X.1060から眺める全体像

2023.9.15

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/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
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(2017-2023)

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)
ISC2 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、2023年9月現在 63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

本日のポイント

- 自分の業務や役割がどのあたりなのか見てみよう
- それぞれの部分で参考になるドキュメントを活用しよう

セキュリティ対応組織の教科書　第3.0版

- 2023-2-13公開
  - https://isog-j.org/output/2023/Textbook_soc-csirt_v3.0.pdf
- 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
  - 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

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
- 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

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

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。

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

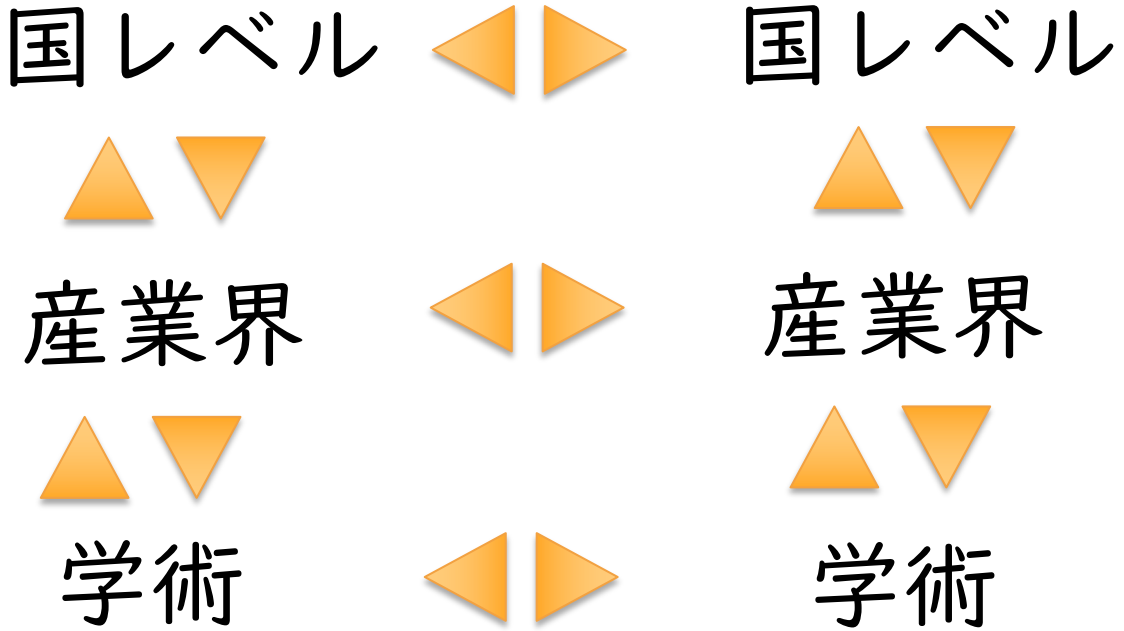
ビジネスリスクとしてのセキュリティの対応へ

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



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

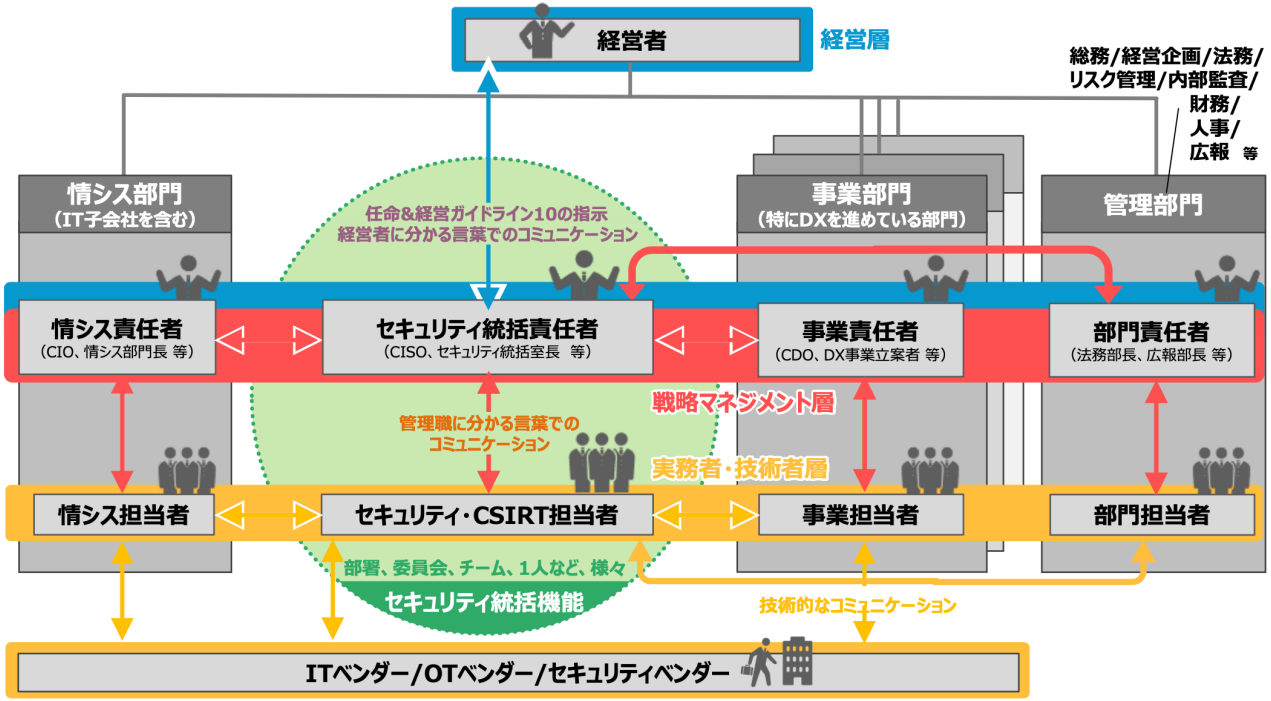
JNSAドキュメント群

CISOハンドブック

SecBok

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

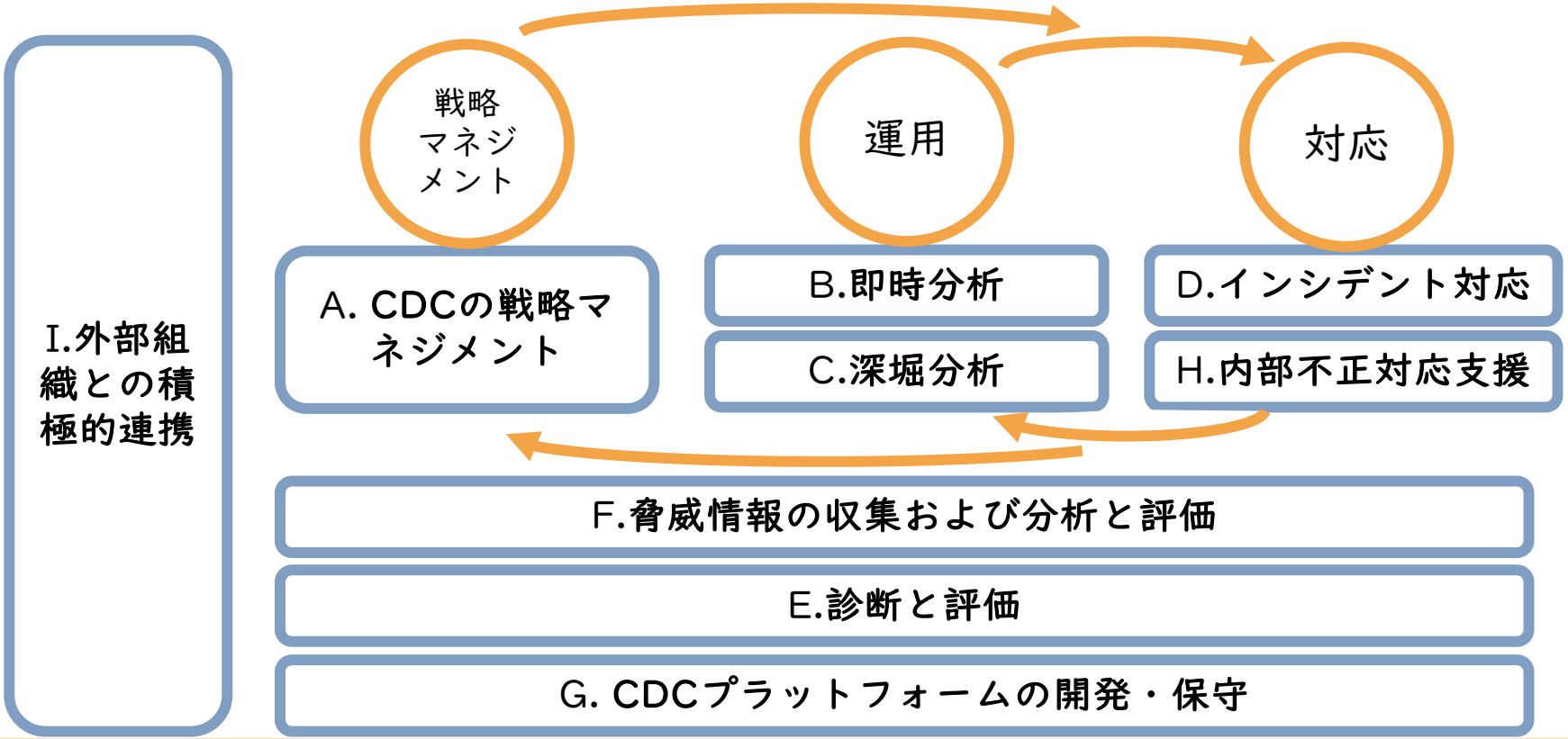
担当、ベンダーとの連携

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

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

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



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

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

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

- 自分の業務や役割がどのあたりなのか知っておこう

- それぞれの部分で参考になるドキュメントを活用しよう