NTT DATA
Trusted Global Innovator

注目されているセキュリティ事故・事件に関する情報 ＜2020年6月版 (第33号)＞(選り抜き版)

2020年6月29日
ＮＴＴデータ先端技術株式会社
セキュリティ事業本部

今回のサマリー

セキュリティインシデント対応組織の成熟度評価方法について
サイバーセキュリティに関する脅威が複雑化・深刻化しているため、CSIRTの現状を評価し機能強化することが求められています。本記事では、CSIRT成熟度モデルであるSIM3を活用し現状のCSIRTを評価する方法について解説します。

セキュリティインシデント対応組織の成熟度評価方法について

1. はじめに

情報セキュリティならびにサイバーセキュリティ対策などに関する必要性への高まりや政府機関からの言及(※)をきっかけに組織や企業にCSIRTが整備されました。

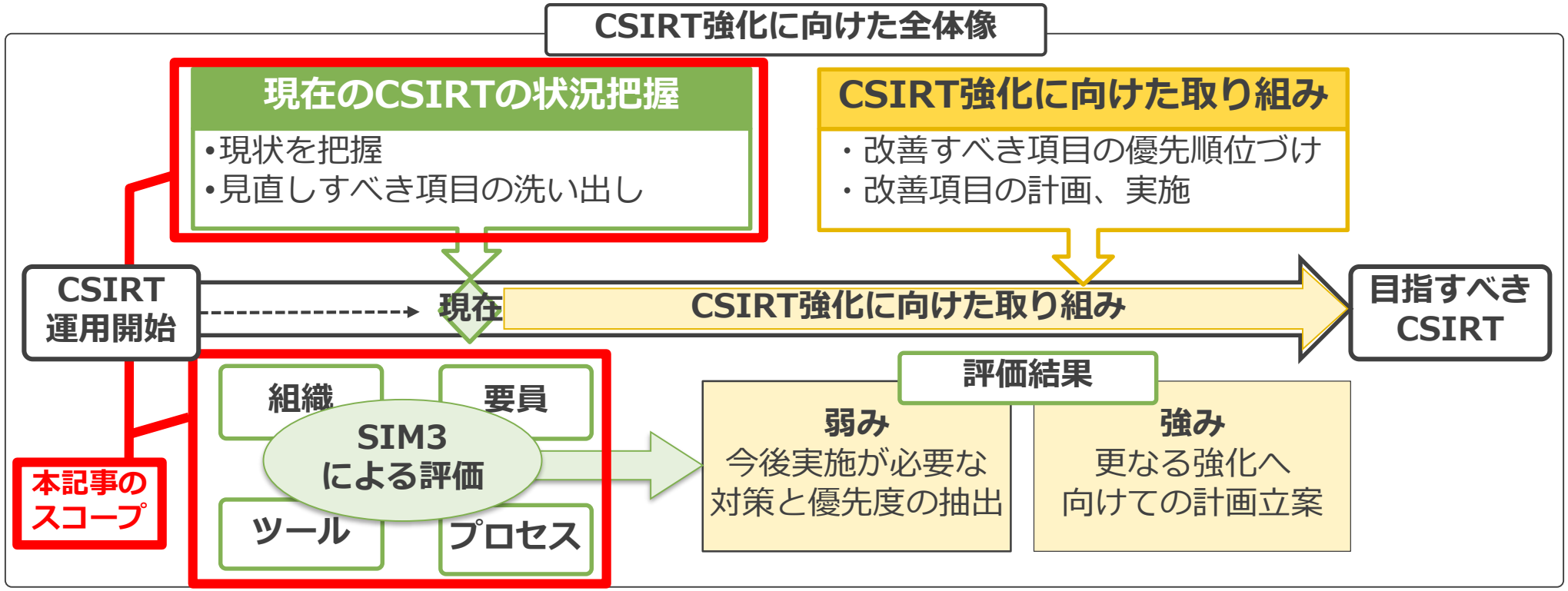
複雑化・深刻化しているサイバーセキュリティに関する脅威の状況を踏まえ、2020年1月29日総務省より「我が国のサイバーセキュリティ強化に向け速やかに取り組むべき事項[緊急提言]の取りまとめについて」が公表されるなど、組織や企業はサイバーセキュリティの改善・強化に取り組む必要性が高まっています。

本記事では、「自組織のCSIRTをどのように評価すればよいのか」について、CSIRT成熟度モデルであるSIM3を活用し、自組織のCSIRTの現状を評価する方法について解説します。

※ 2012年1月19日、内閣官房内閣サイバーセキュリティセンター(NISC)より、「情報セキュリティ対策に関する官民連携の在り方について」の中で、CSIRT(※1)の整備、各組織間連携の必要性などについて明記されました。
※ CSIRT (Computer Security Incident Response Team):セキュリティインシデントの被害を極小化することを目的とした活動組織のこと。

2. SIM3の概要、CSIRT強化に向けた全体像について

SIM3(Security Incident Management Maturity Model)とは、
主にヨーロッパで活用している、CSIRTの成熟度評価を行うモデルのことで、インシデント対応を行う組織の位置づけ、育成計画、インシデント時のツール、運用プロセスなどについて考慮(評価)するべき項目を列挙しており、その項目毎の成熟度を測定することで、組織や企業の「強み」と「弱み」などを可視化し、現状把握と今後の改善、強化につなげるツールとなっています。
ENISA(欧州ネットワーク・情報セキュリティ機関)は、EU各国のナショナルCSIRTの改善、強化の際にSIM3を利用しています。



3. SIM3の構成要素について (1/3)

SIM3を活用し現状のCSIRTを評価を行う前に、SIM3の構成要素である「評価分野」「レベル」「レーダーチャート」の３つについて説明します。

■ 評価分野

評価分野では、「組織」「要員」「ツール」「プロセス」の4つから構成され、次のような観点によりそれぞれ評価を行います。

評価分野	説明
組織 (Organization)	CSIRTとしての承認や目的、サービス範囲など、全10項目について評価を行います。
要員 (Human)	行動指針や要員の配置数、スキルマップ、トレーニング機能など、全7項目について評価を行います。
ツール (Tools)	CSIRTが利用するツールやデータ、各種情報の取り扱いなど、全10項目について評価を行います。
プロセス (Process)	エスカレーションやインシデントの予防・検知・対応、フィードバックなど、全17項目について評価を行います。

このように評価分野は、全44パラメータ(※)の評価項目から構成されます。

※ SIM3:Security Incident Management Maturity Model
http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf

3. SIM3の構成要素について (2/3)

■ レベル

評価分野の44パラメータの各評価項目に対して、自組織の状況に最も適したレベルを選択します。その選択基準レベルとして「０から４」の5つから構成され、次のような観点により選択します。

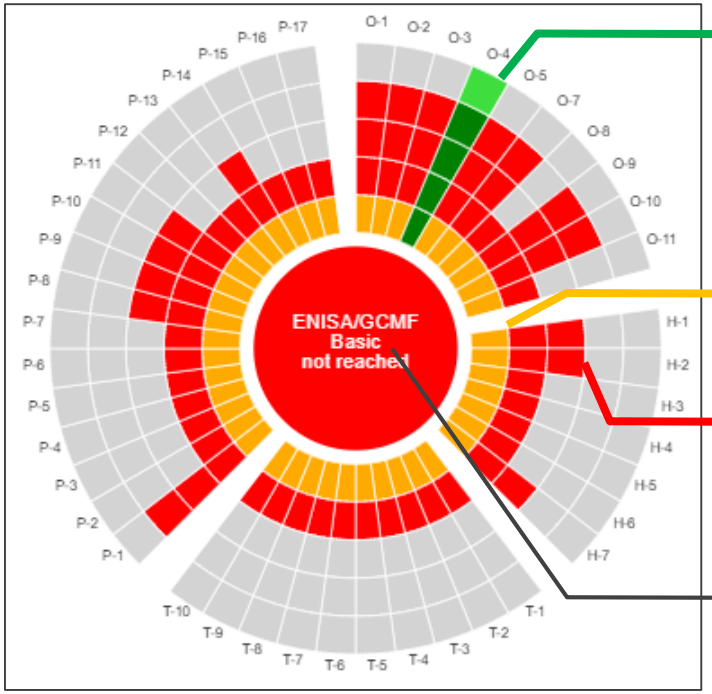
レベル	説明
0	業務として定義していない。
1	業務として認知しているが、文書化されていない。
2	業務として定義および文書化しているが、チーム管理者は正式に承認していない。
3	業務として定義および文書化している。かつ、チーム管理者は正式に承認している。
4	レベル３を満たしつつ、定期的に実務の内容確認、改善を実施している。

評価分野のパラメータをどのようにレベル選択を行うのかについては、「評価方法例について」のページで具体的に説明します。

3. SIM3の構成要素について (3/3)

■ レーダーチャート

評価分野の44パラメータの各評価項目に対してレベル選択を行った結果、項目毎の評価についてグラフ化され、自組織の「強み」「弱み」を把握することができます。



目指すべき設定値を超えて選択している（レベル4を選択時）

現在選択している（レベル０を選択時）

目指すべき設定値（レベル2）

凡例

緑：レベル選択が目指すべき設定値と同じ　または　目指すべき設定値を超えている

橙：現在選択している

赤：目指すべき設定値

「Basic(※)」「Advanced」など評価指標が準備されています。
※サンプル画面は「Basic」となります。

Open CSIRT –SIM3 Self Assessment
http://sim3-check.opencsirt.org/#/

このように、SIM3の３つの構成要素について説明しました。

本記事では、「SIM3を活用した現状のCSIRTを評価する方法」について解説しているため、評価結果の分析で利用するレーダーチャートについての説明は省略します。

4. 評価方法例について (1/2)

SIM３の構成要素である「評価分野(項目)」「レベル」を活用し、現状のCSIRTを評価する方法として、「評価分野(項目)：組織」の一部を例に挙げ説明します。

■具体例

組織の「O-1：信任」の該当パラメータの説明内容を確認します。

分野	項番	項目名 (英語名)	説明
組織	O-1	信任 (Mandate)	CSIRT組織やその活動が上位のマネジメントレベル(経営層など)から承認されているか。

上記パラメータ説明を踏まえ、自組織の状況が最も適しているレベルを以下から選択します。この際、現状のCSIRTを評価する目的であるため、背伸びをしたレベル選択をしないよう注意が必要です。(本記事ではレベル３を選択)

レベル	説明
0	業務として定義していない。
1	業務として認知しているが、文書化されていない。
2	業務として定義および文書化しているが、チーム管理者は正式に承認していない。
3	業務として定義および文書化している。かつ、チーム管理者は正式に承認している。
4	レベル３を満たしつつ、定期的に実務の内容確認、改善を実施している。

このように、全44パラメータについてレベルを選択していきます。

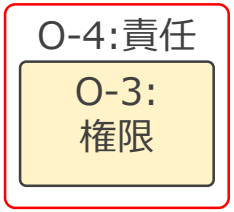
4. 評価方法例について (2/2)

次に、レベル選択時にて他のパラメータと整合性を合わせる必要があります。

例えば、下表の様にO-3(権限)、O-4(責任)をレベル3と選択した場合、 O-3はO-4と一致またはO-4の範囲内に収まるように正しく業務設計を行っている必要があります。

分野	項番	項目名(英語名)	説明	選択レベル
組織	O-3	権限 (Authority)	CSIRTが活動目的を達成するための権限を有しているか	3
	O-4	責任 (Responsibility)	コンスティテュエンシー(サービス対象者)に対しどのような活動の責任を負っているか	3

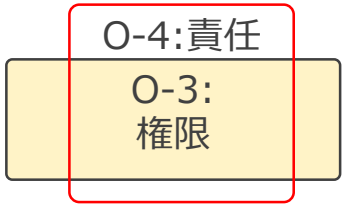
正しい業務設計時のイメージ



しかし、運用当初はそれぞれレベル３であっても現段階でO-3がO-4の範囲を超えていることが考えられ、運用中にて業務に不整合が生じたことになります(右図)。

この場合、O-3とO-4についてレベル２,1,０のいずれかから自組織の現状を踏まえて、レベルを選択する必要があります。

不整合が発生したイメージ



このように、全パラメータを俯瞰し整合性を合わせながら「現状把握、見直しすべき項目の洗い出し」を行います。

5. まとめ

本記事では、SIM3を活用した現状のCSIRTを評価する方法について、「評価分野(項目)：組織」の一部に焦点を当て解説しました。また、他のパラメータについても同様の考え方で評価が行えます。

本記事を参考に評価を行い複雑化・深刻化しているサイバーセキュリティに関する脅威に対応できるよう、CSIRTの改善・強化に取り組むことをお勧めします。この際、自組織が到達する目標値は、自組織のリソースや予算などの実情に合わせ実現可能性のある設定値にする必要があります。

SIM3を活用する際は、本記事で触れた以外にも以下点について注意が必要となります。

- 44パラメータ全てを評価することが目的ではなく、自組織のミッションに応じてCSIRTの機能として改善・強化すべき業務を明確化し実施することが求められます。
- O-6のパラメータは現在欠番扱いとなっており、全パラメータ数は44項目となります。
- レーダーチャートの基準値は、ナショナルCSIRT(※)が目指す基準値となっているため、やや高めに設定されています。

※ナショナルCSIRT:国や地域を代表してセキュリティインシデントを対応するCSIRTのこと。
日本の場合は「JPCERT/CC」が該当します。

6. 参考URL

- 情報セキュリティ対策に関する官民連携の在り方について
  https://www.nisc.go.jp/conference/suishin/ciso/dai4/pdf/1-1.pdf
- 総務省｜「我が国のサイバーセキュリティ強化に向け速やかに 取り組むべき事項[緊急提言]」の公表
  https://www.soumu.go.jp/menu_news/s-news/02cyber01_04000001_00093.html
- Open CSIRT Foundation
  https://opencsirt.org/csirt-maturity/sim3-and-references/
- ENISA
  https://www.enisa.europa.eu/
- SIM3:Security Incident Management Maturity Model
  http://opencsirt.org/wp-content/uploads/2019/12/SIM3-mkXVIIIc.pdf
- Open CSIRT –SIM3 Self Assessment
  http://sim3-check.opencsirt.org/#/

NTT DATA

Trusted Global Innovator