7.1 概要

LIDS（Linux Intrusion Detection System）とSELinux（Security-Enhanced Linux）は，いずれも，Linuxカーネルに組み込まれたセキュリティ・ツールで，UNIX/Linuxの従来からの利用者（管理者rootと一般ユーザ）とアクセス属性（ディレクトリとファイル）のみで構成・制御されるセキュリティのメカニズムからよりきめ細かなセキュリティ・メカニズムへと転換させるものです．

従来のアクセス権限は実行されるプログラムのユーザIDと，ファイルやディレクトリ（のアクセス属性）とが個別に決まるもので，DAC（Discretionary Access Control；任意アクセス制御）と呼ばれます．

一方，セキュアOSでは，ユーザとファイルやディレクトリ，さらに実行プロセスなどを組み合わせてアクセス権限を限定してセキュリティ制御します．システム内でのアクセスをより細かく制限することでシステムの侵害を防止可能になります．そのため，単にrootであるからシステム・ファイルにアクセスできるとか，所有者であるから自分のファイルへアクセスできるなどというわけにはいきません．こうした仕組みをMAC（Mandatory Access Control；強制アクセス制御）と呼びます．

同じ，セキュアOSでもLIDSは，MACをある程度簡単な設定・制御でアクセス権限を制限設定しますが，SELinuxではより詳細な（したがって，より複雑な）設定・制御で制限設定します．

7.2 LIDS

LIDSは，ファイルへのアクセス権限とプロセスのケーパビリティ（capability；アクセス能力）とを組み合わせたルールをアクセス権限リストACL（Access Control List；アクセス制御リスト）として登録し，この登録された一つ一つのエントリ（ルール）によりアクセスを制御します．これをさらに，システムのステート（稼働状態）に応じて設定して，アクセスを厳密に規定したセキュリティ制御です．

LIDSのACL設定はiptablesのようなルール設定で，設定後の保存ファイルは`passwd`ファイルのような形式の設定・保存形式となっています．

なお，ここで使用するLIDSは次のようなパッケージです．

kernel 2.6.25/2.6.26用パッチLIDS 2.2.3rc5：`lids-2.2.3rc5-2.6.25.patch`

lidstoolsパッケージ：lidstools-2.2.7.5.tar.gz

7.2.1 LIDSのセキュリティ制御の仕組み

LIDSでは，アクセスを実行するアプリケーション（バイナリやスクリプトなどのプログラム）をサブジェクト，ファイルやディレクトリなどアクセス対象（そして，権限）をオブジェクトと呼びます．そして，あるサブジェクトがあるオブジェクトに対して処理を行う場合に，サブジェクトに対するルール，あるいは，そのオブジェクトに対するルール，さらには，その両方に対するルールをもとにその処理の範囲（読んだり，書いたりなどの範囲）が限定されることになります．

つまり，システム上のすべての処理が，サブジェクトとオブジェクトという要素のアクセスの権限や能力の範囲内でしか行えないようにして，管理者（あるいは，管理者のプログラム）であればすべてのアクセスが可能になる，という全権を与える従来のUNIX/Linuxの属性処理（DAC）ではない厳密なセキュリティ制御の仕組みを提供します．これがLIDSのセキュリティ制御です．

LIDSでは，このサブジェクトとオブジェクトのアクセスをシステムの稼働状態に応じて設定することで，システム・ブート時のモジュール組み込みについても，管理者（あるいは管理者プログラム）であっても制限することが可能になります．

なお，LIDSでは，コマンドとしてLIDS設定用の`lidsconf`とLIDS運用・制御用の`lidsadm`という2種類のコマンドを使用します．

7.2.2 LIDSのセキュリティ制限の設定

サブジェクトとしてのプロセスやオブジェクトとしてのファイルに対するセキュリティ制限はACLのルールというかたちで一つ一つ設定していきます．

ファイルへのアクセス制限

ファイルに対するアクセス権限設定には，次の四つがあります．

DENY	：アクセス禁止
READONLY	：読み込みのみ許可
APPEND	：読み込みと追加を許可
WRITE	：すべて（読み書き，および，削除）を許可

なお，これらのアクセス権限は，通常のLinuxのファイル属性よりも優先されます．

プロセスのケーパビリティ

プロセスのアクセス能力（ケーパビリティ）には，**リスト7.1**のようなものがあります．

これらのケーパビリティを与えるか否かなどの操作設定には，次のようなものがあります．

GRANT：ケーパビリティを与える（一般のケーパビリティに対するもの）
ENABLE/DISABLE：ケーパビリティを有効/無効にする（拡張機能のみに適用）

リスト7.1　LIDSケーパビリティの一覧

```
●一般ケーパビリティ
    CAP_CHOWN          ：chown/chgrp
    CAP_DAC_OVERRIDE：DACアクセス
    CAP_DAC_READ_SEARCH：DAC読み込み
    CAP_FOWNER         ：ユーザID とオーナID 違い
    CAP_FSETID         ：実行ユーザID とオーナID 違い
    CAP_KILL           ：実有効ID とプロセスID違い
    CAP_SETGID         ：setgid
    CAP_SETUID         ：set*uid
    CAP_SETPCAP        ：転送権限
    CAP_LINUX_IMMUTABLE：不変か，付け加えられるファイル特性
    CAP_NET_BIND_SERVICE：1024未満のポートへのバインディング
    CAP_NET_BROADCAST：マルチキャストのブロードキャスト/リスニング
    CAP_NET_ADMIN    ：インターフェース/ファイア・ウォール/ルーティング 変更
    CAP_NET_RAW        ：RAWソケット（ping）
    CAP_IPC_LOCK     ：共有メモリ・セグメントのロック
    CAP_IPC_OWNER    ：IPC所有者のチェック
    CAP_SYS_MODULE   ：カーネルモジュールの挿入と削除
    CAP_SYS_RAWIO    ：ioperm/ioplアクセス
    CAP_SYS_CHROOT   ：chroot
    CAP_SYS_PTRACE   ：ptrace
    CAP_SYS_PACCT    ：プロセス・アカウンティングの設定
    CAP_SYS_ADMIN    ：管理者の重み
    CAP_SYS_BOOT     ：reboot
    CAP_SYS_NICE     ：nice
    CAP_SYS_RESOURCE：リソース制限の設定
    CAP_SYS_TIME     ：システム時間の設定
    CAP_SYS_TTY_CONFIG：TTY設定
    CAP_MKNOD          ：mknodの特別な許可
    CAP_LEASE          ：ファイルにリースを許可
    CAP_HIDDEN         ：システムからプログラムを隠す

●拡張ケーパビリティ
    LIDS_CAP_KILL_PROTECTED（旧CAP_KILL_PROTECTED）：保護されているプロセスを
                                                    killさせる機能
    LIDS_CAP_PROTECTED（旧CAP_PROTECTED）：シグナルからプロセスを保護
    LIDS_EXEC          ：ほかのプログラムの起動
    LIDS_SANDBOX       ：サンドボックス化機能
    LIDS_SOCKET_CREATE       ：ソケットの作成
```

```
LIDS_SOCKET_CREATE_TCP ：TCPソケットの作成
LIDS_SOCKET_CREATE_UDP ：UDPソケットの作成
LIDS_SOCKET_CONNECT    ：ソケットの接続
LIDS_SOCKET_BIND       ：ソケットのbind
```

ACLの設定方法

LIDSのACL設定は，lidsconfコマンドでACLエントリのルールを追加していくことで行います．主なコマンドは次のようなものです．

```
lidsconf -A <ACLルール>（ACLへのルールの追加）
lidsconf -D <ACLルール>（ACLからのルールの削除）
lidsconf -Z            （ACLからの全ルールの削除）
```

これらの設定はlids.confファイル(*7.1)に変換保存されます．

なお，lidsconfコマンドで権限を設定するときは，LIDS が無効になっているか，LFS (*7.2)になっている必要があります．

また，ACL設定を行ったあとは必ず，有効化するために次のコマンドを実行する必要があります．

```
lidsconf -C     （lids.confとlids.capからlids.*.aclの再生成）(*7.3)
lidsadm -S -- +RELOAD_CONF     （リロード．カーネルへの読み込み）
（または，システム再起動）
```

そのほか，ACL設定の基本的な設定手順は，

① システム全体のデフォルトの設定を行う

② 各サブジェクト，各オブジェクトの設定を行う

というような手順が一般的です．

なお，ACL設定したファイルやプログラムなどを置き換えたりした場合などファイル・システムのiノード番号が変わった場合には，必ず次のコマンドでACLの更新を行っておく必要があります(ACLのファイルやプログラムなどファイル・システム関係の設定は，iノード番号をもとに行っているため)．

```
lidsconf -U（ACL設定のiノード番号の更新）
```

この点は特に注意が必要な重要ポイントです．システム関係のファイルは，ACL設定されたものが多く，そのため，viなどで設定変更した場合には，iノード番号が変わるために，ACL設定が正常には動作しなくなる場合がしばしば起こります．したがって，システム・ファイルなどの変更後(特に，/etc/lids内のlids設定ファイルの変更時に注意)は，必ずこの更新を行って(リロードして)反映を有効にしなければなりません．

なお，ACL設定を行うときには，あらかじめ(念のため)「lidsconf -U」，

(*7.1) **lids.confファイル**：lidsconfで自動生成されるLIDSのACL設定ファイル．

(*7.2) LFS：LIDS Free Session．LIDS有効下でLIDS設定を行える状態．後述．

(*7.3) **lids.cap**：lids.confから生成されるLIDSのACL権限ファイル．
lids.*.acl：LIDSのステートに対応したACLの実体でカーネル組込用のバイナリ・ファイル．