セキュリティ監査・チェックリスト

2006 年 7 月　ＰＣネットワークの管理活用を考える会：情報モラル・セキュリティ分科会作成

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
信頼性	① 個人情報について、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、またその記録を残しているか 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仕組み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 個人情報を収集する際、利用目的と範囲を明確に特定しているか ⑧ 個人情報を収集する際、利用目的と範囲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、また、窓口は明確になっているか ⑩ 対応履歴の保管がなされているか ⑪ 保管されている履歴は，迅速に照会可能か ⑫ 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	管理規定 運用規程

項　　目	チェックポイント	関係条文・資料
信頼性	ミ対応、再発防止策など） ⑬ 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 ⑭ 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） ⑮ 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 ⑯ 個人情報の内容、レベルに応じた権限レベルの設定がされているか。 ⑰ 付与したユーザＩＤで、不要になったものの削除が速やかに行われているか。また、定期的な棚卸を行い適切なＩＤ付与が保てているかをチェックしているか。 ⑱ 個人情報へのアクセス記録を残すような手続きになっているか（アクセス開始・終了日時等）	管理規定 運用規程
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 離席した場合、他人にパソコンを操作されないようになっているか 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、または紙等で保管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）	社内規定 管理規則

項　　目	チェックポイント	関係条文・資料
安全性	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 パソコンや記憶媒体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 廃却記録が，保管されているか（物理的な廃却処理を行った場合，その証拠写真等を含む。） ⑫ 廃却記録は，迅速に照会可能か ⑬ 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 ⑭ 定期的なパスワードの変更が行われているか	管理規定 運用規程

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 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） ⑨お客様から預かった「個人情報ファイル」については、会社で一意に認識できるように、台帳管理しているか。また、その原本を、全社一括して保存しているか ⑩パートナー企業に貸し出す、自社またはお客様の「個人情報ファイル」について、会社でその出納状況を明確に管理しているか	管理規定 運用規程
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 不正に新しいバージョンを使用していないか ③ 会社または上司が社員に違法コピーを指示または強要していないか ④ 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	管理規定 運用規程
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	管理規定 運用規程

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	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、ハードウエアのリースが完了しても、新しいハード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ソフトウェア購入部門の一本化等，ソフトウェア購入ルールが規定され，適切に運用されているか	管理規定 運用規程

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、実施しているか ② データバックアップを定期的に実施しているか 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 バックアップを実施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 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実施しているか（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	管理規定 運用規程

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	かを責任者が確認しているか ⑬リカバリ手順が，明確に規定されているか ⑭リカバリ手順に従ってリカバリ作業の訓練を行っているか ⑮ リカバリ訓練の記録は保管されているか ⑯ 期的な、復旧の訓練を行っているか（復旧操作手順の検証、システムの正常な稼動の検証） ⑰リストアの手続きは明確になっているか	管理規定 運用規程
バックアップの災害対策	① バックアップは本体そば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に保管していないか 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	管理規定 運用規程

ウイルス対策編

項　　目	チェックポイント	関係条文・資料
ウイルス対策ソフト	① パソコンにウイルス対策ソフトを導入しているか ② 古いバージョンのウイルス対策ソフト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ワクチンソフトのサーバ側プロセス動作状況は，常時監視されているか（例．ウイルスバスターコーポレートエディションのサーバモジュール） 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	管理規定 運用規程
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	管理規定 運用規程

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古いOSを使用していないか（例．95，98，NT ） ③パッケージソフトウエアの購入に際し、ライセンス管理と連携しているか ④ 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 ⑤ 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 ⑥ 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 ⑦ コンピュータを撤去した場合、不要な磁気テープ等の記憶媒体がコンピュータールーム内に放置されていないか ⑧ 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な状況はないか ⑨ 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（社外との接続基準があるか） ⑩ 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 ⑪ 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 ⑫ 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 ⑬ 稼動している本番システムにおいて、プログラム移行を行う際にテストの検証が、開発者とシステム管理者とで行われているか	管理規定 運用規程

項　　目	チェックポイント	関係条文・資料
信頼性	⑭ 本番環境へのプログラムの移行作業は、システム管理者（運用担当者）で行われており、開発担当者が含まれていないか ⑮ 障害が発生した場合の、対応について、その障害のレベルを定義し、そのレベルに応じた報告・対応手順を作成しているか。 ⑯ 障害対応マニュアルが整備されており、定期的にマニュアルに従った訓練を行っているか ⑰ 障害発生時は、障害対応手順書に基づいて行われており、その記録が作成され且つ、一定期間保存されているか ⑱ オペレーションは、あらかじめ作成された規定、手順書に基づいて行われており、その記録が作成され且つ、一定期間保存されているか ⑲ 臨時のオペレーションについては、システム管理者の承認を受けた指示書に従って行われているか。また、その記録が作成され且つ、一定期間保存されているか	管理規定 運用規程
安全性	① 予想される地震、火災、水害、盗難等の災害に対して、コンピュータールームの安全対策を講じているか 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 ③ 防災設備に対する点検／整備は，適切に行われているかまた，点検／整備記録は，適切に保管されており，迅速に照会可能か（例．消火器の使用期限，煙感知器の定期点検　等々）	管理規定 運用規程