資料３

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 ～
(案)

◇◇　目次　◇◇

１．はじめに

現在、e-Japan 重点計画に基づく電子政府・電子自治体等の構築が進められている。電子政府・電子自治体をより安全に構築するためには、これらを構成する情報システムのセキュリティを確保する事が必要であるが、プライバシーに関する意識の高まりなどを踏まえ、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。

さらに、従来はコンピュータのオペレーティングシステム（OS）は、ベンダーから市販されているものを利用する事が当然であったが、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「Linux」と呼ばれる 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る様になった。

このような状況を踏まえ、総務省は、平成１５年６月より政策統括官（情報通信担当）主催の調査研究会として「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い、OS 選定のあり方について検討を行ってきた。

本報告書は、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。

本報告書が、電子政府・電子自治体等のセキュリティレベルの一層の向上への一助となれば幸いである。

２．電子政府、電子自治体におけるセキュリティ確保の重要性の高まり

2.1 電子政府、電子自治体をとりまく状況

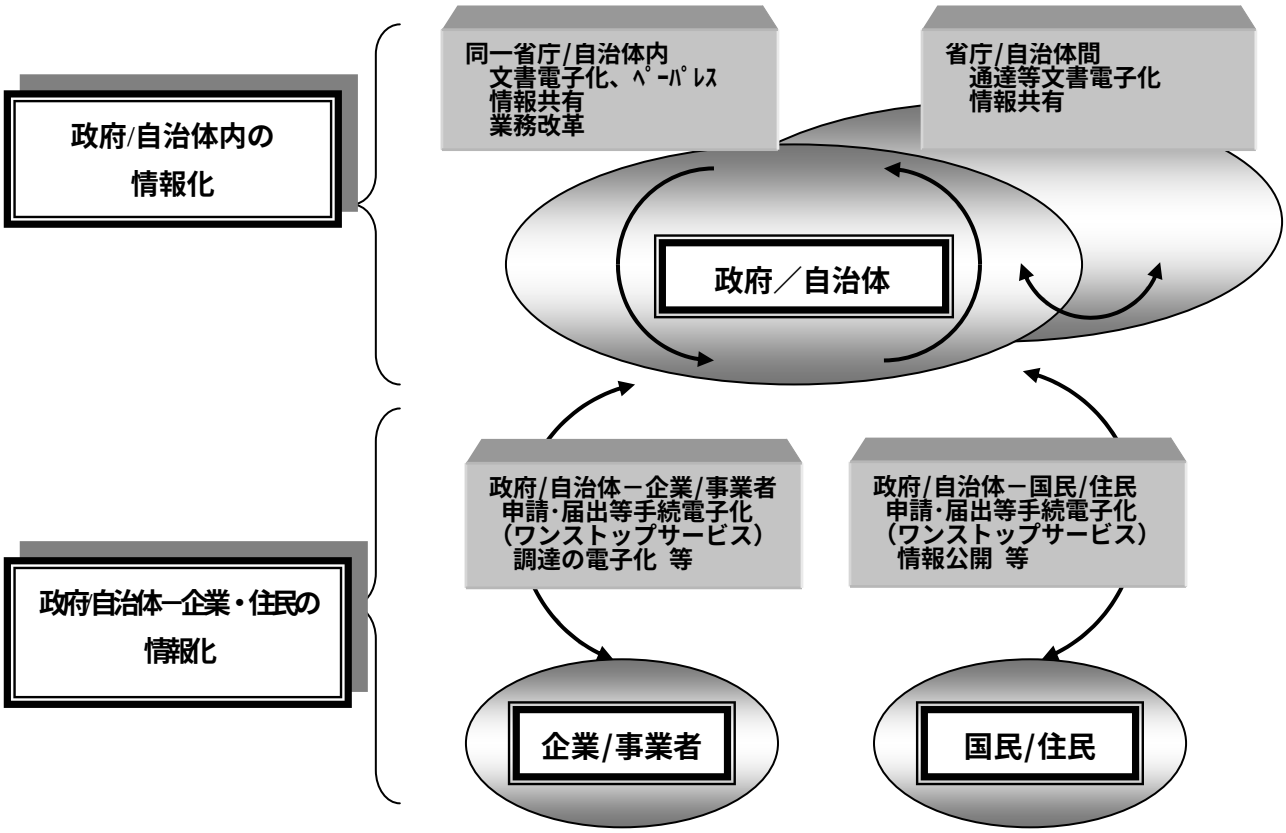
(1)政府、自治体における情報通信技術利用の広がり

情報通信技術の発展と社会の情報化の進展により、政府（中央官庁）及び自治体（地方公共団体）における情報化も急速に進んできている。1960 年代の財務・会計業務などの基幹業務の電算化にはじまり、1990 年代半ばからのインターネットの普及等によって、情報通信技術の活用は国民/地域住民、事業者へのサービス提供や広報・公聴などへと拡がりつつある。

当初、情報通信技術の活用は電算化による業務効率化をその目的としていたが、電子申請、電子入札といったサービス、ホームページ等を活用した広報活動、電子掲示板、パブリックコメント等による公聴活動など様々な業務、行政サービスを電子化することによって、行政改革、地域活性化に資することが期待できることから、「電子政府」、「電子自治体」の構築が大きな課題として、取り上げられるようになっている。

政府/自治体、企業/事業者、国民/住民といった主体に着目すると、電子政府、電子自治体は以下の図のように整理でき、行政内の情報化、行政-企業/住民の情報化の２つに大別できる。

図表2-1　電子政府、電子自治体の全体像



■政府/自治体（行政）内の情報化

電子決裁、文書の電子化、グループウェアなど行政事務の高度化、効率化を目的とした行政事務の電子化やそのためのインフラ整備。

また、霞が関 WAN など中央省庁間、自治体間における行政事務の電子化やそのためのインフラ整備。

■政府/自治体－企業・住民間の情報化

申請・届出等行政手続きの電子化や調達の電子化など利用者の利便性向上、負担軽減といった行政サービスの向上を目的とした行政事務の電子化やそのためのインフラ整備。

電子政府、電子自治体では、あらゆる業務が電子化の対象となるため、以下のような行政事務で扱われるあらゆる情報が電子的に扱われることになる（情報資産）。

■政府/自治体（行政）内

・個別業務に関連する情報（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
・グループウェア、電子メール

■政府/自治体－企業・住民間

・電子申請、電子入札
・広報、情報公開

国では、各種計画等を策定して、こうした電子政府、電子自治体の構築の推進を図っている。高度情報通信ネットワーク社会推進戦略本部（IT 戦略本部）の「e-Japan 戦略Ⅱ（2003 年 7 月 2 日）」においては、IT の利用促進に重点がおかれ、行政サービスも重点領域 7 分野のひとつにあげられ、24 時間 365 日ノンストップ・ワンストップの行政サービスを提供するとともに、業務の効率化を目指すものとしている。「e-Japan 戦略Ⅱ」の策定に引き続き、2003 年 7 月 17 日には各府省情報化統括責任者連絡会議において、今後の電子政府構築に当たっての基本的な方針と取り組みを示した「電子政府構築計画」が決定された。こうした計画に沿い、電子政府構築に向けた取り組みが行われており、例えば、ホームページの掲載情報検索、行政手続案内や申請・届出様式の検索といったサービスの提供を行う「電子政府の総合窓口」も機能充実が図られており、各府省、地方公共団体等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を整備することも計画されている。

一方、自治体を対象としたものでは、総務省（当時自治省）から 2000 年 8 月「IT 革命に対応した地方公共団体における情報化施策等の推進に関する指針」、2001 年 10 月「電子政府・電子自治体推進プログラム」と策定されてきたが、その改訂版として 2003 年 8 月に「電子自治体推進指針」が示された。この指針では、電子自治体を「地方公共団体の行政機能をバーチャルなサイバー空間に再現しようとするものであり、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を構築しようとするもの」とし、またその構築の目的として、「住民の満足度の向上」「簡素で効率的な行政運営の実現」「地域の活性化・地域 IT 産業の振興」があげられた。そして、地方公共団体における重要課題として以下の項目があげられている。

○ 電子自治体の構築を推進するための体制の整備等
- ・CIO（最高情報統括責任者）を中心とする全庁的な推進体制の整備
- ・職員の情報リテラシーの向上及び IT 専門人材の育成・確保
- ・電子自治体構築計画の策定

○ ネットワーク基盤及び認証基盤の整備
- ・庁内 LAN 及び一人一台パソコンの整備
- ・総合行政ネットワーク（LGWAN）の構築及び利用の推進
- ・住民基本台帳ネットワークシステムの構築及び運用
- ・住民基本台帳カードの積極的な活用
- ・公的個人認証基盤の整備

○ 行政手続のオンライン化の推進
- ・行政手続の簡素化・合理化の徹底
- ・申請・届出等手続に関する汎用受付システムの構築
- ・電子調達、電子申告、電子決済、電子投票の導入に向けた取組み
- ・住民等利用者の視点に立った電子自治体窓口（ポータルサイト）の実現

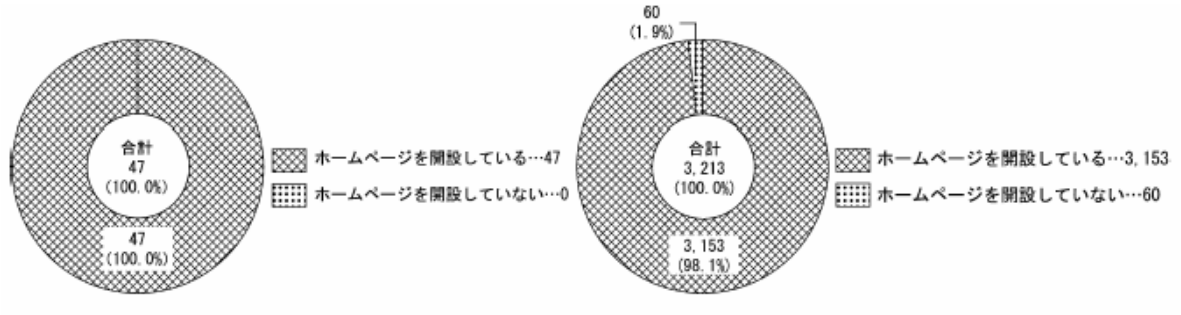
○ 住民と行政のコミュニケーションの拡大

○ 内部管理業務の電子化の推進

こうした指針等のもと、電子自治体構築の動きは着実に進んでおり、ホームページを開設している自治体はほぼ100%となっている（2003年4月1日時点）。また、申請･届出等の行政手続きのオンライン化をみると、都道府県では2割が導入済みであり、整備中、導入検討中を含めれば100%となる。市町村でも約半数の自治体が電子申請実施に向けた取り組み（導入済み8団体）を行っている。

図表2-2 ホームページ開設状況（2003年4月1日時点）

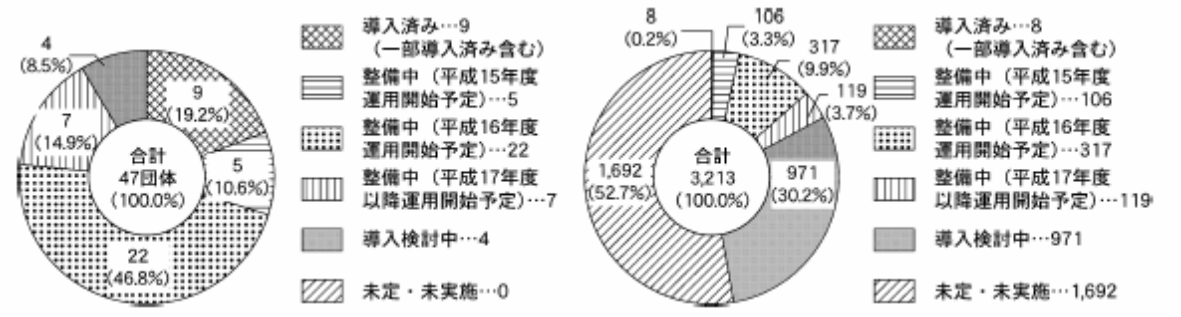
都道府県　　市町村



資料：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」2003年10月

図表2-3 申請・届出等の行政手続きのオンライン化（電子申請）の実施状況（2003年4月1日時点）

都道府県　　市町村



資料：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」2003年10月

(2)セキュリティ確保の重要性の高まり

情報システム、ネットワークの活用が広がることにより、情報システムのダウン、コンピュータ・ウイルスや不正アクセス、個人情報の流出など、様々な事件が起こるようになっている（下図参照）。特に、政府や国の機関、地方公共団体などを対象として、ホームページ改ざんなどのサイバーテロが行われたことは記憶に新しい。

図表2-4 最近の情報システム、ネットワークの被害例

インシデントの種別	概　要
ブラスター及びその亜種の感染	2003年8月に猛威を振ったMicrosoft Windowsの脆弱性を悪用したワーム「ブラスター」及びその亜種により、政府・自治体のシステムに被害が生じた。日本郵政公社、航空自衛隊、東京都庁、大阪府庁、山口県庁など全国で70以上の機関が感染し、システム障害などの実害があった。なお、当ワームの発生1ヶ月前に狙われた脆弱性の修正プログラムが提供されており、発生前までに修正プログラムを適用することで、感染を防いだ政府・自治体も多かった。
文部科学省のホームページ改ざん	2003年12月、文部科学省のシステムが不正アクセスを受け、同庁のホームページが改ざんされた。自衛隊のイラク派遣に批判する内容に書き換えられており、政府を対象とした攻撃と考えられる。
地方公共団体のホームページ改ざん	2003年度には、秋田県鳥海町、新潟県津南町などが不正アクセスにより、ホームページ改ざんの被害を受けている。
国土地理院の情報漏えい	国土地理院のホームページでデータ提供を申し込んだ利用者3505件の個人情報が、2003年9月から4ヶ月間、外部から閲覧可能な状態にあった。システムの設定ミスが原因であった。個人情報は閲覧可能な状態であっても、その個人情報が実際に流出することは確認されていない。
鳥取県の情報漏えい	鳥取県のホームページから、県行事の応募者89人と韓国の友好都市の消防隊員39人の個人情報が、最長9ヶ月間、外部から閲覧可能な状態であった。その後、インターネット掲示板に掲載されるなど、これらの個人情報が流出していたことが判明している。ともに内部資料をホームページに掲載したというミスであった。
(財)日本データ通信協会の情報漏えい	2003年6月、同協会のホームページ上の講演会申込み用のCGIに脆弱性があり、講演会申込者210人の個人情報が外部から閲覧状態であった。更に同じ脆弱性を悪用され、電子メールやウェブサイトを通じて感染するウイルス「VBS_REDLOF.A」を埋め込まれ、同協会の特定のページにアクセスするとウイルスに感染する状態にされていた。

IT が経済活動や市民生活を支える社会インフラの一部となっていることから、こうした情報システムの不具合や悪意をもった攻撃などによる被害は、住民の生活や事業者の業務に支障をきたすだけでなく、経済活動といった社会全体の活動すべてに大きな影響を及ぼすようになっており、セキュリティ確保の取り組みの重要性は、ますます高まっている。こうしたことから、セキュリティ確保のための取り組みとして、国際的にも ISO（国際標準化機構）を中心に、情報セキュリティのマネジメント体系を示した ISO/IEC17799 をはじめとして様々な標準策定などが行われ、わが国においてもこうした取り組みを受けた施策が行われるようになっている。

図表2-5 情報セキュリティに関わる主な国際標準等

名称	概　要
OECD 情報セキュリティガイドライン	1992 年に OECD が示した、情報システムのセキュリティに関する各国政府・公共部門及び民間機関の組織的かつ整合性のとれた協調的対応を可能とする枠組み。情報セキュリティの概念を示すとともに、公共部門・民間部門すべての情報システムに適用されるガイドラインとして、責任の原則をはじめとして 9 つの原則を提示。2002 年改訂。
ISO/IEC 17799	情報資産を保護するための経営管理上の対策を規定した 2000 年策定の国際標準規格。British Standard Institute（英国規格協会）から発行された BS7799 パート 1（情報セキュリティ管理実施基準）が国際標準化されたもので、わが国では JIS X 5080 が制定された。
ISO/IEC 15408	IT 関連製品及び情報処理システムのセキュリティレベルを評価する目的で 1999 年に策定された国際標準規格。わが国では JIS X 5070 が制定された。セキュリティの観点から、情報技術に関連した製品やシステムが適切に設計され、その設計が正しく実装されているかどうかを評価するための基準。
ISO/IEC TR13335	情報セキュリティ管理をするための手引書で、各組織のセキュリティレベルを確保し、維持するためのガイドライン。ISO/IEC 17799 が、「情報資産」の保護を目的としているのに対し、ISO/IEC 13335 は、「情報システム」の保護を目的に技術的な視点からみたガイドラインとなっている。

図表2-6 わが国における情報セキュリティに関わる主な制度等

名称	概　要
情報通信ネットワーク安全・信頼性基準	情報通信ネットワークの安全、信頼を図るための全体からみた対策項目について網羅的に整理、検討を行い、ハードウェア及びソフトウェアに備えるべき機能やシステムの維持と運用まで総合的に取り入れた基準。昭和 62 年策定。基準のうち一定の対策が実施されている情報通信ネットワークを登録し公表する制度として「情報通信ネットワーク安全・信頼性対策実施登録規程」がある。

情報セキュリティ評価・認証制度	**「ISO/IEC 15408（JIS X 5070）」に基づき、政府が利用するIT関連製品のセキュリティ機能・品質をチェックする制度で、2001 年運用開始。独立行政法人製品評価技術基盤機構（NITE）が経済産業省より委託を受け事業を実施している。**
情報セキュリティマネジメントシステム適合性評価制度	**日本情報処理開発協会より2002年から提供されている制度。個別の問題ごとの技術対策の他、組織のマネジメントとして自らのリスク評価により必要なセキュリティレベルを定め、プランを持ち、資源配分を行って、システムを運用する。**
情報セキュリティ監査制度	**情報セキュリティ監査を有効に普及させるための制度で、「情報セキュリティ監査」を実施する際に準拠する基準の策定、「情報セキュリティ監査」を行う主体を登録する「情報セキュリティ監査企業台帳」創設を柱とする。2003 年 4 月より運用が開始された。**

(3)電子政府・電子自治体におけるセキュリティ確保に関わる取り組み

経済活動や市民生活のベースとなるとともに、個人情報なども多く扱う行政においては、情報セキュリティの確保は特に重要であるとの認識がわが国政府においてもなされており、体制の整備及び指針策定等が行われている。

従来、各省庁では、その情報システム部門を中心としてセキュリティ確保のための対策が講じられてきた。例えば、1999 年には「行政情報システムの安全対策指針」（行政情報システム各省庁連絡会議幹事会了承）が策定されている。

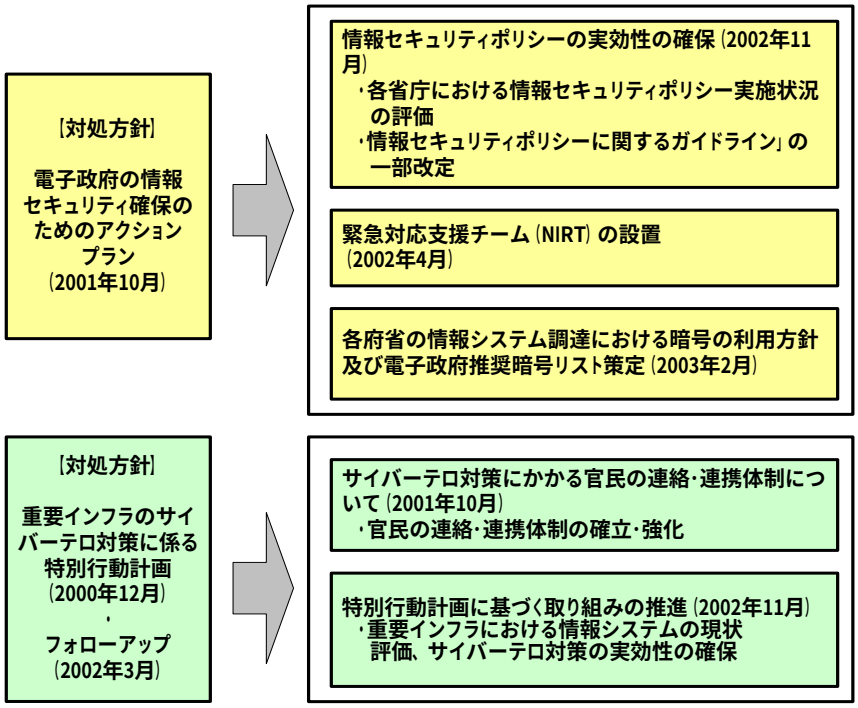
IT 戦略本部の e-Japan 重点計画（2001 年 3 月）では、「高度情報通信ネットワークの安全性及び信頼性の確保」が重点政策分野として打ち出され（「e-Japan 重点計画-2003」でも重点政策分野として取り上げられている）、そのなかで、電子政府・電子自治体に関わるものとして以下が取り上げられた。

○ 政府部内における情報セキュリティ対策
- ・情報セキュリティポリシーの評価・見直しの実施
- ・政府におけるセキュリティ水準の高い製品等の利用の促進
- ・情報セキュリティ技術評価・認証事業の実施

○ 重要インフラのサイバーテロ対策
- ・官民の連絡・連携体制の構築
- ・内閣官房における緊急対処体制の整備　/等

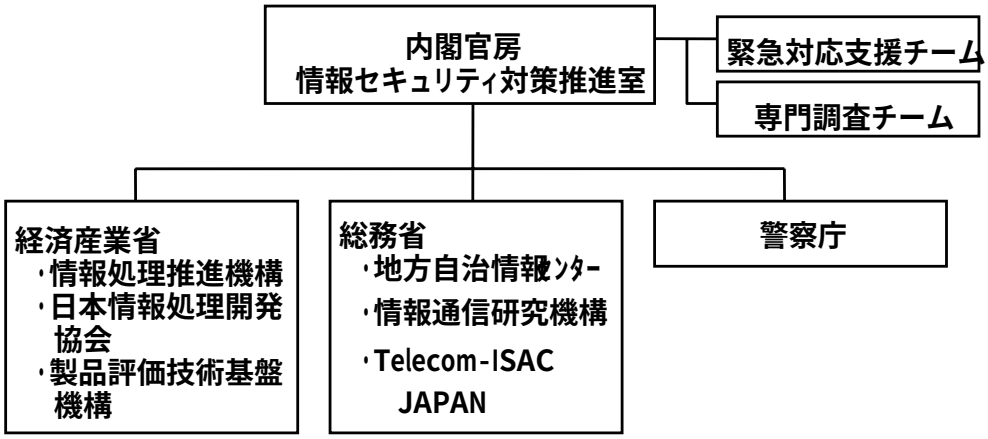
これを受け、「電子政府の情報セキュリティ確保のためのアクションプラン（2001 年 10 月、情報セキュリティ対策推進会議）」の策定、また、プランに沿った施策が行われている。

図表2-7 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及び重要インフラのサイバーテロ対策に係る特別行動計画と対応する施策等



政府のセキュリティ問題を担い、関係各省庁との連携・協力を図る内閣官房情報セキュリティ対策推進室は、2000 年 2 月に発生した官公庁の Web サイト改ざん事件を期に 2000 年 12 月に設立された。同室では、関係省庁との連携のもと、電子政府の情報セキュリティ確保や重要インフラのサイバーテロ対策など、官民における情報セキュリティ確保のための施策推進に取り組んでいる。

図表2-8 わが国における情報セキュリティ関連組織



一方、自治体においても、従来より情報化施策等の推進に当たっての情報セキュリティ確保の重要性が認識され、対策が行われてきた。例えば、昭和 62 年には、「地方公共団体コンピュータ・セキュリティ対策基準」が策定されている。近年、住民基本台帳ネットワークや総合行政ネットワークなどの稼動に伴い、情報セキュリティ確保のための取り組みの重要度を高めており、「電子自治体推進指針（総務省、2003 年 8 月）」では、「情報セキュリティ対策と個人情報保護の徹底」として、不正アクセス等による個人情報の漏洩等を防ぐための情報セキュリティ対策の重要性が指摘され、情報セキュリティポリシーの策定・運用と情報セキュリティ監査の推進、個人情報保護法制を踏まえた個人情報保護条例の制定又は見直し、情報セキュリティ研修の充実・強化が示されている。

以下に電子自治体のセキュリティ対策に関わる取り組み等を示す。

図表2-9 電子自治体の情報セキュリティに関わる取り組み等

名称	概　要
地方公共団体のためのコンピュータセキュリティに関する調査研究（2000 年 3 月）	ネットワーク利用の広がりといった情報環境変化に対応して、昭和 6 2 年に策定された「地方公共団体コンピュータ・セキュリティ対策基準」を見直し、あらためて対策基準のあるべき姿についてまとめられた。地方公共団体のためのコンピュータ・セキュリティ対策基準の具体案が示された。
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、2003 年 3 月一部改定）	地方公共団体における情報セキュリティポリシー策定に資するために、地方公共団体において情報セキュリティ対策を推進するために必要となる情報セキュリティポリシーに関する基本的な考え方、策定、運用及び見直し方法について記述したガイドライン。
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（2002 年 2 月）	地方公共団体の情報セキュリティの確保について、想定される脅威（リスク）、組織・職員の対応のあり方、人材教育のあり方等について、技術的な観点を含めた検討を行い、今後の地方公共団体における情報セキュリティ施策に対する提言として取りまとめられた。
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調査研究（2003 年 12 月）	情報セキュリティ監査の在り方について調査研究を行い、「地方公共団体情報セキュリティ管理基準」、「地方公共団体情報セキュリティ監査実施手順」「セルフチェックリスト」を「地方公共団体情報セキュリティ監査ガイドライン」として示した。これにあわせて総務省では 2003 年度中の自己点検、2004 年度中のセキュリティ監査実施を地方公共団体に要請した。また、地方公共団体からの相談等に応じるための体制の整備など、地方公共団体における情報セキュリティ監査の実施を促進していくための条件整備を進めるとした。

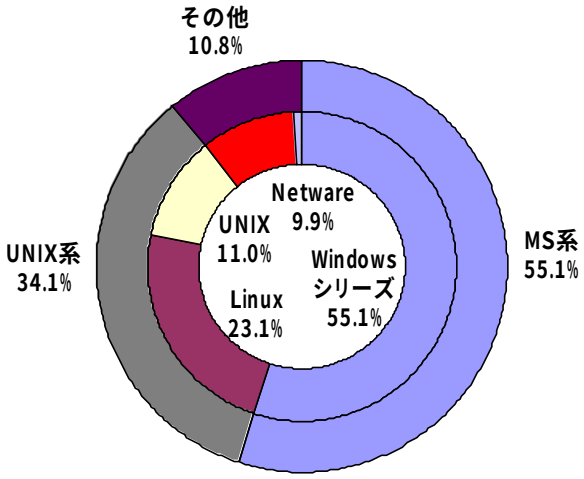
2.2 OS を中心とした情報システム関連全般の動向

情報セキュリティの面では、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いため、選択や維持運用に留意が必要である。ここでは、政府、自治体のシステムに適用される可能性がある汎用ＯＳを中心としたＯＳのトレンドについて、みていくこととする。

(1)サーバ OS

広く普及しているサーバ OS は、マイクロソフト社の Windows 系（以後、MS 系）と UNIX 系（Linux を含む）に大別できる。IDC 社の調査によると、2002 年の全世界のサーバ OS 市場における有償ライセンス出荷数のシェアは、MS 系が 55.1%、Unix 系が 34.1%であり、双方で全体の 89%を占めている。但し、これは有償ライセンス出荷数のシェアであり、ネットワークを通じて無償で頒布されている Linux 等は含まれていない。

図表2-10　サーバOS市場における有償ライセンス出荷数のシェア（2002年、世界シェア）



出所：IDC「Worldwide Client and Server Operating Environments Forecast, 2002-2007」より作成

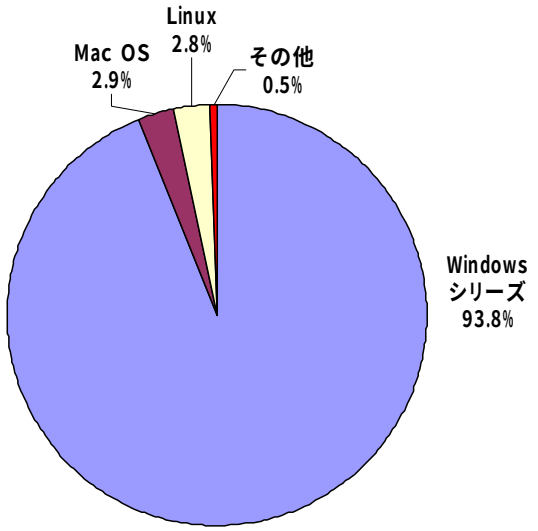
図表2-11　MS系OSとUNIX系OS（Linuxを含む）

MS 系 OS	UNIX 系 OS（Linux を含む）
1980 年代初頭よりパーソナルコンピュータ向け OS の MS-DOS を提供していたマイクロソフト社は、1985 年に GUI、マルチタスク、操作性の統一などを特徴とした OS、MS-Windows を発売した。以後、この Windows シリーズは爆発的に普及し、現在ではクライアント OS において高いシェアを有している。 サーバ OS においては、Windows シリーズの Windows サーバ（Windows Server 2003 等）がネットワークサーバ等のサーバ OS として広く利用されている。	UNIX は 1968 年に米 AT&T 社ベル研究所で開発された OS である。ハードウェアに依存しない言語（C 言語）での記述やコンパクトなソースコードにより、多くのプラットフォームに移植された。その後、学術機関やコンピュータメーカーが独自に変更を加え、多くの派生 OS が開発された。現在では UNIX に似たシステム体系を持った OS を総称的に UNIX 系と呼ぶことが多い。現在では大手コンピュータメーカーが開発している製品 OS とオープンソースの UNIX 系 OS とがある。製品 OS の UNIX は一般に商用 UNIX と呼ばれ、Sun Microsystems 社の Solaris (SunOS)、IBM 社の AIX、Hewlett-Packard 社の HP-UX などがある。オープンソースの UNIX 系 OS には、Linux や FreeBSD 等がある。UNIX 系 OS はサーバ OS として広く利用されている。

(2)クライアント OS

クライアント OS では、マイクロソフト社の Windows シリーズが高いシェアを有している。IDC 社の調査によると、2002 年の全世界のクライアント OS 市場における有償ライセンス出荷数の 93.8%を MS 系が占めている。その他に、クライアント OS としてアップル社の Mac OS やオープンソース OS の Linux 等が利用されているが、シェアは小さい。但し、これは有償ライセンス出荷数のシェアであり、無償で頒布されている Linux 等は含まれていない。

図表2-12　クライアントOS市場における有償ライセンス出荷数のシェア（2002年、世界シェア）



出所：IDC「Worldwide Client and Server Operating Environments Forecast, 2002-2007」より作成

(3)オープンソース・ソフトウェアの利用の進展

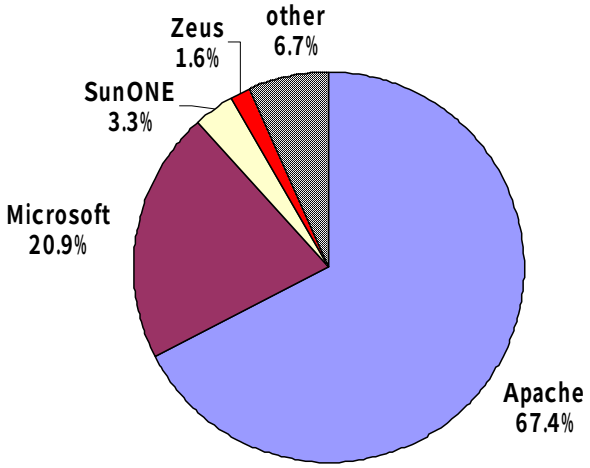
近年、特にサーバ OS において、これまでの製品 OS に加えてオープンソース OS の利用が増えてきている。

代表的なオープンソース OS である Linux は、全世界の開発者による機能拡張や安定性向上等が図られたり、国内外の大手メーカ等による Linux への対応が始められたりしたこと等もあり、普及が進展している。IDC 社の調査によると全世界のサーバ OS の有償ライセンス出荷数に占める Linux のシェアは 2002 年に約 23%に達している。国内においても、企業・団体等で OS の選択肢の一つとして位置づけられるようになっている。

また、オープンソース OS 上で利用できるオープンソース・ソフトウェアの利用も広がっている。

Netcraft 社の調査によると、2003 年 12 月時点における世界の Web サーバのシェア（利用サーバ台数）は、オープンソース・ソフトウェア Apache が 67.4%を占めており、2002 年 12 月より 5.4%の増加となっている。

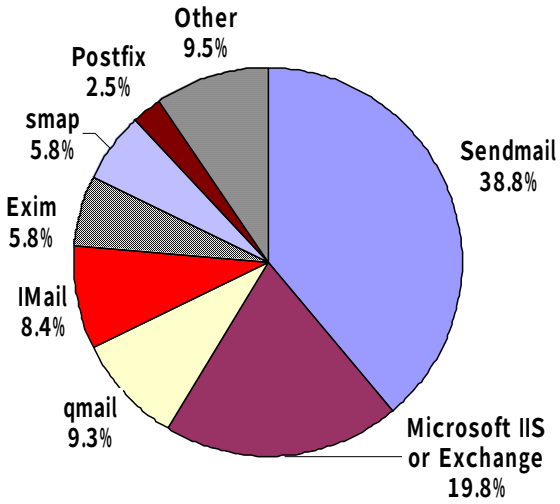
図表2-13　Webサーバで利用されているソフトウェア比率（利用サーバ台数）
（2003年12月時点、世界シェア）



出所：http://news.netcraft.com/archives/web_server_survey.htmlより作成

メールサーバにおいても、オープンソース・ソフトウェアの Sendmail がほとんどの UNIX 系 OS に標準として採用されるなど、インターネットにおける標準的なものとして位置づけられている。2003 年 4 月に実施された調査によると、全世界のメールサーバの約 39%において Sendmail が利用されている。

図表2-14　メールサーバで利用されているソフトウェア比率（利用サーバ台数）
（2003年4月時点、世界シェア）

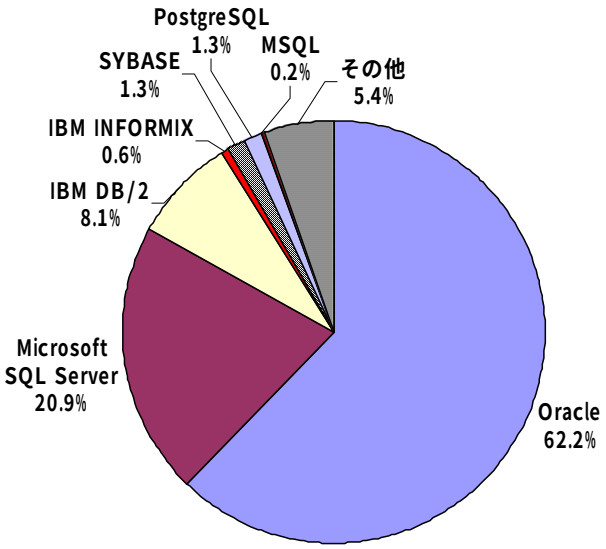


出所：http://www.credentia.cc/surveys/smtp/latest/より作成

DBMS（データベース管理システム）においては、商用ソフトである Oracle や Microsoft SQL Server、IBM DB/2 等の利用が主であるものの、PostgreSQL 等のオープンソース・ソフトウェアの利用も行われ始めている。社団法人日本情報システム・

ユーザー協会の「ユーザ企業 IT 動向調査 2003」によると、2002 年度の国内における DBMS 導入企業数のシェアトップは Oracle の 62.2%である。一方、オープンソース・ソフトウェアの PostgreSQL のシェアは 1.3%である。

図表2-15　国内におけるDBMSの採用状況（導入企業数）
（2002年度、国内シェア）



出所：社団法人日本情報システム・ユーザー協会「ユーザ企業IT動向調査2003」

ア　オープンソース・ソフトウェアとは

オープンソース・ソフトウェアとは、ソースコードが公開され、誰でも自由に改変することが可能であり、また再頒布の自由が認められているソフトウェアである。オープンソース・ソフトウェアの定義としては、オープンソース・ソフトウェアの推進活動を行う非営利団体 Open Source Initiative(OSI)によるものが用いられることが多い。オープンソース・ソフトウェアによる OS をオープンソース OS と呼ぶ。

オープンソース OS と対比する概念として、製品 OS がある。製品 OS とは、MS 系、UNIX 系にかかわらず、ソフトウェア・メーカーが製品として販売している OS であり、独占的（proprietary）OS と呼ばれることもある。

図表2-16　OSIによるオープンソースの定義（"Open Source Definition"）

①再頒布の自由 Free Redistribution
オープンソース・ソフトウェアのライセンス（以下、ライセンス）は、複数のプログラムの集合体の一部として、ソフトウェアを販売もしくは無料で頒布することを制限してはならない。また、ライセンスは、このような販売に対して使用料（royalty）もしくはその他料金を要求してはならない。

②ソースコードの公開 Source Code

オープンソースのプログラムはソースコードを含まなければならない。コンパイル済み形式だけでなく、ソースコードでの頒布も許可されなければならない。ソースコードが頒布されない場合は、複製に妥当な値段でソースコードを入手できる手段で、望むらくはインターネット経由の無料ダウンロードで用意しなければならない。また、ソースコードを意図的に分かりにくくしてはならない。プリプロセッサや変換プログラムの出力等の中間出力形式は認められない。

③変更及び派生ソフトウェア作成の自由 Derived Works

ライセンスはソフトウェアの変更及び派生ソフトウェアの作成に対して制限をかけてはならない。また、派生ソフトウェアをオリジナルソフトウェアのライセンスと同じ条件で頒布することを許可しなければならない。

④作者のソースコードの一貫性 Integrity of The Author's Source Code

ライセンスがバイナリ構築の際にプログラムを変更する目的でソースコードと共にパッチファイルの頒布を許可する場合にのみ、改変されたソースコードの再頒布を制限できる。ライセンスはソースコードを改変して作成したソフトウェアの頒布を明示的に許可しなければならないが、派生ソフトウェアにオリジナルソフトウェアと異なる名前又はバージョン番号をつけるように義務付けても構わない。

⑤個人やグループに対する差別の禁止 No Discrimination Against Persons or Groups

ライセンスはいかなる個人もしくは団体を差別してはならない。

⑥利用する分野に対する差別の禁止 No Discrimination Against Fields of Endeavor

ライセンスは特定の分野でのプログラム使用（例えば企業における使用）を制限してはならない。

⑦ライセンスの継承 Distribution of License

プログラムに付与された権利は、そのプログラムが再頒布された全ての者（団体）に対して付与されなければならない。この権利をプログラムが再頒布された全ての者に対して認めるために、追加的なライセンスを必要としない。（ソフトウェアの機密保持契約などの間接的な方法でソフトウェアを囲い込んではならない。）

⑧特定製品でのみ有効なライセンスの禁止 License Must Not Be Specific to a Product

プログラムに付与された権利は、特定のソフトウェア頒布物の一部分であることに依存してはならない。プログラムをその頒布物から抜き出しても、オリジナルソフトウェアに付与された権利と同等の権利を、プログラムを再頒布される全ての者（団体）は付与されなければならない。

⑨他のソフトウェアを制限するライセンスの禁止 The License Must Not Restrict Other Software

オープンソース・ソフトウェアと共に頒布される他のソフトウェアに対して、ライセンスは制限を加えてはならない。例えば、ライセンスは、オープンソース・ソフトウェアと同じ媒体で一緒に頒布されたソフトウェアに対して、オープンソース・ソフトウェアであることを義務付けてはならない。

⑩ライセンスは技術に対して中立でなければならない The License Must be technology-neutral

特定の技術もしくはインタフェースに依存するライセンスを禁止する。

参考：http://www.opensource.jp/osd/osd-japanese.html

オープンソース・ソフトウェアは 1990 年代末に登場したソフトウェア・ライセンスの概念であり、その原型には Richard M. Stallman 氏のフリーソフトウェア（自

由なソフトウェア）がある。

フリーソフトウェアとは、フリーソフトウェア財団（Free Software Foundation）の定義によれば、①いかなる目的であれ、プログラムを実行する自由（第 0 の自由）、②プログラムの動作を研究し、必要に応じて改変する自由（第 1 の自由）、③プログラムの複製を再頒布する自由（第 2 の自由）、④コミュニティ全体の利益になるように、プログラムを改良し、改良点を公表する自由（第 3 の自由）という 4 つの自由が認められているソフトウェアを指す。加えて第 1 の自由と第 3 の自由の前提条件として、ソースコードが入手可能でなければならない。フリーソフトウェアの目標は、誰もが自由に使用できる自由なソフトウェアを開発し、自由に共有することによって、独占的なソフトウェアに頼らずとも済むようにすることである。

しかしながら、こうした Stallman 氏の思想にはややもするとビジネスと相容れない方向で極端に解釈されがちな部分もあった。その後、Linux の普及などを受けて、フリーソフトウェアへの関心が高まる中で、OSI により、フリーソフトウェアの思想を汲みながらビジネスにも受け入れられやすいようにしたオープンソース・ソフトウェアの概念が定義された。

イ　代表的なオープンソース・ソフトウェアのライセンス

オープンソースの概念は OSI の定義により定められているが、オープンソース・ソフトウェアのライセンス形態は一様ではない。具体的なライセンス内容は個々のオープンソース・ソフトウェアによって異なることが多い。OSI では、2004 年 1 月時点で、47 ライセンス（同名ライセンスの異なるバージョンを含む）をオープンソース・ソフトウェアのライセンスとして認定している。

以下に代表的なオープンソース・ソフトウェアライセンスである GNU GPL（GNU General Public License）と Berkeley Software Distribution License（BSD ライセンス（修正版））の概要を整理する。

①GNU GPL（GNU General Public License）

GNU プロジェクトのソフトウェア・ライセンスである。派生物及び派生物を含む頒布物全体に対しても GPL が適用されることを条件に、ソフトウェアの複製・再頒布、使用、変更・修正の自由を保証する。ソースコードは入手可能でなければならない。つまり、GPL ソフトウェアを改変すると、改変部分のソースコードを公開し、誰でも複製・再頒布、使用、変更・修正を自由に行えるように

しなければならない。排他的プログラムへの統合を禁止している。

②BSD ライセンス（修正版）(Berkeley Software Distribution License)

再頒布の際に、著作権表示、再頒布条件表示及び無保証かつ責任を負わない旨の宣言をすることを条件に、ソフトウェアの複製・再頒布、使用、変更・修正を行うことができる。また、改変後のソースコードの開示義務はないため、コードを非公開にし、独占的プログラムとリンクすることができる。

ウ　代表的なオープンソース OS

①Linux

Linux は、1991 年、当時フィンランドの大学生であった Linus Torvalds 氏によって開発された UNIX クローンなオペレーティング・システムであり、コミュニティの多くの開発者の協力を得て、頻繁にバージョンアップがなされている。Linux は、GNU GPL の適用を受けるオープンソース OS であり、インターネット等により誰でも無料でダウンロードすることが可能である。しかし、Linux を利用するために必要又は有用なプログラムを個別にインストールする作業は煩雑であり、これらのプログラムをパッケージ化したディストリビューションが利用されることが多い。

②FreeBSD

FreeBSD はカリフォルニア大学バークレイ校が開発した BSD（Berkley Software Distribution）版 Unix4.4 BSD Lite をもとに、Intel 社製プロセッサを搭載した PC で動作するように改良された OS であり、BSD ライセンスに基づいたオープンソース OS である。ボランティアの開発者により開発が進められている。

エ　オープンソース OS の開発体制とサポート体制

ここでは代表的なオープンソース OS である Linux の開発体制、サポート体制について整理する。

①開発体制

Eric Steven Raymond 氏の論文「伽藍とバザール」[1]の中で示されているよう

[1] 1997 年の発表後、幾度か改訂されている。
原文の最新版は http://www.catb.org/~esr/writings/cathedral-bazaar/に掲載されている。

に、ソフトウェアの開発方法は、「伽藍方式（Cathedral）」と「バザール方式（Bazaar）」に大別できる。

伽藍方式は、少数の優れた開発者だけで計画及び体制を築き、そのグループ内で開発が行われ、ある程度まとまるまでプログラムを公開しない開発手法である。開発の経過は部外者には非公開であることが多い。大聖堂（Cathedral）の建築のように、大掛かりな開発であることから、Eric Steven Raymond 氏が「伽藍方式」と名付けた。現在、一般的に営利企業で取り入れられている手法である。

一方のバザール方式では、従来の大規模開発等とは異なり、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により開発が進められる。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、開発スピードを速め、完成度を高めるといったことが実現されている。

Linux の開発はバザール方式で行われている。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、開発は誰でも行える。開発者のコミュニケーションはメーリングリストを通じて行われている。メーリングリストでは、開発の方向性等に関する議論についても行われ、開発者のコンセンサスの形成が図られている。

個々の開発者が開発したソースコードは、メールを介して、Linux のコアチームに対して提案される。提案されたソースコードは、コアチームにより評価され、最終的には Linux の開発者である Linus Torvalds 氏によって、公式なバージョンに採用されるかどうかが判断される。コアチームは、ネットワーキング、ヘルプシステム、グラフィックスなど Linux のサブシステムの開発リーダーを務めるメンテナーと呼ばれる開発者によって構成されている。

オープンソース・ソフトウェアであっても、より組織だった開発モデルを採用する場合もある。例えば、Web サーバの Apache では、より組織だった開発を続けていくために The Apache Software Foundation が設立されている。

②サポート体制

・開発コミュニティによるサポート

Linux にバグやセキュリティホール等が発見された場合には、開発コミュニティのメーリングリストに報告され、議論がなされる。Linux の開発コミュニティにおけるメンテナーと呼ばれる開発リーダーが報告を受けた箇所の修正を

行うことが多いとされている。

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ことに留意する必要がある。もっとも製品 OS でも契約によりそのような強制は行えないことが一般的である。反面、システム・インテグレータ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によるサポート

ディストリビュータが販売する製品パッケージには、インストールプログラムやマニュアル等があり、動作環境等の検証も行われた上で提供される。

製品パッケージには、Linux の導入や設定、利用方法等に関する単純なユーザ・サポートサービスが一定期間、無償で提供されるケースが多い。無償で入手したディストリビューションの場合には、こうしたサポートサービスを受けることはできないが、別途、有償でサポートを購入できる場合がある。

ユーザ・サポートサービスの他に、Linux システムの導入支援や運用支援、技術支援、教育研修サービス等の提供を行うディストリビュータもある。

・システム・インテグレータによるサポート

システム・インテグレータでは、インストールや運用、他の OS システムからの移行等に関する支援、教育研修等のサービスを提供している。また、障害などが発生した場合の技術支援サービスもある。開発コミュニティやディストリビュータによる修正が期待できないバグ等があった場合でも、Linux のソースコードが公開されていることから、利用者が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によって、バグ等の修正が行える可能性はある。

・サードパーティによるサポート

ディストリビュータが販売する製品パッケージには、通常、サポートサービスが一定期間提供される。

ディストリビュータのサポートサービス終了後、そのディストリビュータに代わって、セキュリティパッチやバグフィックスなどのアップデートを有償で継続的に提供するサードパーティもある。

(4)製品 OS のソースコード開示

オープンソース OS と対比する概念として、製品 OS がある。製品 OS とは、MS 系、UNIX 系にかかわらず、ソフトウェア・メーカーが製品として販売している OS であり、独占的（proprietary）OS と呼ばれることもある。

製品 OS でも一定の条件下でソースコードの開示が行われている。

ア　マイクロソフト社のソースコード開示

①シェアードソースイニシアティブ

製品 OS 開発とオープンソース・ソフトウェア開発の両方の長所を取り入れるため、2001 年 5 月、マイクロソフト社はシェアードソースイニシアティブ（SSI）を開始した。SSI では、ソフトウェア業界のイノベーションを維持するために重要な知的財産はマイクロソフト社が保持したまま、顧客、パートナー、独立系デベロッパ、研究者、学生、関心を持つ個人ユーザなど、より広範なユーザが MS 系 OS のソースコードを入手できるようにした。

ソフトウェア開発者の世界的なコミュニティの成長を促進し、ソースコードを入手した開発者が自由に新しいソリューションを考え出し、ビジネス等に活かすことができるライセンシングとなっている。また、研究ツール及び教育ツールとして世界中の大学にソースコードを提供している。ライセンシングの対象者、対象とする OS の種類に応じて、様々なプログラムが用意されており、ソースコードの扱いは各プログラムで異なる。例えば、政府機関・自治体等を対象としたプログラムはガバメント・ソース・ライセンシング・プログラム（GSLP）であり、このプログラムではソースコードを参照できるが、改変等はできない。

図表2-17　主なシェアードソースプログラム及びライセンス

名称	概要
エンタープライズ・ソース・ライセンシング・プログラム (ESLP)	顧客である企業がデバッグを含めた社内での開発及びサポート目的で、Microsoft Windows ソースコードにアクセスが可能。
システムインテグレータ・ソース・ライセンシング・プログラム (SISLP)	Windows プラットフォームを利用して優れたカスタマサポートとコンサルティングを提供するために、システム・インテグレータは、ソースコードにアクセスすることができる。
OEM ソース・ライセンシング・プログラム (OSLP)	OEM カスタマを対象としたプログラム。Windows ベースの OEM ハードウェア製品の開発及びエンドユーザーサポートの参考のために Windows ソースコードにアクセスできる。

マイクロソフト・リサーチ・ソース・ライセンシング・プログラム (MRSLP)	ライセンスを付与された機関の研究者、教員、スタッフ、及び学生を対象としたプログラム。教育目的及び政府機関と産業分野での委託研究のために提供しているソースコード及び関連機密情報を使用、複製、及び修正できる。
ガバメント・ソース・ライセンシング・プログラム(GSLP)	政府機関・自治体等を対象としたプログラム。組織内に導入された Windows プラットフォームで実行するアプリケーション及び製品の開発とサポートの目的で Windows ソースコードにアクセスすることができる。これは、ESLP を基盤としており、私的組織と公的機関のライセンシングの違いを補うよう設定されている。

資料：マイクロソフト社資料より作成

②ガバメント・セキュリティ・プログラム

2003 年 1 月に発表された Government Security Program (GSP)は、Windows プラットフォームのセキュリティに対する信頼を高めるために、各国政府に対して、必要な Windows のソースコード及びその他の技術情報へのアクセスを一定条件のもとに提供するプログラムである。GSP では Windows のソースコードへのアクセスを無償で提供している。また、マイクロソフト社と政府との情報交換などを通じて、より緊密で相互に信頼できるパートナーシップを確立する。GSP は、世界 60 カ国以上が参加資格をもつプログラムであり、ロシア、NATO、英国、中国、台湾をはじめとして、複数の国や国際機関が参加を表明している。

GSP は、国（政府）向けのプログラムであり、地方自治体を対象にしたものではない。また、ソースコードのリファレンスは専用のツールを利用してオンラインで行うため、ソースコードの改変等を自分の環境で行うことはできない。政府のシステムに関わるコンサルタント、システム・インテグレータは、契約の元、リファレンス可能だが、政府のシステム構築を手がける事業者に対して、政府との契約前に GSP を適用することはできないため、入札時の段階で収集できる情報が少ないことが想定される。

図表2-18　GSLPとGSPの比較

ガバメント・ソース・ライセンシング・プログラム (GSLP)	ガバメント・セキュリティ・プログラム（GSP）
・ サポートを主眼としたコードアクセスの提供 ・ マイクロソフト製品を使用する政府機関にソースコードへのアクセスを提供 ・ 暗号化技術の提供なし ・ コード関連文書の提供なし ・ 研究施設を利用したり、検証したりする機会なし ・ 企業向けソース・ライセンシング・プログラムと類似 ・ マイクロソフト製品のユーザとして政府機関を対象としたプログラム ・ 対象を米国、EU＋8 カ国に限定（計 26 カ国）。 ・ 国内で複数の GSLP ライセンスの取得が可能（政府機関による調整は不要） ・ 2001 年秋より開始	・ セキュリティの解析を主眼としたコードアクセスの提供 ・ 政府と信頼関係のあるパートナーシップを確立するためのより広範なフレームワーク ・ セキュリティの解析を行えるようにソースコード（暗号化技術を含む）へのアクセスを提供 ・ マイクロソフト製品ユーザである必要なし ・ マイクロソフト米国本社訪問など、パートナーシップ確立のための積極的な対話 ・ より広範な国々を対象（現在 60 カ国以上が参加可能） ・ （政府が希望する場合は）調整役をつとめる政府機関が、政府に代わってソースコードにアクセス ・ 2003 年 1 月より開始

資料：マイクロソフト社資料より作成

ウ　IBM 社の AIX のソースコード開示

①政府の一次契約者に対するライセンシング

IBM 社は、通常、AIX のオブジェクト・コードのみをライセンスしているが、AIX のソースコードへのアクセスを必要とする政府プロジェクトにおいては、そのプロジェクトの一次契約者（SIer）に対して、AIX ソースコードを別途有償でライセンスしている。AIX ソースコードのライセンシングは、IBM 社と一次契約者との間で締結する機密保持契約の下に行われるが、この契約には知的財産に関する追加的な条項が含まれる。なお、一次契約者は、AIX ソースコードのライセンシングの前提条件となる、第三者のソースコード（ATT System V 3.2 等）にアクセスできる権利を有している必要がある。

②政府に対する開示

政府に対する AIX ソースコードの開示に関して、IBM 社は、「AIX ソースコードを貴重な会社の資産と考えているため、政府から要請があった場合には、IBM 社の知的財産を保護しつつ、政府の基本的な要求を満たすことの可能性を探るため

の協議を行いたい」としている。

エ　Sun Microsystems 社の Solaris のソースコード開示

Solaris のソースコードについては、製品開発、研究や保守を目的とする一定の条件のもとに開示されている。

これにより、ハードウェアを開発するベンダーが Solaris を稼働させるのに必要な改変を施したり、Solaris を販売保守するベンダーが高度な顧客技術支援提供したりすることが可能となる。

現在、Solaris 9 について、教育機関に対し、Sun Microsystems 社が開発した最新技術を共有する事により、新たな研究への支援を提供する。開示されている Solaris のソースコードには、カーネル、ネットワーク機能、ファイルシステム、ウインド環境等が含まれる。

Solaris のソースコードは以下に示すプログラムにて提供される。

①Sun Hardware Partner Program (SHWP)

ハードウェアを開発する OEM パートナー向けのプログラム。Solaris をベースとする、OEM ハードウェア製品の開発及びエンドユーザーサポートの為に Solaris ソースコードにアクセスする事が可能。

さらに、OEM ハードウェア製品に対応した Solaris のバイナリライセンスを再配布する事も可能である。

②Solaris 9 Source Code Program

- Solaris Partner Source

  Solaris を販売保守する Sun Microsystems 社のパートナーが、自社のユーザサポートの為に Solaris へのソースコードを参照する事が可能。

- Education Partner Source

  教育機関を対象に、研究や教育を目的とした、Solaris のソースコードへの参照を提供。

オ　ヒューレット・パッカード社の HP-UX ソースコード開示

ヒューレット・パッカード社(以下 HP 社)は、自社のエンタープライズ 64bit UNIX OS である HP-UX に関して、そのソースコードへのアクセスを一定条件(契約に定められる)のもとに許可するための製品を従来より有償で提供している。

この製品は、HP-UX ソースコード製品(SCP:Source Code Product)と呼ばれている。(以下 HP-UX SCP と表記)

HP-UX SCP は、システム・インテグレータや大手ユーザに社内でのアプリケーション開発やサポートを目的とする HP-UX ソースコードへのアクセスを提供するために用意されたものである。

HP-UX ソースコードを利用することで、社内においてトラブルシュートなどのサポート活動や、アプリケーションの移行・開発などをより詳細なレベルで高度に実施することが可能となる。

HP-UX SCP により提供されるソースコードは、HP 社の企業秘密であり、その取り扱いには制限があることに注意すべきである。提供されるソースコードに関する知的財産権は、すべて HP 社が所有し、第三者へのサブライセンス、再ライセンス、提供、移管、開示などは許可されない。また、ソースコードは、参照のみが許可され、改変及びビルド作業、他のソフトウェアへの部分的な利用も許可されない。また、米国政府の輸出規制や、HP 社以外から提供されている部分についてはその提供元との契約などの制約により、HP-UX SCP では提供されないコードやモジュールがあることにも注意する必要がある。

(5)Trusted OS とセキュア OS

OS の脆弱性を狙ったコンピュータ・ウイルスやワームや不正アクセスの被害の増加等による情報セキュリティ意識への高まりに伴い、Trusted OS やセキュア OS が注目されている。

Trusted OS とは、1985 年の米国国防総省指令で規定されたセキュリティ製品の評価基準 TCSEC (Trusted Computer System Evaluation Criteria)及び TCSEC の補足規定集(レインボーシリーズ)において、B-Division に準拠する全てのセキュリティ機能を有しており、B-Division 以上の認定を受けたオペレーティング・システムのことである。

Trusted OS とは、元来 TCSEC において TCB（Trusted Computing Base）として表現された概念が OS に適用されたことが起源であると考えられる。構造的なセキュリティを実現するためには、システムの保護機構は不正がなく下位層から体系的に実装されているべきであるとされている。その意味では、一定の体系的かつ定量的な機能要件と保証要件について、第三者の信頼できる機関により評価が行われ認証されていることが重要である。

セキュア OS とは、TCSEC B-Division に準拠するセキュリティ機能を部分的に有するオペレーティング・システムを指すことが多い。また、Trusted OS とは異なり、政府機関や第三者機関による認定を必要としない。

なお、TCSEC に始まるレインボーシリーズや欧州の ITSEC の策定後、国際的な統一基準の導入の必要性が高まり、アメリカ、イギリス、オランダ、カナダ、ドイツ、フランスの 6 カ国で国際統一基準作成プロジェクト「Common Criteria (CC)プロジェクト」が始まった。1999 年 6 月には CC プロジェクトで策定された国際基準 CC を ISO 標準化し、「ISO/IEC15408 情報技術セキュリティ評価基準」が制定された。我が国においても 2000 年 7 月に ISO/IEC15408 に対応する国内標準として JIS X 5070 が制定されている。

ISO/IEC15408 は、情報技術セキュリティの観点から、情報技術に関連した製品やシステムが適切に設計され、その設計が正しく実装されているかどうかを評価するためのセキュリティ評価基準となっている。米国においては、以下のプロテクション・プロファイルが定義され、いくつかの OS について認証されている。

・CAPP（Control Access Protection Profile）
・LSPP（Labeled Security Protection Profile）
・RBACPP（Role-Based Access Protection Profile）

３．電子政府、電子自治体の構築にあたり意識すべき事項

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

(1)電子政府・電子自治体に対する脅威・脆弱性の例

情報セキュリティに関連する脅威・脆弱性のなかで、電子政府・電子自治体として特に注意すべきものとして、図表 3-1 に示すものがあげられる。特に、汎用受付システム（電子申請）といった外部とのアクセスや、霞ヶ関 WAN、総合行政ネットワーク、住民基本台帳ネットワークなど官庁、地方公共団体間を結ぶネットワーク、システムの構築が進められるなか、ネットワークに関わる脅威はますます大きくなっていくものと想定される。例えば、総合行政ネットワークにより地方公共団体が相互接続されることによって、セキュリティ対策の水準が低い地方公共団体がセキュリティホールになり、ネットワーク全体の脅威となりかねない。

図表3-1 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	
意図的な行為によるもの	**･ 個人情報のリストなどの物理的媒体による持ち出し（紙、電磁媒体等）** **･ 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	**･ 電子メールの送信誤りなど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** **･ 長期間パスワードを変更しないなど不適切なユーザ ID･パスワード管理による無権限使用** **･ PC の紛失･盗難、廃棄･返却時等の情報漏洩** **･ 設計、運用システム管理に関連する資料の不適切な管理によるネットワーク仕様の外部流出**
■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などネットワーク経由の不正アクセスによるデータ改ざん **･ ネットワーク経由の不正アクセスによる個人情報流出などの情報漏洩** **･ スパムメールの中継など不正行為の踏み台** **･ DoS 攻撃などサーバの運用妨害**	
■インターネットの利用に伴う脅威･脆弱性	
ウイルス感染によるもの	**･ 個人所有 PC 経由でウイルスに感染** **･ メールを経由したウイルス感染** **･ サーバ間のアクセスで広がるワームに感染**
受動的攻撃サイトへのアクセスに伴うもの	**･ ホームページから送り込まれたプログラムによるシステム損壊･保存情報の漏洩**
セキュリティレベルの低いネットワークとの接続に伴うもの	**･ 他組織のウイルス感染などのトラブルが自組織にも波及**
■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」（2002年2月）を元に作成

(2)電子政府・自治体で取り扱う情報に求められる情報セキュリティ確保の要件

OECDが1992年に発表した”Guideline for the Security of Information Systems”により、情報セキュリティ確保のための手段として、機密性（Confidentiality）の確保、完全性（Integrity）の確保、可用性（Availability）の確保が挙げられた。その後、この三点は情報セキュリティを考慮する上で重要な要件として定義されるようになった。しかし、インターネットの発展、情報システムの普及等の情報環境の変化にともない、情報セキュリティの目標事項にこれら三点だけでなく、真正性（Authenticity）の確保、責任追跡性 (accountability)の確保等を加えることも多くなった。

図表3-2　情報セキュリティ確保のための一般的な手段

機密性の確保	情報ごとに許可された者だけが読み出しができること
完全性の確保	情報の改ざん、破壊、滅失等を防止することができること
可用性の確保	サービス停止の防止、停止時間の短縮を図ることができること
真正性の確保	利用者、処理方法、システム及び情報が実態通りに識別されることを保障すること
責任追跡性の確保	情報に証拠を提供し、実際の行為者が責任を避けることを防ぐことができること

図表3-2の要件のうち、真正性の確保、責任追及性の確保についてはある特定の情報よりも、一連の行為等に対して必要とされる側面が大きいため、ここでは電子政府・自治体で取り扱う情報に求められる要件の整理・分類を行うことを主眼として機密性の確保、完全性の確保、可用性の確保の観点から整理・分類を実施した。

ア　機密性が求められる情報

政府・自治体が取り扱う情報には、個人情報をはじめとした機密性の確保が求められる情報がある。機密性が求められる情報としては、例えば、情報公開法における不開示情報がある。情報公開請求に対して、不開示にできる情報は、不開示とする以上、漏洩防止など機密性の確保が求められる。

図表3-3　機密性が求められる情報例

・情報公開法に定められる不開示情報（政機関の保有する情報の公開に関する法律第五条第一項から第六項）

① 特定の個人を識別できる情報（個人情報）
② 法人の正当な利益を害する情報（法人情報）
③ 国の安全、諸外国との信頼関係等を害する情報（国家安全情報）
④ 公共の安全、秩序維持に支障を及ぼす情報（公共安全情報）
⑤ 審議・検討等に関する情報で、意思決定の中立性等を不当に害する、もしくは不当に国民の間で混乱を生じさせる恐れのある情報（審議検討等情報）
⑥ 行政機関又は独立行政法人等の事務・事業の適正な遂行に支障を及ぼす情報（事務事業情報）

・機密性が求められるその他の情報例

処理中の許認可・登録等の申請にかかる情報　等

イ　完全性が求められる情報

壊されたり、改ざんされたりしてはならない情報がある。そのような情報は完全性が求められる情報である。完全性が求められる政府・自治体で取り扱う情報の例としては、許認可・登録等の申請文書、処分書など原本に相当する情報、政策等の審議、検討、決定に関する文書、政策等を公表する文書（公開情報）などである。また、起案・決裁文書等についても完全性が求められる。

図表3-4　完全性が求められる情報例

① 許認可・登録等の申請文書、処分書
② 政策等の審議、検討、決定に関する文書
③ 政策等を公表する文書
④ その他の起案、決裁文書　等

ウ　可用性が求められる情報

可用性が求められる情報とは、使いたい時にいつでも使うことができるように、常

に使用可能な状態にしておかなければならない情報である。例えば、許認可・登録の申請は、常に申請書類を確実に受理しなければならない。したがって、許認可・登録等の申請にかかる情報には可用性が求められる。

図表3-5　可用性が求められる情報例

①　許認可・登録等の申請にかかる情報　　等

エ　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

上記の分類を踏まえた上で、一例として政府・自治体で取り扱う具体的な情報資産について、それぞれの求められるセキュリティ要件及びその重要度をまとめた。ただし、一概に政府・自治体といえども、組織によって取り扱う情報そのものが異なり、求められるセキュリティ要件やその重み付け等も異なることに留意が必要である。

例えば、住民基本台帳や戸籍等は個人情報であり、情報公開法上の不開示情報として機密性が求められるだけでなく、改ざんや破壊されてもならないため、完全性の確保も必須となる。しかしながら、これらの情報の可用性については、業務時間帯には確実に使用できなければならないものの、必ずしも 24 時間常に使える状態までは求められない場合がある。このような場合には、可用性の確保は重要であるが、必須ではないと言える。ただし、政府・自治体によっては、24 時間、確実に使用できることを要求する場合も想定される。その場合には可用性の確保は必須条件となる。このように、それぞれの組織によって求められるセキュリティ要件や重要性は異なり、下表はあくまでも一例であることに留意しなければならない。

図表3-6　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　／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の方策

電子政府、電子自治体で取り扱う情報に関するセキュリティを確保するために、機密性の確保、完全性の確保、可用性の確保、真正性の確保、責任追跡性を確保するための方策を情報システムに講じる必要がある。ここでは、個々にその必要性について整理する。

(1)機密性確保の必要性

ア　無権限アクセスの防止

電子政府、電子自治体における情報システムでは、法令等に基づいて取得・保有する多数の個人情報等を取り扱うことから、機密性の確保が必要である。特に近年、庁外とのネットワークによる接続や庁内のネットワーク化が進展し、これらの情報資産への内外からのアクセス経路が多様化していることから、機密性に対する脅威が増大していくことが懸念される。

機密性を確保するためには、これらの情報へのアクセスや処理は、権限を与えられた者だけが行えるようにし、権限の無いもののアクセスを防止しなければならない。そのためには、本人真性確認、ユーザごとのアクセス制御、アクセスログ、侵入検知、ポリシーの設定・運用及び監査等の取り組みを行うことが必要となる。

イ　ウイルス対策

コンピュータ・ウイルス等の中には、感染後、システム内部の情報を外部に送信するといった動作を行うものがある。万一、こうしたコンピュータ・ウイルス等に感染した場合、機密性の高い情報が外部に流出する恐れがある。

そのため、コンピュータ・ウイルス等への感染を防止する仕組みが必要である。具体的には、コンピュータ・ウイルス等による情報流出への対策、プロセス監視、対策の恒常的な維持・運用及び監査等が必要となる。

ウ　データの保管／持ち出し、情報送出の防止

政府、自治体では法令等に基づいて取得・保有する個人情報等が多数あるとともに、これらの情報を長期的に保有する必要がある。

機密性を保ちながら、これらの情報を保管するためには、職員が許可なくこれらの情報を庁外へ持ち出すことやメール等により庁外へ送信すること等を防がなければならない。また、誤操作等により情報が外部へ送出されることを防止することも必要である。

そのためには本人真性確認、ユーザごとのアクセス制御、アクセスログ、フールプルーフ、情報フロー制御、暗号制御、対策の恒常的な維持・運用及び監査等の取り組みが必要となる。

エ　推論攻撃対策

公開されているデータベースに対して、工夫して行った検索結果を複数組み合わせて分析することにより、非公開情報である機密情報やプライバシーを推測するといった推論攻撃が行われる危険性がある。電子政府、電子自治体においては、個人情報等の機密情報を数多く取り扱うことから、データベースを実装する際には、推論制御など、推論攻撃を防ぐための対策が必要となる。

(2)完全性確保の必要性

ア　情報改ざんの防止

電子政府、電子自治体で取り扱う情報の中には、各種証明の基本情報となるものが多く含まれており、これらの情報が改ざんなどの被害を受けると、個人や法人の利益を損なったり、行政事務の執行等に影響を及ぼしたりする危険性がある。こうした被害を生じさせないために、情報の改ざんを防止する仕組み、情報が改ざんされているかどうかを判断する仕組み、情報が改ざんされていることが分かった場合にバックアップされている情報から元の正しい情報に復旧できる仕組みを備える必要がある。

そのため、本人真性確認やユーザごとのアクセス制御、アクセスログ、データバックアップ、ポリシーの策定・運用及び監査等が必要である。

イ　情報破壊、滅失の防止

電子政府、電子自治体で取り扱う情報には、破壊や滅失などの被害を受けることにより、個人や法人の利益を損なったり、行政事務の執行等に影響を及ぼしたりする危険性がある。このような被害を防ぐためには、権限を有さない者が情報にアクセスし、破壊、滅失するのを防ぐことだけでなく、権限を有する者が誤って情報を破壊、滅失することについても防がなければならない。また、情報破壊、滅失が発生したことを検知する仕組み、情報破壊、滅失が発生した場合に、バックアップされている情報から元の情報を復旧できる仕組みを備える必要がある。

そのためには、本人真性確認やユーザごとのアクセス制御、アクセスログ、ロールバック機能、データバックアップ、ポリシーの策定・運用及び監査等が必要である。

(3)可用性確保の必要性

ア　サービス停止の防止

電子政府、電子自治体の実現により、行政文書の電子化、ペーパレス化及び情報ネットワークを通じた情報共有・活用や、国民や住民、企業等との間の行政手続きのオンライン化が行われる。この結果、原則として行政手続きが 24 時間受付可能となり、国民や住民、企業の利便性の向上が期待される。これに伴い、これらの情報システムがいつでも利用したい時に利用できないと、国民や住民、企業の利便性が損なわれたり、行政執行に支障が生じたりする恐れがあり、電子政府、電子自治体が円滑に機能しなくなる。そのため、できるだけサービス停止が発生しないよう可用性を確保する取り組みを行う必要がある。

そのためには、平均故障間隔の長い安定したシステムや安定した OS を選択し、壊れにくく動作不良を起こさないシステムを導入することで、サービスの停止を防止できる。また、万一、ハードウェア等に故障が生じたとしてもサービス停止を招かないよう、ハードウェアを二重化する等のフォールトトレランスを図ることも重要である。他にも、ウイルス感染によるシステム停止を防止するためにウイルス対策を行うことが必要である。

イ　サービス停止時間短縮

万一、サービスが停止した場合においても、なるべく停止時間を短くし、速やかにサービスの復旧が行えることが重要である。システムである以上、メンテナンス等のためにやむをえずサービスを止めなければならないこともある。サービス停止時間を短縮するためには、平均故障間隔の長い安定したシステム、安定した OS やパッチ導入等のメンテナンスが容易な OS を選択することやサービス停止が生じた場合にも容易に復旧可能なシステムを選択することが重要である。

また、システム更改時等におけるサービス停止時間を短縮するためには、データのポータビリティを確保することが重要となる。

ウ　高負荷への対応

電子申請や電子調達等、国民や住民、企業との間でオンラインにより情報をやり取りするシステムでは、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ることが懸念される。こうした場合にもサービス停止等の障害が発生しないよう、クラスタリングの導入や負荷分散機能の導入などの対策を施すことが必要である。

(4)真正性確保の必要性

ア　なりすましの防止

正当な使用者以外の情報システムへのアクセスや処理、職務権限を越えた情報へのアクセスや処理等を防止するために、使用者の確実な本人認証等を通じて、なりすましを防止しなければならない。

(5)責任追跡性確保の必要性

ア　否認の防止

電子政府、電子自治体における情報システムでは、電子文書等の授受等に関する事後否認を防止する必要がある。行為者が実際に行為を行った証拠を提供し、その行為者が行った行為に対して否認することを防がなければならない。システムや情報へのアクセスの成功・失敗の記録などのアクセスログを残すことや、電子署名等により身元確認の証拠となる否認防止機能が必要となる。

3.3 取り扱う情報に起因し、システムに求められるその他の事項

(1)利用・運用の容易性

電子政府、電子自治体における情報システムを検討する際には、セキュリティの確保以外にも利用・運用の容易性を考慮する必要がある。

①導入及びカスタマイズの容易性

電子政府、電子自治体における情報システムの利用・運用性を検討する上で、OS のインストール等がしやすいか、業務に合わせたカスタマイズ等が容易に行えるかどうかを考慮する必要がある。

②業務に必要なアプリケーションの充実、入手容易性

OS に対応した既存のアプリケーション等が充実しているかどうか、また、それらのアプリケーションの入手が容易であるかどうかを考慮する必要がある。

③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

OS に対応したハードウェアが充実していなければ、使用できる機器が限られてしまう。システムや OS の動作保証がなされているハードウェアが充実しているか、それらのハードウェアの入手・購入は容易であるかどうかを考慮する必要がある。

④運用情報の提供機能

システムを円滑に管理するためには、機器のパフォーマンス等に関する情報を把握する必要がある。管理ツールなどを通じて運用情報の監視や管理が容易に行えるかどうかを考慮する必要がある。

⑤セキュリティ機能設定の容易性

セキュリティポリシーに則して、セキュリティ機能の設定を容易に行えるかどうかが重要である。また、デフォルトで不要なサービスや機能が排除されるなどのセキュリティ上の配慮がなされているかどうかを考慮する必要がある。

⑥操作性

堅牢なシステムを構築しても、システムを管理するためのツールが使いにくければ、管理しにくく、新しい脅威への対応が難しくなる。また、複雑な操作系は管理者の設定ミスなどを誘発する恐れがある。そのため、操作性が良いかどうかが重要な要件となる。

⑦スケーラビリティ

システムの構築後、ユーザ数の増加等、処理量が当初の想定以上になるケースを予想する必要がある。処理量の増加に対応し、性能や機能を拡張することやハードウェアを追加する等のスケーラビリティを確保できるかどうかを検討する必要がある。

⑧システム開発・保守を担う人材の充実

導入する OS や OS に関連したソフトウェアに精通した開発技術者が充実していると、業務にあわせたシステムの構築や OS のカスタマイズ等を円滑に行うことができる。また、運用後にシステムの修正等が必要になった際にも、迅速な対応が期待できる。情報システムの利用・運用を容易にするためには、導入したシステムや OS の開発・保守を担う人材が充実しているかが重要な要件となる。

(2)サポート体制

システムの運用を行っていく上で、システムに関連した情報提供や修正プログラムの提供等のサポートが継続的に利用可能であるかどうか、サポート体制が充実しているかどうかは重要な問題である。

①情報提供、情報公開状況（日本語対応　等）

システム管理者はシステムの管理・維持のために、導入したシステムに関連する最新情報を常に入手しつづける必要がある。そのため、このような情報が豊富に公開されているのか、すばやく提供されているのか、さらに情報が日本語化されているのかといった点を考慮する必要がある。

②カスタマイズ部分を含めた動作保証

業務に合わせて OS のカスタマイズが必要となった場合などでも、カスタマイズ部分を含めて OS の動作保証が行われることが望ましい。このような場合に、動作保証が得られるのか、あるいは条件次第で得られるのかどうかを検討する必要がある。

③パッチ等の供給体制（提供速度　等）

システム導入後に、システムに関連する脆弱性が発見された場合に、導入システムに対応した修正プログラムが迅速に提供される体制が整っているのか、さらに提供される修正プログラムは十分な検証を経て提供されているのかどうかを検討する必要がある。

④サポートサービス提供状況、サポート継続期間

サポートサービス継続期間が明確になっている必要がある。その上で、導入を検討するシステムの運用期間に対して、十分な期間サポートサービスが継続される見込みがあるのかどうか、さらにはサポートサービス期間を延長できる可能性があるのかどうかを考慮しなければならない。

(3)漢字コードへの対応

電子政府、電子自治体における情報システムでは国内外の人名や法人名、地名等を大量に扱う必要性がある。そのため、人名や地名などに使われている漢字を正確に処理できることが必要である。

①異体字等の導入容易性

人名や地名に用いられている漢字は多様であり、これまでにコード化された漢字

に含まれない漢字や、字体の違いにも対応することが求められる。そのため、異体字等の導入容易性について検討する必要がある。

②他システムとの整合容易性

人名や地名等の漢字を特定のシステム内でのみ正確に処理するだけではなく、これらの漢字を他のシステムとの間で正確にやり取りできることが求められる。そのため、他システムにおいてもこれらの漢字を正確に処理できるよう、他システムとの整合容易性を考慮する必要がある。

3.4 電子政府、電子自治体推進にあたり留意すべき事項

電子政府、電子自治体構築を進めていく際には、特に行政が運用するシステムであることに鑑み、以下のような点に留意することが必要である。

ア　長期的視点

行政のシステムでは長期にわたって情報の機密性・可用性を保っていくことが必要となる。そのため、OS のパッチの適用をはじめとして、システムのサポートを継続的に受けることができることが重要である。また、システムの更改の際には、行政文書が継続的に利用できる（文書の見え方が変わらない）こと、データのポータビリティが確保されること、データフォーマットの置換等に多大な費用を要しないこと等、次回の調達で調達先を限定する仕様としないことへの留意が必要になる。

また、法律の改正などに伴ってアプリケーションレベルのシステムの更新が頻繁に行われる、異体字をはじめとして多くの漢字を扱うことが必要といった行政でのシステムの特徴に応じて電子化の取組みを進めていくことが重要である。

裁判所からの命令に対応してシステムの構造を示す文書及びデータの開示が可能でなければならない。

イ　委託事業者との契約

システムの継続的な運用を可能とするためには、システムの品質とともに、バグ・セキュリティホールなど OS に関わる不具合等が発生した際の責任の所在や、パッチ提供をはじめとする長期的なサポートの体制、第三者の知的財産権の抵触等のリーガルリスクへの対応など、システムの構築・運用に関わる留意点について、システムの構築・運用の委託事業者との契約において明確にしておくことが重要である。

ウ　コスト

予算の効率的運用、投資効果最大などの観点からコスト面からの検討が必要である。一般に高いセキュリティ機能を実現するには、調達コストも高くなる傾向がある。情報資産の特性に応じて、適切なセキュリティ対策を決定するとともに、導入コストだけではなく運用コストを含めたトータルコストに関する検討を行うことが重要である。

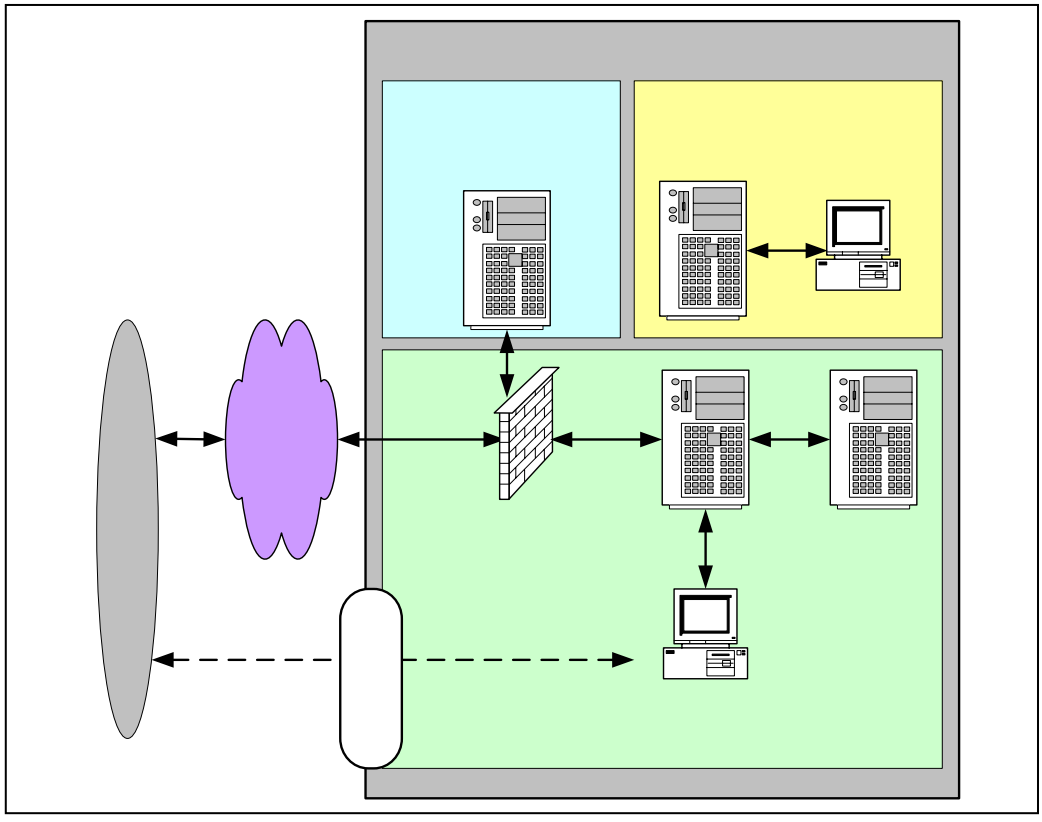
3.5 電子政府、電子自治体におけるシステム構成モデル

電子政府、電子自治体におけるシステム構成には様々な形態があるが、以下の図に示す構成をシステム構成のモデルとして、本調査研究会ではシステムに求められる要件等について検討した。

フロント系システムは、ホームページ閲覧や電子申請等で国民/企業がインターネットを経由してアクセスするシステムで、Web サーバ等ファイアウォールの外側で DMZ（非武装地帯）に置かれている。業務用サーバ等は LAN などで結ばれており、住民サービスや行政執行が行われている。また、全庁的なシステムとは独立した個別業務システムがある。

従来、住民基本台帳や税関連のシステムをはじめとする基幹業務系のシステムは他のシステムと切り離されて運営されているケースが多かったが（下の図の個別業務システムのかたち）、電子化に伴ってフロント系のシステムにつながることが多くなってきている。

図表3-7　電子政府、電子自治体のシステム構成とセキュリティの検討対象



４．電子政府、電子自治体向けシステムに求められる要件

4.1 セキュリティ要件

(1)機密性の確保

ア　無権限アクセスの防止

①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、各使用者の端末又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。

②ユーザ毎のアクセス制御

【概要】

無権限アクセスを防止するためには、セキュリティポリシーに基づき、使用者毎に、業務要件に従って、システム内のファイルや情報資源、システムの機能へのアクセス権を制御する機能を備えていることが必要となる。適切なアクセス制御が行えなければ、機密情報の漏洩や滅失、き損等の事故に繋がる恐れがある。

アクセス制御の方法として、使用者や使用者グループの情報に基づき、アクセス制御を行う、任意アクセス制御（Discretionary Access Control）があり、多くのOS ではこの機能を備えている。任意アクセス制御では自分の所有する情報資源へのアクセス権を任意に設定・変更することができる。

業務上の要件により、さらに厳格なアクセス制御を実現する方法として、使用者に与えられる役割に基づいてアクセス制御を行う役割ベースのアクセス制御（Role Based Access Control）や、全ての使用者や処理が強制的にアクセス制御を受ける強制アクセス制御（Mandatory Access Control）がある。

従来の OS では、管理者全員にスーパーユーザ権限が与えられるなど、管理者には必要以上の権限が付与されている。それに対し、役割ベースのアクセス制御の機構は、管理のための一連の作業を担うユーザに制限付きの管理権限を割り当てることを可能にする。ここで付与される管理権限は一連の管理作業を果たすために必要十分な権限である。これにより、従来のシステム管理者権限のように大きな権限ではなく、業者やオペレータなどの役割に対して必要最小限の権限を与えることが可能となり、情報の漏洩や改ざんなどの脅威の極小化が行い得る。

しかし、これらの厳格なアクセス制御の導入は、運用に大きな負荷がかかることに留意する必要がある。

【実装する機能イメージ】

□ アクセス制御ポリシーを容易に設定・変更できる機能を備えているか。
□ 任意のアクセス制御に対応できるか。
□ 役割ベースのアクセス制御に対応できるか。（但し、運用に大きな負荷がかかる懸念がある）
□ 強制アクセス制御に対応できるか。（但し、運用に大きな負荷がかかる懸念がある）

③アクセスログ

【概要】

セキュリティポリシーでの規定からのずれを検出することや、セキュリティ事故や事件が生じた場合の証拠となるように、システムの使用を要求してきた使用者に対して、利用者 ID やログオン・ログオフ日時、システムへのアクセスの成功・失敗の記録、ファイルや情報資源へのアクセスの成功・失敗の記録等を作成し、一定期間保存することが望ましい。

アクセスログは、時刻等の記録内容の正確性を確保するために、不正な消去や改ざんを防止するなど、適切に保存するための対処を施す必要がある。

【実装する機能イメージ】

□ システム監視や、セキュリティ事件・事故の証拠として必要となるシステムの事象や使用状況等を、十分に記録する機能を備えているか。
□ アクセスログの盗難、改ざん、消去等を防止する機能を備えているか。
□ アクセスログの盗難、改ざん、消去等を検知する機能を備えているか。
□ アクセスログの分析が容易に行えるための機能を備えているか。
□ アクセスログを監視し不正アクセス等が生じた場合に管理者に通報する機能等を備えているか。
□ 時刻を正確に保つための機能を備えているか。
□ アクセスログの記録対象とする情報を容易に設定・変更できる機能を備えているか。

④侵入検知

【概要】

無権限アクセス等の不正行為への検知・対処を可能とするために、ネットワークやシステム上における行動パターンやアクセスパターン等を監視・分析し、不正行為を検出する侵入検知機能を備えることが望ましい。

使用者の行動パターンや、アクセスパターン等を監視・分析することで、通常のアクセスや利用とは異なる不正行為を検知する機能を備えた侵入検知（IDS）ソフトウェア等を導入することで実現することができる。

侵入検知システムには、監視対象とするサーバ上の処理や通信等を監視するホストベースの IDS や、ネットワーク上を流れるパケットを監視するネットワークベースの IDS 等がある。

【実装する機能イメージ】

□ 想定される脅威を、誤報が少なく正確に検知できる機能を備えているか。

□ネットワークが高速であったり、高い負荷がかかったりした場合でも、照合・分析処理が行える能力を備えているか。
□不正行為や疑わしい行為等を検知した場合に、管理者等に通報する機能等を備えているか。
□検知した情報の分析が容易に行えるための機能を備えているか。
□不正行為や疑わしい行為等を検知した場合に、当該セッションを切断する等の防御機能を備えているか。

イ　ウイルス対策

①コンピュータ・ウイルス等による情報流出への対策

【概要】

コンピュータ・ウイルス等の中には、感染後、情報システム内のファイルを外部に送信するものがあり、個人情報等の漏洩に繋がる恐れがある。

ウイルス対策ソフトを導入し、コンピュータ・ウイルス等への感染を防止するとともに、万一、感染した場合にも、コンピュータ・ウイルス等による外部への情報流出を防止するための対処を施す必要がある。

【実装する機能イメージ】

□外部から受信する情報やソフトウェアに対して、コンピュータ・ウイルス等の有無を検出する機能を備えているか。
□外部に発信する情報やソフトウェアに対して、コンピュータ・ウイルス等の有無を検出する機能を備えているか。
□コンピュータ・ウイルス等による外部への情報流出を防止する機能を備えているか。

②プロセス監視

【概要】

コンピュータ・ウイルスや、ネットワーク上の情報資産を盗聴するようなソフトウェア、ネットワークの状態を探索するソフトウェア等の不正な動作を検知することを可能にするために、システム上で動作しているプロセスに対して、不正なプロセスの有無やプロセス数等を監視し、コンピュータ・ウイルス等の動作を検知・抑制する機能を備えることが望ましい。

【実装する機能イメージ】

□システム上で動作するプロセスに対して、不正なプロセスの検知等を行う機能を備えているか。

ウ　データの保管／持ち出し、情報送出の防止

①本人真性確認

4.1(1)ア①と同じ。

②ユーザ毎のアクセス制御

4.1(1)ア②と同じ。

③アクセスログ

4.1(1)ア③と同じ。

④フールプルーフ

【概要】

誤操作等により、意図せず情報を送出するといった事故を防止するために、データの送信や削除などの指示が行われた際に確認メッセージ等を表示する等、使用者による誤操作を防止するための機能が実装されていることが望ましい。

【実装する機能イメージ】

□ 使用者によるデータの誤送信を防止するための機能を備えているか。
□ 使用者によるデータの誤削除等の誤操作を防止するための機能を備えているか。

⑤情報フロー制御

【概要】

接続経路等を制限することにより、認められない情報の送出やアクセスが行われるリスクを軽減することができる。

セキュリティポリシーに基づき、外部ネットワークとの接続箇所や内部ネットワークセグメント間等において、発信元や送信先等によって、パケットやメッセージ等の情報の流れを制御すること等により、認可された経路以外からのアクセスを防止することができる。

【実装する機能イメージ】

□ 発信元や送信先等に応じて経路指定や破棄等の制御が行える機能を備えているか。
□ 経路指定等を容易に設定・変更できる機能を備えているか。

⑥暗号制御

【概要】

情報の機密性を保護するために、ファイルや通信経路等の暗号化を行う機能を備えていることが望ましい。意図せず情報が流出した場合でも、暗号化を施していることにより、情報の機密性が破られるリスクが低減される。

暗号を導入する際には、職員の異動やハードウェアの故障等による暗号鍵の紛失や破壊等が生じた場合でも、情報を復号可能とする鍵管理の仕組みを備えることを検討する必要がある。

OS を選定する際には、業務上の要件によって求められる暗号強度を満たすような、暗号アルゴリズムや暗号鍵の長さに対応できるかどうかを検討することが必要である。

【実装する機能イメージ】

□ ファイル暗号化機能を備えているか。
□ 暗号化通信機能を備えているか。
□ 業務上求められる暗号強度を満たす暗号アルゴリズムや暗号鍵の長さに対応できるか。
□ 暗号鍵の紛失や破壊等が生じた場合でも、情報を復号可能とする鍵管理の仕組みを備えているか。

エ　推論攻撃対策

①推論制御

【概要】

公開されているデータベース等から非公開情報である機密情報等が推測されることを防止するために、データベースの構築・運用に際しては工夫が必要である。例えば統計情報を公開する際には、母集合の要素数が一定以下ならば公開しない、検索式に用いることができる属性数を制限するといった方法を取り入れることが必要となる。

【実装する機能イメージ】

□ 複数の検索結果等から非公開情報が推測されることが無いように、母集合の要素数が一定以下ならば公開しない等の推論制御を考慮したシステム設計となっているか。

(2)完全性の確保

ア　情報改ざんの防止

①本人真性確認

4.1(1)ア①と同じ。

②ユーザ毎のアクセス制御

4.1(1)ア②と同じ。

③アクセスログ

4.1(1)ア③と同じ。

④データバックアップ

【概要】

情報システム内の情報が改ざんされた場合でも、適切なデータバックアップの実施により、情報の復元が可能になるなど、被害を最小限に留めることができる。データバックアップは、通常、上書きできないようにした媒体に定期的に保管する。但し、データバックアップを行った媒体が流出し、情報漏洩等の被害が生じないよう、管理を徹底することに留意しなければならない。

【実装する機能イメージ】

□システム内のデータを格納するのに十分な容量があり、信頼性の高い蓄積媒体が扱えるか。
□バックアップ作業を自動化する機能を備えているか。
□バックアップした情報の履歴管理を行う機能を備えているか。

イ　情報破壊、滅失の防止

①本人真性確認

4.1(1)ア①と同じ。

②ユーザごとのアクセス制御

4.1(1)ア②と同じ。

③アクセスログ

4.1(1)ア③と同じ。

④ロールバック機能

【概要】

職員等による誤操作等により情報の破壊や滅失等の事故が生じたとしても、職員等が行った操作や処理を、一定時間や回数まで実行前の状態に戻すロールバック機能を備えることにより、情報を元の状態に復旧することが可能となる。

また、処理の途中で異常終了した等の場合等にも、部分的に完了した処理をロールバックすることにより、何も処理が行われていない状態に戻すことが可能となり、情報の完全性を保つ上で効果が高い。

【実装する機能イメージ】

□ 使用者が行った操作や処理について、一定時間や一定回数まで実行前の状態に戻す機能を備えているか。

□ 処理の途中での異常終了等の際に、部分的に完了した処理を元に戻す機能を備えているか。

⑤データバックアップ

【概要】

第三者からの攻撃や職員の誤操作、機械の故障等により、情報システム内の情報が破壊、滅失した場合でも、適切なデータバックアップの実施により、情報の復元が可能になるなど、被害を最小限に留めることができる。データバックアップは、通常、上書きできないようにした媒体に定期的に保管する。但し、データバックアップを行った媒体が流出し、情報漏洩等の被害が生じないよう、管理を徹底することに留意しなければならない。

【実装する機能イメージ】

□ システム内のデータを格納するのに十分な容量があり、信頼性の高い蓄積媒体が扱えるか。

□ 自動的にスケジューリングしてバックアップする機能を備えているか。

□ バックアップした情報の履歴管理を行う機能を備えているか。

(3)可用性の確保

ア　サービス停止の防止

①平均故障間隔の長い安定したシステムの選択

【概要】

平均故障間隔（稼働中のシステムで、ある故障の回復後から、次に故障を起こすまで正常に動作する時間の平均）が長いほど信頼性が高く、故障する可能性が低い。デバイスの故障がシステム全体のサービスの停止にもつながることから、ハードディスクなど摩耗をはじめとした経年変化を受ける部品を利用したデバイスでは平均故障間隔に留意することが必要である。

【実装する機能イメージ】

□ 平均故障間隔の長い機器を利用することができるか。

②二重化等のフォールトトレランスがなされたシステムの導入

【概要】

システムのサービス停止を防止するためには、システムに障害が発生した時に、障害発生時の被害を最小限度に抑え、正常な動作を保ち続けるための代用サーバを用意するという二重化などのフォールトトレランスに考慮することが重要である。

OS のシステムを止めずにハードウェアを交換できる機能や OS によるソフトウェア的な RAID の実現ができる機能などの利用により、フォールトトレランスを高めることができる。ただし、OS 単独で実現するというより、OS とハードウェアの連携によって高可用性を実現することが必須であり、ハードウェアレベルで対応することも多い。

【実装する機能イメージ】

□ ハードウェアの冗長化に対応し、システムの一部に故障が発生しても処理を継続する能力を備えているか。

□ システムを止めずにハードウェアの交換が行える機能（ホットスワップ機能）を備えているか。

□ ソフトウェア RAID 機能を備えているか。

□ ハードウェア RAID に対応した機器を利用することができるか。

③安定した OS の選択

【概要】

バグをはじめとするシステムの不具合が少なく、サービス停止の頻度が少ない OS、また、長時間安定して動作することができる OS など安定した OS を選択することにより、システムのサービス停止を防ぐことにつなげられる。

システムをサービス停止するケースとして、脆弱性に対応するための修正プログラムの適用が考えられる。修正プログラム適用の作業後、再起動が必要となる OS があり、サービス停止を余儀なくされる。一方、修正プログラムの適用が必要となるプロセスだけの再起動で済むものもある。

【実装する機能イメージ】

□ 修正プログラムの適用後にシステム全体の再起動を要しない等、サービス停止の頻度を少なくするための配慮がなされているか。

④ウイルス対策

【概要】

コンピュータ・ウイルス、ワーム、トロイの木馬など、データ消去といった被害を及ぼすものをはじめとして利用者の意図していない動作を行うように、OS 等の脆弱性を利用して作成されたプログラムが、メールで送られてきたり、Web にアクセスしたりする際に感染することがある。これらのコンピュータ・ウイルス等のため、システムが被害を受け、サービスが停止する可能性がある。その対策のため、セキュリティホールを修正したパッチを適用したり、ウイルス検出ソフトなどを利用したりすることが必要である。修正プログラムの適用がウイルス対策には有効であるが、パッチをあてる際に再起動が必要になることがあり、余儀なくサービスが停止せざるを得ないことがある。

【実装する機能イメージ】

□ システムの要件に応じて、ファイアウォール、サーバ、クライアント端末等にウイルス対策ソフトを導入することができるか。

□ 全ての端末に対して、ウイルス対策ソフトのパターンファイル更新を自動的に行える機能を備えているか。

イ　サービス停止時間短縮

①平均故障間隔の長い安定したシステムの選択

4.1(3)ア①と同じ

②復旧が容易なシステムの選択

【概要】

ソフトウェアのバグや過大な負荷がシステム等にかかることなどの要因のため、サービスの停止が起こることは避けられない。そのため、サービスの停止が起こった際にその停止時間を極力短縮していくことが、システムの運用者に求められることである。サービス停止時間を短縮するための一つのアプローチとして、復旧が容易であることがある。

そのために、ある決まった時点でのファイルシステムの内容をバックアップする機能や、システム停止時にファイルの損傷を最小にする機能などを有し、復旧を容易にする機能を有していることが求められる。

データが損傷した場合のために、復旧ツールが用意されているケースもあるが、これは逆にセキュリティの面では脆弱であるともいえる。

【実装する機能イメージ】

□障害等発生時にファイルシステムの整合性等を検証する機能を備えているか。
□損傷したファイルを復旧するツールを備えているか。
□決まった時点でのファイルシステムの内容を自動的にバックアップする機能を備えているか。
□ファイル更新履歴を記録するなどして、ディスク障害等により破損したファイルの復旧を迅速に行うための機能を備えているか。

③安定した OS の選択

4.1(3)ア③と同じ

④パッチ導入等のメンテナンスが容易な OS の選択

【概要】

バグや脆弱性の発見により、修正プログラムを適用することが必要になるが、このパッチをあてる際のサービス停止時間が短いことが求められる。また、セキュリティ面を考えると、パッチの適用等が確実に行われることが必要となってくるが、

そのため自動的なアップデート機能をもっている OS もある。

【実装する機能イメージ】

□ システムに必要となるパッチ等を判断し、自動的にアップデートする機能を備えているか。

ウ　高負荷への対応

①クラスタリングの導入

【概要】

アクセスが多くなるなどでシステムに高負荷がかかることにより、レスポンスタイムが遅くなったり、最悪の場合はサーバの停止となったりする。そこで、機器を並列に運用することで、すなわち複数のコンピュータを相互に接続し（クラスタリング）、1 台が停止してもシステム全体が止まることがなく、処理を続行したまま修理や交換が行えるといった機能が提供されている。ハードウェアとの連携が必要になってくるが、OS で対応しているものと、OS に機能が無くアプリケーションでの対応が必要になってくるものがある。

【実装する機能イメージ】

□ 複数の独立したサーバを組み合わせ、単一のサーバのように運用するクラスタリングを実現できるか。

②負荷分散機能の導入

【概要】

アクセスが多くなるなどでシステムに高負荷がかかることにより、レスポンスタイムが遅くなったり、最悪の場合はサーバの停止となったりする。そこで、並列に運用されている機器間での負荷がなるべく均等になるように処理を分散して割り当てることで、一つの機器にかかる負荷を減らし、システムの可用性を高めることができる。複数の CPU を効率よく均等に使うためのプロセススケジューリングなどが行われている。

【実装する機能イメージ】

□ 並列に運用する複数のサーバの負荷をなるべく均等になるよう制御する機能を備えているか。

□ 複数の CPU を効率よく使うためのプロセススケジューリング等の機能を備えているか。

(4)真正性の確保

ア　なりすましの防止

①本人真性確認

4.1(1)ア①と同じ。

(5)責任追跡性の確保

ア　否認の防止

①アクセスログ

4.1(1)ア③と同じ。

②否認防止（電子署名等）

【概要】

電子申請や電子調達等では、後から申請内容を否定することや、申請行為そのものに関わったこと等が否定されることを不可能とする仕組みを整えることが必要である。

そのため、例えば、発信情報や受信情報に対して、電子署名などの改ざん不能な技術を用いて、発信者、受信者の身元確認のための証跡を付与する機能、検証する機能を備えることが望ましい。

【実装する機能イメージ】

□ 電子署名などにより発信者、受信者の身元確認のための証跡を付与・検証する機能を備えているか。

(6)ポリシーの策定・運用及び監視

ア　ポリシーの策定・運用及び監視

【概要】

セキュリティを確保するためには技術的な対応だけではなく、運用面での対処を徹底する必要がある。

利用者個人の裁量で情報の扱いが判断されることのないよう、組織として意思統一され明文化された文書である情報セキュリティポリシーを策定することが必要である。どのような情報資産をどのような脅威からどのように守るのかについての基本的な考え方並びに情報セキュリティを確保するための体制、組織及び運用を含め規定しなければならない。

前述の(1)から(5)について継続的に確保するためには、当初開発の際の一時的な技術的対応にのみ依存するのではなく、システム開発プロセスにおける標準的な手順の一部として、セキュリティ要件を検討するプロセスやチェックポイントを明確に規定することが必要である。これにより、開発あるいは保守時において、ポリシーに従った一貫性のあるセキュリティレベルを維持できるような体制が整うと考えられる。

また、ポリシーの実効性を確保するために、システムの使用者等がポリシーを遵守しているかどうかについて常に監視・確認しなければならない。その際、ポリシーそのものの問題点やポリシーが実態と整合しているかどうかを評価することも重要である。

4.2 その他の要件

(1)利用・運用の容易性

①導入及びカスタマイズの容易性

【概要】

業務の電子化に伴い、サーバ、クライアントともその数が増加していくことが想定される。そのため、OS のインストールが容易であるなど OS の導入が容易であることが求められる。最近の OS では、インストールの際に GUI が利用できるようになっている。

また、システム利用側の要求条件等に合わせるために、OS のカスタマイズが必要になるケースがある。そこで、OS のカスタマイズを容易におこなえるようにするためにツールの提供やソースコードの公開などが行われている。

【要件実現のイメージ】

□ インストールすべき機能をシステム管理者が選択するためのインタラクティブな仕組みなどを備えてきるか。

□ ハードウェアの機能を自動識別しインストールすべきファイルを峻別する、インテリジェントなインストーラを備えているか。

□ ＯＳのカスタマイズを行うためのツールやソースコードが提供されているか。

②業務に必要なアプリケーションの充実、入手容易性

【概要】

システムの構築には、データベースをはじめとして様々なアプリケーションソフ

トが必要になる。開発期間短縮やコストを低く抑えるためには、当該 OS に対応したアプリケーションが豊富に出回っていること、また、それらが市販やネット上での公開がされているなど入手が容易であることが求められる。

また、日本語対応しているアプリケーションが多いこと、ネットなどでアプリケーションに関する情報が豊富に出回っているといったことも要件の一つである。

【要件実現のイメージ】

□業務に必要となるアプリケーションソフトが容易に入手できるか。
□業務に必要となるアプリケーションソフトの選択肢が潤沢か。
□業務に必要となるアプリケーションソフトが利用する職員にも容易に理解できるものか。

③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

【概要】

当該 OS に対応したアプリケーションと同様、当該 OS の動作の保証（動作確認）が行われているサーバ、周辺機器等のハードウェアが豊富に出回っていることで、システム導入コストを低く抑えることができる。

動作保証がされている機器の入手を容易にするため、対応確認済みのハードウェアの認定制度を設けている OS もある。

【要件実現のイメージ】

□必要な機能を実現するためのハードウェアについて、当該ＯＳによる動作保証がなされている機器が豊富にあるか。

④運用情報の提供機能

【概要】

システム管理を容易にし、継続的なサービス運用につなげるためには、サーバのパフォーマンスの異常検知、ディスク使用率など、運用情報が容易に把握（管理）できることが必要である。OS で管理ツールが標準で提供されていることもある。また、追加ソフトウェアとして様々なツールが提供されている。

【要件実現のイメージ】

□運用管理者が、機器やソフトウェアの状況を容易に把握できるツールがあるか。
□運用管理を自動化するためのツールがあるか。

⑤セキュリティ機能設定の容易性

【概要】

セキュリティ対策を有効に機能させるためには、セキュリティポリシーに基づいたセキュリティ機能の設定を確実に行う必要がある。しかし、多岐にわたる設定を適切に設定することは容易ではないことから、こうした設定が容易に行えること、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、一括してセキュリティ機能を設定できるツール等が提供されていること等、セキュリティ機能を容易に設定できる工夫がなされているかどうかを検討する必要がある。

【要件実現のイメージ】

□ セキュリティに係る機能の設定状況を一括して閲覧するためのツールがあるか。
□ セキュリティに係る機能を一括して設定するためのツールがあるか。

⑥操作性

【概要】

堅牢なシステムを構築しても、システムを管理するためのツールが使いにくければ、管理しにくく、新しい脅威への対応が難しくなる。また、複雑な操作系では設定ミス等を誘発する恐れがある。そのため、管理ツールが GUI 等の使いやすいインタフェースになっていること等、操作性に留意する必要がある。

【要件実現のイメージ】

□ 管理のためのツールの操作性が優れているか。
□ 管理のためのツールに誤操作防止機能が備わっているか。

⑦スケーラビリティ

【概要】

システムの導入後、ユーザ数や接続機器の増加により、システムの処理量が増える可能性がある。しかし、これらの増加に合わせて、全く新しいシステムを構築していては手間もコストもかかってしまう。そのため、このような規模等の増加に柔軟に対応し、システムの性能や機能を向上させることができるか、ハードウェア等の追加等が容易に行えるかといった、システムに拡張性について考慮する必要がある。

【要件実現のイメージ】

□ 多様なハードウェアに対応しているか。

□ ハードウェアの追加や交換がなされた場合の初期設定が、情報セキュリティ上、安全側に寄っているか。
□ ハードウェアの追加や交換を行った際に、追加・交換前と同等の設定にする事が容易か。

⑧システムの開発・保守を担う人材の充実

【概要】

システムの導入にあたっては、導入する OS 等の開発・保守を担う人材が充実しているかどうかを考慮する必要がある。

導入する OS や OS に関連したソフトウェアに精通した開発技術者等が充実していれば、業務にあわせたシステムの構築や OS のカスタマイズ等を円滑に行えることが期待できる。また、運用後にシステムの修正や拡張等が必要になった際にも、迅速な対応が期待できる。

【要件実現のイメージ】

□ 導入システムに関する人材が豊富か。
□ 導入システムの改修・保守が、納入事業者以外でも実施可能か。

(2)サポート体制

①情報提供、情報公開状況（日本語対応　等）

【概要】

システム管理者は、システムの運用期間中、当該システムや OS 等に関連する技術情報、セキュリティ情報等を収集し、最新の動向を把握する必要がある。そのため、導入システムや OS に関連する情報が豊富に、また迅速に提供されることが望まれる。さらに、英語による情報提供との時間差なく、正確に日本語化された情報が提供されることが望ましい。

【要件実現のイメージ】

□ 日本語の情報が潤沢かつ迅速に提供されるか。
□ オリジナルの言語と、日本語とで、提供される情報の量に差は無いか。

②カスタマイズ部分を含めた動作保証

【概要】

業務に即した情報システムを構築する上で、OS にカスタマイズを加える必要が

生じる場合がある。このように OS のカスタマイズが必要となった場合などでも、カスタマイズ部分を含めて OS の動作保証が得られるのか、あるいは条件次第で得られるのか等に留意する必要がある。

【要件実現のイメージ】

□ＯＳにカスタマイズを加えた場合の動作保証範囲が明文化されているか。

□ＯＳにカスタマイズを加えた場合の保証者の責任分解がきちんとなされているか。

③パッチ等の供給体制（提供速度　等）

【概要】

システム導入後、システムに関連する脆弱性が発見された場合に、導入システムに対応した修正プログラムが迅速に提供される体制が整っていなくてはならない。さらに、それらの修正プログラムの提供が、十分な検証が行われた上でなされているのかどうかに留意する必要がある。

【要件実現のイメージ】

□修正プログラムを迅速に配布する体制が整っているか。

□過去の修正プログラムにより、脆弱性がどの程度確実に対処されているか。

④サポートサービス提供状況、サポート継続期間

【概要】

システムの継続的な運用を行う上で、十分な期間サポートサービスが利用できなければならない。

導入したシステムや OS のサポート期間が明確となっているのか、その上で、導入するシステムの運用期間に対して十分な期間サポートサービスが継続される見込みがあるのかどうかを検討しなければならない。さらには、サポートサービス期間を延長できる可能性があるのかどうかを含めて考慮する必要がある。

【要件実現のイメージ】

□サポートサービスの提供期間が明確となっているか。

□サポートサービス終了後に、サードパーティによるサポートを期待できるか。

(3)漢字コードへの対応

①異体字等の導入容易性

【概要】

電子政府、電子自治体における情報システムでは国内外の人名や法人名、地名等を大量に扱う必要性がある。そのため、人名や地名などに使われている漢字を正確に処理できることが必要である。そのため、異体字を含め多くの漢字を扱える文字コードに対応していることや、その漢字に対応したフォントを利用できること、もしくは文字コードに存在しない文字を容易に組み込むことができること等に留意する必要がある。

【要件実現のイメージ】

□アプリケーション上で多数の外字を利用することができるか。
□アプリケーション上で外字を容易に利用することができるか。
□外字を利用したデータについても、検索等が容易にできるか。

②他システムとの整合容易性

【概要】

電子政府、電子自治体における情報システムでは、当該システムで異体字等の多様な漢字を処理できるだけではなく、同じ庁内の他のシステムや他の自治体におけるシステム等との間でこれらの漢字を正確にやり取りできることも必要である。そのため、異なる OS を採用している他システム等でも、文字化けを起こさず、正確に文字を表記できることや、プリンタ等の出力機器からも正確に出力できることが必要である。

【要件実現のイメージ】

□電子ファイルと外字フォントとをセットで扱うことができるか。
□外字データも他の情報システムで利用可能か。

(4)コスト

【概要】

情報システムに求められるセキュリティ機能や重要性は、対象となる業務や取り扱う情報資産の特性により異なる。これらの特性を考慮した上で構築しようとするシステムや OS にどこまでのセキュリティ機能が必要となるのか、どのような要件が重要となるのか等を十分に検討した上で、コストを検討する必要がある。ここでは、コス

トを考えるときの観点として、以下の 5 つをあげる。

①必要なハードウェアの導入コスト

システムに求められる性能を実現する上で必要となるハードウェアの仕様を検討し、その導入コストを検討する必要がある。ハードウェアに要求される性能は、導入する OS によって異なる可能性があることに留意しなければならない。また、周辺機器のコスト等を含めて比較検討を行う必要がある。

②OS の導入コスト

OS の導入コストについて、OS ライセンスコスト、インストールコスト、システム管理者及び利用者への教育コスト等を含めて検討する必要がある。

③アプリケーションの導入コスト

OS だけではなく業務に必要となるアプリケーションの導入コストを検討する必要がある。導入する OS によってアプリケーションの充実状況は異なることから、既存アプリケーションの利用が可能であるのか、既存アプリケーションにカスタマイズが必要になるのか、あるいはアプリケーション開発を行う必要があるのか等に留意しながら検討する必要がある。

④システム開発・変更コスト

導入する OS によって、OS のソースコードの公開状況やシステム改変の自由度、開発ノウハウの蓄積状況等が異なる。また、OS により要求機能に対する得手不得手があることから、適切な OS を選択しなければ、多くの開発コストを要する場合もある。OS を選定する際には、OS の導入コスト等のみならず、システム開発・変更コストについても比較検討を行う必要がある。

⑤運用コスト

導入する OS 等によって、サポートサービスやバージョンアップ等の体制が異なることから、それらに要するコスト等も異なる。また、安定的な運用が行える見込みが高いのかどうかによっても運用コストは異なる。

【考慮すべき事項】

- □ システム利用予定期間を踏まえ、後年度のシステム変更コストも含め、全体のコストが最も低廉と見込まれるシステムは何か。
- □ システム利用予定期間を踏まえ、初期コスト、後年度のシステム変更コストも含め、コストの経年変化が最も小さいシステムは何か。

(5)リーガルリスク

【概要】

①不具合等に関する責任の所在の明確さ

システム・インテグレータ、ディストリビュータ、サードパーティ等とのサポートサービスの契約においては、バグ、セキュリティホールなど OS に関わる不具合等の発生した際に対応できる当事者もしくは対応すべき者について、明確にしておくことが重要である。

【考慮すべき事項】

□ システム納入者、運用者に対する責任の所在が明文化されているか。

□ システム納入者にとって不可抗力（システム納入者が対応できない部分）がどこにあるのか確認しているか。

②第三者の著作権、知的財産権への抵触に関する責任の所在の明確さ

【概要】

出自が明確で、開発がどのように行われてきたか公開されているなど、第三者の知的財産権への抵触についての責任の所在が明確となっているソフトウェアを利用することは、特許侵害といったリスクを軽減することに役立つ。

【考慮すべき事項】

□ 導入されるシステムに含まれる種々の知的財産（製品ソフトウェアなら第三者から導入して含まれているモジュール、オープンソース・ソフトウェアなら各コントリビューション）の由来が明確になっているか。

図表4-1　電子政府、電子自治体向けシステムに求められる要件一覧

- セキュリティ要件
  - (1)機密性の確保
    - ア　無権限アクセスの防止
      - ①本人真性確認
      - ②ユーザ毎のアクセス制御
      - ③アクセスログ
      - ④侵入検知
    - イ　ウイルス対策
      - ①コンピュータ・ウイルス等による情報流出への対策
      - ②プロセス監視
    - ウ　データの保管／持ち出し、情報送出の防止
      - ①本人真性確認
      - ②ユーザ毎のアクセス制御
      - ③アクセスログ
      - ④フールプルーフ
      - ⑤情報フロー制御
      - ⑥暗号制御
    - エ　推論攻撃対策
      - ①推論制御
  - (2)完全性の確保
    - ア　情報改ざんの防止
      - ①本人真性確認
      - ②ユーザ毎のアクセス制御
      - ③アクセスログ
      - ④データバックアップ
    - イ　情報破壊、滅失の防止
      - ①本人真性確認
      - ②ユーザ毎のアクセス制御
      - ③アクセスログ
      - ④ロールバック機能
      - ⑤データバックアップ
  - (3)可用性の確保
    - ア　サービス停止の防止
      - ①平均故障間隔の長い安定したシステムの選択
      - ②二重化等のフォールトトレランスがなされたシステムの導入
      - ③安定した OS の選択
      - ④ウイルス対策
    - イ　サービス停止時間短縮
      - ①平均故障間隔の長い安定したシステムの選択
      - ②復旧が容易なシステムの選択
      - ③安定した OS の選択
      - ④パッチ導入等のメンテナンスが容易な OS の選択

- ウ　高負荷への対応
  - ①クラスタリングの導入
  - ②負荷分散機能の導入
- (4)真正性の確保
  - ア　なりすましの防止
    - ①本人真性確認
- (5)責任追跡性の確保
  - ア　否認の防止
    - ①アクセスログ
    - ②否認防止（電子署名等）
- (6)ポリシーの策定・運用及び監査
  - ア　ポリシーの策定・運用及び監査

その他の要件

- (1)利用・運用の容易性
  - ①導入及びカスタマイズの容易性
  - ②業務に必要なアプリケーションの充実、入手容易性
  - ③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
  - ④運用情報の提供機能
  - ⑤セキュリティ機能設定の容易性
  - ⑥操作性
  - ⑦スケーラビリティ
  - ⑧システムの開発・保守を担う人材の充実
- (2)サポート体制
  - ①情報提供、情報公開状況（日本語対応　等）
  - ②カスタマイズ部分を含めた動作保証
  - ③パッチ等の供給体制（提供速度　等）
  - ④サポートサービス提供状況、サポート継続期間
- (3)漢字コードへの対応
  - ①異体字等の導入容易性
  - ②他システムとの整合容易性
- (4)コスト
  - ①必要なハードウェアの導入コスト
  - ②OS の導入コスト
  - ③アプリケーションの導入コスト
  - ④システム開発・変更コスト
  - ⑤運用コスト
- (5)リーガルリスク
  - ①不具合等に関する責任の所在の明確さ
  - ②第三者の著作権、知的財産権への抵触に関する責任の所在の明確さ

５．まとめ

(1)クライアントに対するまとめ

ア　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、セキュリティに関する機能については、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。

また、クライアント端末は、利用者の認証の最前線を担うものであることから、利用者を認証するためのハードウェア等に対する直接的な攻撃に対しての十分な備えも求められる。

イ　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。

システム利用に習熟していない職員であっても容易に操作が覚えられる、利用できるよう、わかりやすいインタフェースを備えていること、各種メニューが適切な表現で日本語化されていること、多様なアプリケーションを統一的な使い勝手で利用できることといった工夫がなされていることが望ましい。また、操作ミス等による誤処理を未然に防ぐための工夫がなされていることが望まれる。

コンピュータ・ウイルスやワーム等の感染被害を防止するためには、セキュリティホール等に対応した修正プログラムの適用を徹底する必要があるが、その際、各クライアント端末に対する適切な修正プログラムを容易かつ確実に適用できる仕組みを取り入れられることが求められる。

ウ　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ワードプロセッサーや表計算、プレゼンテーション資料作成等のアプリケーションが充実していることが望ましい。また、これら業務用アプリケーションで作成した資料を、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。

エ　クライアント OS の多様性の確保

組織内で使用するクライアント OS を単一の OS に統一した場合、操作性や運用性

等の面で有利な点が多数あるものの、当該 OS の脆弱性を悪用したコンピュータ・ウイルス、ワーム等が発生した場合に、これにクライアント端末が連鎖的に感染し業務が完全に停止してしまう恐れがある。実際、2003 年 8 月の MS ブラスターワームの感染被害が広がった際に、システム停止に繋がるといった事例が発生している。このような連鎖的被害の拡大を防ぎ、業務の継続を図る上では、組織内のクライアント OS を多様化することも有効な方策の一つとなり得る。

(2)業務用サーバに対するまとめ

ア　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機密性や完全性、可用性のレベルは異なる。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、業務の特性を踏まえ、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、OS を選択することが求められる。

イ　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

利用される業務が、庁内ネットワーク内の処理を主とするものであるのか、あるいは、電子申請や電子調達等の外部との処理を主とするものであるのかによって、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が優先されるかが異なる。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。

(3)フロントエンドサーバに対するまとめ

ア　情報セキュリティ侵害の防止

フロントエンドサーバはインターネットと接続するシステムであることから、Web の改ざんやサービス妨害攻撃などの情報セキュリティ侵害の脅威にさらされる。そのため、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が重要である。

イ　外部から重要な情報へのルートの遮断

外部からの情報セキュリティ侵害の脅威にさらされることから、フロントエンドサーバには重要な情報を保存してはならない。また、これらの情報を格納している内

部のシステムに、外部から直接アクセスできるルートが確保できないようにすることが求められる。

電子申請や電子調達等、国民や住民との間で情報をやり取りする際には、一時的に保存される情報についても、第三者によるアクセスや改ざん等が行われないよう対策を施すことが必要である。

ウ　可用性の確保

電子申請や電子調達等、国民や住民との間で情報をやり取りするシステムでは、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ることが予想される。このような場合にも、サービスの停止等の障害が発生しないよう、ピーク量等を想定し、クラスタリングや負荷分散機能等を導入する等、対策を施すことが重要である。

(4)システム全般に関するまとめ

電子政府、電子自治体における情報システムは、ハッカーやコンピュータ・ウイルス等を介した不正行為によるネットワークへの侵入、情報の改ざん・破壊・窃盗・漏洩等の脅威にさらされる。また、職員の単純ミス、ヒューマンエラー等による個人情報の漏洩等の危険性がある。電子政府、電子自治体における情報システム構築に当たっては、これらの脅威に対して、情報セキュリティ対策を適切に施し、個人の権利利益の侵害等が生じることがないようにすることが最重要課題である。

情報システムに求められるセキュリティ機能やその重要性は、対象となる業務や取り扱う情報資産の特性により異なる。従って、調達者自らが、これらの特性を考慮した上で、構築しようとするシステムの OS に、どこまでのセキュリティ機能が必要となるのか、どのような要件が重要となるのか等を十分に検討した上で、調達仕様書等に、これらのセキュリティ要件を記述する必要がある。

OS の調達に際しては、OS の機能面だけではなく、サポートサービス等の運用面での検討が重要である。情報システムを、セキュリティを保ちながら継続的に利用していくためには、サポートサービスが十分に提供される必要がある。当該 OS にセキュリティホール等の脆弱性が発見された場合には、その修正プログラムが速やかに提供されることが望ましい。そのため、調達時の仕様書や契約書等に修正プログラムの作成等の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求められる。

また、行政のシステムは長期にわたって運用を行うことから、システム更改等の際にも情報が継続的に利用できるよう、オープンな標準に準拠した技術を活用するなど、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。

さらに、情報システムの構築・運用に当たっては、予算の効率的運用、投資効果の最大化などの観点から、運用コスト等を含めたコスト面に関する検討が必要である。その際には、OS の導入コストだけではなく、必要となるハードウェア、アプリケーションの導入コストやシステムの開発・変更コスト、運用コスト等を会わせたトータルコストに関する検討を行うことが必要である。

(5)オープンソース OS の考え方

オープンソース OS として代表的な Linux や FreeBSD は、UNIX の持つ機能の実装を目指したこと等もあり、機能的には UNIX 系 OS の一つとして捉えられ、製品 OS との機能的な違いは少ない。

しかし、オープンソース OS の利用にあたっては開発やサポートの形態が製品 OS とは異なっていることに留意する必要がある。

ア　継続的なサポートサービスの提供の条件化

オープンソース OS は、世界的に分散した個人によるコミュニティによって開発されている。直接の営利目的で開発されていないことから、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、万一、修正プログラムの提供がなされない場合であっても、オープンソース OS の場合には、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。

そのため、オープンソース OS を利用する場合には、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にするために、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望ましい。サポートサービスの提供が得られる契約によって調達したならば、オープンソース OS であるか製品 OS であるかによる違いは少なくなり、個々のシステムに求められる要件に従って、最適な OS の選択が可能となる。但し、アーキテクチャ上の欠陥については、サポートの範囲での改善を期待することは困難であることには留意する必要がある。

６．おわりに

電子政府・電子自治体の情報システムは、フロント系と業務系という全く異なる役割を果たすシステムが組み合わさって構成されており、さらに業務系システムは、極めて多岐にわたる処理業務の特質に合わせ、多数のコンピュータの組み合わせで構成されている。このため、電子政府・電子自治体に用いられるコンピュータに求められる機能は、個々のコンピュータがこなすべき業務に応じて多様に変化するため、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。

また、UNIX 系 OS や Windows 系 OS をそのまま利用した場合には、その情報セキュリティ水準には限界があることから、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のソフトウェアの導入が必要である。

このため、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、総合評価方式による調達手続きをより一層活用し、「『特定の OS』またはそれと同等以上のもの」といった形で OS 等を実質限定するのではなく、

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及び品質を抽出し、
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・セキュリティを含めた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

することが適当であることを、本調査研究会は提言する。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、多様性が確保されるものと考える。

なお、情報システムの世界は日進月歩であり、その発展は非常に急であることから、今回、本調査研究会で行った検討結果も、じきに陳腐化してしまう可能性もある。このため、システム調達者は、本報告書の記載を参考にしながら、その時々の最新の情報を踏まえて判断すべきである。

このため、今後も本調査研究会と同様の検討が継続的に続けられることを期待する。

付録１

◇◇ 用語解説 ◇◇

CIO（Chief Information Officer）

情報システムや情報戦略における組織内の最高責任者のこと。最高情報責任者、もしくは情報統括役員と訳される。

CPU（Central Procession Unit）

日本語では中央演算処理装置と呼ばれ、コンピュータの各種装置の制御やデータの演算処理を行う。

DBMS（DataBase Management System）

データベースの操作・管理をするためのソフトウェア。データに対するアクセス要求の処理を行う。

DMZ（DeMilitarized Zone：**非武地帯**）

組織内部のネットワークとインターネット等の外部ネットワークとの中間に設ける領域。Web サーバなどの外部に公開するサーバを、インターネット側からの不正な攻撃から守るために設けられる。

DoS **攻撃**（Denial of Service）

サービス不能攻撃。コンピュータやネットワークに不正に大量のデータを送ること等により、業務を妨害する攻撃。

GPL（General Public License）

GNU プロジェクトのソフトウェア･ライセンス体系。GPL ソフトウェアはソースコードが公開されており、複製・再頒布、使用、変更・修正は自由に行えるが、改変部分のソースコードを公開する必要がある。

GUI（Graphical User Interface）

アイコンと呼ばれる絵記号を利用し、ほとんどの操作をマウスにより実現することができるインタフェースである。アイコンにより利用者はプログラムやファイルの機能や内容を直感的に理解し、利用することができる。

ITSEC（Information Technology Security Evaluation Criteria）

1990 年にドイツ・フランス・イギリス・オランダの 4 カ国により定められた、情報システム製品の評価基準。

OEM（Original Equipment Manufacturer）

相手先ブランドで販売される製品を製造すること。もしくは、相手先ブランドで販売される製品を製造するメーカー。製品供給を受けたメーカーは、自社ブランドで販売する。

RAID（Redundant Arrays of Inexpensive Disks）

複数のハードディスクを組み合わせて 1 台のハードディスクとして管理する技術であり、性能向上や安全性確保のために利用される。専用のハードウェアにより実現する方法と、ソフトウェアにより実現する方法とがある。

Sendmail (sendmail)

Eric Allman 氏が UNIX 用に開発した電子メール配送ソフトウェア。元々、オープンソース・ソフトウェアとして開発されたが、現在では商用版もある。大文字で始まる Sendmail が商用版、小文字で始まる sendmail がオープンソース版である。

TCSEC（Trusted Computer System Evaluation Criteria）

米国国防総省により定められた、軍事用途の情報システム製品の評価基準。

Telecom-ISAC Japan（Telecom Information Sharing and Analysis Center Japan）

インシデント情報共有センター。情報セキュリティに関連する情報収集及び情報共有を行うインターネットサービスプロバイダの事業者団体。

アクセス制御

コンピュータシステムの情報などの資源に対するアクセスや処理を、権限を与えられた者だけが行えるように制御すること。

アクセスログ

コンピュータへの接続履歴を記録したもの。アクセスログを解析することにより、そのコンピュータがどのように操作されたのか明らかにすることができる。

異体字

同じ意味であるが、字体だけが異なる漢字が複数存在する場合、標準的な字体と異なる字体を異体字という。邊や國等は異体字の例である。

オブジェクト・コード

コンピュータが理解できる言語(マシン語)で記述されたプログラム。人間がプログラミング言語を使って作成したソースコードを、コンパイラなどの変換ソフトウェアを使ってオブジェクト・コードに変換する。

カーネル

OS の基本機能を実現するソフトウェア。OS の中核部分として、周辺機器の監視、メモリの管理、ファイルシステムの管理などを提供する。

強制アクセス制御（Mandatory Access Control）

全ての使用者や処理に対して強制的に行うアクセス制御。

クライアント

コンピュータネットワークにおいて、サーバに接続し、サーバの提供する機能やデータ

を利用するコンピュータ。

クラスタリング
複数のコンピュータを相互に接続し、あたかも一つのシステムのように機能させる技術。

コンパイル
人間が記述したソフトウェアの設計図（ソースコード）をコンピュータ上で実行可能な形式に変換すること。

コンピュータ・ウイルス
何らかの被害を及ぼすように作られたプログラム。自己伝染機能、潜伏機能、発病機能のうち、少なくとも一つ以上の機能を有する。

サーバ
コンピュータネットワークにおいて、自身が有する機能やデータを他のコンピュータに提供するコンピュータ。

情報セキュリティポリシー
組織全体の情報システムにおける情報セキュリティに関する基本方針。セキュリティ対策基準や個別具体的な対策実施手順などを規定し、脅威が発生した時の対策手順、判断基準、責任の所在を明確にすることが多い。

情報フロー制御
情報の発信元や送信先等に応じて、情報が流れる経路等を制御する機能。

修正プログラム（パッチ）
既に完成しているプログラムに対して、部分修正を行うプログラム。修正を行うために必要な差分情報のみを記述している。

スケーラビリティ
システムの利用者数や処理の増加等に応じて、システムの性能や機能を向上させることができる能力。

スパムメール
勝手に送り付けられるメール、商品広告目的の希望していない商用メールなど、無差別に、また大量に発信されるメール。迷惑メールとも呼ばれる。

セキュリティホール
設計ミスなどによって生じた、ソフトウェアやシステムのセキュリティ上の弱点。セキュリティホールがあると、悪意のあるユーザに Web 情報の改ざんや機密データ漏洩などの不正行為をされる危険がある。ソフトウェアにセキュリティホールが発見された場合、その対策のための修正プログラムが通常無償で配布される。

ソースコード

特定のルールに従った記述法（プログラミング言語）を用いて記述したソフトウェアの設計図。人間が読める形式になっているが、コンピュータが実行できる形式ではない。

ソフトウェア

ハードウェアに対して、アプリケーションソフトなどコンピュータを動作させる手順・命令をコンピュータが理解できる形式で記述したもの。

ディストリビューション

ディストリビュータが販売する製品。製品としてパッケージする際に採用するソフトが会社により異なるため、同じ Linux であってもディストリビューションの細部は異なる。

ディストリビュータ

ソフトウェアやハードウェアの卸売りを行う業者。Linux では、Linux カーネルに、OS として機能するために必要又は有用なソフトウェアをパッケージ化して販売する業者を指す。

デバッグ

プログラム等の開発過程でバグを取り除く作業のこと。

デフォルト

ソフトウェア等の出荷時の設定値。全ての項目を設定するのは容易ではないため、一般的な設定が初期値として設定される。

トラブルシュート

原因を明らかにし、トラブルを解決すること。

トロイの木馬

普通のソフトウェアに見せかけて、利用者に被害を与える不正なプログラム。実行すると、悪質な利用者がシステムにアクセスするための裏口を仕掛けたり、機密情報を外部に送信したりする等の被害を与える。

任意アクセス制御（Discretionary Access Control）

使用者や使用者グループの情報に基づいたアクセス制御。

バイナリ

二進数の数値で表現されるデータ。コンピュータが理解して実行できるデータ形式である。文字データ以外のデータ形式全般のことを指す。

バグ

プログラムに含まれる不具合。プログラムを、バグの無い完全な状態で作成することは非常に難しいため、開発過程ではバグを取り除く作業(「デバッグ」と呼ばれる)が重要となる。

ハードウェア

マイクロプロセッサ（処理装置）、半導体メモリや磁気ディスク（記憶装置）、キーボードやマウス（入力装置）、プリンタやディスプレイ（出力装置）など、コンピュータを構成している電子回路や周辺機器。

ファイアウォール

コンピュータやネットワークを、外部からの不正な侵入から守るための防御システム。

フォールトトレランス

万一、障害が発生したとしても、正常な動作を継続する、データ損失などの被害を最小限度に抑えるための機能。

プリプロセッサ

人間が記述したソフトウェアの設計図（ソースコード）をコンピュータ上で実行可能な形式に変換する（コンパイル）前段階で、処理を加えるためのプログラム。

フールプルーフ

誤操作等により、意図せずデータの削除や送信を行う等の事故を防ぐために、これらの指示が行われた場合に確認メッセージを表示するなど、使用者による誤操作を防止するための機能。

プロセス

OS のカーネルの管理下におかれた実行中のプログラムのことを言う。通常、1 つのプログラムは 1 つのプロセスとなるが、複数のプロセスを生成するプログラムもある。

プロテクション・プロファイル

IT 製品について、要求者あるいは利用者の立場から必要と思われるセキュリティ要件を規定したもの。ISO/IEC15408 に準拠するセキュリティを確保するために定義した要求条件を既定した仕様書。セキュリティ設計仕様書(ST)を作成するに当たって参照する。

マルチタスク

一つの OS 下にて同時に複数の処理を並行して行なう OS の機能。

メーリングリスト

電子メールの一斉同報を行なうシステム。参加者のメールアドレスのリストと投稿先メールアドレスを作成し、投稿先メールアドレスに送信されたメールがリストに登録されている参加者のメールアドレスに同時配信される仕組み。

役割ベースのアクセス制御（Role Based Access Control）

使用者に与えられる役割に基づいたアクセス制御。

ロールバック機能

システムに行われた操作について、一定時間や回数まで実行前の状態に戻す機能。誤操

作等が行われた際に、情報を元の状態に戻すことができる。

ワーム

コンピュータに寄生し、自らの複製をネットワークなどにコピーし、自己増殖を行いながら、何らかの被害を及ぼすように作られたプログラム。他のプログラムに寄生せずに自己増殖する点で、ワームはウイルスと区別される。

付録２

セキュアＯＳに関する調査研究会構成員

（敬称略）

座長	村岡　洋一	早稲田大学副総長
	有田　正史	サン・マイクロシステムズ株式会社　システム技術統括本部 第一システム技術センター センター長
	石井　秀明	監査法人トーマツ　エンタープライズリスクサービス部　マネジャー
	泉澤　仁	富士通株式会社 エンタプライズシステム事業本部 Ｌビジネス推進統括部プロジェクト部長
	泉名　達也	パーソナルメディア株式会社 代表取締役
	斎　直人	東日本電信電話株式会社 研究開発センタ　サイバーシステム開発 PG 担当課長
	今井　秀樹	東京大学生産技術研究所情報・システム部門教授
	大木　一浩	特別非営利活動法人 OSPI 理事
	大野　浩之	独立行政法人通信総合研究所非常時通信グループ リーダー
	後藤　省二	三鷹市企画部情報推進室長
	阪田　史郎	日本電気株式会社 研究所 研究企画部 エグゼクティブエキスパート
	坂村　健	東京大学大学院情報学環・学際情報学府教授
	佐藤　慶浩	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
	高澤　真治	オープン・ソース･デベロップメント･ラボ(OSDL)ジャパン　ラボディレクタ
	高橋　正和	インターネットセキュリティシステムズ株式会社　IT企画室長
	田中　芳夫	日本アイ・ビー・エム株式会社 理事 開発製造、企画・事業推進担当
	寺本　振透	西村ときわ法律事務所　弁護士
	土居　範久	中央大学理工学部情報工学科教授
	中尾　康二	KDDI 株式会社 技術開発本部 情報セキュリティ室長
	中上　昇一	株式会社日立製作所 公共システム事業部電子行政事業企画本部 ソリューション創造部
	東　貴彦	マイクロソフト株式会社　取締役
	平野　正信	レッドハット株式会社　代表取締役
	水谷　寛正	トヨタ自動車株式会社 ネットワーク事業部技術室利用企画Ｇ　担当課長
	山田　伸一	株式会社NTTデータ　ビジネス開発事業本部　副事業本部長
	脇　英世	東京電機大学情報通信工学科教授