公開資料

セキュリティ対応組織（SOC, CSIRT）の教科書

ハンドブック

（2018 年9月発行）

日本セキュリティオペレーション事業者協議会

はじめに

このハンドブックは、初めてセキュリティ対応のことを考える方でもセキュリティ対応する組織がどのようなものなのか理解していただけるよう、「セキュリティ対応組織（SOC, CSIRT）の教科書」から、セキュリティ対応組織の役割やその成熟度モデル（ISOMM）に関する部分を取り上げ、わかりやすくなるよう一部表現も変えながら取りまとめたものです。

ハンドブックを通してセキュリティ対応する組織の形をどう考え、作り上げたり、日々運用したりすると良いのかイメージしていただきたいと思います。

日々のセキュリティ対応業務の中でより具体的な課題に直面した場合には、ぜひ原典である「セキュリティ対応組織（SOC, CSIRT）の教科書[1]」をご覧いただき、さらに理解を深めていただければ幸いです。

[1] https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

セキュリティ対応組織とは

「セキュリティ対応組織」という言葉に明確な定義があるわけではありません。企業や組織ごとにその形はバラバラです。

しかしながら、どのような形であれ企業や組織がセキュリティに取り組まなければならないのは、**事業におけるセキュリティリスク低減**のためです。

例えば個人情報漏えいやサイバー攻撃によるシステム停止などのセキュリティ事故のように、セキュリティリスクが具体的な影響として現れるとそれを**インシデント**と呼びます。

セキュリティ対応組織[2]とはそのセキュリティリスク低減のため、**インシデントの発生を抑制し、発生してしまったとしても被害を最小化する任務を負う組織**と言えるでしょう。

[2] 「セキュリティ対応組織」という言葉は少し冗長なので、このハンドブックでは以降「セキュリティチーム（あるいは単にチーム）」と表現することとします。

セキュリティ対応のまわしかた

では、どうやってセキュリティリスクを低減するよう営んでいけばいのでしょうか？

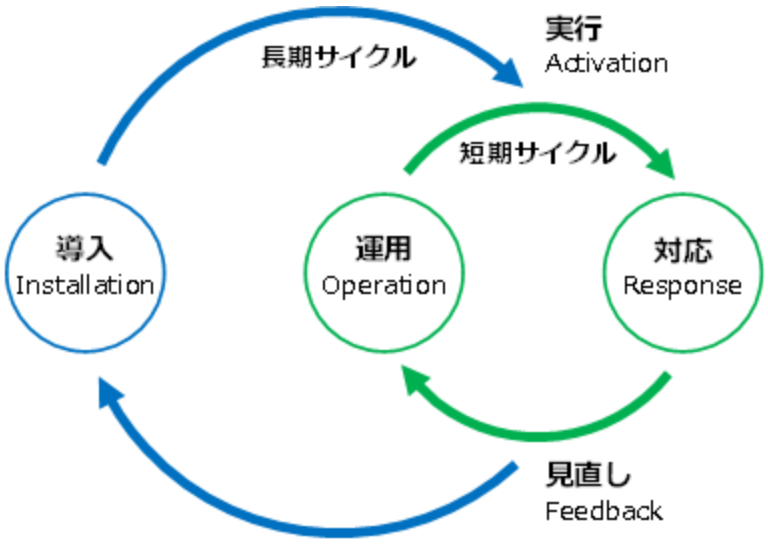
まずはセキュリティ対応に「**導入**」「**運用**」「**対応**」という3つの工程があることを理解する必要があります。

導入	セキュリティに関するルールやシステムなど、セキュリティチームを運営するうえで必要となる仕組みを考え、導入する工程
運用	導入された仕組みがしっかりと働いていることを確認し、インシデントが発生していないか常に目を光らせる普段（平時）の工程
対応	日々の運用の中でインシデントを発見したり、第三者から指摘されたりという、いわゆる有事に対処する工程

これらの工程はそれぞれ独立したものではないということに注意してください。インシデントを発見した後はなぜそれが起こってしまったか運用をスピーディーに見直さなければならないし（短期サイクル）、それが運用でカバ

ーできる範囲を超えてしまったら、より長期的な取り組みとして新しい仕組みをしっかり考えなければなりません（長期サイクル）。

これを図示すると下記のようになります。

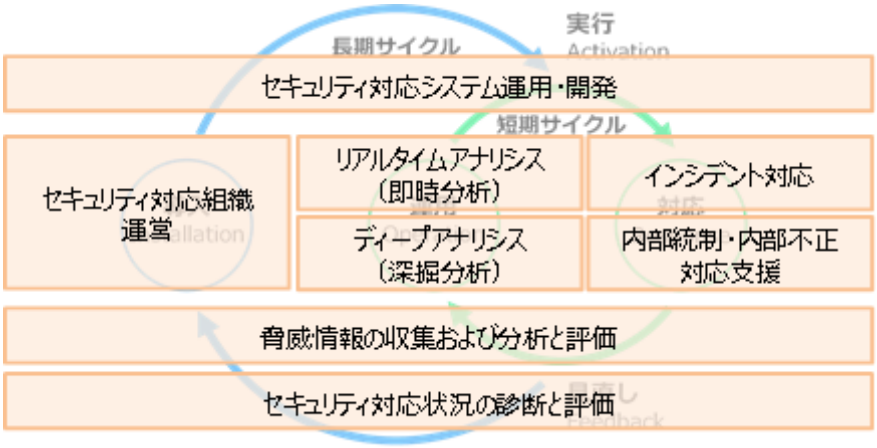


このように**セキュリティ対応には３つの工程があり、それぞれ短期と長期のサイクルで見直し、実行していく**ことで改善していくものなのです。

セキュリティチームの仕事とは

ここからは、3 つの工程と短期・長期サイクルをうまくまわしていくために、セキュリティ対応が具体的にどのような仕事内容となるのか紹介していきます。

先ほどの図に照らし合わせ、まずは業務を大きく 9 つのカテゴリーに分けて説明していきます。



すべの業務を自身のセキュリティチームだけで行う必要はありません。別の部署に手伝ってもらったり、専門の企業にアウトソースしたりといった選択も可能なので、無理のないところから取り組む気持ちで読み進めてください。

◆「導入」の業務

A．セキュリティ対応組織運営

何をどう守っていくかセキュリティチームの活動内容を決め、取り組みを仕切っていくお仕事

◆「運用」の業務

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

C．ディープアナリシス（深堀分析）

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

◆「対応」の業務

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

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、総務や法務を支援するお仕事

◆ 「実行」するための業務

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

◆ 「見直し」するための業務

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

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取りまとめ、次に生かすお仕事

◆ その他の業務

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、会を催したり、セキュリティ仲間を増やすお仕事

これらをさらに細分化し54の役割に分類したものが別紙「セキュリティ対応の役割一覧」です。詳しくはそちらをご覧ください。

何から取り組むべきか

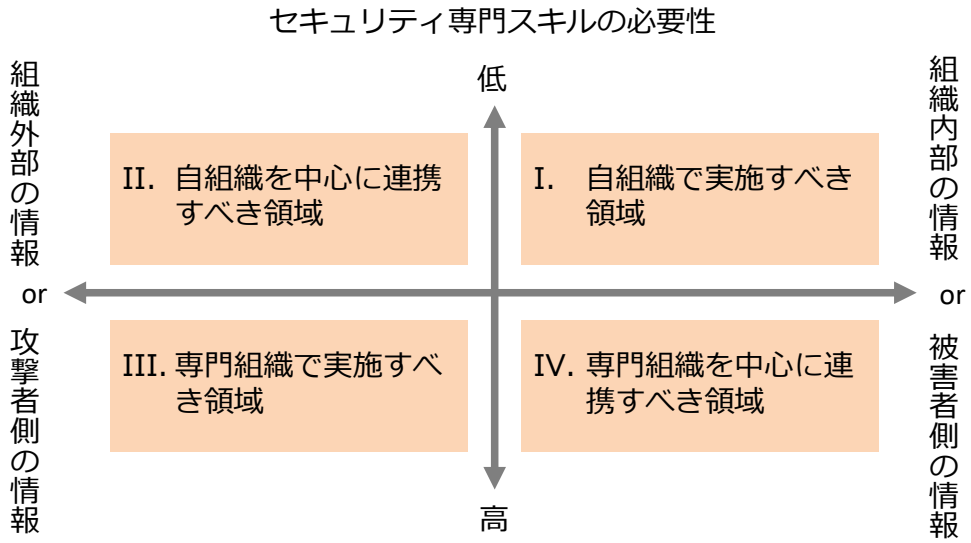
取り組むべき業務を9カテゴリー54種の役割に分類しましたが、どこから実現していけばよいのか、その優先度を2つの軸で考えてみます。

① 必要なのはセキュリティ専門スキル?それとも社内スキル?

② 扱うのは攻撃者（社外）の情報?被害者（社内）の情報?

セキュリティ専門スキルが必要で攻撃者側の情報を扱う業務であれば専門家へ依頼（アウトソース）した方が賢明です。一方で、社内の情報を社内調整しながら扱っていくような仕事は、事情をよく分かっている自分たちで優先的に取り組むべきです。

この考え方を図にすると次のような4領域になります。



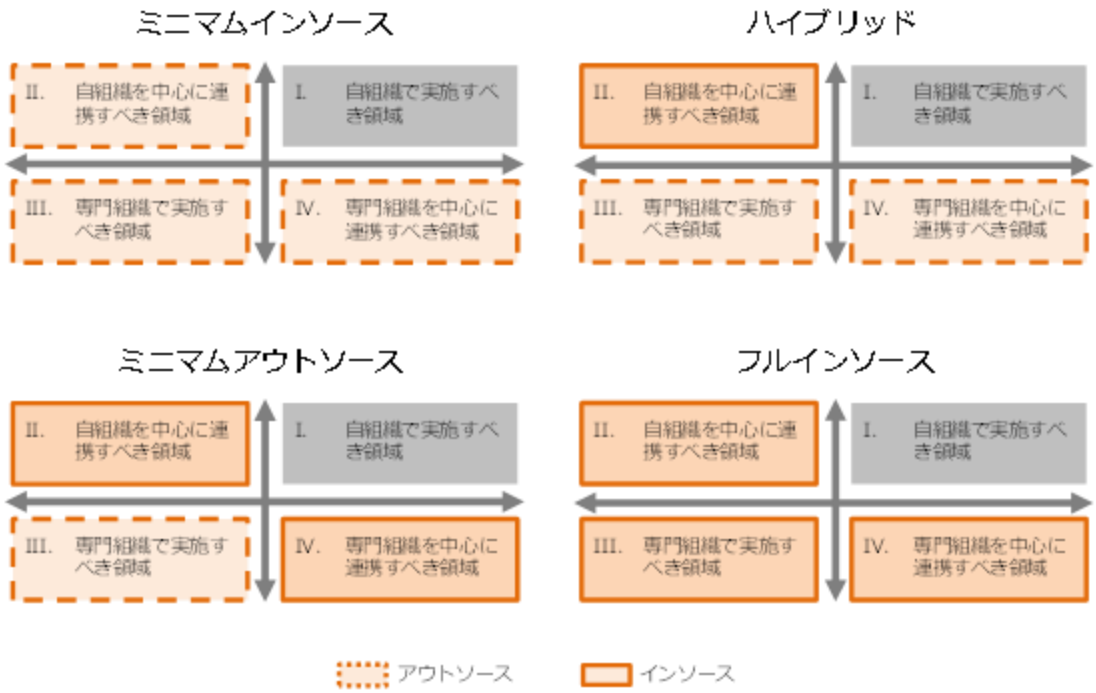
自らのチームで取り組む優先度は、I、II、IV、III の順となります。

これらの領域に、54の役割を当てはめてみると次のようになります。

これにより取り組むべき役割の優先度を考えることができます。あとは、自分たちでどこまで頑張るか線を引けば、セキュリティチームの役割がはっきりと決まります。

どこまで取り組むべきか

4領域のうちどこまで自チームでやるか（インソース）決めることになりますが、パターンとしては以下の4つとなります。



一般的には、自分でできることが最少の状態「ミニマムインソース」から始まります。必ずしもすべてを自分たちで実施する「フルインソース」を目指す必要はありません。所属している会社や組織の方針、予算、人材の能力などによって柔軟に選択されるべきです。

重要なのは、どのパターンを目指すにしても決められた役割をしっかりこなせること、つまり「チームの**成熟度**が高い」状態を目指すことです。

セキュリティチームの成熟度とは

セキュリティ対応組織の成熟度は下記の観点で測ることができます。この成熟度モデルを ISOMM（ISOG-J SOC/CSIRT Maturity Model：イソム）と呼びます。

◆ インソースの場合：**属人ではなく組織的な営みになっているか**

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	+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	評価外

◆ アウトソースの場合：**サービスを活用しきれているか**

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	評価外

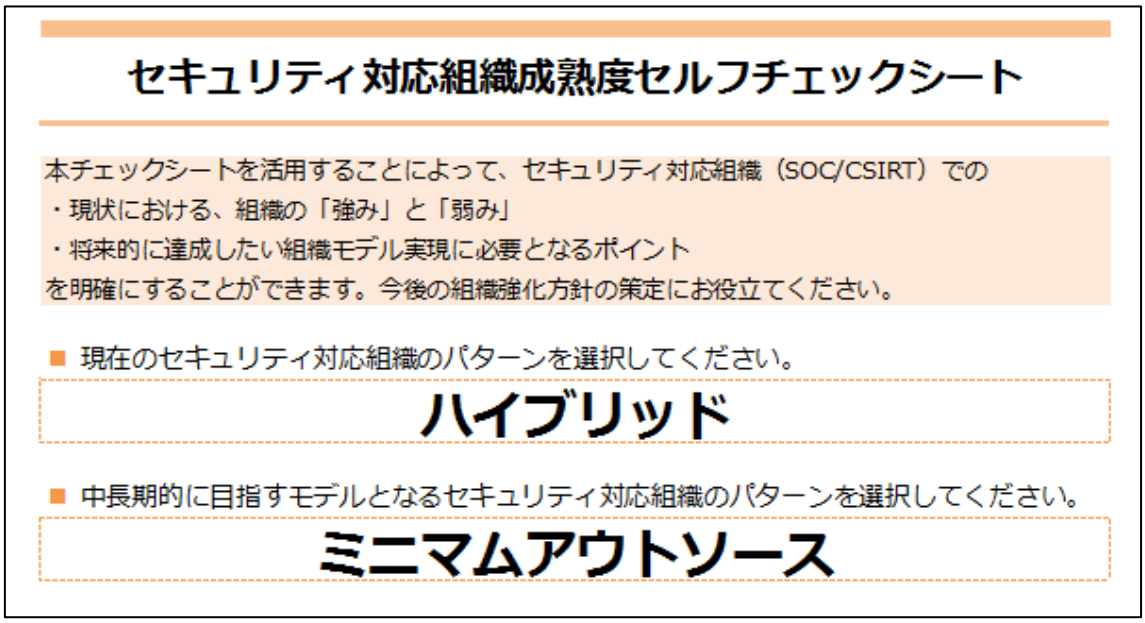
そして、この指標を簡単にチェックするためのツールとして、「セキュリティ対応組織成熟度セルフチェックシート[3]」を使ってみましょう。

[3] https://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

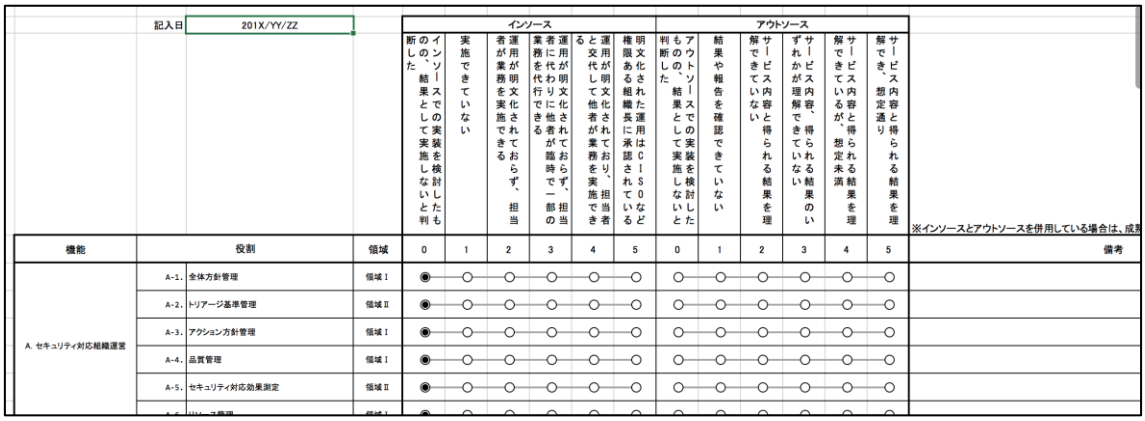
成熟度セルフチェックシートの使い方

セルフチェックシートの使い方は簡単です。

① ４つの組織パターンから、今の姿と、目指したい姿を選択する

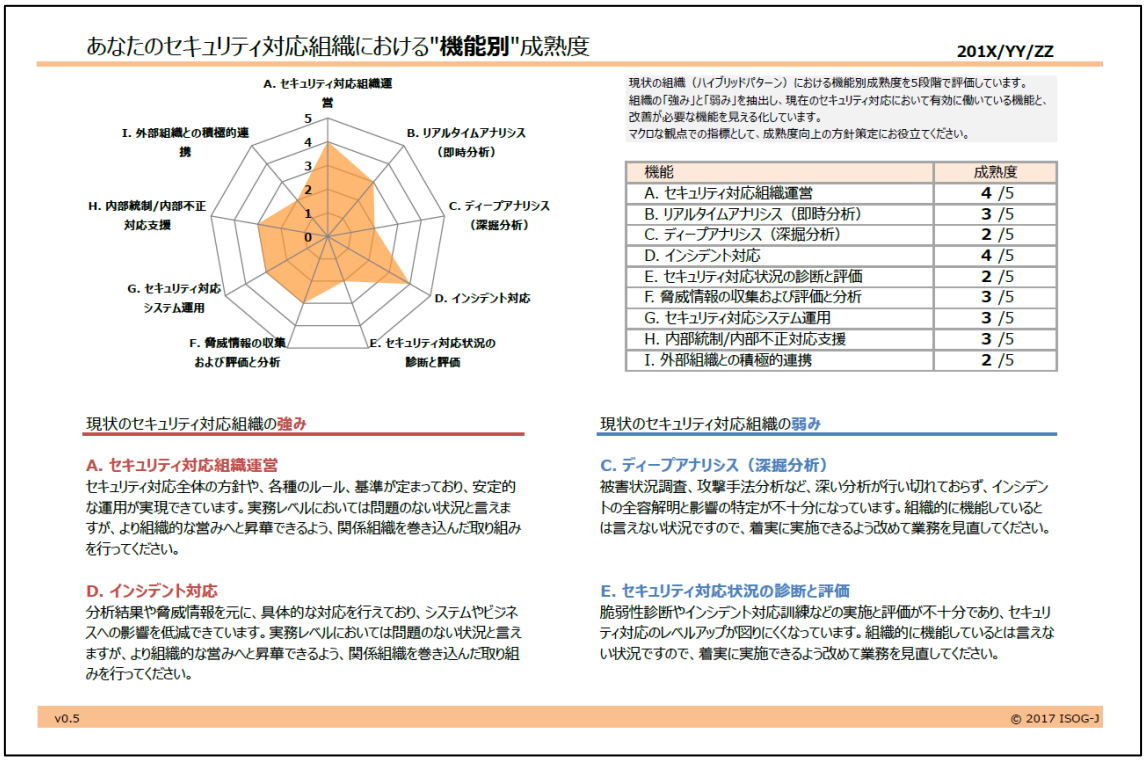


② 指標にそって採点する



たったこれだけで、自動的に2つの観点で成熟度が見える化されます。

◆ 機能別成熟度

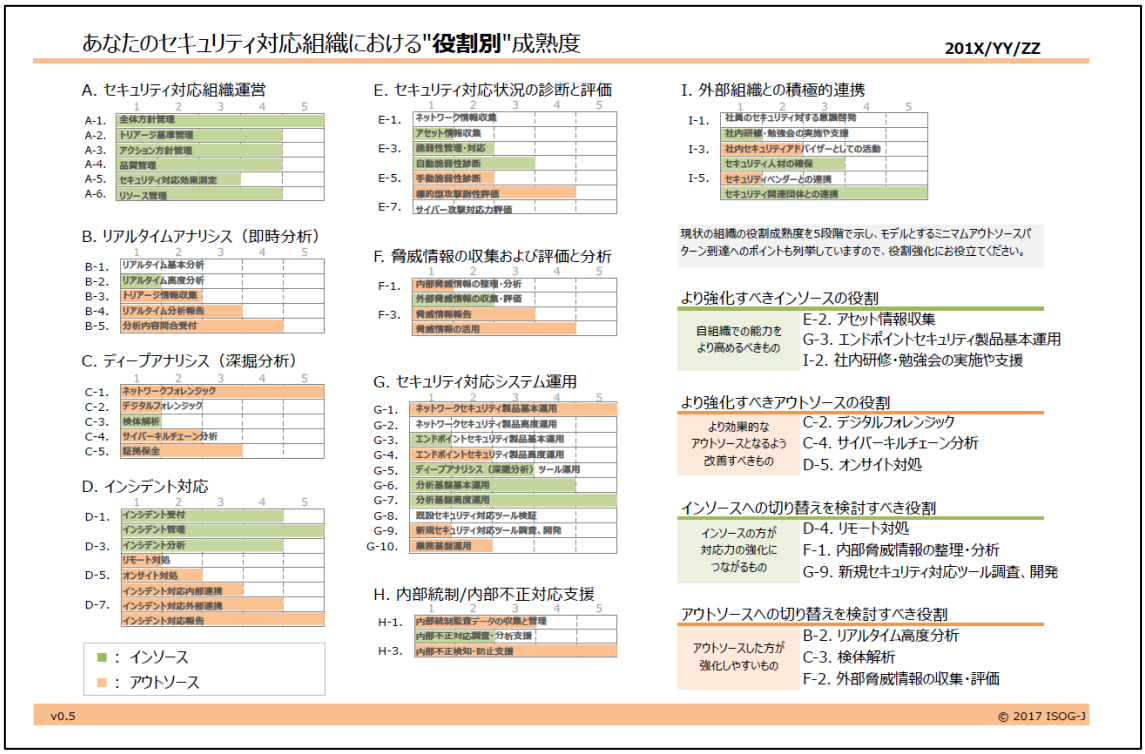


9つの業務カテゴリー別に成熟度がポイント化されます。

また、現在の「強み」と「弱み」、それらについてのコメントが自動的に表示されます。

この結果は、セキュリティ対応について、俯瞰的な視点で考えたり、セキュリティに責任を持つ上層部に説明したりするときなどに役立ちます。

◆ 役割別成熟度



こちらはより詳細に54の役割それぞれについて成熟度がポイント化されます。インソース、アウトソースの両面で、今後どの役割を改善していくべきかが右下に自動的に表示されます。

この結果は、セキュリティ対応についてより具体的な観点で考えたり、関係する現場担当者同士や管理者の間で意識を合わせ合わせたりするときなどに役立ちます。

おわりに

セキュリティ対応は自分一人で考えるのはとても難しいものです。

ですが、ガイドラインとして「セキュリティ対応組織（SOC, CSIRT）の教科書」をベースに考えていけば、今何ができていて何が足りないのか、これから何をすべきなのか、少しずつ整理していくことができるはずです。

成熟度セルフチェックシートも、少なくとも半年に一度は活用しながら、自身のセキュリティチームの営みがよりよいものとなっているのか見える化し、さらにレベルアップを目指していただければ幸いです。

日本セキュリティオペレーション事業者協議会 （ISOG-J）は引き続き、セキュリティオペレーション事業者の連携によって生まれるノウハウやナレッジをわかりやすくみなさまへお伝えできるよう、活動を続けてまいります。