情報セキュリティマネジメント試験合格講座 午後試験対策 07

- CSIRT の構築

1. CSIRT（Computer Security Incident Response Team）
サイバーセキュリティに係るインシデントなどに対処する組織であり、一般的には、サイバーセキュリティに関する窓口機能を有する場合が多くなっている。対外窓口には、自組織の Web サイトの脆弱性に関して外部からの通報を受ける窓口と、他の CSIRT と〔 連 〕する窓口の双方が含まれる。

サイバーセキュリティに係るインシデントは〔 攻撃 〕や Web サーバの改ざんなど多様であり、連絡や〔 連 〕を行う相手も多様であるため、こうした対処を行うチームや機能を被害が発生してから構築しようとしても不可能である。そのため、被害がないうちから構築しておくことが重要である。

2. CSIRT の構築方法
近年 CSIRT の重要性が強調されているのは、適切なサイバーセキュリティ対策を講じているような組織でも、サイバー攻撃の被害を完全に防ぐことは困難な状況であるという認識が広まりつつあるためである。以下では、CSIRT 構築に向けて、組織内で検討、実施すべき事項の例を示している。

3. 組織内の状況把握
CSIRT の体制をどのようにするかの検討に先立ち、関係者への聞き取り調査などにより、次のような状況を把握しておく必要がある。

(1) 各部門の主要業務のフローとサイバー攻撃による影響の可能性
(2) 部門間での対策状況や脅威情報の共有および連携の状況
(3) 各部門の〔 者 〕および〔 ソン 〕
(4) インシデント対応に関する規則類

4. 経営層への提案と承認の獲得
CSIRT の構築や運用には、インシデントが発生した際に、原因追求や被害状況の調査のために、部門横断的な調整が必要になるなどの理由から、〔 〕の理解と協力が必要不可欠である。

しかし、CSIRT の構築や運用には当然ながら費用がかかるため、「インシデントが起こらないようにすれば、そのような組織は不要ではないか」と考える経営層もいるかもしれない。

サイバー攻撃で大きな被害が生じた経験がない組織であれば、経営層に CSIRT 設立に関する承認を得るのは容易でない場合がある。

そこで、〔　　〕というロジックなどを用いながら、経営層の理解と協力を得られるように提案するとよいであろう。

経営層向けの説明資料を作るために、次のような作業を行うことが考えられる。

- ✓ CSIRT の必要性を訴求する材料集め
  サイバー攻撃に関するニュースや、セキュリティベンダが作成した被害にあった企業の調査レポートなどを利用し、他社におけるインシデントの件数、インシデント発生による被害や財務への影響を示す統計データなどを提示する。

- ✓ CSIRT のメリットを訴求する材料集め
  CSIRT によってインシデント発生時の早期対応だけではなく、インシデント発生時のリスク低減が見込めることの説明、CSIRT によってインシデント収束までの期間短縮が想定でき、それにより財務への影響低減が見込めることの説明、〔　　〕ことを対外的に訴求することによる企業イメージの向上の説明などを提示する。

5. CSIRT 構築作業チームの設置
   CSIRT の構築を担当するメンバーを集める。前項の状況把握を通じてインシデント対応のスキルや能力を有する人材を発掘すると同時に、新たな組織を構築する際に調整が必要な部門へ働きかけを行うことも重要である。

   関係部門としては、情報セキュリティ部門のほか、情報システムの運用や保守部門、リスクマネジメント部門、〔　広　　〕部門などが関係する。こうした働きかけを行う際には、CISO などが主導していることをアピールすることで、CSIRT の存在を周知できることから各部門の情報を得られやすく、スムーズに調整できる点でも有効である。

6. CSIRT の設計

組織にとって最適な CSIRT の形態は、組織の特徴によって様々である。そこで、CSIRT 構築作業チーム内での議論を通じて、構築する CSIRT における以下の内容を明らかにした上で、文書として取りまとめる。

(1) CSIRT の目的(組織における役割)
(2) 提供するサービス(インシデントマネジメント、連絡窓口、監視業務)
(3) サービスのレベル(24 時間体制、部門間の調整機能のみ)
(4) サービスの提供対象(活動範囲)
(5) サービスの提供主体(自社要員が対応、専属／兼務、外部サービス利用)
(6) 組織内での権限(〔　　ク 〕との接続を切る権限を持つ)
(7) 新たに策定すべき規則など
(8) 運営上のポイント(特に重視する部門や事業など)

7. 予算・人員の確保

CSIRT 運営に必要な要員と費用を明らかにする。このとき、〔　　〕とインシデント対応時の双方についての試算が必要である。インシデント対応についても、小規模なものと大規模なものとでは費用が変わってくるため、複数のシナリオで試算する必要がある。

8. CSIRT の設計で検討すべき役割・機能・権限

CSIRT を構築する場合には、どのような役割や機能をどのようなチームで実施するのかなどによって、様々な実現方法が存在する。

組織内の情報システム部門が 24 時間の運用・監視・障害対応サービスを提供しているのであれば、CSIRT が新たに同様の機能を担う必要は無く、CSIRT が担うべき機能は〔　　〕としての役割が主体になる可能性がある。一方、各部門に IT 関連のトラブル対応のスキルをもった要員がほとんどいないような場合は、CSIRT が障害対応機能を兼務することで、効率的な IT 活用ができる可能性がある。このように、CSIRT が担うべき役割や機能は組織の状況によって様々である。同様に権限についても、サイバー攻撃が行われた場合に、CSIRT が全社一律の外部とのネットワークの接続の遮断などを行うことに難色を示す部門が出てくる可能性がある一方、セキュリティ上の判断は CSIRT に任せたいという場合もあり得る。いずれにせよ組織にあった運営方針を定めることが重要である。

9. CSIRT の組織上の位置付け

CSIRT を実際の部門とするのではなく、各部門との兼務によるメンバーで構成される〔　　〕組織として運営されている例もある。既存の情報システム管理部門やリスク管理部門との関係についても色々なパターンがあり、部門内の一部として CSIRT が運営されていることもある。組織内での CSIRT に期待される役割に応じて、最適な位置付けについて検討することが望まれる。

10. 連絡窓口

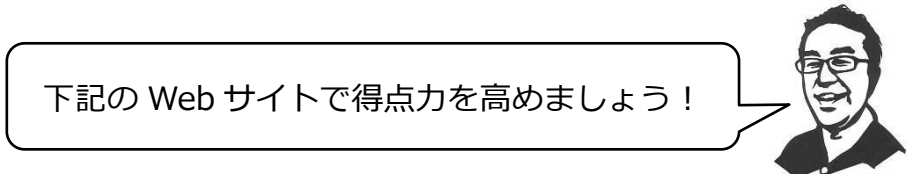
インシデント発生時に、CSIRT は組織内および組織外との連絡窓口の機能を果たすことも求められる。ただし、利用者からの問合せなどの対応まで行うと、本来のインシデント対応業務への対応ができなくなることも懸念される。インシデント発生時の窓口機能として、以下のような役割分担を行うことが考えられる。

(1) CSIRT：監督官庁などへの報告、グループ企業や取引先などへの連絡、経営層への報告、社内各部門へのアナウンス
(2) 広報部門：マスコミ取材対応
(3) サポートセンタ：顧客からの取い合わせへの対応
(4) 社内ヘルプデスク：従業員からの問合せ対応

11. 幹部との連絡体制

CISO などが CSIRT の指揮・命令系統のトップを兼ねることがある。この場合は CISO などへ通常のルートで報告することになるが、CISO などが直接 CSIRT の指揮・命令系統を有しない場合は CISO などと緊密な情報共有ができる体制を構築しておくことが重要である。最高情報責任者（〔 C　　〕）についても、社内システムや対外的な業務用サービスの提供に責任を負っていることもあり、緊密な関係を維持する必要がある。こうした責任者以外の役員については、CISO などから連絡する体制や、CSIRT から直接連絡する体制などを、組織の事情に応じて構築する。

出典：IPA「サイバーセキュリティ経営ガイドライン」



- ✓ 翔泳社「情報セキュリティマネジメント要点整理＆予想問題集」
- ✓ 情報セキュリティマネジメント試験合格講座　http://rakupass.com/security/