問１　ネットワークシステムの設計に関する次の記述を読んで，設問 1～4 に答えよ。

機械メーカの X 社は，顧客に販売した機械の運用・保守と，機械が稼働している顧客の工場の自動化支援に関する新事業を拡大しようとしている。

機械は工作装置及び通信装置の 2 種類である。工作装置には，センサ，アクチュエータなどを制御する機構（以下，デバイスという），及びレイヤ 2 スイッチが内蔵されている。通信装置は，デバイスをインターネットに接続するための機器で，エッジサーバ，ファイアウォール及びレイヤ 3 スイッチが内蔵されている。

X 社の情報システム部は，新事業用のサービス基盤システム（以下，X システムという）を計画中である。情報システム部に所属するネットワーク担当の W さんが，X システムの構想について，検討を行っている。

〔X システムの構想〕

X システムは，X 社が運用・保守を行う顧客の工場内の機器，X 社内のサーバ，及びそれらを接続するためのネットワーク機器から構成されている。

X システムの導入構成例を図 1 に示す。

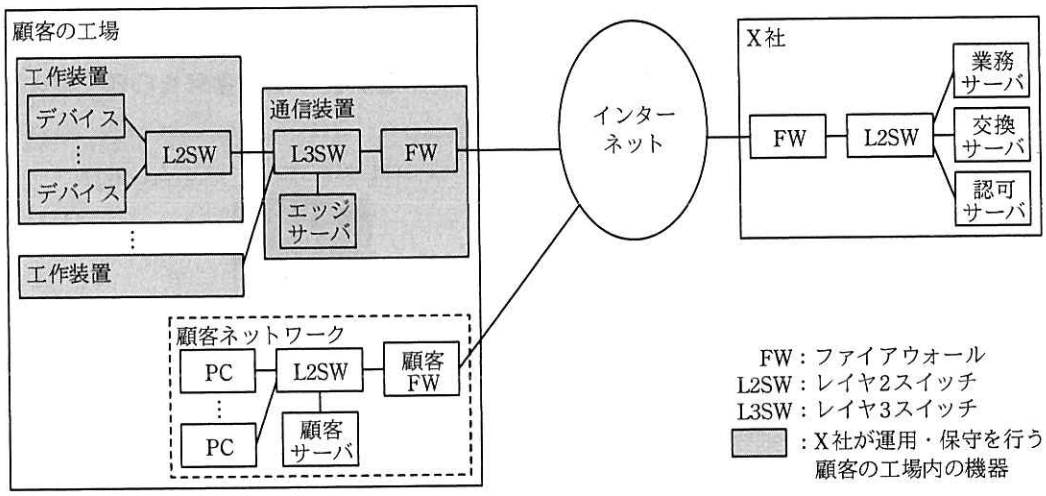


図１　X システムの導入構成例（抜粋）

X システムの業務アプリケーションプログラムは，エッジサーバと業務サーバ上で

動作する。これらのサーバとデバイスは，デバイスの運用・保守に関する情報を，自動的に交換する。この情報交換に関する説明を次に示す。

・工作装置と通信装置を接続し，顧客の工場内に X システム専用のネットワークを構成する。顧客ネットワークは利用しない。

・publish/subscribe 型のメッセージ通信プロトコル MQTT（Message Queuing Telemetry Transport）を使って，交換サーバを介して，デバイス，エッジサーバ及び業務サーバの間でメッセージを交換する。

・デバイス，エッジサーバ及び業務サーバに MQTT クライアント機能を，交換サーバに MQTT サーバ機能をそれぞれ実装する。

業務サーバは，顧客向けに API（Application Programming Interface）を提供する。顧客は，インターネット経由で API にアクセスし，デバイスの運用・保守に関する情報を参照する。この API に関する説明を次に示す。

・X 社の業務サーバと認可サーバに HTTP サーバ機能をそれぞれ実装する。

・顧客は，顧客サーバに，API アクセス用の Web アプリケーション（以下，WebAP という）と HTTP サーバ機能を実装する。

・顧客は，PC の Web ブラウザを使い，顧客サーバを経由して，API にアクセスする。

・X 社の認可サーバは，顧客サーバから API へのアクセスを認可する。

W さんは，上司から，X システムの構想に関する四つの技術検討を指示されている。四つの技術検討項目を次に示す。

・ネットワークセキュリティ対策

・MQTT を使ったメッセージ交換方式

・API にアクセスする顧客サーバの管理

・エッジサーバを活用する将来構想

〔ネットワークセキュリティ対策〕

X システムは，インターネット及び顧客の工場内の X システム専用のネットワークを利用するので，これらの X 社外の通信区間に関するネットワークセキュリティ対策が必要となる。W さんが検討したネットワークセキュリティ対策を次に示す。

・情報の漏えい及び改ざん対策のために TLS を利用する。TLS には，情報を［　ア　］する機能，情報の改ざんを［　イ　］する機能，及び通信相手を［　ウ　］する機能がある。

・工場内の機器と X 社内の機器との通信は，いずれもクライアントサーバ型の通信であり，機器間の［　エ　］コネクションの確立要求は，工場から X 社の方向に行われる。それを踏まえて，次の侵入及びなりすまし対策を採用する。

- X 社に設置された FW を使った対策
- ①通信装置内の FW を使った対策
- ② TLS の機能を使った，デバイス及びエッジサーバに関する対策

〔MQTT を使ったメッセージ交換方式〕

W さんは，MQTT を使ったメッセージ交換方式を調査した。

このメッセージ交換方式では，固定ヘッダ，可変ヘッダ及びペイロードから構成された MQTT コントロールパケットを使う。MQTT コントロールパケットの種別を表 1 に示す。

表 1　MQTT コントロールパケットの種別（抜粋）

種別	用途	固定ヘッダ，可変ヘッダ又はペイロードに含まれる情報
CONNECT	クライアントからサーバへの接続要求	（省略）
CONNACK	CONNECT に対する確認応答	（省略）
PUBLISH	メッセージの送信	QoS レベル[1]，トピック名[2]，パケット ID[3]，メッセージ
PUBREC	メッセージ受信の通知	パケット ID[3]
PUBREL	メッセージリリースの通知	パケット ID[3]
PUBCOMP	メッセージ送信終了の通知	パケット ID[3]
SUBSCRIBE	クライアントからサーバへの購読要求	QoS レベル[1]，トピック名[2]，パケット ID[3]
SUBACK	SUBSCRIBE に対する確認応答	パケット ID[3]

注[1] QoS レベルは，送信者と受信者間のメッセージの送達確認手順を指定する識別子である。
[2] トピック名は，メッセージの種類を表す識別子である。
[3] パケット ID は，PUBLISH 又は SUBSCRIBE に付与する識別子である。

MQTT を使ったメッセージ交換方式の通信シーケンス例を図 2 に示す。

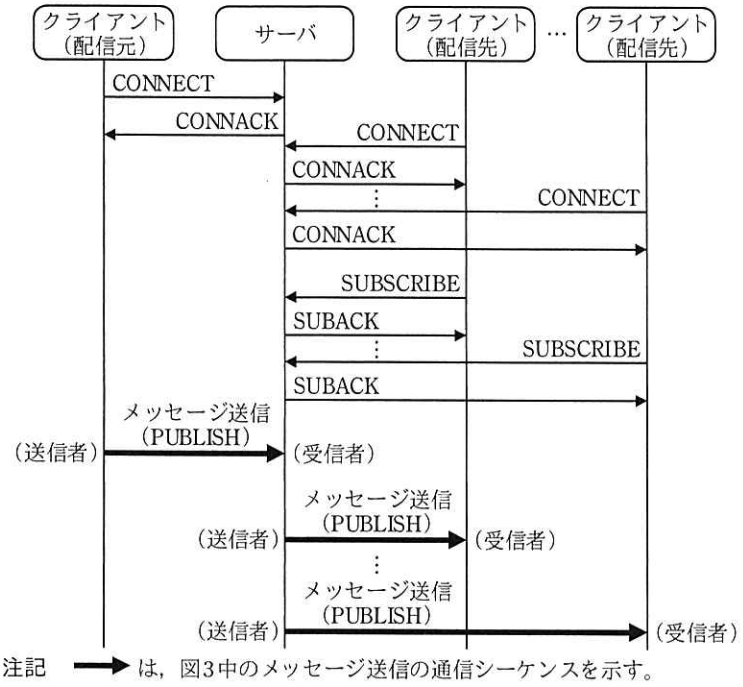


図 2　MQTT を使ったメッセージ交換方式の通信シーケンス例

図 2 中の通信シーケンスでは，配信元から複数の配信先へメッセージが配信されている。通信シーケンスの説明を次に示す。

・クライアントは，サーバの TCP ポート 8883 番にアクセスし，TCP コネクションを確立する。この TCP コネクションは，メッセージ交換の間は常に維持される。

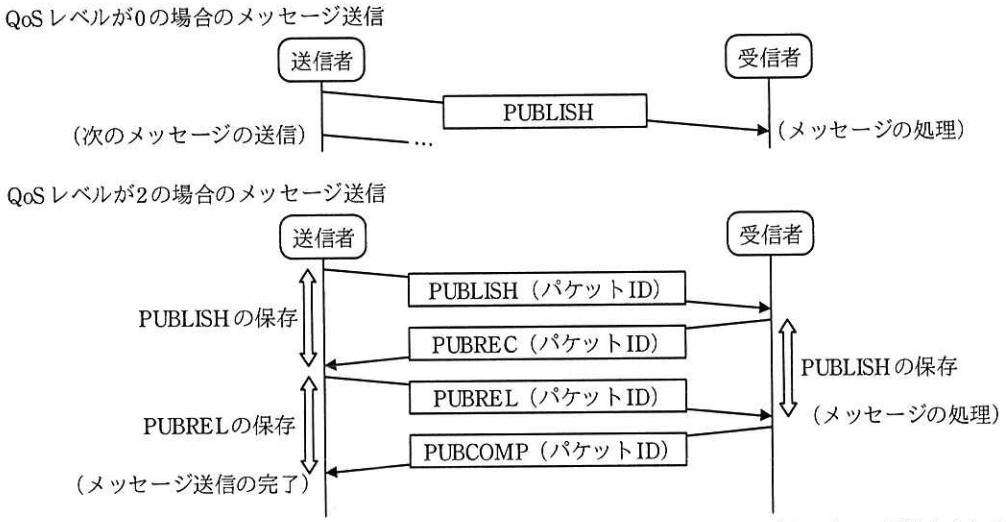
・クライアントは CONNECT を送信し，サーバは CONNACK を返信する。

・配信先となるクライアントは，サーバに SUBSCRIBE を送信し，購読対象のメッセージを，トピック名を使って通知する。サーバはクライアントに SUBACK を返信し，購読要求を受け付けたことを通知する。

・配信元クライアントは，PUBLISH を使ってサーバにメッセージを送信する。

・メッセージを受信したサーバは，PUBLISH に含まれるトピック名について購読要求を受け付けている全てのクライアントに，そのメッセージを送信する。

PUBLISH を使ったメッセージ送信では，QoS レベルを使って送達確認手順を指定する。QoS レベルとメッセージ送信の通信シーケンスを図 3 に示す。



注記 1　QoS レベルが 2 の場合，送達確認を行う PUBLISH を識別するために，パケット ID が付与される。
注記 2　QoS レベルが 2 の場合，受信者は，メッセージの処理を開始した以降に受信した PUBLISH は，パケット ID の重複にかかわらず新しいパケットとみなす。

図 3　QoS レベルとメッセージ送信の通信シーケンス

図 3 中の通信シーケンスの説明を次に示す。

・QoS レベルが 0 の場合，MQTT 層における PUBLISH の送達確認は行わない。TCP 層による送達確認だけが行われる。

・QoS レベルが 2 の場合，MQTT 層においても PUBLISH の送達確認が行われる。MQTT 層の送達確認の説明を次に示す。

- TCP コネクションが切断された場合のために，PUBLISH 及び PUBREL は送信者によって保存され，送信者から受信者への再送に利用される。
- ③ PUBLISH を受信した受信者は，メッセージの処理を始める前に送信者に PUBREC を送信し，その応答である PUBREL を受信してからメッセージの処理を開始する。
- PUBREL を送信した送信者は，その応答である PUBCOMP を受信してから，メッセージ送信を完了する。

次に W さんは，X システムの 2 種類のメッセージ交換について，トピック名，QoS レベル，及び配信元と配信先を整理した。

X システムのメッセージ交換を図 4 に示す。

項番	メッセージ交換の概要	QoS レベル	トピック名	メッセージ
1	業務サーバから，特定のデバイス Di に対して，設定情報を送信する。 業務サーバ → 交換サーバ → デバイスDi	2	config/Di	デバイス Di の設定情報
2	全てのデバイス Di（i=1，2，…，m）から，業務サーバ及び同じ工場のエッジサーバに対して，稼働情報を定期的に送信する。 デバイスD1 → 交換サーバ → 業務サーバ ⋮ デバイスDm → 交換サーバ → エッジサーバ	0	status/Di	デバイス Di の稼働情報

注記　Di は，デバイスの識別子を表す。

図４　Ｘシステムのメッセージ交換

図４の説明を次に示す。

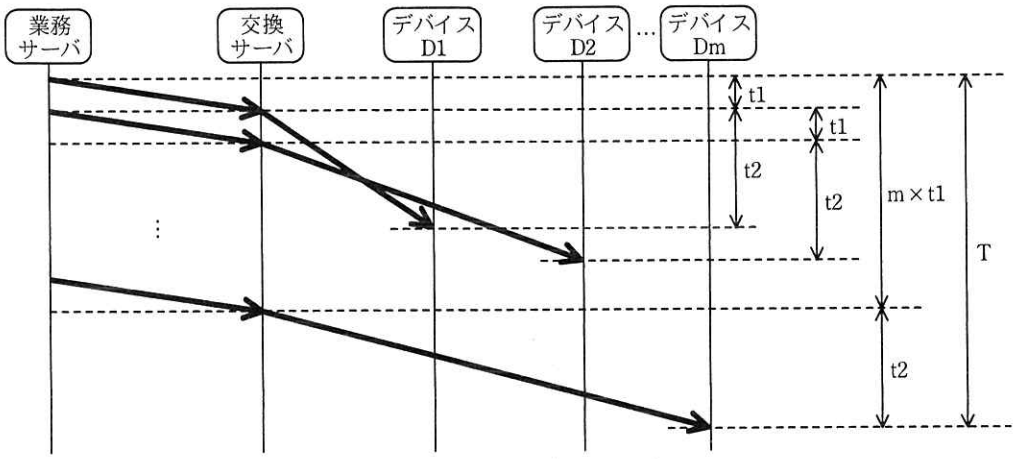
・項番 1 では，デバイス Di は，あらかじめ［　オ　］を交換サーバに送信し，トピック名が［　カ　］の PUBLISH が送信されるようにする。

・項番 1 では，QoS レベルとして 2 が使用されている。交換サーバからデバイス Di への PUBLISH 送信中に［　キ　］が電源断などで非稼働になった場合，その PUBLISH は，［　ク　］の中に保存され，稼働再開後に再送される。

・項番 2 では，QoS レベルとして 0 が使用されている。これは，［　ケ　］及びエッジサーバは安定した稼働が見込めるからである。

W さんは，1 台の業務サーバが 6,000 台のデバイスの設定を変更する場合の送信時間（T）を概算した。

W さんが T の概算に用いた通信シーケンスを図５に示す。



注記　太線の矢印は，QoS レベルが2の場合のメッセージ送信を表す。

図 5　W さんが T の概算に用いた通信シーケンス

図 5 中の装置の処理時間を無視し，図 5 中の t1 及び t2 は，それぞれの装置間の RTT（Round Trip Time）の 2 倍に等しいとし，LAN の RTT を 20 ミリ秒，WAN の RTT を 200 ミリ秒とすると，T は次のように概算できる。

$T = m \times t1 + t2 = 6{,}000 \times 2 \times 20 + 2 \times 200$（ミリ秒）≒ 4（分）

この概算を基に，W さんは，次のように報告することにした。

・TCP コネクションが正常であれば，全デバイスへの設定情報の送信は 4 分間程度で完了する。

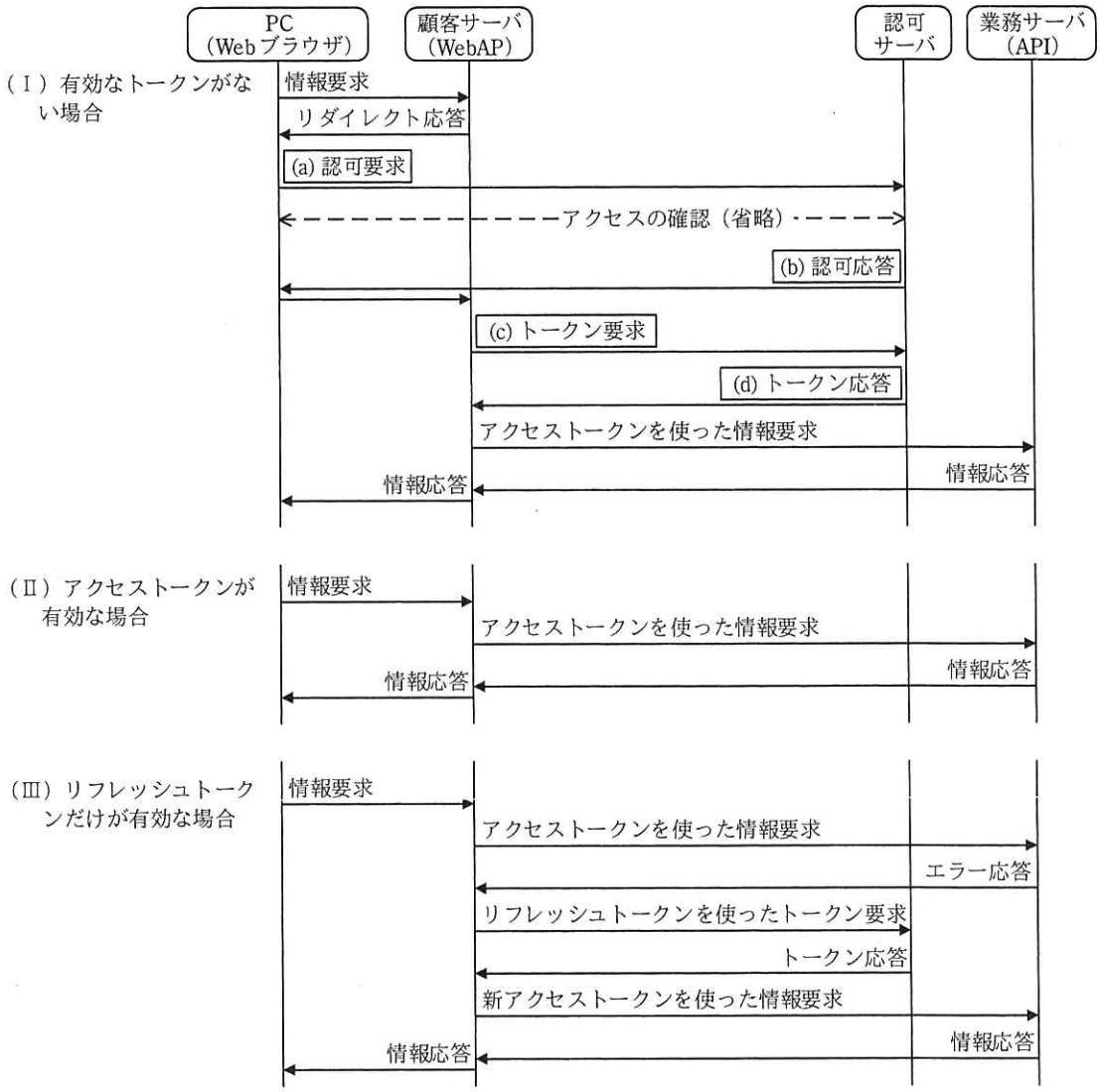
・ただし，図 1 に示すように，［　　コ　　］は同一拠点に設置されている必要がある。

〔API にアクセスする顧客サーバの管理〕

W さんは，顧客サーバからの API アクセスに関する検討を行った。

X システムでは，認可サーバを使って，顧客サーバからの API アクセスを認可する。契約及びサービス仕様の変更が顧客ごとに発生するので，それらを前提とした認可の仕組みが必要になる。W さんは，認可コード，アクセストークン，及びリフレッシュトークンを使った，認可の仕組みを採用することにした。

X システムの API アクセスの通信シーケンスを図 6 に示す。



(a) 認可要求：
```
GET /authorize?redirect_uri=【WebAPIのURI】（省略）
HOST:【認可サーバ】
```

(b) 認可応答：
```
HTTP/1.1 302 Found
Location: 【WebAPIのURI】?code=【認可コード】
```

(c) トークン要求：
```
POST /token HTTP/1.1
（省略）
（省略）code=【認可コード】&redirect_uri=【WebAPIのURI】（省略）
```

(d) トークン応答：
```
HTTP/1.1 200 OK
(省略)
【アクセストークン】,【リフレッシュトークン】(省略)
```

図 6　X システムの API アクセスの通信シーケンス

図 6 中の（Ⅰ）に示すように，有効なトークンがない場合，Web ブラウザから

WebAP への情報要求は，［　サ　］サーバにリダイレクトされる。認可応答では，認可要求で通知された URI を用いたリダイレクトによって，［　シ　］に認可コードが通知される。続いて，認可コードを用いたトークン要求とトークン応答が行われ，WebAP はアクセストークンとリフレッシュトークンを獲得する。

図 6 中の（Ⅰ）～（Ⅲ）に示すように，業務サーバへの情報要求には，アクセストークンが用いられる。アクセストークンには，アクセス可能な API と有効期間に関する情報が含まれており，業務サーバはそれらの情報からアクセスの可否を決める。アクセストークンの有効期間を過ぎた場合でも，［　ス　］の有効期間内であれば，利用者の確認を行わずに，新しいアクセストークンが発行される。

X システムでは，顧客ごとに異なるアクセストークンを定義し，認可サーバに格納しておく。ある顧客に提供する API の範囲が変わる場合，X 社は認可サーバのアクセストークンを変更する。W さんは，④アクセストークンの有効期間を 10 分間，リフレッシュトークンの有効期間を 60 分間と想定し，トークンの運用を確認した。

図 6 の通信シーケンスでは，図 6 中の“(a) 認可要求”の redirect_uri パラメタが書き換えられ，図 6 中の［　セ　］に含まれる認可コードが意図しない宛先に送信される可能性がある。W さんは，その対策として“redirect_uri パラメタの確認”を行うことにした。これは，図 6 中の［　ソ　］サーバに，HTTP リクエストに含まれる URI とあらかじめ登録されている絶対 URI が一致することを確認させる，という対策である。⑤顧客向けの API 利用ガイドラインには，この対策に必要な顧客への依頼内容を明記することにした。

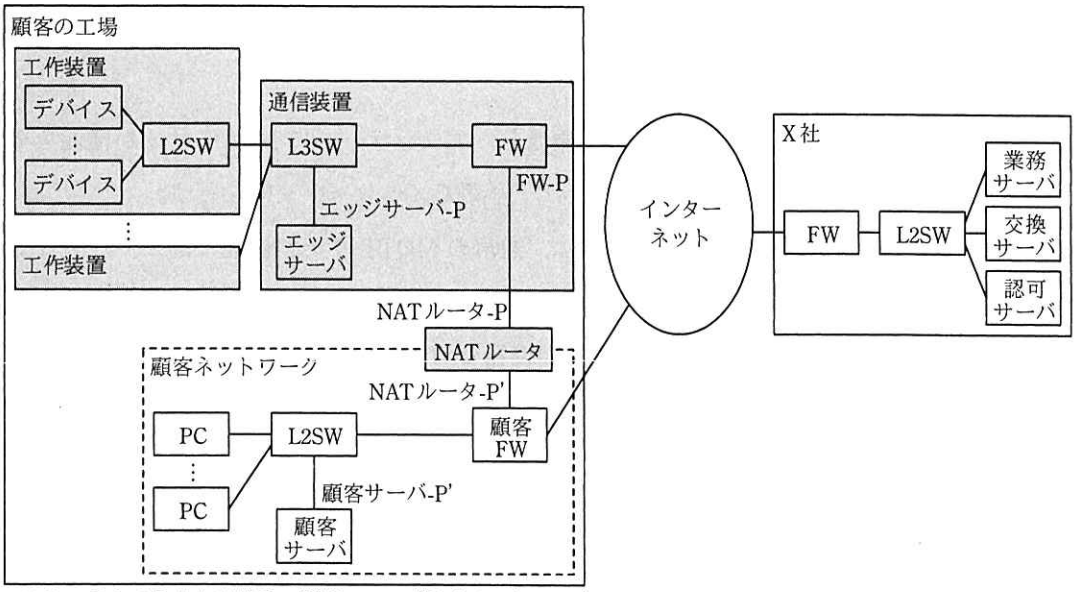
〔エッジサーバを活用する将来構想〕

図 4 中のメッセージ交換では，X 社内の交換サーバを利用するので，顧客の企業秘密を含むような設定情報及び稼働情報（以下，これらを内部情報という）は，対象外としている。しかし，内部情報についても図 4 と同様にメッセージ交換を行いたい顧客も多い。X 社では，エッジサーバを活用して，内部情報も X システムに取り込む将来構想をもっている。

顧客サーバが一つの場合について，将来構想で追加される X システムのメッセージ交換例を図 7 に，W さんが考えた将来構想におけるネットワーク構成案を図 8 に，それぞれ示す。

メッセージ交換の概要	トピック名	メッセージ
顧客サーバと同じ工場のデバイス Di（i=1，2，…，m'）間で，エッジサーバを使って，顧客の工場に閉じた情報交換を行う。 顧客サーバ ←→ エッジサーバ ←→ デバイスD1 … デバイスDm'	Confidential/Di	デバイス Di に関する内部情報

図７　将来構想で追加されるＸシステムのメッセージ交換例



ddd-P　：Xシステムにおける，機器dddのプライベートIPアドレス
ddd-P'：顧客ネットワークにおける，機器dddのプライベートIPアドレス

図８　Ｗさんが考えた将来構想におけるネットワーク構成案（抜粋）

図８に示すように，Ｗさんは，NATルータを使って，顧客ネットワークとＸシステムを接続する案を考えた。NATルータは，1：1静的双方向NATとして動作させ，図８中のNATルータ-PとNATルータ-P'を利用して，宛先IPアドレスと送信元IPアドレスの両方を変換させる。

Ｗさんが考えた将来構想におけるメッセージの流れを図９に示す。

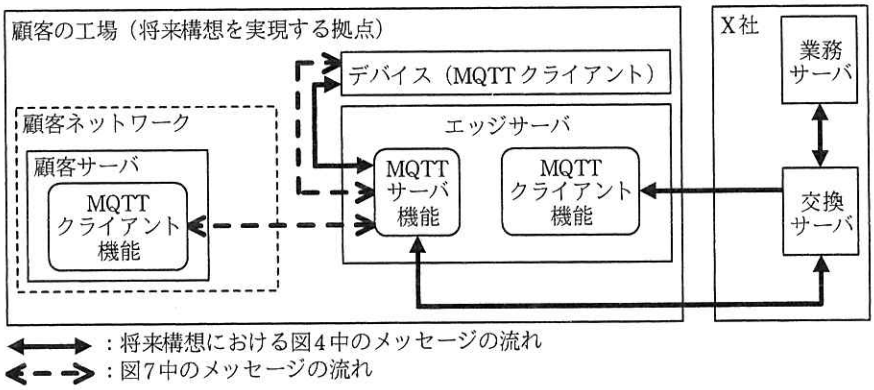


図9　Wさんが考えた将来構想におけるメッセージの流れ

図9の説明を次に示す。

・顧客サーバにMQTTクライアント機能を，エッジサーバにMQTTサーバ機能をそれぞれ実装し，顧客サーバとエッジサーバ間でメッセージ交換を行う。

・エッジサーバのMQTTサーバ機能は，通常のMQTTサーバ機能に加えて，メッセージをほかのMQTTサーバと送受信する機能（以下，MQTTブリッジという）をもつ。Xシステムのデバイスは複数の機器とTCPコネクションを確立できないので，このMQTTブリッジを利用する。

・⑥MQTTブリッジには，トピック名をあらかじめ定義しておき，そのトピック名のメッセージを交換サーバと送受信させる。

Wさんは，図7～9を使って，ネットワークの動作について検討し，将来構想への対応が可能であると判断した。

Wさんは，以上の検討結果を上司に報告した。X社の情報システム部は，Xシステム構想を実現するためのプロジェクトを発足させた。

設問1　〔ネットワークセキュリティ対策〕について，(1)～(3)に答えよ。

(1)　本文中の［　ア　］～［　エ　］に入れる適切な字句を答えよ。

(2)　本文中の下線①の対策を，50字以内で述べよ。

(3)　本文中の下線②の対策を，30字以内で述べよ。

設問２　〔MQTT を使ったメッセージ交換方式〕について，(1)～(4) に答えよ。

(1) 図 3 中の QoS レベルが 0 の場合のメッセージ送信について，TCP の再送機能だけではメッセージの消失が防げないのはどのような場合か。45 字以内で具体的に答えよ。

(2) 本文中の下線③について，PUBREL を受信するまで，メッセージの処理を保留する目的を，20 字以内で述べよ。

(3) 本文中の［　オ　］～［　ケ　］に入れる適切な字句を答えよ。

(4) 本文中の［　　コ　　］に入れる適切な機器名を全て答えよ。

設問３　〔API にアクセスする顧客サーバの管理〕について，(1)～(3) に答えよ。

(1) 本文中の［　サ　］～［　ソ　］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，提供する API の範囲を変更する場合，変更が有効になるのは，X 社がアクセストークンを変更してから最長で何分後かを答えよ。

(3) 本文中の下線⑤について，顧客への依頼内容を，40 字以内で述べよ。

設問４　〔エッジサーバを活用する将来構想〕について，(1)～(4) に答えよ。

(1) 図 8 中の NAT ルータについて，顧客ネットワークから X システムの方向の通信におけるアドレス変換の内容を，60 字以内で具体的に述べよ。

(2) 図 8 中の顧客 FW について，X システムとの接続のために，新たに許可が必要になる通信を 40 字以内で答えよ。

(3) 本文中の下線⑥について，定義するトピック名を全て答えよ。

(4) 図 7～9 中の顧客サーバを 1 台追加する場合，X システム側で必要となる対応を二つ挙げ，それぞれ 30 字以内で述べよ。