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-AcrobatDC/Acrobat2017 での設定方法 ★

目次

〔編集責任〕
独立行政法人 情報処理推進機構

なお、本実践編は、アドビシステムズ株式会社の協力の下、作成されております。

〔発 行〕
２０１８年 7月３１日

〔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。

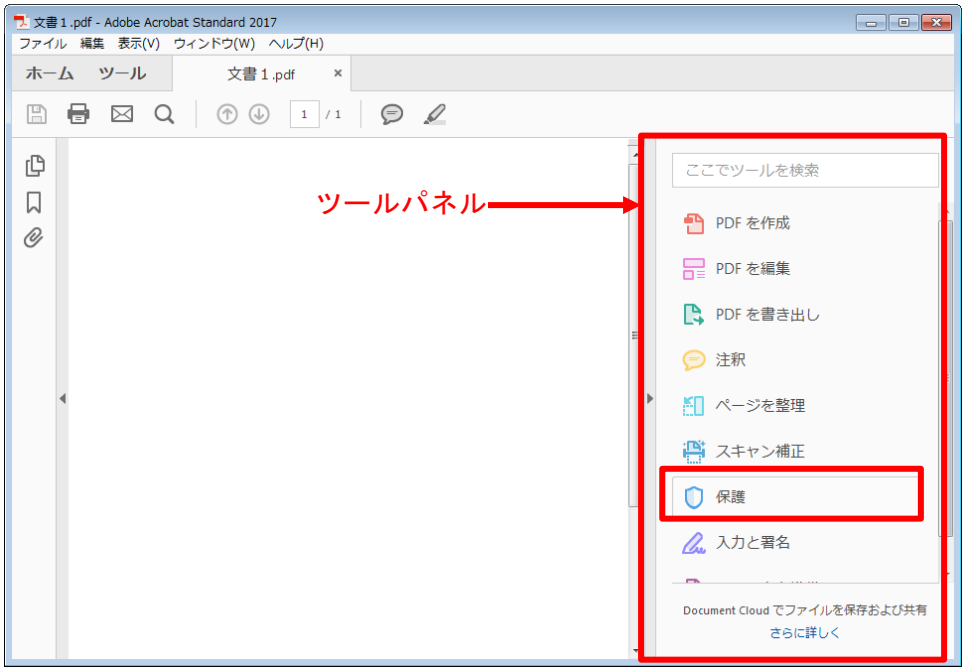
IPA　セキュリティセンター：　　isec-info@ipa.go.jp

実践編－AcrobatDC/Acrobat2017 での設定方法

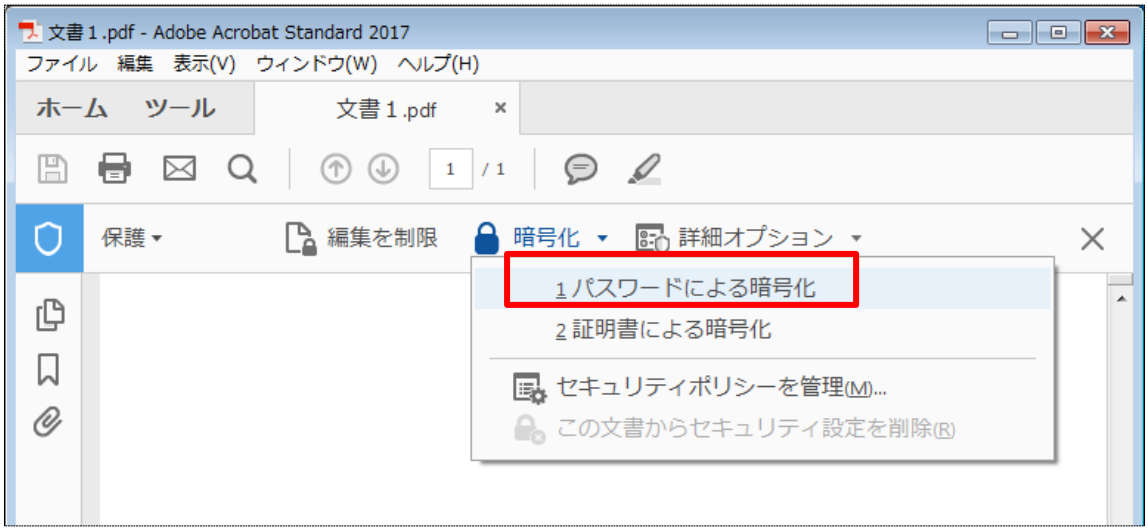
B.1　ファイルへの暗号化設定の有効化（保存方法）

- ファイルへの暗号化設定のパスワードによる有効化（保存方法）

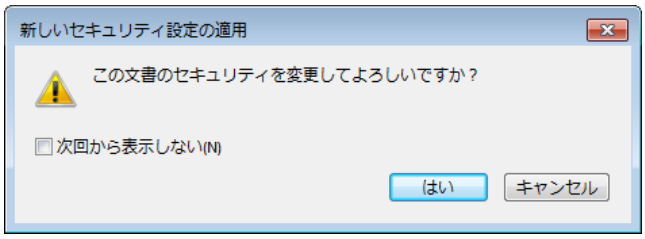
1.〔ツールパネル〕の〔保護〕をクリックする。



2.〔保護〕ツールバーの〔暗号化〕から〔パスワードによる暗号化〕を選択する。

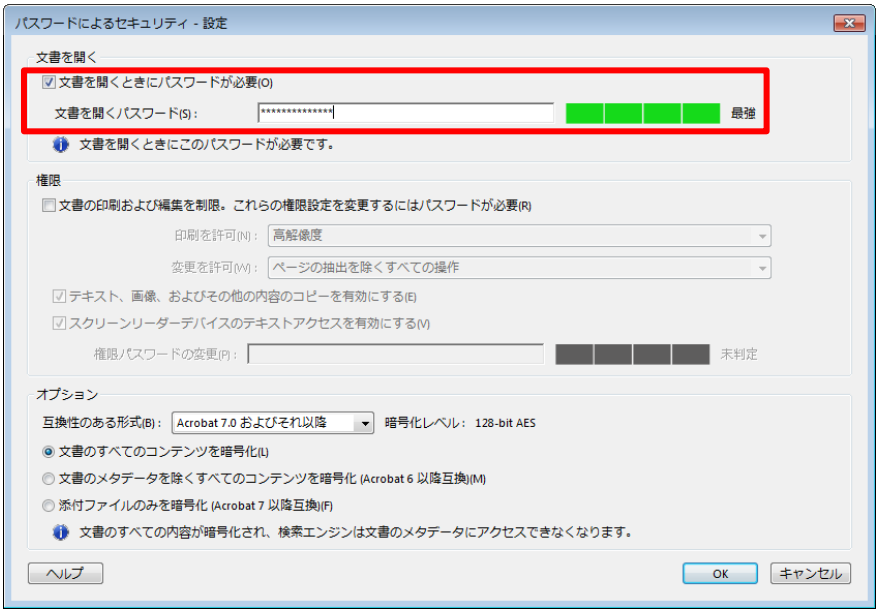


3. 〔はい〕をクリックする。



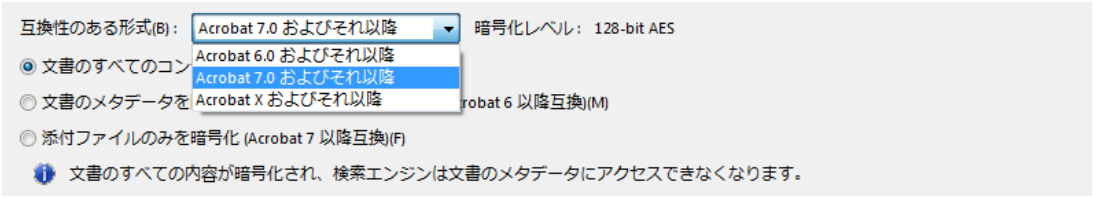
4. 〔文書を開くときにパスワードが必要〕のチェックボックスをオンにし、パスワードを入力して〔OK〕をクリックする。

【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



【暗号化レベル】

「互換性のある形式」を変更することにより暗号化レベルが変わります。

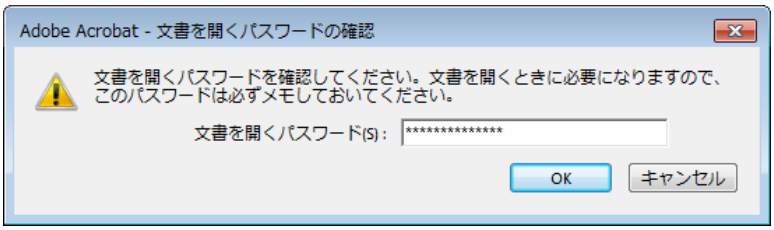


電子政府推奨暗号リストに記載されている暗号化レベルを選択してください。選択した暗号化レベルで使用されるすべての暗号技術が電子政府推奨暗号リストに記載されている必要があります。Acrobat の暗号化レベルと電子政府推奨暗号との対応を下表に示します。

互換性のある形式	暗号化レベル	電子政府推奨暗号
Acrobat 6.0 およびそれ以降	128-bit RC4	×
Acrobat 7.0 およびそれ以降	128-bit AES	×[1]
Acrobat X およびそれ以降	256-bit AES	○

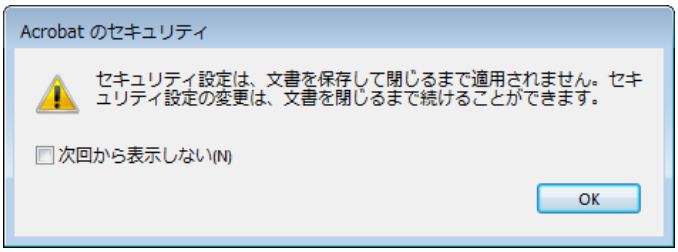
電子政府推奨暗号を使用する場合には〔Acrobat X およびそれ以降〕を選択します。

5. パスワードを再度入力し、〔OK〕をクリックする。



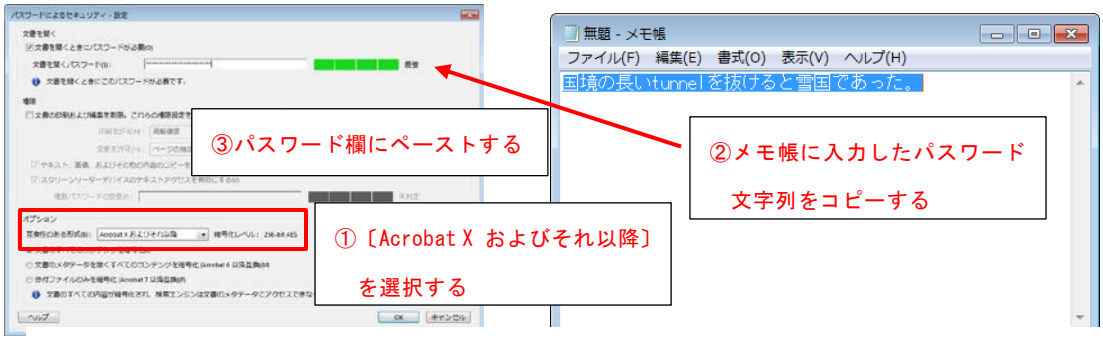
※ 文書を保存するまで、暗号化は有効にならないことに注意

[1] 128-bit AES 自体は電子政府推奨暗号リストに記載されている。しかしながら、「Acrobat 7.0 およびそれ以降」の設定では、パスワードから暗号鍵を導出する際に電子政府推奨暗号リストに記載されていないアルゴリズムが使われるため、ここでは×としている。



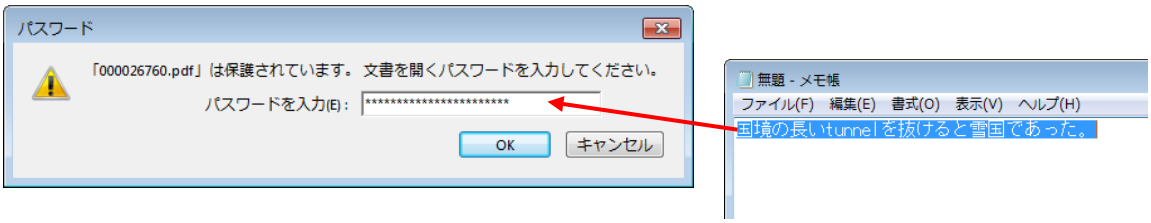
【日本語のパスワード】

暗号化レベルを〔Acrobat X およびそれ以降〕にすると、日本語（ユニコード文字）のパスワードが使用できるようになります。日本語を使うとパスワードに使用できる文字種が大幅に増え、パスワードが破られにくくなります。ただし、パスワード欄に直接日本語を入力することができません。いったんメモ帳などに入力してから、コピー&ペーストします。



先に、互換性のある形式を〔Acrobat X およびそれ以降〕にしておかないとパスワード欄にペーストできません

文書を開くときも同様です。パスワードを要求されたら、いったんメモ帳などに入力してからコピー&ペーストしてください。



【FIPS モード】

Adobe Acrobat には、PDF の暗号化方法を米国連邦情報処理規格（FIPS）に準拠したものに制限する FIPS モードが用意されています。 FIPS モードでは、RSA BSAFE Crypto-C Micro Edition (ME) 3.0.0.1 暗号モジュールによる FIPS 140-2 承認アルゴリズムが使用されます。

次のセキュリティオプションは Adobe Acrobat の FIPS モードでは使用できません。

・　パスワードによる暗号化で文書を保護することはできません。

- Self-Sign デジタル ID （自己作成の電子証明書）を作成したときに、ファイルに保存することができません。Windows証明書ストアには保存できます。
- RC4 暗号化アルゴリズムが使用できません。FIPS モードで PDF ファイルを暗号化するには、AES 暗号化アルゴリズムしか使用できません。
- MD5 または RIPEMD160 ダイジェスト方式は使用できません。
- FIPS モードでは、FIPS に準拠しないアルゴリズムを使用して保護された文書を開き、表示することができます。ただし、変更して保存することはできません。

したがって、FIPS モードで使用する場合には、パスワードによる暗号化が使用できません。「B.2 ファイルへの暗号化設定の電子証明書による有効化（保存方法)」を参照して、証明書による暗号化を使用してください。

Adobe Acrobat を FIPS モードで起動するには、Windows レジストリで以下の設定を行っておきます。

- Adobe Acrobat DC（Continuous）の場合

  [HKEY_CURRENT_USER¥Software¥Adobe¥Adobe Acrobat¥DC¥AVGeneral]

  "bFIPSMode"=dword:00000001

- Adobe Acrobat DC（Classic）の場合

  [HKEY_CURRENT_USER¥Software¥Adobe¥Adobe Acrobat¥2015¥AVGeneral]

  "bFIPSMode"=dword:00000001

- Adobe Acrobat 2017の場合

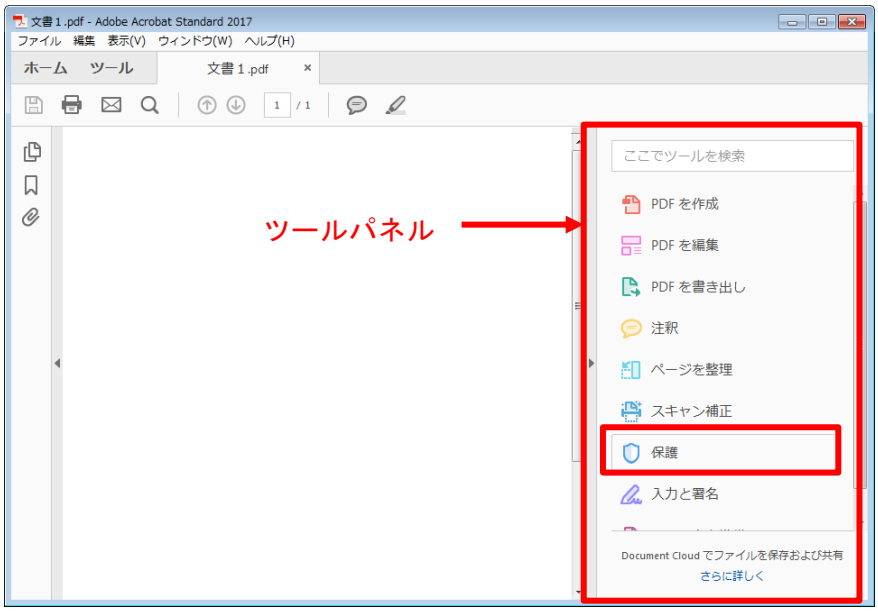
  [HKEY_CURRENT_USER¥Software¥Adobe¥Adobe Acrobat¥2017¥AVGeneral]

  "bFIPSMode"=dword:00000001

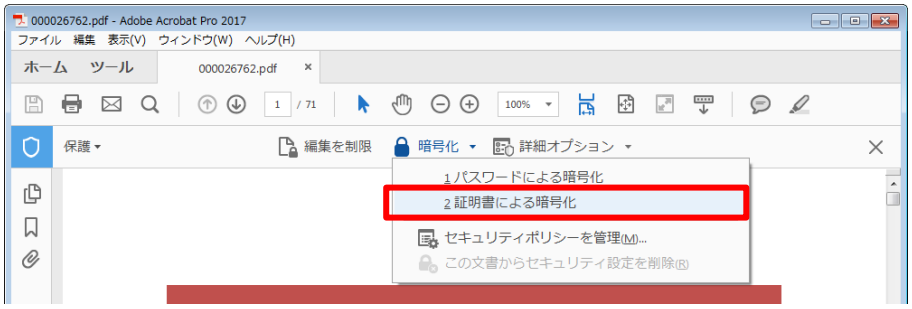
[参考]ファイルへの暗号化設定の電子証明書による有効化（保存方法）

PDF の暗号化には、電子証明書を使用して、文書の閲覧が可能な受信者を指定する方法もあります。公開鍵暗号を使用するもので、暗号化の際に受信者の公開鍵証明書を指定します。あらかじめ受信者の公開鍵証明書を用意しておきます。また、自分が開けるようにするため、自身の電子証明書も用意しておきます。

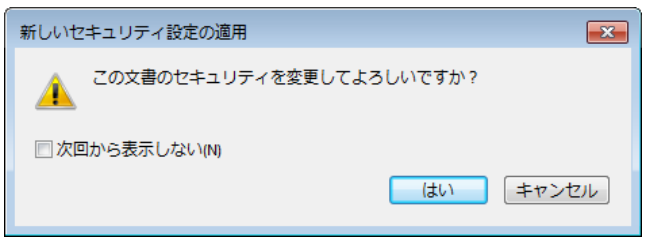
1. 〔ツールパネル〕の〔保護〕をクリックする。



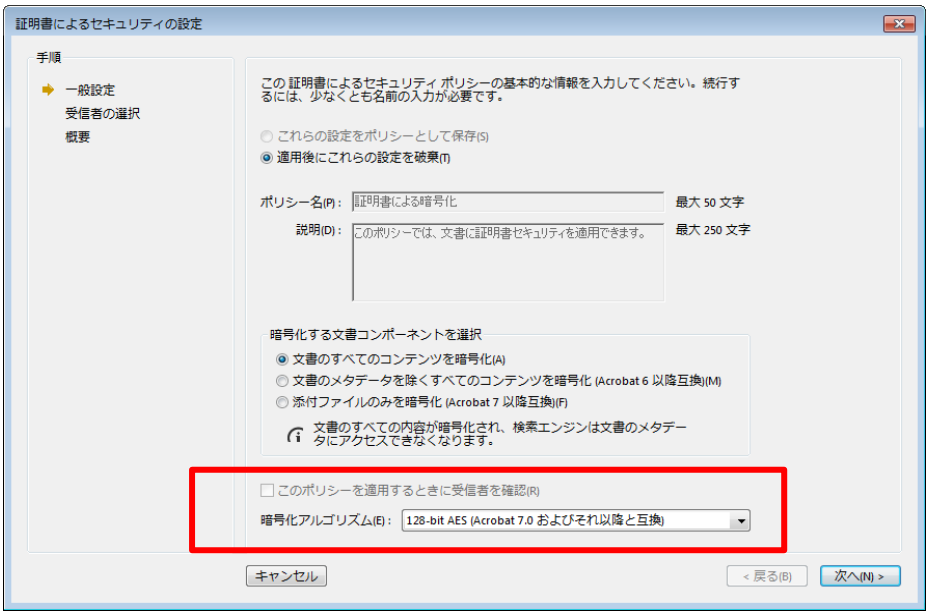
2. 〔保護〕ツールバーの〔暗号化〕から〔証明書による暗号化〕を選択する。



3. 〔はい〕をクリックする。

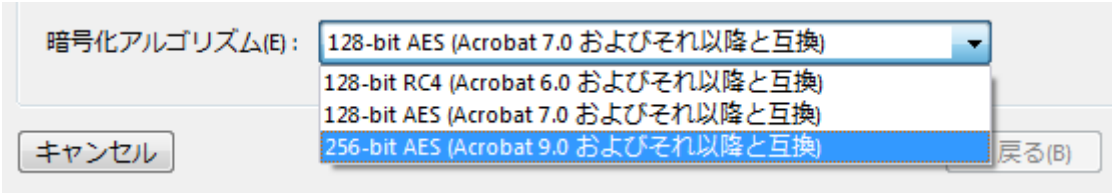


4. 暗号化アルゴリズムを確認して〔次へ〕をクリックする。



【暗号化レベル】

「暗号化アルゴリズム」を変更することにより暗号化レベルが変わります。



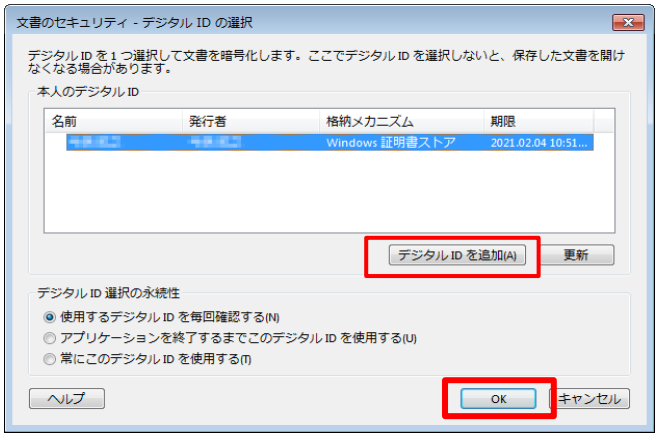
電子政府推奨暗号リストに記載されている暗号化レベルを選択してください。選択した暗号化アルゴリズムで使用されるすべての暗号技術が電子政府推奨暗号リストに記載されている必要があります。Acrobat の暗号化アルゴリズムと電子政府推奨暗号との対応を下表に示します。

暗号化アルゴリズム	電子政府推奨暗号
128-bit RC4（Acrobat 6.0 およびそれ以降と互換）	×
128-bit AES（Acrobat 7.0 およびそれ以降と互換）	×[2]
256-bit AES（Acrobat 9.0 およびそれ以降と互換）	○

電子政府推奨暗号を使用する場合には〔256-bit AES（Acrobat 9.0 およびそれ以降と互換)〕を選択します。

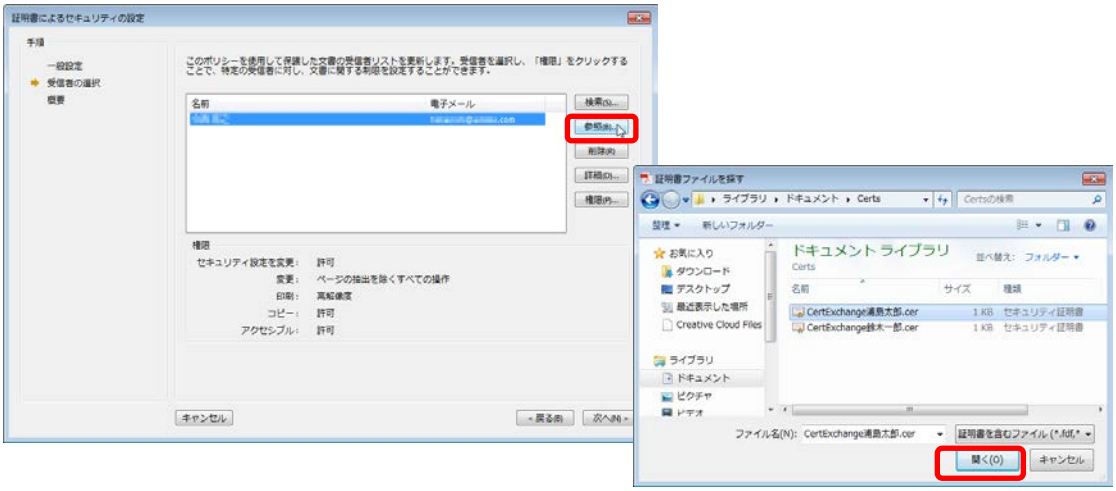
[2] 128-bit AES 自体は電子政府推奨暗号リストに記載されている。しかしながら、「Acrobat 7.0 およびそれ以降」の設定では、パスワードから暗号鍵を導出する際に電子政府推奨暗号リストに記載されていないアルゴリズムが使われるため、ここでは×としている。

5. 自分のデジタルID（＝電子証明書）を選択し、〔OK〕をクリックする。

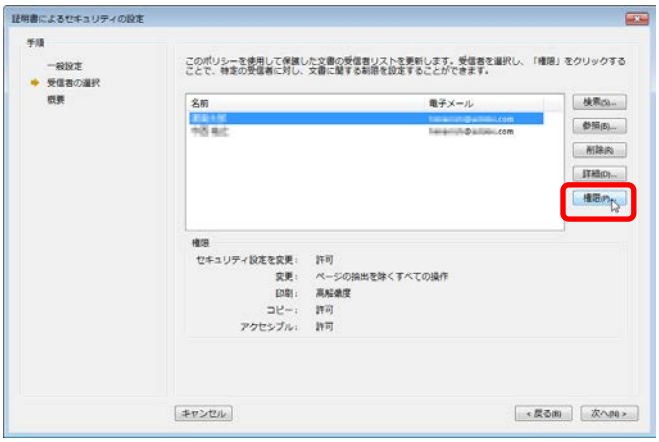


本人のデジタル ID が表示されない場合は、〔デジタル ID を追加〕をクリックして自分の電子証明書を追加する。

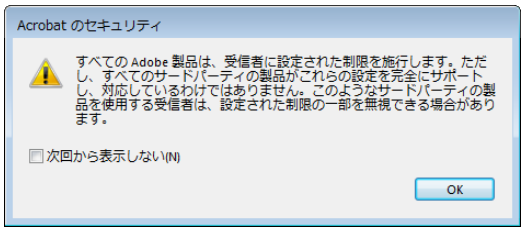
6. 〔参照〕をクリックして受信者の公開鍵証明書を選択し、受信者を追加する



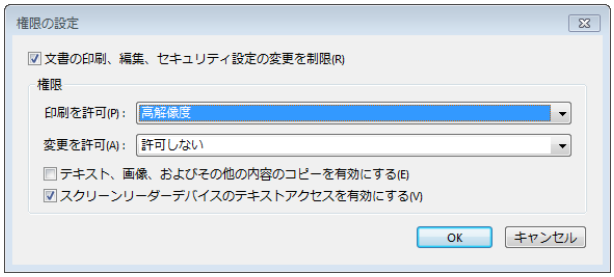
7. 受信者の利用権限を設定する。受信者を選択して〔権限〕をクリックする。



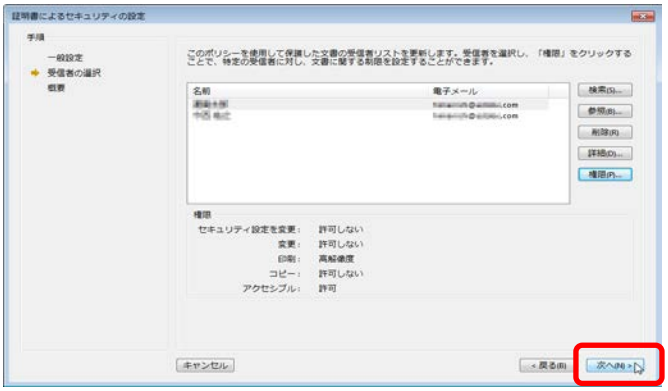
次の注意が表示されたら〔OK〕をクリックする。



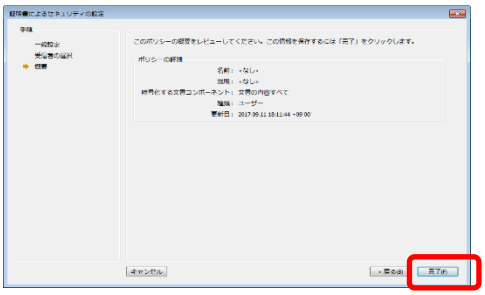
8. 〔権限の設定〕ダイアログボックスで、印刷や内容の編集・コピーの権限設定を行う。



9. 受信者全員を追加したら〔次へ〕をクリックする。



10. 〔完了〕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