SC

平成29年度　秋期
情報処理安全確保支援士試験
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。

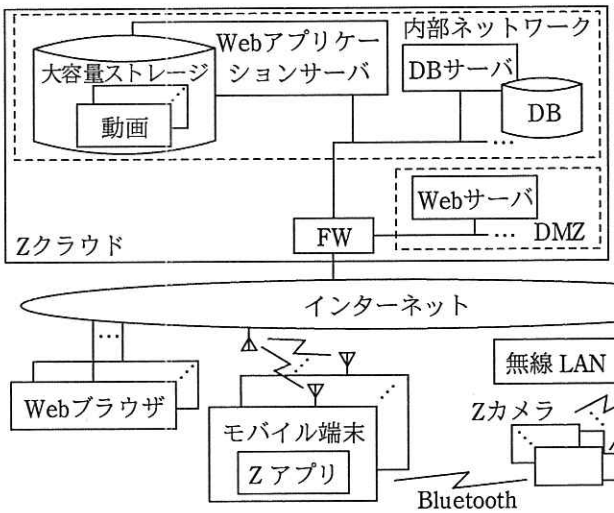
〔問2を選択した場合の例〕

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　IoT 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 1～3 に答えよ。

Z 社は，従業員数 100 名のファブレス企業であり，ネットワークカメラを使ったクラウド型ビデオ監視システム（以下，Z システムという）を開発し，個人及び小規模事業者向けに提供している。Z システムは，留守宅や事務所を監視する防犯用途での利用が多いが，最近では，外出中にペットの様子を確認するなど，用途が広がっている。Z システムの概要を図 1 に示す。



DB：データベース
FW：ファイアウォール
モバイル端末：スマートフォン又はタブレット
Zカメラ：Z社が販売しているネットワークカメラ
Zクラウド：Zカメラを利用するための様々な機能を提供するクラウドサービス
Zアプリ：Zカメラの設定やZクラウドの操作のためのモバイルアプリケーション

注記 1　DMZ から内部ネットワークへは，Web サーバから Web アプリケーションサーバへの HTTP 通信だけが，FW で許可されている。内部ネットワークから DMZ への通信は，FW で拒否されている。
注記 2　Z クラウドの管理者は，管理用端末を用いて，インターネット経由で Z クラウドを運用管理している。運用管理作業は次のルールに従い実施される。
通常時：管理用端末を用いて，Z 社内又は委託先社内で実施
緊急時：貸与された管理用モバイル端末を用いて，自宅で実施することも可
注記 3　Web サーバのコンテンツ，及び Web アプリケーションサーバのプログラムの変更は，Z クラウドの管理者だけが実施できる。これらの変更作業は全てログに記録される。

図 1　Z システムの概要

Z 社には，本社機能と，次の四つの部がある。

- 開発部：製品及びサービスの企画，要件定義及び基本設計を行う。詳細設計及び製造は外部に委託している。
- 品質保証部：委託先から納入される製品の受入テストを行い，製品の品質管理を統括している。

・ 運用統括部：Z クラウドの運用管理を統括する。運用管理は外部に委託している。
・ 営業部：営業，マーケティング，カスタマセンタにおける利用者サポートなどの業務を統括する。カスタマセンタの業務は，外部に委託している。

〔Z カメラの詳細〕

Z カメラの仕様は，次のとおりである。

・組込み OS である L-OS を使用しており，無線 LAN を使用して，インターネット経由で Z クラウドに接続される。
・全ての操作は，Z アプリから Z クラウド経由で行われる。動画撮影，動画参照を含む操作インタフェースは Z カメラ自体にはない。ただし，無線 LAN 接続の設定は，Z アプリから Bluetooth 経由で行われる。
・HDMI，USB などの物理インタフェースがなく，外部記憶媒体は接続できない。
・撮影した動画は Z クラウドに送信され，大容量ストレージに保管される。
・バッファ用の小規模ストレージがあるが，Z クラウドに送信した動画はそこから速やかに消去される。
・無線 LAN 経由では外部からの要求を待ち受けないようになっている。

〔Z クラウドの詳細〕

Z クラウドは，Z カメラ操作及び動画管理のアプリケーションを提供する SaaS 型のサービスであり，パブリッククラウド事業者 W 社の IaaS サービス上で稼働している。Z クラウドの構築と運用は，アプリケーション開発・運用サービスを提供している V 社に委託している。Z クラウドの仕様は，次のとおりである。

(1) アプリケーションプログラムの種類と呼出し

Web サーバの URL に応じて，Web アプリケーションサーバ上の異なるアプリケーションプログラムが呼び出される。アプリケーションプログラムの一覧を表 1 に示す。

表1　アプリケーションプログラムの一覧

名称	URL [1]	用途
Web IF	https://xxxx/web-if/ [2]	・Web ブラウザから，利用者情報と Z カメラを登録・変更する。
アプリ IF	https://xxxx/apl-if/ [2]	・Z アプリから，Z カメラの操作，動画参照を行う。
カメラ IF	https://xxxx/cam-if/ [2]	・Z カメラから，動画を受信する。 ・Z カメラからのリクエストに応じて，操作コマンド及び設定情報を送信し，ファームウェアを配信する。

注 [1]　アプリケーションプログラムのコンテキストルート [3]に対応する Web サーバのリクエスト URL

[2]　URL 中の xxxx は Z クラウドの Web サーバの FQDN を示す。

[3]　Web アプリケーションサーバ上で動作させる，個々のアプリケーションプログラムの最上位のパス

(2)　利用者情報の登録・変更

利用者が Z カメラを登録する際に，利用者情報の登録が済んでいないと，利用者情報の登録を求められる。利用者は，Web ブラウザを用いて Web IF にアクセスし，次の利用者情報を登録する。

・利用者情報：氏名，住所，郵便番号，電話番号，電子メールアドレス，利用者 ID 及びパスワード

登録時には自動的に 10 進数 12 桁の利用者番号が付与される。利用者番号は，Web IF の利用者登録完了画面上に表示される。また，利用者登録完了通知書に記載され，登録した住所に郵送される。

利用者情報と利用者番号は，DBMS で暗号化され，DB に格納される。ここで，パスワードは 256 ビットのハッシュ値に変換された後に暗号化されて格納される。DB へのアクセスは，DB アクセスログに記録される。

利用者は，Web ブラウザを用いて Web IF にアクセスし，利用者情報の変更を行うことができる。利用者情報が変更された場合，電子メールで利用者に通知される。

(3)　Z カメラの登録

利用者は，Web ブラウザを用いて Web IF にアクセスし，登録した利用者 ID とパスワードでログインした後，利用者 ID ごとに 10 台までの Z カメラを登録できる。登録時に入力する項目は，Z カメラのシリアル番号の英数字 16 桁と，製品パッケージに同梱されている初期設定用パスコードの英数字 24 桁である。シリアル

番号は利用者の利用者番号とともに，DBMS で暗号化され，DB に格納される。パスコードは 256 ビットのハッシュ値に変換された後に暗号化されて格納される。

譲渡や転売などの理由で，登録済みの Z カメラが他の利用者によって登録された場合，Z カメラの利用者を変更するとともに，変更されたことを元の利用者に電子メールを送って通知する。

パスコードはカスタマセンタを通じて申請することによって，再生成することができる。

(4) 動画の保管

Z クラウドの大容量ストレージには，利用者 ID ごとのフォルダが設定され，Z カメラ 1 台当たり 12 時間分の動画を無償で保管できる。さらに，有償オプションで 720 時間分に容量を拡大できる。動画は，暗号化されずに保管される。

(5) 接続・通信

・インターネットから Web サーバへの接続は，HTTP over TLS（以下，HTTPS という）だけが許可されている。

・Web サーバと Web アプリケーションサーバ間は HTTP を使って，Web アプリケーションサーバと DB サーバ間は DBMS 固有のプロトコルを使って通信する。

・Z カメラにはカメラ IF の URL が，Z アプリにはアプリ IF の URL が，それぞれ組み込まれており，Z カメラ及び Z アプリは Web サーバに HTTPS の POST メソッドを用いて通信する。

・Z カメラは，カメラ IF との通信ごとに，Z カメラのシリアル番号，初期設定用パスコードのハッシュ値，及びファームウェアのバージョン情報を送信する。

・Z クラウドから Z カメラへの各種操作コマンド及び設定情報の送信とファームウェアの配信は，Z カメラが定期的にカメラ IF にアクセスすることによって行われる。

〔Z アプリの詳細〕

Z アプリの仕様は，次のとおりである。

(1) 初回の利用者認証

Z アプリは，モバイル端末にインストールされると，自動的に UUID バージョン 4 形式の 128 ビットのデータ（以下，UUID という）を生成し，端末内に保存する。

Z アプリの初回利用時には，次のように利用者認証が行われ，Z クラウドに UUID を通知する。

・Z アプリは，Web IF で登録した利用者 ID とパスワードを利用者に入力させる。

・Z アプリは，アプリ IF に利用者 ID，パスワード及び UUID を送信する。

・アプリ IF は，利用者 ID とパスワードで認証した後，認証に成功した場合は UUID を利用者 ID に結びつけて保管する。

・同一利用者による複数端末の使用を考慮し，Z クラウドでは，利用者 ID ごとに最大 5 個の UUID が保管され，5 個を超えた場合は古い UUID から順に上書きされる。

(2) 2 回目以降の利用者認証

Z アプリの 2 回目以降の利用時には，次のように利用者認証が行われる。

・Z アプリは，アプリ IF に UUID を送信する。

・前回認証成功以降に利用者情報の変更がなかった場合，UUID を用いて認証される。

・前回認証成功以降に利用者情報の変更があった場合，又は結び付けられた利用者 ID がなかった場合は，Z アプリは再度，利用者 ID とパスワードを利用者に入力させ，アプリ IF に利用者 ID，パスワード及び UUID を送信する。アプリ IF は，利用者 ID とパスワードで認証し，認証が成功した場合，UUID を利用者 ID に結び付けて保管する。

(3) Z カメラの無線 LAN 接続の設定

Z アプリは，Bluetooth のシリアルポートプロファイルで Z カメラに接続し，Z カメラの無線 LAN 接続の設定を行う。この際，Z カメラは利用者が入力した Z カメラのシリアル番号と初期設定用パスコードを使って利用者を認証する。

(4) Z カメラの操作と撮影した動画の参照

Z アプリは，利用者認証に成功すると，カメラ操作又は動画参照のいずれかを選択する画面を表示する。

カメラ操作が選択された場合，利用者 ID に関連付けて登録されている Z カメラの一覧を表示する。利用者は操作するカメラを一覧から選択し，操作を指示する。Z アプリは，アプリ IF に要求を送信し，結果を表示する。

動画参照が選択された場合，動画の一覧を表示する。利用者は一覧から動画を

選択し，再生やダウンロードなどの操作を指示する。Z アプリは，アプリ IF に要求を送信し，結果を表示する。

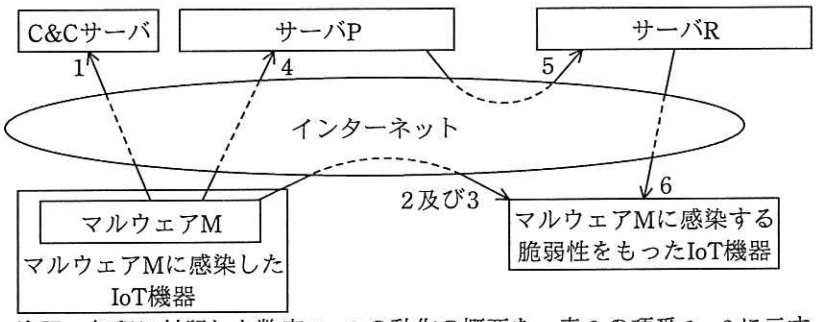
〔IoT 機器のマルウェア感染〕

ある日，Z 社のカスタマセンタに外部のセキュリティ研究者 X 氏から，Z カメラにセキュリティ上の脆弱性があり，マルウェア M に感染するリスクがあるという連絡があった。国内外の多数の IoT 機器が，マルウェア M に感染してボット化し，攻撃者に悪用されて大規模 DDoS 攻撃を引き起こしているので，Z カメラは速やかに対応する必要があるとのことであった。

これを受けて Z 社では，対策チームを編成した。品質保証部の B 主任が責任者として選任され，部下の E 君とともに対応することになった。指摘を受けた Z カメラの脆弱性について，B 主任が X 氏から得た情報は，次のとおりである。

・Z カメラの L-OS にログインできる管理者アカウントが無効化されていない。
・工場出荷時に設定された管理者アカウントのパスワードが単純であり，さらに，利用者が変更することもできない。

マルウェア M の感染の仕組みを図 2 及び表 2 に示す。



注記　矢印に付記した数字 1～6 の動作の概要を，表 2 の項番 1～6 に示す。

図 2　マルウェア M の感染の仕組み（概要）

表2　マルウェアMの感染の仕組み（動作の概要）

項番	動作の概要
1	HTTPを用いてC&Cサーバと通信し，ボットとして活動する。
2	ランダムにIPアドレスを選び，TCPポート23，2323へのTELNET接続，及びTCPポート22，6789へのSSH接続を要求する。
3	項番2でTELNET又はSSH接続に成功した場合は，様々なIoT機器で用いられたことのある，工場出荷時のログインIDとパスワードのリストを用いて，ログインを試行する。
4	項番3でログインに成功した場合，接続先IPアドレス，ポート番号，ログインID及びパスワードの情報をサーバPに送信する。
5	サーバPは，受信した情報をサーバRに送信する。
6	サーバRは，サーバPから受信した情報に基づいて対象機器にアクセスしてログインする。その後，wget又はtftpコマンドを用いてマルウェアMを対象機器にダウンロードし，実行する。
7	項番6でダウンロードされたマルウェアMは，項番1～4の動作を行う。

〔Zカメラのセキュリティ検査と対策〕

B主任は，マルウェアM又はその亜種にZカメラが感染するおそれがあるかを調べるため，図2と表2の情報を基にしたセキュリティ検査を，セキュリティ専門業者のD社に依頼した。D社によるセキュリティ検査の内容と結果の概要を表3に示す。

表3　Zカメラのセキュリティ検査の内容と結果の概要

項番	検査項目	検査内容	検査結果
1	a	1～65535のTCPポートにSYNを送信し，①応答結果からポートが開いているかどうか確認する。	TCPポート2323が開いていた。
2	プロトコル確認	開いているポートに対し，様々なプロトコルで接続を試みる。	TELNETで接続できた。
3	ログイン試行	項番2で確認したプロトコルで接続し，マルウェアMが使用するログインIDとパスワードのリストを用いて，ログインを試みる。	同一のログインIDで複数回ログインに失敗しても，アカウントロックは発生しなかった。最終的に，ログインできた。
4	ダウンロード	ログイン後に，wget，tftpコマンドを用いて，外部サーバからファイルがダウンロードできるか確認する。	wgetコマンドによって，外部サーバからファイルをダウンロードできた。
5	プロセス起動	項番4でダウンロードしたファイルが起動できるか確認する。	ダウンロードしたファイルを起動できた。
6	（省略）	項番5で起動したプロセスが，b できるか確認する。	（省略）

検査結果から，Z カメラがマルウェア M 又はその亜種に感染するおそれがあることが判明した。

表 3 の項番 1 の検査結果について，B 主任が開発部に確認したところ，委託先が開発時に使ったデバッグ用プログラムとその起動スクリプトが，出荷版のファームウェアにそのまま残されていたことが分かった。B 主任は，既に出荷済みの Z カメラがあることに配慮し，②対策を関係部署に依頼した。

さらに，Z カメラの脆弱性がほかにないか D 社に調査を依頼した。発見された脆弱性は開発部で対処した。

〔Z システムにおけるリスクの特定〕

Z 社では，Z カメラに脆弱性が複数あったことを受け，Z システムの脆弱性がほかにないことを確認することにした。Z カメラについては対処したので対象外とし，Z システムの構成に従って，次を対象とした脅威について，D 社に調査を依頼した。

・Z カメラとカメラ IF 間の通信（以下，カメラ IF 通信という）
・Z クラウド
・Web ブラウザと Web IF 間の通信
・Z アプリ
・Z アプリとアプリ IF 間の通信

〔カメラ IF 通信に対する脅威〕

カメラ IF 通信に対する脅威については，次のように調査し，対応した。

(1) 想定される攻撃と検査方法

D 社からは，カメラ IF 通信について，想定される攻撃が幾つか提示された。具体的な攻撃とその攻撃が成功するかの検査方法を表 4 に，検査システムの概要を図 3 に示す。

表4　カメラ IF 通信に対して想定される攻撃と検査方法（抜粋）

項番	想定される攻撃	検査方法
1	[c] による暗号通信の盗聴	・TLS 終端装置[1)]の付いたプロキシサーバを用いて，Z カメラと Z クラウド間の HTTPS 通信の内容を復号して確認できるか検査する。 ・TLS 終端装置が，クライアントとの TLS 接続において使用するサーバ証明書を複数準備し，サーバ証明書の違いによる動作の違いを検証する。
2	攻撃者による [d] を使った偽 Z クラウドへの誘導	・偽 Z クラウド上で稼働している偽カメラ IF に Z カメラを接続させて，Z カメラが操作できるか検査する。 ・同様に，偽カメラ IF を使用して，偽 Z クラウドが Z カメラから動画を受信できるか検査する。 ・偽 Z クラウドにおける Web サーバのサーバ証明書は，項番 1 で TLS 終端装置が使用したものを流用する。

注[1)]　クライアントと Web サーバの間に設置され，クライアントからの TLS 接続を終端し，Web サーバと新たな TLS 接続を開始することによって HTTPS 通信の内容を確認できる装置

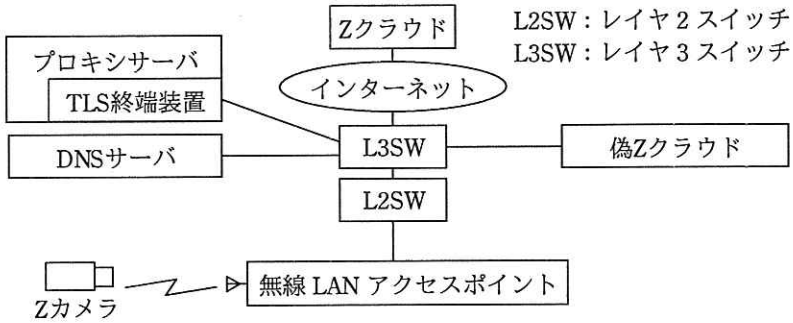


図3　検査システムの概要

D 社は，一般的な無線 LAN に対する攻撃としては，暗号化されていない又は暗号強度の弱い無線 LAN の盗聴があることを説明した。これに対し，B 主任は，カメラ IF 通信は，[e] によって暗号化されているので，通信内容を盗聴されるおそれがないことを説明した。

(2)　検査システムとサーバ証明書

検査では，次の二つのサーバ証明書をプライベート認証局で発行し，TLS 終端装置で一つずつ使用した。

証明書 1：サブジェクトのコモンネーム（以下，CN という）が Z クラウドの FQDN である証明書

証明書 2：CN が，Z クラウドの FQDN と異なる証明書

なお，検査に当たっては，③プライベート認証局のルート証明書を，テスト対象のZカメラに，信頼されたルート証明機関のものとして登録していない。

(3) 検査結果と対応

・表4の項番1の検査結果：証明書1を使用した場合は通信でき，さらに通信内容を復号して確認することができた。しかし，証明書2を使用した場合は通信できなかった。

・表4の項番2の検査結果：証明書1を使用した場合は，偽Zクラウド環境に接続させて，Zカメラの操作と動画の受信ができた。しかし，証明書2を使用した場合は，偽Zクラウド環境に接続させられなかった。

D社は，検査結果を受けて，表4の項番1，2の攻撃についてZカメラにおける問題点と対策案をまとめ，B主任に報告した。B主任はこの報告を基に，対策を関係部署に依頼した。

〔Zクラウドに対する脅威〕

Zクラウドに対する脅威と対策状況について，D社から表5が提示された。

表5 Zクラウドに対する脅威と対策状況

整理番号	想定される脅威	対策状況
A1	利用者アカウントのなりすまし	Web IF・アプリ IFにおける不正ログイン対策が不足している。
A2	管理者アカウントのなりすまし	④第三者による不正アクセスを防止するため，利用者認証に加えて，アクセス元の端末を制限しており，十分な対策が取られている。
B1	DDoS攻撃	V社がDDoS対策ソリューションを導入しており，十分な対策が取られている。
C1	Webアプリケーションサーバ上のアプリケーションプログラムの脆弱性を突いた攻撃	Webアプリケーションサーバ上のアプリケーションプログラムの脆弱性を突いた攻撃のリスクを軽減するための対策が取られていない。
C2	OSやミドルウェアなどのシステム基盤の脆弱性を突いた攻撃	未確認であり，V社の脆弱性管理の状況を確認する必要がある。
D1	業務委託先を含めた従業員・役員（以下，内部者という）による犯行	（省略）
D2	内部者の過失	（省略）

次は，表5についての，B主任とE君の会話である。

B主任：Zクラウドにおけるリスクと，表5の想定される脅威の関係を教えてください。

E君　：動画の漏えいの原因としては，表5の整理番号A1，A2，C1，C2，D1，D2の脅威が考えられます。また，Zクラウドの Web サーバ上にあるコンテンツの予期せぬ変更の原因としては，表5の整理番号［　f　］の脅威が考えられます。

次は，表5の整理番号A1についてのB主任とE君の会話である。

B主任：まず，対策状況を確認したいので，Web IF及びアプリ IFの利用者IDとパスワードを用いた認証に関する不正ログイン対策について説明してください。

E君　：どちらも，認証に失敗するごとに，その利用者IDでログインできない期間を5秒間から最大24時間まで指数関数的に長くしていき，成功すると元に戻す仕組み（以下，ログイン制限という）によって不正ログインを防いでいます。

B主任：最近は，ほかの Web サイトから漏えいした利用者 ID とパスワードのリストを悪用した，いわゆるリスト型攻撃が増えているそうです。ブルートフォース攻撃ならログイン制限で防げる可能性が高いですが，⑤リバースブルートフォース攻撃やリスト型攻撃は，ログイン制限では防ぐのが難しいというのがD社の見解です。

E君　：なるほど。それでは，利用者 ID とパスワードに加えて，ほかの利用者情報，例えば電話番号や電子メールアドレスも使って認証するように変更すれば，防げるのではないでしょうか。

B主任：その方法は，リバースブルートフォース攻撃には効果がありますが，⑥リスト型攻撃については，防げない場合があります。

E君　：確かにそうですね。では，利用者 ID とパスワードに加えて，⑦Zクラウドと各利用者だけが知っていて，利用者以外が入手するのが困難な情報で追

加認証すれば，安全性を高められます。

B主任：そうですね。しかし，利用者にとっては，ログインするたびに追加認証を求められるのは面倒ですから，必要な場合だけに限定しましょう。平常時は，利用者はZアプリを使ってZクラウドにログインします。利用者IDとパスワードによる認証が必要となるのはごく限られた状況だけなので，平均すると利用者1人当たり，年1回程度です。

E君　：分かりました。リバースブルートフォース攻撃やリスト型攻撃を念頭に置いて，⑧平常時と異なる状況が発生していると判断される場合において，追加認証する方法を考えてみます。

表5の整理番号C1については，開発委託先との契約に⑨必要な条項を追加することにした上で，納品時にWebアプリケーションプログラムの脆弱性検査を実施することが決まった。

表5の整理番号C2について，運用統括部に確認した結果は，次のとおりである。

・OS，ミドルウェアなど，Zクラウドのシステム基盤については，V社が毎年，年度末にセキュリティ専門業者の脆弱性検査を受けている。
・脆弱性検査の結果，重大な問題が指摘された場合，V社は，定期メンテナンス時に，脆弱性修正プログラムを適用するか，又は回避策を実装している。

D社からは，脆弱性を突いた攻撃が頻繁に発生する昨今の状況を踏まえると，⑩構成管理を導入した脆弱性対応の仕組みを構築する必要があるとの指摘を受けた。B主任は，運用統括部に，構成管理と脆弱性対応の仕組みを見直すよう依頼した。

次は，表5の整理番号D1，D2についてのE君とB主任の会話である。

E君　：利用者は，自分のZカメラで撮影した動画が，他者に見られることを心配しています。利用者の立場からすると，内部者に見られることにも不安を感じるので，故意か過失かにかかわらず，内部者にも見ることができないような仕組みが必要です。

B 主任：⑪動画も暗号化すべきですね。早急に検討を進めてください。

Z 社は，D 社の協力の下，ほかの脅威についても検討し，対策を立案した。開発部は，これらの対策を取り入れた次期バージョンの開発に着手した。

設問 1　〔Z カメラのセキュリティ検査と対策〕について，(1)～(4)に答えよ。

(1) 表 3 中の［ a ］に入れる検査項目の名称を答えよ。

(2) 表 3 中の下線①について，ポートが開いている場合と閉じている場合に期待される応答結果を，それぞれ解答群の中から全て選び，記号で答えよ。

解答群

ア　ACK 受信　　イ　FIN ACK 受信　　ウ　FIN 受信
エ　RST ACK 受信　　オ　RST 受信　　カ　SYN ACK 受信
キ　SYN 受信　　ク　応答なし

(3) 表 3 中の［ b ］に入れるプロセスの動作を，30 字以内で具体的に述べよ。

(4) 本文中の下線②について，出荷済みの Z カメラに対する対策を，60 字以内で具体的に述べよ。

設問 2　〔カメラ IF 通信に対する脅威〕について，(1)～(3)に答えよ。

(1) 表 4 中の［ c ］，［ d ］に入れる攻撃手法を解答群の中から選び，記号で答えよ。

解答群

ア　DNS キャッシュポイズニング攻撃　　イ　サービス不能攻撃
ウ　サイドチャネル攻撃　　エ　辞書攻撃
オ　セッション固定攻撃　　カ　中間者攻撃
キ　水飲み場型攻撃　　ク　リフレクション攻撃

(2) 本文中の［ e ］に入れる適切な字句を英字で答えよ。

(3) 本文中の下線③について，プライベート認証局のルート証明書を信頼されたルート証明機関のものとして登録してはいけない理由を，30 字以内で述べよ。

設問３　〔Z クラウドに対する脅威〕について，(1)～(10)に答えよ。

(1) 表 5 中の下線④について，アクセス元の端末を制限する方法として Z システムに適した方法を，25 字以内で具体的に述べよ。

(2) 本文中の［　f　］に該当する全ての脅威を，表 5 中の整理番号で答えよ。

(3) リバースブルートフォース攻撃の攻撃手法を，40 字以内で述べよ。

(4) 本文中の下線⑤について，ログイン制限では防ぐのが難しい理由を，40 字以内で述べよ。

(5) 本文中の下線⑥について，防げないのはどのような場合か。50 字以内で具体的に述べよ。

(6) 本文中の下線⑦について，Z カメラが譲渡や転売される可能性を考慮に入れて，追加認証する適切な方法を，25 字以内で述べよ。

(7) 本文中の下線⑧について，Z クラウドにおけるログイン認証の状況を踏まえて，平常時と異なる状況だと判断されるのはどのような場合か。40 字以内で述べよ。

(8) 本文中の下線⑨について，委託契約に盛り込むべき条項を，25 字以内で具体的に述べよ。

(9) 本文中の下線⑩について，構成管理を導入していない場合の問題点を，40 字以内で述べよ。

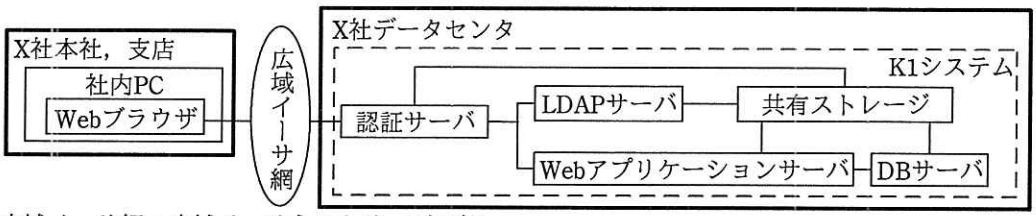
(10) 本文中の下線⑪について，表 5 の整理番号 D1，D2 への対策として，共通鍵暗号方式による暗号化を検討する。内部者のうち，特に Z クラウドの管理者に見られないことを重視した場合，共通鍵の生成，動画の暗号化及び復号を行う Z システムの構成要素を，それぞれ図 1 中から選んで答えよ。また，その場合の共通鍵の安全な共有方法を，25 字以内で述べよ。

問2　データ暗号化の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10,000名の生命保険会社である。X社では，業務担当者が契約の情報を管理するシステム（以下，K1システムという）を，15年前から運用している。K1システムは，X社データセンタに設置されており，次の4種類のサーバ及び共有ストレージで構成されている。

・データベース（以下，DBという）サーバ：被保険者の氏名，生年月日，住所，電話番号，医療情報・健康情報など（以下，被保険者情報という）及び契約条件（以下，被保険者情報と契約条件を併せて契約情報という）を保管
・Webアプリケーションサーバ：契約情報を管理する業務アプリケーションが稼働
・LDAPサーバ：利用者IDとパスワードを保管
・認証サーバ：リバースプロキシとして運用

K1システムの論理構成を図1に示す。



広域イーサ網：広域イーサネットサービス網

図1　K1システムの論理構成

〔K1システムの現在の運用〕

現在，K1システムは，次のように運用されている。

(1)　災害対策

・バックアップセンタには，K1システムと同じ論理構成のバックアップシステムが用意されており，通常時は開発環境・テスト環境として利用されている。

(2)　本番環境における作業担当

・定型運用作業（K1システムの起動及び停止，DB及びファイルのバックアップなど）：オペレータが担当

・DBMS と Web アプリケーションサーバソフトウェアとを除いたミドルウェア及び OS の設定変更作業・非定型運用作業：システム管理者が担当

・DBMS，Web アプリケーションサーバソフトウェア及び業務アプリケーションの設定変更作業・非定型運用作業：業務アプリケーション管理者が担当

(3) オペレータ及び管理者に付与される権限

・オペレータとシステム管理者には，DBMS と Web アプリケーションサーバソフトウェアとを除くミドルウェア及び OS 上の全ての操作権限が付与されており，その他の権限は付与されていない。

・業務アプリケーション管理者には，DBMS，Web アプリケーションサーバソフトウェア，業務アプリケーション，及び業務アプリケーションのログに関する全ての操作権限が付与されており，その他の権限は付与されていない。

(4) リスク対策

X 社では，契約情報の漏えい防止に最優先で取り組んでいる。そのため，K1 システムでは，次のような対策を行っている。

・社内 PC 上の Web ブラウザと Web アプリケーションサーバ間の通信は，TLS プロトコルによる暗号化通信である。

・Web アプリケーションサーバ上の業務アプリケーションと DB サーバ間は，Java プログラムから DB に接続するための API である JDBC の暗号化通信を利用している。

・契約情報は，業務アプリケーションが，共通鍵暗号方式で暗号化し，DB サーバに保管している。

・業務処理を行う際，業務アプリケーションは，DB サーバから契約情報を読み出して復号する。

〔K1 システムにおける課題〕

現在，X 社は，K1 システムの更改を計画している。更改後のシステム（以下，K2 システムという）では，契約者が PC の Web ブラウザ及びスマートフォンのアプリからインターネットを介して K2 システムにアクセスし，契約情報の参照，被保険者情報の更新などを行えるようにする。また，K2 システムにおいても，K1 システムにおける運用を引き継ぎ，契約情報の漏えい防止を最優先とした。

X 社は，K2 システムの要件定義において，システム開発ベンダ Y 社の支援を受けることにした。Y 社が K1 システムの仕様を確認したところ，DB サーバに保管する契約情報の暗号化及び復号の仕組みに問題があることが判明した。Y 社は，X 社に対して次の指摘を行った。

指摘 1　契約情報の暗号化に鍵長 56 ビットの DES アルゴリズム（以下，56bitDES という）が使われている。鍵長 256 ビットの AES アルゴリズムに変更すべきである。

指摘 2　契約情報の暗号化及び復号に用いる鍵が平文でファイルに保管されており，オペレータ及びシステム管理者に当該ファイルのアクセス権が付与されている状況である。安全な鍵管理の仕組みに変更すべきである。

指摘 1 に関して，Y 社から次の根拠が示された。

［ a ］の安全対策基準（日本国内において金融機関などがよりどころとすべき共通の安全対策基準）では，［ b ］暗号リスト（電子政府における調達のために参照すべき暗号のリスト）などに記載されている暗号技術を採用するのが望ましいとしているが，当該暗号リストにおいて，56bitDES は推奨されていない。また，次の前提条件に基づいて試算した結果から，今日では，56bitDES の解読に必要な PC の台数は，攻撃者が現実的に調達可能な台数である。

・1998 年に開催された第 2 回 DES 解読コンテストにおいて，4 万台の PC で 56bitDES の全鍵空間の 80％を探索し，40 日で解読した。
・解読所要時間はプロセッサの MIPS 値に反比例する。
・1998 年のコンテストで使われた PC に搭載されたプロセッサの MIPS 値を，540 MIPS と仮定する。
・2017 年製の PC に搭載されたプロセッサの MIPS 値を，133,920 MIPS と仮定する。
・40 日間で鍵空間の 80％を探索するために必要な，2017 年製の PC の台数を試算する。

〔暗号方式の検討〕

X 社には，危たい化した暗号技術を使っているシステムが K1 システム以外にも複数あった。そこで，Y 社からの指摘を踏まえ，X 社は，暗号技術を含む暗号方式の社

内標準について検討した。その結果，契約情報を業務アプリケーションではなくDBMSで暗号化してDBに保管する方式（以下，DB暗号方式という）を社内標準として，X社の全システムに適用することにした。DB暗号方式の設計に当たって，X社は次のシステム標準と要件を定義した。

システム標準1　業務アプリケーションはJavaで開発する。

システム標準2　DBMSには，暗号化機能及びDBレプリケーション機能がある製品Dを採用する。

要件1　製品DのDBに保管される情報を暗号化及び復号する機能（以下，表領域暗号化機能という）を用いて，DBに保管される契約情報を暗号化する。

要件2　契約情報の暗号化及び復号に用いる鍵を，暗号モジュールを用いて保護する。

暗号モジュールとは，暗号化，復号，乱数生成，鍵管理などの機能を提供するハードウェア又はソフトウェアのことである。NISTが定めた［　c　］140-2は，暗号モジュールに求められるセキュリティ要件を定義したものである。

X社は，暗号モジュールに，Q社の製品Hを採用した。また，X社は，複数のサーバからネットワーク経由で1台の製品Hの機能を利用するために，Q社が提供しているソフトウェア製品であるHクライアントとHサーバも採用した。

製品Hは，［　c　］140-2 Level 4の要件を満たすハードウェアの暗号モジュールであり，サーバに取り付けられるPCI Expressカードである。製品Hは，製品Hを取り付けたサーバ（以下，HSMサーバという）上で稼働するプログラム（以下，ローカルプログラムという）に対して独自のAPI（以下，API-Xという）を提供し，ローカルプログラムからAPI-Xを呼び出すことで，暗号化，復号，乱数生成，データの暗号化及び復号に使用する鍵（以下，データ鍵という）の生成，データ鍵の保管，並びに保管したデータ鍵の削除を行う。また，製品Hは，製品H，及び製品Hに保管するマスタ鍵を管理するプログラム（以下，ユーティリティプログラムという）を導入した専用の管理端末に対して，製品H自身に対する管理インタフェースを提供する。

K2システムにおける契約情報の暗号化機能の概要を図2に示す。図2において，Hサーバはローカルプログラムに該当する。

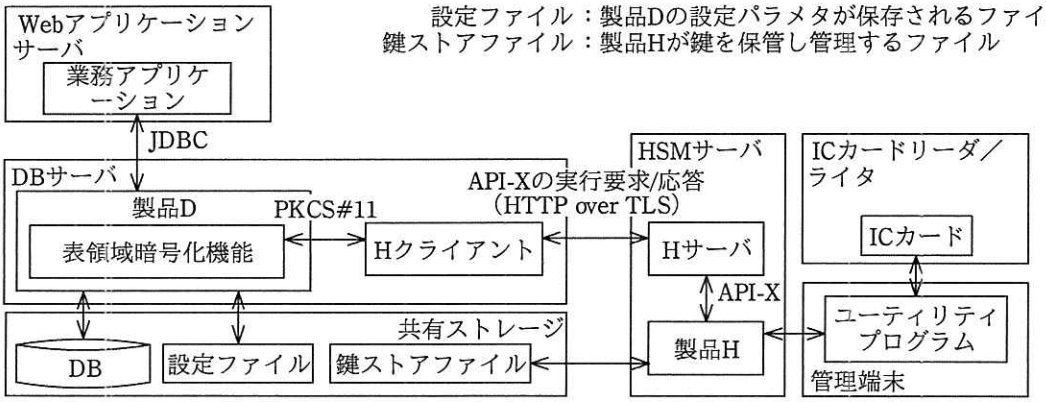


図 2　K2 システムにおける契約情報の暗号化機能の概要

製品 H の仕様は次のとおりである。

仕様 1　初期化

管理端末上でユーティリティプログラムを起動し，製品 H 経由で鍵ストアファイルを作成した後，マスタ鍵を生成し，製品 H を利用可能な状態にする。

・マスタ鍵は，3 人の鍵管理者が別々に管理端末から入力した 256 ビットの値（以下，部分鍵という）の排他的論理和によって生成され，製品 H のメモリ内に保持される。製品 H のメモリは，製品 H の内蔵バッテリによって駆動する。

・部分鍵は，管理端末に接続された IC カードリーダ／ライタを用いて，別々の IC カードに保管することができる。その際，鍵管理者は 6 桁の PIN を入力し，かつ，部分鍵を記録した IC カードを別々に保管する必要がある。

・IC カードから部分鍵を読み出す際は，PIN の入力が必要になる。

仕様 2　乱数の生成

ローカルプログラムから乱数を生成する API-X を呼び出すと，製品 H が乱数を生成し，API-X の出力値として返す。

仕様 3　鍵の生成

・ローカルプログラムが，データ鍵の識別子（以下，データ鍵 ID という）をパラメタに設定して，データ鍵生成の API-X を呼び出すと，製品 H がデータ鍵を生成する。

・生成されたデータ鍵は，製品 H においてマスタ鍵で暗号化され，データ鍵 ID とともに鍵ストアファイルに保管される。

・既に鍵ストアファイルに存在しているデータ鍵 ID を指定してデータ鍵を生成し

ようとすると，API-X の処理結果はエラーとなる。

仕様 4　暗号化又は復号

・ローカルプログラムが，データ鍵 ID，及び，暗号化又は復号を行うデータを，パラメタに設定して，暗号化又は復号の API-X を呼び出す。

・製品 H は，鍵ストアファイルから暗号化されたデータ鍵を読み出してマスタ鍵で復号し，復号されたデータ鍵でデータの暗号化又は復号を行った後，暗号化又は復号されたデータを，API-X の出力値として返す。データの暗号化又は復号は製品 H 内で行われ，復号されたデータ鍵は，製品 H 内だけに存在する。

・鍵ストアファイルに存在しないデータ鍵 ID を指定して暗号化又は復号を行おうとすると，API-X の処理結果はエラーとなる。

仕様 5　マスタ鍵のゼロ化

製品 H には，内蔵バッテリで駆動するセンサが内蔵されている。①センサが次のいずれかを検知すると，製品 H は，メモリ上に保持されているマスタ鍵をゼロ化するとともに，自身を使用不能で，かつ，元に戻せない状態にする。

(a)　電気的短絡（ショート）の発生などによる規定の範囲を超える電源電圧の発生

(b)　製品 H のカバーのこじ開け又は損傷

内蔵バッテリが切れそうな場合，製品 H は HSM サーバを介して警告メッセージを出力し，早期のバッテリ交換を促す。内蔵バッテリの交換手順として，(a)の発生を回避する手順が提供されている。

H クライアントと H サーバを用いると，HSM サーバとは別のサーバで稼働するプログラム（以下，リモートプログラムという）からネットワークを介して製品 H を利用できる。H クライアントは，リモートプログラムが稼働するサーバに導入され，リモートプログラムに対して PKCS#11 の API を提供する。H サーバは HSM サーバに導入され，TLS 通信を介して H クライアントに製品 H の機能を提供する。

H クライアントと H サーバの仕様は次のとおりである。

(1)　API-X の実行要求

・リモートプログラムが H クライアントを呼び出すと，H クライアントは，受け取った PKCS#11 の API 呼出しを API-X の実行要求に変換して，H サーバに送

信する。

・API-X の実行要求を受信した H サーバは，API-X を呼び出し，その実行結果を応答として H クライアントに返す。ただし，鍵生成の場合，H クライアントは，内部でデータ鍵 ID を 0 から順番に採番して H サーバに API-X の実行要求を送信し，鍵生成が成功した場合にデータ鍵 ID を API-X の出力値としてリモートプログラムに返す。鍵生成が失敗した場合，H クライアントはリモートプログラムにエラーを返す。

(2) H サーバに対する負荷分散

H クライアントは，複数の H サーバに API-X の実行要求を振り分ける負荷分散機能をもっている。負荷分散機能の概要は次のとおりである。

・H クライアントに，複数の H サーバの IP アドレス又はホスト名を登録する。

・H クライアントは，登録された H サーバのうち稼働している H サーバに，ラウンドロビン方式で API-X の実行要求を送信する。

製品 D の表領域暗号化機能には，PKCS#11 の API を提供する暗号モジュールが必要である。製品 D の表領域暗号化機能の仕様は次のとおりである。

仕様 A　DB を作成する際，表領域暗号化の設定が有効になっていると，製品 D は PKCS#11 の API を用いて DB マスタ鍵を生成する。この際，DB マスタ鍵及び DB マスタ鍵の識別子（以下，DB マスタ鍵 ID という）が暗号モジュール内に保存され，DB マスタ鍵 ID が API の出力として製品 D に返される。製品 D は，DB マスタ鍵 ID を設定ファイルに保存し，同時にメモリ上に保持する。

仕様 B　表領域を作成する際，表領域暗号化の設定が有効になっていると，製品 D は PKCS#11 の API を用いて乱数を生成する。生成された乱数は，データの暗号化鍵・復号鍵（以下，DB データ鍵という）として，製品 D のメモリ上に保持される。同時に，製品 D は PKCS#11 の API を用いて DB データ鍵を DB マスタ鍵で暗号化する。暗号化された DB データ鍵は，表領域の一部としてディスクに書き込まれる。

仕様 C　データをディスクに書き込む際，製品 D は，保持している DB データ鍵でデータを暗号化した後，ディスクに書き込む。

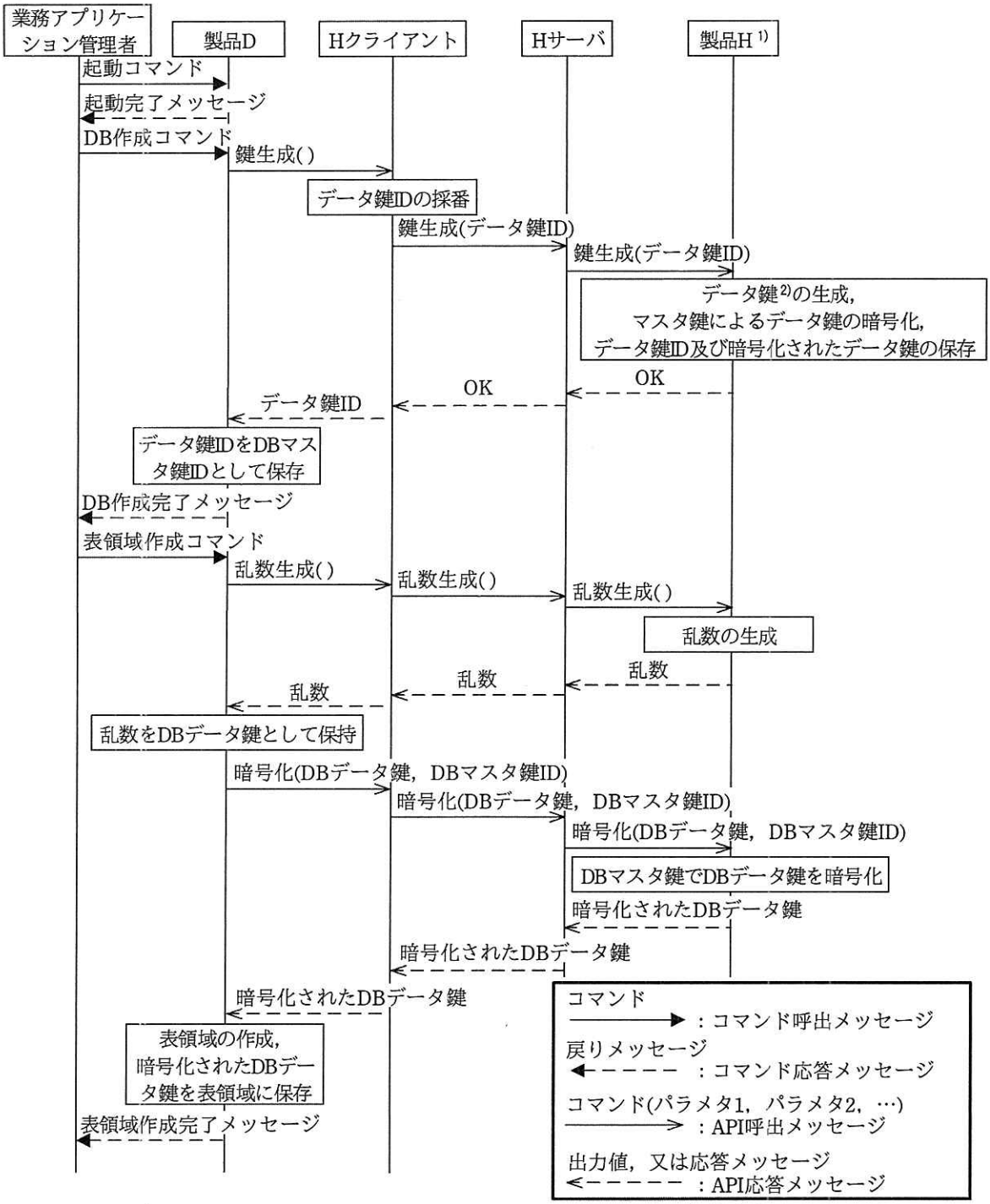
仕様 D　ディスクからデータを読み込む際，製品 D は，まず，ディスク上からデー

タを読み込んだ後，読み込まれた暗号化データを，保持している DB データ鍵で復号する。

仕様 E　製品 D は，停止する際，メモリ上に保持している DB データ鍵をゼロ化する。

K2 システムの DB 暗号方式では，製品 D の表領域暗号化機能に必要な暗号モジュールとして製品 H が用いられる。また，製品 D の表領域暗号化機能の仕様における DB マスタ鍵及び DB マスタ鍵 ID が，それぞれ，製品 H の仕様におけるデータ鍵及びデータ鍵 ID に該当する。

K2 システムの DB 暗号方式における DB の初期化処理の概要を，図 3 に示す。図 3 中では，製品 D の表領域暗号化機能の仕様のうち，仕様 A と仕様 B を記載している。



注記 1　製品 D と H クライアント間のコマンドは，PKCS#11 の API を意味する。
注記 2　H クライアントと H サーバ間のコマンドは，API-X の実行要求を意味する。
注記 3　H サーバと製品 H 間のコマンドは，API-X を意味する。
注 1)　製品 H の初期化は既に行われている。
2)　製品 H によって生成されたデータ鍵は，DB マスタ鍵として扱われる。

図 3　K2 システムの DB 暗号方式における DB の初期化処理の概要

〔DB サーバ及び HSM サーバの構成設計〕

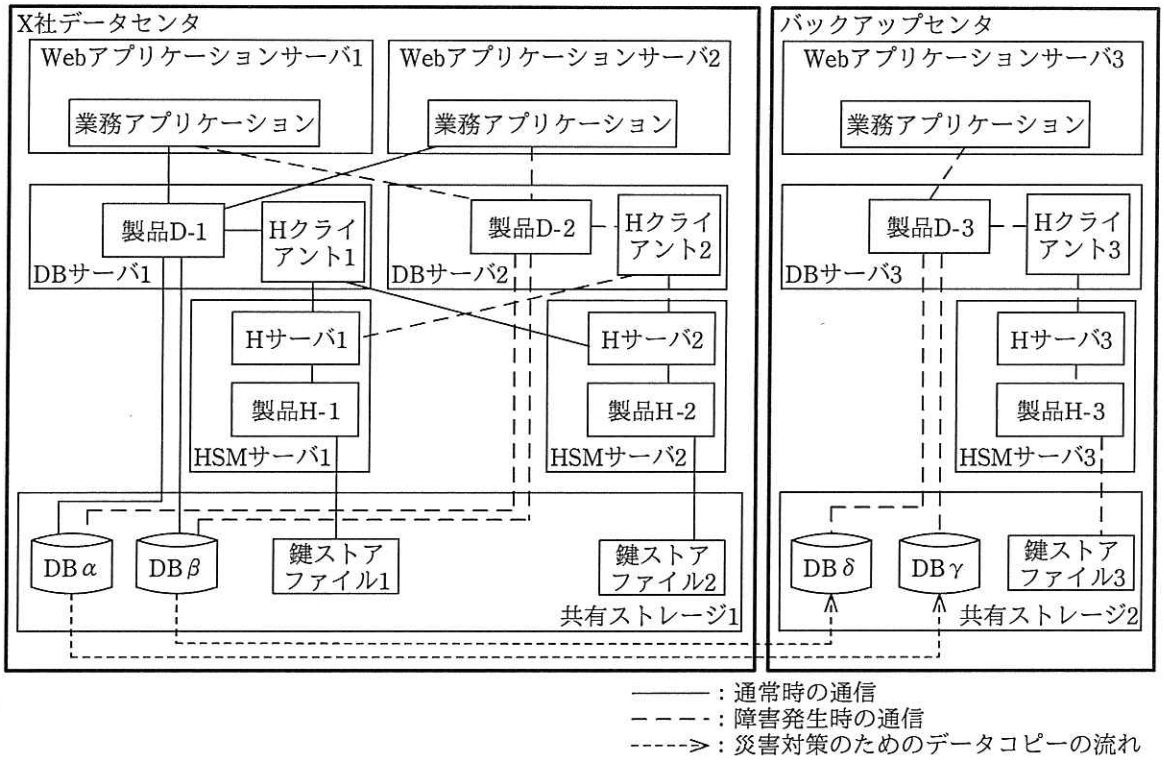
X 社は，K2 システムのサーバ構成について，Y 社に次の要件で設計を依頼した。

・DB サーバをアクティブ・スタンバイの 2 台構成にする。

・災害対策として，製品 D の DB レプリケーション機能を用いて，X 社データセンタの DB からバックアップセンタの DB に，定期的にデータをコピーする。

・HSM サーバは，K2 システム以外のシステムの DB サーバを含めた全 DB サーバからも共有できるようにする。

Y 社が設計した K2 システムのサーバ構成を図 4 に示す。



注記 1　製品 D-2 は，製品 D-1 に対するスタンバイ構成である。

注記 2　DBα及び DBγには被保険者情報が保管され，DBβ及び DBδには契約条件が保管される。

図 4　K2 システムのサーバ構成（抜粋）

Y社は，K2システムにおけるDB及び表領域の作成手順を次のように設計した。

(i) HSMサーバ1だけを稼働させ，他のHSMサーバは停止させておく。

(ii) DBサーバ1だけを稼働させ，他のDBサーバは停止させておく。

(iii) 製品D-1上で，DBαを作成する。

(iv) 製品D-1上で，DBβを作成する。

(v) 製品D-1上で，DBαに対応する表領域1を作成する。

(vi) 製品D-1上で，DBβに対応する表領域2を作成する。

(vii) 全てのHSMサーバ及び全てのDBサーバを停止させる。

(viii)鍵ストアファイル1を，鍵ストアファイル2及び鍵ストアファイル3にコピーする。

（以下，省略）

Y社は，DB暗号方式において，Hクライアント及びHサーバの仕様では複数システムのDBサーバから1台のHSMサーバを共有することはできないとX社に伝えた。そこで，X社が開発元のQ社に問い合わせたところ，Q社からは，来月リリースされる新しいバージョンのHクライアント及びHサーバに次の機能を追加するという回答を得た。

・Hクライアントを一意に識別する識別子（以下，Hクライアント IDという）を設定し，Hサーバに鍵生成を要求する際に従来のデータ鍵IDにHクライアントIDを付け加えて送信する。

・Hサーバは，Hクライアントから送信された鍵生成要求を処理する際，Hクライアント IDと従来のデータ鍵IDを結合した，新たなデータ鍵IDをパラメタとして，鍵生成のAPI-Xを呼び出す。Hクライアントは，新たなデータ鍵IDをDBマスタ鍵として製品Dに返す。

複数の業務システムのDBサーバが1台のHSMサーバを共有する場合の構成を，図5に示す。

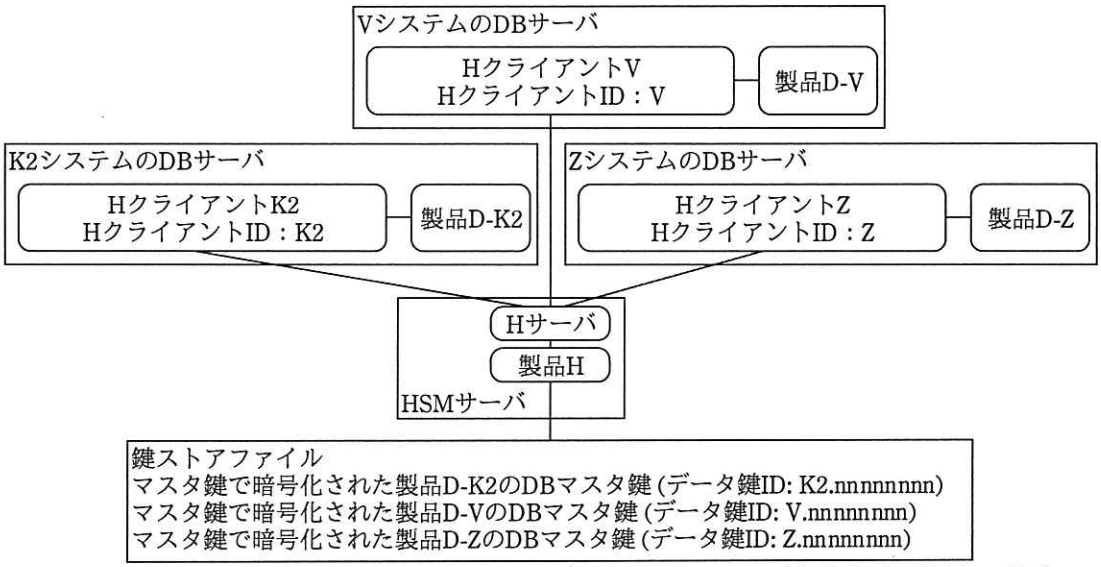


図 5　複数の業務システムの DB サーバが 1 台の HSM サーバを共有する場合の構成

〔K2 システムにおけるリスク対策の補完〕

X 社は，DB 暗号方式を実装した K2 システムについて，契約情報の漏えいリスクを分析した。リスク分析の結果，次の対策を追加することになった。

対策 1　不審なアクセスがないか監視する。具体的には，週次で，業務アプリケーションのログから，業務時間外のアクセス及び大量の契約情報へのアクセスがないかチェックし，もしあれば，その内容を確認する。

対策 2　DB サーバ又は Web アプリケーションサーバのメモリダンプをファイルに出力した場合，次の作業に対して，作業者，作業日時及び作業内容を履歴として残す。

・メモリダンプのファイルへの出力
・メモリダンプファイルへのアクセス
・メモリダンプファイルを保管した外部記憶媒体の利用
・メモリダンプファイルの消去

K2 システムの設計を終えた X 社は，更改作業に向けて準備を開始した。

設問1　〔K1システムにおける課題〕について，(1)～(3)に答えよ。

(1) 本文中の［ a ］，［ b ］に入れる適切な字句を，［ a ］は英字4字で，［ b ］は英字8字で，それぞれ答えよ。

(2) Y社が提示した前提条件に基づいて試算した場合，2017年製のPCを利用したとして，同じ時間内に56bitDESを解読するには，PCは最低何台必要か。答えは，小数第1位を切り上げて整数で求めよ。ここで，133,920=540×248である。

(3) 指摘2の状況によって，誰が，どのような方法で契約情報を取得するリスクが発生するか。60字以内で述べよ。

設問2　〔暗号方式の検討〕について，(1)～(5)に答えよ。

(1) 本文中の［ c ］に入れる適切な英字4字を答えよ。

(2) 製品Hの仕様1の効果を，1人の鍵管理者が三つの部分鍵を入力し，3枚のICカードに保管して管理する場合と比べて，25字以内で述べよ。

(3) ICカードに記録される部分鍵は，何を実施した場合にどのような目的のために必要か。場合と目的をそれぞれ15字以内で述べよ。

(4) 本文中の下線①によって実現される暗号モジュールの性質を，7字以内で答えよ。

(5) X社の運用規程で，製品Hを運搬する場合，必ず静電気防止シートで覆うように定めた。これは，静電気防止シートで覆わなかった場合に発生し得る不都合な事象を想定し，配慮したものである。その事象及びその事象によって実行される製品Hの機能を，それぞれ40字以内で述べよ。

設問3　〔DBサーバ及びHSMサーバの構成設計〕について，(1)，(2)に答えよ。

(1) DB及び表領域の作成手順中，(i)の代わりにHSMサーバ1とHSMサーバ2の両方を稼働させておいた場合，(ii)から(viii)までのどの手順がエラーとなるか。一つ選び，記号で答えよ。また，エラーが発生するAPI-Xのコマンド及びAPI-Xのエラーの原因を，それぞれ35字以内で具体的に述べよ。

なお，コマンドについては図3の形式，図3中の用語，及び図4中の用語を用い，鍵はどのDBのものかも記述すること。ここで，最初のAPI-Xの実行要求は，Hサーバ1に送信される。

(2) Hクライアントにおいて，Hクライアント IDをデータ鍵IDに付け加える

機能がなかった場合，特定の条件においてDB作成がエラーになる。その条件を40字以内で述べよ。

設問4　〔K2システムにおけるリスク対策の補完〕について，(1)，(2)に答えよ。

(1)　対策1は，誰がどのような方法で契約情報を取得するリスクに対する対策か。リスクを45字以内で述べよ。

(2)　対策2は，誰がどのような方法で契約情報を取得するリスクに対する対策か。リスクを50字以内で述べよ。

〔 メ モ 用 紙 〕

〔 メ モ 用 紙 〕

6. 退室可能時間に途中で退室する場合には，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。