サイバー攻撃・内部不正対策のトレンド

株式会社ソリトンシステムズ

Rev003-1602

サイバー攻撃と内部不正

- **2014年　内部不正による情報漏洩**
  - 3504万件の顧客情報漏洩
  - 名簿業者、不正競争防止、多重派遣…
  - 役員6人に総額260億円の損害賠償など

- **2015年　サイバー攻撃による情報漏洩**
  - 約125万件の年金番号含む個人情報漏洩
  - 日本の官民をターゲットに攻撃は継続

法整備・ガイドライン改訂

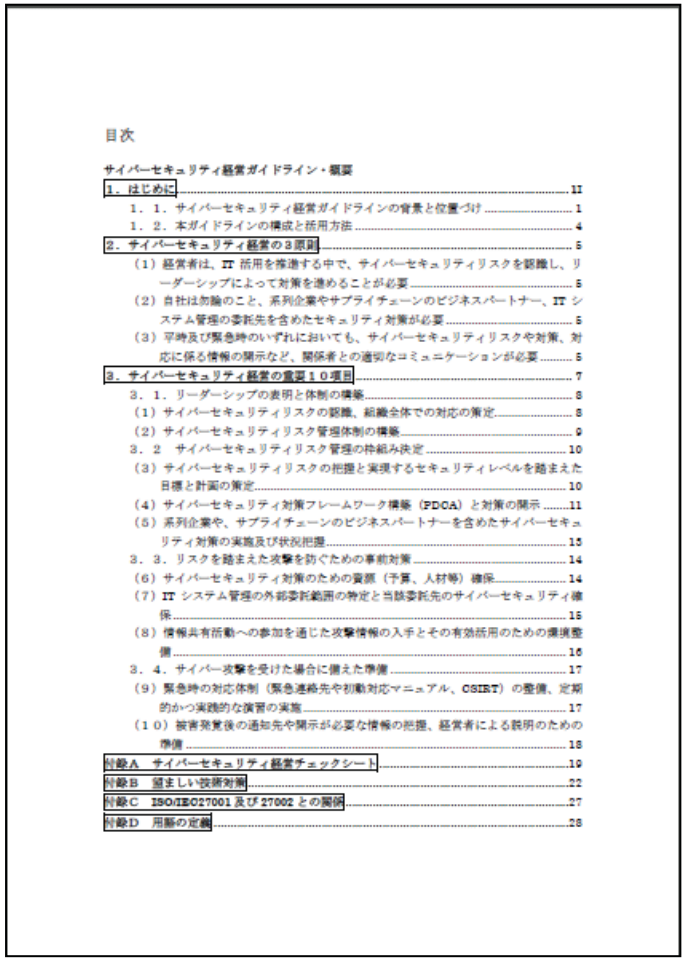
法令・ガイドラインなど	時期	概要	
サイバーセキュリティ基本法	2014.11	国家レベルでサイバーセキュリティを強化する指針	
営業秘密管理指針改定	2015.1	不競法により保護される営業秘密の明確化	
組織における内部不正ガイドライン改訂	2015.3	第三版。ISMSの規格改訂（JIS Q 27001:2014）や営業秘密管理指針の全部改訂への対応など	
金融監督指針の改訂	2015.6	金融安対基準第8版追補改訂にて「運113 サイバー攻撃対応態勢」が追加	 
不正競争防止法の改訂	2015.7	罰則強化、「営業秘密」の立証負担軽減	
個人情報保護法改正	2015.9	マイナンバー見据えての改正 全面施行までに体制強化が求められる	
マイナンバー施行	2015.10	特定個人情報の取扱いに関しての対策が必要	 
サイバーセキュリティ経営ガイドラインV1.0公開	2015.12	サイバー攻撃リスク対処は、経営者の役割	
秘密情報の保護ハンドブック	2016.2	企業の秘密情報の漏洩対策のため経産省が制定	
有価証券報告書への サイバーリスク掲示義務化	2016.？	金融庁は、2016年中に義務化を検討	

「サイバー攻撃対策」と「内部不正対策」は経営課題

 ：サイバー攻撃　  ：内部不正

サイバーセキュリティ経営ガイドライン

- 経産省より2015年12月に公開
- サイバー攻撃対策は経営課題であると明言
- 米国NISTフレームワークをベースに作成されている
- 経営者向け「3原則」と CISO向け「重要10項目」
- 法的拘束力はないが 順守すれば、保険の割引に。 今後、**事実上の順守事項**となる 可能性あり。



目次

http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

※CISO（最高情報セキュリティ責任者）

サイバーセキュリティ経営の3原則

① 経営者は、IT活用を推進する中で、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

- セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい。このため、サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップをとって対策を推進しなければ、企業に影響を与えるリスクが見過ごされてしまう。

② 自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要

- 子会社で発生した問題はもちろんのこと、自社から生産の委託先などの外部に提供した情報がサイバー攻撃により流出してしまうことも大きなリスク要因となる。このため、自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュリティ対策が必要である。

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、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

- ステークホルダー（顧客や株主等）の信頼感を高めるとともに、サイバー攻撃を受けた場合の不信感を抑えるため、平時からのセキュリティ対策に関する情報開示など、関係者との適切なコミュニケーションが必要である。

経営者の同意を得たうえで、具体的な対応策をCISOや情報セキュリティ担当が実施することで、サイバーセキュリティ経営を実現

サイバーセキュリティ経営の重要10項目

経営者は、CISO等に対して、以下の１０項目を指示し、着実に実施させることが必要である。

リーダーシップの表明と体制の構築
(1) サイバーセキュリティリスクの認識、組織全体での対応の策定
(2) サイバーセキュリティリスク管理体制の構築
サイバーセキュリティリスク管理の枠組み決定
(3) サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
(4) サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
(5) 系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握
リスクを踏まえた攻撃を防ぐための事前対策
(6) 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
(7) ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
(8) 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のための環境整備
サイバー攻撃を受けた場合に備えた準備
(9) 緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施
(10) 被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備