

（8）第7次NACCSにおける認証方法＜2＞



2023年11月22日
輸出入・港湾関連情報処理センター株式会社

第7次NACCSにおけるインターネット経由の接続における認証方法の検討の結果、「政府機関等のサイバーセキュリティ対策のための統一基準（令和3年度版）」及び「政府機関等の対策基準策定のためのガイドライン（令和3年度版）」で推奨されている多要素認証方式を引き続き採用することとし、多要素認証方法においては、複数の認証方法を比較・検討したうえで、現行システム（第6次NACCS）での実績を鑑み、『デジタル証明書』による認証を行うこととなりました。

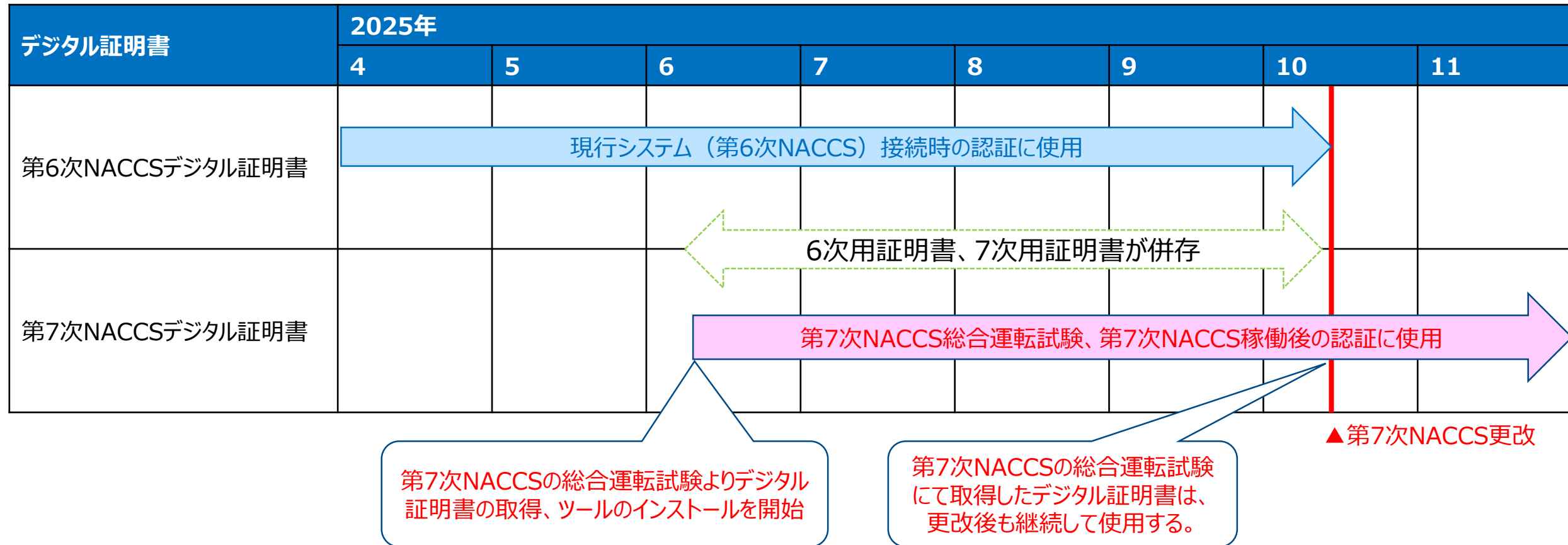
多要素認証方法	検討結果
デジタル証明書	現行システムにて提供しているnetNACCS、WebNACCSへの対応に加え、第7次NACCSで新たに対応するモバイル対応、インターネット経由の自社システム接続（netAPI）にも対応が可能であり、実績のある認証方法である。

第7次NACCSにおいてもデジタル証明書を採用するにあたり、各課題について、以下の対策を講じることといたします。

No.	課題	対策
1	インストール・更新作業が煩雑で、手間がかかる。	「1年ごとの更新」の期間を見直し、 デジタル証明書の有効期限を発行日から5年とする 。これにより、更新の頻度を少なくし、NACCS利用における利用者様のご負担の軽減を図る。
2	1年ごとの更新に手間がかかる。	
3	スマートフォンにインストールできず、スマートフォンからのWebNACCS利用ができない。	Windows OS以外にiOSやAndroid OSへのインストールを可能にし、スマートフォンからの利用を可能とする。
4	Windows OSにしかインストールできない。	
5	システム管理者権限でなければインストールできない。	PCでの利用においては、一般の権限によるツールのインストールを可能とする。システム管理者権限を不要とすることで、システム管理者でなければツールのインストールができないという不便さを解消する。
6	再発行の際に1営業日かかる。	即時の再発行を可能とする。（土、日、祝も可能とする）

2. 第7次NACCS用デジタル証明書の取得及びツールインストールについて

第7次NACCS更改に伴い、新たに第7次NACCS用デジタル証明書の取得、ツールのインストールが必要となります。デジタル証明書の取得は、以下のスケジュールを想定しております。詳細については今後の説明会等でご案内いたします。



- 現在のデジタル証明書は、認証コード1、2の2つのコードで取得していただいておりますが、第7次NACCS用デジタル証明書では、認証コード1、2、3の3つのコードで取得していただくこととなります。
なお、第7次NACCS用デジタル証明書の認証コードについては、総合運転試験の開始までにNSSにてご確認いただくことを想定しております。
- 第7次NACCS用デジタル証明書の認証コード3は、デジタル証明書が再発行されると変更されます。
- デジタル証明書の有効期限について、現在はお客様側で取得した日から3年※1ですが、第7次NACCS用デジタル証明書では、NACCSセンターでの発行日（お客様側で取得可能となったタイミング）から5年間の有効期限となります。
（再発行の際も同様です。）
- 第7次NACCS用デジタル証明書は、発行日以降一定期間取得が行われない場合、再発行申請が必要となります。
（現行のデジタル証明書と同様です。）
- 第7次NACCSのデジタル証明書の取得に際しては、新たに追加で契約する必要は無く、現在契約している論理端末名に紐づく同じ認証コードを用いて取得が可能です。

取得方法やスケジュール等の詳細な情報は、今後の説明会等で順次ご案内いたします。
お客様へはお手数をお掛けしますが、ご協力の程、よろしく願いいたします。

※1…2023年8月23日以降に新規取得、更新、再発行後の取得したデジタル証明書は、第6次NACCS稼働中は有効となるよう変更になりました。