2014年度活動報告と2015年度活動計画

1. 2014年度活動報告概要

2014年度、国内では大規模な個人情報漏洩事件が報じられ、個人情報管理の適切性を見直すきっかけになりました。このインシデントは、個人情報保護法の改定にも影響しています。またITツール主体の情報セキュリティ対策の脆弱性も露呈しました。
リコーグループでは2013年度に報告した不正アクセスによる一部ページの改ざんを機にCSIRTを組織化しました。現在までに培われた情報セキュリティマネジメントシステムとの一貫性を保って、CSIRT活動か展開されています。2014年度、CSIRTは世界レベルの活動として展開しバーチャルワンITを目指しました。

2014年度のグループISMS（ISO27001）統一認証を継続しました。また、ISO/IEC 27001/2013（JIS Q 27001/2014）への移行が完了しました。
特にリスク概念のマネジメントシステム共通化は、リスク定義を抽象化し理解し難い印象を与えました。しかし「情報セキュリティ目的」、「リスク」、「リスク源」、「事象」、その「結果」の関係は「原因が事象を発生させ結果が生じる」となりシンプルなものになりました。

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）統一認証の維持

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。
2014年度、グループISMS（ISO27001）統一認証の継続審査を受審し、認証を継続しています。
国内17社、海外48社、計65社が認証を取得しています。（2015年1月）
株式会社ソフトコム（国内）が新規拡大審査を受審し、新たに統一認証に加わりました。

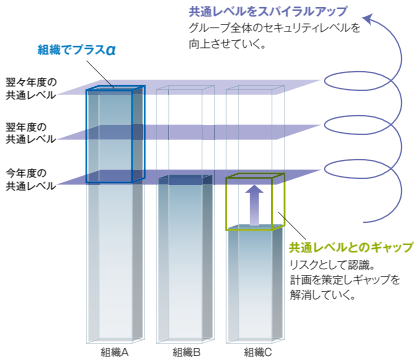
2014年度継続審査にてISO/IEC 27001/2013（JIS Q 27001/2014）への移行が完了しました。
新規格への移行のため、まず改訂内容を十分に把握し、リコーグループ標準および情報セキュリティ対策共通基準を見直しました。新たに対応が必要な要求事項と管理策を絞り込み、具体的な施策として周知徹底したため新規格に速やかにかつ効率よく移行できました。
また新規格で追加された管理策の多くが、すでに情報セキュリティ対策共通基準に取り組まれていたことも効率化を促進しました。
これをもとに、リスクアセスメント・ツールなどISMS関連のITツールを更新しました。

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。

2015年度の活動計画
2015年度は継続審査を受審し認証を継続します。

リンク：認証取得記事

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。

2014年度は、ITセキュリティ実装に関する要求事項を世界レベルで規定する新たな取り組みを開始しました。

情報セキュリティ対策共通基準の下位の規定として「ITセキュリティガイドライン　第1版」をリリースしました。情報セキュリティ対策共通基準は「What」を規定し、このガイドラインはITによる「How」を具体化しました。

ITセキュリティガイドライン

(1) 目的

最低限のセキュリティ要件と、世界各拠点によって組み込まれるべきセキュリティ事件・事故に対する十分で効率的な対策を提供する最良の手法を確立する。

(2) 内容概要

■本ガイドで対象とする領域とシステム
■セキュリティログの収集と監視
■ログの管理
■ウィルス駆除とマルウェアの検出
■インターネットの脆弱性チェック
■Webアプリケーションの試験
　等々

2015年度の活動計画

世界各拠点のITセキュリティ実装状況を把握し、「ITセキュリティガイドライン」を改訂します。この改訂時、情報セキュリティ対策共通基準も併せて検証します。

世界共通に要求すべき事項、各拠点・各国での組み込み事項をITの実装と運用方法の両面から最適化し、情報セキュリティ活動の有効性・効率性を高めていきます。

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ています。「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。

2014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) 2014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や気付きを収集し、改善点を手順書に反映しました。
2	有事の際のシステム稼動確認訓練	システムごとの確認手順書の有無を調査し、および手順書に課題が無いかを検証し、必要に応じて手順の作成、改訂を推進しました。

(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継続しています。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。

ご参考
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

2015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プロセスの拡充を進め、訓練の実施によりプロセスを定着させ、これを評価しさらなる改善を推進します。
1. 事業継続の視点による、各ITシステムの重要度に応じた対策状況の確認
2. 定期的な訓練実施によるBCPマネジメント・実施プロセスの定着
3. BCPプロセスの国内関連会社との連携強化、訓練実施によるプロセスの拡充

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を狙いとした教育の継続

eラーニングによる リコーグループの全従業者を対象としたセキュリティ教育実施しました。
教育内容は、インターネットへの社外秘情報の流出につながりかねない許可のない情報持出し、パソコンにファイル共有ソフトを導入するリスクを再確認し警告しました。
増加傾向にある標的型攻撃の手口を周知し、メールに添付されたファイルやURLを安易に開かないよう指導し、OSやウィルス対策ソフトを最新に更新するよう意識付けました。
また、リコーグループソーシャルメディアポリシーの規定から、SNSへの不用意な投稿による炎上を招かぬよう啓発しました。

2015年度の活動計画
リコーグループの階層別教育の一環として実施される管理者向けのマネジメント教育に「情報の管理責任者としての役割と責任」を組み込みます。
管理すべき情報とその取り扱い手順を明確にすることや、情報を安全・安心に活用するための業務手順の見直し、セキュリティインシデントへの対応など、管理者としての役割と責任を明確化し、情報セキュリティが適切にマネジメントされることを狙いとします。
全従業者を対象にした教育では、リコーグループの情報セキュリティの考え方とIT環境を取り巻く変化や個人情報保護の観点に対応した日常の順守事項を再確認します。

リンク：知識の天窓記事

2014年度活動報告と2015年度活動計画

6. 情報セキュリティインシデントの再発防止

2014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インシデントはありませんでした。

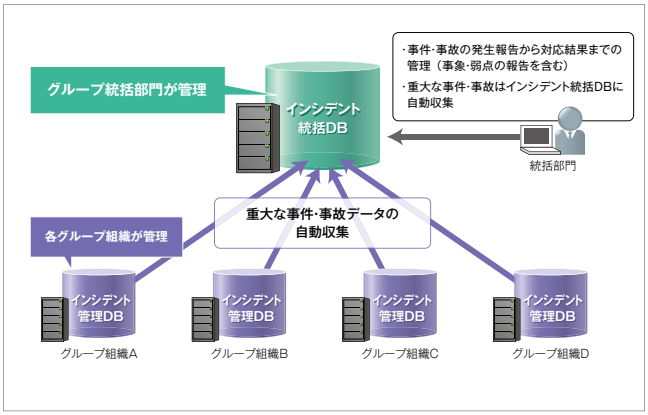
2013年度は不正アクセスによる一部ページの改ざんという重大なインシデントが発生し報告しました。
これはサイバー攻撃という脅威を身近に実感させる大きなインシデントでした。
これを機にCSIRT*1活 動の重要性が認識され、外部の支援などを得て早期の解決を図りました。しかしサービスの再開には約2ヶ月を要してしまいました。
これらの一連の対応は、危機感とともにCSIRTの活動を大きく加速させ、世界レベルの推進体制（バーチャルワンIT）により一貫性のある展開の原動力と なりました。

*1CSIRT（Computer Security Incident Response Team）:外部ネットワークを介してのコンピュータへの攻撃や脅威、セキュリティインシデントに対処する組織体の略称。

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

(1) インシデント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、日常発生しがちなインシデントについては、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) インシデント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。

リンク：事件･事故管理



2015年度の活動計画

引き続き重大なインシデントの発生ゼロが目標です。
また、ISO/IEC 27001/2013（JIS Q 27001/2014）の改訂に伴い新たなリスクマネジメントの概念からインシデント管理を見直します。すなわちインシデントの定義、およびエスカレーションすべきインシデントの特定など、インシデント管理全般を改訂します。
サイバー攻撃などで外部ネットワークを介してのコンピュータ･セキュリティインシデントはCSIRTと連携して早期解決を図ります。
その他の情報セキュリティインシデントについても教育での周知･徹底や内部監査での確認など、マネジメントシステムを回しIT活用による予防と再発防止に取り組みます。

7. バーチャルワンITによるCSIRT活動（新規報告内容）

「6.情報セキュリティインシデントの再発防止」でも述べましたが、2013年度、サイバー攻撃を機にCSIRTを組織化し、短期間に世界レベルのチームとしました。

2014年度の目標

地域や会社の枠にとらわれることなく、グループ・グローバルな人材を有効活用し（バーチャルワンIT）、「未然防止」、「早期発見」、「迅速対応」の3つの視点でコンピュータ・セキュリティ事件・事故に対応する世界レベルの推進体制を構築する。

2014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コンピュータ・セキュリティインシデントはありませんでした。

2014年9月23日～9月25日、リコー・グローバル・セキュリティ・サミットがドイツのミュンヘンで開催されました。

http://jp.ricoh.com/security/management/news/news_004.html（国内）

http://www.ricoh.com/security/management/news/news_004.html（海外）

世界レベルでの連絡体制を構築し、CSIRTの年間活動計画（Annual Plan）を策定しました。

2015年度の活動計画

世界レベルの連絡体制のもと、バーチャルワンITによるグローバルCSIRTの運用を開始します。またPSIRT*2との連携を強化し一貫性のある情報セキュリティを目指します。また「ITセキュリティガイドライン 第2版」をリリースします。

*2PSIRT（Product Security Incident Response Team）：製品への攻撃や脅威、セキュリティインシデントに対処する組織体の略称。