ＩＳＩＳＳ通信

Ishikawa Small and Medium Businesses Information Security Support News

Ｈ３０．１
Ｖｏｌ．１７

経営者が中心となった サイバーセキュリティ対策を!!

会社をサイバー攻撃から守るためには、経営者がリーダーシップを取ってサイバーセキュリティ対策を推進する必要があります。その指針となる「サイバーセキュリティ経営ガイドライン」が、平成２９年１１月、Ver2.0に改訂され、経済産業省から公表されたことに伴い、改訂された「サイバーセキュリティ経営の重要１０項目」のほか、「経営者が認識すべき３原則」の各項目についてご紹介します。

○ 経営者が認識すべき3原則

１　経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要

２　自社は勿論のこと、ビジネスパートナーや委託先も含めたサプライチェーンに対するセキュリティ対策が必要

３　平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策に係る情報開示など、関係者との適切なコミュニケーションが必要

○ サイバーセキュリティ経営の重要10項目

＜経営者がリーダーシップをとったセキュリティ対策の推進＞

（サイバーセキュリティリスクの管理体制の構築）

１　サイバーセキュリティリスクの認識、組織全体での対応方針の策定

２　サイバーセキュリティリスク管理体制の構築

３　サイバーセキュリティ対策のための資源（予算、人材等）確保

（サイバーセキュリティリスクの特定と対策の実装）

４　サイバーセキュリティリスクの把握とリスク対応に関する計画の策定

５　サイバーセキュリティリスクに対応するための仕組みの構築

６　サイバーセキュリティ対策におけるPDCAサイクルの実施

（インシデント発生に備えた体制構築）

７　インシデント発生時の緊急対応体制の整備

８　インシデントによる被害に備えた復旧体制の整備

＜サプライチェーンセキュリティ対策の推進＞

９　ビジネスパートナーや委託先等を含めたサプライチェーン全体の対策及び状況把握

＜ステークホルダーを含めた関係者とのコミュニケーションの推進＞

１０　情報共有活動への参加を通じた攻撃情報の入手とその有効活用及び提供

※　「サイバーセキュリティ経営ガイドライン Ver2.0」の詳細は、経済産業省の Web サイトをご参照ください。

サイバー犯罪（インターネットに関する犯罪）の通報やご相談は・・・

石川県警察本部生活環境課サイバー犯罪対策室

076－225－0110　　cyber@police.pref.ishikawa.lg.jp