情報セキュリティマネジメント試験合格講座 午後試験対策 02

- 経営者の責任の明確化

1. 経営者の責任
   内部不正対策は経営者の責任であり、経営者は基本となる方針を組織内外に示す「基本方針」を策定し、役職員に周知徹底しなければならない。経営者は、「基本方針」に基づき対策の実施のためのリソースが確保されるよう、必要な決定、指示を行わなければならない。

2. どのようなリスクがあるのか？
   経営者が、内部不正対策は自らの責任で行うことの強い意識を持ち、組織の経営戦略または経営方針に照らして、内部不正がもたらす組織運営への影響の把握を行わないと、組織が内部不正対策を行うにあたっての基本方針を定めることが困難となる。そして、経営者がリーダーシップをとり、「基本方針」を策定しないと、社内外における経営責任の所在があいまいになり、実効性のある管理体制の整備が困難となる。

   「基本方針」は経営者の内部不正防止に向けた意志を伝えるものでもあり、策定しないと経営者の意志が役職員に伝わらず、具体的な対策を立てることや役職員に内部不正対策を周知徹底することが困難になる。さらに、経営者が、「基本方針」に基づく対策の実施のために必要なリソース確保のための決定、指示を行わないと、やはり、実効性のある管理体制の整備が困難となる。

3. 対策のポイント
   経営者は、経営戦略または経営方針に照らして、内部不正に起因する組織運営への負の影響を把握した上で、内部不正対策の大枠となる基本方針を策定し、内部不正対策の方向づけを行わなければならない。

   経営者は対策を実効性のあるものとするために、リソース確保のために必要な決定、指示を行い、さらに、実施状況をモニタリング（定期的な報告によって継続的に状況を把握していること）、評価することによって基本方針や組織内リソース配置を定期的に見直していく必要がある。これらについて、経営者は自ら以下の対策を把握し、組織内において責任を持ち、対外的な説明責任を持つ。

(1) 経営戦略または経営方針に照らして、内部不正がもたらす組織運営への影響を把握する。

(2) 基本方針を策定する。

(3) 策定した基本方針を実行するために必要な人材や予算などのリソース確保のための決定を行い、指示する。

(4) 策定した基本方針に照らし合わせ、役職員に内部不正対策を教育などによって周知徹底する。

(5) モニタリングおよび評価の結果をもとに、基本方針や組織内のリソース配分を定期的に見直す。

(6) 重要情報とそれ以外の情報を区別する。さらに、重要情報を事業上の重要度などを考慮していくつかに分類することが望まれる。

(7) 重要情報の区別および分類は、社会背景や事業環境などとともに変化するため、定期的に見直す必要がある。

- 総括責任者の任命と組織横断的な体制構築

4. 総括責任者
経営者が総括責任者の任命、並びに、管理体制および実施策の承認を行い、経営者主導の取り組みであることを組織全体に示さなければならない。総括責任者は、基本方針に則り組織横断的な管理体制を構築しなければならない。

また、実施策を策定しなければならない。ただし、経営者が組織全体に目が届く組織であれば、自ら内部不正対策の実施にあたり、管理体制を必ずしも構築する必要はない。

5. どのようなリスクがあるのか？
経営者が総括責任者の任命および実施する対策を承認しないと、必要な予算や人事を割り当てることが難しいことから、実効的な管理体制の構築が困難になる。

内部不正の対象となる重要情報は組織内の多岐にわたる部門に存在するため、組織横断的な管理体制が構築できないと、組織として効果的・効率的な対策や情報管理ができないだけでなく、対策や情報管理が徹底されない恐れがある。対策や情報管理が徹底されていないと、内部不正が発生してしまう危険が高まる。

6. 対策のポイント

経営者が主導となり内部不正対策を組織内に徹底させるための体制を構築・運用する。具体的には以下のような対策を定めて運用することになる。

(1) 総括責任者には、事業を考慮した実効的で効果的な内部不正対策を実現するために情報セキュリティと経営を理解できる者を任命する。

(2) 総括責任者は、組織横断的な管理体制や関連部門の役割を具体化、明文化し、その役割を徹底させる必要がある。責任部門は総括責任者とともに組織全体での内部不正対策の実施策と実施体制を構築する。事業の規模などに応じ、重要情報の取り扱いに関する専門部署や委員会を設置する。

(3) 組織横断的な管理体制の構築では、総括責任者が対策実施の管理・運営の要員として各部門の部門責任者や担当者などを任命する。

(4) 内部不正対策を組織内に徹底させるための体制の構築にあたっては、部門責任者、担当者などに求められる能力を明確化する必要がある。構築した体制において能力の不足が認められる場合には、能力向上に向けた取り組みの実施や、組織外からの専門家の採用を検討し、役割に応じて必要な知識、ノウハウの習得を図れるように、総括責任者はそれを支援しなければならない。

(5) 組織内で、内部不正防止の管理体制の他、プライバシー保護、危機管理対策、コンプライアンス対策、などの関連の体制を構築する際には、経営者が主導し、それらの間の役割分担や連携の在り方を明確にする。

(6) 重要情報の取り扱いに係る業務が業務委託先にまで及ぶ際には、必要に応じて、業務委託先までを含んだ連携体制を構築する。なお、一般的に、情報の取り扱いに係る業務の外部委託においては、専門的組織に業務を担わせることによる効率化などのメリットが考えられる。

その一方で、内部不正対策の実施においては、リスクが増大する可能性も考えられる。このため、情報の取り扱いに係る業務については、組織内部で行う場合と委託で行う場合のいずれが適切かを効率とリスクのバランスを考えた上で検討していくことが必要である。

✓ 最高責任者
基本方針を策定し、これを取締役会の決議で決定する。また、最高責任者は、企業などの経営を理解し、具体的な対策を実施、推進する役割である総括責任者を任命する。

✓ 総括責任者
経営者の基本方針に基づき組織全体の具体的な管理策の作成および管理策に基づいた対策を実施し、対策状況を確認するとともに、見直しを行う。

✓ CISO（Chief Information Security Officer）
経営層から任命される最高情報セキュリティ責任者であり、企業や組織において情報セキュリティの全体の責任を担う役職。

✓ CPO（Chief Privacy Officer）
経営層から任命される個人情報保護管理者であり、企業や組織において個人データの安全管理に関する責任および権限を有する役職。

✓ 部門責任者
部門規模が大きい場合、各部門から当該部門の責任者として任命される。総括責任者の指示のもと、自らが担当する部門における対策を実施し、対策状況を確認するとともに、見直しを行う。

出典：IPA「組織における内部不正防止ガイドライン」 2017 年 1 月改訂（第 4 版）