NW

令和７年度　春期
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。

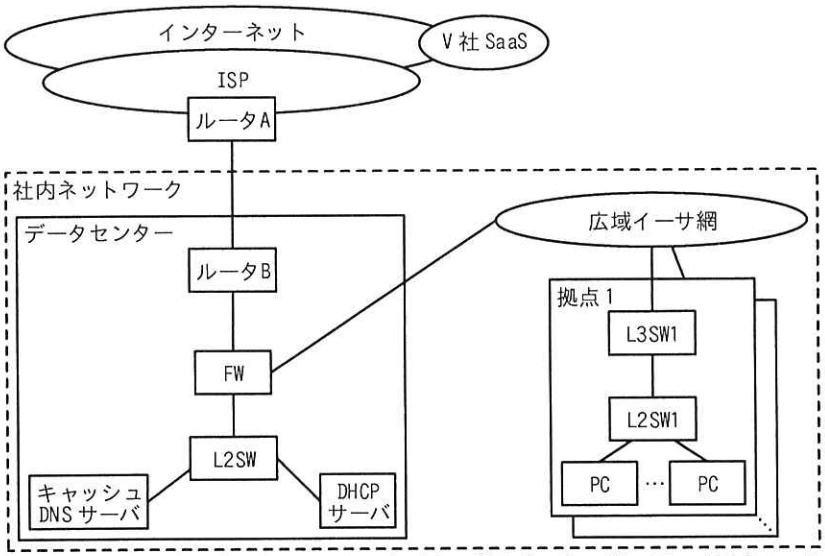
問1　社内ネットワークのIPv6対応に関する次の記述を読んで，設問に答えよ。

Q社は全国に拠点をもつ大手の電機メーカーである。Q社で利用される社内ネットワークにはIPv4アドレスだけが割り当てられており，従業員は社内ネットワークに接続されたPCを利用して，社内Web，電子メール，ファイル共有，チャットやWeb会議などのサービスを提供するV社SaaS，及びインターネット上のWebサイトにアクセスして業務を行っている。

Q社で利用しているSaaSやWebサイトのIPv6の対応状況，及び近年のIPv6普及率の向上を踏まえ，情報システム部はIPv6の調査と社内ネットワークのIPv6対応について検討することにした。IPv6の調査と社内ネットワークのIPv6対応の検討は，情報システム部のP主任が担当することになった。

〔社内ネットワークの概要〕

Q社の現状の社内ネットワーク構成を図1に示す。



L2SW：レイヤー2スイッチ　L3SW：レイヤー3スイッチ　FW：ファイアウォール
ISP：インターネットサービスプロバイダ
広域イーサ網：広域イーサネットサービス網

図1　Q社の現状の社内ネットワーク構成（抜粋）

図1の概要を次に示す。

・社内ネットワークのPC，ネットワーク機器及びサーバにはIPv4アドレスを割り当てている。

・ルータBにはデフォルトルート及びNAPTを設定している。

・FWでは，ステートフルパケットインスペクションを用いたアクセス制御を行っていて，許可及び拒否した通信のログを記録している。

・ルータB，FW及び各拠点のL3SWは，OSPFv2を用いて経路制御を行っている。

・ルータBは，OSPFv2でデフォルトルートを配布している。

・データセンターと各拠点との間は，レイヤー2の広域イーサ網で接続されている。

・PCは，IPv4アドレス，デフォルトゲートウェイ及びキャッシュDNSサーバに関する情報を，DHCPサーバから取得している。

〔IPv6対応の方針〕

V社SaaSの一部及びインターネット上のWebサイトの一部は，現時点ではIPv6に対応していない。P主任は，社内ネットワークのIPv6対応後もIPv4のネットワークへの接続を確保する必要があると考えて，社内ネットワークには，IPv4とIPv6のデュアルスタックのネットワークを採用する方針で，IPv6対応について検討することにした。

〔IPv6におけるアドレス解決〕

IPv6におけるアドレス解決では，IPv4のARPに相当する機能をもつ，RFC 4861で規定されたNeighbor Discovery Protocol（以下，NDPという）が用いられる。

IPv4のARPによるアドレス解決では，要求元のノードは，求めるMACアドレスに対応するIPv4アドレスをARPリクエストの［ a ］フィールドに入れて，［ b ］キャストで送信する。次に，ARPリクエストを受信した，要求されたIPv4アドレスをもつノードは，自身のMACアドレスをARP［ c ］の送信元MACアドレスフィールドに入れて，要求元のノード宛てに送信する。

IPv6のNDPによるアドレス解決では，要求元のノードは，求めるMACアドレスに対応するIPv6アドレスをICMPv6のNeighbor Solicitation（以下，NSという）メッセージに入れて，マルチキャストで送信する。次に，NSメッセージを受信した，要求

されたIPv6アドレスをもつノードは，Neighbor Advertisement（以下，NAという）メッセージに自身のMACアドレスを入れて，要求元のノード宛てに送信する。

〔IPv6アドレスの割当て〕

NDPは，ICMPv6のNSメッセージ及びNAメッセージに加えてRouter Solicitation（以下，RSという）メッセージやRouter Advertisement（以下，RAという）メッセージなども用いて，アドレス解決以外の次の機能を実現している。

・データリンク層で通信可能な範囲にあるルータを発見する機能
・サブネットプレフィックスやデフォルトルータを決定するための情報を，ノードに通知する機能
・利用予定のIPv6アドレスがほかのノードで利用されていないか確認する重複アドレス検出機能

IPv6アドレスの構造，使用方法及び自動設定については，RFC 4291で規定されたIPv6アドレス体系，及びRFC 4862で規定されたSLAAC（IPv6 Stateless Address Autoconfiguration）に規定されている。

IPv6アドレスは128ビットで構成され，［ d ］ビットずつを“：”で区切って表される。2001:db8:aabb:1::1/64を例とするIPv6アドレスの構造を図2に示す。

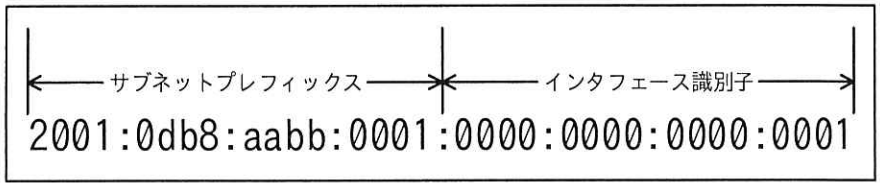


図2　2001:db8:aabb:1::1/64を例とするIPv6アドレスの構造

IPv6アドレスには，リンクローカルユニキャストアドレス（以下，LLAという）とグローバルユニキャストアドレス（以下，GUAという）がある。①LLAはある範囲でネットワークインタフェースを一意に識別できるIPv6アドレスであり，サブネットプレフィックスには“fe80::/64”を用いる。GUAは，IPv6で構成されるインターネットを含むグローバルなネットワークで，ネットワークインタフェースを一意に識

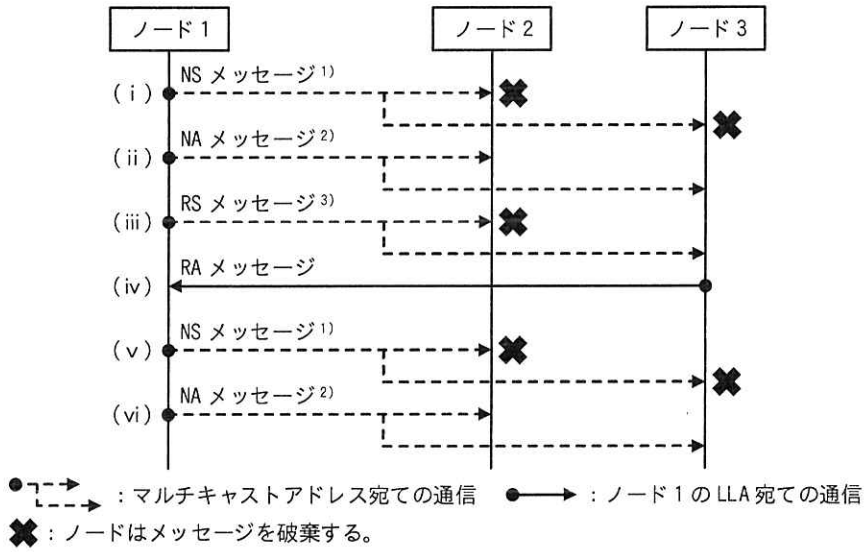
別できるIPv6アドレスである。

インタフェース識別子の生成方法を次に示す。

・疑似乱数関数を用いてランダムなインタフェース識別子を生成する方法

・［ e ］ビットのMACアドレスから［ f ］ビットのModified EUI-64形式のインタフェース識別子を生成する方法

ノード1におけるNDP及びSLAACを用いたIPv6アドレスの生成処理を図3に示す。なお，Q社の社内ネットワークの拠点1においては，ノード1及びノード2はPCであり，ノード3はL3SW1である。



注1) 宛先IPv6アドレスは要請ノードマルチキャストアドレスであり，ノード1が宛先アドレスフィールドに入れるIPv6アドレスの下位24ビットと，宛先のノードのインタフェース識別子の下位24ビットが同じ場合に受信される。

注2) 宛先IPv6アドレスは全ノードマルチキャストアドレスである。

注3) 宛先IPv6アドレスは全ルータマルチキャストアドレスである。

図3　ノード1におけるNDP及びSLAACを用いたIPv6アドレスの生成処理

図3中の処理(i)～(vi)の概要を次に示す。

(i)　ノード1は，仮のLLAを生成してNSメッセージに入れて送信し，ほかのノードからNAメッセージの応答がないことを確認する。

(ii)　ノード1は，仮のLLAを正式なLLAとしてNAメッセージに入れて，全ノード

マルチキャストアドレス宛てに送信する。

(iii) ノード 1 は，RS メッセージを全ルータマルチキャストアドレス宛てに送信する。

(iv) RS メッセージを受信したノード 3 は，GUA の生成に用いるサブネットプレフィックス，及びデフォルトルータを決定するための情報を RA メッセージに入れて，ノード 1 宛てに送信する。

(v) ノード 1 は，RA メッセージのサブネットプレフィックスと生成したインタフェース識別子を組み合わせた仮の GUA を NS メッセージに入れて送信し，ほかのノードから NA メッセージの応答がないことを確認する。

(vi) ノード 1 は，仮の GUA を正式な GUA として NA メッセージに入れて，全ノードマルチキャストアドレス宛てに送信する。

ノード 1 は，ノード 3 を経由して外部のノードと通信を行うために，処理(iv)で受信した，RA メッセージの送信元であるノード 3 の LLA を [g] に設定する。

Q 社のネットワークにおける IPv6 アドレスの割当てについて，P 主任が調査した結果の一部を次に示す。

・Q 社は，ISP から，プレフィックス長が 48 又は 56 の GUA の割当てを受けることができる。

・ISP から割り当てられた GUA を，プレフィックス長が 64 のネットワークに分割して，利用することができる。

・SLAAC を利用して，PC の LLA，GUA，及び [g] を自動で設定することができる。

・ルータ B，FW 及び各拠点の L3SW には，LLA 及び GUA を静的に割り当てることができる。

・固定の MAC アドレスから Modified EUI-64 形式のインタフェース識別子を生成する方法は非推奨である。

PC のインタフェース識別子が疑似乱数関数を用いてランダムに生成される場合，②利用者のプライバシー保護に有用であるが，PC 管理の観点で考慮が必要になると

P 主任は考えた。

〔IPv6 の名前解決〕

IPv4 の名前解決と比べて IPv6 の名前解決では，512 バイトよりも大きな DNS メッセージを送受信する可能性が高い。DNS の機能を拡張するために RFC 6891 で規定された Extension Mechanisms for DNS version 0（以下，EDNS という）では，スタブリゾルバとフルサービスリゾルバとの間，及びフルサービスリゾルバと権威 DNS サーバとの間で，UDP 上で送受信される DNS メッセージのサイズの上限を緩和している。

P 主任は，IPv6 アドレスの名前解決について，フルサービスリゾルバであるキャッシュ DNS サーバを管理する情報システム部の R 係長に相談した。2 人の会話を次に示す。

P 主任：社内ネットワークを IPv6 に対応させることになった場合に，キャッシュ DNS サーバに IPv6 アドレスを割り当てる必要がありますか。

R 係長：不要です。キャッシュ DNS サーバは IPv4 のネットワーク上で DNS メッセージを送受信して，FQDN に対応する IPv6 アドレスを解決できます。例えば，IPv6 と IPv4 の両方に対応する Web サイトの名前解決を行う場合に，PC は AAAA レコードと A レコードを用いて名前解決を要求することで，IPv6 アドレスと IPv4 アドレスの両方を取得します。

P 主任：FQDN から IPv6 アドレスと IPv4 アドレスの両方を解決した場合，Q 社の PC はどのように動作するのですか。

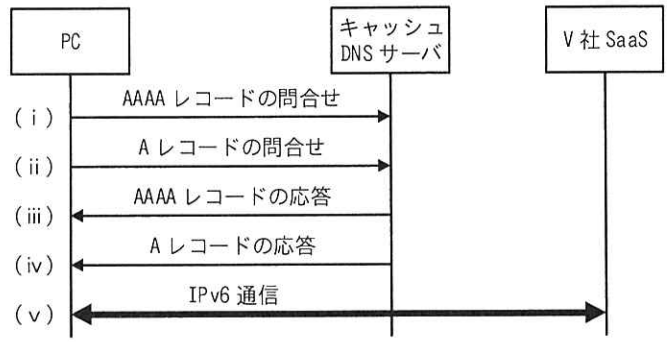
R 係長：AAAA レコードと A レコードの応答をほぼ同じタイミングで受信した場合には，IPv6 を優先して通信を行います。

P 主任：IPv6 の DNS メッセージは，IPv4 の DNS メッセージよりもサイズが大きくなると考えています。UDP 上で送受信される DNS メッセージのサイズには上限がありますが，何か対応が必要でしょうか。

R 係長：Q 社のキャッシュ DNS サーバは EDNS に対応済みです。PC から名前解決の要求を受けたキャッシュ DNS サーバが，権威 DNS サーバに問い合わせる場合を例に説明します。キャッシュ DNS サーバは，まず，DNS を利用して権威 DNS サーバの EDNS の対応可否を確認します。EDNS を利用できるときには，両方のサーバ間で調整した最大のメッセージサイズまでであれば，512 バイトを超

える DNS メッセージであっても UDP で送受信します。DNS メッセージが最大のメッセージサイズを超えるときや，EDNS に対応していない権威 DNS サーバと 512 バイトを超える DNS メッセージを送受信するときには，［ h ］で送受信することになります。

P 主任が作成した DNS の通信例を図 4 に，V 社 SaaS の FQDN に対する AAAA レコードの応答例を図 5 に示す。



注記　キャッシュ DNS サーバと権威 DNS サーバとの間の通信は省略する。

図 4　P 主任が作成した DNS の通信例（抜粋）

;; ANSWER SECTION:				
saas.example.com.	3600	IN	CNAME	dual-saas.example.net.
dual-saas.example.net.	240	IN	AAAA	2001:db8:xxxx::10
dual-saas.example.net.	240	IN	AAAA	2001:db8:xxxx::20
;; AUTHORITY SECTION:				
example.net.	172800	IN	NS	ns1.example.net.
example.net.	172800	IN	NS	ns2.example.net.
;; ADDITIONAL SECTION:				
ns1.example.net.	172800	IN	A	198.51.100.α
ns2.example.net.	172800	IN	A	198.51.100.β

注記 1　saas.example.com.は，V 社 SaaS の FQDN である。
注記 2　2001:db8:xxxx::10 及び 2001:db8:xxxx::20 は GUA である。
注記 3　198.51.100.α及び 198.51.100.βはグローバル IPv4 アドレスである。

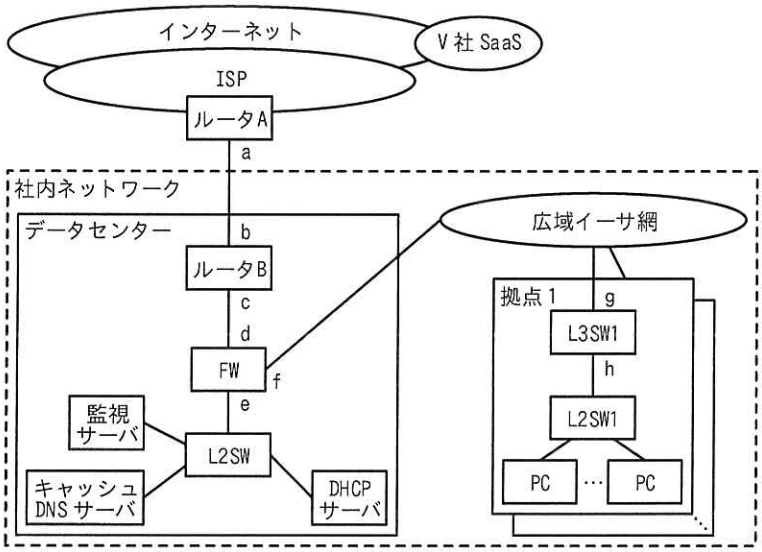
図 5　V 社 SaaS の FQDN に対する AAAA レコードの応答例（抜粋）

③IPv6 のネットワークだけが不通となった場合に，利用している OS や Web ブラウザによっては従業員が異常に気付くことができず，情報システム部に異常を連絡で

きない可能性があると P 主任は考えた。IPv6 のネットワークの異常を検知するために，データセンターに監視サーバを導入して，IPv6 のインターネットへのアクセスや，各拠点の L3SW の GUA に対して ping6 コマンドによる監視を行うことにした。

〔IPv6 ネットワークの設計〕

P 主任は，図 1 の社内ネットワークを基に，IPv4 と IPv6 のデュアルスタックのネットワークを設計した。P 主任が設計した社内ネットワーク構成を図 6 に示す。



ネットワーク機器に割り当てる IPv6 アドレス一覧

機器名	インタフェース名	LLA/プレフィックス長	GUA/プレフィックス長
ルータ A	a	fe80::1/64	未割当て
ルータ B	b	fe80::2/64	未割当て
	c	fe80::1/64	未割当て
FW	d	fe80::2/64	未割当て
	e	fe80::1/64	2001:db8:yyyy:1::1/64
	f	fe80::1/64	2001:db8:yyyy:2::1/64
L3SW1	g	fe80::2/64	2001:db8:yyyy:2::2/64
	h	fe80::1/64	2001:db8:yyyy:3::1/64

注記 1　a～h は各ネットワーク機器のインタフェース名を示す。

注記 2　2001:db8:yyyy:1::/64～2001:db8:yyyy:3::/64 は GUA のサブネットプレフィックスである。

図 6　P 主任が設計した社内ネットワーク構成（抜粋）

図6の概要を次に示す。

・IPv4のネットワーク設計に関する変更はない。

・PC，ネットワーク機器及び監視サーバには，IPv4アドレスに加えてIPv6アドレスを割り当てる。

・ISPからQ社に割り当てられるGUAを，2001:db8:yyyy::/48として設計する。

・ルータBには，ルータAのLLAをネクストホップとするデフォルトルートを設定する。

・ルータB，FW及び各拠点のL3SWは，OSPFv3を用いてIPv6の経路制御を行う。

・OSPFv3ではLLAを用いて隣接関係を確立してIPv6の経路制御を行うので，④FWと各拠点のL3SWとの間の，PCやサーバを接続しないネットワークにGUAを割り当てる必要はないが，静的に割り当てる。

・ルータBは，OSPFv3でデフォルトルートを配布する。

・⑤PCは，SLAACを用いてIPv6アドレス及びデフォルトルータを設定する。

ルータB，FW及びL3SW1のIPv6の経路情報を表1に示す。

表1　ルータB，FW及びL3SW1のIPv6の経路情報（抜粋）

項番	機器名	静的経路制御又は経路制御プロトコル名	宛先ネットワーク	ネクストホップのIPv6アドレス	出口インタフェース名
1	ルータB	静的経路制御	::/0	ア	イ
2		静的経路制御	2001:db8:yyyy::/48	なし	Null[1)]
3		OSPFv3	2001:db8:yyyy:3::/64	ウ	エ
4	FW	OSPFv3	::/0	オ	カ
5		OSPFv3	2001:db8:yyyy:3::/64	キ	ク
6	L3SW1	OSPFv3	::/0	ケ	g

注[1)]　IPパケットを廃棄するためのインタフェースである。

IPv6のネットワーク設計について，P主任は情報システム部のS課長に，図6及び表1を用いて説明した。2人の会話の一部を次に示す。

P主任：ISPには，Q社にプレフィックス長が48のGUAを割り当ててもらえることを確認しました。図6及び表1はISPから割り当てられるGUAを2001:db8:yyyy::/48として作成しています。ISPのルータAには，ルータBのLLAをネクストホ

ップとする 2001:db8:yyyy::/48 宛ての静的経路が設定されます。

S 課長：表 1 の経路情報について説明してください。

P 主任：項番 1 は，ISP を経由してインターネットにアクセスするためのデフォルトルートです。項番 2 は，ISP から割り当てられるプレフィックス長が 48 の GUA のうち，使用されない GUA が存在するので設定します。⑥項番 2 の経路情報を設定しない場合，ルーティングループが発生します。⑦項番 1 と項番 2 の両方の経路情報に該当する IP パケットの転送では，ルータ B は項番 2 の経路情報を選択します。社内ネットワークの経路制御には OSPFv3 を利用します。項番 3 と項番 5 は，拠点 1 のネットワーク宛ての経路情報です。項番 4 と項番 6 は，ルータ B から配布されるデフォルトルートによって登録される経路情報です。

S 課長：IPv6 のネットワークは，IPv4 のネットワークと比較して情報セキュリティ面で違いはありますか。

P 主任：異なる点があります。IPv4 のネットワークでは FW によるアクセス制御に加えて，ルータ B に［　i　］を設定しているので，インターネットから社内ネットワークには簡単に通信できない設計になっています。IPv6 のネットワークでは［　i　］を利用しないので，FW のアクセス制御の設計については慎重に検討する必要があります。

S 課長：FW では，インターネットから社内ネットワーク宛ての全ての通信を拒否する設定を行えばよいのでしょうか。

P 主任：IPv6 の通信では，ICMPv6 メッセージを通信の制御に利用しているので，ICMPv6 メッセージを拒否すると通信障害を発生させるおそれがあります。例えば，中継する機器が MTU サイズよりも大きいサイズの IP パケットを転送できないときに，⑧中継する機器から送信元にタイプ 2 の ICMPv6 メッセージである“Packet Too Big”を送信する PMTUD（Path MTU Discovery）に利用されています。ほかにも，ICMPv6 メッセージのタイプによっては FW で許可すべきものがあるので，調査する予定です。

P 主任による IPv6 の調査と IPv6 対応の検討の結果は情報システム部で承認されて，社内ネットワークへの IPv6 導入において活用されることになった。

設問１　本文中の［ a ］～［ c ］に入れる適切な字句を答えよ。

設問２　〔IPv6 アドレスの割当て〕について答えよ。

(1)　本文中の［ d ］～［ f ］に入れる適切な数値を答えよ。

(2)　本文中の下線①について，LLA が有効な範囲を 20 字以内で答えよ。

(3)　図 3 中の処理(ｉ)及び(ｖ)を行う目的を，55 字以内で答えよ。

(4)　図 3 中の処理(ii)の正式な LLA が fe80::8:800:200c:417a であり，処理(iv)の RA メッセージに含まれるサブネットプレフィックスが 2001:db8:aabb:1::/64 であった場合に，処理(ｖ)で生成される仮の GUA 及びプレフィックス長を答えよ。

(5)　本文中の［ g ］に入れる適切な字句を答えよ。

(6)　本文中の下線②について，P 主任がこのように考えた理由を，20 字以内で答えよ。

設問３　〔IPv6 の名前解決〕について答えよ。

(1)　本文中の［ h ］に入れる適切な字句を答えよ。

(2)　図 5 中の AAAA レコードの応答について，“saas.example.com.”にアクセスするための V 社 SaaS の IPv6 アドレス，及び V 社 SaaS の IPv6 アドレスを管理している権威 DNS サーバの FQDN を，図 5 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，従業員が異常に気付くことができないと P 主任が考えた理由を，45 字以内で答えよ。

設問４　〔IPv6 ネットワークの設計〕について答えよ。

(1)　図 6 中の a～d のインタフェース名について，GUA を割り当てない目的を，50 字以内で答えよ。

(2)　本文中の下線④について，GUA を“静的に”割り当てることによって得られる利点を，経由するネットワーク機器を調べるときに使用されるコマンド名を用いて，45 字以内で答えよ。

(3)　本文中の下線⑤の設定を行うために，各拠点の L3SW で行われる動作を，ICMPv6 のメッセージ名を用いて 40 字以内で答えよ。

(4)　表 1 中の［ ア ］～［ ケ ］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，表 1 中の項番 2 の経路情報を設定しない場合に，インターネットから未使用の GUA 宛てに送信された IP パケットを，ルータ A

及びルータ B はどのように処理するか。IPv4 の“TTL”と同じように用いられる，“ホップリミット”という字句を用いて 35 字以内で答えよ。

(6) 本文中の下線⑦について，表 1 中の項番 2 の経路情報が選択されるのはなぜか。25 字以内で答えよ。

(7) 本文中の［　i　］に入れる適切な字句を答えよ。

(8) 本文中の下線⑧について，PMTUD によって何が検出されるか。20 字以内で答えよ。

問２　IoT システムの設計に関する次の記述を読んで，設問に答えよ。

Y 社は，LP ガスメーターを製造し，全国の LP ガス販売業者に販売している。このたび，Y 社では，LP ガス販売業者向けに LP ガス使用量の遠隔検針サービスを開始することになり，遠隔検針機能をもつ Y 社製 LP ガスメーター（以下，G メーターという），G メーターを管理するサーバなどから構成される IoT システムを開発することにした。

IoT システム開発プロジェクトチームの責任者には，W 課長が任命された。W 課長は，IoT システムの要件として次の二つを設定し，プロジェクトチームのメンバーでネットワーク技術者の X 主任に，IoT システムの機能と構成の検討を指示した。

(1)　G メーターは全国に設置されるので，全国規模で提供可能な IoT 向けの無線回線を利用すること

(2)　G メーターは電池で動作させるので，長時間の稼働を可能にすること

〔IoT 向けの無線技術の調査と無線回線の選定〕

最初に，X 主任は，IoT 向けの無線技術を調査し，調査結果を次のようにまとめた。

・IoT 向けには，LPWA（Low Power Wide Area）と呼ばれる，低［ a ］電力の無線通信技術が利用される。

・LPWA は，セルラー系と非セルラー系の二つに大別される。［ b ］系には LoRaWAN，Sigfox などがあり，［ c ］系には LTE-M（LTE Cat.M1），NB-IoT（LTE Cat.NB1）などがある。

・LoRaWAN，Sigfox は，日本では Sub-GHz 帯の一つである 920 MHz 帯を利用する。920 MHz 帯は Wi-Fi が利用する周波数帯と同様に，［ d ］バンドと呼ばれる周波数帯であるが，2.4 GHz 帯と比べて電波［ e ］の影響が少ない。

・LTE-M，NB-IoT は，［ f ］と呼ばれる標準化プロジェクトが作成した技術仕様を基に，通信事業者が全国規模で構築した LTE 網でサービスが提供されている。

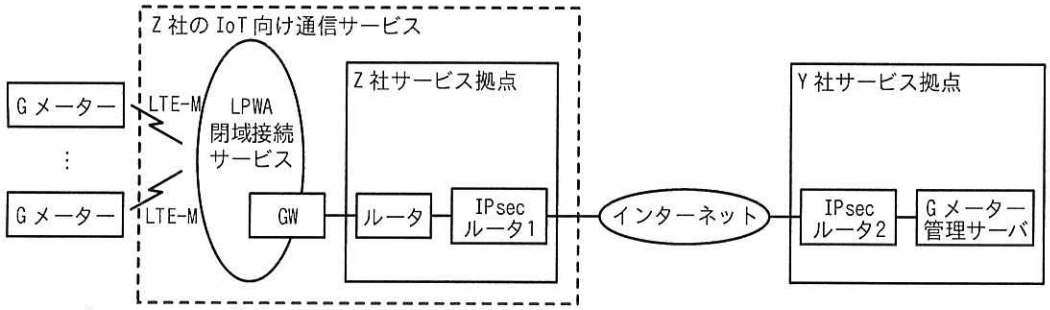
調査の結果，LTE-M を利用すれば全国の幅広い地域で IoT システムを稼働させることができることが分かった。次に，X 主任は，LTE-M を利用した IoT 向けのサービスを提供している企業の中から Z 社を選定し，Z 社の IoT 向け通信サービスについて調

査することにした。

〔Z 社の IoT 向け通信サービスの調査〕

Z 社の IoT 向け通信サービスは，LPWA 閉域接続サービスと IPsec VPN を用いて顧客ごとに閉域網を構成する。

Z 社の IoT 向け通信サービスを利用したときの IoT システムの構成を図 1 に示す。



GW：IP ネットワークに接続するためのゲートウェイ

注記　G メーター管理サーバは，G メーターと通信して検針データを収集するサーバである。

図 1　Z 社の IoT 向け通信サービスを利用したときの IoT システムの構成（抜粋）

Z 社は，GW とルータとの間を専用線で接続し，Z 社サービス拠点と Y 社サービス拠点との間は IPsec VPN で接続することによって，Y 社向けの閉域網を構成する。

図 1 中の IPsec ルータ 1 で動作する IKEv2 は，IPsec ルータ 2 との間で，四つのメッセージの交換を［　g　］往復で行い，SAD（Security Association Database）を作成する。IPsec ルータ 1 の SPD（Security Policy Database）中のセレクターには，［　h　］宛てのパケットを受信したとき，SAD を参照して IPsec の処理を行うことが設定されている。

閉域網が構成されることによって，G メーターと IPsec ルータ 2 に接続する予定の G メーター管理サーバとの通信は，プライベート IP アドレスで行うことができる。G メーターには，通信事業者が契約者を識別する情報を記録している［　i　］カードを装着する。

X 主任は，Z 社の IoT 向け通信サービスの利用料を，次の条件を基に試算した。

・G メーター1 台当たりの 1 回の検針時の通信量を 100 バイトとし，1 時間ごとに検針を実施する。

・通信費は 1 か月の通信量 1,000 バイト当たり 1 円とし，G メーターごとに割り当てる 1 回線当たりの基本料金は月額 300 円とする。

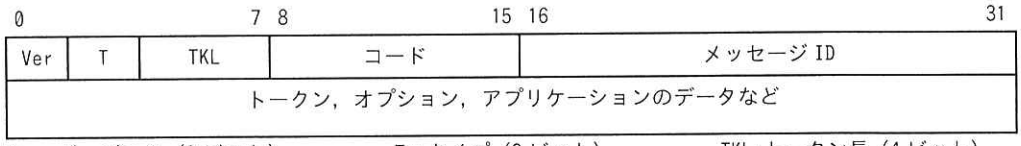
この条件から，Z 社の IoT 向け通信サービスを利用すると，1 か月が 30 日の場合，G メーター1 台当たりの検針に必要な 1 か月の利用料は［　j　］円なので，LP ガス販売業者向けに安価な遠隔検針サービスを提供できることが分かった。

次に X 主任は，G メーターと G メーター管理サーバとの間でデータを送受信するための通信プロトコルを検討した。IoT 向けの通信プロトコルには，RFC 7252 で標準化された CoAP（Constrained Application Protocol）と OASIS 標準メッセージングプロトコルである MQTT（Message Queuing Telemetry Transport）がある。CoAP は，Web システムにおける API の形式である［　k　］アーキテクチャを採用しているので，Web 技術で IoT システムを構築する場合に適している。そこで，X 主任は，CoAP について調査した。

〔CoAP の調査〕

CoAP は，伝送効率を考慮して標準では UDP を利用し，データの保護が必要な場合は，RFC 9147 で標準化された DTLS（Datagram TLS）を利用することができる。

CoAP のメッセージ形式を図 2 に示す。



Ver：バージョン（2 ビット）　T：タイプ（2 ビット）　TKL:トークン長（4 ビット）

注記　先頭の 4 バイトは固定長ヘッダーである。

図 2　CoAP のメッセージ形式

CoAP では，確認が必要なメッセージ（以下，CON という），確認が不要なメッセージ（以下，NON という），確認応答メッセージ（以下，ACK という），リセットメッセージの 4 種類が定義されており，図 2 中のタイプでメッセージ種類を指定する。CoAP サーバ及び CoAP クライアントは，CON を受信したときは ACK を返送し，NON を受信したときは ACK を返送しない。

図2中のコードは，要求の場合，メソッドコードを示し，応答の場合，レスポンスコードを示す。メソッドコードを表1に，レスポンスコードを表2に示す。

表1　メソッドコード（抜粋）

コード	メソッド名	説明
0.01	GET	指定したリソースを取得する。
0.02	POST	指定したリソースを作成する。
0.04	DELETE	指定したリソースを削除する。

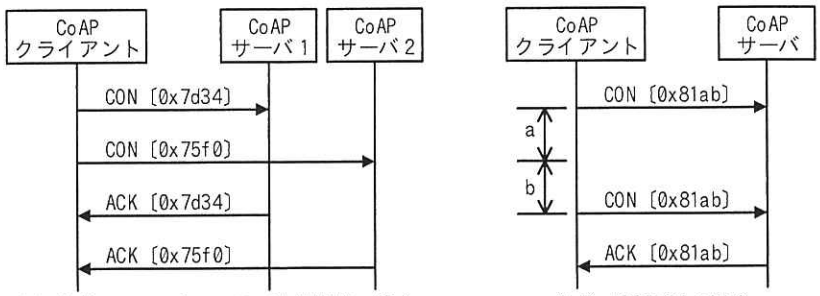
表2　レスポンスコード（抜粋）

コード	状態	説明
2.01	Created	リクエストが正常に処理され，指定したリソースが作成された。
2.02	Deleted	リクエストが正常に処理され，指定したリソースが消去された。
2.05	Content	リクエストが正常に処理され，指定したリソースが取得された。

メッセージ ID は，要求と応答のメッセージを関連付けるとともに，メッセージの重複を検出するのに使用される。CoAP は，［　l　］層のプロトコルである UDP 上での動作を前提としている。通信品質の劣るネットワークなどでは，パケットが［　m　］で到着したり，［　n　］して出現したり，通知なしに消失したりすることがあるので，CoAP は，メッセージ ID を利用することによって，送受信が正しく行われるための仕組みを実装している。

トークンは，要求した情報と応答された情報を関連付けるために使用される。CoAP クライアントはトークンの値によって，どの要求に対して応答された情報なのかを判断する。

CON と ACK を用いた通信例を図3に示す。



（ｉ）複数のサーバへの CON 連続送信の場合　　（ｉｉ）ACK 不達の場合

注記１　〔〕内の 0x は，x の後ろに続く数字又は文字が，16 進数であることを示す。

注記２　〔〕内の 16 進数は，メッセージ ID である。

図３　CON と ACK を用いた通信例

図３中の(ｉ)では，CoAP クライアントは，CON に対して返送された ACK によって，CON が CoAP サーバに到達して処理されたことが分かることを示している。CoAP では，図３中の(ｉ)に示したように，ACK の受信を待たずに連続して CON を送信することができる，非［　o　］通信が行われる。

(ii)では，ACK 不達時に，CON の再送によって CON 又は ACK を確実に到達させることを示している。(ii)に示したように，CoAP クライアントは CON を送信後，デフォルトのタイムアウト時間である a の時間 ACK の受信を待ち，ACK が受信できなかった場合は，指数［　p　］と呼ばれる方式で算出した b の時間経過後に CON を再送する。図３で示したように，CoAP では，CON に対する ACK の返送及び CON の再送によって，パケットロスなどが発生するネットワークを利用した場合も，確実な通信を行うことができる。

IoT 向けの機器は，サーバにデータの提供を要求する場合がある。このような場合，要求したデータと応答されたデータを関連付けるのにトークンが利用される。

機器がサーバにデータの提供を要求したときのトークンの使用例を図４に示す。

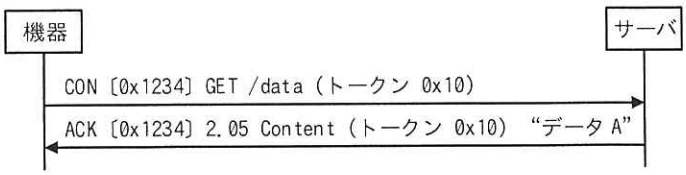


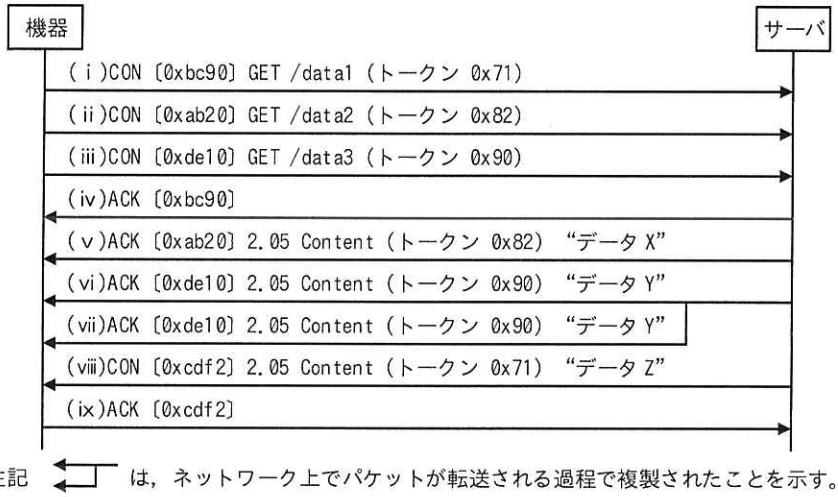
図４　機器がサーバにデータの提供を要求したときのトークンの使用例

図 4 では，機器がサーバ宛ての CON の中で，提供を求めるデータに 0x10 という値のトークンを指定している。この要求を受信したサーバは，提供するデータに 0x10 という値のトークンを付与して応答する。機器は，トークン値から要求したデータとしてデータ A が回答されたことを知ることができる。

図 4 中の ACK には，Content のデータも含まれている。このように，CoAP では，ACK に Content のデータを加えて送信する，ピギーバックと呼ばれる応答方式が利用される。

機器が連続してサーバに異なるデータの提供を要求する場合もある。

機器が連続してサーバに異なるデータの提供を要求したときの応答例を図 5 に示す。



注記 ⇦⌐ は，ネットワーク上でパケットが転送される過程で複製されたことを示す。

図 5　機器が連続してサーバに異なるデータの提供を要求したときの応答例

図 5 中の①(ⅳ)は，サーバが要求を受信したときにデータをすぐに送信できない場合の応答である。②(ⅱ)を受信したサーバはデータを送信できている。(ⅶ)は，ネットワーク上の何らかの原因によって，(ⅵ)と重複した ACK が機器に到達したことを示している。③(ⅶ)を受信した機器は，ACK が重複したものであると判断して，対応する処理を行う。

CoAP 通信で，データの保護が必要な場合は DTLS を利用する。DTLS は，TCP 通信のアプリケーション層のデータを暗号化する TLS の機能を UDP に適用した技術である。

DTLS バージョン 1.3（以下，DTLS 1.3 という）は，TLS バージョン 1.2（以下，TLS 1.2 という）と異なった方法で ClientHello メッセージの送信を求める。

TLS 1.2 と DTLS 1.3 のハンドシェークの違いを図 6 に示す。

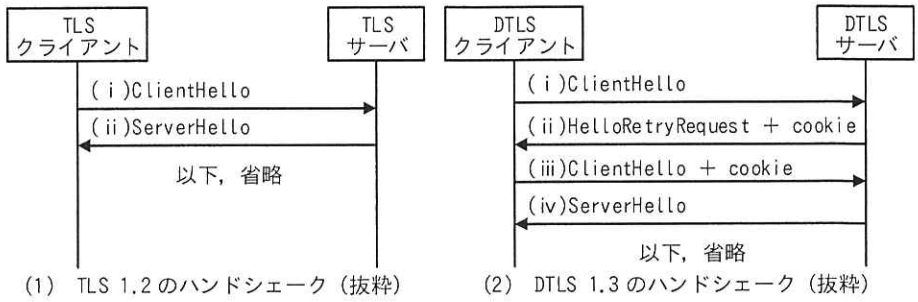


図 6　TLS 1.2 と DTLS 1.3 のハンドシェークの違い

図 6 中の(1)に示した TLS 1.2 のハンドシェークを UDP 上で行うと，④攻撃者が（ⅰ）の ClientHello メッセージの送信元を偽装して送信した場合，TLS サーバはパケットサイズの大きな(ⅱ)の ServerHello メッセージを返送することになり，TLS サーバが DDoS 攻撃の加害者になるおそれがある。この攻撃に対処するために，(2)に示した DTLS 1.3 のハンドシェークでは，（ⅰ）の ClientHello メッセージを受信した DTLS サーバが，（ⅱ）の HelloRetryRequest メッセージに cookie を添付して送信する。（ⅱ）を受信した DTLS クライアントは，受信した cookie を添付した（ⅲ）の ClientHello メッセージを再度送信する。⑤ DTLS サーバは，（ⅲ）に添付された cookie を検査し，cookie が不正な場合は対応する処理を行う。

無線回線の選定及び G メーターと Y 社拠点に導入する G メーター管理サーバとの間で利用する CoAP の調査が終わったので，X 主任は，IoT システムの機能と構成の検討に取り掛かった。

〔IoT システムの機能と構成の検討〕

まず，X 主任は，G メーター開発技術者から G メーターが送受信できる情報の説明を受け，次の 2 点の主要な機能を実現するための方式を検討した。

(1)　遠隔検針

(2)　異常通知

Gメーター管理サーバは数万台のGメーターを管理することを前提に，Gメーターで CoAP クライアント機能を，Gメーター管理サーバで CoAP サーバ機能を動作させることにした。

X主任が考えた，Gメーターの動作を次に示す。

(1)について，Gメーターは1時間ごとに LP ガスの流量積算値を測定して，測定時刻と測定値（以下，測定データという）をメモリに記録し，毎日午前0時の測定の後，⑥ランダムな時間経過後に，前日に測定した1時間ごとの測定データを 24 回に分けてGメーター管理サーバに送信する。⑦ LP ガスの流量積算値の測定又は測定データ送信後，次の測定を行う時刻までの間は，Gメーターはスリープ状態になる。

(2)について，G メーターはウェイクアップして測定を行うタイミングを利用して，Gメーター自身の稼働状態をチェックし，異常を検知したときに異常内容をGメーター管理サーバに送信する。

X主任は，Gメーターの動作を基に，GメーターとGメーター管理サーバとの間の通信方法をまとめた。Gメーターと Gメーター管理サーバとの間の通信の概要を図7に，Gメーターによる測定と測定データの送信タイミングを図8に示す。

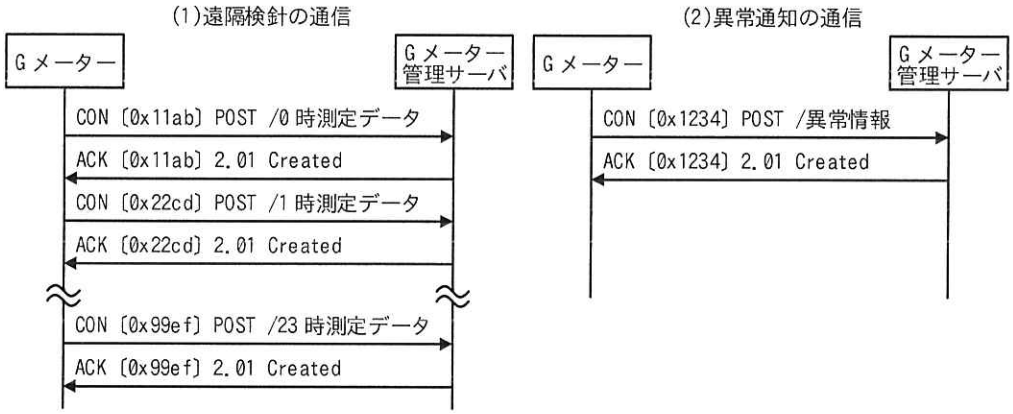


図7　Gメーターと Gメーター管理サーバとの間の通信の概要

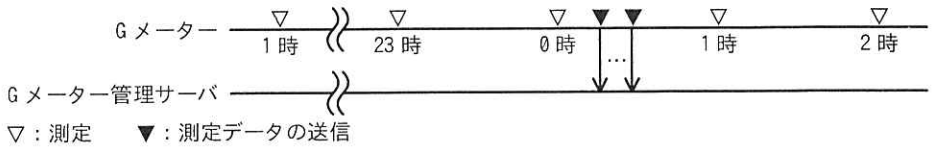


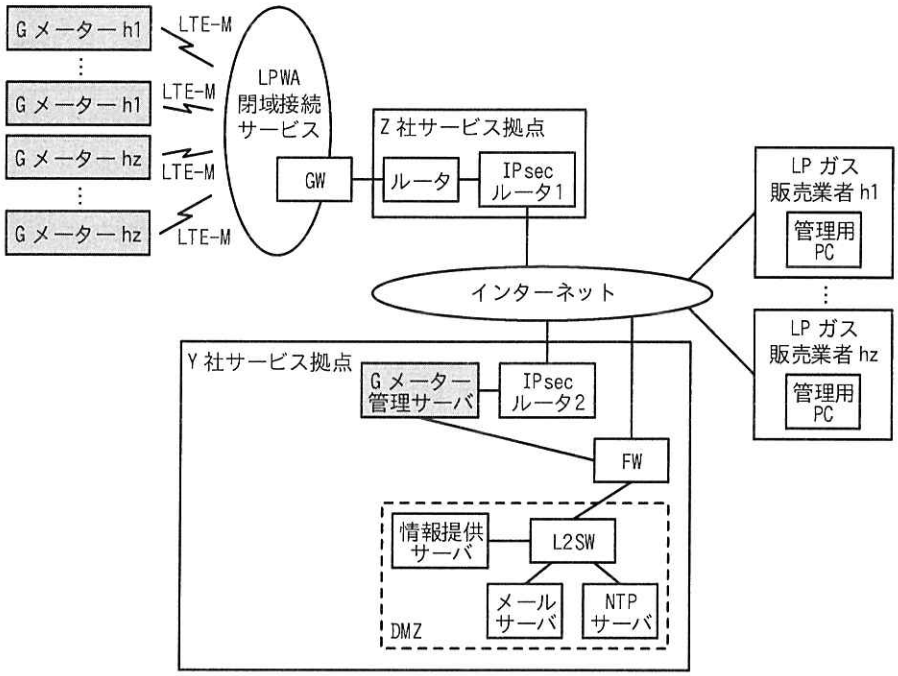
図8　Gメーターによる測定と測定データの送信タイミング

図7中の（1）及び図8に示したように，Gメーターは，毎日午前0時の測定を行った後，1時までの間のランダムな時間経過後に，1時間ごとに記録した1日分24件の測定データを，それぞれPOSTメソッドでGメーター管理サーバに送信する。これによって，図7中の(1)では，GメーターがPOSTメソッドを24回発行することになる。⑧CoAPでやり取りされるIPパケットの数は，HTTPバージョン1.1を利用して同様の方法で測定データを送信する場合と比べると少ないので，測定データの通信時間は短くて済む。

図7で示したCoAP通信でDTLSを利用すると，Gメーターで実施する通信処理の負荷が，Gメーターの性能に影響を与えるおそれがある。そこで，X主任は，⑨今回開発するIoTシステムでは，DTLSを利用しなくてもCoAP通信のセキュリティは確保されると判断し，DTLSは利用しないことにした。

Gメーターは図8に示した動作を行うので，時計機能の実装が必要になる。Gメーターに精度の高いリアルタイムクロックを実装しても，⑩Gメーターを長時間稼働させると時刻の誤差が無視できないほど大きくなるおそれがある。そこで，X主任は，⑪Gメーターに時刻の誤差を抑えるための処理を組み込むことにした。

これらの検討を基に，X主任は，IoTシステムの構成を設計した。X主任が設計したIoTシステムの構成を図9に示す。



L2SW：レイヤー2スイッチ　　FW：ファイアウォール

注記1　図中の網掛けは，CoAP 通信を行う機器を示す。

注記2　G メーターh1 は，LP ガス販売業者 h1 社が所有する G メーターであり，G メーターhz は，LP ガス販売業者 hz 社が所有する G メーターである。

図 9　X 主任が設計した IoT システムの構成（抜粋）

図 9 中の Y 社サービス拠点のサーバは，NTP サーバとの間で時刻同期を行う。

G メーター管理サーバは，全 G メーターから 1 日分の測定データを受信した後に，2 時から G メーターごとに LP ガス消費量などを集計する。集計したデータは LP ガス販売業者別に情報提供サーバに送信される。情報提供サーバは，受信した情報を LP ガス販売業者向けに公開する。

G メーターから送信される異常情報は，G メーター管理サーバを介して情報提供サーバに送信される。情報提供サーバは，LP ガス販売業者宛ての異常通知メールを作成し，メールサーバに送信する。

IoT システムの機能と構成の検討が完了したので，X 主任は，検討結果を W 課長に報告した。W 課長は，報告内容を基に，IoT システム開発の概要を経営会議で提案した。提案内容が承認され，IoT システム開発プロジェクトが本格的に開始されることになった。

設問１　本文中の［ a ］～［ f ］に入れる適切な字句を答えよ。

設問２　本文中の［ g ］～［ k ］に入れる適切な字句又は数字を答えよ。

設問３　〔CoAP の調査〕について答えよ。

(1)　本文中の［ l ］～［ p ］に入れる適切な字句を答えよ。

(2)　本文中の下線①について，(iv)で送信できなかったデータが送信されるメッセージを，図 5 中の(ｉ)～(ix)で答えよ。また，そのメッセージが(ｉ)の要求に対する応答であると判断できる理由を，15 字以内で答えよ。

(3)　本文中の下線②について，サーバが送信した ACK を，図 5 中の(ｉ)～(ix)で答えよ。

(4)　本文中の下線③について，受信した機器が重複した ACK であると判断する理由及び実施する処理を，それぞれ 30 字以内で答えよ。

(5)　本文中の下線④について，攻撃者が行う偽装の内容を，40 字以内で具体的に答えよ。また，その攻撃は，複数の DDoS 攻撃の手法の中で，何と呼ばれる手法の攻撃か。攻撃名を答えよ。

(6)　本文中の下線⑤について，cookie が正しい場合に DTLS サーバが判断できることを，30 字以内で答えよ。また，cookie が不正のものであると判断した場合に DTLS サーバが行う対応を，30 字以内で答えよ。

設問４　〔IoT システムの機能と構成の検討〕について答えよ。

(1)　本文中の下線⑥について，測定データの送信をランダムの時間控えることによる効果を，35 字以内で答えよ。

(2)　本文中の下線⑦について，スリープ状態になることによる効果を，25 字以内で答えよ。

(3)　本文中の下線⑧について，HTTP バージョン 1.1 を利用した場合，やり取りする IP パケットの数が多くなる理由を，35 字以内で答えよ。

(4)　本文中の下線⑨について，DTLS を利用しなくてもセキュリティが確保されると判断した理由を，30 字以内で答えよ。

(5)　本文中の下線⑩について，時刻の誤差によって発生する問題を，30 字以内で答えよ。

(6)　本文中の下線⑪について，時刻の誤差を抑えるために考えられる，CoAP 通信を利用した処理の内容を，40 字以内で答えよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

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。