

Ⅲ 第6次NACCSにおけるセキュリティ対策

平成27年1月15日

輸出入・港湾関連情報処理センター株式会社



1. 第6次NACCSにおけるセキュリティ対策

- 第6次NACCSにおいては、現行システムで実施しているセキュリティ対策を踏襲しつつ、セキュリティの一層の強化を図る。

※政府が定めるセキュリティ基準（統一技術基準）に準拠。

- 本資料では、第6次NACCSで実施するセキュリティ対策のうち、ご利用者様に影響する部分についてのみ説明する。

項目	現行システム	次期システム
パスワードの最小文字数	特に制限していない	6文字以上8文字以下とする。
パスワードに含める文字種	特に制限していない	半角英大文字と半角数字を、それぞれ必ず1文字以上含める。
パスワードの履歴管理	特に世代管理を行っていない	3世代管理し、パスワード変更時において3世代前までのパスワードは使用不可とする。
パスワード変更機能	UR Y業務を使用する	現行システムと同様とする。
パスワードのキャッシュ不可	特に制御していない	Web NACCSにおいてブラウザのパスワードキャッシュ機能を不可とする。
前回ログイン情報の通知	特に通知していない	NACCSパッケージソフト及びWeb NACCS使用時において前回ログイン時の情報を表示する。
システム利用に関する規約等の提示	NACCS掲示板にて提示	NACCS掲示板での提示に加え、Web NACCSのログインページから規約等の表示ページに移動できるようにする。
緊急時における特定利用者のシステムの利用制限	NACCSセンターにて制限可能	現行システムと同様とする。

netNACCS及びWebNACCSにおいては、インターネットを使用してNACCSにアクセスするため、前頁に示した対策に加え、以下のセキュリティ対策を実施する。

1. SSL (Secure Socket Layer) による通信の暗号化 (盗聴・改ざん防止)
2. クライアントデジタル証明書による端末の特定 (正規端末以外からの利用制限)

なお、WebNACCSは携帯端末からも利用可能であるが、携帯端末からの利用においても上記と同様の対策を実施する。

※ WebNACCS (APS業務) におけるセキュリティ対策については別途提示する。