セキュアＯＳに関する調査研究会
第３回　議事要旨

【日時】　　平成 15 年 9 月 17 日（水）14 時～16 時

【場所】　　経済産業省別館 8 階　827 会議室

【出席者】

〔研究会構成員（敬称略）〕

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、大木構成員（小林代理）、後藤構成員、阪田構成員、坂村構成員（越塚代理）、高橋構成員、村岡座長、佐藤構成員、高澤構成員、田中構成員、寺本構成員、中上構成員、東構成員、平野構成員、山田構成員（坂本代理）

〔総務省〕

清水政策統括官、寺崎参事官、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、高島地域情報政策室係長

【配布資料】

資料１　セキュア OS に関する調査研究第２回議事要旨（案）

資料２　行政システムのセキュリティについて

資料３　セキュア OS に関する調査研究会　論点整理（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

（１）行政システムのセキュリティについて

泉澤構成員から、資料２に沿って説明。

（２）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３に沿って説明。

〔質疑応答・討議〕

・資料 3（セキュア OS に関する調査研究会　論点整理（案））では守るべき対象をシステムとしているようだが、守るべき対象はシステムではなく、情報である。政府が扱っている情報の重要度に関する一覧表があれば良い。情報公開法でも公開の対象とならない情報の基準等を参考にすれば良いと思う。民間のベスト・プラクティスを参考にして、民間が棚上げしている問題をシステムや OS でカバーすることをこの場で議論すればよい。民間ではたとえ情報漏えいが発生しても、損害賠償を行えばよいという割り切りが行われている。しかし、行政では同じようにはいかない。資料 3 の p.6 の横軸はソースコードのオープン性よりもソースコードの検証の可能性を軸にした方が良いと思う。縦軸はソースコードが明示的に評価されているか、いわゆる認定制度の対象になるかというところで考える方がよい。

・資料 2（行政システムのセキュリティについて）の補足として、次の 6 点を挙げる。1 点目は、法律や制度の変更に伴い、行政のアプリケーションレベルのシステムの変更が頻繁にある点である。この点は、常に自治体のシステムの大きな問題となっている。2 点目は、個人情報を部門間でやりとりすることが非常に多い。市町村にはネットワークがつながっている出先拠点が多いことが 3 点目。基幹系業務では汎用機のユーザが多いことが 4 点目。5 点目は、トラブルが発生したときの影響が大きいこと。6 点目は、個人情報は条例により保護の対象としているので、個人情報の保護は議会や市民のコントロール下にあることを意識しておく必要がある。

・情報だけでなくシステム自体を守ることも必要であろう。セキュアの中にフォルト・トレランス、障害に対する強さを含めるのかどうかを考える必要がある。情報を守るためにどこまでコストをかけるかが問題である。民間では、最終的にお金に換算され、情報の価値に見合ったセキュリティ対策でなければならないという判断がなされる。しかし、行政の場合には情報の価値よりも多くのコストをかけなければならない場合もあるし、また、情報の価値そのものが評価しにくいという難しさがある。また、日本の OS が一種類となるのは危険ではないだろうか。この委員会で日本における OS の多様性について議論できれば良いと思っている。

・民間ではシステム障害に対する補償を契約で定めるが、行政のシステム障害では被害を受けた市民と行政の間に契約がない。また、自治体のシステム損害により損害を被った市民が金銭的な補償を当該自治体に求め、裁判所が補償金の支払いを命じた場合、その補償金は市民からの税金が元手となる。民間では損害賠償は損害を与えた企業もしくは保険会社が支払うが、市民の税金が賠償金となる。これらが民間と行政で異なる点である。また、外交上の機密情報が漏れるなど、国家全体として国益を損なわれた場合、どのように考えるかを議論する必要があるだろう。

・セキュアOS、セキュリティ関連では防衛庁や警察庁など様々な省庁で議論されている。また、米国では国防総省がレインボーシリーズ（中でもTrusted OSの要件を定めたTCSEC-Trusted Computer Security EvaluationCriteriaという分冊が特に有名）という調達仕様書群にて、20 年近く前からセキュリティ関連の議論を進めており、軍用関連のセキュリティ基準を定

めている。本研究会では、これらの既存の調査・研究と整合性をとる必要があるだろう。また、トータルなセキュリティという視点では、追跡機能で攻撃元を突き止めることも考えられる。OS と他のセキュリティ機器との連携で達成できるようなセキュリティ機能に関しての議論も必要と思う。

・オープン性を評価軸にするよりも、改変の可能性を評価軸に入れていただきたい。

・オープンソース、クローズドソースのそれぞれに関して、安全性が高まる要件を挙げた上で、「オープン」と「クローズド」という言葉を用いた方が、オープンソースそのものを定義するよりも良いのかもしれない。

・安全かどうかは、オープン性と直接関係なく、どれだけテストをしたかではないか。たとえオープンであったとしても、見る人が少数であれば、いくら改変できても意味がない。セキュリティを定義するのに、オープンという軸を用いるのは間違っていないか。

・セキュリティ対策は完全ではないため、万が一被害を受けた時に早急に行う対策もセキュリティとして考慮しなければならない。

・システムが攻撃され、崩された時、そこから回復するためには人間が動かなければならない。人間がどうやって動かなければならないかを議論する必要があるのではないだろうか。そして、人間が動き続けるために必要な条件は何かを議論すれば良いのではないか。例えば、いくらオープンソースでもコードが混乱した状態の OS では誰も見たくなく、意味がないだろう。

・資料 3 の 4 ページに関しては、情報のこととシステムのことが混同している。情報の機密性、完全性、可用性を守ることが情報セキュリティであり、これを守るために次のレイヤーとしてシステムで対策を講じることなる。タイトルの「セキュリティ要件」では広いので、「情報のセキュリティ」として、内容もシステムの対策の話が書かれているので、機密性、完全性、可用性の次の行でとめれば良いのではないか。

・セキュリティとしては、運用をしていく中で何か起きた時にどうやって対策を行うことができるのかも重要である。例えば、どうやってコンピュータを極めて短い時間でメンテナンスできるか、パッチをどうやって安全に当てていくかということである。また、このような運用面でのセキュリティを評価する仕組みについても議論する必要があると思う。

５．その他

次回は、10 月中旬から下旬の開催を予定している。

６．閉会