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。

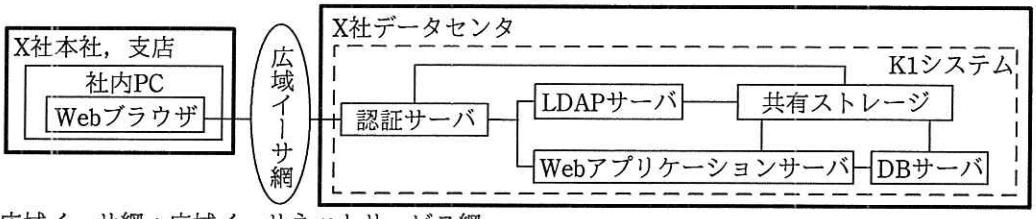
・データベース（以下，DB という）サーバ：被保険者の氏名，生年月日，住所，電話番号，医療情報・健康情報など（以下，被保険者情報という）及び契約条件（以下，被保険者情報と契約条件を併せて契約情報という）を保管

・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。

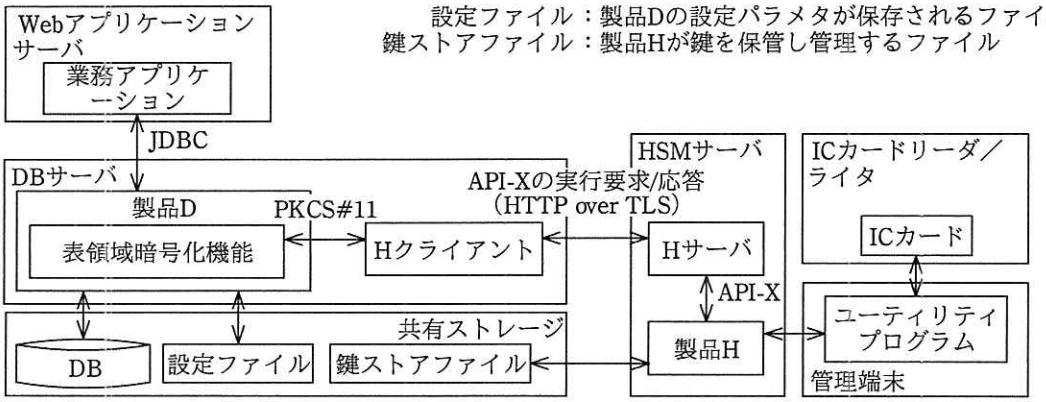


図 2　K2 システムにおける契約情報の暗号化機能の概要

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。

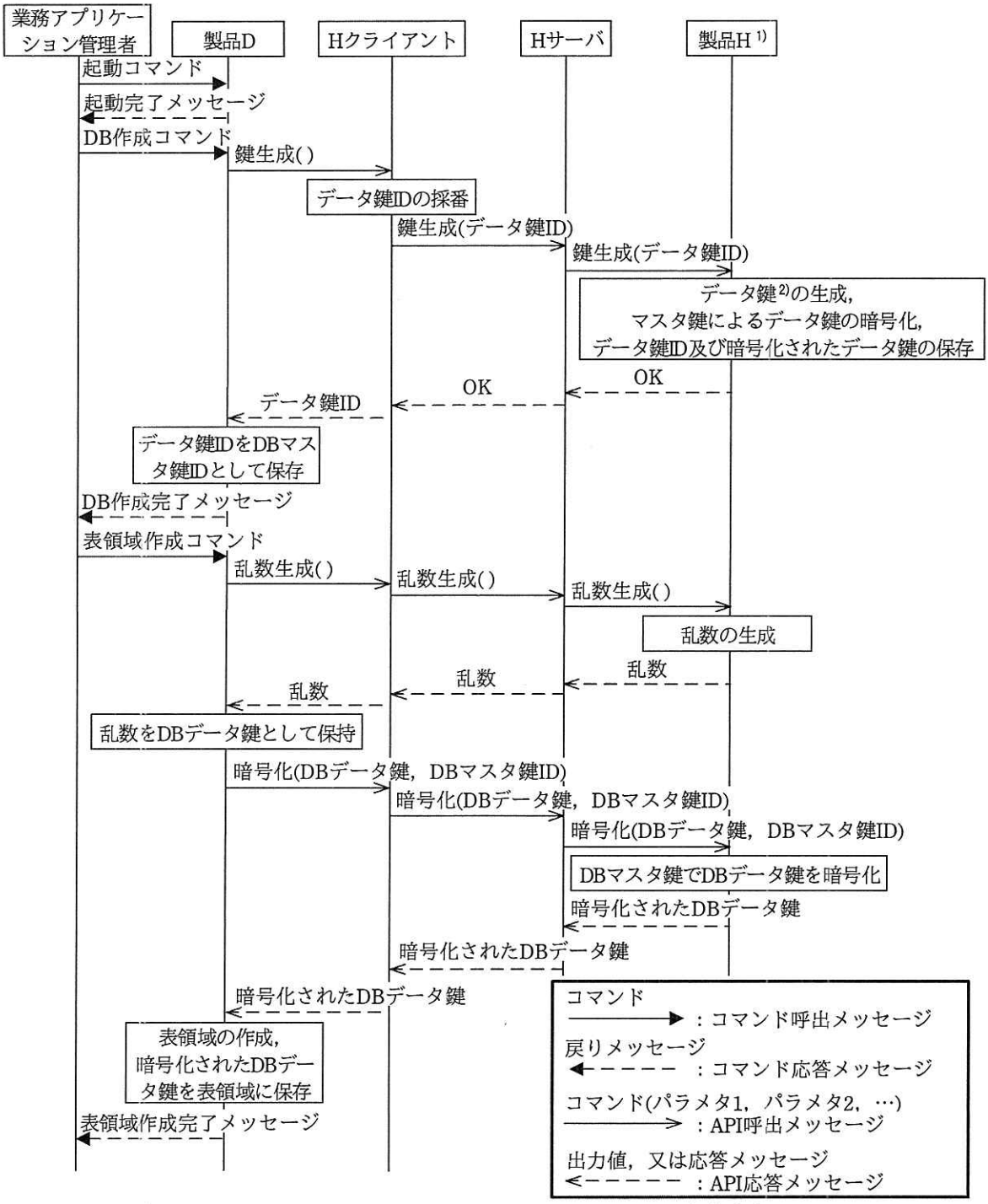
仕様 D　ディスクからデータを読み込む際，製品 D は，まず，ディスク上からデー

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〕

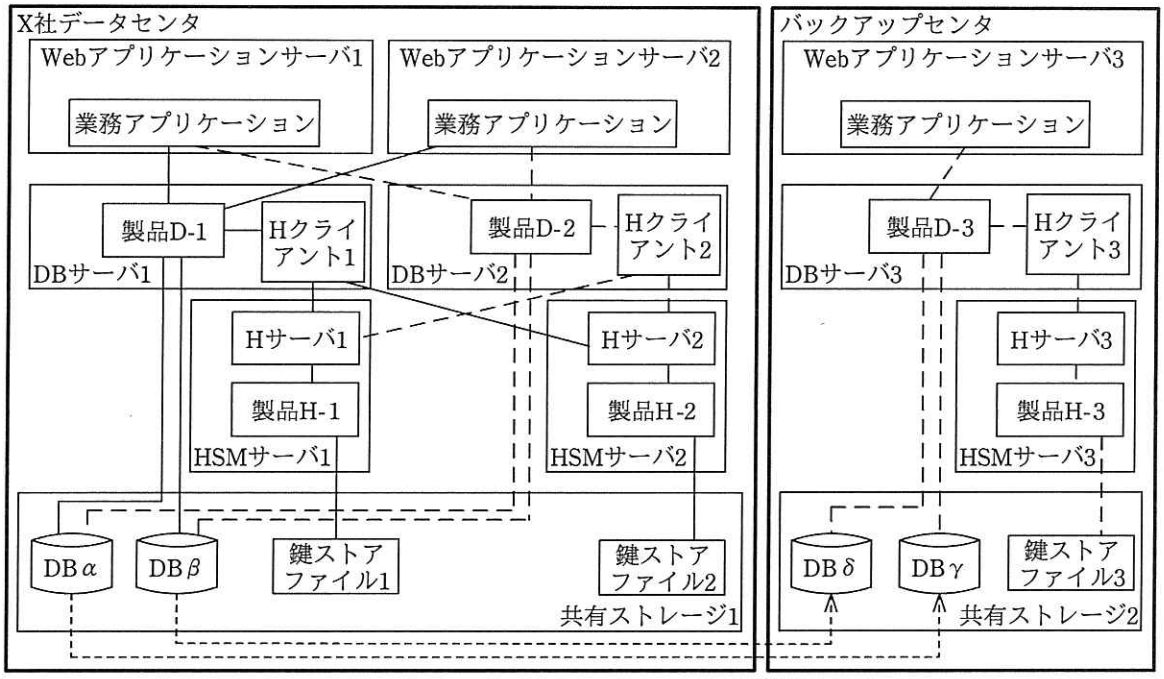
X 社は，K2 システムのサーバ構成について，Y 社に次の要件で設計を依頼した。

・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。



———：通常時の通信
－－－－：障害発生時の通信
-----➢：災害対策のためのデータコピーの流れ

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。

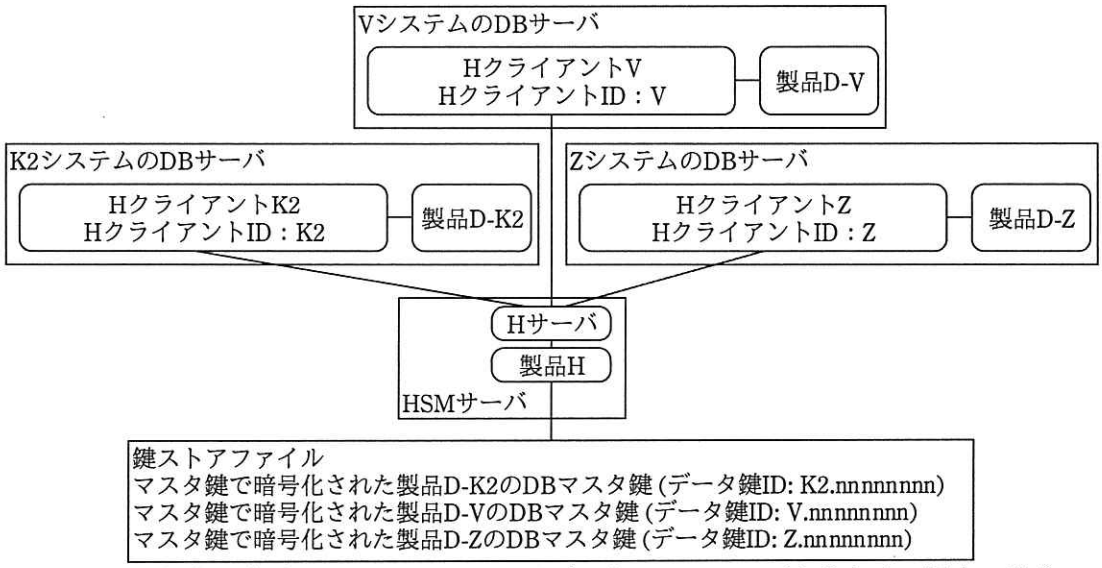


図5　複数の業務システムのDBサーバが1台のHSMサーバを共有する場合の構成

〔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。