X.1060って何なん？

適当にX.1060の説明をして、
自分に関係ありそうだなぁ、
と思う人を増やすための怪文書

2022/11/26
脆弱性対応研究会
<--!脆弱性対応研究会としての見解であり、勧告作成者の意図と異なる可能性があります-->

X.1060って何なの？

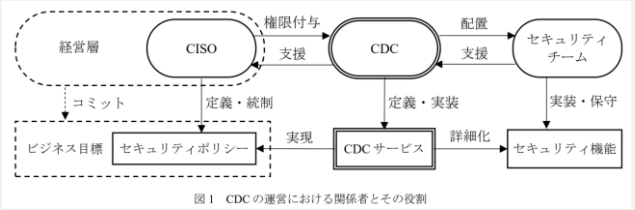

図1　CDCの運営における関係者とその役割

- フレームワーク
  - 組織レベルでの戦略的なセキュリティ対応を実現するフレームワーク。
  - 組織のセキュリティを実現するために、<u>サイバーディフェンスセンター（CDC）</u>がどのようにセキュリティサービスを決定し、実施すべきかを示している。
  - 上述の通り組織戦略を対象としており、個々の技術や設定はこのフレームワークには含まれていない。
    - 必要に応じて、別途提供されている情報を利用する。
    - 日本であれば、経産省：サイバーセキュリティ経営ガイドライン、セキュリティ対応組織の教科書、等を参照する必要がある。他国であれば同様の、その国に合った資料を利用する
      - 今までは、これらの資料を基に戦略的な検討をしていたが、X.1060によって「戦略から該当資料を参照する」という（本来あるべきと思われる）逆方向に参照できるようになった。

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

※サイバーディフェンスセンター（CDC）
「組織において、ビジネス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」。所謂、情シスやCSIRTなど。

X.1060で何ができるの？

できる事

- CDC（CSIRTなど）の構築設計
  - 何を実装するべきかの指標がある → CDCサービスカテゴリとリストとしてまとまっている
  - インソース/アウトソースなどの検討指標がある
  - 構築後のアセスメント（評価）指標がある
  - マネジメントサイクル（短期/長期での改善活動）の指標がある

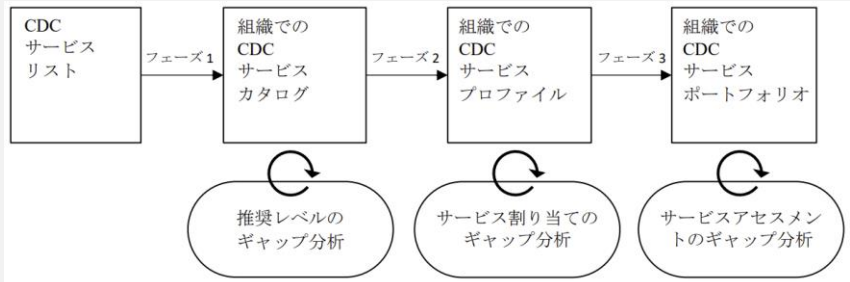

図7　CDC評価プロセス

できない事

- CDCの活動の詳細設計
  - CDCサービスカテゴリとリストはあるが、「どこまでやるべきか/どのようにやるのか」は記載が無い
    - 例えば、[カテゴリーF：脅威情報の収集および分析と評価][F-3.外部脅威情報の収集・評価]はあるが、どのように脅威情報を収集するか、どのような観点で評価するか、は含まれていない
    - これらは、別途存在するであろう資料を参照することで対応する必要がある

X.1060はどんな人向け？

想定される利用者像は、以下と思われる

- CDCを構築する人
  - これからCSIRTを構築する、既存CSIRTの改善をする、等
- 現状を改善したい人
  - CSIRTの活動を検証/改善する、組織としてのセキュリティ対応を棚卸する、等
    - CDC担当者目線での自組織の充足範囲点検、CSO（最高セキュリティ責任者）やCISO（最高情報セキュリティ責任者）などの組織レベルでの充足範囲点検、等
- セキュリティ対策を勉強する人
  - セキュリティコンサルティングを行う人、セキュリティについて学ぶ人
    - どの視点で何が必要なのか、必須/任意な機能と考えてよいものは何か、等の判断情報として

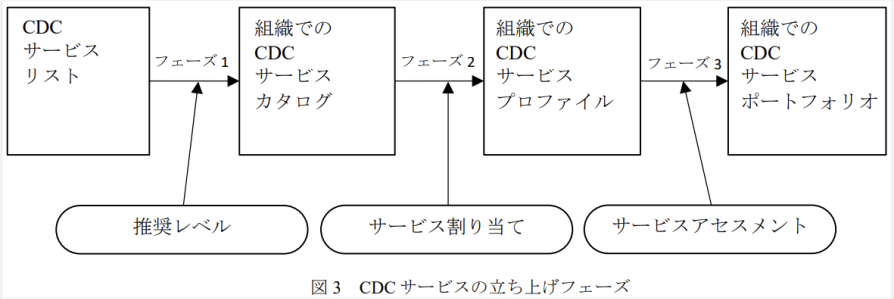

図 3　CDC サービスの立ち上げフェーズ

想定されていないと思われる者

- 特定の技術に対する詳細な解説
  - CDCサービスリストの各サービスの、詳細な実施方法など

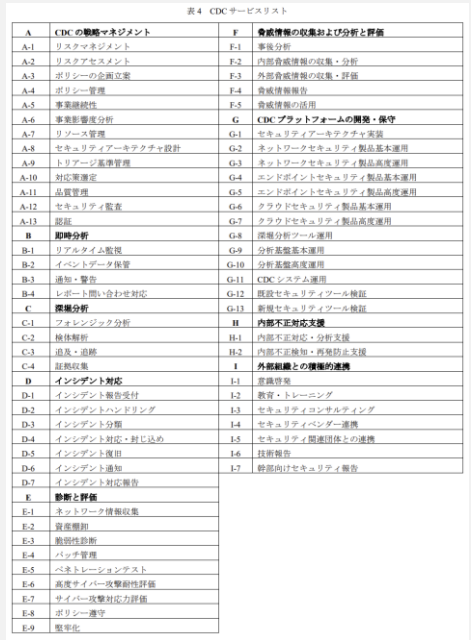
表 4　CDC サービスリスト

A	**CDC の戦略マネジメント**	**F**	**脅威情報の収集および分析と評価**
A-1	リスクマネジメント	F-1	事後分析
A-2	リスクアセスメント	F-2	内部脅威情報の収集・分析
A-3	ポリシーの企画立案	F-3	外部脅威情報の収集・評価
A-4	ポリシー管理	F-4	脅威情報報告
A-5	事業継続性	F-5	脅威情報の活用
A-6	事業影響度分析	**G**	**CDC プラットフォームの開発・保守**
A-7	リソース管理	G-1	セキュリティアーキテクチャ実装
A-8	セキュリティアーキテクチャ設計	G-2	ネットワークセキュリティ製品基本運用
A-9	トリアージ基準管理	G-3	ネットワークセキュリティ製品高度運用
A-10	対応層選定	G-4	エンドポイントセキュリティ製品基本運用
A-11	品質管理	G-5	エンドポイントセキュリティ製品高度運用
A-12	セキュリティ監査	G-6	クラウドセキュリティ製品基本運用
A-13	認証	G-7	クラウドセキュリティ製品高度運用
B	**即時分析**	G-8	探索分析ツール運用
B-1	リアルタイム監視	G-9	分析基盤基本運用
B-2	イベントデータ保管	G-10	分析基盤高度運用
B-3	通知・警告	G-11	CDC システム運用
B-4	レポート問い合わせ対応	G-12	既設セキュリティツール検証
C	**深堀分析**	G-13	新規セキュリティツール検証
C-1	フォレンジック分析	**H**	**内部不正対応支援**
C-2	検体解析	H-1	内部不正対応・分析支援
C-3	追及・追跡	H-2	内部不正検知・再発防止支援
C-4	証拠収集	**I**	**外部組織との積極的連携**
D	**インシデント対応**	I-1	意識啓発
D-1	インシデント報告受付	I-2	教育・トレーニング
D-2	インシデントハンドリング	I-3	セキュリティコンサルティング
D-3	インシデント分類	I-4	セキュリティベンダー連携
D-4	インシデント対応・封じ込め	I-5	セキュリティ関連団体との連携
D-5	インシデント復旧	I-6	技術報告
D-6	インシデント通知	I-7	幹部向けセキュリティ報告
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		

X.1060もう少し詳細を？

以下を参照すると良さそう。

- ITU
  - X.1060: Framework for the creation and operation of a cyber defence centre
    - https://www.itu.int/rec/T-REC-X.1060-202106-I
    - ITUの資料なので、日本語版は無い
- 一般社団法人 情報通信技術委員会（TTC）
  - JT-X1060- 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
    - https://www.ttc.or.jp/document_db/information/view_express_entity/1423
    - 日本語訳、として参照するのがよさそう
- 日本セキュリティオペレーション事業者協議会（ISOG-J）
  - セキュリティ対応組織の教科書 v2.1（2018年09月）
    - https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html
- 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

X.1060もう少し詳細を？

脆弱性対応勉強会で、本勧告のエディタを務めた方にお話を頂きます。そこで聞こう。

- https://zeijyakuseitaioukenkyukai.connpass.com/event/266469/
- 2022/12/03（土曜）、人数制限有り。必要なら再度実施予定（キャンセル待ちが多ければ）。