

不正アクセス発生時のフォレンジック調査の有効活用に向けた着眼点（概要）

（個人情報保護法サイバーセキュリティ連絡会・令和8年1月16日）

○不正アクセス被害を受けた際に、その**発生原因・被害範囲の把握や効果的な再発防止策の実施**のために、専門の調査会社に**フォレンジック調査を依頼しながら対応することは有用**です。

○実効性のあるフォレンジック調査を行う観点から、組織における**平時からの備え**や、適切な**初期対応**を行うことが重要です。

○本資料は、このようなフォレンジック調査の性質を踏まえ、実効性のあるフォレンジック調査を行うための「**参考資料**」として、個人情報取扱事業者や行政機関等が、①平時から備えておくと効果的な事項、②不正アクセス被害を受けた場合に注意すべき事項、③フォレンジック調査の活用に関する事項を下記のとおり整理したものです。

①平時からの備え



自組織のIT環境を把握し、不正アクセスに備えましょう。

ポイント

- 各種台帳・ネットワーク構成図の作成
 - ログの保管
 - 不正アクセスへの対応フローの整理
- 本資料P9からP22を参照

②有事対応の注意点



証拠保全を意識しながら、不正アクセスに対応しましょう。

ポイント

- 適切な情報連携・封じ込め対応
 - 不用意な端末初期化等の回避
 - 調査会社へのフォレンジック調査依頼
- 本資料P23からP26を参照

③フォレンジック調査の活用



明らかになった事実関係を適切に理解・評価し、再発防止に努めましょう。

ポイント

- フォレンジック調査の前提事項の確認
 - フォレンジック調査結果の根拠の確認
 - 原因に対応した再発防止策の確認
- 本資料P27からP39を参照