【磐梯町職員勉強会資料】

価値創出のためのデジタルガバナンス

～磐梯町DX戦略を支える守りと攻めの情報セキュリティ～

技術士事務所　稲葉ITガバナンス研究所

稲葉　裕一

2021年5月24日

デジタル価値創出のための磐梯町ガバナンスについて、DX戦略を支える情報セキュリティの観点から、民間企業で取組んだ事例を基に説明いたします

概要説明（アブスラクト）

5月12日に国会でデジタル改革関連法が可決・成立しました。9月1日にはデジタル庁が設置され政府は日本全体のデジタル社会形成に向けて活動が加速されます。

磐梯町においては、他の地方自治体と同様に少子高齢化、地域経済の停滞等、様々な課題に直面しています。そのため、「誰もが自分らしく生きられる共生社会」というミッションと、「自分たちの子や孫たちが暮らし続けたい魅力あるまちづくり」というビジョンを実現するため、磐梯町のデジタル社会形成に向けたDX（デジタルトランスフォーメーション）に取り組んでいるとお聞きしました。

デジタルやITを手段に真の価値を創出するためには、利便性向上等の「効果」の実現と、情報セキュリティ等の「リスク」や費用対効果等の「資源」の管理について、それらのバランスを取る「ITガバナンス」が極めて重要です。

本勉強会では、策定済みで既に実行に移している磐梯町のDX戦略をさらに進め【効果】、町民や政府（国民）からお預かりした大切な税金、交付金を最大限有効活用するために【資源】、車の両輪としての「攻め」と「守り」の情報セキュリティ管理態勢を整備すること【リスク】について議論していきます。

実践事例として、講師が大手損害保険会社在職時に主体的に対応した、同保険グループのITサービス会社の情報セキュリティ管理態勢の整備について紹介いたします。

そして、この事例を参考に、磐梯町の情報セキュリティマネジメントシステム（ISMS）を構築・導入し、ISMS認証を取得して、DX戦略実行へアクセルペダルを踏み込んで行くことを皆様と一緒に考えます。

本資料の意見に関する部分については講師の私見であり、講師が所属していた組織や関連する団体の公式見解ではありません。

大手損害保険グループや大手監査法人において、また、政府CIO補佐官として、DXガバナンスや情報セキュリティに豊富な実務経験を持つITガバナンスの専門家です

講師紹介

技術士事務所 稲葉ITガバナンス研究所

稲葉 裕一（いなば　ゆういち）

技術士（情報工学部門）、公認情報システム監査人（CISA）、システム監査技術者

■ 主な業務経歴

- 大手損害保険グループの持株会社においてCOBIT 4.1を活用したグローバルグループITガバナンス態勢の構築に従事
- 大手損害保険グループのITサービス会社においてCOBIT 5を活用したGRC態勢の構築に従事
- 大手監査法人にてCOBIT 5を活用した金融機関向けITガバナンス態勢構築の助言・支援サービス提供に従事
- 内閣官房IT総合戦略室の政府CIO補佐官として、府省のデジタル・ガバメント計画にPMO、PJMOとして従事すると共に、デジタル庁設置に伴うデジタル社会形成価値創出のためのITガバナンス態勢整備の論議に参画

■ ISACA活動

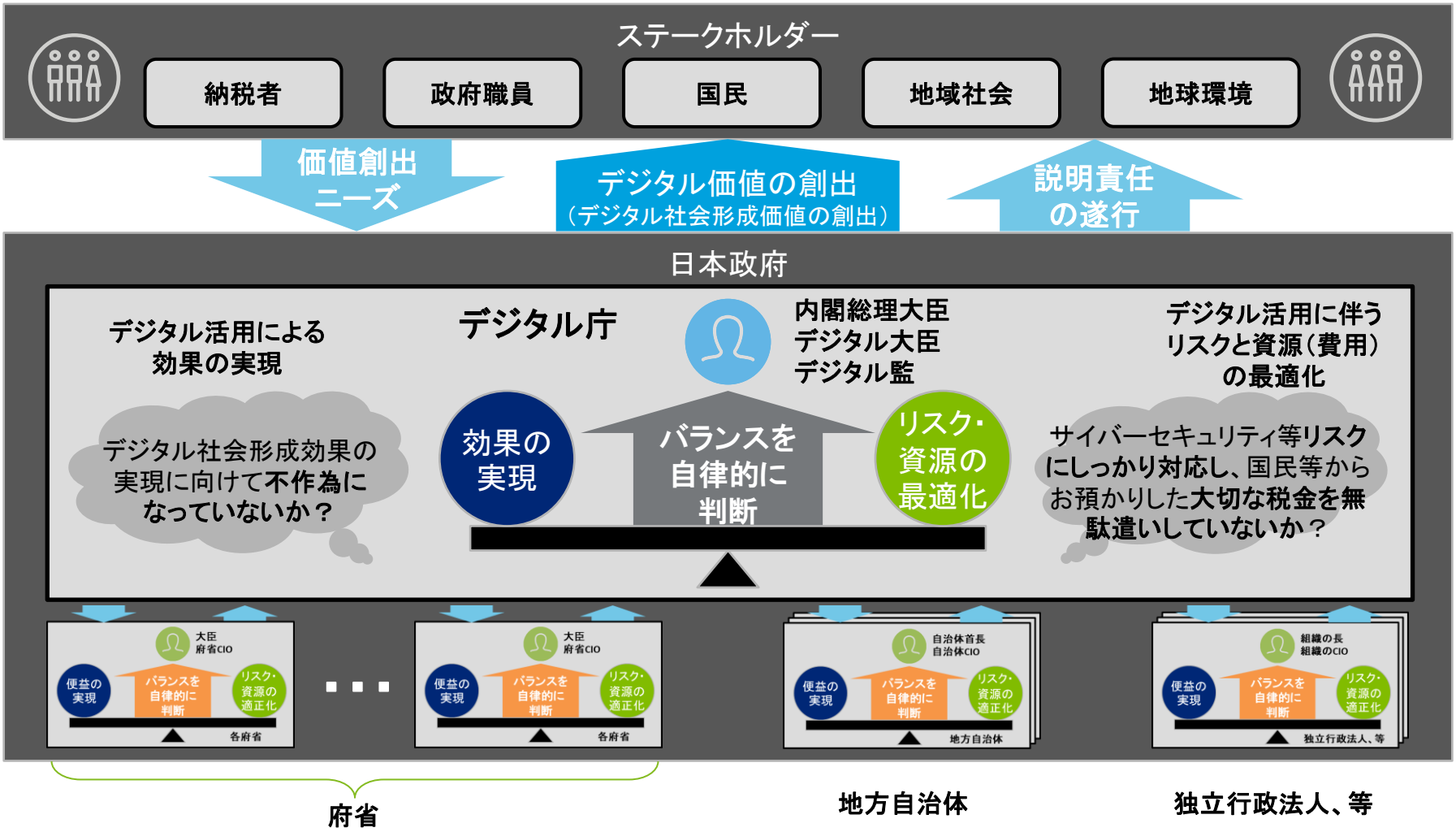
- 東京支部基準委員（COBIT関連文書の翻訳やCOBITの国内普及活動に従事）
- ISACA国際本部 前GRASC1委員（アジア・パシフィック地域 政府・規制当局等提唱委員）
- ISACA国際本部 前CEATF委員（COBIT Enterprise Assessment Task Force）

目次

Ⅰ. 政府全体のガバナンス

デジタル社会形成価値を創出するため、政府はデジタル庁を設置して、効果の実現とリスクや資源の最適化のバランスを自律的に判断するITガバナンスに取り組みます

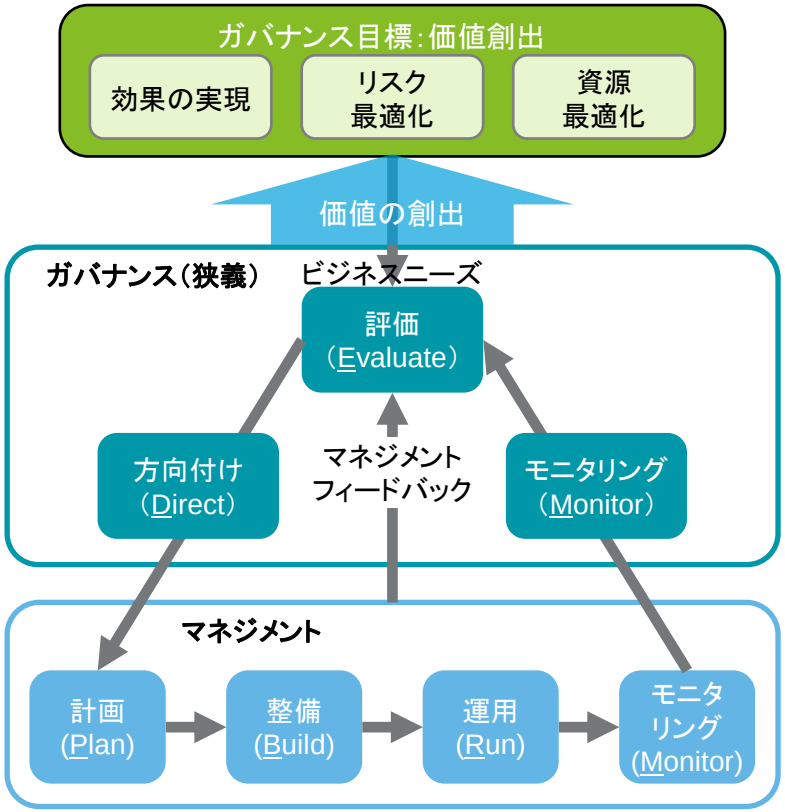
デジタル庁主体による政府全体のITガバナンス



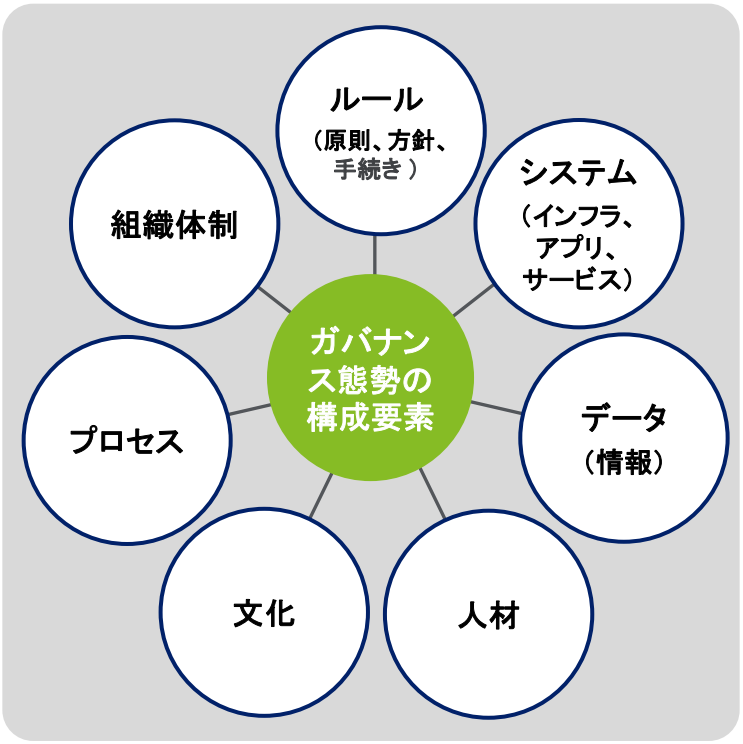
デジタル社会形成価値創出のためには、COBITフレームワークを参考に、7つのガバナンスの構成要素を意識して、ITガバナンス態勢を整備する必要があります

価値創出のための政府全体のITガバナンス態勢の整備

ガバナンス態勢の全体像



7つのガバナンス態勢の構成要素



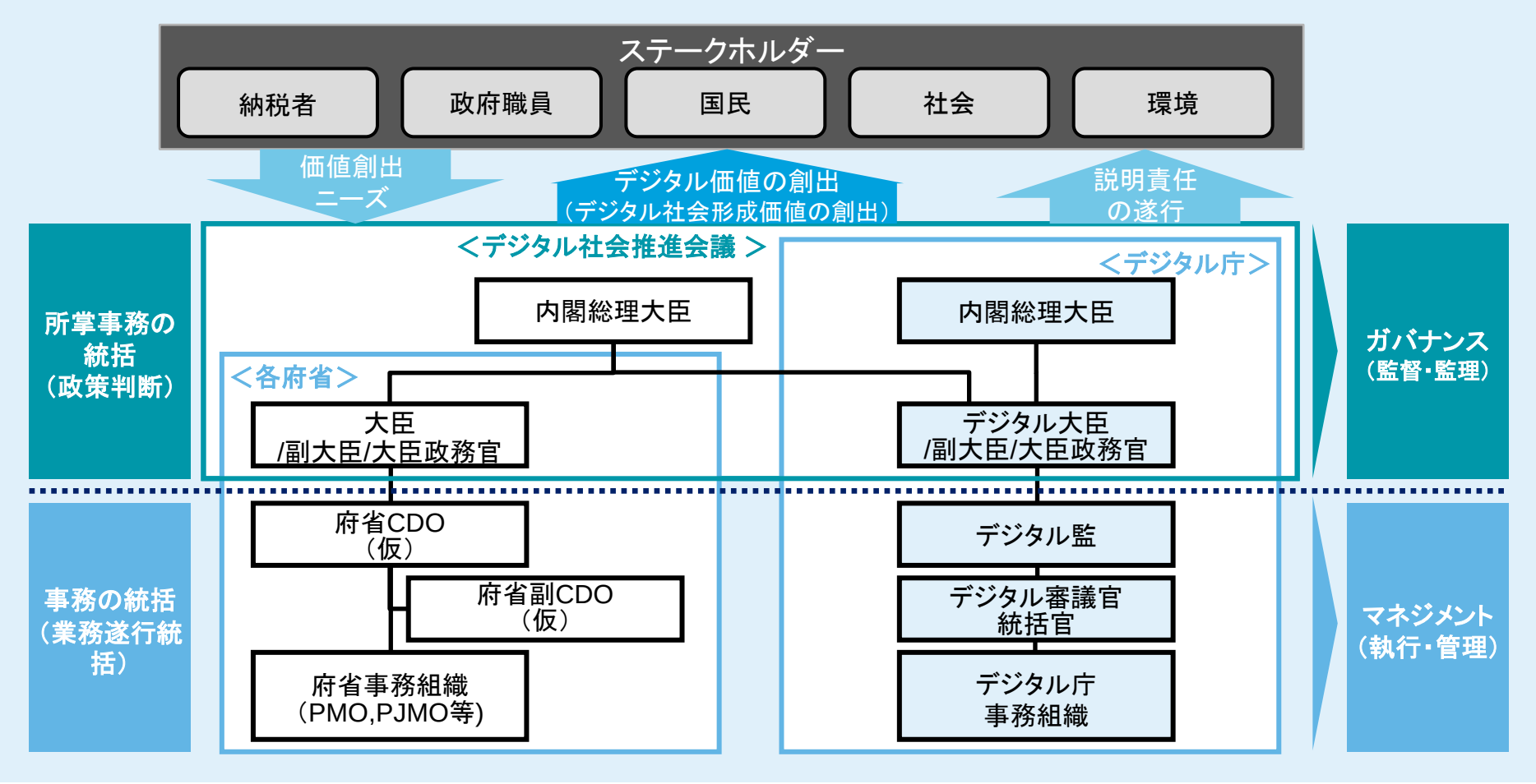
出所：COBIT® 2019 フレームワーク：序論および方法論, 2018年12月（一部講師が加筆修正）

（注1）COBIT（Control OBjectives for Information and related Technology）は、非営利団体ISACAが提供するITガバナンスのためのフレームワーク。

（注2）「ガバナンス態勢」における「ガバナンス」とは、「ガバナンス（狭義）＝監督・監理」と「マネジメント＝ 執行・管理」の両者を含めた広義の意味で使っている

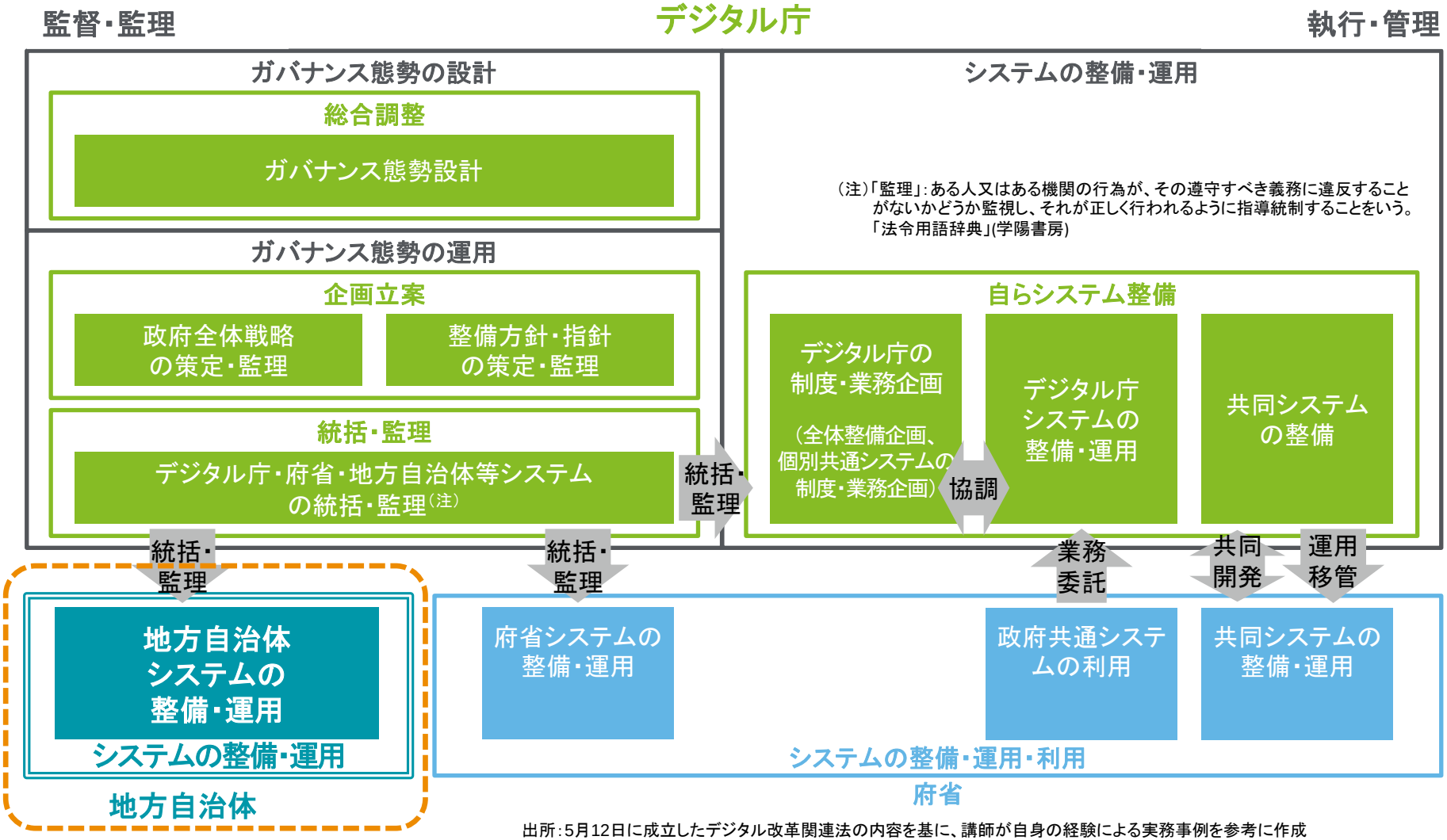
成立したデジタル改革関連法に従って、総理大臣/デジタル大臣のガバナンス（政策判断）の下で、デジタル監のリーダーシップによりマネジメント（事務遂行統括）を行います

政府のガバナンス態勢



デジタル庁は、政府全体のデジタル化推進の司令塔として、各府省や地方公共団体等を含めたITガバナンス態勢によりデジタル価値を創出していきます

政府全体のガバナンス態勢における地方自治体の位置づけ

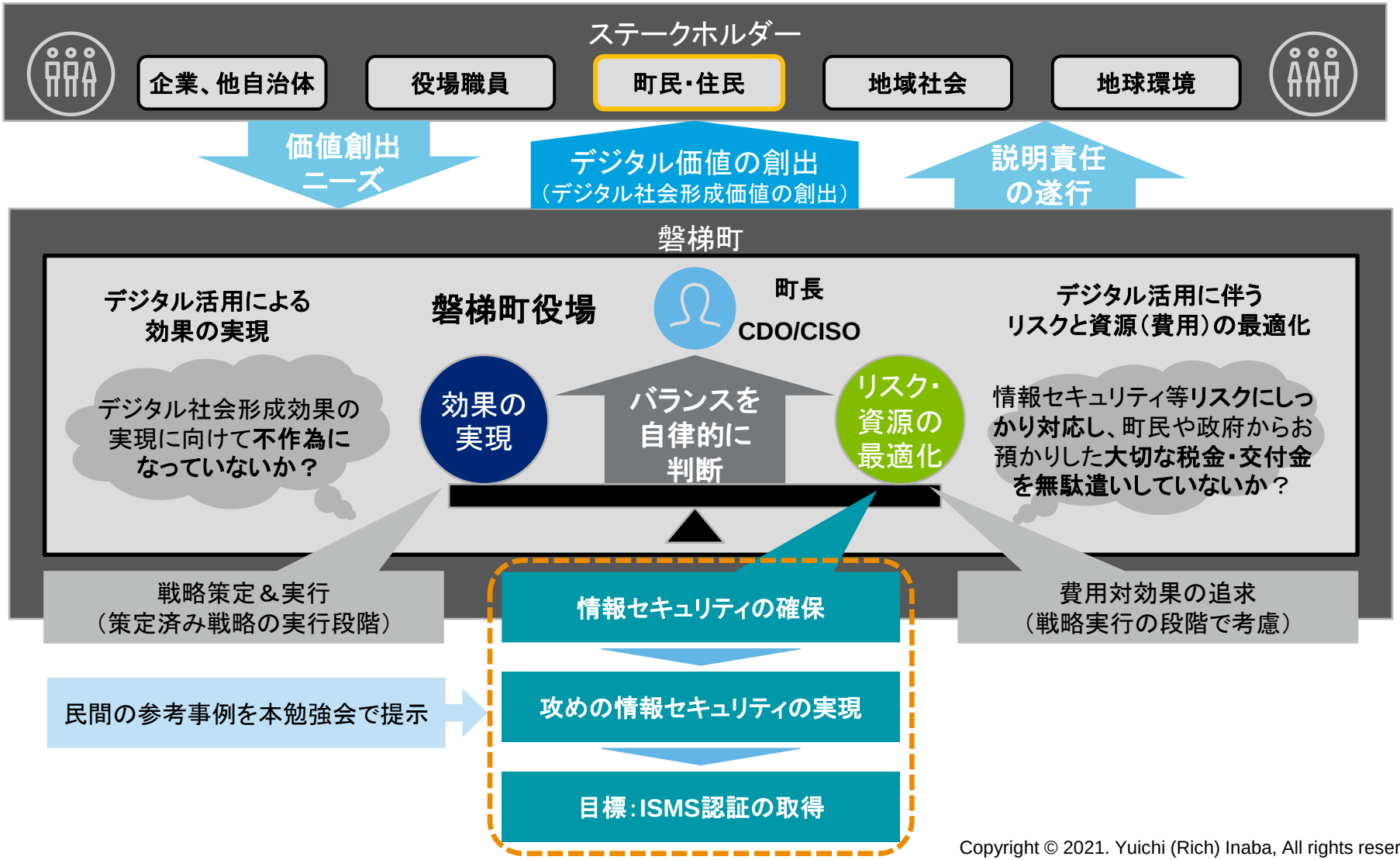


出所:5月12日に成立したデジタル改革関連法の内容を基に、講師が自身の経験による実務事例を参考に作成

Ⅱ. 磐梯町のガバナンス

磐梯町がデジタル社会形成価値を創出していくためには、磐梯町役場の強力なガバナンスが必要であり、取組中のDX戦略に加え攻めの情報セキュリティについて考えます

磐梯町のITガバナンスの方向性（DX戦略と攻めの情報セキュリティ）



磐梯町のDX目標を達成するためのDX戦略の実現に向け、さらに加速させるためには、その基盤となる「守りと攻めの情報セキュリティ」への舵取りが重要です

磐梯町のDX戦略を支える情報セキュリティ

目標

①デジタル化はまちの将来を救う

②デジタル共生社会の実現

③先行者利益の確保

行動指針

職員行動指針の明確化

町のミッション（使命）

町民全員を幸せにする
～共生社会の実現～

町のビジョン（将来像）

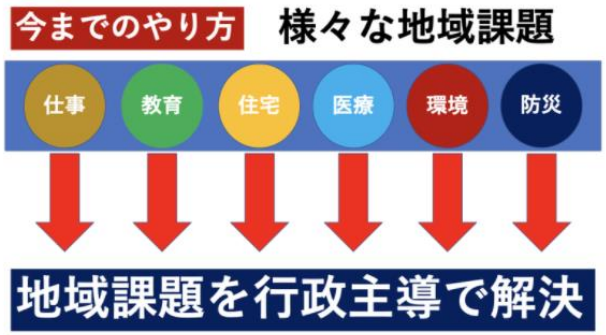
自分たちの子や孫たちが暮らし続けたい魅力あるまちづくり
～共創・協働のまちづくり～

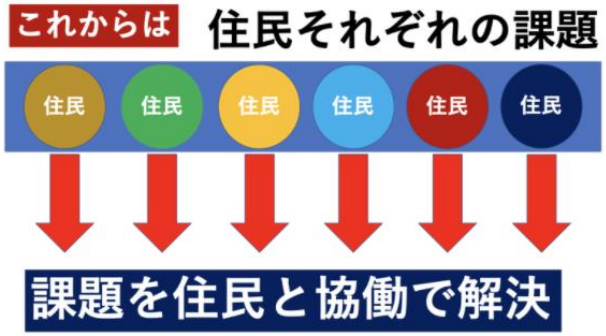
町のバリュー（行動規範）

町民起点（価値観の共有）

※町民『起点』とは、『町民『視点』』と意味が違います。『視点』は町民とは別のサイドに立って考えるという意味ですが、『起点』というのははっきりと町民のサイドに立つことです。

戦略





出所：磐梯町ホームページ（https://bandai-town.note.jp/n/ndd776d4f2319）の画面情報を基に講師が情報を付加

基盤

磐梯町DX戦略実行を支える守りと攻めの情報セキュリティ管理態勢

Ⅲ. 民間企業の情報セキュリティガバナンス態勢整備

～大手損害保険グループのITサービス会社の事例～

（注）本セクションの内容は、講師が大手損害保険会社在職時に取り組んだ情報セキュリティのガバナンスについてであり、
日本CISO協会による2014年度「CISO No.1 of the Year」を受賞した際に提出した評価資料を基に作成しています。
https://cisojapan.org/ciso-award-pr/

講師が大手損害保険会社在職時に取り組んできた、守りから攻めへの情報セキュリティガバナンスの事例について、皆様と共有させていただければと思います

大手損害保険グループのITサービス会社概要

設立	1983年9月 大手損害保険会社のシステム開発会社として設立
沿革	2004年10月 大手損害保険会社と準大手損害保険会社の システム会社3社が合併して 新ITサービス会社として発足
社員数	1,381名（2014年4月1日現在）
業務	大手損害保険グループの情報システムの 企画・提案・設計・開発・保守・運用
お客様	大手損害保険グループの各保険事業会社、等
受賞	日本CISO協会 第1回「CISO 10 Award 2014」

守りの情報セキュリティに追われる現状を打破し、社員がいきいきとスピード感を持って業務遂行できるような、価値創出を目指した攻めの情報セキュリティへ舵を切りました

背景 ～ 守りから攻めに転じる情報セキュリティへ

守りの情報セキュリティばかりで大変 ～ 会社の将来への不安

↓

お客様と気持ちをシェアしてお客様価値を共に創出しなければ・・・

↓

社員がいきいきとスピード感を持って業務遂行できるようにしたい

↓

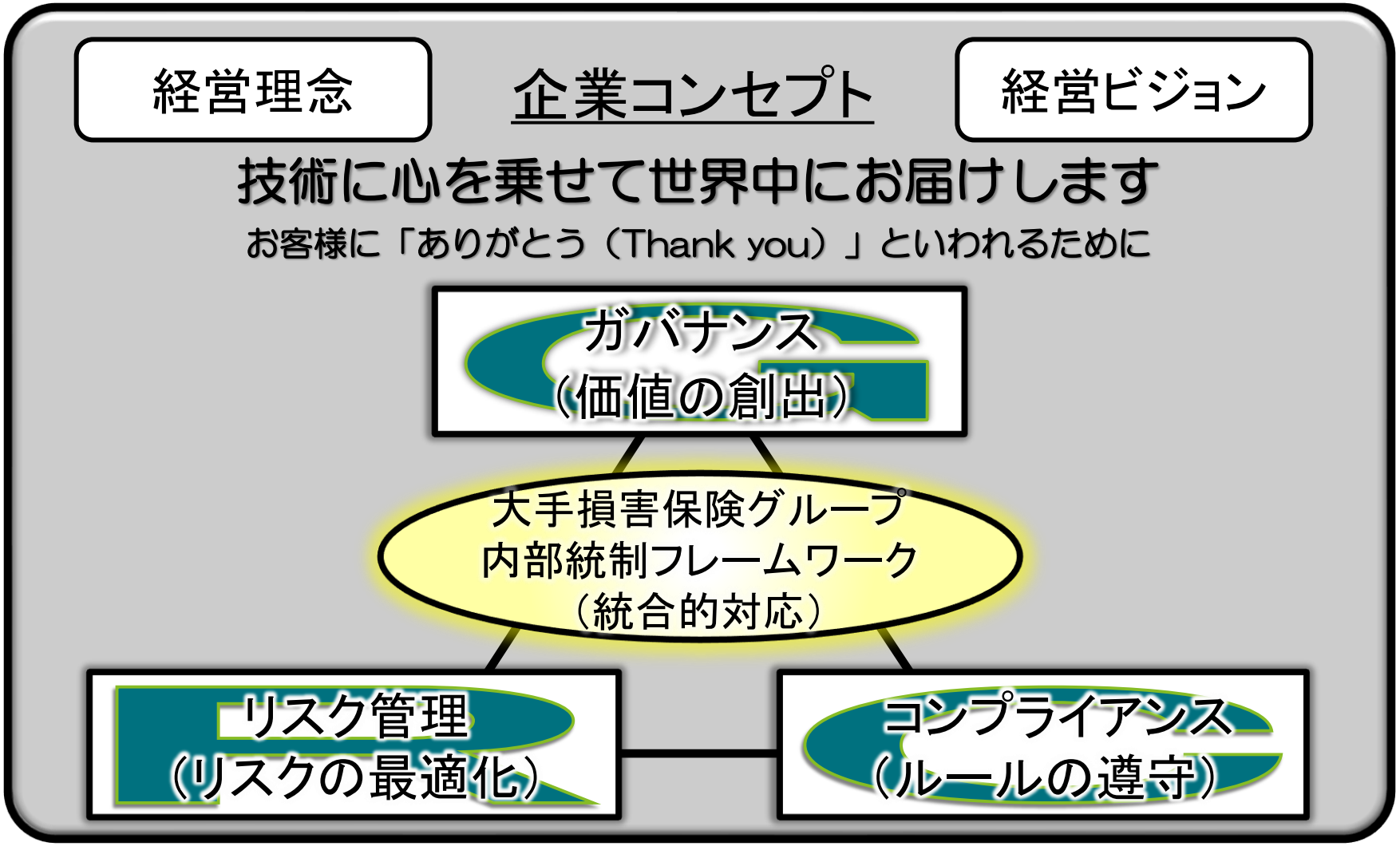
情報セキュリティルールを最適化すると共にシンプルにすべき

↓

価値創出を目指した攻めの情報セキュリティへ

このITサービス会社では、価値を創出するガバナンス、リスクを最適化するリスク管理、ルールを遵守するコンプライアンスの3つをバランスを取る態勢を整備しました

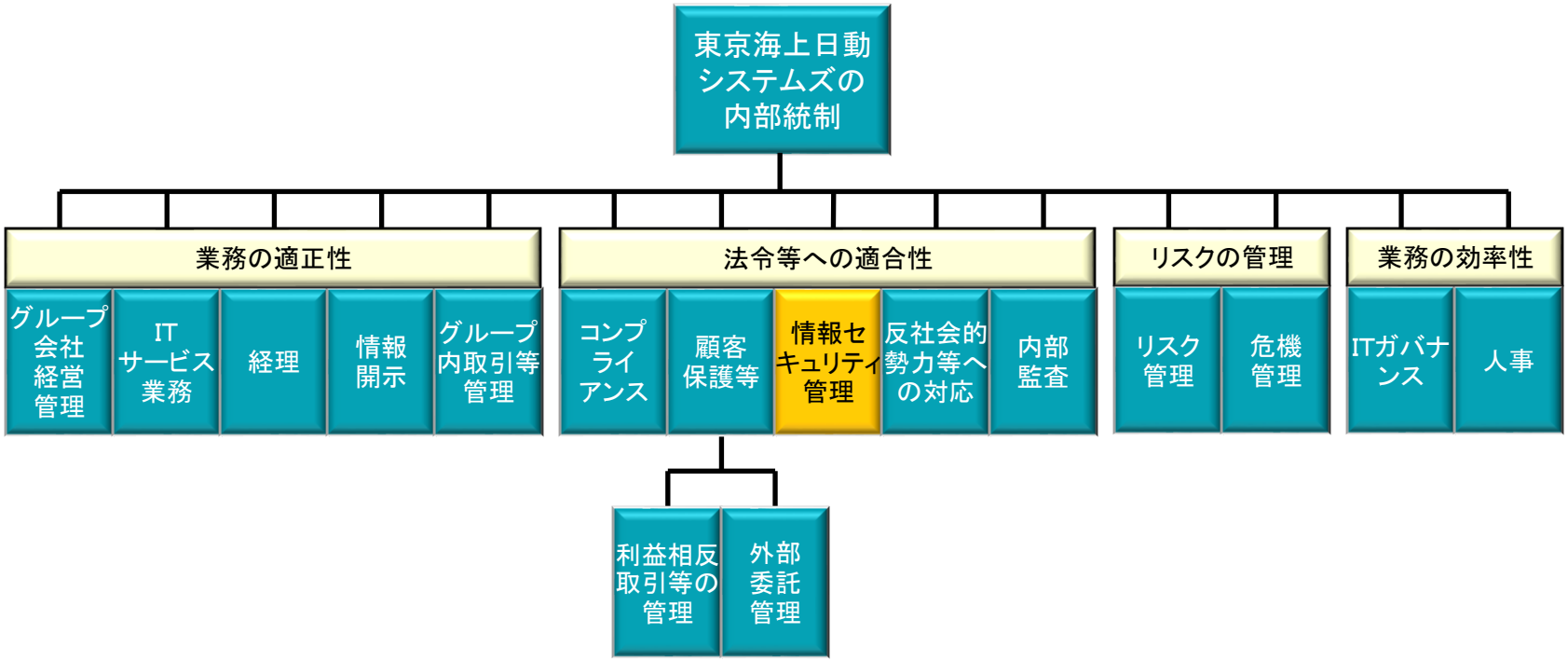
ITサービス会社のGRCの概念



このガバナンス態勢（GRC）の中核となるのは各種の内部統制管理から構成される内部統制フレームワークであり、中でも「情報セキュリティ」が中心的な位置づけです

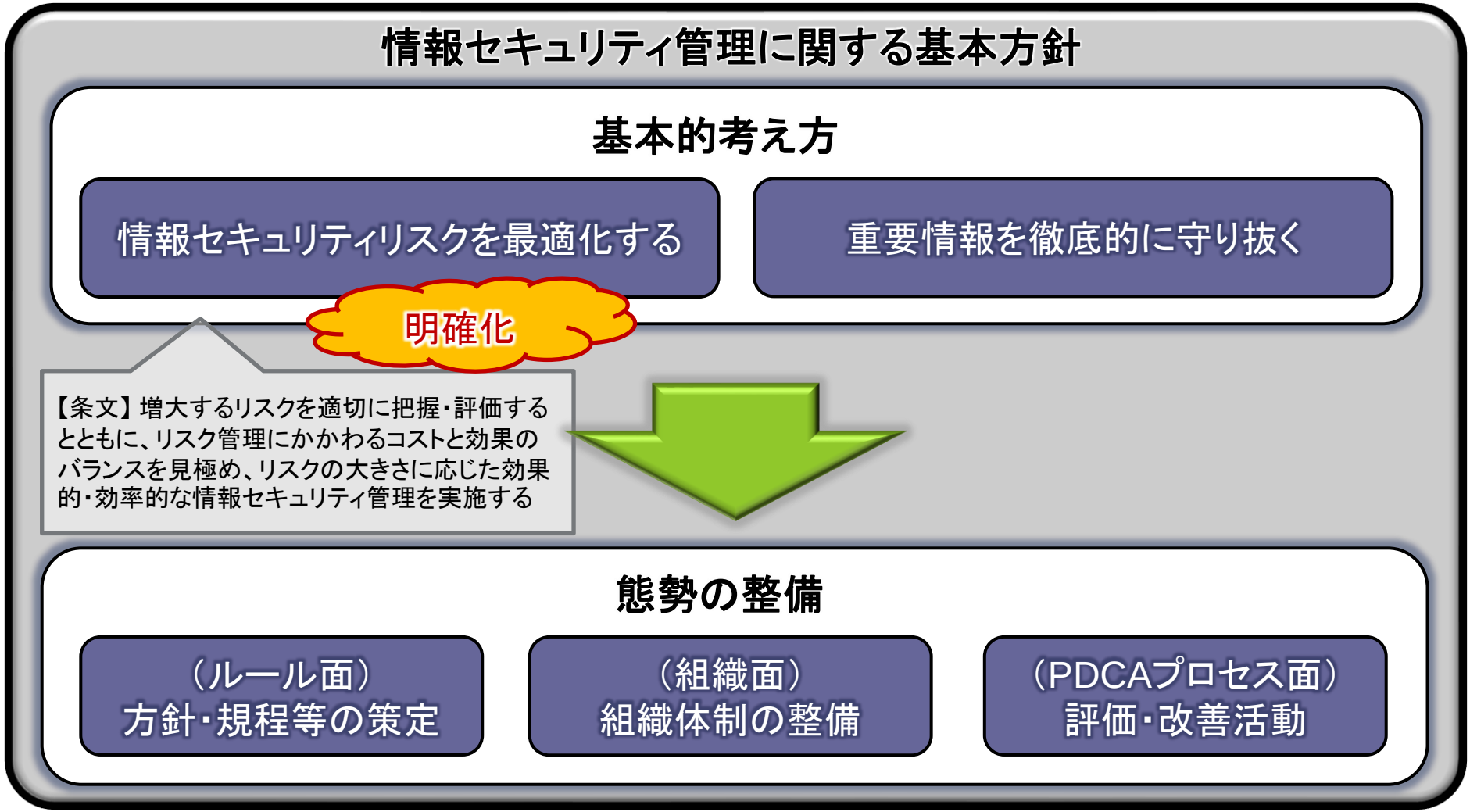
ITサービス会社の内部統制

- GRC態勢により以下の16の内部統制領域をガバナンス
- 「情報セキュリティ管理」はその中心的な領域に位置づけられる



情報セキュリティの基本的な考え方として、戦略実現のためリスクを積極的に取って新しいことにチャレンジしていくような、「攻め」の情報セキュリティを明確にしています

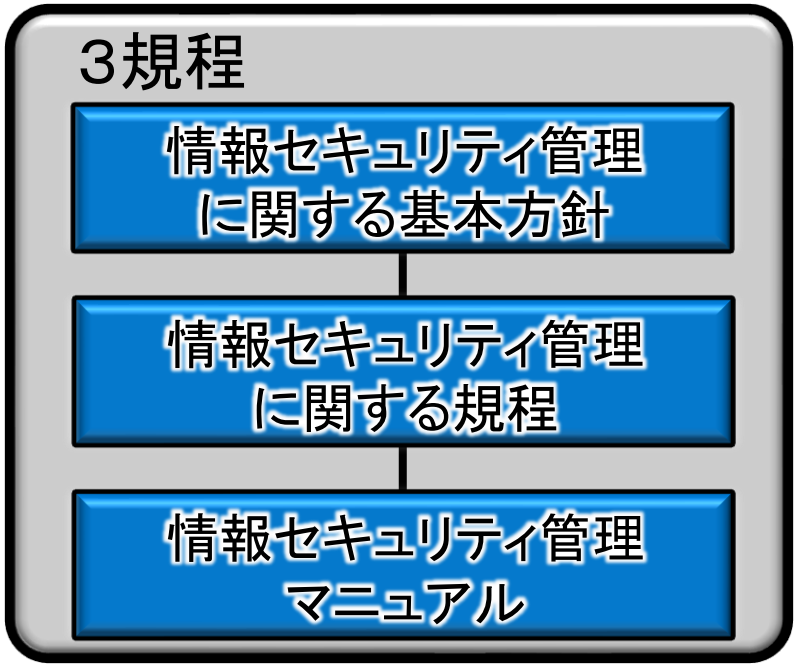
ITサービス会社の情報セキュリティ管理に関する基本方針

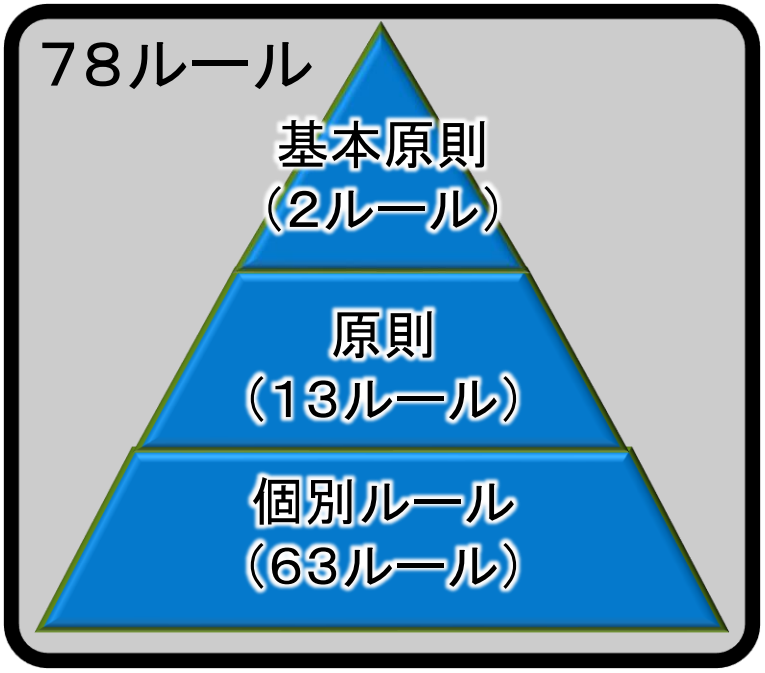


情報セキュリティのルールについて、新しいリスクにしっかり対応し、職員が自ら考え実行できるように過剰なルールをとことん廃止しプリンシプルベースで統廃合しました

情報セキュリティルールの最適化、シンプル化

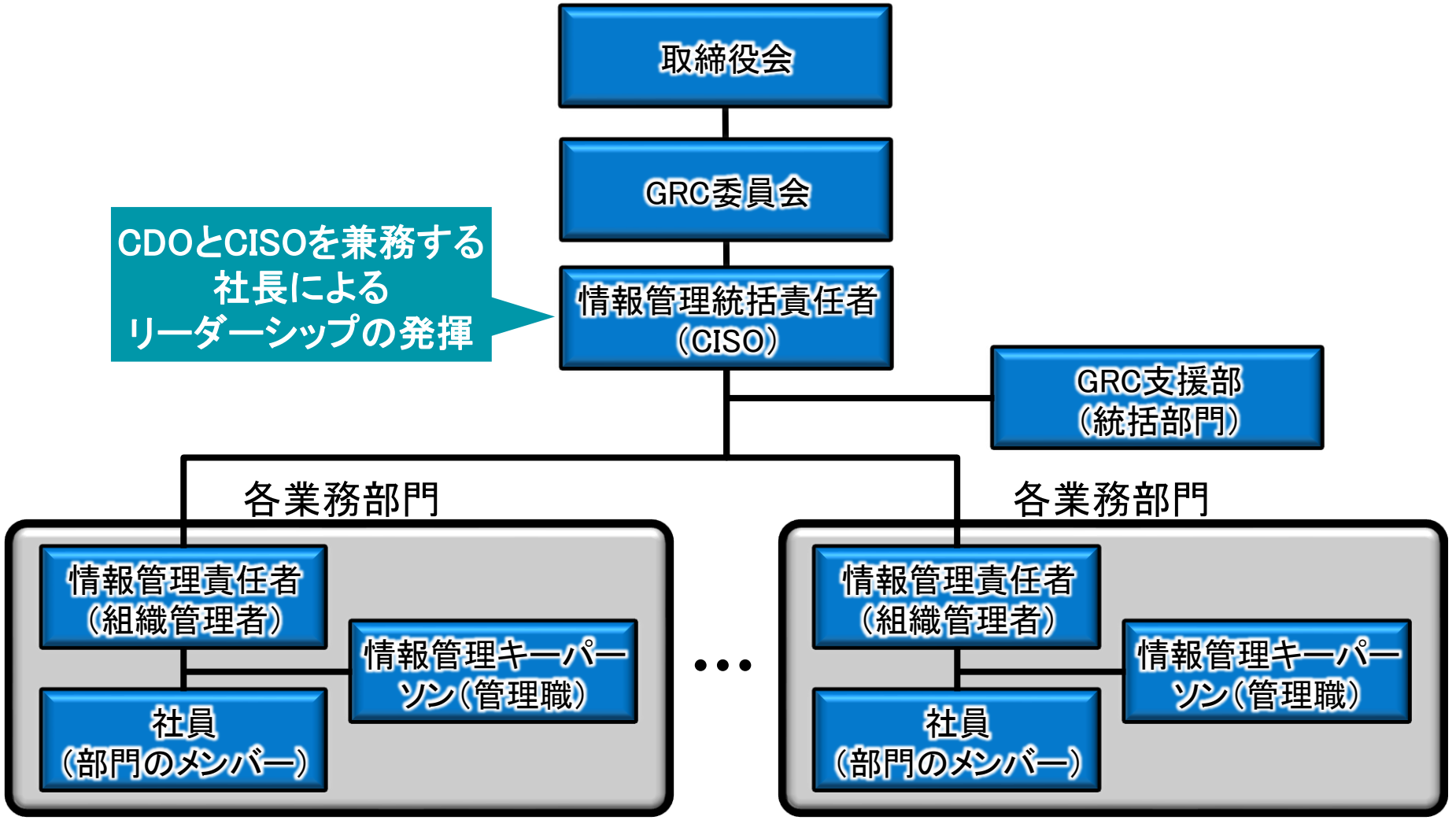
- 徹底的なルールの見直し
  - ✓【最適化】サイバーセキュリティをはじめとする重要リスク、新しいリスクにしっかり向き合い、過剰な統制ルールをとことん軽減・廃止する
  - ✓【シンプル化】プリンシプルベースでルールを統廃合する
- 結果：（改革前）15規程318ルール ➡ （改革後）3規程78ルール





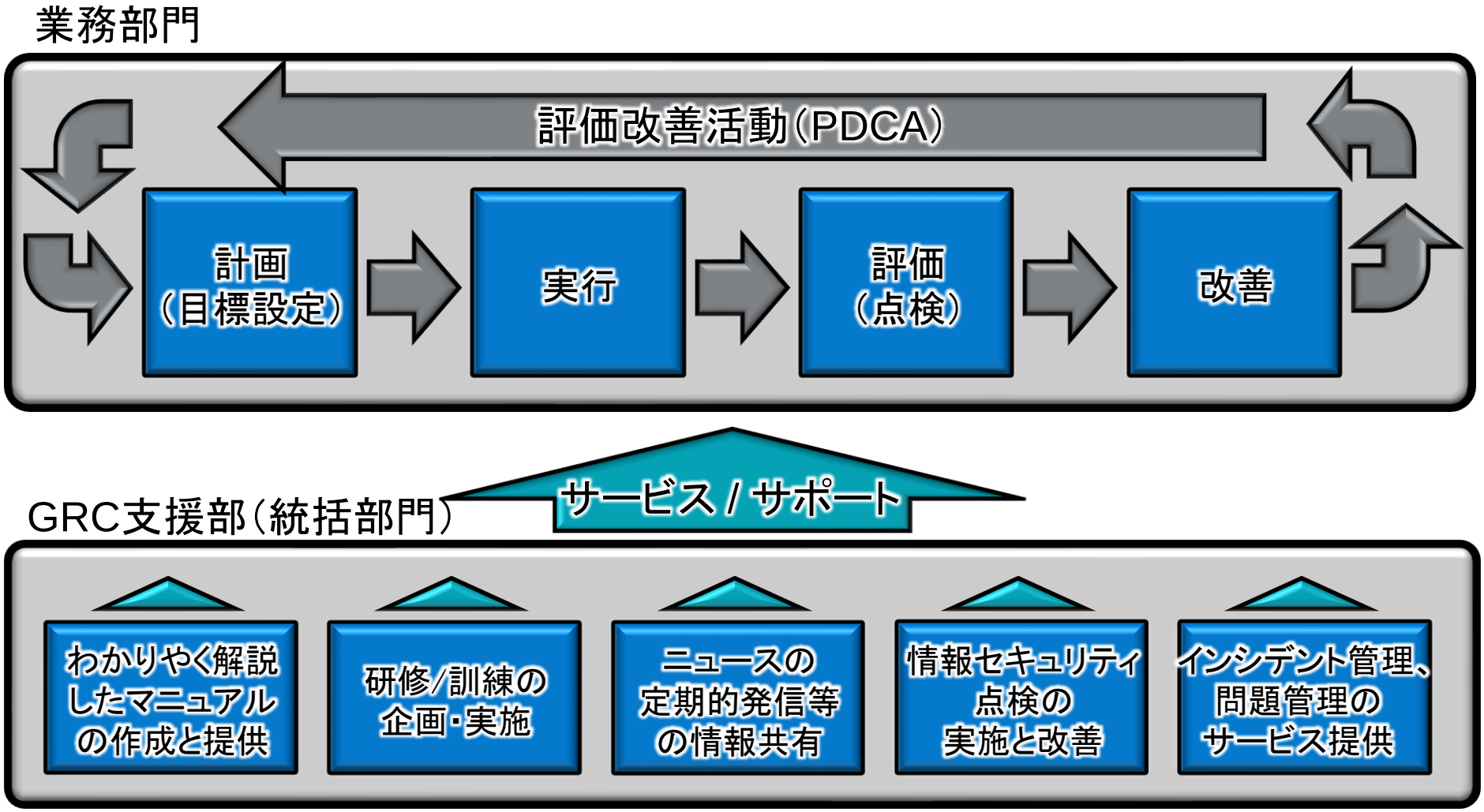
取締役会等のガバナンスの下、CDOとCISOを兼務する社長が自らリーダーシップを発揮し、職員が自ら考え行動するような、情報セキュリティ管理体制を整備しました

情報セキュリティ管理体制



業務部門の職員が主体的に計画、実行、評価、改善のPDCAサイクルによる評価・改善活動を行い、情報セキュリティ統轄部門による手厚いサポートを行いました

情報セキュリティ管理 評価・改善活動



情報セキュリティ改革を断行し、以後、重要情報をしっかり守りながら、攻めの情報セキュリティにより、社員がいきいきとスピード感を持ってお客様価値を提供しています

まとめ

ITサービス会社の情報セキュリティ改革

- ✓ 価値創出を目指したGRC態勢における中心的な内部統制領域として対応
- ✓ 守りから攻めの情報セキュリティへ改革
  - 時にはリスクを取ってでもチャレンジするリスクの最適化を実現
- ✓ 情報セキュリティ管理態勢の構築
  - 新しいリスクへ対応し、シンプルでわかりやすいルール体系へ
  - CISO、情報管理責任者による情報セキュリティ管理体制を構築
  - 業務部門による主体的PDCA実行、統括部門の包括的サポート

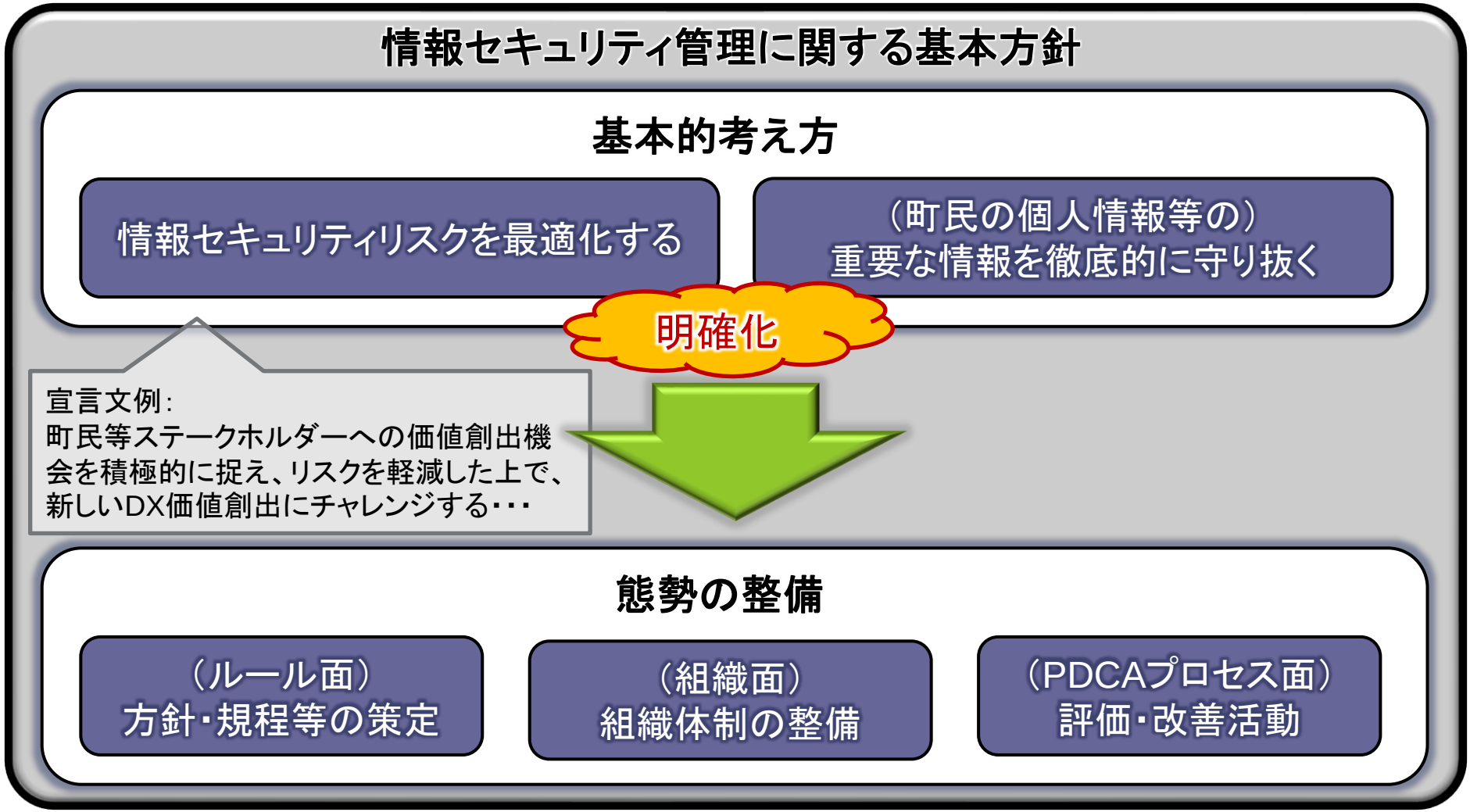
ITサービス会社の現在（改革の成果）

- ✓ 重要情報をしっかり守りながら、攻めの情報セキュリティにより、社員がいきいきとスピード感を持って、お客様価値を提供している。

Ⅳ. 磐梯町のDXを支える情報セキュリティ管理に向けて

新しいDX機会を積極的に捉え、リスクを軽減した上で価値創出にチャレンジするため、ルール、組織、プロセスによる態勢整備方針を明確化してはいかがでしょうか

磐梯町の情報セキュリティに関する基本方針案（たたき台）

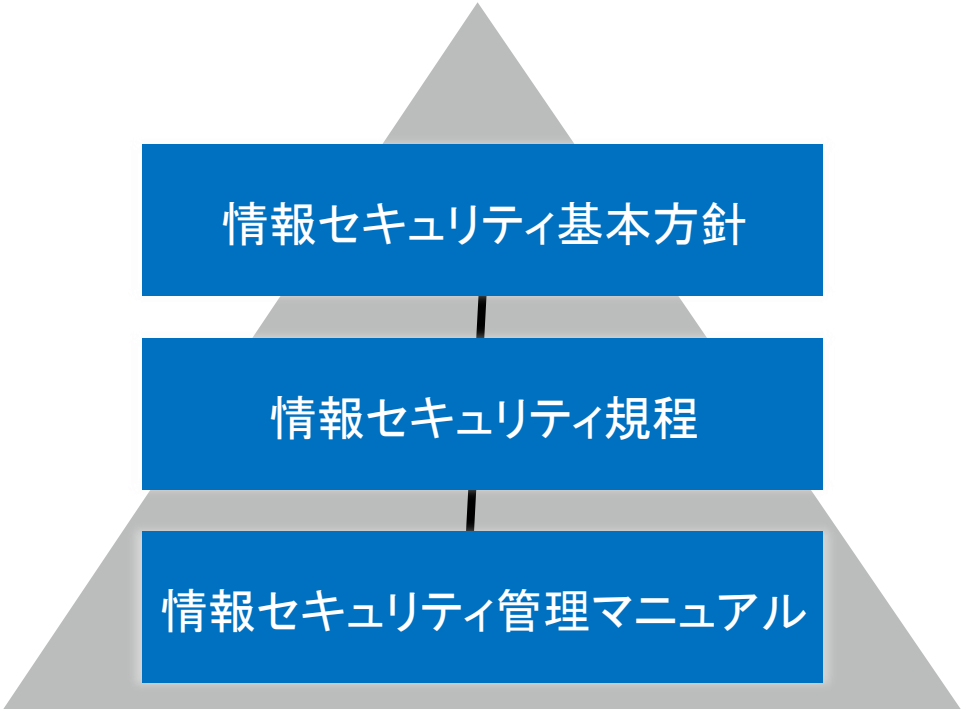


その際、既存の情報セキュリティに関するルールを徹底的に見直し、方針・規程・マニュアル3階層で整理統合して、実務に即したものにしていくべきです

情報セキュリティルールの構造化、最新化の必要性

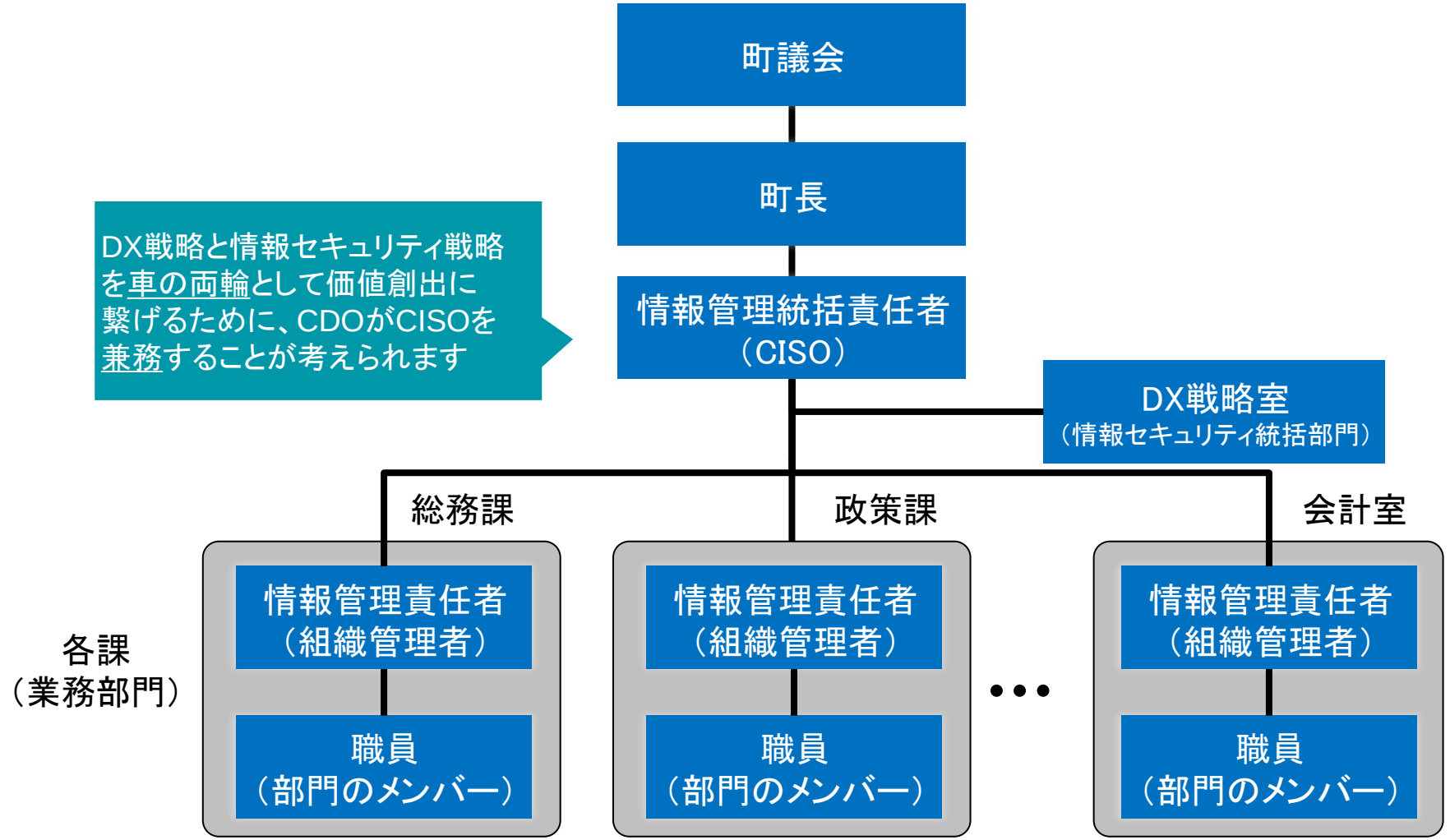
■ ルールの策定・見直し

- ✓ 【構造化】方針・規程・マニュアルの3階層のルール体系を整備する
- ✓ 【方針の策定】価値創出のためのリスク最適化を明文化する
- ✓ 【ルールの最新化】環境の変化に対応して、不要になったルールを削除し、新しいリスク、大きいリスクへの対応ルールを追加する



CISOのリーダーシップの下、職員が自律的に情報セキュリティに取り組むような管理体制を整備し、戦略推進に向けCISOは現行のCDOが兼務することが考えられます

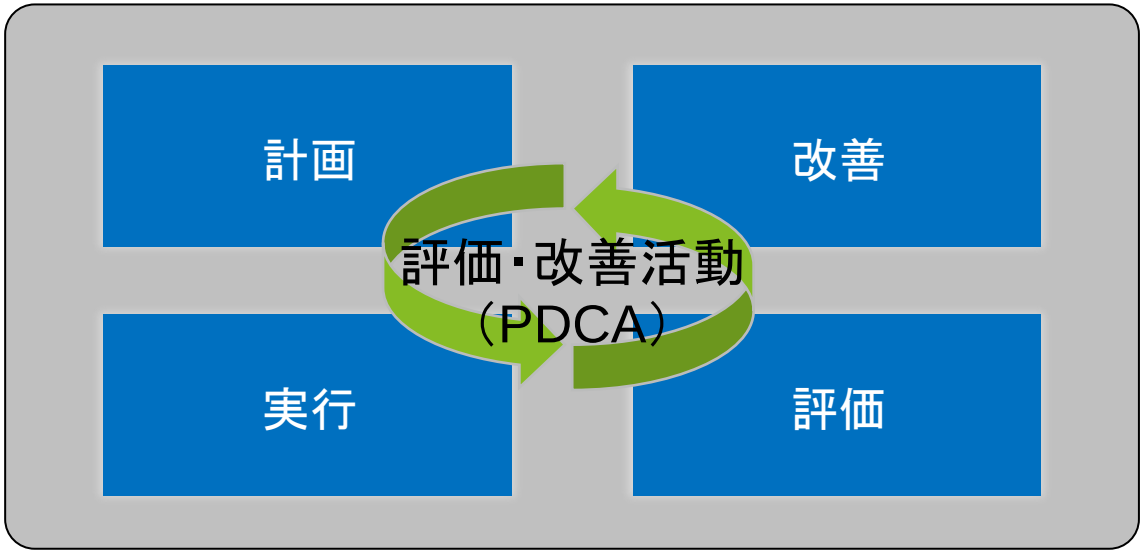
情報セキュリティ管理体制（たたき台）



DX戦略を実行するための攻めの情報セキュリティ管理を目指し、情報セキュリティ管理態勢整備を計画・実行し、評価・改善（PDCA）活動を行います

情報セキュリティ管理　評価・改善活動（ISMSの構築・導入）

各課/係
（業務部門）

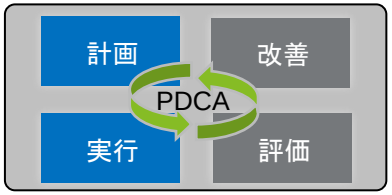


DX戦略室
（情報セキュリティ統括部門）

支援

- 基本方針の作成 ルールの見直し・最新化
- 研修/訓練の企画・実施
- ニュースの定期的発信等の情報共有
- 情報セキュリティ点検（ISMS対応）
- インシデント管理、問題管理の支援

このような情報セキュリティに関するPDCAサイクルの遂行については、まず、情報セキュリティマネジメントシステム（ISMS）を構築・導入することから始めます

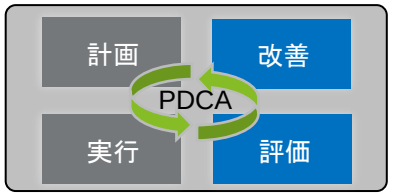


ISMSの構築・導入のステップ（計画と実行）

ISMSの体制の確立	• ISMSの構築・導入のため、ISMS管理責任者とISMS推進チーム、および、ISMS内部監査責任者とISMS内部監査チームの設置・任命
ISMS適用範囲の定義	• ISMSにおける管理の対象を明確にするため、適切なインプットに基づき、ISMSの適用範囲とその境界線の明文化
情報セキュリティ方針の確立	• 情報セキュリティに関する基本的な取組みや原則を内外に表明するため、ISMSにおける基本方針の策定
情報セキュリティリスクアセスメントの実施	• 自社の特性に応じたISMSを確立するため、保有している情報資産の特定、脅威・脆弱性・影響の特定、リスクの分析・評価
ISMS文書の作成	• ISMSの各マネジメントプロセスの管理の手法の明文化
ISMSの導入教育	• 確立した手順を実際の業務に適用できるようにするために、各担当者やチーム、部門への教育

出所：ISO/IEC27001:2013を基に講師が作成

続いて、構築・導入したISMSについて、内部監査を実施してマネジメントレビューのインプットとするなど、評価・改善活動を行います



内部監査の実施（評価と改善）

監査の計画	• 年度監査計画の策定 • 監査員の割り当て
監査の準備 （チェックリスト）	• 個別スケジュール表の作成 • 内部監査チェックリストの作成（ISO/IEC 27001を参照）
監査の実施	• 文書・記録の確認 / 活動の観察 • 面談（インタビュー）の実施
監査の報告 （監査報告書の作成）	• 監査結果の報告（目的、範囲、チーム、監査活動、監査所見と証拠、監査結論、監査基準、等） • マネジメントレビューへの情報提供
監査のフォローアップの実施	• 不適合が発見された場合、被監査部門による是正措置の実施 • 監査部門による是正措置、再発防止策の有効性評価等フォローアップ

出所：ISO/IEC27001:2013を基に講師が作成

内部監査部門による点検については、ISO/IEC 27001に基づくチェックリストを活用することにより、ISMS認証取得に繋げることが一般的です

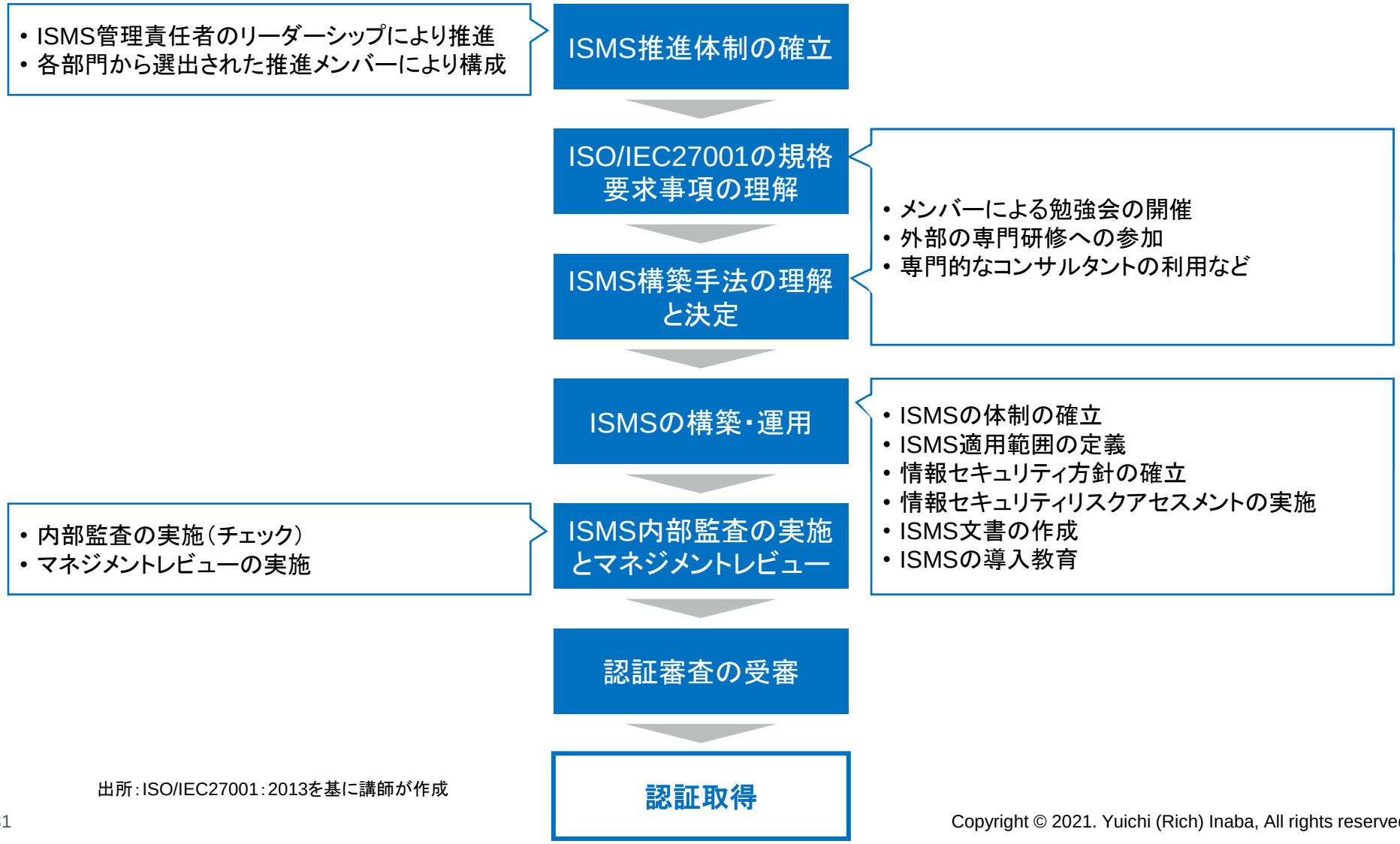
ISMS認証取得に向けたチェックリストの例

規格項目		チェック内容	確認する文書・記録	デジタル変革戦略室	総務課	政策課	町民課	商工管理課	農林課	建設課	会計室	コメント	評価結果	備考
4 組織の状況	4.1 組織及びその状況の理解	外部及び内部の課題を決定し、明確化して いるか	「リスク一覧表」「事業計画書」等	●										
	4.2 利害関係者のニーズ及び期待の理解	以下の寧項を決定し、明確化しているか 1) ISMSに関連する利害関係者 2) 利害関係者の情報セキュリティに関連 する要求事項	「リスク一覧表」「顧客との契約書」等	●										
	4.3 情報セキュリティマネジメントシステム（ISMS）の適用範囲の決定	以下の事項を考慮して適用範囲を決めてい るか 1) 4.1に規定する外部及び内部の課題 2) 4.2に規定する要求事項 3) 組織が実施する活動と他の組織が実施する活動との間のインターフェース及び依存関係	「リスク一覧表」顧客との契約書」等	●										
	4.4 情報セキュリティ マネジメントシステム	ISO27001:2013 (JISQ27001:2014)の要求事 項に従って、情報セキュリティマネジメントシ ステム(ISMS)を確立し、実施し、維持し、か つ継続的に改善を行う仕組みになっているか	「リスク一覧表」顧客との契約書」等	●										
5 リーダーシップ	5.1 リーダーシップ及びコミットメント	経営層は以下の事項を実施しているか 1) 情報セキュリティ方針及び情報セキュリティ目標を確立し、それらが組織の戦略的な方向性と両立することを確実にする。 2) 組織の事業プロセスへの情報セキュリ ティマネジメントシステム(ISMS)要求事項へ の統合を確実にする。 3) 情報セキュリティマネジメントシステム (ISMS)に必要な経営資源が利用可能であることを確実にする。 4) 有効な錆報セキュリティマネジメント及び 情報セキュリティマネジメントシステム (ISMS)要求事項への適合の重要性を周知する。 5) 情報セキュリティマネジメントシステム (ISMS)がその意図した成果を達成することを確実にする。 6) 情報セキュリティマネジメントシステム (ISMS)の有効性に寄与するよう社員を指揮し、支援する。 7) 継続的な改善を推進する。 8) その他の關連する管理層がその責任の領域においてリーダーシップを実証するよう、その管理層の役割を支援する。	「ISMSマニュアル」「マネジメントレビュー議事録」	●										

出所：ISO/IEC27001：2013を基に講師が作成

情報セキュリティに関する内部管理機能の強化や、町民等ステークホルダーへの安全・安心を提供するために、ISO/IEC27001認証の取得を目指すことが考えられます

ISMS認証取得のステップ



出所：ISO/IEC27001：2013を基に講師が作成

さあ、磐梯町のITガバナンス態勢を整備しISMS認証を取得して、新生デジタル庁と歩調を合わせ、磐梯町のデジタル社会形成価値を創出しましょう

デジタル社会形成価値の創出

磐梯町のステークホルダーへのデジタル社会形成価値創出

企業、他自治体 / 役場職員 / 町民・住民 / 地域社会 / 地球環境

目標

①デジタル化はまちの将来を救う
②デジタル共生社会の実現
③先行者利益の確保

行動指針

職員行動指針の明確化

町のミッション（使命）
町民全員を幸せにする
～共生社会の実現～
町のビジョン（将来像）
自分たちの子や孫たちが暮らし続けたい魅力あるまちづくり
～共創・協働のまちづくり～
町のバリュー（行動規範）
町民起点（価値観の共有）

※町民『起点』とは、『町民『視点』』と意味が違います。『視点』は町民とは別のサイドに立って考えるという意味ですが、『起点』というのははっきりと町民のサイドに立つことです。

戦略

今までのやり方　様々な地域課題

仕事 / 教育 / 住宅 / 医療 / 環境 / 防災

地域課題を行政主導で解決

これからは　住民それぞれの課題

住民 / 住民 / 住民 / 住民 / 住民 / 住民

課題を住民と協働で解決

ISMS認証取得済みの「守りと攻めの情報セキュリティ管理態勢」

End of Document