業務仕様書

1. 契約件名：おまかせセキュリティ事故駆け込み窓口 遠隔サポートによるログ調査業務

2. 業務の目的：

パソコン１台（以下、対象パソコン）に関わるセキュリティ事故について、対象パソコンのログ等を調査することで、特定期間内に発生したセキュリティ事故の影響、原因を可能な範囲で調査することを目的とします。調査は、感染後の侵入原因に関する調査、感染後の不審なファイルに関する挙動調査、特定のシステム等に対する不正な操作に関する調査を主とします。

3. 提供期間：

契約締結後に実施するヒアリング調査及び解析用ログ等受領後から 2 週間とします。

4. 本業務の提供フロー：

以下のフローに従って業務を実施します。

(0) ヒアリング調査

対象パソコンの状況（感染の痕跡、発生日時、ファイルの変更履歴、その他アプリケーションの起動など）を電話・メール等によりヒアリングさせて頂きます。

ヒアリングの際には、アンチウィルスによる検知日時及び感染被疑ファイルが重要となりますので、準備頂くようにお願い致します。

(1) 遠隔サポート事前準備

オペレータの指示に従い、お客様は対象パソコンにリモートサポートツールをインストールしていただきます。

リモートサポートツールによりオペレータ端末と対象パソコンを接続後、ログ等を取得するための解析専用ツールをオペレータ端末から対象パソコンへ転送します。

環境要因等によりリモートサポートツールが使用できない場合、お客様にログ収集をお願いすることがあります。

(2) リモートサポートツールによる情報収集

対象パソコンにて解析専用ツールのファイル圧縮を解凍し、ツールおよびコマンド等を実行することでオペレータが対象パソコンのログを収集します。

(3) 解析用ログ等の受領

収集したログ等のファイルを対象パソコン上で圧縮後、リモートサポートツールにより、オペレータ端末に転送し、弊社解析環境にて調査可能な状態とします。

(4) 対象パソコンのログ調査

特定期間内における対象パソコンのログ等を調査し、感染被疑ファイルに関する不審な可能性がある挙動（ファイルの作成、実行有無の確認、ファイルの変更履歴、その他アプリケーションの起動状況等）及びその関連ファイルを抽出致します。

(5) 調査結果の報告等

調査内容に基づき不審な可能性がある挙動及びその関連ファイルを調査通知書にまとめ、提出及び報告いたします。

(6) 報告会の実施

報告会を希望する場合には、調査報告書を基にした報告会を実施いたします。報告会は1回のみ遠隔（Microsoft Teamsを利用）による実施とし、実施時間は概ね1時間程度となります。

(7) その他、上記に附随又は関連する業務

5. 環境条件：

以下の環境条件を対象パソコンで満たすこと

(1) オペレーティングシステム

・Windows10 Home / Windows10 Pro / Windows10 Education /Windows10 Enterprise

・Windows11 Home / Windows11 Pro / Windows11 Enterprise

(2) ハードディスク空き容量

・10Gバイト以上

(3) ネットワーク環境

・インターネット接続環境

・リモートサポートツールに関わる通信の疎通確保（Firewall/Proxy等の許可設定）

(4) ソフトウェア環境

・ファイル圧縮解凍ソフトウェア（ZIP形式）の事前インストール

6. 利用ツール：

以下のツールを対象パソコン上でインストール及び実行する

(1) リモートサポートツール

・オプティマ社 OptimalRemoteクライアント

・動作条件等：https://www.optim.co.jp/optimal-remote/

(2) 解析専用ツール

・サイバーディフェンス社　CDIR-C、CDIR-A

・動作条件等： https://www.cyberdefense.jp/products/cdir.html

7. 解析データ範囲：

・対象パソコンから解析専用ツール及びコマンド等で収集したログデータ

・不揮発性データ（HDD/SSD）のみ対象。揮発性データ（メモリ情報）は対象外

8. 納品物：

調査・報告した内容を取りまとめた調査通知書を納品物とする

9. 業務完了通知：

業務期間終了時に業務完了通知書を提出する

10. その他：

(1) 調査対象に対象パソコンの台数を増やすこと、もしくは対象パソコン以外の FW のログファイル等の電子ファイルを追加することも可能です。但し、別途調査費用が必要となります。FW のログファイルについては、事前に当社により解析が可能であると判断された製品のログに限ります。

(2) 調査の起点となる日時（アンチウィルスソフト等による感染を検知した日時等）から遡って調査を実施します。遡りの日数は、おおむね 3 日程度になります。

(3) 本業務における免責事項を別紙 免責事項に示します。

(4) 本仕様書に記載されていない事項については、両社で協議のうえ、決定するものとします。

(5) 本業務では調査対象パソコンに関するご質問のみ受付可能であり、一般的なご質問については別途「受付窓口（無償)」へ問合せいただきます。

(6) 本サービスで得られたログ情報については、当社にて管理の上で、サービス提供完了後、1 か月経過後に削除致します。なお、マルウェアの検体等に関わる情報が含まれる場合には、公共の利益または研究を目的として保持し、その目的のためだけに利用し、お客様から得られたデータであることを特定できないように匿名化を行った上で、これらを開示することがあります。

(7) アンチウィルスソフト等の感染検知がない端末での感染有無、アカウント窃取有無、及び情報漏洩有無の証跡を目的とした調査ではありません。

(8) お客様から本サービスの問合せ受付期間は、サービス提供完了後 1 か月とします。

(9) 本業務の応対時間は平日 9 時～17 時（祝日、年末年始は除く）となります。

以上

免責事項

① 東日本電信電話株式会社は、申込者の問題・課題等の特定、解決方法の策定、解決または解決方法の説明を保証するものではありません

② 東日本電信電話株式会社は、オペレータの説明に基づいて申込者が実施した作業及びオペレータが遠隔で実施した作業の内容について保証するものではありません

③ 東日本電信電話株式会社は、オペレータの説明に基づいて申込者が実施した作業、オペレータが遠隔で実施した作業で生じる申込者の損害について責任を負いません

④ 本業務は、メーカー、ソフトウェアハウス及びサービス提供事業者が提供する正規サポートを代行するサービスではありません。問合せの内容によっては、問合せの対象となるモバイル端末、ソフトウェア（ＯＳ）等をそれぞれ提供するメーカー、ソフトウェアハウス、サービス提供事業者等のホームページを紹介することや、それぞれに対して申込者自身で直接問合せすることを依頼するに留める場合があります

⑤ オペレータの説明に基づいて申込者が実施した作業、オペレータが遠隔で実施した作業に関連して、申込者のＩＤ又はパスワードで実行された操作は、申込者による操作であるとみなし、これに伴い生じる申込者の損害について、東日本電信電話株式会社は責任を負いません

⑥ 本業務は、あらゆるウイルスへの対応、不正通信の遮断及びセキュリティ対策機能を保証するものではなく、本業務により生じた申込者の損害及び申込者の行為又は申込者が利用する通信機器その他の機器の動作を通じて第三者が被った損害について、申込者は自己の責任でこれを解決するものとします

⑦ 申込者は、本業務により第三者に対し損害を与えた場合は、自己の責任でこれを解決するものとします

⑧ 東日本電信電話株式会社は、本業務により生じる結果について、本業務で利用する設備の不具合、故障または第三者による不正侵入、商取引上の紛争、法令等に基づく強制的な処分その他の原因を問わず、責任を負いません

⑨ 東日本電信電話株式会社は、事象の完全な解析及び解析結果の精度について保証するものではありません

⑩ 東日本電信電話株式会社は、以下の場合に十分にサポートを行えない可能性がありますが、サポート内容について一切の責任を負いません

- 痕跡となるデータが消去、変更されている場合
- ハードディスク（HDD/SSD）が暗号されている場合
- 環境条件を満たしていない場合
- 利用ツールが正常動作しない場合
- オペレータによる対象パソコンへの遠隔操作及び操作指示を拒否された場合
- 解析に必要なヒアリング（インシデント発生状況及び発生日時、ネットワーク構成、システム運用状況等）が十分に行えていないと東日本電信電話株式会社が判断した場合

⑪ 東日本電信電話株式会社が提示する解決策は、参考情報として提示するものであり、今後いかなるセキュリティインシデントを発生させないことを保証するものではありません

⑫ 提供いただいたデータの中に、著作権で保護された著作物、申込者以外の第三者の権利情報が含まれている場合において、東日本電信電話株式会社は一切の責任を負いません