

「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



セキュリティ対応

- 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. 分析結果問合せ受付

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に対する意識啓発
- 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）

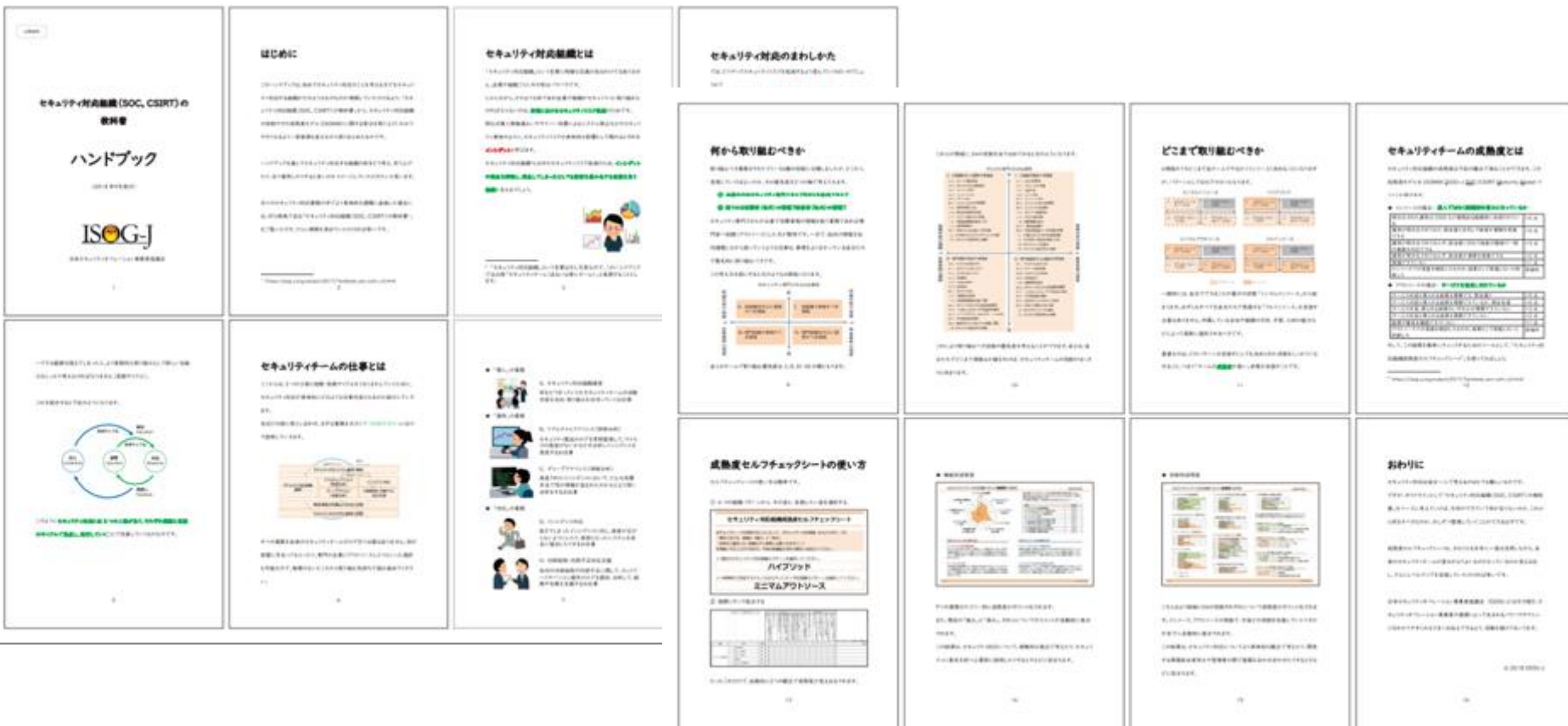


セキュリティ
対応組織の教科書
ハンドブック v1.0



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

	A セキュリティ対応組織運営 何れも欠けてはならない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	ドメイン管理 セキュリティ事故が起きたときの対応優先度を定める
A-3	ポリシー方針管理 セキュリティ事故が起きたときの対応方針を決める
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	セキュリティ対応策策定 全体としてのセキュリティ対策がとれているか評価をまとめ、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出力を常時監視して、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 基本分析で見えない場合、より多くのログやデータを一時的に分析する
B-3	ドメイン情報収集 対応優先度を決め、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仕掛けたことを報告し、対応を促す
B-5	分析結果報告書作成 報告した内容について問い合わせに対応する
	C ティーフアナリシス（深層分析） 発見されたインシデントにおいて、どんな攻撃手段で何が情報が高まったのかなど、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終わらなかつた詳細な分析を行う
C-2	デジタルフォレンジック 捜査に連なると検定可能なものを確保する
C-3	検体解析 ファイルなどのような動きをするものごとを解析する
C-4	攻撃手法解析 これまでの分析結果全てをまとめ、攻撃の経路や手法を明らかにする
C-5	結果策定 資料など法的対応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 即時分析で見つけたら、外部からの依頼で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を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応していくべきかを判断する
D-4	IR-IT対応 監視センターからメールで対応、確認する
D-5	ホスティング対応 現場に駆けつけ対応、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）との連絡、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（警察、取引企業）などとの説明、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、対応内容について報告する
	E セキュリティ対応状況の診断と評価 定期的な診断やメール調べる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 与るネットワークの構成を把握する
E-2	アセット情報収集 与るシステム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、リスクシステムを把握、対応する
E-4	自動脆弱性診断 脆弱な診断として、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	脆弱性診断報告書作成 脆弱性診断結果により脆弱な攻撃へに脆弱性が指摘される
E-7	サイバー攻撃対応の評価 サイバー攻撃対応訓練を行い、きちんと対応できるか確認する

ISOG-J 日本セキュリティオペレーション事業者協会

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

	F 脅威情報の収集および分析と評価 ネットワーク上のセキュリティニュースやドメインチームで見つけたインシデントを監視し、対応を促すお仕事
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、中長期的な改善策を整理する
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や脆弱性を収集し、未対応の脅威がないか確認する
F-3	脅威情報報告 社内外部の脅威情報や定期的なレポートの報告する
F-4	脅威情報の活用 脅威情報を関係者へ提供し、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運用したり、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積極的に活用する
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積極的に活用する
G-5	ティーフアナリシス深層分析ツール運用 フォレンジックやデジタルフォレンジックのツールを管理、運用する
G-6	分析結果基本運用 SI/MDMなどのツールで分析した結果を管理、運用する
G-7	分析結果高度運用 SI/MDMなどのツールで分析した結果を、より深い情報を引き出す
G-8	脆弱性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やトライアルなどを実施する
G-10	業務継続性確保 レポート生成や報告が受け付けられるような必要なシステム運用する
	H 内部統制・内部不正対応支援 社内で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、調査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 内部監査において必要なデータを集めるためのツール、定期的なレポートする
H-2	内部不正対応の調査・分析支援 内部不正が発覚した場合のログ情報の提供やツールを渡し、支援する
H-3	内部不正検知・防止支援 内部不正が検知されないよう、検知や防止ができるように検知する
	I 外部組織との連携的連携 社内社外問わず勉強会などへ参加したり、会を催したり、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に対する意識啓蒙 業種のインシデント事例などを元に社員へ意識啓蒙する
I-2	社内研修・勉強会の実施や支援 自分たちが習得した内容を他社へ共有し、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 関係部門などに対して、セキュリティの観点での相談や支援などを行う
I-4	セキュリティ人材の確保 人事と連携して、人材の確保や育成、流出防止施策などを行う
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の連携 セキュリティ関連団体へ参加し、情報共有、連携の輪を広げる

© 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！！



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)

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）の現状における、組織の「強み」と「弱み」を将来的に達成したい組織モデル表現に必要な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。

ミニмумインソース

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。

ハイブリッド

セキュリティ対応組織のパターン



※ 詳細は資料書 第6章をご参照ください。

機能	項目	評価	インソース					アウトソース					備考	
			1	2	3	4	5	1	2	3	4	5		
A. セキュリティ対応組織運営	※1. 基本方針策定	現状	●	○	○	○	○	○	○	○	○	○	○	
	※2. SOPの策定	現状	●	○	○	○	○	○	○	○	○	○	○	
	※3. 方針の策定	現状	●	○	○	○	○	○	○	○	○	○	○	
	※4. 役割													
	※5. セキュリティ対応組織の責任													
	※6. SOPの策定													
	※7. セキュリティ対応組織の責任													
	※8. SOPの策定													
	※9. セキュリティ対応組織の責任													
	※10. SOPの策定													
B. リアルタイムアナリシス (即時分析)	※11. 脅威情報の収集													
	※12. 脅威情報の収集および評価と分析													
	※13. 脅威情報の収集および評価と分析													
	※14. 脅威情報の収集および評価と分析													
	※15. 脅威情報の収集および評価と分析													
	※16. 脅威情報の収集および評価と分析													
	※17. 脅威情報の収集および評価と分析													
	※18. 脅威情報の収集および評価と分析													
	※19. 脅威情報の収集および評価と分析													
	※20. 脅威情報の収集および評価と分析													

あなたのセキュリティ対応組織における“機能別”成熟度

201X/YY/ZZ



現状の組織（ミニмумインソースパターン）における機能別成熟度を右図で評価しています。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出しています。マクロな観点での組織として、成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	3.0 / 5
B. リアルタイムアナリシス (即時分析)	4.0 / 5
C. ディープアナリシス (深層分析)	4.0 / 5
D. インシデント対応	4.0 / 5
E. セキュリティ対応状況の把握と評価	3.0 / 5
F. 脅威情報の収集および評価と分析	3.0 / 5
G. セキュリティ対応システム運用	3.9 / 5
H. 内部統制/内部不正対応支援	3.0 / 5
I. 外部組織との積極的連携	4.0 / 5

現状のセキュリティ対応組織の強み

B. リアルタイムアナリシス (即時分析)
各種システムで収集される情報をもとに、即時性の高い分析が行われ、迅速で適切なインシデント対応に繋がっています。実務レベルにおいては問題のない状況と見えますが、より組織的な取り組みと昇華できるよう、関係組織を巻き込んだ取り組みを行ってください。

C. ディープアナリシス (深層分析)
被害状況調査、攻撃手法分析など、深い分析が行われ、インシデントの全容解明と影響の特定に繋がっています。実務レベルにおいては問題のない状況と見えますが、より組織的な取り組みと昇華できるよう、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

H. 内部統制/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負担が大きくなっています。組織的に機能していない部分がありますので、業務の範囲、改善が必要となります。

F. 脅威情報の収集および評価と分析
組織内外の脅威情報収集、活用が満足に行えておらず、各種分析、インシデント対応など、他の機能の改善につなげられていません。組織的に機能していない部分がありますので、業務の範囲、改善が必要となります。

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

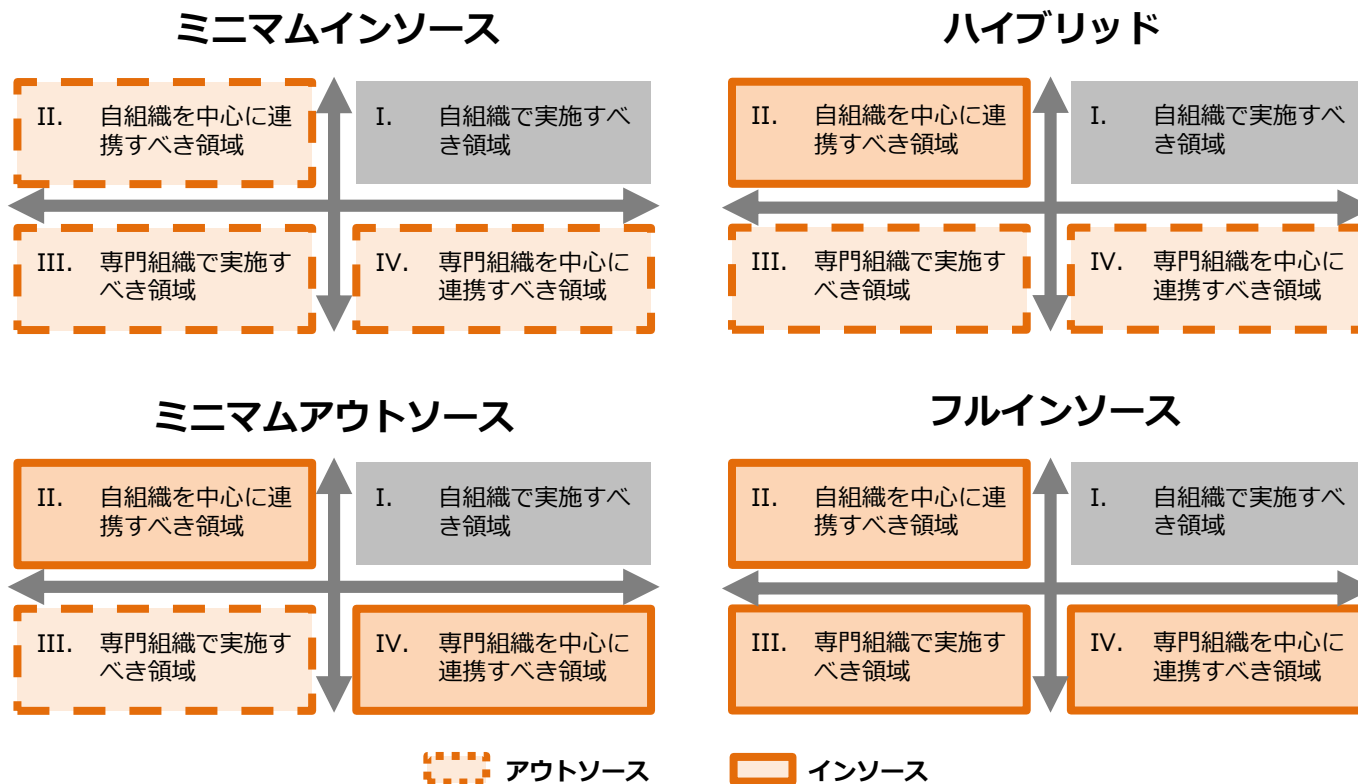
1. セキュリティの対応の全体を知る
2. 自組織でどこを対応するか決める
3. 自組織の現在のパターンを知る
4. 今後どんなパターンになりたいかを決める
5. 現在の範囲でどこまでできているかをする
6. チェック結果を見て、どこを強化するかを決める

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）



将来的には
ミニマムアウトソース
を目指すぞ！！



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なポイント

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。



機能	役割	領域	インソース						アウトソース					備考		
			0	1	2	3	4	5	0	1	2	3	4		5	
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 リアソン/基本分析	領域II	○	○	○	○	○	○	○	○	○	○	○	○	○		

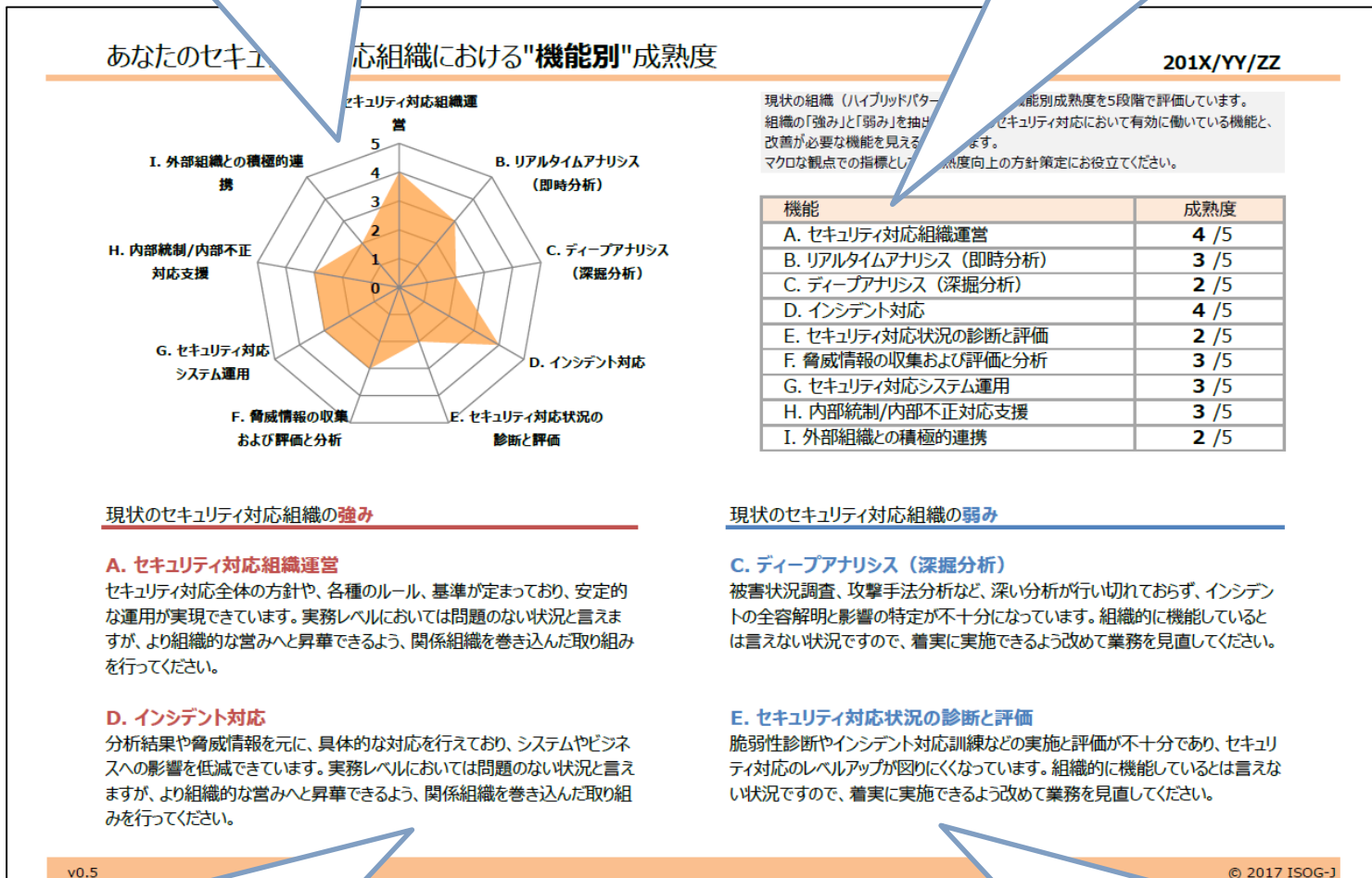
インソースとアウトソース、それぞれの観点において、6段階で評価。

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



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

あなたのセキュリティ対応組織における"役割別"成熟度

201X/YY/ZZ

A. セキュリティ対応組織運営

	1	2	3	4	5
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）

	1	2	3	4	5
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. 分析内容問合せ受付	■	■	■	■	■

C. ディープアナリシス（深掘分析）

	1	2	3	4	5
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. サイバーキルチェーン分析	■	■	■	■	■
C-5. 証拠保全	■	■	■	■	■

D. インシデント対応

	1	2	3	4	5
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. リモート対応	■	■	■	■	■
D-5. オンサイト対応	■	■	■	■	■
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	■	■	■	■	■

■ : インソース
■ : アウトソース

E. セキュリティ対応状況の診断と評価

	1	2	3	4	5
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. 標的型攻撃脆弱性評価	■	■	■	■	■
E-7. サイバー攻撃対応力評価	■	■	■	■	■

F. 脅威情報の収集および評価と分析

	1	2	3	4	5
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

	1	2	3	4	5
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

	1	2	3	4	5
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

	1	2	3	4	5
I-1. 社員のセキュリティに対する意識啓発	■	■	■	■	■
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	■	■	■	■	■

現状の組織の役割成熟度を5段階で示し、モデルとするミニマムアウト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、役割強化にお役立てください。

より強化すべきインソースの役割

自組織での能力をより高めるべきもの

- E-2. アセット情報収集
- G-3. エンドポイントセキュリティ製品基本運用
- I-2. 社内研修・勉強会の実施や支援

より強化すべきアウトソースの役割

より効果的なアウトソースとなるよう改善すべきもの

- C-2. デジタルフォレンジック
- C-4. サイバーキルチェーン分析
- D-5. オンサイト対応

インソースへの切り替えを検討すべき役割

インソースの方が対応力の強化につながるもの

- D-4. リモート対応
- F-1. 内部脅威情報の整理・分析
- G-9. 新規セキュリティ対応ツール調査・開発

アウトソースへの切り替えを検討すべき役割

アウトソースした方が強化しやすいもの

- B-2. リアルタイム高度分析
- C-3. 検体解析
- F-2. 外部脅威情報の収集・評価

v0.5

将来に向けての改善点

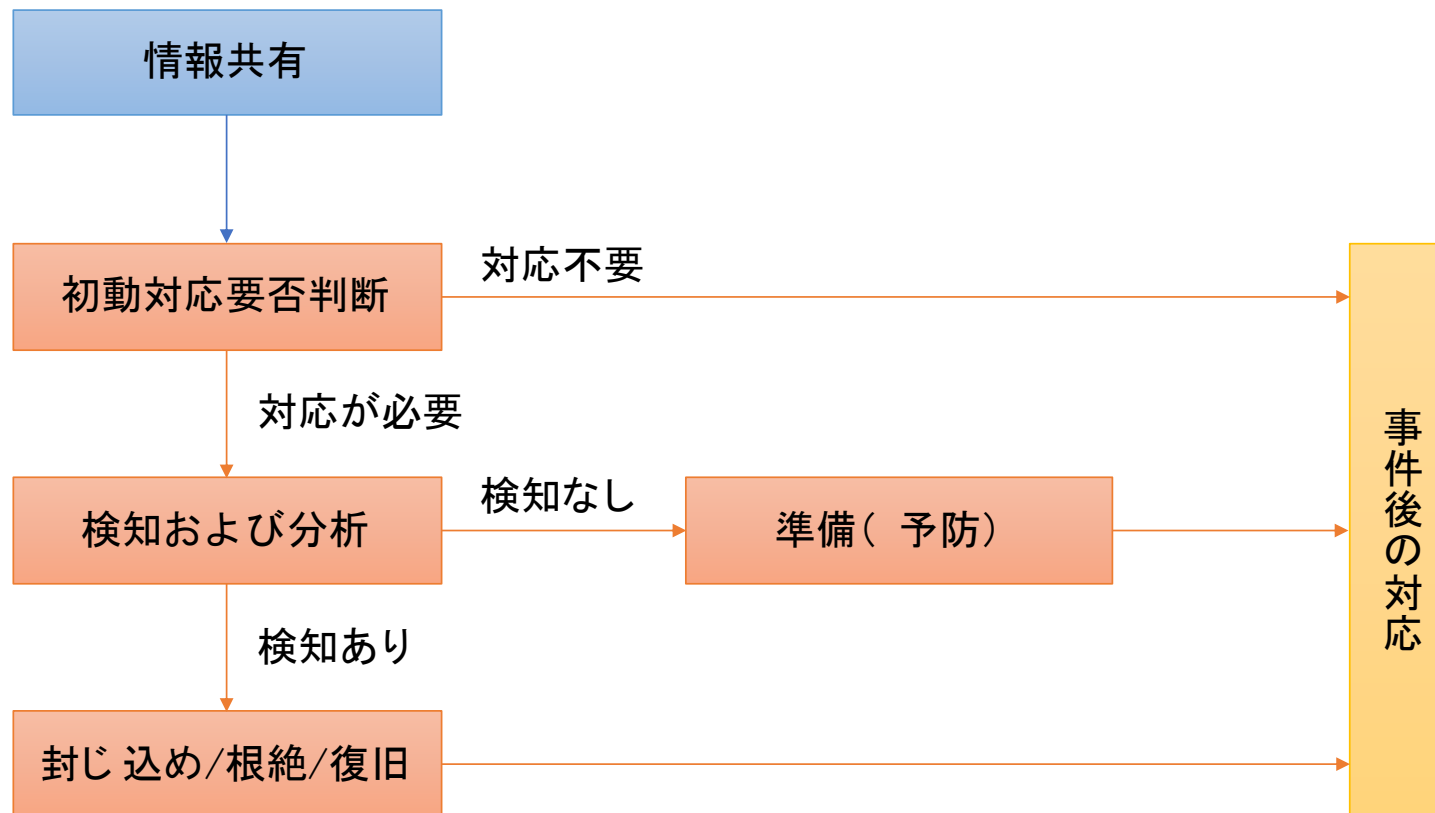
チェック時のFAQ

- 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。**

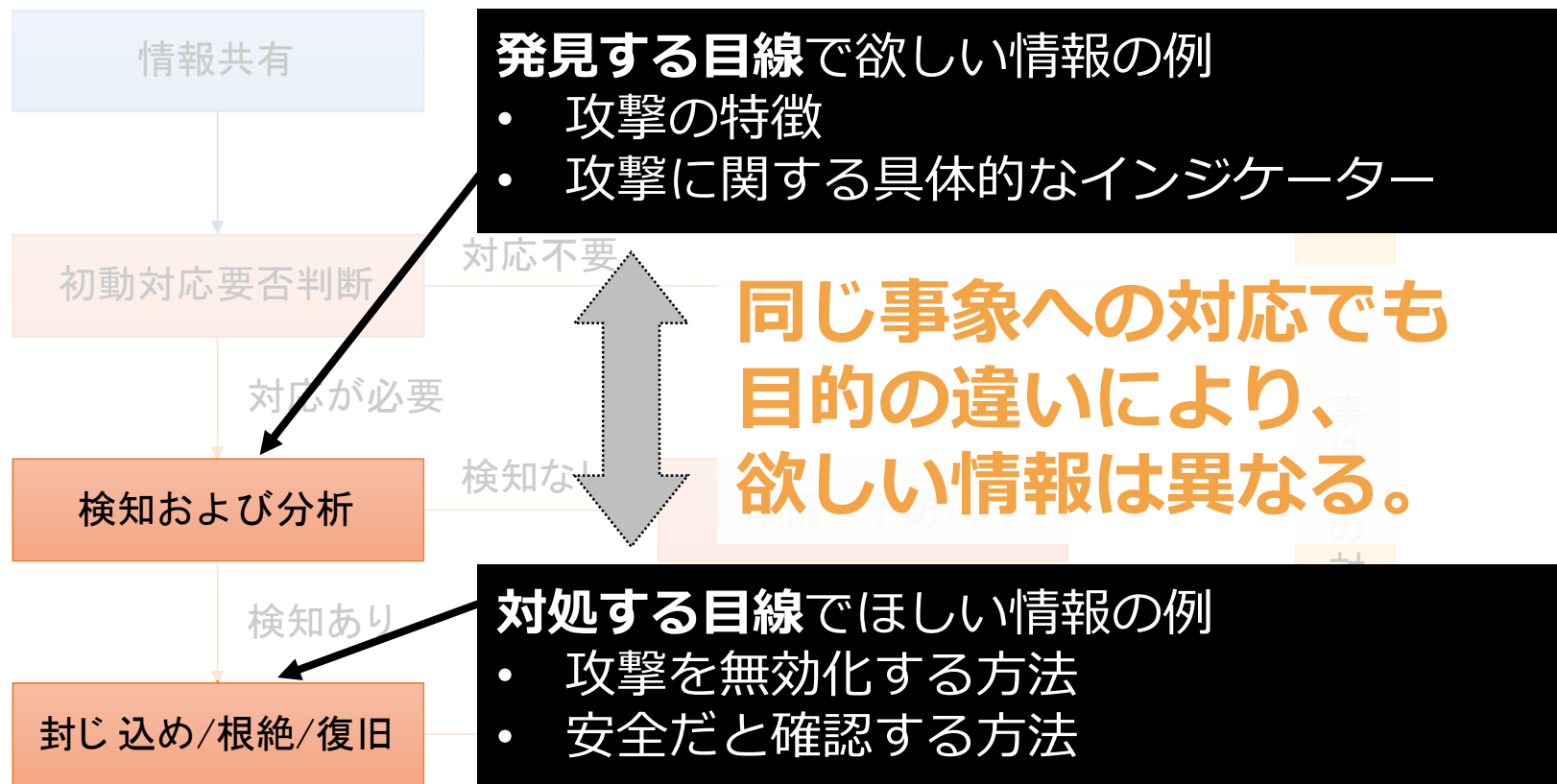
セキュリティ対応組織 (SOC,CSIRT)強化に向けた サイバーセキュリティ情報共有の 「5W1H」

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？

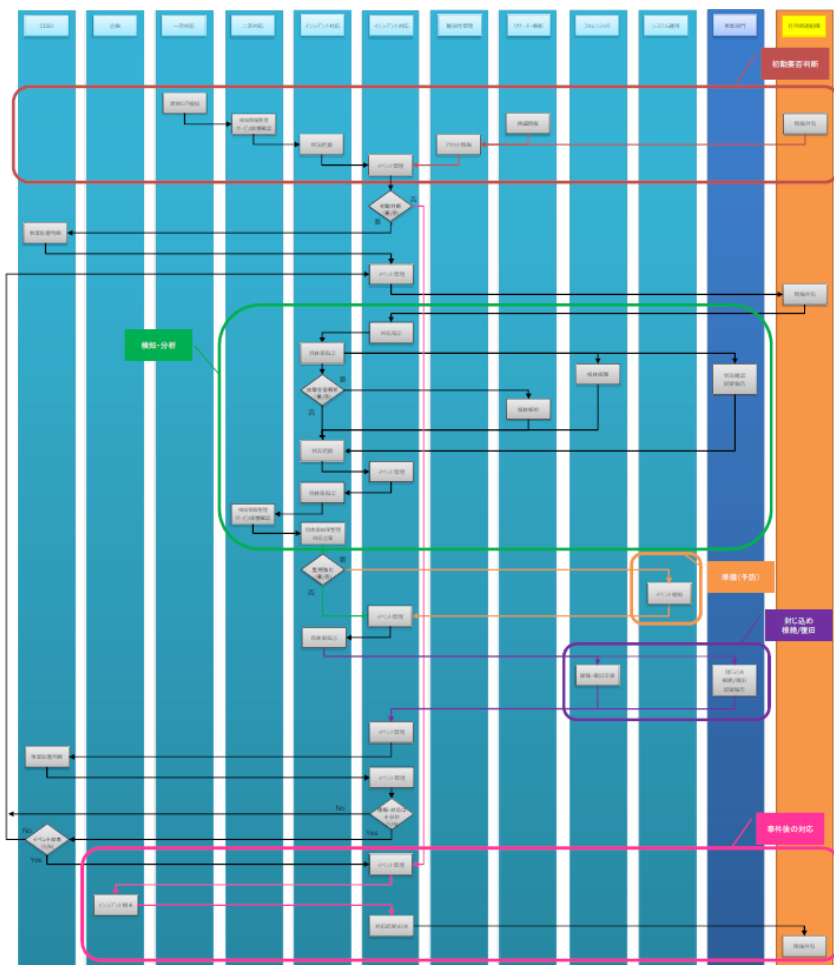
参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P2

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)

The screenshot shows the ISOG-J website interface. At the top, there is a navigation bar with '日本語' and 'English' tabs. The main header features the ISOG-J logo and the text 'Information Security Operation providers Group Japan'. Below the header, there is a navigation menu with 'About us', 'Membership Organizations', 'Activities', and 'Contact'. The main content area is titled 'HOME > Activities > publications'. Under the 'Activities' tab, there is a 'Publications' section. The featured publication is 'Six Ws on cybersecurity information sharing for enhancing SOC/CSIRT', Version 1.0 (October 2017, English edition released February 2018). The text of the publication is displayed, discussing the necessity of information sharing across organizations and the challenges faced. A link to the PDF version is provided, along with a 'Send feedback (SurveyMonkey)' button. At the bottom, there is a link to the Japanese edition. On the right side, there is a sidebar with 'Activities' and '関連リンク' (Related Links) section, which includes logos for JNSA, JPCERT/CC, IPA, IA Japan, and WASForum.jp.

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



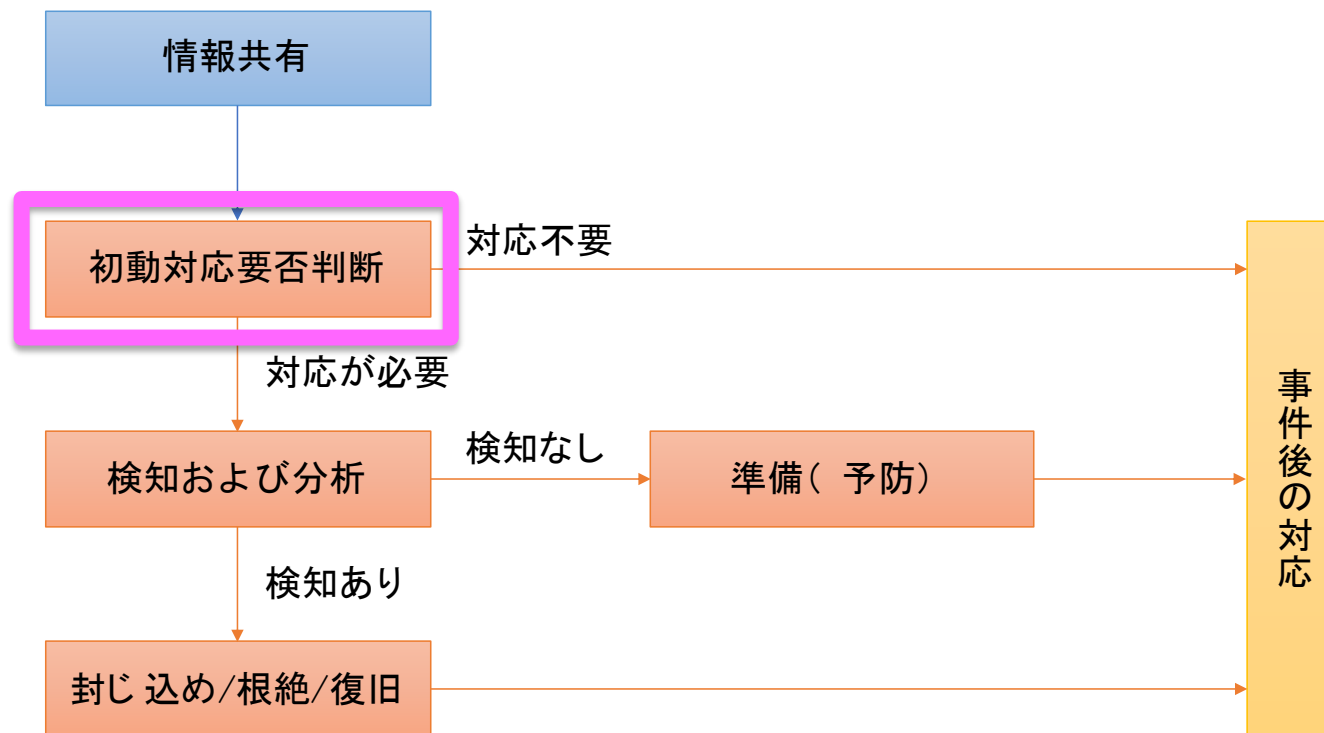
B. リアルタイムアナリシス E. セキュリティ対応状況の診断と評価 H. 内部統制・内部不正対応支援
(即時分析)



C. ディープアナリシス 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
(深堀分析)

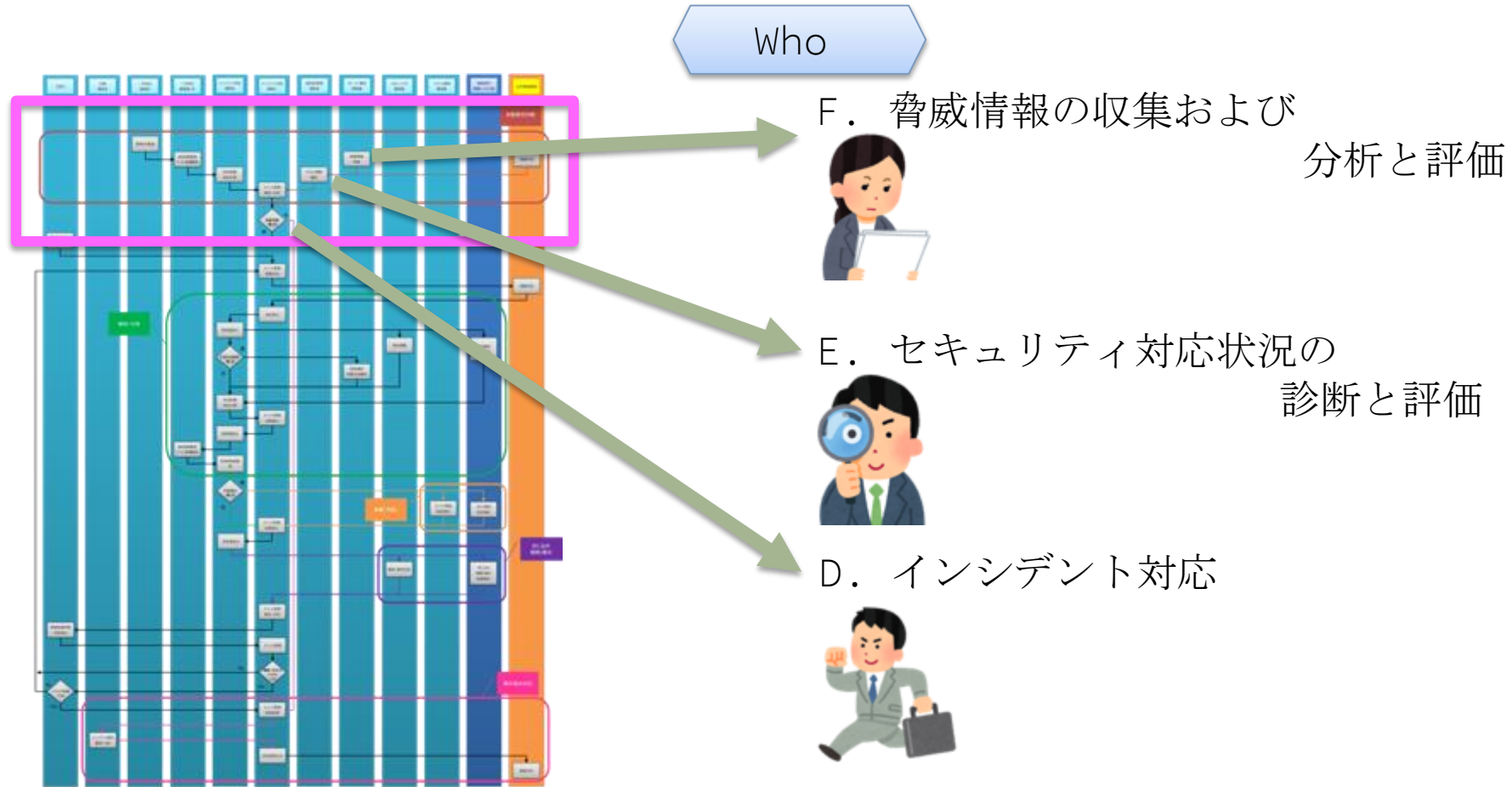


共有情報を用いたセキュリティ対応の流れ（Why&When）

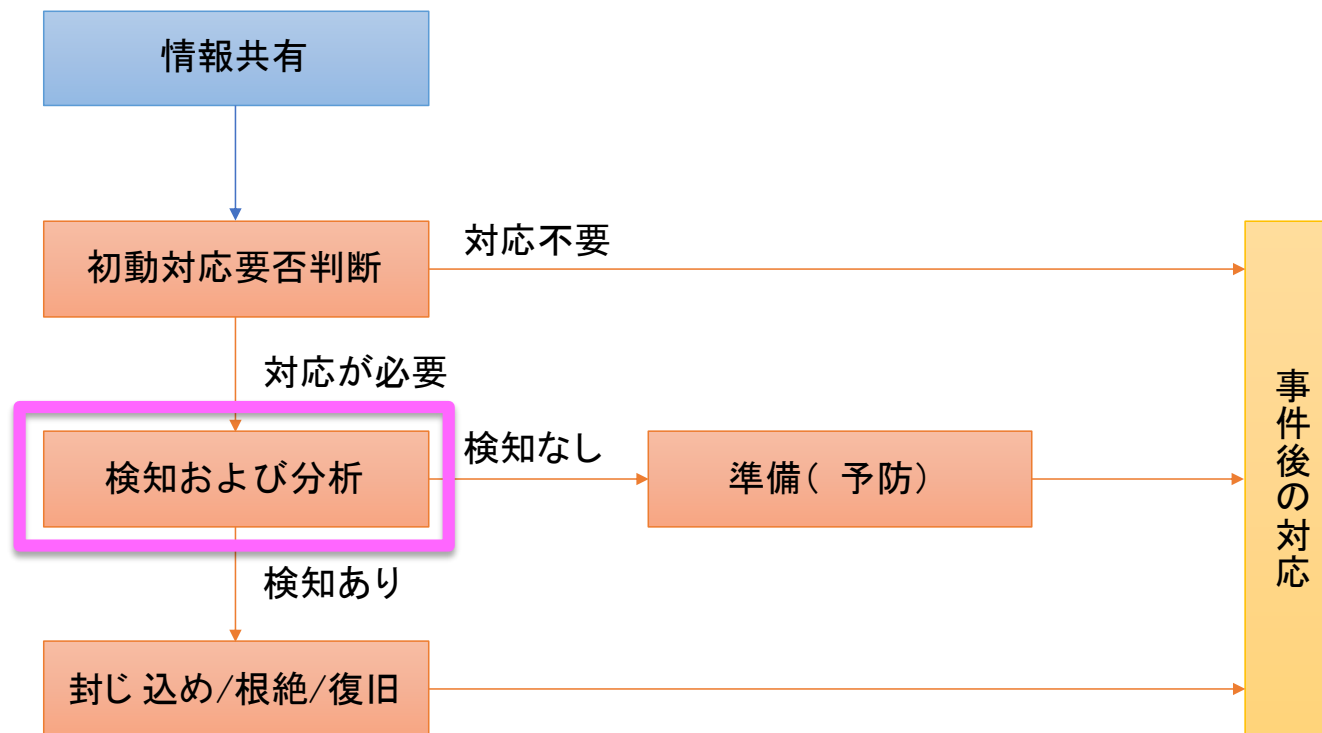


参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P4

初動対応



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

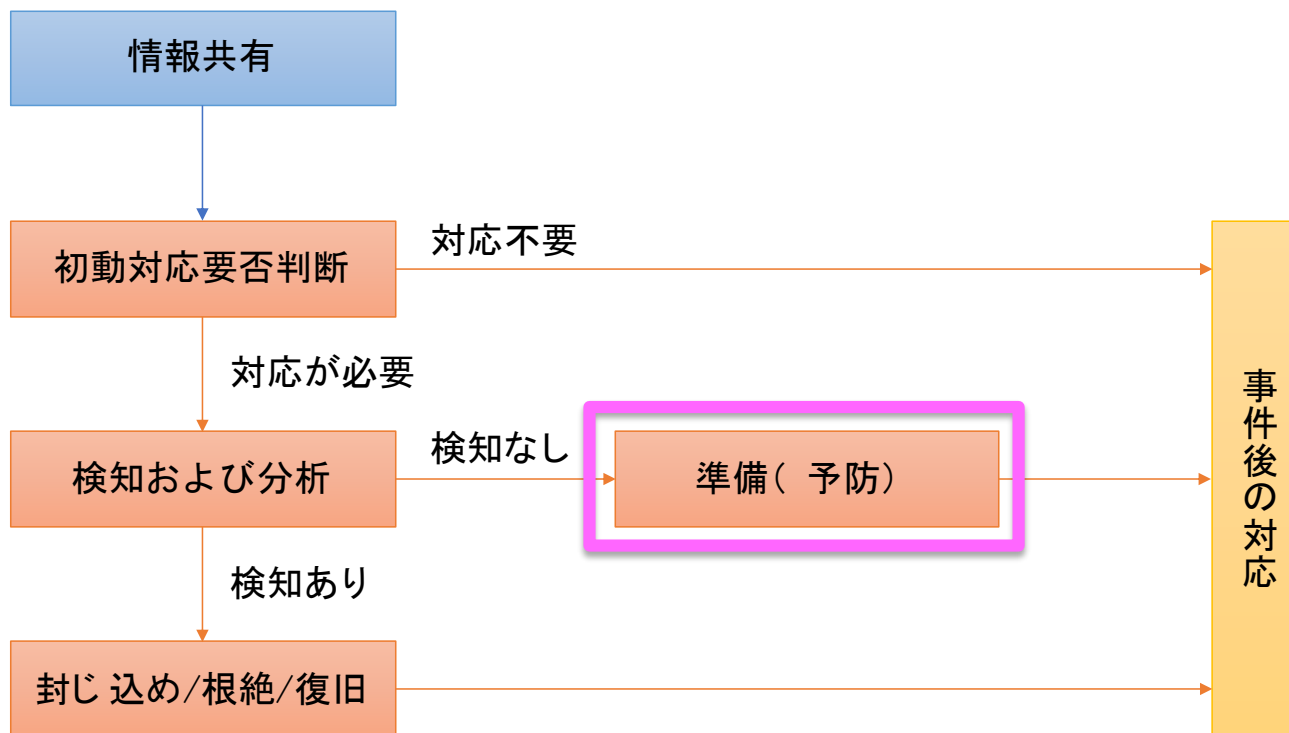


B. リアルタイムアナリシス

(即時分析)

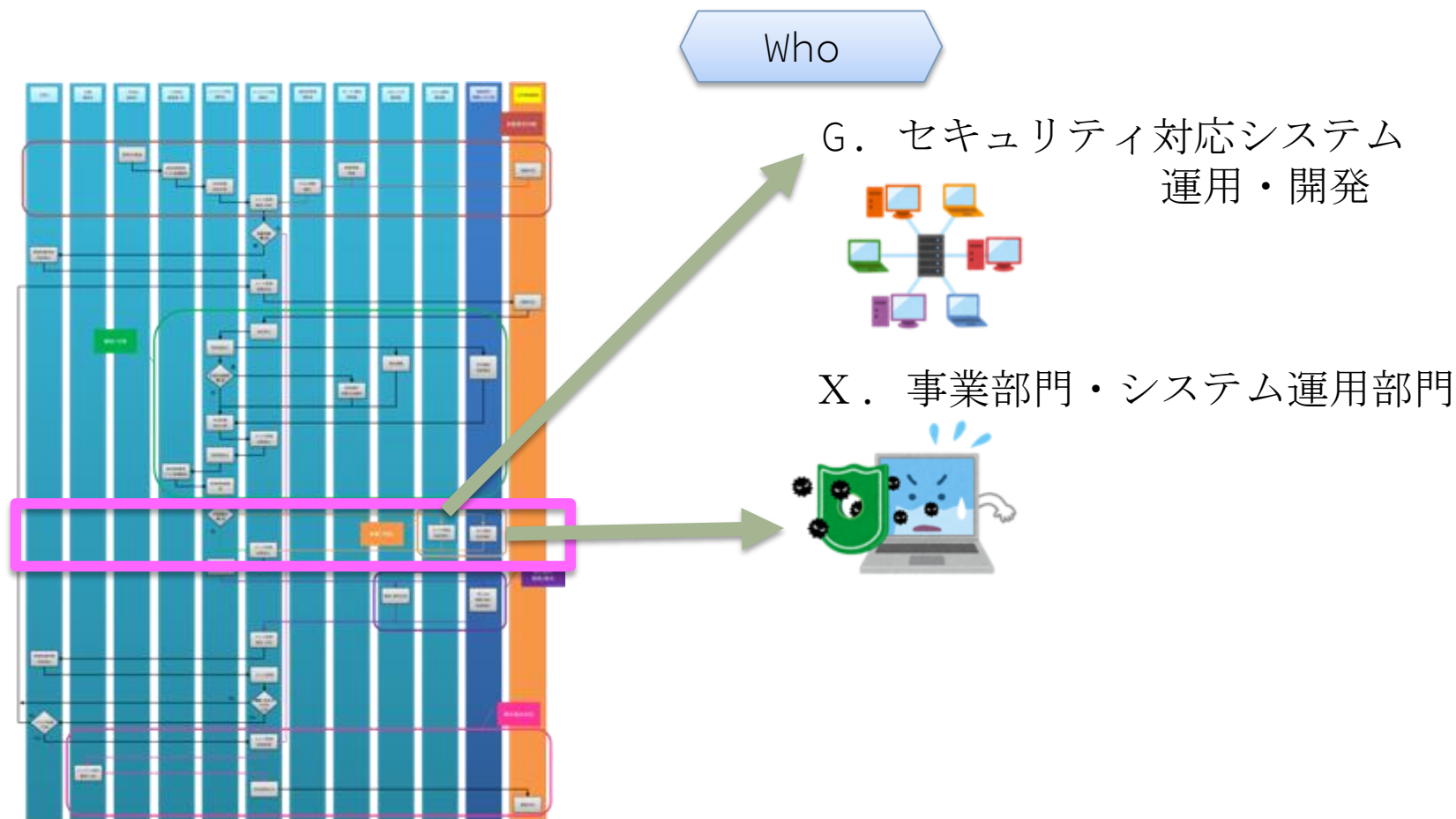


共有情報を用いたセキュリティ対応の流れ（Why&When）

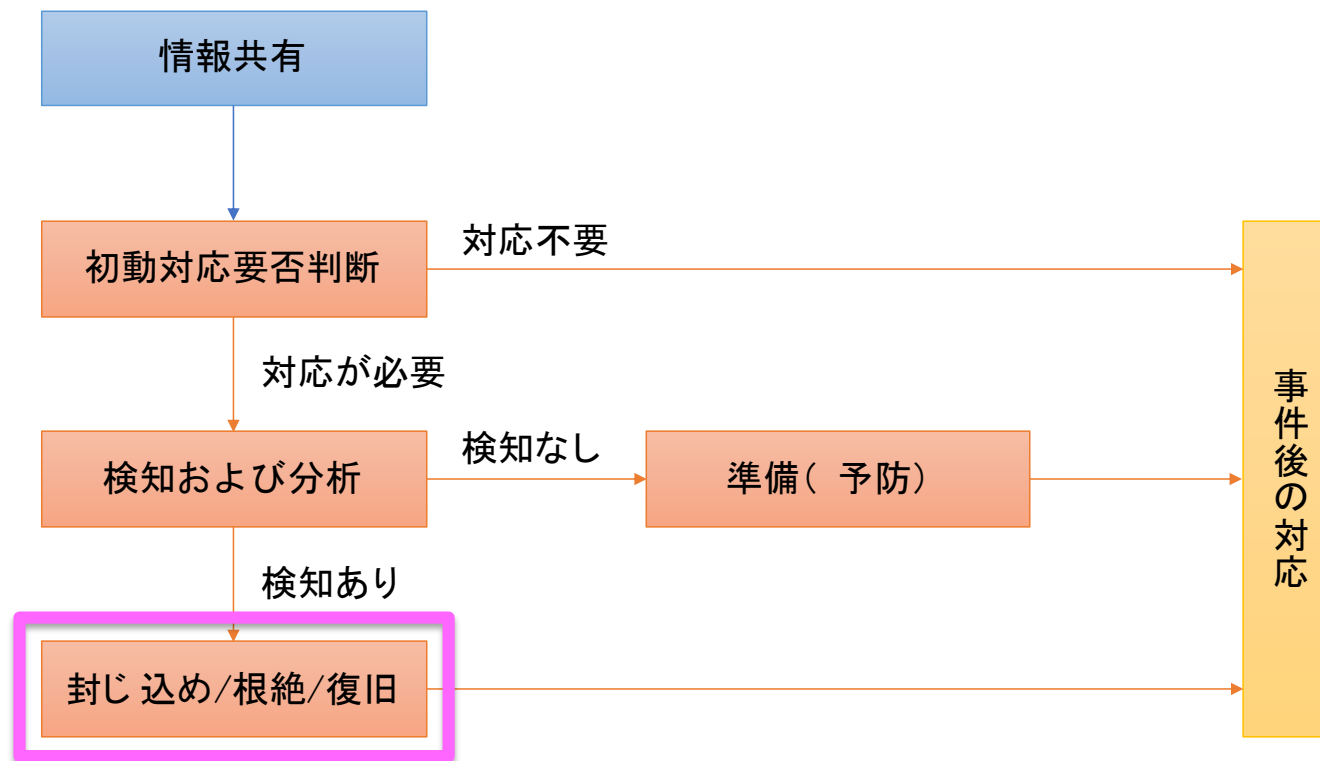


参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P4

準備（予防）

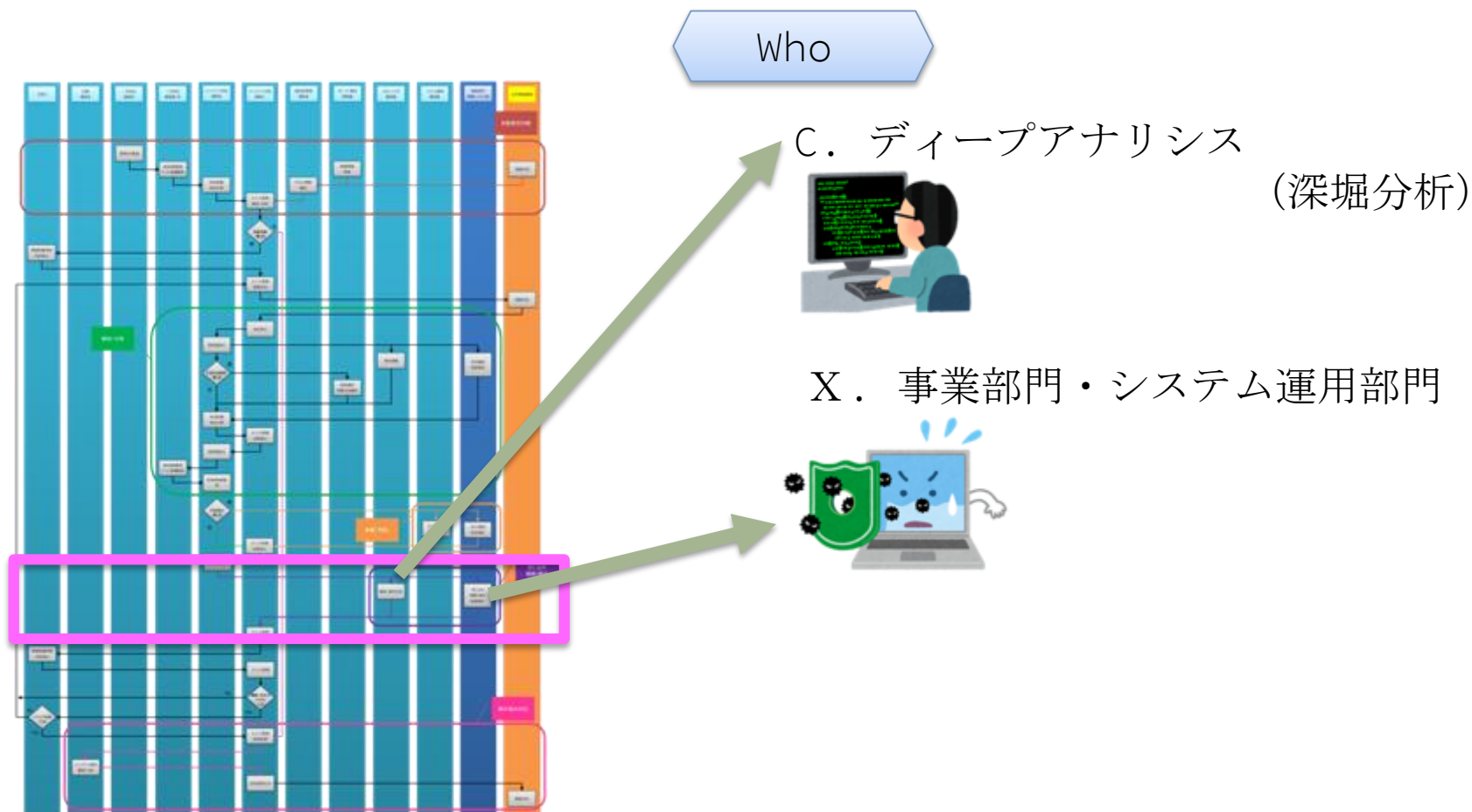


共有情報を用いたセキュリティ対応の流れ（Why&When）

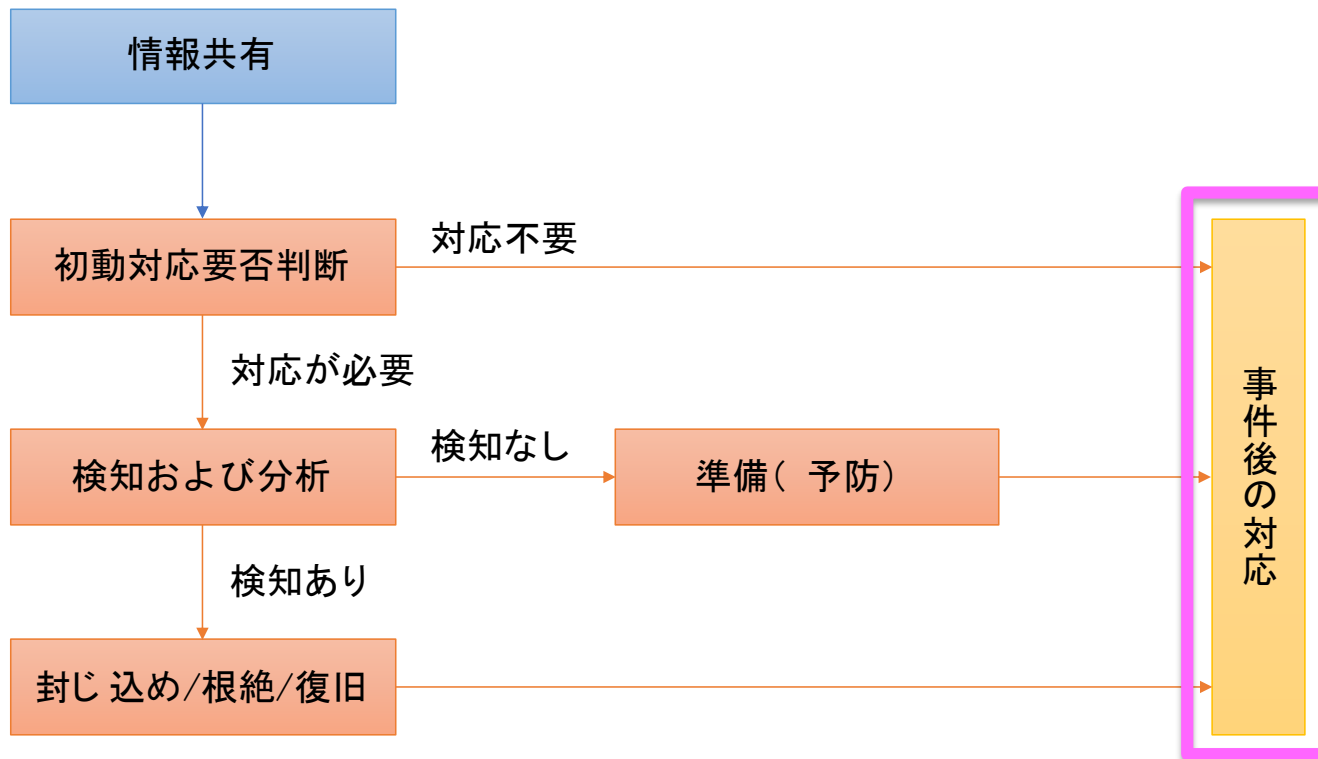


参照：ISOG-J『サイバーセキュリティ情報共有の「5W1H」』P4

封じ込め/根絶/復旧



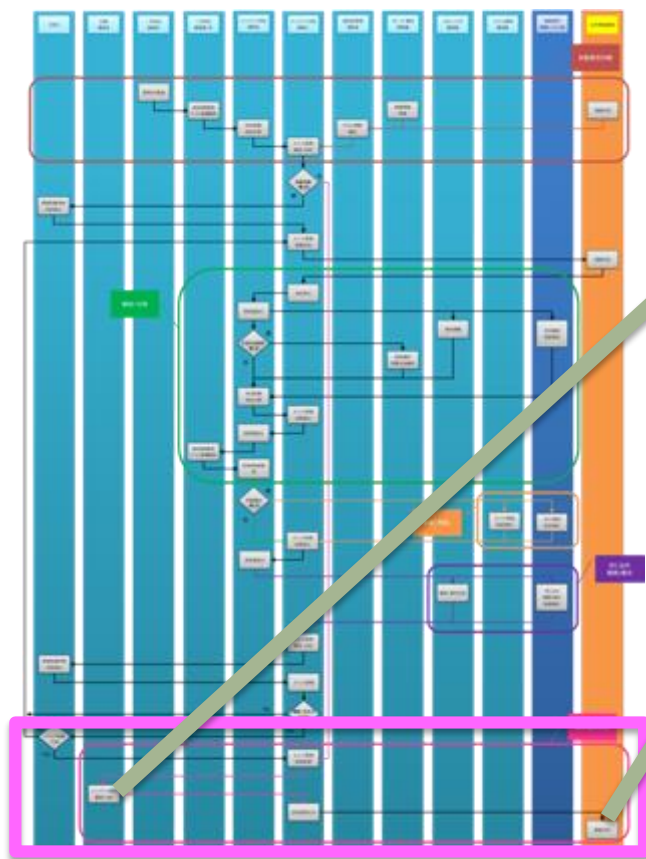
共有情報を用いたセキュリティ対応の流れ (Why&When)



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。



The screenshot shows the ISOG-J website with a navigation menu at the top. The main content area is titled '活動紹介' (Activity Introduction) and lists several documents:

- Webシステム/Webアプリケーションセキュリティ要件書 Ver.3.0 (2019年1月)**: A document regarding security requirements for web systems and applications, published in January 2019.
- セキュリティ対応組織の教科書 ハンドブック v1.0 (2018年9月)**: A handbook for security response organizations, published in September 2018.
- Webアプリケーション脆弱性診断ガイドライン (2018年5月)**: Guidelines for web application vulnerability assessment, published in May 2018.
- セキュリティ対応組織の教科書 v2.1 (2018年3月)**: An updated handbook for security response organizations, published in March 2018.
- セキュリティ動静マップ2017年まとめ (2018年1月)**: A summary of security activities for 2017, published in January 2018.

On the right side of the page, there is a '関連リンク' (Related Links) section with logos for JNSA, JPCERT/CC, IPA, IA japan, and WASForum.jp.

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

(アイコン提供)

いらすとや <https://www.irasutoya.com/>

- 本資料は クリエイティブ・コモンズ 表示 4.0 国際 ライセンスの下に提供されています。
 - <https://creativecommons.org/licenses/by/4.0/legalcode.ja>
- 本資料に登場する会社名、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。本資料内では「®」や「™」は明記しておりません。
- 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>