LINUXWORLD CONFERENCE & EXPO

オープンソースの活用動向と Linux の選択肢。そのセキュリティ対策

日本ヒューレット・パッカード株式会社
佐藤　慶浩

2004年6月4日

講師経歴

佐藤　慶浩（さとう　よしひろ）
日本ヒューレット・パッカード株式会社
ネットワーク・ソリューション本部　担当部長

yosihiro.com

1986 年。日本アポロコンピュータ(株)入社。International R&Dに所属。マサチューセッツ州チェルムスフォード市にて日本語環境製品の開発に従事。
1990 年。日本ヒューレット・パッカード(株)入社。新製品のテクニカル・マーケティングとして、ＯＳＦ／1、分散環境コンピューティング技術、マルチメディア技術、ハイアベイラビリティ技術、インターネット技術をＨＰ社の製品提供と相応して順次担当。この間 1993年からの 2 年間はカリフォルニア州クパチノ市にてセキュリティ製品の仕様開発に従事。
1996 年、米国駐在中に計画した製品群の出荷が始まったため、現在は主としてセキュリティ・ソリューションのコンサルティングに従事している。
1997 年以後は、通常のコンサルティング活動の他に、ＪＰＣＥＲＴ／ＣＣのヒューレット・パッカード対応窓口を担当。また、ＦＩＳＣ(金融情報システムセンタ、ＪＩＳＡ（情報サービス産業協会）、ＪＵＡＳ（日本情報システム・ユーザ協会）、システム監査人協会や各種有料セミナにて情報セキュリティポリシー策定方法論についての講演をしている。

情報処理学会(www.ipsj.or.jp/)　正会員
情報処理推進機構(www.ipa.go.jp/)セキュリティセンター　非常勤研究員
金融情報サービスセンター(www.fisc.or.jp/)セキュリティポリシー研究会　委員
情報処理学会 情報規格調査会(www.itscj.ipsj.or.jp/) SC 27/WG 1 小委員会(ISOｾｷｭﾘﾃｨ)　委員
情報処理学会 情報規格調査会(www.itscj.ipsj.or.jp/) SC 22 アドホック メンバー
杉並区住基ネット調査会(www.city.suginami.tokyo.jp/) 技術専門委員
情報ネットワーク法学会(www.in-law.jp/) 理事　**セキュアＯＳと基盤ソフトウエアに関する研究会**
経済産業省　セキュリティホールに関する法律の諸外国調査委員会　委員
総務省　セキュアＯＳに関する調査研究会　構成員
情報処理推進機構（www.ipa.go.jp/）情報システム等の脆弱性情報の取り扱いに関する研究会　委員
NPO オープンソースデベロップメントラボ（www.osdl.jp/）　Enterprise Linux for Public Sector　ワークショップ　メンバー

LINUXWORLD CONFERENCE & EXPO

講演内容

総務省　研究会報告書の活用

サポート

セキュリティの強化

その他

総務省　研究会報告書の活用

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書

電子政府・電子自治体における OS 導入のあり方について ～セキュアOS に関する調査研究会報告書～

平成16年4月
セキュアOS に関する調査研究会

OSS (オープンソース・ソフトウェア)活用のツボ

教わるのではなく、学ぶという意識

コスト意識

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書

目次

1．はじめに
2．電子政府、電子自治体におけるセキュリティ確保の重要性の高まり
3．電子政府、電子自治体の構築にあたり意識すべき事項
4．電子政府、電子自治体向けシステムに求められる要件
5．まとめ
6．おわりに

総務省　研究会報告書

目次

1．はじめに
2．電子政府、電子自治体におけるセキュリティ確保の重要性の高まり
3．電子政府、電子自治体の構築にあたり意識すべき事項
4．電子政府、電子自治体向けシステムに求められる要件
5．まとめ
6．おわりに

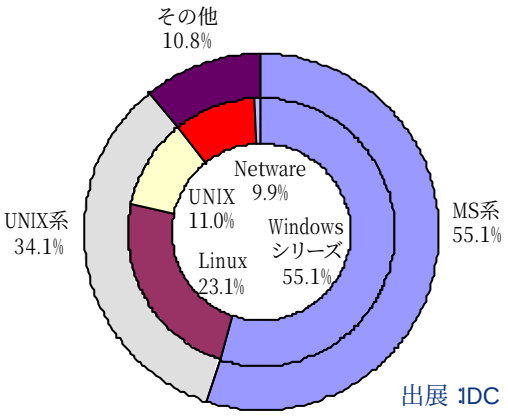
LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
2．電子政府、電子自治体におけるセキュリティ確保の重要性の高まり

総務省　研究会報告書
2.2 OS を中心とした情報システム関連全般の動向

(1)サーバOS

図表2-10　サーバOS市場における有償ライセンス出荷数のシェア（2002年、世界シェア）

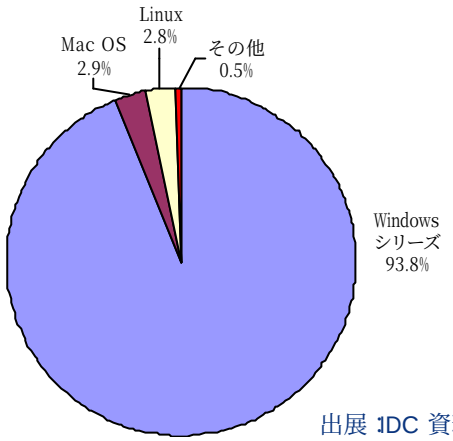


出展：IDC 資料（2004）より作成

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
2.2 OS を中心とした情報システム関連全般の動向

(2) クライアントOS　図表2-12 クライアントOS 市場における有償ライセンス出荷数のシェア（2002 年、世界シェア）

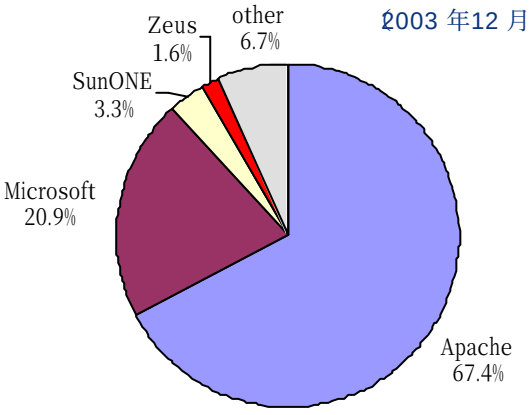


出展：IDC 資料（2004）より作成

総務省　研究会報告書
2.2 OS を中心とした情報システム関連全般の動向

(3) オープンソース・ソフトウェアの利用の進展

図表2-13 Web サーバで利用されているソフトウェア比率（利用サーバ台数、2003 年12 月時点、世界シェア）



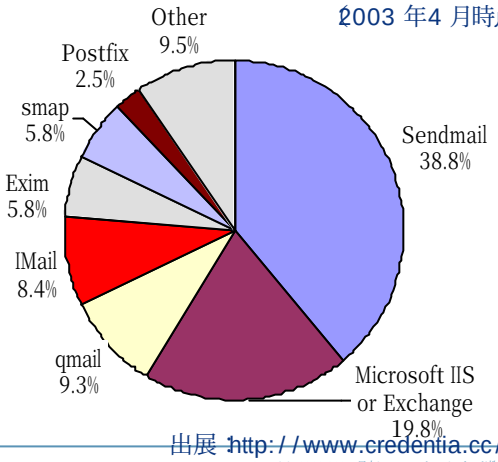
出展：Netcraft 社資料（http://www.netcraft.com/）より作成

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
2.2 OS を中心とした情報システム関連全般の動向

(3) オープンソース・ソフトウェアの利用の進展

図表2-14 メールサーバで利用されているソフトウェア比率（利用サーバ台数ベース、2003 年4 月時点、世界シェア）

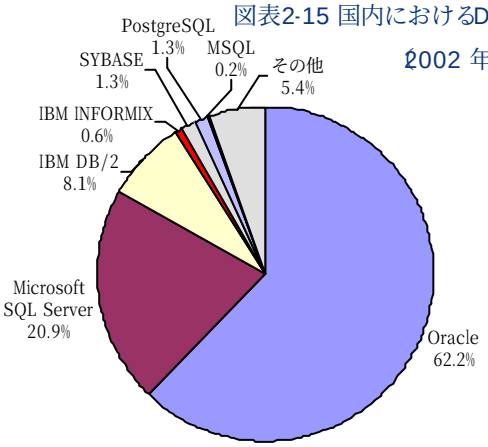


出展：http://www.credentia.cc/surveys/smtp/200304/ より作成

総務省　研究会報告書
2.2 OS を中心とした情報システム関連全般の動向

(3) オープンソース・ソフトウェアの利用の進展

図表2-15 国内におけるDBMS の採用状況（導入企業数ベース、2002 年度、国内シェア）



出展：社団法人日本情報システム・ユーザー協会「ユーザ企業IT 動向調査2003」

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
2.2 OS を中心とした情報システム関連全般の動向

(3)オープンソース・ソフトウェアの利用の進展

フリーソフトウェア財団（Free Software Foundation）による
フリーソフトウェアの定義
①いかなる目的であれ、プログラムを実行する自由（第0 の自由）
②プログラムの動作を研究し、必要に応じて改変する自由（第1 の自由）
③プログラムの複製を再頒布する自由（第2 の自由）
④コミュニティ全体の利益になるように、プログラムを改良し、改良点を公表する自由（第3 の自由）

加えて第１の自由と第３の自由の前提条件として、ソースコードが入手可能でなければならない。

総務省　研究会報告書
2.2 OS を中心とした情報システム関連全般の動向

(3)オープンソース・ソフトウェアの利用の進展

図表2-16 OSI によるオープンソースの定義（"Open Source Definition"）
①再頒布の自由 Free Redistribution
②ソースコードの公開 Source Code
③変更及び派生ソフトウェア作成の自由 Derived Works
④作者のソースコードの一貫性
⑤個人やグループに対する差別の禁止
⑥利用する分野に対する差別の禁止
⑦ライセンスの継承
⑧特定製品でのみ有効なライセンスの禁止
⑨他のソフトウェアを制限するライセンスの禁止
⑩ライセンスは技術に対して中立でなければならない

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
2.2 OS を中心とした情報システム関連全般の動向

(3)オープンソース・ソフトウェアの利用の進展

オープンソース・ソフトウェアのライセンス形態

OSI では、2004 年1月時点で、47 種類のライセンス（同名ライセンスの異なるバージョンを含む）をオープンソース・ソフトウェアのライセンスとして認定している。

- GNU GPL（GNU General Public License ）
  → Linux
- Berkeley Software Distribution License（BSD ライセンス）
  → FreeBSD

総務省　研究会報告書
2.2 OS を中心とした情報システム関連全般の動向

(3)オープンソース・ソフトウェアの利用の進展

オープンソースOS の開発体制とサポート体制

- 開発コミュニティによるサポート
- ディストリビュータによるサポート
- システム・インテグレータによるサポート
- サードパーティによるサポート

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
2.2 OS を中心とした情報システム関連全般の動向

(4)製品OS のソースコード開示

●マイクロソフト社のソースコード開示
①シェアードソースイニシアティブ
Enterprise/System Integrator/OEM/Research/Government
②ガバメント･セキュリティ･プログラム
● IBM 社の AIX のソースコード開示
①政府の一次契約者に対するライセンシング
②政府に対する開示
● Sun Microsystems 社のSolaris のソースコード開示
①Sun Hardware Partner Program (SHWP)
②Solaris 9 Source Code Program
●ヒューレット･パッカード社のHP-UX ソースコード開示
①HP-UX ソースコード製品(SCP:Source Code Product)

総務省　研究会報告書
2.2 OS を中心とした情報システム関連全般の動向

製品OS のソースコード開示

図表2-16 OSI によるオープンソースの定義 "(Open Source Definition")
①再頒布の自由 Free Redistribution
②ソースコードの公開 Source Code
③変更及び派生ソフトウェア作成の自由 Derived Works
④作者のソースコードの一貫性
⑤個人やグループに対する差別の禁止
⑥利用する分野に対する差別の禁止
⑦ライセンスの継承
⑧特定製品でのみ有効なライセンスの禁止
⑨他のソフトウェアを制限するライセンスの禁止
⑩ライセンスは技術に対して中立でなければならない

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書

目次

総務省　研究会報告書
３．電子政府、電子自治体の構築にあたり意識すべき事項

LINUXWORLD CONFERENCE & EXPO

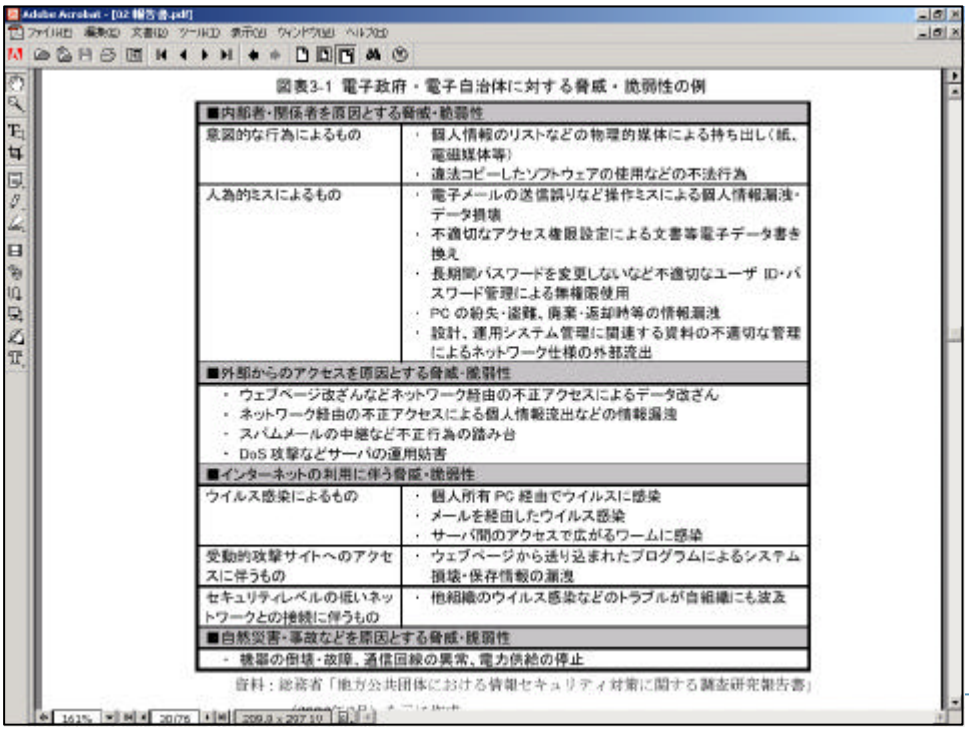
総務省　研究会報告書
３. 電子政府、電子自治体の構築にあたり意識すべき事項

3.1 電子政府・電子自治体で取り扱う情報に求められるセキュリティ
3.2 取り扱う情報に起因し、システムに求められるセキュリティ確保の方策
3.3 取り扱う情報に起因し、システムに求められるその他の事項
3.4 電子政府、電子自治体推進にあたり留意すべき事項
3.5 電子政府、電子自治体におけるシステム構成モデル

総務省　研究会報告書
3.1 電子政府・電子自治体で取り扱う情報に求められるセキュリティ

図表3-1 電子政府・電子自治体に対する脅威・脆弱性の例

LINUXWORLD CONFERENCE & EXPO



図表3-1 電子政府・電子自治体に対する脅威・脆弱性の例

■内部者・関係者を原因とする脅威・脆弱性	
意図的な行為によるもの	・個人情報のリストなどの物理的媒体による持ち出し（紙、電磁媒体等） ・違法コピーしたソフトウェアの使用などの不法行為
人為的ミスによるもの	・電子メールの送信誤りなど操作ミスによる個人情報漏洩・データ損壊 ・不適切なアクセス権限設定による文書等電子データ書き換え ・長期間パスワードを変更しないなど不適切なユーザ ID・パスワード管理による無権限使用 ・PC の紛失・盗難、廃棄・返却時等の情報漏洩 ・設計、運用システム管理に関連する資料の不適切な管理によるネットワーク仕様の外部流出
■外部からのアクセスを原因とする脅威・脆弱性	
・ウェブページ改ざんなどネットワーク経由の不正アクセスによるデータ改ざん ・ネットワーク経由の不正アクセスによる個人情報流出などの情報漏洩 ・スパムメールの中継など不正行為の踏み台 ・DoS 攻撃などサーバの運用妨害	
■インターネットの利用に伴う脅威・脆弱性	
ウイルス感染によるもの	・個人所有 PC 経由でウイルスに感染 ・メールを経由したウイルス感染 ・サーバ間のアクセスで広がるワームに感染
受動的攻撃サイトへのアクセスに伴うもの	・ウェブページから送り込まれたプログラムによるシステム損壊・保存情報の漏洩
セキュリティレベルの低いネットワークとの接続に伴うもの	・他組織のウイルス感染などのトラブルが自組織にも波及
■自然災害・事故などを原因とする脅威・脆弱性	
・機器の倒壊・故障、通信回線の異常、電力供給の停止	

資料：総務省「地方公共団体における情報セキュリティ対策に関する調査研究報告書」

総務省　研究会報告書
3.1 電子政府・電子自治体で取り扱う情報に求められるセキュリティ

図表3-2 情報セキュリティ確保のための一般的な手段

●機密性の確保
　情報ごとに許可された者のみが読み出しができること
●完全性の確保
　情報の改ざん、破壊、滅失等を防止することができること
●可用性の確保
　サービス停止の防止、停止時間の短縮を図ることができること
●真正性の確保
　利用者、処理方法、システム及び情報が実態通りに識別されることを保証すること
●責任追跡性の確保
　情報に証拠を提供し、実際の行為者が責任を避けることを防ぐことができること

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
3．電子政府、電子自治体の構築にあたり意識すべき事項

3.1 電子政府・電子自治体で取り扱う情報に求められるセキュリティ
3.2 取り扱う情報に起因し、システムに求められるセキュリティ確保の方策
3.3 取り扱う情報に起因し、システムに求められるその他の事項
3.4 電子政府、電子自治体推進にあたり留意すべき事項
3.5 電子政府、電子自治体におけるシステム構成モデル

総務省　研究会報告書
3.2-3 取り扱う情報に起因し、システムに求められるセキュリティ確保の方策 とその他の事項

セキュリティ機能

- **機密性確保の必要性**
  - 無権限アクセスの防止
  - ウイルス対策
  - データの保管／持ち出し、情報送出の防止
  - 推論攻撃対策
- **完全性確保の必要性**
  - 情報改ざんの防止
  - 情報破壊、滅失の防止
- **可用性確保の必要性**
  - サービス停止の防止
  - サービス停止時間短縮
  - 高負荷への対応
- **真正性確保の必要性**
  - なりすましの防止
- **責任追跡性確保の必要性**
  - 否認の防止

その他の機能

- **利用・運用の容易性**
  - 導入及びカスタマイズの容易性
  - 業務必要なアプリケーションの
  - 充実、入手容易性
  - 動作保証がなされているハード
  - ウェアの充実、入手容易性
  - 運用情報の提供機能
  - セキュリティ機能設定の容易性
  - 操作性
  - スケーラビリティ
  - システム開発・保守を担う人材の充実
- **サポート体制**
  - 情報提供、情報公開状況
  - カスタマイズ部分を含めた動作保証
  - パッチ等の供給体制
  - サポートサービス提供状況、継続期間
- **漢字コードへの対応**
  - 異体字等の導入容易性
  - 他システムとの整合容易性

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
3.4 電子政府、電子自治体推進にあたり留意すべき事項

長期的視点
委託事業者との契約
コスト

総務省　研究会報告書

目次

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
４．電子政府、電子自治体向けシステムに求められる要件

図表4-1 電子政府、電子自治体向けシステムに求められる要件一覧

機能要件：52分類（92項目）

（PDF　63ページ）

総務省　研究会報告書

目次

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
５．まとめ
(1)クライアントに対するまとめ

○ **操作性**
　クライアントOSは、職員が日々業務で使用するものであることから、使いやすいことが求められる。
　使いやすいインタフェース、各種メニューの日本語化等の使い勝手に関する工夫や、操作ミス等による誤処理を未然に防止するための工夫等がなされていることが望ましい。

○ **一般業務用アプリケーションの充実**
　一般業務に必要となるアプリケーションが充実していることが望ましい。また、これらアプリケーションで作成した資料が、文字化け等を起こさずに確実に印刷できなければならない。

○ **クライアントOSの多様性の確保**
　クライアントOSを統一した場合、操作性や運用面等で有利な点が多数あるものの、当該OSの脆弱性の影響を一斉に被る恐れもある。連鎖的被害の拡大を防ぎ、業務の継続を図る上では、クライアントOSを多様化することも有効な方策の一つとなり得る。

総務省　研究会報告書
５．まとめ
(2)業務用サーバに対するまとめ

○ **業務特性に応じたセキュリティ機能の確保**
　業務によって、取り扱う情報資産に求められるセキュリティ要件は異なる。一般に高いセキュリティ機能を実現するためには、より多くのコストが必要となることから、業務特性を踏まえ、どこまでのセキュリティ機能を要するのか検討した上で、適切なOSを選択しなければならない。

○ **クライアントとの接続性、フロントエンドサーバとの接続性とのバランス**
　庁内ネットワーク内の処理を主とする業務か、電子申請や電子調達等の外部との処理を主とする業務であるのかにより、OS選択において、クライアントとの接続性の良さ、フロントエンドサーバとの接続性の良さのどちらを優先すべきかが異なる。

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
５．まとめ
(3)フロントエンドサーバに対するまとめ

○ **情報セキュリティ侵害の防止**
　フロントエンドサーバは外部からの脅威にさらされることから、デフォルトで不要なサービス・機能が排除されていることや、セキュリティポリシーに即したセキュリティ設定が容易に行えること、外部からの情報セキュリティ侵害を防止する仕組みを備えていること等が重要である。

○ **外部からの重要な情報へのルートの遮断**
　フロントエンドサーバに重要な情報を保存してはならない。一時的に保存される情報についても、不正アクセスや改ざんなどが行われないよう対策を施すことが必要である。
　重要な情報を格納している内部システムに、外部から直接アクセスできるルートが生じないようにしなければならない。

○ **可用性の確保**
　アクセスの集中やサービス妨害攻撃等によりシステムに高負荷がかかった場合にも、サービス停止等の障害が発生しないよう対策を施すことが重要である。

総務省　研究会報告書
５．まとめ
(4)システム全般に関するまとめ

- **情報セキュリティ対策**
　情報システムへの脅威に対して、情報セキュリティ対策を適切に施し、個人の権利侵害等が生じないようにすることが最重要課題である。

- **個々のシステムに応じたセキュリティ要件の検討**
　調達者自らが、業務や情報資産の特性を考慮した上で、具体的なセキュリティ要件及びその優先順位を検討しなければならない。

- **サポートサービスの確保**
　情報システムの継続的な利用には、サポートサービス等が確実に提供されることが重要である。契約書等の条件に組み込む等の対応が必要である。

- **次回調達先を限定しない仕様の選択**
　オープンな標準に準拠した技術を活用するなどして、次回の調達時に調達先を限定する仕様とならないよう配慮する必要がある。

- **トータルコストの検討**
　導入コストのみならず、システムの開発・変更コスト、運用コスト等を合わせたトータルコストの検討が必要である。

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
５．まとめ
(5)オープンソースOSの考え方

○ **継続的なサポートサービスの提供の条件化**
　代表的なオープンソースOSであるLinuxやFreeBSD等はUNIXのもつ機能の実装を目指したこともあり、機能的にはUNIX系OSの一つとして捉えられる。
　オープンソースOSは、直接の営利目的で開発されていないことから、OSに瑕疵があったとしても、開発者に直接OSの修正や修正プログラムの提供を強制する関係を確立できない。しかし、ソースコードが公開されていることから、システム・インテグレータ等に修正プログラムの開発を依頼することは可能である。
　オープンソースOSを利用する場合には、修正プログラム等のサポートサービスが確実に得られるよう、調達時の仕様書や契約書等にサポートサービスの提供を条件として盛り込むといった対応を行うことにより、製品OSとの違いは少なくなると考えられる。

総務省　研究会報告書

目次

LINUXWORLD CONFERENCE & EXPO

総務省　研究会報告書
６．おわりに

必要な情報セキュリティ水準を確保しつつ、業務にも利用しやすい情報システムを調達するためには、OS等の銘柄指定を行わず、OS以外の追加のソフトウェアが必要な場合も考慮した上で、次のとおり実施すべきと考える。

①情報システムの調達者が、当該システムに求められる機能及び品質を抽出し、
②自治体のセキュリティポリシー等を考慮して、守るべき情報資産や想定脅威から必要とされるセキュリティ要件について洗い出し、
③当該機能・セキュリティを含めた品質を網羅した機能要件仕様書を作成し、
④かつ、当該機能・品質の重要性について重み付けを行った上で、
⑤当該重み付けを元にした総合評価方式（提案募集型）の競争入札を実施

これにより、電子政府・電子自治体用のＯＳは、それぞれの情報システムに最適なものが選択されるとともに、多様性が確保される。

高村さんによる基調講演でのキーワード

「選択肢が多いこと」として、Linux にも期待する

OSとしてのレベルはOK
※パッチ・サポートの提供義務を契約に盛り込む。（ことにすればよい）
※セキュリティについては、追加のソフト必要な場合もある。（と思えばよい）

売り方と買い方をよくすれば実用可能

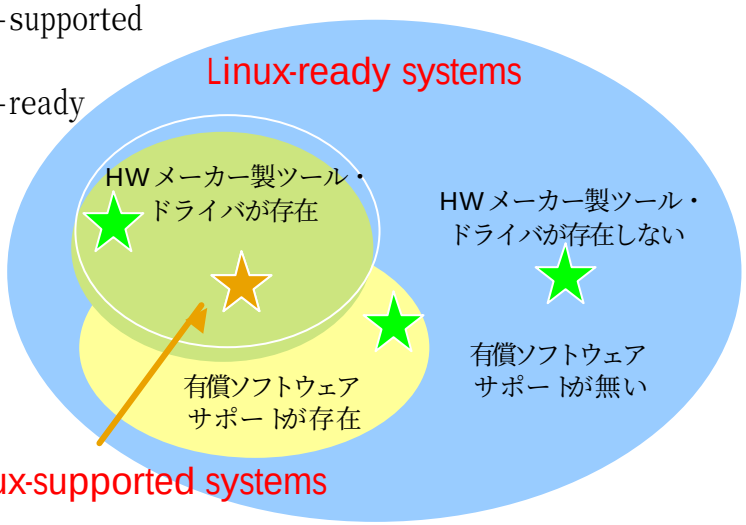
「何を買うか」ではなく、「どう運用するか」
↓
運用のために必要な人手と金をかければよい（かけなければならない）

LINUXWORLD CONFERENCE & EXPO

サポート

OSS (オープンソース・ソフトウェア)活用時のポイント: supported なのか ready なのか

Linux-supported
or
Linux-ready



LINUXWORLD CONFERENCE & EXPO

OSS（オープンソース・ソフトウェア）活用時のポイント：supported なのか ready なのか

オープンかクローズかの定義はあいまい。
Linux コミュニティの「オープンソースの定義」に関する主張：
①ソースコードが公開されていること
②ソースコードの改変による再配布が許可されていること

しかし、信頼性の観点では、オープンであるかどうかではなく；
ソースコードの検証可能性（ソースコードを検証できるか）
ソースコードの検証実現性（ソースコードを検証する人がいるか）
ソースコードの認定可能性（ソースコードを認定する費用原資があるか）
脆弱性問題のわかりやすさ（わかりやすい資料を誰が用意するのか）
脆弱性問題の周知徹底（告知の徹底を誰が図るのか）
ソースコードの修正可能性、実現性（修正でき、修正する人がいるか）
対処方法のわかりやすさ（わかりやすい資料を誰が用意するのか）
対処方法の周知徹底（告知の徹底を誰が図るのか）

OSS（オープンソース・ソフトウェア）活用時のポイント：supported なのか ready なのか

システム全体（縦横）の信頼性を検討する必要がある。
OSの信頼性だけを論じるのは片手落ち、あるいは、無意味。

オープンソースOSの上で稼動するアプリケーション・サービスの多数が、フリーソフトになりやすい。

オープンソースは、フリーライセンスになりやすい。
フリーソフトでは、不具合や脆弱性への対処方法の探索と適用は利用者の義務。
Linux の有償サポート契約者の恩恵による無償利用者の錯覚。

LINUXWORLD CONFERENCE & EXPO

OSS (オープンソース・ソフトウェア)活用時のポイント: supported なのか ready なのか

システムの信頼性を高めるには:

ソースコードを検証する人達が、参照することができ、かつ、
それを第3者に認定してもらう原資があり、かつ、
脆弱性が発見されれば、それがわかりやすく周知徹底され、かつ、
対処方法を開発する人がおり、それが再配布可能になり、かつ、
対処方法ががわかりやすく周知徹底されること。

オープンソースか、クローズソースかは、上記の役割を担う組織(who)や方策(how)が異なるだけである。

Linux ＋ Linux 上のサービスの課題:

- 誰が検証するのか?
- 誰が認定費用を負担するのか?
- 誰が不具合や脆弱性の対処方法をわかりやすく周知徹底するのか?

セキュリティ強化

LINUXWORLD CONFERENCE & EXPO

セキュアOS関係のソフトウェア

NSA SELinux
　日立ソフトウェアエンジニアリング
HiZARD
　ミラクル・リナックス
Secuve TOS
　NECソフト東北
PitBull
　インフォコム、ヒューコム
Compartment Guard for Linux
　日本ヒューレット・パッカード

日経コンピュータ7月号にて特集予定

情報ネットワーク法学会
セキュリティ技術研究部会　セキュアＯＳ研究会

http://in-law.jp/

情報ネットワーク法学会
Information Network Law Association Japan
I N-Law
い　ん　ろ　う　？

LINUXWORLD CONFERENCE & EXPO

その他

OSS (オープンソース・ソフトウェア)活用時のポイント: その他の事項

日本語処理

管理

- システム管理 (マネジメント・ソフトウェア)
- ユーザ管理 (プロビジョニング・ソフトウェア)

経済性

法的責任

LINUXWORLD CONFERENCE & EXPO

まとめ

適材・適所でオープンソースを活用できる。

機能要件を定めて、選定することで選択肢が広がる。

オープンソースということ自体で、信頼性が左右されるものではない。

すべてをオープンソースにするというのは中期的にはなく、他と混在する。

セキュリティ対策の向上のために、オープンソースという特性で必要なことを検討して実践する。

信頼性の向上には、技術は一翼にすぎない。人的体制や法制など、さまざまな環境構築により向上させる必要がある。

本日の資料

http://yosihiro.com/speech/

yosihiro.com