PART 9

# 緊急時の対応例

本章では、CompuSec導入後にコンピューターが起動できなくなった場合の例を挙げ、その対応について記載しております。各項目に該当しない場合は、サポートセンターまでご連絡ください。

## 9-1　CompuSecをアンインストールせずにリカバリーした

リカバリーシステムがMBR領域までリカバリーしない場合が多く、リカバリー中の再起動などで、リカバリーが続行できないなどの現象が見られます。
この様な場合は、「10 オリジナルのMBRを復元する」に従って、MBRを復元してください。

オリジナルMBRが無い場合は、Windows® のセットアップディスクを使ったMBR修正方法にて代用してください。

- Windows® 7、Windows Vista® については、「11 Windows® 7、Windows Vista® の回復環境でMBRを修正する」を参照してください。

- Windows® XPについては、「12 Windows® の回復コンソールでFIXMBRを行う」を、参照してください。

オリジナルのMBRデータが無く、MBRの修正のみを行った場合、MBRのセクター1にCompuSecで書き込んだ内容が残るため、リカバリー後でもCompuSecのインストールはできません。その際はサポートセンターまでご連絡ください。

## 9-2　暗号化／復号中に、強制的に電源をオフにした

電源オフに限らず、処理中にWindows®がハングアップした場合も、基本的にハードディスク内容が読めなくなってしまい、お客さまでは処理できない状態となってしまいます。
この場合、原則として工場出荷時にリカバリーするより他に方法がございません。
ただしライセンス版ユーザーの場合、有償メニューで「PC復旧パック」をご用意しておりますので、サポートセンターまでお問い合わせください。

## 9-3　ブート前認証後、OSが起動せず（暗号化なし）

ハードディスクが暗号化されておらず、OS側の障害により起動できない場合は、通常通りWindows®の修復や上書きインストールなどを行ってください。
または、別のPCへハードディスクを接続し、データを退避後、ハードディスクを障害PCに戻してから、オリジナルMBRの復元「10 オリジナルのMBRを復元する」とシステムのリカバリーを行ってください。

## 9-4　ブート前認証後、OSが起動せず（暗号化済み）

ハードディスクが暗号化済みで、OSの障害により起動できない場合は、ブート前サービス機能の「8-1-6 緊急時の復号」を使って、復号してください。
その後は、通常通りWindows®の修復や上書きインストールするか、データを退避後にオリジナルのMBRを復元し、システムをリカバリーするなどを行ってください。

## 9-5　ブート前認証画面が表示せず or 認証不可（暗号化なし）

まず、オリジナルのMBRを復元「10 オリジナルのMBRを復元する」してWindows®が起動することを確認してください。Windows®が起動するならば、先にお客さまデータの退避を行い、システムのリカバリーをお勧めいたします。
リカバリーをせず、そのシステムで引き続き運用する場合は、強制アンインストールを行うことになりますので、サポートセンターまでご連絡ください。

## 9-6　ブート前認証画面が表示せず or 認証不可（暗号化済み）

ブート前認証が行えないと、「緊急時の復号」による復号処理ができません。この様な場合は、別のPCにCompuSecをセットアップし、**2台目以降の内蔵ハードディスクとして接続し**、データの退避や復号などを行ってください。

別のPCにCompuSecを導入する際は、

- **CompuSec単体版**
  障害PCへCompuSecを導入した際に生成された、SecurityInfo.datファイルからハードディスクの暗号化キーを読み込ませてください。
  USB接続のハードディスクケースなどを使う場合は、ハードディスクの暗号化キーを一旦読み込み、リムーバブルメディアキー部に同じ数値を手動で書き込んでください。

- **GlobalAdmin管理下**
  **障害PCと同じコンピューター名に設定し**、インストールしてください。

  GlobalAdmin管理下では、ハードディスクの暗号化キーを、リムーバブルメディアキーに設定することができませんので、USB接続のハードディスクケースなどを使ってのディスク参照は不可能です。

なお、ハードディスク上のデータに構わずリカバリーを行って良い場合は、オリジナルのMBRを復元後に、リカバリーを行ってください。

# オリジナルのMBRを復元する

CompuSecをアンインストールせずに、システムのリカバリーを行うと、MBR領域まで復元されるかどうかは、PCメーカーや機種などにより異なります。
また、バックアップソフトを使って復元させた場合にも同様のことが考えられます。
このため、リカバリー後にもCompuSecの認証画面が表示されたり、CompuSecのインストールができない場合があります。
これは、CompuSecをインストールする際に保存した、オリジナルのMBRを復元することで回避できます。

**注意**

**CompuSecをインストールする際に保存した .mbrファイルは、PCメーカーさまオリジナルのMBRデータとなりますので、CompuSecを再インストールする際は、上書きせず、別途保管しておいてください。**

**この手順は、原則として緊急避難的に操作していただく内容ですので、お客さまにて操作を間違えた、改変したMBRを組み込んで、PCの動作がおかしくなったなどに対する保証は致しかねますことをご承知ください。**

**※CompuSec 4.18.6以降のバージョンでは、CompuSec自身がインストール先フォルダー内（C:\Program Files\CE-Infosys\CompuSec）に、compusec_track0_backup.datと言うファイル名で、MBRデータを保存しています。但し、こちらはアンインストール時に削除されます。**

**重要**
**ハードディスクが暗号化されている状態では、MBRの復元を行わないでください！**

## 10-1　インストールランチャーによるMBRの復元

CompuSecのインストールCDを挿入すると、インストールランチャーが起動します。
このインストールランチャーから、MBRを復元させることができます。
ダウンロード版やGlobalAdmin管理のCompuSecのインストールランチャーにも、同じ機能があります。

**重要**
**但し、Windows® 上からMBRを復元させる場合は、必ずCompuSecがアンインストールされた状態か、システムをリカバリーした後に行ってください。CompuSecはMBRを保護していますので、Windows® 上からでは正常にMBRを復元できません。**

**1** Windows® が起動している状態で、CompuSecのインストールCDを挿入すると、インストールランチャーが起動します。自動で起動しない場合や、ダウンロード版では、「csinstall(インストールはこちら).exe」を、直接実行してください。

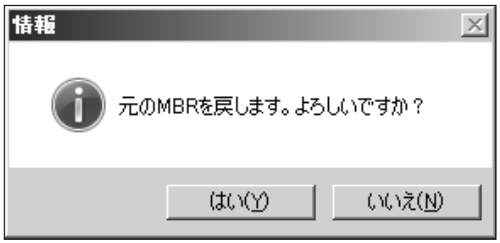
**2**


この画面が表示されている状態で、キーボードよりCtrl + 3を入力してください。（Ctrlを押しながら、テンキーではない方の3のキーを押してください）

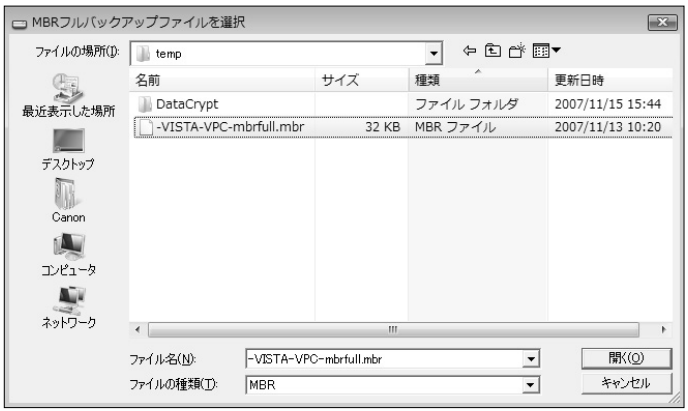
**3**


右上部に「MBRの復元］ボタンが表示されます。

**4**




［MBRの復元］をクリックし、確認メッセージに対して［はい］をクリックしてください。




CompuSec導入時に保存したMBRファイルを選択し、［開く］をクリックしてください。

**5**


MBRの復元に成功すると、次のメッセージが表示されますので、［OK］をクリック後、必ずPCを再起動してください。

再起動後、Windows® が起動するかをご確認ください。

## 10-2　ツールFDによるMBRの復元

**1**


まず、PCを起動できるフロッピーディスクを作成します。
Windows® 7 / XP、Windows Vista®）が動作しているPCで、フロッピーディスクをフォーマットしてください。
その際「MS-DOSの起動ディスクを作成する」にチェックを入れて、実行してください。

**2**

ツールプログラムを、フロッピーディスクへコピーします。
CompuSecインストールCD内または、ダウンロードしたものを展開後の、\tool\mbr_RWフォルダー内にあるファイルをすべて、作成した起動ディスクへコピーします。

**3**

CompuSec導入時に保存した、オリジナルのMBRデータを、mbrfull.mbr と言うファイル名へ変更して、フロッピーディスクへコピーしてください。

**4**

このフロッピーディスクで、問題のPCを起動してください。

**5**

しばらくすると画面にDOSプロンプト（a:＼>）が表示されますので、
mbr［Enter］
と入力してください。（mbr.batを実行します）
a:＼>　mbr　［Enter］
（［Enter］は、Enterキーです）

**6** 画面に、次のようなメッセージが表示されます。

作成したフロッピーディスクには、日本語フォントの設定がありませんので、日本語部は文字化けし、正常に表示されません。

```
実行するオプションを選択してください。(番号入力)
0-62までのセクタをバックアップします    : 1
0-62までのセクタをリストアします        : 2
終了                                    : 0

Select a option you want to execute.(Enter number)
Back up the sectors from 0 - 62         : 1
Restore the backup sectors              : 2
Exit                                    : 0
```

**7** MBRデータを復元しますので、キーボードより「2」を入力してください。

**8** MBRを処理している画面がしばらく続き、再度**6**項のメッセージが表示されますので、「0」を押して終了します。

**9** フロッピーディスクを取り出し、PCを再起動させ、Windows®が起動することを確認してください。

PART 11

# Windows® 7、Windows Vista® の回復環境でMBRを修正する

**ハードディスクが暗号化されている場合は、BOOTRECを実行してもWindows®を起動することはできませんので、暗号化されたままBOOTRECを実行しないでください。**
**事前に、ハードディスクの復号処理を済ませておく必要があります。**

Windows® 7、Windows Vista®の回復環境で、BOOTRECコマンドを発行すると、CompuSecが書き換えたMBRを、Microsoft®標準のMBRへ書き換えることができます。
**Windows®は起動するようになりますが、CompuSecで書き換えたMBRは複数セクターに渡るため、後でオリジナルのMBRに復元しておくことを忘れないでください。**

## 11-1　パッケージ製品のセットアップディスクで起動する

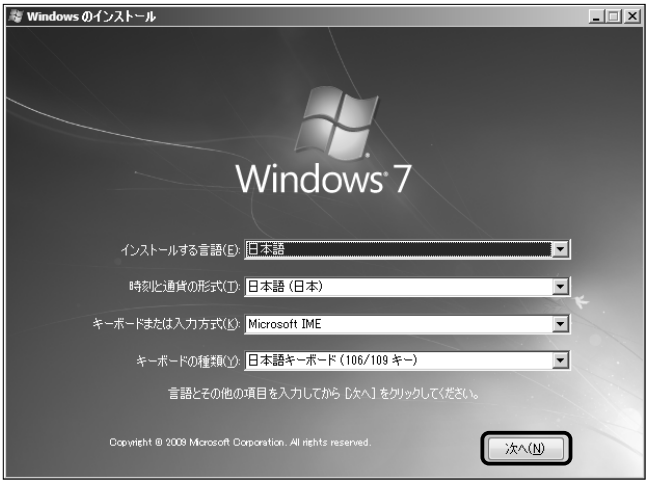
PCに添付されているリカバリー用ディスクでは、回復環境を起動できない場合が多いようです。
但し、リカバリーディスクのセット内容によっては、OSだけをインストールできるセットアップディスクが含まれている場合がありますので、念のためご確認ください。

基本的には、純粋なOSとしてのセットアップディスクが必要です。
Windows® 7、Windows Vista®のセットアップディスクを用意してください。

※DVDドライブから起動するには、BIOSの設定をし直さなければならない場合があります。DVDドライブから起動しない場合は、BIOS設定を確認してください。
USB外付けドライブの場合、古いPCまたはドライブでは、起動できない場合があります。

**1** DVDドライブにWindows® 7、Windows Vista®のセットアップディスクを入れ、PCを起動してください。

**2**

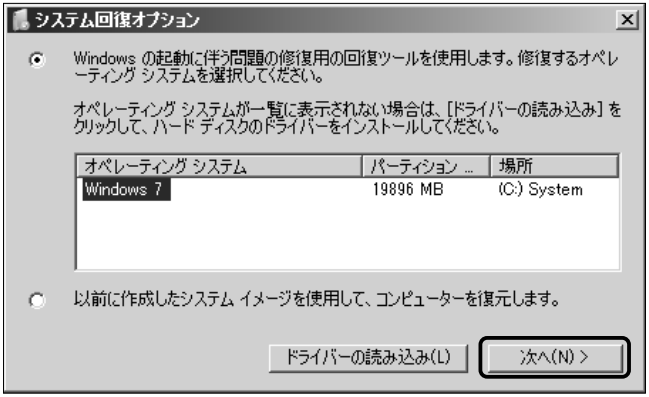



画面に「Press any key to boot from CD...」と表示されますので、何かのキーを押してください。この画面が表示されますので、[次へ]をクリックしてください。

**3**

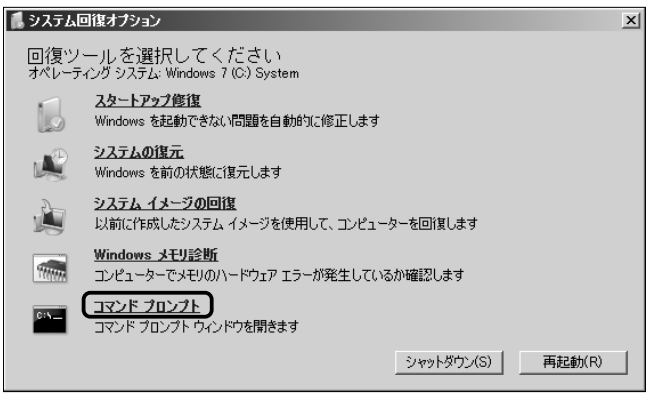

[コンピューターを修復する]をクリックしてください。

**4**



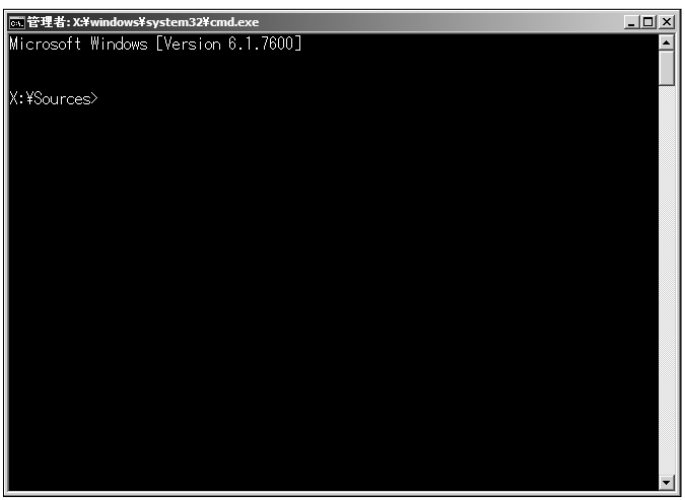

「システム回復オプション」の画面にて［次へ］をクリックしてください。

**5**




「回復ツールを選択してください」の画面で、「コマンドプロンプト」をクリックしてください。

**6**




コマンド入力用のウィンドウが表示されます。

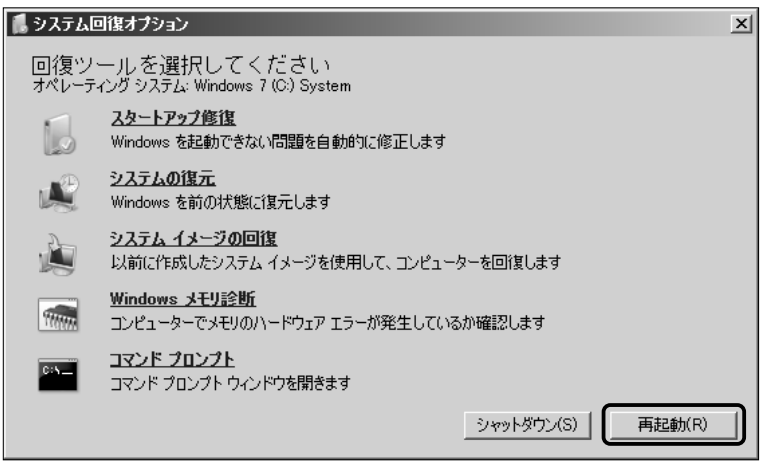
**7**


キーボードよりMBRを修復するコマンドとして、bootrec /fixmbr［Enter］と入力してください。
（［Enter］は、Enterキーです）

**8**


「操作は正常に終了しました。」とのメッセージが表示されたら、キーボードより exit［Enter］と入力して、ウィンドウを閉じてください。
（［Enter］は、Enterキーです）

**9**




［再起動］をクリックして、Windows Vista®セットアップディスクを取り出してください。

再起動後に、ブート前認証画面および、シングルサインオン画面が表示されず、Windows®のログオン方式でログオンできるかを確認してください。

PART 12

# Windows® XPの回復コンソールでFIXMBRを行う

**ハードディスクが暗号化されている場合は、FIXMBRを実行してもWindows®を起動することはできませんので、暗号化されたままFIXMBRを実行しないでください。**
**事前に、ハードディスクの復号処理を済ませておく必要があります。**

Windows® XPの回復コンソールを起動し、FIXMBRコマンドを発行することで、CompuSecが書き換えたMBRを、Microsoft®標準の物へ書き換えることができます。
**Windows®は起動するようになりますが、CompuSecで書き換えたMBRは、複数セクターに渡るため、後でオリジナルのMBRに復元しておくことを忘れないでください。**

※SATAタイプのハードディスクでは、BIOSでドライバーを切り替えることができない場合があります。その場合は、そのPC用のSATAドライバーを入手して、セットアップディスクで起動させる際にF6キーを押して、別途読み込ませてください。

## 12-1　パッケージ製品のセットアップディスクで起動する

コンピューターに添付されているリカバリーディスクで、回復コンソールを起動できない物が多いようです。
但し、リカバリーディスクのセット内容によっては、OSだけをインストールできるセットアップディスクが含まれている場合がありますので、念のためご確認ください。

基本的には、純粋なOSとしてのセットアップディスクが必要です。
Windows® XPのセットアップディスクを用意してください。

※CDドライブから起動するには、BIOSの設定をし直さなければならない場合があります。CDドライブから起動しない場合は、BIOS設定を確認してください。USB外付けドライブの場合、古いPCまたはドライブでは、起動できない場合があります。

1 CDドライブにWindows®のセットアップディスクを入れ、PCを起動します。

2 画面に「Press any key to boot from CD...」と表示されますので、何かのキーを押してください。

3 「セットアップへようこそ」というメッセージが表示されたら、Repair（修復）の「R」を押します。

4 キーボードのタイプを入力します。

## 12-2 Windows® XPのセットアップ起動FDで起動する

Microsoft®のWebサイトにて「Windows® XPのインストール用起動ディスクを入手する方法」（http://support.microsoft.com/kb/880422/ja）を参照し、起動ディスクを作成するためのモジュールを入手してください。

1 ダウンロードしたモジュールを実行すると、別ウィンドウが開き、起動用ディスクを作成するドライブ名を問い合わせてきます。
Aなど、該当するフロッピードライブ名を入力してください。
以降は、メッセージに従って、6枚の起動用フロッピーを作成します。

2 作成した起動用フロッピーの1枚目を使ってコンピューターを起動し、セットアップ画面が出るまで、2～6枚目までのフロッピーを差し替えていきます。

3 「セットアップの開始」という画面が表示されたら、R=修復（画面下に表示）の「R」を押します。

4 キーボードのタイプを入力します。

## 12-3　FIXMBRを実行

Windows® XPの回復コンソール起動後の操作となります。起動方法にかかわらず、共通の手順となっています。

**1** Windows® 回復コンソールが起動すると、次のメッセージが表示されます。

> Microsoft® Windows® XP（TM）回復コンソール。
>
> 回復コンソールはシステムの修復と回復機能を提供します。
> EXITと入力すると、回復コンソールを終了し、コンピュータを再起動します。
> 1：C:\WINDOWS
> どのWindows®インストールにログオンしますか？
> （取り消すにはEnterキーを押してください）

**2** 該当するWindows®の番号を入力してください。（1［Enter］）
（［Enter］は、Enterキーです）

**3** Administratorアカウントのパスワードを入力するように求められますので、入力してください。
（パスワードが無い場合は、Enterキーのみ入力）

**4** コマンドプロンプトが表示されます。（c:\Windows＞）

**5** C:\windows＞　に対して、FIXMBR［Enter］と、キーボードより入力してください。
（［Enter］は、Enterキーです）

**6** 「新しいMBRを書き込みますか？」との問い合わせに対し、Y［Enter］を入力してください。
「新しいブートレコードは正しく書き込まれました。」と表示されたら、終了です。

**7** C:\windows＞　に対して、EXIT［Enter］を実行すると、PCが再起動します。
（［Enter］は、Enterキーです）

**8** ブート前認証画面が表示されずに、Windows®が起動するかを確認してください。

# よくある質問と回答

## 13-1　システム関連

ここに挙げられていない事例に関しては、インターネットでCompuSecサポート情報ページ（http://canon-its.jp/supp/cs/）へアクセスしてご確認ください。

### Q1　CompuSecが対応しているOSはなんですか?

Windows® 7/ XP、Windows Vista®に対応しています。
CompuSecがインストールされた状態で、サービスパックの適用やMicrosoft® Updateを行うこともできます。
なお、本バージョン（5.2）よりWindows® 2000はサポート対象外です。

### Q2　CompuSec導入後にOSをアップグレードすることはできますか?

Windows® XPからWindows® 7などへの、OS自体が異なるようなアップグレードはできません。
CompuSecをアンインストールしてから、OSのアップグレードを行ってください。

### Q3　Windows® 7、Windows Vista® UltimateのBitLockerと共存できますか?

BitLockerが無効で且つ、CompuSecによるハードディスクの暗号化を行わなければ、共存できます。
**ハードディスクを暗号化したい場合は、「BitLockerのみ」または「CompuSecのみ」による暗号化としてください。**
**両方とも暗号化を実行してしまうと、システムの運用に支障をきたし、場合によっては正常に起動できなくなりますので、BitLockerとCompuSecを併用しての暗号化は行わないでください。**

### Q4　CompuSec導入後にWindows® 7 / XPやWindows Vista®の復元ポイント使って、以前の状態へ復元できますか?

**CompuSecを導入する前の復元ポイントで、復元しないでください。システムが正常に起動しなくなります。**

CompuSec導入後に作成された復元ポイントについては、ハードディスクの暗号化の有無に関わらず、利用可能です。

### Q5　CompuSec導入後にハードディスクにチェックディスクを行うことはできますか?

ハードディスクを暗号化していない状態であれば、特に問題なく実行できます。
ハードディスクを暗号化した後では、Windows®上からのみ行うことができます。

**OSのCDでブート後の回復コンソールや、ハードディスクを別のPCに接続するなど、外部からチェックディスクを実行すると、データが破壊されてしまいます。**

Windows®が起動せず、修復する必要がある場合は、「8 ブート前サービス機能」の「緊急時の復号」を利用して復号した後、OSの修復やチェックディスクなどを行ってください。

### Q6　CompuSec導入後にハードディスクのデフラグを行うことはできますか?

ハードディスクの暗号化の有無に関わらず、OS標準機能のデフラグツールであれば問題なく行えます。但し、市販のデフラグソフトを利用する場合、CompuSecでインストールされた隠しファイルを移動することができず、デフラグが途中で止まってしまう場合があります。

**注意**

**CompuSecでインストールされた隠しファイルを移動してしまうと、CompuSecの認証機能などに障害が出てしまいます。**

市販のデフラグソフトを利用する場合は、事前に該当ファイルをデフラグの対象外に設定するなどで回避できます。(任意のファイルをデフラグ対象外に設定する機能がある場合に限ります)
※Windows®標準搭載のデフラグ機能に関してはこの限りではありません。CompuSecでインストールされる隠しファイルに関しては、製品CD-ROMのルートフォルダーにあるreadme.txtを参照ください。

## 13-2　暗号化／復号関連

### Q1　CompuSecは、どのような働きをするのですか?

暗号化されたメディアに対してすべての読み書きを途中で横取りし、書き込み時はデータを暗号化フォーマットへ書き込み、読み出すときはこれを復号します。この時の暗号化／復号の処理そのものは、ユーザーは意識せず、通常通りの操作のまま運用できます。

### Q2　40GBのハードディスクを暗号化するのに、どのくらい時間がかかりますか?

PCやハードディスクの性能にもよりますが、ノートPCタイプで「作業中に暗号化」を行った場合、約2時間かかります。

暗号化手順として「ブート前に暗号化」も選択できますが、所要時間は「作業中に暗号化」に比べて、数倍必要となる上、処理中に電源を落とすことができません。
**※復号に関しても同様です。**

### Q3 コンピューターのどの部分を暗号化するのですか?

物理的なハードディスク単位、つまりドライブすべてのファイルやフォルダーを含めた、全体を暗号化します。パーティション単位での暗号化はできません。
例えるなら、ファイルシステムを暗号化フォーマットに書き換えている、ということになりますので、ファイルその物は暗号化していません。

### Q4 CompuSecの暗号化アルゴリズムは何ですか?

CompuSec単体版では、ハードディスクやリムーバブルメディアなど、すべてのメディアで、AES 256bitのみを使用しています。AES 128bitやExtended DES 112bitは選択できません。
GlobalAdmin管理下でのハードディスク暗号化アルゴリズムは、AES 256bitのみです。リムーバブルメディアは、AES 256bit、AES 128bit、Extended DES 112bitでの暗号化を選択できます。

どのアルゴリズムを利用するかは、GlobalAdminで設定するポリシーで決まりますので、クライアントPC側で自由に選ぶことはできません。

### Q5 「作業中に暗号化」が開始されません。どうしたら良いでしょうか?

まず、「3-3-2 ハードディスク暗号化の管理ボタン」の手順に従って、暗号化設定を「暗号化未処理」に変更し、コンピューターを再起動してください。
再度「作業中に暗号化」と設定しても処理が開始されない場合は、CompuSecを再インストールすることをお勧めします。

**※ Windows®起動後、「作業中に暗号化」が実際に始まるまでは多少時間を要します。相当な時間待っても開始されない場合にのみ、本手順にて暗号化設定の変更や、CompuSecのアンインストールを行ってください。**

### Q6 DataCryptで暗号化したファイルを、暗号化ファイルにパスワード設定するなどをして、CompuSecを導入していないPCで参照させることはできますか?

できません。DataCryptで暗号化したファイルに関しては、CompuSecを導入し且つ、DataCryptの公開鍵を持っているPC（ユーザー）でのみ参照（復号）することができます。

## 13-3　CompuSec認証関連

### Q1　「ログオン失敗回数制限につき、システム停止しました」とのメッセージが表示されて、キー入力を受け付けません。

CompuSec単体版での認証ミスは3回までとなっております。このメッセージが表示された場合は、コンピューターの電源を入れ直して、正しいユーザIDとパスワードで認証してください。
GlobalAdmin管理下では（標準で）5回までですが、ポリシーにより回数が異なる場合があります。詳細はGlobalAdmin管理者にお問い合わせください。

### Q2　ブート前認証時にID、パスワードを入力しても「このコンピュータへのアクセス権がありません」と表示されます。

ユーザID、パスワード入力後に、このメッセージが表示される場合は、ユーザIDが間違っているか、そのコンピューターに割り当てられていないことを意味します。
まずは、入力するユーザID名が間違っていないかを確かめてください。ユーザIDは大文字、小文字を区別します。

### Q3　ブート前認証時にID、パスワードを入力しても「パスワードが違います。やり直して下さい」と表示されます。

ユーザID、パスワード入力後に、このメッセージが表示される場合は、パスワードが間違っていることを意味します。
パスワードが間違っていないかを確かめてください。パスワードは大文字、小文字を区別します。
GlobalAdmin管理下では、パスワード入力ミスが一定の回数を超えると、User IDがロックされ、一時的に使用不能となるポリシーが設定されている場合があります。
User IDがロックされた場合は、GlobalAdmin管理者にお問い合わせください。

### Q4　ユーザIDを忘れました。どうすればいいでしょうか。

CompuSecをインストールする際に保存した、「SecurityInfo.dat」ファイルを電子メールに添付して、サポートセンターまで送付してください。折り返しユーザIDについてご連絡いたします。
GlobalAdmin管理下の場合は、GlobalAdmin管理者にお問い合わせください。

### Q5　パスワードを忘れました。どうすればよいでしょうか。

CompuSec単体版では、パスワードリセットコードを使って、パスワードをリセットしてください。
GlobalAdmin管理下では、GlobalAdmin管理者と連絡を取り、パスワードをリセットできます。
パスワードのリセット手順については、「8-1-2 パスワードのリセット」を参照してください。

**Q6　パスワードリセットコードを忘れました。どうすればよいでしょうか。**

CompuSecをインストールする際に保存した、「SecurityInfo.dat」ファイルを電子メールに添付して、サポートセンターまで送付してください。
折り返し、パスワードリセットコードについてご連絡いたします。

## 13-4　その他

**Q1　ユーザIDとパスワードを入力しても、画面が暗いままでOSが起動しません。**

USB接続のメモリーやハードディスク・CDドライブおよびSDカードなどが装着されたままの場合は、OSを起動することができません。
USB機器やSDカードなどを取り外した状態で、PCを起動し直してください。

**Q2　CompuSec単体版をアンインストールしたいが、SecurityInfo.datファイルがありません。**

「3-3-4　セキュリティファイルのバックアップ」に従って、SecurityInfo.datファイルを再生成してください。
他のCompuSecで生成されたSecurityInfo.datファイルはご利用できません。

**Q3　CompuSec SWダウンロード版を再インストールしましたが、登録レスポンスコードを受け取れません。**

CompuSec SWダウンロード版では、インストールごとにライセンス番号が、ランダムで変化する仕様となっております。
このため、「再インストール後のライセンス番号」では、「取得済みの支払証明コード」と、組み合わせが異なるため、製品登録を行うことができません。
（「ライセンス番号」と「支払証明コード」は、対になっております。）

CompuSecを再インストールした場合の、製品登録に関しましては、最初に支払証明コードを取得した際の、電子メールに記載されている「ライセンス番号」と「支払証明コード」を、サポートセンターまでお知らせください。
折り返し、再インストールした場合の製品登録手順についてご連絡いたします。

**最新のFAQにつきましては、弊社ホームページ（http://canon-its.jp/supp/cs/）にて掲載しております。**

## 13-5　SDカードの取り扱いについて

昨今のコンピューターでは、SDカードスロットを持つ機種が多くなってきました。初期のSDカードスロットでは問題ありませんでしたが、現行機種の多くはドライバーが変わり、次のような現象を確認しています。

(1)「リムーバブルメディア暗号化」では、ドライブとして認識できませんので、別途カードリーダーなどを介して、暗号化モードを利用してください。
※マイコンピューター上に、あらかじめSDカードスロット分がリムーバブルドライブとして見えている物は、暗号化メディアとして利用できます。
メディアを挿入して初めてドライブが出現するタイプでは、暗号化メディアとして利用できません。

(2) CompuSec導入後、SDカードスロットにメディアを挿入したままでPCを起動させると、ブート前認証後は画面が暗くなったままで、Windows®が起動できない、または起動動作が異常に遅い場合があります。
SDカードスロットより、メディアを取り出した状態でコンピューターを起動するようにしてください。

(3) Windows®が起動中にSDカードを挿入または、取り出した際に、Windows®がブルースクリーンのエラーを出力し、落ちてしまうことがあります。
SDカード挿入時と、取り出し時でデスクトップ状態が変化していると発生しやすい傾向にあります。
但し、すべてのSDカードでは再現せず、現在は一部のメディアのみで確認されている状況です。
なお、カードリーダーなどを介して利用する場合は、問題ありません。

## 13-6　CompuSecを強制削除する方法について

CompuSecを導入直後からOSが起動しない。USB機器や、SDカードの類は接続されておらず、USBに関するBIOS設定を変更しても回避できないなど、PC固有の問題や原因が特定できない場合は、そのPC（環境）ではCompuSecを利用することができない可能性があります。
その様な場合は、CompuSecを強制削除して、PCの原状復帰を試みてください。

CompuSecを強制削除する前提として、
・CompuSec導入直後で、ハードディスクを暗号化していないこと。
・ハードディスクは暗号化されていたが、「緊急時の復号」が済んでいること。

**ハードディスクが暗号化された状態（または暗号化/復号中）の場合は、適用できませんので、ご注意**

**ください。**
**万が一適用してしまうと、ハードディスクのデータが読めなくなります。**

CompuSecを強制削除する手順は、次の通りとなります。

1．オリジナルのMBRを復元します。
「10-2　ツールFDによるMBRの復元」にて、オリジナルのMBRを復元してください。
FD ドライブ（USB接続も含む）が無い場合は、「12-1　パッケージ製品のセットアップディスクで起動する」を実行し、「12-3　FIXMBRを実行」を行ってください。

2．CompuSecを強制削除します。
PCを起動し、CompuSecのインストールCD-ROM内、Installフォルダー下にある、setup.exeを実行してください。（ダウンロード版の場合は、展開したフォルダー内）

［アンインストール］が選択できる場合は、アンインストールを実行してください。
（CompuSec Proの場合、e-Identityの初期化もされます。Admin版除く）

［アンインストール］が選択できない場合は、「サービスとアップデート」から［CompuSecドライバの削除］ボタンを選択してください。
（この時、CompuSec Pro（単体版）では、e-Identityの初期化は行われませんので、別途サポートセンターにて初期化処理を行う必要があります）

自動的に再起動され、CompuSecの強制削除は完了です。

3．MBRの復元時にFIXMBRを実行していた場合。
「10-1　インストールランチャーによるMBR の復元」を実行して、オリジナルのMBRを復元してください。

## 13-7　Windows® 7、Windows Vista®環境でのご注意

### （1）USB-FDDの仕様について

Windows® 7、Windows Vista®へCompuSec 5.xを導入後、USB接続のフロッピーディスクドライブ（以下、USB-FDD）を、メディアを挿入したまま接続すると、エラーでOSが強制終了してしまう現象を確認しています。

CompuSecの暗号化設定で「作業中に暗号化」や「作業中に復号」を実行中に、メディアが挿入されたUSB-FDDを装着すると、OSが強制終了してしまいますので、その後のOS起動が不可能となります。

また、暗号化処理中に限らず、通常のアプリケーションの運用中にも、この現象により、お客さまのデータが消失することがあり得ますので、USB-FDDをご利用の際は、メディアが挿入されていないことを確認してから接続するようにしてください。

この問題につきましては、現在調査中です。

### （2）「コンピューターの修復」機能について

Windows® 7、Windows Vista®がプレインストールされているPCには、エラー修復のツールが、あらかじめ特殊なパーティションにインストールされているものがあります。
これらのツールは、Windows®起動時に［F8］キーを押したり、前回異常終了後に表示される、「コンピューターの修復」メニューから起動されます。

CompuSec導入後はこれらのツールは使用しないでください。
別パーティションの回復用ツールが、CompuSec用MBRを書き換え、PCが正常に起動しない恐れがあります。