情報セキュリティに関する「情報通信ネットワーク 安全・信頼性基準」の見直しについて

情報セキュリティに関する「情報通信ネットワーク 安全・信頼性基準」（以下「安全・信頼性基準」という。）の見直しにあたって、以下の項目について検討を行った。

1．他の情報セキュリティに関するガイドラインとの比較

安全信頼性基準と、特に整合性の確認が必要と考えられる2つのガイドラインとの比較を行った。

1．1 内閣官房情報セキュリティセンターの「重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針（第3版）対策編」との比較

当該指針には存在して、安全・信頼性基準にはない情報通信ネットワークのセキュリティに関する項目の照合を行った（照合結果は別添のとおり）。照合した結果、安全・信頼性基準は当該指針をほぼカバーしていると考えられる。

1．2 （社）電気通信事業者協会の「電気通信分野における情報セキュリティ確保に係る安全基準（第2版）」との比較

1．1と同様に照合を行った（詳細な照合結果は別添のとおり）。当該基準については、1．1の指針を参考に策定されたものであるため、照合結果も同様となった。

2．「情報通信ネットワーク 安全・信頼性基準」と情報セキュリティに関する事故事例との比較

最近の情報セキュリティに関する事故について、事故の要因となった問題点を公開された情報から分析し、安全・信頼性基準と照らし合わせ、安全・信頼性基準に不足している項目はないか確認を行った。確認結果は、次ページのとおりであり、安全・信頼性基準に記載されている項目によって、事故の要因となった問題点をカバーできていることが確認できた。

２．１　レンタルサーバ業者の事故　（その他の電気通信事業ネットワークに該当）

（同社の第三者調査委員会による調査報告書を参考に作成）

２．１．１　事故の概要

特定のサーバー群に対して実施されたメールシステム障害解消のためのメンテナンスを実施したところ、更新プログラムの不具合により、顧客の大量のデータが消失した。本来更新プログラムはプライマリーディスクのみにあてられるものの、社内マニュアルを無視した担当者の独自仕様により同一筐体内のバックアップディスクにも同時に適用してしまい、データの復元が不可能となった。

その後、消失した大量のデータを復元するために、十分に検証を行わずにオープンソースソフトウェアの復元プログラムを用いて、消失データの復元を実行し、リカバードファイルを顧客に提供したところ、第三者のデータが含まれていたことが判明した。

２．１．２　安全・信頼性基準との比較

事　故	問題点	安全信頼性基準の該当箇所	対　策
・データの消失 ・メール送受信不可	データの復元ができない	別表第１　設備等基準 第１　設備基準 １　一般基準 （10）ソフトウェアの信頼性向上対策	ウ　システムデータ等の重要データの復元ができること。
	プライマリーディスクとバックアップディスクの同時更新	別表第１　設備等基準 第１　設備基準 １　一般基準 （10）ソフトウェアの信頼性向上対策	イ　ソフトウェア及びデータを変更するときは、容易に誤りが混入しないよう措置を講ずること。
	プログラムによってデータの完全消去が可能	別表第１　設備等基準 第１　設備基準 １　一般基準 （10）ソフトウェアの信頼性向上対策	イ　ソフトウェア及びデータを変更するときは、容易に誤りが混入しないよう措置を講ずること。

	システム変更に関する社内マニュアルの無視	別表第2　管理基準 2　ネットワーク施工管理 (2)作業工程の明確化等	作業工程を明確にするとともに、その管理を行うこと。
	同一筐体内へのバックアップ保存	別表第2　管理基準 6　データ管理 (5)ファイル等の遠隔地保存	重要なプログラム、システムデータ及び利用者に関するデータのファイル等については、前世代及び現世代のものを地域的に十分隔たった場所に別に保管すること。
第三者に他者のデータを提供	十分な検証もないまま復元プログラムの使用	別表第1　設備等基準 第1　設備基準 1　一般基準 （10）　ソフトウェアの信頼性向上対策	ア　ソフトウェアを導入する場合は、品質の検証を行うこと

2．2　オンラインゲーム業者の事故　（その他の電気通信事業ネットワークに該当）

（経済産業省ニュースリリースを参考に作成）

2．2．1　事故の概要

同社のオンラインサービスのサーバーへの不正侵入により、数千万人の利用者の個人情報が流出した。事故後の調査で、同社のオンラインサービスの委託先において、CIOなどの情報セキュリティに関する専門的な責任者が不在であること、異常発生時における報告連絡体制に係る規程等の未整備であること、公知の脆弱性について自社の確認体制が整えられていないこと、委託先との間で個人情報の取扱等、安全管理措置を遵守させる契約が締結されていないこと等、情報セキュリティ対策が十分に講じられていないことが指摘された。

2．2．2　安全・信頼性基準との比較

事　故	問　題　点	安全信頼性基準の該当箇所	対　策
個人情報の漏えい	ネットワークへの不正侵入	別表第1　設備等基準 第1　設備基準 1　一般基準 （10）　ソフトウェアの信頼性向上対策	オ　ソフトウェアには、サイバー攻撃等に対する脆弱性がないように対策を継続的に講ずること。

		別表第1　設備等基準 第1　設備基準 1　一般基準 （11）情報セキュリティ対策	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こと
	情報セキュリティに関する専門的な責任者の不在	別表第3　情報セキュリティポリシー策定のための指針 2　情報セキュリティの管理 （1）方針立案 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。
	異常発生時における報告連絡体制に係る規程等の未整備	別表第2　管理基準 9　非常事態への対応 （1）　体制の明確化	ア　連絡体系、権限の範囲等の非常時の体制を明確にすること。
	公知の脆弱性に対する自社の確認体制の未整備	別表第2 5　情報セキュリティ管理 （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。
	委託先との間に個人情報の取扱等、安全管理措置を遵守させる契約の未締結	別表第2 3　ネットワーク保全・運用 （6）委託保守運用管理	ア　保守の委託を行う場合は、契約書等により保守作業の範囲及び責任の範囲を明確にすること。

2．3　電気通信事業者の事故　（電気通信回線設備事業用ネットワークに該当）

（同社報道資料を参考に作成）

2．3．1　事故の概要

同社の業務委託先の元社員によって不正プログラムが投入され、基地局に設置された ATM 伝送装置の内部データが破損し、基地局とセンター設備の間で通信がで

きなくなった。これにより、3G回線を利用した音声・パケット通信等のサービスが使用しづらくなった。

２．３．２　安全・信頼性基準との比較

事　故	問　題　点	安全信頼性基準の該当箇所	対　策
通信サービスが使用しづらい	業務委託先の元社員による情報セキュリティの脅威	別表第2 3 ネットワーク保全・運用 （6）委託保守運用管理	ア 保守の委託を行う場合は、契約書等により保守作業の範囲及び責任の範囲を明確にすること。 イ 保守を委託する場合は、作業手順を明確にするとともに、監督を行うこと。
	不正プログラムの混入	別表第1　設備等基準 第1　設備基準 1　一般基準 （11）情報セキュリティ対策	ケ コンピュータウイルス及び不正プログラム混入対策を講ずること。
	不正プログラムによるATM伝送装置の内部データの破損	別表第1　設備等基準 第1　設備基準 1　一般基準 （11）情報セキュリティ対策	シ 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取を防止する措置を講ずること。

２．４「標的型サイバー攻撃の事例分析と対策レポート」（（独）情報処理推進機構（2012年1月））　（ユーザネットワークに該当）

２．４．１　概要

国内企業、衆議院・参議院が、外部から情報窃取型の標的型攻撃メールを送付され、添付されていたウイルスがシステム内部に侵入し、情報が流出してしまう事故が発生した。これを受けて、（独）情報処理推進機構が標的型サイバー攻撃への対策レポートを発行した。このレポートに記載されている対策と安全・信頼性基準との比較を行った。

２．４．２　安全・信頼性基準との比較

事　故	対　策	安全信頼性基準の該当箇所	対　策
情報 漏えい	1）システム入り口での防御 ・ファイアウォール ・最新のウイルス対策ソフト ・侵入検知／防止システム	別表第１　設備等基準 第１　設備基準 １　一般基準 （１１）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 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　コンピュータウイルス及び不正プログラム混入対策を講ずること。 ナ　ネットワークの不正使用を防止する措置を講ずること。
	2）脆弱性対策 ・OS やサーバーソフトウェアの定期的な脆弱性診断 ・OS やサーバーソフトウェアに関する脆弱性情報の時期を逸しない収集と修正プログラムの適用 ・ウェブアプリケーションへの脆弱性の作り込みの回避 ・ウェブアプリケーションファイアウォール（WAF）	別表第１　設備等基準 第１　設備基準 １　一般基準 （１０）　ソフトウェアの信頼性向上対策	オ　ソフトウェアには、サイバー攻撃等に対する脆弱性がないように対策を継続的に講ずること。 ケ　定期的にソフトウェアを点検し、リスク分析を実施すること。
		別表第１　設備等基準 第１　設備基準 １　一般基準 （１１）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。
		別表第２ ５　情報セキュリティ管理 （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。

	3) 標的型攻撃ルートでの対策 ・スパムフィルタ ・URL フィルタ ・外部メディア利用規則、強制利用抑止	別表第1 設備等基準 第1 設備基準 1 一般基準 （11）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 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。 シ 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取を防止する措置を講ずること。
		別表第2 3 ネットワーク保全・運用管理 (4) 監視、保守及び制御	イ 情報通信ネットワークの動作状況を監視し、必要に応じ、接続規制等の制御措置を講ずること。
	4) ウイルス活動の阻害および抑止 （出口対策） ・端末間、他部署間のネットワーク通信の制限（ウイルスの組織内蔓延抑止） ・組織の端末からの外部通信はプロキシを経由させる等の経路制御 ・組織内ネットワーク量の監視（異常さを早期に検知しウイルスの蔓延を早期に発見） ・知財等のある重要なサーバーはインターネットから隔離	別表第1 設備等基準 第1 設備基準 1 一般基準 （11）情報セキュリティ対策	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。 エ インターネットへ接続する場合は、開放網と閉域網とを区別したネットワーク構成を採用すること。 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こと。 シ 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取を防止する措置を講ずること。
	5) アクセス制御 ・ ユーザ認証 ・ アクセスするプログラムの特定（ホワイトリスト化）	別表第1 設備等基準 第1 設備基準 1 一般基準 （11）情報セキュリティ対策	サ 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 シ 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取を防止する措置を講ずること。
	6) 情報の暗号化 ・ 通信路の暗号化（Virtual Private Network などの利用） ・ ファイルの暗号化 ・ 暗号鍵管理	別表第1 設備等基準 第1 設備基準 1 一般基準 （11）情報セキュリティ対策	テ 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。
		別表第2 6 データ管理 （4）データの記録物の管理	ア 設備の仕様及び設置場所等のデータ並びに利用者に関するデータの記録物については、重要度による分類及び管理を行うこと。
		別表第2 6 データ管理 （6）重要データの漏えい防止対策	重要な設備情報（特に他社のセキュリティ情報等）の漏えいを防止するための適切な措置を講ずること。
	7) システム監視、ログ分析 ・ ネットワークログ取得・分析 ・ サーバログ取得・分析 ・ アクセスログの監査（DB 監査ツールなど含む）	別表第1 設備等基準 第1 設備基準 1 一般基準 （11）情報セキュリティ対策	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。
	8) 管理統制およびコンテンジェンシープラン（事前準備・事後対応） ・ セキュリティポリシーの徹底 ・ 海外を含むグループ会社間でのセキュリティガバナンス ・ 危機対応体制の整備	別表第2 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。

	標的型攻撃メールが届いた場合の対応	別表第2 10　教育･訓練 (2)教育・訓練の内容	キ　情報セキュリティに関する教育･訓練を行うこと。

目次

別表第１　設備等基準・・・・・・・・・・・・・・・・・・・・・・・・１

別表第２　管理基準・・・・・・・・・・・・・・・・・・・・・・・・・８

別表第３　情報セキュリティポリシー策定のための指針・・・・・・１４

別表第４　危機管理計画策定のための指針・・・・・・・・・・・・・１９

【実施指針について】 ◎：実施すべきである。　○ ：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○・・・基準への反映 △・・・解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業	その	自営	ユー			
第1　設備基準								
(10)ソフトウェアの信頼性向上対策	ア ソフトウェアを導入する場合は、品質の検証を行うこと。	◎	◎	◎＊	◎＊			
	イ ソフトウェア及びデータを変更するときは、容易に誤りが混入しないよう措置を講ずること。	◎	◎	◎＊	◎＊			
	ウ システムデータ等の重要データの復元ができること。	◎	◎	◎＊	◎＊			
	エ ソフトウェアには、異常の発生を速やかに検知、通報する機能を設けること。	○	○	○	○			
	オ ソフトウェアには、サイバー攻撃等に対する脆弱性が無いように対策を継続的に講ずること。	◎	◎	◎＊	◎＊	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（イ）情報セキュリティに付いての脅威【要検討事項】 セキュリティホール、不正プログラム及びサービス不能攻撃など様々な脅威に対して、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。 ○サービス不能攻撃 ・通信フィルタリング ・通信回線の冗長化 ・通信事業者との連携 ・電子計算機、通信回線装置及び通信回線の監視と記録	
						電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	3．（1）共通 ネットワークを脅威から保護するために、また、ネットワークを用いた業務用システム及び業務用ソフトウェア（処理中の情報を含む。）のセキュリティを維持するために、ネットワークを適切に管理し、制御しているか	
	カ モバイルインターネット接続サービスにおいて、新しいシステムの導入に当たっては、実際に運用する場合と同一の条件や環境を考慮し、ハードウェアの初期故障、ソフトウェアのバグによる障害が可能な限り発生しないよう十分なシミュレーションを実施すること。	◎	◎	―	―			
	キ IP系接続サービスにおいては、現用及び予備機器の切替えを行うソフトウェアは十分な信頼性を確保すること。	◎	◎	―	―			
	ク ソフトウェアの導入、更新にあたってはウイルス等の混入を防ぎ、セキュリティを確保すること。	◎	◎	◎＊	◎＊			
	ケ 定期的にソフトウェアを点検し、リスク分析を実施すること。	◎	◎	○	○			
(11)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。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	3．（2）サイバー攻撃対策 サイバー攻撃（DDoS攻撃等）から、サーバ、ルータ、その他のIPネットワーク設備を保護するため、特定の通信が攻撃に使用される場合を想定し、物理又は論理ポートや、IPアドレス、プロトコル毎に、IT障害を防止するために必要最小限の範囲で通信フィルタリング又は帯域制御を行なうことを可能としているか サービスによっては、信号処理レベルでの通信制御や、利用者認証、アクセス権限管理等と連動した通信フィルタリング等を行なうことを可能としているか	

【実施指針について】 ◎：実施すべきである。　○ ：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○・・・基準への反映 △・・・解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業	その	自営	ユー			
	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、開放網と閉域網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。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（イ）情報セキュリティに付いての脅威【要検討事項】 セキュリティホール、不正プログラム及びサービス不能攻撃など様々な脅威に対して、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。 ○セキュリティホール ・情報収集 ・対応計画の策定 ・対応内容の記録 ・定期チェック ・不正アクセスの監視・検出（IDSの使用） ・通信フィルタリング（ファイアウォール） ・外部ネットワークからの遮断等 ・アンチウイルスソフトウェアの使用（端末、ゲートウェイ）、メンテナンス、定期検査、セキュリティパッチ適用 ・利用していない通信ポート等の非活性化、マクロ実行の抑制 ・早期発見・早期回復対策（監視、障害の検出、障害箇所の切り分け、障害時の縮退・再構成、取引制限、リカバリ機能）	
	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こと。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（ア）情報セキュリティ確保のために求められる機能【要検討事項】 主体認証（利用者及び機器等の認証）、アクセス制御、権限管理、証跡管理、負荷分散、冗長化など基本的な情報セキュリティ機能の観点から、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。	
						電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	システム上に格納されている重要情報への不正アクセスを検知するための措置を講じているか	
	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。	◎	◎	◎	◎			

【実施指針について】 ◎：実施すべきである。　○ ：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目	対策	実施指針				資料名	内容	
		事業	その	自営	ユー			
	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。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	3.（2）サイバー攻撃対策 定期的に、及び必要に応じて随時に、セキュリティパッチ等を適用することにより、サイバー攻撃に利用される恐れがあるソフトウェア等の脆弱性を修復しているか セキュリティパッチ等の適用のための具体的運用方法を定めているか	
	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。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（イ）情報セキュリティに付いての脅威【要検討事項】 セキュリティホール、不正プログラム及びサービス不能攻撃など様々な脅威に対して、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。 ○不正プログラム ・情報収集 ・OS／アプリケーションのセキュリティ設定 ・アンチウイルスソフトウェアの導入 ・パターンファイルの更新 ・パッチ適用 ・定期的なウイルス検査	
						電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	3.（2）サイバー攻撃対策 電気通信サービス利用者又は他の事業者の電気通信設備から受信したプログラム等により、事業者の意図に反する動作を行なうこと等により電気通信サービスの提供に重大な支障を及ぼすことがないよう、電気通信設備は必要な防護措置を講じているか	
	コ ネットワークの機能を管理・運営するコンピュータから重要な情報が漏えいしないように、電磁波の低減対策、又は電磁環境に配慮した上で漏えい電磁波をマスクする措置を講ずること。	◎＊	◎＊	◎＊	◎＊			
	サ 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。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（ア）情報セキュリティ確保のために求められる機能【要検討事項】 ○主体認証 ・主体認証機能の導入 ・主体認証技術の選択（知識、所有、生体認証、及び多要素認証等） ・利用者IDの管理 ・主体認証情報の管理（暗号化、パスワードの定期変更・最低文字数の制限等） ・利用者の責任（パスワードの利用、端末管理、クリアデスク・クリアスクリーン方針） ・不正使用検知時における主体認証の利用停止措置	

【実施指針について】 ◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○・・・基準への反映 △・・・解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業	その	自営	ユー			
						電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	3．（1）共通 すべての情報システム及びサービスへのアクセスを許可及び無効とするために、利用者の登録・登録削除についての正式な手順を備えているか 特権の割当て及び利用は、制限し、管理しているか 利用することを特別に認可したサービスへのアクセスだけを、利用者に提供しているか 遠隔利用者のアクセスを管理するために、適切な認証方法を利用しているか 3．（2）サイバー攻撃対策 サイバー攻撃の踏み台として発信者身元偽装に悪用されないため、利用者認証を行なうシステムにおいて、パスワードの厳格な管理や、強い認証機能の導入等、不正アクセス対策を徹底しているか 3．（3）重要情報漏えい対策 システム利用にあたりアクセス管理を行うために、利用者の識別・認証等のシステムを導入し、アクセス制限等を実施しているか	
	シ 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取を防止する措置を講ずること。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（ア）情報セキュリティ確保のために求められる機能【要検討事項】 ○アクセス制御 ・アクセス制御機能の導入 ・利用者アクセスの管理（利用者登録、特権管理、利用者パスワードの管理、利用者アクセス権のレビュー等） ・ネットワークのアクセス制御方針の策定	
						電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1．（1）共通 情報システムを監査するツールの誤用又は悪用を防止するために、それらのツールへのアクセスが抑制されているか 2．（1）共通 あらゆる形式の通信設備を利用した情報交換を保護するために、正式な交換方針、手順及び管理策を備えているか 2．（2）サイバー攻撃 外部からアクセス可能なサーバ等に格納された情報について、その利用者に対する利用の許容範囲を定め、適切なアクセス管理を実施しているか	
	ス 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。	○	○	○	○			
	セ アクセス失敗回数の基準を設定するとともに、基準値を越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。	○	○	○	○			

【実施指針について】 ◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○・・・基準への反映 △・・・解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業	その	自営	ユー			
	ソ 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。	○	○	○	○	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	3.（3）重要情報漏えい対策 利用者のアクセス履歴を記録し、定期的に監査を実施しているか	
	タ 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。	○	○	○	○			
	チ 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。	○	○	○	○			
	ツ 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。	○	○	○	○			
	テ 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。	○	○	○	○			
	ト 適切な漏話減衰量の基準を設定すること。	◎	◎	◎＊	◎＊			
	ナ ネットワークの不正使用を防止する措置を講ずること。	○	○	○	○			
第2　環境基準								
1　センターの建築物								
(1)立地条件及び周囲環境への配慮	ア 強固な地盤上の建築物を選定すること。ただし、やむを得ない場合であって、不同沈下を防止する措置を講ずる場合は、この限りでない。	◎	◎	◎＊	◎＊	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	4.（1）共通 装置は、環境上の脅威及び災害からのリスク並びに認可されていないアクセスの機会を低減するように設置又は保護されているか	
	イ 風水害等を受けにくい環境の建築物を選定すること。ただし、やむを得ない場合であって、防風、防水等の措置を講ずる場合は、この限りでない。	◎	◎	◎＊	◎＊			
	ウ 強力な電磁界による障害のおそれのない環境の建築物を選定すること。ただし、やむを得ない場合であって、通信機械室等に電磁シールド等の措置を講ずる場合は、この限りでない。	◎	◎	◎	◎			
	エ 爆発や火災のおそれのある危険物を収容する施設に隣接した建築物は回避すること。	○	○	○	○			
(2)建築物の選定	ア 耐震構造であること。	◎	◎	◎＊	◎＊			
	イ 建築基準法（昭和25年法律第201 号）第2条に規定する耐火建築物又は準耐火建築物であること。	◎	◎	◎＊	◎＊			
	ウ 床荷重に対し、所要の構造耐力を確保すること。	◎	◎	◎	◎			
(3)入出制限機能	ア 建築物の出入口には、施錠機能を設けること。	◎	◎	◎	◎			

【実施指針について】 ◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○・・・基準への反映 △・・・解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業	その	自営	ユー			
	イ 通常利用する出入口には、設備の重要度に応じた適切な入出管理機能を設けること。ただし、これに準ずる措置を講ずる場合は、この限りでない。	◎	◎	◎	◎			
	ウ セキュリティを保つべき領域の具体的な基準を設定し、運用すること。	◎	◎	◎	◎			
(4)火災の検知、消火	ア 自動火災報知設備を適切に設置すること。	◎	◎	◎＊	◎＊			
	イ 消火設備を適切に設置すること。	◎	◎	◎	◎			
2　通信機械室等								
(1)通信機械室の位置	ア 自然災害等の外部からの影響を受けるおそれの少ない場所に設置すること。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	4.（1）共通 電気通信事業を提供するための交換設備等の電気通信設備を収容する施設の物理的なセキュリティを設計し、適用しているか 電気通信事業を提供するために電気通信設備が設置された部屋の物理的なセキュリティを設計し、適用しているか 電気通信事業を提供するために電気通信設備を設置している物理的に隔離された運用区画の物理的なセキュリティを設計し、適用しているか	
	イ 第三者が侵入するおそれの少ない場所に設置すること。ただし、第三者が容易に侵入できないような措置が講じられている場合は、この限りでない。	◎	◎	◎	◎			
	ウ 浸水のおそれの少ない場所に設置すること。ただし、やむを得ない場合であって、床のかさ上げ、防水壁等の措置を講ずる場合又は排水設備を設置する場合は、この限りでない。	◎	◎	◎＊	◎＊			
	エ 強力な電磁界による障害のおそれの少ない場所に設置すること。ただし、やむを得ない場合であって、電磁シールド等の措置を講ずる場合は、この限りでない。	◎	◎	◎	◎			
(2)通信機械室内の設備等の設置	ア 保守作業が安全かつ円滑に行える空間を確保すること。	◎	◎	◎	◎			
	イ じゅう器等には、通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。	◎	◎	◎	◎			
(3)通信機械室の条件	ア 重要な設備を収容する通信機械室は、専用に設け、十分な強度を持つ扉を設けること。	◎	◎	◎＊	◎＊			
	イ 床、内壁、天井等に使用する内装材は、通常想定される規模の地震による落下、転倒等を防止する措置を講ずること。	◎	◎＊	◎＊	◎＊			
	ウ 床、内壁、天井等に使用する内装材には、建築基準法第2条に規定する不燃材料又は建築基準法施行令（昭和25年政令第338号）第1条に規定する準不燃材料若しくは難燃材料を使用すること。	◎	◎＊	◎＊	◎＊			
	エ 静電気の発生又は帯電を防止する措置を講ずること。	◎＊	◎＊	◎＊	◎＊			
	オ 通信機械室に電源設備等を設置する場合は、必要に応じ、電磁界による障害を防止する措置を講ずること。	◎	◎	◎	◎			

【実施指針について】 ◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第1　設備等基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）〔○・・・基準への反映 △・・・解説への反映〕
項目	対策	実施指針				資料名	内容	
		事業	その	自営	ユー			
	カ 通信機械室の貫通孔には、延焼を防止する措置を講ずること。	◎＊	◎＊	◎＊	◎＊			
(4)入出制限機能	ア 出入口には、施錠機能を設けること。	◎	◎	◎	◎			
	イ 重要な設備を収容する通信機械室の出入口には、入出管理機能を設けること。また、設備の重要度に応じた適切な入出管理機能を設けること。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	4．（1）共通 情報及び情報処理施設のある領域を保護するために、物理的セキュリティ境界（例えば、壁、カード制御による入口、有人の受付）を用いているか セキュリティを保つべき領域は、認可された者だけにアクセスを許すことを確実にするために、適切な入退管理策によって保護されているか	
	ウ セキュリティを保つべき領域の具体的な基準を設定し、運用すること。	◎	◎	◎	◎			
(5)データ類の保管	ア システムデータ等の重要なデータは、データ保管室又は専用のデータ保管庫に収容すること。	◎	◎	◎＊	◎＊			
	イ データ保管室及びデータ保管庫には、施錠機能を設けること。	◎	◎	◎＊	◎＊			
	ウ データ保管室及びデータ保管庫には、必要に応じ、電磁界による障害を防止する措置を講ずること。	◎	◎	◎	◎			
	エ データ保管庫には、通常想定される規模の地震による転倒及び移動を防止する措置を講ずること。	◎	◎	◎＊	◎＊			
	オ データ保管室及びデータ保管庫には、必要に応じ、耐火措置を講ずること。	◎	◎	◎＊	◎＊			
(6)火災の検知、消火	ア 自動火災報知設備を適切に設置すること。	◎	◎	◎	◎			
	イ 消火設備を適切に設置すること。	◎	◎	◎	◎			

【実施指針について】 ◎：実施すべきである。　○ ：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）（○・・・基準への反映　△・・・解説への反映）
項目	対策	実施指針				資料名	内容	
		事業	その	自営	ユー			
1.ネットワーク設計管理								
(5)品質・機能検査の充実化	ウ セキュリティ対策の手法、事前確認を十分行うこと。	◎	◎	◎	◎			
2.ネットワーク施工管理								
(4)委託工事管理	ウ 外部委託における情報セキュリティ確保のための対策を行うこと。	◎	◎	◎	◎			
3.ネットワーク保全・運用管理								
(6)委託保守管理	ア 保守の委託を行う場合、契約書により保守作業の範囲及び責任の範囲を明確にすること。	◎	◎	◎	◎			
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。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティの基本方針の策定 ○自己点検・内部監査の実施 ・情報セキュリティ対策の見直し	
						電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1．組織・体制及び資源の対策 （1）共通 情報セキュリティ基本方針は、あらかじめ定められた間隔で、又は重大な変化が発生した場合に、それが引き続き適切、妥当及び有効であることを確実にするためにレビューされているか	
(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。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(2)イ(ウ)不正アクセスによる脅威への対策【要検討事項】 保護すべき情報が保存されたPCや外部記録媒体の盗難、紛失及び当該PCや外部記録媒体からの情報漏えいを防止するための措置や、保護すべき情報を処理するウェブやメール等のアプリケーションからの情報の漏えいを防止するための措置が明示されるべきである。	
(3)情報セキュリティ監査の実施	監査のチェック項目の策定と定期的な内部･外部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。	◎	◎	○	○	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア　組織・体制及び資源の対策 （ア）組織・体制及び人的資源の確保【要検討事項】 ○自己点検・内部監査の実施 ・自己点検の実施 ・内部監査の実施 ・情報セキュリティ対策の見直し （ウ）外部監査等による情報セキュリティ対策の評価【参考事項】 技術的な対策は多くの事業者で行われているが、今後は外部監査等による情報セキュリティ対策の評価を行うことが望ましい。 ・情報セキュリティ監査等の実施 ・情報セキュリティ対策の見直し	
(4)コンピュータウィ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。	◎	◎	－	－			

【実施指針について】 ◎：実施すべきである。　○：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）（○・・・基準への反映　△・・・解説への反映）
項目	対策	実施指針						
		事業	その	自営	ユー	資料名	内容	
	イ コンピュータウィ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。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1.（1）共通 社会環境や技術環境等の変化に伴ってIT障害を引き起こす新たな脅威が顕在化した際、それらの脅威を要因とするIT障害によるサービスへの影響等を考慮し、必要に応じて適切な対策を導入しているか	
(6)知識・技能を有する者の配置	情報セキュリティに関する資格の保有者等一定以上の知識・技能を有する者を配置すること。	◎＊	◎＊	◎＊	◎＊	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1.（1）共通 電気通信サービスを安定的かつ確実に提供するため、情報セキュリティに関する専門的な知識・技能を有する者を配置しているか そのような人材を配置・育成等するための具体的な計画を策定しているか	
(7)情報セキュリティに関する利用者への周知	情報通信ネットワークに対して利用者が与える又は情報通信ネットワークの利用者が受ける可能性のある影響とその対策について利用者に周知すること。	◎	◎	－	－	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1.（1）共通 電気通信サービスの提供又は電気通信設備の運用における情報セキュリティ確保の取組み状況に係り、その実施体制や対策状況などを、提供する情報の範囲に留意しつつ、利用者等が容易に知りえる方法によって公表しているか	
(8)社内の重要情報の管理	ア ネットワーク内の装置類やサービスの属性に応じた情報を分類すること。	◎	◎	◎	◎			
	イ 情報管理に関する内部統制ルールを整備すること。	◎	◎	◎	◎	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	2.（1）共通 情報及び情報処理施設と関連する資産のすべてについて、組織の中に、その管理責任者を指定しているか 組織に対しての価値、法的要求事項、取扱いに慎重を要する度合い及び重要性の観点から、情報を分類しているか 2.（3）重要情報漏えい対策 各組織における重要情報の管理責任者を組織の長に定めて、重要情報の管理に努めているか 重要情報の範囲を明確にし、管理すべき重要情報について、重要情報管理責任者の管轄組織毎に保管リストを作成・維持しているか 重要情報へのアクセスはログ取得・保管を義務付け、その管理方法・運用ルールを定めているか	
(9)サイバー攻撃に備えた管理体制	サイバー攻撃発生時の迅速な情報共有方法を確立すること。	◎	◎	－	－	電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1.（2）サイバー攻撃対策 情報セキュリティインシデントに対する迅速、効果的で整然とした対応を確実にするため、責任体制及び手順を確立しているか	
6.データ管理								

【実施指針について】 ◎：実施すべきである。　○ ：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目	対策	実施指針				資料名	内容	
		事業	その	自営	ユー			
(1)体制の明確化	作業の分担、連絡体系、責任の範囲等のデータ管理体制を明確にすること。	◎	◎	◎	◎			
(2)基準の設定	データ管理基準を設定すること。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）イ（イ）情報の取扱い【要検討事項】 情報の作成、入手、利用、保存、移送、提供及び消去等、情報のライフサイクルに着目し、各段階における情報セキュリティ対策が明示されるべきである。 ○情報の作成と入手 ・目的外の作成・入手の禁止 ・台帳等作成 ・作成・入手時における情報の格付けと取扱制限の決定 ・作成時点の情報の格付けの継承 ・格付けの変更手続き ○情報の利用 ・情報の利用に関する許可及び届出に係る措置 ・目的外利用の禁止 ・格付け及び取扱制限に従った情報の取扱い ・格付け及び取扱制限の見直し ・アクセス履歴の保存 ・アクセス制御・出力制御 ・離席時の対策（端末ロック等） ○情報の保存 ・格付けに応じた情報の保存（アクセス制御、記録媒体の保管、パスワード・電子署名・暗号化による保護、バックアップ・複写、更新履歴管理の取扱い等の記載） ・情報の保存期間に従った管理 ○情報の移送 ・情報の移送に関する許可及び届出に係る措置 ・作業責任者・手続きの明確化 ・作業担当者の識別、認証、権限付与 ・移送手段の選択 ・書面の保護対策 ・電磁的記録の保護対策（パスワード設定、暗号化、電子認証等）） ○情報の提供 ・提供に関する許可及び届出 ・付加情報の削除 ○情報の消去 ・情報の消去に関する許可及び届出 ・電磁的記録の消去手続き（消去の確認、消去記録の保管等） （1）ウ（ア）情報セキュリティ確保のために求められる機能 ○権限管理 ・権限管理機能の導入 ・利用者IDと主体認証情報の付与管理 ・利用者IDと主体認証情報における代替手段等の適用 ○証跡管理 ・証跡管理機能の導入実施 ・証跡取得と保存 ・取得した証跡の点検、分析及び報告 ・証跡管理に関する利用者への周知	

【実施指針について】 ◎：実施すべきである。　○ ：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）（○・・・基準への反映　△・・・解説への反映）
項目	対策	実施指針				資料名	内容	
		事業	その	自営	ユー			
(3)作業の手順化	データ取扱作業の手順化を行うこと。	◎	◎	◎	◎			
(4)データの記録物の管理	ア 設備の仕様及び設置場所等のデータ並びに利用者に関するデータの記録物については、重要度による分類及び管理を行うこと。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）イ（ア）情報の格付け【要検討事項】 取扱う情報について、その重要度に応じた適切な措置を講じるため、機密性、完全性、可用性の観点から、情報の格付け（ランク）や、取扱制限（例：複製禁止、持出禁止、再配布禁止）が明示されるべきである。 ○重要性に応じた適切な措置 ・試算の洗出し（体制。洗出し項目、洗出し基準等） ・情報のライフサイクルと情報の格付けに応じた情報セキュリティ対策	
						電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	2．（1）共通 すべての資産を明確に識別し、また、重要な資産すべての目録を作成し、維持しているか 2．（3）重要情報漏えい対策 重要情報の全社的な管理方針に基づく情報のランク付けにより、その重要度に応じた取扱いを行なっているか 重要情報の具体的な取扱い方法を定めているか 情報に括り付けられたランクの表示方法、及び、ランクに応じた保管ルールとその運用方法を定めているか	
	イ 設備の仕様及び設置場所等のデータ並びに利用者に関するデータに対する従事者の守秘義務の範囲を明確にするとともに、その周知、徹底を図ること。	◎	◎	◎	◎			
	ウ 利用者の暗証番号等の秘密の保護に配慮すること。	◎	◎	◎	◎			
	エ 記録媒体の性能向上やシステム間の接続の拡充などによるリスク・脅威の拡大に応じた適時の点検・見直しを行うこと。	◎	◎	◎	◎			
(5)ファイル等の遠隔地保管	重要なプログラム、システムデータ及び利用者に関するデータのファイル等については、前世代及び現世代のものを地域的に十分隔たった場所に別に保管すること。	○	○	○	○			
(6)重要データの漏えい防止対策	個人情報以外の重要な設備情報（特に他社のセキュリティ情報等）の漏えいを防止するための適切な措置を講ずること。	◎	◎	○	○	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（2）イ（ア）保護すべき情報の類型化【要検討事項】 漏えい対策の対象となる保護すべき情報を類型化し、明示されるべきである。 ○保護すべき情報の類型化 ・情報分類の指針、情報のラベル付け及び取扱い、重要情報の格付け ・情報資産の洗出し方法（体制、洗出し項目、洗出し基準）、情報、情報システムについてのランク付け ・情報資産の機密性、完全性、可用性に基づく分類 ・安全管理上の重要度に応じた分類（安全性が損なわれた場合の影響の大きさに応じた分類） ・個人データ取扱台帳の整備、リスクアセスメント結果に応じた分類	

【実施指針について】 ◎：実施すべきである。　○ ：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）（○・・・基準への反映 △・・・解説への反映）
項目		対策	実施指針			資料名	内容	
			事業	その	自営	ユー		
							（2）イ（イ）保護すべき情報の管理 保護すべき情報及び当該情報が記録された媒体を安全に取扱う（作成、入手、利用、保存、移送、提供及び消去等）ための措置が明示されるべきである。 ○情報の作成と入手 ・目的外の作成・入手の禁止 ・台帳等作成 ・作成・入手時における情報の格付けと取扱制限の決定 ・作成時点の情報の格付けの継承 ・格付けの変更手続き ○情報の利用 ・情報の利用に関する許可及び届出に係る措置 ・目的外利用の禁止 ・格付け及び取扱制限に従った情報の取扱い ・格付け及び取扱制限の見直し ・アクセス履歴の保存 ・アクセス制御・出力制御 ・離席時の対策（端末ロック等） ・要保護情報の利用にあたっての措置（情報交換の方針及び手順、取外し可能な媒体の管理、重要情報の内部漏えい、盗難、紛失、流出への対策） ・書類や電子媒体の持ち出し管理（書類等の保管ルール、端末への資料の保管、持出しに関するルールや制限） ○情報の保存 ・格付けに応じた情報の保存（アクセス制御、記録媒体の保管、 パスワード・電子署名・暗号化による保護、バックアップ・複写、 更新履歴管理の取扱い等の記載） ・情報の保存期間に従った管理 ・安全な場所への保管（自然災害を被る可能性が低い地域への保管、外部記録媒体の耐火、耐熱、耐水及び耐湿を講じた施設への保管） ・内容表示の記号化（媒体等に保存情報内容が想定できるタイトル表示をすることの禁止） ・バックアップの分散、隔地保管 ○情報の移送 ・情報の移送に関する許可及び届出に係る措置 ・作業責任者・手続きの明確化 ・作業担当者の識別、認証、権限付与 ・移送手段の選択 ・書面の保護対策 ・電磁的記録の保護対策（パスワード設定、暗号化、電子認証等） ○情報の提供 ・情報の提供に関する許可及び届出 ・付加情報の削除 ○情報の消去 ・情報の消去に関する許可及び届出 ・電磁的記録の消去手続き（消去の確認、消去記録の保管等）	

【実施指針について】 ◎：実施すべきである。　○ ：実施が望ましい。　－：対象外。
◎＊：技術的な難易度等を考慮して段階的に実施すべきである。

別表第2　管理基準

情報通信ネットワーク　安全・信頼性基準						根拠資料		論点（方向性）（○・・・基準への反映　△・・・解説への反映）
項目	対策	実施指針				資料名	内容	
		事業	その	自営	ユー			
						電気通信分野における情報セキュリティ確保に係る安全基準（第2版）	1．（2）イ（イ）保護すべき情報の管理 重要情報の管理について全社的な管理責任者を定め、重要情報に対する全社的な管理方針を定めているか 1．（5）重要情報漏えい対策 重要情報の管理について全社的な管理責任者を定め、重要情報に対する全社的な管理方針を定めているか	
7.環境管理								
(1)建築物の保全	保全点検を定期的に行うこと。	◎	◎	◎	◎			
(2)空気調和設備の保全	保全点検を定期的に行うこと。	◎	◎	◎	◎			
8.防犯管理								
(1)体制の明確化	防犯体制を明確にすること。	◎	◎	◎	◎			
(2)管理の手順化	防犯管理の手順化を行うこと。	◎	◎	◎	◎			
(3)建築物、通信機械室等の入出管理	建築物、通信機械室等の入出管理を行うこと。	◎	◎	◎	◎	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）エ（ア）施設と環境【要検討事項】 入退出の管理や安全区域の確保、停電時、断水時の対応等情報システムの設置・運用に係る施設や環境面での対策が明示されるべきである。 ○入退出の管理 ・入退出管理（障壁、施錠、主体認証、入退出履歴の記録、継続的に立ち入る者の承認、侵入監視装置の設置、最小限の施設表示） ・訪問者、清掃業者及び物品の搬出入業者の管理（身分の記録、入室審査手順、立ち入り制限区域の設定、職員等の立ち会い・付き添い、ストラップ・ID カード、情報システムに接触できない場所での受け渡し）	
(4)かぎ、暗証番号等の管理	出入口のかぎ及び暗証番号等の適切な管理を行うこと。	◎	◎	◎	◎			
(5)防犯装置の管理	防犯装置の保全点検を定期的に行うこと。	◎	◎	◎	◎			
(6)入出管理記録の保管	入出管理記録は、一定の期間保管すること。	○	○	○	○			
9.非常事態への対応								
(1)体制の明確化	ア 連絡体系、権限の範囲等の非常事態時の体制を明確にすること。	◎	◎	◎	◎			
	イ 非常事態時における社員・職員、復旧に必要な業務依託先などへの連絡手段、社員・職員の参集手段の確保等の体制を整えること。	◎	◎	○	○			
	ウ 非常事態時における広域応援体制を明確にすること。	○	○	○	○			
	エ 相互接続を行う事業者等の間において、非常災害時の連絡体制や連絡内容を明確にすること。	◎	◎	○	○			
	オ 非常事態時における応急活動、復旧活動に際しては、国等の関係機関との連絡体制を明確にすること。	◎	◎	○	○			
	カ 非常事態時において、応急活動、復旧活動にかかわる連絡手段を確保するために必要な措置を講ずること。	◎	◎	○	○			
(2)復旧対策の手順化	復旧対策の手順化を行うこと。	◎	◎	◎	◎			
10.教育・訓練								
(1)体制の明確化	教育・訓練に関する計画の策定及び実施を行う体制を明確にすること。	◎	◎	◎＊	◎＊	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ア（イ）情報セキュリティの人材の育成等【参考事項】 知的財産としての「人財」という観点から、情報セキュリティ人材の育成や要員の管理を行うことが望ましい。	
(2)教育・訓練の内容	キ 情報セキュリティに関する教育・訓練を行うこと。	◎	◎	◎	◎			

別表第3　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準		根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目	対策	資料名	内容	
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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティ基本方針の策定	
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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティに関する組織体制の整備（責任者・責任部門・委員会等の設置、役割・責任分担の明確化等）	
(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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○教育・訓練の実施 ・情報セキュリティ対策の教育・訓練計画の策定 ・教育・訓練実施記録の保管	
(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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティ関係規程の整備（違反への対処、例外措置等）	
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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・IT障害発生時の体制・対応手順の整備（「重要インフラの情報セキュリティ対策に係る第2次行動計画」が想定するサイバー攻撃、非意図的要因、災害や疾病等の脅威が引き起こすIT障害に関わる情報の集約及び共有体制を含む）	
(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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○自己点検・内部監査の実施 ・自己点検の実施 ・内部監査の実施 (ウ)外部監査等による情報セキュリティ対策の評価【参考事項】 ・情報セキュリティ監査等の実施	

別表第3　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準		根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目	対策	資料名	内容	
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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ア（ア）組織・体制及び人的資源の確保【要検討事項】 ○自己点検・内部監査の実施 ・情報セキュリティ対策の見直し （ウ）外部監査等による情報セキュリティ対策の評価【参考事項】 ・情報セキュリティ対策の見直し	
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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ア（ア）組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティに関する組織体制の整備（責任者・責任部門・委員会等の設置、役割・責任分担の明確化等）	
(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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ア（ア）組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティ基本方針の策定	
(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。			

別表第3　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準		根拠資料		論点（方向性）（○･･･基準への反映　△･･･解説への反映）
項目	対策	資料名	内容	
(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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（2）イ（ア）保護すべき情報の類型化【要検討事項】 ○保護すべき情報の類型化 ・情報分類の指針、情報のラベル付け及び取扱い、重要情報の格付け ・情報資産の洗出し方法（体制、洗出し項目、洗出し基準）、情報、情報システムについてのランク付け	
(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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（2）イ（ア）保護すべき情報の類型化【要検討事項】 ○保護すべき情報の類型化 ・情報資産の機密性、完全性、可用性に基づく分類 ・安全管理上の重要度に応じた分類（安全性が損なわれた場合の影響の大きさに応じた分類）	
(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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ア（ア）組織・体制及び人的資源の確保【要検討事項】 ○組織・体制の確立 ・情報セキュリティ基本方針の策定	
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。				
【構成例のため、以下省略。】				
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。			

別表第3　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準		根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目	対策	資料名	内容	
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16年総務省告示第695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、情報システムの使用権を、必要な者に、必要な期間与え、情報システムの利用資格に関する義務・責任を明確化する。また、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。			

別表第3　情報セキュリティポリシー策定のための指針

情報通信ネットワーク　安全・信頼性基準					根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目				対策	資料名	内容	
			(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 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。			

別表第4　危機管理計画策定のための指針

情報通信ネットワーク　安全・信頼性基準		根拠資料		論点（方向性）（○･･･基準への反映　△･･･解説への反映）
項目	対策	資料名	内容	
1　目的				
危機管理計画は、サイバーテロについてあらかじめ対処方法を定めておくことで、実際にサイバーテロが発生した場合に迅速な対応を可能とし、早期に現状へ復旧し、被害の拡大を防ぐことを目的とするものである。この指針は、電気通信事業用ネットワークにおいてサイバーテロが発生した場合の緊急対応体制を整備するため、危機管理計画策定の指針として定めたものである。 電気通信事業用ネットワーク以外のネットワークにおける危機管理計画についても対象とするネットワーク、想定される攻撃等を考慮し、本指針を参考として策定されることが望ましい。				
2　サイバーテロの定義等				
(1)　サイバーテロの定義	サイバーテロは、コンピュータウィルスやハッカーによつて個人が被害を受けるものとは異なり、国家等の重要システムを機能不全に陥れるものであることから、この指針におけるサイバーテロの定義は、「ネットワークを通じて各国の国防、治安等をはじめとする各種分野の情報システムに侵入し、データを破壊、改ざんするなどの手段で国家等の重要システムを機能不全に陥れる行為」とする。			
(2)　攻撃対象となる重要インフラ	サイバーテロの攻撃対象となつた場合、その産業、企業のみならず、広く国民生活に重大な影響が及ぶこととなる重要インフラとして、情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス（地方公共団体を含む）等が想定される。			
(3)　重要インフラの相互依存性	各重要インフラは、他の重要インフラと独立して存立するのではなく、相互に依存し存立しており、ある重要インフラが攻撃を受けた場合、関連する他の重要インフラも影響を受ける場合が多々あることから、重要インフラを保有してサービスを提供する事業者は、他インフラへの影響も考慮した対策が必要である。			
(4) 主な攻撃方法				
サイバーテロにおける主な攻撃方法の具体例としては、次のものがある。				
ア　物理的な攻撃	電気通信施設に不正侵入し、ネットワーク管理センターを占拠する等によりネットワークのコントロールを奪い、これをまひさせるような攻撃			
イ　ホームページ改ざん	思想的な意図等により社会に広くアピールするため、ホームページの掲載内容を改ざんするもの			
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　コンピュータウィルス	強力な感染力と破壊力を持つウィルスによる攻撃			
オ　不正侵入（なりすまし）	他人になりすまして侵入し、データの改ざん、削除を行うほか、他への攻撃にも使用			
3　危機管理計画の策定				
危機管理計画の策定に当たつて配慮すべき内容を以下に示す。				
(1) 対象				
ア 攻撃				
対象とするべき電気通信ネットワークのぜい弱な部分の具体例は次のとおりである。これを参考として、各電気通信事業者の状況により大規模な影響が出ることを想定し、対象となる攻撃を明確に規定する。				
(ｱ) 固定・移動電話網	物理的な攻撃、意図的なふくそうによる攻撃			
(ｲ) 移動電話網	電波による不正アクセス、電波による通信妨害			
(ｳ) 専用回線網及び中継回線網	電波妨害			
(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) ネットワークの機	電磁波による情報漏えい			
イ 被害規模の対象範囲				

別表第4　危機管理計画策定のための指針

情報通信ネットワーク　安全・信頼性基準			根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目		対策	資料名	内容	
		各電気通信事業者の状況により大規模な影響が出ることを想定して、被害規模の対象範囲を明確に規定する。 その際には、電気通信事業法施行規則（昭和60 年郵政省令第25 号）第58 条の報告を要する重大事故の基準も参考とする。			
(2) 予防					
必要に応じて次のハッカー対策、コンピュータウィルス対策等を規定し、サイバーテロに対する予防措置を					
ア インターネットに接続するための機器の配置及び構成		(ｱ) ファイアウォール等を設置して適切な設定を行う。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（イ）情報セキュリティについての脅威【要検討事項】 セキュリティホール、不正プログラム及びサービス不能攻撃など様々な脅威に対して、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。	
		(ｲ) 非武装セグメント構成を採用する。			
		(ｳ) 開放網と閉域網とを区別したネットワーク構成を採用する。			
		(ｴ) telnetやftp等サービス提供に不用な通信の接続制限を行う。			
		(ｵ) 最新の情報セキュリティ技術を採用する。			
		(ｶ) 攻撃元を特定できる機能と攻撃元のトラヒックを遮断する仕組み等を採用す			
イ ソフトウェア上の対策		(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) 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。			
ウ 監視、管理等		(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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（ア）情報セキュリティ確保のために求められる機能【要検討事項】 主体認証（利用者及び機器等の認証）、アクセス制御、権限管理、証跡管理、負荷分散、冗長化など基本的な情報セキュリティ機能の観点から、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。	
		(ｲ) コンピュータからの漏えい電磁波の低減対策、又は電磁環境に配慮した上で漏えい電磁波をマスクする措置を講ずる。			
エ 不正アクセス防止のためのシステム上の設定		(ｱ) 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。			
		(ｲ) 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取を防止する措置を講ずる。			
		(ｳ) 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。			
		(ｴ) 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。			
		(ｵ) 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。			
		(ｶ) ネットワークへのアクセス履歴の表示又は照会が行える機能を設ける。			
		(ｷ) 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。			
		(ｸ) 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。			
		(ｹ) アクセスにおける本人認証手段には、端末認証（MACアドレス、シリアル番号等）や生体認証（指紋、静脈等）など、高度な認証方式の導入を検討する事が望ましい。			
オ 通信の秘密の保護		(ｱ) 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。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）エ（エ）通信回線及び通信回線装置【要検討事項】 ○構築時 ・通信の暗号化 ・通信性能の確保	
		(ｲ) 適切な漏話減衰量の基準を設定する。			
カ ネットワークの不正使用の防止		ネットワークの不正使用を防止する措置を講ずる。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（ア）情報セキュリティ確保のために求められる機能【要検討事項】 主体認証（利用者及び機器等の認証）、アクセス制御、権限管理、証跡管理、負荷分散、冗長化など基本的な情報セキュリティ機能の観点から、当該情報システムへ導入すべき情報セキュリティ要件が明示されるべきである。	

別表第4　危機管理計画策定のための指針

情報通信ネットワーク　安全・信頼性基準			根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目		対策	資料名	内容	
キ 新たな手法による攻撃に対するハード・ソフト対策の体制強化		ネットワークシステムの脆弱性に対処できるように内部統制や社内ルールを随時見直し、新たな手法による攻撃に対しても迅速にハード・ソフト両面で対処できる体制を確立・強化する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）ウ（ア）情報セキュリティ確保のために求められる機能【要検討事項】 ○自己点検・内部監査の実施 ・内部監査の実施 ・情報セキュリティ対策の見直し	
ク 他の利用者へ悪影響を与えている利用者に対する一時利用停止の明確化		他の利用者に悪影響を与えている事象を洗い出し、当該事象への対応方針を策定し、利用者の合意形成を図る。			
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					
(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			重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（1）エ（エ）通信回線及び通信回線装置【要検討事項】 通信回線及び通信回線装置の構築から運用、運用終了又は停止に至るまでの対策が明示されるべきである。	
	(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、攻撃側サーバーの速やかな停止を依頼する。			
		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			
		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) 伝送交換設備への攻撃からの復旧対策	A 重要な伝送路設備には、応急復旧用ケーブルの配備等の応急復旧対策を講ずる。			
		B 移動用交換設備の配備等の応急復旧対策を講ずる。			
		C 災害時等において、衛星地球局等の無線設備により、臨時電話等の設置が可能であること。			
		D 移動体通信基地局と交換局の間の回線に障害が発生した場合等に、無線設備により、臨時に対向の電気通信回線の設定が可能であること。			
		E 移動体通信基地局に障害が発生した場合等に、可搬型無線基地局により、臨時の電気通信回線の設定が可能であること。			
		F 他の伝送設備の障害時に、通信の疎通が著しく困難となつた場合、予備の設備等により臨時の電気通信回線の設定が可能であること。			
イ 緊急時における対処には、高度な判断を必要とする場合があることから、責任と権限を有する適切な者が速やかに判断を行うことができるように規定する。			重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	（2）ア（ア）事業継続性確保のための個別対策の実施【要検討事項】 ○未然防止措置 ・指揮命令系統の明確化 ・権限委譲、代行順位の決定	
ウ 複数の電気通信事業者に障害が発生し、その影響が波及して被害が拡大していくことが想定されることから、障害情報等を交換し被害を最小限に抑えるために、国、電気通信事業者、事業者団体等の関係者間で連絡体制、運用方法を明確に規定する。					
(4) 原因判明時の措置		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 障害の発生状況及び影響の拡大防止に対する協力に関して、電気通信事業者から利用者への周知方法等について規定する。			
		ウ 障害の発生原因が判明し、再度攻撃にさらされるおそれがある場合における障害の発生防止のため、必要な措置を講じることを規定する。			
		エ ネットワークを介して、他分野の重要インフラ事業者と情報システムを相互接続している場合には、サイバーテロ対策に関し互いの連絡・連携体制を必要に応じ構築する。			

別表第4　危機管理計画策定のための指針

情報通信ネットワーク　安全・信頼性基準		根拠資料		論点（方向性）（○･･･基準への反映 △･･･解説への反映）
項目	対策	資料名	内容	
(5) 危機管理計画の見直し等	ア 技術の進展に伴い、サイバーテロによる攻撃方法等が、変化していくと考えられるため、適宜危機管理計画の見直しを行うことを規定する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ウ(ア)情報セキュリティ確保のために求められる機能【要検討事項】 ○自己点検・内部監査の実施 ・内部監査の実施 ・情報セキュリティ対策の見直し	
	イ サイバーテロが発生した際の対処を円滑に行えるよう、必要に応じサイバーテロの発生を想定した訓練を実施することを規定する。	重要インフラにおける情報セキュリティ確保に係る「安全基準等」策定にあたっての指針 対策編	(1)ア(ア)組織・体制及び人的資源の確保【要検討事項】 ○教育・訓練の実施 ・情報セキュリティ対策の教育・訓練計画の策定 ・教育・訓練実施記録の保管	