大学 CSIRT における SIM3 の活用

松村 宣顕 [1)], 内山 巧 [1)], 永井 一弥 [1)], 吉田 由美子 [1)], 不破 泰 [1)], 菊池 聡 [1)]

1) 信州大学 セキュリティ・インシデント・レスポンス・チーム

matsumura@shinshu-u.ac.jp

Application of SIM3 for University CSIRT

Noriaki Matsumura [1)], Takumi Uchiyama [1)], Kazuya Nagai [1)], Yumiko Yoshida [1)]
Yasushi Fuwa [1)], Satoru Kikuchi [1)]

1) Security Incident Response Team, Shinshu Univ.

概要

SIM3 と呼ばれる CSIRT 組織成熟度評価のモデルを国立大学法人の CSIRT に適用し現状分析を実施した。組織（O; Organization）人材（H; Human）ツール（T; Tool）プロセス（P; Process）の 4 象限 44 項目で評価し、CSIRT 構築時の成熟度を明らかにした。本報では、CSIRT の課題を概観した上で、SIM3 を活用して大学 CSIRT の現状を分析した結果を報告する。そして、CSIRT 形骸化防止と継続的改善に関する展望を述べる。

1 はじめに

ネットワークが世界を覆いデータが駆け巡る現在の社会状況においては、営利企業に限らず全ての組織にとって、サイバーセキュリティは組織経営と密接不可分となっている。組織の活動がデジタル化するなかで、サイバーセキュリティは、組織が成長し、あらゆる面で良い方向に変化していくための基盤である。

サイバーセキュリティは、組織の状況に応じた技術的対策と組織的対策の適切な組み合わせが肝要である。しかし、一般にサイバーセキュリティとは技術的課題であると認識される傾向がある。2020 年の情報処理推進機構（IPA）の調査報告書[1]において、サイバーセキュリティに関する予算が、人材ではなく技術投資に集中していることが指摘されていることからもこの傾向がわかる。組織的対策を疎かにして、技術的対策に頼る運用体制は、継続性の限界を早める。そこに適切な組織マネジメント体制を確立することが重要である。

サイバーセキュリティに関する組織的対策に CSIRT（シーサート; Computer Security Incident Response Team）の構築と運用があげられる。CSIRT とはサイバーセキュリティに関わるインシデントに対処するための組織の総称である。CSIRT を構築する組織は増大する傾向にある。信州大学においても、他部門との兼任メンバーによる体制ではあるものの、CSIRT を構築しネットワーク監視とインシデント対応に実績をあげている。CSIRT の増加は社会全体のセキュリティの向上に寄与する。一方で、構築しただけで活動実態のあまりない、または、質の低い形骸化した CSIRT も登場することとなった。信州大学では CISRT の形骸化防止の観点から、Open CSIRT Foundation の公開する SIM3（Security Incident Management Maturity Model）[2]を活用し、CSIRT の現状分析と継続的改善に取り組んでいる。

本報では、CSIRT の課題を概観した上で、SIM3 を活用して大学 CSIRT の現状を分析した結果を報告する。そして、CSIRT 形骸化防止と継続的改善に関する展望を述べる。

2 CSIRT の課題

日本シーサート協議会（NCA）によれば、2007 年の NCA 発足時の加盟チーム数が 6 であったのに対して、2021 年 8 月 5 日時点では加盟チーム数が 423 と増加している[3]。一般に、サイバーセキュリティに関する技術的対策が重要視される傾向があるなかで、我が国における組織的対策が少しずつ進んでいることが伺える。

他方で、構築しただけで活動実態のあまりない、形骸化した CSIRT も登場することとなった。萩原・杉浦（2017）は「名ばかり CSIRT」としてこの問題を提起している[4]。萩原・杉浦（2017）は我が国の CSIRT には 2 つの課題があると指摘する。

第 1 の課題が、CSIRT が経営層から真の承認を

得られていないことである。彼らは、CSIRT の資源（人員・予算）不足の観点から、経営層から真の承認を得られていないと考察している。

第 2 の課題が、CSIRT と本務の差別化の難しさである。本来は、リスク対策部門・総務部門が CSIRT を担うのが適しているのであるが、実際には情報システム部門が兼務する傾向が強いと指摘している。

これらを CSIRT 実務担当者の視点から換言すれば、次の 2 点が現実的な課題と言える。

(1) 資源（人員・予算）の不足

(2) 情報システム部門の CSIRT 兼務

萩原・杉浦（2017）は、これらの課題を背景に身の丈に合った CSIRT を構築すべきと提言する。加えて、CSIRT の最低要件として「使命（Mission）・役務（Service）・活動範囲（Constituency）の定義」「信頼できる窓口の構築」「経営層の真の承認」をあげている。

3 SIM3

2.で示した課題を背景に、信州大学では SIM3 を活用し CSIRT の現状分析と継続的改善に取り組んでいる。ここでは、SIM3 の概要を説明した上で、信州大学 CSIRT に SIM3 を適用した結果の概要を報告する。

SIM3 は Open CSIRT Foundation の公開する CSIRT の組織成熟度評価のモデルである。欧州連合（EU）で広く活用され、我が国では NCA を中心に利用されている。EU や我が国で活用されている国際的な組織成熟度評価のモデルを基に現状分析することで、客観的指標に基づく CSIRT の評価と計画的な改善が可能となる。また、SIM3 の適用結果を共有することは、学内の利用者や経営層に対して CSIRT の活動の透明性を高めるという効果がある。2.で示した資源（人員・予算）の不足等の課題と併せて提示することで、CSIRT の置かれている状況が詳らかになる。資源（人員・予算）配分を決定する経営層はその決定に客観的指標を要する。CSIRT に関する資源（人員・予算）配分の客観的指標としても SIM3 は活用できる。

SIM3 は CSIRT の理想形に対して、自組織の CSIRT の現状を組織（O; Organization）人材（H; Human）ツール（T; Tool）プロセス（P; Process）の 4 象限 44 項目（パラメータ）で成熟度を自己評価し可視化するモデルである。

組織（O）象限では、信頼性の高い CSIRT サービスの基盤を提供するために、経営層から CSIRT メンバーが文書で任命されているか、サービス対象者が文書で規定されているか、CSIRT サービスの内容が文書で定義されているかなど 10 項目で成熟度を評価する。

人材（H）象限では、CSIRT メンバーの行動指針が文書化されているか、CSIRT メンバーの要員構成について文書化されているか、CSIRT メンバーに対するトレーニングについて規定し文書化しているかなど 7 項目で成熟度を評価する。

ツール（T）象限では、CSIRT メンバーがインシデント対応を行うためのツールや情報源について規定し文書化しているかなど 10 項目で成熟度を評価する。

プロセス（P）象限では、インシデント予防・対応のプロセス、インシデント対応における経営層・広報部門・法務部門へのエスカレーションプロセスが定められ文書化されているか、機密情報の取扱いプロセスが定められ文書化されているか、定例ミーティングが定められているかなど 17 項目で成熟度を評価する。

SIM3 では、4 象限 44 項目の各項目に対してレベル 0 からレベル 4 までの 5 段階で評価する。44 項目すべてについて評価することで、自組織の CSIRT がどういう状況にあるのかを可視化できる。EU の専門機関である欧州ネットワーク・情報セキュリティ機関（ENISA; European Network and Information Security Agency）は SIM3 を基に「ENISA CSIRT maturity assessment model」[5]を公開し、SIM3 の 4 象限 44 項目の各項目について、次の 3 タイプの要求値を示している。

- Advanced Maturity Level
- Intermediate Maturity Level
- Basic Maturity Level

本報では、このうち、ENISA の Basic Maturity Level の要求値を目標値とする。ここで、要求値については注意が必要である。上記の ENISA の要求値は National CSIRT 向けの値である。National CSIRT レベルの評価は組織によっては必ずしも必須ではないため、組織の状況に従い、CSIRT 毎に検討して要求値（目標値）を定めることが重要である。信州大学では、現時点で ENISA の要求値を目標に設定し継続的改善に取り組んでいる。

図 1 に信州大学 CSIRT（信州大学 セキュリティ・インシデント・レスポンス・チーム; SUSIRT）

構築時の SIM3 適用結果と ENISA Basic Maturity Level の要求値を示す。表 1 には、4 象限における SUSIRT の ENISA Basic Maturity Level 到達率を示す。図 1 と表 1 から、ツール（T）象限の到達率が高く、組織（O）人材（H）プロセス（P）象限の到達率が低いことがわかる。すなわち、SUSIRT においても、技術的対策の到達率が比較的高く、組織的対策の到達率が低いことが明らかである。

図 1 から ENISA Basic Maturity Level の要求値と SUSIRT 構築時の SIM3 適用結果の差が 2 レベル分存在する項目があることがわかる。それらが次の 3 項目である。

- O-7: SERVICE LEVEL DESCRIPTION
- O-9: INTEGRATION IN EXISTING CSIRT SYSTEMS
- P-1: ESCALATION TO GOVERNANCE LEVEL

これらは最優先で改善に取り組むべき項目である。そのほか、差が 1 レベル分存在する項目が 22 あり、22 項目についても継続的改善が必須である。ただし、22 項目についてはレベル差が 1 で同水準であるため、どの項目を優先的に改善するか、改善項目の優先順位が直ちには明らかとならなかった。他の情報を参考に優先順位を検討する必要がある。SIM3 は CISRT の現状分析に有用なモデルであるものの、CSIRT 形骸化防止のための、改善項目の優先順位付けについては具体的に提示していない。

4 展望

SIM3 を活用して SUSIRT 構築時の現状を分析した結果の概要を 3 で報告した。ここでは、CSIRT の形骸化防止と継続的改善に関する展望を述べる。

SUSIRT では、ENISA Basic Maturity Level の要求値に達しなかった項目の改善に継続的に取り組む。このとき、ENISA Basic Maturity Level の要求値と SUSIRT 構築時の SIM3 適用結果の差が 2 レベルと大きかった O-7・O-9・P-1 の 3 項目の改善を優先的に実施する。差が 1 レベルの 22 項目についても順次改善を行う。加えて、定期的に SIM3 による現状分析を行う予定である。

SUSIRT は本報執筆時点で仮想的組織であり、専任教職員及び専用の予算が存在しない状況にある。すなわち、2.で示した課題の双方に該当する。資源（人員・予算）の不足等の課題の状況で、すべての改善項目を短期間で実施することは現実的に困難である。したがって、改善項目の効率的な優先順位決定と実施が形骸化防止のために重要である。今後、SIM3 適応結果に従い改善を進めるとともに、次項も検討していく方針である。

- 改善項目の優先順位決定法
  SIM3 では改善項目の優先順位付けについて具体的に提示していないため、ENISA Basic Maturity Level の要求値と SIM3 適用結果の差・改善項目の実行可能性・改善項目の組織への影響度をパラメータとして導入し、優先順位決定法の定式化を検討する。また、具現化するツールの作成も検討する。
- 改善項目の実施方法
  資源（人員・予算）の不足や情報システム部門の CSIRT 兼務の状況における、改善に対する内発的モチベーションを高める方法を検討する。

5 おわりに

本報では、CSIRT の課題を概観した上で、SIM3 を活用して大学 CSIRT の現状を分析した結果の概要を報告した。そして、CSIRT 形骸化防止と継続的改善に関する展望を述べた。引き続き、SIM3 を活用して、CSIRT 形骸化防止に資する取り組みを実施し、組織的対策の到達率を高める方針である。

国際的に活用される CSIRT の組織成熟度評価のモデル SIM3 を基に分析することで客観的指標に基づく評価ができる。CSIRT の組織成熟度向上と経営層による資源（人員・予算）配分に向けて、SIM3 による CSIRT の定期的分析と継続的改善の実施が重要である。

SIM3 は文書化要求の多いモデルである。CSIRT 運用に関する文書化に初期工数はかかるものの、文書化が済み、SIM3 に従った運用が回れば、CSIRT 活動の透明性の向上に加えて、属人性を避けた安定した CSIRT 運用が浸透し、CSIRT の継続性の向上に繋がる。

参考文献

[1] 情報処理推進機構、企業の CISO やセキュリティ対策推進に関する実態調査-調査報告書-、p.11、情報処理推進機構、2020.

[2] Open CSIRT Foundation: SIM3 Model & References, https://opencsirt.org/csirt-maturity/sim3-and-references/ (accessed 2021-09-20).

[3] 日本シーサート協議会: 会員一覧, https://www.nca.gr.jp/member/ (accessed 2021-09-20).
[4] 萩原健太, 杉浦芳樹: CSIRT の最低要件, 情報処理学会コンピュータセキュリティシンポジウム 2017 論文集, Vol.2017, No.2, pp.950-954（2017）.
[5] European Network and Information Security Agency (ENISA): ENISA CSIRT maturity assessment model, https://www.enisa.europa.eu/publications/study-on-csirt-maturity (accessed 2021-09-20).

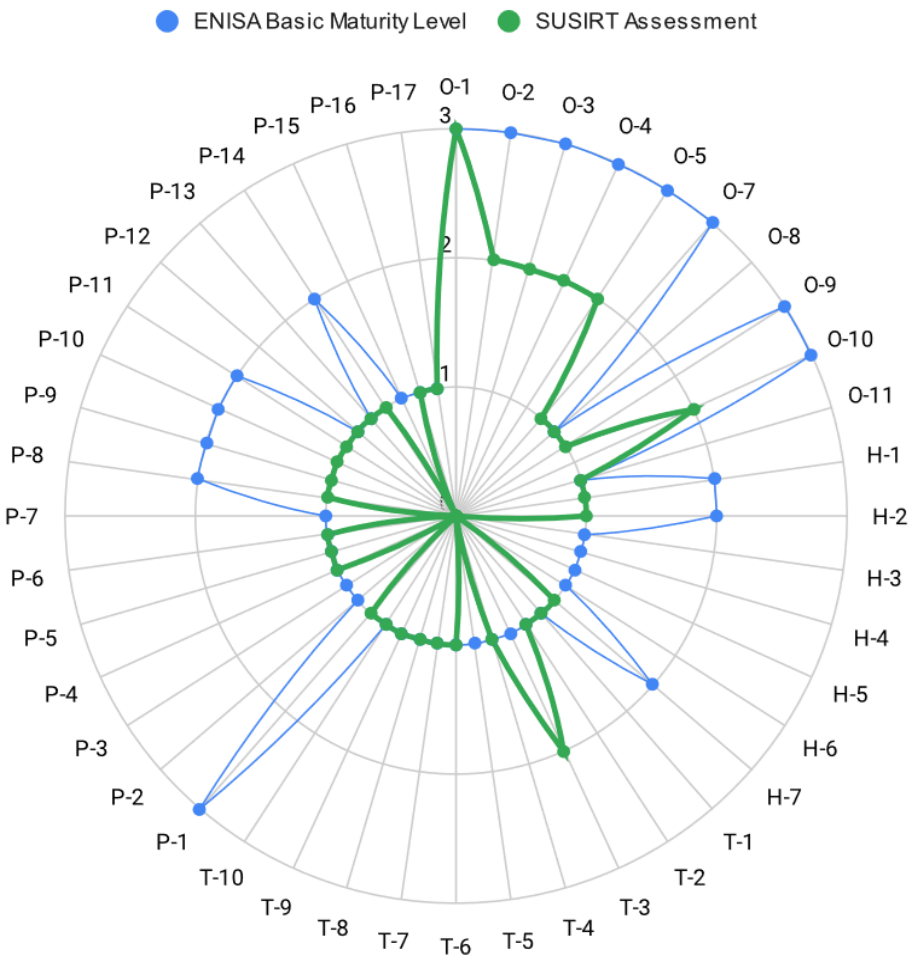

図 1　SUSIRT 構築時の SIM3 適用結果と ENISA Basic Maturity Level

表 1　象限毎の ENISA Basic Maturity Level 到達率

象　限	到達項目数	全項目数	ENISA Basic Maturity Level 到達率
組　織（O; Organization）	3	10	30%
人　材（H; Human）	0	7	0%
ツ ー ル（T; Tool）	9	10	90%
プロセス（P; Process）	7	17	41%