が誘導しようとする受信者の行動を，40 字以内で述べよ。

(2) 本文中の下線（イ）で，比較する二つのドメインを，50 字以内で述べよ。

(3) 本文中の下線（ウ）について，Y 社には 3 台のメールサーバがあるが，その

中でメール中継サーバのIPアドレスを記述する理由を，30字以内で述べよ。

(4) Y社でSPFを導入するとき，社外向けDNSサーバへのSPFレコードの追加とともに，SPFによる認証処理を実施することになる。その認証処理を実施させるサーバ名を，図1中の名称で答えよ。また，認証処理を正しく行うには，そのサーバでなければならない理由を，30字以内で述べよ。

設問3 〔プロキシサーバの復号機能の実現方法〕について，(1)～(3)に答えよ。

(1) 既設のプロキシサーバの場合，SSLセッションはどの機器間で開設されるかを，図3中の名称で答えよ。

(2) 本文中の下線（エ）の情報を，20字以内で答えよ。

(3) 本文中の下線（オ）について，失敗する理由を，40字以内で述べよ。

設問4 〔パケットフィルタリングの検討〕について，(1)～(4)に答えよ。

(1) 表4，5のパケットフィルタリングルールを適用するポートA，Bを，図1中のポートIDで答えよ。また，通信の方向を，IN又はOUTで答えよ。

(2) 表4中の項番2のパケットフィルタリングルールの目的を，25字以内で述べよ。

(3) 本文中の下線（カ）で，N主任が表4への追加を指示したパケットフィルタリングルールを，表4の記述方法で答えよ。

(4) 表4中の項番3，4の二つのパケットフィルタリングルールによって制御される通信の内容を，70字以内で述べよ。

設問5 〔入口対策と出口対策の実施項目〕について，(1)～(3)に答えよ。

(1) プロキシサーバの交換によって，新たにログとして取得できる情報について，60字以内で述べよ。

(2) 本文中の下線（キ）で定めるべき規程の内容を三つ挙げ，それぞれ30字以内で述べよ。

(3) 本文中の下線（ク）によって期待される効果を，30字以内で述べよ。