
Cybersecurity-Frameworkを用いた 対策案合意形成手法の提案

東京電機大学 情報セキュリティ研究室
福島章太

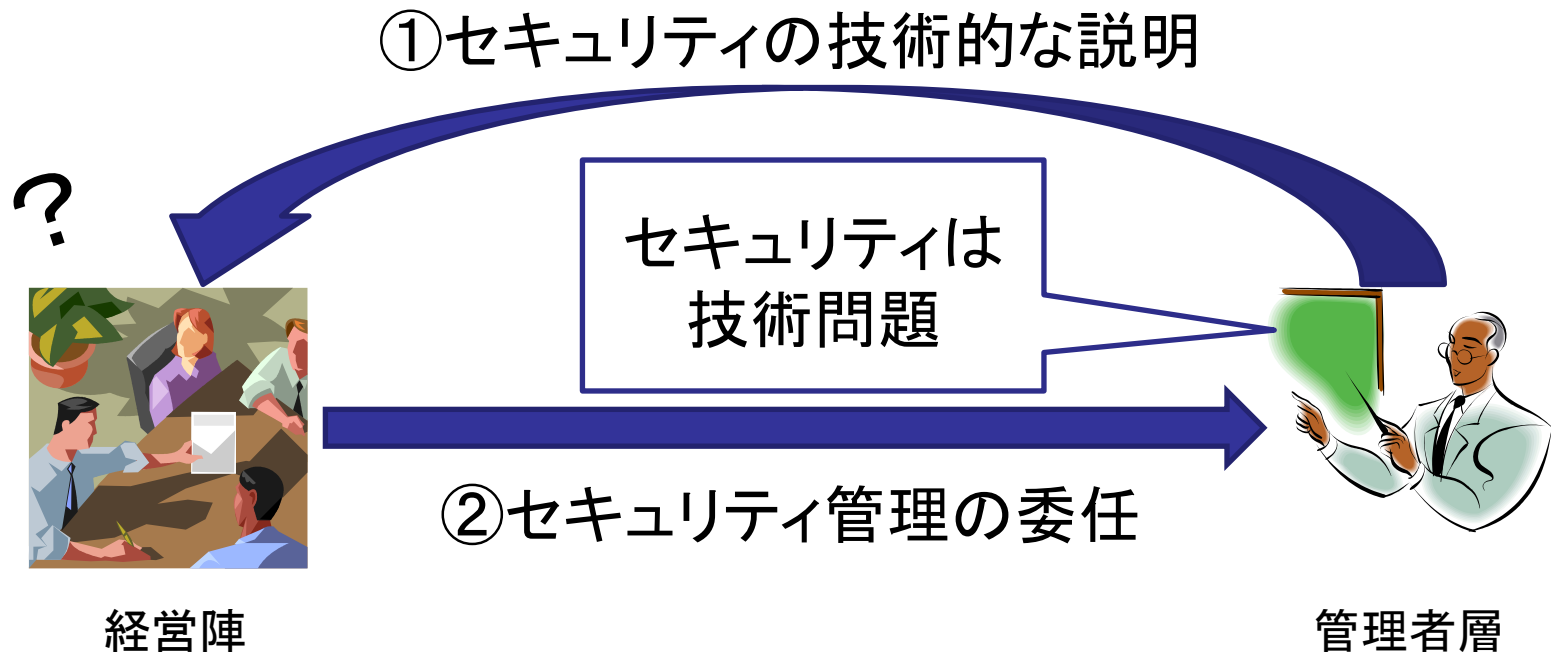
- 背景
- 課題
- 提案
- 実装
- 今後の方針
- まとめ

- 背景
- 課題
- 提案
- 実装
- 今後の方針
- まとめ

- 現状
- Cybersecurity-Frameworkについて
- IntelのCybersecurity-Framework利用例
- 本研究の目的について

- 現状
- Cybersecurity-Frameworkについて
- IntelのCybersecurity-Framework利用例
- 本研究の目的について

- 経営陣と管理者層のセキュリティ管理に対する共通認識が乏しい



係長セキュリティから社長セキュリティへ: 日本的経営と情報セキュリティ,
2010年, 林紘一郎「情報セキュリティ総合科学第2号」収録

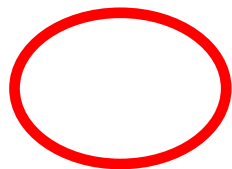
- アプローチの一つ「Cybersecurity-Framework」

- 現状
- Cybersecurity-Frameworkについて
- IntelのCybersecurity-Framework利用例
- 本研究の目的について

■ Cybersecurity-Frameworkとは

- ▶ 2014年に米国国立標準技術研究所(NIST)が公表
- ▶ セキュリティリスク管理原則を企業が適用できるようにする
- ▶ セキュリティのリスクを把握・管理・表現することを補助する
- ▶ 3つの要素から成り立つ
 - フレームワークコア
 - フレームワークインプレメンテーションティア
 - フレームワークプロファイル

- フレームワークコアとは
 - ▶ セキュリティリスクを管理する上で役に立つ主な成果一覧
 - ▶ 機能、カテゴリー、サブカテゴリー、参考情報からなる



■ フレームワークインプレメンテーションティアとは

- ▶ 企業がセキュリティのリスクをどのように捉えているか、リスク管理にどのようなプロセスを実施しているかの段階
- ▶ ティア1～ティア4まで段階がある

ティア1:
部分的である

ティア2:
リスク情報を
活用している

ティア3:
繰り返し適用
可能である

ティア4:
適応している

- フレームワークプロファイルとは
 - ▶ 企業の要件に基づいて調整されたフレームワークコア
 - ▶ 企業がフレームワークコアから必要なカテゴリーを選択し、それに基づいて現状や目標を記述する
 - ▶ サイバーセキュリティの現状と目標を比較する為に使用可能

■ まとめ

フレームワークコア（コア）

- ・ 対策をすることで効果が得られることが認められた分野一覧

フレームワークインプレメンテーションティア（ティア）

- ・ リスク管理の認識やプロセスを4段階で示したもの

フレームワークプロファイル（プロファイル）

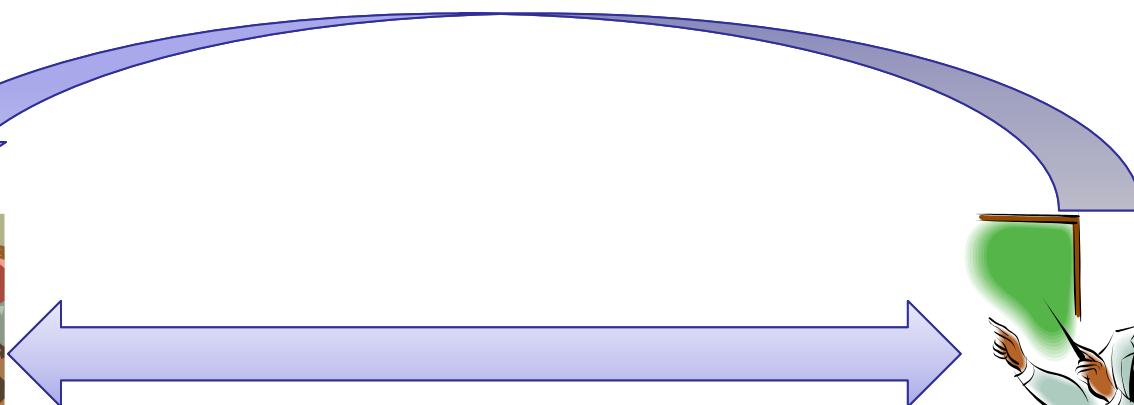
- ・ 企業がコアから必要なカテゴリーを抜粋し、評価したもの

■ 経営陣と管理者層のリスクコミュニケーションに有効

①評価したプロファイルで現状のセキュリティを説明



経営陣



②リスクコミュニケーション



管理者層

どの規模の企業にもそのまま適用可能ではない
→各企業で部分的に**独自のカスタマイズが必要**

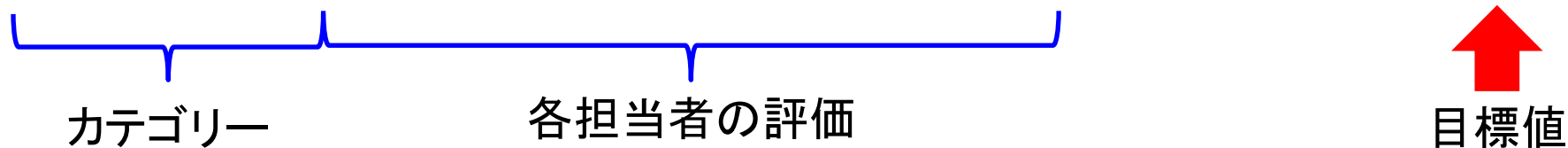
- 現状
- Cybersecurity-Frameworkについて
- IntelのCybersecurity-Framework利用例
- 本研究の目的について

■ Pilot Projectについて

- ▶ 米Intel社は“Pilot Project”としてフレームワークを試用した
- ▶ 4つのフェーズで7ヶ月間行動
 1. ティアの目標設定
 2. 現状評価
 3. 結果を分析
 4. 結果を協議

- プロジェクトの全体的な方針について
 - ▶ コアのサブカテゴリーは簡略化のため利用しない方針にした
→代わりにカテゴリーを独自に充実させた
 - ▶ ティアについて
→ティア毎に独自の定義を設け、評価の指標とした

- 評価結果について
 - ▶ 各担当者の現状評価とティアの目標値を比較した



■ まとめ

CISOやCISO補佐等のセキュリティ専門家が
カテゴリー毎に目標ティアを設定



各分野の担当者がカテゴリー毎に現状のティアを入力



目標と現状を比較し、意思決定者とコミュニケーション

- 現状
- Cybersecurity-Frameworkについて
- IntelのCybersecurity-Framework利用例
- 本研究の目的について

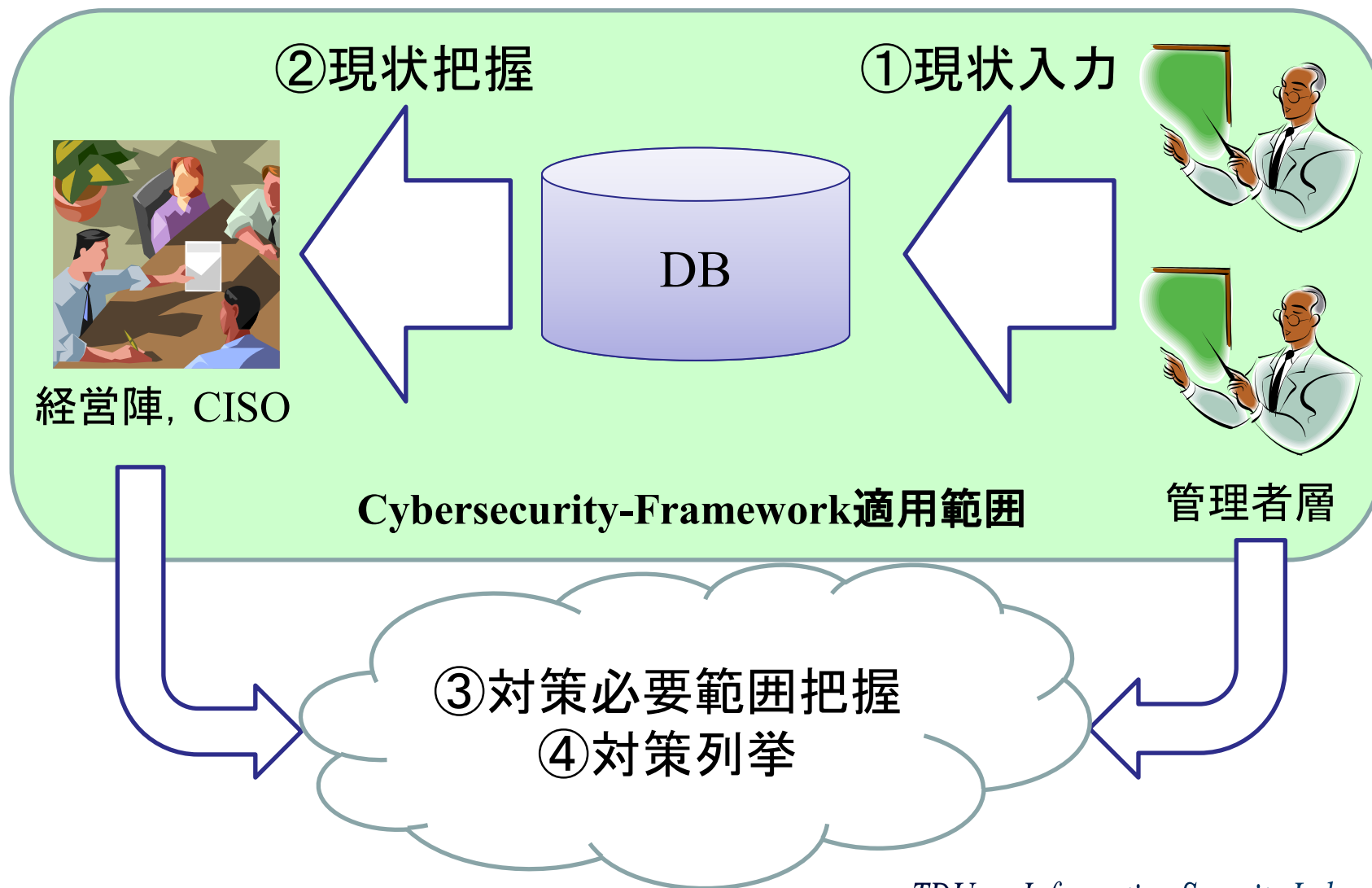
■ Cybersecurity-Frameworkの課題

- ▶ 組織の要件を満たすためには**目標に至るための対策**が必要
- ▶ フレームワークは現状と目標の差異を分析するためのもの



対策案を列挙・選定するという部分まで至っていない

■ 経営陣・管理者層の利用イメージ



- 本研究の目的

- ▶ 現状のティアが目標に到達するための対策を列挙し、
選定する手法が必要



Intelの利用例を基に対策列挙手法を提案

■ 本研究の目的



- 背景
- 課題
- 提案
- 実装
- 今後の方針
- まとめ

■ 現状把握イメージ

	管理者1	管理者2	管理者3	管理者4	目標値
カテゴリー 1	1	2	2	2	2
カテゴリー 2	2	3	1	2	3
カテゴリー 3	1	2	1	3	3
カテゴリー 4	4	3	3	4	4
カテゴリー 5	3	4	3	4	4

- 一般的に対策の効果は定量的・定性的に表される
- 対策列挙をする際の課題
 - ▶ 従来の様に対策の効果の数値とすると問題が発生する
 - 対策1と2を実行しただけでティアの定義を満たすとは限らない

対策一覧

対策名	上昇ティア
【対策1】 外部講師による教育	0.7
【対策2】 リスク情報で対策会議	0.5

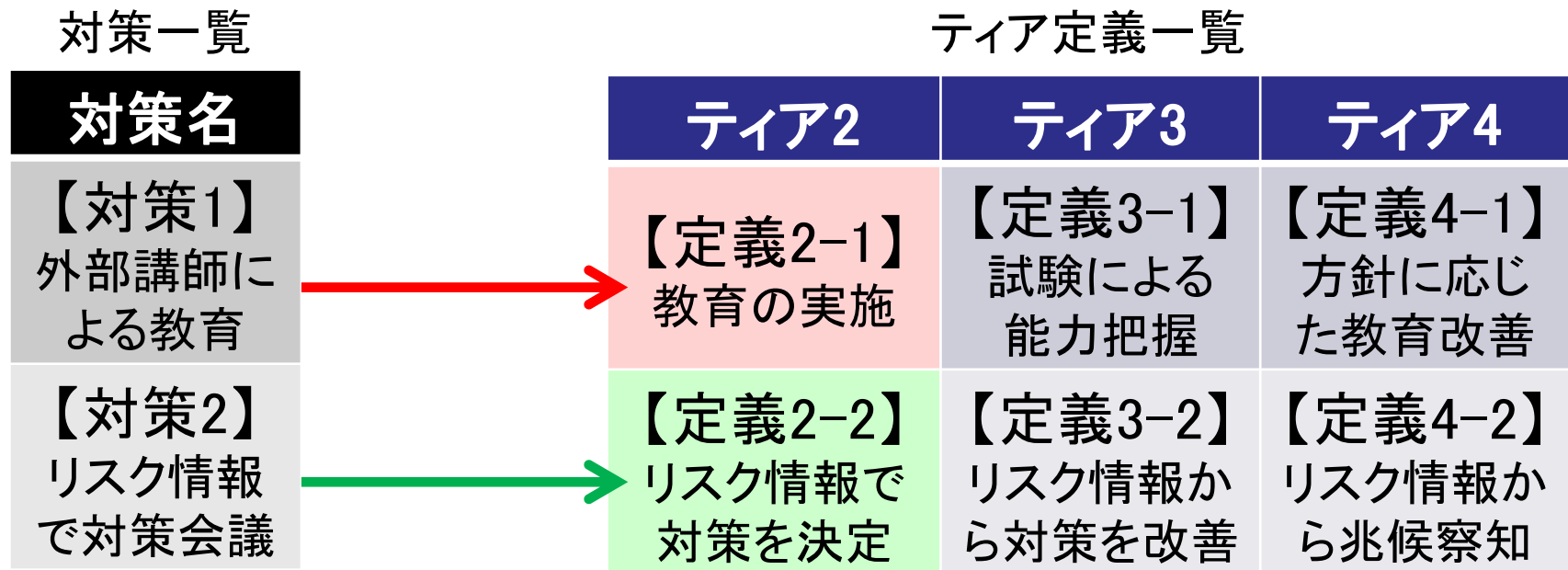
ティア定義一覧

ティア2	ティア3	ティア4
【定義2-1】 教育の実施	【定義3-1】 試験による能力把握	【定義4-1】 方針に応じた教育改善
【定義2-2】 リスク情報で対策を決定	【定義3-2】 リスク情報から対策を改善	【定義4-2】 リスク情報から兆候察知

- 背景
- 課題
- 提案
- 実装
- 今後の方針
- まとめ

- 対策の効果を、ティア定義の不足部分を補う形とする

- 例：

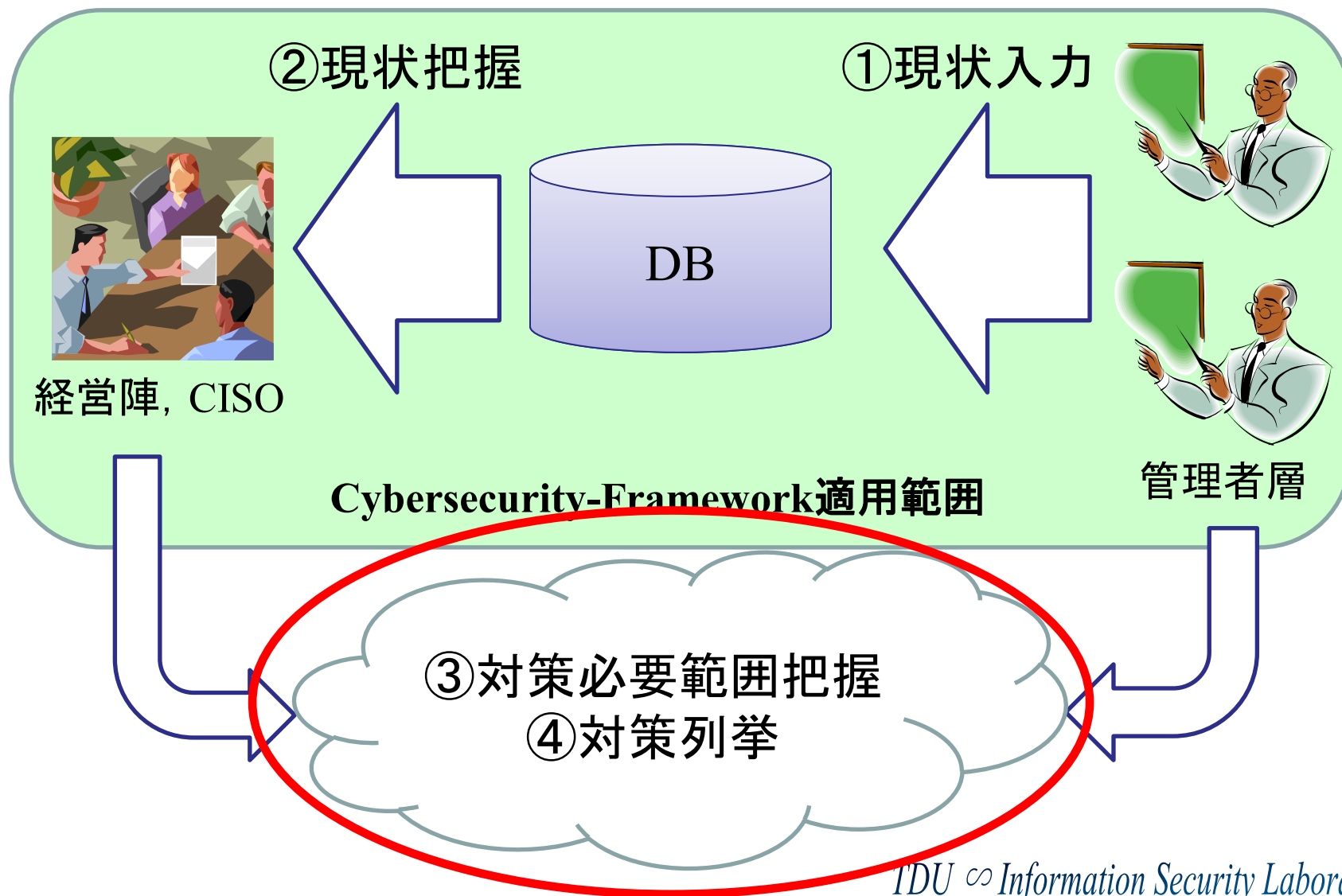


- 満たしたティア定義に応じてティアを算出
 - ▶ 対策後の状況とティアの値に矛盾が無くなる

ティア定義一覧

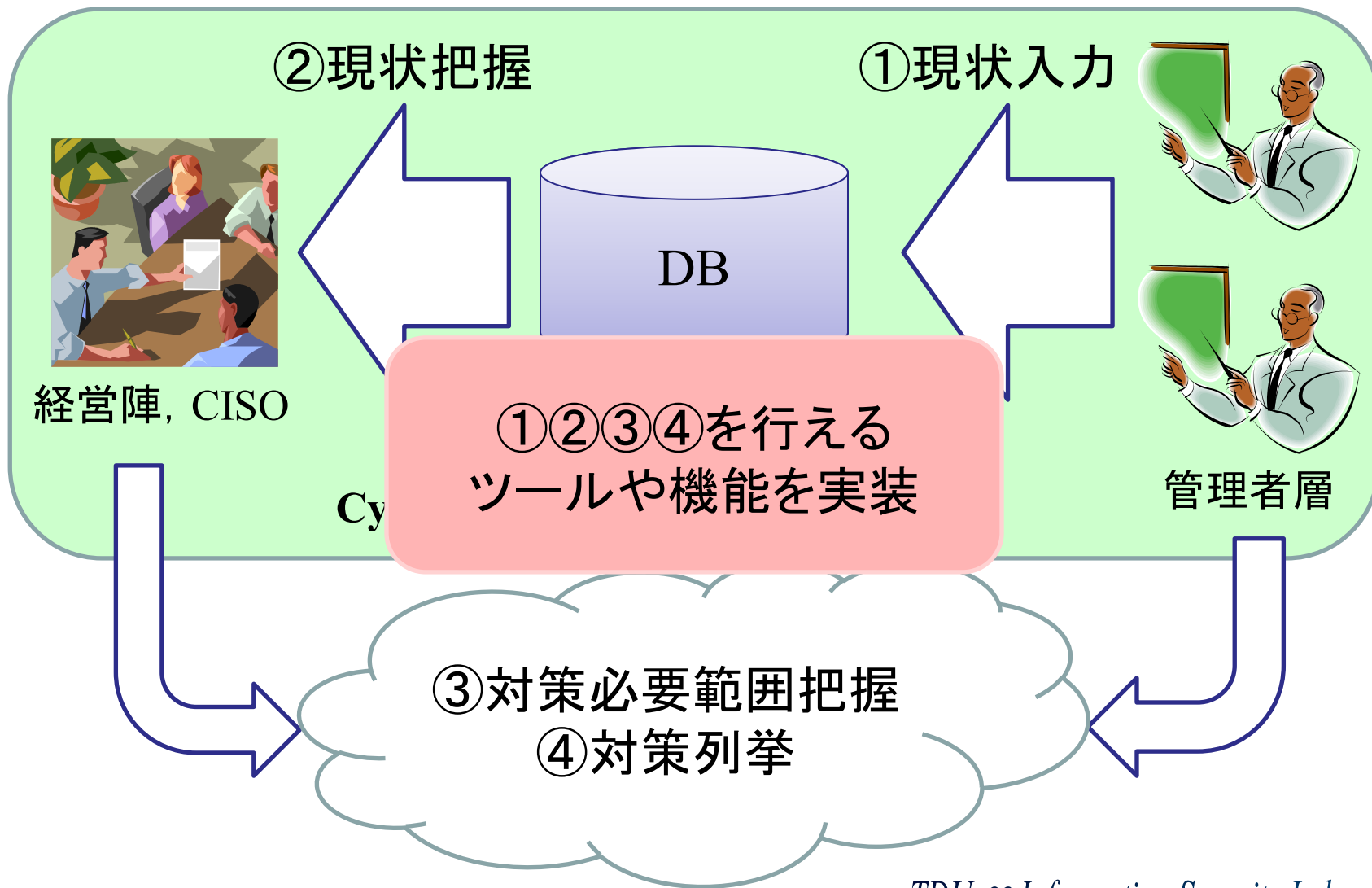
ティア2	ティア3	ティア4
【定義2-1】 教育の実施	【定義3-1】 試験による 能力把握	【定義4-1】 方針に応じた教育改 善
【定義2-2】 リスク情報で優先順 位付け	【定義3-2】 リスク情報から対策 を改善	【定義4-2】 リスク情報から兆候 察知

■ 経営陣・管理者層の利用イメージ



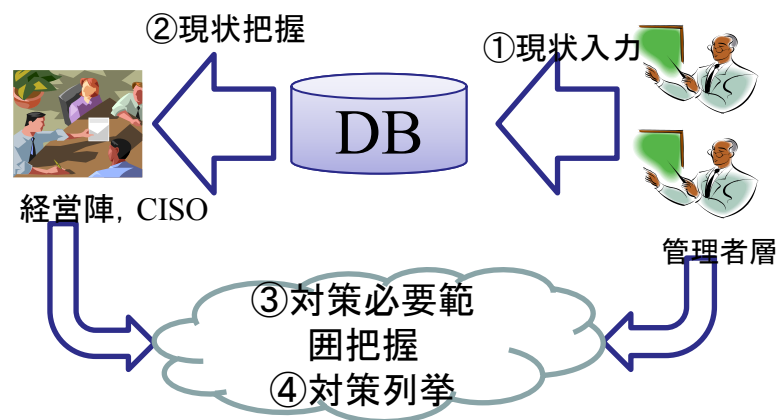
- 背景
- 課題
- 提案
- 実装
- 今後の方針
- まとめ

■ 経営陣・管理者層の利用イメージ

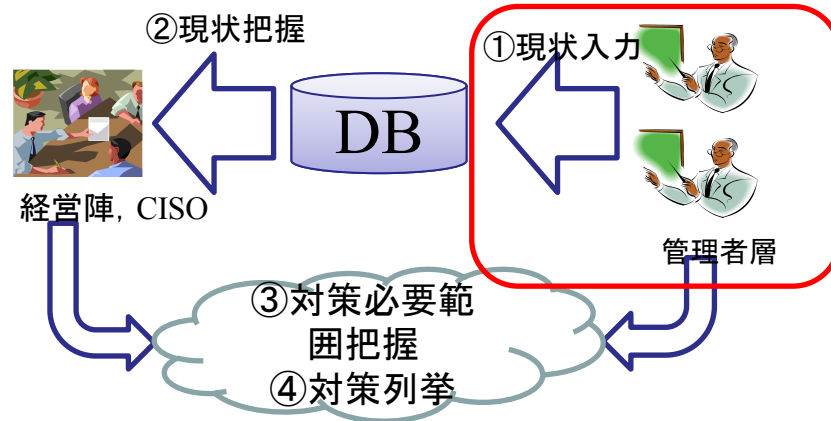


■ 開発ツール・機能一覧

- ① 現状入力ツール
- ② 現状把握ツール
- ③ 対策必要範囲把握機能
- ④ 対策列举機能



■ 現状入力イメージ



評価対象 (カテゴリー一覧)



管理者

カテゴリー名
カテゴリー1
カテゴリー2
カテゴリー3

評価項目 (ティア定義一覧)

ティア2	ティア3	ティア4
定義2-1	定義3-1	定義4-1
定義2-2	定義3-2	定義4-2
定義2-3	定義3-3	定義4-3

- 管理者に対する現状入カツール
 - ▶ カテゴリー毎に達成しているティア定義を選択可能
 - ▶ 満たしているティア定義から現状のティアを算出
 - ▶ ティア定義に厳密な現状評価が可能となった

現状入カツール

ID.AM資産管理

説明

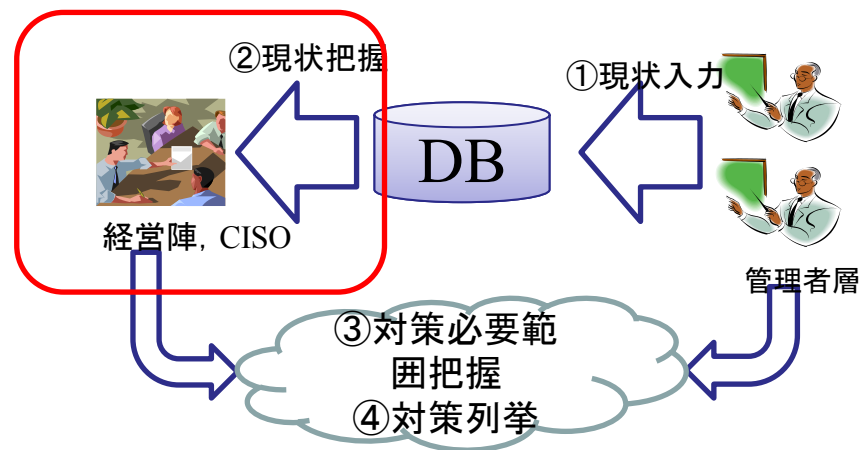
組織が事業目的を達成することを可能にするデータ、職員、デバイス、システム、施設を特定し、事業目標と自組織のリスク戦略との相対的重要性に応じて管理している。

ティア

ID	定義
2-1	従業員はトレーニングを受けている。
3-1	従業員は責任と役割を理解している。
3-2	従業員は責任と役割を実行できるスキルを持っている。
4-1	従業員は企業のニーズに合わせて自ら知識を拡充している
4-2	従業員は定期的に講演を受けている。

次へ

■ 現状把握イメージ



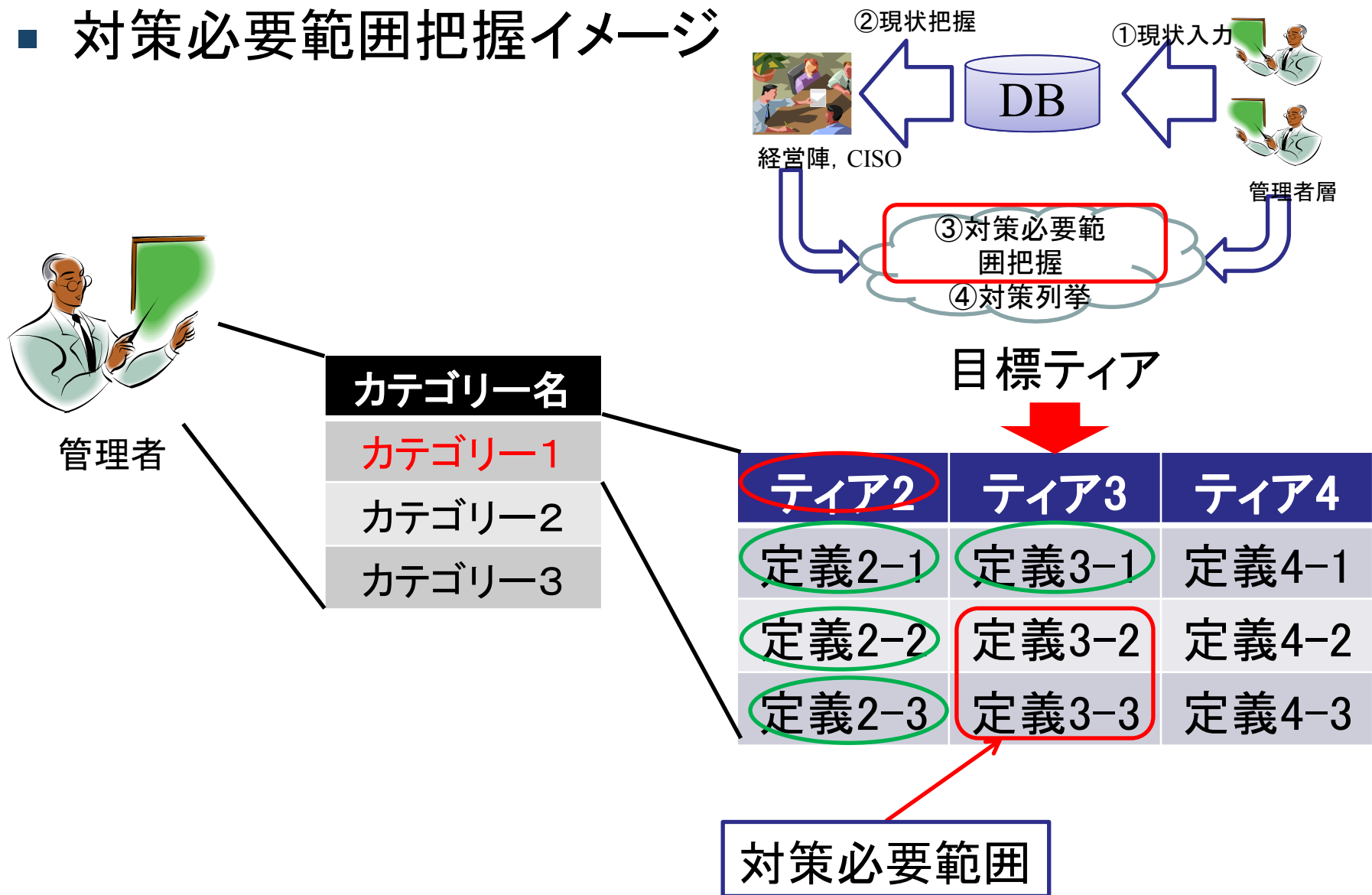
	管理者1	管理者2	管理者3	管理者4	目標値
カテゴリー 1	1	2	2	2	2
カテゴリー 2	2	3	1	2	3
カテゴリー 3	1	2	1	3	3
...	...	...	...	...	...

■ 現状把握ツール

- ▶ 管理者毎にどのティアに至っているか閲覧可能
- ▶ 管理者と経営陣の認識の差異を比較することも可能
- ▶ 経営陣に対してティアの数値による現状報告が可能となった

カテゴリ名	ネットワーク	データプロテクション	管理者平均	経営陣評価	全体平均	目標値	リスクギャップ
▼ 機能							
▼ 特定							
資産管理	3	1	2	2	2	3	-1
ガバナンス	2	2	2	3	2	4	-2
リスクアセスメント	2	2	2	2	2	4	-2
リスク管理戦略	1	2	1	2	1	3	-2

■ 対策必要範囲把握イメージ

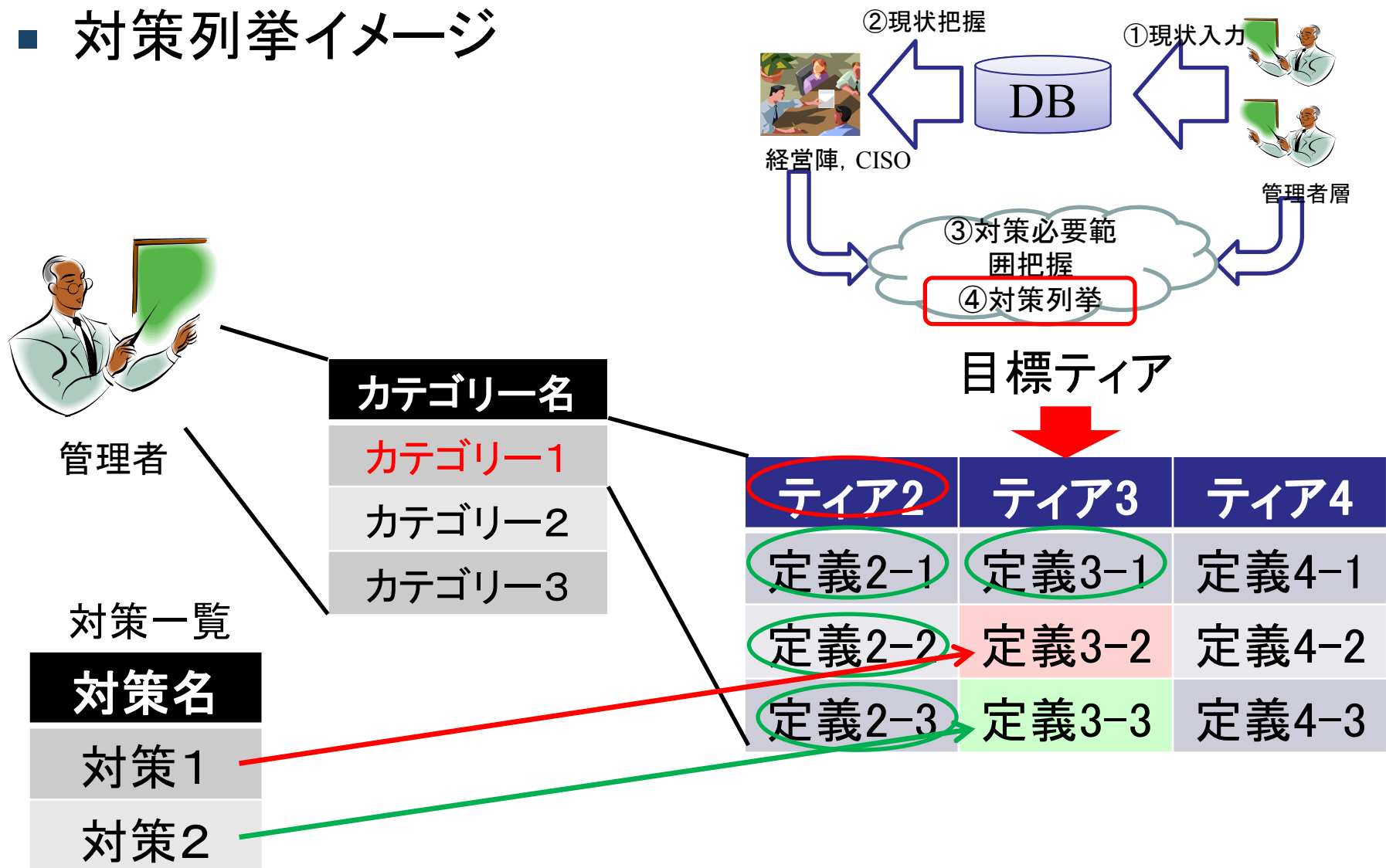


■ 対策必要範囲把握機能

- ▶ ○ : 現状満たしているティア定義
- ▶ × : 満たす必要があるティア定義 (対策が必要な部分)
- ▶ — : 満たす必要がないティア定義

カテゴリ名	2-1	3-1	3-2	4-1
▼ カテゴリ				
▼ 資産管理				
ネットワーク	○	○	○	—
データプロテクション	×	×	×	—

■ 対策列举イメージ



- ▶ 対策が影響する管理者、カテゴリー、ティア定義を選択可能
- ▶ 定義に厳密な対策を列挙することが可能となった

TDU ∞ Information Security Laboratory

■ 提案・実装の利点

- ▶ フレームワークの、目標と現状の差分を取るという点に加え、目標に至る為に**対策が必要な範囲が分かるようになった**
- ▶ 目標に至るための**具体的な対策を列挙出来るようになった**



- 背景
- 課題
- 提案
- 実装
- 今後の方針
- まとめ

- 提案の実用性を検証
- 対策選定を補助する機能作成
 - ▶ 各対策の効果を明示する機能
 - ▶ 対策後のティアを表示する機能
 - ▶ 対策案の最適化
- 機能・利便性の充足
 - ▶ カテゴリー編集機能
 - ▶ GUIの調整
 - ▶ プログラムの最適化

- 背景
- 課題
- 提案
- 実装
- 今後の方針
- まとめ

- 経営陣と管理者層のセキュリティリスクに対するコミュニケーションが上手くいっていない
 - ▶ NISTのCybersecurity-Frameworkというアプローチがある
- フレームワークは対策について講じられていない
 - ▶ Intelの例から経営陣との合意を図れる対策列挙手法を提案
 - ▶ 対策列挙手法を利用出来るようにツールを実装
- 提案・実装により目標に至るための対策列挙が可能に
- 今後は提案手法の実用性を検証する

試適用のプロセス案

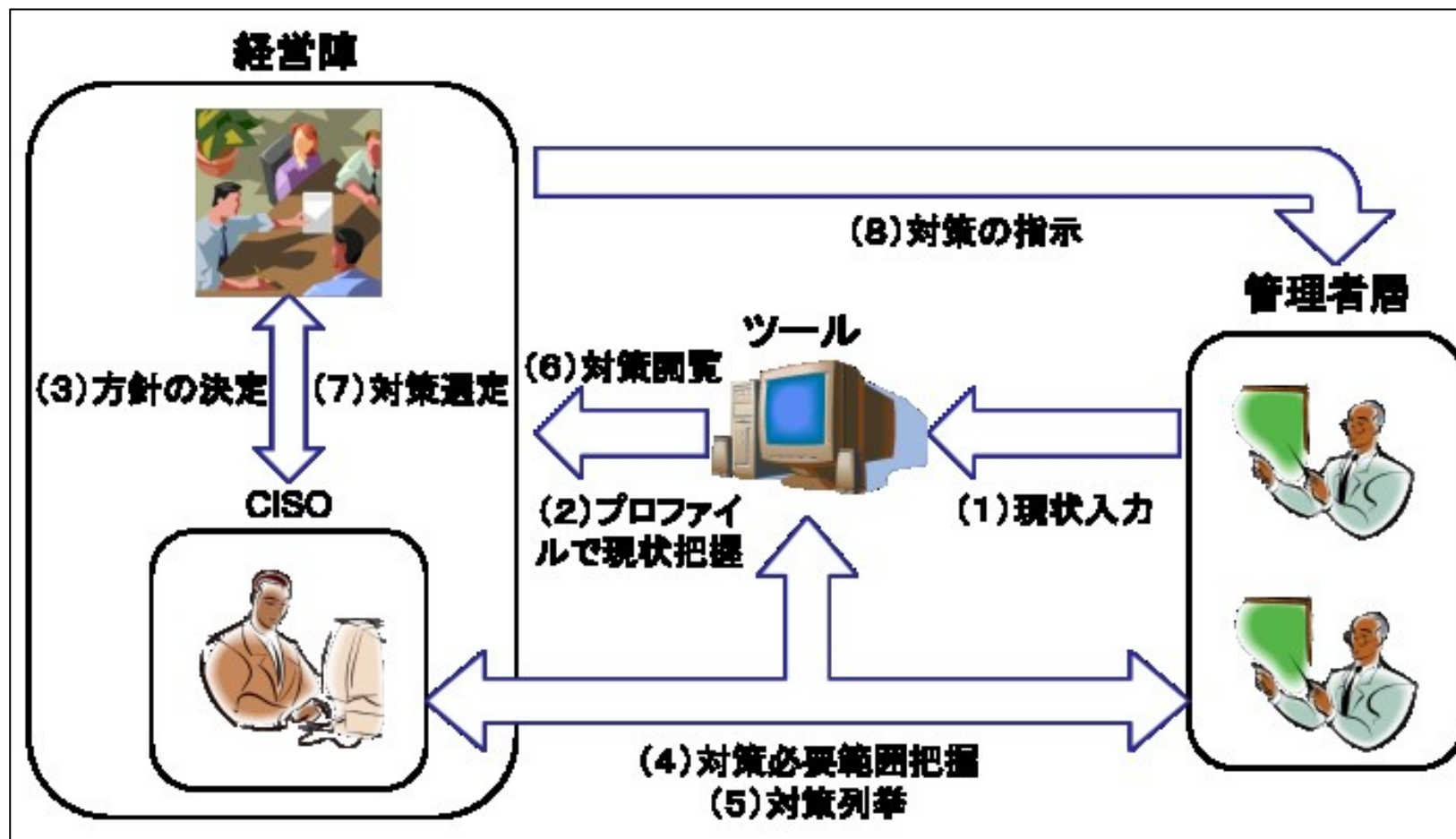
東京電機大学 情報セキュリティ研究室
福島章太

- 各管理者・カテゴリー毎のティアを
目標値にするための対策を列挙する手法を提案

	管理者1	管理者2	管理者3	管理者4	目標値
カテゴリー 1	1→2	2	2	2	2
カテゴリー 2	2	3	1	2	3
カテゴリー 3	1	2	1	3	3
...	...	...	...	...	...

- 研究室内の情報管理体制に不備はないか
- 提案手法である対策列挙手法は実行可能か
- 列挙した対策を実行することでティアは上昇するか
(or ティアの定義が部分的にでも満たされるか)

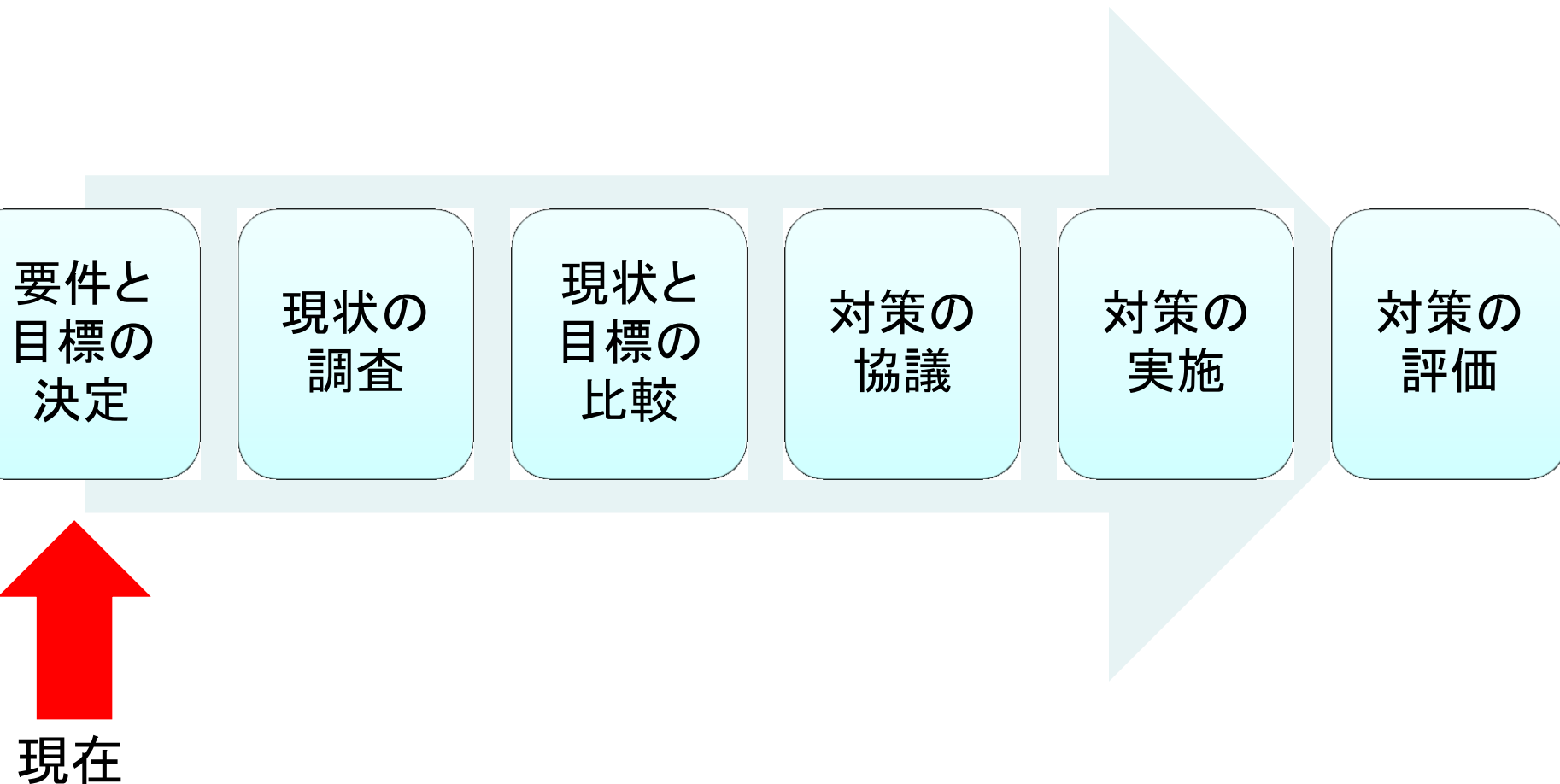
■ 提案手法のプロセス



■ 試適用の役割分担案

- ▶ 経営陣: 佐々木先生 (結果閲覧と対策指示)
- ▶ CISO: 福島 (試適用の進行役)
- ▶ 管理者層: 研究室内の各系のリーダー
(主に外部に漏れてはいけない情報を持つ係)

■ プロセス案の概念図



- 経営陣と管理者層のセキュリティリスクに対するコミュニケーションが上手くいっていない
 - ▶ NISTのCybersecurity-Frameworkというアプローチがある
- フレームワークは対策について講じられていない
 - ▶ Intelの例から経営陣との合意を図れる対策列挙手法を提案
 - ▶ 対策列挙手法を利用出来るようにツールを実装
- 提案・実装により目標に至るための対策列挙が可能に
- 今後は提案手法の実用性を検証する