

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？どうしたらなるの？」

セキュリティのお仕事を世界から見よう (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？



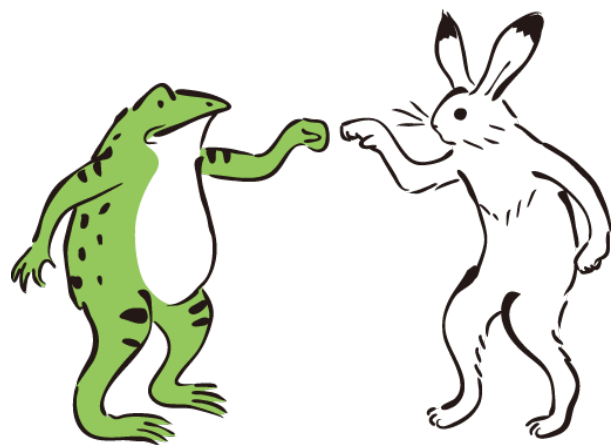
SIerの開発担当



突然の異動



やるしかない



こうなりました



あれこれありまして



社外のコミュニティで活動



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

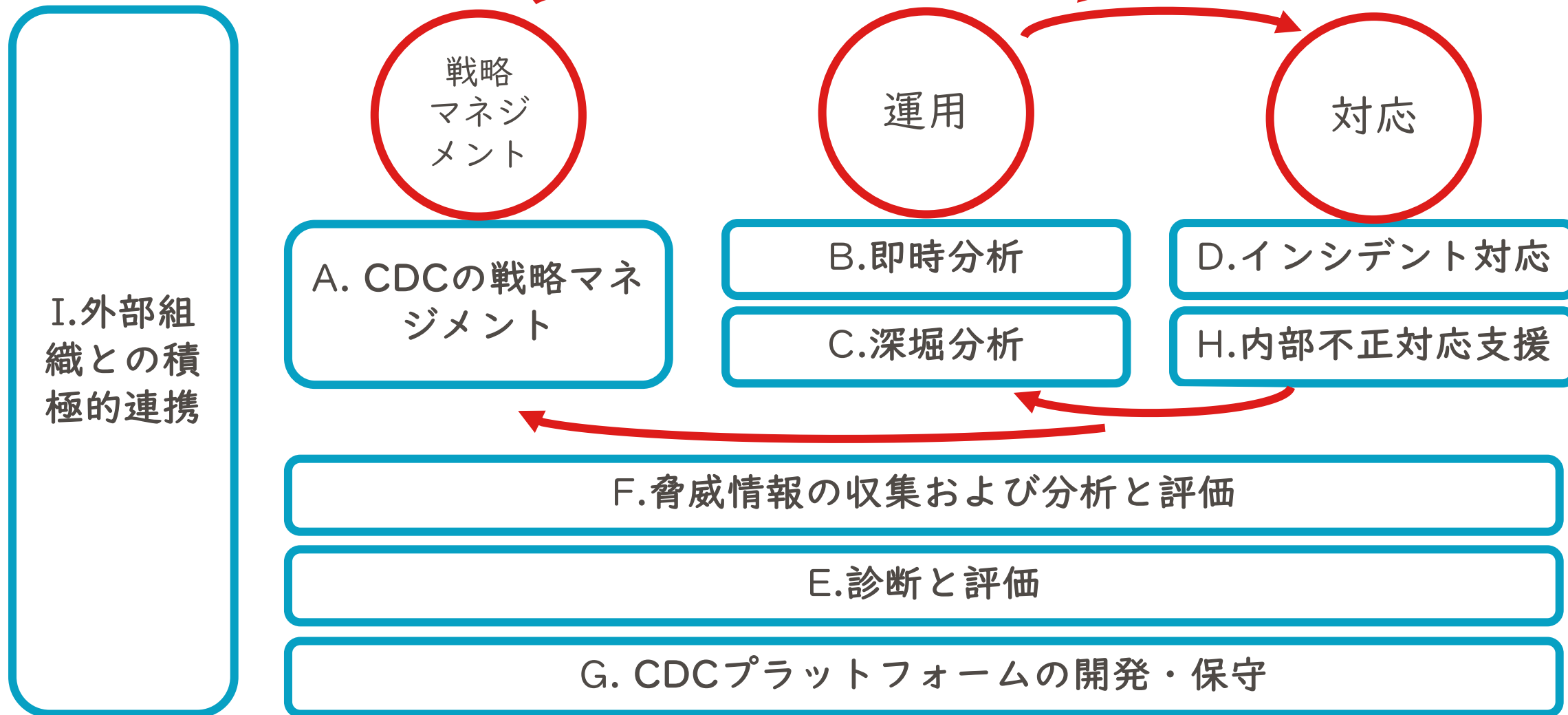
組織におけるサイバーディフェンスセンター(CDC)を構築と運用をし、効果的に
改善を続けるフレームワークである。組織におけるセキュリティを実現する
セキュリティサービスの選定と実装を示す。
CSOやCISO、およびCSOやCISOをサポートする方が対象となる。

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	F	脅威情報の収集および分析と評価	5
B	即時分析	4	G	CDCプラットフォームの開発・保守	13
C	深堀分析	4	H	内部不正対応支援	2
D	インシデント対応	7	I	外部組織との積極的連携	7
E	診断と評価	9			

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-8	セキュリティアーキテクチャ設計
A-2	リスクアセスメント	A-9	トリアージ基準管理
A-3	ポリシーの企画立案	A-10	対応策選定
A-4	ポリシー管理	A-11	品質管理
A-5	事業継続性	A-12	セキュリティ監査
A-6	事業影響度分析	A-13	認証
A-7	リソース管理		

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-6	高度サイバー攻撃耐性評価
E-2	資産棚卸	E-7	サイバー攻撃対応力評価
E-3	脆弱性診断	E-8	ポリシー遵守
E-4	パッチ管理	E-9	堅牢化
E-5	ペネトレーションテスト		

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-8	深堀分析ツール運用
G-2	ネットワークセキュリティ製 品基本運用	G-9	分析基盤基本運用
G-3	ネットワークセキュリティ製 品高度運用	G-10	分析基盤高度運用
G-4	エンドポイントセキュリティ 製品基本運用	G-11	CDCシステム運用
G-5	エンドポイントセキュリティ 製品高度運用	G-12	既設セキュリティツール検証
G-6	クラウドセキュリティ製品基 本運用	G-13	新規セキュリティツール検証
G-7	クラウドセキュリティ製品高 度運用		

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

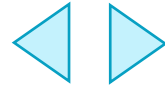
I. 外部組織との積極的連携

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

自分の組織で実施する

(インソース)

予算や人材、スキル
色々な制約



外部へ委託する

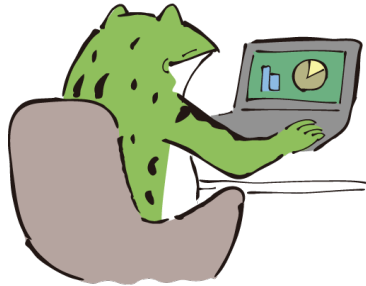
(アウトソース)

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

	ユーザ企業における組織の例	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		
			サイバーセキュリティ対策に関するタスクの割合が高いもの	← →	サイバーセキュリティ以外のタスクが占める割合が高いもの
経営層	取締役会 執行役員会議	・サイバーセキュリティ意識啓発 ・対策方針指示 ・ポリシー・予算・実施事項承認	セキュリティ経営 (CISO)	デジタル経営 (CIO/CDO)	企業経営 (取締役)
戦略マネジメント層	内部監査部門 (外部監査を含む)	・システム監査 ・セキュリティ監査	セキュリティ監査	システム監査	
	管理部門 (総務、法務、広報、調達、人事等)	・BCP対応 ・官公庁、法令等遵守対応 ・記者・広報対応 ・調達・契約・検収 ・施設管理・物理セキュリティ ・内部犯行対策		法務 経営リスクマネジメント	
	セキュリティ統括室	・リスクアセスメント ・ポリシー・ガイドライン策定・管理 ・サイバーセキュリティ教育 ・社内相談対応 ・インシデントハンドリング	セキュリティ統括		
	経営企画部門 事業部門	・事業戦略立案 ・システム企画 ・要件定義・仕様書作成 ・プロジェクトマネジメント		デジタルシステム戦略	事業ドメイン (戦略・企画・調達)
設計・開発・テスト	デジタル部門 ／事業部門 (専門事業者への外注を含む)	・セキュアシステム要件定義 ・セキュアアーキテクチャ設計 ・セキュアソフトウェア方式設計 ・テスト計画		デジタルシステムアーキテクチャ	
		・基本・詳細設計 ・セキュアプログラミング ・テスト・品質保証 ・パッチ開発 ・脆弱性診断	脆弱性診断・ペネトレーションテスト	デジタルプロダクト開発	
実務者技術者層	運用・保守	・構成管理、運用設定 ・脆弱性対応 ・セキュリティツールの導入・運用 ・監視・検知・対応 ・インシデントレスポンス ・ペネトレーションテスト ・現場教育・管理 ・設備管理・保全 ・初動対応・原因究明・フォレンジック ・マルウェア解析 ・脅威・脆弱性情報の収集・分析・活用	セキュリティ監視・運用	デジタルプロダクト運用	事業ドメイン (生産現場・事業所管理)
研究開発		・セキュリティ理論研究 ・セキュリティ技術開発	セキュリティ調査分析・研究開発		

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

ユーザ企業における組織の例
 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

※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

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