セキュリティ関連OSS の成熟度評価Ver1.0, 日本ＯＳＳ推進フォーラム サーバ部会セキュリティＴＦ, 平成20 年3 月

大分類	小項目	製品例	OSSの有無	該当するOSS	OSSの利用状況	OSSが利用されていない場合の阻害要因							OSSが存在し無い場合の阻害要因						推奨度
						サポート	信頼性	性能	機能	日本語対応	その他	コメント	マーケットサイズ	特許	法律	標準化	ベンダーが非協力	コメント	
ネットワーク																			
	不審な通信の検出、排除																		
	セキュリティ監査	ISS Internet Scanner	あり	Nessus, nmap, RNA	○-たまに利用される	レ	レ		レ	レ		・検出された結果の信頼性の問題 ・日本語によるレポーティング機能が無い							4
	IDS	ISS Real Secure Network Sensor, Enterasys Dragon Sensor	あり	Snort, prelude	◎-よく利用されている				レ	レ		・日本語によるレポーティング機能が無い ・商用製品では、公表されていないが エンジン部分がSnortのものがある							8
	IPS	ISS Proventia Network IPS,CheckPoint IPS 1, 3Com Tipping Point	なし		×-利用されていない							処理速度が重視される場合には、ハードウェア込みのApplianceが多い。性能限界で使える環境が限定される	レ						3
	ファイヤーウォール				◎-よく利用されている														10
	ネットワークFW	Firewall-1（チェックポイント）	あり	NetFilter + Iptables	◎-よく利用されている														10
	WebアプリFW	NetContinuum、Citrix web application firewall	あり	mod_security, guardian@janperz.net	△-あまり利用されていない			レ											5
	検閲																		
	不正PCの検知	Cisco NAC、MS NAP、TCG TNC, Windows 2003 Server	なし		×-利用されていない	レ			レ			市販製品もあまり多く利用されていない。ハードと抱き合わせのものも多くOSSの場合は、ソフトウェアだけになるのでやや不利か？							2
	通信の暗号化																		
	VPN	沢山ある　CheckPoint VPN1, Cisco, Netscreen他	あり	OpenVPN	×-利用されていない	レ		レ				処理速度が重視される場合には、ハードウェア込みのApplianceが多い。性能限界で使える環境が限定される							2
	その他				◎-よく利用されている														
	認証	A10 Networks ID Series, CA Identity Manager	あり	OpenSAML	△-あまり利用されていない														6
	PKI	沢山ある, F5 Big-IP, Entrust Authority etc.	あり	OpenSourcePKI(NSS,JSS,PSM)	◎-よく利用されている														10
	電子署名、電子証明書	沢山ある, NEC SecureWare, VeriSign Trusted Messaging	あり	GPG, OpenSSL	◎-よく利用されている														10
	ICカード	多数存在	？	Linuxに対応するR/Wは幾つか存在、SDK for Felica <Reference Code 2.0>のようなLinuxで使える開発ツールも存在、Linuxを使った組込み機器も存在	△-あまり利用されていない							一部アクセスできるだけ。 開発環境を買わないと、ドライバやライブラリが手に入らない。	レ	レ	レ	レ	レ	特許・法律は影響あまり無し	2
	生体情報	静紋、指紋認証機器	？	指紋認証のUSB系では使えるものもある。株式会社応用電子の「FKEY」は、組込みLinuxで利用している。	△-あまり利用されていない							機器内部で認証しないものは、ソフトが対応していないとダメ(静紋) 機器内部で認証するものは、ドライバの対応状況でまちまち。	レ	レ	レ	レ	レ	特許・法律は影響あまり無し	2
	認証連携(OpenID)	http://openid.net/	ある	ライブラリ Apacheライセンス															
	シングルサインオン	Microsoft Passport、 CA Single Sign-On、HP IceWall SSOなど多数	あり	OpenSSO	○-たまに利用される			レ	レ			・SUNが主導するOSS ・製品（Sun Java System Access Manager） のSSO部分を公開 ・SSOのコアのみ							6
				JOSSO (Java Open Single Sign-On)	×-利用されていない	レ		レ				・サイト行方不明 ・The BSD Licenseの元で公開							2
				CAS(Central Authentication Service)	◎-よく利用されている			レ				・http://www.ja-sig.org/products/cas/ ・多くの利用実績（大学が多い） ・名古屋大学で拡張したCAS-2							9
				opentrust-pam	△-あまり利用されていない	レ	レ	レ		レ		・http://opentrust-pam.sourceforge.net/ ・OpenSUSEで利用可能 ・日本語対応は無し。そもそもフランス語が多い							2
	通信ログの収集	HP OpenView、日立JP1/Cm2	あり	WireShark(ethreal)	◎-よく利用されている														10
サーバ																			1
	認証	SoftEther CA RSA Authentication Manager	あり	OpenLDAP,FreeRADIUS,PAM	◎-よく利用されている							認証システムの中のパーツとしては利用が拡大しつつあるが、認証方式の特許に関わる問題、統合管理機能(MSのADなど）の不足、ドキュメントの不足等の現状が考えられる。							10
	アクセス制御																		
	MAC		あり	SELinux, TOMOYO Linux, AppArmor	△-あまり利用されていない	レ			レ			管理系が弱い。商用サポートが少ない。利用が難しい。既存の管理者が扱えない。特に遠隔集中管理に難がある。							4
	脆弱性監査ツール	ISS Internet Scanner	あり	Nessus(2.*),	◎-よく利用されている							検出エンジン等に対して信頼性の問題はある（どこまで網羅的に実施してくれるのか不安）が、一定の検査は実施してくれる点からよく使われている。							10
	暗号化	多数存在	あり	OpenSSL, OpenSSH	◎-よく利用されている														10
	ファイルシステム	MS EFS	あり	ecryptfs, TrueCrypt	△-あまり利用されていない	レ	レ		レ										3
	URLフィルター	Synaptive LYRIS Mailshield Server、BlueQuartz	あり	dansguardian, ufdbguard, squidguard	△-あまり利用されていない					レ		知名度がない。そもそも使われない。							0
	メールフィルター	多数存在	あり	spamassassin	○-たまに利用される					レ		Windowsですでに安い製品が多数出ている。							7
	メール監査	Synaptive LYRIS Mailshield Server, GUARDIANWALL	あり	SquidGuard, UFDBGuard, DANSGuadian	△-あまり利用されていない	レ	レ	レ	レ	レ		・日本語コミュニティが少ない ・障害発生時の復旧方法にはアプリケーション以外にOSの運用知識が必要となる。 アプリケーション単体で二重化やバックアップをサポートしているものは少ない。 ・規模に応じて負荷分散等のカスタマイズが必要になるが、公開されている情報は少ない。 カスタマイズにはアプリケーション単体の知識ではなくOS及びネットワークに関する知識が必要となる。 ・ターゲットとなるメールを検索できる機能。個々のアプリケーションについては完成度は十分な領域に達しているため、成熟度は高いと言える。 しかし全ての機能を盛り込み総合的な管理が可能なアプリケーションは商用製品以外に無いため、その分野での成熟度は低い。 ・業務停止に関わるミッションクリティカルな要件には「保障」に関する問題が発生する							1
	改ざん検知																		1
	ファイル	TripWire製品版	あり	TripWire、AIDE、Osiris	○-たまに利用される														8
	ログファイル		あり	chkrootkit	△-あまり利用されていない	レ			レ			運用で対応（例、ログの集中管理）							4
	ファームウェア、OS自体	MS BitLocker™, Safeboot	あり	TrustedGrub、Grub-IMA	×-利用されていない	レ	レ	レ	レ			・大手ディストロで非サポート ・実績が少ない ・若干性能低下(起動時間の増加) ・標準化が不十分 ・SWの完全性をHWで保護						特許：TCG参加企業はRANDで利用可能	0
	ログ管理																		
	クライアントログ管理		なし	-	×-利用されていない								レ						3
	サーバログ管理	File Server Audit(NSD)	あり	SNARE - Auditing and EventLog Managem	△-あまり利用されていない		レ	レ	レ			業務システムなどで利用されるためにはTivoliなどとの連携機能などが必要							3
	ログ解析	LogWeb	あり	Logzer Web Log Analyzer	△-あまり利用されていない			レ	レ	レ		対応できるログフォーマットが少ない。レポーティングが顧客提出可能なほど品質が高くない。							3
		Logstorage（インフォサイエンス）		Webstats															1
																			1
																			1
	ウィルス対策（サーバ・クライアント）	AVG, Avira antivir, F-Secureアンチウィルス, ServerProtext for Linux	あり	ClamAV	○-たまに利用される	レ			レ			アンチウィルスは、サポート（パターン更新）が最重要だが、信頼性に問題。Linuxサーバの1/3はウィルス対策ソフトを入れていない。安全だと思われている。振る舞いなどによるウィルスチェック、リアルタイム検出などの機能が弱い。集中管理機能がない。							6
	情報漏洩防止																		
	ドキュメント管理(IRM)	Office Professional Edition 2003 (MS)	なし	セキュアOSが多少近いがOSSにはあまりない。セキュアOSでは機密レベルだけであるが、それに応じてさまざまな制御ができる必要あり。	×-利用されていない							デファクトなOffice スイーツがないためではないか？ OpenOfficeにこうした機能があるのか？		レ					3
		LeakProof（日立）																	1
		秘文（日立ソフト）																	1
		セキュリティプラットフォーム（ハミングヘッズ）																	1
クライアント																			
	認証																		
	スマート・カード/USBトークン		あり	pam_usb	×-利用されていない														4
	ワンタイム・パスワード		あり	otp	×-利用されていない														4
	バイオメトリクス認証				×-利用されていない														4
	セキュリティ・チップ(TCG/TPM)		なし		×-利用されていない														4
	情報漏洩防止																		
	外部デバイス制御	Windows VISTA (MS)	あり	USB System Lock	△-あまり利用されていない							Linuxを対象としたものはクライアントLinuxの浸透に応じて利用拡大か？							6
		eX WP(Quality Corporation)																	1
		Portshutter(富士通)																	1