JNSA 電子署名 スキルアップTF
JIPDEC あんしんかんCafe

IT製品の調達における セキュリティ要件リストに関する 認定制度の勉強会

2014.09.29

JNSA 電子署名WG
WGメンバ　小川

IT製品の政府調達リストを改訂

- 「ITセキュリティ評価及び認証制度等に基づく認証取得製品分野リスト」が

- 「IT製品の調達におけるセキュリティ要件リスト」になった。

- 経済産業省ではパブコメも実施した。

- 独立行政法人情報処理推進機構（IPA）では利用ガイドラインを作成した。

政府調達リストは利用されているか？

- 要件リストは、政府調達だけでなく、民間企業や組織においても、IT製品調達する際に想定される脅威に対抗できる製品の調達に活用することができる。
- でも、国内民間企業で利用されていますか？

この勉強会の趣旨

- この勉強会では、①要件リストと②参照している認定制度の動向を理解し、

- セキュリティベンダやユーザが疑問に思っていることや課題、問題意識について議論します。
（②は以下の制度）

  - CC（JICEC）

  - JCMVP/CMVP

リストの対象製品分野

対象とする製品分野を拡充していきます

IPA

対象製品分野	製品分野定義
デジタル複合機（MFP）	プリント機能を有し、さらに、スキャン、FAX、コピー機能のうちいずれか２つ以上の機能を装備している製品
ファイアウォール	インターネットと内部ネットワークの境界に配置され、パケットの内容と事前に定義されたルールに基づきパケット通過を制御する製品
不正侵入検知/防止システム（IDS/IPS）	ネットワークやシステムの稼動状況を監視し、組織内のコンピューターネットワークへの外部からの侵入を報告、防御する製品
OS(サーバOS に限る)	コンピュータのハードウェア制御・操作のために用いられる基本ソフトウェア
データベース管理システム（DBMS）	共有データとしてのデータベースを管理し、データに対するアクセス要求に応える製品
スマートカード（IC カード）	プラスチック製カード等に IC チップを埋め込み、情報を記録できるようにした製品

対象候補	製品分野定義
USB メモリ	製品自体に USB コネクタを備えており、別途 USB 接続ケーブル等を用いる必要がない、フラッシュメモリを内蔵した持ち運び可能な記憶装置

まずは6つの
製品分野を対象
（今後拡充予定）

セキュリティへの需要がありつつも、市場に要件を満たす製品、ISO/IEC15408認証取得製品が揃っていない分野は「対象候補」と位置付け。
状況を検討し、「対象製品分野」に移行していく。
（今後拡充予定）

政府調達での本制度の活動について
http://www.ipa.go.jp/security/jisec/seminar/documents/cc_semi_20140728_2.pdf

CCとJCMVPの活用

IT製品の調達におけるセキュリティ要件リスト

IPA

製品分野名	デジタル複合機（MFP）

セキュリティ上の脅威	① 他の利用者による不正な操作 各利用者が複合機を操作するにあたり、取り扱う文書データに適切な保護（データアクセス権、各種操作の制御等）を行うことができなければ、蓄積される文書及び文書関連データの漏えい、情報の改ざんなどが発生する。
	② 通信データの盗聴、改ざん 複合機を利用（プリント、スキャン等）するために使用するPCやファイルサーバと複合機の間でやりとりされるネットワーク上の通信データが盗聴、改ざんされる可能性がある。
	③ 管理機能への不正なアクセス 取り扱う文書データに対する設定された規則（セキュリティポリシー）や複合機の利用者情報を管理する機能等に対して、操作できる者を適切に識別認証できない場合には、不正に操作される可能性がある。
	④ 複合機のソフトウェアの改ざん・破損 複合機のソフトウェアが改ざん・破損された場合、設定されたセキュリティポリシーが適切に実施されない可能性がある。
	⑤ 監査ログの改ざん・不正な削除 不正行為の発生を追跡するために取得した監査ログが保護されていない場合には、改ざん・削除される可能性がある。その結果、不正行為が発生しても検出することができない。
	⑥ 複合機内に保存された文書データの漏えい（リース終了返却、または廃棄処理時） プリントやコピー、FAX機能で扱われる文書データは、複合機のHDD/SSD等の記憶媒体に一時的または継続的に保存される場合があり、リース終了返却、または廃棄処理となった複合機から、それらの文書データが漏えいする可能性がある。これらの文書データは、物理的に消去されていない場合、表面的にはアクセスできないようになっていても復元される可能性がある。

国際標準に基づくセキュリティ要件	対抗できる脅威
[1]：IEEE Std 2600.1™-2009,Protection Profile for Hardcopy Devices,Operational Environment A Version 1.0 [3] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③ ④, ⑤, ⑥
[2]：U.S. Government Approved Protection Profile - U.S. Government Protection Profile for Hardcopy Devices Version 1.0 (IEEE Std. 2600.2™-2009) [4] （ISO/IEC15408(Common Criteria)に基づいたセキュリティ要求仕様）	①, ②, ③ ④, ⑤, ⑥

- 製品分野特有の「セキュリティ上の脅威」を列挙
  - ➢ 何が保護資産なのか？
  - ➢ 保護資産に対する脅威は何か？
  - ➢ 考慮すべき脅威のベースライン

- 上記脅威に対抗できる「国際標準に基づくセキュリティ要件」を提示
  - ➢ ISO/IEC15408（Common Criteria)に基づいたセキュリティ要求仕様
  - ➢ ISO/IEC19790(暗号モジュール対するセキュリティ要求事項)も活用

政府調達での本制度の活動について
http://www.ipa.go.jp/security/jisec/seminar/documents/cc_semi_20140728_2.pdf

CCの問題点（cPPの資料から）

1．イントロ

これまでのCC評価での問題点

IPA

- 各国独自のPPによる重複した評価
  - 同じ製品分野で各国から異なるPP（セキュリティ要件）が作成されたため、一つの製品についてそれぞれのPPに適合sる評価が求められる
- 評価機関・評価者による評価品質のバラツキ
  - CEM（評価方法）は、さまざまな製品に対応するため、抽象的な記述となっており、技術分野に対応した具体的な評価方法がないため、加盟国間・評価機関間で評価品質の均一性を維持することが困難であった
- PP適合でないベンダー独自仕様（ST）に基づく認証製品
  - その製品本来のセキュリティ機能が評価対象から外されていたり、実現不可能な前提条件や運用環境、組織のセキュリティ方針などをもとに評価されることがあり、調達対象として活用できない認証製品があった
- EAL4等の評価では、評価コスト・期間がかかり過ぎる
  - 評価に18か月程度かかることがあり、新製品をタイムリーに調達できない
  - 製品ベンダーにとって、販売機会を逸することがあった

今後はJCMVPと混在する

CCRA/ICCC 2013報告
http://www.ipa.go.jp/security/jisec/seminar/documents/CCRAReport_20131114.pdf

本日のタイムテーブル

1	勉強会趣旨	JNSA 電子署名WGメンバ 小川	16:00 - 16:15 (15分)
2	要件リストとCCの動向	IPA 情報セキュリティ認証室 中村様	16:15 - 16:55 (40分)
3	JCMVPの動向	IPA 情報セキュリティ認証室 櫻井様	16:55 - 17:15 (20分)
4	ベンダ視点	日本セーフネット（株） 亀田様	17:15 - 17:30 (15分)
5	ベンダ視点	ジェムアルト 相原様	17:30 - 17:45 (15分)
6	ディスカッション＆QA	会場参加者	17:45 - 18:00 (15分)

※本日のお約束

- 念のためTweetなしで。
- 資料は、後日公開しますが、それなりの内容に加工される予定です。（笑）
- 懇親会参加者は、参加費を小川かJIPDECの佐藤さんに申し出てください。

ここからは私見

1. CC認証取得製品とCMVP認証取得製品は少ない。

2. OSやプロトコルスタックに入っている暗号コアなどは
   認証取得されているかわからない。

3. バージョンアップした製品が、保証継続されているか？
   新たに認証取得したのか？は、わからない。

4. ベンダーの自社評価（独自評価）の程度や深さはわからない。

5. 調達者は、調達の都度、上記の１～５を個々に調査している。

事例：一般のユーザーは理解できるだろうか？

Store | Mac | iPod | iPhone | iPad | iTunes | Support

OS X：セキュリティの認定と検証

言語 日本語

この記事には、主要製品の認定、暗号の検証、および OS X プラットフォームに対するセキュリティガイダンスに関するリンクが含まれています。

次のトピックをクリックして、詳細情報を確認してください。

- Common Criteria の認定
- FIPS 140-2 適合性検証

Volatility Statements

製品のメーカーから Volatility Statements を提供される必要がある政府組織およびその関連機関は、メールで AppleFederal@apple.com までご依頼いただければ入手可能です。その際、ご依頼の政府機関名、Apple 製品名、製品のシリアル番号、および政府の技術ご担当者名を記載してください。

独自に確認

Common Criteria Certification

Common Criteria は、国際的に承認されている一連のセキュリティ規格であり、IT 製品のセキュリティ機能に対して明確で信頼性の高い評価を提供しています。製品がセキュリティ規格 Common Criteria Certification を満たしていることを独自に査定することによって、お客様に IT 製品を安心してお使いいただき、十分な情報に基づいて判断していただけるようにしております。

Common Criteria Recognition Arrangement (CCRA) には、26 カ国が加盟し、同じレベルの信頼性で IT 製品の認定を承認することに賛同しています。

OS X：セキュリティの認定と検証
http://support.apple.com/kb/HT5588?viewlocale=ja_JP

事例：一般のユーザーは理解できるだろうか？

暗号モジュール評価

すべての Apple FIPS 140-2 適合性検証証明書は、CMVP Vendor ページ (http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401vend.htm) にあります。

OS X Mavericks v10.9

- 証明書 #2015 - Apple OS X CoreCrypto モジュール v4.0
  - 証明書 - http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#2015
  - セキュリティポリシー - http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2015.pdf
- 証明書 #1956 - Apple OS X CoreCrypto カーネルモジュール v4.0
  - 証明書 - http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#2016
  - セキュリティポリシー - http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp2016.pdf

関連記事：

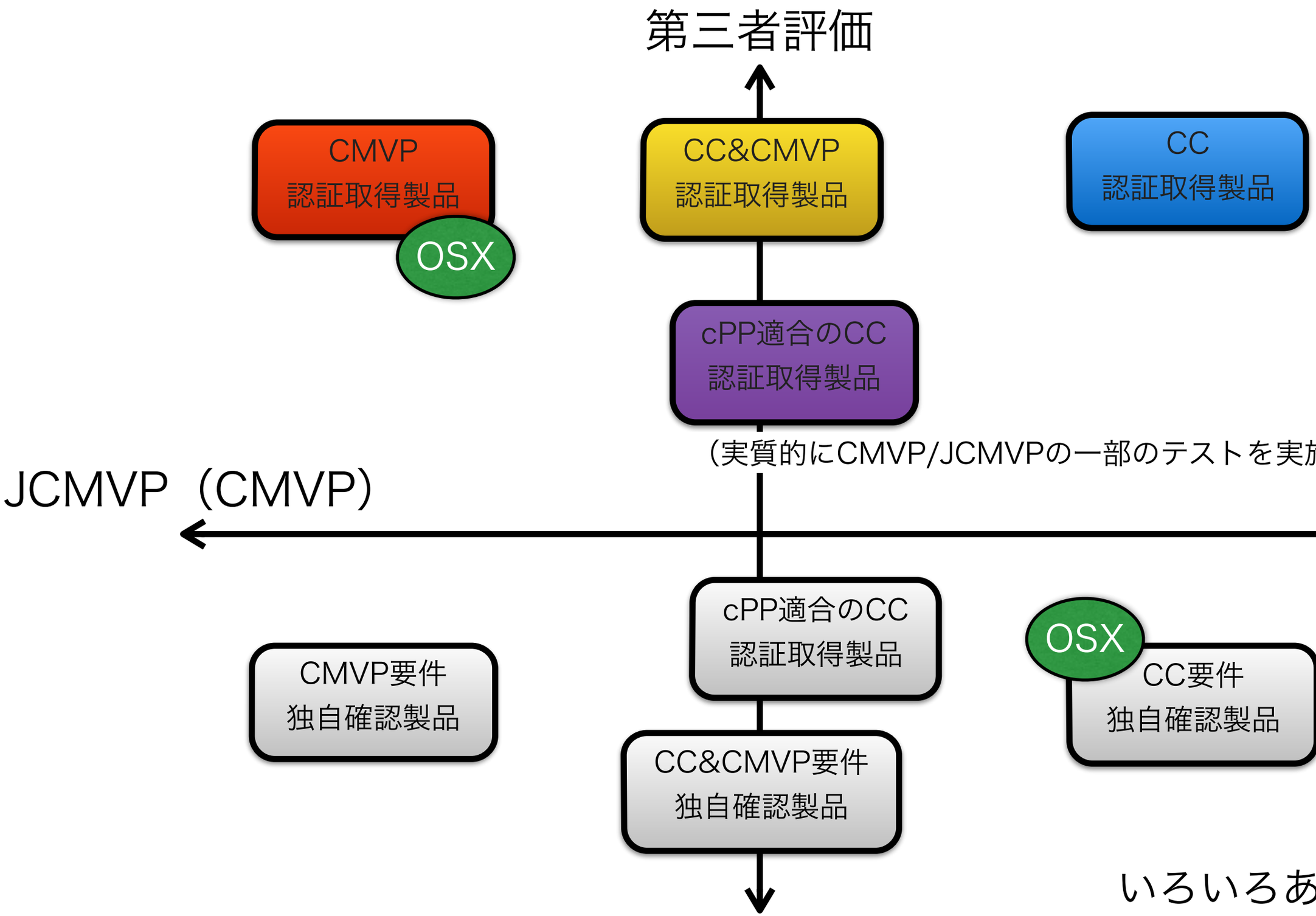
- OS X Mavericks：Apple OS X FIPS 暗号モジュール v4.0

OS X Mountain Lion v10.8

- 証明書 #1964 - Apple OS X CoreCrypto モジュール v3.0
  - 証明書 - http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#1964
  - セキュリティポリシー - http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1964.pdf
- 証明書 #1956 - Apple OS X CoreCrypto カーネルモジュール v3.0
  - 証明書 - http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/1401val2013.htm#1956
  - セキュリティポリシー - http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140sp/140sp1956.pdf

OS X：セキュリティの認定と検証
http://support.apple.com/kb/HT5588?viewlocale=ja_JP

整理してみましょう



いろいろありすぎて
わからない..

セキュリティ要件リストの利用を推進するために

- CCの情報、CMVPの情報が少ない。
  cPPの情報はさらに少ない。

- 第三者認証とベンダー独自評価の違いを説明する資料が不足している。

- 調達者が個々に調べた結果を共有するスキームも必要ではないか？