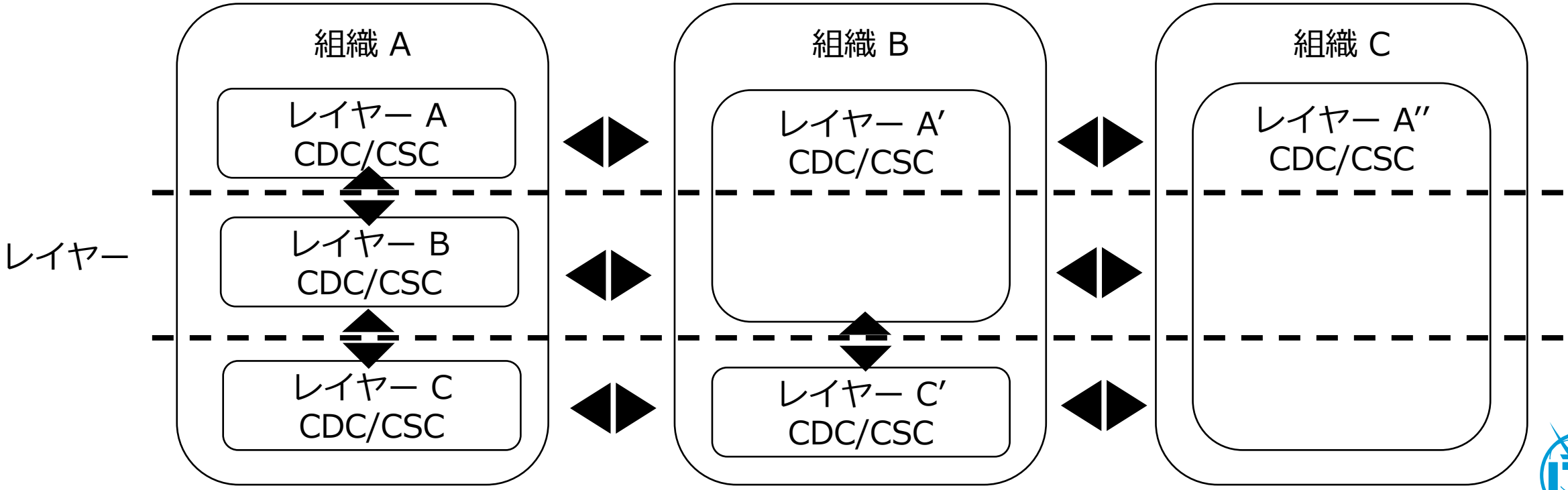
# ITU-T X.1060
# チュートリアル

# なぜX.1060を利用するのか？

# 共通言語として

- サイバーセキュリティに関して幅広く誰もが使える共通の言語である
- ベストプラクティスとしてセキュリティサービスを体系化して列挙している

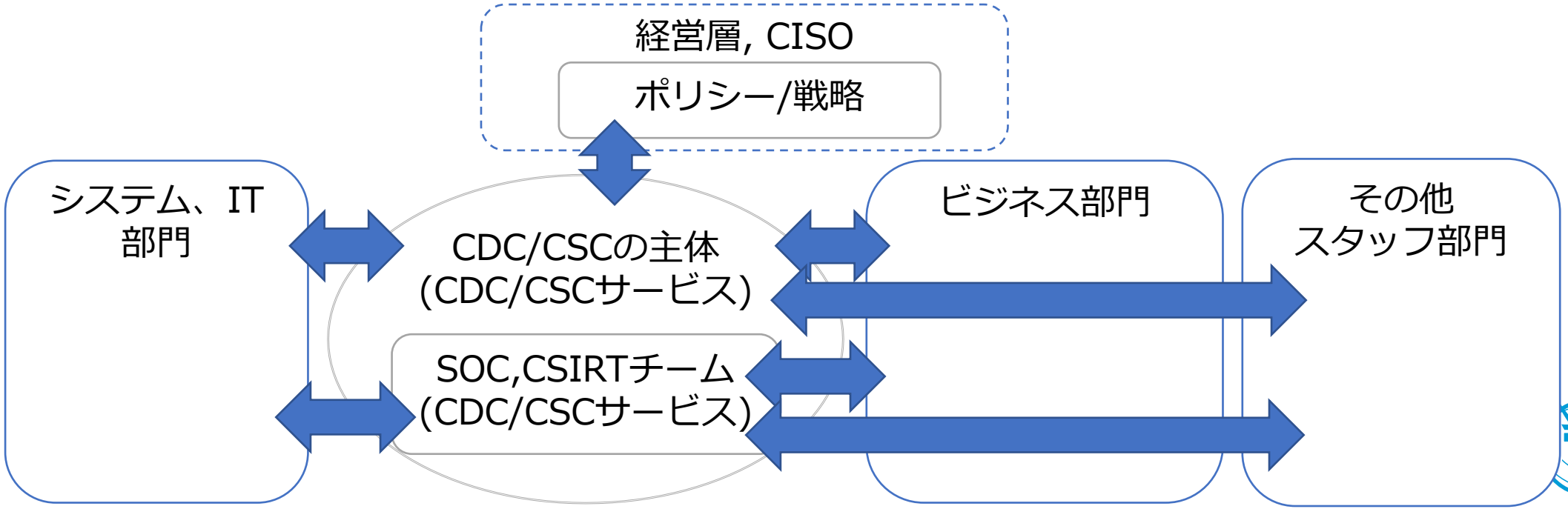


# CDC/CSC = 既存の組織を包含する幅広いコンセプト

- CDC/CSCは新たなコンセプトを示している
- しかしながら、新しい組織ではなく、既存の機能によって実現されうる
- すでにX.1060のサービスがあり、関連する組織が一緒に動いているなら、CDC/CSCがあると言える
- **CDC/CSCはCSIRTやSOCを含む幅広いコンセプトで、それらをサービスの一部として含んでる**
- CDC/CSCのコンセプトは、情報システム部だけではない、サイバーインシデントの幅広い影響に対応するための組織において重要になっている。

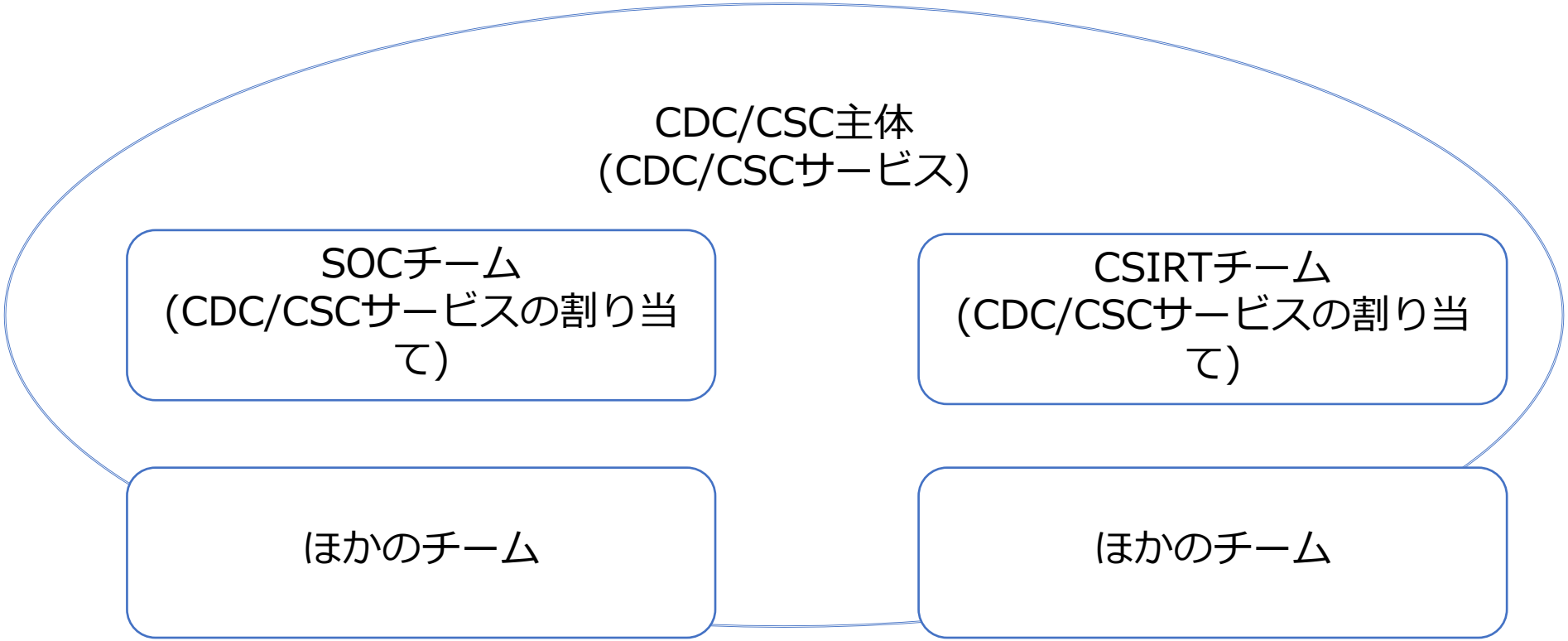
# CDC/CSCはビジネスリスクに対応するセキュリティサービスを提供する

- サイバーセキュリティは重要なビジネスリスクの一つとして考えられている
- サイバーセキュリティのリスクを取り扱うために、既存のSOC, CSIRT, CIRTだけではなく、幅広いセキュリティサービスが必要である。



# セキュリティサービスを受け持つチームはSOCやCSIRTと呼ばれていることもある

- 組織にすでにSOCやCSIRTがあり、CDC/CSCのサービスを実装しているなら、CDC/CSCの一部を実装していると考えられる



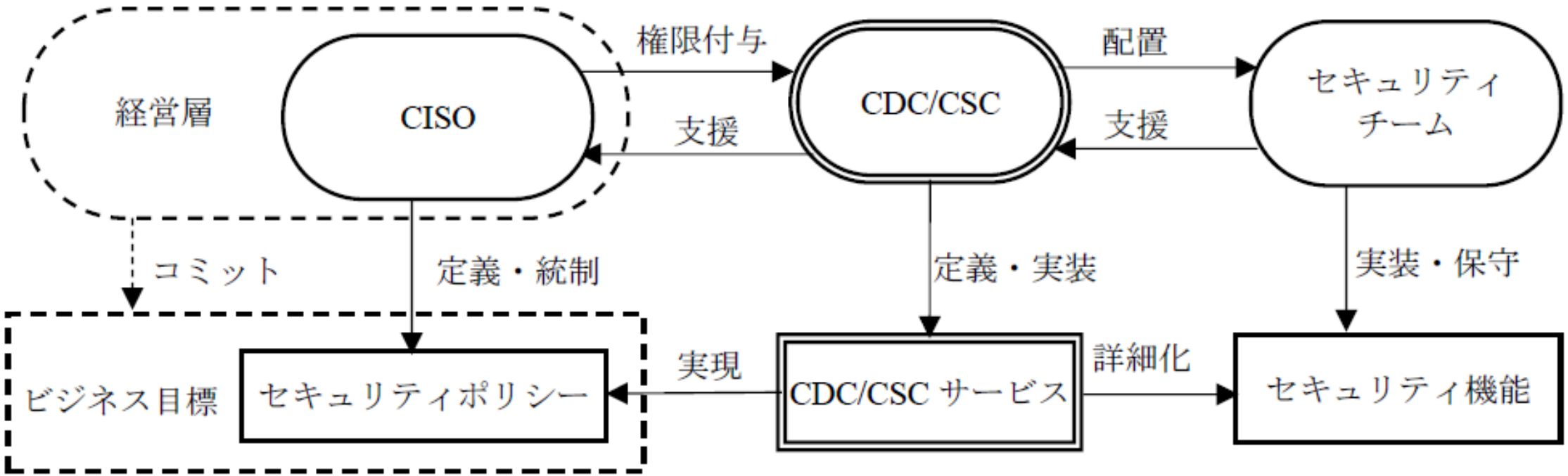
# ITU-T勧告X.1060の概要
# CDC/CSCとは?

# X.1060

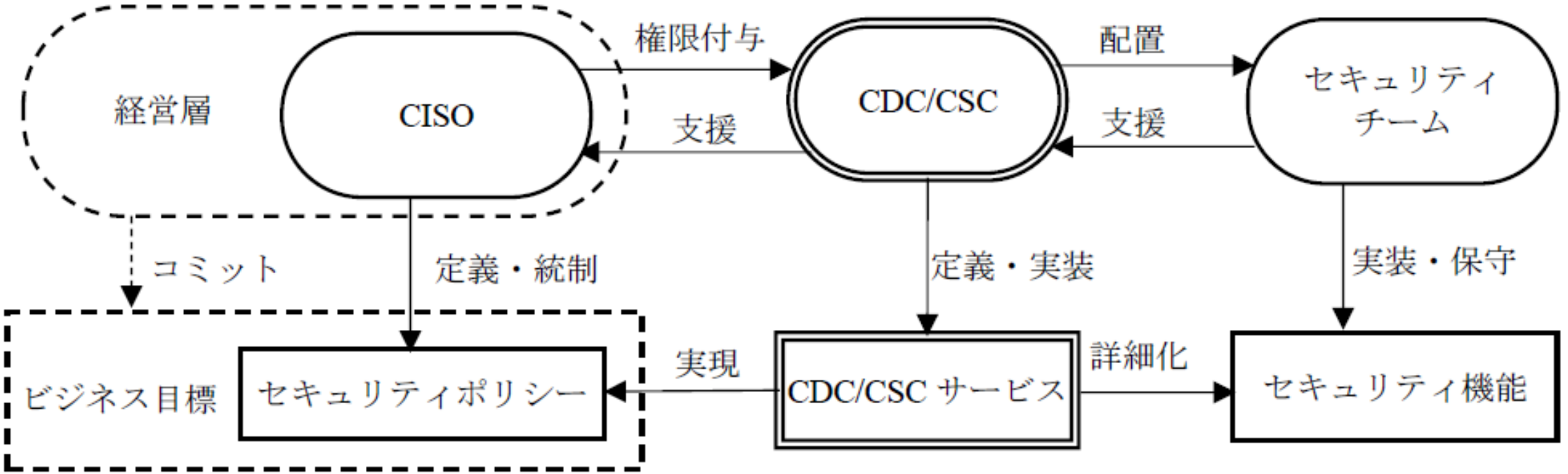
- タイトル
  - **サイバーディフェンスセンター/サイバーセキュリティセンターを構築・運用するためのフレームワーク**
- 規定範囲
  - X.1060は、組織がサイバーディフェンスセンター/サイバーセキュリティセンター(CDC/CSC)を構築、マネジメントするとともに、その有効性を評価するためのフレームワークを提供するものである。このフレームワークは、組織のセキュリティを実現するために、CDC/CSCがどのようにセキュリティサービスを決定し、実施すべきかを示している
  - この勧告は、最高セキュリティ責任者(CSO)や最高情報セキュリティ責任者(CISO)など、組織のセキュリティの責任を持つ経営幹部レベル、およびそれを補佐するセキュリティ管理者を対象としている

# 「サイバーディフェンスセンター/サイバーセキュリティセンター(CDC/CSC)」とは何か？

- 定義
  - CDC/CSCは組織において、ビジネス活動におけるサイバーセキュリティリスクを管理するためのセキュリティサービスを提供する主体



# 組織におけるCDC/CSC




| | | | |
|---|---|---|---|
| 経営層は事業の目的にコミットする | CISOはサイバーリスクの管理のためにセキュリティのポリシーを定義してコントロールする | CDC/CSCはCISOにより権限移譲され、セキュリティポリシーの実現にむけてCDC/CSCサービスを定義して実装する | CDC/CSCはCDC/CSCサービスを構成するセキュリティの機能を実現するためにリソースを割り当てる |

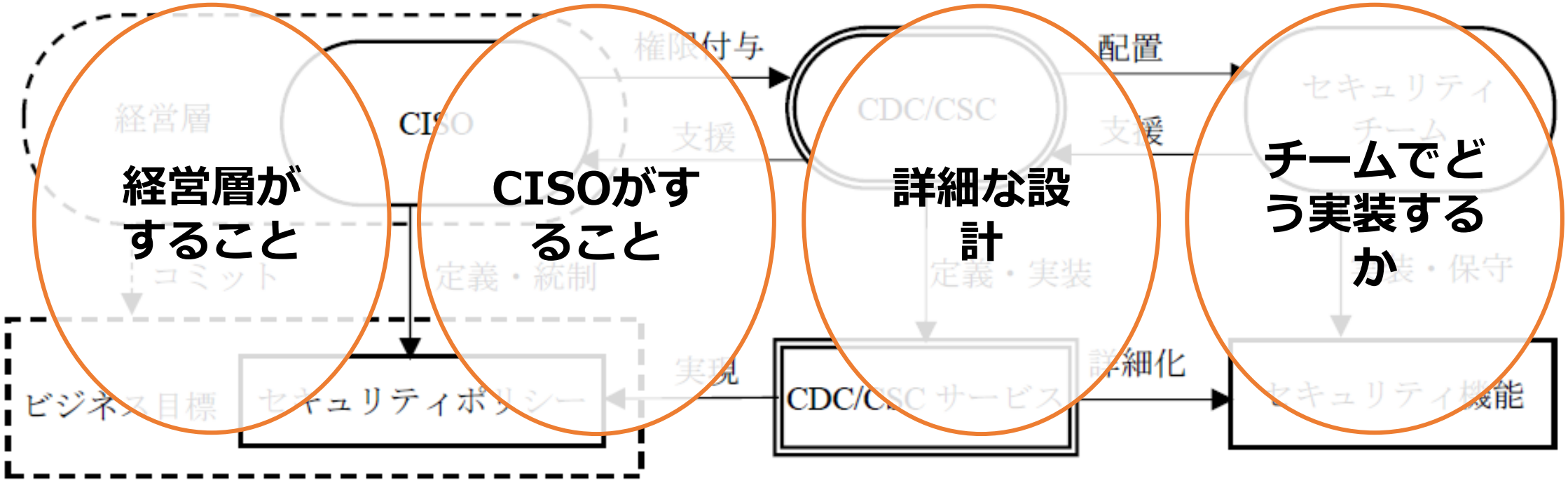
# CDC/CSCは主体であり、組織によって名前や形は様々である

- 「CDC/CSC」といった名前の組織やユニットを設けることが目的ではない。名前はそれぞれの組織により様々である
- どのようにセキュリティサービスを実装するかによるものであり、CDC/CSCの名前や形態は組織の中で様々である

# X.1060はフレームワークのみを提供している

- X.1060はCDC/CSCを構築・運用するためのフレームワークだけを提供している
- 組織において、実際にCDC/CSCサービスを実装するためには、既存の様々なドキュメントを活用することが必要である

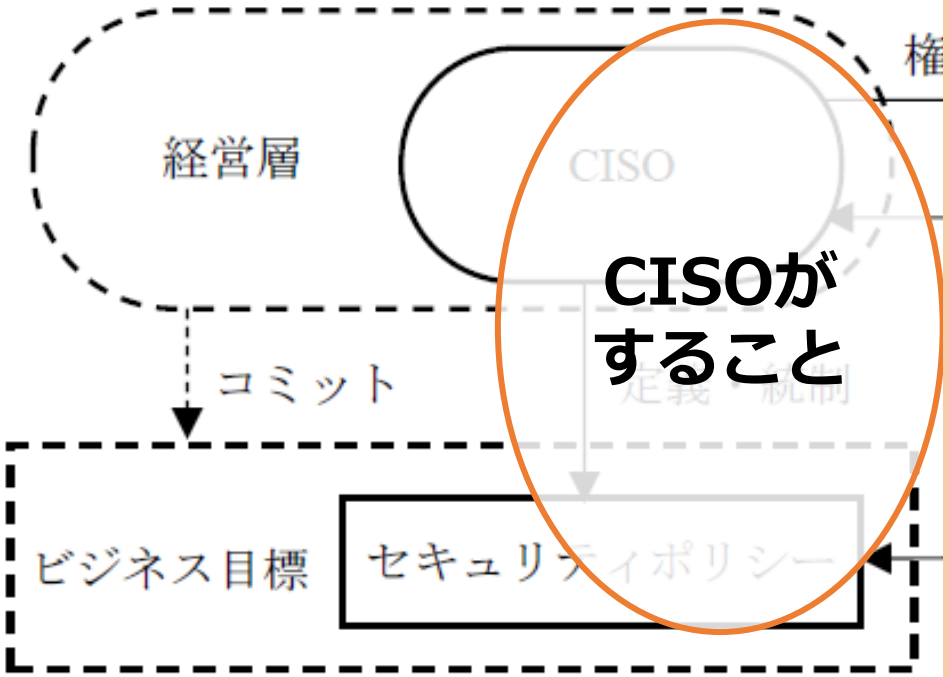
# X.1060に書かれていないこと



# X.1060に書かれていないこと


X.1060には経営層が何をするかは示していない
- サイバーセキュリティの重要性を認識する
- CISOを選任する
- CISOに明確な指示を行う
- CDC/CSCの設置を決定する

# X.1060に書かれていないこと

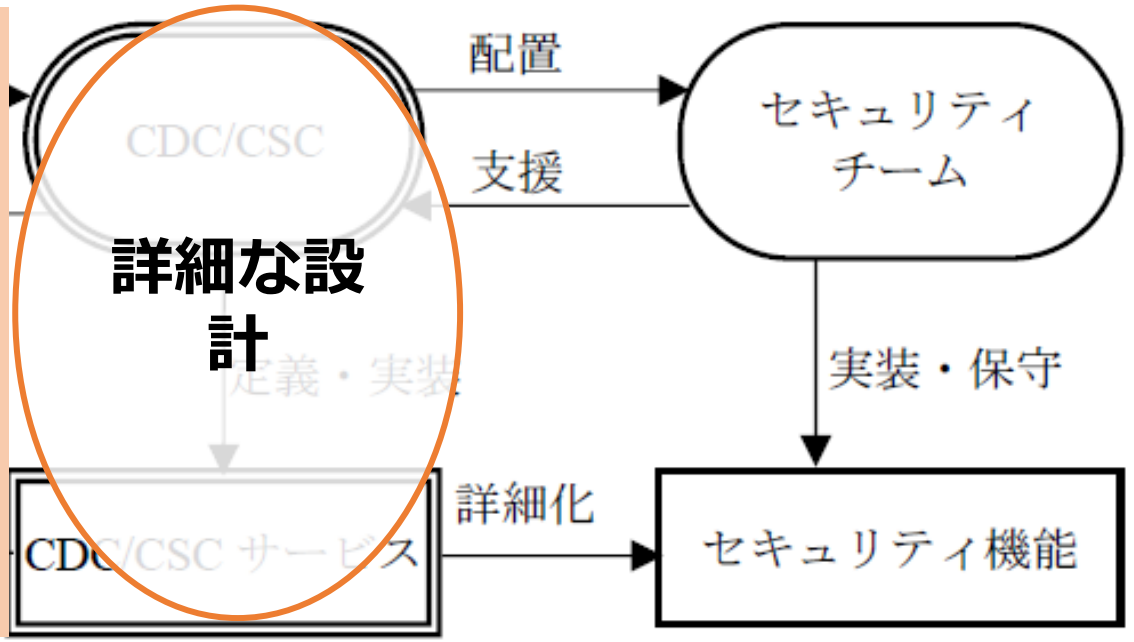



X.1060はCISOが何をするかは示していない

- 以下の2点からセキュリティポリシーを決定すること
  - 組織のビジネス環境やビジネスの目的を考慮する
  - 経営層からの指示
- CDC/CSCの設立について経営層へ啓発して推進する

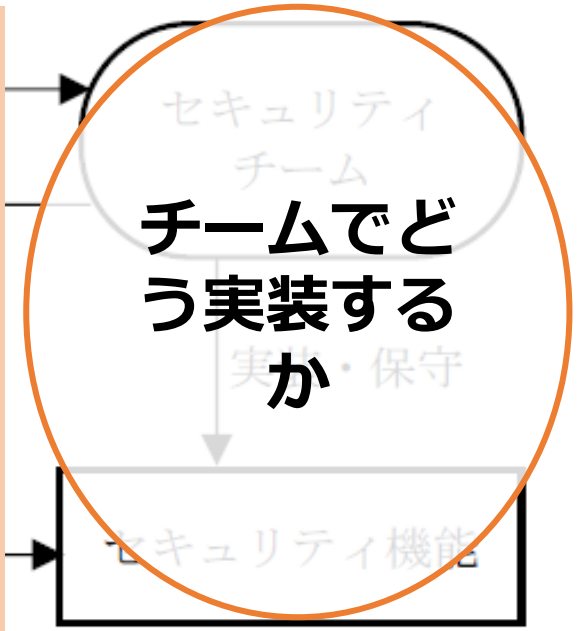
# X.1060に書かれていないこと

X.1060はそれぞれの組織におけるCDC/CSCの詳細な設計は示していない



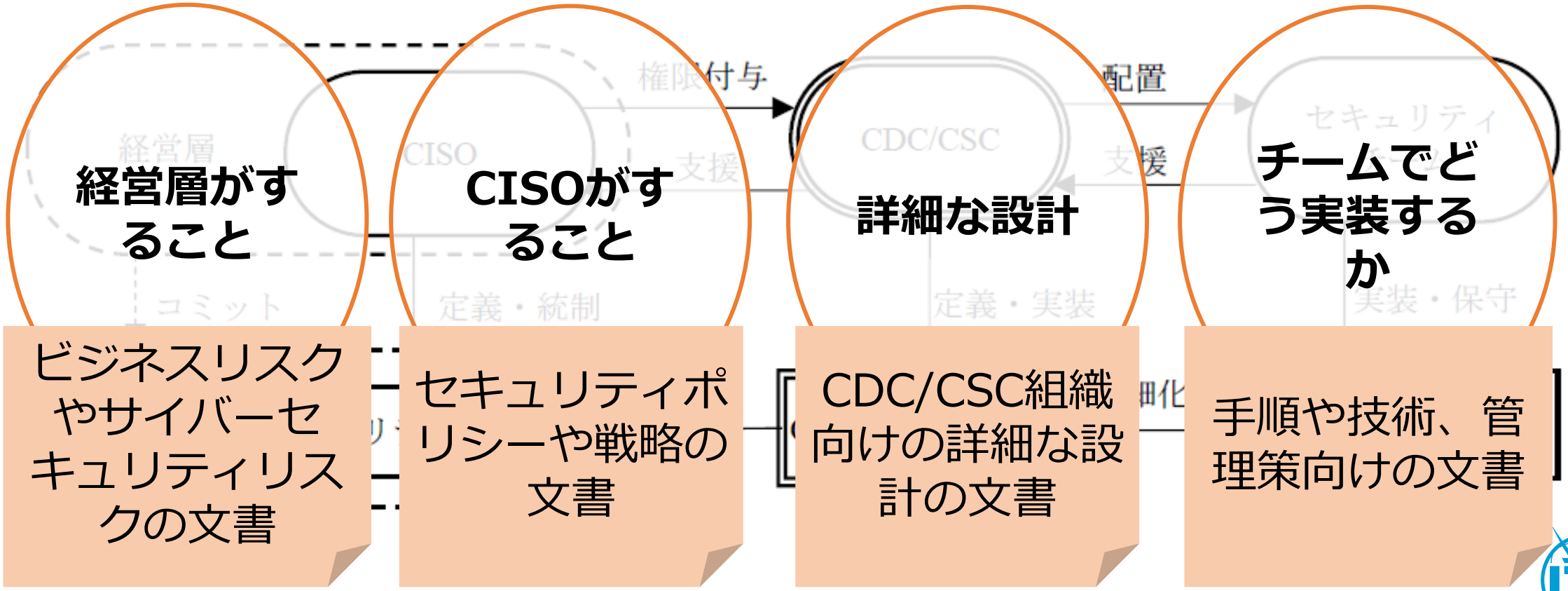
# X.1060に書かれていないこと

X.1060は以下に示すような内容を元にCDC/CSCのサービスをどう実装するかを示していない
- どんなシステムやプロセスが利用されているか
- CDC/CSCサービスのそれぞれのスコープ



# X.1060に書かれていないこと

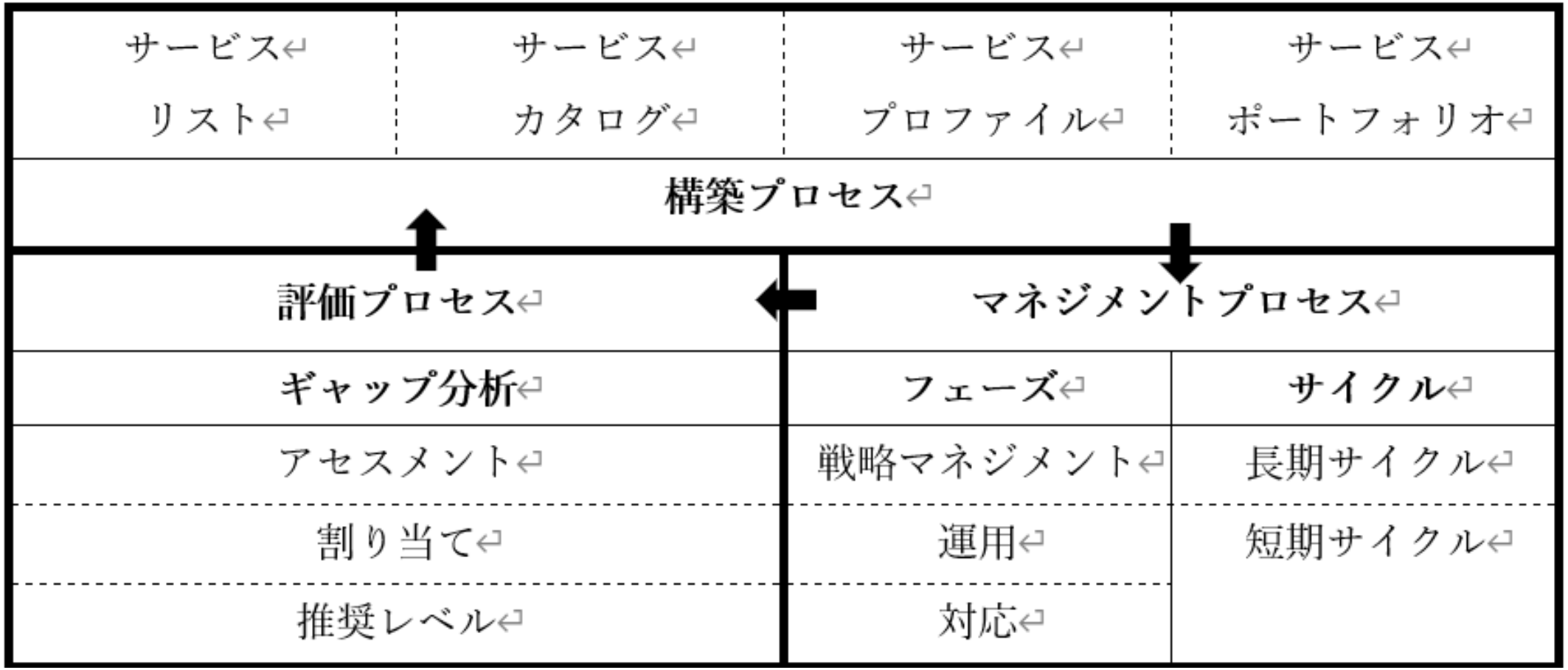
- X.1060を詳細化するには、ほかのガイドラインや文書を利用する



# サイバーディフェンスセンター/サイバーセキュリティセンターを構築・運用するためのフレームワーク

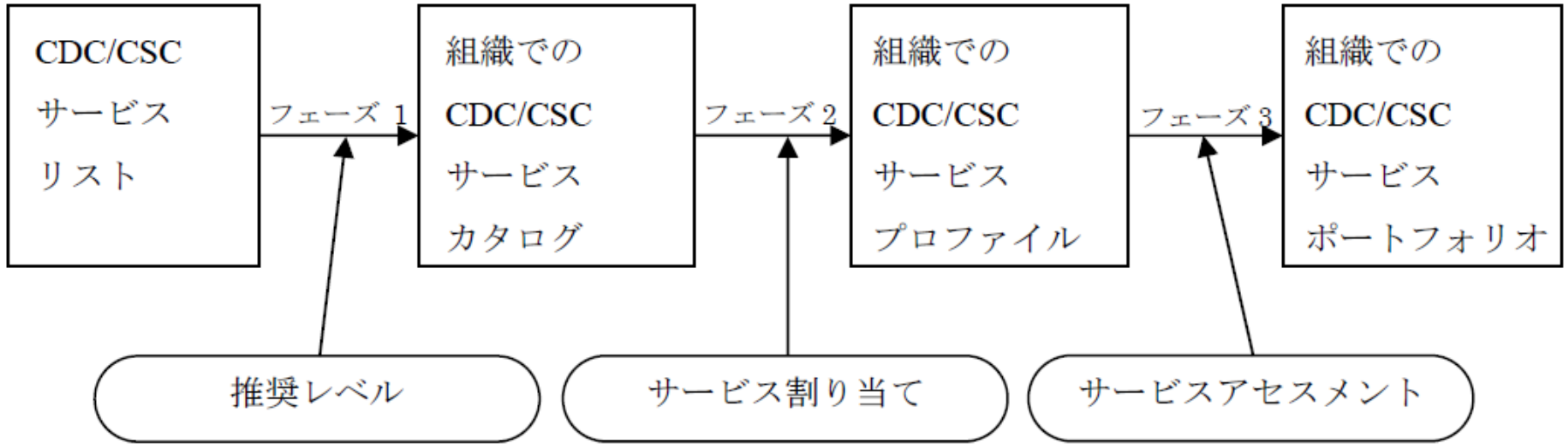
# フレームワーク

- セキュリティの活動を行う3つのプロセス
- **構築 - マネジメント – 評価**



# 構築プロセス

プロセス




成果物

| サービス | 推奨レベル | サービス<br>割り当て | サービススコア | |
|---|---|---|---|---|
| | | | 現状 | あるべき姿 |
| サービス① | ベーシック | インソース(AB 部門) | 3 | 5 |
| サービス② | スタンダード | アウトソース(Z-MSSP) | 2 | 4 |
| サービス③ | アドバンスド | 未割り当て | 1 | 2 |

←サービスリスト→

←――――サービスカタログ――――→

←――――――サービスプロファイル――――――→

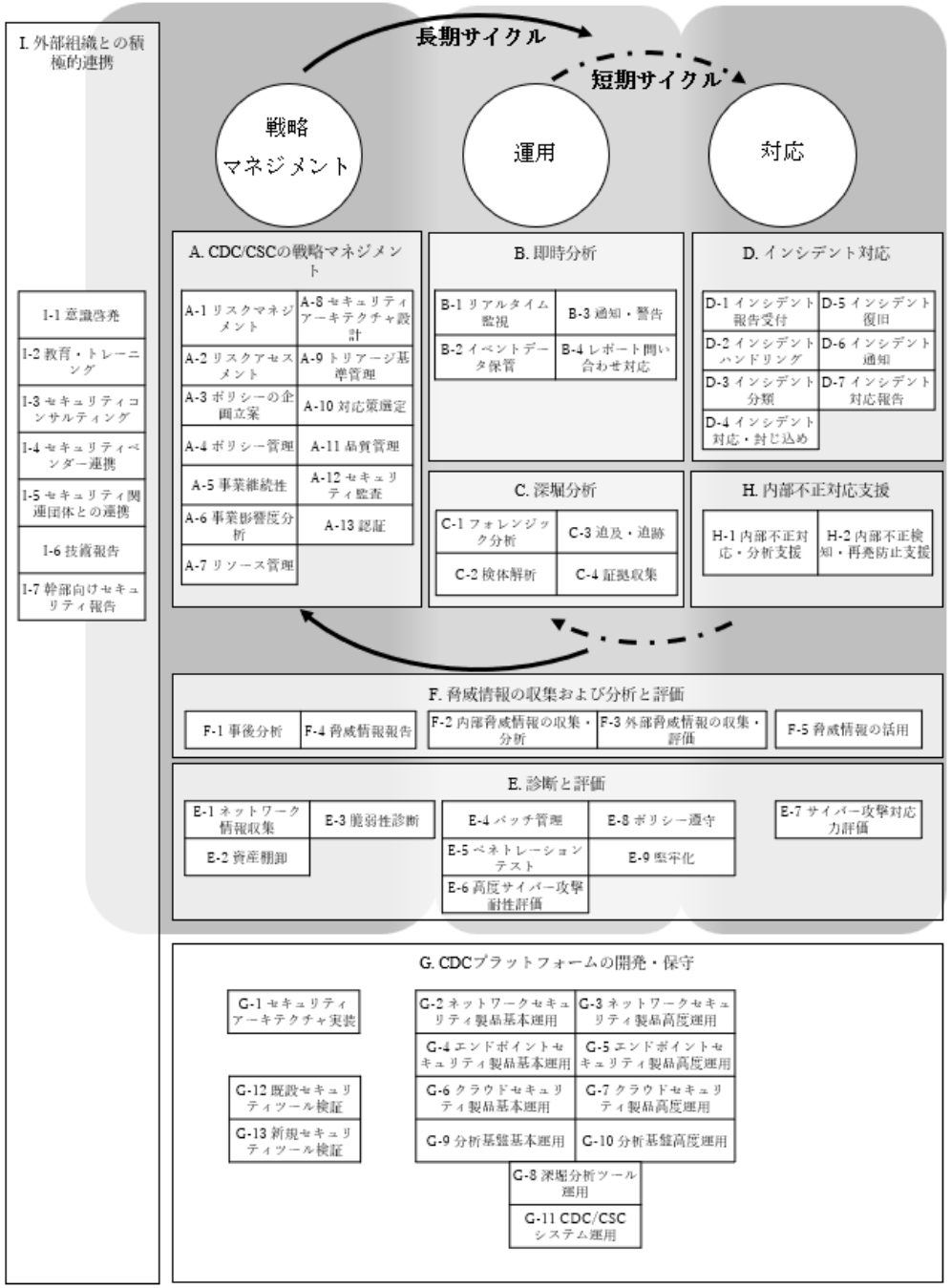
←――――――――――サービスポートフォリオ――――――――――→

# CDC/CSCサービスカテゴリー

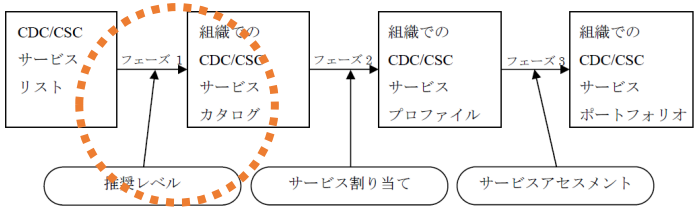
| サービスカテゴリー | | サービス数 |
|---|---|---|
| A | CDC/CSCの戦略マネジメント | 13 |
| B | 即時分析 | 4 |
| C | 深堀分析 | 4 |
| D | インシデント対応 | 7 |
| E | 診断と評価 | 9 |
| F | 脅威情報の収集および分析と評価 | 5 |
| G | CDC/CSCプラットフォームの開発・保守 | 13 |
| H | 内部不正対応支援 | 2 |
| I | 外部組織との積極的連携 | 7 |

# CDC/CSCサービスリスト

| | | | |
|---|---|---|---|
| A | CDC/CSCの戦略マネジメント | E-5 | ペネトレーションテスト |
| A-1 | リスクマネジメント | E-6 | 高度サイバー攻撃耐性評価 |
| A-2 | リスクアセスメント | E-7 | サイバー攻撃対応力評価 |
| A-3 | ポリシーの企画立案 | E-8 | ポリシー遵守 |
| A-4 | ポリシー管理 | E-9 | 堅牢化 |
| A-5 | 事業継続性 | F | 脅威情報の収集および分析と評価 |
| A-6 | 事業影響度分析 | F-1 | 事後分析 |
| A-7 | リソース管理 | F-2 | 内部脅威情報の収集・分析 |
| A-8 | セキュリティアーキテクチャ設計 | F-3 | 外部脅威情報の収集・評価 |
| A-9 | トリアージ基準管理 | F-4 | 脅威情報報告 |
| A-10 | 対応策選定 | F-5 | 脅威情報の活用 |
| A-11 | 品質管理 | G | CDC/CSCプラットフォームの開発・保守 |
| A-12 | セキュリティ監査 | G-1 | セキュリティアーキテクチャ実装 |
| A-13 | 認証 | G-2 | ネットワークセキュリティ製品基本運用 |
| B | 即時分析 | G-3 | ネットワークセキュリティ製品高度運用 |
| B-1 | リアルタイム監視 | G-4 | エンドポイントセキュリティ製品基本運用 |
| B-2 | イベントデータ保管 | G-5 | エンドポイントセキュリティ製品高度運用 |
| B-3 | 通知・警告 | G-6 | クラウドセキュリティ製品基本運用 |
| B-4 | レポート問い合わせ対応 | G-7 | クラウドセキュリティ製品高度運用 |
| C | 深堀分析 | G-8 | 深堀分析ツール運用 |
| C-1 | フォレンジック分析 | G-9 | 分析基盤基本運用 |
| C-2 | 検体解析 | G-10 | 分析基盤高度運用 |
| C-3 | 追及・追跡 | G-11 | CDC/CSCシステム運用 |
| C-4 | 証拠収集 | G-12 | 既設セキュリティツール検証 |
| D | インシデント対応 | G-13 | 新規セキュリティツール検証 |
| D-1 | インシデント報告受付 | H | 内部不正対応支援 |
| D-2 | インシデントハンドリング | H-1 | 内部不正対応・分析支援 |
| D-3 | インシデント分類 | H-2 | 内部不正検知・再発防止支援 |
| D-4 | インシデント対応・封じ込め | I | 外部組織との積極的連携 |
| D-5 | インシデント復旧 | I-1 | 意識啓発 |
| D-6 | インシデント通知 | I-2 | 教育・トレーニング |
| D-7 | インシデント対応報告 | I-3 | セキュリティコンサルティング |
| E | 診断と評価 | I-4 | セキュリティベンダーとの連携 |
| E-1 | ネットワーク情報収集 | I-5 | セキュリティ関連団体との連携 |
| E-2 | 資産棚卸 | I-6 | 技術報告 |
| E-3 | 脆弱性診断 | I-7 | 幹部向けセキュリティ報告 |
| E-4 | パッチ管理 | | |



# 構築プロセス
# フェーズ1: カタログを作る



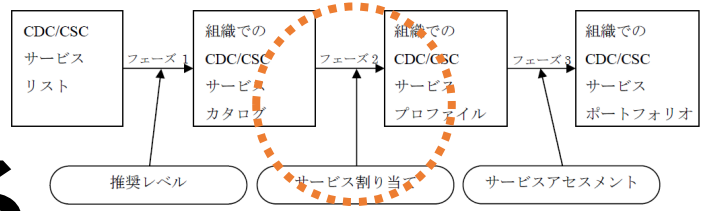

- X.1060付録のCDC/CSCサービスから次のレベルで選ぶ
- 必要であればサービスを追加することもできる

| ウェイト | 説明 |
|---|---|
| 不要 | 不要と判断されたサービス |
| ベーシック | 実装すべき最低限のサービス |
| スタンダード | 一般的に実装が推奨されているサービス |
| アドバンスド | 高いレベルのCDC/CSCサイクルを実現する場合に要求されるサービス |
| オプション | 想定されるCDC/CSCの形態に応じて任意に選択されるサービス |

# CDC/CSCサービスの推奨レベルを使う

| サービス | 推奨レベル | サービス割り当て | サービススコア | |
|---|---|---|---|---|
| | | | 現状 | あるべき姿 |
| A-1. リスクマネジメント | ベーシック(必須) | | | |
| A-2. リスクアセスメント | ベーシック(必須) | | | |
| … | | | | |
| B-1. リアルタイム監視 | ベーシック(必須) | | | |
| B-2. イベントデータ保管 | スタンダード(標準) | | | |
| … | | | | |

# 構築プロセス
# フェーズ2:プロファイルを作る




- カタログ中のサービス提供に責任を持つ組織を決定する
- 割り当ての方針は以下のタイプを参照して決定する

| タイプ | 説明 |
|---|---|
| インソース | 組織内のチームのサービスを実現する。責務を負う担当を明確にする。 |
| アウトソース | 組織外のチームでサービスを実現する。委託先を明確にする。 |
| 併用 | インソースとアウトソースを併用する。責務を負う担当と委託先を明確にする。 |
| 未割当 | 組織に存在すべきサービスはあるが、割り当てられない。 |

- 以下の図はインソースとアウトソースの考え方を示している

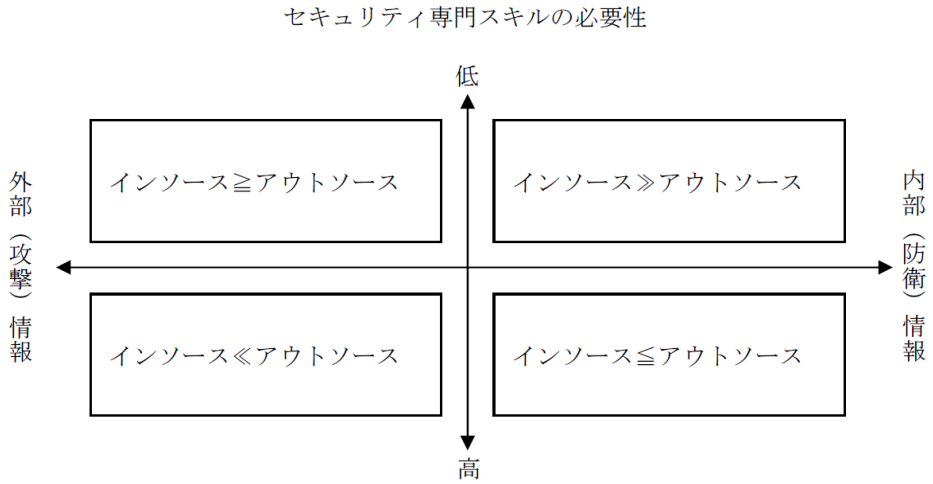
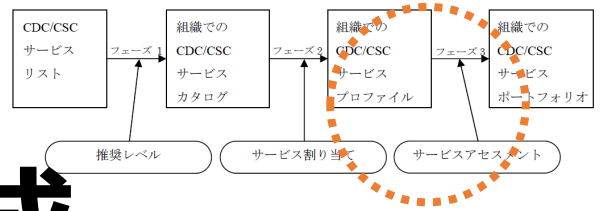



図 5　調達の象限

# CDC/CSCのサービス割り当てを使う

| サービス | 推奨レベル | サービス割り当て | サービススコア | |
|---|---|---|---|---|
| | | | 現状 | あるべき姿 |
| A-1. リスクマネジメント | ベーシック(必須) | インソース (部署AB) | | |
| A-2. リスクアセスメント | ベーシック(必須) | インソース (部署AB) | | |
| … | | | | |
| B-1. リアルタイム監視 | ベーシック(必須) | アウトソース (Z-MSSP) | | |
| B-2. イベントデータ保管 | スタンダード(標準) | アウトソース (Z-MSSP) | | |
| … | | | | |

# 構築プロセス
# フェーズ3: ポートフォリオの作成




- 割り当て状況に応じて、現在と目標のスコアを設定する
- スコアを決めるために、以下の基準を参考にできる

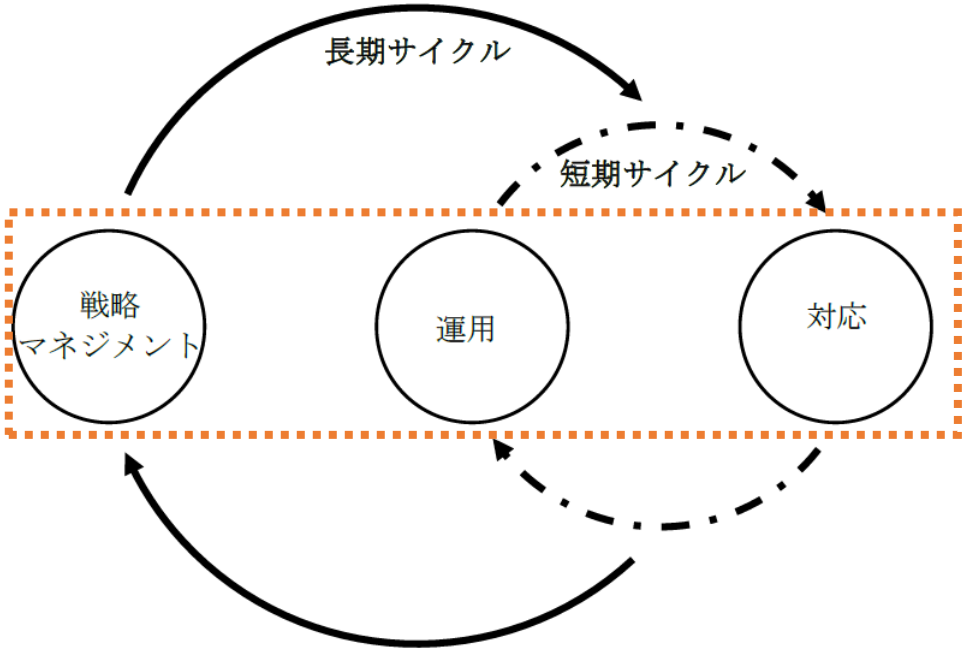
| インソースの場合 | |
|---|---|
| 明文化された運用が CISO など権限ある組織長に承認されている | +5 点 |
| 運用が明文化されており、担当者と交代して他者が業務を実施できる | +4 点 |
| 運用が明文化されておらず、担当者に代わりに他者が臨時で一部の業務を代行できる | +3 点 |
| 運用が明文化されておらず、担当者のみが業務を実施できる | +2 点 |
| 実施できていない | +1 点 |
| インソースとしては実施しないと決めた | 適用外 |

| アウトソースの場合 | |
|---|---|
| サービス内容と得られる結果を理解でき、想定通り | +5 点 |
| サービス内容と得られる結果を理解できているが、想定未満 | +4 点 |
| サービス内容、得られる結果のいずれかが理解できていない | +3 点 |
| サービス内容と得られる結果を理解できていない | +2 点 |
| 結果や報告を確認できていない | +1 点 |
| アウトソースとしては実施しないと決めた | 適用外 |

# CDC/CSCのサービスアセスメントを使う

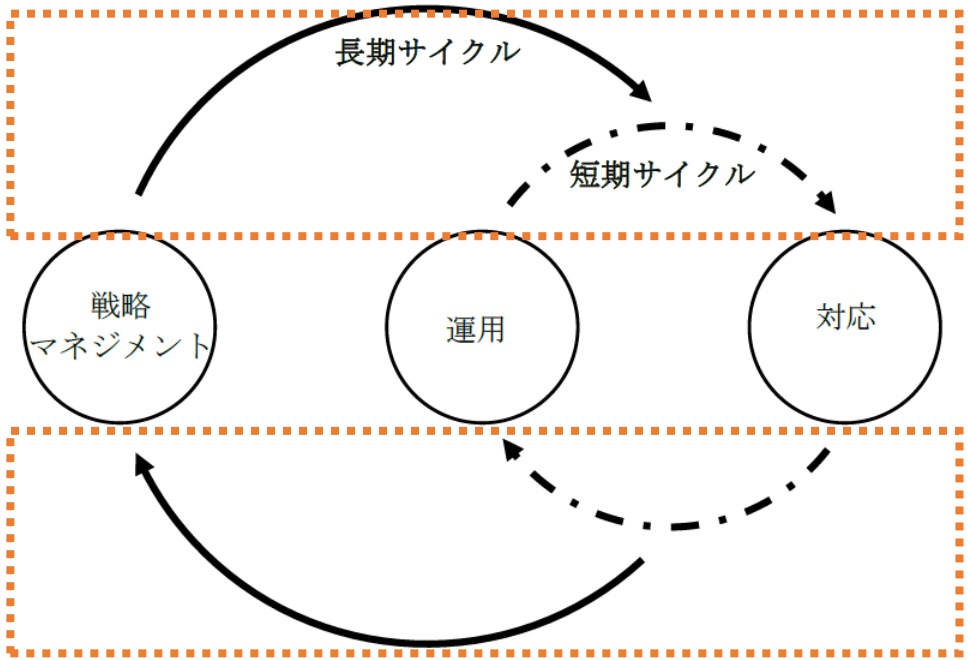
| サービス | 推奨レベル | サービス割り当て | サービススコア | |
|---|---|---|---|---|
| | | | 現状 | あるべき姿 |
| A-1. リスクマネジメント | ベーシック(必須) | インソース (部署AB) | 3 | 4 |
| A-2. リスクアセスメント | ベーシック(必須) | インソース (部署AB) | 3 | 4 |
| … | | | | |
| B-1. リアルタイム監視 | ベーシック(必須) | アウトソース (Z-MSSP) | 2 | 3 |
| B-2. イベントデータ保管 | スタンダード(標準) | アウトソース (Z-MSSP) | 2 | 3 |
| … | | | | |

# マネジメント プロセス - 3つのフェーズ



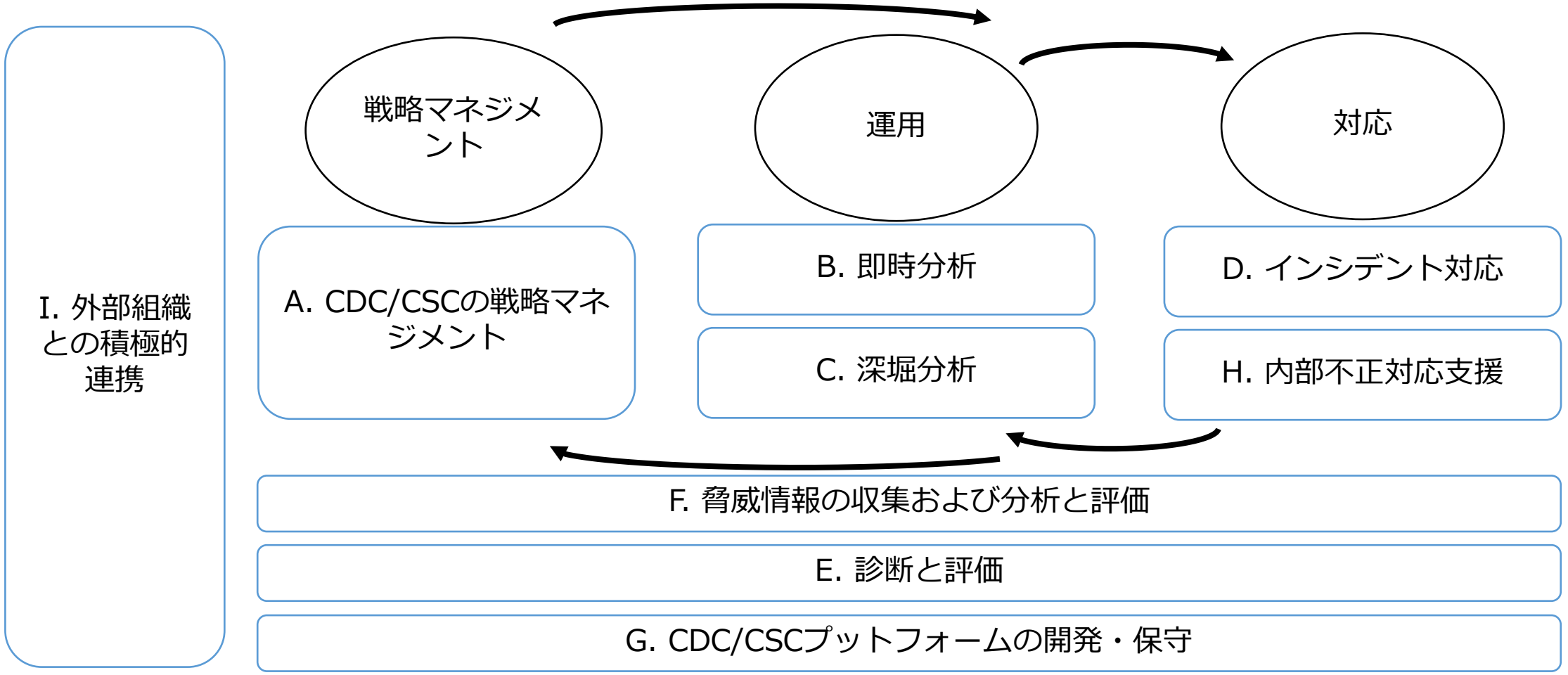

1. 戦略マネジメントフェーズ
   - 戦略マネジメントは、*CDC/CSC*の長期的な発展を保証するための定義、設計、計画、管理、認証などに関する戦略的サービスに対する責務と説明責任を有する
2. 運用フェーズ
   - 導入した仕組みのメンテナスを行う
   - 平時の日常的な業務である
   - 一般的にはインシデント検知の分析や、セキュリティ関連システムの監視・保守などの活動が含まれる。
   - このような業務を行うチームは、セキュリティオペレーションセンター*(SOC)*と呼ばれることが多い
3. 対応フェーズ
   - 分析によってイベントが検知された場合、インシデント対応が発動される。
   - このフェーズは有事の対応となる
   - そのチームはコンピュータセキュリティインシデント対応チーム*(CSIRT)*と呼ばれることが多い。
   - 対応フェーズへのインプットは、運用フェーズからだけと限らず、第三者からの報告や通知も同様に対応する必要がある

# マネジメントプロセス – 2つのサイクル




1. 短期サイクル
   - “運用”と “対応”は日々行われる
   - 問題の解決のために、例えば、単純作業の自動化、分析ツールの精度改善、報告項目の見直しで継続的な改善が必要になり、短期サイクルにおいては、すでに割り当てられたリソース(人、予算、システム)の中で実施することとなる
2. 長期サイクル
   - 新たなリソースの割り当てを必要とする見直しは、長期サイクルで扱われるべきである
   - 短期サイクルの見直しの中で現行システムでは解決できない課題が見つかった場合には、新しいセキュリティ製品の導入、セキュリティポリシーの抜本的な見直し、セキュリティシステムの大規模な構成変更など、長期的な視点と計画に基づき対応する必要がある

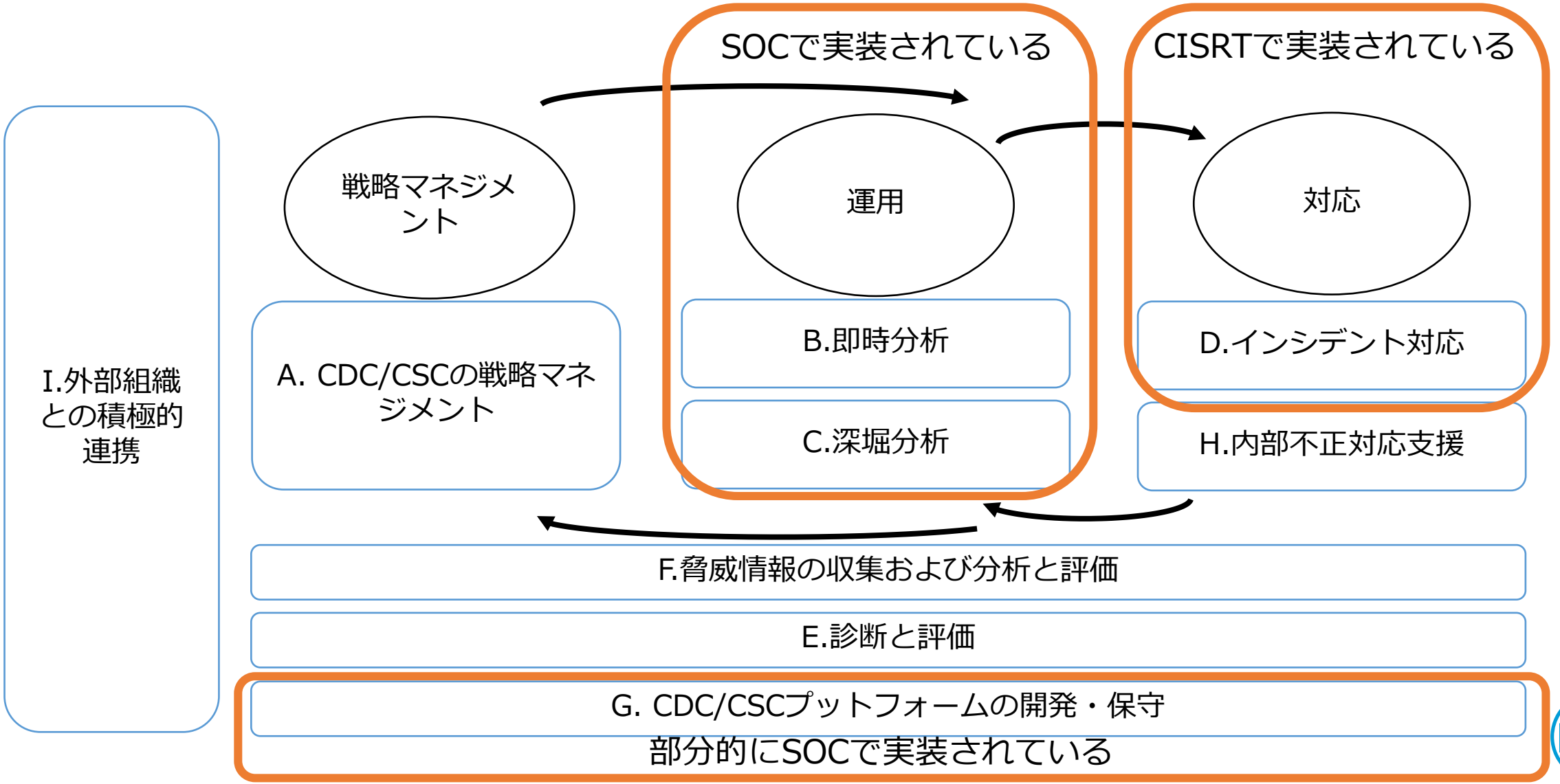
# サービスカテゴリーとマネジメントプロセスのマッピング



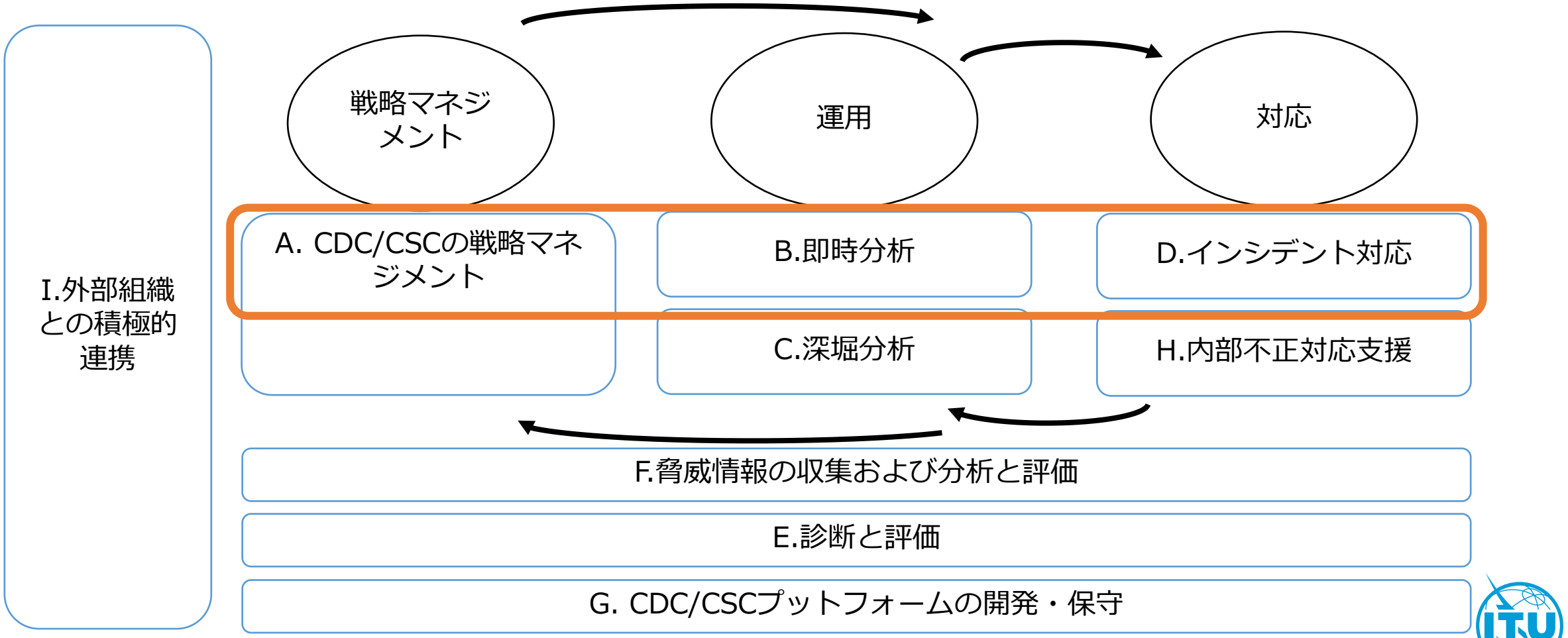
# 必要なサービスから実装をする

- サイバーセキュリティのためのセキュリティサービスの優先度と組織のリソースから決定される
- X.1060は組織を継続的に改善することを勧めているフレームワークである

# ケース: すでに運用と対応がある場合



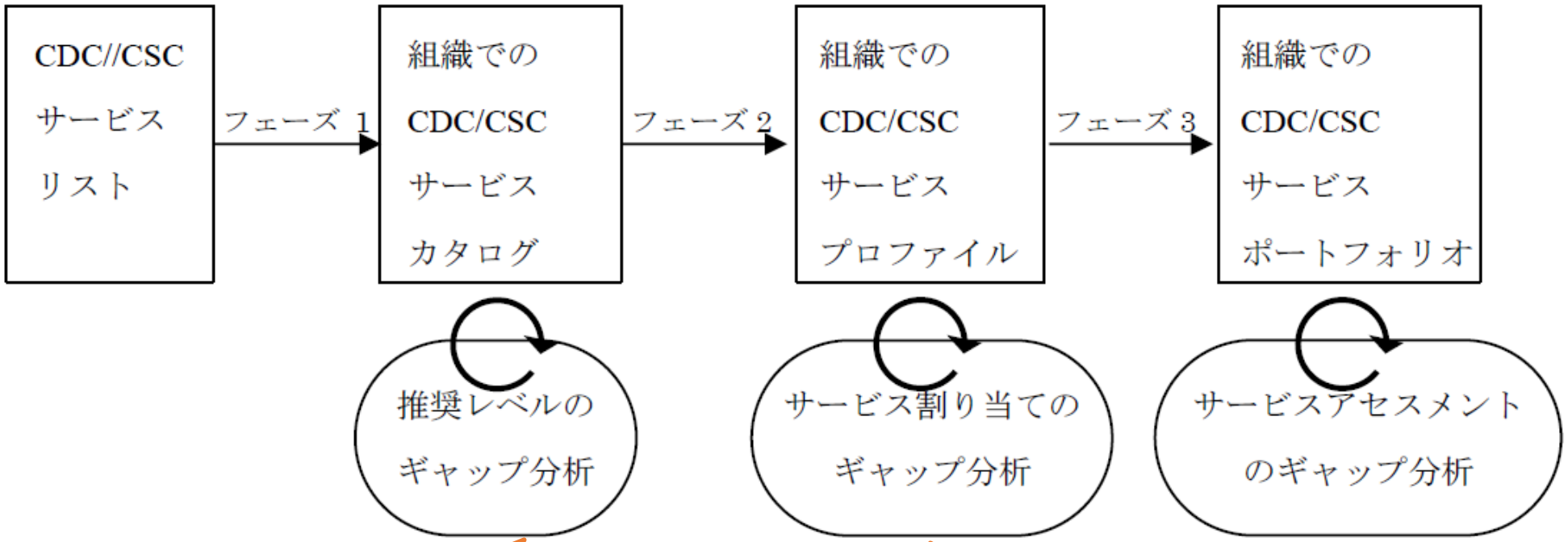
# ケース: マネジメントプロセスを始めるために最小限実装をする



# 評価プロセス

注:

サービスカタログ、プロファイル、ポートフォリオのそれぞれの見直しのプロセスは、構築プロセスで定義されています

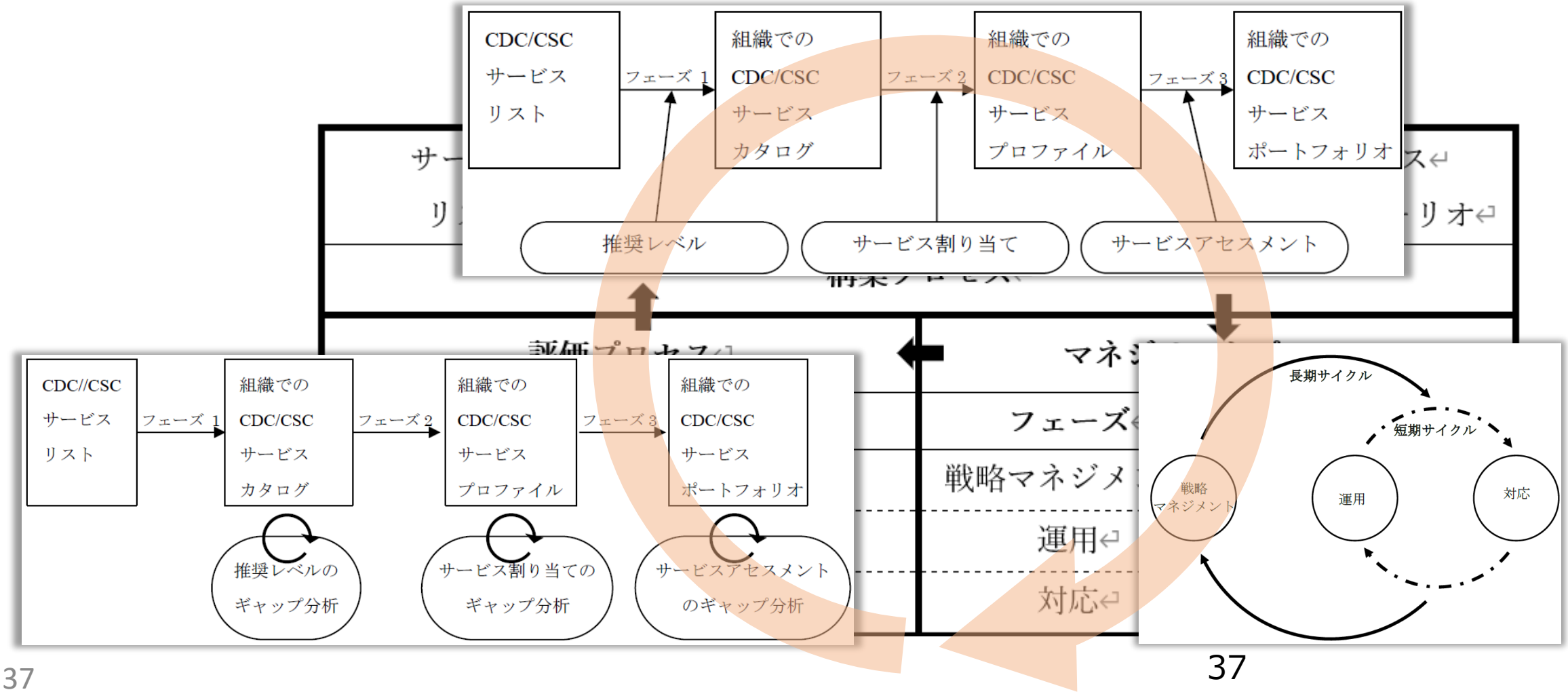



サービスカタログで選んだサービスの過不足はないか？

サービスプロファイルの割り当は適切だったか？

サービスポートフォリオで決めた目的のスコアは達成できているか？

# X.1060 サイバーディフェンスセンター/サイバーセキュリティセンターの構築・運用のためのフレームワーク






37

# Thank you