『社会からの要求に応えるために』

～情報セキュリティの意識醸成と維持・増強への取組み～

RICOH
imagine. change.

2017年1月26日、2月2日

リコーリース株式会社

Driving Sustainability for Our Future. 持続可能な社会を、ビジネスの力で。

アジェンダ

RICOH
imagine. change.

１．企業概要・事業概要・企業理念

２．マネジメントシステムへの取組み

３．改善活動事例紹介

４．これからの活動（目指す姿）

会社概要

RICOH
imagine. change.

商号	リコーリース株式会社（RICOH LEASING COMPANY, LTD.）
本社事業所	東京都江東区東雲一丁目7番12号
代表者	代表取締役社長執行役員　瀬川　大介
上場市場	東京証券取引所第一部
資本金	78億9,686万円
売上高	2,758億円
従業員数	928名（連結）
設立	1976年（昭和51年）12月 
事業拠点	２４拠点

事業説明

RICOH
imagine. change.

サービス	商品
リース・割賦事業	リース レンタル クレジット・割賦 （事務用・情報関連機器、医療機器、環境関連など）
金融サービス事業	ローン（個人・法人） 売掛金集金代行サービス 請求書発行代行サービス カード事業 資産管理サービス 介護報酬ファクタリングサービス

リコーリースの社会への提供価値

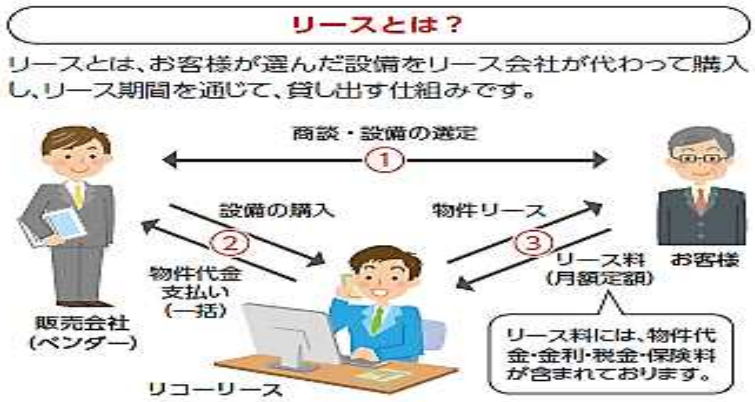
世のなかに、広く早く設備を行き渡らせたい

1972年、リコーはPPC900(リコー初の普通紙にコピーが取れる機械)を発売しました。価格は従来の3倍と購入(一括支払い)が難しく、また当時は高額な機器しか扱わないリース会社が多かったため、少額の機器を取り扱うリース会社として1976年にリコーリースが設立されました。

中小企業への支援

日本には中小企業が約380万社あり、全企業の99.7%を占めています。当社のお客様は約40万社で、そのなかの98%を占める約39万社が中小企業です。リースを通じて中小企業全体の1割にあたるお客様の事業を支援することで、日本経済の活性化に貢献していきます。

※2016年版中小企業白書を参考



特色

- 主要なお客様である中堅・中小企業
- 小口分散による優良な資産
- 「販売支援リース」と効率化された「業務処理の仕組み」

企業理念・行動規範

RICOH
imagine. change.

リコーウェイ

創業の精神

三愛精神

人を愛し
国を愛し
勤めを愛す

経営理念

私たちの使命

私たちの目指す姿

私たちの価値観

信頼を未来へ
リコーリース

4つの重要活動領域

企業理念

私たちの使命

私たちは常にチャレンジします。
変化に向かって迅速に独自性のあるサービスを提供し活力ある社会の実現に貢献します。

基本姿勢

1. お客さまやお取引先の期待を超えるサービスを提供し続けます。
2. 社員一人ひとりを尊重し、豊かさの充実に努め、いきいきと働ける環境をつくります。
3. 社会環境と調和した企業活動により、地域・社会に貢献します。
4. 健全な経営と企業価値の増大を通じて、株主の期待に応えます。

行動指針

1. 徹底的にお客さまやお取引先の立場にたって行動します。
2. 広く深く考え、スピーディーに行動します。
3. 誇りと責任をもって、誠実に行動します。

当社・情報セキュリティ沿革

RICOH
imagine. change.

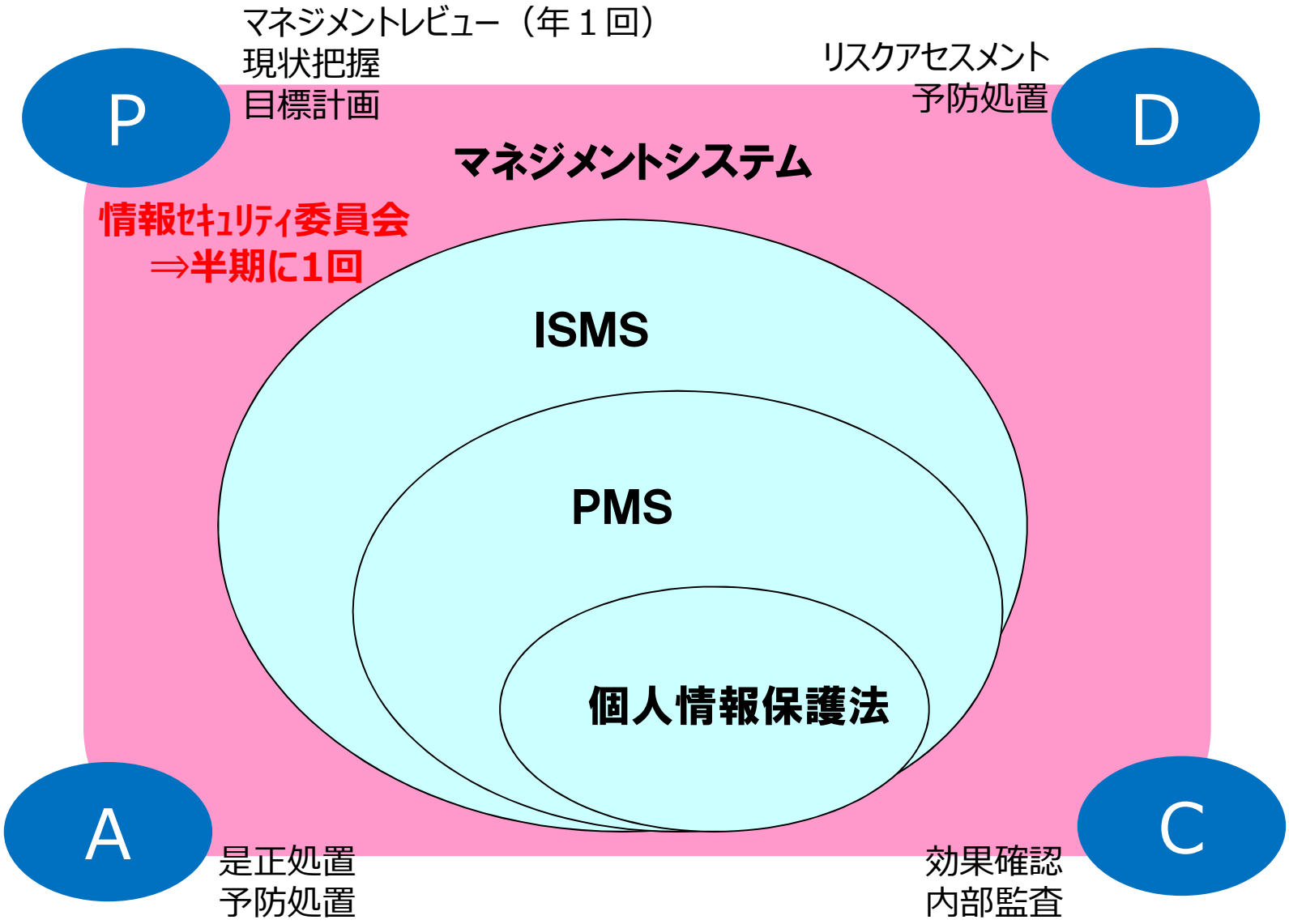
ＩＳＭＳと個人情報保護（ＰＭＳ）とを一体にし継続的に改善しながら運営

	イベント
2002年　4月	「ISMS適合性評価制度」運用開始（日本規格）
2002年10月	ISMS及びPMSの構築を開始　※１
2003年10月	ISMS認証取得　**：リース会社第1号**
2004年　7月	プライバシーマーク付与　**：リース会社第1号**
2004年10月	ISMS(ver2.0)＆BS7799認証取得　**：グループ統一認証**　※２
2005年　4月	「個人情報保護法」施行
2005年10月	ISMS国際規格化　ISO/IEC 27001：2005（翌年JIS化）
2006年　5月	JIS Q 15001：2006改訂
2007年　1月	ISO/IEC27001へ移行認証
2013年10月	ISO/IEC27001改訂：2013（翌年JIS化）

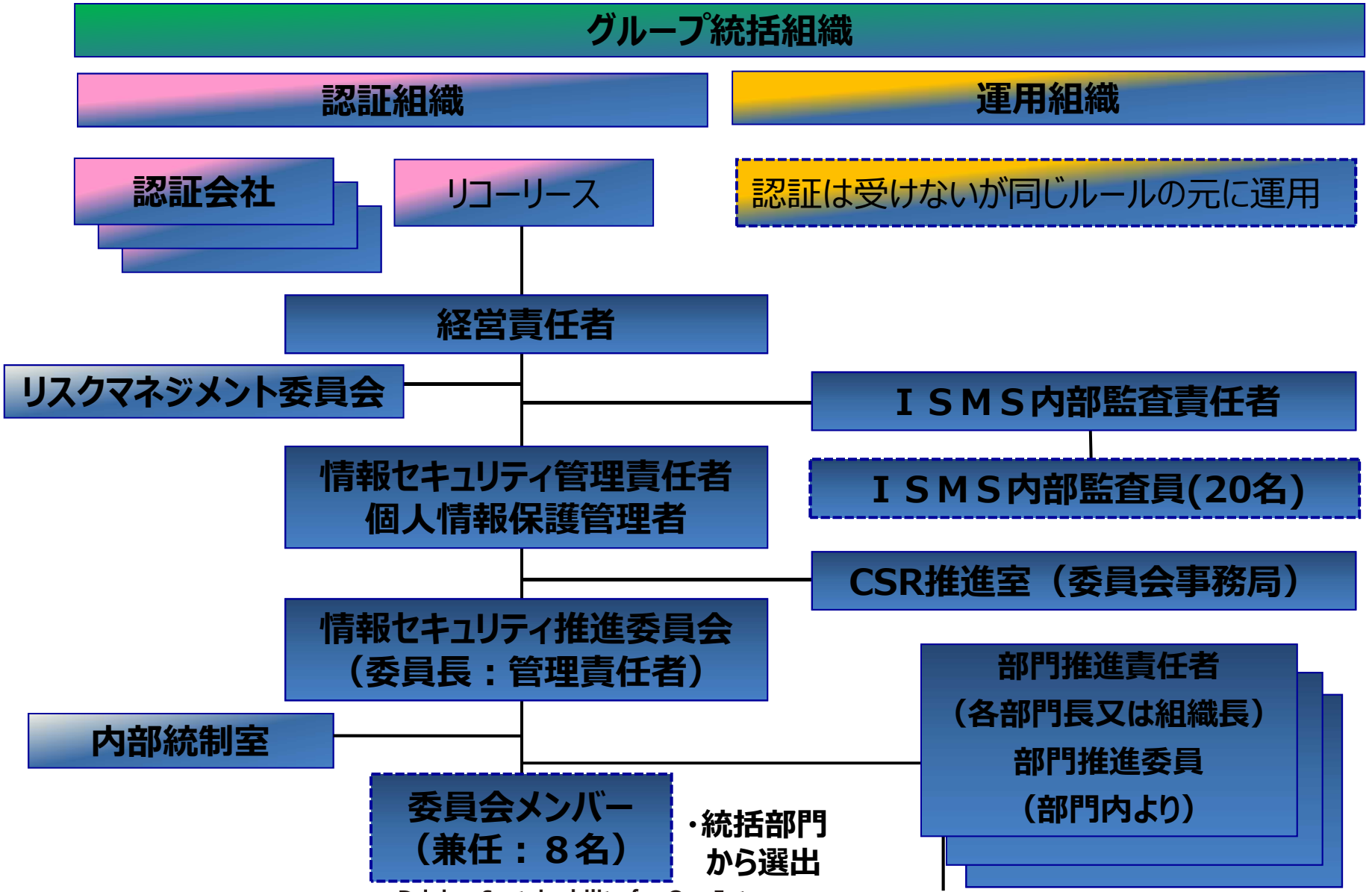
※１．ﾏﾈｼﾞﾒﾝﾄｼｽﾃﾑを構築に当って、コンサル会社を利用（当時は、「意識」、「ノウハウ」無し）
※２．「統一認証」～グループ（国内）会社全て（90社、1284サイト、52,000名の規模）での統一認証は「世界初」、「世界最大規模」。

マネジメントシステム考え方

RICOH
imagine. change.

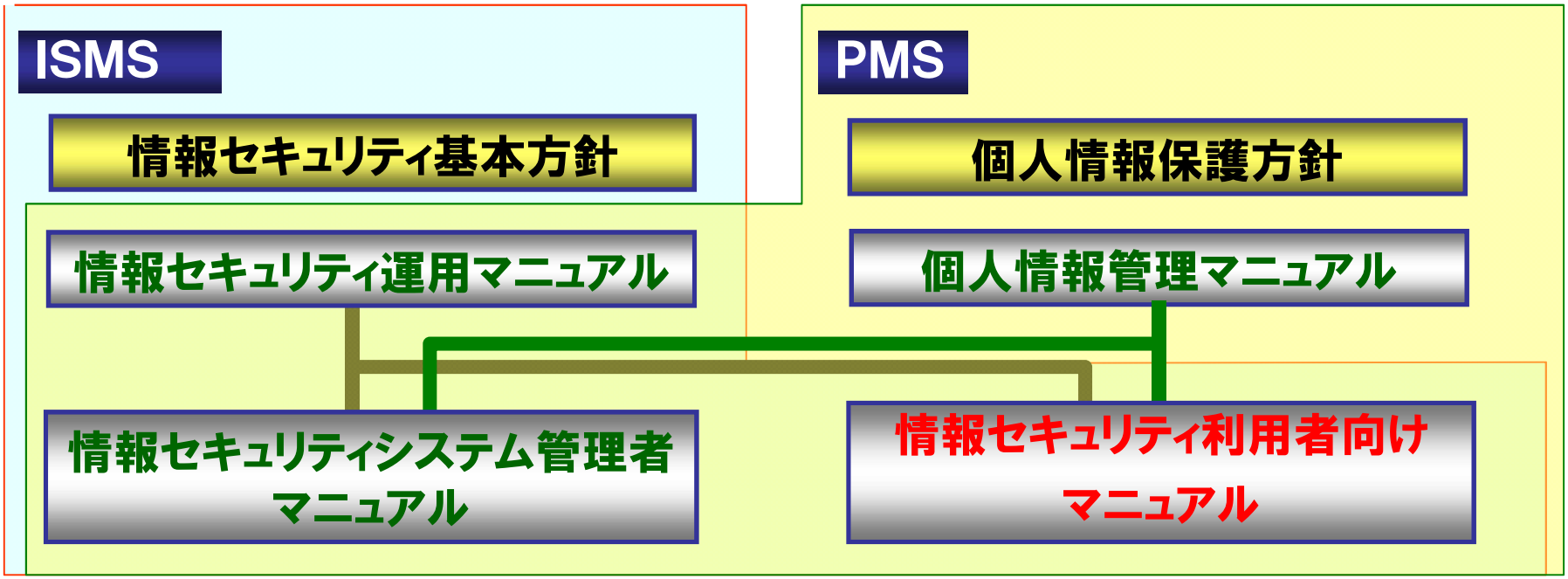


運用組織体系


グループ統括組織
認証組織
運用組織
認証会社
リコーリース
認証は受けないが同じルールの元に運用
経営責任者
リスクマネジメント委員会
ＩＳＭＳ内部監査責任者
ＩＳＭＳ内部監査員(20名)
情報セキュリティ管理責任者
個人情報保護管理者
CSR推進室（委員会事務局）
情報セキュリティ推進委員会
（委員長：管理責任者）
部門推進責任者
（各部門長又は組織長）
部門推進委員
（部門内より）
内部統制室
委員会メンバー
（兼任：８名）
・統括部門
から選出

ISMS＆PMS　マニュアル体系

RICOH
imagine. change.



マニュアル	経営陣・管理責任 推進委員、監査員	部門推進責任者 (部門長・推進担当)	システム部門 管理者	一般従業員 (派遣など含む)
情報セキュリティ運用 マニュアル	○	○	○	
情報セキュリティ 利用者向けマニュアル	○	○	○	○
情報セキュリティ ｼｽﾃﾑ管理者マニュアル			○	
個人情報管理 マニュアル	○	○	○	

個人情報の取扱い

RICOH
imagine. change.

「開示請求」と「問い合わせ」

情報セキュリティ利用者向けマニュアル

１）　お客様の個人情報保護に関する規則・ガイドライン

２）　役員及び従業員個人情報保護に関する規則・ガイドライン

・個人情報の利用目的の特定・取得・利用の遵守事項
・個人情報の適正管理義務
・個人情報の開示・訂正・削除・利用停止等
・個人情報に関する苦情及び相談

個人情報の開示請求及び問い合わせに関する手順書

１）　「開示請求」に関する運用ルール

２）　「お問い合わせ」業務の運用ルール

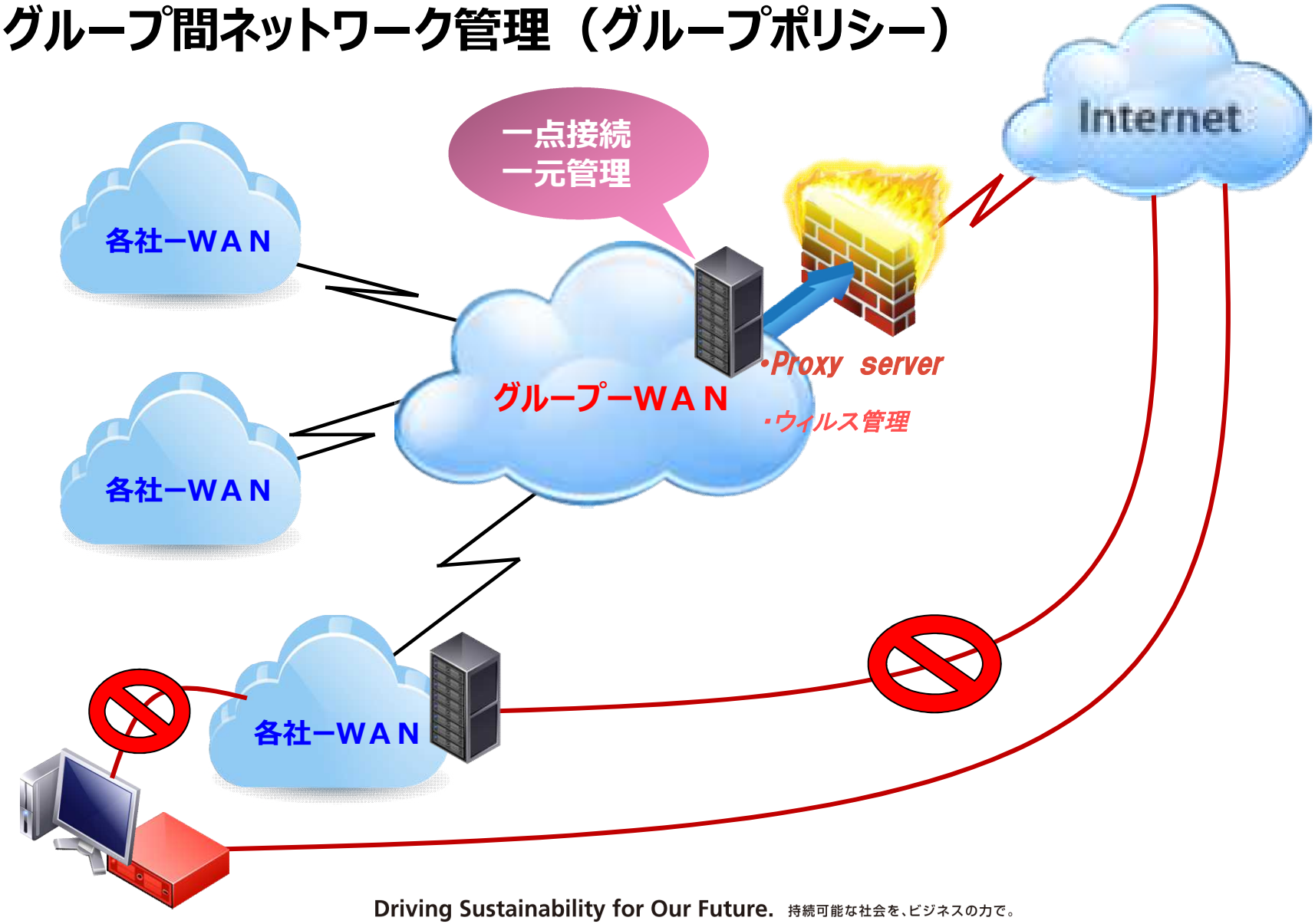
改善活動の事例紹介

RICOH
imagine. change.

マネジメントシステムを構築以来、弊社がこれまでに実施してきた「取組み」、「施策」、「設備導入」などを紹介させていただくことで、皆さまの個人情報保護＆情報セキュリティへの困り事、悩み事の解決の一助になれば幸甚です。

ネットーワーク環境

グループ間ネットワーク管理（グループポリシー）



居室の入退出管理

RICOH
imagine. change.

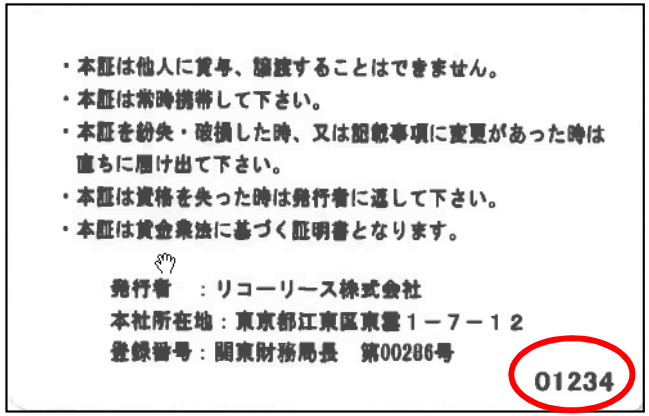
IDカード導入目的

セキュリティー区画、入退室管理エリアを設定、明示し、適切な権限（レベルⅠ～Ⅲ）に基づく入退室管理を実施し、情報管理品質の維持、向上と防犯に備える。

情報管理品質の向上
（不正アクセス、情報漏洩、盗難、紛失などの抑止）

防犯レベルの向上
（全業務従事者の安全面の向上）

※ログ情報により、入出者モニタリング（各エリア間の初回通過者）を監視

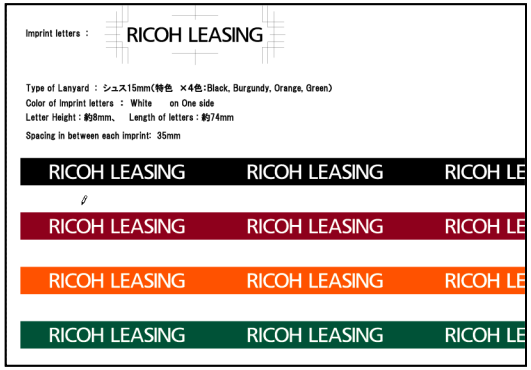

・本証は他人に貸与、譲渡することはできません。
・本証は常時携帯して下さい。
・本証を紛失・破損した時、又は記載事項に変更があった時は直ちに届け出て下さい。
・本証は資格を失った時は発行者に返して下さい。
・本証は貸金業法に基づく証明書となります。

発行者　：リコーリース株式会社
本社所在地：東京都江東区東雲１－７－１２
登録番号：関東財務局長　第00286号

01234

（金融監督庁指導）
社員証の裏面右下のナンバリング
貸金業法上の証明書となる為、
一意な番号を付与し、カードを管理する必要がある。

ストラップの色で従業員の種別を判定

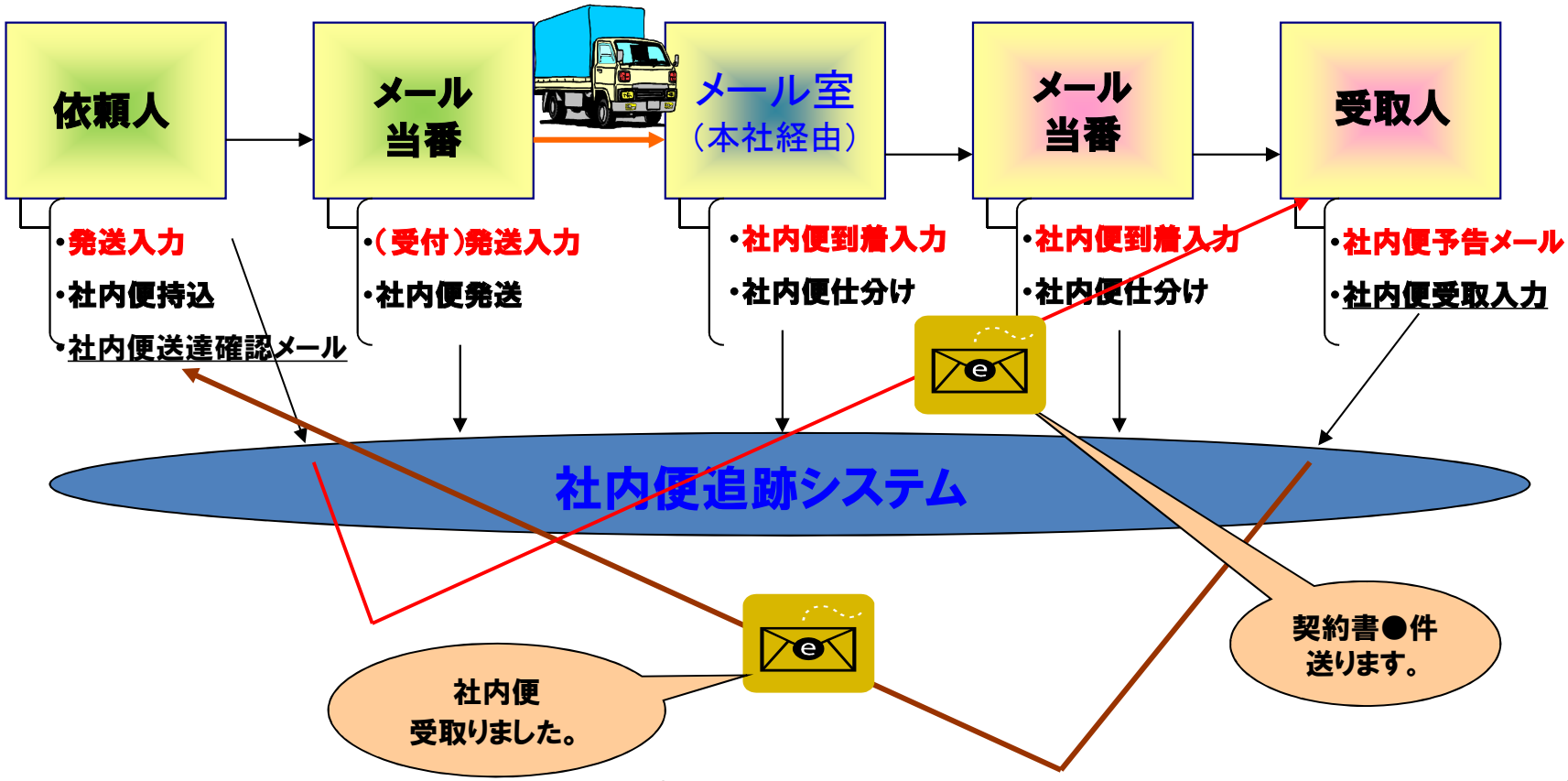


社内便管理

社内便追跡システムの導入

1.「送ります」「受取りました」を、自動で「お知らせ」メール・・・事前に認識ができる
2. 荷物の配達状況・配達履歴はWeb「社内便追跡システム」で確認できる
3. メール室（部門の郵便係含）はバーコード利用で効率化。

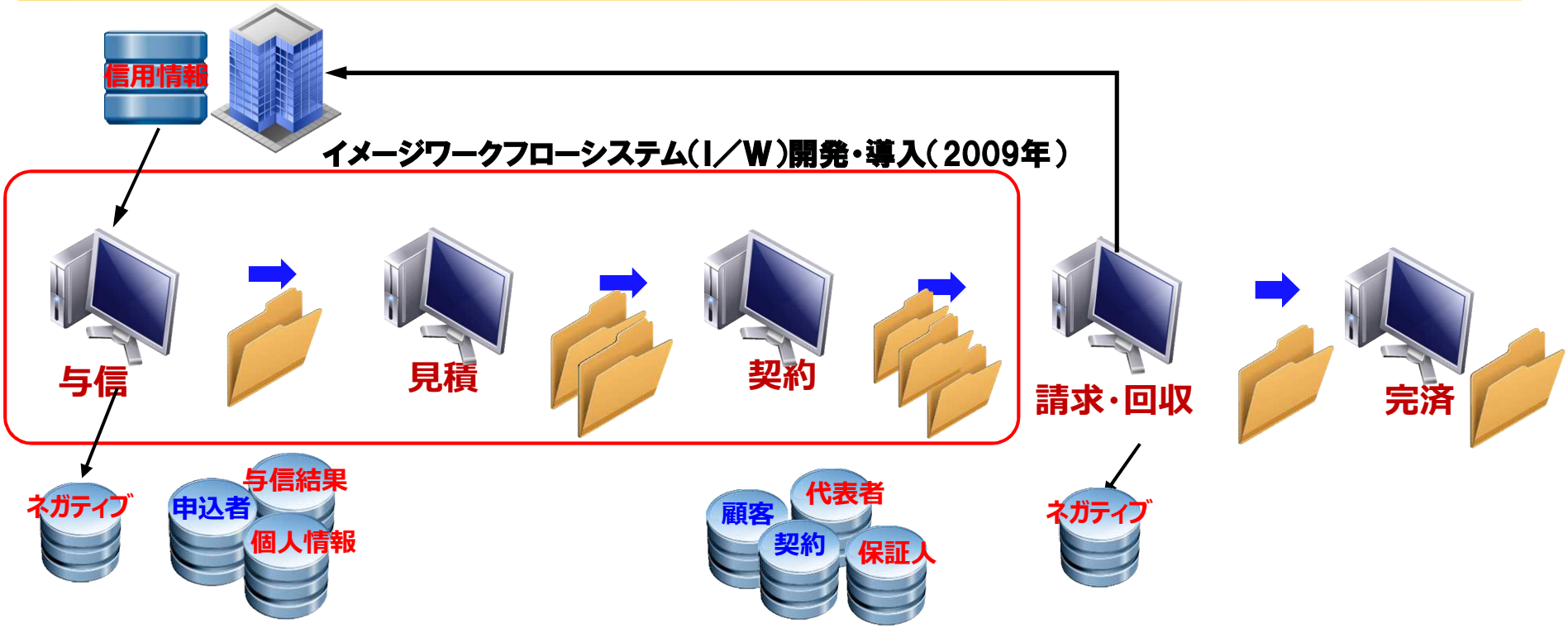
●システムの概要



ﾍﾟｰﾊﾟｰﾚｽ＆ﾘｽｸ回避＆業務効率

RICOH
imagine. change.

紙ありき文化から脱却



プリントせずイメージ化⇒「紙」情報の移動による“紛失”するリスクを回避

業務効率アップ（顧客満足）⇒資料の待ちが発生しない　～　与信回答時間の短縮

「紙」媒体の保管リスクを回避（スペース不要）

情報資産管理＆リスク分析

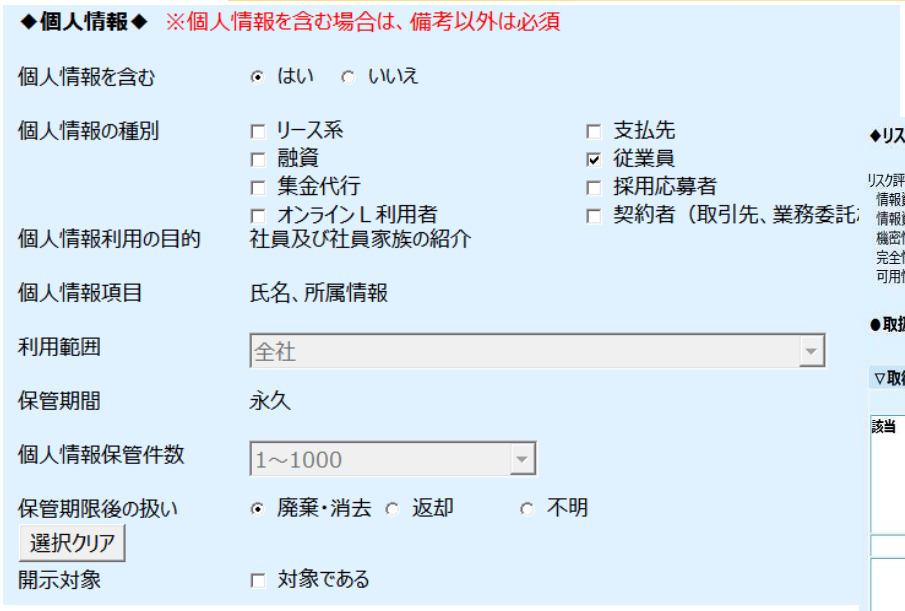
RICOH
imagine. change.

【問題・課題】

内部監査等でチェックを繰り返すが、統一性が図れない。

・情報資産台帳とリスクアセスメントが一連作業（管理）になっていない
・情報資産の洗い出しに漏れがある
・同じ職種、環境下であっても、「Ｃ・Ｉ・Ａ」価値評価が責任者によってバラバラ
・情報資産に対するリスクアセスメントで「脅威」の洗い出しにバラつきがある

Excel管理からツール化へ



該当	脅威ID	脅威内容	属性 C	属性 I	属性 A	脅威のレベル	具体例	脆弱性（現状の管理）	脆弱性のレベル
	2001	アクセスが許可されている者の錯誤による情報（データ）の持ち出し・漏洩 （業務上で誤って持ち出し）	1	0	0				
☑	2002	アクセスが許可されている者の故意による情報（データ）の持ち出し・漏洩 （不正持ち出し）	1	0	0	1	室員による持ち出し	USBポート経由での媒体への書き出しは申請・承認手続き。罰則規定・秘密保持契約・行動規範署名で抑止。	1

【見直し時期】
・定期見直し（年１回）
・随時見直し（組織変更、事業展開による新たな情報取得）

情報機器への対応

RICOH
imagine. change.

Ⅰ．媒体への書き込みセキュリティ対策
・全パソコンのＵＳＢポート閉じる（解放は業務上必要に応じ承認制）
・ＵＳＢメモリー貸し出し制（上司承認後、情報システム部門より貸出）

Ⅱ．モバイルパソコン管理
・申請による会社貸与のパソコンのみ使用可（持ち込み不可）
・ハードディスク暗号化（ＵＳＢキーによる解除）
・ワンタイムパスワードによる管理

Ⅲ．会社貸与携帯電話
・ロック機能の設定必須
・ＭＤＭ（モバイルデバイス管理）導入による監視・管理

MDMとは：iPhone、iPad、Androidなどのスマートフォンおよびタブレット端末をリモートで一元管理できるサービス。端末紛失・盗難時は、リモートロックやリモートワイプ（初期化）などによって、素早い対応で第三者への情報漏えいを防止。

内部監査

RICOH
imagine. change.

内部監査での悩み事・・・。

効率的かつ有効性の高い内部監査をおこないたいが。。。

「監査がマンネリ化している」、「監査が儀礼的になっている」

課題・問題

・内部監査員の確保
　～事務局以外は**全員が兼務者**
　～育成には時間（経費）を要する

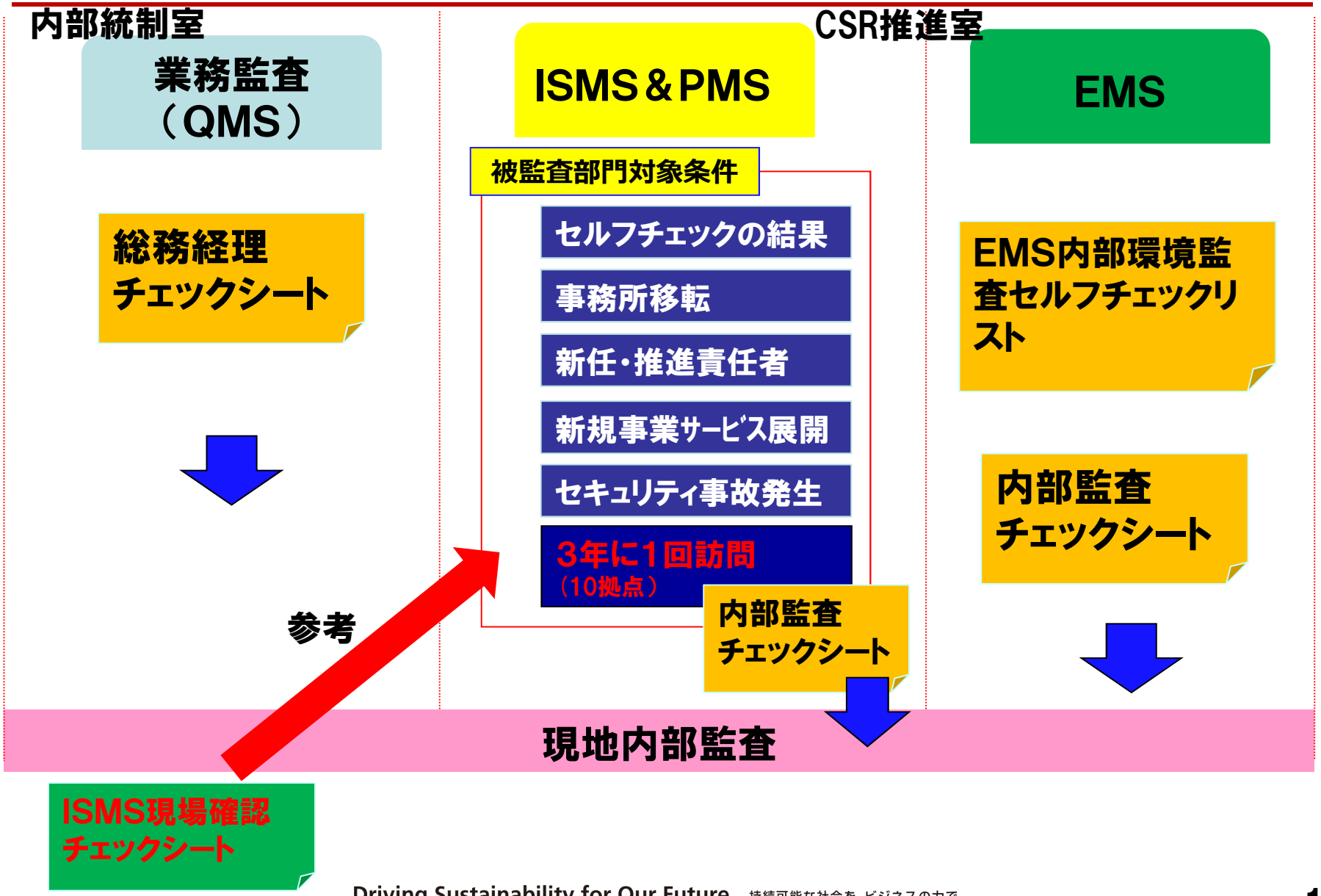
・内部監査員の力量
　～年１、２回の実績ではレベル上がらず
　～主業務で時間がなく専門教育を受けられない

} 標準的「ﾁｪｯｸﾘｽﾄ」による監査

有効：監査員の質を上げるため、業務に沿った内容の監査に切替

内部監査員見直し、内部監査教育実施、チェックリストを変更

内部監査


内部統制室
業務監査
（QMS）
総務経理
チェックシート
CSR推進室
ISMS＆PMS
被監査部門対象条件
セルフチェックの結果
事務所移転
新任・推進責任者
新規事業サービス展開
セキュリティ事故発生
3年に1回訪問
（10拠点）
EMS
EMS内部環境監査セルフチェックリスト
内部監査
チェックシート
参考
内部監査
チェックシート
現地内部監査
ISMS現場確認
チェックシート

有効性評価

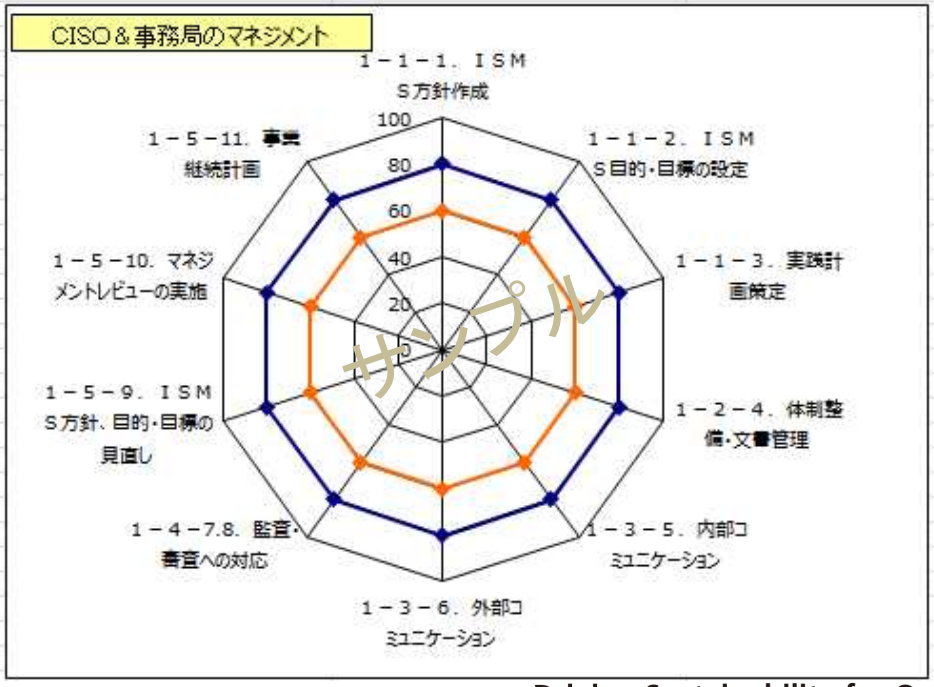
内部監査の結果で評価

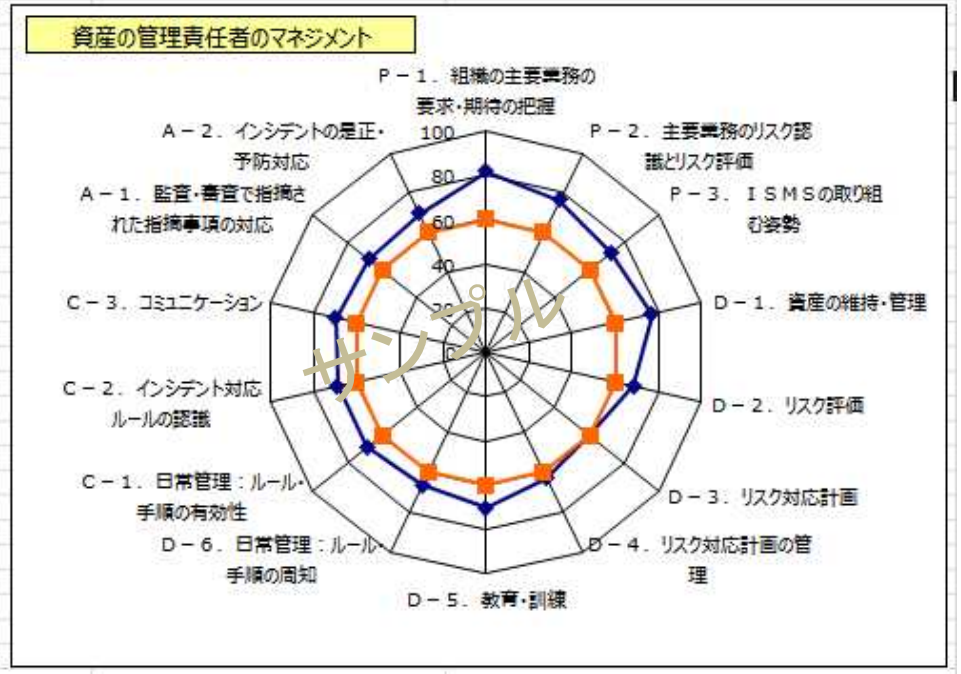
判定方法：　内部監査項目をＰＤＣＡサイクル工程に分類し、管理策に紐付けて項目毎に評価。
　　20点、40点、60点、80点、100点により有効性を評価する。

判定基準：　内部監査部門での内部監査項目（管理策）評価の平均値を算出し、効性の判断をする。

結果　：　監査項目全てについて６０点以上であった。

判定　：　詳細管理策にもとづく施策は有効と評価する。





委託先管理監督

RICOH
imagine. change.

委託先選定・継続判断の評価

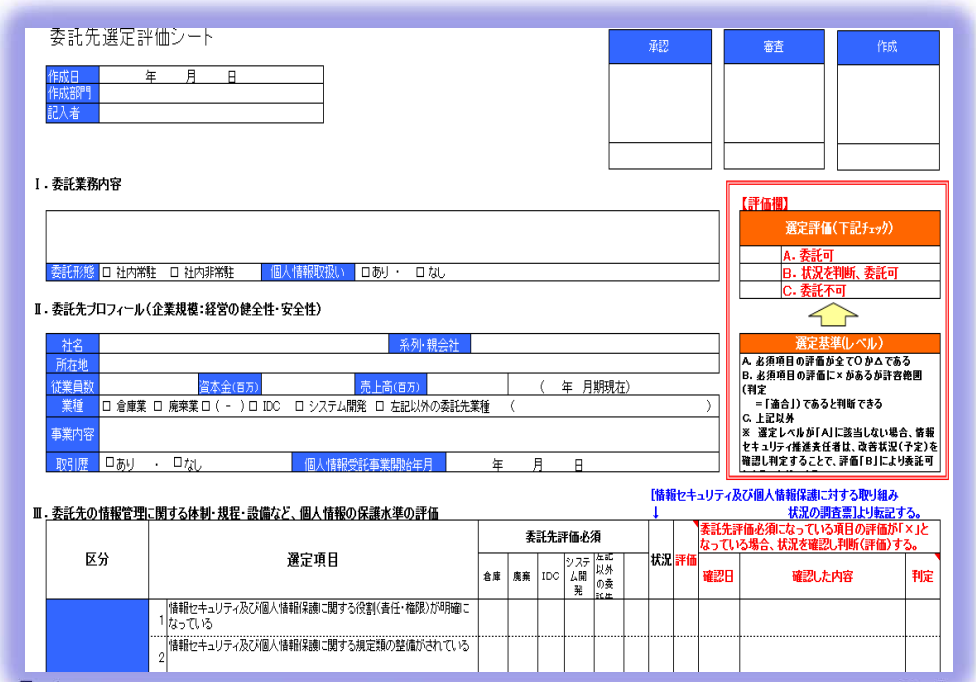
業務委託先における情報漏えい事件・事故発生防止

※委託先：書類廃棄、書類保管、業務委託、システム開発委託、産廃・売却.etc

■委託先選定評価を年１回実施
・アンケート形式 → 回答受取 →
担当部門で「評価シート」を用いて評価（ポイントスコア）

「調査チェックシート」

Ⅰ．組織的安全管理（a．実施済み/該当しない　b．実施を検討している　c．実施していない）				
項番	確認項目	a	b	c
1	情報セキュリティ及び個人情報保護に関する役割（責任・権限）が明確になっていますか	□	□	□
2	情報セキュリティ及び個人情報保護に関する規定類の整備がされていますか	□	□	□
3	情報セキュリティ及び個人情報保護に関して、規定類に従った運用がなされその記録がとられていますか	□	□	□
4	個人情報及び重要な情報資産の管理台帳の整備がされていますか	□	□	□
5	個人情報及び重要な情報資産の管理台帳の更新を適時に行なっていますか	□	□	□
6	情報セキュリティ及び個人情報保護について、事故や不測の事態に対する規定・手順が定められていますか	□	□	□
7	情報セキュリティ及び個人情報保護について、事故や不測の事態に対する連絡体制が整備されていますか	□	□	□
8	情報セキュリティ及び個人情報保護について、事故や不測の事態に対して再発防止へ繋がる仕組みがあり、その取組みが行なわれていますか	□	□	□
9	内部監査を定期的に実施していますか	□	□	□
10	内部監査の結果に基づいた是正措置、改善活動が行なわれていますか	□	□	□
	①委託業務の「再委託」を行なっていますか			


委託先選定評価シート

承認	審査	作成

作成日	年　月　日
作成部門	
記入者	

Ⅰ．委託業務内容

委託形態 □ 社内常駐 □ 社内非常駐　個人情報取扱い □あり・ □なし

【評価欄】

選定評価（下記チェック）
A．委託可
B．状況を判断、委託可
C．委託不可

選定基準（レベル）
A．必須項目の評価が全て○かΔである
B．必須項目の評価に×があるが許容範囲（判定＝「適合」）であると判断できる
C．上記以外
※　選定レベルが「A」に該当しない場合、情報セキュリティ推進責任者は、改善状況（予定）を確認し判定することで、評価「B」により委託可

Ⅱ．委託先プロフィール（企業規模：経営の健全性・安全性）

社名		系列・親会社		
所在地				
従業員数		資本金（百万）	売上高（百万）	（　年　月期現在）
業種	□ 倉庫業 □ 廃棄業 □（－）□ IDC □ システム開発 □ 左記以外の委託先業種 （　）			
事業内容				
取引歴	□あり　・　□なし	個人情報受託事業開始年月	年　月　日	

Ⅲ．委託先の情報管理に関する体制・規程・設備など、個人情報の保護水準の評価

【情報セキュリティ及び個人情報保護に対する取り組み状況の調査票】より転記する。

区分	選定項目	委託先評価必須 倉庫	廃棄	IDC	システム開発	左記以外の委託先	状況	評価	確認日	確認した内容	判定
	1 情報セキュリティ及び個人情報保護に関する役割（責任・権限）が明確になっている										
	2 情報セキュリティ及び個人情報保護に関する規定類の整備がされている										

委託先評価必須になっている項目の評価が「×」となっている場合、状況を確認し判断（評価）する。

インシデント管理

報告ツールの電子化

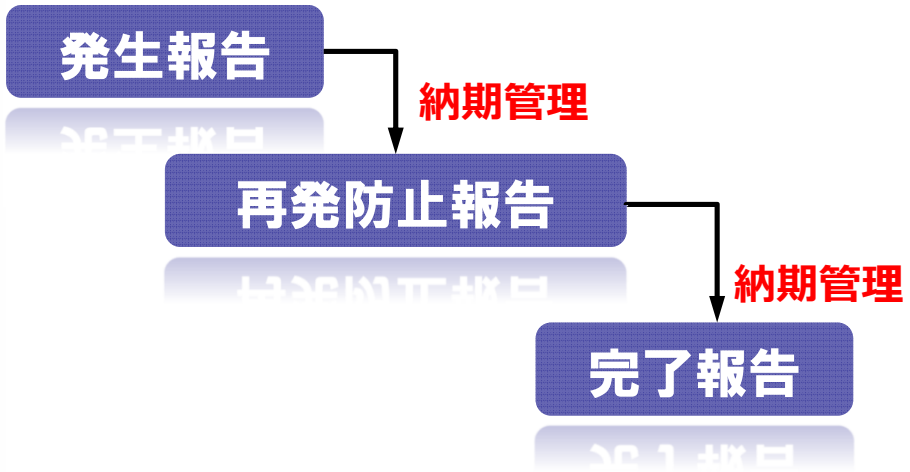
■メリット

1. 電子化により迅速な報告がおこなわれる(「紙」様式の報告書による情報の滞留)
2. 適切な承認フローが回る(本部長レベル、管理責任者まで必須)
3. 対応期限の管理(自動メールによる警告、督促)
4. 全社レベルでの情報(事例)共有
5. インシデント分析のための情報収集

情報セキュリティ事故報告書

発生報告作成中

報告者	
報告者部門名	
発生日	2016/11/2
発生時間	17:30 時ごろ発生
発生部門	
事故を起こした人の属性	○ 社員（準社員、契約社員含む） ● 派遣社員
事故を起こした人の性別	○ 男 ● 女
事故を起こした人の年代	『２０代』
事故を起こした人の年次（入社から何年か）	『１年目』
事故を起こした人の本業務経験年数	『１年目』
事故が発生した時期（事故となる作業をした時期）	● 繁忙期 ○ 繁忙期ではない 『契約締め最終日』



予防処置

電子メール

■制約事項

①送信メール容量制限

②誤送信防止機能

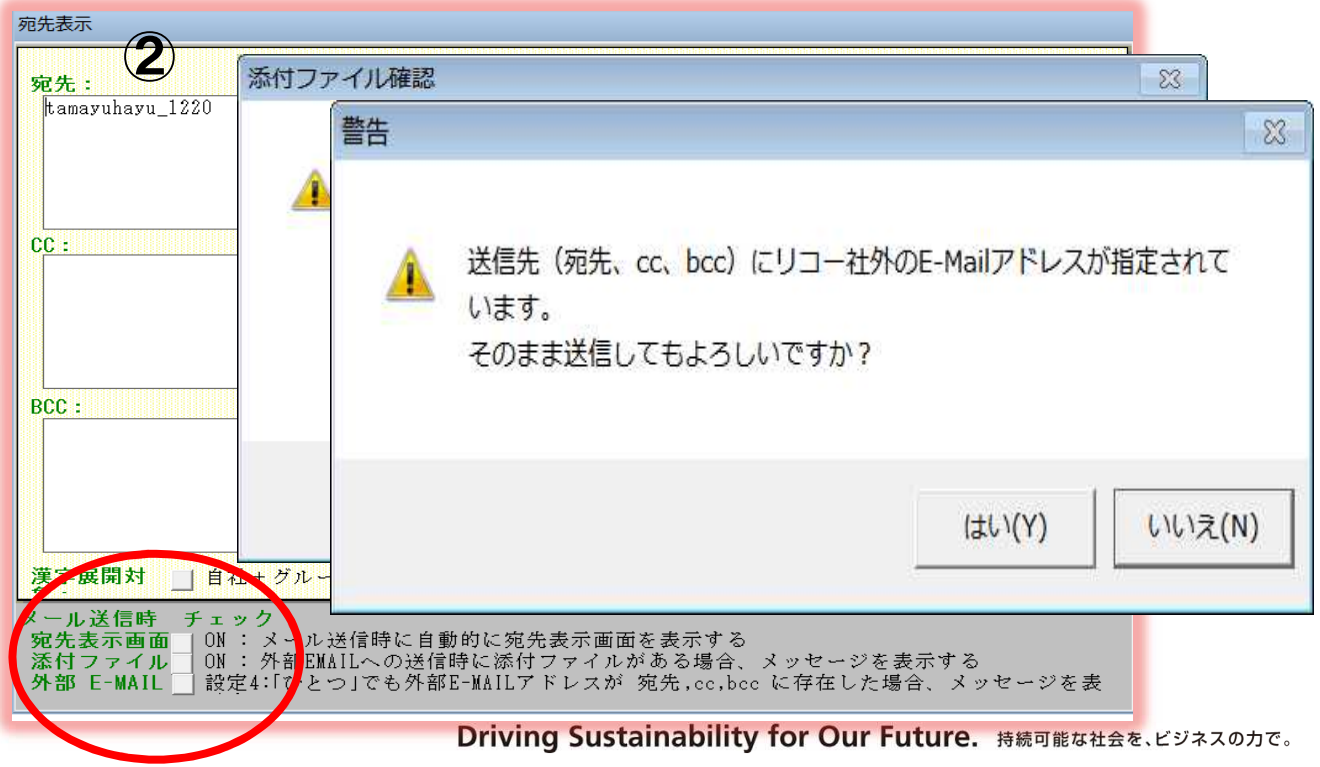
③添付ファイル自動暗号化＋パスワード付与

④自動転送機能の禁止

※「上長承認機能」の導入検討：業務の滞留を懸念して見送った・・・。

③社外宛先が含まれるメールの添付ファイルを自動暗号化して、パスワードの追いメール発信する仕組み

～件名に固定文字列
"##RICOH-ENCRYPTED##"を入力する



予防処置

RICOH
imagine. change.

電子メール

標的型メール攻撃の多発報告！！

・2015年6月、日本年○機○が個人情報約125万件が外部に流出
・2015年12月から、メール受信が頻繁に発生
　実在する配送会社に成りすまし、「荷物の配達通知」を装った迷惑メール

「標的型メールに対する訓練」実施
添付ファイル開封率＝29.6%（2016.1）

・2016年４月から、「ＥＭＳ-日本郵政」を装った偽メールが蔓延
　メール内容も巧妙化（正確な日本語に）
・以降、「領収書」、「見積ＦＡＸ依頼」など業務に関連した件名のメールが増える

「標的型メールに対する訓練」実施
添付ファイル開封率＝0.94%（2016.7）

・2016年7月から、ネットワーク・セキュリティ強化を実施
　・入口対策（*FireEye*）:「.exe、.js、.wsf、.scr形式と、この形式ファイルを含む.zip形式を受信拒否」➡ マルウェア感染端末低減

予防処置

RICOH
imagine. change.

FAX誤送信

誤送信がなくならない！！

↓

2人によるＦＡＸ番号の読み合わせを義務

↓

人的ミス減らず。。。

機器（MFP)セキュリティー機能を活用

①宛先強制確認
②ファクス宛先繰り返し入力（2回）
③直接入力制限（宛先表の登録された先のみ）
④同報送信禁止機能（宛先表の選択間違い）

予防処置

RICOH
imagine. change.

FAX受信

夜間・休日の受信ファックス放置

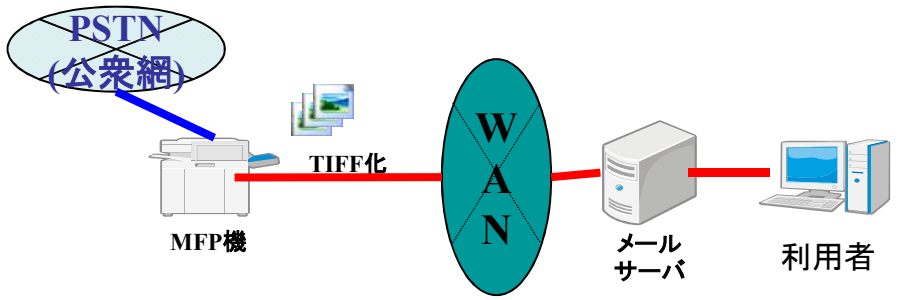
↓

清掃業者等の第三者に対するリスク

↓

FAX受信リスク軽減

①ストック機能の活用（メモリー内ストック）
②イメージ（PDF、TIFF化）によるメール転送



教育

RICOH
imagine. change.

情報セキュリティ教育の目的：情報セキュリティ意識の向上・浸透

情報セキュリティポリシーなどの組織内の情報セキュリティ上のルールを守る
風土作りが大切

教育

・全社統一教育　～「e-Learning」を利用して
　①グループ認証用の統一教材
　②弊社独自の教材（理解度テスト：有効性＝終了条件100点）

・臨時教育　～　環境変化による部門教育
　①採用、人事異動、事業所移転など

・【重要】新任推進責任者教育・・・責任者の意識改革が最重要
（組織の風土に影響がでる）

・実施状況確認　～「全社教育実施報告ＤＢ」による管理（依頼・督促）
・コミュニケーション　～「全社掲示板」による情報共有（随時）

グッドプラクティス

RICOH
imagine. change.

自発的推進活動

FAX誤送信、書類誤発送などミスがなくならない

遊びごころ

担当役員の発案→「意識」改革
トップダウンによる浸透

業務部門
“情報セキュリティ事故ゼロ「チャレンジ駅伝」”
自主的な動きが生れた。

※駅伝ルール：「１区＝１ヶ月」を担当した１組織が事故ゼロの”たすき”を繋いでいく

事故防止の役割	☑“たすき”担当（輪番）によるFAX番号等のWチェック体制 ☑朝礼での啓蒙、毎朝情報発信 ☑運用ルールの抜き打ちチェック ☑FAX番号のインターネット検索確認 ☑直送の推進（ハンド作業の廃止）

これからの活動

RICOH
imagine. change.

故意によるものは別として、
全ての業務が全自動（人の手が介在しない）にならない限り、インシデントはゼロにはならない。

人が介在しないように業務改善（無駄な作業の排除を含め）は進めるべきである。
ではあるが、最後は「人の意識」が重要。

如何に情報セキュリティを社内に浸透かせるか、
人の「意識」に自然と根付かせるかが永遠の課題。

RICOH
imagine. change.

RICOH
imagine. change.

Driving Sustainability for Our Future. 持続可能な社会を、ビジネスの力で。