「情報漏洩対策」のためのチェックシート　（脅威と対策）［2004.07.16］

| 管理項目 | トリガー | 想定される事象 | 人的対策 | 教育による対策 | 運用技術（ツールの導入）による対策 | 設備／体制による対策 |
|---|---|---|---|---|---|---|
| 経営者 | セキュリティ対策を軽視 | ・基本方針の未定義<br>・社員への不徹底<br>・上記に伴う、社員モラルの低下 | ○ | ・経営者、幹部へのセキュリティ教育<br>・情報漏洩に伴う被害（コスト）を理解してもらう | | |
| システム管理者 | 関連法制度（著作権、個人情報漏洩等）の知識不足 | | ○ | ・システム管理者への法令・倫理教育 | ・セキュリティ対策の実現を支援するツールの学習、導入検討 | |
| | 企業倫理・システム監査部門からの監査不足 | | | | オペレーション監視（ログ取得）ツールの導入 | システム監査部門の設置、監査の実施 |
| 社員<br>（派遣社員含む） | 公共スペース（社内休憩所、通勤途上、飲食時）での業務関連会話 | 第三者へ社外秘情報の流出 | ○ | ・社会人としての基本モラル教育<br>・規程教育 | | 社内規程 |
| | 退職（派遣契約満了）後の事務所出入り | | ○ | | 退職従業員IDの早期無効化 | 社内規程＋入退出管理 |
| | ビジネス（従業員用の）用手帳の紛失 | | ○ | | 手帳の廃止、電子ツール化（暗号化） | 社内規定＋肌身離さない習慣 |
| | 誘惑による副収入狙い機密文書、名簿の持出 | 名簿売買業者、競合会社への流出 | ○ | 社会人としての基本モラル教育 | モラル教育 | |
| | 会社への逆恨みによる資料持出 | | ○ | | 適切な人事管理、コミュニケーション | |
| | IDカード（通門証など）の紛失 | 侵入・不正アクセスを誘引 | ○ | 規程教育 | 生態認証 | ・運用規定と紛失時の連絡体制の確立<br>・「ID抹消作業」の迅速化 |
| | 会社のPCの持出（業務都合上） | 機密情報をコピーされる | ○ | | 機密ファイルの暗号化 | 運用規程 |
| 派遣会社<br>業務委託会社 | 情報漏洩を禁止する契約の不備 | 機密保持契約だけでは対応できない、情報漏洩リスク | | | | 情報漏洩リスクを回避する契約締結 |
| 印刷物 | 安易な廃棄、裏紙再使用 | 一般ごみとして社外流出 | ○ | ・職場の整理整頓<br>・規程教育 | | ・文書取扱い規程（廃棄／再利用に関する規程）<br>・廃棄印刷物仕分け体制 |
| | 自宅持ち帰り、電車の中での印刷物閲覧 | 家庭ごみとして流出、部外者の目に触れる | ○ | ・社会人としての基本モラル教育<br>・規程教育 | | ・文書取扱い規程（社外持ち出しに関する規程） |
| | プリンター上に印刷物を放置 | 権限外人員の目に触れる | ○ | ・職場の整理整頓<br>・社会人としての基本モラル教育 | | |
| | 配布用コピー資料の原稿置忘れ | 権限外人員の目に触れる | ○ | ・職場の整理整頓<br>・社会人としての基本モラル教育 | | 対応機能を持ったコピー機の採用（複写用トレイへの原稿置忘れには有効な音声アラーム） |
| | 窓があいていた（コピー機やプリンタの傍） | 風による散乱　→　権限外人員、社外への流出 | ○ | ・職場の整理整頓<br>・社会人としての基本モラル教育 | | 窓の鍵を施錠固定、レイアウト上の配慮 |
| | PCからのFAX送信あて先を間違う | 社外流出 | ○ | | ・アドレス帳データの統一管理<br>・PC　FAXの禁止（モデムの削除） | |
| | 離席時の書類の放置 | 権限外人員の目に触れる | ○ | ・職場の整理整頓<br>・社会人としての基本モラル教育 | | ・仕掛かり案件BOXの設置<br>・離席時収納を徹底 |
| | 清掃業者による机上のメモ、書類等の流出 | 一般ごみとして社外流出 | ○ | ・職場の整理整頓<br>・社会人としての基本モラル教育 | | |
| 文書ファイル／<br>バックアップ媒体 | 施錠無し保管，保管庫への入退室管理の不備 | 権限外人員の目に触れる，不正持ち出しを誘引 | ○ | 規程教育 | 文書管理システム導入（文書の電子化） | ・社内規定（ファイリング／バックアップ 規定）<br>・保管庫の入退室管理システム |
| | 内容・機密レベルの安易な表示（ロッカー，ファイル背表紙） | 不正持ち出しを誘引 | ○ | | | |
| | ファイル・メディア内の格納文書の未把握 | 何が、どこにあるか不明 | ○ | | | |
| クライアントPC | HD未除去のままPC廃棄やリース・レンタルPC機返却 | 未消去データの社外流失 | ○ | PC使用に際する、セキュリティ教育 | データ消去ツール、HDの破壊 | リース/レンタル会社との返却PCHDDの処理に関する取り決め／契約 |
| | PCの紛失、盗難 | 未消去データの社外流失 | ○ | PC使用に際する、セキュリティ教育 | BIOSパスワード、HD暗号化 | ・クライアントPCに重要データは保存させない<br>・モバイルPCに関する運用規程 |
| | FD,CDなど記録済メディア媒体の廃棄、紛失、盗難 | 未消去データの社外流失 | | ・PC使用に際する、セキュリティ教育<br>・職場の整理整頓 | データ消去・媒体破壊 | |
| | 公共の場でモバイルPC使用（第三者による画面の覗き見） | 第三者への開示と同じ | ○ | PC使用に際する、セキュリティ教育 | 狭視野フィルタの採用 | 社内規程（禁止すべき） |
| | 画面の覗き見（社内） | 権限外人員の目に触れる | ○ | PC使用に際する、セキュリティ教育 | 狭視野フィルタの採用 | パーティション導入<br>レイアウト上の配慮（重要プロジェクトは別室／別棟へ隔離）<br>入退室管理の徹底 |
| | 離席時の画面とキーボードのロック忘れ | 成りすまし、権限外人員の操作を誘引 | ○ | PC使用に際する、セキュリティ教育 | ・スクリーンセーバ・パスワードロックの設定<br>・ロック用デバイスの採用（USBトークン） | |
| | 退社時（電源切断忘れ、ログオンしたまま） | 成りすまし、権限外人員の操作を誘引 | ○ | PC使用に際する、セキュリティ教育 | 集中電源制御 | |
| | 出力先ネットワークプリンタ間違い（関係者外秘の流出） | 社外流出 | ○ | PC使用に際する、セキュリティ教育 | 余分な出力先は設定しない | プリンタの分散配置（例. セグメント毎に必要数量を配置） |
| | メールの宛先の誤記入及び余分な宛先記入 | 対象者以外への開示につながる | ○ | PC使用に際する、セキュリティ教育 | アドレス帳データの統一管理 | |
| | MS-Officeドキュメントのプロパティ | 作成者情報の流出 | ○ | PC使用に際する、セキュリティ教育 | プライバシーオプションの設定 | |
| | MS-Officeドキュメントの変更履歴 | 対象者以外への開示につながる | ○ | PC使用に際する、セキュリティ教育 | | |
| | 「共有設定」不適切 | 権限外人員のアクセスを誘引<br>HotSpotなどのグローバルアドレス接続時のリスク回避 | ○ | PC使用に際する、セキュリティ教育 | ツールによる「共有設定」把握、解除 | PCにデータは保存禁止（データは全てファイルサーバへ） |
| | 共用PC（部門共用、出張者用） | アカウント（パスワード）の安易な設定<br>ゲストアカウントの運用徹底 | | PC使用に際する、セキュリティ教育 | オペレーション監視（ログ取得）ツールによる監視 | |
| | 管理者が認めないソフトウエア（P2Pソフト・仮想VPNソフト）の使用 | 社外流出<br>権利問題のあるファイル・ウイルス感染ファイルの流入 | ○ | PC使用に際する、セキュリティ教育 | ツールによるインストール監査、禁止ソフトの起動制御 | PCを限定して使用を許可 |
| | コンピュータウイルス | 添付ファイルとして流出 | ○ | PC使用に際する、セキュリティ教育 | ウイルス対策ソフト、セキュリティパッチ適用管理 | 軽率なメール添付ファイルの実行 |
| | スパイウェア | 不正アクセス | ○ | PC使用に際する、セキュリティ教育 | スパイウェア対策ツール導入 | 社内教育・啓蒙（業務に関係のないサイトにアクセスしない）、 |
| | OS、アプリケーションの脆弱性 | 不正アクセス | ○ | PC使用に際する、セキュリティ教育 | セキュリティ・パッチ適用管理ツール、検疫ネットワーク | WindowsUpdateの実行 |
| | リモート回線の設定情報の漏洩 | 不正アクセス | | PC使用に際する、セキュリティ教育 | | 保守契約に運用ルールを明記 |
| | パケットキャプチャの無断設置 | 権限外人員のアクセスが可能になる | ○ | PC使用に際する、セキュリティ教育 | | 社内規程（発覚時に厳重処分） |
| | 安易なパスワード設定 | 成りすまし、不正アクセスの誘引 | ○ | PC使用に際する、セキュリティ教育 | ドメインポリシー、アプリケーション側で規制 | 社内規程（文字種・数を規程） |
| | 社外ネットワーク（ホットスポットなど）でのクラッキング | 不正アクセス | ○ | PC使用に際する、セキュリティ教育 | 社外ネットワーク使用時の危険性を教育・啓蒙 | ホットスポットへの会社のPCの接続は禁止 |
| | 権限を持つ者による漏洩 | 不正持ち出し | ○ | PC使用に際する、セキュリティ教育 | システム操作ログ取得、ダウンロードファイルの強制暗号化 | |
| | 2ちゃんねる等の社外掲示板書き込み | 第三者への開示と同じ | ○ | 社会人としての基本モラル教育 | WEBフィルター、システム操作ログ取得 | 社外掲示版へのアクセスは禁止 |
| | 電子メール転送 | 社外流出 | ○ | PC使用に際する、セキュリティ教育 | メールフィルター | |
| | 私物PCの持込、ネットワーク接続 | 社外流出 | ○ | PC使用に際する、セキュリティ教育 | MACアドレス登録管理、検疫ネットワーク | 私物PCの持ち込みは原則禁止 |
| | 初心者ユーザや重役ユーザを装って，システム管理者に電話し，アカウント・パスワードを聞きだす | 成りすまし、不正アクセス | ○ | PC使用に際する、セキュリティ教育 | | 業務フローの徹底、抜き打ちチェック |
| | ゲームなどを装ったフロッピーをターゲットに郵送する．机に置いておく． | スパイウエアを送り込まれる | ○ | PC使用に際する、セキュリティ教育 | | 抜き打ちチェック |
| | ハードディスクの交換 | 修理時の社外流出 | | | 修理手順規程（確実なデータ抹消・破棄） | 修理運用規程 |
| | PC本体の故障 | | | | ハードディスクは外して（ダミーディスクで）修理依頼 | 修理運用規程 |
| 複合機 | 「メモリー・HD」に残ったデータ | 権限外人員の目に触れる | | | | 機種によっては、対策済み |