－法人認証カード＆電子認証キット－

電子署名による文書管理

電子認証キット製造・販売
法人認証カードサービス　技術提供

法律とコンピューター
株式会社リーガル®

法人認証カードサービス 提供

日本電子認証株式会社

Copyright(C)2009N.D.Ninsho Co.,Ltd.All Rights Reserved

目　　次

電子文書の改ざん防止に効果的な「電子署名」----------1
電子署名とパスワードによる保護との違い

電子署名の仕組み----------2
電子署名は秘密鍵の確実な管理が前提

法人認証カードサービスのご紹介----------3
実際に電子署名を行う場合の注意点

電子署名が活用可能な文書の例示----------4
長期間の改ざん防止が必要な場合の手順
改ざん防止と情報漏洩防止の両立も可能

電子署名を付した文書を暗号化した場合のご注意----------5

操作手順の説明

1. 電子署名----------7

2. 電子署名の内容確認----------10

3. 電子署名を付した文書を元に戻す----------13

4. 長期保存のため複数の電子署名を付す----------14

5. 電子署名を付した文書をさらに暗号化----------16

6. 暗号化した文書の復号(暗号化した状態から戻すこと)-------19

電子文書の改ざん防止に効果的な「電子署名」

電子文書を「情報資産」として活用する前提として、正当な権利を持たない人に変更されていないこと－改ざん防止を確実にしておくことが不可欠です。(「完全性」の確保と呼ばれています)

電子申請や電子入札で広く一般的に利用されている「電子署名」は、“簡単・確実・低コスト”な情報セキュリティ対策として、貴社の文書管理にも役立つ技術と思われます。

電子署名の場合

★電子署名は、改ざん防止技術の定番

★書面は押印、電子文書は電子署名で正式文書へ

★ICカード型の電子証明書を利用すると、”はんこ”と同様に目に見える管理が可能

★ネットワーク環境全体にセキュリティ対策を講じる場合と比較して、低コストで改ざん検知が可能

★電子署名に利用する電子証明書は、電子申請や電子入札にも利用可能、業務効率の向上にも貢献

通常の場合

★パスワードによる保護は、パスワードを共有する関係者間では保護がない状態に近い

★ネットワーク環境全体にセキュリティ対策を講じる場合、コスト増大とログ監視業務の負担が発生

電子署名とパスワードによる保護との違い

電子署名を付した場合、下表のように「アイコン表示」、「保存状態」、「保存時に必要なもの」が異なりますので、不注意によるミスなどによって偶然に内容が改ざんされるリスクが軽減されます。

これに対してパスワードで保護するだけの場合は、原本として保存しておきたい電子文書であっても、編集中の電子文書と見かけ上は大差がないことから、簡易なセキュリティ対策としての効果しか望めません。

区分	アイコン表示	保存状態	保存時に必要なもの
電子署名の場合	PKCS#7のアイコン (パソコンによって表示が異なる場合もあります)	(暗号化されたイメージ)	法人認証カード 電子認証キット
	特有のアイコンなので区別が容易 不注意などによる改ざんリスク軽減	**閲覧に専用ソフトが必要 暗号化で情報漏洩も確実に防止**	**印鑑と同様の物理的な管理で、 簡単・確実・低コストに改ざん防止**
パスワードの場合			パスワード
	編集中の場合も見かけに大差がなく、不注意による改ざん・誤消去あり	自由に閲覧できる場合は、改ざんと情報漏洩のリスク	パスワードが漏えいした場合は、気づかないうちに無防備な状態

電子署名の仕組み（電子認証局会議事務局作成「電子署名活用ガイド」参照）

【電子署名】

書面における印鑑の押印に相当するものとして、電子文書では「電子署名」があります。

電子署名では、まず電子文書からハッシュ値を算出し、公開鍵暗号方式における「秘密鍵」でハッシュ値を暗号化します。

この暗号化されたハッシュ値が押印に相当し、電子証明書は印鑑証明書の役割を担います。

【復号】

暗号化された符号を元に戻すことを復号といいます。

「秘密鍵」で暗号化された場合は、「公開鍵」でのみ復号が可能になります。

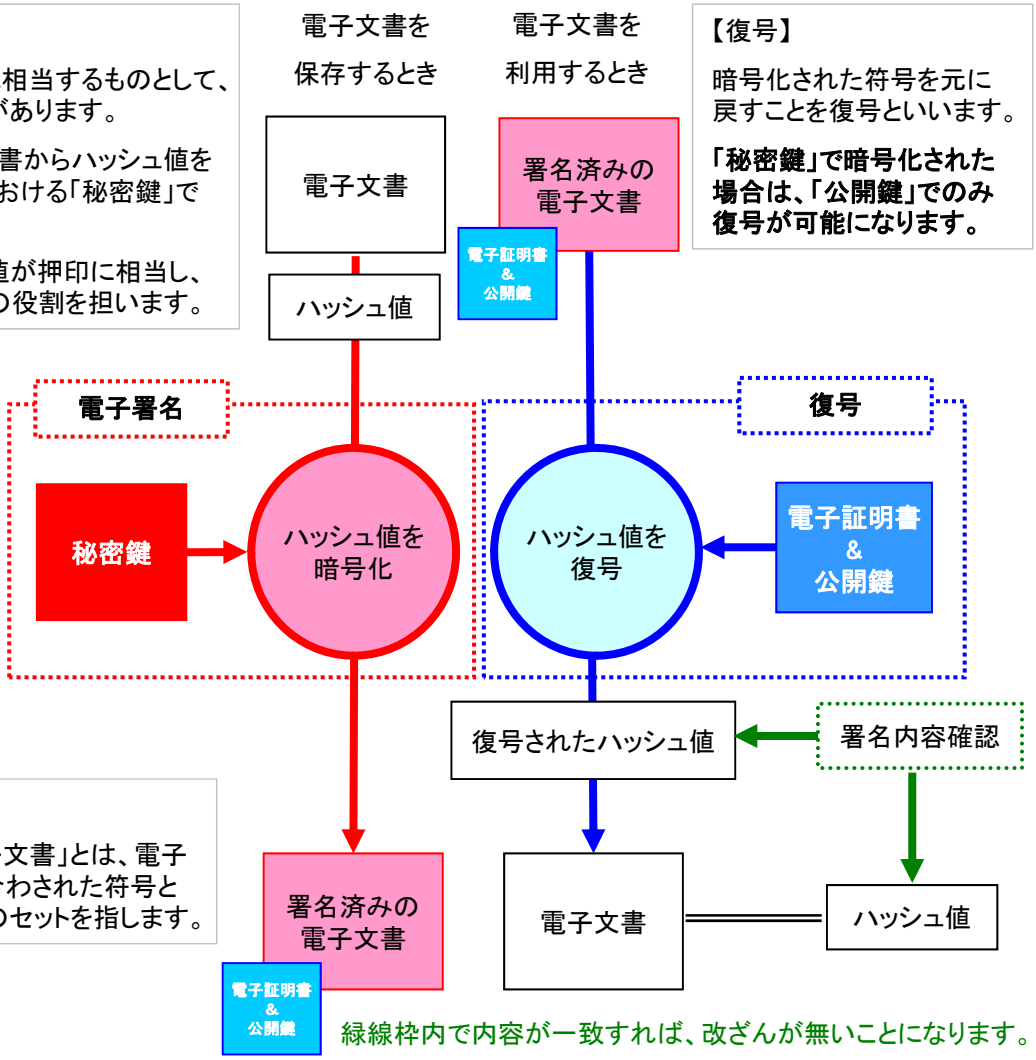
【秘密鍵】

「公開鍵」と対の関係にある符合のことです。

外部流出や不正使用の防止が不可欠です。

【署名済みの電子文書】

ここでいう「署名済みの電子文書」とは、電子署名と電子証明書が組み合わされた符号と電子文書（平文=ヒラブン）のセットを指します。



緑線枠内で内容が一致すれば、改ざんが無いことになります。

電子署名は秘密鍵の確実な管理が前提

電子署名は「秘密鍵」に外部流出や不正使用のリスクが生じないことが前提となっていますので、「秘密鍵」は文字通りの機密情報として確実な管理が求められます。

その点、ICカード型の電子証明書は、以下のような特長があることから「目に見える確実な管理」が可能です。

【ICカード型電子証明書の特長】

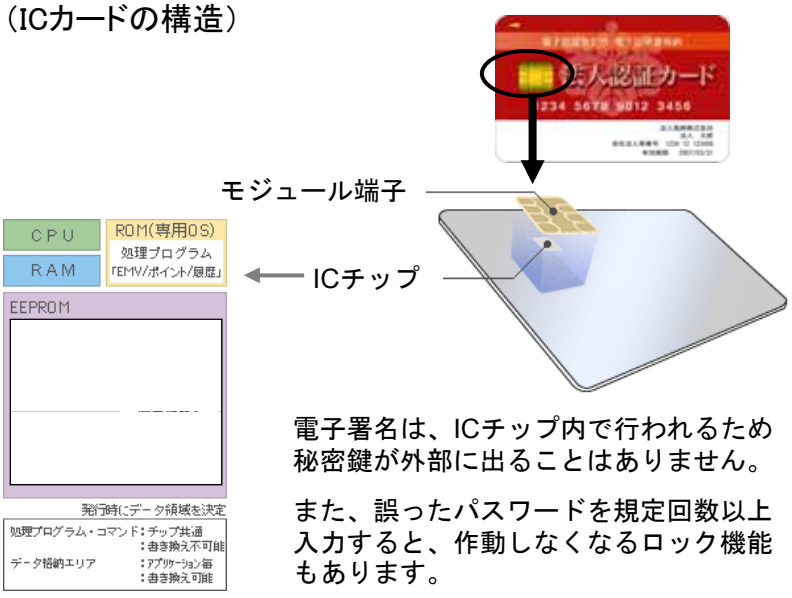
1.コピーが不可能

2.秘密鍵が外部に出ない構造

3.不正アクセスに対するロック機能

4.物理的な目に見える管理が可能

（ICカードの構造）



電子署名は、ICチップ内で行われるため秘密鍵が外部に出ることはありません。

また、誤ったパスワードを規定回数以上入力すると、作動しなくなるロック機能もあります。

法人認証カードサービスのご紹介

法人認証カードサービスは、法人認証カード、電子ICカードスタートキット、電子認証キットの3点で構成されています。

これらは、管理業務の業務効率向上に役立つ電子申請に広く利用できるほか、電子署名などによる文書管理にも活用することができます。

【法人認証カード】

法務省が発行する「商業登記に基づく電子証明書」をICカードに格納したセキュリティサービス

ICカード型としては、電子申請に最も幅広く利用可能

【ICカードスタートキット】

法人認証カード専用のICカードリーダ

ICカードリーダのドライバーとICカードの制御ソフトであるICカードマネージャがセットになっている

【電子認証キット】

商業登記に基づく電子証明書の取得などの機能

電子文書への電子署名などの便利なオプション機能も充実

「商業登記に基づく電子証明書」取得用ソフトウェアのベストセラー

実際に電子署名を行う場合の注意点

実際に電子署名を行う場合は、以下の点にご注意ください。

注意点	説　明
電子証明書（秘密鍵）は慎重に管理する	電子証明書（秘密鍵）は、企業印と同様に「いつ・誰が・どのような目的に利用したか」について慎重に管理する
電子証明書の有効期限を確認する （有効期限切れ、無効の状態では電子署名ができませんのでご注意ください）	電子証明書の残存有効期間が電子文書を保存したい期間をカバーできるか確認する １枚の電子証明書ではカバーできない長期間の保存が必要な場合は、有効期間の到来時期に新たな電子証明書による電子署名の追加を行う
電子署名を行うパソコンを特定しておく	電子署名や電子申請などに利用するパソコンを特定しておくと、会社が認めていない用途への乱用防止に効果的
電子署名するファイル名は、元のファイルと同名にする	電子署名された電子文書を元の状態に戻すとき、ファイル名を的確につけることができる
元の状態の拡張子をファイル名の途中に含める **（末尾は、必ず「.p7s」にする）**	電子署名された電子文書を元の状態に戻すとき、元のファイルの拡張子を的確につけることができる
パスワード保護付きのZIPファイルに圧縮する（任意）	電子認証キットがあっても閲覧できなくなる 情報漏洩対策として、暗号化機能もあり（４ページ参照）

電子署名が活用可能な文書の例示

電子署名は、どのような形式の電子文書にも付すことが可能です。ただし、商取引に伴う各種文書（契約書など）は、原則として書面での保管が法令で義務づけられていますのでご注意ください。

○顧客名簿 ○会議資料 ○プレゼン資料 適している ○ 保存必要	編集加工の頻度が高い ○ＦＡＸなどの送付状 ○会議の開催案内 ○ＰＯＰ広告原稿 × 不向き 保存不要
○社内規程 ○統計資料 ○人事関係資料 ○社員名簿 ○棚卸記録 最　適 ◎ 編集加工の頻度が低い	× 不向き ○忘年会などの開催案内 ○臨時休業の案内

長期間の改ざん防止が必要な場合の手順

法務省が発行する「商業登記に基づく電子証明書」は、最長の有効期間が27ヶ月なので、それ以上の長期に渡って電子文書の改ざん防止が必要な場合は、複数の電子署名を付すことになります。(１４ページ参照)

最長27ヶ月 → 最長27ヶ月 → 最長27ヶ月

初代の電子証明書

二代目

三代目（以後 ∞）

有効期限が切れたり、代表者の交代などにより無効になった場合は、新しい電子証明書で電子署名を追加します。

追加できる電子署名の数に制限はありませんので、長期間の改ざん防止が可能です。

改ざん防止と情報漏洩防止の両立も可能

電子認証キットの「電子文書を暗号化」という機能を利用すると、暗号化に使用した法人認証カードがないと内容を見ることができなくなります。電子署名と併用することにより、改ざんと情報漏洩という電子文書の二大リスクを同時に排除することが可能です。（５ページ、１６ページ参照）

なお、電子署名と暗号化を両方行った場合、元の状態に戻すときは、まず暗号化した文書を復号（もとに戻すこと）した後、さらに電子署名を付した状態から元に戻すという2つの手順が必要です。

電子署名で改ざん防止

暗号化で情報漏洩防止

目に見える管理が可能な法人認証カードだからこそ、確実な情報漏洩の防止が期待できます。

カード管理で閲覧を制限

電子署名を付した文書を暗号化した場合のご注意

暗号化された電子文書は、暗号化に使用した法人認証カードがないかぎり復号（元に戻すこと）は不可能です。

「有効期限切れ」または「無効」となる場合は、必ず暗号化に使用した法人認証カードで復号を済ませてください。

なお、有効期限切れまたは無効となった後でも復号は可能です。

重　要

暗号化に使用した法人認証カードの処分は慎重に！

復号する前に法人認証カードを処分してしまうと、暗号化した電子文書を元に戻すことが不可能になりますので、充分にご注意ください。

【暗号化に使用した法人認証カードを廃棄する手順の例示】

「有効期限切れ」、代表者の交代等による「無効」となった法人認証カードは、以下の例の手順を踏んで慎重に処分してください。

ステップ　1	暗号化に使用した法人認証カードを使用して、すべての暗号化文書を復号（暗号化する前の状態に戻すこと)します
ステップ　2	電子署名を付した状態に戻ります
ステップ　3	新しい 法人認証カードで電子署名を追加します これにより、次の有効期限まで改ざん検知が可能になります
ステップ　4	情報漏洩対策として暗号化も追加して行う場合は、ステップ３で電子署名に使用した電子証明書で暗号化も行います
ステップ　5	念のため、ステップ1で復号が漏れている文書がないか慎重に再確認します
ステップ　6	ステップ５により、廃棄処分しても支障が生じないことを充分に確認した後、「有効期限切れ」や「無効」となった 法人認証カードを**※適宜処分**してください。

※不測の事態に備えて物理的に破壊・廃棄しない場合は、「使用不可」などと明記した封筒に入れ、封緘した上で金庫等に保存しておくなどの処分方法も考えられます。

操作手順の説明

1. 電子署名----------7

2. 電子署名の内容確認----------10

3. 電子署名を付した文書を元に戻す----------13

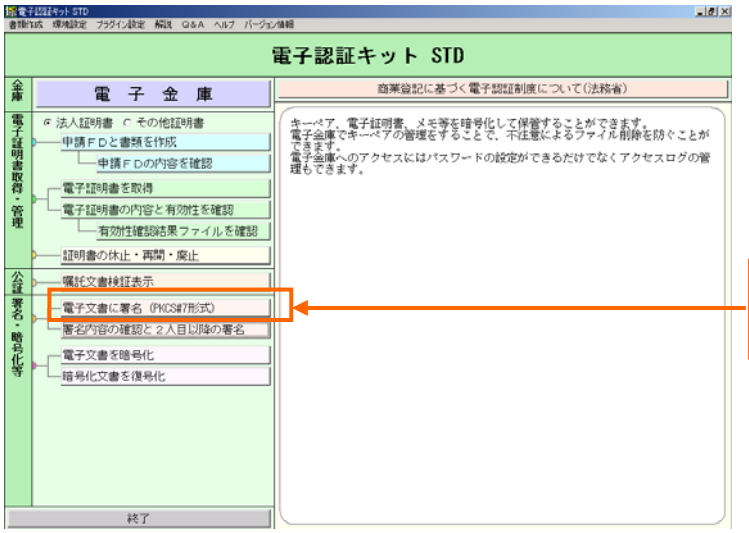
4. 長期保存のため複数の電子署名を付す----------14

5. 電子署名を付した文書をさらに暗号化----------16

6. 暗号化した文書の復号(暗号化した状態から戻すこと)-------19

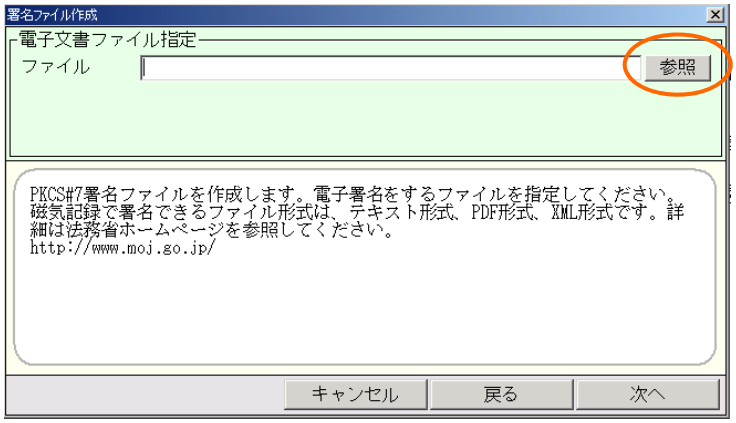
1.電子署名

電子認証キットの起動、パソコンにICカードリーダを接続、ICカードリーダに法人認証カードを挿入した状態で操作を始めてください。



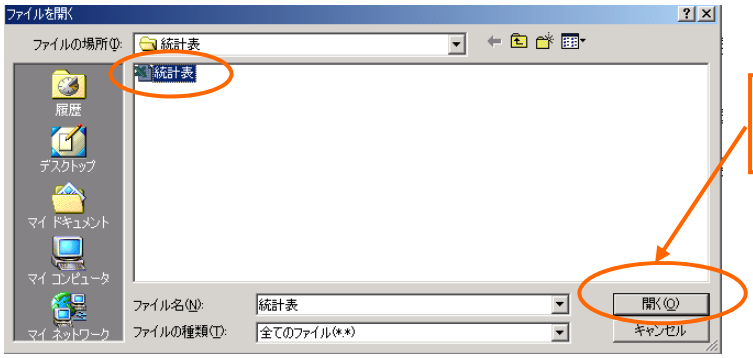
1

「電子文書に署名（PKCS#7)」をクリック



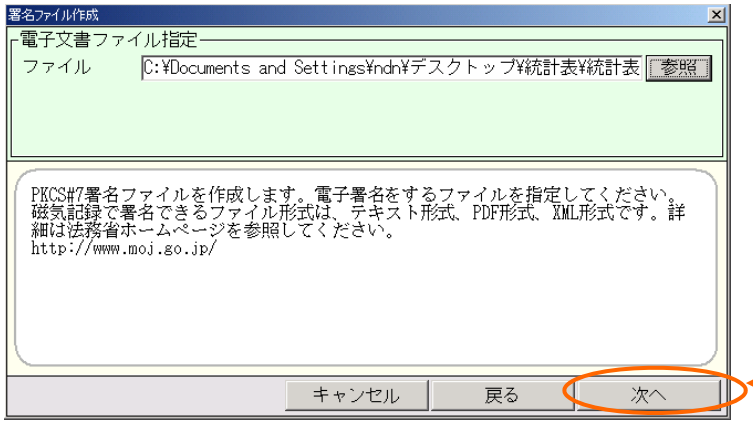
2

「参照」をクリック



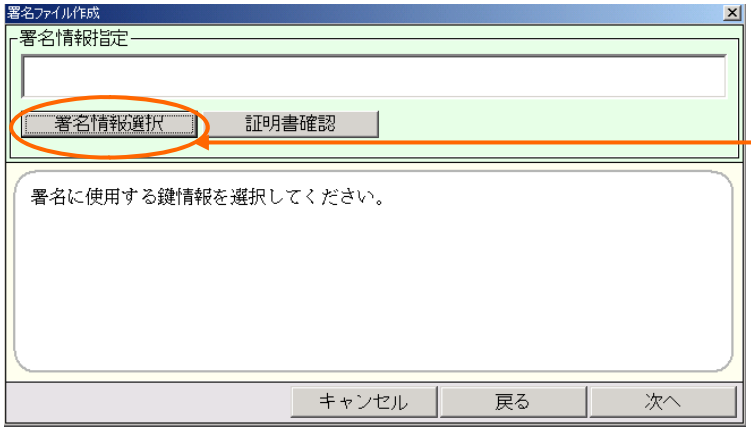
3

電子署名するファイルを選択して「開く」をクリック



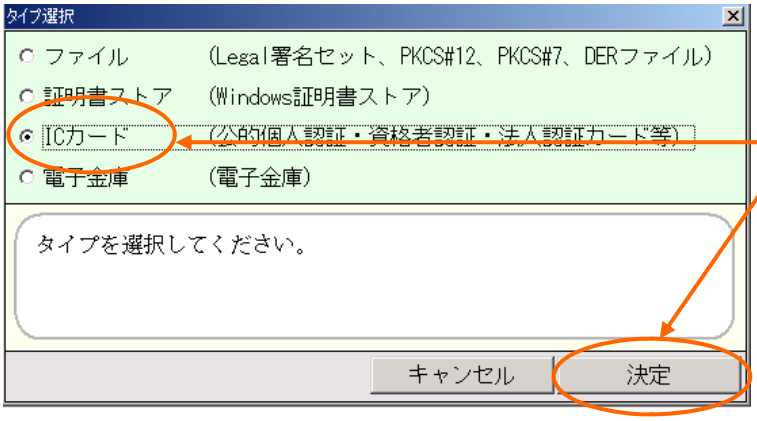
4

「次へ」をクリック



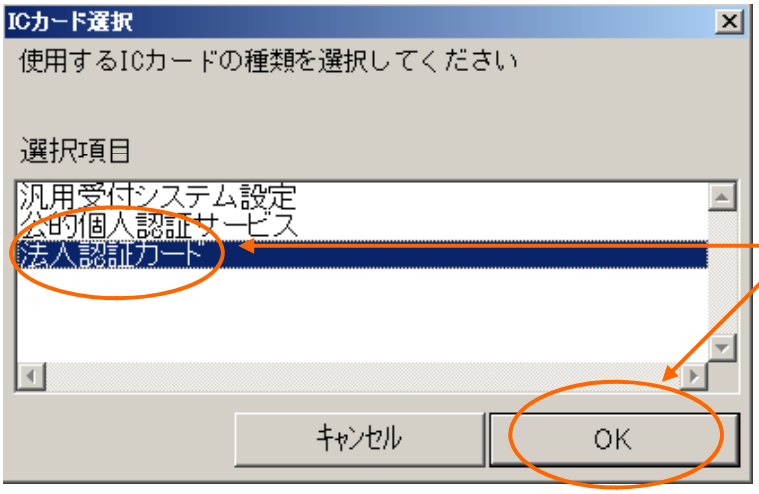
5

「署名情報選択」をクリック



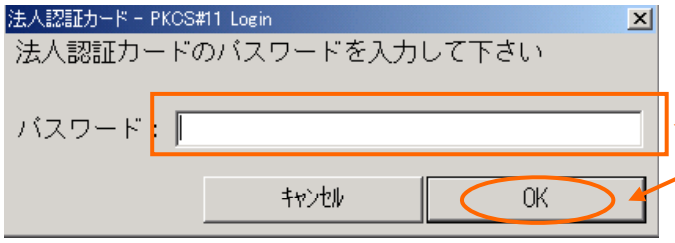
6

「ICカード」を選択して「決定」をクリック



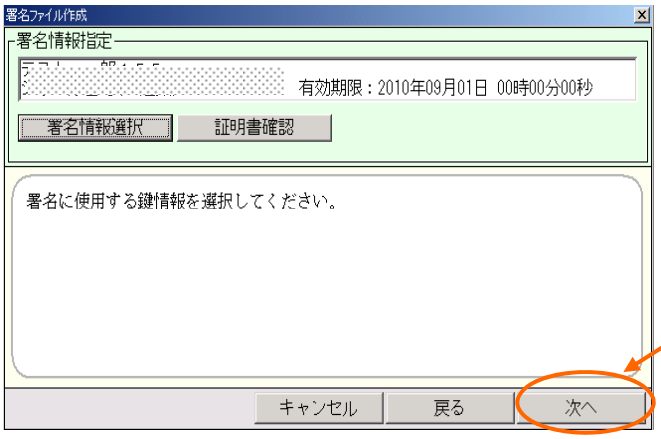
7

「l法人認証カード」を選択して「OK」をクリック



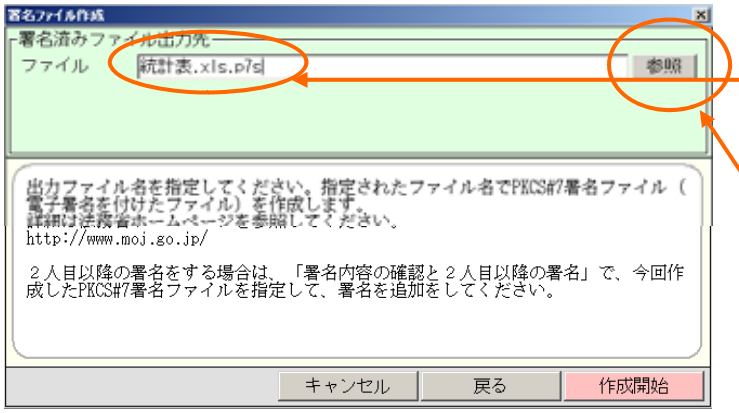
8

「パスワード」(PIN)を入力して「OK」をクリック



9

「次へ」をクリック



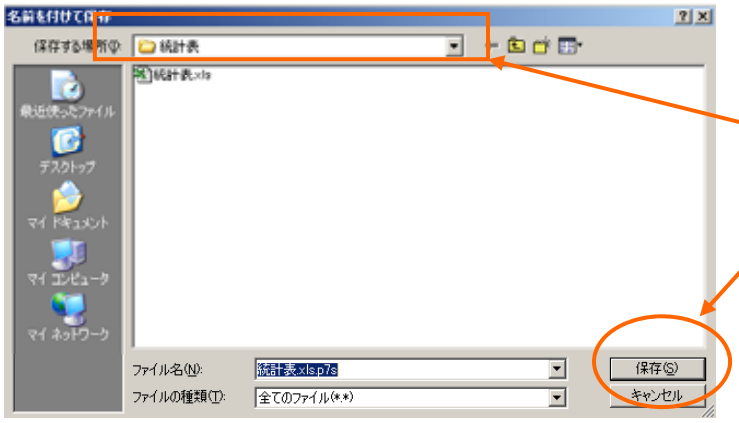
１０

ファイル名の後に拡張子「.p7s」を入力

元のファイルの拡張子（.xls等）をファイル名に含めると、元の状態に戻すときに便利です。

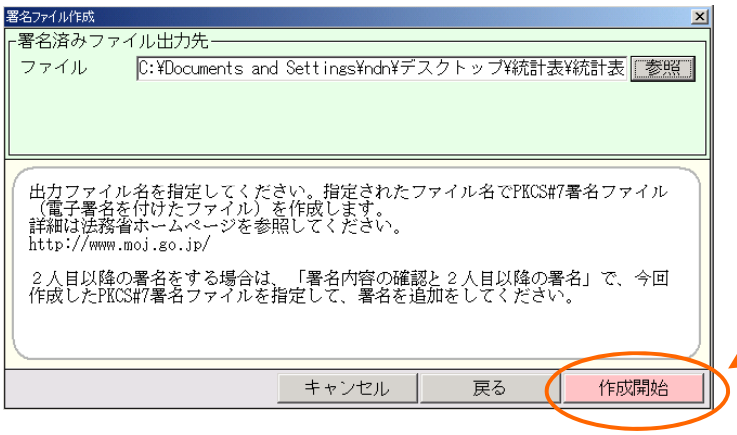
１１

「参照」をクリック



１２

保存するフォルダを選択して「保存」をクリック



１３

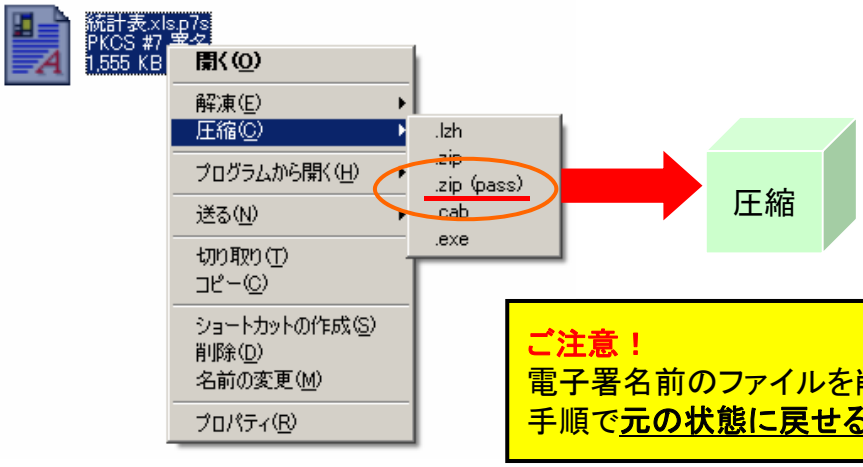
「作成開始」をクリック

１４

「OK」をクリックして完成

【ご参考　その1】

パスワードによる保護機能があるZIPで圧縮すると、安全性の向上とファイルサイズの圧縮が可能です。

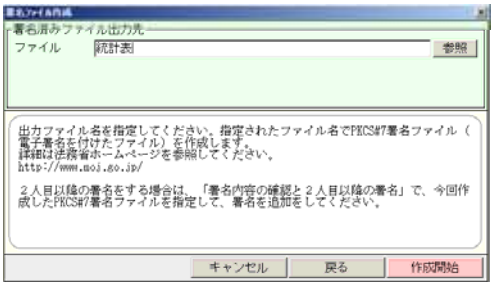


ご注意！
電子署名前のファイルを削除する場合は、13ページの手順で**元の状態に戻せることを必ず確認**してください。

【ご参考　その２】

ご説明した手順と異なる手順で電子署名を行った場合の現象と対処方法は次のとおりです。

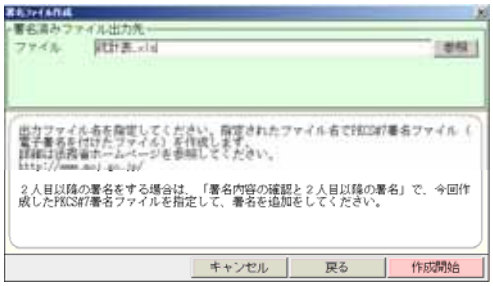
ファイル名の末尾に拡張子「.p7s」を入れなかった



対処方法

PKCS＃7形式で保存されないので、ファイル名の末尾に「.p7s」の拡張子を追加する

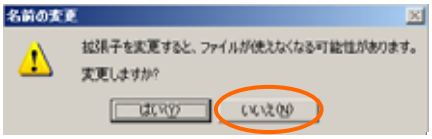
ファイル名に原本の拡張子(.xls)を入れたが、末尾に拡張子「.p7s」を入れなかった



対処方法

エクセル形式で保存されるがこのままでは開けないので、電子署名をもう一度やり直す

電子署名した後に拡張子を変更しようとした

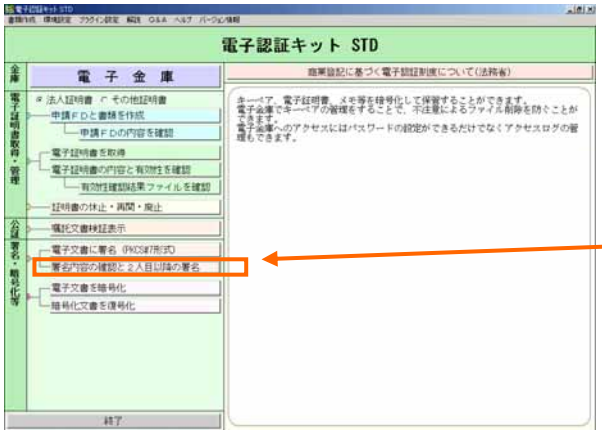


対処方法

「いいえ」をクリックする

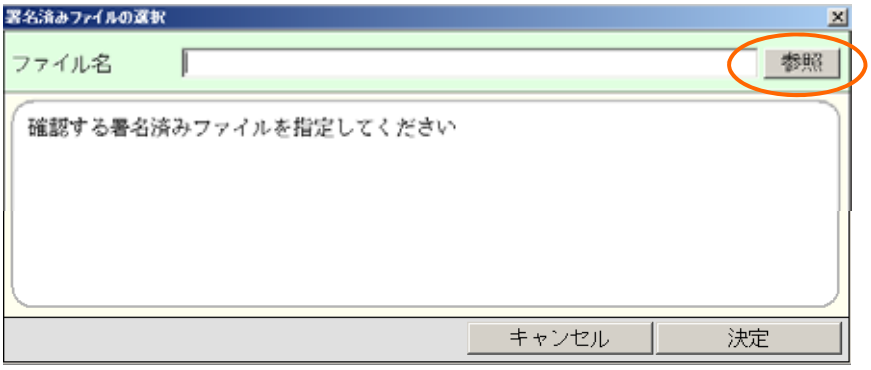
2.電子署名の内容確認

電子認証キットを起動させた状態で操作を進めてください。この操作では、ICカードリーダと法人認証カードは使用しません。



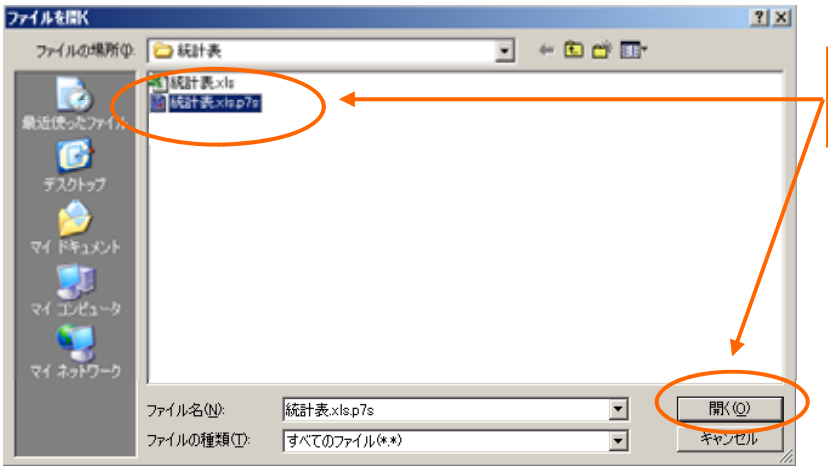
1

「署名内容の確認と２人目以降の署名」をクリック



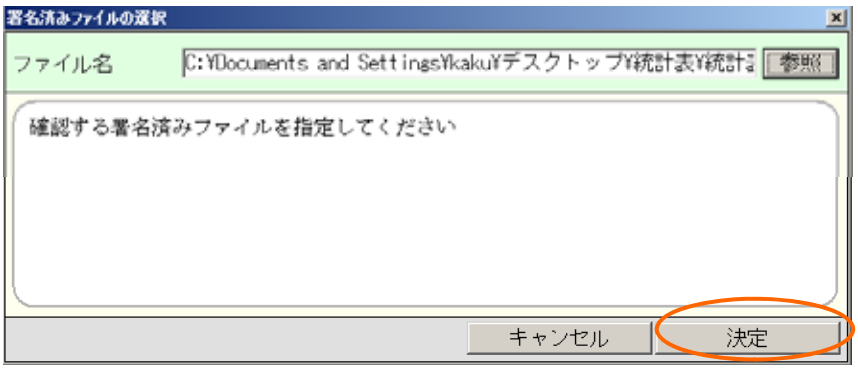
2

「参照」をクリック



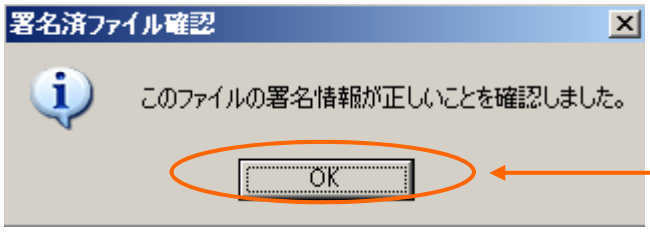
3

電子署名の内容を確認するファイルを選択して「開く」をクリック



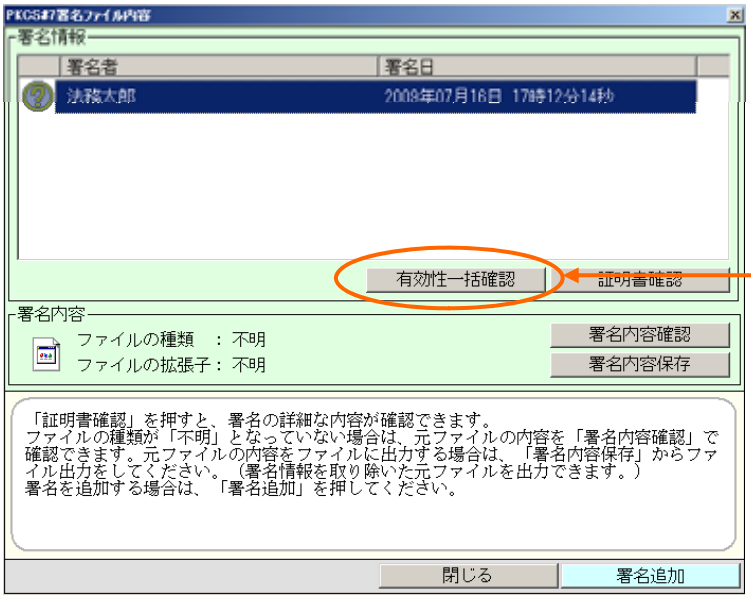
4

「決定」をクリック



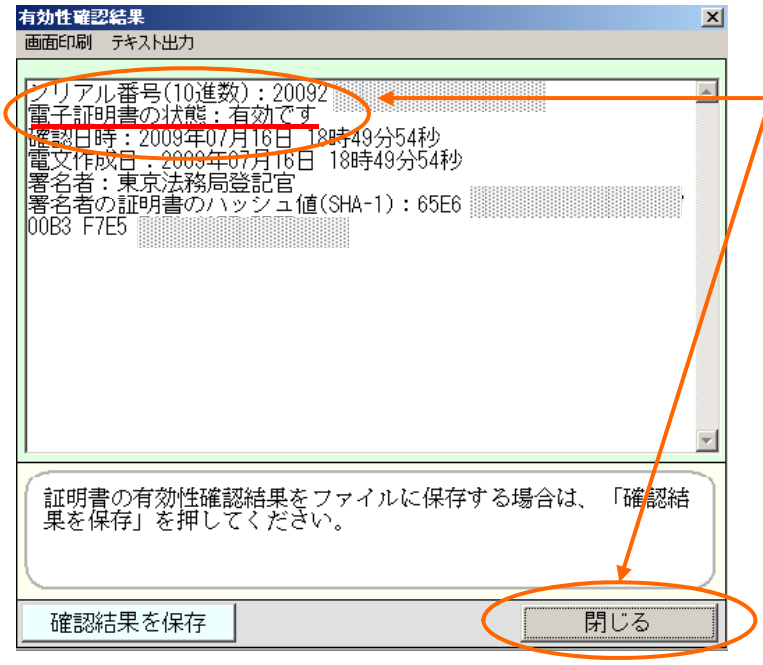
5

「OK」をクリック



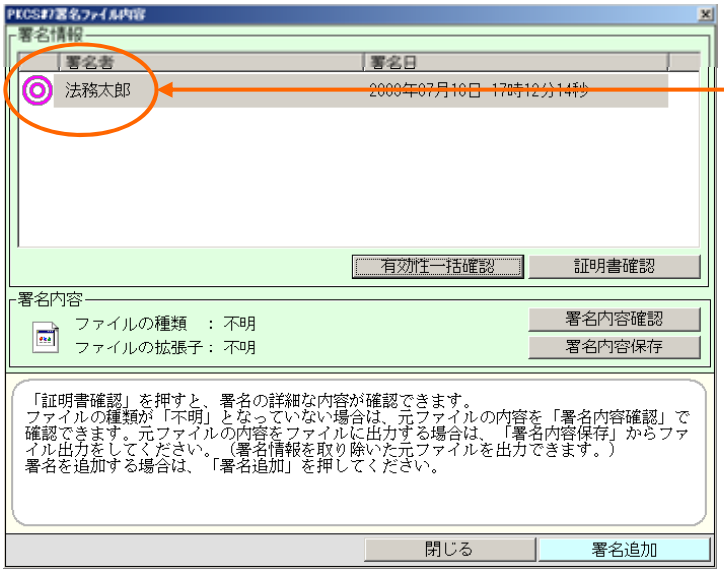
6

「有効性一括確認」をクリック



7

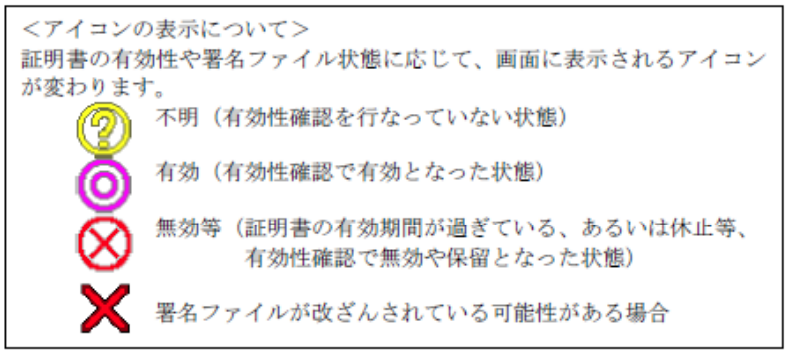
「電子証明書の状態」を確認して「閉じる」をクリック



8

電子署名された文書について有効性の確認結果が表示される。
「◎」が表示された場合は、改ざんがなく電子署名も有効な状態を表しています。
「×」が表示された場合は、改ざんされている可能性があることを示しています。

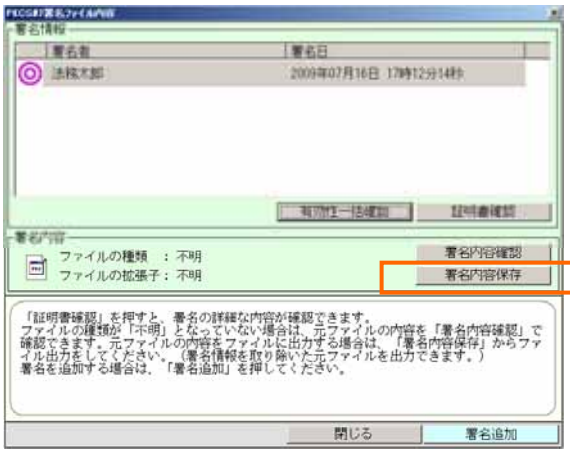
【電子認証キットにおける有効性の確認結果の凡例】



3.電子署名を付した文書を元に戻す

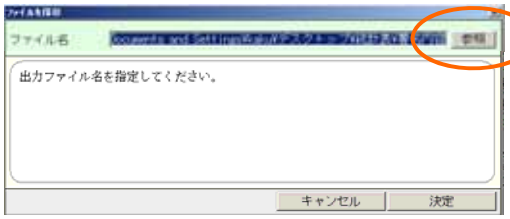
電子認証キットを起動させた状態で操作を進めてください。この操作では、ICカードリーダと法人認証カードは使用しません。

「2.電子署名内容の確認」から連続した操作になります。以下の説明は、１２ページからの続きです。



1

「署名内容保存」をクリック

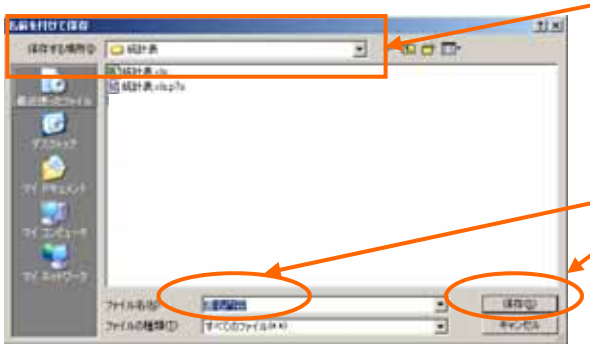


2

「参照」をクリック

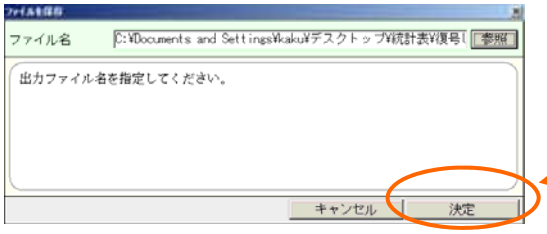
3

「保存する場所」を選択



4

ファイル名の初期表示は「署名内容」なので、「元のファイル名+元のファイルの拡張子」の内容でファイルを変更して「保存」をクリック

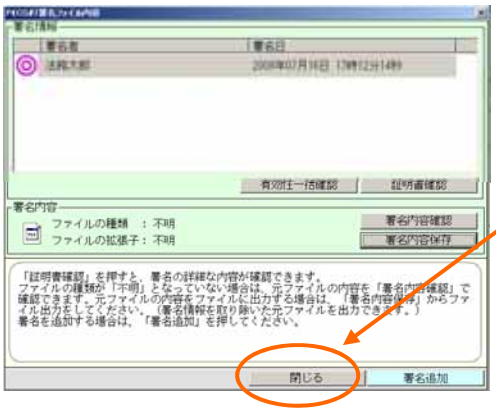


5

「決定」をクリック

6

「OK」をクリック

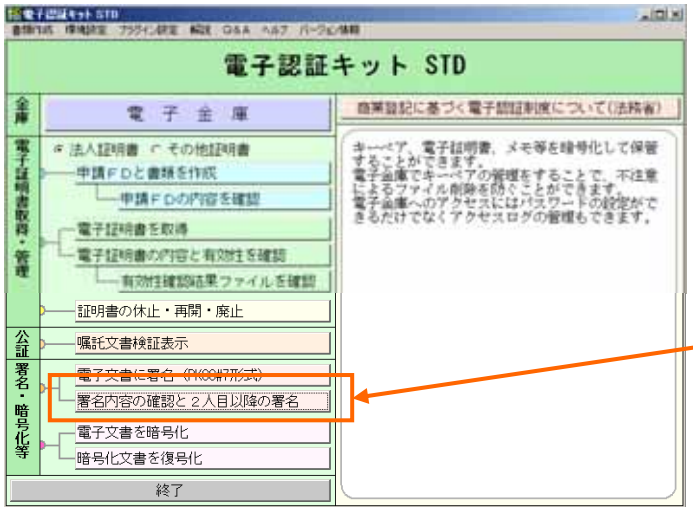


7

「閉じる」をクリック

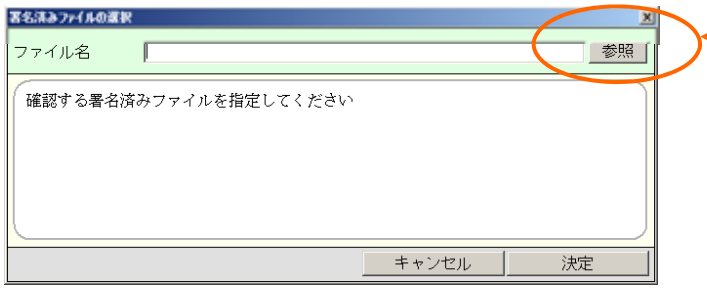
4.長期保存のため複数の電子署名を付す

電子認証キットの起動、パソコンにICカードリーダを接続、ICカードリーダに法人認証カードを挿入した状態で操作を始めてください。



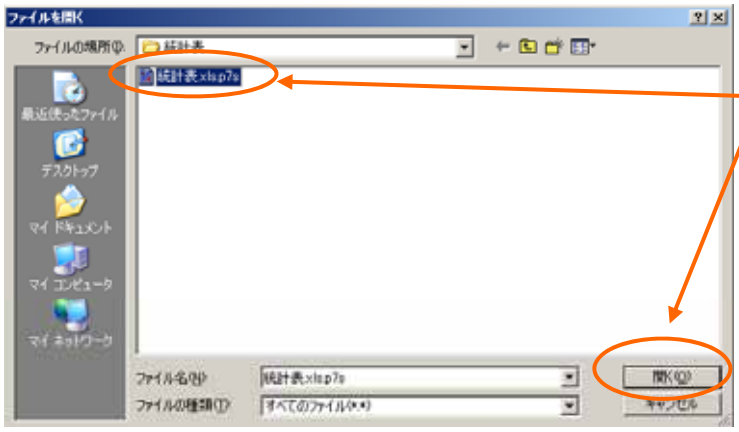
1

「署名内容の確認と２人目以降の署名」をクリック



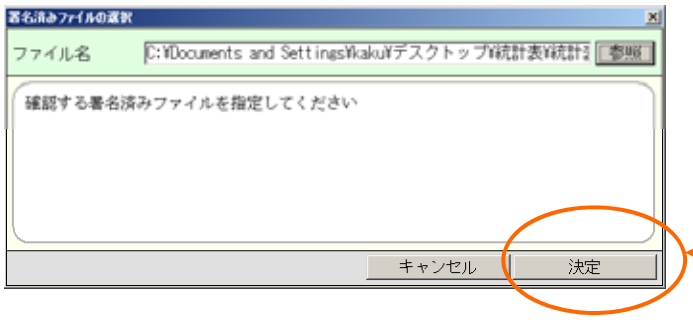
2

「参照」をクリック



3

署名を追加するファイルを選択して「開く」をクリック

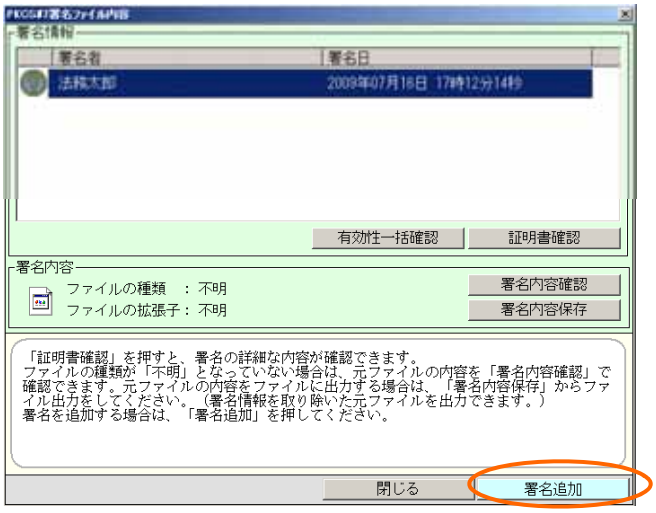


4

「決定」をクリック

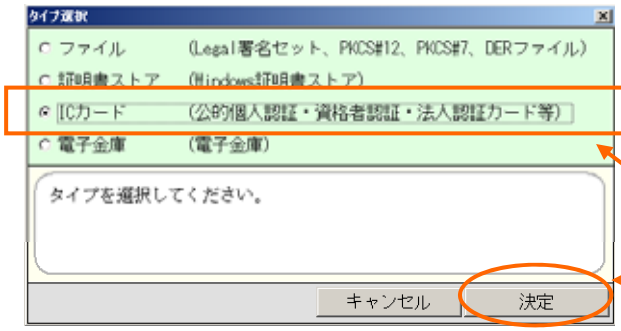
5

「OK」をクリック



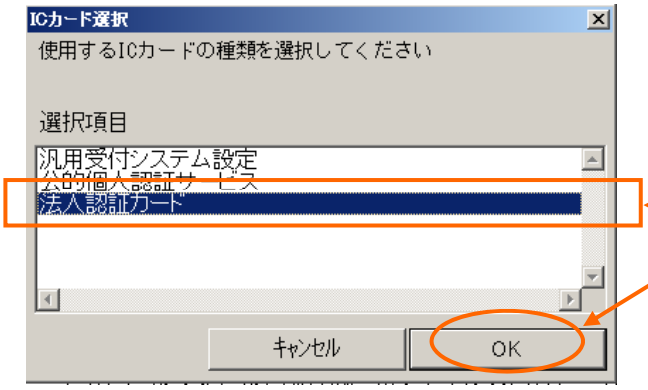
6

「署名追加」をクリック



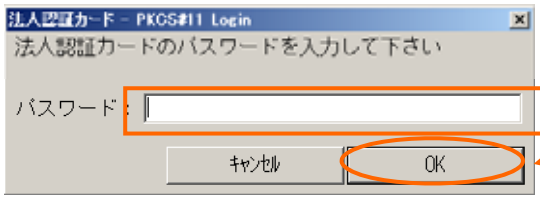
7

ICカードを選択して「決定」をクリック



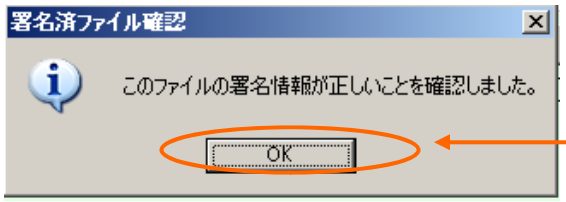
8

法人認証カードを選択して「OK」をクリック



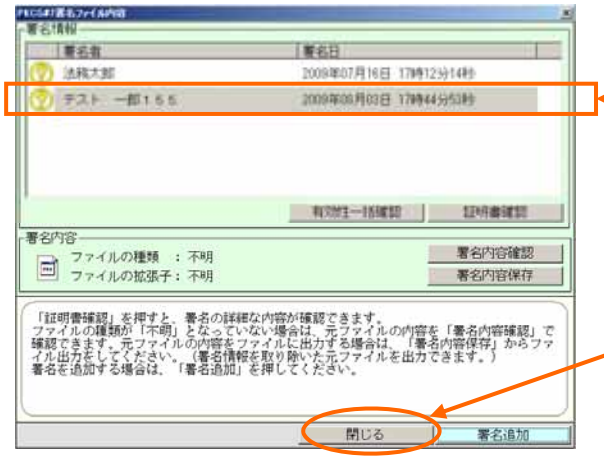
9

「パスワード」(PIN)を入力して「OK」をクリック



１０

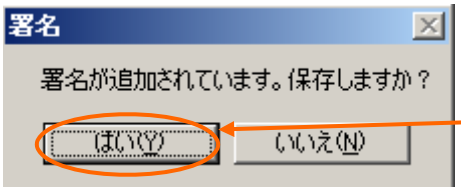
「OK」をクリック



追加した電子署名の情報が表示されます

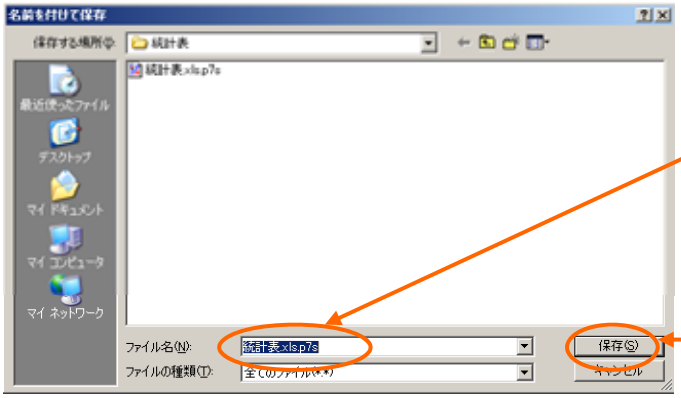
１１

「閉じる」をクリック



１２

「はい」をクリック



１３

ファイル名の後に拡張子「.p7s」を入力

元のファイルの拡張子(.xls等)をファイル名に含めると、元の状態に戻すときに便利です。

１４

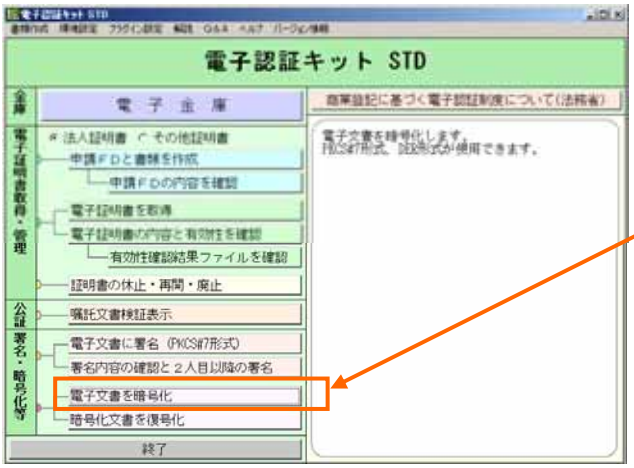
「保存」をクリック

１５

「OK」をクリック

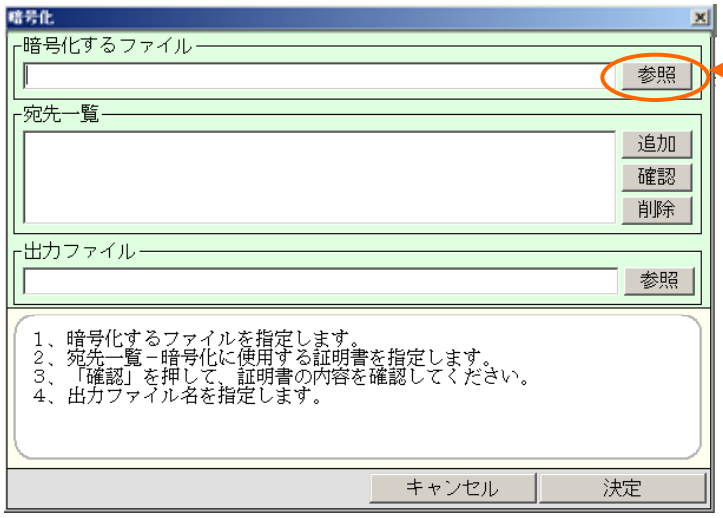
5.電子署名を付した文書をさらに暗号化

電子認証キットの起動、パソコンにICカードリーダを接続、ICカードリーダに法人認証カードを挿入した状態で操作を始めてください。



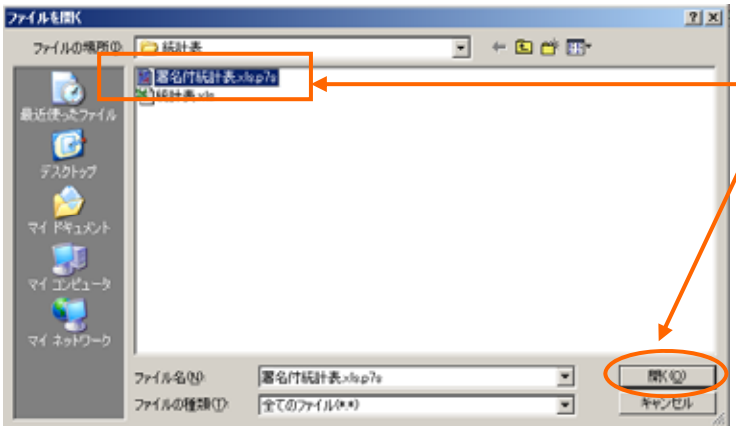
１

「電子文書を暗号化」をクリック



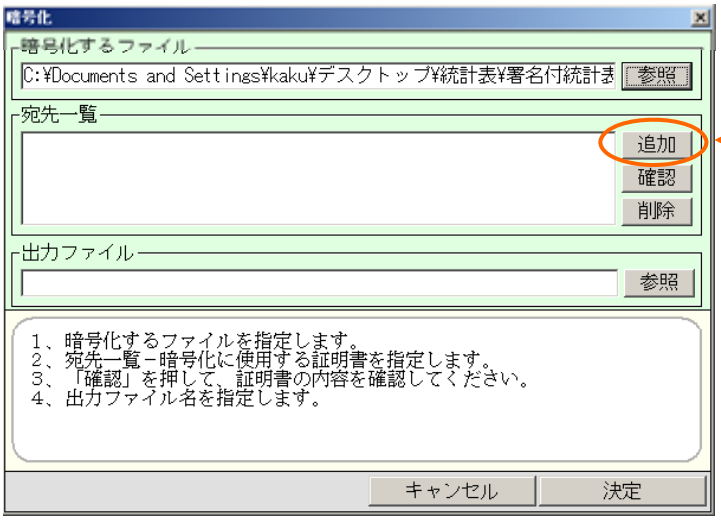
２

「参照」をクリック



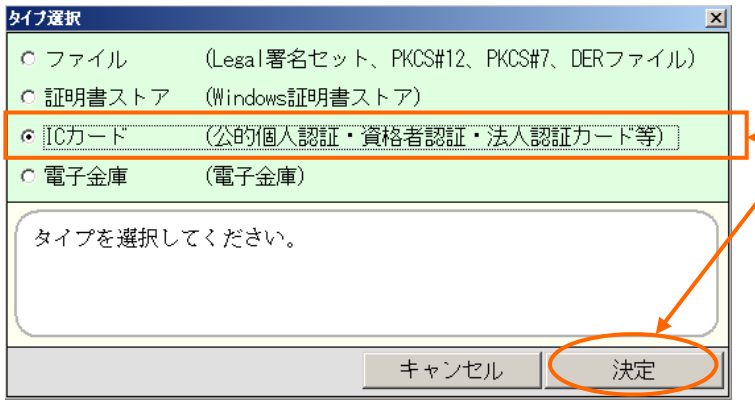
3

電子署名したファイルを選択して「開く」をクリック



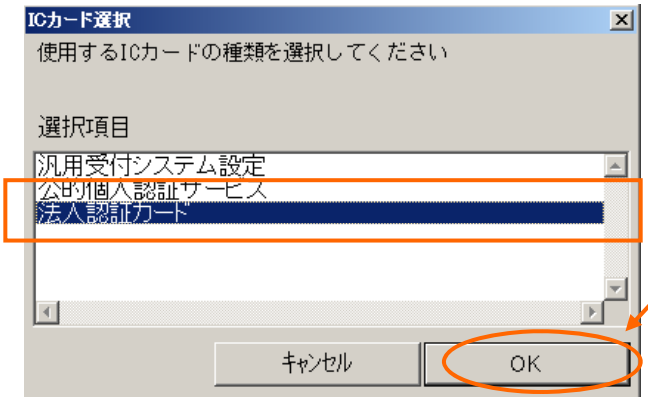
4

「追加」をクリック



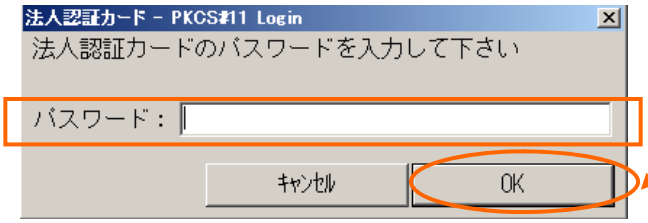
5

ICカードを選択して「決定」をクリック



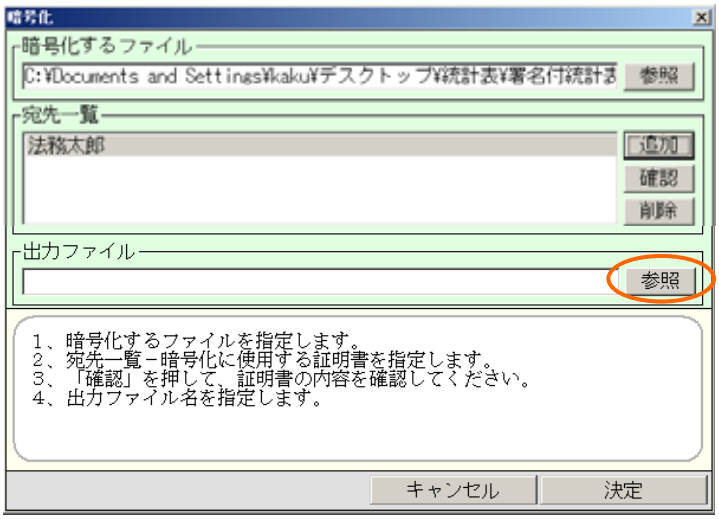
6

法人認証カードを選択して「決定」をクリック



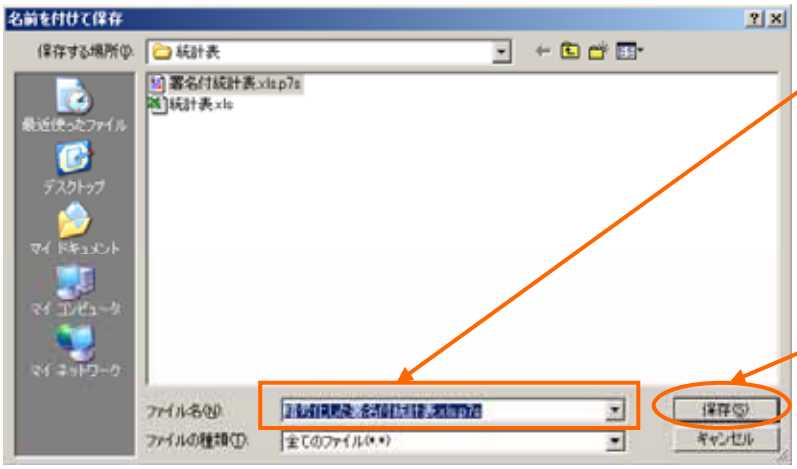
7

「パスワード」(PIN)を入力して「OK」をクリック



8

「参照」をクリック



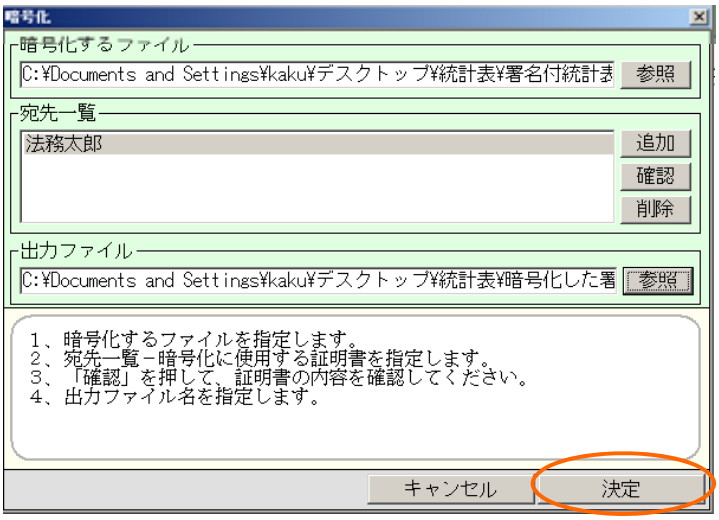
9

ファイル名の後に拡張子「.p7s」を入力

元のファイルの拡張子(.xls等)をファイル名に含めると、元の状態に戻すときに便利です。

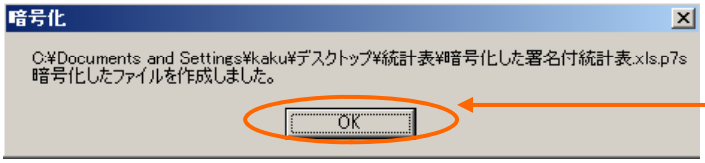
１０

「保存」をクリック



１１

「保存」をクリック



１２

「保存」をクリック

区別がつくように、ファイル名に「暗号化」の表示を加えた例

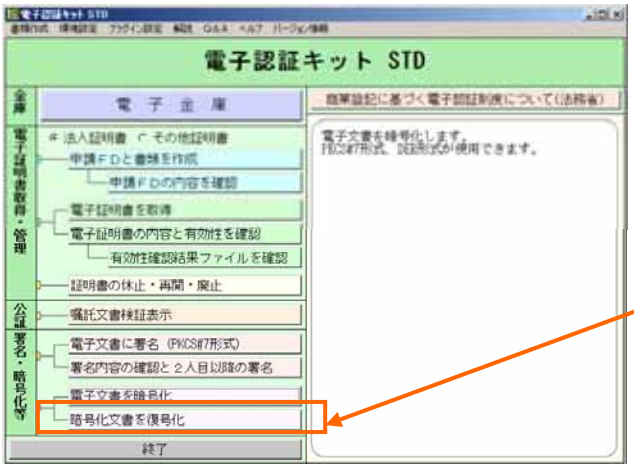
暗号化、電子署名の状態から戻した場合の拡張子が.xls(エクセル)になるように名前の付け方を工夫している

電子署名を付した場合と同じアイコンになりますので、電子署名のみの場合と暗号化も行った場合を混同しないように、それぞれのファイル名のつけ方を区別すると便利です。

6. 暗号化した文書の復号（暗号化した状態から戻すこと）

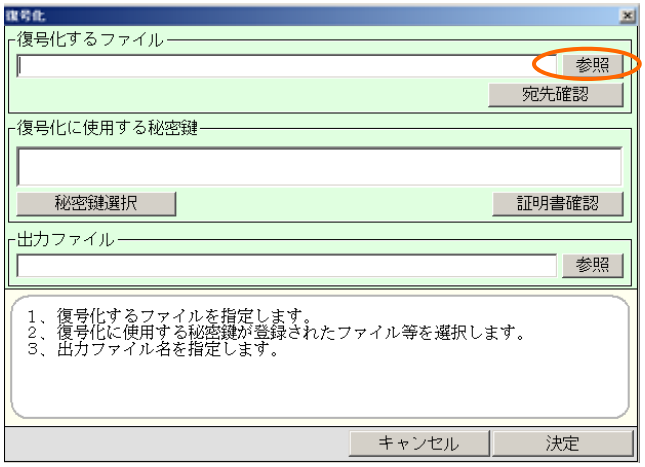
電子認証キットの起動、パソコンにICカードリーダを接続、ICカードリーダに法人認証カードを挿入した状態で操作を始めてください。

なお、復号は、暗号化に使用した法人認証カードがないと行うことができません。



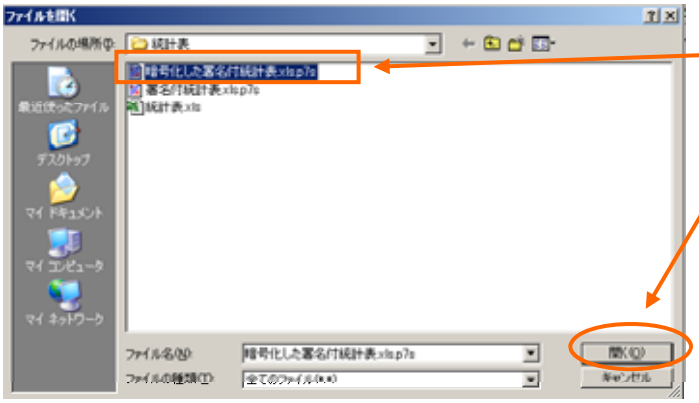
1

「電子文書を復号化」をクリック



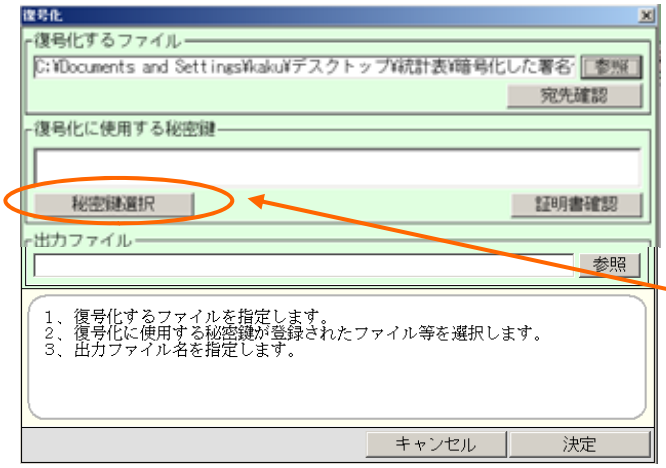
2

「参照」をクリック



3

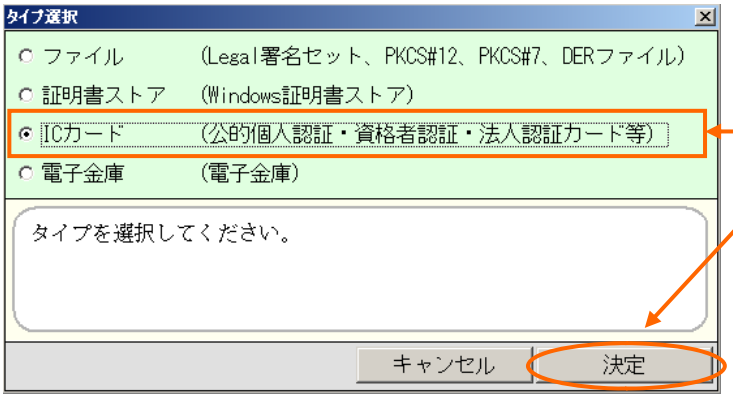
復号するファイルを選択して「開く」をクリック



【参考】ICカードは秘密鍵が外部に出ません
法人認証カードは秘密鍵が外部に出ない構造になっていますので、電子文書に物理的な”鍵”をかけたような効果が得られます。

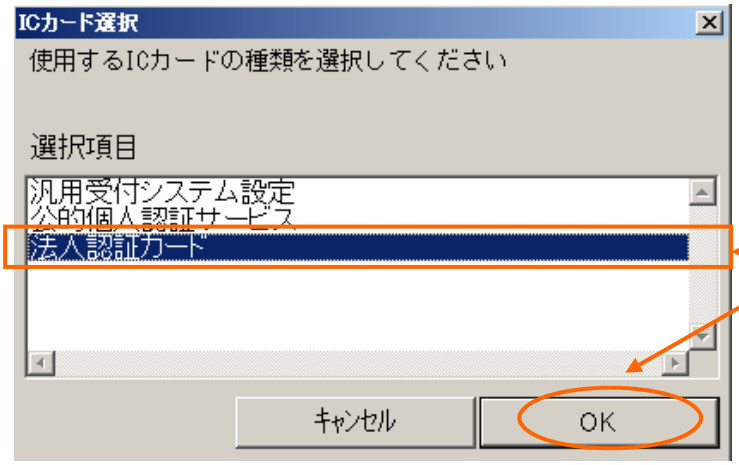
4

「秘密鍵選択」をクリック



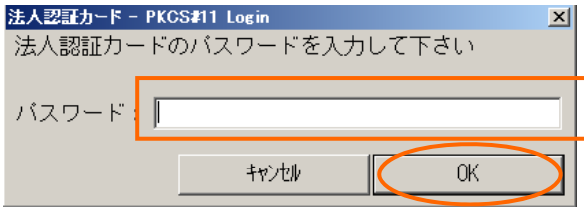
5

ICカードを選択して「決定」をクリック



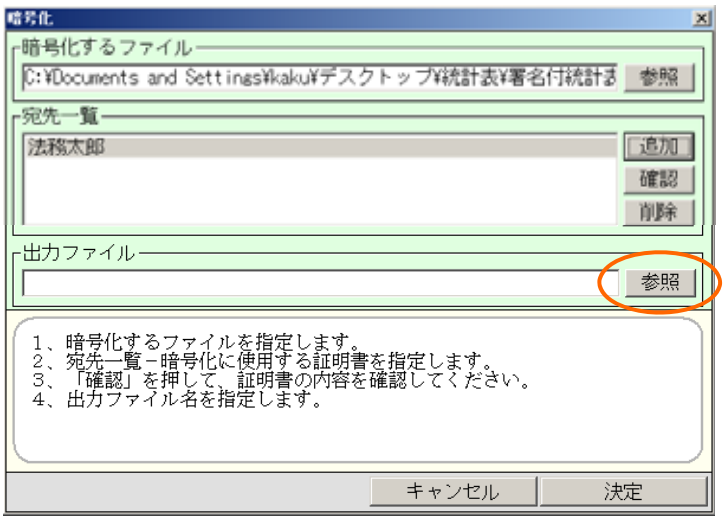
6

法人認証カードを選択して「OK」をクリック



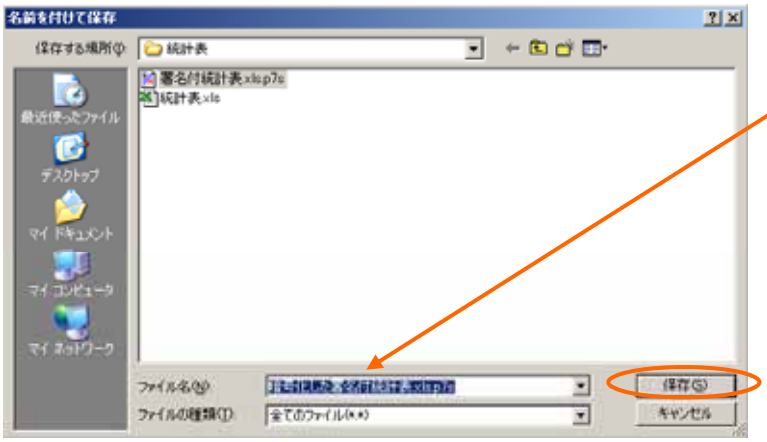
7

「パスワード」(PIN)を入力して「OK」をクリック



8

「参照」をクリック



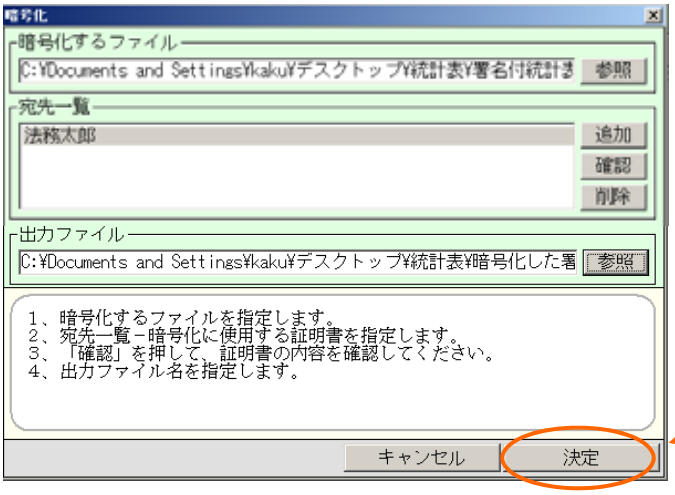
9

ファイル名の後に拡張子「.p7s」を入力

元のファイルの拡張子(.xls等)をファイル名に含めると、元の状態に戻すときに便利です。

１０

「保存」をクリック



１１

「決定」をクリック

１２

「OK」をクリック

区別がつくように、ファイル名に「復号」の表示を加えた例

復号後のファイルは、電子署名を付した状態に戻ります。

電子署名を付した電子文書を暗号化した場合もアイコンの表示が同じになりますので、混同を避ける工夫として、それぞれのファイル名のつけ方を区別すると便利です。

この手順で復号された電子文書は、電子署名を付された状態です。電子署名を付された状態からさらに元の状態に戻す場合は、１３ページの手順に従って操作をしてください。