物理的セキュリティから入る
情報セキュリティ

ーファシリティに対して、どのような要求があるのかー

平成24年（2012年）2月

リコージャパン株式会社
コンサルティング推進室 広口正之

RICOH

目次

本セミナーのねらい

RICOH

- ねらい
  - 情報セキュリティも、まず、物理的なセキュリティから始まります。
  - 東日本大震災を踏まえて、事業継続計画や情報セキュリティの観点から期待される、ファシリティマネジメントについて紹介します。
- 概要
  - ネットワーク的なセキュリティや、社員教育も必要ですが、まず、最初に物理的なセキュリティが必要です。
  - 物理的なセキュリティは強制的な対策
    ⇒ 外部侵入や、内部不正行為などを、効果的に防止可能。
  - 事業継続計画においても、代替拠点の確保、耐震対策、水害対策などが必要。
  - 要求事項を知らずに、建物や室内を設計してしまうと、あとになって設計変更の要求が来たり、顧客の満足度が低くなったりするかもしれません。

◆ 講師：広口正之

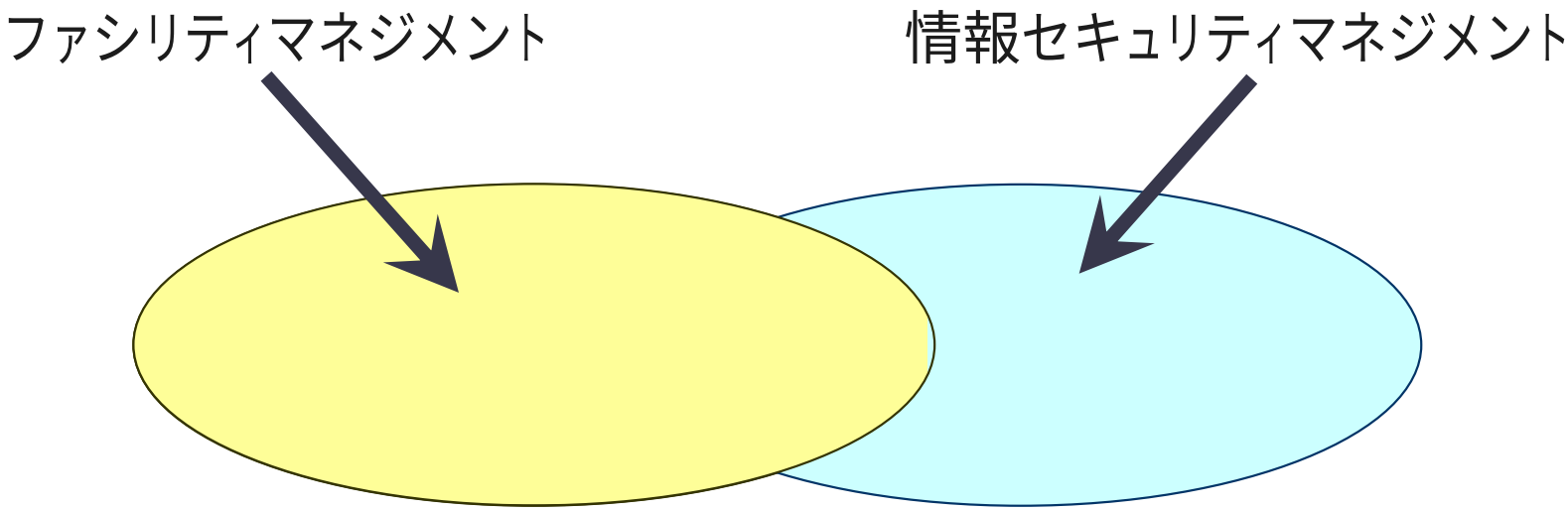
- 所属
  - リコージャパン株式会社　ソリューションマーケティング本部
    コンサルティング推進室 リーダー
- 職歴
  - 1982年から、コンピューターメーカーに勤務。プログラム開発、システム開発を経験。スタンフォード大学にて、コンピュータサイエンスを専攻。
  - 2002年から、セキュリティ専門会社にて、ＩＳＭＳ、侵入試験、セキュリティ監視センター、個人情報保護などに携わる。
  - 2005年から、リコーグループにて、情報セキュリティ、個人情報保護のコンサルティング、研修講師、世界各国の情報セキュリティ調査などを実施。
  - 2011年から、リコージャパン株式会社にて現職。
- 資格、委員、著書
  - CISSP、CISA、QSA、ISMS主任審査員、公認情報セキュリティ主任監査人、公認システム監査人、システム監査技術者、情報セキュリティアドミニストレータ、ネットワークスペシャリスト、データベーススペシャリスト、システムアーキテクトなど
  - 情報処理技術者試験委員（2006年4月～）。
  - 著書：「実際にあった46の情報セキュリティ事件」、リックテレコム
  - 共同執筆：「情報セキュリティインシデントに関する調査報告書」、JNSA

1. はじめに

RICOH

ファシリティとセキュリティ

- ファシリティとは
  - 「土地、建物、構築物、設備等」のこと。
    （ＪＦＭＡのウェブサイトによる）
- 情報セキュリティとは
  - 情報の機密性、完全性、可用性を維持すること。
    （国際規格 ISO/IEC 27001の定義）



◆ セキュリティとは

RICOH

- セキュリティ / Security
  - 原義： se(=without)+cure(=care)、心配する必要がない
  - 防衛、防護、保護、安全保障、警備
    - (例) 「セコム」は、「セキュリティ・コミュニケーション (Security Communication)」を略した造語
  - 安心、確信
  - 保証、担保
  - 証券 (セキュリティーズ)
    - 価値のある紙 (証券) で、その価値を保証している
    - (例) 野村證券は、Nomura Securities Co.,Ltd
  - 情報セキュリティ： 情報が防御されていること

2．物理的セキュリティの考え方

RICOH

◆ セキュリティは、「合せ技」で守る

RICOH

- 人的セキュリティ
  - 雇用契約、守秘義務契約、教育訓練
- 組織的セキュリティ
  - 組織体制の整備、社内規程の整備、定期的改善、事件事故対応
- 物理的セキュリティ
  - 入退館、盗難防止、物理的保護
- 技術的セキュリティ
  - 本人認証、アクセス制御、ログの採取と点検、ウイルス対策、不正アクセス対策、暗号化、監視

(注)　この分類は、経済産業省の個人情報保護法ガイドラインなどに基づいている。なお、3つに分類する考え方もある。

◆ 多層防御、縦深防御

RICOH

- 多層防御、縦深防御が望ましい。
  - 一つの強固な防衛ラインよりは、複数の防御ラインのほうが、突破しにくい。
  - 「マジノ線」は、ドイツ軍に突破された、
  - インドの安全の手引きが参考になる。
  - 外堀、内堀、石垣、城門、櫓、三の丸、二の丸、本丸なども、多層防御、縦深防御の例。

（松本城）

◆ マジノ線

RICOH

- マジノ線とは
  - 第一次世界大戦後の 1936年に、フランスがドイツ国境を中心に構築した要塞線である。当時のフランス陸軍大臣、アンドレ・マジノにちなんで命名された。
  - ベルギー、ルクセンブルクの国境から、地中海まで延びていた。

- ドイツ軍は、マジノ線を迂回した。
  - 第二次世界大戦開戦後の 1940年5月に、ドイツ軍は、マジノ線を迂回して、ベルギー、ルクセンブルグ付近のアルデンヌの森からフランス領内に侵攻した。
  - アルデンヌの森は自然の要害であったため、戦車は通れないと判断して、フランス軍は要塞を構築していなかった。
  - マジノ線を突破された英仏連合軍は、十分な反撃もできないまま敗退し、フランスはパリを放棄し、降伏した。

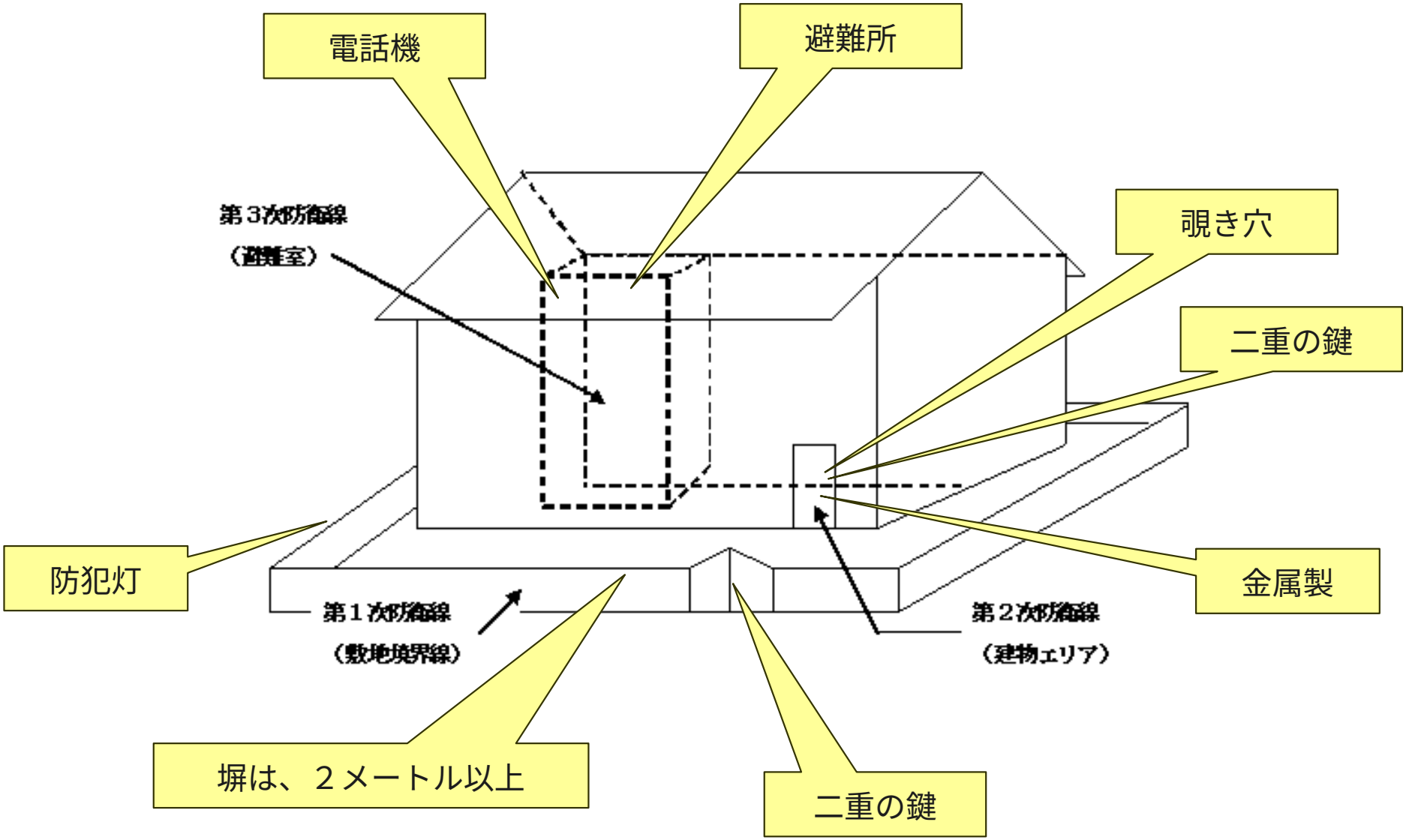
◆ インドの安全の手引き

RICOH

- 3つの防衛線による住居安全対策
  - (1) 住居敷地境界線、(2) 建物外周、(3) 建物内部の3カ所に物理的、段階的な防衛線を設け、これらに人的･物的両面から必要な対策をとり、外部からの侵入などの住居に対する各種の危険から防護するという考え方が極めて効果的です。
- 第1次防衛線
  - 外周の防衛線で、独立家屋の場合には敷地境界線、集合住宅の場合には共通の出入口 (ロビー玄関外側の扉) です。
- 第2次防衛線
  - 内周の防衛線で、独立家屋の場合は住宅建物地域 (建物エリア) の外周を構成する線、集合住宅の場合には住宅部分の外周を構成する防衛線です。
- 第3次防衛線
  - 内周の防衛線で、独立家屋、集合住宅いずれの場合も第2次防衛線内に設けた避難区域 (通常主寝室) に設定する防衛線です。

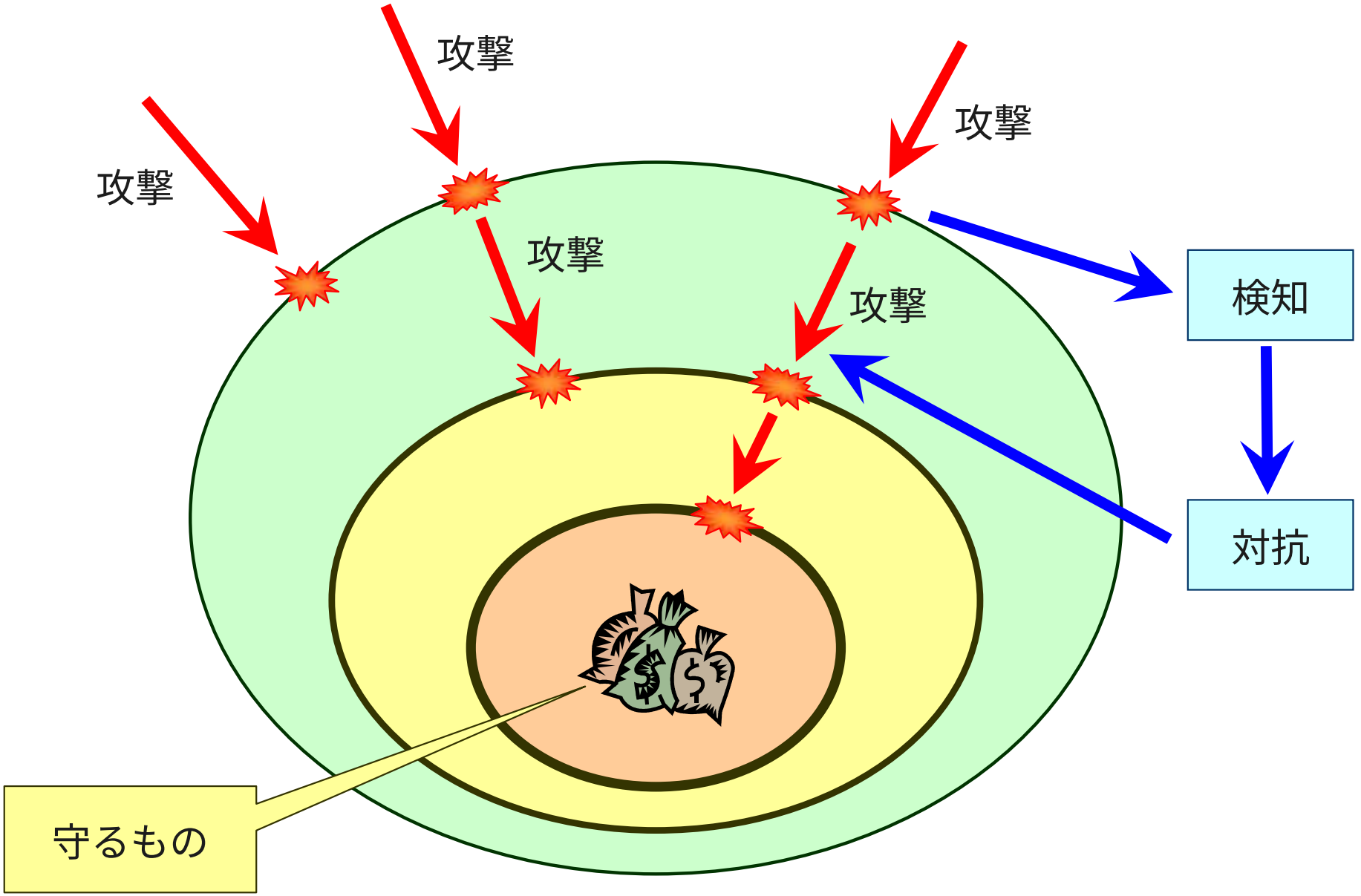
出典：外務省 海外安全ホームページ、在留邦人向け安全の手引き、在インド日本国大使館

◆ インドの安全の手引き



出典：外務省 海外安全ホームページ、在留邦人向け安全の手引き、在インド日本国大使館

◆ 多層防御、縦深防御

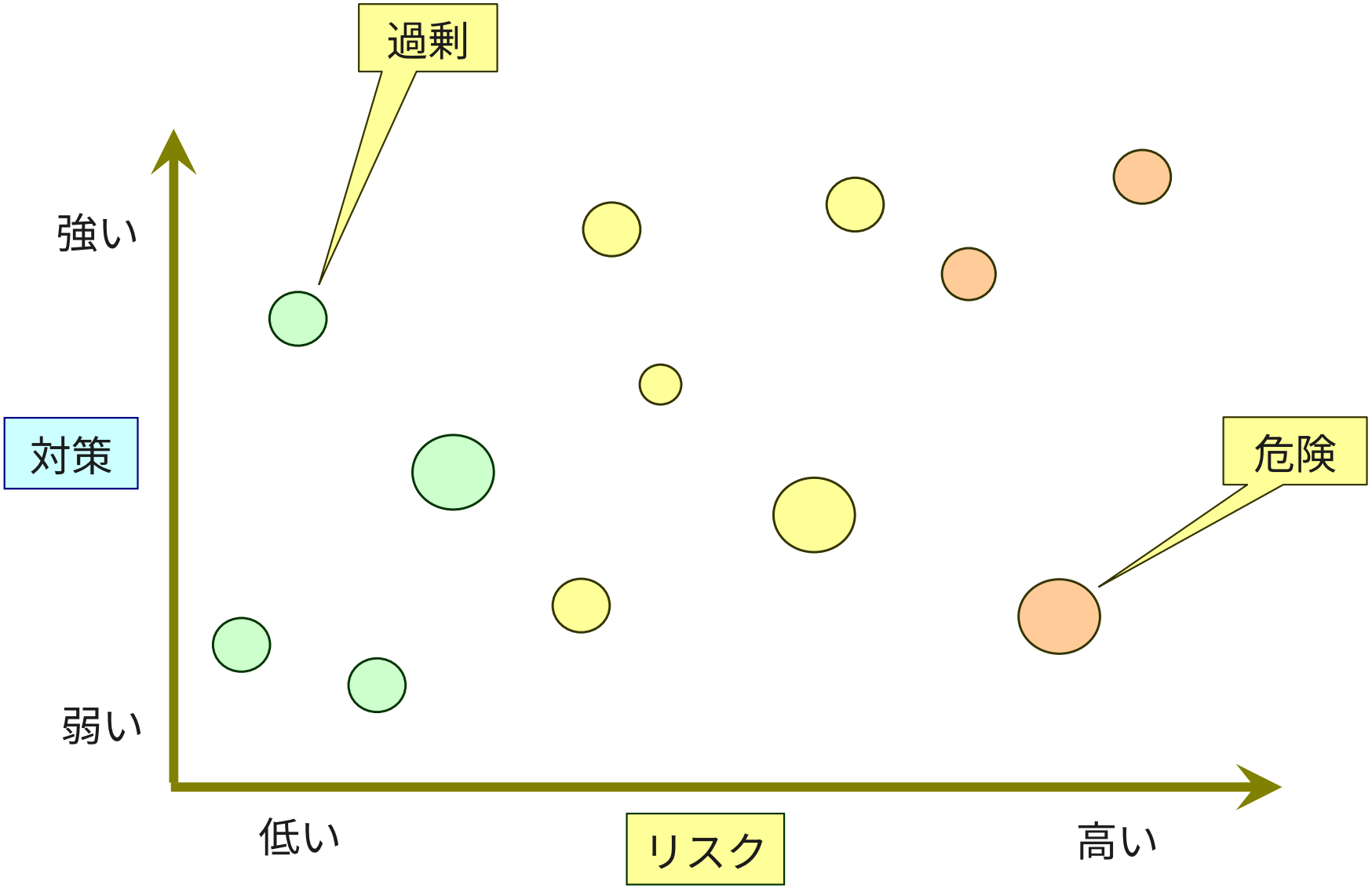


◆ グルーピング、ゾーンニング

RICOH

- リスクに応じた対策をとるべきである。
  - 対策は、少ないと危険であるが、やりすぎても無駄になる。
- しかし、対策を細分化しすぎると、対応しきれなくなる。
  - どの対策をとればよいのか、分かりにくい。
  - 運用の手間が増えて、大変。
- グループ、ゾーンに分けて、対策を考えるのがよい。
  - リスクも下げることができるし、手間も少ない。

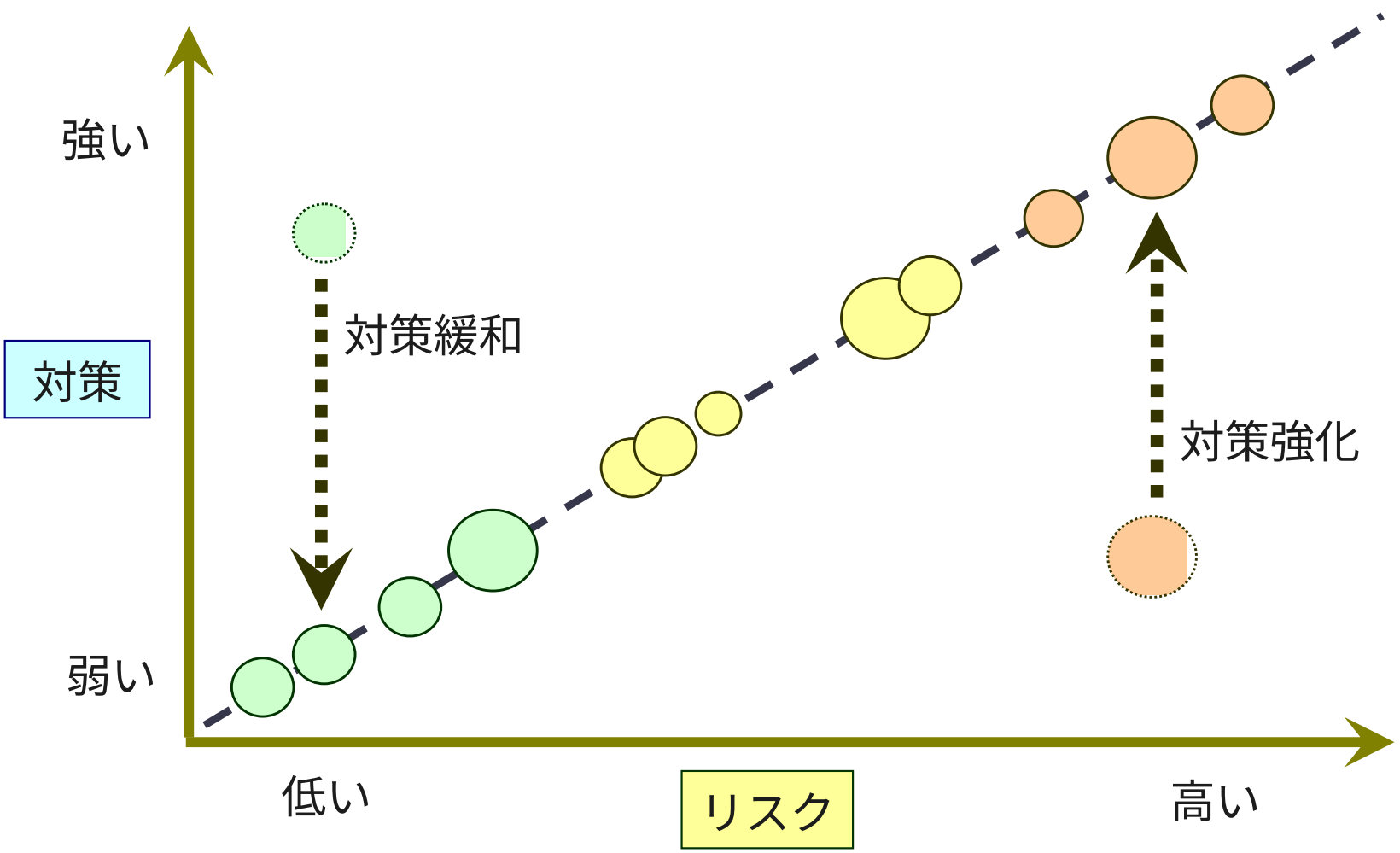
◆ 無秩序状態



◆ リスクに見合った対策をとるべき？

RICOH

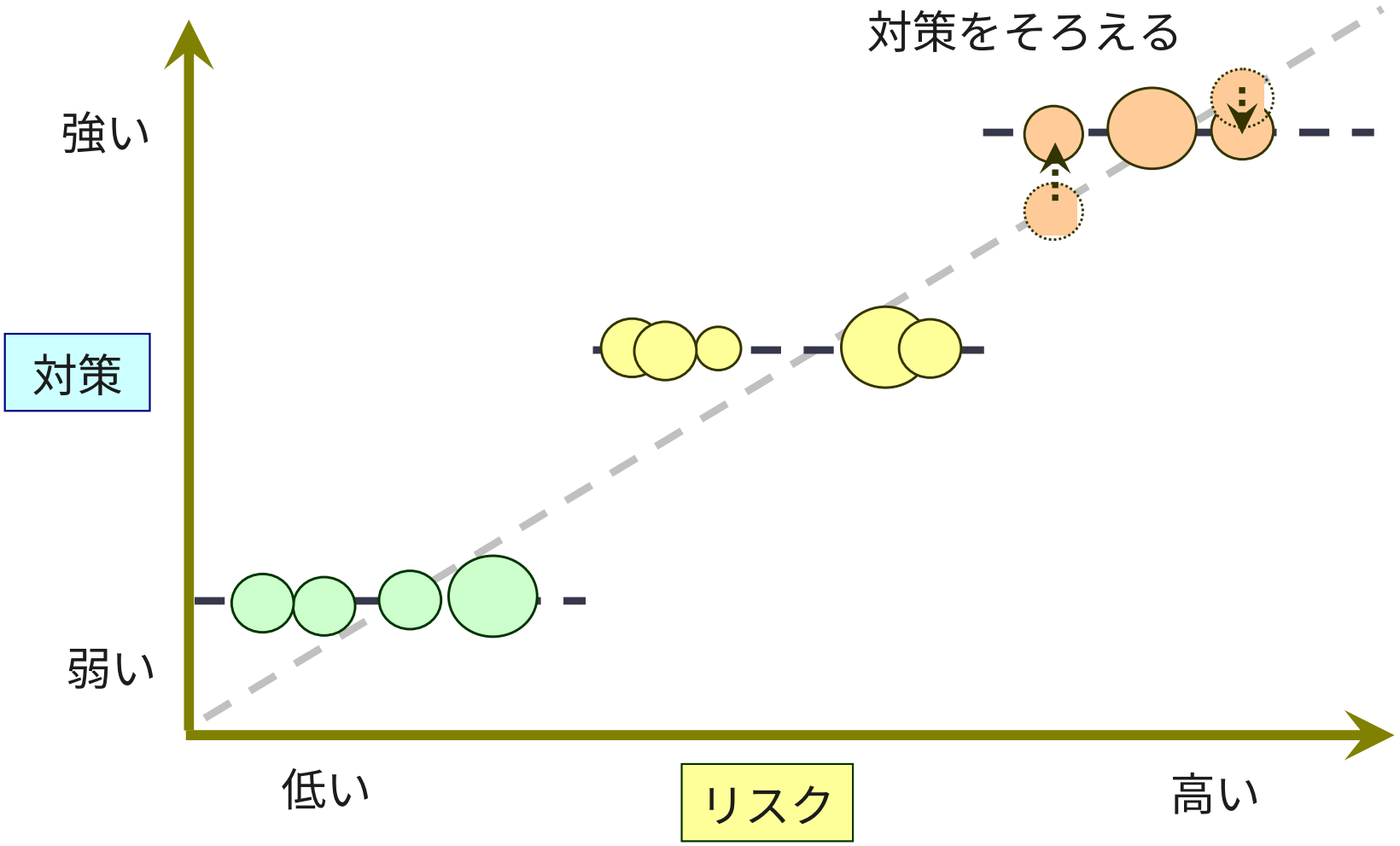
リスクに応じた対策をとると、過不足はないが...



◆ グループごとに対策を講じる

RICOH

グループに分けると、対応しやすくなる



3．国際規格

― お墨付きがあると、安心 ―

RICOH

◆ 国際規格 ISO/IEC 27001

RICOH

- 情報セキュリティの要求事項を記述したもの。
- 英国規格 BS7799-2 がベースとなっている
- もともとは、ベストプラクティス。
  - いろいろな組織で実施している対策を網羅したもの。
- 一般的な要求事項を記載している。
  - まったく該当しない場合は、除外できる。
  - どのレベルの対策を採用するのかについては、事業者が決めること。
- 準拠すると、「ＩＳＭＳの認証」が取得できる。
  - ２０１２年１月１３日現在、３９６５組織が取得。

◆ 物理的セキュリティも含まれる

RICOH

- 全体で、１３３の対策（管理策）が要求されている。

5	セキュリティ基本方針
6	情報セキュリティのための組織
7	資産の管理
8	人的資源のセキュリティ
9	物理的及び環境的セキュリティ
10	通信及び運用管理
11	アクセス制御
12	情報システムの取得、開発及び保守
13	情報セキュリティインシデントの管理
14	事業継続管理
15	順守

(A.9.1.1) 物理的セキュリティ境界

情報や、情報処理設備の存在する領域を保護するために、物理的セキュリティ境界を設けなければならない。

- 実施例
  - 建物や、敷地境界を、強固にする。
  - かんぬき、警報装置、錠前などを設ける。
  - 不在時に、ドアと窓を施錠する。
  - 有人受付を設ける。
  - 防火扉を設ける。
  - 物理的な侵入者検知システムを設置する。

（規格には著作権があるため、規格の表現を変更しています。原文は規格をご覧ください。）

(A.9.1.2) 物理的入退管理策

セキュリティを保つ必要がある領域は、許可された人だけがアクセスできるよう、適切な入退管理対策によって保護しなければならない。

- 実施例
  - 訪問者の入退の日付、時刻を記録する。
  - 認証システムを設置する。
    - 暗証番号錠、物理鍵、磁気カード、ICカード、生体認証
  - 社員、職員、訪問者が、証明書などを常時表示する。
  - 重要な領域への立ち入りは、必要最小限にする。

（規格には著作権があるため、規格の表現を変更しています。原文は規格をご覧ください。）

◆ 多要素認証　(三要素認証、二要素認証)

RICOH

- What you have、所有物、持っているもの
  - 物理鍵、磁気カード、ICカード、社員証、パスポート
- What you know、記憶、知っていること
  - 暗証番号 (PIN) 、パスワード、画像、位置 (パターン)
- What you are、生体、存在そのもの
  - 指紋、掌形、網膜、虹彩、顔、静脈、声紋、耳形、DNAなど
- 多要素認証
  - 複数の要素を組み合わせると、安全性が高くなる。

(A.9.1.3) オフィス、部屋及び施設のセキュリティ

敷地や、建物、部屋に対する物理的なセキュリティ対策を検討し、構築しなければならない。

- 実施例
  - 安全衛生の規則を整備する。
  - 重要な領域には、一般者の来訪がないようにする。
  - できれば、建物が目立たないようにする。表示は最小限にする。
  - 重要な領域は、案内板に表示しない。
  - 一般の人が、内線電話帳を閲覧できないようにする。

（規格には著作権があるため、規格の表現を変更しています。原文は規格をご覧ください。）

(A.9.1.4) 外部及び環境の脅威からの保護

火災や、洪水、地震、爆発、テロ行為などの自然災害、または、
人為災害による被害を受けないよう、物理的な保護対策を検討し、
採用しなければならない。

- 実施例
  - 危険物、可燃物は、重要な領域から遠ざける。
  - 予備機は、本番機から離れた場所に設置する。
  - バックアップデータは、実データから離れた場所に保管する。
  - 適切な消火器を配備する。

（規格には著作権があるため、規格の表現を変更しています。原文は規格をご覧ください。）

◆ 消火方式

RICOH

- 粉末式、強化液式、泡式
  - 消火後、電気機器を腐食、絶縁劣化させるおそれがある。
- ガス式
  - ハロン、フロン：温室効果ガスなので、原則使用禁止
  - 炭酸ガス、CO_2：窒息するおそれがある。
  - 代替フロン：FM200など
- スプリンクラー
  - サーバ室、マシン室では、できるだけ避けたい。
  - ウェットパイプよりは、ドライパイプがよい。
- 水
  - 純水式、ミスト式の消火器もある。

(A.9.1.5) セキュリティを保つべき領域での作業

RICOH

セキュリティを保つ必要がある領域における作業について、
物理的な保護対策や保護方針を検討し、採用しなければならない。

- 実施例
  - 重要な領域は、知る必要のある人にしか、知らせない。
  - 重要な領域の作業には、必ず、監督者を置くようにする。
  - 重要な領域が無人のときは、物理的に施錠し、定期的に点検する。
  - 画像、映像、音声などの記録装置の持ち込みは、原則的に禁止する。

（規格には著作権があるため、規格の表現を変更しています。原文は規格をご覧ください。）

(A.9.1.6) 一般の人の立寄り場所及び受渡し場所

一般の人が立ち寄る場所や、立ち入ることができる場所は、管理しなければならない。また、このような場所には、情報処理設備はできるだけ設置しないこと。

- 実施例
  - 建物外部からの受け渡し場所へのアクセスを制限する。
  - 受け渡し場所は、配達要員が無関係の領域にアクセスしないですむようにする。
  - 受け渡し場所の内部ドアが開いているときは、外部ドアは閉める。
  - 入荷物は、持ち込み時に安全性を確認する。
  - 入荷物を持ち込むときに、記録を付ける。
  - できれば、入荷場所と、出荷場所を分離する。

（規格には著作権があるため、規格の表現を変更しています。原文は規格をご覧ください。）

(A.9.2.1) 装置の設置及び保護

RICOH

情報装置は、環境上の脅威や、災害、不正アクセスなどのリスクが低下するように設置、または、保護しなければならない。

- 実施例
  - 作業領域へのアクセスは、必要最小限にする。
  - のぞき見ができないようにする。
  - セキュリティレベルの高いものと低いものを混在させない。
  - 盗難、火災、爆発、煙害、水害、塵埃、振動、化学的汚染、電力供給妨害、通信妨害、電磁波放射、破壊などのリスクに対策を講じる。
  - コンピュータ周辺で、飲食、喫煙をしない。
  - 温度、湿度などの環境条件を監視する。
  - 落雷の影響から保護する。
  - 作業現場などの環境から保護する。

（規格には著作権があるため、規格の表現を変更しています。原文は規格をご覧ください。）

(A.9.2.2) サポートユーティリティ

情報装置は、電源、通信回線、ガス、水道などのサポート
ユーティリティの不具合による影響から保護しなければならない。

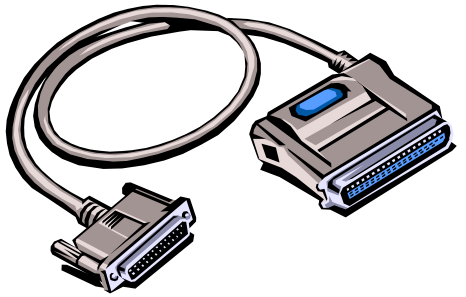
- 実施例
  - 無停電電源装置 (UPS) を設置する。
  - 非常用発電機を設置する。
  - 非常停止用の緊急スイッチを設ける。
  - 警報システムを導入する。
  - 提供者との間に、複数の連絡手段を確保する。

（規格には著作権があるため、規格の表現を変更しています。原文は規格をご覧ください。）

(A.9.2.3) ケーブル配線のセキュリティ

データ通信ケーブルや、電源ケーブルの配線は、通信傍受や、
ケーブルの損傷から保護しなければならない。

- 実施例
  - ケーブルを床下に配線する。天井に配線する。
  - 電線管路を使用する。
  - 電源ケーブルと、通信ケーブルを隔離する。直角交差させる。
  - 誤接続防止のために、ケーブルにラベルを付ける。
  - 配線表を作成する。
  - ケーブルに接続されている機器を探索する。



（規格には著作権があるため、規格の表現を変更しています。原文は規格をご覧ください。）

4．事業継続計画

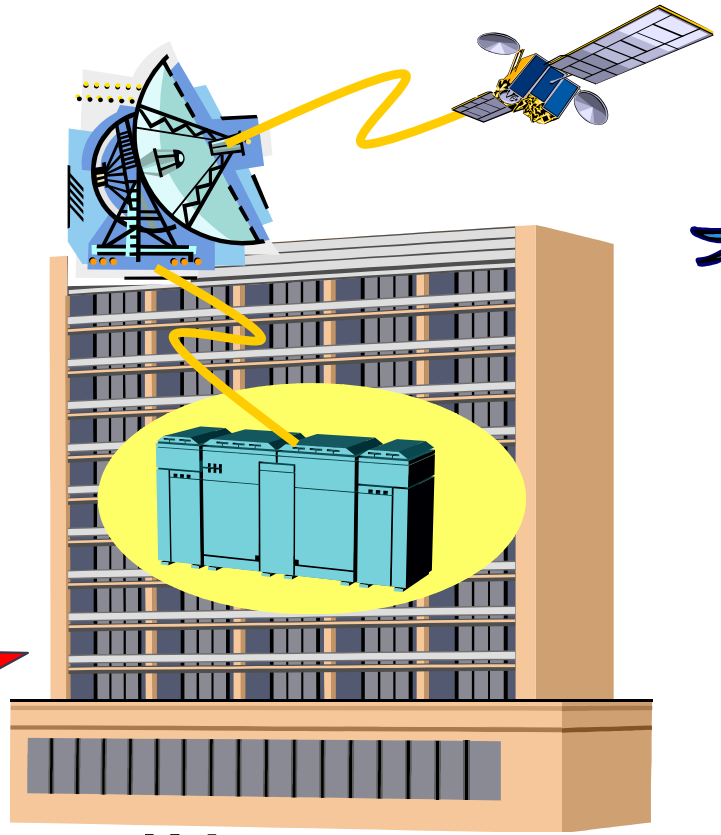
RICOH

◆ 事業継続の妨害要因

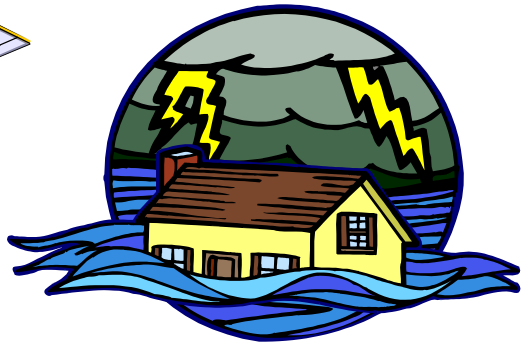
RICOH

事業継続を妨害する要因は、地震だけではありません。

火災対策は？



情報システムのバックアップ対策は？



水害対策は？

サイバーテロ対策は？

地震対策は？

◆ 事業の中断を引き起こす、さまざまな事象

RICOH

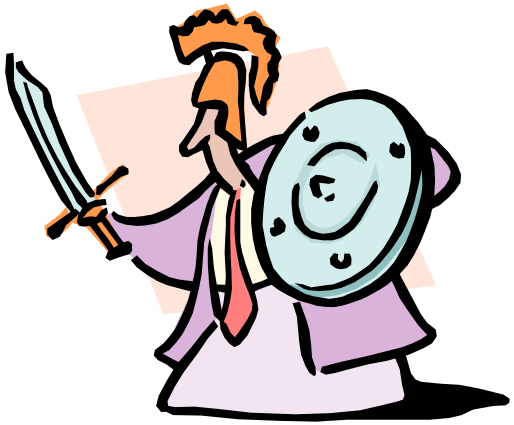
1．広域に被害を及ぼす事象
- ・地震、津波
- ・大規模風水害
- ・疫病

2．局所的に被害を及ぼす事象
- ・火災
- ・停電
- ・爆破テロ

3．情報システム単独の障害
- ・サイバーテロ
- ・ハードウェア故障
- ・アプリケーション障害
- ・コンピュータウィルスの蔓延

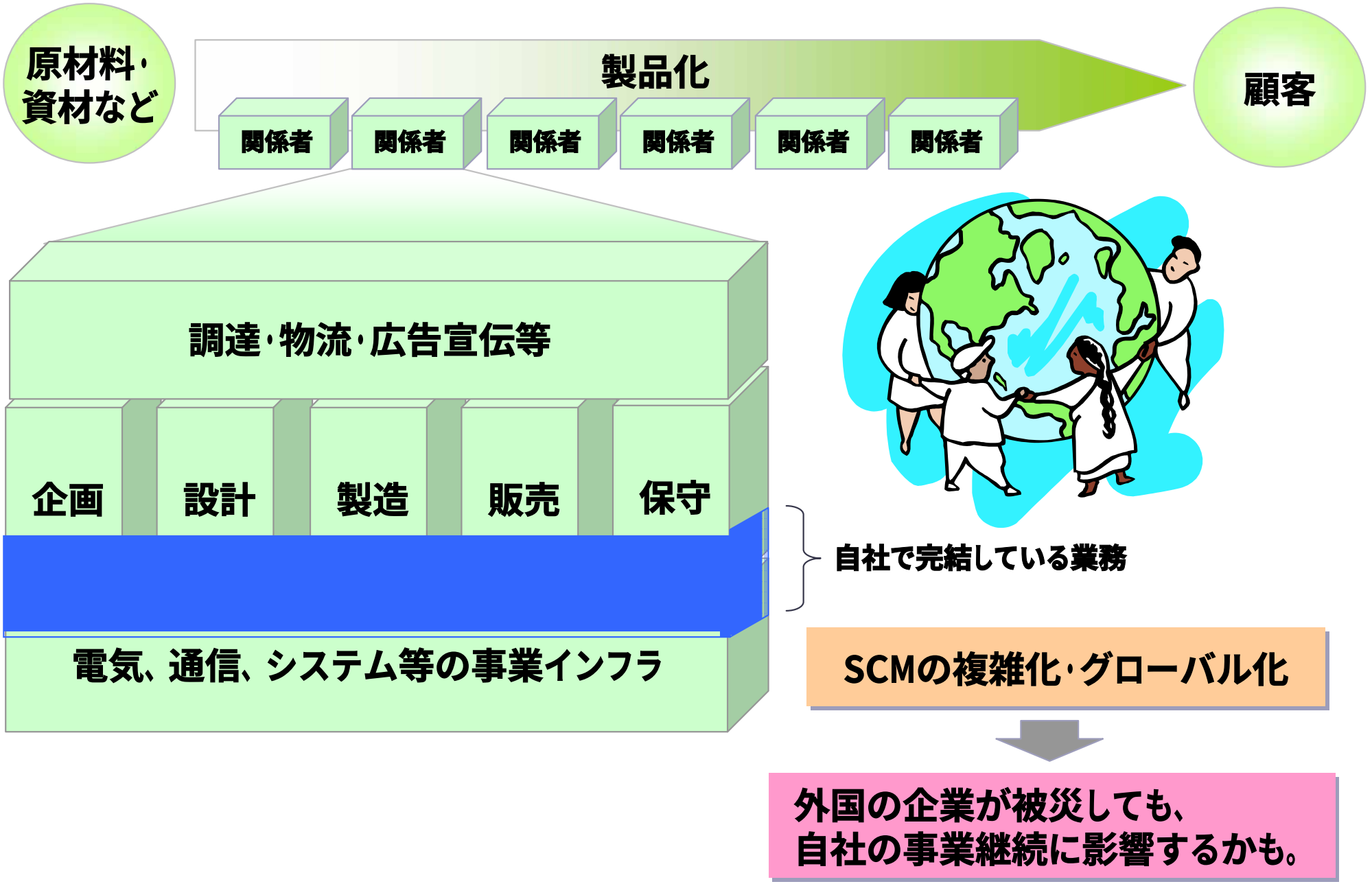
4．経営資源の急激な不足
- ・材料・部品等の供給の停止（委託先の事業中断など）
- ・要員の不足（事故、疾病など）
- ・物流の停滞
- ・財務の悪化
- ・市場の急激な変化や停滞

5．その他
- ・法的要求・社会的要求の変化
- ・食品や薬品に対する安全性の要求

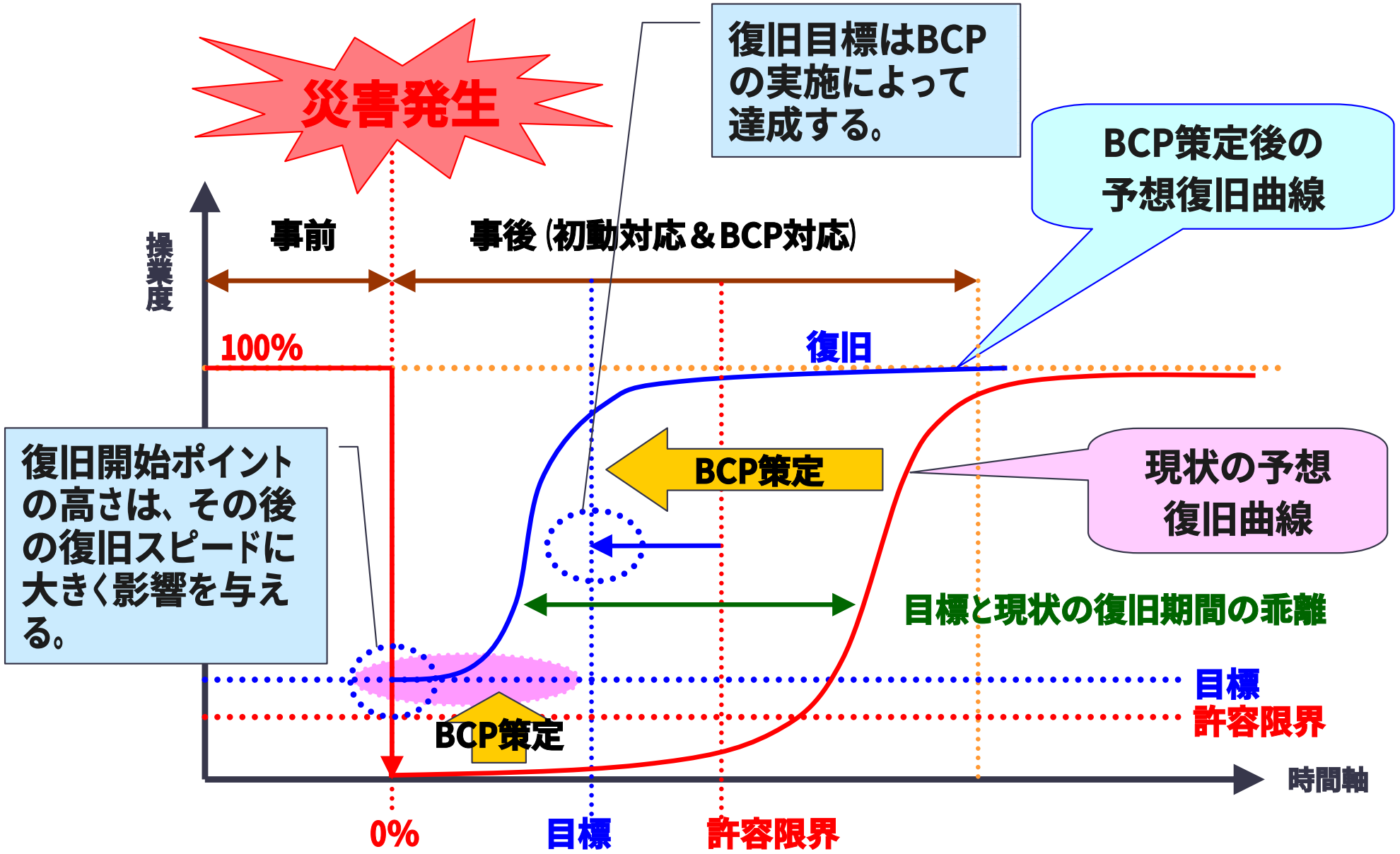


◆ BCPとSCM (サプライチェーンマネジメント)

RICOH



◆ BCPの基本概念



参考：内閣府「事業継続ガイドライン第二版」平成21年11月

◆ 復旧期間ごとの再配置戦略の概要

RICOH

担当 / 復旧時間	社内	契約	臨時
月単位	・再構築又は再配置	・拡張商用復旧サイト契約(許可される場合)	・再建築、賃貸、又は購入
週単位	・サイト上のプレハブ建築 ・他の用途の設備を活用	・復旧サイトでの拡張 ・契約したプレハブ及び移動ユニット	・設備付きのオフィス ・下請手続き
日単位	・社内復旧サイト ・既存設備の活用 ・在宅勤務	・商用復旧サイト ・相互契約 ・移動施設 ・下請手続き	・管理されたオフィス(利用可能な場合)
時間単位	・多様な場所に他の業務からスタッフを移動する	・契約商用復旧サイトのみに対する小さなチームの再配置＊	・なし
即時	・各活動に対する多様な場所	・商用復旧サイトのみで契約されたITの「切り換え」を開始	・なし

＊ 数時間以内に利用可能になるが、ロジステック及び福利の問題のために、業務を1日又は2日以内に再開できる可能性は低い。

出典： 事業継続マネジメント(BCM)実践ガイドライン

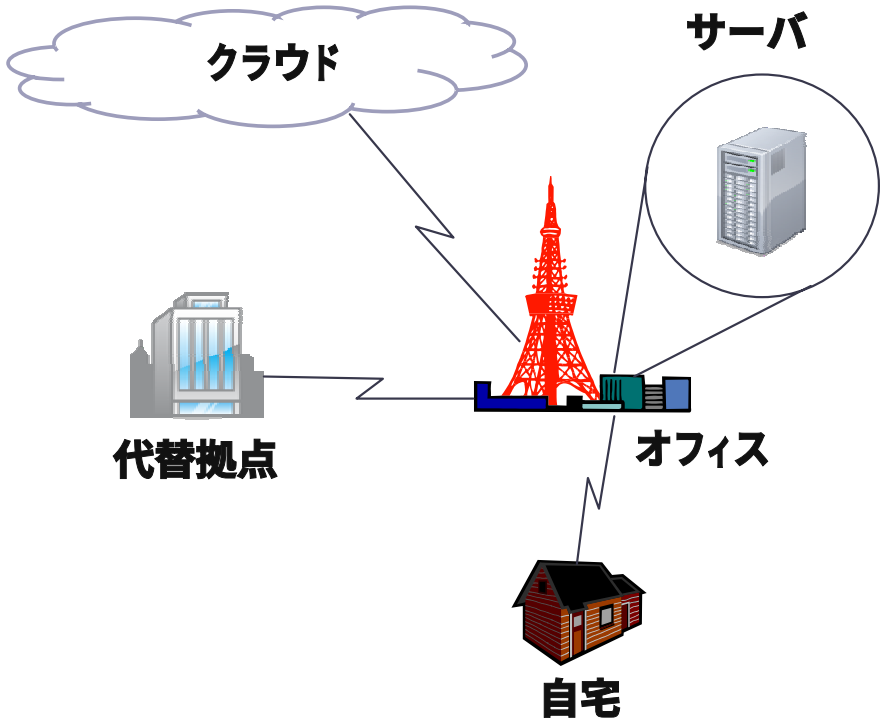
◆ ＢＣＰにおける、物理的対応

RICOH

- 現拠点の強化
  - 建物の耐震補強
  - サーバや設備の固定、転倒防止
  - 電源対策、水害対策
- 拠点の移転
- 他拠点の強化
  - 代替拠点としての機能を持たせる
  - フロアレイアウト変更、通信回線強化
  - サーバ、パソコン設置、机、椅子の追加
- 新拠点の確保
  - ホットサイト、ウォームサイト、コールドサイト

◆ ＢＣＰの派生ビジネス

- 代替拠点契約･工事
  - ホットサイトや、コールドサイトの確保
- 通信回線契約･工事
  - 通信手段の確保
- サーバ耐震･免震工事
  - 地震対策
- サーバリモートアクセス
  - 自宅勤務
- クラウドコンピューティング
  - バックアップ、リモートアクセス
- 媒体保管サービス
  - バックアップの安全な保管



お知らせ

RICOH

■ コピー機だけではありません

- ■ 事業継続計画（ＢＣＰ）策定支援・体制構築支援
- ■ ＩＳＭＳ構築・認証取得コンサルティング
- ■ プライバシーマーク認定取得コンサルティング
- ■ ＰＣＩ ＤＳＳ評価、試験、構築コンサルティング
- ■ 審査員研修、監査人研修
  - ■ プライバシーマーク審査員研修、ＩＳＭＳ審査員研修
  - ■ 公認情報セキュリティ監査人研修、ＢＣＭＳ審査員研修
- ■ 情報セキュリティ監査・レベルチェック実施
- ■ ＩＴコンサル（クラウド導入支援、業務改善、ＲＦＰ作成）
- ■ ものづくり（人材育成、整理整頓、５Ｓ、工程改善、環境）

■ コンサルティング、研修実績

■ 官公庁、地方自治体、金融、情報、通信、医療、印刷、教育、サービス、製造、不動産、石油等の各分野におけるコンサルティング、研修実績があります。

◆ 連絡先

RICOH

- 会社：　リコージャパン株式会社
- 所属：　ソリューションマーケティング本部　コンサルティング推進室

- 所在地：104-0061
  東京都 中央区 銀座 6-14-6
  第2リコービル　3F

- Mail:
  masayuki_hiroguchi@ricoh-japan.co.jp

- Phone:
  03-6278-0751