

C47 これからのセキュリティ組織の 道標（みちしるべ）

InternetWeek2022

ISOG-J



NTTテクノクロス株式会社
セキュアシステム事業部/クロステックセンター 開発技術部門(SENG)/
情報セキュリティ推進部 TX-CSIRT/経営企画部 広報室
エバンジェリスト

武井 滋紀

日本セキュリティオペレーション事業者協議会(ISOG-J) 副代表、WG6 リーダー
InternetWeekプログラム委員(2017-2022)

ITU-T SG17 WP3 Q3 X.1060 Editor
NTTグループ セキュリティプリンシパル
情報処理安全確保支援士(009938)
(ISC)2 CISSP, CCSP

ネットワークに関連したシステムの開発や構築を経てセキュリティに関連した業務へ。各社のセキュリティ運用体制などのコンサルティングに従事するとともにエバンジェリストとして活動。

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、2022年11月現在 61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: いそぐじえい

本日のポイント

- 新しい概念ではあるが、日本ではこれまでの取り組みの延長で進めることは可能
- これまでにある様々なドキュメントやガイドラインの使い所には気を付ける
- できるところから始めて、継続的に改善を続ける

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構築・運用のフレームワーク」

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)を構築と管理をし、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。

あれから1年

X.1060の公開とInternetWeek2021から1年

- 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TTC標準規格となった。
- 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

使われ始めたX.1060

- 参照し始める国、参考にしたいという地域
- もう使ってみたという国
- ITU-T SG17の他の勧告の策定で参照される

なるほど、わからん

X.1060/JT-X1060を使いこなすためには

そこに至る背景

使うメリット

X.1060/JT-X1060
フレームワーク

どう使ったらいいか??

詳細に書かれていない背景

情シスの
一部



SOC /
CSIRT



セキュリティ統括
サイバーディフェンス
センター

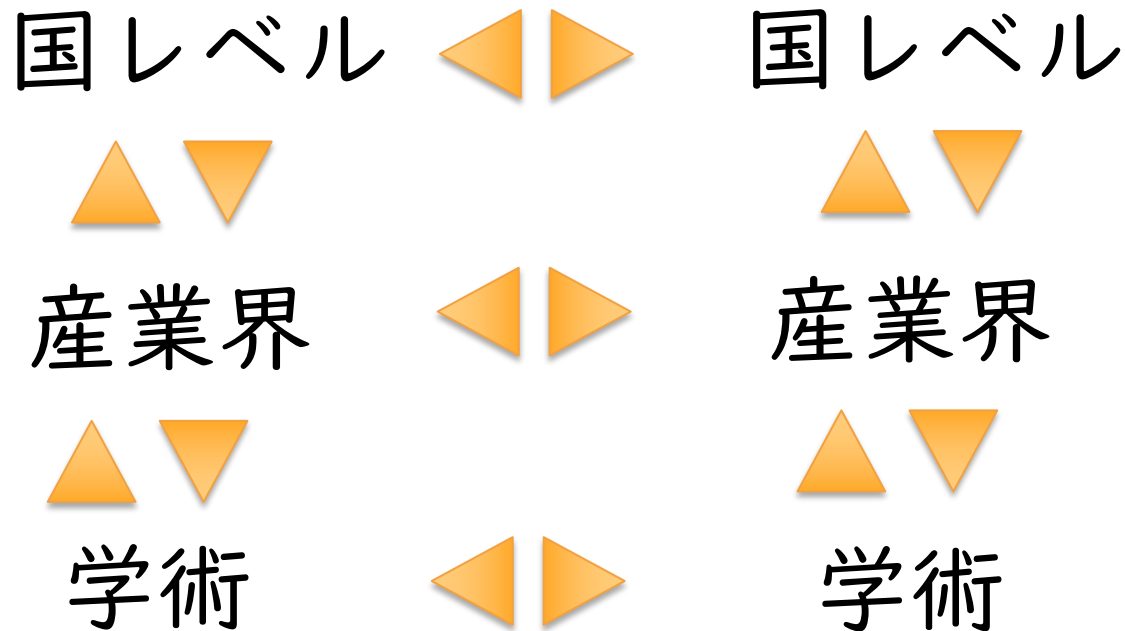
ビジネスリスクとしてのセキュリティの対応へ

対応する部署や組織の拡大・連携

親会社・子会社、海外支店、国内外の取引先

X.1060/JT-X1060を使うメリット

国際レベルでやるべきことの共通の認識を持つ



X.1060/JT-X1060はどう使ったらいいか？

よく聞かれること

- サイバーディフェンスセンターって何？
- この文書の使い所はどこか？
- すでにSOC/CSIRTがあるのですが
- 我々はすでに***を参考にしています
- 日本で使うならどうしたらいいの？

サイバーディフェンスセンター？

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。



これからのセキュリティ対応組織を定義したもの。
組織によって名前は様々。

今でもSOC/CSIRTの定義は組織ごとにバラバラ

日本では？

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2.0版)

https://www.meti.go.jp/policy/netsecurity/mng_guide.html



「セキュリティ統括」にマッピングされる

新たな組織を作るのではなく、これまでの取り組みの延長線上にある。

X.1060/JT-X1060における組織体制

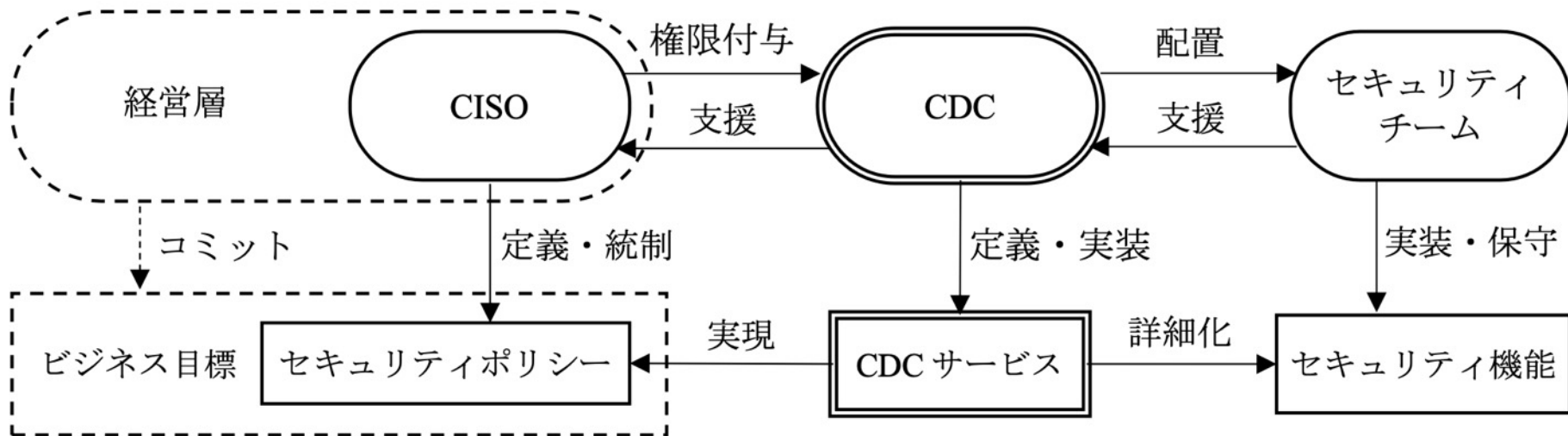


図1 CDCの運営における関係者とその役割

図はJT-X1060より

日本のドキュメントとの比較

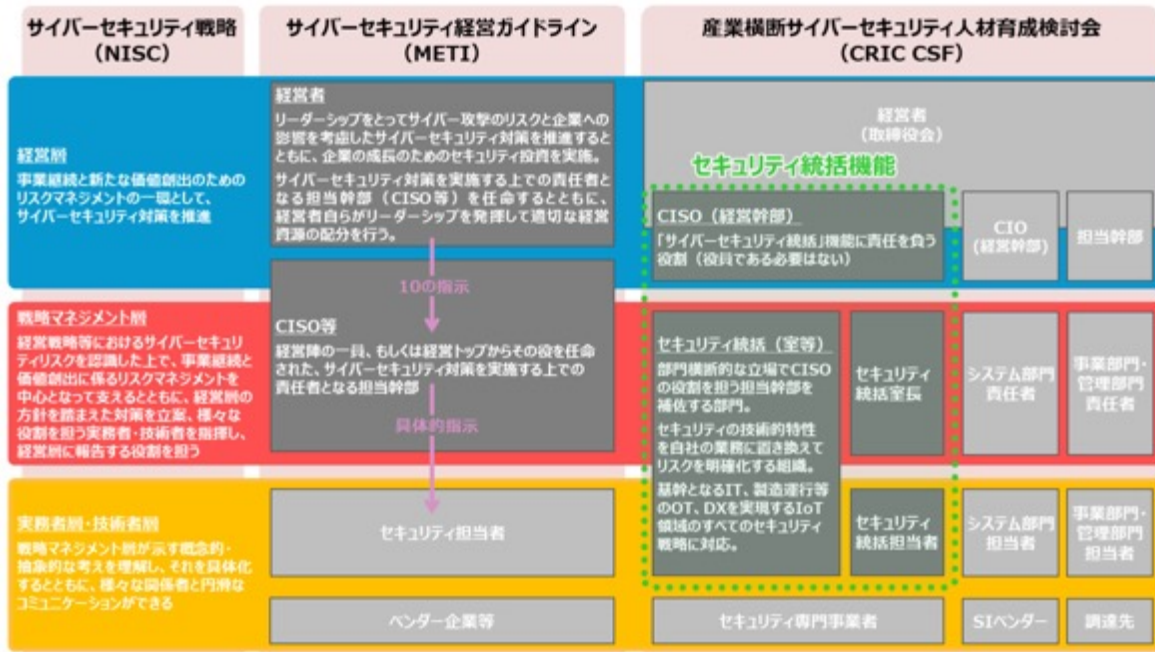
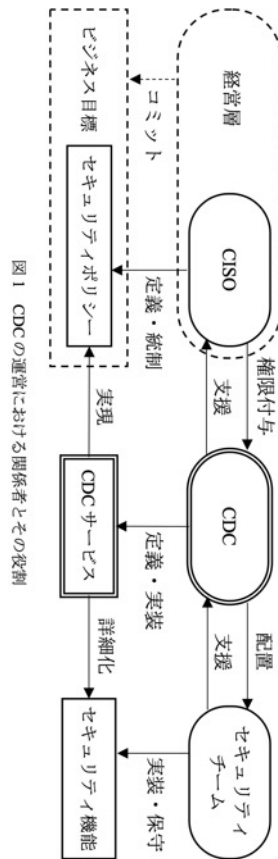


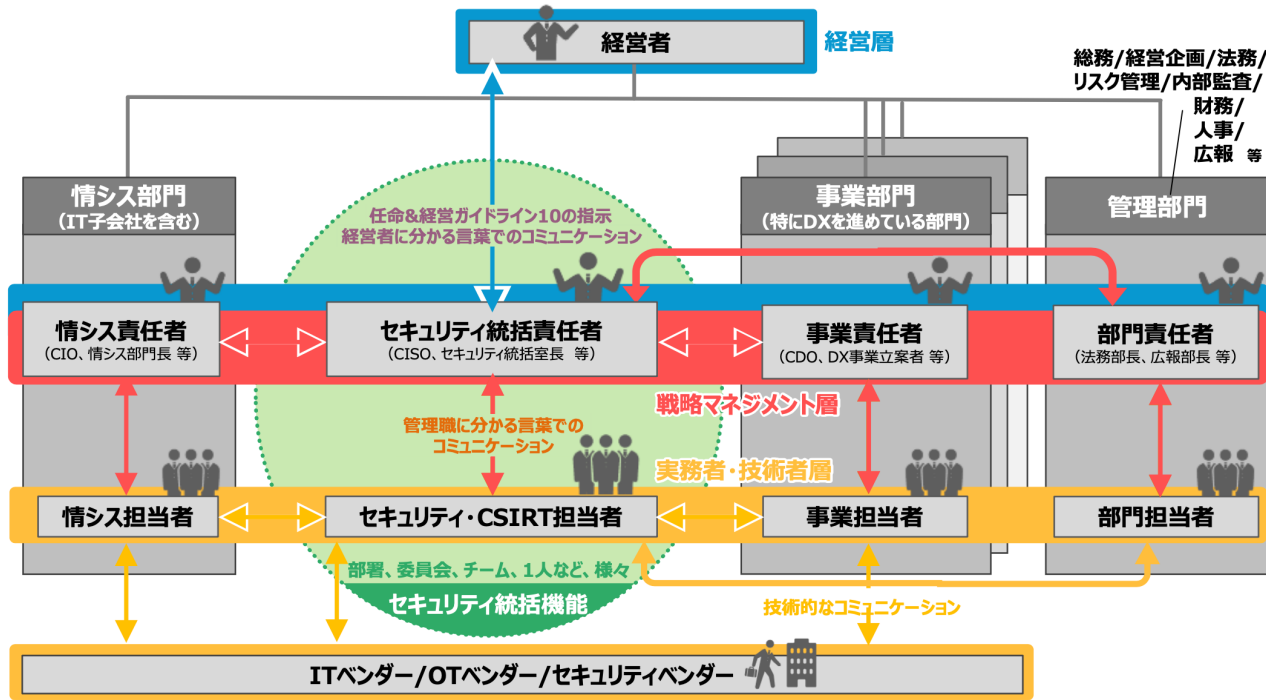
図5 セキュリティ統括機能の位置付け (1)

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



セキュリティ統括機能のイメージ

図表8 セキュリティ統括機能のイメージ



横の連携

担当、ベンダーとの連携

組織をどう作るかの全体の流れ

経営層

サイバーセキュリティ経営ガイドラインを読む
10の指示を理解する。CISOを任命し権限を付与する



CISO

指示に従いセキュリティ体制を構築する
セキュリティポリシーを決める
X.1060/JT-X1060など参考にする



セキュリティ統括

サービスの割り当て・権限の付与、各チームと連携する
X.1060/JT-X1060など参考にする



セキュリティチーム

割り当てられたサービスのプロセスや手順を実装する
各種ガイドラインや手順などを参考にする

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

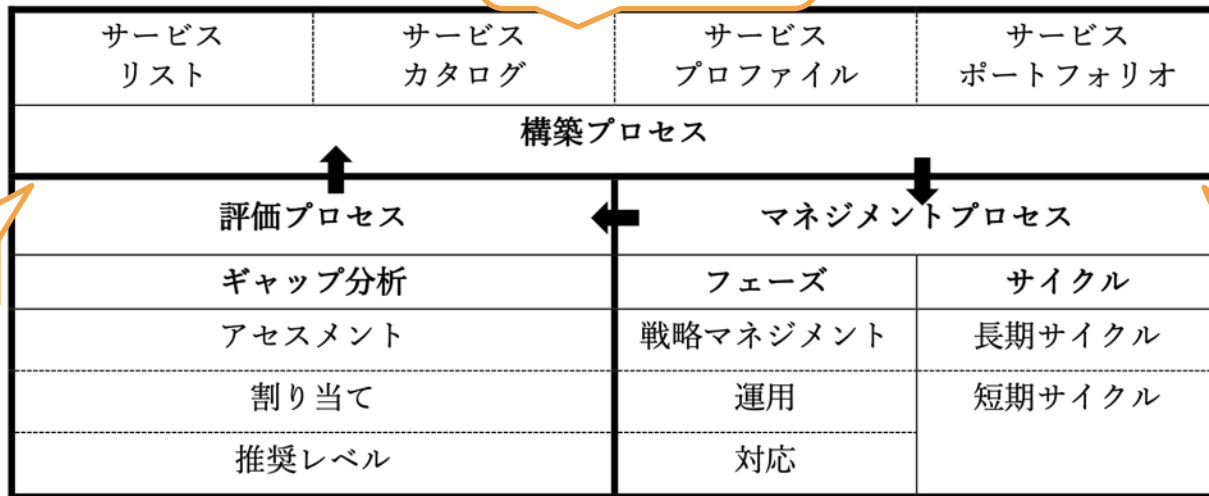
ポイント

- X.1060/JT-X1060はセキュリティ対応の全体の体制をどう構成するか
の文書
 - これ1つでSOCができるとかCSIRTができるという位置付けのものではない
- すでにSOC/CSIRTがあるのですが
 - これからの組織体制を示したもので、SOC/CSIRTの内容も含むので、できている部分は良いとして、今後どうするか
の参考に。
- 我々はすでに*** を参考にしています。
 - それぞれのドキュメントは使い所があるので、それぞれに合ったレイヤーや場所
で参照いただければと思います

使ってみた、時の話

フレームワーク概要

構築



評価

マネジ
メント

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

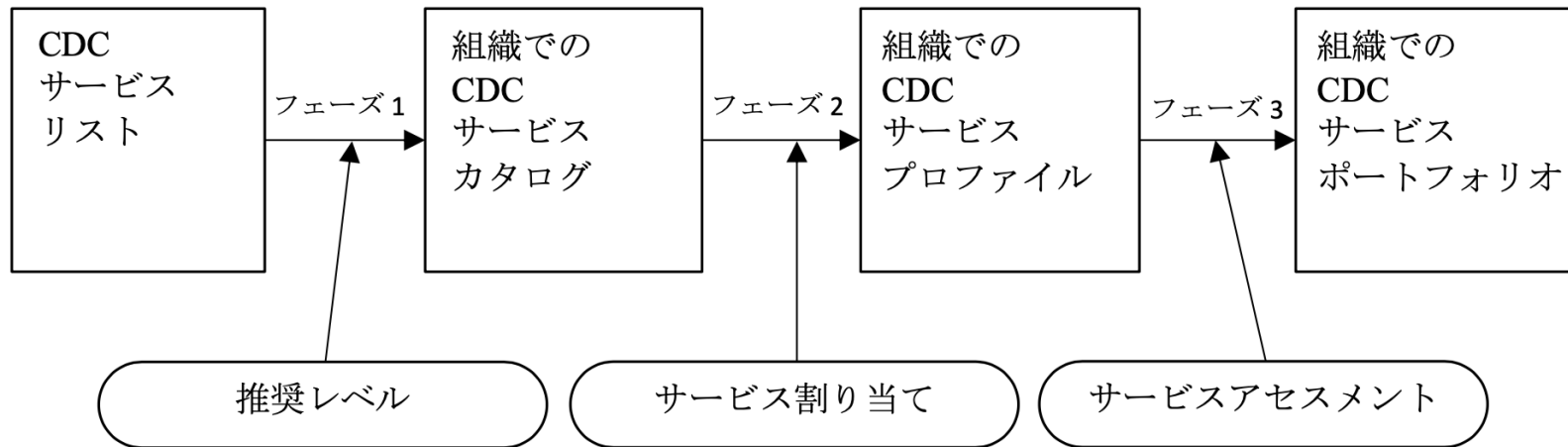


図3 CDCサービスの立ち上げフェーズ

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

構築プロセス時 サービスを選ぶ

9つのカテゴリー、64のサービスから実施すべきものを選択
選択時に実施する推奨レベルも設定する



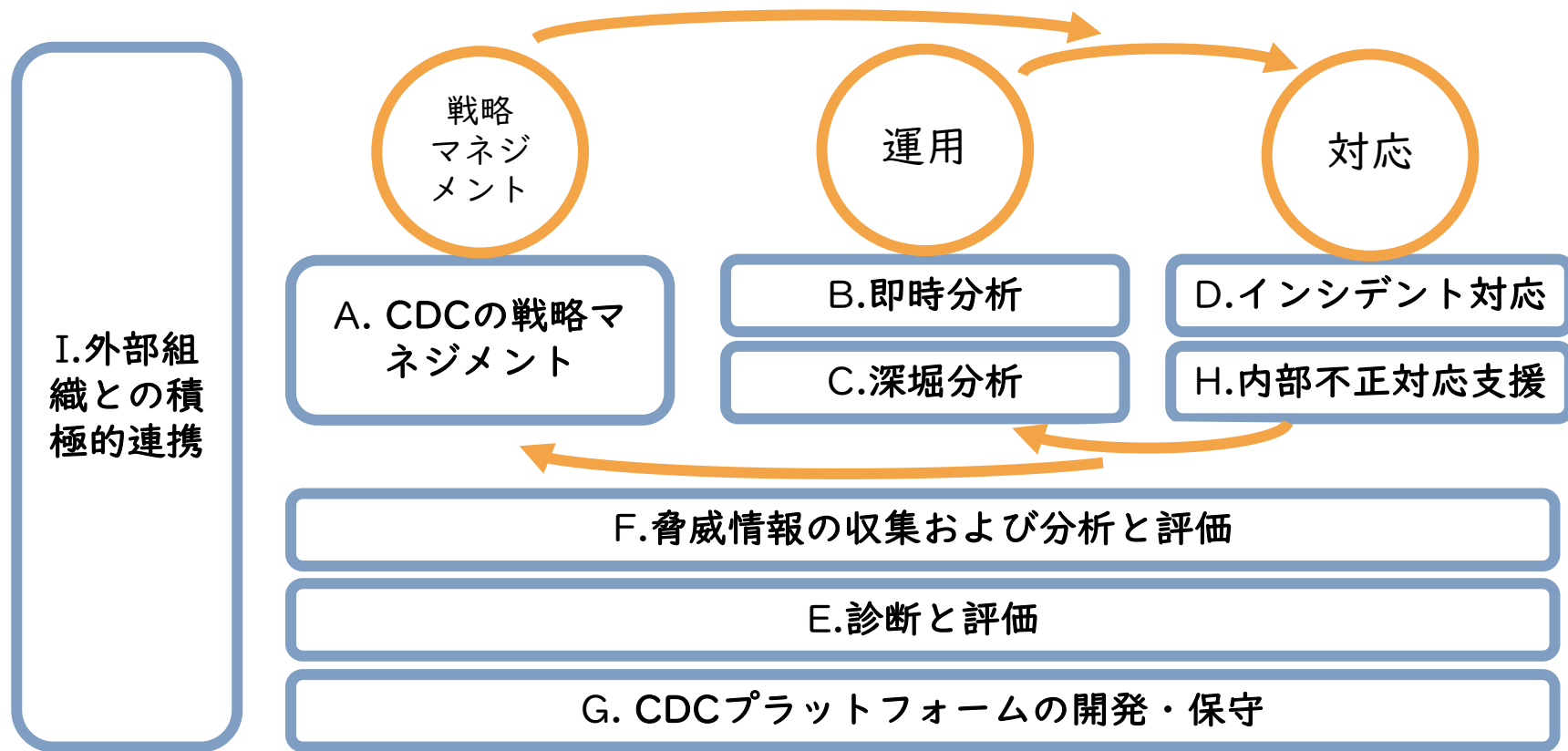
今、すでにやっているものをマッピングしておく

後段のマネジメントプロセスが実施できるように選んでおく

必要だが一覧になれば独自で追加する

推奨レベルは自組織でどの程度必要かを基準にする

サービスカテゴリーとマネジメントプロセスとのマッピング



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

構築プロセス時 どこで行うかを定める

全部自分達でできない！

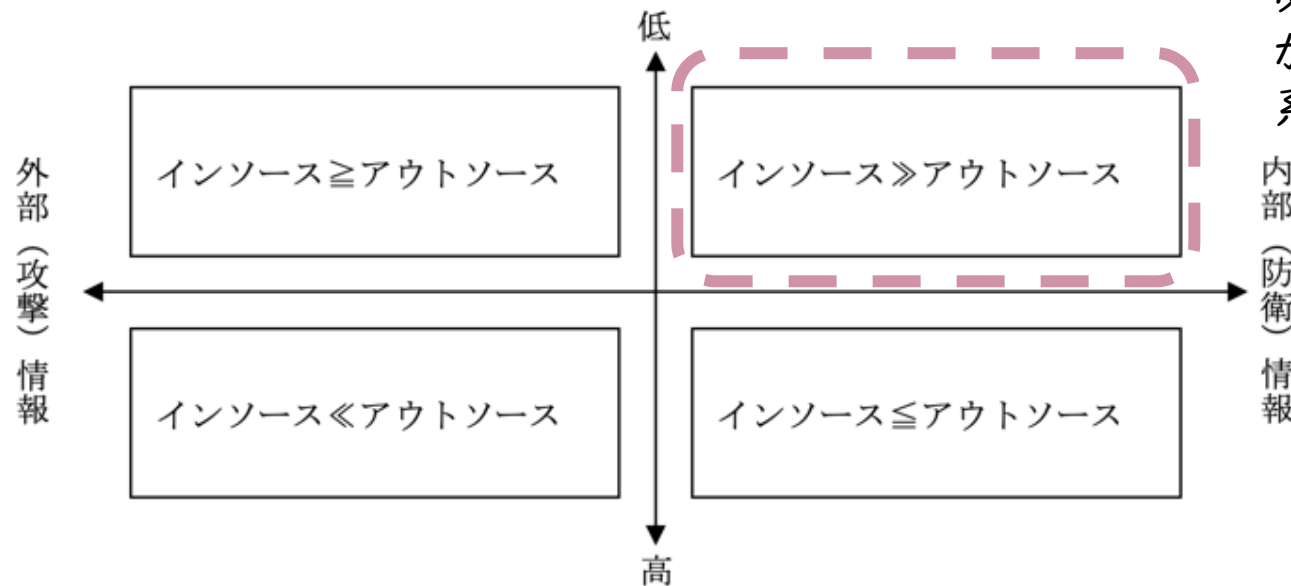


最低限やるべきことは行い、あとはアウトソースする

全てアウトソースすることはおすすめされない

構築プロセス：サービスのアサイン

セキュリティ専門スキルの必要性



セキュリティ専門スキルの必要性が低い、内部の情報を中心となるマネジメント系を中心に自前で実施する

判断や責任を持つのは自組織であることを意識

図5 調達の対象

図はJT-X1060より

構築プロセス時 スコアを決める

最終的には、サービスポートフォリオの一覧を作る

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
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→

図はJT-X1060より

構築プロセス：サービスのアセスメント

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

セルフアセスメント
 今のスコア
 目標のスコア
 2つを決める

図はJT-X1060より

マネジメントプロセス

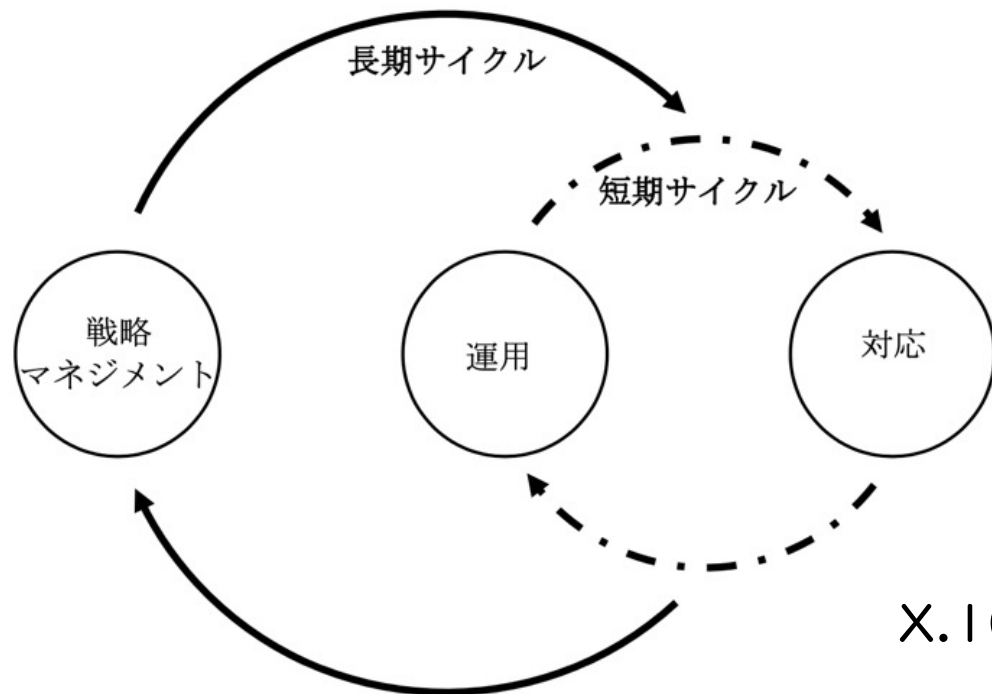


図6 CDC マネジメントプロセス

サービスは具体的にどんなプロセス、どんな手順??

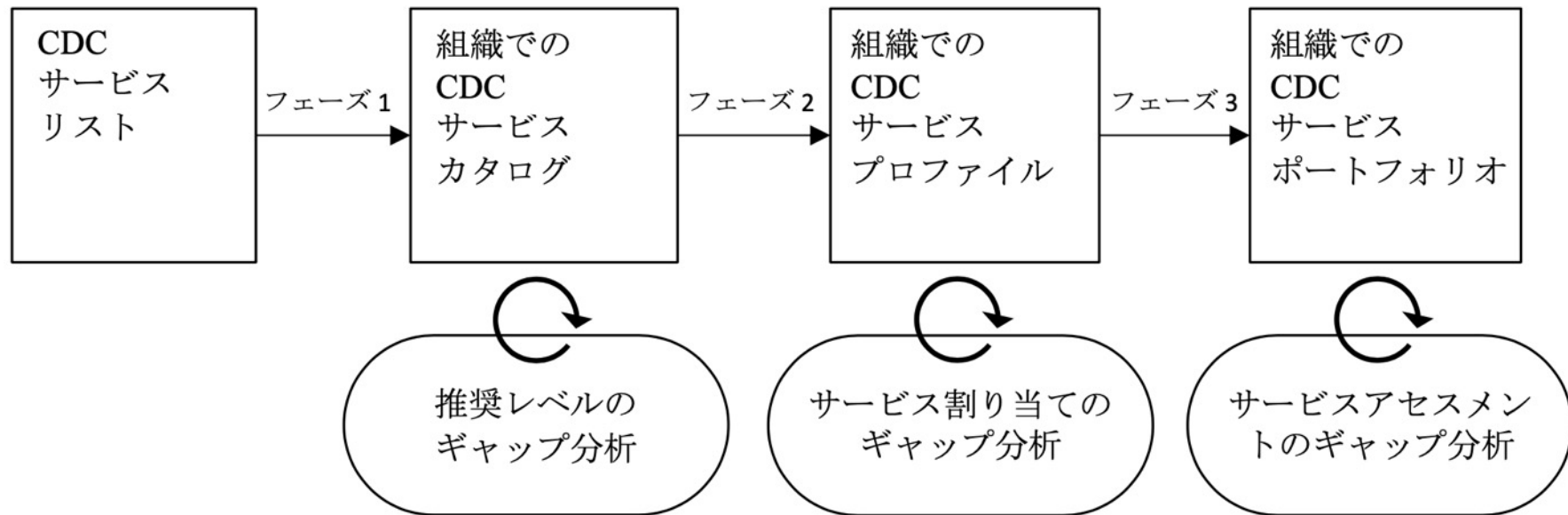


既存のドキュメントやガイドライン、すでに参考に使っているものがあればそれを活用する

X.1060/JT-X1060は全体として
どうするかのみ記載

図はJT-X1060より

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定める

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？

どこで行うかを定める（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？

評価プロセス

評価のタイミングは？



それぞれの組織次第です。監査などで決まっていればそれを活用しても良いです

ビジネスの環境の変化のタイミングで随時見直すのがスムーズに対応できるでしょう

評価プロセス

課題があるのはわかっているが、変えられない！



適切に権限は委譲されていますか？

継続的に改善を続けるフレームワークです。

本日のまとめ

- 新しい概念ではあるが、日本ではこれまでの取り組みの延長で進めることは可能
 - 組織の名前の問題ではなく、何をするかを重視する
- これまでにある様々なドキュメントやガイドラインの使い所には気を付ける
 - これ一つでOKというものはない。自分達に合ったものを利用する
- できるところから始めて、継続的に改善を続ける

- ・本資料の著作権は日本セキュリティオペレーション事業者協議会(以下、ISOG-J)に帰属します。
- ・引用については、著作権法で引用の目的上正当な範囲内で行われることを認めます。引用部分を明確にし、出典が明記されるなどです。
- ・なお、引用の範囲を超えられる場合もISOG-Jへご相談ください(info (at) isog-j.org まで)。
- ・本文書に登場する会社名、製品、サービス名は、一般に各社の登録商標または商標です。®やTM、©マークは明記しておりません。
- ・ISOG-Jならびに執筆関係者は、このガイド文書にいかなる責任を負うものではありません。全ては自己責任にてご活用ください。