デジタル証明書の見直し

2019年9月12日

輸出入・港湾関連情報処理センター株式会社

1．デジタル証明書の見直し

netNACCS、WebNACCSにて利用しているデジタル証明書以外の認証方法について、多要素認証を考慮した検討を行う。

区　分	概　　要	備　考
1．個別検討事項	デジタル証明書の見直し	
2．現行仕様	NISCの政府機関の情報セキュリティ対策のための統一技術基準に準拠しており、netNACCS、WebNACCSの利用の際デジタル証明書を取得し、利用者ID/パスワードと組み合わせた多要素認証を行っている。	
3．見直しの経緯 （利用者の要望等）	①デジタル証明書に関する煩雑な取得・更新作業や頻繁な問合せ対応が、利用者およびNACCSセンターの負担となっている。 ②iOSおよびAndroid端末でのデジタル証明書の取得が困難なため、モバイル端末での利用ができない。	
4．次期仕様	①デジタル証明書利用時の課題を解決する認証方法を検討する。 ②モバイル端末での多要素認証方法について検討を行う。	
5．その他	今回は現状の課題の把握のみとし、次期仕様については、今後詳細検討の場にて提示する。	

一般的に言われる多要素認証の必要性

- ✓ 「なりすまし」や「不正ログイン」等のセキュリティ上の脅威が年々増加している。
- ✓ 上記のような脅威を防ぐために採用される対策のひとつとして、「多要素認証」が推奨されている。
  （ID、パスワードのみではセキュリティ対策が弱い時代となっている。）
- ✓ 扱う情報やシステムの役割が重要な程、セキュリティ対策を重視する必要がある。

NACCSとは

- ✓ 日本の貿易手続きを支えるミッションクリティカルシステム。
  （NACCSが停止すると、日本の輸出入が停止する可能性もある。）
- ✓ 民間企業、行政機関等の様々な利用者が接続する共通プラットフォーム。
- ✓ 安定性・信頼性を最重視するシステム。

NACCSは、様々な利用者が接続し、日本の貿易手続きを支える公共的インフラであることから、セキュリティ対策は重要。

NACCSは、多要素認証が必要なシステムと考える。

デジタル証明書利用に係る主な課題を以下に整理する。

No	課題	内容
1	取得作業の煩雑さ	デジタル証明書（インストールツール含む）を取得するための作業が煩雑である。センター側でも取得に係る問合せ対応に時間を要し、毎月250件程度の問合せがある。
2	有効期限	証明書に１年間の有効期限があり、更新作業を要する。
3	端末入替時作業の煩雑さ	端末入替時にセンターに再発行処理等の手続きが必要となり、原則最低１営業日を要する。
4	モバイル端末への対応	iOSおよびAndroid端末ではデジタル証明書の取得ができず、モバイル端末でのNACCS利用ができない。

デジタル証明書利用時の課題を解決する認証方法を検討する。

モバイル端末での多要素認証方法について検討する。