# D1-2 これからのセキュリティ組織はこう作る！
## ～教科書をもとにやってみよう！～

ISOG-J WG6

2024.11.25



© 2024 ISOG-J

# 本日のISOG-J WG6メンバー紹介

武井　滋紀
NTTテクノクロス株式会社

稲垣　洋平
株式会社 日本総合研究所

井上　圭
株式会社ラック

角田　玄司
ネットワンシステムズ株式会社

河島　君知
NTTデータ先端技術株式会社

野尻　泰弘
NECソリューションイノベータ株式会社

© 2024 ISOG-J

# 今日はこんなお話をします

- ITU-T勧告X.1060と「セキュリティ対応組織(SOC/CSIRT)の教科書」(以下、教科書)の概要
- 10月17日に公開した「教科書第3.2版」の概要と追加されたポイントのお話

- 実際に自分の組織をアセスメントしてみるハンズオン
  - ISOG-Jの教科書第3.2版の本文と付録のExcelシートを使います！
  - アンケートサイトでも回答できるように用意しています！


© 2024 ISOG-J

# アクセス先URL

- ISOG-J セキュリティ対応組織の教科書リリースページ
  - https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html
  - 本文のPDFと付録のセルフアセスメントシートをご用意ください

- アンケートサイト
  - （SurveymonkeyURL、当日公開）
  - みんなで回答するとその結果が見えます！ぜひこちらにも！
  - 後で資料に追記して期間限定で公開します（一般公開はしません）


© 2024 ISOG-J

# 日本セキュリティオペレーション事業者協議会

Information Security Operation providers Group Japan(ISOG-J)

2008年設立、2024年9月現在68社加盟、およそ300人のメンバー
(親団体はJNSA。オブザーバーに総務省と経済産業省)

代表：武智 洋(日本電気株式会社)
副代表：阿部 慎司(GMOサイバーセキュリティ byイエラエ株式会社)
副代表：早川 敦史(GMOサイバーセキュリティ byイエラエ株式会社)
副代表：武井 滋紀(NTTテクノクロス株式会社)

| | |
|---|---|
| セキュリティオペレーションガイドラインWG (WG1) | 上野 宣(株式会社トライコーダ) |
| セキュリティオペレーション技術WG (WG2) | 川口 洋(株式会社川口設計) |
| セキュリティオペレーション認知向上・普及啓発WG (WG4) | 阿部 慎司(GMOサイバーセキュリティ byイエラエ株式会社) |
| セキュリティオペレーション連携 (WG6) | 武井 滋紀(NTTテクノクロス株式会社) |

今日はここの話が中心です。


© 2024 ISOG-J

# セキュリティ対応組織の教科書　第3.2版

- 2024-10-17公開(第3.1版はその1年前)
  - https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html
- 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
  - 野尻 泰弘, NECソリューションイノベータ株式会社
  - 吉田 佳音, 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
  - 早川 敦史, GMO サイバーセキュリティ byイエラエ株式会社
  - 井上 博文
  - 角田 玄司,ネットワンシステムズ株式会社
  - 青木 翔, 株式会社日立製作所
  - 後藤 啓太, SCSKセキュリティ株式会社
  - 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
  - 藤原 稔也, NTT データ先端技術株式会社
  - 石橋 拓己
  - 稲垣 洋平, 株式会社日本総合研究所
  - 竹之内 一晃, パーソルクロステクノロジー株式会社
  - 宇野 文康, 日立システムズ株式会社
  - 井上 圭, 株式会社ラック
  - ISOG-J WG6 メンバー

© 2024 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”

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


© 2024 ISOG-J

# 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
- 日本側関係者
  - 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


© 2024 ISOG-J

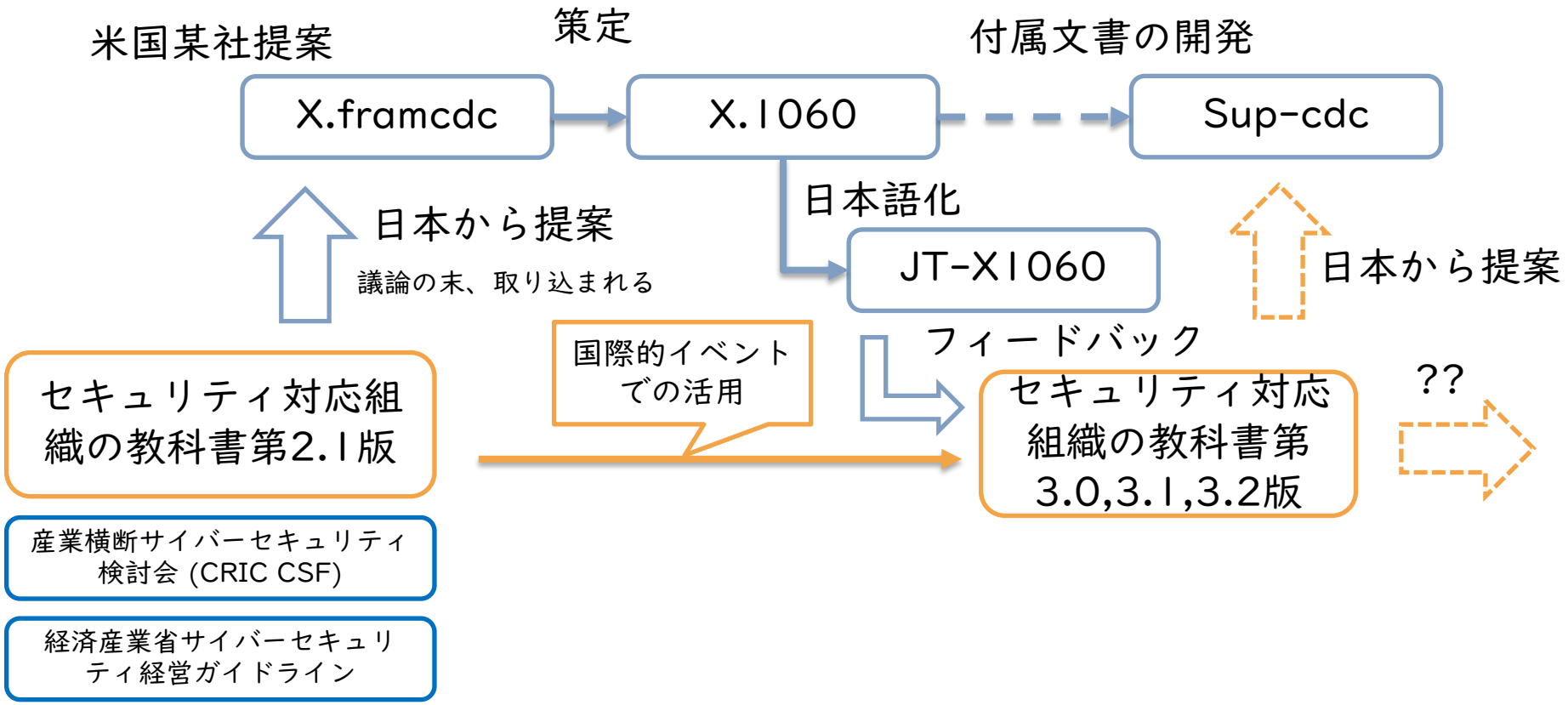
# 特設ページのロゴも日本から！

ロゴは阿部さんデザイン
SG17事務局から総務省に貸与依頼

Youtube JPCERT/CCチャンネル
阿部さん出演説明動画


© 2024 ISOG-J

# 教科書のこれまで





© 2024 ISOG-J

# 教科書第3.2版で追加されたお話

- エグゼクティブサマリ
  - トップダウンで読んで組織作りに利用していただきたい！
- セルフアセスメントシートが復活
  - 第2.1版でも人気だったあのシートが復活しました！
- どうから着手したらいいか実例を追記
  - 64のサービスをどこから着手するかの考え方の例を追加しました


© 2024 ISOG-J

# X.1060に至る背景

ビジネスリスクとしてのセキュリティ

広がり続ける組織と連携の幅

▼

情シスの一部　　SOC / CSIRT

新たな組織体の必要性


© 2024 ISOG-J

# Cyber Defence Centre, 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。


© 2024 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

国レベル ◀▶ 産業界 ◀▶ 学術

「セキュリティ」では「何をするか」


© 2024 ISOG-J

# X.1060/JT-X1060における組織体制

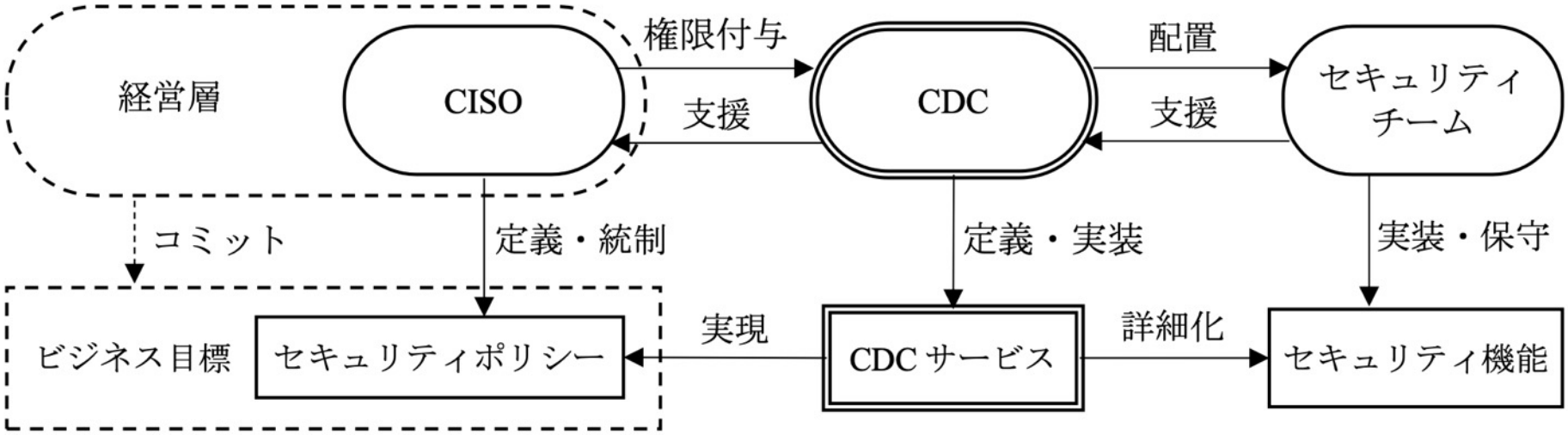
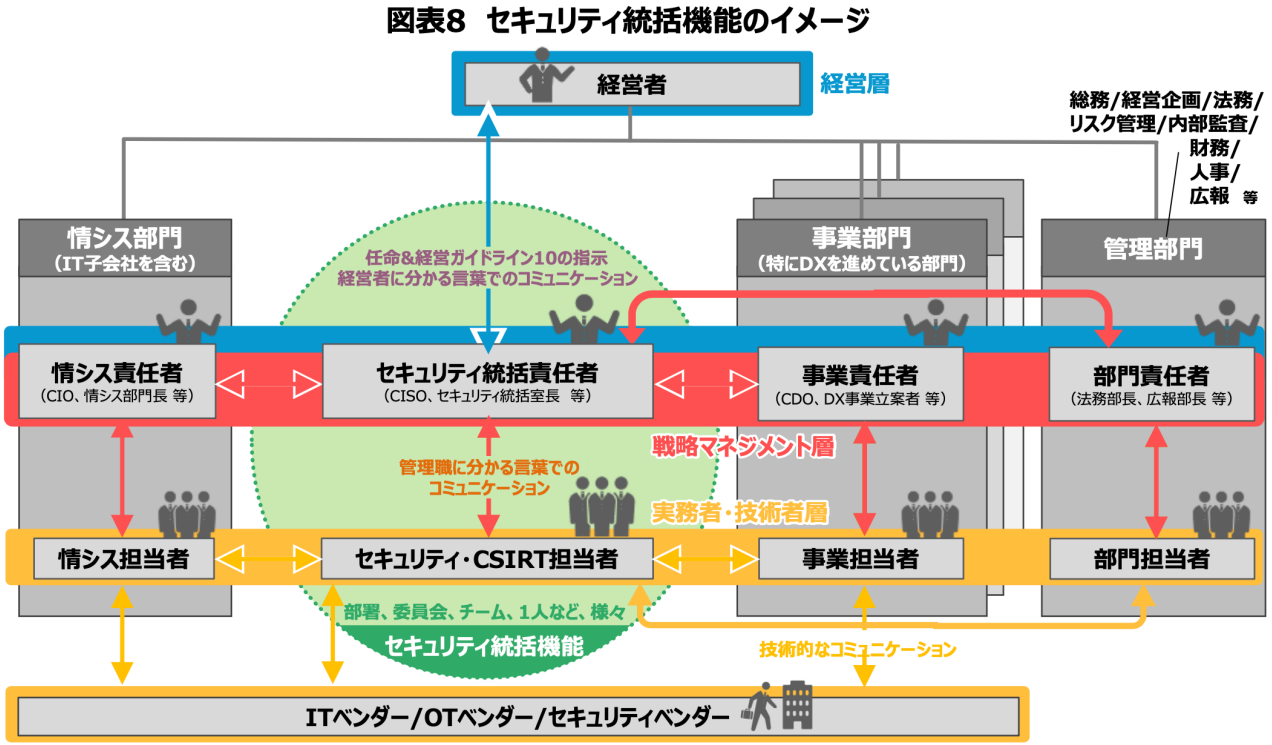



図 1　CDC の運営における関係者とその役割

図はJT-X1060より


© 2024 ISOG-J

# セキュリティ統括機能のイメージ



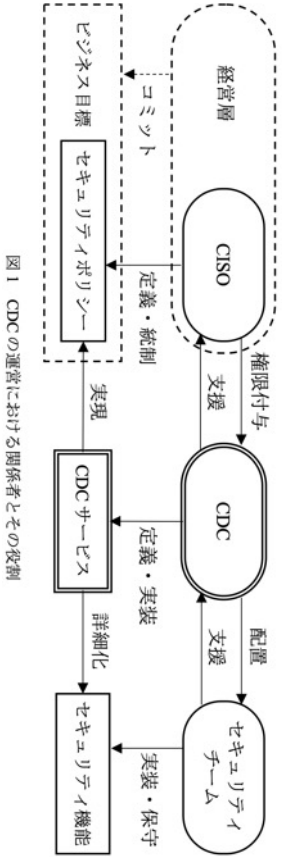




図1　CDCの運営における関係者とその役割

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


© 2024 ISOG-J

# 構築フェーズ


© 2024 ISOG-J

# X.1060の構築は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


© 2024 ISOG-J

# 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 |
| | | |

© 2024 ISOG-J

# X.1060, ISOG-J セキュリティ対応組織の教科書

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


© 2024 ISOG-J

## 64……

「どれからやればいいですか？」

「全部やるのは無理です」

後半ハンズオンをやりながら説明します


© 2024 ISOG-J

# サービスポートフォリオシート

- X.1060の構築プロセスの結果、最終的に作成される「サービスポートフォリオ」をExcelシート化したもの
- 64のサービスに対して、推奨レベル、割り当て、サービススコアを記入できる。
  - サービスの概要についてもシートに入っているので参考にできます。

| 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(As-Is) | あるべき姿(To-Be) |
| (サービス名) | （ウェイト） | (実施場所) | (スコア) | (スコア) |


© 2024 ISOG-J

# インソース・アウトソース

| タイプ | 説明 |
| --- | --- |
| インソース | 組織内のチームでサービスを実現する。責務を負う担当を明確にする。 |
| アウトソース | 組織外のチームでサービスを実現する。委託先を明確にする。 |
| 併用 | インソースとアウトソースを併用する。責務を負う担当と委託先を明確にする。 |
| 未割り当て | 組織に存在すべきサービスはあるが、割り当てられていない |


© 2024 ISOG-J

# アセスメントのスコア

## インソースの場合

| スコア | 説明 |
|---|---|
| 5 | 明文化された運用はCISOなど権限ある組織長に承認されている |
| 4 | 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 |
| 3 | 運用が明文化されておらず、担当者に代わり他者が臨時で一部の業務を実施できる |
| 2 | 運用が明文化されておらず、担当者が業務を実施できる |
| 1 | 実施できていない |
| 評価対象外 | インソースでの実装を検討したものの、結果として実施しないと判断した |

## アウトソースの場合

| スコア | 説明 |
|---|---|
| 5 | サービス内容と得られる結果を理解でき、想定通り |
| 4 | 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 |
| 3 | 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 |
| 2 | サービス内容と得られる結果を理解できていない |
| 1 | 結果や報告を確認できていない |
| 評価対象外 | アウトソースでの実装を検討したものの、結果として実施しないと判断した |


© 2024 ISOG-J

# サービスポートフォリオシート

セキュリティ対応組織の教科書第3.1版からexcelシートをそのまま付録に

組織内の推奨レベル

どこでやるか

今のスコア

目標のスコア

サービスの解説

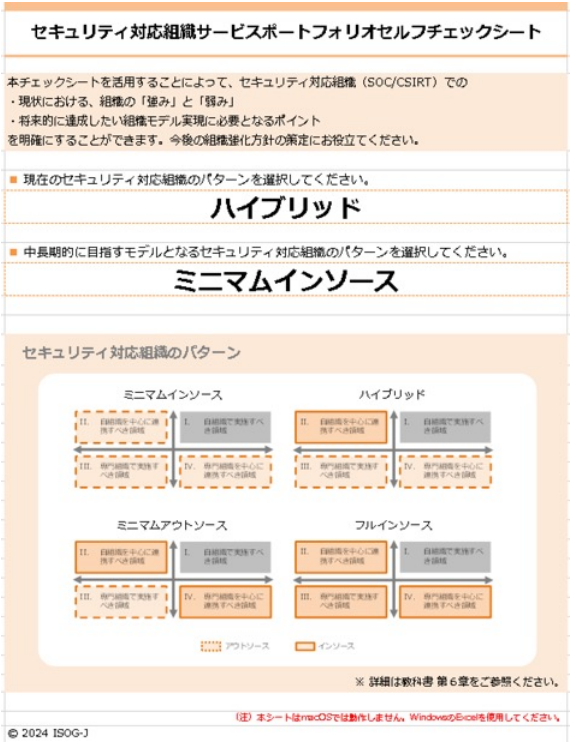
| | A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|---|
| 1 | カテゴリー | サービス | | 推奨レベル | サービス割り当て | サービススコア | | 解説文 |
| 2 | | 項番 | 名称 | | | 現状(As-Is) | あるべき姿(To-Be) | |
| 3 | | | | | | | | |
| 4 | A. CDC の戦略マネジメント | A-1 | リスクマネジメント | | | | | 「リスクマネジメント」サービスは、リスクに対して組織を方向づけ、コントロールできるよう、A-2からA-13を含む統括的な活動を実現する。 |
| 5 | | A-2 | リスクアセスメント | | | | | 「リスクアセスメント」サービスは、組織の資産や脅威、セキュリティ対策の観点から、組織のリスクレベル把握を実現する。 |
| 6 | | A-3 | ポリシーの企画立案 | | | | | 「ポリシーの企画立案」サービスは、具体的なセキュリティポリシーの定義や、ガイドラインの作成に関するすべての活動を支援する。 |
| 7 | | A-4 | ポリシー管理 | | | | | 「ポリシー管理」サービスは、ポリシーや組織の規定を評価して定期的に見直しや、新たな外部要件（例えば、規制やガイドライン）への準拠を実現する。 |
| 8 | | A-5 | 事業継続性 | | | | | 「事業継続性」サービスは、組織の事業継続計画の実現や実行が正しく行われるために必要な経営上の機能を支援する。 |
| 9 | | A-6 | 事業影響度分析 | | | | | 「事業影響度分析」のサービスは、様々なイベントやシナリオから起こり得る影響の体系的なアセスメントを実現する。このサービスは、発生しうる損失の規模を組織が理解するのに役立つ。直接的な金銭的損失だけでなく、利害関係者の信頼喪失や風評被害など、その他の影響も対象となる場合もある。 |
| 10 | | A-7 | リソース管理 | | | | | 「リソース管理」サービスは、各種セキュリティ活動を支えるリソース（人、予算、システムなど）計画と、各サービスへの適切な割り当てを実現する。 |
| 11 | | A-8 | セキュリティアーキテクチャ設計 | | | | | 「セキュリティアーキテクチャ設計」サービスは、ビジネスをセキュアにするためのアーキテクチャの確立を実現する。<br>システムの設計やビジネスプロセスの制約（例えば、サプライチェーン）を考慮した各種セキュリティ対策をまとめ、CDCのプラットフォーム（カテゴリーGにあるような）の開発や維持を実現する。 |



© 2024 ISOG-J

# セルフアセスメントシート

## 第2.1版のものからX.1060に合わせて刷新されました！



セキュリティ対応組織サービスポートフォリオセルフチェックシート

本チェックシートを活用することによって、セキュリティ対応組織（SOC/CSIRT）での
・現状における、組織の「強み」と「弱み」
・将来的に達成したい組織モデル実現に必要となるポイント
を明確にすることができます。今後の組織強化方針の策定にお役立てください。

■ 現在のセキュリティ対応組織のパターンを選択してください。

ハイブリッド

■ 中長期的に目指すモデルとなるセキュリティ対応組織のパターンを選択してください。

ミニマムインソース

セキュリティ対応組織のパターン



※ 詳細は教科書 第6章をご参照ください。

（注）本シートはmacOSでは動作しません。WindowsのExcelを使用してください。

© 2024 ISOG-J

記入日 202X/YY/ZZ

| | | | インソース | | | | | | アウトソース | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 新のイ…ソ…結果としての実装を検討したも…判 | 実施できていない | 運用が明文化されておらず、担当者が業務を実施できる | 運用が明文化されており、担当者が業務に代わり代行できる | 運用が明文化されており、担当者が業務を実施できると | 権限ある組織長に承認されているなど明文化された運用は0…10 | アウトソースでの実施を検討したも…判断した | 結果や報告を確認できていない | サービス内容と得られる結果を理解できていない | 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 | 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 | サービス内容と得られる結果を理解でき、想定通り | ※インソースとアウトソースを併用している場合は、成熟度の高い方をチェックしてください。 |
| カテゴリー | サービス | 領域 | 0 | 1 | 2 | 3 | 4 | 5 | 0 | 1 | 2 | 3 | 4 | 5 | 備考 |
| A.CDOの戦略マネジメント | A-1. リスクマネジメント | 領域 I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-2. リスクアセスメント | 領域 I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-3. ポリシーの企画立案 | 領域 I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-4. ポリシー管理 | 領域 I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-5. 事業継続性 | 領域 I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-6. 事業影響度分析 | 領域 I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-7. リソース管理 | 領域 I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-8. セキュリティアーキテクチャ設計 | 領域 II | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |



© 2024 ISOG-J

## あなたのセキュリティ対応組織における"カテゴリー別"ポートフォリオ

202X/YY/ZZ

現状の組織（ハイブリッドパターン）におけるカテゴリー別成熟度を5段階で評価しています。
組織の「強み」と「弱み」を抽出し、現在のセキュリティ対応において有効に働いている機能と、改善が必要な機能を見える化しています。
マクロな観点での指標として、成熟度向上の方針策定にお役立てください。

| カテゴリー | 成熟度 |
|---|---|
| A. CDCの戦略マネジメント | 2.7 /5 |
| B. 即時分析 | 2.8 /5 |
| C. 深掘分析 | 3.0 /5 |
| D. インシデント対応 | 2.6 /5 |
| E. 診断と評価 | 2.7 /5 |
| F. 脅威情報の収集および分析と評価 | 2.8 /5 |
| G. CDCプラットフォームの開発・保守 | 3.0 /5 |
| H. 内部不正対応支援 | 2.0 /5 |
| I. 外部組織との積極的連携 | 2.3 /5 |

### 現状のセキュリティ対応組織の強み

残念ながら「強み」と言えるサービスはありません。

### 現状のセキュリティ対応組織の弱み

**H. 内部不正対応支援**
内部統制、内部不正に関する対応の支援を十分行えておらず、ガバナンスやコンプライアンス面で貢献しにくくなっています。組織的に機能しているとは言えない状況ですので、着実に実施できるよう改めて業務を見直してください。

**I. 外部組織との積極的連携**
対外組織との連携が希薄であり、組織のレベルアップ、存在価値の向上につなげることができていません。組織的に機能しているとは言えない状況ですので、着実にできるよう改めて業務を見直してください。

v3.2

## あなたのセキュリティ対応組織における"サービス別"ポートフォリオ

202X/YY/ZZ

A. CDCの戦略マネジメント

| | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 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

| | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 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. 深掘分析

| | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 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

| | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 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 | | | | | |

■：インソース　■：アウトソース

E. 診断と評価

| | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 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

| | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 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

| | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| G-1. | リスクマネジメント | | | | | |
| G-2. | リスクアセスメント | | | | | |
| G-3. | ポリシーの企画立案 | | | | | |
| G-4. | ポリシー管理 | | | | | |
| G-5. | 事業継続性 | | | | | |
| G-6. | 事業影響度分析 | | | | | |
| G-7. | リソース管理 | | | | | |
| G-8. | セキュリティアーキテクチャ設計 | | | | | |
| G-9. | トリアージ基準管理 | | | | | |
| G-10. | 対応策選定 | | | | | |
| G-11. | 品質管理 | | | | | |
| G-12. | セキュリティ監査 | | | | | |
| G-13. | 認証 | | | | | |

H. 内部不正対応支援

| | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 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

| | | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|---|
| 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との連携 | | | | | |
| 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 | | | | | |

現状の組織のサービス成熟度を5段階で示し、モデルとするミニマムインソースパターン到達へのポイントも列挙していますので、サービス強化にお役立てください。

**より強化すべきインソースのサービス**

目組織での能力をより高めるべきもの
- I-5. セキュリティ関連団体との連携
- I-7. 幹部向けセキュリティ報告
- F-5. 脅威情報の活用

**より強化すべきアウトソースのサービス**

より効果的なアウトソースとなるよう改善すべきもの
- A-12. セキュリティ監査
- I-3. セキュリティコンサルティング
- G-13. 新規セキュリティツール検証

**インソースへの切り替えを検討すべきサービス**

インソースの方が対応力の強化につながるもの
- I-2. 教育・トレーニング
- G-11. CDCシステム運用
- D-6. インシデント通知

**アウトソースへの切り替えを検討すべきサービス**

アウトソースした方が強化しやすいもの
- I-6. 技術報告
- I-4. セキュリティベンダーとの連携
- H-2. 内部不正検知・再発防止支援

v3.2

© 2024 ISOG-J



© 2024 ISOG-J

# マネジメントフェーズ


© 2024 ISOG-J

# マネジメントプロセス

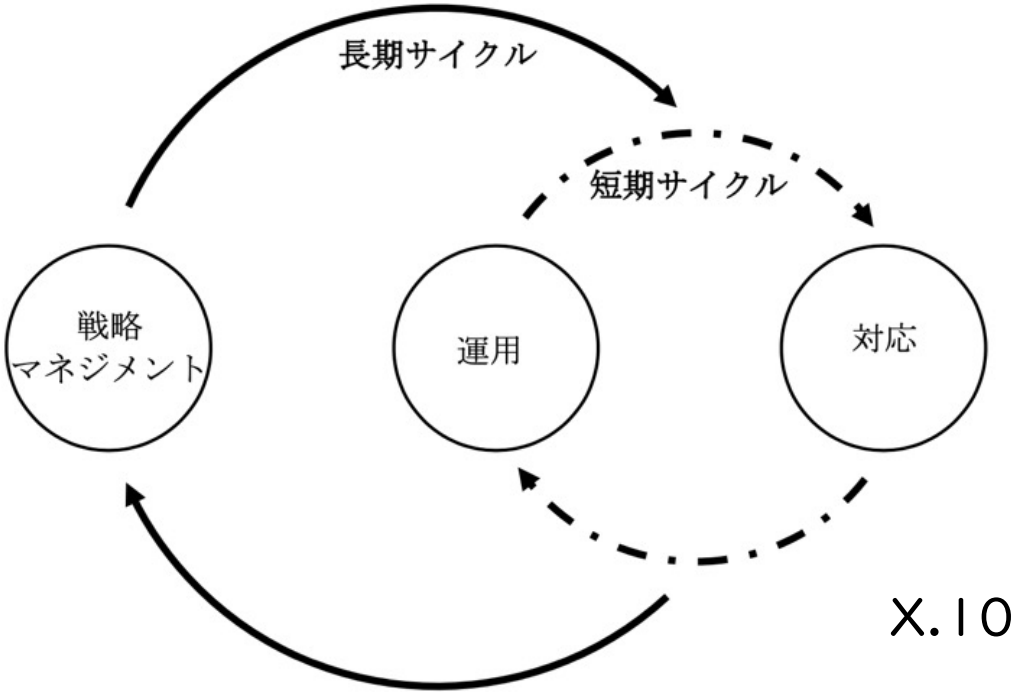



図 6　CDC マネジメントプロセス

サービスは具体的にどんな
プロセス、どんな手順？？

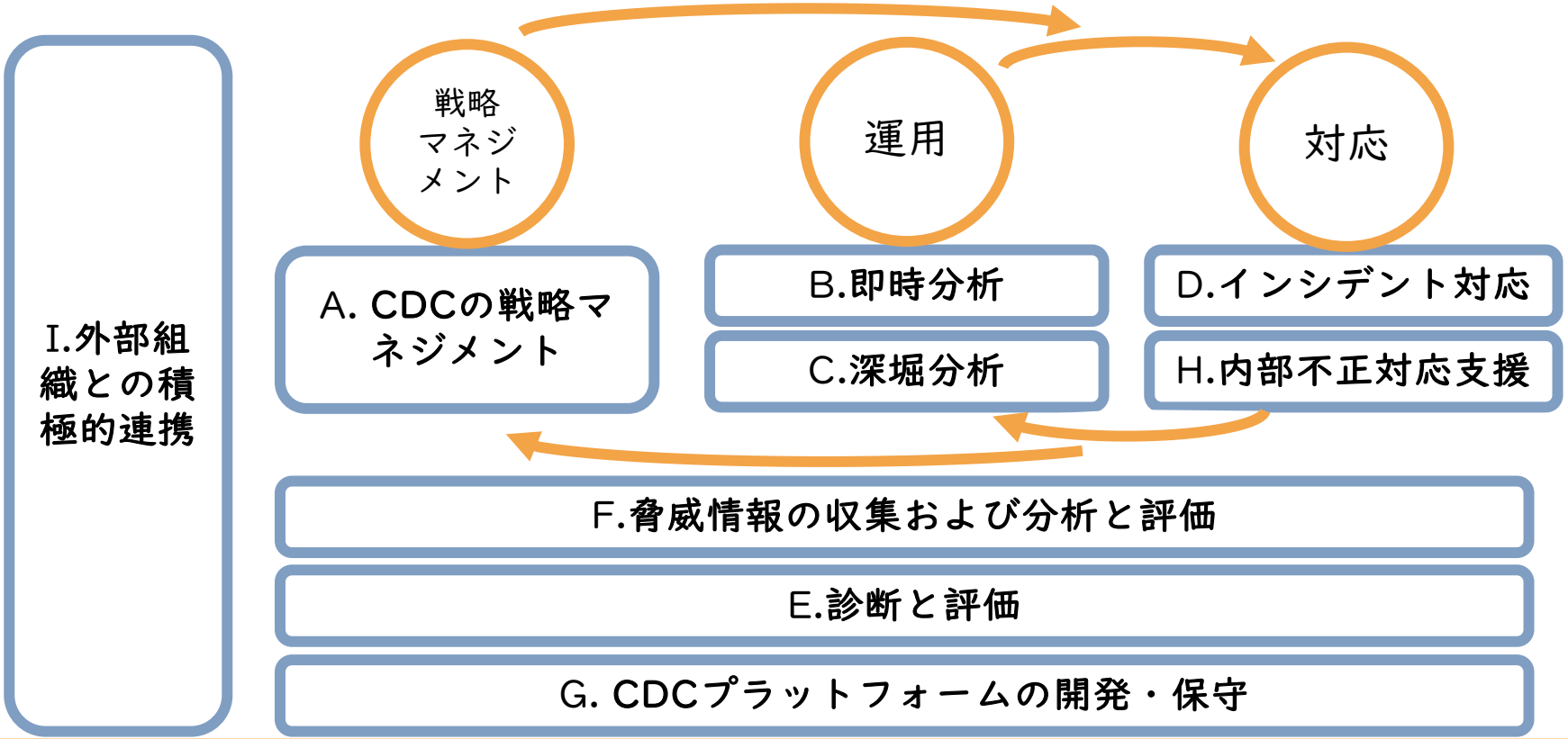
既存のドキュメントやガイドライン、すでに参考にしているものがあればそれを活用する

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


© 2024 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




© 2024 ISOG-J

# 評価フェーズ


© 2024 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？


© 2024 ISOG-J

# ここまでのまとめ

- X.1060/JT-X1060の実用書としてのセキュリティ対応組織の教科書第3.2版
- フィードバックを受けて毎年コンテンツを追加しています

- セルフアセスメントシートや、どこから着手するかも含めて日本で使いやすいものになっています！
- ぜひご活用ください！


© 2024 ISOG-J

# ハンズオン


© 2024 ISOG-J

# アクセス先URL

- ISOG-J セキュリティ対応組織の教科書リリースページ
  - https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html
  - 本文のPDFと付録のセルフアセスメントシートをご用意ください

- アンケートサイト
  - （SurveymonkeyURL、当日公開）
  - みんなで回答するとその結果が見えます！ぜひこちらにも！
  - 後で資料に追記して期間限定で公開します（一般公開はしません）


© 2024 ISOG-J

# X.1060の構築は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

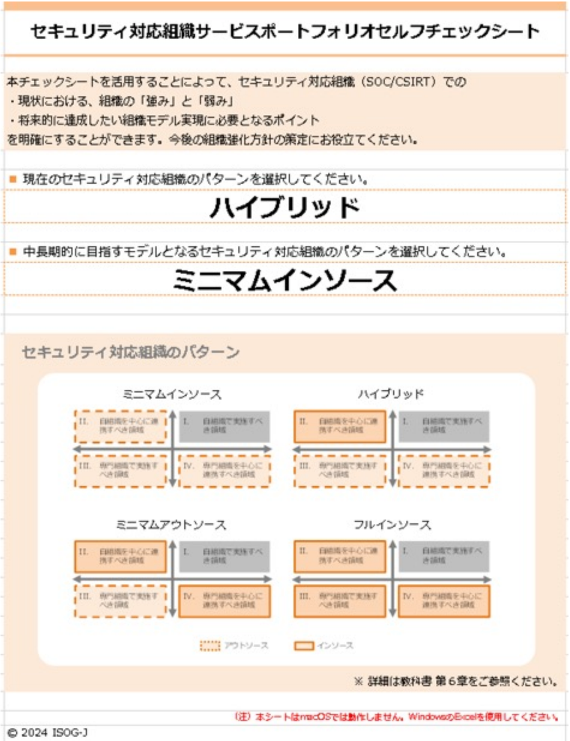
今のスコアと目標のスコアを決める（サービスポートフォリオを作る）

- 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


© 2024 ISOG-J

# セルフアセスメントシート

インソースとアウトソースの組織の形から、強みや弱みもわかります




記入日 202X/YY/ZZ

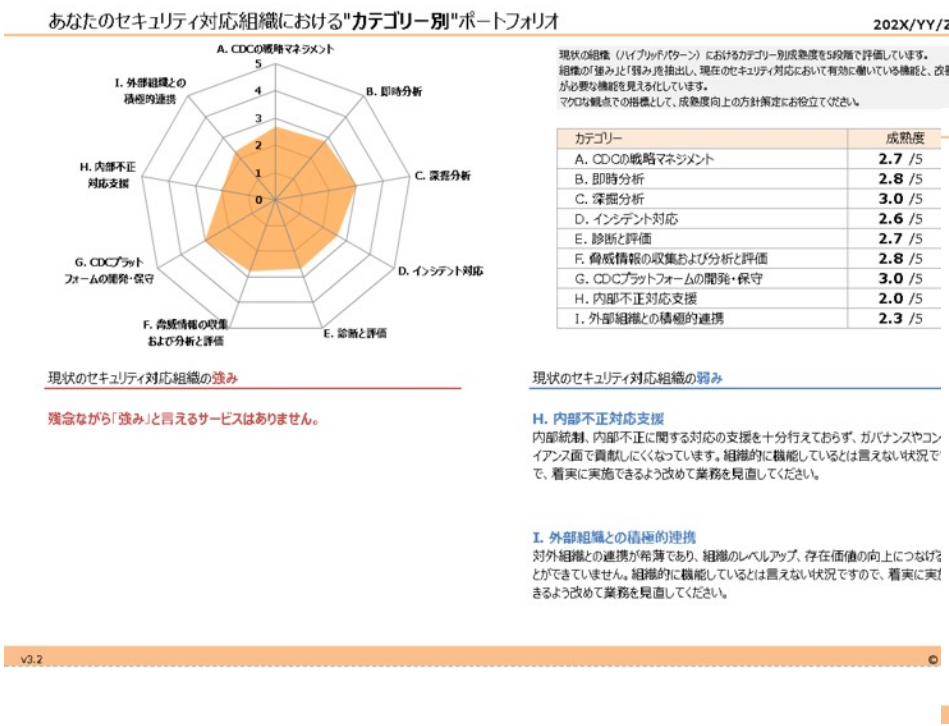
| カテゴリー | サービス | 領域 | インソース 0: インソースでの実装を検討したものの、結果として実施しないと判断した | インソース 1: 実施できていない | インソース 2: 運用が明文化されておらず、担当者が業務を実施できる | インソース 3: 運用が明文化されておらず、担当者に代わり他者が臨時で一部の業務を代行できる | インソース 4: 運用が明文化されており、担当者と交代して他者が業務を実施できる | インソース 5: 明文化された運用はCISOなど権限ある組織長に承認されている | アウトソース 0: アウトソースでの実装を検討したものの、結果として実施しないと判断した | アウトソース 1: 結果や報告を確認できていない | アウトソース 2: サービス内容と得られる結果を理解できていない | アウトソース 3: 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 | アウトソース 4: 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 | アウトソース 5: サービス内容と得られる結果を理解でき、想定通り | 備考 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A. CDOの戦略マネジメント | A-1. リスクマネジメント | 領域I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-2. リスクアセスメント | 領域I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-3. ポリシーの企画立案 | 領域I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-4. ポリシー管理 | 領域I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-5. 事業継続性 | 領域I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-6. 事業影響度分析 | 領域I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-7. リソース管理 | 領域I | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |
| | A-8. セキュリティアーキテクチャ設計 | 領域II | ● | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | ○ | |

※インソースとアウトソースを併用している場合は、成熟度の高い方をチェックしてください。


© 2024 ISOG-J

# セルフアセスメントシート

スコアを入れるとグラフなどで可視化されます



© 2024 ISOG-J

# 構築プロセスを順に進めるなら

1. 64のサービスで、社内や組織内ですでに実施しているかどうかをマッピングする
2. 64のサービスそれぞれに、推奨度を決める
    1. やらないサービスを決定する
3. 実施するサービスに、実施するチームを割り当てる
4. 実施するサービスにスコアを設定する


© 2024 ISOG-J

とは言ったものの

どこからやればいいのか問題


© 2024 ISOG-J

「どれからやればいいですか？」

「全部やるのは無理です」


© 2024 ISOG-J

はい。全部実施するのは難しいです

自組織でリスクアセスメントをして
必要なサービスから実施してください


© 2024 ISOG-J

「……はぁ」


© 2024 ISOG-J

## ということで

今日は自組織で必要そうなサービスから見てみましょう


© 2024 ISOG-J

# 考え方

1. すでに社内や自組織内でやっているサービスをマッピングする

2. 構築プロセスの次、マネジメントプロセスで動く組織を意識して選択する

3. インソースとアウトソースの考え方から、自組織に必要そうなものから考える


© 2024 ISOG-J

# 考え方1

1. すでに社内や自組織内でやっているサービスをマッピングする
    1. 法律や規制、ガイドラインですでにやることになっているものを明らかにする
    2. やらなければならないものは必要なはず
    3. すでにやっているということは必要性があるはず


© 2024 ISOG-J

# 考え方2

- マネジメントプロセスで動く組織

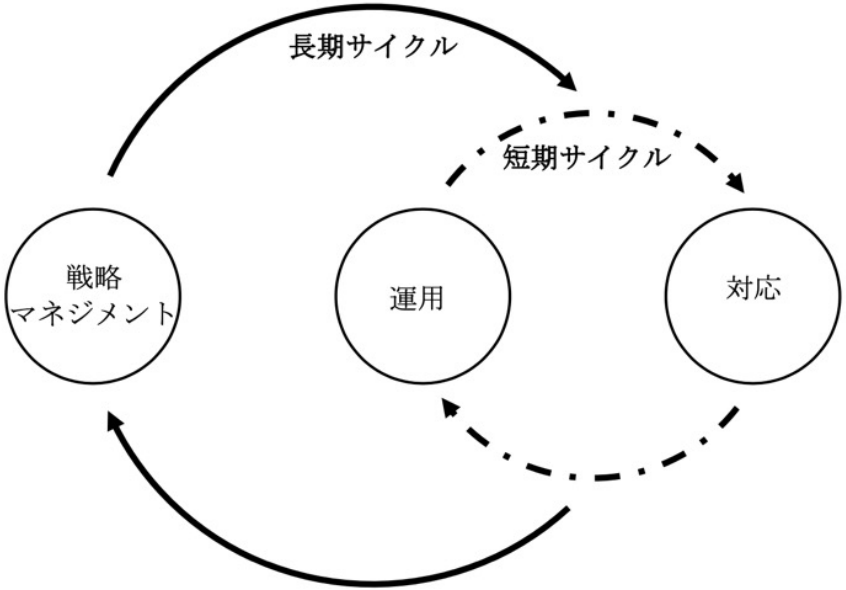


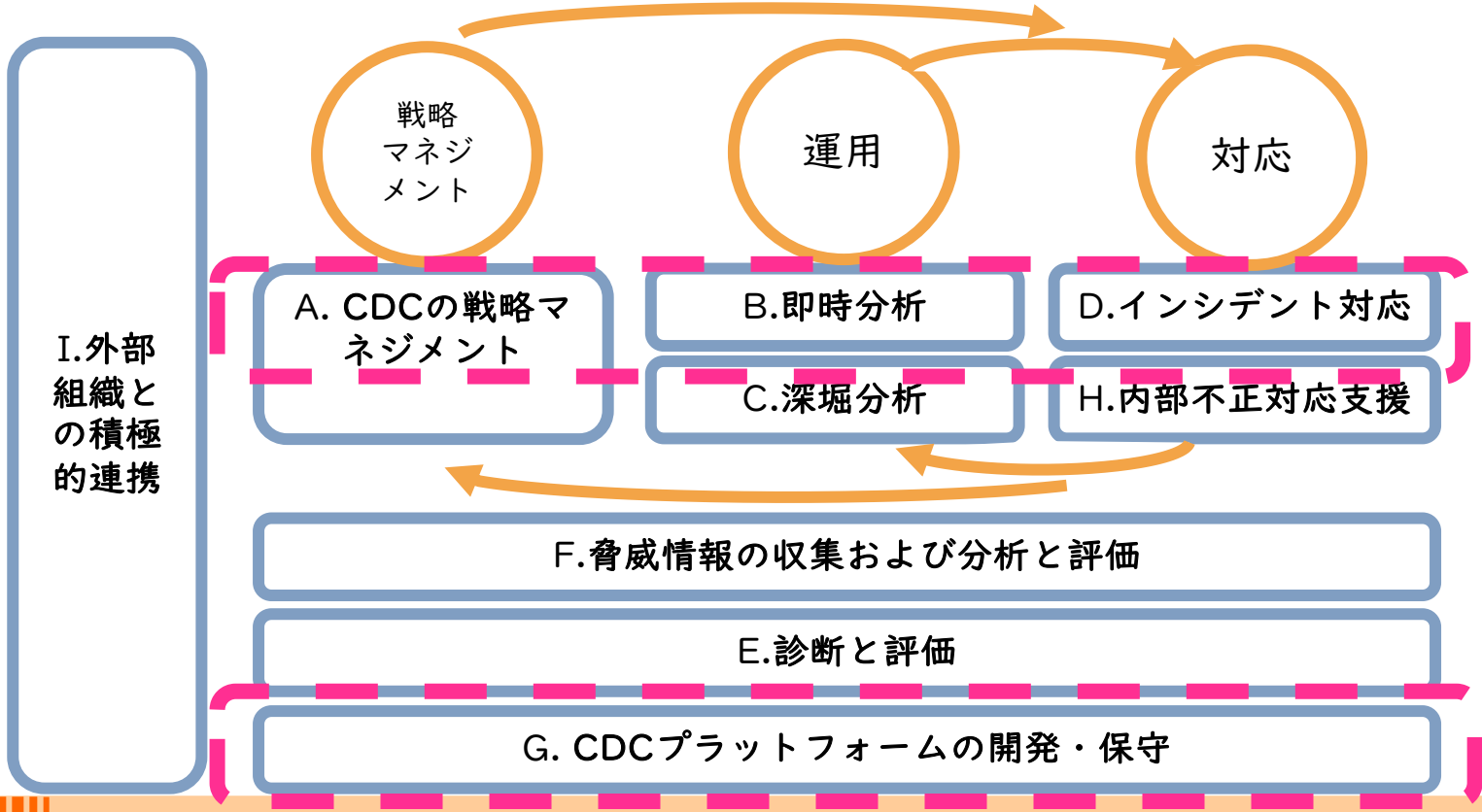

図6　CDCマネジメントプロセス

構築したら日々の運用のマネジメントです。
この2つのサイクルを動かすことで日々の運用ができます

図はJT-X1060より


© 2024 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




カテゴリ
A→G→B→D
の流れを意識
してサービス
を選択します

© 2024 ISOG-J

# 考え方3

- インソースとアウトソースの考え方

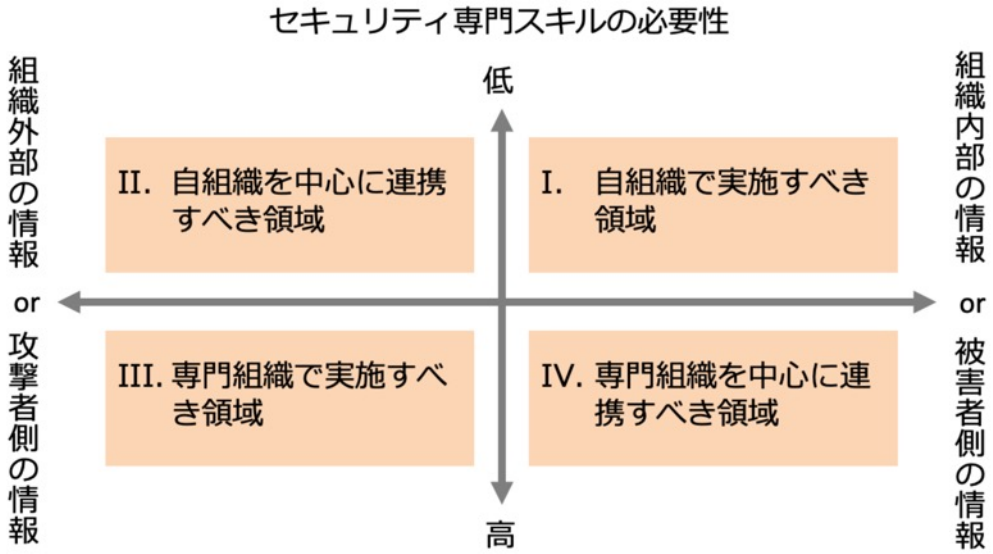



図 14　セキュリティ対応の4領域

自組織でやりそうなところから見る
I. 自組織で実施すべき領域
↓
II. 自組織を中心に連携すべき領域
IV. 専門組織を中心に連携すべき領域
↓
III. 専門組織で実施すべき領域


© 2024 ISOG-J

# 64のサービスを割り当ててみると

図 16 セキュリティ対応の役割分担

目安として、それぞれの領域にサービスが割り当てられています

これまでの考え方を当てはめてみると、
「右上の領域」で「カテゴリA,D,G」のもの
「左上の領域」で「カテゴリA,D」のもの
「右下の領域」で「カテゴリB,G」のもの
「左下の領域」で「カテゴリD,G」のもの

あたりからやってみましょう


© 2024 ISOG-J

# (参考)インソース・アウトソース

| タイプ | 説明 |
| --- | --- |
| インソース | 組織内のチームでサービスを実現する。責務を負う担当を明確にする。 |
| アウトソース | 組織外のチームでサービスを実現する。委託先を明確にする。 |
| 併用 | インソースとアウトソースを併用する。責務を負う担当と委託先を明確にする。 |
| 未割り当て | 組織に存在すべきサービスはあるが、割り当てられていない |


© 2024 ISOG-J

# (参考)アセスメントのスコア

## インソースの場合

| スコア | 説明 |
|---|---|
| 5 | 明文化された運用はCISOなど権限ある組織長に承認されている |
| 4 | 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 |
| 3 | 運用が明文化されておらず、担当者に代わり他者が臨時で一部の業務を実施できる |
| 2 | 運用が明文化されておらず、担当者が業務を実施できる |
| 1 | 実施できていない |
| 評価対象外 | インソースでの実装を検討したものの、結果として実施しないと判断した |

## アウトソースの場合

| スコア | 説明 |
|---|---|
| 5 | サービス内容と得られる結果を理解でき、想定通り |
| 4 | 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 |
| 3 | 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 |
| 2 | サービス内容と得られる結果を理解できていない |
| 1 | 結果や報告を確認できていない |
| 評価対象外 | アウトソースでの実装を検討したものの、結果として実施しないと判断した |


© 2024 ISOG-J

それでは、セルフアセスメントシートを埋めてみましょう


© 2024 ISOG-J

# 進め方

1. 領域Iから順にA,B,D,Gのサービスをセルフアセスメントしてみます
2. Excelシートで該当のものを埋めてみてください
3. Surveymonkeyのアンケートサイトでも回答してみてください
    1. アンケートに答えると、他の皆さんと比較した結果も見えるようになります
    2. Excelシートが使えない方もアンケートサイトで回答できます
    3. 結果は後日資料に追記して参加者のみ一定期間ダウンロードできるようにします
    4. 結果については一般公開はしません


© 2024 ISOG-J

# アクセス先URL

- ISOG-J セキュリティ対応組織の教科書リリースページ
  - https://isog-j.org/output/2023/Textbook_soc-csirt_v3.html
  - 本文のPDFと付録のセルフアセスメントシートをご用意ください

- アンケートサイト
  - （SurveymonkeyURL、当日公開）
  - みんなで回答するとその結果が見えます！ぜひこちらにも！
  - 後で資料に追記して期間限定で公開します（一般公開はしません）


© 2024 ISOG-J

# アンケートサイトの活用

- （SurveymonkeyURL、当日公開）

- 4つのブロックごとに今日の参加者がどんな状況なのかお互いの参考にできます。ぜひ入力してみてください

- データは匿名化しますので気にせず入力してみてください

- わからないところはISOG-J WGメンバーにその場でも相談できます！


© 2024 ISOG-J

# I. 自組織で実施すべき領域のサービス

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-10. 対応策選定
A-11. 品質管理
D-2. インシデントハンドリング
D-6. インシデント通知
D-7. インシデント対応報告
G-11. CDCシステム運用

- （SurveymonkeyURL、当日公開）
- 入力が終わったら「次へ」を押してください
  - 結果が反映されます


© 2024 ISOG-J

# II. 自組織を中心に連携すべき領域

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-12. セキュリティ監査
A-13. 認証
D-1. インシデント報告受付
D-3. インシデント分類

- （SurveymonkeyURL、当日公開）
- 入力が終わったら「次へ」を押してください
  - 結果が反映されます


© 2024 ISOG-J

# IV. 専門組織を中心に連携すべき領域

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
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-4. エンドポイントセキュリティ製品基本運用
G-6. クラウドセキュリティ製品基本運用
G-9. 分析基盤基本運用
G-12. 既設セキュリティ対応ツール検証

- （SurveymonkeyURL、当日公開）
- 入力が終わったら「次へ」を押してください
  - 結果が反映されます


© 2024 ISOG-J

# III. 専門組織で実施すべき領域

D-4. インシデント対応・封じ込め
D-5. インシデント復旧
G-3. ネットワークセキュリティ製品高度運用
G-5. エンドポイントセキュリティ製品高度運用
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-10. 分析基盤高度運用
G-13. 新規セキュリティツール検証

- （SurveymonkeyURL、当日公開）
- 入力が終わったら「**戻る**」を押してください
  - 「完了」を押すとアンケートが終了してしまい、戻れなくなります


© 2024 ISOG-J

# ここから先は？

- 今日は全部のスコアリングまでしていませんが、後でゆっくりやってみてください
- 他のカテゴリC,E,F,H,Iは、すでに実施しているもの、必要そうなところから追加してみてください

カテゴリ
C:深堀分析
E:診断と評価
F:脅威情報の収集および分析と評価
H:内部不正対応支援
I:外部組織との積極的連携

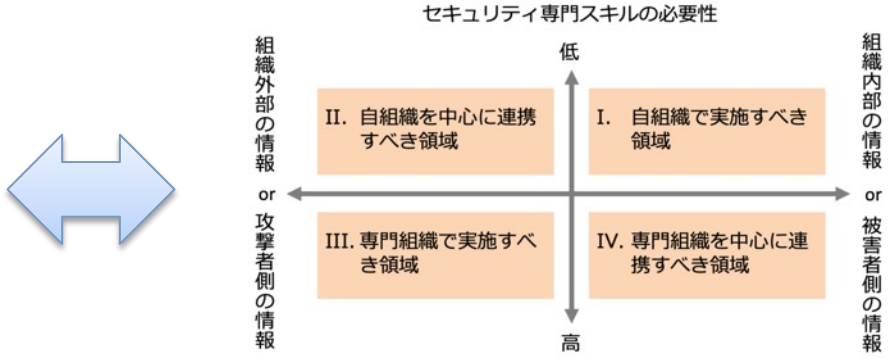


図 14　セキュリティ対応の4領域


© 2024 ISOG-J

## セルフアセスメントシートを作ったあとは？

全部を5にすることは
目標ではありません！

目標の組織の形になるまで
継続的に見直しを続けましょう

「PD~~CA~~」
で終わったりしませんよね？


© 2024 ISOG-J

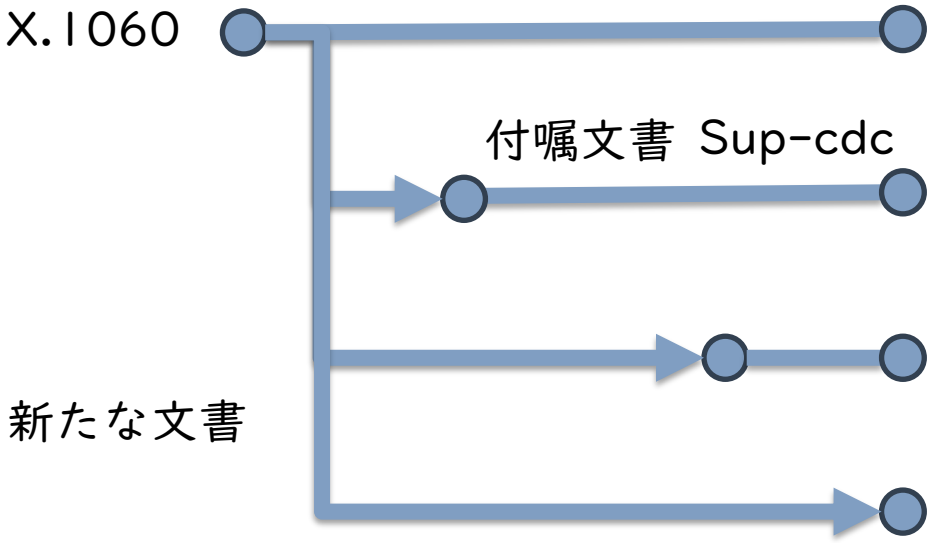
# X.1060の標準化の現場から


© 2024 ISOG-J

# X.1060の今後

- 広がる文書、高まる期待

アフリカエリアからの活用について
注目が高まっている





© 2024 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。


© 2024 ISOG-J