C23 あつまれ！セキュリティ運用ピーポー

あつまれ！X.1060ピーポー！
～セキュリティ対応組織の教科書の活用～

2024.7.26

ISOG-J 武井滋紀

NTTテクノクロス株式会社
セキュアシステム事業部/デジタル革新部　開発技術部門/
経営企画部 情報セキュリティ推進部門　TX-CSIRT
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(2017-2024)

ITU-T SG17 WP3 Q3 X.1060-rev Editor, Sup-cdc 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)
ISC2 CISSP, CCSP
ISACA CISA

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、2024年7月現在 67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)
- https://isog-j.org/
  - Facebook ページ: /isogj
  - ISOG-J の読み方: いそぐじぇい

本日のポイント

- 構築フェーズで補足が入ったよ！
- 付録がついたよ！
- 実はまだ議論しています

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”

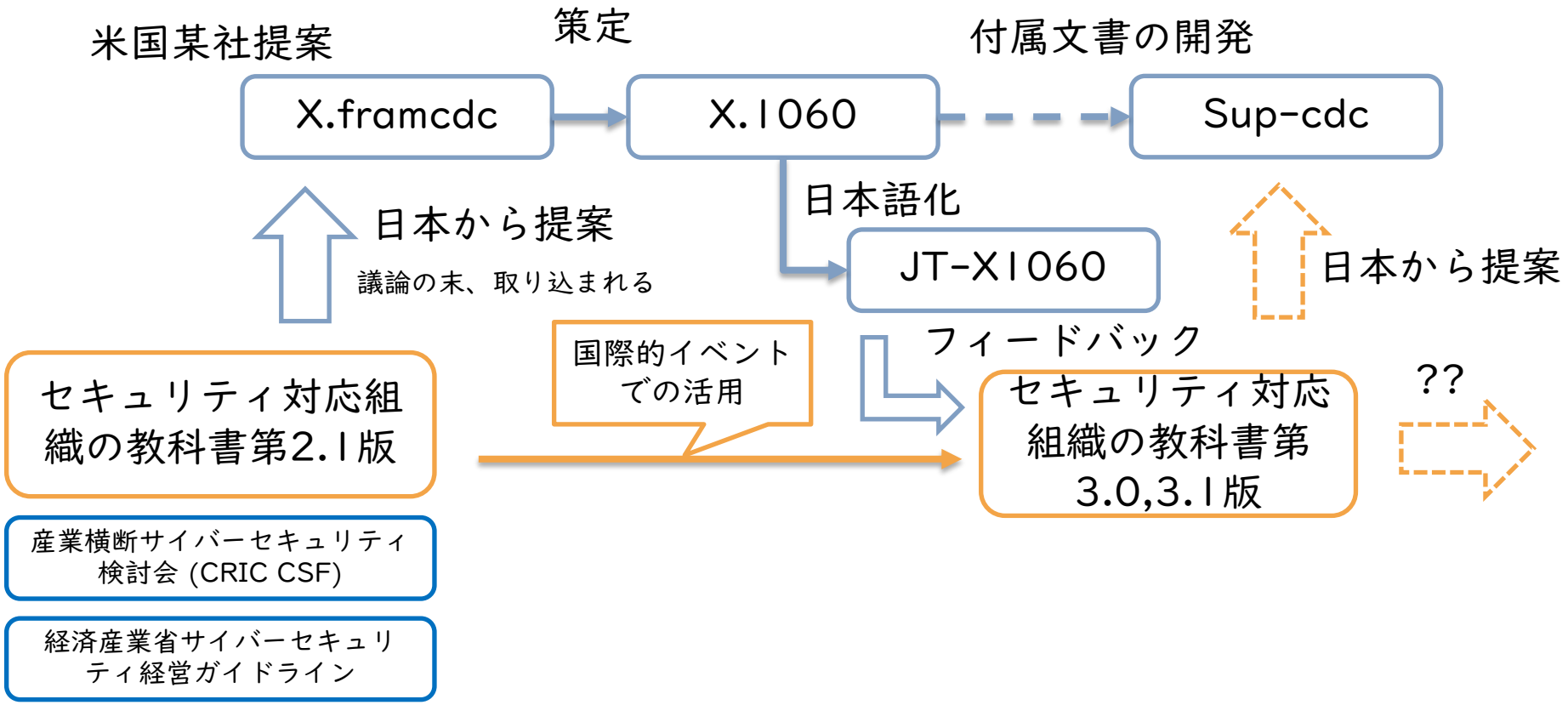
配布URL: https://www.itu.int/rec/T-REC-X.1060-202106-I

2022年2月に情報通信技術委員会(TTC)でJT-X1060がTTC標準規格に

「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」

日本語版配布URL:
https://www.ttc.or.jp/document_db/information/view_express_entity/1423

成り立ち



ITU-T 勧告 X.1060

- 2021-6-29承認, 2021-10-11英語版公開
  - アラビア語、中国語、スペイン語、フランス語、ロシア語でも公開
- 日本側関係者
  - 武智 洋, コントリビューター, 日本電気株式会社
  - 阿部 慎司, エディタ, GMO サイバーセキュリティ byイエラエ株式会社
  - 武井 滋紀, エディタ, NTTテクノクロス株式会社
  - 永沼 美保, ITU-T SG17 WP3 Q3ラポータ, 日本電気株式会社

- ITU-T SG17内特設ページ
  - https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/X1060.aspx

特設ページのロゴも日本から！

ロゴは阿部さんデザイン
SG17事務局から総務省に貸与依頼

Youtube JPCERT/CCチャンネル
阿部さん出演説明動画

セキュリティ対応組織の教科書　第3.1版

- 2023-10-17公開
  - https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html
- 第2.1版をITU-T勧告X.1060に合わせて改版したもの
- 執筆者
  - 早川 敦史, NECソリューションイノベータ株式会社
  - 武井 滋紀, NTTテクノクロス株式会社
  - 彦坂 孝広, NTTテクノクロス株式会社
  - 河島 君知, NTT データ先端技術株式会社
  - 阿部 慎司, GMO サイバーセキュリティ byイエラエ株式会社
  - 野尻 泰弘, NECソリューションイノベータ株式会社
  - 川田 孝紀, NTT セキュリティ・ジャパン株式会社
  - 本橋 孝祐, NTT セキュリティ・ジャパン株式会社
  - 角田 玄司,ネットワンシステムズ株式会社
  - 竹之内 一晃, パーソルクロステクノロジー株式会社
  - 青木 翔, 株式会社日立製作所
  - ISOG-J WG6 メンバー

第3.0版から
さらに
使いやすく！

付録
サービス
ポートフォリオシート
付き！

X.1060に至る背景

ビジネスリスクとしてのセキュリティ

広がり続ける組織と連携

▼

情シスの一部　　SOC / CSIRT

なんとかなれーッ！じゃない！！

Cyber Defence Centre, 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

国レベル  産業界  学術

「セキュリティ」では「何をするか」

X.1060/JT-X1060における組織体制

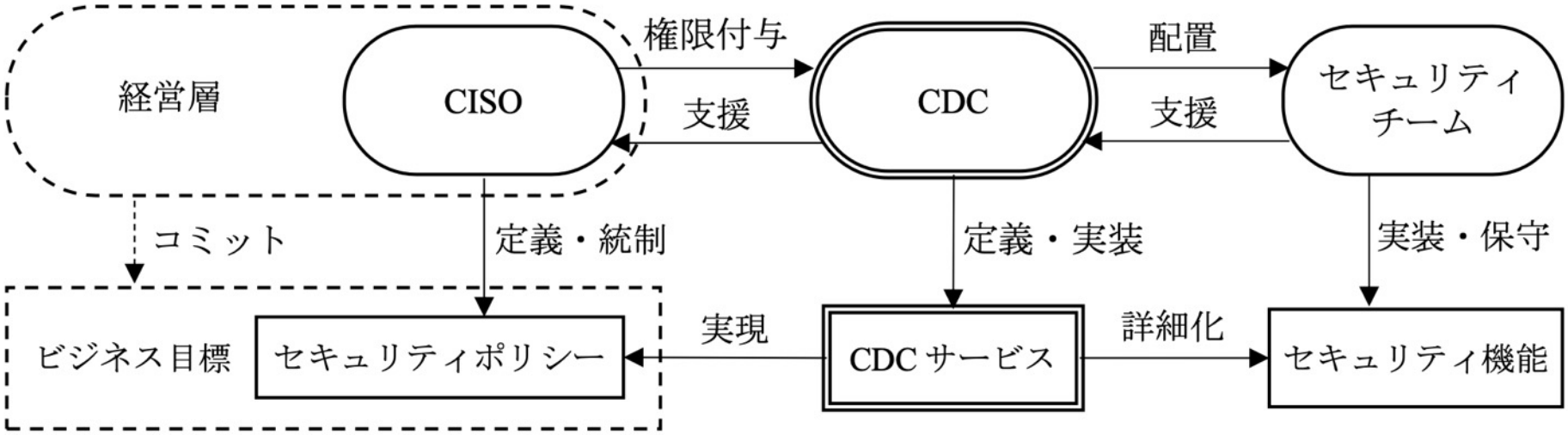
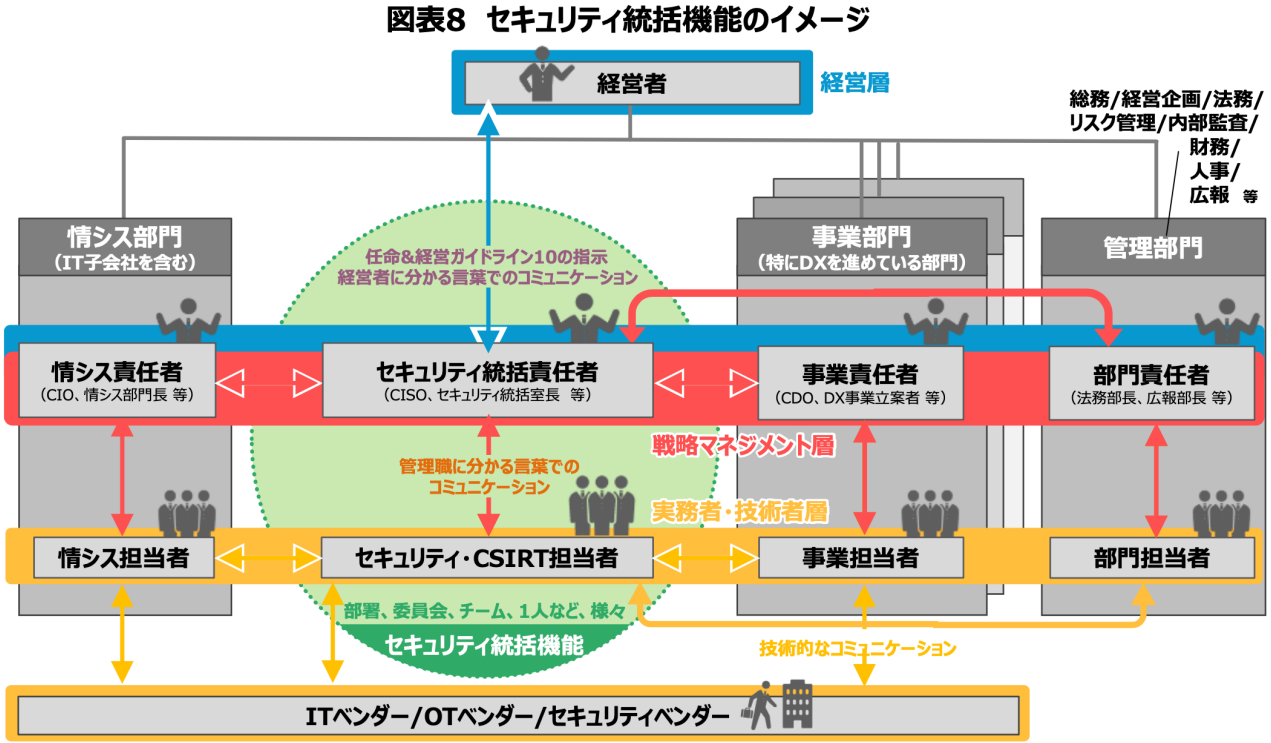


図 1　CDC の運営における関係者とその役割

図はJT-X1060より

セキュリティ統括機能のイメージ



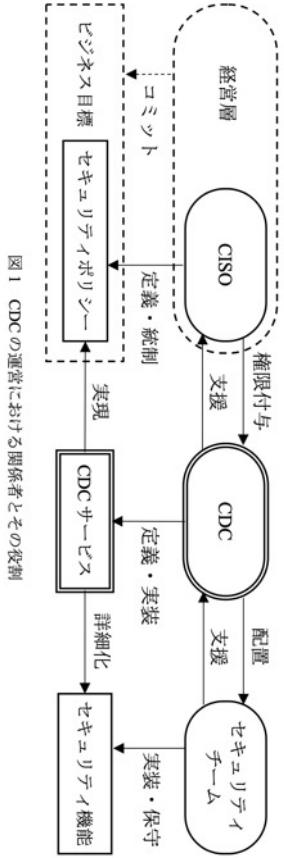


図1　CDCの運営における関係者とその役割

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

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 3.0 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

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

▼

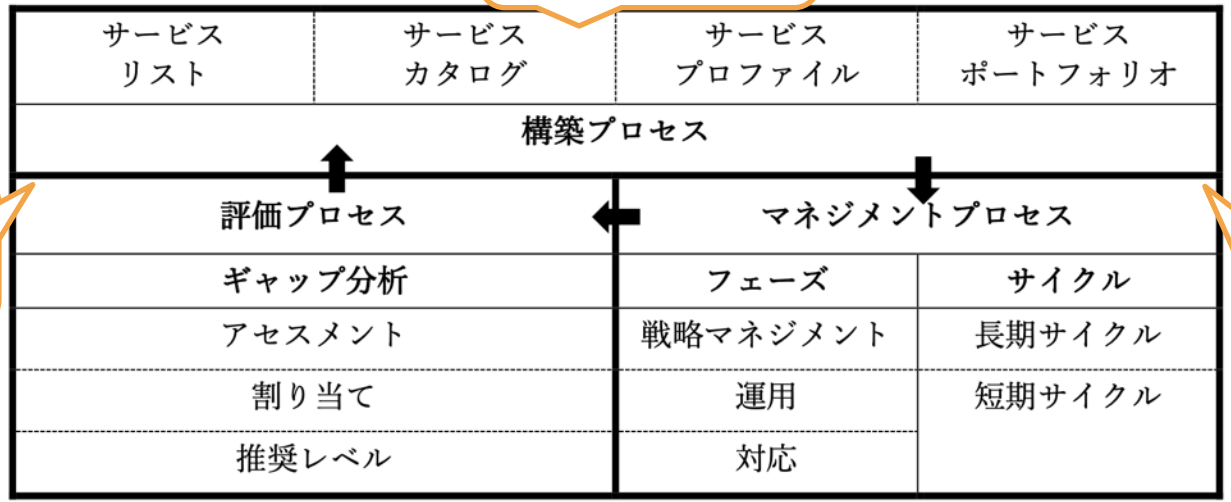
割り当てられたサービスのプロセスや手順を実装する
セキュリティチーム　各種ガイドラインや手順などを参考にする

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

構築フェーズ

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

サービスカテゴリ、サービスリスト

- 9つのサービスカテゴリ、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

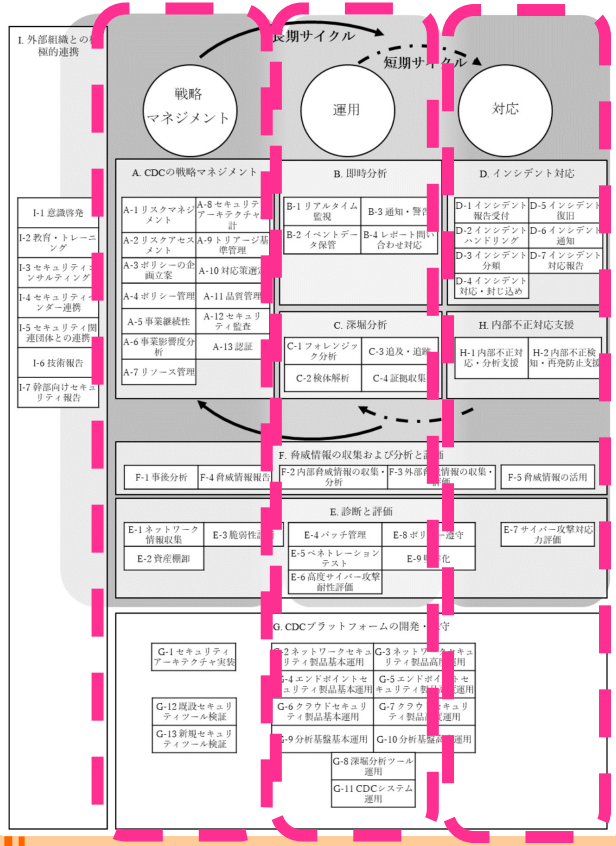
F	脅威情報の収集および分析と評価	5
G	CDCプラットフォームの開発・保守	13
H	内部不正対応支援	2
I	外部組織との積極的連携	7

第3.1版では推奨レベルの解釈を追加

表 9 X.1060/JT-X1060 の CDC サービスの推奨レベル [16] と実施すべき優先度

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 （必須）	実施すべき最低限のサービス （必ずやるべき必須のサービス）
スタンダード （標準）	一般的に実装が推奨されているサービス （標準的に必要となるサービス）
アドバンスド （推奨）	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 （よりしっかりしたセキュリティを実現するために推奨されるサービス）
オプション （任意）	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 （任意で必要となるサービス）

マネジメントプロセスでサービスを分類してみる



実は縦の意味があった

表 8「戦略マネジメント」「運用」「対応」に関連するそれぞれのカテゴリーのサービスの分類

カテゴリー	戦略マネジメント	運用	対応
A	A-1～A-13	–	–
B	–	B-1～B-4	–
C	–	C-1～C-4	–
D	–	–	D-1～D-7
E	E-1～E-3	E-4, E-5, E-6, E-8, E-9	E-7
F	F-1, F-4	F-2, F-3	F-5
G	G-1, G-12, G-13	G-2～G-11	–
H	–	–	H-1, H-2
I	I-1～I-7	–	–

セルフアセスメント、サービススコアの考え方

- 0から5
- 0：やらない、不要と判断した
  - 「判断した」ことの記録が大事

全部5にすることが正解ではない

属人でいいなら3でもいいじゃない

構築では最終的にサービスポートフォリオを作る

セキュリティ対応組織の教科書第3.1版からexcelシートをそのまま付録に

組織内の推奨レベル

どこでやるか

今のスコア

目標のスコア

サービスの解説

	A	B	C	D	E	F	G	H
1	カテゴリー	サービス		推奨レベル	サービス割り当て	サービススコア		解説文
2		項番	名称			現状(As-Is)	あるべき姿(To-Be)	
3								
4	A. CDC の戦略マネジメント	A-1	リスクマネジメント					「リスクマネジメント」サービスは、リスクに対して組織を方向づけ、コントロールできるよう、A-2からA-13を含む統括的な活動を実現する。
5		A-2	リスクアセスメント					「リスクアセスメント」サービスは、組織の資産や脅威、セキュリティ対策の観点から、組織のリスクレベル把握を実現する。
6		A-3	ポリシーの企画立案					「ポリシーの企画立案」サービスは、具体的なセキュリティポリシーの定義や、ガイドラインの作成に関するすべての活動を支援する。
7		A-4	ポリシー管理					「ポリシー管理」サービスは、ポリシーや組織の規定を評価して定期的に見直しや、新たな外部要件（例えば、規制やガイドライン）への準拠を実現する。
8		A-5	事業継続性					「事業継続性」サービスは、組織の事業継続計画の実現や実行が正しく行われるために必要な経営上の機能を支援する。
9		A-6	事業影響度分析					「事業影響度分析」のサービスは、様々なイベントやシナリオから起こり得る影響の体系的なアセスメントを実現する。このサービスは、発生しうる損失の規模を組織が理解するのに役立つ。直接的な金銭的損失だけでなく、利害関係者の信頼喪失や風評被害など、その他の影響も対象となる場合もある。
10		A-7	リソース管理					「リソース管理」サービスは、各種セキュリティ活動を支えるリソース（人、予算、システムなど）計画と、各サービスへの適切な割り当てを実現する。
11		A-8	セキュリティアーキテクチャ設計					「セキュリティアーキテクチャ設計」サービスは、ビジネスをセキュアにするためのアーキテクチャの確立を実現する。システムの設計やビジネスプロセスの制約（例えば、サプライチェーン）を考慮した各種セキュリティ対策をまとめ、CDCのプラットフォーム（カテゴリーGにあるような）の開発や維持を実現する。

マネジメントフェーズ

マネジメントプロセス

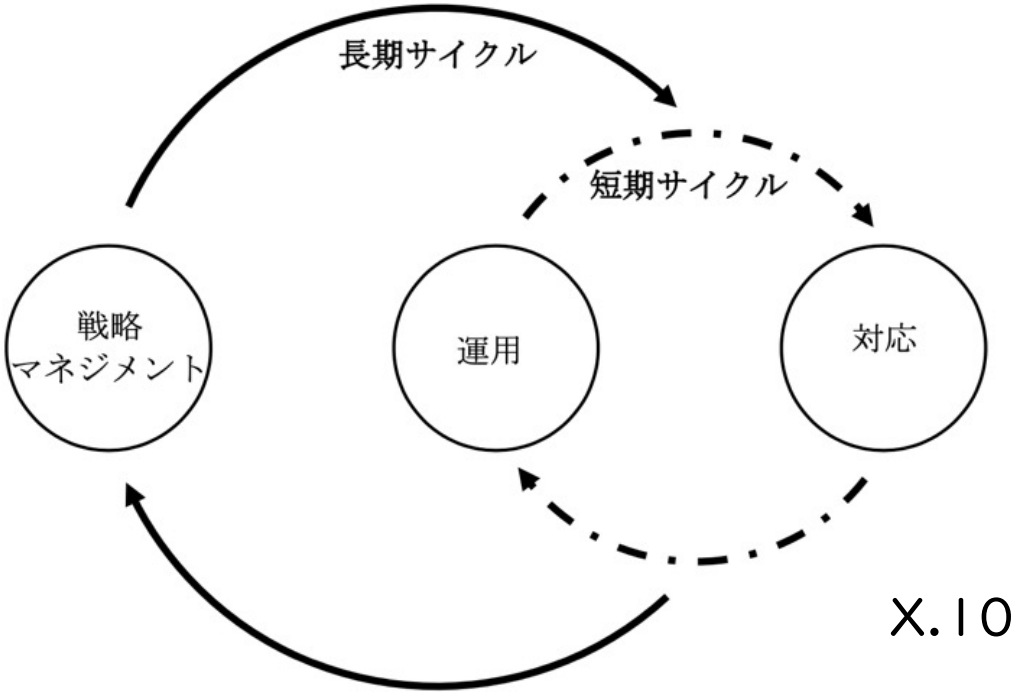


図 6　CDC マネジメントプロセス

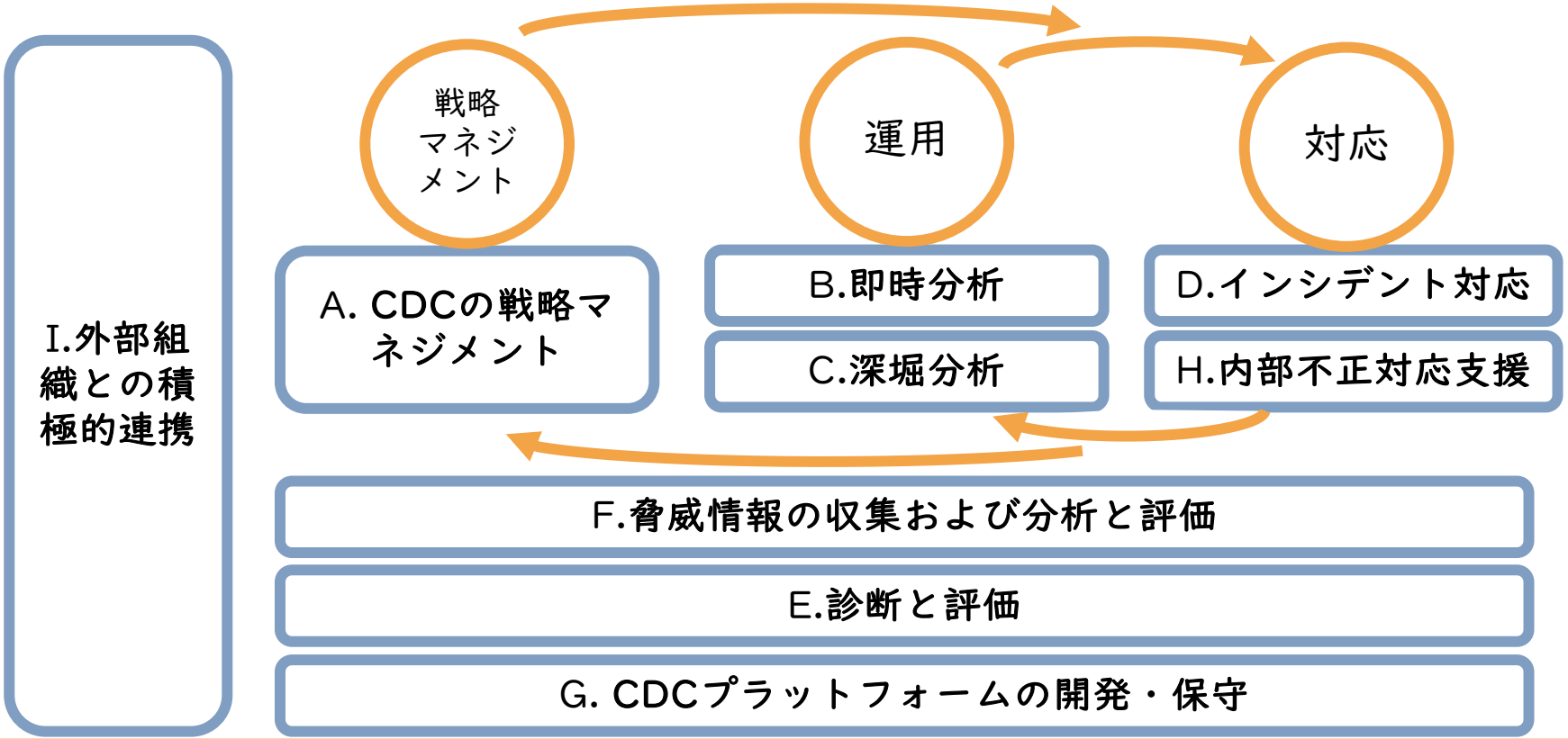
サービスは具体的にどんな
プロセス、どんな手順？？

既存のドキュメントやガイドライン、すでに参考にし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

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



評価フェーズ

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）

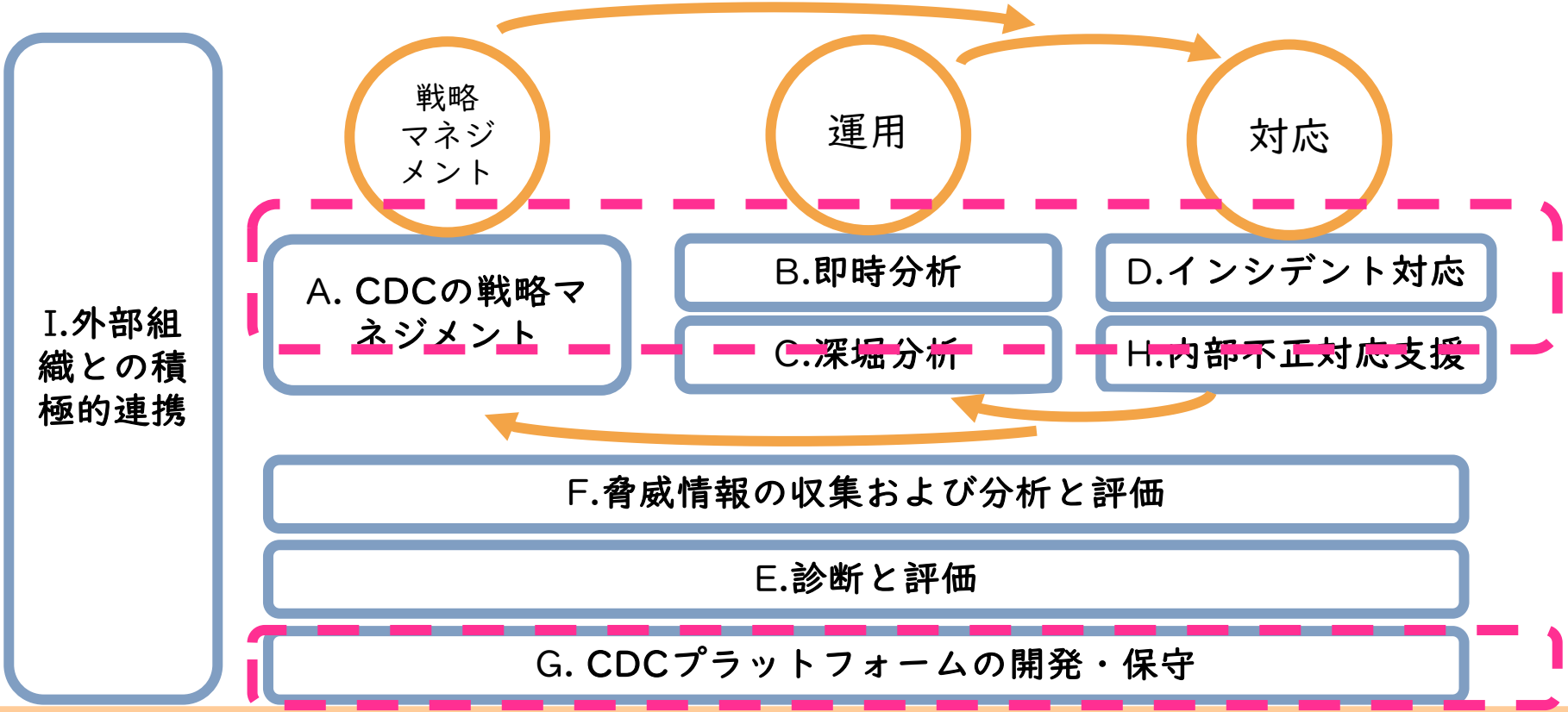
- それぞれのサービスのスコアをセルフアセスメントで測る

今のスコアはどうなった？
目標は変わったか？

よくある話

- 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

64は多い！どれからやれば良い？



懸念していること

- セキュリティの部署（チーム）は、ある（って言ってる）
  - 見ている範囲の認識は合っていますか？
- 改善したいができない
  - 権限は委譲されていますか？
  - 状況（社外、法規制、攻撃方法）は常に変化しています
- 「親会社や取引先からこれをやれば良い、というリストがある」
  - それは最低限取引のためにやるべきもの。自組織や会社全体として必要なことはできていますか？

使い方のポイント

- 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
  - 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

本日のまとめ

- 構築フェーズで補足が入ったよ！
  - どれをどこでどれくらいやる、は難しい
- 付録がついたよ！
  - 活用お願いします！
- 実はまだ議論しています
  - **3.2版がほぼできてきた！解説とかが増えます!**