# 『経営者による情報セキュリティ強化の手引き』
## ― あなたの組織のセキュリティ対策は？ ―

## (1)本手引きの目的

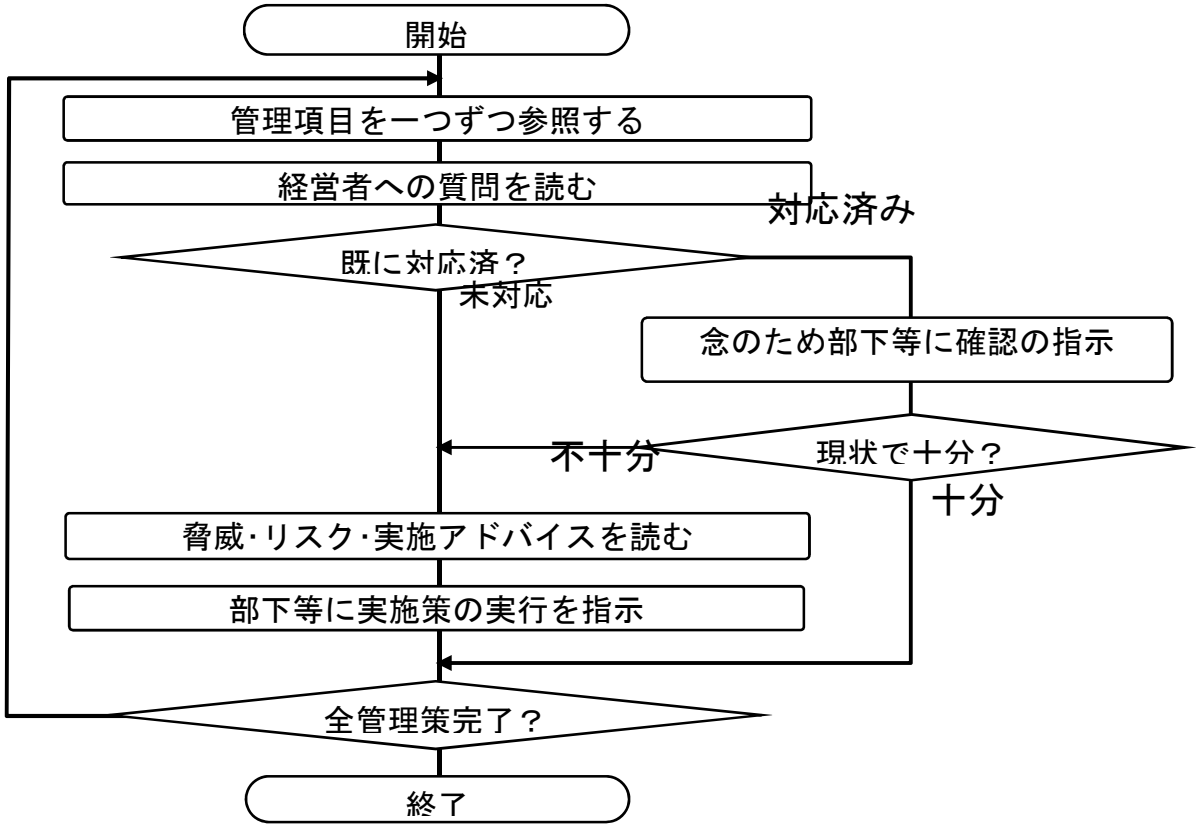
この手引きは、中小組織の経営者が、情報セキュリティの向上と強化を図るために、自組織のセキュリティレベルと課題を掌握し、追加対応の要否を判断し、もし追加対応が必要であれば実施策の実行を社内の担当者やITベンダー等に指示することを支援するために作成したものである。基本的な事項を網羅しているので、経営者にとどまらず、セキュリティ管理者

## (2)本手引きの根拠

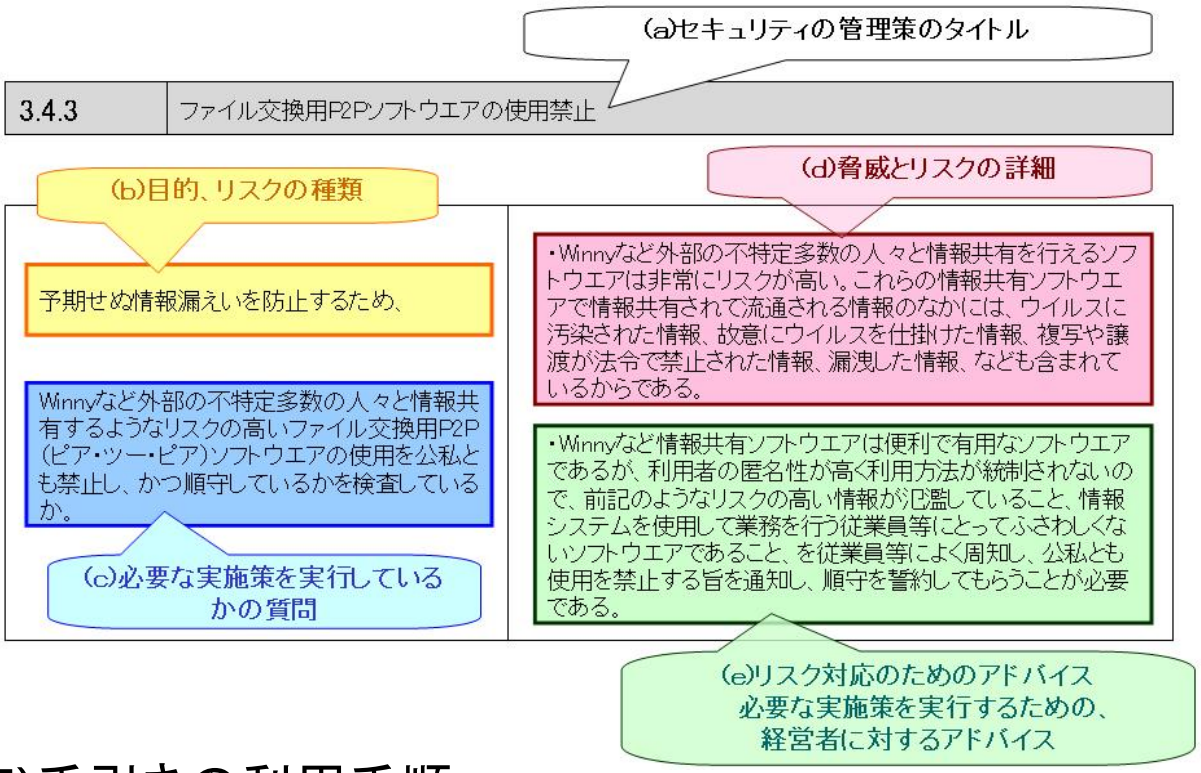
本手引きは、JIS Q 27002の管理策のサブセットに基づいている。

そのため、業務委託を請ける際に発注元から情報セキュリティの評価アンケートや第二者監査を要請された場合にも対応でき、将来ISMSに取り組むための基礎としても有効である。

## (3)手引きの活用方法



# (4)手引きの内容の見方




# (5)手引きの利用手順

**(a)の各セキュリティの管理策毎に**

**(b)の目的、リスク内容に対して、(c)の実施策を実行しているかを判断**

**(ア)実行していない場合**

(d)の脅威とリスクの詳細から、当社でこの脅威にさらされる情報資産があるかを判断

なし ——＞対応は不要

あり ——＞対応が必要

————＞(e)のリスク対応のアドバイスに従って、
経営者がリスク対応計画(何をどのレベルで)を立てて、部下やＩＴベンダーに管理策の実施を指示

**(イ)実行している場合**

(d)の脅威とリスクの詳細から、当社でこの脅威にさらされる情報資産があるかを判断

なし ——＞追加の対応は不要

あり ——＞ (e)のリスク対応のアドバイスから、
自社で現状実行している実施策で十分かどうかを判断

十分 ——＞追加の対応は不要

不十分——＞(e)のリスク対応のアドバイスに従って、

# (6)本手引き利用上の注意事項

**本手引きは、前記「(1)本手引きの目的」で述べたように、主として中小組織の経営者向けに作成されたものであるが、併せて情報セキュリティ担当者向けの教育研修の一教材としても、本手引きが幅広く活用されることを願っている。 ただし、ご使用の場合には、作成者及び著作権所有者が以下であることを明示してください。**

**「JSSA システム監査学会 情報セキュリティ研究プロジェクト（2008年7月1日）」**

# (7)経営者による情報セキュリティ強化の手引き

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| I | 従業員等のセキュリティ | | |
| 1.1 | 従業員等採用時の管理 | | |
| 1.1.1 | 従業員等の役割と責任 | 組織として情報セキュリティに対応するために、情報セキュリティ基本方針(ポリシー)を定め、ポリシーに従って従業員等(役員及び従業員)のセキュリティに関する役割及び責任を明確にし、文書化しているか。 | ・複雑化する情報システムにおいて、情報システムやデータを確実に保護することは容易ではない。<br>・情報システムやデータを確実に保護するためには、全社的なセキュリティ基本方針に基づいて、従業員等が行動する必要がある。<br>・従業員等のセキュリティに対する役割及び責任は、組織の情報セキュリティ基本方針に従って定め、文書化することが望ましい。<br>・正社員に対しては、雇用契約の際に、セキュリティの諸規程を提示し、役割と責任を契約書の中で明確にする必要がある。派遣社員、パート、アルバイトに対しては、正社員の場合に準じて、役割と責任を契約書の中で明示する。<br>・従業員等が、情報セキュリティ上の脅威、弱点、違反、事故など、未遂を含めて検出した場合の迅速な報告についての手順を定めることが必要である。<br>・検出した情報セキュリティ上の脅威、弱点、違反、事故及びそれらにつながる事象については、是正・予防処置を講じて、それらの発生を防止しなければならない。<br>・具体化した役割と責任は、適切であるか否かを日常的に見直し、また定期的に内部監査等で各部署での運用が有効に行われているかを確認し、継続的に改善していくことが望ましい。 |
| 1.1.2 | 従業員等の選考 | 従業員等の規律意識の甘さや悪意な行動から情報漏えいなどが発生することを防止するために、保護が必要な情報を取扱う業務に従事する従業員等の選考は適切な手順で行っているか。 | ・従業員等の情報管理の甘さや、故意による情報の持ち出しによって、情報が漏えいしたという事故・事件が度々報道されている。<br>・保護が必要な情報を取扱う業務には、セキュリティ規則の重要性を認識しそれを順守できる従業員等を選考し担当させなければならない。<br>・特別高いセキュリティが要求される業務に従事する者の選考については、満足のいく推薦状の入手、応募者の履歴書・提示された資格・公的証明書の点検、法令が特段認めた範囲での信用調査や犯罪記録の点検などを含むことが望ましい。<br>・選考では限界もあるため、入社直後は、機密性レベルが比較的低い業務を担当させ、信頼できることを確認できた後、機密性レベルが高い業務へ変更するなどの考慮も必要である。 |
| 1.1.3 | 雇用の条件 | 盗難・不正行為または施設の不正使用などを防止するため、従業員等には、情報セキュリティに対する義務と責任を記載した雇用契約書に同意を求めた上、署名させているか。 | ・内部の者による情報流出が度々報道されている。社内の者が会社の情報を持ち出すことは容易であるので、これを牽制する必要がある。<br>・従業員等との間では、業務上、知り得たすべての情報について、非開示の契約を締結する。<br>・契約書には、情報の開示、非開示にかかわらず、会社の許可なく、情報を持ち出さないという内容を含ませる。<br>・情報の非開示と合わせて、個人情報の持ち出し禁止を徹底しておくことも重要である。<br>・情報持ち出しといえば、ネットワーク経由、電子記録媒体、紙媒体だけを想定するが、人の記憶による持ち出しも注意が必要である。記憶には量的限界もあるが、記憶した内容を毎日外部でメモしたり、電子化して蓄積すれば、結果として多量の機密情報の漏えいとなるので、十分な注意が必要である。<br>・雇用契約解除後も、情報の非開示について、雇用契約の中に明記しておくとともに、退職時の誓約書の中にも明示する。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 1.1.4 | 委託先の選定 | 委託先でのセキュリティ事故の発生を防止するために、セキュリティ要求事項や評価基準を定め、それに沿って委託先候補を審査し、選定しているか。 | ・委託先の従業員等の情報管理の甘さや、故意による情報の持ち出しによって、委託した業務から情報が漏えいしたという事故・事件が度々報道されている。<br>・保護が必要な情報を取扱う業務を委託する場合、セキュリティ規則の重要性を認識しそれを順守できる事業者を選定しなければならない。<br>・自社の要求事項に合っているかを評価するために委託先選定基準を定め、それに基づいて委託先候補を審査し、選定する。<br>・委託形態の変化や法改正時は、委託先選定基準を見直し、必要があれば改訂する。<br>・委託先候補の評価を行う際に、必要があれば、委託先候補の企業に責任者が出向いて、業務委託先に立ち入り、現場を監査するなどの方法で実態を確認する必要がある。<br>・情報セキュリティ事故の発生、負債の増加、資金繰りの悪化など、業務委託先の状況は変化するので、委託先の審査は適時に行う必要がある。<br>・二次請負(再委託)に関しては、認めるのか認めないのかを明示し、認める場合の条件は何かを明確にしておくことが必要である。 |
| 1.1.5 | 業務委託の条件 | 契約後のトラブルを防止するため、業務委託先には、情報セキュリティに対する義務と責任を記載した業務委託契約書に同意を求めた上、署名させているか。 | ・業務委託先や委託先従業員による情報流出が度々報道されている。業務委託先の情報セキュリティを委託先に任せるのではなく、発注者としての情報セキュリティ要求事項を明確に委託先に伝え順守してもらう必要がある。そのためには、自社の情報セキュリティルールに適合する内容の業務委託契約を締結し、関係する従業員等に周知させることが重要である。<br>・業務委託先とその従業員等との間で、業務上知り得たすべての情報について、守秘義務の契約を締結していることを、業務委託先責任者に確認し、業務委託契約の中に明記する。<br>・業務委託契約終了後も、守秘義務が存続することを、業務委託契約に明記する。<br>・業務委託先の従業員等が、担当の途中で退職するケースも多いので、退職後の連絡先などを業務委託先の管理項目として要求しておくことも必要である。<br>・最初から犯行を前提に潜入していると考えられる場合もあるため、退職や契約解除後も、注意が必要である。<br>・業務委託契約では、委託業務を推進するために必要な情報のみに限定してアクセスを認めることを徹底する。<br>・委託業務に不必要な情報へのアクセスは認めないが、万一アクセスした場合には契約違反としてペナルティを課すことを約束させる。<br>・モニタリングなどにより、業務委託契約から逸脱した行為がないか確認する。<br>・セキュリティの面で必要ならば、委託先の従業員等の交代を要求できる契約内容にしておく。<br>・業務委託先の従業員等が当社内に常駐して業務を遂行する場合、その従業員等に対して当社の情報セキュリティルールを説明して厳格に守るよう約束させなければならない。(委託先の従業員等が、当社では禁止されている情報資産の個人的な利用を行い、その結果、社外サイトに書き込みした内容が問題になったケースもあるので、委託以外の行為をしないよう、徹底することが大切である。)<br>・業務委託契約は、一覧表などを作成して契約満了日や守秘義務契約終了日などを一元的に管理し網羅的に把握することが望ましい。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 1.2 | 雇用中の従業員等の管理 | | |
| 1.2.1 | 経営者の責任 | 組織内の構成員全体にセキュリティを徹底するため、経営者は、セキュリティ方針を示し、その順守を従業員等に求め、確認をしているか。 | ・従業員がセキュリティ事故を起せば、対外的には経営者の監督責任が問われる。そのため、経営者は情報セキュリティについて明確な方針と順守事項を、従業員に対して示す必要がある。<br>・経営者は、情報セキュリティが全社で適切に適用され、維持、運用されていることを定期的に確認できる仕組みになっているかを確認する必要がある。<br>・経営者は、各部門責任者が、従業員に関する情報セキュリティの課題を把握し、報告するようにしているかを確認しなければならない。<br>・部門責任者を通じて情報セキュリティを徹底することが基本であるが、経営者自らが前面に出て陣頭指揮した場合には、その徹底度は大きく向上するので、経営者の取り組みが重要である。<br>・情報セキュリティ規程の制定者となることや、社内の情報セキュリティ推進のトップとなり、直接的に指示することが望まれる。<br>・社長自らの言葉で、自社の目指すところを指し示すことが大事である。経営目標と情報セキュリティは、表裏一体の関係でもあり、経営の方向に必要な情報セキュリティ対策は、明快に要求しなければならない。<br>・悪い報告がタイムリーにあがってくる仕組を整備することと、経営者が悪い報告も聞く姿勢をもっていることが重要である。 |
| 1.2.2 | 情報セキュリティの意識向上と教育訓練 | 情報セキュリティの意識向上のため、すべての従業員等は、職務に関連する組織の方針及び手順について教育や訓練を受けているか。 | ・情報セキュリティは、たった一人の不注意でも、大きな事故につながりかねないので、全員に対する教育が重要になる。<br>・セキュリティ意識向上のための教育訓練は、情報やサービスへのアクセス権を認める前に行われるべきである。<br>・教育訓練では、情報処理設備の正しい利用法、ソフトウェアの利用及び懲戒手続に関する情報についての教育に加えて、セキュリティ要求事項、法的責任及び実務管理を含むことが望ましい。<br>・教育内容は、情報セキュリティ規則の変更と環境変化に対応して、適宜改訂できるようにする。<br>・規則を定めた時だけでなく、周知徹底するために繰り返し教育する計画を準備する。<br>・派遣や業務委託で新たな人が着任した場合、自社の情報セキュリティ規則を周知する教育の機会を設け、徹底する仕組みにする。<br>・情報セキュリティ管理で重要な役割を担う役員、部門責任者を教育から除外してはならない。<br>・教育では、最低限徹底したい内容に絞り徹底することが重要である。<br>・教育は、繰り返し実施しないと、その効果が希薄になるため、定期的に実施しなければならない。<br>・情報セキュリティは、全員への教育が大事であり、そのためには、各部門の受講状況のフォローが欠かせない。 |
| 1.2.3 | 懲戒手続 | セキュリティ違反を繰り返さないため、セキュリティ違反を犯した従業員等に対する正式な懲戒手続を備えているか。 | ・情報セキュリティ違反者に対し、懲戒などの手続きを定める。<br>・違反の程度を公正に判断できる基準を策定する。<br>・違反があれば厳正に処分し、その内容を社内に開示して従業員等に周知することで、再発防止策とする。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 1.3 | 従業員等の退職または異動時の管理 | | |
| 1.3.1 | 雇用終了や異動時の管理 | 業務から外れる者による会社の情報の利用を絶つため、雇用の終了時や異動時の手続を、規則などで明確に定めているか。 | ・雇用の終了や転出と同時に、各種のアクセス権などを削除できる仕組みにしておくことが重要である。<br>・退職者本人に届くメールを気にして、メールアカウントを残すことがないような仕組みも必要である。<br>・入館カードなどの完全回収ができているかも大切なポイントである。<br>・解雇などにより、突然に雇用終了となる場合は、即刻、すべての情報資産にアクセスできなくしなければならない。 |
| 1.3.2 | 資産の返却 | 許可されない情報の利用を防ぐため、雇用、契約終了時に、従業員等が所持する会社の情報資産すべてを返却させているか。 | ・雇用や契約が終了した後も、従業員等が会社の情報や業務上で作成した情報を保持していては、情報の漏えいリスクが高まる。<br>・従業員等に対して、情報資産は、業務上で自ら作成した情報を含めて、すべて会社からの貸与であることを周知し、会社に返却させる仕組みが必要である。<br>・退職間際での情報持ち出しなどを防ぐために、モニタリング強化による情報流出防止策を講じることが望ましい。<br>・従業員等が保有する業務上の重要な知識については、それを文書化し会社に引き継がせることが望ましい。 |
| 1.3.3 | アクセス権の削除 | 業務から外れる者による情報へのアクセスを絶つため、すべての従業員等の情報及び情報処理施設に対するアクセス権は、雇用、契約の終了時に削除しているか。また、変更に合わせて修正しているか。 | ・業務から外れた者を管理したり監督したりすることはできないので、業務から外れた者が会社の情報資産をアクセスできたり保持していたりすると、リスクが高まる。<br>・すべての従業員に対し、契約満了、または業務終了のいずれか早い方のタイミングに合わせ、すべてのアクセス権及び利用者ID・アカウントを削除する仕組みが必要である。<br>・また、該当者が使用していたパソコンは、アクセス権削除と同時に撤去し、他に悪用されないような措置を講じる。<br>・後日、証拠として必要となると思われるメールのアーカイブやログなどは、管理者だけがアクセスできるように確保しておく。 |
| | | | |
| Ⅱ | 設備関連のセキュリティ | | |
| 2.1 | 執務室・サーバ室のセキュリティ管理 | | |
| 2.1.1 | 物理的な境界 | 部外者の無断侵入を防止するため、外部との境界に物理的な障壁を設けているか。特に、サーバなど重要な機器は一般の執務スペースと隔離された部屋に設置しているか。 | ・境界を設けず、誰でも入れるようにしてしまうと、情報の持ち出し、盗み見、不正な持ち込みなどの管理が困難になる。社内でも、アクセス者を限定すべきサーバの設置や極秘情報の保管等は、部屋を分けてセキュリティレベルを変えた方が望ましい。<br>・壁、床、天井は、容易に破壊されず、隙間から侵入できない構造になっている必要がある。<br>・出入り口は容易に破壊できない施錠可能なドアであることが必要で、非常口、防火扉、ガラス窓の配置や構造にも注意が必要である。<br>・構造上、弱点がある場合には、有人の受付を設けたり、監視装置を設置することにより、常時不正侵入を防止する仕組みを検討する。<br>・入館時に、共連れ(入館権限のない人が、入館権限のある人に続いて入館する)を防止できる設備を設けるとともに、運用面でも、自分の後ろから続いて入る人がいないか確認することを励行させることも重要である。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 2.1.2 | 入退室時の管理 | 業務上必要のない入退を把握するため、従業員等の入退室の記録及び来訪者の訪問記録をとっているか。また、その記録を定期的にチェックしているか。 | ・休日、夜間など、無人時の入室や、不要な部外者の立ち入りが全く把握できていないと、情報の紛失や漏えいの際、調査の手がかりがないことになる。不必要な入退室や訪問の記録から不正行為が発覚することもある。<br>・毎日、最初の入室者と最後の退室者の時刻、氏名を記録する。24時間稼働しているような場合は、1日に1度以上定時に、異常がないかどうか点検の上、記録すると良い。来訪者については、社名、氏名、用件、訪問先、訪問時刻を記入し、終了後、面会者が確認の上、退出時刻を記入し、署名する。また、単に記録を取っているだけだと、記録漏れや記入ミス、不正な記録があっても見逃すことになる。<br>・ある程度のコストはかかるが、人的な監視や入退管理ができない場合、電子的な認証のための装置を導入することにより効率的な管理が可能となる。<br>・オフィス内で業務を行うものには社員証や入室許可証などを身につけさせ、入室を許可された者かどうかをすぐにわかるようにする。 |
| 2.1.3 | エリアのセキュリティレベルの設定 | 社内でのセキュリティのレベルを明確にするため、業務の機密度に応じてエリアを分割し、壁や施錠扉により隔離しているか。 | ・社内の機密情報を、役員のみや部外秘等に分類したとしても、それを保管したり取り扱う場所が区分されていないと、権限外の人も簡単に閲覧や利用ができてしまう恐れがある。<br>・一般的には、「誰でも自由に出入りできるスペース」(受付ロビーなど)、「社員と許可された来訪者が出入りできるスペース」(応接室等)、「社員のみが出入りできるスペース」(執務室)、「限られた社員のみが出入りできるスペース」(サーバ室、データ保管庫等)に分けられる。<br>・各エリアの境界は、通常の施錠扉の他にICカードや、指紋などの生体認証と電子ロックを組み合わせる方法がある。さらに、開施錠記録(入退記録)を自動的に取得する、監視カメラを設置するなどを機密度に応じて使い分けると良い。<br>・重要な情報を保管してある場所には、あえてそれを示す表示をせず、部外者からわかりにくくすることも必要である。<br>・個人情報などの機密レベルが高い情報を扱う部門は、一般執務室と分離独立させ、部外者が入れなくすることが望ましい。 |
| 2.1.4 | 災害への対応 | 重要な情報が火災や水害などで滅失、き損するのを防止するため、サーバ室など重要なスペースの設置場所や素材に留意しているか。 | ・自然災害などの脅威は、影響が広範囲であり、人的な対応も難しいため、一度発生すると業務が停止し、再開までに長期間を要したりする。<br>・サーバ室などの床、壁面には難燃性の素材を使用すべきであり、サーバ室内には、段ボールなど燃えやすいものを置かないことも重要である。<br>・部屋には火災検知器及び消火器、消火栓を近くに設置する。<br>・河川や海の近くのような、洪水、高潮による水害の恐れがある場所では、地下や1階などにサーバ室を設置しないなどの配慮も必要である。 |
| 2.1.5 | セキュリティを保つべき領域での作業 | 機密情報が作業中の不正等により漏えいしないため、作業場所の詳細を非公開にしたり、撮影・録音禁止などの措置をとり、必要に応じて監視カメラなどを設置しているか。<br>また、個人情報等を扱う担当者は、部外者からのアクセスが物理的に制限された場所で作業をしているか。 | ・複製を簡単に実行できる携帯機器を誰でも入手できるので、悪意を持った作業者がいれば、機密情報が複製されて持ち出され、情報が漏えいするので注意が必要である。<br>・携帯電話のカメラ機能や、携帯音楽プレーヤーの録音機能やデータ保存機能なども対象になるため、運用には注意を要する。<br>・私物は作業場所に持ち込ませず、ロッカーに保管させる。退出時に持ち物検査を行う、透明なビニールの手提げなどを貸与して作業場内で携行させる等の措置も有効である。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 2.1.6 | 一般の人の立寄り場所及び受渡し場所 | 重要な機密情報が、部外者の目に触れたり、盗み見されるのを防ぐため、荷物の受け渡し場所は、執務スペースから隔離したスペース(受付など)に限っているか。 | ・荷物や郵便等の配達員、ベンダーマシンのメンテナンス要員等の部外者が容易に執務室に入れる状況では、書類などが紛失しても、犯人を特定することができない。<br>・一般の人が立ち寄る場所や荷物の配達・集配の受渡し場所は、執務場所と隔離する必要がある。<br>・大型の荷物を搬入したりするために室内に入る場合は、来訪者カードなどに記入させ、入退記録をとるとともに、担当者が随行し、監視することが必要である。 |
| 2.2 | パソコン・サーバ等の情報機器のセキュリティ管理 | | |
| 2.2.1 | コンピュータ設置時における留意点 | 情報・通信機器が盗難されたり、災害や環境変化等により故障したり、使用不可能になることを防ぐため、設置場所を考慮して、盗難や災害などに対する予防策を講じているか。 | ・コンピュータ等の設置場所や設置方法が不適切であると、盗難されたり、あるいは、地震、火災、水害、温度変化等による故障や作業中の事故が起こりやすくなる。また、災害発生時の被害が大きくなる可能性が高い。<br>・サーバーは専用の部屋に設置し、部外者を近づけないようにする。また、地震時の転倒防止対策として、サーバラックをボルトで床に固定したり、L字クランプで倒れにくくする。タワー型の機器は、転倒防止器具やL字クランプ、ベルトなどで倒れにくくしたり、机上に置かないようにする。<br>・サーバー室には消火器を備え付ける。その際、電子機器は水や薬品に弱いため、二酸化炭素などのガス消火器を設置することが望ましい。<br>・落雷対策として、サーバー及び通信機器などはアースを確実にとる。雷サージ保護機能付の電源タップを用いると良い。<br>・サーバー室内や、コンピュータでの作業時には飲食禁止とすることも検討する。 |
| 2.2.2 | 電源等の安定供給 | サーバなど重要な情報・通信機器の正常動作を確保するため、電源や空調等が安定供給されるような対策を講じているか。 | ・停電、断水、公衆回線の通信不良などにより、電気が安定供給されなかったり、冷却がされなかったりすると、情報・通信機器が正しく動作しなかったり、故障する可能性が高くなり、業務に支障をきたす恐れがある。<br>・電源等は定期的に点検するとともに、停電時など、電源供給が絶たれた場合に、どれくらいの時間なら影響を与えないかによって無停電電源装置(UPS)の容量を設計し、設置をすることが必要である。なお、UPSの有効期間を確認し、交換等を定期的に行う。また、非常時の際の作業手順を文書化しておくことが望ましい。 |
| 2.2.3 | ケーブル配線のセキュリティ | 電源やLAN、電話線等のケーブル損傷や情報の傍受を防ぐため、これらのケーブル類を適切に敷設し、管理しているか。 | ・不用意な作業や事故によりケーブルが切断されたり、誤ってケーブルを抜いてしまうことにより、回線が不通になったり、データが破壊されたり、情報機器が故障することがある。<br>・ケーブル類は、なるべく露出させずに床下や天井、壁面などに敷設することが望ましい。また、情報処理設備のケーブル配線は複雑になりがちなので、まとめて束ねたり、色を変えたりケーブルごとにラベルをつけるなどしてわかりやすくすることが有効である。さらに、誤った配線や許可のない配線によるトラブルを防止するために、配線図を作成して、確認できるようにしておく必要がある。<br>・機器の廃棄や移設時、不必要となるケーブルの撤去を義務づけ、放置されない仕組が必要である。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 2.2.4 | コンピュータの保守 | サーバーやパソコン、通信機器など重要な機器が故障して業務に重大な支障が出ることを防ぐため、情報通信機器の保守体制、手順が明確になっているか。 | ・情報通信機器の故障は原因を特定するのが難しく、修理も専門性が必要となるため、正しい使用方法に従って運用し、故障時には速やかに修復対応ができる体制を整備する必要がある。<br>・各メーカーや業者と適切な保守契約を結ぶとともに、関係する従業員が契約内容や保守記録がわかるようにしておくこと。パソコン本体や記憶装置を保守のため社外に持ち出したり、外部の保守作業者が作業をする場合には、作業中のデータ破壊や情報漏えいの危険があるため、機密情報をバックアップした上、消去しておくことが望ましい。これが不可能な場合もあるので、保守契約には秘密保持条項を含ませる、社内での保守作業を監視するなどの対策も必要になる。 |
| 2.2.5 | 社外でパソコンを使用する場合のセキュリティ対策 | 社外でパソコンを使用する際の、紛失・盗難、情報漏えい、滅失、き損などのリスクを低減するため、対策を講じているか。 | ・移動中の置き忘れや盗難、紛失、屋外や公共の場でのノートパソコンの画面盗み見による情報漏えい、事故によるデータの滅失・き損、通信中の漏えいなど、社外でのパソコン利用には社内とは異なる様々なリスクが存在する。<br>・盗難・紛失時の情報漏えいを防止するために、パソコンにはパスワードを設定するのが効果的である。ただし、パソコン起動時のパスワードだけでは、ハードディスクだけを抜き取られて情報漏洩する場合があり、また暗号化による対策も、かけ忘れや推測しやすいパスワードにより容易に破られることもあるので、複数の対策を組み合わせて実施する必要がある。<br>・社外でのパソコン利用（在宅も含む）には、事前の許可をルール化するのが前提である。 |
| 2.2.6 | パソコンを廃棄する場合のセキュリティ対策 | パソコンを廃棄した際に、廃棄したパソコンを入手した業者や中古ユーザが残っていたデータを読み取り、そこから情報漏洩することを防ぐため、廃棄前にハードディスクを物理的に破壊するか、あるいは専用消去ソフトウェアにてデータを削除しているか。 | ・単なるファイルの削除やフォーマットだけでは、完全にデータは消えず単に読み出せない処理をしているだけなので、データ復活ソフトなどを使用することによりデータが復元され情報漏洩する可能性が高い。<br>・データを復元不可能にするためには、ハードディスクを破壊する、ドリルで穴を開けるなどの物理的な処理をすることが確実だが、断片的な情報からデータを読み取る技術もあるので、専用のデータ消去ソフトと併用するのが最も確実である。専用ソフトによる消去であれば簡単にデータを再利用不可能な状態にし、ハードディスク自体は再利用可能となる。ただし、ソフトウェアによる処理の場合は、確実に処理したことを記録し漏れのないようにする必要がある。 |
| 2.2.7 | パソコンの移動 | 社外へ持ち出したパソコンの紛失・盗難により情報が漏えいするリスクを回避するため、パソコンの社外への持ち出しを原則禁止とし、必要な場合は事前許可制とした上、持ち出し時のルールを明確にしているか。 | ・社内で通常使用しているパソコンを社外に持ち出すと、持ち出し中に紛失、盗難にあった場合、個人情報や営業秘密などのデータ、メールの情報などが外部の第三者に漏えいする可能性が高い。さらに、長期間社内LANから切断されることによりウイルス対策ソフトのパターンファイル（最新ウイルス情報）が更新されず、社内LAN以外のネットワークなどへの接続によって、ウイルス感染の危険も高まる。<br>・パソコンの社外への持ち出しは事前許可制とし、誰がどのパソコンを持ち出しているかが明確になるようにする。また、持ち出し期限を設定し、返却、持ち帰りの確認も行う。<br>・日常使用しているパソコンを持ち出すことは極力さけ、持ち出し用のパソコンや媒体を用意することが望ましい。<br>・オフィス移転などで大量のパソコンを移設させる場合、業者の専用ラックで施錠できるタイプのサービスがあるので、これを利用すれば安全性が高まる。社員が個人で運ぶような方法は、事故のもとであり極力避けるべきである。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| Ⅲ | 情報を取扱う局面のセキュリティ | | |
| 3.1 | 運用の手順及び責任分担 | | |
| 3.1.1 | パソコンやサーバの操作手順書の整備 | 業務の継続性を確保するために、担当が替わってもすぐにパソコンで業務が行えるように、従業員等がパソコンで業務を行うときの操作について、「パソコン業務操作マニュアル」を整備しているか。 | ・「パソコン業務操作マニュアル」で操作手順を決めておくことは、①業務効率・ミス防止、②業務の継続性、③不正防止、のために有効である。<br>・ASPサービス利用やパッケージ利用の業務システムの場合は、サービス提供(開発)元から、分かりやすい操作マニュアルの提供を受け常備すべきである。<br>・自社開発の業務システムの場合、操作手順を業務操作者の立場に立って過不足なく記載した操作マニュアルを作成して常備すべきである。また、業務システムを変更したときは随時操作マニュアルに反映すべきである。<br>・業務担当者にとっては、業務上で発生する案件について、業務システムのどの手順に従って具体的にどのように操作・入力すべきかなどの実務上のノウハウも必要なので、それら業務独自の内容も標準操作マニュアル及び外部提供の操作マニュアルに追記することが重要である。<br>・操作マニュアルを整備しても活用しないで放置したら、維持もされなくなりいざという時に利用できない。定期的に、業務をローテーション又は繁忙期・不在時などの交代支援などで別の者に担当させることで、操作マニュアルの活用機会を作って、それによって気づいた点を操作マニュアルに追記する等の維持・更新を行うべきである。<br>・不正防止の観点から、操作マニュアル通りに業務を行ったか、例外操作が発生したかを、業務日報等で報告させ、上司は、操作マニュアルの整備に関心を持ち、常時実用に役立つものにすることが重要である。記載のない操作が発生したら、それを操作マニュアルに反映すべきである。 |
| 3.1.2 | 情報機器やソフトウエアの変更の申請・審査承認・実施記録の管理 | 情報システムの変更時に発生しうる障害を防止するため、情報システムの安全性を確認した上で、経営者が変更を承認するような手続きになっているか。 | ・たった一つの蟻の穴から堤防が決壊する比喩のように、たった1台のセキュリティの弱い情報機器を接続したことで、会社中のシステムへの不正アクセス・ウイルス感染・改ざんなどの被害に遭うということがある。<br>・ソフトウエアの最新版をインストールする場合でも、インストール後に最新のパッチを当てたり、セキュリティを高めるような設定をしたり、時には関連する他のソフトウエアにも同様の処置をしないと、セキュリティホールが存在したままになる場合もある。<br>・情報処理設備及びソフトウエアやシステムの導入・変更時には、事前に経営者に申請し、セキュリティ知識のある者を含めてリスク評価をし、情報システムの安全性を確認した上で承認する手続きとする。<br>・社内に専門家が居なければ、ベンダーなどに検討をしてもらう必要がある。機器を売ることだけが目的のセールス社員に「問題ない」の一言返事をもうらうだけではなく、きちんと検討を依頼して、責任の所在と検討した範囲が明確に記された書面で報告を受取るべきである。 |
| 3.1.3 | 業務の処理者・承認者の分離、情報機器の利用者・変更者の権限分離 | 作業者の思い込みミスや不正が露見しないまま業務が進むのを防止するため、一連の業務の節々で上司の承認や業務担当者以外の者の確認作業を入れる手順にし、牽制が働くようになっているか。 | ・会社が用品を購入する場合に、要求・発注・検収・支払の担当を分けることで、経理上の不正を防止するという考えと同じ事を、情報処理のそれぞれのプロセスでも考えなければならない。<br>・工程ごとに検査を行うという方法もあるが、全体でみると膨大な検査工数になり、実現不可能である。次工程はお客様という考えがあるが、次工程の作業のなかで前工程の不正や誤りが全て露見するというような業務処理の流れにすることが理想である。<br>・不正や誤りの防止・牽制のために、作業者・点検者の名前・日時を記載した記録を残すことが重要である。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 3.1.4 | 開発・試験を実行する環境の本番システム環境からの分離 | 開発やテストは、運用中の業務システムや業務データに影響を与えないように、隔離環境で行っているか。また、業務データをそのまま開発・テスト用に使うことを禁止しているか。 | ・開発や試験では、未完成の不完全なシステムを用いたり、故意に誤った操作をし結果を確認したり、多くの作業者が関与したりするため、開発や試験の作業場面は、元々セキュリティのリスクが高い環境であるという認識を持つことが必要である。<br>・開発や試験環境は、運用中のシステム環境に悪影響を与えないために、独立させ、隔離する必要がある。<br>・開発や試験に対して、本番の業務データをそのまま使用することは、データの破壊、消去あるいは流出の可能性があるため、行ってはならない。 |
| 3.2 | 業務委託時のセキュリティ管理 | | |
| 3.2.1 | 業務委託時のセキュリティの確認と合意 | 自社が要求するセキュリティを達成するために、業務委託先との契約内容（要求事項）を検討し、契約を締結しているか。また、契約後は、規定事項が実行されていることを確認しているか。 | ・自社内でその業務を行う場合と同等以上のセキュリティ水準を委託先に要求しないと、自社のお客に対する責任が果たせない。<br>・業務委託先が、自社が要求するセキュリティの仕組みを構築し、実際に運用できるだけの技術力・管理力・経営資源があるかを評価してからでないと、業務委託を行ってはならない。<br>・委託先のサービス約款や契約書には、受託条件が記載されている。業務上必要とされる要件及びセキュリティ要件を満足しているかを十分確認することが必要である。<br>・「誠意をもって行う」、「善良な管理義務を果たす」のような民法上当然な義務の記載で済ますことなく、セキュリティ上行うべき事項、行ってはならない事項について、必要なものを全て列挙すべきである。“常識だから”という理由で記載を省略してはならない。<br>・約款や契約書に記載されていない事項については、委託先に確認し、確認した結果は委託先から書面でもらうことが必要である。約款や契約書の契約日付よりも前に確認したことは、契約書に盛り込むか引用させ、または契約後に書面で再確認すべきである。<br>・委託先のサービス約款には、免責事項や利用者の責任が記載されている。これらは、自社のリスクになる。これが発生した場合の対応を検討し、自社のリスクを評価し、リスクへの対応方法を決め、社内の関係者及び経営者の合意を得ておく必要がある。 |
| 3.2.2 | 業務委託先の点検 | 発注者が最終責任を果たすため、業務委託先の業務実施状況について、現場を確認したり、定期的に報告させたり、内容を点検しているか。 | ・委託先でセキュリティ事故が発生しても、対外的には当社の責任になる。発注者は、委託先監督責任を果たすために、委託先の業務内容を確認する必要がある。<br>・契約で、サービス状況についての定期的な報告義務を定め、受取った報告書をきちっと点検し、必要であれば指示等をしなければならない。<br>・委託先が順守すべき事項を定めた契約を締結するだけでは足らない。契約で定めた事項を順守しているかを、発注者が点検する必要がある。例えば、再委託を禁止しているような場合は、それが順守されているかを確認する。<br>・個人情報保護法では、発注者に、委託先監督義務が定められている。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 3.2.3 | 業務委託のプロセス変更の事前確認 | 委託先での業務・サービスの実施プロセスの変更により、提供される業務・サービスに支障を来たさないため、変更について事前に報告を受けているか。それらの変更に対応したセキュリティ管理策にしているか。 | ・個人情報保護法では、発注者に、委託先の監督義務が定められている。これは、委託先が順守すべき事項を定めた契約を締結するだけでは足らない。実施プロセス（人・設備・手順）の変更等に際しても、契約で定めた事項が継続して順守できているかを、発注者が点検する必要もある。<br>・提供されるサービスに影響が出る可能性のある重要な提供プロセスの変更を事前に報告する義務を契約で定め、その通り実施させ、報告された変更について提供されるサービス及び自社への影響のリスクを評価し、必要な処置を取らなければならない。 |
| 3.3 | 情報システムの拡張計画及び情報システム導入時の受入れ試験 | | |
| 3.3.1 | 情報システムの余力・残容量の測定・評価と拡張計画 | 事業継続性確保のため、情報システムの余力・残容量を定期的に測定して、能力・容量が不足する前に拡張・増設するように計画しているか。 | ・情報システムの能力・容量が不足すると、突然システムがダウンする恐れがある。業務量が一時的に集中したような場合でも、このような現象につながる場合もある。<br>・あらかじめベンダー等の専門家に情報システムを評価してもらって、余力・残容量の限度値や業務量集中の限度値などを決めて、監視を行う必要がある。 |
| 3.3.2 | 情報システム導入時の受入れ試験 | 情報機器やソフトウエアの新規導入時及び更新時には、障害が発生する可能性があり、それを防止するために、受け入れ試験を実施してから、業務に使うようにしているか。 | ・情報機器やソフトウエアを運用システムに導入してから問題点が発見されると、問題の対策完了までの間又はシステムを元に戻すまでの間、業務が中断する等甚大な影響が出る恐れがある。<br>・運用システムに導入する前に、導入システムに対して十分な時間をかけて綿密な試験を実施し、問題ないことを確認しなければならない。<br>・試験は、導入する情報機器やソフトウエアのみだけでなく、既存システムとの整合性を含めて、確認する必要がある。<br>・既存システムを熟知している社員やベンダーと共に、試験計画を検討した上で、試験する必要がある。<br>・導入前の試験を専用の試験環境で行うのか、既存の運用環境に組み込んで試験するのか、それぞれの試験の有効性や運用環境に及ぼす影響のリスクなどを評価・検討する必要がある。 |
| 3.4 | 悪意のあるデータ・ホームページからの保護 | | |
| 3.4.1 | ウイルス・フィッシング等に対する予防対策 | セキュリティホールをなくし、不正アクセスで攻撃されるのを防止するため、全てのパソコン及びサーバのOS、オフィスソフト、Webブラウザ、業務ソフトウエアなどに対し最新のパッチをあてるようにしているか。 | ・最新のパッチがあたっていなかったパソコン及びサーバが残っていたために、不正アクセスなどの攻撃に遭って、基幹システムが破壊され2週間以上業務を中断せざるを得なくなったというケースが複数のIT企業で発生している。<br>・最新のパッチを、全てのパソコン及びサーバにもれなくあてるための手順を確立する必要がある。キャビネット等に保管されているノートパソコンなどにパッチをあてるのが漏れるのを、どのように防止するのかということを含めて検討が必要である。<br>·使用するソフトウェアのライセンス管理を適切に行わないと、セキュリティパッチ情報が入手できない場合がある。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 3.4.2 | ウイルス対策ソフトの利用 | 業務で使用する機器がウイルスに感染するのを防ぐため、ウイルス対策ソフトウエアを全てのパソコン及びサーバを対象に設定し、常時稼動させているか。また、ウイルス定義が最新になるように更新しているか。 | ・ウイルスは電子メール、デジタル媒体、ソフトウエア媒体などに含まれて、外部から社内に入り込む。ウイルス対策が不完全なパソコン/サーバでこれらを扱うことによって感染し、感染したパソコン/サーバに色々な悪さをしたり、更にネットワークに接続された別のパソコン/サーバへの悪さや二次感染を引き起こし、またこれらパソコン/サーバにある情報を外部へ送り出したり、パソコンにあるアドレス帳を悪用してそのアドレスへウイルスを転送することもある。<br>・感染したウイルスが、自社で開発・製造した商品に入り込んで、出荷した商品を通して、全国のお客様に迷惑をかけるという事故例もたびたび報告されている。<br>・ウイルス対策ソフトを、全てのパソコン／サーバを対象に常時稼動させることが必須である。<br>・自宅のパソコンからのリモートアクセスを認めているような企業では、自宅のパソコンのウイルス対策も完全にさせる必要がある。 |
| 3.4.3 | ファイル交換用P2Pソフトウエアの使用禁止 | 予期せぬ情報漏えいを防止するため、Winnyなど外部の不特定多数の人々と情報共有するようなリスクの高いファイル交換用P2P（ピア・ツー・ピア）ソフトウエアの使用を公私とも禁止し、かつ順守しているかを検査しているか。 | ・Winnyなど外部の不特定多数の人々と情報共有を行えるソフトウエアは非常にリスクが高い。これらの情報共有ソフトウエアで情報共有されて流通される情報のなかには、ウイルスに汚染された情報、故意にウイルスを仕掛けた情報、複写や譲渡が法令で禁止された情報、漏洩した情報、なども含まれているからである。<br>・Winnyなど情報共有ソフトウエアは便利で有用なソフトウエアであるが、利用者の匿名性が高く利用方法が統制されないので、前記のようなリスクの高い情報が氾濫していること、情報システムを使用して業務を行う従業員等にとってふさわしくないソフトウエアであること、を従業員等によく周知し、公私とも使用を禁止する旨を通知し、順守を誓約してもらうことが必要である。 |
| 3.4.4 | Webブラウザのセキュリティ設定 | 個人データや機密情報を扱うパソコンなどは、リスクを極力低減させるために、Webブラウザのセキュリティを高に設定したり、電子メールをテキスト形式に限定しHTMLメールを使用禁止にしたりしているか。 | ・不正アクセスは色々な手口が用いられるが、WebブラウザでのJavaやActiveXコントロールの動作、HTMLメール形式の電子メールがその手口に使われることがある。<br>・不正アクセスの手口に利用される可能性がすこしでも高いものは、業務上利用しなくて済むものであれば、使用できないようにあらかじめパソコンの設定をすべきである。 |
| 3.4.5 | 許可されていないソフトウェアの利用の禁止 | 予期せず情報を破壊されたり改ざんされたりすることを防ぐため、業務で用いるパソコンには、組織で許可したソフトウェアのみをインストールするような工夫や手続をしているか。 | ・製品として販売されているソフトウエアのほかに、無償のフリーソフトウエアが出回っているが、品質保証がないフリーソフトウエアはその分製品のソフトウエアよりもリスクが高い。従業員等が勝手にこれらのソフトウエアを会社のパソコンにインスツールするのは危険である。<br>・業務で利用するパソコンで利用するソフトウェアは、システム管理者が確認し、組織で許可したアプリケーションのみを使う。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 3.5 | バックアップ | | |
| 3.5.1 | パソコン・サーバ上のデータ・システムのバックアップ取得 | 情報システムの障害・故障でのデータの損傷・滅失に備えるため、定期的にバックアップを取得し安全な場所に保管しているか。 | ・情報システムの信頼性は高くなってはいるが、情報機器の磨耗・劣化などによる故障、ネットワークやソフトウエアなどの性能上の限界やぜい弱性による障害、などでシステムダウンやデータ破壊を起こすことがある。これらの障害・故障の時期を予知することはできないし、また同じ機器でも、一つ一つでばらつきがでる。<br>・どの機器のデータがいつ損傷・消失しても、業務中断から一定の時間内に業務を復旧することができるように、その復旧に必要なデータをバックアップしておくことが必要である。<br>・バックアップは許される復旧時間の限度に応じて、バックアップ取得サイクル時間を決める必要がある。<br>・バックアップは、蓄積したデータだけでなく、ソフトウエア、ソフトウエア修正情報、設定情報、定義等、多方面の情報に及ぶ。<br>・バックアップを安全な場所に保管すること、復旧の手順が明確になっていること、復旧手順がスムーズに行えるように訓練されていること、も求められる。事業継続のために、火災や大地震で事業所が罹災した場合の復旧をどのように行うかについても考えておく必要がある。 |
| 3.6 | ネットワークのセキュリティ管理 | | |
| 3.6.1 | ネットワークの利用方針とセキュリティ方針の策定 | ネットワーク経由の不正アクセスから情報システムを保護するため、全体のネットワークセキュリティを専門家やITベンダーに設計させて、設計したネットワークセキュリティ方針を明確にしているか。 | ・情報機器に対する物理的対策を実施しても、ネットワークに対する技術的対策が疎かでは、情報システムの情報を保護することはできない。ネットワーク経由の不正アクセスは目に見えないので、なおさら厄介である。<br>・ネットワークセキュリティは、ネットワークとセキュリティの両方を理解し、実績のある専門家やITベンダーによって、設計される必要がある。ネットワークとセキュリティに強いベンダーなどに依頼するのがよい。<br>・ネットワークのセキュリティ設計をしっかり行っても、その方針を守って維持していかなければ意味がない。したがって、維持していくための体制・ネットワーク設置・変更の手続きが確実に実施できるようにする必要がある。 |
| 3.6.2 | ネットワークサービスの利用方針とセキュリティ方針の策定 | ネットワークセキュリティ確保のため、ネットワークサービス各機能をサーバ上に設定したり、外部のサービス機能の利用を申し込んだりする場合、そのサービス機能のセキュリティについての評価と必要な対応策についての検討を専門家やITベンダーに行わせているか。 | ・ネットワークに関するサービス機能としては、メールサーバ、Webサーバ、ウイルス検疫、ファイル転送、など色々なサービスがある。どれも、セキュリティに大きく影響する機能である。機能的な便利さ、経費面だけにとらわれずに、全体的なセキュリティへの影響を十分評価し、必要な対応策を検討する必要がある。<br>・ネットワークサービス機能のセキュリティは、ネットワークのセキュリティと一緒に検討が必要なので、実績のある専門家やITベンダーによって、評価・検討を行う必要がある。ネットワークとセキュリティに強いベンダーなどに依頼するのがよい。<br>・またネットワークサービス機能の運用や維持についても、方針や手続きを明確にする必要がある。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 3.7 | 書類・取外し可能な媒体・パソコン内臓のディスク装置等の情報の安全保護 | | |
| 3.7.1 | 書類・取外し可能な媒体の利用方針と取扱い手順の策定 | 情報漏えい防止のため、パソコンの外部媒体の使用・持ち出し・持ち込みについて制限等の管理ルールを決め、それが守られているかを点検しているか。 | ・“物品”など有形物については独占的な所有権・使用権など法的な権利が認められ、これらの権利を侵害する損壊・詐取・窃盗などの禁止・罰則(刑罰)によって、保護が図られている。しかし、“情報”については元々人と人との日常のコミュニケーションの中で伝達が行われていることから、情報の入手、複写、持ち出し、口外、受け渡しを直接規制する法令・罰則はない。住民票データ21万件を自分のMOにコピーして名簿業者に売った学生アルバイトが無罪放免になった事例もある。<br>・個人情報の漏洩等で本人に迷惑をかけないように、事業者がきちんと個人情報を管理することが法令等で要求されている。上記のように悪意で持ち出そうとする者に対する法的な規制はないから、社内規則によって過失や故意による個人情報の流出を禁止して違反者に罰則を与えるという対策が必須である。性善説に基づくあいまい(誠意をもって、忠実に、等)な表現の社内規程だけでは不適当である。<br>・営業秘密については不正競争防止法で不正利用を規制しているが、社内で漫然と取扱っている情報は営業秘密とみなされず法的保護はされない。事業者が社内で営業秘密の情報をきちんと区分・識別表示、作成者・配布・開示者の限定、安全な保管・安全な廃棄等を社内規則で決めて、実際にそれが実行されていないといけない。<br>・パソコンの外部媒体の使用・持ち出し・持ち込みについて制限を設けることが必要である。また、それが守られているかの点検も必要である。<br>・許可したパソコンの外部媒体については、その使用・保管・持ち出し・持ち込み・廃棄についての許可を得る手続き、媒体の管理方法、記録についてのルールを決める必要がある。<br>・私物の媒体については、社内への持ち込み・利用を禁止することが重要である。 |
| 3.7.2 | 書類・取外し可能な媒体、パソコン内臓のディスク装置の安全な処分 | 業務で使用していて不要になったパソコンの外部媒体の安易な廃棄による情報漏えいを防止するため、その廃棄管理ルールを決め、それが守られているかを点検しているか。 | ・廃棄する媒体に記録されているデータを、単なるファイルの削除やフォーマットだけで処理するだけでは、完全にデータは消えず単に読み出せない処理をしているに過ぎないので、データ復活ソフトなどを使用することによりデータが復元し、廃棄した媒体から情報漏洩する可能性が高い。<br>・業務で使用していたパソコンの外部媒体については、そこに記憶された情報について、記憶、利用、消去について許可を得る手続き、媒体の管理方法、記録についてのルールを決める必要がある。<br>・媒体を廃棄する場合又は媒体を再利用する場合、その許可、媒体に含まれる情報の完全な消去の方法、消去の実施と記録、媒体の安全な廃棄の方法、廃棄の記録、等の手続きを決め、それが守られているかを点検しなければならない。 |
| 3.7.3 | 秘密情報の保護手順の策定 | 重要な情報資産を守るため、情報の機密区分とそれに応じた取り扱い及び保管手順を定め、その通り実施しているか。 | ・営業秘密は社内できちんと秘密として適切に管理して保護していないと、不正競争防止法による不正利用からの保護の対象にならない。<br>・個人情報は法令によって、取り扱う個人情報を特定し、利用目的を定め、利用目的を公表し、公表・同意した範囲でのみ取得・利用・提供することができる。また、保有する個人情報のデータの適正化、安全保護、個人データについての開示等への対応を行わなければならない。<br>・事業者は、営業秘密や個人情報を適切に保護するために、社内のすべての情報について、情報区分・識別表示・作成者・配布・開示者の限定・安全な保管・安全な廃棄等を社内規則で決めて、実行しなければならない。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 3.7.4 | システム管理者用文書などの情報の利用者の制限 | 不正な操作を防止するため、システムを運用管理する者だけが利用すべき仕様書類は、他の者に見せないように管理しているか。 | ・ネットワーク、情報システム、業務システム及びデータベースに関する仕様書等を許可されない者が見ることにより悪用されると、情報システム上のデータが不正アクセスされる恐れがある。<br>・ネットワーク、情報システム、業務システム及びデータベースに対するアクセス権やセキュリティ設定方法と設定内容は、システムを運用管理する者だけが知れるようにし、その他の者には知られないようにしなければならない。<br>・システムを運用管理する者が、誤りや不正をしないように、また事業継続のために、システムを運用管理する者の行動を別の管理者が監督するようにしなければならない。 |
| 3.8 | 情報の安全な受渡し | | |
| 3.8.1 | FAX・電話を含む各種の情報受渡しの安全についての方針及び手順 | FAX、留守番電話、携帯電話の取扱いについて、情報漏えいを防止するため、取扱いルールを設けているか。 | ・FAXの送信先誤り、留守番電話の録音が別の者に聞かれる、携帯電話の話が周りのものに聞かれる、携帯電話の紛失・盗難などによる情報漏えいは、いつ起こるかもしれない。<br>・FAX、留守番電話、携帯電話の取扱いについて、適切な安全策を講じることで、これらによる情報漏えいを防止する必要がある。 |
| 3.8.2 | お客や委託先など外部との安全な情報受渡しについての手順の策定と合意 | 個人情報や機密情報を、顧客や委託先等と安全確実に受け渡すため、あらかじめ安全な受渡し方法を取決めた上で、情報の受渡しを行っているか。 | ・個人情報や機密情報の受渡しの際に、紛失、盗難、成りすまし等によって情報流出が発生する可能性がある。<br>・安全で確実な方法で受け渡すように、顧客や委託先との間で、情報の受渡し方法について取り決めをしておく必要がある。 |
| 3.8.3 | 事業所間の文書・媒体・情報機器の安全な配送についての手順の作成 | 事業所間等で個人情報・機密情報を配送する場合のセキュリティ確保のため、配送する記憶媒体やその情報の保護方法をルールで定めているか。 | ・個人情報や機密情報の配送時に、紛失、盗難、のぞき見、破損等によって情報の流出や滅失が発生する可能性がある。<br>・配送中のリスクを想定して、これらに対する防御策又は万一の場合でも内容が漏れないように暗号化するなどの安全保護を図る必要がある。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 3.8.4 | インターネットによる外部のWebアクセス・電子メール通信の安全についての手順の作成 | インターネットのWebや電子メール等を利用した情報の授受について、ウイルス、偽サイト、パスワード盗聴、電文の盗み見、電文の改ざん等の被害に遭わないために、予防策を講じるようにルールを定めているか。 | ・会社のパソコンを使い、インターネット経由で外部と電子メールを送受信したり、外部のWebへアクセスし情報をダウンロード／アップロードしたり、外部の掲示板に投稿したりすると、会社の機密情報・個人情報が流出することがありえる。<br>・このようなインターネットを通しての外部との通信は、業務上必要なものに限定したり、可能ならツール等で制限することが望ましい。<br>・業務上で許可を得て個人情報・機密情報を電子メールで通信する場合は、暗号化・パスワードで保護するようにしなければならない。<br>・また、従業員が故意や過失で、外部に個人情報・機密情報を送信することや、業務上参照が禁止された外部ホームページを参照することを抑止するために、ツールで送受信内容や送受信先をチェック(フィルタリング)したり、クライアントパソコンの操作・通信についてのログを取得し記録確認したりする等の牽制策も検討が必要である。 |
| 3.8.5 | 社内の情報共有・グループウエアの安全な利用についての手順の作成 | 社内の共用サーバ、電子キャビネット、グループウエアなどで情報共有した情報を保護するため、業務上必要な者だけにその情報のアクセス許可を与えるような仕組みが整備され、それが守られて運用されているか。 | ・社内の共用サーバ、電子キャビネット、グループウエアなどの情報共有で、蓄積された情報のアクセスを無条件で全員に許可すると、適切な情報保護が行えない。<br>・社内における情報共有は、共有される従業員等全員に許可されている情報のみに限定する、利用者が限定された情報は許可された者だけがアクセスできるようにアクセス制限する、利用者の利用方法を限定(表示のみ、印刷可、写し保存可、更新可、削除可等)する必要がある情報はそれだけが可能なように情報のアクセス権を設定する、等のアクセス制御を行うような仕組みが必要になる。<br>・また、社内で共用される情報が誤って社外にそのまま転送等で送信されないように制限する必要がある。 |
| 3.9 | 電子取引サービスの安全 | | |
| 3.9.1 | 電子商取引の安全策 | 取引の安全を期すため、電子商取引については、禁止するか、必要な場合許可制で利用させるようにしているか。 | ・従業員等が単独で商品・サービスの出品や購入などの電子商取引を行えるようにしておくと、誤った取引や不正な取引のリスクが高まる。<br>・正式な許可のない電子商取引を禁止しなければならない。<br>・業務上利用が必要であれば、事前に責任者の許可を得て、また、取引の個々の結果に対して責任者が承認するような手順を設ける必要がある。 |
| 3.9.2 | オンライン取引の安全策 | オンライン取引の安全を期すため、オンライン取引については、禁止するか、必要な場合許可制で利用させるようにしているか。 | ・従業員等が単独で、株取引・入出金・切符購入などのオンライン取引を行えるようにしておくと、誤った取引や不正な取引のリスクが高まる。<br>・正式な許可のないオンライン取引を禁止しなければならない。<br>・業務上利用が必要であれば、事前に責任者の許可を得て、また、取引の個々の結果に対して責任者が承認するような手順を設ける必要がある。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 3.9.3 | 外部公開ホームページに掲載する情報の承認と安全保護策 | 会社の信頼を損なわないため、外部向けのホームページに掲載するコンテンツの事前の承認手続きを定め、実施しているか。また、外部向けホームページのウェブサーバへの不正侵入やホームページの改ざん防止策について定めているか。 | ・インターネットを通じて外部に公開するホームページに掲載するコンテンツは、対外的な影響が大きいので、信頼性の確保が不可欠である。<br>·ホームページに掲載するコンテンツの信頼性を確保するために、コンテンツの内容を事前に社内で審査・承認する手続きが必要である。<br>・外部向けのホームページは、不正侵入・改ざんに対する防止策を講じると共に、万一の改ざん・破壊・故障を考慮して短時間に復旧できるように対策を講じておく必要がある。 |
| 3.1 | 情報システム及び人的作業のセキュリティ監視 | | |
| 3.10.1 | パソコン・サーバ・ネットワークの操作や異常についてのログ取得 | 個人情報・機密情報を含むサーバ及びパソコンに対する誤った操作やアクセスの異常を検出するため、監査ログを記録し点検しているか。 | ・不正アクセスの防止には、予兆の検出が重要である。<br>・不正アクセスや誤ったアクセスの検出のために、個人情報・機密情報を含むサーバに対する操作やアクセスの異常についてのログ（監査ログ）を記録し、定期的に点検する必要がある。 |
| 3.10.2 | 業務システム・データベースの利用が適切かの監視 | 個人情報や機密情報などのデータの不正利用を早期発見するため、データに対するアクセスを記録し、データの不正利用がないかを点検しているか。 | ・アクセスを許可された従業員等が、データを不正に検索・参照することは容易である。このことが、データの不正持ち出しや流出という事件・事故の誘因にもなっている。<br>・許可のないデータへの不正アクセス、及び、アクセス権を許可された者によるデータの不正利用を防止又は牽制するために、個人情報・機密情報を管理するサーバや業務システムに対するデータアクセスを記録し、点検することが望ましい。 |
| 3.10.3 | 取得したログの情報が消失・破壊されないように保護 | ログ機能が誤って停止したり、採取したログが不正アクセス・改ざんされないため、ログ機能を保護する対策を講じているか。 | ・不正アクセスを行うものは、不正アクセスの痕跡を消すために、ログを消去しようとする。そのため、採取したログが不正アクセス・改ざんされないように保護することが必要である。<br>・また十分な容量のログ領域を確保し、ログ機能が停止しないように配慮することが必要である。<br>・情報の不正アクセスから長い期間が経過してから漏洩の事実が判明することがある。したがって、定期的にログをアーカイブし、将来に調査ができるように、一定期間アクセスを禁止して保管することが必要である。 |
| 3.10.4 | 実務管理者及び運用担当者の作業日誌の点検 | トレーサビリティ確保のため、個人情報や機密情報を含む情報を取り扱う業務の実施・操作・運用を行う者には、作業日誌を付けさせ、業務の責任者が点検し、記録を保管しているか。 | ・従業員等の業務を点検・監督しないと、誤りや不正があってもその露見が遅れる。<br>・個人情報・機密情報を含む情報を取り扱う業務を適正に運用したかどうかを確認できるように、業務の実施・操作・運用を行う者は、作業日誌を付け、実施内容や検出した事象を記録し、業務の責任者の点検を受け、これらの記録を保管する必要がある。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 3.10.5 | 発生した情報機器の障害についての記録と対処 | 障害等の再発防止のため、検出した障害を記録し、分析し、是正・予防処置に活かしているか。 | ・検出した障害を放置すると、障害が繰り返し発生したり、より重度の障害が発生することがある。<br>・ヒヤリハットや軽度の障害が、重度の障害の前兆である場合がある。<br>・検出した障害は、それがヒヤリハットや軽度の障害であっても、記録し、分析し、是正・予防処置に活かす必要がある。<br>・検出した障害の、報告・記録・対処・是正予防処置の手順を定めて、その通りに実行すべきである。 |
| 3.10.6 | パソコン・サーバのコンピュータ時刻の同期 | ログの記録の正確性を確保するため、サーバ及びパソコンのコンピュータ時刻を同期させているか。 | ・サーバ及びパソコンのコンピュータ時刻が同期していないと、サーバ及びパソコンのログの調査が容易に行えない。<br>・サーバ及びパソコンのコンピュータ時刻を同期させるソフトウエアツールがあるので、これらを導入し・設定しておく。 |
| | | | |
| Ⅳ | 情報資産利用時のセキュリティ | | |
| 4.1 | 情報の利用制限の方針策定 | | |
| 4.1.1 | アクセス制御の方針策定と見直し | 情報システムやデータの利用を適切に制御するために、アクセス制御の方針を定めて文書化し、関係者に周知するとともに、環境や技術等の変化に対応して方針の見直しを行っているか。 | ・複雑化する情報システムにおいて、情報システムやデータを確実に保護するためには、アクセス制御の方針について基本設計し、文書化しておく必要がある。<br>・アクセス制御の基本設計の中で、<br>－システムの利用者に関する方針<br>－システム管理者等の特別なアクセス権（特権）に関する方針<br>－ネットワーク利用に関する方針<br>－基本ソフトウエアのアクセス制御に関する方針<br>などを定める。<br>・アクセス制御の目的は、正当な利用者による情報資産の正当な利用は許可し、不当な利用者による情報資産の利用は不可能になるように制御することである。<br>・保有する情報資産に対し、正当な利用者であるか否かの判定をする必要がある<br>・情報の利用制限を定めるためには、はじめに取り扱うすべての情報の機密度を明確にし、次に情報の機密度に応じて利用者を制限する必要がある。<br>・機密度の低い情報の利用制限は意味がないし、機密度の高い情報への利用制限を怠ると情報漏えいのリスクが高くなる<br>・情報の活用による便益とリスクのバランスを考慮して利用制限を決めることが大事である。<br>・アクセス制御の方針に基づき、アクセス権限付与者、付与判断基準、付与手順などの具体的なルールや手続きを文書化し、関係者全員に周知徹底することが重要である。<br>・方針は環境や技術等の変化に対応して見直しする必要がある。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 4.2 | 情報システム利用者の管理方法 | | |
| 4.2.1 | 情報システムの利用者登録と削除 | 許可された者だけが情報を利用できるようにするために、情報システムのすべての利用者に対し、利用者ID及びアクセス権の登録と削除のルールを定め運用しているか。 | ・許可されていない者による情報システムの利用によって情報の不正利用や漏えいのリスクが高まるので、情報システムの利用者を制限する必要がある。<br>・情報は許可された者だけが利用できるように、利用者に利用者IDと初期パスワードを発行し、情報システムや情報へのアクセス時には、利用者IDとパスワードによる認証を行う。<br>・利用者IDと初期パスワードの発行は、正式な申請・発行手続きを定めて行う。<br>・組織内での役割によって利用できる情報は異なるので、役割に準じて利用者IDのアクセス権（利用権限）を設定するルールを定め文書化する。<br>・異動、退職などに伴って発生する利用者IDとアクセス権の変更は速やかにかつ確実に実施する。<br>・ルールに従って利用者IDとアクセス権が付与（もしくは剥奪）されていることを定期的に確認することも大事である。 |
| 4.2.2 | 特別なアクセス権（特権）の管理 | システム管理者等へ付与する特別なアクセス権（特権）の不正使用を防止するために、特権の付与ルールを定め、厳密に管理しているか。 | ・特別なアクセス権（特権）を付与された利用者（例えば情報システムの管理者）はすべての情報を利用できてしまうので、限られた者だけに付与し、さらに不正利用を防止する仕組みをつくる必要がある。<br>・特権を割当てるルールを定め文書化する。<br>・特権の付与は、管理責任者を定めて厳密に管理することが大事である。<br>・特権の付与と剥奪の状況は、随時記録しておく必要がある。<br>・特権を利用した作業は、常に記録させ、管理者が点検するようにする。<br>・特権は、特定の人に集中しないよう、権限を分け、牽制がきく付与体系とする。 |
| 4.2.3 | 利用者のパスワードの管理 | 情報システムの不正利用を防止するために、利用者に対して初期パスワードの発行とパスワードの変更のルールを定め周知しているか。 | ・パスワードの発行と変更を適切に行わないとパスワードの不正使用によって情報システムの不正利用のリスクは高まる。<br>・初期パスワードの発行と利用者が最初に使うときの変更のルールを定め周知する必要がある。<br>・同じIDとパスワードを複数人で利用するグループ・パスワードは、できるだけ使用しないことが望ましい。<br>・グループ・パスワードを利用せざるを得ない場合は、利用者と利用時間の記録、パスワードの他人への告知の禁止、グループから退会者が出た場合の速やかなパスワード変更などのルールを定めて運用する必要がある。 |
| 4.2.4 | 利用者のアクセス権の見直し | 退職や異動などによる役割の変更に伴う情報の不正利用を防止するために、該当する利用者に対してアクセス権を適時かつ定期的に見直しているか。 | ・退職時に情報システムのアクセス権を削除することを忘れると、不正利用のリスクが高まる。<br>・アクセス権は必要がなくなった時点で速やかに剥奪する。<br>・アクセス権は定期的に見直すことが重要である。<br>・特に特権の見直しは頻繁に実施する必要がある。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 4.3 | 情報システム利用者の順守事項 | | |
| 4.3.1 | パスワードの使用方法 | パスワードの推測や漏えい等による情報システムの不正利用を防止するために、パスワードの選択と利用の仕方をきちんと定め利用者に周知するとともに、守られているかを定期的に確認しているか。 | ・パスワードの類推や漏えいは、他人によるなりすましを誘発し、情報システムへの不正アクセスのリスクが高まる。<br>・情報システムの利用者がパスワードを決める際には、質の良いパスワードを選択させる。<br>・質の良いパスワードの選択の仕方、定期的な変更の仕方などの運用ルールを定める。<br>・パスワードを目に触れるところに記録しておくことは、不正使用のリスクを高めるので、絶対にしない。<br>・運用ルールが守られているかを定期的に確認し、再徹底することが大事である。 |
| 4.3.2 | 無人状態の情報機器の保護 | サーバーの操作端末やコピー機等の無人状態の情報機器が不正利用されないように、保護と管理のルールを定め周知するとともに、定期的に確認しているか。 | ・サーバーの操作端末やコピー機等の無人状態に置かれる情報機器は、不正利用されるリスクが高い。<br>・サーバーの操作端末や業務専用端末等は、利用中又は利用を中断して離席するときは、ログオフするかパスワード付スクリーンセーバを起動するなどによって、他の者に操作されないようにする。<br>・監視できない場所に無人状態に置かれるコピー機などは、利用者カードがないと利用できないようにする。<br>・コピー機に書類を置き忘れないよう注意する。 |
| 4.3.3 | 離席時、退社時のパソコンの保護(クリアスクリーン) | パソコンを利用していないときに他人に不正利用されないために、離席時や退社時のパソコンの保護と管理のルールを定め周知するとともに、定期的に確認しているか。 | ・パソコン利用時に一時席を離れたとき、他の者に操作されたり情報を不正に読み取られるリスクが高まる。<br>・離席時には、パスワード付スクリーンセーバの起動等の保護(クリアスクリーン)対策を運用ルールで定める。<br>・退社時には施錠管理できる場所に収納するとかチェーンで盗難防止を計る等の対策が必要である。 |
| 4.3.4 | クリアデスク | 机上のメモや書類などを盗み見されないために、机上の整理整頓に関するルールを定め周知するとともに、定期的に確認しているか。 | ・離席時に机上に書類や記録媒体を放置することは、盗み見、紛失、盗難のリスクが高まり、情報漏えいの観点から極めて危険である。<br>・クリアデスクに関するルールを定め周知することが必要である。<br>・常に机上を整理整頓しておき、退社時には一切モノを置かないようにすることが重要である。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 4.4 | ネットワークの利用制限の方針策定 | | |
| 4.4.1 | ネットワークサービスの使用についての方針 | ネットワークの利用によって生じる脅威に対処するために、ネットワーク及びネットワークサービスの利用に関する方針と規程を定め周知しているか。 | ・ネットワークサービスの設定ミスやセキュリティホール(脆弱性)を放置すると、不正アクセスの攻撃対象になり危険である。<br>・ネットワークサービスの導入前に、情報システム全体への影響とセキュリティの確保について検討が必要である。<br>・導入を決めたネットワークサービスについては、ネットワーク及びネットワークサービスの利用に関するセキュリティ方針と規程を定め文書化する。<br>・利用者に応じて、ネットワーク及びネットワークサービスの利用制限を定める。<br>・規程を順守させるための方法を定め周知状況を定期的に確認する。<br>・方針・規程は環境の変化に対応して適宜更新する必要がある。 |
| 4.4.2 | 外部から接続する利用者の認証 | ネットワークを介しての外部からの不正利用を防止するために、外部から接続する利用者を認証する適切な方法を定めているか。 | ・外部からのネットワーク接続には、従業員によるモバイル情報機器の接続、顧客や委託先による接続などがあるが、一方で情報の破壊、改ざんや漏えいを目的とした悪意ある者による不正な接続もある。<br>・外部からの不正なネットワーク接続が行われると、甚大な影響を引き起こすので、技術と管理の両面から防止策を講じる必要がある。<br>・認証の技術的な方法の導入と運用はITベンダーに依頼する。<br>・外部からの利用者は登録を許可したものに限ることとし、登録と削除に関する運用ルールを規程として定める。<br>・ネットワーク接続の記録をとる。<br>・登録の方法、規程そして認証方法は、定期的に確認する。 |
| 4.4.3 | ネットワークにおける装置識別の利用 | 無許可の者からのネットワーク接続を拒否するために、特定の場所または装置からのみネットワーク接続する方式を利用しているか。 | ・オフィス内に万遍なく有線あるいは無線ネットワークが敷設されると、接続が容易で便利になる一方で、悪意ある者による不正な接続の危険も高まる。<br>・ネットワーク接続を許可する場合には、事前にパソコンに設定した固有の識別(MACアドレス、IPアドレス等)が一致するか否かの認証(装置識別)を行うことで、不正な接続を防止する。<br>・装置識別の仕組みの導入及び運用のための手順書作成に関してはITベンダーに依頼する。 |
| 4.4.4 | 遠隔診断用及び環境設定用ポートの保護 | ネットワーク管理者や運用を委託したITベンダーが、サーバ等を外部から遠隔操作する場合のセキュリティ確保のために、利用ルールを定め、厳格に運用しているか。 | ・サーバの24時間運転を確保するためには、夜間や休日の監視及び万一の場合のサーバの再起動が必要になる。そのために、ネットワーク管理者や運用を委託したITベンダーは、外部からサーバ等を監視・操作するための接続を利用するが、これらの外部接続が悪用されたら、情報システムの安全性は保証されない。<br>・外部からの監視・操作のための接続の仕組み、利用方法、そしてネットワーク管理者の退職・変更時の対応を含む管理については、ITベンダーに依頼する。 |
| 4.4.5 | ネットワークの領域分割 | 基幹業務のセキュリティを高めるために、基幹業務と他とのネットワークの領域分割を利用しているか。 | ・従業員向けの社内情報共有システム(メールやファイル共有)、基幹業務システム(財務会計・人事管理、サービス提供等)、そしてインターネット等の外部接続システム(E-mailやWebシステム)は、それぞれ、セキュリティの要求レベルが異なる。<br>・これらのシステムが混在するある程度の規模のネットワークでは、それぞれのシステムを独立させてセキュリティを確保することが有効であり、そのためにネットワークを分割する。<br>・具体的な設計及び導入方法についてはITベンダーに依頼する。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 4.4.6 | ネットワークの接続制御 | インターネット等の外部の共有ネットワークに接続する場合のセキュリティを確保するために、ファイヤーウオールを設置したり、利用者の利用制限を定め周知しているか。 | ・インターネット等の共有ネットワークを利用する場合、外部からの不正アクセス、電子メールによるウイルス感染、外部サイトによるフィッシングなどの脅威にさらされていることを意識しておく必要がある。<br>・外部からの不正アクセスに対しては、ファイアウオールを設置し安全をはかる。<br>・ウイルス対策ソフトウエアを導入する。<br>・インターネット利用のルールを定め周知する必要がある。<br>・新たな脅威が生まれるのに応じて、利用ルールは適宜見直す必要がある。<br>・利用者のルールの順守状況を定期的に確認する。 |
| 4.4.7 | ネットワークの経路制御 | セキュリティを高めるために、業務上必要なネットワークにしか接続できないように経路の制御をしているか。 | ・社内や開発委託先の従業員等、あるいは許可されて外部から接続する関係者が、業務上必要がないのに、基幹系やサービス提供のシステムが存在するLAN等に接続できるようになっていると、これらシステムへの不正アクセスのリスクが高まる。<br>・利用者が業務上必要なネットワークにのみ接続でき、他のネットワークへの接続を遮断するように、経路を制御することが望ましい。<br>・経路の制御については、ファイヤーウオール/ルータ/プロキシサーバ等で設定できるが、その必要性と設計、導入と運用手順書の作成はITベンダーに依頼する。 |
| 4.5 | 基本ソフトウェア（OS）のセキュリティ設定 | | |
| 4.5.1 | セキュリティに配慮したログオン手順 | 基本ソフトウエアの不正利用を禁止するために、基本ソフトウエアへのログオン（利用開始）手順をきちんと定めているか。 | ・パソコンやサーバの利用は、そこに内蔵された基本ソフトウエアの起動から始まるので、基本ソフトウエアの利用に関する管理は、パソコンやサーバの利用に関する管理と同じことを意味する。<br>・複数のユーザに利用されるサーバの場合、基本ソフトウエアの直接利用や設定変更は、特別に許可されたシステム管理者に限定される。<br>・ログオン手順の設計と運用方法は、ITベンダーに依頼する。<br>・ログオン手順の中で、利用が許可されていない者の不正ログオンを禁止する仕組みを実現する。 |
| 4.5.2 | 利用者の識別と認証 | 基本ソフトウエアの不正利用を禁止するために、利用者を識別し認証するようにしているか。 | ・利用者の識別と認証の方法は、ITベンダーに依頼する。<br>・基本ソフトウエアは許可された者のみが利用できるように、利用者を識別し認証する。 |
| 4.5.3 | パスワード管理システム | 良質のパスワードを維持するために、利用者のパスワードの変更を管理しているか。 | ・パスワードの管理ルールの作成及び管理ツールの採用は、ITベンダーに依頼する。<br>・利用者毎にIDとパスワードの変更を管理するツールとそのルールを定めることが必要である。<br>・パスワードの管理ルールは定期的に確認する。<br>・パスワードの定期的な変更を利用者に促し、変更を確認することが大事である。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 4.5.4 | システムユーティリティの使用制限 | システム管理者用のシステムユーティリティの不正利用を防止するために、利用ルールを定め、厳格に管理しているか。 | ・システムの機能や動作環境、利用者権限、セキュリティ等の設定を行うシステムユーティリティは、システム管理のための特別なソフトウエアであるので、一般の使用は大きなリスクをともなうので禁止する。<br>・システムユーティリティの利用制限の方法と管理は、ITベンダーに依頼する。<br>・システムユーティリティは特別に許可された情報システム管理者のみが利用できるようにルールを設定する。<br>・そのために利用者を厳格に識別し認証する手順を使用する。<br>・システムユーティリティを利用したシステムの変更は、そのつど記録を取り定期的に確認する。 |
| 4.5.5 | セッションのタイムアウト | 使用が一定時間中断した場合におけるリスクに対応するために、システムを強制的に遮断する仕組みにしているか。 | ・パソコンや業務システムの使用を中断したまま席を外す等で長時間放置すると、別の者に操作されるリスクが高まる。<br>・使用の中断が一定時間経過したら、画面や通信を強制的に遮断し、パスワードの再入力あるいは再ログインによってしか使用が再開できないようにする。 |
| 4.5.6 | 利用時間の制限 | 取り扱いに慎重を要する業務ソフトウエアは、リスクを軽減するために、利用時間の制限をしているか。 | ・業務処理の終了後も業務システムを利用可能にしておくことは、不正アクセス、不正利用の温床になり危険である。<br>・必要なときにだけシステムを立ち上げ、終了後は速やかに停止させる等によって利用制限をする。<br>・制限が必要な業務ソフトウエアの有無を確認し、制限方法を検討する必要がある。 |
| 4.6 | 業務ソフトウェアの利用者制限 | | |
| 4.6.1 | 情報の利用制限 | 業務システムのセキュリティを確保するために、当該業務システム（ソフトウエア及び情報）の利用者を、正当な権限を持つ者に制限しているか。 | ・権限のない者による業務システムの利用は、情報の正確性、安全性、機密性を損なう。<br>・業務システム（ソフトウエア及び情報）の利用制限は、組織全体の利用制限の方針に従う必要がある。<br>・業務システムの利用者に対する利用制限（例えば、書き込み、読み出し、削除、変更など）をきちんと定め文書化するとともに、定期的に確認することが重要である。<br>・業務システムの利用は業務と密接に関連しているため、利用者の役割に応じて厳密に権限を設定すべきである（例えば、書き込み・変更・削除ができる権限、参照だけしかできない権限等）。 |
| 4.6.2 | 取り扱いに慎重を要するシステムの隔離 | 機密レベルの高い情報のセキュリティを強化するために、機密情報を扱うシステムは隔離された専用ルームに設置し、入退室を厳重に管理する等の措置を講じているか。 | ・機密情報を扱うシステムは、特別に設置された部屋に隔離施錠し、入退室の管理が必要になる。<br>・隔離された場所が確保できない場合は、管理責任者を定めて厳格に管理する。<br>・システムの利用状況と履歴、及び入退室の記録を保有し、定期的に確認することも大事になる。 |

| 項番 | 項目 | 経営者への質問 | 脅威とリスクの喚起と実施のためのアドバイス |
|---|---|---|---|
| 4.7 | モバイル情報機器の利用に関する管理 | | |
| 4.7.1 | モバイル情報機器利用のルールと管理 | ノートパソコン、携帯電話、ICカードなどの携帯可能なモバイル情報機器の持ち出し及び持ち込み時におけるセキュリティ確保のために、これらの携帯情報機器の利用に関するルールと罰則規定を定め周知しているか。 | ・モバイル情報機器の置き忘れ、紛失、そして盗難による顧客の個人情報などの機密情報の漏えいは、組織に甚大な損害を与える。<br>・モバイル情報機器の利用、特に組織外への持ち出しに関するルールを明文化し周知徹底することが重要になる。<br>・原則として組織内で使用している機器の持ち出し、外部からの機器の持ち込みは禁止する。<br>・持ち出す場合には、機器内の記録情報(とりわけ機密情報)は暗号化する。<br>・ルール違反の場合の罰則規定もきちんと定めておく。<br>・モバイル情報機器の利用による事故が発生した場合には、きちんと報告させ記録する。<br>・環境の変化に対応してルールの定期的な確認と見直しも必要である。<br>・モバイル情報機器利用者の意識向上のためには定期的な教育訓練も必要である。 |
| 4.7.2 | テレワーキングのルールと管理 | 自宅などの外部で業務をする場合(テレワーキング)のセキュリティを確保するために、許可するか否かも含めて、このような作業形態に関するルールと管理の方法を定め周知しているか。 | ・自宅、出張先のホテルなどで業務を行うことは、情報セキュリティの観点からリスクが高いと意識しなければならない。<br>・テレワーキングのためのルールは、組織全体の情報セキュリティ方針に基づいて定める。<br>・テレワーキング場所のセキュリティ環境が重要であり、場所の確認が必要である。<br>・物理的セキュリティとシステム的セキュリティが確保されない場所でのテレワーキングは禁止する。<br>・盗み見や盗難などの危険にさらされている場所でのテレワーキングは禁止する。<br>・自宅であってもウイルスやWinny、不正侵入などの外部からの脅威にさらされている場合のテレワーキングは禁止する。<br>・住環境を共にする家族や友人による情報漏えいが起こりえるので注意が必要である。<br>・自宅で業務に使用する情報機器については、家族との共用を厳禁する。<br>・環境の変化に対応してルールは定期的に見直す必要がある。<br>・ルール違反の場合の罰則規定も定める。 |