

2012年度活動報告と2013年度活動計画

1.2012年度活動報告概要

ワークスタイルの変革をキーワードとして、業務プロセスやオフィス環境、個々の従業員の行動などが大きく変わってきています。スマートデバイスの活用、クラウドサービスの普及や定着など、新たな利便性は新たなリスクを生み出しています。これらの情報セキュリティの機密性と可用性の両立を、ITによるセキュリティ対策の組み込みと運用方法の改善により推進しています。

リコーグループは社会環境への変化に対し、ルールとしてのリコーグループ標準や情報セキュリティ対策共通基準の改訂、eラーニングによる教育、内部監査による確認と是正など、PDCAマネジメントシステムを回し情報セキュリティレベルをスパイラルアップしています。

2.グループISMS(ISO27001)統一認証の維持

グループISMS(ISO27001)統一認証の継続審査を受け、ISMSの認証を継続しました。

以下の組織が新規拡大審査を受け、統一認証に加わりました。(国内22社、海外47社、計69社)

- ・国内 リコープロダクションプリントソリューションズ・ジャパン株式会社
- ・海外 Ricoh India Ltd. Ricoh UK Products Ltd.

情報セキュリティのマネジメントの適切な運用が確認されました。

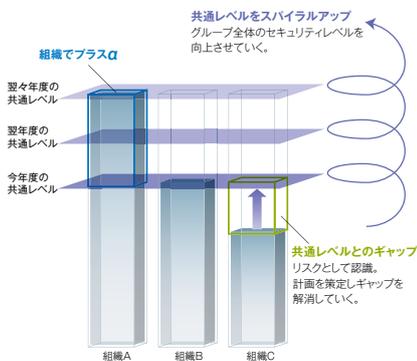
2013年度の活動計画

2004年度に統一認証を取得し、3年ごとに更新してきました。2013年度は3回目の更新審査を受審し認証を継続します。新しいワークスタイル、クラウドサービスの普及と定着、スマートデバイスの活用など、10年にわたる認証の更新と継続は、環境の変化や技術革新への継続的な取り組みの成果です。

3.「情報セキュリティ対策共通基準」の継続的改善と展開

情報セキュリティ対策共通基準は、「グループ全体のセキュリティレベルの確保」と「リスクアセスメントの最適化」を狙っています。情報の移送・送信・持ち出しなど情報資産の特性別に、日常的な取扱いに関する管理項目をまとめベースラインとしています。新たな脅威や、新たなIT機器の普及に応じて、継続的改善を進めています。

2012年度は、実質的セキュリティの強化と業務の効率化を図りました。暗号化などITによるセキュリティ対策の組み込みとこれに伴う情報持ち出し手続きの廃止や簡略化による運用負荷の軽減を推進し、機密性と可用性を向上させました。



2013年度の活動計画

新しいワークスタイルに対応した情報セキュリティ対策共通基準を、使用現場とともに策定しグローバルに展開します。また、情報セキュリティ活動の有効性を高め、情報活用の上昇のために、IT技術の実装と運用方法の両面から改善を推進します。

4.リコーグループの事業継続計画・管理の拡充

当初、リコーグループのビジネス特性からお客様設置機器を継続してご活用いただくため、画像ソリューション事業における「サプライ供給と保守サービス」をBCM^{*1}の対象としていました。

2011年度以降、東日本大震災での経験をふまえ、BCM検討の対象事業分野を見直し、設計・開発、生産・調達、販売など、すべての事業分野に拡大し活動しています。具体的な活動プロセスの質、量、および地域もこれに伴い拡大しました。

2012年度、ITシステム関連では以下を実施しました。

- ・ 想定リスクの見直しとBCM検討対象事業分野の拡大に合わせたITシステム対応計画の策定・実施
- ・ IT要員の行動に必要な関連ドキュメントの整備
- ・ IT要員の行動手順の定着と訓練

2013年度、ITシステム関連の活動計画

引き続き、防災対策、事業継続計画の両面から改善・拡充に取り組んでいきます。

- 防災対策 — 災害を想定し、被害をできるだけ小さくする対策
- 事業継続計画 — 重要業務を継続するための計画と準備
- ・ 従来の活動の振り返りと官公庁などから公表される被害想定の変化にもとづく、災害対策データセンターの考え方などのIT-BCP^{*2}基本方針の見直し
- ・ IT要員への行動手順の定着を目的とした継続的な訓練と、訓練を通じた課題の抽出、改善策検討

*1：BCM(business continuity management)事業継続マネジメント

*2：BCP(business continuity plan)事業継続計画

5. 情報セキュリティへの意識向上に向けた教育の継続

リコーグループの全従業員を対象とした教育を実施しました。

ISMSに関する方針、セキュリティ施策の周知と日常のセキュリティ習慣の定着を狙った行動の確認に加え、

- ・ 標的型攻撃など世の中で最近発生している事件・事故への日常の対応策
- ・ ソーシャルメディアへの情報公開の範囲や著作権などのルール

についての最新情報を提供しました。

国内リコーグループでは、eラーニングサイト「知識の天窗」を利用し、約4万人が教育を受講しました。

2013年度の活動計画

リコーグループの全従業員を対象に、情報セキュリティ方針や施策、日常の順守事項の確認のための教育を継続します。また新しいワークスタイルにともなう技術革新の利便性と情報セキュリティの脆弱性、その機密性と可用性の両立など、以下を重点化します。

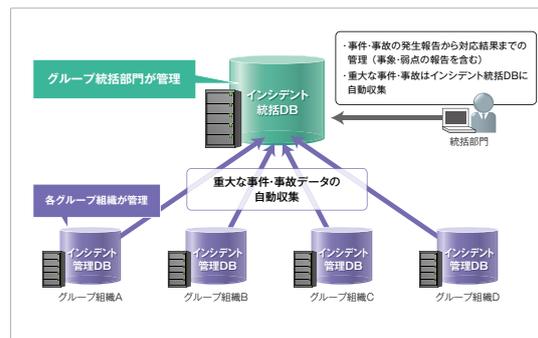
- ・ ITの進化に伴う新しい分野のルールの徹底
例: スマートデバイスの活用ルール、ソーシャルメディアルール、クラウド利用ルールなど

6. IT活用による情報セキュリティ事件・事故の再発防止

2012年度、外部への発表、審査機関や監督機関に報告を要する重大な事件・事故はありませんでした。

以下のステップでマネジメントシステムを回し、事件・事故の予防と再発防止に取り組んでいます。

- (1) 事件・事故情報とその再発防止策のグループ内共有は、継続して実施しています。
- (2) パソコンや外部記憶媒体の紛失など、日常発生しがちな事件・事故については、情報セキュリティ教育に取り入れ、再発防止策の周知・徹底を図りました。
- (3) 事件・事故情報や教育での徹底事項は、情報セキュリティ内部監査での重点監査項目とし、グループへの徹底と改善を推進しました。



2013年度の活動計画

引き続き重大な事件・事故の発生ゼロが目標です。

軽微な事件・事故は再発防止を図り、かつ重大な事件・事故に至る予兆ととらえ未然防止を図ります。

引き続き、教育の仕組みや内部監査の仕組みと連動し、事件・事故情報を提供し、再発防止と予防処置の有効性を追求します。