JNSA

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

情報セキュリティ対策としての個人スキル向上と組織開発

セキュリティ・エデュケーション・アライアンス・ジャパン
事務局長　持田 啓司

2006 年 5 月 30日

そもそもセキュリティ設計に教育が必要な理由

- 大事なものは何か？
  - 立場の違いで異なる判断基準
    - 何が大事か？
    - 脅威に対する判断基準の違い
    - 絶対や真理がない
- 大事なものを守る＝セキュリティ設計
  - 守るとは？
    - 何を
    - 誰から
    - 何のために
    - どうやって
    - いくらかけて

    ●不安(脅威)の明確化
    ●対策の検討実施
- 組織として共通認識にする必要がある
  - 「大事なもの」と「そのためのセキュリティ設計」に対する共通認識
  - 意識の共有化のために教育が必要

最近の話題から・・・・・
内部統制に関するITへの対応例

- IT成熟度診断
  - COBIT、e-BAT etc
- ERP、BPM、ワークフローなどのビジネスプロセス系ツール使用
  - 情報システムの完全利用と業務遂行記録
- セキュリティ機能
  - 不正アクセス、改ざん防止、内部統制診断等
- BCM対応
  - システムダウン対応・バックアップ等
- 内部統制の限界への対応
  - リスク保有、コンプライアンス、コーポレートガバナンス、モラル・倫理

内部統制と教育との関係

- IT部門担当者の教育
  - 企業倫理、守秘義務、誠実性
  - 技術知識
- 全スタッフの教育
  - 企業倫理、守秘義務、誠実性
  - 利活用におけるセキュリティの責任と実践
- 経営者の教育
  - 企業倫理、守秘義務、誠実性
    - 組織内のいずれの者よりも、統制環境に係る諸要因及びその他の内部統制の基本的要素に影響を与える組織の気風の決定に大きな影響力を有している。

教育の重要性と現状の対応

- ISMSなどで明記
  - しかし、具体的教育内容と手法は不明確
- 情報漏えい事件の状況
  - 多くの場合、すでに啓蒙教育等を実施していた
  - 責任者コメント「今後、仕組みの見直しとより一層の教育の徹底を図る」
- 提供側も対症療法的な教育提案に終始
  - 緊急避難的教育がほとんど
  - 組織開発の観点は見えてこない

情報セキュリティ人材不足 (IT専門家)

- 技術者不足の面は、雇用や経済の面など多方面から叫ばれている。
  - 総務省 情報通信ソフト懇談会 最終報告書(2003/12)
    情報通信人材の不足は42万人、うちセキュリティ人材は12万人と推計
- 考えられる要因
  - 雇用環境の正社員減少
  - キャリアチェンジ不足
  - 学校教育
  - 人材交流
  - 職人的教育

参考データ：情報処理技術者試験

平成17年春期 業務別	受験者数	合格者数
情報処理関係	89,193名	12,174名
非情報処理関係	49,570名	11,349名

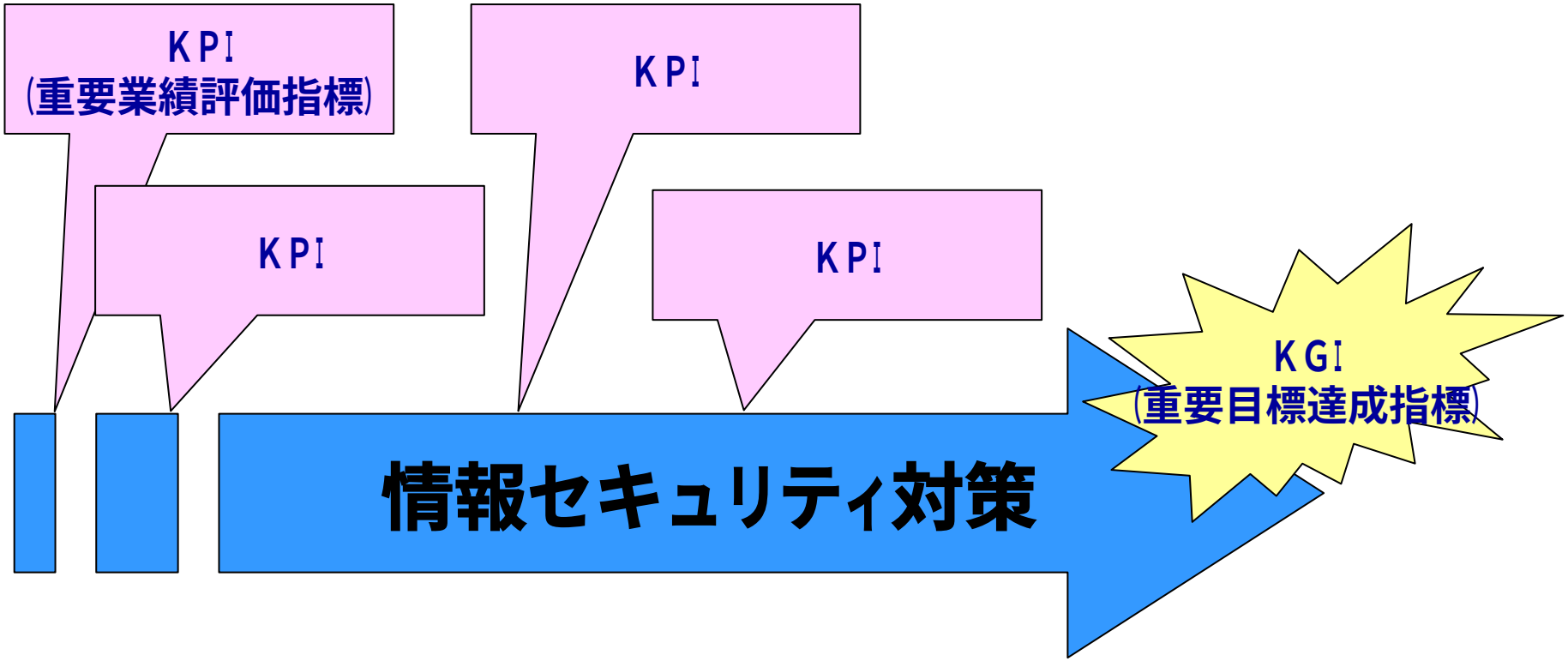
(出典：IPA情報処理技術者試験センター統計情報)

情報セキュリティ人材不足 (トップマネジメント)

- **経済産業省情報セキュリティ教育研究会開催**
  - 2003**年度、組織の責任者** (CISO) **への教育検討のため発足。**
  - 2004**年6月発表**
    - http://www.meti.go.jp/policy/netsecurity/edu_report.html
  - **求める人材像**
    - **セキュリティ対策における、予算・全部門への権限を持ち、システム的対策も含めて外注管理(丸投げではない)ができる。いわゆるジャッジをする人材。**
    - **情報セキュアドよりも高スキル。**

(**出典**:METI **情報セキュリティ教育研究会報告書**)

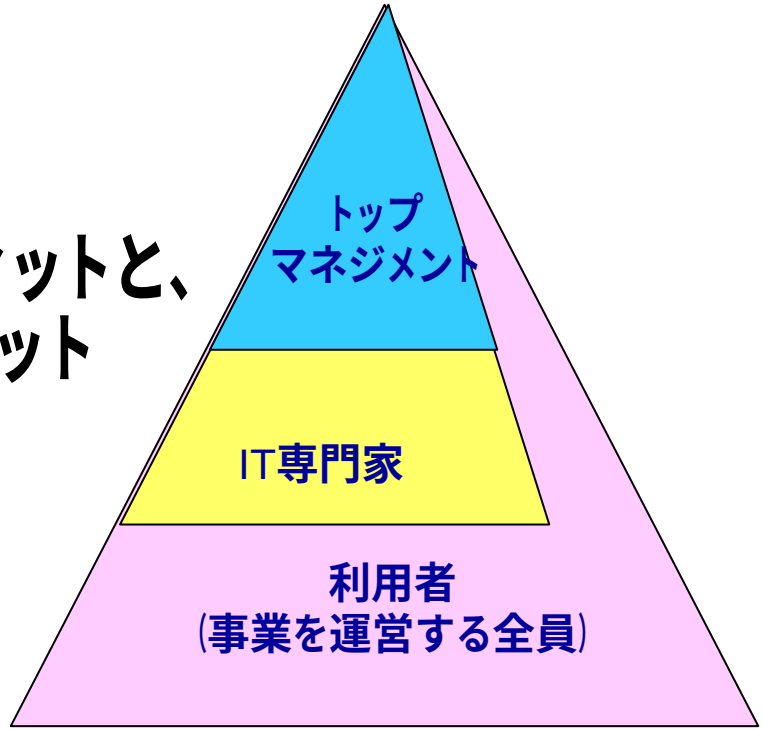
情報セキュリティ対策と評価の考え方



- トップマネジメントの理解不足で、対策の評価方法に差
- 対策の評価は、売り上げや利益などのKGIとは違う考え方が必要
- KPI (それぞれの関連性も含めて) メインで考え、KGIは参考に。

教育のためのセグメント分け

- 情報資産の活用に“人”が関与する限り、「絶対」はありえない。
- 実践に移すために、まず最初に全体を理解するための人材育成が必須。
- 教育にも設計が必要
  - 誰に、どのような内容を、どのようにして。
- 技術的な対策のためのスキルセットと、モラルや意識といったマインドセットにわける。
- 対象者
  - IT専門家・トップマネジメント・利用者の三本柱。



JNSA推奨教育ワーキング概要

- 人材育成における現状の課題
  - 必要性は叫ばれている
  - 製品販売に関連した教育多数（デモ、操作教育）、短期的・場当たり的
  - 組織全体を総括して各種対策を行うための人材配置を前提としたもの不在
- ワーキングの目的
  - スキルセットを強化するための現存する教育コースを活用し、セキュリティ人材の効率的な育成と、組織力の強化につなげたい。
- 検討内容
  - 組織の底辺からそれぞれの情報セキュリティ専門職種への育成プロセスを示すことのできる教育の在り方
  - 組織として隙の無い人材育成構築のための教育プログラム
  - 知識や実施能力の伝達は必要であり、スキルセットとしての現状の教育コースを調査し、必要とされている職種別の人材育成フロー作成

検討フェーズごとのワーク

- 情報セキュリティスキル項目検討
  - 情報セキュリティスキルをくまなく洗い出すために、IPAスキルマップ、経済産業省教育研究会、情報セキュアド試験スキル標準、CISSPcbkを参考に、詳細スキル項目を作成。
- 対象教育コース(資格)調査・検討
  - 市場にある情報セキュリティ教育(資格)を抽出し、そのカリキュラムを調査して、前フェーズでまとめたスキル項目と比較検討。
- 職種別必要スキル項目検討
  - 情報セキュリティに関わる職種を選定・分類。
  - それぞれの職種ごとに必要なスキル項目を検討。
- キャリアパス作成
  - 情報セキュリティ専門職種ごとに、教育コースを研修ロードマップとしてチャートで表現。

情報セキュリティスキル項目検討

- IPAスキルマップを中心に、経済産業省教育研究会、情報セキュアド試験スキル標準、CISSPcbkなどの技術項目などを追加して、体系化。
  - IPAスキルマップは技術項目で分けてあり、職務による業務知識という観点で区分してあるものよりも整理しやすかった
- 設計思想や経営面の視点の項目がなかったため、「セキュリティアーキテクチャ」や「事業継続経営(BCM)」などを大分類として盛り込んだ。
- 活用上の注意点
  - スキル項目は日々変化していく。
  - 視点によって体系化の仕方は変わる。

情報セキュリティスキル項目作成イメージ

作業シート

METI教育研究会	情報セキュアドスキル標準	スキルマップ	CISSP cbk	知識	技能
あああああああ	ａａａａａａ	ＡＡＡＡＡＡ	アクセスコントロール	○	○
いいいいいいい	ｂｂｂｂｂｂ		セキュリティ原則	○	○
ううううううう	ｃｃｃｃｃｃ	ＣＣＣＣＣＣ	識別(Identificatio	○	---
えええええええ			バイオメトリクス	○	○
おおおおおおお	ｅｅｅｅｅｅ			○	---
かかかかかかか	ｆｆｆｆｆｆ	ＦＦＦＦＦＦ	承認(Authorizatior	○	○
	ｇｇｇｇｇｇ	ＧＧＧＧＧＧ	シングルサインオン	○	○
くくくくくく	ｈｈｈｈｈｈ		アクセス制御モデル	○	○
けけけけけけ	ｉｉｉｉｉｉ	ＩＩＩＩＩＩ		○	---
こここここここ	ｊｊｊｊｊｊ	ＪＪＪＪＪＪ	アクセス制御コント	○	---
さささささささ			アクセス制御手法(A	○	○
しししししし	ｌｌｌｌｌｌ	ＬＬＬＬＬＬ	管理上の制御(Adm	○	○
	ｍｍｍｍｍｍ	ＭＭＭＭＭＭ	物理的制御(Physi	○	○
	ｎｎｎｎｎｎ	ＮＮＮＮＮＮ	論理的制御(Logic	○	○
そそそそそそ	ｏｏｏｏｏｏ	ＯＯＯＯＯＯ		○	○
たたたたたた	ｐｐｐｐｐｐ		アクセス制御監視(A	○	---
ちちちちちち	ｑｑｑｑｑｑ		アクセス制御に対す	○	○
つつつつつつ		ＲＲＲＲＲＲ	Teleconmmunications	○	○
	ｓｓｓｓｓｓ	ＳＳＳＳＳＳ	Open System Interc	○	○
とととととと	ｔｔｔｔｔｔ	ＴＴＴＴＴＴ		○	---
なななななな	ｕｕｕｕｕｕ	ＵＵＵＵＵＵ	6.Presentation l	○	○
にににににに			5.Session layer	○	○
ぬぬぬぬぬぬ	ｗｗｗｗｗｗ	ＷＷＷＷＷＷ	4.Transport laye	○	○
	ｘｘｘｘｘｘ		3.Network layer	○	---
ののののののの	ｙｙｙｙｙｙ	ＹＹＹＹＹＹ	2.Data Link laye	○	○
はははははは	ｚｚｚｚｚｚ	ＺＺＺＺＺＺ		○	---

完成シート

スキル項目	知識	技能
あああああああ	○	○
いいいいいいい	○	○
ううううううう	○	---
えええええええ	○	○
おおおおおおお	○	---
かかかかかかか	○	○
きききききききき	○	○
くくくくくく	○	○
けけけけけけ	○	---
こここここここ	○	---
さささささささ	○	○
しししししし	○	○
すすすすすす	○	○
せせせせせせ	○	○
そそそそそそ	○	○
たたたたたた	○	---
ちちちちちち	○	○
つつつつつつ	○	○
てててててて	○	○
とととととと	○	---
なななななな	○	○
にににににに	○	○
ぬぬぬぬぬぬ	○	○
ねねねねねね	○	---
ののののののの	○	○
はははははは	○	---

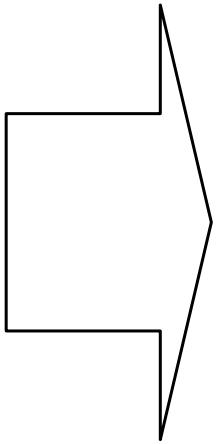
対象教育コース(資格)調査・検討

- 現存する情報セキュリティ教育(資格)をピックアップして、そのカリキュラムで学習できるスキル項目を調査。
- 活用上の注意点
  - スキル項目ごとの解説分量(ページ数)までは比較をしていない。
  - これが全てではない
    - 掲載されていなければ、スキル項目とカリキュラムをチェックすることで、対象範囲が明確になる

対象教育コース(資格)調査 取りまとめイメージ

スキル項目リスト

スキル項目
あああああ
いいいいいい
ううううううう
えええええええ
おおおおおお
かかかかかか
きききききき
くくくくくく
けけけけけけ
ここここここ
ささささささ
ししししししし
すすすすすす
せせせせせせ
そそそそそそ
たたたたたた
ちちちちちち
つつつつつつ
ててててててて



教育コース調査

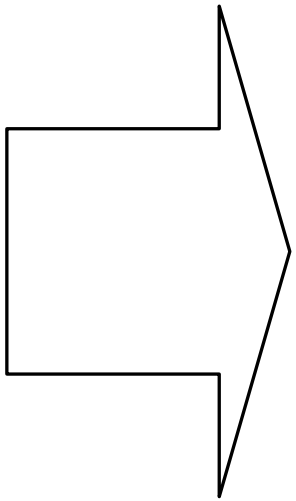
A社 aコース	A社 bコース	A社 cコース	B社 dコース	B社 eコース	C社 fコース
○		○	○		○
○		○	○		○
○		○			○
			○		
○		○	○	○	
○		○	○		
					○
	○		○		
○	○		○		○
○	○				
○	○		○		○
○	○		○		
			○		
	○		○	○	○
○		○			○
○	○	○		○	○
○	○			○	○
	○	○	○		○
			○		

職種別必要スキル項目検討

- 代表的な職種の選定
  - IT専門家・・・次の5職種。
    - 設計、NW/SYSTEM構築、アプリ開発、ポリシー構築、運用
  - 利用者・・・組織において情報を活用する全ての人材。
  - CISO・・・・組織のトップ・役員レベル。
- 必要スキルの表示方法
  - 実装あるいは対応を実施する者・・・・・◎
  - 知識として必要な場合・・・・・・・・・・・・・○
  - 業務に直接影響ない場合・・・・・・・・・・×
- 活用上の注意点
  - 職種は代表的なものであり、組織によって守備範囲は変わる。
  - 実際の業務と対象職種をかぶせてみることで、漏れているセキュリティ対策が見えてくる。
  - セキュリティ人材以外が実装するものもある。
    - 物理セキュリティなど

職種別必要スキル作成イメージ

スキル項目
ああああああ
いいいいいい
ううううううう
えええええええ
おおおおおお
かかかかかか
きききききき
くくくくくく
けけけけけけ
ここここここ
ささささささ
ししししししし
すすすすすす
せせせせせせ
そそそそそそ
たたたたたた
ちちちちちち
つつつつつつ



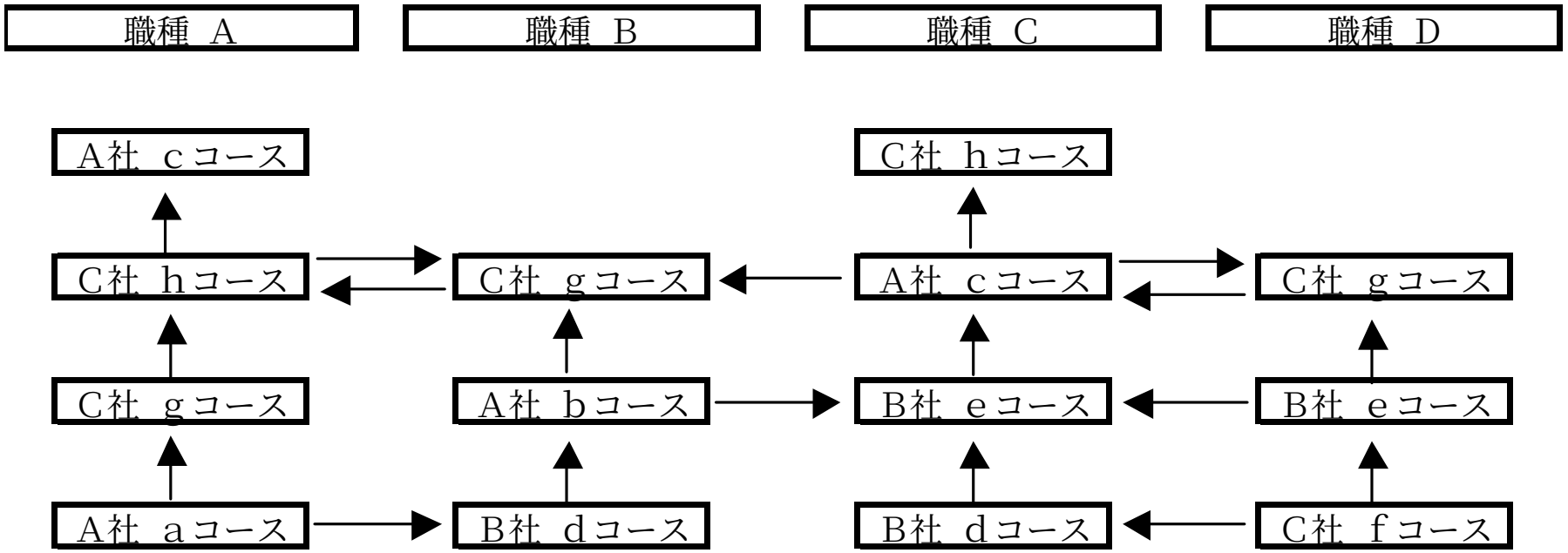
職種 A	職種 B	職種 C	職種 D	職種 E
○	◎	○	×	×
○	◎	×	○	×
○	◎	×	○	×
◎	◎	×	○	×
○	○	×	◎	○
○	○	×	◎	×
◎	○	×	○	×
◎	◎	×	○	×
○	◎	×	○	×
○	◎	×	○	×
○	◎	○	○	×
○	×	○	×	○
◎	×	○	×	○
◎	×	○	×	○
○	×	○	×	◎
○	×	○	×	◎
○	×	○	×	○
◎	×	○	×	○

キャリアパス作成

- スキルアップだけでなく、キャリアチェンジの際の教育検討にも活用できる。
- セキュリティ対策を考えた人事異動の際の参考に出来る。
- 活用上の注意点
  - 職種は代表的なものであり、組織によって必要教育コースは変わる。
  - 実際は、スキルを活用することによりキャリアは形成される。
    - 受講すればその職種になれるものではない

研修ロードマップ 作成イメージ

職種別研修ロードマップ



教育コースの充実で
人的対策は万全か？

- 個人情報保護（法・対策）
- CSR「企業の社会的責任」
- コーポレートガバナンス
- 内部統制（会社法、日本版SOX法）
- BCM「事業継続経営」　　etc…

セキュリティ設計

- システム的
- 物理的
- 管理的
- 人的

でもこれって
セキュリティ？

それでも
インシデントは
多発？

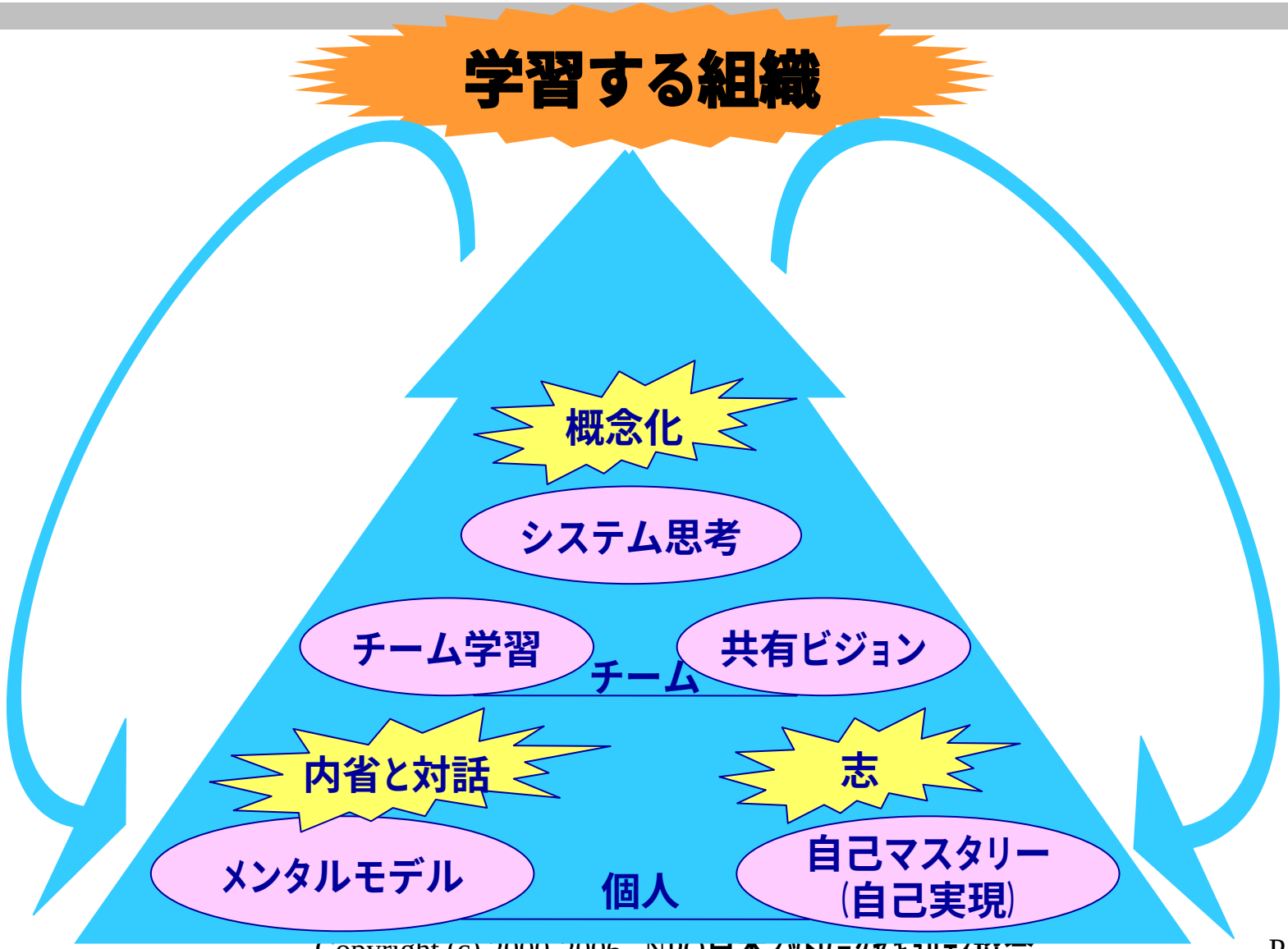
問題の根本は？

- 意識やモラルの問題
  - 正社員化、報酬、賞罰
    → 長期的に見てほとんど影響しない
  - 組織成立要件（意思疎通、貢献意欲、共通目的）
    いわゆるマインドセットといわれる部分
    → 大きく影響

解決のための糸口

- マインドセットを鍛える仕組みを作ること
  - 組織成立要件（意思疎通、貢献意欲、共通目的）を向上させる仕組みを、業務プロセスに組み込む
- 「学習する組織」の5つの規律を参考に
  - 自己マスタリー（自己実現）
    自分のあるべき姿を明確にし、自分の選んだ目標に向かって自己啓発を続ける組織環境を作り出す
  - メンタルモデル
    各自が持っている思い込みや固定概念を内省し改善し続ける
  - 共有ビジョン
    組織内のメンバーが目的意識を共有し、良い意味で一枚岩になるための重要な要素
  - チーム学習
    チームのメンバーの望んでいる成果を生み出すために、対話を通じて個人の総和以上の力を生み出そうとするもの
  - システム思考
    様々な要素が複雑に絡み合っている問題を、相互関係を明らかにしながら解決策を見出すもの

5つの規律の関係性



人材・組織開発の構成要素

	個人	組織
スキルセット	一般的な座学や 実機演習などの 研修コース	ISO27001 etc／ISMS による運用体制
マインドセット	“学習する組織”などの構築	

マインドセットに働きかける
スキルセット強化の仕組み
(教育コースや運用体制)も必要