業種別の全社的リスクとIT ガバナンス体系

環境と経済の両立に向けて

ERM by industry and so IT Governance

リスクとガバナンスセミナー

AStar総合研究所

猿　田　　礎

序論

１．　金融業中心のリスク管理から

製造業のリスク管理へ

1．1　IOTシステムと情報漏えい

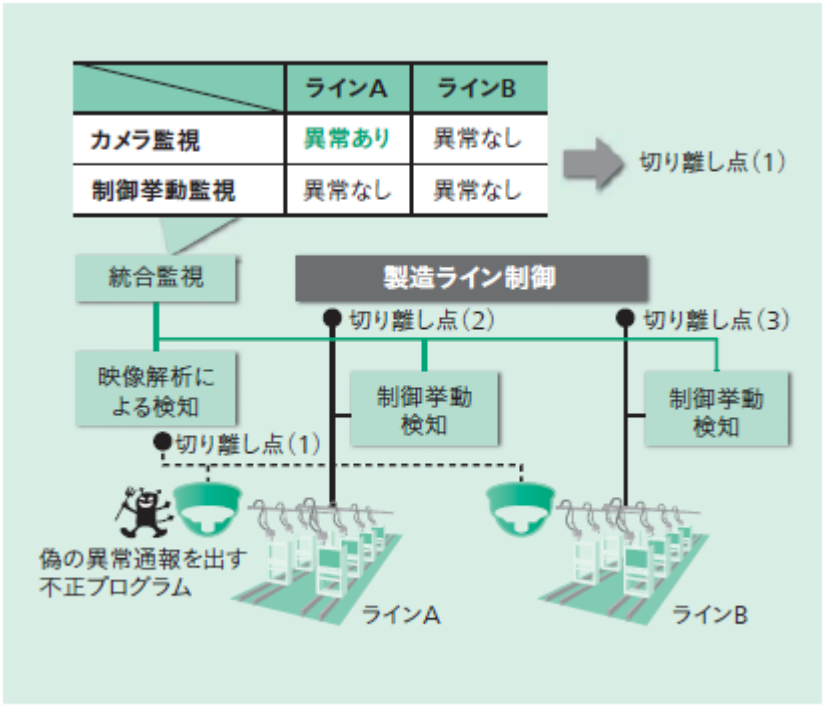


図3｜製造ラインにおける問題検知時の挙動

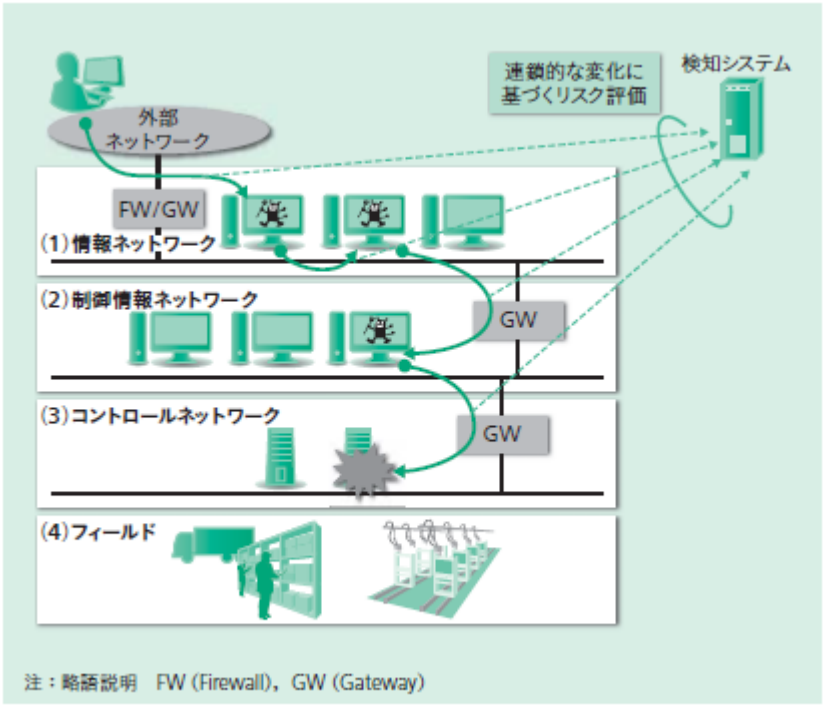


図4｜IoTバリューチェーン構成

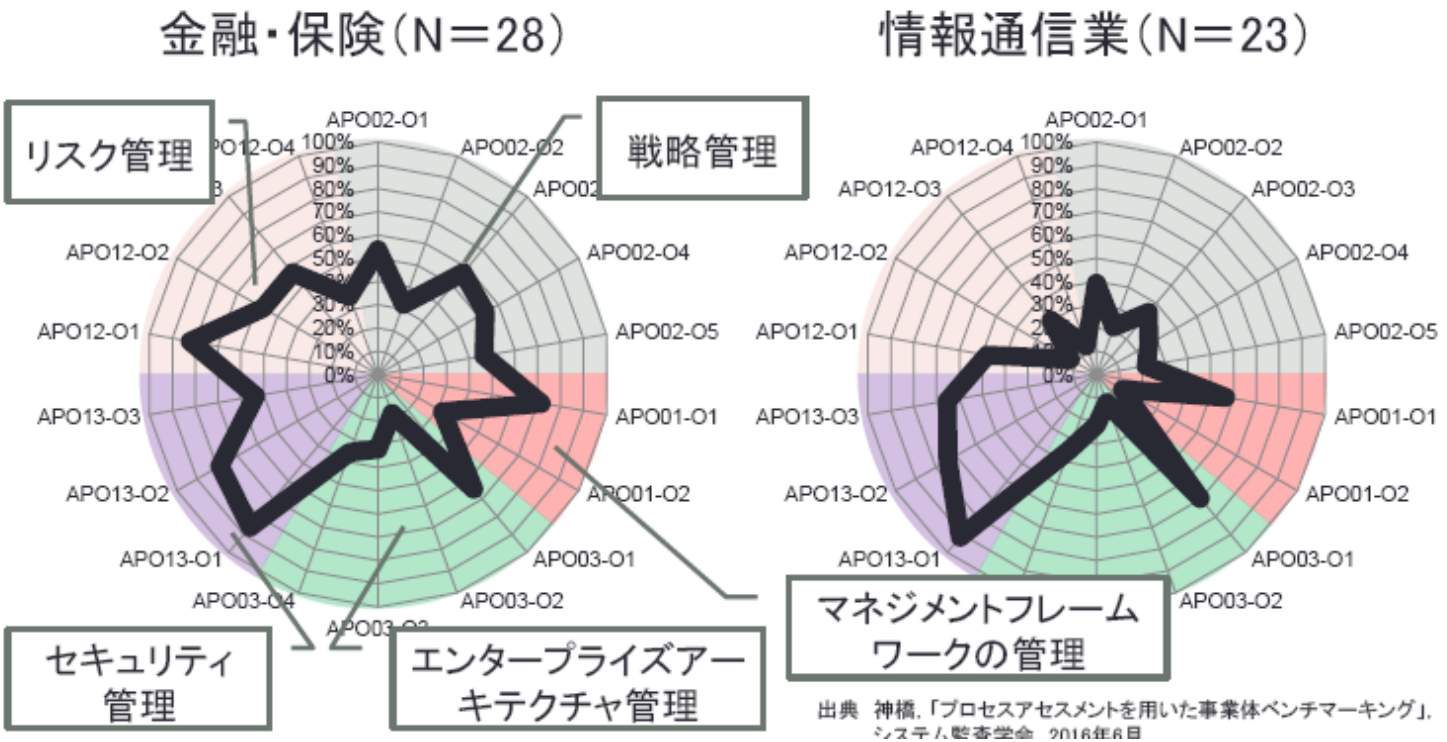
出典：田中　普輔等,日立評論「IOTシステムとセキュリティ課題と解決アプローチ」

１．２　サイバーセキュリティ基本法

サイバーセキュリティ基本法
情報の漏えい、滅失又は毀損の防止
情報の安全管理のために必要な措置
情報システム、情報通信ネットワークの安全性、信頼性確保のために必要な措置
に関わる法律

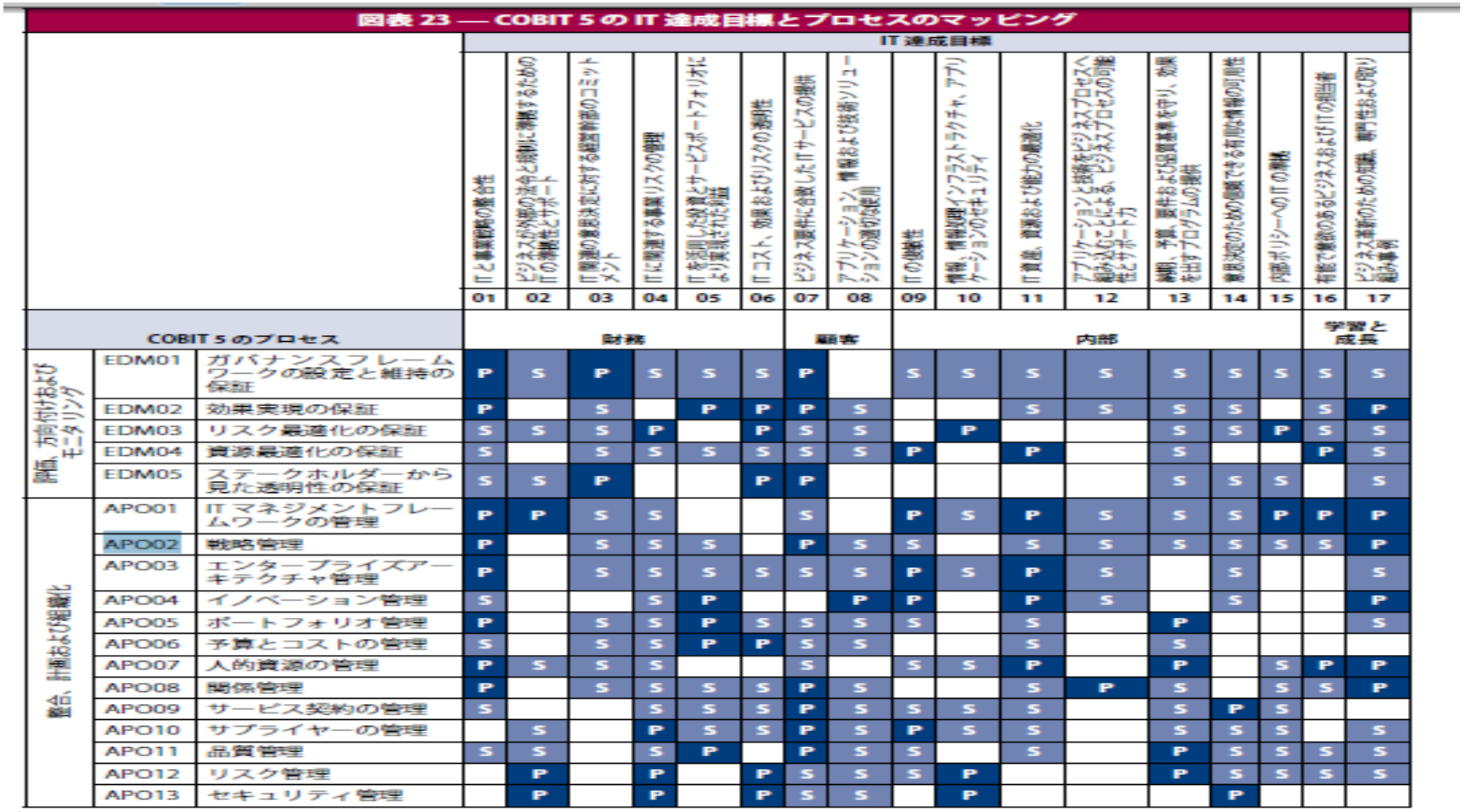
出典：サイバーセキュリティ基本法などを参考に編集

1．3　業種別に関する知見



出典：神橋　基博,システム監査学会30回研究大会 「プロセスアセスメントを用いた事業体ベンチマーキング」

1.3-1　グラフの解説



図表 23 — COBIT 5 の IT 達成目標とプロセスのマッピング

			IT達成目標																
			IT と事業戦略の整合性	ビジネスが法律の遵守と規則に準拠するためのITの準備性とサポート	IT関連の意思決定に対する経営幹部のコミットメント	IT に関連する事業リスクの管理	IT を活用した投資とサービスポートフォリオにより実現された価値	IT コスト、効果およびリスクの透明性	ビジネス要件に合致したITサービスの提供	アプリケーション、情報およびテクノロジーソリューションの適切な使用	IT の俊敏性	情報、情報処理インフラストラクチャ、アプリケーションのセキュリティ	IT資産、資源および能力の最適化	アプリケーションと技術をビジネスプロセスへ組み込むことによる、ビジネスプロセスの可能性とサポート力	納期、予算、要件および品質基準を守り、効果を出すプログラムの選択	意思決定のための信頼できる有用な情報の可用性	内部ポリシーへのITの準拠	有能で動機のあるビジネスおよびITの担当者	ビジネス革新のための知識、専門性および前向きな考え
			01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17
COBIT 5 のプロセス			財務						顧客		内部							学習と成長	
調整、方向付けおよびモニタリング	EDM01	ガバナンスフレームワークの設定と維持の保証	P	S	P	S	S	S	P		S	S	S	S	S	S	S	S	S
	EDM02	効果実現の保証	P		S		P	P	P	S			S	S	S	S		S	P
	EDM03	リスク最適化の保証	S	S	S	P		P	S	S		P			S	S	P	S	S
	EDM04	資源最適化の保証	S		S	S	S	S	S	S	P		P		S			P	S
	EDM05	ステークホルダーから見た透明性の保証	S	S	P			P	P						S	S	S		S
整合、計画および組織化	APO01	IT マネジメントフレームワークの管理	P	P	S	S			S		P	S	P	S	S	S	P	P	P
	APO02	戦略管理	P		S	S	S		P	S	S		S	S	S	S	S	S	P
	APO03	エンタープライズアーキテクチャ管理	P		S	S	S	S	S	S	P	S	P	S		S			S
	APO04	イノベーション管理	S			S	P			P	P		P	S		S			P
	APO05	ポートフォリオ管理	P		S	S	P	S	S	S	S		S		P				S
	APO06	予算とコストの管理	S		S	S	P	P	S	S			S		S				
	APO07	人的資源の管理	P	S	S	S			S		S	S	P		P		S	P	P
	APO08	関係管理	P		S	S	S	S	P	S			S	P	S		S	S	P
	APO09	サービス契約の管理	S			S	S	S	P	S	S	S	S		S	P	S		
	APO10	サプライヤーの管理		S		P	S	S	P	S	P	S	S		S	S	S		S
	APO11	品質管理	S	S		S	P		P	S	S		S		P	S	S	S	S
	APO12	リスク管理		P		P		P	S	S	S	P			P	S	S	S	S
	APO13	セキュリティ管理		P		P		P	S	S		P				P			

出典：ISACA　COBIT5

要修正

1.4 COSO ERM 2017

COSO ERM Integrating with Strategy & Performanceが発刊された。（2017/June）

主な特徴

1. 戦略とパフォーマンスの統合を実行
2. 戦略策定プロセスとパフォーマンス実行時でリスクを考慮した事業活動
3. 選好と許容などのリスク価値の考え方に重点
4. 目標設定時、戦略策定時、パフォーマンス実行時のリスクを考慮
5. 戦略策定時、実行時のリスクテイクの実践
6. 5つ構成要素と洗練された20の原則の提示
7. 最終版として発表

出典：COSO ERM Integrating with Strategy & Performance 2017/June

２　本論

２．１　全社的リスク管理（COSO　ERM）

２．１．１　　COSO　VS　COSO　ERM

COSOはアカウント指向

COSO　ERMはマネジメント指向である

２．１．２　日本企業のITガバナンス策

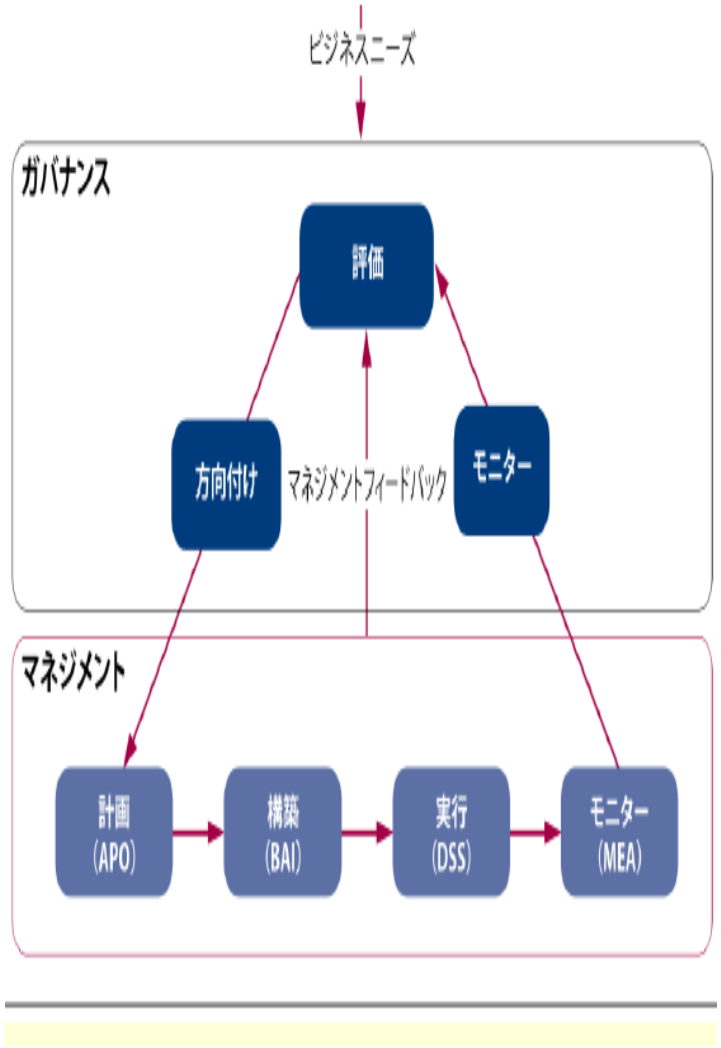
カシオ計算機	情報システム部員の役割を見直し、業務改革とそのためのシステムを提案できるようにした。
コスモ石油	業務部門と情報システム部門が相互に協調する体制を整えた。
凸版印刷	事業部門ごとにシステムを開発する体制から本社主導で開発する体制に変更した。
日産自動車	新規案件の企画・管理と機能拡張案件の開発は自社内で行う体制を整え、運用管理などはアウトソーシングした。
三菱電機	情報システム部員のコンサルティング能力養成のため「ＩＴ企画標準ガイドライン」を作成し、部員を教育。本社主導で全体最適の情報システム化。

(『日経コンピュータ　2001年10月８日号』p.51 (日経ＢＰ社)より抜粋のうえ要約)

出典：石島　隆,大阪成蹊大学　研究紀要　第1巻第1号 「ITガバナンスとIT統制」

２．１．３　価値ガバナンスとITガバナンス

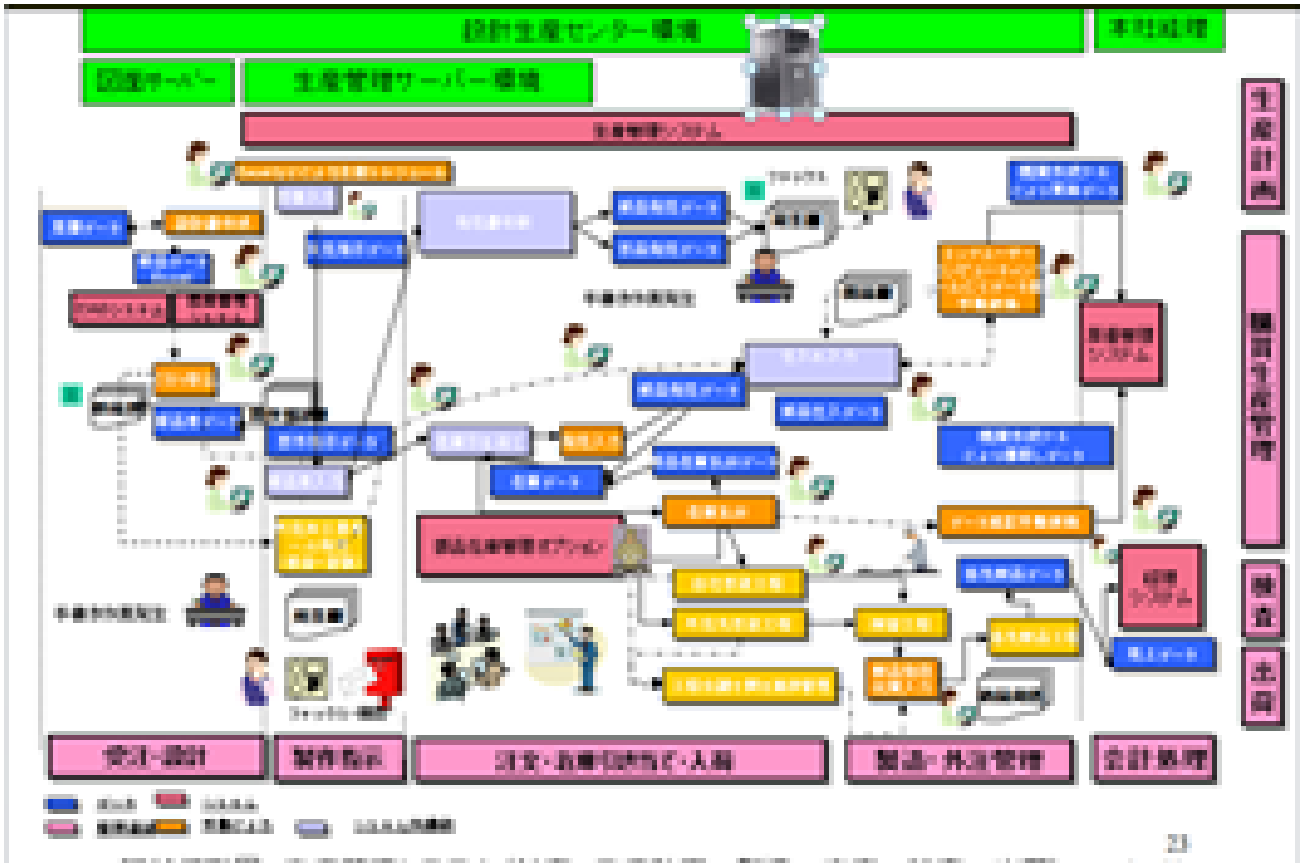
Val-ITActivity		COBIT 5.0 Practice	
VG1.4	企業にとっての価値を定義する。	EDM02.02	価値最適化体制の評価方向付け
VG3.1	ポートフォリオの種類を定義する。	EDM02.02	価値最適化体制の評価方向付け
VG3.2	分類(ポートフォリオ内)を定義する。		
VG3.3	個々の分類ごとに評価基準を策定し、伝達する。		
VG3.4	基準を重み付けする。		
VG3.5	個々の分類ごとに節目でのレビューとその他のレビューに関する要件を定義する。		
VG5.1	主要な測定指標を特定する。	EDM02.03	価値最適化体制のモニタリング
VG5.2	情報収集のプロセスとアプローチを定義する。		
VG5.3	報告の方法と技法を定義する。		
VG5.4	成果改善策を明確化し、監視する。		
VG6.1	得られた教訓を取り入れる。		



出典：ISACA　VALーIT　ISACA　COBOT5.0

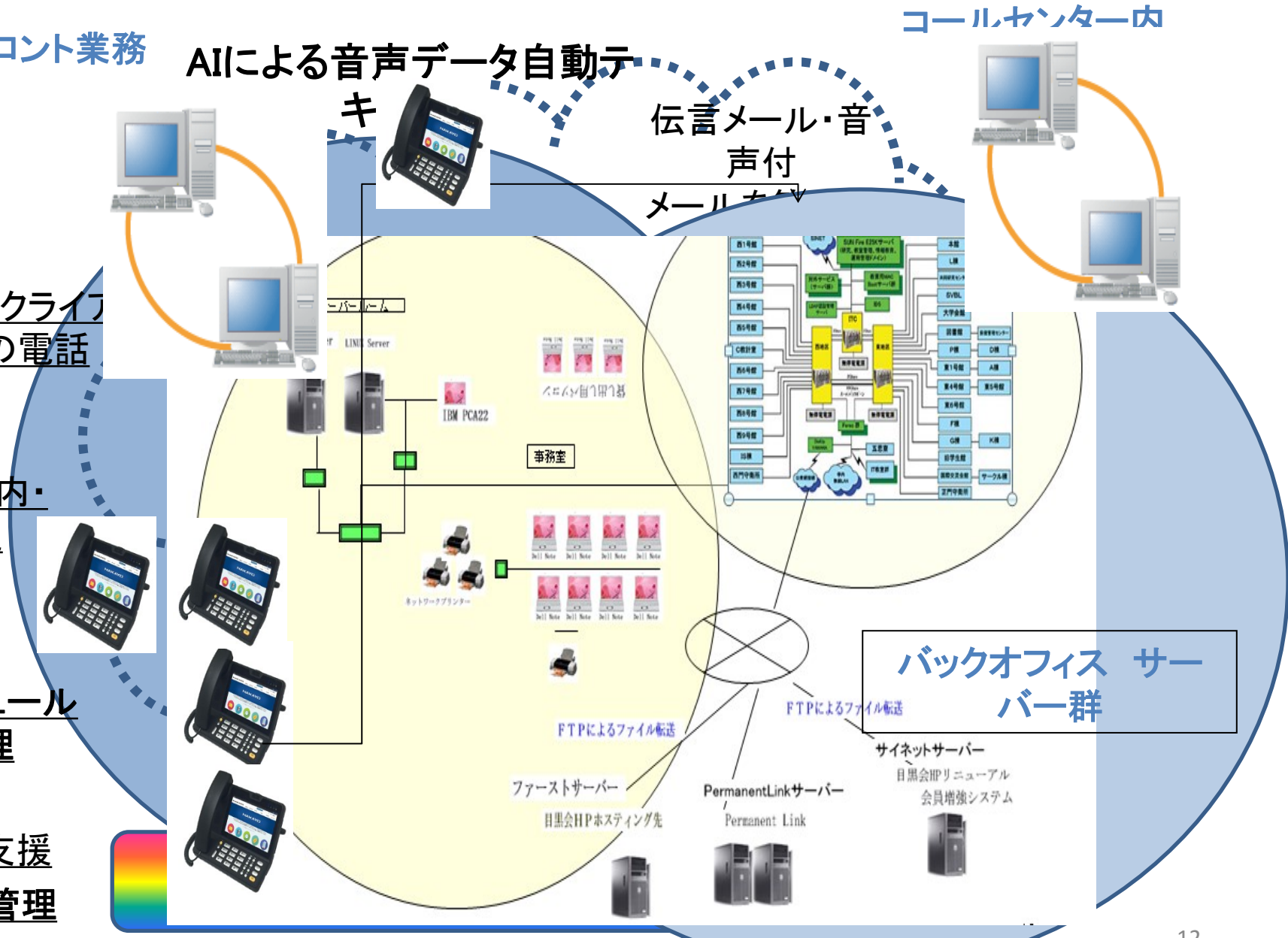
２．２　実例分析

２．２．１　監査例１　製造業



出典：株式会社AStarコンサルティング事業部コンサルティング部

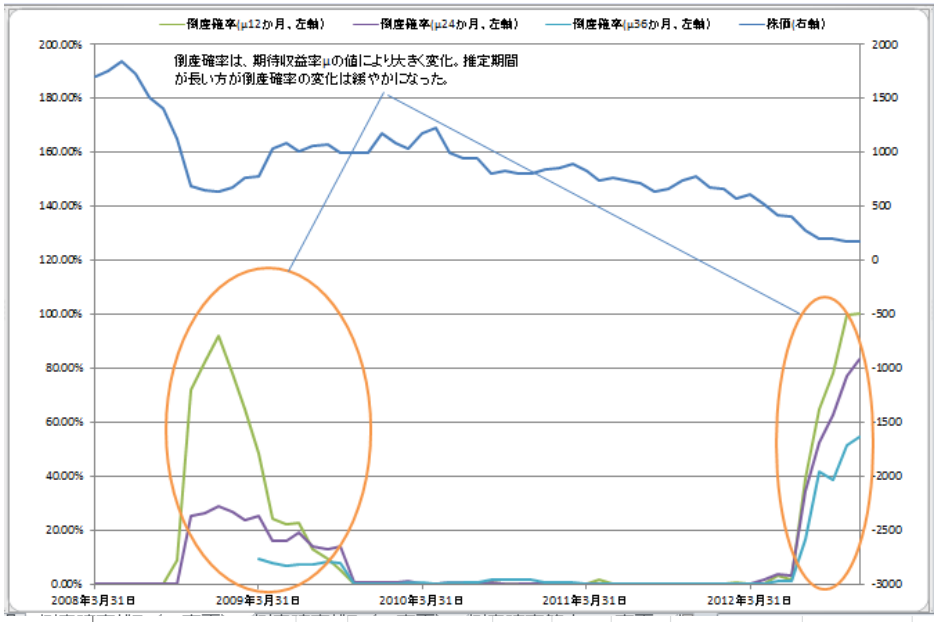
２．２．２　監査例2　通信業



出典：AStar総合研究所　基礎技術部

2．2．3　監査例3　電子メーカ

項目	内容
1. 前提の確認	ヴィジョン～行動指針確認
	自社の能力（技術・開発・調達・生産・販売）分析
	業績の推移（SBU毎の推移）
	戦略一般方向（コア・コンピタンス）確認
	経営計画の確認（短期・中期・長期）
	現状の組織構造確認（組織分掌等の確認）
2. 環境分析	外部環境のマクロ・ミクロ分析
	自社の財務体質の確認（マートン法による分析）
	自社のポジショニング確認（PPM.SWOT…）
	内部環境の問題分析（因果ネット～問題構造）
3. 仕組み分析	現状の仕組み分析（業務フロー）



日付	無リスク金利r(無担保コールレート)	残存期間	株式価値期待収益率μ※	株式価値オN(d1)		N(d2)	倒産確率N(-d*2)(12か月)	株式価値V(EX)最適化差
2008年3月31日	0.641%	1	-29.27%	0.279	1.000	1.000	0.01%	1,881,525,608,578
2008年4月30日	0.522%	1	-23.51%	0.284	1.000	1.000	0.00%	1,940,392,702,589
2008年5月31日	0.527%	1	-23.51%	0.284	1.000	1.000	0.00%	2,043,687,792,080
2008年6月30日	0.572%	1	-30.26%	0.286	1.000	1.000	0.01%	1,920,400,104,623
2008年7月31日	0.519%	1	-31.57%	0.291	1.000	1.000	0.06%	1,672,714,029,822
2008年8月31日	0.516%	1	-36.41%	0.295	1.000	1.000	0.17%	1,554,979,841,800
2008年9月30日	0.544%	1	-61.61%	0.339	1.000	1.000	8.63%	1,250,648,072,762
2008年10月31日	0.384%	1	-96.60%	0.555	0.986	0.979	72.00%	763,050,822,369
2008年11月30日	0.318%	1	-103.89%	0.547	0.986	0.979	82.31%	715,290,727,228
2008年12月31日	0.103%	1	-115.07%	0.516	0.990	0.985	92.20%	706,405,128,132
2009年1月31日	0.128%	1	-99.93%	0.540	0.988	0.982	77.96%	751,943,823,499
2009年2月28日	0.109%	1	-92.31%	0.565	0.987	0.979	64.95%	850,796,113,442
2009年3月31日	0.088%	1	-78.07%	0.569	0.987	0.978	48.41%	861,903,112,312
2009年4月30日	0.113%	1	-53.22%	0.661	0.979	0.960	24.35%	1,139,578,084,062
2009年5月31日	0.099%	1	-53.19%	0.661	0.980	0.961	22.12%	1,200,666,577,847
2009年6月30日	0.110%	1	-54.45%	0.662	0.977	0.958	22.47%	1,114,031,986,661
2009年7月31日	0.105%	1	-35.78%	0.659	0.979	0.960	12.82%	1,169,566,981,011
2009年8月31日	0.110%	1	-26.42%	0.659	0.979	0.961	9.48%	1,194,002,378,525
2009年9月30日	0.103%	1	-12.07%	0.628	0.982	0.968	5.10%	1,108,478,487,226
2009年10月31日	0.112%	1	36.64%	0.342	1.000	1.000	0.00%	1,100,703,588,017
2009年11月30日	0.113%	1	42.80%	0.329	1.000	1.000	0.00%	1,097,371,488,356
2009年12月31日	0.094%	1	60.70%	0.348	1.000	1.000	0.00%	1,296,186,768,129
2010年1月31日	0.095%	1	47.07%	0.369	1.000	1.000	0.00%	1,203,998,677,508
2010年2月28日	0.097%	1	29.61%	0.367	1.000	1.000	0.00%	1,144,020,883,610
2010年3月31日	0.082%	1	40.98%	0.380	1.000	1.000	0.00%	1,298,408,167,903
2010年4月30日	0.096%	1	17.81%	0.273	1.000	1.000	0.00%	1,361,718,061,462
2010年5月31日	0.089%	1	-8.59%	0.350	1.000	1.000	0.02%	1,101,814,287,904
2010年6月30日	0.096%	1	-5.85%	0.345	1.000	1.000	0.01%	1,050,722,093,102
2010年7月31日	0.098%	1	-10.61%	0.340	1.000	1.000	0.02%	1,051,832,792,989
2010年8月31日	0.095%	1	-29.05%	0.372	1.000	0.999	0.35%	893,002,709,148
2010年9月30日	0.113%	1	-18.31%	0.371	1.000	0.999	0.11%	922,991,606,097
2010年10月31日	0.093%	1	-22.04%	0.372	1.000	0.999	0.18%	883,006,410,165
2010年11月30日	0.090%	1	-20.48%	0.373	0.999	0.999	0.15%	894,113,409,035

出典：株式会社AStar総合研究所　マートンモデルによる経営環境分析による戦略監査

２．２．４　監査例4
通信業のサイバーセキュリティ監査

個別計画書に基づく下記の項目の監査結果について以下のとおり報告します。

監査対象	重要監査テーマ
通信事業者におけるサイバーセキュリティ法に関わる監査一式	通信事業者におけるサイバーセキュリティ法に関わる監査
目的	サイバーセキュリティ基本法に定義されている「世界的規模で生じている急激かつ大幅な社会経済構造の変化に適確に対応することの緊要性にかんがみ、高度情報通信ネットワーク社会の形成に関する施策を迅速かつ重点的に推進すること」に関しての一翼を担っている通信事業者としての責務と確認。
範囲・手続の概要	セキュリティ監査一覧の内容をヒアリング及び閲覧

出典：株式会社AStar　システム監査事業部　セキュリティ部　サイバーセキュリティ監査報告書

２．２．５　監査例５
金融通信事業者の監査

金融業

金融庁検査マニュアルを参考として

「金融円滑化編チェックリスト」

「信用リスク管理態勢チェックリスト」

「法令等遵守態勢の確認検査用チェックリスト」による

監査・助言

出典：株式会社AStar　システム監査事業部　システム監査部　システム監査部例

３．結論

３．１　システム監査とセキュリティ監査

システム監査	全体	情報システムの整備状況	よりシステムの機能より
		情報システムの運用状況	よりシステムの機能より
セキュリティ監査	セキュリティ	マネジメントを含む情報システムの整備状況	より人為的
		マネジメントを含む情報システムの運用状況	より人為的

システム監査基準にセキュリティ監査は

セキュリティ監査基準書に準拠することが記載されているのでシステム監査は情報システム全体の監査である

出典：株式会社AStar　システム監査事業部　システム監査基準書を元に編集

要修正？

３．２　業種別の全社的リスクとITガバナンス体系

監査	リスク	全業種	製造業	金融業	業務・システム	監査事例対応番号
	情報セキュリティ 情報漏洩					
		情報全般	製造機密	金融ノウハウ	知財情報システム	今回事例無
信頼性	個人情報	顧客情報		個人情報 個人の財務	顧客管理システム	事例５
	財　　務			企業の財務	財務システム	今回事例無
	システム	誤動作	IOTにより高まる	合算値の不一致	全システム	事例２
安全性	戦　　略	経営管理			経営管理システム	事例３
効率性	業　　務 オペレーショナル	生産管理	生産ライン業務		生産システム	事例１
コンプライアンス		説明責任	差無	差無	全システム	事例４
可用性	情報セキュリティ	情報全般	IOTにより高まる	顧客ニーズ	全システム	序論１．１

SDGsにおけるCOSO ERM 2017の活用

- SDGsとは
  - 「Sustainable Development Goals（持続可能な開発目標）」の略称
  - 2015年9月の国連サミットで採択され国連加盟193か国が2016年～2030年の15年間で達成するために掲げた目標。
  - SDGsの目標とターゲット
    - 17の目標と169のターゲットがあり、さらに詳細版である230の指標を策定、Tier1～3の3種類がある。
- SDGsの取組ステップとCOSO ERM 2017のアプローチ
  - 日本企業の多くはCSR活動の一環として認識し活動しているが、世界の企業はSDGsをビジネスチャンスと捉えて実現している。
  - 企業がSDGsに取り組むステップとCOSO ERM 2017のアプローチには共通項が多く、活用には有効である。
  - 企業がSDGsに取り組む際の事業リスクをCOSO ERM 2017フレームワーク*を用いてSDGsビジネスを構築することが可能である。
  - COSO ERM 2017のフレームワーク*を採用すると、ネガティブなリスク、ポジティブなリスクの両方に対応可能である。

•COSO ERM 2017 フレームワーク：5つの構成要素と20の原則
•出典：一般社団法人イマココラボ　https://imacocollabo.or.jp

SDGsの取組ステップとCOSO ERM 2017の主な原則の関連

SDGsの取組ステップとCOSO ERM 2017の主な原則との関連を示す

SDGsの取組みステップ	COSO ERM 2017の主な原則
1. SDGsを理解する	COSO ERM 2017の理解
2. 優先課題を決定する	2-6 ビジネス状況の分析 2-7 リスク選好の定義 3-10 リスクの特定 3-11 リスク重要度の評価 3-12 リスク優先順位の決定
3. 目標を決定する	2-9 事業目標の形成 2-8 代替戦略案の評価
4. 経営へ統合する	1-2 オペレーション階層の構築 1-3 要求される文化の定義 1-4 コア価値徹底の表明
5. 報告とコミュニケーションを行う	4-16 リスクとパフォーマンスレビュー 5-20 リスク・文化・パフォーマンスのレポート

注）□-■
□：5つの構成要素を番号で示した
■：20原則の番号

1. ガバナンスと文化
2. 戦略と事業目標
3. パフォーマンス
4. レビューと改版
5. 情報、コミュニケーションとレポーティング

•出典：COSO ERM 2017（5つの構成要素と20の原則）
•出典：一般社団法人イマココラボ　https://imacocollabo.or.jp

SDGsの17の目標

出典：一般社団法人イマココラボ
https://imacocollabo.or.jp

Sustainable development goals - United Nations
URL: http://www.un.org/sustainabledevelopment/sustainable-development-goals/
Communications materials - United Nations Sustainable Development
URL: http://www.un.org/sustainabledevelopment/news/communications-material/

出典

1.田中　普輔等,日立評論「IOTシステムとセキュリティ課題と解決アプローチ」

２.サイバーセキュリティ基本法などを参考に編集

3.神橋　基博,システム監査学会30回研究大会 「プロセスアセスメントを用いた事業体ベンチマーキング」

4.ISACA　COBIT5

5. COSO ERM Integrating with Strategy & Performance (2017/June)

6.石島　隆,大阪成蹊大学　研究紀要　第1巻第1号 「ITガバナンスとIT統制」

7.ISACA　VAL－IT　ISACA　COBOT5.0

8.株式会社AStarコンサルティング事業部コンサルティング部

9.AStar総合研究所　基礎技術部

10.株式会社AStar総合研究所　　マートンモデルによる経営環境分析による戦略監査

11.株式会社AStar　システム監査事業部　セキュリティ部　サイバーセキュリティ監査報告書

１2,株式会社AStar　システム監査事業部　システム監査部　システム監査部例

１3,株式会社AStar　システム監査事業部　システム監査基準書を元に編集

１4.一般社団法人イマココラボ SDGs, https://imacocollabo.or.jp

御連絡はこちらに

株式会社ＡＳｔａｒ総合研究所

東京都渋谷区桜丘町26-1　セルリアンタワー15階

Email：institute@astarnet.jp