Control Self-Assessment

CSAアンケート・ナビ

－雛形で理解するCSAアンケートガイド－

2020年6月25日版

CIAフォーラム

CSA実践研究会（ No.d2 ）

Control Self-Assessment

目次

はじめに

Part Ⅰ　CSAアンケートの企画

Part Ⅱ　CSAアンケートの作成

Part Ⅲ　CSAアンケートの実施

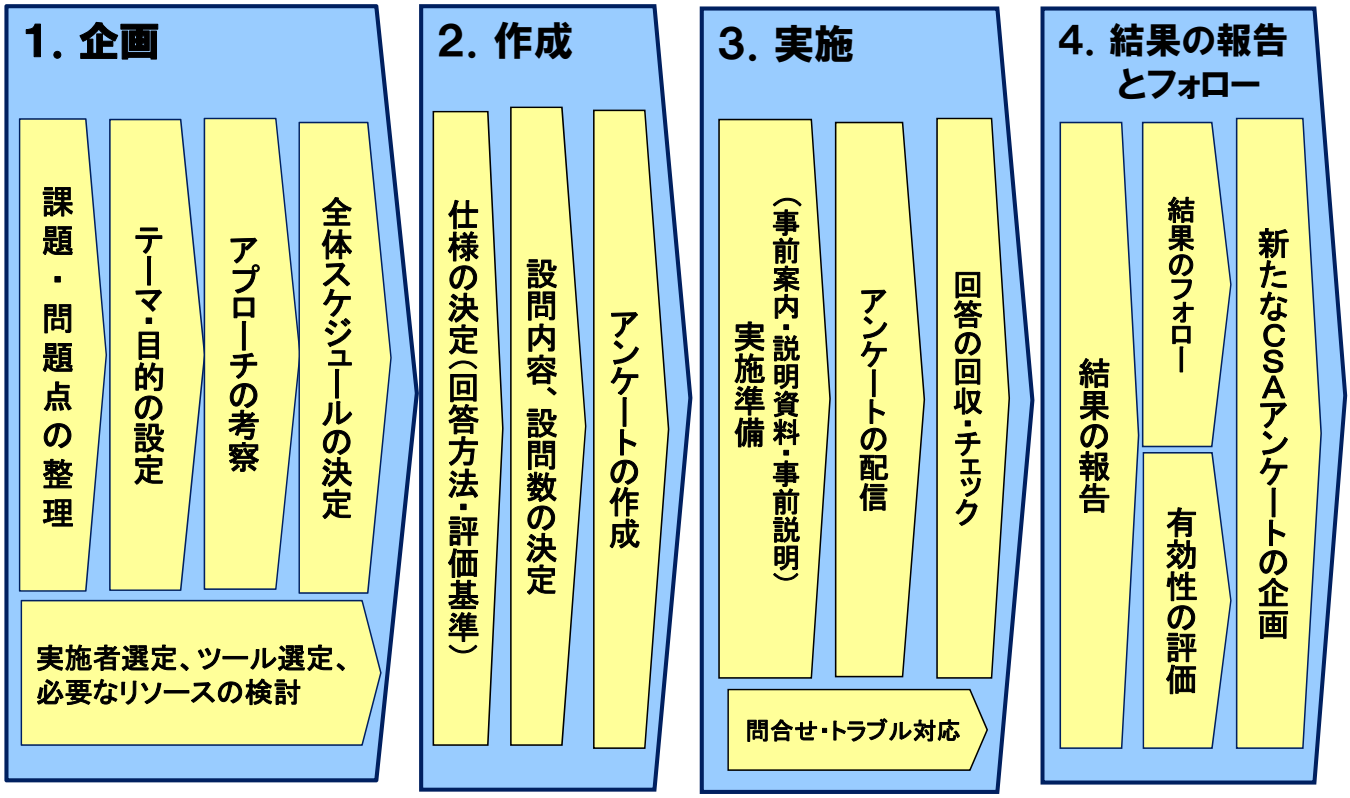
Part Ⅳ　CSAアンケート結果の報告とフォロー

おわりに

Appendix

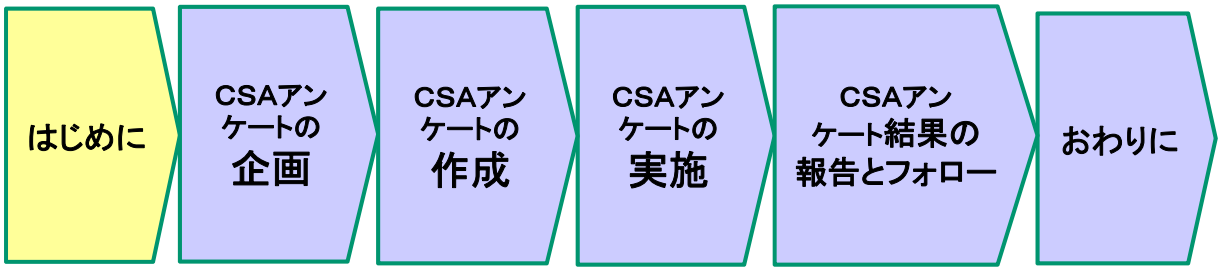
- テンプレート
- アンケート雛形を用いた分析例
- 参考資料

CSAアンケートプロセス



Control Self-Assessment

はじめに



Control Self-Assessment

Control Self-Assessment

本冊子の目的

- 本冊子は、CSAアンケートの企画・推進に、初めて取り組もうとしている内部監査部門、リスクマネジメント部門などの方のためのガイドです。
- CSAアンケートは比較的取り組みやすく、活用範囲の広いツールですが、効果的に推進するためには、検討すべき事項が多くあります。
- 本冊子には、CSAアンケートを効果的に推進するための留意事項をいろいろと盛り込んでいます。
- 本冊子がこれからCSAアンケートを推進されるみなさんのお役に立てれば幸いです。

Control Self-Assessment

CSAアンケート・ナビの特徴

- 「企画」-「作成」-「実施」-「報告・フォロー」と、CSAアンケートで実施することを時系列・網羅的に解説しました
- そのまま使える「CSAアンケート雛形ファイル」および解説資料を付けました
  - 「CSAアンケート雛形ファイル」を実際に確認していただくとより理解が深まります
- Appendixにテンプレート、分析例および参考資料をつけました。
  - CSAアンケート実施に必要な書類をテンプレートとして添付しました。
  - CSAアンケート雛形を用いた分析事例を添付しています。
  - CSAを知る上で役立つ情報を参考資料として添付しました

CSAとは

- CSAとは？
  - 統制自己評価（Control Self-Assessment: CSA）は、 管理者と従業員が、組織のリスクマネジメントとコントロール プロセスの妥当性を評価するために利用できる手法です。
  - 内部監査人は、CSAの利用により、高いリスクまたはその懸念のある領域に監査計画の焦点を絞るための関連情報を入手できます。
  - 管理者や従業員のリスクやコントロールに関する理解を深め、コントロールの改善に向けた活動を促進することができます。
  - CSAには、いくつかの形式がありますが、いずれの方法によっても、CSAの究極的な価値は、経営者の目標達成を支援することにあります。

Control Self-Assessment

CSAの形式－1

- CSAの形式－代表的な2つの形式
  - アンケート形式
    - 主催部署が、業務やプロセスに関係する人（責任者や担当者など）に質問書を送付し、リスクやコントロールの自己評価を記入してもらい、主催部署で回収・集計・分析を行なうものです。
  - ワークショップ形式
    - その業務やプロセスに関係する人（責任者や担当者など）の参加により、ファシリテーターの進行のもとに議論を行い、リスクやコントロールの弱点などを識別し、そのリスクを管理するための対応策を合意するものです。
- どちらの形式がより優れているということはなく、形式の特徴を理解し、目的、内容などに相応しい形式を選ぶことが大切です。
- 2つの形式を組み合わせて実施することでより効果的になるケースもあります。

Control Self-Assessment

Control Self-Assessment

CSAの形式-2

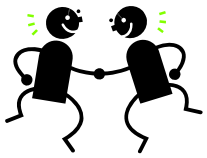
	アンケート形式	ワークショップ形式
メリット	・多人数を対象とすることが可能である ・対象者の日程調整の必要がない ・対象者間で匿名性が確保される	・参加者の合意形成ができる ・参加者間で情報交換、議論がある ・必要に応じて、焦点を絞り込める
デメリット	・対象者の理解や意識を確認できない ・テーマや質問が硬直的となる ・評価結果は対象者の合意ではない	・時間を拘束するため多人数の参加は難しい ・参加者間では匿名性がなく、率直な議論が行われる保証はない ・組織風土によっては受け容れにくい

Control Self-Assessment

アンケート形式のCSA とは

- アンケート形式のCSAとは？
  - 活用できる範囲が広く、柔軟に実施できるのがアンケート形式です。その理由は、直接足を運べない海外子会社等に対しても実施することができ、また一度に多くの回答を集めることにより、幅広い対象の意見を一定の精度で把握できるからです。
  - しかし、精度を高めるためには工夫が必要です。
- アンケートを成功させるためには？
  - すべての実施者がアンケートの目的と評価基準を理解すること
  - 誤解されにくい質問内容とすること
  - 誠実に回答する気風・組織文化があること

  などが必要です。



- そのための準備としては？
  - 目的と設問の内容が食い違うなど、アンケートに不備や分かりにくい点があってはうまくいきません。
  - CSAアンケートの価値や目的などについて、実施者によく理解しておいてもらうための取組みが必要です。

Control Self-Assessment

アンケート形式CSAのメリット

- 一般的に次のようなメリットが考えられます。
  - 多人数や幅広い範囲を対象とすることが可能であり、対象者の日程調整や移動の必要がなく、物理的な負担が少ない。
  - 対象者間の匿名性が確保されることにより、精神的な負担も少ない。
  - サンプルを増やすことができ、場合によっては全数調査も可能となるため、統計上の信頼性を確保することができる。
  - 重要なルールや誤解しやすい事項の認識を促すことができる。
- 内部監査部門にとっては、次のようなメリットが期待できます。
  - 幅広く現場の問題やリスクを洗い出すことにより、状況把握ができる。
  - 規程の整備・運用状況等、明確に定められたコントロールを効率的に評価することができる。
  - 監査リソースをリスクの高い分野に集中することにより、監査のコストの削減ができる。

Control Self-Assessment

アンケート形式のCSAが活用できる場面

- アンケート形式のCSAは、比較的柔軟なツールであり、範囲、対象者（実施者）を検討することで次のような様々な局面で利用することが可能です。
  - 全社的なリスクやコントロールの評価
  - 部門横断的な一連の業務のリスクやコントロールの評価
  - 組織横断的な統一ルールの整備・運用状況の評価
  - 内部監査計画立案のためのリスクの分布状況の把握
  - 監査対象分野、組織におけるリスクの特定と評価
  - 監査対象分野、組織におけるコントロールの整備、運用評価
  - 内部監査結果を受けての改善策の検討
- アンケート形式のCSA結果を集計することで、リスクやコントロール状況を可視化でき、CSA実施者や責任者に気づきを与え、改善活動を促進することが可能です。

Control Self-Assessment

こんな場面で使えます－1

・ 内部監査計画立案のためのリスクの分布状況の把握

～内部監査人AとBのやりとり～

A「困ったなぁ」

B「どうしたの？」

A「今度の〇〇部門の監査、私が主任になったんだけど、あんまり経験が無い分野なので、どこにフォーカスすればいいか分からないんだよね」

B「リスクの状況は分かってる？」

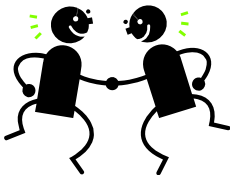
A「リスクの抽出もだいたいのコントロール内容も分かってるんだけど、実際どれくらいコントロールが効いてるかが分からない。つまり残存リスクが不明」

B「ここで悩んでても仕方ないさ。答えは現場にあるんだから、現場に聞けばいいんだよ」

A「どうやって？部門長には軽く聞いたけど、ピンと来なかった」

B「CSAアンケートしてみれば、全員の意見が聞けるじゃない」

A「そうか！その手があったね。よしさっそくやってみよう」



Control Self-Assessment

こんな場面で使えます－2

・ 組織横断的な統一ルールの整備・運用状況の評価

～情報セキュリティ担当Cと内部監査人Dのやりとり～

C「困ったなぁ」

D「どうしたの？」

C「最近いろんなところで情報漏洩が問題になってるだろう？上からうちの会社は大丈夫なんだろうね？ちゃんと確認しとけよ、って言われてね」

D「本社は細かく管理されてるでしょ？」

C「子会社が問題なんだよね。本社と同じルールを全子会社にも適用しているけど、正直どこまできちんと守られてるか分からない。というか、本当に浸透しているのかも自信がない。全部の子会社まわる時間もないし」

D「なるほど。子会社によってまちまちかも知れないね」

C「そうなんだ。できてない子会社を選んで指導に行きたい。そのためには、だいたいでいいからルールの浸透度とか遵守度が分かるといいんだけどな」

D「CSAアンケートしてみれば、概要が分かるんじゃないかな」

C「そうか！その手があったね。よしさっそくやってみよう」

Control Self-Assessment

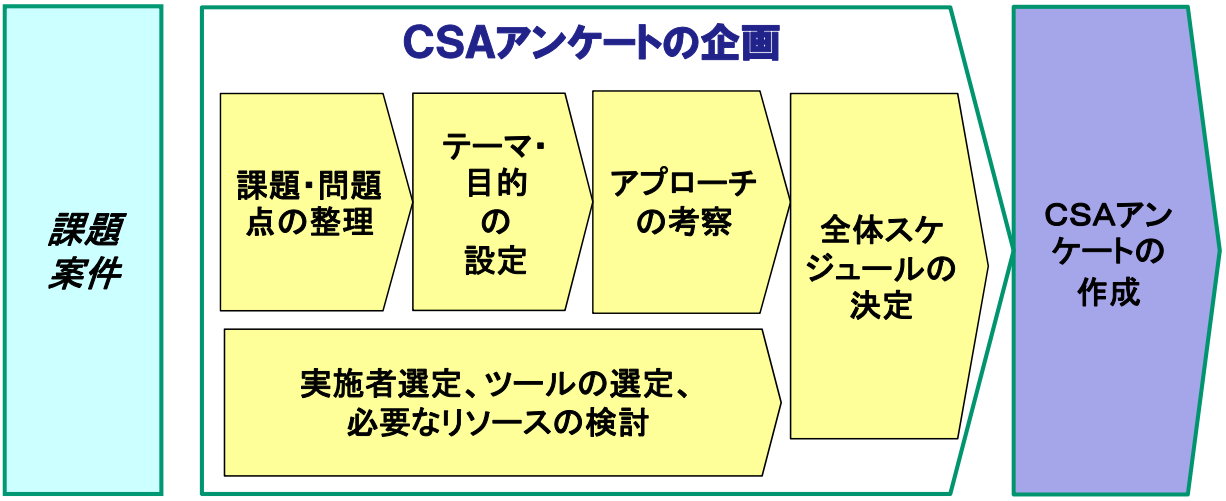
Part Ⅰ CSAアンケートの企画

1. 課題・問題点の整理
2. テーマ・目的の設定
3. アプローチの考察
4. 実施者の選定
5. ツールの選定
6. 必要なリソースの検討
7. 全体スケジュールの決定

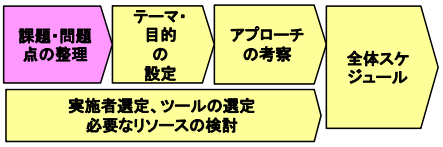
Control Self-Assessment

CSAアンケートの企画

・ 課題やニーズを正確に把握して明確な「目的」「テーマ」を設定しましょう。



課題・問題点の整理－1



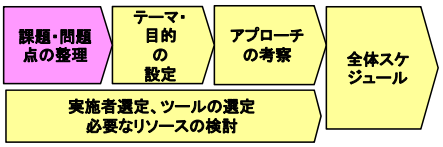
CSAを推進するにあたり、どのような課題や問題があるかを整理します。

《課題の例》

- 経営者から要請された課題・問題点
- 内部監査での識別された課題・問題点
- 現場からの相談等で認識された課題・問題点　など
- 内部統制の課題・問題点の具体的な事例
  - 新たに買収し、子会社となった企業の監査を行いたいが、管理状況が全く分からない
  - 利益率が低迷しており、見積書承認において、利益管理の統制が確実に実施されているかどうか疑わしい。
  - 最近メンタルヘルスで休職する社員が増加しており、各組織での社員の管理が適切に行われているか疑問である。
  - グループ共通の方針を制定したが、各社で方針に沿った管理が行われているかを確認したい。
  - 子会社の情報セキュリティ管理状況にリスクがないかを確認したい。

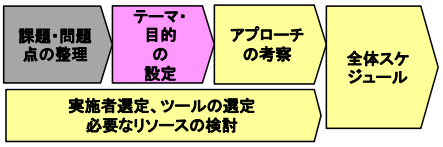
Control Self-Assessment

課題・問題点の整理－2



- 課題を解決するためのツールとしてCSAを利用することについて経営陣や部門の責任者等に説明し、理解とサポートを得ましょう。
- CSAアンケートを成功させるためには、経営陣、責任者のコミットを得ることが重要です。
- CSAを推進する際のステークホルダーは下記の通りです。
  - CSAの報告を受ける経営陣、部門の責任者等のプロセスオーナー
  - CSAの実施者
    - 組織管理者、実務責任者等
  - CSA推進担当事務局
    - リスク管理部門、内部統制推進部門等
    - 内部監査部門

テーマの設定

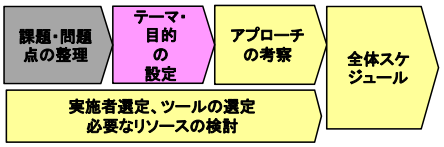


課題・問題点となっている事項について、テーマを設定します。

- テーマを設定する際の観点、留意点
  - どのようなリスクが想定できるか
  - どのようなテーマ・業務に分類されるか
  - そのテーマに関する主管部署はどこか
  - テーマに関する法令、規程、手順書はあるか
  - テーマの事例
    - 労働条件・労働環境
    - 資産管理（固定資産、商品、リース、備品、文書）
    - 教育・人事評価
    - 利益管理、経費管理
    - 法令順守（事業に関連する法令）
    - 業務の有効性・効率性
    - 情報セキュリティ管理

Control Self-Assessment

目的の設定

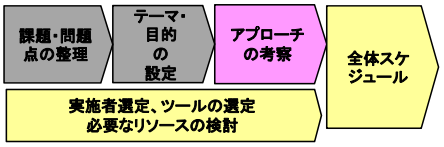


整理された課題・問題点とテーマから、アンケート形式のCSAを実施する目的を設定します。

- 目的の例
  - 重要リスクの抽出／リスクの重要度
  - 残余リスクの状況
  - コントロールの整備状況
  - コントロールの運用状況
  - 改善状況の把握　　など

- 目的を設定する際の留意点
  - 経営者のリスク選好、リスク許容度
  - CSAが機能する組織基盤、土壌を有しているか
    - アンケートに率直に回答する組織風土であるか？
    - 経営者、責任者はアンケート結果を受け入れる姿勢があるか？
  - CSA全体のフレームワークにおけるアンケートの位置付け
    - アンケート単独か、ワークショップとの組み合わせか。
    - アンケートは1回のみか、複数実施するか。

アプローチの考察



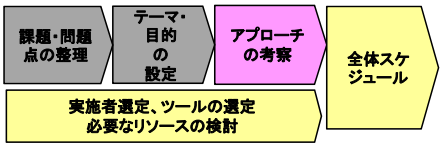
- 実施するCSAの全体の流れを想定し、どのようなアプローチを選択するかを考えます。
  - アプローチの流れ把握（縦軸）
  - アプローチのタイプ把握（横軸）
  - アプローチのゴール把握（何を改善するか）

- 全体の流れの中でアンケートをどこに位置付けるかを明確にします。

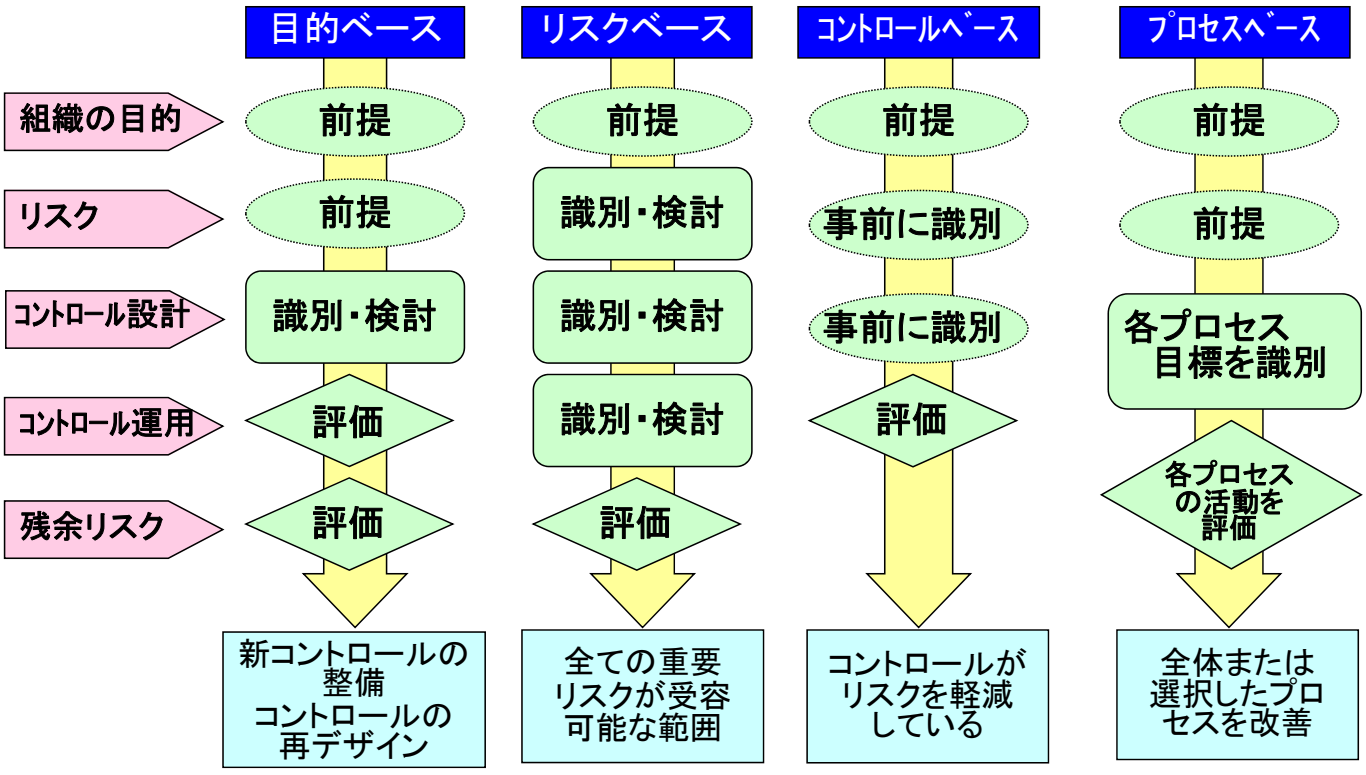
《位置付の例》
  - リスクの洗い出しに活用し、重要なリスクの受容可能性把握
  - リスク状況把握に活用し、以降は別アプローチで対応
  - 整備状況把握に活用し、整備の改善を促す
  - 運用状況把握に活用し、重要な統制の改善を促す
  - 統制の有効性評価に活用し、残余リスクの把握と統制の改善を促す

Control Self-Assessment

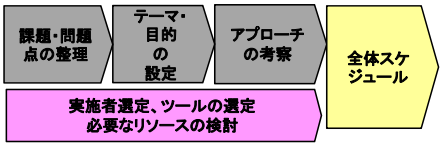
アプローチの事例



アプローチ（AP）のタイプ別活動手順



CSAアンケート実施者の選定



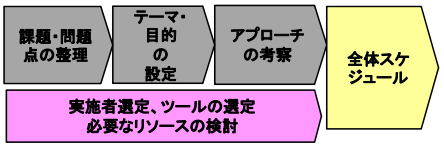
- CSAアンケートの目的、内容、位置付けにマッチした実施者（対象者）を選定しましょう。

《実施者の例》

- 実施企業・実施部門
  - 全企業
  - サンプリングした企業
  - 特定の機能を有する企業
  - 社内全部門
  - 特定の部門
- 実施者
  - 全従業員
  - 特定の階層（経営層/実務責任者（管理職）/実務担当者）
    - 複数の階層を対象
  - 特定の業務の関係者
  - ランダムにサンプリングした者

Control Self-Assessment

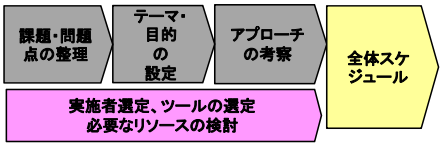
ツールの選定



- ツールの選定
  - Excel・Word
    - 手軽に使え、自由な仕様でアンケートを作り込むことができます。
    - 自ら作成しますので、手間がかかったり、操作に関する知識や技術が必要となる場合があります。
    - 対象の実施者数が多くなると、回収、集計、分析等の手間がかかります。
  - アプリケーション（Webアプリ含む）
    - 回収、集計、分析などが自動でできるため、規模の大きいアンケートでも対応できます。
    - 近年はWebアプリ等で安価に使えるものもありますが、セキュリティ等への留意が必要です。
      - SurveyMonkey
      - DIPSurvey-Free
    - アプリケーションの仕様に従う必要がありますので、思い通りのアンケートができない場合もあります。

Control Self-Assessment

必要なリソースの検討

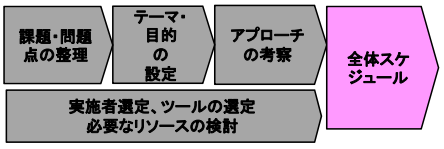


Control Self-Assessment

- CSAアンケートを実施するために必要なリソース（人材、IT環境など）の洗い出しを行いましょう。

《検討ポイント》
- アンケート規模はどの程度となるか。
  - 対象企業、部門、人数他
- 集計作業にかける時間と人員をどの程度になるか。
- どのようなツール（Excel、アプリケーション他）を選定するか。
  - ツールを利用する場合、ノウハウは必要か。
  - 研修・トレーニングの必要性
- 回答の適切性確認に関するフォローをどの程度実施するか。
- 事例や参考となるサンプルはないか。

全体スケジュールの決定



Control Self-Assessment

- 実施するCSAの企画がかたまったら、全体のスケジュールを決定します。
- スケジュールに盛り込む内容（例）
  - アンケート作成期間
  - アンケートの実施時期
    - 実施者への説明会
    - 実施案内
  - アンケート集計・分析期間
  - フィードバック時期
  - 最終報告

Appendix（テンプレート）参照
「CSAアンケート企画書」

Control Self-Assessment

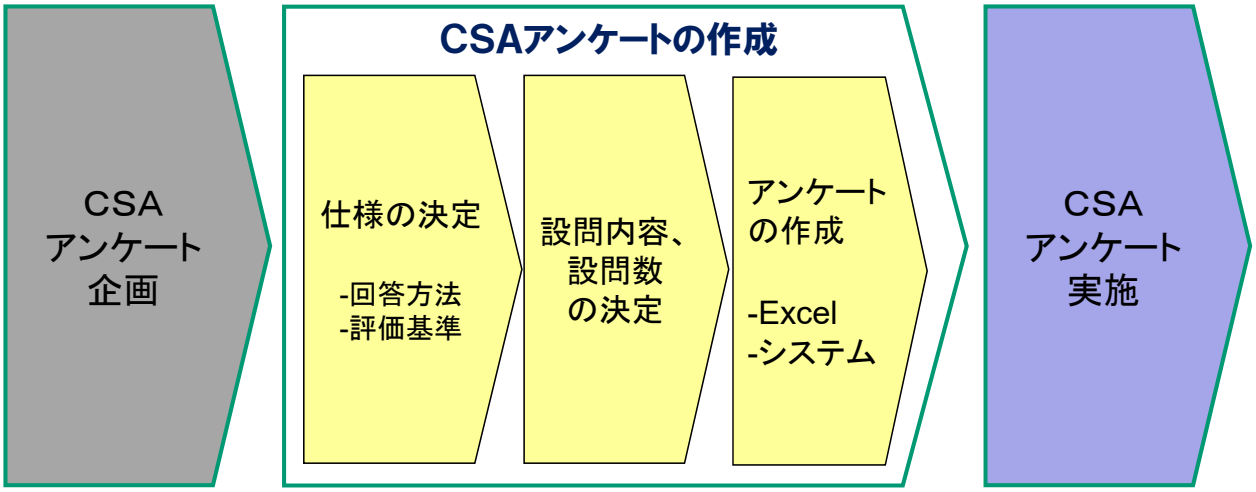
Part Ⅱ　CSAアンケートの作成

１　アンケート仕様の決定
２　アンケートの設問内容、設問数の決定
３　アンケートの作成

Control Self-Assessment

CSAアンケートの作成

・　CSAアンケートの企画段階で計画したことが、適切に実施できるように、アンケートを作成しましょう。



アンケート仕様の決定－1

仕様の決定 → 設問内容設問数の決定 → アンケート作成

アンケートの目的、実施者が決まったら、回答方法、評価基準などのアンケートの仕様を決定します。

《回答方法》-1

実施者にどのような形式で回答してもらうかを決めます。

- 記述式
  - 実施者が質問に対してフリーで記述する形式
    例：自組織のリスクを具体的に記載、自組織の統制上の弱点を具体的に記載等
  - メリット
    - 実施者が自らの言葉で記載するため、納得感がある。
  - デメリット
    - 実施者ごとに書き方が異なるため、集計、分析が難しくなる
    - 実施者にとって、記載が面倒である。

Control Self-Assessment

アンケート仕様の決定－2

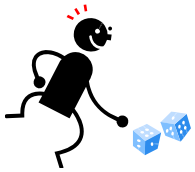
仕様の決定 → 設問内容設問数の決定 → アンケート作成

《回答方法》-2

- 選択式

  あらかじめいくつかの選択肢を用意し、実施者に選択してもらう形式

  〈選択肢の例〉
  - 考えを選ぶ
    - Yes（はい）/ No（いいえ）
    - そう思う/どちらかと言えばそう思う/どちらかと言えばそう思わない/そう思わない
    - 全てある/一部ある/全くない
  - レベルやランクを選ぶ
    - A／B／C
    - 低／中／高
    - 1／2／3／4／5



  - メリット
    - 選択するだけなので、回答が容易／回答が一律なので集計、分析が容易
  - デメリット
    - 一律の回答なので詳細はわからない
    - 実施者がレベルやランクの基準を正しく理解せず、不適切な回答を選択する

Control Self-Assessment

アンケート仕様の決定－3

仕様の決定 → 設問内容設問数の決定 → アンケート作成

《評価基準》

－ 回答の基準（レベル・ランク評価の場合）

・ レベル・ランクの選択式の場合は、レベルやランクの定義を明確しておく必要があります。

・ Yes（はい）／No（いいえ）の場合であっても、どのようなケースがYes（はい）に該当するのかなどを明確にしておく必要があります。

－ 回答の評価

評価の例

・ Yes　1点　No　0点

・ Yesの数でポイント

・ 設問単位のレベル判定

・ 項目単位のレベル判定

・ 総合評価

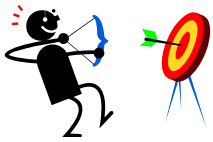
	Yesの数	ポイント
レベルH	6	5
レベルM	5～3	3
レベルL	2～0	0

Control Self-Assessment

設問内容・設問数の決定－1

仕様の決定 → 設問内容設問数の決定 → アンケート作成

- 回答方法、評価基準などのアンケートの仕様が決まったら、具体的な設問内容、設問数を決定します。
- 実施者が回答しやすいようわかりやすい文章にします。
- 実施者によって解釈が変わってしまうことがないように、明確な文章にしましょう。



≪ポイント≫

✓ 5W1Hを意識し、一文の長さを短めに書く

✓ 実施者が馴染みやすい、理解しやすい用語を選定する。

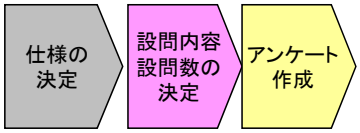
　✓ 専門用語を避け、平易な言葉に置き換える、など工夫も必要です。

✓「対象（誰、どこ、何についての質問なのか）」について明確にする。

✓「時期（過去・現在・未来）」を明確にする。

Control Self-Assessment

設問内容・設問数の決定－2



- **実施者が理解しやすいように、設問を分類したり、流れ（設問の順番）を意識して設問を構成しましょう。**
  - 先に総合的、一般的な質問をした後に、具体的、詳細な内容の質問をするなど、工夫します。

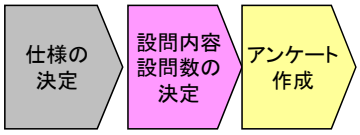
  ≪例≫
  - 設問を2つに分類し、1⇒2の順番で回答するようにする。
    1．整備状況に関する質問
    2、運用状況に関する質問

- **実施者がスムーズに回答に入れるように、簡単な答えやすい質問を最初にします。**
- **実施者がイメージしやすいように数値化できるものは、数値化します。**

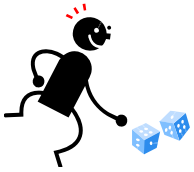
  ≪例≫
  - **頻繁に ⇒ 週2回以上、高額 ⇒ 1000万円以上　など**
- **質問に多くのことを盛り込みすぎないようにします。**
  - 特に一つの質問で2つ以上の内容を聞かないように気をつけます。

Control Self-Assessment

設問内容・設問数の決定－3



- **設問内容を検討する際には、あらかじめ設問数をどのくらいにするかを考えておきましょう。**
  - 厳密に何問と決める必要はありませんが、設問数が多くなりすぎないよう、あらかじめ想定した質問数を意識して設問内容を検討することが必要です。
  - 集計、分析のために項目毎の設問数を揃えた方がよい場合もあります。
- **何問がベストという正解はありませんが、アンケート1回での設問数は30～40問程度が目安と考えられます。**
  - アンケートを企画しているとあれも、これもといろいろ盛り込んでしまい、設問数が多くなりがちですが、思い切って絞ることも大事です。
  - 設問数が多すぎると、実施者のやる気が失われ、回答の精度が低下してしまうケースもあります。
  - 1回のアンケートですべてを評価しようとせずに、複数回の実施、テーマを絞り込むなどの工夫した方が、有用な結果が得られる場合があります。



Control Self-Assessment

アンケートの作成

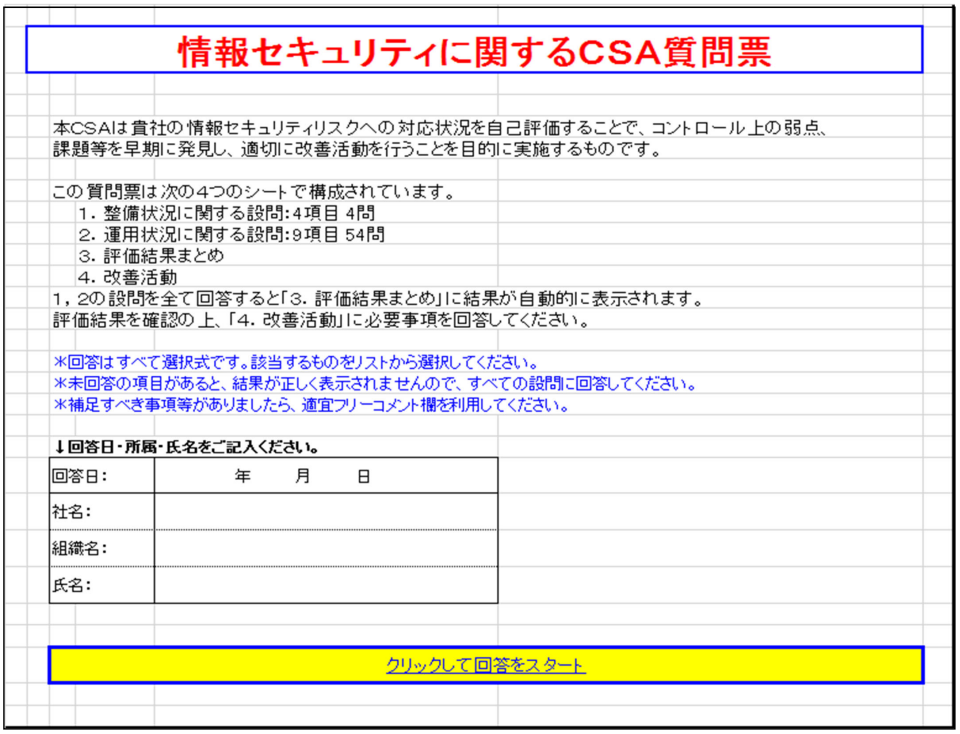
仕様の決定 → 設問内容設問数の決定 → アンケート作成

- アンケートを作成する前に設問内容の一覧表を作り、設問全体の流れ、設問間の整合性等を確認しましょう。

  〈確認内容の例〉
  - 実施者が答えやすい流れとなっているか。
  - 設問が前後しているようなことはないか。
  - 設問間で矛盾していることはないか。
  - 重複する内容となっていないか。
- Excel等で自作する場合は、レイアウト、回答方法等を工夫し、実施者にとって回答しやすく、集計が容易になるようなフォーマットにしましょう。

Control Self-Assessment

CSAアンケート作成事例：Excel File



情報セキュリティに関するCSA質問票

本CSAは貴社の情報セキュリティリスクへの対応状況を自己評価することで、コントロール上の弱点、課題等を早期に発見し、適切に改善活動を行うことを目的に実施するものです。

この質問票は次の4つのシートで構成されています。
1. 整備状況に関する設問:4項目 4問
2. 運用状況に関する設問:9項目 54問
3. 評価結果まとめ
4. 改善活動

1，2の設問を全て回答すると「3. 評価結果まとめ」に結果が自動的に表示されます。
評価結果を確認の上、「4. 改善活動」に必要事項を回答してください。

＊回答はすべて選択式です。該当するものをリストから選択してください。
＊未回答の項目があると、結果が正しく表示されませんので、すべての設問に回答してください。
＊補足すべき事項等がありましたら、適宜フリーコメント欄を利用してください。

↓回答日・所属・氏名をご記入ください。

回答日:	年　月　日
社名:	
組織名:	
氏名:	

クリックして回答をスタート

≪附属資料≫参照
「CSAアンケート雛形（情報セキュリティに関するCSA）」
「CSAアンケートファイル解説」

Control Self-Assessment

Control Self-Assessment

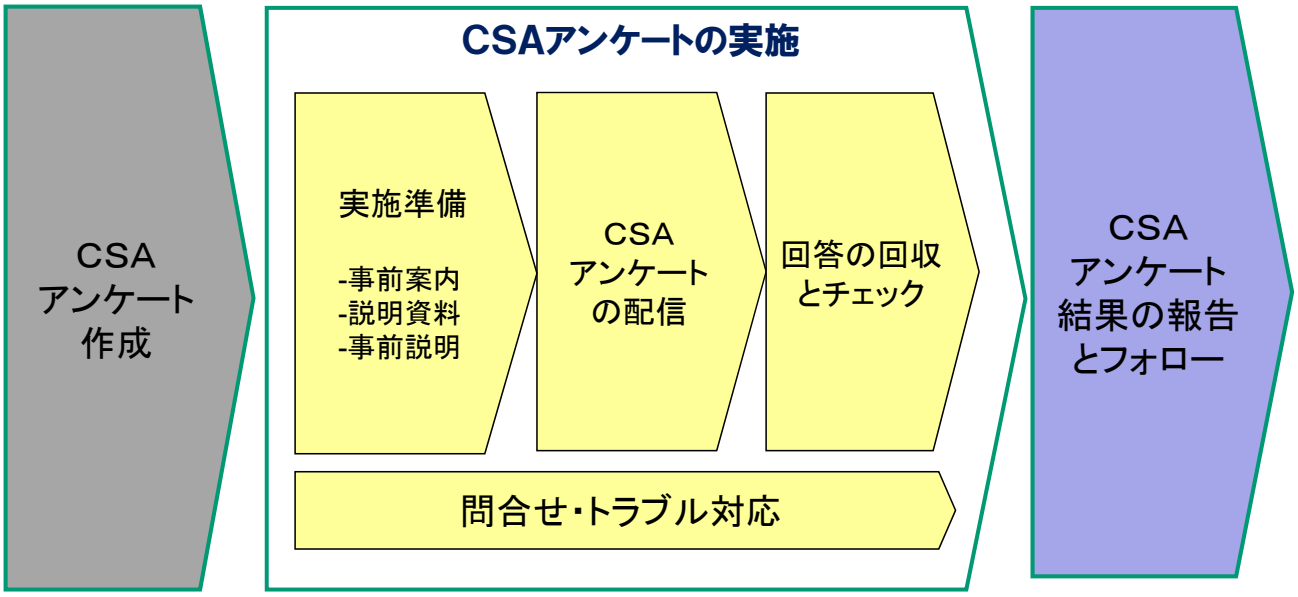
PartⅢ　CSAアンケートの実施

1　実施準備
　事前案内／説明資料／事前説明
2　CSAアンケートの配信
3　回答の回収とチェック
4　問合せ･トラブル対応

Control Self-Assessment

CSAアンケート実施

・　いよいよアンケートの実施です。実施者に趣旨、評価基準等を正しく理解していただき、適切な回答をしてもらうようにしましょう。



実施準備：事前案内（責任者向け）

- CSAアンケートを円滑に行うために、事前に責任者宛に案内（協力依頼）を送付しましょう。
  - 依頼状の項目（例）
    - 目的
      - CSAアンケートの実施目的
    - 依頼事項
      - CSAアンケート対象者
        - 必要なサポート等の依頼
    - スケジュール
      - 事前説明会（実施する場合）
      - アンケート実施時期
      - アンケート集計・分析期間
      - アンケートのフィードバック時期

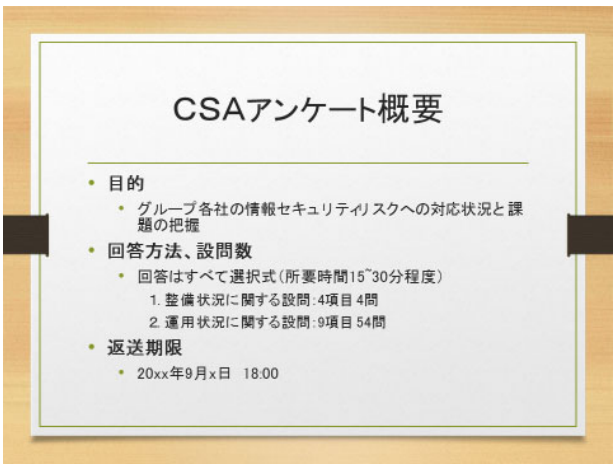
Appendix（テンプレート）参照
「CSAアンケート実施案内（責任者向け）」

Control Self-Assessment

実施準備：説明資料

実施準備 → アンケートの配信 → 回答の回収チェック
問合せ・トラブル対応

- アンケートの目的、回答方法などを実施者に理解していただくために、説明資料を作成しましょう。



Appendix（テンプレート）参照
「CSAアンケート説明用資料」

実施準備：事前説明

実施準備 → アンケートの配信 → 回答の回収とチェック
問合せ・トラブル対応

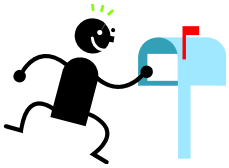
- 初めてCSAアンケートを実施する場合は可能であるならば、事前説明会を実施しましょう。
- アンケートの実施要領に加えて、CSA、リスク、コントロールについても説明しましょう。
- 実施者にアンケートの目的、方法やCSA、リスク、コントロールについて正しく理解していただくことが、質の高い結果やコントールの改善につながります。
  - 複数の階層で実施する場合など、実施者の理解レベルに差がある時は、レベル別に事前説明の内容を変えることも有効です。
- 事前説明として考えられる内容
  - CSAアンケートの目的、実施方法
    - CSAアンケートに期待される効果
    - CSAアンケートに臨む上での注意点
  - リスクとコントロールに関する概説
  - COSO、ERMなどのフレームワークに関する解説
  - リスク、コントロールの事例紹介

Control Self-Assessment

CSAアンケートの配信（実施者向け）

実施準備 → アンケートの配信 → 回答の回収とチェック
問合せ・トラブル対応

- アンケートの実施者に、下記の内容を記載したCSAアンケート依頼状を作成して、配信しましょう。
- 依頼状の項目
  - CSAアンケートのテーマと目的
  - 設問数
    - 設問数に加えて、所要時間の目安なども明記します。
  - 回答期間（回答期限）
    - 期限に間に合わない場合はあらかじめ連絡をいただくよう明記します。
  - 全体スケジュール
    - 報告・フォローアップのスケジュールを含め、CSAアンケートの全体像を提示しましょう。アンケートの期日管理を適切に行うために不可欠な情報です。
  - 問合せ先
    - 問合せ先には、推進部門責任者と担当者（具体的な質問に対応）を記載しましょう。
- 添付ファイル
  - CSAアンケート回答用ファイル（又はアンケートサイトのURL）
  - CSAアンケート用説明資料



Appendix（テンプレート）参照
「CSAアンケート実施案内（実施者向け）」

Control Self-Assessment

回答の回収とチェック－1

Control Self-Assessment

1）回答の回収

－ 適切にリマインド、催促を行い、回答を全件回収するようにしましょう。
- 回答期限の間際になったら、必要に応じて、未回答の方に対してリマインドをするようにします。
- 回答期限を過ぎても未回答な場合は督促を実施します。

－ 未回答者への対応はアンケート企画段階で検討しておきましょう。
- 回答期限の延長はどこまで可能とするか
- 長期不在者への対応（代理回答を認めるかなど）

実施準備 アンケートの配信 回答の回収とチェック
問合せ・トラブル対応

回答の回収とチェック－2

Control Self-Assessment

2）回答のチェック

－ **回収したCSAアンケート回答は集計する前に、個々の回答内容をチェックします。**
- 未回答の設問はないか
- 回答内容、方法は適切か
  - 回答基準に従っていない回答はないか。

－ **未回答の設問がある、回答内容、方法が不適切と思われる場合には、対象となる実施者に確認の上、再回答を求めます。**
- レベル・ランクの選択式の場合は、レベルやランクの定義を正しく理解しないままに回答している場合がありますので、留意が必要です。
- 実施者が評価基準を正しく理解できるよう説明しましょう。

－ **自己評価であっても、評価基準は企画側で設定したものに従うということを実施者に徹底しましょう。**
- 自己評価なので、自分の評価基準で評価してよいと誤解する実施者がいる場合があります。

問合せ・トラブル対応－1

- **実施者から問合せを受けた場合には、丁寧に対応しましょう。**
  - 実施者に適切に回答してもらうため、設問内容、評価基準に関する問合せには丁寧に対応することが大切です。
  - 実施者がアンケート内容、評価基準を正しく理解していないと、アンケートの実施目的を達成することができなくなります。
  - 問合せ対応は、実施者のCSAアンケートへの理解を促すための良い機会となります。
- **問合せ対応において、回答を誘導しないように留意しましょう。**
  - 評価基準に従い、実施者自身が評価することが重要です。
- **万一、トラブルになってしまった場合は、責任者が対応しましょう。**
  - 具体的な対応方法は、状況に応じて決定することになりますが、CSA企画・推進部門の責任者が直接対応することが、円満な解決に繋がることが多いようです。

実施準備 アンケートの配信 回答の回収とチェック
問合せ・トラブル対応

問合せ・トラブル対応－2

- **問合せについては、記録を残すようにします。**
  - 日時、問合せ者、問合せ内容、回答内容、対応者など
  - 問合せは、実施者の理解、意識等を探るのに重要な手掛かりとなります。
  - 実施者が誤解しやすい点などがわかりますので、アンケートのレベルアップに役立てることができます。
- **問合せ記録を実施者への啓発に活かしましょう。**
  - 問合せの多い事項に関しては、FAQ等を作成して実施者へ共有すると実施者の理解を促すことができます。
  - 問合せにより把握した実施者が誤解しやすい点などを資料としてとりまとめて配付する、研修を実施するなど、実施者のCSAアンケートへの理解を深める活動を行いましょう。

Control Self-Assessment

Control Self-Assessment

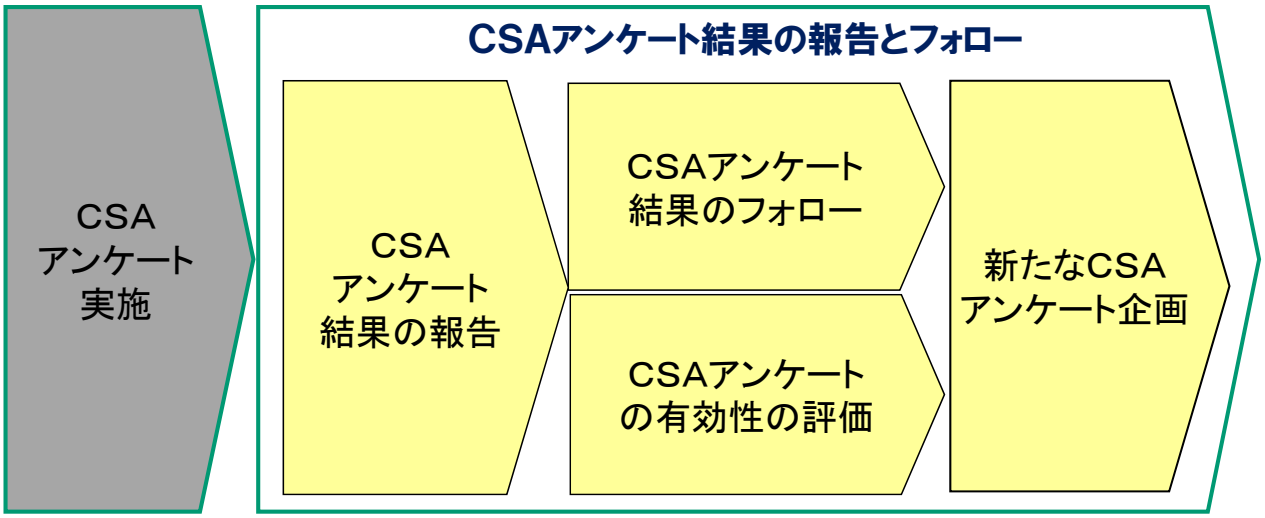
PartⅣ CSAアンケート結果の報告とフォロー

1　CSAアンケート結果の報告
2　CSAアンケート結果のフォロー
3　CSAアンケートの有効性の評価
4　新たなCSAアンケートの企画

Control Self-Assessment

CSAアンケート結果の報告とフォロー

- CSAアンケートの結果を報告書にまとめ、関係者に配付して　改善につなげましょう。
- CSAアンケートの結果をフォローし、改善計画が実施されていることを確認しましょう。
- 実施したCSAアンケートの有効性を評価し、次回以降のCSAアンケートの内容、プロセス等の改善につなげましょう。



CSAアンケート結果の報告－1

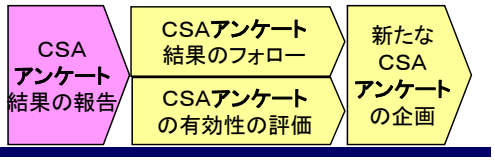
- 報告の責任
  - CSAアンケートの結果は、報告書として対象となった会社の経営陣、部門の責任者等の関係者に報告する必要があります。
  - 次の点に関して、報告する責任があります。
    - ◆ 集計結果と分析
      - ➢ コントロールの状況（整備・運用）
      - ➢ リスクの状況（残余リスク）
    - ◆ 改善のためのアクションプラン
      - ➢ アクションプランが効果的であるためには、下記に留意する必要があります。（SMART）
        - ✓ 具体的であること（Specified）
        - ✓ 効果が測定可能であること（Measurable）
        - ✓ 達成可能であること（Attainable）
        - ✓ 現実的であること（Realistic）
        - ✓ 期限が定められていること（Time-bound）

CSAアンケート結果の報告－2

- 報告の内容
  - 報告書に盛り込む事項には次のようなものがあります。
    - 目的／テーマ
    - アプローチ
    - 実施背景
    - 実施者
    - スケジュール
    - 評価基準
    - 集計・分析結果
      - リスクの状況
      - 内部統制の状況（強み・弱点）
    - 改善のための提言
    - 改善案の実施に当たって考えられる障害
  - 実施したCSAアンケートの目的を達成するために必要な事項を盛り込んで効果的な報告書を作成しましょう。
  - 報告書は一本ではなく、報告先にあわせて複数作成するケースもあります。

Appendix参照
テンプレート:「CSA実施報告書」
アンケート雛形を用いた分析例

CSAアンケート結果の報告－3



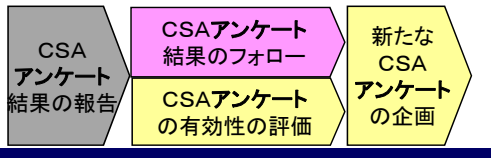
Control Self-Assessment

- CSA実施者へのフィードバック
  - CSAアンケートの集計、分析結果は可能な限り実施者にフィードバックしましょう。
  - 集計・分析結果から得られたリスクの状況、内部統制の状況（強み・弱点）を実施者にフィードバックすることで、組織や部門の改善活動を推進します。
  - リスク、コントロールを評価するだけでなく、その評価結果を改善活動へと繋げることでCSAは有効に機能します。

＜改善活動へのアプローチ方法＞

- CSAアンケート実施時に評価と同時にCSA実施者が改善策を検討する
- CSAアンケート実施後に集計・分析結果をフィードバックした上で、CSA実施者が改善策を検討する
- CSAアンケートで認識された課題について、CSAワークショップを開催し改善策を検討する

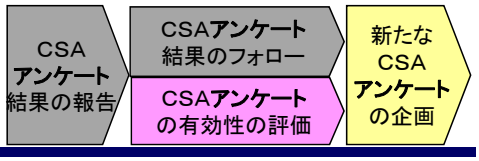
CSAアンケート結果のフォロー



Control Self-Assessment

- CSA企画・推進者は、CSAアンケートの結果をフォローし、改善策が適切に実施または処理されていることを確認する必要があります。
- 一方、内部監査部門はCSA企画・推進を担っているか否かにかかわらず、下記の責任、役割があります。
  - 内部監査部門はCSAの結果をフォローし、提案が適切に実施または処理されていることを検証する責任を負っている。
  - 監査計画ではCSAを通じて識別されたリスクを考慮する必要がある。
  - 内部監査部門はCSAの結果の正確性を検証するためにレビューを実施し、CSAによる改善策の妥当性を確認する。

CSAアンケートの有効性の評価－1



Control Self-Assessment

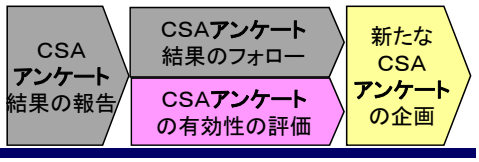
CSAアンケートの実施者、対象となった会社、部門の責任者に対して調査を行い、CSAアンケートの有効性を評価し、改善を図りましょう。

・CSAアンケート実施者への調査

- 実施者がCSAアンケートの目的を理解できたか。
- 実施者が評価基準を理解できたか。
- 関係する主要なリスク、コンロールが適切に取り上げられたか。
- アンケート結果、改善策は、自組織のマネジメントに役立つものなったか。
- 設問数、内容、構成は適切だったか。
- アンケートの仕様は回答しやすいものであったか。
- CSA全般に関する意見、要望他

Appendix（テンプレート）参照
「CSAアンケートに関するサーベイ」

CSAアンケートの有効性の評価－2



Control Self-Assessment

・ CSAの対象となった会社、部門の責任者に対する調査

- CSAアンケートの目的、テーマは適切であったか。
- CSAアンケート結果は、自社、自部門のマネジメントに役立つ情報であったか。
- 主要なリスク、コントロールが適切に取り上げられたか。
- 改善策は識別したリスクの軽減、業務の一層の効率化において、有効であったか。
- 従業員の生産性およびモラールの向上といった点において有効であったか。
- その他CSA全般に関する意見、要望

調査はアンケート又はヒヤリングで実施します。会社、部門の責任者への調査は満足度や要望をより的確に把握するために、ヒヤリングを実施することが望ましいです。

新たなCSAアンケートの企画－1

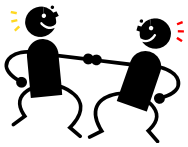
Control Self-Assessment

- CSAアンケートを1回実施しただけでは、その効果は限定的なものになってしまいます。
- リスク、コントロールを自ら評価し改善するというCSAのサイクルを繰り返すことで、実施者のリスク、コントロールへの理解が深まります。
- 実施したCSAアンケート結果を適切にフォローすることに加えて、CSAアンケートの有効性を評価した結果を活かして新たなCSAアンケートを企画しましょう。
- 同じ内容、方法の繰り返しですと、マンネリ化、形骸化する可能性がありますので、定期的に内容、方法を見直して、効果的なCSAアンケートとなるようにしましょう。
  - ワークショップ形式のCSAと組み合わせることも効果的です。

新たなCSAアンケートの企画－2

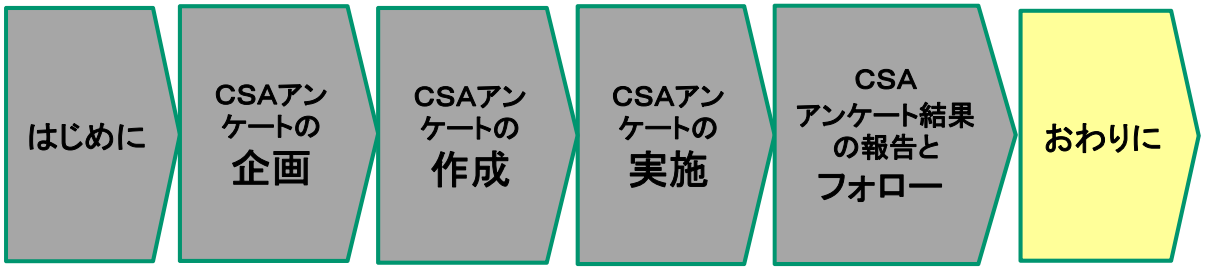
Control Self-Assessment

- CSAアンケートを継続的に実施するために、各回のCSAアンケートの企画からフォローまでのプロセスを適切に実施し、着実に成果を上げていきましょう。
  - 初めてCSAアンケートを実施する場合は、いきなり大規模に実施するのではなく、やりやすいテーマ、部門などを選定したパイロット実施を行い、成果を得るという方法も有効です。
- CSAアンケートの継続的な実施により、CSA実施者、部門の責任者のリスクマネジメントに対する責任感や説明責任の意識も醸成され、組織全体の内部統制レベルの向上につながります。
- CSAアンケートをリスクマネジメントと内部統制の浸透の推進ツールとして繰返し活用し、リスクに強い組織づくりに貢献しましょう。



Control Self-Assessment

おわりに



Control Self-Assessment

おわりに

- 「CSAアンケート・ナビ」を一通り読むことで、CSAアンケートについてご理解いただけましたか？
- CSAアンケートは一見簡単に出来そうに思えますが、効果的に実施するためには、検討すべき事項が多くあります。
- 適切に企画すれば、リスク評価、コントロール評価などを広範囲に効率的に実施することができます。
- まずは「CSAアンケート・ナビ」を参考に、やりやすいテーマでCSAアンケートを企画、実施してみましょう。
- 「CSAアンケート・ナビ」をガイドに効果的なCSAアンケートを実施し、企業、組織に付加価値を与えましょう。

Control Self-Assessment

Appendix

- テンプレート
- アンケート雛形を用いた分析例
- 参考資料

Control Self-Assessment

テンプレート

- CSAアンケート企画書
- CSAアンケート実施案内（責任者／実施者）
- CSA実施報告書
- CSAアンケートに関するサーベイ

CSAアンケート企画書

CSA アンケート 企画書

20xx 年 7 月 x 日

作成： 本社管理本部システム管理部　担当 xx

内部監査部　担当 yy

目的	グループ各社の情報セキュリティリスクへの対応状況と課題を明らかにする
テーマ	対象会社における情報セキュリティコントロールの自己評価
アプローチ	コントロールベースアプローチ
アンケート実施背景	20xx 年 1 月に本社部門別業務監査を実施したところ、デジタル情報の漏洩に関する無視できない残存リスクが確認された。技術・工事本部で貸出用 USB メモリの在庫管理が行われておらず、所在不明な USB メモリがあった。詳細を確認したところ、USB を紛失していたが、個人情報が格納されていないとの理由で、管理本部には報告されなかった。 全社的な大枠のルールは存在していたが、外部記憶媒体（USB メモリなど）の管理は各部門に任されており、技術・工事本部ではルールの整備がなされていないことが根本原因であった。 その後管理本部が 4 月に新ルールを設定したが、同様の問題はグループ会社にも存在することが懸念されるため、まずは各子会社の現場レベルでの状況を把握するとともに、必要な改善を実施することとなった。今回の CSA アンケートはその第一ステップとして、システム管理部と内部監査部と共同でグループ各社の情報セキュリティコントロールの自己評価を行い、残存リスクを各社が自ら把握するためものである。あわせて各社が検討している、または検討すべき改善活動についても自ら把握し、本社に報告して戴く。
メンバー	オーナー　：　本社管理本部長 実施責任者：　本社管理本部システム管理部長／内部監査部長 実施窓口　：　本社管理本部システム管理部 xx　（窓口） 内部監査部 yy 実施担当者：　各グループ会社のシステム責任者
対象	xxx 株式会社　情報システム部　xx 株式会社 xxx　管理グループ xx xxx co., Ltd. General Admin Div.　xx
スケジュール	20xx 年 7 月末まで　アンケート準備、質問対応 20xx 年 8 月 x 日　アンケート実施依頼（責任者・実施者） 20xx 年 8 月 x 日　グループ情報システム連絡会にてアンケートの実施要領説明 20xx 年 9 月 x 日　アンケート回収 20xx 年 10 月 x 日　集計・分析⇒報告書提出

CSAアンケート実施案内（責任者向け）

Control Self-Assessment

xxx 株式会社
CEO　xx 様

CSA アンケート　実施ご協力のお願い

20xx 年 7 月 x 日
本社管理本部本部長　xxx
内部監査部長　xxx

グループ各社の情報セキュリティリスクへの対応状況と課題を把握するとともにグループ全体のセキュリティレベルの向上を企図し、CSA アンケートを実施いたします。つきましては以下のご協力をお願いいたします。

記

1. CSA アンケートの目的
グループ各社の情報セキュリティリスクへの対応状況と課題を明らかにする。

2. 依頼事項
貴社情報システム部長の xx 様をご担当としてアンケートの回答を依頼する予定ですので、あらかじめご了解ください。また、必要なサポート等のご配慮をいただきますようお願いいたします。
なお、ご担当として他の方をご指名いただく場合は、お手数ですが 7 月 x 日までにご連絡いただきますようお願いいたします。

3. 今後のスケジュール
20xx 年 7 月末まで　アンケート準備、質問対応
20xx 年 8 月 x 日　実施者へアンケート依頼状送付
20xx 年 8 月 x 日　グループ情報システム連絡会にてアンケートの実施要領説明
20xx 年 9 月 x 日　アンケート回収
20xx 年 10 月 x 日　アンケート結果集計、分析
20xx 年 11 月以降 各社への結果フィードバック

ご協力のほど、お願い申し上げます。

以上

CSAアンケート実施案内（実施者向け）

xxx 株式会社情報システム部
　xx 様

CSA アンケート　実施のお願い

20xx 年 8 月 x 日
本社管理本部システム管理部 xxx
内部監査部 yyy

貴社 CEO xx 様のご了解をいただきましたので、CSA アンケートにつきご担当いただくこととなりました。以下の要領にしたがい、期限までにアンケートの回答をお送りくださいますようお願いいたします。

記

1. CSA アンケートの目的
　グループ各社の情報セキュリティリスクへの対応状況と課題の把握。

2. CSA アンケート内容・実施
　添付いたしましたアンケートの質問事項にしたがい、貴社の情報セキュリティコントロールの状況に基づき回答欄にご記入ください。
　回答はすべて選択式で、設問数は下記の通りです。回答所要時間は 15～30 分程度です。
　　1．整備状況に関する設問：4 項目　4 問
　　2．運用状況に関する設問：9 項目　54 問
　詳細はアンケートフォームに記載してございます。全項目ご記入されましたら、下記の宛先までご返送ください。
　なお、8 月度のグループ情報システム連絡会にてアンケートの実施要領説明を行いますので、よろしくご出席のほどお願い申し上げます。

3. 返送期限
　20xx 年 9 月 x 日　18:00

4. 返送宛先
　本社情報システム管理部 xx
　　メールアドレス： infosysdiv@xxx.co.jp
　　電話： 03-xxxx-xxxx　（平日 9:00~18:00）
※ 問合せ対応窓口も上記となっておりますので、不明点等ございましたらお問い合わせください。

5. スケジュール
　20xx 年 8 月 x 日　アンケートのお願い送信
　20xx 年 8 月 x 日　グループ情報システム連絡会にてアンケートの実施要領説明
　20xx 年 9 月 x 日　アンケート提出期限
　20xx 年 10 月 x 日　アンケート結果集計、分析
　20xx 年 11 月以降 結果フィードバック

よろしくご協力のほど、お願い申し上げます。

以上

CSAアンケート説明用資料－1

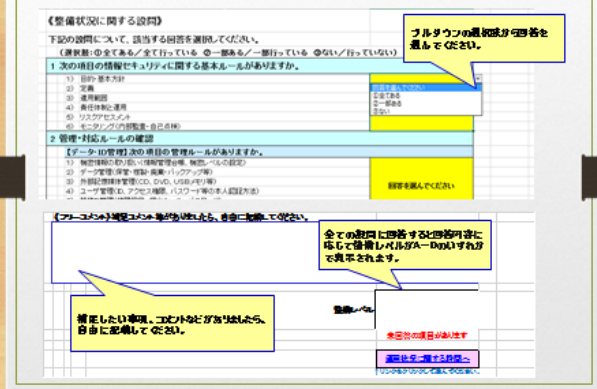
Control Self-Assessment

CSAアンケートの実施について

情報セキュリティリスクへの対応状況

20XX年8月×日
本社管理本部システム管理部
内部監査部

整備状況に関する設問-①

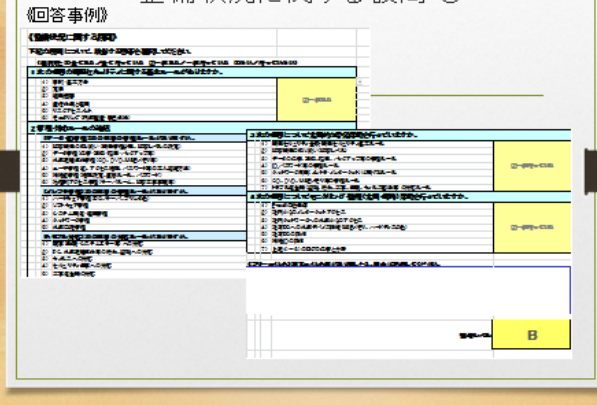


CSAアンケート概要

- **目的**
  - グループ各社の情報セキュリティリスクへの対応状況と課題の把握
- **回答方法、設問数**
  - 回答はすべて選択式(所要時間15~30分程度)
    1. 整備状況に関する設問:4項目　4問
    2. 運用状況に関する設問:9項目　54問
- **返送期限**
  - 20xx年9月x日 18:00

整備状況に関する設問-②

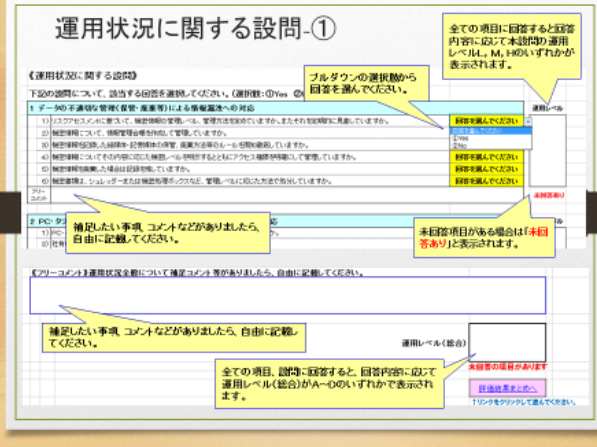
《回答事例》



CSAアンケートファイルの構成

- 表紙
- 整備状況の評価:4項目
- 運用状況の評価:9項目
- 評価結果まとめ
- 改善活動

運用状況に関する設問-①



CSAアンケート説明用資料-2

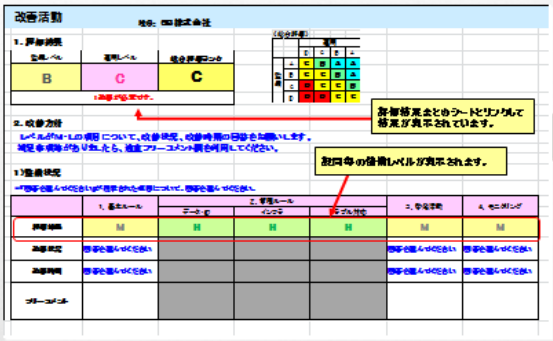
Control Self-Assessment

運用状況に関する設問-②

《回答事例》

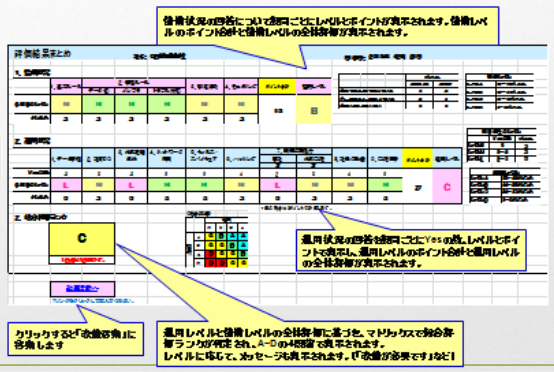
改善活動-①

評価結果がM・Lの項目について、改善状況、改善時期について回答してください。



評価結果まとめ

全ての設問の回答が終わったら、「評価結果まとめ」シートで結果を確認してください



改善活動-②

整備状況と同様に評価結果がM・Lの項目について、改善状況、改善時期について回答をしてください。

総合評価ランク

- 整備レベルと運用レベルのマトリックスで総合評価ランクが判定されます。
- Bランク以下の場合、現状の管理について改善を検討することが必要です。

		運用			
		D	C	B	A
整備	A	C	B	A	A
	B	C	C	B	A
	C	D	C	C	B
	D	D	D	C	C

レベル	コメント
A	問題ありません。
B	改善の余地があります。
C	！改善が必要です。
D	！！早急に改善が必要です。

CSAアンケート窓口

本社システム管理部××

メールアドレス：infosysdiv@xxx.co.jp

電話：03-xxxx-xxxx（平日9:00～18:00）

- ご不明な点等がございましたら、お気軽にお問い合わせください。
- 回答終了後は上記窓口にファイルを返送してください。

CSA実施報告書-1

ＣＳＡ実施報告書

２０××年１月２０日

実施期間：　　２０××年１０月～２０××年１２月
実施担当部署：　本社管理本部システム管理部、内部監査部

１．目　的：グループ各社の情報セキュリティリスクへの対応状況と課題を明らかにする
２．テーマ：対象会社における情報セキュリティコントロールの整備・運用状況の評価
３．対　象：全グループ子会社（１８社）　システム管理部門責任者
４．方法・アプローチ：アンケート方式ＣＳＡ／コントロールベースアプローチ
５．ＣＳＡ実施概要
　１）ＣＳＡアンケートファイル（資料１　参照）
　　設問数：６０（整備状況評価：６　／　運用状況評価：５４（６問×９項目））
　２）説明会
　　システム管理部門責任者連絡会の場で、ＣＳＡ説明会を開催した。
　３）アンケートファイルの送付・提出
　　E-Mail でＣＳＡアンケートと説明資料一式を送付し、記入後のＣＳＡアンケートの返送を依頼し、全件回収した。提出されたＣＳＡアンケートは全て内容を点検し、記入洩れ、評価基準の誤解による誤り等があった場合は再提出を依頼した。

６．評価基準
　１）整備状況評価（整備レベル）
　　回答を下表の基準に従い、ポイント化し、ポイント数に応じ、整備状況のレベルをＡ～Ｄの４段階の判定を行った。

	ポイント	
	設問1,3,4	設問2
①全てある/全て行っている	5	3
②一部ある/一部行っている	3	1
③ない/行っていない	0	0

整備レベル	
レベルA	24～21ポイント
レベルB	20～12ポイント
レベルC	11～6ポイント
レベルD	5～0ポイント

　２）運用状況評価（運用レベル）
　　Yes の数に応じてポイント化し、ポイント数に応じ、運用状況のレベルをＡ～Ｄの４段階の判定を行った。

項目単位のレベル		
	Yesの数	ポイント
レベルH	6	5
レベルM	5～3	3
レベルL	2～0	0

運用レベル	
レベルA	50～45ポイント
レベルB	44～35ポイント
レベルC	34～10ポイント
レベルD	9～0ポイント

1

3）総合評価

総合レベルを整備レベルと運用レベルのマトリックスで評価した。

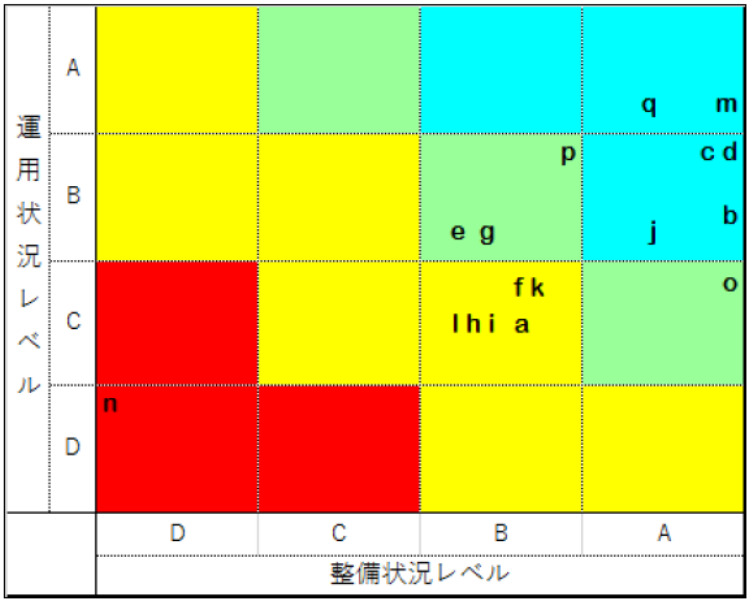
《総合評価》

		運用			
		D	C	B	A
整備	A	C	B	A	A
	B	C	C	B	A
	C	D	C	C	B
	D	D	D	C	C

7．評価結果

1）総合評価

対象 18 社の管理状況の概要は下表の通りであった。1 社を除き整備レベルはＢ以上であり、グループとして一定レベルを確保していると考えられる。しかし、運用状況レベルに関しては、7 社がレベルＣであり、改善が必要である。総合評価Ｄランクの 1 社（ｎ社）については早急な改善が必要である。



2）コントロール状況

項目単位でのコントロールレベルの状況は下記の通りであった。

①整備状況

１社を除き、各項目のルールは一定レベル以上に整備されていた。ただしルールの内容については今後個別に確認を行う必要がある。

項目	回答社数				レベル比率		
	L	M	H	計	L	M	H
1 情報セキュリティに関する基本ルール	1	7	9	17	5.9%	41.2%	52.9%
2 管理・対応ルール							
データ・ID管理ルール	1	5	11	17	5.9%	29.4%	64.7%
インフラ管理ルール	1	6	10	17	5.9%	35.3%	58.8%
トラブル対応ルール	1	4	12	17	5.9%	23.5%	70.6%
3 定期的な啓発活動	1	7	9	17	5.9%	41.2%	52.9%
4 モニタリング・監視（定期・常時）	1	7	9	17	5.9%	41.2%	52.9%

②運用状況

データ管理（保管、廃棄）、情報機器処分時の対応について、レベルＬの比率が高い傾向となり、管理状況に課題が認められた。一方、ネットワーク利用、委託業者管理については、レベルＨが５０％を超えており、比較的高いレベルの管理が行われていた。

レベルＬの比率が高く管理レベルが低いデータ管理、情報機器処分時の対応については、グループとしての対応を検討する必要がある。

項目	回答社数				レベル比率		
	L	M	H	計	L	M	H
1 データの不適切な管理（保管・廃棄等）による情報漏洩への対応	5	5	7	17	29.4%	29.4%	41.2%
2 PC・タブレット・スマートフォン等の盗難、紛失による情報漏洩への対応	2	7	8	17	11.8%	41.2%	47.1%
3 USBメモリ等の外部記憶媒体の盗難、紛失による情報漏洩への対応	2	7	8	17	11.8%	41.2%	47.1%
4 ネットワーク利用による情報漏洩への対応	2	6	9	17	11.8%	35.3%	52.9%
5 社内PCのウィルスやスパイウェア感染による情報漏洩への対応	1	9	7	17	5.9%	52.9%	41.2%
6 ネットワーク上のハッキングによる情報漏洩への対応	1	13	3	17	5.9%	76.5%	17.6%
7 情報機器処分時のデータ消去が不十分だったことによる漏洩	4	14	3	21	19.0%	66.7%	14.3%
【自社で実施】	2	4	1	7	28.6%	57.1%	14.3%
【外部業者へ委託】	2	10	2	14	14.3%	71.4%	14.3%
8 社員の故意による情報漏洩への対応	1	9	7	17	5.9%	52.9%	41.2%
9 委託業者からの情報漏洩への対応	3	4	10	17	17.6%	23.5%	58.8%

８．今後の対応

今回のＣＳＡ結果について、各社へのフィードバックを行うとともに、コントロールレベルの低い項目について、改善の検討を依頼する。

並行して、突出して管理レベルの低いｎ社については、内部監査を実施する。また、管理レベルの低かった項目についても、内部監査の実施を検討する。

（以　上）

CSAアンケートに関するサーベイ-1

Control Self-Assessment

CSAアンケートに関するサーベイ

20xx 年 12 月
本社管理本部システム管理部／内部監査部

ご多忙中のところ、ＣＳＡアンケートにご協力いただき有難うございました。
今後のＣＳＡアンケートの品質向上のための参考にさせていただきますので、以下についてご回答いただきますようお願い申し上げます。

ＣＳＡアンケートテーマ：
回答日：　　年　　月　　日

会社名		部署名		氏 名	

各項目について貴方の考えに最も近いものを選んで下さい。
なお、“③どちらかと言えばそう思わない”または“④そう思わない”を選んだ場合は、お手数ですがコメント欄に具体的な理由のご記入をお願いします。

１．アンケート形式のＣＳＡについて

１）アンケート目的は理解できた。
①そう思う　②どちらかと言えばそう思う　③どちらかといえばそう思わない　④そう思わない
コメント:

２）アンケート期間は適切だった。
①そう思う　②どちらかと言えばそう思う　③どちらかといえばそう思わない　④そう思わない
コメント:

３）アンケートの設問数は適切だった。
①そう思う　②どちらかと言えばそう思う　③どちらかといえばそう思わない　④そう思わない
コメント:

４）アンケートファイルの使い勝手に問題はなかった。
①そう思う　②どちらかと言えばそう思う　③どちらかといえばそう思わない　④そう思わない
コメント:

５）アンケートの設問内容はわかりやすかった。
①そう思う　②どちらかと言えばそう思う　③どちらかといえばそう思わない　④そう思わない
コメント:

1/2

CSAアンケートに関するサーベイ-2

Control Self-Assessment

6）アンケートの設問内容はテーマに対して適切だった。
①そう思う　②どちらかと言えばそう思う　③どちらかといえばそう思わない　④そう思わない
コメント:

7）アンケートの内容はテーマの主要なリスク、コントロールを網羅していた。
①そう思う　②どちらかと言えばそう思う　③どちらかといえばそう思わない　④そう思わない
コメント:

8）アンケートの評価結果、改善策は、自組織のマネジメントに役立つ。
①そう思う　②どちらかと言えばそう思う　③どちらかといえばそう思わない　④そう思わない
コメント:

9）アンケートを通じて、リスク、コントロールの考え方が理解できた。
①そう思う　②どちらかと言えばそう思う　③どちらかといえばそう思わない　④そう思わない
コメント:

2．今回のＣＳＡアンケートで取り上げたリスク以外で重要なリスクがありましたら、具体的にご記入ください。

3．ＣＳＡアンケート全般についてご意見、ご要望などありましたら自由にご記入ください。

（以　上）

ご協力ありがとうございました。

2/2

Control Self-Assessment

アンケート雛形を用いた分析例

Control Self-Assessment

CSAアンケート評価結果概要

評価結果まとめ　　社名：6B株式会社　　回答日：2015年 12月 21日

1. 整備状況

	1. 基本ルール	2. 管理ルール			3. 啓発活動	4. モニタリング	ポイント合計	整備レベル
		データ・ID	インフラ	トラブル対応				
各項目のレベル	M	H	H	H	M	M	18	B
ポイント	3	3	3	3	3	3		

	ポイント	
	設問1,3,4	設問2
①全てある/全て行っている	5	3
②一部ある/一部行っている	3	1
③ない/行っていない	0	0

整備レベル	
レベルA	24～21ポイント
レベルB	20～12ポイント
レベルC	11～6ポイント
レベルD	5～0ポイント

2. 運用状況

	1. データ管理	2. 社有PC	3. 外部記憶媒体	4. ネットワーク利用	5. ウィルス・スパイウェア	6. ハッキング	7. 情報機器処分		8. 社員の故意	9. 委託業者	ポイント合計	運用レベル
							自社	外部委託				
							有	有				
Yesの数	3	5	3	6	6	4	2	5	4	6	27	C
各項目のレベル	L	M	L	H	H	M	L	M	M	H		
ポイント	0	3	0	5	5	3	0	3	3	5		

＊無の場合は5ポイントで計算します。

項目単位のレベル		
	Yesの数	ポイント
レベルH	6	5
レベルM	5～3	3
レベルL	2～0	0

運用レベル	
レベルA	50～45ポイント
レベルB	44～35ポイント
レベルC	34～10ポイント
レベルD	9～0ポイント

2. 総合評価ランク

C

！改善が必要です。

《総合評価》

整備＼運用	D	C	B	A
A	C	B	A	A
B	C	C	B	A
C	D	C	C	B
D	D	D	C	C

改善活動へ

↑リンクをクリックして進んでください。

- 雛形のCSAアンケートを実施すると実施者毎に上記のような結果が得られます。
- この評価結果を集計し、リスク、コントロールの状況を分析することができます。

Control Self-Assessment

集計・分析サンプル①

- 「総合評価まとめシート」をそのまま活用し、会社別・項目別の一覧表で報告を行う。
- 項目数や会社数が多くない場合は、この方法が効率的である。

《整備状況に関する設問》

全てある(全て行っている):1　一部ある(一部行っている):2　ない(行っていない)

	A社	B社	C社	D社	E社	F社	G社	H社	I社	J社	K社	L社	M社	N社	O社	P社	Q社
1 情報セキュリティに関する基本ルール	M 3	H 5	H 5	H 5	M 3	H 5	H 5	M 3	M 3	H 5	M 3	M 3	H 5	L 0	H 5	M 3	H 5
2 管理・対応ルール																	
データ・ID管理ルール	H 3	H 3	H 3	H 3	M 1	M 1	M 1	M 1	H 3	H 3	H 3	M 1	H 3	L 0	H 3	H 3	H 3
インフラ管理ルール	H 3	H 3	H 3	H 3	M 1	M 1	M 1	M 1	M 1	H 3	H 3	M 1	H 3	L 0	H 3	H 3	H 3
トラブル対応ルール	H 3	H 3	H 3	H 3	M 1	H 3	M 1	H 3	M 1	H 3	H 3	M 1	H 3	L 0	H 3	H 3	H 3
3 定期的な啓発活動	M 3	H 5	H 5	H 5	H 5	M 3	H 5	M 3	M 3	H 5	M 3	M 3	H 5	L 0	H 5	H 5	M 3
4 モニタリング・監視(定期・常時)	M 3	H 5	H 5	H 5	M 3	H 5	M 3	M 3	H 5	M 3	H 5	M 3	H 5	L 0	H 5	M 3	H 5
整備レベル／ポイント計	B 18	A 24	A 24	A 24	B 14	B 18	B 16	B 14	B 16	A 22	B 20	B 12	A 24	D 0	A 24	B 20	A 22

《運用状況に関する設問》

Yes:1　No:0

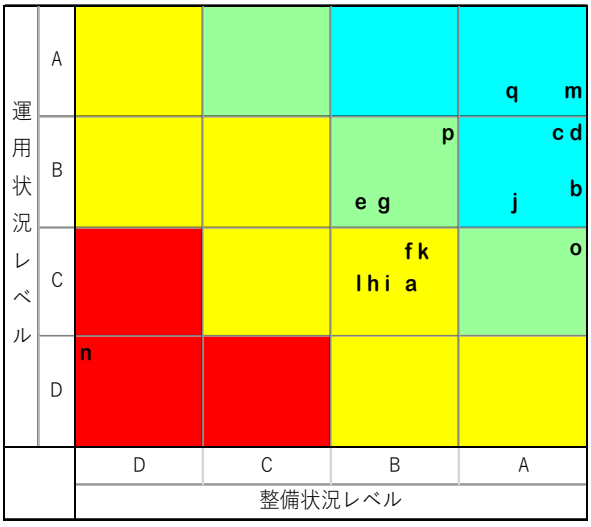
	A社	B社	C社	D社	E社	F社	G社	H社	I社	J社	K社	L社	M社	N社	O社	P社	Q社
1 データの不適切な管理(保管・廃棄等)による情報漏洩への対応	L 0	H 5	H 5	H 5	H 5	M 3	H 5	L 0	L 0	M 3	M 3	L 0	H 5	L 0	M 3	M 3	H 5
2 PC・タブレット・スマートフォン等の盗難、紛失による情報漏洩への対応	M 3	H 5	H 5	M 3	M 3	M 3	L 0	H 5	M 3	M 3	M 3	H 5	H 5	L 0	H 5	H 5	H 5
3 USBメモリ等の外部記憶媒体の盗難、紛失による情報漏洩への対応	L 0	M 3	H 5	H 5	H 5	H 5	M 3	M 3	M 3	M 3	H 5	M 3	H 5	L 0	M 3	H 5	H 5
4 ネットワーク利用による情報漏洩への対応	H 5	H 5	H 5	H 5	M 3	L 0	M 3	M 3	M 3	M 3	H 5	H 5	H 5	L 0	M 3	H 5	H 5
5 社内PCのウィルスやスパイウェア感染による情報漏洩への対応	H 5	M 3	M 3	H 5	L 0	H 5	M 3	H 5	M 3	M 3	M 3	M 3	H 5	M 3	M 3	H 5	H 5
6 ネットワーク上のハッキングによる情報漏洩への対応	M 3	M 3	M 3	M 3	H 5	H 5	M 3	M 3	M 3	M 3	M 3	M 3	H 5	L 0	M 3	M 3	M 3
7 情報機器処分時のデータ消去が不十分だったことによる漏洩																	
1)情報機器を処分する際、データ消去を自社で行っていますか？	①Yes	①Yes	①Yes	②No	②No	②No	②No	①Yes	②No	②No	②No	②No	②No	①Yes	①Yes	②No	①Yes
【自社で実施】	L 0	M 3	H 5	N/A 5	N/A 5	N/A 5	N/A 5	M 3	N/A 5	N/A 5	N/A 5	N/A 5	N/A 5	L 0	M 3	N/A 5	M 3
2)情報機器を処分する際、データ消去を外部業者に委託していますか？	①Yes	①Yes	①Yes	①Yes	①Yes	①Yes	①Yes	②No	①Yes	①Yes	①Yes	①Yes	①Yes	②No	①Yes	①Yes	②No
【外部業者へ委託】	M 3	M 3	H 5	M 3	M 3	L 0	H 0	N/A 0	M 0	M 3	L 0	M 3	M 3	N/A 5	M 3	M 3	N/A 5
8 社員の故意による情報漏洩への対応	M 3	H 5	M 3	H 5	H 5	H 5	M 3	M 3	M 3	H 5	M 3	M 3	M 3	L 0	M 3	H 5	H 5
9 委託業者からの情報漏洩への対応	H 5	H 5	H 5	H 5	M 3	M 3	H 5	L 0	M 3	H 5	M 3	L 0	H 5	L 0	H 5	H 5	H 5
運用レベル(総合)	C 27	B 40	B 44	B 44	B 37	C 34	B 35	C 30	C 29	B 36	C 33	C 30	A 46	D 8	C 34	B 44	A 46
	BC	AB	AB	AB	BB	BC	BB	BC	BC	AB	BC	BC	AA	DD	AC	BB	AA
総合評価	C	A	A	A	B	C	B	C	C	A	C	C	A	D	B	B	A

B:35～44ポント

Control Self-Assessment

集計・分析サンプル②

- レベル(運用状況・整備状況)をリスクマトリックス化し、全体の状況を俯瞰する。



ランク	総合評価		
A	6社	管理レベル高	低リスク
B	4社	管理レベル中の上	中リスク1
C	6社	管理レベル中の下	中リスク2
D	1社	管理レベル低	高リスク

所見

- 対象17社の管理状況の概要は表の通りである。
- 1社を除き整備レベルはB以上であり、グループとして一定レベルを確保していると考えられる。
- 運用状況レベルは7社がCであり、改善が必要である。
- 総合評価Dランクの1社については早急な改善が必要である。

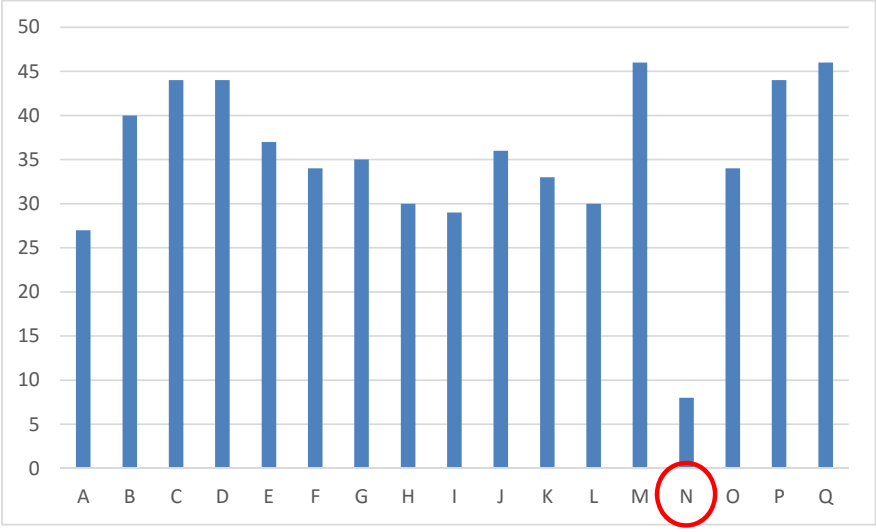
会社名	a社	b社	c社	d社	e社	f社	g社	h社	i社	j社	k社	l社	m社	n社	o社	p社	q社
整備	18	24	24	24	14	18	16	14	16	22	20	12	24	0	24	20	22
運用	27	40	44	44	37	34	35	30	29	36	33	30	46	8	34	44	46

Control Self-Assessment

集計・分析サンプル③

- 各会社の総合評価を横並びにして、報告書を作成する。
- 各会社のITセキュリティの管理レベルを、経営陣が迅速に確認できる。

会社別の総合評価データ



所見

- 管理レベルが高評価（35点以上）は、10社。
- 管理レベルが中評価（10点～34点）は、6社。
- 管理レベルが低評価は1社。N社である。早急に改善方針の提出を求める必要がある。

Control Self-Assessment

集計・分析サンプル④

- 個社ごとに報告書を作成する。
- 詳細を確認したい会社に対しては、アンケート項目別の分析を行う。

A社の個社データ

所見

- 基本ルールの未設定、管理対応ルールの未設定といった、ITコントールの整備状態に問題がある。
- PC廃棄や外部情報媒体の使用に関するルールが無く、ITアセットの管理状態は特に問題である。

Control Self-Assessment

参考資料

Control Self-Assessment

CSAの定義

- CSA (Control Self-Assessment)とは
  - 業務に責任を持つ者が内部統制の有効性を検証し、評価するプロセスである。

CSA(Control Self-Assessment:統制自己評価)とは

- 内部統制の有効性が検証され、評価されるプロセスである。この目的とは、すべてのビジネス目的が達成されるであろうという合理的な保証を与えるものである。(IIA、1998年)
- 正式に文書化されたプロセスでビジネス機能に直接関与する経営者やワークチームが、
  - 稼働しているプロセスの有効性を判断し、かつ
  - いくつかの(または全ての)ビジネス目的達成の機会が合理的に保証されているかどうかを判定する。(IIA、1995年)

《出典:統制自己評価ガイド/CCSA資格認定試験スタディガイド》

Control Self-Assessment

CSAの目的

- CSAの目的
  - 経営目標の達成に対する合理的な保証の付与
  - 内部監査への価値の付加
  - 業務担当部門の関与を高めることでの価値の付加

- その他の名称；
  - Control/Risk Self-Assessment (CRSA)
  - Management Self Assessment
  - Risk and Control Self-Assessment (RCSA)
  - Business Self Assessment

《出典：CCSA資格認定試験スタディガイド》

Control Self-Assessment

CSAの歴史

- CSAは1980年代後半、Gulf CANADA（カナダのエネルギー会社）の内部監査チームが開発した手法と言われています。
  - 従来のインタビュー方式より、各部のマネージャー、業務スタッフを集め、ワークショップを行う方が質の高い情報と効果が得られることを発見しました。
  - 内部統制の有効性と組織の業務プロセスを把握、評価するために活用されました。
  - ワークショップの手法を体系化し、10年間で500回以上のワークショップを実施しました。
- CSAは、1990年代に欧米の内部監査部門の内部統制評価ツールとして、普及しました。
- IIAや内部監査人達により情報交換、研究され、CSA実施を支援するための試験と資格であるCCSAの確立にまで発展しました。

《出典：月刊監査研究　2008.8　No.411　CSA（コントロール・セルフアセスメント）と内部監査》

CSA資料集

・ http://www.iiajapan.com/data/CSA_TOP.html

「CSAアンケート・ナビ」検討・作成メンバー

CIAフォーラム研究会 No. d2
CSA実践研究会

森 康裕、佐藤亜紀、板本正夫、小林啓嗣、山崎伸子
岡田 勝、徳野誠一、坂東英明、小平幸秀、荒雄一郎
西面隆弘、平田 肇、犬塚伸司、後藤恵子（座長）

《順不同》

「CIAフォーラム」は、CIA資格保持者の研鑽および相互交流を目的に活動する、社団法人日本内部監査協会（IIA-JAPAN）の特別研究会である。各研会は、担当の座長が責任をもって自主的に運営し、研究期間、目標成果を設定し、研究成果を発信している。

本資料は、CIAフォーラムNo.d2 CSA実践研究会が、その活動成果として取りまとめたものである。資料に記載された意見やコメントは、研究会の「見解」であり協会の見解を代表するものではなく、協会がこれを保証・賛成・推奨等するものでもない。