平成17年度内閣官房情報セキュリティセンター委託調査

電子政府で利用する情報システムへのセキュリティ機能を強化したＯＳの適用可能性等に関する調査研究

報告書

みずほ情報総研株式会社

目　次

はじめに

社会が情報ネットワークと IT 機器への依存度を高めていく中で、行政においても電子政府の名のもとに行政機能・サービスをインターネット等の情報ネットワークを通じて遂行・提供する動きが加速している。こうした中で、電子政府における情報セキュリティを高め、情報管理を適切に行っていくことは必須の要件であり、これを実現するためには電子政府で利用する情報システムの基盤を堅固なものとしていくことが欠かせない。情報システムの基盤の重要な位置を占めるのがオペレーティングシステム（OS）であり、これを乗っ取られたり、不正に操作されると情報システム全体の安全性が損なわれる恐れがあることから、OS のセキュリティ強化は電子政府における情報セキュリティ対策の要としての役割を担うものと言える。

内閣官房において平成 16 年度に実施した「電子政府におけるセキュリティに配慮した OS を活用した情報システム等に関する調査研究」はこうした背景のもと、セキュリティ機能を高めた OS を電子政府の中でいかに利用していくべきかについて、「強制アクセス制御」や「最少特権」など、OS のセキュリティ機能を考える上で必要となる知識の入門的な説明を交えて整理したものである。こうしたセキュリティ機能を備えた OS は「トラステッド OS」や「セキュア OS」と呼ばれ、極めて高いセキュリティレベルを要求される環境においては以前から導入されていたが、導入費用の高さや運用の難しさなどの理由により、電子政府で用いる情報システムを含む一般的な環境で利用される例は少なかった。しかるに最近、オープンソースソフトウェアの形態で提供されるセキュア OS や、既存の OS がその改良の過程でセキュア OS に近い機能を備えるようになったものなどが出現しているのに加え、商用セキュア OS への認知が拡大したことにより、セキュリティを重視して導入する事例が増加し、また OS のセキュリティ機能に関心が高まるといった傾向が見られるようになっている。

上述の平成 16 年度の調査研究では、まず情報システムの用途に応じて Web サーバ、認証局、文書管理システムの 3 種類を想定し、セキュア OS を適用することの可能性と期待される効果について検討を行った。さらに、セキュア OS 上でアプリケーションを利用する場合のアクセス制御のあり方について、OS との連携の緊密さに関する 3 つのタイプを設定し、それぞれの実現可能性について上記の 3 種類の用途毎に考察することを通じて、電子政府で利用する情報システムにおいてセキュア OS を導入することの有用性について提言を試みた。しかしながら、限られた時間で幅広い分野について検討を行ったこともあり、セキュア OS の適用可能性については理論上の検討にとどまっており、実際に導入を検討する際に参考とすべき、先行事例を通じて体得された具体的なメリットや、構築時に留意すべきポイントなどの知見が十分に集積されているとは言い難い状況にある。

そこで、本年度の調査においてはセキュア OS の電子政府システムへの適用可能性について、

先行事例調査を中心により個別具体的な検討を行った。セキュア OS を導入している先行事例の調査では、調査のターゲットが電子政府システムであるところから、官公庁における導入事例を中心とした調査を目指したものの、セキュア OS の導入事例自体が少なく、またセキュリティ上の懸念により回答を控えた組織が多かったことから、広く民間組織を含めた事例調査となった。これは結果的にセキュア OS の多様な事例の把握ができたものと考えている。

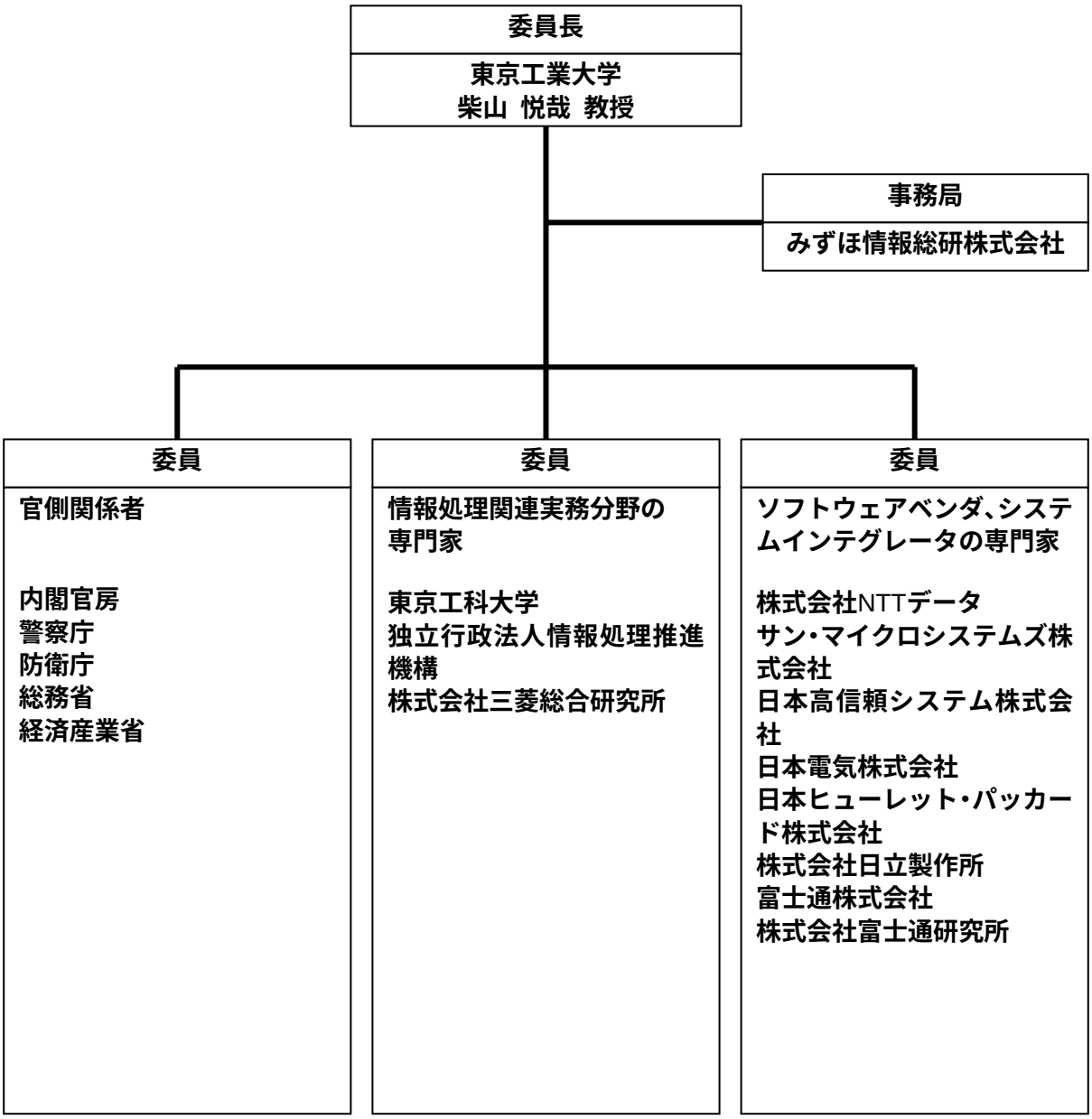
本調査のとりまとめに際しては、電子政府で利用する情報システムでの利用を想定し、情報システムの調達関係者を想定した内容となっているが、本成果はこれにとどまらず一般の情報システムの利用者、調達者においても有効に活用し得るものと期待している。

本報告書は内閣官房情報セキュリティセンター（NISC）において開催した「電子政府で利用する情報システムへのセキュリティ機能を強化したＯＳの適用可能性等に関する調査研究」検討委員会での４回にわたる議論と、同委員会の活動の一環として実施された導入事例調査の結果をもとに、みずほ情報総研株式会社がとりまとめたものである。議論に参加して頂いた委員の皆様と、ご多忙の中ご協力頂いた事例調査先組織のご担当者の皆様に、この場を借りて心より御礼を申し上げたい。

本調査研究報告書が、今後、電子政府等の情報セキュリティレベルを向上させる一助となれば幸いである。

実施体制

本調査研究は下記に示す各専門家から構成される検討委員会を編成の上実施し、その検討結果をもとに報告書を取り纏めたものである。



検討委員会委員等名簿

○民間委員（敬称略）

	氏 名	所 属 機 関 等
委員長	柴山 悦哉	東京工業大学大学院 情報理工学研究科 教授
委員	木下 俊之	東京工科大学コンピュータサイエンス学部 教授
委員	浅原 健	株式会社三菱総合研究所 科学技術研究本部戦略技術研究部 研究部長
委員	蒲田 順	株式会社富士通研究所 ITコア研究所セキュアコンピューティング研究部
委員	櫻庭 健年	株式会社日立製作所 システム開発研究所 主任研究員
委員	佐藤 慶浩	日本ヒューレット・パッカード株式会社 個人情報保護対策室 室長
委員	澤田 栄浩	日本高信頼システム株式会社 代表取締役社長
委員	寺澤 慎祐	サン・マイクロシステムズ株式会社 政策推進営業開発本部 市場開発部 部長
委員	原田 季栄	株式会社NTTデータ 基盤システム事業本部 オープンソース開発センタ 技術開発担当 シニアスペシャリスト
委員	宮川 寧夫	情報処理推進機構セキュリティセンター情報セキュリティ技術ラボラトリー 主任研究員
委員	宮田 義文	富士通株式会社 プロダクトビジネス企画本部 事業開発室
委員	依田 透	日本電気株式会社 e-ガバメントソリューション推進本部システムマネージャー
オブザーバ	岡野 直樹	サン・マイクロシステムズ株式会社 政策推進営業開発本部 政府・自治体営業開発部 ナショナルセキュリティグループ シニアアーキテクト

○官側委員（敬称略）

	氏 名	所 属 機 関 等
委員	青木 信義	内閣官房 情報セキュリティセンター 内閣参事官
委員	沓澤 正道	内閣官房 情報セキュリティセンター 内閣参事官補佐
委員	金剛 章	内閣官房 情報セキュリティセンター 内閣事務官
委員	高村 信	内閣官房 情報セキュリティセンター 内閣事務官
委員	田辺 雄史	内閣官房 情報セキュリティセンター 内閣事務官
委員	藤巻 和則	内閣官房 情報セキュリティセンター 内閣事務官
委員	堀内 雄人	警察庁 情報通信局 情報管理課 課長補佐
委員	亀田 健一	防衛庁技術研究本部 技術部 技術情報管理課 情報ネットワーク管理室 情報ネットワーク管理係 防衛庁技官
委員	佐藤 史生	防衛庁 技術研究本部 第2研究所 第1部 情報システム研究室
委員	小川 浩史	防衛庁 長官官房 情報通信課 情報保証室 部員
委員	加藤 智之	総務省 情報通信政策局 情報セキュリティ対策室 推進係長
委員	上原 智	経済産業省 商務情報政策局 情報政策ユニット 情報処理振興課 係長
委員	村野 正泰	経済産業省 商務情報政策局 情報政策ユニット 情報セキュリティ政策室 課長補佐

○検討委員会事務局

	氏 名	所 属 機 関 等
事務局	佐藤 能行	みずほ情報総研株式会社 社会システム評価部 部長
事務局	冨田 高樹	みずほ情報総研株式会社 社会システム評価部 シニアコンサルタント
事務局	中山 和郎	みずほ情報総研株式会社 社会システム評価部 コンサルタント

本報告書のポイント

○ セキュア OS のセキュリティ機能を導入することによる影響

セキュア OS はセキュリティの向上効果をもたらす反面、その導入が下記のような影響を及ぼす可能性があり、導入に際して十分な検討が必要。

①アプリケーションの動作への影響

セキュア OS では、最少特権の考え方のもとで個々の主体のもつアクセス権限を必要最小限にするようなポリシーを設定した上で、強制アクセス制御により強制力をもってそのポリシーをシステム全体に適用する。このとき、アプリケーションが必要とするアクセス権限以上の権限が与えられていないとアプリケーションは正常に動かないため、これを回避するためにアプリケーションの振る舞い（どの場面で、どの権限を用いてどのような動作をするか）の分析が重要になる。独自に開発したアプリケーションであれば問題はないが、市販パッケージソフトウェアを用いる場合はアプリケーションに対する探索的な分析を行わざるを得ない。時間的に余裕が無いなどの理由により、アプリケーションの安全性よりも動作を優先して「必要最小限」を大幅に上回る権限を与えてしまい、セキュア OS を導入したにもかかわらずセキュリティ強化の効果が不十分となる結果に陥りやすい。

②システムの運用管理への影響

システム管理者に対する内部統制の観点からセキュア OS 活用するには、通常の OS において 1 種類で扱われていた管理者を、ポリシー管理者、オペレータ、監査者など役割に応じて複数のアカウントに分割し、それぞれに必要最小限の特権のみを与える必要がある。この結果、管理者が特権的な操作を必要とする場合に、セキュア OS 上では通常の OS で行っていた動作・作業が不可能になり、作業効率の低下やコスト増を招く可能性がある。

○ アプリケーションにおけるセキュア OS との連携の可能性

Web サーバ向けのポリシーモデルを対象として、セキュア OS の機能を利用するような連携の可能性について、具体的な用途の想定のもとに以下の 2 例についてケーススタディを実施。

①シンプルな情報公開サイトの場合

静的なコンテンツのみの情報公開を行う Web サイトの場合、Web サーバプログラムの静的コンテンツに対するアクセス権限に“ 読み取り ”のみを許可し、アクセスログに対するアクセス権限に“ 追加書き込み ”のみを許可する。これにより、既存のソフトウェアを改造することなしに、静的コンテンツへの改ざん行為や、アクセスログの削除操作からの保護が可能。

②動的コンテンツを含むユーザごとに提供される情報が異なるサイトの場合

ユーザを認証し、それぞれ異なる動的なコンテンツを公開するような Web サイトの場合、コンテンツ生成モジュールを認証されたユーザ権限で起動し、アクセス対象となるリソースの管理をユーザ毎に分離することで、動作権限の必要最小化が実現される。さらにユーザ認証モジュールにおいて、アクセス権限を「読み取り」としてユーザ管理情報の改ざんを防ぐ。こうしたアクセス制御により、万一侵入が成功した場合でもシステムや他のユーザへの影響拡大が抑制される。

ただし、大規模 Web サイトを中心に利用される servlet（J2EE）や ASP.NET、また DBMS によるリソース管理のもとでは、OS のユーザに応じたアクセス制御を実現することは困難。高水準な処理性能を維持しつつセキュリティレベルを高めるには、OS、Web アプリケーションプログラムそれぞれに改良が必要。

○ OS のセキュリティ機能を活用したアプリケーションの構築

特定の業務を対象に専用のアプリケーションを構築している情報システムなどでは、セキュア OS のセキュリティ機能を活用し、OS と緊密に連携したアプリケーションとして構築することで、以下の効果により対象となる情報システムのセキュリティをさらに高めることができる。

・アプリケーション等の権限が奪取された場合の影響の最小化

・アプリケーション等の管理者による特権の範囲の最少化

・複数のアプリケーションにまたがる統一的なアクセス制御の実現

このとき、相互に連携するアプリケーション全てについて、OS のアクセス制御機能を利用するか、OS のアクセス制御に不適切な影響を及ぼさない形で設計する必要がある。このためのアプリケーションの構築手順は以下の通り。

1）アプリケーションにおける機能の流れの整理

2）ミドルウェア等の振る舞いの把握

3）アクセス制御に関する OS とアプリケーションとの役割分担の決定

4）アプリケーションからの OS のアクセス制御機能の利用

○ セキュア OS の先行導入事例調査と得られた知見

セキュア OS の適用に伴う影響や効果に関する知見を得ることを目的として、ヒアリングないし書面による先行導入事例調査を実施。独立行政法人研究機関、大学、民間企業、団体等計 8 例への調査を通じて、次の成果を得た。

①セキュア OS の導入目的

・導入目的としては、「外部からの攻撃に対する耐性強化」が主流

・内部統制を目的とするものも少数ながら有り

②システムの導入・構築におけるポイント

・セキュア OS を用いたシステムでは、「最初の設計が重要」

・アプリケーション間の連携を対象に「データの流れ」と「アクセス制御の流れ」をみる必要あり

・設計書を否応なく厳格に書かざるを得ないことが、結果的にメリットになる

③システムの管理・運用におけるポイント

・管理負荷は高めだが、運用ツールを構築時に作り込むことで通常と同程度に抑え得る

・アプリケーションの脆弱性対策のパッチを緊急で適用する必要がないことの効果は大

・専門的知識・スキルを有する人材の育成は難しい

④課題と要望

・GUI 操作への期待が大きい

・セキュア OS に関する解説資料や導入ガイドラインの提供が望まれている

○ 電子政府システムにおいて、セキュア OS の適用が特に望まれるケース

セキュア OS の導入にはセキュリティを高める効果と、それに伴う制約や課題とのトレードオフが存在するが、セキュア OS の適用による効果が各種の制約による弊害を上回り、セキュア OS を適用することが望ましいケースは以下の通り。

①「要保護情報」を扱うサーバ：電子政府において、外部向け、内部向けを問わず、要保護情報を全く含まないサーバは考えにくく、ほとんどのサーバでアクセス制御や権限管理が必要。

②インターネットに直接接続する必要のあるサーバ、ゲートウェイ：「ゼロデイ攻撃（0-day attack）」による被害は最小限に止めることが可能。さらに一定のリスクが許容できる程度の重要度のシステムであれば、セキュア OS の適用を通じて運用コストを大幅に削減できる。

③通常以上の内部統制を必要とする内部サーバ：情報漏洩や改ざんが行われた際の影響が特に大きいシステムや、国民の関心の高い情報を扱うシステムなどの場合、最少特権機能やデュアルロック（デュアルコントロール）機能を用いて管理者特権をもつ者による内部犯行を相互牽制したり、操作ログの改ざんを困難にすることが有効。

④外部からのメンテナンスを行う必要のあるサーバ：組織内に情報システムに関する専門的知識を有する職員がおらず、ベンダのオペレータが常駐することもないような場合、セキュア OS であれば外部からメンテナンスする際に利用する管理者アカウントの権限を必要最小限にすることができ、万一アカウントの認証情報が漏洩した際の影響を最小限にすることが可能。

○ セキュア OS の適用シナリオ

電子政府におけるセキュア OS の適用方法として、以下の４つのシナリオを想定。

①最小限のセキュリティ機能のみを利用：通常 OS をセキュア OS へ置換、もしくはセキュア OS 機能を有効化する以外の変更を最小限にするもの。導入に関する負荷、セキュア OS の適用効果はいずれも最小。

②OS のセキュリティ機能のみを強化：アプリケーションを改造することなく利用する場合は、本シナリオがセキュリティ向上に最も有効。アプリケーションの動作分析等、システムポリシー設定時の作業負荷は大きい。

③OS とアプリケーションそれぞれでセキュリティを強化：OS とは独立の強制アクセス制御機能を備えたアプリケーションを専用に開発することでセキュリティを向上。登録する必要のあるユーザ数が多いアプリケーションや、１つのサーバ上でアプリケーションを複数動作させる場合に好適。

④OS とアプリケーションの連携によりセキュリティを強化：OS の強制アクセス制御機能をアプリケーションから利用することにより、最も強固なセキュリティを実現することが可能。構築経験を有するベンダは稀少で割高になるが、セキュア OS の効果を最大限に活用するには最適。

○ 今後に向けた取組み

本調査の成果をもとに、電子政府におけるセキュア OS をより効果的に活用するには、今後以下のような取組みが必要と思慮。

①電子政府におけるユースケースの想定：文書管理システム等、一般論として扱うことが難しい用途に向け、より具体的な導入条件をユースケースとして想定した上で、それぞれにおけるセキュア OS の適用イメージを検討。

②構築の際に留意すべきポイントの抽出：先行導入に携わった担当者から得たコメントをもとに、セキュリティを確保したシステムを構築するために欠かせないポイント（OS の機能要件、ポリシー設定）の整理・とりまとめを行う。「チェックリスト」のようにまとめることも想定。

③構築時のガイドライン（指針）となるドキュメントの整備：電子政府で利用する情報システムにおいて、セキュア OS を用いてシステムを構築する調達者に有用となるもの。担当者によって知識に大きな差があることが想定されるため、その差に応じてそれぞれにとって有用と判断されるようなドキュメントとする工夫が必要。

第１章 調査の方針

第１章では、「強制アクセス制御」や「最少特権」ならびに「デュアルロック」等の機能を実装することにより、セキュリティ機能を強化した OS（以下、セキュア OS と呼ぶ）の適用可能性に関する調査を行った背景と、本年度実施した調査の方針について示す。

１.１ 調査の背景

「はじめに」の項で述べたように、平成 16 年度に実施した「電子政府におけるセキュリティに配慮した OS を活用した情報システム等に関する調査研究」（文献[1]）は、電子政府で利用するシステムにおけるセキュリティの確保において OS の担う役割が大きいにも関わらず、OS のセキュリティ機能に関する知識が十分に普及していないとの認識のもと、電子政府におけるセキュア OS の適用可能性について入門的な説明を交えて分析を行ったものである。

一方セキュア OS に関してはここ数年、以下のような動きがあり、セキュア OS に対する注目度はこれまで以上に高まりつつある。

（１）通常の OS におけるセキュア OS 機能の提供

これまで、セキュア OS もしくはトラステッド OS（Trusted OS）は高いセキュリティを要求される限られた用途においてのみ利用される傾向が強く、結果的にコスト高になることが多かった。ところが 2005 年以降、オープンソースの OS として普及している Linux のカーネルに LSM（Linux Security Module）ならびにこれを用いて実装された SELinux が標準で組み込まれた結果、主要な Linux ディストリビューションにおいて、特別なインストール等を行うことなしにセキュア OS の機能を利用することが可能となっている。また、HP-UX 11i2、Solaris10 などサーバ用途で広く用いられている OS についても、これまでセキュア OS のみが提供してきた機能を部分的に実装してきており、OS のコストに関する限り、通常の OS と同程度のコストでセキュア OS の機能を利用することが可能となっている。

（２）政府機関統一基準の策定

2005 年 12 月に公表された「政府機関の情報セキュリティ対策のための統一基準」において、「強化遵守事項」として、「強制アクセス制御」と「最少特権」ならびに「デュアルロック」という、セキュア OS が提供するアクセス制御機能を設けることが定められた。

１.２ 本年度の実施方針

以上の背景のもと、本調査ではセキュア OS を実際に導入するためにどのようなことに留意す

べきかを理解できるよう、以下の項目に関する分析を通じてセキュア OS の適用可能性について検討した。第 2 章以降の構成は、ここに示した方針のもとに実施された調査結果の時系列的な実施順序に基づいている。

1.2.1 セキュア OS の導入がもたらす影響

セキュア OS に移行する際に直面する最大の課題は、「これまで利用していたアプリケーションが動作しなくなる」ことである。これがどのような条件で発生するのか、回避するためにはどのような方策があるかといった事項を、セキュア OS のアクセス制御機能とアプリケーションの動作との関係をもとに整理する。

1.2.2 アプリケーション構築におけるセキュア OS 機能の活用

市販のパッケージソフトウェアなどを使用せず、業務専用のアプリケーションを構築・運用しているような場合は、そのシステムの OS をセキュア OS にすることで、セキュア OS の機能を活用してアプリケーションのセキュリティをさらに高めることができる。反面、市販のアプリケーションをセキュア OS で利用すると、利用するアプリケーションによってはセキュア OS によるセキュリティ向上の効果が限定的となることがある。こうしたアクセス制御機能に関するセキュア OS とアプリケーションの連携の可能性について、代表的な用途を例に解説する。

1.2.3 事例調査

以上の説明を通じてセキュア OS 上でアプリケーションを動作させるために留意すべき事項を把握した上で、すでにセキュア OS を用いた運用の実績がある事例について、OS のセキュリティ機能を高めようとした目的とその効果、運用上の留意点や課題などについて、各事例の当事者へのヒアリング調査を通じて得た具体的な把握内容をもとに分析する。

1.2.4 電子政府で利用する情報システムへの適用可能性の検討

事例調査を中心とするこれまでの調査結果をもとに、政府機関統一基準に準拠した強制アクセス制御機能や最少特権機能をセキュア OS の導入を通じて利用しようとする場合に留意すべき事項を整理した上で、既存アプリケーション（市販パッケージ等を含む）の利用と専用アプリケーションの構築の 2 種類に分けて適用方法の検討を行う。

第２章 セキュア OS の導入がもたらす影響

第２章では、既存の情報システムにセキュア OS を導入した場合の影響について、最も影響が大きいと考えられるアプリケーションの動作に関するものを中心に整理する。

２.１ セキュア OS を導入する際に直面する課題

セキュア OS を導入することで、情報システムのセキュリティを高めることができる反面、導入対象となる情報システムの構築や運用にはセキュア OS に特有の要件や制約が加わるため、状況によっては導入時の課題となることがある。要件や制約は大別するとアプリケーションの動作に関するもの、ポリシー設定に関するもの、運用・動作に関するものの３つに大別できる。ここでは、そのそれぞれについて具体的にどのような特徴・現象が課題になるのかを整理する。なお、実際のセキュア OS の導入に際しては、ベンダでの対応によりここに挙げた課題が回避されている場合もあり、課題とされている事項でも必ずしも影響が生じるとは限らない。

２.１.１ アプリケーションの動作に関する課題

セキュア OS 上では各アプリケーションは必要最小限のアクセス権限を与えられて動作するのが原則である。一方既存のアプリケーションはそうした考え方のもとで設計されていないものも少なくない。こうしたアプリケーションのうち、必要最小限のアクセス権限を超えたリソースへのアクセスを行っているものについては、セキュア OS 上でアクセス権限を分離しようとすると動作しなくなってしまうことがある。特に、アプリケーションが管理者特権で動作している場合は、権限の分離を行う必要性が高いことから影響が大きくなりやすい。

アプリケーションの動作への影響についての検討はセキュア OS の導入効果を高めるために重要な事項であり、２.２節にて詳しく議論する。

２.１.２ ポリシー設定に関する課題

セキュア OS の導入の目的は、通常の OS と比較してより詳細なアクセス制御を行うことにより、本来の目的以外の不適切なアクセスを排除するところにある。そこでこのアクセス制御を行うためのポリシー設定は極めて重要な作業となるが、通常の OS と比較したポリシーの内容が一般に著しく複雑になることから、設定操作に関して課題が生じることも少なくない。

具体的な課題については、代表的なものとしては以下が挙げられる。

（１）設定すべき項目が多い

これはポリシー設定・変更に関わる絶対的な操作量が多くなることを意味する。単に項目が増

えた分だけ作業が増えるのではなく、それぞれが相互に関連するため、作業負荷の増加量はポリシー項目の数に比例する以上のものとなる。もっとも、実際の導入場面では設定負荷を最少にするための工夫が講じられており、セキュア OS の設定に際して常に膨大な設定が必要なわけではない。こうした設定場面において、ポリシーについての十分な理解と設計を経ずにあやふやな設定操作を行うと、アプリケーションが動作しなくなる可能性が高くなる。これを回避するために単純にポリシー設定を甘くするようでは、セキュア OS を導入した意味が無くなってしまう。

（2）OS 毎に概念が異なる

これはセキュア OS やトラステッド OS の種類によって、アクセス制御を行うための機能を指す名称が異なっていることを意味している。現在製品として提供されているセキュア OS はそれぞれ独自の研究開発成果に基づくものであるため、製品が異なると名前だけでなく、設定方法なども全く別のものとなり、あるセキュア OS で得た知見が別の OS で活かせない結果ともなっている。

（3）GUI が使えない場合がある

現在では通常の OS では GUI（グラフィカルユーザインタフェース）が利用できるのが一般的である。これに対してセキュア OS やトラステッド OS では、操作性よりもセキュリティの高さを優先した結果、テキストベース（キャラクタユーザインタフェース、CUI）で操作を行う仕様となっている製品が存在する。実際の運用管理における作業の生産性においては、CUI であることは問題にはならず、むしろコマンドをまとめて間違いなく操作する場合などでは GUI よりも便利な場合も多いが、導入時の抵抗感などの面で GUI が利用できることのメリットも大きい。

（4）必要なツールが整備されていない

（1）で示した通り、セキュア OS の特徴を活かした運用を行うためにはポリシー設定作業に多くの負荷が発生するが、設定される内容には一定の規則性があり、多くの項目はある条件をもとに機械的に設定内容を決めることが可能である。そこで、ポリシー設定用のツールがあれば作業の負荷を軽減することが期待される。しかしながら、現在提供されているツールは対象が特定の OS に限定されたり、設定可能な内容が限られたものであることが多い。そこで、利用条件によっては全くツール利用の恩恵を得られないこともある。

2.1.3 運用・管理に関する課題

セキュア OS の運用管理については、原則として通常の OS と異ならないことが原則である。ただし、以下の点で通常の OS とは異なる対応が求められる場合がある。

（1）ポリシーのメンテナンスに伴う専門的知識の必要性

上述の通り、セキュア OS では複雑なポリシー設定の中でアプリケーションを動作させることになるため、例外的な条件が生じた場合にアプリケーションにエラーが生じることが通常の OS と比較して多くなることが予想される。周辺条件が変化した場合もポリシーの修正が必要となるが、現在の製品においてはポリシーの修正には専門的な知識が必要となることが多く、情報システムの利用側組織の管理担当者はもとより、ベンダによるメンテナンスを行う場合であっても、通常の体制では対応できない場合がある。

（2）管理者特権の分割に伴う管理負荷の増大

通常の OS の場合、管理者特権があると対象となるシステムについて全てを操作できる権限が得られるため、リスクの大きさと背反して操作は効率よく行うことができる。一方セキュア OS においては、後述（2.2.2（2）、19 ページ）するように内部統制の強化を目的として管理者特権を目的に応じて複数のアカウントに分けて割り当てることがあり、こうした場合は作業の種類に応じて複数のアカウントを使い分けなければならない。このような特徴が管理作業の負荷増大をもたらす場合がある。

２.２ セキュア OS のセキュリティ機能とその影響

前節で示した課題のうち、セキュア OS の導入がアプリケーションや運用・管理に及ぼす影響については、セキュア OS が提供するセキュリティ機能を活用することでより一層生じやすくなることから、導入に際して十分な検討を行っておく必要がある。そこで、強制アクセス制御や最少特権など、セキュア OS の機能が及ぼす影響について整理する。

２.２.１ セキュア OS におけるセキュリティ機能：強制アクセス制御と最少特権

セキュア OS の定義は厳密には定められていないが(米国 NSA 策定の LSPP(Labeled Security Protection Profile）を利用した製品を指すこともある)、一般には強制アクセス制御と最少特権の２つの機能を備えていることをその要件としていることが多い。このことからも明らかなように、強制アクセス制御と最少特権はセキュア OS のセキュリティ機能の主要な役割を担うものである。それぞれの機能の概要を以下に示す。

（１）強制アクセス制御

これまで通常の OS で用いられてきたアクセス制御の方法は、任意アクセス制御(Discretionary Access Control：DAC）と呼ばれる。これに対し、あるシステムポリシーをそのコンピュータシステム内のユーザやプログラムに対して強制できる機能が**強制アクセス制御**（Mandatory Access Control：MAC）である。強制アクセス制御のもとでは、ファイルの所有者やプログラムの実行者であっても、自らの思い通りに制御することはできず、不正なプログラムの実行や無権限者によるアプリケーションの実行を防止することができるなどのセキュリティ上の効果が得られる。

（２）最少特権

通常の OS において、UNIX や Linux であれば root、Windows では Administrator という名前で知られる管理者（スーパーユーザ）アカウントは、システムの設定や管理のためのオールマイティな権限を持つ。これは、シンプルな構成での管理を行う上で有効である反面、万一この管理者アカウントが攻撃者に乗っ取られた場合は完全にそのコンピュータを自在に操られてしまうというリスクがある。さらに、システム管理者は自ら行った操作の証跡となる記録（ログ）を自由に削除できるため、システム管理者に対する内部統制が機能しないといった、セキュリティ上の問題を内包する。そこで、コンピュータシステム内の主体（ユーザやプログラム）の持つ強力な権限を役割や用途に応じて分割し、個々の権限は必要最小限にするという考え方を、**最少特権**（least privilege）と呼ぶ。最少特権化することにより、不正侵入を受けた場合の影響の局限化、最小化や、管理者特権をもつユーザに対する相互牽制機能といった効果が期待できる。

２.２.２ セキュリティ機能がもたらす影響

上述したような強制アクセス制御と最少特権の２つの機能を導入することで生ずる影響について、以下に例示する。

（1）アプリケーションの動作への影響

セキュア OS では、最少特権の考え方のもとで個々の主体のもつアクセス権限を必要最小限にするようなポリシーを設定した上で、強制アクセス制御により強制力をもってそのポリシーをシステム全体に適用することになる。このとき、設定したアクセス権限とアプリケーションが必要とするアクセス権限が一致していないと、動作に必要な権限が得られないため、アプリケーションが動かなくなってしまう。

例えば Web サーバにおいて、Web の閲覧者から入力されたリクエストをもとに内部のデータベースを呼び出して検索し、結果を Web ブラウザに表示するようなサービスを考える。この場合、システムポリシーにおいて Web サーバの実行とデータベースの実行とをそれぞれ適切な条件のもとで許可するアクセス権限設定を行う必要があるが、許可の範囲を必要以上に狭くすると本来認められるべき動作が不可能になってしまい、逆に広くすると不正なアクセスの遮断が困難になる。このような内部構造や連携関係をもつサービスにおいては、実装に際してサービスで使用するアプリケーションの振る舞いを予めよく分析・把握しておくことが重要となる。Web サーバの場合であれば、適切な入力に基づく応答のほか、誤入力や悪意のある操作、データベース側の異常や通信の不調など、実際の運用場面で想定されるあらゆる動作を列挙した上で、それらに対する適切な対応を可能にするようなアクセス権限設定の組み合わせを用意することになる。

このとき、Web サーバ上で利用するアプリケーションが自組織用に開発されたもの（カスタム開発）であればその設計資料やソースコードを参照できるので、ポリシー設定をアプリケーションの振る舞いに応じた形で動作するように設計を見直し、再構築することで対応することは容易である。しかしながら、データベースなどに市販パッケージソフトウェアを用いているような場合は、アプリケーションの動作に関する十分な情報が得られない場合が多い。その場合はアプリケーションの振る舞いを探索的に把握せざるを得ないため、前述したような実際に想定される Web サーバの運用場面の全てについて、システムポリシーを適切に設定することは容易なことではない。開発スケジュールの都合による時間的余裕の無さなどから振る舞いの分析が不十分なまま、Web サーバとしての動作を優先させるために、アプリケーションに対して「必要最小限」を上回る権限を与えることになりがちである。この結果、セキュア OS を導入したにも関わらず、最少特権化によるセキュリティ強化の効果が不十分となる場合が生ずることになる。

（2）システムの運用管理への影響

システム管理者に対する内部統制の観点からセキュア OS のセキュリティ強化機能を効果的に活用しようとすると、通常の OS において１種類で扱われていた管理者を、システムポリシー管理者、ユーザアカウント管理者、バックアップのオペレータ、監査者など役割に応じて複数のアカウントに分割し、それぞれに必要最小限の特権しか与えないようにする必要がある。この結果、アプリケーションの中でシステムないし管理者が特権的な操作を必要とする場合、セキュア OS 上では通常の OS で行っていた所定の動作・作業が不可能になる可能性がある。

例えば Web サーバの場合、管理者の特権は以下のように分割することができる。

① OS のポリシーの制御（設定、修正）

② Web アプリケーションを扱うユーザの管理（登録、削除、パスワード再設定）

③ システムとアプリケーションの実行制御（起動、停止）、修正パッチの適用

④ システムのバックアップ

⑤ ①～④に関する管理者による操作のログの閲覧（監査）、保存、削除

このような分割をすることにより、本来バックアップ操作のみの役割をもつ管理者が、必要のないデータを閲覧したり、自らの作業履歴を改ざんするような不正を防ぐことができる。また、万が一の場合に③の管理者特権を不正侵入者に奪われるようなことがあっても、①や②の管理者権限に割り当てられているポリシーの変更や不正ユーザの作成などができないため、乗っ取りによる影響を最小限に抑えることができる。反面、アプリケーションに修正パッチを適用するような場合、アプリケーションのバージョンが変更になることでポリシーの修正が必要になることがあるが、③の管理者の権限では①の操作は不可能であるため、必ず両者が連携して操作を行う必要がある。こうした結果、Web サーバを適切に動作させるための運用管理作業に要するコストは、どうしても通常の OS よりも増大してしまうことになる。

２.３ アプリケーションの動作とセキュリティ機能との関係

これまで、セキュア OS を導入するなど OS のセキュリティ機能を高めたとき、アプリケーションが動作しなくなる原因として、システムポリシーの設定が不適切であることや、アプリケーションの動作に必要となる権限が本来あるべき必要最小限を超えていることなどを示してきた。ここでは、こうしたアプリケーションの動作と OS のセキュリティ機能との関係について、さらに詳細な検討を行う。

２.３.１ セキュア OS やトラステッド OS におけるアプリケーションの動作の仕組み

かつてトラステッド OS の導入が開始された頃、その API（Application Program Interface、画面への表示、データの入出力など OS が提供する機能をアプリケーション側から利用するために OS が用意しているインタフェース機能）は通常の OS とは異なる独自のものであったため、トラステッド OS に対応したアプリケーションしか動作しない問題があった。一方現在のセキュア OS は、通常の OS としても利用可能な製品や、通常の OS で動作するアプリケーションの動作を保証しているものが中心であり、OS の設定を適切に行うことで通常の OS と同じアプリケーションが動作する場合が多い。これはセキュア OS が提供する API が通常の OS と互換性を有するように設計されるようになったためである。しかしながら、API は互換性があっても OS の内部は当然のことながら異なり、セキュア OS ではセキュリティ機能を強化した実装が行われている。そこでセキュア OS のシステムポリシーに反する条件のもとでアプリケーションが動作しようとすれば、OS によってその動作が制限されることになる。

アプリケーションが実行しようとする内容がシステムポリシーを満足しているかどうかの判別は、アプリケーションの動作を多数の「システムコール」と呼ばれるきわめて単純化した手続きに細分化した中で行われるので、仮にどこかのシステムコールでシステムポリシー違反が生じ、その結果としてアプリケーションが動作しなくなったとしても、アプリケーションの利用者からはどこでエラーになったのかがわかりにくい。こうした理由により、「セキュア OS にするとアプリケーションが動作しなくなる」という印象を利用者に与える結果となっている。

なお導入（インストール）時点における OS のシステムポリシーの設定方針は、セキュア OS の種類に応じて以下の２種類に大別される。

① 導入時点ではすべてのアプリケーションの動作が禁止されており、必要な設定を解除していくことでアプリケーションの動作を可能にするもの（SELinux の strict ポリシー等）

② 導入時点ではすべてのアプリケーションの動作が可能であり、セキュリティ強化の立場から不要な動作権限の制限（ロックダウン）を行っていくもの（Trusted Solaris 等）

２.３.２ セキュリティ機能とアプリケーションの動作とのトレードオフの関係

前述した強制アクセス制御や最少特権等の機能は、アプリケーションの動作やシステムの操作に関して OS により強力な制約を加えることを通じて、セキュリティを高める仕組みである。しかしながらこれまでの検討を通じて、アプリケーションを動作させるため、こうした制約を緩める必要が生じる場合もあることがわかる。この場合、OS が用意しているセキュリティ機能が十分に機能しなくなる。このように、セキュリティ機能とアプリケーションの動作はトレードオフの関係にある。

また、市販のパッケージソフトウェアなど、アプリケーションに手を加えることが困難な場合において、当該アプリケーションが下表に例示するような条件を課すものであれば、表の右列に示すような影響が避けられない。このような条件を備えたアプリケーションについては、たとえセキュア OS 上で動作させても、本来セキュア OS が提供すべきセキュリティ機能を発揮させることは難しく、セキュリティを十分に高めることができない。

表 2-1　アプリケーションの課す条件がもたらすセキュリティ上の影響の例

アプリケーションが課す条件	セキュリティ上の影響
アプリケーションを構成するプログラムの一部が、管理者権限を示す特定の名称（root、Administrator 等）での実行を要求する	• アプリケーションに対する強制アクセス制御機能の導入が困難になる場合がある • 管理者権限の最少化が不完全になる場合がある
アプリケーションを構成するプログラムを保存しているディレクトリに対してアプリケーションが書込みを行い、その書込み先の変更が不可能	• 強制アクセス制御機能を用いてアプリケーションの改ざんを防ぐことが困難になる
アプリケーションが処理の過程で一時的に作成するデータの保存先の変更が不可能	• 強制アクセス制御機能を用いてアプリケーションの動作を攻撃者による不正から保護することが困難になる場合がある
アプリケーションが生成するログファイルの保存先の変更が不可能	• 強制アクセス制御機能、最少特権機能を用いてログファイルの改ざんを防止することが困難になる場合がある

第３章 アプリケーションに対するセキュア OS 機能の活用

前章では既存のアプリケーションをセキュア OS 上で動作させる場合の影響を中心に、セキュア OS の導入による課題について整理した。第３章では視点を変えてセキュア OS の提供するセキュリティ機能を積極的に活用する方法について、具体的な用途に応じたケーススタディを紹介するとともに、セキュア OS の機能を活用するためにアプリケーション、ミドルウェアに求められる要件などを示す。

３.１ セキュア OS とアプリケーションとの連携可能性の整理

OS とアプリケーションの連携の考え方としては、昨年度の調査研究「電子政府におけるセキュリティに配慮した OS を活用した情報システム等に関する調査研究」（文献[1]）において、セキュア OS の適用形態のモデルが示されている。標準的なシステムをアプリケーション、ミドルウェア、OS、ハードウェアといった 4 階層に分類し、適用されるアプリケーション、ミドルウェアのタイプ別に 3 つの適用形態モデルを提示している。

- モデル①：セキュア OS のみ適用モデル
  強制アクセス制御機能を有さないアプリケーション、ミドルウェアを利用
- モデル②：セキュア OS 適用、かつアプリやミドルのセキュリティ機能強化モデル
  OS の強制アクセス制御機能とは別に、強制アクセス制御機能をはじめとするセキュリティ機能の強化を行ったアプリケーション、ミドルウェアを利用
- モデル③：セキュア OS 適用、かつアプリやミドルのセキュア OS 機能利用モデル
  OS の強制アクセス制御機能を有効活用したアプリケーション、ミドルウェアを利用

モデル①は、既存のアプリケーション、ミドルウェアに特に変更を加えないことが前提となっている。そこで、セキュア OS にて提供される強制アクセス制御のポリシー設定は、アプリケーションやミドルウェアの動作を詳細に解析しながら行うことになる。

例えば SELinux におけるアクセス制御の手段である Type Enforcement を設定する場合、制御対象となるアプリケーションから起動される可能性のある得るすべてのプログラムに対して、アクセスの挙動を把握するだけではなく、プログラムの親子関係や相互の連携構造についても把握しなければ適切な設定を行うことはできない。アプリケーション、ミドルウェアがセキュア OS の機能を有効に活用できるかどうかの判断には OS 及びアプリケーションに関する高度な知識が要求されるため、理想的なアクセス制御の設定を実現することは容易ではない。

モデル②は、アプリケーション、ミドルウェアが独自にセキュリティ機能を強化していることから、アプリケーション、ミドルウェアの内部処理に踏み込んでセキュア OS による強制アクセス制御を事細かに強制させる必要性が小さくなる。アプリケーション、ミドルウェア内でアクセス制御がそれぞれ強化されているため、セキュア OS 側に要求される設定としてはアプリケーション、ミドルウェアの単位で影響するリソース範囲に必要な権限の設定を行えばよい。

しかしアプリケーション、ミドルウェアにバッファ・オーバーフローやストリング・フォーマットバグ等の脆弱性によってプログラム動作の制御を奪われてしまった場合は、アプリケーション、ミドルウェアの単位でアクセス可能なすべてのリソースに影響が及ぶことは避けられず、リスクの範囲が大きくなるので注意が必要である。

モデル③は、セキュア OS を適用する場合において理想的なモデルと考えられる。セキュア OS にて提供する強制アクセス制御機能を有効に動作させるために、既存のアプリケーション、ミドルウェアを改造、または新規に開発することにより、セキュア OS 側で決定するセキュリティポリシーを満たすようなシステムが構築できる。

しかし全くのゼロベースからアプリケーション、ミドルウェアなどを開発しようとすると、モデル①、モデル②と比較してシステムの初期導入時のコストが増大するのは避けられない。オープンソースをベースとして有効利用し、初期コストを抑える方策が考えられるが、この場合はモデル①と同様、アプリケーション、ミドルウェアの動作を理解した上で改造を行っていく必要がある。改造によっても目標に応じたセキュリティポリシーの実現や、高度なセキュリティレベルの達成は可能であるが、ベースとなるアプリケーション等に関する高度な知識と開発経験を備えていなければ成功は望めない。また、商用実績があるオープンソースで、開発ベースの候補となるアプリケーション、ミドルウェアは、どれも強制アクセス制御による動作制御、最少特権構造を念頭において開発されてきたものではない。ソースコードこそ公開されていても、実装仕様や設計コンセプトをまとめたドキュメントが存在しないケースがほとんどである。こうした状況を考慮すると、むしろゼロベースで設計及び開発を行う方が効率的になる可能性もある。

３.２ セキュア OS とアプリケーションとの連携のケーススタディ

前節にて示した各モデルの特性を踏まえ、セキュア OS とアプリケーションの連携に関するケーススタディを示す。ここでは、既存の Web サーバのポリシーモデルについて、セキュア OS の機能を利用するためのアクセス制御の設定や改造の可能性について検討する。

ここで想定される Web サーバとしては、著名な製品である Microsoft 社の Internet Information Server、オープンソースソフトウェアの Apache などが挙げられる。これらは標準のインストール状態において強制アクセス制御（MAC）機構を実装していないため、おおむねモデル①のケースに該当する。

３.２.１ シンプルな情報公開サイトの場合

アクセスするユーザごとに制御されるべきコンテンツなどを含まない、シンプルな静的なコンテンツのみを情報公開する Web サイトであれば、アクセス制御対象となるサブジェクトは「Web サーバプログラム」、オブジェクトは主として「静的コンテンツ」と「アクセスログ」を考慮すればよい。つまり Web サーバプログラムの静的コンテンツに対するアクセス権限に“ 読み取り ”のみを許可し、Web サーバプログラムのアクセスログに対するアクセス権限に“ 追加書き込み ”のみを許可すれば、Web サーバプログラムに何らかのセキュリティホールが存在し、攻撃されて不正なプログラムが実行されてしまったとしても、静的コンテンツへの改ざん行為や、アクセスログの削除操作は防止される。既存の著名 Web サーバソフトウェアを特に改造することなく、セキュア OS の機能を十分に活用することが可能であると考えられる。

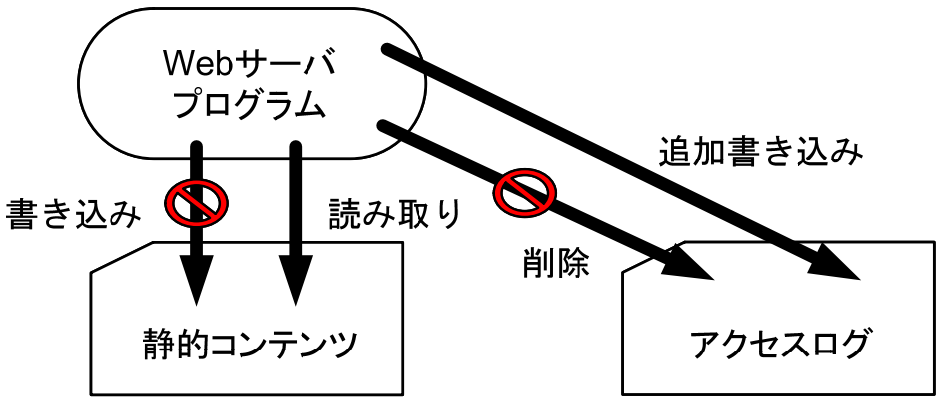


図 3-1　シンプルな情報公開サイトの場合

リスクの適切な分散を行うには、強制アクセス制御のポリシーを設定する前提条件として、不要な権限を排除するために初期設定条件に「設定を行っていないプログラム（プロセス）のオブジェクトに対するアクセス権限は、すべて拒否」（All Denial）という条件が必要になる。実際に

Web サーバプログラムには、サーバとして動作するための設定ファイルの読み込み、読み込まれたコンテンツをリクエスト元に対して送信するための権限設定なども必要になるため、図３－１に示される設定だけでは正しく動作しない。正常に動作させるには、Web サーバプログラムの振る舞いの詳細を把握した上で、各種オブジェクトに対する操作権限の設定を行う必要がある。

３.２.２ 動的コンテンツを含むユーザごとに提供される情報が異なるサイトの場合

アクセスするユーザごとにアクセス制限されるべきリソースを持ち、動的なコンテンツを公開する Web サイトを考える。ユーザを認証し、動的なコンテンツを生成する過程で Web サーバプログラム以外に Web アプリケーションプログラムを起動する必要が発生する。ここでは「ユーザ認証モジュール」と「コンテンツ生成モジュール」が動作するケースを想定する。

まずコンテンツ生成モジュールについては、ユーザからの要求毎にユーザ情報に基づいて各リソースへアクセスする権限が必要になる。そこで OS レベルで設定される当該プログラムの権限としては、通常はすべてのユーザのリソースへアクセス可能な権限が設定される。つまりこのモジュールにセキュリティホールが存在して攻撃され、不正なプログラムが実行されてしまうと、すべてのユーザのリソースに不正行為が行われてしまう可能性がある。

このようなリスクを低減するためには、コンテンツ生成モジュールの動作権限を必要最小限に絞り込む必要がある。コンテンツ生成モジュールは、各動作のタイミングにおいて、要求元ユーザ以外のユーザのリソースへアクセスする必要はないため、“ 認証された個々のユーザ権限の範囲で動作すること ” が最小限の条件である。つまりコンテンツ生成モジュールの起動が、認証されたユーザ権限で起動され、アクセス対象となるリソースの管理もユーザ毎に分離されていれば、このアクセス制御は実現される。この場合、コンテンツ生成モジュールのバグにより制御権を奪われたとしても、ユーザ情報に基づく権限内での不正行為にとどまるため、他のユーザへ影響が拡大することはない。

ユーザ認証モジュールは、アクセス元を確認するために動作するプログラムであり、すべてのユーザ ID、パスワードに対してアクセスする必要がため、コンテンツ生成モジュール同じような最小権限設定を行うことはできない。しかしユーザ認証モジュールのユーザ管理情報（すべてのユーザ ID、パスワード）に対するアクセス権限を「読み取り」のみとしてその他一切の権限を与えなければ、当該モジュールの脆弱性によりプログラム制御権限を奪われた場合でも、ユーザ管理情報への改ざん行為を防止することができ、また各ユーザの管理するリソースを含めた任意のアクセスも防止される。ユーザ ID やパスワードの漏洩をアクセス制御で防止することはできないが、ハッシュなどの暗号技術などの対策を講じることによって、パスワード値そのものの漏洩を防ぐことは可能であり、被害を最小限に抑えることが可能である。

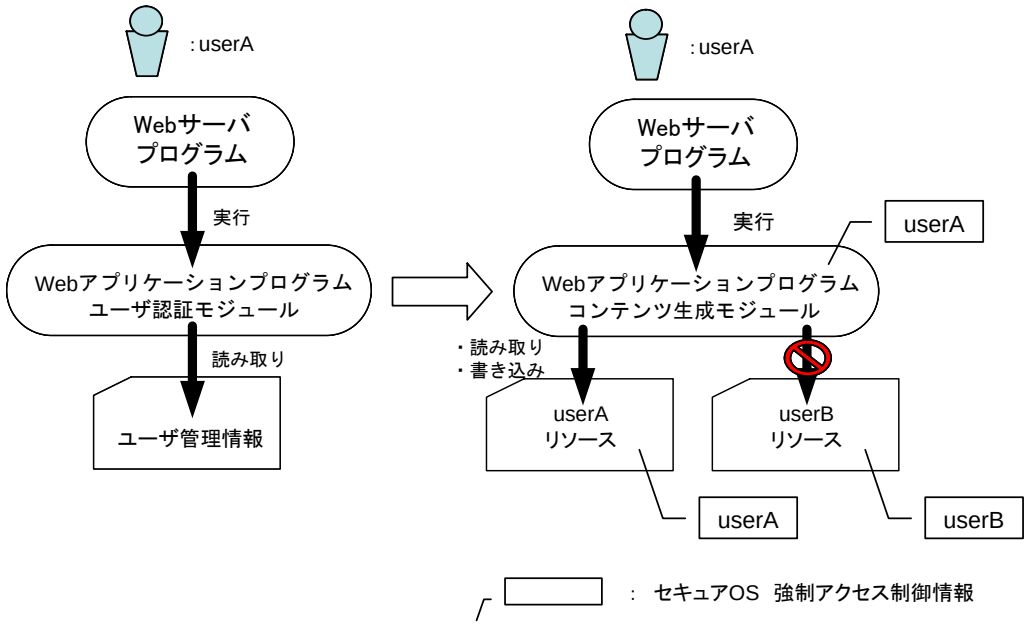


図 3-2 動的コンテンツを含むユーザごとに提供される情報が異なるサイトの場合の処理

しかし本ケースで想定する強制アクセス制御の実現には課題がある。本方式では、制御されるユーザごとにプロセスが起動される仕組みが必要となる。小規模 Web サイトなどでは、個別動作ごとにプロセスを起動する CGI も根強く利用されてはいるが、大規模 Web サイトにおいては高いパフォーマンスを維持するために、処理オーバヘッドの大きいプロセスを複数起動することを必要としない servlet（J2EE）や ASP.NET などの利用が現在主流となっている。これらで開発された Web アプリケーションプログラムに対しては、本ケースで示した方法による強制アクセス制御は実現することができない。

またリソース管理の面でも課題が残る。大規模 Web サイトにおいて扱われるリソースは、DBMS で管理されるデータ集合体であり、複数のファイルに分割されるものではない。しかし制御対象オブジェクトとして DBMS レコードを定義することは困難であり、ゆえにユーザ毎の制御ラベルを設定するようなアクセス制御はできない。ユーザ毎に制御ラベルを設定する際の単位系（例えばファイルなど）でリソースを分割することは技術的には可能であるが、ファイル単位の処理も複数のプロセス起動と同様に負荷が大きいため DBMS のメリットであるデータの高速処理を大きく阻害する恐れがある。

現段階でのセキュア OS 技術、及び著名な Web アプリケーションプログラムをベースとした検討範囲においては、処理性能とセキュリティレベルはトレードオフの関係にならざるを得ない。高水準な処理性能を維持しつつ、セキュリティレベルを高めるには、OS、Web アプリケーション

プログラムそれぞれに改良が必要である。OS 側に要求される改良としては、OS が制御する対象であるサブジェクトにスレッド等も加味した制御単位の細分化が挙げられる。また OS が制御するオブジェクトには、DB レコードなどの扱いが可能になることが期待される。Web アプリケーションプログラムに要求される改良としては、OS が扱えるサブジェクト、オブジェクト単位とをベースとした仕様設計及び実装を行うことなどが考えられる。

３.３ OS のセキュリティ機能を活用したアプリケーションの構築

特定の業務を対象に専用のアプリケーションを構築している情報システムなどでは、モデル③をもとにセキュア OS のセキュリティ機能を活用し、OS と緊密に連携したアプリケーションとして構築することで、対象となる情報システムのセキュリティをさらに高めることができる。

本節ではその効果と構築の考え方について示す。

３.３.１ OS のセキュリティ機能の活用による効果

アプリケーションにおいて OS のセキュリティ機能を活用することによる効果としては、以下の（１）～（３）に示すような事項が挙げられる。

（１）アプリケーション等の権限が奪取された場合の影響の最小化

アプリケーションやミドルウェアに存在する脆弱性により、それらの動作権限を攻撃者に万一奪われた場合でも、アクセス制御を OS で行っていれば攻撃者はアクセス権を変更することができない。アプリケーションやミドルウェアでアクセス制御をしている場合の被害についてはアプリケーション等の設計に依存するが、最悪の場合はアプリケーション上でのアクセス制御による効果を攻撃者に無効にされてしまう可能性がある。

（２）アプリケーション等の管理者による特権の範囲の最少化

アプリケーションやミドルウェアでアクセス制御を行う場合、ユーザの識別はアプリケーションやミドルウェアの内部で作成されたユーザアカウントによって行われる。よって、こうしたアカウントに関する権利の設定を行うアプリケーションの管理者は、アプリケーション内の全てのユーザを上回る特権をもつことになり、アプリケーションにおける内部統制が不十分となる恐れがある。アクセス制御を OS で行っていれば、アプリケーション管理者も OS で設定されたアクセス権限の範囲でしか制御できないため、万一内部犯行が企てられるような場合でも影響範囲を狭めることができる。

（３）複数のアプリケーションにまたがる統一的なアクセス制御の実現

アプリケーション（ミドルウェアとの組合せを含む）の動作がアプリケーション内部に閉じている場合、すなわちアプリケーションの動作が他のアプリケーションや OS の動作に影響を与えない場合は、アクセス制御を OS とアプリケーション内部のいずれで実施しても、情報システムのセキュリティ面からの影響の相違は小さい。しかしながら、実際のアプリケーションにおいては、あるアプリケーションが別のアプリケーションやサービスを呼び出すことがないもののほうが珍しい。複数のアプリケーションに関わるアクセス制御をアプリケーション毎に制御しようと

すると、両者の整合性の確保はきわめて困難になる。このような場合は、OS においてアクセス制御の方針を強制力をもって定め、各アプリケーションは OS の機能を利用することを通じて、自らのアクセス制御を実現させることが、統一的なアクセス制御のために有効である。

3.3.2 OS のセキュリティ機能を活用したアプリケーション構築の方法

上述のように、OS のセキュリティ機能を活用するためには、相互に連携するアプリケーション全てが OS のアクセス制御機能を利用するか、OS のアクセス制御に不適切な影響を及ぼさない形で設計されている必要がある。こうした設計を行うためには、以下の要件を満たした形でアプリケーションを構築することが考えられる。

（1）アプリケーションにおける機能の流れの整理

情報システムの構築に先立ち、システム上で動作させようとする主要なアプリケーションを対象に、情報と制御の流れをフロー図などにより整理する。これがアクセス制御をシステムポリシーの形で実装する時の前提条件となるため、異常データが入力された場合や攻撃を受けた場合、連携するアプリケーションが応答しない場合など、想定されるあらゆる場面を想定して、あるべき動作を定めることが望ましい。

（2）ミドルウェア等の振る舞いの把握

アプリケーションの動作に際してミドルウェアを必要とする場合、OS 上でミドルウェアがどのような振る舞いをするかについても（1）と合わせて把握しておく必要がある。ミドルウェアについては製品を利用する場合など、詳細な設計資料を入手できないこともある。この場合はミドルウェアを実際に動作させながら、どのようなアクセスを行うかを探索的に把握する必要が生ずることもあり、構築コストの増加要因となり得る。

（3）アクセス制御に関する OS とアプリケーションとの役割分担の決定

ユーザの種類に応じたアクセス制御を行う場合、ユーザ管理を OS で行うか、アプリケーションで行うかの役割分担を予め決めておく必要がある。通常の OS における一般的なアクセス制御の方法では、OS 上にアプリケーション用のユーザを作成してアプリケーションはこのユーザ権限で動作させ、アプリケーションを利用するユーザの識別はアプリケーション上に作成したユーザアカウントをもとに行うことが多い。これに対して、OS のアクセス制御機能を活用するアプリケーションにおいては、OS 上に作成したユーザアカウントをもとに強制アクセス制御を行うこともできる。このような強制アクセス制御機能を実装するのが、3.1 節においてモデル③として定義した方法である。一方、OS とは独立してアプリケーションのセキュリティ機能を強化する方法が

モデル②である。モデル②とモデル③のどちらが適切かは、以下に示すようにアプリケーションの用途やユーザの数などによって決まると考えられる。

- モデル②の場合、アプリケーションに脆弱性が存在してアプリケーションの制御が乗っ取られた場合、アプリケーションで行っているユーザ単位のアクセス制御が無効となる可能性がある。これに対し、モデル③では OS レベルでアクセス制御を行っているため、たとえアプリケーションが乗っ取られても、乗っ取られたプログラムに関係するユーザ以外への影響は最小限に抑えられることが期待される。従って、モデル③はデータベースサーバのように、極めて重要な情報を保持するアプリケーションの被害を最少化するために適している。
- モデル③の場合は、アプリケーションを利用するすべてのユーザのアカウントを OS 上に作成しなければならないため、ユーザの数が多くなるとバックアップ作業などを通じて OS の管理の手間が増す。また、OS のユーザアカウントの数が多いと、ユーザの認証情報が漏洩することにより OS に不正侵入されるリスクが高まることを意味する。セキュア OS を適切に運用している場合は、アクセス権限を制限されたユーザアカウントの漏洩に過剰に神経質になる必要はないが、不要なリスクを下げる観点から、アプリケーション上にのみユーザアカウントを作成し、ユーザの認証情報が漏洩した場合の影響を当該アプリケーションに限定することは検討されて良い。また、１台のサーバで複数のアプリケーションを動作させる必要がある場合は、OS で認証するよりもアプリケーション上で認証するほうが、被害の局限化に有効となる場合もある。このような判断が有効なアプリケーションとしては、インターネットなど外部ネットワークに向けて設置されるプロキシサービスなどが想定される。

（4）アプリケーションからの OS のアクセス制御機能の利用

（3）においてモデル③を選択した場合は、アプリケーションの開発に際して OS のセキュリティ機能をアプリケーションから呼び出す必要がある。このような呼び出しの実装手段として、TAPI（TSIX Application Programming Interface、TSIX は Trusted Security Information Exchange の略称）が用意されている。TAPI は POSIX の 1003.6（注：現在は廃止されている）で規定されたインタフェース仕様であり、この規格に基づいて開発されたアプリケーションであれば、異なるセキュア OS のもとで動作させることが可能な互換性を有する。

一方、強制アクセス制御（MAC）に関するラベル情報をネットワークを介して伝達することを目的として、セキュア OS の業界標準として「MaxSix」と呼ばれる規格をかつて利用することができた。これにより、例えば HP と Sun とで通信しても互換性が確保された。現在、MaxSix は使われていないが、これは高いセキュリティを求めるシステムであれば、マルチベンダで構築することであえて管理を複雑にする必然性はなく、異なるプラットフォーム間での連携に関する需要がなかったためである。

現時点においては、日本国内にて TAPI のような仕様をもとに開発されたアプリケーションはほとんど存在せず、開発を行う場合も専門知識をもったベンダに発注することが必須となるため構築コストが割高になることは避けがたい。ただし、ここで示したような OS のセキュリティ機能を利用することによってアプリケーションのセキュリティが向上することは確実であり、セキュリティを重視するアプリケーションの構築の際には、こうした開発方法を念頭においた検討を行うことが望まれる。

第４章 セキュア OS 導入事例の分析

本章では、セキュア OS の適用に伴う影響や効果に関する知見を得ることを目的として実施した、先行導入事例に関する調査内容とその分析結果について示す。

４.１ 調査の方法

今回の事例調査の実施方針と具体的な方法について示す。

４.１.１ 調査の実施方針

事例調査を通じて有効な成果を得るには、調査先組織の協力を得ることが必須の要件となる。このとき、これまでセキュア OS を導入してきた機関は、機微な情報を扱うことを目的に導入した場合も多く、今回の調査には積極的な対応が困難との姿勢を示すことが予想された。そこで、調査に際しては事例調査先組織名はすべて匿名として扱うこととした。

事例調査先組織に対して匿名調査である旨を示す際には、以下の事項を明示している。

- 報告書掲載時には、機関名、社名は表記せず、「研究機関」「民間金融機関」等の表現とする。また、ネットワークやシステムに関する情報から組織を特定することが可能な箇所については、特定不能となるように記述を調整するものとする。
- 報告書の掲載内容については事前にヒアリング先に確認いただき、不都合な点の指摘を受けた場合は修正を行う。

４.１.２ 調査で用いる手法

広範な情報収集を行うための調査手法として、もっとも望ましいのはアンケート調査である。ただし、前述の通りセキュア OS の導入事例についてはセキュリティの観点から消極的な回答が多いと予想される中でアンケートを実施した場合、回収率が低下し、回収できた場合でも調査票で無回答となる項目が増え、実質的に有効な結果が得られないことが予想された。

そこで、今回の調査においては、協力側組織に対し、セキュリティに関係する項目について情報提供したくない場合は回答不要の旨を示した上で、提供可能な範囲で有用な情報を聞き取ることが可能なヒアリング調査を中心に実施することとした。さらに、組織によっては第三者の調査者が介入することで情報の漏洩への懸念が生じる恐れがあることから、セキュア OS のベンダを経由した書面によるヒアリング調査を併用している。

4.1.3 ヒアリング項目の詳細

ヒアリング調査において利用したヒアリング項目は、以下の通りである。

（1）システムの概要

① システムの名称・利用目的

オンライン手続、外部システムとの連携、文書管理などを想定する。

② プラットフォームの種類

使用 OS について、可能であればバージョンまで聞くとともに、利用しているミドルウェアなどもこの項目で伺う。

③ システム上で用いるアプリケーションの種類

汎用製品であれば製品名を問う。自社専用である場合はその旨を確認した。

④ システムが接続されるネットワークの種類

インターネット、社内 LAN、専用網等の種類を問う。システムによってはネットワークの種類から組織名やシステム内容が特定される恐れがあるため、可能な限り抽象化して取りまとめている。

（2）システムが現在の構成案に決定するまでの検討経緯

① 対象とするシステムにおけるセキュリティの考え方

セキュア OS を導入するに際しての組織におけるセキュリティの方針について尋ねた。

② OS 等の選定に際して、特に重視した要件はどのようなものか

OS の選定経緯を把握するための質問として、複数の候補の中から、選定に際してどのような条件を重視したかを尋ねている。具体的には、特定のアプリケーションの動作保証、外部リスクへの強靱性、可用性、コスト等が想定されている。

③ 比較対象としたプラットフォームの種類と、採用に至らなかった理由

OS 選定時に比較した別のセキュア OS があった場合はその名称と、なぜ選定しなかったかの理由について調査している、

④ システム運用におけるセキュリティに関する要件、SLA（Service Level Agreement）等には

どのようなものを含むか

システムの調達に際してセキュリティ要件や SLA を明記した場合は、その有無と定性的な内容について尋ねている。

⑤ 準拠した規程、ガイドライン等

前項とは別に、情報システムのセキュリティ要件として、特定の規程やガイドラインへの準拠を明示したかどうかについて尋ねている。具体例としては、ISO/IEC15408、業界団体によるもの、自社のセキュリティポリシー等のシステムに関わる規定事項、当該システム専用ルール等が想定される。

（3）アクセス制御の具体的な実施方針

① OS の「管理者アカウント」の種類と権限を、目的に応じてどのように分割しているか

OS の管理者特権における最少特権の導入状況を尋ねる項目である。具体的には以下の 2 点について質問している。

ア）目的：権限被奪取時の影響抑制、内部犯行防止 等

イ）分割：アプリケーション管理者、アカウント管理者、保全担当者、監査者 等

② アクセス制御に関する設定を行う際に利用しているツールの有無、名称等

ポリシー設定の際に利用しているツールがあれば、その種類と効果などについて尋ねた。このとき、OS に付属しているツールであっても、利用している場合はツールの一種として整理している。

③ アプリケーションにおけるアクセス制御と OS によるアクセス制御との役割分担の状況

セキュア OS とアプリケーションの連携方法について尋ねている。連携の例示として、いずれかに限定して運用しているのか、目的別に分担か、二重構造かを挙げたが、後述のとりまとめにあるように、具体的な連携の例はほとんどみられなかった。

④ 運用における職員と構築ベンダとの役割分担

システムの運用に際して、職員と構築ベンダとの役割分担について尋ねる項目である。

（4）システム運用上の特徴と課題

① 運用において認識される課題や不便・不都合な事項のうち、セキュア OS の特徴（強制アクセス制御、最少特権 等）に起因するものはあるか

セキュア OS であることに起因する不都合の有無について尋ねている項目であるが、実際にはより広範に、OS に関わる不便や不都合について質問している。

② 運用時の作業負荷は通常の OS と比べるとどうか

セキュア OS を使うことで、通常の OS と比較して作業負荷が増大しているかどうかを尋ねている。併せて、実際に負荷が増大していると回答された場合は、その原因としてどのようなものが考えられるかを、ポリシー設定のメンテナンス、利用者管理、リソース管理等などの例示の上で尋ねている。

③ OS やアプリケーションのログファイルの利用方針（詳細度、参照方法 等）

当該システムにおけるログファイルの利用状況について尋ねている。

（5）その他

以上の調査項目とは別に、参考情報として質問した内容を示す。

① セキュア OS 導入時のポイント

セキュア OS を用いたシステムを導入した経験をもとに、セキュア OS の導入を成功に至らしめるために重要と考えられる項目をポイントとして尋ねた。

② セキュア OS 導入時のメリット

これまでの経験から、セキュア OS にしたことで実感されるメリットとしてどのようなものがあるかを尋ねた。

③ 電子政府での利用に際して

本調査の趣旨を鑑み、電子政府でセキュア OS を導入することについて、自らの経験と照らしてその有効性についてのコメントを得ている。

④ 今後の予定、その他

調査対象組織において予定している、調査対象システムに関わるシステム更新等の予定について、可能な範囲で情報を得ている

４.２ 導入事例の調査結果

前項に示したヒアリング項目について、調査対象組織から得た回答を整理する。

４.２.１ ヒアリング調査結果の要旨

今回のヒアリング調査においては、以下に示す８組織から回答を得ることができた。以下にその要旨をとりまとめた結果を順に示す。なお、事例の表示順序は調査実施の時系列による。

表 4-1　事例調査結果の一覧

	調査先組織の分類	OS の種類	調査方法
事例１	金融系民間企業	PitBull Foundation Suite	インタビュー
事例２	独立行政法人研究機関	PitBull .Compack, PitBull LX	インタビュー
事例３	国立大学法人	PitBull LX	インタビュー
事例４	独立行政法人研究機関	Trusted Solaris	インタビュー
事例５	民間企業	Virtual Vault	インタビュー
事例６	団体	（無回答）	書面
事例７	団体	TOMOYO Linux	インタビュー
事例８	民間企業	PitBull Foundation Suite	書面

表 4-2　事例1

		事例１（金融系民間企業）
適用モデル（昨年度報告書の３種類）		モデル①
1. システムの概要	①システムの名称・利用目的	基幹系と監視システム、メンテナンスシステム（バックアップ等）との間のゲートウェイ（構築中）
	②プラットフォームの種類	PitBull（Foundation Suite）
	③アプリケーションの種類	ゲートウェイとしての利用に限定
	④ネットワークの種類	内部ネットワーク：基幹系（15～20程度のサブシステムから構成される24時間稼動のシステム）、外部ネットワーク：監視とメンテナンスのための閉じたアウトソーシング環境
2. 構成案の検討経緯	①セキュリティの考え方	アウトソーシングで内外ネットワークにまたがるゲートウェイが避けられないため、オペレーションIDの実効範囲の限定とログの取得強化などを通じセキュリティ向上を図る
	②OS選定時に特に重視した要件	外部リスクに対する強靭性（ただしコストが高くつくことが欠点、この用途ではパフォーマンスは不要）
	③比較したプラットフォームの種類と採用に至らなかった理由	Trusted Solaris、PowerBroker OSよりむしろ、セキュリティ情報が入るベンダを選定
	④セキュリティに関する要件、SLA等	特になし
	⑤準拠した規程、ガイドライン等	BIS（Bank for International Settlements）は意識
3. アクセス制御の方針	①管理者特権の最少化の状況	以下の要領で社内人材教育と専門領域を分離： ・システム運用者とセキュリティオフィサーとを分離し牽制を確保 ・システム運用を専門ベンダへアウトソーシングのためオペレーション権限を限定。なお、監査はセキュリティオフィサーが実施
	②利用しているツール	非常に高い費用が必要なことと、使い込まれたものがないことにより、しばらくはOSのみで運用の予定
	③アプリケーションとOSによるアクセス制御の役割分担の状況	技術ベンダに委任。ただし、データベース部分の制御を区分する
	④構築における職員とベンダの役割分担	基本要件を職員が提示、実装を導入ベンダで実施
	⑤運用における職員とベンダの役割分担	以下の役割区分を考えている： ・システムオフィサー、セキュリティオフィサー（社員） ・オペレータ（設定・保守作業をアウトソーシング）
4. 運用上の特徴と課題	①運用上の課題や不都合で、セキュアOSの特徴に起因するもの	（運用開始前につきなし） 監査ログの分析ツール等、周辺ツールの充実が欠かせない

		事例１（金融系民間企業）
	②運用時の作業負荷は通常のOSと比べるとどうか	（運用開始前につきなし）
	③OSやアプリケーションのログファイルの利用方針	ログの種類は、細かく取る予定 特に外部からの操作情報を詳細に記録
5. その他	①セキュアOS導入時のポイント	
	②セキュアOS導入時のメリット	
	③電子政府での利用に際して	セキュアOSを普及させるには人材が不足している 管理する人材の確保及び内包化が一番の課題
	④今後の予定、その他	2006年の3～4月頃にはリリースの予定

表 4-3 事例2

		事例２（独立行政法人研究機関）
適用モデル（昨年度報告書の３種類）		モデル①
1. システムの概要	①システムの名称・利用目的	WWW、Mail、Proxy、CGI、FTP （2001年7月から1年以内に導入、以後変更なし）
	②プラットフォームの種類	Solaris7,8＋PitBull .Compack Solaris7＋PitBull LX（一部WWWサーバ）
	③アプリケーションの種類	Apache、CPMS、Squid、Proftpd
	④ネットワークの種類	外部ネットワーク：インターネット 内部ネットワーク：組織内LAN
2. 構成案の検討経緯	①セキュリティの考え方	00年の省庁Web改竄を契機に、セキュリティ対策なしのサーバ公開は認めないとの指導があり、対策レベルを高めた
	②OS選定時に特に重視した要件	導入当時、PitBull以外に商用トラステッドOSの選択肢がなかった
	③比較したプラットフォームの種類と採用に至らなかった理由	（同上）
	④セキュリティに関する要件、SLA等	サーバが乗っ取られないこと、万一乗っ取られても拡大しないこと。導入当時SLA等は未普及
	⑤準拠した規程、ガイドライン等	導入当時、存在せず
3. アクセス制御の方針	①管理者特権の最少化の状況	サーバ管理者、アプリ管理者の2階層に分割。 監査用のアカウントは作成していない。 個人情報を扱っておらず、内部犯罪を考慮したポリシーにはしていない（Dual lockなし）。
	②利用しているツール	構築ベンダが作成した運用支援ツールを使用
	③アプリケーションとOSによるアクセス制御の役割分担の状況	文書管理等と異なり、サーバ上のユーザ数は限定されるため、2重構造のままでよい
	④構築における職員とベンダの役割分担	構築時のポリシーは、ベンダに設計支援してもらいながら自作。トラステッドOSはここが最も重要であるので、かなり時間を割いて対応
	⑤運用における職員とベンダの役割分担	職員：通常の運用管理。営業時間内の監視 構築ベンダ：不具合、異常時のトラブルシュート（アプリを含む包括的サポート契約だが24hでない）
4. 運用上の特徴と課題	①運用上の課題や不都合で、セキュアOSの特徴に起因するもの	コマンドラインベースのため、導入時に職員にその教育（ベンダによる研修コース）を要した PitBullで製品の組合せによる不具合が発生するが、海外製品のためレスポンスが悪い面もある
	②運用時の作業負荷は通常のOSと比べるとどうか	アプリのバージョンアップ対応負荷は通常の1.2倍程度。運用項目が多いので、当然負荷は高い
	③OSやアプリケーションのログファイルの利用方針	アプリはログ解析ツールにより収集 不正アクセス監視については、IDSにより対応

		事例２（独立行政法人研究機関）
5. その他	①セキュアOS導入時のポイント	最初の設計（要件定義）が重要。ここが不適切だとアプリが連携しない。後での権限見直しは難しい データの流れより、「アクセス権限の流れ」が重要 一旦動き出してしまえば、それほど問題はない
	②セキュアOS導入時のメリット	運用要員減によるコスト削減（監視等） セキュリティホール対応をタイムリーに行わなくてよいことによる時間的余裕
	③電子政府での利用に際して	機微な情報の取り扱いに際して、セキュアOSの使用は社会的信用を得るためにも必須
	④今後の予定、その他	来年度リプレース予定。ネイティブなセキュアOSにすることも検討。

表 4-4 事例3

		事例３（国立大学法人）
適用モデル（昨年度報告書の３種類）		モデル①
1. システムの概要	①システムの名称・利用目的	対象システムは以下の2種類（2002年導入）: －遠隔講義支援システム －鍵管理システム（PKIではなく、物理的な施錠）
	②プラットフォームの種類	Turbo Linux Server 6.5＋PitBull LX （ただし現状ではTurbo Linuxはサポート対象外）
	③アプリケーションの種類	Apache、Tomcat、PostgreSQL、Squid、SSH （いずれも標準的なもの。Turbo Linuxに付属）
	④ネットワークの種類	外部ネットワーク：インターネット 内部ネットワーク：学内、サテライトオフィス、認証用
2. 構成案の検討経緯	①セキュリティの考え方	外からの侵入対策とWebサーバのセキュリティホールへの対応を主眼に置く。個人情報漏洩と踏み台にされることの防止を目的
	②OS選定時に特に重視した要件	セキュリティよりは、システム構築ベンダにおける利便性を重視。本用途で高い可用性は求められない
	③比較したプラットフォームの種類と採用に至らなかった理由	FreeBSDなども候補になっていたが、今回はシステム構築ベンダがLinuxに慣れていた
	④セキュリティに関する要件、SLA等	2002年の段階では何もなかった
	⑤準拠した規程、ガイドライン等	特に考慮していない
3. アクセス制御の方針	①管理者特権の最少化の状況	管理者アカウントとしては以下の3種類を設定： －大学側の運用者 －システム構築ベンダ －PitBullベンダ
	②利用しているツール	特にツールはなく、テキストエディタ程度。 通常は設定変更の必要なし。動作状態の確認程度
	③アプリケーションとOSによるアクセス制御の役割分担の状況	本システムはゲートウェイ的な要素が強いため、連携の必要なし
	④構築における職員とベンダの役割分担	サービスとインフラの切り分けがきれいにできるように設計してもらった。セキュリティに関するポリシーはPitBullのベンダが担当
	⑤運用における職員とベンダの役割分担	運用の主体は大学、業者の担当は、パッチの更新、システムの更新の変更程度。夜間の契約などはなし 大学内に技術支援できるスタッフがいないのが課題
4. 運用上の特徴と課題	①運用上の課題や不都合で、セキュアOSの特徴に起因するもの	現状では深刻な不具合はない 過去3年少々の間で、アプリケーションのリプレースなどの大がかりなバージョンアップは実施していない

		事例３（国立大学法人）
	②運用時の作業負荷は通常のOSと比べるとどうか	設定変更の際の特権へのログイン、ファイルの転送の制限などで作業負荷が増えるのは確か
	③OSやアプリケーションのログファイルの利用方針	現時点では詳細なログはとっていない 主としてネットワーク側の管理センターが全体を監視
5. その他	①セキュアOS導入時のポイント	アプリ、IPアドレス、ネットワークの切り分けがポイント アプリ毎に以下のガイドラインがあるとよい: ・安全のためにはどのポートをどう使いどう組合せるか ・ロックダウン（サービスや利用方法の限定化）の説明
	②セキュアOS導入時のメリット	純粋なOSのメンテナンスとしては、コスト軽減の効果があった
	③電子政府での利用に際して	
	④今後の予定、その他	微妙な手直しのみ 認証データベースの見直しの際に併せて検討

表 4-5　事例4

		事例４（独立行政法人研究機関）
適用モデル（昨年度報告書の３種類）		モデル②（アプリを一部改造）
1. システムの概要	①システムの名称・利用目的	外部から内部ネットワークのリソースを利用するためのゲートウェイ（2004年～2005年導入）
	②プラットフォームの種類	Trusted Solaris 8
	③アプリケーションの種類	OpenSSH（ポートフォワーディング）、Apache（リバースプロキシ）（いずれもオープンソースから構築）
	④ネットワークの種類	外部ネットワーク：インターネット 内部ネットワーク：組織内ネットワーク（VPN用のため）
2. 構成案の検討経緯	①セキュリティの考え方	telnetサービスをOpenSSHで暗号化することを目的 SecurID認証用アプリがトラステッドOSでサポートされないため、ゲートウェイと別に認証用サーバを用意
	②OS選定時に特に重視した要件	オープンソース対応とトータルなサポートが得られることがポイント。要件はあくまでSSHを使えること
	③比較したプラットフォームの種類と採用に至らなかった理由	比較候補としてはPitBullも考えたが、今回の目的においては価格が高かった
	④セキュリティに関する要件、SLA等	最初は実験的に導入したこともあり、サービスレベルとして厳しい要求はしていない
	⑤準拠した規程、ガイドライン等	組織のポリシー（外部との分断を定めている）
3. アクセス制御の方針	①管理者特権の最少化の状況	トラステッドOSの目的は、侵入され踏み台になることの防止であり、管理者権限の分割は目的ではない 通常運用でOS自体を管理する場合とアプリの設定を行う場合とで、作業別に管理者権限を使い分け
	②利用しているツール	OSが提供するツールのみで運用
	③アプリケーションとOSによるアクセス制御の役割分担の状況	アクセス制御はOSの機能を用いて実施 OpenSSH、Apacheに対して独自のラベルを作り設定
	④構築における職員とベンダの役割分担	導入に際してはかなりのディスカッションを実施 仕様確定時にOS、アプリの設定をレビュー ベンダからラベルの概念などを教わった
	⑤運用における職員とベンダの役割分担	ベンダが担当したのは導入時のみ。運用はすべて職員で行っている。作業の手順書はSunで作成
4. 運用上の特徴と課題	①運用上の課題や不都合で、セキュアOSの特徴に起因するもの	セキュアOSを管理する端末もセキュアOSという制限（トラステッドパス）を設けた影響が大きい オープンソース導入時に、認証処理を行うソースコードにパッチを当て、ラベルの付け替えを実施

		事例４（独立行政法人研究機関）
	②運用時の作業負荷は通常のOSと比べるとどうか	OpenSSHとApacheがOS標準でなく、管理にOS提供のツールが使えず、コマンドラインでの操作が必要
	③OSやアプリケーションのログファイルの利用方針	Trusted Solarisとアプリケーションのログを取得している程度
5. その他	①セキュアOS導入時のポイント	ラベルに関する解説資料があるとよい セキュアOSの導入に関して、このような用途にはこうすべきというガイドや、当り前となるべき使い方のパッケージのようなものがあれば導入側は楽になる
	②セキュアOS導入時のメリット	セキュアOSを用いたゲートウェイであれば、管理者は心理的に安心できる。アプリケーションのパッチが公開されたからといって慌てて適用する必要がない
	③電子政府での利用に際して	ゲートウェイはOSがしっかりしていないと信頼性を確保できない。セキュアOSが当り前に使われるべき
	③ 今後の予定、その他	Trusted Solaris 10で認証を含むゲートウェイの運用すべてをトラステッドOS上で行うことを検討

表 4-6　事例5

		事例５（民間企業）
適用モデル（昨年度報告書の３種類）		モデル②
1. システムの概要	①システムの名称・利用目的	アクセスサーバ（ゲートウェイにおけるカスタマーコントロールのためのフロントエンドサーバ） （2000年10月導入）
	②プラットフォームの種類	OS: HP Virtual Vault 4.5（以下、VVOS） ミドルウェア: MirrorDisk for VVOS＋プラットフォーム
	③アプリケーションの種類	専用アプリケーション（自社開発）
	④ネットワークの種類	外部ネットワーク:公衆網 内部ネットワーク:専用線網
2. 構成案の検討経緯	①セキュリティの考え方	ユーザにWebインタフェースでカスタムコントロール機能を提供する際、そこがセキュリティホールとなることを防ぐため、VVOSを用いてサーバの内部、外部を分離し、攻撃の影響を外部側に止める
	②OS選定時に特に重視した要件	外部リスクへの強靭性 ネットバンク等での導入実績を評価
	③比較したプラットフォームの種類と採用に至らなかった理由	①の要件を満たす製品は他に該当例なし
	④セキュリティに関する要件、SLA等	妨害を受けた場合でもサービスが確保されることを最優先
	⑤準拠した規程、ガイドライン等	TCSEC レベルB準拠であること
3. アクセス制御の方針	①管理者特権の最少化の状況	システム管理者、Webインタフェース管理者、アプリ起動用、自社保全用、委託会社保全用の5つの特権アカウントを設け、それぞれに必要最小限のアクセス権、実行権を付与
	②利用しているツール	Virtual Vault付属ツールを使用
	③アプリケーションとOSによるアクセス制御の役割分担の状況	OSレベルでユーザがアクセス可能なパーティションとGW本体に接続されるパーティションとを分離するとともに、プロセスによるアクセスを3階層に分けて制御
	④構築における職員とベンダの役割分担	自社で提示した要件をもとにシステムベンダが設計、構築。OSベンダは①教育コース提供、②開発手法の紹介、③アーキテクチャレビュー、の３点で支援
	⑤運用における職員とベンダの役割分担	社内保守運用部門が主体 必要によりベンダがサポート
4. 運用上の特徴と課題	①運用上の課題や不都合で、セキュアOSの特徴に起因するもの	特になし
	②運用時の作業負荷は通常のOSと比べるとどうか	GUIベースの運用ツールを構築時に作り込んであるので、通常のOSを運用する場合と差は認められない

		事例５（民間企業）
	③OSやアプリケーションのログファイルの利用方針	概ね通常通り
5. その他	①セキュアOS導入時のポイント	どんな手段を用いてもリスクをゼロにすることはできないが、論理としてここまでガードしておけばまず大丈夫だろうと考えられるシステム構成をとれること ミドルウェアを用いる場合は、その機能設計が整然としていないと動作しなかったり脆弱性を生む恐れがある
	②セキュアOS導入時のメリット	論理的な明確なバウンダリーが作れることで、安心感が得られる 設計書を否応なく厳格に書かざるを得ない
	③電子政府での利用に際して	形だけセキュアOSの機能を導入しても意味がない セキュリティに詳しいプロフェッショナルに依頼する必要がある 電子政府システムで何をやりたいかによって、最適解は異なる
	③ 今後の予定、その他	

表 4-7　事例6

		事例６（団体）
適用モデル（昨年度報告書の３種類）		不明
1. システムの概要	①システムの名称・利用目的	認証局（電子証明書の発行）
	②プラットフォームの種類	（無回答：ただしサーバは複数ある）
	③アプリケーションの種類	製品と社内開発アプリケーションの両方を運用
	④ネットワークの種類	外部ネットワーク：オンライン申請受付サーバ（インターネット） 内部ネットワーク：オフライン申請受付サーバ（社内LAN）、メンテナンスとシステム内連携用回線（専用回線）
2. 構成案の検討経緯	①セキュリティの考え方	設備の区分けとして「セキュリティゾーン」を設け、アクセス者の種類に応じたルールを策定 管理情報のレベルとして「セキュリティレベル」を設け、アクセス者に応じて必要最低限の情報を利用可能
	②OS選定時に特に重視した要件	・特定のアプリケーションの動作保証 ・可用性
	③比較したプラットフォームの種類と採用に至らなかった理由	（無回答）
	④セキュリティに関する要件、SLA等	実験運用の位置づけで想定復旧時間等は設けず ただしポリシー文書では復旧への努力を行う旨を示す
	⑤準拠した規程、ガイドライン等	内部規程（RFC2527、RFC3647、ECOM認証局運用ガイドラインV1.0、WebTrust for CA（AICPA/CICA）等を参照の上作成）
3. アクセス制御の方針	①管理者特権の最少化の状況	目的：サーバの権限被奪取時の影響抑制、内部不正抑止 分割：システム管理者、サーバ、監査者等
	②利用しているツール	アクセス制御に社内開発のソフトウェアを使用
	③アプリケーションとOSによるアクセス制御の役割分担の状況	アプリケーション実行に関しては基本的に二重構造 システム管理とアプリケーション保守に関してはアプリケーションではなく、OSによるアクセス制御を利用
	④構築における職員とベンダの役割分担	
	⑤運用における職員とベンダの役割分担	基本的に職員が保守 ハードウェアの不良に対してはベンダが対応
4. 運用上の特徴と課題	①運用上の課題や不都合で、セキュアOSの特徴に起因するもの	最少特権。追求しすぎると人員不足に陥るため、運用費用に合わせた特権の調整が必要となった
	②運用時の作業負荷は通常のOSと比べるとどうか	作業工程が複雑になりがちで、運用に必要な情報の文書化や引継ぎの負荷が大きい

		事例６（団体）
	③OSやアプリケーションのログファイルの利用方針	サーバによって異なるが、一部デバッグレベルで記録し、他は通常のレベルで記録
5. その他	①セキュアOS導入時のポイント	
	②セキュアOS導入時のメリット	
	③電子政府での利用に際して	
	③ 今後の予定、その他	

表 4-8 事例7

		事例7（民間企業）
適用モデル（昨年度報告書の３種類）		モデル①
1. システムの概要	①システムの名称・利用目的	・名称：無回答 ・目的：インターネットからの入会申込、資料請求、属性（住所等）変更等を行う
	②プラットフォームの種類	1) ファイアウォールサーバ（下図の網掛け部） OS： Fedora Core 3＋TOMOYO Linux クラスタリング： Heartbeat、ロードバランサ：Pound、メールサーバ： Postfix、DNSサーバ：BIND 2) Web＋データベースサーバ OS： RedHat EnterpriseLinux 4ES Webサーバ： Apache、DBサーバ： MySQL、テープバックアップ： AFbackup
	③アプリケーションの種類	・インターネット入会用アプリケーション（ベンダ作成の業務アプリケーション） ・上記OSSミドルウェア以外の商用ソフトウェアとして、Sophos AntiVirusを導入 ・ファイアウォールサーバについては、その機能を以下を用いて実現： －iptables －リバースプロキシ ・その他、IDSとしてtripwire（ホスト系）とsnort（ネットワーク系）を導入。
	④ネットワークの種類	・外部ネットワーク（インターネット） ・内部基幹ネットワークとは分離（クライアントPC経由のオフラインでのデータ移動） －収集したデータはクライアントPCから1日1回、基幹LANにデータを反映。 ・Active-Standbyの冗長化構成を採用。 ・対象の会員数は百万名を超えるが、入会申し込みサービスであり会員となった人が繰り返しアクセスする必要がないこと、及びオンラインで登録できることをあまり宣伝していないため、サーバの規模は2台のクラスタリング程度で済んでいる。

		事例７（民間企業）
2. 構成案の検討経緯	①セキュリティの考え方	・考え方は次の通り。 構成： －基幹システムとの接続形態（端末PCを経由した二重扉） －アプリケーションゲートウェイ型のF/W －セキュアOS（TOMOYO Linux）の採用 －ホスト型IDS／ネットワーク型IDSの採用 －アンチウィルスソフトの採用 フィルタリングポリシー： －必要な通信のみ、ポートを開放 検知／通知： －アクセス違反は直ちにメールで通知 ミドルウェア実行アカウント： －Apache、MySQLは一般ユーザ権限で動作 プログラミング： －SQLインジェクション対策等、セキュリティに留意したAP設計
	②OS選定時に特に重視した要件	・選定に際して特に重要視した要件： －IAサーバ上で動作すること －OSSであること －セキュアOSであること（F/Wサーバ） －ベンダにおいて検証済みであること ・コストの抑制手段としてオープンソースソフトウェア（OSS）を採用。「OSSであること」は、本件においてコストメリットの面で有利に働いている。 ・TOMOYO Linuxはベンダの自社製品であるため、ベンダにおいて中身を詳細に把握していることを強みと評価した。 ・TOMOYO Linuxのドキュメントの整備状況としては、使うための必要最小限のものは提供されており、不自由は感じなかった。
	③比較したプラットフォームの種類と採用に至らなかった理由	・比較対象としたプラットフォームとしてはFreeBSDを検討。ただし、以下の理由により採用は困難であった。 －当時はマルチCPUへの対応が不十分であった。 －ハードベンダのOS対応に関するサポート（デバイスドライバ類）がLinuxと比較して不足していた。 ・SELinuxについては、導入を一時期検討したこともあったが設定が非常に細かく、（コスト的、技術的に）運用できないと判断した。SELinuxではポリシー違反としてログにラベル情報が出力されるのに対し、TOMOYOは、ファイル名単位で出力されるため、感覚的に扱いやすい。またSELinuxほど細かい制御は本件では必要ないと判断した。

		事例７（民間企業）
	④セキュリティに関する要件、SLA等	・セキュリティに関するSLAに類するものは下記の通り。詳細な項目は立てていない。 －緊急時には直ちに（ASAP）対応 －毎月1回、セキュリティ状況の報告を実施
	⑤準拠した規程、ガイドライン等	・外部の規程、ガイドライン等の参照は特になし。 ・基本設計書におけるポリシー相当事項について、以下の内容で顧客と同意。 ［注：以下「〇ポリシー→実現手段」として表記］ 〇システム提供前にセキュリティ監査を実施 →セキュリティ診断サービスを受診 〇適切なセキュリティパッチの適用と定期的なログ監査を行う →セキュリティ状況を毎日チェックし、毎月1回、セキュリティ状況を報告 〇個人情報の漏洩を防止 →不必要なデータはインターネット公開サーバ上に置かない（必要最低限の情報のみ取得） →暗号化（SSL通信、個人情報を暗号化してDBに格納） 〇システムへのアクセス制御を導入 →サービス利用以外でのインターネットからの接続不可 →インターネット接続システムと機関システムの直接接続不可 〇運用者外注時を考慮し、内部犯行対策も実施 →認証（パスワード認証、指紋認証）、証跡（ログ収集解析、Webカメラ等）、入退室管理
3. アクセス制御の方針	①管理者特権の最少化の状況	・目的：権限奪取時の影響抑止、システム運用者識別 ・分割：OS管理者、業務アプリケーション管理者、システム運用者
	②利用しているツール	・ツールは特になし（手作業で設定）。サーバにX環境を導入したくなかったため、GUIを使おうとは考えていない。 ・セキュリティ強化OS（TOMOYO Linux）にはポリシー学習機能があり、これはツールの一種とみることができる。また、TOMOYO Linuxではポリシーの状態をツリーで示し、全体構成を理解しやすくするツールも提供されている。

		事例７（民間企業）
	③アプリケーションとOSによるアクセス制御の役割分担の状況	・アクセス制御と役割分担に関しては、以下のように目的別で使用。 －セキュリティ強化OSによる、カーネルレベルでの強制アクセス制御（セキュリティホール対策） －iptablesによるアクセス制御（パケットフィルタリング） －リバースプロキシによるWebサーバアクセス制御［パス／ファイル名や拡張子］（コンテンツアクセス制御） －Apacheベーシック認証によるアクセス制御（会員認証）
	④構築における職員とベンダの役割分担	・デザイン等の静的コンテンツの作成をコンテンツ作成会社に委託したのを除き、ベンダにてすべての開発・構築を担当。
	⑤運用における職員とベンダの役割分担	・システムの運用は、クライアントPCを介したデータの移動を含め、すべてベンダにおいて実施している。
4. 運用上の特徴と課題	①運用上の課題や不都合で、セキュアOSの特徴に起因するもの	・使用したセキュアOS（TOMOYO Linux）に起因する課題・不便・不都合等としては、以下が挙げられる。 －24時間365日の運用中における、商用機でのポリシー学習が非常に不便である。 （ドメイン名やSSL証明書の変更による、ミドルウェア設定変更作業など） －セキュリティを強化する目的で、OS標準のユーザ認証に加えて追加認証を行っているが、それが原因でOSユーザ追加の手順が煩雑になっている。 －再起動を伴わないポリシーの削除（TOMOYO Linux最新版では対応）。 ・ポリシー違反がでた場合、当該事項をポリシー違反でないと変更設定しても良いかどうかの判断には技量が不可欠であり、明確な基準はない。 ・TOMOYO Linuxのバージョンアップについては、TOMOYO Linux自体の正式版の公開から日が浅く、これまでのところ最新版に更新しないことによる悪影響の可能性がないめ修正していない。 ・Fedora Core 3のバージョンアップについても、導入するモジュールを絞っており、パッチが公開されても導入したモジュールに関係ない場合が多いため更新の頻度は抑えられている。

		事例７（民間企業）
	②運用時の作業負荷は通常のOSと比べるとどうか	・商用機と全く同じ構成の開発機がない場合、ポリシーのメンテナンス（学習、削除など）が非常に難しい。学習に際しては、想定されるあらゆるケースを試す必要があるので、負荷は大きい。 ・ポリシーのメンテナンスを行うためには、アプリケーションの動作（どのリソースを使い、どのライブラリを呼ぶか）を把握できる技術レベルが要求される。 ・バグフィックス、セキュリティフィックスによるアップデート後のデグレード確認は、セキュアOSの採用如何によらず大変である。 ・ただし、セキュアOSに伴う負荷は多いものの、運用コストは保守に関する委託費用の範囲内には収まっている。
	③OSやアプリケーションのログファイルの利用方針	・syslog-ngを用いて一括収集管理を行っている。 ・通信プロトコルとして（UDPでなく）TCPを使用し、ログの取りこぼしを防止。 ・収集したログを分類（INFO、WARNING、ERROR）し、ERRORに関しては外部メール転送によるシステム運用者への通知を実施。 ・ログファイルに対して、任意文字列による絞り込みやファイル切替機能を有する閲覧アプリケーションを開発。 ・ログファイルは世代管理して、日次でHDD別領域へ、月次でテープ媒体へのバックアップを実施。 ・テープ媒体は二次保管庫（専門業者）への保管を実施。 ・これまでのところ、問題となるようなログの検出例はない。ユーザ登録時の設定不備などの設定ミスによるポリシー違反の検出例などはある。 ・ログの監視は複数人で行っている。

		事例７（民間企業）
5. その他	①セキュアOS導入時のポイント	・セキュアOSの導入による運用コストの増分は、最終的に発注したユーザの負担増となることに留意してOSを選定する必要がある。現在のSELinuxのように設定の細かいセキュアOSではポリシーの作成とその正当性の検証の負担が大きく、コストが高くなってOSSを導入するメリットが薄れてしまう。 ・現在のところ、TOMOYO Linuxを使ってシステムを構築するには、通常のLinuxを使ったSIの経験のほか、カーネルのコンパイルを行うための知識や、アプリケーション、ミドルウェアの動作（設定、ライブラリなど）についての把握などのスキルが求められる。 ・今回の構成のように規模の小さなミドルウェアであればポリシー違反のトレースも可能であるが、規模の大きいOracleなどになると全ての遷移を追うことは厳しいかもしれない。ポリシーが一旦複雑化すると、修正することは非常に困難になる。 ・全てのセキュアOSで守ろうとするとポリシーの策定が大変である。PostgreSQLにおけるSQLインジェクション対策に関するもののみについてポリシーを書くといった対応は考えられる。アプライアンス製品のようにアプリケーションの変化が少ないものであれば、セキュアOSでも問題は少ないのではないか。 ・セキュアOSを入れたことだけで安心するのでは話が違う。ポリシーの質が高いことをどのように確認するかが重要。その点、TOMOYO Linuxはセキュリティとメンテナンス性とのバランスに優れていると考えられる。
	②セキュアOS導入時のメリット	・OSのセキュリティホール対策として導入効果があった。Fedora Core 3の脆弱性が発見されても、ポリシーに記述されている以外の処理は受け付けないため、当該パッチなどの動作確認を十分に終えてから適用すればよい。パッチ適用のタイミングとしては、アプリケーションの改修などのタイミング（システム全体の検査）に合わせて対応している（半年、1年といった単位）。ただし、DoSアタック対策などのパッチは例外として速やかに適用。 ・未公開のセキュリティホールによるzero-day attackに対する対策として有用である。
	③電子政府での利用に際して	（調達コストについて） ・セキュアOS導入時の工数は、通常の2倍程度となった。ただし、これは本事例が構築ベンダにおけるTOMOYO Linuxの最初の利用事例であることが影響している。
	④今後の予定、その他	

表 4-9　事例8

		事例8（民間企業）
適用モデル（昨年度報告書の３種類）		モデル②
1. システムの概要	①システムの名称・利用目的	トラステッド・ゲートウェイ・システム システムメンテナンス系の統括管理と事故発生時のトレーサビリティ拡充を目的とし、機密ラベル情報を利用した接続先制御を実現
	②プラットフォームの種類	Solaris8+PitBull Foundation Suite for Solaris
	③アプリケーションの種類	データベース、Webアプリケーション、他。 （アプリケーション） ・OS付属のサービスアプリケーションを改良 ・システム専用にGUIアプリケーションを開発 （トラステッドOS対応） ・バッチ処理用にアプリケーションを開発 （トラステッドOS対応） ・データベース
	④ネットワークの種類	
2. 構成案の検討経緯	①セキュリティの考え方	（セキュリティ要件） ・システム管理者による証拠隠滅（ログ消去、改竄）を阻止すること ・不正侵入の踏み台にならないこと ・高い信頼性の確保 ・内部不正の抑止
	②OS選定時に特に重視した要件	・トラステッドOSの採用 ・データベースを含む特定のアプリケーションの動作 ・MLS機能 ・コンパートメント機能 ・コマンド実行制限 ・役割制御 ・最少特権
	③比較したプラットフォームの種類と採用に至らなかった理由	
	④セキュリティに関する要件、SLA等	
	⑤準拠した規程、ガイドライン等	システム運用セクションの課題解決型であり、特に準拠した規定は無い。
3. アクセス制御の方針	①管理者特権の最少化の状況	（管理者アカウントの権限分割） ・情報システムセキュリティオフィサー（Information System Security Officer） ・特権ユーザ（Privileged User） ・一般ユーザ（General User）
	②利用しているツール	・独自開発のGUIアプリケーションを利用している。

		事例８（民間企業）
	③アプリケーションとOSによるアクセス制御の役割分担の状況	・専用アプリケーションを開発。
	④構築における職員とベンダの役割分担	・構築ベンダーと共に要求定義から仕様策定まで実施。
	⑤運用における職員とベンダの役割分担	・トラステッド・ゲートウェイ・システムには数百名のアカウントが登録されており、日々の申請手続きにより専用GUIとバッチ処理で対応。 ・役割分担については回答不可。
4. 運用上の特徴と課題	①運用上の課題や不都合で、セキュアOSの特徴に起因するもの	・申請ルールが厳格になり、手続きが面倒になった。 ・障害時など他のサーバの設定情報を確認して手がかりを得ようとしても、簡単にはできなくなった。
	②運用時の作業負荷は通常のOSと比べるとどうか	・トラステッド・ゲートウェイ・システム導入前は、システムに問題が起きると社内調査の後、出入りのベンダーへも調査の手を広げていた。ログファイルが、ある一定期間消去されていたこともあり、システム管理者権限による何らかの作業痕跡を感じるも証拠が残らず、捜査が暗礁に乗り上げることがあったが、本システム導入後は、当該運用項目に関する負荷は極端に下がった。
	③OSやアプリケーションのログファイルの利用方針	・いつ、誰が、どこから、どこにアクセスして、何をしたか、を記録。
5. その他	①セキュアOS導入時のポイント	・アプリケーション開発ベンダーがトラステッドOSの仕様を知らないため、設計・開発、検証、トラブルシュートの各フェーズでスケジュールに遅延が見られた。 ・最初の設計段階が最も重要。
	②セキュアOS導入時のメリット	
	③電子政府での利用に際して	（留意すべき事項） ・初期段階では技術習得に苦労した。 ・利用者の運用負担を軽減させるGUI提供は必須である。その為、開発手法にまで踏み込んだ、或いはGUI開発ツール提供を行い、利用者レベルであってもGUIカスタマイズが容易に行える様な仕掛けがあると良い。
	④今後の予定、その他	

4.2.2 セキュア OS の適用目的と用途に関する各事例の比較

前項で示した 8 事例について、調査結果をもとに、調査項目ごとに各事例から観察されるセキュア OS の特徴について考察する。

なお、表中に示すモデルの構成図で用いる構成要素の示す意味は以下の通りである。

- 表中の「外部ネットワーク」「内部ネットワーク」は、調査対象とするサーバが設置されたネットワークから見て相対的に外側（よりインターネットに近い）、内側（より組織内ネットワークに近い）であることを示す。
- 図内の長方形がサーバに対応し、さらに黒色の太線で囲んだものがセキュア OS を用いて構築されたサーバを表す。
- 図はあくまでもセキュア OS を用いたサーバのネットワーク内での位置づけを比較することを目的に作成したものであり、他のネットワーク構成要素については大幅に簡略化している場合がある。

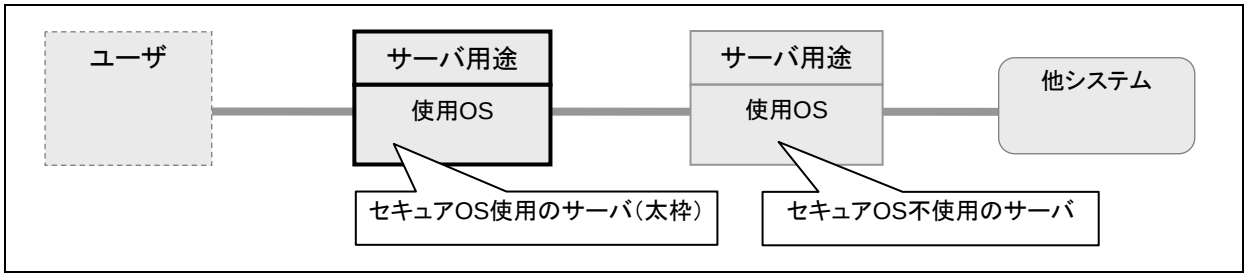


図 4-1　セキュア OS の適用目的と用途の比較に関する凡例

表 4-10　セキュア OS の適用目的と用途の比較（1）

	外部ネットワーク	セキュアOSを導入したシステムが設置されたネットワーク			内部ネットワーク	セキュアOS化の目的としての脅威
事例1	監視システム メンテナンスシステム		ゲートウェイ PitBull FS Solaris		基幹系 システム	・運用者の不正 ・メンテナンス、監視用インタフェースを通じた攻撃
事例2	一般 （不特定多数）	Proxyサーバ SQUID PitBull FS Solaris 7	Web, FTP, CGIサーバ Apache, proftpd PitBull FS, LX Solaris 7, 8	CGI処理用 バックエンドサーバ	CGI処理用 バックエンドサーバ	・サーバの乗っ取り ・乗っ取られたサーバを経由した被害の拡大
事例3	学生・職員 （特定多数）		Webサーバ （遠隔講義支援システム） PitBull LX Turbo Linux		制御先システム （鍵管理）	・外部からの侵入 ・Webサーバのセキュリティホールへの攻撃
事例4	サービス利用者 （特定少数）		ゲートウェイ リバースプロキシ OpenSSH, Apache Trusted Solaris	認証サーバ	操作用環境 Trusted Solaris 内部サーバ Webサーバ	・外部からの侵入 ・サーバが踏み台となること

表 4-11　セキュア OS の適用目的と用途の比較（2）

	外部ネットワーク	セキュアOSを導入したシステムが設置されたネットワーク	内部ネットワーク	セキュアOS化の目的としての脅威
事例5	サービス利用者 （特定多数）	Webサーバ 専用アプリ Virtual Vault ゲートウェイ	基幹システム	・Webサーバのセキュリティホールへの攻撃 ・万一の場合のサービスへの影響波及
事例6	申請者 （不特定多数）	認証局 オンライン申請 専用アプリ OS不明		・サーバの権限被奪取時の影響波及 ・内部不正
事例7	入会希望者 （不特定多数）	ファイアウォール ロードバランサ TOMOYO Linux Fedora Core 3 Webサーバ DBサーバ Apache, MySQL RedHat EL 4ES	オフラインでの授受 基幹システム	・権限被奪取時の影響波及 ・パッチ適用のタイムラグへの攻撃 ・zero-day attack
事例8	システム管理者 メンテ担当者 （特定少数）	システムメンテ系 ゲートウェイ 専用アプリ PitBull FS Solaris 8	内部システム	・システム管理者による内部不正 ・不正侵入により踏み台になること

4.2.3 事例調査におけるポイント

調査結果をもとに、調査項目ごとに各事例から観察されるセキュア OS の特徴について考察する。なお、枠で囲った部分は各項における調査結果のポイントに相当する。

（1）セキュア OS の導入目的

- **導入目的としては、「外部からの攻撃に対する耐性強化」が主流**
- **内部統制を目的とするものも少数ながら有り**

本項については、調査した全ての組織から回答が得られている。

- 今回対象とした事例の多くが、外部からの攻撃等に対する耐性強化を目的としている。うち、最少特権化による内部統制も併せて目的とするものが２例ある（事例１、６）。
- システムメンテナンス系の統括管理と事故発生時のトレーサビリティ拡充といった、組織における内部統制を主眼においているものが１例含まれる（事例８）。

（2）セキュア OS の適用モデルについて

- **モデル①が半数を占め、モデル③の適用事例は無し**

本項については、適用モデルが不明の事例６を除く７例を分析対象としている。

- モデル別の内訳は、モデル①が４件、モデル②が３件である。ただし、モデル②の前提となるアプリケーション上での強制アクセス制御についてはその定義が難しい面もあり、ここではアプリケーションにおいて独自のアクセス制御を行っているものを含む。
- 上述のモデル別の比率がこれまでセキュア OS を導入した組織におけるモデルの構成比を示していると断定はできない。なぜなら、今回の事例調査の対象となった組織はセキュア OS の特徴をよく把握しているが故に調査に同意されたところも多いと推察され、こうした組織では必然的にモデル②を適用する可能性が高くなりがちである。そこで、実際の導入状況においてはモデル①に分類される組織が多いことも予想される。
- モデル③についてはセキュア OS のアクセス制御機能を活用した設計と開発が必要であるため今回の調査対象には含まれていないが、事例５についてはミドルウェアの機能設計の状況をベンダを通じて把握した上でアプリケーションを設計しているなど、部分的にモデル③に基づいた適用がなされているとみることができる。

（3）システムの導入・構築について

- **セキュア OS を用いたシステムでは、「最初の設計が重要」**
- **アプリケーションの連携を対象に「データの流れ」と「アクセス制御の流れ」をみる必要あり**
- **設計書を否応なく厳格に書かざるを得ないことが、結果的にメリットになる**

システムの導入と構築時期におけるセキュア OS 選定の経緯と構築上の留意点について、特徴的な意見として以下のような指摘が得られた。

- セキュア OS のベンダ、インテグレータ以外が構築した事例も 1 例あるが、その構築ベンダが習熟した OS をベース OS とし、打合せの機会を増やすことで対応している（事例 3）。
- セキュア OS で動作しない認証アプリケーションを利用する必要があるため、やむなくシステム構成を変更（別サーバを追加）する必要のあった事例も見られる（事例 4）。
- セキュア OS を用いたシステムでは、「最初の設計が重要」であり、この段階で運用時のあらゆる場面を想定した網羅的な検討が行われていないと、条件によって動かなくなるケースが出る恐れがあり、運用段階に影響が及んでしまう。システムを動くようにするだけであればポリシーを緩くすることで容易に対応は可能であるが、それではセキュア OS にした意味が失われる。ただし、一旦動き出してしまえば、それほど問題はない。
- 複数のアプリケーションが連携するシステムの場合、データの流れと同様に「アクセス権限の流れ」をみる必要がある。
- ミドルウェアを用いる場合は、その機能設計が整然としていないと動作しなかったり脆弱性を生む恐れがある。
- 曖昧な仕様では動かないので、否応なく設計書を厳格に書かざるを得ないことが結果的にメリットとなっている。通常の OS 上での開発のように、納期切迫などの理由で設計書の詳細度が粗くなるようなことがない。
- アクセス制御に関するアプリケーションと OS の連携に関しては、用途がいずれもゲートウェイ的なもので多くのユーザを登録する性質のものではないため、連携は行われていない。ただしサービス利用時の認証に関しては、認証サーバとアプリケーションとでそれぞれ個別にユーザ管理を行う必要性と煩雑さが指摘されている。
- セキュア OS の導入コストについては、高いと認識されているが影響は限定的。通常のシステムの 1.5 倍となった例では、システムベンダの開発分が 1.3 倍、残りが OS ベンダの分になる。コスト増の要因としては、パーティション間通信の設計・開発工数、ログ収集機能の作り込みなどが挙げられている。
- 調達コストに関してはシステム一式で調達したり、入札とすることで OS そのものの割高感は減殺されるとの指摘がある。

（4）システムの管理・運用について

- **管理負荷は高めだが、運用ツールを構築時に作り込むことで通常同様の負荷にもできる**
- **アプリケーションの脆弱性対策のパッチを緊急適用する必要がないことの効果は大**
- **専門的知識・スキルを有する人材の育成は難しい**

システム稼働開始後の運用状況に関する指摘の例として、以下の項目が挙げられる。

- 通常の OS とは異なる運用が必要となる面があり、ベンダ作成の手順書を用いるなどして対応。管理負荷は通常の OS よりは多少高くなる傾向がみられる。ただし、GUI ベースの運用ツールを構築時に作り込むことにより、通常の OS を運用する場合と運用負荷に差は認められないとする例もある（事例５）。
- アプリケーションの脆弱性に対するパッチについては、緊急に対応する必要がないことで管理者の負荷低減に寄与していることでは、導入済み組織の意見は一致。ただしオープンソースを独自にセキュア OS 対応にしている場合は、パッチ適用後のソースコードを改めてセキュア OS 対応にする必要があり、運用上の大きな負荷である。
- 上記の管理者の負荷低減効果により、少人数で多くのサーバの管理が可能になることで、セキュア OS による運用コスト削減があることが指摘されている（事例２）。
- いずれの組織も、セキュア OS 導入時の運用体制のまま現時点まで継続しており、システム構成の見直しをした場合の影響等は把握できていない。アプリケーションを変更する場合の、権限の委譲などの設定の見直しは難しいとの意見がある。
- セキュア OS の操作に独自の知識、スキルを必要とするため、運用担当者の後継者に関する人材確保・育成の難しさへの懸念の声もある。

（3）課題と要望

- **GUI 操作への期待が大きい**
- **セキュア OS に関する解説資料や導入ガイドラインの提供が望まれている**

セキュア OS の導入に関する課題と要望として、次のような意見が得られた。

- GUI での操作を望む声が大きい。OS がそもそも GUI をもたない場合と、OS の非標準のアプリケーションを使用しているために GUI を利用できない場合とがある。
- ベンダ提供のもの以外にセキュア OS に関する情報がなく、予め定められた手順以外の応用や工夫を考えることが難しいことから、アクセス制御の方法に関する解説資料があるとよいとの指摘がある。
- 上述した「最初の設計時の重要性」に鑑み、アプリケーション毎の導入のガイドラインを期待する意見がある。これは、使われそうなアプリケーション候補をリストアップした上で、それを安全に使うにはどのポートをどう使い、アプリケーションをどう組み合わせればよい

かの指針を示すものとなる。

- さらに前項を発展させ、「当り前となるべき使い方のパッケージ」を用意することで導入が容易になると指摘されている。
- ロックダウン（サービスや利用方法を限定化することでセキュリティを高めるための設定）の具体的な方法の説明についても要望があるが、運用は組織毎にケースバイケースとならざるを得ず、一般論としてまとめることは難しいと思われる。今後、事例が増加した段階で検討すべき課題である。

４.２.４ ヒアリングで得られなかった情報

以上の結果とは対照的に、当初予期していながらヒアリング調査を通じて得られなかった情報について以下にその例を挙げる。

（１）OS 製品の偏り

2006 年 3 月時点において、セキュア OS が話題になる場合にはその例として SELinux が取り上げられることが最も多くなりつつあるが、本調査ではそれとは対照的に SELinux の導入事例についてはいずれも交渉不調に終わった。

実験的性質の強いディストリビューションである Fedora Core を除くと、Linux の主要ディストリビューションがカーネルを SELinux ベースにしたのはここ 1 年程度の動きである。一般に OS の新バージョンを用いたシステムを構築するのはリリース後半年程度は時間を置き、OS の安定性を確認してからというケースが多いことから、SELinux のセキュリティ機能を利用して実用システムを構築しているユーザが実際に少ないことによるところが大きいものと推察される。

（２）内部向けシステム

文書管理システム等、内部向けシステムでの利用事例はこれまでのところ見あたらない。これが事例がないのか、ヒアリングに応じられないかは不明である。

このほか管理者特権の最少化やデュアルロックの取組み事例は、ヒアリング結果の中では少数派となっている。なおヒアリング 8 件中 3 件はシステム管理者による応対であり、こうした担当者を対象に「管理者の内部犯行」対策を把握することは困難であった。

第５章 電子政府への適用可能性

本章では、2005 年 12 月に公表された「政府機関の情報セキュリティ対策のための統一基準」においてセキュア OS が提供する機能に関して言及している項目について、セキュア OS を適用することでどのような対応が可能かを検討するとともに、第４章の調査の結果に基づく課題を踏まえた電子政府における導入計画のイメージについて議論する。

５.１ 統一基準におけるセキュア OS 適用の位置付け

「政府機関の情報セキュリティ対策のための統一基準（2005 年 12 月版(全体版初版)）」[2]（以下、政府機関統一基準」）は IT 戦略本部の下に設置された情報セキュリティ政策会議における議論を踏まえ、内閣官房情報セキュリティセンターにより以下の方針に基づき作成された文書である。

- 、「情報」を守ることを目的に作成（「情報」とは、情報システム内部に記録された情報、情報システム外部の電磁的記録媒体に記録された情報及び情報システムに関係がある書面に記載された情報をいい、書面に記載された情報には、電磁的に記録されている情報を記載した書面（情報システムに入力された情報を記載した書面、情報システムから出力した情報を記載した書面）及び情報システムに関する設計書が含まれる）
- 本統一基準は、行政事務従事者のうち、情報及び情報システムを取り扱う者に適用
- すべての府省庁が情報セキュリティの確保のために採るべき対策、及びその水準を更に高めるための対策の基準を定めたもの
- これまでの「情報セキュリティポリシー策定ガイドライン（平成１２年７月１８日付情報セキュリティ対策推進会議決定)」に代わるもの

この政府機関統一基準に基づき電子政府で利用する情報システムの情報セキュリティに関する要件を策定する際に OS の機能に影響する項目を、本報告書の巻末に抽出して示す。

５.１.１ セキュア OS の機能の適用に関する項目

政府機関統一基準では、その 1.1.2(5)項において、情報資産の重要性や取り巻く脅威の大きさに応じて「基本遵守事項」と「強化遵守事項」の 2 段階の対策レベルを定めている。

このうち、特に重要な情報とこれを取り扱う情報システムにおいて、各府省が必要性を判断して選択すべきとされる「強化遵守事項」において、「強制アクセス制御」と「最少特権」ならびに「デュアルロック」というセキュア OS が提供するアクセス制御機能を設けることが定められている。なお、上述の各機能について、機能の具体的な要求事項については政府機関統一基準ならびにその解説書のいずれにおいても特に示されていない。

5.1.2 情報の分類に関する項目

政府機関統一基準が対象とする情報について、下表の要領で機密性、完全性、可用性の 3 種類の観点から格付けを行い、その重要性に応じた適切な措置を講ずることが定められている。このうち、機密性２情報と３情報（＝要機密情報）、完全性２情報（＝要保全情報）及び可用性２情報（＝要安定情報）をあわせて「要保護情報」と呼び、政府機関統一基準においてアクセス制御を行うことが定められている。

表 5-1　機密性・完全性・可用性による情報の格付け

	格付け	分類基準	取扱制限
機密性	機密性３情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報	例）複製禁止 再配付禁止 暗号化必須
	機密性２情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報	
	機密性１情報	機密性２情報又は機密性３情報以外の情報	
完全性	完全性２情報	行政事務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	例） ○年○月○日まで保存
	完全性１情報	完全性２情報以外の情報（書面を除く。）	
可用性	可用性２情報	行政事務で取り扱う情報（書面を除く。）のうち、滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	例） 1 時間以内復旧
	可用性１情報	可用性２情報以外の情報（書面を除く。）	

（出典：文献[2] 解説書別添資料 A.1.2 による）

５.２ 省庁における適用可能性と課題

第４章での事例調査結果と前節において示した政府機関統一基準の内容とを踏まえ、電子政府で利用する情報システムを対象に、統一基準のもとでセキュア OS を適用することによる効果と課題について検討する。

５.２.１ セキュア OS の適用が特に望まれるケース

情報システムにおけるセキュリティのみを考慮するのであれば、電子政府用であるか、サーバ用であるか、外部に公開しているかの如何に関わらず、通常の OS よりセキュア OS を導入する（もしくは、セキュア OS としても利用できる OS のセキュリティ機能を有効にする）ことが望ましいことは言うまでもない。ただし、２.１節で述べたように、セキュア OS を導入することで、用途や使用環境によってはアプリケーションの動作や構築・運用における制約など、セキュリティ以外の面でのネガティブな方向での影響が大きくなることがある。そのため、現状ではすべての場合にセキュア OS を導入することは必ずしも適切ではない。セキュア OS を適用すべきかどうかは、セキュリティをさらに高める必要性や効果と、それに伴う制約や課題とのトレードオフによって判断することになる。

ここでは、こうしたトレードオフを踏まえた上で、セキュア OS の適用による効果が各種の制約による弊害を上回ることで、セキュア OS を適用することが望ましいケースとして、以下の（１）～（４）に示す例が想定される。

（１）「要保護情報」を扱うサーバ

前節で整理した統一基準による情報の格付けにおいて、機密性、完全性、可用性のいずれかの確保に適切な措置を必要とする情報は「要保護情報」であり、要保護情報を取り扱う情報システムについてはアクセス制御や権限管理を行う必要があると判断すべきことが定義されている。

これに従って、電子政府において扱われる情報について検討してみると、例えば「担当者限り」を公開範囲とする文書は機密性が求められるため、言うまでもなく要保護情報である。一方、公開 Web サーバに掲載される情報は、一般向けに公開すべき情報であるため機密性こそ必要とされないものの、悪意の第三者により情報が書き換えられた場合の影響が大きいため完全性が要求されるとともに、情報が利用できないのでは Web としての意味をなさないことから可用性も求められるため、これも要保護情報である。こうして考えていくと、外部向け、内部向けを問わず、要保護情報を全く含まないサーバは考えにくく、電子政府で利用される情報システムにおけるサーバのほとんどでアクセス制御や権限管理を行う必要がある。

政府機関統一基準においてはアクセス制御や権限管理を行う場合、基本遵守事項として任意アクセス制御、強化遵守事項においては強制アクセス制御機能と最少特権機能の利用を求めている

ため、強化遵守事項に従う場合はセキュア OS を適用することになる。このとき、強化遵守事項は「特に重要な情報とこれを取り扱う情報システムにおいて、各府省庁において、その事項の必要性を検討し、必要と認められるときに選択して実施すべき対策事項」とされている。よって、サーバで扱う情報や情報システムとしての重要性の高さがセキュア OS を適用するかどうかの判断基準となることになる。しかしながら、「重要性のある情報をまったく扱わないサーバ」や「重要性の乏しい情報システム」などは考えにくいため、電子政府で用いるサーバの多くがセキュア OS の適用対象になるものと考えられる。

なお、統一基準が要保護情報の要件とする機密性、完全性、可用性の 3 要素のうち、可用性の面からの重要性については、サーバの多重化、ハードウェアの高信頼化などが対策の中心となるのが一般的であるため、セキュア OS を適用することによる効果は他の要件と比べれば小さい。

（2）インターネットに直接接続する必要のあるサーバ、ゲートウェイ

インターネットに直接接続されるサーバは、OS に脆弱性が発見されると同時にそれを悪用した攻撃に直面することになる。特にいわゆる「ゼロデイ攻撃（0-day attack）」と呼ばれる、脆弱性対策のパッチが公開される前に、攻撃のためのワームやウィルス等の悪意のソフトウェアが出現する場合は、直ちに通常の運用を止めない限り、サーバを乗っ取られたり、情報を外部に取り出される恐れがある。したがって、24 時間 365 日運用するようなサーバにおいてはいつでもこうした緊急事態に対応できるような体制を確保しておくことが欠かせず、運用コストの削減の重大な障壁となっている。

一方セキュア OS であれば、アプリケーションに脆弱性があっても攻撃による被害は最小限に止めることが可能である。例えば Web サーバの場合であれば、強制アクセス制御機能を用いてコンテンツを読込み専用にすることで改ざんを防ぐとともに、アプリケーションを乗っ取られても OS に被害が拡大することがない。これにより、上述のような緊急事態の生ずるリスクはきわめて小さくなる。こうしてセキュア OS を適用することで、Web サーバの完全性、可用性を高めることが可能となる。

また、必ずしも重要性が高くないシステムの場合は、セキュア OS を適用する別のメリットが期待できる。すなわち、セキュア OS が上述の「ゼロデイ攻撃」等の脅威に対して強いことを活かし、業務時間外の緊急事態への対応の体制を省いてしまうのである。通常の OS であればサーバの乗っ取りが成功した場合の被害の大きさを考慮すればとても許容できるものではないが、セキュア OS であればアプリケーションの脆弱性を攻撃されたとしても、最悪でもアプリケーションが本来の機能を提供できなくなる程度の被害で済むため、こうしたリスクが許容できる程度の重要度のシステムであれば、セキュア OS の適用を通じて運用コストを大幅に削減できる。

最後に留意すべきは、セキュア OS であればあらゆる脆弱性に対して被害の抑制効果があるわ

けではないことである。セキュア OS そのものに脆弱性が存在した場合は、通常の OS と同様の被害が生ずる恐れがある。セキュリティ評価・認証制度（ISO/IEC 15408、コモンクライテリア（CC））における高度の認証を取得している OS の場合は、こうした脆弱性を生じさせないための対策が講じられていることを第三者による評価結果を通じて検証することが可能であり、こうした仕組みは脆弱性の発生を一定程度抑制するものと期待される。ただし、脆弱性が存在しないことが保証されているわけではない。

（3）通常以上の内部統制を必要とする内部サーバ

現在、電子政府に限らずあらゆる組織において内部統制の確立が求められているところではあるが、情報漏洩や改ざんが行われた際の影響が特に大きいシステムや、国民の関心の高い情報を扱うシステムなどの場合、通常の水準以上の内部統制を実現することが望ましい。こうした場合には、セキュア OS の最少特権機能を用いて管理者特権をもつ者による内部犯行を相互牽制したり、操作ログの管理者による改ざんが困難にすることが有効である。また、管理者特権を扱う職員にとっても、通常の OS では管理者特権の万能性ゆえに自らの潔白を証明することが困難であるのに対し、セキュア OS であれば無用の疑いを受ける可能性が小さくなることから、メリットは大きいと言える。

なお、トラステッド OS が提供するデュアルロック（デュアルコントロール）機能を用いることで、システムに重大な影響を及ぼす操作に関しては複数の管理者による操作を必須とさせることができる。これは、内部犯行の抑制のほか、誤操作によるトラブルの発生の抑制にも効果が期待される。

（4）外部からのメンテナンスを行う必要のあるサーバ

組織内に情報システムに関する専門的知識を要する職員がおらず、ベンダのオペレータが常駐することもないような場合は、組織外部からリモートによる保守・運用を行うことが避けられない。保守・運用の際には管理者特権が必要となるが、リモートから特権を利用できるような設定が存在すると、万一アプリケーションや OS に脆弱性が存在した場合に、攻撃者が管理者特権を活用しやすくなる場合が多い。

このような場合でも、セキュア OS であれば最少特権機能により、外部からメンテナンスする際に利用する管理者アカウントの権限を必要最小限にすることができ、万一の際にアカウントの認証情報が漏洩した際の影響を最小限にすることが可能となる。

5.2.2 電子政府におけるセキュアOSの導入上の課題と対策

一方、セキュア OS を電子政府に導入するにあたって、予め認識しておくべき課題とその対策方針としては、以下が挙げられる。

（1）専門的知識をもった管理担当者の不足の懸念

ヒアリング結果によれば､セキュアOSを用いてセキュアな情報システムを構築するためには、構築当初の設計が重要である旨が複数の回答者から得られている。これは、調達側とベンダの双方において、設計に深く関与する必要があることを意味する。しかしながら、現在の電子政府システムにおいては、すべての情報システムにおいてこうした設計に関与できる担当者を確保するのは難しいことが懸念される。

こうした条件において、設計能力の高いベンダに発注することができれば、課題を一定程度緩和することは可能である。ただし、電子政府における情報システムの調達においては競争入札が原則であり、そうした特定の能力を備えたベンダに限定して発注できるとは限らないことにも留意する必要がある。もっとも、最近のセキュリティへの関心の高まりの中で、セキュア OS への取り組みを強化しているベンダも増えつつあり、第４章で紹介した先行導入事例の各機関がかつて直面した課題と比較すれば、状況は改善されている。これに対して、調達側での設計への関与についてはこれまでの運用体制の延長上では困難と考えられ、今後の電子政府における人材育成・活用に関する支援施策に依存するところが大きい。

（2）導入時、運用時のコストの増大

セキュア OS そのものの費用については、通常の OS でもセキュア OS と同様のセキュリティ機能を備えた製品が増えてきたこともあり、必ずしも通常の OS と比較して高コストになることはない。ただし、導入時に適切なシステムポリシーを設定するためには、通常の OS と比較すると複雑かつ慎重を要する作業が必要となり、構築ベンダ側のスキルも必要となるため、人的コストを中心に割高になることが多い。これに対して運用コストについては、トラブル対応を中心に専門知識を有する人材が必要となるためコスト高になり得る一方、ヒアリング結果からはセキュア OS の導入が単にセキュリティ向上にとどまらず、総合的なコスト削減効果があるとの意見も得られており、必ずしもコスト増大につながるわけではない。しかしながら、初めてセキュアOSを導入する場合などは、セキュア OS ならではのトラブルへの対応に備え、ある程度の運用コストの増大を考慮しておくべきである。その際、セキュリティに配慮することによるコスト抑制効果は具体的な数字には現れにくいため、導入時のコストが割高になることへの理解を得るのは必ずしも容易ではないことに留意する必要がある。

一方、調達コストについては、システムを競争入札などを経て調達する場合は、仮に割高なコ

ストが必要であったとしても入札の過程で吸収されてしまう場合がある。ただしこの場合はベンダが適正な代価を得ることができないことを意味するので、品質確保の面から望ましいことではない。

なお運用コストについては、ヒアリングを通じて構築時に運用ツールを作り込んでおくことで、通常の OS と変わらないコストで運用することは可能との指摘も得られている。

５.３ 今後のセキュア OS の適用の考え方

これまでの検討結果を踏まえ、電子政府で利用する情報システムにおけるセキュア OS の適用可能性と適用の方針・留意点を、適用モデル毎に示す。

５.３.１ セキュア OS の適用シナリオ

３.１節（22 ページ）で示したモデルの３分類をもとに、電子政府におけるセキュア OS の適用可能性について検討する。このとき、第２章で述べたようにアプリケーションの動作の可否が重大な影響を及ぼすことを考慮し、適用モデル①を以下のようにさらに２分して扱うものとする。

- **適用モデル①ａ：**アプリケーションが動作することや、システム構築時のコスト増を回避することを優先し、システムポリシーの設定や最少特権化を最小限にとどめるもの。
- **適用モデル①ｂ：**セキュリティ向上の効果を最大限発揮させることを優先し、十分な時間・コストを投入して最適なシステムポリシーを設定するもの。

これらと他の２種類のモデルとによる合計４種類のシナリオをもとに、セキュア OS の適用可能性について整理すると以下のようになる。

（１）最小限のセキュリティ機能のみを利用（適用モデル①ａ）

電子政府システムでこれまで用いてきた通常の OS をセキュア OS に置き換えること、もしくはセキュア OS 相当のセキュリティ機能を有効にすること以外の変更は最小限として適用するシナリオである。通常の OS に上乗せの形で導入するセキュア OS で、ベースとなる OS で動作するアプリケーションであれば動作が可能なもの（PitBull など）や、通常の OS がセキュア OS にもなるようなもの（HP-UX、Solaris など）であれば、アプリケーションの種類に関わらず適用が可能であるなど、適用上の制約はほとんどない。導入に関する負荷も４つのシナリオの中で最も小さいが、その分セキュア OS の適用効果も最小限となる。適用効果のうち、内部犯行防止のための管理者特権の分割･最少化やログファイルの書込み専用化による改ざん防止などの措置は、アプリケーションの種類にかかわらず可能である場合が多いため、通常の OS と比較しても一定の適用効果は期待することができる。一方、強制アクセス制御機能による被害拡大の抑止などの効果については、こうした適用方法が考慮された一部の OS（PitBull など）を除き、通常の OS と大差ないものとならざるを得ない。

（２）OS のセキュリティ機能のみを強化（適用モデル①ｂ）

市販のパッケージ製品（機能をカスタマイズする場合を含む）や、オープンソースソフトウェアとして配布されているアプリケーションにおいて、アプリケーションレベルで強制アクセス制御機能を備えたものは現状ではほとんどない。したがって電子政府システムにおいてこうしたア

プリケーションを改造することなく利用する場合、本シナリオが最もセキュリティを高めることができる手段となる。本シナリオでは、情報システムの構築の際に、実行を許可されたアプリケーションの振る舞いをもとに（利用しないアプリケーションやサービスプログラムは実行制限を施す必要あり）、システムポリシーの設定を通じてアプリケーションを含むすべてのプログラムのアクセスを必要な範囲に制限する。すなわち、アプリケーションに手を加えない範囲で、最大限のセキュリティ強化を行うことになる。システムポリシーの設定に際して、市販パッケージなどではアプリケーションの内部情報が得られないことも多く、こうした場合はトラブル場面等を含む、想定されるあらゆる条件のもとでアプリケーションを動作させ、その振る舞いをもとにポリシーを決めていく必要があるため、こうした作業負荷が構築時のコスト増に結びつくことになる。

なお、こうしたアクセス制限を行うことにより、（１）のシナリオと比較してどの程度セキュリティ向上の効果が高まるかについてはアプリケーションの特徴に依存する。アプリケーションが表 2-1（21 ページ）に示すような条件を課す場合は、（１）との差は小さくなる。

（３）OS とアプリケーションそれぞれでセキュリティを強化（適用モデル②）

OS とは独立した強制アクセス制御機能を備えたアプリケーションを専用として開発することにより、セキュリティを高めるシナリオである。

３.３.２（３）で示したように、登録する必要のあるユーザ数が多いアプリケーションを構築する場合や、１つのサーバ上でアプリケーションを複数動作させるような場合には本シナリオの適用が適切であると考えられる。このほか、本シナリオではシステムの構築に際して TAPI（３.３.２参照）のようなセキュア OS 特有のインタフェースを利用する必要がないため、こうしたまだ日本のベンダにおいては特殊といえる開発条件を望まないときにも、本シナリオの適用が適している。

（４）OS とアプリケーションの連携によりセキュリティを強化（適用モデル③）

OS の提供する強制アクセス制御機能をアプリケーションから利用することにより、最も強固なセキュリティを実現することが可能なシナリオである。上述の通り、アプリケーションの開発に際しては、セキュア OS の提供する独自のインタフェース（TAPI 等）を利用する必要があり、こうした条件での構築経験を有するベンダは日本では少ないため、現時点では構築上の選択肢が少ない上に割高になるのは避けられない。ただし、セキュア OS の効果を最大限に活用するには本シナリオが最適であり、今後は適用事例が増えていくものと考えられる。

以上の４種類のシナリオについて、セキュリティ向上の効果、システムの構築期間、構築コスト等について比較した結果を次表に示す。

表 5-2　セキュア OS 適用のシナリオの種類に応じた効果の比較

		適用モデル①a	適用モデル①b	適用モデル②	適用モデル③
		最小限のセキュリティ機能のみを利用	OS のセキュリティ機能のみを強化	OS とアプリケーションそれぞれでセキュリティを強化	OS とアプリケーションの連携によりセキュリティを強化
セキュリティ向上の効果	アプリケーションの未知の脆弱性への攻撃	△	○	○	◎
	アプリ管理者による内部犯行	×	○	○	◎
	OS 管理者による内部犯行	○	◎	◎	◎
市販パッケージの使用		可	可	不可 （セキュリティ強化製品であれば可）	不可
オープンソースソフトウェアの使用		可	可	要改造 （セキュリティ強化済みであれば不要）	要改造
専用アプリケーションの開発		可	可	可	可
構築に要する期間		通常 OS 並み	ポリシーの設定と調整に要する期間が長い	アプリ開発に要する期間が長い （強化方法に依存）	アプリ開発に要する期間が長い （強化方法に依存）
構築コスト		通常 OS 並み（OS の費用のみ上乗せ）	割高	割高	最も割高
ベンダの選定に関する留意点		特になし	ポリシー設定を自分で行わない場合は信頼できる OS ベンダの選定が重要	セキュア OS 上でのシステム開発経験のあるベンダの選定が重要	セキュア OS の API を用いたシステム開発経験のあるベンダの選定が重要
対応可能なベンダの数		多い	少ない	少ない	きわめて少ない

記号凡例 ◎：最も効果が大きい
○：十分な効果を有する
△：多少の効果を有する
×：通常の OS とほとんど差がない

５.３.２ 既存アプリケーションを利用する場合の留意点

ここでは適用モデル①ｂを例に、既存アプリケーション（市販パッケージ等を含む）をセキュア OS 上で利用するシステムを構築する際に留意すべき事項を、導入の場面別に示す。電子政府システムの調達に際しては以下の要件を考慮の上、調達仕様を定めることになる。

（１）OS の選択

アプリケーションを動作させるプラットフォームとしてセキュア OS を選択する際には、ターゲットとする市販パッケージが動作することが最大の要件となる。最近のセキュア OS 製品（PitBull、HP-UX、Solaris 等）の場合、通常の OS 用の製品の動作を保証している製品も多いため、こうした保証のあるものを選択するとアプリケーションに関するトラブルを回避することができる。一方、SELinux の場合は現状で動作保証されるのは、targeted ポリシーのもとで、OS に付属するアプリケーションを動作させる場合に限られる。

（２）システムの設計・構築

既存パッケージを利用する場合は、アプリケーション開発が不要であるため本場面に相当する作業に要する負荷は小さい。ただし、アプリケーションが連携して動作するような場合はその情報と制御の流れを整理しておくことが、（３）の作業を容易にするために重要である。

また、Trusted Solaris のように、セキュア OS の種類によっては構築時点ではアクセス制御を行わない状態にシステムポリシーが設定されているものがあり、このような OS においては速やかに（３）の手順を行わない限り、セキュリティ機能に関しては通常の OS と同様の効果しか得られないことになる。

（３）システムポリシーの設定

既存アプリケーションが行う可能性のあるあらゆるアクセスを想定した上で、これを失敗させない範囲でシステムポリシーの設定を通じてアクセス制御の設定を行うことになるが、人手でこうした作業を行うのは手間を要する上に誤りが生ずる恐れがある。セキュア OS 製品のうち、Compartment Guard for Linux（HP）や TOMOYO Linux（NTT DATA）にはポリシー自動生成機能があり、通常の動作環境において想定されるアプリケーションの振る舞いをもとに、システムポリシーを OS が生成する。いずれも完全な自動化を実現するものではないが、作業負荷の軽減には有効な手段である。

５.３.３ 専用アプリケーションを構築する場合の留意点

適用モデル③を例に、組織専用のアプリケーションを新たに開発したり、過去に通常の OS での利用を前提に開発したアプリケーションをセキュアOSの導入に際して改造する場合について、システムを構築する際に留意すべき事項を、前項と同様に導入手順に従って場面別に示す。

（１）OS の選択

適用モデル③の場合は、セキュア OS のアクセス制御機能を活用したアプリケーションの開発経験を有するベンダの選定が重要である。よって OS の選択は、システム構築に携わるベンダの選択によって自動的に決まることも多くなる。複数の OS に対応可能なベンダの場合は、アプリケーションの用途等に応じてベンダと協議のもとで OS を選択することになる。

（２）システムの設計・構築

適用モデル③の場合は、本場面での作業が最もコストを要する作業となる。事例調査において指摘されているように、構築の過程で運用管理のためのツールも同時に作り込んでおくことで、特殊なスキルや知識を必要とすることなく運用を行うことも可能となるため、トラブル対応等まで含んだシステムの利用場面を想定した上で、設計を行うことが望ましい。

（３）システムポリシーの設定

アプリケーションを自ら設計・開発する場合は、設計時点でその振る舞いを把握できているため、システムポリシーをアプリケーションの動作に合わせて適切に設定することは、前項の市販パッケージの例に比べれば容易である。

第６章 おわりに

本調査で実施した調査内容のとりまとめと、今後に向けて求められる取り組みについて示す。

６.１ 調査のまとめ

本調査では、電子政府で利用する情報システムにおいて、セキュア OS に代表されるセキュリティ機能を強化した OS の適用可能性について、導入に先だって考慮しておくべき事項に関する検討を行った。

まず、セキュア OS の導入による影響として、アプリケーションの動作に関するものを整理し、ケーススタディの分析をもとに対処方針について検討するとともに、OS のセキュリティ機能を最大限に活用するためには、アプリケーションを OS と連携させる形態で構築することが有効であることを示した。さらに、先行する導入事例の分析を通じて、セキュア OS 上にシステムを構築する際の留意事項や課題について明らかにした。

こうした結果をもとに、「政府機関の情報セキュリティ対策のための統一基準」で打ち出された対策を OS のセキュリティ機能を用いてどのように実現するかの検討を行い、４種類のシナリオに基づいた電子政府における適用可能性について示している。

６.２ 今後に向けた取組み

本調査の成果をもとに、電子政府におけるセキュア OS の活用をより効果的に実践するため、今後以下のような取組みが行われることが期待される。

６.２.１ 電子政府におけるユースケースの想定

これまで、Web サーバ、認証局、文書管理システムを挙げてきたが、分析の過程で、Web サーバ、文書管理システムについては、多くの形態が想定され、一般論として扱うことが難しいことが明らかになっている。そこで、より具体的な導入条件をユースケースとして想定した上で、それぞれにおけるセキュア OS の適用イメージを検討することが望ましい。そうした複数の適用イメージの中から、実際にはいくつかのグループへの類型化が可能であると推察される。

６.２.２ 構築の際に留意すべきポイントの抽出

ヒアリングの結果、先行導入に携わった担当者からのコメントには、導入に際して留意すべきポイントとして比較的共通の意見が含まれていると考察される。

そこで、こうした知見をセキュリティを確保したシステムを構築するために落とせないポイント

（OS の機能要件、ポリシー設定）として、整理・とりまとめを行うことが考えられる。このとりまとめ結果は、状況によっては「チェックリスト」のようにまとめることも想定される。

こうしたとりまとめにおける懸念材料としては、報告書冒頭で示したように、セキュア OS は OS の製品毎にかなり仕様が異なっており、知見の集約が OS の相違によって妨げられる恐れがあることが指摘される。こうした仕様の相違の吸収について、何らかの工夫を行うことが求められる。

６.２.３ 構築時のガイドライン（指針）となるドキュメントの整備

以上のとりまとめ結果をもとに、電子政府で利用する情報システムにおいてセキュア OS を用いてシステムを構築する場合のガイドライン（指針）となるドキュメントを整備すると、調達者において有用となることが想定される。ベンダ、SIer によっては、こうした構築上のノウハウを差別化の手段として利用しているケースがあるため、こうしたベンダの利害と背反することなく、導入を促進するツールとして調達者、構築事業者から受容されるような形でとりまとめることが望まれる。

本ガイドラインの主たるターゲットは情報システムの調達者となることは言うまでもないが、担当者によって知識に大きな差があることが想定されるため、その差に応じてそれぞれにとって有用と判断されるようなドキュメントとする工夫への取組みが求められる。

参考　政府機関統一基準における関連記述の抜粋

（文中の下線は本報告書において付記したもの）

1.1.2 **本統一基準の使い方**

(5) **対策レベルの設定**

情報セキュリティ対策においては、対象となる情報資産の重要性や取り巻く脅威の大きさによって、必要とされる対策は一様ではない。また、該当する情報システム及び業務の特性に応じて、各対策項目で適切な強度の対策を実施すべきである。したがって、本統一基準においては、各対策項目で対策の強度に段階を設け、採るべき遵守事項を定めている。この段階を「対策レベル」と呼び、以下のように定義する。

(a) **「基本遵守事項」は、保護すべき情報とこれを取り扱う情報システムにおいて、必須として実施すべき対策事項**

(b) **「強化遵守事項」は、特に重要な情報とこれを取り扱う情報システムにおいて、各府省庁において、その事項の必要性の有無を検討し、必要と認められるときに選択して実施すべき対策事項**

以上より、各府省庁は、基本遵守事項以上の対策を実施することとなるが、当該情報システム及び業務の特性を踏まえ、リスクを十分に勘案した上で、対策項目ごとに適切な対策レベルを選択しなければならない。

3.2.3 **情報の保存**

趣旨（必要性）

行政事務においては、その事務の継続性を確保するなどの必要性から情報を保存する場合があるが、情報の保存を続ける限り、当該情報の漏えい、滅失、き損及び改ざん等が発生するおそれも継続する。

これらのことを勘案し、本項では、情報の保存に関する対策基準を定める。

遵守事項

(1) **格付けに応じた情報の保存**

【基本遵守事項】

(a) **情報システムセキュリティ責任者は、電子計算機に保存された要保護情報について、適切なアクセス制御を行うこと。**

解説：電子計算機に記録された情報に関して、機密性、完全性及び可用性の格付けに応じ、電子計算機の機能を活用して、必要のない者に情報へアクセスさせないためのアクセス制御を可能な範囲で実施することを求める事項である。

電子計算機におけるアクセス制御は、電子計算機、オペレーティングシステム、アプリケーション及びファイル等を単位として行うことができ、これらを選択し組み合わせて、適切なアクセス制御を実現する。

4.1.2 **アクセス制御機能**

趣旨（必要性）

主体認証によって、許可された主体だけが情報システムを利用できることになるが、情報システムを複数の主体が利用し、そこに重要度の異なる複数種類の情報がある場合には、どの主体がどの情報にアクセスすることが可能なのかを情報ごとにアクセス制御する必要がある。

これらのことを勘案し、本項では、アクセス制御に関する対策基準を定める。

遵守事項

(1) **アクセス制御機能の導入**

【基本遵守事項】

(a) **情報システムセキュリティ責任者は、すべての情報システムについて、アクセス制御を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、アクセス制御を行う必要があると判断すること。**

解説：アクセス制御を行う前提として、情報システムセキュリティ責任者は、各情報システムについて、アクセス制御を行う必要性の有無を検討しなければならない。要保護情報を取り扱う情報システムにおいては、アクセス制御を行う必要があると判断すること。

なお、アクセス制御方式やセキュリティに配慮した OS に関する用語の解説については、内閣官房情報セキュリティセンターによる「電子政府におけるセキュリティを配慮した OS を活用した情報システム等に関する調査研究」を参照のこと。

http://www.bits.go.jp/inquiry/pdf/secure_os_2004.pdf

(b) **情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、アクセス制御を行う機能を設けること。**

解説：情報システムの利用者やそのグループの属性に応じてオブジェクト（制御対象）へのアクセス権を任意に設定できる方式（任意アクセス制御：DAC）を利用すること。なお、「任意アクセス制御（DAC：Discretionary Access Control）」とは、主体が客体に設定したアクセス制御について、その設定がそれ以後継承されるかが任意である方式であり、この方式では、その客体にアクセス許可されている主体が別の客体を作成し複製等する際に、元のアクセス制御を新しい客体のアクセス制御として継承するかは当該主体の任意であり、変更が可能である。

【強化遵守事項】

(c) **情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、利用者及び所属するグループの属性以外に基づくアクセス制御の機能を追加すること。**

解説：情報システムの利用者や所属するグループの属性に応じてオブジェクト（制御対象）へのアクセス権を任意に設定できる方式のほか、情報システムの利用者やそのグループの属性以外に基づくアクセス制御を追加すること。

情報システムのグループの属性以外に基づくアクセス制御としては、例えば以下の方式が挙げられる。

・アクセス・コントロール・リスト（ＡＣＬ）制御

情報システムの利用者やそのグループの属性以外に基づくアクセス制御としては、例えば以下の方式が挙げられる。

・利用時間による制御

・利用時間帯による制御

・同時利用者数による制限

・同一ＩＤによる複数アクセスの禁止

・IP アドレスによる端末制限

(d) **情報システムセキュリティ責任者は、アクセス制御を行う必要があると認めた情報システムにおいて、強制アクセス制御機能を設けること。**

解説：強制アクセス制御機能(MAC)の組み込みを導入すること。

強制アクセス制御機能を備えたものとして、トラステッドＯＳやセキュアＯＳ等で実装したものもある。

(2) **行政事務従事者による適正なアクセス制御**

【基本遵守事項】

(a) **行政事務従事者は、情報システムに装備された機能を用いて、当該情報システムに保存される情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定をすること。**

解説：情報システムに行政事務従事者自らがアクセス制御設定を行う機能が装備されている場合には、行政事務従事者は、当該情報の格付けと取扱制限の指示内容に従って、必要なアクセス制御の設定を行うことを求める事項である。例えば、要機密情報であれば、不適当な者から参照されないよう、読取制限の属性を付与し、完全性２情報であれば、不適当な者から変更されないよう、上書き禁止の属性を付与することがこれに当たる。

ただし、複製禁止の取扱制限がされていたとしても、情報システムに複製禁止とする機能がなければ、そのアクセス制御の設定をすることはできない。その場合には、情報システムが備えていない機能については、行政事務従事者が取扱上注意することで、その指示を遵守することになる。

4.1.3 権限管理機能

趣旨（必要性）

主体認証情報の機密性と完全性、及びアクセス制御情報の完全性を守ることは重要である。これらの機密性や完全性が損なわれると、主体認証やアクセス制御の機能に問題がなくとも、正当ではない主体からの情報へのア

クセスを許してしまうことになる。

これらのことを勘案し、本項では、権限管理に関する対策基準を定める。

遵守事項

(1) **権限管理機能の導入**

【基本遵守事項】

(a) **情報システムセキュリティ責任者は、すべての情報システムについて、権限管理を行う必要性の有無を検討すること。この場合、要保護情報を取り扱う情報システムについては、権限管理を行う必要があると判断すること。**

解説：権限管理を行う前提として、情報システムセキュリティ責任者は、各情報システムについて、アクセスする主体の権限管理を行う必要性の有無を検討することを求める事項である。要保護情報を取り扱う情報システムにおいては、権限管理を行う必要があると判断すること。

なお、アクセス制御は、主体から客体へのアクセス条件を制限することで客体に対してのアクセス許可を管理することである。それに対して、権限とは、主体に付与される許可のことをいい、権限管理とは、主体に対する許可を管理することである。その主体が情報システムの管理を担う場合には、その主体に対して管理者権限を与える場合もある。

(b) **情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、権限管理を行う機能を設けること。**

解説：権限管理を行う機能を設ける必要性があると認められた場合に、当該機能を情報システムに設けることを求める事項である。

【強化遵守事項】

(c) **情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、最少特権機能を設けること。**

解説：管理者権限を持つ識別コードを付与された者が、管理作業をする時に限定してその識別コードを利用することを可能とする最少特権機能を、情報システムに設けることを求める事項である。

(d) **情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、主体認証情報の再発行を自動で行う機能を設けること。**

解説：情報システムの利用を開始している主体が、主体認証情報の再発行を要求した場合には、当該情報システムにおいて、その主体により重要な情報が既に作成されている可能性があることから、再発行する主体認証情報を他の者が知り得ないように、新規に主体認証情報を発行する場合に比べて、一層安全な機能を設けることを求める事項である。

なお、再発行を自動化して他の者による操作を必要とすることなく主体認証情報を再発行することにより、安全性を強化することができる。

(e) **情報システムセキュリティ責任者は、権限管理を行う必要があると認めた情報システムにおいて、デュアル**

ロック機能を設けること。

解説：不正操作及び誤操作を防止するために、情報システムにデュアルロック機能を設けることを求める事項である。デュアルロック機能とは、行為に対して、少なくとも 2 名の者が操作しなければその行為を完遂できない方式のことである。

（出典：文献[2]による）

基礎資料、引用文献及び参考資料

[1] 内閣官房情報セキュリティセンター, 電子政府におけるセキュリティを配慮したOSを活用した情報システム等に関する調査研究, みずほ情報総研, 2005年.

[2] 内閣官房情報セキュリティセンター, 政府機関の情報セキュリティ対策のための統一基準(2005 年 12 月版(全体版初版)) 解説書, NISD-K303-052C, 2005年.

[3] 情報処理推進機構(IPA), 強制的アクセス制御に基づく Web サーバーに関する調査･設計に関する調査 報告書, 2005年.

[4] 情報処理振興事業協会(IPA), オペレーティングシステムのセキュリティ機能拡張の調査, 2002年.