暗号鍵を保護するHSM
(ハードウェア・セキュリティ・モジュール)
～役割、DNSSECとの関係、使い方

- HSMとは
- DNSSECとHSM
- HSMの使い方

東京エレクトロン デバイス株式会社

CN事業統括本部 松永 豊

matsunaga.y@teldevice.co.jp

CISSP® Certified Information Systems Security Professional

HSMとは

暗号鍵の役割
公開鍵暗号を使った電子署名（デジタル署名）の場合

Aliceの
秘密鍵

＋

私は100円
借りました

署名付与

計算

署名

ありす

私は100円
借りました

署名検証

Aliceの
公開鍵

逆の計算

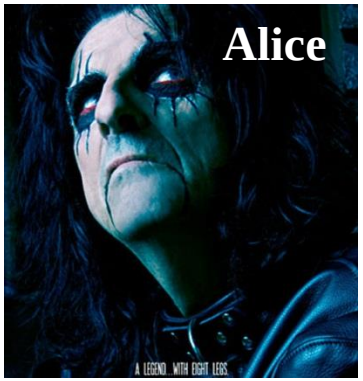
Aliceの
公開鍵ですよ

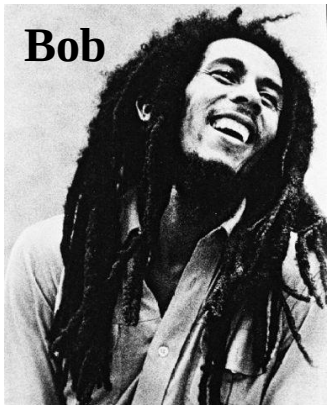
証明書または信頼の連鎖

•確かにAliceが書いた
•書き直されていない

Private Key
秘密鍵あるいはプライベート鍵、私有鍵
＝印鑑

Public Key
公開鍵
＝印鑑証明





- AliceがBobに約束をしたい
- Aliceしか持っていない印鑑
  =秘密鍵で「署名」をつける

秘密鍵が盗まれると…

ITmedia ニュース > セキュリティ > 認証局が不正なSSL証明書を発行、Googleユーザーを…

2011年08月31日 07時26分 更新

認証局が不正なSSL証明書を発行、Googleユーザーを狙う攻撃が発生

大手SSL認証局からGoogleなどのWebサイト用の不正なSSL証明書が発行された。Googleによると、これを使って同社のサービスとユーザーとの通信に割り込もうとする攻撃が発生しているという。

[鈴木聖子，ITmedia]

印刷／PDF　ツイート 68　g+1 11　Pocket 1　通知

PR ノエビアの決断~Cloud Firstでの全社システムリニューアル

PR 【富士通】ディスクストレージシステム市場売上シェア No.1

オランダの大手SSL認証局DigiNotarからGoogleなどのWebサイト用の不正なSSL証明書が発行され、これを使ってGoogleサービスとユーザーとの通信に割り込もうとする攻撃が発生している。Google、Firefox、Microsoftなどの主要Webブラウザメーカーは8月30日までに、ユーザー保護のための対策を表明した。

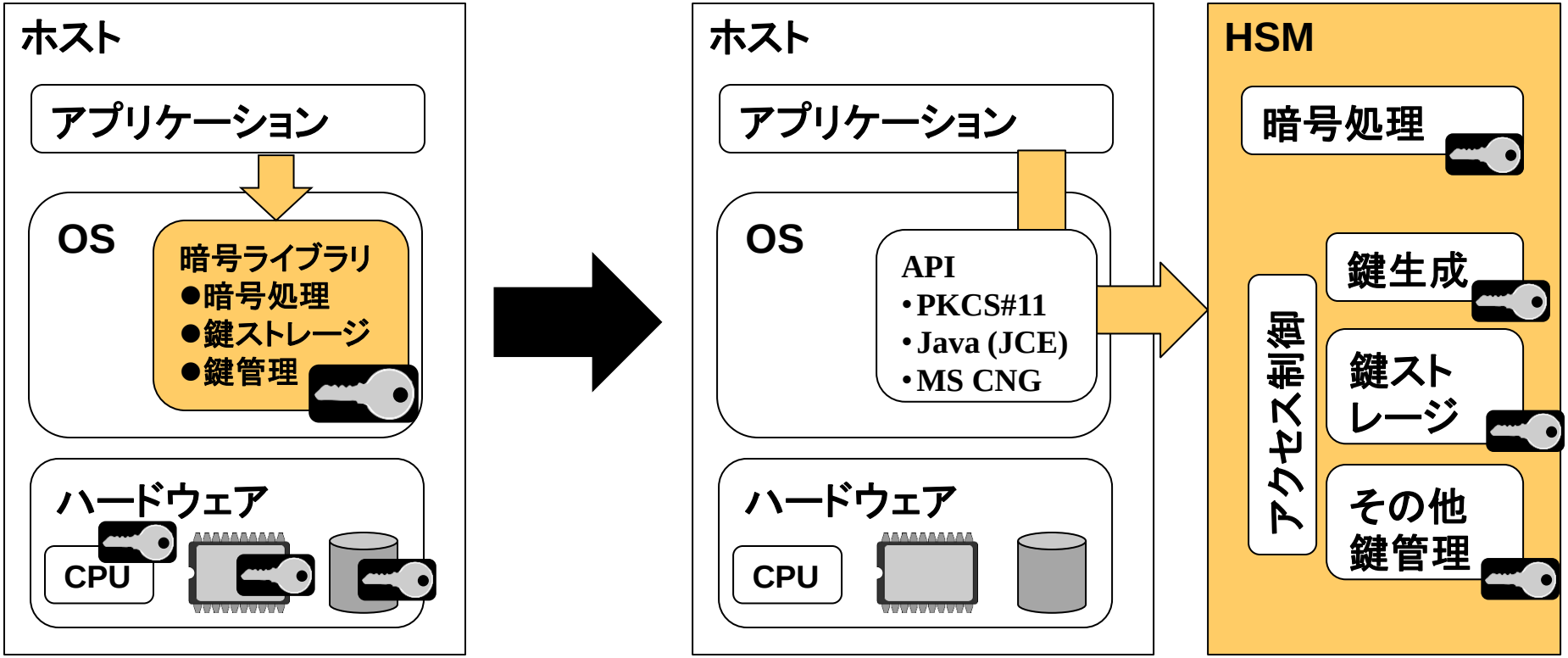
← この事件は秘密鍵流出ではなく、Webサイトのハッキングらしいですが…

- 秘密鍵流出でも同様の危険
  - なりすまし
  - 盗聴
  - サービス停止

HSMとは

- **HSM (ハードウェア・セキュリティ・モジュール)**
  - 暗号モジュール (cryptographic module) の一種

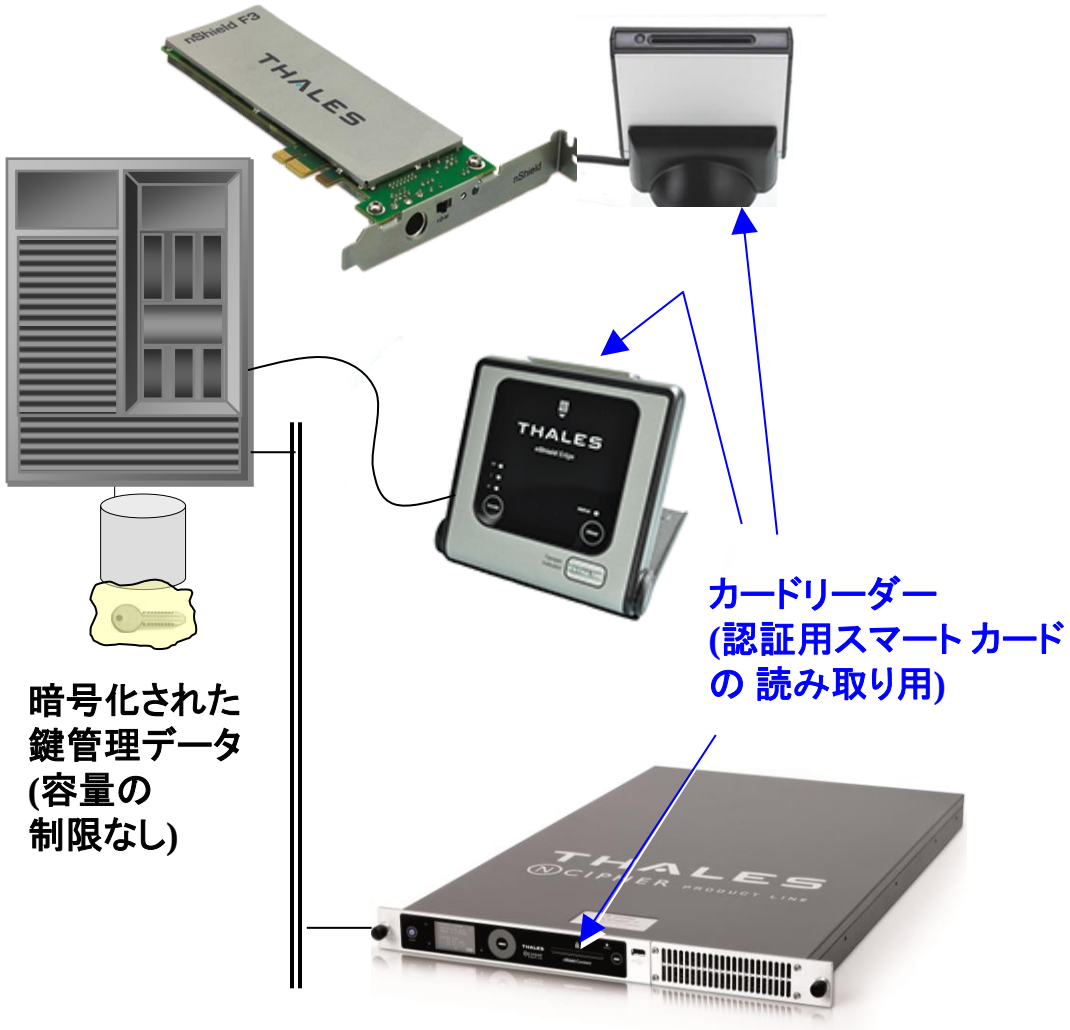
主な機能:
- 暗号鍵管理(生成、保存、復元、廃棄等)
- 暗号処理(暗号化/復号、署名など)
- アクセス制御



HSMの標準

- **FIPS 140-2**
  - 米NIST (国立標準技術研究所)が定める基準
  - 複数のレベル: 物理的要件と役割ベース認証はLevel 2から
  - Level 3で耐タンパー性 (tamper-detection/response)

HSMの形態



■ ボード型
- PCIスロット

■ 外付け型
- USB

■ ネットワーク型
- イーサネット

HSMのメーカー

A Review of Hardware Security Modules Fall 2010

http://www.opendnssec.org/2011/01/12/a-review-of-hardware-security-modules/

C.1 Certification levels - The validations only covers the actual cryptographic chip, not the complete HSM including administration, backup etc. It is also worth to note that the certifications are firmware specific and the modules need to be re-certified for each new firmware version.

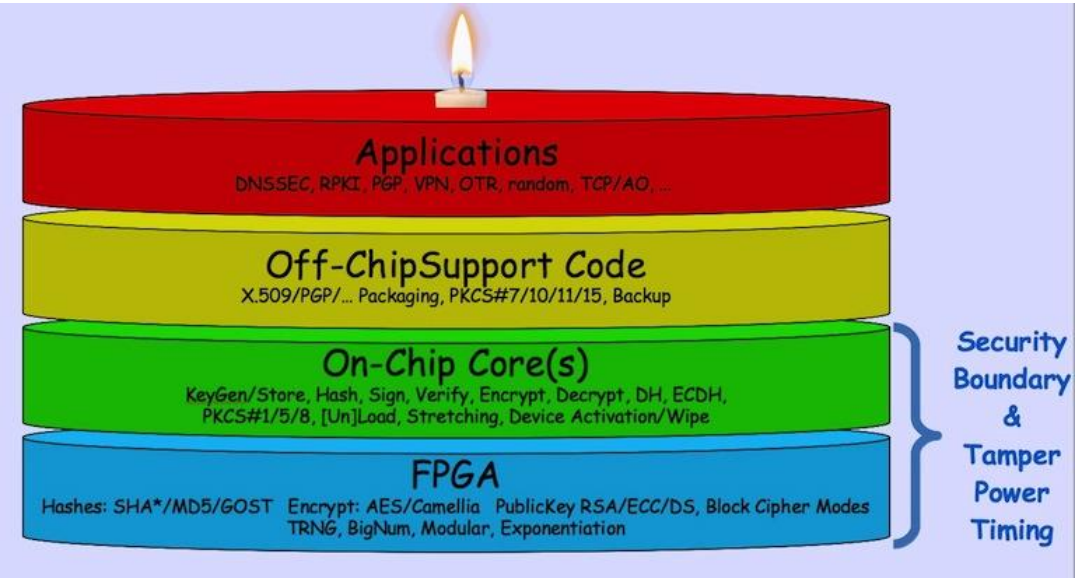
Module	Findings by the test team
AEP Keyper	FIPS 140-2 Level 4, FCC part 15 Class B, BSEN60950 Safety, BSEN61000 Susceptibility Performance B, BSEN55022 Level B Emissions
Safenet Luna	FIPS 140-2 Level 3 when using Trusted Path Authentication with PED keys (see security model) and Level 2 if using password authentication. CC EAL 4+
Thales nShield	FIPS 140-2 Level 3, CC EAL4+.
Utimaco CryptoServer	The model we tested, CryptoServer Se-Series LAN, is in the process of being FIPS 140-2 Level 3 validated. The CryptoServer CS-Series LAN is FIPS 140-2 Level 3 and ZKA (German Credit Association) validated".

C.2 Supported authentication methods – All of the modules use password protection on the PKCS#11 token for application usage.

Module	Findings by the test team
AEP Keyper	Smartcards for Security Officers and Operators. A minimum of two separate cards are required for security related operations.
Safenet Luna	Password or client certificates for appliance administrators. Password or PED keys for HSM admin and partition owners. A PED key is essentially an integrated smartcard used to authorize operations using the PED (Pin Entry Device).
Thales nShield	The Administrator and Operator Card Sets consists of smartcards. In addition softcards can be used for key wrapping.
Utimaco CryptoServer	All administrators/users can be authenticated using the following methods: Password (plain, SHA-1, HMAC) Client certificates stored on smartcard or in a key file. Direct smartcard logon onto the CryptoServer

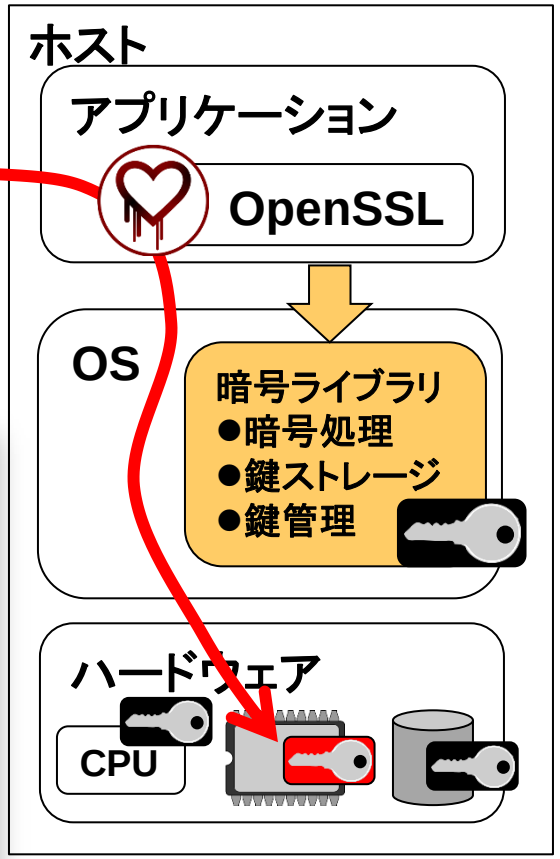
その他の暗号モジュール

- スマートカード(SmartCard-HSM) http://www.smartcard-hsm.com
  - スマートカード内で鍵の生成、署名などが可能
- ソフトウェア(SoftHSM) http://www.opendnssec.org/softhsm/
  - HSMなしでPKCS#11を利用するためのソフトウェア
  - 鍵データは平文でDBに保存
- オープンハードウェア：Cryptech
  - ~ trac.cryptech.is
- HSMとの違い：
  - FIPS認証
  - 耐タンパー性
  - 処理性能
  - 利用者の認証
  - 鍵管理

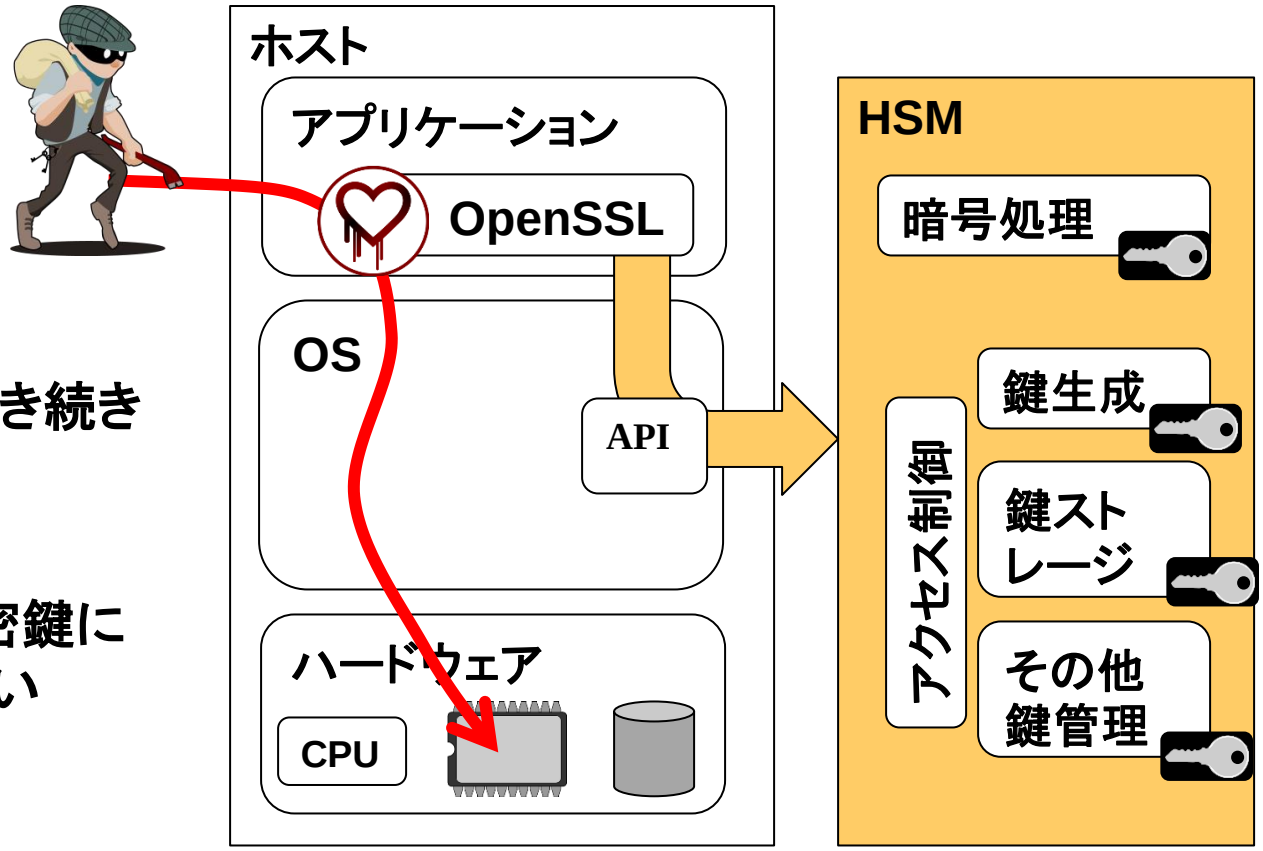


HSMの効果
例えば、ハートブリード

- 秘密鍵が危険にさらされた例：OpenSSL Heartbleed
- メモリ上の秘密鍵も取得される可能性
  - SSL通信の盗聴やサーバーなりすましの危険



OpenSSL Heartbleed ー HSM利用の場合



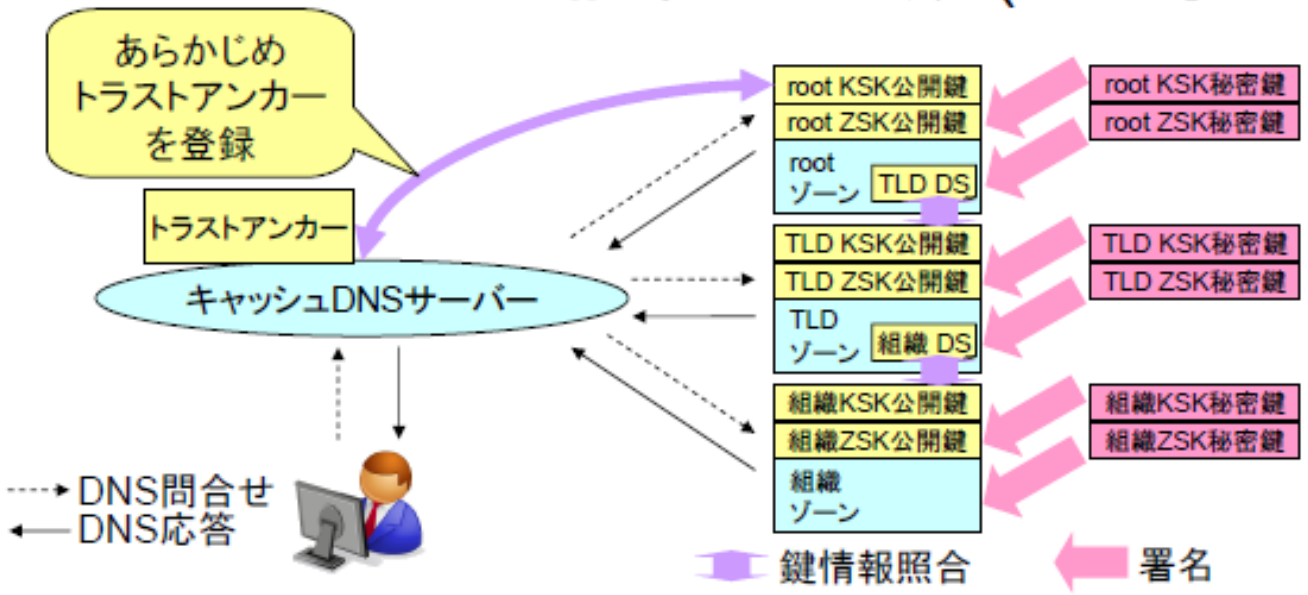
- Heartbleedの危険は引き続き存在
- ただし、サーバーの秘密鍵にアクセスされることはない

DNSSECとHSM

DNSSECと暗号鍵

JPRS

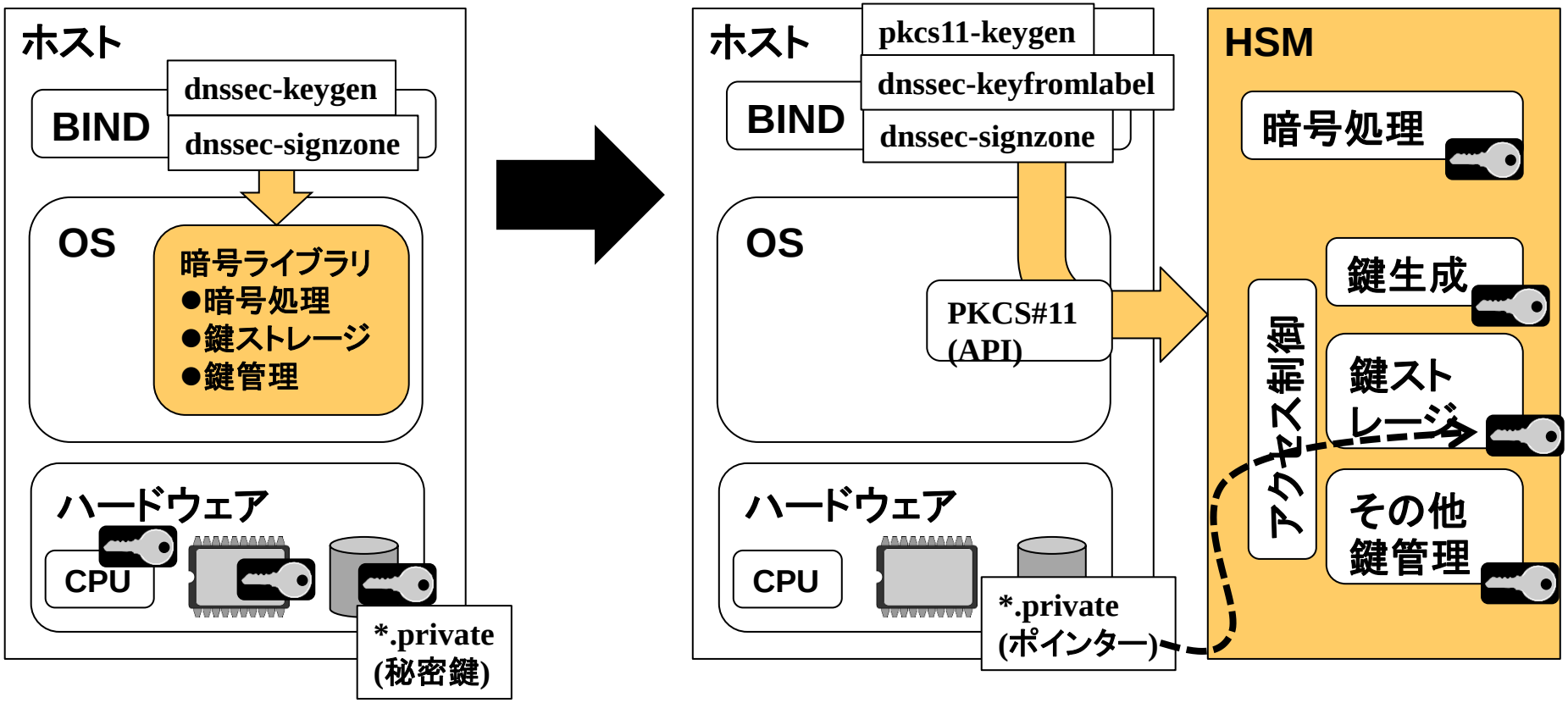
DNSSECの信頼の連鎖(DS導入後)



- 親ゾーンのZSKでDSに署名することにより、信頼の連鎖を構築
  - 親ゾーンに登録したDSと子ゾーンのKSKの公開鍵の情報を照合
- バリデーターがDNS応答の署名を検証
  - 通常の場合、キャッシュDNSサーバーがバリデーターとなる
  - キャッシュDNSサーバーにrootゾーンのKSK公開鍵またはDSを登録する
    ➔トラストアンカー

「DNSSECの概要」2013年5月29日DNSSEC 2013 スプリングフォーラム
株式会社日本レジストリサービス(JPRS) 舩戸正和

DNSSECでHSMを利用する



HSM利用のメリット

「HSM を利用した DNSSEC の運用に関する考察」
DNSSEC ジャパン 運用技術 WG
http://dnssec.jp/?page_id=792

1. 暗号鍵の保護
   - 秘密鍵が平文で流出する可能性を低減
2. 安全な鍵のバックアップ
   - HSMでは安全な鍵情報のバックアップ手段を提供
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 → 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
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

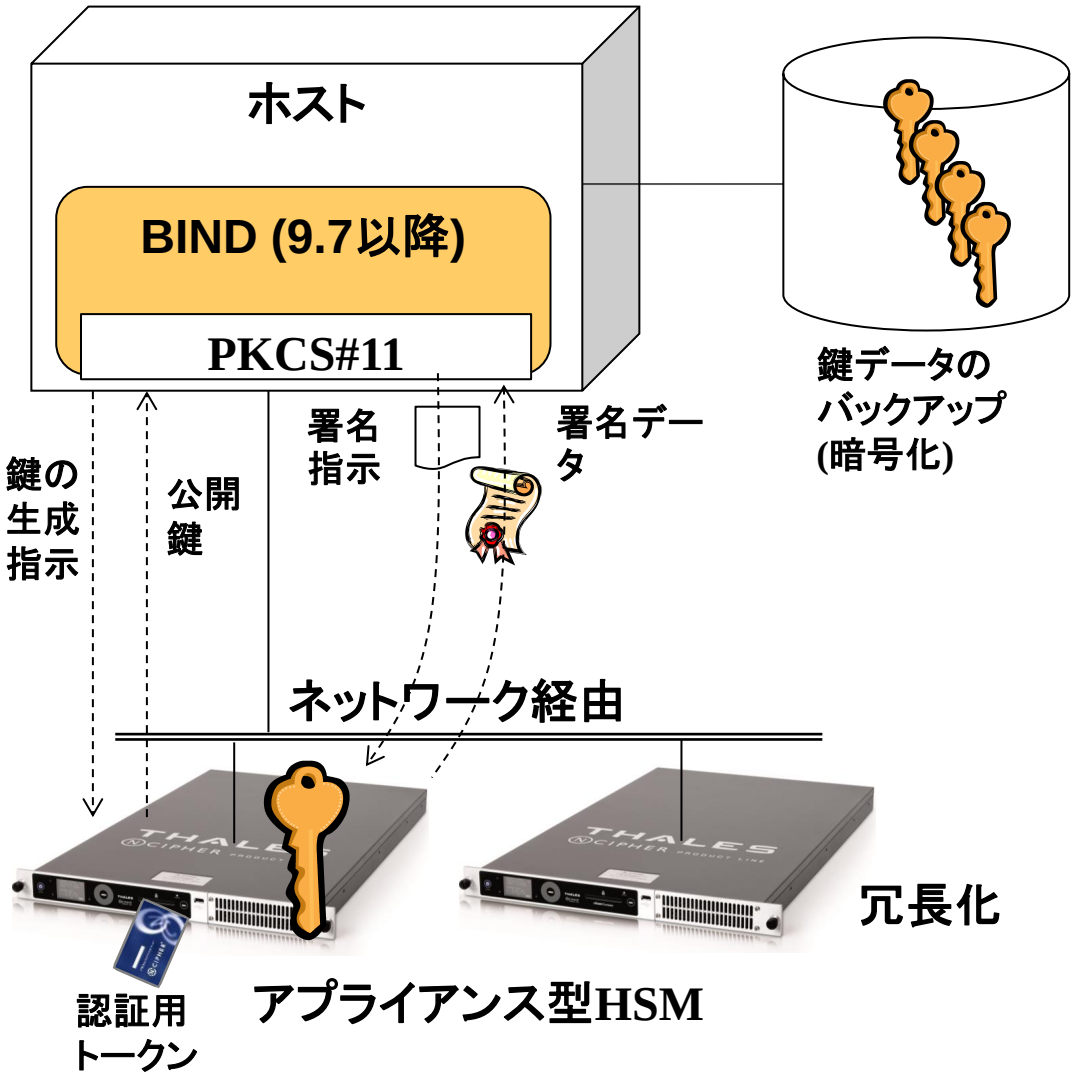
運用ポリシー／DPSとHSM

- DPS(DNSSEC Practice Statement)とは、DNSSECの運用内容を明文化し、情報公開するための文書です。
  - 「DPSとは」https://www.nic.ad.jp/ja/basics/terms/dps.html
- フレームワークが仕様化されている
  - RFC 6841 A Framework for DNSSEC Policies and DNSSEC Practice Statements
  - 4.5.2項：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

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。

HSMの使い方

HSM利用システムの構成例 (ネットワーク型の場合)

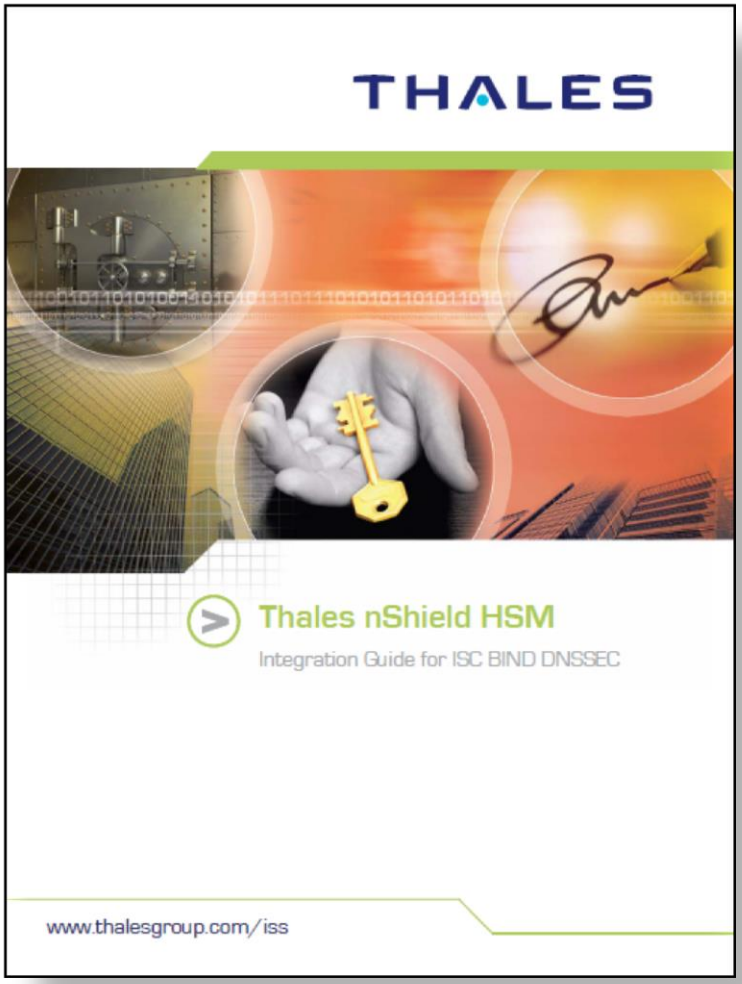


- ボード型の場合は
  ホストのPCIスロットに
  装着
  - ホストごとに1枚ずつのことが多い
  - 鍵データは共有可能
    - 製品機能に依存

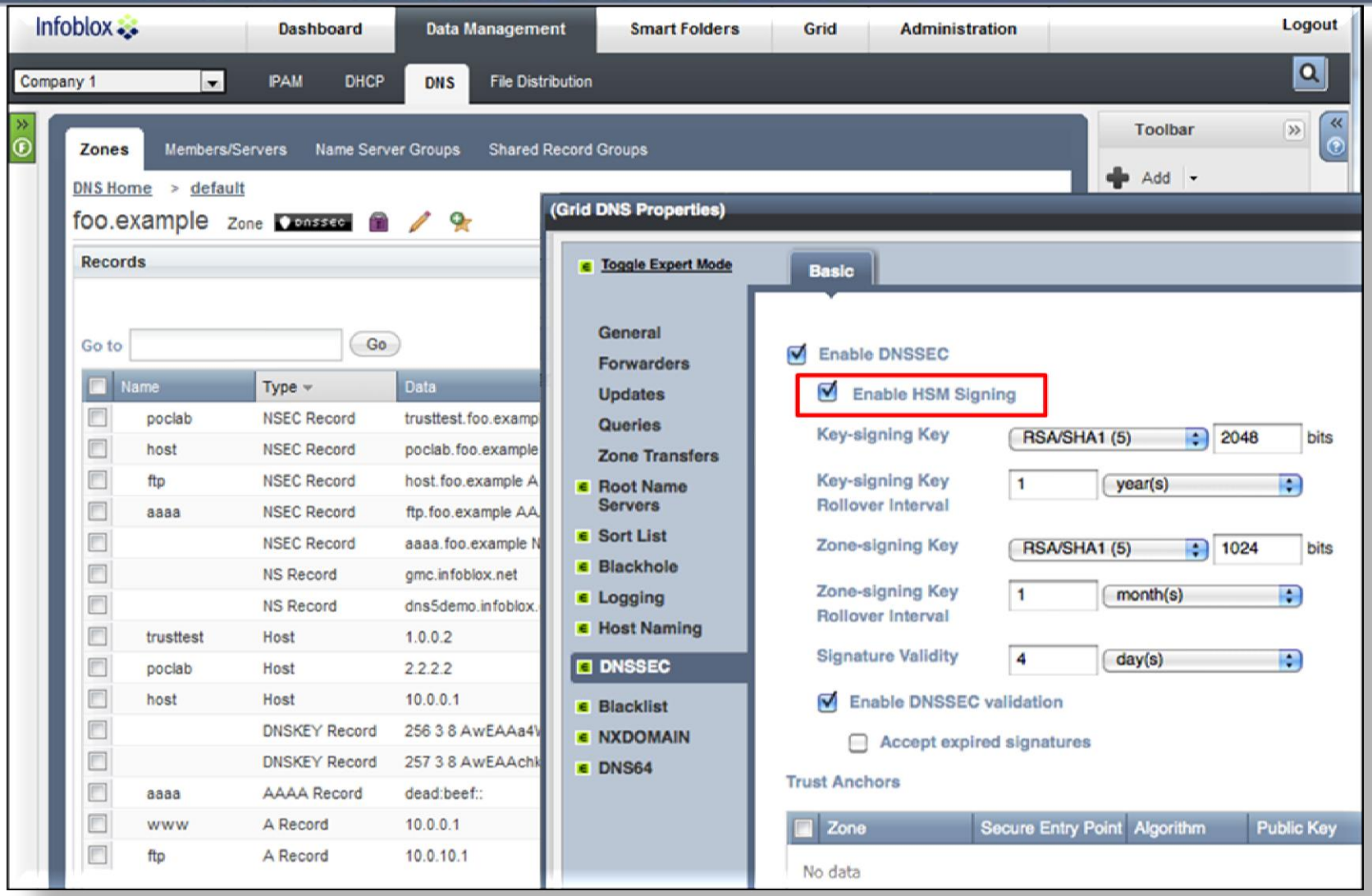
HSMの使い方

■ HSM導入の流れ

- 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 …）



HSMの使い方


Infoblox
Dashboard
Data Management
Smart Folders
Grid
Administration
Logout
Company 1
IPAM
DHCP
DNS
File Distribution
Zones
Members/Servers
Name Server Groups
Shared Record Groups
Toolbar
Add
DNS Home > default
foo.example Zone
dnssec
Records
Go to
Go
Name
Type
Data
poclab NSEC Record trusttest.foo.examp
host NSEC Record poclab.foo.example
ftp NSEC Record host.foo.example A
aaaa NSEC Record ftp.foo.example AA
NSEC Record aaaa.foo.example N
NS Record gmc.infoblox.net
NS Record dns5demo.infoblox.
trusttest Host 1.0.0.2
poclab Host 2.2.2.2
host Host 10.0.0.1
DNSKEY Record 256 3 8 AwEAAa4V
DNSKEY Record 257 3 8 AwEAAchk
aaaa AAAA Record dead:beef::
www A Record 10.0.0.1
ftp A Record 10.0.10.1
(Grid DNS Properties)
Toggle Expert Mode
Basic
General
Forwarders
Updates
Queries
Zone Transfers
Root Name Servers
Sort List
Blackhole
Logging
Host Naming
DNSSEC
Blacklist
NXDOMAIN
DNS64
Enable DNSSEC
Enable HSM Signing
Key-signing Key
RSA/SHA1 (5)
2048
bits
Key-signing Key Rollover Interval
1
year(s)
Zone-signing Key
RSA/SHA1 (5)
1024
bits
Zone-signing Key Rollover Interval
1
month(s)
Signature Validity
4
day(s)
Enable DNSSEC validation
Accept expired signatures
Trust Anchors
Zone
Secure Entry Point
Algorithm
Public Key
No data

DNSSECとHSM
HSMを利用した場合の運用

■ JP DPSの例 https://jprs.jp/doc/dnssec/jp-dps-jpn.v1.2.html

4.2.2. それぞれのタスクに必要な人員数
署名鍵運用担当者による担当タスク遂行の際は、複数人の構成とする。
KSKのアクティベーションを含むタスクを遂行する際は、これにアクティベーション立会担当者を加えた構成とする
4.2.3. 個々の役割に対する本人性確認と認証
重要設備を操作する権限は、操作を行う人員ごとに設定される。重要 設備の使用においては、操作を行う人員を認証のうえ、予め設定された操作権限が付与される。
4.2.4. 権限の分離
署名鍵運用担当者とアクティベーション立会担当者は、同一人員が任命されることはない。これにより、署名鍵運用担当者のみによるKSKのアクティベーションを不可とする。

HSMではこれらを機能として提供

- 利用時にスマートカードの認証が必要
- 定められた人数が揃わないと操作不可

■ Root ZoneのDPS https://www.iana.org/dnssec/icann-dps.txt

4.2.2. Number of persons required per task
(中略)
Tier 6: Physical access to cryptographic hardware (HSM) and activation material requires one out of two of the Safe Controller #1s, and one out of the two Safe Controller #2s in addition to the Trusted Persons required at Tier 5 and 7.
Tier 7: Activation of HSM requires three out of seven Crypto Officers.

まとめ

- **HSMは、鍵の管理をするハードウェアです**
  - HSMを使う場合、暗号鍵は外には存在しない
  - アプリケーションから呼び出して使うもの
- **HSMの利用価値**
  - 暗号鍵の保護
  - 運用の簡素化、可用性の向上
  - 処理性能の向上

HSMの要否を検討するにあたって

- 鍵が流出する恐れはないか？
  → その時に何が起こるか？
- 運用ポリシーは実際に運用可能か？
- 鍵の運用ポリシーがサービス停止を引き起こすことはないか？
- 事故時に管理体制を説明できるか？