暗号化 USBFlashDisk デバイスの取り扱いについて

版	日付		記述			
	発行		作成	確認	承認	
版	日付		記述			
	発行		作成	確認	承認	
版	日付	2017/12/05	記述	新規発行		
1	発行	プロフェッショナルサービス	作成	大島龍博	確認	承認

初めに

暗号化ファイルシステムとして、Linux では、cryptsetup が、Windows10 では、BitLocker が標準で搭載されている。

本書では、RedHawk Linux 上で、暗号化 USB Flash Disk デバイスについての使用方法を示す。

cryptsetup

cryptsetup を利用して、LUKS(Linux Unified Key Setup)をコマンドラインから使用する方法を下記に示す。

デバイスを認識することが可能であれば、下記　/dev/sdb1　の様に認識される。

```
# dmesg|tail
[ 8137.338708] scsi 10:0:0:0: Direct-Access     Flash      Drive UT_USB20     0.00 PQ: 0 ANSI: 2
[ 8137.338881] sd 10:0:0:0: Attached scsi generic sg2 type 0
[ 8137.339700] sd 10:0:0:0: [sdb] 248000 512-byte logical blocks: (127 MB/121 MiB)
[ 8137.340317] sd 10:0:0:0: [sdb] Write Protect is off
[ 8137.340319] sd 10:0:0:0: [sdb] Mode Sense: 00 00 00 00
[ 8137.341071] sd 10:0:0:0: [sdb] Asking for cache data failed
[ 8137.341074] sd 10:0:0:0: [sdb] Assuming drive cache: write through
[ 8137.372971]  sdb: sdb1
[ 8137.375596] sd 10:0:0:0: [sdb] Attached SCSI removable disk
[ 8780.410946] NET: Registered protocol family 38
```

この/dev/sdb1 に対して、初期化を行う。この際、必ず大文字３文字で”YES”を入力する事。その後、パスフレーズ（パスワード）の入力を行なうが、大文字、小文字、数字を混ぜて 8 文字以上で、英数交じりのパスフレーズが必要である。

まず、ptadmin で登録を行い、正常にマウントされている状態で、以下の操作をコマンドラインで行う必要がある。

```
# umount /dev/sdb1
# cryptsetup luksFormat /dev/sdb1

WARNING!
========
This will overwrite data on /dev/sdb1 irrevocably.

Are you sure? (Type uppercase yes): YES
Enter passphrase:  パスフレーズを入力
Verify passphrase:  パスフレーズを入力
```

「-c」オプションや「-s」オプションを使用して、 暗号化方式や鍵の長さを指定することも出来る。

cryptsetup -c 暗号化方式 -s 鍵長 luksFormat デバイスファイル

デフォルトの暗号化方式は、aes-cbc-essiv:sha256 。

初期化が終了すると、下記のように（open 後）使用することが可能になり、/dev/mapper 下にデバイスが表示される。

```
# ls /dev/mapper/
centos-home   centos-root   centos-swap   control

# cryptsetup luksOpen /dev/sdb1 USBFlash
Enter passphrase for /dev/sdb1: パスフレーズを入力

# ls /dev/mapper/
USBFlash   centos-home   centos-root   centos-swap   control
```

名称は何でもよい

/dev/mapper 下にデバイスが表示されたら、通常の ext2,ext3,ext4 か xfs としてファイルシステムとしてフォーマットが出来るが、windows 系のファイルフォーマット(fat,vfat 等)は使用できない、以下にその他の注意事項を示す。

- RedHawk V7.0.x で、xfs フォーマットしたメディアは、RedHawk6.0.x でマウントエラーが発生することがある。
- RedHawkV6.0.x で xfs フォーマットしたものは、その他の版で利用可能。
- ext4 ファイルフォーマットは、RedHawk7.x 以外では利用できない。
- 全ての RedHawk で LUKS を使用するには、ext2,ext3 ファイルを利用する事。

```
# mkfs.ext3 /dev/mapper/USBFlash
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
OS type: Linux
Block size=1024 (log=0)
Fragment size=1024 (log=0)
Stride=0 blocks, Stripe width=0 blocks
30600 inodes, 121936 blocks
6096 blocks (5.00%) reserved for the super user
First data block=1
Maximum filesystem blocks=67371008
15 block groups
8192 blocks per group, 8192 fragments per group
2040 inodes per group
Superblock backups stored on blocks:
        8193, 24577, 40961, 57345, 73729

Allocating group tables: done
Writing inode tables: done
Creating journal (4096 blocks): done
Writing superblocks and filesystem accounting information: done
```

又は

```
# mkfs.xfs -f /dev/mapper/USBFlash
meta-data=/dev/mapper/EncriptUSB isize=256    agcount=4, agsize=7621 blks
         =                       sectsz=512   attr=2, projid32bit=1
         =                       crc=0        finobt=0
data     =                       bsize=4096   blocks=30484, imaxpct=25
         =                       sunit=0      swidth=0 blks
naming   =version 2              bsize=4096   ascii-ci=0 ftype=0
log      =internal log           bsize=4096   blocks=853, version=2
         =                       sectsz=512   sunit=0 blks, lazy-count=1
realtime =none                   extsz=4096   blocks=0, rtextents=0
```

フォーマットが終了すると通常のようにマウントして使用することが出来る。

```
# mount /dev/mapper/USBFlash /mnt
# df -T
ファイルシス                タイプ     1K-ブロック       使用      使用可 使用% マウント位置
devtmpfs                    devtmpfs      6056676          0     6056676       0% /dev
tmpfs                       tmpfs         6084172        188     6083984       1% /dev/shm
tmpfs                       tmpfs         6084172       9388     6074784       1% /run
tmpfs                       tmpfs         6084172          0     6084172       0% /sys/fs/cgroup
/dev/mapper/centos-root xfs              52403200 13549344    38853856      26% /
none                        tmpfs         6084172     132264     5951908       3% /tmp
/dev/sda1                   xfs           5621760     617188     5004572      11% /boot
/dev/mapper/centos-home xfs             911897560    2138712 909758848       1% /home
tmpfs                       tmpfs         1216836         12     1216824       1% /run/user/0
/dev/mapper/USBFlash    ext3            113972       1567      106309       2% /mnt

# umount /mnt
```

Open した暗号化ファイルシステムを Close する。

```
# cryptsetup luksClose USBFlash
```

正常に終了すると、USBFlashDisk 挿入時に以下のパスフレーズを入力するための、ポップアップダイアログが表示され、パスフレーズが一致すれば、通常使用が可能になる。

正常にマウントされた場合には、デスクトップ上には、鍵付きアイコンが表示されている。

BitLocker

Windows10 の BitLocker によって暗号化されたディスクを、Linux で読取り専用マウントする手順を以下に示す。

下記手順では、ディスクの内容すべてを復号化し、Linux 上のディスクイメージファイルとしてコピーが生成され、そのイメージファイルをループバックデバイスとしてマウントする。

このため、ディスクイメージファイルと同等の領域を必要とする。

下記手順では、コピー先のテンポラリ領域に、tmpfs(RAMDISK)を使用するが、実ファイルでも可能である。この際、コピー先のイメージファイルは手動で消去する必要がある。

1. **CentOS のリポジトリから、下記、3 つの RPM ファイルをダウンロードしてインストールする。**

RedHawk6.x の場合

- https://centos.pkgs.org/6/epel-x86_64/mbedtls-2.6.0-1.el6.x86_64.rpm.html
- https://centos.pkgs.org/6/epel-x86_64/dislocker-libs-0.7.1-1.el6.x86_64.rpm.html
- https://centos.pkgs.org/6/epel-x86_64/dislocker-0.7.1-1.el6.x86_64.rpm.html

RedHawk7.x の場合

- https://centos.pkgs.org/7/epel-x86_64/mbedtls-2.6.0-1.el7.x86_64.rpm.html
- https://centos.pkgs.org/7/epel-x86_64/dislocker-libs-0.7.1-1.el7.x86_64.rpm.html
- https://centos.pkgs.org/7/epel-x86_64/dislocker-0.7.1-1.el7.x86_64.rpm.html

```
# rpm -ivh mbedtls-2.6.0-1.el7.x86_64.rpm
警告: mbedtls-2.6.0-1.el7.x86_64.rpm: ヘッダー V3 RSA/SHA256 Signature、鍵 ID 352c64e5: NOKEY
準備しています...                ################################# [100%]
更新中 / インストール中...
   1:mbedtls-2.6.0-1.el7         ################################# [100%]

# rpm -ivh dislocker-libs-0.7.1-1.el7.x86_64.rpm
警告: dislocker-libs-0.7.1-1.el7.x86_64.rpm: ヘッダー V4 RSA/SHA1 Signature、鍵 ID 87e360b8: NOKEY
準備しています...                ################################# [100%]
更新中 / インストール中...
   1:dislocker-libs-0.7.1-1.el7  ################################# [100%]

# rpm -ivh dislocker-0.7.1-1.el7.x86_64.rpm
警告: dislocker-0.7.1-1.el7.x86_64.rpm: ヘッダー V4 RSA/SHA1 Signature、鍵 ID 87e360b8: NOKEY
準備しています...                ################################# [100%]
更新中 / インストール中...
   1:dislocker-0.7.1-1.el7       ################################# [100%]
```

2. tmpfs の作成

下記の例では、512M バイトの RAMDISK を生成している。

```
# mkdir /tmp/ramdisk
# mount -t tmpfs -o size=512m tmpfs /tmp/ramdisk
# df
ファイルシス                1K-ブロック       使用      使用可 使用% マウント位置
devtmpfs                    6056676          0     6056676       0% /dev
tmpfs                       6084172        204     6083968       1% /dev/shm
tmpfs                       6084172       9384     6074788       1% /run
tmpfs                       6084172          0     6084172       0% /sys/fs/cgroup
/dev/mapper/centos-root    52403200 13796676    38606524      27% /
none                        6084172     146908     5937264       3% /tmp
/dev/sda1                   5621760     617188     5004572      11% /boot
/dev/mapper/centos-home    911897560 2959260 908938300        1% /home
tmpfs                       1216836         20     1216816       1% /run/user/0
tmpfs                        524288          0      524288       0% /tmp/ramdisk
```

3. 暗号化ディスクの内容の復号化とコピー

下記の例では、デバイス/dev/sdb1 の内容を復号化し、/tmp/ramdisk 下の ntfs にコピーしている。

```
# dislocker -v -V /dev/sdb1 -u 暗号化パスワード -- /tmp/ramdisk/ntfs
```

4. 復号化されたディスクイメージのマウント

下記の例では、ディスクイメージファイルをループバックデバイスとして、/mnt にマウントしている。

```
# mount -o loop,ro /tmp/ramdisk/ntfs /mnt
# df
ファイルシス                1K-ブロック       使用      使用可 使用% マウント位置
devtmpfs                    6056676          0     6056676       0% /dev
tmpfs                       6084172        204     6083968       1% /dev/shm
tmpfs                       6084172       9384     6074788       1% /run
tmpfs                       6084172          0     6084172       0% /sys/fs/cgroup
/dev/mapper/centos-root    52403200 13796676    38606524      27% /
none                        6084172     147156     5937016       3% /tmp
/dev/sda1                   5621760     617188     5004572      11% /boot
/dev/mapper/centos-home    911897560 2959260 908938300        1% /home
tmpfs                       1216836         20     1216816       1% /run/user/0
tmpfs                        524288     123984      400304      24% /tmp/ramdisk
/dev/loop0                   123724       5436      118288       5% /mnt

# ls /mnt
System Volume Information    test.txt
```

5. 使用デバイスのアンマウント

使用後は、デバイスをアンマウントする。

```
# umount /mnt
# umount /tmp/ramdisk/
# df
ファイルシス                1K-ブロック       使用      使用可 使用% マウント位置
devtmpfs                       6056676          0     6056676       0% /dev
tmpfs                          6084172        204     6083968       1% /dev/shm
tmpfs                          6084172       9384     6074788       1% /run
tmpfs                          6084172          0     6084172       0% /sys/fs/cgroup
/dev/mapper/centos-root       52403200 13796676    38606524      27% /
none                           6084172     147156     5937016       3% /tmp
/dev/sda1                      5621760     617188     5004572      11% /boot
/dev/mapper/centos-home      911897560 2959260 908938300       1% /home
tmpfs                          1216836         20     1216816       1% /run/user/0
```