

セキュアOSに関する調査研究会
第6回 議事要旨(案)

【日時】 平成16年2月10日(木)14時～16時

【場所】 経済産業省別館10階 1020会議室

【出席者】

〔研究会構成員(敬称略)〕

村岡座長、有田構成員(岡野代理)、石井構成員、泉澤構成員、泉名構成員、斎構成員、阪田構成員、後藤構成員、坂村構成員(越塚代理)、佐藤構成員、高澤構成員(小園井代理)、田中構成員、寺本構成員、中尾構成員、中上構成員、東構成員、平野構成員(夏代理)、山田構成員

〔総務省〕

鈴木政策統括官、桜井参事官、野津情報流通振興課長、武田情報セキュリティ対策室長、赤阪情報流通振興課長補佐、高村情報セキュリティ対策室長補佐
(オブザーバー)

上田情報システム企画官、高島地域情報政策室地域情報化係長

【配布資料】

- 資料1 セキュアOSに関する調査研究会 第5回 議事要旨(案)
- 資料2 セキュアOSに関する調査研究会 報告書骨子
- 資料3 セキュアOSに関する調査研究会 報告書(叩き台)
- 資料4 OSに関する構成員アンケート結果(イメージ)

【議事概要】

1. 開会
2. 配布資料確認
3. 前回議事録の確認

4. 議事概要

(1) 報告書について

〔質疑・討議〕

- ・リーガルリスクとして考慮しなければならない問題点は明らかになっているが、それに対して自治体が具体的にどのように対処したら良いのかわかりにくい。例えば、留意すべき点を踏まえた契約書の例文などがあれば、調達の際にさらに便利になるのではないか。
- ・現状以上に具体的に書くためには、個別システムを想定しなければならない。報告書では、どのようなシステムにも適用できることを念頭においているため、抽象的にならざるを得ない部分がある。
- ・法律の意見はいずれかの当事者の立場からの主張であり、個別的になる。システム調達の当事者である政府・自治体、住民、SIer やベンダーのいずれかの立場に偏った内容は盛り込まないほうが良いと思う。
- ・セキュリティを確保する上では、常に世の中の動きにあわせて見直す必要がある。報告書に監査・評価するプロセスが必要であるといった記述があると良い。
- ・報告書では、マネージメント・プロセスとして、どのように扱うべきかに関して議論していない。したがって、監査のようなマネージメントに関する記述は、セキュリティ要件を列挙する箇所よりもまとめ部分で記述したほうが良いと思う。報告書として、電子政府、電子自治体に特有の脅威や脆弱性として、どのようなものがあるのかに関する記述が必要であると考えます。
- ・「電子政府、電子自治体の構築にあたり意識すべき事項」に電子政府、自治体特有の脅威、脆弱性など意識すべき事項を加えたいと思う。
- ・セキュア OS に関する研究会報告書であるのに、冒頭のあたりがオープンソース OS の報告書のように見えてしまう。オープンソース OS に関するトレンドだけでなく、OS のセキュリティに関する記述を加えるべきではないか。
- ・最近のセキュリティ事案を挿入する場合、商用 Unix 系の事案が書けない。これは、事案が実際に存在しないのか、公表されていないだけなのか。
- ・商用 Unix 系のパッチの数は他と変わらないと思う。しかし、商用 Unix 系では、パッチのデリバリーをサポートビジネスとしていることが多く、契約をしているユーザであれば、パッチは当てられるので被害に至ることは少ないと思う。
- ・セキュリティ事案を記述するのであれば、パッチのデリバリーについても記述する必要がある。IBM、ヒューレットパカード、サン・マイクロシステムズの構成員の方々には、商用 Unix 系のパッチ・デリバリー体制について、文案を頂きたい。
- ・TCSEC 等は 80 年代の話である。最近の SELinux 等の動向を追記できないか。
- ・報告書の対象が自治体システム導入者であることを考えると、Trusted OS、Secure OS を記述する必要はないと思う。

- ・「クライアントに対するまとめ」にセキュリティに関する記述がない。「エ」としてクライアントのセキュリティに関する記述が必要ではないか。

(2) セキュア OS に関する調査研究会 報告書骨子(案)

[質疑・討議]

- ・製品を特定せずに評価を行うのか。製品ごとに強みが異なり、例えば広く Unix 系として、各 Unix 製品を「or」でくくると、全ての機能が満たされることになるが。
- ・特定の OS を想定していただいても、特定した OS をわかるように回答してもらっても構わない。製品によって異なるということであればその旨記述して頂きたい。評価者の立場が変われば、想定する OS も変わると思っている。
- ・Unix 系と MS 系に分類した理由は何か。Open 系と商用系の方が本文との整合性が取れて良いのではないか。
- ・以前、この研究会で「機能」に着目して、分けたほうが良いと決めたと思う。また、政府・自治体の調達の観点から、このような分け方のほうが便利である。
- ・OS に機能を持つか、ソフトによって機能を実現するのはベンダーのシステムモデルやビジネスモデルの問題である。
- ・OS に機能があって望ましい場合と、機能があるために他のソフトとの相性が悪くなることもある。このような柔軟性を含めた表現にできないか。例えば、「OS に機能があり、他のソフトによる代替を許す」、「OS に機能があり、他のソフトによる代替を許さない」、「OS に機能はないが、追加ソフトによる実現できる」、「OS に機能はなく、追加ソフトによっても実現できない」の4通りである。
- ・よく知らない読者が読むと、アンケート結果を鵜呑みにする危険性がある。
- ・アンケートは、報告書に沿って実施するものである。事前にご相談させて頂いたところでは、意見はバラバラになり、一方に偏ることはないと思う。報告書を単独で使用することはあるが、アンケート結果を単独で使用することはない。アンケートは常に報告書と一緒にする。

5. その他

アンケートは、選択肢を修正の上、来週に構成員にメールで配布する。

報告書については、本日の修正点の他にも気づいた点があれば、指摘していただきたい。全ての修正を行った上で、次回の研究会の前に配布したい。

今回は、3月下旬の開催を予定している。

6. 閉会