InternetWeek2022 【学生・若手歓迎】「セキュリティの仕事、どんなことしているの？どうしたらなれるの？」

セキュリティのお仕事を世界から見てみよう（武井の場合）

2022.11.24

NTTテクノクロス株式会社　武井　滋紀

あらすじ

- 武井の場合

- X.1060にみるセキュリティのお仕事

武井の場合

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/
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。

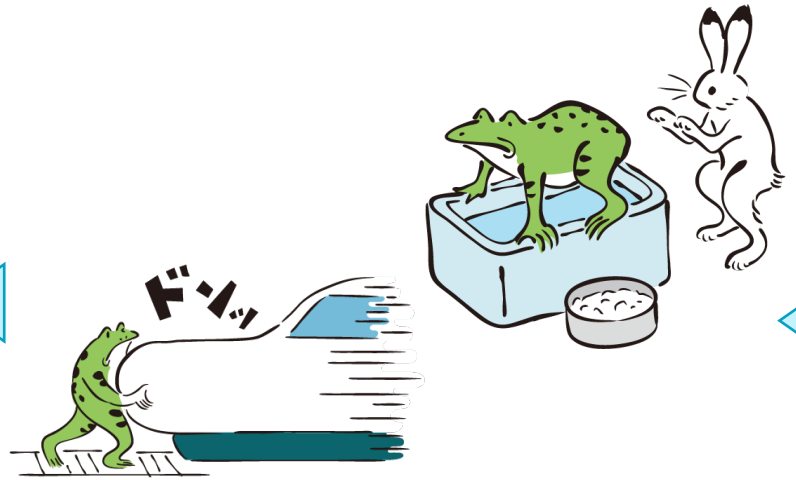
どうしてこうなった？

SIerの開発担当

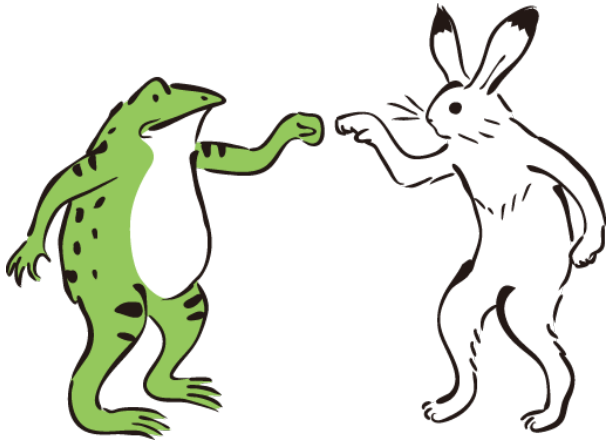
突然の異動

やるしかない

社外のコミュニティで活動



あれこれありまして



こうなりました

X.1060にみるセキュリティのお仕事

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

一般社団法人　情報通信技術委員会(TTC)にて、日本の標準 JT-X1060 へ(2022年2月)

「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

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)を構築と運用をし、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。

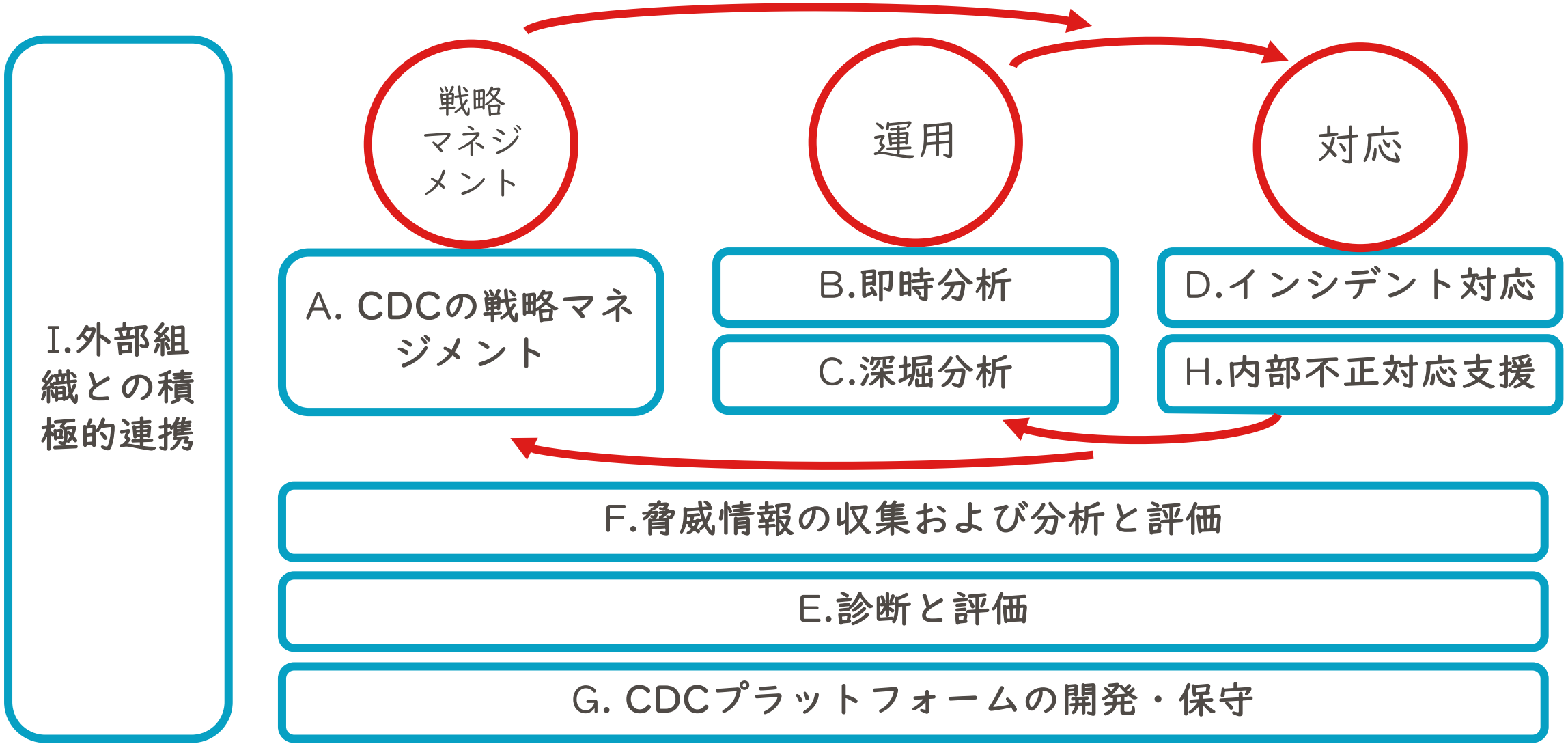
サービスカテゴリー、サービスリスト

- 9つのサービスカテゴリー、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

サービスカテゴリーとマネジメントプロセスとのマッピング



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

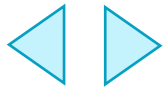
H-1	内部不正対応・分析支援
H-2	内部不正検知・再発防止支援

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

インソースとアウトソース

自分の組織で実施する



外部へ委託する

（インソース）

（アウトソース）

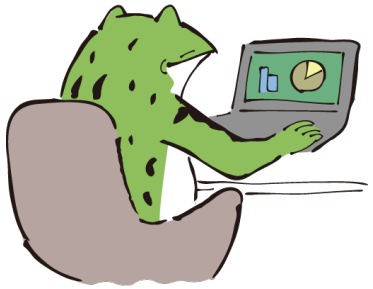
予算や人材、スキル
色々な制約

ベンダー、専門業者、
マネージドサービス
プロバイダー(MSSP)

サービスを提供する側（アウトソーサー）

サービスを提供する側でも色々なお仕事がある

研究・企画・開発



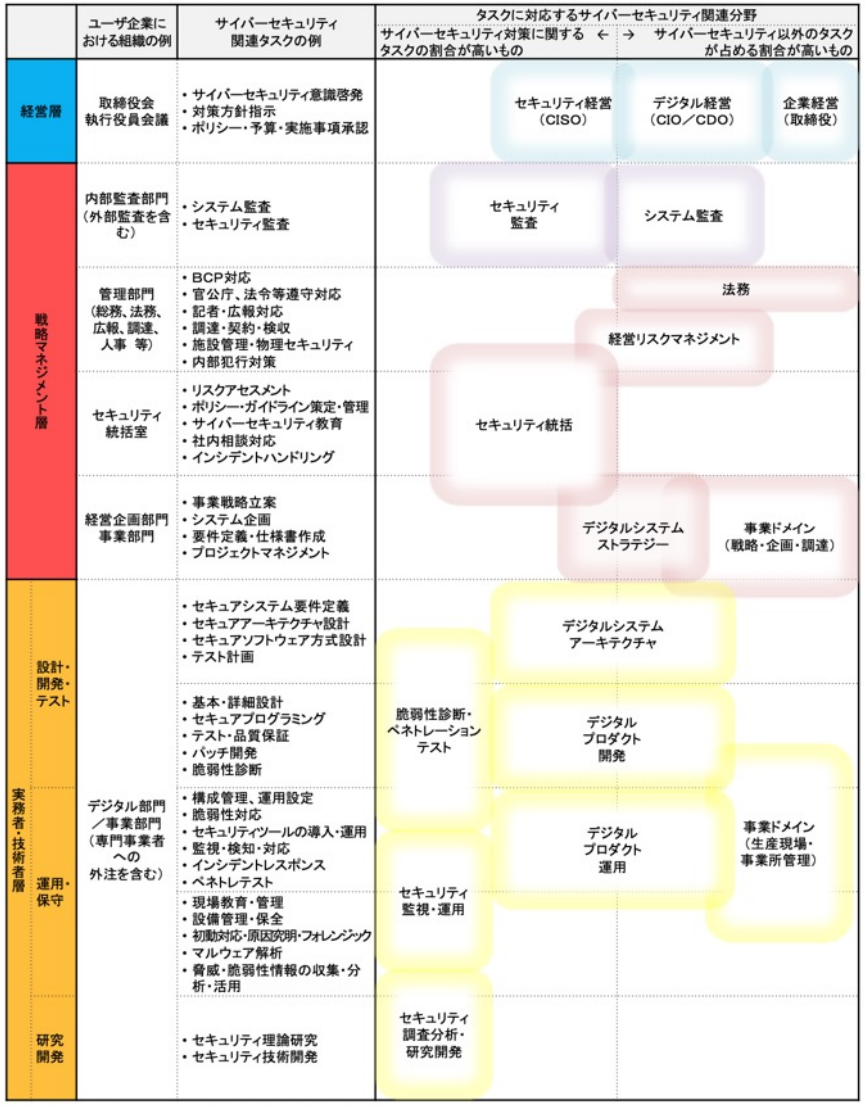
運用

サポート

営業

IPA ITSS+も参考に

図表6　ITSS+（セキュリティ分野）で定義されている17分野



※クラウド、アジャイル、DevSecOps等により境界は曖昧化の傾向
※チップ/IoT・組み込み/制御システム/OS/サーバ/NW/ソフト/Web等の取扱う技術の種類や事業分野によりタスクやスキルは大きく異なる

ITSS+（プラス）・ITスキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報
https://www.ipa.go.jp/jinzai/itss/itssplus.html#section1-6

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/tebiki_taisei_jinzai.html

ユーザ企業のおける組織の例
サイバーセキュリティ関連タスクの例
タスクに対応するサイバーセキュリティ関連分野

まとめ

- 組織の中でどんなことをしているか
- やりたいことは組織の中にある？外部に委託する側にある？
- サービスを提供する側の中でも色々な役割がある
- 変わる状況の中で、自分はどうなりたいのか考え続ける

イラスト：ダ鳥獣戯画　https://chojugiga.com/