【FISC サイバーセキュリティ参考情報 No.7】
平成 27 年 12 月 11 日
公益財団法人　金融情報システムセンター

組織内 CSIRT の整備

Ⅰ 問合せ内容

組織内 CSIRT はどのように整備すればよいか。どこから何をすればよいのか定まらない。

Ⅱ 関連する FISC 安全対策基準

基準番号	小項目	項番	解説
【運 113】	サイバー攻撃対応態勢を整備すること。	2	未然防止策・事前対策には、以下のような例がある。
【技 43】	外部ネットワークからの不正侵入防止機能を設けること。	参考 4	サイバー攻撃対応態勢の整備のため、組織内 CSIRT（Computer Security Incident Response Team）を整備することは、迅速かつ適切な対応や、収集した情報の一元化による早期警戒体制の構築、及び関係者間での情報共有に有効と考えられる。（以下略）

Ⅲ 留意点及び参考情報

平成 27 年６月に発刊した『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版追補改訂）』において、サイバーセキュリティに関する基準を抜本的に強化しております。基準【運 113】「サイバー攻撃対応態勢を整備すること。」の【項番２】、及び、基準【技 43】（参考４）に、組織内 CSIRT の整備に関する記載がございますのでご参照ください。

また、当センターでは、サイバーセキュリティに関する国内・海外の動向について、継続的に調査研究活動を進めております。この調査研究活動で得られた「組織内 CSIRT の整備」に関する情報については、当センターが主催する「地区別セミナー」「訪問サービス」等の講演活動や、「FISC サイバーセキュリティ参考情報」を通じて、継続的に情報還元して参ります。