シ．製造業　シ社

事業概要	電子機器製造		
従業員	約 12,000 人	プライバシーマーク取得	なし（グループ内の一部の会社で取得あり） ISMS　あり
保有個人データ件数	4,239 件の台帳を保有 10 万人超(海外現地法人含む)の社員情報を保有		

１．個人情報保護に関する概要

（１）保有する個人情報の件数、種類、利用目的

・個人情報を管理する 4,239 件の台帳を保有している。各台帳は管理者のみ閲覧可能であるため、各台帳が包含する個人情報保有数は分からず、総数は把握していない。

・従業員の個人情報は、国内ではグループ企業全体で 4 万人弱、全世界では 10 万人超(現地法人含む)である。

・個人情報の種類：事業活動に伴うお客様、社員の個人データ

・個人情報の利用目的：

(1) 商品、サービスに関する情報の提供及びご提案
(2) 商品、サービスの提供
(3) 代金の請求、回収
(4) 商品、サービスの企画及び利用に関する調査、アンケート等のお願い及びその後の連絡
(5) 統計資料の作成
(6) 資材購入、部品調達等の連絡及び問合せ
(7) 支払い、請求書の作成等の事務処理
(8) お問合せ内容についての対応状況の確認と対応品質の向上
(9) 採用活動、株主・退職者への連絡及び問合せ
(10) その他一般事務の連絡及び問合せ

・利用目的は事業毎に分けている。年に数度は見直している。

（２）個人情報保護担当部署

・IT ソリューション本部(社内情報システム部門内)、IT ソリューション企画センター、情報セキュリティ室（同社グループ全体の統括)。

（３）個人情報保護管理者の有無・位置付け

・各構築組織（ISMS の活動単位であり、グループで約 56 組織）毎に個人情報保護管理責任者を置いている。

・位置付けは、その構築組織での個人情報保護に関する最高責任者。

（４）認証取得の有無（時期）、認証の種類、その認証を取得した理由・効果

・毎年 12 月に ISMS グループ統一認証を取得している。

・グループ全体の情報セキュリティの取組を客観的な認証という形で実現することで顧客を始めとするステークホルダーに納得・信頼いただき、事業経営への貢献が図れる。

・ISMS は全社で取得している。2002 年から検討を開始した。個人情報保護法など法制度の変更、ISMS の規格化、情報紛失事故を発端に、CEO からのトップダウンにより、全社取得の検討を開始した。

（５）個人情報保護に向けた取組経緯

・2004 年 12 月に ISMS グループ統一認証を取得。

・2005 年 4 月 1 日から全面施行される個人情報保護法の対応として社長直轄組織である個人情報統括室を発足し、1 年 3 ヶ月間にわたって活動。

・個人情報統括室の活動を開始した当初、グループの各構築組織より個人情報保護全般に亘る質問や問合せが殺到し、対応に苦慮した。

・費用は、専従者 6 名と兼務者 4 名、計 10 名での約 1 年 3 ヶ月分の活動に要した額が相当する。

・2006 年 4 月に ISMS 推進統括組織と個人情報統括室を統合し、現在は社内情報システム部門内に位置付けられている。

（６）個人情報の保有・管理・提供等に関する業界の特徴

・OA 機器業界では、顧客の機微な個人情報は少ないものの、個人客の他に、企業や官公庁も顧客としており、保有・管理・提供等は頻繁に行われている。

・“情報”を扱っている業界であるので、個人情報の事故を発生させることは即会社の信頼を失うことであり、慎重で確実な対応が要求されている。

２．個人情報の適切な保護のための取組について

（１）準備（規程・体制づくり）

（社内の各機能分野から広く人材を集めて全社体制で推進。外部リソースも活用）

・社内の各機能分野（人事、法務、広報、販売、IT など）から広く人材を集め、個人情

報統括室を設置し、同室を中心とした全社体制で個人情報保護を推進した。

（２）個人情報の取得

・取得に関しては、その詳細をグループ共通基準として定め、更に別途、各構築組織の特異性を考慮した各社基準を適宜定めて対応している。また、棚卸時の基準としてグループ横断的な共通基準を設け、ISMS のリスクアセスメント時に棚卸を実施している。
・グループ基準はイントラネット上に掲載している。

（３）個人情報の利用（第三者提供を含む）

・利用目的はホームページ上に、事業毎に利用目的を記載している。
・詳細は「１.（１）保有する個人情報の件数、種類、利用目的」を参照。

（共同利用は、ホームページ上に、いつ・誰に・何を、提供するか明記）

・共同利用について、事業と利用目的との関係を明確に定めた上で、どのような共同利用者に対して、どのような情報を、どのような場合に提供するか、事業毎に整理してホームページ上に記載している。
・グループに新たな企業が加わった際は、オプトアウト方式で共同利用をするため、“承継前にご本人に同意を得ている、または通知、または公表した利用目的の達成に必要な範囲内で利用する”とホームページ上に記載している。

（４）個人情報の管理

①情報の管理体制

（グループ共通基準を作成。全社が遵守すべき「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）

・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、全社が遵守すべき「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。

（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）

・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 ソリューション本部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たて実行する。
・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。

（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）

・全組織の目標設定は IT ソリューション本部が行う。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。

（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）

・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。

（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）

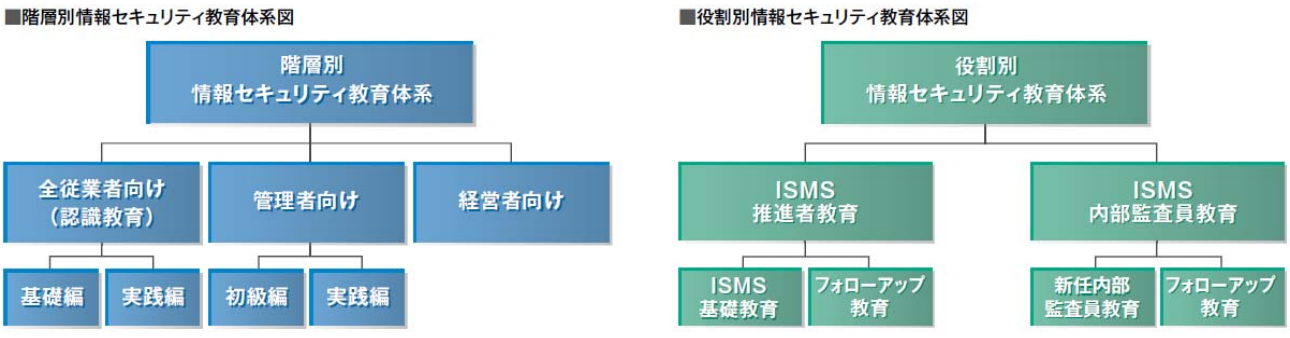
・以前は個人情報の管理とそれ以外の情報資産の管理は分かれていたが、2007 年から ISMS の台帳で個人情報の管理ができるようにした。
・効率化を図るべく、個人情報特有のアセスメント項目を追加し、情報資産と個人情報の管理を一体化して運用している。

②従業員への教育方法

（階層別・役割別に教育を実施。全従業員が基礎知識と実践知識を身に付けるよう教育）

・社内規定はグループ基準、各社基準を中心としたもので整備されており、周知徹底のための各種階層別教育が整備されている。
・階層別教育と役割別教育を行っている。階層別教育は、経営層・管理層・全従業員の三つに層別して情報セキュリティ教育を行っている。
・基本的には、毎年 1 度は全従業員が受けることを義務付けている。全従業員向けでは、情報セキュリティとは何か、および業務情報を取り扱うにあたっての基本的な行動ルールを教育し、更に、理解度確認のため試験を行っている。また、全従業員向けと管理者向けにはそれぞれ、基礎編と実践編がある。
・教育ツールは基本的には e ラーニングを導入しているが、製造現場は紙で教育をおこなっている。
・役割別教育は、ISMS 推進者・内部監査員に対して、それぞれ基礎教育とフォローアップ教育を行っている。具体的な事例や PDCA の管理プロセスが組織に浸透していくことに焦点を当てた教材を開発し、教育をおこなっている。教育実施後は、受講者アンケートを分析・評価し、教育プロセスの改善を図っている。

図表　教育体系



③盗難対策

（IC カードによるプリント出力認証、印刷ログ管理、業務内容に応じた複合機の利用制限を実施）

・IC カード(社員証)を、社内の入退室管理、PC へのログイン、プリント出力時の認証に適用している。

・この IC カードを活用し、業務内容に応じた複合機の利用機能制限、ログ管理を行っている。

・紙文書を PDF 化する際、全従業員の権限に応じた閲覧・印刷のアクセス権を付与して暗号化することで、共有文書の情報漏えい防止を図っている。

④ノート PC の安全対策

・メールはサーバ側にコピーを保存している。

・その他のファイルは、拡張子をリスト登録しておき、有事の際にどのようなファイルが PC に格納されていたのか説明できるようにしている。

・前出のグループ基準・各社基準での規程を始め、共通基準での各種管理策の徹底、適宜発信するグループ全従業員向け通達、ノート PC 類の持出し管理データベースでの管理、部門毎の個別教育ツールなどで対応している。

・ノート PC を持ち出す場合は、申請が必要で、持出し管理 DB での管理を義務付けている。ノート PC を持出し禁止としている部門もある。

・持ち出す場合は、ハードディスクのパスワードの設定や、重要情報持ち出し時の暗号化ソフトの使用、返却時と併せてのパソコン内データの確認を義務付けている。これらはグループ会社では徹底されている。

・携帯電話の管理も課題である。現在では、個人を特定できないような登録を促すほか、キーロック機能・リモート消去機能付き携帯電話の購入を推奨している。また、携帯電話紛失時は、同社内のヘルプデスクを通じてキャリアに連絡がいき、データをリモート消去する体制を構築している。

⑤外部委託先管理

・基本的には契約で個人情報の管理について規定している。

・外部委託先には個人情報の取り扱いを制限している。社外からの閲覧はさせない。社内において USB メモリの書き出し制限を課している。

・委託先の格付けは、行っている組織もあれば、行っていない組織もある。

・立ち入り検査は一部では行っている。請求書の配送業者など、個人情報を渡さざるを得ない業者には、適宜同社が直接監査を行っている。

⑥日常点検・確認の方策

・特徴的な取り組みはなし

⑦初歩的ミスの防止

（三つの予防策で電子メールの誤送信を抑止）

・メール誤送信を抑止するため、メールソフトをカスタマイズして誤送信を 3 つの方法で抑止している。

・ⅰ）すべての宛先の表示と確認：　電子メールソフトで、送信ボタンを押すと宛先表示画面が表示され、宛先が漢字で表示される。宛先の間違いがないかを再度確認させる。

・ⅱ）社外メールでファイル添付する場合の暗号化の確認：　社外へメールを配信する際に添付ファイルがある場合、暗号化したかどうかを確認する画面が表示される。

・ⅲ）社外ドメインの確認：　メールの宛先に社外のドメインが含まれている場合、その旨を告知して再確認を促す。

（５）個人情報の消去・破棄

・前出のグループ基準と各社基準にその対応方法を明記している。また、全従業員向け各種教育等で繰り返し啓蒙しており、必要な装置としてのシュレッダーや廃棄箱等は各職場に完備している。

・リサイクル用紙・シュレッダー・溶解などの分別を各職場で徹底している。個人情報が入っているものはシュレッダーで処理している。

・パソコンの廃棄については、ディスク消去を行った上で、米国国防総省推奨方式でデータを消去して証明書をとる、若しくは、物理的に破壊すること、どちらかを義務付けている。

（６）個人情報の監査

・ISMS での内部監査、外部審査時に個人情報の監査も実施しており、日常的な点検は各部門の個別教育ツールや昼朝礼での注意喚起等で対応している。

（７）苦情処理・顧客対応

・原則としてグループ全体のお客様対応窓口を一本化し、社内の処理ルートを定め、対応には専門部隊があたって苦情処理や顧客対応をしている。

（８）事故発生時の対応

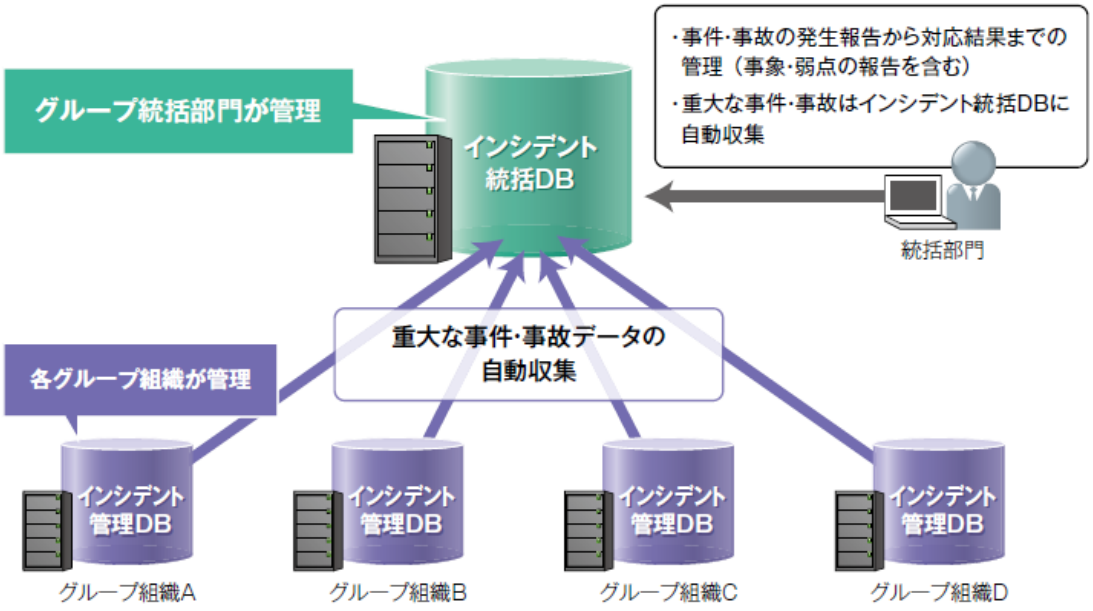
（事件・事故の発生報告から対応結果までの管理と重大な事件・事故の報告を自動化）

・インシデント管理データベース：　グループ各組織は、事件・事故の発生報告から対応結果までの管理と、事象・弱点を報告できるツール「インシデント管理データベー

ス」を使い、事件・事故情報を共有している。また、報告者に対策納期遅れを自動で知らせるエージェント機能を付加するなど各種の工夫を加えている。これにより事件・事故対応の迅速化、情報の共有化、各組織でのツール維持のための負荷軽減などの利点がある。機微情報が入っていることから、各管理データベースは各部門の、報告過程にいる人と、各組織の ISMS 担当者のみしか閲覧できない。

・インシデント統括データベース：　グループ各組織のインシデント管理データベースに報告された事件・事故のうち、特に重要な事件・事故については、リアルタイムにインシデント統括データベースに反映される。重要な事件・事故は、例えば「社外秘以上の情報を格納した USB メモリ、パソコンなど電子媒体の紛失・盗難事件・事故」のように定義されている。グループ統括部門は、重大な事件・事故に対して、原因分析と暫定対策、恒久的な再発防止策、予防策を検討し、グループ各組織にフィードバックしている。

図表　インシデント管理 DB によってグループ全組織の事件・事故の報告管理方法を統一



以上