マネジメント講座

GDPR入門 ⑦　網羅的なセキュリティー対策

一般データ保護規則（GDPR）では、個人データのセキュリティー対策が求められ、最新技術、対策費用、個人データの取り扱いの性質、本人の権利、左記図表に示す対策についてリスクベースアプローチに基づく網羅的な対応計画の立案と対策実施が重要となる。

適切な対策実施に向けたリスク対応計画の立案や実際の対策実施結果の記録を必要に応じて保持することも重要である。

平時において各組織では、適切なセキュリティー対策であることを示すために記録をもって網羅的に説明できなければ、適切なセキュリティー対策を実施していることにはならない恐れがある。

事故など有事が発生した場合にも今まで適切にセキュリティー対策を実施していたことを説明するために過去の客観的な証拠として記録が必要になることも考えられる。

法令要件を満たすだけでなくステークホルダーに自組織がGDPRに準拠した活動を実施している組織であることを理解してもらう必要がある。

そのためGDPRに準拠した対応を実施している証明として、自組織でこれまで立案した計画の記録や対策を実施していたことを示すログなどを提示できなければ、ステークホルダーは当該組織で適切なセキュリティー対策が実施できているのか理解・評価できず、当該組織を信頼することはできないであろう。

プライバシー保護と説明責任の実現に向けて、法令で求められている最低限の記録だけでなく、ステークホルダーに信頼し続けてもらうためにどのような記録が必要か組織内で検討し、実行することをお勧めしたい。

（SOMPOリスクマネジメント取締役　宮崎義久）

セキュリティー対策を実施する際に含める事項

個人データの仮名化及び暗号化
取り扱いシステム及び取り扱いサービスの現在の機密性、完全性、可用性及び回復性を確保する能力
物的又は技術的なインシデントが発生した際、適時な態様で、個人データの可用性及びそれに対するアクセスを復旧する能力
取り扱いの安全性を確保するための技術上及び組織上の措置の有効性の定期的なテスト、評価及び評定のための手順

（注）SOMPOリスクマネジメント作成

2019年2月5日
日経産業新聞