（別紙3）

参考資料

令　和　３　年　５　月　12　日

電気通信事業ガバナンス検討会

事　　務　　局

安全・信頼性対策に関する制度における関連規定

（データの安全管理及びサイバーセキュリティ対策関係抜粋）

事業用電気通信設備規則（抜粋）

（事業用電気通信設備の防護措置）

第六条　事業用電気通信設備は、利用者又は他の電気通信事業者の電気通信設備から受信したプログラムによつて当該事業用電気通信設備が当該事業用電気通信設備を設置する電気通信事業者の意図に反する動作を行うことその他の事由により電気通信役務の提供に重大な支障を及ぼすことがないよう当該プログラムの機能の制限その他の必要な防護措置が講じられなければならない。

（事業用電気通信設備を設置する建築物等）

第十五条　事業用電気通信設備を収容し、又は設置する建築物及びコンテナ等は、次の各号に適合するものでなければならない。（略）

四　当該事業用電気通信設備を収容し、又は設置する通信機械室に、公衆が容易に立ち入り、又は公衆が容易に事業用電気通信設備に触れることができないよう施錠その他必要な措置が講じられていること。

（通信内容の秘匿措置）

第十七条　事業用電気通信設備（特定端末設備を除く。以下この節、次節及び第四節において同じ。）は、利用者が端末設備等を接続する点において、他の通信の内容が電気通信設備の通常の使用の状態で判読できないように必要な秘匿措置が講じられなければならない。

２　有線放送設備の線路と同一の線路を使用する事業用電気通信設備（電気通信回線設備に限る。）は、電気通信事業者が、有線一般放送の受信設備を接続する点において、通信の内容が有線一般放送の受信設備の通常の使用の状態で判読できないように必要な秘匿措置が講じられなければならない。

（蓄積情報保護）

第十八条　事業用電気通信設備に利用者の通信の内容その他これに係る情報を蓄積する場合にあつては、当該事業用電気通信設備は、当該利用者以外の者が端末設備等を用いて容易にその情報を知得し、又は破壊することを防止するため、当該利用者のみに与えた識別符号の照合確認その他の防止措置が講じられなければならない。

電気通信事業法施行規則（抜粋）

（管理規程）

第二十九条　法第四十四条第二項の総務省令で定める管理規程の内容は、次のとおりとする。

一　電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の方針に関する事項

ホ　情報セキュリティの確保のための方針に関すること。

三　電気通信役務の確実かつ安定的な提供を確保するための事業用電気通信設備の管理の方法に関する事項

ハ　事業用電気通信設備の設計、工事、維持及び運用に関すること。

ホ　情報セキュリティ対策に関すること。

リ　防犯対策に関すること。

総務省告示第六十七号（抜粋）

電気通信事業法施行規則第二十九条第二項※に規定する細目は、次の表の上欄に掲げる区分に従い、それぞれ同表の下欄に掲げるものとする。

事業用電気通信設備の設計、工事、維持及び運用に関すること	（１）設備の設定におけるデータの誤設定及び誤り入力防止並びに関連する設備間の設定の整合性に関すること。 （２）設備の不具合を事前に発見するための設備の試験に関すること。 （１３）維持及び運用に関すること。 （１４）通信の秘密の確保に関すること。
ソフトウェアの信頼性の確保に関すること	（３）定期的なソフトウェアのリスク分析及び更新に関すること。
ふくそう、事故、災害その他非常の場合の報告、記録措置及びに周知に関すること	（２）速やかな故障の検知及び故障設備の特定に関すること。
利用者の利益の保護の観点から行なう利用者に対する情報提供に関すること	（３）利用者が理解しやすい情報の提供に関すること。
事故の再発防止のための対策に関すること	（１）事故発生時の記録に基づく事故の内容・原因の分析・検証に関する具体的な取組及び再発防止策の策定に関すること。 （２）事故の内容・原因・再発防止等、事故の収束後の情報公開に関すること。

※電気通信事業法施行規則
第二十九条（管理規定）
（略）
第二項
前項各号に掲げる事項には、総務大臣が別に告示する細目を含むものでなければならない。

管理規程記載マニュアル（抜粋）

１．事業用電気通信設備の管理の方針に関する事項

（ホ）情報セキュリティの確保のための方針に関すること。

・情報セキュリティ確保のための基本方針の策定及び見直しに関すること。
（ガイドライン：安信基準別表第３「情報セキュリティポリシー策定のための指針」）

・基本方針の公表に関する取組。

・不正アクセス等への対処を定めた危機管理計画の策定及び見直しに関すること。
（ガイドライン：安信基準別表第４「危機管理計画策定のための指針」）

管理規程記載マニュアル（抜粋）

３．事業用電気通信設備の管理の方法に関する事項

（ハ）事業用電気通信設備の設計、工事、維持及び運用に関すること。

(13)維持及び運用の委託に関すること。

・業務委託先の選別の評価要件に関すること。
・保守の委託契約の中に含める内容に関すること。
・委託した保守作業の監督に関すること。

(14)通信の秘密の確保に関すること。

・通信の秘密に属する事項（通信内容のほか、通信当事者の住所・氏名、発信・受信場所及び通信年月日等通信の構成要素並びに通信回数等通信の存在の事実の有無を含む。）の保管方法・ファイル保管室等への入退室管理など、上記情報へのアクセスの制限方法

（ホ）情報セキュリティ対策に関すること。

・情報の分類及び重要情報の管理に関すること。
・情報の管理に関する内部統制ルール
・情報漏えい防止対策
・外部委託時の情報セキュリティ対策
・サイバー攻撃への対処
・情報セキュリティに関する最新の技術情報等を踏まえた情報セキュリティ対策の見直し。
・定期的な監査の実施に関すること。
・監査の確認項目の策定に関すること。
・監査結果を踏まえた情報セキュリティ対策全体の見直しに関すること。
・サプライチェーンリスクを考慮した対策に関すること。

（リ）防犯対策に関すること。

・防犯管理の手順化に関すること。
・建築物、通信機械室等の入出管理に関すること。
・出入口の鍵及び暗証番号等の適切な管理に関すること。
・防犯装置の定期的な保全点検に関すること。
・入出管理記録の保管に関すること。

情報通信ネットワーク安全・信頼性基準（抜粋）

別表第１　設備等基準

第１　設備基準

１．一般基準

（８）情報通信ネットワークの動作状況の監視等

コ　インターネットの経路制御情報等の制御信号のうち不要又は不正なものの送受信を防ぐために有効な機能を設けること。

（９）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。

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。

（１０）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、ｆｔｐ等サービス提供に不要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機能を設けること。

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　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抑圧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。

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。

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。

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。

タ　ネットワークへのアクセス履歴の表示又は照会を行う機能を設けること。

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接続する場合に、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。

情報通信ネットワーク安全・信頼性基準（抜粋）

別表第１　設備等基準（続き）

第１　設備基準

２．屋外設備

(13) 第三者の接触防止

ア　設備に第三者が容易に触れることができないような措置を講ずること。

イ　とう道等には、施錠等の侵入を防止する措置を講ずること。

第２　環境基準

１．センターの建物等

(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。

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。

２．通信機械室等

(1)通信機械室の位置

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。

(2)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。

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。

３．空気調和設備

(2)空気調和設備室への入出制限

出入口には、施錠機能を設けること。

情報通信ネットワーク安全・信頼性基準（抜粋）

別表第２　管理基準

第１　方針

4. 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）情報セキュリティポリシーの公表

情報セキュリティポリシーを公表すること。

（3）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。

第２　体制

2. 各段階における体制

（4）情報セキュリティ対策

ア 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。

イ 外部委託先を含めた作業の分担、連絡体系、責任の範囲等の情報セキュリティ対策体制及びデータ管理体制を明確にすること。

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。

（9）防犯対策

ア 防犯体制を明確にすること。

イ 防犯管理の手順化を行うこと。

情報通信ネットワーク安全・信頼性基準（抜粋）

別表第２　管理基準（続き）

第3. 方法

1. 平常時の取組

(2)教育・訓練

キ 防犯に関する教育・訓練を行うこと。

ク 情報セキュリティに関する教育・訓練を行うこと。

(3)設計

エ 重要な機器を調達する場合は、サプライチェーンにおける情報セキュリティを考慮した機器を調達すること

(5)維持・運用

シ 通信の秘密の確保に関する取組を実施すること。

(6)情報セキュリティ対策

ア 情報セキュリティに関する情報収集を行うこと。

イ 情報セキュリティ対策についてその手法及び事前確認を十分行うこと。

ウ 最新の情報セキュリティに関する技術情報や業界の動向を入手し、それらを情報セキュリティ対策に反映させること。

エ コンピュータウィルス並びに端末及びソフトウェアの脆弱性に関する情報を入手したときは、必要に応じて、緊急連絡先に直ちに連絡すること。

オ コンピュータウィルス並びに端末及びソフトウェアの脆弱性に関する情報を入手したときは、必要に応じて、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サイトへの掲示、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。

カ ネットワーク内の装置類やサービスの属性に応じて情報を分類すること。

キ データ管理基準を設定すること。

ク 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。

ケ データ取扱作業の手順化を行うこと。

コ 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。

サ 利用者の暗証番号等の秘密の保護に配慮すること。

シ 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や脅威の拡大に応じた適時の点検及び見直しを行うこと。

ス 情報管理に関する内部統制ルールを整備すること。

セ 監査時における確認項目の策定と定期的な内部監査及び外部監査を実施し、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。

ソ 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。

タ サイバー攻撃への対策を講ずるとともに、発生時には迅速に情報共有する方法を確立すること。

チ 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つた場所に別に保管すること。

ツ コンピュータウィルス又は不正プログラムが混入した際に、情報通信ネットワークに対して利用者が与え、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。

別表第２　管理基準（続き）

第3. 方法

1. 平常時の取組

(11)防犯対策

ア 防犯管理の手順化を行うこと。
イ 入出管理記録は、一定の期間保管すること。
ウ 建築物、通信機械室等の入出管理を行うこと。
エ 出入口の鍵、暗証番号等の適切な管理を行うこと。
オ 建築物、防犯装置等の保全点検を定期的に行うこと。
キ 防犯に関する教育・訓練を行うこと。
ク 情報セキュリティに関する教育・訓練を行うこと。

情報通信ネットワーク安全・信頼性基準（抜粋）

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。

情報通信ネットワーク安全・信頼性基準（抜粋）

別表第３　情報セキュリティポリシー策定のための指針（続き）

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。

⑴　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。

⑵　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。

⑶　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。

⑷　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。

別表第３　情報セキュリティポリシー策定のための指針（続き）

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。

情報通信ネットワーク安全・信頼性基準（抜粋）

別表第４　危機管理計画策定のための指針

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

情報通信ネットワーク安全・信頼性基準（抜粋）

別表第４　危機管理計画策定のための指針（続き）

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)　ネットワークの機能を管理・運営するコンピュータ

電磁波による情報漏えい

イ　被害規模の対象範囲

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図る。

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。

(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る。

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。

情報通信ネットワーク安全・信頼性基準（抜粋）

別表第４　危機管理計画策定のための指針（続き）

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。

(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。

(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。

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。

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

情報通信ネットワーク安全・信頼性基準（抜粋）

別表第４　危機管理計画策定のための指針（続き）

(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。

(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)　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。

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　当該障害がサイバーテロによるものであることが判明した場合は、一定のルートで国、電気通信事業者、事業者団体等の関係者に通知することが可能なよう、(3)ウと同様に伝達ルート等をあらかじめ定めておく。

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。

(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。

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。

情報通信ネットワーク安全・信頼性基準 解説（抜粋）

第1 設備基準
1. 一般基準

（８）情報通信ネットワークの動作状況の監視等
コ　インターネットの経路制御情報等の制御信号のうち不要又は不正なものの送受信を防ぐために有効な機能を設けること。

解説

インターネットの経路制御情報（通信の到達性を確保するため、各事業者が設定し、接続する事業者間であらかじめ送受信されるものであり、当該情報に基づいてパケットの転送経路の制御が行われる。）等制御信号のうち不要又は不正なものの送受信を防ぐために有効な機能を設ける。

経路制御情報は、ある事業者の誤設定により大量かつ詳細な経路制御情報が不要に送信又は受信されてしまうと、他の事業者に広範囲かつ甚大な影響を及ぼすことが想定される。同様に、不正な経路制御情報が送信又は受信されてしまうと、他の事業者に重大な影響を及ぼす懸念がある。

インターネットの安定性を確保するため、不要又は不正な経路制御情報をルータにおいてフィルターする仕組みや、一定量以上の経路制御情報を受け取らないようリミッターを設定する仕組みがあり、このような設定は、経路制御情報の受信防止又は送信防止の有効な手段になり得る。

例えば、他の電気通信事業者から経路制御情報を受信する際は、Prefixフィルター※1により、細かい経路制御情報を受信しないよう設定したり、AS-PATHフィルター※2により、長いAS-PATH長の経路を受信しないよう設定したり、リミッターにより、設定した閾値以上の経路制御情報を受信しないよう設定したりする対応が考えられる。また、経路制御情報を他の電気通信事業者等に配信する際は、Prefixフィルターにより、自らのAS内部で使用している細かい経路制御情報をそのまま外部に配信しないようにする設定が考えられる。

しかしながら、こうした設定が自らの利用者や他事業者にも影響を与える恐れがあることから、各事業者がそれぞれのネットワーク構成及び他事業者との接続状況等を熟知した上で当該設定の影響を十分に検討し、かつ、それぞれの運用の考え方に照らして、柔軟かつ適切な設定を行うことが重要である。

なお、不要又は不正な経路制御情報の送受信による障害の発生を防止するためには、あらかじめ接続先と当該情報の送受信の範囲を明確にすることも有効である。

※1　Prefixは、IPアドレスの中のネットワークアドレスを示す部分をいう。Prefixの長さはアドレス空間の深さを表し、PrefixフィルターはそのPrefixの長さを基にフィルタリングを行うフィルターをいう。
※2　ASはAutonomous Systemの略で、ある経路制御方針によって運営されるネットワークのことをいう。宛先に到達するまでに経由したASのリストをAS-PATHといい、AS-PATHフィルターはこのAS-PATHを基にフィルタリングを行うフィルターをいう。

第1 設備基準
1. 一般基準

(9) 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。

サイバー攻撃等に関する最新の情報収集に努め、ソフトウェアに脆弱性が発見された場合には、迅速なパッチ適用等によりいち早く脆弱性を取り除く等、各事業者が検討して必要な対策を講じることが適当である。

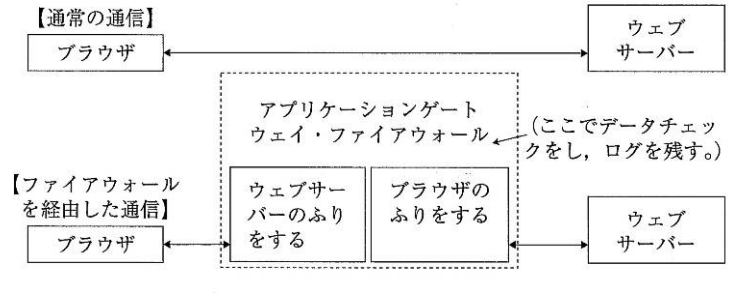
ク ソフトウェアの導入又は更新に当たつては、ウイルス等の混入を防ぎ、セキュリティを確保すること。

情報通信ネットワークにおいてソフトウェアの重要性が増大しており、信頼性の高いソフトウェアを採用することやソフトウェア更新時の信頼性を確保することが必要である。

(10) 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。

ファイアウォールは、インターネットからサイト等への入口で関所的な役割を果たすもので、その仕組みから、大きく分けるとパケットの伝送をコントロールする「パケットフィルタリング」と通信を中継するプロキシ・プログラムを使用する「アプリケーションゲートウェイ」の２つの機能に分けられる。

●措置例●
このような機能を理解し、ファイアウォールを導入し、適切な設定を行い運用することが必要である。
ファイアウォールの導入に当たっては、ファイアウォールの二重化等効果的な方法を専門業者に委託することも考えられる。



アプリケーションゲートウェイの機能の例

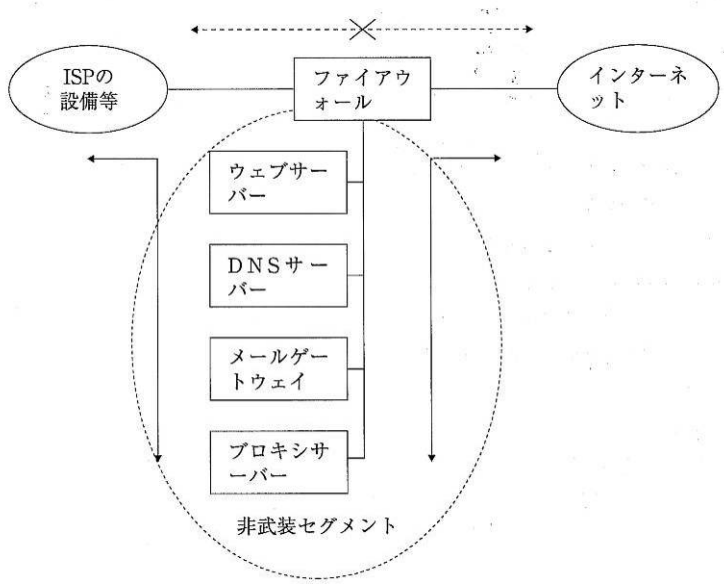
イ　インターネットへ接続する場合は、非武装セグメント構成を採用すること。

解説

非武装セグメント（DMZ: demilitarized zone）は、ファイアウォールに接続されるセグメントであり、インターネット側又は内部ネットワーク側からアクセスできる。ファイアウォールに加えて、このDMZを設けることにより、内部ネットワークへのアクセスは、DMZサーバ群からのみ許容されインターネットから直接アクセスすることを制限するため、内部ネットワークのサーバへの外部からの不正アクセスに対し、信頼性を高めることができる。

●措置例●

外部のインターネットと内部のネットワークの間にファイアウォールを設置し、そのファイアウォールに接続される非武装セグメントを構成し、このセグメントに公開用WEBサーバ、メールサーバ等を配置する。



非武装セグメントの例

ウ　インターネットへ接続する場合は、telnet、ftp等サービス提供に不要な通信の接続制限を行うこと。

解説

不正アクセス等を回避するためtelnet（システムリモート制御プロトコル）やftp（ファイル転送プロトコル）等については、外部からのアクセスの制限を行うなどとともに、サーバが提供するサービスについても必要最小限のサービスに限定することが必要である。

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。

解説

インターネットは不特定多数の者が利用するネットワークであるため、広く一般に公開するネットワークとセキュリティの確保が不可欠な自社内ネットワークは、区別したネットワーク構成とする必要がある。

●措置例●

開放網と閉域網とのネットワーク構成については、物理的に明確に区別させる方法と仮想閉域網（VPN：Virtual private network）により措置する方法の２つがある。このうち仮想閉域網については、暗号化や認証技術等を使用して閉域網を構成するものである。

オ　インターネットへ接続する場合は、サーバ等におけるセキュリティホール対策を講ずること。

解説

セキュリティホールは、ハッカーからの攻撃の標的となるところから、これを未然に防止するため、最新のセキュリティホール情報の収集やセキュリティホール検知ソフト等の活用により、セキュリティホールの検知に努めることと、これが確認された場合、最新のパッチの投入を行うなど適切、かつ、迅速な対応が必要である。

●措置例●

１　適時なソフトウェアのバージョンアップの実施、又はパッチの適用
２　セキュリティホールとなるdaemon（基本的なプロセスをバックグラウンドで実行するプログラム）の停止
３　最新のセキュリティ情報に基づく対応の実施

等

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機能を設けること。

解説

ネットワークやサーバ等の重要部分の監視は、ハッカー等からの脅威を防止する意味からも重要であり、また、異常が発見された時の対応も含め、対応体制を確立しておくことが必要である。

●措置例●

具体的な対応としては、第１に、不正アタックや侵入者の検知等を行うIDS（intrusion detection system：侵入検知システム）の導入が挙げられるが、このシステムは、急速な発展を遂げているところであり、システムの導入・更改に当たっては最新のシステムの導入が必要である。

また、侵入が検知された場合の通報者、通報方法等についてもシステム導入時点において決定しておくことが必要である（無線呼出により通報するようなシステム構成も可能である）。

第２には、日常的な監視体制の確立や攻撃を受けた際の対応手順をあらかじめ決めておくこと、重要ファイルのバックアップ、情報セキュリティ技術のスキルアップ等の取り組みが必要である。

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。

解説

情報セキュリティ対策として有効な手段といわれているのは、ネットワーク等の監視と一体的にセキュリティ対策上重要なログの記録及び保存を行い、その解析により適切な措置を講ずることである。

ログは、ネットワークやサーバ等で発生した各種の情報を記録、保存できるものであるが、適切なログ管理を行うためにはログの定期チェックなどの体制整備が不可欠である。

なお、ログは「通信の秘密」に属する事項であるが、セキュリティ対策のため必要かつ相当な範囲でログを保存することは正当な業務行為として違法性がないものと考えられる。しかし、通信の秘密の保護の観点からは、その取扱いには特に慎重な配慮が必要であり、原則として取扱規程においてその保存期間を適切に定め、保存期間を超えたものは遅滞なく消去することが必要である。

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。

解説

インターネットでは、不特定多数の者がアクセスを行い、その中に悪意を持った第三者によるサイバーテロの脅威が存在するおそれがある。インターネットでサイバーテロを防御するには、「自分の家の鍵は自分でかける」といった自衛が基本である。サイバーテロの手法はコンピュータ技術の進展に伴い、日々多様化する傾向にあるため、その対策に関してもできる限り継続的に最新の情報セキュリティ技術を採用することが必要である。

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。

解説

コンピュータウイルスは、新種のウイルスが日々大量に発生する中で、被害の拡大も危倶されるところであり、ウイルスの種類によっては、自らが加害者となる危険性がある。したがって、各機関から発せられるウイルス情報の収集など日常的に危機意識を持ち、何時でも適切な対応が可能な体制づくりが必要である。

ネットワーク上からパスワードを取得して自動送出する不正プログラムやDDoS攻撃に加担する不正プログラム等の混入についても同様に、日常的な危機意識の醸成が不可欠である。

（参考） DDoS攻撃

DDoS（Distributed Denial of Service：分散協調型サービス拒否）攻撃とは、複数の場所からWWWサーバなどに処理能力を超える大量のデータを送りつける等の方法により、そのサーバなどをダウンさせる攻撃である。

●措置例●

1　常駐監視機能を持ったウイルス対策ソフトを使用
2　ウイルス対策ソフトに使用するウイルスパターンファイルは常に最新のものを利用
3　クライアントPC、ファイルサーバ、メールサーバ等について、それぞれウイルス対策ソフトを導入
4　外部アクセスが可能なネットワークには、ウイルス侵入をリアルタイムで警告する機能を持ったウイルス対策ソフトを利用

等

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抑圧する措置を講ずること。

ネットワークの機能を管理・運営するコンピュータから企業情報や個人情報等の重要な情報が漏えいしないように対策を講じる必要がある。

漏えい電磁波の主な発生部位としてCRTディスプレイ、信号ケーブル等があげられるところから、この部分への措置が必要である。

●措置例●

1　CRTディスプレイに代えて液晶ディスプレイを使用
2　信号ケーブルについては、光ファイバーケーブルを使用
3　筐体等からの電磁波漏えいについては、情報機器そのもののシールドに加えて、建物全体又は通信機械室等をシールド
4　電源ラインやコネクタ部分等からの電磁波漏えいについては適切なフィルタを挿入
5　CRTディスプレイ等から漏えいする電磁波の信号と類似の信号を発生させることにより、漏えいする電磁波から情報が分離することができないように電磁環境に十分配慮して情報をマスク

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。　等

当事者に対して固有のパスワード等の情報を付与し、それを直接キー入力するか又はIDカード、ICカード等に蓄積し読み取らせることやディジタル署名等により、正当な利用者の識別・確認を行う機能を設ける。又は、声紋、指紋等の個人にとって固有な事象を判別することにより、本人の識別・確認を行う。

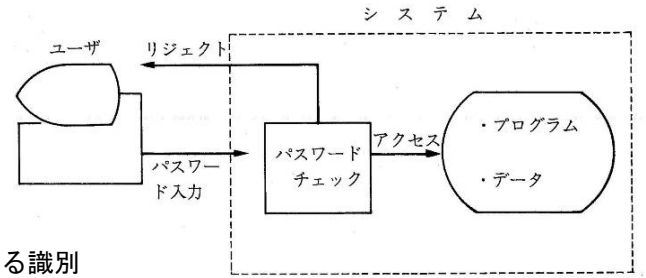
●措置例●

1　パスワードによる識別、確認方法

利用者の識別、確認の手段の中でもパスワードによる方法は、IDカード、鍵などと組み合わせて多くのシステムで採用されており、英数字及び特殊文字を含む４～８桁の文字から構成されるのが一般的である。パスワードの桁数は、利用者の総数と、人間が容易に記憶できる長さとの兼ね合いで決定される。

なお、パスワードの漏えいの防止の観点から、パスワードを画面に表示したり、プリンタに印字したりするなどしてパスワードが第三者の目に触れることのないよう、充分な配慮がなされなければならない。また、ハッカー（コンピュータ侵入者）対策として、利用者に対しては、パスワードを厳重に管理する（短いパスワードや容易に想定できるパスワードの使用を避けるとか、パスワードを頻繁に変更する）ように注意を喚起することが重要である。また、システムがユーザの利用権を確認した上でおり返し電話するコールバック方式の採用等が考えられる。

パスワードによる利用者の識別、確認の例を以下に示す。



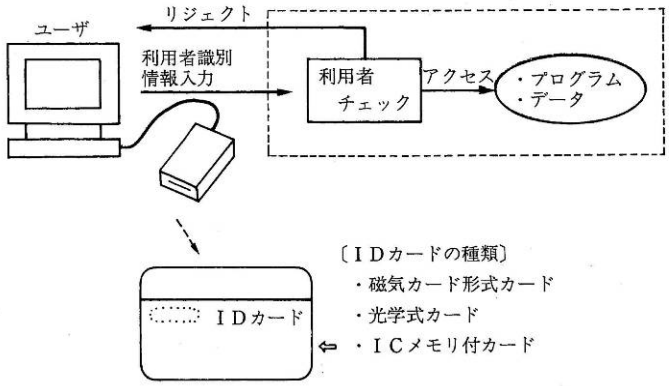
パスワードによる識別

２　IDカードの使用

IDカードの使用は、利用者の識別のために金融機関等で一般に用いられている方法であり、正当なIDカードを持っていれば、それを所持する人は正当な利用者としてみなされる。これは、パスワード等を利用した確認と併用されることが多い。

IDカードには、プラスチックに磁気ストライプをセットした磁気カード形式、ホログラフィック模様をセットした光学式、あるいは、ICメモリを埋め込んだ書き込み可能なものなどがある。

IDカードによる利用者の識別、確認の例を以下に示す。



IDカードによる識別

３　指紋

あらかじめ記憶させた指紋とスキャナで読み込んだ指紋の特徴を比較して利用者の正当性を確認しようとするものであり、高度な画像情報処理技術が要求される。

４　声紋

人間の音声は多数の異なる周波数の合成であることから、その周波数群を分析し、その中からいくつかの周波数を取り出し、これを紋様として視覚化したものが声紋であり、その特徴を識別し利用者を確認する。

５　手形

手の大きさ、指の太さ、長さなどの特徴を識別し、使用者を確認する。

６　署名

筆順、筆圧、速度、加速度等をあらかじめ計測し基準データとして登録しておき、端末を利用する時の実測データと比較して判別する。

情報通信ネットワーク安全・信頼性基準 解説（抜粋）

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。

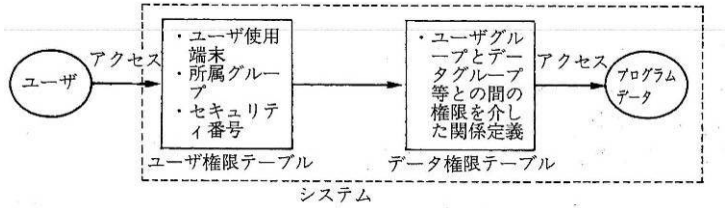
解説

システムにアクセスを行う利用者や運用者等に対し、アクセス可能領域や使用可能な命令の範囲に制限を設けること等により、システムや他人のデータの破壊や窃取を防止する。

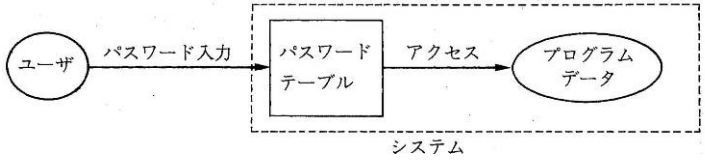
コンピュータ資源（データ、ディスク・ボリューム、テープ・ボリューム、プログラム等）の破壊やデータの不当な開示を防止するためには、コンピュータ資源へのアクセスを適切にコントロール（アクセス・コントロール）することが必要である。誰がどのような範囲でコンピュータ資源にアクセスできるか明確な基準を設定することがアクセス・コントロールの基礎である。アクセス・コントロールの具体例を以下に示す。

●措置例●

１ アクセス権限テーブルによる方法



２　パスワードによる方法



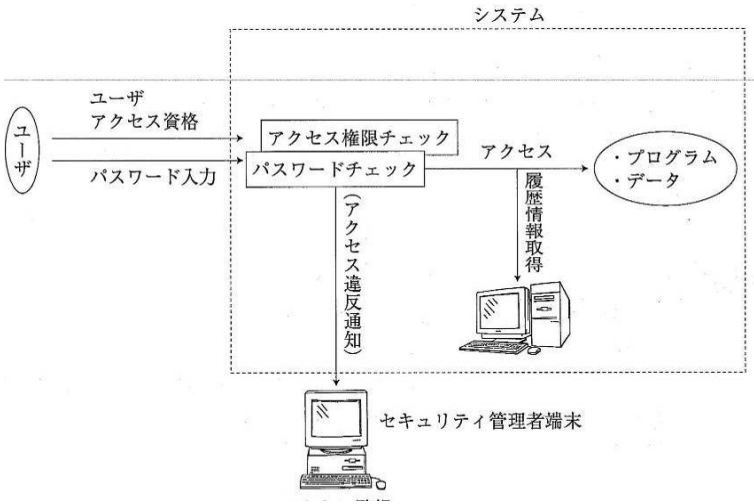
情報通信ネットワーク安全・信頼性基準 解説（抜粋）

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。

パスワード盗用を防止するため、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。
排除する条件として一般的な単語のほか、次のような条件を設定することも考えられる。
●措置例●
１　パスワードの最低文字数
　パスワードの最低文字数を定めておき、それに満たないものは排除する。
２　文字の種類の組合せ
　アルファベット（A～Z）、数字（0～9）及び特殊文字（．、－）の3種類の文字の組合せを条件とする。
３　同一文字の使用制限
　7777…のような同一文字のパスワードを設定しないよう、異なる文字を一定数以上使用していないパスワードは排除する。
４　login名の使用制限
　login名と同じ若しくは含むものの使用を制限する。

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。
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。

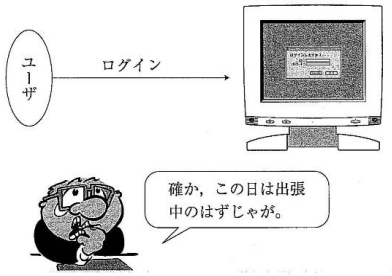
セ　不正アクセス等に対処するため、アクセス失敗回数の基準を設け、基準値を超えたものについては履歴を残しておく機能を設ける。
ソ　保護が必要な情報については、そのアクセス要求を記録し、定期的に分析・報告すると同時に、問題発生時の監視根拠として保存する機能を設ける。なお、アクセス違反があったときにセキュリティ管理者端末に通報するなどの機能を設けることも有効である。



アクセス監視

タ　ネットワークへのアクセス履歴の表示又は照会を行う機能を設けること。

ユーザが不正アクセスの有無を確認できるようにするため、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。



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。

利用者が講じるべき防御策として、パスワードの随時変更を始めとするパスワードの管理が重要であることから、不正アクセスに対処するため、利用者に対して注意喚起する機能を設けることが有効である。

解説

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接続する場合に、再開の意思を確認する機能を設けること。

悪質なハッカーの一般的な傾向としては、一定期間以上ネットワークを利用していない、いわゆる休眠状態の利用者のネットワークやID、セキュリティの甘いサーバを探し、そこをベースキャンプとして活動する場合が多い。

そこで、ユーザへの注意喚起として、長期遊休ユーザのログイン時には、プロバイダー側から利用者に対して本人の確認を行うとともに、再開の意思を確認する機能を設ける。

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。

通信される情報の機密の度合いにより、利用者またはネットワークにおいて秘話化措置や暗号化措置を講じる。

●措置例●

１　秘話化措置

同一の電話回線に接続される他の電話機等によって通話の内容が聴取されないように秘話措置の付加等の措置を講ずる。

２　暗号化措置

暗号の目的は、正当な送受信問でのみ意味を理解できるメッセージ交換を可能にし、第三者に情報が渡っても理解できない様にすることである。通信回線上での暗号化はどの部分に暗号機能を持たせるかにより以下のように分類される。

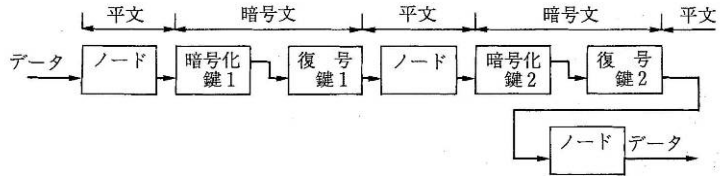
①　リンク暗号方式

②　ノード暗号方式

③　端点間暗号方式（エンド・ツー・エンド方式）

①　リンク暗号方式

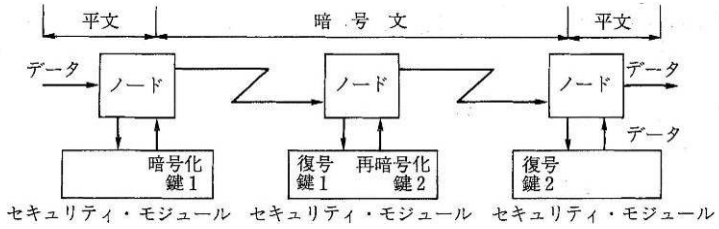
ネットワーク内で隣接するノードとノードを接続するリンク上でのみ暗号化されているがノードで処理されている間は平文となっている方式である。情報の行先を示す経路情報を暗号化することも可能である。



リンク暗号方式

②　ノード暗号方式

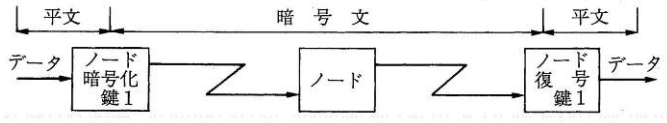
この方式は、リンク方式の弱点（ノードで処理されている問は平文となっている）を補うもので、データはノード内のセキュリティ・モジュールにより暗号化、復号及び再暗号化が行われる方式である。経路情報は平文のままである（暗号化してはならない）。



ノード暗号方式

③　端点間暗号方式（エンド・ツー・エンド方式）

データはユーザ間の伝送全体を通じて一貫して暗号化されている方式である。リンクやノード暗号方式とは異なり、端点間暗号方式では各ユーザは数個の鍵を持ち、暗号を使用する相手ユーザ毎に鍵を使い分けることができる。データは最終目的地に到着して初めて復号が行われ、中間ノードやそれに付属するセキュリティ・モジュールにおいては決して平文の形を取らない。経路情報は平文のままである（暗号化してはならない）。



端点間暗号方式

リンクやノードの暗号方式では暗号機能はネットワークでのみ実行され、ユーザにとっては透過であるといえる。

端点間暗号方式の場合、暗号機能がシステム・サービスを通じて自動的に提供されるときにはユーザにとって透過である。（もしユーザが特別な暗号化が必要ならば暗号使用は透過でなくなる。）

透過な端点間暗号方式をサポートする上でシステムが行わなければならないサービスのひとつは、通信を行うユーザ間のデータを暗号化し復号化するための暗号鍵の選択ないし割当である。

ホスト側に暗号機能を組み込む方法としては以下の方法がある。

①　中央処理装置（CPU）自体へ組み込む

②　フロント・エンド・プロセッサへ組み込む

③　CPUチャネルに付加する独立装置に組み込む

どの方法を採るかについては費用対効果の比較検討が必要であるが、③の方法は設計方式の異なるCPUに適応する場合でも一種類の装置設計で良いという利点がある。

リンクの暗号方式では、暗号化されたデータが通過する通信路にあるすべてのノードの入出口に独立した暗号装置を備えなければならない。

また、ノード暗号方式では、暗号化されたデータが通過する通信路にあるすべてのノードが独自のセキュリティ・モジュールを備えていなければならない。

一方、端点間暗号方式では暗号化されたメッセージを作り出し、受け取るノードだけが暗号能力を備えていればよいことになり、ネットワーク内で暗号機能を具備すべき箇所が著しく減少する。

ト　適切な漏話減衰量の基準を設定すること。

アナログ系音声伝送サービスにおいて、了解性漏話による通信内容の漏えいを防止するため、ネットワークとして適切な漏話減衰量を設定し、ネットワーク構成する交換設備や伝送路設備等毎に基準を設定する。

了解性漏話は誘導回線から被誘導回線へ情報が伝達され、他人に通信の内容が漏えいする現象である。この了解性漏話の規定は、電気通信回線設備の端点（利用者の設置する端末設備または他の電気通信事業者との接続点）における必要条件規定であり、事業者はこの端点において了解性漏話がないように自らの電気通信回線設備の各構成要素を設計しなければならない。

ここで、了解性漏話の度合いを支配する要因としては、電話機の伝送品質、室内騒音、発声レベル、回線雑音、局内雑音、加入者線路損失、及び漏話減衰量の周波数特性等種々であり、了解性漏話を規定するためには、これらの要因について条件を設定する必要がある。しかしながら、これらの要因は、必ずしも全利用者全事業者にとって同一ではない。

一例として、数字了解度を基本とする了解性漏話に関する管理上の目標設定例を以下に示す。

〔目標 その１〕

漏話による数字了解度は、ほとんどの加入者において、30%を越えないものとする。

〔目標 その２〕

目標その１を満足するために、交換設備、伝送設備等の漏話減衰量は次表の値をめざすべきこととする。

設　備　種　別	漏　話　減　衰　量	記　　事
搬　送　回　線	66dB	
音　声　回　線	68dB	中継器挿入回線を含む
加　入　者　線	68dB	
交　　換　　局	70dB	

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。

ネットワークが不正使用されることを防止するため、たとえば、呼の設定に係る情報が漏えいしないように十分な暗号化を行う、ネットワークへの接続要求時にユーザ認証を行うなどの措置を行う。

２．屋外設備

(13)　第三者の接触禁止
　ア　設備に第三者が容易に触れることができないような措置を講ずること。
　イ　とう道等には、施錠等の侵入を防止する措置を講ずること。

解説

屋外設備に対し、第三者が容易に触れることができないような措置を講ずる。なお、無線設備に対しては、電波法第３０条において、人体への危害や物件への損傷を防止するため、容易に立ち入りできないように安全施設を設置することが義務づけられている。

●措置例●

１　敷地内への立ち入り防止、設備への接触を防止するため防止柵を設置する。
- 防止珊は高さ２m程度とし、簡単に乗り越えられない構造とする。
- 防止柵は外部から容易に破壊されない構造とし、必要により、防犯警報装置を設置する。

２　多条数のケーブルを収容するとう道や重要ケーブルを収容するマンホール等においては、施錠、接着、封印等の侵入防止装置を講ずる。

３　架空電線の支持物については、有線電気通信設備令及び同施行規則で定めるところによる。

第２ 環境基準

１．センターの建物等

(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。

解説

出入口には施錠機能を設ける。

●措置例●

１　出入口の扉は、建築基準法施行令第112条第1項に規定される特定防火設備、防火戸等、防犯上、防火上十分な性能を有するものを使用し、施錠機能を設ける。扉の錠は、非常時においても、従事者の安全を考慮し、屋内から鍵を用いることなく、解鍵が容易な機能を有しているものとする。また、自動扉の場合は、停電時においてもバッテリー等により開閉可能なものとする。

２　受付と出入口が離れている場合はリモートロックが可能な錠を設備し、モニターテレビとインターホンにより入出制限を行う。

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。

解説

建築物の通常利用する出入口には、受付や監視装置等の入出管理機能を設ける。

「これに準ずる措置」とは、通信機械室に入出管理機能を設ける措置をいう。

●措置例●

1　通常利用する出入口は１カ所とし、警備員を配置する。出入口では入出管理が可能な受付を設ける。

- 入退館者の識別及び記録を行う。
- インターホン等による非常時の担当部門への連絡
- 持ち込み物品及び持ち出し物品の確認。
- 出入口のリモートロック

2　主要出入口の入退出は、電気錠を使用した入出管理装置により入退館資格を識別し、記録及び扉の開閉を行うことが望ましい。また、入出管理装置は、　技術の進展に沿って適時見直すことが望ましい。

入出管理装置例：

① 磁気カード装置　磁気カードをカードリーダーに挿入して解錠する。
② ホログラムカード装置　レーザー光で刻印したカードをカードリーダーに挿入して解錠する。
③ ICカード　プラスチックカードにICチップを内蔵させたカードで、磁気カードに比べ記憶容量が非常に大きく、偽造や不正使用が難しく、情報の機密保持性、安全性が極めて高い特徴がある。カードリーダーで読み取り解錠する。
④ 電磁波カード装置　カードをセンサーに近づけることにより解錠する。
⑤ 暗証番号入力装置　プッシュボタンにより暗証番号を入力し解錠する。
⑥ 生体認証装置　登録された掌形、掌紋等の生体情報を識別し解錠する。

3　監視用テレビシステム等を設置し、重要区画、主要出入口の監視を行う。

4　重要な設備を収容する建築物においては、必要に応じて防犯警報装置を設置する。

防犯警報装置例：

① マグネットスイッチ：磁気の動作により窓や扉の開閉を感知する。
② 赤外線感知器：侵入者が赤外線ビームを遮断することにより検知する。
③ 振動感知器：ガラス面等に接着しておき破壊時の振動を検知する。
④ トラップセンサー：塀や柵等に取り付けて張力や電流の変化により乗り越え、切断等を検知する。

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。

解説

電気通信設備を保守・維持・運用する者以外の者が、みだりに施設に入室して事業用電気通信設備を操作して、運用を妨げたり通信の秘密を侵したりすることがないよう、各々の領域のセキュリティのあり方について適切な基準を設定し、運用することが必要である。

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。
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。

解説

自然災害時の影響を考慮し、又、外部より第三者が容易に侵入できないよう建築物内での適正な場所に通信機械室を設ける。

「第三者が容易に侵入できないような措置」とは、建築物の間仕切の構造が十分な強度を有する等、第三者が容易に侵入できないようにすることをいう。

●措置例●

イの具体例としては、外部者が多く出入りする玄関の付近、又はエレベーターホール付近などを避けることが考えられる。

(4)　入出制限機能
ア　出入口には、施錠機能を設けること。

解説

第２　環境基準　１　センターの建築物（3）入出制限機能 アの項参照

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。

解説

第２　環境基準　１　センターの建築物（3）入出制限機能 イの項参照

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。

解説

第２　環境基準　１　センターの建築物（3）入出制限機能 ウの項参照

(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。

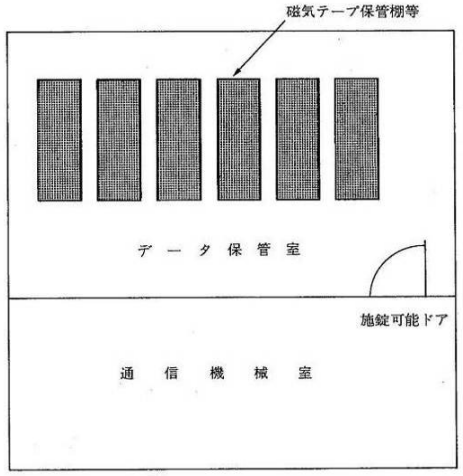
解説

システムデータ等の重要なデータを安全に保管できるよう、施錠機能を具備したデータ保管室又は専用のデータ保管庫を設置する。

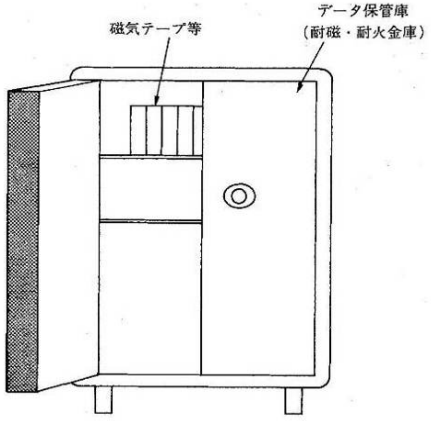
データ保管室は、防火区画が設けられている場合は、防火区画内に設ける。データ保管室に設けない場合はデータを耐火保管庫に収容する。保管庫の設置に際しては、転倒防止等の耐震措置を講ずる。データ保管室及びデータ保管庫は、必要に応じ、電磁界による障害防止措置を講ずる。

●措置例●

１　データ保管室は、室名等の表示を行わない。入出管理を徹底し、不正行為を防止するため、専用の独立した部屋とする。
２　出入口の扉は十分な強度を持たせ、施錠機能を備える。
３　出入口は１か所とし、前室を設ける。
４　耐磁気措置を必要とする場合は、耐磁気保管庫を設置する。
５　データ保管室は、単独の防火区画とし、空調ダクト、扉、開閉部等も防火区画を形成する構造とする。
６　火災の検知、消火機能を有するデータ保管室である場合、データが適切に二重保管されている場合を除き、データを保管する金庫等は耐火措置を講ずる。



データ保管室の例



データ保管庫の例

3. 空気調和設備

(2)　空気調和設備室への入出制限 出入口には、施錠機能を設けること。

解説

出入口には施錠機能を設ける。

●措置例●

1　空気調和設備室の扉は防犯、防火上十分な強度を持たせ、施錠機能を備える。扉の錠は、非常時においても、従事者の安全のため室内から鍵を用いることなく解鍵が容易なものとする。

2　暗証番号入力装置やシリンダ錠を使用する。

別表第２　管理基準

第1 方針

4. 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。

解説

安定的なサービスの提供、利用者保護の視点からも情報資産のリスク管理は不可欠である。セキュリティポリシーは、コンピュータウイルスなどによる情報漏えい等、情報資産の損失に対する抑止、予防、検知、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、方向性を定めた内容となる。

セキュリティポリシー策定にあたっては、「別表第3情報セキュリティポリシー策定のための指針」を参考とすることが適当である。また、技術動向や組織体制の変化に応じて適宜見直しを行うことが必要である。

(2)　情報セキュリティに関する取組み
　　情報セキュリティポリシーを公表すること。

解説
　策定したセキュリティポリシーは、公表することによって利用者に対する情報セキュリティに対する自社の取組を周知することができるので、策定次第、速やかに公表することが望ましい。

(3)　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。

解説
　不正アクセスやサイバーテロ等について予め対処を定めておくことにより、実際にこれらが発生した場合迅速な対応が可能となる。危機管理計画の対象、責任体制、役割、対応内容と手順等を明確化させるとともに、模擬訓練等の実施についても明らかにしておくことが必要である。危機管理計画ガイドライン策定にあたっては、「別表第４危機管理計画策定のための指針」を参考とすることが適当である。
　また、技術革新や社会の変化に応じた事例の洗い出しや組織体制の変化等に応じて適宜、次のような観点から対処方針の見直しを行うことが適当である。

●措置例１●
　DoS攻撃等のサイバー攻撃等の大量通信等によるサービスへの影響を防止するため、これらの通信を遮断する等の対応が必要となる。
　このような場合の対処にあたっては「電気通信事業者における大量通信等への対処と通信の秘密に関するガイドライン」（社団法人日本インターネットプロバイダー協会・社団法人電気通信事業者協会・社団法人テレコムサービス協会・社団法人日本ケーブルテレビ連盟2007年５月30日策定）を参考とする。

●措置例２●
　重大な影響を及ぼすサイバー攻撃や、１社のみでは解決が難しい攻撃に対しての他の事業者との協力体制等について検討する。
　　１　情報共有する体制の整備
　　２　他社へ協力を依頼するルートの整備
　　３　規制や接続拒否の実施基準の策定

●措置例３●
　高度なセキュリティを実現するネットワークを構築するため、本人認証の手段として、端末認証（MACアドレス、シリアル番号等）、生体認証（指紋、静脈等）等、により高度な認証方式の導入を検討する。

●措置例４●
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、新手の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。

第2 体制

2. 各段階における体制

(4) 情報セキュリティ対策
ア 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。

解説

ネットワークを管理する者として、情報セキュリティに関する一定以上の専門的な知識・技能を有する者（資格保有者等）を配置し、不正アクセスやコンピュータウイルスなどに対する対策を実施することは、ネットワークの安定的かつ確実な運用を確保する上で重要な要素となる。

イ 外部委託先を含めた作業の分担、連絡体系、責任の範囲等の情報セキュリティ対策体制及びデータ管理体制を明確にすること。

解説

データ管理体制を明確にし、作業の分担、連絡体系及び責任の範囲を明確にする。

●措置例●

データ管理体制の例として以下のものがある。

１ 対象データを取り扱う部門の総責任者として、安全管理責任者等を設置し以下の担務を行う。
① データ取扱い方法の決定
② 監査の実施

２ 安全管理責任者の下で実際に安全管理を実行する者として安全管理者を設置し以下の担務を行う。
① 安全管理担当者へのデータ取扱い方法の具体的指示
② 工事・作業の状況の管理

３ 安全管理者の下で実際に事務を処理させるため安全管理担当者を指名する。
① 入室管理
② 鍵の保管・管理
③ プログラム、データ（ファイル、ドキュメントを含む）の保管・管理
④ 作業状況報告

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。

解説

業務を外部委託する場合には、守秘義務・保持契約を取り交わすとともに守秘義務・保持契約条項の具体化、秘密保持に係る誓約書の徴収、外部委託先の監査実施、監査時のチェック項目、監査において不具合が発見された際の是正処置依頼・是正処置結果の確認等を定めた情報管理規程の策定等、委託先の取組を明確化する。

(9)　防犯対策
ア　防犯体制を明確にすること。

解説
防犯体制を明確にし、分担及び責任の範囲を明確にする。データの改ざん、窃取等に結び付く破壊活動、妨害工作又は盗難等の故意の人為的災害は、その手段、時期、場所等を予測できないため、防犯管理には十分な配慮が必要となる。
建築物及び設備面から立てられた防犯対策は、例えば建築物の周囲、外面及び開口部分、設備を設置した部屋のそれぞれの防犯対策が有機的に結合、機能するような体制作りによって、目的とする機能を発揮する。

イ　防犯管理の手順化を行うこと。

解説
異常事態発生時の対処を含め、管理の方法について手順化しておく。
異常事態発生時には、第一次対応が最も重要であるため、状況を正確に報告できることに重点を置き、代理者を含め、各人の責任分担を明確にするとともに、連絡・報告、現状分析、対策等に関し、即応できるように予め手順化しておく。

第3. 方法

1. 平常時の取組

（２）教育・訓練
キ　防犯に関する教育・訓練を行うこと。

解説

防犯に関して、通常時の保安作業及び異常事態発生時の措置について、必要な能力を養うための教育・訓練を行う。

●措置例●

１　専門家による講義
２　ビデオ教材等の教育教材による学習
３　OJT

このうち、OJTは、仕事を体験させ、機会をとらえて訓練生に必要な指導を行う方法である。すなわち、仕事の方法、手順等、仕事に直接関連する具体的、実際的な知識あるいは仕事に対する考え方、心構え（取り組む姿勢）を即効的に教える場合に効果的である。防犯の教育・訓練としてOJTによる方法は特に有効である。

なお、OJTによる訓練のバックグランドとしてある程度の体系的な知識が必要であるので、OJTの前提として１および２による訓練が必要である。

ク　情報セキュリティに関する教育・訓練を行うこと。

解説

一般社員等に対し、通信の秘密の保護、各種データに関する守秘義務、パスワード管理の重要性及びコンピュータウイルスの脅威等について教育・訓練を行い、モラルの向上等を図ることが、適切なセキュリティ対策を推進する上で重要な要素となる。

●措置例●

新たな技術やリスク管理等に対応した技術者を育成するため、業界団体等による研修コースの活用などがある。

（３）設計
エ　重要な機器を調達する場合は、サプライチェーンにおける情報セキュリティを考慮した機器を調達すること

解説

サイバー攻撃等の脅威に対する安全・信頼性対策の１つとして、セキュリティ対策を講じることが重要である。

内閣サイバーセキュリティセンター（ＮＩＳＣ）において「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」が作成・公表されているが、この中でセキュリティ上の脅威への対策として「サプライチェーン･リスク」への対応が求められている。

上記リスクは機器の調達の段階で検討することで軽減することができるため、機器の調達に当たっては考慮するよう努める必要がある。

（５）維持・運用
シ　通信の秘密の確保に関する取組を実施すること。

解説

「通信の秘密」は、電気通信事業法第４条において侵してはならない旨規定されている。ここでいう通信は、音声に限らずデータ伝送も適用されることに留意しつつ、事業者は、通信の秘密について厳格に対処することが必要である。

(6)　情報セキュリティ対策
ア　情報セキュリティに関する情報収集を行うこと。

解説

サイバー攻撃等の脅威に対する安全・信頼性対策の一つとしてセキュリティ対策を講じることは極めて重要である。情報セキュリティ対策については、定期的な情報収集をすることにより常に最新の情報を確保しておくことが必要である。

イ　情報セキュリティ対策についてその手法及び事前確認を十分行うこと。

解説

サービスに大きな影響を及ぼしかねないサーバ等機器の容量や評価・試験方法等について、事前に十分確認する。またネットワークに影響が生じる可能性があるセキュリティ対策やふくそう時の端末動作についても事前に試験、確認する。

ウ　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。

解説

情報セキュリティ技術の高度化のスピードは、著しく、それだけに陳腐化の速度も速いといえる。最新のセキュリティ技術の情報やセキュリティ事業者の商品の開発動向等の把握とその活用は、適切なセキュリティ対策を推進する上で重要な要素となる

●措置例●

具体的には、最新の次の技術を採用することが適当である。

１　暗号技術
２　ユーザ認証技術
３　アクセス・コントロール技術
４　不正アクセス検知技術等

また、ISO（国際標準化機構）/IEC（国際電気標準会議）等によりシステム管理のガイドライン（下記参照）や技術基準が策定され、我が国でもそれらを参照しながら情報セキュリティ関連のガイドラインや技術基準が作成されているため、これらのガイドラインを考慮することが望ましい。

（参考）

１　電気通信事業における情報セキュリティマネジメントガイドライン(ISM-TG)

ISO/IEC17799をベースに、電気通信事業者が遵守すべき情報セキュリティマネジメントを実践するための規範を、業界ガイドラインとして策定したものであり、「電気通信分野における情報セキュリティ対策協議会」にて2006年６月29日に決定している。

２　セキュリティ評価基準等(ISO/IEC 15408 等)

ISO/IEC 15408 は、欧米各国・地域でそれぞれ独自に定めていたセキュリティ評価基準を統一化して国際標準化したものであり、1999年12月にISO/IECで制定された。

国内においては、ISO/IEC 15408 と同等の規定であるJIS X 5070 を策定するとともに、2001年より、ISO/IEC 15408 に基づくITセキュリティ評価及び認証制度が独立行政法人情報処理推進機構により運用されている。

エ　コンピュータウィルス並びに端末及びソフトウェアの脆弱性に関する情報を入手したときは、必要に応じて、緊急連絡先に直ちに連絡すること。

解説

ウイルス発生時緊急情報の収集、通報を円滑に行うため、電気通信関係団体で構成する対策会議が、平成12年５月に設置され、緊急連絡体制が確立されている。コンピュータウイルス発生等の緊急情報は、緊急連絡網を通して関係事業者に周知され、かつ、被害状況の情報収集も円滑に行われるシステムとなっている。各事業者は、これらの連絡網やT-CEPTOAR等にコンピュータウイルスやサイバー攻撃に関する情報を提供する体制の確立が必要である。

オ　コンピュータウィルス並びに端末及びソフトウェアの脆弱性に関する情報を入手したときは、必要に応じて、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サイトへの掲示、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。

解説

コンピュータウイルスは、自社内ネットワークへの感染及び利用者のネットワークやパソコン端末に感染する可能性があることから、大規模な拡大が危倶される情報を入手したときは、その対策を含めた情報を速やかに関係者に提供する必要がある。利用者への情報提供手段としては、ウェブへの掲示、メールニュース等が考えられる。

カ　ネットワーク内の装置類やサービスの属性に応じて情報を分類すること。

解説

取扱規程及び管理責任者を適切に設定する等により、情報の管理に関する内部統制ルールの整備を行うことは、情報を適切に保護し維持するために必要である。重要情報の流失防止のためにも、内部統制ルールに関する事項の整備を行うことが必要である。

これらの実施の適切性を担保するために、ISMS認証等の外部認証の活用も有効である。

●例　情報漏えい対策●

社内O&M(Operation & Maintenance)システム等のウイルス対策は行っても、社員・職員、外部の業務委託先など個人用PCにおける対策をチェックすることには限界がある。

従って、自宅へ持ち帰っての業務禁止、個人用PCへのファイル交換SW使用禁止等、社員・職員・委託先等への教育が不可欠であり、また、外部媒体（USBメモリー等）からのウイルス感染も考慮して、個人用の外部媒体使用禁止なども検討する必要がある。

自宅での業務を許可する場合においては、盗難・紛失されても遠隔操作でデータを消去・ロックできるPCを利用するなど、自衛策を講じる必要がある。

キ　データ管理基準を設定すること。

解説

　データの取扱いを行う上で、データの入力、処理、出力及び保管時等における基準を設け、その管理を行う。又、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の世代管理の基準を設け、その管理を行う。利用者の暗証番号等の取扱いにおいても、管理基準を設け、他への漏えいを防止する。

　また、事業者からベンダに送付されるサーバ障害ログ等、電気通信事業者以外の者が取り扱う情報の管理方法や、業務の委託（請負）先での情報管理方法についても具体的にドキュメントに定め、電気通信事業者による管理方法の変更がある場合にもベンダや委託先へ迅速に適用されることが必要である。

●措置例●

以下の項目について入出力処理及び保管時等のデータ管理基準を定める。

また、外部に委託する場合のデータ管理基準も同様の基準を定め、委託先が確実にデータ管理基準を順守していることを確認するための監査を実施する。

1　対象データの指定方法
2　データ取扱いの優先度、重要度の分類方法
3　分類された重要度による取扱い方法
4　データの保管方法
5　データ運用・管理の記録方法
6　データの正確性、正当性、妥当性の確認方法
7　データ移転時の処理方法
8　パスワード等の管理方法
9　データ管理の責任者の責務
10　障害等により機器が事業者から委託先へ移された場合のデータ取扱い基準と方法

ク　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。

解説

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、その重要度による分類を行い、取扱い者の制限を含め重要度に応じた管理を行う。

●措置例●

通信の秘密の保護、データ保護及び復元の可能性の度合いに応じ、設備に係るデータ及び文書類に関する重要度の分類を行い、この分類に基づき、コピーの禁止、発行部数限定、保有者限定、媒体の種類に応じた廃棄処分方法等の取り扱い範囲を内規等のドキュメントに定める。

ベンダ等事業者以外での保守作業が増加しており、通信の秘密や個人情報などの漏えいを防止するために、故障物品内に格納された情報の漏洩防止対策を講じることが必要である。また、記録媒体の性能向上が著しく、容量が大きいがサイズは小さくなっていることから、保管については紛失、盗難などに十分に配慮する必要がある。

●措置例●

１　事業者からベンダに送付されたサーバの障害ログ媒体の扱いの取り決め等、事業者以外の者が取り扱う情報の管理方法を明確にする。

２　委託（請負）先での情報管理方法や選定方法を具体化して、ドキュメントに定め、事業者の管理方法の変更を迅速に織り込んでいく。

ケ　データ取扱作業の手順化を行うこと。

解説

通常時のデータ取扱い作業について手順化を行った上で手順書を作成し、それに従って作業を行う。

手順化に当たっては、通信の安定的な疎通を図るため、各作業の目的（意味）、位置付け（関連）が明確に管理者及び作業者に理解され、データの重要度に応じた管理者及び作業者の責任範囲と権限との整合性が確保されており、非常事態発生時の措置への移行が円滑かつ混乱なく行われるよう配慮されていることが望ましい。

また、通信の秘密保護のため、データの漏えいに十分注意がなされており、データの保護に関しても取扱いが特定の者のみに偏らない等、データ取扱いの基準に合致していることが要求される。

コ　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。
サ　利用者の暗証番号等の秘密の保護に配慮すること。

解説

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で秘密を要するものについては、従事者の守秘義務の範囲を明確にし、その周知、徹底を図る。

通信設備の設計、運用及び保守に係るデータ及び文書類は間接、直接を問わず、通信度にクラス分けを行い、それぞれ取扱いに携わっている従事者に対し、データ及び文書類の持っている意味を十分に理解させ倫理を確立し、秘密性・重要度に応じた守秘義務を負わせる。業務を外部に委託する場合には、委託先がデータ管理基準を適切に設定し、確実に守る体制であることを確認する。

●措置例●

1　社内における範囲

業務上必要な場合を除いて開示しない。

2　社外における範囲

裁判所、警察等法律上照会権限を有する者から照会があった場合でも、公共の福祉を除いて、原則として開示しない。従って、やむを得ず開示する場合の手続については、あらかじめ定めておく必要がある。

また、従事者が在職中に知り得た情報を第三者に漏らしたり、自ら利用したりしてはならない。

重要度	データ、文書等	管理方法
A	・IDカードの仕様書 ・パスワードの登録簿 等、セキュリティを保持する上で大きな影響を与えるもの	特別に指定された者のみによって厳重に保管され、それ以外の者が見ることは許されない。
B	設備の仕様書、配置図等のうち、セキュリティを保持する上で大きな影響を与えるもの	管理責任者の元に管理され、業務遂行上必要と認められる場合は、管理責任者の許可を得て見ることができる。
C	上記以外	管理責任者の元に管理され、必要時には特に許可を得ないで見ることができる。 ただし、業務遂行上、外部の者に見せる必要が生じた場合には、管理責任者の許可が必要。

シ　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や脅威の拡大に応じた適時の点検及び見直しを行うこと。

解説

複数のシステムが複雑に接続する場合には、それぞれのシステムだけではなく、その相互作用によるリスク・脅威の評価も必要になるため、技術革新に合わせた適時の点検・見直しが必要である。

ス　情報管理に関する内部統制ルールを整備すること。

解説

取扱規程及び管理責任者を適切に設定する等により、情報の管理に関する内部統制ルールの整備を行うことは、情報を適切に保護し維持するために必要である。重要情報の流失防止のためにも、内部統制ルールに関する事項の整備を行うことが必要である。

これらの実施の適切性を担保するために、ISMS認証等の外部認証の活用も有効である。

●例　情報漏えい対策●

社内O&M(Operation & Maintenance)システム等のウイルス対策は行っても、社員・職員、外部の業務委託先など個人用PCにおける対策をチェックすることには限界がある。

従って、自宅へ持ち帰っての業務禁止、個人用PCへのファイル交換SW使用禁止等、社員・職員・委託先等への教育が不可欠であり、また、外部媒体（USBメモリー等）からのウイルス感染も考慮して、個人用の外部媒体使用禁止なども検討する必要がある。

自宅での業務を許可する場合においては、盗難・紛失されても遠隔操作でデータを消去・ロックできるPCを利用するなど、自衛策を講じる必要がある。

セ　監査時における確認項目の策定と定期的な内部監査及び外部監査を実施し、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。

解説

情報資産の保持という観点から、サービスを提供する当事者以外の第三者、例えば外部機関又はネットワーク運用部門と独立した部門等によるセキュリティ監査制度を導入し、不正アクセスやコンピュータウイルスなどによる情報漏えい対策等の問題点の把握等適切に努めることが必要である。監査制度導入にあたっては、より具体的なチェック項目を定め、定期的に監査を実施することが必要である。この監査結果を受け情報セキュリティ対策等全体の見直しを行うことが必要であるが、この監査制度の位置づけを明確にし、組織内で強制力が働くような仕組みにしておくことが必要である。

また、電気通信事業に係る個人情報や重要なシステム情報が外部委託先から漏えいすることを防止するため委託先等の外部機関についても電気通信事業者と同様な情報セキュリティ対策を施すことが必要である。

●措置例１●

業務を外部委託する際に守秘義務・保持契約の義務化と守秘義務・保持契約条項を明確化するとともに、外部委託先の監査チェック項目と監査の実施方法、是正処置依頼と処置結果の確認方法等、委託先との確認項目を具体的にドキュメント化し、委託先の取組みを明確化する。

●措置例２●外部監査のチェック項目の策定と定期的な内部・外部監査の実施

外部監査を依頼する場合は、チェック項目を依頼先と検討して策定することが必要である。内部監査を実施する場合は、設備の責任者立会いの元で実施することが必要である。また、年に１回以上の監査を実施することが必要である。

ソ　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。

解説

情報通信システムの重要性に鑑み、システムを停止・機能低下させるおそれのある重要なシステム情報の流出については、その事実を的確に把握し対策を講ずる。

タ　サイバー攻撃への対策を講ずるとともに、発生時には迅速に情報共有する方法を確立すること。

解説

サイバー攻撃には社内への影響だけでなく、広く事業者全体への重大な影響を及ぼす攻撃がある。サイバー攻撃に対する社内への準備とともに、事業者全体に影響を及ぼす重大な攻撃の発生に対しては可能な限り迅速に情報を共有し被害の拡大を防ぐ方策が必要である。このため、あらかじめ社内に留めるレベルか、広く事業者間で共有すべき情報の基準を明確にしておくことが必要である。

●措置例●

T-CEPTOAR等において、以下の項目について情報共有の在り方を確立する。

１　サイバー攻撃の危険度
２　事業者間での情報共有
３　国に提供する情報

チ　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。

解説

広域災害に対処するため、重要なプログラムや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は前世代のファイルも含め、同一ファイルを地域的に十分隔たった場所に別に保管しておく。

●措置例１●

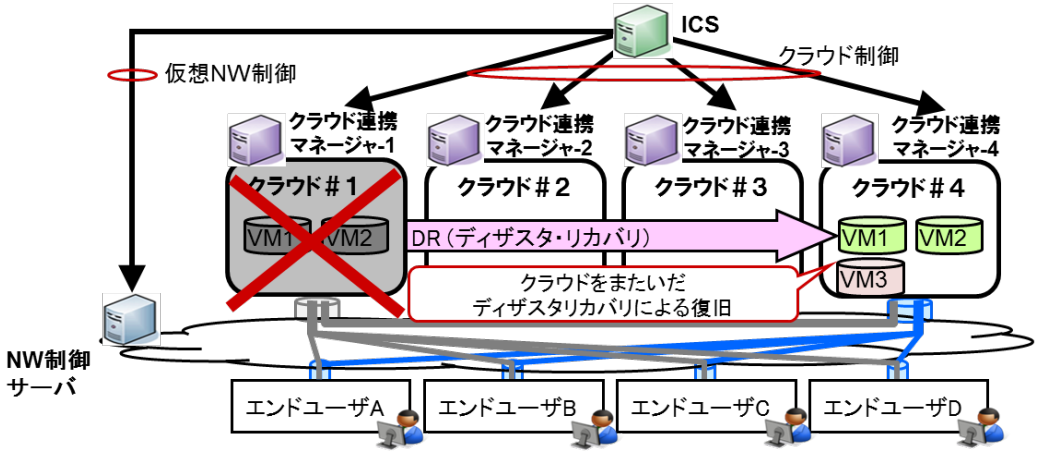
媒体の火災等による破壊あるいは盗難等の事故防止のため、重要なデータ・ファイルやプログラム・ファイルは、同一のものを離隔保管する。広域災害も考慮し、安全性を確認の上、十分に離れた距離に設置された通信センターや離隔地に設けた保管設備に保管する。

やむを得ず同一ビル内で離隔保管を行う場合は、防火区画上の分離、耐火金庫を使用する等の安全対策上の措置を講じ、なるべく離れた場所に保管する。データ・ファイルやプログラム・ファイルを離隔地に伝送する方法としては、高速回線を用いて伝送する方法とトラック（空気調和設備付き）等によって運搬する方法がある。

保管ファイルの更新の周期や送達方法はシステムの回復に要する時間等を考慮して定める。

●措置例２●

クラウドサービスを提供する電気通信事業者においては、インタークラウド技術を活用して地理的に分散するクラウド間を跨がったディザスタリカバリを実行することにより、遠隔地にデータ・ファイルやプログラム・ファイルを運搬する方法もある。



インタークラウドサービス機能（ICS）を活用した複数クラウド連携の例

ツ　コンピュータウィルス又は不正プログラムが混入した際に、情報通信ネットワークに対して利用者が与え、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。

解説

利用者がDDoS（分散協調型サービス拒否）攻撃の踏み台となった場合に与えるネットワークへの影響や携帯電話端末への不正プログラムの侵入等を回避するため、利用者に対してその脅威と対策について周知する必要がある。

(11)　防犯対策

ア　防犯管理の手順化を行うこと。

解説

異常事態発生時の対処を含め、管理の方法について手順化しておく。

異常事態発生時には、第一次対応が最も重要であるため、状況を正確に報告できることに重点を置き、代理者を含め、各人の責任分担を明確にするとともに、連絡・報告、現状分析、対策等に関し、即応できるように予め手順化しておく。

イ　入出管理記録は、一定の期間保管すること。

解説

異常事態の発生時に状況分析を行うことができるよう受付簿や監視装置で取得したビデオテープ等の記録物について、一定の期間、保管管理を行う。

●措置例●

受付簿について、日時、氏名、会社名、連絡先、被面会者名、目的等、必要事項を記入させるとともに、年１、２回実施状況を監査する。ビデオテープ等の目視できない媒体の保管に当たっては、外部ラベルに日時、取扱者等必要事項を記入するとともに、必要な時に再現できるよう保管方法を考慮する。

ウ　入建築物、通信機械室等の入出管理を行うこと。

解説

監視装置や受付等により入出管理を行う。

●措置例●

不法な侵入が行われないよう、侵入口となり易い出入口、窓、排気口、排煙口等の定期点検を実施するとともに、通常の手段で利用され易い出入口については監視装置や受付者を置き、入出者の状況及び入出時の手荷物の状況について管理する。

又、それらのビデオテープや受付簿等の記録物について管理を行う。

外部からの入室者には、それが明確に判定できる表示の着用を義務付け、その立ち入り場所についても入室の目的、資格等により制限する。

エ　出入口の鍵、暗証番号等の適切な管理を行うこと。

解説

出入口の鍵の使用状況、暗証番号の付与状況については、現状の把握を行い適切に管理する。

●措置例●

出入口の鍵には、金属鍵、磁気カード鍵など実態のあるものと暗証番号など実体のないものとがあり、実体のあるものについては常にその存在場所を把握できるように、又、実体のないものについては、運用方法等によりその暗証番号を窃取されないように、管理要領を作成し、それを遵守する。

実体のあるものの管理要領としては、鍵自体の複製を防止するとともに使用数を限定し、使用者・管理者を明確に区別するとともに、出来れば一人では使用出来ない方法が望ましい。実体のないものは、運用中に暗証番号は窃取されることが想定されるため、適宜番号の変更を行う等、運用面からの管理も有効となる。

オ　建築物、防犯装置等の保全点検を定期的に行うこと。

解説

1　各種の監視装置や警報装置等の防犯装置は、定期点検を行い、正常に動作するようにしておく。

2　建築物に損壊、漏水等不良箇所が発生していないか定期的に点検する。（テナントビルのような場合は、その建築物の管理者等により点検されていればよい。）

3　建築物に損壊、漏水等不良箇所があると、これにより電気通信設備が被害を受け、場合によっては人体へ被害を与えることがある他、その発生原因が人為的なものであれば、通信設備の破壊を目的としたものとも考えられるため、建築物の状況を定期的に点検する。

4　空気調和設備が正常に機能するよう定期的に点検する。（テナントビルのような場合は、その建築物の管理者等により点検されていること。）

5　電気通信設備を良好な状態で運転を継続させるためには、その環境条件が整備されていることが必要であり、特に周囲の温度、湿度及び塵検量を適正に保たなければならない。空気調和設備の信頼度は電気通信設備の信頼度に影響するため、空気調和設備の良好な稼働を図るため、定期点検を行い、空気調和の対象となる室の温度、湿度及び塵挨の定期点検を行う。

●措置例●

1　防犯装置の稼働状況が、外部から一見して確認できるような表示機能を有するとともに、表示内容と機能状態とが一致していることを確認するため、定期点検を行う。保全点検の実施時期、試験項目、試験方法、実施者、確認者、記録方法等を定めた管理要領を作成し、点検の実施状況を検査する。また、各種監視装置及び警報装置のリセット等の操作について、特定者以外の者が不正に操作できないよう取扱規程を明確にし、遵守状況を管理する。

2　建築物の点検箇所、点検方法、期間、確認責任者、管理状況簿への記入方法等を定めた建築物管理要領を定め、継続的な管理を実施する。漏水検知器、火災報知設備等については、テストを行い、機能が十分発揮できるかどうかを確認する。

①　温度・湿度等については、記録計を設置し監視する。

②　操作盤・バルブ等については、定常状態を表示しておく。

③　水質等については、汚濁されていないかどうかを監視する。

④　予備機器がある場合には、その稼働テストを行う。

企業のリスクマネジメントおよび
クライシスマネジメント実態調査2020

（再掲）「企業のリスクマネジメントおよびクライシスマネジメント実態調査2020」

- デロイトトーマツグループ「企業のリスクマネジメントおよびクライシスマネジメント実態調査2020年版」（2021年3月）において、「サイバー攻撃・ウイルス感染等による情報漏えい」が国内第3位・海外第5位となり、ともに順位が上昇。
- また、「グループガバナンスの不全」については、国内第8位で上昇し、前回同様で海外第2位になるとともに、新たな選択肢である「事業に影響するテクノロジーの変革」が国内第7位、海外第9位。

2020年はCOVID-19の影響に加え、気候変動・サイバー攻撃等の外部環境変化への対応やDX対応・グループガバナンス等の内部変革が上場企業の課題として浮き彫りになった

日本国内と海外拠点それぞれにおける、優先して着手が必要と思われるリスク（Q2、Q4のサマリー）

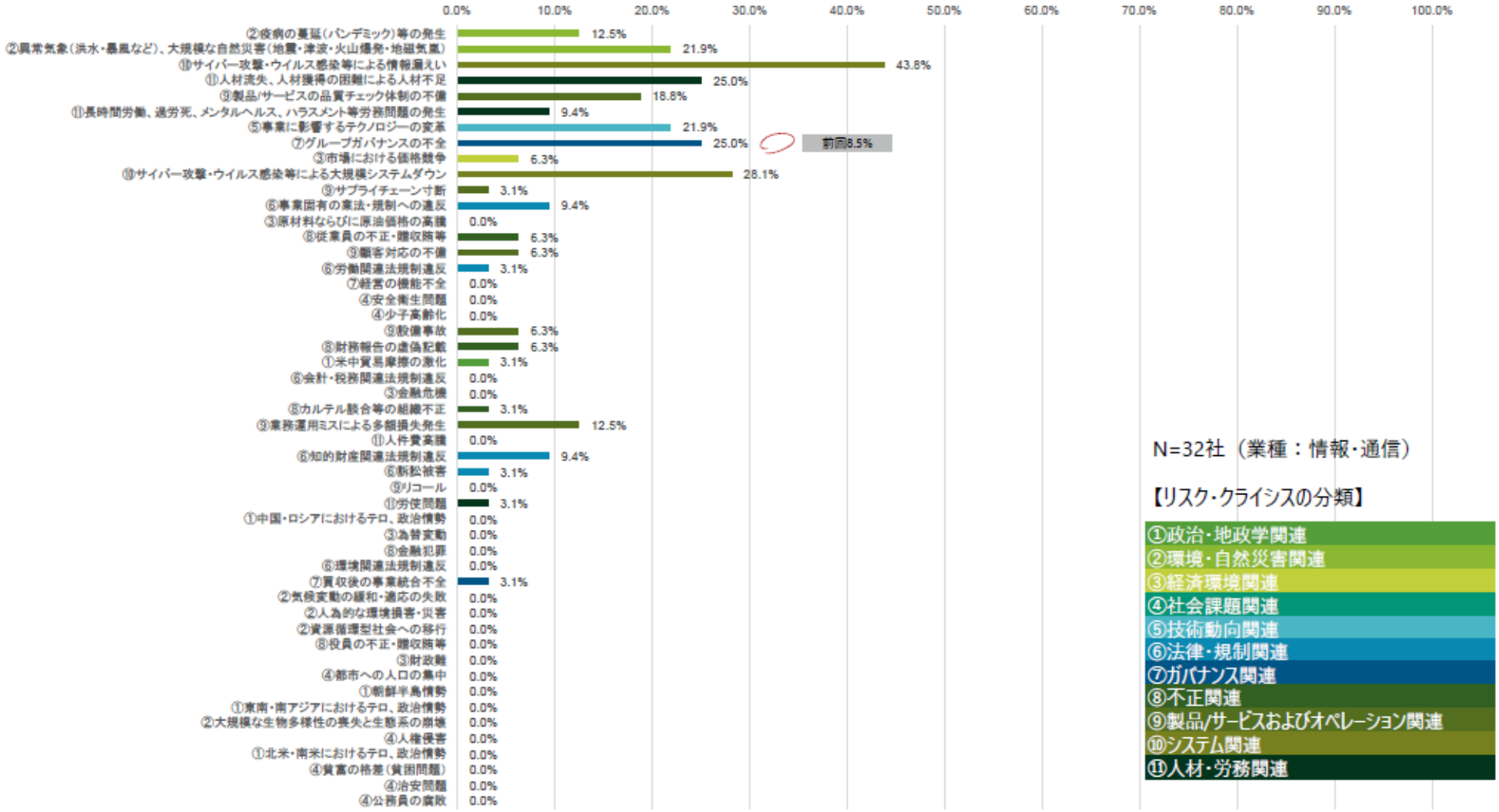
日本国内			海外拠点	
疫病の蔓延（パンデミック）等の発生（②）	34.4%（24）	第1位	疫病の蔓延（パンデミック）等の発生（②）	39.6%（27）
異常気象（洪水・暴風など）、大規模な自然災害（地震・津波・火山爆発・地磁気嵐）（②）	30.9%（1）	第2位	グループガバナンスの不全（⑦）	18.5%（2）
サイバー攻撃・ウイルス感染等による情報漏えい（⑩）	21.3%（5）	第3位	異常気象（洪水・暴風など）、大規模な自然災害（地震・津波・火山爆発・地磁気嵐）（②）	13.5%（5）
人材流失、人材獲得の困難による人材不足（⑪）	19.5%（2）	第4位/第3位	製品/サービスの品質チェック体制の不備（⑨）	13.5%（3）
製品/サービスの品質チェック体制の不備（⑨）	15.7%（4）	第5位	サイバー攻撃・ウイルス感染等による情報漏えい（⑩）	11.7%（10）
長時間労働、過労死、メンタルヘルス、ハラスメント等労務問題の発生（⑪）	12.5%（11）	第6位/第5位	人材流失、人材獲得の困難による人材不足（⑪）	11.7%（6）
事業に影響するテクノロジーの変革（⑤）	11.7%（-）	第7位	為替変動（③）	10.4%（8）
グループガバナンスの不全（⑦）	11.4%（9）	第8位	市場における価格競争（③）	9.5%（11）
市場における価格競争（③）	10.8%（7）	第9位	事業に影響するテクノロジーの変革（⑤）	9.0%（-）
サイバー攻撃・ウイルス感染等による大規模システムダウン（⑩）	10.8%（12）	第9位/第10位	従業員の不正・贈収賄等（⑧）	8.6%（4）

※（ ）カッコ内は前回順位
※各項目名に続く（ ）内の番号は、本調査において設けたリスクおよびクライシスの種類上の分類

【出典】デロイト トーマツ グループ「企業のリスクマネジメントおよびクライシスマネジメント実態調査 2020年版」(2021年３月)

グループガバナンスのリスク回答が、前回8.5%から今回25.0%へ大幅に増加。事業の多角化・拡大に伴うガバナンスの課題が浮き彫りになったと考えられる

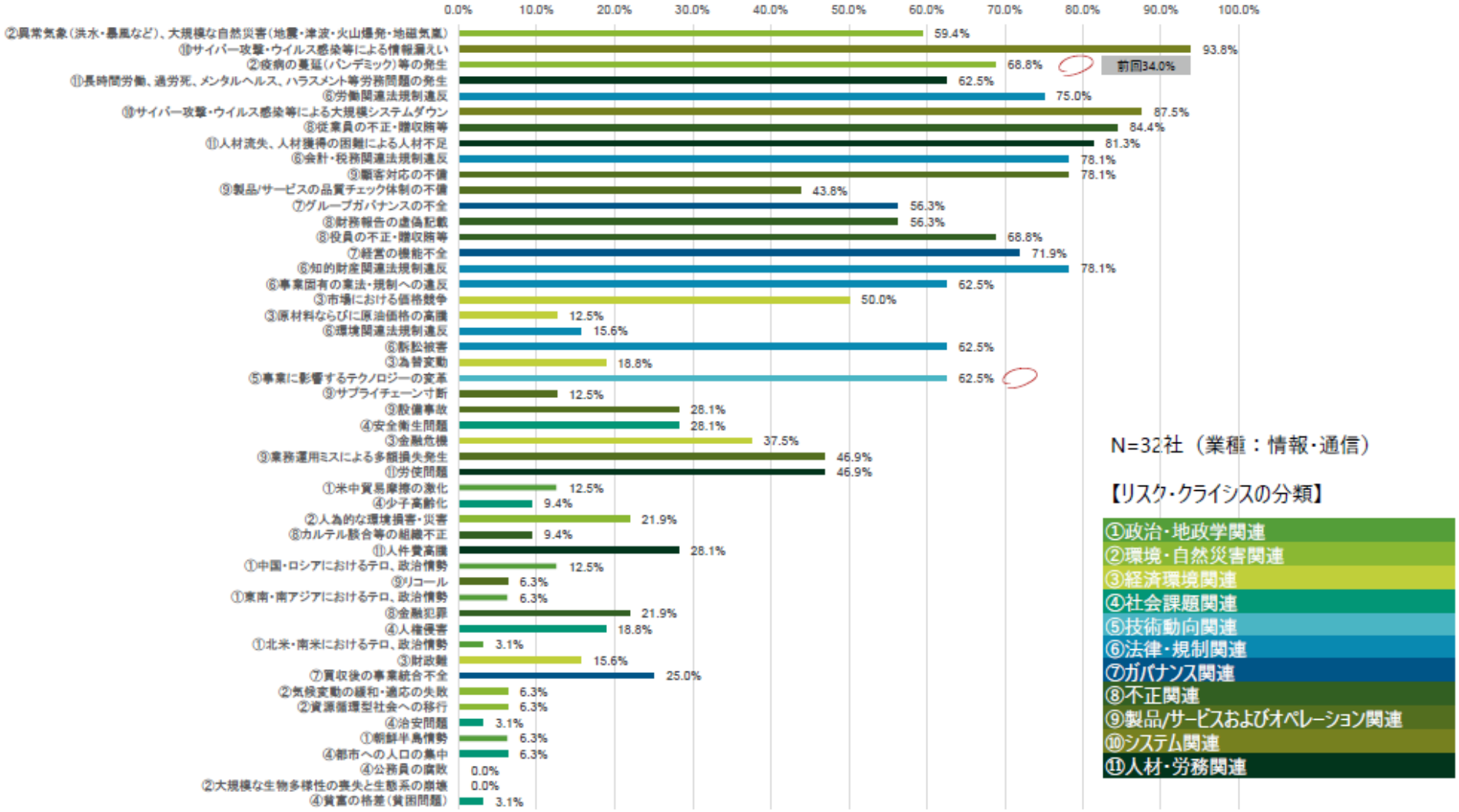
Q2.日本国内において、貴社が優先して着手が必要と思われるリスク（回答者のうち、業種：情報・通信を選択した回答のみの結果）



【出典】デロイト トーマツ グループ「企業のリスクマネジメントおよびクライシスマネジメント実態調査 2020年版」(2021年３月)

新たに追加した「事業に影響するテクノロジーの変革」が62.5%と全業種中で最も高い。5Gによるイノベーションや新たに生じるリスクへの対応が求められていると考えられる

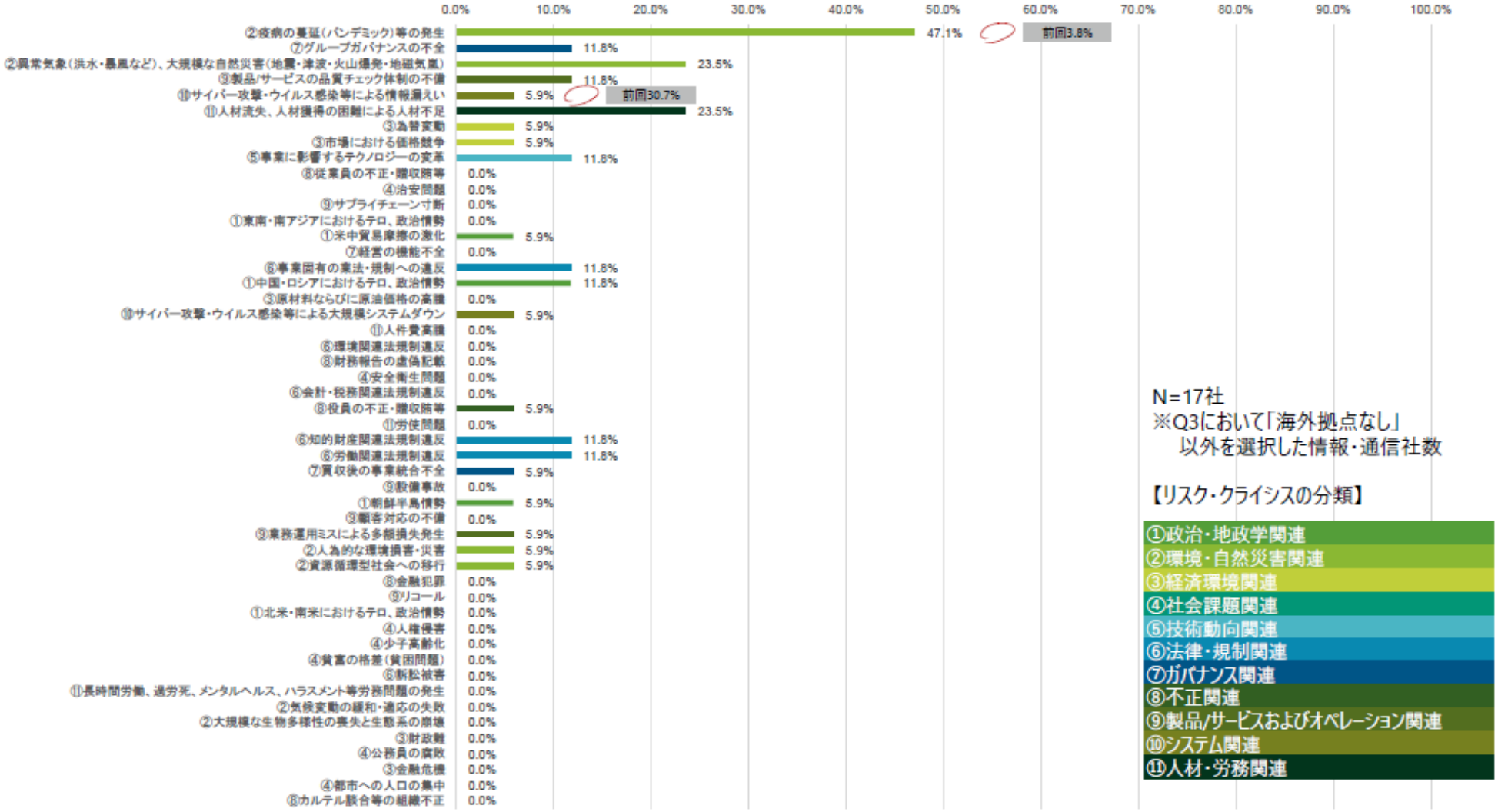
Q1.日本国内において、貴社がマネジメント対象としているリスクの種類（回答者のうち、業種：情報・通信を選択した回答のみの結果）



【出典】デロイト トーマツ グループ「企業のリスクマネジメントおよびクライシスマネジメント実態調査 2020年版」(2021年３月)

パンデミックのリスク回答は前回から大幅に増加しているが、情報漏えいのリスク回答は前回30.7%から今回5.9%へ大幅に減少している

Q4.海外拠点において、貴社が優先して着手が必要と思われるリスク（回答者のうち、業種：情報・通信を選択した回答のみの結果）



【出典】デロイト トーマツ グループ「企業のリスクマネジメントおよびクライシスマネジメント実態調査 2020年版」(2021年３月)

調査目的と調査方法について

■調査目的

✓ 国内上場企業における、「リスクマネジメント」および「クライシスマネジメント」の対応状況を把握し、現状の基礎的データを得ること

✓ 調査の実施および結果の開示を通じ、国内上場企業における「リスクマネジメント」ならびに「クライシスマネジメント」の認識を高めること

✓ 2020年版については、COVID-19の影響および対応に関する設問を追加した

■調査対象および回答企業数

日本国内に本社を構える上場企業約3,500社を対象とし、有効回答社数は343社

■調査方法

2020年10月中旬～10月末日にかけ、郵送にて調査を実施

■調査項目

【第1部】・・・上場企業が着目しているリスクの種類

【第2部】・・・上場企業が経験したクライシスの分析

【第3部】・・・上場企業のCOVID-19に対する対応状況

※詳細な調査項目とその結果は、本資料以降のページにて取り上げる。

また、「リスクマネジメント」と「クライシスマネジメント」については、それぞれ以下のように定義する。

○**リスクマネジメント**：企業の事業目的を阻害する事象が発生しないように防止する、その影響を最小限にとどめるべく移転する、または一定範囲までは許容するなど、リスクに対して予め備え体制・対策を整えること

○**クライシスマネジメント**：どんなに発生しないよう備えても、時としてリスクは顕在化し、企業に重大な影響を与えるクライシスは発生し得ることを前提に、発生時の負の影響・損害（レピュテーションの毀損含む）を最小限に抑えるための事前の準備、発生時の迅速な対処、そしてクライシス発生前の状態への回復という一連の対応を図ること

【出典】デロイト トーマツ グループ「企業のリスクマネジメントおよびクライシスマネジメント実態調査 2020年版」(2021年３月)