UNIX サーバ『SPARC M10』と
THALES『nShield Solo+』
検証報告書

2015/11/10

文書名称	UNIX サーバ『SPARC M10』と THALES『inShield Solo+』			文書番号	
備　考		承　認	確　認	作　成	東京エレクトロン デバイス株式会社 CN カンパニー
			加藤	斎藤	

目次:

1. 検証趣旨 / 概要

UNIX サーバ『SPARC M10』シリーズの既存、新規ユーザー様に安心して、THALES『nShield Solo+』シリーズ(暗号鍵と暗号処理を保護する PCI Express カード型 HSM)をご使用いただくために、動作確認と性能検証を実施しました。

2. 検証

2-1. 実施日

2015 年 03 月 06 日～2015 年 03 月 19 日

2-2. 検証場所

富士通検証センター（東京・浜松町）

2-3. 検証構成

表 1：使用検証サーバスペックと OS 一覧

型番名	スペック一覧	OS
SPARC M10-1	■ハードウェア CPU:SPARC64X(2.8GHz/16 コア) メモリ:128GB(16GBx8 枚) HDD:600GBx1 本 ■ファームウェア XCP:2240 POST3.7.0 Hypervisor:1.3.2 OpenBoot:4.36.1	Solaris 0.5.11 (Oracle Solaris 11.2.7.4.0) ■制御ドメイン OS(Solaris 11.2) ホスト名：M10-1r1 CPU：8core メモリ：65GB SRU：15021 ESF：5.1 ■I/O ルートドメイン OS(Solaris 11.2) ホスト名：ldom1 メモリ：60GB ディスク：40GB SRU：15021 ESF：5.1

図 1：SPARC M10 シリーズ

表 2：検証対象 THALES 製品

製品名	フォームファクタ	インターフェース	ファームウェア Version	サポートソフトウェア
nShield 500+ F3	PCI low-profile	PCI Express 1.1 / 2.0 互換	2.51.10	11.70 for Solaris

図 2：nShield Solo+シリーズ

2-4. 検証項目概要

本検証では、基本動作確認、性能評価を実施しました。

基本動作確認は、nShield Solo+が SPARC M10 に問題なく装着出来ること、及び nShield Solo+用ドライバが正常にインストールされ、nShield Solo+がアクセス可能なデバイスとして認識されることを確認致しました。

性能評価は、代表的な暗号リズムにおいて、IO ルートドメイン / 制御ドメインの 2 項目について検証を実施致しました。

代表的な暗号リズムは、RSA、3DES、AES128/256 で、それぞれ bit 数、byte 数を変えて数パターンの性能測定を実施致しました。

1). 基本動作確認

① 装着の確認

nShield Solo+が SPARC M10 に装着出来る事

② ドライバ（モジュール）のインストール確認

nShield Solo+用ドライバが正常にインストール出来る事

③ デバイスの認識

nShield Solo+がデバイスとして正常に認識出来る事

2). 性能評価

測定環境において性能評価ツール“perfcheck コマンド”を使用して、負荷試験を実行し、処理回数、所要時間、平均時間、レイテンシ、Rate の性能測定を実施致しました。

3. 検証及び結果

3-1. 基本動作確認

装着、ドライバのインストール、デバイスの認識は問題なく実施できることを確認致しました。下記にインストールの実施結果を提示します。

pkgadd -d ./nfast.pkg

The following packages are available:

1 NCctls nCipher Core Tools (recommended)

(sparc) 2.33.7cam6

2 NChwcrhk Crypto Hardware Interface (CHIL) plugin

(sparc) 1.14.6cam598

3 NChwcrhkg CHIL patch for The GNU Privacy Guard

(sparc) 1.14.6cam598

4 NChwsp nCipher Hardware Support (mandatory)

(sparc) 2.33.7cam9

5 NCjavasp nCipher Java Support (including KeySafe)

(sparc) 2.33.7cam1

6 NCjcecsp nCipherKM JCA/JCE provider classes

(sparc) 1.24.13cam16

7 NCncsnmp nCipher SNMP monitoring agent

(sparc) 0.19.1cam71

8 NCnhfw nCipher Signed netHSM firmware files

(sparc) 2.33.7cam6

9 NCpksig nCipher PKCS#11 provider

(sparc) 1.95.1cam6

10 NCprngd Random number daemon

(sparc) 0.0.5cam39

Select package(s) you wish to process (or 'all' to process

all packages). (default: all) [?,??,q]:

Processing package instance <NChwsp> from </cdrom/secworld-solaris-user-11.70.00/solaris/2_7/nfast/nfast.pkg>

nCipher Hardware Support (mandatory)(sparc) 2.33.7cam9

nCipher Corporation Ltd

Processing package information.

Processing system information.

Verifying disk space requirements.

Checking for conflicts with packages already installed.

```
## Checking for setuid/setgid programs.
Installing nCipher Hardware Support (mandatory) as <NChwsp>
## Installing part 1 of 1.
/opt/nfast/bin/anonkneti
/opt/nfast/bin/cfg-mhsm
/opt/nfast/bin/cfg-mkdefault
/opt/nfast/bin/cfg-pushnethsm
/opt/nfast/bin/cfg-reread
/opt/nfast/bin/chkserv
/opt/nfast/bin/config-serverstartup
```

3-2. 性能評価

性能評価試験では測定環境において“perfcheck コマンド“を使用し、IO ルートドメイン / 制御ドメインの 2 項目について、以下の代表的な暗号リズムにおいて、それぞれ以下のパラメータの性能測定を実施致しました。

＜試験を実施した暗号アルゴリズム＞

・RSA 署名処理（1024bit/2048bit/2096bit）
・3DES 復号処理 / 暗号化処理（40byte/1024byte/8192byte）
・AES128 復号処理 / 暗号化処理（40byte/1024byte/8192byte）
・AES256 復号処理 / 暗号化処理（40byte/1024byte/8192byte）

1). IO ルートドメインの測定結果

RSA1024bit署名処理	
処理回数	131072
所要時間(秒)	229.33
平均時間(秒)	0.0017
レイテンシ (ms)	1.9029
Rate (signatures/s)	571.542

RSA2048bit署名処理	
処理回数	32768
所要時間(秒)	223.38
平均時間(秒)	0.0068
レイテンシ (ms)	8.8308
Rate (signatures/s)	146.6891

RSA4096bit署名処理	
処理回数	8192
所要時間(秒)	100.71
平均時間(秒)	0.0123
レイテンシ (ms)	28.8931
Rate (signatures/s)	81.342

3DES復号処理(40byte)	
処理回数	16384
所要時間(秒)	1.47
平均時間(秒)	0.0001
レイテンシ (ms)	0.1496
Rate (signatures/s)	435.2397

3DES復号処理(1024byte)	
処理回数	16384
所要時間(秒)	13.73
平均時間(秒)	0.0008
レイテンシ (ms)	1.4205
Rate (signatures/s)	1192.9657

3DES復号処理(8192byte)	
処理回数	16384
所要時間(秒)	108.38
平均時間(秒)	0.0066
レイテンシ (ms)	11.384
Rate (signatures/s)	1209.3303

AES128復号処理(40byte)

処理回数	16384
所要時間(秒)	1.26
平均時間(秒)	0.0001
レイテンシ (ms)	0.116
Rate (signatures/s)	509.682

AES128復号処理(1024byte)

処理回数	16384
所要時間(秒)	8.31
平均時間(秒)	0.0005
レイテンシ (ms)	0.841
Rate (signatures/s)	1972.4153

AES128復号処理(8192byte)

処理回数	16384
所要時間(秒)	65.58
平均時間(秒)	0.004
レイテンシ (ms)	6.4143
Rate (signatures/s)	1998.728

AES256復号処理(40byte)

処理回数	16384
所要時間(秒)	1.35
平均時間(秒)	0.0001
レイテンシ (ms)	0.1126
Rate (signatures/s)	474.0705

AES256復号処理(1024byte)

処理回数	16384
所要時間(秒)	8.33
平均時間(秒)	0.005
レイテンシ (ms)	0.8284
Rate (signatures/s)	1967.3892

AES256復号処理(8192byte)

処理回数	16384
所要時間(秒)	64.27
平均時間(秒)	0.0039
レイテンシ (ms)	6.6131
Rate (signatures/s)	2039.4262

3DES暗号化処理(40byte)

処理回数	16384
所要時間(秒)	1.49
平均時間(秒)	0.0001
レイテンシ (ms)	0.1417
Rate (signatures/s)	430.8934

3DES暗号化処理(1024byte)

処理回数	16384
所要時間(秒)	13.67
平均時間(秒)	0.0008
レイテンシ (ms)	1.4515
Rate (signatures/s)	1198.4499

3DES暗号化処理(8192byte)

処理回数	16384
所要時間(秒)	108.22
平均時間(秒)	0.0066
レイテンシ (ms)	11.3533
Rate (signatures/s)	1211.1136

AES128暗号化処理(40byte)

処理回数	16384
所要時間(秒)	1.28
平均時間(秒)	0.0001
レイテンシ (ms)	0.1145
Rate (signatures/s)	501.8825

AES128暗号化処理(1024byte)

処理回数	16384
所要時間(秒)	8.31
平均時間(秒)	0.0005
レイテンシ (ms)	0.903
Rate (signatures/s)	1971.9367

AES128暗号化処理(8192byte)

処理回数	16384
所要時間(秒)	65.31
平均時間(秒)	0.004
レイテンシ (ms)	6.9706
Rate (signatures/s)	2006.8498

AES256暗号化処理(40byte)

処理回数	16384
所要時間(秒)	1.36
平均時間(秒)	0.0001
レイテンシ (ms)	0.1376
Rate (signatures/s)	471.7593

AES256暗号化処理(1024byte)

処理回数	16384
所要時間(秒)	8.33
平均時間(秒)	0.0005
レイテンシ (ms)	0.8565
Rate (signatures/s)	1967.7127

AES256暗号化処理(8192byte)

処理回数	16384
所要時間(秒)	64.98
平均時間(秒)	0.004
レイテンシ (ms)	6.6371
Rate (signatures/s)	2017.2261

2). 制御ドメインの測定結果

RSA1024bit署名処理	
処理回数	131072
所要時間(秒)	228.88
平均時間(秒)	0.0017
レイテンシ (ms)	1.9357
Rate (signatures/s)	572.6652

RSA2048bit署名処理	
処理回数	32768
所要時間(秒)	223.38
平均時間(秒)	0.0068
レイテンシ (ms)	8.763
Rate (signatures/s)	146.6902

RSA4096bit署名処理	
処理回数	8192
所要時間(秒)	100.75
平均時間(秒)	0.0123
レイテンシ (ms)	28.9652
Rate (signatures/s)	81.3103

3DES復号処理(40byte)	
処理回数	16384
所要時間(秒)	1.46
平均時間(秒)	0.0001
レイテンシ (ms)	0.1456
Rate (signatures/s)	437.1435

3DES復号処理(1024byte)	
処理回数	16384
所要時間(秒)	13.72
平均時間(秒)	0.0008
レイテンシ (ms)	1.3905
Rate (signatures/s)	1193.7937

3DES復号処理(8192byte)	
処理回数	16384
所要時間(秒)	108.7
平均時間(秒)	0.0066
レイテンシ (ms)	11.3852
Rate (signatures/s)	1205.8024

AES128復号処理(40byte)	
処理回数	16384
所要時間(秒)	1.24
平均時間(秒)	0.0001
レイテンシ (ms)	0.1175
Rate (signatures/s)	514.7074

AES128復号処理(1024byte)	
処理回数	16384
所要時間(秒)	8.29
平均時間(秒)	0.0005
レイテンシ (ms)	0.8384
Rate (signatures/s)	1976.1771

AES128復号処理(8192byte)	
処理回数	16384
所要時間(秒)	64.18
平均時間(秒)	0.0039
レイテンシ (ms)	6.3221
Rate (signatures/s)	20142.3124

AES256復号処理(40byte)	
処理回数	16384
所要時間(秒)	1.34
平均時間(秒)	0.0001
レイテンシ (ms)	0.1206
Rate (signatures/s)	476.6171

AES256復号処理(1024byte)	
処理回数	16384
所要時間(秒)	8.32
平均時間(秒)	0.0005
レイテンシ (ms)	0.8511
Rate (signatures/s)	1969.7867

AES256復号処理(8192byte)	
処理回数	16384
所要時間(秒)	64.55
平均時間(秒)	0.0039
レイテンシ (ms)	6.597
Rate (signatures/s)	2030.4948

3DES暗号化処理(40byte)	
処理回数	16384
所要時間(秒)	1.47
平均時間(秒)	0.0001
レイテンシ (ms)	0.1447
Rate (signatures/s)	436.0279

3DES暗号化処理(1024byte)	
処理回数	16384
所要時間(秒)	13.67
平均時間(秒)	0.0008
レイテンシ (ms)	1.387
Rate (signatures/s)	1198.6231

3DES暗号化処理(8192byte)	
処理回数	16384
所要時間(秒)	108.97
平均時間(秒)	0.0067
レイテンシ (ms)	11.4187
Rate (signatures/s)	1202.8204

AES128暗号化処理(40byte)	
処理回数	16384
所要時間(秒)	1.28
平均時間(秒)	0.0001
レイテンシ (ms)	0.1194
Rate (signatures/s)	501.1456

AES128暗号化処理(1024byte)	
処理回数	16384
所要時間(秒)	8.29
平均時間(秒)	0.0005
レイテンシ (ms)	0.8984
Rate (signatures/s)	1976.0908

AES128暗号化処理(8192byte)	
処理回数	16384
所要時間(秒)	64.42
平均時間(秒)	0.0039
レイテンシ (ms)	6.5882
Rate (signatures/s)	2034.5513

AES256暗号化処理(40byte)	
処理回数	16384
所要時間(秒)	1.35
平均時間(秒)	0.0001
レイテンシ(ms)	0.1166
Rate (signatures/s)	473.0642

AES256暗号化処理(1024byte)	
処理回数	16384
所要時間(秒)	8.31
平均時間(秒)	0.0005
レイテンシ(ms)	0.8511
Rate (signatures/s)	1971.3393

AES256暗号化処理(8192byte)	
処理回数	16384
所要時間(秒)	65.39
平均時間(秒)	0.004
レイテンシ(ms)	6.6633
Rate (signatures/s)	2004.3146

4. 検証まとめ

今回の基本動作検証、性能評価検証の結果により、UNIX サーバ『SPARC M10』シリーズをお使い頂くお客様に THALES『nShield Solo+』をご利用頂けることを示せたと思います。

ただし、THALES 社としては『nShield Solo+』を仮想 OS 上で利用いただくことについて動作保証をしておりません。導入をご検討いただける際は、事前に仮想 OS 環境で動作確認を実施されることをお勧め致します。また、下記のお問い合わせ先まで必ずご相談をいただくようお願い致します。

THALES『nShield Solo+』は、デジタル証明書の発行にも使用される署名用秘密鍵や、PKI サーバアプリケーションのトランザクションにおいて最先端のスピード、セキュリティ、スケーラビリティと管理性を提供する HSM(ハードウェア・セキュリティ・モジュール / FIPS 140-2 レベル 3 認定 HSM)。です。高性能な暗号処理機能を提供すると同時に、暗号鍵およびアプリケーションを保護します。

THALES『nShield Solo+』は、サーバのカードスロットに装着する HSM です。暗号鍵を安全で耐タンパー性ハードウェアの環境で保護し、サーバ上のアプリケーションから呼び出す形で使用し、暗号化と電子署名などの暗号処理機能を提供します。 カードスロットは、PCI Express をサポートしています。

THALES 社の nShield シリーズの詳細については、別資料『THALES（タレス）紹介資料』をご確認ください。

本製品と UNIX サーバ『SPARC M10』シリーズを併せてご利用頂くことで、より多くのお客様環境に HSM による鍵管理の環境を提供できることを願っております。

5. お問い合わせ先

東京エレクトロン デバイス株式会社
CN カンパニー CN 第一営業本部 パートナー第一営業部 (担当：斎藤 隆之)
TEL：03-5908-1962
E-mail: nctech@teldevice.co.jp
URL: http://cn.teldevice.co.jp/product/detail/nshield_solo