2015年度活動報告と2016年度活動計画

1. リコーグループ情報セキュリティ活動

リコーグループは社会環境の変化に対応し、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、内部監査や外部審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、日々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。

〔国内のトピック〕

2015年9月3日、「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律案」（9月9日公布）が成立し、個人情報の定義が明確化されました。今後はそれぞれの取扱いに関する政令などが定められる見込みです。リコーグループでは、「個人番号関係事務」を担当する部署を明確にし、グループ共通の取扱規定の策定などを実施しました。

番号法の公布に伴い「リコーグループ　個人情報保護基本方針」、「特定個人情報の利用目的と取扱いについて」を改訂し公開しています。

リコーグループ　個人情報保護基本方針:
http://jp.ricoh.com/privacy/
特定個人情報の利用目的と取扱いについて:
http://jp.ricoh.com/privacy/index_2.html

2. グループISMS（ISO27001）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。2015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16社、海外48社、計64社が認証を取得しています。（2016年2月）

テクノレント株式会社（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。

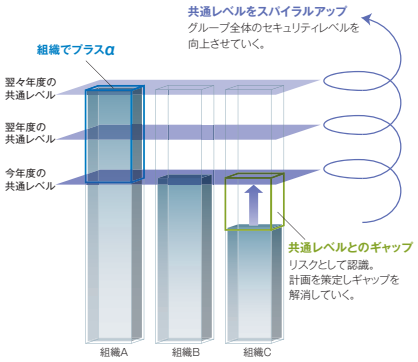
2016年度の活動計画

2016年度は4回目の更新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、順守すべき個々のルールが網羅されています。



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。新たな脅威の出現や、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。

2015年度、情報セキュリティ対策共通基準に関する新たな基準追加はありませんでした。

国内では共通基準を基にルールの解説、及び事例を「情報セキュリティガイドライン」としてまとめました。

2016年度の活動計画

ビジネスでは、タブレット、パソコンなどを携行して社外で使用することが日常になりました。シンクライアントやクラウド利用とは異なり、ハードディスクに情報を保持するパソコンは、紛失した場合に情報漏えいのリスクがあります。リコーグループでは「情報の持出し」の際のリスク低減策として、2013年から順次、ノートパソコンのハードディスク暗号化を運用しています。

2016年度はこの運用をグループに徹底することを狙いとして、社外に持出すパソコンのハードディスク暗号化を必須とし情報セキュリティ対策共通基準を改定します。また情報セキュリティガイドラインの充実と展開を継続します。

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://jp.ricoh.com/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。

2015年度も例年通り、訓練の実施やその結果による改善などを実施し、実効性の高い事業継続計画の維持に努めました。

(1) 2015年度に実施した訓練

	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 (初動開始、被災状況確認、災害対策本部設置、本部活動開始まで)	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、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は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、情報量、更新の頻度などを判断基準として使い分けています。

2016年度、ITシステム関連の活動計画

引き続き、防災対策(※1)、事業継続計画(BCP(※2))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、対策状況の確認
2. 定期的な訓練実施
3. 国内関連会社との連携強化、訓練実施

※1 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
※2 BCP(Business Continuity Plan):事業継続計画、「万が一の大災害や事故」が発生した場合に、それによる被害を最小限に抑え、事業をすぐに復旧し継続するための計画

5. 情報セキュリティの意識向上を狙いとした教育の継続

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、リコーグループの階層別教育の一環として実施しました。

リコーグループの全従業者を対象とした情報セキュリティ教育をeラーニングで実施しました。

教育内容は、日常のセキュリティ習慣として定着させたいパソコンの管理やメールの送受信など業務情報の基本的な取り扱いに加え、使い方によっては思わぬインシデントにつながるソーシャルメディアおよびクラウドサービス利用におけるルール・注意事項を含んでいます。

情報セキュリティ教育は一部の国内ご販売店様にもeラーニングで展開しました。英語対応の従業者向けには教育内容を英訳したファイルを社内に公開しています。

また、役員向けには、近年増加している標的型攻撃の手口の説明や被害に遭わないための対策を再確認し警告しました。

標的型攻撃についての警告は、グループ内への発信・掲示などの方法で情報提供し、メールに添付されたファイルやURLを安易に開かないこと、OSやウイルス対策ソフトを最新に更新することの重要性を周知しています。

2016年度の活動計画

新入社員を対象に、従来リコーグループ共通の集合教育で実施している情報セキュリティ教育を、eラーニングに変更します。
リコーグループの情報セキュリティの考え方をはじめ、入社後すぐに必要なセキュリティ知識と行動を、個々の理解度に合わせて受講できるため、理解度の向上が期待できます。また、グループ各社の教育スケジュールの最適なタイミングに組み込めます。
全従業者には、社会の変化やIT環境の変化によるセキュリティリスクに関する必要な情報提供や周知を目的とした教育を継続します。

リンク:知識の天窓記事

6. インシデントの発生と再発防止

6.1. インシデントの報告

2015年度、重大インシデントとして次の2件が発生し外部に発表しました。

(1) お客様の情報を含むノートパソコンの盗難
発生内容:
お客様情報を含むノートパソコンの盗難に関するお詫びとご報告
http://www.ricoh.co.jp/notice/2015/1102_1.html
再発防止策:
セキュリティ対策の強化を実施するほか、社内標準規定の見直しおよび充実、お客様情報および個人情報の重要性に関する社員教育の再徹底、情報の取り扱いに関する内部監査を徹底します。

(2) システム障害による各種サービス不具合
発生内容:
システム障害のサービス復旧のお知らせ
http://www.ricoh.co.jp/sales/notice/160316_1.html
再発防止策:
原因は冗長系を構成する機器のドライバーソフトウェアの不具合でした。ドライバーソフトウェアおよびボードの交換を実施し、正常な動作を確認しました。

6.2. グループ内インシデントの管理

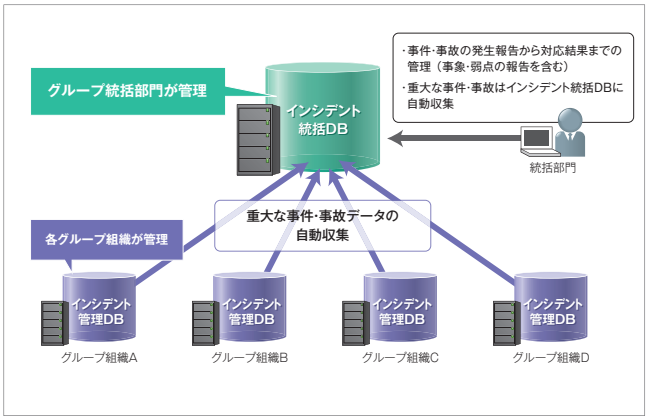
以下のステップでグループ内インシデントの予防と再発防止に取り組んでいます。

(1) 情報の共有:
インシデント情報と再発防止策をグループ内で共有しています。

(2) 教育による周知·徹底:
パソコンや外部記憶媒体の紛失、ウイルス感染など、日常発生し得る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、防止策の周知·徹底を図っています。

(3) 内部監査:
インシデント情報や教育での徹底事項は、内部監査での重点項目とし、グループへの徹底と改善を推進しています。

(4) マネジメントレビュー:
インシデントの分析結果をマネジメントレビューで報告し、再発防止策の有効性をトップマネジメントにて確認しています。



2016年度の活動計画

パソコンや外部記憶媒体の紛失による情報漏えいを防止する対策を継続します。
サイバー攻撃など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(*)が早期解決を図ります。
その他の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。

* CSIRT(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。

リンク:事件·事故管理

7. ITセキュリティ

2014年度にリリースした「ITセキュリティガイドライン」を「ITセキュリティ要求事項(IT Security Requirements)」と名称を変更し、第4版をリリースしました。
世界各拠点において、この要求事項(最低条件)と現在の実装とのギャップ分析を行い、拠点ごとに識別されたギャップに対する対策の優先順位を決め、2016年度以降の実施計画と予算配分に反映しています。
2015年度、アジアの関連会社のインターネット公開システムへの不正アクセスが確認されましたが、CSIRT(*)による適切な対処で実害は確認されませんでした。

2016年度の活動計画

ギャップ分析結果に基づいたセキュリティ対策の最適化と「ITセキュリティ要求事項」の追加項目の内容検討を実施します。
また、生産関連会社での要求事項(最低条件)と現在の実装とのギャップ分析を実施し、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。
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。

* CSIRT(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。