国際標準レベルのセキュリティ組織実現に向けた取り組み

JNSA全国セミナー
2024

日本セキュリティオペレーション事業者協議会

Information Security Operation providers Group Japan(ISOG-J)

2008年設立、2024年9月現在68社加盟、およそ300人のメンバー
(親団体はJNSA。オブザーバーに総務省と経済産業省)

代表：武智 洋(日本電気株式会社)
副代表：阿部 慎司(GMOサイバーセキュリティ byイエラエ株式会社)
副代表：早川 敦史(GMOサイバーセキュリティ byイエラエ株式会社)
副代表：武井 滋紀(NTTテクノクロス株式会社)

セキュリティオペレーションガイドラインWG (WG1)	上野 宣(株式会社トライコーダ)
セキュリティオペレーション技術WG (WG2)	川口 洋(株式会社川口設計)
セキュリティオペレーション認知向上・普及啓発WG (WG4)	阿部 慎司(GMOサイバーセキュリティ byイエラエ株式会社)
セキュリティオペレーション連携 (WG6)	武井 滋紀(NTTテクノクロス株式会社)

今日はここ

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

**そろそろ3.2版がリリースされます！
さらにコンテンツが増えます！**

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

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

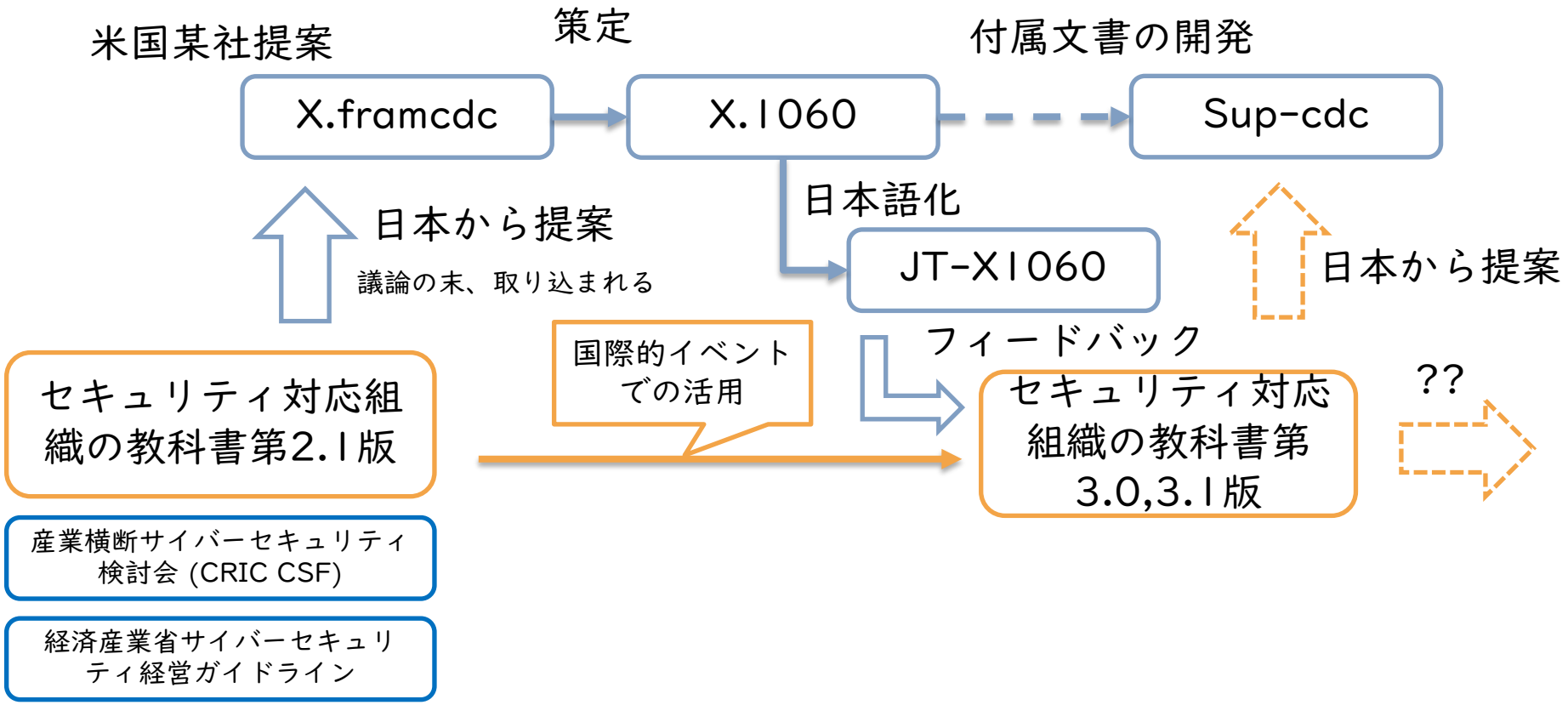
- ITU-T SG17内特設ページ
  - https://www.itu.int/en/ITU-T/studygroups/2022-2024/17/Pages/X1060.aspx

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

教科書のこれまで



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の幅

▼

情シスの一部　　SOC / CSIRT

新たな組織体の必要性

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

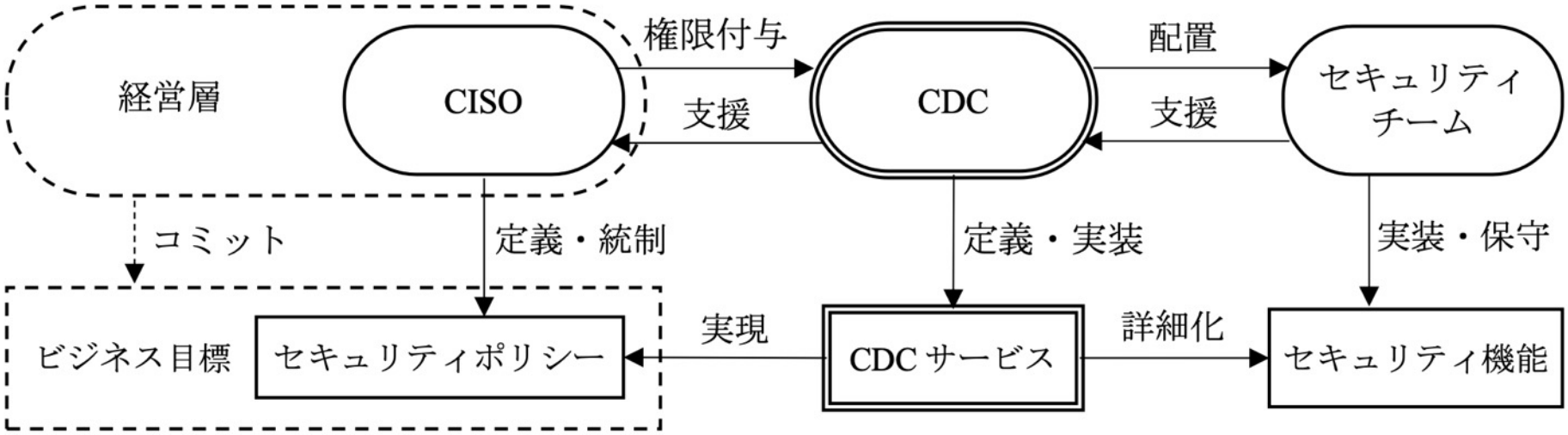
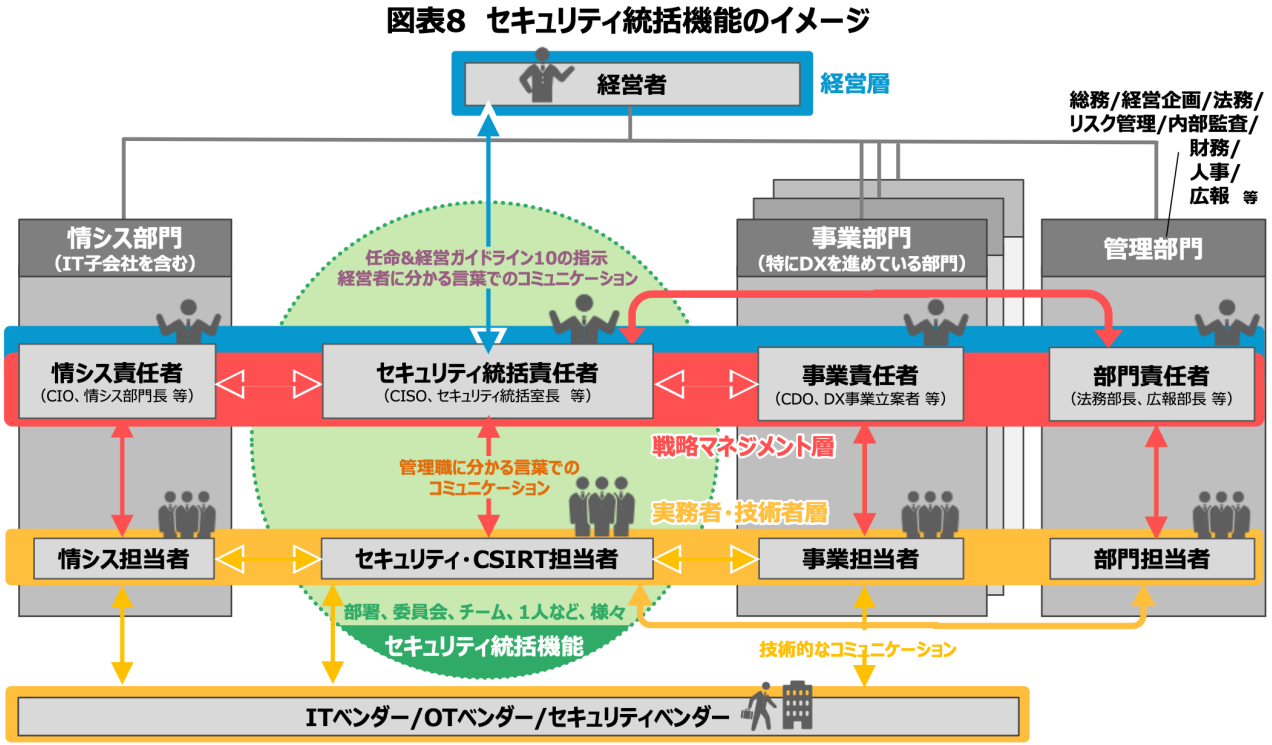
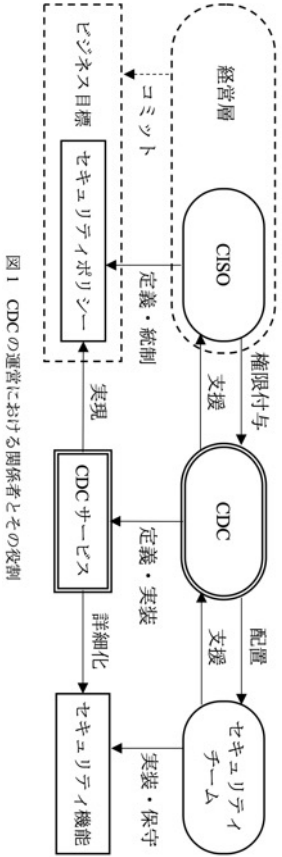


図 1　CDC の運営における関係者とその役割

図はJT-X1060より

セキュリティ統括機能のイメージ





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

様々なドキュメントとその使い所

“色々あるのはわかるが、どれを使ったらいいの？”
“すでに***を参照しています”

経済産業省、IPA、CRIC CSF

日本シーサート協議会、FIRST

ISMS, ISO/IEC, ISO, NIST, ENISA などなど

それぞれのドキュメントには使い所がある

経営層向け：経済産業省、IPA、CRIC CSF

セキュリティ組織を作るなら

セキュリティ統括、CDC向け：
X.1060/JT-X1060, セキュリティ対応組織の教科書

CSIRTを作るなら

CSIRT向け：日本シーサート協議会、FIRST

実際どうするかを知りたいなら

具体的な管理策：ISMS, ISO/IEC, NIST, ENISA などなど

経営層向け

- 経済産業省、サイバーセキュリティ経営ガイドラインと支援ツール
  - https://www.meti.go.jp/policy/netsecurity/mng_guide.html
- 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
  - https://www.ipa.go.jp/security/economics/csm-practice.html
- 産業横断サイバーセキュリティ検討会(CRIC CSF)、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　（統括室キット）
  - https://cyber-risk.or.jp/contents/

CSIRT向け

- 一般社団法人日本シーサート協議会、各種ドキュメント
  - https://www.nca.gr.jp/
- FIRST、FIRST CSIRT Service Framework V2.1
  - https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1
- FIRST、Team Types Within the Context of FIRST Services Frameworks Version 1.0
  - https://www.first.org/standards/frameworks/csirts/team-type_1-0
  - セキュリティ組織をCSIRT, ISAC, PSIRT, SOCの４つに分類
  - CDCについても言及があり、今後2つのドキュメントは整理される予定

使い所に気をつけよう

それぞれのドキュメントには想定される
読み手、使い方があります

“我々はISMSでゴニョゴニョ”

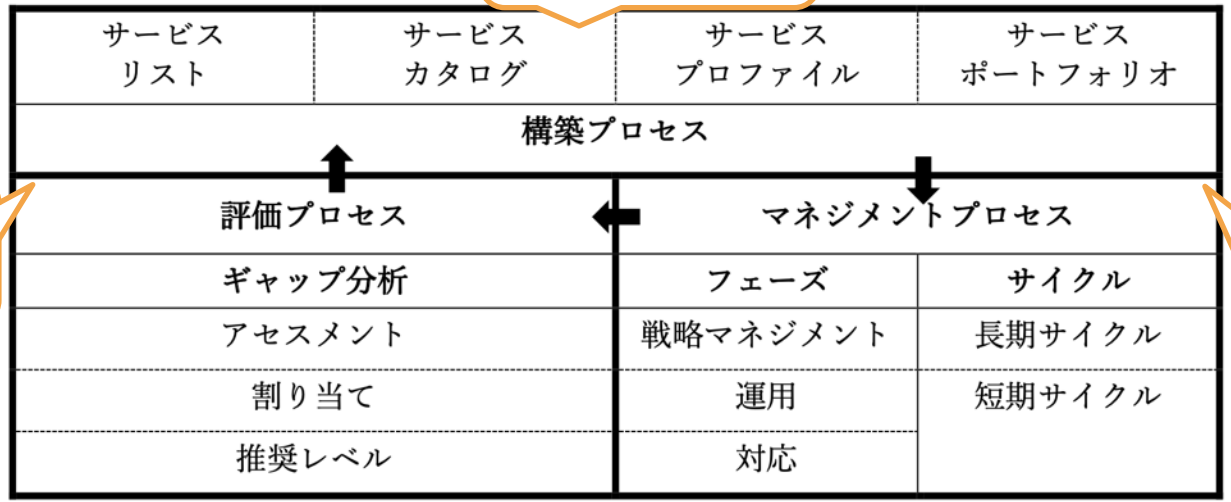
どのレイヤで話をしてますか？
それだけで大丈夫ですか？全体が見えてますか？

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

X.1060の構築は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

サービスポートフォリオシート

- X.1060の構築プロセスの結果、最終的に作成される「サービスポートフォリオ」をExcelシート化したもの
- 64のサービスに対して、推奨レベル、割り当て、サービススコアを記入できる。
  - サービスの概要についてもシートに入っているので参考にできます。

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(As-Is)	あるべき姿(To-Be)
(サービス名)	（ウェイト）	(実施場所)	(スコア)	(スコア)

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）

インソース・アウトソース

タイプ	説明
インソース	組織内のチームで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。
未割り当て	組織に存在すべきサービスはあるが、割り当てられていない

アセスメントのスコア

インソースの場合

スコア	説明
5	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
4	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
3	運用が明文化されておらず、担当者に代わり他者が臨時で一部の業務を実施できる
2	運用が明文化されておらず、担当者が業務を実施できる
1	実施できていない
評価対象外	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

アウトソースの場合

スコア	説明
5	サービス内容と得られる結果を理解でき、想定通り
4	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
3	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
2	サービス内容と得られる結果を理解できていない
1	結果や報告を確認できていない
評価対象外	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

X.1060, ISOG-J セキュリティ対応組織の教科書

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

サービスポートフォリオシート

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

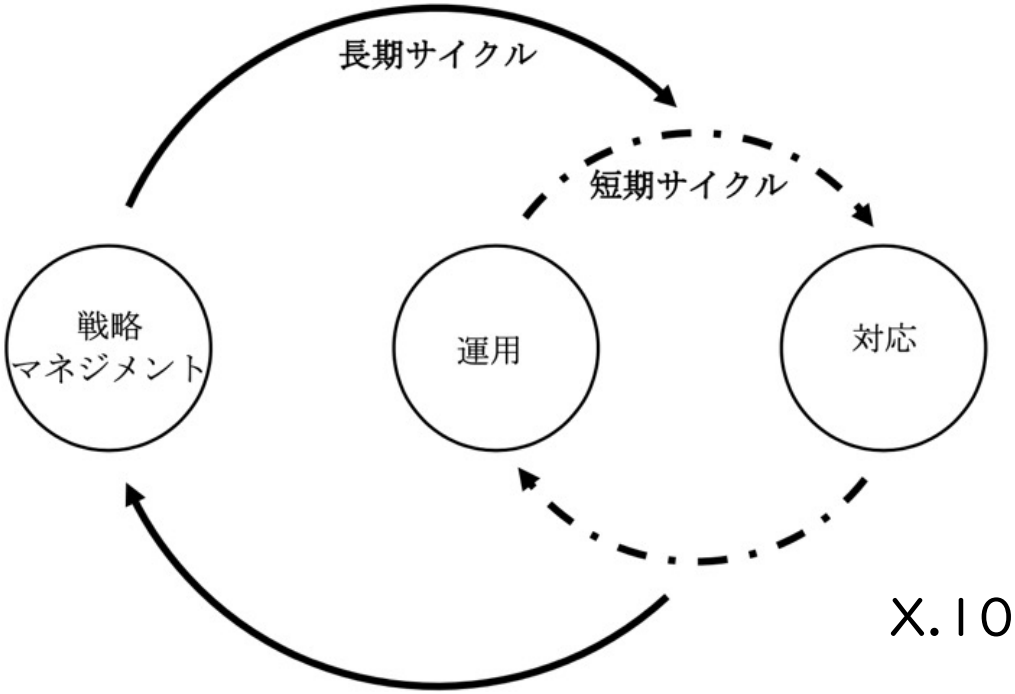


図 6　CDC マネジメントプロセス

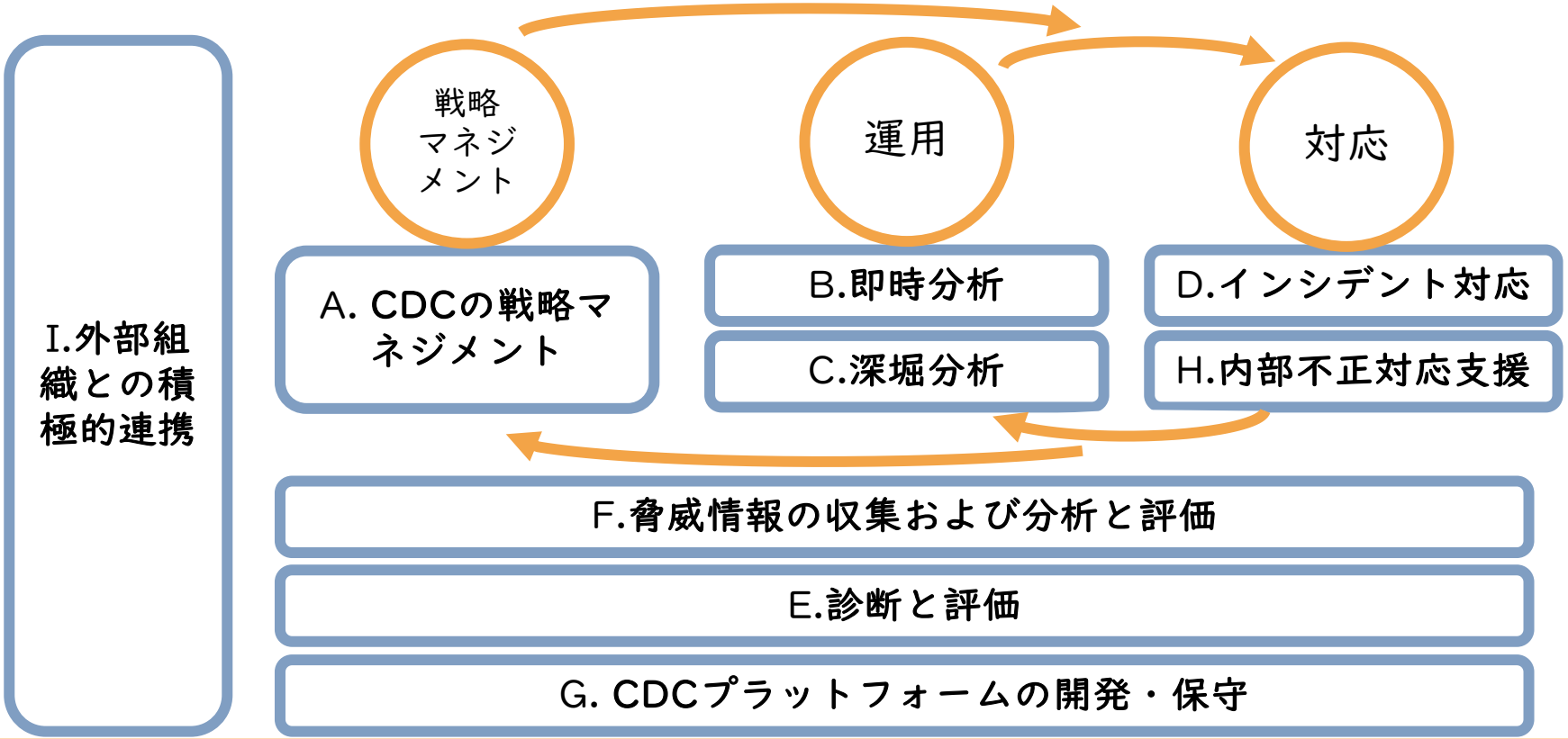
サービスは具体的にどんな
プロセス、どんな手順？？

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？

よし、X.1060/JT-X1060、ISOG-Jの文書を使おう

とは言ったものの、9つのカテゴリ
64のサービス？？

“どこから手をつけたらいいの？”

正論：組織をリスクアセスメントして、組織にとって重要なサービスを優先度を高くして順に選んでください

“で、どこから手をつけたらいいの？”

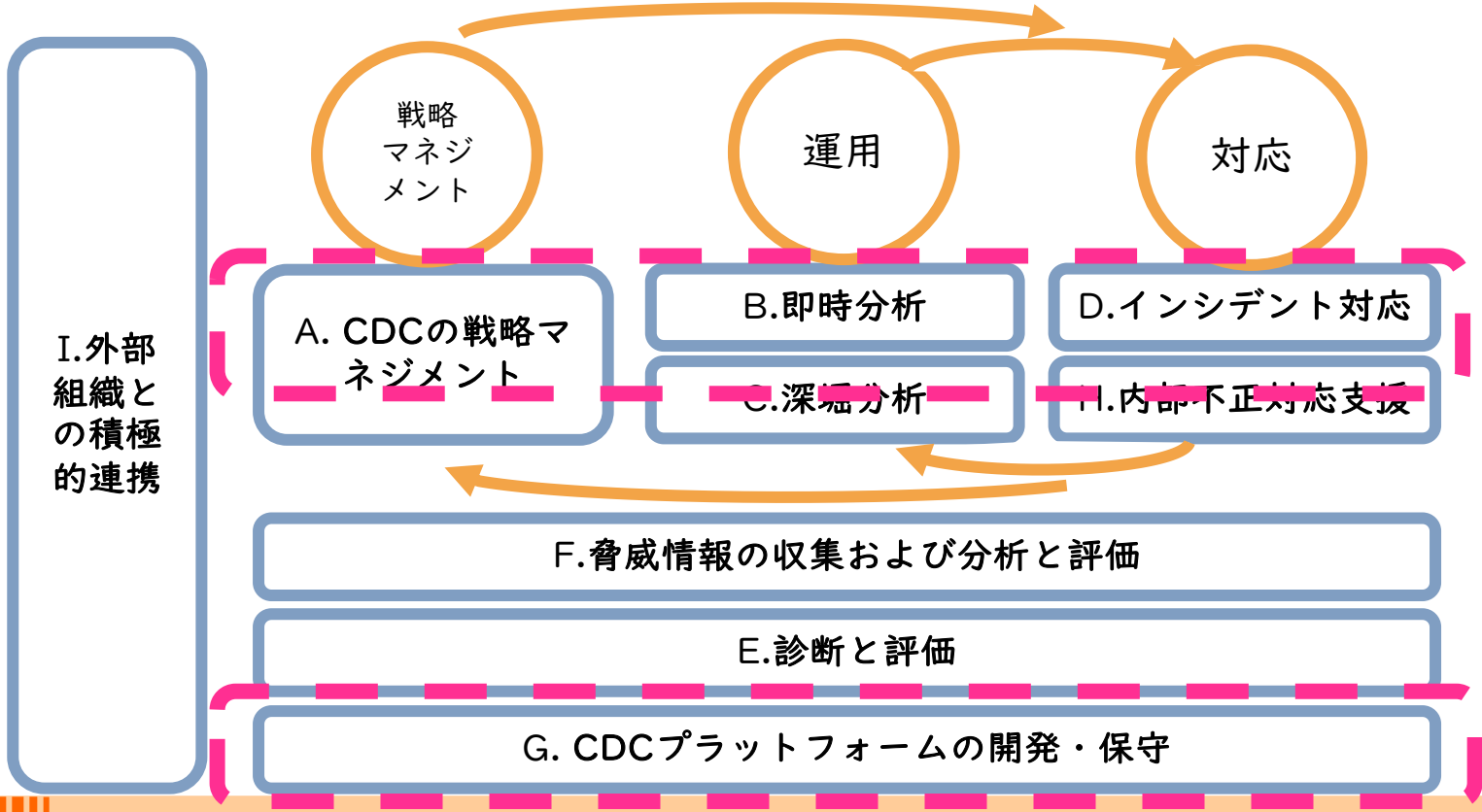
3.2版ではどこから着手するか例を提示

- 日々のマネジメントサイクルで運用が回らないのは問題
- まずは運用が回るところから優先度をあげて着手しよう

- 運用の3つのフェーズ
  - 戦略マネジメント：カテゴリA、CDCの戦略マネジメント
  - 運用：カテゴリB、即時分析
  - 対応：カテゴリD、インシデント対応

  - 共通して監視運用に必要なカテゴリG、CDCプラットフォーム開発・保守

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



カテゴリ
A→G→B→D
の流れを意識
してサービス
を選択します

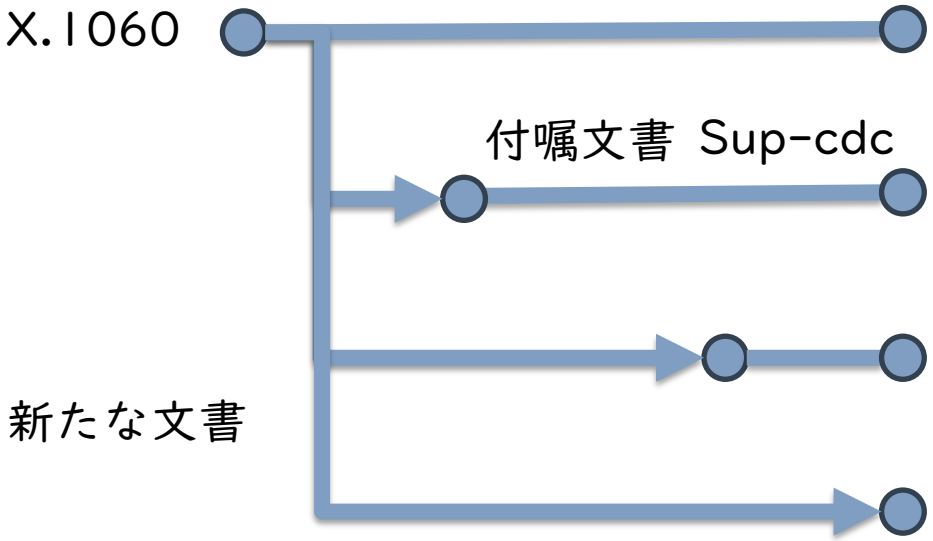
その他、3.2版ではこんなコンテンツが追加されます

1. エグゼクティブサマリー
   - 経営層にこのドキュメントを読んで欲しい、という思いから追加。トップダウンで組織改善をしたい方に。
2. サプライチェーンにおけるセキュリティ対応組織の必要性
   - 国際的な共通言語としてのX.1060は国内外の拠点とのセキュリティ組織を作る際に利用できます。
3. 見直しタイミング
   - フレームワークとして改善を続けることが重要です。どんなタイミングで見直しをするのか、例を追加しました。
4. サービスをどのように選ぶか
   - 確かに、64全部の中からどう選ぶかはなかなか難しい話です。一つの考え方の例を示します。
5. サービスポートフォリオセルフチェックシートを追加
   - 2.1版の付録だったセルフチェックシートが帰ってきました！どこが弱点でどこを強化すべきか可視化できます！

X.1060の今後

- 広がる文書、高まる期待

アフリカエリアからの活用について
注目が高まっている



改訂作業開始

X.1060の実用書
成立まであと少し

成熟度に向けた指標の検討中

FIRST CSIRT Service Frameworkとの
関連の検討作業開始