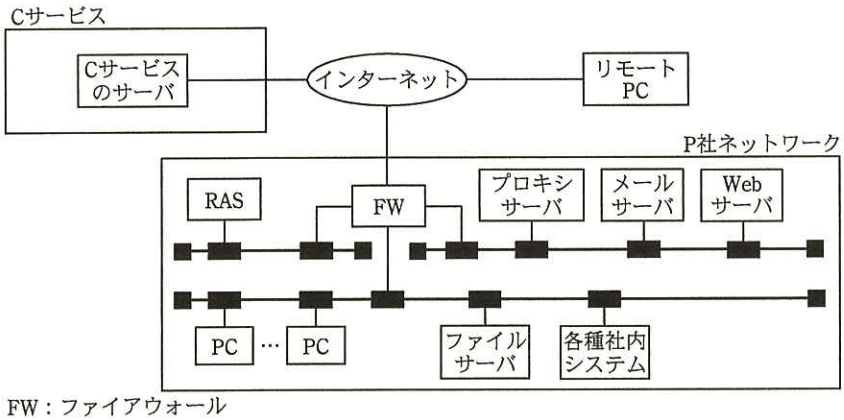
問3　パブリッククラウドサービスの安全な利用に関する次の記述を読んで，設問1～3に答えよ。

P社は，経営コンサルティングを行っている，従業員数60名の会社であり，オフィスは東京にある。P社には，オフィスに常勤している従業員と，主に客先や自宅で作業を行い，打合せのときだけオフィスに出社する従業員がいる。

社内にファイルサーバを設置して利用していたが，容量は十分であるものの検索の機能が不十分なことから，高機能のファイル共有サービス（以下，Cサービスという）を提供しているC社と契約し，Cサービスを利用し始めた。Cサービスは，ブラウザ経由でアクセスできるSaaS型パブリッククラウドのサービスである。P社は，Cサービスのサーバ内にP社専用の領域を確保して，使用履歴，作成者名，メモなどの情報を添えた上でプロジェクト資料を保管している。P社では，Cサービスを活用することで，検索を高速に行えるようになり，業務効率が格段に向上するものと見込んでいる。

客先や自宅で作業を行う従業員には，社外で利用するためのPC（以下，リモートPCという）を貸与しており，リモートPCをインターネットに接続できれば，リモートアクセスサーバ（RAS）経由で社内に接続し，社内システムにアクセスできる。客先や自宅からCサービスへのアクセスは，P社ネットワークを経由せずに直接行う。ネットワーク構成の概要を図1に示す。



FW：ファイアウォール

図1　ネットワーク構成の概要

〔C サービスの認証の強化〕

C サービスの契約と利用者管理については，総務部の X 課長が管理責任者を務めている。C サービスの採用については，C サービスが停止するような事態が発生した場合の事業継続について具体的対策を 1 年以内にまとめることを条件に社長の了承を得ていた。

契約後に，“あるパブリッククラウドサービスから，パブリッククラウドサービス会社の管理が不十分であったのでパスワードが大量に漏えいし，保存されていたデータが漏えいした”との報道があった。漏えいがあったパブリッククラウドサービス会社は C 社ではなかったが，報道を聞いた P 社の社長は，C サービスで保管している情報が漏えいして多大な損害が発生することを懸念し，X 課長に，C サービスを利用する際の認証の強化を検討するように指示した。X 課長は，部下の Q さんに，認証の強化策を調査するよう指示した。

Q さんはまず，C サービスのセキュリティに関する機能を表 1 にまとめた。

表 1　C サービスのセキュリティに関する機能（抜粋）

番号	項目	機能	備考
1	利用領域へのアクセス制御	契約会社ごとに割り当てられた領域だけにアクセスできる。	P 社が契約している領域は，200 G バイトである。
2	利用者管理	契約会社内の管理責任者が，C サービスの利用者管理機能を使って自社の利用者 ID を管理する。	管理責任者は，アクセス履歴も確認できる。
3	通信路暗号化	通信路は，サーバ認証による SSL で暗号化される。	
4	利用者認証	Web 画面で入力された利用者 ID（会社が利用者に付与したメールアドレスを利用者 ID として使用）とパスワードを，C サービス内で照合し，利用者認証を行っている。認証情報は，利用者 ID とパスワードが必須である。 追加オプションとして，ログイン手続中に，利用者のメールアドレスに送信したワンタイムパスワードも入力する方式（以下，追加認証方式という）が用意されている。	全ての契約会社の利用者が，同じ URL の Web 画面からログインする。

Q さんは，利用者が個人所有の携帯電話メールアドレスを活用することも視野に入れて，追加認証方式の利用について検討した。検討結果を(1)～(3)に示す。

(1)　業務上の支障の有無

次の理由から，業務上の支障はないと判断した。

・P 社では，P 社が契約した携帯電話を多くの従業員に貸与しており，個人所有を含めると全従業員が携帯電話を利用できる。

・携帯電話の故障，紛失などが年に数件発生しているが，個人所有の場合も含めて，携帯電話業者に依頼すれば速やかに同一電話番号かつ同一メールアドレスで利用が再開できる。

なお，P 社貸与の携帯電話は，盗難，紛失があった場合には必ず総務部に連絡することになっている。盗難届，紛失届を受けると総務部は，速やかに対応している。

(2) 認証強度

他のパブリッククラウドサービスで利用者のパスワードが漏えいした事件を踏まえ，C サービスの利用者 ID とパスワードが漏えいした場合であってもなりすましが困難であるかどうかを評価することにした。

(3) 追加認証方式の手順

Q さんは，追加認証方式について，次の手順案を作成した。

・C サービスの利用者 ID 登録手順案（図 2）

・C サービスの利用者 ID 変更手順案（図は省略）

・認証の手順案（図 3）

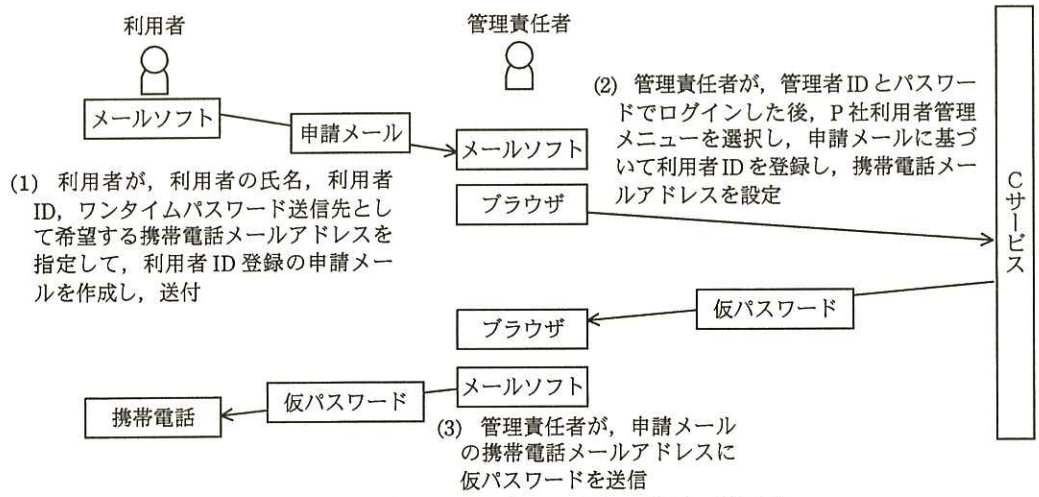
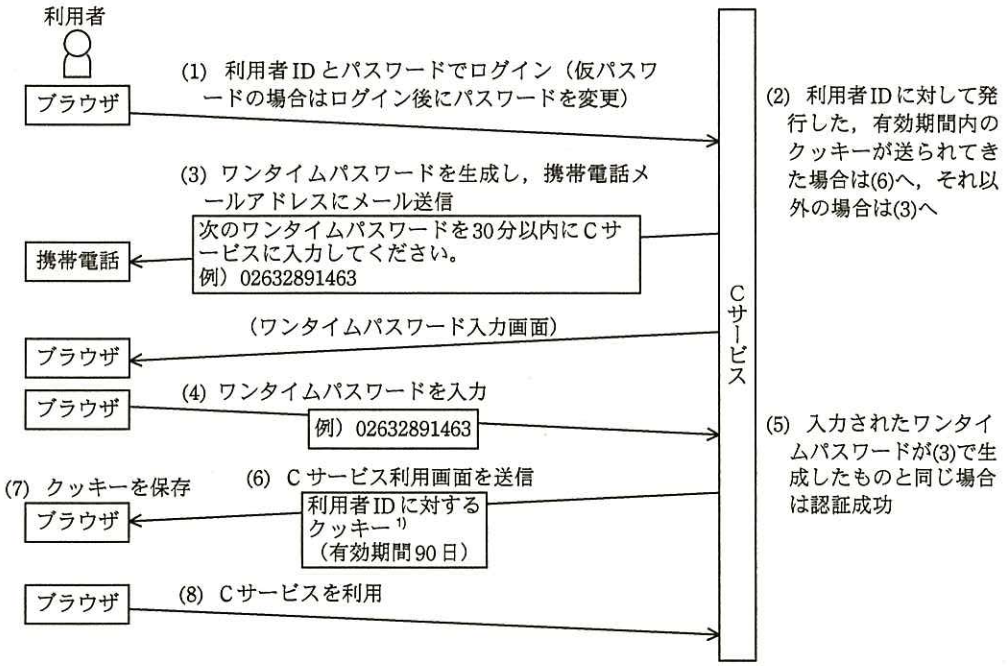


図 2　C サービスの利用者 ID 登録手順案（抜粋）



注[1] (5)で認証が成功した場合だけ新たにクッキーが生成され，ブラウザに保存される。
同じ利用者IDに対してさらに他のクッキーが生成された場合でも，このクッキーは90日間有効である。

注記 ログイン状態が24時間以上継続すると，自動的にログアウトされ，再度(1)から認証を行う。

図3 認証の手順案（抜粋）

Q さんが手順案を X 課長に提示したところ，“図 2 の手順では，①第三者が利用者になりすまして，仮パスワードを簡単に入手できてしまう”と指摘された。

さらに，“個人の携帯電話が盗まれ，かつ，利用者 ID とパスワードが推測されてしまったときに，② C サービスが不正使用され，しかも，それが長期間続くおそれがある”と指摘された。Q さんは，それらの指摘に対応するため，手順を修正し，対策を追加した。

修正後，追加認証方式は，十分な認証強度をもっていると判断され，P 社では追加認証方式を採用することになった。

〔C サービスを利用できない場合の対応〕

Q さんは，C サービスが停止するような事態が発生した場合の具体的な対策を検討し，表 2 にまとめた。

表2　Cサービスが停止するような事態が発生した場合の具体的な対策

想定シナリオ	求められる業務レベル	事前準備として実施すること	想定シナリオが現実化してから実施すること
C サービスのサーバが被災し，停止するが，2週間後に元どおり再開する。	業務効率の低下は許容するが，C サービス停止の 24 時間後にはプロジェクト資料を使う業務を再開できる。	[a] しておく。	ファイルサーバを用いて，[b] する。ただし，C サービス復旧後は，C サービスの利用を再開する。
C 社が，1か月後に C サービスの提供を終了すると通知し，実際に 1 か月後にサービス終了となる。	業務効率を低下させることなく業務を継続できる。	C サービスに代替可能なサービスを選定しておく。 C サービスからの [c] を確認しておく。	代替サービスと契約する。 代替サービスのセットアップ（ID 登録や設定）を行う。 C サービスのデータを代替サービスに移行する。 代替サービスの利用方法を従業員に周知する。

表 2 の内容は承認され，P 社の事業継続計画に盛り込まれた。定期的に訓練が実施されることになり，その後，新しい手順で C サービスの利用が開始された。

設問 1　本文中の下線①について，どのような方法で第三者が仮パスワードを入手することができるか。また，その対策としてどのように本人確認すればよいか。それぞれ 25 字以内で述べよ。

設問 2　本文中の下線②について，不正使用が長期間続く理由を 30 字以内で，対策を 70 字以内で具体的に述べよ。

設問 3　表 2 中の [a] ～ [c] に入れる実施事項を，[a] は 35 字以内で，[b] は 25 字以内で，[c] は 15 字以内で述べよ。