セキュリティ監査・チェックリスト

個人情報編（一部のチェックポイントは重複します）

項　　目	チェックポイント	関係条文・資料
基本方針	① セキュリティポリシーや社内規程で個人情報保護についての基本方針を明記しているか ② 個人情報保護のための組織（委員会など）を設置しているか ③ 個人情報保護に関する全社的な責任者を決めているか（経営トップまたはそれに替わる人）	セキュリティポリシー 社内規程
信頼性	① 個人情報ついて、それぞれのデータについての管理責任者を決めているか ② 個人情報保護に関する教育を定期的に実施しているか ③ 個人情報の管理について、運用管理規程が整備されているか（暗号化、バックアップ手続き、アクセスコントロール、委託管理ルールなど） ④ 個人情報が保存されているパソコンの持ち出しや、盗難についてのルールが決められ、実施されているか ⑤ 個人情報保護のために必要とされるツールが導入されているか ⑥ 個人所有のパソコンを会社に持ち込んで会社の業務に利用していないか（スタンドアロン（単独使用）もあるが、社内 LAN 接続の例もある） ⑦ 個人情報を収拾するに際して、利用目的を明確に特定しているか ⑧ 個人情報を収拾するに際して、利用目的を本人に通知すると共に、同意を得ているか ⑨ 本人からの個人情報の開示や利用停止の要求があった場合、本人確認手続きを含めて、迅速に対応できる手続きが整備されているか ⑩ トラブル発生時に迅速に対応できるよう、対策が検討されているか（初期処置、調査体制、マスコミ対応、再発防止策など） ⑪ 監査担当が、社内の個人情報の取り扱いルールの実施状況や運用状況を定期的にチェックしているか	社内規程 職務分掌規程 業務フロー 保管基準

項　　目	チェックポイント	関係条文・資料
	⑫ 社外へのソフトウエア開発の委託のための「ソフトウエア開発依託契約書」を作成しており、そこには個人情報保護についての記載があり、その内容は妥当であるか(委託先に立ち入って監査ができるなど) ⑬ 社外へのソフトウエア開発については「ソフトウエア開発依託契約書」を締結し、決裁を受けるなど正式な手続きを経ているか	
安全性	① 個人情報が保存されているコンピュータについて、ルールに基づいた情報漏えい防止のための適切な対策が実施されているか（暗号化、IC カード、ログイン ID など） ② 個人情報を保管しているサーバーへのアクセス制御が適切に実施されているか ③ 容易に推測できるパスワードを使用していないか。パスワードを画面の横に貼り付けるなどをしていないか ④ 個人情報を取り扱うパソコンや個人を特定し、アクセス制御や暗号化を実施しているか ⑤ 個人情報の入力中や参照中に離席した場合、画面を初期画面に戻すことを励行しているか ⑥ 個人情報について、どのような情報がどのコンピュータに保存されているかを常時把握しているか（コピーを含む） ⑦ 社外からのアクセスに対して、情報漏洩対策が実施されているか（ファイアーウォールなど） ⑧ ネットワーク上を流れる個人情報データの盗聴を防ぐため、暗号化など適切なセキュリティ対策を実施しているか ⑨ 個人情報についての変更や参照についてのアクセスログが確保され、迅速に確認できるよう整備されているか ⑩ 個人情報を保管しているパソコンの廃棄についての規程が整備され、適切に運用されているか ⑪ 委託先との個人情報の受け渡しについて、着実に記録を取っているか	職務分掌規程 業務フロー 保管基準

コンプライアンス編（ソフトウエア・ライセンス管理）

項　　目	チェックポイント	関係条文・資料
台帳管理と証書保管	① ライセンス管理台帳を作成しているか、あるいはQNDなどのパソコン管理ツールを導入しているか ② ライセンス管理台帳と実際のパソコンにインストールされている内容とが一致していることを定期的に確認しているか ③ 自部署で購入したソフトウエア(標準ソフトウエア以外）についてもライセンス管理台帳に記載されているか ④ ライセンス管理台帳は作成しているが記載項目が不充分でライセンス確認ができない状態でないか ⑤ ライセンス証書が保存されているか ⑥ ライセンス証書が個人管理になっていないか ⑦ ライセンス証書と機器との関連が明確か(部門全体としての管理ができているか) ⑧ ライセンス証書のシリアルNoと実際にインストールされているシリアル No.が一致しているか（サンプリング検査で確認する）	職務分掌規程 業務フロー 保管基準
ライセンス不足・違法コピー	① 許諾されたライセンス数以上のソフトウエアをインストールしていないか ② バージョンアップ費用を支払わずに新しいバージョンを使用していないか ③ 経費削減対策として上司が社員に違法コピーを指示していないか ④ 「駅すぱあと全国版」（所要時間計算ソフト）、「ゼンリン地図」（地図表示ソフト）など、個人所有のソフトウエアを会社のパソコンにインストールしていないか(現在ではインターネットを利用して無料で同様のサービスが受けられる)	職務分掌規程 業務フロー 保管基準
ボリュームディスカウントで購入したソフトウエアの取り扱い	① パソコンソフトをソフトウエアと一緒にリースしていないか マイクロソフト社のライセンス契約では、EA 契約、セレクト契約、オープンライセンス契約など、ソフトウエアを大量に購入することでコストダウンを図ることが可能であるが、これらの契約条項では、第３者への再リース及び再レンタルが禁	職務分掌規程 業務フロー 保管基準

項　　目	チェックポイント	関係条文・資料
ボリュームディスカウントで購入したソフトウエアの取り扱い	止されている。従ってこれらのパソコンをソフトと一緒にリースすることは契約違反となる。ソフトウエアをリース契約に含めずに別途購入していれば、ソフトウエアのリースが完了しても、新しいソフトウエア上でソフトウエアは継続して使用することが可能であるし、バージョンアップすることも可能である。（つまりそのままのバージョンであれば新たにソフトウエアを購入することは不要である） ② 安いコストでソフトウエアを購入できるにもかかわらず、通常の（高い）価格で購入していないか（セレクト契約やＥＡ契約を知らない、または知っていても自部署で独自に購入しているなど）	

バックアップ編

項　　目	チェックポイント	関係条文・資料
サーバーバックアップ	① システムバックアップを必要な都度、確保しているか ② データバックアップを定期的に確保しているか ③ バックアップは取っているがバックアップ媒体に日付を記入しているか、また、どのバックアップ媒体が最新のものであるかが明らかか ④ バックアップ媒体は担当者が個人的に机の引出しなどに入れており、責任者が確認をしていない、などの状況はないか ⑤ バックアップは取っているがチェックリストへの記載などのルールがないため、適切なタイミングで取っているか、確認できない状況でないか ⑥ 自動的にバックアップを取るようにセットしている場合、ログをチェックするなど、バックアップが正しく取られたことを確認しているか ⑦ システム変更で生じるトラブルを元に戻すために、システム変更前のシステムについてはバックアップを取っていても、変更後のバックアップを確保しているか ⑧ バックアップを確保するルールはあるが台帳への記載がなく、責任者の確認が行われていない、などの状況はないか	職務分掌規程 業務フロー 保管基準

項　　目	チェックポイント	関係条文・資料
	⑨ 社外の要員まかせになっており、当社責任者がそれぞれのデータについてのバックアップのタイミングや方法の妥当性について確認していないし、台帳などを定期的に確認していないなどの状況はないか ⑩ ＣＡＤデータについてもバックアップを確保しているか（ＣＡＤの担当者任せとなっていることが多い） ⑪ バックアップはテープに取っているがメディアは数年間マシンに入れたままで、書きこみエラーなどの確認やバックアップが実際に有効に機能するか確認をしていないなどの状況はないか ⑫ システムバックアップについてはシステムの変更毎に取ることになっていても、実施したかどうかを責任者が確認しているか	
バックアップの火災対策	① バックアップは本体横のミラーディスクだけではないか ② バックアップ媒体をサーバーの近くに置いてないか（盗難防止も必要） ③ バックアップは取っているが、磁気媒体用保管庫に保管せずに、金庫（紙幣用）に保管していないか。（金庫で保管しても、火災発生時は庫内が高温となり磁気媒体は読めなくなる） ④ ＣＡＤサーバーのバックアップを担当者の机の引出しの中などで保管していないか ⑤ 磁気媒体用保管庫はあるがバックアップを適切なタイミングで保存しているか（サーバーの中に入れたままで取り出していない） ⑥ バックアップを保存している磁気媒体用保管の扉が開いたまま放置されていないか	職務分掌規程 業務フロー 保管基準

ウイルス対策編

項　　目	チェックポイント	関係条文・資料
ワクチンソフト	① パソコンにワクチンを導入しているか ② 古いバージョンのワクチンをインストールしていないか。（ほとんど役に立っていないことを理解していない。パターンファイルの更新も行っていない、など。バージョンが古い場合、パターンファイルが提供されていないということも知らないこともある） ③ ゲートウエイサーバーでのウイルス対策を実施しているか	職務分掌規程 業務フロー 保管基準
ファイル共有	① 個人用パソコンでファイル共有を許可していないか ② サーバーで、Cドライブをファイル共有していないか ③ ファイル共有しているサーバーのアクセス制御は適切に設定されているか	職務分掌規程 業務フロー 保管基準

その他編

項　　目	チェックポイント	関係条文・資料
信頼性	① 古い機器を使用していないか メーカー保守の終了期限を過ぎた通信機器や専用端末は老朽化してトラブルが発生しても保守用パーツがない。トラブルを未然防止する観点から計画的な機器の更新が必要である ② パッケージソフトウエアの購入について、決裁を受けるなど正式な手続きを経ているか ③ コンピュータルームの空調が不充分な場合、サーバーがダウンするおそれがないか ④ 情報システム要員の担当が分かれており交代（バックアップ）ができない状況でないか ⑤ 独自のシステムを構築している場合、仕様書が整備されているか ⑥ ホストコンピュータを撤去した場合、不要な磁気テープがEDPルーム内に放置されていないか ⑦ 設備トラブルに際しては外注業者に任せきりになっており、頻繁にトラブルが発生していても再発防止対策などが十分に検討されていないよう	職務分掌規程 業務フロー 保管基準

項　　目	チェックポイント	関係条文・資料
	な状況はないか ⑧ ネットワーク接続に関する契約書（又は覚書）を締結して、ネットワーク接続してデータ交換などを行っているか ⑨ 基幹システムの新システムへの移行については「システム移行計画書」を作成して工数を把握し、事前にトラブル時の対策を立てた上で実施しているか ⑩ 業務マニュアルは情報システム担当者任せにすることなく、各部門の業務担当者が主体となって作成しているか ⑪ 委託先にシステムの仕様や運用について、詳細な確認をしているか、丸投げにしていないか	
安全性	① 海岸隣接地域の場合、コンピュータ設置階などについては水害対策を実施しているか ② サーバーなどの重要機器は地震対策を考慮した場所に設置しているか	職務分掌規程 業務フロー 保管基準