○総務省告示第三十六号

昭和六十二年郵政省告示第七十三号（情報通信ネットワーク安全・信頼性基準）の一部を次のように改正する。

令和五年二月二十二日

総務大臣　松本　剛明

次の表により、改正前欄に掲げる規定の下線を付し又は破線で囲んだ部分をこれに順次対応する改正後欄に掲げる規定の下線を付し又は破線で囲んだ部分のように改める。

改正後

［第１～第５　略］

別表第１　設備等基準

項目	対策	実施指針				
		電気通信回線設備用ネットワーク	特定線設事用非置業ネットワーク	その他の電気通信業用ネットワーク	自営情報通信ネットワーク	ユーザーネットワーク
第１．設備基準						
１．一般基準						
［(1)～(8)　略］						
(9)　ソフトウェアの信頼性向上対策	［ア～キ　略］					
	ク　ソフトウェアの導入又は更新に当たつては、コンピュータウィルス等の混入を防ぎ、セキュリティを確保すること。	◎	◎	◎	◎*	◎*
	［ケ　略］					
	コ　交換機の制御等に用いられる重要なソフトウェアについては、復元できるよう複数世代のものを保管すること。	◎	◎	－	－	－
	サ　交換機の制御等に用いられる重要なソフトウェアについては、ソフトウェア不具合等により電気通信役務の提供が停止することがないよう、当該ソフトウェアの導入・更新時は十分な検証を行い、その信頼性を確保すること。	◎	◎	－	－	－
［(10)　略］						

改正前

［第１～第５　同左］

別表第１　設備等基準

項目	対策	実施指針				
		電気通信回線設備用ネットワーク	特定線設事用非置業ネットワーク	その他の電気通信業用ネットワーク	自営情報通信ネットワーク	ユーザーネットワーク
第１．設備基準						
１．一般基準						
［(1)～(8)　同左］						
(9)　ソフトウェアの信頼性向上対策	［ア～キ　同左］					
	ク　ソフトウェアの導入又は更新に当たつては、ウィルス等の混入を防ぎ、セキュリティを確保すること。	◎	◎	◎	◎*	◎*
	［ケ　同左］					
	コ　交換機の制御等に用いられる重要なソフトウェアについては、復元できるよう複数世代のものを保管すること。	◎	－	－	－	－
	サ　交換機の制御等に用いられる重要なソフトウェアについては、ソフトウェア不具合等により電気通信役務の提供が停止することがないよう、当該ソフトウェアの導入・更新時は十分な検証を行い、その信頼性を確保すること。	◎	－	－	－	－
［(10)　同左］						

⑾ 通信の途絶防止対策	通信の途絶を防止する措置を講ずること。	◎*	◎*	－	◎*	－
［⑿～⒂　略］						
［２．～４．　略］						
［第２．　略］						

［注１～３　略］

別表第２　管理基準

項目	対策	実施指針				
		電気通信回線設備事業用ネットワーク	特定回線非設置事業用ネットワーク	その他の電気通信事業用ネットワーク	自営情報通信ネットワーク	ユーザネットワーク
［第１．・第２．　略］						
第３．方法						
１．平常時の取組						
⑴ 基本的取組	［ア　略］					
	イ　情報通信ネットワークの現状を調査・分析する作業の手順化を行うこと。	◎	◎	◎*	◎*	◎
	［ウ　略］					
［⑵　略］						
⑶ 設計	［ア～チ　略］					
	ツ　電気通信事業者が当該電気通信事業者以外の者が提供する設備を利用して電気通信役務を提供する際には、当該設備を利用する電気通信事業者自らが、電気通信設備として	◎	◎	－	－	－

⑾ 通信の途絶防止対策	通信の途絶を防止する措置を講ずること。	◎*	－	－	◎*	－
［⑿～⒂　同左］						
［２．～４．　同左］						
［第２．　同左］						

［注１～３　同左］

別表第２　管理基準

項目	対策	実施指針				
		電気通信回線設備事業用ネットワーク	特定回線非設置事業用ネットワーク	その他の電気通信事業用ネットワーク	自営情報通信ネットワーク	ユーザネットワーク
［第１．・第２．　同左］						
第３．方法						
１．平常時の取組						
⑴ 基本的取組	［ア　同左］					
	イ　情報通信ネットワークの現状を調査・分析する作業の手順化を行うこと。	◎	◎*	◎*	◎*	◎
	［ウ　同左］					
［⑵　同左］						
⑶ 設計	［ア～チ　同左］					
	ツ　電気通信事業者が当該電気通信事業者以外の者が提供する設備を利用して電気通信役務を提供する際には、当該設備を利用する電気通信事業者自らが、電気通信設備として	◎	－	－	－	－

	必要とされる技術基準を満たしていることを確認すること。					
［(4)　略］						
(5)　維持・運用	［ア～カ　略］					
	キ　設備を設置する建築物及び空気調和設備の定期的な保全点検を実施すること。	◎	◎	◎*	◎	◎
	［ク～セ　略］					
［(6)　略］						
(7)　ソフトウェアの信頼性確保	［ア～オ　略］					
	カ　使用しているソフトウェアの安全・信頼性の基準及び指標を策定すること。	◎	◎	◎*	○	○
	キ　交換機の制御等に用いられる重要なソフトウェアについては、機器等の製造・販売を行う者等関係者との契約書等において、サービスの提供の継続に重要と考えられる有効期限等の情報を確認できることを明示すること。	◎	◎	－	－	－
	ク　ソフトウェアに有効期限が設定されている場合は、電気通信事業者が自ら又は機器等の製造・販売を行う者等関係者との契約等を通じて、確実に管理すること。	◎	◎	－	－	－
［(8)～(11)　略］						
(12)　現状の調査・分析・改善	［ア・イ　略］					
	ウ　情報通信ネットワークの維持及び運用に関して、現状の調査・分析作業の手順化を行うこと。	◎	◎	◎*	◎*	◎
	［エ・オ　略］					
［(13)　略］						

	必要とされる技術基準を満たしていることを確認すること。					
［(4)　同左］						
(5)　維持・運用	［ア～カ　同左］					
	キ　設備を設置する建築物及び空気調和設備の定期的な保全点検を実施すること。	◎	◎*	◎*	◎	◎
	［ク～セ　同左］					
［(6)　同左］						
(7)　ソフトウェアの信頼性確保	［ア～オ　同左］					
	カ　使用しているソフトウェアの安全・信頼性の基準及び指標を策定すること。	◎	◎*	◎*	○	○
	キ　交換機の制御等に用いられる重要なソフトウェアについては、機器等の製造・販売を行う者等関係者との契約書等において、サービスの提供の継続に重要と考えられる有効期限等の情報を確認できることを明示すること。	◎	－	－	－	－
	ク　ソフトウェアに有効期限が設定されている場合は、電気通信事業者が自ら又は機器等の製造・販売を行う者等関係者との契約等を通じて、確実に管理すること。	◎	－	－	－	－
［(8)～(11)　同左］						
(12)　現状の調査・分析・改善	［ア・イ　同左］					
	ウ　情報通信ネットワークの維持及び運用に関して、現状の調査・分析作業の手順化を行うこと。	◎	◎*	◎*	◎*	◎
	［エ・オ　同左］					
［(13)　同左］						

［２．　略］	［２．　同左］
３．事故収束後の取組	３．事故収束後
［略］	［同左］

［注　略］

別表第３　情報セキュリティポリシー策定のための指針

［１～４　略］

５　情報セキュリティポリシーの構成例

［略］

［１　略］ ２　方針 ［⑴　略］ ⑵　情報資産に関する方針 ［ア　略］ イ　情報システム ［略］ ［(ｱ)～(ｴ)　略］ (ｵ)　コンピュータウィルス 業務で使用する機器がコンピュータウィルスに感染した場合、多大な被害が発生する可能性があるため、感染の予防及び防止が重要である。そこで、コンピュータウィルスに関しても管理体制を確立し、予防及び防止並びに感染時の対策を明確化する。また、コンピュータウィルス等による情報漏えいの防止対策も明確化する。 また、コンピュータウィルスによる情報漏えいが懸念されるため、情報漏えいを発生させる懸念のあるソフトウェアの導入を防止する等の予防措置を明確化するとともに、コンピュータウィルスに感染した場合の情報漏えいの防止対策を明確化する。 ［ウ　略］	［１　同左］ ２　［同左］ ［⑴　同左］ ⑵　［同左］ ［ア　同左］ イ　［同左］ ［同左］ ［(ｱ)～(ｴ)　同左］ (ｵ)　コンピュータウイルス 業務で使用する機器がコンピュータウイルスに感染した場合、多大な被害が発生する可能性があるため、感染の予防及び防止が重要である。そこで、コンピュータウイルスに関しても管理体制を確立し、予防及び防止並びに感染時の対策を明確化する。また、コンピュータウイルス等による情報漏えいの防止対策も明確化する。 また、コンピュータウイルスによる情報漏えいが懸念されるため、情報漏えいを発生させる懸念のあるソフトウェアの導入を防止する等の予防措置を明確化するとともに、コンピュータウイルスに感染した場合の情報漏えいの防止対策を明確化する。 ［ウ　同左］

別表第４　危機管理計画策定のための指針

［１　略］

２　サイバーテロの定義等

［⑴～⑶　略］

⑷　主な攻撃方法

［略］

［ア・イ　略］

ウ　分散協調型サービス拒否（以下「ＤＤｏｓ」という。）攻撃

複数の場所からサーバの処理能力を超える大量のデータを送り付けるなどの方法によりサーバを停止させるもの

別表第４　危機管理計画策定のための指針

［１　同左］

２　［同左］

［⑴～⑶　同左］

⑷　［同左］

［同左］

［ア・イ　同左］

ウ　分散協調型サービス拒否（以下「ＤＤｏｓ」という。）攻撃

複数の場所からサーバーの処理能力を超える大量のデータを送り付けるなどの方法によりサーバーを停止させるもの

［エ・オ　略］	［エ・オ　同左］
3　危機管理計画の策定	3　［同左］
［略］	［同左］
⑴　対象	⑴　［同左］
ア　攻撃	ア　［同左］
［略］	［同左］
［(ｱ)～(ｳ)　略］	［(ｱ)～(ｳ)　同左］
(ｴ)　ＩＰネットワーク サーバ等への攻撃、モバイルインターネットアクセスへの攻撃、コンピュータウィルス	(ｴ)　ＩＰネットワーク サーバー等への攻撃、モバイルインターネットアクセスへの攻撃、コンピュータウィルス
［(ｵ)　略］	［(ｵ)　同左］
［イ　略］	［イ　同左］
⑵　予防	⑵　［同左］
［略］	［同左］
［ア　略］	［ア　同左］
イ　ソフトウェア上の対策	イ　［同左］
(ｱ)　インターネットに接続する場合は、サーバ等におけるセキュリティホール対策を講ずる。	(ｱ)　インターネットに接続する場合は、サーバー等におけるセキュリティホール対策を講ずる。
［(ｲ)　略］	［(ｲ)　同左］
ウ　監視、管理等	ウ　［同左］
(ｱ)　インターネットに接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバ及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されるよう措置する。 また、ネットワーク上のパケット並びにサーバ及びネットワーク機器の動作に関するログの適切な記録及び保存を行う。	(ｱ)　インターネットに接続する場合は、不正アクセス等に関するネットワーク監視機能並びにサーバー及びネットワーク機器の監視機能を設け、異常が発見された場合は自動的に管理者に通知されるよう措置する。 また、ネットワーク上のパケット並びにサーバー及びネットワーク機器の動作に関するログの適切な記録及び保存を行う。
［(ｲ)　略］	［(ｲ)　同左］
［エ～ク　略］	［エ～ク　同左］
ケ　サーバ等への攻撃が発生した際の迅速な情報共有方法の確立	ケ　サーバー等への攻撃が発生した際の迅速な情報共有方法の確立
⑶　発生時の復旧対応	⑶　［同左］
ア　復旧対応としては、必要に応じて次の項目を規定するとともに、既存の障害復旧マニュアル等を活用することも規定する。	ア　復旧対応としては、必要に応じて次の項目を規定するとともに、既存の障害復旧マニュアル等を活用することも規定する。
(ｱ)　サーバ等への攻撃からの復旧対応	(ｱ)　サーバー等への攻撃からの復旧対応
Ａ　ＤＤｏＳ攻撃により通信不能となつた場合、攻撃側サーバの速やかな停止を依頼する。	Ａ　ＤＤｏＳ攻撃により通信不能となつた場合、攻撃側サーバーの速やかな停止を依頼する。
Ｂ　サーバのルート権限を奪われる等により不正な処理を開始した場合、サーバを停止する又はネットワークから切断し再起動する。	Ｂ　サーバーのルート権限を奪われる等により不正な処理を開始した場合、サーバーを停止する又はネットワークから切断し再起動する。

C　サーバが何らかの原因により不正な処理を開始した場合、ルート権限で不正な処理のプロセスを排除する。 D　サーバへの侵入の痕跡を発見した場合、サーバをネットワークから隔離する。 E　サーバ等が通信不能となつた場合、通信不能箇所を特定し再起動などの処置を行う。 ［(イ)　略］ ［イ・ウ　略］ ［(4)・(5)　略］	C　サーバーが何らかの原因により不正な処理を開始した場合、ルート権限で不正な処理のプロセスを排除する。 D　サーバーへの侵入の痕跡を発見した場合、サーバーをネットワークから隔離する。 E　サーバー等が通信不能となつた場合、通信不能箇所を特定し再起動などの処置を行う。 ［(イ)　同左］ ［イ・ウ　同左］ ［(4)・(5)　同左］
備考　表中の［　］の記載は注記である。	