第10回脆弱性対応勉強会
X.1060の概要と使い所
X.1060の概要

2022.12.3

ISOG-J

X.1060とは

- 2021年6月29日にITU-T(国際電気通信連合の電気通信標準化部門)で国際勧告になった、サイバーリスク対応のための組織のフレームワーク

タイトル：
“Framework for the creation and operation of a cyber defence centre”

「サイバーディフェンスセンターを構築・運用するためのフレームワーク」

配布URL: https://www.itu.int/rec/T-REC-X.1060-202106-I

日本語版は？

- 2022年2月に一般社団法人　情報通信技術委員会(TTC)にて、JT-X1060が標準として決定した。
- X.1060が日本での標準として日本語で利用できます。
- 本資料の図表もこちらを引用しています。

タイトル：
「サイバーディフェンスセンターを構築・運用するためのフレームワーク」

配布URL:
https://www.ttc.or.jp/document_db/information/view_express_entity/1423

X.1060の背景とスコープ

背景

サイバーセキュリティはビジネスリスクの一つとなった
セキュリティの影響がシステムだけではなく事業など多岐に渡る
ビジネスの周辺環境や法律や規制などの影響も受けるようになった

ビジネスの目的にあったセキュリティ対策をリーダーシップを持って
実現できる仕組みが必要となっている。

スコープ

組織におけるサイバーディフェンスセンター(CDC)を構築と運用をし、効果的に改善を続けるフレームワークである。組織におけるセキュリティを実現するセキュリティサービスの選定と実装を示す。
CSOやCISO、およびCSOやCISOをサポートする方が対象となる。

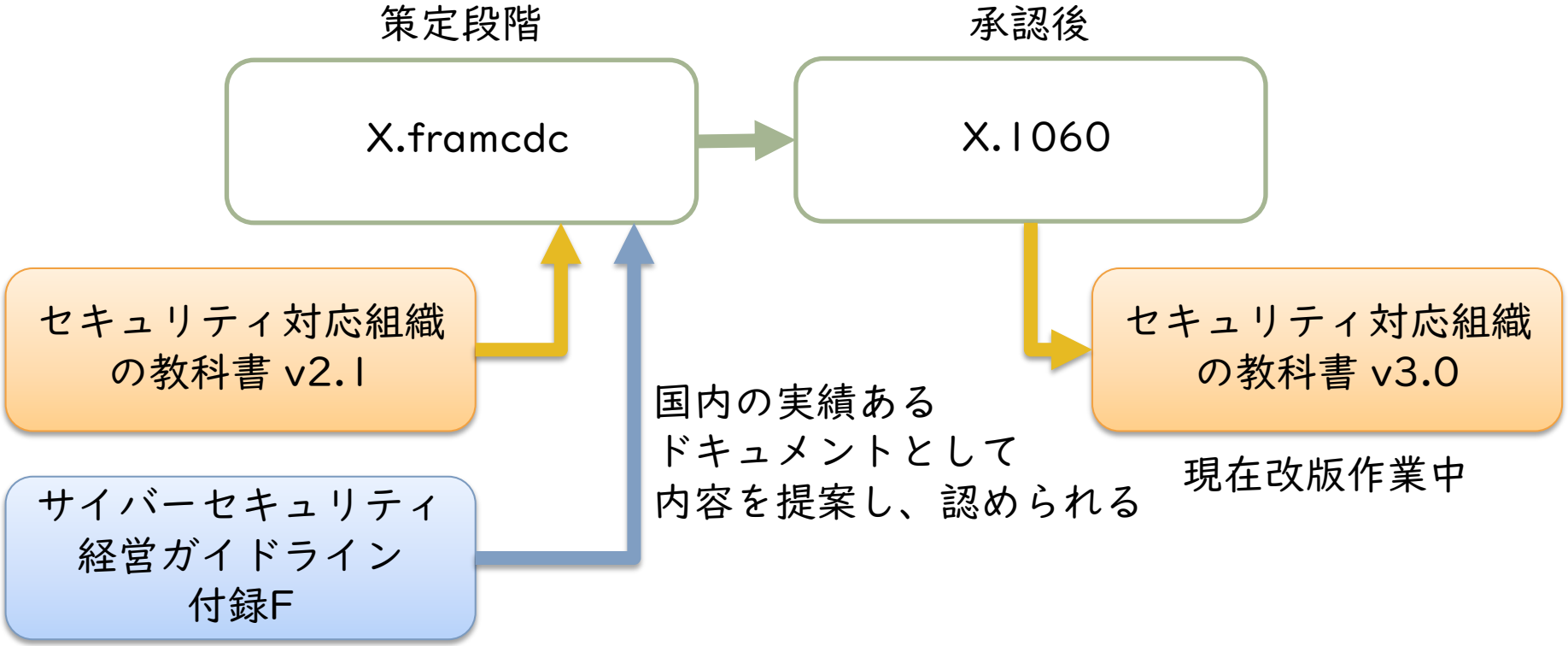
ポイント

- 新しい組織を作るわけではなく、現在のSOCやCSIRTを包含した形

- フレームワークで提示されたセキュリティサービスを実施しているなら、すでにCDCを部分的に構築していると考えられる

- 今後目指す姿として考えていただきたい

X.1060と関連ドキュメントのイメージ



各種ドキュメントとの立ち位置

フレームワーク　実践 （どこで、何をするか）

X.1060

経済産業省　サイバーセキュリティ経営ガイドライン 一式

IPA サイバーセキュリティ経営ガイドライン
Ver 2.0 実践のためのプラクティス集

産業横断サイバーセキュリティ検討会
　人材定義リファレンス及びスキルマッピング
　ユーザ企業のためのセキュリティ統括室　構築・運用キット

日本シーサート協議会(NCA)　ドキュメント 一式
CSIRTマテリアル
CSIRT人材の定義と確保

SIM3
Security Incident Management Maturity Model

日本セキュリティオペレーション事業者協議会(ISOG-J) ドキュメント一式
セキュリティ対応組織(SOC/CSIRT)の教科書

セキュリティ対応組織アセスメント

JNSAドキュメント群

CISOハンドブック

SecBok

X.1060概説

X.1060における組織体制

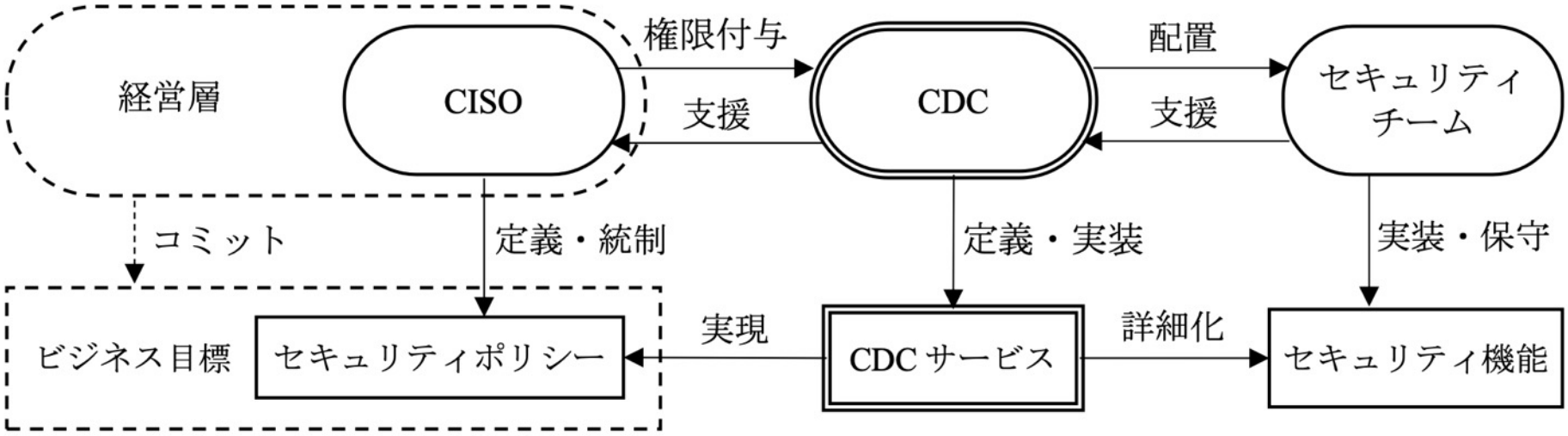


図 1　CDC の運営における関係者とその役割

図はJT-X1060より

日本のドキュメントとの比較

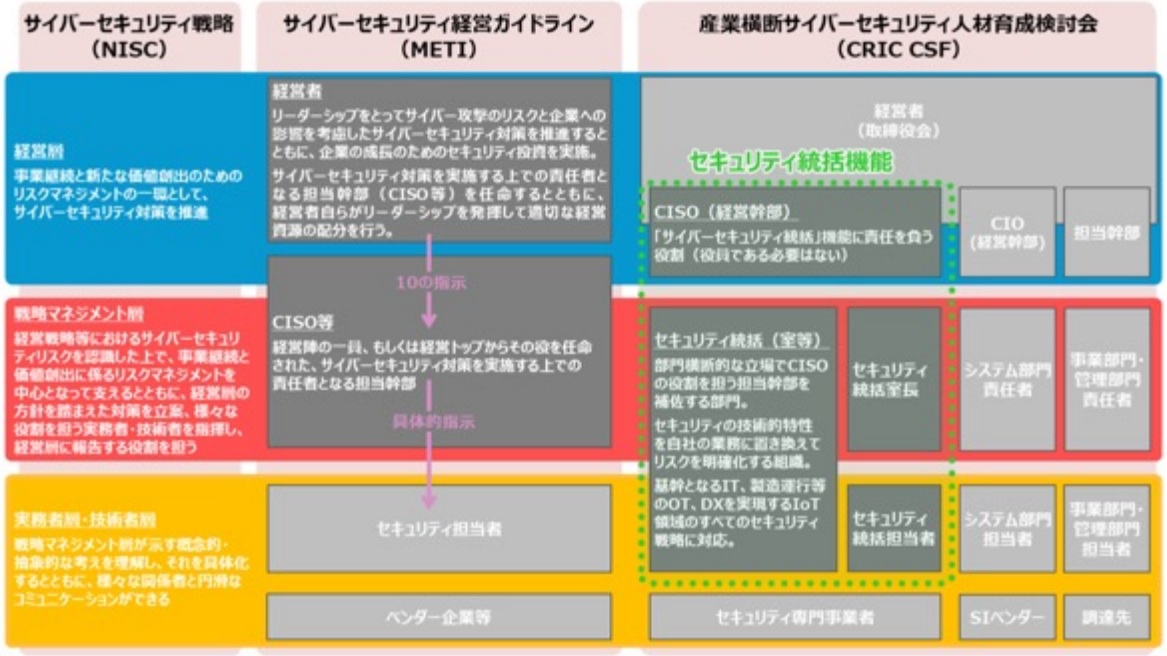


図 5　セキュリティ統括機能の位置付け（1）

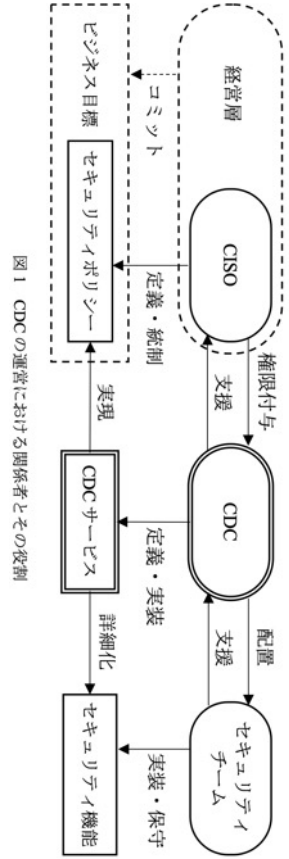


図 1　CDCの運営における関係者とその役割

経済産業省　サイバーセキュリティ経営ガイドライン
付録F サイバーセキュリティ体制構築・人材確保の手引き 第1.1版

フレームワーク概要

構築

評価

マネジメント

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
構築プロセス			
評価プロセス		マネジメントプロセス	
ギャップ分析		フェーズ	サイクル
アセスメント		戦略マネジメント	長期サイクル
割り当て		運用	短期サイクル
推奨レベル		対応	

図2　サイバーディフェンスセンターを構築・運用するためのフレームワーク

図はJT-X1060より

構築プロセス

構築プロセス

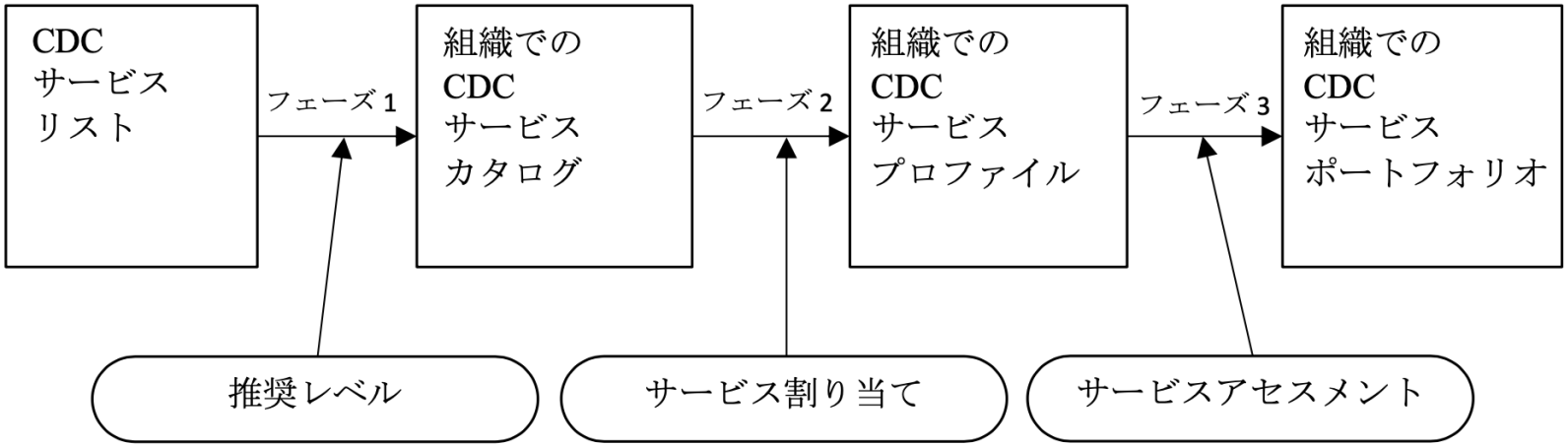


図 3　CDC サービスの立ち上げフェーズ

構築は3段階

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

図はJT-X1060より

構築は3つのフェーズ

サービスを選ぶ（サービスカタログを作る）

- サービスリストを参考に選び、どのサービスをどれくらいの推奨レベルで行うかを決める

どこで行うかを決める（サービスプロファイルを作る）

- それぞれのサービスは内製で実施するか、外部委託するか

今のスコアと目標のスコアを決める（サービスポートフォリオを作る）

- それぞれのサービスのスコアをセルフアセスメントで測る

構築プロセス：サービスリスト

X.1060
9つのカテゴリー
64のサービス

一覧になければ
追加しても良い

ISOG-J
9つのカテゴリー
54のサービス(※)

※ISOG-Jの教科書もX.1060に合わせて更新します。
図はJT-X1060より

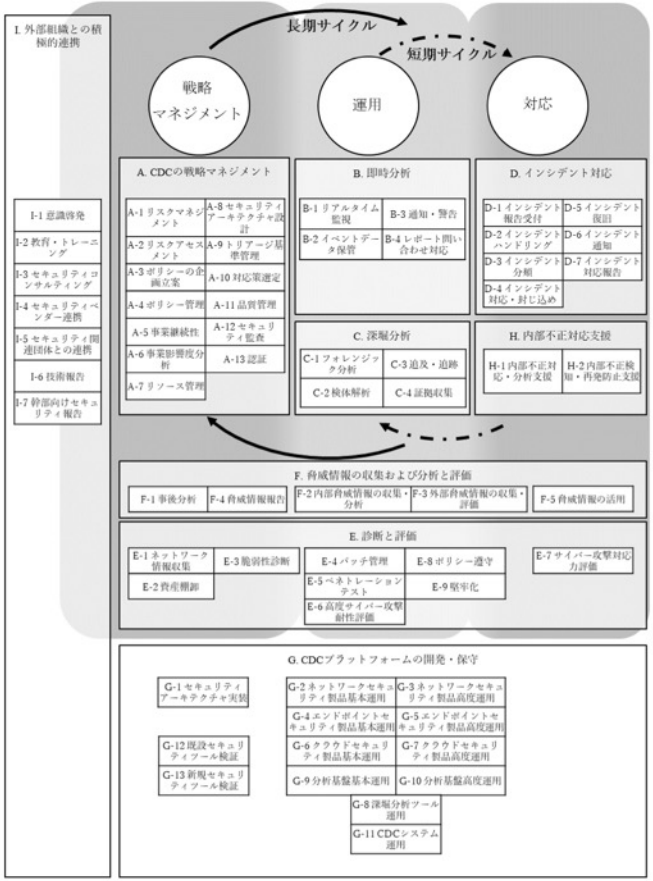


図8　CDCサービスカテゴリー

サービスカテゴリー、サービスリスト

- 9つのサービスカテゴリー、64のサービスリスト

A	CDC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

A.CDCの戦略マネジメント

A-1	リスクマネジメント
A-2	リスクアセスメント
A-3	ポリシーの企画立案
A-4	ポリシー管理
A-5	事業継続性
A-6	事業影響度分析
A-7	リソース管理

A-8	セキュリティアーキテクチャ設計
A-9	トリアージ基準管理
A-10	対応策選定
A-11	品質管理
A-12	セキュリティ監査
A-13	認証

B. 即時分析

B-1	リアルタイム監視
B-2	イベントデータ保管
B-3	通知・警告
B-4	レポート問い合わせ対応

C. 深堀分析

C-1	フォレンジック分析
C-2	検体解析
C-3	追及・追跡
C-4	証拠収集

D. インシデント対応

D-1	インシデント報告受付
D-2	インシデントハンドリング
D-3	インシデント分類
D-4	インシデント対応・封じ込め
D-5	インシデント復旧
D-6	インシデント通知
D-7	インシデント対応報告

E. 診断と評価

E-1	ネットワーク情報収集
E-2	資産棚卸
E-3	脆弱性診断
E-4	パッチ管理
E-5	ペネトレーションテスト

E-6	高度サイバー攻撃耐性評価
E-7	サイバー攻撃対応力評価
E-8	ポリシー遵守
E-9	堅牢化

F. 脅威情報の収集および分析と評価

F-1	事後分析
F-2	内部脅威情報の収集・分析
F-3	外部脅威情報の収集・評価
F-4	脅威情報報告
F-5	脅威情報の活用

G. CDCプラットフォームの開発・保守

G-1	セキュリティアーキテクチャ実装
G-2	ネットワークセキュリティ製品基本運用
G-3	ネットワークセキュリティ製品高度運用
G-4	エンドポイントセキュリティ製品基本運用
G-5	エンドポイントセキュリティ製品高度運用
G-6	クラウドセキュリティ製品基本運用
G-7	クラウドセキュリティ製品高度運用

G-8	深堀分析ツール運用
G-9	分析基盤基本運用
G-10	分析基盤高度運用
G-11	CDCシステム運用
G-12	既設セキュリティツール検証
G-13	新規セキュリティツール検証

H. 内部不正対応支援

H-1	内部不正対応・分析支援
H-2	内部不正検知・再発防止支援

I. 外部組織との積極的連携

I-1	意識啓発
I-2	教育・トレーニング
I-3	セキュリティコンサルティング
I-4	セキュリティベンダー連携
I-5	セキュリティ関連団体との連携
I-6	技術報告
I-7	幹部向けセキュリティ報告

推奨レベル

9.2. CDC サービスの推奨レベル

組織にとって最適な CDC サービスを実現するため、各サービスの必要性を表 1 に示す 5 つのレベルで考える。このレベルを用いることで、サービス実施の優先順位を明確にすることができる。

表 1　CDC サービスの推奨レベル

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 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 の形態に応じて任意に選択されるサービス

出典：JT-X1060

構築プロセス：サービスのアサイン

X.1060/JT-X1060

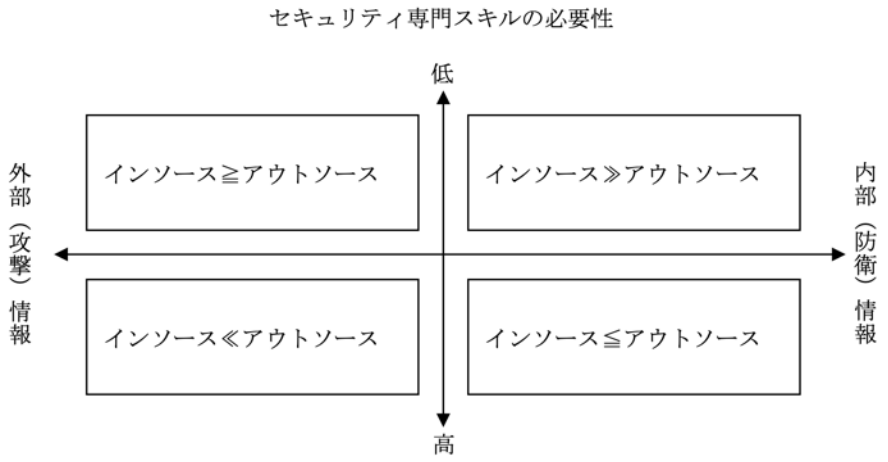


図5　調達の象限

図はJT-X1060より

ISOG-J

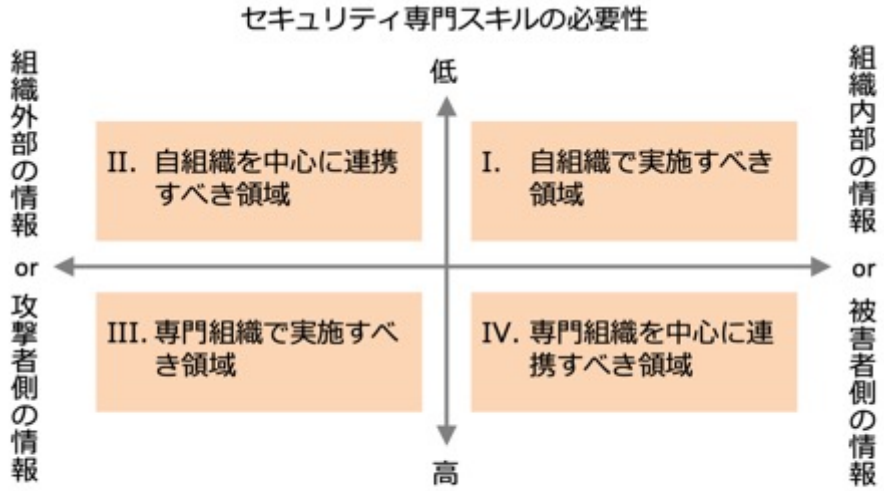


図 4　セキュリティ対応の4領域

図はセキュリティ対応組織の教科書より

構築プロセス：サービスのアセスメント

X.1060/JT-X1060

表3　CDCサービススコア

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

図はJT-X1060より

ISOG-J

- 自組織でその役割を実施する場合（インソース）
  - 明文化された運用は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）
  - インソースでの実装を検討したものの、結果として実施しないと判断した（評価対象外）

- 専門組織でその役割を実施する場合（アウトソース）
  - 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）
  - アウトソースでの実装を検討したものの、結果として実施しないと判断した（評価対象外）

今後の呼び方は成熟度から変更します。

マネジメントプロセス

マネジメントプロセス

日々の改善を実行する

X.1060/JT-X1060

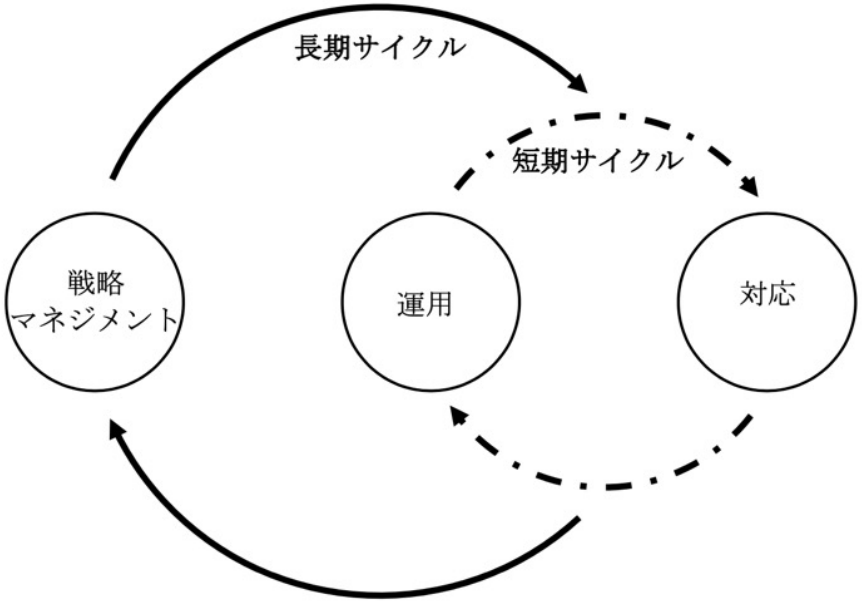


図6　CDCマネジメントプロセス

ISOG-J

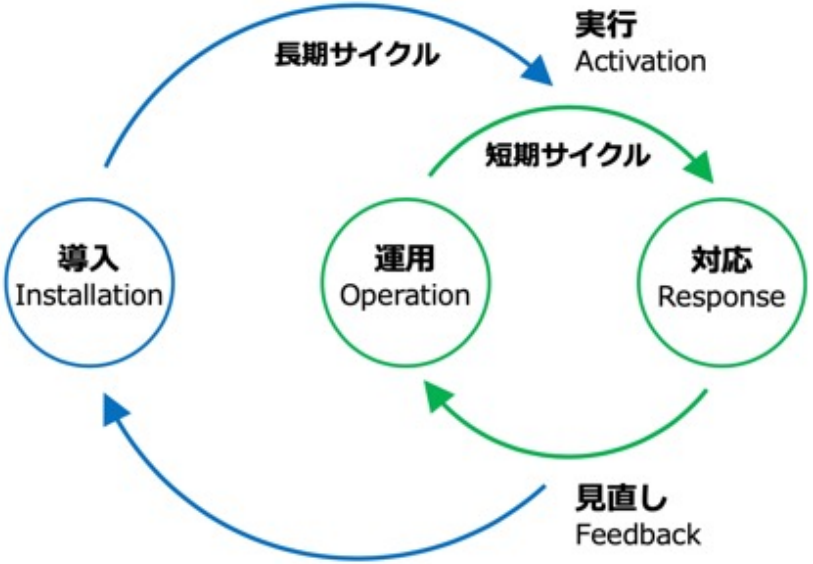
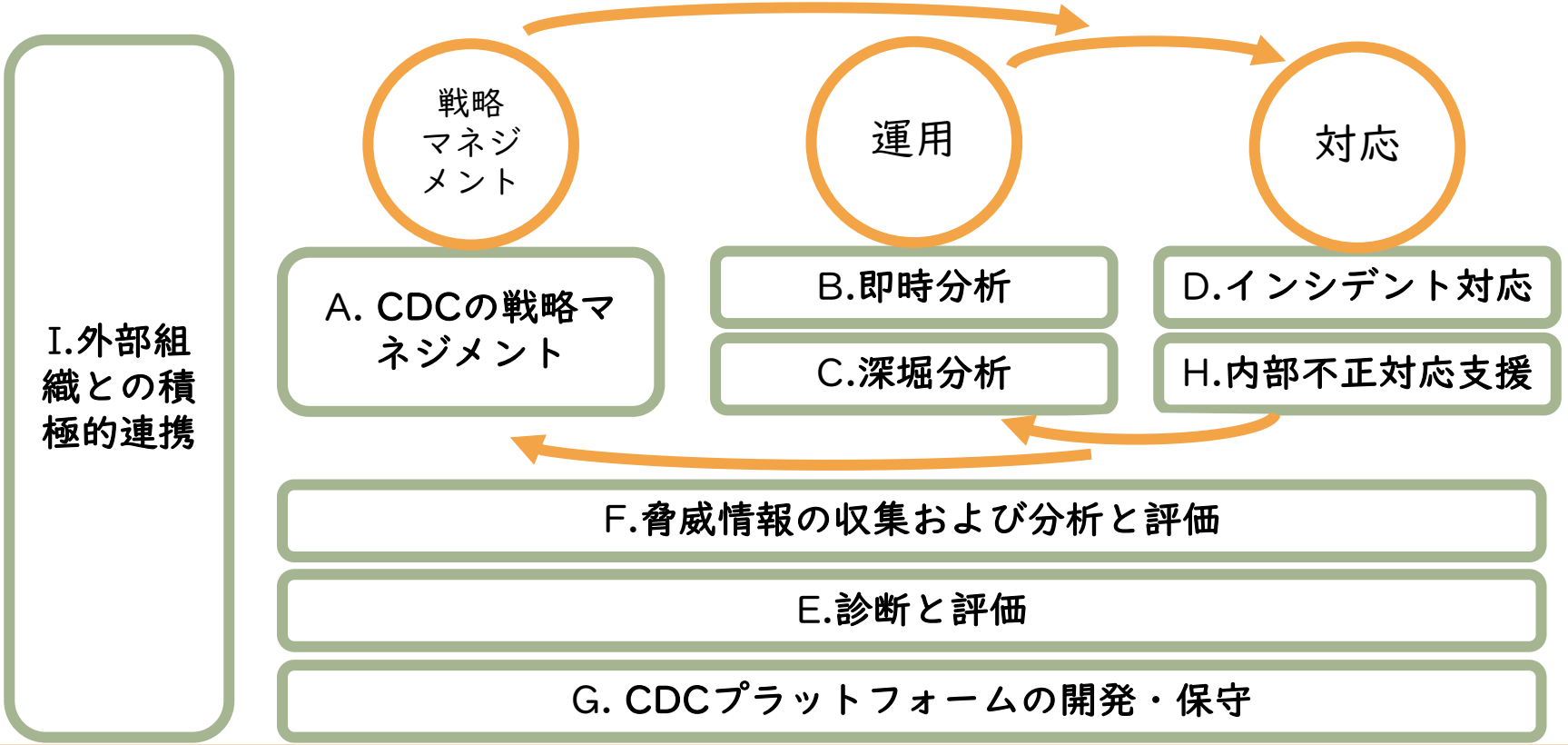


図 1　セキュリティ対応実行サイクル

図はJT-X1060より

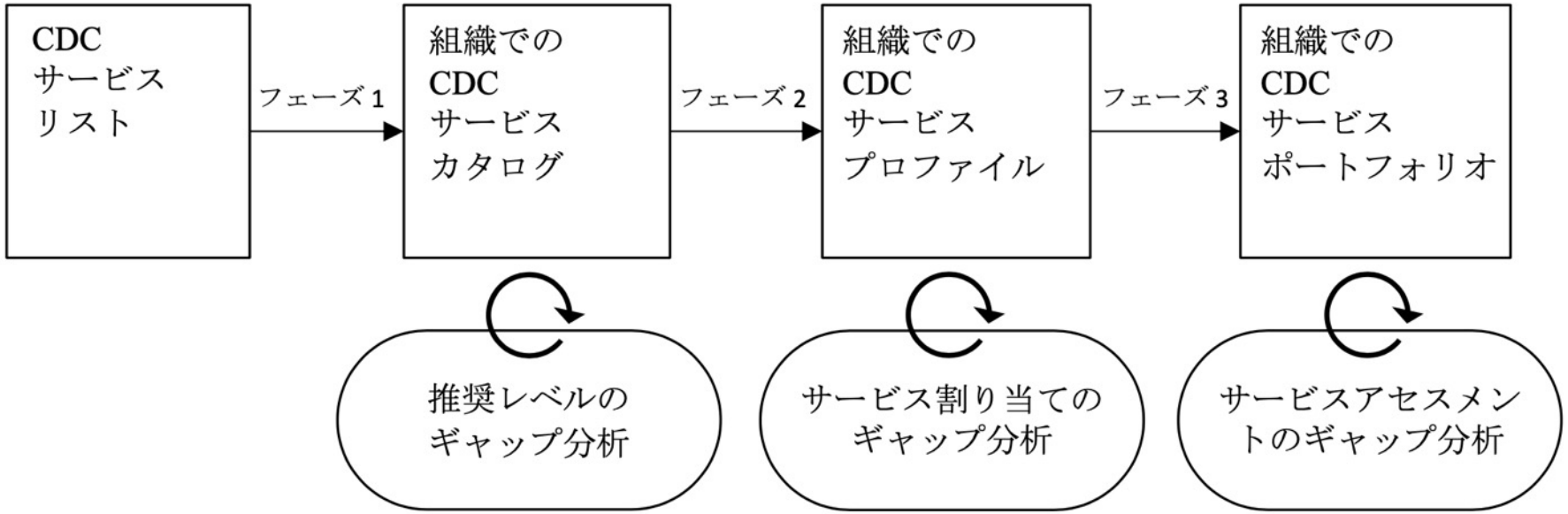
図はセキュリティ対応組織の教科書より

サービスカテゴリとマネジメントプロセスとのマッピング



評価プロセス

評価プロセス



図はJT-X1060より

図 7　CDC 評価プロセス

構築で行った3つのフェーズそれぞれで見直しをする

評価は構築した3つのフェーズの振り返り

サービスを選ぶ（サービスカタログを作る）

- サービスリストを参考に選び、どのサービスをどれくらいの推奨レベルで行うかを決める

選んだものは妥当だったか？
状況の変化に対応しているか？

どこで行うかを決める（サービスプロファイルを作る）

- それぞれのサービスは内製で実施するか、外部委託するか

このままで良いか？
割り当てを変えるか？

今のスコアと目標のスコアを決める（サービスポートフォリオを作る）

- それぞれのサービスのスコアをセルフアセスメントで測る

今のスコアはどうなった？
目標は変わったか？

経営環境や事業環境、セキュリティの状況は
常に変化します。

継続的な改善を！

フレームワーク概要

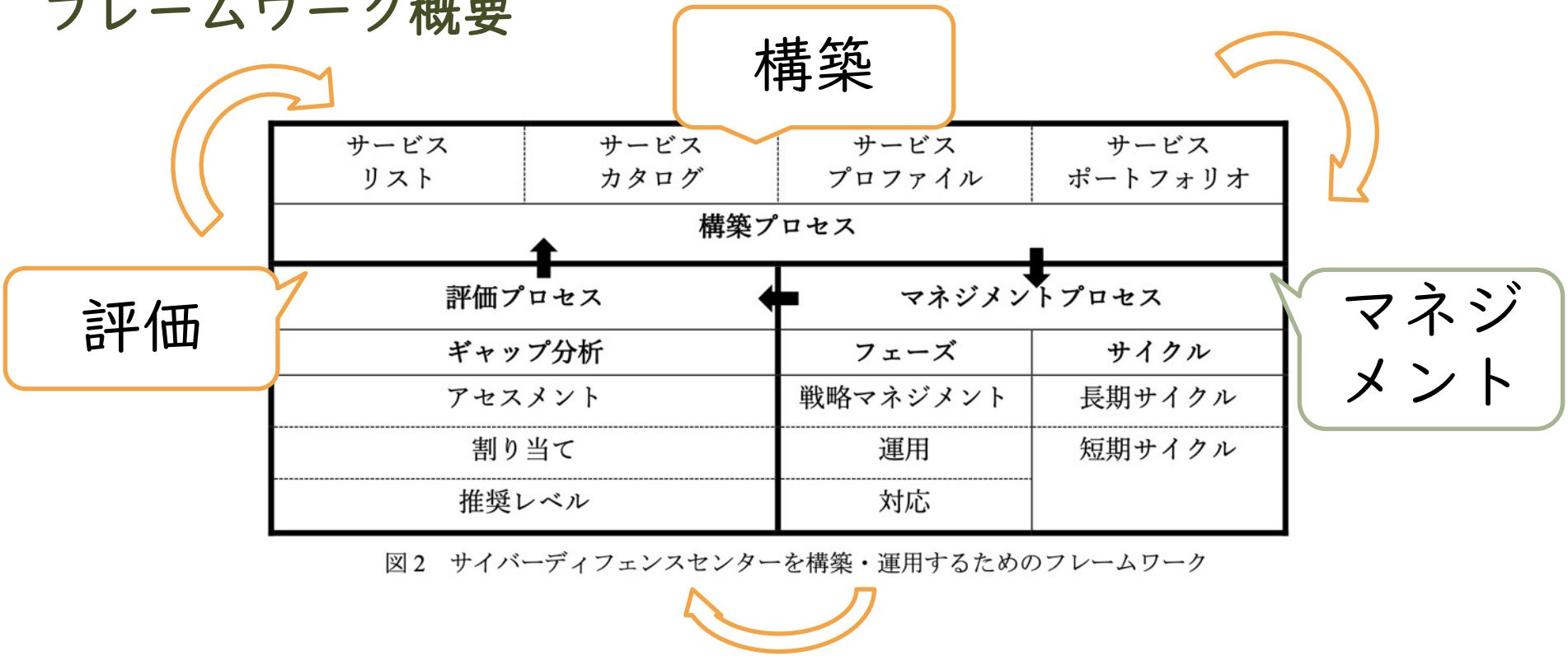


図2　サイバーディフェンスセンターを構築・運用するためのフレームワーク

図はJT-X1060より

X.1060のまとめ

- 新しい組織を作るわけではなく、現在のSOCやCSIRTを包含した今後のセキュリティの組織の形
- 日本のドキュメントを参考にフレームワークを実現できる
- 継続的に改善を続けて変化への対応を

X.1060を実現するための参考となるドキュメント群(ISOG-J)

ITU-T X.1060：国際標準のフレームワーク

具体的な実現方法の参考書

セキュリティ対応組織の教科書

X.1060に対応したv3.0に更新予定

情報共有の考え方

MSSの選び方

セキュリティ対応組織の強化に向けた
サイバーセキュリティ情報共有「5W1H」

マネージドセキュリティサービス選定ガイドライン