別紙

通知カード及び個人番号カードに関する技術的基準の一部を改正する件（案）に対する意見募集の結果について

No.	ご意見の概要	回答	修正措置
1	3(2)にあるような業務の委託は、当面、認めるべきでない。委託を認めずに運用した状況を見て、問題がないようであれば委託も可に広げる方針にするべきである。	3（2）に規定しているように、委託先を選定するにあたっての事前の委託者によるチェックや、委託先事業者における同様のセキュリティ対策の実施、業務委託後の委託者による監督により、委託先におけるセキュリティの確保を図ることとしています。	なし
2	3(3)の報告は、案のままだと、”問題なかった””〇件”という数語でも足りることになる。もっと詳しく、基準に適合した業務を行ったことを示す報告となるよう、内容と様式を定めるべきである。	3（3）の総務大臣に対する報告については、総務省において定型の報告フォーマットを作成の上、民間事業者による報告の際にはそちらを使用していただく予定です。	なし
3	基準だけでなく、基準に適合すると認定する仕組み・手続き（申請など）についても同時に意見公募するべきである。認定の仕組み・手続きがないのであれば、不適当である。	ご意見として承ります。	なし
4	2(4)のカで、識別符号と暗証符号だけの管理も認めているが、一般に識別符号と暗証符号による管理方法で破られた例がいくつもあるのだから、少なくとも当面は認めず、オの方法がとれる者だけにするべきである。 仮に識別符号と暗証番号による管理方法を認める場合についても、その管理方法や暗証符号に関する具体的な基準を示す必要があると考える。また、システム機能として定められた基準の維持を強制するような機能（暗証の複雑性担保や定期的変更など）の導入を推奨すべきと考える。	2（4）カの方法については、身体的な障害等のやむを得ない事情を理由として、生体認証を行うことが困難な方について、特別に設けられた規定となっており、原則としては生体認証を行うこととなります。 識別符号と暗証符号の管理方法等については、事前に民間事業者に決めていただき、審査の過程で総務省において内容を確認することで、安全な管理となるよう進める予定であり、告示においてより個別具体の基準を示す必要はないものと考えます。	なし
5	3(1)オの「業務に係る記述に関し充分な知識及び経験」とあるが、どのような知識と経験で「充分」とするのか資格・年数など具体的に定めるのでなければ、「具体的基準」とは言えない。	ご指摘いただいた、3(1)オにおいて配置すべきとされている従業員の知識及び経験の程度については、従業員が担う職務の権限と責任に応じ、各民間事業者が作成する規程等の中で明確かつ適切に定めていただくことを予定しています。 なお、認定の要件として具体の資格や経験年数を要求する予定はありません。	なし
6	2(4)では、ウで「適切な場所」、オで「適切に管理し、外部に漏えいすることを防止するための措置」となっているが、「適切」というだけでは、何が適切なのかの判断は人によって違うので、基準の役割を果たさない。 適切な場所とは、どのような場所か（例えば錠の条件などがあるのか）、どのような内容の管理なら適切なのか、客観的基準を定めるべきである。	「端末機が盗取又は不正に操作されないよう」な適切な場所とは、字句のとおり、不特定又は多数の権限のないものが、容易に端末機に触れることができないような場所ということであり、具体的には、このような適切な場所を各民間事業者において、その実情に応じ確保していただくことを想定しています。	なし

7	2(3)イについて、通信データ摂取の防止が可能な方式の例示が必要と考えます。「TLS 1.2 , IPSec等のプロトコルで、暗号化方式としてAES128,RSA2048,SHA256または同等以上の強度を有する方式」などの記載があると望ましいと考えます。 【NPO日本ネットワークセキュリティ協会】	ご意見として承ります。	なし
8	2(4)イについて、これらの「措置」について、具体的な技術ガイダンス（たとえばIPA等が作成した文書等）を参照することを指定する必要があると考えます。	２（４）イについては、民間事業者がアプリ搭載を行う際には、機構が提供するクラウドサービスを利用することが必須とされており、当該クラウドサービスの標準的なメニューとして、２（４）イの要請を満たすプログラムをご準備しております。	なし
9	2(4)オの指紋認証については、以前より偽造リスクが指摘されており、偽造防止に関する技術基準の指定が必要と考えます。また、情報管理についても、別途なんらかのガイダンスを示す必要があると考えます。	ご意見として承ります。	なし
10	本改正に断固反対である。 そもそもの決定に反対である。 何故、個人情報カードを民間と共用しようなどと考えるのか。明らかに行政で閉じておくべきである。 民間に開放すると、凄まじいまでのセキュリティ攻撃に晒されるのは確実である。 コンビニエンスストアや各種小売でカードを出すだけで、あらゆる波長の電磁波による情報取得（例：布や革を透視して個人番号記載部分を見る事が可能な装置や、各種のICチップに対する攻撃）に晒されるのであるが、その様な事態に国民を晒す事は非常に罪な事と断言する。 これはOSのセキュリティ云々ではなく、チップの耐タンパ性と露出回数の問題であり、端末機のセキュリティについての検討は正直に言ってあまり効果が無い。そもそも、多くは端末機によって攻撃が行われるのではなく、行政がその存在を認めていないような装置によって攻撃が行われるのだが、それを意識しているのか。恐らく「各委員は皆それを知っていたが、不正な組織犯罪集団の一部と繋がりがあるので黙っていた。」という様な状況で検討が行われたのであろう（機械的に出る結論に注意が行われないのは、つまりそういう事である。）。 日本において、人が銃で殺される時は、警察官が持つ銃によってではなく、不法に出回っている銃で殺されるのである。そういう事を知っていて（知らないはずがない）、何故この様な「確実に大きな穴の存在が分かるのに、制御可能な問題点しか言及せず改正を行う」様な事をするのか。国民に対して非常に問題ある態度であると当方は考える。 本件については、明らかに委員会等の不徳によってなされた決定であると断じる。 国民としてこの様な決定を断固として拒否するし、阻止を行っていく所存である。	ご意見として承ります。	なし