情報漏えいを防ぐための
モバイルデバイス等
設定マニュアル

～安心・安全のための暗号利用法～

★★★　実践編　★★★

IPA 独立行政法人情報処理推進機構
セキュリティセンター

目次

実践編 I. 情報保護対策の具体的手法例 2
A) 端末ロックでの利用者認証による保護 3
B) ファイルの暗号化による保護 4
C) ドライブ（全記憶領域）／フォルダ（特定領域）の暗号化による保護 5

実践編 II. ユースケースと対策例 8
ユースケース 1：情報価値レベル 1 の情報を含むファイルが保存された USB メモリを持ち運ぶ場合 8
ユースケース 2：情報価値レベル 2 の情報が保存されたスマートフォンを持ち運ぶ場合 9
ユースケース 3：情報価値レベル 3 の情報が保存されたノート PC を持ち運ぶ場合 12

実践編 III. 代表的な製品の具体的な設定方法の実例 14
① Windows 7, Windows 8 での設定方法一例 15
A.1 端末ロックによる利用者認証の有効化（利用者認証の設定方法） 15
A.2 端末ロックによる利用者認証の安全性強化（利用者認証失敗時の動作設定方法） 26
C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化 32
② iOS 6 での設定方法一例 42
A.1 端末ロックによる利用者認証の有効化（利用者認証の設定方法） 42
A.2 端末ロックによる利用者認証の安全性強化 45
C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化 50
③ Android 4.x での設定方法一例 51
A.1 端末ロックによる利用者認証の有効化（利用者認証の設定方法） 51
A.2 端末ロックによる利用者認証の安全性強化 53
C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化 56
④ Microsoft Office（Word, Excel, Powerpoint）での設定方法一例 59
B.1 ファイルへの暗号化設定の有効化（保存方法） 59
⑤ Adobe Acrobat（PDF ファイル）での設定方法一例 62
B.1 ファイルへの暗号化設定の有効化（保存方法） 62
⑥ Imation 指紋認証付 USB メモリでの設定方法一例 66
C.3 端末起動時および端末ロックによる利用者認証の安全性強化（バイオメトリクス認証設定、回復用パスワード（マスターパスワード）設定） 66

実践編 I. 情報保護対策の具体的手法例

本実践編では、各種の対策項目を実施するにあたって、**具体的に何をすべきか**の観点で代表的な対策例を挙げています。

なお、対策例を読むうえでの注意事項は以下の通りです。

《注意事項》

- 「以下の設定をすべて行う」との記述がある場合、当該項目に記載された**対策例をすべて実施**する必要があります。一部だけを実施した場合、適切な水準の対策にはなっていない場合があります。
- 「少なくとも①の対策を実施」とある場合、当該項目に記載された対策例のうち、**①の対策は必ず実施**する必要があります。そのうえで、そのほかの対策例を追加実施することで安全性がさらに高まります。
- 「以下の方法のいずれかまたは併用」とある場合、当該項目に記載された対策例のうち、利用環境等を勘案して**適切と思われる方法を一つまたは複数選択して実施**することになります。
  なお、対策例一つ一つが同程度の安全性を高める、というわけではありません。例えば、利便性に非常に優れているが安全性の向上が大きくないもの、反対に安全性は大きく向上するが運用コストがかかるものなど、いくつかの特徴をもった対策例が併記されています。どの対策例を採用するかは利用環境等を踏まえて、**リスクに応じた費用対効果の高い対策を選択**してください。また、基本的には、**実施する対策例が多くなるほど安全性が高まります**。
- 「注意」とある記述は、**対策を実施するにあたって必ず守る**必要があります。ここの注意事項が守られていなかった場合、せっかく対策を行われていたとしても、実質的な対策としては機能していない可能性があります。

A) 端末ロックでの利用者認証による保護

A.1 端末ロックによる利用者認証の有効化

以下の設定を**すべて**行う。

① 端末ロックによる利用者認証機能を有効にする

② 端末がロックされるまでの時間や条件を適切に設定する

A.2 端末ロックによる利用者認証の安全性強化

少なくとも①の対策を実施することにより、端末ロックによる利用者認証の安全性を強化する。

① 一定回数以上端末ロックによる利用者認証に失敗した場合、端末の完全ロック（特別な解除処理をしない限り以後の利用者認証を受け付けない)、もしくは一定期間ロックアウト（一定時間利用者認証を受け付けない）する。後者の場合、ロックアウトする時間は、利用環境や扱う情報価値レベルに応じて適切に設定すること

② パスワード長を大きくしたり、利用する文字種類を増やしたり、ピクチャーパスワードを利用するなど、パスワードの複雑度を高める

A.3 端末ロックによる利用者認証のさらなる安全性強化

以下の方法の**いずれかまたは併用**により、端末ロックによる利用者認証の安全性をさらに強化する。

① パスワード強度チェックに合格したパスワードを利用する

② 複数のパスワード認証を設定する（端末立ち上げ時（BIOS 起動時)、OS 起動時、画面ロック時、等）

③ トークン認証（IC カード、USB トークン、SIM カードなどの利用者認証用トークンを使った利用者認証）（場合によってはパスワード認証を併用）を利用する

④ ワンタイムパスワード認証を利用する

⑤ バイオメトリクス認証を利用する

⑥ 認証サーバによる利用者認証を利用する

⑦ リモートロック機能を利用し、紛失・盗難した端末に遠隔でロックをかける機能を有効にする（リモートワイプ機能での代用も可）

注意：

※ 複数のパスワードを使う場合、共通のパスワードもしくは類似したパスワードにしないこと。なお、すべてをパスワードだけで認証する場合には、少なくとも一つはパスワード強度チェックに合格したパスワードを利用することを強く推奨する

※ ③でパスワード認証を設定しない場合､端末と利用者認証用トークン(IC カード､USB トークンなど）とは物理的に一緒の場所に保管しないこと。携帯する際にも、同じ所

持品のなかに入れないこと

※ ②～⑤において、救済用のパスワード[1]（マスターパスワードなど）を設定する場合には、少なくともパスワード強度チェックに合格したパスワードを利用し、安全な場所に当該救済用パスワードを別途保管しておくこと。決して端末・媒体と一緒に携帯してはならない

B）ファイルの暗号化による保護

B.1 ファイルへの暗号化設定の有効化

パスワードを使用してファイルごとに暗号化する。

B.2 暗号化ファイルに対するアクセス制御の強化

以下の方法の**いずれかまたは併用**により、ファイル暗号化されたデータへのアクセス制御を強化する。

① パスワード強度チェックに合格したパスワードを利用する
② 一定回数以上パスワード認証に失敗した場合、データを破棄または復号禁止状態する
③ 復号可能な有効期限や有効回数を設定する

注意：

※ 端末ロックによる利用者認証用パスワードなど、他のパスワードと同じパスワードにしないこと

B.3 暗号化ファイルに対するアクセス制御のさらなる強化

以下の方法の**いずれかまたは併用**により、ファイル暗号化されたデータへのアクセス制御をさらに強化する。

① 専用ソフトが導入された端末でのみ復号可能な設定にする
② 認証サーバによる復号権限の確認を強化する、もしくは鍵管理サーバで暗号鍵を管理する
③ リモートロック機能を利用し、紛失・盗難した端末に遠隔でロックをかける機能を有効にする
④ リモートワイプ機能を利用し、紛失・盗難した端末に格納されるデータの消去または初期化を行う機能を有効にする

[1] 利用者認証用トークン（IC カード、USB トークンなど）が利用できなくなったり、バイオメトリクス認証が正しく認識しないなど、通常とは違う方法で利用者認証をする必要が生じた際に利用するパスワードのこと

C) ドライブ（全記憶領域）／フォルダ（特定領域）の暗号化による保護

C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

以下の設定を**すべて**行う。

① 端末ロックによる利用者認証機能を有効にする（A.1 と同様）

② 端末がロックされるまでの時間や条件を適切に設定する（A.1 と同様）

③ ドライブ／フォルダの暗号化機能を有効にする

④ 一定回数以上端末ロックによる利用者認証に失敗した場合、端末の完全ロック（特別な解除処理をしない限り以後の利用者認証を受け付けない）、もしくは一定期間ロックアウト（一定時間利用者認証を受け付けない）する。後者の場合、ロックアウトする時間は、利用環境や扱う情報価値レベルに応じて適切に設定すること（A.2 と同様）

⑤ パスワード長を大きくしたり、利用する文字種類を増やしたり、ピクチャーパスワードを利用するなど、パスワードの複雑度を高める（A.2 と同様）

C.2 端末起動時の利用者認証の有効化

以下の設定を**すべて**行う。

① 端末起動時の利用者認証機能を有効にする

② 端末ロックによる利用者認証とは異なるパスワードを設定する

注意：

※ 端末起動時の利用者認証が複数設定される場合、共通のパスワードもしくは類似したパスワードにしないこと

※ 携帯電話・スマートフォン・USB メモリ・外付けドライブストレージなどの機種によっては、端末ロックによる利用者認証（A.1）と端末起動時の利用者認証（C.2）が自動的に同じ設定になる場合がある。その場合には C.2. を実施しなくてよい

※ BIOS[2]設定の変更が必要となるため、必要があれば、パソコン等の知識を有する人の助言を仰ぐこと。BIOS設定に失敗すると端末自体が起動しなくなる恐れがある

C.3 端末起動時および端末ロックによる利用者認証の安全性強化

以下の方法の**いずれかまたは併用**により、端末起動時および端末ロックによる利用者認証の安全性を強化する。

① パスワード強度チェックに合格したパスワードを利用する。特に、すべての利用者認証がパスワードだけで認証する場合には、共通のパスワードもしくは類似したパスワードに設定しないこととし、少なくとも一つはパスワード強度チェックに合格したパスワードを利用することを強く推奨する

[2] Basic Input / Output System

② トークン認証（IC カード、USB トークン、SIM カードなどの利用者認証用トークンを使った利用者認証）（場合によってはパスワード認証を併用）を利用する
③ ワンタイムパスワード認証を利用する
④ バイオメトリクス認証を利用する
⑤ 認証サーバによるアカウント認証を利用する
⑥ リモートロック機能を利用し、紛失・盗難した端末に遠隔でロックをかける機能を有効にする（リモートワイプ機能での代用も可）

注意：

※ ②でパスワード認証を設定しない場合、端末と利用者認証用トークン（IC カード、USB トークン、SIM カードなど）とは物理的に一緒の場所に保管しないこと。携帯する際にも、同じ所持品のなかに入れないこと

※ ②～④において、救済用のパスワード[3]（マスターパスワードなど）を設定する場合には、少なくともパスワード強度チェックに合格したパスワードを利用し、安全な場所に当該救済用パスワードを別途保管しておくこと。決して端末・媒体と一緒に携帯してはならない

C.4 暗号化データに対するアクセス制御の強化

以下の方法の**いずれかまたは併用**により、暗号化されたデータへのアクセス制御を強化する。

① 復号可能な有効期限や有効回数を設定する
② 端末・媒体内でのみ復号し、外部へのデータ出力を禁止する
③ 限定された端末でのみ復号可能な設定にする
④ リモートワイプ機能を利用し、紛失・盗難した端末に格納されるデータの消去または初期化を行う機能を有効にする

C.5 暗号鍵の管理強化

以下の方法の**いずれかまたは併用**により、暗号鍵を暗号化されたデータとは別の場所に保管する。

① 暗号鍵を、ドライブやメモリなどの記録媒体とは異なる、端末・媒体内のハードウェアチップに格納する
② 暗号化されたデータとは異なる媒体に暗号鍵を格納する
③ 鍵管理サーバに格納する

[3] 利用者認証用トークン（IC カード、USB トークン、SIM カードなど）が利用できなくなったり、バイオメトリクス認証が正しく認識しないなど、通常とは違う方法で利用者認証をする必要が生じた際に利用するパスワードのこと

C.6 セキュリティ認証製品の採用

JCMVP 認証取得製品、CMVP (FIPS140-1/FIPS140-2)認証取得製品、CC 認証取得製品のいずれかを利用する。

実践編 II. ユースケースと対策例

特によくおこり得る情報漏えいの 3 つのケースについて、想定すべきリスクと実施すべき対策の一例について示します。また参考までに、具体的な設定方法の例がある場合には、その該当箇所をページ番号で記します。

ユースケース 1: 情報価値レベル 1 の情報を含むファイルが保存された USB メモリを持ち運ぶ場合

解説編 3.2 節を参考にすると、情報価値レベル 1 には以下のような情報が該当します。

- 本人が特定されない形での個人識別情報（会員番号のみ、等）
- 本人が特定されない形での本人に付随する情報（生年月日のみ、職業のみ、等）

このケースの場合、仮に情報漏えいしたとしても本人が特定されない情報であることから重大な悪影響が生じる可能性は小さいと考えられるため、紛失した USB メモリを拾得した人に興味本位で情報が簡単に見られることだけを防止できればとりあえずよいと考えられます。

その場合の必要なベースラインの対策レベルは「1」となりますので、USB メモリの場合は、解説編 44 ページの対策レベル 1-1 または対策レベル 1-2 が最低基準の対策となります。

【対策を施さない場合に想定すべきリスク】

- USB メモリを拾得した第三者が、PC に接続して、端末内の情報を簡単に見る

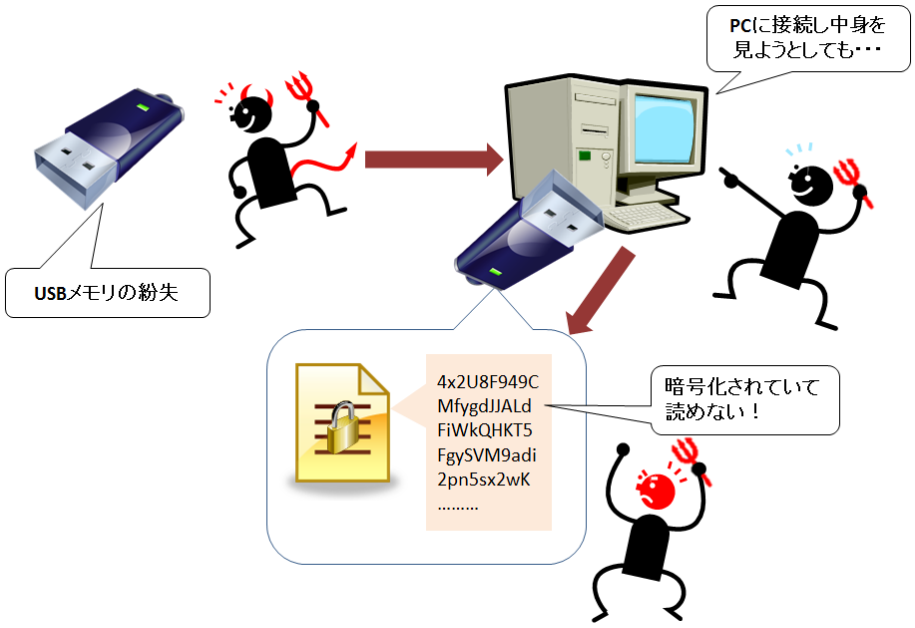
【実施すべき対策】

例えば**対策レベル 1-2** を選択した場合は、最低限、以下のような設定が必要になります。

実施すべき対策	具体的な設定方法の一例	ページ番号
B.1 ファイルへの暗号化設定の有効化	Microsoft Office でのファイル暗号化設定	P. 59
	Adobe Acrobat でのファイル暗号化設定	P. 62

【対策を施すことで期待できること】

紛失や盗難した USB メモリが第三者に拾得されて、興味本位で PC に接続してデータを見られても、ファイルが暗号化されていれば元の情報自体を見ることはできなくなります。



ユースケース 2：情報価値レベル 2 の情報が保存されたスマートフォンを持ち運ぶ場合

解説編 3.2 節を参考にすると、情報価値レベル 2 には以下のような情報が該当します。

- 本人を特定するための公開情報ではあるが、本人が公開範囲を一定程度コントロールできる情報（電話帳、個人の公開情報の組み合わせ、等）
- 本人が特定されない形での生活様式（行動パターン）が明らかになる可能性がある情報（アンケート調査結果、等）
- 無関係の人に対しては開示する必要性がない情報（関係者外秘情報、等）
- いずれ公開される情報であるが、その時点では公開されていない情報（公開前の講演資料、等）

このケースの場合、情報漏えいした情報がいずれ公開されるものであったり、限られた範囲内では比較的自由に流通するような情報であることから、情報漏えいすること自体によって重大な悪影響が生じる可能性は小さいものと考えられます。しかし、原則的には情報を持っている人の管理下に置いて公開する範囲が決められるべき情報であることから、紛失・盗難したスマートフォンを拾得した第三者が安易に情報を見ることがないようにする対策を行うべきです。

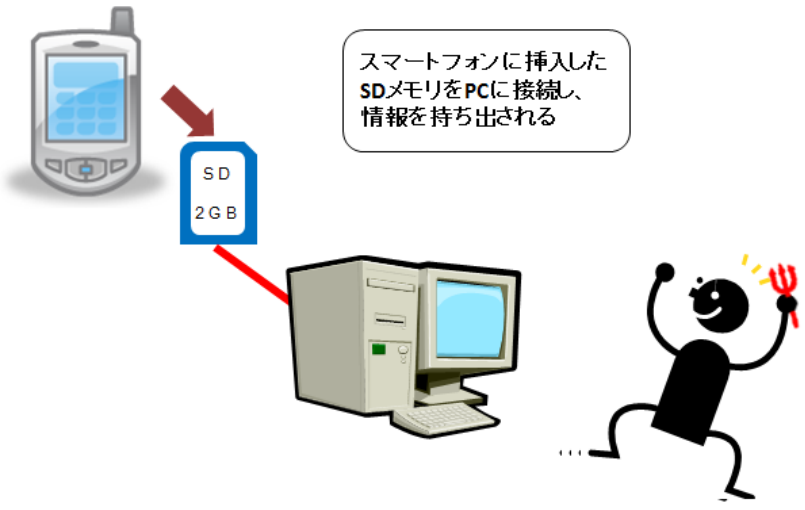
その場合の必要なベースラインの対策レベルは「2」となりますので、スマートフォンの場合は、解説編 41 ページの対策レベル 2-1 または対策レベル 2-2 が最低基準の対策となります。

【対策を施さない場合に想定すべきリスク】

- スマートフォンを盗んだ第三者が端末内の情報を見る

- 端末内の情報を USB 接続したパソコンから情報を持ち出される

- 端末に挿入した SD メモリを抜かれて情報を持ち出される



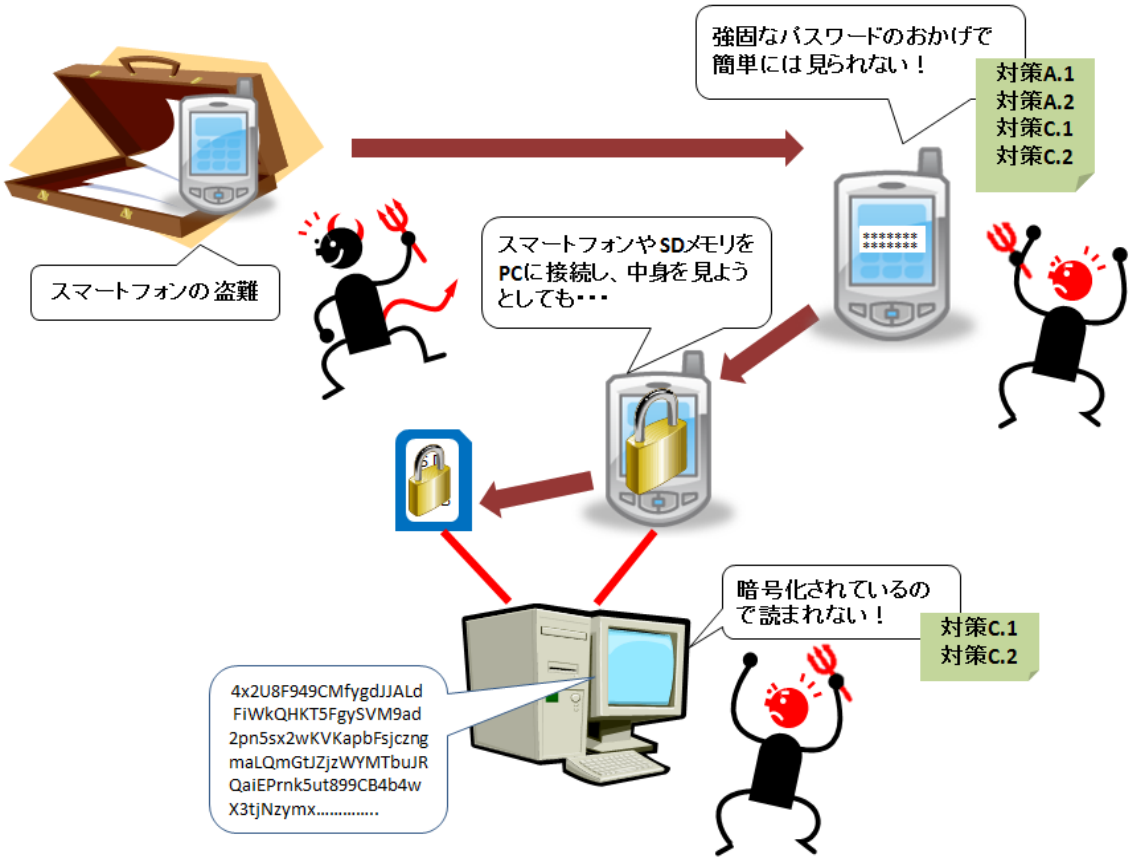
【実施すべき対策】

例えば**対策レベル 2-1** を選択した場合は、最低限、以下のような設定が必要になります。

実施すべき対策	具体的な設定方法の一例	ページ番号
A.1 端末ロックによる利用者認証の有効化	iOS での利用者認証設定	P. 42
	Android での利用者認証設定	（P. 51）
A.2. 端末ロックによる利用者認証の安全性強化	iOS での安全性強化	P. 45
	Android での安全性強化	P. 53
C.1. ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化	iOS では自動設定	－
	Android での端末暗号化設定	P. 56
C.2. 端末起動時の利用者認証の有効化	iOS, Android とも端末ロックによる利用者認証と共用（変更不可）	－

【対策を施すことで期待できること】

端末ロックによる利用者認証の安全性を高めることで、紛失・盗難にあっても第三者が情報を見られる可能性を低減できます。また、本体及び外部メモリのデータ領域を暗号化しておくことによって、端末ロックがかかっている状態でデータを持ち出されたり見られたりしても、元の情報自体を見ることはできなくなります。



ユースケース 3：情報価値レベル 3 の情報が保存されたノート PC を持ち運ぶ場合

解説編 3.2 節を参考にすると、情報価値レベル 3 には以下のような情報が該当します。

- 本人と個人識別情報を結び付ける情報（氏名と社員番号や会員番号などとの組み合わせ、等）
- 本人を特定でき、かつ本人に付随する公開されていない情報（家族の構成情報、資産情報、疾病歴、等）
- 本人を特定でき、生活様式（行動パターン）が明らかになる可能性がある情報（学業成績、購入履歴情報、等）
- 業務秘密として管理すべき情報（研究開発成果、営業情報、社外秘情報、等）

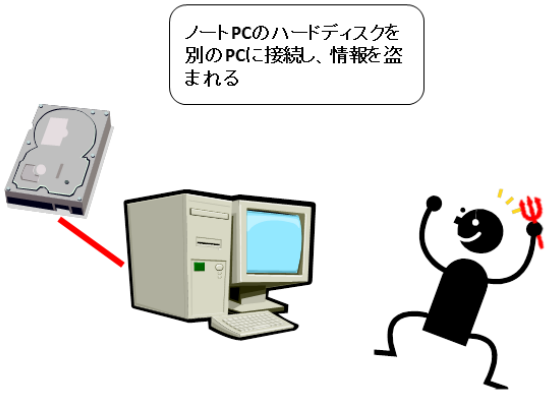
このケースの場合、漏えいした情報によって重大な悪影響を及ぼす可能性があり、企業としての信用棄損のみならず、場合によっては損害賠償等の実害が発生する可能性も否定できません。したがって、仮にノートパソコンを紛失・盗難したとしても、その中の情報が漏えいしないようにできるだけ厳格な管理を行う必要があります。

その場合の必要なベースラインの対策レベルは「3」となりますので、ノートパソコンの場合は、解説編 37 ページの対策レベル 3-1 または対策レベル 3-2 が最低基準の対策となります。

【対策を施さない場合に想定すべきリスク】

- パスワードクラックにより情報を盗まれる

- ハードディスクから直接情報を盗まれる



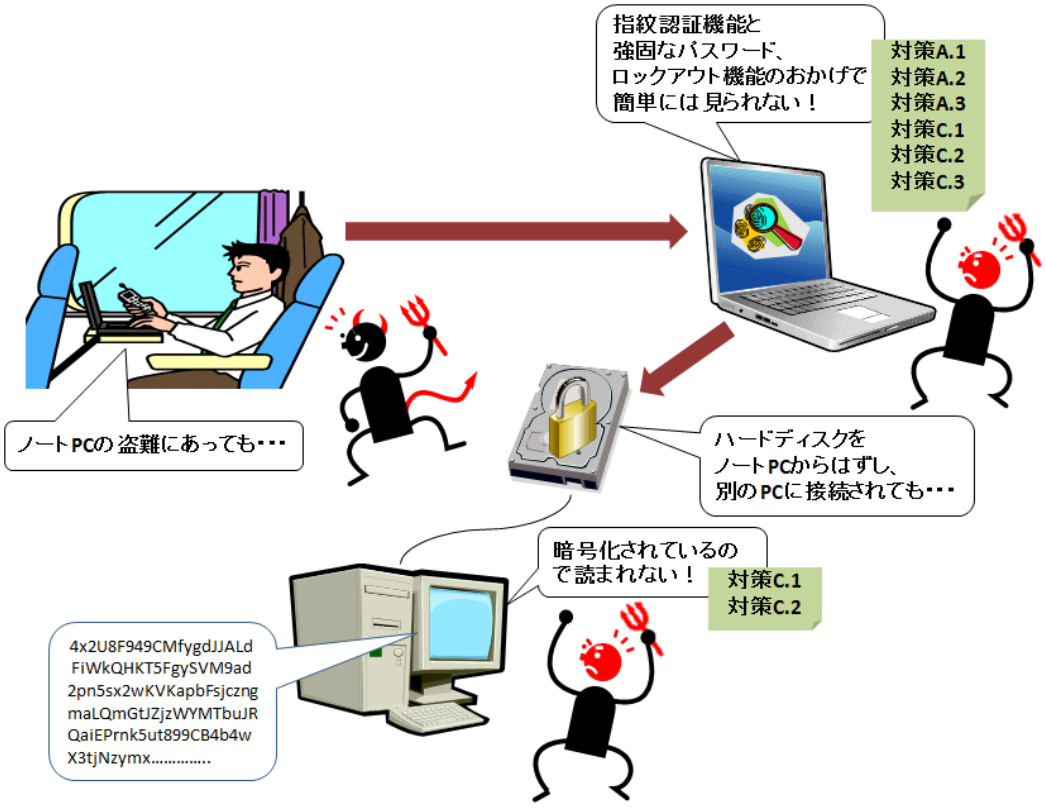
【実施すべき対策】

例えば**対策レベル 3-1** を選択した場合は、最低限、以下のような設定が必要になります。

実施すべき対策	具体的な設定方法の一例	ページ番号
A.1 端末ロックによる利用者認証の有効化	Windows での利用者認証設定	P. 15
A.2 端末ロックによる利用者認証の安全性強化	Windows でのアカウントのロックアウト設定	P. 26
A.3 端末ロックによる利用者認証のさらなる安全性強化	指紋認証機能の有効化	—
C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化	BitLocker によるドライブ暗号化設定	P. 32
C.2 端末起動時の利用者認証の安全性強化	BitLocker では自動設定	—
C.3 端末起動時および端末ロックによる利用者認証の安全性強化	指紋認証機能の有効化	—
	救済用パスワードに、Microsoft の非公式ツールなどのパスワード強度チェックに合格した強固なパスワードを設定	解説編 2.4.2.2 節 2.4.2.3 節

【対策を施すことで期待できること】

盗難や紛失によってノートパソコンが第三者の手にわたっても、強固なパスワードの設定やロックアウト機能の有効化、バイオメトリクス認証の設定など対策を多重化するにより、ノートパソコンにログインされることを困難にします。また、ハードディスクを別の PC に接続することで中身を見られても、データが暗号化されているため情報を見ることができません。



実践編 III. 代表的な製品の具体的な設定方法の実例

解説編 3.3 節及び実践編 I.での対策を実施するに当たり、広く使われている以下の製品について、具体的な設定方法を紹介します。各社が取扱説明書やホームページ等で提供している情報と併せて活用してください。

① Windows 7, Windows 8 での設定方法一例
- ✧ A.1 端末ロックによる利用者認証の有効化（利用者認証の設定方法）
- ✧ A.2 端末ロックによる利用者認証の安全性強化（利用者認証失敗時の動作設定方法）
- ✧ C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化（ドライブ暗号化（BitLocker）の設定方法、フォルダ暗号化（EFS[4]を利用）の設定方法）

② iOS 6 での設定方法一例
- ✧ A.1 端末ロックによる利用者認証の有効化（利用者認証の設定方法）
- ✧ A.2 端末ロックによる利用者認証の安全性強化
- ✧ C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

③ Android 4.x での設定方法一例
- ✧ A.1 端末ロックによる利用者認証の有効化（利用者認証の設定方法）
- ✧ A.2 端末ロックによる利用者認証の安全性強化
- ✧ C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化（スマートフォン端末・タブレット端末での暗号化設定方法）

④ Microsoft Office（Word, Excel, Powerpoint）での設定方法一例
- ✧ B.1 ファイルへの暗号化設定の有効化（保存方法）

⑤ Adobe Acrobat（PDF ファイル）での設定方法一例
- ✧ B.1 ファイルへの暗号化設定の有効化（保存方法）

⑥ Imation[5]指紋認証付USBメモリでの設定方法一例
- ✧ C.3 端末起動時および端末ロックによる利用者認証の安全性強化（バイオメトリクス認証設定、回復用パスワード（マスターパスワード）設定）
  ※「C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化」の設定を含む

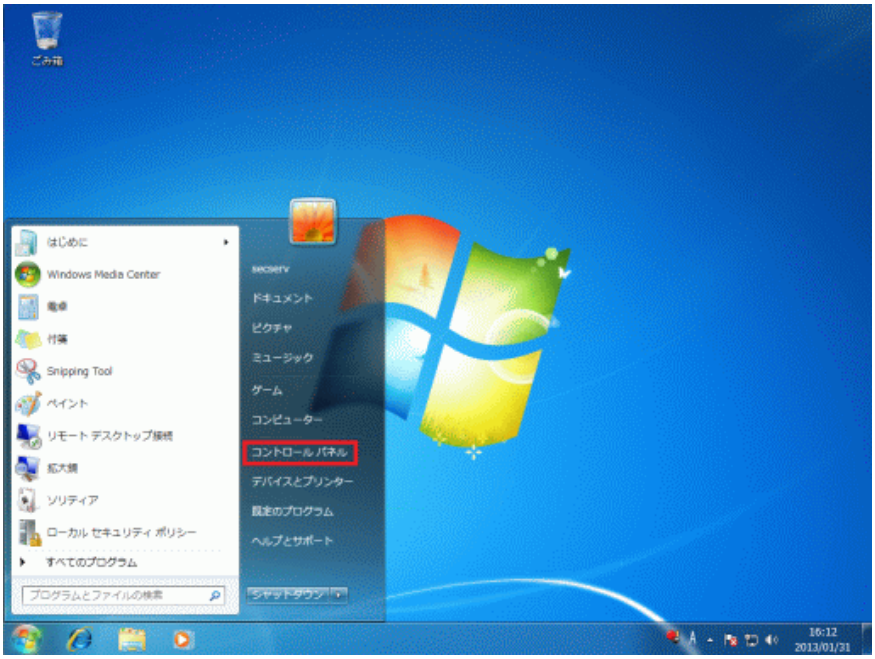
[4] Encrypting File System
[5] 指紋認証付 USB メモリは各社から色々な製品が出ているが、セキュリティ認証規格（解説編 2.4.3.2 節参照）を取得している製品は多くない。ここでは、CMVP 認証を取得している製品例として Imation 社の製品を取り上げた

① Windows 7, Windows 8 での設定方法一例

A.1　端末ロックによる利用者認証の有効化（利用者認証の設定方法）

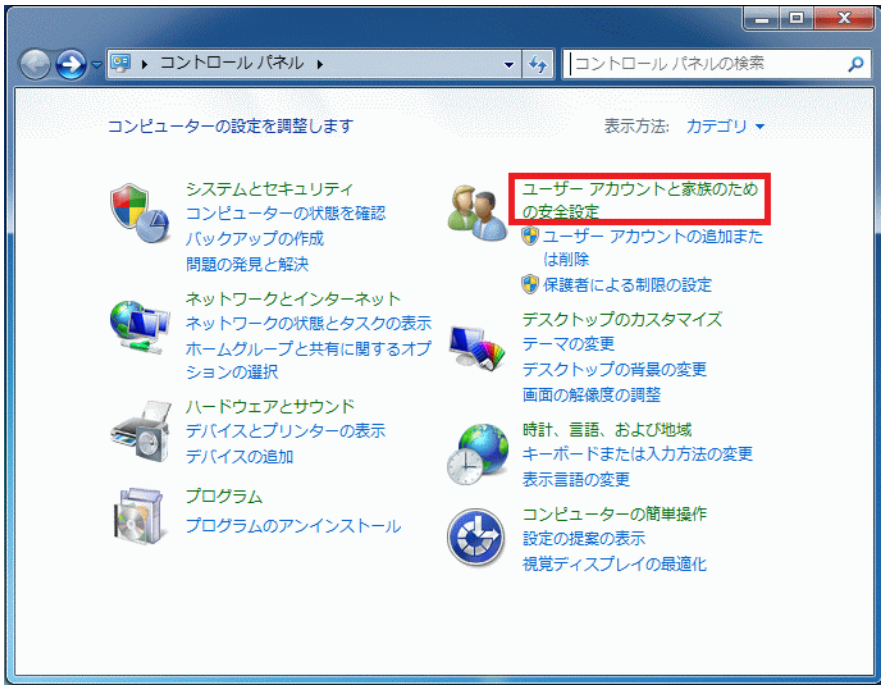
- **Windows 7**

1. 〔スタート〕ボタンからコントロールパネルを起動する。

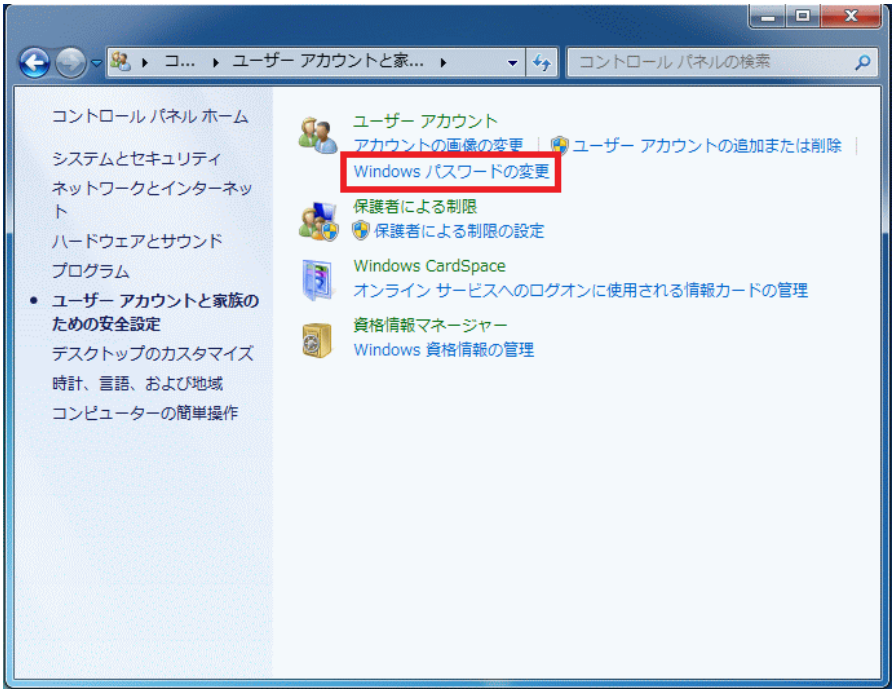


2. 〔ユーザーアカウントと家族のための安全設定〕をクリックする。

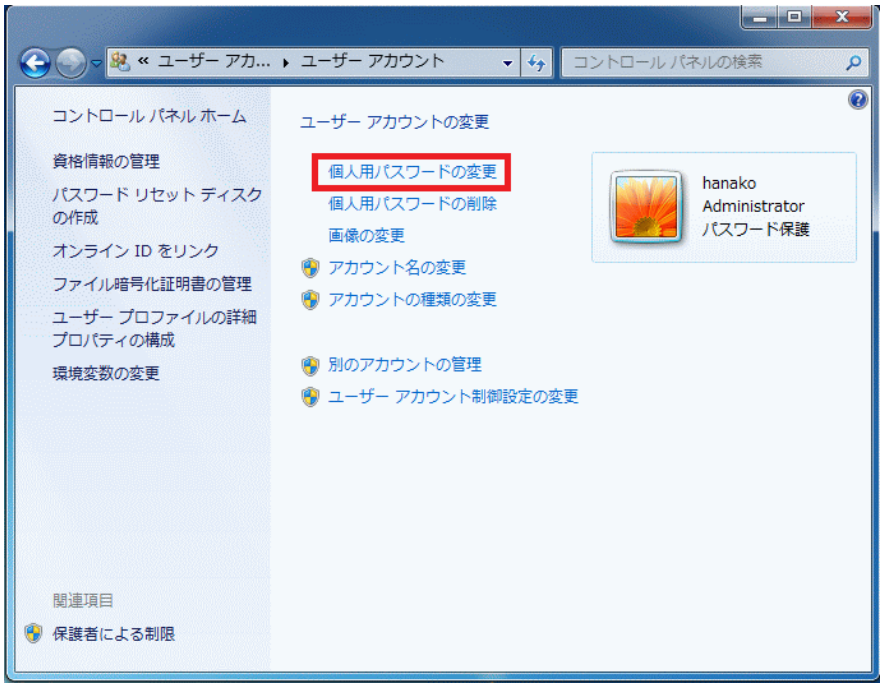
Windows パスワードがすでに適切に設定されている場合には、2.～5.の手順を省略できる。なお、すべてのユーザーアカウントに対して、Windows パスワードが設定されていることが必要である。



3. 〔Windows パスワードの変更〕をクリックする。

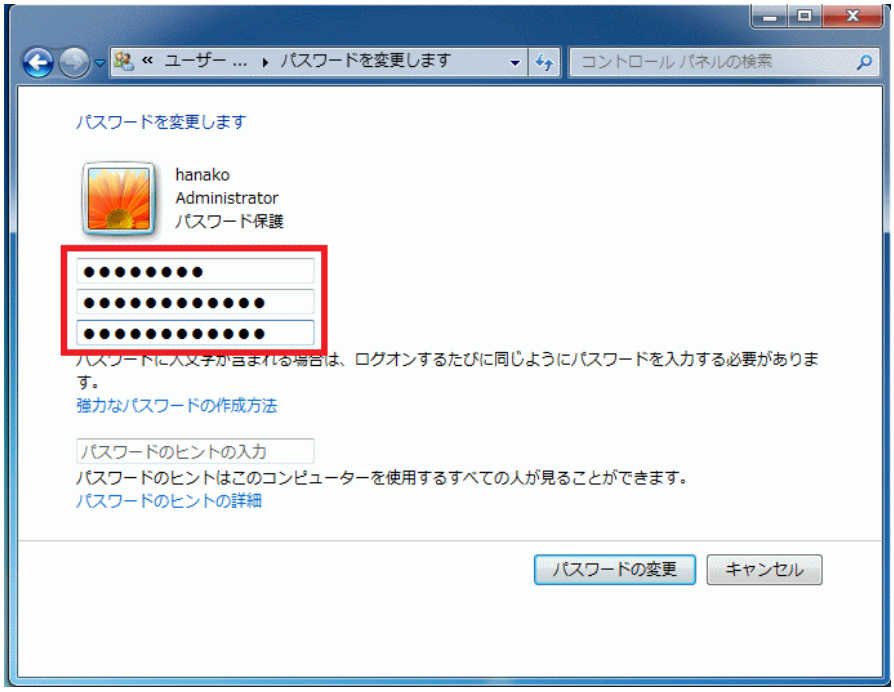


4. 〔個人用パスワードの変更〕をクリックする。

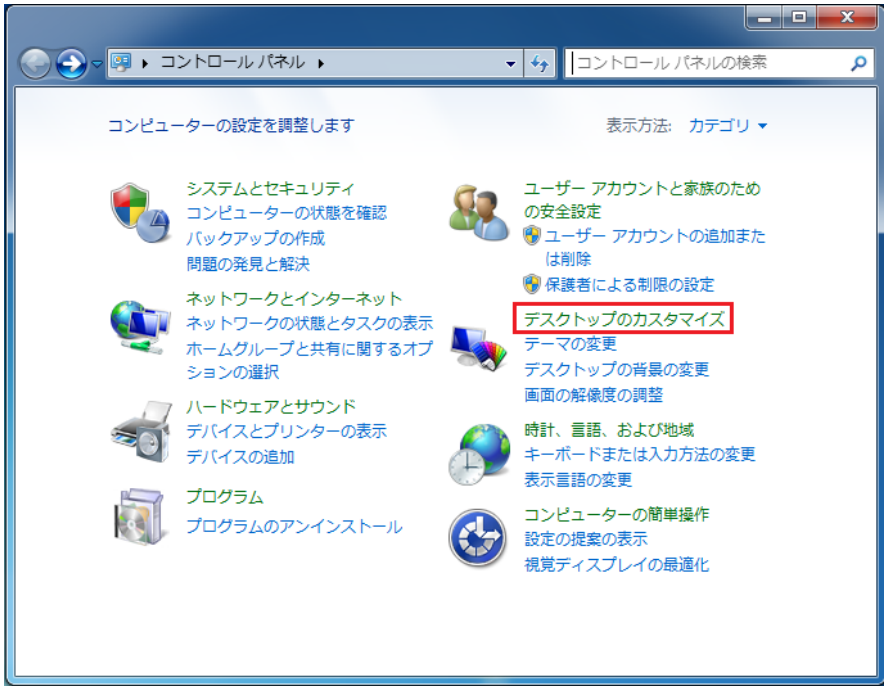


5. 現在のパスワードを上段のテキストボックスに入力し、新しいパスワードを中段・下段のテキストボックスに入力して〔パスワードの変更〕をクリックする。

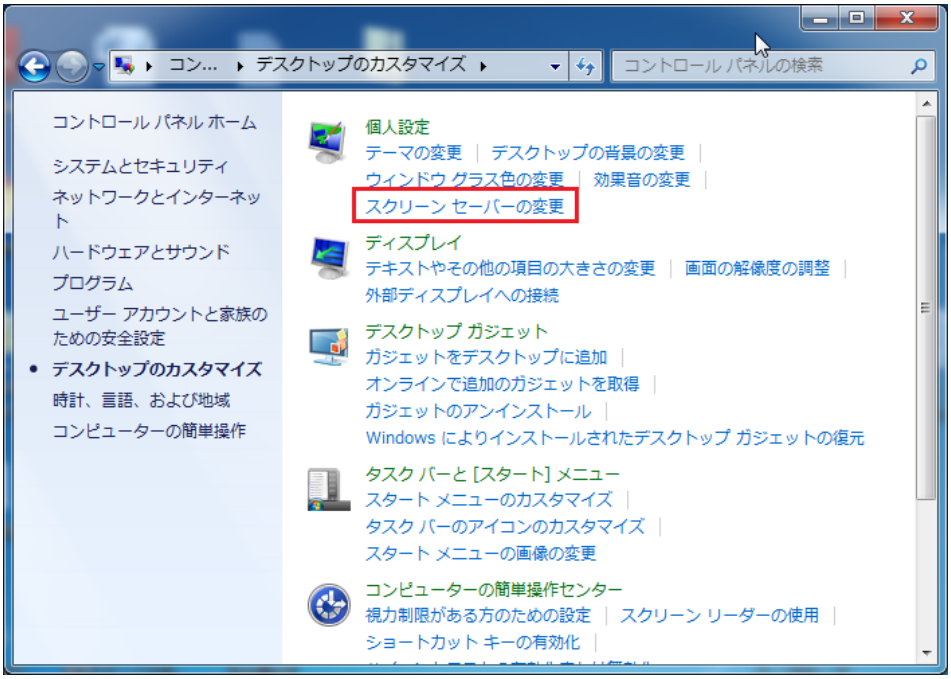
【注意】 パスワードについては、解説編 2.4.2.2 節を踏まえ、適切に設定すること。最低でも英数字（0-9, A-Z, a-z）8 文字以上とすることを強く推奨する



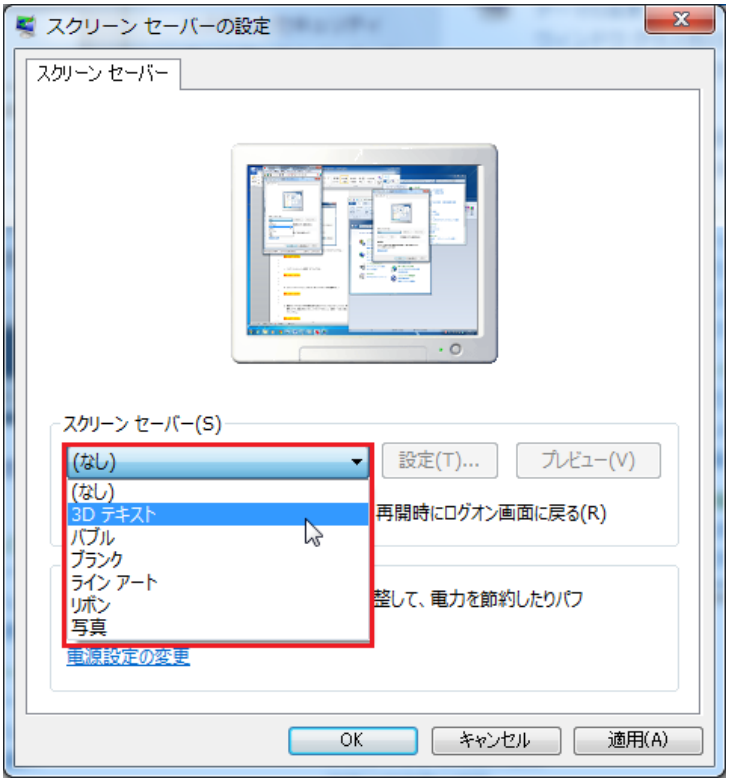
6. コントロールパネルに戻り、〔デスクトップのカスタマイズ〕をクリックする。



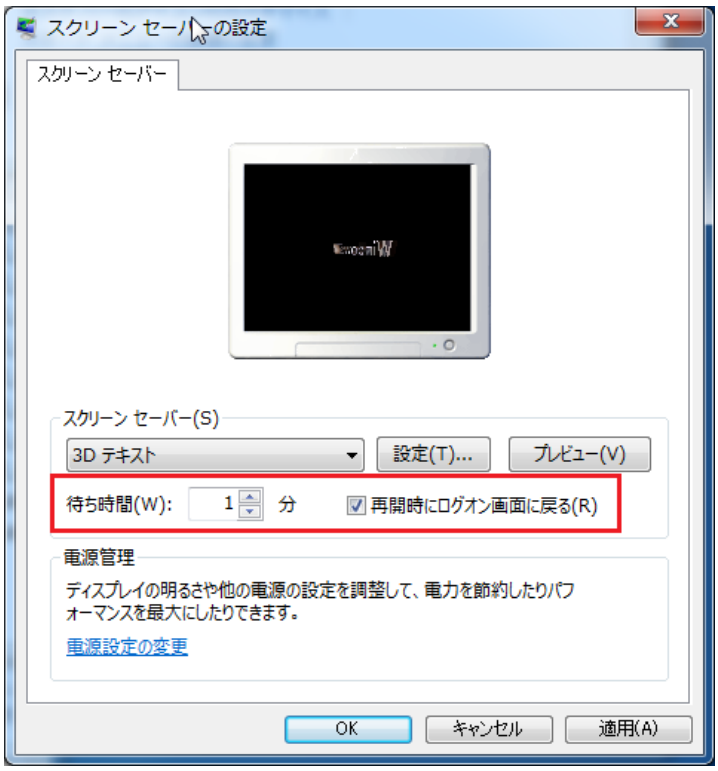
7. 〔スクリーンセーバーの変更〕をクリックする。



8. スクリーンセーバーとして〔(なし)〕及び〔(バブル)〕以外を選択する。

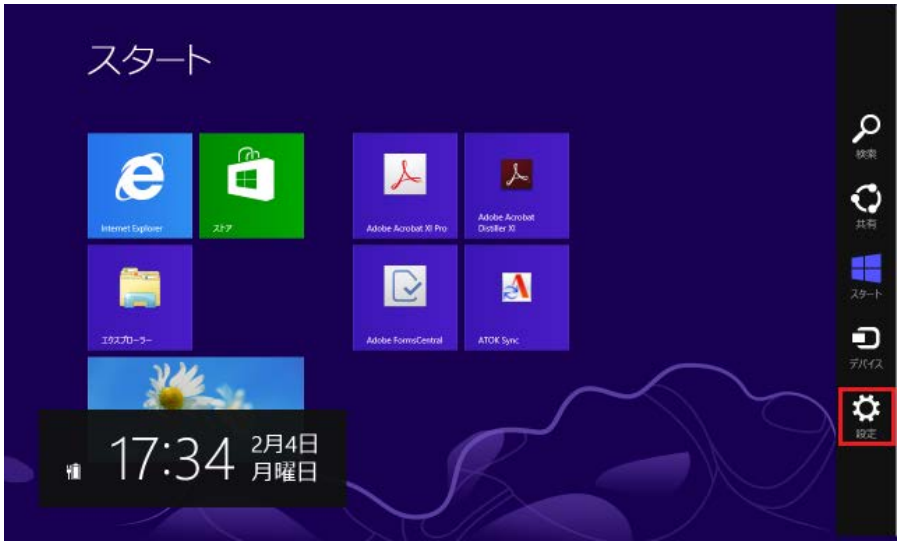


9. 画面がロックするまでの待ち時間を適切に設定（5 分以内での設定を推奨）したうえで、〔再開時にログオン画面に戻る〕のチェックボックスをオンにし、〔適用〕→〔OK〕の順にクリックする。

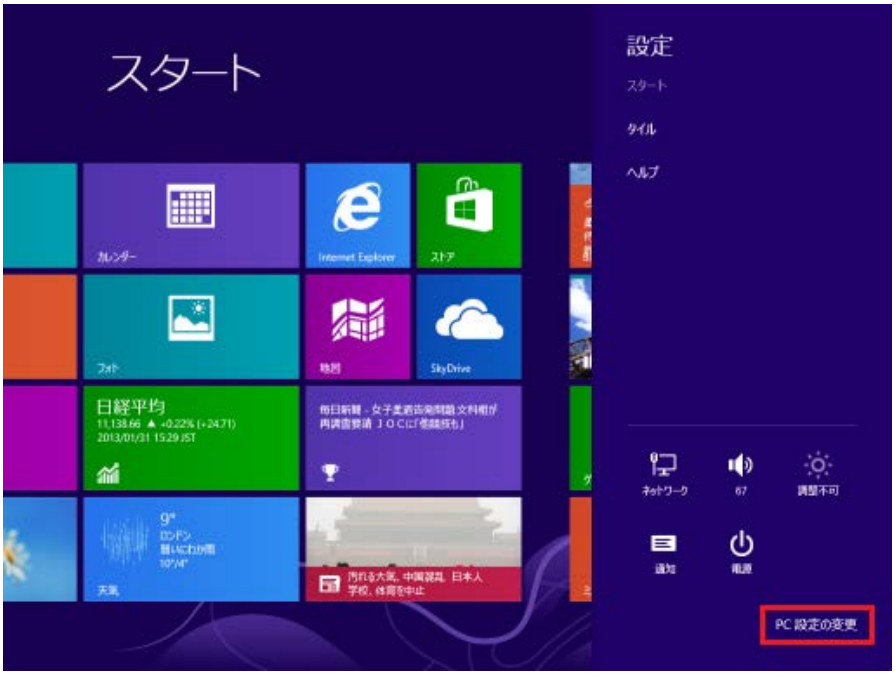


- **Windows 8**

1. 右のメニューから〔設定〕をクリックする。

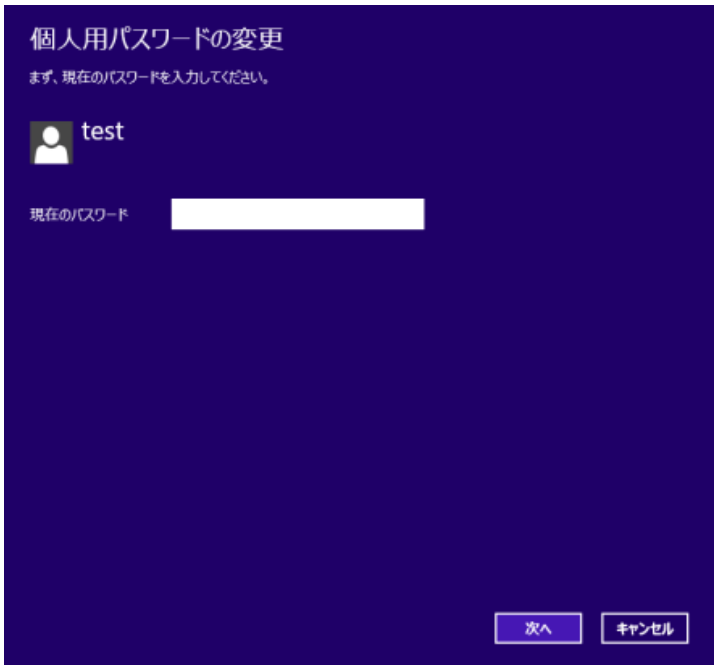


2. 〔PC 設定の変更〕をクリックする。



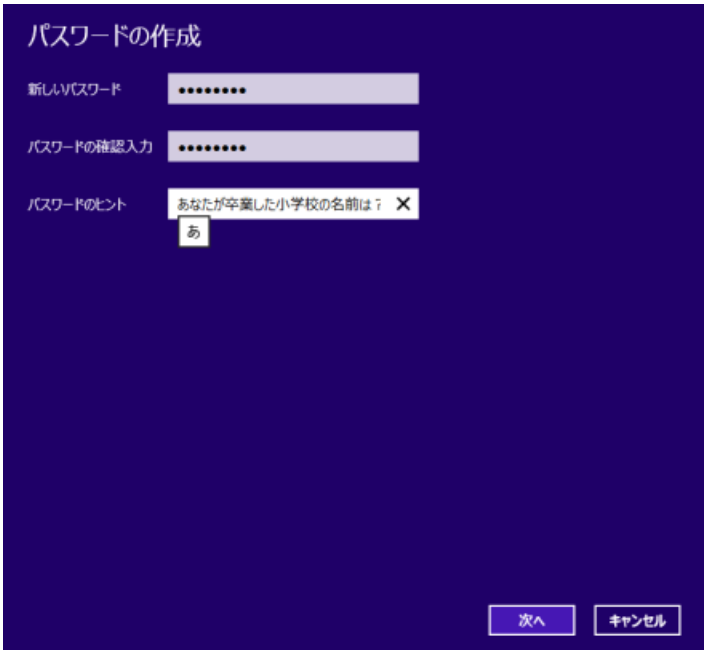
3. 〔ユーザー〕をクリックし、〔個人用パスワードの変更〕をクリックする。
Windows パスワードがすでに適切に設定されている場合には、4.～6.の手順を省略できる。なお、すべてのユーザーアカウントに対して、Windows パスワードが設定されていることが必要である。

4. 現在のパスワードを入力し、〔次へ〕をクリックする。

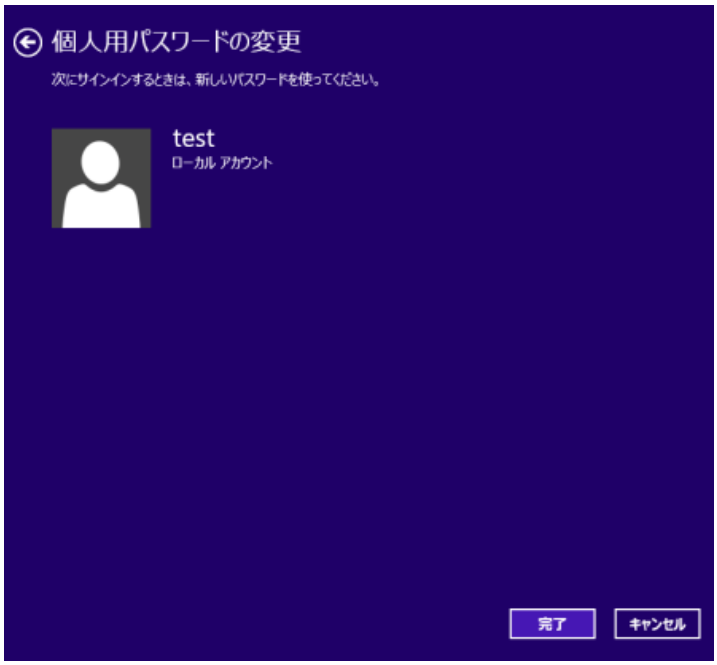


5. 新しいパスワードとパスワードのヒントを入力し、〔次へ〕をクリックする。

【注意】 パスワードについては、解説編 2.4.2.2 節を踏まえ、適切に設定すること。最低でも英数字（0-9，A-Z，a-z）8 文字以上とすることを強く推奨する

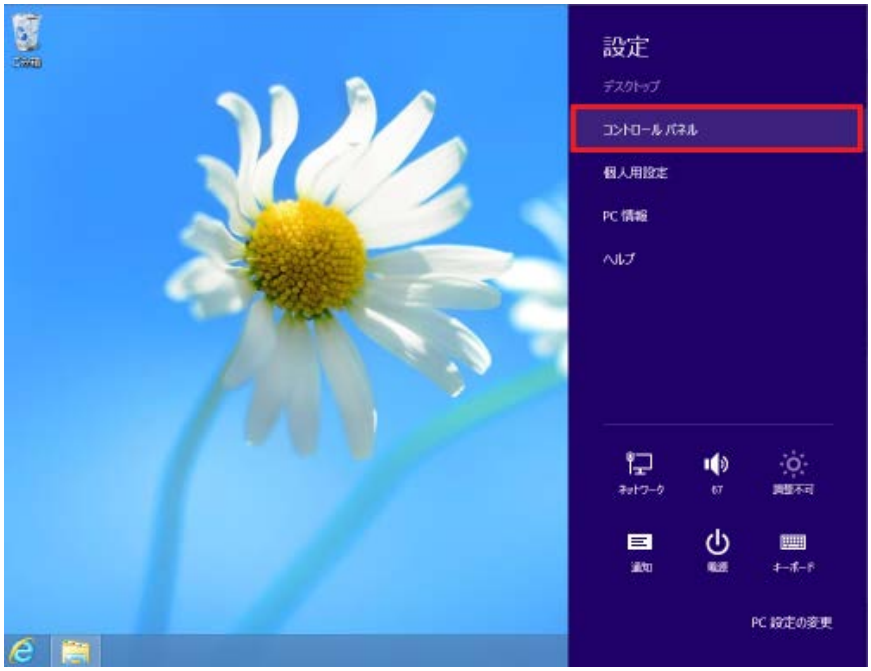


6. 〔完了〕をクリックする。

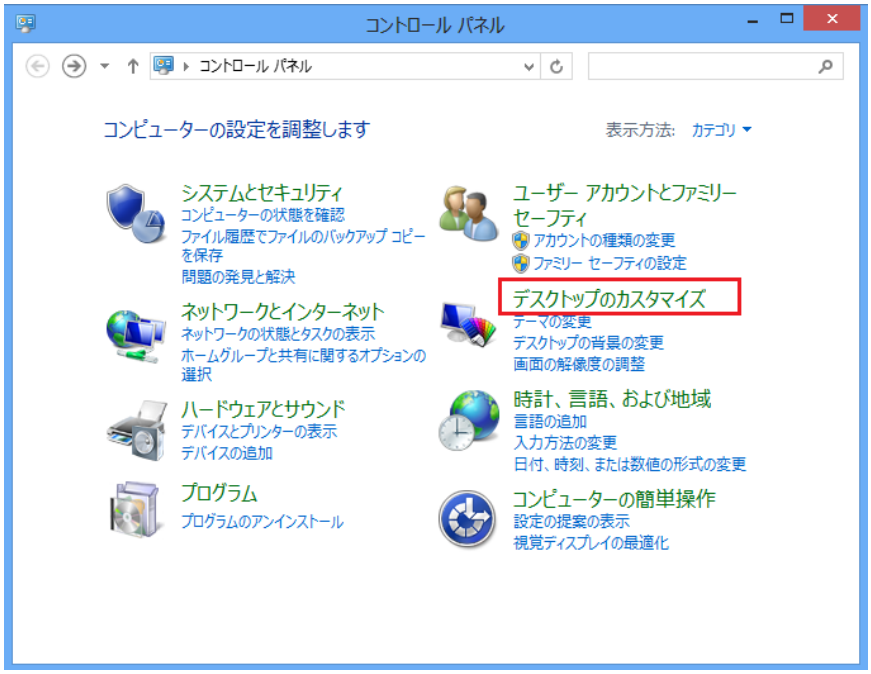


7. デスクトップ右のリボンから、〔設定〕をクリックする。

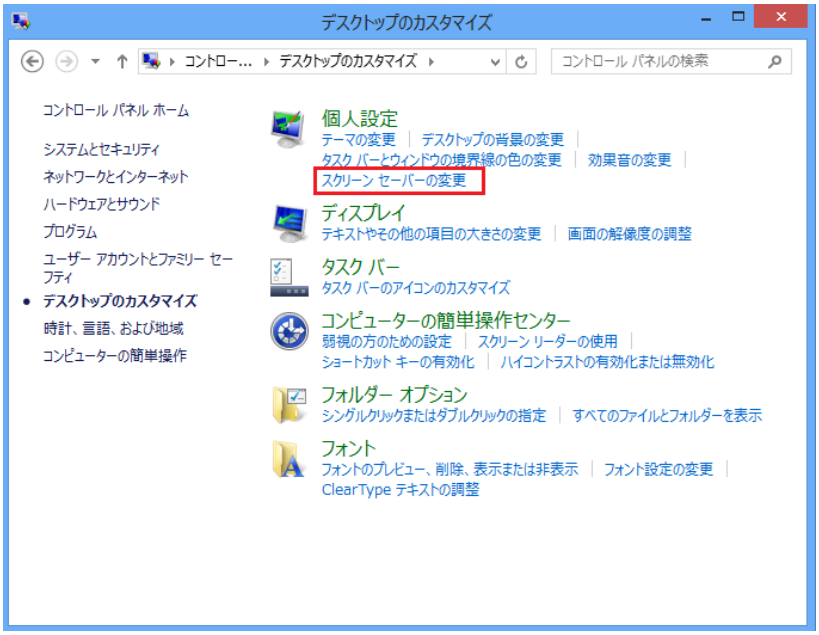
8. 〔コントロールパネル〕をクリックする。



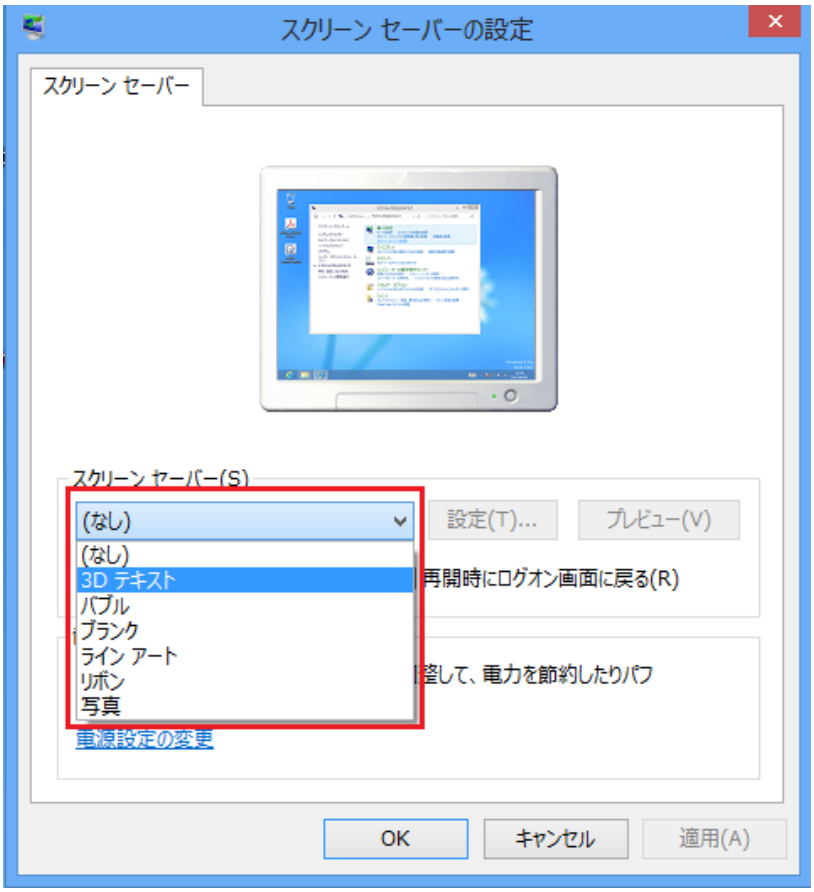
9. 〔デスクトップのカスタマイズ〕をクリックする。



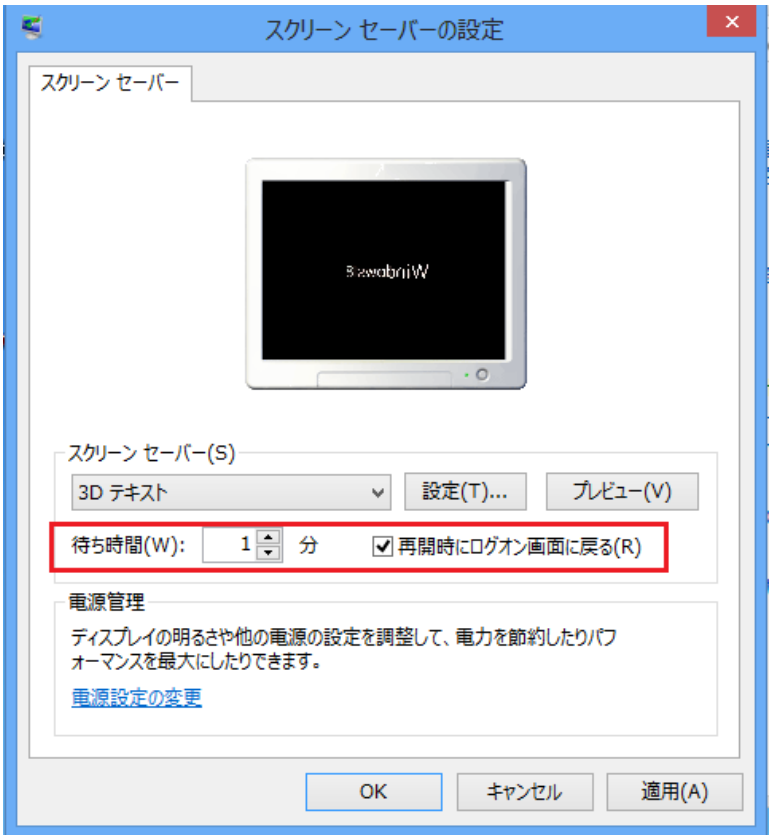
10. 〔スクリーンセーバーの変更〕をクリックする。



11. スクリーンセーバーとして〔(なし)〕及び〔(バブル)〕以外を選択する。



12. 画面がロックするまでの待ち時間を適切に設定（5 分以内での設定を推奨）したうえで、〔再開時にログオン画面に戻る〕のチェックボックスをオンにし、〔適用〕、〔OK〕の順にクリックする。

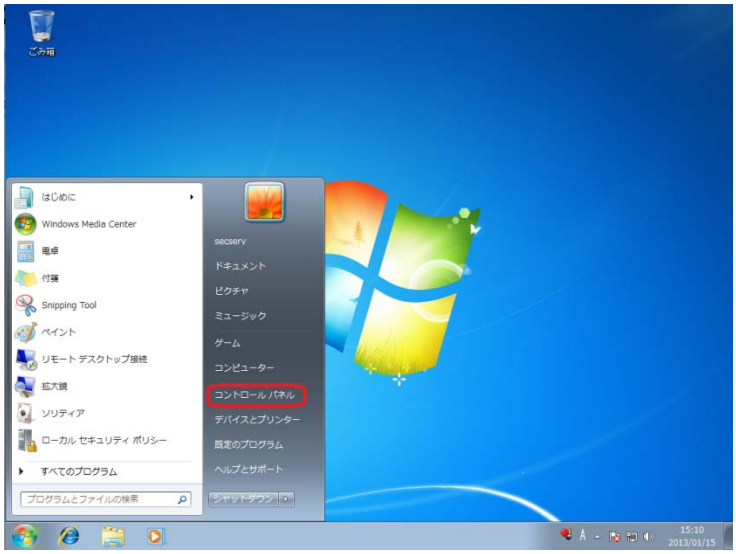


A.2　端末ロックによる利用者認証の安全性強化（利用者認証失敗時の動作設定方法）

- **Windows 7、Windows 8 共通**

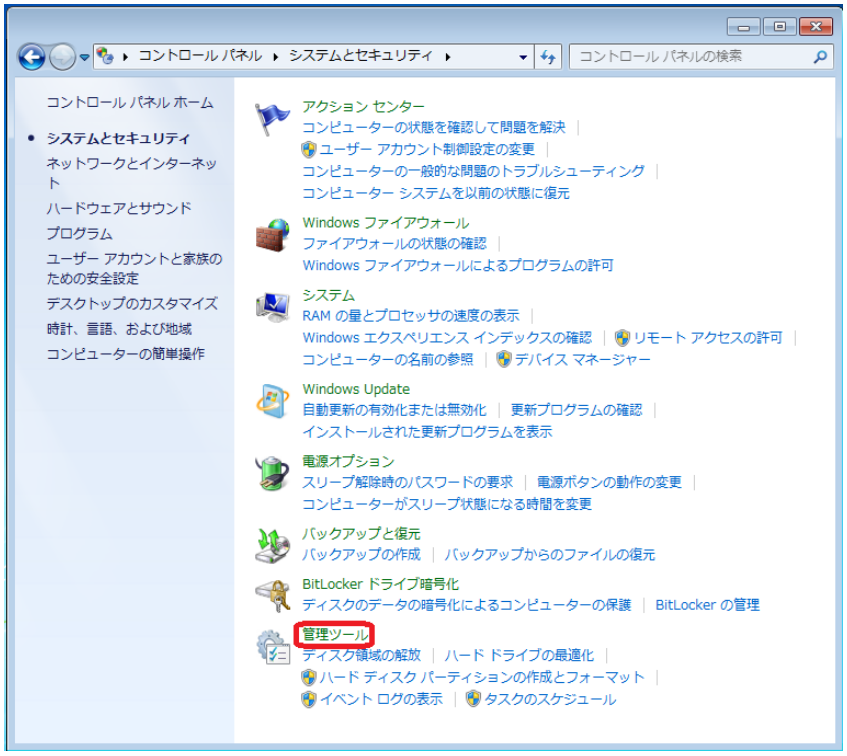
1. 以下の方法でローカルセキュリティポリシー（Windows 7）またはローカルグループポリシー（Windows 8）を開く。

- Windows 7 の場合
  - 〔スタート〕ボタンからコントロールパネルを起動する。

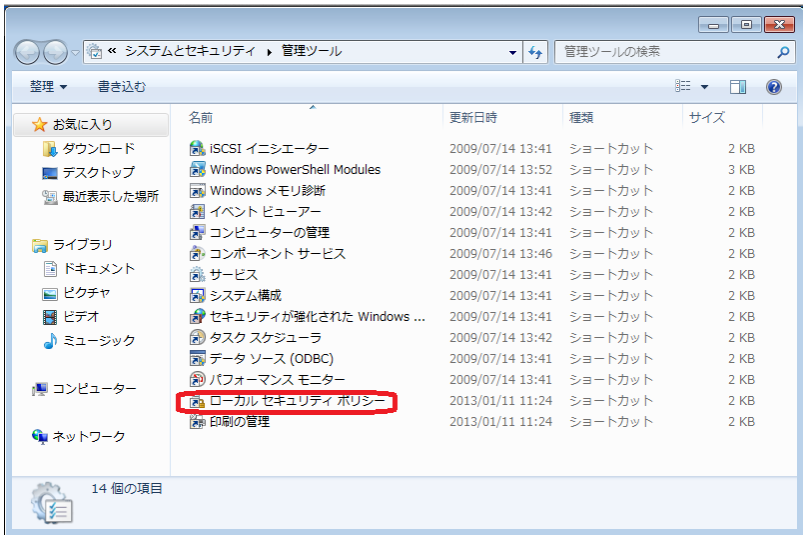


  - 〔システムとセキュリティ〕をクリックする

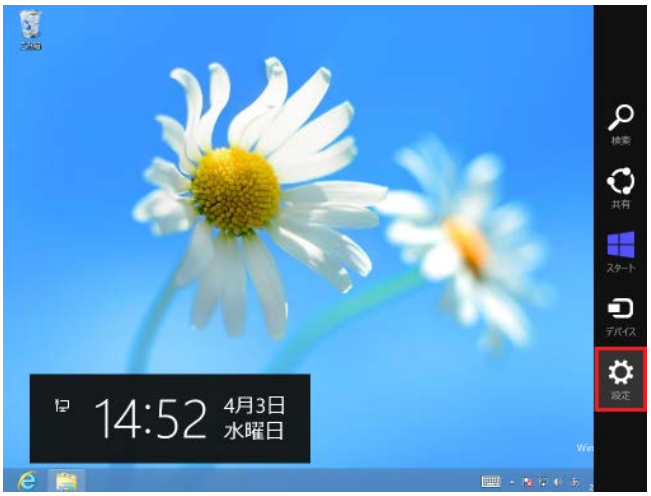
➢　〔管理ツール〕をクリックする。



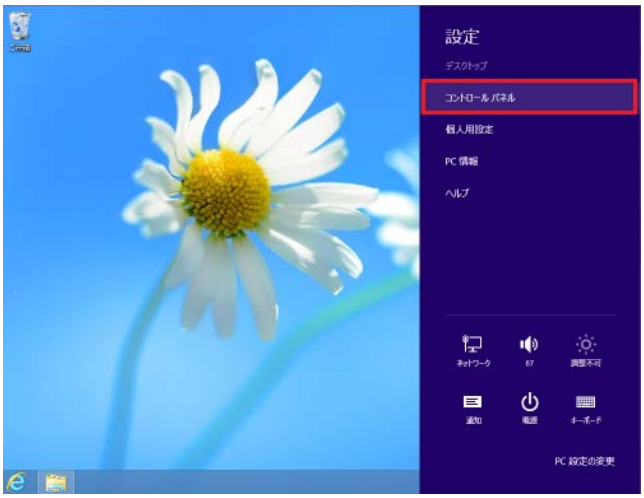
➢　〔ローカルセキュリティポリシー〕をダブルクリックする。



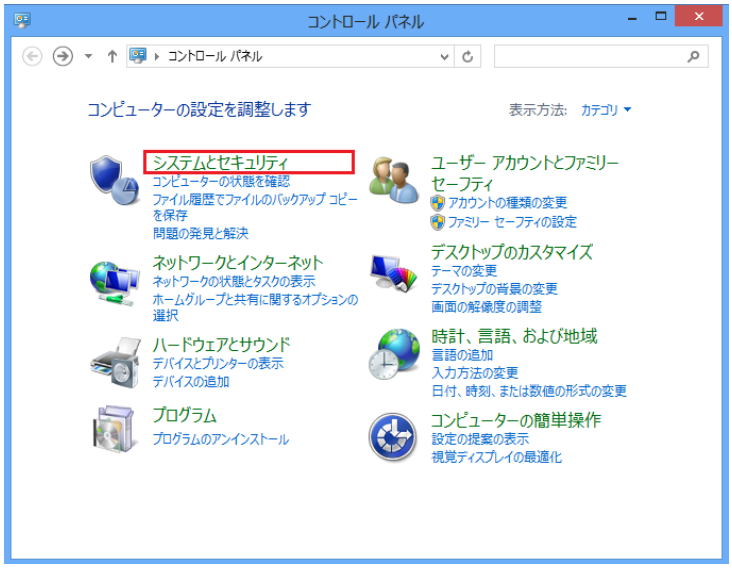
- Windows 8 の場合
  - デスクトップ右のリボンから、〔設定〕をクリックする。



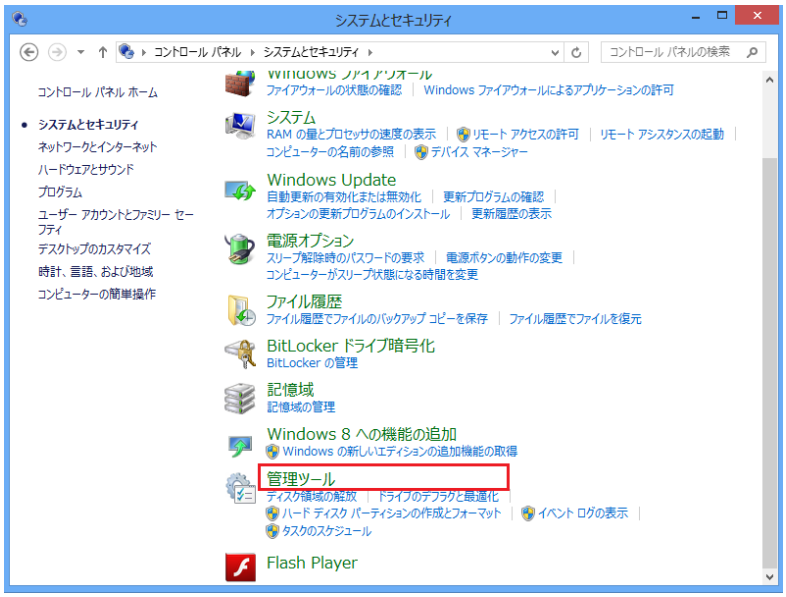
  - 〔コントロールパネル〕をクリックする。



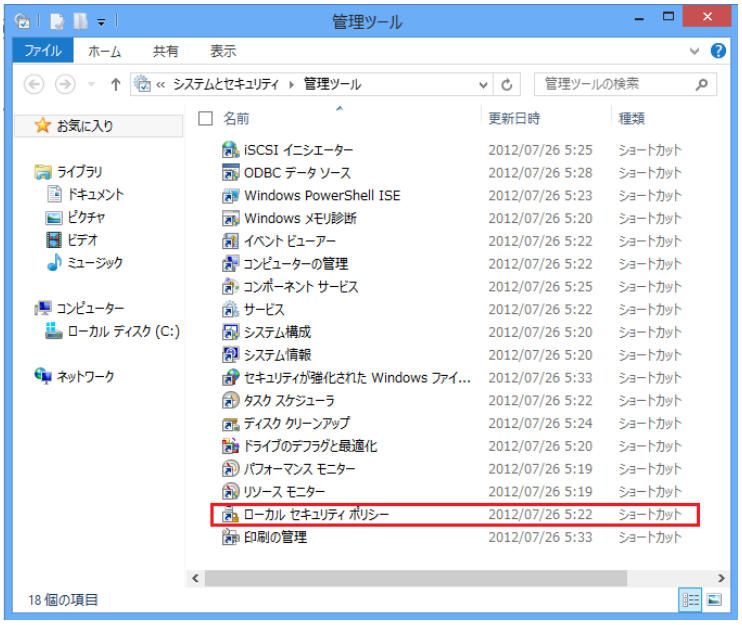
  - 〔システムとセキュリティ〕をクリックする。



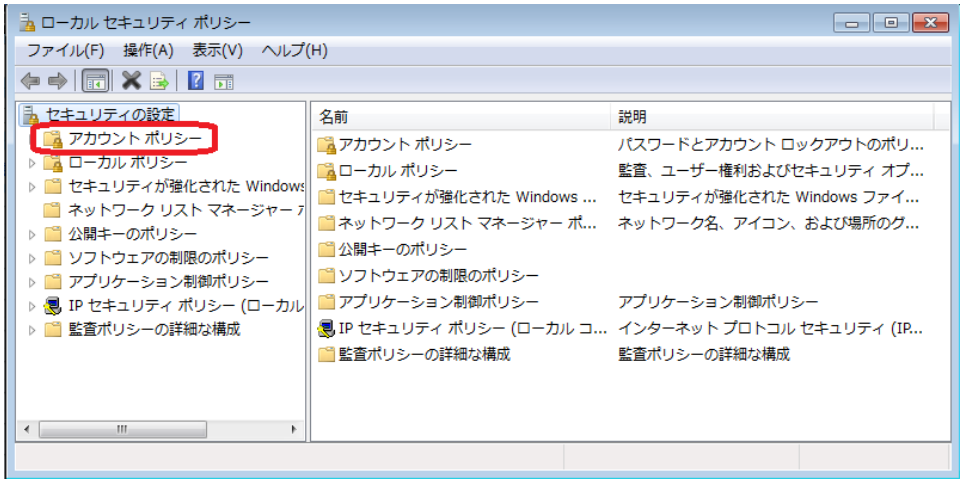
➢　〔管理ツール〕をクリックする。



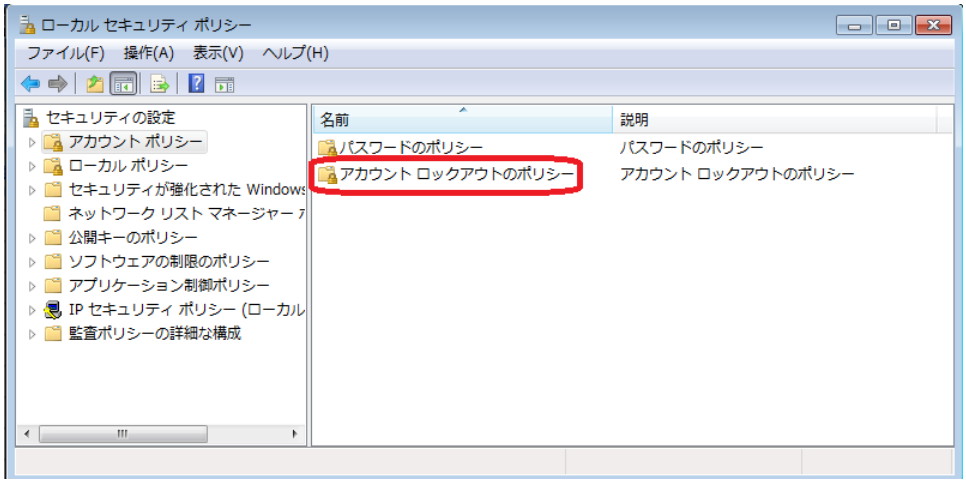
➢　〔ローカルセキュリティポリシー〕をダブルクリックする。



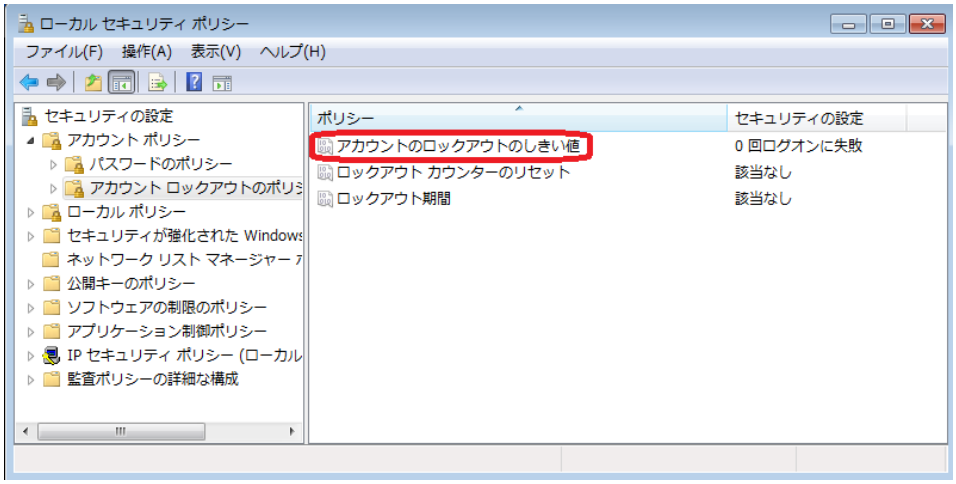
2. 〔アカウントポリシー〕をクリックする。



3. 〔アカウントロックアウトのポリシー〕をダブルクリックする。

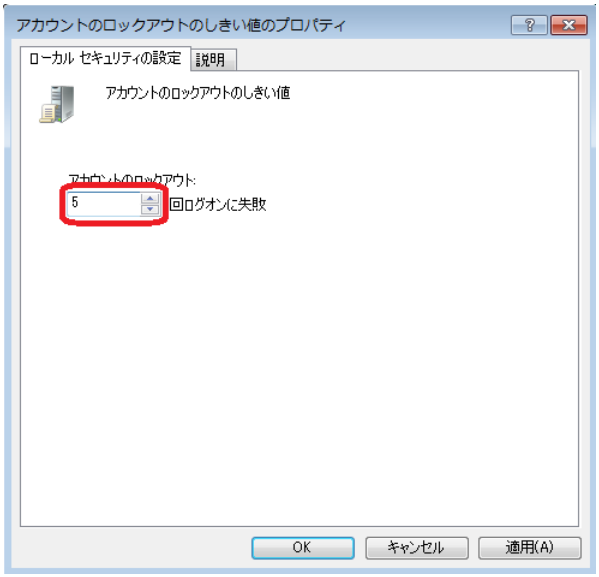


4. 〔アカウントロックのしきい値〕をダブルクリックする。



5. テキストボックスに、何回ログオンに失敗したらロックアウトするか、回数を入力し、〔OK〕をクリックする。

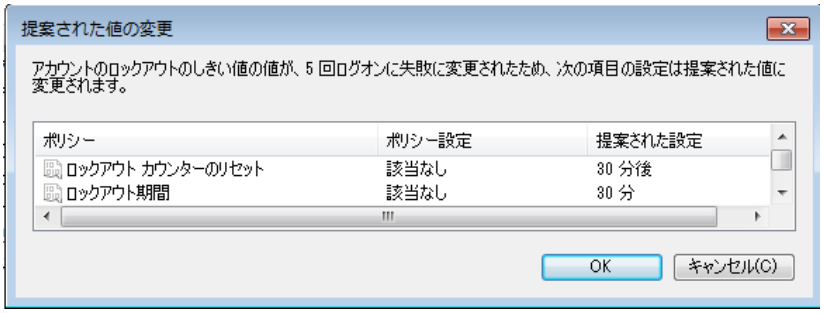
※ 回数は持ち歩く情報の情報価値レベルに応じて決定する。例として、オンラインバンキングではおおむね 5 回に設定されている



6. 〔ロックアウトカウンターのリセット〕及び〔ロックアウト期間〕の設定が自動的に変更されるので、内容を確認のうえ、〔OK〕をクリックする。必要に応じて、それらの設定を変更する。

※ ロックアウトカウンターは利用者認証の連続失敗回数をカウントしたものである。リセット時間が経過すると連続失敗回数が 0 に戻る

※ ロックアウト時間は、利用者認証の連続失敗によるロックアウトが解除され、利用者認証が再開できるようになるまでの時間を決めるものである



C.1　ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

- **EFSによるフォルダ暗号化** [6]

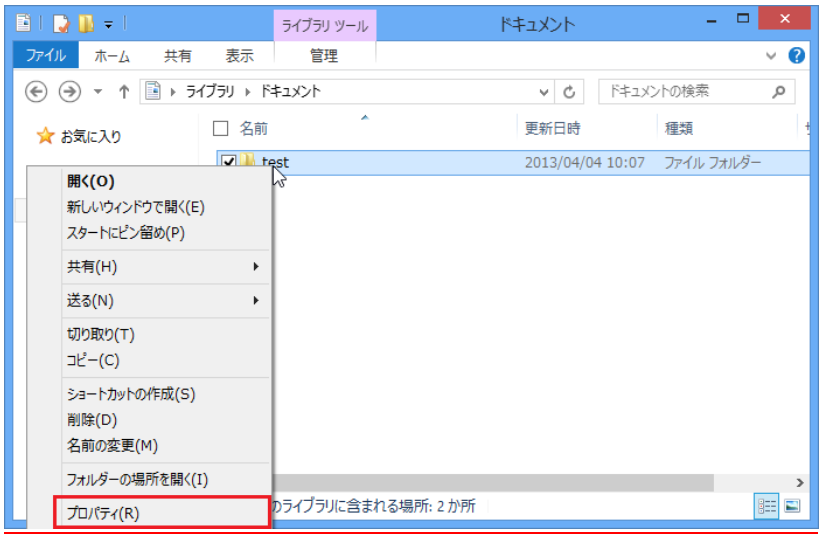
※ パソコン等の機種によっては、BIOS 設定を変更することにより、あらかじめ EFS によるドライブ暗号化（BIOS 設定でのセキュリティ項目中にあるハードディスク暗号化やハードディスク保護を有効化）を行うことができる。この設定をした場合、個々にフォルダ暗号化の設定をしなくても自動的にフォルダ暗号化が有効になる

※ なお、BIOS 設定に失敗するとパソコン自体が起動しなくなる恐れもあるため、必要があれば BIOS の設定変更を行う前にパソコン等の知識を有する人の助言を仰ぐこと

※ EFS ではシステムファイルの暗号化はできない

【注意】暗号化や復号に使用する証明書を紛失すると復号できなくなるため、証明書のバックアップ [7]をし、紛失しないように安全な場所に別途保管すること。特に、OSの再インストールをした場合、EFSで利用する暗号鍵が自動的に更新され、証明書も新たに設定されるため、証明書のバックアップがないと復号できなくなることに注意

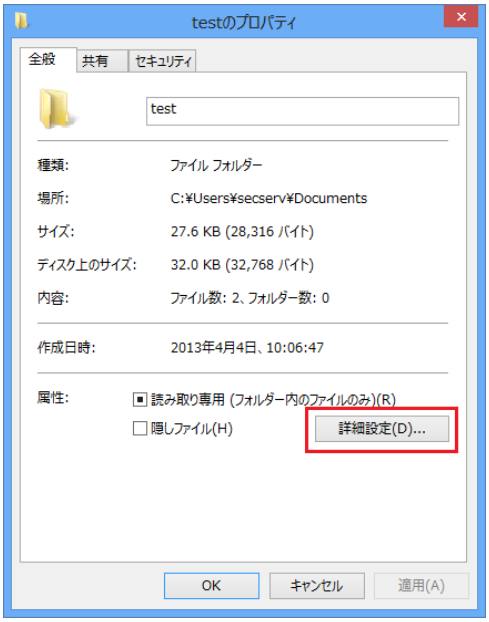
1. 暗号化するフォルダを右クリックし、〔プロパティ〕をクリックする。



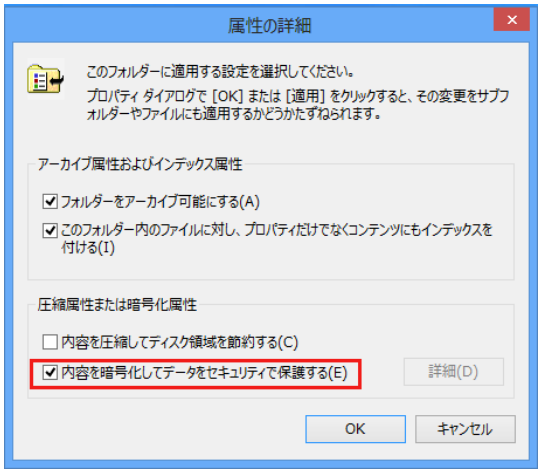
[6] EFS は、Windows7 Professional、Windows7 Ultimate、Windows7 Enterprise、Windows8 Professional. Windows8 Enterprise（ボリュームライセンス提供のみ）で全ての機能が使用可能

[7] http://windows.microsoft.com/ja-JP/windows7/Back-up-Encrypting-File-System-EFS-certificate 参照

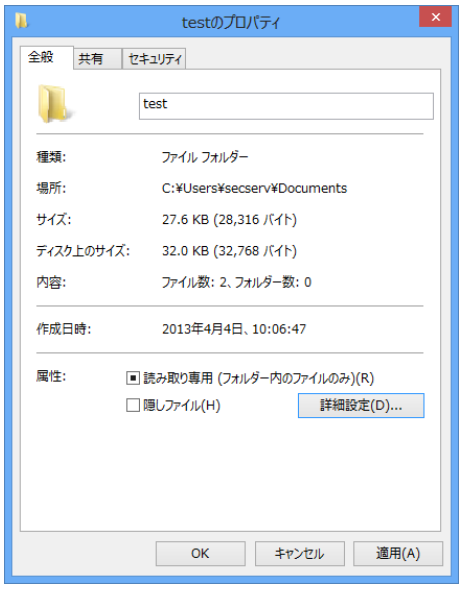
2. 〔詳細設定〕をクリックする。



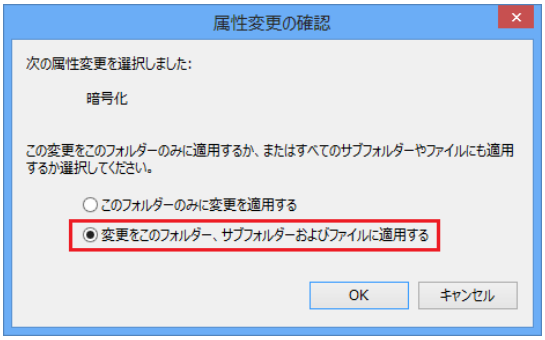
3. 〔内容を暗号化してデータをセキュリティで保護する〕チェックボックスをオンにし、〔OK〕をクリックする。



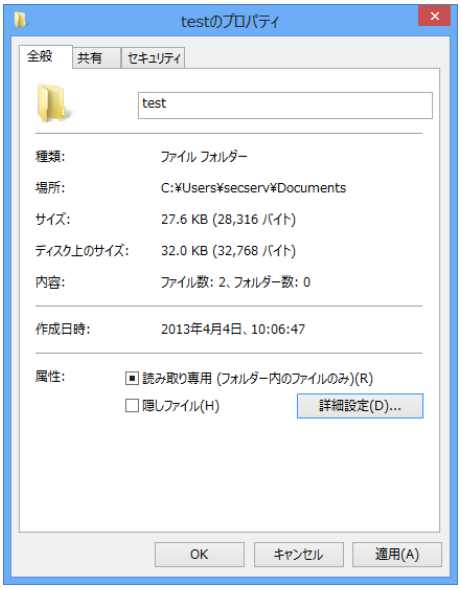
4. 〔適用〕をクリックする。



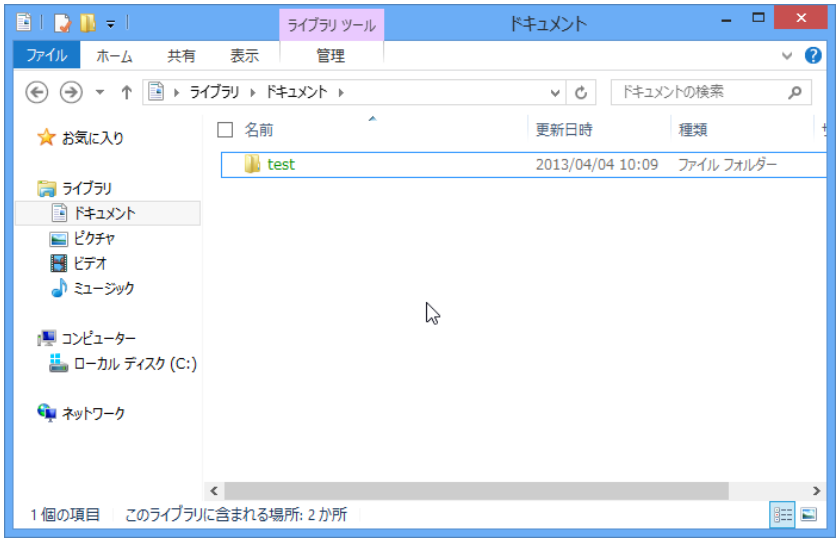
5. 〔変更をこのフォルダー、サブフォルダーおよびファイルに適用する〕ラジオボタンをオンにし、〔OK〕をクリックする。



6. 〔OK〕をクリックする。



7. 暗号化されたフォルダは緑色で表示される。



- **BitLockerによるドライブ暗号化** [8]

【警告】ドライブ暗号化は、まれに暗号化設定に失敗することがあり、最悪の場合、暗号化前の状態にすら戻せなくなることがあるため、暗号化を行う前に必ずバックアップを取ること

【注意】回復キー[9]を紛失すると非常時にPCを使える状態にすることができなくなるので、紛失しないように安全な場所に別途保管すること

■ **Windows 8 Professional 版以上がインストールされた TPM 搭載のパソコンで、TPM に保存されている暗号鍵を使って暗号化及び復号を行い、回復キーを USB メモリに保存するケース**

※ TPM を利用することで、「C.5 暗号鍵の管理強化」も満たす

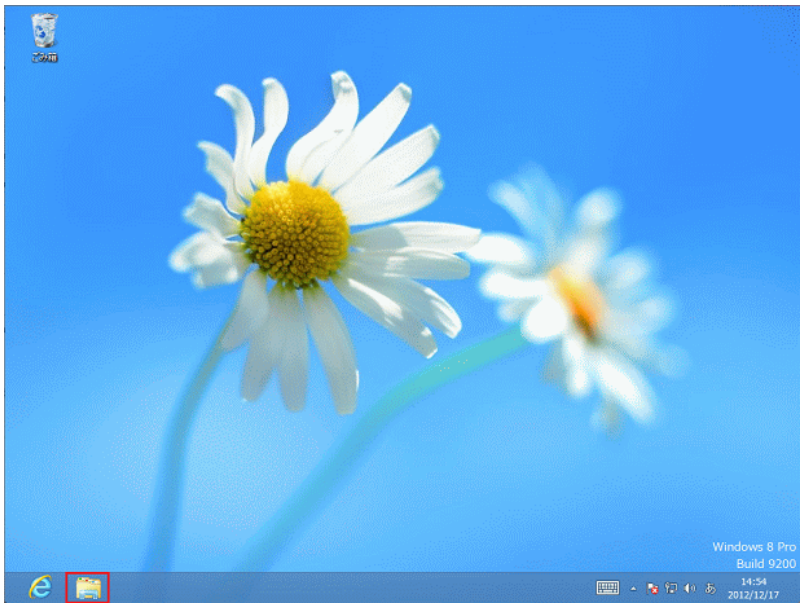
※ 上記以外のケースで BitLocker を利用する際には手順や設定内容が一部異なるところがある。詳しくは、マイクロソフトが提供している情報を参考にすること

---

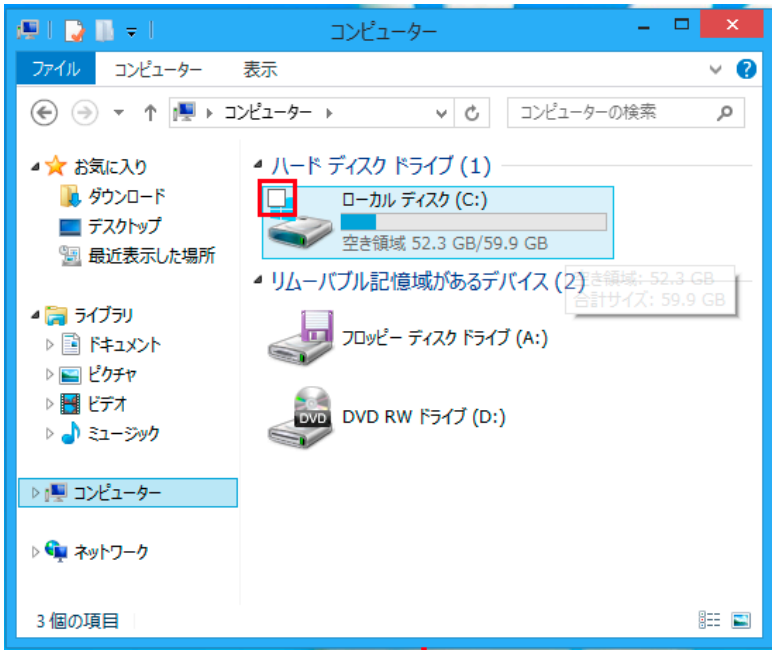
[8] BitLocker は、Windows Vista Ultimate、Windows Vista Enterprise、Windows 7 Ultimate、Windows 7 Enterprise、Windows 8 Professional、Windows 8 Enterprise、Windows Server 2008 で使用可能

[9] BitLocker では、復号のための暗号鍵とそれを紛失した時のための回復キーの 2 つの暗号鍵が生成される

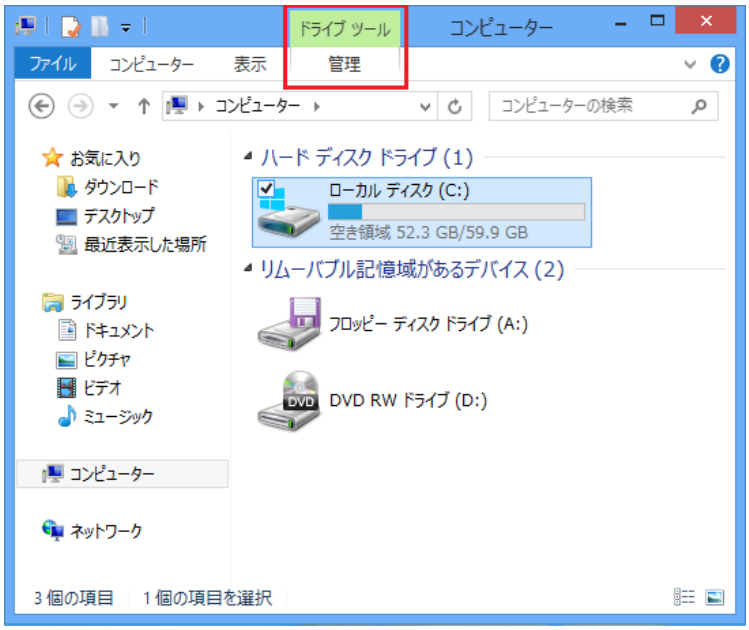
1. デスクトップから〔エクスプローラー〕を起動する。



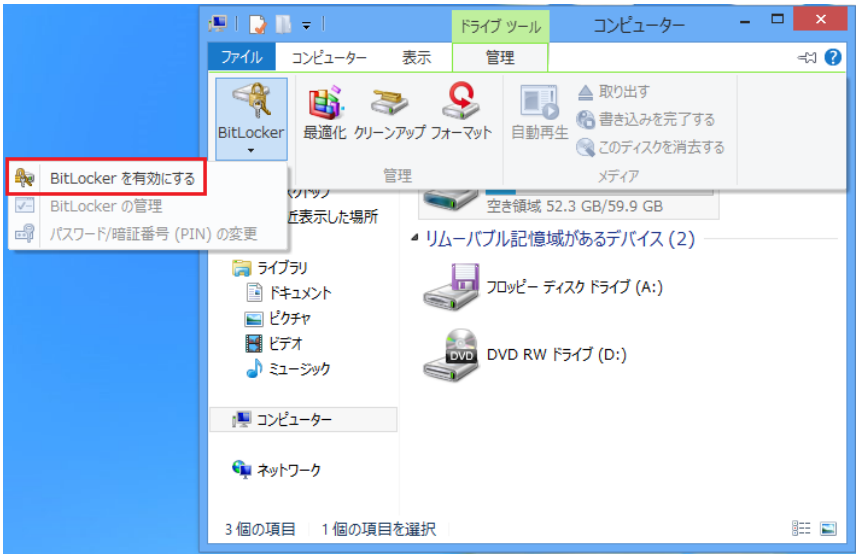
2. 〔コンピューター〕をクリックし、〔ローカルディスク〕の左上にあるチェックボックスをオンにする。



3. 〔ドライブツール〕の〔管理〕タブをクリックする。

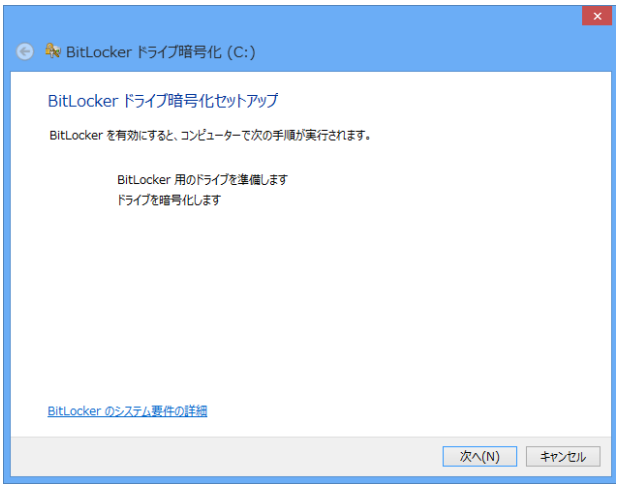


4. 〔BitLocker〕をクリックし、〔BitLocker を有効にする〕を選択する。

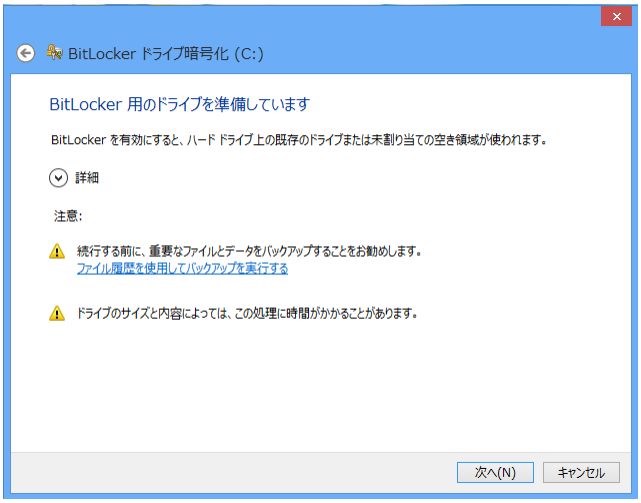


5. BitLocker セットアップのダイアログが表示されるので、〔はい〕をクリックする。

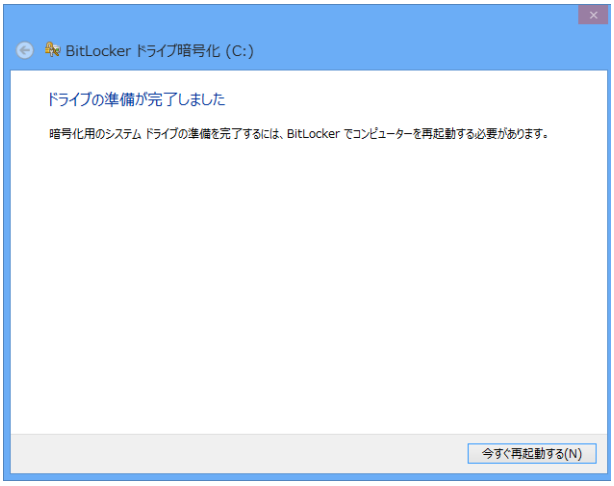
6. PC の構成の確認が行われ、暗号化セットアップのダイアログが表示されるので、〔次へ〕をクリックする。



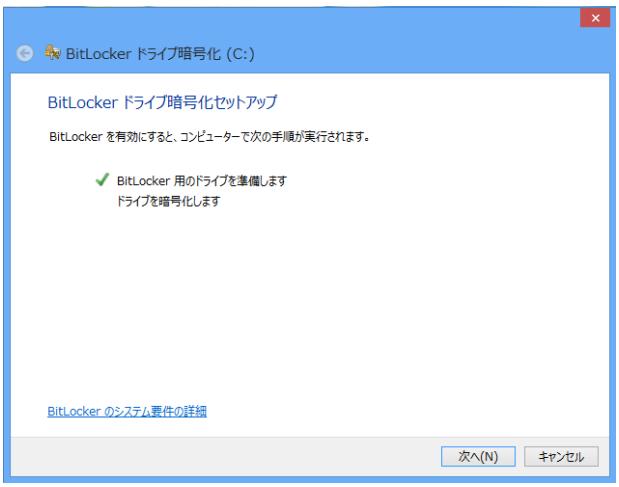
7. ファイルやデータのバックアップを行い、〔次へ〕をクリックする。



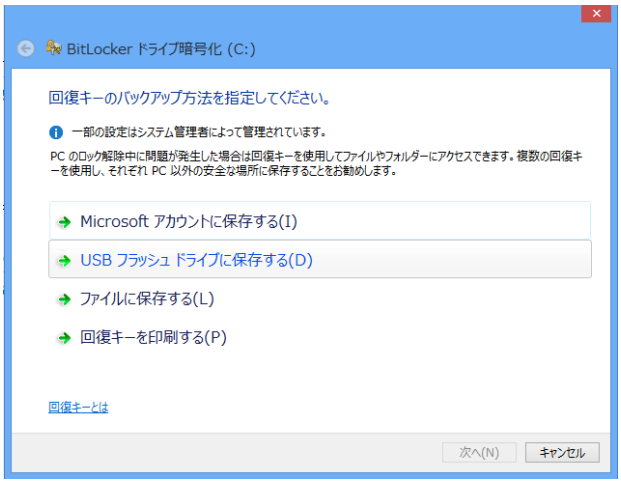
8. 再起動を促すダイアログが表示されるので、〔今すぐ再起動する〕をクリックする。



9. 再起動後、再度暗号化セットアップのダイアログが表示されるので、〔次へ〕をクリックする。

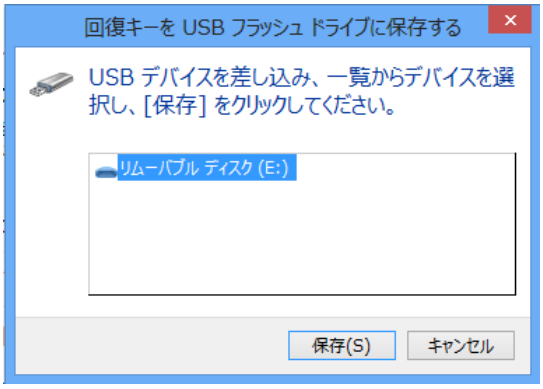


10. 〔USB フラッシュドライブに保存する〕をクリックする。



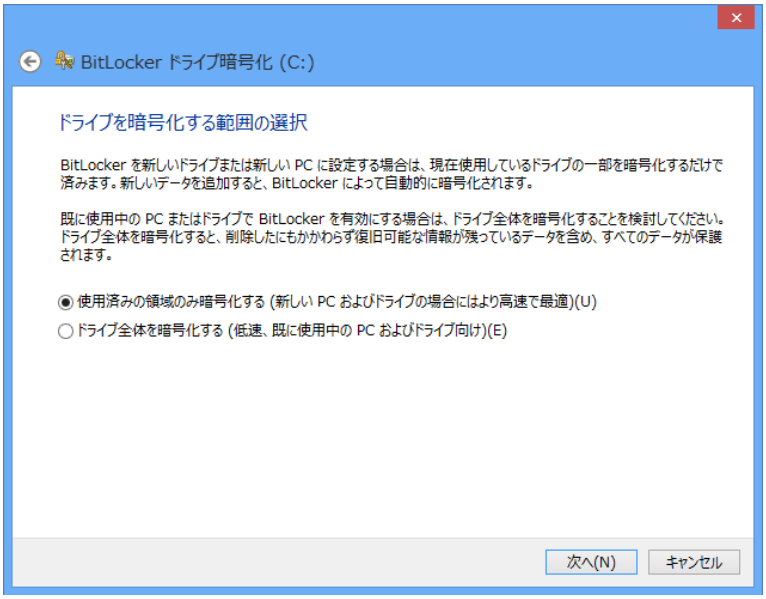
11. USB メモリを挿入し、〔USB フラッシュドライブに保存する〕を選択して〔保存〕をクリックする。

※ 回復キーを入れた USB メモリは、パソコンとは隔離された安全な場所に保管し、非常時以外は利用できないようにすること

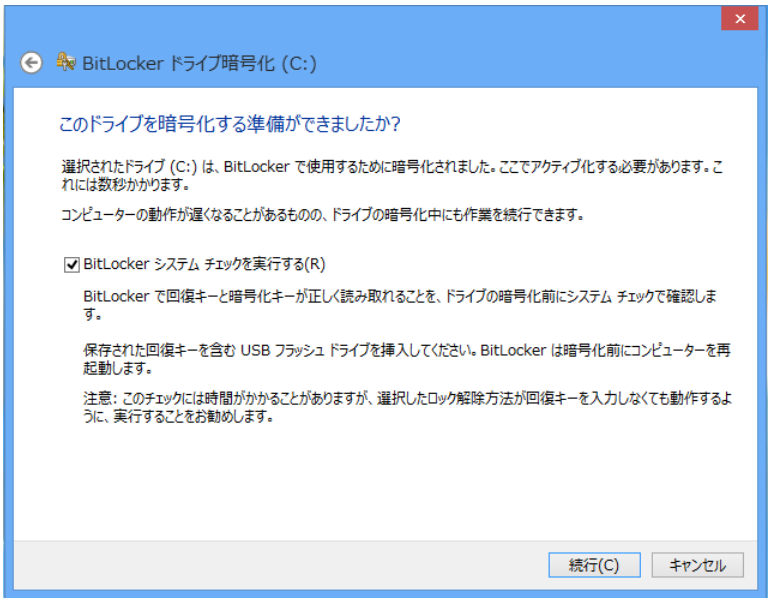


12. 〔使用済みの領域のみ暗号化する〕または〔ドライブ全体を暗号化する〕のどちらかを選択し、〔次へ〕をクリックする。

※ 〔使用済みの領域のみ暗号化する〕を選択した場合、Windows が使用していないと判断した領域は、たとえデータが残っていたとしても、暗号化されないことに注意。実際には、表面上は削除されたデータであっても、データ本体はそのまま残っていることがある

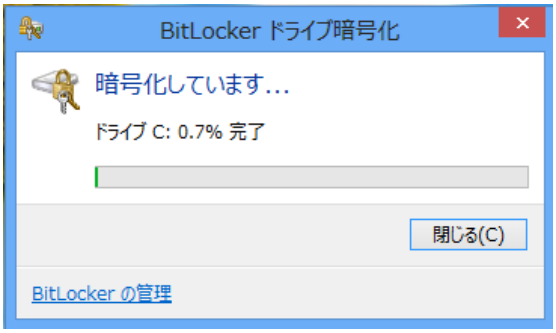


13. 〔BitLocker システムチェックを実行する〕のチェックボックスをオンにし、〔続行〕をクリックする。



14. 再起動を促すダイアログが表示されるので、〔今すぐ再起動する〕をクリックする。

15. 再起動後、暗号化が開始される。



16. 暗号化が完了すると、以下のダイアログが表示される。

② iOS 6 での設定方法一例

A.1　端末ロックによる利用者認証の有効化（利用者認証の設定方法）

【注意】4 桁パスコードは、簡易的な端末ロックにすぎないことに注意。テンキーでパスコードを入力するので、ショルダーハッキング（肩越しの覗き見）やテンキーの汚れなどでもパスコードの入力位置がわかり、パスコードが特定できることも多い

【注意】「A.2　端末ロックによる利用者認証の安全性強化」の対策と併用することを強く推奨する

1. 〔設定〕から〔一般〕をタップする。

2. 〔パスコードロック〕をタップする。

3. 〔パスコードをオンにする〕をタップする。

4. 4 桁のパスコードを入力する。

5. 再度パスコードを入力する。

6. 〔パスコードを要求〕をタップする。

7. パスコードを要求するまでの時間を適切に設定（デフォルトでは即時）し、タップする。

A.2　端末ロックによる利用者認証の安全性強化

- 端末ロックアウトの設定（利用者認証失敗時の動作設定方法）

【警告】 iOS 6 では 10 回連続して端末ロックによる利用者認証に失敗すると**自動的に初期化**されるように設定することが可能である。なお、**初期化されると保存されている全データが消去される**ため、必要に応じて、バックアップを取っておくこと

1.　〔設定〕から〔一般〕をタップする。

2.　〔パスコードロック〕をタップする。

3. 〔データを消去〕をオンにする。

4. 〔使用〕をタップする。

- **簡単なパスコード[10]以外を使えるようにする**

1. 〔設定〕から〔一般〕をタップする。

2. 〔パスコードロック〕をタップする。

[10] iOS では 4 桁の PIN（暗証番号）のことを「簡単なパスコード」、それ以外のいわゆるパスワードのことを「(簡単ではない）パスコード」と呼んでいる

3. 〔簡単なパスコード〕をオフにする。

4. パスコードを入力する。

5. 新しいパスコードを入力し、〔次へ〕をタップする。

【注意】 パスコードについては、解説編 2.4.2.2 節を踏まえ、適切に設定すること。最低でも英数字（0-9，A-Z，a-z）8 文字以上とすることを推奨する

6. 再度新しいパスコードを入力し、〔完了〕をタップする。

C.1　ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

- iOS 6 では自動でデータの暗号化が行われるので、**「A.2　端末ロックによる利用者認証の安全性強化」**を実施する。

③ Android 4.x での設定方法一例

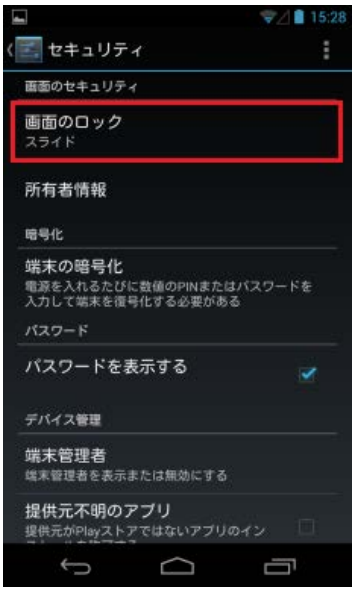
A.1　端末ロックによる利用者認証の有効化（利用者認証の設定方法）

【注意】PIN は、簡易的な端末ロックにすぎないことに注意。テンキーで PIN を入力するので、ショルダーハッキング（肩越しの覗き見）やテンキーの汚れなどでも PIN の入力位置がわかり、PIN が特定できることも多い

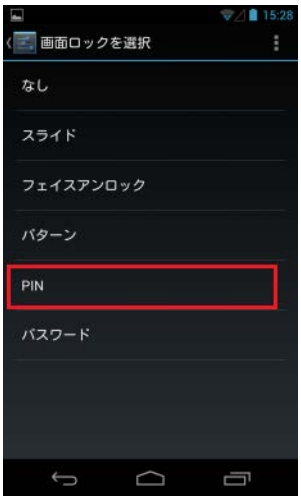
【注意】ここでは、PIN での設定を記載しているが、端末ロックアウトの設定が iOS よりも弱いことに鑑み、極力 PIN ではなく、パスワードを設定することを強く推奨する。「A.2　端末ロックによる利用者認証の安全性強化」も合わせて参照すること

1. 〔設定〕の〔セキュリティ〕をタップする。

2. 〔画像のロック〕をタップする。



3. 〔PIN〕をタップする。



4. PIN を入力し、〔次へ〕をタップする。

5. PIN を再度入力し、〔次へ〕をタップする。

A.2　端末ロックによる利用者認証の安全性強化

- **端末ロックアウトの設定（利用者認証失敗時の動作設定方法）**

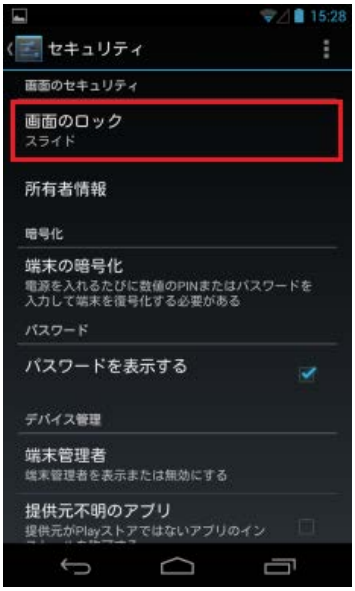
Android4.x では、5 回連続して端末ロックによる利用者認証に失敗すると、一定時間のロックアウト期間が自動的に動作する。ただし、iOS 6 とは違い、初期化されることはない。

※ ロックアウトに至る利用者認証の連続失敗回数やロックアウト期間の設定を変更することができない Android 搭載機種が多い

- **パスワードを設定**

1. 〔設定〕の〔セキュリティ〕をタップする。

2. 〔画像のロック〕をタップする。



3. 〔パスワード〕をタップする。

4. パスワードを入力し、〔次へ〕をタップする。

【注意】 パスワードについては、解説編 2.4.2.2 節を踏まえ、適切に設定すること。
最低でも英数字（0-9, A-Z, a-z）8 文字以上とすることを強く推奨する

5. パスワードを再度入力し、〔OK〕をタップする。

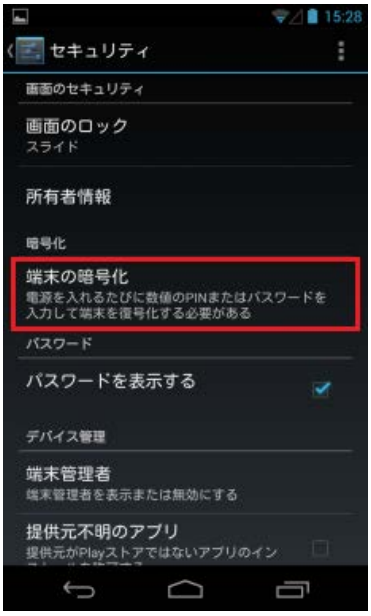
C.1　ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化

※ 事前に**「A.2　端末ロックによる利用者認証の安全性強化」**の設定（パスワード設定）をしておく必要がある

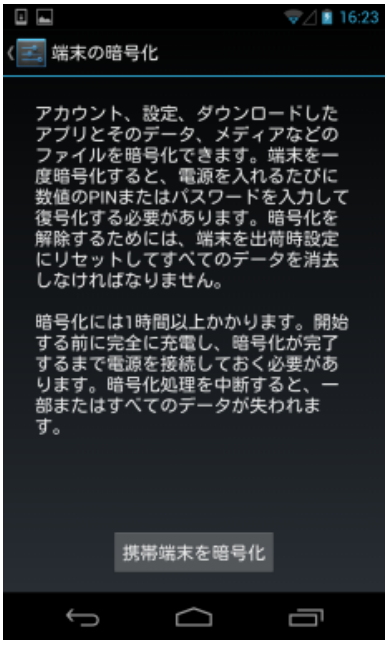
【警告】ドライブ暗号化は、まれに暗号化設定に失敗することがあり、最悪の場合、暗号化前の状態にすら戻せなくなることがあるため、暗号化を行う前に必ずバックアップを取ること

1. 〔設定〕の〔セキュリティ〕をタップする。

2. 〔端末の暗号化〕をタップする。



3. 〔携帯端末を暗号化〕をタップする。



4. 端末ロックによる利用者認証で使うパスワードを入力し、〔次へ〕をタップする。

5. 〔携帯端末を暗号化〕をタップする。

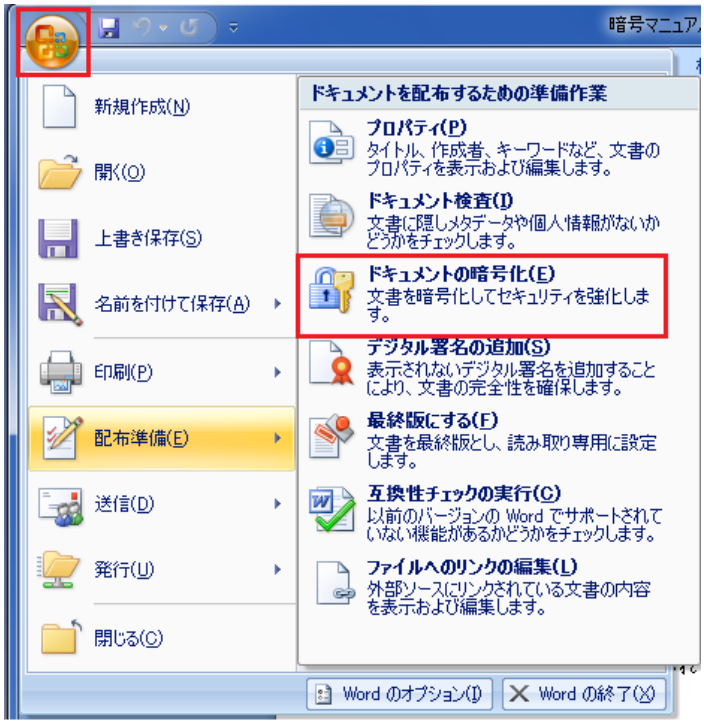
※ SD カードなどの外部メディアが使用可能な場合は、外部メディアも暗号化すること

④ Microsoft Office（Word, Excel, Powerpoint）での設定方法一例

B.1　ファイルへの暗号化設定の有効化（保存方法）

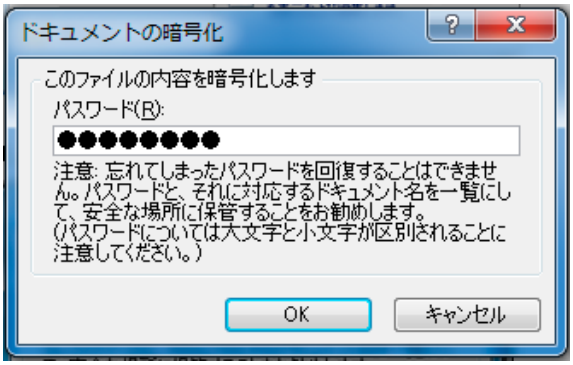
- Office 2007

1. 〔Office ボタン〕をクリックし、〔配布準備〕から〔ドキュメントの暗号化〕を選択する。

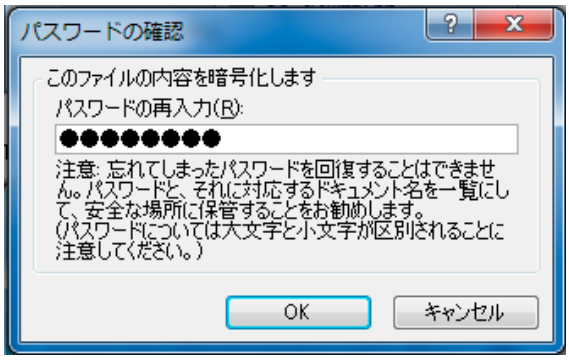


2. パスワードを入力し、〔OK〕をクリックする。

【注意】パスワードについては、解説編 2.4.2.2 節を踏まえ、適切に設定すること



3. 再度パスワードを入力し、〔OK〕をクリックする。

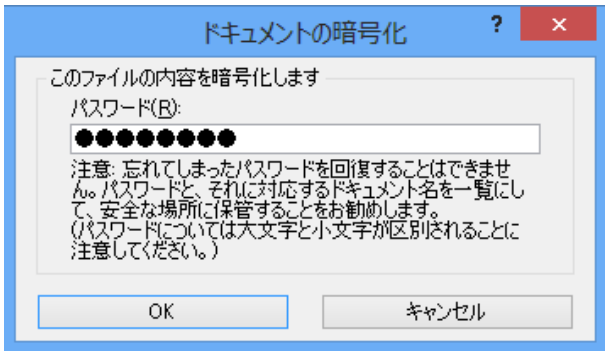


- **Office 2010**

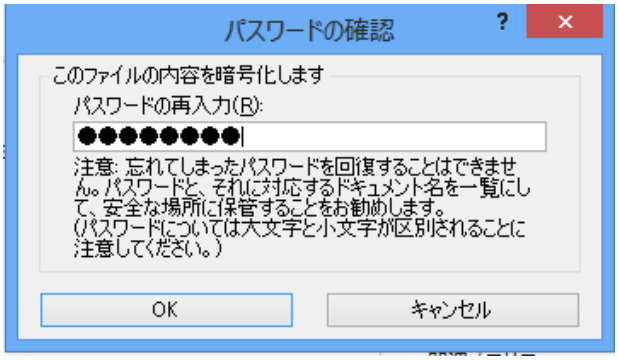
1. 〔ファイル〕タブの〔情報〕を選択し、〔文書の保護〕をクリックして〔パスワードを利用して暗号化〕を選択する。

2. パスワードを入力し、〔OK〕をクリックする。

【注意】パスワードについては、解説編 2.4.2.2 節を踏まえ、適切に設定すること



3.　再度パスワードを入力し、〔OK〕をクリックする。

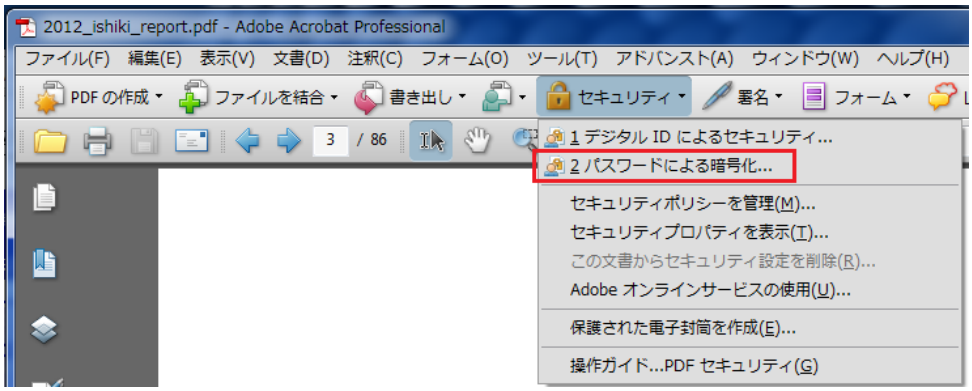


⑤ Adobe Acrobat（PDF ファイル）での設定方法一例

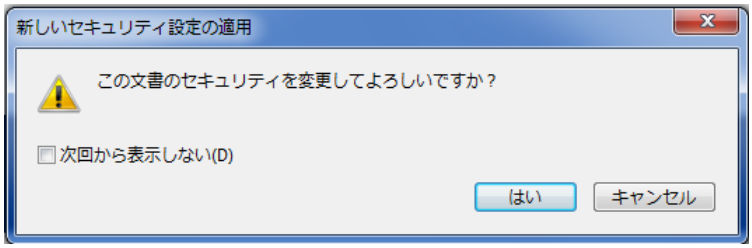
B.1　ファイルへの暗号化設定の有効化（保存方法）

- **Acrobat 9**

1. 〔セキュリティ〕から〔パスワードによる暗号化...〕を選択する。

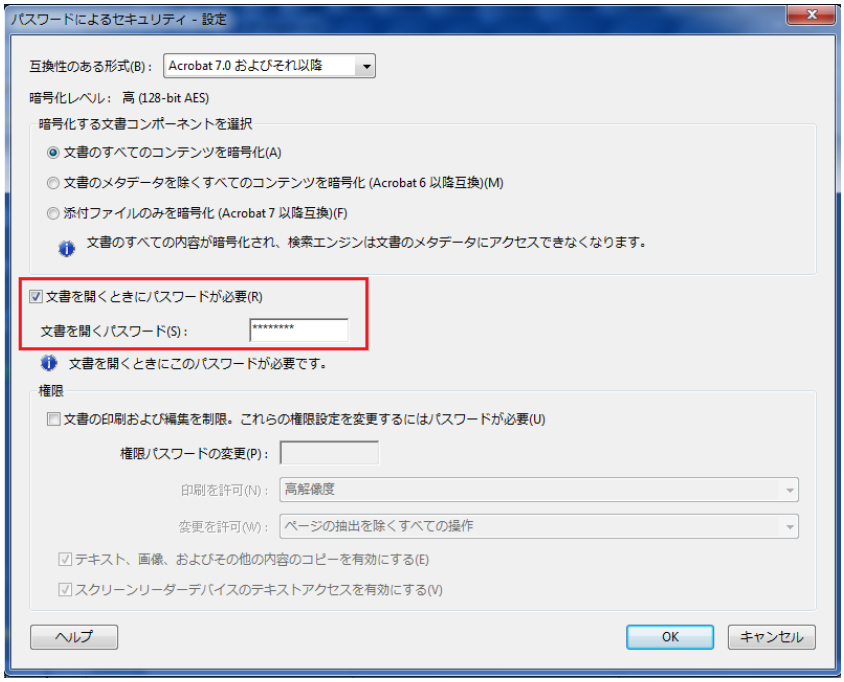


2. 〔OK〕をクリックする。

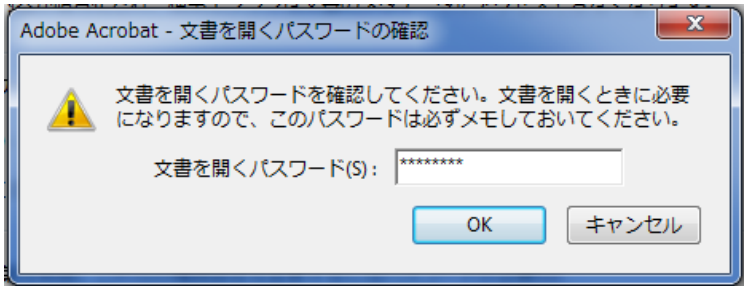


3. 〔文書を開くときにパスワードが必要〕のチェックボックスをオンにし、〔文書を開くパスワード〕にパスワードを入力して〔OK〕をクリックする。

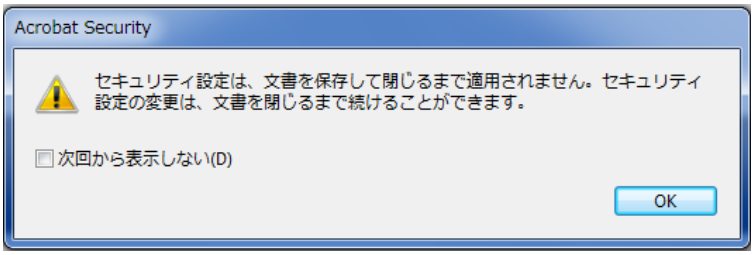
【注意】パスワードについては、解説編 2.4.2.2 節を踏まえ、適切に設定すること



4. パスワードを再度入力して〔OK〕をクリックする。

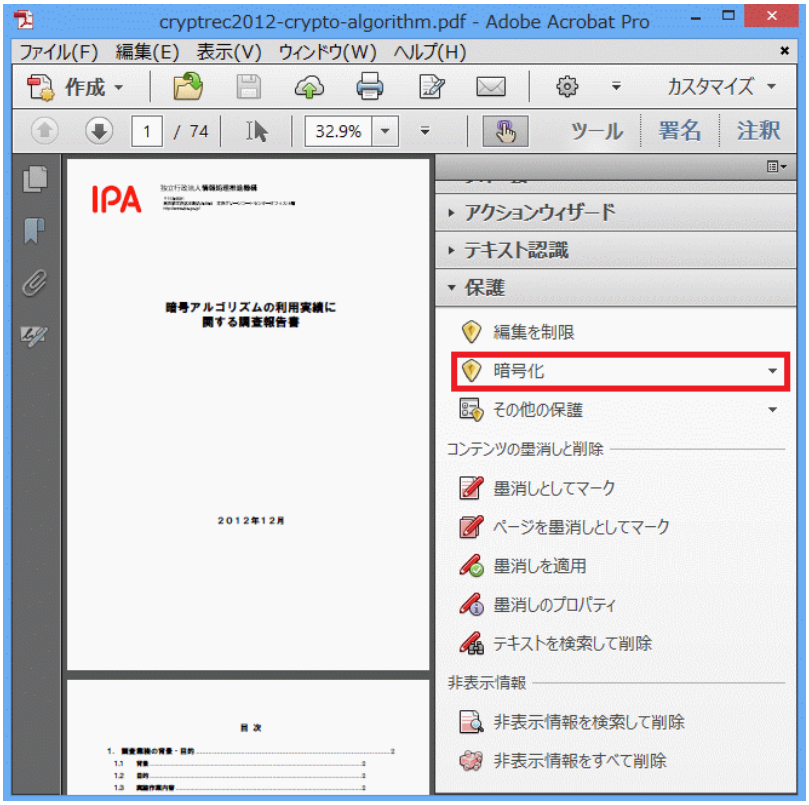


※ 文書を保存するまで、暗号化は有効にならないことに注意

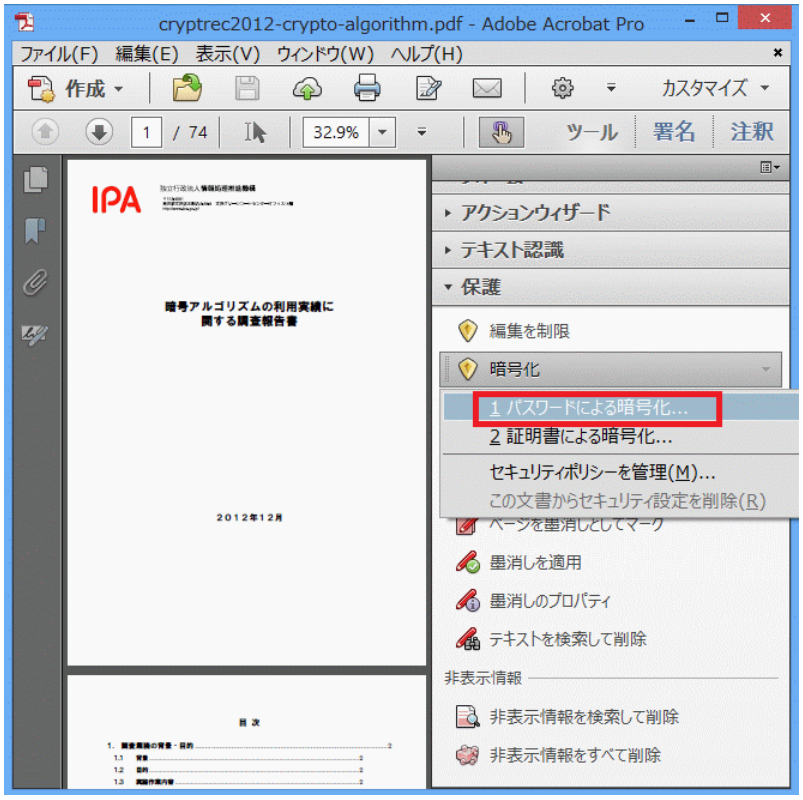


- **Acrobat XI**

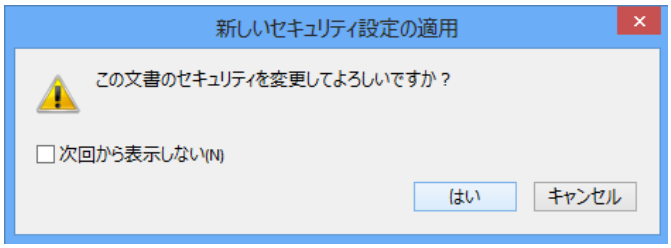
1. 〔ツール〕から〔保護〕をクリックし、〔暗号化〕をクリックする。



2. 〔パスワードによる暗号化〕を選択する。

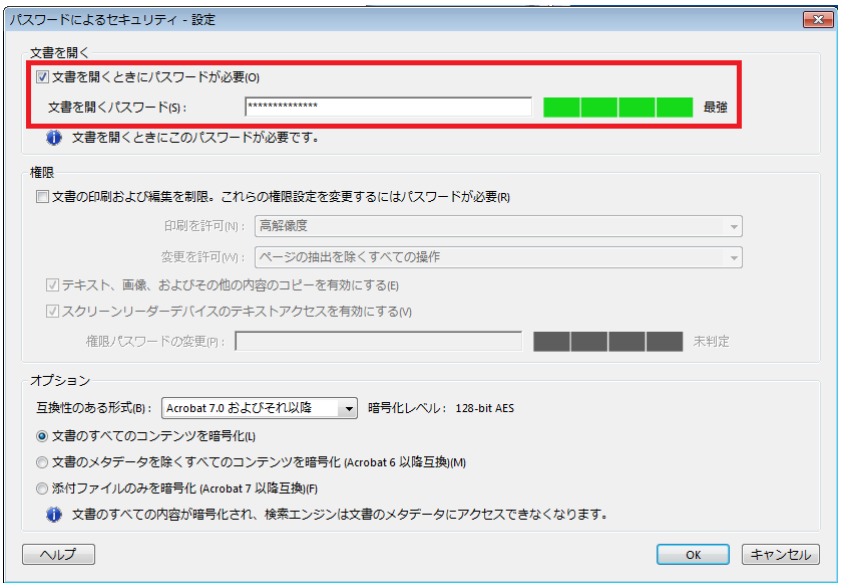


3. 〔OK〕をクリックする。

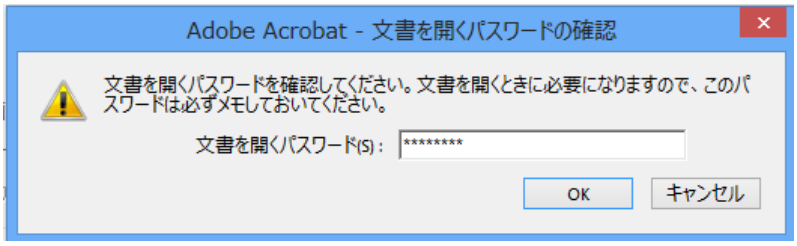


4. 〔文書を開くときにパスワードが必要〕のチェックボックスをオンにし、パスワードを入力して〔OK〕をクリックする。

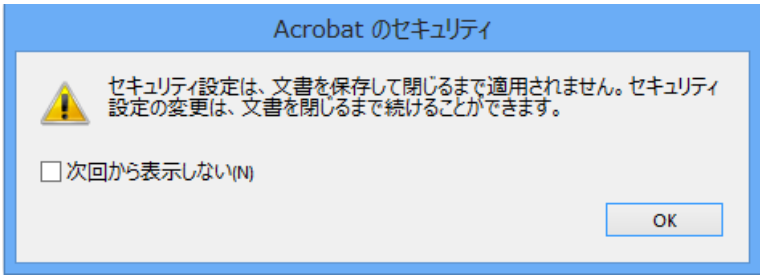
【注意】パスワードについては、解説編 2.4.2.2 節を踏まえ、適切に設定すること。また、パスワード入力欄の横にあるパスワード強度チェックのレベルを参考にすること



5. パスワードを再度入力し、〔OK〕をクリックする。



※ 文書を保存するまで、暗号化は有効にならないことに注意



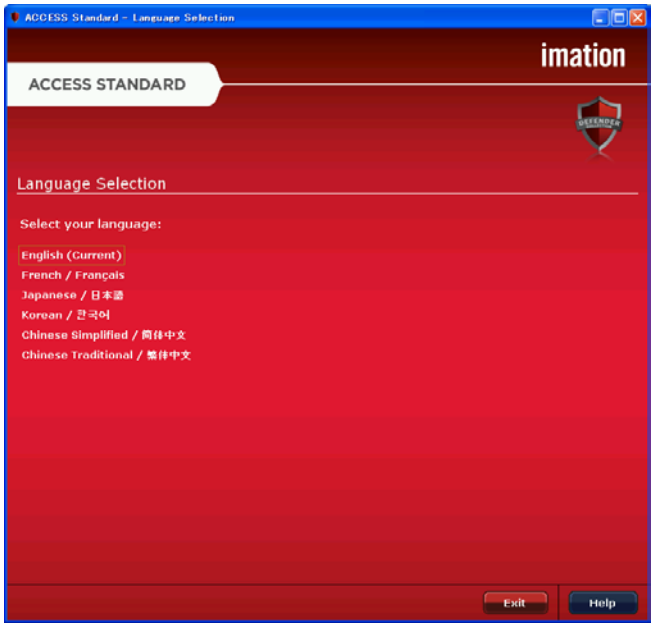
⑥ Imation 指紋認証付 USB メモリでの設定方法一例

C.3　端末起動時および端末ロックによる利用者認証の安全性強化（バイオメトリクス認証設定、回復用パスワード（マスターパスワード）設定）

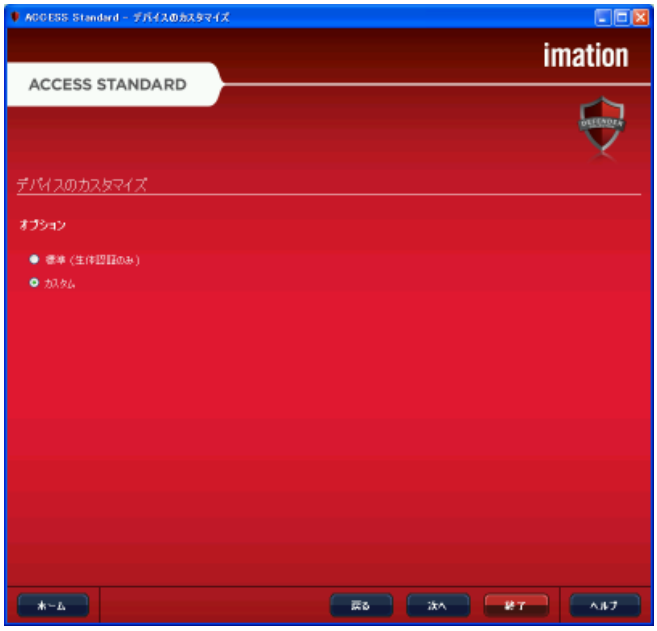
- セキュリティ USB メモリ DEFENDER F200+BIO

※「C.3 端末起動時および端末ロックによる利用者認証の安全性強化」による利用者登録をすれば、自動的に暗号化領域（C.1 ドライブ／フォルダの暗号化設定と端末ロックによる利用者認証の有効化）が設定される。

1. 設定に使用する言語を選択する。



2. オプションで〔カスタム〕を選択する。



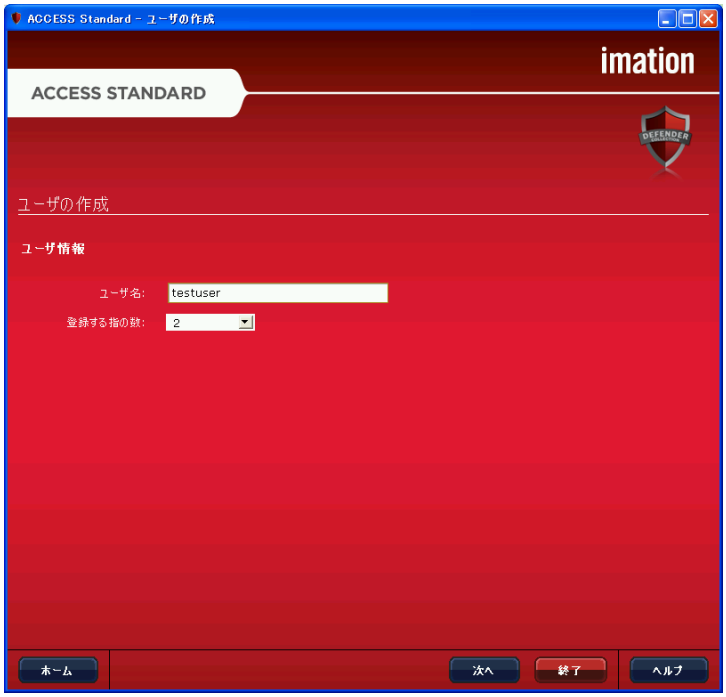
3. バイオメトリクス認証の認証精度（生体認証のセキュリティレベル）を適切なレベルに変更する。

※ ここでの認証精度はデフォルト値が 1/4500 になっている。この意味は、4500 人に 1 人ぐらいの確率で他人を正規の利用者と誤認する可能性があることを示している。したがって、この値が小さいほど安全性が高くなるので、できるだけ小さい値にすることを推奨する。ただし、正規の利用者も認証に失敗する回数が増えて利便性が低下したり、そもそも指紋登録自体ができないといったことが発生する場合があることにも注意が必要。詳しくは、解説編 2.4.2.3 節を参照のこと

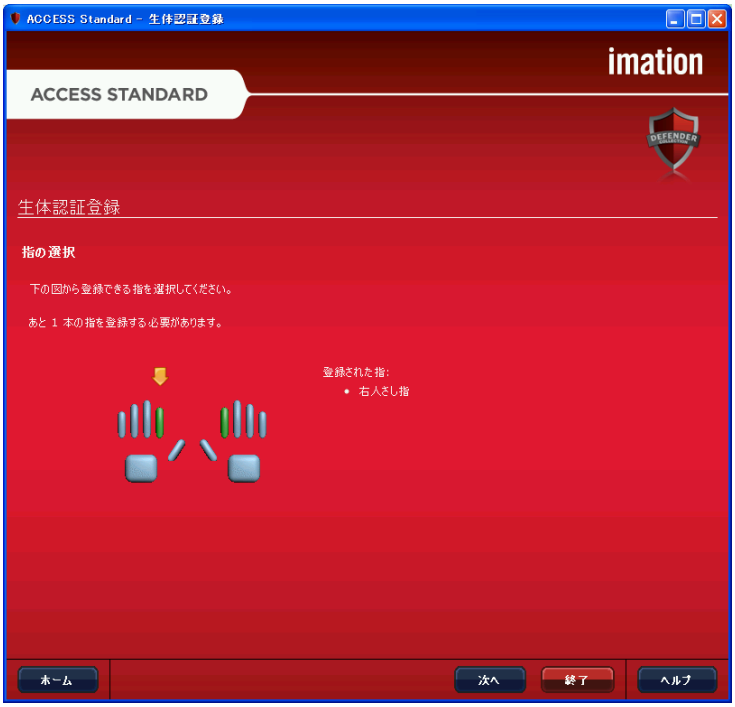
4. 管理ツール使用時に要求する管理者パスワードを入力し、〔次へ〕をクリックする。

【注意】 管理者パスワードについては、解説編 2.4.2.2 節及び 2.4.2.3 節を踏まえ、非常時のみ利用することを前提として、通常時の利用は想定しない、極めて強固なパスワード（完全にランダムに選ばれた長い文字列）を適切に設定すること。また、非常時にだけ取り出せる、安全な場所に記録保管すること。間違っても、携帯させないこと

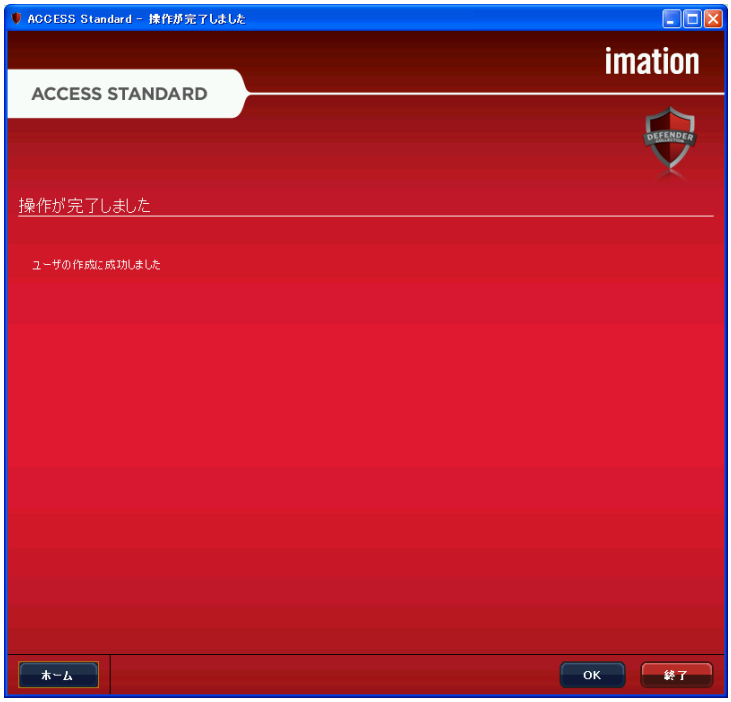
5. ユーザ名と指紋を登録する指の数を入力し、〔次へ〕をクリックする。



6. 登録する指を選択し、〔次へ〕をクリックする。



7. 登録が完了したら、〔OK〕をクリックする。



著作・制作　　独立行政法人 情報処理推進機構（IPA）

編集責任

執筆者　神田 雅透　独立行政法人 情報処理推進機構
山口 利恵　独立行政法人 産業技術総合研究所
一瀬 小夜　独立行政法人 産業技術総合研究所

協力者　満塩 尚史　内閣官房 政府 CIO 室 政府 CIO 補佐官
（経済産業省 CIO 補佐官併任）
中西 悦子　総務省 総合通信基盤局電気通信事業部データ通信課 企画官
二木 真明　アルテア・セキュリティ・コンサルティング 代表
沢田 登志子　一般社団法人 EC ネットワーク 理事
松本 泰　セコム株式会社 IS 研究所
コミュニケーションプラットフォームディビジョン マネージャー
松尾 正浩　三菱総合研究所 公共ソリューション本部 主席研究員
宮内 宏　宮内宏法律事務所 弁護士

〔発 行〕
２０１３年 4月２３日　第1版

〔問い合わせ先〕

本マニュアルについてのご意見・ご要望がございましたら、下記までご連絡ください。次回改訂の際などに参考にさせていただきます。なお、個別のご質問・ご要望等にはお応えいたしかねる場合もございますので、予めご了承ください。

IPA 技術本部セキュリティセンター　暗号グループ：　isec-crypt-inq@ipa.go.jp