

○総務省告示第 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 年 月 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。

【第1～第5 略】
別表第1 設備等基準

【第1～第5 同左】
別表第1 設備等基準

項目	対策	実施指針				
		電気線 通信回 線設備 用ネット ワーク	特定 回線設 置用ソ フトウ ェア	その他 電気通 信用ソ フトウ ェア	自 情 報 通 信 ソ フト ウ ェ ア	ユ ー ザ ソ フト ウ ェ ア
		◎	◎	◎	◎*	◎*

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	ク	ク	ク	ク
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。	◎	◎	◎	◎*	◎*
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業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】

項目	対策	実施指針				
		電気線 通信回 線設備 用ネット ワーク	特定 回線設 置用ソ フトウ ェア	その他 電気通 信用ソ フトウ ェア	自 情 報 通 信 ソ フト ウ ェ ア	ユ ー ザ ソ フト ウ ェ ア
		◎	◎	◎	◎*	◎*

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	ク	ク	ク	ク
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。	◎	◎	◎	◎*	◎*
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業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】

(11) 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。	◎*	◎*	—	◎*	—
	【(12)～(15) 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				
		電気通信回線設備用ネットワーク	特定線設置用ネットワーク	その他の電気通信用ネットワーク	自営情報ネットワーク	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						
(1) 基本的取組	【ア 略】 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】				
【(2) 略】						
(3) 設計	【ア～チ 略】 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業務を提供する際には、当該設	◎	◎	—	—	—

(11) 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。	◎*	—	—	◎*	—
	【(12)～(15) 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				
		電気通信回線設備用ネットワーク	特定線設置用ネットワーク	その他の電気通信用ネットワーク	自営情報ネットワーク	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						
(1) 基本的取組	【ア 同左】 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】				
【(2) 同左】						
(3) 設計	【ア～チ 同左】 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業務を提供する際には、当該設	◎	—	—	—	—

	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】	◎	◎	◎*	◎*	◎

	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) 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】	◎	◎*	◎*	◎*	◎

<table border="1"> <tr><td>[(13) 略]</td></tr> <tr><td>[2. 略]</td></tr> <tr><td>3. 事故収束後の取組</td></tr> <tr><td>[略]</td></tr> </table>	[(13) 略]	[2. 略]	3. 事故収束後の取組	[略]	<table border="1"> <tr><td>[(13) 同左]</td></tr> <tr><td>[2. 同左]</td></tr> <tr><td>3. 事故収束後</td></tr> <tr><td>[同左]</td></tr> </table>	[(13) 同左]	[2. 同左]	3. 事故収束後	[同左]
[(13) 略]									
[2. 略]									
3. 事故収束後の取組									
[略]									
[(13) 同左]									
[2. 同左]									
3. 事故収束後									
[同左]									
<p>[注 略]</p> <p>別表第3 情報セキュリティポリシー策定のための指針</p> <p>[1～4 略]</p> <p>5 情報セキュリティポリシーの構成例</p> <p>[略]</p>	<p>[注 同左]</p> <p>別表第3 情報セキュリティポリシー策定のための指針</p> <p>[1～4 同左]</p> <p>5 情報セキュリティポリシーの構成例</p> <p>[同左]</p>								
<p>[1 略]</p> <p>2 方針</p> <p>〔(1) 略〕</p> <p>〔2〕 情報資産に関する方針</p> <p>〔ア 略〕</p> <p>イ 情報システム</p> <p>〔略〕</p> <p>〔(イ)～(ロ) 略〕</p> <p>〔(イ)～(ロ) 略〕</p> <p>〔ウ 略〕</p> <p>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つい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。</p>	<p>[1 同左]</p> <p>2 方針</p> <p>〔(1) 同左〕</p> <p>〔2〕 情報資産に関する方針</p> <p>〔ア 同左〕</p> <p>イ 情報システム</p> <p>[同左]</p> <p>〔(イ)～(ロ) 同左〕</p> <p>〔(イ)～(ロ) 同左〕</p> <p>〔ウ 同左〕</p> <p>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つい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。</p>								
<p>別表第4 危機管理計画策定のための指針</p> <p>[1 略]</p> <p>2 サイバーテロの定義等</p> <p>〔(1)～(3) 略〕</p> <p>(4) 主な攻撃方法</p> <p>[略]</p> <p>〔ア・イ 略〕</p> <p>ウ 分散協調型サービス拒否 (以下「DDoS」という。) 攻撃</p>	<p>別表第4 危機管理計画策定のための指針</p> <p>[1 同左]</p> <p>2 同左]</p> <p>〔(1)～(3) 同左]</p> <p>(4) 主な攻撃方法</p> <p>[同左]</p> <p>〔ア・イ 同左]</p> <p>ウ 分散協調型サービス拒否 (以下「DDoS」という。) 攻撃</p>								

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

【エ・オ 略】

3 危機管理計画の策定

【略】

(1) 対象

ア 攻撃

【略】

【(イ)～(ウ) 略】

(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、コンピュータウイルス

【(イ) 略】

【イ 略】

(2) 予防

【略】

【ア 略】

イ ソフトウェア上の対策

(イ) 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。

【(イ) 略】

ウ 監視、管理等

(イ) 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。

【(イ) 略】

【エ～ク 略】

ク 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

(3) 発生時の復旧対応

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。

(イ) サーバ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った場合、攻撃側サーバの速やかな停止を依頼する。

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

【エ・オ 同左】

3 危機管理計画の策定

【同左】

(1) 対象

ア 攻撃

【同左】

【(イ)～(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、コンピュータウイルス

【(イ) 同左】

【イ 同左】

(2) 予防

【同左】

【ア 同左】

イ ソフトウェア上の対策

(イ) 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。

【(イ) 同左】

ウ 監視、管理等

(イ) 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。

【(イ) 同左】

【エ～ク 同左】

ク 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

(3) 発生時の復旧対応

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。

(イ) サーバ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った場合、攻撃側サーバの速やかな停止を依頼する。

<p>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、<u>サーバ</u>を停止する又はネットワークから切断し再起動する。</p> <p>C <u>サーバ</u>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。</p> <p>D <u>サーバ</u>への侵入の痕跡を発見した場合、<u>サーバ</u>をネットワークから隔離する。</p> <p>E <u>サーバ</u>等が通信不能となった場合、通信不能箇所を特定し再起動などの処置を行う。</p> <p>【(4) 略】 【イ・ウ 略】 【(4)・(5) 略】</p>	<p>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、<u>サーバ</u>を停止する又はネットワークから切断し再起動する。</p> <p>C <u>サーバ</u>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。</p> <p>D <u>サーバ</u>への侵入の痕跡を発見した場合、<u>サーバ</u>をネットワークから隔離する。</p> <p>E <u>サーバ</u>等が通信不能となった場合、通信不能箇所を特定し再起動などの処置を行う。</p> <p>【(4) 同左】 【イ・ウ 同左】 【(4)・(5) 同左】</p>
<p>備考 表中の「」の記号は法記である。</p>	