各種成果物で実現する、これからの国際標準レベルのセキュリティ組織

JNSA全国サイバーセキュリティセミナー2021

ISOG-J

自己紹介

- 武井　滋紀　です。
- JNSAのISOG-Jの方から来ました
  - ISOG-J 副代表、セキュリティオペレーション連携WG(WG6)リーダー
- NTTテクノクロス株式会社
  - セキュアシステム事業部　アソシエイトエバンジェリスト
  - 2016年度までは社名が「NTTソフトウェア株式会社」でした
  - NTTグループ セキュリティプリンシパル
  - ITU-T SG17 WP3 Q3 X.1060 Editor
  - CISSP、情報処理安全確保支援士

ISOG-J とは

- 日本セキュリティオペレーション事業者協議会
  - the Information Security Operation providers Group Japan
  - 2008年創立、2021年11月現在 56組織が加盟
  - プロのセキュリティオペレーター、事業者の集まり
  - 業界の発展のために課題を議論したり、互いに情報を出し合うことで外部へ成果を発表する団体です
  - 親団体は日本ネットワークセキュリティ協会(JNSA)
- http://isog-j.org/
  - Facebook ページ: /isogj
  - ISOG-J の読み方: いそぐじぇい

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

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。

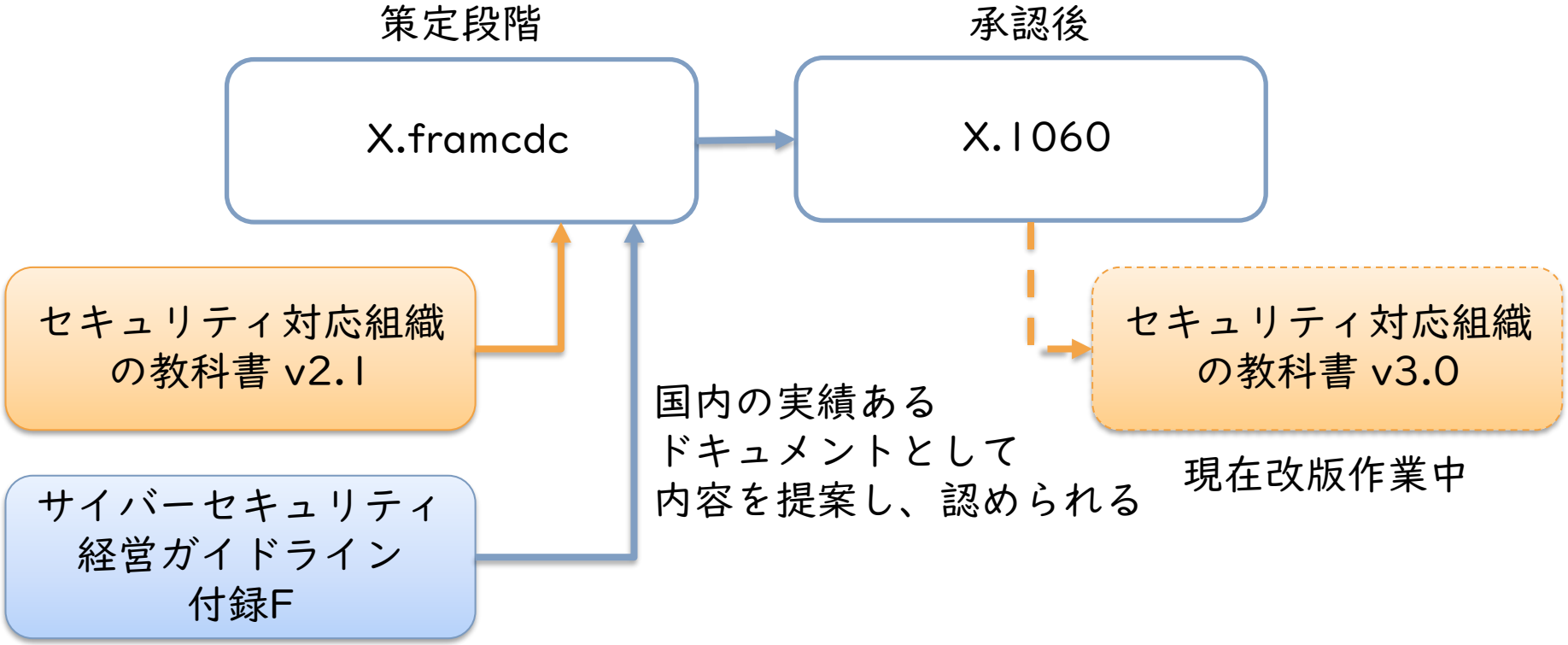
ポイント

- 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における組織体制

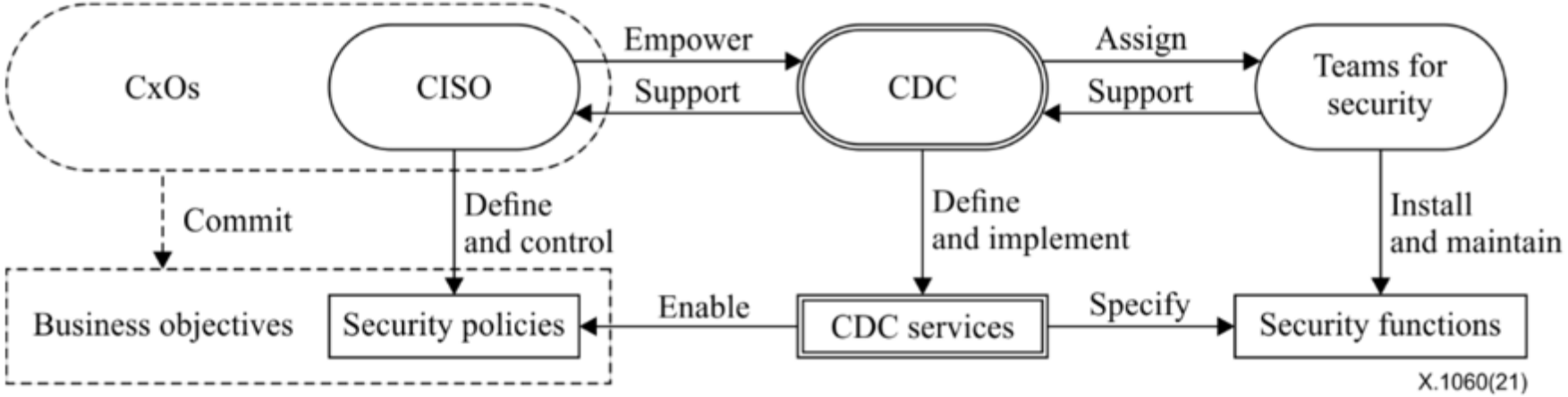


Figure 1 – Stakeholders and their roles for CDC operation

日本のドキュメントとの比較

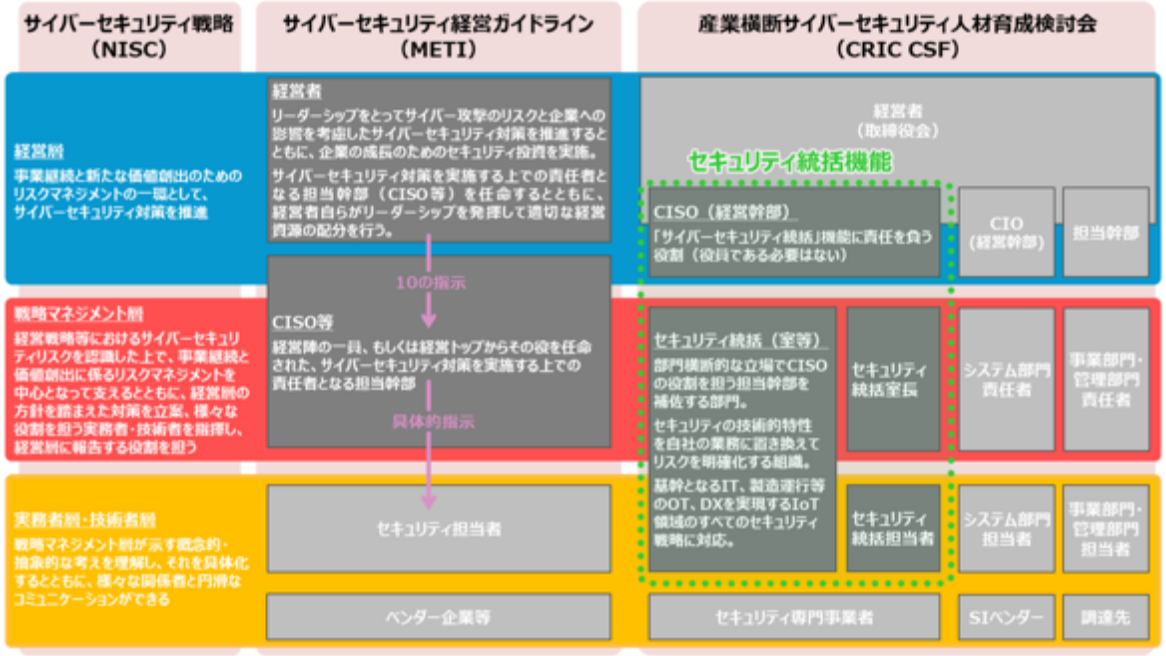


図 5　セキュリティ統括機能の位置付け（1）

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

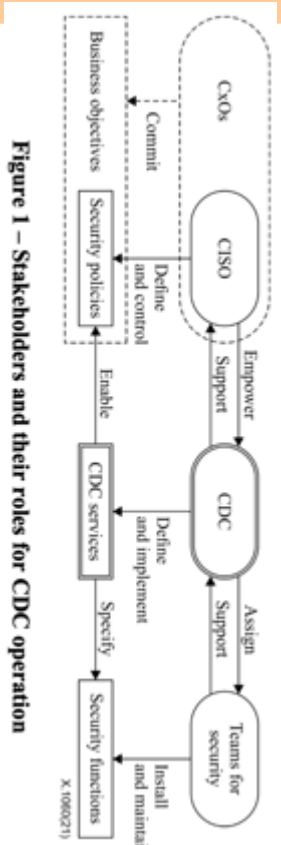


Figure 1 – Stakeholders and their roles for CDC operation

フレームワーク概要

構築

評価

マネジメント

Service list	Service catalogue	Service profile	Service portfolio
Build process			
Evaluation process		Management process	
Gap analysis		Phases	Cycles
Assessment		Strategic management	Long cycle
Assignment		Operation	Short cycle
Recommendation level		Response	

X.1060(21)

Figure 2 – Framework for the creation and operation of a CDC

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。

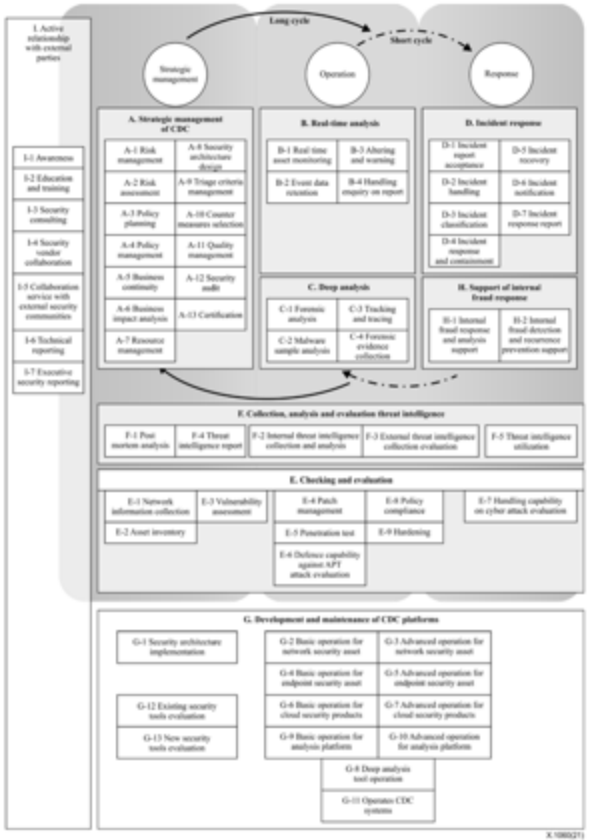


Figure 8 – CDC service categories

構築プロセス：サービスのアサイン

X.1060

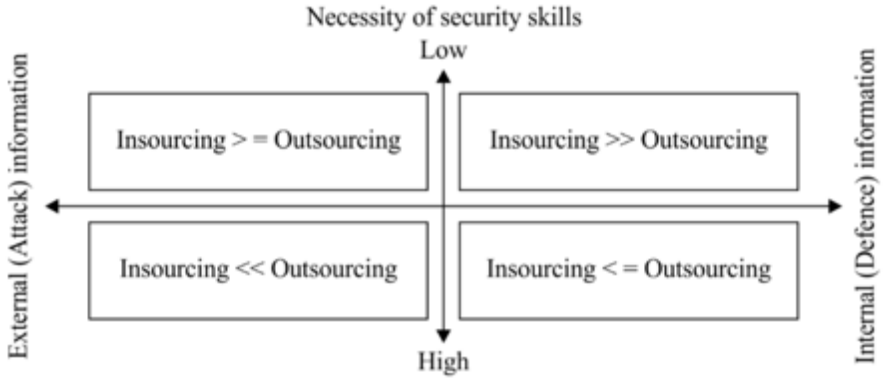


Figure 5 – Sourcing quadrants

ISOG-J

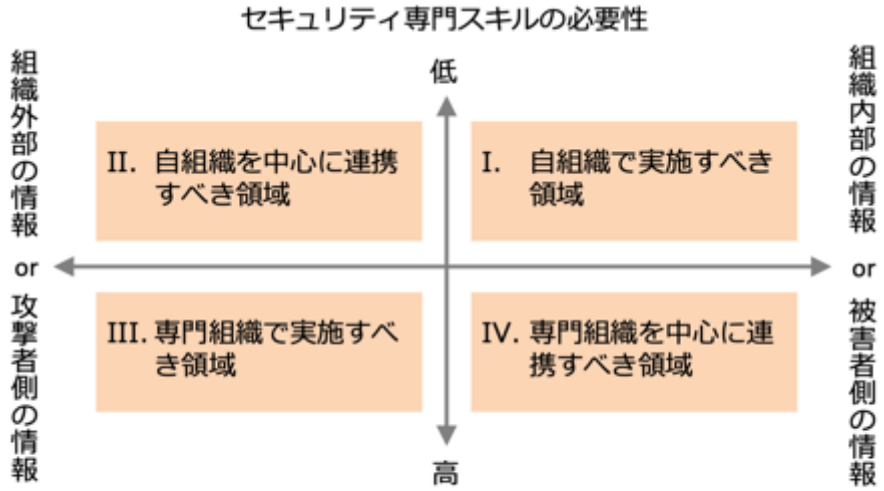


図 4　セキュリティ対応の4領域

構築プロセス：サービスのアセスメント

X.1060

Table 3 – CDC service scores

For insource	
Documented operation is authorized by CISO or other organizational director who has appropriate responsibilities	+5 points
Operation is documented and others can play the role of existing operator	+4 points
Operation is not documented, and others can play the partial role of existing operator temporarily	+3 points
Operation is not documented, and the existing operator can play role	+2 points
Operation is not working	+1 point
Decided not to implement by insourcing	N/A

For outsource	
Content of service and expected output are understood and their outputs are as expected	+5 points
Content of service and expected output are understood but their outputs are not as expected	+4 points
Either content of service or expected output is not understood	+3 points
Both content of service and expected output are not understood	+2 points
Nether output nor report is not reviewed	+1 point
Decided not to implement by outsourcing	N/A

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

X.1060 日々の改善を実行する ISOG-J

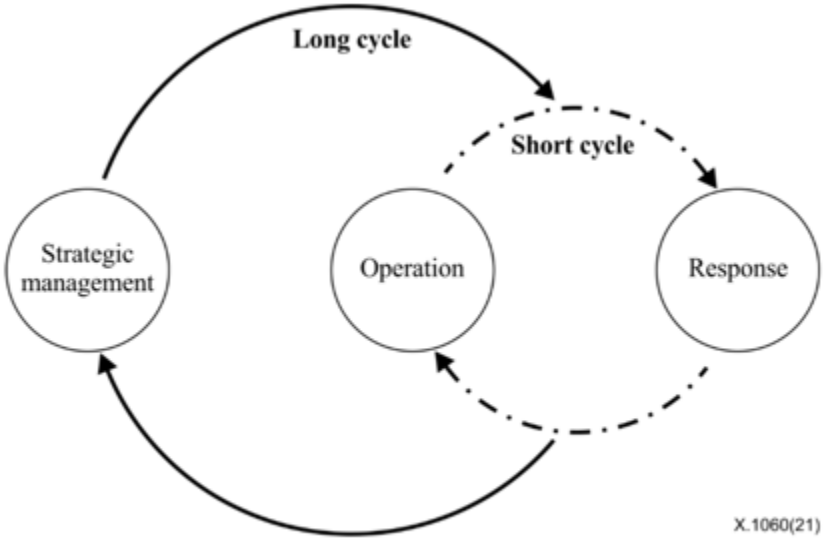


Figure 6 – CDC management process

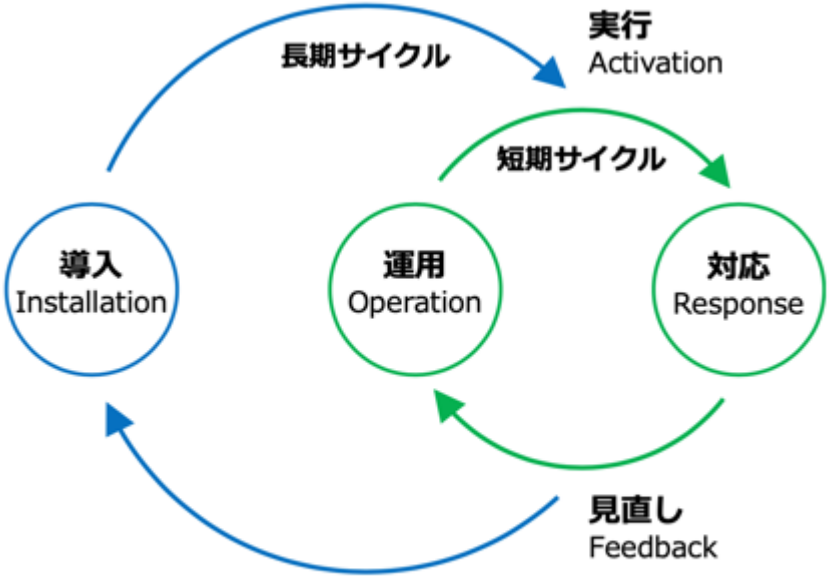


図 1　セキュリティ対応実行サイクル

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

構築

評価

マネジメント

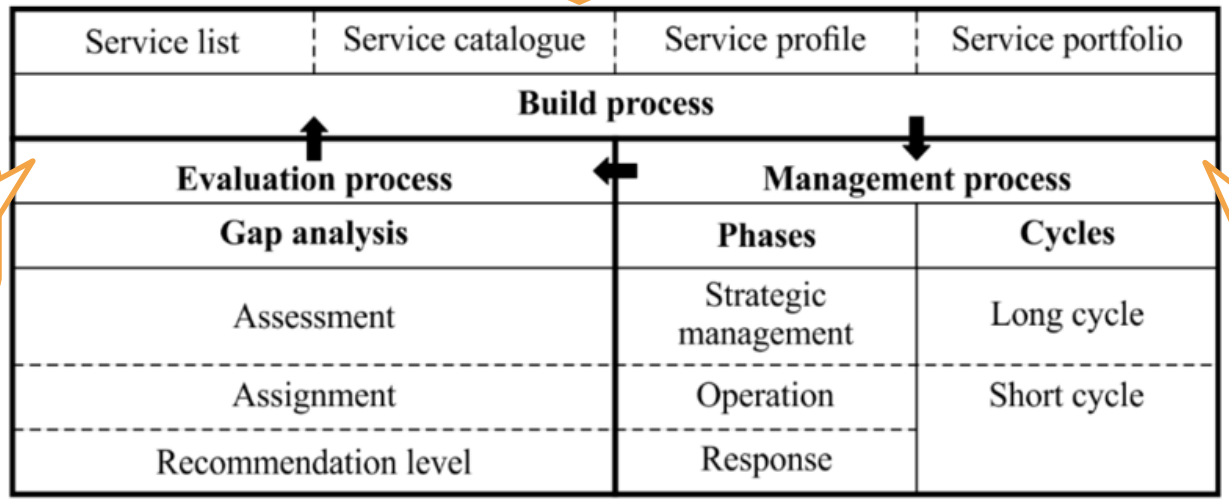


Figure 2 – Framework for the creation and operation of a CDC

まとめ

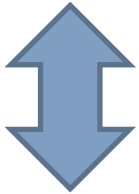
- 新しい組織を作るわけではなく、現在のSOCやCSIRTを包含した今後のセキュリティの組織の形

- 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)

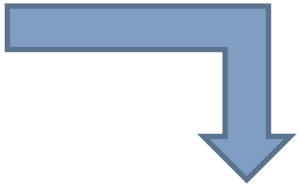
X.1060：国際標準のフレームワーク



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

ISOG-J ホームページ
https://isog-j.org
よりダウンロード可能

セキュリティ対応組織の教科書も更新を予定しています