紹介

KYBにおける技術情報漏えい防止活動の取り組み

佐　藤　晃　彦

1　はじめに

昨今，新聞やニュースで，故意による個人情報の流出やサーバへの不正アクセスによる仮想通貨の流出など，情報漏えいに関する事故が多く報じられている．もし，KYBで情報漏えい事故が発生し，新聞やニュースなどに取り上げられた時，お客様や取引先様にご迷惑，ご心配をおかけする事態になり得る．

本報では，当社が取り組んでいる技術情報漏えい防止活動について紹介する．

2　本活動の背景

近年，IT化の進展，工場の海外進出，外部からの不正アクセスや内部関係者による不正な情報の持出しなど，情報を脅かすセキュリティリスクは多岐にわたっている．当社においてもパソコンや携帯電話などの紛失による社外へ情報が漏えいする可能性が懸念される．

企業は様々な機密情報を取り扱っているが，製造業である当社は，大半が技術的な情報が書かれた資料（以下技術情報）を扱っている．技術情報は，「当社の技術的優位性を保つために有効で，関係者しか知り得ない技術的な情報」である．これは，関係者以外に非公開で，全従業員が会社として職場として守るべき情報である．

もし，技術情報の流出が発生した場合，お客様や取引先様からの信用失墜につながりかねない．更に，競合会社に対する競争力の低下を招く重大な事象となる．本活動は，国際規格であるISO27001に則り実施しているため，技術情報以外の個人情報や営業情報など当社が保有している全ての企業秘密に適用することができる．

3　ISO27001の概要

3.1　ISO27001の特徴

ISO27001は，当社で認証を取得しているISO9001（品質マネジメントシステム）やISO14001（環境マネジメントシステム）と同様のマネジメントシステムの規格である．ISO27001にもISO9001，14001と同じくPDCAサイクルの構築，適用範囲の決定，リーダシップの関与，文書化の要求事項が定められている．しかし，ISO9001や14001との違いは，本文である要求事項の他に，情報セキュリティを実現するうえで必要な運用の具体的方策が，詳細管理策の附属書Aに示されている（図１）．

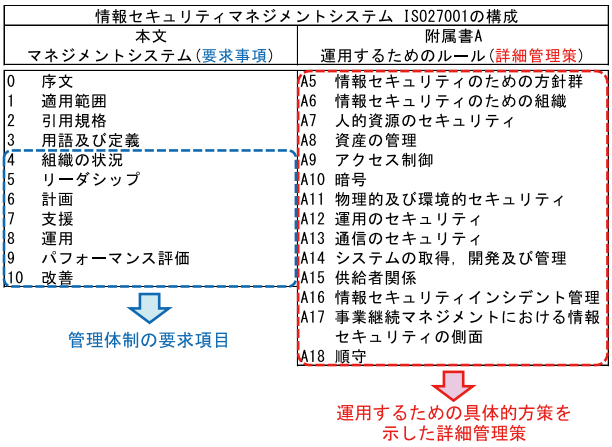

図１　ISO27001の構成

情報セキュリティとは，情報の機密性[注1)]，完全性[注2)]及び可用性[注3)]を維持しなければならないとISO27000：2014に定義されている．

注１）機密性：情報を許可されていない第三者へ漏らさない，触れさせないこと

注２）完全性：誤った情報にしない，させないこと

注３）可用性：使いたいときにすぐに情報を使えるようにすること

3.2　情報セキュリティマネジメントシステム

情報漏えいリスクに対して，効果的かつ，効率的

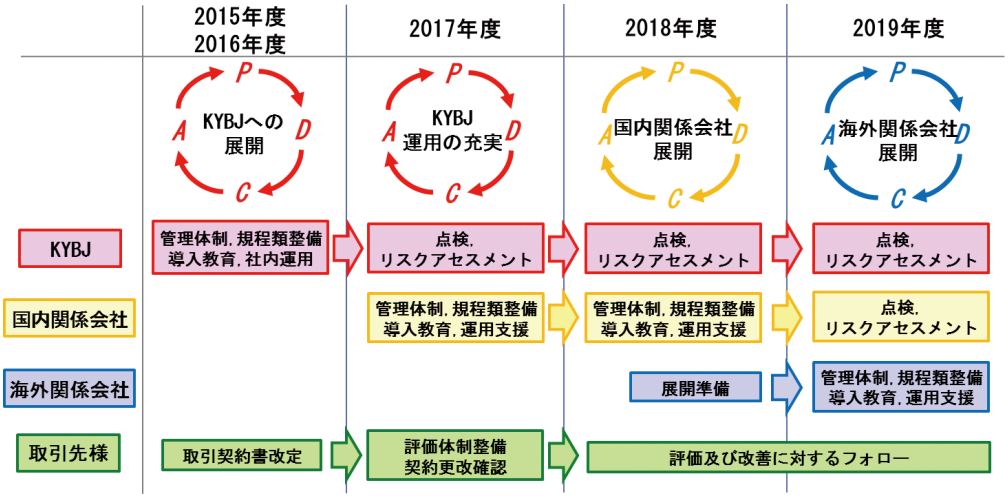

図２　KYBグループ各社への展開概要

に対処するためには，組織で情報セキュリティマネジメントシステム（以下ISMS[注4)]）を導入，構築することが不可欠である．これを具体的に言うと，会社として企業秘密を守ることを宣言する企業行動指針，PDCAサイクルを実行するための組織と仕組みを構築し，情報漏えいが発生しない状態を維持するために，ルールに従い運用を行い，適正に運用されているか定期的に確認，改善を実施し，新たなリスクの評価と対応をしていくことで，継続的に情報セキュリティのレベルを向上させることである．

注４）ISMS：Information Security Management System

3.3　情報セキュリティ体制を構築する要求事項

ISO27001の要求事項は，図３に示すように組織がPDCAサイクルを実行するためには何をするべきか示されている．

4 組織の状況
4.1 組織及びその状況の理解
4.2 利害関係者のニーズ及び期待の理解
4.3 情報セキュリティマネジメントシステムの適用範囲の決定
4.4 情報セキュリティマネジメントシステム
5 リーダーシップ
5.1 リーダーシップ及びコミットメント
5.2 方針
5.3 組織の役割、責任及び権限
6 計画　*Plan*
6.1 リスク及び機会に対処する活動
6.1.1 一般
6.1.2 情報セキュリティリスクアセスメント
6.1.3 情報セキュリティリスク対応
6.2 情報セキュリティ目的及びそれを達成するための計画策定
7 支援
7.1 資源
7.2 力量
7.3 認識
7.4 コミュニケーション
7.5 文書化した情報
8 運用　*Do*
8.1 運用の計画及び管理
8.2 情報セキュリティリスクアセスメント
8.3 情報セキュリティリスク対応
9 パフォーマンス評価　*Check*
9.1 監視、測定、分析及び評価
9.2 内部監査
9.3 マネジメントレビュー
10 改善　*Act*
10.1 不適合及び是正措置
10.2 継続的改善

※1から3は本規格の適用範囲、引用規格、用語及び定義が記載されている．

図３　ISO27001要求事項の構成

3.4　情報セキュリティを運用するための管理策

附属書Aの詳細管理策は，組織が情報セキュリティを実現するために，組織的，人的，物理的，技術的な観点[1)]から自社の管理策を決定し，実施するための具体的な方策が示されている．

⑴組織的安全管理策

技術情報に対して，従業員の責任と権限を明確に定め，規程類や手順書を整備，運用し，その実施状況を確認し，必要に応じた改善を行うことである．

⑵人的安全管理策

従業員に対して，秘密保持契約の締結や教育，訓練を実施することである．

⑶物理的安全管理策

社屋や事務所への入退館（室）の管理，外部からの侵入による盗難防止などの措置を行うことである．

⑷技術的安全管理策

技術情報や，それを取り扱う情報システムへのアクセス制御，監視など技術的な対策を行うことである．

4　当社の技術情報漏えい防止活動

図２に示すように当社では本活動を2015年度から開始した．活動は当社国内拠点（本社，支店，各工場）を皮切りに，国内関係会社，海外関係会社の順に展開を進めている．また，当社の取引先様に対しても情報漏えい防止活動の展開を行っている．本活動の構築は表１に示す順で行う．

表１　本活動の構築

⑴	方針と活動体制の整備
⑵	決まりごとの構築と遵守の徹底
⑶	従業員教育体制の構築
⑷	決まりごとに基づいた運用とその確認
⑸	新たな脅威への対応とISMSの有効性評価
⑹	取引先様管理体制の整備と運用

4.1　方針と活動体制の整備

⑴方針の整備

技術情報漏えい防止活動を当社として取り組む姿

勢を社内および社外へ示すために，最上位の方針として，「技術情報セキュリティ方針」を整備した．

⑵活動体制の整備

技術情報漏えいに対する従業員の意識を高め，会社全体で活動を行うために，当社では図４に示すように技術情報管理組織を構築した．

技術情報管理委員会は，本社機能部門，各工場，国内関係会社から選出された委員で構成されている．

活動推進キーマンは，各部門から選出してもらい，部門への本活動の展開，啓蒙活動を行っている．

監査責任者と内部監査者は，独立性を担保するために技術情報管理委員会から独立した者を選出する．

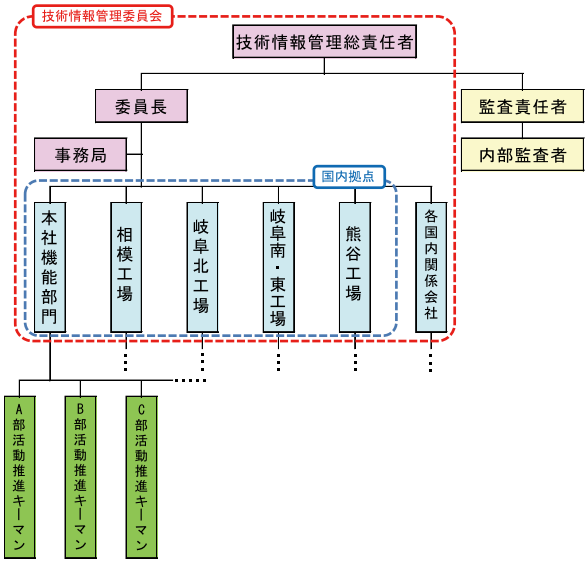

図４　技術情報管理組織

4.2　決まりごとの構築と遵守の徹底

当社で扱う技術情報の定義を行い，会社として，職場として遵守するべき技術情報取扱のルールを整備した．更に，ルールを違反した際の罰則を周知し，遵守を徹底した．

⑴技術情報漏えい防止規程類の整備

当社では，ISO27001の要求事項，詳細管理策（附属書A）と社内規程類を確認し，ISOに対応できていない部分に対して規程類の整備を実施した．

実施内容としては技術部門では，技術情報の管理体制についての規程と技術情報の取扱規則を制定し，その他機能部門である法務，総務，人事，IT部門では規程類を確認し，修正，追加を行った．

⑵従業員や退職者からの漏えい防止の徹底

当社入社時に，新入社員へ社内の秘密を保持し，第三者に漏えいさせないこと，及びルールに違反した場合には罰則が適用されることを誓約書などで合意していることを確認した．

また，退職者からの情報漏えいを防止するために，技術情報の返却と，退職後に当社の情報を漏えいしないことが記載されている誓約書への記入を確認した．

4.3　従業員教育体制の構築

⑴技術情報漏えい防止の基本的な考え方

自らが所有している技術情報を誰に対して伝える必要があるのか，誰から技術情報を隔離する必要があるのか，もし技術情報が漏えいしたときにどのような影響を及ぼすのかを考慮した上で，運用方法を決める必要がある．

⑵従業員向け教育内容の検討

前述の基本的な考え方に基づき，従業員が当社の技術情報を漏えいさせないように意識を高め，決まり事を理解，遵守してもらうために，技術情報漏えい防止規程類に従い，「技術情報保護９つのルール」を定義した（表２）．以下に各項目の実施目的とポイントを記載する．

表２　技術情報保護９つのルール

項目	内容
①	発行部門と受取部門の義務
②	機密分類および識別表示
③	技術情報の開示および回収管理
④	可搬記憶媒体の管理
⑤	持ち出し管理
⑥	クリアデスク・クリアスクリーンの実施
⑦	技術情報の保管・保存
⑧	技術情報の消去・廃棄
⑨	技術情報の流出が発覚したときは

①発行部門と受取部門の義務

技術情報を取り扱う役割に応じて，実施事項を明確にするために，文書を発行する人（部門）を「発行部門」，文書を受け取る人（部門）を「受取部門」として，それぞれの役割での実施事項を定義した．また，文書を他部門へ再配付する時に発行部門に確認することを明確化した．

②機密分類および識別表示

作成した技術情報を全ての従業員が同じように取扱を行えるようにするために，作成する文書に機密レベル，開示範囲により「社外極秘」，「関係者外秘」，「社外秘」，「公開情報」と機密分類を明確化し，文書に表示するように定義した．（表３）

③技術情報の開示および回収管理

社内，または社外関係者に開示した技術情報の所在を明らかにするために，技術情報を配付する

表３　識別表示と開示範囲

識別表示	開示範囲
社外極秘	当社内でも特に限定された従業員
社外秘	当社全従業員
関係者外秘	当社内関係者，秘密保持契約を締結した当社外関係者
公開情報	全ての者

時は配付先の記入を行うようにした．また，社外に配付した技術情報の配付・回収管理を徹底するようにした．

④可搬記憶媒体の管理

可搬記憶媒体から，意図せずに技術情報が流出することを防止するために，USBメモリなどの可搬記憶媒体の使用を原則禁止，個人所有のUSBメモリの使用を禁止した．また，やむを得ず使用する時は会社が許可したUSBメモリのみ使用することができることを明確に定義した．

⑤持出し管理

技術情報を社外へ持ち出した時に情報漏えいを防止するために，添付データがある電子メールを社外の関係者へ送付する時のパスワード付加や，社外の輸送業者を使い重要文書や試作品などを送る時の実施事項を定義した．

⑥クリアデスク・クリアスクリーンの実施

関係者以外に情報を不用意に見られないようにするために，従業員が帰宅，外出する時は，技術情報が記載されている書類を机上に放置しない，パソコンはシャットダウンすることを定義した．

⑦技術情報の保管・保存

保管，保存されている技術情報の盗難，紛失を防止するために，電子データや書類などの紙媒体など異なる形態の情報を，機密分類に基づき適切な場所と方法で保管，保存することを定義した．

⑧技術情報の消去・廃棄

技術情報を確実に廃棄，再利用できないようにし，漏えいを防止するために，作成した技術情報を廃棄時に情報を読み取られないようにシュレッダなどで破砕，破壊処分を行う．また，社外に廃棄を委託する場合は，廃棄証明書を取得するように定義した．

⑨技術情報の流出が発覚したときは

万が一技術情報漏えい事故が発生した時の対応を正確，かつ迅速に行い，同様の事故を再発防止するために，事故発生時は速やかに上司と事務局へ報告するようなルールを定義した．

⑶従業員教育の実施

前項で定義した，「技術情報保護９つのルール」を従業員へ周知，徹底させるために，当社に従事する全従業員へ教育を実施した．教育の方法は表４に示す方法で行い，ルールを周知徹底した．

表４　従業員への教育方法と対象者

教育方法	対象者
事務局が講義	活動推進キーマン， 定期採用新入社員
eラーニング	【PC環境あり】 幹部従業員，一般従業員， パート従業員，派遣従業員
紙資料（抜粋版）配付	【PC環境なし】 一般従業員，パート従業員， 派遣従業員
契約時誓約書の読み合わせ	日本語が理解できない外国人従業員
各工場人事部門から資料配付	中途採用従業員，不定期採用パート従業員，派遣従業員

4.4　決まりごとに基づいた運用とその確認

「技術情報保護９つのルール」が，各部門で実施されているか運用状況を確認するために，定期的に部門へ点検を実施している．点検は，情報の取扱状況について事前に被点検部門の活動推進キーマンが職場の点検を行い，その結果に基づき監査者は実際に事務所などの現場に出向いて取扱状況の点検を実施する．もし，不適合事項や改善の機会が抽出された場合は，被点検部門は速やかに計画を立案し，改善を実施する．その中でも情報漏えいリスクが高く，不適合事項があれば，改善後に監査者による再点検を実施することもある．

4.5　新たな脅威への対応とISMSの有効性評価

⑴新たな脅威への対応

ルール運用時に，環境の変化による脅威や新たなリスクとなり得る項目を抽出して対応するために，リスクアセスメントを実施している．もし，新たなリスクが抽出された場合は，事務局でリスクに対して評価を行い，リスクを低減させる対策を行う．

⑵ISMSの有効性評価

会社として技術情報漏えい防止活動が有効に機能しているか，有効性評価と呼ばれる手法を用いて評価を実施している．有効性評価は，本活動を行う中で過不足（やりすぎな部分，足りない部分など）は無いか，ISMSの運営に対する課題は無いかなどを抽出することである．これにより次年度以降に

ISMSが有効に機能していることを確認でき，部門での効率的な運用へつなげていくことができる．ここで課題が抽出された場合，有効に機能するように当社のISMSの改善を行う．

4.6　取引先様管理体制の整備と運用

図面や技術情報を開示している当社の取引先様から情報漏えいが発生しないように，取引先様にも技術情報漏えい防止活動の展開を行っている．これにより取引先様から情報が漏えいするリスクを低減させることができる．

⑴取引基本契約書の改定

既存の取引契約を確認し，情報保護の項目などに一部不足部分があったので契約書の改定を実施した．

新規取引先様は改定した契約書で契約を行い，既存の取引先様は改定部分の覚書の締結を行った．

⑵情報の取扱状況に関する調査

当社取引先様の情報の取扱状況を把握するために，「機密情報の取扱に関する調査票」を取引先様へ配付し，調査を実施した．この調査票で判定点が芳しくない取引先様に対しては，指摘と改善を依頼した．

5　おわりに

本活動を通して，従業員に当社の保有する技術情報が重要な財産であることを伝えることができた．2016年度より全従業員に対して教育を実施してから，現在のところ重大な情報漏えい事故は発生してなく，本活動が効果的に機能していると考えている．

今後は本活動を海外関係会社にも展開し，当社グループから情報漏えい事故を発生させないように引き続き活動を継続していく．

参　考　文　献

1）個人情報保護委員会：個人情報保護に関する法律についてのガイドライン（通則編），pp 88-98，（2019年１月）．

著　者

佐藤　晃彦

2008年入社．技術本部技術企画部技術標準化推進室．基盤技術研究所，電子技術センターを経て現職．技術情報漏えい防止推進業務に従事．