第10回脆弱性対応勉強会
X.1060の概要と使い所
X.1060の使い所

2022.12.3

ISOG-J

© 2022 ISOG-J

本日のポイント

- 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
- 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
- できるところから始めて、継続的に改善を続ける

© 2022 ISOG-J

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”

「サイバーディフェンスセンター構築・運用のフレームワーク」

配布URL: https://www.itu.int/rec/T-REC-X.1060-202106-I

© 2022 ISOG-J

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。

© 2022 ISOG-J

勧告になった後どうなったか

© 2022 ISOG-J

X.1060のその後

- RG-AFRが国のCSIRTとかの設置に活用したい、と考えた
- SG17全体として支援する、となった。
- 手始めにX.1060をベースにどれくらい現在セキュリティサービスを実装できているか、アフリカ諸国にアンケートを取ることになった

© 2022 ISOG-J

なるほど、わからん

© 2022 ISOG-J

今回の提案

- X.1060を読んだ反応「なるほど、わからん」

- 「……。チュ、チュートリアルの資料を提案します……。」
  - ここに至るまでの膨大な議論や経験の蓄積
  - 書ききれていない背景となる内容
  - フレームワークではあるが、実践書ではない
  - 全体からすると細かい実施方法や何をすべきかなどまではカバーしていない

© 2022 ISOG-J

X.1060/JT-X1060を使いこなすためには

そこに至る背景　　使うメリット

X.1060/JT-X1060
フレームワーク

どう使ったらいいか？？

© 2022 ISOG-J

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

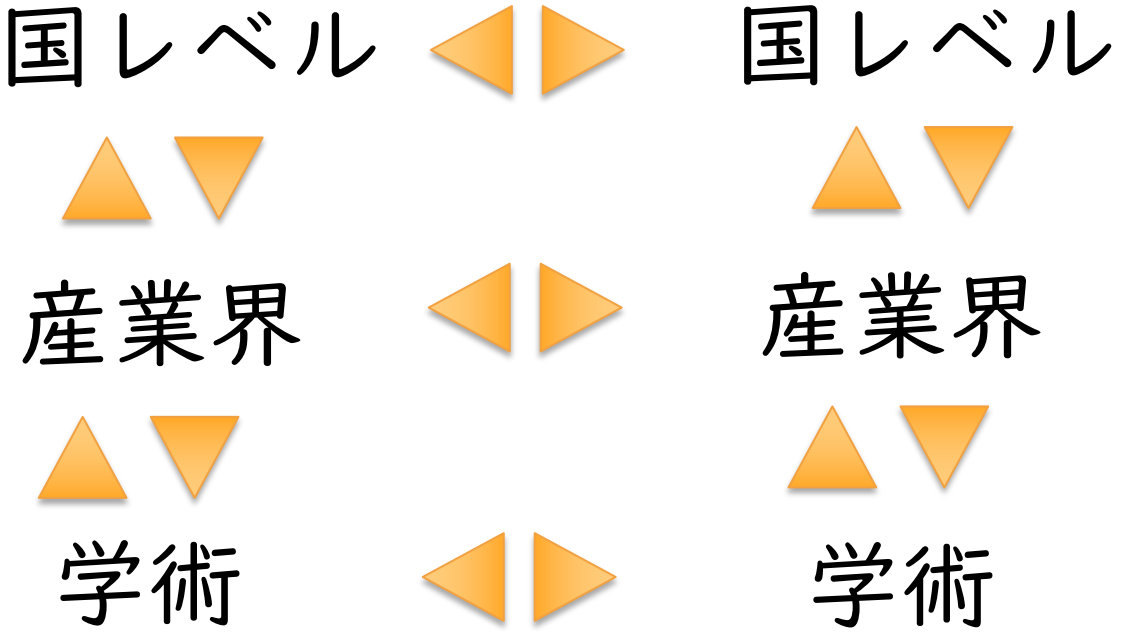
対応する部署や組織の拡大・連携

親会社・子会社、海外支店、国内外の取引先

© 2022 ISOG-J

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



© 2022 ISOG-J

標準を利用することの利益

- 共通言語として、やるべきこと（サービス）が認識される

- 組織の内外でサービスの分担や割り当ての際に、同じサービスの範囲での定義ができる
  - 政府<->産業界<->ベンダー　それぞれの共通認識
  - 会社間や国家間でのセキュリティのやるべきことの共通認識

- 政府、産業界、学術系で専門性の共通の認識ができる
  - 人材の育成、雇用、業務の定義での活用

© 2022 ISOG-J

使い所の話

© 2022 ISOG-J

X.1060/JT-X1060はどう使ったらいいか？

よく聞かれること

- サイバーディフェンスセンターって何？
- この文書の使い所はどこか？
- すでにSOC/CSIRTがあるのですが
- 我々はすでに***を参考にしています
- 日本で使うならどうしたらいいの？

© 2022 ISOG-J

サイバーディフェンスセンター？

組織において、ビジネス活動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。

これからのセキュリティ対応組織を定義したもの。
組織によって名前は様々。

今でもSOC/CSIRTの定義は組織ごとにバラバラ

© 2022 ISOG-J

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。

© 2022 ISOG-J

X.1060/JT-X1060における組織体制

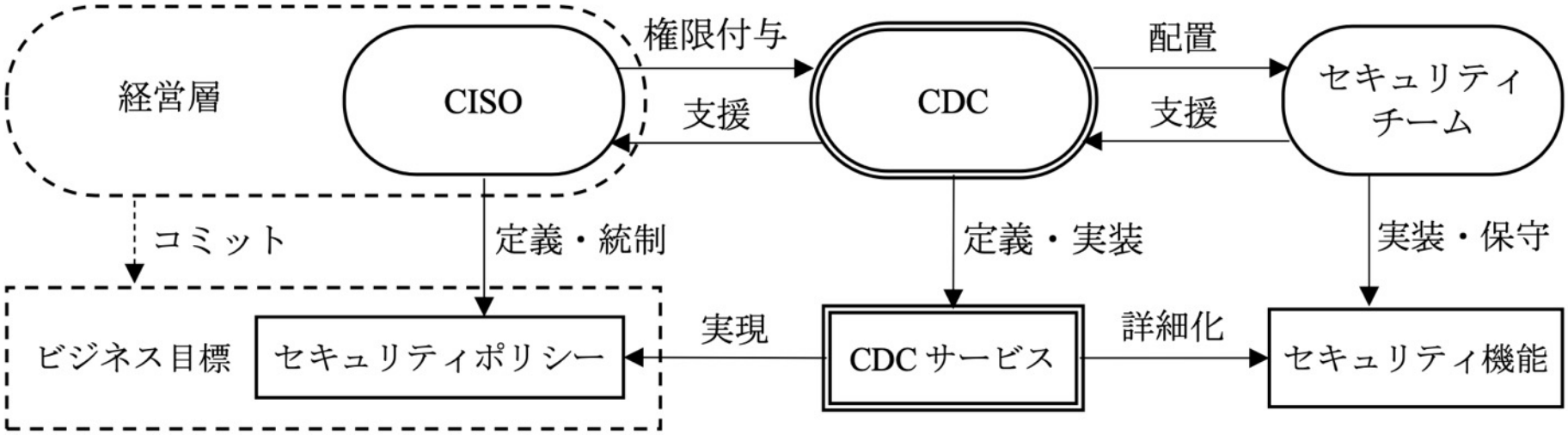


図 1　CDC の運営における関係者とその役割

図はJT-X1060より

© 2022 ISOG-J

日本のドキュメントとの比較

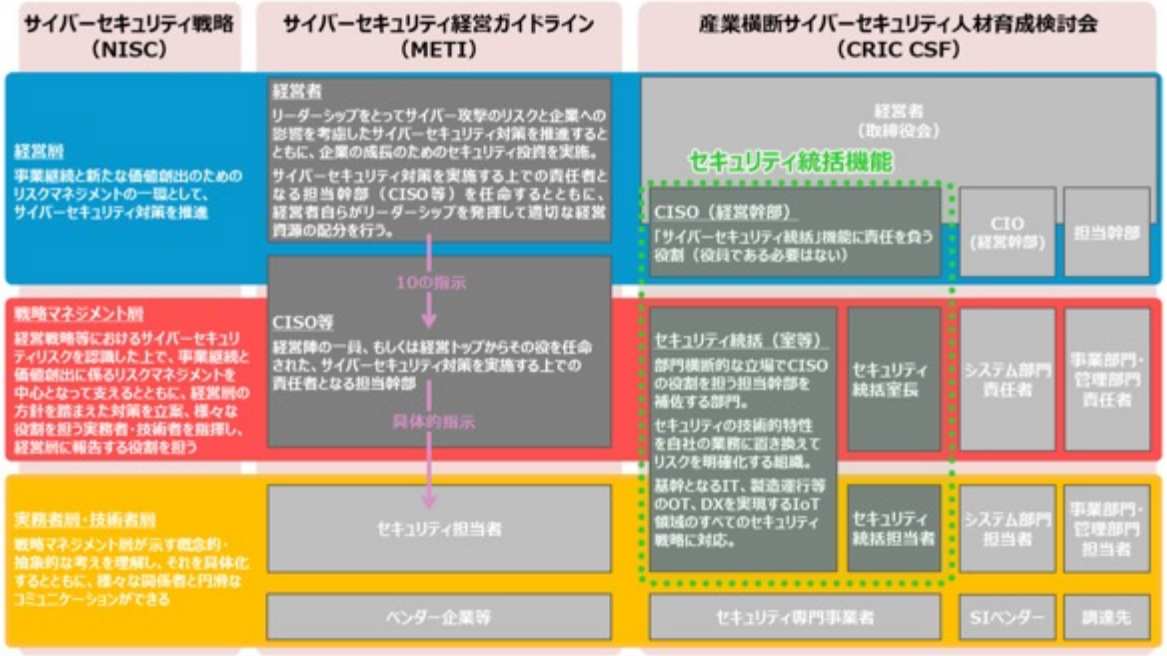


図 5　セキュリティ統括機能の位置付け（1）

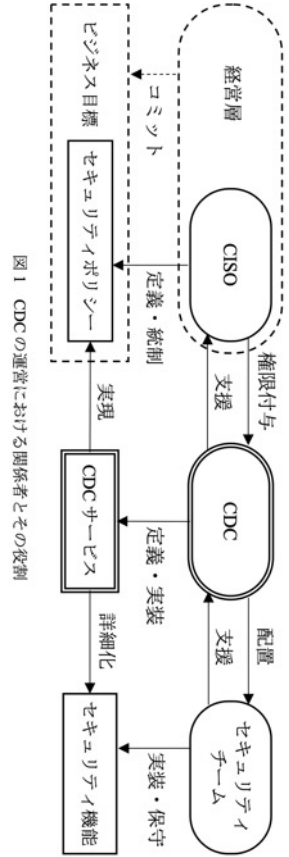


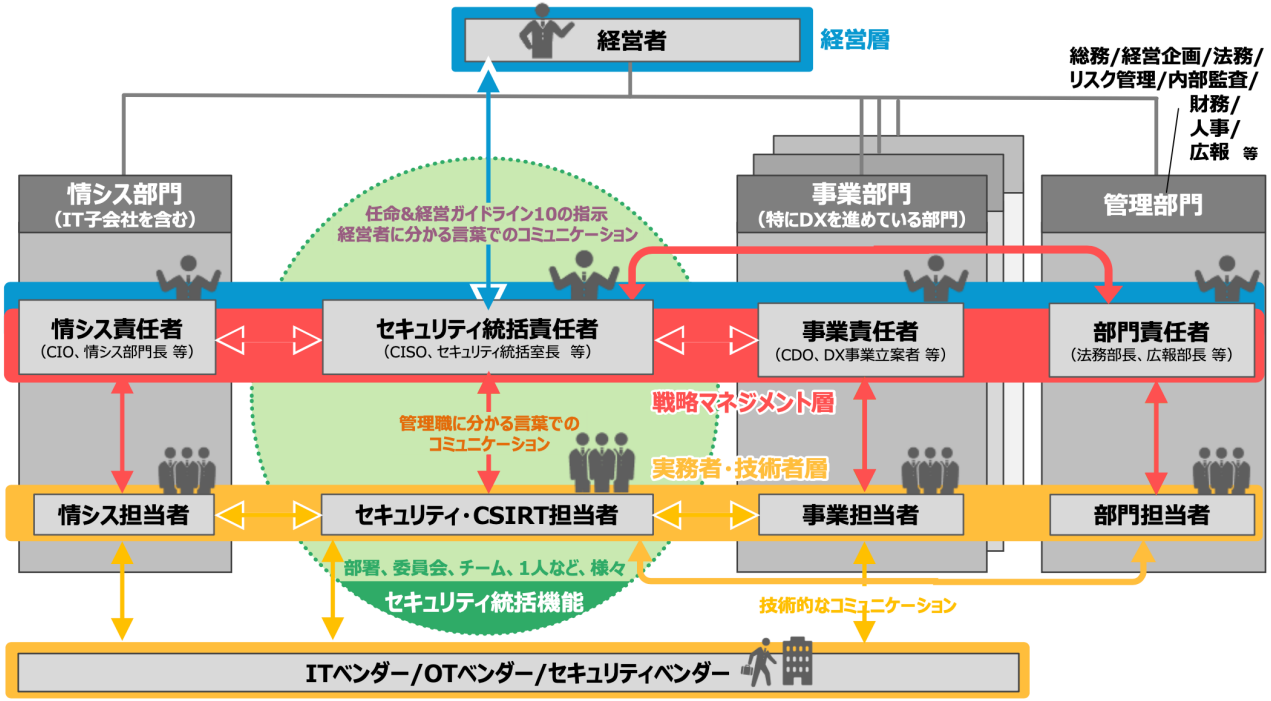
図 1　CDCの運営における関係者とその役割

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1.1版

© 2022 ISOG-J

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

© 2022 ISOG-J

組織をどう作るかの全体の流れ

経営層　サイバーセキュリティ経営ガイドラインを読む
10の指示を理解する。CISOを任命し権限を付与する

▼

CISO　指示に従いセキュリティ体制を構築する
セキュリティポリシーを決める
X.1060/JT-X1060など参考にする

▼

セキュリティ統括　サービスの割り当て・権限の付与、各チームと連携する
X.1060/JT-X1060など参考にする

▼

割り当てられたサービスのプロセスや手順を実装する
セキュリティチーム　各種ガイドラインや手順などを参考にする

© 2022 ISOG-J

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

© 2022 ISOG-J

ポイント

- 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

© 2022 ISOG-J

使ってみた、時の話

© 2022 ISOG-J

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

© 2022 ISOG-J

構築プロセス

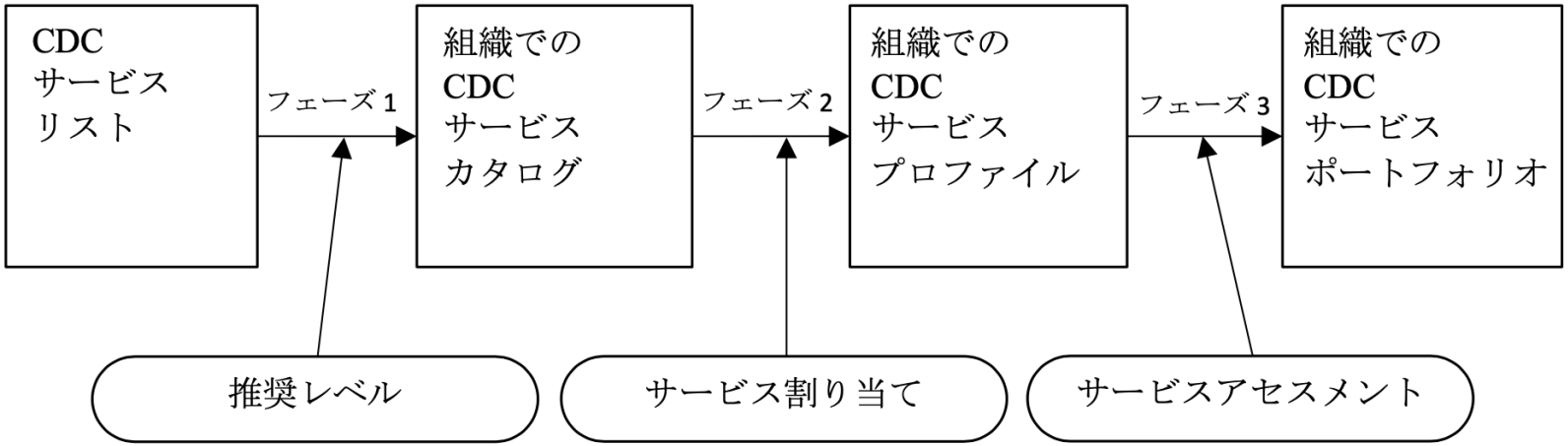


図 3　CDC サービスの立ち上げフェーズ

構築は3段階

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

図はJT-X1060より

© 2022 ISOG-J

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

© 2022 ISOG-J

構築プロセス時　サービスを選ぶ

９つのカテゴリー、64のサービスから実施すべきものを選択

選択時に実施する推奨レベルも設定する

今、すでにやっているものをマッピングしておく

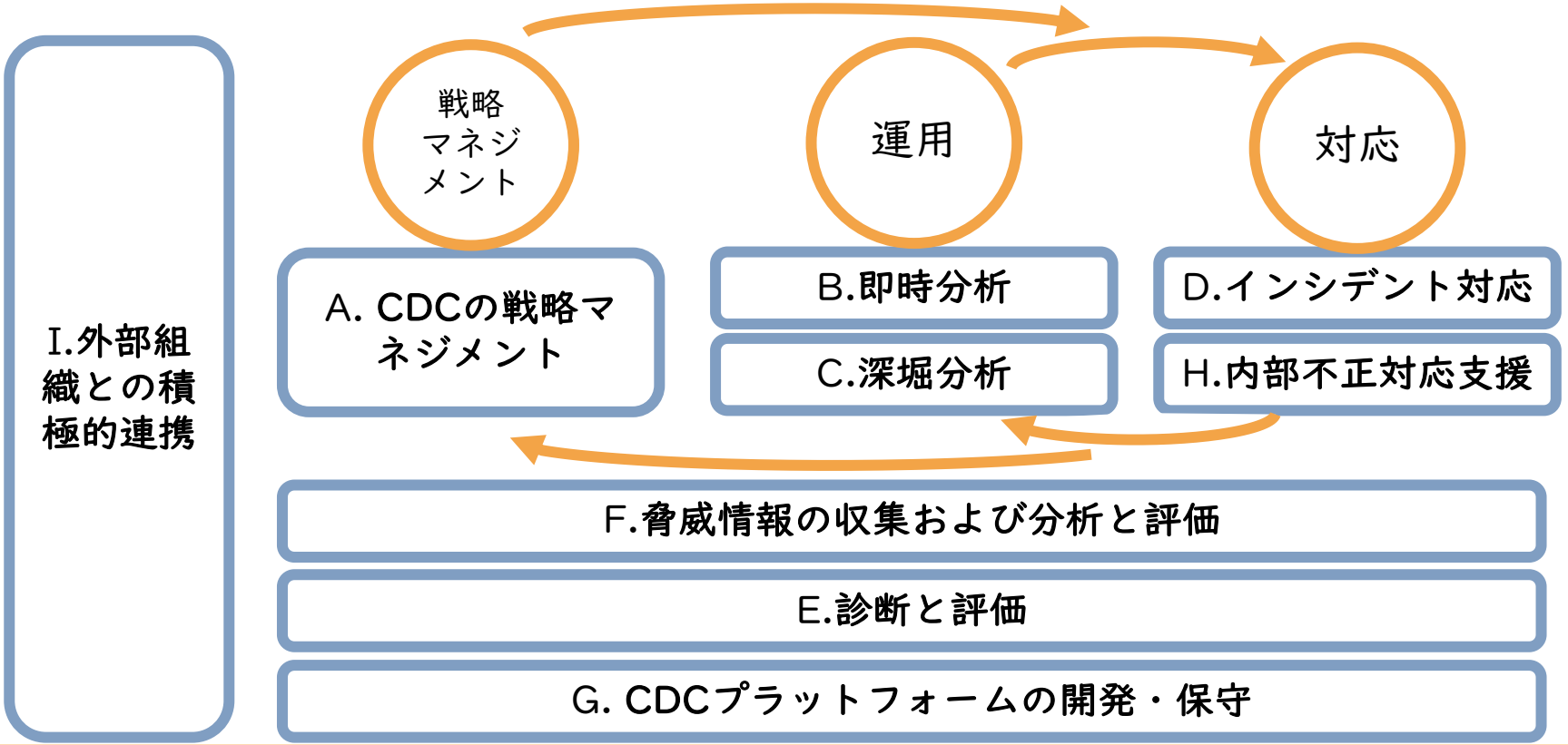
後段のマネジメントプロセスが実施できるように選んでおく

必要だが一覧になければ独自で追加する

推奨レベルは自組織でどの程度必要かを基準にする

© 2022 ISOG-J

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



© 2022 ISOG-J

推奨レベル

9.2. CDC サービスの推奨レベル

組織にとって最適な CDC サービスを実現するため、各サービスの必要性を表 1 に示す 5 つのレベルで考える。このレベルを用いることで、サービス実施の優先順位を明確にすることができる。

表 1　CDC サービスの推奨レベル

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	実装すべき最低限のサービス
スタンダード	一般的に実装が推奨されているサービス
アドバンスド	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
オプション	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

出典：JT-X1060

© 2022 ISOG-J

どこから手をつけるのか？

- 「できるところからやろう」
  - X.1060は継続的に改善を続けるフレームワーク
  - いきなり全てのサービスを実装できる組織はない。予算の問題、人員の問題、スキルの問題。
  - ベストプラクティスとしての64のサービスの中から優先度を決めて、できるところから着手する。

© 2022 ISOG-J

すでにSOC, CERT/CSIRTがある

- すでに部分的にセキュリティ統括、CDCを実装している、と考えることができる。
- サービスにマッピングして、どこができているかを明らかにする。
- サービス全体の優先度から見て、足りない部分の補強から着手する

© 2022 ISOG-J

サービスの選択時の考え方

- 実際のマネジメントプロセス（運用時）に運用が回ることを前提として最小限から考える
- リスクと予算から、最低限どこが必要かを決める

- すでにあるサービスをマッピングして、どこから始めるかを考える。
- 構築の最後のフェーズでセルフアセスメントで現状と目標を決める。
  - 「今はやらない」、「今はあるができていない」を認識する

© 2022 ISOG-J

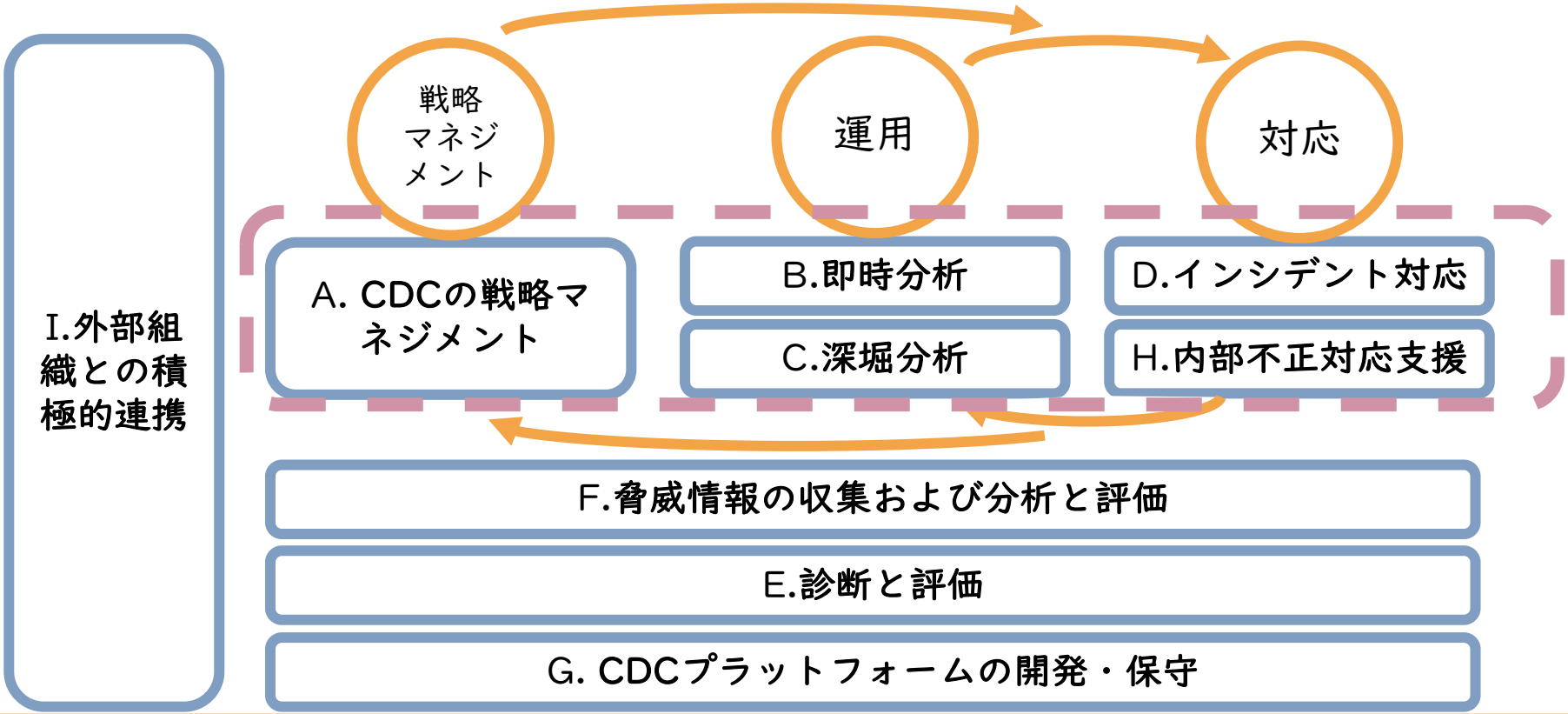
これからゼロからセキュリティの活動を始めたい

- セキュリティの活動を日々行う「マネジメント」プロセスと、サービスカテゴリのマッピングから、最低限継続的に運用をするためのサービスから実装する。

- 全部を自前で実装するのではなく、外部のアウトソースを活用することも検討する。
  - マネジメント系の判断をする部分は外部へ委託すべきではないので、そこは自分たちで行うことは認識しておく。

© 2022 ISOG-J

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



© 2022 ISOG-J

構築プロセス時　どこで行うかを決める

全部自分達でできない！

最低限やるべきことは行い、あとはアウトソースする

全てアウトソースすることはおすすめされない

© 2022 ISOG-J

構築プロセス：サービスのアサイン

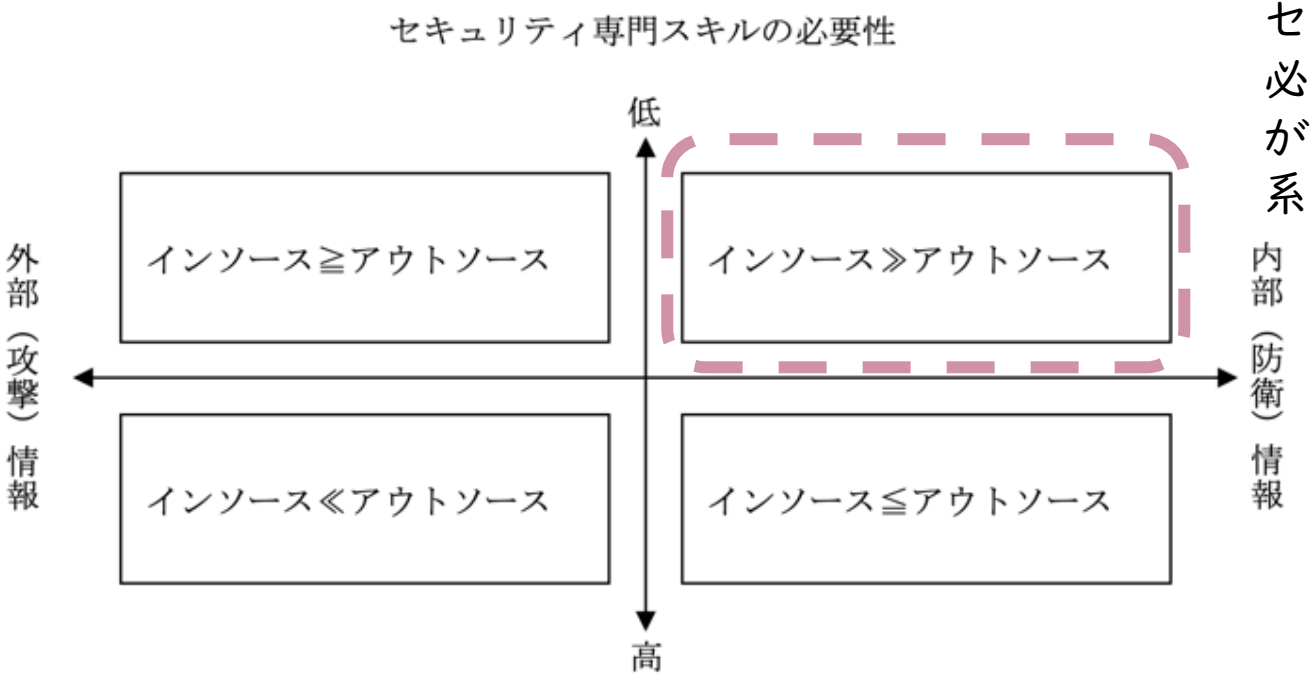


図5　調達の象限

セキュリティ専門スキルの必要性が低い、内部の情報が中心となるマネジメント系を中心に自前で実施する

判断や責任を持つのは自組織であることを意識

図はJT-X1060より

© 2022 ISOG-J

「割り当て」を意識する

- 全てをインハウスで行うのではなく、アウトソースやハイブリッドで行うことを意識する。

- やるべき全体像から、どこに割り当てるか。全体を俯瞰する。

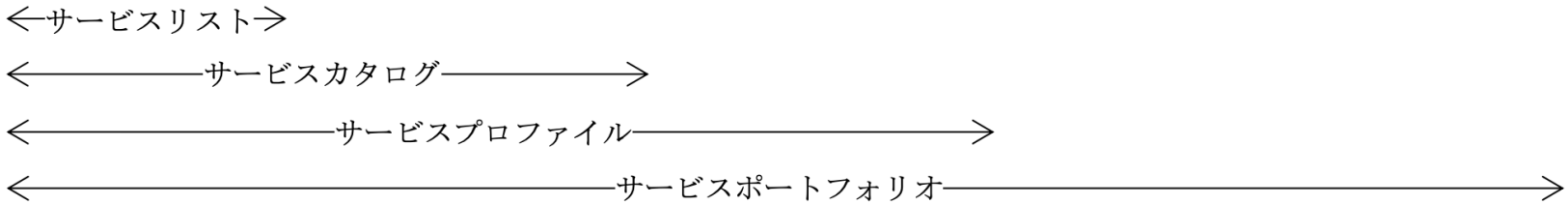
- SOCやCERT,CSIRT、セキュリティ統括やCDCといった名前は割り当てたチームにどのようなネーミングをするか、というだけ。
  - その名前のチームがどのようなサービスを持つかは組織によってバラバラ

© 2022 ISOG-J

構築プロセス時　スコアを決める

最終的には、サービスポートフォリオの一覧を作る

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	あるべき姿
サービス①	ベーシック	インソース(AB 部門)	3	5
サービス②	スタンダード	アウトソース(Z-MSSP)	2	4
サービス③	アドバンスド	未割り当て	1	2



図はJT-X1060より

© 2022 ISOG-J

構築プロセス：サービスのアセスメント

表3　CDCサービススコア

インソースの場合	
明文化された運用がCISOなど権限ある組織長に承認されている	+5点
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	+4点
運用が明文化されておらず、担当者に代わりに他者が臨時で一部の業務を代行できる	+3点
運用が明文化されておらず、担当者のみが業務を実施できる	+2点
実施できていない	+1点
インソースとしては実施しないと決めた	適用外

アウトソースの場合	
サービス内容と得られる結果を理解でき、想定通り	+5点
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	+4点
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	+3点
サービス内容と得られる結果を理解できていない	+2点
結果や報告を確認できていない	+1点
アウトソースとしては実施しないと決めた	適用外

セルフアセスメント
今のスコア
目標のスコア
2つを決める

図はJT-X1060より

© 2022 ISOG-J

さまざまなドキュメントやガイドの使い所を間違えない

- X.1060は組織のフレームワーク。個々のサービスのガイドラインや手順書ではない。
- ガイドラインや手順書はそれぞれのサービスをどう実装するか、どうするかを決めるときにそれぞれ参考にするもの。

NIST SP800との違いは？
ISMS, ISO 27001との違いは？
MITRE ATT&CKで対策をしているんだ。
FIRSTのドキュメントを参照しているんだ。

© 2022 ISOG-J

マネジメントプロセス

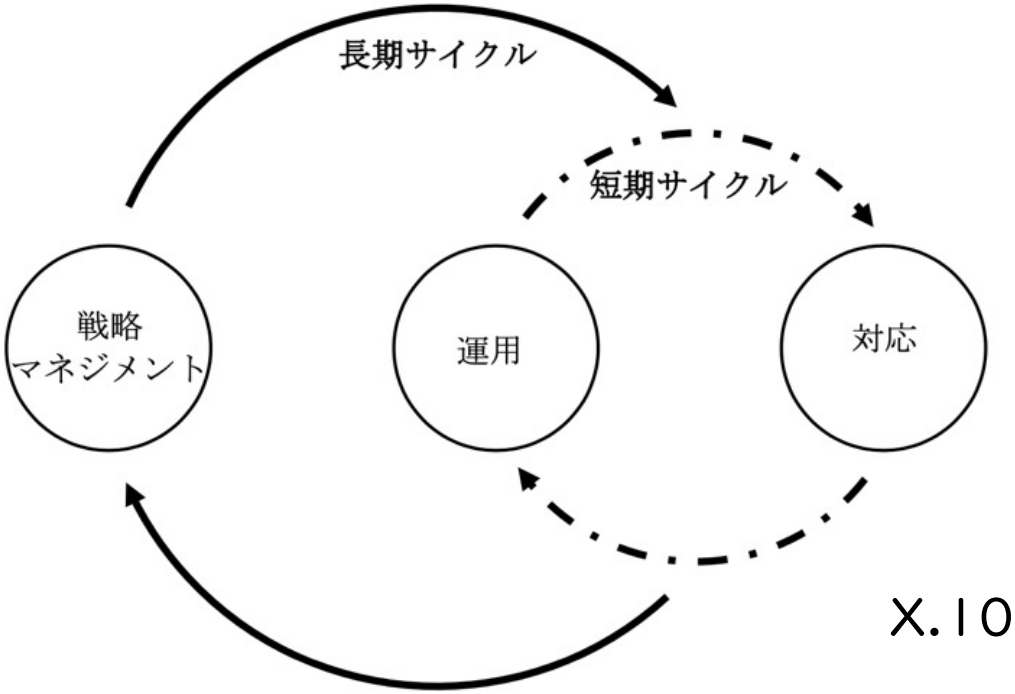


図 6　CDC マネジメントプロセス

サービスは具体的にどんな
プロセス、どんな手順？？

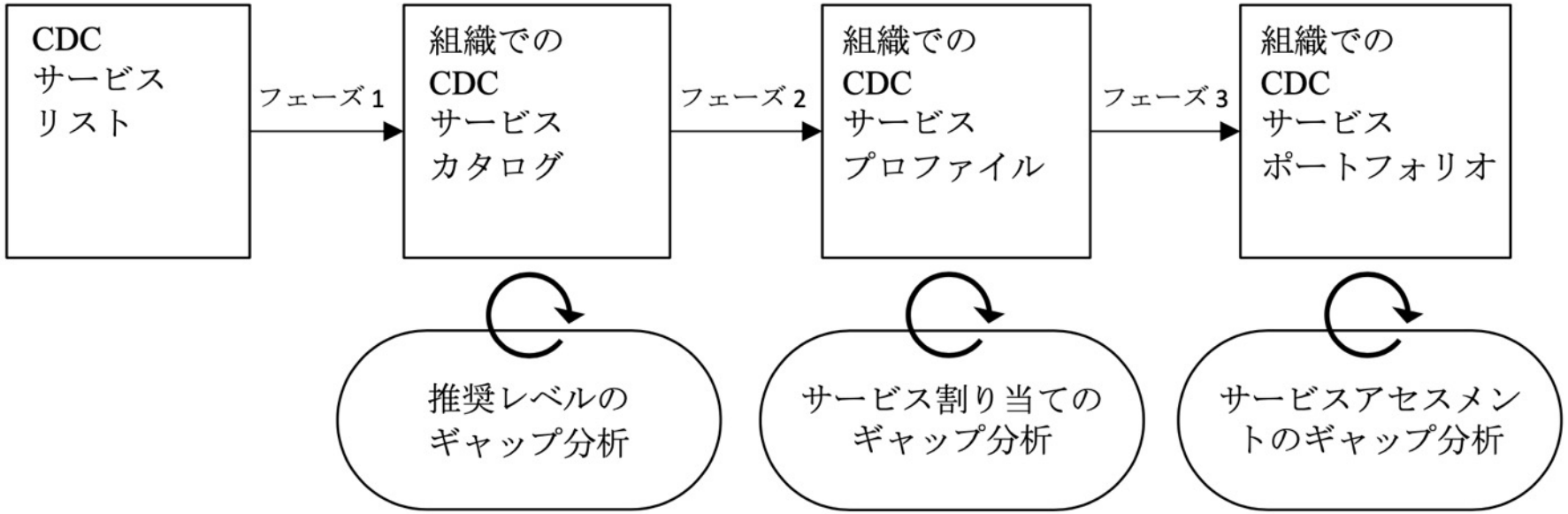
既存のドキュメントやガイドライン、すでに参考にしているものがあればそれを活用する

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

© 2022 ISOG-J

評価プロセス



図はJT-X1060より

図 7　CDC 評価プロセス

構築で行った3つのフェーズそれぞれで見直しをする

© 2022 ISOG-J

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？

© 2022 ISOG-J

評価プロセス

評価のタイミングは？

それぞれの組織次第です。監査などで決まっていればそれを活用しても良いです

ビジネスの環境の変化のタイミングで随時見直すのがスムーズに対応できるでしょう

© 2022 ISOG-J

評価プロセス

課題があるのはわかっているが、変えられない！

適切に権限は委譲されていますか？

継続的に改善を続けるフレームワークです。

© 2022 ISOG-J

本日のまとめ

- 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

© 2022 ISOG-J

今後の予定

- 2月末の次回の会議での承認に向けて、ブラッシュアップ中。
- 11月か1月にアフリカエリアとの会議で議論（遠隔）
- それまでに国内でも議論して知見を反映

© 2022 ISOG-J

次回以降の予定

- 議長からはなんでpptxなの？文書じゃないの？と言うツッコミもあるので、いずれ文書としてまとめ直して提出、する？？
  - 日本の知見が反映できるなら、どんどん入れる

- アフリカエリアだけではなく、利用したいこれからの国々へ利用を働きかけて、日本発の考え方を広げる。

© 2022 ISOG-J

・本資料の著作権は日本セキュリティオペレーション事業者協議会(以下、ISOG-J)に帰属します。
・引用については、著作権法で引用の目的上正当な範囲内で行われることを認めます。引用部分を明確にし、出典が明記されるなどです。
・なお、引用の範囲を超えると思われる場合もISOG-Jへご相談ください(info (at) isog-j.org　まで)。
・本文書に登場する会社名、製品、サービス名は、一般に各社の登録商標または商標です。®やTM、©マークは明記しておりません。
・ISOG-Jならびに執筆関係者は、このガイド文書にいかなる責任を負うものではありません。全ては自己責任にてご活用ください。

© 2022 ISOG-J