官報
（号外）
大蔵省印刷局発行
明治二十五年二月二十一日　第三種郵便物認可

目次

告示

○郵政省告示第五百四十六号

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。

平成十二年八月二十九日

郵政大臣　平林　鴻三

第2に次の一号を加える。

8　「情報セキュリティポリシー」とは、情報資産の損失に対する抑止、予防、検知及び回復について、組織的・計画的に取り組むために定める統一方針であり、情報セキュリティを実践するための基本的な考え方及び方向性を定めたものをいう。

第4を第5とし、第3の次に次の一項を加える。

第4　配慮すべき事項

別表第2に基づき、情報セキュリティポリシーを策定するに当たっては、別表第3の「情報セキュリティポリシー策定のための指針」に配慮すること。

別表第1の表第1の(8)の項を次のように改める。

(8) 情報セキュリティ対策	ア　インターネットへ接続する場合は、ファイアウォールを設置して適切な設定を行うこと。	○	○	○	○	○	○	○	○	○
	イ　インターネットへ接続する場合は、非武装セグメント構成を採用すること。	○	○	○	○	○	○	○	○	○
	ウ　インターネットへ接続する場合は、telnetやftp等サービス提供に不用な通信の接続制限を行うこと。	○	○	○	○	○	○	○	○	○
	エ　インターネットへ接続する場合は、公開域とを区別したネットワーク構成を採用すること。	○	○	○	○	○	○	○	○	○
	オ　インターネットへ接続する場合は、サーバー等におけるセキュリティホール対策を講ずること。	○	○	○	○	○	○	○	○	○
	カ　インターネットへ接続する場合は、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障害発生機能を設け、異常が発見された場合は自動的に管理者に通知されること。	○	○	○	○	○	○	○	○	○
	キ　インターネットへ接続する場合は、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こと。	○	○	○	○	○	○	○	○	○
	ク　インターネットへ接続する場合は、最新の情報セキュリティ技術を採用すること。	○	○	○	○	○	○	○	○	○
	ケ　コンピュータウィルス及び不正プログラム混入対策を講ずること。	○	○	○	○	○	○	○	○	○
	コ　利用者の識別・確認を要する通信を取り扱う情報通信ネットワークには、正当な利用者の識別・確認を行う機能を設けること。	○	○	○	○	○	○	○	○	○
	サ　アクセス可能領域及び使用可能な命令の範囲に制限を設ける等のシステムの破壊並びに他人のデータの破壊及び窃盗を防止する措置を講ずること。	○	○	○	○	○	○	○	○	○

	シ　利用者のパスワードの文字列をチェックし、一般的な単語を排除する機能を設けること。	○	○	○	○	○
	ス　アクセス失敗回数の基準を設定するとともに、基準値を超えたものについては、履歴を残しておく機能を設けること。	○	○	○	○	○
	セ　保護することが求められる重要な情報については、その情報に対するアクセス要求を記録し、保存する機能を設けること。	○	○	○	○	○
	ソ　ネットワークへのアクセス履歴の表示あるいは照会が行える機能を設けること。	○	○	○	○	○
	タ　一定期間以上パスワードを変更していない利用者に対して注意喚起する機能を設けること。	○	○	○	○	○
	チ　一定期間以上ネットワークを利用していない利用者がネットワークにアクセスする際に、再開の意思を確認する機能を設けること。	○	○	○	○	○
	ツ　機密度の高い通信には、秘話化又は暗号化の措置を講ずること。	○	○	○	○	○
	テ　適切な漏話減衰量の基準を設定すること。	◎	◎	◎*	◎*	◎*
	ト　ネットワークの不正使用を防止する措置を講ずること。	○	○	○	○	○

別表第2の表中10の項を11の項とし、同表9の項中「キ　通信の秘密の保護及びデータの保護に関するモラルの向上を図ること。」を「キ　情報セキュリティに関する教育・訓練を行うこと。」に改め、同項を同表10の項とし、同表中8の項を9の項とし、7の項を8の項とし、6の項を7の項とし、5の項を6の項とし、4の項の次に次のように加える。

5　情報セキュリティ管理						
(1)　情報セキュリティポリシーの策定	情報セキュリティポリシーを策定し、適宜見直しを行うこと。	◎	◎	◎	◎	◎
(2)　危機管理計画の策定	不正アクセス等への対処を定めた危機管理計画を策定し、適宜見直しを行うこと。	◎	◎	◎	◎	◎
(3)　情報セキュリティ監査の実施	第三者によるセキュリティ監査を実施し、その結果を踏まえ情報セキュリティ対策全体の見直しを行うこと。	◎	◎	◎	○	○
(4)　コンピュータウイルス情報緊急通報体制の整備	ア　新たなコンピュータウイルスを発見した場合等、コンピュータウイルスに関する情報を広く一般に周知する必要があるときは、電気通信業界で定めた緊急連絡先に、直ちに連絡すること。	◎	◎	◎	—	—
	イ　コンピュータウイルスに関する情報を入手したときは、自社内に対して速やかに周知するとともに、利用者に対してウェブへの掲示、メールニュース等適切な方法により速やかに情報提供する等、被害の拡大を防止するための措置を講ずること。	◎	◎	◎	◎	◎
(5)　情報セキュリティに関する情報収集	最新の情報セキュリティに関する技術情報や業界動向を入手し、それらを情報セキュリティ対策に反映させること。	◎	◎	◎	◎	◎

別表に次の1表を加える。

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　目的

この指針は、情報通信ネットワークの健全な発展に寄与することを目的とし、適正なリスク管理を実現させるための基本となる情報セキュリティポリシー策定のための指針として定めたものである。

2　情報セキュリティの管理

情報セキュリティを適切に管理していくためには、情報セキュリティの「方針立案」、「対策実施」、「運用・監視」及び「監査・診断」の各段階において、以下の対策を行う必要がある。

(1)　方針立案

ア　情報セキュリティポリシー及び実施手順の策定

情報セキュリティを適正に管理していくために、組織における情報セキュリティ対策に関する統一方針として情報セキュリティポリシーを策定する。

また、情報セキュリティポリシーに基づき、実際の業務・作業レベルまで考慮した情報セキュリティ実施手順を策定する。

イ　情報セキュリティ組織体制の整備

情報セキュリティに関して、責任所在の明確化やセキュリティ情報の共有化を行うために、情報セキュリティ組織体制を整備する。

(2)　対策実施

情報セキュリティポリシーの普及・教育

情報セキュリティポリシーが適正に実施されるよう、普及・教育活動を行い、情報セキュリティに対する自覚や意識の向上を目指す。

(3)　運用・監視

ア　情報セキュリティポリシーに沿った運用

情報セキュリティポリシーを理解し、情報セキュリティポリシーに沿った運用を適正に実行する。

イ　例外の管理

業務を遂行する中で、情報セキュリティポリシーが適用できない場合が発生する可能性もある。情報セキュリティポリシーから逸脱した際に、適正に管理する仕組みを確立する。

ウ　情報セキュリティ侵害時の対応の明確化

情報セキュリティ侵害が起きた際、速やかに侵害の事実、状況を伝達できるよう伝達経路を明確化する。

(4)　監査・診断

ア　情報セキュリティ監査

情報セキュリティポリシーが組織内において正しく実行されていることを把握するため定期的に監査する。

イ　情報セキュリティポリシーの見直し

情報セキュリティ監査結果や情報セキュリティを取り巻く環境等を考慮し、情報セキュリティポリシーを定期的に見直し、改訂を行う。

3　情報セキュリティポリシーの構成等

情報セキュリティの環境は技術動向、組織状況により変化することから、次のように情報セキュリティポリシーを目的、原則及び方針の三段階に階層化させることで、下位の方針のみを見直し、時代・環境変化に対応することができる。

(1)　目的

情報セキュリティポリシーにおいて最も基本となるもので、組織としての情報セキュリティへの取組の目的を定めるものである。最高権限者の声明として記述し、組織全体で積極的に情報セキュリティに取り組むことを明確化することが望ましい。

(2)　原則

目的に基づき、情報セキュリティを実現するための組織方針、組織理念等組織の基本的な考え方を定めるものである。利便性とセキュリティのバランスをどのように取るかといった、情報セキュリティ全体の考え方の根幹となる。

(3)　方針

原則に基づき、情報セキュリティを実現するための基本方針をテーマごとに具体化し定めるものである。各方針に対し、責任の所在を明確化する必要がある。

(4)　実施手順

定められた情報セキュリティポリシーを確実に実施するため、情報セキュリティポリシーに基づき、具体的な手順や方法を実施手順として定めることが一般的である。実施手順では、情報システムが最低限備えるべき具体的セキュリティ要件や、各情報システムの利用方法等、各方針に沿い、実際の業務、手順、方法等を記述することとなる。

4　情報セキュリティポリシーの策定

情報セキュリティポリシーは、組織として取り決めた最も重要な規程となるため、組織の幹部の関与により策定することが一般的である。

情報セキュリティポリシーの策定に当たり、各部門の業務に何らかの制約や変更を要請することがあるため、経営企画部門、総務部門といった社内規定を担当する部門が中心となり、各部門よりメンバーを召集して策定の為のチームを設立し、策定を行うことが望ましい。

なお、情報セキュリティポリシーには、情報システム部門、人事部門、監査部門等の部署の役割が非常に大きいため、これらの部門からの積極的参加を要請する。

また、外部コンサルティングサービスを提供する機関を活用し、策定に当たってのスケジュール、策定方法、記述事項等についての助言を得ることが好ましい。

情報セキュリティポリシーを策定する際の実施手順を以下に示す。

(1)　情報セキュリティポリシー策定チームの編成

各部門よりメンバーを召集し策定のためのチームを設立する。

(2)　「目的」及び「原則」の明確化

組織としての情報セキュリティに関する考えの根幹となる「目的」及び「原則」を定める。

(3)　情報セキュリティポリシーの適用範囲の明確化

情報セキュリティポリシーがどの範囲まで適用されるのかを明確化する。

(4)　情報資産の洗い出し

現在、組織が保有する情報資産とその価値を明確化する。

(5)　情報資産を取り巻く脅威とその脅威に対するリスクの分析

保護すべき情報資産を明らかにし、脅威の発生頻度、影響度を基にリスクを分析する。

(6)　「方針」の明確化

各情報資産を保護するために、組織としてどのような方針をもって対策を行うかを明確化する。

5　情報セキュリティポリシーの構成例

情報セキュリティポリシーの構成例と各項目における記述内容を以下に示す。

ここでは、方針を「情報セキュリティ運営に関する方針」と「情報資産に関する方針」に大きく分け、前者では管理の各段階に応じた項目、後者では情報資産の大きな区分である「情報」、「情報システム」、そして、情報資産を保護するための「アクセス制御」という項目立てとしている。

1　総則

(1)　目的

情報セキュリティの必要性と組織としての情報セキュリティの目的を記述する。最高権限者の声明として記述することで、情報セキュリティに対して組織全体で積極的に取り組むことを表明することが望ましい。

(2)　適用範囲

人、組織、場所、情報資産、技術等の切り口で情報セキュリティポリシーが適用される範囲を明確化する。

(3)　用語及び定義

情報セキュリティポリシー内で用いる用語の意味を明確にし、読者が共通の解釈の下、理解・判断できるよう用語の定義を行う。

(4)　原則

組織としての情報セキュリティに対する考え方の根幹となる原則を明確にし記述する。すべての方針、対策等は、ここで記述される原則に準拠しなければならない。例として、法令の遵守を原則として記述した場合、この原則に準拠し各組織員の役割等を方針にて定める。

2　方針

(1)　セキュリティ運営に関する方針

ア　情報セキュリティ組織

組織内の情報資産を管理し、セキュリティを担保する仕組みを確立する。具体的には、経営陣による情報セキュリティフォーラムの設立と、情報セキュリティに関する責任者の割当てを行う。また、組織内で働く外部業者を適用範囲に含む際は、その管理方法（契約時の必須項目等）を明確化する。

イ　普及・教育

情報セキュリティに対する知識と意識を向上させ、適用範囲内すべての人が情報セキュリティポリシーを理解し、遵守するよう、情報セキュリティポリシーの普及・教育活動を行うことを記述する。

ウ　例外の管理

情報セキュリティポリシーから逸脱する事項を管理・統括する組織・方法を明確にする。費用対効果を分析した結果、情報セキュリティポリシーに準拠することが得策ではない事項等が発生した際の対処方法を明確にすることで、逸脱発見者が迅速に対応を行い、組織として逸脱事項を管理・統括する体制を整備する。

エ　情報セキュリティ侵害時の対応

適用範囲内において、情報セキュリティ侵害が発生した際の対応手順を明確化することで、発生時に迅速に対応できる体制、方法を確立する。また、情報セキュリティポリシー違反者及びその監督責任者に対する罰則についても記述する。

オ　情報セキュリティ監査

情報セキュリティポリシーが組織内において正しく実行されていることを把握するため、定期的に監査する必要がある。監査組織と監査結果を把握する者を明確化する。

カ　情報セキュリティポリシーの改訂

情報セキュリティ監査結果や情報セキュリティを取り巻く環境等を考慮し、情報セキュリティポリシーを定期的に見直し、改訂を行う。改訂手順についても明確化する。

(2)　情報資産に関する方針

ア　情報

適用範囲内の情報についての管理方法を明確化することで、情報の漏えい、破壊、改ざん等を防止する。また、プライバシーにかかわる情報を取り扱う際に遵守すべき事項を明確化する。

(ア)　情報管理

情報の漏えい、破壊、改ざん等による被害等に応じて、情報を区分する。情報の区分と情報の取得・生成、保管、流通、利用及び廃棄という各段階における情報の取扱方法を明確にし、組織員による情報の取扱方法を統一化する。

(イ)　プライバシー情報

通信の秘密を含むプライバシー情報の漏えいは深刻な権利利益侵害につながるおそれが高いため、電気通信事業者に対しては、「電気通信事業における個人情報保護に関するガイドライン」(平成10年郵政省告示第570号)が制定されている。

プライバシー情報の適切な利用と保護が極めて重要であるとの認識により、プライバシー情報の取扱いについては、個別の項目を設け、個人情報の収集、利用・提供、適正管理、責任の明確化等について、遵守すべき方針を明確に記述する。

イ　情報システム

適用範囲内の情報システム上にて取り扱われる電子情報の漏えい、破壊、改ざん等の防止及び情報システム停止による損害の抑止を目的とし、情報システムについての管理方法(設計、構築及び運用方法)を明確化する。

(ア)　情報システム設計・構築

情報システムの設計、構築時における管理体制と、情報システムに実装すべきセキュリティ機能(アクセス制御機能、フロー制御機能、暗号化制御機能等)を明確化する。

(イ)　情報システム運用・停止

情報システムを適切に運用するための管理体制と実施事項を明確化する。また、情報システム障害時の対応策についても明確化する。

(ウ)　情報システムの使用権

情報システムの利用資格管理が適切に行われないと、情報システムの不正利用を招く危険がある。そこで、情報システムの利用資格に関する業務・責任を明確化する。また、情報システムの使用権を、必要な者に、必要な期間与え、情報システムの不正利用の定義を明確化する。

(エ)　ネットワークセキュリティ

ネットワークは情報流通の基盤であるとともに、情報侵害の経路ともなり得るため、適切に把握・管理することが必要である。セキュリティ侵害を防止するため、管理体制・実施事項を明確化する。

(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。

ウ　アクセス制御

適用範囲内の情報システムの利用、建物への入館、事務室及び機械室への入室等に際しては、情報資産を保護するため、個人を識別・認証し、情報へアクセスする際に審査することが必要である。そこで、利用者を限定・把握できるよう実施事項を明確化する。

附　則

この告示の施行の際現に昭和六十二年郵政省告示第七十四号(情報通信ネットワーク安全・信頼性対策実施登録規程)第八条の規定による登録を受けている情報通信ネットワークについては、その登録の有効期間までは、なお従前の例による。

公告

諸事項

公示催告

次の申立人から別紙目録表示の証書について公示催告の申立てがあったので、その所持人は、定められた公示催告期日までに当裁判所に権利を届け出ると同時に証書を提出してください。もし公示催告期日までに届出及び提出がない場合には、その無効を宣言することがあります。

平成12年(へ)第21号
神奈川県横須賀市本町3－27－1－1501
申立人　北野　時吉
申立人代理人弁護士　雨宮　真也
公示催告期日　平成13年3月6日午後1時30分
平成12年8月2日　川越簡易裁判所
(別紙)　目　録
銘柄　日本シイエムケイ株式会社株券
種類枚数　1000株券1枚
記号番号　404　1905
一株の金額　50円
最終名義人　申立人
最終所持人　申立人

平成12年(へ)第9号
名古屋市昭和区鶴舞2丁目2番18号
申立人　奥村遊機株式会社
代表者代表取締役　森　康二
代理人弁護士　森　進
同　加藤　倫子
同　鈴木　誠
同　森田　尚男
公示催告期日　平成13年3月12日午後1時20分
平成12年8月2日　函館簡易裁判所
(別紙)　目　録
約束手形　1通
手形番号　BD03862
金額　394,800円
支払期日　平成12年5月31日
支払地　函館市
支払場所　株式会社北海道銀行湯川支店
振出日　平成12年4月20日
振出地　函館市
振出人　有限会社統一観光　代表取締役　山本明姫
受取人　申立人
最終所持人　申立人

平成12年(へ)第4号
東京都国分寺市東恋ケ窪4丁目26番地の9
申立人　東進産業株式会社
代表者代表取締役　永山　宗春
公示催告期日　平成13年3月12日午後1時30分
平成12年8月1日　白河簡易裁判所
(別紙)　目　録
約束手形　1通
手形番号　BD28723
金額　4,815,385円
支払期日　平成12年12月10日
支払地　福島県白河市
支払場所　株式会社東邦銀行白河支店
振出日　平成12年6月20日
振出地　福島県白河市
振出人　株式会社エムテック　代表取締役　室政道
受取人　申立人
最終所持人　申立人

平成12年(へ)第15号
名古屋市北区長田町2丁目17番地
申立人　株式会社ナゴヤ保缶化学工業社
代表者代表取締役　三口　妙子
公示催告期日　平成13年3月14日午後1時30分
平成12年8月2日　四日市簡易裁判所
(別紙)　目　録
約束手形　1通
手形番号　BI35524
金額　676,000円
支払期日　平成12年8月31日
支払地　三重県四日市市
支払場所　株式会社東海銀行富田支店
振出日　平成12年5月10日
振出地　三重県三重郡川越町
振出人　谷口石油精製株式会社　取締役社長　谷口　晃
受取人　中部ボイラーサービス株式会社
裏書人　中部ボイラーサービス株式会社
被裏書人　申立人
最終所持人　申立人

平成12年(へ)第10号
新潟県上越市大豆2丁目14番26号
申立人　赫巻　カツ
公示催告期日　平成13年3月15日午前10時
平成12年8月2日　高田簡易裁判所
(別紙)　目　録
銘柄　株式会社ナルス株券
種類枚数　100株券1枚
記号番号　0012568
一株の金額　50円
最終名義人　赫巻　至
最終所持人　申立人