４．個人情報の適切な管理の場面

（１）個人情報の管理システム（物理的・技術的措置を中心に）

本節では、特に情報システムを中心とした技術的安全管理措置や、施設や設備、個人情報を含む書類等の事業所内及び事業所外における物理的安全管理措置に着目して事例を取り上げている。

例えば、情報システムに関しては、個人情報にアクセスできる端末そのものを可能な限り少なくしている事例（⑲）や、個人情報専用のネットワークを構築している事例（㉕）などを紹介している。その他、電子メールの送受信について問題がありそうな内容の場合は、自動的に送信停止を行うようなシステムを開発した事例（⑦）、営業担当者の携帯電話紛失による情報漏えいを防止するために、利便性とセキュリティ強化に配慮した独自システムを導入したような事例（㊷）も紹介している。

さらに、個人情報を含むファイルを取り扱う作業については逐一管理者にメールで自動的に連絡が行くようなシステムを開発した事例（㉛）も紹介している他、専門チームでPC監視を行っているような事例（㊻、㊼）もある。

また、物理的安全管理措置としては、取り扱う機密情報（個人情報を含む）の種類によって執務フロアの区画を分け、それぞれの区画におけるアクセス権限や使用可能機器を細かく規定している事例（⑭、㉗）や、外出の際には個人情報を紛失しにくい作りにした専用カバンの使用を義務付けたり（㉘）、事業所内においては個人情報の機密レベルに応じて色の着いたシールで分類管理を行って施錠管理している事例（⑪）、セキュリティレベル区分された職場ごとに職員に異なるベストの着用をさせる事例（㊽）など、日常的に使用する設備・備品等について工夫することで適切な管理を図っている事例なども紹介している。

本節で紹介している取組事例

4-(1)-①：個人情報の重要度にあわせた管理方策の分類
4-(1)-②：扱う個人情報セキュリティ水準に合わせて、機械的管理とソフトな管理を使い分ける
4-(1)-③：個人情報が記載された伝票類は施錠管理、特に顧客名簿は日々の枚数チェック等管理体制強化
4-(1)-④：外商担当者は個人情報をイニシャル等の形式で登録
4-(1)-⑤：物理的・技術的管理を徹底
4-(1)-⑥：生体認証で入退室を管理している
4-(1)-⑦：特定のキーワードを含む電子メールはサーバで送信を自動的に停止する
4-(1)-⑧：“三点セット”による入退室管理

4-(1)-⑨：バーコードによるトレーサビリティ確保
4-(1)-⑩：システム上の安全管理
4-(1)-⑪：情報の機密分類に応じてシールで色分け
4-(1)-⑫：私有パソコンの持ち込み禁止、社内使用パソコンの持ち出し禁止
4-(1)-⑬：センシティブ情報へのアクセスは物理的に厳しく管理
4-(1)-⑭：建物内における“セキュリティ区画”の設置
4-(1)-⑮：ファイル共有ソフト（Winny 等）対策の徹底
4-(1)-⑯：リモートアクセスの脆弱性に対して、アクセス権限の対象・期間的に厳格な制限実施
4-(1)-⑰：個人情報を集中管理するデータセンターにおいて特に厳重な管理を実施
4-(1)-⑱：ファイル共有ソフトは自己チェックとソフトで二重にチェックを行う
4-(1)-⑲：個人データを保管するサーバにアクセスできる端末は 1 校舎に 1 台のみ設置
4-(1)-⑳：センシティブな個人情報は紙媒体でのみ管理し、大量漏えいを防止している
4-(1)-㉑：データの授受は手渡し又はセキュリティ便を利用
4-(1)-㉒：キャビネットは開閉を記録者名で管理
4-(1)-㉓：専用金庫、専用カバンなどの使用により、物理的管理を徹底
4-(1)-㉔：社外携行時は氏名や住所を 2 つに分けることで、「個人の特定が容易でない形式」で保有
4-(1)-㉕：独自アプリケーションの開発により本社への報告迅速化、営業職員が個人情報を保有し続けるリスクの回避を実現
4-(1)-㉖：個人情報専用のネットワークを構築し、外部との接続を遮断
4-(1)-㉗：個人情報取扱エリアを特定し、業務を集中化
4-(1)-㉘：検針ターミナルから離れるとアラームが鳴り、置き忘れ・盗難を防ぐ
4-(1)-㉙：グループ会社店舗の端末からは外部媒体に書き込みができなくしている
4-(1)-㉚：データベースのアクセスログの定期点検を実施。時間外や休日のログに注目
4-(1)-㉛：個人情報を含むデータに関するアクションは全て個別に管理者に通知
4-(1)-㉜：退職者にも Winny 対策を徹底
4-(1)-㉝：個人情報を 3 種類の台帳で管理
4-(1)-㉞：リスク分析の義務付けで、不必要な個人情報を大幅に削減
4-(1)-㉟：ツールを導入により台帳管理を効率化、高度化
4-(1)-㊱：グループ共通基準を作成。全社が順守すべき「必要対策」と各社ごとの「推奨対策」の二段階チェックにより、各社に最適なセキュリティ対策を実施
4-(1)-㊲：全社方針を元に機能毎に構成される本社統括組織が年度計画・セキュリティを立案し、関連企業はその計画を元に運営する
4-(1)-㊳：組織の成熟度に応じてレベル分けされた目標を指標に、本社内と関連会社内の二段階で年度目標を設定している

4-(1)-㊴：組織の成熟度は、セルフチェックと内部監査を組み合わせて総合的に評価

4-(1)-㊵：ISMS の台帳に個人情報保護の項目を追加して情報資産と個人情報の管理を一体化して効率的に運用

4-(1)-㊶：ログ取得に注力し、有事に備えている

4-(1)-㊷：携帯電話のメール送受信の制限による漏えいリスクの低減と利便性をバランス

4-(1)-㊸：USB メモリへの書き出しは顧客ニーズに合わせ、限定パソコンで部長決裁の上で実施

4-(1)-㊹：個人情報等が含まれる書類の収納スペースを狭くすることで不要な個人情報等を削減

4-(1)-㊺：問合せデータベースは、独自 ID で個人を特定し、個人情報を不可視に

4-(1)-㊻：社員が使用している PC を専門チームにより常時監視

4-(1)-㊼：退職予定者は、特に厳しく監視・管理

4-(1)-㊽：データセンター内をセキュリティレベルに応じて区分し、区分ごとに色分けしたベストを職員に着用させている

4-(1)-㊾: 複数のサーバに情報を分散し、保管することで、よりセキュアな環境で管理

4-⑴-①【個人情報の重要度にあわせた管理方策の分類】

（製造業：約 300,000 人（グローバル））

・A 社では個人情報を、「内部使用のみ」、「機密（コンフィデンシャル）」、「個人情報厳秘」、の 3 段階に分けて、それぞれについて管理基準を定めている。上記のそれぞれのレベルに合わせ、「保管方法」「アクセス権者」「持ち出し可否」「複製・複写可否」「配布・通信手段」「廃棄要否」「他社への開示に際する秘密保持契約の要否」などを規定している。

・定期的に個人情報の棚卸を行っている。目的・取得方法・取得者・管理者・件数などの情報を一覧表（インベントリー・リストと呼称）にしている。棚卸時に「活用しない」データを削除するようにしている。

・消費者の個人情報を送付しなければ場合には、できる限り個人情報にしない取組みを行っている（お客様の氏名は、姓のみを表示するなど）。

4-⑴-②【扱う個人情報セキュリティ水準に合わせて、機械的管理とソフトな管理を使い分ける】（卸売業：約 170 人）

・E 社では個人情報を取り扱う執務室については管理レベルを分けており、入室可能な者をそもそも相当程度絞り込んでいる。

・最もセキュリティが厳しく、入室可能者が限定されているのが、ガスの使用量やガス漏れ等をオンラインで集中管理しており、大量の個人データが蓄積されているシステムのある部屋であり、ID カードリーダーで入室管理を行っている。

・個人情報を特に扱うような部署については、入室時に必ず「入室理由」、「入室時間」、「面会者」、などについて記帳するようになっている。この記帳が面倒であるので、入室することなく用件を済ませる工夫（その部屋で執務している従業者を入口の内線電話で呼び出す形で話や用件を伝える等）をしている。

4-⑴-③【個人情報が記載された伝票類は施錠管理、特に顧客名簿は日々の枚数チェック等管理体制強化】

（小売業（百貨店・スーパー）：約 10,000 人）

・F 社では顧客名簿や各種伝票においては、保管方法・期間・最終処理方法等について基準を設け、管理を徹底。

・特に顧客名簿においては、チェックシートを活用し、日々の獲得枚数、廃棄枚数、ファイルごとの総枚数管理を徹底している。

・また、顧客情報システムから出力される「顧客リスト」の運用（出力・配布・管理・回収）については、受渡時の枚数や回収予定日の確認、施錠管理などを徹底している。

4-⑴-④【外商担当者は個人情報をイニシャル等の形式で登録】

（小売業（百貨店・スーパー）：約 10,000 人）

・F 社では携帯電話には個人情報を登録しないことをルールとしている。外商担当者は、個人情報をイニシャルで登録するなど、個人情報と識別できない形で登録することになっている。また、ラインの中で誰がどの情報を持っているか登録することになっている。

4-⑴-⑤【物理的・技術的管理を徹底】（小売業（物販）：約 450 人）

・G 社では社用 PC には、規定により許可された以外のアプリケーションのインストールは禁止されており、情報システム部で監視できる体制となっている。

・アプリケーションの起動のログはすべて取っている。

・FD や USB メモリなど、外部メディアへの書き出しは一切できないようになっており、書き込もうとするとブロックがかかる。

・またそれ以外の外付け機器を接続しても同様である。

4-⑴-⑥【生体認証で入退室を管理している】（小売業（通販等）：約 520 人）

・H 社では監視カメラの設置、入館管理時の IC カードによる管理、及び記録メディアや携帯電話の持ち込みの禁止をしている。

・サーバ室など機密度の高い部屋は、入室権限を最小限の人数に抑え、さらに生体認証で入退管理室を実施している。また、コールセンターはセンシティブな情報が多いため、センター長の許可がなければ社長であっても入室できないシステムにしている。

・情報漏えい防止ソフトを導入し、暗号化をしている。

4-⑴-⑦【特定のキーワードを含む電子メールはサーバで送信を自動的に停止する】

（小売業（通販等）：約 520 人）

・H 社では電子メールの利用において、特定のキーワードが含まれるものはサーバで自動的に送信がストップされる仕組みを導入している。添付ファイルがあるものはすぐには送信できず、システムの担当者が中身をチェックして問題がなければ送信するようになっている。

4-⑴-⑧【“三点セット”による入退室管理】（信用業：約 3,700 人）

・I 社ではコールセンターや事務センターといった個人情報を取り扱うことの多い部署において、指紋認証、監視カメラ、個人私物ロッカーの“三点セット”を用いて、入退室管理を行っている。

4-(1)-⑨【バーコードによるトレーサビリティ確保】（信用業：約 3,700 人）

・I 社では個人情報を含む書類等の授受は、自社開発したシステムを活用して、バーコードによる追跡（トラッキング）ができるようにしている。これによってリアルタイムで書類等の所在が確認できる。

4-(1)-⑩【システム上の安全管理】（信用業：約 3,700 人）

・I 社では重要な情報が集中する「システムセンター」で、情報セキュリティの標準規格である「ISO27001（ISMS)」の認証を取得している、また、専管するチームを設置し、技術・設備・運用の各面から安全管理に努めている。

4-(1)-⑪【情報の機密分類に応じてシールで色分け】（信用業：100 人未満）

・K 社では情報を、極秘、機密、その他の３つに分類し、極秘情報は赤色シールを付けて、常時施錠されるキャビネットに保管している。機密情報は黄色シールを付けて、終業時にキャビネットを施錠して管理している。

4-(1)-⑫【私有パソコンの持ち込み禁止、社内使用パソコンの持ち出し禁止】
（情報サービス業：約 6,700 人）

・L 社では個人所有のパソコンをはじめとする私有情報機器の社内持ち込みを禁止している。

・社内使用パソコンは原則として社外持ち出し禁止としている。職種によりノート PC の社外持ち出しが必要な従業者は社内では専用の外部 HDD を用い、この外部 HDD は社外に持ち出しができない運用としている。このため、社外に持ち出したノート PC には機密情報が存在しない。業務上止むを得ず機密情報を持ち出す場合は暗号化を行う運用としている。

4-(1)-⑬【センシティブ情報へのアクセスは物理的に厳しく管理】
（情報サービス業（ソフトウェア）：約 400 人）

・N 社では個人情報保護マネジメントシステムの移行に合わせてリスクマネジメントを強化。情報のリスクランクに応じた安全管理を実施。

・入退室管理では、守衛による IC カードゲートと入館確認、事務所内に入るための IC カードゲートシステム、CPU ルームに入るための入室チェックの厳重な多重チェック体制を構築。

・ログインには登録者のみに付与されたログイン ID が必要である。

・重要な個人情報は、ネットワーク接続禁止で、独立したサーバで管理している。

・クレジットカード情報の取り扱いについては、汎用機で処理、アクセス権を設定し、

厳しい入退室管理とセキュリティ対策を実施。
・ファイル共有ソフト等 P2P ソフト対策のため、『一斉送信監視ソフト』により監視。また、『ライセンス違反検知ソフト』により、P2P ソフト等のインストールを監視。

4-⑴-⑭【建物内における“セキュリティ区画”の設置】

（情報サービス業：約 1,600 人）

・O 社では「情報へのアクセスコントロール」と「取扱いのトレーサビリティ（追跡性）」を目的として、執務エリア（システム開発室）をセキュリティレベル別に 4 段階のセキュリティ区画に分けている。

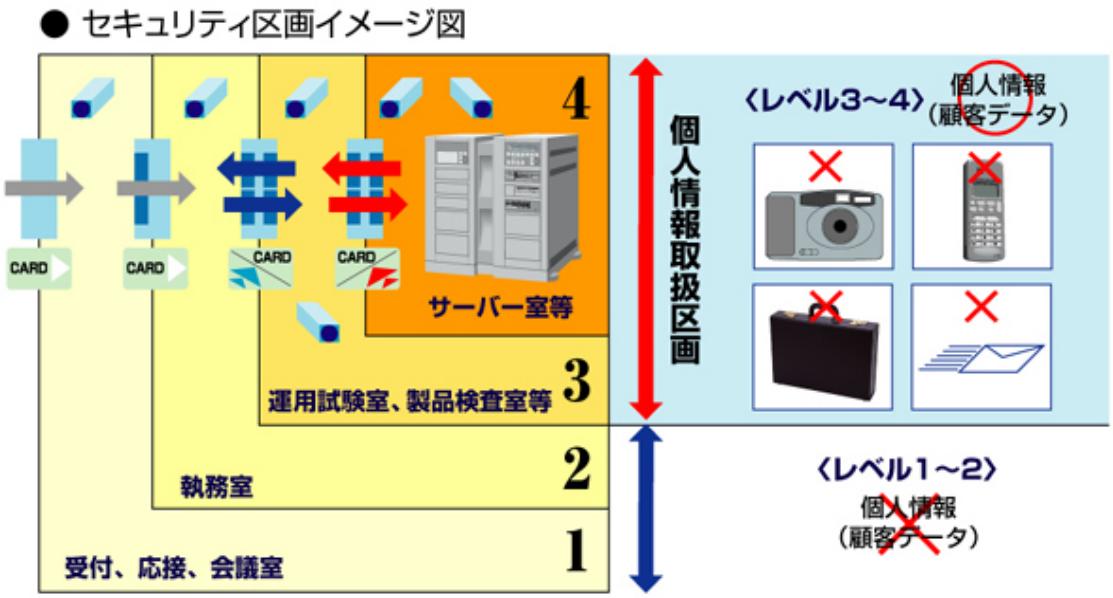
＜セキュリティ区画レベル４，３（個人情報取扱区画）＞

・セキュリティ区画レベル４はサーバ室等で顧客データ（個人情報）が保管されているエリアである。セキュリティ区画レベル３はシステム運用試験や製品検査を行うエリアであり、顧客データ（個人情報）を実際にハンドリングして運用テストなどを実施する。
・セキュリティ区画レベル４，３のエリアにのみ顧客データ（個人情報）の持ち込みが許されている。又は、その２つのエリアにおいては、カメラ、携帯電話の持ち込みが禁止されており、カバンの使用、及び電子メールの発信等も禁止されているなどそれぞれの設備対策が施されている。セキュリティ区画レベル４，３に設置された社内ネットワークがセキュリティ区画レベル２の執務室の社内ネットワークやインターネットと分離されているため電子メールの送受信やインターネット Web の閲覧はできず、顧客データ（個人情報）の漏えいや外部からの不正アクセスを防いでいる。
・セキュリティ区画レベル４，３では入室者が特定されており、入室作業者の作業状況を監視カメラで記録、入退室者の入退室記録が IC 入退室管理装置と監視カメラで行われている。
・顧客から送付された郵送物の中に、システムに関する問合せや確認のために、個人情報が記録された画面のハードコピー等が送付されている場合があるため、開封作業は同区画内で行っている。また、郵送でなく FAX で送付される場合もあるため、同区画内に設置した個人情報受信専用 FAX で受信している。

＜セキュリティ区画レベル２，１＞

・受付・応接・会議室がセキュリティ区画レベル 1、執務室（システム開発室）はセキュリティ区画レベル 2 とされており、顧客データ（個人情報）は存在してはいけないエリアとなっている。

図表　セキュリティ区画の構造



4-(1)-⑮【ファイル共有ソフト（Winny 等）対策の徹底】（情報サービス業：約 1,600 人）

・O 社では、社会問題となっている Winny 等による個人情報漏えい事故が、個人情報や業務情報を会社から自宅に持ち帰り私物のパソコンを使って作業をしていたために重要情報の漏えい事故が発生していることを踏まえ、社員情報、企業機密情報、業務情報などを許可無く持ち出すことを禁止した。もちろん、これらの情報を自宅へ持ち帰って自宅で作業をすることも禁止している。

・社内においても私物のパソコンや私物のＵＳＢメモリ等の外部媒体を持ち込んで作業をすることを禁止している。この方法もファイル共有ソフトによる漏えい防止対策の一環としている。

・社内 LAN に接続されている全国の事業所すべてのパソコンについて、インストールされているプログラムや作成されているファイルを検索するツールが備わっている。このツールによりファイル共有ソフトの存在確認を定期的に行っている。

・毎年、従業者の自宅の私物パソコンについて点検し報告させているが、昨今の漏えい事故件数増加を背景として平成 20 年度から点検を 2 回（半期毎）に増やした。

4-(1)-⑯【リモートアクセスの脆弱性に対処するため、アクセス権限の対象・期間的に厳格な制限を実施】（情報サービス業：約 1,600 人）

・O 社では、リモートアクセスにおけるセキュリティの技術面の脆弱性は以前から認識されており、今まではルール整備は行ったものの、実際にはルールが完全に守られていない可能性があった。

・平成 20、21 年度に、特にリモートアクセスに関する脆弱性対策を対策の 1 つに掲げ、

具体的には以下のようなリモートアクセスの仕組みの見直しを行った。

ア）シンクライアントを大量導入し、データの持ち歩きを一層制限した。

イ）会社貸与のシンクライアント端末等、登録が済んだ機器以外は社内ネットワークに接続できないようにした。

ウ）リモートアクセスで外部から利用できるシステム・サービスごとに利用者を事細かに分類した。

エ）リモートアクセスの利用者 ID の有効期間を最長 3 ヶ月とし、利用を継続したい場合には再申請を行うこととした。

オ）通常の個人情報保護教育に加えて、リモートアクセスの利用者に対しては、セキュリティ教育の受講を義務化した。

4-(1)-⑰【個人情報を集中管理するデータセンターにおいて特に厳重な管理を実施】
（複合（情報システム／製造）：約 500 人）

・R 社では重要情報はすべて、データセンターを持つ事業所で厳重管理している。他拠点の情報のバックアップも当該事業所で管理しており、施錠管理、入退出管理（カード）、監視カメラ、暗証番号と指紋認証によって厳しい管理がなされている。特に重要度の高い情報が管理されているサーバルームへの入室には指紋認証、パスワード入力、IC カードの 3 種類の認証が採用されており、入室は一人ずつしかできない。

・パスワードは月に 1 度変更を義務付けている。

4-(1)-⑱【ファイル共有ソフトは自己チェックとソフトで二重にチェックを行う】
（複合（情報システム／製造）：約 500 人）

・R 社では、従業者が各自のパソコンにファイル共有ソフトが入っていないかどうかを自己チェックし、申告した。その後ウイルスチェックソフトでファイル共有ソフトの有無をチェックした。チェックは毎月実施している。

4-(1)-⑲【個人データを保管するサーバにアクセスできる端末は 1 校舎に 1 台のみ設置】
（その他サービス業（教育、学習支援）：約 190 人）

・T 社では個人データを本社のサーバに集約しており、当該サーバにアクセスできる端末は校舎に 1 台のみ設置している。以前は従業者全員が自分の端末内に情報を持っていたが、それを一度すべて消去して上記の仕組みを導入した。

・中央管理しているサーバについては、アクセスログが残り、どの端末からアクセスがあったかがわかるようになっている。

4-(1)-⑳【センシティブな個人情報は紙媒体でのみ管理し、大量漏えいを防止している】
（その他サービス業（エステティックサロン）：非公開）

・W 社では店舗において、利用者の個人情報をすべて紙媒体で管理している。店舗ごとに鍵のかかるロッカーに保管し、ロッカーは帰宅時に施錠している。サロン責任者が施錠の責任者となり、紙情報は、サロン責任者の指示がなければ持ち出せない規則となっている。

4-(1)-㉑【データの授受は手渡し又はセキュリティ便を利用】
（その他サービス業（印刷・広告）：約 11,000 人）

・X 社では外部とのデータの授受において、手渡し又はセキュリティ便を利用している。
・工場間など社内でのデータの授受では、鍵つきジュラルミンケースで運ぶ個人情報専用便を利用している。
・データのやり取りは専用伝票で記録しており、受け取りから返却又は破棄までが管理できるようになっている。

4-(1)-㉒【キャビネットは開閉を記録者名で管理】
（その他サービス業（印刷・広告）：約 110 人）

・Y 社では共有のキャビネットはいつ誰が開けて何を取り出したかを紙で記録するようにしている。スペアキーを持っている者をリスト化している。

4-(1)-㉓【専用金庫、専用カバンなどの使用により、物理的管理を徹底】
（その他サービス業（債権回収支援）：約 30 人）

・γ社では契約社員については個人情報を保管する場合には、指定された特殊な専用金庫を使用することを義務付けた。
・外回り時には専用のカバンを使用することを義務付け、そのカバンは必ずチェーンで自分とつなぐようにしている。とにかくカバンを肌身離さないことを徹底するために実施しており、車の運転中でもチェーンが問題ないように、助手席にカバンを置いた場合の距離やチェーンの具合なども確かめ、金具店に特注して作成してもらったものである。
・専用カバンについては、使いやすく、出し入れの途中で紙やデータが外に落ちにくいもの、ということで既製品を選んで指定している。

4-(1)-㉔【社外携行時は氏名や住所を 2 つに分けることで、「個人の特定が容易でない形式」で保有】（その他サービス業（債権回収支援）：約 30 人）

・γ社では社外に個人情報を携行する必要がある場合は、紙媒体の場合でも、データの場合でも、個人情報は 2 つ（2 枚の紙、2 つのファイル）に「氏と名」「住所の前半と後半」のように分けて管理しており、万が一、片方が紛失しても個人を特定できないようにしている。

・2 つのデータの照合は個人ごとの番号で実施している。

4-(1)-㉕【独自アプリケーションの開発により本社への報告迅速化、営業職員が個人情報を保有し続けるリスクの回避を実現】

（その他サービス業（債権回収支援）：約 30 人）

・γ社では営業の契約社員等が債務者等を訪問した際の対応等について迅速に本社に報告し、また契約社員等がデータの形で個人情報を保有し続けることによるリスクを回避するために、携帯端末を使用して本社のサーバに直接的に情報を送信できるアプリケーションを開発した。

・このアプリケーションを使用すれば、携帯端末で個人情報を呼び出すことができ、その個人に対して行った対応等を携帯端末で書き込み、本社サーバに送信すれば一切の情報が携帯端末には残らないようにできるというものである。

・紙ベースでの個人情報の取扱いはどうしても紛失リスクが大きいため、一定のコストを要してアプリケーションを開発した。

・不正アクセスを防止するため、通信回線は IP-VPN（閉域網）を使用し、暗号化と併用することでセキュリティを確保している。

4-(1)-㉖【個人情報専用のネットワークを構築し、外部との接続を遮断】

（その他サービス業（債権回収支援）：約 30 人）

・γ社では社内での電子データでの個人データの取扱いにおいては、インターネット等外部環境との接続を遮断している。

・専用サーバ、クライアントパソコンは管理ソフトを導入し、物理的なコピーや記録媒体による持ち出しができないように制限をかけている。

4-(1)-㉗【個人情報取扱エリアを特定し、業務を集中化】

（その他サービス業(印刷・広告：11,000 人)）

・X 社では、全国にある個人情報を取り扱う業務を、それぞれの事業所のセキュリティエリアに集中させている。同エリアでは、他のエリアと物理的に切り分け、作業者を特定・極少化し、許可された者以外の入退管理を厳密に行っている。

・作業はセキュリティエリア内のみで行うことにしており、作業中に想定し得るケアレスミスに対し、事故発生につながらないような工程ルールの適正化・標準化・教育・運用（記録・点検・監査）の徹底を行っている。

4-(1)-㉘【検針ターミナルから離れるとアラームが鳴り、置き忘れ・盗難を防ぐ】

（電気・ガス・水道業：約 1,000 名）

・イ社では、検針のハンディターミナルについてはIDとパスワードを入力しないと起動できないようになっている。
・機器紛失の危険を回避するために、担当検針員が検針ターミナルから2、3メートル以上離れるとアラームが鳴るようになっている。

4-(1)-㉙【グループ会社店舗の端末からは外部媒体に書き込みができなくしている】
（電気・ガス・水道業：約1,000名）

・イ社では、サービスショップの端末に関しては、別媒体へ情報が保存できないように設定している。社内の端末に関しても制限を設けている。
・オフィスのセキュリティ管理の強化に取り組んでおり、建物によってはRFIDカードによる入退室管理を行っているところもある。

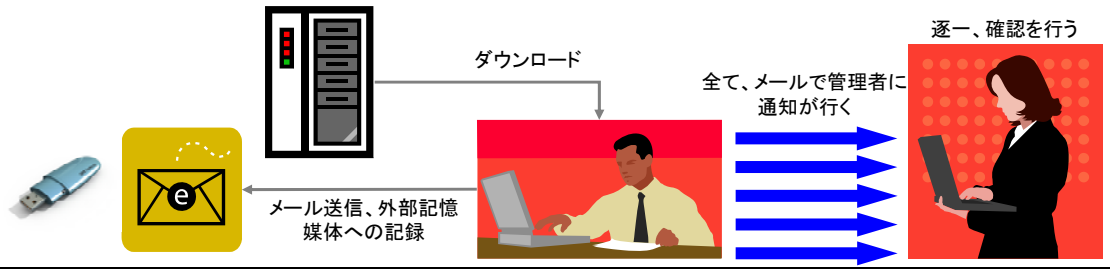
4-(1)-㉚【データベースのアクセスログの定期点検を実施。時間外や休日のログに注目】
（小売業(通販等):約1,800名）

・オ社で、データベースのアクセスログを取得し、定期的（少なくとも3ヶ月に1度）に点検している。時間外、休日等のアクセス状況に着目している。
・PCの操ログも取得している。セキュリティポリシーを設定し、ポリシーに抵触する操作が発生した場合、通知が電子メールで事務局、内部監査担当、システム担当に送付される。公開はしていないが、監視基準が定められており、不正操作と判断された場合、監視責任者より警告が発信される体制になっている。

4-(1)-㉛【個人情報を含むデータに関するアクションは全て個別に管理者に通知】
（信用業：約2,000名）

・カ社で、個人別に権限が決まっており、業務に関係する情報のみダウンロード権限がある。ダウンロード権限がある人の場合には、ダウンロードの際に毎回上長へ通知され、ダウンロードされた情報と同じものが上長へも送信される。また、いつどのような情報をダウンロードしたかを示すリストが作成され、それを上長がチェックする。
・また、個情報を電子メールで送信したり、外部記憶装置に移す場合には暗号化をすることが定められており、個人情報を暗号化する際に、どのような個人情報を暗号化したのかということについて上長に電子メールで連絡がいくようになっている。
・電子メーの本文や添付ファイルに個人情報が含まれるかどうかをチェックするシステムをつくり、個人情報が含まれるものを送信すると上長や個人情報管理責任者にメールが送信される。その際、暗号化しているかどうか上長が確認する。

図表　個人情報を含むアクションの管理者への通知（イメージ）



4-(1)-㉜【退職者にも Winny 対策を徹底】

（情報サービス業(アウトソーシング等)：約 2,700 人）

・キ社では、Winny などのファイル共有ソフトは、使用禁止。

・全従業者に対して、過去に持ち帰ったファイル等を削除することを指示し、本人の署名つきの確認書を取っている。

・退職者に対しては、過去 3 年間にさかのぼり、ファイル等を削除したことをチェックすることを依頼する文書を郵送し、やはり本人の署名つきの確認書を返送してもらっている。

4-(1)-㉝【個人情報を 3 種類の台帳で管理】

（製造業：約 26,000 人）

・サ社では、保有する個人情報をリスクが高い業務で扱う個人情報（台帳 A1）とリスクが高くない業務で扱う個人情報（台帳 A2）に分けて台帳管理している。また、顧客から委託を受けて管理している個人情報（台帳 B）については別途台帳を整備している。台帳の具体的な項目は、次表を参照のこと。

図表　台帳 A2 サンプル（リスクが高くない業務で扱う個人情報）

図表　台帳 B サンプル（顧客から委託を受けて管理している個人情報）

・台帳 A1 に載せる情報は、リスクが高い業務において扱う個人情報である。なお、これらの業務は、更にリスクレベルに応じて、a）信用情報・金融取引情報を継続的に扱うなど特にリスクが高い業務、b)メールマガジン送信のみを行う業務、c)それ以外の業務の三つに分類し、それぞれ管理について定めた細則に従って業務運営をしている。a）特にリスクが高い業務では、フォレンジック対応（アクセスログを記録する等のアクセスに関する証跡を残す仕組みの導入）にしている。また、データベースは別個に設置しており、情報毎にアクセス制限も設けている。

4-(1)-㉞【リスク分析の義務付けで、不必要な個人情報を大幅に削減】

（製造業：約 26,000 人）

・サ社では個人情報の台帳（A1, A2）に「リスク分析の実施の有無」という項目を追加設置したところ、個人情報の件数が 1 割以上減少した。それまでリスク分析は各事業部の裁量にゆだねているところがあったが、義務付けして台帳でチェックすることができ、必要以上に個人情報を所持することを抑止できるようになった。

・その一例として、ある部門での個人情報集約が挙げられる。当該部門は本来ならばデータベースはひとつでよいにも関わらず、「リスク分析の実施の有無」項目を追加以前は、部の複数の従業員が個人情報を保有していた。しかし同項目を追加したことで、リスク分析実施の負荷を回避するため、各個人が保有していた情報を集約しようという流れになった。

4-(1)-㉟【ツールの導入により台帳管理を効率化、高度化】（製造業：約 26,000 人）

・サ社では同社は各台帳（4-(1)-㉝及び㉞を参照）の管理を各事業部に任せている。このため、問題点を即時に特定し、色付けしてハイライト表示するツールを導入することで、各事業部内で問題把握が出来る仕組みを整えた。

・具体的には、リスクが比較的高くない業務で扱う個人情報を記録する台帳（A2）に信

用情報が含まれている場合、リスク分析がおこわなれていない場合、利用者の範囲が適切でない場合、利用目的が適切でない場合に、各項目が、赤や黄色でハイライトされる仕組みとなっている。
・台帳の各項目は自由記入ではなく、プルダウンによる選択式にして管理を効率化している。

4-(1)-㊱【グループ共通基準を作成。全社が順守すべき「必要対策」と各社ごとの「推奨対策」の二段階チェックにより、各社に最適なセキュリティ対策を実施】
（製造業：約 12,000 人）

・シ社では同社では、2007 年 3 月にグループ共通基準を策定している。共通基準では、情報資産を、ⅰ）情報コンテンツ、ⅱ）物理的資産、ⅲ）IT システム、ⅳ）サービス、ⅴ）協力組織に大別し、それぞれに業務上の重要性の程度によって、全社が順守すべき「必要対策」と、各社ごとに異なる「推奨対策」の二段階チェック項目を定めている。
・グループとして順守すべき「必要対策」については、各現場の情報資産管理責任者が当該情報資産に適用される要求事項・セキュリティレベルと現状の管理レベルを比較し、乖離の有無を確認しながらリスク評価し、リスク対応のための管理策を実施する。
・また、管理者のリスク評価・対応を簡易化するシステムを作成し、このシステムを活用することで、各社のセキュリティ活動の結果を統括部門に集約し、共通基準の評価・改善に役立てている。
・各社の業務特性によって任意に選択できる「推奨対策」については、同様の比較により、各現場の特性に合わせてリスク対応の必要性を判断することができ、さらに組織の機能・特色・状況によって順守すべき追加事項がある場合は、独自の管理策を付加することができる。

4-(1)-㊲【全社方針を元に機能毎に構成される本社統括組織が年度計画・セキュリティ対策を立案し、関連企業はその計画を元に運営する】（製造業：約 12,000 人）

・シ社では共通基準の運営は、過去に発生した事故を参考にしながら、IT 関連の専門部署が全社年度方針を立案し、それを元に各組織は活動計画を立てて実行する。
・業務内容によって共通基準が異なることから、国内販売機能統括、海外販売機能統括、生産機能統括、関連会社統括など、機能毎に分かれた統括組織が本社にある。各統括組織が年度計画・各業務範囲内のセキュリティ対策を立案する。関連企業や関連部門は、その計画を元に対応する。
・生産機能よりも販売機能の方が個人情報の取り扱いが多いため、販売機能は個人情報の取り扱いが厳格化されている。全社で足並みをそろえようとすると、活動計画についても差が現れるため進めづらいという苦労がある。

4-(1)-㊳【組織の成熟度に応じてレベル分けされた目標を指標に、本社内と関連会社内の二段階で年度目標を設定している】（製造業：約 12,000 人）

・シ社では全組織の目標設定は IT 関連の専門部署が行う。それとは別に組織毎に異なる目標値の設定も行っている。組織毎の目標設定は、国内販売であれば、販売事業本部の目標に国内販売会社が追加する形で目標設定する、といった形式をとっている。

・セキュリティの三要素（機密性・完全性・可用性）の中では、可用性を中心に目標設定を行っている。

・目標値は組織の成熟度に応じてレベル分けされている。同レベルは販売部門が作成したものであり、標準化されている。

4-(1)-㊴【組織の成熟度は、セルフチェックと内部監査を組み合わせて総合的に評価】（製造業：約 12,000 人）

・シ社では組織の成熟度は、セルフチェックと内部監査を組み合わせて総合的に評価している。

・セルフチェックは、各組織および個人が実施する。内部監査は、セキュリティ部門が客観的に評価する。

・セルフチェックと内部監査の結果をあわせて、全社レベルで評価する。この評価は 2005 年からおこなっている。

・業務内容によって目標レベルが異なるため、同評価は、組織の評価との連動はしていない。

4-(1)-㊵【ISMS の台帳に個人情報保護の項目を追加して情報資産と個人情報の管理を一体化して効率的に運用】（製造業：約 12,000 人）

・シ社では、従来、個人情報の管理とそれ以外の情報資産の管理を分けていたが、2007 年からは ISMS の台帳で個人情報の管理ができるようにした。

・個人情報特有のアセスメント項目を追加し、情報資産と個人情報の管理を一体化して、効率化を図っている。

4-(1)-㊶【ログ取得に注力し、有事に備えている】（製造業：約 2,000 人）

・ス社ではキーボードに至るまで資産管理、ログ取得の対象にしており、詳細に把握している。何かが生じたときに、どうして、どのように生じたのかをトレースできれば良いと考えており、そのためにログを詳細に取得することに注力している。

4-(1)-㊷【携帯電話のメール送受信の制限による漏えいリスクの低減と利便性をバランス】（製造業：約 2,000 人）

・ス社では携帯電話は、従来は営業については個人用携帯電話を使用させており、公用の電話のみ、電話番号の頭に特別な番号をつけるだけで、会社が通話料金を自動的に負担するという仕組みで運用していた。
・しかし、携帯電話の紛失によって、個人情報が紛失してしまうリスクが高いため、会社から携帯電話を支給する方式とした。
・支給に際しては、携帯電話からはメールの送受信ができないように設定（ロック）しており、携帯電話から通常のメールは一切できない。
・しかし、メールを全て禁止すると、顧客先を回っている営業の業務遂行には問題が生じるので、特別なアプリケーションを導入して、会社のメールアドレスで受信したメールを携帯電話で閲覧できるようにした。但し、閲覧しかできないようになっており、添付ファイルは見られないようになっているなど一定の制限を課している。
・また、安否確認をする場合のみ、メールが携帯電話に送信されるようになっている。安否確認のメールはサーバ上で「ホワイトリスト」に登録し、メールを送受信できるようにしている。
・上記の仕組みだと、会社に届いたメールを携帯電話で閲覧するためには、アプリケーションを起動しないとメールが届いているのかどうかすらわからないという問題があった。そこで、「件名」と「送信元」の情報のみの通知を携帯電話で受信できるようにカスタマイズして営業の利便性にも配慮した。
・携帯電話の紛失時には、携帯電話会社の汎用サービスであるメモリーの消しこみ、GPSによる携帯電話の所在確認を利用している。
・メールの保全が J-SOX 対応で必要であったこともあり、このような対応をした。
・どこに電話をかけたのかということは請求電話明細でわかるようになっているので、ログとしてチェックができるようになっている。
・携帯電話をかける際には、全社統一の番号を入力してロックを解除しないと、電話がかけられないようになっている。このロックは 1 分ごとに必ずかかるようになっている。これは携帯電話キャリアから求められた対応である。その面倒さに、当初は社員からも不平不満が出たが、1 ヶ月程度で慣れた。
・着信と同時に相手を識別できないと顧客である医師に対して失礼にあたる場合があるため、アドレス帳は使えるようにしている。その代わり、遠隔操作でアドレス帳を消去できるようにしている。公衆電話から自分の携帯電話に電話（規定回数）することにより、消去できる。

4-(1)-㊸【USB への書き出しは顧客ニーズに合わせ、限定パソコンで部長決裁の上で実施】（情報サービス業(ソフトウェア)：約 5,500 人）

・セ社ではパソコンから USB メモリへは暗号化した情報しか書き出せないようにしている。ただ、お客様のニーズもあるので、予め決められた一部のパソコンからは平文で

書き出せるようにしているが、このパソコンも情報管理対策本部が認定したものに限定し、使用する場合は、部長の許可が必要である。

・在宅勤務を認めているが、自宅で作業をする際には、自宅のパソコンを使用いても、自宅のパソコンの性能・利用環境とは切り離して、シンクライアントパソコンとして使用できるようにするための特殊な USB メモリも配布している。ただし、基本的には在宅勤務の場合には、会社で使用するパソコンとは別のパソコンを支給している。

・自宅パソコンの使用を選択した場合には、そのパソコンの点検も年に一度実施している。特殊なソフトを活用することで、パソコン内に問題のあるファイルや個人情報がないかをチェックしている。特定ソフトの使用チェックも行っている。この施策はパートナー会社にも実施をお願いしている。

・自宅パソコンについては個人の持ち物ではあるが、対策について強いお願いをしている。チェックを実施した上で、「何も異常は無かった」、「異常はあったが対処した」ということについて、確認書を作成し、押印した上で提出してもらっている。

4-(1)-㊹【個人情報等が含まれる書類の収納スペースを狭くすることで不要な個人情報等を削減】（情報サービス業(ソフトウェア)：約 5,500 人）

・セ社ではノートパソコン、個人情報や機密情報が含まれている関連書類については、帰宅時・外出時には専用に会社から支給する鞄へ格納して、施錠可能なロッカーに入れるようにしている。このロッカーの幅を非常に狭くしており、一定以上の文書が発生した場合には、電子化や共用のキャビネットを使うように指導したことで、不要な文書の削減（電子化）や保管コストの削減にも寄与した。

4-(1)-㊺【問合せデータベースは、独自 ID で個人を特定し、個人情報を不可視に】（情報サービス業（アウトソーシング等）：約 30 人）

・タ社では問い合わせデータベース検索において、同社が独自に発行する個人 ID を表記する仕組みとし、個人情報を一覧表示できなくしている。なお、以前は携帯メールアドレス一覧を表示していた。

・問い合わせ管理システムを導入し、細かな管理権限の制御を行えるようにし、必要最低限の内容のみ、共有できるようにした。

4-(1)-㊻【社員が使用している PC を専門チームにより監視】（情報サービス業(ポータル)：約 3,600 人）

・ツ社では教育以外に、社員が使っている PC を監視下に置き、どの URL を見ているか、ネット上にどういう情報を流しているかを把握している。

・法務コンプライアンス部に監視チームがあり、3～4 人で監視している。情報が漏えいした形跡があれば、社員は上長、派遣社員は派遣会社、委託先は、業務委託先にヒア

リングをおこなう。

4-(1)-㊼【退職予定者は、特に厳しく監視・管理】

（情報サービス業(ポータル)：約 3,600 人）

・ツ社では退職が予定されている社員に対しては、情報の持ち出しが起きないように厳しく監視している。

・退職日の手続きに工夫をしており、出社最終日は人事部への手続きのみをおこない、自席に戻ることができない仕組みとなっている。また、できるだけ早く本人の社員アカウントを停止するようにしている。

・社員が退職する際は、秘密保持に関する誓約書を取っている。誓約書は入社時・新たな役職に就く際も取っている。同誓約書の有効期限は特に設けていない。

4-(1)-㊽【データセンター内をセキュリティレベルに応じて区分し、区分ごとに色分けしたベストを職員に着用させている】

（情報サービス業(ポータル)：約 3,600 人）

・ツ社では顧客情報は特定のデータセンターに保管されており、同センターには警備員が配置され、金属探知機が設置されている。

・セキュリティレベルに応じて施設内の保管場所を区分している。職員は入場時に保管場所の区分ごとに指定された色のベストの着用が義務付けられており、区分を誤って入場している者がいないかを容易に判別できるようにしている。

・施設内には電話も印刷機も設置していない。顧客情報を一覧で表示できるようなツールや表は作成していない。

4-(1)-㊾【複数のサーバに情報を分散し、保管することで、よりセキュアな環境で管理】

（その他サービス業(印刷・広告：約 10,000 人)）

・テ社では、データを分割し、暗号化した上で、複数のサーバ上に分散して保管するアプリケーションを開発し、使用している。

・例えば、あるファイルを A,B,C に分割し、三台のサーバーにそれぞれ、「A と B」、「A と C」、「B と C」を保存する。すると一台のサーバから情報を復元することを防ぐことができるほか、 一台が毀損した場合でも、残り二台が健全であればファイルを復元することが可能となる。