



電子政府情報セキュリティ技術開発事業

「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」

調査報告書

平成14年2月

日立ソフトウェアエンジニアリング（株）

はじめに

政府は、2003 年度までに行政の効率化や国民負担の軽減を目標に行政手続きを電子化する電子政府の基盤を構築することを目指している。

電子政府の構築は、デジタル経済・社会の1つのモデルであり、その中で実施される情報セキュリティ確保のための対策もまた、広く民間の範となるものとなり、それによって、我が国のネットワーク全体の安全性・信頼性を高め、さらに、具体的に進みつつある同様な取り組みと連携していくことにより国際的な貢献につながることも期待される。

一方、ホームページの改ざん、データ破壊、サーバをパンクさせるサービス妨害攻撃(DoS 攻撃)やコンピュータウイルスなどの電子的な攻撃を目的としたいわゆるサイバーテロのような大規模な攻撃が行われることが懸念されている。

このような状況を鑑み、秘匿性、完全性の要件のための情報の隔離を強制するメカニズムを持ち、不正な情報の読出し・改ざん、アプリケーションレベルのセキュリティメカニズムの回避を防ぎ、悪意のまたは不良なアプリケーションによるダメージを最小限に留めるオペレーティングシステムレベルでのセキュリティ機能が必要とされている。

そこで、現在開発・提供されているセキュアオペレーティングシステムの動向・機能概要の調査を行い、ソースコードが公開されているセキュアオペレーティングシステムのセキュリティメカニズムの実装方法を調査し、また、セキュアオペレーティングシステムの環境を実際の構築する中でその問題点・留意点を調査することで、サイバーテロの脅威に対抗するための、的確かつ効果的なセキュリティ対策、および、電子政府における情報セキュリティ確保をする上での技術的な支援となることを本報告書の目的とする。

本文中の製品名は、一般に各社の登録商標、商標、または商品名である。

本文では、TM、©、®マークは省略している。

本報告書は、以下3つの編から構成されている。

- 第 編 調査概要編

- 1 2 システムのセキュリティ機能に関する概要調査

- 第 編 実装方法調査編

- SELinux 及び TrustedBSD の実装方法に関する調査

- 第 編 環境構築検証編

- SELinux の構築方法に関する調査

用語の説明

用 語	説 明
DES/3DES	Data Encryption Standard 共通鍵暗号化方式の代表的な規格。機密外重要情報の暗号方式として米国政府に採用されている。
ACL	Access Control List 特定のオブジェクト(ファイル等)へのアクセス(読み、書き、実行、追加、変更、削除、作成等)が許可されたサブジェクトのリスト。
Bell-LaPadulaモデル	Bell-LaPadula モデルは、サブジェクト、オブジェクト、アクセス操作を定義し、サブジェクト及びオブジェクトは特定のセキュリティクラスに属する。サブジェクトは、それよりも高いレベルのセキュリティクラスを持ったオブジェクトを読むことができない。また、サブジェクトは、それよりも低いセキュリティクラスのオブジェクトへの書き込みができない。このモデルは、オレンジブック要件の基礎となっているコンピュータセキュリティ方針モデルである。
Bibaモデル	Biba モデルは、機密性(不正アクセスに対する保護)と保全性(不正改竄に対する保護)の区別に着目している。一連の規則が記述されたコンピュータセキュリティ方針の保全モデルで、このモデルでは、サブジェクトは自己よりも信頼度の低いオブジェクトやほかのサブジェクトには依存しない。
Blowfish	Bruce Schneier 氏によって考案された 448bit 可変長キーのフリー暗号アルゴリズム。 http://www.counterpane.com/
Capability	Capability とは、資格・権限・能力を意味し、従来のスーパーユーザ(root)が持っていた権限を細かく分割し、プロセスに不必要に権限を与え過ぎないようにするために使われる。例えば、システムの時刻を変更するには従来のシステムでは実行プロセスがスーパーユーザ権限を持つ必要があったが Capability を採用しているシステムでは「CAP_SYS_TIME」という資格に限定してプロセスに権限を与える。
CC	Common Criteria for Information Technology Security Evaluation IT セキュリティの国際的な評価基準。1980 年代始めにアメリカで開発された「Trusted Computer System Evaluation Criteria(TCSEC)」及び、1990 年代始めにヨーロッパで開発された「Information Technology Security Evaluation Criteria (ITSEC)」を統合して開発された、国際的な IT セキュリティ評価基準。
Credential	資格証、証明書、信任状、保証書等の意味で使用され、Credential データはアクセス操作での認可・認証に使用される。
DAC	Discretionary Access Control 任意アクセス制御 「アクセス制御」参照。
domain	強制アクセス制御技術の 1 つである Type Enforcement にて、アクセス制御のために利用されるラベル。この domain ラベルは、適切なセキュリティポリシーに基づいてあらかじめサブジェクトに対して付与される。

用語	説明
dominance	優位にたつこと。MLSにおける機密レベル間の関係を表す。機密ラベルAの機密種別が機密ラベルBの機密種別よりも高く、機密ラベルAのカテゴリが機密ラベルBのカテゴリをすべての含む場合に、機密ラベルAは機密ラベルBより優位にあるという。
DTE	Domain and Type Enforcement domainとtypeラベルによる強制アクセス制御技術。TEでファイルとセキュリティ属性を1対1で表現していたのに対して、DTEは同一のセキュリティ属性を持つファイルを部分的にファイル階層構造で簡潔に表現することでアクセス制御テーブルの拡大を抑える拡張を施している。
Flask	Flux Advanced Security Kernel SELinuxで採用されている、OSレベルでのセキュリティアーキテクチャ。
GFAC	Generalized Framework for Access Control GFACとは、データを変更可能にする権限や、執行、決断、アクセス制御データの分離、などの一般的なフレームワーク法である。
IPsec	IPパケットの機密性及び、完全性を保証するための機構を備えたプロトコルで、VPNを実現するために最も良く利用される。
ITSEC	Information Technology Security Evaluation Criteria 1990年代始めにヨーロッパで開発されたITセキュリティ評価基準。
Kerberos	ネットワーク認証プロトコル。安全性の低いインターネットを介した2台のホスト間で双方向の認証を可能にするプロトコル。Key Distribution Center(KDC)と呼ばれる仲介サーバを利用するという特徴を持つ。
LOMAC	Low Water-Mark Mandatory Access Control フリーUNIXのカーネルをターゲットとして開発されている、強制アクセス制御機能を提供するロードブルカーネルモジュール。開発元はNetworks Associates, inc.のセキュリティ調査部門NAI Labsである。
LSM	Linux Security Module Linuxシステムにおいて、合理的にセキュリティ拡張パッケージをサポートするためのフレームワークとなるロードブルカーネルモジュール。
MAC	Mandatory Access Control 強制アクセス制御 「アクセス制御」参照。
MD5	Message Digest #5 メッセージダイジェスト関数アルゴリズムのうちの1つ。1方向ハッシュ関数。
MLD	Multi Level Directory 異なる機密ラベルを持つファイルとサブディレクトリを格納できるディレクトリ。
MLS	Multi-Level Security MLSとは、機密レベルの異なる複数のユーザが同時にシステムへアクセスできることを言う。MLSを採用したシステムでは、各ユーザはアクセスを許可されたデータだけにアクセスできる。

用語	説明
NAI	Network Associates Technology, inc. 米国のネットワークやセキュリティ関連の企業。2000/3/16には、米国防省(DOD: Department of Defense)から軍用ネットワークのセキュリティ機能強化プロジェクトに関し3年間650万ドルの契約を獲得した。
NSA	The National Security Agency 国家安全保障局は国防総省の所属機関。
poly-instantiation/polyinstantiated object	ラベル付けによる MAC において、同じディレクトリに名前が同一のファイルでも、付与されているラベルによって異なるファイルとして扱われるオブジェクトのこと。
RBAC	Role-Based Access Control オブジェクトに対するアクセスのパーミッションを役割(role)に関連付け、この役割をユーザに割り当てることによって、ユーザにその役割に許可されたパーミッションを獲得させるアクセス制御方式。
RIPEND	RIPEND は、ヨーロッパの RACE Integrity Primitives Evaluation(RIPE)プロジェクトのために開発された。128 ビットのハッシュ値を生成していたが、アルゴリズムを強力し、RIPEND-160 と名前を変え、160 ビットのメッセージダイジェストを生成するように変更された。
role	ユーザをその役割に応じて分類するためのセキュリティラベル。
RSA	1977年にマサチューセッツ工科大学の3人の技術者、Rivest、Shamir、Adleman が発表した公開鍵暗号化方式の規格である。これは Diffie-Hellman 鍵交換方式の考え方をベースにしている。RSA による暗号の強さは、非常に大きい数は因数分解することが難しいと言う事実に基づいている。
SHA1	Secure Hash Algorithm 1 SHA1 は、Secure Hash Standard(SHS)の一部として NSA により開発された。最初に発行されたアルゴリズムは改良され SHA1 と名づけられ、160 ビットのメッセージダイジェストを生成する。
SLD	Single Level Directory 同一の機密ラベルを持つファイルとサブディレクトリを格納する、MLD 内の隠しサブディレクトリ。
TCSEC	Trusted Computer System Evaluation Criteria 1980年代始めにアメリカで開発された IT セキュリティ評価基準。
TE	Type Enforcement サブジェクトがアクセス可能なオブジェクトを必要最小限に規制する強制アクセス制御技術。サブジェクト及び、オブジェクトにはこのアクセス制御のために利用されるラベルが付与される。それらは、domain 及び、type と呼ばれる。
type	強制アクセス制御技術の1つである Type Enforcement にて、アクセス制御のために利用されるラベル。この type ラベルは、適切なセキュリティポリシーに基づいてあらかじめオブジェクトに対して付与される。

用語	説明
VPN	Virtual Private Network インターネット上に実現される、あたかも自分だけが利用できるプライベートな仮想ネットワーク。VPNの実現には、暗号や認証の技術が利用される。
アクセス制御	アクセス制御には強制アクセス制御 (MAC: Mandatory Access Control) 及び、任意アクセス制御 (DAC: Discretionary Access Control) がある。MAC は、システムのサブジェクトとオブジェクトの関連を強制的なセキュリティポリシーとして定義し、システムがそのアクセス制御方針を運用するアクセス制御方式。DAC は、ユーザ ID あるいは、グループ ID に基づいてオブジェクトへのアクセスを制御するアクセス制御方式。
オブジェクト	サブジェクトによってアクセスされる受動的な実体。ファイル、ディレクトリ、ソケット等が該当する。オブジェクトにはタイプが割り当てられる。タイプとは、オブジェクトに関連するセキュリティ属性を表すものであり、オブジェクトは割り当てられたタイプによって分類され、アクセスを制御される。
オレンジブック	TCSEC の通称。
カテゴリ	コンパートメントともいう。機密ラベルの項目の一つであり、情報の分野を表す。
サービス妨害攻撃	Denial of Service attack インターネットサーバ(例えば、Web サーバ)に対して、大量のリクエストパケットを送りつけ、その結果サーバの資源を使い尽くして、システムを利用できない状態に陥れる攻撃方法。
サブジェクト	オブジェクトにアクセスを行う能動的な実体。ユーザ、プロセス等が該当する。
セキュリティポリシー	Security Policy 広義では、企業等の組織内でのセキュリティに関する方針のこと。狭義では、システムにおけるアクセス制御における制御方針。
セキュリティラベル	オブジェクトのセキュリティレベルを表すラベル。
セキュリティレベル	情報の重要度を表すもので、センシティブティラベル(機密種別とカテゴリで構成される)に基づく。センシティブティラベルとは、オブジェクトのセキュリティレベルを表すとともに、オブジェクトが有するデータの機密レベルを示すラベルである。強制アクセス制御を採用するシステムでは、センシティブティラベルに基づいて、サブジェクトにオブジェクトへのアクセスを許可するかどうか決定される。
パーミッション	サブジェクトとオブジェクトのアクセス権の関係で、ファイルに対するパーミッションには、読み取り・書き込み・実行がある。
ラベル付け	オブジェクトに対して、セキュリティラベルを付与すること。
悪意あるコード	システムに対して不正な行ためを働くべく作成されたコード。
悪意あるモバイルコード	インターネット上に存在する悪意あるコード。

用語	説明
完全性	Integrity 情報セキュリティの目標事項のひとつ。正確で完全であり、データとそれを格納する情報システムが正確で完全であることを確保する。故意または偶然による情報の改竄や破壊の防止を目的とするセキュリティ概念。情報の偽造や改竄を防止する。
監査	監査とは、高信頼システムにおいてセキュリティ関連の操作を記録、調査、検証することである。監査の分野では、サブジェクトからオブジェクトへのアクセスに関連した操作をイベントと呼び、監査のことをイベントロギングという。
機密ラベル	sensitivity label サブジェクトとオブジェクトに付与される機密度を表すラベル。機密種別とカテゴリで構成される。
機密情報	Sensitive Information 悪用されたり改竄されたりすると所有者やシステムに多大な影響を与えるような情報。
許可上限	clearances ユーザに割り当てられた機密ラベル。ユーザがアクセスできる情報の上限を設定するものである。
最小特権	least privilege 従来のシステムのように root ユーザにすべての権限を与えるのではなく、そのプロセスまたはユーザがプログラムを実行するのに必要な最低限の権限を与えるセキュリティの概念である。
特権	privilege ユーザ、プロセス、プログラムに与えられる特別な権限で、ファイルへのアクセス権限などをいう。通常、重要なシステム資源へのアクセスはシステム管理者だけに与えられる。
認可	authorization 認証の後に、各ユーザのシステム資源へのアクセスを権限に応じて許可する過程。典型的には、ACL (Access Control List) の機構が利用されている。
認証	authentication 認証、もしくは本人認証は、ユーザが本人であることを証明する過程をいう。認証のプロセスは、典型的には、ユーザの知識として自らの名前とパスワードやパスフレーズの入力を本人であることの証拠として要求する。近年、ユーザの持ち物（例：スマートカード）や、ユーザの身体的特徴（バイオメトリクス）に基づく認証機構も普及しつつある。