

日本DPO協会第4回専門研究部会セミナーあいさつ

2021年3月25日(木)15:00~16:30

「企業価値を創造するコンプライアンス経営  
—情報法コンプライアンスとクライシスマネジメント  
を中心として—」

一般社団法人日本DPO協会代表理事

堀部 政男

(一橋大学名誉教授・元個人情報保護委員会委員長)

# 「日本DPO協会 第4回専門研究部会セミナー 開催のお知らせ」から

- 今回は、その第4回目として、当協会顧問の高野一彦先生に標記のテーマでセミナーの講師を務めていただきます。高野先生は、日頃、企業実務に近いところで、コンプライアンス経営およびリスクマネジメントの在り方を研究され、多方面でその成果を展開されています。今回は、講義形式で企業のコンプライアンス経営とリスクマネジメントの近時の傾向を、情報法を中心としながらも、企業の事業活動にかかわるリスクについて少し広めに俯瞰していただくとともに、具体的な事例を織り交ぜながらクライシスマネジメント各論にも触れて頂きます。また、今後、当協会会員を対象にしたクライシス・シミュレーション・トレーニング(有事対応訓練)に繋げていくことを念頭において、お話いただきます。

## あいさつ 堀部政男

# 「プライバシー：マネジメントによる関与の重要性」

- 今日、当協会の高野一彦顧問のレクチャーをじっくり拝聴する時間を取っている。ここでは、そのほんの一部に関連する「プライバシー」について、プライバシーマークとの関連でマネジメントによる関与の重要性を改めて考えてみることにする。
- 近年、プライバシーは、企業にとって、重要な関心事になってきている。
- プライバシー保護が万全になされていることが、企業価値を高めている。
- ここでは、通商産業省ガイドラインに基づくプライバシーマーク制度（1998年4月1日創設）におけるマネジメントの役割の重視の例を見る。

# 通産省ガイドラインに基づくプライバシーマーク 制度(1998年4月1日)

- JIPDEC(日本情報処理開発協会)のワーキンググループの座長を務め、1997年7月から1998年3月まで通産省ガイドラインをどのように実施するかについて議論した。ワーキンググループは、通産省ガイドラインに基づくプライバシーマーク制度を提案した。JIPDECは、1998年4月1日から「プライバシー保護の信頼のマークを付与する制度」を実施した。
- 1998年9月、私が委員長を務める原案起草委員会が、通産省ガイドラインに基づく日本工業規格(JIS)を策定するために、日本規格協会(JSA)に設置された。原案は、日本工業規格委員会によって検討され、JIS Q 15001:1999(個人情報保護に関するコンプライアンス・プログラムの要求事項)が1999年3月に公表された。

# プライバシーマークシステム 審査基準としてJIS Q 15001採用

- その後、プライバシーマークシステムは、1999年4月1日以降、審査基準としてJIS Q 15001を採用してきている。JIS Q 15001は、1980年OECDプライバシーガイドラインの8原則を参照し、また、EUデータ保護指令(95/46/EC)の概念の多くを参考にしたもので、1999年版は、第1版となった。そのタイトルは、2006年の第2版で**JIS Q 15001 : 2006 (個人情報保護マネジメントシステム—要求事項)**に変更された。JIS Q 15001の第3版は2017年12月20日に公表された。
- JIS Q 15001 : 2017では、「トップマネジメント」の役割の重要性を強調していると言える。

# トップマネジメントの役割重視の例①

- 以下、JIPDECの「プライバシーマーク付与適格性審査基準」(2018年1月12日(2020年11月20日改訂))から部分的に引用する。ただし、ここに記載する関係で、フォーマットは変えた。トップマネジメントは、20ヶ所で使われている。
- 【プライバシーマーク付与適格性審査との関係】
- 審査項目のうち、**トップマネジメント**に関する項目は、原則として、実施基準2.8に定める現地審査において事業者の代表者に対するインタビューを行うことにより確認する。
  
- A.3.2.1 内部向け個人情報保護方針
- No.1 【審査項目】**トップマネジメント**は、個人情報保護目的を説明できること。
- 【確認方法・エビデンス】・**トップマネジメント**による説明
- No.3 【審査項目】**トップマネジメント**は、内部向け個人情報保護方針を文書化した情報を、組織内に伝達し、必要に応じて、利害関係者が入手可能にするための措置を講じていること。
- 【確認方法・エビデンス】・**トップマネジメント**による説明、・措置

## トップマネジメントの役割重視の例②

- 《留意事項》
- 審査項目1. は、**トップマネジメント**に対し、組織の目的、個人情報保護目的、内部向け個人情報保護方針との関係を確認するための項目である。
- A.3.2.2 外部向け個人情報保護方針
- No.3 【審査項目】**トップマネジメント**は、外部向け個人情報保護方針を文書化した情報について、一般の人が入手可能な措置を講じていること。
- 【確認方法・エビデンス】・**トップマネジメント**による説明、・措置
- (例)・トップページから外部向け個人情報保護方針へのリンク(ウェブサイトに掲載する場合)

## トップマネジメントの役割重視の例③

- A.3.3.4 資源, 役割, 責任及び権限
- No.2 【審査項目】個人情報保護管理者は, 個人情報保護マネジメントシステムの見直し及び改善の基礎として, **トップマネジメント**に個人情報保護マネジメントシステムの運用状況を報告する旨が内部規程として文書化されていること。
- 【確認方法・エビデンス】・組織の各部門及び階層における個人情報を保護するための権限及び責任に関する規定(A.3.3.5 d))
- No.3 【審査項目】個人情報保護監査責任者は, 監査を指揮し, 監査報告書を作成し, **トップマネジメント**に報告する旨が内部規程として文書化されていること。
- 【確認方法・エビデンス】・組織の各部門及び階層における個人情報を保護するための権限及び責任に関する規定(A.3.3.5 d))



# トップマネジメントの役割重視の例④

- No.5 【審査項目】トップマネジメントが、個人情報保護のための人的資源を説明できること。
- 【確認方法・エビデンス】・トップマネジメントによる説明、・体制（例）・体制図
- A.3.4.2.9 匿名加工情報
- 【留意事項】
- 確認方法・エビデンスの「方針の有無」とは、方針を文書化した情報を求めるものではなく、トップマネジメント等が方針を説明することでもよい。

# トップマネジメントの役割重視の例⑤

- A.3.7.1 運用の確認
- No.4 【審査項目】個人情報保護管理者は、定期的に、及び適宜に**トップマネジメント**に運用の確認の状況を報告していること。
- 【確認方法・エビデンス】・運用の確認の記録(A.3.5.3 i))