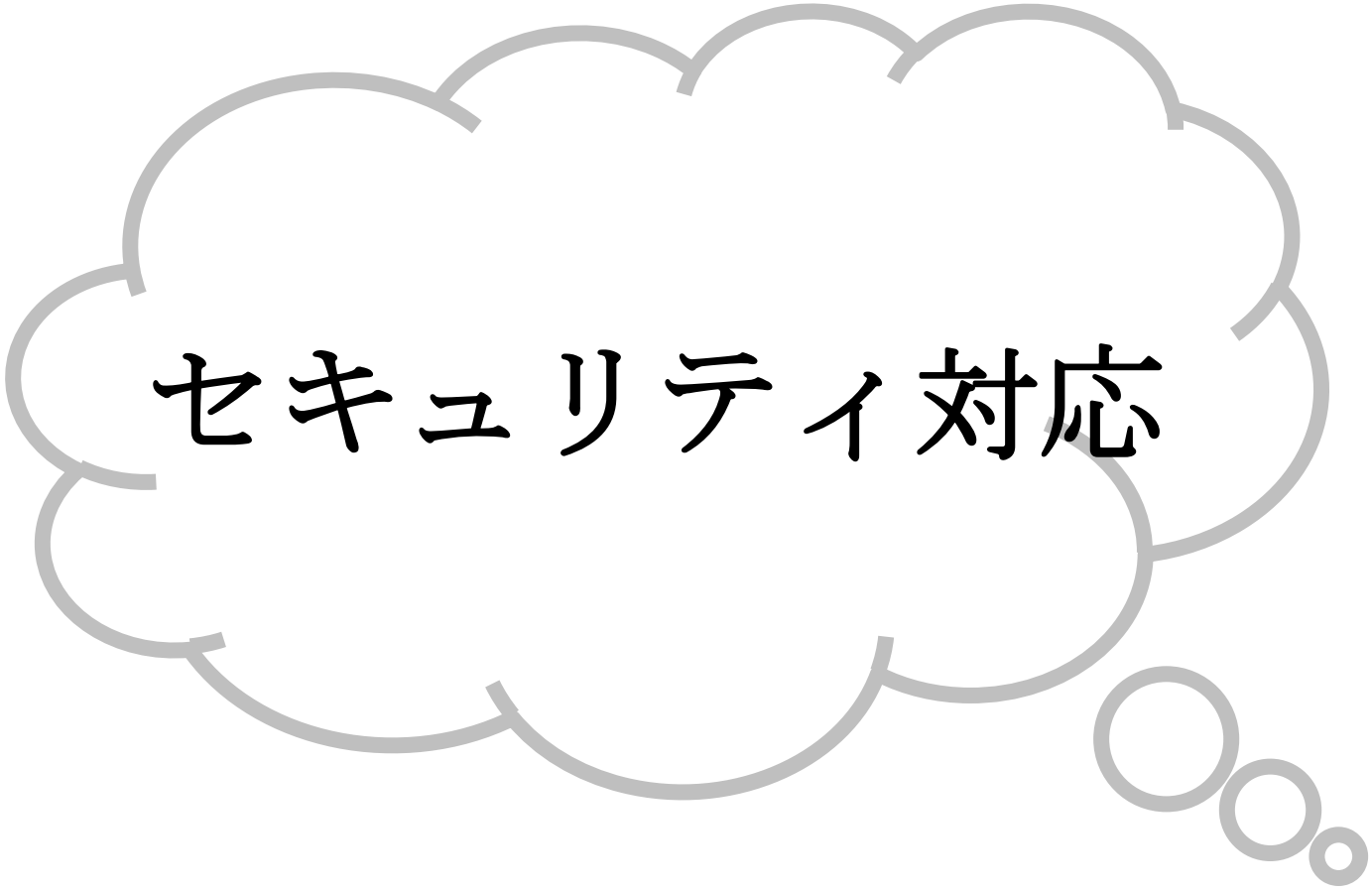
「セキュリティ対応組織（SOC/CSIRT）の教科書」ハンドブック化と情報共有の「5W1H」改版について

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

ＮＴＴセキュリティ・ジャパン株式会社
アナリストチームリーダー兼マネージャー / セキュリティプリンシパル

阿部 慎司

セキュリティ対応組織の教科書
ハンドブック
と
成熟度セルフチェックシート
ISOMM
(ISOG-J SOC/CSIRT Maturity Model)
のご紹介



- 経営者の思うセキュリティ対応
- セキュリティ責任者が思うセキュリティ対応
- 現場が思うセキュリティ対応

立場によって考えることが異なることを理解しつつ
それぞれに合った考え方（ガイドライン）を把握する

セキュリティ対応組織の教科書 v2.1

セキュリティ対応する組織が持つべき

9の機能と

その機能が担うべき

54の役割を定義

A．セキュリティ対応組織運営
A-1．全体方針管理
A-2．トリアージ基準管理
A-3．アクション方針管理
A-4．品質管理
A-5．セキュリティ対応効果測定
A-6．リソース管理

B．リアルタイムアナリシス（即時分析）
B-1．リアルタイム基本分析
B-2．リアルタイム高度分析
B-3．トリアージ情報収集
B-4．リアルタイム分析報告
B-5．分析結果問合受付

C．ディープアナリシス（深掘分析）
C-1．ネットワークフォレンジック
C-2．デジタルフォレンジック
C-3．検体解析
C-4．攻撃全容解析
C-5．証拠保全

D．インシデント対応
D-1．インシデント受付
D-2．インシデント管理
D-3．インシデント分析
D-4．リモート対処
D-5．オンサイト対処
D-6．インシデント対応内部連携
D-7．インシデント対応外部連携
D-8．インシデント対応報告

E．セキュリティ対応状況の診断と評価
E-1．ネットワーク情報収集
E-2．アセット情報収集
E-3．脆弱性管理・対応
E-4．自動脆弱性診断
E-5．手動脆弱性診断
E-6．標的型攻撃耐性評価
E-7．サイバー攻撃対応力評価

F．脅威情報の収集および分析と評価
F-1．内部脅威情報の整理・分析
F-2．外部脅威情報の収集・評価
F-3．脅威情報報告
F-4．脅威情報の活用

G．セキュリティ対応システム運用・開発
G-1．ネットワークセキュリティ製品基本運用
G-2．ネットワークセキュリティ製品高度運用
G-3．エンドポイント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高度運用
G-5．ディープアナリシス(深掘分析)ツール運用
G-6．分析基盤基本運用
G-7．分析基盤高度運用
G-8．既設セキュリティ対応ツール検証
G-9．新規セキュリティ対応ツール調査、開発
G-10．業務基盤運用

H．内部統制・内部不正対応支援
H-1．内部統制監査データの収集と管理
H-2．内部不正対応の調査・分析支援
H-3．内部不正検知・防止支援

I．外部組織との積極的連携
I-1．社員のセキュリティ対する意識啓発
I-2．社内研修・勉強会の実施や支援
I-3．社内セキュリティアドバイザーとしての活動
I-4．セキュリティ人材の確保
I-5．セキュリティベンダーとの連携
I-6．セキュリティ関連団体との連携

上司は読んでくれるだろうか…

もっと簡単に「セキュリティ対応組織の教科書」を理解したい（してもらいたい）

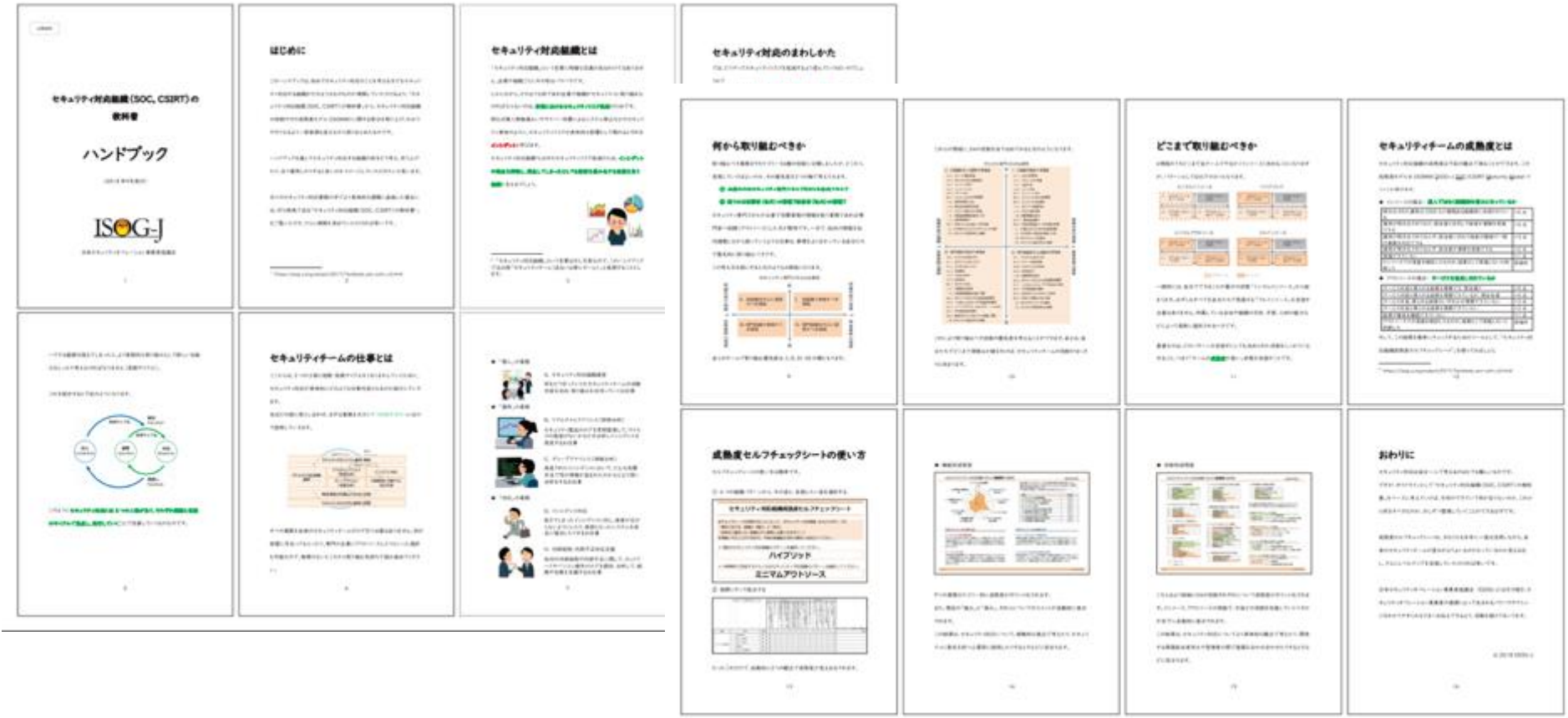
セキュリティ対応組織の教科書 ハンドブック v1.0

読みやすい概要版。

A3　8up両面で

印刷にちょうどいい

16ページ+1枚



https://isog-j.org/output/2017/Textbook_soc-csirt_handbook_v1.0.pdf

日本セキュリティオペレーション事業者協議会 ISOG-J

セキュリティ対応組織（SOC/CSIRT）の教科書 ハンドブック 別紙

セキュリティ対応の役割一覧

A	**セキュリティ対応組織運営**	
	何をどう守っていくのかセキュリティチームの活動内容を決め、具体的な取り組みを仕切っていくお仕事	
A-1	全体方針管理	セキュリティ対応全体の活動についての方針を管理し、推進する
A-2	トリアージ基準管理	セキュリティ事故が起こってしまったときの対応優先度を決める
A-3	アクション方針管理	セキュリティ事故が起こってしまったときの対処方針を決める
A-4	品質管理	運用や対応において問題がなかったか把握し、改善する
A-5	セキュリティ対応効果測定	全体としてのセキュリティ対策がうまくいっているか指標をまとめ、効果を確認する
A-6	リソース管理	セキュリティ対応に必要な予算、人員、システムを計画し、配分する

B	**リアルタイムアナリシス（即時分析）**	
	セキュリティ製品のログを常時監視して、ウイルスの感染がないかなどを分析し、インシデントを発見するお仕事	
B-1	リアルタイム基本分析	ネットワークやサーバーのログを分析する
B-2	リアルタイム高度分析	基本分析で足りない場合、より多くのログやデータ等含めた分析する
B-3	トリアージ情報収集	対応優先度を決めるため、分析結果以外の関連情報を集める
B-4	リアルタイム分析報告	リアルタイム分析で分かったことを随時まとめて報告する
B-5	分析結果照合受付	報告した内容について問い合わせ対応する

C	**ディープアナリシス（深掘分析）**	
	発見されたインシデントにおいて、どんな攻撃手法で何の情報が盗まれたのかなど、より深い分析をするお仕事	
C-1	ネットワークフォレンジック	リアルタイムで行いきれなかった詳細な分析を行う
C-2	デジタルフォレンジック	被害に遭った端末で何が起こったのか明らかにする
C-3	検体解析	ウイルスがどのような動きをするものだったか解析する
C-4	攻撃全容解析	これまでの分析結果全てをふまえ、攻撃の目的や手法を明らかにする
C-5	証拠保全	裁判などのために必要な証拠を保存しておく

D	**インシデント対応**	
	起きてしまったインシデントに対し、被害が広がらないようにしたり、原因となったシステムを安全に復旧したりするお仕事	
D-1	インシデント受付	即時分析で見つかった、外部からの指摘されたインシデントを受け付ける
D-2	インシデント管理	受け付けたインシデントの対応進捗管理を行う
D-3	インシデント分析	受け付けたインシデントをどのように対処していくべきか判断する
D-4	リモート対処	監視センターなどからリモートで対処、復旧する
D-5	オンサイト対処	現場に駆けつけて対処、復旧する
D-6	インシデント対応内部連携	社内の関係者（経営者、関係部門）などへ報告、協力依頼する
D-7	インシデント対応外部連携	社外の関係者（顧客、取引企業）などへの説明、調整をする
D-8	インシデント対応報告	インシデントの影響や原因、対処内容についてとりまとめる

E	**セキュリティ対応状況の診断と評価**	
	脆弱性診断や標的型メール訓練などによりセキュリティがきちんと守られているか評価するお仕事	
E-1	ネットワーク情報収集	守るべきネットワークの構成を把握する
E-2	アセット情報収集	守るべき端末やサーバーの情報に加えてアプリケーションの情報も収集する
E-3	脆弱性管理・対応	ネットワークやアセット情報と脆弱性情報を突き合わせ、問いシステムを把握、対応する
E-4	自動脆弱性診断	簡易な診断として、機械的な脆弱性診断を行う
E-5	手動脆弱性診断	より正確な診断として、手動による脆弱性診断を行う
E-6	標的型攻撃耐性評価	標的型メール訓練などにより高度な攻撃へに耐えられるか確かめる
E-7	サイバー攻撃対応力評価	サイバー攻撃対応訓練を行い、きちんと対応できるか確かめる

F	**脅威情報の収集および分析と評価**	
	ネット上のセキュリティニュースやこれまでチームで見つけたインシデントを随時まとめ、次に生かすお仕事	
F-1	内部脅威情報の整理・分析	社内で発生したインシデントに関する情報を集めや長期的な改善案を整理する
F-2	外部脅威情報の収集・評価	公開された セキュリティ情報を収集し、未対策の脅威がないか確認する
F-3	脅威情報報告	内部外部の脅威情報を定期的に取りまとめ報告する
F-4	脅威情報の活用	脅威情報を関係者へ展開し、みんなに活用してもらう

G	**セキュリティ対応システム運用・開発**	
	セキュリティ対応に必要なシステムを設置したり、管理したりするお仕事	
G-1	ネットワークセキュリティ製品基本運用	ネットワークセキュリティ製品の設置や設定、その運用を行う
G-2	ネットワークセキュリティ製品高度運用	ネットワークセキュリティ製品のオプション機能などをより便利に活用する
G-3	エンドポイントセキュリティ製品基本運用	エンドポイントセキュリティ製品の導入や設定、その運用を行う
G-4	エンドポイントセキュリティ製品高度運用	エンドポイントセキュリティ製品のオプション機能などをより便利に活用する
G-5	ディープアナリシス（深掘分析）ツール運用	フォレンジックやウイルス解析のためのツールを管理、運用する
G-6	分析基盤基本運用	SIEMなどに代表される分析用システムを導入、運用する
G-7	分析基盤高度運用	SIEMのカスタマイズや検知開発により、より高い性能を引き出す
G-8	既設セキュリティ対応ツール検証	すでにあるセキュリティ製品のバージョンアップ検証などを行う
G-9	新規セキュリティ対応ツール調査、開発	今後導入予定の新たなセキュリティ製品の資料作やトライアルなどを実施する
G-10	業務基盤運用	レポート生成や問合せ受付などの業務上必要なをシステム運用する

H	**内部統制・内部不正対応支援**	
	社内の内部統制や内部不正に関して、ネットワークやパソコン操作のログを提供、分析して、経費や法務を支援するお仕事	
H-1	内部統制監査データの収集と管理	内部監査などに必要なデータを集められるようにし、定期的にレポートする
H-2	内部不正対応の調査・分析支援	内部不正が発覚した際のログ情報の提供などを通し支援する
H-3	内部不正が検知・防止支援	内部不正が起こされないよう、検知や防止ができないか検討する

I	**外部組織との積極的連携**	
	社内社外問わず勉強会などへ参加したり、自ら催したり、セキュリティ仲間を増やすお仕事	
I-1	社員のセキュリティ対する意識啓発	実際のインシデント事例などをもとに社員へ意識啓発する
I-2	社内研修・勉強会の実施や支援	自分たちが得た知見を他の社員に対して広めていく
I-3	社内セキュリティアドバイザーとしての活動	開発部門などに対して、セキュリティの観点での助言や支援などを行う
I-4	セキュリティ人材の確保	人事と連携して人材の登用確保に、流出防止施策などを打つ
I-5	セキュリティベンダーとの連携	製品やサービスを提供するベンダーと良好な関係を築く
I-6	セキュリティ関連団体との連携	セキュリティ関連団体へ加盟し、情報共有、活用の幅を広げる

© 2018 ISOG-J

https://isog-j.org/output/2017/Textbook_soc-csirt_handbook_v1.0_appendix.pdf

ハンドブック読んだよ！
ではまずは自組織の状況を把握
してから組織づくりしなきゃね！！

やったぜ！

セキュリティ対応組織力

＝

それぞれの機能と役割が実行できているか

自組織の力を
どう把握するか？

セキュリティ対応組織
成熟度セルフチェックシート
ISOMM(ISOG-J SOC/CSIRT Maturity Model)

https://isog-j.org/output/2017/Textbook_soc-csirt_v2.1_maturity-checklist.xlsx

ISOMMの使い方

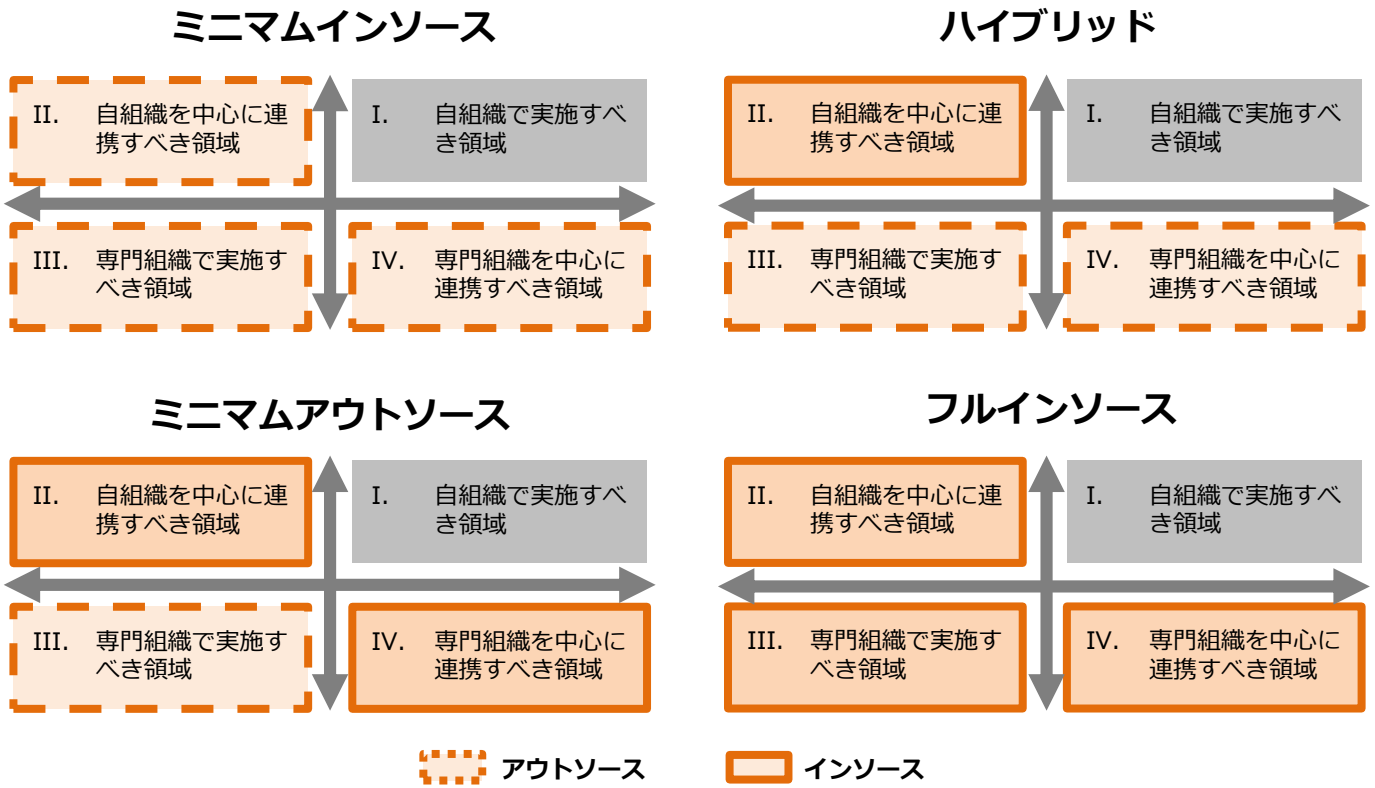
ISOMMの使い方概要

1.セキュリティの対応の全体を知る
2.自組織でどこを対応するか決める
3.自組織の現在のパターンを知る
4.今後どんなパターンになりたいかを決める
5.現在の範囲でどこまでできているかをする
6.チェック結果を見て、どこを強化するかを決める

セキュリティ対応組織パターンを自覚する（教科書を参考）

役割を専門性や組織の内外で
四象限に整理

セキュリティ対応組織パターンを自覚する（教科書を参考）



セキュリティ対応組織成熟度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。

ミニマムアウトソース

現在と将来的なモデルとするパターンを選択。

	記入日	201X/YY/ZZ		インソース						アウトソース						
				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	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	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	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	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	サービス内容は理解できているが、得られる結果は理解できない	サービス内容は理解できていないが、得られる結果は理解できている	サービス内容と得られる結果を理解できている	※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。
機能	役割		領域	0	1	2	3	4	5	0	1	2	3	4	5	備考
A セキュリティ対応組織運営	A-1.	全体方針管理	領域Ⅰ	◉	○	○	○	○	○	○	○	○	○	○	○	
	A-2.	トリアージ基準管理	領域Ⅱ	○	◉	○	○	○	○	○	○	○	○	○	○	
	A-3.	アクション方針管理	領域Ⅰ	○	○	◉	○	○	○	○	○	○	○	○	○	
	A-4.	品質管理	領域Ⅰ	○	○	○	○	○	○	○	◉	○	○	○	○	
	A-5.	セキュリティ対応効果測定	領域Ⅱ	○	○	○	○	○	○	○	○	◉	○	○	○	
	A-6.	リソース管理	領域Ⅰ	○	○	○	○	○	○	○	○	○	◉	○	○	
	B-1.	リアルタイム基本分析	領域Ⅱ	◉	○	○	○	○	○	○	○	○	○	○	○	

インソースとアウトソース、それぞれの観点において、6段階で評価。

スコアの付け方

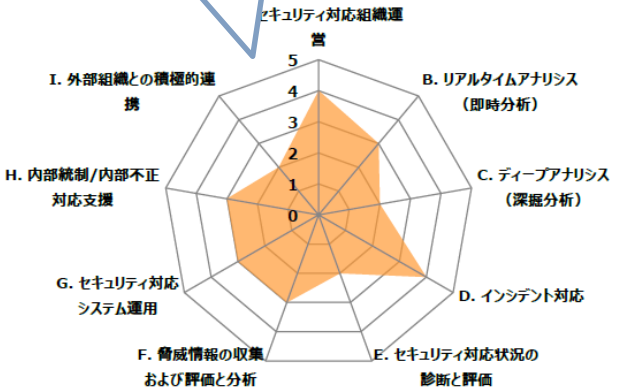
	インソース	アウトソース
0	インソースでの実装を検討したものの、結果として実施しないと判断した	アウトソースでの実装を検討したものの、結果として実施しないと判断した
1	実施できていない	結果や報告を確認できていない
2	運用が明文化されておらず、担当者が業務を実施できる	サービス内容と得られる結果を理解できていない
3	運用が明文化されておらず、担当者に代わりに他者が臨時で一部の業務を代行できる	サービス内容、得られる結果のいずれかが理解できていない
4	運用が明文化されており、担当者と交代して他者が業務を実施できる	サービス内容と得られる結果を理解できているが、想定未満
5	明文化された運用はCSIOなど権限ある組織長に承認されている	サービス内容と得られる結果を理解でき、想定通り

機能別レーダーチャート

レーダーチャートの数値一覧

あなたのセキュ　応組織における"**機能別**"成熟度

201X/YY/ZZ



現状の組織（ハイブリッドパター　能別成熟度を5段階で評価しています。
組織の「強み」と「弱み」を抽出　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　ます。
マクロな観点での指標とし　熟度向上の方針策定にお役立てください。

機能	成熟度
A. セキュリティ対応組織運営	**4** /5
B. リアルタイムアナリシス（即時分析）	**3** /5
C. ディープアナリシス（深掘分析）	**2** /5
D. インシデント対応	**4** /5
E. セキュリティ対応状況の診断と評価	**2** /5
F. 脅威情報の収集および評価と分析	**3** /5
G. セキュリティ対応システム運用	**3** /5
H. 内部統制/内部不正対応支援	**3** /5
I. 外部組織との積極的連携	**2** /5

現状のセキュリティ対応組織の**強み**

A. セキュリティ対応組織運営
セキュリティ対応全体の方針や、各種のルール、基準が定まっており、安定的な運用が実現できています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

D. インシデント対応
分析結果や脅威情報を元に、具体的な対応を行えており、システムやビジネスへの影響を低減できています。実務レベルにおいては問題のない状況と言えますが、より組織的な営みへと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

現状のセキュリティ対応組織の**弱み**

C. ディープアナリシス（深掘分析）
被害状況調査、攻撃手法分析など、深い分析が行い切れておらず、インシデントの全容解明と影響の特定が不十分になっています。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。

E. セキュリティ対応状況の診断と評価
脆弱性診断やインシデント対応訓練などの実施と評価が不十分であり、セキュリティ対応のレベルアップが図り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。

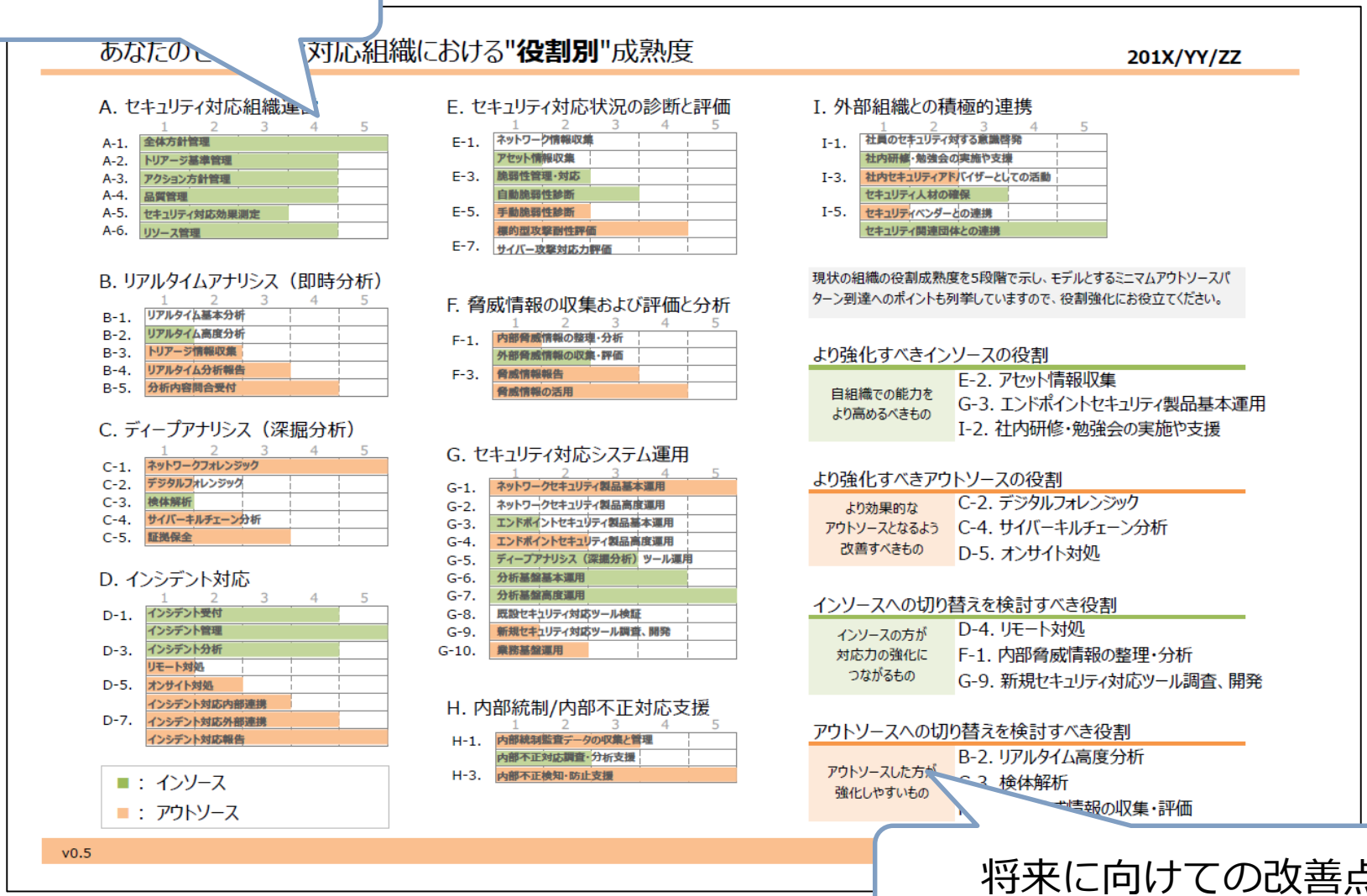
v0.5

© 2017 ISOG-J

現在の「強み」：成熟度高

現在の「弱み」：成熟度低

役割別成熟度グラフ



将来に向けての改善点

チェック時のFAQ

- 判断も何もせずに、「何もしていない」場合は1点
- 現状が把握できておらず、わからない場合も1点
- チェックする立場により評価が変わります。
  立場の違いによる認識の差を可視化できますので、
  気にせずチェックしましょう
- 最近できた組織では「わからない」や「できていない」
  のは当然です。ありのままをチェックして見ましょう

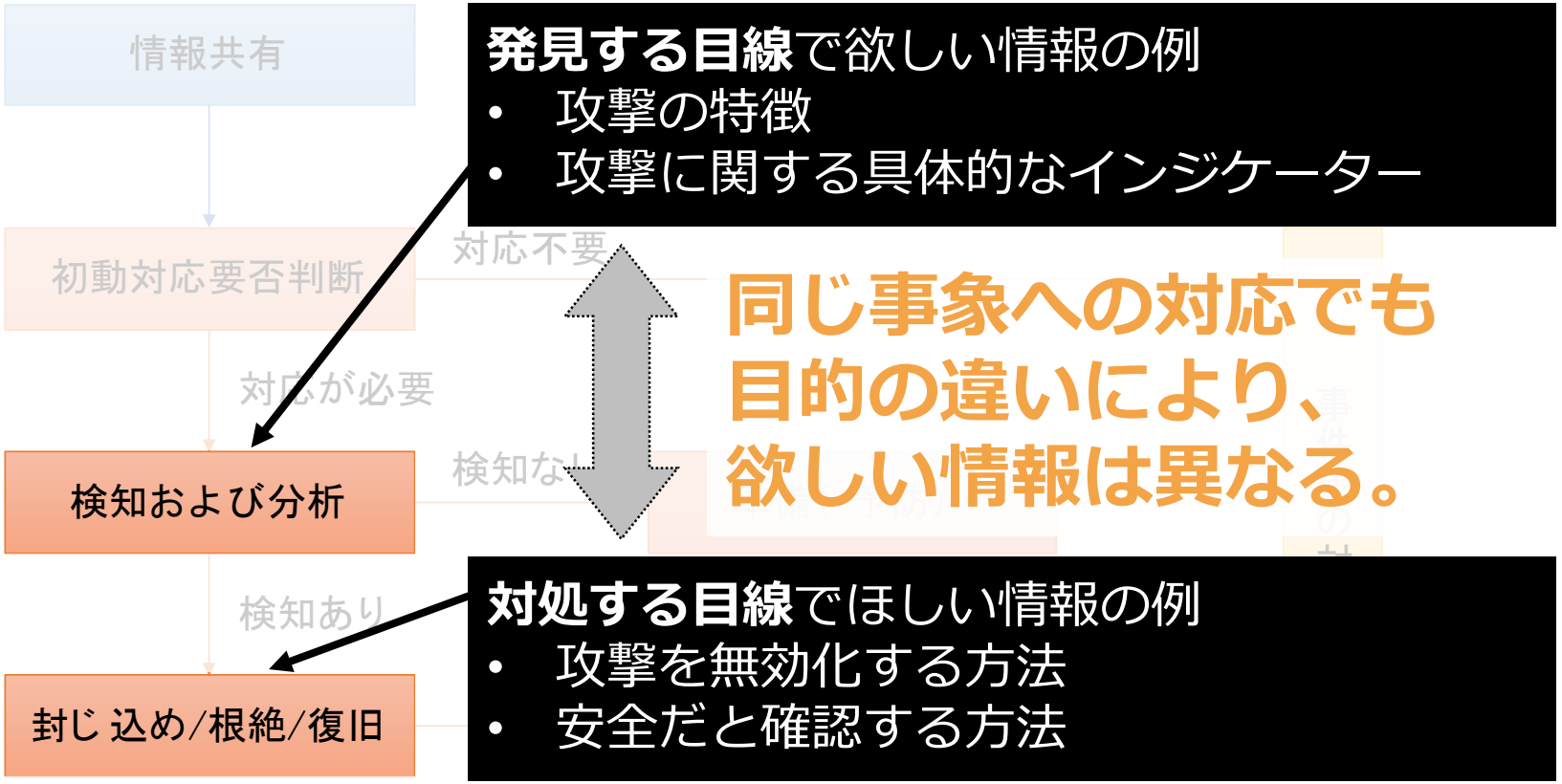
セキュリティ対応組織における、現状の把握と今後の方針策定にご活用ください。

セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」

情報共有を出発点としたセキュリティ対応をしっかり考えておく必要がある

参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」 』P4

情報共有を出発点としたセキュリティ対応



情報の受け渡しにおいてお互いに明確にすべき点

サイバーセキュリティ情報共有における 5W1H

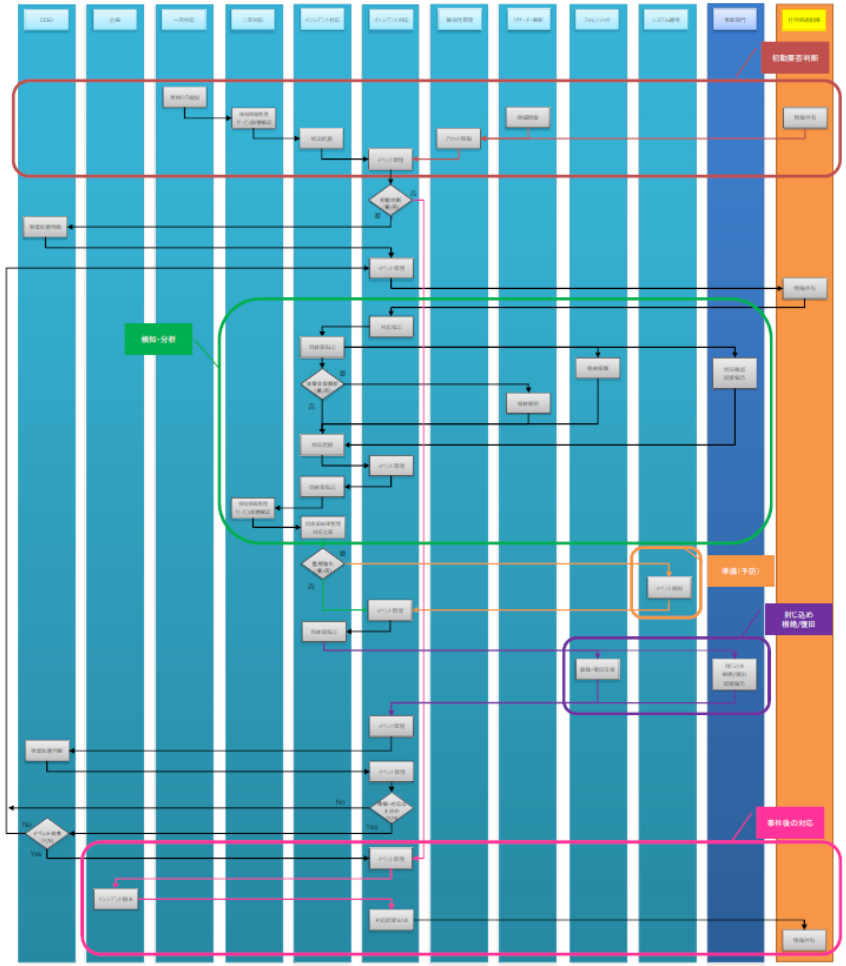
	発信側	受信側
Why	何を目的に	何を目的に
When	どのようなタイミングで	どのようなタイミングで
What	何の情報を	何の情報を
Where	どの情報共有の場において	どの情報共有の場から得て
Who	誰が	誰が
How	どのように	どのように
	発信するのか？	活用するのか？

参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」 』P2

5W1H 文書、英語版をリリースしました！

- リリース後、各所からの要望を受け…英語版を作成！
  - ISOG-J 初の英語文書リリース
- Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT
  - 英語では “6W” になるんですね…
  - 「セキュリティ対応組織」の部分はいい感じにならず… SOC/CSIRT としました
- 翻訳: Ryu Hiyoshi (NTT Security)

第2版のアップデート内容（予定）



対応の流れを理解しやすいよう、情報共有を発端としたセキュリティ対応のフローを作成。

脆弱性情報をキャッチした場合など、具体的な事例を用いた要点のまとめなども掲載予定。

インシデント対応に活躍する９つの機能（Who）

A．セキュリティ対応組織運営

D．インシデント対応

G．セキュリティ対応システム運用・開発

B．リアルタイムアナリシス

E．セキュリティ対応状況の（即時分析）

H．内部統制・内部不正診断と評価

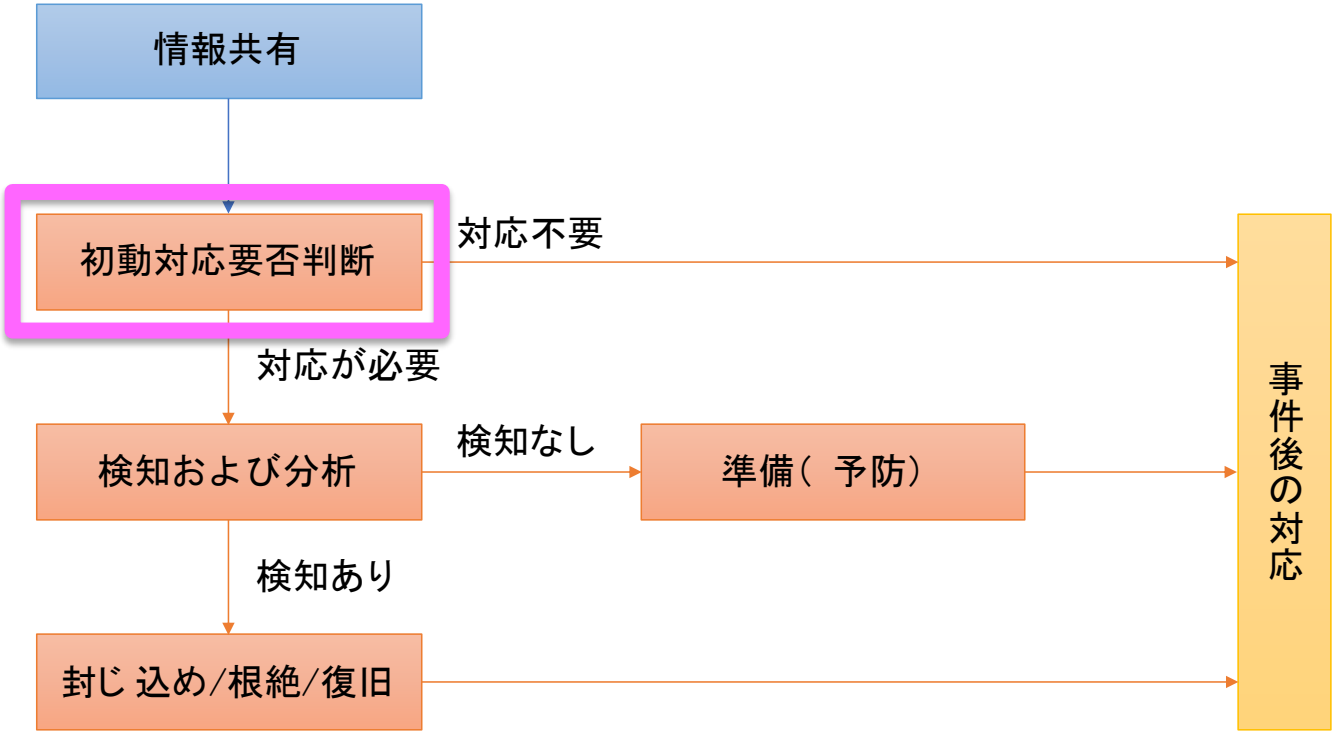
対応支援

C．ディープアナリシス

F．脅威情報の収集および（深堀分析）

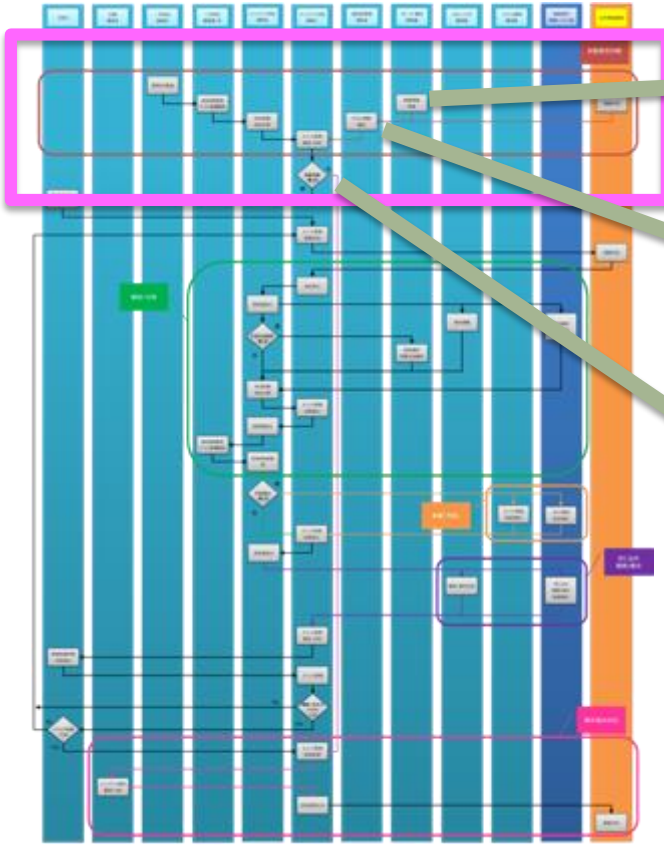
I．外部組織との積極的連携と分析と評価

共有情報を用いたセキュリティ対応の流れ（Why&When）



参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」 』P4

初動対応



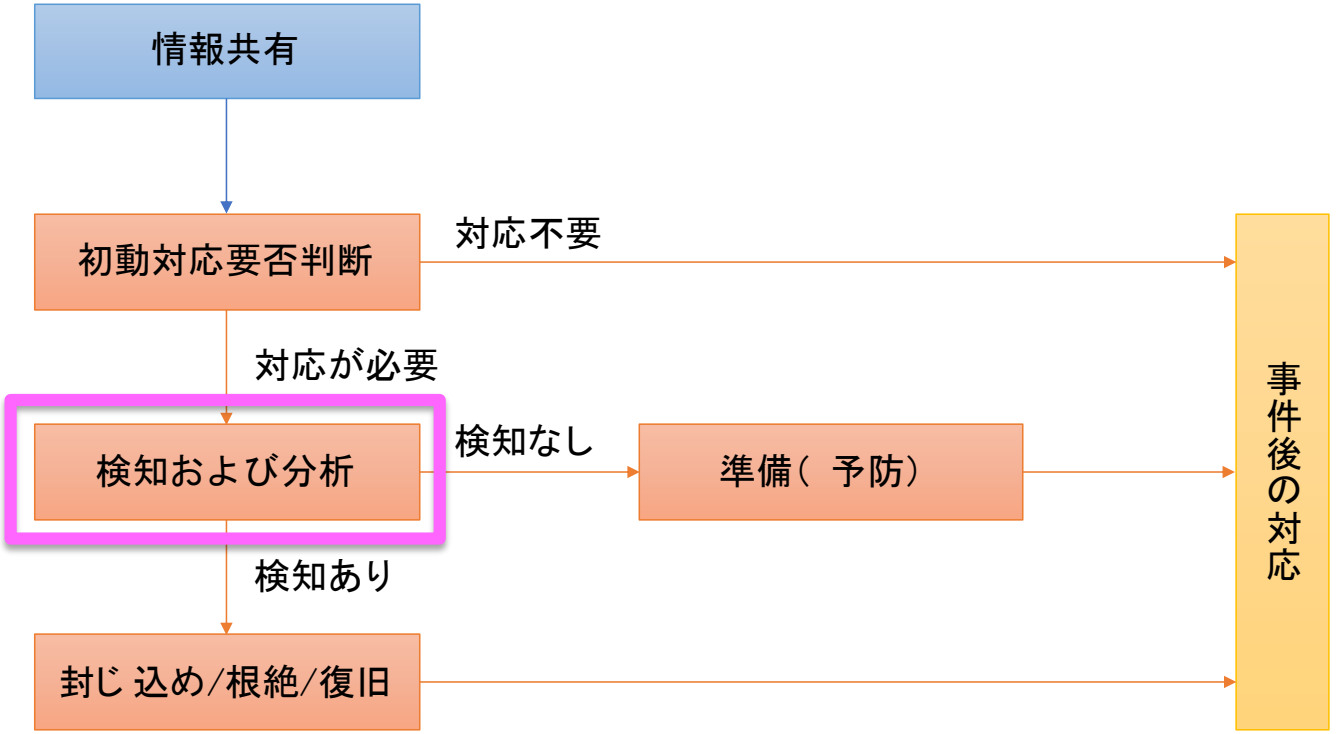
Who

F．脅威情報の収集および
分析と評価

E．セキュリティ対応状況の
診断と評価

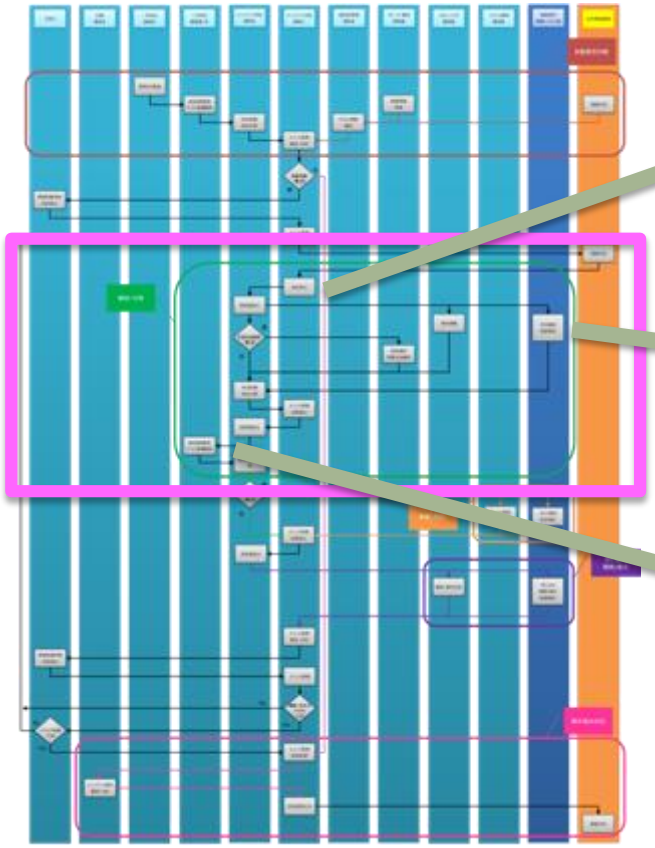
D．インシデント対応

共有情報を用いたセキュリティ対応の流れ（Why&When）



参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」 』P4

検知および分析



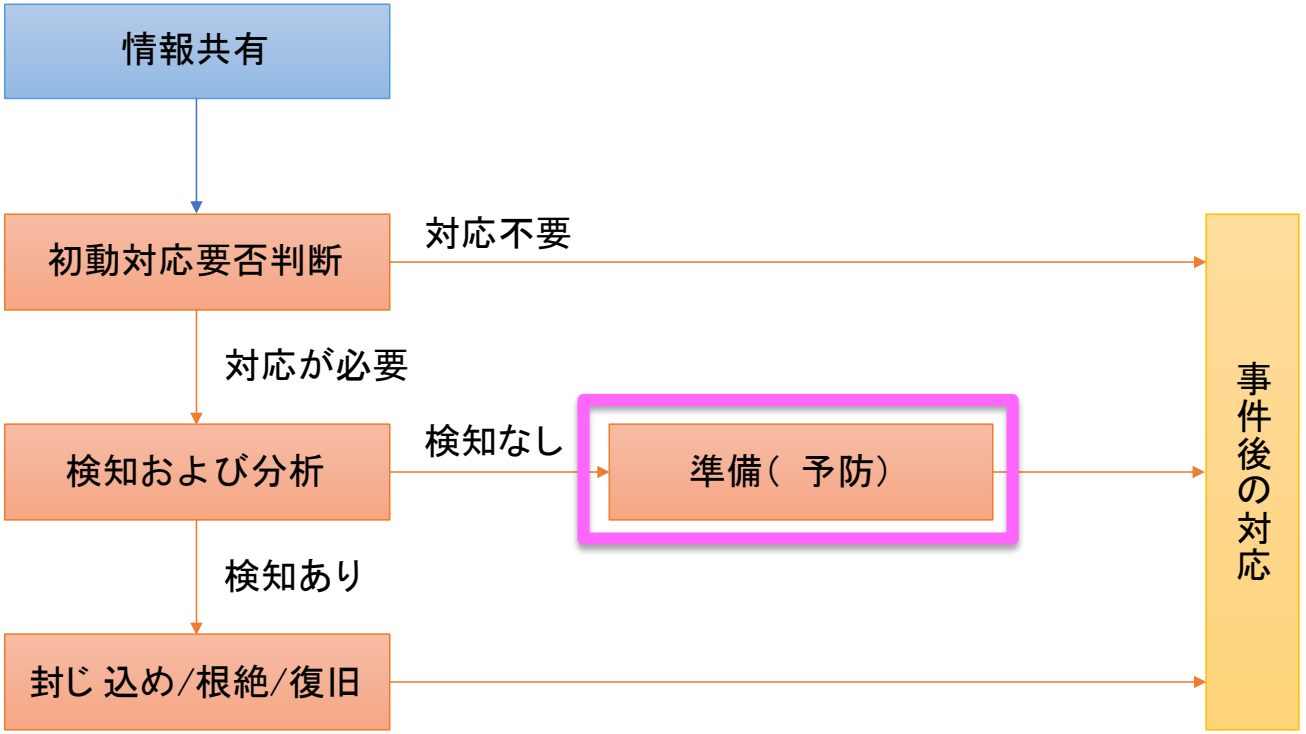
Who

D．インシデント対応

X．事業部門・システム運用部門

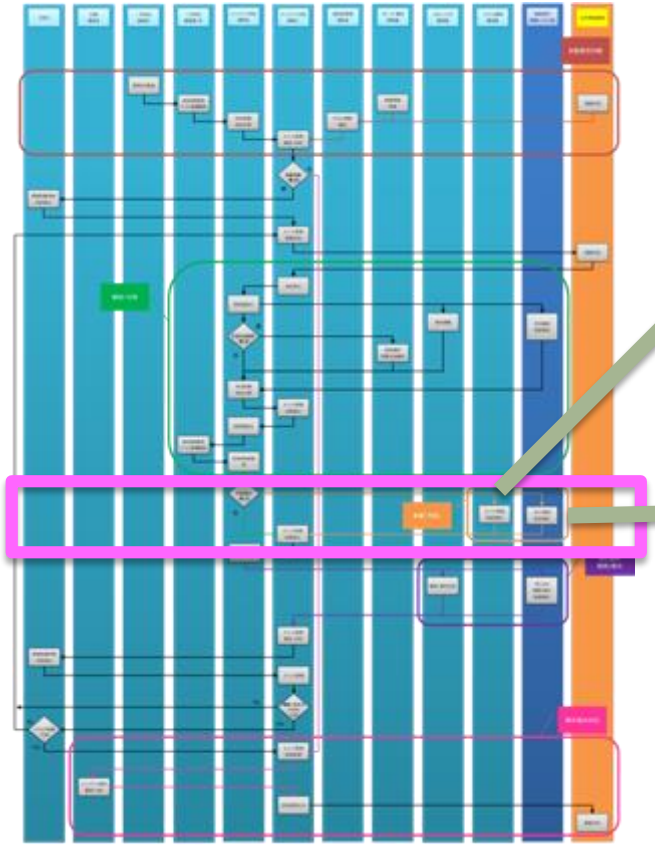
B．リアルタイムアナリシス
（即時分析）

共有情報を用いたセキュリティ対応の流れ（Why&When）



参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」 』P4

準備（予防）



Who

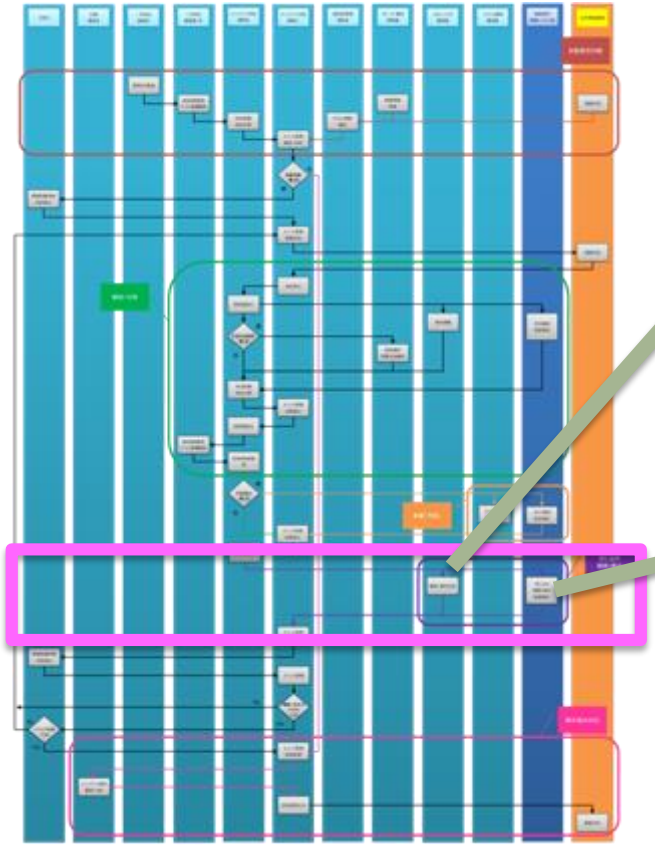
G．セキュリティ対応システム
運用・開発

X．事業部門・システム運用部門

共有情報を用いたセキュリティ対応の流れ（Why&When）

参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」 』P4

封じ込め/根絶/復旧



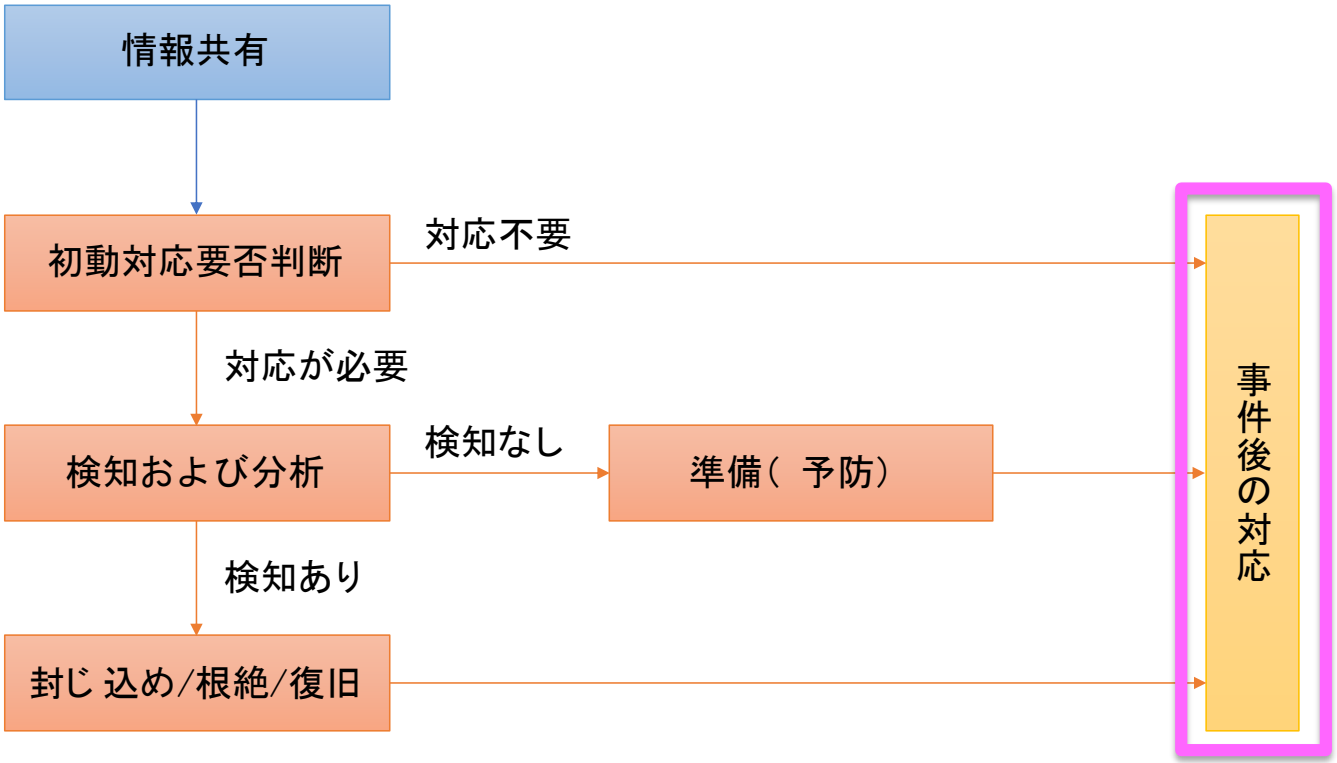
Who

C．ディープアナリシス

（深堀分析）

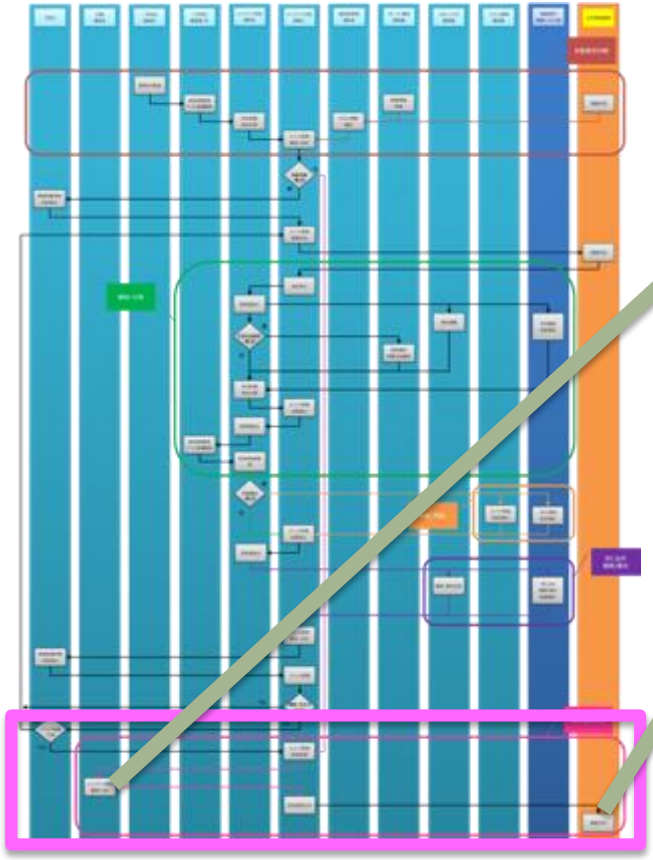
X． 事業部門・システム運用部門

共有情報を用いたセキュリティ対応の流れ（Why&When）



参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」 』P4

事件後の対応



Who

Ｆ．脅威情報の収集および分析と評価

Ｉ．外部組織との積極的連携

各種資料は
ISOG-J ホームページ
https://isog-j.org
よりダウンロード可能です。

https://isog-j.org/activities/result.html

（アイコン提供）
いらすとや　https://www.irasutoya.com/

- 本資料に関し、利用実態を把握するため、ご利用の際にはISOG-Jの窓口（info（at）isog-j.org）までご一報いただけますと幸いです。
- 本資料に関するご意見、ご要望などは下記よりご連絡ください。
  - https://jp.surveymonkey.com/r/W9HCMFP