

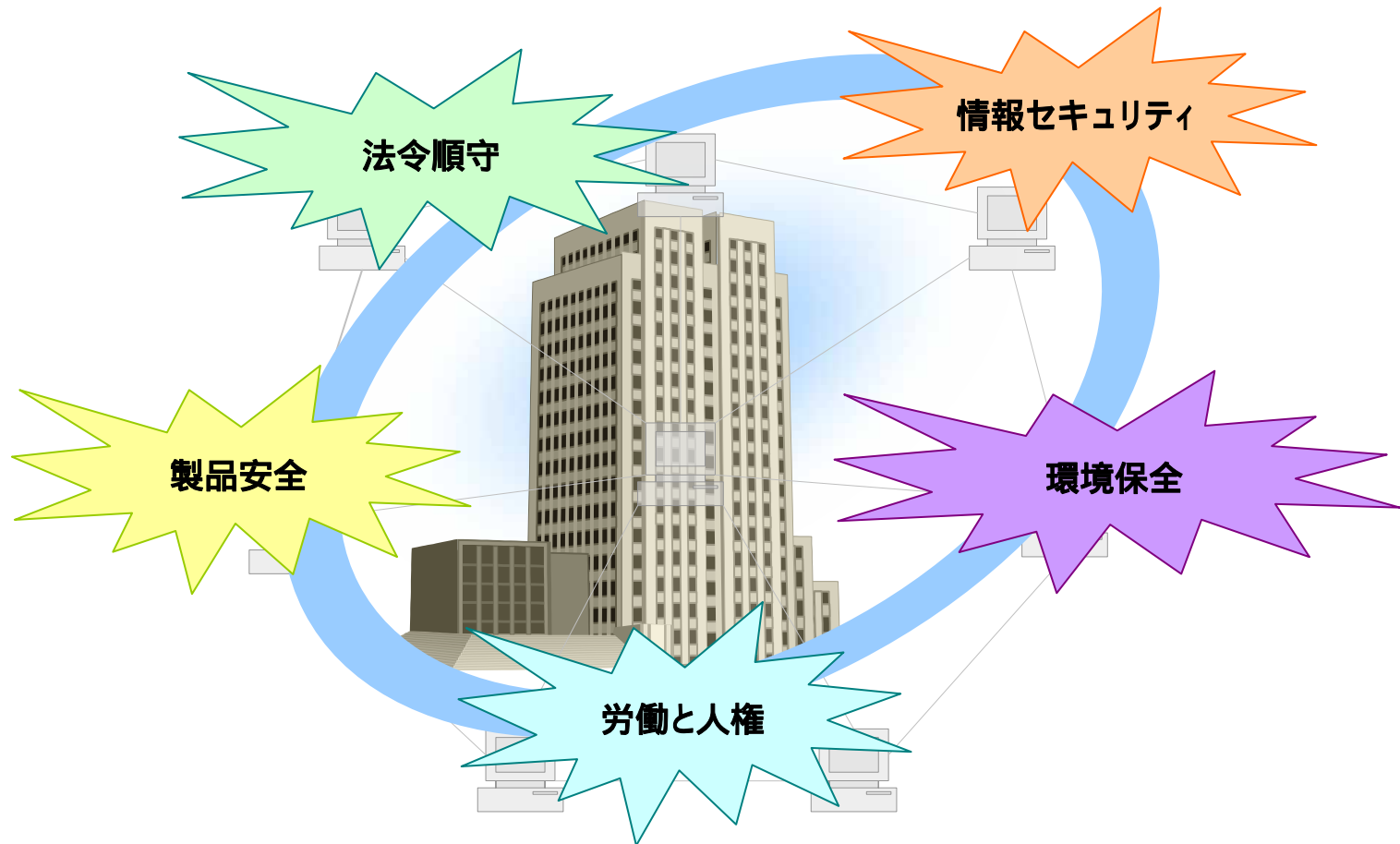
コンプライアンスの問題点と対策

- M@gicPolicyQUICK Ver.3.2 -

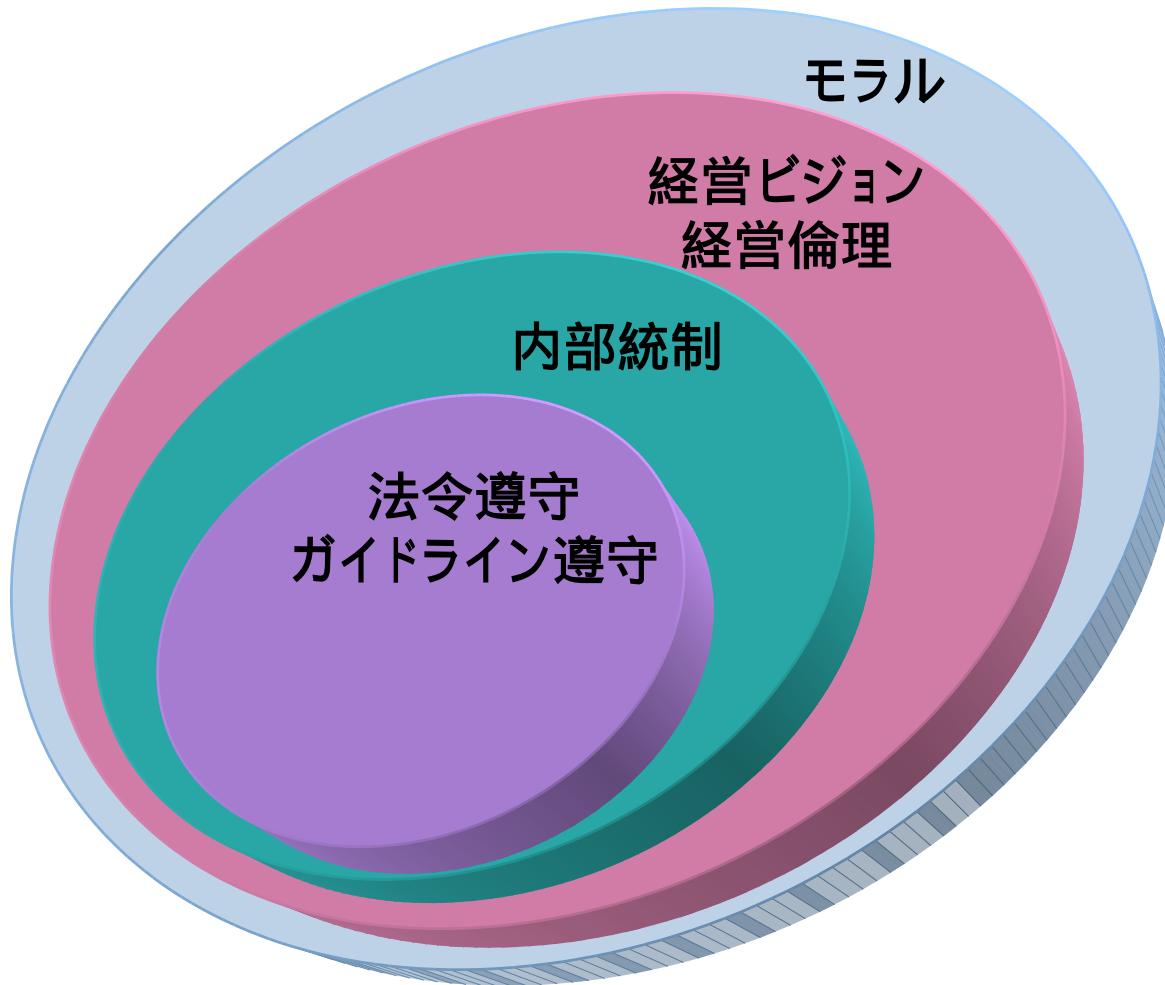
株式会社アズジェント

2008.2

重要性を増す『企業の社会的責任』

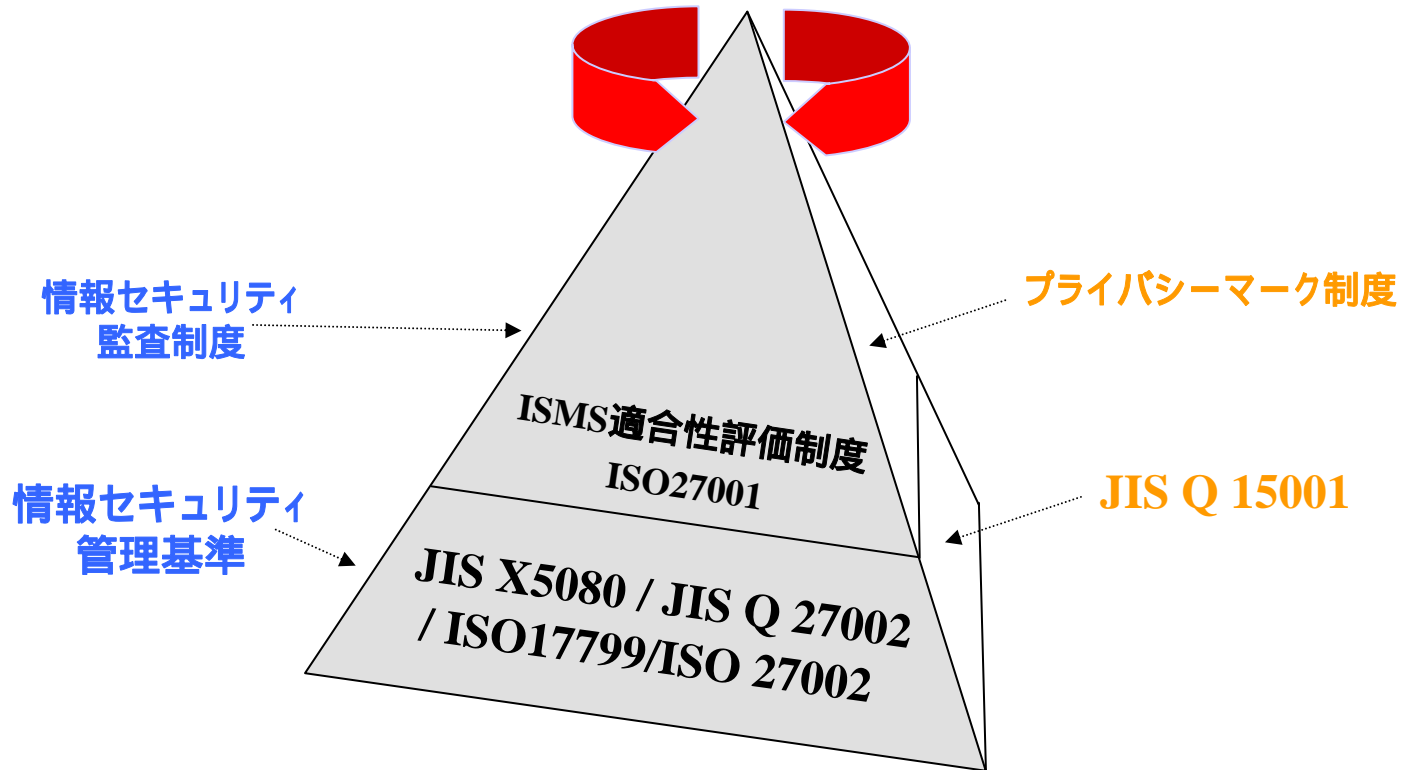


そもそもコンプライアンスとは？



それで・・・
セキュリティコンプライアンスは・・・

セキュリティコンプライアンス



国内外とも旧名称から27000シリーズへの以降フェーズ

経営者の意識の変化



タイプ1

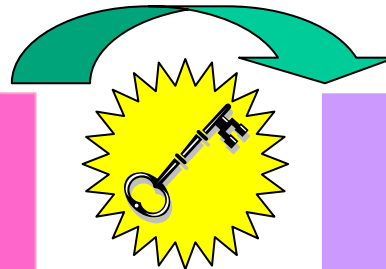
- ・必要なのか？
- ・面倒くさくないのか？
- ・初期コストと時間が掛かるのでは？



認証という形式だけを取得

又は

ほうっておく



タイプ2



- ・未然に損失を防ぐ
- ・平準化される
- ・状況の可視化による現状改善



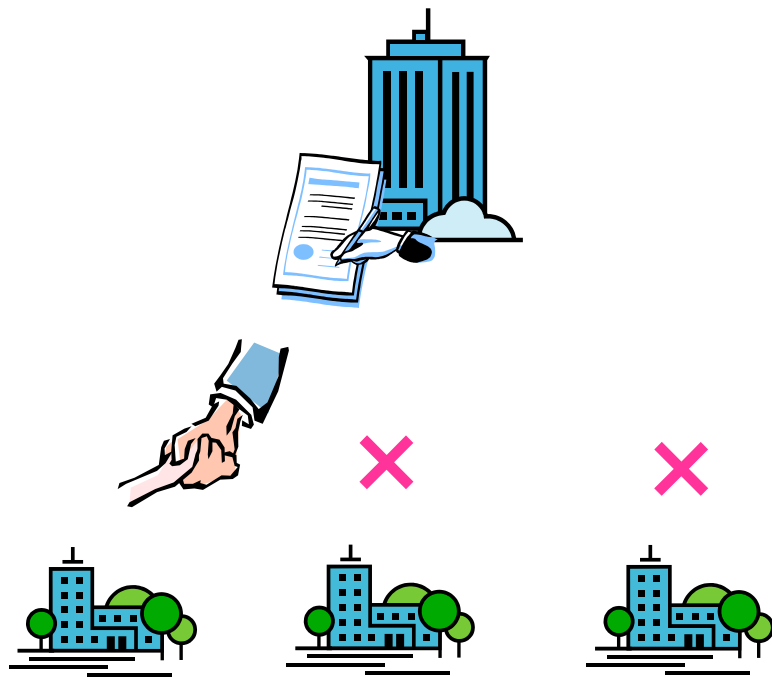
セキュリティ強度を上げたい



結果：コストセーブ、競争力UP

PDCAによる競争力UPとは

受注にあたり元受企業から、SLAを求められる



Service Level Agreement: 客先が求めるセキュリティ基準に基づく運用を保証等する契約

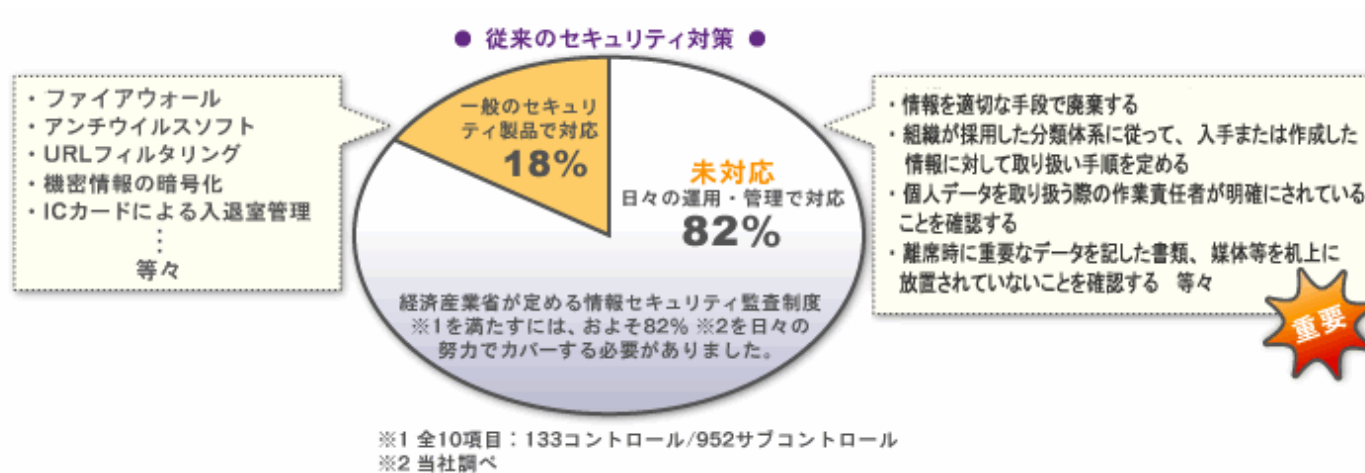
受注環境の変化

元受企業などが、取引や発注を行うにあたり、セキュリティにおいても、一定水準以上のセキュリティレベルの維持を取引の条件とし、取引先を選別するケースが増えてきている。

PDCAサイクルが運用に乗っているか否かを競争力として考慮しなければいけない社会環境になってきている。

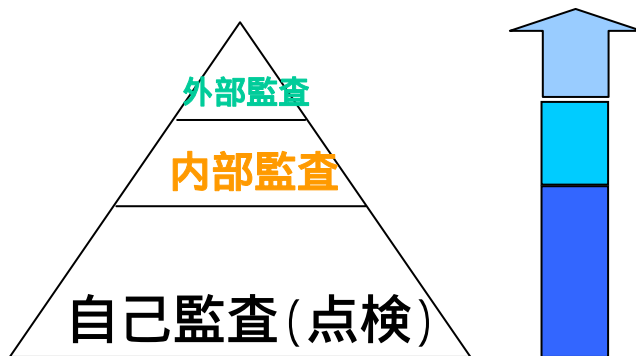
バックアップ知識 セキュリティ商品と基準の乖離

セキュリティ商品で対応できる項目は18%



バックアップ知識 自己監査(点検)

監査側面からの視点

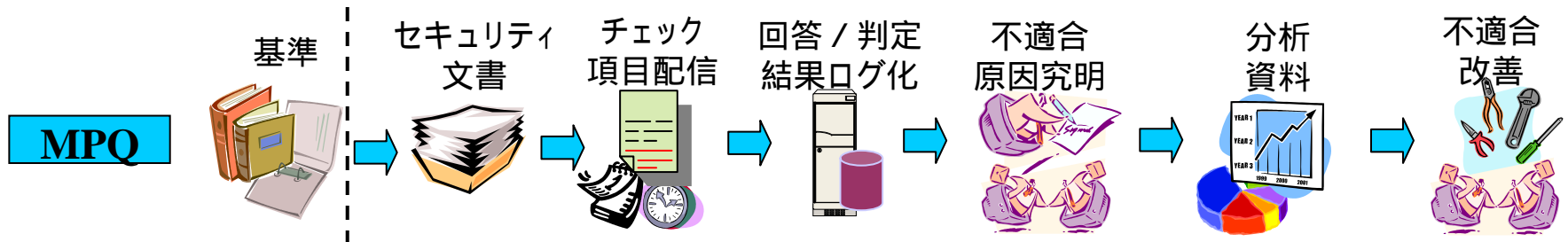


自己監査すらできていない組織では、内部監査や外部監査の意味が無い。

自己監査(点検)とは

- 組織として、一人一人が何をしなければいけないか、何をしてはいけないか、が明確になっていなければならない。
- その上で、各人が明確化されたアクションを実施できたか否かを自己チェックできなければならない。

一連の動作概要



Ver .3.2の開発コンセプト



汎用的な自己点検フレームワーク

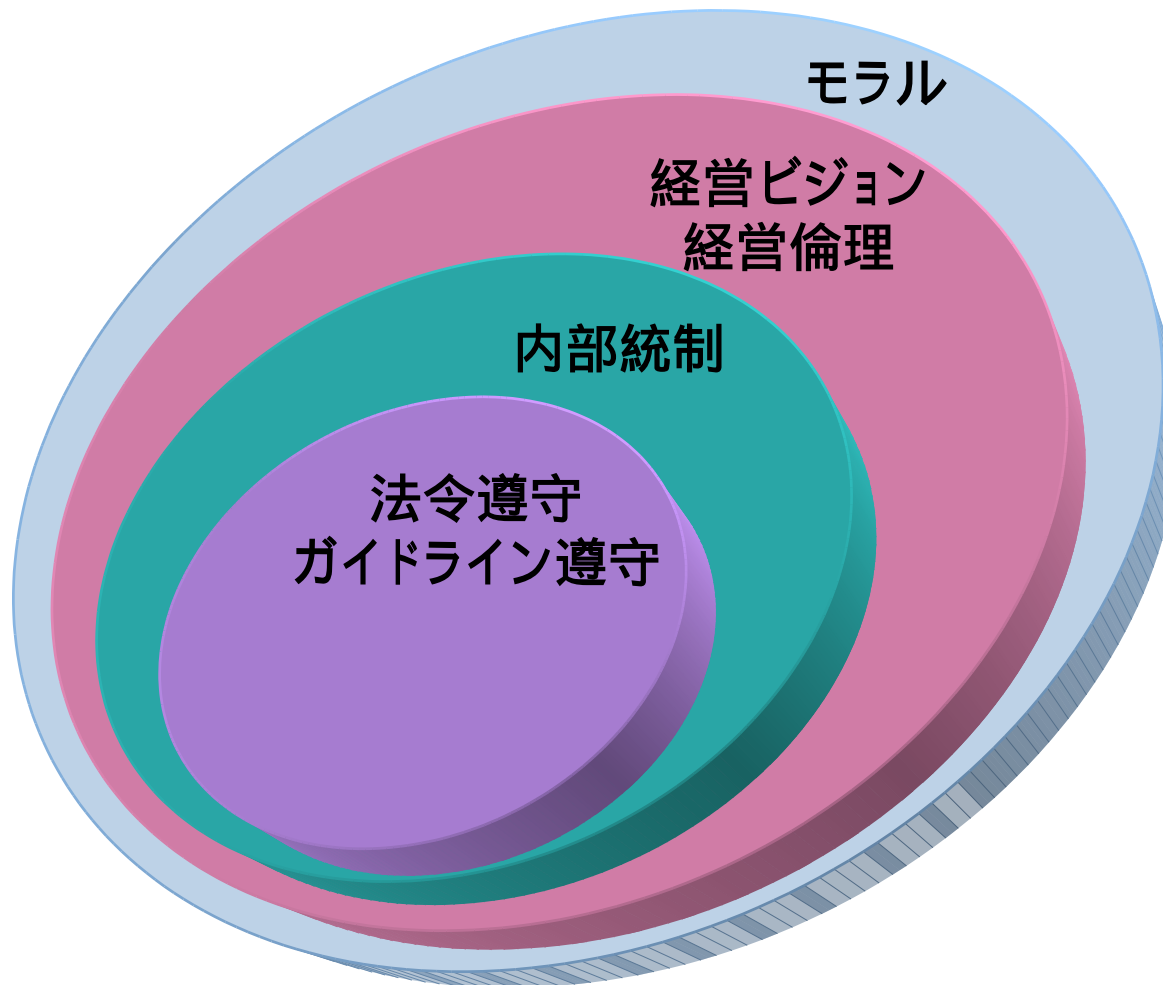
情報セキュリティ
+ コンテンツ

J-SOX

EMS/QMS

汎用改善
(社内、業務、営業、マネ
ジメント)

経営者の視点は・・・



何の為に、何を選択？

目的



競争力アップ
社会的責任の履行
社内カイゼン等々

対象分野

ISMS

(個人情報保護含)

コンテンツ有

J-SOX

(金融商品取引)

コンテンツ無

環境

(EMS: ISO 14000)

コンテンツ無

品質

(QMS: ISO 9000)

コンテンツ無

汎用改善

(社内、業務、営業、
マネジメント)

コンテンツ無

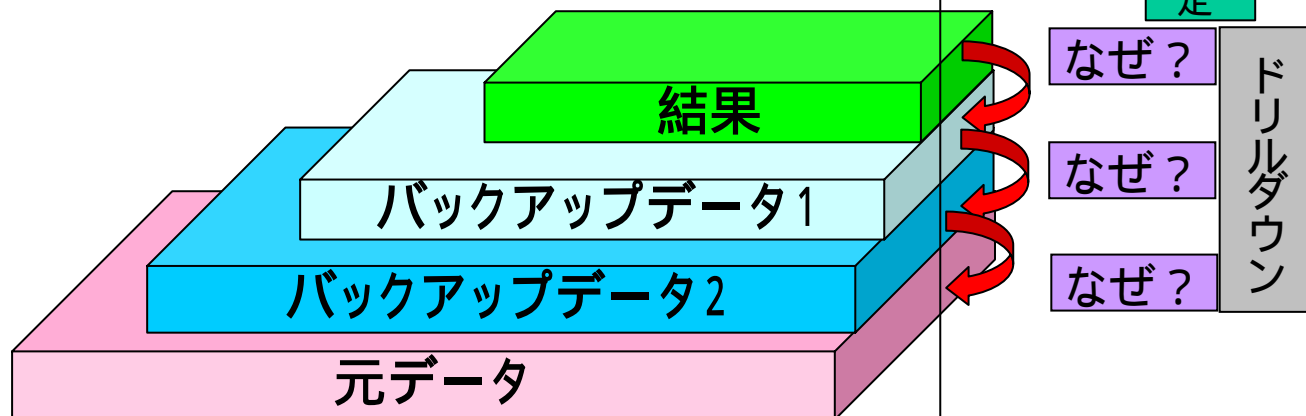
...

バックアップ知識 意思決定のためのプロセス

ミドルマネジメントのタスク

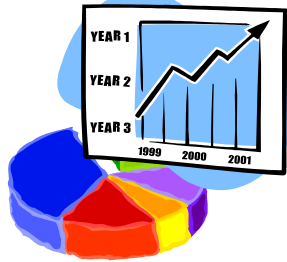
経営層のプロセス

- ・意思決定の為の見える化
- ・ドリルダウンをサポートする為のバックアップデータ



マネジメントのポイントは2つ

その1: 的確な分析



問題点把握 > 原因特定 > 対策指示・立案

その2: 進捗管理

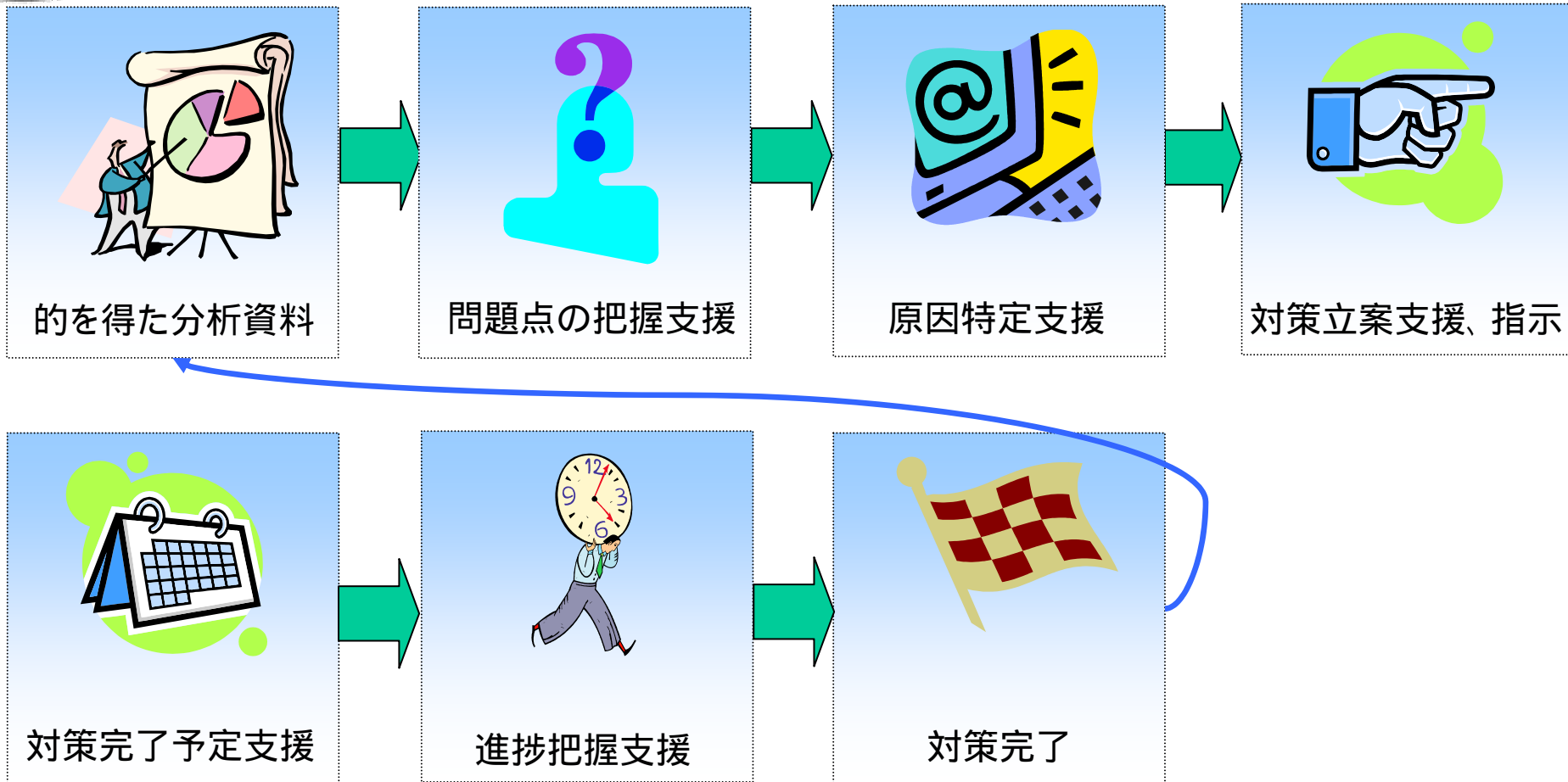


> 対策完了予定日の決定 > 進捗把握 > 対策完了

マネジメントは「的確な分析」と「対策の進捗管理」が欠けると成立しない

特に  で解決できる点は？

マネジメントの支援

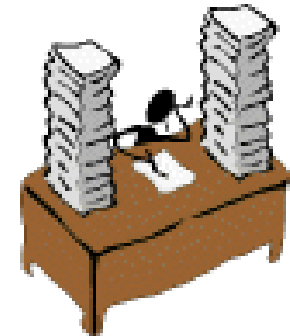


たとえば・・・

結果の集計

問題点

- 集計作業が煩雑
 - ・ 自己監査(点検)や、内部監査のアンケート形式の場面
 - ・ 量が増えるとExcelエラーが多発し集計が困難
 - ・ 回答時にフォーマットが変更される等が多発し、結局手作業で集計
例) 回答セルを間違える、セルを追加しコメントを挿入 等



M@gicPolicyQUICKで解決

- 集計作業の軽減ができる
 - ・ ワンクリックで正確な集計ができる

集計結果の分析

問題点

- 集計結果の分析作業まで手が回らない
 - ・ 自己監査(点検)、内部監査、外部監査の場合
 - ・ 部門比較、不適合率、及びその改善率の推移まで分析に手が回らない

M@gicPolicyQUICKで解決

- **集計結果の分析作業が大幅に軽減できる**
 - ・ 部門毎の比較や、未判定率、発生した不適合率、その改善率がワンクリックで表示、期間毎の比較等も簡単にできる



改善状況の把握

問題点

- 各項目の改善状況が把握できない
 - ・ 改善項目、対象部門が増えてきた場合
 - ・ 『対応完了』『対応中』『未対応』等の改善状況の進捗把握が困難



M@gicPolicyQUICKで解決

- **改善状況が簡単に把握できる**
 - ・ 部門毎の改善状況や、対応状況毎の検索・表示ができる

トレーサビリティ

問題点

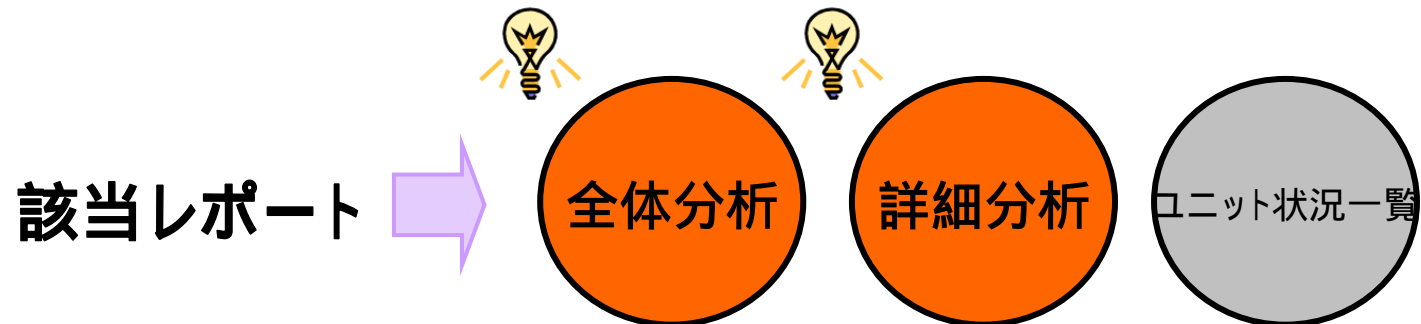
- 過去の自己点検、監査履歴、規程類等の管理が煩雑
 - ・ 自己点検、監査履歴が増えてきた場合
 - ・ 書類、電子データ、E-mail等 必要な情報の管理が煩雑
 - ・ 規程類や手順書の更新が頻繁に行われ履歴管理が煩



M@gicPolicyQUICKで解決

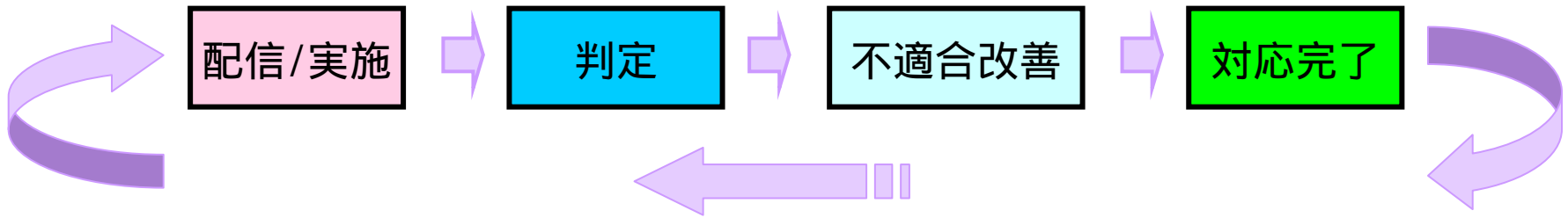
- **過去の監査(点検)履歴が簡単に確認できる**
 - ・ 運用情報(監査(点検)結果、分析結果、コミュニケーション履歴改善状況)が一元的に管理されており、簡単に検索・表示ができる

的確な分析のポイント

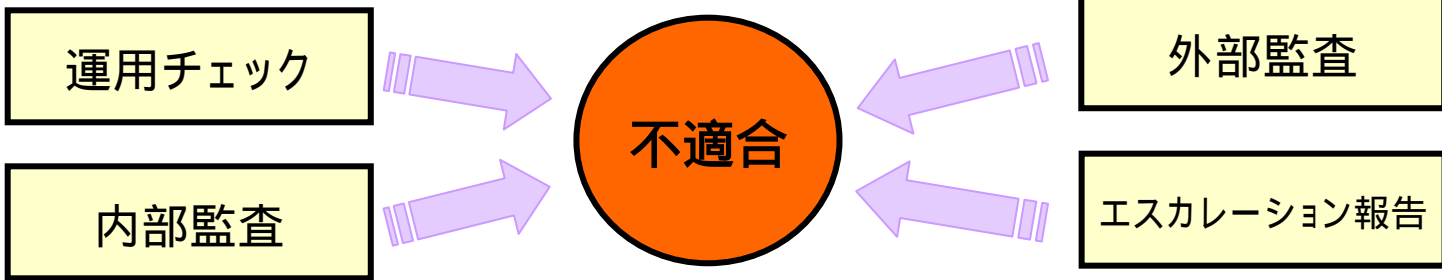


『もれなく』分析する

ライフサイクルからの視点



発見要因からの視点



『ダブリなく』分析する

比率からの視点

判定が未完了のまま放置している割合

- **判定未完了率**: $(A - B) / A$

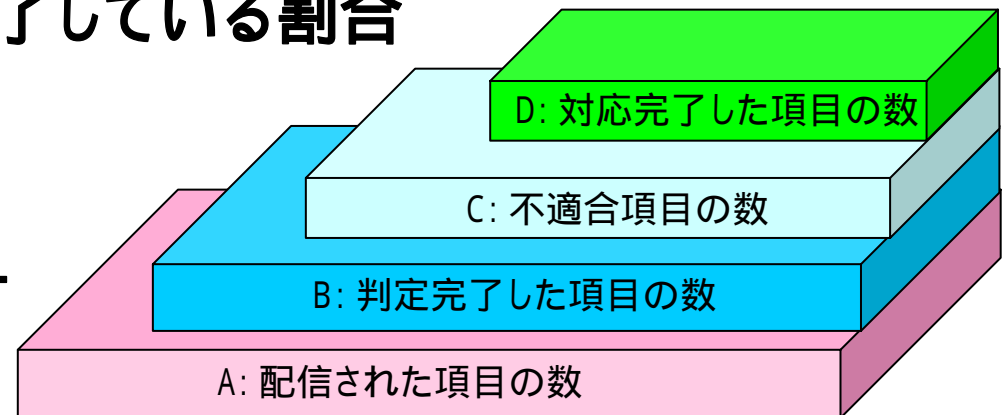
不適合の発生している割合

- **不適合率**: C / B

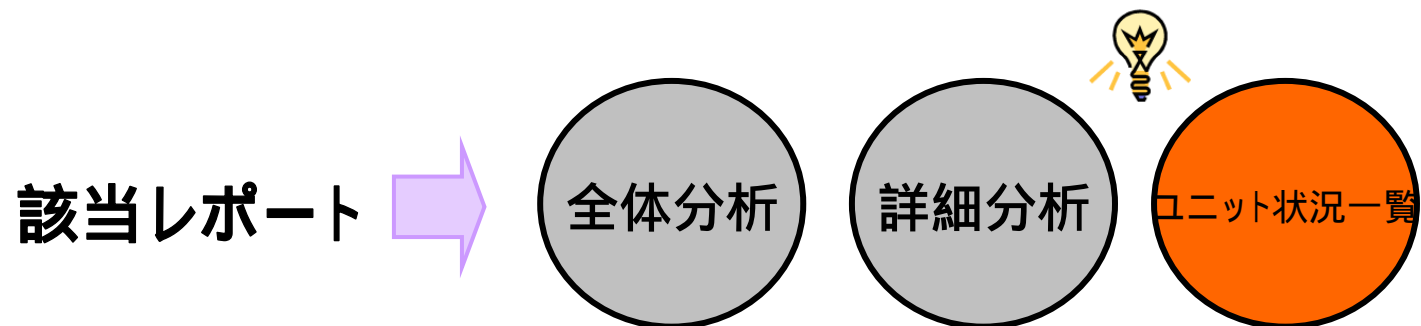
発生した不適合が対応完了している割合

- **不適合改善率**: D / C

さらに上記を分類別に表示可



進捗管理のポイント



『見える化』して進捗管理する

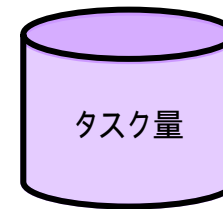
タスク量からの視点



A部



B部



C部

期日からの視点

超過 (指定された対応期限を過ぎた項目)

経過 (上記以外のTODO表示後日数が過ぎた項目)

予定 (タスクの開始予定)

予定 (タスクの終了予定)

今日時点

時間

こんな使い方も・・・



汎用的な自己点検フレームワーク

情報セキュリティ
+ コンテンツ

J-SOX

EMS/QMS

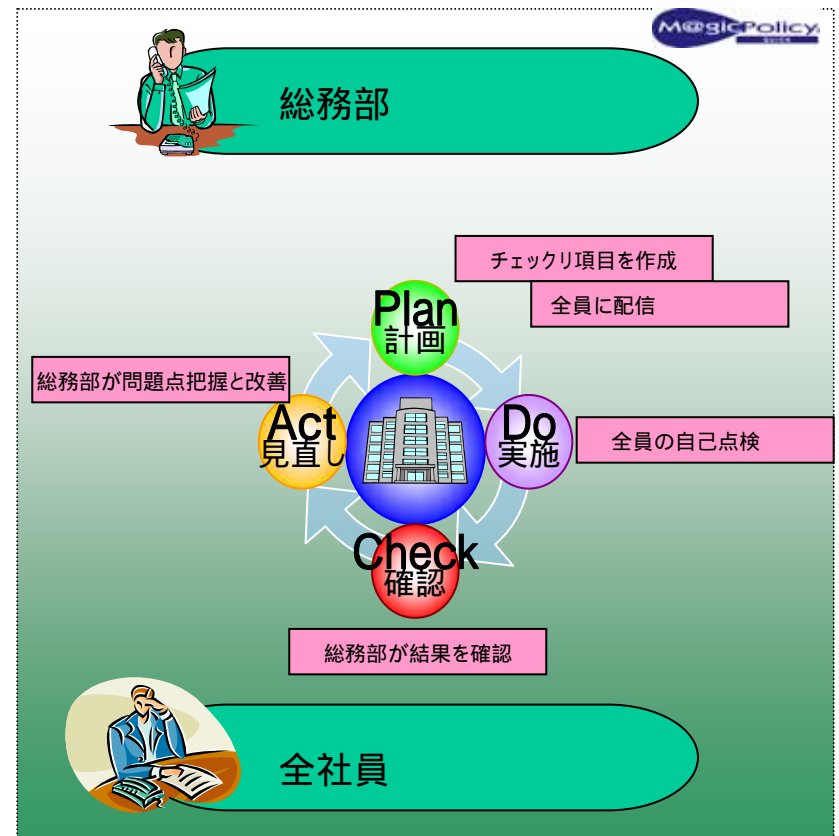
汎用改善

(社内、業務、営業、マネ
ジメント)

こんな使い方 - 社内改善 -

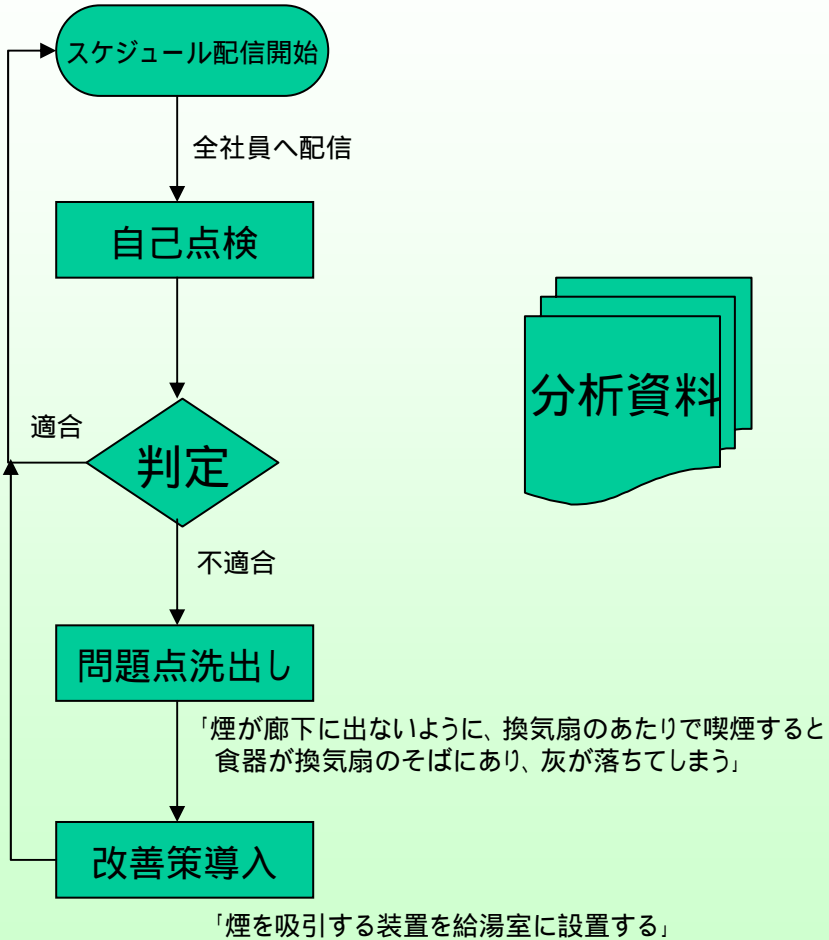
全社員に関連するマナー向上

給湯室での喫煙時に、食器類に灰を落とす人がいて困る！



総務部

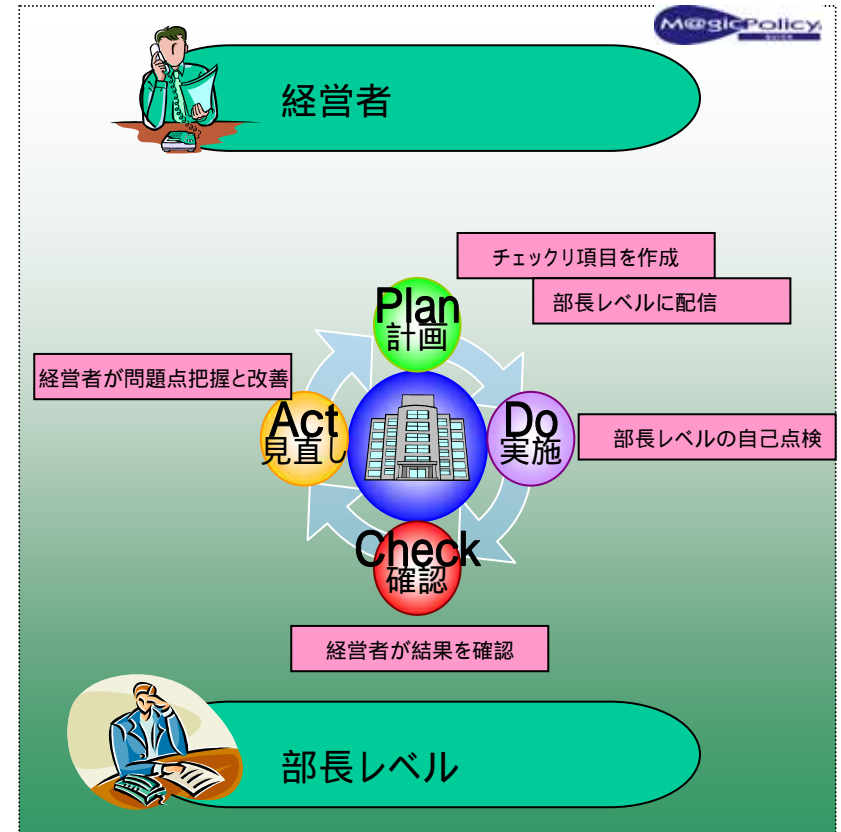
総務部用項目 「給湯室で喫煙時に食器に灰を落としていませんか？」



こんな使い方 - マネジメント改善 -

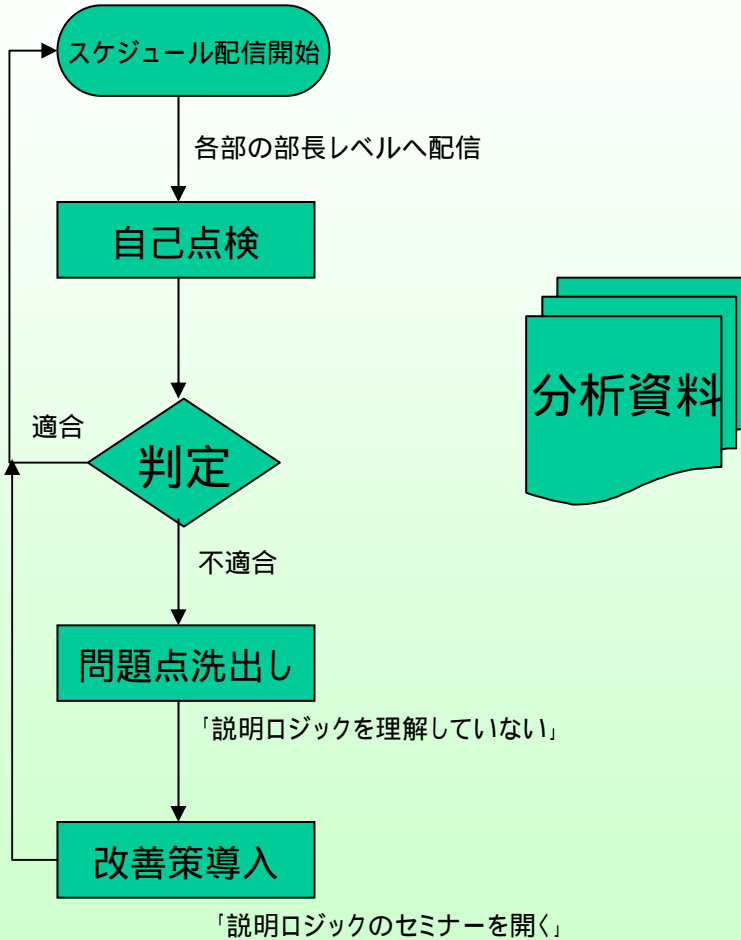
経営者の考え方の浸透

部長会での報告が、時間ばかりかかり、要領を得ていない！



経営者

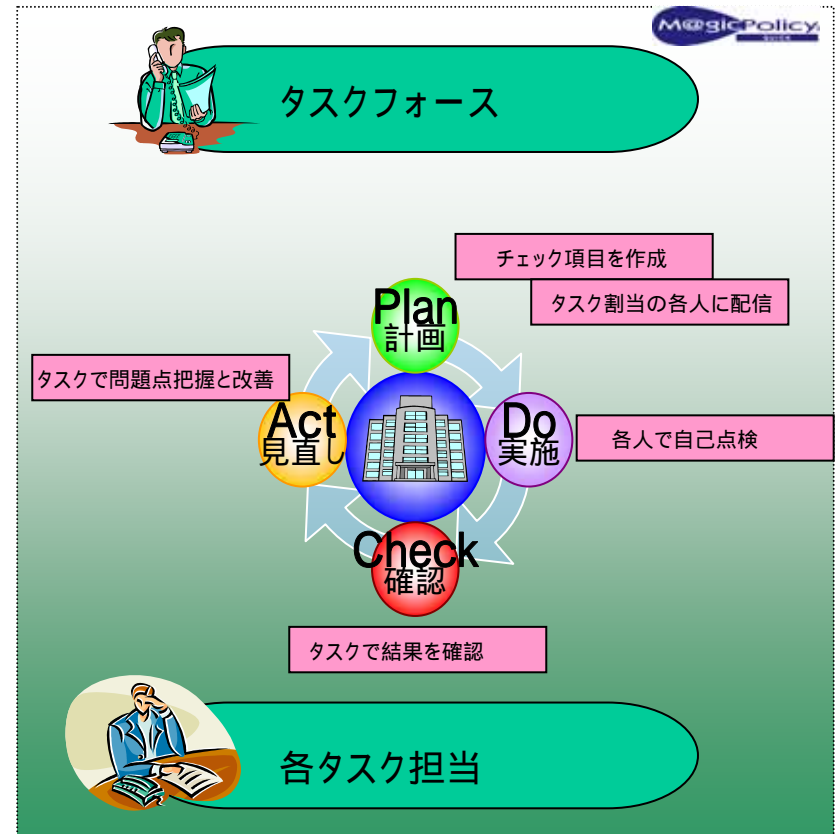
総務部用項目 「打合せは結論を先、質問が出たらなぜならを徹底していますか？」



こんな使い方 - タスク改善 -

タスクフォースでの進捗管理

複数部門にまたがる、タスクフォースの役割分担と進捗がマネジメントできず、効率が悪い！



タスクフォース

総務部用項目

「検証は期日までに終了しますか？」

⋮

総務部用項目

「商品パッケージングは期日までに終了しますか？」

スケジュール配信開始

各タスク担当へ配信

自己点検

適合

判定

不適合

問題点洗出し

「検証サーバが不足して技術検証の一部が間に合わない」

改善策導入

「下期予算のIT部門のサーバ購入時期を前倒しし、
検証サーバとして臨時で1ヶ月間利用する」

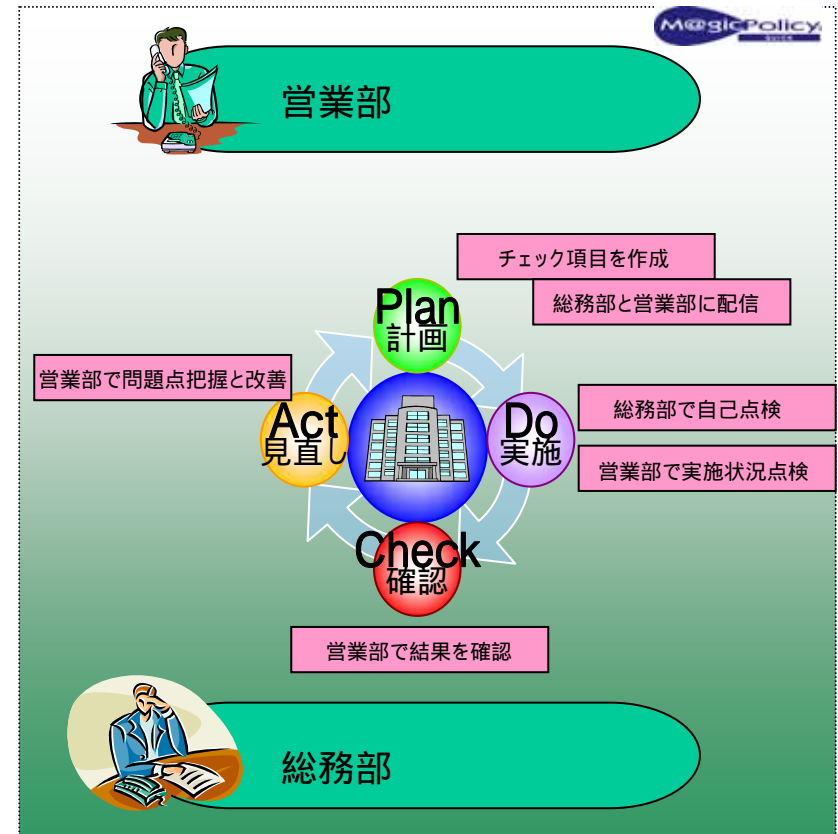
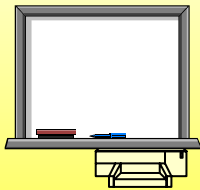
分析資料

こんな使い方

- 業務改善(クロス利用) -

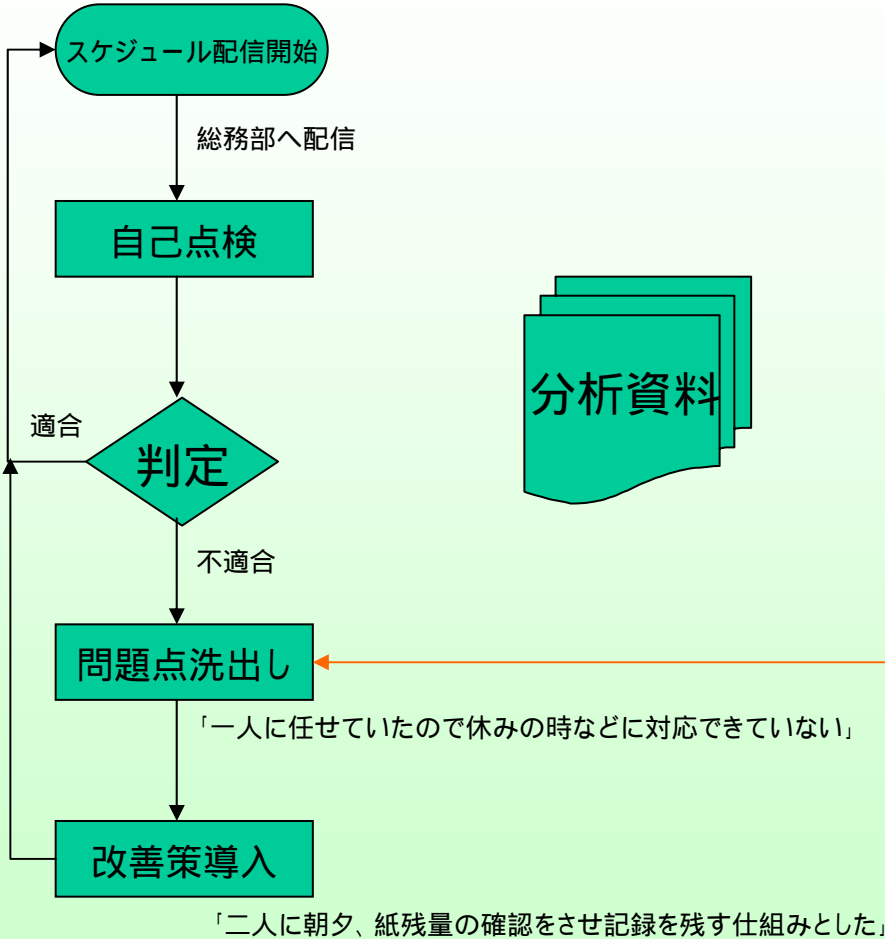
他部署がからむ身近な問題

コピーボードを使おうと思うと、いつも紙が無い！
 総務部は、毎日点検して、紙を入れてくれないと！



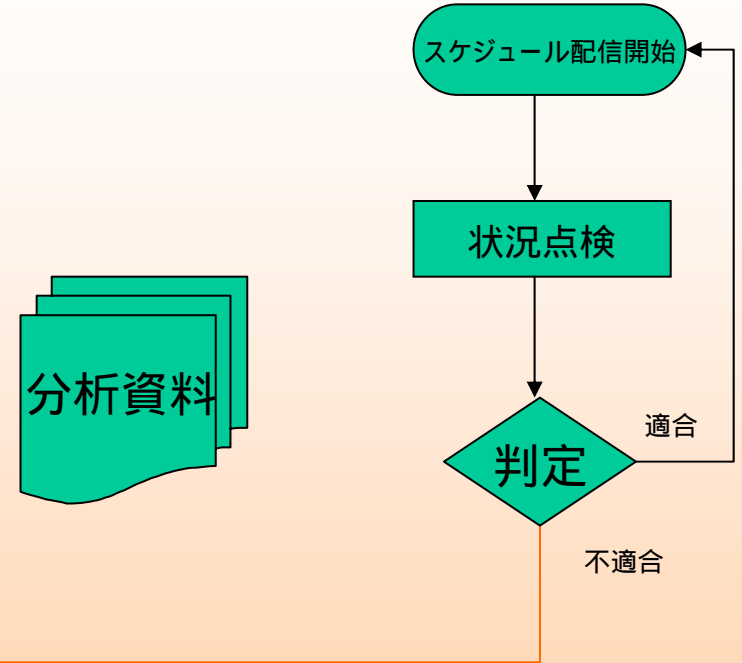
総務部

総務部用項目 「コピーボードは紙切れしないように補充していますか？」

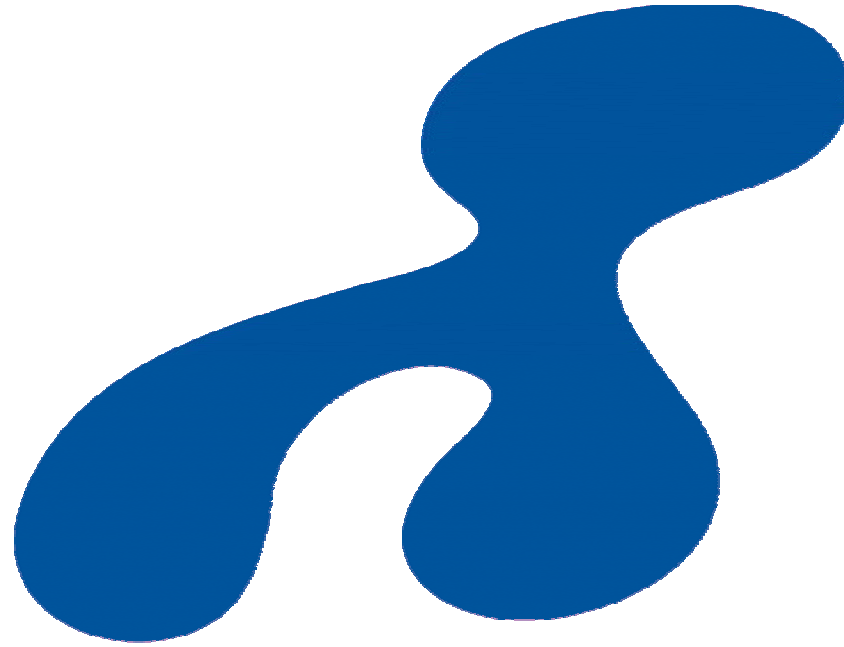


営業部

営業部用項目 「コピーボードは紙切れ無く、使うときに利用できますか？」



Asgent



One Step Ahead of The Game
Asgent
アズジェント