ヒアリングシート_調査

1. 本件について以下の情報をお聞かせください。

(1) 本件事象の概要と目的

(2) 本件発覚のきっかけと発覚日時

※ウイルス対策ソフトの検知により発覚した場合は下記の情報もお聞かせください。

・当該ソフトの製品名、メーカー名、パターンファイルや定義ファイルのバージョン

・検出名

・隔離/削除の状況

(3) 本件事象が発生したと思われる日時

2. 調査対象について以下の情報をお聞かせください。

(1)監査ツール等のご使用有無

※ご使用中の場合は下記の情報もお聞かせください。

・当該ソフトの製品名、メーカー名、事象発生時点のバージョン

・USB ポートや LAN ポートの使用禁止等の制限有無

(2) ご提供いただけるログの種類

※データの流れが分かるログ（プロキシ、FW、NetFlow など）やその他ログ全般について

※上記 1. (1)の目的によってはご提供不要となる場合もございます。

(3) アップデートの適用状況

※Windows アップデートなどパッチ適応の頻度や設定（自動更新 or 手動）状況についてご教示ください。

(4) 対象端末の情報

・機種情報（メーカー、型番等）

・OS

・ストレージの容量

・暗号化、パスワードロック等の制限有無

・その他特記事項

・用途（サーバー or クライアント）

(5) 対象端末の現在の状態

(6) 対象端末を普段使用しているアカウント情報

・アカウント名

・当該アカウントの利用者数
・当該アカウントの管理者権限の有無
・種類（ローカル or ドメインアカウント）

3. 調査に関するご希望をお聞かせください。

(1) 実施時期

(2) 保全データのお渡しを必要とする場合のデータ格納先
※格納先メディア（HDD 等）を独自にご用意いただく、あるいは弊社での用意を希望するといったご要望をお聞かせください。保全データのお渡しを要さない場合にはご回答不要です。

(3) その他のご希望

4. その他・備考

(1) 調査に必要な証拠保全作業を実施する際、最も迅速な方法は対象コンピュータから内蔵ストレージを取り外し、専用機器を使用して実施する方法です。なお、一部のノート PC 等においては内蔵ストレージを取り外すことで保証対象外になる可能性がございます。取り外しの可否がある場合は事前にお聞かせください。

(2) 証拠保全対象端末の状態に応じて電源を投入させていただく場合がございます。その際、レジストリやログ情報等のデータが変化、もしくは新たな情報の追記等が発生致します。ご了承ください。

(3) 調査においてメールに関する作業を要する場合には、使用されているメーラーの種類やバージョン等の情報を併せてご教示ください。

(4) 調査開始までは現在の状態に一切手を加えないことをお勧め致します。ただし、調査対象端末が暗号化されている場合には事前に解除した状態でのご提供をお願い致します。