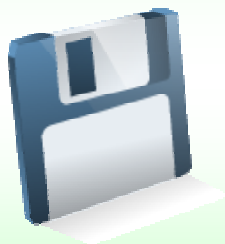


電子申請入門講座(電子証明書編)

e-Taxなどの電子申請で使う電子証明書のご紹介

商業登記に基づく電子証明書

(法務省が法人を証明しています)



ファイル形式



ICカード形式

民間認証局発行の電子証明書

(民間認証局が自然人を証明しています)



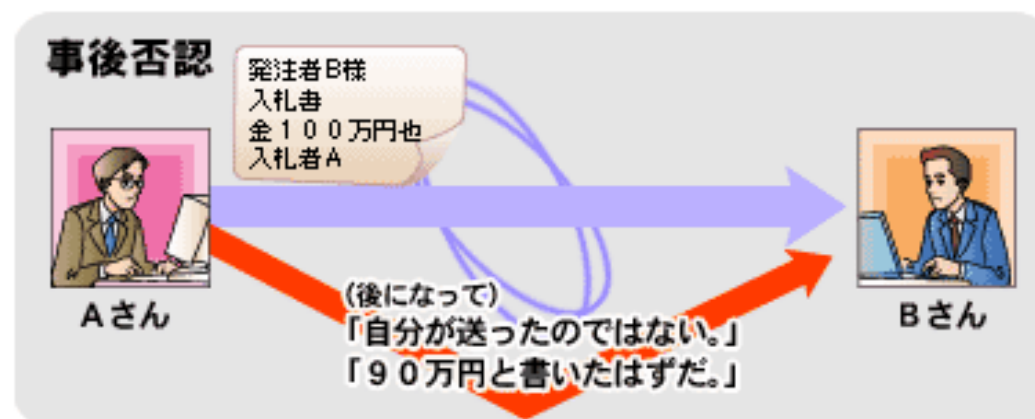
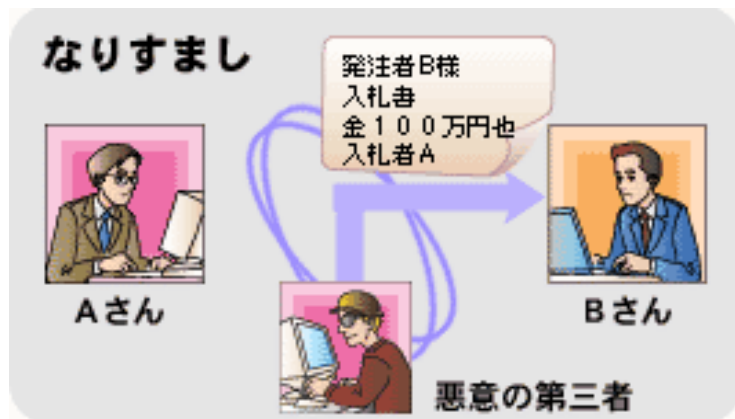
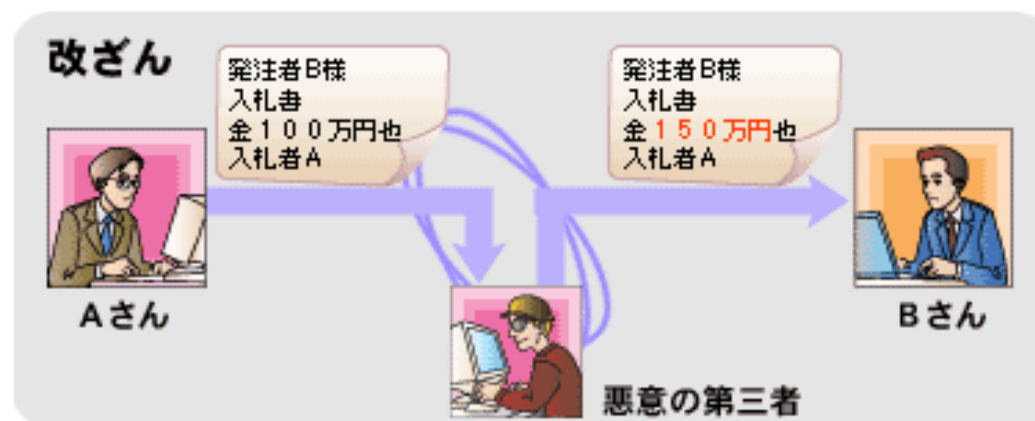
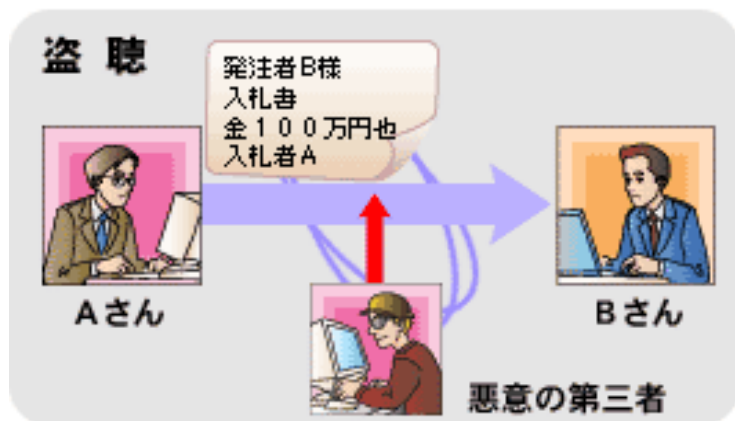
1.電子申請とインターネット

インターネット社会には、「盗聴」、「改ざん」、「なりすまし」、「事後否認」といった脅威が潜んでいるため、電子申請を安全に行うために次のような対策が講じられています。

盗聴の防止 暗号化通信

改ざん・なりすまし・事後否認の防止 電子署名(公開鍵と対を成す秘密鍵という符号で実施)

なりすまし・事後否認の防止 電子証明書(公開鍵の持主を証明する電磁的記録)による認証



2.電子申請の安全性 - 「公開鍵暗号方式」 -

電子申請によって申請者と行政庁の間を行き交う電子データは、「公開鍵暗号方式」という暗号方式によって安全性が保たれています。

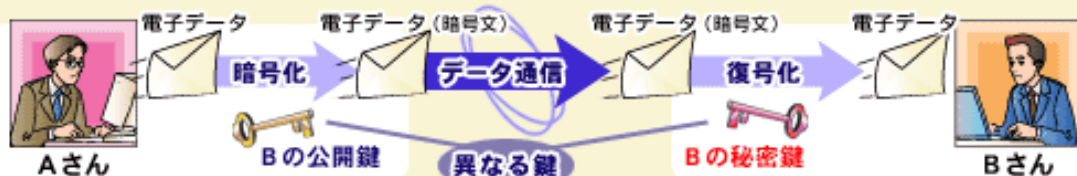
公開鍵暗号方式 暗号化、復号化する際に異なる鍵を使用する暗号方式です。

Bさんの公開鍵はインターネットを通じて誰でも取得できる。

Bさんの秘密鍵はBさんだけが持っている。



Bさんの公開鍵で暗号化した電子データはBさんの秘密鍵でのみ復号化できる。



電子データの内容がわかるのは送信したAさんとBさんだけ

AさんとBさんの間で安全な暗号化通信が実現(第三者が盗み見ることは不可能)

【暗号化】

電子データを一定の規則に従って第三者が見ても分からないデータに変換すること
電子申請で申請する電子データは、申請者の「秘密鍵」で暗号化します。

【復号化】

第三者が見ても分からないデータを一定の規則に従って元の電子データに変換すること
行政庁は、申請者の「秘密鍵」で暗号化された電子データを「公開鍵」で復号化します。

【鍵】

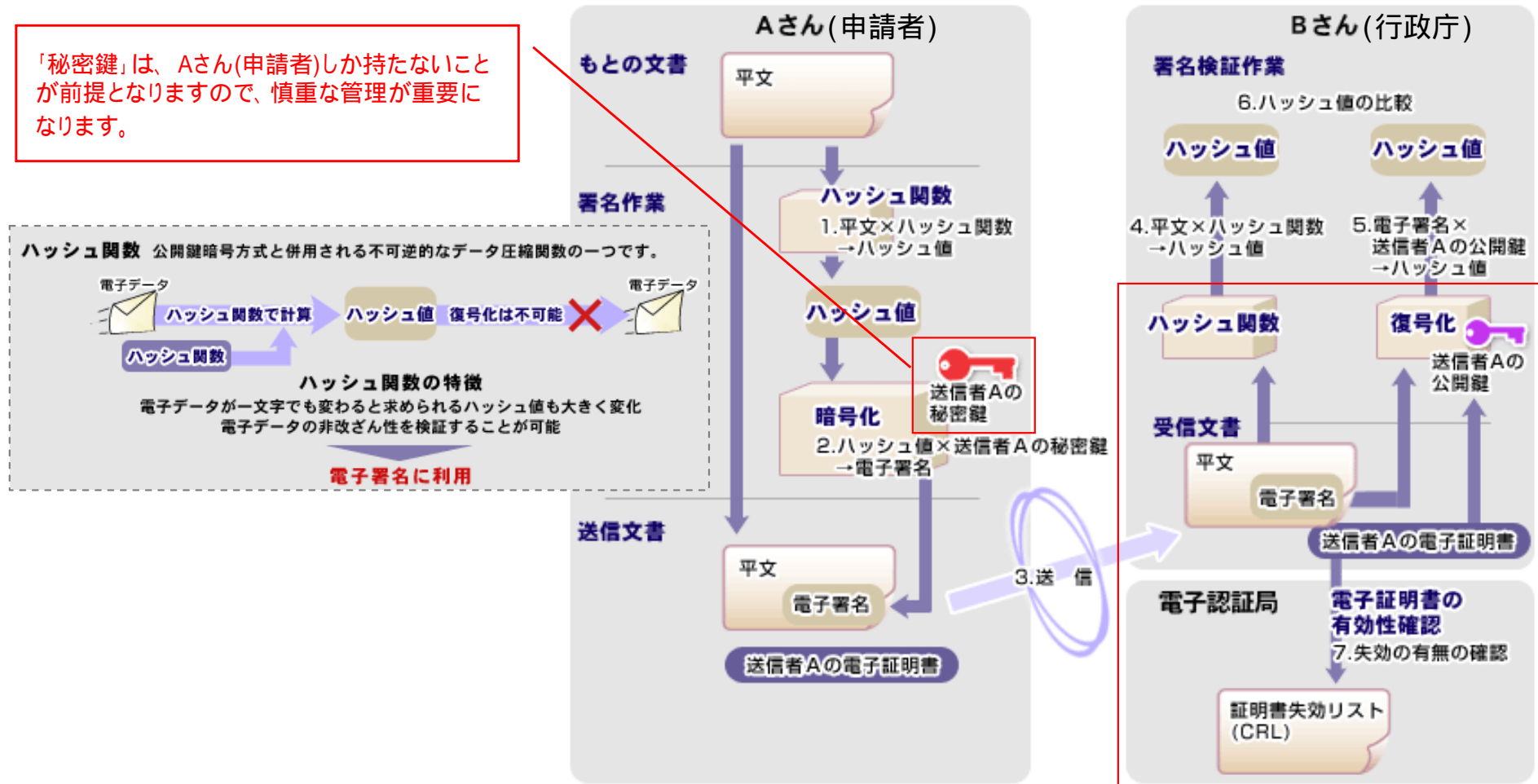
電子データを変換する一定の規則のこと
電子申請で採用されている「公開鍵暗号方式」では、「公開鍵」と「秘密鍵」という2つで一对の「鍵」を使用します。

なお、「電子証明書」とは「秘密鍵」と対を成す「公開鍵」の持主を認証局が証明する電子データを指し、「秘密鍵」と一緒にICカードなどに格納されます。

3.公開鍵暗号方式と電子証明書の関係

電子署名をすることによって、公開鍵に対応する秘密鍵の持ち主によって署名されたことを確認できますが、Aさんが本当にその秘密鍵の持ち主でしょうか？しっかり確認しないと、なりすましや事後否認が発生する可能性があります。この問題を解決する方法の一つとして、秘密鍵と公開鍵が間違いなくAさんのものであることを電子認証局が証明（電子証明書）します。

「秘密鍵」は、Aさん(申請者)しか持たないことが前提となりますので、慎重な管理が重要になります。



4. 「電子証明書」を身近なものに例えると？

書面による取引等においては、取引相手方の「本人性」、「法人の存在」、「代表権限の存在」を確認するための手段として、印鑑証明書・資格証明書が広く利用されています。

一方、インターネット経由で電子申請を行う場合、「秘密鍵」による電子署名及び電子証明書による電子認証が印鑑証明書・資格証明書の代替として機能します。例えてみると、「秘密鍵」は電子的な企業実印、「電子証明書」は印鑑証明書にそれぞれ相当するといえます。

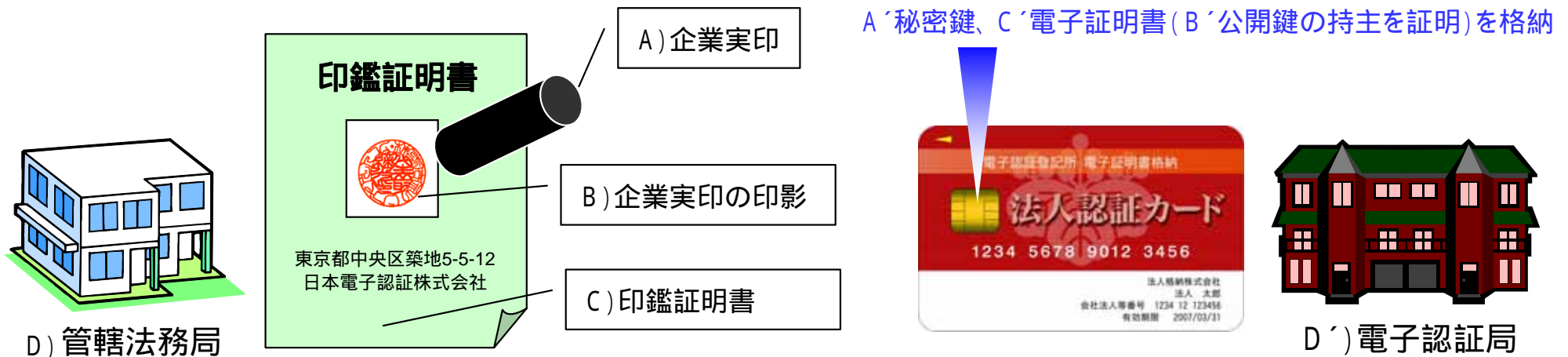
企業実印の要素

- A) 企業実印
- B) 企業実印で押印した印影
- C) 印鑑証明書 (印影に対応する印章の持主を証明)
- D) 管轄法務局 (印鑑証明書発行)

対応

電子認証の要素

- A') 秘密鍵 (電子署名に使用)
- B') 公開鍵 (秘密鍵と"対"の関係、復号化に使用)
- C') 電子証明書 (公開鍵の持ち主を証明)
- D') 電子認証局 (電子証明書発行)



5.電子証明書の分類

法人を証明する電子証明書は、法務省が発行する「商業登記に基づく電子証明書」に限られます。ほかの認証局は、いずれも自然人（個人）を証明する電子証明書を発行します。

民間認証局の場合は、証明対象が自然人であることから、発行申込に住民票の写し(市区町村で発行される原本)や印鑑登録証明書の提出が必要になります。

これに対して「商業登記に基づく電子証明書」は、発行申込に住民票の写しなどの提出は不要です。

	商業登記に基づく電子証明書		公的個人認証 カード	民間認証局が発行する 電子証明書
	ファイル形式	法人認証カード ICカード形式		
電子証明書の形式	ファイル形式	ICカード形式	ICカード形式	ファイル形式 ICカード形式
発行者	法務省		区市町村	日本電子認証ほか (民間会社)
証明対象	法人		自然人	自然人
証明される 主な項目	商号・本店住所・代表者名・ 代表者の資格		住所・氏名・ 生年月日・性別	住所・氏名 (所属企業名・企業住所等)
法人が利用 する場合の 主な用途	電子申請全般 一部の電子入札		e-Tax	電子入札コアシステム e-Taxほか

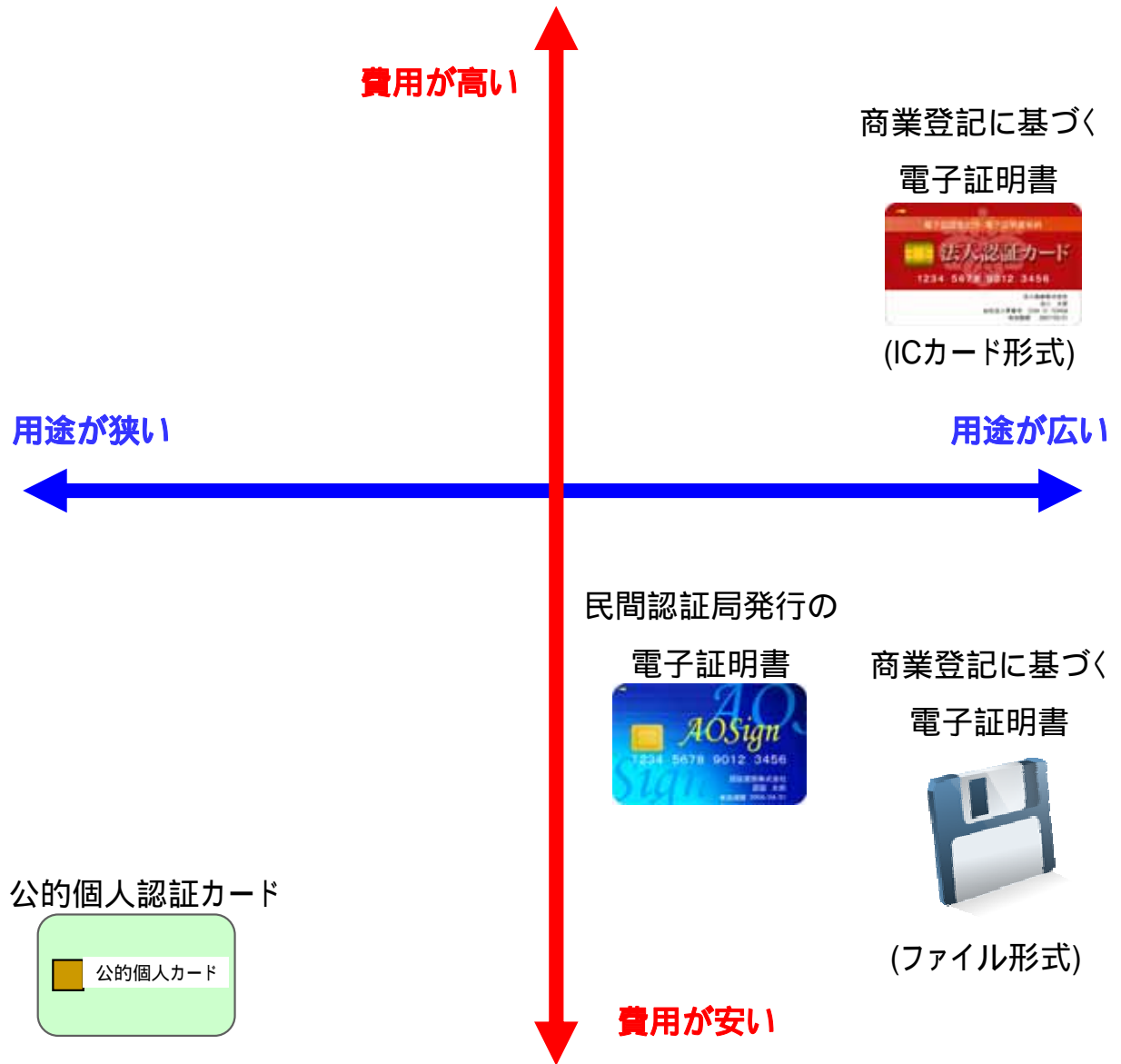
6.電子申請における各電子証明書の位置づけ

「商業登記に基づく電子証明書」は、電子申請において最も幅広い用途に利用できます。

ファイル形式とICカード形式の2つがあり、ICカード形式の法人認証カードは、不正コピー等が不可能であることなどから、セキュリティを重視する企業の利用が増加しています。

民間認証局の電子証明書は、電子入札で広く利用されていますが、電子申請では「商業登記に基づく電子証明書」と比べると用途が限定されます。

公的個人認証カードは、費用は最も低廉ですが、法人として利用できる用途は極めて限定的となります。（例/e-Tax）



7. 商業登記に基づく電子証明書の留意点 - 格納媒体 -

破損・紛失・盗難
不正コピー
秘密鍵の社外流出

用途が幅広いだけに、商業登記に基づく電子証明書の管理は、次のようなリスクに留意する必要があります。

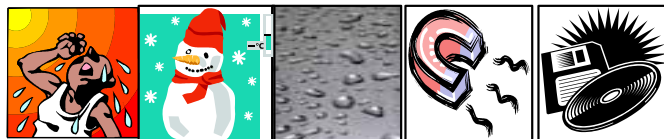
【ファイル形式の場合】

CD-ROMやフロッピーディスクなどに格納する場合は、破損などに注意が必要。
管理が不十分な場合は、不正なコピーや社外流出のリスクが発生。ハードディスク保存の場合は特に注意！

【ICカード形式の場合】

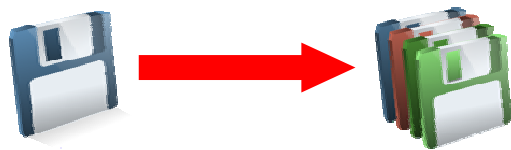
頑丈で破損などに強く、パスワード管理によって不正アクセスを確実に防止。
コピーが不可能で、秘密鍵などの機密データが外部に出ない構造。

1. フロッピーディスクは壊れやすい

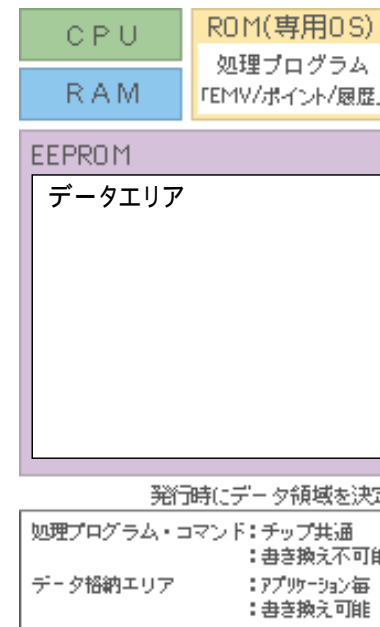
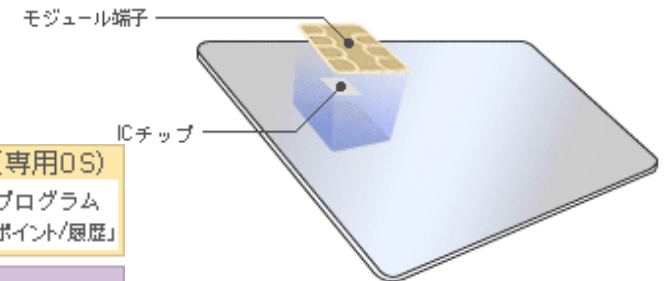
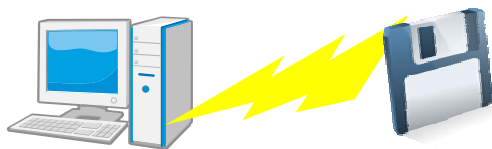


暑さ 寒さ 結露 磁気 傷・磨耗

2. コピーが簡単に作れる



3. 不注意によって秘密鍵が社外流出する



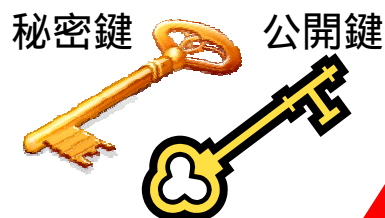
ICカードは、カード自体が不正アクセスを拒否する機能を持っており、パスワードの入力ミスが連続し規定回数に達すると不正アクセスと判断し、カード機能の停止、カード内データの消去などを設定することが可能です。

また、コピーも不可能です。

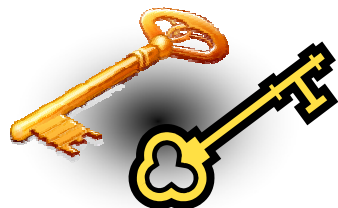
8.商業登記に基づく電子証明書の留意点 - 作成工程 -

電子証明書を格納する媒体がいくら頑丈であっても、「鍵ペア」の作成や電子証明書のダウンロードの工程で安全管理を怠ると、不正コピーや社外流出のリスクが発生しますので、複数人で手順を確認するなどの慎重が必要です。

商業登記に基づく電子証明書を自社で取得し、ファイル形式で利用する場合は、専用のソフトを利用して「秘密鍵」と「公開鍵」の「鍵ペア」を自ら作成する必要があります。



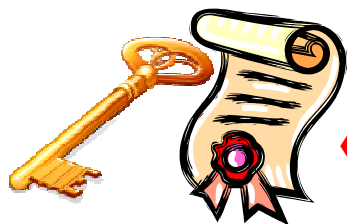
「鍵ペア」



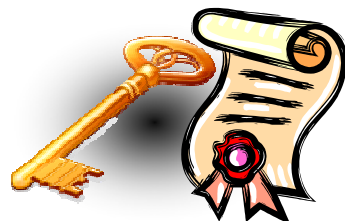
「鍵ペア」(不正コピー)

【鍵ペアの作成段階の留意点】

不正コピー、不注意などによる社外流失を防止するため、「鍵ペア」の作成は、複数人で慎重に行うことをお奨めします。



秘密鍵 電子証明書



秘密鍵(悪用のリスク)

【電子証明書をダウンロードする段階の留意点】

電子証明書をダウンロードすると、「鍵ペア」に含まれる「秘密鍵」と組み合わせ、電子署名などが可能になりますので、慎重に取り扱う必要があります。このダウンロードも複数人で手順を確認しながら行うことをお奨めします。



ICカードやUSBトークンは、不正コピーなどの防止に優れた格納媒体ですが、電子証明書の発行に関する全工程について安全管理をしないと、不正コピーなどを完全に防ぐことは困難です。

9. (ご参考) 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、高いセキュリティレベルを保つ施設と作業手順によって、商業登記に基づく電子証明書をICカードに格納します。ICカード型の電子証明書としては、国の電子申請に最も幅広く利用できる点も魅力です。法人認証カードで電子申請に挑戦してみませんか？

AOSignサービスで培った「電子署名法・認定認証業務」のノウハウを結集！

