経済産業省
Ministry of Economy, Trade and Industry

企業における
情報セキュリティガバナンスの確立促進

資料11

政策の背景＆情報セキュリティ確保のための施策

経済産業省
Ministry of Economy, Trade and Industry

我が国産業の競争力強化	ＩＴを基盤とした情報の利活用は競争力の源泉
競争力強化を阻害する情報セキュリティに係る要因	しかし、<u>企業の情報資産に対する脅威は増大の一途</u>　⇒　事件・事故が多数発生
企業の情報セキュリティ強化は情報セキュリティ基本計画に位置づけ	【 第二次情報セキュリティ基本計画 】（計画期間　2009年度～2011年度） （2009年2月 情報セキュリティ政策会議（議長：内閣官房長官）にて決定） ● 企業における情報セキュリティ対策の推進は、政府・地方公共団体、重要インフラ、個人における対策とともに<u>４本柱の一つ</u>。 ● 「政府は企業における情報セキュリティ対策の実施状況を世界トップクラスの水準にすることを目指して最大限の努力を行う」 ● 企業に係る第一の情報セキュリティ政策として「情報セキュリティガバナンスの経営の一環としての認識の定着とそれに応えられるツールの存在」を位置づけ。

経済産業省では、企業の情報セキュリティの確立を支援するため、情報セキュリティマネジメントシステム（ISMS）適合性評価制度、情報セキュリティ監査制度、情報セキュリティ対策ベンチマーク等の整備を行ってきたところ

経済産業省今回の取組

企業の情報セキュリティを確立する上で解決されていない課題

（１）経営層が情報セキュリティの観点から何をすべきか不明確
（２）ＩＳＭＳを実装しようとしても法令との関係が分からない
（３）業務委託先での情報漏えい対策等の実施方策が分かりにくい
（４）実施状況の「見える化」のため信頼できる民間格付機関が必要

課題に対応して策定したガイダンス類

（１）情報セキュリティガバナンス導入ガイダンス
（２）情報セキュリティ関連法令の要求事項集
（３）アウトソーシング・セキュリティ対策ガイダンス
（４）情報セキュリティ格付機関の規律に関する基準

今回策定したガイダンス類の概要

経済産業省
Ministry of Economy, Trade and Industry

●情報セキュリティガバナンス導入ガイダンス

情報資産の利活用と、それを支えるリスク管理の一環としての情報セキュリティ対策は重要な経営課題。情報セキュリティの観点からガバナンスの仕組みを構築・運用する手法として以下のモデルを提示。

①経営者が情報セキュリティに係る**全体方針を決定**し実施責任者として**CISO（＊）を任命**
②CISOは組織内の情報セキュリティの状況を**モニタリング・報告する仕組みを構築**
③監査役は**情報セキュリティガバナンスの有効性を評価**、状況に応じて経営者に改善を勧告
④経営者は情報セキュリティの取組を利害関係者に開示、評価を受ける仕組みを構築（**情報セキュリティ報告書**）

●情報セキュリティ関連法令の要求事項集

社会からの要請として法令遵守（コンプライアンス）体制の確立を行うことは企業の責務。会社法、個人情報保護法、不正競争防止法、労働法等の法令を遵守し、かつ、情報セキュリティの「適切性」を確保するため、情報セキュリティ確保の観点から、これら法令の要求事項を提示。

●アウトソーシング・セキュリティ対策ガイダンス

拡大する企業間取引に際して企業間を往来する情報の適正な管理をどのようにおこなうべきかの指針を示すべく、アウトソーシングに係る情報セキュリティを確保するための方策について提示。

●情報セキュリティ格付機関の規律に関する基準

情報セキュリティ格付けを行う機関における客観的な公平性を担保するための要件を「情報セキュリティ格付制度に対する規律」としてとりまとめ。

※上記のガイダンス類は、５月１日から、パブリックコメント意見募集中。

情報セキュリティガバナンス確立促進政策

経済産業省
Ministry of Economy, Trade and Industry

内閣官房 情報セキュリティセンター	経済産業省	（独）情報処理推進機構
政府全体の情報セキュリティ戦略である第二次情報セキュリティ基本計画に「企業の情報セキュリティ」位置付け	制度、ガイドライン等の整備	経済産業省が整備する各種ガイダンス類を具体的に適用するための手順書を策定、中小企業への普及推進、情報セキュリティ対策ベンチマークの普及、等

民間情報セキュリティ格付け機関	日本セキュリティ監査協会等	（財）日本情報処理開発協会	ISO/IEC SC27（情報セキュリティ）	日本商工会議所 全国商工会連合会
情報セキュリティ格付けの促進	セキュリティ監査の促進、企業監査役関連組織との連携	情報セキュリティガバナンスとISMS認証をセット化	策定したガイダンス等の国際標準化に向けた取り組み	中小企業の情報セキュリティ対策の促進

企業全般に働きかけ