不正プログラム対応
実施手順書

作成者	恩納村　総務課
作成日	平成 29 年 11 月 30 日
最終更新日	

目　　次

１．目的

本手順書は、コンピュータウイルスやマルウェア等の不正プログラムによって引き起こされる情報システムの停止やデータの漏えい、破壊などの被害拡大を防止することを目的とする。

２．対象範囲

本手順書は、情報システム管理者及び情報システム担当者等の情報システムに係る職員等を対象とする。

３．実施事項

（１）組織体制

① 情報システム管理者は、情報システムに係る外部委託業者との連絡体制を確立する。

② 情報システム管理者は、コンピュータウイルス等の不正プログラムの感染・侵入時に迅速に対応するために、不正プログラム対応窓口を設置し、職員に周知する。

③ 不正プログラム対応窓口担当者は、コンピュータウイルス等の不正プログラムの感染・侵入時の被害状況を把握し、一次対応を実施する。

（２）不正プログラムに関する情報収集

情報システム管理者は、不正プログラムに関する最新情報を常に収集し、新種のコンピュータウイルス等の不正プログラムの感染・侵入時の復旧方法を事前に整備しておく。

（３）不正プログラムに関する利用者への周知

① 情報システム管理者は、不正プログラム発見時の利用者の処置について、周知する。

② 情報システム管理者は、情報システムに接続されているパソコンの利用者に対し、不正プログラムに関する情報を発信し、利用者の不正プログラムに対する意識向上を図る。

（４）不正プログラム感染・侵入時の対応手順

① 不正プログラム対応窓口担当者は、利用者からの不正プログラムの感染・侵入の連絡を受けたら、利用者に対し、自分自身では処理をしないことを指示し、現場に急行する。

② 不正プログラム対応窓口担当者は、利用者のパソコンを庁内ネットワークか

ら切断する。

③　連絡を受けた利用者のパソコンの不正プログラム対策ソフトウェアのパターンファイル（定義ファイル）が最新のものであるかを確認する。

④　パターンファイル（定義ファイル）が最新であることを確認したのち、対象のパソコンに対し、不正プログラム対策ソフトウェアのフルスキャンを実行し、不正プログラムが検知されるかどうかを確認する。

⑤　不正プログラムが検知された場合は、その不正プログラムの情報を確認する（不正プログラムに関する情報収集で得た情報で確認するか、又は情報システムに係る外部委託業者へ確認する。）。

⑥　検知された不正プログラムによる影響範囲を特定し、復旧対応を実施する。

⑦　不正プログラムの影響範囲が、庁内ネットワーク全体又は外部ネットワークへ拡大している場合は、全てのネットワークを停止し、緊急連絡体制に従い、関係課及び統括情報セキュリティ責任者に連絡し、問題の沈静化を図る。

（５）事後対応手順

①　情報システム管理者は、復旧対応後に、利用者からの不正プログラムの感染・侵入の連絡から復旧対応までの詳細を様式「不正プログラム対応報告書」に記録し、保管する。

②　情報システム管理者は、不正プログラムの感染・侵入の原因を追究し、再発防止策を検討する。

４．例外事項

業務都合により、本手順書の実施事項を守ることができない状況が発生した場合は、統括情報セキュリティ責任者へ報告する。

［改定履歴］

版	更新年月日	改定理由及び内容	承認	審査	担当
1.0 版	平成 29 年 11 月 30 日	新規制定			

＜様式＞

不正プログラム対応報告書

1.　発見者の所属・氏名

所属課名：

氏名：

2. 不正プログラム名称（不明な場合は症状）

3. 発見年月日

4. 使用機種・OS・接続形態

・機種－

・OS－

・ネットワーク－

5. 発見方法

□セキュリティソフトが検知

□目視により発見

□外部からの連絡

□その他（　　）

6. 推定される感染経路

□国内　　□海外　　□不明

□電子メール、□ダウンロードファイル　□外部からの媒体

□その他（　　）

7. 被害状況

□感染前に駆除（またはファイルを削除等）したため被害無し

□PC（　）台、□外部媒体（CD/DVD（　）枚、USBメモリ（　）個、その他（　　）（　）個）

□その他（　　）

8. 回復処理

・回復方法

不正プログラム対策ソフトウェアで駆除または削除

□ファイル（メール）の削除、□初期化

□その他（　　）

・回復に要した人日－（　）人×（　）日（0.5日単位で記述）

9. その他