NW

令和元年度　秋期
ネットワークスペシャリスト試験
午後Ⅱ　問題

試験時間	14:30 ～ 16:30（2時間）

注意事項

1. 試験開始及び終了は，監督員の時計が基準です。監督員の指示に従ってください。
2. 試験開始の合図があるまで，問題冊子を開いて中を見てはいけません。
3. **答案用紙への受験番号などの記入は，試験開始の合図があってから始めてください。**
4. 問題は，次の表に従って解答してください。

問題番号	問1，問2
選択方法	1問選択

5. 答案用紙の記入に当たっては，次の指示に従ってください。
   (1) B又はHBの黒鉛筆又はシャープペンシルを使用してください。
   (2) **受験番号欄**に**受験番号**を，**生年月日欄**に**受験票の生年月日**を記入してください。正しく記入されていない場合は，採点されないことがあります。生年月日欄については，受験票の生年月日を訂正した場合でも，訂正前の生年月日を記入してください。
   (3) **選択した問題**については，次の例に従って，**選択欄**の**問題番号**を**○印**で囲んでください。○印がない場合は，採点されません。2問とも○印で囲んだ場合は，はじめの1問について採点します。
   (4) 解答は，問題番号ごとに指定された枠内に記入してください。
   (5) 解答は，丁寧な字ではっきりと書いてください。読みにくい場合は，減点の対象になります。

〔問2を選択した場合の例〕

選択欄	
1問選択	問1
	(問2)

注意事項は問題冊子の裏表紙に続きます。
こちら側から裏返して，必ず読んでください。

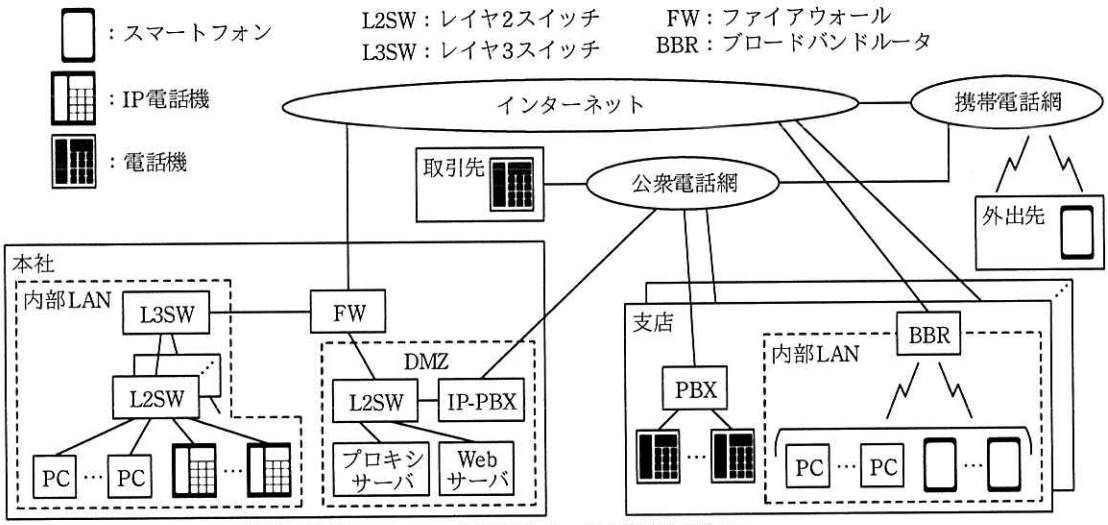
問1　クラウドサービスへの移行に関する次の記述を読んで，設問1～4に答えよ。

D社は，本社及び複数の支店をもつ中堅の運送事業者である。ファイアウォール，Webサーバ，プロキシサーバ，IP-PBX，PBXなどから構成されているD社システムを使って，社内外の通信と運送管理業務を行っている。

D社の情報システム部は，D社システムの老朽化に伴い，システムの更改を検討中である。

〔現行のD社システム〕

現行のD社システムの構成を図1に示す。



注記　ネットワーク及び機器の接続について，中継要素の一部を省略している。

図1　現行のD社システムの構成（抜粋）

図1の概要を次に示す。

(1) 全社のPCから，本社のWebサーバ及びインターネットにアクセスする。

(2) 本社のPCからインターネットへのアクセスは，プロキシサーバを経由する。

(3) 支店のPCから本社のWebサーバへのアクセスは，インターネットを経由する。

(4) 本社のDMZ及び全社の内部LANはプライベートIPアドレスで運用されてお

り，FW と BBR では NAT 機能及び NAPT 機能が動作している。例えば，上記 (2) 中のインターネットへのアクセスでは，FW の NAPT 機能によって，IP パケット中のプロキシサーバの IP アドレスが変換される。同様に，上記 (3) 中のインターネット経由の Web サーバへのアクセスでは，BBR の NAPT 機能によって IP パケット中の［　ア　］の IP アドレスが変換される。さらに，［　イ　］の NAT 機能によって，IP パケット中の Web サーバの IP アドレスが変換される。

(5) IP-PBX は SIP サーバの機能をもつ。また，IP 電話機，及び電話用ソフトウェア（以下，SIP-AP という）を搭載したスマートフォン（以下，スマホという）は SIP ユーザエージェント（以下，SIP UA という）として機能する。IP 電話機及び SIP-AP の間では，SIP プロトコルによる接続制御によって通話セッションが確立し，RTP プロトコルによる通話が行われる。

(6) SIP UA が IP-PBX に位置情報登録を依頼する際，SIP UA は SIP メソッド［　ウ　］を使ってリクエストを行う。その際，［　エ　］を認証するために“HTTP ダイジェスト認証方式”が用いられる。認証情報がないリクエストを受け取った IP-PBX はチャレンジ値を含むレスポンス“401 Unauthorized”を返す。SIP UA はチャレンジ値から生成した正しいレスポンス値を送り，IP-PBX はレスポンス“［　オ　］”を返す。

(7) 一部の支店ではスマホを社員に貸与し，次のように利用させている。

・支店では，BBR，インターネット及び FW を経由して，スマホの Web ブラウザから本社の Web サーバへアクセスする。また，<u>①同様に FW を経由して，スマホの SIP-AP と本社の IP 電話機間で通話を行う</u>。

・外出先では，携帯電話網，インターネット及び FW を経由して，スマホの Web ブラウザから本社の Web サーバへアクセスする。また，スマホの SIP-AP から取引先への電話については，本社の公衆電話網の電話番号からの発信となるように，携帯電話網，インターネット，FW 及び［　カ　］を経由させる。

B さんは情報システム部のネットワーク担当である。情報システム部長から指示があり，D 社システム更改のネットワークに関する検討を行っている。

B さんに伝えられた D 社システム更改の方針を次に示す。

(1) 運用負荷の軽減

・IaaS を利用し，本社の FW，Web サーバ及びプロキシサーバを撤去する。

・クラウド PBX サービスを利用し，本社の IP-PBX 及び支店の PBX を撤去する。

・無線 LAN 及び PoE（Power over Ethernet）を利用し，構内配線を減らす。

(2) スマホの活用

・全社員にスマホを貸与し，全社及び外出先で，電話機及び PC を補完する機器として利用させる。

(3) 新システムへの段階的移行

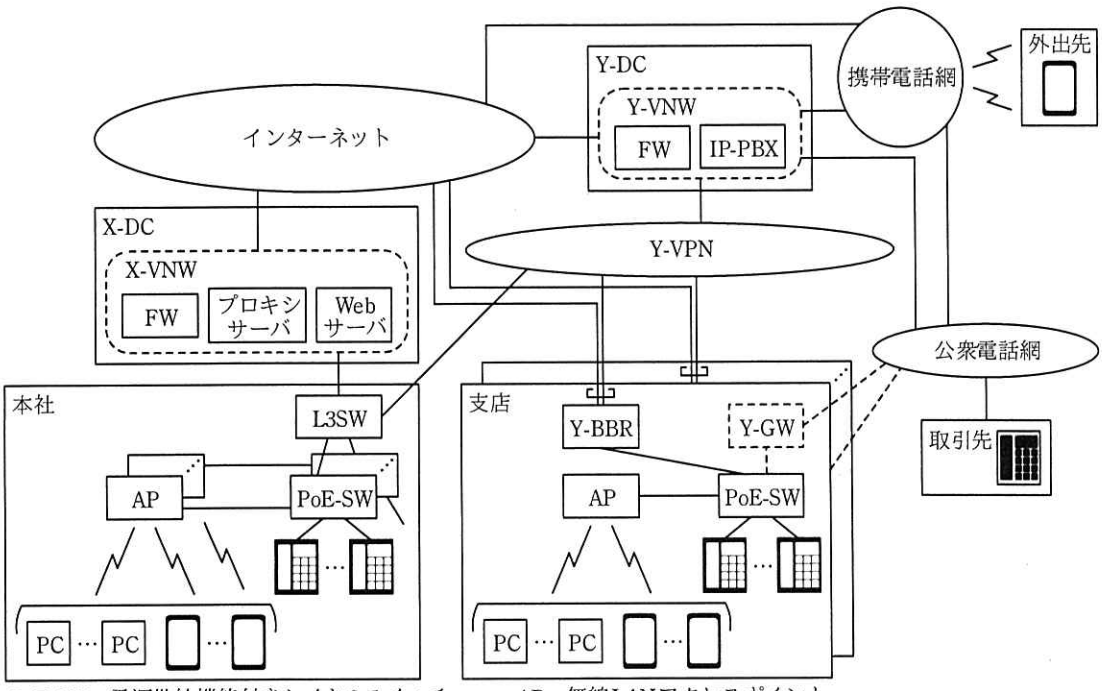
・現行システムから新システムへの切替えは，拠点単位に段階的に行う。

〔クラウドサービスの利用〕

D 社システムの更改では，X 社が提供する IaaS と，Y 社が提供するクラウド PBX サービスを利用する。利用するクラウドサービスの概要を表 1 に，B さんが考えた新 D 社システムの構成を図 2 に，それぞれ示す。

表 1　利用するクラウドサービスの概要

サービス名	説明
IaaS	X 社のデータセンタ（以下，X-DC という）内に，D 社の仮想 LAN（以下，X-VNW という）と仮想サーバを構成する。 次のオプションサービスを利用する。 ・インターネット接続：X-VNW 内に FW を構成し，X-VNW とインターネットを接続する。 ・専用線接続：イーサネット専用線を使って，本社と X-VNW を接続する。
クラウド PBX サービス	Y 社のデータセンタ（以下，Y-DC という）内に，D 社の仮想 LAN（以下，Y-VNW という），IP-PBX 及び FW を構成する。IP-PBX は，インターネット，携帯電話網，公衆電話網及び Y 社の閉域網（以下，Y-VPN という）と接続する。 次のオプションサービスを利用する。 ・専用線接続：イーサネット専用線を使って，本社と Y-VPN を接続する。 ・PPPoE（Point-to-Point Protocol over Ethernet）接続：Y 社のブロードバンドルータ（以下，Y-BBR という）を支店に設置し，PPPoE を用いて，支店を Y-VPN 及びインターネットに接続する。 ・ゲートウェイ接続：Y 社のゲートウェイ（以下，Y-GW という）を一部の支店に設置し，支店を公衆電話網に接続する。 ・SIP-AP の利用：スマホに Y 社のクラウド PBX サービス用の SIP-AP を搭載し，電話機と同じような操作を可能にする。



PoE-SW：電源供給機能付きレイヤ2スイッチ　　AP：無線LANアクセスポイント

注記1　Y-GW を設置しない支店がある。

注記2　ネットワーク及び機器の接続について，中継要素の一部を省略している。

図2　Bさんが考えた新D社システムの構成（抜粋）

図2中のネットワークについてBさんが整理した内容を次に示す。

(1) Y-BBR は，二つの PPPoE セッションを提供する。一つはインターネット接続に，もう一つはクラウド PBX サービス利用に用いられる。

(2) Y-VPN は，Y社のクラウド PBX サービスを利用する顧客が共用する IP-VPN である。RFC 3031 で標準化されている［　キ　］の技術が用いられている。

(3) D 社の異なる拠点間の通話が他の拠点を経由しないように，Y-VPN の網内は［　ク　］構成となっている。

(4) 新たに構成する，X-VNW，Y-VNW 及び全社の内部 LAN の IP アドレスは，現行のプライベート IP アドレスとは重ならないアドレス空間を利用する。

(5) 全社の内部 LAN では静的ルーティングを用いる。全社の AP はブリッジモードで動作させ，PC とスマホを収容する。収容端末の IP アドレス及びデフォルトゲートウェイの IP アドレスは，AP の DHCP 機能を使って配布する。本社の収容端末のデフォルトゲートウェイは L3SW，支店の収容端末のデフォルトゲート

ウェイは［　ケ　］である。

(6) 電話に関する図2中の通信経路を表2に示す。

表2　電話に関する図2中の通信経路（抜粋）

項番	発信	着信	通信経路
1-1	本社の IP 電話機	本社の IP 電話機	シグナリング：本社～Y-VPN～Y-VNW～Y-VPN～本社 通話：本社
1-2		支店の IP 電話機	シグナリング：本社～Y-VPN～Y-VNW～Y-VPN～支店 通話：本社～Y-VPN～支店
1-3		取引先の電話機	シグナリング・通話共：本社～Y-VPN～Y-VNW～公衆電話網～取引先
2-1	支店の IP 電話機	取引先の電話機	シグナリング・通話共：支店～Y-VPN～Y-VNW～公衆電話網～取引先
2-2			シグナリング：支店～Y-VPN～Y-VNW～Y-VPN～支店～公衆電話網～取引先 通話：支店～公衆電話網～取引先
3-1	本社の スマホ	本社の IP 電話機	シグナリング：本社～Y-VPN～Y-VNW～Y-VPN～本社 通話：本社
3-2	支店の スマホ		シグナリング：支店～Y-VPN～Y-VNW～Y-VPN～本社 通話：［　a　］

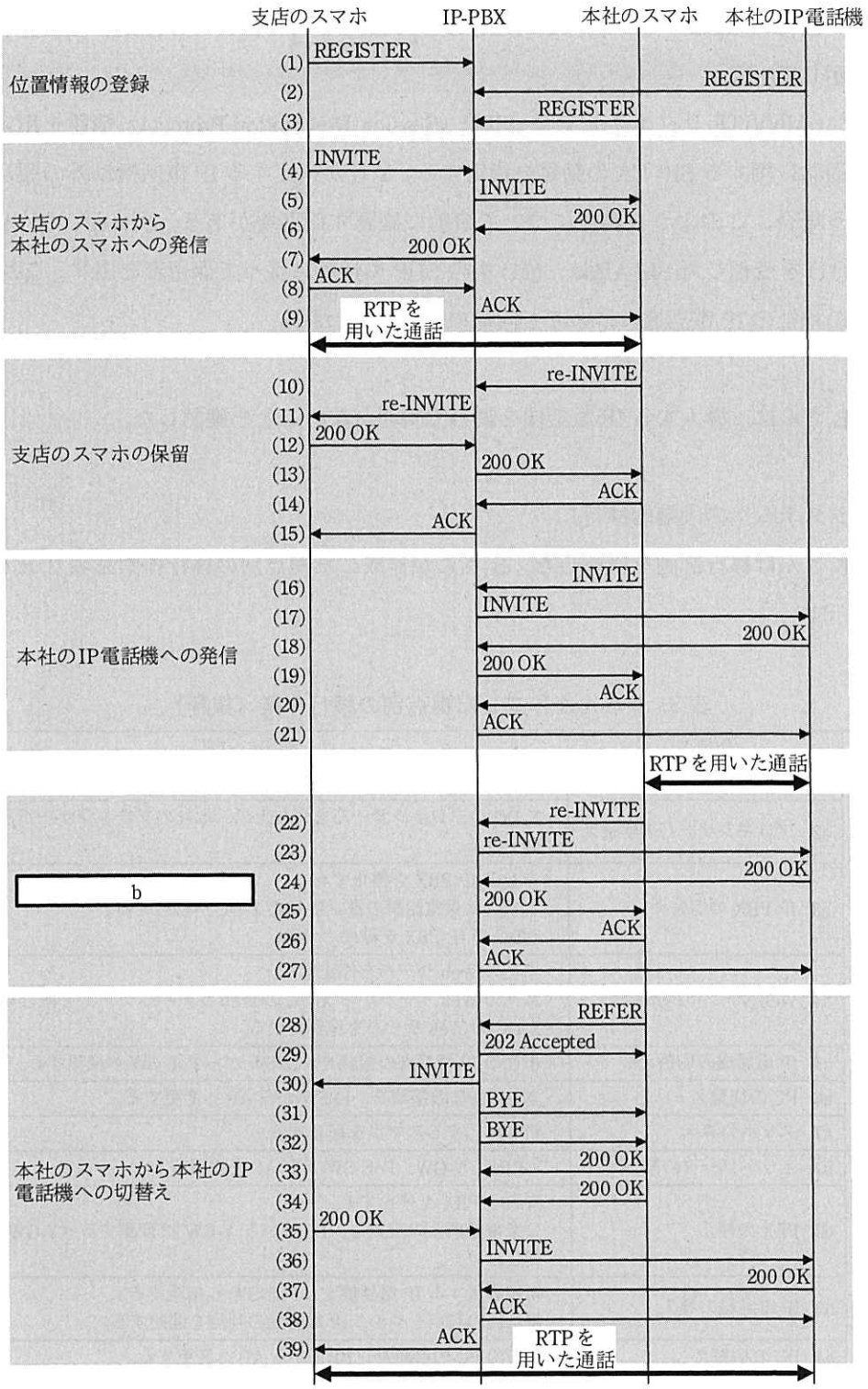
〔スマホの活用〕

スマホの SIP-AP を使うと，電話機と同等の操作ができる。その一例が，通話中の電話を別の電話機に転送する操作（以下，保留転送という）である。B さんは，保留転送の通信仕様を Y 社に問い合わせた。Y 社からの回答を次に示す。

(1) 開始されているダイアログ内で送信される INVITE リクエストを，re-INVITE リクエストという。保留転送を行うスマホは，IP-PBX に次の四つの SIP リクエストを送信する。

- re-INVITE リクエストを送信し，相手の電話機を保留状態にする。
- INVITE リクエストを送信し，転送先の電話機を呼び出す。
- re-INVITE リクエストを送信し，転送先の電話機を保留状態にする。
- REFER リクエストを送信し，セッションを切り替える。

(2) 保留転送に関する通信シーケンス例を図3に示す。



注記1　(1)～(39)は，シーケンス番号を表す。

注記2　Tryingなど，一部のシーケンスを省略している。

図3　保留転送に関する通信シーケンス例

(3) 図 3 の通信シーケンスは，利用者が［　コ　］を操作して保留転送を行う例を示している。

(4) re-INVITE リクエストでは，SDP（Session Description Protocol）情報を用いて，通話に関する SIP UA の動作を指定する。Y 社が指定する IP 電話機以外の製品を使う場合，このような動作について事前に確認する必要がある。例えば，図 3 中の (11) を受信した SIP-AP は，(11) 中の SDP の情報に従って保留音を出す。②図 3 中の本社の IP 電話機についても同様の動作が行われる。

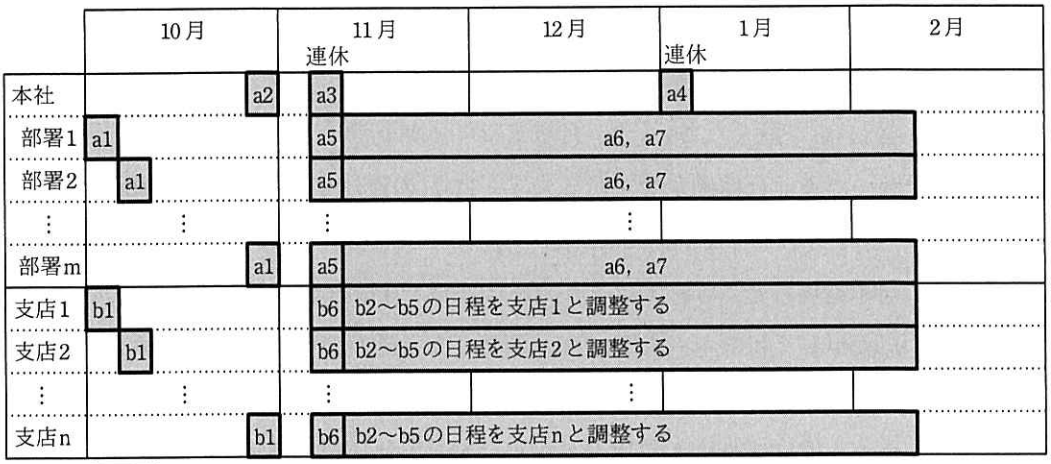
B さんは，導入する IP 電話機を調べて問題がないことを確認した。

〔新システムへの段階的移行〕

B さんは移行計画を検討した。B さんが作成した拠点別の移行作業を表 3 及び図 4 に示す。

表 3　B さんが作成した拠点別の移行作業（抜粋）

拠点名	作業名	作業の内容
本社	a1　ネットワークの準備	・本社の PoE-SW 及び AP を設置する。
	a2　プロキシサーバの切替え	・X-DC のプロキシサーバを立ち上げ，本社のプロキシサーバと並行稼働させる。
	a3　IP-PBX の切替え	・本社の IP-PBX を停止する。 ・本社の公衆電話網の電話番号を Y-DC へ移行する。 ・Y-DC の IP-PBX を稼働させる。
	a4　Web サーバの切替え	・本社の Web サーバを停止する。 ・本社の Web サーバから X-DC の Web サーバへデータを移行する。 ・X-DC の Web サーバを稼働させる。
	a5　IP 電話機の切替え	・本社の IP 電話機の接続を，L2SW から PoE-SW へ変更する。
	a6　PC の切替え	・本社の PC の接続を，L2SW から AP へ変更する。
	a7　スマホの導入	・新規導入するスマホを配布する。
支店	b1　ネットワークの準備	・Y-BBR，Y-GW，PoE-SW 及び AP を設置する。
	b2　PBX の停止	・支店の PBX を停止する。 ・公衆電話網との接続を，PBX から Y-GW へ変更する（Y-GW 設置の支店だけ）。
	b3　IP 電話機の導入	・新規導入する IP 電話機を，PoE-SW へ接続する。 ・電話機の利用をやめ，IP 電話機の利用を開始する。
	b4　PC の切替え	・支店の PC の接続を，BBR から AP へ変更する。
	b5　スマホの導入	・新規導入するスマホを配布する。
	b6　既存のスマホの切替え	・支店のスマホの SIP-AP を，Y 社クラウド PBX サービス用のものに変更する。

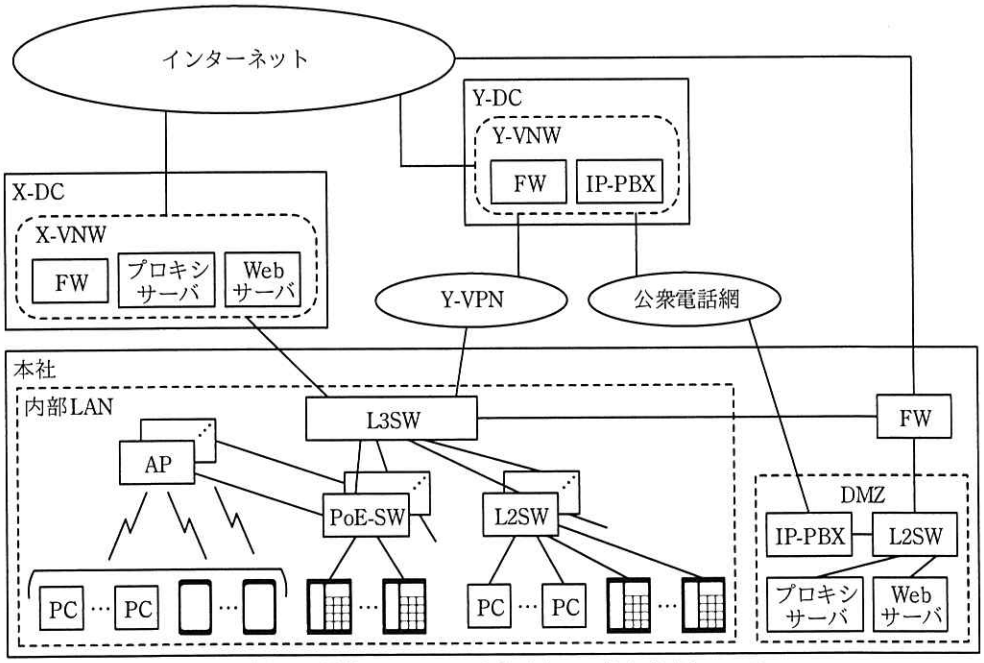


注記1　　中の記号は，表3中の作業名に付与された識別子を表す。

注記2　mは部署の数，nは支店の数をそれぞれ表す。

図4　Bさんが作成した拠点別の移行作業（抜粋）

次にBさんは，表3を基に切替期間中のネットワーク環境を検討した。Bさんが作成した切替期間中の本社のネットワーク構成を図5に示す。



注記　ネットワーク及び機器の接続について，中継要素の一部を省略している。

図5　Bさんが作成した切替期間中の本社のネットワーク構成（抜粋）

B さんは，表 3，図 4，5 を持参し，移行計画について情報システム部長に相談した。その時の B さんと部長の会話を次に示す。

B さん：図 4 をご覧ください。10 月末までにネットワークの準備を終え，プロキシサーバを並行稼働させておきます。11 月の連休を利用して IP-PBX を切り替え，1 月の連休を利用して Web サーバを切り替えます。

部長　：図 4 を見ると，本社では 2 か月以上掛けて PC を切り替えるようだね。

B さん：台数が多く利用者への配慮も必要なので，長めの切替期間を設けています。

部長　：なるほど。

B さん：また，③切替期間中の本社の内部 LAN では，現行環境と新環境を分離します。

部長　：その方が安全だ。ところで，本社の IP 電話機は一斉に切り替えるのだね。PC と同様に段階的に切り替えた方が良いと思うが。

B さん：Y 社に相談しましたが，Y-DC の IP-PBX と本社の IP-PBX との連携は複雑なので断念しました。二つの IP-PBX を同時に稼働させることは可能ですが，その場合には，それぞれに収容された IP 電話機間の内線通話ができません。また，［　c　］と IP 電話機の切替えの順序関係によって，一部の IP 電話機では，一時的に［　d　］ができなくなります。

部長　：了解した。次に，表 3 中の作業 a2 にあるプロキシサーバの並行稼働について説明してくれないか。

B さん：プロキシサーバには，プロキシ機能と DNS 機能をもたせています。並行稼働中は，それぞれの機能について，本社のプロキシサーバと X-DC のプロキシサーバの両方を稼働させます。さらに，X-DC のプロキシサーバの DNS 機能をスレーブ DNS サーバとし，本社のプロキシサーバの DNS 機能からゾーン転送を行います。

部長　：プロキシ機能はどのように切り替えるのかな。

B さん：現在，本社の PC からは本社のプロキシサーバを使っています。表 3 中の作業 a6 で PC を切り替えるときに，PC の設定情報を変更し，X-DC のプロキシサーバを使うようにします。

部長　：Web サーバは，1 月の連休を利用して切り替えるのだね。

B さん：はい。④切替えは，プロキシサーバの設定変更によって行います。

部長　：本社の切替えは大体良さそうだ。次に，支店の切替えを確認しよう。図 4 を見ると，本社と同様に長めの切替期間を設けるのだね。

B さん：支店ごとに日程を調整することになります。3 か月程度必要です。

部長　：支店ごとに作業 b2～b5 を実施するわけだが，日程調整の際，何か制約はあるのかな。

B さん：一つの支店について，作業［　サ　］と作業［　シ　］は一斉に行う必要があります。それ以外の作業は切替期間内であればいつでも実施できます。

部長　：了解した。支店と早めに切替日程を調整して，それぞれの支店について，PBX がいつから撤去可能になるのかを図 4 に追記してほしい。⑤本社についても，FW，Web サーバ，プロキシサーバ及び IP-PBX がいつから撤去可能になるのか，図 4 に追記してくれないか。

B さん：はい。分かりました。

その後，B さんは，見直した移行計画を含む検討結果を情報システム部長に報告した。B さんの検討結果に基づき，D 社システムの更改が開始された。

設問 1　〔現行の D 社システム〕について，(1)～(3) に答えよ。

(1) 本文中の［　ア　］，［　イ　］及び［　カ　］に入れる適切な機器を，図 1 中の機器名で答えよ。

(2) 本文中の［　ウ　］～［　オ　］に入れる適切な字句を答えよ。

(3) 本文中の下線①のために，FW において許可している通信を二つ挙げ，それぞれ 30 字以内で答えよ。

設問 2　〔クラウドサービスの利用〕について，(1)～(3) に答えよ。

(1) 本文中の［　キ　］～［　ケ　］に入れる適切な字句を答えよ。

(2) 表 2 中の［　a　］に入れる適切な字句を，表 2 中の字句を用いて答えよ。

(3) 表 2 中の支店の IP 電話機から取引先の電話機への通信経路が，項番 2-1 と項番 2-2 の 2 通りになる理由を，30 字以内で具体的に述べよ。

設問３　〔スマホの活用〕について，(1)～(4)に答えよ。

(1) 本文中の［　コ　］に入れる適切な字句を，図 3 中の字句を用いて答えよ。

(2) 図 3 中の［　b　］に入れる適切な字句を答えよ。

(3) 図 3 中のシーケンス番号 (31)，(32) の二つの BYE リクエストについて，BYE リクエストと同じ Call-ID をもつ INVITE リクエストのシーケンス番号を，一つずつ答えよ。

(4) 本文中の下線②について，同様の動作を，シーケンス番号を用いて 35 字以内で述べよ。

設問４　〔新システムへの段階的移行〕について，(1)～(5)に答えよ。

(1) 本文中の下線③に必要となる機器の設定を，図 5 中の字句を用いて 60 字以内で述べよ。

(2) 本文中の［　c　］，［　d　］に入れる適切な字句を，それぞれ 20 字以内で答えよ。

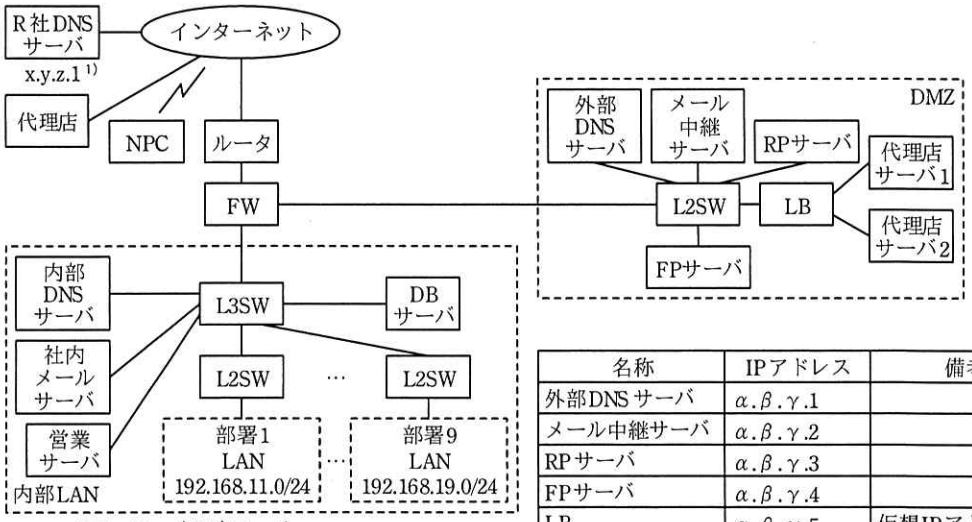
(3) 本文中の下線④の設定変更を行うプロキシサーバの設置場所を答えよ。また，変更内容を 50 字以内で述べよ。

(4) 本文中の［　サ　］，［　シ　］に入れる適切な字句を答えよ。

(5) 本文中の下線⑤中の全ての機器は，どの時点で撤去可能になるか。20 字以内で答えよ。また，その時点まで撤去できない機器を，全て答えよ。

問2　ネットワークのセキュリティ対策に関する次の記述を読んで，設問 1～6 に答えよ。

W 社は，IT 製品の卸売会社であり，国内外のベンダ 50 社の製品を，500 社の販売代理店に卸している。W 社では，販売代理店向けに販売代理店支援システム（以下，代理店システムという）を，自社営業員向けに営業支援システム（以下，営業システムという）を稼働させている。W 社の本社 LAN の構成を図 1 に示す。



FW：ファイアウォール
RP サーバ：リバースプロキシサーバ
FP サーバ：フォワードプロキシサーバ
DB サーバ：データベースサーバ
L2SW：レイヤ 2 スイッチ
L3SW：レイヤ 3 スイッチ
LB：負荷分散装置
NPC：ノート PC

名称	IP アドレス	備考
外部 DNS サーバ	α.β.γ.1	
メール中継サーバ	α.β.γ.2	
RP サーバ	α.β.γ.3	
FP サーバ	α.β.γ.4	
LB	α.β.γ.5	仮想 IP アドレス
代理店サーバ 1	192.168.1.1	
代理店サーバ 2	192.168.1.2	
内部 DNS サーバ	192.168.10.1	
社内メールサーバ	192.168.10.2	
営業サーバ	192.168.10.10	
DB サーバ	192.168.10.20	

注記 1　DMZ の公開サーバ用のグローバル IP アドレスのネットワークアドレスは，α.β.γ.0/28 である。
注記 2　W 社の NPC は，部署 1～9 の LAN に接続されている。
注 1)　x.y.z.1 は，ISP 事業者である R 社の R 社 DNS サーバに付与されたグローバル IP アドレスを示す。R 社 DNS サーバは，スレーブ DNS サーバとして利用されている。

図 1　W 社の本社 LAN の構成

本社 LAN の各システム又は各機器の構成，機能及び動作は，次のとおりである。

・代理店システムは，DMZ の LB，代理店サーバ及び内部 LAN の DB サーバから構成されている。代理店サーバは 2 台あり，LB で負荷分散されている。

・営業システムは，DMZ の RP サーバと内部 LAN の営業サーバから構成されている。外出先からの営業システムの利用は，RP サーバ経由で行われる。

・内部 LAN の各部署の NPC から，インターネット上の Web サイトへのアクセス，及び DMZ と内部 LAN のサーバから，マルウェア対策ソフトの定義ファイル更新のためのベンダの Web サイトへのアクセスは，FP サーバ経由で行われる。
・外部 DNS サーバは，DMZ のゾーン情報を管理するだけでなく，再帰的な名前解決を行うフルリゾルバとしても機能している。外部 DNS サーバはマスタ DNS サーバであり，インターネット上の R 社 DNS サーバをスレーブ DNS サーバとして利用している。
・メール中継サーバは，社外のメールサーバ及び社内メールサーバとの間で，電子メール（以下，メールという）の転送を行う。
・内部 DNS サーバは，内部 LAN のゾーン情報を管理し，当該ゾーンに存在しないホストの名前解決要求は，外部 DNS サーバに転送する。
・社内メールサーバは，社員のメールボックスを保持し，内部 LAN の NPC との間でメールの送受信を行う。

昨今，サイバー攻撃が増加しており，情報システムは，情報漏えい，Web サービスの妨害，サーバの不正利用などの脅威にさらされている。そこで，W 社では，本社 LAN のセキュリティ対策を見直すことにした。情報システム部の M 課長は，ネットワーク運用担当の N 主任に，本社 LAN のセキュリティ対策の見直しを指示した。

N 主任は，部下の J さんへの指導を兼ねて，J さんと一緒に本社 LAN のセキュリティ対策を見直すことにした。

〔本社 LAN のセキュリティ対策の状況〕

まず，N 主任は J さんに，本社 LAN のセキュリティ対策の状況について確認した。その時の，2 人の会話を次に示す。

N 主任：本社 LAN のセキュリティ対策の状況を説明してくれないか。
J さん ：はい。本社 LAN は，FW でインターネットからの IP パケットをフィルタリングしています。また，FP サーバでは，フィルタリングソフトウェアを稼働させて，URL フィルタリングを行っています。DMZ と内部 LAN のサーバではマルウェア対策ソフトが稼働しており，インターネット上のベンダ

の Web サイトにアクセスし，マルウェア定義ファイルが更新されているときは，自動でダウンロードするように設定されています。サーバ OS やミドルウェアへのセキュリティパッチの適用は，サーバ運用担当が実施しているとのことです。

N 主任：分かった。それでは，FW のフィルタリングの詳細を調べてくれないか。

J さんは，FW の設定内容を調査し，通信を許可する FW のルールを表 1 にまとめた。

表 1　通信を許可する FW のルール

項番	アクセス経路	送信元 IP アドレス	宛先 IP アドレス	プロトコル／ポート番号
1	インターネット→DMZ	any	α.β.γ.1	UDP/53 [1]
2		ア	α.β.γ.1	TCP/53
3		any	α.β.γ.2	TCP/25
4		any	α.β.γ.3	TCP/80，TCP/443
5		any	α.β.γ.5	TCP/80，TCP/443
6	DMZ→インターネット	α.β.γ.1	any	TCP/53 [2]，UDP/53
7		α.β.γ.2	any	TCP/25
8		α.β.γ.4	any	TCP/80，TCP/443
9	DMZ→内部 LAN [3]	α.β.γ.2	192.168.10.2	TCP/25
10		α.β.γ.3	192.168.10.10	TCP/80，TCP/443
11		192.168.1.1	192.168.10.20	TCP，UDP/アクセス用ポート番号
12		192.168.1.2	192.168.10.20	TCP，UDP/アクセス用ポート番号
13	内部 LAN→DMZ	192.168.10.1	α.β.γ.1	UDP/53 [1]
14		192.168.10.2	α.β.γ.2	TCP/25
15		192.168.10.1	α.β.γ.4	TCP/8080 [4]
16		192.168.10.2	α.β.γ.4	TCP/8080 [4]
17		192.168.10.10	α.β.γ.4	TCP/8080 [4]
18		192.168.10.20	α.β.γ.4	TCP/8080 [4]
19		部署 1～9 の LAN	α.β.γ.4	TCP/8080 [4]
20		部署 1～9 の LAN	α.β.γ.5	TCP/80，TCP/443

注記 1　内部 LAN から行われる，DMZ のサーバの運用管理用通信の許可ルールは省略している。
注記 2　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。
注 [1]　DNS の応答は，TCP フォールバックが発生しないので，UDP/53 だけを許可している。
[2]　古い DNS サーバの存在を考慮して，TCP/53 の通信を許可している。
[3]　DMZ から内部 LAN のサーバへの通信は，直接 IP アドレスを指定して行われる。
[4]　TCP/8080 は，代替 HTTP のポートである。

〔FW のフィルタリング内容の調査結果〕

J さんは，表 1 を N 主任に説明した。その時の 2 人の会話を次に示す。

J さん　：調べたところ，FW で許可している通信は，表 1 のとおりになっていました。

N 主任：現在の設定で，［　a　］スキャンとポートスキャンには対応できているようだ。DoS 攻撃は，送信元 IP アドレスを偽装して行われることがある。我が社が利用している ISP では，①利用者のネットワークとの接続ルータで，uRPF（Unicast Reverse Path Forwarding）と呼ばれるフィルタリングを行っているので，偽装されたパケットが当社に到達することは少なくなっていると考えられる。しかし，DoS 攻撃がなくなっているわけではない。DoS 攻撃への対策状況について，J さんの考えを聞かせてくれないか。

J さん：②DMZ の全ての公開サーバを対象とするブロードキャストアドレス宛てのスマーフ（smurf）攻撃のパケットは，FW でブロックされます。クローズのポート宛てに UDP パケットを送ると，RFC 792 で規定された［　b　］パケットが送信元 IP アドレス宛てに返送されるのを悪用し，サーバのリソースを消費させる UDP フラッド（UDP flood）攻撃も，FW の設定で防げていると思います。

N 主任：そのとおりだ。しかし，SYN フラッド（SYN flood）攻撃については対策が必要だ。どのような対応が必要なのかを検討してくれないか。

J さん　：分かりました。SYN フラッド攻撃について調べてみます。

〔SYN フラッド攻撃手法と対策技術〕

J さんが，SYN フラッド攻撃手法と対策技術について調査した内容を次に示す。

SYN フラッド攻撃は，SYN パケットを受信したサーバが，TCP コネクション確立のために数十バイトのメモリを確保しなければならない仕様を悪用し，攻撃者が大量の SYN パケットを標的のサーバに送りつけてサーバをダウンさせる攻撃である。

例えば，インターネットから図 1 中のメール中継サーバ宛てに送信される，TCP/25 の SYN パケットは，表 1 中の項番［　c　］のルールによってメール中継サーバに転送される。SYN パケットを受信したメール中継サーバは，コネクション確立のためにメモリを確保し，ACK パケットの返送がなくても，確保したメモリを

一定時間解放しない。また，ACK パケットが返送されて不正なコネクションが確立された場合は，更に長い時間メモリが解放されない。そのため，メール中継サーバが大量の SYN パケットを受信すると，大量のメモリを消費して正常に稼働できなくなるおそれがある。

SYN フラッド攻撃の防御技術には，ディレイドバインディングと SYN クッキーがある。ディレイドバインディング技術を図 2 に示す。

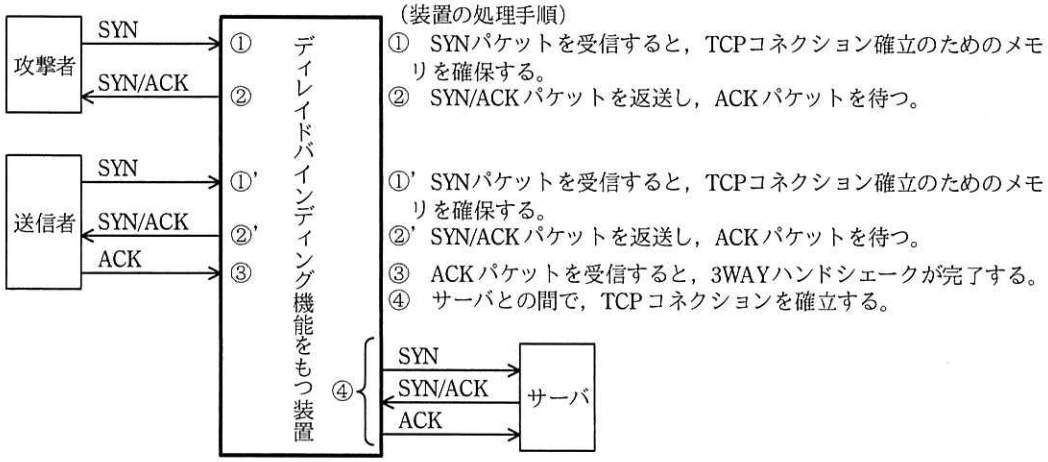


図 2　ディレイドバインディング技術

図 2 の方式によって，サーバでの不要なメモリ確保を抑止できる。しかし，図 2 の方式には，装置のメモリ容量によって同時接続数が制限される弱点がある。一方，SYN クッキーでは，この弱点が改善されている。SYN クッキー技術を図 3 に示す。

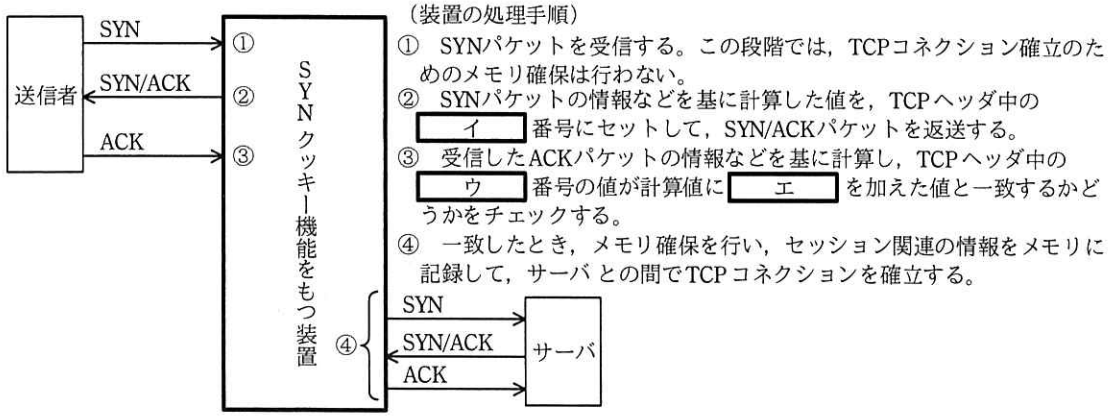


図 3　SYN クッキー技術

図 3 の方式は，パケット中の該当するコネクションに関連する情報などに，特別な演算によって計算した変換値をクッキーとして，TCP ヘッダ中のシーケンス番号に埋め込んで，通信の状態を監視するものである。

J さんは，二つの防御技術を比較した結果，③ SYN クッキーの方式では同時接続数の制限が緩和されることが分かったので，SYN クッキー技術をもつ IPS（Intrusion Prevention System）の導入を N 主任に提案した。その時の 2 人の会話を次に示す。

J さん ：SYN フラッド攻撃への対策が必要です。SYN クッキー技術をもつ IPS の導入を提案します。

N 主任：分かった。IPS を導入すれば，SYN フラッド攻撃だけでなく様々な不正な通信も遮断できるので，導入を検討しよう。そのほかに，DMZ のサーバが送信元偽装の目的で踏み台にされる可能性について，考えを聞かせてくれないか。

J さん ：④ FP サーバについては，FW の設定で防止できています。⑤メール中継サーバについては，サーバ自体の転送設定で防止しています。外部 DNS サーバについても大丈夫だと思います。

N 主任：外部 DNS サーバは，DNS リフレクタ攻撃の踏み台にされる可能性がありそうだ。安全面を考慮すれば，構成変更が必要になるかもしれない。対応策を考えてくれないか。

J さんは，外部 DNS サーバの構成上の問題点について考えた。外部 DNS サーバは，ゾーン情報管理サーバ（以下，コンテンツサーバという）の機能と，フルリゾルバの機能をもつので，表 1 中の項番 1 と項番 6 の通信が許可されている。フルリゾルバによるインターネット上のホストの名前解決は，［ d ］と［ e ］からの要求に対応できればよいが，コンテンツサーバは，インターネット上の不特定のホストからの名前解決要求に応答する必要がある。そこで，外部 DNS サーバを，コンテンツサーバとして機能する DNS サーバ 1 と，フルリゾルバサーバとして機能する DNS サーバ 2 に分離すれば，踏み台にされる可能性は低くなると考えた。その場合，表 1 中の項番 6 のルールの変更が必要になる。DNS サーバ 1 に $\alpha.\beta.\gamma.1$，DNS サーバ 2 に $\alpha.\beta.\gamma.6$ を割り当てたときの，表 1 の変更内容を表 2 に示す。

表2　表1の変更内容

項番	アクセス経路	送信元IPアドレス	宛先IPアドレス	プロトコル／ポート番号
6	（省略）	オ	カ	（省略）

J さんは，検討結果を N 主任に説明した。J さんの説明を受けた N 主任は，外部 DNS サーバの構成変更後の，DNS サーバへの攻撃についての調査を指示した。

〔DNS サーバへの攻撃と対策〕

J さんは，DNS サーバへの攻撃の中でリスクの大きい，DNS キャッシュポイズニング攻撃の手法について調査した。J さんが理解した内容を次に示す。

DNS キャッシュポイズニング攻撃は，次の手順で行われる。

(i) 攻撃者は，偽の情報を送り込みたいドメイン名について，標的のフルリゾルバサーバに問い合わせる。

(ii) フルリゾルバサーバは，指定されたドメインのゾーン情報を管理するコンテンツサーバに問い合わせる。

(iii) ⑥攻撃者は，コンテンツサーバから正しい応答が返ってくる前に，大量の偽の応答パケットを標的のフルリゾルバサーバ宛てに送信する。

(iv) フルリゾルバサーバは，受信した偽の応答パケットをチェックし，偽の応答パケットが正当なものであると判断してしまった場合，キャッシュの内容を偽の応答パケットを基に書き換える。

(ii) の問合せパケットと，(iii) の応答パケットの情報を表3に示す。

表3に示すように，(ii) の問合せパケットの送信元ポート番号には特定の範囲の値が使用されるケースが多いので，攻撃者は，(iii) の偽の応答パケットを正当なパケットに偽装しやすくなるという問題がある。調査の結果，この問題の対応策には，送信元ポート番号のランダム化があることが分かった。

表3 （ii）の問合せパケットと，（iii）の応答パケットの情報（抜粋）

項番	ヘッダ名	項目名	問合せパケットの情報	応答パケットの情報
1	IP ヘッダ	送信元 IP アドレス	フルリゾルバサーバの IP アドレス	キ
2		宛先 IP アドレス	コンテンツサーバの IP アドレス	ク
3		プロトコル	UDP	UDP
4	UDP ヘッダ	送信元ポート番号	n [1]	ケ
5		宛先ポート番号	53	コ
6	DNS ヘッダ	識別子	m [2]	サ
7		フラグ中の QR ビット	0（問合せ）	1（応答）

注 [1] n には特定の範囲の値が設定されるケースが多い。
注 [2] m には任意の値が設定される。

J さんは，⑦外部 DNS サーバの構成変更によって，インターネットからの DNS サーバ 2 へのキャッシュポイズニング攻撃は防げると判断した。さらに，万が一の場合に備え，DNS サーバ 2 には，送信元ポート番号のランダム化に対応した製品の導入を提案することにした。

J さんは，調査結果と対応策を N 主任に説明し，DNS サーバ 2 には送信元ポート番号のランダム化対応の製品の導入が了承された。

〔マルウェアの内部 LAN への侵入時の対策〕

次に，2 人は，マルウェアの内部 LAN への侵入時の対策について検討した。

ネットワークのセキュリティ対策を行っても，ソーシャルエンジニアリングなどによって W 社内の情報が漏えいすると，内部 LAN の NPC は，マルウェアに侵入されるおそれがある。NPC に侵入したマルウェアは，攻撃者が管理・運営する C&C（Command & Control）サーバとの間の通信路を設定した後，C&C サーバ経由で攻撃者から伝達された命令を実行して，自身の拡散や C&C サーバへの秘密情報の送信などを行うことがある。このとき，C&C サーバの IP アドレスが特定できれば，FP サーバで C&C サーバとの通信は遮断できる。しかし，Fast Flux と呼ばれる手法を用いて，IP アドレスの特定を困難にすることによって，C&C サーバなどを隠蔽する事例が報告されている。

Fast Flux は，特定のドメインに対する DNS レコードを短時間に変化させることによって，サーバの追跡を困難にさせる手法である。Fast Flux 手法が用いられたときのマルウェアによる C&C サーバとの通信例を，図 4 に示す。

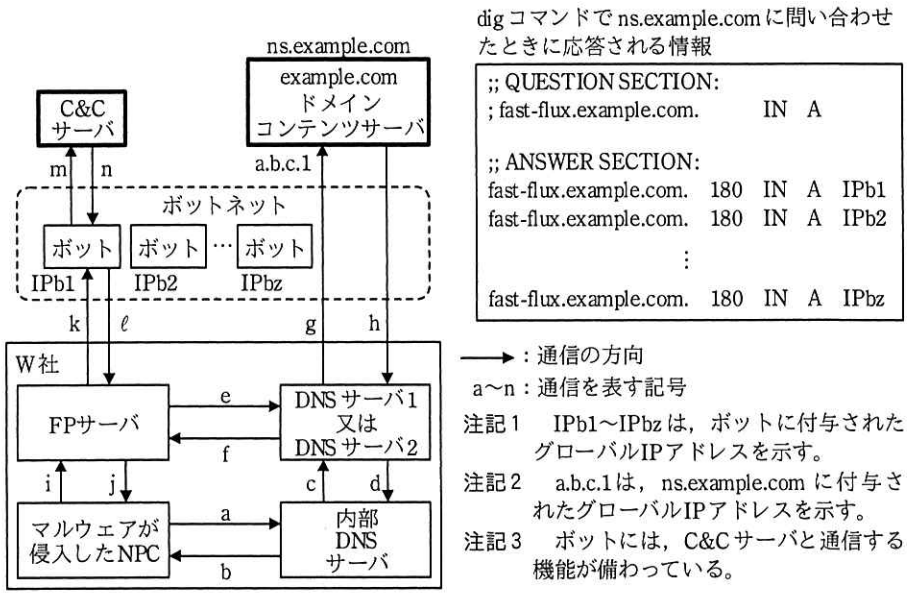


図 4 Fast Flux 手法が用いられたときのマルウェアによる C&C サーバとの通信例（抜粋）

攻撃者は，example.com ドメインを取得してコンテンツサーバ（ns.example.com）を設置する。図 4 中の ns.example.com には，fast-flux の FQDN に対する A レコードとして大量のボットの IP アドレス，及び DNS ラウンドロビンが設定される。

図 4 には，W 社の内部 LAN の NPC に侵入したマルウェアが，fast-flux.example.com にアクセスした後，ボットに備わる機能を利用して，C&C サーバとの間で行われる通信を示している。⑧図 4 中の example.com ドメインのコンテンツサーバの設定の場合，マルウェアが，一定間隔で fast-flux.example.com へアクセスを行えば，毎回，異なる IP アドレスで，ボットを経由して C&C サーバと通信することになる。

このような方法を用いることによって，C&C サーバの IP アドレスを隠蔽できる。しかし，マルウェアが同一の FQDN のホストにアクセスすることになるので，fast-flux.example.com へのアクセスによって C&C サーバとの通信が行われることが判明すれば，FP サーバの URL フィルタリングで C&C サーバとの通信は遮断できる。攻撃者は，これを避けるために Domain Flux と呼ばれる手法を用いることがある。

Domain Flux は，ドメインワイルドカードを用いて，あらゆるホスト名に対して，同一の IP アドレスを応答する手法である。Fast Flux と Domain Flux を組み合わせることによって，C&C サーバの FQDN と IP アドレスの両方を隠蔽できる。図 4 に示した構成の Fast Flux と Domain Flux を組み合わせたときの，ns.example.com に設定

されるゾーンレコードの例を図5に示す。

```
$ ORIGIN    example.com.
                        IN      NS      ns.example.com.
ns          86400       IN      A       a.b.c.1
*           180         IN      A       IPb1
*           180         IN      A       IPb2
                        :
*           180         IN      A       IPbz
```

図5　ns.example.com に設定されるゾーンレコードの例（抜粋）

このような攻撃が行われた場合を想定し，2人は，現行の FP サーバを HTTPS 通信の復号機能をもつ機種に交換し，プロキシ認証を併せて行うことにした。交換する FP サーバでのプロキシ認証のセキュリティを高めるために，社内の NPC の Web ブラウザで，オートコンプリート機能を無効にし，ID，パスワードのキャッシュを残さないようにすることにした。また，内部 LAN に侵入したマルウェアの活動を早期に検知するために，⑨ FP サーバと FW のログを定期的に検査することにした。

以上の検討を基に，N 主任と J さんは，(1) IPS の導入，(2) 外部 DNS サーバの構成変更と新機種の導入，(3) FP サーバの交換，(4) NPC の設定変更，及び (5) ログの定期的な検査から成る5項目の実施案をまとめ，M 課長に提出した。

2人がまとめた実施案は，経営会議で承認され，実施に移されることになった。

設問1　本文中の［　a　］～［　e　］に入れる適切な字句又は数値を答えよ。

設問2　表1中の［　ア　］に入れる適切な IP アドレスを答えよ。また，項番2のルールによって行われる通信の名称を答えよ。

設問3　〔FW のフィルタリング内容の調査結果〕について，(1)，(2) に答えよ。

(1)　本文中の下線①について，フィルタリングの内容を，70字以内で述べよ。

(2)　本文中の下線②の IP アドレスを答えよ。

設問4　〔SYN フラッド攻撃手法と対策技術〕について，(1)～(5) に答えよ。

(1)　図3中の［　イ　］～［　エ　］に入れる適切な字句又は数値を答えよ。

(2)　本文中の下線③の，制限が緩和されるのは，ディレイドバインディング方

式よりメモリ消費量が少なくて済むからである。その理由を，35 字以内で述べよ。

(3) 本文中の下線④について，防止できていると判断した理由を，40 字以内で述べよ。

(4) 本文中の下線⑤について，防止するためにメール中継サーバに設定されている処理方法を，50 字以内で述べよ。

(5) 表 2 中の［ オ ］，［ カ ］に入れる適切な字句を答えよ。

設問 5 〔DNS サーバへの攻撃と対策〕について，(1)～(3) に答えよ。

(1) 表 3 中の問合せパケットに対して，フルリゾルバサーバが正当な応答パケットと判断するパケットの内容について，表 3 中の［ キ ］～［ サ ］に入れる適切な字句又は数値を答えよ。

(2) 本文中の下線⑥では，大量の偽の応答パケットが送信される。当該パケット中で，パケットごとに異なる内容が設定される表 3 中の項目名を，全て答えよ。

(3) 本文中の下線⑦について，防げると判断した根拠を，60 字以内で述べよ。

設問 6 〔マルウェアの内部 LAN への侵入時の対策〕について，(1)～(5) に答えよ。

(1) 図 4 中で，fast-flux.example.com の名前解決要求と応答の通信を a～n の中から全て選び，通信が行われる順番に並べよ。

(2) 本文中の下線⑧について，DNS サーバ 2 がキャッシュした DNS レコードが消去されるまでの時間（分）を答えよ。

(3) 図 5 のようにゾーンレコードが設定された場合，C&C サーバを効果的に隠蔽するための，マルウェアによる C&C サーバへのアクセス方法について，25 字以内で述べよ。

(4) 本文中の下線⑨について，FP サーバのログに，マルウェアの活動が疑われる異常な通信が記録される場合がある。その通信の内容を，35 字以内で述べよ。

(5) 内部 LAN の NPC に侵入したマルウェアが，FP サーバを経由せずに C&C サーバの FQDN 宛てにアクセスを試みた場合は，マルウェアによる C&C サーバとの通信は失敗する。通信が失敗する理由を，40 字以内で述べよ。

6. 退室可能時間中に退室する場合は，手を挙げて監督員に合図し，答案用紙が回収されてから静かに退室してください。

退室可能時間	15:10 ～ 16:20

7. **問題に関する質問にはお答えできません。**文意どおり解釈してください。
8. 問題冊子の余白などは，適宜利用して構いません。ただし，問題冊子を切り離して利用することはできません。
9. 試験時間中，机上に置けるものは，次のものに限ります。

   なお，会場での貸出しは行っていません。

   受験票，黒鉛筆及びシャープペンシル（B 又は HB），鉛筆削り，消しゴム，定規，時計（時計型ウェアラブル端末は除く。アラームなど時計以外の機能は使用不可），ハンカチ，ポケットティッシュ，目薬

   これら以外は机上に置けません。使用もできません。
10. 試験終了後，この問題冊子は持ち帰ることができます。
11. 答案用紙は，いかなる場合でも提出してください。回収時に提出しない場合は，採点されません。
12. 試験時間中にトイレへ行きたくなったり，気分が悪くなったりした場合は，手を挙げて監督員に合図してください。