2013年度活動報告と2014年度活動計画

1.2013年度活動報告概要

2013年度はサイバー攻撃、特に企業などの情報システムを狙った「標的型攻撃」が大きな脅威となりました。リコーグループにおいても、関連会社のサイトが改ざんされ、お客さまにご迷惑をおかけする結果を招いてしまいました（「6.T活用による情報セキュリティ事件・事故の再発防止」参照）。
ワークスタイルの変革をキーワードとして、社内SNSの導入による業務プロセスの改革が進められ、オフィス環境、個々の従業者の行動などが大きく変わりつつあります。利便性の追求は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を伴い、新たなリスクを広範囲に生み出しています。これらの情報セキュリティの機密性と可用性の両立を、情報セキュリティ対策共通基準の改訂と周知、およびITによるセキュリティ対策（例:持ち出しパソコンのハードディスクフル暗号化の推進）の組み込みと運用方法の改善により推進しています。

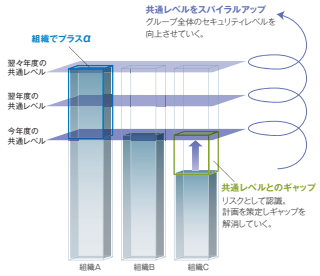
リコーグループは社会環境への変化に対し、ルールとしてのリコーグループ標準や情報セキュリティ対策共通基準の改訂、eラーニングによる教育、内部監査による確認と是正など、一貫性のあるPDCAマネジメントシステムを回し情報セキュリティレベルをスパイラルアップしています。

2.グループISMS（ISO27001）統一認証の3回目更新

リコーグループは2004年12月にグループISMS（ISO27001）統一認証を取得しました。以降、外部審査機関による1年ごとの継続審査、3年ごとの更新審査を受審し、認証を継続しています。
3回目の更新審査を2013年度に受審し、2014年度は認証を継続します。
国内19社、海外47社、計66社が認証を取得しています。（2013年12月）
国内外ともに、新たに認証に加えた組織はありませんでした。
認証範囲については、認証機関作成の「リコーグループ認証範囲 / Ricoh Group Registration Scope」を参照してください。
http://www.bsigroup.com/ja-JP/ISO27001/ricoh/

2014年度の活動計画
2014年度は継続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。
またISO/IEC 27001/2013（JIS Q 27001/2014）に移行します。

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」を狙いとしています。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。

2013年度はISO/IEC 27001:2013（JIS Q 27001:2014）が改訂され、情報セキュリティ対策共通基準もこれに対応し整合性を確保しました。

改訂内容の多くは、リコーグループISMSが従来から進めている施策と合致するものでした。たとえば「5.1b)組織のプロセスへのISMS要求事項の統合」は「特別に意識しなくても、あたりまえにセキュアな行動が取れる組織体質をめざす（情報セキュリティ体質）」という業務と一体化した情報セキュリティ活動によって認証取得当初からすでに対応済みです。

一方、新たな技術への取り組みとしては「業務のクラウドシステム利用要求」に応える基準を盛り込みました。技術革新の目覚しい分野のため、細かい規制をかけずに利用部門とシステム運用部門で検討を重ね適切な構築・運用を進めることとしています。

2014年度の活動計画

2013 年から、グループでは 「新しいワークスタイルへの変革」への取り組みが始まりました。 この試行経験を踏まえ、 新しい取り組みを支える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、 情報活用の自由度を上げるために、 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

リコーグループにおけるガバナンスとして、リスクマネジメントの詳細が公開されました。「リコーグループのBCP（事業継続計画）」に関する詳細は以下を参照してください。

http://www.ricoh.com/ja/governance/risk.html

ここではITインフラにおける事業継続計画・管理に焦点を絞り活動内容を報告します。

2013年度は、訓練の実施やその結果による改善など、事業継続計画の基盤を盤石なものとしてより具体的な施策を展開しました。これは継続してPDCAを確実に回していくフェーズに移行した結果です。

(1)2013年度に実施した訓練

以下の訓練を実施しました。

	訓練内容	訓練結果のフィードバック
1	有事の際の初動対応訓練（被災状況確認、災害対策本部設立判断など）	訓練後、参加者から手順や手順書の記載内容に関する意見を聴取し、手順書に反映し改訂しました。
2	有事の際のシステム稼動確認訓練	確認手順の有無確認および、手順書に課題が無いかの検証を行い、必要に応じて手順の作成、改訂を依頼しました。
3	国内関連会社（リコージャパン（株））のIT部門との初動対応連携訓練	初動対応で想定された連携における基本動作の確認を実施しました。フィードバックすべき事項は特にありませんでした。

(2)データの継続性の確保（バックアップ体制）

情報システムの実データとバックアップデータの同時被災による喪失は、事業の継続に致命的な影響を与えます。

バックアップデータの遠隔データ保管を基本としていますが、バックアップテープの運送による物理的な移送に加え、クラウド環境へのオンラインバックアップを追加しました。これらはバックアップデータの重要性、その量、更新の頻度などを判断基準として使い分けています。

ニュース

リコーインダストリー株式会社、リコーテクノロジーズ株式会社の東北事業所、および株式会社リコーの電装ユニットカンパニーの各社がISO22301事業継続マネジメントシステム(BCMS)認証を取得し2013年12月に登録を完了しました。
経済産業省のホームページではリコーグループの以下の取り組みが紹介されています。

■ リコーグループのBCPに関する基本的な考え方、復旧目標などを解説
■ サプライヤー向けセミナー開催の背景と目的を解説
■ BCP/BCMS構築にあたり重要なポイントを解説

http://www.meti.go.jp/policy/economy/hyojun/group-ms/index.html
http://www.meti.go.jp/policy/economy/hyojun/group-ms/c_group_17.html

2014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より具体的な改善・拡充に取り組んでいきます。

1.BCP対象となる重要ITシステムの見直しと対策状況の確認
2.定期的な訓練実施の定着
　PDCAのマネジメントシステムとしての実施を計画しています。
3.連携訓練を行う国内関連会社の範囲拡大
　連携すべき国内関連会社を重点化し訓練の拡大を計画しています。

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

*BCMS(business continuity management system) 事業継続マネジメントシステム
*BCM(business continuity management) 事業継続マネジメント
*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者を対象としたeラーニング教育を実施しました。
ITの進化に伴う新しい分野（SNSなど）のルールの徹底に関する設問とともに、従来からの基本的なルールの順守に関する設問も含めたコンテンツとしました。特に「あなたならどうする?」という問い掛け形式の設問で受講者に気づきを与え、より深い理解を求めました。
国内リコーグループでは、eラーニングサイト「知識の天窓」を利用し、約4万人が教育を受講しました。
その他、例年の階層別、役割別教育として新入社員やISMS推進事務局など、それぞれの階層に適したeラーニング教育や集合教育を実施いたしました。

2014年度の活動計画

リコーグループの全従業者を対象に、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。

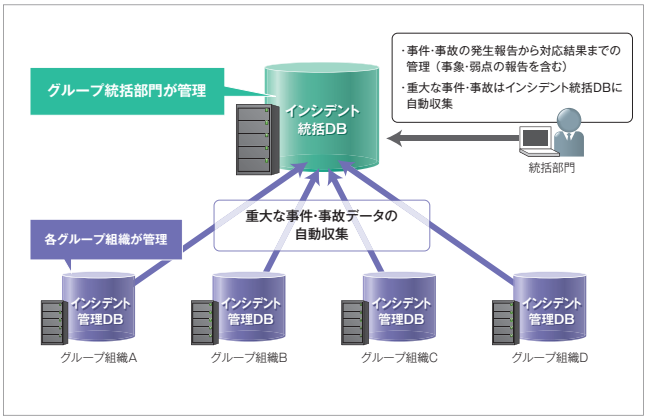
■ ITの進化に伴う新しい分野のルールの徹底
　例:スマートデバイスの活用ルール、ソーシャルメディアルール、クラウド利用ルールなど

6.IT活用による情報セキュリティ事件･事故の再発防止

2013年度は外部への発表を要する重大な事件･事故が発生しました。
詳細は以下をご参照ください。
「プリントアウトファクトリー」サイト改ざんに関するお知らせ
http://www.ricoh.co.jp/sales/news/130603.html
対象期間に当該サイトを閲覧された皆さまにご迷惑とご心配をお掛けしましたことを深くお詫び申し上げます。今回の事態を厳粛に受け止め、再発防止に取り組んでまいります。

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、2011年度から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･徹底を図ります。
(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。



2014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。
今後は増加の見込まれるWeb関連の事件･事故に力点を置きながら、従来の情報セキュリティ事件･事故についても教育の仕組みや内部監査の仕組みと連動し、更なるIT活用による予防と再発防止に取り組んでまいります。