

■ 情報セキュリティガイド（システム利用者編） ■

本システムで取り扱う情報は 入国者等の機微情報です！

遵守しない場合、情報流出等のきっかけになり得る事項をまとめました。
是非、ご一読いただき、適切な情報管理をお願いします。

1 ID・パスワードの管理は厳密に

- ◇ 推測されにくいパスワードを設定する。
- ◇ 個人パスワードを使い回しさない（本システム専用とする）。
業務終了、離席・帰宅時はサインアウト（ログアウト）する。
- ◇ 本システムの利用端末には、ID・パスワードを保存しない。
- ◇ ID・パスワードを委託契約を締結した委託業者以外の他者に教えない。

2 ウィルス対策ソフトを適切に

- ◇ ウィルス対策ソフトを導入し、パターンファイル等を自動更新し、適切に運用する。

3 OS、ソフトウェアを最新に

- ◇ OS、ソフトウェアについて、最新のセキュリティ対策パッチを適用（インストール）する。

4 盗み見防止へ配慮

- ◇ 離席時や手元から離す場合は端末をロックする。
- ◇ ID やパスワードの入力時は手元を見られないようにする。

- ◇ 盗み見の恐れがある場合は、覗き見防止フィルタ付ける。

5 情報・端末の利用は適切に

- ◇ 業務遂行の目的以外で情報及びシステムを利用しない。
- ◇ 端末、USB メモリ、CD-R 等に個人情報等を保存しない。
端末を第三者へ貸与しない。
- ◇ 端末に安全性の確認できないアプリケーションをインストール、利用しない。
- ◇ 端末を安全性の確認できないネットワーク（無料の Wi-Fi 等）に接続して、システムを利用しない。

6 移動時のシステム利用は不可

- ◇ 公共交通機関等での移動時はシステムを利用しない。

7 外出時に盗難防止

- ◇ 外出時の置き忘れ、盗難に注意する。
- ◇ 網棚等には置かない。駐車中の車中も不可。

8 ウイルス感染が疑われたら

- ◇ 端末をネットワークから切り離し（LAN線を抜く、無線 LAN を切断する等）、すぐにシステム管理者等に連絡を。

情報漏えい・改ざん、システム障害などが起こったり、
起こりそうだと感じたら、すぐにシステム管理者等へ連絡を！