xSIRT（Security Incident Response Team）について

○経済社会のデジタル化の進展に伴い、業務等のデジタル化、製品等のネットワーク接続、デジタルサービスの開発、他サービスとの連携などが増加する一方、そうした変化を狙うサイバー攻撃もみられています。

このため、DX with Cybersecurityを推進するためには、迅速で柔軟な開発・対処、新たなリスクに対応した監視・対処のプラクティスが必要となると考えられます。

○具体的には、サイバーセキュリティ対策を設計段階から織り込みつつ、迅速で柔軟な開発を可能とする体制（部署間連携や人材登用、プロセス整理を含む）や効率的な影響分析、組織をまたいだ連携などが考えられます。

○実際に、様々な企業において、企業内の情報システムを対象とするCSIRTに限らず、製品・サービスを対象としてインシデント対応を行う組織（xSIRT: Security Incident Response Team）が立ち上げられています。

（対象と組織呼称の関係の例）
- CSIRT　　：企業内の情報システム
- PSIRT　　：顧客に販売されネットワークに接続された製品
- DSIRT/SSIRT　：顧客が利用するデジタルサービス

○このような機能の導入に当たり参考としていただくべく、次ページには各xSIRTの特徴的な機能や規模感等を取りまとめています。

＜参考＞xSIRTごとの特徴

xSIRT	対象	主な活動	設置部署	規模感
PSIRT （Product Security Incident Response Team）	PSIRTは、顧客に販売されネットワークに接続された製品および顧客の安全確保・情報保護を対象として、セキュリティ・インシデントに対処する。 ここでいう製品にはハードウェア製品とソフトウェア製品がある。	インシデントの検知や受付を経て、 CSIRTが設置されている場合はCSIRTと分担・連携しつつ、製品に係る原因分析や影響範囲の調査、問題への対応、復旧を行う。 更に、製品の顧客へのパッチ提供や対策支援等の脆弱性対応なども行う。 活動の際には、製品開発や品質管理を担う部署と協調することが求められる。	事業部門ごとに、製品開発や品質管理を担う部署と連携する部署として設置されることが多い。 その際、製品開発プロセスにおけるセキュリティ・バイ・デザインの管理を兼ねる場合もある。また、複数の事業部門がある場合は、全組織的に統括的なPSIRTが置かれる場合がある。	事業部門毎にPSIRTが設置され、それぞれに数名の人員を配置することがみられるが、組織によっては他の業務と兼務となる場合もある。 全組織的に統括的なPSIRTでは、事業部門とは別途、数名程度配置することがみられる。
DSIRT/ SSIRT （Digital Service Security Incident Response Team）	Service SIRTは、顧客が利用するデジタル・サービスの継続的提供・品質維持および顧客の資産保護・情報保護を対象として、セキュリティ・インシデントに対処する。	インシデントの検知や受付を経て、 デジタル・サービスを提供する事業部門が原因分析や影響範囲の調査、問題への対応、復旧を行うが、Service SIRTは、各事業部門を横断的・俯瞰的に確認し、事業部門に対して実務的な助言・支援を行う。 主に、サービス企画時のサービスリスク分析、サービスの不正を検知する監視ロジックの設計・更新支援、大規模サービスインシデント発生時の対応が挙げられる。 全組織的なCSIRTがある場合は必要に応じ連携する。	デジタル・サービスを提供する事業部門と横並びの独立部署、もしくは、各事業部門のセキュリティ担当を集めたバーチャル組織として設置されることが多い。	一部の先進的な取組を行う企業で設置がみられる。 顧客に提供するデジタル・サービスが複数でも類似する場合には、人員の増加は少ないと考えられる。
（参考）CSIRT（組織内CSIRT） （Computer Security Incident Response Team）	組織内CSIRTは、組織内の業務運営に用いるコンピュータやネットワークといった情報システムの安定稼働とそこで取り扱われる情報保護を対象として、セキュリティ・インシデントに対処する。 ※全組織的なセキュリティ統括機能が設置される場合はその機能の1つとして上記を担う。	インシデントの検知や受付を経て、その原因分析や影響範囲の調査、問題への対応、復旧を行う。あるいは、そのための技術支援を関係部署に提供する。 経営層や関係部署との連絡調整や情報共有なども行う。 平常時には、パッチ適用などの脆弱性対応、従業員への普及啓発・注意喚起なども担う。	情報システム部門やIT部門と呼ばれる部署に設置されることが多い。 なお、インシデントの検知や深堀分析をSOC (Security Operation Center)と呼ばれる専門組織が担い、CSIRTと連携する場合が多い。自組織CSIRTと外部の専門組織の役割分担は組織によって異なる。	大きな組織では、数名から十数名の人員を配置することが多くみられる。一方、ユーザ企業では組織によっては他の業務と兼務となる場合が多くみられる。 各部署にセキュリティ対応力が備わっている場合、問題に直接対応する必要がないため、組織内CSIRTの規模は小さくなる。

注1：以上は各xSIRTと呼ばれるものの特徴的な機能や規模感等を中心に整理を試みたものであり、企業・組織内にそれぞれ別個に体制として設ける必要性を示すものではありません。また、体制の検討にあたっては、近年、デジタル技術の活用の進展に伴い、全社的なリスクマネジメントが必要となってきていることにも留意が必要です。

注2：上記のほか、製造業などにおいては自社の工場や生産ラインの安定稼働や作業員の安全確保の為に、サイバー攻撃の監視・対処を行うFSIRT(Factory Security Incident Response Team)と呼ばれる組織が生産管理部門に設置される場合もあります。

（出典）「DX with Cybersecurity実践に向けた人材の確保、育成、活躍促進に係る主な政策課題と方向性」（2021年6月2日 サイバーセキュリティ戦略本部 普及啓発・人材育成専門調査会） 一部加工

＜参考＞「サイバーセキュリティ戦略」（2021年9月28日閣議決定）抜粋

４．４．２　人材の確保、育成、活躍促進

（１）「DX with Cybersecurity」に必要な人材に係る環境整備

②企業・組織内での機能構築、人材の流動性・マッチングに関する取組

今後、業務等のデジタル化、製品等のネットワーク接続、デジタルサービスの開発や他のサービスとの連携などが増加する中で、迅速で柔軟な開発・対処、新たなリスクに対応した監視・対処のプラクティスが必要となる。特に、前者の実践に当たっては「セキュリティ・バイ・デザイン」の考え方の重要性も一層増し、企画部門や開発運用部門と企業・組織内のセキュリティ機能との連携・協働が一層重要となると考えられる。一方で、こうした機能の構築や普及に向けては、必ずしも参照できる導入事例や人材の蓄積が十分とは言えないのも事実である。

また、人材の活躍の場という観点では、コロナ禍への対応の結果として雇用環境の変化や労働時間管理のあり方の明確化等を踏まえ、兼業・副業といった柔軟な雇用形態の活用の機会が今後増していくと考えられる。また、デジタル改革の動きを踏まえ、国の機関のみならず、地方自治体を含め、行政分野における業務改革を含むデジタル化関連業務における人材需要が今後増していくと考えられる。社会全体で「DX with Cybersecurity」を推進していくためには、働き方や雇用形態の多様化、デジタル改革の推進を機会としてIT・セキュリティ人材の流動性・マッチング機会の促進が図られるための環境整備が必要である。

したがって、これらの動向や人材の偏在等を考慮しつつ、企業・組織内での機能構築やIT・セキュリティ人材の確保・育成に関するプラクティス実践の促進に向け、人材ニーズに係る実態把握とあわせ、実際のインシデントを踏まえた普及啓発や、参考となる手引き資料の活用促進、人材の活躍等の先進事例の収集・整備、ポータルサイト等を通じた積極的な発信、学び直しの機会の提供に取り組む。

また、特に地域・中小企業においてセキュリティ人材の不足が顕著であるところ、地域における「共助」の取組や、産業界と教育機関との連携促進・エコシステム構築を通じ、プラクティスの実践に当たって参考となるノウハウやネットワークの提供を行う。