金情総　29－56
平成 29 年 5 月 31 日
公益財団法人　金融情報システムセンター

『金融機関等におけるコンティンジェンシープラン策定のための手引書（第３版追補３）』の発刊について

当センターでは、『金融機関等におけるコンティンジェンシープラン策定のための手引書（第３版追補３）』を発刊いたしました。

『金融機関等におけるコンティンジェンシープラン策定のための手引書』（以下、『コンテ手引書』という）は、金融機関等がコンティンジェンシープランを策定、見直しを行う際に参考とすることを目的として発刊しており、金融機関等が個々の経営判断によりコンティンジェンシープランを策定する際の基本的な手順やポイント等を記載しております。

昨今、サイバー攻撃による被害が拡大し、その攻撃手口が高度化・巧妙化しているため、金融機関等ではサイバー攻撃を想定したコンティンジェンシープランの策定について関心が高まっております。これまでの『コンテ手引書』にもサイバー攻撃リスクに関する記載があるものの、現状のサイバー攻撃リスクへの対応として、十分とは言えない状態となっておりました。今回の『コンテ手引書』の改訂では、このような問題意識のもと、サイバー攻撃リスクに関する記載について見直しを行いました。

※改訂のポイントについては、別紙をご参照ください。

＜本件に関する問い合わせ＞
公益財団法人　金融情報システムセンター　監査安全部　栗田、萩原、樽井
（03-5542-6054）

公益財団法人　金融情報システムセンター（FISC）　https://www.fisc.or.jp

別紙

○改訂のポイント

自然災害と異なるサイバー攻撃リスクの特性として、被害の全容や原因を特定・把握するまでに時間を要することや、初めは小さいと思われた被害が次第に深刻な被害へ発展することがあるため、サイバー攻撃の発生を早期に検知することや、態勢及び対応手順を事前に整備することが重要となる。そのため、これまでの『コンテ手引書』で記載していた事後の対策に加え、態勢整備や平時における運用、インシデント発生時の対応についても記載している。

・態勢整備

金融機関等が全社的かつ主体的にサイバー攻撃への対応に取り組む必要性があることから、経営層がリーダーシップを発揮し対策を推進することや、外部委託先を含めた態勢整備を行うことなどについて記載した。

・平時の運用

サイバー攻撃による被害拡大防止やサイバー攻撃への迅速な対応を行うため、サイバー攻撃を早期に検知することや攻撃情報等の収集・共有など、主にインシデント対応組織が、平時の運用を行うにあたっての考慮事項を記載した。

・インシデントレスポンス

金融機関等がサイバー攻撃対応手順を整備する際に、必要な対応や考慮事項として、インシデントが発生した際の原因の調査・分析や被害拡大防止、復旧などのプロセスについて記載した。

以　上