

セキュリティ関連OSSの成熟度評価

Ver 1.0

2008年3月21日

日本OSS推進フォーラム

サーバ部会 セキュリティTF

<http://www.ipa.go.jp/software/open/forum/>

目次

1. はじめに	3
1.1 本資料の目的.....	3
1.2 対象読者.....	3
1.3 本資料で明らかにすること.....	3
1.4 本資料の改版方針.....	4
2.1 セキュリティ情報のカテゴライズ.....	4
2.2 調査範囲.....	4
2.3 表の見方.....	4
2.4 推奨度の計算方法.....	5
3. 結果の概要	6
3.1 推奨度の結果.....	6

1. はじめに

1.1 本資料の目的

オープンソースソフトウェア(OSS) の利用は急速に拡大している。

従来から利用されてきたUNIX やWindows、あるいは、Oracle のような商用ソフトウェアと異なり、OSS は、プラットフォームベンダ、システムインテグレータ(Sier)、ディストリビュータ、独立ソフトウェアベンダ(ISV)等がそれぞれのハードウェア(HW)、ミドルウェア(MW)、サービスとの組み合わせにおいて、高い自由度で利用できることに特色がある。

近年個人情報漏洩や機密情報漏洩事件、侵入攻撃による Web 改ざんなど事件が数多く報道されている。また、個人情報保護法やいわゆる日本版 J-SOX 法の施行により、セキュリティに関連する製品やソリューションに注目が集まっている。

そのようなセキュリティ製品に関しても OSS に関連した HW 製品・MW 製品・サービス等が多数存在するが、特定ベンダによる一元的な商用ソフトウェアに比べて、ベンダの提供する情報に凸凹があるために、利用者がいろいろなベンダの製品・サービスを比較検討する際に OSS に関連した製品を検討対象の俎上に載せる事への障害となることもある。

本資料は、情報システム分野におけるセキュリティ上の課題と、それに対応する商用ソフトウェア及び OSS ソフトウェアを対応付ける事により、商用製品と OSS ソフトウェアでそれぞれカバーしている範囲を明確化するためのものである。これにより、利用者は商用製品と OSS に関連した製品のそれぞれを互いに補間し合うように利用して行き、より効果的にセキュリティ製品の導入を推進していくことが可能となる。

1.2 対象読者

本資料は、開発者側ではなく、セキュリティ製品の導入を検討しているエンドユーザ、及びそれらユーザに対してサービスの提供を実施するシステムインテグレータ(Sier)といったユーザ側を対象としている。

1.3 本資料で明らかにすること

本資料では、情報システム分野におけるセキュリティ上の課題と、それに対応する商用ソフトウェア及び OSS ソフトウェアを対応付ける事により、商用製品と OSS ソフトウェアでそれぞれカバーしている範囲を明確化する。

なお、本評価は、あくまでも本 TF 内で評価したものである。この評価例は、情報が古いなど、現状に合わない場合がある。また、この評価例について、本 TF や評価者が責任を負うものではない。今回の評価・推奨度に対して意見等があった場合には連絡して頂ければ幸いである。

1.4 本資料の改版方針

本資料は以下の取扱方針とする。

- 年に一回程度定期的に本 TF にて内容の妥当性をチェックし、必要があれば改訂する。
- 今回カバーしなかったジャンルに対しても逐次調査を継続し、必要があれば改訂する。
- OSS 利用者、あるいは、ベンダ各位のご意見により、適宜、過不足を補う。

2. 技術情報の詳細

2.1 セキュリティ情報のカテゴライズ

本セキュリティ情報を検討する際には、セキュリティ情報を系統だて扱っている基準が必要となる。そのため、「政府機関の情報セキュリティ対策のための統一基準(2005 年 12 月版(全体版初版))(以下、統一基準)」を元に、該当統一基準内で必要とされるセキュリティ対策に対応した関連技術を検討している。その結果を受けて、セキュリティ対策のジャンルをカテゴライズし、それらに対応した商用技術と OSS での対応技術項目をあげている。

2.2 調査範囲

今回は、セキュリティ対策の以下の分野について調査を行った。

- ネットワーク
- サーバ

さらに各分野内で、暗号化や認証などといった詳細技術を項目としている。

2.3 表の見方

別表のように、セキュリティ対策のジャンルをカテゴライズし、それぞれのカテゴリに対応する政府の統一基準、商用製品と OSS・Linux 関連製品のカバーする範囲を記載している。

また、商用製品に対応する OSS・Linux 関連製品の利用状況を以下で評価している。

- (よく利用されている)
- (たまに利用される)
- (あまり利用されていない)
- × (利用されていない)

さらに、OSS・Linux 関連製品が利用されない理由として、以下の観点でチェックし、必要な場合はコメントを記載している。

- サポート
- 信頼性
- 性能
- 機能

- 日本語対応
- その他

商用製品に対する OSS・Linux 製品が存在していない場合には、存在していない理由を以下の観点でチェックし、必要な場合はコメントを記載している。

- マーケットサイズ
- 特許
- 法律
- 標準化
- ベンダーが非協力

最後にそれらを総合的に判断し、各 OSS・Linux 製品の製品としての完成度を加味した「推奨度」を記載している。

2.4 推奨度の計算方法

製品推奨度の計算方法は、以下を基準とした。

- (よく利用されている) 10 点
- (たまに利用される) 8 点
- (あまり利用されていない) 6 点
- × (利用されていない) 4 点
- 空白 (OSS が存在していない) 1 点

さらに、OSS・Linux 関連製品が利用されない理由及び、OSS・Linux 製品が存在していない理由でチェックが一つある度に、1 点減点している。

これにより、「特に使われない理由は存在していないのに、あまり利用されていない」といった OSS 製品と「使われない理由が存在しているために、あまり利用されていない」OSS 製品との値が明確になるようにしている。

尚、最終的に推奨度が 0 点以下になってしまった場合には、0 点となるようにしている。

3. 結果の概要

3.1 推奨度の結果

2.4 による計算方法により推奨度が高かったものを以下に示す。

10点 (OSS を積極的に利用すべきもの)

大分類	中・小項目	OSS
ネットワーク	ネットワーク FW	NetFilter + Iptables
	PKI	OpenSourcePKI(NSS,JSS,PSM)
	電子署名、電子証明書	GPG, OpenSSL
	通信ログの収集	WireShark(ethreal)
サーバ	認証	OpenLDAP,FreeRADIUS,PAM
	脆弱性監査ツール	Nessus(2.*),nmap
	暗号化	OpenSSL

8-9点 (OSS で十分なもの)

大分類	中・小項目	OSS
ネットワーク	IDS	Snort
	シングルサインオン	CAS (Central Authentication Service)
サーバ	改竄検知(ファイル)	TripWire

6-7点 (制約があるが OSS で十分なもの)

大分類	中・小項目	OSS
ネットワーク	シングルサインオン	OpenSSO
サーバ	メールフィルター	SpamAssassin
	ウィルス対策 (サーバ・クライアント)	ClamAV

ビジネスモデル TF メンバー一覧

<メンバ> (五十音順)

岩城 正吾	株式会社ブロードバンドタワー
女部田 武史	株式会社日本総研ソリューションズ
面 和毅	サイオステクノロジー株式会社
木戸 啓介	グローバルサイン株式会社
小島 浩之	アイピー・テレコム株式会社
才所 秀明	日立ソフトウェアエンジニアリング株式会社
鈴木 友峰	株式会社日立製作所
田口 裕也	株式会社 JTS
田端 利宏	岡山大学
古田 真己	サイオステクノロジー株式会社
榊本 圭	株式会社 NTT データ
宗藤 誠治	日本アイ・ビー・エム株式会社

所属は本資料公開時点のもの

商標について

Linux は、Linus Torvalds の米国およびその他の国における登録商標または商標です。

Windows は、米国 Microsoft Corporation.の米国およびその他の国における登録商標です。

UNIX は、The Open Group の登録商標です。

その他、記載されている会社名、製品名は各社の登録商標または商標です。