資料2

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～
【概要版】（案）

平成16年3月

1　はじめに

電子政府･電子自治体をより安全に構築･運用に向けて、情報セキュリティの高度化がますます重要な課題となっている。

また一方で、近年、誰もが自由に利用可能であることを前提としたオープンソースソフトウェアとして開発されたOSに対する関心が高まり、情報システムのセキュリティ高度化の選択肢として期待されている。

このような状況を踏まえ、総務省では、平成15年6月より「セキュアOSに関する調査研究会」を開催し、わが国の電子政府･電子自治体等のシステムに利用し得る様々なOSについて、セキュリティ面を中心に運用面、コスト面等の様々な観点から検討及び評価を行ってきた。

今般、セキュアOSに関する調査研究会による調査結果及びOS選定のあり方に関する提言をとりまとめたものである。

平成１６年3月

2.1 電子政府、電子自治体をとりまく状況

電子政府・電子自治体の推進計画等

●IT戦略本部「e-Japan戦略Ⅱ」（2003年7月2日）
- 重点領域7分野の一つに「行政サービス」が挙げられ、24時間365日ノンストップ・ワンストップの行政サービスの提供、業務の効率化を目指す。

●各府省情報化統括責任者連絡会議
「電子政府構築計画」（2003年7月17日）

●総務省「電子自治体推進指針」（2003年8月）
- インターネットを通じて、原則として24時間365日、いつでもどこからでも誰もが簡便かつ安全に行政サービスにアクセスし、その便益をひろく享受することを可能とする環境の構築を目指す。

電子政府・電子自治体の進展

●電子政府の進展
- ホームページの掲載情報検索、行政手続案内や申請・届出様式の検索等のサービスを行う「電子政府の総合窓口」の機能充実
- 各府省、自治体等とのシステムと連携し、関連手続を一括してオンライン申請できるワンストップサービスの整備を計画

●電子自治体構築の進展（2003年4月1日現在）
- ホームページの開設（都道府県100%、市町村98.1%）
- 申請・届出等の行政手続きのオンライン化（都道府県19.2%）

（総務省「地方公共団体における行政情報化の推進状況調査」）

情報セキュリティ侵害事案の発生

●コンピュータウイルス等の感染被害
- ブラスターによる政府・自治体システムへの被害発生

●ホームページ改ざん
- 省庁・自治体ホームページの改ざん被害

●情報漏洩
- 自治体ホームページからの個人情報漏洩　／等

セキュリティ確保の重要性の高まり

情報セキュリティ確保に関わる取り組み

●電子政府の情報セキュリティ確保のためのアクションプラン（2001年10月）

●重要インフラのサイバーテロ対策に係る特別行動計画（2000年12月）、フォローアップ（2002年3月）

●地方公共団体における情報セキュリティポリシーに関するガイドライン（2001年3月）、一部改訂（2003年3月）

●地方公共団体における情報セキュリティ監査のあり方に関するガイドライン（2003年12月）

2.2 OSを中心とした情報システム関連全般の動向

●OSの種類

- Windows系OS
- UNIX系OS
  - 商用UNIX
  - オープンソースOS
    (Linux、FreeBSD等)

} 製品OS

} オープンソースOS

●製品OSのソースコード開示

製品OSは、ソフトウェア・メーカーが製品として販売するOS。
製品OSでも一定の条件下でソースコードが開示される。
<例>

- マイクロソフト社のソースコード開示
  - シェアードソースイニシアティブ
  - 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
  - 政府の一次契約者に対するライセンシング
- Sun Microsystems社のSolarisのソースコード開示
  - Sun Hardware Partner Program
  - Solaris 9 Source Code Program
- ヒューレット・パッカード社のHP-UXのソースコード開示

●オープンソースOSの利用の進展

ソースコードが開示され、誰でも自由に改変することが可能で、また再頒布の自由が認められているOS。代表的なOSは、Linux、FreeBSD等。

近年サーバOSの分野でオープンソースOSの利用が増加。

➢開発スタイル

Linuxの開発はコミュニティと呼ばれる個人が中心となり、ルールや命令系統の少ない方法で実施。開発プロセスはオープンにされており、公開されているソースコードをもとに開発は誰でも可能。開発の初期の段階から公開し、多くの開発者による評価・試験を受けて、頻繁に更新を行うことにより、開発スピードを早め、完成度を高めることを実現。

➢サポート体制

Linuxにバグ等が発見された場合には開発コミュニティに報告され修正。営利目的で開発されていないため、OSに瑕疵があったとしても、開発者に直接OSの修正等を強制する関係を確立できない(もっとも製品OSでも契約によりそのような強制はできないのが一般) 反面、SI等の納入者に対してOSのソースコードを知っている以上は修正を契約によって強制する関係を確立し得る。

ディストリビュータ等が販売する製品パッケージでは、一定期間のサポートサービスを提供。

ソースコードが公開されていることから、技術力のあるシステム・インテグレータ等に依頼することで、修正プログラム等の入手が可能。

※OSに脆弱性があると上位のアプリケーションをいかにセキュアに構築しても意味が無く、OSの選択や維持管理に留意が必要

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

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
＜意図的なもの＞
- 個人情報などの物理的媒体による持ち出し
- 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＞
- 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
- 不適切なID・パスワード管理による無権限使用　／等

◎外部からのアクセスを原因とする脅威・脆弱性
- ホームページ改ざん
- 不正アクセスによる情報漏洩
- DoS攻撃などサーバの運用妨害　／等

◎インターネットの利用に伴う脅威・脆弱性
- ウイルス感染
- ホームページから送りこまれたプログラムによる
  システム損壊
- セキュリティレベルの低いネットワークとの接続
  による他組織のトラブルの波及

◎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」をもとに作成

一般的な情報セキュリティ確保の要件

◎機密性の確保：
無権限アクセス、情報送出、持ち出し、盗聴の防止

◎完全性の確保：
情報の改ざん、破壊、滅失等を防止

◎可用性の確保：
サービス停止の防止、停止時間の短縮、更改時のデータのポータビリティ

情報資産・組織により求められる要件は異なる

政府・自治体で取り扱う情報資産に求められるセキュリティ要件例

	機密性	完全性	可用性
税、国保・年金、住民基本台帳、戸籍、外国人登録、印鑑登録、財務会計、人事・給与　／等	◎	◎	○
文書管理　／等	○	◎	△
グループウェア、電子メール　／等	△	△	△
電子申請、電子入札　／等	◎	◎	◎
広報、情報公開、施設予約　／等	△	○	△

◎：必須　○：重要　△：あることが望ましい

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、その他の事項

セキュリティ確保

➢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

その他の事項

➢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

4．電子政府、電子自治体向けシステムに求められる要件

(要件例) 無権限アクセスの防止／本人真性確認

【概要】

無権限アクセスを防止するためには、システムを使用することを要求してきた使用者を識別して、正当な使用者であることを確認する機能が必要である。業務によっては、各使用者の端末または所在地の識別等の確認を要する場合もある。

本人真性確認は、通常、「本人の記憶に基づくもの (パスワード等)」、「本人の所有物に基づくもの (ICカードなど)」、「本人に固有な特徴に基づくもの (生体認証 (指紋や網膜等))」の認証要素を単独又は組み合わせることにより行われる。

本人の記憶に基づく本人真性確認では、なりすまし、パスワードの盗聴、繰り返し攻撃、パスワード等を格納したファイルの盗難・辞書攻撃 (辞書単語を用いたパスワードの総当たり攻撃) 等の脅威にさらされる恐れがあり、これらに対抗できるセキュリティ機能を備えることが求められる。本人の所有物に基づく本人真性確認では、所有物の盗難等の危険性があり、本人の記憶に基づく本人認証と組み合わせること等が求められる。

本人に固有な特徴に基づく本人真性確認では、他人を本人と認識する誤認識や偽造した生体情報によるなりすまし等の危険性がある。

業務上の要件によっては、毎回変化する1回限りの使い捨てパスワードを使うワンタイムパスワードや生体認証、暗号技術を利用した認証等、より攻撃に強い認証方法を採用することも考えられる。

【実装する機能イメージ】

- □ 繰り返し使用者確認の失敗が許される上限回数を設定し、それ以上失敗した場合にアカウントをロックする等の機能を有するか。(但し、意図的に失敗を繰り返し、可用性を損なう攻撃を受ける懸念がある)
- □ 端末認証に対応できるか。
- □ ICカード等の所有物認証に対応できるか。
- □ 生体認証に対応できるか。
- □ ワンタイムパスワードに対応できるか。
- □ 暗号技術を利用した認証に対応できるか。

5．まとめ
(1)クライアントに対するまとめ

○ セキュリティ機能の確保

クライアント端末は、一般職員が直接利用するものであることを踏まえて、一般職員には設定変更が出来ないような仕組みが具備されるとともに、管理者がセキュリティ対策等を複数端末に対して一括して実施できる仕組みを備えることが必要である。

○ 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、各種メニューが適切な表現で日本語化される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ることが必要である。

○ 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。

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を選択することが求められる。

○ **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。**業務の特性を踏まえ、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のバランスを考慮しながら、OSを選択することが求められる。**

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することが求められる。

○ 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。

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する必要がある。

- **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。

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。

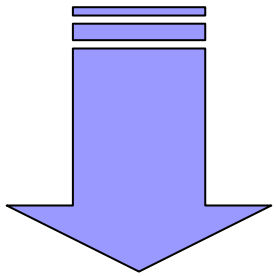
オープンソースOSは、開発者とユーザの間に直接の契約関係がないことから、OSに瑕疵があったとしても、開発者に直接OSの修正や修正プログラムの提供を強制する関係を確立できない。しかし、ソースコードが公開されていることから、システム･インテグレータ等に修正プログラムの開発を依頼することは可能である。

オープンソースOSを利用する場合には、製品OSと同等またはこれ以上の水準で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が考えられる。

おわりに

本調査研究会により、次のことが明らかに。

- **電子政府･電子自治体に用いられるコンピュータ全てに対し、最適である特定のOSを選定することは困難である。**
- **高度な情報セキュリティ水準が求められる場合には、OSのカスタマイズや追加ソフトウェアの導入が必要**



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、次のとおりと実施することが適当であると考える。

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・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・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、多様性を確保。