セキュアＯＳに関する調査研究会
第４回　議事要旨

【日時】　　平成 15 年 10 月 23 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（山口代理）、石井構成員、泉澤構成員、泉名構成員、斎構成員、大木構成員（小林代理）、阪田構成員、高澤構成員（小薗井代理）、高橋構成員、田中構成員、寺本構成員、土居構成員、中上構成員（松田代理）、東構成員、平野構成員、山田構成員（中村代理）、脇構成員

〔総務省〕

清水政策統括官、武井情報流通振興課長、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課企画官、瀬脇地域情報政策室課長補佐

【配布資料】

資料１　セキュア OS に関する調査研究第３回議事要旨（案）

資料２　セキュア OS に関する調査研究会　論点整理（検討の方向性）案

【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

・セキュア OS に関する調査研究会　論点整理（案）

高村課長補佐から、資料２に沿って説明。

〔質疑・討議〕

・セキュリティ確保のための一般的な手段として、真正性の確保も追加すべきではないか。本人確認を行った後、アクセス制御、フロー制御、推論制御、暗号制御がある。

・OS を認証実績の「多少」で評価しているが、認証実績があっても例えばオレンジブックの B と C では大きな違いがある。また、Windows や Linux でも数年後にはセキュリティの高い OS が市場に出る予定であり、現状の OS を評価するのは適当ではない。

・OS だけではなく、クライアントやサーバも含めたシステムとして考えるべきであろう。セキュリティはシステム全体で確保するもので、クライアント端末も含めて議論すべき。

・具体的にどのような環境で使用するかを決めないと、どの OS が良いかという評価はできない。

・p.13 の要件として追加すべき項目に、将来の環境変化の対応容易性を含めてはどうか。短期間に陳腐化するような機能・性能を有する OS はセキュアとは言えない。また、セキュアな OS 評価の重要な点として、どれだけ多くの人がその OS をサポートしているかという点もあると思う。

・OS 評価における時間軸はどのように考えているのか。つまり、ある特定バージョンの OS を評価して、10 数年その評価した OS を使うようにするのか、それとも OS のバージョンアップに追随して継続的に評価していくつもりなのか。

・バージョンアップに追随して評価するのではなく、既存の OS を評価することを考えている。

・確かに新しい OS を各社とも開発しているが、いつ登場するか分からない。それに登場したとしても今まで使っていたアプリケーションがその新しい OS で正常に動作するとは限らない。そのため、期間を決めて評価すること、もしくは調達の時のサポート期間を定めることで時間軸の問題は解消するのではないか。

・まだ公表されていない製品を評価することはできない。製品に対する将来ビジョンやサポートに対する考え方を評価しても良いのではないか。

・契約時にどれくらいの期間サポートしてくれるのかを評価の時間軸としたい。

・漢字コードに関連して他のシステムとの整合性を考えた場合、標準等に準拠しているかどうかを評価尺度とすると客観的に評価しやすいのではないか。また、漢字コードは OS より上のレイヤーでの問題ではないか。OS の必須機能を絞った上で評価したほうが良いのではないか。

・完全性という観点から、外字は OS で管理する必要がある。フォントを操作することであたかも改ざんされたように見える可能性もある。

・漢字コードは地名・人名への対応で問題となる。人名では、申請で入力された名

前の文字と役所から発行される名前の文字が異なることが一番の問題である。

・国・政府としてより多くの漢字を扱えることが理想である。

・もし国のシステムが損害を受けたとき、その責任をどうするかが問題である。私企業であれば、損害賠償を請求し、損害の責任をシステム会社等に負わせるが、政府や地方公共団体が同じような発想でよいのか。

・セキュリティ認証の取得には、所定の文章を用意して、実験を行う必要があるので、コストがかかる。結果として資金力のあるメーカーの製品が有利となり、オープンソース系にとっては難しいのが現状ではないか。認証実績という軸でオープンソース系と製品系を評価するのは無理ではないか。それに認証制度は確かに第三者機関が評価するので良いのかもしれないが、全てその機関に任せることになって、信頼性はあるのか、という問題がある。

・既存の OS に対する評価はあくまでも参考として行うものであり、メインはシステム調達の際に注意しなければならない要件を列挙することである。OS の評価は各 OS をグルーピングした上で、各構成員の方々に行っていただくつもりである。

・評価項目は客観的である必要がある。一つの OS でもある観点からはセキュアでも、別の観点からはセキュアでないこともありうる。使い方によって評価が変わってしまう。評価の結果が一人歩きすることだけは避けたい。

・ウイルス対策、安定した OS といったことをどうやって評価するのか。OS として評価すべきものを絞る必要があると思う。

・セキュリティはユーザのスキルに依存するところがある。機能的な面だけで評価するだけではなく、運用上の評価もあっても良いのではないか。

・中央官庁が本気で設定を施したシステムと、SIer が納入したまま、買ったままのシステムとではセキュリティレベルが異なる。どのような設定の状態の OS を評価するのか。またコストの評価は難しい。

・評価はユーザサイドの視点で行いたい。どの状態で評価するのかは、システムとして納入された状態を想定している。

・新規調達とリプレースでは異なる。マイグレーションの容易性ということが評価の尺度となるのではないか。調達の際には Service Level Agreement を結ぶことになると思うが、SLA においてセキュリティをどのように考えるかが重要である。Shared Service というものがあるが、アクセス権限をどこまで与えて管理するのかという問題がある。

５．その他

次回は、11 月下旬以降の開催を予定している。

６．閉会