



2019年 第8号 ご挨拶

中国子会社での不正事案に関連した適時開示が増えてきています。内部統制の整備は着実に進んでいる一方で、中国では子会社の数は多いものの1社ずつの規模がそれほど大きくないことから、管理のために十分なリソース、費用、時間を掛けることができず、各業務プロセスごとに不正リスクに対する意識をもって「実効性」あるチェックが必ずしもできていないのかもしれませんが、一度、不正が発生すると信用度が著しく失墜し、それを回復するための費用は、その防止策に費やすものより大きくなるばかりでなく、過年度にわたって訂正報告書を作成しなければならなかったり、連結決算発表スケジュールに影響したりと非常に煩雑な作業を伴う場合が少なくありませんので、日頃からの体制整備が極めて肝要です。さらに中国にける法規準則の要求も年々高まっています。サイバーセキュリティもその一つで、その実施細則が出てきています。会社の実態を把握し、法規準則に十分な体制を構築するには相応の時間が掛かりますので、早めの準備と対応が必要です。

KPMG 中国 GJP 中国総代表 高部 一郎

1. 日本企業の不正に関する実態調査

今回の「日本企業の不正に関する実態調査」は、2018年6月末時点の全上場企業3,699社（REIT、外国企業、日本銀行除く）に対して直近3か年を調査対象期間として実施し、429社から回答を入手しました（回答率約11.6%）。

今回の調査によって、発生した不正の損害額は、日本国内または海外を問わず、子会社で発生した不正の方が大きくなる傾向がありました。不正発生の根本原因として最も多かった回答は、前回調査と同様に「属人的な業務運営」で、次いで「行動規範などの倫理基準の未整備または不徹底」でした。一方で不正の発見経路として最も多かった回答は、「内部からの通報」が最も多く、海外子会社においては、「会計記録等の確認・承認・モニタリング手続き」が最も多くありました。

> [全文はこちら](#)（日本語）

2. Forensic Focus

危機が発生した場合に最悪なのは、発生した結果に対処する計画を持っていないことです。危機的状況はさまざまに起こり得るものであり、ガバナンスの担当者は、打撃を受ける可能性のある危機の種類と、発生した状況に対処する最善の方法を予測することが不可欠です。時間は危機の本質であり、計画を実施するアプローチとスピードを管理することは、すなわち、危機をどの程度うまく管理し、価値の損失を軽減できるかに直結します。企業が直面する危機シナリオの種類とそれらがどのように開示されるのか、そして開示の結果と良好な対応計画について解説します。

> [全文はこちら](#) (英語のみ)

3. 中国サイバーセキュリティ法対応における重要ポイント

当法律の目的は、法人・個人の権利や社会公共の利益の保護、及び国家安全保障となっており、義務履行対象者は、中国に存在するほぼ全ての企業・組織が該当します。重要ポイントとして、①セキュリティ等級保護 ②個人情報保護 ③重要情報インフラ ④データ越境伝送の4つが挙げられます。

①及び②については、既に施行済みの条例や国家標準が存在するため、早急な対応が求められます。特に等級保護に関しては公安当局が制定・施行した監督指針に基づいた積極的な取締が行われています。③及び④については、現時点において正式施行に至っている条例や国家標準等の細則が存在しないため、一部業界向けを除き取締事例は出ておりませんが、当局から個人情報や中国大陸内のサーバに保存するよう指導された事例は発生しております。

> [全文はこちら](#) (日本語)

Contact us お問い合わせ先

GJP China Markets: gjpmarkets.china@kpmg.com

Tel: [+86 \(21\) 2212 2247](tel:+862122122247) (日本語)