

平成 19 年度 春期 テクニカルエンジニア（情報セキュリティ） 午後Ⅱ問題

問 1 基幹 Web システムにおけるセキュリティ設計に関する次の記述を読んで，設問 1 ～ 4 に答えよ。

X 社は，従業員数 2,000 名の中堅信販会社である。X 社では，大型汎用機で構成された基幹システムによって，各支店と現金自動預払機（ATM）を通じた融資サービスを提供している。X 社は，現行基幹システムの老朽化対策と事業拡大を目的として，代理店及び一般顧客がインターネット経由でも融資サービスを利用できる新しい基幹 Web システム（以下，C システムという）を開発し，システム移行後に現行基幹システムを廃棄することにした。現在，X 社内では，情報システム部門において，C システムの要件整理が完了し，概要設計を終えようとしている。

C システムの Web サーバで動作する業務アプリケーションは，融資受付サービス，融資受付代行サービス，残高照会サービス，入出金サービス及び顧客情報検索サービスの五つの業務サービスを提供する。これらの業務サービスのうち，顧客情報検索サービスでは，各支店の営業員による支店 PC からのアクセスに対して，営業員の認証が行われる。認証が正常に行われた後，営業員が口座をもつ顧客の口座番号，カナ姓，カナ名，電話番号の各項目を任意に指定して顧客情報を検索すると，検索結果リストが表示される。また，検索効率向上のために，カナ姓の一部又はカナ名の一部の指定による部分一致検索を可能にする。表示された検索結果リストから，営業員が任意の顧客を選択すると，当該顧客の顧客情報及び債権管理情報が表示される。

C システムの運用管理は，現行基幹システムと同様に，システム管理者，データベース（DB）管理者，業務アプリケーション管理者という 3 種類の運用管理者によって行われることが決まっており，複数の役割を兼任することは禁止されている。サーバ及びネットワーク機器を運用管理するシステム管理者は，X 社情報システム部門又は運用委託業者の従業員の中から任命され，X 社データセンタ内で各サーバ及びネットワーク機器を直接操作する。DB を運用管理する DB 管理者は，X 社情報システム部門又は運用委託業者の従業員の中から任命され，X 社データセンタ内で DB サーバを直接操作する。業務アプリケーションを運用管理する業務アプリケーション管理者は，X 社情報システム部門又は運用委託業者の従業員の中から任命され，X 社データセンタ内で Web サーバを直接操作する。

C システムの品質要件（抜粋）を図 1 に，C システムが遵守すべき X 社の情報セキュリティ標準（抜粋）を図 2 に，それぞれ示す。

- ・顧客情報検索の応答時間は 3 秒以内とする。
- ・ピーク時においては，最大 50 件／秒までの顧客情報検索サービスを処理可能とする。
- ・顧客数は最大 100 万人とする。
- ・計画停止時間は 2 時間以内とする。
- ・X 社の情報セキュリティ標準を遵守する。
- ・テーブル内のレコードが氏名（姓及び名の両方）及び生年月日を含む場合は，キー項目以外の各データ項目を暗号化し，暗号鍵を定期的に変更する。

図 1 C システムの品質要件（抜粋）

1. 情報分類

X 社情報セキュリティポリシーに基づき, X 社内で取り扱う情報を, 公開情報, 社内情報, 機密情報, 極秘情報に分類する。

- (1) 公開情報とは, 社外に公開可能な情報である。
- (2) 社内情報とは, X 社内だけで取り扱い, 社外に公開しない情報である。
- (3) 機密情報とは, X 社の人事, 経営戦略に関する情報及び顧客に関する情報（取引口座, 融資取引, 与信, 債権に関する情報など）である。
- (4) 極秘情報とは, 融資取引において, 顧客の本人確認のために使用する暗証番号である。

2. セキュリティ対策

X 社内においては, それぞれの情報分類に関して次のセキュリティ対策を実施する。

2.1 公開情報に関するセキュリティ対策

(省略)

2.2 社内情報に関するセキュリティ対策

社内情報に関しては, 次の 的セキュリティ対策を実施する。

- (1) オフィスエリアに保管する。オフィスエリアは, 監視カメラ又は警備員によって出入口が監視されているエリアとする。

2.3 機密情報に関するセキュリティ対策

機密情報に関しては, 社内情報に関する対策に加えて, 次の 的セキュリティ対策及び 的セキュリティ対策を実施する。

- (1) 的セキュリティ対策
 - ・オフィスエリア内に設けた制限エリアに保管する。制限エリアは, 指紋認証による入退室管理を行い, 必要最小限の運用管理者だけが入室可能なエリアとする。
- (2) 的セキュリティ対策
 - ・アクセスの際は, 利用者本人であることを確認するために, 利用者認証を実施する。
 - ・権限をもつ利用者だけにアクセスを限定するために, アクセス制御を実施する。
 - ・疑わしいアクセスを発見し, アクセス元の個人を特定できるようにするために, アクセス記録を取得し, 1年間保管する。
 - ・制限エリアから外に持ち出す場合, 及び通信回線を介して制限エリアの外へ送信する場合は, 暗号化を実施する。暗号鍵は定期的に変更する。

2.4 極秘情報に関するセキュリティ対策

極秘情報に関しては, 機密情報に関する対策に加えて, 次の 的セキュリティ対策を実施する。

- (1) 的セキュリティ対策
 - ・電子記憶媒体に保存する場合は, 暗号化を実施し, 暗号鍵を定期的に変更する（ただし, データ処理のために一時的に保管し, 処理終了後に消去される場合はこの限りでない）。

図2 X社の情報セキュリティ標準（抜粋）

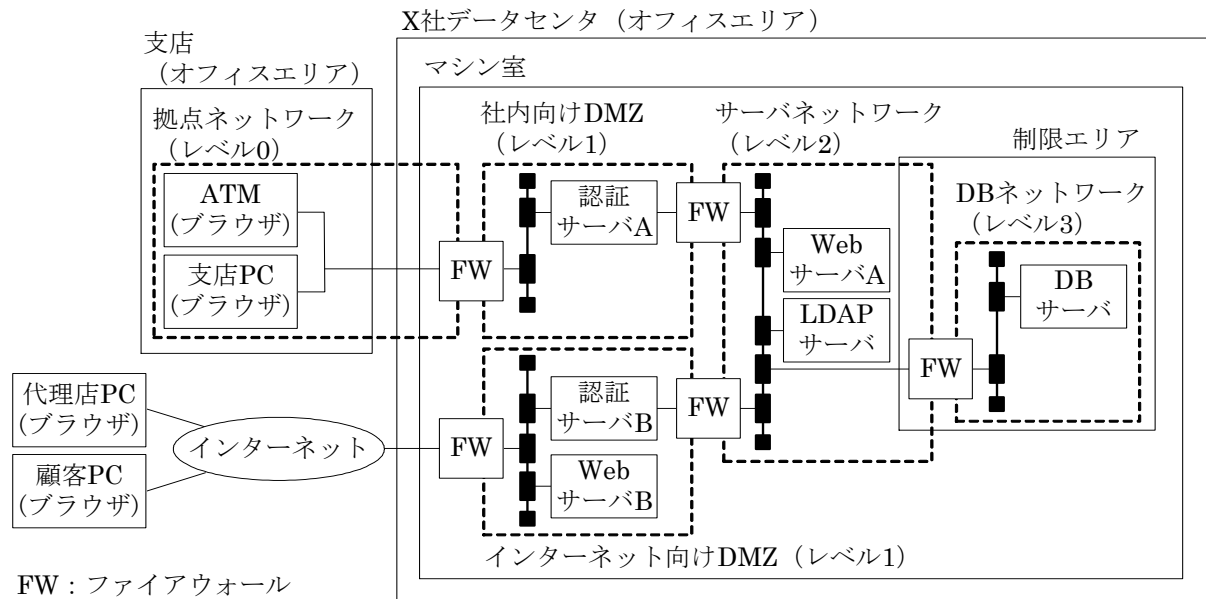
これまで，X 社においては，C システムの概要設計に対して，セキュリティの観点からの検証が行われていたが，設計者のスキル不足から，検証作業が遅れていた。X 社は，進捗の遅れを取り戻すために，SI ベンダの Y 社に C システムの概要設計に対する検証作業と必要な改善を依頼した。Y 社のセキュリティ技術者である T 氏は，X 社内で C システムの設計全体のリーダーとセキュリティ設計担当を兼任している S 氏から，C システムの概要設計について説明を受けた。後日，T 氏は，改善案をまとめて，S 氏との検討に臨んだ。次は，そのときの T 氏と S 氏のやり取りである。

[システム構成の改善]

T 氏：まず，C システムのシステム構成改善案について，ご説明します。考慮すべき点が幾つかあるので，C システムのネットワークセキュリティ設計方針を図 3 にまとめました。この設計方針に基づいて作成した C システムのシステム構成改善案を図 4 に，システム構成改善案の補足説明を図 5 に示します。

1. ファイアウォールで区分された X 社内のネットワークをセキュリティゾーンとする。各セキュリティゾーンに対して，次のセキュリティレベルを割り当てる。
 - レベル 0：クライアント PC を配置する社内ネットワーク
 - レベル 1：DMZ
 - レベル 2：認証された利用者に対して業務サービスを提供するサーバを配置するネットワーク
 - レベル 3：DB を配置するネットワーク
2. 各セキュリティレベルのセキュリティゾーンに配置可能な蓄積データ（一時的な保管データは除く）の情報分類は，次のとおりとする。
 - レベル 0：公開情報
 - レベル 1：公開情報
 - レベル 2：公開情報，社内情報
 - レベル 3：公開情報，社内情報，機密情報，極秘情報
3. 各セキュリティゾーンでは，セキュリティレベルに応じて次のセキュリティ対策を実施する。
 - レベル 0：オフィスエリアに配置する。
 - レベル 1：オフィスエリアである X 社データセンタ内のマシン室に配置する。マシン室は IC カードによる入退室管理を行い，必要最小限の運用管理者だけが入室可能なエリアとする。
 - レベル 2：レベル 1 と同じ対策を実施する。
 - レベル 3：マシン室内に設けた制限エリアに配置する。
4. セキュリティゾーンの構成及び通信は，次のとおりとする。
 - ・セキュリティレベルが 2 以上異なるセキュリティゾーンは隣接させない。
 - ・運用管理のための通信は，セキュリティゾーン内だけで行う。
 - ・セキュリティゾーン間の通信は，隣接するセキュリティゾーン間だけで許可する。
 - ・セキュリティゾーン内の通信には制約を設けない。
 - ・インターネットは，レベル 1 のセキュリティゾーンに隣接させる。

図 3 C システムのネットワークセキュリティ設計方針



注 ルータは，記述を省略している。

インターネットは，どのセキュリティレベルにも該当しない。

図4 Cシステムのシステム構成改善案

- ・ 認証サーバはリバースプロキシとして動作する。ブラウザからは，認証サーバが Web サーバに見える。
- ・ 認証サーバは，ブラウザから入力された認証情報を LDAP サーバに送信し，LDAP サーバは認証サーバから受信した認証情報と登録された認証情報を比較して，認証結果を認証サーバに返す。
- ・ 業務アプリケーションのうち，一部の融資受付サービスを提供する業務アプリケーションは，利用者認証を必要としないため，Web サーバ B に配置される。その他の業務アプリケーションは Web サーバ A に配置される。
- ・ 業務アプリケーションと DBMS との間においては，コネクションプーリングを使用する。すなわち，業務アプリケーションが DBMS の利用者 ID を使用して確立したコネクションを，複数のトランザクションで共用する。DBMS からは，業務アプリケーションとの間において確立されたコネクションが，1 人の DBMS 利用者に見える。

図5 システム構成改善案の補足説明

S 氏 : X 社内で検討した構成では，認証サーバと Web サーバ B を DMZ に配置し，それ以外のサーバはすべて同じネットワークに配置していました。①Web サーバ A と DB サーバを別のセキュリティゾーンに配置したのはなぜでしょうか。

T 氏 : この二つのサーバについては，運用管理者の作業内容と②情報セキュリティ標準を考慮して，このような配置にしました。

S 氏 : 了解しました。

[利用者認証とログ管理の改善]

T 氏 : 次に，C システムのセキュリティ設計について検討しましょう。利用者認証の設計は複雑でした

ので，内容を再確認させてください。

S 氏：C システムの業務サービスは，3 種類の利用者認証を使用します。業務サービスが使用する利用者認証を，表 1 に示します。

表 1 業務サービスが使用する利用者認証

| | アクセス認証 | 取引認証 | DB 認証 |
|----------------------|--|------------|--|
| 認証機能の実装箇所 | 認証サーバ | 業務アプリケーション | DBMS |
| 使用する認証情報 | 業務サービスの利用者 ID (以下，業務ユーザ ID という) 及びパスワード (以下，業務パスワードという) | 口座番号及び暗証番号 | DBMS の利用者 ID (以下，DB ユーザ ID という) 及びパスワード (以下，DB パスワードという) |
| 認証情報の保管場所 | LDAP サーバ | DB | DBMS |
| 認証対象の利用者又は認証情報の割当て対象 | 各支店営業員，各代理店営業員，各顧客，各 ATM | 各顧客 | 各 DB 管理者，業務アプリケーション |

T 氏：認証については了解しました。ログ管理についても確認させてください。

S 氏：ログ管理は，DB サーバで動作する DBMS が，実行された SQL 文，SQL 文の実行結果（成功か失敗か），SQL 文が実行された年月日時分秒，及び SQL を実行した DB ユーザ ID をアクセス記録として取得し，保存することで実現します。

T 氏：③このログ管理方式では，御社の情報セキュリティ標準を遵守できないので変更すべきでしょう。改善策として，④ログの取得箇所を変更し，アクセス記録で個人を特定できるようにする方式を提案します。ただし，そのためには，必要な情報を認証サーバから Web サーバの業務アプリケーションに渡す必要があります。この方式では，実行された SQL 文，SQL 文の実行結果，及び SQL 文が実行された年月日時分秒も記録できます。

S 氏：ログ管理については DB 担当者に任せていたので，見落としていました。今後は DB 担当者との連携を強化するようにします。

[データ暗号化の検討]

T 氏：最後に，データ暗号化について検討しましょう。

S 氏：暗号化及び復号の処理は，業務アプリケーションがハードウェア暗号モジュールの機能呼び出して，データ項目ごとに順次処理する方式にしました。DBMS がもつデータ暗号化の機能を使用する方式も検討しましたが，今回は安全な鍵管理機能をもっているハードウェア暗号モジュールを採用することにしました。C システムの DB 設計案を，表 2 に示します。

表 2 C システムの DB 設計案

| テーブル名 | キー項目 | データ項目 | | | | | | |
|----------------|-----------------|--------|--------------|------|-----|------|------|-----|
| | | 暗証番号 | 住所 | カナ姓 | カナ名 | 電話番号 | 生年月日 | 勤務先 |
| 顧客 TBL | 口座番号 | 暗証番号 | 住所 | カナ姓 | カナ名 | 電話番号 | 生年月日 | 勤務先 |
| 取引 TBL | 取引番号 | 年月日時分秒 | 口座番号 | 入出金額 | — | — | — | — |
| 与信 TBL | 口座番号 | 与信残高 | 与信限度額 | — | — | — | — | — |
| 債権回収 記録 TBL | 口座番号， 年月日時分秒 | 取引番号 | 顧客との 連絡記録 | — | — | — | — | — |

T 氏：DB に保管されるデータの暗号化は，システムのセキュリティ以外の品質にも様々な影響を与えます。まず，顧客情報検索サービスにおける部分一致検索の応答時間への影響を評価してみました。顧客情報検索サービスの部分一致検索は，DBMS の LIKE 演算子を使った方式となっています。例えば，カナ姓に対して“オオタ*”という条件で検索すると，処理される SQL 文に LIKE ‘オオタ%’ という検索条件が付き，カナ姓の項目が“オオタ”で始まるレコードが検索されます。今回使用する DBMS 製品は，特定の列を索引項目として定義すると，索引項目のデータとテーブルにおける当該レコードの位置情報から成る索引を生成します。索引中のレコードは索引項目の順に並んでおり，索引項目による検索が効率よく行われます。カナ姓を索引項目とした場合，索引を読んで“オオタ”で始まる各レコードの位置が分かると，テーブルに対してはレコード位置を基に検索結果の各レコードだけを読みればよいこととなります。検索結果が 100 件となる部分一致検索の処理時間について，弊社の DB 技術者の協力を得て概算したところ，索引項目が暗号化されない場合は，索引による効果が大きく，約 1 秒という結果になりました。一方，索引項目を暗号化すると，索引による効果は得られず，テーブルの全レコードに対して順次アクセスすることになるので，約 500 秒という結果になりました。

S 氏：処理時間を 1 秒以内に抑えるために，DB サーバの資源を 500 倍に増強することは不可能ですね。

T 氏：暗号化による影響はこれだけではありません。顧客 TBL に対して，図 1 の品質要件で要求されている暗号鍵の変更を行った場合，それに伴って必要となるデータ移行時間を評価してみました。C システムにおける，データ移行時間の概算見積りを，弊社の DB 技術者の協力を得て図 6 にまとめてみました。

| |
|--|
| <p>〔前提条件〕</p> <ul style="list-style-type: none"> ハードウェア暗号化モジュールの性能データから，1 データ項目当たりの暗号化及び復号の処理時間をそれぞれ 1 ミリ秒とする。 顧客 TBL のレコード 1 件当たりの順次読み込み及び順次書き込みの処理時間は，それぞれ約 0.5 ミリ秒である。 <p>〔データ移行時間の概算見積り〕</p> <p>データ移行時間</p> $= (0.5 \text{ ミリ秒/件} + 1 \text{ ミリ秒/項目} \times 7 \text{ 項目/件} + 1 \text{ ミリ秒/項目} \times 7 \text{ 項目/件} + 0.5 \text{ ミリ秒/件}) \times 100 \text{ 万件}$ $= 15,000 \text{ 秒 (4 時間 10 分)}$ |
|--|

図 6 C システムにおけるデータ移行時間の概算見積り

S 氏：⑤このデータ移行時間は長すぎますね。部分一致検索の応答時間と暗号鍵変更に伴うデータ移行時間，この二つの問題を解決する方法はありませんか。

T 氏：DB 設計を変更して，暗号化の対象となるデータ項目数を減らすことが考えられます。⑥顧客 TBL から部分一致検索に使う二つのデータ項目を抜き出して，それぞれ検索 TBL A と検索 TBL B の二つのテーブルに分けます。また，口座番号を意味のない内部 ID に変換する変換 TBL を作り，検索 TBL A，検索 TBL B 及び顧客 TBL のキー項目を内部 ID に変更します。こうすれば，暗号化の対象となるデータ項目数は一つとなり，C システムの品質要件を満たし，必要な機能を実現することができます。

S 氏：これでうまくいきそうですね。

X 社は引き続き Y 社の支援を受け，予定どおりのスケジュールで C システムの概要設計を終えることができた。

設問 1 図 2 中の ， に入れる適切な字句を，それぞれ 2 字で答えよ。

設問 2 システム構成の改善について，(1)，(2) に答えよ。

- (1) 本文中の下線②で考慮した情報セキュリティ標準の内容を，40 字以内で具体的に述べよ。
- (2) 本文中の下線①のサーバ配置はどのような効果をもたらすか。運用管理者の種類と保護する情報分類を含めて，55 字以内で述べよ。

設問 3 利用者認証とログ管理の改善について，(1)，(2) に答えよ。

- (1) 本文中の下線③の理由を，50 字以内で述べよ。
- (2) 本文中の下線④の具体的な内容について，ログ取得を実装すべき箇所と，個人を特定するために記録すべき情報を含めて，30 字以内で述べよ。

設問 4 DB 設計の改善について，(1)～(3) に答えよ。

- (1) 暗号鍵変更に伴うデータ移行処理の内容を，40 字以内で述べよ。
- (2) 本文中の下線⑤が問題となる理由を，40 字以内で具体的に述べよ。
- (3) 本文中の下線⑥について，変換 TBL，検索 TBL_A，検索 TBL_B 及び顧客 TBL に含めるべきキー項目とデータ項目を，解答欄の表に，それぞれ 4 字以内で記入せよ。

問 2 社内システムのセキュリティ対策に関する次の記述を読んで，設問 1～5 に答えよ。

A 社は，東京に本社があり，関東に工場や営業所をもつ従業員数 5,000 名の製造業者である。A 社では，数年前から社内業務の電子化を推進しており，従業員の日常業務に活用させるため，昨年までに各部署に必要な台数分のノート PC が配布されている。また，本社と，工場及び営業所（以下，これらを拠点という）に業務サーバを設置している。本社から接続されたインターネットを利用して，電子メール（以下，メールという）の送受信や，Web サーバによる情報発信を行っている。本社には情報システム部門があり，社内ネットワーク及び情報システム（以下，社内システムという）を管理している。図 1 に，A 社の社内システム構成を示す。

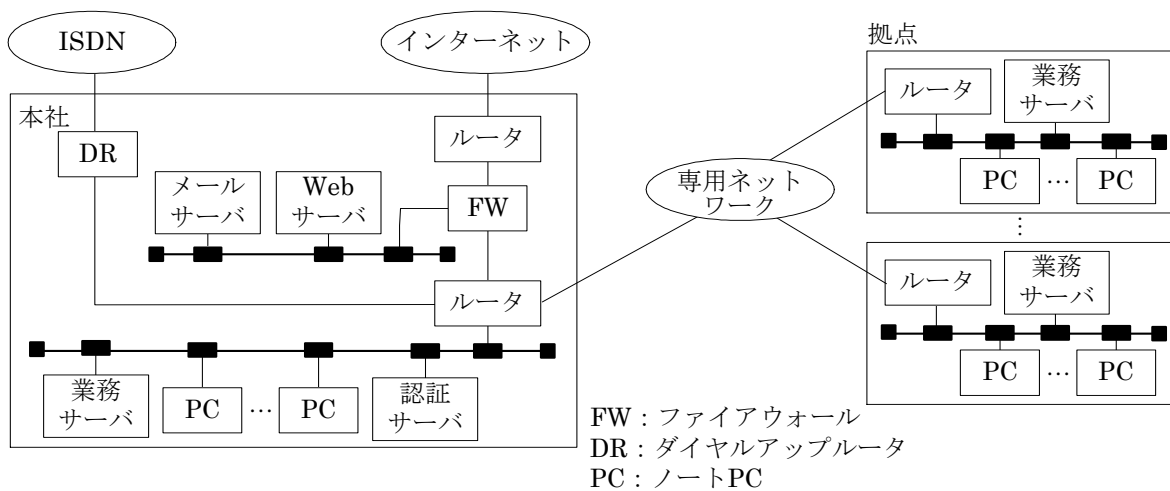


図 1 A 社の社内システム構成

外出することが多い営業部員を中心とする 50 名の従業員（以下，利用者という）は，外出先からメールサーバや各自の拠点の業務サーバを利用するために，会社から貸与されたノート PC を社外に持ち出し，PHS サービスを介してリモートアクセスを行っている。利用者は，ダイアルアップルータ（DR）を介して社内システムにアクセスする。その際，メール送受信には，SMTP と POP を使用している。また，業務サーバへのアクセスには，TCP/IP 上の独自プロトコルが使われている。A 社では，事業拡大に伴って海外にある委託業者への出張が増加していること，及びより高速な回線を用いて社外から業務サーバにアクセスしたいという要望があることの 2 点を考慮して，リモートアクセスシステムをインターネット経由に構築し直すことにした。

一方，A 社の経営陣は，情報漏えいが頻発している社会的背景を踏まえて，情報統括役員（CIO）を中心としたプロジェクトチームを組織し，社内システム全体のセキュリティ対策の見直しを行うことを指示した。コンサルタント会社によるセキュリティ診断の結果，1) リモートアクセスシステムにおける利用者認証，2) ノート PC に保存されているデータに関するセキュリティ対策，3) ウイルス感染に関するセキュリティ対策，の三つの問題点が指摘された。

そこで，情報システム部門の B 君は，プロジェクトチームの作業の一環として，指摘された三つの問題点に関する対策を含め，上司の C 氏と共同でリモートアクセスシステムの再構築を検討することになった。

〔既存のリモートアクセスシステムにおける利用者認証〕

まず，B 君は C 氏とともに，既存のリモートアクセスシステムに関して指摘された問題点の精査を行うことにした。次は，そのときの B 君と C 氏の会話である。

C 氏：既存のリモートアクセスシステムに関するセキュリティ診断の結果を確認しよう。

B 君：不正侵入の防止策として，利用者認証を実施していますが，運用面での問題点が指摘されています。

C 氏：なるほど。それでは，利用者の認証方式について，具体的に説明してくれ。

B 君：利用者を認証するために，認証サーバを設置して，DR への接続時に利用者 ID とパスワードのチェックを行います。また，PHS 端末を用いたアクセスなので，念のため DR は発信者番号に基づいた接続制限を行っています。

C 氏：利用者がノート PC や PHS 端末を紛失したときの対応はどうなっているのか，説明してくれ。

B 君：紛失した利用者から，紛失した場所と時刻，最後にリモートアクセスした時刻を電話で連絡してもらい，その利用者のアカウントの 措置を行い，DR の を見て，不審なリモートアクセスがないか確認しています。

C 氏：認証に使用するパスワードはどのように管理されているのかね。

B 君：リモートアクセスに使用するパスワードには有効期限を設け，利用者に対して，1 か月ごとに更新するように義務付けています。有効期限までにパスワードを更新しないと，アクセスできなくなるので，そのときはパスワードの初期化が必要となります。パスワードが失効した利用者や，パスワードを忘れた利用者からは，メールでパスワード初期化の依頼があります。情報システム部門でパスワードの初期化を行い，初期化によって設定された暫定パスワードをメールで返信し，直ちにパスワードを変更するようにお願いしています。

C 氏：パスワード管理について問題点が指摘されているということだったが。

B 君：はい。緊急の場合には，外出先からの電話による問合せに対し，①利用者 ID だけを聞いて暫定パスワードを教えることもあります。また，パスワードの更新に当たっては，過去に使用したことのあるパスワードと新しいパスワードを照合し，同一であれば別のパスワードを設定するように指示します。同じパスワードを再使用できないので，パスワードを覚えることが利用者にとって負担になっているようです。中には，付せん書き留めて，ノート PC に張り付けている利用者もいるようです。

C 氏：それは問題だな。リモートアクセスシステムの再構築を機に，問題解決を図ることにしよう。

〔リモートアクセス方式の変更〕

B 君と C 氏は，現在の DR 経由のリモートアクセスをインターネット経由に切り替えることにした。利用者は，公衆無線 LAN サービスや，インターネットサービスプロバイダが提供する動的 IP 割当てによるインターネットアクセスサービスを利用し，リモートアクセスシステムを介して社内システムにアクセスする。図 2 に，A 社の新しい社内システム構成案を示す。

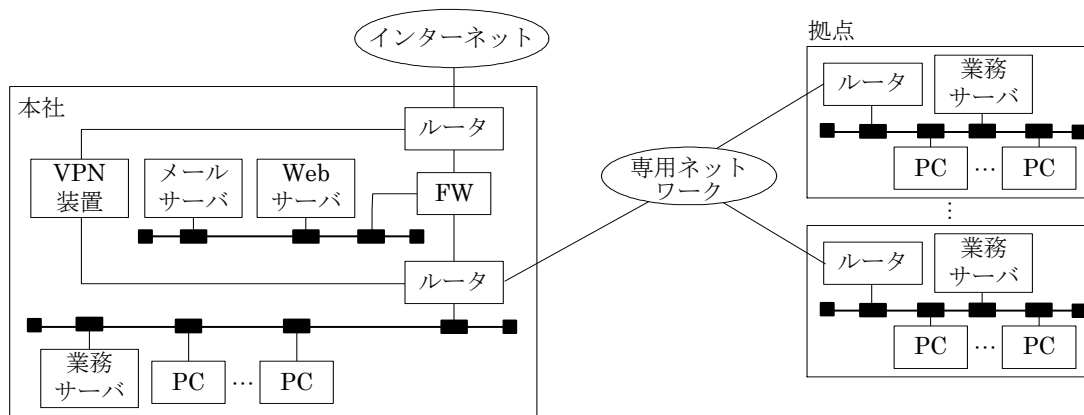


図2 A社の新しい社内システム構成案

C氏：それでは，リモートアクセス方式について検討しよう。インターネット上でVPNを構成する手段として，IPsecを用いる方法（以下，IPsec-VPNという）があるが，IPsec-VPNについて少し説明してくれないか。

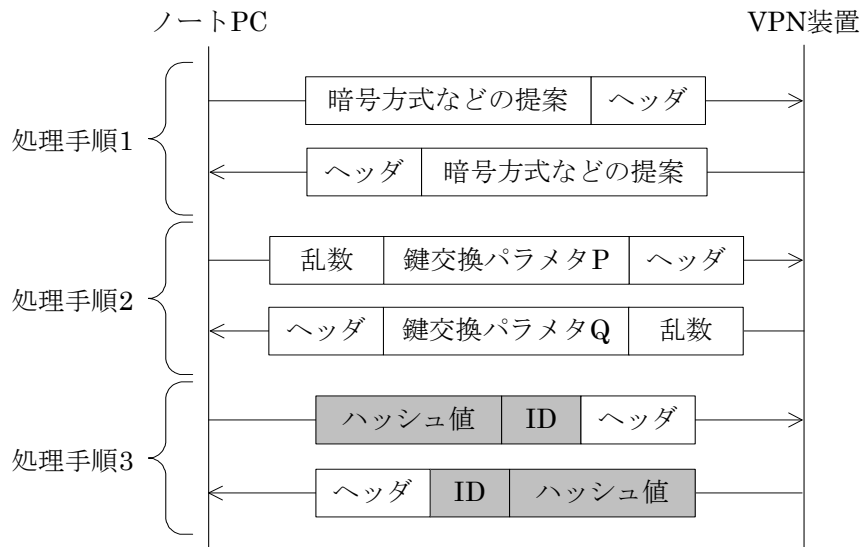
B君：はい。IPsec-VPNでは，暗号通信に先立ち，暗号方式の決定や鍵の交換，相互認証のためのプロトコルとして を使用します。 によって生成された共通鍵は， というIPパケットのフォーマット仕様に従って送受信するデータの暗号化に使用されます。

C氏：相互認証はどのような方式にするのかね。

B君：事前共有鍵を用いた方式にしようと思います。 のフェーズ1には，メインモードとアグレッシブモードがあり，リモートアクセスの利用形態に依存してどちらかを使います。メインモードでは，端末のIPアドレスをIDとし，それに事前共有鍵を割り当てます。一方，アグレッシブモードでは，利用者IDなど運用者が独自に設定したIDに対して事前共有鍵を割り当てます。

C氏：それでは，まずメインモードから説明してくれ。

B君：図3にメインモードの概要を示します。



注 ネットワーク部分は暗号化されていることを表す。

図 3 メインモードの概要

B 君：処理手順 1 では，使用する暗号方式やハッシュアルゴリズムなどが決定されます。次に，処理手順 2 では，暗号化で用いる共有鍵が生成されます。鍵交換パラメタは鍵共有アルゴリズムである e アルゴリズムに使用されます。鍵交換パラメタ P は，ノート PC がランダムに生成した一時鍵情報 p から計算された値で，鍵交換パラメタ Q は，VPN 装置がランダムに生成した一時鍵情報 q から計算された値です。鍵交換パラメタ P, Q からは，一時鍵情報 p, q は計算できません。鍵交換パラメタ Q と一時鍵情報 p を組み合わせて e アルゴリズムで計算した値は鍵交換パラメタ P と一時鍵情報 q を組み合わせて e アルゴリズムで計算した値と一致します。この値を e アルゴリズムの出力値と呼びます。この出力値を計算すると，ノート PC が保持していた一時鍵情報 p や，VPN 装置が保持していた一時鍵情報 q は，直ちに削除されます。一方，処理手順 2 で交換した乱数と事前共有鍵を利用して，マスタ鍵が生成されます。また，マスタ鍵と e アルゴリズムの出力値などを使用して，セッション鍵が計算されます。最後に，処理手順 3 では，ID とハッシュ値の交換が行われます。ハッシュ値は，鍵交換パラメタなどを入力として，マスタ鍵を鍵情報として用いた鍵付きハッシュ関数によって計算されます。ノート PC や VPN 装置はハッシュ値を受信すると，その値が正しいかどうかを検証します。

C 氏：次に，もう一方のアグレッシブモードについても説明してくれ。

B 君：はい。図 4 にアグレッシブモードの概要を示します。

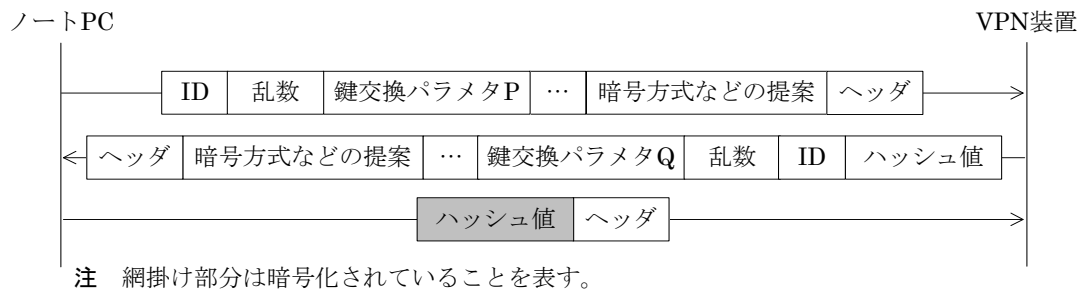


図4 アグレッシブモードの概要

B 君：認証手法，セッション鍵の生成方法はメインモードとほぼ同じです。

C 氏：使用できる ID に違いがあるようだから，リモートアクセス時のネットワーク環境も考慮して，どちらのモードを採用したらよいか検討してくれ。

B 君：はい。分かりました。

〔利用者認証方式の変更〕

C 氏：次に，利用者認証の運用面での問題点について検討しよう。現在の利用者認証方式では，パスワード管理を行うために，利用者と運用者双方に負担がかかっている。パスワードが正しく運用されればよいが，現状では困難のようだ。利用者の利便性を考慮して，**f** 認証の導入を検討してみよう。指紋や虹彩を用いた **f** 認証は，パスワードを管理する必要がないので有効な方法だと思う。一般に，その認証精度は，**g** 拒否率と **h** 受入れ率の組合せで評価される。通常は **g** 拒否率よりも **h** 受入れ率が十分に低くなるように設定されているようだ。

B 君：そうしますと，認証でのリトライ回数の上限も **g** 拒否率を考慮して設定した方がよいということですね。IPsec-VPN でのリモートアクセスに対し，**f** 認証をどのように適用すればよいでしょうか。

C 氏：指紋認証デバイス（以下，認証デバイスという）を，リモートアクセスシステムの利用者に配布して，その中に事前共有鍵を格納する方式がよいだろう。認証デバイスでは，指紋認証に成功しないと，格納されている事前共有鍵を使用できないようにできる。また，認証デバイスは，使用する PC の認証を行うので，会社が貸与したノート PC 以外からのアクセスを制限できるね。

B 君：リモートアクセスシステムは，指紋の照合に成功することと，ノート PC と認証デバイスの組合せが正しいことの 2 点を確認して認証するわけですね。それでは，認証デバイスを利用した方式について検討を進めたいと思います。

C 氏：認証デバイスの配布方法，初期登録方法，及び認証デバイスを紛失した際の運用手順についても検討してくれ。

〔ノート PC に保存されているデータに関するセキュリティ対策〕

次に，B 君と C 氏は，ノート PC に保存されているデータに関するセキュリティ対策を検討することにした。

- C 氏：リモートアクセスに使用するノート PC の管理は利用者に任せているが、どのような指導を行っているか確認しよう。
- B 君：ノート PC からの機密情報の漏えいを防止するために禁止規定を設けています。具体的には、貸与されたノート PC 以外で業務を行わない、貸与されたノート PC には決められたソフトウェアだけをインストールする、などの事項を厳守するように周知徹底しています。
- C 氏：情報漏えいの観点からは、それ以外の対策も考える必要があるね。ノート PC に保存されるデータとしては、業務で使用するファイル（以下、業務データという）とメールの 2 種類がある。そのため、ノート PC や認証デバイスが盗まれた場合の対策が必要だから、対策案を挙げてくれ。
- B 君：はい。ノート PC にはなるべくデータを保存しないようにするというのはいかがでしょうか。対策案としては、まず、メールに使用するプロトコルを IMAP に移行してもらいます。また、業務データは業務サーバの個人データ領域に保管し、使用するとき、その都度ノート PC にダウンロードし、使用後は速やかにアップロードして、ノート PC 内の業務データを直ちに削除してもらおうようにします。
- C 氏：その対策案では、メールや業務データがノート PC に残ってしまう可能性を否定できない。②ノート PC のハードディスク全体に関する対策も併せて考える必要がある。その際には、認証デバイスも活用してくれ。
- B 君：分かりました。ハードディスク全体に関する対策も含めて検討します。

[ウイルス感染に関するセキュリティ対策]

最後に、B 君と C 氏は、セキュリティ診断の結果として指摘された、ウイルス感染への対策を行うことにした。A 社では、ノート PC の管理は従業員に任せており、情報システム部門が許可しているウイルスチェックソフトの中から、従業員が選んだウイルスチェックソフトをインストールしていた。その結果、セキュリティ診断によって、ウイルスチェックソフトがインストールされていないノート PC や、ライセンス契約が切れて最新のパターンファイルに更新できなくなったウイルスチェックソフトが発見された。そこで、これまでのウイルス対策に加えて、全社的に統一されたウイルス対策を検討することになった。

幾つかの製品を調査した結果、FW にメールウイルスチェック機能を搭載することにした。この機能には、FW を通過しようとするメールをいったん代理受信し、ウイルスがなければ FW 自身が SMTP を使ってメールサーバへチェック済メールを送信するプロキシモードと、ノート PC とメールサーバ間の SMTP セッションを横取りしてウイルスチェックを行い、ウイルスがなければ送信元 IP アドレスを変更せずにそのまま転送する透過モードがある。B 君は、デフォルト設定であるプロキシモードでメールウイルスチェック機能を使用することにした。また、ウイルスメール発見時には、FW が、社内の送受信者にウイルス警告メールを送信する設定も行い、運用を開始した。

メールウイルスチェック機能導入後、しばらくたってから、A 社からのメールがあて先に届くまでに時間がかかるようになった。A 社のメールサーバは、不正メールの中継を防止するために、SMTP の送信元 IP アドレスを基に A 社のネットワークから送信されたメールだけを転送している。B 君がメールサーバを調べてみると、大量の転送待ちのメールがメールサーバに滞留していることが判明した。これらのメールは、A 社の従業員が送信したものではない不正メールであり、A 社のメールサーバが社外からのスパムメールの中継に利用されていたことが確認された。

メールサーバのログを分析したところ，メールウイルスチェック機能の設定に起因することが判明した。B君は，FWのメールウイルスチェック機能を透過モードで動作するように設定変更を行い，不正メールの転送に利用されてしまう問題を解決した。

その後，ある従業員のノートPCから大量のウイルスメールが送信されているという報告があった。B君が調査した結果，③その従業員は，図5に示すウイルス警告メールの指示どおりに対策を実施したためにウイルスに感染したことが分かった。

ウイルス警告

ファイアウォールのウイルスチェック機能が，あなたの送信メールからウイルスを検知しました。このウイルスは，メールを介して拡散する最新のウイルスで，PCのウイルスチェックソフトでは駆除できません。次の対策を実施してください。

(1)あなたのPCのウイルスを駆除するために，次のソフトウェアをダウンロードして実行してください。

<http://example.com/tool/Remove-XY9998-x86.exe>

(2)実行後に，必ずPCの再起動を行ってください。

ウイルスチェックサービス

図5 従業員あてに通知されたウイルス警告メールの本文

B君は，全従業員に，④この事例から学ぶべき注意事項について厳守するように周知徹底した。また，業務用ソフトウェアに対するセキュリティパッチや修正プログラムを保管し，従業員がそれらをダウンロードできるパッチサーバを社内ネットワークに設置した。さらに，多様化するウイルスの脅威に対抗するために，ノートPCに対しても統一したウイルス対策が必要であると判断し，すべてのノートPCに対して，同一のウイルスチェックソフトを導入することにした。

B君とC氏はその後も検討を重ね，リモートアクセスシステムの再構築と社内システム全体のセキュリティ対策を完了させることができた。

設問1 既存のリモートアクセスシステムの検証について，(1)，(2)に答えよ。

- (1)本文中の ， に入れる適切な字句を答えよ。
- (2)本文中の下線①の対応の問題点を，30字以内で述べよ。

設問2 IPsec-VPNの導入について，(1)～(4)に答えよ。

- (1)本文中の ～ に入れる適切な字句を答えよ。
- (2)図3及び図4のハッシュ値を検証する目的は何か。25字以内で述べよ。
- (3)攻撃者は，フェーズ1終了後に事前共有鍵と送受信されたすべてのデータを入手できたとしても，セッション鍵を計算できない。その理由を35字以内で述べよ。

- (4) B 君はメインモードとアグレッシブモードのどちらを採用すべきか。採用すべきモードを答えよ。また，採用理由を，ネットワーク環境に着目して 40 字以内で述べよ。

設問 3 利用者認証方式について，(1)，(2) に答えよ。

- (1) 本文中の ～ に入れる適切な字句を答えよ。
(2) 認証デバイスを紛失した際に，直ちに VPN 装置で実施すべき事項を 20 字以内で述べよ。

設問 4 ノート PC に保存されているデータに関するセキュリティ対策について，(1)，(2) に答えよ。

- (1) C 氏が指摘した以外に，ネットワーク接続環境の観点から，B 君が述べた対策案だけを実施した場合に生じるデータ可用性に関する問題点を，35 字以内で述べよ。
(2) 本文中の下線②に関して，ノート PC のハードディスクに施すべきセキュリティ対策を，認証デバイスの活用法も含めて 45 字以内で述べよ。

設問 5 ウイルス感染に関するセキュリティ対策について，(1) ～ (3) に答えよ。

- (1) メールサーバがスパムメールの中継に利用された理由を，メールサーバの設定内容に着目して 55 字以内で述べよ。
(2) 本文中の下線③について，ウイルスに感染してしまった原因を 55 字以内で述べよ。また，FW がウイルスを検知できなかった理由を 40 字以内で述べよ。
(3) 本文中の下線④について，パッチ適用に関して周知徹底すべき注意事項を，45 字以内で述べよ。