

コンピュータウイルス対策基準

平成7年7月7日(通商産業省告示第429号)(制定)
平成9年9月24日(通商産業省告示第535号)(改定)
平成12年12月28日(通商産業省告示第952号)(最終改定)

コンピュータウイルス対策基準を次のように定め、平成7年7月1日から施行する。
なお、平成2年通商産業省告示第139号は、平成7年6月30日限り廃止する。

1. 主旨

本基準は、コンピュータウイルスに対する予防、発見、駆除、復旧等について実効性の高い対策をとりまとめたものである。

2. 用語の定義

本基準に用いられる主な用語の定義は、以下のとおりである。

(1) コンピュータウイルス(以下「ウイルス」とする。)

第三者のプログラムやデータベースに対して意図的に何らかの被害を及ぼすように作られたプログラムであり、次の機能を一つ以上有するもの。

(1)自己伝染機能

自らの機能によって他のプログラムに自らをコピーし又はシステム機能を利用して自らを他のシステムにコピーすることにより、他のシステムに伝染する機能

(2)潜伏機能

発病するための特定時刻、一定時間、処理回数等の条件を記憶させて、発病するまで症状を出さない機能

(3)発病機能

プログラム、データ等のファイルの破壊を行ったり、設計者の意図しない動作をする等の機能

(2)ソフトウェア

システムプログラム、アプリケーションプログラム、ユーティリティプログラム等のプログラム

(3)システム

ハードウェア、ソフトウェア若しくはネットワーク又はこれらの複合体

(4)ワクチン

ウイルスの検査、予防又は修復のいずれかの機能を含むソフトウェア

(5)バックアップ

プログラム、データ等と同一の内容を別の媒体に記録すること。

(6)ファイル

記憶装置又は記録媒体上に、電子的又は光学的に記録されているプログラム、データ等

(7)保守機能

システムを正常な状態に維持するための機能

(8)セキュリティ機能

プログラム、データ等の機密性、保全性及び可用性を確保するための機能

3. 構成

本基準は、システムユーザ基準、システム管理者基準、ソフトウェア供給者基準、ネットワーク事業者基準及びシステムサービス事業者基準から成り、その構成及び内容は、以下のとおりである。

(1)システムユーザ基準(18項目)

システムを利用する者(以下「システムユーザ」とする。)のための対策をまとめたもの。

(1)ソフトウェア管理(2項目)

システムユーザが導入するソフトウェアに対する対策についてまとめたもの。

(2)運用管理(12項目)

システムユーザがシステムを利用する上での対策についてまとめたもの。

(3)事後対応(3項目)

システムユーザがウイルスを発見した場合の対策についてまとめたもの。

(4)監査(1項目)

ウイルス対策が適切に実施されていることを監査する項目についてまとめたもの。

(2)システム管理者基準(31項目)

システムを導入、維持及び管理する者(以下「システム管理者」とする。)のための対策についてまとめたもの。

(1)コンピュータ管理(8項目)

システム管理者がハードウェア及びソフトウェアを導入及び更新する場合の対策についてまとめたもの。

(2)ネットワーク管理(5項目)

システム管理者がネットワークを導入及び更新する上での対策についてまとめたもの。

(3)運用管理(9項目)

システム管理者がシステムを維持及び管理する上での対策についてまとめたもの。

(4)事後対応(6項目)

システム管理者がウイルスを発見した場合及びシステムユーザから発見の連絡を受けた場合の対策についてまとめたもの。

(5)教育・啓蒙(2項目)

システム管理者及びシステムユーザに対して行うウイルス対策の教育・啓蒙についてまとめたもの。

(6)監査(1項目)

ウイルス対策が適切に実施されていることを監査する項目についてまとめたもの。

(3)ソフトウェア供給者基準(21項目)

ソフトウェアの開発並びにソフトウェア製品の開発、製造及び出荷を行う者(以下「ソフトウェア供給者」とする。)のための対策をまとめたもの。

(1)開発管理(9項目)

ソフトウェア及びソフトウェア製品の開発並びに開発環境の導入、更新及び管理に関する対策についてまとめたもの。

(2)製品管理(3項目)

ソフトウェア製品の製造及び出荷をする場合の対策についてまとめたもの。

(3)事後対応(7項目)

ソフトウェア供給者がウイルスを発見した場合及び製品のユーザから発見の連絡を受けた場合の対策についてまとめたもの。

(4)教育・啓蒙(1項目)

ソフトウェア供給者に対して行うウイルス対策の教育・啓蒙についてまとめたもの。

(5)監査(1項目)

ウイルス対策が適切に実施されていることを監査する項目についてまとめたもの。

(4) ネットワーク事業者基準(15項目)

パソコン通信等のネットワークを介して情報を提供する事業者(以下「ネットワーク事業者」とする。)のための対策をまとめたもの。

(1) システム管理(2項目)

ネットワーク事業に用いるシステムを導入及び更新する上での対策についてまとめたもの。

(2) 運用管理(4項目)

ネットワーク事業に用いるシステムを維持及び管理する上での対策についてまとめたもの。

(3) 事後対応(6項目)

ネットワーク事業者がウイルスを発見した場合及びネットワークのユーザから発見の連絡を受けた場合の対策についてまとめたもの。

(4) 教育・啓蒙(2項目)

ネットワーク事業者及びネットワークのユーザに対して行うウイルス対策の教育・啓蒙についてまとめたもの。

(5) 監査(1項目)

ウイルス対策が適切に実施されていることを監査する項目についてまとめたもの。

(5) システムサービス事業者基準(19項目)

システムの管理、保守、レンタル等のサービスを行う事業者(以下「システムサービス事業者」とする。)のための対策をまとめたもの。

(1) システム管理(5項目)

サービスに用いるシステムを導入及び更新する上での対策についてまとめたもの。

(2) 運用管理(6項目)

サービスに用いるシステムを維持及び管理する上での対策についてまとめたもの。

(3) 事後対応(6項目)

システムサービス事業者がウイルスを発見した場合及びサービスを受けているユーザから発見の連絡を受けた場合の対策についてまとめたもの。

(4) 教育・啓蒙(1項目)

システムサービス事業者に対して行うウイルス対策の教育・啓蒙についてまとめたもの。

(5) 監査(1項目)

ウイルス対策が適切に実施されていることを監査する項目についてまとめたもの。

4. システムユーザ基準

a. ソフトウェア管理

(1) ソフトウェアは、販売者又は配布責任者の連絡先及び更新情報が明確なものを入手すること。

(2) オリジナルプログラムは、ライトプロテクト措置、バックアップの確保等の安全な方法で保管すること。

b. 運用管理

(1) 外部より入手したファイル及び共用するファイル媒体は、ウイルス検査後に利用すること。

(2) ウイルス感染の被害が最小となるよう、システムの利用は、いったん初期状態にしてから行うこと。

(3) ウイルス感染を早期に発見するため、システムの動作の変化に注意すること。

(4) ウイルス感染を早期に発見するため、最新のワクチンの利用等により定期的にウイルス検査を行うこと。

(5) 不正アクセスによるウイルス被害を防止するため、パスワードは容易に推測されないよう

に設定し、その秘密を保つこと。

(6)不正アクセスによるウイルス被害を防止するため、パスワードは随時変更すること。

(7)不正アクセスによるウイルス被害を防止するため、システムのユーザIDを共用しないこと。

(8)不正アクセスによるウイルス被害を防止するため、アクセス履歴を確認すること。

(9)不正アクセスによるウイルス被害を防止するため、機密情報を格納しているファイルを厳重に管理すること。

(10)システムを悪用されないため、入力待ちの状態では放置しないこと。

(11)ウイルス感染を防止するため、出所不明のソフトウェアは利用しないこと。

(12)ウイルスの被害に備えるため、ファイルのバックアップを定期的に行い、一定期間保管すること。

c. 事後対応

(1)ウイルスに感染した場合は、感染したシステムの使用を中止し、システム管理者に連絡して、指示に従うこと。

(2)ウイルス被害の拡大を防止するため、システムの復旧は、システム管理者の指示に従うこと。

(3)ウイルス被害の拡大を防止するため、感染したプログラムを含むフロッピー ディスク等は破棄すること。

d. 監査

(1)ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。

5. システム管理者基準

a. コンピュータ管理

(1)ウイルス対策を円滑に行うため、コンピュータの管理体制を明確にすること。

(2)ウイルス感染を防止するため、機器を導入する場合は、ウイルス検査を行うこと。

(3)ウイルス感染を防止するため、コンピュータにソフトウェアを導入する場合は、ウイルス検査を行うこと。

(4)ウイルス被害に備えるため、システムにインストールした全ソフトウェアの構成情報を保存すること。

(5)オリジナルプログラムは、ライトプロテクト措置、バックアップの確保等の安全な方法で保管すること。

(6)不正アクセスによるウイルス被害を防止するため、システムのユーザ数及びユーザのアクセス権限を必要最小限に設定すること。

(7)ウイルス被害を防止するため、共用プログラムが格納されているディレクトリに対するシステムのユーザの書き込みを禁止すること。

(8)ウイルス被害を防止するため、システム運営に必要なのないプログラムは削除すること。

b. ネットワーク管理

- (1) ウイルス対策を円滑に行うため、ネットワークの管理体制を明確にすること。
- (2) ウイルスに感染した場合の被害範囲を特定するため、ネットワーク接続機器の設置状況をあらかじめ記録し、管理すること。
- (3) ウイルス被害に備えるため、緊急時の連絡体制を定め、周知・徹底すること。
- (4) 不正アクセスによるウイルス被害を防止するため、ネットワーク管理情報のセキュリティを確保すること。
- (5) 不正アクセスによるウイルス被害を防止するため、外部ネットワークと接続する機器のセキュリティを確保すること。

c. 運用管理

- (1) システムの重要情報の管理体制を明確にすること。
- (2) 不正アクセスからシステムの重要情報を保護するため、システムが有するセキュリティ機能を活用すること。
- (3) パスワードを容易に推測されないようにするため、安易なパスワード設定を排除すること。
- (4) ウイルスの被害に備えるため、運用システムのバックアップを定期的に行い、一定期間保管すること。
- (5) ウイルス被害を防止するため、匿名で利用できるサービスは限定すること。
- (6) 不正アクセスを発見するため、アクセス履歴を定期的に分析すること。
- (7) ウイルス感染を早期に発見するため、システムの動作を監視すること。
- (8) ウイルス感染を早期に発見するため、最新のワクチンの利用等により定期的にウイルス検査を行うこと。
- (9) システムの異常が発見された場合は、速やかに原因を究明すること。

d. 事後対応

- (1) ウイルス感染の拡大を防止するため、感染したシステムの使用を中止すること。
- (2) ウイルス感染の拡大を防止するため、必要な情報をシステムユーザに、速やかに通知すること。
- (3) ウイルス被害の状況を把握するため、ウイルスの種類及び感染範囲の解明に努めること。
- (4) 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。
- (5) ウイルス被害の再発を防止するため、原因を分析し、再発防止対策を講ずること。
- (6) ウイルス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。

e. 教育・啓蒙

- (1) ウイルス対策のレベルアップを図るため、ウイルス関連情報を収集して周知・徹底すること。
- (2) セキュリティ対策及びウイルス対策について、システムユーザの教育・啓蒙を行うこと。

f. 監査

- (1) ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。
-

6. ソフトウェア供給者基準

a. 開発管理

- (1) 開発ツールからウイルスが開発システムに感染するのを防ぐため、開発ツールの管理体制を明確にすること。
- (2) パスワードの漏えいを防ぐため、パスワードを厳重に管理すること。
- (3) 不正利用によるウイルス被害を防止するため、開発システムを厳重に管理すること。
- (4) 不正アクセスによるウイルス被害を防止するため、ネットワーク等を利用した開発システムへのアクセスに対しては、セキュリティを強化すること。
- (5) 不正アクセスによるウイルス被害を防止するため、開発者のアクセス権限を必要最小限に設定すること。
- (6) 開発段階のプログラムに対して開発者、修正者及び責任者を明確にし、厳重に管理すること。
- (7) ウイルス被害に備えるため、開発段階のプログラムのバックアップを行い保存すること。
- (8) 不正利用を防止するため、開発終了時にプログラム内のデバッグ機能を確実に取り除くこと。
- (9) ウイルス感染を早期に発見するため、最新のワクチンの利用等により定期的にウイルス検査を行うこと。

b. 製品管理

- (1) 製品の製造段階でのウイルス感染を防止するため、専用のシステム又は機器を用いて複製を行うこと。
- (2) ウイルス感染を防止するため、製品の原本は、厳重に管理すること。
- (3) 製品の流通段階でのウイルス感染を防止するため、ライトプロテクト、密封包装等の対策を施すこと。

c. 事後対応

- (1) 製品のウイルス感染を発見した場合は、流通を停止し、製品のユーザに情報を通知するとともに製品の回収を行うこと。
- (2) ウイルス感染の拡大を防止するため、感染した開発システムの使用を中止すること。
- (3) ウイルス感染の拡大を防止するため、必要な情報を関連する全てのソフトウェア供給者に、速やかに通知すること。
- (4) ウイルス被害の状況を把握するため、ウイルスの種類及び感染範囲の解明に努めること。
- (5) 安全な復旧手順を確立して、開発システムの復旧作業にあたること。
- (6) ウイルス被害の再発を防止するため、原因を分析し、再発防止対策を講ずること。
- (7) ウイルス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。

d. 教育・啓蒙

- (1) ウイルス対策のレベルアップを図るため、ウイルス関連情報を収集して周知・徹底すること。

e. 監査

- (1) ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。
-

7. ネットワーク事業者基準

a. システム管理

(1) ウイルスに感染した場合の被害範囲を特定するため、ネットワーク事業に用いるシステムの設定状況をあらかじめ記録し、管理すること。

(2) ウイルス被害に備えるため、緊急時の連絡体制を定め、周知・徹底すること。

b. 運用管理

(1) 不正アクセスによるウイルス被害を防止するため、ネットワークのユーザのアクセス権限を必要最小限に設定すること。

(2) ウイルス被害を防止するため、ファイルを公開する前に、最新のワクチンの利用等によりウイルス検査を行うこと。

(3) 不正アクセスによるウイルス被害を防止するため、パスワード等のネットワーク管理情報を厳重に管理すること。

(4) ウイルス被害に備えるため、利用状況の履歴を常に記録し、一定期間保存すること。

c. 事後対応

(1) ウイルス被害の拡大を防止するため、ウイルスを含むファイルの公開を停止すること。

(2) ウイルス感染の拡大を防止するため、必要な情報をネットワークのユーザ及び他のネットワーク事業者へ、速やかに通知すること。

(3) ウイルス被害の状況を把握するため、ウイルスの種類及び感染範囲の解明に努めること。

(4) 安全な復旧手順を確立して、その情報をネットワークのユーザに通知すること。

(5) ウイルス被害の再発を防止するため、原因を分析し、再発防止対策を講ずること。

(6) ウイルス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。

d. 教育・啓蒙

(1) ウイルス対策のレベルアップを図るため、ウイルス関連情報を収集して周知・徹底すること。

(2) セキュリティ対策及びウイルス対策について、ネットワークのユーザの教育・啓蒙を行うこと。

e. 監査

(1) ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。

8. システムサービス事業者基準

a. システム管理

- (1)ソフトウェアは、販売者又は配布責任者の連絡先及び更新情報が明確なものを入手すること。
- (2)不正利用を防止するため、保守機能を含むソフトウェア及びその情報は厳重に管理すること。
- (3)オリジナルプログラムは、ライトプロテクト措置、バックアップの確保等の安全な方法で保管すること。
- (4)サービスに用いるディスクは、初期化したディスクを用いて、オリジナルプログラムから作成すること。
- (5)ウイルス被害に備えるため、サービスに用いるディスクの構成情報を保存すること。

b. 運用管理

- (1)ウイルス被害に備えるため、サービスに用いるシステムの管理体制を明確にすること。
- (2)ウイルス感染を防止するため、サービスに用いるシステムは、最新のワクチンの利用等により事前にウイルス検査を行うこと。
- (3)ウイルス被害に備えるため、ウイルス検査履歴等を一定期間保管すること。
- (4)ウイルス感染を防止するため、一度サービスに用いたシステムは、続けて他のサービスに利用しないこと。
- (5)ウイルス被害を防止するため、サービスに必要としない機器は切り離すこと。
- (6)サービスに用いるディスクへのウイルス感染を防止するため、ライトプロテクト措置を行うこと。

c. 事後対応

- (1)ウイルス感染の拡大を防止するため、サービスに用いている感染したシステムの使用を中止すること。
- (2)ウイルス感染の拡大を防止するため、必要な情報をサービスを受けているユーザに、速やかに通知すること。
- (3)ウイルス被害の状況を把握するため、ウイルスの種類及び感染範囲の解明に努めること。
- (4)安全な復旧手順を確立して、サービスに用いているシステムの復旧作業にあたること。
- (5)ウイルス被害の再発を防止するため、原因を分析し、再発防止対策を講ずること。
- (6)ウイルス被害の拡大及び再発を防止するため、必要な情報を経済産業大臣が別に指定する者に届け出ること。

d. 教育・啓蒙

- (1)ウイルス対策のレベルアップを図るため、ウイルス関連情報を収集して周知・徹底すること。

e. 監査

- (1)ウイルス対策の実効性を高めるため、ウイルス対策についてのシステム監査の報告を受け、必要な対策を講ずること。

9. 留意事項

- (1)本基準は、コンピュータの種類、システムの形態又はソフトウェアの相違等の実態に則して活用すること。
- (2)ソフトウェア供給者基準、ネットワーク事業者基準及びシステムサービス事業者基準は、各事業者特有の観点からまとめた基準であることから、各事業に用いるシステムの導入に当たっては、システム管理者基準を活用すること。
- (3)システム自体の安全対策については、「情報システム安全対策基準」(平成7年通商産業省告示第518号)を活用すること。

(4)システム監査の実施については、「システム監査基準」(平成8年1月30日通産省広報)を活用すること。

(5)本基準は、原則として、企業等の組織を対象としているが、個人ユーザも活用することができる。

(6)コンピュータ不正アクセス対策については、「コンピュータ不正アクセス対策基準」(平成8年通商産業省告示第362号)を活用すること。

(7)コンピュータウイルス、不正アクセス、災害等の対策としては、警察庁からも「情報システム安全対策指針」(平成9年国家公安委員会告示第9号)が発表されており、本基準と併せて活用することにより、情報システムのセキュリティを高めることができる。

○通商産業省告示第139号 平成2年4月10日 コンピュータウイルス基準制定

○通商産業省告示第429号 平成7年7月7日 コンピュータウイルス基準改訂

○通商産業省告示第535号 平成9年9月24日 コンピュータウイルス基準改訂

[経済産業省告示第2号]

平成7年通商産業省告示第429号(コンピュータウイルス対策基準を定める件)に基づき、経済産業大臣が別に指定する者を次のように定める。

なお、平成12年通商産業省告示第951号(コンピュータウイルス対策基準に基づく経済産業省大臣が別に指定する者)は廃止する。

平成16年1月5日 経済産業大臣 中川 昭一

1. 名称 独立行政法人情報処理推進機構
2. 主たる所在地 東京都文京区本駒込二丁目二十八番八号