IT-Professor
コンピューター ウイルス対策基準

2021 年 10 月

IT-Professor(株) IT 部

秘 Confidential

更新履歴

	更新日	更新箇所	更新内容
1	2021/10	初版	

秘 Confidential

1. 趣旨・目的

この実施基準は、IT-Professor（以下、IT-P と称す）グループ情報セキュリティポリシー第 8 章(第 21、22、23 条)の規定に基づき、コンピューターウイルスに対する予防・検知・駆除・復旧等の対策について、必要な基準を定めたものである。

2. 定義

本基準で用いる主な用語の定義は、以下のとおりとする。

1) コンピューターウイルス(以下「ウイルス」とする。)

プログラムやファイルなどに対して破損や削除、通信機器も含むコンピュータ動作の妨害等ユーザーの予期しない、意図的に被害を及ぼすよう作成されたプログラムであり、次の能力を有するものをいう。

- 自己伝染機能
- 潜伏機能
- 発症機能

2) ウイルス対策ソフトウェア

ウイルスの検出や除去、感染予防の機能を含むソフトウェアをいう。

3. 対象

1) 対象となる情報資産

- すべての PC およびサーバー
- 電子化情報を記録した外部媒体ネットワーク(通信回線、通信機器)

4. 役割

次のとおり役割を定義する。

1) IT 部長

- ウイルス感染の防止および万一の感染時に的確に対処するため、管理体制を確立する。
- ウイルス対策内容の決定、IT-P グループ内への対策適用および体制整備、対策状況の把握や改善など、IT-P グループにおけるウイルス対策全般を統括する。

秘 Confidential

2) コンピューターウイルス対策統括担当者

・ IT部長の指示に基づき、IT-Pグループにおけるウイルス対策全般を統括する業務を担う。

3) コンピューターウイルス対応部門責任者

・ 本実施基準で定めたウイルス対策を適切に実施するため、コンピューターウイルス対応責任者を配置し、自部門の管理体制を整備する。

・ 自部門におけるウイルス対策の適用および情報資産に対する対策を管理する。

・ 自部門の管理体制を変更する場合、コンピューターウイルス対策統括担当者へ届出を行う。

4) コンピューターウイルス対応責任者

・ コンピューターウイルス対応部門責任者の指示に基づき、ウイルス対策を管理する。

5) 従業員等

・ コンピューターウイルス対応部門責任者またはコンピューターウイルス対応責任者の指示に従い、情報資産のウイルス対策を実施する。

5. 遵守事項

ウイルス感染による業務への影響等危険性を理解するとともに、ウイルスの侵入・感染および感染時の被害拡大を防止するため、本基準で定めた事項を遵守しなければならない。

1) ウイルス対策ソフトウェアの導入

i すべての PC およびサーバーに常駐型のウイルス対策ソフトウェアを導入すること。

ii ウイルス対策ソフトウェアは、コンピューターウイルス対策統括担当者が指定したソフトウェアを導入することとする。

iii ウイルス対策ソフトウェアには、常時スキャン機能および定義ファイルの自動更新機能を備えていなければならない。

iv ウイルス対策ソフトウェアのバージョンおよび製品パッチ等は、コンピューターウイルス対策統括担当者の指示に基づき、最新の状態に更新すること。

v ウイルス対策ソフトウェアは、ウイルスの侵入・感染および感染時の被害拡大を防止するため、センターでの集中管理とする。

2) ウイルス対策ソフトウェアの利用

i PC およびサーバーに導入したウイルス対策ソフトウェアは、常時スキャンおよび定義ファイルの自動更新の設定を常に有効とし、許可なく設定の変更および機能の停止を行ってはならない。

秘 Confidential

ii 定義ファイルは、日々最新の状態であることを確認すること。

3) 日常のウイルス被害防止対策

i 電子メールおよびインターネットの利用にあたっては、IT-P グループで指定した標準ソフトウェアを利用することとし、許可なく設定を変更してはならない。

ii 送信元不明の電子メールに添付されたファイルや、実行形式のまま添付されたファイルなど、不審な添付ファイルに対しては、ウイルス対策ソフトウェアにて走査し、安全が確認されない限り、不用意な操作を行ってはならない。

iii ファイルを添付して電子メールを送信する場合、ウイルス対策ソフトウェアにて走査し、当該ファイルのウイルス感染が無いことを必ず確認しなければならない。

iv 社外 Web サイトを利用する際は、信頼できるサイトのみの参照に限定し、出所不明なデータおよびプログラムのダウンロードおよびプログラムの実行を行ってはならない。

4) ウイルスに関する情報提供

IT 部は、ウイルスに関する情報を収集し、IT-P グループに向けて適宜情報提供を行う。

5) ウイルス対策ソフトウェアにてウイルスを検知した場合

i ウイルス対策ソフトウェアの駆除機能を使用してウイルスを駆除しなければならない。

ii ウイルスの検知または駆除結果に関しては、体制および連絡ルートに従い、コンピューターウイルス対策統括担当者に報告しなければならない。

6) ウイルス侵入・感染時の対応

i ウイルス侵入および感染の兆候と思われる症状を発見した場合には、直ちに LAN などのネットワークケーブルを外し、PC や情報システムの利用を中止しなければならない。また、体制および連絡ルートに従い、コンピューターウイルス対策統括担当者に報告を行い、指示に従わなければならない。

【ウイルス侵入・感染の兆候と思われる事象の例】

- PC または情報システムが使用中に突然停止するなど動作しなくなった。
- ファイルが無くなる。または、見知らぬファイルが作成されていた。
- 送信した覚えのないメール送信が行われていた。
- Word や Excel 等利用時に、不審なダイアログメッセージの表示や、文書内容が勝手に変更された。

ii ウイルス対策ソフトウェアの定義ファイルバージョンおよび最終更新日を確認し、最新でない場合、更新を行うこと。また、当該 PC またはサーバーに対してウイルス対策ソフトウェアにて走査し、ウイルスが検知されるか確認を行わなければならない。

iii ウイルスが検知された場合は、ウイルス対策ソフトウェアの駆除機能を使用して駆除しなければならない。また、検知されなかった場合は、コンピューターウイルス対策統括担当者の指示に基づ

秘 Confidential

き、ログ情報や環境の確認を行うなど指示に従わなければならない。

iv コンピューターウイルス対応部門責任者およびコンピューターウイルス対応責任者は、ウイルスまたはウイルスと思われる症状を発見した場合、遅滞なく、コンピューターウイルス対策統括担当者へ報告し、指示に従わなければならない。

v コンピューターウイルス対策統括担当者は、報告内容および被害状況を確認し、各部門等へ対策を指示しなければならない。

vi センターでの集中管理機能等にて、コンピューターウイルス対策統括担当者がウイルスの侵入もしくは感染の兆候を発見し、対策を指示する場合、従業員等はその指示に従わなければならない。

7) 情報システムに対するウイルス対策

部門長等またはコンピューターウイルス対応部門責任者は、情報システムの開発または運用管理において、次のとおり対策を講じること。

i ウイルス感染の防止および万一の感染時に的確に対処するため、管理対象を明確にし、管理体制を確立すること。

ii PC およびサーバーに導入するすべてのソフトウェアは、機能修正および脆弱性対応が最新の状態で適用すること。

iii 導入したソフトウェアに関する製品サポート情報、脆弱性に関する情報を適宜入手すること。また、特段の理由がない限り、最新の状態を維持しなければならない。

iv ウイルス感染を防止するため、オリジナルプログラムは、ライトプロテクト措置(書き込み禁止)を行うこと。また、万一の被害に備え、バックアップの確保等安全な方法で保管すること。

v ウイルス感染を防止するため、情報システムに導入するソフトウェア、データ等は、ウイルス対策ソフトウェアを最新の状態に維持し、常時スキャンを有効とすること。

vi 情報システムがウイルス感染した場合、システムの使用を中止し、ウイルス対策統括担当者に遅滞なく報告するとともに、利用者に対し速やかに利用中止の通知を行うこと。

(報告内容)

発生日時、場所、資産管理番号、ウイルス対策ソフトウェアの製品名・バージョン・定義ファイルバージョン等、発生事象、検知時の操作内容など

vii 万一の感染時に備え、安全な復旧手順を確立して、システムの復旧作業にあたること。

viii ウイルス被害の再発を防止するため、原因を分析し、再発防止対策を講じること。

ix ウイルス被害の拡大および再発を防止するため、必要な情報をウイルス対策統括担当者に届け出ること。

x 情報システムの利用ユーザーに対し、ウイルス対策やその他情報セキュリティ対策について、適宜啓発・教育を行うこと。

8) 緊急時における IT 理部長の権限

ウイルス感染等により緊急の対応が必要となる場合には、被害状況に応じて IT 部長の判断によ

秘 Confidential

り、ネットワークの遮断やシステム停止等の措置を講じる。

(判断基準例)

・ 複数事業所で同時に同一ウイルスに感染または同一ネットワーク上で多数の PC 等にウイルス感染が確認され、即座に駆除されなかった場合

・ 情報システムがウイルス感染し、即座に駆除されなかった場合

・ IT-P グループ外部からの不正アクセスまたは攻撃を検知した場合

・ IT-P グループ内部から社内または外部に向け、異常な数のアクセス行為を検知した場合

6. 例外事項

法令または別途定められた規程等により特別の定めがある場合には、責任体制に基づき適切に判断し処理しなければならない。

7. 公開の範囲

本基準は、「社外秘」とし、IT-P グループの従業員等を対象に公開する

8. 改廃

本基準は、定期的に見直しを行うこととし、IT 部にて適宜改定を行うこととする。

また、改定が必要と判断された場合は、速やかに変更を行い、責任体制(情報セキュリティ管理体制)を通じ、その内容をすべての従業員等に周知することとする。

改附則

本基準は、2021 年 10 月 1 日より適用とする。

秘 Confidential