総務省
MIC Ministry of Internal Affairs and Communications

マイナンバーカードの安全性


マイナちゃん

令和2年4月8日
総務省自治行政局
住民制度課


マイキーくん

マイナンバーカードの安全性のポイント

① 落としても他人が使うことができない

- 顔写真入りのため対面での悪用は困難。
- オンラインで使用するためには本人しか知らない暗証番号が必要。
- 不正に情報を読み出そうとするとICチップが壊れる仕組み。

② 大切な個人情報は入っていない

- プライバシー性の高い情報はマイナンバーカードのICチップに入っていない。
- 税や年金などの情報は、各行政機関において分散して管理。

  ⇒ 仮にマイナンバーが他人に知られても芋づる式に個人情報が漏れることはない。

③ 24時間365日体制で一時利用停止を受付

マイナンバーカードの安全性

なりすましはできない

✓ 顔写真入りのため、
対面での悪用は困難。

万全のセキュリティ対策

➢ 紛失・盗難の場合は、
24時間365日体制で停止可能

➢ アプリ毎に暗証番号を設定し、
一定回数間違うと機能ロック

➢ 不正に情報を読み出そうとすると、ICチップが壊れる仕組

大切な個人情報は入っていない

✓ ICチップ部分には、
税や年金などの
個人情報は記録されない。

マイナンバーを見られても個人情報は盗まれない

✓ マイナンバーを利用するには、
顔写真付き身分証明書等での
本人確認があるため、悪用は困難。

オンラインの利用には マイナンバーは使われない

知って安心！マイナンバーカードの使い方

持ち歩き方

普通に持ち歩いていいの？

ええんじゃよ。キャッシュカードの感覚が近いかの。失くさないようにするのじゃよ！

暗証番号

暗証番号を友達に教えても大丈夫？

キャッシュカードと同様、他人に教えてはいけないのじゃ。
暗証番号はマイナンバーカードを利用するために必要な大事なものじゃよ！

提示方法

銀行や勤務先などでマイナンバーの提示を求められたときはどうすればいい？

おもて・うら両面を見せるのじゃ。

じゃあレンタルショップなどで、身分証明書として使うときは？

おもて面を見せるのじゃ。
その際、うら面のマイナンバーは見られても大丈夫じゃが、マイナンバーを書き留めたりコピーを取ることはダメなのじゃ。

SNSへカードの画像の投稿は？？

こんなに安全なら、
カードを自慢しても大丈夫？

マイナンバーを誰かに知られても大丈夫なように安全対策は施されているが、不特定多数の目に入る場所への投稿は禁止されているのじゃ！

リーフレット　カードの安全性

マイナンバーカードの３つのギモンに マイナンばあちゃんがお答えします！

① うら面のマイナンバーを他人に見られたらどうなるの？

見られても他人は悪用できない仕組みなのじゃ！

② マイナンバーで預貯金額や医療などのあらゆる情報を国から監視されるの？

監視はしていないしできないのじゃ！

③ マイナンバーカードを落としたり失くしたりしたらどうしよう…

安心せい、まずは電話じゃ！

ポイント１

他人があなたのマイナンバーを使って手続することはできません！

マイナンバーを使う手続では顔写真付の身分証明書での本人確認が行われます。

マイナンバーを知られても、あなたの個人情報を調べることはできません！

- マイナンバーの利用範囲や、収集・保管などは法令で厳しく制限されています。
- 個人情報を一元管理する仕組みではないため、情報が芋づる式で漏れることはありません。（ポイント２参照）

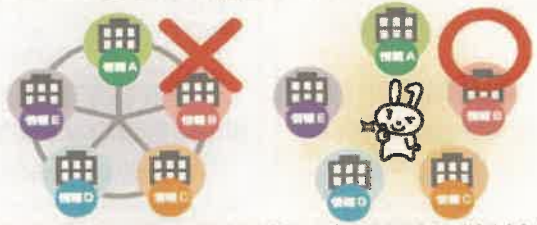
マイナンバーを悪用した場合には厳しい罰則があります！

例えば…
マイナンバーを扱うことができる人が、自分または誰かの不正な利益のためにマイナンバーを提供した場合は、３年以下の懲役か150万円以下の罰金、もしくは両方が科されます。

※罰則は他にもあります。

ポイント２

マイナンバー制度はあなたの情報を１か所に集めて管理する仕組みではありません！



手続を受付ける行政職員だけが、その手続に必要な情報に限ってアクセスすることが許されています。

不正なアクセスが行われないように、第三者機関の「個人情報保護委員会」が監視・監督しています。

ポイント３

24時間365日体制にてマイナンバーカードの一時利用停止を受付！

キャッシュカード等と一緒だね！

0120-95-0178

通話料無料！
外国語にも対応！（英・中・韓・スペイン・ポルトガル）

詳しくはうら面を見てね

カードのICチップには、税や年金などのプライバシー性の高い情報は入っていません！

健康保険証として使えるようになっても（2021年３月（予定）スタート）、健診結果や薬剤情報がICチップに入ることはないんだね。

カード利用には暗証番号等の認証が必要です！

- 暗証番号を一定回数間違うとカードがロック
- 不正に情報を読み出そうとするとICチップが壊れる

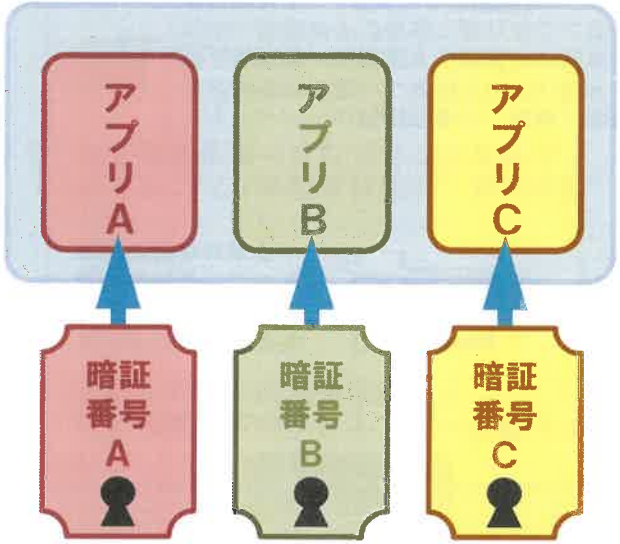
他人が悪用できないようになっているんだね！

※上記はリーフレットの内面のみ表示

マイナンバーカードのセキュリティ対策

暗証番号

■ アプリケーション毎に異なる暗証番号の設定可能



■ 暗証番号の入力を一定回数以上間違うとカードがロックされる

《イメージ》

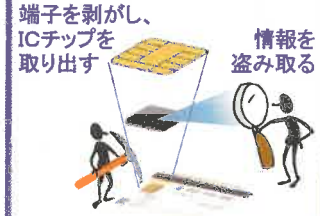
耐タンパー性

■ ＩＣチップは偽造を目的とした不正行為に対する **耐タンパー性** を有する。

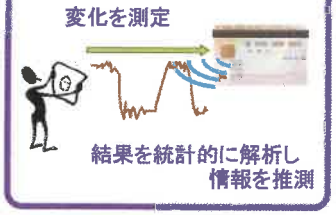
※タンパー(tamper)：
「干渉する」「いじくる」「いたずらする」「勝手に変える」の意

偽造目的の主な不正行為

① ICチップを取り出し、電気的または物理的に情報を不正に読み出す



② ICチップの電力消費量や処理時間等を測定・解析し、情報を推測



個人番号カードのＩＣチップは、①と②の両方に対抗できる

①に対して

- 光が当たるとメモリ内容消去
- メモリ回路素子が表面から観察できない
- 電圧異常、クロック異常等の検知で動作停止
- メモリ素子の物理配置ランダム化&暗号化により、解読不可

②に対して

消費電力、処理時間をかくはんすることで、読み取った信号の統計的な解析を困難にする

ＩＳＯ/ＩＥＣ１５４０８認証

■ セキュリティ機能評価の国際標準の認証を取得

●ＩＳＯ/ＩＥＣ１５４０８認証とは

- コンピュータシステムや製品のセキュリティ機能の評価を行うための基準であるCC（Common Criteria）の国際標準
- スマートカードが必要とするセキュリティの要件を記述
- スマートカードの製品調達者は、CCに基づき、PP（Protection Profile：利用者のセキュリティ要件を記述した要件仕様書）を作成
- 開発者は、PPに基づき、ST（Security Target：セキュリティ開発方針を厳密に記述したセキュリティ設計仕様書）を作成し、これを実装した製品を開発
- 評価機関が以上の課程を評価し、認証機関が認証

マイナンバーカードに格納される公的個人認証サービスについて

公開鍵暗号方式

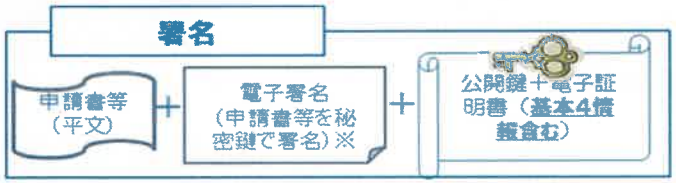
公的個人認証サービスが採用する暗号方式。秘密鍵と公開鍵はペアとなっており、片方の鍵で暗号化されたものは、もう一方の鍵でしか復号できない性質をもつ。

署名用電子証明書

（性質）
インターネットで電子文書を送信する際などに、署名用電子証明書を用いて、文書が改ざんされていないかどうか等を確認することができる仕組み

（利用局面）
e-Taxの確定申告等、文書を伴う電子申請等に利用される。

（利用されるデータの概要）



※電子署名法（平成12年法律第102号）の「電子署名」に該当し、同法第3条による「真正な成立の推定」の対象になり得る。

署名用秘密鍵

※ カードの中の格納された領域から外に出ることがない

※ 秘密鍵を無理に読みだそうとすると、ICチップが壊れる仕組み

電子証明書のイメージ

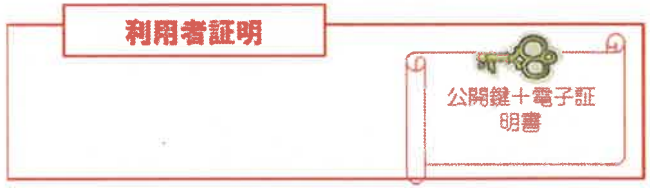
※基本4情報を記録

利用者証明用電子証明書

（性質）
インターネットを閲覧する際などに、利用者証明用電子証明書（基本4情報の記載なし）を用いて、利用者本人であることのみを証明する仕組み

（利用局面）
マイナポータルのログイン等、本人であることの認証手段として利用される。

（利用されるデータの概要）



利用者証明用秘密鍵

※ カードの中の格納された領域から外に出ることがない

※ 秘密鍵を無理に読みだそうとすると、ICチップが壊れる仕組み

電子証明書のイメージ

※基本4情報の記録なし

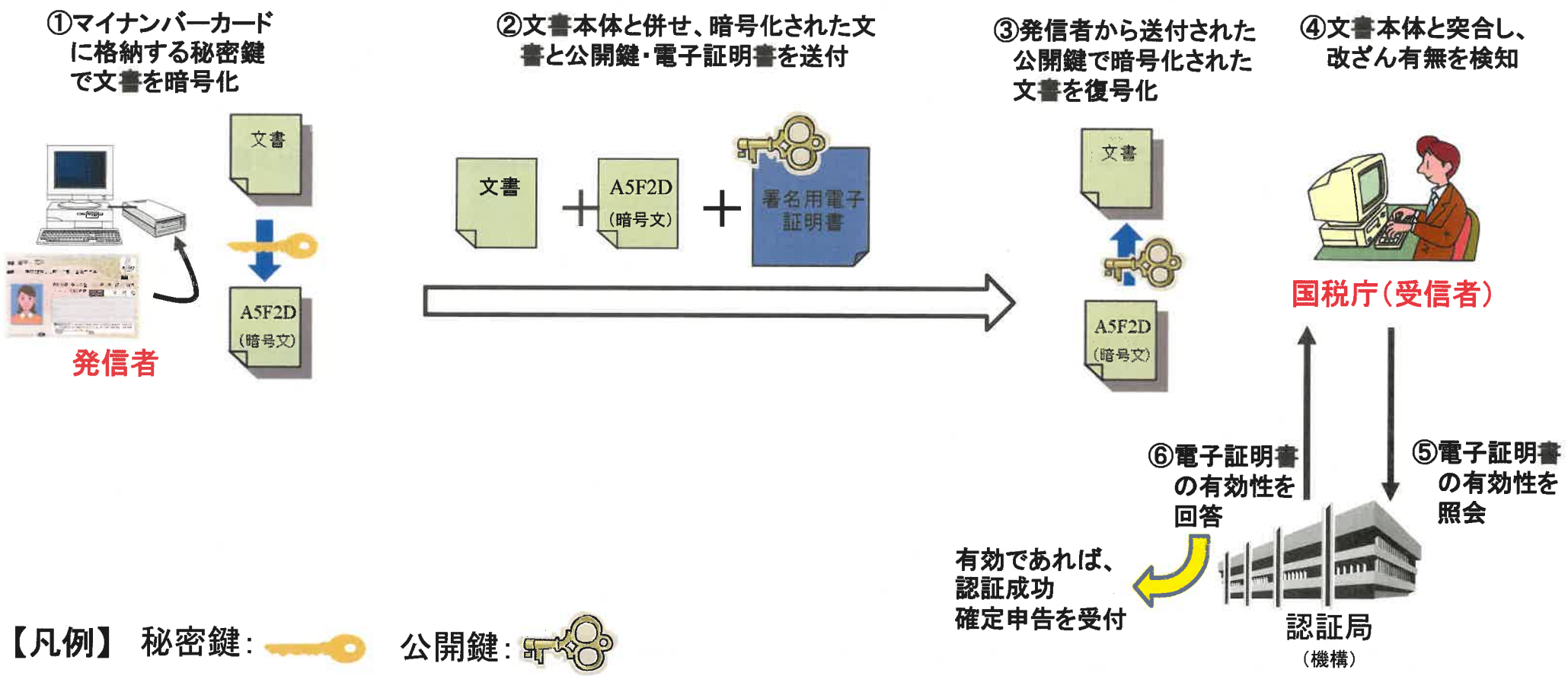
公的個人認証サービスの仕組み（署名用電子証明書）

（1）発信者がマイナンバーカードに格納されている秘密鍵を用いて文書を暗号化し、その秘密鍵とペアとなっている公開鍵とともに元の文書、暗号化した文書を送付。

（2）受信者は発信者から送付を受けた公開鍵を用いて暗号化した文書を復号し、文書本体と突合し、改ざんの有無を検知。

（3）受信者は送付を受けた署名用電子証明書の有効性を確認。

【確定申告における例】

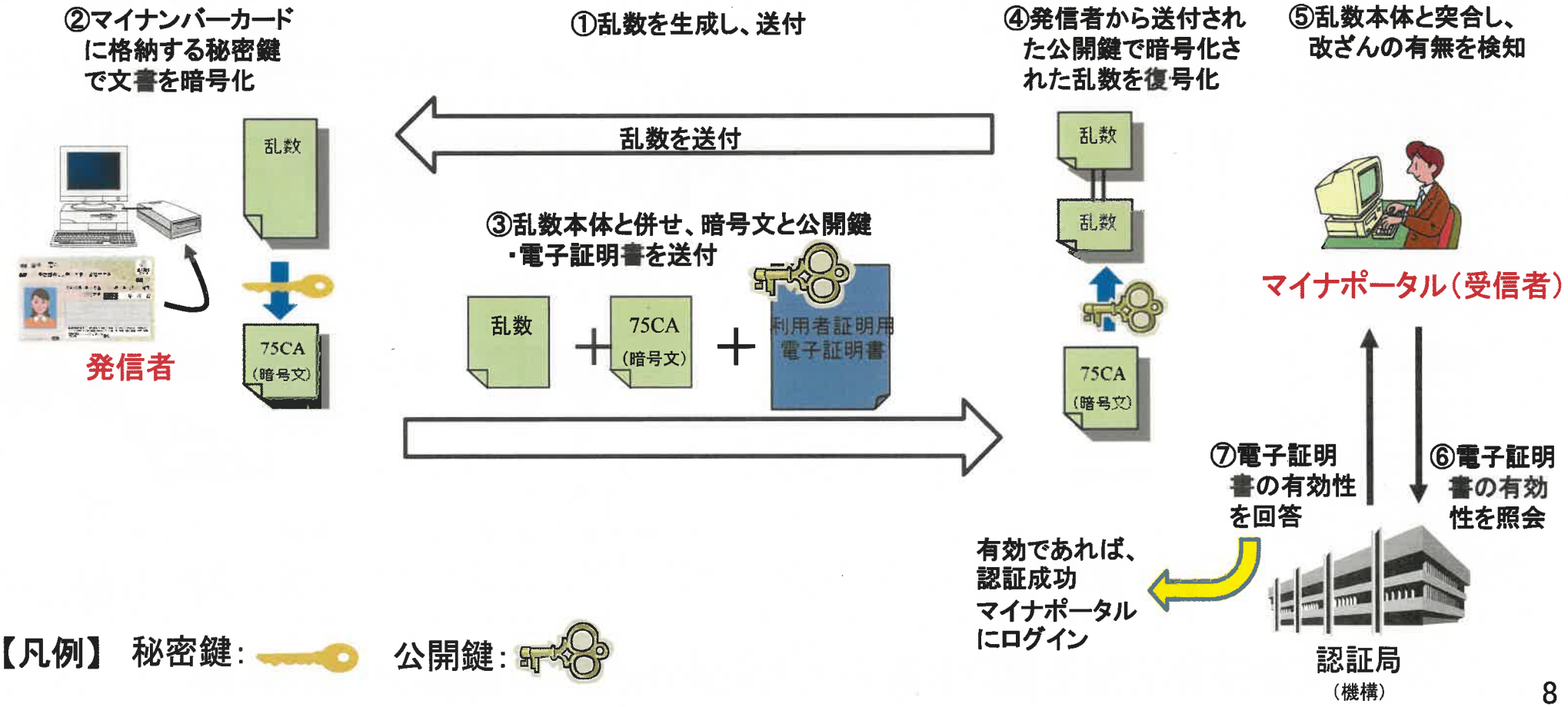


【凡例】 秘密鍵： 公開鍵：

公的個人認証サービスの仕組み（利用者証明用電子証明書）

（1）受信者から乱数を送付
（2）発信者がマイナンバーカードに格納されている秘密鍵を用いて文書を暗号化し、その秘密鍵とペアとなっている公開鍵とともに元の乱数、暗号化した乱数を送付。
（3）受信者は発信者から送付を受けた公開鍵を用いて暗号化した乱数を復号し、乱数本体と突合し、改ざんの有無を検知。
（4）受信者は送付を受けた利用者証明証電子証明書の有効性を確認。

【マイナポータルにおける例】



安全・安心な認証サービスの提供（電子署名と電子利用者証明）

1．文書を伴うアクセス

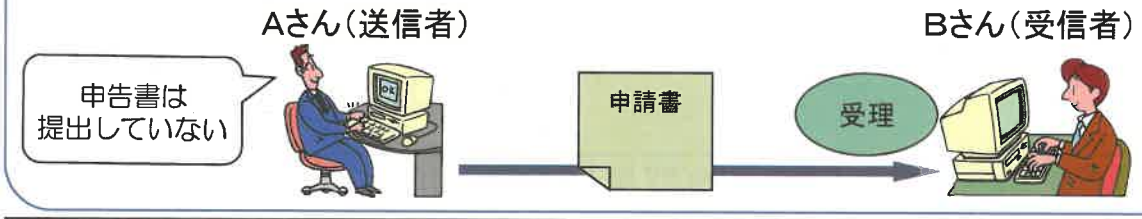
①　成りすまし　（申請書の正しい送信者を受信者が確認できない）

※CさんがAさん名義の申請書を勝手に作成し送信する

②　改ざん　（申告途中で申告書の書き換えが行われる）

※デジタル文書は、手書きの文書と異なり、改ざんされても痕跡が残らず、改ざん箇所を発見することは、実際上不可能

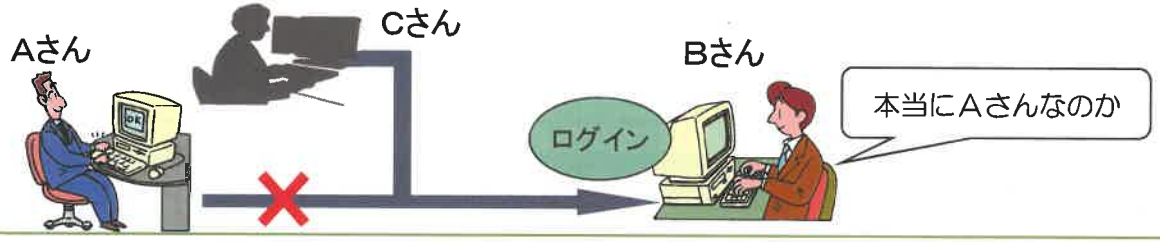
③　送信否認　（送信内容の否認を防止することが困難）



※オンラインで送信されてきた申請・届出に基づいて、手続を進行させていたところ、送信者からそのような送信はしていないとの否認をされる危険性がある

2．文書を伴わないアクセス

①　成りすまし　（←アクセスする本人の特定が困難）



※CさんがAさんに成りすまし、勝手にログインをする

対策

電子署名

- ○送信者が本人であることを確認
- ○文書が改ざんされていないことを確認
- ○送信者は送信内容を否認することができない

対策

電子利用者証明

- ○送信者が本人であることを確認

マイナンバーカードを紛失した場合の対応～24時間365日体制のコールセンターとカードセキュリティ対策～

カードの紛失

本人が気付く

コールセンターに連絡

本人が気付かない

コールセンターに連絡

第三者が拾得

警察に拾得物として届いた場合、本人又は発行市町村に連絡してもらうよう警察庁に依頼

本人が気付かない

悪用を試みる

第三者が拾得

コールセンター対応

- 24時間365日体制にて対応
- 紛失の連絡を受け付け次第、一時停止処置対応
- 日本語以外の言語にも対応
  （英語・中国語・韓国語・スペイン語・ポルトガル語を予定）
- 第三者が拾得した場合、早急に市町村へ連絡し、本人に連絡を行うように対応

市町村窓口

手元に戻る場合

- 市町村窓口へ
- 一時停止を解除し、本人利用の再開

手元に戻らない場合

- 市町村窓口へ
- 廃止を行い、再交付を申請

セキュリティ対策により悪用困難

顔写真付きであることに加え、ICチップにはプライバシー性の高い個人情報は記録されない

アプリ毎に異なる暗証番号を設定し、入力を一定回数以上間違うとカードがロック

ICチップは偽造を目的とした不正行為に対する耐タンパー性を有する

※タンパー（tamper）：「干渉する」「いじくる」「いたずらする」「勝手に変える」の意

マイナンバー制度における個人情報の管理（分散管理）

- ✕ マイナンバー制度が導入されることで、各行政機関等が保有している個人情報を**特定の機関に集約**し、その集約した個人情報を各行政機関が閲覧することができる**『一元管理』**の方法をとるもの**ではない**。
- ○ マイナンバー制度が導入されても、従来どおり個人情報は**各行政機関等が保有**し、他の機関の個人情報が必要となった場合には、マイナンバー法別表第二で定められるものに限り、情報提供ネットワークシステムを使用して、情報の照会・提供を行うことができる**『分散管理』**の方法をとるもの**である**。