感染症サーベイランスシステム利用者の皆さま

厚生労働省
Ministry of Health, Labour and Welfare

# 情報セキュリティガイド

**このシステムは「感染症者の機微情報」など重要情報を扱うシステムです**

**感染症情報に関連して、WHOや公的機関などを狙ったサイバーセキュリティ事案が懸念されています。情報流出防止のため、このリーフレットの記載事項を遵守し、適切な情報管理を徹底してください。**

## 1．ID・パスワードは厳密に管理しましょう

- 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さない（この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。
- システムの利用端末にID・パスワードを保存しない。
- ID・パスワードを他者に教えない。
- IDの発行、変更、停止、削除の必要がある際は、必ずシステム利用管理者へ事前に申し出て、利用者アカウント変更等の手続きを行う。

## 2．ウイルス対策ソフトを適切に使用しましょう

- ウイルス対策ソフトを導入した上で、パターンファイル等を自動更新し、適切に運用する。
- 業務用のパスワード・メールアドレスを外部サイトで使用しない。
- パスワードは、大文字と小文字、記号と数字を組み合わせるなど推測困難なものに設定する。

## 3．OS、ソフトウェアを最新に保ちましょう

- OS、ソフトウェアは、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．盗み見防止に注意しましょう

- 離席時や、端末を手元から離す場合は、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を付ける。

## 5．情報・端末は適切に利用しましょう

- 業務遂行の目的以外で情報と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。
- USBメモリ接続時にウイルススキャンを実施し、感染が拡大しないようにする。
- 端末を第三者へ貸与しない。
- 端末に管理責任者の許可のない、業務上不要なアプリケーションをインストール、利用しない。
- システム利用時に、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）に接続しない。

## 6．端末を外部で使用する際は 紛失防止を心がけ システム利用を最小限にしましょう

- 外出時にやむを得ず利用する場合は、情報機器の取り扱いに十分注意をする。あわせて、安全性の確認できていない公衆無線LAN は利用しない。
- 公共交通機関等での移動時はシステムを利用しない。
- 持ち出す端末には、必要最小限のアプリケーションのみをインストールする。
- 端末の盗難、紛失時した場合は、すみやかに管理者等に連絡し、指示を仰ぐ。
- 外出時の置き忘れ、盗難に注意する。
- 電車の網棚、駐車中の車の中など紛失・盗難リスクの高い場所には置かない。

## 7．不要情報はすみやかに消去しましょう

- 端末に保存された情報が職務上不要となった場合は、すみやかに情報を消去する。
- 端末を廃棄する場合には、記録媒体内に情報が残留しないよう、全ての情報を復元できないように抹消する。

## 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ケーブルを抜く、無線LANを切断する等）、すぐにシステム管理者等に連絡する。

**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、**
**すぐにシステム利用管理者等へご連絡ください**