2012 年 4 月 17 日
DNSSEC ジャパン
運用技術 WG

HSM を利用した DNSSEC の運用に関する考察

目次

1. はじめに

1.1. 背景

2010 年 7 月のルートサーバー導入を契機に導入が始まった DNSSEC 技術では、ルートゾーンや各 TLD の対応だけでなく、権威 DNS サーバーの対応が必要不可欠だが、その導入には様々なノウハウが必要となる。

そこで我々DNSSEC ジャパンでは、検証や導入実績に基づいた各種ノウハウを文書化し提供してきた。 その一環として権威 DNS サーバーへの DNSSEC 導入設計で重要な検討要素となる鍵管理についても、チェックリストを作成・公開した[1]。しかし鍵管理の一ツールである HSM (ハードウェア・セキュリティ・モジュール) についてその意義や利用方法の情報が不足しているという声があったため、DNSSEC における HSM の利用について調査・検討を行った。 その結果を、ここに考察として報告する。

DNSSEC ジャパンとしては、本報告によって健全な DNSSEC 対応のコンテンツ DNS サーバーを構築する一助になれば幸いである。

1.2. 目的

本報告では、権威 DNS サーバーへの DNSSEC 導入において、HSM の導入意義や利用方法の情報と HSM 導入要否の判断の材料を提供することを目的としている。

1.3. 想定する読者

本報告の読者としては、既に権威 DNS サーバーを運用しており、且つ、権威 DNS サーバーへの DNSSEC 導入を検討している、あるいは既に実施した、ISP、DNS サーバー運用者を想定している。本報告の完全な理解のためには、DNSSEC の概念と、DNSSEC における鍵管理の要件について基本的な理解があることが望ましい。

DNSSEC ジャパンが公開している下記の文書を参考にするとよい。

・DNSSEC の仕組みと現状 [2]

・DNSSEC 導入に当たって [3]

・DNSSEC における鍵管理 [4]

1.4. 注意事項

- 免責事項

  本ドキュメントの内容は保証されたものではない。下記 Web サイトの免責事項を確認のうえ、本ドキュメントを使用して頂きたい。

  http://dnssec.jp/?page_id=16

- 問合せ先

  本ドキュメントに関する改善点等のコメントは下記事務局まで連絡頂きたい。

  DNSSEC ジャパン事務局 ＜sec@dnssec.jp＞

1.5. 謝辞

本文書を作成するにあたり、貴重な時間を割いてご協力いただきました以下の皆様に深く感謝いたします。
DNSSEC ジャパン 運用技術ワーキンググループ
編集: 東京エレクトロン デバイス株式会社

2. HSM とは

2.1. HSM の概要

HSM (ハードウェア・セキュリティ・モジュール)は暗号モジュールの一種で、暗号鍵など重要な情報を物理的に保護する機能を持ったものを指す。
暗号モジュールの規格は、米国連邦標準規格である FIPS 140-2 [5]で定められたものが広く利用されている。 FIPS 140-2 には認定制度があり、認定された製品のリストが公開されている[6]。 FIPS 140-2 には 4 段階のレベルが規定されているが、物理的な対策が規定されているのはレベル 2 以上であり、従って HSM の要件としてはレベル 2 以上の認定を取得していることがひとつの指標となる。 レベル 2 では暗号鍵情報への物理的な侵害の証跡を提供できること、レベル 3 では物理的なアクセスを防止できることが求められる。 つまり侵害の証跡を残すだけでなく情報流出の防止まで求める場合にはレベル 3 が必要となる。
HSM 以外の暗号モジュールについては、DNSSEC ジャパンの「DNSSEC における鍵管理[4]」に解説がある。

HSM の形態は大きく分けて 3 種類ある。

1) 汎用のコンピューターに接続（PCI スロット、USB 等）
2) ネットワーク接続（アプライアンス）
3) 特定の機器に組み込み（支払い端末等）

論理的には HSM は暗号処理を必要とするアプリケーションから呼び出されて暗号処理を実行する。 その呼び出しには、HSM が提供する API を利用する。 代表的な API に PKCS#11、Microsoft CryptoAPI / CNG、Java JCE などがある。 アプリケーションやホストとの関係の例として、HSM 利用の概念図を本報告の 3.2 項に示す。
暗号鍵は HSM の中で生成され、HSM 内に保存され、暗号処理実行時に HSM 内で利用される。 従って HSM 利用時には暗号鍵は外部からアクセス可能な状態(例えばサーバー上のファイルやメモリなど)で存在することがなく、持ちだしたり改竄したりできないことで暗号鍵を保護できる。

2.2. HSM が守るもの・守らないもの

HSM を含む暗号モジュールは暗号鍵情報を安全に保管することと、保管している暗号鍵を使った暗号処理を安全に実行することを目的としている。

HSM を利用するアプリケーションの安全性を高めるものではないため、アプリケーションや HSM が接続されるコンピューターの安全性は別途考慮する必要がある。

FIPS 140-2 でも、暗号モジュールを利用するコンピューター等のシステムが用途や環境にとって適切なセキュリティレベルを提供していることを確認する必要があるとしている。

ただし仮にサーバーが不正利用された場合でも、HSM で保護された暗号鍵を持ち出すことは（ファイルシステムに保存する場合と異なり）できない。

2.3. HSM 運用の基礎知識

HSM は、セキュリティを確保するための仕組みを提供している。 導入や運用の際には、その仕組みに従った手順を実施する必要がある。

導入の一般的手順:

- HSM のハードウェアと必要なソフトウェアの導入
- HSM 管理のための認証設定
- 利用する暗号鍵領域のセットアップ
- 暗号鍵アクティベーションための認証設定
- アプリケーションから HSM を利用するための設定

HSM 管理のためと暗号鍵アクティベーションのための二種類の認証が、アクセス制御のために必要になる。 アクティベーションとは、保管している暗号鍵を利用可能にする手続きのことで、アプリケーションから暗号鍵へのアクセスを開始する時に必要になる。

認証の手段として、物理的なトークン（スマートカードや何らかの鍵等）やソフトウェアのトークン（パスワード等）が利用可能である。 このうち物理的なトークンを利用するための機器が HSM には用意されている（スマートカードリーダーなど）。 認証の手段や登録人数などについてセキュリティポリシーを満たす形で設計する。 例えば鍵生成に複数人の立会を必須とするようなポリシーを強制する形で実装できるなど、ポリシーを形にしてその運用を証明できる所が HSM の大きなメリットとなる。

運用（HSM の利用）:

- 認証: 導入時に設定した暗号鍵をアクティベーションするための認証手順の実施
- HSM 機能の利用(鍵の生成、暗号処理、署名等): アプリケーションから実行
- 可用性の確保

HSM は稼働中にはアプリケーションから利用される形態となり、特に直接操作することは少ない。 注意すべき点は、利用開始時に、導入時に決めた認証設定に従った認証手順が必要となることである。 (例えばスマートカード挿入やパスワード入力など。)

可用性について述べると、故障等により HSM が利用できなくなるとアプリケーションも利用できなくなる。 従って HSM は冗長化して導入されることが多い。

運用（HSM の管理）:

- 鍵管理環境の変更
- データのバックアップと復元
- 障害時の再セットアップ

認証パラメーターの設定など鍵管理環境の変更や、障害時の対処などの場合に HSM の操作が必要になる。 そういった際に独特なのは、導入時に設定した HSM 管理用の認証設定に従う必要があることである。 たとえば、管理用のスマートカードを持った管理者が設定された人数揃わないと管理操作ができない。

3. DNSSEC と HSM

3.1. DNSSEC と HSM の関係

DNSSEC は DNS のレコードに電子署名を付加することで、レコードの出自が正しいことと、レコード内容が改竄されていないことを証明できるようにする。 電子署名には、公開鍵暗号方式という仕組みが使われ、権威サーバーの秘密鍵(private key)を使って電子署名を付加し、秘密鍵と対になる公開鍵(public key)を使ってデータの正当性を検証できる[7]。 あるドメインで電子署名に使われている秘密鍵を入手できれば、そのドメインになりすまして電子署名を任意のデータに付加することが可能になってしまうため、秘密鍵の保護が重要となる。

(公開鍵は検証用に広く公開される前提のものであるため、保護の必要はない。ただし、ある公開鍵が特定の組織のものであることの証明は重要で、そのために「信頼の連鎖(chain of trust)」という仕組みが使われる[7]。)

BIND 等の DNS ソフトウェアで鍵を生成する場合、標準的には秘密鍵もサーバーのファイルシステム上に保管される。 ファイルシステムが参照できれば秘密鍵にアクセスできてしまう環境ではセキュリティ強度が不充分と考えられる場合に、HSM の利用がセキュリティ強化の選択肢となる。

BIND の開発元 ISC が開催したウェブセミナーでは、DNSSEC における HSM の利用について、次のように説明している[8]。

- ファイルシステムは、権限を取得したユーザーによるローカルの攻撃に対して常に脆弱
- 重要な(“high value”)ゾーンはより強固なセキュリティが必要
- HSM は秘密鍵を取り出し不可能にしてくれる

3.2. DNSSEC における HSM のシステム設計

DNSSEC に対応した DNS サーバーでは、オプションとして HSM 利用の機能を提供するようになってきている。 従ってそういった HSM 対応済み DNS サーバーを利用することで、特に開発作業なしに DNSSEC に HSM を適用できる。

BIND ではバージョン 9.7 より PKCS#11 という API がサポートされ、HSM が利用できるようになった。 鍵生成に dnssec-keygen の代わりに pkcs11-keygen コマンドを使用して、HSM 内に鍵を生成することができる。

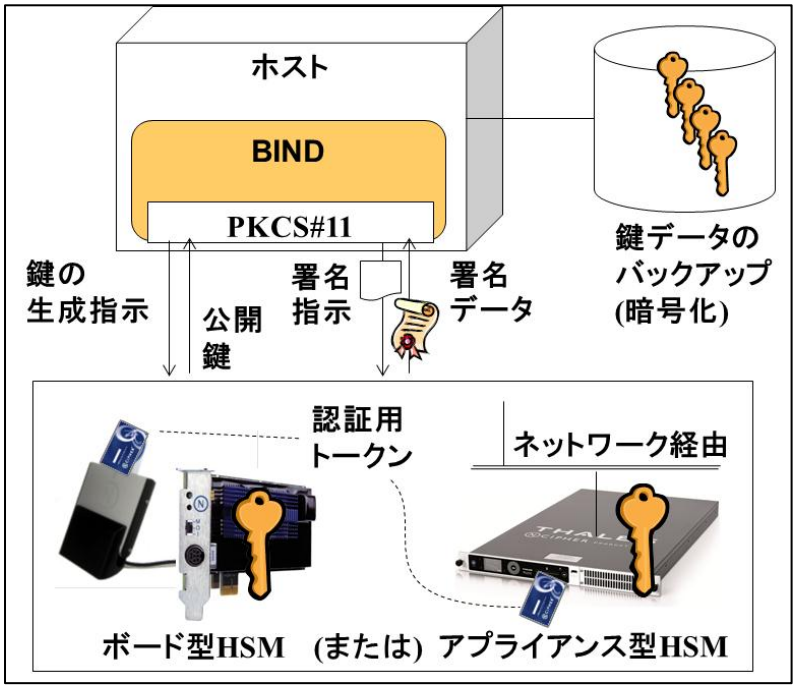

図 1 BIND からの HSM 利用概念図

BIND で HSM を使って DNSSEC の鍵を作る場合のおおまかな流れは次のようになる。

- HSM と HSM 用ソフトウェアのインストール、セットアップ
- BIND と OpenSSL のセットアップ（インストールと pkcs#11 対応)
- 暗号鍵ペアの生成（KSK と ZSK、pkcs11-keygen コマンド）
- 鍵ファイルの作成（dnssec-keyfromlabel コマンド）
- 鍵生成の確認（pkcs11-list コマンド）
- これ以降は HSM 未使用時と基本的に同じ（dnssec-signzone …）

具体的な手順は BIND のマニュアルに記載があり[9]、HSM 機種ごとの情報はメーカーから提供されている[10]。

商用 DNS サーバー製品で管理 GUI があるものでは、HSM の利用も GUI で簡単にできる場合がある。 そうした場合はセットアップが簡単になり、専用コマンドなどを気にする必要もなくなる。

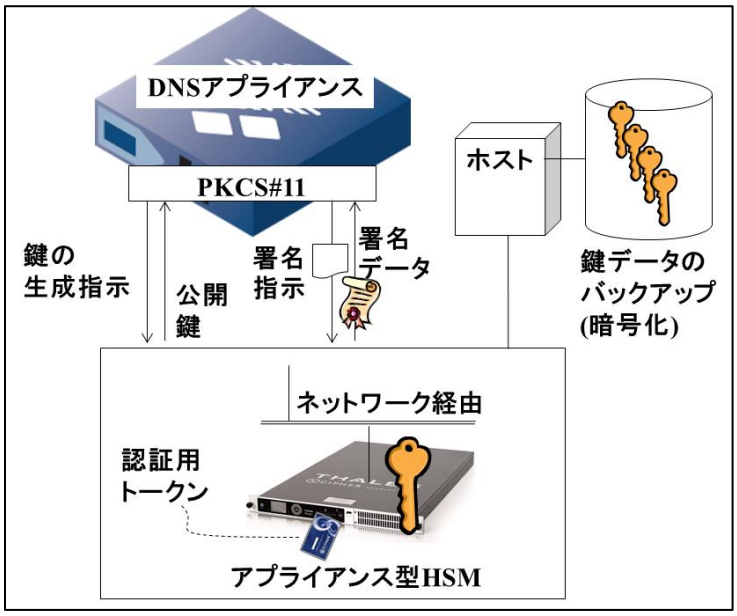

図 2 DNS アプライアンスからの HSM 利用概念図

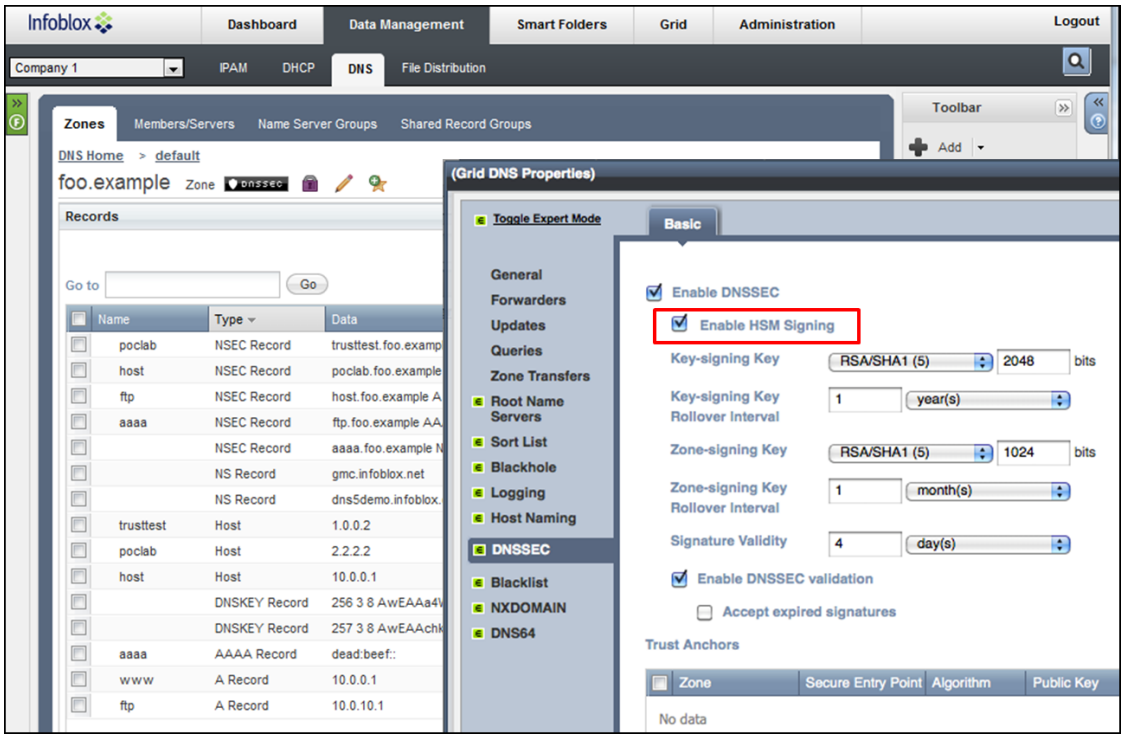

図 3 DNS アプライアンスで HSM 使用を設定する画面例（赤枠は筆者追加）

3.3. HSM 導入のメリット

HSM 導入に関して負担になる要素として、導入コスト、システム構成要素の増加、独特の運用手順への対応などが考えられる。
導入要否の判断においては、これら負担要因と得られるメリットとの比較が必要になる。
その検討のために、HSM 導入のメリットとして考えられる点を考察した。

1) 暗号鍵の保護 – HSM を利用すると、秘密鍵が平文で流出する可能性を低減できる。 サーバーのハードディスク上に秘密鍵を保管することが許容できないシステムでは、HSM の利用が有望な選択肢となる。
2) 安全な鍵のバックアップ – 平文で暗号鍵を管理するシステムでは、バックアップデータに暗号鍵が平文で含まれる可能性もあり、流出の可能性が格段に高まる。一般的に HSM では安全な鍵情報のバックアップ手段を提供している。
3) 運用ポリシーの確実かつ迅速な実装 – DNSSEC を利用するシステムの運用ポリシーでは暗号鍵の運用に詳細かつ煩雑な内容が規定されることがある。 そうした場合、HSM の導入によってポリシー遵守を確実にすることでセキュリティ強度を高められ、人的対応削減によりコストを抑えつつ迅速な対応が可能になる。
4) アカウンタビリティ – HSM 利用時は利用手順や認証手続きが強制されるため、セキュリティ対策状況やポリシー遵守状況を対外的に説明することが容易になる。 その結果、例えばドメイン名のなりすましといった事件が発生した時に原因の可能性をある程度狭められる（内部関係者による暗号鍵の持ちだしは除外等の）効果がある。

上記 4 項目のうち、3）項については自明ではないと思われるため、3.4 項で説明する。

3.4. DNSSEC 運用ポリシーと HSM

HSM 導入によって、運用ポリシー、特にセキュリティ対策を実装する際に、セキュリティ対策の確実性を向上し、コスト抑制のメリットがあることを前項 3.3 の 3）で指摘した。 事実過去の事例として、セキュリティ要件が事実上実装不可能、あるいは現実的でないといったケースの解決策として HSM が利用されている。
ここでは DNSSEC の運用ポリシー実装における HSM の効果を考察する。

題材として、現在 IETF で標準化が進められているポリシーの枠組み「DNSSEC Policy & Practice Statement Framework [11]」(2012 年 04 月現在ドラフト、以下「DPS フレームワーク」と呼ぶ)の鍵管理に関する部分を検討した。
DPS は、DNSSEC のポリシーと実装（Policy & Practice）の宣言文（Statement）ということでつまり、「DNSSEC の運用内容を明文化し、情報公開するための文書」 [12] だ。
DPS フレームワークは、DPS を執筆するドメイン管理者やゾーン運用者を支援する枠組

み（お手本）として開発されており、つまり DNSSEC の運用を計画する時に何を決めるべきかのリストを提供する。

DPS フレームワークでは DNSSEC の運用に関する広範なポリシー項目が紹介されている。 その中で技術的なセキュリティコントロール(Technical Security Controls)を説明する 4.5 項では、暗号鍵とアクティベーション・データ(暗号鍵を利用可能にするための情報)の保護が中心となっている。特に DPS フレームワークの 4.5.2 項は秘密鍵の保護と暗号モジュールの技術的制御について決定すべき内容を定めている。 その 10 項目のうち、HSM によって実装が用意になると思われる項目を
表 1 に解説する。

表 1 DPS フレームワーク 4.5.2 項で HSM が効果的な項目

DPS 項目の要約	HSM を利用することによる効果
鍵生成に使われる暗号モジュールが準拠すべき標準規格	例としてあげられている FIPS 140-2 への準拠を提供する。
複数人による秘密鍵管理（M 名のうち N 名、の M と N を規定）	スマートカード認証等により M 名のうち N 名を強制する形で実装できる。
秘密鍵のバックアップ有無と、バックアップのセキュリティ対策	秘密鍵を暗号化するなど、安全なバックアップを容易に取得できる。
秘密鍵の保管形態（平文か暗号か、分割か）	秘密鍵を暗号化した上でアクセス権限を分割した形で保管する機能を提供する。
秘密鍵アクティベーションの方法（担当者定義、認証等）	アクティベーションに複数人の多要素認証を強制する一方、M 名のうち N 名といった柔軟な運用を提供できる。
秘密鍵の破棄（担当者、方法）	認証を強制した上で残存データのない破棄操作を提供できる。

DPS フレームワーク 4.5 項ではこの他にも鍵生成や鍵ペアの管理、アクティベーションデータなどについて規定しており、HSM 利用によってポリシー策定や実装、運用を支援できる。

つまり、HSM を利用することにより、あらたに仕組みを開発すること無くポリシーを実装でき、しかも確実にポリシーが適用されていることを証明することができる。

本報告の 5.1 項ではこうした DPS の策定と HSM 活用の事例を紹介する。

3.5. HSM 導入でメリットが考えられるユースケース

どういう組織やシステムで HSM の導入にメリットがあるかを検討した。 管理するゾーン情

報の規模や性質と、ドメインが示す組織の性質の 2 つの側面があると考えられる。

1） ゾーンの規模や性質

一般的に管理するドメインの数やゾーン情報が大規模なほど、鍵管理も手間がかかるので、HSM によるセキュリティ対策の明確化が有用になると考えられる。

例えば opendnssec.org で公開している HSM Buyers' Guide [13]では、利用シナリオによる HSM の適合性をまとめている。 その要約を表 2 に示す。（なおこの資料では、ソフトウェア的な暗号モジュールなども含めて「HSM」と表現している。）

表 2 DNS ゾーンの利用シナリオと暗号モジュール

シナリオ	内容	暗号モジュール（「HSM」）の適合性
1	少数の小規模静的ゾーン	USB トークンやスマートカードで充分
2	少数の大規模静的ゾーン	USB トークンやスマートカードで充分
3	多数の小規模静的ゾーン	簡単な HSM (simple HSM)で充分
4	多数の大規模静的ゾーン	HSM の利用を推奨
5	動的ゾーン、数にかかわらず	HSM の利用を推奨

なおこの資料では、HSM を選定する際の注意点として、以下の 2 点を指摘している。

- 管理できる鍵の数は、ゾーン数の何倍かの(large multiple)容量があること
- 鍵の生成と署名の処理性能に注意すること

一般に、鍵の生成には署名処理よりはるかに長い時間がかかるため、より注意が必要となる。

2) サイトの性質

規模的な要素の他に、ドメインの性質によって暗号鍵の保護が重要になる場合があると考えられる。 秘密鍵が万一流出した場合のリスクが高いと考えられる、例えばフィッシングやなりすましの攻撃により多大な被害が考えられるようなドメインでは、HSM による保護を検討する必要がある。 海外の事例でも、第 5 章で紹介するルートゾーンの他に、金融機関などで HSM が導入されている。

DNS/DNSSEC への攻撃によるリスクが大きい組織には、次のようなものが考えられる。

- ウェブサイト: フィッシングの対象やドメインなりすましによって被害が大きいサイト (金融機関、ショッピング、ポータル、会員制サイト等)
- 電子メール: メールの横取りやなりすましで大きな被害が想定される組織
- サービス事業者: 上記のようなコンテンツのドメイン管理を請け負う組織
- 管理体制: 鍵の生成、保管、更新、バックアップ、廃棄などに工数をかけられない組織

4. HSM 導入の注意点

HSM 導入時に注意しておくべきだと考えられる項目を検討した。

4.1. 運用面の注意点

- 運用ポリシーとパラメーターを決めておく
  HSM 導入時には設定すべき内容がある(2.3 項を参照)。 主体となるのは暗号鍵をアクティベートできる管理者の人数や認証方法で、すなわち運用ポリシー(DPS)に依存する。 従って HSM の導入計画を立てる前に運用ポリシーを決めておく必要がある。
- バックアップ
  HSM が管理する鍵データのバックアップについても導入計画と同時に検討した方が良い。 HSM 製品はたいてい鍵を暗号化してバックアップする機能を提供しているが、バックアップ時や復旧時における操作担当者立ち会いの要否や、ディザスタリカバリ用バックアップデータの遠隔地コピー作成手順などが製品により異なるので、確認の上計画を立てる必要がある。
- 障害対応
  HSM が障害のため停止したような場合は、2.3 項で説明した二種類の認証のうち、HSM 管理の認証手順が必要になる。 従って障害対応手順は、必要となる認証手順(とそれに必要な管理者の召集などを含めた対応手順)を踏まえて計画する必要がある。

4.2. セキュリティ上の注意点

HSM は暗号鍵情報の保護を目的としており、セキュリティ対策をより確実に実装する手段を提供するが、DNSSEC や DNS のシステム全体を保護するものではない。 2.2 項で説明したように、アプリケーション(例えば BIND)のセキュリティはしっかり対策しておく必要がある。

例えば BIND が稼働するサーバーの管理者権限を取得すれば、不正な DNS レコードを作成してそれに署名し、公開できる可能性がある。

HSM を利用することの効果は、そうした場合も含めて、暗号鍵情報を持ち出せなくすることにある。 つまり、例えば DNS サーバーを不正利用された場合においても、暗号鍵情報を持ちだしてまったく異なる場所で本来のドメイン管理者になりすまして任意レコードの電子署名を作成する、といった攻撃に対する対策となる。

DNS インフラへの不正アクセスや悪用に対する対策は本報告の趣旨と異なるが、たとえば次のような対策が(HSM を導入する場合でも)必要と考えられる。

- サーバーの適切な配置(ファイアウォールの内側つまり LAN 側へのマスターサー

バー設置等）

- アクセス制御（ユーザー認証、アクセス元のフィルター等）
- 適切な構成や設定（不要なサービスの停止、ディレクトリの権限設定、ゾーン転送や再帰的問い合わせの制限等）
- 使用ソフトウェアの脆弱性への迅速な対応

5. 導入事例

DNSSEC の暗号鍵保護の目的で HSM を導入した事例を紹介する。 民間企業でもサービス・プロバイダーや金融機関で該当する事例があるという報告があるが、具体的な情報が公開されていないため、今後の情報公開を待ちたい。

5.1. ルートゾーン

DNS のルートゾーンでは、KSK 秘密鍵を HSM に格納して管理している [14]。

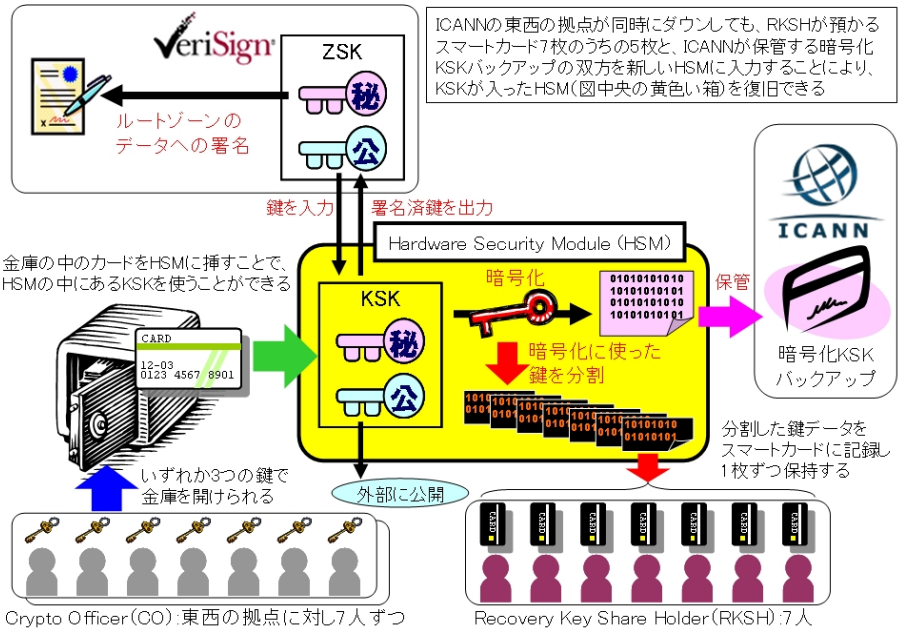

図 4 ルートゾーンにおける KSK の管理方法（出典：JPRS.JP）

ルートゾーンの DPS は KSK と ZSK に分けて公開されている。 KSK の DPS では、ICANN における鍵管理のポリシーが記載されている[15]。

例えば KSK の秘密鍵を格納する HSM を活性化（アクティベーション）する際には、クリプト・オフィサー（CO）という役割を割り当てられた 7 名のうち 3 名が揃って認証される必要がある。

また KSK 秘密鍵のバックアップは暗号化した上でコピーを作成するが、その際の暗号化鍵はリカバリー・キー・シェア・ホルダー（RKSH）という役割を割り当てられた 7 名のうち

5 名が揃って認証されると利用可能な形で保存される。
いずれの場合も、M 名のうち N 名という認証を実施する手段として、HSM のスマートカード認証の仕組みが用いられている。

ルートゾーンの DPS ではこれらの他に、秘密鍵が暗号化されたバックアップ以外には HSM の外に持ち出されないことや、鍵の破棄を確実にすること、鍵ペア生成の手順として参照しているキー・セレモニー・ガイド[16]などにおいて、HSM の機能を活用したポリシーが定められている。

あるドメインの DNSSEC 対応において策定する権限分散の度合いは、そのドメインの重要性などによるリスク管理ポリシーに依存すると考えられる。 7 名のうち 5 名といったポリシーは一般的に高い運用負荷が想定されるためである。 ただし鍵管理において一定の認証ポリシーを実装しようとする場合、ポリシー実装と運用の明確化と強制をシンプルに実現するツールとして HSM を利用できることが、ルートゾーンの事例からわかる。

6. まとめ

HSM の導入と運用には一定の費用がかかるが、3.3 項で説明したように独自のメリットがある。

1) 暗号鍵の保護
2) 安全な鍵のバックアップ
3) 運用ポリシーの確実かつ迅速な実装
4) アカウンタビリティ

ネットワークの健全な運用にとって極めて重要な要素である DNS を保護するための DNSSEC への対応に際し、本報告が HSM 導入要否に関する検討の一助になれば幸いである。

参考文献

[1] DNSSEC ジャパン、DNS サーバ DNSSEC 導入鍵管理チェックリスト ＜http://dnssec.jp/wp-content/uploads/2011/04/20110316-dnssec-techwg-keymgmt-checklist.pdf＞
[1] DNSSEC ジャパン、DNS サーバ DNSSEC 導入鍵管理チェックリスト ＜http://dnssec.jp/wp-content/uploads/2011/04/20110316-dnssec-techwg-keymgmt-checklist.pdf＞
[2] DNSSEC ジャパン、DNSSEC の仕組みと現状 ＜http://dnssec.jp/wp-

content/uploads/2010/11/20101122-techwg-DNSSEC-mechanisms-and-status.pdf >
[3] DNSSEC ジャパン、DNSSEC 導入に当たって < http://dnssec.jp/wp-content/uploads/2010/11/20101122-techwg-DNSSEC-deployment.pdf >
[4] DNSSEC ジャパン、DNSSEC における鍵管理 < http://dnssec.jp/wp-content/uploads/2011/04/20110317-dnssec-techwg-keymgmt.pdf >
[5] NIST、FIPS PUB 140-2 < http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf >
[6] NIST、Module Validation Lists < http://csrc.nist.gov/groups/STM/cmvp/validation.html >
[7] JPRS、DNSSEC とは < http://dnssec.jp/wp-content/uploads/2010/07/20100721-whats_dnssec-sakaguchi.pdf >
[8] ISC、DNSSEC Key Management Best Practices (Part 1 of 3) < http://www.isc.org/files/DNSSEC_Key_Management.pdf >
[9] BIND 9 Administrator Reference Manual (9.8) PKCS #11 (Cryptoki) support < http://ftp.isc.org/isc/bind9/cur/9.8/doc/arm/Bv9ARM.ch04.html#pkcs11 >
[10] Thales nShield HSM Integration Guide for ISC BIND DNSSEC < http://www.thales-esecurity.com/Resources/~/media/Files/Integration%20Guides/ISC_BIND_DNSSEC_9_7_3_UNIX_2.ashx >
[11] IETF、DNSSEC Policy & Practice Statement Framework < http://tools.ietf.org/html/draft-ietf-dnsop-dnssec-dps-framework-07 >
[12] JPNIC、DPS とは < http://www.nic.ad.jp/ja/basics/terms/dps.html >
[13] Opendnssec.org、HSM Buyers' Guide < https://wiki.opendnssec.org/display/DOCREF/HSM+Buyers%27+Guide >
[14] JPRS、ルートゾーンにおける KSK の管理方法 < http://jprs.jp/dnssec/doc/root_tcr.html >
[15] DNSSEC Practice Statement for the Root Zone KSK operator < http://www.root-dnssec.org/wp-content/uploads/2010/06/icann-dps-00.txt >
[16] Root Zone DNSSEC KSK Ceremonies Guide < http://www.root-dnssec.org/wp-content/uploads/2010/05/draft-icann-dnssec-ceremonies-01.txt >