情報セキュリティ監査人のための監査ヒント集

システム監査学会　情報セキュリティ専門監査人部会

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
1. 情報管理		
1-1. コンピュータ(サーバ、パソコンなど)内の情報		
入力	取得した情報を機密性レベルなどで分類しているか	他者から取得した情報は、社内で的確かつ効率的な管理を行うため、当該情報の保管管理者が、管理対策を明確にした機密性レベルなどによる分類をして管理策を講じなければならない。 情報の管理責任者や保管管理者を明確に定めていないケースが散見される。 機密保持契約がある場合は、契約担当者が情報保管管理者に対し、契約内容による順守事項を契約部門以外でも容易にわかる内容で周知しておくべきである。
	取扱者の権限・責任を明確にしているか	Web から直接入力し、受け取る情報は、その処理を可能な限り自動化し、従業員がアクセス(確認、訂正など)しなくて良いようなシステムにする努力が重要である。 情報を入力した人からの問い合わせに限り、厳密な本人確認を行うとともに、参照／更新できる人は、お客様対応部門などに限定していないと、情報流出のリスクが大きくなる。 システム担当者のアクセスを認めているケースもあるが、リスクが高い。
	預った個人情報や重要情報などの保管は、特定のサーバに限定しているか	個人情報や経営情報、開発情報など重要な情報は、サーバ管理者もアクセスすべきでないため、アクセス権限を大幅に絞り込むが、そのサーバに一般情報と同居させると、一般情報へのアクセスも制限することになり、現実的ではなく、そのために、サーバを分離させるのが良い。
	外部で作成された情報はコンピュータ･ウイルスをチェックしてから使用しているか	ファイアウォール上で、コンピュータ･ウイルスをチェックする場合、圧縮形式ファイルはチェックできないので、ウイルス･チェックをしていない旨、受信者へ明確に伝達しないと危険である。 その場合は、パソコン上でもチェックすることを徹底しておくべきである。
送信	外部へ送信(情報開示)する場合のルールが明確になっているか	外部へ情報を送信し開示する場合、許可権限者の承認を得るルールがあり、運用できなければならない。 送信した内容を、ログに保存するとともに、定期的に内容を確認し、違反がないかチェックする。 重要な情報の発信については、メールシステムに機能を組み込むことにより、発信者の上司などへ自動的に、CCする方法もある。
	送信データ保護のためのセキュリティ措置を講じているか	重要な情報を社外へ送信する場合、ルールとして、データを暗号化する、ファイルにパスワードを設定する、セキュアにファイルを授受できる ASP サービスを利用するなどの対策があり、必要性に応じて、活用すべきである。 パスワードを設定した場合、そのパスワードは、別のメールに分けて送信しないと有効でなく、徹底しなければならない。
	メールの誤送信対策ができているか	うっかりミスによる誤送信対策は、社外への業務連絡一斉送信などは、専用システムが望ましく、個別に発信する場合は、次のような運用を徹底する方法もある。 1) アドレスは、都度入力でなく、アドレス帳に登録し、利用する。 2) アドレス帳は、社内と社外を大別し、混同しにくくするとともに、同姓同名の識別などを徹底する。 3) アドレス帳に、業務用アドレスとプライベート用アドレスの両方を登録している場合、間違えると社外へ発信することになるので、大別させ、注意させる。 4) 相互に知られたくない送信先は、BCC を使用する。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
加工	加工	参照権限と更新権限を明確に分離し、更新権限を絞ることが大切である。 外部記録装置は、情報流出の経路となるので、利用できる人やパソコンを限定しなければならない。
	バックアップを適切に作成しているか	バックアップは、データはもちろん、必要なソフトウェア、ドキュメント類も含めて作成し、業務継続性を保証できなければ意味がない。 重要な情報のバックアップは、暗号化などにより、元の情報と同程度のセキュリティ強度で保護し、保管しなければならないが、失念しているケースもある。
消去	不要になったファイルは速やかに削除しているか	変更履歴すべてを保存するのではなく、保存の必要なファイルを認識し、不必要な情報を削除しなければ、業務の混乱につながる。 ファイルの保存期限を明確にし、その期限を過ぎれば、削除するなどの仕組か運用が必要である。
	パソコン等を廃棄／修理に出す場合、情報の保護措置をしているか	すべての情報を削除し、いななる方法でも情報が漏えいしない対策が必要である。 廃棄の場合、物理的にハードディスクを破壊し、再生不可にすることが望ましい。
1-2. コンピュータ(サーバ、パソコンなど)以外の電子媒体内の情報		
取得	情報の開示先を限定できているか	契約により、情報開示範囲が特定されていて、契約の範囲を超えた組織や人との情報共有の事実があれば、契約違反となること理解させ、徹底しなければなせない。 社内での情報共有の延長線上として、社外から預かっている情報の取り扱いを的確にしなければならない。
	情報授受内容を確認しているか	情報授受時、その件数などを確認するとともに、記録として保存される仕組を準備すべきだが、案外できていない。 第三者(郵便、宅配、バイク便など)を経由した授受の場合、他からの依頼物とのとり違いが発生していないか、受け取り部門で確認できる運用にすべきである。
移送	情報を外部へ持ち出す承認方法が明確化しているか	情報を外部へ持ち出す場合、申請や承認などのルールが明確で、持ち出し台帳に記入など、そのルールどおり運用しなければならず、運用できないようであれば、ルールを見直すべきである。 組織変更などによる業務移管が発生した場合、変更と同時に、情報も移設すること。また、情報管理台帳の追加／削除を記録でき、情報管理者も、変更内容を掌握していなければならない。 重要な情報を複製する場合、複製物に連番を付与し、複製物ごとの保管管理者を登録し、回収／廃棄するまで、管理しなければならない。
	持出用媒体への書き込み管理ができているか	持出用媒体に書き込みできる人やパソコンを限定すべきである。そのために、USBポートやCD/DVDドライブは、書き込み権限のない人は、操作できなくすることが望ましい。 媒体に書き込む場合、バックアップ作成などの理由で、複数作成するなど、必要以上の作業をしていないかチェックできていること。
	持ち出す情報の保護策がとられているか	どのような手段でも、紛失などのリスクが考えられるため、必要に応じて、暗号化するなどの判断できる運用とすべきである。
	外部作成の記録媒体持ち込み時、ウイルスチェックをしているか	外部で作成した情報を持ち込む場合、ネットワーク経由の時と同様に、持ち込んだ人が、水際でウイルスチェックを実施するよう周知徹底しなければならない。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
保管	保管方法を徹底できているか。	保管期限を明記し、保管期限を超えた場合、廃棄する。また、廃棄の責任者を記録する。 保管の記録があり、定期的な棚卸を実施し、過不足がある場合、追求する運用にしなければならない。 貸出の必要がある場合、貸出台帳に記入し、返却も管理できていることが重要である。また、期日までに返却されない場合、督促しなければならない。
廃棄	情報の廃棄	重要な情報は、当該ファイルを削除した後、関係ない情報を上書きするなど、元の情報が残らないよう対応することが望ましい。
	媒体の廃棄	媒体を廃棄する場合、再利用ができないよう、物理的な破壊するなど、万全の措置を実施する。
1-3. 紙媒体の情報		
取得	取得した情報の機密性レベルを判断し、適切な保管ができているか	取得した情報は、社内での管理を適切に実施するため、自社の情報管理方法に適合させるのが望ましく、機密性レベルを判断し、当該の保管／管理方法を適用するのがよい。 契約で、社内に適用している保管／管理方法と異なる部分については、情報を伝達すると同時に、契約で要求されている内容も伝えなければならない。 取得した時点で、情報管理台帳に登録し、漏れが発生させないようにすること。 社内に、同一書類を、複数人が受け取った場合、すべてを保管するのか、一部のみ原本として保管するのか、ルールを定めて、その選択に見合った保管を行う。
	取得情報の内容を確認しているか	取得した情報が、授受の記録内容と合致しているか、確認すること。 封筒から取り出す場合、その一部が、封筒に取り残していないか確認するよう、徹底すること。
移送	情報を外部へ持ち出す承認方法が明確化しているか	情報を外部へ持ち出す場合、申請や承認などのルールが明確で、持ち出し台帳に記入など、そのルールどおり運用しなければならず、運用できないようであれば、ルールを見直すべきである。 組織変更などによる業務移管が発生した場合、変更と同時に、情報も移設すること。また、情報管理台帳の追加／削除を記録でき、情報管理者も、変更内容を掌握していなければならない。 重要な情報を複製する場合、複製物に連番を付与し、複製物ごとの保管管理者を登録し、回収／廃棄するまで、管理しなければならない。
利用	情報の閲覧／持出を制限しているか	重要な情報を閲覧する場合、認められた人が、許可された場所でのみ閲覧し、その閲覧記録を残さなければならない。閲覧スペースは、一般オフィスとは情報を授受できないよう分離されており、作業していることが一般オフィス側からも見えるようにガラスなどで仕切られていることが望ましい。 保管場所から持ち出す場合、その承認ルールが明確で、的確に運用しなければならない。
	情報の複製を制限できているか	重要な情報をコピーなど複製する場合、申請／承認を経て、許可される仕組にしなければならない。 重要な情報の閲覧場所に、デジタルカメラやカメラ機能付き携帯電話を持ち込んだり、撮影したりできないよう、制限すべきである。
保管	保存期限を明確にできているか	書類の必要／不必要を明確にするため、保存期限を明確にし、フォルダの背表紙などに明示し、期限を超えれば、廃棄できるようにすべきである。 必要以上に長い保存期間を設定していないか確認すべきである。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
保管	同一ファイル(バインダ)内に、利用目的や機密性レベルが異なる情報を混在させていないか	ひとつのファイル(バインダ)内に、参照権限の異なる人がアクセスする情報を混在させると、参照する権限がない情報までアクセスできるリスクがあるので、情報の混在を禁止しなければならない。 異なる業務の情報を混在させると、担当外の業務に関する情報まで見れる。 機密性レベルの異なる情報を混在させると、低いレベルのみアクセスできる人は、高いレベルの情報が混在することにより、低いレベルの情報も見れなくなるので、フォルダを分割すべきである。
廃棄	廃棄処理が確実にできているか	重要な情報の廃棄は、他の書類とは明確に分別し、一度投入すると取り戻せないような廃棄箱へ捨てるなどの方策をとるべきである。 重要な情報の廃棄は、専門業者による溶融など、厳密な漏えい防止対策を講じなければならない。
	再利用による漏えい防止対策ができているか	環境保護の観点で、一度、印刷／コピーに利用した紙の裏面を再利用している場合、重要な書類までも再利用し、情報漏えいにつながるリスクがあるので、その行為を禁止しなければならない。
1-4. その他の情報(人の記憶)		
利用	記憶内容の流出を制限できているか	知り得た機密情報を、外部に無断で開示させないようにするため、従業員と、契約書／誓約書で制限する。 従業員が、退職後に、情報を開示しないようにするために、退職時も誓約書を提出させる。 毎日少しずつ自分の頭脳に記憶し、帰宅後に記録をすれば、日数をかけることにより、大量の情報持ち出しにもつながるので、職業倫理意識の低い人は、個人情報や経営情報など機密性レベルの高い業務から外すなどの措置を講じた方が良い。また、機密性レベルの比較的低い業務を担当する中で、職業倫理観の確立した人のみ、重要な業務へ配置転換する方法もある。
2. 組織的対策		
2-1. 組織･体制の確立		
組織体制の整備	情報セキュリティ推進のための運営組織を設置しているか	全社の組織図の中に、情報セキュリティ推進を担当する組織を明確に位置づける。 企業規模などの関係で、推進組織を設置できない場合でも、推進するための委員会を設けるなど代替手段を用意し、実績を積み重ねることにより、恒常組織に格上げできるような配慮をするのも一つの方法である。 少なくとも、情報セキュリティ推進責任者を明確にし、社内外に開示しなければならない。 情報セキュリティ推進責任者は、言い訳をできないよう、専任者するのが望ましい。責任者の専任が困難な場合、専任の担当者を置くことが基本である。
	情報セキュリティに関する事件、事故が発生した場合、すみやかに報告される仕組があるか	情報セキュリティ事故は、緊急の対応を要する場合も多いため、関連部門に対し、すみやかに連絡／報告される仕組にしなければならない。 情報セキュリティ事故は、内容を開示することにより、被害が拡散する場合もあるので、開示範囲は必要最小限に絞るべきである。 社外に影響を与える事故は、事業への影響を心配するあまり開示に消極的になりがちであるが、外部へ積極的に公表すべきである。 対外に影響がある事故の場合、経営者に対してもタイムリーに報告する仕組がなければならない。 被害拡散の応急措置ができた段階で、社内に事故内容とその対策を周知し、再発防止に努めなければならない。
	情報セキュリティ対策の妥当性を検証する機能を設置しているか	情報セキュリティ推進組織を中心に、情報セキュリティの取り組み、推進をしていても、適切で効果的な内容か検証するため、内部監査部門を設置し、チェックすることが望ましい。内部監査部門での検証が難しい場合、外部の審査機関などに要請する方法もある。 社内での脆弱性検査では発見できない脆弱性が残る場合もあるため、外部の専門機関に依頼するなどの対策望ましい。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
組織体制の整備	情報セキュリティに関する経営トップの果たすべき役割を明確にしているか	情報セキュリティ推進責任者から、定期的に情報セキュリティ課題を報告するよう、指示すべきである。経営トップ自らが忙しいからと言って、逃げていたのでは情報セキュリティのレベルは向上しない。事故が起こってからの対策では、後手に廻ることが多い。 事業の重点ポイントと連動し、情報セキュリティ対策の優先順位について、指示すべきである。 今後の事業展開から想定できる情報セキュリティ･リスクについて、事前に対策するよう、情報セキュリティ推進責任者に指示しなければならない。また、情報セキュリティ推進責任者は、事業の方向性から、新たな対応策を経営トップに進言できるレベルでないと、その責務を果たせない。 事故が発生した場合、外部に対し、先頭に立って、事故内容などを開示するよう努めなければならない。
職掌の分離と責任の明確化	業務機能の職掌分離により相互牽制できるが、多くの機能を特定の人に集中させていないか	システム変更の権限を有する人と、システムを利用してデータを更新できる人は、分離すべきである。 システムを開発／変更する人と、システムを操作(オペレーション)する人は、分離すべきである。開発環境と本番環境の担当者を分離できない場合、少なくとも、アカウントを分割し、同時ログインできないなど最低限の対策を導入すべきである。 情報セキュリティの個別課題の対策をする人と、課題解決を確認する人は、分離されていて、対策が計画どおり進捗できるようけん制機能があることが望ましい。 お客様個人情報にアクセスしなければならない業務は、お客様対応部門など特定の部門に集約し、アクセス権限者を最小に分離することで、リスクを軽減できる。
2-2. 規程の整備		
規程の作成	規程は経営ポリシーを反映させた内容になっているか	情報セキュリティ対策は、営業(事業)活動とどちらを優先するか二者択一を迫られる局面もあるため、情報セキュリティ規程は経営の目指すところを反映した内容になっていないと、判断がぶれる場合も出てくる。 情報セキュリティ規程は、外部コンサルタントが提示した内容そのままで、他社でも通用するような内容になっていれば、自社の経営ポリシーと表裏一体とは言えず、空疎なルールになる。 これだけは外したくないというコンセプトを含めるべきである。
	規則やルールは経営環境の変化に適合できるよう適時改訂できるか	規則やルールは、自社の経営環境の変化に合わせ、手直しも必要である。 基本ポリシーをなす情報セキュリティ規程を安易に改訂すると、方向性が変化することにもなることや、最高意思決定機関(取締役会など)の承認を得るために時間も要するので、普遍的な内容に留めるのが望ましい。
	規則の根底となる考え方を明示できているか	規則は、「べからず集」になる傾向があり、すべての規則を全従業員が覚えるのも難しいため、その考え方の基本を提示し、理解を容易にすべきである。 覚えるべき規則は少ないことが望ましいため、すべての項目を規則に盛り込むのではなく、運用手引やマニュアルなど必要時だけ参照するドキュメントを準備し、分割することが望ましい。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
3. 人的対策		
3-1. 契約		
従業員との契約	入社時の雇用契約に情報セキュリティ条項を含めているか	入社時の雇用契約の中に、守秘義務などの情報セキュリティ条項も入れる。 在職時だけでなく、退職後も一定期間、守秘義務が発生する条項を入れ、退職時は、別途、誓約書を提出させる。 守秘義務をより強く意識させるため、雇用契約とは別紙とし、単独でサインを求めるような対策も一つの方法である。 入社時の契約内容は、すぐに忘れる傾向にあるので、契約があるからと安心せず、教育などの手段と併用し、繰り返し擦り込むことも重要である。 大学や前職での守秘義務契約があるか確認し、契約が存在する場合、本人および上司に、その契約を順守させなければならない。
	管理職昇格時に責任者としての誓約書を提出させているか	新たに組織責任者となった人に対し、当該組織における情報セキュリティ管理者であることを認識するための誓約書を求め、管理者の役割を理解させることが良い。 本人だけでなく、部下の事故にも責任があることを明記する方が良い。
	退職時に機密保持に関する確認書を取得しているか	退職時に、退職後の情報開示を制限するとともに、社内から情報を持ち出していないことを証明する確認書に同意させるべきである。 記憶している情報についても、開示制限があることを徹底しておくべきである。 再就職する場合、再就職先で、当社との守秘義務契約が存在することを、再就職先に伝えるよう確認しておく。
派遣元との契約	派遣契約に守秘義務事項を含めているか	派遣契約の中に、派遣社員が順守すべき内容、派遣元として管理すべき内容を含める。 派遣開始前に、情報セキュリティ教育を実施することを要求する。 派遣元での教育とは別に、受け入れ時点で、自社でも教育する。 派遣終了後も、守秘義務契約が有効であることを確認する。
業務委託（外部委託）先との契約	外部委託契約には情報セキュリティに関わる契約内容が含まれているか	業務委託(外部委託)先との契約に、機密保持事項、守秘義務事項などを含める。 業務委託先との守秘義務契約の前提として、業務委託先企業とその従業員間での守秘義務契約が締結されていることを確認する。 必要に応じ、業務委託先の状況について、監査や確認をできる条項を含める。 契約で縛るだけでなく、業務委託の人が見てはならない情報を見れないような社内のシステムにする。 再委託を認めるか、認めないか、明確にし、認める場合には、その条件を明快にする。
	外部委託契約内容の徹底を確認しているか	外部委託契約の内容について、業務委託先の全従事者に徹底されているか、責任者に確認する。
3-2. 教育･訓練･指導		
従業者へ規則の周知･徹底	最新の規則類を常時閲覧できるようにしているか	いつでも閲覧できるようにするため、イントラネットのわかりやすい場所に掲示する。また、必要な部分のみ照会できるよう、検索機能を備えていることが望ましい。 規則類が改訂されると、タイミングよく改訂内容を反映できる。 規則以外に、実際の業務や行動に必要となる事項の解説が、運用マニュアルやFAQとして整備する。 規則を運用する中で、今までの判断根拠など、従業者にわかりやすく開示しておく。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
従業者へ規則の周知･徹底	タイムリーでインパクトある話題を引用し再徹底できているか	一番インパクトがあるのは、社内で発生した事故であり、最近発生したセキュリティ事故などを取りあげ、再発させないために規則の内容を徹底する。 規則の中で、徹底する必要性が高い内容について、毎月、順番に取りあげ、キャンペーンのように周知するのも一つの方法である。
	周知するために考えられる手段を用いているか	徹底するためには、一つの手段だけでは十分でないため、複数の手段を併用する。 1) イントラネットでの掲示 2) 電子メールによる周知 3) 携行用カードの作成、配布 4) 啓発用ポスターの社内掲示 5) e-learning による教育
	新たに就業する人にも徹底できているか	ルールなど作成した時は、全従業者に徹底するが、中途採用などで入社した人には周知漏れもあるので、規則を徹底できる機会を設ける。 業務委託者や派遣従業者を受け入れた時、個別に社内規則の必要な部分を徹底できる機会を設ける。
従業者に対する教育･訓練	セキュリティ教育の体系や計画があるか	情報セキュリティ教育の重点を定め、重要度の高い対象者、コンテンツ、タイミングなどを考慮した教育体系を整備しなければならない。 毎回同じ内容ではなく、その時点で重要で徹底したい内容を中心に計画を策定する。 教育体系にもとづき、教育すべき重点項目を含んだ教育計画を策定しなければならない。
	教育ニーズと連動したセキュリティ教育を実施しているか	それぞれのタイミングに合わせた内容で教育するのが効果的である。 1) 全社員対象の定期教育(毎年、毎四半期など) 2) 入社時教育(新卒、中途採用など) 3) 職場異動時教育(担当業務変更によるセキュリティ教育が必要な場合) 4) 管理職昇格時教育 5) 経営幹部向け教育
	セキュリティ担当者にも教育や訓練を実施しているか	各部門のセキュリティ担当者を対象とした教育／訓練を実施する。 セキュリティに関する的確な判断力を養い行動に移せるためのOJT教育を実施する。セキュリティに精通した経験者が直接指導できる場の提供が望ましく、セキュリティ委員会活動を通じて教えるなどの方法もある。
3-3. 従業者の監督･監視		
行動監視	従業者の行動を監視(モニタリング)できているか	入退館ゲートの通過、入退室ドアの解錠、セキュリティエリアへの入退室などにより行動を記録する。 オフィス内、高セキュリティ室、サーバ室、通路、階段など、必要に応じて、監視カメラでモニタリングし、録画内容を確認する。 ファイル、データへのアクセスを記録する。 パソコンの操作履歴を監視する。 メールなどによる外部への情報持ち出しログを記録する。 社外サイトへのアクセスにより、外部への情報持ち出しを記録する。
業務管理	必要な報告が適切に実施されるよう徹底しているか	情報セキュリティの事故やインシデントが、タイミング良く、必要な階層にまで報告されるよう徹底する。 リスクが予見される場合、事前に報告されるようにする。また、そのために、定期的にリスクを棚卸するよう徹底する。 役員会、経営責任者会議など、各階層で、情報セキュリティを議論できる風土に改革する。また、阻害する要因を除去する努力が重要である。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
業務管理	賞罰は厳密に運用できているか	情報セキュリティに関する違反や怠慢に関して、賞罰など、基準にあてはめ、厳密に運用できないと、真の徹底に限界がある。また、そのための判断基準は、明確にしておく必要がある。 賞罰の結果について、社内に開示し、全員に知らせることで、セキュリティ事故の再発防止に役立てることもできる。社内開示であっても、その内容を社外にリークされることも想定した開示内容にする配慮も必要である。
4. 技術的対策		
4-1. アクセス管理		
識別と認証	アクセス権限は、特定の人に集中することなく、利用目的ごとに分離、分割できているか	アクセス権限は、システム管理者用、データベース管理者用、システム運用者用、システム利用者用など、利用目的ごとに分離、分割しなければ、厳密な内部統制ができない。 システム管理者やシステム利用者で業務内容の異なることを把握した上で、IDが発行されていないと、多くの権限が、特定の人に集中し、不正行為につながるとともに、不正行為の発見も難しくなることを理解しておかなければならない。
	正当なアクセス権限を保有している者の識別と認証ができているか	1) アクセス権限者の識別 正当なアクセス権限を保有している者であることを識別できるようにする。機密性レベルに応じ、生体認証などの補完的認証方法を採用する。 2) パスワードの強度 ID、パスワードでの認証が基本であり、パスワードは、他人が知ることができないとともに、容易に類推できないような対策をする。パスワードの強度を確保するため、ITリテラシーが低い利用者でも記憶できるレベルの複雑さで、類推しづらい範囲に設定すべきである。定期的なパスワード変更は必須として、難しい文字列を要求し過ぎると、パスワードをメモする結果にもつながるので、注意が必要である。 3) パスワード変更 パスワード変更は、システムで、期限を指定し、期日までに変更しないと、アクセスできないようにする。強制的な変更が望ましい。 4) シングル･サインオン 社内外に多くのシステムが存在し、システムごとに、ID、パスワードが設定されていると、パスワードの記憶が困難になるので、全体で、シングル･サインオン･システムの採用を検討するなど対策する。パスワードは、システムが自動発行するのではなく、利用者が記憶しやすい文字列を指定できる方式が望ましい。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
アクセス権限（アカウント）の管理	アクセス権限の付与／削除の仕組みができているか	1) アクセス権限付与の限定 アクセス権限の付与／削除など、必要最小限のアクセス対象者、アクセス範囲、アクセス可能期間に限定しなければならない。許可された期間を過ぎると、自動的に権限が削除されることが望ましい。業務が予定どおりに完了せず、引き続き、権限が必要な場合は、継続利用申請が組み込まれていれば、解決できる。 2) アクセス権限の棚卸 付与された権限が適切かどうか、定期的に棚卸ができ、確認できる仕組を備えるべきである。その場合は、情報資産管理責任者か組織責任者が、すべての権限について、棚卸して、不必要な権限を削除できるようにすべきである。 3) 不必要な権限の削除 機密性レベルが高い情報などのアクセス権限を付与したまま放置しない。付与する期間を、3ヵ月などの一定期間とし、それを超えると、再申請が必要にするなどの方法をとれば、さらに厳密な権限管理が可能となる。特に、退職者、担当業務変更者など、権限を喪失した直後に削除できる仕組が必要である。 4) 業務委託先の権限管理 業務委託先からの個人情報漏えいなどが課題になっており、業務委託先に付与した権限についても、十分な管理を行う必要がある。社員にばかり目がいき、業務委託は忘れがちである。 5) アクセス制限 イントラネットの掲示板など、業務委託や派遣の人が不必要な情報へはアクセスできないようコントロールしなければならない。面倒だからという理由で放置され、アクセスできるケースもあるので、確認する。
	アカウントの付与管理ができているか	1) アカウント付与規則と権限分離 アカウント付与に関する規則が定め、申請者、承認者、登録者など権限が分離される内容にする。また、的確に運用され、牽制機能を働かせることが重要である。権限を分離しておかないと、一人の意志だけで、不正なアカウントの設定を許すことになる。 2) 例外対応を視野に入れた承認ワークフロー 緊急時に、担当者が不在などの状況が発生した場合でも、代行者に対し付与対応が可能にるよう、例外対応も吸収できる承認ワークフローでないと、不正な権限付与の温床となね。例えば、承認者が長期不在で、業務が停滞することを懸念し、複数の人に、承認権限を付与しているケースが見かけられるが、長期不在時は、代行承認者による承認ができるワークフローにすべきである。 3) 例外対応の補完的措置 承認者が復帰した時点で、代行承認者に付与した権限が削除されることとセットで仕組化しなければならない。例えば、甚大な天災が発生し、日常、本人がアクセス権限を保有しない情報資産に急遽アクセスする必要が生じた場合を想定し、例外的なケースとして諦めるのか、対応可能にする緊急時付与のフローを準備しておくのか、いずれかの判断をしておくことも必要である。
	アクセス権限管理が適切か	1) アクセス権限の全体管理 情報資産から見た個別のアクセス権限管理だけでなく、すべてのアクセス権限について総合的に管理する必要がある。利用者ごとに、付与されているすべての権限を把握できる仕組も必要である。システム個別から権限付与を見るだけでなく、個人からもすべての権限を見えるようにして、上司からの確認が容易にできる必要性がある。そのためには、人事データベースなどとの連携も必要であり、全体管理ができなければならない。 2) アクセス権限の強制削除機能 アクセス権限の強制削除機能を備えるべきである。不正発覚など、権限を強制削除する必要が生じた場合、その削除完了までの許容時間を明確にするとともに、その許容時間内に強制削除できる仕組にしておく。不正行為が発覚した時点で、すべての権限をはく奪すべきであるが、それに対応できる仕組を用意しておく。仕組がない場合、それぞれの情報資産管理者へ即刻連絡し、個別に権限削除する方法でも良いので、指示系統を整備しておく必要がある。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
アクセス制御	権限付与対象者は必要最小限になっているか	権限付与する対象者について、常時、必要最小限に絞り込める仕組が必要である。権限付与は、作業するために申請しても、不要になった時点でタイムリーに削除申請せず、放置しているケースが多い。 例外的なケースや利便性の観点から、もしかして必要になる場合があるかもしれないぐらいの判断で、不必要な人にまで権限付与されるケースもある。 権限の削除によって本人の位置づけが低下するなど誤解による精神的な抵抗感も理解できるが、的確な絞り込みを実施する割り切りも必要である。
	個人(アカウント)ごとのアクセス制御になっているか	アプリケーションアカウントのように、共有アカウントにせず、利用者個人を特定でき、アクセスログからも、個人を識別、特定できる仕組にしなければならない。
	クライアント(パソコン)の利用制限ができているか	必要に応じて、利用できるクライアント、日時など、制限することで、リスクを低減できる場合もある。 アクセスを認めるオフィス、ネットワーク、クライアント(パソコン)を制限することにより、想定外の不正アクセスを未然に防止することができる。 社内に踏み台サーバが設置されているケースなど、アクセス可能経路を十分に調査、確認しておく必要がある。
	データベースに直接アクセスできないようにしているか	システム利用者が、アプリケーションシステム経由ではなく、直接、データベースを参照、更新できないよう、アクセスを制御しなければならない。
	システム管理者のアクセスログを取得し、保存しているか	システム管理者のアクセスログは、システム利用者とは別のアクセスログを残し、ログを改ざん困難にするため、システム管理者本人がアクセスできないサーバ上に保存することが望ましい。 例えば、ログ専用サーバを設置し、各サーバからのログを回収する設定にし、ログ専任者が分析すれば、ログ改ざんの危険性は、かなり低くなる。
	アカウントの一元的管理ができているか	入社、退職、休職、業務委託開始／終了などの異動内容と同期化できるような管理体制にすべきである。 例えば、人事部門管理のデータベースとの自動連携が望ましい。
	アカウント管理と権限管理が連動しているか	不正行為の発覚、懲戒による突然の退職などでアカウントを削除する場合、当該アカウントに付与されているすべての権限について、それぞれの対象システムから、アカウントが削除される仕組になっていることが望ましい。
情報資産へのアクセス管理と監視	情報資産別にアクセス管理ができているか	実際に付与されているアクセス権限について、申請書や台帳の調査を通し、アクセス権限の集中や牽制上問題となる重複がないか確認すべきである。 1) 参照権限、更新権限など分離状況を確認する。 2) 情報資産別に、アクセス権限を付与するルールがある。 3) アクセス権限を許可する承認者が明確になっている。 4) 例えば、アプリケーションシステムごとに、アクセス管理しているケースを見かけるが、データベースに対し、複数のアプリケーションシステムからアクセスできることが一般的になっているので、データベースあるいはデータ項目ごとに、アクセス管理をするべきである。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
情報資産へのアクセス管理と監視	アクセス可能グループを管理できているか	従業者が多い企業(組織)では、個人ごとのアクセス権限管理だけでは、サーバ増設、担当業務変更など、迅速に権限変更することが難しくなるので、補完する機能として、権限グループを設定して管理するのが現実的である。 情報の機密性レベル、本人の職種(業務)、本人の職位、本人の所属組織などの分類、あるいはその組み合わせで、アクセスを許可するグループを管理できるような仕組を設けると、正確かつ迅速な対応が可能となる。 個別の設定でも良いが、変更に対する設定など、煩雑かつエラーも心配であり、アクセス管理をグループ単位に設定し、個人を、そのグループに紐づけするようにした方が、合理的である。
	組織変更への対応ができているか	組織間の職場異動、職位の変更、担当業務の変更などが生じた場合、その変更内容に連動して、アクセス権限をタイミング良く変更できるようにすべきである。 組織間での業務移管が発生した場合など、組織単位に許可された情報資産に、アクセス権限の追加や削除が発生するが、対応できなければならない。また、情報資産の再編も同様である。 例えば、業務を、小さなユニットへ分割し、それぞれの組織は、いくつかのユニットを担当することとすれば、ユニット単位で業務が移管されたと考えれば、簡単な仕組になる。
	情報資産の組み合わせによる機密性レベル変化に対応できるようになっているか	複数の情報資産に同時アクセスできる場合、その組み合わせにより、機密性レベルが高くなるケースがあるが、そのような観点からの検討や対応も必要である。 例えば、顧客コードに紐づく氏名、住所、電話番号、生年月日のデータベースと、顧客コードに対するクレジットカード番号のデータベースが、別々にアクセスする場合と、同時にアクセスできる場合では、機密性レベルが異なると定義するのが、一般的である。
	機密性レベルが高い情報資産は、特別のアクセス管理をしているか	機密性レベルが高い情報資産の場合、アクセスできる居室やネットワークなど制約が必要かどうか判断しておかなければならない。また、そのコントロールを実現させる。 例えば、お客様個人情報にアクセスする必要がある業務は、すべて一つの部門に集中させ、部門を分散させない方が、安全である。
	複数件同時アクセスに関する制限ができているか	機密性レベルが高い情報資産について、同時にアクセスできる件数に制限を設けることでリスクを低減できるが、その判断ができていて、その制限に基づき、アクセスを制限できることが重要である。 例えば、機密性レベルが高い個人情報などでは、1件別のアクセスのみ許可し、複数件を同時にアクセスできないようにし、情報流出が発生した場合でも、その被害を最小限度にとどめられる方法がある。
	アクセス経路の管理ができているか	踏み台サーバ経由などのルートによる不正アクセスが発生しないよう、すべての経路を管理し、ネットワークのポート制御など不必要な経路は閉じなければならない。
	データベースのアクセスログを監視できているか	すべてのデータベースに対するアクセスの記録がとられ、アクセス権限がない情報資産にアクセスを試みようとするログが取得され、正当なカクセスか確認できる仕組が必要である。
	パソコン操作のモニタリングができているか	パソコン上での挙動について、ログ収集など、モニタリングができていると、情報セキュリティ管理レベルが向上する。 モニタリング結果を解析し、不正な行為を発見した場合、適切な措置ができる運用面での対応も重要である。 このようなシステムの導入により、パソコンのリソースを大きく占有される場合もあるので、十分な事前検討も必要である。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
4-2. パソコン管理		
クライアント管理	情報流出対策ができているか	情報流出を防止するため、USBポートの利用制限、CD-ROM／DVDドライブの利用制限、無線LANの利用制限など、対策を定め、実行することが、有効な手段となる。 特に、ノートパソコンで、無線LANを利用している場合、社内での無線LANではなく、ホットスポットなどを経由して、大量に情報を持ち出されるリスクが存在する。
	パソコンの現物管理ができているか	パソコンが常時管理され、所在不明などの場合、常に把握できる状態にしておかなければならない。 貸出管理も適切に運用する必要がある。
	ライセンス管理ができているか	ソフトウェアのライセンスについて、クライアントごとに管理され、違法コピーがないことを保証できなければならない。 ソフトウェアによっては、クライアント単位での契約ではなく、利用アカウント数や同時アクセス数などの単位で契約するものもあり、社内に混在しても、適切に管理できるようにしなければならない。
	フリーソフトのインストールは許可制にしているか	フリーソフトをインストールする場合、そのソフトの挙動が、クライアントやシステム、ネットワーク全体に悪影響を及ぼす場合があるが、インストールを許可するホワイトリストや、仕組(社内ミラーサイトなど)を備えることが望ましい。
不正ソフトウェア対策	ウイルス対策ソフトを導入し、最新バージョンに更新しているか	ウイルス対策ソフトウェアを導入し、最新バージョンに自動的にアップデートできる仕組にしなければならない。 ゲートウェイとクライアント(パソコン)との両方で二重に対策されることが望ましい。 可能であれば、ゲートウェイとクライアントでは、異なるベンダーの製品を導入すれば、新種ウイルス対策に対応する時間差が生じた場合でも、早く対応できたソフトウェアが機能し、有効な場合がある。 LAN接続で対策ソフトをアップデートする設定の場合、モバイル用パソコンなど、不定期にLAN接続するパソコンの対策も組み入れなければならない。 自宅からのリモートアクセスを認めている場合、自宅のパソコンも、ウイルス対策ソフトが、最新状態にしてあることを求めなければならない。
	セキュリティ対策パッチの適用を全員が確実にできているか	OSやブラウザソフトなど、毎月のように頻繁にセキュリティパッチが提供されるソフトに関し、自動的にアップデートできる設定にしておくべきである。 セキュリティパッチが公開された場合など、全従業員に周知し、注意喚起することも重要である。
	組織として認めていないソフトウェア導入を検知できるようになっているか	組織(企業)として、インストールを認めていない「ファイル共有ソフト」などがインストールされた場合、自動的に検知し、削除できるような対策をとることが望ましい。
5. 物理的対策		
5-1. 入退室／入退館管理		
オフィス・レイアウト	部外者を通す応接室、会議室の配置に問題はないか	来客などの部外者を通す応接室、会議室は、執務スペースを通らずに入れるように設置することが望ましい。通らざるを得ない場合は、社員が随行するよう規定しておく。 以前は、「内部に通されることを親密性の現れ」と歓迎する人が大半であったが、情報セキュリティ意識の高まりとともに、「内部に部外者を通すような企業は信用できない」と見る人が増えたことも意識し、そのような運用は避けた方が良い。 来客スペースと執務スペースとが完全に分離され、来客が執務スペースに入る必要性がないレイアウトが望ましい。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
オフィス・レイアウト	部外者が機密情報に接触しやすい動線になっていないか	外部の人が通行する際に、盗み見や抜き取りの危険があるため、プリンタ、FAX、資料棚、オープンな作業スペースを、通路際に配置しないようにすべきである。
入退館管理	外部と自社の敷地の境界は、部外者が容易に出入できないようにしているか	容易に乗り越えられない壁の高さ、鉄条網、監視カメラ、警備員の配置など、リスクの大きさにより適切な対策を行う。 テナントビルに入居している場合は、ビル共有スペースと自社スペースの境界線で、部外者などの不正な侵入を防ぐことが重要である。
	窓から侵入される危険はないか	重要な情報を扱う業務は、窓からの侵入リスクもあるので、窓のない部屋で利用・保管するようにすることが望ましい。 1階などアクセスしやすい場所にある窓には、侵入者を感知するセキュリティ装置の設置、防犯カメラでの監視など、対策を行なうことが望ましい。 機密性レベルが高い情報を扱うオフィスでは、内通している人を窓の下に待機させておき、窓から書類や外部記憶媒体などを落下させ、外部に持ち出せる方法がリスクとして存在するので、窓を開けなくする対策も必要である。
	共連れ防止ができているか	ICカードだけの認証でドアから入れる場合は、1枚のICカードで複数人が同時に入室できる共連れ現象になるので、一人ずつしか通過できないフラッパーゲートなどで防止することが望ましい。
	非常口の管理ができているか	重要な情報を扱う部門は、社外との接点になり得る非常口での不正な情報授受をできない対策が必要である。非常口では、部外者と書類の授受ができるなど、情報持ち出しリスクの多い場所であり、機密性レベルの高い情報を扱うオフィスは、専用ビルで、非常口のコントロールもしやすいことが望ましい。外階段とつながる非常出入口や、防火扉など開放されていたり、開錠されていると、不正侵入のリスクが高くなる。
入退室管理	執務室への入室／退室制限ができるようになっているか	リスクに応じて、次の措置を選択し、実施すべきである。 1)「関係者以外立ち入り禁止」「STAFF ONLY」などの表示 2) 常時施錠 3) ICカード、生体認証などにより入退管理 4) 見慣れない人を見かけた時は、社員が積極的に声をかけることを励行するだけでも効果があるので、従業員教育に含めておく。 5) 来訪者が立ち入る許可エリアごとに、名札やストラップの色分けなど、瞬間に判断できる区分をしておく。 6) 喫煙コーナなど、共用スペースについては、来訪者用と従業員用を分離することにより、情報が漏れることを防ぐ。 「立入禁止」の表示をしておくだけでも、間違って入室することはなくなる、抑止効果があるなどのメリットがある。 ただし、「サーバ室」「機密情報」などの具体的な表示は、逆に部屋の中を推測できる情報の表示を避ける。
	ドアなどの鍵管理ができているか	すべての鍵について、管理者及び保管場所を明確しておかなければならない。 緊急用の保管鍵、キーボックスの鍵は、誰でもすぐわかる場所を避けて置いているか。
	重要な場所への入退管理をしているか	リスクの大きさにより、ICカードだけでなく、生体認証などの他の方法と併用するなど対応すべきである。生体認証には指紋、静脈、瞳の虹彩、顔認証等がある。
	社員の入退室の記録を取っているか	すべての入室、退室を記録する。社員は、最初の入室者実績と最後の退室者実績を記録するのが一般的である。サーバ室などは出入りの都度記録する。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
入退室管理	来訪者の入退室の記録を取っているか	来訪者の社名、氏名、用件、面会者、日時等を記録する。ただし、受付付近での集配者の場合は不要とする。 来訪者は、事前に来訪予定を登録し、その登録された内容と確認し、入室を許可する。 事前登録がない場合は、担当の社員に確認した後、入室を許可する。
	入退室記録は定期的にチェックしているか	記録漏れ、記入間違いがないか、管理者が週や月単位で確認し、確認記録をとる。 入室を許可した全員が退室し、オフィス内に滞留していないことを確認する。
5-2. 持ち出し／持ち込み管理		
持ち出し／持ち込み管理	ネットワーク経由の不正持ち出しを防止できているか	メールへのファイル添付、社外サイトへのファイルや情報のアップロード、社外へのファイル転送、社外サイトへの書き込みなどの手段による不正持ち出し対策をとる。 フィルタリングを利用したアクセス制限や、アクセスログの解析による追跡などの有効な手段がある。
	電子媒体による持ち出し管理ができているか	USBメモリ、CD-ROMなどの電子媒体による不正な情報持ち出しを禁止しなければならない。 電子媒体の持ち出しを止める方法としては、ボディチェックなど現実的ではないので、むしろ、電子媒体への書き出しを制限する方が容易である。 USBメモリの取扱いには特に注意する。PCのUSBポートを無効化したり、外部媒体への保存をできなくする方法もある。
	紙媒体による持ち出し管理ができているか	プリント、コピーなど、必要以上に印刷した事実を把握し、持ち出しを追及できるようにすべきである。 重要情報を保管しているエリアからの書類持ち出しをチェックできることが望ましい。 原本が、電子化されている場合は、印刷関連を重点的に管理すればよい。
	パソコンの持ち込み管理ができているか	個人用ノートパソコンを持ち込み、ファイルコピーなどを防止する対策が必要であり、社内LANに接続できるパソコンを制限すべきである。例えば、管理外パソコンからの情報漏洩、ウイルス感染を防止するため、登録済みMACアドレスのパソコンのみ接続を許可する。
	パソコンの持ち出しを制限しているか	持ち出し専用パソコンを用意して、社内LANへの接続を許可制にするなどの運用をすればリスク軽減が可能である。 1) 事前申請により業務上の必要性とセキュリティを勘案の上、パソコン持ち出しを許可する。 2) 許可なく、ノートパソコンのローカルドライブに、ファイルをコピーすることを制限する。 3) ハードディスクの暗号化、BIOSレベルのパスワード設定など、必要な対策を行う。
	電子機器の持ち込み制限ができているか	電子機器（カメラ付携帯電話、携帯オーディオプレーヤー、デジカメ、ICレコーダなど）、及び媒体（USBメモリなど）の持ち込みを必要性に応じて制限する。 パソコンにつないでデータをコピーできたり、撮影や録音によりデータを持ち出すことができるため、機密情報を取り扱う部屋やサーバ室などには持ち込ませないなどの対策を検討する必要がある。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
5-3. 物理的管理、盗難対策		
セキュリティ区画	重要な情報の取扱場所を限定しているか	取扱場所を限定するとともに、次の対策をとる。 1) 重要情報を取り扱う場所には許可された者のみが入れるよう管理する。 2) 厳重な入退室管理を実施する。 3) 私物などの持ち込み／持ち出しを禁止する。 4) 機密性レベルやアクセス権限者が混在することによる情報漏えいを防止するため、内部で部屋を分割するなど対策する。
クリアデスク	電子媒体、紙紙媒体などが放置されていないか	取り外し可能な外部記憶媒体、紙の情報（機密情報、個人情報など）を机上、棚上に放置させない。（クリアデスク） パソコンのデータをコピーして持ち去ることが容易にできるため、電子媒体は、空であっても放置させない。
クリアスクリーン	覗き見防止／なりすまし対策ができているか	離席時に画面ロック、パスワード付スクリーンセーバの起動、ログオフなどにより覗き見防止／なりすまし対策をとらせる。 スクリーンセーバは副次的に利用するべきで、自主的に画面ロックを掛けてから離席することが望ましい。スクリーンセーバの起動時間は5分以内が望ましい。
施錠管理	パソコンの盗難防止対策ができているか	ワイヤーロックの設置、施錠ロッカーへの収納等を励行する。 ディスクの暗号化による漏洩防止も有効である。
	取り外し可能な記録媒体（CD-R、MOなど）の盗難防止対策ができているか	施錠管理および管理者による使用管理を確実に行う。 USBメモリの場合は、自動暗号化や指紋認証付が有効である。
機密情報の保管場所	機密性レベルに見合った保管場所となっているか	個人情報、営業秘密など重要度に応じて保管場所を分けているか。 「極秘」「社外秘」「開示可」といったラベル付けをし、機密度に応じたセキュリティを考慮した保管場所を明確化することが望ましい。 保管場所は施錠装置を付ける。
5-4. 機器類の物理的保護		
水害対策	漏水への対策ができているか	サーバ室の上に水の配管がないようにすることが望ましい。サーバ類の冠水だけでなく、床下ケーブルの浸水も大きな障害となるため、対策しておく。 火災時、スプリンクラーが作動した際に、電子機器に影響を与えないためにサーバは容易に水をかぶらないように配置する。スプリンクラーは、異物の衝突などの衝撃だけでも作動する可能性があるので、その場合の放水に注意する。
	洪水対策ができているか	サーバ等電子機器が、洪水などにより水につからないよう、設置する場所を配慮する。 地下に設置している場合、窓がある場合は要注意である。
電源対策	サーバ用無停電電源装置（UPS）を設置しているか	瞬断（瞬間的な停電）でも再起動して接続できなくなったり、データが破壊されるおそれがあるため、UPSを備える。
	電源ケーブルの配線は適切か	タコ足配線、延長ケーブル利用など事故が発生しやすい配線にならないよう徹底する。 ホコリの堆積による漏電リスクもあるため、設置状態なども確認する。
通信対策	配線構造が適切か	配線を誤って切断したり、プラグを引き抜いたりしやすい構造にならないよう設置する。 床上、足下へのケーブル露出、サーバ裏の配線スペースの取り回しを確認する。
	通信回線のバックアップ回線が備えられているか	専用線、光回線、ADSL、ISDNなどを必要に応じて組み合わせて、リスク分散をした代替ルートを確保する。

項　目	確　認　内　容	ア　ド　バ　イ　ス　内　容
地震対策	地震発生時に備えた転倒対策ができているか	リスクに応じて次の対策を実施する。 1) サーバは震度5程度以上の地震でも転倒しない対策を施す。 2) サーバラックに固定し、コンクリートにボルト固定。 3) L字クランプや転倒防止金具、ベルトで補強する。 4) タワー型PCサーバを机上に立てておかない。