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

ＯＳのセキュリティ機能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 と同じ機能を備えるようになったものなどの出現により、セキュリティを重視する用途で導入する事例の増加や、OS のセキュリティ機能への関心の高まりといった傾向が見られるようになっている。

しかし、こうした OS におけるセキュリティ機能は、実質的な機能が互いにほぼ同じであっても OS のベンダ毎に異なる名前で呼ばれていることがある。また、セキュリティ機能を有効化するために前提条件や制約が伴うこともある。こうした状況の中で、これまでの通常の OS の利用者が、セキュリティ強化の観点から情報システムを OS レベルから見直そうとしても、必要とする OS セキュリティ機能を利用することができるかどうかの判断に迷ったり、誤解したりすることが懸念される。

そこで本調査研究では、OS が提供するセキュリティ機能について、その種類と用途に応じてどのような機能が現状において利用可能なのかを把握することを目的として、情報の整理と分析を行った。また、一般社会においてはセキュリティ強化のための対策を講じることで、管理コストの増大や利便性の低下などの副作用が生じざるを得ないことも多いが、OS においても同様にセキュリティを強化することで設定作業の増大・高度化や操作上の制約を招くことがある。こうしたセキュリティ強化に伴う負の影響を緩和する手段として、各 OS ベンダは各種のツールやドキュ

メント、サポートサービス等をベンダが提供している。本調査研究ではこうした周辺状況についても OS の機能と同様に整理するものとした。

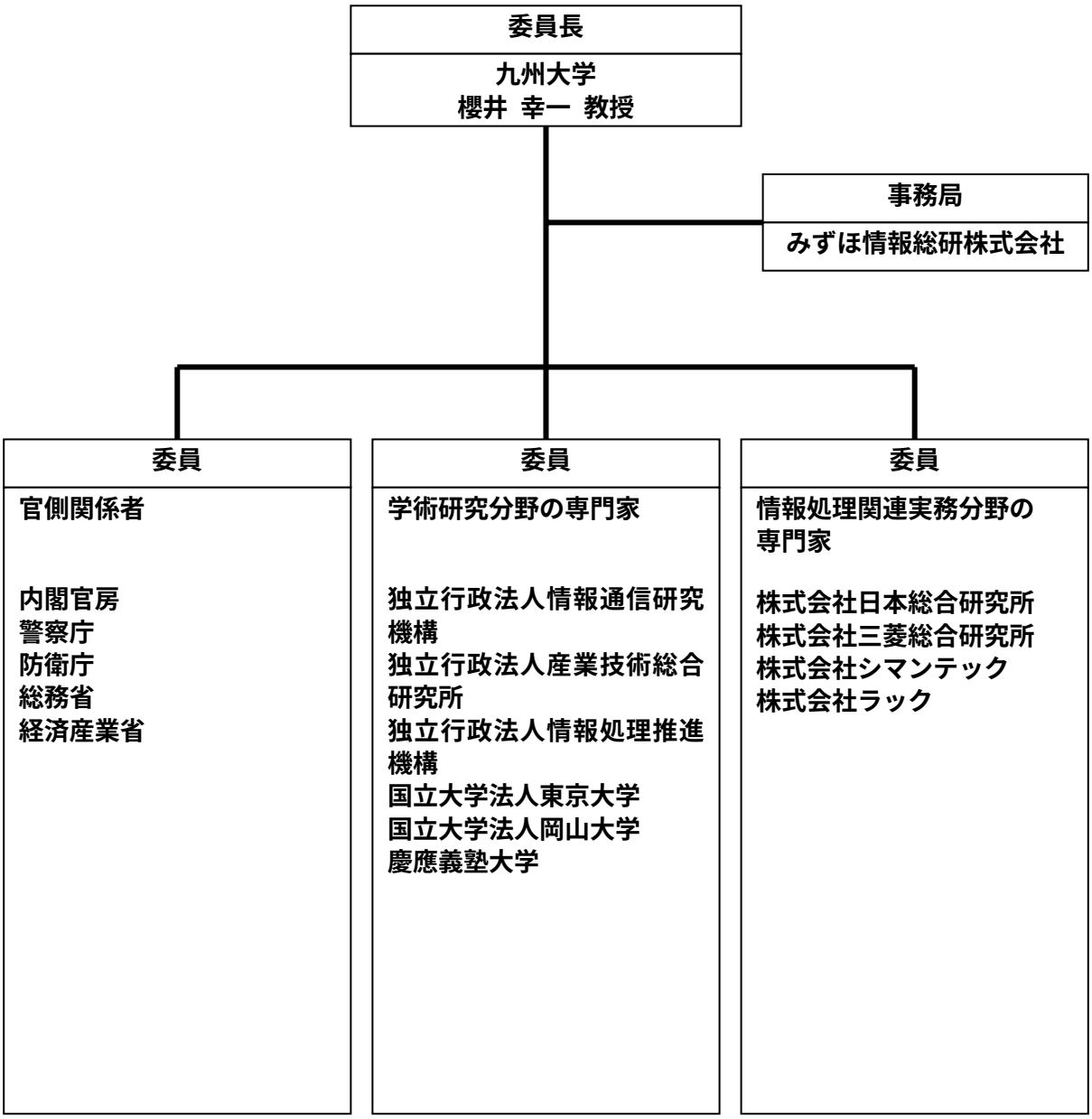
調査対象や条件の選定に際しては、電子政府で利用する情報システムでの利用を想定し、情報システムの調達関係者に向けた結果の整理・とりまとめを行っているが、本成果はこれにとどまらず一般の情報システムの利用者、調達者においても有効に活用し得るものと期待している。

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「OS のセキュリティ機能に関する調査研究」検討委員会での５回にわたる議論と、同委員会上で開催した OS ベンダによる製品のプレゼンテーションの結果をもとに、みずほ情報総研株式会社がとりまとめたものである。この場を借りて、議論に参加して頂いた委員の皆様と、情報提供頂いた OS ベンダ各社に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の一層の向上への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とりまとめたものである。



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	櫻井 幸一	九州大学 大学院システム情報科学研究院 情報工学部門 教授
委員	河野 健二	慶應義塾大学 理工学部 情報工学科 助教授
委員	田端 利宏	岡山大学 大学院自然科学研究科 産業創成工学専攻 助教授
委員	大山 恵弘	東京大学 大学院情報理工学系研究科 コンピュータ科学専攻 助手
委員	黒田 正博	独立行政法人情報通信研究機構 ワイヤレスアプリケーショングループ グループリーダー
委員	大岩 寛	独立行政法人産業技術総合研究所 情報セキュリティ研究センター ソフトウエアセキュリティ研究チーム 研究員
委員	宮川 寧夫	独立行政法人情報処理推進機構 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	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	女部田 武史	株式会社日本総合研究所 技術本部
委員	生田 安克	株式会社シマンテック ソリューション営業事業部 公共営業部 部長
委員	白井 雄一郎	株式会社ラック SNS事業本部 シニアコンサルタント
オブザーバ	山内 正	株式会社シマンテック ソリューション営業事業部 公共営業部 コンサルタント
オブザーバ	倉林 俊介	株式会社ラック SNS 事業本部 マネジメントコンサルティングサービス部 コンサルタント

○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

○ 調査対象

本調査は OS のセキュリティ機能としてどのような機能が現状において実際に利用可能なのかを把握することを目的として、以下の 7 種類の OS を対象に実施。OS ベンダによるプレゼンテーションと関連資料の提供をもとに、検討委員会における議論を通じて内容を検討。

- Windows Server 2003（米国 Microsoft 社）
- AIX 5L（米国 IBM 社）
- Compartment Guard for Linux（日本ヒューレット・パッカード（株））
- HP-UX 11i（米国ヒューレット・パッカード社）
- PitBull（LX / Foundation）（米国アーガスシステムズ社）
- SELinux（米国 NSA 他、本調査では製品例として Red Hat Enterprise Linux 4 を選定）
- Solaris 10 / Trusted Solaris（米国 Sun Microsystems 社）

これらの調査に加えて、SELinux と FreeBSD（TrustedBSD を含む）とを対象に、そのセキュリティ機能に関する技術的特徴について整理。

○ OS のセキュリティ機能別の分析結果

調査結果より、OS のセキュリティ機能別に以下の傾向が観察された。

①OS のアクセス制御機能の特徴

- 強制アクセス制御機能は Red Hat、HP-UX、PitBull（Foundation Suite）、Solaris（Trusted Solaris を含む）の各 OS が提供。このほか PitBull（LX）が情報の機密区分（classification）による上下関係の概念をもたない強制アクセス制御機能を提供。また Compartment Guard for Linux は、コンパートメントで隔離された相互間で強制アクセス制御に相当する機能を実現可能。これ以外の OS については、任意アクセス制御のみとなる。
- マルチレベルセキュリティ（MLS）は PitBull（Foundation Suite）と Trusted Solaris で利用可能。このうち PitBull（Foundation Suite）は、MLS に関するプロテクション・プロファイルである MLOSPP の暗号実装を除く範囲での認証申請中。
- 最少特権機能は、強制アクセス制御を提供する各 OS と、「アプライアンス・プロテクション機構」と呼ぶ独自の機能を実装する Compartment Guard for Linux が提供。
- コンパートメント化機能は以下の OS が提供するが、名称・内容ともに相違がある。
  - HP-UX：Security Containment 機能
  - Compartment Guard for Linux：コンテインメント機構、コミュニケーションガード機

構、ファイルガード機構
  - PitBull（LX）：ドメインベースアクセス制御（DBAC）
  - Solaris：仮想化（zones）
  - AIX：仮想化機能
- デュアルロック機能は PitBull（Foundation Suite）において利用可能。

②運用上の操作性

- GUI（グラフィカルユーザインタフェース）ベースでのアクセス制御等の操作は、PitBull を除く各製品で可能。

③支援ツールの提供状況

- Red Hat：外部ツールが利用可能。
- HP-UX、Solaris：システムポリシーの設定管理の支援ツールを OS の一部として提供。
- PitBull：通常の OS 用のアプリケーションを動作させるためのツールを提供。
- AIX：アクセス制御を強化するための製品が利用可能。
- Windows：RBAC としての制御を容易にするツールを無償提供。

④サポート体制

- OS のサポート期間については、「10 年」などの年数で定めている製品（HP-UX）と世代数で定めている製品（Solaris）がある。また PitBull のように通常の OS との組み合わせによる利用を前提とした製品では、サポート期間はベースとする OS のサポート期間に対応。
- 脆弱性対応については、いずれの製品についても必要な体制が整備されている。

⑤ドキュメントの整備状況

- ドキュメントの公開対象をライセンス契約者に限定せず、Web による一般のアクセスを可能とする例が多い。Red Hat、HP-UX、Windows 等は開発用のマニュアル類も公開。
- 日本語ドキュメントの比率はベンダによって相違があるものの、構築や運用に際して最低限必要となるドキュメントについては、いずれの OS も日本語版を提供。

⑥アプリケーションのユースケース

- 本項については、いずれのベンダからも有用な情報の提供は無し。アプリケーションの動作はその設計に依存する要素が大きく、一般論としての説明が困難なためと推察。

⑦アプリケーションと OS の連携状況

- OS とアプリケーションとの連携よりも、アプリケーションが無改造で動作することのアピールに重点が置かれており、連携に関する言及は少ない。

⑧導入実績

- トラステッド OS、セキュア OS としての機能を有する製品については、政府機関、軍事関連機関、金融機関等での利用例が紹介されている。

⑨Common Criteria 等の認証取得

- 通常の OS でも取得が可能な CAPP（Controlled Access Protection Profile）に基づくものが中心。LSPP（Labeled Security Protection Profile）については、Trusted Solaris 8 において取得済み、Red Hat と PitBull（Foundation Suite）において審査中。
- 認証の保証レベルについては、一般に民生用で最高レベルとされる EAL4 に拡張項目を付けて EAL4+としているものが多い。
- 拡張項目としては、Microsoft Windows における ALC_FLR（欠陥修正）のように、OS の欠陥に対する修正のマネジメントに対する保証の例などがみられる。

○ OS のセキュリティ機能の利用可能性

OS のセキュリティ機能のうち、現状において利用可能性が確認されたものと、利用可能性が確認できなかったものはそれぞれ以下の通り。

①システムポリシーに関する機能

- 強制アクセス制御機能や最小特権機能については、セキュア OS として提供、販売されている OS においてはいずれも利用可能であることが確認された。
- アクセス制御機能の名称が製品毎に異なるため、製品間の機能の比較は容易ではない。こうした中で LSPP などのプロテクションプロファイルへの準拠性に関する情報は、機能把握の手段として有用。

②運用・管理に関する機能

- デュアルロック機能はトラステッド OS として販売されている製品において利用可能。ただし民間での導入事例はほとんどない。
- 運用・管理の支援ツールは OS に組み込まれた形で提供されることも多いため、外部ツールが存在しなくても支援手段が提供されていないとは限らないことに留意の必要あり。
- 各ベンダから多くの情報が日本語で提供されている。かつてはトラステッド OS を利用しようとすると英語のドキュメントを参照せざるを得ない状況も存在したが、現在は概ね必要な事項の参照を日本語で行うことが可能。

③利用可能性の確認ができなかった事項

- 情報の格付けに基づくアクセス制御：米国国防総省においてトラステッド OS を用いた事例はあるものの、国内には公表事例がなく、ベンダにおいても紹介可能な事例を持ち合わせていないことが推察される。
- 異種 OS の混在環境におけるアクセス制御の連携：OS ベンダが異なると機能に関する呼び方、用語から異なるほどの相違がある中で、同一のネットワーク内部で異なるベンダ製品を組み合わせて使用している事例がほとんど存在しない。

○ 今後の展望

今後の展開としては以下の取組みが求められる。

- 政府機関統一基準における強制アクセス制御と最少特権への言及を踏まえた、調達時に OS のセキュリティ機能を要求する場合の雛形となるような要求仕様書の策定への応用。
- 仮想ではあるが現実性を備えたユースケースを多数想定した上での、それぞれの条件における利用可能性の検討。

第１章 OS に求められるセキュリティ機能とは何か

電子政府が行政機能における手続きや文書管理を電子化し、情報ネットワークを通じてそのサービスの提供や情報の交換を行うものである以上、電子政府で利用する情報システムは情報ネットワークに起因する多様な脅威に直面することは避けられない。

第１章では、情報システムにおける各種の脅威によってもたらされるリスクのうち、OS において対処することが望ましい対策は何かについて明らかにするとともに、こうした対策を実現するために OS が提供するセキュリティ機能を整理する。さらに、こうしたセキュリティ機能を利用する上で併せてどのようなことに留意する必要があるかについて考察する。

１.１ 電子政府で利用する情報システムにおけるリスクとその対策

電子政府で利用する情報システムにおいて想定される脅威と、それによる情報セキュリティ上のリスクについて、それぞれの脅威毎に特徴を整理すると、以下のようになる。

（1）アプリケーションの脆弱性を利用した不正アクセス

これは、アプリケーションの脆弱性を利用して攻撃者が非公開のファイルを読んだり、情報の書き換えや削除を行ったり、他のプログラムを動作させる権利を取得することで、情報漏洩やデータの改ざんなどの被害を生じさせるものである。

攻撃の方法としては、攻撃者が直接アクセスする場合のほか、ウイルスやワームの形で侵入させたり、トロイの木馬として送り込んだりすることもある。攻撃がが成功すると、攻撃者はアプリケーションのプログラムを動作させるために利用しているユーザの権限を得ることが多い。任意アクセス制御（Discretionary Access Control：DAC）機能で構成される通常の OS のもとでは、ユーザの権限を奪った攻撃者は、そのユーザの所有する全てのファイルやプログラムに関するアクセス制御の設定を自由に変更することができる。結果として、ユーザの所有するファイル全てが攻撃のリスクにさらされることになる。

一方、アプリケーションを動作させている OS が強制アクセス制御（Mandatory Access Control：MAC）機能のもとで運用されていれば、各ユーザは管理者に設定されたアクセス制御に関する設定を緩和することができない。よって、仮にアプリケーションを動作させているユーザの権限を奪ったとしても、アプリケーションを動作させるために与えられている権限以上の操作を行うことは不可能である。すなわち、読込みが禁止されているファイルの中身を見ることは出来ず、書込みが禁止されているファイルの改ざんもできない。結果的に、攻撃による被害は最小限に抑制される。

また、強制アクセス制御機能では、各ユーザに与える権限が集中的に管理・運用されるため、

アクセス制御の設定に関する利用者のミスを防ぎ、ポリシー設定の整合性を高める効果も得られる。

（２）管理者特権を奪取される不正アクセス

前項で示した不正アクセスの最悪のケースが、攻撃者が管理者特権を得てしまうものである。Windows や通常の UNIX などの OS においては、１種類の管理者特権で OS 上のあらゆる操作が可能となっており、これが攻撃者に奪われてしまえば、もはや被害を防ぐ手だてはない。

一方、OS のセキュリティ機能として強制アクセス制御と最少特権の両機能が提供されていれば、これらを用いて OS 全体の制御を攻撃者に奪われるのを防ぐことができる。すなわち、最少特権（Least Privilege）機能を用いると、管理者の役割をその目的に応じてアクセス制御、ユーザ管理、運用などの複数の管理者ユーザに分割することができる。さらに、強制アクセス制御機能により、アクセス権限の割当や変更の権限を担う管理者を除き、管理者であってもアクセス権限の変更を不可能にするとともに、アクセス制御の管理者権限は運用時は利用できないように設定しておく。このようにすることで、仮に運用中にプログラムの実行を操作する管理者特権が攻撃者に奪われたとしても、攻撃者はファイルの中身を見たり、削除したりすることができない。よって管理者特権が奪われるような状況においても、被害を抑制することが可能となる。

（３）リモートメンテナンス用のインタフェースからの不正侵入

情報システムの運用をアウトソーシングしている場合、情報システムのメンテナンスのために外部からのリモートメンテナンスのインタフェースを用意することが避けられないケースも多い。こうしたインタフェースの設定の不備や、ログイン用アカウント情報の漏洩が生じた場合、外部からの攻撃手段として利用される恐れがある。こうしたリスクに対し、強制アクセス制御機能と最少特権機能を利用してリモートメンテナンスからログイン可能なアカウントで利用できる特権やアクセスできる範囲を限定しておくことで、不正侵入による被害が抑制される。

（４）内部犯行

通常の OS の場合、管理者特権をもつ利用者が不正を行うと、操作ログの改ざんを証拠を残すことなく行うことが可能であるため、検出が困難なことが問題となっている。これに対して、最少特権機能を適用するとオペレーションを行う管理者にはログの削除等の権限を与えないことが可能となり、こうした不正の抑制が可能となる。

以上に挙げた例のほか、リスクとその対策についてより詳しく整理したものを、表１－１に示す。

表 1－1　電子政府で利用する情報システムにおけるリスクとその対策の例

脅威 （リスクの発生要因）	リスク	リスクの分類			対策	
		機密性	完全性	可用性	OSのセキュリティ機能によるもの 〇＝セキュアOSの機能 △＝通常のOSの機能	左記以外によるもの
OSの脆弱性を利用した不正アクセス（ウイルスやワーム等を含む）	機密情報へのアクセスを通じた情報の外部漏洩	●			〇強制アクセス制御と最少特権により、一部のアカウントを乗っ取られた場合でも機密情報へのアクセスを防止 〇コンパートメント／ゾーン化により、不正アクセスの影響範囲を限定	〇IDS等による不正アクセス等の監視
	Webなどの情報の改ざん、情報の消去		●		〇強制アクセス制御と最少特権により、一部のアカウントを乗っ取られた場合でも情報の書き換えを防止 〇コンパートメント／ゾーン化により、不正アクセスの影響範囲を限定	〇IDS等による不正アクセス等の監視
	サーバ機能のマヒ			●	〇強制アクセス制御と最少特権により、一部のアカウントを乗っ取られた場合でも必要なプロセスの停止や不正プログラムの起動を防止	〇IDS等による不正アクセス等の監視
	サーバの踏み台化				〇強制アクセス制御と最少特権により、一部のアカウントを乗っ取られた場合でも不正プログラムの起動を防止	〇IDS等による不正アクセス等の監視
アプリケーションやスクリプトの脆弱性を利用した不正アクセス（ウイルスやワーム等を含む）	機密情報へのアクセスを通じた情報の外部漏洩	●			〇最少特権によりアプリケーションの権限を必要最小限にすることによる被害の波及防止	〇アプリケーションやスクリプトの脆弱性検査 〇IDS等による不正アクセス等の監視
	Webなどの情報の改ざん、情報の消去		●		〇最少特権によりアプリケーションの権限を必要最小限にすることによる被害の波及防止	〇アプリケーションやスクリプトの脆弱性検査 〇IDS等による不正アクセス等の監視

脅威 （リスクの発生要因）	リスク	リスクの分類			対策	
		機密性	完全性	可用性	OSのセキュリティ機能によるもの 〇＝セキュアOSの機能 △＝通常のOSの機能	左記以外によるもの
（前ページから続く）	サーバ機能のマヒ			●	△アプリケーションへの資源割り当ての制限	〇アプリケーションやスクリプトの脆弱性検査 〇IDS等による不正アクセス等の監視
	サーバの踏み台化				〇強制アクセス制御と最少特権により、別のプロセスの起動を防止	〇アプリケーションやスクリプトの脆弱性検査 〇IDS等による不正アクセス等の監視
リモートメンテナンス用のインタフェースからの不正侵入	機密情報へのアクセスを通じた情報の外部漏洩	●			〇最少特権によりリモートメンテナンス時の権限を必要最小限に制限し、機密情報へのアクセスを防止 △ログの分析による不正侵入検知	〇リモートメンテナンス用の認証方式の高度化
	Webなどの情報の改ざん、情報の消去		●		〇最少特権によりリモートメンテナンス時の権限を必要最小限に制限し、被害範囲を局限化 △ログの分析による不正侵入検知	〇リモートメンテナンス用の認証方式の高度化
	サーバ機能のマヒ			●	〇最少特権によりリモートメンテナンス時の権限を必要最小限に制限し、不正なプログラムの起動を抑制 △ログの分析による不正侵入検知	〇リモートメンテナンス用の認証方式の高度化
内部犯行	機密情報へのアクセスを通じた情報の外部漏洩	●			〇強制アクセス制御と最少特権によるアクセスログの改ざん防止 〇デュアルロックによる犯行の抑止	
	データベース等の情報の改ざん、消去		●		〇強制アクセス制御と最少特権によるアクセスログの改ざん防止 〇デュアルロックによる犯行の抑止	

１.２ セキュリティ機能の分析時に考慮すべき項目

ここでは、前項で指摘した OS のセキュリティ機能による効果を発揮させるべく、OS が備えるセキュリティ機能を分析、比較する際に考慮すべき項目について整理する。

１.２.１ OS のアクセス制御機能に関するもの

OS が提供するセキュリティ機能において、重要な役割を担うのがアクセス制御に関する諸機能である。こうしたアクセス制御に関連する機能を以下に列挙する。

（１）強制アクセス制御（Mandatory Access Control：MAC）

一般的に利用されている OS においては、リソースやプログラムに対する読込み、書込み、実行等のアクセスに関する割当や設定変更の権限は、そのリソースやプログラムの所有者（オーナ）が保持している。こうし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。これに対して、OS におけるアクセス権限の管理者が定めたポリシーのもとで、全てのファイルやプログラムのアクセス権限が一元的に制御され、所有者が設定を緩めたりすることができないアクセス制御の方法が、強制アクセス制御（Mandatory Access Control：MAC）である。本来の強制アクセス制御は、米国国防総省の規則として制定された Trusted Computer System Evaluation Criteria（TCSEC）において Bell-LaPadula モデル（詳細は文献[1]を参照）を実現するためのアクセス制御の方法を指したが、現時点では上述の意味で利用されることが多い。

いわゆるセキュア OS の定義において、最少特権とともに本機能が実装されていることをその必要条件とするのが一般的である。TCSEC におけるトラステッド OS の定義では本機能が必須となっている。

（２）最少特権（Least Privilege）

OS のアドミニストレーション（管理）用ユーザなどに与えられる特権（管理者特権）を、その用途に応じて必要最小限のみを割り当てることができる機能である。一般に用いられる OS においては、管理用ユーザに複数の名前を割り当てることが可能でも、管理者特権においてはどの名前でも同じにならざるを得ないのが普通である。一方最少特権機能を備えた OS では、アクセス制御、ユーザ管理、プログラムの実行、メンテナンスなどの管理の用途毎に異なる管理用ユーザを作成し、それぞれの用途毎に必要最小限の管理者特権を与えることができる。

いわゆるセキュア OS の定義において、強制アクセス制御とともに本機能が実装されていることをその必要条件とするのが一般的である。TCSEC におけるトラステッド OS の定義では本機能が必須となっている。

（3）マルチレベルセキュリティ（Multiple Level Security：MLS）

マルチレベルセキュリティとは、各ファイルを、例えば「機密」「極秘」「秘」「公開」などとレベル付けをすることにより、各ユーザが自身に割り当てられたレベルよりも上／同等／下のファイルに対して行うことが可能な操作を制御するものである。

一般にいわゆるセキュア OS としての必要条件とはされないが、TCSEC におけるトラステッド OS の定義では本機能の実装が求められている。

（4）マルチカテゴリセキュリティ（Multiple Category Security：MCS）

マルチレベルセキュリティと似ているが、レベルによる上下関係を持たないカテゴリに属するファイルに対して、各ユーザが可能な操作を制御するものである。

マルチレベルセキュリティと同様、セキュア OS としての必要条件とはされていない。

（5）コンパートメント化

狭義の強制アクセス制御機能には含まれないが、OS 内部においてユーザやプログラムがアクセスできる範囲の区切りを設け、この区切りを同時に複数運用しながら相互のアクセスを遮断することができる機能を指す。本機能についての呼び方は OS によって異なり、コンパートメント、ゾーンなどと呼ばれる。（3）の MLS や（6）の RBAC を実現するための機能として実装されている場合もある。

（6）ロールに基づくアクセス制御（Role-Based Access Control：RBAC）

ロールに基づくアクセス制御（RBAC）は、ユーザの役割に応じた「ロール」を定義し、ロール単位でアクセスできるデータやプログラムの設定を行うものである。同じ役割を担う複数のユーザを同一ロールに割り当てることで、管理の手間を省く効果がある。

RBAC 機能は、OS によってドメイン、ラベル、タイプエンフォースメント、コンパートメントなど、それぞれ独自の概念に基づくアクセス制御機能を用いて実装されている。よって、RBAC 機能を利用する際の設定方法も OS 毎に異なるため、設定可能な内容の相違に留意する必要がある。

（7）デュアルロック

デュアルロックは、OS に対する重要な設定変更を行う場合に、2 名以上の指定人数の管理者による操作を要求すること通じて、運用時の組織内部の不正を防ぐための仕組みである。一般にいわゆるセキュア OS としての必要条件とはされないが、TCSEC におけるトラステッド OS の定義

では本機能の実装が求められている。

１.２.２ OS の周辺、付加価値に関するもの

OS の機能に関する特徴のうち、前項に示した OS のアクセス制御に関する特徴以外の項目で比較することが有用と考えられるものを挙げる。

（１）運用上の操作性

OS に対する操作を行う場合の操作方法に関する特徴を整理する項目である。本調査では OS の用途として、一般利用者が直接利用するクライアント端末ではなく、サーバやゲートウェイでの適用を想定しているため、操作の主体は OS の管理者となることから、本項目は管理上の操作性についての比較に相当する。

本項に該当する項目としては、以下が挙げられる。

① GUI（グラフィックユーザインタフェース）による操作の可否

近年の操作環境として標準的となった、GUI（グラフィカルユーザインタフェース）を用いた操作が可能か、あるいは従来からのコマンドラインによる操作（CUI、キャラクタユーザインタフェース）を用いる必要があるかで大別される。CUI では操作すべきオペレーションを利用者がコマンドの形で個別に指示するのが一般的であるのに対し、GUI は操作すべき内容を画面上から選んで指示することができるため、熟練者でなくても使いこなせると受け取られている面がある。ただし、GUI であっても十分な知識がなしに操作を行うとシステムが不適切な設定の状態に置かれる恐れがあることには変わりなく、GUI であれば未熟な管理者であっても運用が可能であることを意味しないことに留意する必要がある。

② 常用しているシステムとの操作の類似性

OS の構成する要素の名称や操作体系などが、広く普及している通常の OS と類似しているかどうかを示す。独自の名称や操作体系を有する OS の場合は、習熟のためにより多くの研修等を行う必要があるのが一般的である。

（２）支援ツールの提供状況

OS の管理運用をより容易に行えるようにするため、OS に付属ないし独立した形で、オペレーションを支援するツールが提供されているかどうかを示す。OS に付属の場合は提供者は OS のベンダとなるが、独立している場合は OS ベンダが提供しているツールのほか、サードパーティのベンダやシステムインテグレータが製品やサービスの一環として提供するツール、ユーザ等がフリーソフトウェアとして提供するツールなど様々な形態をとる。

目的に応じてツールを分類すると、以下のようになる。

① ポリシー設定支援ツール

システムの構築時にアクセス制御のためのポリシー設定を行う際、煩雑な設定操作の負荷を軽減したり、設定内容の相互矛盾や設定ミスによるセキュリティホールを検出することなどを目的としたツールである。ツールを利用するタイミングはシステムの構築時と構成変更時のみであり、通常の運用時には必要ないため、ツールの利用者がユーザではなく、システムの構築ベンダのみとなる場合もある。

② ユーザやリソースの管理支援ツール

ユーザの登録、削除やユーザのグループないしロールの追加、削除、記録装置や特権に対するアクセス権の付与、削除等、システムが提供するリソースに対する操作を、ユーザが OS に対して直接行う代わりにツール上で行うことで、操作性の向上や矛盾する設定の防止等の効用をもたらすものである。こうした目的のツールは OS の一部として組み込まれていることも多く、ツールが提供されていないことが操作性の悪さを意味するわけではないことに留意が必要である。

（3）サポート体制

OS に起因すると思われるトラブルや、OS のセキュリティ対策等に関するサポートにどのような種類があるか、そのサポートを実現するためにどのような体制が構築されているかを示すものである。サポートの提供主体は OS 製品ベンダのほか、システムインテグレータ等なども含まれる。OS 製品のユーザが無料で利用できるサポートはサービスの種類が限定され、24 時間 365 日のサポートなどは別の有料サービスとなっているのが一般的である。よって、サービスの評価に際してはシステムの目的に適合したサポートのサービスが適切なコストで利用できるかどうかを検討する必要がある。

（4）ドキュメントの整備状況

OS に関するドキュメントとしてどのようなものが提供されているかを示す。ドキュメントの形態として以下の分類が想定される。

- 提供主体：OS ベンダが提供するもののほか、他の事業者が提供するもの、ユーザ会等が提供するものがある。
- 入手費用：一般に OS ベンダが提供するものは無料のものが中心であるが、限定した用途のものについては有料で提供されるものがある。OS ベンダ以外の事業者が提供するものは有料であることが多い。

• 媒体：紙媒体、CD や DVD 等の電子媒体、ネットワーク上での提供などに大別される。
• 契約の要否：ドキュメントの種類によっては、提供者以外の参照を禁じている場合がある。

ここで対象とするドキュメントの種類としては、以下に示すものが挙げられる。

① ユーザマニュアル等

OS の使用方法について解説するものである。初心者向けのチュートリアルなどもこの分類に含まれる。

② デベロッパーズマニュアル

OS 上でのアプリケーションの開発を行う際に必要な情報を提供するドキュメントである。ここに分類されるドキュメントについては OS に付属せず、別途入手する必要があるものが多い。

③ OS の仕様に関するドキュメント

OS の機能や性能等について、具体的な仕様を記述したドキュメントである。OS についてのホワイトペーパとも呼ばれる。後述する Common Criteria に関する認証取得に際してのセキュリティターゲット（ST）もこれに類するものである。

（5）アプリケーションのユースケース

OS 上でどのようなアプリケーションを動かすことが可能かを、その動作環境等とともに示すものである。実際に導入されているかどうかに限定されないものであり、導入事例よりは想定範囲が広いものと考えて差し支えない。

（6）アプリケーションと OS の連携状況

OS と、その上で動作させるアプリケーションとの間で、どのような連携が可能かを示すものである。連携の内容としては、ユーザやリソースに関するアクセス制御を一元的に行えるようにすることなどが想定される。

（7）導入実績

OS がこれまでどのような組織・機関において導入されているかを示すものである。自組織と規模や用途が類似している組織において導入実績があれば、機能や性能が要求仕様を満たす可能性が高いとみることができる。また、導入実績が多ければそれだけ多様な用途で利用されていることで、OS における不安定な要素が少なくなっていることが期待される。ただし、導入済み組織の中にはセキュリティ上の懸念から、自組織で導入していることを非公開にするところも多く、公開されている導入事例が限定されていることが、実際の導入事例が少ないことを必ずしも意味し

ないことがあるので留意が必要である。特にセキュア OS に分類される OS を導入している場合において、この傾向が顕著である。

（８）Common Criteria 等の認証取得

ソフトウェアに関する情報セキュリティの国際標準として、ISO/IEC15408 に基づく評価・認証制度がその参加国によって運営されている。これは一般に Common Criteria（CC）[1]と呼ばれ、OS においてもその認証を取得しているものが存在する。

以下に、この認証取得に際して留意すべき事項を整理する。

① セキュリティターゲット（ST）について

OS のセキュリティ機能として保証されている具体的な内容については、認証取得の際に用いられたセキュリティターゲット（Security Target：ST）を参照する必要がある。この際に留意すべきポイントを以下に示す。

- ST の評価対象（Target Of Evaluation：TOE）記述には、保証される機能と範囲について記載されている。
- TOE が、最小構成インストールであるのか、付加的なアプリケーション、ユーティリティソフトウェアが含まれるかは TOE 記述で表現されている内容から判断しなければならない。
- 評価済みプロテクションプロファイル（PP）として、OS が提供すべきセキュリティ要件を定義しているもの（CAPP、SLPP、MLOSPP 等）に準拠することが宣言されていることが多い。
- PP に準拠するとは、PP の要求事項を正確に実現していることを意味する。これに対して単に PP を参考として利用している場合もあり、注意が必要である。
- PP に準拠していれば、必要なセキュリティ機能が確実に評価されているため、評価対象となった範囲実体についてそれほど注意を払う必要性はない。

範囲の差で注意すべきは、対象領域が広いほど何らかの脆弱性が含まれる可能性が高まることを意味する。したがって対象領域が広く宣言している TOE である場合、より多くの可能性について検査が実施されたことを意味する。ST にはこの TOE 範囲について、論理的範囲と物理的範囲という観点から説明される。この記載を比較することによって、保証された TOE 範囲を理解することができる。論理的範囲、物理的範囲とは具体的には以下の通りである。

[1] Common Criteria の詳細については、昨年度報告書[1]付録 C（３）参照。

ア）論理的範囲

論理的範囲とは「機能の範囲」のことで、TOE が提供する機能、特にセキュリティ機能について説明されることによって理解することができる。PP に準拠、または PP を利用している場合は、ほぼ横並びの説明になるが、中には PP の構成をベースとしながら、各製品にて特徴的なセキュリティ機能を追加し、評価対象に含めているケースもある。

イ）物理的範囲

物理的範囲は、「ソフトウェアコンポーネントの範囲」のことで、TOE を構成するソフトウェアコンポーネント、モジュールについて説明されることによって理解することができる。TOE の名称に製品の名称をそのまま利用しているケースが多く、あたかも当該製品のすべてのソフトウェアコンポーネントが評価されたように見えるケースがあるが、本説明によって実際に評価された範囲を判断することができる。しかし公開される ST のほとんどが、それぞれ独自の説明を行っているケースが多く、単純に比較することはできない。例えば、インストールされるソフトウェアコンポーネントをファイル単位で記載しているものもあれば、物理的な構成について特に明示的な記載のない ST も存在する。したがって現状では、OS インストール最小構成のソフトウェアコンポーネントが確かに保証されているかどうか比較することは困難である。

ただし PP に準拠している場合は、PP にて想定される脅威、組織のセキュリティ方針に対して必要十分なセキュリティ機能（セキュリティ要件）を実装していることの評価を受けていることは確実であるため、実際に評価されたソフトウェアコンポーネントの範囲の大小が及ぼす影響は少ない。

ウ）保証レベル

保証レベルは、宣言された機能が「どこまで詳細にチェックが行われたか」ということを示すものであり、レベルが高いほど強固なセキュリティ機能を実装しているという意味ではない。PP に準拠している場合は、PP の要求事項として明示される保証レベルでの評価が実施されたことになるが、PP を参考利用している場合は、それぞれ任意の保証レベルが設定されている。取得している保証レベルは、必ずチェックする必要がある。

② プロテクションプロファイル（PP）について

OS に関するプロテクションプロファイルとして、OS 製品の認証の際に利用されるものを以下に示す。これらはいずれも米国国防総省（DoD）のセキュリティ要件に基づき、国家安全保障局（NSA）が作成したものである。ここではその特徴について整理する。

ア）CAPP（Controlled Access Protection Profile）

アクセス制御に、ユーザ識別情報に基づくオブジェクト（ディレクトリ、ファイルなど）のアクセス制御（いわゆる任意アクセス制御（DAC））を要求する。

TCSEC の C2 レベルに相当する。

イ）LSPP（Labeled Security Protection Profile）

CAPP の要求するアクセス制御に加え、ユーザを「クリアランス」と呼ぶ追加情報で区分し、クリアランスに応じてオブジェクトをアクセス制御すること（いわゆる強制アクセス制御（MAC））を要求する。

TCSEC の B1 レベルに相当する。

ウ）MLOSPP（Multilevel Operating System Protection Profile）

情報の機密度に応じたマルチレベルセキュリティを扱うもの。強制アクセス制御（MAC）のほか、強制インテグリティ制御（Mandatory Integrity Control：MIC）と暗号化機能を要求する。

TCSEC の B2 レベルに相当する。

エ）SLOSPP（Single Level Operating System Protection Profile）

商用 OS を対象としたもので、単一のレベル区分と認証、任意アクセス制御、監査と暗号化の各機能を要求する。

（9）その他

上記（1）～（8）に該当しない特徴や、OS に関する今後の動向などが想定される。

第２章 各 OS の特徴とセキュリティ機能

第２章では、実際に利用可能 OS を対象に、それぞれがどのようなセキュリティ機能を備えているかについて整理する。

２.１ 調査の実施要領

２.１.１ 対象候補 OS の抽出

本来であればセキュリティ機能を強化した全ての OS を対象に調査を行うことが望ましいが、限られたリソースで調査することを考慮し、これまでの導入実績、知名度、歴史的経緯等を踏まえ、以下の OS を対象として調査を実施している。このうち SELinux については、カーネル 2.6 より SELinux に相当する機能が Linux の標準カーネルに組み込まれたこともあり、多くの OS ベンダより SELinux のセキュリティ機能に対応した製品が提供されているが、代表例として一製品を選定している。

表 ２－１　調査対象とした OS の種類

対象OS	開発元	プレゼンテーション依頼先
Windows Server 2003	米国Microsoft社	マイクロソフト（株）
AIX 5L	米国IBM社	日本IBM（株）
Compartment Guard for Linux	日本ヒューレット・パッカード（株）	日本ヒューレット・パッカード（株）
HP-UX 11i	米国ヒューレット・パッカード社	
PitBull（LX / Foundation）	米国アーガスシステムズ社	インフォコム（株）
SELinux	米国NSA他	レッドハット（株） （Red Hat Enterprise Linux 4）
Trusted Solaris	米国Sun Microsystems社	サン・マイクロシステムズ（株）
Solaris 10		
FreeBSD （TrustedBSDを含む）	The FreeBSD Project （The TrustedBSD Project）	

2.1.2 調査方法

（1）OS 製品ベンダによる情報提供

本調査において、次表のような依頼要領をベンダに提示し、これに基づいて委員会の席上にて各ベンダよりプレゼンテーションが実施された（2005 年 9 月）。後述する調査結果は、このプレゼンテーションにおいて示された内容をもとに、後日実施した補足調査による成果を加えてとりまとめたものである。

表 2－2　ベンダへの依頼要領

自社製品 OS が備える、「OS によるアクセス制御を中心としたセキュリティ機能」について、電子政府システムでの利用を想定し、以下の要素も考慮した説明をお願いします。

- **運用管理上の操作性（支援ツールの提供等を含む）**
- **サポート体制**
- **ドキュメントの整備状況**
- **OS のセキュリティ機能を利用したアプリケーション**
  （ユースケース、OS のセキュリティ機能との連携状況）
- **導入実績（可能であれば）**

（2）SELinux と FreeBSD/TrustedBSD に関する調査

委員による OS 機能の比較検討に際して、主として OS の技術的側面からの情報提供を目的として、以下の 2 種類を対象にそれぞれ国内の代表的な専門家によるプレゼンテーションを実施した（2005 年 11 月）。

表 2－3　技術的要素を中心とした OS 機能に関するプレゼンテーション

対象 OS	説明者	所属
SELinux	才所秀明氏	日立ソフトウェアエンジニアリング（株）
FreeBSD/TrustedBSD	佐藤広生氏	独立行政法人 情報処理推進機構（IPA）

２.２ 調査結果

２.１.２の調査方法によりとりまとめた成果を各社毎に提示する。掲載順序はプレゼンテーションの発表順と一致している。なおプレゼンテーションは 2006 年 9 月に実施したが、その後 2006 年 3 月までに各 OS に関して生じた変更事項については極力反映するよう努めている。

とりまとめに際して根拠とした情報源を、下表による略記にて各項目の見出し末尾に示す。

表 ２－４　情報源に関する凡例

[プレゼン]	プレゼンテーション時に配布された資料によるもの
[Web]	Web サイトに掲載されているもの
[外部]	ベンダ以外の情報源によるもの
[補足]	プレゼンテーション以後のベンダへの質問等によるもの

（１）Red Hat Enterprise Linux

1. OS のアクセス制御機能の特徴

○セキュア OS の特徴（強制アクセス制御、最少特権）に関するアクセス制御機能

- SELinux によるセキュリティ機能

◆SELinux の特徴 [プレゼン]

－強制アクセス制御（MAC）の機能を持った Linux（≠TrustedOS）であり、NSA（米国国家安全保障局）と Secure Computing 社による 10 年来の研究成果によるもの

－OS レベルでのセキュリティアーキテクチャである Flask（Flux Advanced Security Kernel）に基づく

－セキュリティモデルは SVO（Subject が Object を Verb する）文脈で解釈

◆SELinux による強制アクセス制御（MAC）の特徴 [プレゼン]

－カーネルモジュールによる完全なアクセス制御

－LSM(Linux Security Module)による実装

－リソース操作に対する制御の粒度が向上

－ほぼ全てのリソースを制御可能

→SELinux が起動している限り攻撃不可能とすることが可能

◆SELinux による強制アクセス制御（MAC）の構成要素［プレゼン］

1) Type Enforcement

・「型強制」→「型にはめる」

・Flask アーキテクチャの SVO にそれぞれドメイン・タイプを定義する

・定義された SVO という文脈をセキュリティコンテキストと呼ぶ

◇プロセス（サブジェクト）にはドメイン

◇リソース（オブジェクト）にはタイプ

◇操作をアクセスベクタとして定義

2) Role Based Access Control

・ロールを定義

◇ロールにはドメインの利用許可が与えられる

・各ユーザは指定されたロールのみ使用可能

◇ユーザには複数のロールを割り当てることが可能

◆Red Hat Enterprise Linux 4 においては、以下の 2 つのポリシーが提供される［プレゼン］

1) Strict Policy

・デフォルトでは全て拒否

・最小権限の原則の徹底

・汎用的なサーバでは適用が難しい

・Fedora Core 2 において採用した際には、多くのユーザから「どうやってオフにするのか？」との質問を受けた

2) Targeted Policy

・エッジサーバを保護

・デフォルトでは全て許可

・Unconfined_t ドメインの追加

◇unconfined_t ドメインで動作するデーモンとシステムプロセスでは、任意アクセス制御（DAC）方式のみをアクセス制御に使用（ID とロールの機能を使用しない）［Web］

・ユーザスペースは全く保護されない

・以下の 13 種類のターゲットを対象

◇httpd, dhcpd, mailman, mysqld, named, nscd, ntpd, portmap, postgresql, squid, syslogd, winbind, snmpd

◇これらのターゲットでは、httpd であれば httpd_t というロールを用いることで強

制アクセス制御（MAC）方式によるセキュリティの強化が可能［Web］

◇Fedora Core 5 では 70 種類に増加

Web：特集記事「Red Hat Enterprise Linux での SELinux の活用」
http://www.jp.redhat.com/magazine/NO12/

○その他のアクセス制御機能

- ExecShield、PIE によるセキュリティ機能［プレゼン］

◆ExecShield は以下の２つの機能から構成

－NX/XD（No eXecute / eXecute Disable）

・Intel：eXecute Disable（Itanium2, x86/EM64T）、AMD：No eXecute

・メモリページの制御を以前は read/write のみ可能だったものに execute も追加

・実装：メモリページに、実行可能・不可能のフラグ（標識）を設定できる

・RHEL3 U3 以降でサポート

－セグメンテーション

・NX/XD 機能を持たない CPU 向け

・x86 プロセッサのメモリ管理機能を利用：実行可能・不可能の２つのセグメントにアプリケーションを分割する

◆PIE（Position Independent Executables、位置非依存実行形式）

－アプリケーションが実行されるたびに、アプリケーションの異なるセクションを、異なるメモリ位置上にランダムに配置する機構

→バッファオーバーフローやスタックオーバーフローといった攻撃手法は、攻撃者がメモリ上の予測可能な位置に任意のコード（プログラム）を置けるのが原因

◆ExecShield + PIE の有効性

－2003 年 11 月 1 日～2004 年 8 月 11 日の期間に Linux 向けに公表されたセキュリティ問題 16 件のうち、11 のスタックバッファオーバーフロー、1 つのヒープバッファオーバーフローについて ExecShield +PIE で防御可能

2. 運用上の操作性

○GUI ベースの操作に関する特徴

- セキュリティレベルの設定［プレゼン］

◆コントロールパネルによる簡便な設定により、SELinux のモード切替、ポリシータイプの変更、ポリシーの大まかな変更が可能

◆system-config-securitylevel パッケージによって標準で提供

- 支援ツール（selpec/sellog/selchk：後述）を GUI ベースで利用可能［プレゼン］

3. 支援ツールの提供状況

○ポリシー設定・管理に関する支援ツール

- 日立ソフトウェアエンジニアリング株式会社が独立行政法人情報処理推進機構（IPA）の委託事業として開発し、GPL ライセンスで一般に公開している下記ツールが利用可能 [プレゼン]

◆selpec（ポリシー設定ツール）

◆sellog（ログ解析ツール）

◆selchk（監査ツール）

○その他の支援ツール

- Red Hat Network：多数のハードウェア管理を容易にするツール［プレゼン］

4. サポート体制

○標準でのサポート

- SELinux のインストールと設定に関して標準でサポートされる範囲［プレゼン］

◆ブーリアン値の設定、ファイルコンテキストの変更、SELinux の無効化

◆以下のサービスが SELinux の targeted ポリシーで動作すること：

httpd, dhcpd, mailman, mysqld, named, nscd, ntpd, portmap, postgresql, squid, syslogd, winbind, snmpd

◆ポリシーの切り替え、アップグレード

◆Access Vector Cache メッセージ（audit ログ）の解決

- targeted ポリシーに対して以下のような変更を加えると、サポート契約が破棄される（後述の GPS にて対応） [Web]

◆デーモンのポリシーに変更を加えること

（特にそれらの変更がアクセスの限定に関係する場合）

◆Red Hat Enterprise Linux の一部であるプログラム用に新しいドメインを追加すること（Red Hat Enterprise Linux の一部ではないプログラムに新しい変更を加えることは、報告されているバグが対象のプログラムと無関係であるかぎり許可）

Web：特集記事「Red Hat Enterprise Linux での SELinux の活用」
http://www.jp.redhat.com/magazine/NO12/

○有償サポート

- GPS（Global Professional Service）での有償サポート［プレゼン］

◆SELinux 対応アプリケーションの作成の助言

◆strict ポリシーの導入

◆ポリシーの新規作成

○サポート体制

- Security Response Center による体制［プレゼン］

◆脆弱性情報に関するモニタリング、対応パッケージとアドバイザリの作成、Red Hat Network による公開

◆Red Hat Enterprise Linux 3 の場合、リリース後最初の 12 ヶ月で critical に分類された脆弱性の 58%、important の 44%が即日対応されている。

5. ドキュメントの整備状況

○OS のセキュリティ機能に関する White Paper 等

- SELinux に関するもの［プレゼン］

◆SELinux ガイド（英語／HTML,PDF）
http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/selinux-guide/

◆RHEL 4 セキュリティガイド（日本語／HTML,PDF）
http://www.redhat.com/docs/manuals/enterprise/RHEL-4-Manual/ja/security-guide/

- Common Criteria［プレゼン］

◆Red Hat | Government（英語／HTML）
http://www.redhat.com/explore/government/

○その他のドキュメント

- マニュアル、サポート等［プレゼン，補足］

◆管理入門ガイド（日本語／HTML,PDF）

http://www.redhat.com/manual/
◆サポートサービスの項目一覧及びサポート方法（日本語／HTML）
http://www.jp.redhat.com/support/service/
◆政府・官公庁向けサイト
http://www.redhat.com/solutions/industries/government/

- 外部のリソース [プレゼン, 補足]

◆selpec/sellog/selchk（日本語／HTML）
http://www.selinux.hitachi-sk.co.jp/tool/selaid/selaid-top.html
◆第 2 回：Red Hat Enterprise Linux セキュリティの概要と特徴（日本語／HTML）
http://www.thinkit.co.jp/free/compare/16/2/1.html
◆Federal Enterprise Architecture（英語／HTML）
http://www.feapmo.gov/fea.asp
◆SELinux Play Server（英語／HTML）
http://www.coker.com.au/selinux/play.html
◆Linux Documentation Project（英語／HTML）
http://www.redhat.com/mirrors/LDP/

- SELinux に関する書籍 [プレゼン, 補足]

◆SELinux システム管理（オライリー・ジャパン, ISBN4-87311-225-7）
http://www.oreilly.co.jp/books/4873112257/
◆SELinux 徹底ガイド（日経 BP 社, ISBN4-8222-2111-3）
http://bpstore.nikkeibp.co.jp/item/main/148222211130.html

6. アプリケーションのユースケース

（なし）

7. アプリケーションと OS の連携状況

○アプリケーションにおける OS のセキュリティ機能を用いたアクセス制御

- NX/XD(No eXecution/eXecution Disable) [プレゼン]：

→同梱されるアプリケーション全てが対応済み

- 以下のサービスを MAC で強化することが可能 [プレゼン, Web]：

httpd、dhcpd、mailman、named、portmap、nscd、ntpd、portmap、mysqld、postgresql、squid、syslogd、winbind、ypbind。

Web：特集記事「Red Hat Enterprise Linux での SELinux の活用」
http://www.jp.redhat.com/magazine/NO12/

8. 導入実績

- 米国の連邦レベルのカスタマーとして、以下の諸機関で導入されている [プレゼン]。

NOAA 海洋大気局）

DOE（教育省）

GSA（共通役務庁）

A.O.U.S.C.（連邦裁判所管理局）

NASA（航空宇宙局）

FAA（連邦航空局）

DHS/FEMA（国土安全保障局/連邦緊急事態管理庁）

DOJ（司法省）

PTO（特許商標庁）

USDA（農務省）

Intelligence Community（情報機関）

U.S. Air Force（空軍）

U.S. Army（陸軍）

U.S. Navy/Marines - CRADA（海軍－共同研究開発協定）

9. Common Criteria 等の認証取得

○Common Criteria への対応（予定も含む）

- NIAP/Common Criteria 認証取得状況 [プレゼン]

◆Red Hat Enterprise Linux 2.1 – EAL 2 (2004 年 2 月に完了)

◆Red Hat Enterprise Linux 3 EAL 3+/CAPP (2004 年 8 月に完了)

◆Red Hat Enterprise Linux 4 EAL 4+/CAPP (2005 年 10 月予定)

◆次の評価の目標：EAL4+/LSPP (2005 年 10 月にアナウンス)

◆認証のレポートとロードマップは以下で公開：

http://www.redhat.com/explore/government

○その他の認証

- DII-COE [プレゼン]

◆Red Hat Enterprise Linux 3 (2004 年 10 月に自己認証が完了)

◆Red Hat Enterprise Linux：DISA によって最初に認証された Linux プラットフォーム

- Federal Enterprise Architecture (FEA) [プレゼン]

  ◆Linux と他のオープンソーステクノロジー（Apache）を OMB により組み込み

  ◆詳細については以下を参照

  http://www.feapmo.gov/fea.asp

10. その他

- Common Criteria [プレゼン]

  ◆RHEL5 + IBM eServer（x/p/zSeries） / Blade Center + TCS（Trusted Computer Systems）での Common Criteria 認証に向け、9 月 27 日、『Common Criteria Evaluation and Validation Scheme (CCEVS)』(共通基準評価と認証スキーム) プログラムに登録したことを発表。

  ◆RHEL5 のリリースは 2006 年下半期を予定。

- Trusted Linux [プレゼン]

  ◆TCS は IBM および Red Hat との共同チームを組み、米中央情報局長官の要件を満たす Trusted Linux を Red Hat 製品（名称未定）として 2006 年にリリースすることを先日発表。

  ◆RHEL5（SELinux）とは別に、TCSEC（Trusted Computer System Evaluation Criteria）の要件を満たすトラステッド OS として実装される予定。

（2）HP-UX 11i

1. OS のアクセス制御機能の特徴

○セキュア OS の特徴（強制アクセス制御、最少特権）に関するアクセス制御機能

- Security Containment 機能（HP-UX 11i v2 の標準機能として提供）[プレゼン]

◆コンパートメント

－関連のないリソースの隔離

－強制アクセス制御の実現

◆柔軟な特権設定（FGP：Fine-grained Privilege）

－Root 特権の細分化

－最少特権による制限

◆Role-based Access Control（RBAC）

－役割ベースの特権管理

- Security Containment 機能の利点［プレゼン］

◆被害の抑制

－万が一攻撃者が侵入に成功しても、被害を最小限にとどめられる

◆軍用仕様(B1/LSPP)の画一的な制御ルールを調節可能

－企業におけるビジネス利用を前提とするアプリケーション互換性と強固なセキュリティの両立

◆トラステッド OS の欠点の克服

－透過性

・オブジェクトラベル情報を集中管理することでコンパートメントの可視化を容易に

→ファイルツリーとのマッピング

－シンプルなモデル

・マルチラベルディレクトリと機密レベルによる複雑性をシンプルな設計により回避

・コンパートメント設定情報はファイルやプロセスと直接関連付けされる

◇バックアップ・リストアが容易

◇別システムへのコンパートメントの複製が容易

－柔軟性

・OS によって強制されたコンパートメント単位のポリシー設定

・定義ルールによるコンパートメント間の通信設定

－アプリケーション互換性

・アプリケーション側の修正なし（透過性）

・パーティショニング、仮想化技術との統合

○その他のアクセス制御機能

- HP-UX11i 基本セキュリティ［プレゼン］

◆OS 内部処理のアノマリー検出システム IDS for kernel

－対不正アクセス

◆Stack buffer overflow protection

－対バッファオーバーフロー攻撃

・アプリケーションの修正不要

・正当なアプリケーションに影響を及ぼさないため、アプリケーション毎の適用・非適用の選択が可能（ゾーン・バイパス機能）

◆HP-UX Install Time Security

－OS インストール時に以下の４種類のセキュリティレベルを選択

・Tools only（Bastille、SSH、Security Patch Check、IPFilter のインストールのみ）

・Host（約 50 の host ベースのロックダウン）

・Managed DMZ（いくつかのセキュアなプロトコルのみを接続）

・DMZ（SSH 以外のコネクションをブロック）

◆HP-UX Bastille

－ホストのセキュリティ要塞化（各種設定変更の支援）

・従来ホワイトペーパ等で提供していた要塞（bastion）ホスト構築ノウハウを手軽かつ確実に実践することを支援

◆HP-UX IPfilter

－DMZ（DeMilitarized Zone）の構築、パケットフィルタリング

◆HP-UX Secure Shell

－対パスワード盗聴

◆HP-UX IPSec

－対なりすまし

- Secure Resource Partitions（SRP）［プレゼン］

◆Security Containment とリソース制御

（PRM（Process Resource Manager）＋WLM（WorkLoad Manager）を統合）

－アプリケーションの SLA（Service Level Agreement）に従った管理

－コンソリデーションによる TCO の削減

◆Resource Entitlement をコンパートメント上のレイヤに構成（CPU、メモリ、I/O 使用率）

2. 運用上の操作性

○GUI ベースの操作に関する特徴

- System Insight Manager の提供 [プレゼン]

◆Web ベース統合監理ツール

－複数サーバの一括管理

・すべての HP サーバをサポート

・障害、システム設定の一括管理

－ブラウザベースのリモート管理

・HP-UX、Windows、Linux 上で動作

－役割ベース認証機能

・OS の認証技術を使用（PAM により、LDAP、Kerberos、NTLM 等に対応可能）

・Restricted SAM での RBAC の考え方を継承

－プラグインによるツールやアプリケーションの拡張に対応

○複数サーバ群の一元管理に関する支援ツール

- OpenView SelectAccess との連携（Identity Management Integration）[補足]
  - ユーザ情報、アクセス権限情報を SelectAccess の LDAP 上で一元管理できる
  - OS へのアクセスの監査ログを SelectAccess の AuditServer でセキュアに（改竄防止）管理できる

3. 支援ツールの提供状況

○ポリシー設定・管理に関する支援ツール

- System Insight Manager（上述）[プレゼン]

○その他の支援ツール

- Process Resource Manager（PRM）[プレゼン]

◆リソース管理ツール

- Workload Manager（WLM）[プレゼン]

◆サービス品質に基づいた動的リソース制御ツール

- セキュリティパッチチェックツール [プレゼン]

◆セキュリティパッチの配布チェック、導入支援

- Serviceguard [プレゼン]

◆高可用性ツール（HA クラスタ製品）

4. サポート体制

○標準でのサポート

- 長期サポート [プレゼン]

◆市場初出荷より最低 10 年のサポートライフ

○有償サポート

- 教育サービス [プレゼン]

◆「セキュリティ管理者のための HP-UX11i システムセキュリティ」コース
－セキュリティの基本概念の紹介を省き、HP-UX 11i が提供するセキュリティの機能を中心に紹介する実践的なもの（実習を含む）
－運用管理者、技術サポート担当者、サーバ構築コンサルティング担当者向け
－HP-UX IPFilter、HIDS、Bastille、SSH、高信頼性モード、JFS ACL、Install Time Security 等

5. ドキュメントの整備状況

○OS のセキュリティ機能に関する White Paper 等

- ホワイトペーパ [プレゼン, Web]

◆ホワイトペーパ全体（日本語）
http://www.hp.com/jp/hpux
◆ホワイトペーパ全体（英語）
http://www.hp.com/go/hpux
◆ホワイトペーパ一覧（日本語）
http://h50146.www5.hp.com/products/software/oe/hpux/developer/document/
◆OS（日本語、一覧）
http://h50146.www5.hp.com/products/software/oe/hpux/developer/document/oe.html

◆ネットワーク&セキュリティ（日本語、一覧）
http://h50146.www5.hp.com/products/software/oe/hpux/developer/document/network.html
－HP-UX のネットワークセキュリティ機能 HP-UX 11i v1 および 11i v2
－HP-UX 11i システムセキュリティ
－HP-UX HIDS（Host Intrusion Detection System）ホスト型侵入検知システム
－stack buffer overflow protection in HP-UX 11i
◆サーバ仮想化/パーティショニング（日本語、一覧）
http://h50146.www5.hp.com/products/software/oe/hpux/developer/document/partition.html
－HP Integrity VM (Virtual Machines）の紹介
－HP-UX Workload Manager による Virtual Partitions の管理
－HP-UX 11i v2 パーティションシステムにおける HP ServiceGuard クラスタ構成
◆HP-UX のネットワーク セキュリティ機能 HP-UX 11i v1 および 11i v2（日本語）
http://www.jpn.hp.com/products/software/oe/hpux/developer/document/pdfs/PDFHS04007-02.pdf
◆HP-UX 11i システムセキュリティ（日本語）
http://h50146.www5.hp.com/products/software/oe/hpux/developer/document/pdfs/PDFHS03-010-01.pdf
◆HP-UX ネットワークセキュリティ（日本語）
http://h50146.www5.hp.com/products/software/oe/hpux/developer/document/pdfs/jhs04036-01.pdf
◆HP-UX Role-Based Access Control による vPars の保護（日本語）
http://h50146.www5.hp.com/products/software/oe/hpux/developer/document/pdfs/PDFHS05033-01.pdf
◆Securing Virtual Partitions with HP-UX Role-Based Access Control（英語）
http://docs.hp.com/en/6771/rbac.vpars.ed400.pdf

○その他のドキュメント

- マニュアル・テクニカルドキュメント [プレゼン, 補足]

◆ドキュメント全体（日本語、一覧）
http://docs.hp.com/ja
◆HP-UX Technical documentation（一覧、英語）
http://docs.hp.com
◆HP-UX システム／ワークグループの管理
（第 8 章 システム管理：システムの安全運用の管理）
http://docs.hp.com/ja/5990-8173/index.html
◆HP-UX11i Security（英語）
http://www.hp.com/products1/unix/operating/security/
◆HP Systems Insight Manager（英語）
http://h18004.www1.hp.com/products/servers/management/hpsim/index.html
◆Internet and Security Solutions（英語）
http://docs.hp.com/en/internet.html
◆Network and Systems Management（英語）
http://docs.hp.com/en/netsys.html

- 解説資料 [Web]

◆HP-UX における役割ベースのアクセス制御
http://h50146.www5.hp.com/products/software/oe/hpux/developer/document/pdfs/PDF

HS05010-01.pdf

◆「だれもが root」を解消する Security Containment（前編）（無料会員制）
http://h50146.www5.hp.com/products/software/oe/hpux/developer/column/sc_01/

6. アプリケーションのユースケース

- Apache による Web サーバ利用あり［プレゼン]。

7. アプリケーションと OS の連携状況

○アプリケーションの動作

- Security Containment 機能の透過性により、アプリケーション側での修正は不要［プレゼン]。

8. 導入実績

- 国内 UNIX 市場シェアは 10 四半期連続 1 位［プレゼン]

9. Common Criteria 等の認証取得

○Common Criteria への対応（予定も含む）

- Common Criteria 認証取得について［プレゼン、補足]
  - ◆ CAPP-EAL4 認定中（HP-UX 11i v2 ）
  - ◆ CAPP-EAL4 取得済（HP-UX 11i v1 ）

10. その他

○認証機能との連携

- PAM/NSS [プレゼン]

  ◆過去の認証システムとも統合可能な認証フレームワークの提供

- Netscape Directory Server および LDAP-UX 統合機能［プレゼン、補足]

  ◆管理者にとって使いやすい一元管理機能の提供

  ※ Netscape Directory Server は Version 7 より Red Hat Directory Server へ名称変更

- HP-UX Kerberus V5 Server/Client [プレゼン]

  ◆ユーザにとって使いやすいシングルサインオン環境の提供

（3）Compartment Guard for Linux

1. OS のアクセス制御機能の特徴

○セキュア OS の特徴（強制アクセス制御、最少特権）に関するアクセス制御機能

- privilege ガード機構［プレゼン］

  ◆各種ガード機構の管理権限を以下のように守る機構

  －最少特権

  －Trusted Chain

  Linux 標準の CAPABILITY によって実現

- アプライアンス・プロテクション機構［プレゼン］

  ◆システム管理者がルール変更をできないようにする機構

  →ユーザ毎に提供する専用ツールで作成した署名付きルールファイルだけをシステムに適用

  ・アプライアンス製品ベンダ向け

  ・アプリケーションソフトベンダ向け

  ・システム管理者向け（操作制限端末の提供）

○その他のアクセス制御機能

- コンテインメント機構［プレゼン］

  ◆すべてのプロセスをコンパートメントという区画に閉じこめる機構

- コミュニケーションガード機構［プレゼン］

  ◆コンパートメント間、あるいはコンパートメントとネットワークの通信を制限する機構

- ファイルガード機構［プレゼン］

  ◆各コンパートメントから、ファイルシステムに対するアクセスを制限する機構

- sticky ガード機構［プレゼン］

  ◆プロセスの sticky ビットを無効化することのできる機構

- signal ガード機構［プレゼン］

◆プロセスに対する signal 送信を無効化することのできる機構
→重要な監視デーモンなど、他のプロセスを kill できなくすることが可能

- モジュールロード・ガード機構［プレゼン］

◆Linux kernel のロードを制限することのできる機構

- イベントログ機構［プレゼン］

◆ルールの許可・不許可などのログを記録する機構

- アラーム機構［プレゼン］

◆特定のイベントに対して、自動的にアクションをする機構

- pass through モード［プレゼン］

◆コミュニケーションガード機構やファイルガード機構などのガード機構のアクセス制限を内部処理しながら、アクセスの抑止だけを解除するモード

2. 運用上の操作性

- 問題箇所の切り分けが可能であるなど、コンセプトで運用管理面に配慮［プレゼン］
- Red Hat Linux/Enterprise Linux 上に構築［プレゼン］

3. 支援ツールの提供状況

○ポリシー設定・管理に関する支援ツール

- ルール自動作成機能（Version3.0）［プレゼン］

◆ターゲットアプリケーションの起動・操作・停止を通じて以下のルールを自動生成
①ファイルガードルール初期作成
②コミュニケーションガードルール初期作成
③ファイル／コミュニケーションガードルール微調整
（ルールの完全自動生成は難しい）

4. サポート体制

○リリースポリシー

- バージョンアップセーフポリシー [プレゼン]

  ◆Compartment Guard for Linux のバージョンアップをする場合に、現行システムの設定情報を全て継承することを将来的に約束

○標準でのサポート

- サポートにおける特長 [プレゼン]

  ◆自社開発製品のため自社でサポート可能

  ◆サポート不要を目標に設計されたもの

○リアクティブサポート

- サポートプラス [Web]

  ◆ハードウェアオンサイト 4 時間対応：標準時間

  ◆ソフトウェアサポート：標準時間

  ◆ソフトウェアアップデート

- サポートプラス 24 [Web]

  ◆ハードウェアオンサイト 4 時間対応：24×7

  ◆ソフトウェアサポート：24×7

  ◆ソフトウェアアップデート

○プロアクティブサポート

- プロアクティブ 24 [Web]

  ◆アカウント管理

  ◆ハードウェアオンサイト 4 時間対応：24×7

  ◆ソフトウェアサポート：24×7

  ◆ソフトウェアアップデート

- クリティカルサービス [Web]

  ◆アカウント管理

  ◆予防サービス

  ◆変更管理

  ◆ハードウェアオンサイトプレミアム

◆ソフトウェアサポート：24×7

◆ソフトウェアアップデート

5. ドキュメントの整備状況

○各種ドキュメント

- ドキュメントにおける特長

  ◆国産製品のため、マニュアルは日本語で記述されている［プレゼン］

  ◆オンラインのコマンドマニュアルは英語で記述、管理ガイドやチュートリアルは日本語で記述［Web］
  http://www1.jpn.hp.com/solutions/infrastructure/security/hpcg/faq.html

6. アプリケーションのユースケース

（資料なし）

7. アプリケーションと OS の連携状況

（資料なし）

8. 導入実績

（資料なし）

9. Common Criteria 等の認証取得

（資料なし）

10. その他

- 国産製品［プレゼン］

（4）PitBull（LX / Foundation）

1. OS のアクセス制御機能の特徴

○PitBull **ファミリーの特徴**

- 標準 OS へのアドオン方式での提供 [プレゼン]

  ◆標準 OS の知識だけでは攻撃できない

  ◆標準 OS 用アプリケーションがそのまま利用可能

  ◆既存のシステムに追加で導入可能

  ◆システム構築時は PitBull を導入するまではセキュア OS に関する知識が不要

- マルチプラットフォーム対応[プレゼン]

  ◆マルチプラットフォームで同一ポリシーを適用可能

  ◆Solaris / AIX / Linux(予定)【Foundation Suite】

  ◆Solaris / AIX / Linux【LX】

  ◆Solaris / AIX / HP-UX / Linux / Windows Server 2000/2003【Protector Plus】

○**セキュア** OS **の特徴（強制アクセス制御、最少特権）に関するアクセス制御機能**

- アクセス制御の方式 [プレゼン]

  ◆MAC／MIC（Mandatory Integrity Control）【Foundation Suite】

  ◆独自方式（DBAC：Domain Based Access Control）【LX】

  ◆独自方式／MAC【Protector Plus】

- 強制アクセス制御（MAC）【Foundation Suite】[プレゼン]

  ◆ファイルに対する強制アクセス制御

  －MLOSPP 準拠：Bell-LaPadula モデル

  －読み出し、書き込み、実行のアクセスを制御

  －システムが可能なアクセスを強要（システム管理者の設定に従う）

  －ファイル所有者は MAC 設定を変更できない

  －ファイル所有者は他者にアクセスを提供できない

  ◆ネットワークに対する強制アクセス制御

  －ファイルへの強制アクセス制御をネットワークに拡張

－システムが可能なネットワークアクセスを強要（システム管理者の設定に従う）
－IP パケット作成者は MAC 設定を変更できない
－アプリケーションは MAC 設定外のアクセスやアクセスの提供ができない
－カーネルレベルで強制 → 回避不可能

- 強制インテグリティ制御（MIC）【Foundation Suite】[プレゼン]

◆MLOSPP 準拠：Biba モデル
－IL (Integrity Label)の上下関係でアクセスを制御
・No write up
・No read down

- ドメインベースアクセス制御（DBAC）【LX】[プレゼン]

◆ドメインセット：読み出し、書き込み、実行の 3 種類

◆ドメインベースのファイルに対するアクセス制御
－MAC を侵入防止専用に改良
・機密区分(Classification)による上下関係を持たない
・読み出し、書き込み、実行の制御を自由に設定可能
◇ドメイン　コンパートメント
－システムが可能なアクセスを強要（システム管理者の設定に従う）
－ファイル所有者は DBAC 設定を変更できない
－ファイル所有者は他者にアクセスを提供できない
－カーネルレベルで強制 →回避不可能
－強制可能なセキュリティポリシー
・アプリケーションが｛読み込める、書き込める、実行できる｝ファイル

◆ドメインベースのネットワークに対するアクセス制御
－ドメイン・ファイル・アクセス制御をネットワークに拡張
－システムが可能なネットワークアクセスを強要（システム管理者の設定に従う）
－IP パケット作成者は DBAC 設定を変更できない
－アプリケーションは DBAC 設定外のアクセスやアクセスの提供ができない
－カーネルレベルで強制 →回避不可能
－強制可能なセキュリティポリシー

・アプリケーションが｛受信できる、送出できる｝IP パケット

- 最小特権【Foundation Suite】[プレゼン]

◆80 種類を越える特権が利用可能

◆特権の提供方法

－最小特権(Least Privilege)：最小限の必要な特権のみを許可

－特権ブラケッティング(Privilege Bracketing)：特権が必要な時にのみ与える

－特権継承禁止：子プロセス起動時に、特権を全て剥奪

- 最小特権【LX】[プレゼン]

◆プロセス・セキュリティ属性

－変更できないプロセスの属性として、以下の分類毎に root 特権の使用を禁止できる

1. ファイルシステム操作
2. システム再起動
3. DAC 制限のバイパス
4. ユーザ ID、グループ ID の変更
5. 特権 TCP/UDP ポートのバインド
6. その他システム操作

－実行ファイルの起動時にプロセスに設定される

－設定後は制限を解除することは root でも不可能

- Dual Control 機能【Foundation Suite】[プレゼン]

◆二人がパスワードを入力しないとログインできない

○その他のアクセス制御機能

- ユーザ認証【Foundation Suite】[プレゼン]

◆ユーザ単位でのセキュリティレベルの設定

◆ログインするネットワーク毎に異なったセキュリティレベルを設定

（例：管理用ネットワークからは管理者ユーザ ID が利用可能、インターネットからは無効、等）

◆PAM 機能により、ログイン・ユーザのラベルをプロセスに付加可能（TELNET, FTP, etc.）

- ユーザ認証【LX】[プレゼン]

◆ユーザ単位での属性の設定

◆同じユーザがコンソールもしくはネットワーク経由でログインする際にそれぞれ異なった属性を設定

◆PAM に対応するログイン機構を使用した属性の設定

－PAM モジュールは PAM の機能を必要とするアプリケーションのみに追加可能

- システム監査機能［プレゼン］

◆イベントログの取得【Foundation Suite】

－システムが選択された監査イベントを記録（例:ログインの失敗、ファイル読み出しの失敗）

－失敗、成功、もしくは両方を記録

－監査レコード：イベント、タイムスタンプ、ユーザ情報(ID, SL, etc.)

◆インテグリティ検査【Foundation Suite、LX】

－インテグリティデータベースにファイル属性を記録

・パーミッションビット、SL、特権、内容のハッシュ、etc.

・指定されたファイルのみ

－インテグリティ検査

・記録された属性と実際の属性を比較

・不一致があれば警告

－ラベル情報のバックアップ保存にも利用可能

- その他の機能【Foundation Suite】[プレゼン]

◆セキュリティゲート

－相互にアクセスが不可能な SL を持つプロセス間の通信を安全に行うゲートウェイプログラム

◆プログラムラウンチャ

－管理者が指定した SL で、安全にプログラムを実行する機能

◆Apache CGI ラウンチャ

－CGI を管理者が指定した Apache 本体プロセスとは異なる SL で起動する機能

◆Web ユーザ認証による HTTP 通信のアクセス制御

－ユーザ認証結果に応じて、異なった SL で動作する Web サーバに接続させる

2. 運用上の操作性

- 操作は telnet 等の CUI（コマンドラインインタフェース）を使いこなせることが前提［プレゼン］。
- マニュアル：

  ◆"PitBull Foundation and Foundation Suite Administration Guide"

  （言語：英語／日本語、媒体：PDF／印刷）

  http://www.argus-systems.com/public/docs/AIX/foundation_suite_admin.pdf

  （英語版のみ公開）

3. 支援ツールの提供状況

○各種支援ツール

- 市販製品（COTS）アプリケーションを新しい環境で守るための統合ツールの提供［Web］

  http://www.pitbull.jp/product/overview/pitbull/0.html

4. サポート体制

○サポート体制

- リセラーチャネルによるエスカレーションフロー［プレゼン］

  ◆Argus←Infocom←｛CRC ソリューション、Hucom、日本高信頼システム｝←（二次リセラー）
- PitBull の販売パートナーであるマスターリセラー各社が独自のサポートメニューを用意［補足］

○標準でのサポート

- 標準製品保守［プレゼン］

  ◆平日 平日 9 時～5 時 ヘルプデスク

  ◆修正モジュールの提供

- 過去のバージョンのサポート［プレゼン］

  ◆ベースの OS（AIX, Solaris, Linux）のサポート期間と一致。

  ◆ベースの OS（AIX, Solaris, Linux）のバージョンアップ頻度に完全には対応しない。

○有償でのサポート

- 拡張保守［プレゼン］

  ◆オンサイトサポート

  ◆24 時間 365 日サポート

○教育コース

- PitBull Foundation Suite 初級管理者トレーニング［プレゼン］
- PitBull Foundation Suite 上級管理者トレーニング［プレゼン］
- PitBull LX 初級管理者トレーニング［プレゼン］

5. ドキュメントの整備状況

（ドキュメント中、日本語版ならびに印刷物は基本的に全て有償）

○OS のセキュリティ機能に関する White Paper **等**

- 各種ドキュメント［補足］

  ◆PitBull Foundation Suite **マニュアル**
  http://www.argus-systems.com/support/documentation/docs_fd_aix.shtml
  （英語版のみ公開）
  －Installation Guide **インストール・ガイド（言語**: **英語/日本語、媒体**: PDF / **印刷）**
  －Security Features User's Guide？ **セキュリティ機能ガイド（言語：英語/日本語、媒体**: PDF / **印刷）**
  －Trusted Facility Manual？ **セキュリティ運用ガイド（言語**: **英語/日本語､媒体**: PDF / **印刷）**
  －Suite Administration Guide？ **アプリケーション管理者ガイド（言語：英語/日本語、媒体**: PDF / **印刷）**
  －MAN Pages？ **オンライン・コマンド・リファレンス（言語：英語、媒体**: UNIX roff - MAN **形式）**
  －Security Features Programmer's Guide？ **セキュリティ機能プログラミングガイド（言語**: **英語、媒体**: PDF**）**
  －MITRE 10649 (1 of 2) - Compartmented Mode Workstation Labeling**（言語**: **英語、媒体**: PDF**）**
  －MITRE 10649 (2 of 2) - Encoding Specification Error Messages **（言語**: **英語、媒体**: PDF**）**
  －PitBull Foundation **入門 （言語**: **英語/日本語、媒体**: PDF**）**
  http://www.argus-systems.com/public/docs/pitbull_gettingstarted.pdf (**英語版のみ未公開**)

  ◆PitBull LX **マニュアル**
  http://www.argus-systems.com/support/documentation/docs_lx_sol.shtml
  （英語版のみ公開）

－Installation Guide **インストール・ガイド（言語**: **英語/日本語、媒体**: PDF / **印刷）**
－Administration Guide？ **管理者ガイド（言語**: **英語/日本語、媒体**: PDF / **印刷）**

◆Knowledge Base（**言語**: **英語、媒体**: **オンライン**-HTML）
http://www.argus-systems.com/support/knowledge_base/lx/index.shtml

6. アプリケーションのユースケース

- 対応アプリケーション［補足］

  http://www.argus-systems.com/public/docs/support_applications.pdf

7. アプリケーションと OS の連携状況

○アプリケーションにおける OS のセキュリティ機能を用いたアクセス制御

（なし）

○アプリケーションの動作

- 標準 UNIX 完全互換［プレゼン］。
  ◆市販アプリケーションが無変更で動作【Foundation Suite、LX】

8. 導入実績

- 国内外で、政府系機関から、金融機関、通信事業者、一般企業まで、幅広くかつ多数の実績［プレゼン、補足］

  http://www.pitbull.jp/product/case_studies/

  http://www.argus-systems.com/product/casestudies.shtml

  オンラインバンキング 金融（銀行） クレディスイス銀行

  B2B 決済サービス EC サービス A 社（米国）

  Web ホスティング IDC B 社（米国）

  情報ゲートウェイ 政府機関 米国中央情報局（CIA）

  マルチレベル機密情報サーバ 政府機関 米国中央情報局（CIA）

  PKI サービス 電子認証サービス TC Trust Center（独）

  教室予約システム 京都大学

  インターネットホームページ C 社（日本）

  オンラインバンキング - Finanz-IT（独）

9. Common Criteria 等の認証取得

○Common Criteria への対応（予定も含む）

- Common Criteria 認証取得状況［プレゼン］

◆MLOSPP（暗号実装を除く）【Foundation Suite】

－米国 IBM と Argus が共同で認証申請中【Foundation Suite】

・PitBull Foundation and Foundation Suite 5.0 for IBM AIX 5L Version 5.2

・第一段階：LSPP (EAL3) → 2006 年前半を予定

・第二段階：MLOSPP (EAL4+)

○その他の認証

- オレンジブック［プレゼン］

◆B1 準拠【Foundation Suite】

◆B1 に匹敵するが準拠せず【LX】

◆MAC【Protector Plus】

10. その他

○今後の予定

- PitBull Foundation Suite 次バージョン［プレゼン］

◆X-Window MLS 対応版

- PitBull LX 次バージョン(Coming Soon) [プレゼン]

◆Linux 版でもログ出力をサポート

（5）Solaris 10 / Trusted Solaris

1. OS のアクセス制御機能の特徴

○セキュア OS の特徴（強制アクセス制御、最少特権）に関するアクセス制御機能

- トラステッド OS の基本機能【Trusted Solaris】[プレゼン]

◆デフォルト否定（明示的な許可がなければ無効となる）

・セキュリティの方針に応じて許可されたアクセス以外は全て拒否

・セキュリティ方針に応じて許可された権限以外の権限は無効

→セキュリティ方針に従ったシステムの構築が可能

→万が一の場合に備えたセキュリティ対策ができる

→既知だけでなく未知の手段による不正の抑止

◆マルチレベル（機密性/従属制に従った情報に対するクラス）

・サブジェクト／オブジェクトの機密ラベル

◇機密分類およびその関係（機密＞重要＞社内＞公開）

◇コンパートメントおよびその関係

◇実際の機密ラベルおよびその関係

→情報本来の価値に応じたアクセス制御をすることができる

→セキュリティ方針を直接的に導入することができる

◆セキュリティ機構（監視／制限／記録）の強化

・セキュリティを根本から考慮した実装

◇米国国防総省基準に準拠するセキュリティを実現

・監視／制御の体制を強化

◇信頼できないものを実行することができない

・特権と役割を導入

◇管理者の役割を複数に分割することによる危機分散（2 man rule）

◇予め許可されなければ特権による承認が得られない

→内部犯罪や誤用の防止

→トロイの木馬（相手の裏をかく不正行為）の抑止

- 特権（Privileges）に関する Process Rights Management【Solaris 10】[プレゼン]

◆権利プロファイルによる“役割ベースのアクセス制御”の実現

◆従来のスーパーユーザを排除し、“最小特権”の実現

－UID による権利の委譲（suser ポリシー）

・UID＝0 の権限の無効化

・微細な特権への置き換え

◆特権の権利プロファイルへの実装、特権セットのプロセスへの実装

－特権による権利の配布（solaris ポリシー）

－以下の 4 種類のセットを用いた特権のモデルを実装

・実効セット（E：Effective Set）

・許可セット（P：Permitted Set）

・継承セット（I：Inheritable Set）

・上限セット（L：Limit Set）

- Solaris 10 におけるアプローチ【Solaris 10】[プレゼン]

◆Trusted Solaris の機能を“Trusted Extension”として提供予定

－Layered Product として提供予定（Solaris10 セキュリティの拡張機能として提供）

－マルチレベル・セキュリティの提供

・マルチレベルデスクトップ環境、マルチレベルネットワーク等

－ハードウェア、ソフトウェア、パッチのフルサポート

・すべてのパッチを適用可能

・Solaris 上のアプリケーションの動作保証

・新しいハードウェアへの対応の遅延がない

○その他のアクセス制御機能

- 仮想化（Zones）に関する Solaris Container【Solaris 10】[プレゼン]

◆仮想実行環境でのサービスの実行による“サーバの要塞化”の実現

◆仮想実行環境におけるセキュリティ境界

－プロセス（Processes）

・特定の特権の取得やシステムコールを制限

・ゾーン内のプロセスのみが参照可能（/proc の仮想化）

－デバイス（Devices）

・ドライバの追加／削除、カーネルモジュールのロード、アンロードは不可

・「安全な」疑似デバイスの一部のみが参照可能（/dev の独自構成）

－ファイルシステム（File System）

・独自のルート（/）とデバイス（/dev）の割当

・共有するファイルシステムはグローバルゾーンからリードオンリーで継承

－ネットワーキング（Networking）

・独自の IP ポート空間に対して IP v4/v6 のアドレスが割り当てられる

・ゾーンへのトラフィックのみが取得可能

- 暗号化フレームワーク【Solaris 10】[プレゼン]

◆暗号化フレームワークにより“安全で信頼できるネットワークコネクション”の実現

－一元的な暗号化サービスのフレームワーク

－暗号化サービス提供者（Provider）のプラグイン

－暗号化サービス利用者（Consumer)のプラグイン

- Secure Deployment [プレゼン]

◆Service Management Facility (SMF)

－暗号化サービス利用者（Consumer)のプラグイン

◆Basic Audit Report Tool (BART)

－ファイルレベル(サイズ/所有者/MD5 checksum/等)の完全性確認

- Access Control [プレゼン、補足]

◆Solaris IP Filter

－パケットフィルタリング機能

- Auditing [プレゼン、補足]

◆Solaris Auditing

－OS 監査機能

2. 運用上の操作性

○GUI ベースの操作に関する特徴

- ユーザインタフェースとして、以下の GUI 操作環境が利用可能［プレゼン]

◆Sun Java Desktop【Solaris 10】

◆Common Desktop Environment【Trusted Solaris】

○異なるセキュリティレベルのネットワーク環境の操作

- Ultra-Thin Client Front-End【Trusted Solaris】［プレゼン］

  ◆ステートレスな Sun Ray 端末を用いることで、Trusted Solaris ベースのシステムのフロントエンドとして一つの端末上で異なるセキュリティレベルのネットワーク環境を実現

3. 支援ツールの提供状況

○ポリシー設定・管理に関する支援ツール

- GUI ベースの管理ツール［プレゼン］

  ◆Solaris Management Console

- CUI ベースの管理ツール［プレゼン］

  ◆表示：roles, profiles, auths, pppriv, pattr, plabel, getpriv

  ◆設定：roleadd, roledel, rolemod, useradd, userdel, usermod, smrole, smuser, smprofile, smexec, setfpriv

○その他の支援ツール

- Solaris Enterprise System【Solaris 10】［Web］

  ◆OS と一体での提供の方向

  http://jp.sun.com/company/Press/release/2005/1201.html

4. サポート体制

○クライアントソリューションデリバリ［プレゼン］

以下の各プロセスについて一貫したソリューションを提供

- アセスメント
- パイロット
- システム設計
- システム構築

○エデュケーションサービス

- トレーニングコース［プレゼン］
- Sun 認定資格［プレゼン］

○製品サポート

- 基本販売期間終了後 5 年（製品の 3 世代目の販売にて終了）［プレゼン］

5. ドキュメントの整備状況

○各種ドキュメント（いずれも日本語）

- ユーザ向けドキュメント【Solaris 10】[プレゼン]

◆Solaris 10 User Collection
－マニュアルの概要
－ユーザズガイド（上級編）
－日本語環境ユーザズガイド、入力方式

◆Java Desktop System Release 3 Solaris 10 Collection
－ご使用にあたって
－ユーザズガイド
－システム管理
－問題の解決方法

◆Java Desktop System Configuration Manager Release 1.1
－ご使用にあたって
－管理ガイド
－開発者ガイド
－インストールガイド

◆Solaris 10 Common Desktop Environment User Collection
－ユーザズガイド
－上級ユーザおよびシステム管理者ガイド

- 管理者向けドキュメント【Solaris 10】[プレゼン]

◆Solaris 10 Release and Installation Collection
－ご利用にあたって、概要、パッケージリスト
－インストールガイド（基本編、カスタム JumpStart.／上級編、ネットワークインストール、Solaris フラッシュアーカイブの作成とインストール、Solaris Live Update のアップデートの計画）
－Sun ハードウェアマニュアル
－ハードウェア互換リスト

◆Solaris 10 International Language Support Collection
－国際化対応言語環境の利用ガイド

◆Solaris 10 on Sun Hardware Collection

◆Solaris 10 System Administration Collection
－Solaris のシステム管理（基本編、上級編、Solaris コンテナ：資源管理と Solaris ゾーン、セキュリティサービス、ネットワークサービス、IP サービス、ネーミングとディ

レクトリサービス：DNS,NIS,LDAP 編、ネーミングとディレクトリサービス：NIS+ 編、デバイスとファイルシステム、システム管理エージェント）
－Solaris のスマートカードの管理
－Solaris のボリュームマネージャの管理
－Solaris のカーネルのチューンアップ・リファレンスマニュアル
－フォントの管理

- 開発者向けドキュメント【Solaris 10】[プレゼン]

◆Solaris 10 Software Developer Collection
－Solaris64 ビット開発ガイド
－Solaris DHCP サービス開発ガイド
－Solaris 動的トレースガイド
－Solaris モジュラーデバッガ
－Solaris セキュリティサービス開発ガイド
－Solaris WBEM 開発ガイド
－Solaris X Window System 開発ガイド
－ToolTalk ユーザズガイド
－JDK 開発ガイド（Solaris 編）
－リンカーとライブラリ
－マルチスレッドのプログラミング
－ONC+開発ガイド
－プログラミングインタフェース

- リファレンスマニュアル【Solaris 10】[プレゼン]

◆Solaris 10 Reference Manual Collection
－SunOS リファレンスマニュアル（ユーザコマンド、システム管理コマンド、システムコール、基本ライブラリ関数、Curses ライブラリ関数、拡張ライブラリ関数、ライブラリインタフェースおよびヘッダ、ファイル形式、標準、環境、マクロ、デバイスとネットワークインタフェース、DDI/DKI カーネル関数）
－JFP リファレンスマニュアル（ユーザコマンド、システム管理コマンド、C ライブラリ関数、ファイル形式、標準、環境、マクロ、デバイスとネットワークインタフェース）

6. アプリケーションのユースケース

（なし）

7. アプリケーションと OS の連携状況

○OS のセキュリティ機能を利用したアプリケーション

- Solaris Enterprise System [Web]

◆PostgreSQL を OS と一体での提供の方向
http://jp.sun.com/company/Press/release/2005/1201.html

○アプリケーションの動作

- バイナリ互換性［プレゼン］

  ◆Solaris2.6 以降で保証（過去 7 年間）

- ソース互換性［プレゼン］

  ◆SPARC と x86/AMD64 の双方で保証

8. 導入実績

- 米国ディフェンス向けソリューション提案構築［プレゼン、補足］

  ◆顧客との協業

  ◆システム刷新検証

  ◆アーキテクチャ確立

  ◆付加価値創造

  －SPAWAR (Space and Naval Warfare Systems Command) [Web]
  http://www.sun.com/solutions/documents/success-stories/snap_gov_spawar_bb.xml

  －JICPAC (Joint Intelligence Center of the Pacific) [Web]
  http://www.sun.com/solutions/documents/success-stories/snap_gov_jicpac_bb.xml

  －U.S. Army TACOM [Web]
  http://www.maximsys.com/aaronsworkarea/2005news.php?var=news

9. Common Criteria 等の認証取得

○Common Criteria への対応（予定も含む）

- 認証取得について

  ◆Solaris 10：EAL4+（評価中）［プレゼン］

  ◆Trusted Solaris 8：EAL4+/CAPP,LSPP,RBACPP［プレゼン］

- プロテクションプロファイル（PP）［プレゼン］

  ◆CAPP（Controlled Access Protection Profile）

  －TCSEC C2 相当、既存のオープンシステム OS の標準的レベル。一般的なログイン認証、アクセス制御、および監査

  ◆RBPP（Role-Based Access Protection Profile）

  －役割による管理を可能とする、中大規模システム求められるレベル。ホストで行われて

いる業務・事務システムなどでは必須となる権限の管理

◆LSPP（Role-Based Access Protection Profile）

－ラベルによる制御を可能とする、防衛システムなどで求められるレベル。必ずしも必要とされないが、機密度の異なるシステム連携では有効

- セキュリティターゲット（ST）[補足]

◆Trusted Solaris 8

http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=152&id=111

◆Solaris 8

http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=152&id=267

◆Solaris 9

http://www.cse-cst.gc.ca/services/ccs/solaris9-e.html

◆Solaris 10

現在評価中

10. その他

- オープンソース化 [プレゼン]

◆Solaris10 については、開発環境、JAVA 関連を OS と組み合わせて「Solaris Enterprise System」として全体をオープンソース化の方向［Web］

http://jp.sun.com/company/Press/release/2005/1201.html

◆Trusted Solaris 10 のオープンソース化は未定（可能性は低い）［プレゼン］

（6）AIX 5L

1. OS のアクセス制御機能の特徴

○セキュア OS の特徴（強制アクセス制御、最少特権）に関するアクセス制御機能

- 管理ロール [プレゼン]

  ◆root 権限の一部を root 以外に割り当て可能 → システム管理機能の分散付与

  －ロールの種類：ユーザの追加および除去、パスワードの変更、ロールの管理、バックアップおよび復元、バックアップのみ、診断の実行、システム・シャットダウン

  －ロールは階層化可能

- 強制アクセス制御、最少特権については、AIXをベースとする以下のOSにて実現 [プレゼン]

  ◆PitBull Foundation Version 4.0 for AIX 5L for Power

  http://www-03.ibm.com/servers/aix/products/aixos/certifications/

  －LSPP EAL4+

  （TCSEC B1 以上）

○その他のアクセス制御機能

- セキュア・システムの導入オプション [プレゼン]

  AIX 5L 5.2 以降では導入時に、BOS（Base Operating System）機能のオプションとして、以下が選択可能：

  ◆TCB（Trusted Computing Base）

  －トラステッド通信パス／トラステッド・シェル

  －システム保全性検査（tcbck コマンド）

  ◆CC CAPP EAL4+ 準拠モード

  64 ビット・カーネルにて提供され、以下の機能を含む：

  －LVM（論理ボリュームマネージャ）

  －JFS2（拡張ジャーナル・ファイルシステム）

  －CDE インタフェースを備えた X Window システム

  －IP v4（Telnet、FTP、rlogin、rsh/rcp）

  －NFS

- 仮想化機能［プレゼン］

◆Hypervisor による論理パーティション（LPAR: Logical Partitioning）

－一つのハードウェア上で複数 OS イメージの動作が可能

－アクセスは Hypervisor が制御

・LPAR 間アクセス

・リソース（プロセッサ、メモリ、I/O アダプタ）間のアクセス

－LPAR 内のプログラムなどから他の LPAR が所有しているリソースやデータへのアクセスは不可能な設計

◆Advanced POWER Virtualization 機構

－Virtual I/O Server

・Ethernet アダプター共有（SEA）

・SCSI / ファイバーチャネル接続ディスク共有

・AIX 5L V5.3, Linux*パーティションをサポート

－マイクロ・パーティショニング

・複数パーティションでプロセッサを共有

・1/10 プロセッサー・パーティション

・AIX 5L V5.3, Linux*, i5/OS** をサポート

－Partition Load Manager

・AIX 5L V5.2, V5.3 をサポート

・プロセッサとメモリ処理要求を最適化

－HMC(ハードウェア・マネージメント・コンソール)による管理

◆仮想化環境でのセキュリティ認定取得

－Common Criteria, Part 2 & EAL4+

（for IBM LPAR for POWER4 for the IBM pSeries p630, p650 and p690）

http://www-03.ibm.com/servers/aix/products/aixos/certifications/bunde_lpar.html

- アクセス制御機能（任意アクセス制御（DAC)） [プレゼン]

◆拡張 ACL (extended permissions)

－基本 ACL で指定できない部分の個別指定が可能（AIXC ACL タイプ）

◆NFS V4

－JFS2、GPFS にてサポート（AIX NFS4 ACL タイプ）

- インターネット・ポート用の任意アクセス制御（DACinet）[プレゼン]

◆ホスト間での通信に関する、TCP ポートのユーザ・ベース・アクセス制御を提供（AIX 5.2/5.3、CAPP EAL4+）

－宛先システム上の管理者は、宛先ポート、発信元のユーザ ID およびホストに基づいてアクセスを制御

－1024 より上のローカル・ポートの追加の権限を root のみに制限することで、ユーザが既知のポートでサーバを実行するのを防止することが可能

- スタック実行使用不可保護（SED）[プレゼン]

◆バッファオーバーフロー(BOF)攻撃対策

－BOF を通して侵入するアタック・コードの実行をブロック

－システム環境の SED モードと実行可能ファイルの SED フラグにて制御

- 監査機能 [プレゼン]

◆監査対象となるイベント

－サブジェクト（プロセスの作成・削除 等）

－オブジェクト（オブジェクトの作成・削除・オープン・クローズ 等）

－インポート／エクスポート（オブジェクトのインポートまたはエクスポート）

－アカウンタビリティ（ユーザの追加・属性変更、ログイン、ログアウト、認証情報 等）

－一般システム管理（特権の使用、システム構成の変更 等）

－セキュリティ違反（アクセス権の拒否、システムエラー 等）

2. 運用上の操作性

○GUI ベースの操作に関する特徴

- SMIT (System Management Interface Tool) [プレゼン]

◆管理インタフェース

－識別および認証手段(ユーザの構成、パスワード設定、ログイン構成など)

－監査手段(BIN モード審査の構成、監査対象イベントの選択、監査証跡の処理など)

－任意アクセス制御(ファイルシステム・オブジェクト用の許可ビットと ACL、IPC 機構、および TCP ポート)

- Web-based System Manager [プレゼン]

3. 支援ツールの提供状況

○Tivoli Access Manager for Operating Systems [プレゼン, Web]

- 従来の UNIX 管理モデルのセキュリティを補強し、UNIX/Linux 環境で動作するアプリケーションに対する階層的なアクセス管理をサポート**（OS とは別製品、エンジンはカーネルのエクステンション）**

  ◆特権管理者(root)の権限悪用を制御・防止

  －root を含むユーザに対する最小特権原則の強化

  ◆セキュリティ管理者によるセキュリティポリシーの設定・強制が可能

  ◆権限チェックは、su 先のユーザ ID ではなく、ログイン時のユーザ ID にて判断

  ◆強力な監査ログ機能によりアクセスの追跡が容易

  －ログイン時のユーザ ID で追跡可能

  ◆強力な改ざん検知/不正プログラムの実行防止機能

  －改ざんされたプログラムは実行不可能

  ◆統合コンソールから複数システムの管理・制御が可能

4. サポート体制

○標準でのサポート

- インシデント対応体制［プレゼン］

  ◆開発チームと、３層のチェンジチーム（修正コードの開発）による体制

5. ドキュメントの整備状況

○OS のセキュリティ機能に関する White Paper 等

- 仮想環境におけるセキュリティに関する WhitePaper（英語のみ）[補足]

  Virtualization Security and Integrity in the IBM eServer POWER5 Environment

  http://www-03.ibm.com/servers/eserver/pseries/hardware/whitepapers/virtualization.pdf

○マニュアル等

- セキュリティ・マニュアル(HTML/PDF ファイル。英語及び日本語のファイル有り)

  ◆AIX 5L Version 5.3 Security

  http://publib.boulder.ibm.com/infocenter/pseries/index.jsp?topic=/com.ibm.aix.doc/aixbman/security/security-kickoff.htm

◆PDF ファイル

http://publib.boulder.ibm.com/infocenter/pseries/topic/com.ibm.aix.doc/aixbman/security/security.pdf

- AIX/ｐSeries に関するマニュアルポータル

◆pSeries and AIX Information Center

http://publib.boulder.ibm.com/infocenter/pseries/topic/com.ibm.helpweb.doc/welcome.htm

○OS のセキュリティ機能に関する解説ページ

- AIX/ｐSeries に関するセキュリティに関する解説ページ（日本語＋英語資料へのリンク）

http://www-06.ibm.com/jp/servers/eserver/pseries/security/

6. アプリケーションのユースケース

（なし）

7. アプリケーションと OS の連携状況

○アプリケーションの動作

- IBM 製品は動作（代表的製品のみ）[プレゼン]：

WebSphere Application Server

WebSphere MQ

DB2 UDB

DB2 Content Manager

Lotus Domino

Tivoli Storage Manager

Tivoli Access Manager for e-business

Tivoli Access Manager for Operating Systems

Tivoli Identity Manager

- ISV ソリューション/製品 [プレゼン]

http://www-6.ibm.com/jp/servers/eserver/pseries/aix/solutions/

8. 導入実績

- 豊富［プレゼン]。

9. Common Criteria 等の認証取得

○Common Criteria への対応（予定も含む）

- Common Criteria 認証取得状況［プレゼン]

  ◆AIX 5L V5.2
  －CAPP EAL4+ augmented by ALC_FLR.1
  (Life cycle support – Basic Flaw remediation)
  http://niap.nist.gov/cc-scheme/vpl/vpl_type.html#operatingsystem

  ◆AIX 5L V5.3
  －認証取得予定

- セキュリティターゲット［補足、Web]

  IBM AIX 5L for POWER V5.2 Maintenance Level 5200-06 Program Number 5765-E62

  http://www.bsi.bund.de/zertifiz/zert/reporte/0302b.pdf

- AIX をベースにする OS 製品の CC 認証［プレゼン]

  ◆PitBull Foundation Version 4.0 for AIX 5L for Power
  CAPP/EAL 4+，LSPP/EAL 4+
  取得中（http://www-03.ibm.com/servers/aix/products/aixos/certifications/）

○その他の準拠事項

- AIX 5L V5.3 の準拠事項［プレゼン]

  ◆Single UNIX Specification V3 (SUS V3)
  －UNIX 03 認証取得予定

  ◆ISO/IEC 9899:1999 C プログラミング言語の国際標準（略称 C99)

  ◆SUS V3 Realtime Option Group（IEEE Standard 1003.1-2001 の以下オプションから構成：POSIX_ASYNCHRONOUS_IO，POSIX_FSYNC，POSIX_MAPPED_FILES, POSIX_MEMLOCK, POSIX_MEMLOCK_RANGE, POSIX_MEMORY_PROTECTION, POSIX_MESSAGE_PASSING，POSIX_PRIORITY_SCHEDULING, POSIX_REALTIME_SIGNALS，POSIX_SEMAPHORES, POSIX_SHARED_MEMORY_OBJECTS，POSIX_SYNCHRONIZED_IO, POSIX_TIMERS）

◆SUS V3 Realtime Threads Option Group（IEEE Standard 1003.1-2001 の以下オプションから構成：POSIX_THREAD_PRIO_INHERIT, POSIX_THREAD_PRIO_PROTECT, POSIX_THREAD_PRIORITY_SCHEDULING）

◆SUS V3 Advanced Realtime option（IEEE Standard 1003.1-2001 の以下オプションから構成：POSIX_ADVISORY_INFO, POSIX_CLOCK_SELECTION, POSIX_CPUTIME, POSIX_MONOTONIC_CLOCK，POSIX_TIMEOUTS，POSIX_BARRIERS, POSIX_SPIN_LOCKS，POSIX_THREAD_CPUTIME）

10. その他

- 利用者認証フレームワーク［プレゼン］

◆Loadable Authentication Module（LAM）

◆PKI 認証

◆EIM(Enterprise Identity Mapping)サポート

（7）Windows Server 2003

1. OS のアクセス制御機能の特徴

○セキュア OS の特徴（強制アクセス制御、最少特権）に関するアクセス制御機能

- 管理者特権の最小化 [補足]

  ◆Windows Server 2003：Administrator は基本的に全権限を持つ

  ◆Windows Server Vista：管理者グループ（Administrators）も含むすべてのユーザを最小限の特権を持つユーザとして実行

- 特権の分割 [補足]

  ◆特権の分割はデフォルトでは行われていないが、サードパーティのミドルウェア等を利用することで可能

○その他のアクセス制御機能

- ACL（Access Control List）によるアクセス制御 [Web]

  ◆DAC ベース

  ◆オブジェクトに添付される随意アクセス制御リスト（DACL）のコンテンツと、ユーザのグループメンバシップを比較して、必要なアクセス権を持っているかどうかを判断

- 役割ベースのアクセス制御（RBAC）[Web]

  ◆Authorization Manager（承認マネージャ, AuthMan）を用いることでロールに基づいたアクセス制御が可能。ロールや権限は階層的に扱うことができ、アプリケーション管理者がユーザの役割とアクセス許可を管理するための Microsoft 管理コンソール(MMC)が提供される。

  －承認マネージャを使用する多層アプリケーションの役割ベースのアクセス制御
  http://www.microsoft.com/japan/technet/prodtechnol/windowsserver2003/technologies/management/athmanwp.mspx

- アクセス制御の Subject について [補足]

  ◆原則として Windows のアクセス制御の subject は user

  －サードパーティの提供するセキュリティ・ミドルウェアによって process を subject にすることも可能

－強いて言えば、アクセス経路（Interactive, Remote, Terminal, etc...）も subject となることは可能

- アクセス制御の粒度の細かさについて［Web］

◆特殊なアクセス許可において制御可能な項目

－フォルダのスキャン/ファイルの実行
－フォルダの一覧表示/データの読み取り
－属性の読み取り
－拡張属性の読み取り
－ファイルの作成/データの書き込み
－フォルダの作成/データの追加
－属性の書き込み
－拡張属性の書き込み
－サブフォルダとファイルの削除
－削除
－アクセス許可の読み取り
－アクセス許可の変更
－所有権の取得
－同期

2. 運用上の操作性

○GUI ベースの操作に関する特徴

（クライアント PC で広く普及している GUI 操作環境が利用可能）

3. 支援ツールの提供状況

○ポリシー設定・管理に関する支援ツール

- グループポリシー管理ツール［プレゼン］

◆Web サイトでダウンロード提供している Group Policy Management Console をツールとして用いることにより、Active Directory + GPMC で簡易に編集展開が可能
http://www.microsoft.com/japan/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx

（設定の実例として、用途、ロール、要求されるセキュリティレベル別に、ガイダンスを提供）

4. サポート体制

○標準でのサポート

- 製品別サポートページ（日本語）[補足]

  http://support.microsoft.com/select/?target=hub

- Windows Server 2003 サポートページ（日本語）[補足]

  http://support.microsoft.com/ph/3198

○サポートの方針

- 製品のサポート期間 [補足]

  サポート範囲は製品・サービスによって異なるが、Server OS などのビジネスソフトウェアは、最低 10 年間のサポートを基本としている。有償ではあるが、10 年以上のサポート延長も可能。

  http://support.microsoft.com/lifecycle/

  ◆期間中のサポート内容：

  －セキュリティ更新の提供：重大なセキュリティの脆弱性が発見された場合にはサポート期間中は、常に無償でセキュリティ更新を開発・提供

  －修正プログラムの提供：セキュリティ以外の諸問題を修正する更新プログラムの提供。(期間の途中から有償)

  ◆Q&A サポート：製品の利用方法、トラブル解決の窓口とサービスの提供。

  （サービスレベルにより、有償、無償あり）

  ◆サポートの方法は、製品単位に行うものと、包括的にサポートする方法を選択可能

  http://www.microsoft.com/japan/microsoftservices/support/SupCompare.asp

5. ドキュメントの整備状況

○各種ドキュメント（日本語、ただし一部は機械翻訳による提供）

- ドキュメントの整備状況 [プレゼン]

  Windows Server 2003 技術情報 インデックス

http://www.microsoft.com/japan/windowsserver2003/techinfo/overview/articleindex.mspx

- 関連書籍（日本語）[補足]

  『インサイド・ウィンドウズ 第 4 版』（OS の機能・機構・実装に関する技術情報）

  http://www.microsoft.com/japan/info/press/JPN_ViewMsPress.asp?Book_id=1019&list_id=1

  http://www.microsoft.com/japan/info/press/JPN_ViewMsPress.asp?Book_id=1022&list_id=1

6. アプリケーションのユースケース

○対応アプリケーション

- 対応アプリケーション（日本語）[補足]

  Microsoft Windows Server 2003 サポートページ

  http://support.microsoft.com/ph/3198?sid=1494

7. アプリケーションと OS の連携状況

○OS のセキュリティ機能を利用したアプリケーション

- SQL Server における OS の認証システムの利用 [補足]

  SQL Server で Windows 統合認証を利用する場合、SQL Server の認証に OS の認証システムを用い、オブジェクト単位でアクセス権限を設定可能。

  ◆SQL Server が管理するデータベースファイルのアクセス権：OS のアクセス制御
  ◆SQL Server が管理するオブジェクト（テーブル、ビュー等）：OS のアクセス制御
  （Windows 統合認証）または SQL 認証の片方または双方が使用可能
  どちらの方式でも、オブジェクト単位および、各種操作毎に、細かく設定可能。また、RBAC による制御も可能。

8. 導入実績

- 導入実績（Windows Server 導入事例／日本語）[補足]

  http://www.microsoft.com/japan/windowsserversystem/mn20581/default.mspx

- その他公的機関等での導入事例多数 [プレゼン]

9. Common Criteria 等の認証取得

○Common Criteria **への対応（予定も含む）**

- 認証取得状況 [Web]

  ◆EAL4+／CAPP（CC EAL4 ALC_FLR.3 付拡張認定）（Windows Server 2003/XP 他）

  －プレスリリース（12 月 15 日）

  http://www.microsoft.com/japan/presspass/detail.aspx?newsid=2535

  －関連資料

  Overview of Windows XP SP2 and Windows Server 2003 Common Criteria Certification

  http://www.microsoft.com/technet/security/prodtech/windowsserver2003/ccc/default.mspx

- セキュリティターゲット（ST）[Web]

  ◆Microsoft Windows Server 2003 and Microsoft Windows XP

  http://niap.nist.gov/cc-scheme/st/ST_VID4025.html

10. その他

○利用者ニーズについて

- 専門家でなくても管理しなければならないユーザへの対応を重視 [プレゼン]

○RMS（Rights Management）について

- 情報管理にあたっては、OS のアクセス制御機能だけでなく、暗号化や複製防止などアプリケーション・レベルの手法も含めて総合的に考えることが必要 [プレゼン]

２.３ OS が提供するセキュリティ機能の詳細

ここでは、２.１.２（２）に示したプレゼンテーションの結果をもとに、OS が備えるセキュリティ機能について、その技術的特徴に関する情報を中心にまとめる。

２.３.１ SELinux

SELinux が提供するセキュリティ機能として、次のような特徴が示されている。

（１）強制アクセス制御の実現方法

SELinux の提供する強制アクセス制御機能は、Linux カーネル（バージョン 2.6 以降）の LSM（Linux Security Module）を利用して動作する。LSM は従来のパーミッションチェックとは異なり、root 権限を含むプロセス権限には依存しないため、動作を回避させることはできない。

ユーザがあるコマンドを実行したときに、OS が行う処理の概要は以下のようになる。

① プロセスのシステムコール
② パーミッションチェック
③ LSM チェックによる SELinux モジュールの呼び出し
④ SELinux モジュールの動作
⑤ SELinux のセキュリティポリシーのチェック
⑥ 処理実行
⑦ セキュリティポリシーに基づいたリソースへのアクセス

（２）強制アクセス制御の実体

SELinux の強制アクセス制御機能の各構成要素について、それぞれの特徴は以下のようになる。

① プロセスのアクセス制御（Type Enforcement：TE）

- サブジェクト、オブジェクトにそれぞれラベルの設定が必須
- サブジェクトのオブジェクトに対する操作の許可は、サブジェクトのラベル、オブジェクトのラベルの組み合わせごとに設定
- 設定されていない操作は、全て拒否する

② オブジェクトクラス（オブジェクトの種類）

- 50 種程度
- 例：ファイル、ディレクトリ、ソケット、共有メモリ

③ オブジェクトクラス毎の操作（アクセスベクタ）

- オブジェクトクラス毎に数種～数 10 種
- 例：read、write、create、append、execute、listen

④ 権限の昇格制御

- プロセスが別のプロセスを起動する場合、起動元となったプロセスと同一ラベルで起動
- 予め関連付けを設定した場合、別のラベルでプロセスを起動することが可能

⑤ ロールベースアクセス制御（RBAC）

- シェルプロセスを起動するユーザに関連付けられているラベルがロール
- シェルプロセスにはロールに対応するラベルが設定される
- 操作の可・不可は、TE の制御下で行われる

⑥ ラベルの呼称

- プロセスに関連付けられるラベル　　：ドメイン
- リソースに関連付けられるラベル　　：タイプ
- ユーザアカウントに関連付けられるラベル　：ロール

（3）利点と課題

他の OS と比較した時の SELinux の利点と課題として、以下の事項が挙げられる。

① 利点

- 非常に細かい粒度でアクセス制御が可能であり、最少特権を実現することが可能

② 課題

- セキュリティポリシー構築支援ツールなどの整備が不十分であり、専門家レベルでしか扱うことが出来ないのが現状
- ポリシー集中管理ツールなどの整備が不十分であり、大規模運用などの環境下に適応できていない

（4）SELinux に関する最近の動向

プレゼンテーションが実施された 2005 年 11 月時点の動向として、以下の傾向が示されている。

① Targeted ポリシーの出現

- アクセス制御対象を限定し、専門家以外でも利用可能な仕組みを整えたポリシー

- 全ての対象を制御する標準ポリシーである Strict ポリシーとは全くコンセプトが異なる
  - ユーザ毎のアクセス制御　　：なし
  - プロセス毎のアクセス制御　　：一部のプロセスのみ
  - アクセス制御対象プログラム　　：FC3 で dhcpd、httpd、syslogd など 8 個
- セキュリティの強度は下がるが、アクセス制御対象が限定化されるため、構築や運用の手間が軽減されるメリットがある

② Multi-Level Security（MLS）と Multi-Category Security（MCS）を実現するポリシー

- MLS 及び MCS に対応するポリシー設定に関する研究活動あり
- Fedora Core 5 にて MCS が提供される予定

③ ポリシー関連ツールの拡充

- 現状では使い勝手は専門家向けのレベルであるが、setools（Tresys 社）、SELinux Policy Editor（日立ソフト）、system-config-security-level（Fedora Core、Red Hat）などがあり、利便性を向上に向けた対応が進んでいる。
- SELinux Policy Server など複数のサーバを対象としたポリシー配布・集中管理を目指したツールなどの研究が行われている。

④ アプリケーションレイヤのオブジェクト制御

- Secure Enhanced X など、データベースや X Window System など、アプリケーションレイヤにおける研究活動が積極的に行われている。

２．３．２ FreeBSD（TrustedBSD）

FreeBSD が提供するセキュリティ機能として、次のような特徴が示されている。

（１）強制アクセス制御の実現方法

FreeBSD（5.3 以降および 6.0 以降）ならびに TrustedBSD において、新しいカーネルセキュリティフレームワークである「TrustedBSD MAC フレームワーク」が実装されている。これは Linux カーネル 2.6 の LSM の仕組みとは異なり、root 権限でも回避されない仕組みとは限らず、読み込むモジュールの実装方法や仕様に依存する。本フレームワークは、コンパイル時またはシステム起動時のカーネルのアクセス制御ポリシーを拡張することによって実現されている。

FreeBSD のアクセス制御モジュールはそれぞれ単独で利用するだけではなく、種別によっては複数の強制アクセス制御モジュールを組み合わせて同時に利用することも可能である。組み合わせ次第で、完全な強制アクセス制御を実現することもできる。

（２）強制アクセス制御を実現するモジュール一覧

強制アクセス制御に関する FreeBSD の主要なモジュールの例を以下に示す。

- mac_biba　：Biba データ完全性保証モデルポリシー
- mac_bsdextended　：ファイルシステム・ファイアウォールポリシー
- mac_ifoff　：インターフェース・スライスポリシー
- mac_lomac　：LOMAC データ完全性モデルポリシー
- mac_mls　：Multi-Level Security ポリシー
- mac_partition　：プロセス区画分離ポリシー
- mac_portacl　：ネットワークポートアクセス制御ポリシー
- mac_seeotheruids　：ユーザ区画分離ポリシー
- SEBSD　：SELinux の Type Enforcement（後述）

（３）FreeBSD におけるセキュリティ機能の提供に関する現状

FreeBSD におけるセキュア OS 機能の提供に関する動向は、プレゼンテーションが実施された 2005 年 11 月時点で以下のようになっている。

- 強制アクセス制御（MAC）を実装するために必要なカーネル側のフレームワークが、ほぼ完成・実装済み。
- そのフレームワークを使った、前述のようなセキュリティポリシーモデルを実現するモジュールが作られている。
- モジュールの完成度はモジュール内容に依存し、モジュールによって異なるが、SEBSD を

除けばいずれも問題なく使用できるレベルとなっている。

- 実運用に必要な柔軟性が欠けていたり、設定ツールやドキュメントが用意されていないケースがあるなど、操作や設定に関する側面ではまだ充実しているとは言えない。
- SEBSD モジュールについては、SELinux の Type Enforcement 機能を、設定の互換性も含めて完全に移植することを目標として実装作業を継続している段階である。

（4）強制アクセス制御モジュール以外のアクセス制御機能

（2）で示した強制アクセス制御に関するモジュール以外で提供されているアクセス制御の例として、chroot 及び jail によるコンパートメント化機能がある。この特徴を以下に示す。

- ファイルシステム、プロセス、ネットワーク機能を分離することが可能。
- アクセス制御の範囲は、コンパートメント化されたファイルシステム内に固定化するため、他のコンパートメントとリソースを共有するなどの自由度はない。
- 強制アクセス制御モジュールを適用する場合と比較した場合、コンパートメント ID に基づく制御といった柔軟なアクセス制御は実現できない。

（5）利用実績　例：mac_bsdextended

FreeBSD の実用的な利用実績としては、以下の例がある。

- 民間企業の社内ユーザ向けサービスとして、mac_bsdextended の利用実績がある。
- 複数ユーザアカウントに対してシェルの利用を許可するが、このアクセス制御モジュールを用いて、本人以外のホームディレクトリへのアクセス制限を行っている。

第３章 セキュリティ機能別の分析・整理

前章では本調査における調査対象 OS 毎に機能を整理したが、ここでは前章における調査結果をもとに、電子政府に関わる情報システムにおいて使用する OS を実際に選定する際に考慮すべき視点について、各 OS の特徴と利用可能な機能に関する分析を行う。

３.１ 調査内容の横断的分析を通じた観察

2.2 において整理した、委員会における各 OS ベンダによるプレゼンテーション結果と質疑の内容をもとに、OS のセキュリティ機能に関する調査項目別に横断的に分析した結果を、「観察される事実」と「考察事項」に分けて整理する。

（１）OS のアクセス制御機能の特徴

① 観察される事実

- 各 OS が提供するアクセス制御に関する機能を、プレゼンテーション内容をもとに比較するとそれぞれ以下のようになる。なお、各機能の意味する内容については、１.２.１項（15 ページ）において示している。

a) 強制アクセス制御

Red Hat、HP-UX、PitBull（Foundation Suite）、Solaris（Trusted Solaris を含む）の各 OS において提供されている。このほか、PitBull（LX）については「ドメインベースアクセス制御」として、情報の機密区分（classification）による上下関係の概念をもたない強制アクセス制御機能が提供されている。また、Compartment Guard for Linux においては、コンパートメントで隔離された相互間で強制アクセス制御に相当する機能を実現することができる。これ以外の OS については、任意アクセス制御のみとなる。

b) マルチレベルセキュリティ（MLS）

PitBull（Foundation Suite）と Trusted Solaris において、機密レベルに応じた階層化に基づくアクセス制御機能を利用可能であることが示されている。このうち PitBull（Foundation Suite）については、マルチレベルセキュリティに関するプロテクション・プロファイルである MLOSPP の暗号実装を除く範囲での認証申請を行っていることがあわせて示されている。

c) 最少特権

強制アクセス制御を提供する Red Hat、HP-UX、PitBull（Foundation Suite、LX）、Solaris（Trusted Solaris を含む）の各 OS と、「アプライアンス・プロテクション機構」と呼ぶ独自の機能でシステム管理者によるルール変更操作を不可能にする機能をもつ

Compartment Guard for Linux において提供されている。

d) コンパートメント化

本機能は OS ベンダによって異なった名称で提供されており、内容にも相違がある。製品ごとの特徴を示すと次のようになる。

i) HP-UX：Security Containment **機能**

最少特権、RBAC などを提供する Security Containment 機能の一部としてコンパートメント化の機能が提供され、関連のないリソースの隔離が可能となるとともに、強制アクセス制御の実現手段としての役割も担っている。ファイルやプロセスはコンパートメント設定情報と関連づけられ、ポリシー設定をコンパートメント単位で行うことができるため、シンプルかつ柔軟なアクセス制御が可能となることが謳われている。

ii) Compartment Guard for Linux：**コンテインメント機構、コミュニケーションガード機構、ファイルガード機構**

すべてのプロセスをコンパートメントと呼ぶ区画に閉じこめ（コンテインメント機構）、コンパートメント間やネットワークとの通信の制限（コミュニケーションガード機構）や、ファイルシステムに対するアクセスの制限（ファイルガード機構）によってコンパートメント化を実現する。

iii) PitBull（LX）：**ドメインベースアクセス制御**（DBAC）

強制アクセス制御に用いるドメインと呼ばれる区分を用いることにより、ファイルとネットワークに対してドメインの設定に基づくアクセス制御を行うことができる。

iv) Solaris：**仮想化**（zones）

Solaris Container による「ゾーン」の設定をもとに、プロセス、デバイス、ファイルシステム、ネットワーキングについて、ゾーン単位で動作の制限を行うことができる。

v) AIX：**仮想化機能**

Hypervisor による論理パーティション（LPAR）の設定により、１つのハードウェア上で複数の OS イメージを動作させることができる。このとき OS 上でのプログラムによるアクセスは Hypervisor によって制御され、他の論理パーティションが所有しているリソースやデータのアクセスは不可能となる。

e) デュアルロック

PitBull（Foundation Suite）においてのみ、利用可能であることが示されている。

- 通常の OS としても利用できる製品（Red Hat、HP-UX、Solaris 等）の場合、強制アクセス制御などセキュア OS に相当する機能は必要に応じてセキュリティを高めるために利用可能な選択的なものとしての位置づけとなっている。
- トラステッド OS としての位置づけをもつ製品（PitBull、Trusted Solaris 等）の場合は、

LSPP やかつての TCSEC への準拠性を示すことも、アクセス制御機能の仕様を表現するための手段となっている。

② 考察事項

- 強制アクセス制御の実現方法については、プログラムやリソースに関する相互のアクセスを排除したいものをコンパートメント化により分離することを重視しているもの（HP-UX、Compartment Guard for Linux、PitBull（LX）、Solaris）と、こうした分離もポリシー設定の中で扱うもの（Red Hat、PitBull（Foundation Suite））とに分かれる。
- アクセス制御機能を有効にすることによるアプリケーションの動作への影響については明示されておらず、別途留意する必要がある。
- アクセス制御機能は製品によってその機能を表象する名称が異なることをはじめとして表現方法が多様であるため、製品間の機能の比較は容易ではない。こうした中で、LSPP などのプロテクションプロファイルへの準拠は、機能を容易に把握するための手段として有用である。

（2）運用上の操作性

① 観察される事実

- 操作性に優れていることの例証として、GUI ベースでアクセス制御等の操作を行えることが PitBull を除く各社より挙げられている。

② 考察事項

- OS の操作性についてプレゼンテーションを通じて具体的な内容を示した例は少ない。これは操作性についての客観的な評価基準を示しにくいことによるものと推察される。
- 実際の運用においては、GUI 環境の提供されている OS であっても必要な操作のみを簡潔かつ安全に行えるように、専用のコマンドやツールを構築時に作り込むケースがあり、GUI による操作の可否が操作性の優劣を決定づけるものではないことに留意する必要がある。

（3）支援ツールの提供状況

① 観察される事実

- セキュア OS の特徴を反映したツールとしてシステムポリシーの設定管理を支援するものが、HP-UX や Solaris で OS の一部として提供され、Red Hat では外部ツールが利用可能となっている。PitBull では通常の OS 用のアプリケーションを動作させるためのツールが提供されている。
- 通常の OS におけるツールとしては、Windows において RBAC としての制御を容易にするツールが無償提供されている。一方 AIX ではアクセス制御を強化するための製品が利用

可能となっている。

- システムポリシーの誤設定等を検出するツールについては、いずれのベンダからも情報提供は行われていない。

② 考察事項

- 上述の通り、ツールは OS に組み込まれた形で提供されることも多いため、外部ツールが存在しないことが即ツールが無いことを意味しないことに留意する必要がある
- 今回の発表においては、ツールによる差別化を強くアピールしている例は見られない。これは、OS のセキュリティ機能を活用する事例が少ないことで、ツールの利用が普及していないことと、構築をシステムベンダが行うケースが多いことからツールへのニーズがこれまで必ずしも高くなかったことによるものと考えられる。

（4）サポート体制

① 観察される事実

- OS のサポート期間については、HP-UX のように「10 年」などの年数で定めている製品と、Solaris のように「最新版より何世代前のバージョンまで」のように世代数で定めている製品がある。また、PitBull のように通常の OS との組み合わせによる利用を前提とした製品では、サポート期間はベースとする OS のサポート期間に対応することが示されている。
- 脆弱性対応については、いずれの製品についても必要な体制が整備されていることが示されている。

② 考察事項

- サポートについては差別化の手段として力点を置いているベンダもあり、多様な形態が示されている。標準サポートと有料のサポートとの区分に関しては、システムの重要性に応じたサポートが選択できるという観点から有効であると考えられる。
- Red Hat における strict ポリシーに関するサポートに示されているように、セキュリティを強化した設定に関するサポートを必要とする場合は、各 OS ベンダ（二次リセラーを含む）が提供する標準サポートの範囲外との扱いとなるためサポート費用が高くなる可能性があることを考慮する必要がある。
- OS のサポート期間は単純に長ければ長いほど良いというわけではなく、特定のバージョンについて長期間サポートするためのコストは製品コストに反映されることになる。システムの想定耐用年数よりも長い分は過剰投資となるが、耐用年数は当初の想定から変化することもあるため、ある程度の余裕に対応したサポートが得られることが望ましい。
- OS のセキュリティ機能を強化してシステムを構築する際には、そうした構築の経験を豊富に有するシステムベンダを除けば、OS ベンダによる何らかのサポートが必要になることが

多い。そこで、OS ベンダにより構築支援や教育などのサポートが提供されていることが重要な要件となる。

- 脆弱性対応については、いわゆるトラステッド OS の機能を備えている場合は脆弱性の種類によっては緊急対応の優先度が低くなることもあり、セキュリティ機能を高めていない通常の運用体制と比較すると重要度は低いが、OS における脆弱性が発見された場合等に備えた対応の体制は欠かせない。

（5）ドキュメントの整備状況

① 観察される事実

- ドキュメントの公開対象をライセンス契約を行った利用者に限定せず、Web を通じて誰でもアクセス可能としている例が多い。中には Red Hat、HP-UX、Windows 等のように、開発用を含めたマニュアル類まで公開している製品も見られる。
- 日本語化されているドキュメントの比率はベンダによって相違があるものの、構築や運用に際して最低限必要となるドキュメントについては、いずれの OS についても日本語版が提供されている。

② 考察事項

- ドキュメントについては、各ベンダから多くの情報が提供されている。かつてはトラステッド OS を利用しようとすると英語のドキュメントを参照せざるを得ない状況も存在したが、現在は概ね必要な事項の参照を日本語で行うことが可能となっている。

（6）アプリケーションのユースケース

① 観察される事実

- 本項については、いずれのベンダからも有用な情報の提供はなされていない。

② 考察事項

- 一般的には、必要があればベンダは何らかの方法でアプリケーションを動作させることが可能である場合が多い。ただしアプリケーションの動作はその設計に依存する要素が大きく、対応の可否はケースバイケースであるため、一般論としてのユースケースの説明は行いにくい面がある。

（7）アプリケーションと OS の連携状況

① 観察される事実

- 強制アクセス制御などの機能を利用しないケースにおいては、データベースアプリケーション等において、アカウント情報を用いたアクセス制御を用いる例がある。

- いわゆるセキュア OS、トラステッド OS に位置づけられる OS においては、OS とアプリケーションとの連携よりも、アプリケーションが無改造で動作することのアピールにプレゼンテーションの重点が置かれており、連携に関する言及は少ない。

② 考察事項

- 現在のシステム構築に際しては、データベースサーバなども含め、OS の上にミドルウェアを実装し、その上にアプリケーションを構築するケースが多いため、OS とアプリケーションが直接連携する場合は必ずしも多くないことが指摘されている。

（8）導入実績

① 観察される事実

- トラステッド OS、セキュア OS としての機能を有する製品については、政府機関、軍事関連機関、金融機関等での利用例が紹介されている。

② 考察事項

- 導入実績については、今回の調査では実態を網羅的に反映した情報の提供は行われていないと考える必要がある。この原因としては、現時点で OS のセキュリティ機能を強化したシステムを利用している組織は自組織に関する情報提供に消極的であることが多く、結果的に事例として公開可能なものが限られてしまうことが挙げられる。

（9）Common Criteria 等の認証取得

① 観察される事実

- 認証取得については、通常の OS であっても取得が可能な CAPP（Controlled Access Protection Profile）に基づくものが中心である。LSPP（Labeled Security Protection Profile）については、Trusted Solaris 8 において取得済み、Red Hat と PitBull（Foundation Suite）において審査中となっている。
- 認証の保証レベルについては、一般に民生用で最高レベルとされる EAL4 に拡張項目を付けて EAL4+としているものが多い。
- 拡張項目としては、Microsoft Windows における ALC_FLR（欠陥修正）のように、OS の欠陥に対する修正のマネジメントに対する保証の例などがみられる。
- トラステッド OS としての位置づけをもつ製品（PitBull、Trusted Solaris 等）の場合は、LSPP やかつての TCSEC への準拠性を示すことも、アクセス制御機能の仕様を表現するための手段となっている。

② 考察事項

- 認証取得については、セキュア OS としての機能の提供に関する客観的な裏付けとなるこ

ともあり、積極的な姿勢を示しているベンダが多い。

（１０）その他

① 観察される事実

- その他の情報としては、OS に関わる将来の予定などが示されている。

３.２ OS のセキュリティ機能の利用可能性に関する考察

ここでは、電子政府に関わる情報システムにおいて利用することを前提に、現時点（2006 年 3 月）において OS のセキュリティ機能としてどのようなものが利用可能かを、これまでの分析結果をもとに考察する。

３.２.１ システムポリシーに関する機能

OS が提供する強制アクセス制御機能と最少特権機能を用いることにより、情報システムのシステムポリシーに関する以下のような機能要件を実現することの可能性について考察する。

（１）強制アクセス制御

セキュア OS として扱われている Red Hat、HP-UX、PitBull、Solaris（Trusted Solaris を含む）において提供されている。このうち PitBull LX における強制アクセス制御は、「侵入防止目的専用に改良されたもの」との位置づけとされ、独自のアクセス制御方式であるドメインベースアクセス制御（DBAC）との組合わせで提供される。

（２）管理者特権の最少化

いずれの OS とも、管理者の役割の種類（権限の割当、ユーザ管理、運用監視、バックアップ等）に応じて複数の管理者アカウントを作成することは可能である。ただし、通常の OS では管理者アカウントを複数作成することができても、それは認証時のパスワードの複数の管理者間で共有することを避けるとともに、誰が操作したかを明らかにすることを主たる目的として提供され、各アカウント間での権限に相違がない場合が一般的である。ここで対象としている管理者特権の最少化を実現するには、ある役割のための管理者アカウントで別の役割に割り当てられている操作を行うことを防ぐ必要がある。

この機能が提供されているのは Red Hat、HP-UX、Compartment Guard for Linux、PitBull、Solaris（Trusted Solaris を含む）、AIX の各 OS となる。

（３）ロールベースのアクセス制御（RBAC）

ロールと呼ばれるユーザアカウントのグループを設定してアクセス権限を設定し、個々の利用者やアプリケーションのために提供されるアカウントがどのロールに属するかを指定することにより、アクセス制御に関するポリシー設定を効率化する機能である、本機能はセキュア OS に限定されるものではなく、Red Hat、HP-UX、Solaris（Trusted Solaris を含む）、Windows において明示的に可能であることが示されている。また、他の OS においても異なる名称にて類似の機能が提供されており、いずれの OS でも機能要件として概ね実現することが可能である。ただ

し、設定するアクセス制御に強制性を伴わせることが可能なのは、セキュア OS としての機能を備える Red Hat、HP-UX、PitBull、Solaris の各 OS に限定される。

（4）コンパートメント化

3.1 節において示したように、OS 内部にコンパートメントを設けて相互間のアクセスを制限する機能は、HP-UX、Compartment Guard for Linux、PitBull（LX）、Solaris の各 OS において利用可能である。ただしここに含まれない、Red Hat、PitBull（Foundation Suite）の各 OS においても、ポリシーを適切に設定することにより、同様の機能を実現することは可能である。コンパートメント化のメリットは、コンパートメント（OS によって呼び方は異なる）を定義することを通じて、相互に分離されることが明確化されるとともに、ポリシーの設計・設定に関する負荷を軽減することであると言える。

なお、プログラムやリソースに関するアクセスの分離のアプローチとしては、上述のように OS 内を分離するのではなく、Windows 用に Microsoft 社が提供している Virtual PC や、UNIX、Linux、Windows のそれぞれで利用できる VMware（VMware 社）のように、本来の OS（ホスト OS）の上で Virtual Machine（VM）と呼ばれるアプリケーションを動作させ、その VM 上で 1 つないし複数の OS（ゲスト OS）を実行することで、ゲスト OS が行うアクセスを制限する方法もある。この場合、ゲスト OS が強制アクセス制御機能を備えた OS でなくても、ホスト OS の側からはゲスト OS に対してコンパートメントに相当する強制的なアクセス制限を行うことができるため、いわゆるセキュア OS やトラステッド OS 上で動作させることが困難なアプリケーションに対するアクセス制御の手法として検討の価値がある。また、AIX では論理パーティション（LPAR）機能により、複数の OS イメージを稼動させることができる。この LPAR 機能も、1 つのハードウェア上で稼動する複数の OS 間での相互干渉を排除し、セキュリティを確保するためのアクセス制御の手段とみることができる。

３.２.２ 運用・管理に関する機能

情報システムの運用や管理に関して OS が提供する機能の利用可能性について考察する。

（1）運用操作におけるデュアルロック機能の導入

システムに重大な影響をもたらす操作に際して、2 名以上の管理者による操作を要求するデュアルロック機能については、PitBull（Foundation Suite）においてデュアルコントロール機能として提供されていることが示されているのみである。セキュリティ要件としてデュアルロック機能を要求する場合は、必然的に本製品を選択することになる。

（2）運用・管理に関する負荷の軽減

OS の運用・管理の負荷を軽減する手段として以下の 2 種類が利用可能である。これらが自組織における情報システムの利用形態に適合している場合は、情報システムに関する負荷の軽減効果を期待できる。ただし機能が OS 付属でない場合は、将来的な OS のバージョンアップに対応するとは限らないため留意する必要がある。

① 支援ツールの提供

Red Hat では、SELinux に関するポリシー設定、ログ解析、監査を支援するためのツールがオープンソースの外部ツールとして提供されている。一方 HP-UX、Solaris、Windows においては、OS の付属機能もしくは自社提供のツールとして、各種の設定を GUI を用いて行えるようになっている。

② ポリシーの自動作成機能の提供

Compartment Guard for Linux では、アプリケーションの動作をもとに強制アクセス制御を設定するためのルールを自動生成することができる。ただし、ルールを完全に自動的に生成することは難しく、ある程度は人手での調整が必要であることが示されている。

第４章 まとめと今後の展望

これまでの各章における分析の結果をまとめるとともに、今回得られた知見をもとに今後取り組むべき施策について展望する。

４.１ 調査結果のまとめ

今回の調査で得られた知見、情報としては以下の内容が挙げられる。

４.１.１ 現在提供されている OS のセキュリティ機能を用いて可能な事項

以下の事項については、現在提供されている OS を用いて必要な機能を実現できることが、OS ベンダによる説明や紹介された事例等を通じて確認された。

（１）強制アクセス制御によるポリシーの強制適用

強制アクセス制御については、セキュア OS の必要条件とみなされていることもあり、セキュア OS として提供、販売されている OS においていずれも利用可能である。強制アクセス制御の導入により、ポリシー設定の整合性を高め、攻撃や設定ミスによる被害の抑制が期待される。

（２）最少特権化による被害の抑制

管理者の特権アカウントやアプリケーションが内部で利用するアカウントを含め､OS 上で設ける全てのアカウントについて、それぞれに割り当てる特権を最少化することについては、セキュア OS として提供、販売されている OS については概ね問題なく利用可能である。実際の運用時にはそれぞれのアカウントのアクセス制御を変更可能な権限を有する管理者アカウントを一時的に無効に設定することにより、仮に一部のプログラムが乗っ取られた場合でも OS のアクセス制御を改変される恐れが小さくなるため、安全性が高まることが期待できる。

（３）デュアルロック機能

昨年度の報告書においても説明している通り、複数名の管理者による認証を経ないとサーバ等に重大な影響を及ぼす作業が不可能な機能であり、デュアルコントロール機能とも呼ばれる。

本機能はかつての TCSEC におけるトラステッド OS の要件とされているものであり、トラステッド OS として販売されている製品において利用することが可能であるため、導入上の困難はないと考えられる。ただし、本調査の調査過程において、民間においてはコスト高になるため、ほとんど導入事例がない旨が指摘されている。

４.１.２ 現状では可能かどうかの確認ができなかった事項

一方、下記の事項については、今回の調査研究では利用可能であることの確認は得られていない。

（１）情報の格付けに基づくアクセス制御

2005 年 12 月に公表された政府機関統一基準においては、情報の格付けのもとで管理を行うことの重要性が示されている。トラステッド OS におけるマルチラベルセキュリティはこうした情報の格付けに応じたアクセス制御のニーズに応えるものであるが、トラステッド OS と位置づけられる製品において、こうした管理が可能であることは示されているが、それ以外のセキュア OS その他の製品では情報の格付けに応じたアクセス制御機能についてのアピールはなされていない。

情報の格付けについては、米国国防総省において実際にトラステッド OS を用いた管理がなされている事例はあるものの、国内では公表されている事例は見あたらず、ベンダにおいても紹介可能な事例を持ち合わせていないことが推察される。こうした結果、今回の調査を通じては情報の格付け機能の利用可能性について十分な情報は得られていない。

（２）異種 OS の混在環境におけるアクセス制御の連携

これまで、セキュア OS やトラステッド OS は各社が独自の研究開発の成果をもとに実装してきているため、OS ベンダが異なると機能に関する呼び方、用語から異なるほどの相違がある。そうした中で、同一のネットワーク内部で異なるベンダ製品を組み合わせて使用している事例についてはほとんど存在しない。新規に調達する場合は、トラブル回避の意味からも複数ベンダをあえて混在させないのは当然である。しかしながら、当初想定されていなかった組織の合併、統合等の状況に応じてシステムの混在が生ずるような状況は、今後電子政府においても想定されることから、何らかの形で今後検証が行われていくことが望まれる。

なお、こうした機能に関する情報は調査方法の制約上得られなかった可能性もあり、情報が得られないことが即不可能であることを意味するものではない。ただし、通常の OS を利用している場合と比較して、高いセキュリティ機能を備えた OS を導入するユーザには、事例の開示に消極的な傾向がある。したがって、OS ベンダとしても導入事例を具体的に紹介することが難しいため、導入者は限られた情報の中で実現の可能性を確認する必要がある。よって現状ではこうした機能が利用可能かどうかの判断には、情報の不足に伴う相応のリスクが伴うことに留意する必要がある。

４.２ 今後の展望

今後、本調査の延長のもとで以下のような展開が期待される。

（１）現実的な調達に向けた要求仕様書の策定への応用

政府機関統一基準において、電子政府における重要な情報を扱うシステムで強制アクセス制御と最少特権の各機能の採用を検討することが示されていることもあり、今後の調達要件の中に OS のセキュリティ機能を含めたものが増えていくことが予想される。ただし、OS のセキュリティ機能を正しく調達要件に反映させていくためには専門的知識が必要であることから、OS のセキュリティ機能を活用する場合の雛形となる要求仕様書の形でとりまとめることが期待される。このとき、本調査の結果を活かし、現在利用できる製品の提供する機能を用いた内容とすることで、より実効性の高いものとすることが可能となる。

（２）多様なユースケースの想定に基づく利用可能性の検討

前節で考察した理由により、事例に基づく利用可能性には限界があることが確認された。そこで、仮想ではあるが現実性を備えたユースケースを多数想定し、それぞれの条件における利用可能性を検討することが、調達者に向けた手助けとなるものと期待される。

付録 製品別情報リソース

（1）Red Hat Enterprise Linux

① OS の特徴に関する情報

- Red Hat Enterprise Linux

  http://www.redhat.co.jp/software/rhel/

② OS のサポートに関する情報

- Red Hat Enterprise Linux サポートページ

  http://www.redhat.co.jp/support/

（2）HP-UX 11i

① OS の特徴に関する情報

- HP-UX

  http://www.hp.com/jp/hpux

② OS のサポートに関する情報

- HP-UX サポート（HP-UX 管理者向け情報）

  http://www.hp.com/jp/support/hpux

（3）Compartment Guard for Linux

① OS の特徴に関する情報

- HP Compartment Guard for Linux

  http://www1.jpn.hp.com/solutions/infrastructure/security/hpcg/

② OS のサポートに関する情報

- カーネルソース及びカーネルパッチ情報

  http://www1.jpn.hp.com/solutions/infrastructure/security/hpcg/kernel_patches.html

（4）PitBull（LX / Foundation）

① OS の特徴に関する情報

- PitBull 日本語公式サイト

  http://www.pitbull.jp/

② OS のサポートに関する情報

- トレーニングサービス

  http://www.pitbull.jp/support/training/

（5）Solaris 10 / Trusted Solaris

① OS の特徴に関する情報

- Solaris 10 オペレーティングシステム

  http://jp.sun.com/software/solaris/10/

- Trusted Solaris オペレーティングシステム

  http://jp.sun.com/software/solaris/trustedsolaris/

② OS のサポートに関する情報

- Solaris 10 OS サービス＆サポート

  http://jp.sun.com/service/solaris10/

- SunSolve Online

  http://sunsolve.sun.com/pub-cgi/show.pl?target=home

（6）AIX 5L

① OS の特徴に関する情報

- IBM AIX 5L

  http://www-06.ibm.com/jp/servers/eserver/pseries/aix/

② OS のサポートに関する情報

- UNIX サーバーサポート

  http://www-06.ibm.com/jp/servers/eserver/pseries/support/

（7）Windows Server 2003

① OS の特徴に関する情報

- Windows Server 2003

  http://www.microsoft.com/japan/windowsserver2003/default.mspx

② OS のサポートに関する情報

- Windows Server 2003 のサポート

  http://www.microsoft.com/japan/windowsserver2003/support/default.mspx

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] 中村雄一・上野修一・水上友宏, SELinux 徹底ガイド －セキュア OS によるシステム構築と運用－, 日経 BP, 2004 年.

（各 OS ベンダ提供の資料名については、本文および付録にて記載につき省略）