NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

「情報セキュリティポリシーサンプル 改訂版概要」

嶋倉　文裕
富士通関西中部ネットテック株式会社
JNSA西日本支部

2015年1月

はじめに

・情報セキュリティポリシーサンプル0.92a版は2002年の作成から１２年を経過しておりますが、今なお根強い人気がありJNSAの公開サイトへのアクセスが毎月1000件を超える一方、改訂要望も多い状況です。

・JNSA西日本支部では、企業の情報セキュリティ対策の支援ツールの位置づけで、クラウドやスマートデバイス、SNSといった新しい技術を取り込むと同時に、更新されたISO/IEC27002:2013とも対応づけた情報セキュリティポリシーサンプルを0.92a版を元に改訂作業を進めています。

・本講演は、現在改訂中の情報セキュリティポリシーサンプルの概要を説明致します。

０．９２版と改訂版の違い

	0.92版	改訂版
作成年	2000年～2001年	2014年～
作成目的	ポリシー作成の概念に留まらず、実際の文書を提示することで、ポリシーの考え方と作り方を提示する	・ISO/IEC27002:2013への対応 ・スマートデバイス、クラウド、SNSなど新技術への対応 ・西日本の成果物との連携
対象企業	小 ⇔ 中 ⇔ 大	小 ⇔ 中 ⇔ 大
関連規格	ISO/IEC17799	ISO/IEC27001:2013 ISO/IEC27002:2013 ISO/IEC27005:2008 ISO/IEC31000:2009
サンプル文書数	31	15予定
PDCA	PDCAあるがD中心	PDCA全て

西日本支部成果物との関係

気付き

- 出社してから退社するまで
  中小企業の情報セキュリティ対策実践手引き
- 略称：9to5

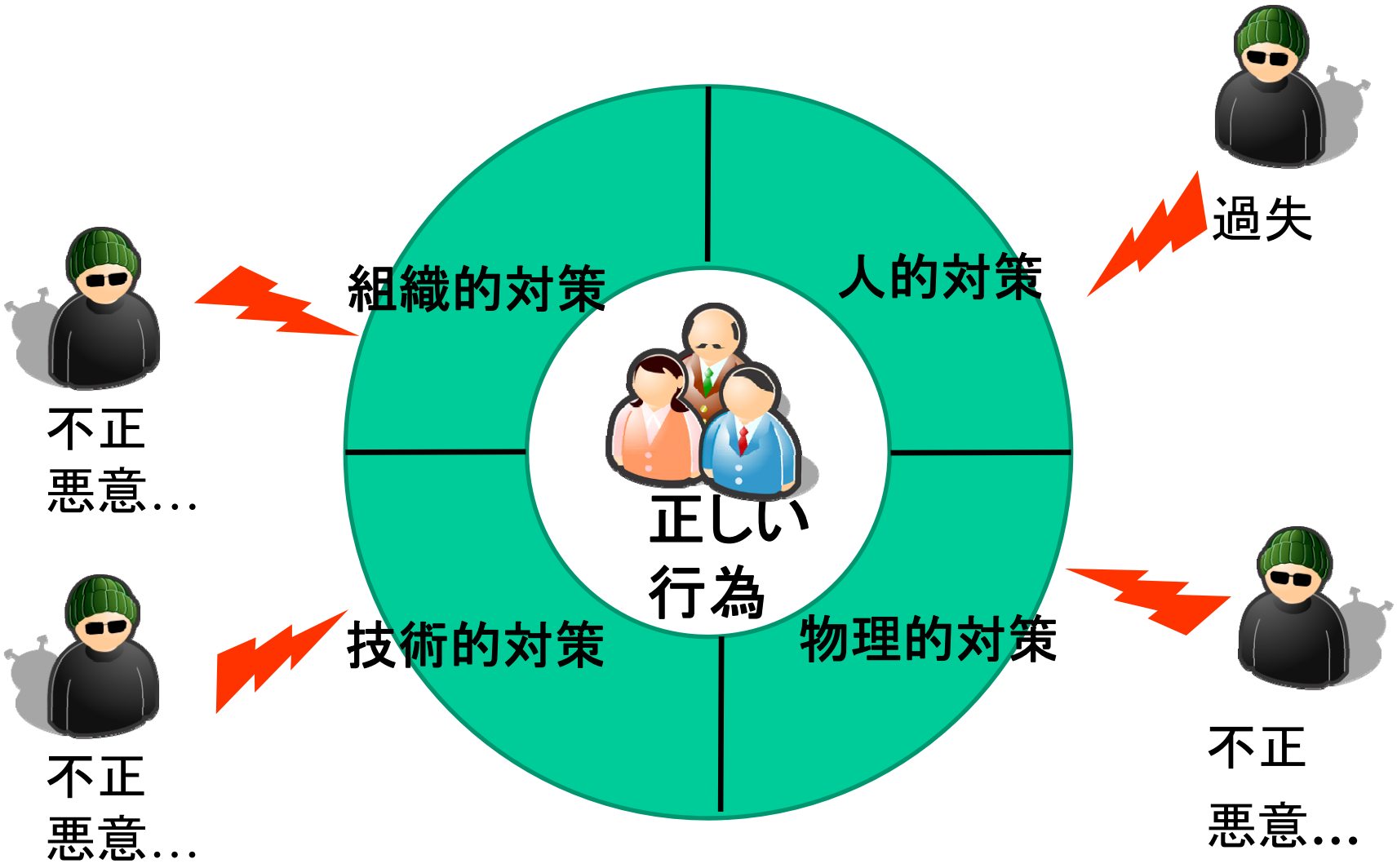
運用

- **情報セキュリティポリシー・サンプル**

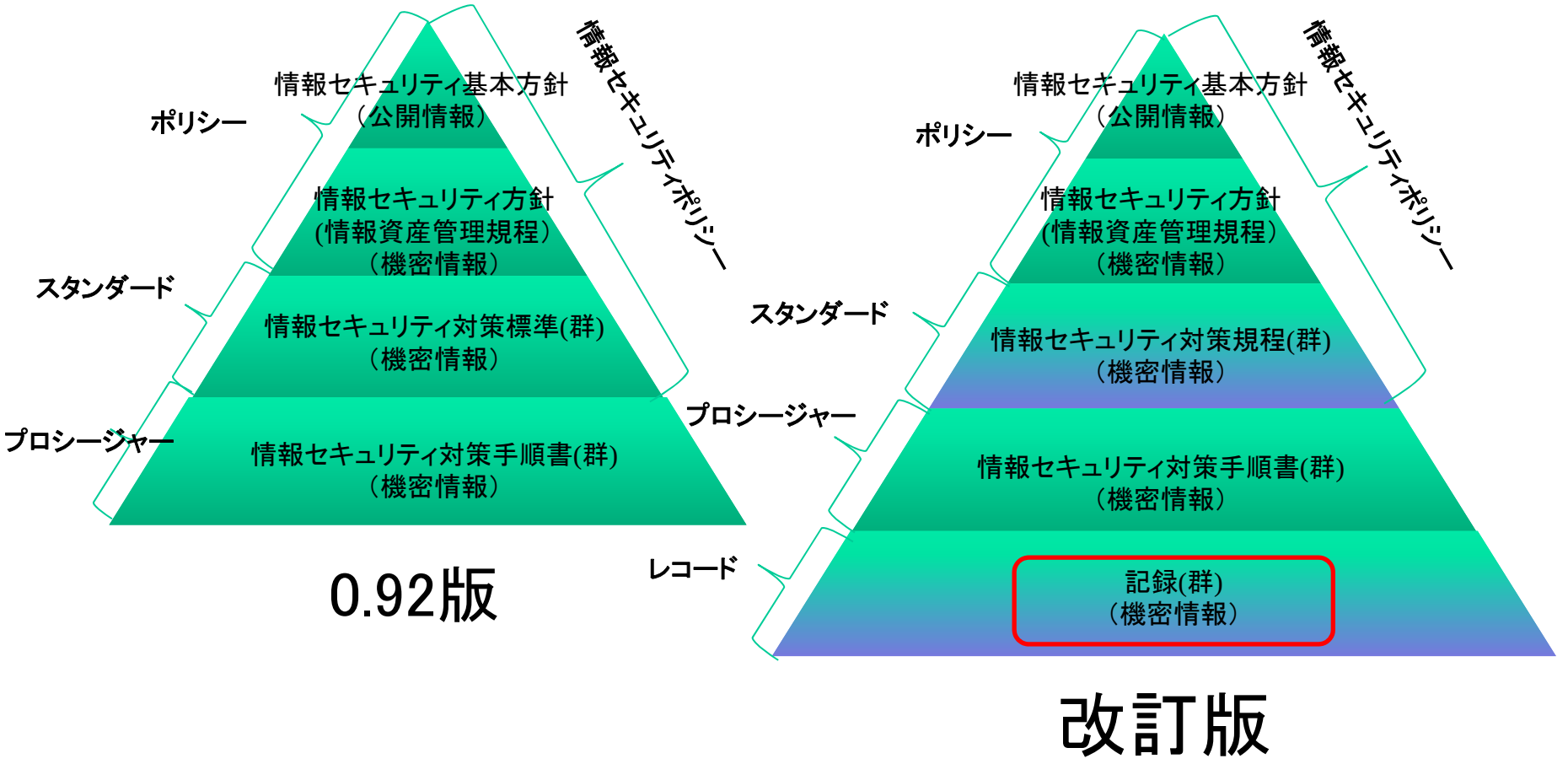
チェック

- 中小企業向け情報セキュリティチェックシート
- 略称：チェックシート

なぜ文書が必要？



文書階層



改訂版情報セキュリティ文書の定義

文書	内容
情報セキュリティ基本方針	情報セキュリティに取り組む姿勢を広く、世の中に宣言する文書。
情報セキュリティ方針	情報セキュリティマネジメントにおける方針を記載する文書。 情報セキュリティに取り組む体制、役割、責任を明確にする。
情報セキュリティ対策規程	導入、遵守すべき情報セキュリティ対策を日常の運用を含め明確にする。 例）ウィルス対策ソフトの導入、パターンファイル自動更新
情報セキュリティ対策手順書	導入、遵守すべき情報セキュリティ対策を実現する製品やその製品で日々、実施すべき具体的な行動を明確にする。 例)JNSA社のウィルス対策ソフトの管理システムからパターンファイルを自動的にPCに配布
記録	情報セキュリティ対策を遵守、運用に伴い作成する記録。 例) JNSA社のウィルス対策ソフトの管理システムでパターンファイル更新が全PCに行われたことを確認する記録

文書パターン

※解説書では、規程=スタンダード

パターン1 1つの規程

規程

⇒小規模ユーザや簡易的に実施する場合

パターン2 対象者ごとの規程

利用者向け規程　運用者向け規程　管理者向け規程

⇒中規模ユーザである程度の公開をする場合

パターン3 目的ごとの規程

構築向け規程　運用管理向け規程　利用向け規程

⇒中・大規模ユーザで一般的に実施する場合

パターン4 項目ごとの規程

パスワードに関する規程　メール利用に関する規程　・・・　更新に関する規程

⇒大規模ユーザで詳細に運用・管理する場合

※情報セキュリティポリシー・サンプル(0.92版)解説書より

0.92版文書

C0. 情報セキュリティ基本方針
C0. 情報セキュリティ方針
C1. ソフトウェア／ハードウェアの購入及び導入標準
C2. 委託時の契約に関する標準
C3. サーバルームに関する標準
C4. 物理的対策標準
C5. 職場環境におけるセキュリティ標準
C6. ネットワーク構築標準
C7. LANにおけるPC、サーバ、クライアント等. 設置/
変更/撤去の標準
C8. サーバ等に関する標準
C9. クライアント等におけるセキュリティ対策標準
C10. 社内ネットワーク利用標準
C11. ユーザー認証標準
C12. ウィルス対策標準
C13. 電子メールサービス利用標準
C14. Webサービス利用標準
C15. リモートアクセスサービス利用標準
C16. 媒体の取扱に関する標準
C17. アカウント管理標準
C18. システム維持に関する標準
C19. システム監視に関する標準
C21. セキュリティ情報収集及び配信標準
C20. プライバシーに関する標準
C21. セキュリティ情報収集及び配信標準
C22. セキュリティインシデント報告・対応標準
C23. 監査標準
C24. セキュリティ教育に関する標準
C25. 罰則に関する標準
C26. スタンダード更新手順に関する標
C27. 専用線及びVPNに関する標準
C28. 外部公開サーバに関する標準
C29. プロシージャ配布の標準

改訂版作成文書

チェックシート、9to5から検討

管理者側

①情報セキュリティ基本方針（ほぼ変更なし？）
②人的管理規程
③委託先管理規程
④文書管理規程（ほぼ変更なし？）
⑤監査規程（ほぼ変更なし？）
⑥物理的管理規程
⑦リスクマネジメント規程
⑧インシデント管理
⑨変更管理
~~⑩IT継続~~
⑪システム開発規程
⑫システム管理規程
⑬ネットワーク管理規程
~~⑭スマートデバイス管理規程~~

利用者側

⑮システム利用規程
~~⑯ネットワーク利用規程~~
⑰スマートデバイス利用規程
⑱ＳＮＳ利用規程

目的単位に集約した！
さらに絞って15項目に！

改訂版と0．92版、西日本成果物

092版	チェックシート/9to5
①情報セキュリティ基本方針	
C0. 情報セキュリティ基本方針 C0. 情報セキュリティ方針	A1. 情報セキュリティ基本方針
②人的管理規程	
C20. プライバシーに関する標準 C24. セキュリティ教育に関する標準 C25. 罰則に関する標準	A2. 責任の明確化 A3. 職務の分離 A7. 法令順守 A8. 秘密保持
③委託先管理規程	
C2. 委託時の契約に関する標準	A4. 委託先の管理 B2. クラウドサービスの利用
④文書管理規程	
C26. スタンダード更新手順に関する標 C29. プロシージャ配布の標準	A6. 規程の文書化とレビュー
⑤監査規程	
C23. 監査標準	A9. 情報セキュリティの確認
⑥物理的管理規程	
C3. サーバルームに関する標準 C4. 物理的対策標準 C5. 職場環境におけるセキュリティ標準	B1. セキュリティ境界と入退出管理
⑦リスクマネジメント規程	
	A5. 情報資産管理台帳
⑧インシデント管理	
C22. セキュリティインシデント報告・対応標準	B3. 障害・事故管理

注）チェックシート/9to5　表中の項番

Ax　チェックシートの「上位」と位置付けたシートの項番

Bx　9to5の情報セキュリティ管理策の項番

改訂版と0．92版、西日本成果物

092版	チェックシート/9to5
⑨変更管理	
	B16. 変更管理
⑪システム開発規程	
	B12. Webの開発管理
⑫システム管理規程	
C3. サーバルームに関する標準 C8. サーバ等に関する標準 C11. ユーザー認証標準 C12. ウィルス対策標準 C16. 媒体の取扱に関する標準 C17. アカウント管理標準 C18. システム維持に関する標準 C19. システム監視に関する標準 C21. セキュリティ情報収集及び配信標準	B2. クラウドサービスの利用 B4. IT継続性 B5. 認証と権限 B7. パッチの適用 B8. ウイルス及び悪意のあるプログラムに対する対策 B9. 記憶媒体の管理 B10. スマートデバイス B13. ログの取得 B14. バックアップ B15. 容量・能力の管理 B17. 構成管理 B19. 暗号化
⑬ネットワーク管理規程	
C6. ネットワーク構築標準 C7. LANにおけるPC、サーバ、クライアント等. 設置/変更/撤去の標準 C27. 専用線及びVPNに関する標準 C28. 外部公開サーバに関する標準	B4. IT継続性 B6. ネットワークのアクセス制限 B5. 認証と権限 B7. パッチの適用 B8. ウイルス及び悪意のあるプログラムに対する対策 B13. ログの取得 B15. 容量・能力の管理 B17. 構成管理 B19. 暗号化

改訂版と0．92版、西日本成果物

092版	チェックシート/9to5
⑮システム利用規程	
C1. ソフトウェア／ハードウェアの購入及び導入標準 C9. クライアント等におけるセキュリティ対策標準 C12. ウィルス対策標準 C13. 電子メールサービス利用標準 C14. Webサービス利用標準 C15. リモートアクセスサービス利用標準	B2. クラウドサービスの利用 B3. 障害・事故管理 B5. 認証と権限 B6. ネットワークのアクセス制限 B7. パッチの適用 B8. ウイルス及び悪意のあるプログラムに対する対策 B9. 記憶媒体の管理 B11. 電子メールの利用 B14. バックアップ B19. 暗号化 B20. アプリケーションの利用 B21. クリアデスク・クリアスクリーン
⑰スマートデバイス利用規程	
C10. 社内ネットワーク利用標準	B10. スマートデバイス
⑱SNS利用規程	
	B18. SNSの利用

改訂方針①

- 0.92版を踏襲する
  - ISO27001付属書Aの網羅性を確保
    - 付属書Aと規程の関連を明確にしつつ改訂
  - ISO27002実施の手引きのレベル感で管理策の追加、削除、修正
  - システム管理者、システム利用者を分離

改訂方針②

・PDCAが回ることを意識

0.92版

- 趣旨
- 対象者
- 対象システム
- 遵守事項
- 例外事項
- 罰則事項
- 公開事項
- 改訂

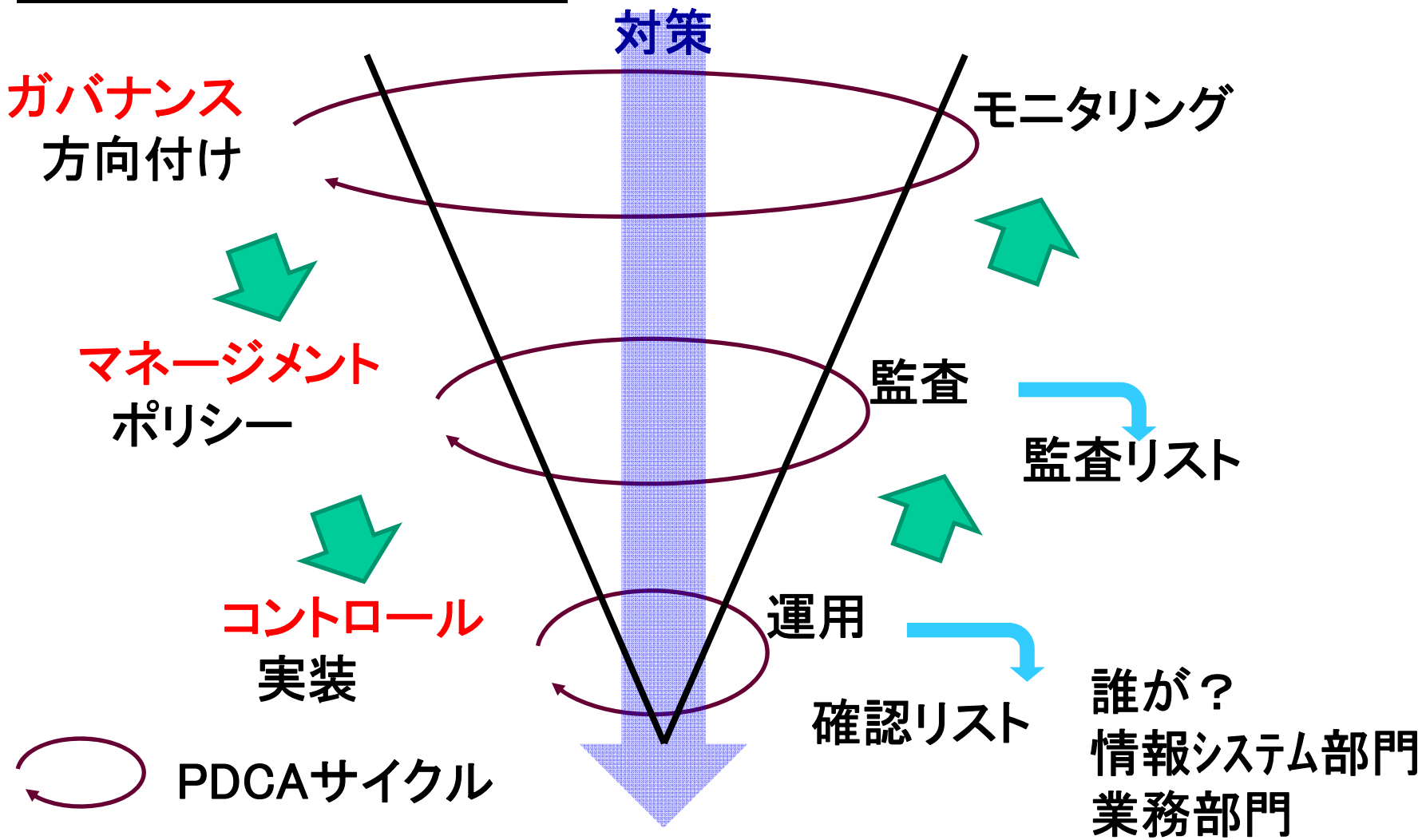
改訂版

- 趣旨/目的
- 対象者
- 対象システム/対象範囲
- 遵守事項
- **運用確認事項**
  - **−運用点検(第三者、自主点検として)**
  - **−記録・エビデンスベースで確認できること**
- 例外事項
- 罰則事項
- 公開事項
- 改訂

本規程に基づき記録運用が管理されている事を定期的に確認すること
なんのために、これも大切

改訂方針②

それぞれにあるPDCA



改訂方針②

	情報システム部門（管理部門）	業務部門（利用部門）
確認したいこと（目的）	(1)対策の定着 ・対策の全社展開 (2)対策の効果 ・脅威の検知、抑止、防御 (3)対策の維持 ・対策の回避、無効化の有無	(1)対策に伴う手続きの定着 ・全社での申請、確認 (2)対策による業務への効果 ・安全な業務遂行 (3)対策に伴う手続きの維持 ・申請/確認行為の無視有無
確認の対象（記録）	(1)システムログ ・ｻｰﾊﾞﾛｸﾞ、PCﾛｸﾞ、ﾈｯﾄﾜｰｸﾛｸﾞ（ｱｸｾｽﾛｸﾞ、ｲﾍﾞﾝﾄﾛｸﾞetc） (2)管理画面 ・統計、適用、検知/防御状況 (3)人(対象：部門管理者) ・定着、課題などのﾋｱﾘﾝｸﾞ	(1)人（対象：自部門） ・手順書&チェックシート ・ワークフロー ・申請書 (2)管理画面 ・適用状況
確認契機	(1)定期的 ・毎週、毎月etc. (2)不定期 ・イベント（ｷｬﾝﾍﾟｰﾝ） ・インシデント	(1)日常業務 ・情報持出し時 (2)定期的 ・毎週、毎月 (3)不定期 ・イベント

運用確認目的

（1）対策の定着
- 対策の実施、実行といった定着の確認

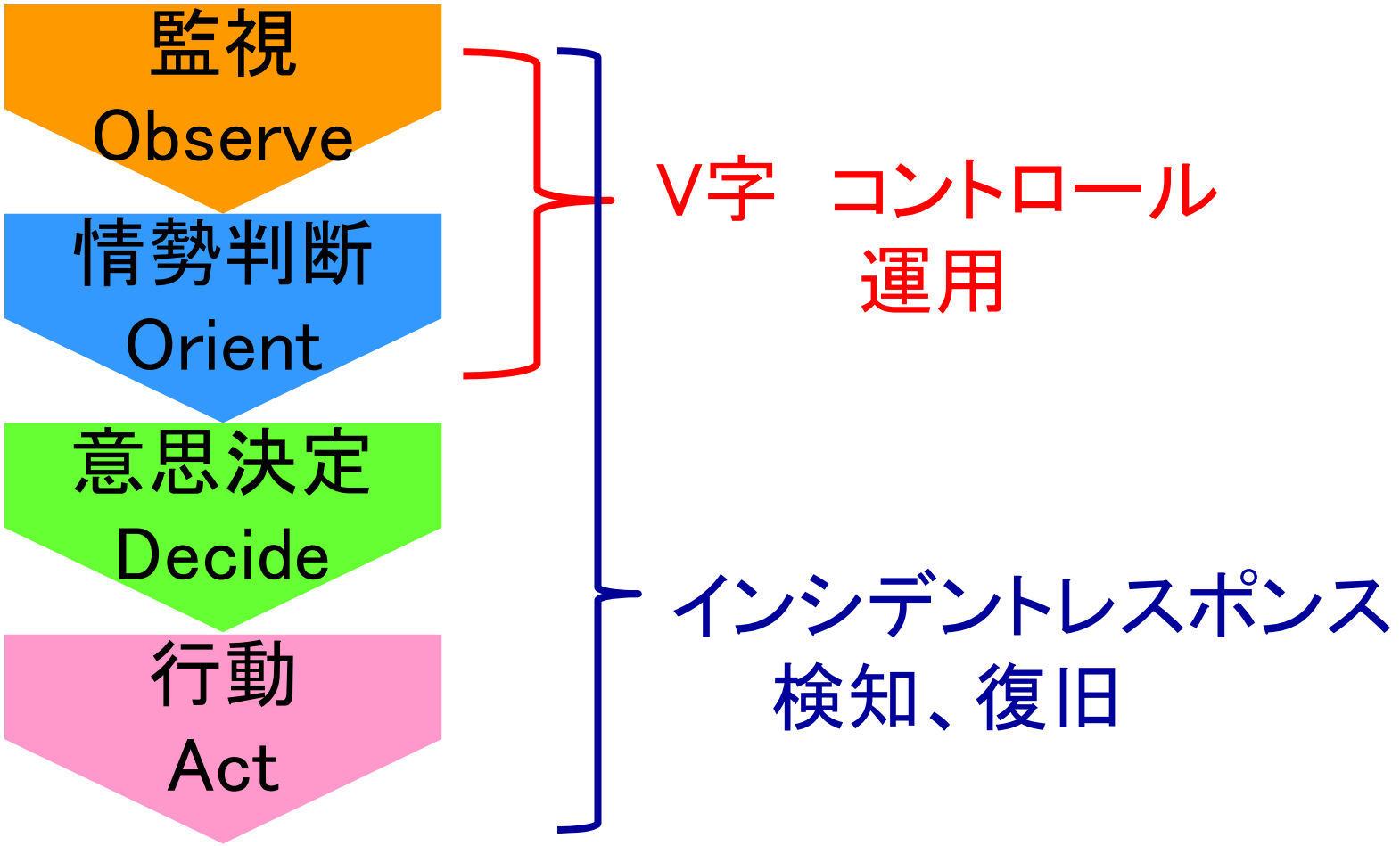
（2）対策の効果
- 脅威を検知し防御していること
- 異常の検知

（3）対策の維持
- 対策の回避、無効化がないこと

運用で確認すべきことの目的、誰が、何をの明確とその実行確認が必要
ポリシーサンプルには、参考事例を記載

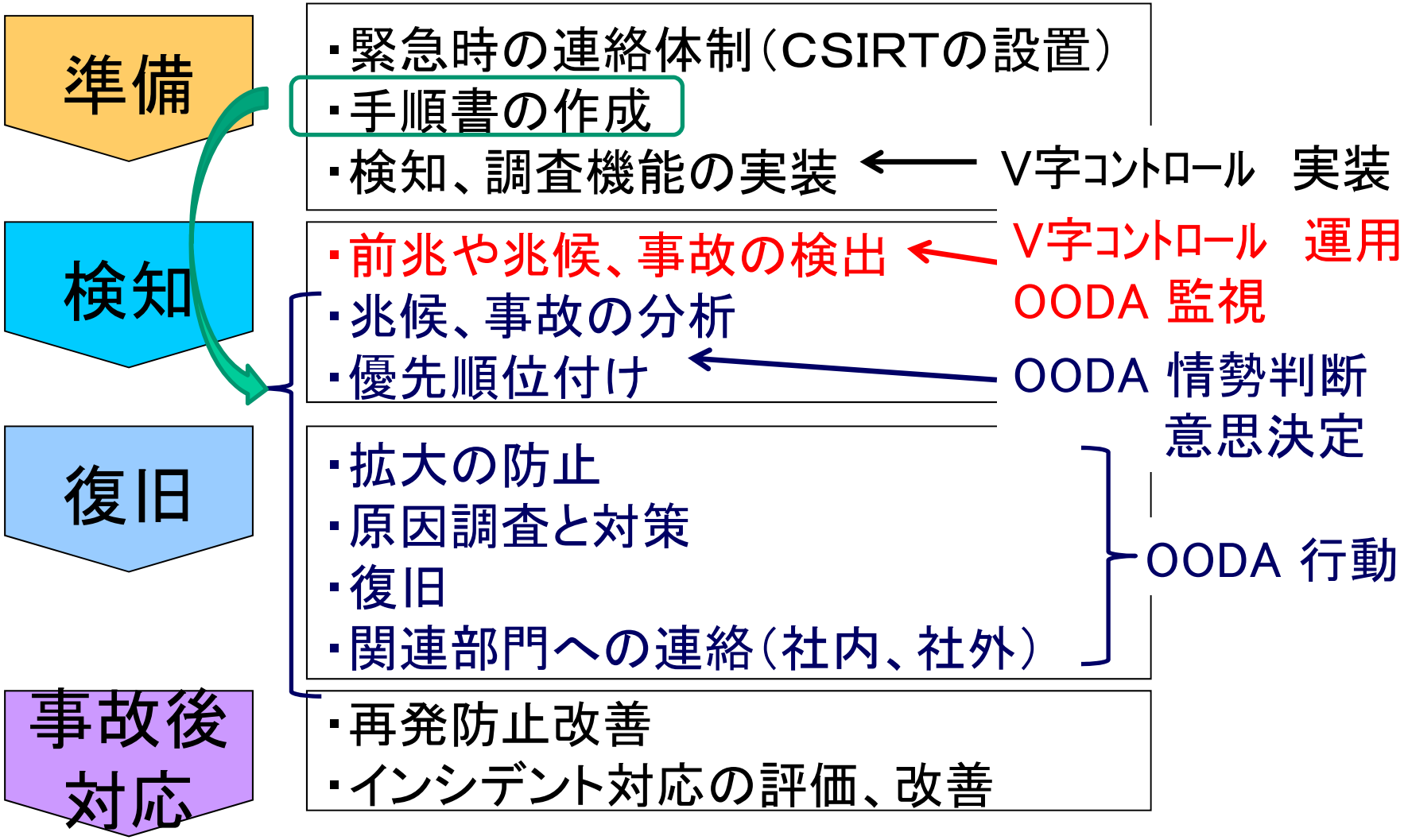
少し脇にそれますが…

OODAループ

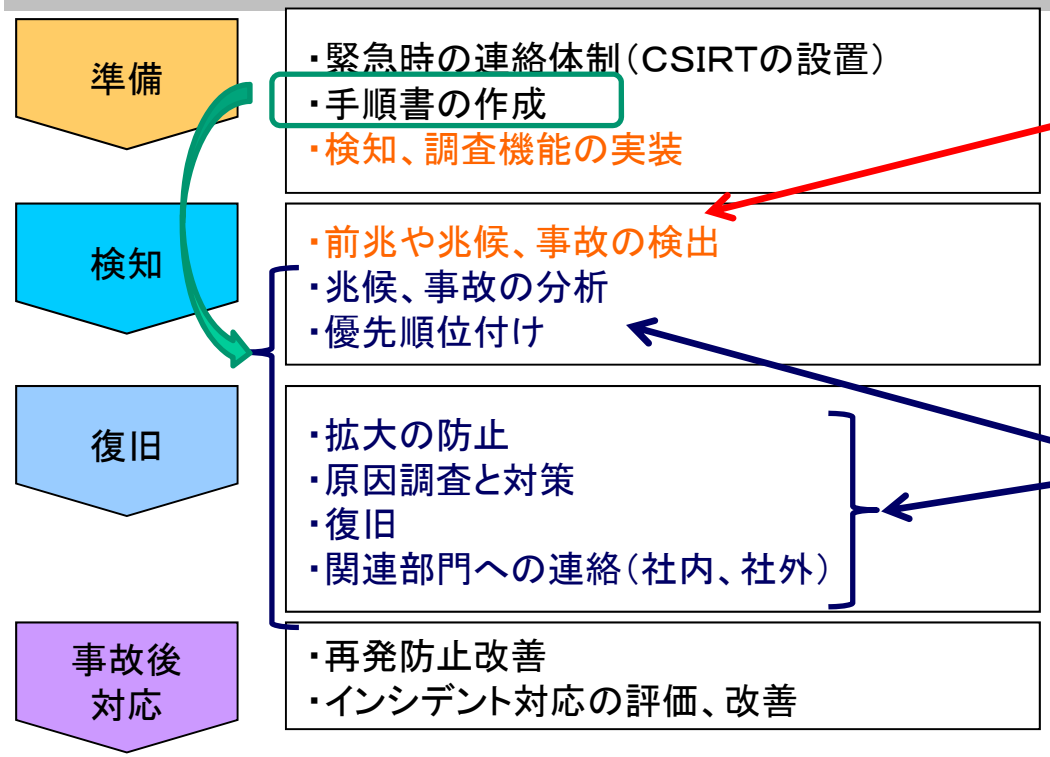


インシデントレスポンス

CSIRT：　Computer Security Incident Response Team



インシデントレスポンスとOODAループと運用確認



V字コントロール　運用確認

OODA 監視

・誰が
・何を
・いつ

OODA 情勢判断
意思決定
行動

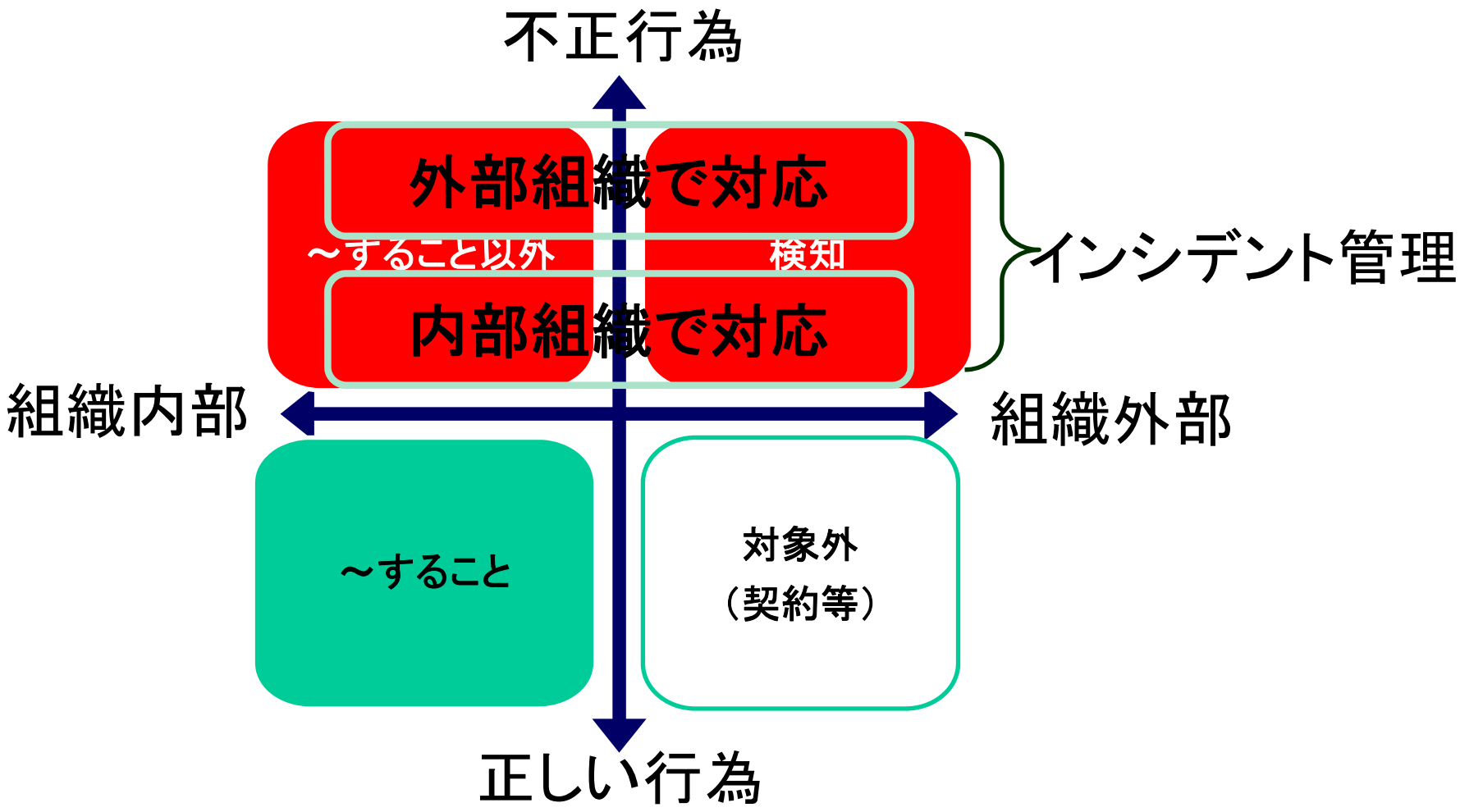
・ポリシーでの運用確認
–防御が機能していること
–被害の検知
両方のチェックが重要

改訂方針③

- ホワイトリスト型の記述を心がける
  - 白と黒の世界
    - ホワイトリスト型表現：白であること
    - ブラックリスト型表現：黒でないこと
  - 白と黒と灰色の世界
    - ホワイトリスト型表現：白であること
    - ブラックリスト型表現：黒でないこと

改訂方針④

- 内部と外部のタスクを明記



改訂方針⑤

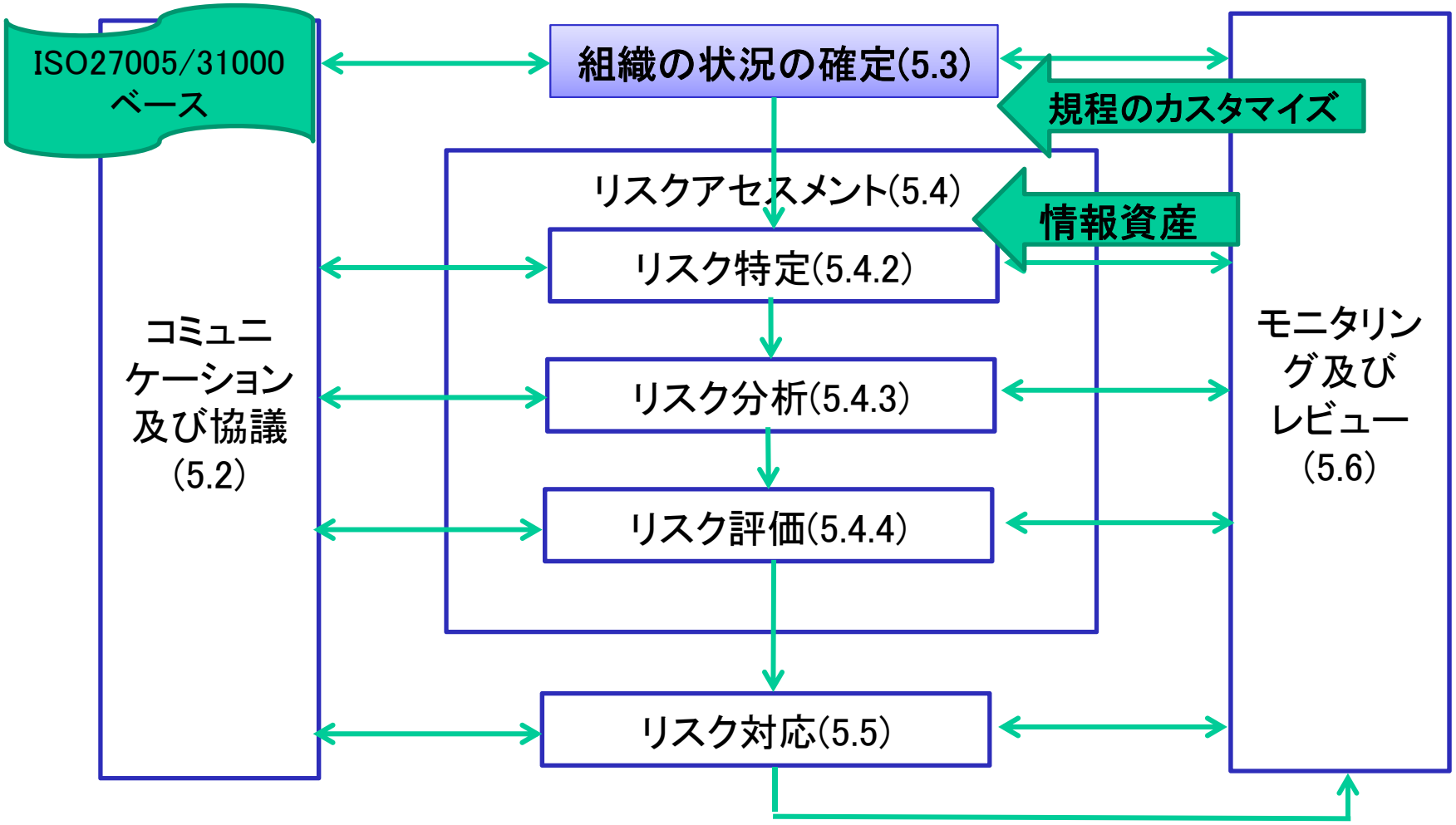
- 主語、対象、役割（行為、記録、確認・承認）を明記

誰が（責任者、管理者、利用者）、何を、どういう責任を果たすのか

後で検証可能な記録に何を残すのか

改訂方針⑥

・ リスクマネジメント規程を導入する



スケジュール

当初、こんな予定で考えていました.....

活動項目	9月～	11月	12月	1月	2月	3月	4月
情報セキュリティ対策規程の作成	→	→					
情報セキュリティ対策規程解説書の作成			→	→			
まとめ					→	→	→

０．９２をベースに再整理を行い、文書は作成しましたが。。遅延しております。。。

遅延理由

対策内容は0．92版を元に再構成
27002:2013を取り込むが、遅延の原因ではない
対策のレベル感、対策の是非は気にしていない

〈主な遅延理由〉
・0．92版にない文書の作成
・再構成と言いながら、記載すべき内容の確認作業
・新規、再構成の文書間の整合性の確認
　記述レベル(とくに対策規程)
　他文書参照先
・想定する企業、システム構成イメージのメンバ間でのぶれ

リスケします

	1月	2月	3月	4月	5月	6月	7月	8月	9月
想定する企業、システム構成イメージ再確認	→								
文書整合性		→	→	→					
解説書				→	→	→			
まとめ							→	→	→

ご清聴ありがとうございました。