LINUXWORLD CONFERENCE & EXPO
The Linux Solution
～Linux 導入について考える。現状の課題と解決策。～

# 電子政府での オープンソース活用と セキュリティ対策の課題と動向

日本ヒューレット・パッカード株式会社
コンサルティング統括本部
セキュリティコンサルティング部
佐藤　慶浩

2003年9月24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
ＨＰコンサルティング統括本部
セキュリティ・コンサルティング部　部長

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
日本ネットワークセキュリティ協会(www.jnsa.org/)　理事
情報処理振興事業協会(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
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
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

## 目次






## 電子政府でのオープンソース活用

経済性
　ライセンス費用を安価にできるのではないか
安全性
　安全性を高められるのではないか
独立性・継続性
　他に依存せずに、将来に渡って供給できるのではないか

オープンソースの対象ソフト
　OS（オペレーティング・システム）
　開発環境ソフトウエア
　アプリケーション・サービス・ソフトウエア
　など

## OSの安全性の模索：セキュアOS

セキュアOSの定義はあいまい。

商用 Unix
- Trusted OS (TCSEC BLS, CMW)
  - 各社 Trusted OS (HP, IBM, Sun, Argus)

Linux
- NSA SE Linux
- Argus PitBull LX
- HP Compartment Guard for Linux
- など

FreeBSD




## OSの安全性

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、安全性の観点では、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負担があるか）
脆弱性問題のわかりやすさ（わかりやすい資料が用意されるか）
脆弱性問題の周知徹底（告知の徹底が図られるか）
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（わかりやすい資料が用意されるか）
対処方法の周知徹底（告知の徹底が図られるか）


## OSが強固なだけでは安全ではない

システム全体（縦横）の安全性を検討する必要がある。
OSの安全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。

イギリスで発生した問題＝Linux 上の Apache にパッチを適用していないことによって発生した。
Linux からすれば、Linux の問題ではないが・・・

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、脆弱性と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錯覚。

## システム（←OS改め）の安全性

システム（←OS改め）の安全性を高めるには：

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、
対処方法が見出されれば、それ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、上記の役割を担う方策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？
- 誰が脆弱性や対処方法をわかりやすく周知徹底するのか？




## OS にまつわる国内動向

総務省
「セキュアOSに関する調査研究会」

経済産業省
「OS調査開発」

IPA（情報処理振興事業協会）
「オペレーティングシステムのセキュリティ機能拡張の調査」
http://www.ipa.go.jp/security/fy13/report/secure_os/secure_os.html

JNSA（日本ネットワークセキュリティ協会）
「セキュアOSとその活用方法研究WG」
意見交換：内閣官房、警察庁、防衛庁、経済産業省、総務省

## セキュアOSに関する国内での技術調査活動

NSA SELinux
http://www.selinux.hitachi-sk.co.jp/ml/

HP Compartment Guard for Linux
http://www.hp.com/jp/hpcg




## 法的側面

セキュリティホールを作った者の責任
セキュリティホールに気づいても報告しなかった者の責任
セキュリティホールの存在を告知しなかった者の責任
セキュリティホールの有無を確認しなかった者の責任
セキュリティホールの告知を受けても対処しなかった者の責任

欧米のセキュリティ強化手法の前提に司法取引がある

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」
→JNSA Network Security Forum 2003 での委員会発表
「へえ」

## 電子政府システムにおける安全性の観点

民間で得られているノウハウは、そのまま実践すべき。
セキュリティに関する情報共有は、民間より以上のものが求められる。

情報の格付け（classification）の徹底（外部／内部サーバではなく）
発注後のセキュリティ対策是正への費用対応（継続的改善のため）

それに加えて検討が必要なことは：

民間でリスク転嫁（移動）している一般論の再確認
- デュアルロックによる抑止
- 有限の機密保持期間
- 委託業務の契約担保
- など




## まとめ

電子政府においては、適材・適所でオープンソースを活用できる。
オープンソースということ自体で、安全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。
安全性の向上には、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。

現在のIT技術を、電子政府で使うのは、リスクと利便性、経済性とのバランスの模索であることを忘れてはならない。（リスク回避は不可能）
民間のバランスと、行政のバランスが違うことが、新たな挑戦である。

## 本日の資料

**http://yosihiro.com/business/**

明日、9月25日午前中に掲載します

yosihiro.com