10'00"00 インターネット10分講座

MIN SEC 1/100S INTERNET

CSIRT (Computer Security Incident Response Team)

今回のインターネット10分講座では、サイバー攻撃など昨今のセキュリティインシデントの増加にともない企業や大学などに設置が進んでいる「CSIRT(シーサート)」について、その背景から設置にあたっての注意、活用のためのノウハウなどを取り上げます。

◆ 1.Computer Security Incident Response Team(CSIRT)設置の背景

国内で継続的に発生しているサイバー攻撃を背景に、昨今Computer Security Incident Response Team (CSIRT、シーサート)を設置する動きが活発化しています。その要因として二つのインシデントがあります。一つ目は2011年に防衛産業組織で発生した標的型サイバー攻撃です。

当該インシデント発生以降、シーサート設置に関する議論は活発化し、当時の政府の情報セキュリティ対策を検討・推進等を行う会議である「情報セキュリティ対策推進会議」において、『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』が公開されました。「漠然と組織間で情報共有を行うのではなく、各組織が情報セキュリティインシデントに関する緊急時対応の機能を有した専門的な部隊「CSIRT」を組織し、官民を含む各組織内CSIRT等の間で、専門的、実務的な連携を図ることが必要」※1とシーサートに言及しています。

さらには2013年には『金融機関等コンピュータ・システムの安全対策基準・解説書(第8版追補)』や2014年には『政府機関の情報セキュリティ対策のための統一基準群』においてもシーサートに言及しています。

そして二つ目のインシデントは2015年に公共機関で発生した標的型サイバー攻撃です。

2015年に発生したインシデント以降は、シーサート設置の議論がさらに活発化するとともに、より一層シーサートの拡充に関する議論が深まっています。また政府機関や民間企業に限らず、地方自治体や学術機関等においてもシーサート設置の議論が活発化するなど、拡大と深化が進んでいます。特に2015年に公開された『サイバーセキュリティ経営ガイドライン』においては「サイバー攻撃を受けた場合、迅速な初動対応により被害拡大を防ぐため、CSIRT(サイバー攻撃による情報漏えいや障害など、コンピュータセキュリティにかかるインシデントに対処するための組織)の整備」や「CSIRT間における情報共有や、日本コンピュータセキュリティインシデント対応チーム協議会(略称:日本シーサート協議会)等のコミュニティ活動への参加による情報収集等を通じて、自社のサイバーセキュリティ対策に活かす」※2など、シーサート間連携や日本シーサート協議会のコミュニティ活用についても言及しています。日本シーサート協議会は2017年1月現在で203の組織が加盟する大きな組織となりました。特に2013年以降のシーサート設置が多く、2016年の1年間で加盟組織数が約2倍近く増加するなど、国内におけるシーサート設置が加速していることが伺えます**(左ページ図1)**。

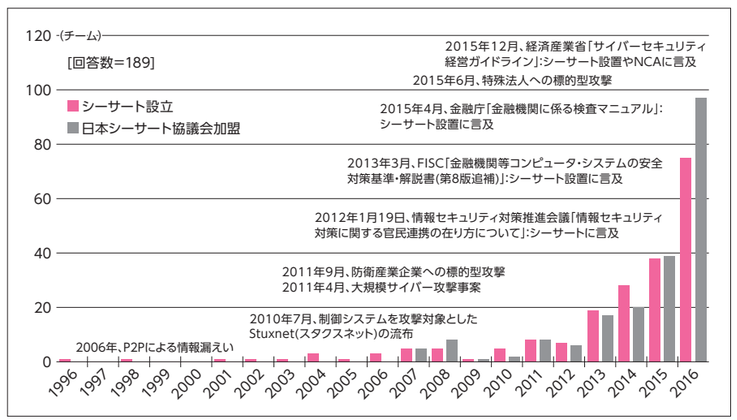

図1:日本シーサート協議会への新規加盟数と加盟チームの設立年の推移

◆ 2.シーサートとは何なのか

シーサートとは「コンピュータセキュリティにかかるインシデントに対処するための組織の総称(機能)であり、インシデント関連情報、脆弱性情報、攻撃予兆情報等を収集、分析し、対応方針や手順の策定などの活動」を行うチームのことです。シーサートは組織の成り立ちや歴史、セキュリティに対する意識、資源等によってシーサートの設置および活動内容が異なるため、百社百様のシーサートがあります。しかしながら、シーサートとして共通して持つべき定義と機能があります。次からその定義と機能について述べていきます。

2.1. シーサートの定義付け

シーサート設置において定義すべき項目は次の四つです。一つ目は「Mission(ミッション(使命))」、二つ目は「Service(サービス(役務内容))」、三つ目は「Constituency(コンスティチュエンシー(活動範囲))」、そして四つ目は「Incident(インシデント)」です。

2.1.1. Mission(ミッション(使命))

既に述べたように外的要因が強まり、経営層が「シーサートを設置せよ」と号令を出す組織もあるようですが、どのような背景であったとしても組織にとって「なぜシーサートが必要なのか」「シーサートでは何を行うのか」といった活動の軸となるミッションを定める必要があります。ミッションを定めておくとシーサート活動に迷いや停滞が生じた時に立ち返ることができ、シーサート活動の大きな助けとなります。

またミッションを検討するに当たっては一個人や一組織だけではなく、関連するさまざまな組織で話し合いをし、シーサート活動を行う予定のメンバーはもちろんのこと、組織全体で共通認識を持っておくように準備、検討をしておきましょう。

2.1.2. Service(サービス(活動内容・役務))

シーサートが提供するサービスはさまざまです。そのためシーサートのミッションに照らし合わせて「シーサートの業務・役務・活動として何をやるべきなのか」を既存(またはシーサート設置に当たって拡張、利用可能な)資源と照らし合わせながら検討する必要があります。

この活動内容の検討で大切なことは「今できることに留めること」です。これはシーサート設置時に、活動内容の対象を広げてしまうと、資源の拡大が今後難しくなることや、活動を行う人員やチームの疲労が進む可能性があるからです。経営層からはより幅広い活動を期待されるかもしれませんが、限られた資源の中で何ができるのかを検討し、できる活動内容から始めるようにしましょう。

日本シーサート協議会が公開している『CSIRTスタータキット』においては、サービスを大きく三つに分類しています**(図2)**。

インシデント 事後対応サービス	・インシデントハンドリング ・コーディネーション ・オンサイトインシデントハンドリング ・インシデントハンドリングサポート ・コンピュータ・フォレンジックス ・アーティファクトハンドリング
インシデント 事前対応サービス	・セキュリティ関連情報提供 ・脆弱性情報ハンドリング ・インシデント/セキュリティイベント検知 ・技術動向調査 ・セキュリティ監査/査定 ・セキュリティツールの開発
セキュリティ品質向上 サービス	・リスク評価・分析 ・事業継続性、災害復旧計画作成・改変 ・セキュリティコンサルティング ・セキュリティ教育/トレーニング/啓発活動 ・製品評価・認定

図2:シーサートのサービス概要※3

一つ目はインシデント発生時の支援内容である「インシデント事後対応サービス」です。例えばインシデント発生時にオンサイト(直接訪問しての)支援を行うのか、また不正プログラムの解析や端末のフォレンジックを行うのかなど、インシデント発生後に活躍するサービスです。

二つ目はインシデントを発生させないことや被害の最小化等を目的とした「インシデント事前対応サービス」です。当然ですがインシデントは発生しないに越したことはありません。そこで普段からインシデントや脆弱性に関する情報収集や、組織内のシステムの異常を早期発見できる仕組み、また早期対処可能な運用体制の構築等を行っておく必要があります。

※1 情報セキュリティ対策推進会議「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」(平成24年1月19日)
http://www.nisc.go.jp/conference/suishin/ciso/dai4/pdf/1-1.pdf

※2 経済産業省「サイバーセキュリティ経営ガイドライン」(平成27年12月28日)
http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf

※3 出展元:日本シーサート協議会「CSIRTスタータキット」

そして三つ目は組織におけるインシデント対応能力を普段から向上させることを目的とした「セキュリティ品質向上サービス」です。ここでは組織のリスク把握や教育・トレーニングの提供等を行い、普段から組織のセキュリティ知識や対応力の向上を図っておく必要があります。

なお、三つのカテゴリに記載されているすべてのサービスを自組織で提供できる組織は、ほぼ存在しません。大切なことは自組織で提供できないサービスを知り、提供できないサービスがあれば代替案をどのようにするのかを検討、準備しておくことです。組織によって提供可能なサービスは異なりますが、自組織の身の丈に合ったサービスを検討し、定義付けていきましょう。

2.1.3. Constituency（コンスティチュエンシー（活動範囲））

組織には数多くのシステムや部門が存在します。組織が有するシステムは自組織で構築・運用しているシステムもあれば、外部に運用を委託しているシステム、または外部サービスを利用している場合もあります。組織が把握、管理しなければならない情報システムは数多く存在し、また組織内外に関係者および関係組織がまたがるため、情報システムのマネジメントは大きな課題です。

シーサート設置時からすべてのシステムに対して、定義したサービスを提供できるのであれば検討する必要はありませんが、資源には必ず限りがあり、サービスの提供範囲を限定しなければなりません。例えば、グローバルに展開している組織であれば、まずは国内のシステムを活動範囲にし、国内で得た経験を活かしてグローバルに展開をしていくように活動範囲を設定する、またはお客様に提供しているサービスで、企業の利益に直結するシステムを対象とし、他のシステムにおいては初期の活動段階では対象とせず、シーサートの活動範囲を追って拡大していくなど、組織によってシーサートの活動範囲の検討を行い、定義付けを行っておくことが必要です。

この活動範囲の定義付けを適切に行わないと、後に自分たちのシーサート活動を苦しめることになります。

インシデントが発生した際に、資源が少ないにもかかわらず、組織全体のシステムに対して対応を求められ、責任も負う可能性があります。（無理をしているにもかかわらず）インシデント対応ができた場合でも、また同じようなことが起こった場合に同様の対応を求められ、現場では疲労や不満が募っていくことでしょう。

また責任が伴うため、シーサートが機能していなかったと経営層が判断すれば、シーサートの予算削減や責任者の処分、場合によってはシーサート自体を解散という議論にも発展しかねません。活動範囲を明確にし、責任の所在を明らかにするとともに、経営層と活動範囲の事前の認識合わせを行っておきましょう。

これらの「ミッション（使命）」「サービス（活動内容）」「コンスティチュエンシー（活動範囲）」はシーサート活動の根幹となります。シーサートを設置し、活動を行うとさまざまな課題に衝突しますが、この三つの要素が確立されていれば、立ち返り、シーサートの検討や活動の確認を行うことができます。シーサートの活動を継続的に行うためにも適切に定義し、また定義した組織は現状に合致したものになっているのか、定期的な確認や見直しを行っていきましょう。

2.1.4. Incident（インシデント）

さて「ミッション」「サービス」「コンスティチュエンシー」の議論をより深く、現実的に行うために必要なことが「インシデント」の定義付けです。

組織にとって何がリスクなのか、守るべき情報資産は何なのかを理解していないとインシデントの定義を行うことは難しいでしょう。何から何を守るべきなのか、脅威や守るべき対象を明確にし、組織にとって何が普段と異なる事象なのか。そしてその事象は組織にとってどれだけ重要な事象なのか（何がインシデントなのか）を定義しておくことが必要です。

例えば会社概要を掲載しているWebページが改ざんされてしまう事象と、組織が運営しているECサイトが改ざんされてしまう事象では組織にとって影響度合いが異なります。このように組織におけるインシデントを、リスクや情報資産を理解した上で定義しておくことが大切です。

2.2. 必要な四つの機能

百社百様あると言われるシーサートですが、シーサートとして持つべき機能があります。ここではその代表的な四つの機能について述べていきます。

2.2.1. Point of Contact

シーサートになくてはならないものが「Point of Contact（＝公開された信頼できる窓口）」です。自組織だけで情報収集やインシデント発生後の対処や調査など、シーサートの活動を行うことは難しく、必ず外部連携が必要となります。またせっかく外部組織が脆弱性やインシデント情報を発見したとしても、通報先がわからないと通報できず、また通報できた場合でもたらい回しにされ、インシデントの発見が遅れることになります。シーサートの顔とも言えるPoint of Contactを定め、定めた窓口を必ず公開するようにしましょう。日本シーサート協議会では加盟組織の外部連携窓口を集約し公開しています。これによりJPCERT/CCや法執行機関、他のシーサートからなどの通報を受けやすい環境を整備しています。

なお、インシデントをはじめとするセキュリティ関連の報告（通報）や問い合わせは、WHOIS DBに登録された連絡先に送付することが国際的にも事実上の標準となっています。当該連絡先にインシデントに関する情報が届いた場合、Point of Contactが中心となり、シーサート全体に速やかに伝わるよう準備しておきましょう。

2.2.2. 技術的な対応

シーサートはサイバー空間に関するインシデントに対して活躍する組織です。サイバー空間の脅威や情報システムに関する最低限の技術的な知識が必要となります。外部から脆弱性情報などを受け取った場合、技術的な視点で脅威を推し量り伝達することや、調整活動、対外的な協力推進などが求められます。この対応を行うためには技術的な知識は必要不可欠です。しかし、誤解をしてほしくないことは、「ホワイトハッカー」と言われるような高度なセキュリティ人材が必要というわけではありません。これらの対応は技術的な要素が関係するとはいえ、外部との折衝や調整を行うことが多く、技術力だけでは不足しています。また考え方によっては技術的な知識は学習によって習得していくことが可能です。そのため技術力が高い人材を発掘するのではなく、「コミュニケーション能力」の高い人材を発掘し、シーサート活動を行うメンバーに加えていきましょう。

2.2.3. 部署（部門）横断

情報システムやセキュリティを所管する組織がシーサートの取りまとめとなっている傾向が強いですが、シーサート活動は部署横断的に行う必要があります。例えばインシデントが発生した際に、公式見解や記者向けの発表を仕切る広報部門や法的な解釈を必要とする場合には法務部門が関連します。またセキュリティ戦略を立案する部門やサイバーセキュリティ教育を実施する教育部門など、シーサートにはさまざまな部門が関係しています。サイバーセキュリティ対策の推進を特定の部門だけが頑張れば良いという「お任せモデル」から組織全体で頑張る「連帯モデル」へと変更していきましょう。

2.2.4. 「レスポンス（Response）」ではなく「レディネス（Readiness）」

既存のインシデントレスポンス体制を活用して、シーサートを構築する組織は多く、既存の体制を活用することはシーサート設置においても正しいプロセスです。しかし、インシデントレスポンス（インシデント発生後の対応）の観点を強く持っている組織は多いですが、インシデントレディネス（インシデントを発生させないようにするための事前対応）の観点が不足している組織が多いのも事実です。このレディネスの観点がないと、今までのインシデント対応体制と何が違うのかという議論に発展するケースも見られます。インシデントレスポンス（事後対処）などの実践的な活動経験を元に、インシデントレディネス（事前対処）を進めることの重要性を理解し、被害の未然防止に努めていくようなシーサート活動を行う必要があります（**図3**）。

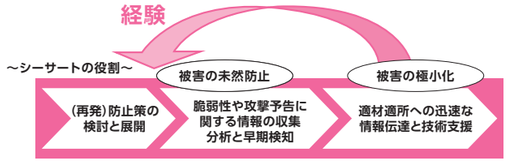

図3：インシデントレディネスとレスポンス概要

◆ 3.日本シーサート協議会加盟状況から見るシーサート

日本シーサート協議会では加盟組織向けに毎年アンケートを実施し、シーサートの現状や活動状況の把握を行っています。ここでは2016年に実施したアンケート内容に基づき述べていきます。

シーサートは技術的な対応を含むため「情報システム管理部門系」が取りまとめを行っている傾向が強く、次いでセキュリティ対策を組織内で専門的に行う「セキュリティ対策部門系」が取りまとめている割合が多くなっています。また割合としては多くはないですが、より部署横断的な観点から「経営企画部門系」や「総務部門系」、さらには組織全体のリスク管理を行う「リスク対策部門系」が取りまとめているシーサートもあります（**図4**）。

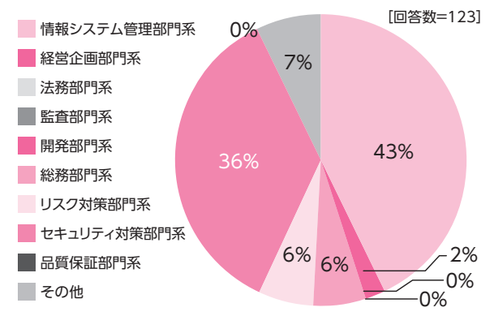

図4：シーサートの取りまとめ部署

情報システム管理部門系やセキュリティ対策部門系がシーサートの取りまとめを行うことは設置がスムーズに進むというメリットがありますが、既存業務の延長線上の要素が強く、より部署横断的にしにくいといったデメリットもあります。

次にシーサートで活動するチーム人数についてです。シーサート設置時においては5名未満が37％、10名未満の割合は合計83％と非常に多く、20名以上でスタートをしているシーサートはわずか2％しかありません。これよりスモー

ルスタートでシーサートを発足している組織が多いことがわかります**(図5)**。

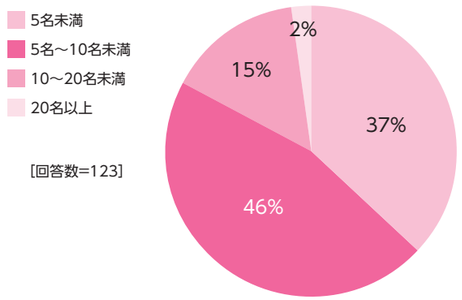

図5：シーサートのチーム人数(設立時)

しかし、活動開始後は割合が大きく変化し、5名未満で活動をしていたシーサートは11%と大きく減少しています。また10名未満の割合も活動前は8割強あった組織も5割弱に減少しています。一方で10名以上の割合は17%から52%まで大きく上昇し、シーサート活動を行うに当たっての拡充が行われていることがわかります。これは活動後にシーサートの必要性を深めることができた組織や、外部連携を行うに当たってさまざまな部門の担当者が連携しなければシーサート活動が難しいことを理解した組織が増加し、より部署横断的にシーサートを支援していることが要因と言えます**(図6)**。

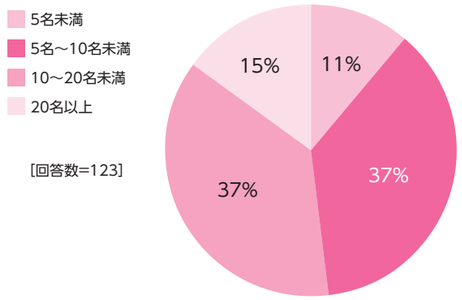

図6：シーサートのチーム人数(活動後)

また実装の形態として独立部署(専任型)でシーサートを実装している組織は12%と少なく、傾向としては金融業界の組織が専任型で行っている傾向が見られます。国内のシーサートのほとんどは兼務型であり、部署横断的にシーサートが設置されています。シーサートの実装形態に確たる答えはないですが、組織内のシーサート活動が最大限発揮できる体制で設置することが望ましいです**(図7)**。

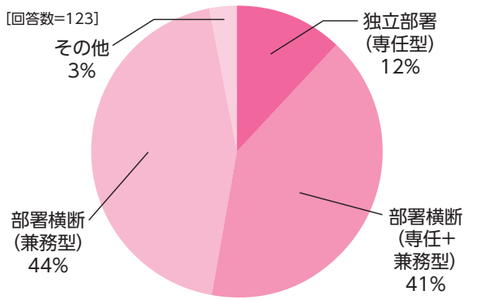

図7：シーサートの実装形態

シーサートの対象としている利用者も変化しています。組織のお客様(顧客)を対象としているシーサートは昨年まで6割前後であったのが4割に減少しています。これは2016年の加盟組織にユーザー組織の加盟が多く進んだことが要因と言えます。またグループ会社全体を利用者としている組織も増加しています。これは加盟組織の増加も一つの要因ですが、運用が進んでいく中でコンスティチュエンシー(活動範囲)の拡大が進んでいることも要因の一つと言えるでしょう**(図8)**。

図8：シーサートのサービス利用者

◆ 4.シーサート設置における勘違い

4.1. 「とりあえずシーサートを作れ」

シーサート設置の背景で述べた通り、政府機関が公開している文書等から経営層も徐々にシーサートを目にまたは耳にする機会が増えてきています。「当社にシーサートがないのであれば早く作れ」といった経営層の言葉がきっかけでシーサート構築が進むことも少なくはありません。しかし、経営層の一言の浅深には大きな差があります。

シーサートは組織の危機管理の一つとなるため、本来は経営層自らがタクトを振り構築を行う方が望ましいですが、往々にして自ら構築に関与することはありません。直接的な構築は行わずとも、最低限組織の危機管理という観点から、指針や方針を示し、シーサートの設置を促すようにしましょう。指針や方針を示されて構築されたシーサートと、すべてを現場に任せて構築されたシーサートでは、組織全体の理解の深さや浸透度が異なります。もし指針や方針を示さず、部下や現場に構築すべてを任せるのであれば、権限および財源の移譲を行った上で構築をすべきです。シーサートは既存の危機管理体制を活用するとはいえ、「とりあえず」で設置できるものではありません。

下図9の通りシーサート構築はプロジェクトの立ち上げから設置に至るまでに数々のプロセスがあります。このプロセスを理解した上で権限と財源を移譲して設置を指示する組織と、理解や移譲を行わずに設置を行おうとしている組織では設置スピードや設置後のシーサートの活動内容に大きな差が生じます。「言うは易し、行うは難し」設置を指示することは素晴らしいことですが、さらに組織に貢献するシーサートにするために、とりあえずではなくシーサートを理解した上で設置を指示し、組織全体で設置を進めていきましょう。

項目①	項目②
プロジェクトの立上げ	目標(構築きっかけの明確化)
	メンバ構成
	スケジューリング
	プロジェクト運営ルール
	経営者/意思決定者の合意
守るべき対象と脅威の把握	社内システムやネットワークの把握
	過去のインシデント情報
	既存のリスク分析結果
既存のインシデントレスポンス体制	既存のインシデントへの事前対応
	既存のインシデントへの事後対応
	既存のセキュリティ向上に向けた取り組み
	既存のインシデントレスポンスに関連する社外組織
	インシデントレスポンスに有効な社外連携体制の確立
既存のセキュリティポリシー およびセキュリティ関連文書	セキュリティポリシー
	災害復旧計画・事業継続性計画
	セキュリティに関連する制約事項や規制
	物理セキュリティに関する制限
基本構想の検討	ミッション、サービスコンスティチュエンシーの定義付け
	インシデントの定義付け
サービスの検討 「インシデント事後対応サービス」	インシデントハンドリング
	コーディネーション
	オンサイトインシデントレスポンス
	インシデントハンドリングサポート
	コンピュータ・フォレンジックス
	アーティファクトリハンドリング
サービスの検討 「インシデント事前対応サービス」	セキュリティ関連情報提供
	脆弱性ハンドリング
	インシデント・セキュリティイベント検知
	技術動向調査
	セキュリティ監査・査定
	セキュリティツールの管理
	セキュリティツールの開発
サービスの検討 セキュリティ品質向上サービス	リスク評価分析
	事業継続性、災害復旧計画作成・改変
	セキュリティコンサルティング
	セキュリティ教育・トレーニング・啓発
	製品評価・認定
社内体制の検討	
社外連携の検討	
リソースの検討	人的リソース
	設備リソース
比較検討	
構築スケジュール検討	
構築	経営層の承認とリソース確保
	社内調整の実施
	サービス対象の説明
	体制整備
	必要文書の作成
シミュレーション	
実施	周知
	サービス対象への提供
	社外連携体制の確立
検証(再検証)	

図9：シーサートの構築プロセス

4.2. 「予算がない」

セキュリティ対策はお金をかければいくらでも実施できることはあり、すべてにおいて最高峰の組織的、人的、物理的、技術的セキュリティ対策を行うことは不可能です。また組織規模や経営層の意識によっても投資できる予算は組織によって異なります。昨今シーサートを構築した組織においてもシーサート活動を行うための予算がない、少ないといった声も聞こえています。

シーサートは情報システム管理部門やセキュリティ対策部門などが中心で、部署横断的ではない(または組織全体にシーサートを理解されていない)シーサートも存在し、シーサート活動が不透明になっている組織が見られます。シーサート活動を牽引する限られた組織は必要ですが、その限られた組織で予算のやりくりを余儀なくされてしまうケースも少なくはありません。

シーサートはもはや「組織になくてはならないもの」と言っても過言ではなく、社会的な責任を果たすという意味においても必要となっています。またシーサートはインシデントに対して適切に対応が行うことができるといった組織のイメージを向上させる効果ももたらし、マーケティング活動の一環とも捉えることが可能です。

つまり情報システム管理部門やセキュリティ対策部門などの限られた部門で予算確保や運営を行うのではなく、CSR活動を行う部門やマーケティング(セールス含む)活動を行う部門においても予算を確保し、シーサートの活動を支援する必要があります。人材だけではなく財源も部署横断的になるように検討していきましょう。

もし部署横断的な予算確保が難しいのであれば、経営層の直接的な予算枠を確保するといったことを検討するのも一つです。経営層が本当にシーサートを理解していれば直接的な予算付けを行うことも不可能ではありません。現場がより経営層の理解を深めていく活動を行うとともに、経営層はシーサートの構築面だけではなく、運用面も踏まえた予算について理解し、双方で合意形成を図っていきましょう。

4.3. 「インシデント対応時にしか活躍しない」

「インシデントが発生した時にはシーサートが活躍する」これも間違った考えではないですが、シーサートで大切なのは先に述べた通りレスポンス(Response)ではなくレディネス(Readiness)です。インシデントを発生させないための活動、または発生しても被害を最小化するための準備が極めて重要です。実空間(社会)のインシデントの例で考えてみましょう。

例えば、私たちは大規模な火災を起こさないためにさまざまな準備を行っています。発生時の問い合わせ先(119番)

を覚えておく。消火器を常備する。検知できるように火災報知機を設置する。原因となる火元の対策をする(例:ガスの元栓を閉めるなど)。そして避難訓練を実施するなどです。これらはいずれも火災に備えるための準備です。

サイバー空間においても同様に普段からの活動、事前の準備が重要になります。119番の記憶はインシデントが発生した時に、どこに通報すれば良いのかを理解しておく、問い合わせ先の事前理解です。消火器の常備は万が一、インシデントが発生しても初期対処を行えるようにする事前準備です。火災報知機は早期検知体制の確保、ガスの元栓を閉めるなどは普段からの運用、避難訓練はインシデントが発生しても冷静かつ的確に対処、回避するための準備です。いずれも準備が大切なことが理解できます。

重複しますが、サイバー空間も同様にレスポンス(Response)ではなくレディネス(Readiness)の視点に重きを置き、インシデントを発生させないようにするための事前対処をシーサート活動で実施することが重要です。

4.4. 「日本シーサート協議会に加盟したから一人前のシーサート」

日本シーサート協議会は各組織で構築したシーサートを一人前のシーサートと認めるための団体ではありません。むしろ加盟はスタートラインに立ったに過ぎず、いかに加盟組織との情報連携などを行っていくのかを検討し、実行していくことが大切になります。

現在、日本シーサート協議会には18のワーキンググループが存在し、各ワーキンググループで活発な議論や成果物の発表が行われています。例えば各組織で発生したインシデントを共有し合い、自組織への活用や対応のアドバイスなどを行うワーキンググループや、収集した海外の情報を共有し合い、組織内への報告方法・テンプレートを検討するワーキンググループなど活動はさまざまです。また昨今では同業種・業態のシーサート間においてインシデント情報の共有をはじめとした連携強化が行われるなど、日本シーサート協議会という「場」を活用した活動が見られます。一方で、シーサートを一人前と判断するための評価手法が必要であることも認識しており、既に日本シーサート協議会ではその検討も開始しています。

日本シーサート協議会への加盟はシーサート活動の一つに過ぎず、ゴールではなくスタートであることを、未加入の組織も加入済みの組織も理解しておきましょう。

4.5. 「コンスティチュエンシー(活動範囲)が拡がらない」

シーサートは最初から組織全体の活動範囲とすることは難しく、まずは対応可能な範囲からシーサートを設置しようと述べました。述べた内容に相違はないですが、シーサートを構築するのであれば、設置したシーサートを今後どのように発展させていくのか、すなわち組織全体の活動範囲となるためにはどうすれば良いのか、スモールスタートといえども中長期の計画も検討しておくべきです。

例えば情報系と言われる業務関連のシステムと、重要インフラ事業者に見られる制御系と言われるシステムでは歴史、概念、運用方法等が大きく異なります。そのため情報セキュリティ最高責任者(CISO)が情報系、制御系いずれにも存在するケースなどもあります。情報系を優先してシーサートを構築すると後に制御系を含めた組織全体としてのシーサートを構築するのが難しいような組織も見られます。このような場合にも経営層(者)の意識が重要で、直接的な指示を出す必要があります。インシデントが発生した場合、より深く頭を下げなくて済むよう、経営層(者)も直接的にシーサート構築や活動範囲の拡大に向けた動きの指示・支援などを行いましょう。

◆ 5.これからのシーサートを考える

これだけシーサートという言葉が新聞や雑誌、政府機関が公開している文書などに記述されている昨今において、シーサートの設置が進んでいることは日本シーサート協議会の加盟数から見ても明らかです。まだまだシーサートは増えていく必要があり、日本シーサート協議会としても加盟組織数の目標を約3,000と定めています。しかし、数の追及も必要ですが、今後必要なのはシーサートの「質」の追及です。現在、シーサートは百社百様あると言われていますが、定義が必要な四つの要素や四つの機能が適切に構築され機能しているのか、また事前対処(Readiness)を適切に考慮された体制になっているのかなど、シーサートを見極めていく段階に入っていると考えます。

日本シーサート協議会ではシーサート構築のガイドである「CSIRTスタータキット」や必要な人材やシーサートの役割を定義した「CSIRT人材の定義と確保」などを公開しています。またシーサートを適切に評価できるための評価手法の検討や、組織において必要な訓練や演習の在り方、情報システムに存在するさまざまなログの分析手法の共有や検討など、多様な議論をワーキンググループの活動を通じて実施しています。

今後もさまざまな「場」を提供し、日本のさらなるセキュリティ向上に貢献してまいります。一日も早く日本シーサート協議会の「仲間」として皆様にお会いできる日を楽しみにしています。

(日本シーサート協議会 副運営委員長 萩原健太)