コンピュータ不正アクセス対策基準

平成8年8月8日（通商産業省告示第３６２号）（制定）
平成9年9月２４日（通商産業省告示第５３４号）（改定）
平成１２年１２月２８日（通商産業省告示第９５０号）（最終改定）

コンピュータ不正アクセス対策基準を次のように定め、平成8年8月8日から施行する。

Ⅰ. 主旨

本基準は、コンピュータ不正アクセスによる被害の予防、発見及び復旧並びに拡大及び再発防止について、企業等の組織及び個人が実行すべき対策をとりまとめたものである。

Ⅱ. 用語の定義

本基準で用いられる用語の定義は、以下のとおりである。

1．コンピュータ不正アクセス（以下「不正アクセス」とする。）

システムを利用する者が、その者に与えられた権限によって許された行為以外の行為をネットワークを介して意図的に行うこと。

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及びそれに付随するデータ

3．コンピュータ

ネットワークに接続され得るコンピュータであり、ルータ、交換機等の通信用コンピュータ及びその他専用コンピュータを含むもの。

4．ネットワーク

通信回線及び通信機器の複合体

5．システム

コンピュータ及びネットワークの複合体

6．ファイル

記憶装置又は記録媒体上に記録されているプログラム、データ等

7．機器

ハードウェア、通信回線又は通信機器

8．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。

9．保守機能

システムを正常な状態に維持するための機能

III．構成

本基準は、システムユーザ基準、システム管理者基準、ネットワークサービス事業者基準及びハードウェア・ソフトウェア供給者基準からなり、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

システムを利用する者（以下「システムユーザ」とする。）が実施すべき対策についてまとめたもの。

（1）パスワード及びユーザID管理（9項目）

システムユーザ自身が使用するパスワード及びユーザIDを管理する際に実施すべき対策についてまとめたもの。

（2）情報管理（7項目）

システムユーザ自身が利用する情報を管理する際に実施すべき対策についてまとめたもの。

（3）コンピュータ管理（6項目）

システムユーザ自身が利用するコンピュータを利用及び管理する際に実施すべき対策についてまとめたもの。

（4）事後対応（2項目）

システムの異常及び不正アクセスをシステムユーザが発見した場合の対応についてまとめたもの。

（5）教育及び情報収集（2項目）

セキュリティ対策に関する教育及び情報の収集についてまとめたもの。

（6）監査（1項目）

不正アクセス対策を適切に実施するための監査についてまとめたもの。

2．システム管理者基準

システムユーザの管理並びにシステム及びその構成要素の導入、維持、保守等の管理を行う者（以下「システム管理者」とする。）が、実施すべき対策についてまとめたもの。

（1）管理体制の整備（7項目）

システム及びその構成要素を管理するための体制を整備する際に実施すべき対策についてまとめたもの。

(2) システムユーザ管理 (10項目)

システムユーザをシステム管理者が管理する際に実施すべき対策についてまとめたもの。

(3) 情報管理 (8項目)

システム全体の情報をシステム管理者が管理する際に実施すべき対策についてまとめたもの。

(4) 設備管理 (18項目)

ハードウェア、ソフトウェア、通信回線及び通信機器並びにそれらの複合体をシステム管理者が管理する際に実施すべき対策についてまとめたもの。

(5) 履歴管理 (4項目)

システムの動作履歴、使用記録等をシステム管理者が記録、分析及び保存する際に実施すべき対策についてまとめたもの。

(6) 事後対応 (6項目)

システム全体の異常及び不正アクセスをシステム管理者が発見した場合並びにシステムユーザからの発見の連絡を受けた場合の対応についてまとめたもの。

(7) 情報収集及び教育 (4項目)

セキュリティ対策に関する情報の収集及びその活用方法並びにシステムユーザへの教育についてまとめたもの。

(8) 監査 (1項目)

不正アクセス対策を適切に実施するための監査についてまとめたもの。

3．ネットワークサービス事業者基準

ネットワークを利用して、情報サービス及びネットワーク接続サービスを提供する事業者 (以下「ネットワークサービス事業者」とする。) が実施すべき対策についてまとめたもの。

(1) 管理体制の整備 (2項目)

ネットワークサービスを行うための体制を整備する際に実施すべき対策についてまとめたもの。

(2) ネットワークサービスユーザ管理 (7項目)

ネットワークサービスユーザをネットワークサービス事業者が管理する際に実施すべき対策についてまとめたもの。

(3) 情報管理 (3項目)

ネットワークサービスユーザ及び事業者自身の情報を管理する際に実施すべき対策についてまとめたもの。

(4) 設備管理 (5項目)

ネットワークサービスに係る機器をネットワークサービス事業者が管理する際に実施すべき対策についてまとめたもの。

(5) 事後対応 (6項目)

ネットワークサービスに係るシステムの異常及び不正アクセスをネットワークサービス事業者が発見した場合並びに発見の連絡を受けた場合の対応についてまとめたもの。

(6) 情報収集及び教育 (3項目)

セキュリティ対策に関する情報の収集及びその活用方法並びにネットワークサービスユーザへの教育についてまとめたもの。

(7) 監査 (1項目)

不正アクセス対策を適切に実施するための監査についてまとめたもの。

4. ハードウェア・ソフトウェア供給者基準

ハードウェア及びソフトウェア製品の開発、製造、販売等を行う者 (以下「ハードウェア・ソフトウェア供給者」とする。) が、実施すべき対策についてまとめたもの。

(1) 管理体制の整備 (2項目)

ハードウェア及びソフトウェアを供給するための体制について実施すべき対策をまとめたもの。

(2) 設備管理 (2項目)

ハードウェア及びソフトウェア製品の開発及び製造に係る機器をハードウェア・ソフトウェア供給者が管理する際に実施すべき対策についてまとめたもの。

(3) 開発管理 (7項目)

ハードウェア及びソフトウェア製品をハードウェア・ソフトウェア供給者が開発及び製造する際に実施すべき対策についてまとめたもの。

(4) 販売管理 (4項目)

ハードウェア及びソフトウェア製品をハードウェア・ソフトウェア供給者が販売等を行う場合に実施すべき対策についてまとめたもの。

(5) 事後対応 (6項目)

開発システムの異常及び不正アクセスをハードウェア・ソフトウェア供給者が発見した場合の対応についてまとめたもの。

(6) 情報収集及び教育 (2項目)

セキュリティ対策に関する情報の収集及びその活用方法並びに製品のユーザに対する教育についてまとめたもの。

(7) 監査 (1項目)

不正アクセス対策を適切に実施するための監査についてまとめたもの。

Ⅳ. 個人ユーザが留意する点

本基準は企業等の組織及び個人を対象としているが、構成の便宜上、組織を対象とした記述となっているため、個人ユーザは以下の項目について留意することにより、不正アクセスからの被害を　防止することができる。

1. 不正アクセスによる被害の予防について

「Ⅴ 1. システムユーザ基準」の「(1) パスワード及びユーザID管理」、「(2) 情報管理」、「(3) コンピュータ管理」の中の必要な項目

2. 不正アクセスによる被害の発見、復旧、拡大及び再発防止について

「Ⅴ　2. システム管理者基準」の「(6) 事後対応」

Ⅴ. 基準項目

1. システムユーザ基準

(1) パスワード及びユーザID管理

1.ユーザIDは、複数のシステムユーザで利用しないこと。
2.ユーザIDは、パスワードを必ず設定すること。
3.複数のユーザIDを持っている場合は、それぞれ異なるパスワードを設定すること。
4.悪いパスワードは、設定しないこと。
5.パスワードは、随時変更すること。
6.パスワードは、紙媒体等に記述しておかないこと。
7.パスワードを入力する場合は、他人に見られないようにすること。
8.他人のパスワードを知った場合は、速やかにシステム管理者に通知すること。
9.ユーザIDを利用しなくなった場合は、速やかにシステム管理者に届け出ること。

(2) 情報管理

1.重要な情報は、パスワード、暗号化等の対策を図ること。
2.重要な情報を送信する場合は相手先を限定し、宛先を十分に確認すること。
3.ファイルの属性は、内容の重要度に応じたアクセス権限を必ず設定すること。
4.コンピュータ及び通信機器を維持、保守するために必要なファイルは、盗用、改ざん、削除等されないように厳重に管理すること。
5.重要な情報を記録した紙、磁気媒体等は、安全な場所に保管すること。
6.重要な情報を記録した紙、磁気媒体等を廃棄する場合は、内容が漏えいしない方法で行うこと。
7.ファイルのバックアップを随時行い、その磁気媒体等を安全な場所に保管すること。

(3) コンピュータ管理

1.コンピュータ、通信機器及びソフトウェアの導入、更新、撤去等を行う場合は、システム管理者の指導の下で行うこと。
2.コンピュータを管理するために与えられた最上位の権限（以下「特権」とする。）によるコンピュータの利用は、必要最小限にすること。
3.特権によりコンピュータを利用する場合は、コンピュータ、場所、期間等を限定すること。
4.コンピュータが無断で利用された形跡がないか、利用履歴等を随時確認すること。
5.コンピュータを入力待ち状態で放置しないこと。
6.パスワードの入力を省略する機能は、システム管理者の指導の下で使用すること。

(4) 事後対応

1.システムの異常を発見した場合は、速やかにシステム管理者に連絡し、指示に従うこと。
2.不正アクセスを発見した場合は、速やかにシステム管理者に連絡し、指示に従うこと。

(5) 教育及び情報収集

1.システム管理者からセキュリティ対策に関する教育を随時受けること。
2.セキュリティ対策に関する情報を入手した場合は、システム管理者に随時提供すること。

(6) 監査

1.システムユーザが行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

2．システム管理者基準

(1) 管理体制の整備

1.システムのセキュリティ方針を確立し、周知･徹底すること。
2.システムの管理体制、管理手順を確立し、周知･徹底すること。
3.緊急時の連絡体制及び復旧手順を確立し、周知･徹底すること。
4.システム管理の業務上知り得た情報の秘密を守ること。
5.システム管理者の権限は、業務を遂行する上で必要最小限にすること。
6.システム管理者は2人以上かつ必要最小限の管理者で、その業務は定期的に交代すること。
7.システム管理者の資格を喪失した者の権限は、速やかに停止すること。

(2) システムユーザ管理

1.システムユーザの登録は、必要な機器に限定し、システムユーザの権限を必要最小限に設定すること。
2.ネットワークを介して外部からアクセスできるユーザIDは、必要最小限にすること。
3.ユーザIDは、個人単位に割り当て、パスワードを必ず設定すること。
4.長期間利用していないユーザIDは、速やかに停止すること。
5.ユーザIDの廃止等の届出があった場合は、速やかに登録を抹消すること。
6.パスワードは、当該システムユーザ以外に知らせないこと。
7.パスワードのチェックを随時行い、悪いパスワードは、速やかに変更させること。
8.パスワードが当該システムユーザ以外に知られた場合又はその疑いのある場合は、速やかに変更させること。
9.特権を付与する場合は、当該システムユーザの技術的能力等を考慮すること。
10.必要としなくなったシステムユーザの特権は、速やかに停止すること。

(3) 情報管理

1.通信経路上の情報は、漏えいを防止する仕組みを確立すること。
2.通信経路上で情報の盗聴及び漏えいが行われても、内容が解析できない機密保持機能を用いること。
3.通信経路上で情報の改ざんが行われても、検出できるような改ざん検知機能を用いること。
4.システム関連のファイルは、システムユーザがアクセスできないように管理すること。
5.重要な情報は、削除、改ざん、漏えい等による被害が少なくなるように分散化すること。
6.重要な情報を記録した紙、磁気媒体等は、安全な場所に保管すること。
7.重要な情報を記録した紙、磁気媒体等を廃棄する場合は、内容が漏えいしない方法で行うこと。
8.ファイルのバックアップを随時行い、その磁気媒体等を安全な方法で保管すること。

(4) 設備管理

1.すべての機器及びソフトウェアの管理者を明確にすること。
2.重要な情報が格納されているか又は重要な処理を行う機器は、許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。
3.移動可能な機器は、盗難防止策を行うこと。
4.システム構成を常に把握しておくこと。
5.機器及びソフトウェアを導入する場合は、セキュリティ機能がセキュリティ方針に適合していることをあらかじめ確認してから行うこと。
6.機器及びソフトウェアの設定情報がシステムに適合していることを随時確認すること。
7.機器及びソフトウェアは、供給者の連絡先及び更新情報が明確なものを利用すること。
8.セキュリティ上の問題点が解決済みの機器及びソフトウェアを利用すること。
9.外部と接続する機器は、十分なアクセス制御機能を有したものを利用すること。
10.システム構成の変更を行う前に、セキュリティ上の問題が生じないことを確認すること。
11.ネットワークを介して外部からアクセスできる通信経路及びコンピュータは、必要最小限にすること。
12.ネットワークを介して外部からシステム管理を行う場合は、認証機能、暗号機能及びアクセス制御機能を設定すること。
13.長期間利用しない機器は、システムに接続しないこと。
14.機器及びソフトウェアの廃棄、返却、譲渡等を行う場合は、情報の漏えいを防ぐ対策を行うこと。
15.ソフトウェア及びシステムファイルの改ざんが生じていないことを随時確認すること。
16.システムが提供するパスワード強化機能は最大限に活用すること。
17.ネットワークの負荷状況を監視すること。
18.システムの利用形態等に応じて、ネットワークを分離すること。

(5) 履歴管理

1.システムのセキュリティ方針に基づいたシステムの動作履歴、使用記録等を記録すること。
2.システムの動作履歴、使用記録等を記録する場合は、改ざん、削除、破壊及び漏えいの防止措置を施すこと。
3.記録したシステムの動作履歴、使用記録等を随時分析すること。
4.記録したシステムの動作履歴、使用記録等は、安全な方法で一定期間保管すること。

(6) 事後対応

1.異常の連絡を受けた場合又は異常を発見した場合は、速やかに原因を追究すること。
2.不正アクセスであることが判明した場合は、関係者と協調して被害の状況を把握すること。
3.関係者と協調して不正アクセス被害の拡大を防止するための処置を行うこと。
4.事前に確立した復旧手順を遂行し、関係者と協調して不正アクセス被害の復旧に努めること。
5.不正アクセス被害の原因を分析し、関係者と協調して再発防止策を行うこと。
6.不正アクセ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。

(7) 情報収集及び教育

1.セキュリティ対策に関する情報を随時収集すること。
2.収集した情報を分析し、重要な情報については速やかに対応すること。
3.システムユーザがセキュリティ対策を行う場合に必要な情報を提供すること。
4.システムユーザに、セキュリティ教育を随時実施すること。

(8) 監査

1.システム管理者が行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

3．ネットワークサービス事業者基準

(1) 管理体制の整備

1.ネットワークサービス事業者の要員の業務範囲を明確にすること。
2.不正アクセスを発見したときの連絡体制及び復旧手順を確立し、周知･徹底すること。

(2) ネットワークサービスユーザ管理

1.ネットワークサービス事業者及びネットワークサービスユーザの責任範囲を明確にすること。
2.ネットワークサービス事業者が提供できるセキュリティサービスを明示すること。
3.ネットワークサービスユーザとの連絡体制を複数確立し、周知･徹底すること。
4.不正アクセスを行ったネットワークサービスユーザに対するサービスを制限できる仕組みを確立すること。
5.ネットワークサービスユーザから要求があった場合、本人の利用情報等を開示すること。
6.ネットワークサービスユーザへの不正アクセスを監視できる仕組みを確立すること。
7.ネットワークサービスユーザの利用情報等を記録できる仕組みを確立すること。

(3) 情報管理

1.ネットワークサービスユーザの情報は、厳重に管理すること。
2.ネットワークサービスユーザの情報を公開する場合は、本人の了解を得ること。
3.ネットワーク構成等の重要な情報は、公開しないこと。

⑷ 設備管理

1.ネットワークサービスに係る機器は、許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。
2.ネットワークサービスに係る機器の管理が常に可能な仕組みを確立すること。
3.ネットワークサービスに係る機器を遠隔管理する通信回線は、複数確保すること。
4.ネットワークサービスユーザにサービスを提供するネットワークは、他の業務のネットワークと分離すること。
5.特定のサービスに関する情報は、そのサービスに関連した機器に限定して流すこと。

⑸ 事後対応

1.異常の連絡を受けた場合又は異常を発見した場合は、速やかに原因を追究すること。
2.不正アクセスであることが判明した場合は、関係者と協調して被害の状況を把握すること。
3.関係者と協調して不正アクセス被害の拡大を防止するための処置を行うこと。
4.事前に確立した復旧手順を遂行し、関係者と協調して不正アクセス被害の復旧に努めること。
5.不正アクセス被害の原因を分析し、関係者と協調して再発防止策を行うこと。
6.不正アクセ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。

⑹ 情報収集及び教育

1.セキュリティ対策に関する情報を随時収集すること。
2.ネットワークサービスユーザがセキュリティ対策を行う場合に必要な情報を提供すること。
3.ネットワークのセキュリティ上の問題及びその対策に関する十分な情報を提供し、必要に応じてその情報を活用するための教育をすること。

⑺ 監査

1.ネットワークサービス事業者が行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

4．ハードウェア･ソフトウェア供給者基準

⑴ 管理体制の整備

1.ハードウェア･ソフトウェア供給者の要員の業務範囲を明確にすること。
2.不正アクセスを発見したときの連絡体制及び復旧手順を確立し、周知･徹底すること。

⑵ 設備管理

1.開発業務に係る機器は、許可を与えられた者以外立ち入れない場所に設置し、厳重に管理すること。
2.開発業務に係るネットワークは、他の業務のネットワークと分離すること。

⑶ 開発管理

1.製品のセキュリティ機能の実装に関する方針を明確にすること。
2.製品は、機密保持機能、認証機能、改ざん検知機能等のセキュリティ機能を設けること。
3.製品のネットワークに係る機能は、セキュリティ上の重要な情報の解析を防ぐ機能を組み込むこと。
4.製品の保守に係る機能は、利用する者を限定する機能を組み込むこと。
5.セキュリティの設定を行わないと製品が利用できない機能を設けること。

6.製品の開発に使用したデバッグ機能等は、出荷前に削除しておくこと。
7.製品のセキュリティ機能が仕様どおり動作するか検査すること。

(4) 販売管理

1.製品は、流通段階における改ざん等を防止するための措置を施すこと。
2.製品は、利用上の制限事項及び推奨事項を明示の上、販売等を行うこと。
3.製品は、供給者の連絡先を明示しておくこと。
4.製品にセキュリティ上の問題が発見された場合は、製品のユーザ及び関係者に情報を通知するとともに、問題を解決するための適切な処置を行うこと。

(5) 事後対応

1.製品開発システムにおける異常を発見した場合は、速やかに原因を追究すること。
2.不正アクセスであることが判明した場合は、関係者と協調して被害の状況を把握すること。
3.関係者と協調して不正アクセス被害の拡大を防止するための処置を行うこと。
4.事前に確立した復旧手順を遂行し、関係者と協調して不正アクセス被害の復旧に努めること。
5.不正アクセス被害の原因を分析し、関係者と協調して再発防止策を行うこと。
6.不正アクセ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。

(6) 情報収集及び教育

1.製品のセキュリティ対策に関する情報を随時収集し、その情報を製品の開発に生かすこと。
2.製品の販売を通じてセキュリティ対策の情報を提供し、必要に応じて教育を行うこと。

(7) 監査

1.ハードウェア・ソフトウェア供給者が行う不正アクセス対策の実効性を高めるため、システム監査の報告を受け、必要な措置を講ずること。

VI. 留意事項

1.本基準は、システムの構成及び利用形態、取り扱う情報等に則して活用すること。
2.ネットワークサービス事業者基準及びハードウェア・ソフトウェア供給者基準は、各事業者特有の観点からまとめた基準であることから、各事業の機器の導入等にあたっては、システム管理者基準も併せて活用すること。
3.コンピュータウイルス対策の実施については、「コンピュータウイルス対策基準」(平成7年7月7日付　通産省告示第429号)を活用すること。
4.システム自体の安全対策の実施については、「情報システム安全対策基準」(平成7年8月29日付　通産省告示第518号)を活用すること。
5.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日付　通産省公報)を活用すること。
6.ソフトウェア管理の実施については、「ソフトウェア管理ガイドライン」(平成7年11月15日付通産省公報)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ィテイを高めることができる。

- 関連告示

平成8年通商産業省告示第３６２号（コンピュータ不正アクセ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９４９号（コンピュータ不正アクセ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