JNSA 2014年度活動報告会
社会活動部会（BoF）

IT環境の変化に対応していく
インシデント対応の模索

パネリスト資料

日本アイ・ビー・エム株式会社
セキュリティ・サービス
2015年6月9日
徳田敏文

CSIRTに求められるもの

事業継続際し技術に加え組織的対処の必要性が向上しており、対応機能の集約化が求められる。

【事故前提の社会】	【組織を取り巻く環境変化】
● 事前対策だけで、インシデントの発生を完全に防ぐことは困難になっている。	● インシデント発生時の被害を最小限に抑え、一刻も早い復旧手段を整備しておく必要がある。
● 情報資産に係るリスクは多様化しており、システム管理部門の判断だけでは対処が困難になっている。	● 包括的な情報セキュリティ対策を実施するには、経営層を含め、組織的な活動が必要になってきている。

CSIRTの役割とは

組織で発生したインシデントに対応する基本的な役割の他、過去の事故や潜在する問題点の調査・分析を行い、インシデント傾向を把握する事が重要となる。

インシデントとは“組織が望んでいない状態に至る可能性がある兆候、全て“を指す
（ISO/IEC18044 Information security incident management）

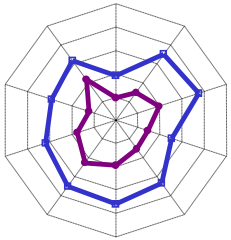
調査

問題点の洗い出し

分析

対策を検討すべきインシデントの明確化

一般的なインシデント事例の把握
組織内で、過去に発生した事故の原因、傾向
同業他社で、過去に発生した事故の原因、傾向
組織内で認識されている危険な兆候の把握
予測される問題の洗い出しと傾向把握



CSIRTの活動範囲

CSIRTのあるべき役割は、会社の業務内容やリスクにより異なるため、
経営層や対応対象からの期待を明確にした上で定義する必要があります。

基本的には組織内で発生したインシデントへの対応だが..

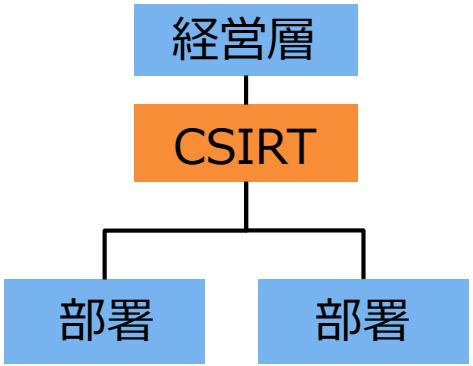
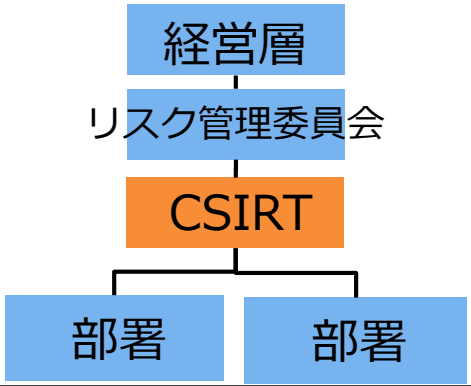
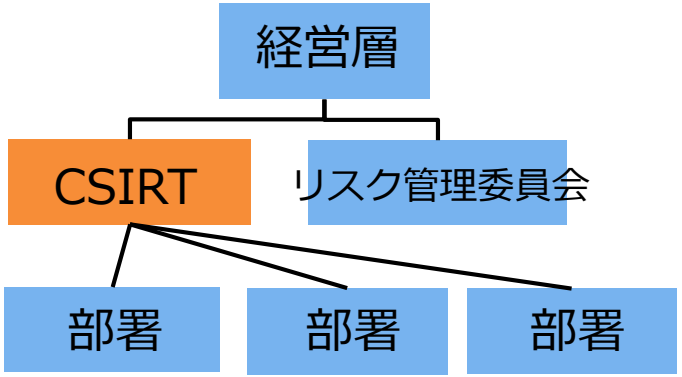
組織内CSIRT

必要な機能は技術的対応か組織的対応か？

既存のIT部門との関係は？

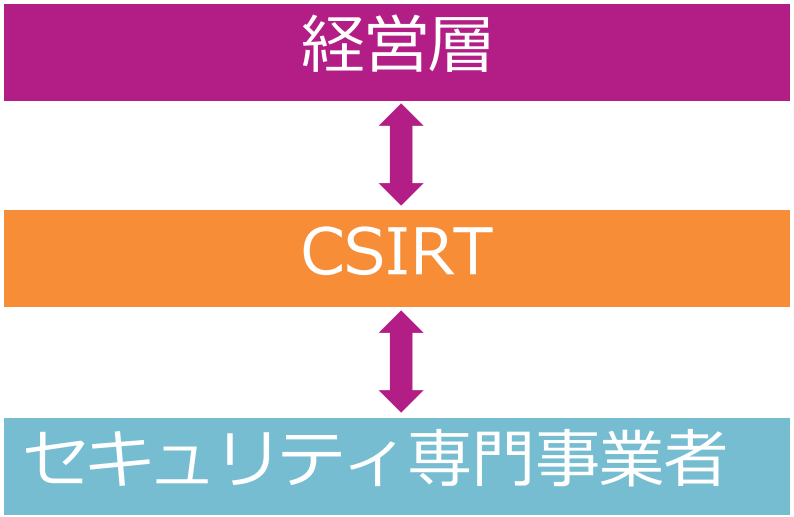
既存のセキュリティ委員会とどう関連づけるか？

CSIRTの組織内での位置付け

経営層直下に設置する	経営層直下のリスク管理委員会の下に設置する	経営層直下に設置しリスク管理委員会と独立させる
		
○利点	経営層への報告が整理されることで、迅速な対応が期待できる。	組織としてのリスクコントロールを専門に扱う委員会の独立により、経営層およびCSIRTの負荷が低減できる。	組織としてのリスクコントロールを専門に扱う委員会の独立により、経営層及びCSIRTの負荷が低減できる。また、柔軟な承認プロセスを設定できる。
×難点	経営層の理解が得られやすいレポート作成など、CSIRTに負荷がかかる。 技術よりは組織を重視する場合に適している	承認プロセスの整備状況により、対策実施までに必要な時間が長くなる場合がある。	職責と権限の定義を誤ると、混乱が発生しやすい。 CSIRTに経営層との間の調整能力が求められる。

経営層に関するセキュリティ・アドバイザーとして

- 新聞等メディアで報道された情報セキュリティ上の問題が自社に影響があるか否かすぐに知りたい
- 他社で発生したセキュリティ事故が自社で発生する可能性があるか知りたい
- 事故発生を予防するための適切な施策は何か知りたい



◎経営層をサポート

効果的に専門家や外部事業者を活用する

◎的確・適切な業務委託と監督
◎成果の評価

ベンダーから見たCSIRT組織に関する課題点

- セキュリティ事故が発生する前提で組織されていますか
  - ✓ 事故発生時の対応方針や優先順位の決定者、報告フローは決まっていますか
- 経営層をサポートできる人員が組織されていますか
  - ✓ 対応方針を決めても経営層の理解ひとつで白紙に戻る事がありませんか
- インシデント発生の前と後で、役割・機能が明確になっていますか