Solution Overview: QUNIE CRO Support

情報セキュリティポリシーアドバイザリーサービス

企業不正調査の豊富な経験を活かし、発生したインシデントの実例を踏まえた情報セキュリティポリシーの見直しをご支援いたします。

代表的な課題

■ 企業の情報セキュリティポリシーは、ISMSなどの規格に基づき個社で作成することが一般的です。しかし、不正・不祥事（インシデント）が実際に発生することを想定した内容になっておらず、インシデント発生の抑止や有事対応において有効に機能しないケースが散見されます。

情報セキュリティポリシー

情報セキュリティポリシーで規定される主な項目

- ✓ 基本方針、適用範囲、体制
- ✓ 人的管理（プライバシー、教育、罰則など）
- ✓ 外部委託先管理
- ✓ 文書情報管理
- ✓ セキュリティ監査
- ✓ システム管理
- ✓ ネットワーク管理
- ✓ SNS利用
- ✓ インシデント報告・対応

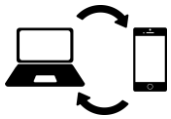
など

実際にインシデントが発生すると、想定外の問題が表面化

メールデータ保管の目的や期間に明確な根拠が無く、調査方法不明、保存期間不足、時間とコストの浪費などが発生する。

会社貸与のPC/携帯電話を調査したいが貸与者から機器調査の同意が得られない。

社用の携帯電話を自宅PCに接続し、バックアップしている。重要な情報が社外のPCに保存されてしまう。



当局対応や不正調査に必要となるリティゲーションホールド(※1)などの諸手続きに関する知見が無い。

※1.訴訟や調査などが合理的に予測された段階で「関連する全ての資料や情報をそのままの状態で保存する」というプロセス

当社サービス提供イメージ

■ インシデント発生を見据えた事前準備を行うことは、対応経験のない企業にとっては非常に難しいことです。QUNIEは、インシデント対応の豊富な経験を有した専門家が実際に発生した事案を基にアドバイスを行うことで、インシデントの発生抑止と効果的な有事対応をご支援いたします。

①現状把握	②評価・分析	③調査報告	④運用支援
• 現状の情報セキュリティポリシー内容確認 • IT環境調査 • 関係部署へのヒアリング	• 公認不正検査士の知見による、改善ポイントの洗い出し • インシデント発生時のリスク分析	• 現状分析結果の提示 • インシデント発生時のリスク分析結果の報告 • 上記を踏まえた改善ポイントと改善案の提示	• 運用体制構築支援 • 社内トレーニング支援 -資料作成 -トレーニングの実施 • 定期的な実態調査支援

株式会社 QUNIE
〒100-8101 東京都千代田区大手町2-3-2 大手町プレイス イーストタワー11F
TEL: 03-3517-2292　FAX: 03-3517-2293
Email: info@qunie.com　https://www.qunie.com

Trusted Global Innovator
NTT DATA Group