第5回情報セキュリティ格付セミナー

オール富士ゼロックスの情報セキュリティ取組み

2017年7月7日

富士ゼロックス株式会社
総務部　情報セキュリティセンター

ご説明内容

1. 情報セキュリティ対応体制

2. 未然防止

3. 有事対応

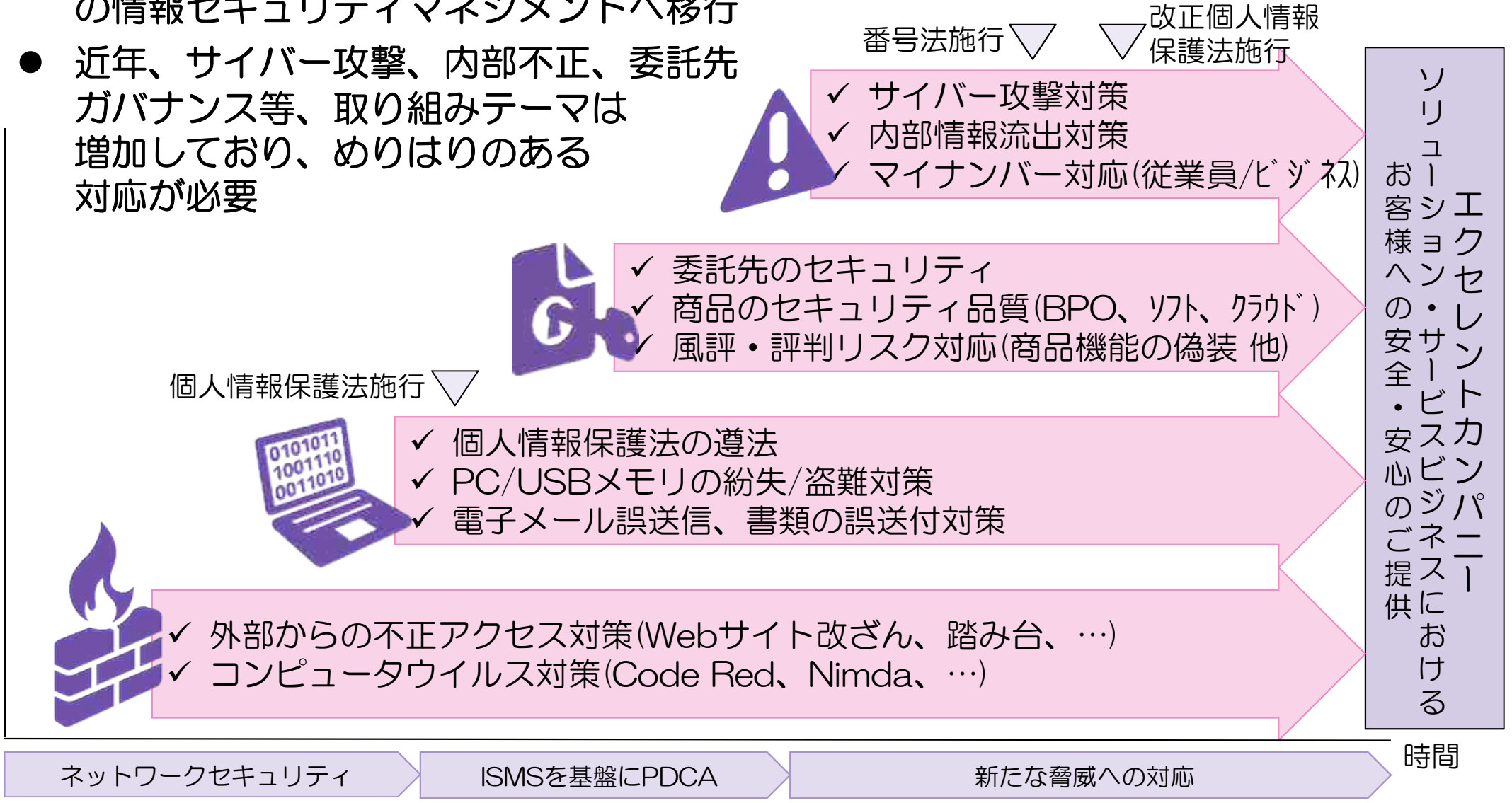
情報セキュリティ対応体制

- ✓ 情報セキュリティ課題は増える一方なので、優先度を決めた対応が必要
- ✓ 単一部門だけでは情報セキュリティの対応は困難であり、組織間連携が必要
  (情報セキュリティ統括部門に加えて、情報システム、法務、広報、品証、…)
- ✓ 情報セキュリティへの対応は、「未然防止」と「有事対応」の両面の視点が必要

FUJI Xerox

情報セキュリティ・リスクの変化への対応

- 個人情報保護法施行(2005年)をきっかけに、IT主体の取り組みから全社をあげての情報セキュリティマネジメントへ移行
- 近年、サイバー攻撃、内部不正、委託先ガバナンス等、取り組みテーマは増加しており、めりはりのある対応が必要

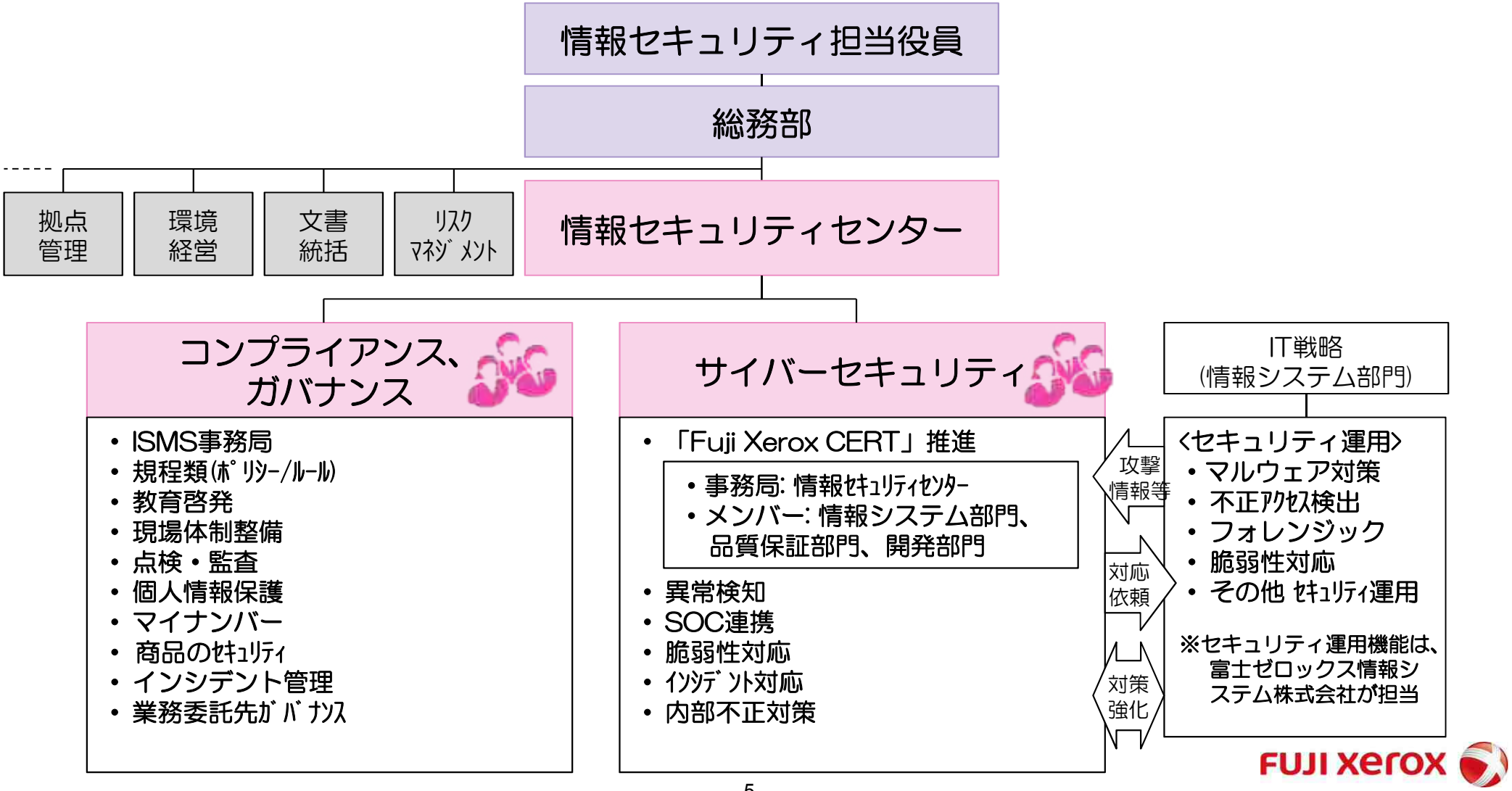


情報セキュリティセンターの取組みテーマ

- 情報セキュリティ対策は、「外部の脅威」と「内部の脅威」を想定し、これらに「未然防止策」と「有事対応」の両面から対策を立案

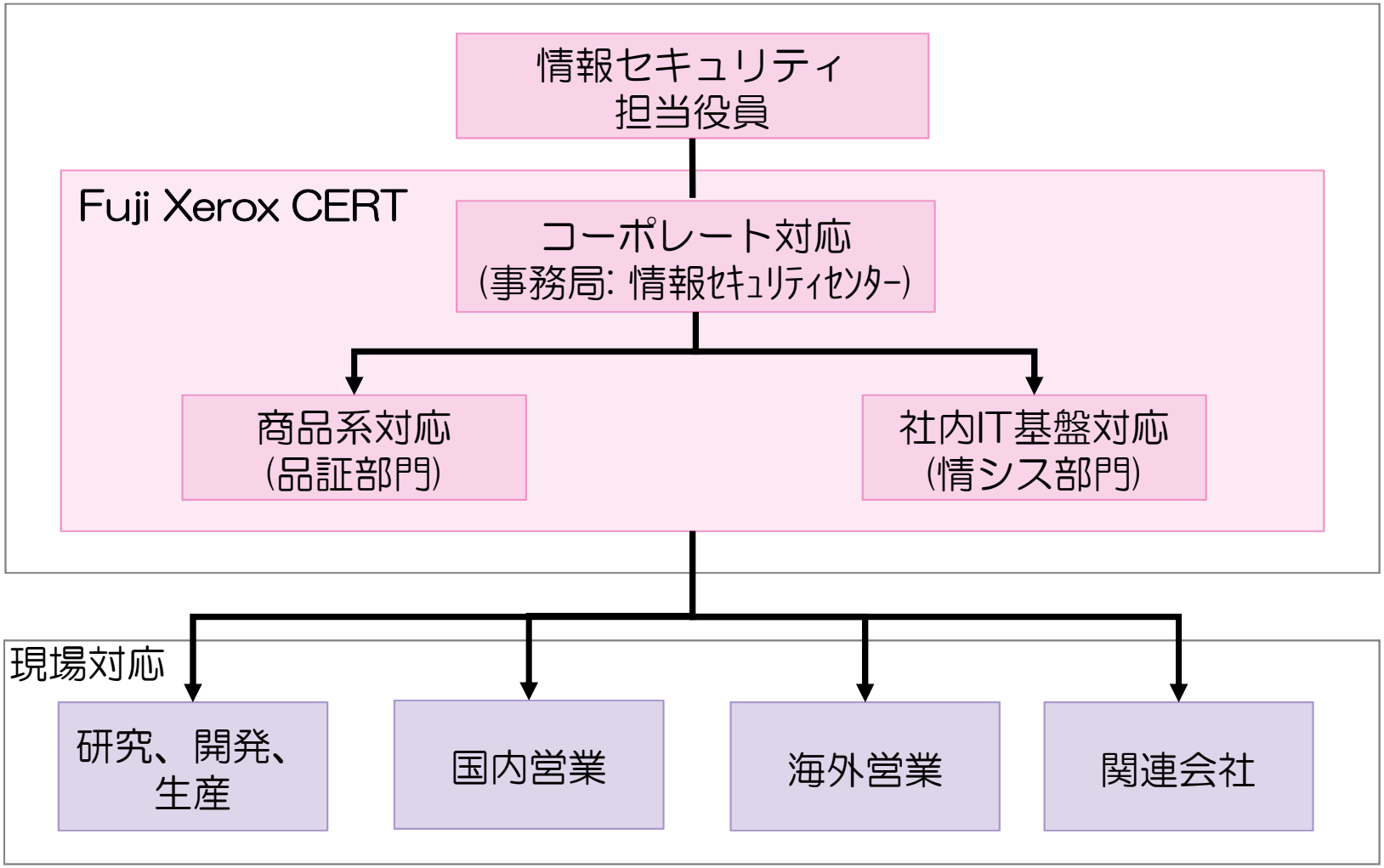
情報セキュリティ体制

- 情報セキュリティは、総務部に設置した「情報セキュリティセンター」が全社を統括
  個人情報保護、ヒューマンエラー、委託先管理、サイバーセキュリティ等、
  情報セキュリティ全般を担当



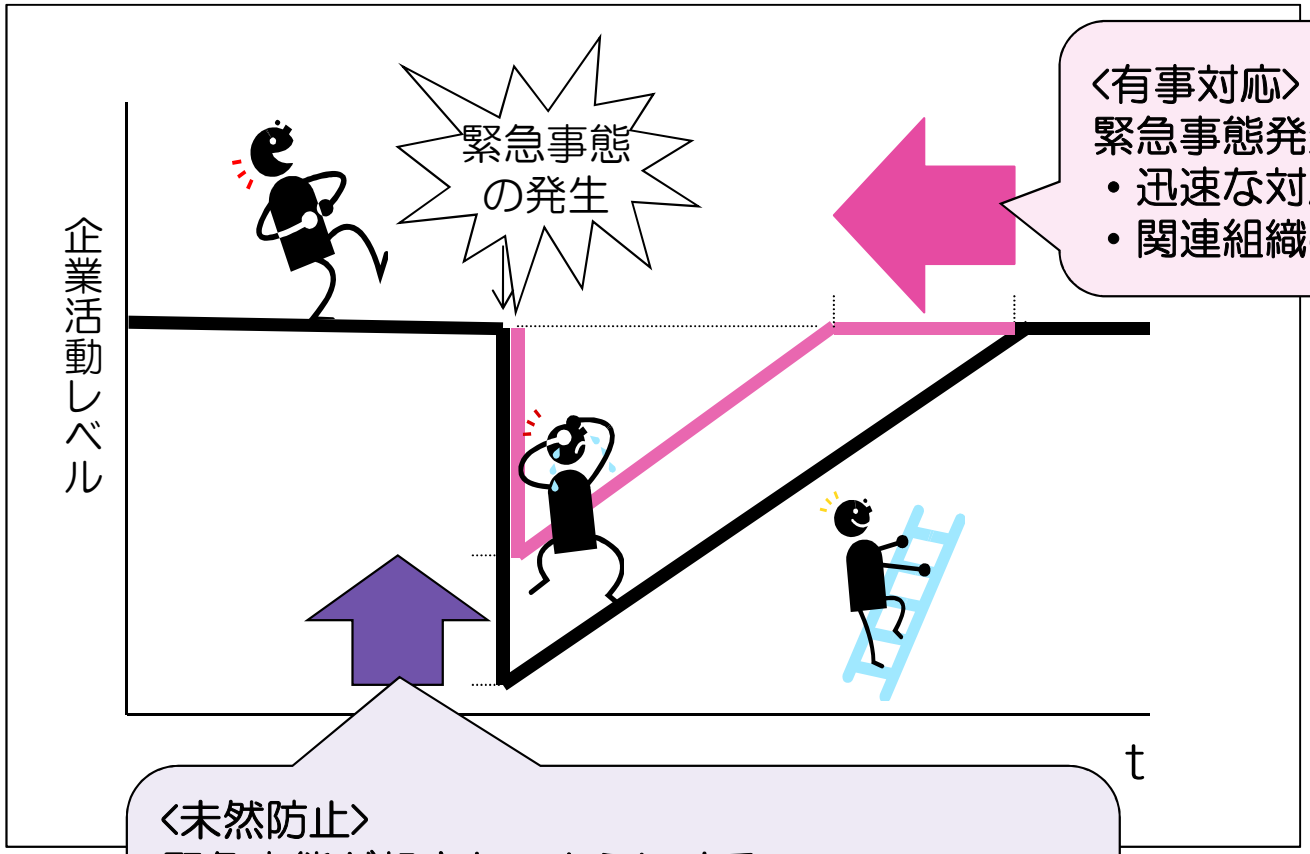
サイバー攻撃への連携対応体制

- 「情報セキュリティセンター」を核としたバーチャル組織による「Fuji Xerox CERT」を運用し、インシデント対応、緊急脆弱性対応等を担当
- 「Fuji Xerox CERT」は、社外組織とも情報連携



情報セキュリティ・リスク対応の考え方

- 万が一の緊急事態発生時に適切に対応することは当然のこと、
  リスクが顕在化しないよう平時からコントロールし、経営リスクの低減に努める。



〈有事対応〉
緊急事態発生時に円滑に対応する
・迅速な対応とエスカレーション
・関連組織の知恵を結集

〈未然防止〉
緊急事態が起きないようにする、
起きても影響が最小限となるようにする
・潜在リスクを抽出する
・リスク強化策を推進する(教育、訓練等)　他

平時と有事における情報セキュリティ取り組み

- 情報セキュリティは、リスクマネジメントの重要なテーマとして、「未然防止」と「有事対応」を推進

未然防止

- ✓ オール富士ゼロックス・リスク抽出
  (重大リスクにフォーカスした全社対応)
- ✓ 情報セキュリティ連絡会
  (国内・海外の現場組織の情報セキュリティ推進者との会議体)
- ✓ 教育・啓発
  (eﾗｰﾆﾝｸﾞ、新卒/ｷｬﾘｱ採用教育、階層別教育)
- ✓ 監査・点検
  (高リスクテーマについて第三者評価の受審)
- ✓ 情報セキュリティレビュー
  (2回/年、経営に情報セキュリティリスクへの対応状況を報告)

有事対応

- ✓ インシデント対応
  - 速報(2時間以内報告)
  - リスク対策検討会
  - 経営へのエスカレーション(緊急連絡)
  - 事故報告管理システムによる記録管理
- ✓ 脆弱性対応
  - 外部からの脆弱性情報の収集
  - 重要性判断に基づく対応指示
    (情報提供、通常、重要)
- ✓ 情報セキュリティの見える化
  (週報、月報としてインシデント情報を経営に報告)
- ✓ 訓練
  (従業員向け訓練とFuji Xerox CERT訓練)

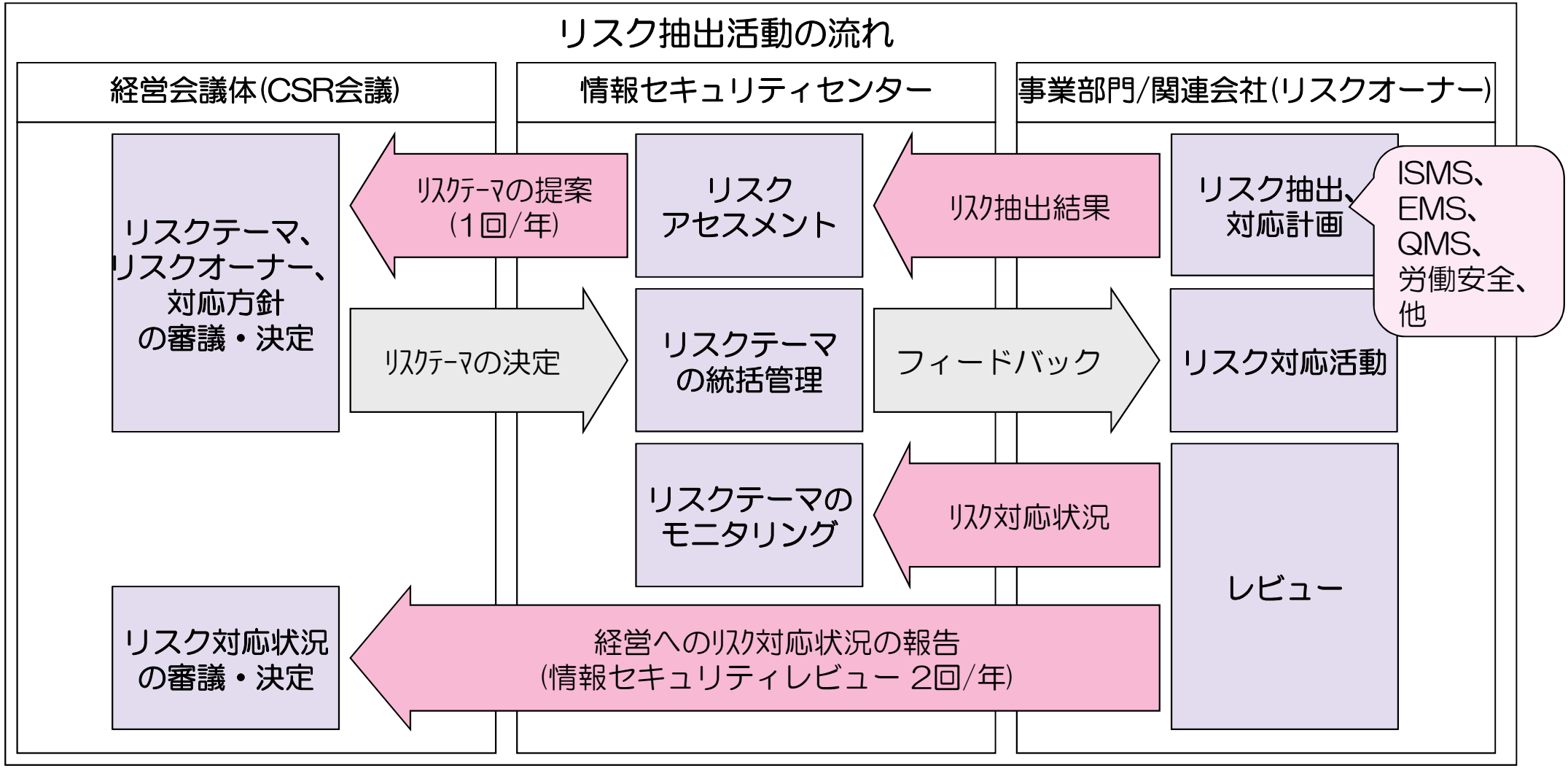
未然防止

- ✓ 情報セキュリティリスクの洗出しを実施し、重点取り組みテーマを決めている
- ✓ 事業を遂行している現場組織(従業員)と共に情報セキュリティを推進
- ✓ 情報セキュリティは他人事ではないと感じてもらう教育・啓発の工夫
- ✓ 内部監査、ISMS審査に加え、社外からセキュリティ耐性を評価してもらう

FUJI Xerox

〈未然防止〉 情報セキュリティ・リスクの抽出

- 毎年オール富士ゼロックス全組織でリスク抽出活動を実施し、
  この中で情報セキュリティの重要なリスクを抽出



〈参考〉リスク抽出支援システム

- リスク抽出項目の変化への対応と入力工数の効率化を図るためにWebシステムを利用

リスクコントロールマトリクスWEB

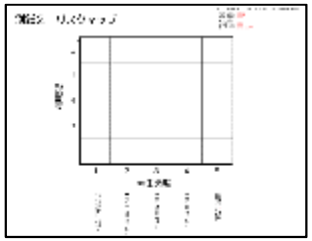
他部門の結果が
見えないようロック

結果をエクセルで
表示可能

昨年データの
コピーが可能

リスクマップの自動作成

リスクマップ



リスク抽出承認シート作成支援

前年度入力データの閲覧が可能

〈未然防止〉情報セキュリティ会議体、情報セキュリティレビュー

- 半期毎に経営会議体で情報セキュリティレビューを開催、
  国内外の現場の情報セキュリティ推進者との会議体(情報セキュリティ連絡会)を開催

〈情報セキュリティ会議体〉

CSR会議
(議長: 情セ担当役員)

情報セキュリティレビューを開催し、リスクへの対応状況を報告

事務局
(情報ｾｷｭﾘﾃｨｾﾝﾀｰ)

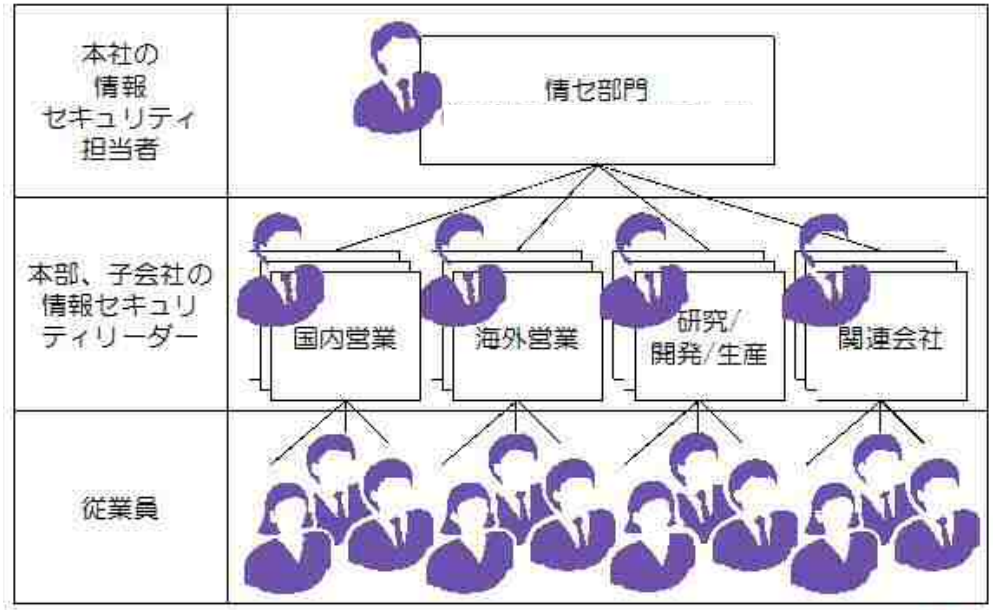
リスク対策検討会

インシデント発生時に関係者を緊急招集し、対応策を協議

情報セキュリティ連絡会

現場のセキュリティ推進責任者をメンバーに情報共有、課題を議論

〈情報セキュリティ連絡会体制〉



〈未然防止〉 情報セキュリティ教育・啓発活動

- 全従業員教育、階層別教育、ハンドブックやポータルサイトを通じての啓発活動

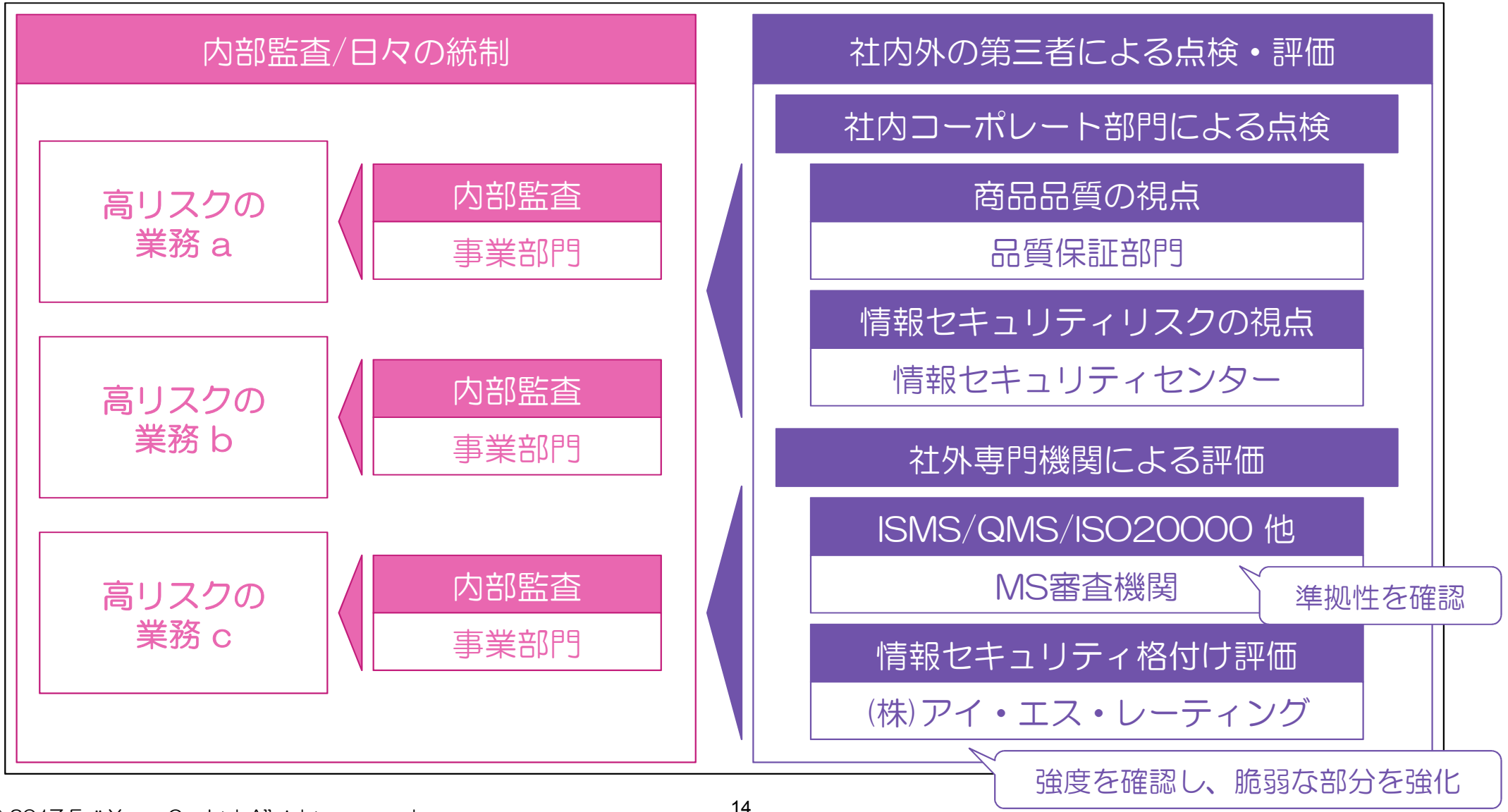
サイバーセキュリティポータルサイト

ビデオによる学習(事故からの学習)

ハンドブックの展開

<未然防止> 監査・点検(第三者評価)

- 情報セキュリティリスクの視点から重要な業務については、内部監査に加え、社外の目による評価・指摘を受け改善し、設定したセキュリティ目標を目指す



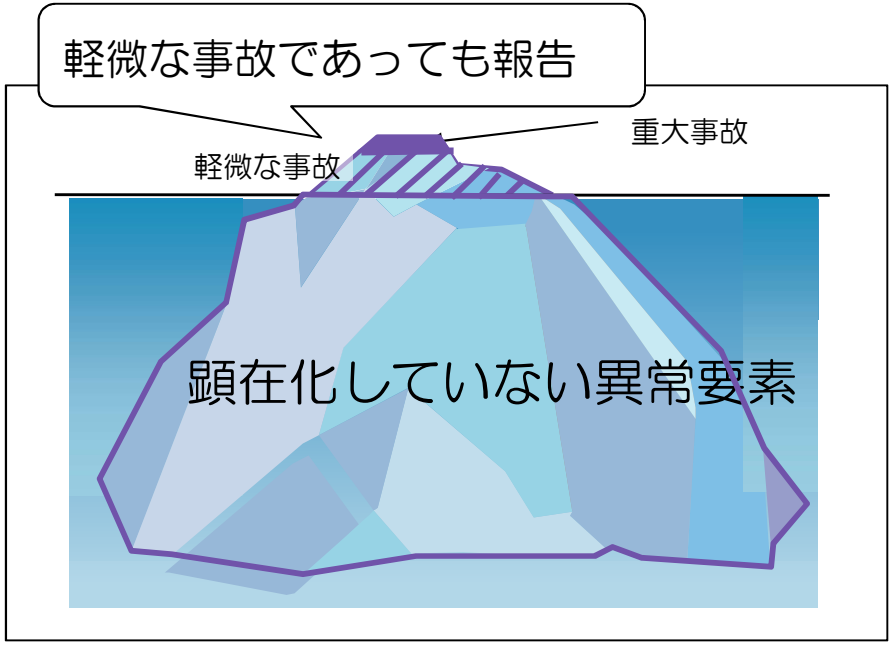
有事対応

- ✓ 現場に情報セキュリティインシデントを即時報告することを繰り返し徹底
- ✓ 情報セキュリティを「見える化」して、経営に情報セキュリティリスク状況を定期報告　(事業部門(従業員)と経営との橋渡し役)
- ✓ 有事への備えとして訓練が重要と考える

FUJI Xerox

〈有事対応〉インシデント対応

- 軽微な事故であっても報告
  - ✓ 当事者は事故の影響を過小評価する傾向にあり、事故が放置されることで、初動対応が遅れ、問題を大きくしてしまう
  - ✓ 事故対応が適切にされないことによって、お客様の信頼を失う



〈情報セキュリティ事故の対応〉

2時間以内報告

事故報告管理システムへ
事故の詳細を入力し、統合管理

毎月事故を
分析・整理

事故
の発生

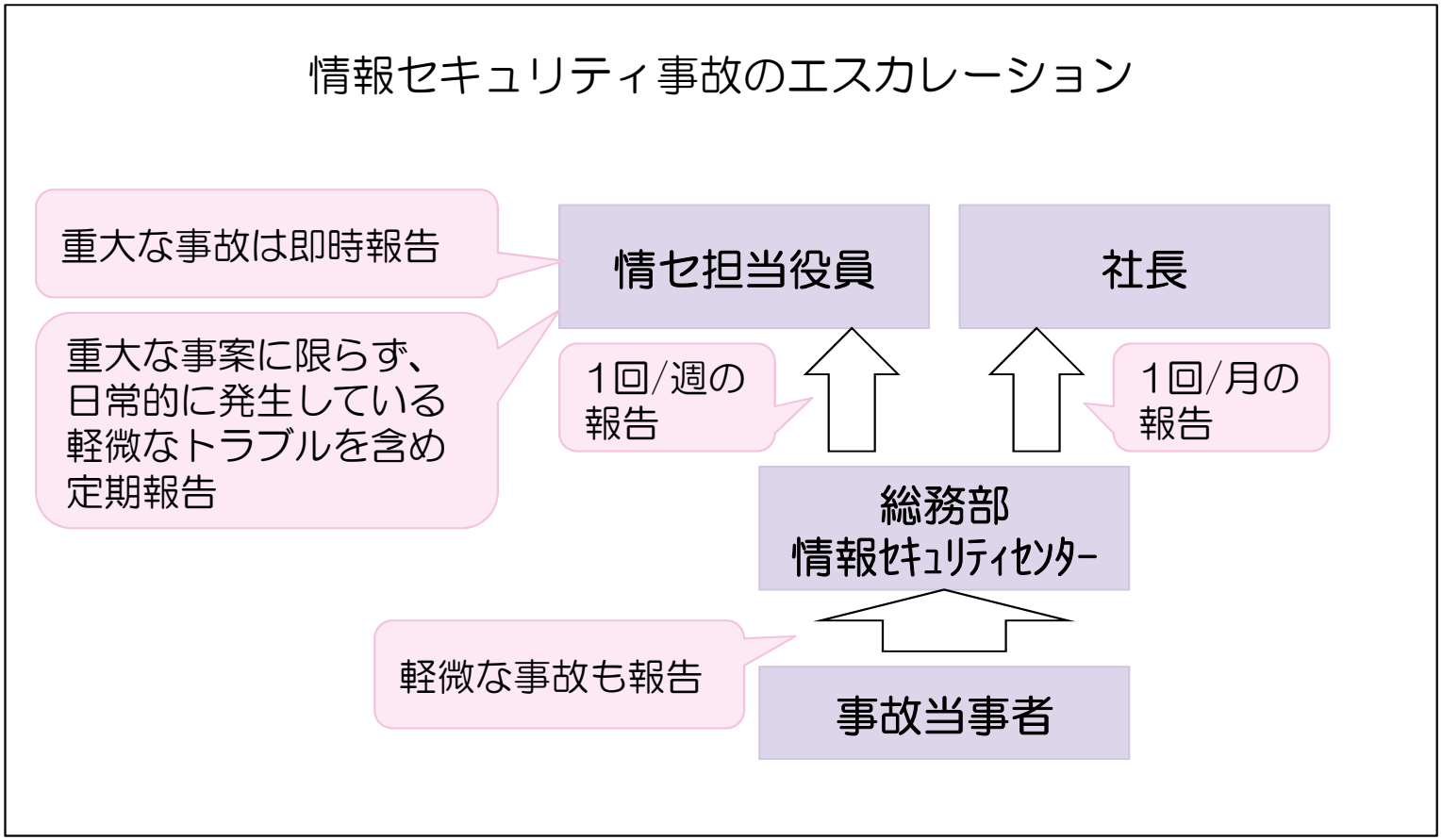
緊急報告 → 詳細報告 → 事故分析

緊急対応 → 対応・ｸﾗｲｼｽ対応 → 再発防止 → 監査

事故情報の
活用

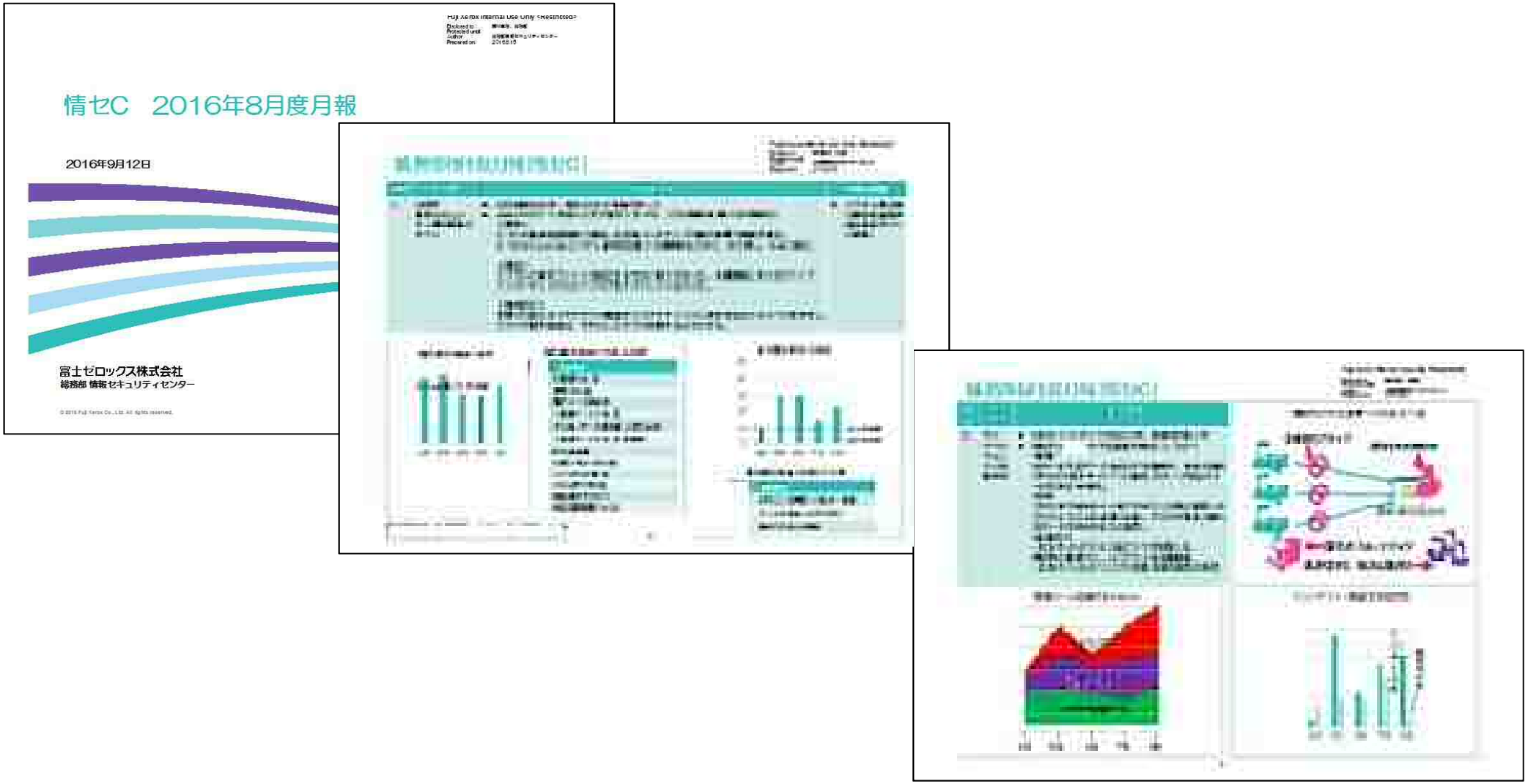
〈有事対応〉 経営へのエスカレーション

- 情報セキュリティは経営にとって重要なリスクテーマであり、
  経営が適切な判断をするためにインシデント情報のエスカレーションを実施



〈有事対応〉 見える化

- インシデント状況、情報セキュリティ活動状況を経営に報告



〈有事対応〉 情報セキュリティ訓練

- 防災訓練や大規模地震対応訓練と同じように、サイバーセキュリティの司令塔機能を検証するためのサイバー攻撃初動対応訓練や従業員の対応力向上を目的にした標的型攻撃メール訓練を実施

	大規模地震 	サイバー攻撃 
司令塔機能の訓練	本部訓練	攻撃発見後の Fuji Xerox CERT訓練
現場・従業員の訓練	安否確認訓練	標的型攻撃メール訓練

<補足> Fuji Xerox CERT訓練

- Fuji Xerox CERTのインシデント対応力向上のため、
  様々なリスクシナリオによる訓練を実施

訓練の目的
- インシデント対応プロセスに慣れ、有事の際、迅速に行動できるようにする
- インシデント対応プロセスの改善サイクルを回し、有事の際のミスや手戻りを防ぐ

訓練頻度　毎月1回（1時間）　　訓練対象者　Fuji Xerox CERTメンバ+関係者

訓練方法　机上演習

実施	訓練シナリオの例
8月	当社公式サイトからの個人情報漏洩 当社公式サイトがSQLインジェクション攻撃を受け、お問い合わせ情報（個人情報を含む）が社外に漏えい
9月	フィッシングによるお客様アカウント情報の悪用 当社のインターネットサービスの偽サイトへの誘導によりお客様のID/パスワードを窃取するフィッシングメールが発生。ID/パスワードが悪用され、不正操作がおこなわれた

普段からリスクはないか想像力を働かせることが重要!
しかし、万が一事故が起きてしまったら、

空振りは許されるが、
見逃しは許されない

疑わしき時は行動する

最悪事態を想定して行動する

FUJI Xerox