別紙 3-Rev005-1912

「InfoTrace 運用支援サービス」のご案内

1. サービス概要

InfoTrace 運用支援サービスは、当社がお客様に代わって InfoTrace Mark II セキュリティログの収集を行い、日常の運用に関わる業務をご支援するクラウドサービスです。
セキュリティログは、セキュリティインシデントの被害を調査する基礎となるデータであり、その収集と分析を当社がお客様に代わって行います。それを基に、お客様の Windows PC で発生したマルウェア検知アラート(以後検知アラート)に対して対処すべきかを判断し、ご報告します。このサービスにはお客様の依頼に基づいたネットワーク隔離と検体削除といった初動対応も含まれます。
インシデントの原因がマルウェアであり、詳細分析・影響範囲特定などセキュリティログのみによる判断が困難な場合は、ご希望に応じて別途オプションとして高度なプロフェッショナルサービスもご提供できます。

2. サービス内容一覧

InfoTrace 運用支援サービスの内容は、以下のとおりです。

サービスメニュー		対応時間
初期導入支援サービス （詳細は 3 .を参照）	初期導入期間中のログチューニング	当社営業時間対応
	初期導入期間中の過検知対応	当社営業時間対応
運用レポート提供サービス （詳細は 4 .を参照）	速報レポートの提供	24 時間 365 日対応
	解説レポートの提供	当社営業時間対応
	ネットワーク隔離の実施	当社営業時間対応
	検体削除と調査	当社営業時間対応
	問合せ対応	24 時間 365 日受付 /当社営業時間対応
運用管理サービス （詳細は 5 .を参照）	月次レポートの提供	
	管理コンソールの提供	
	サービス用クライアントのバージョンアップ	
オプションサービス （詳細は 6.を参照）	定例会の実施	
	プロフェッショナルサービス	

3. 初期導入支援サービス

3-1. 初期導入期間中のログチューニング

- InfoTrace 運用支援サービス開始後、一か月間を目安に対応します。
- サービス利用端末が出力するセキュリティログのうち、インシデント対応において重要度が低い情報を監視除外します。
- 端末の負荷に応じて取得すべきログを調整します。
  例：開発環境でのコンパイル・デバッグのログの除外、アプリケーション設定ファイルの読み込みログの除外

※注：設定変更後はサービス利用端末の再起動が必要です。

3-2. 初期導入期間中の過検知対応

- InfoTrace 運用支援サービス開始後、一か月間を目安に対応します。本期間中は検知アラートへの対応は行いません。
- 本期間中はマルウェア対策機能をノンブロックモードでご利用いただきます。
- ヒアリングシートに記載いただいた業務アプリケーションを例外リストに登録し、マルウェア対策機能の検知対象から除外します。
- 検知アラートから過検知と判断したファイルを例外リストに登録します。
- 当社で過検知と判断できない場合は、サービス管理者に確認後、例外リストに登録します。
- 例外リストの追加登録は当社営業時間内に対応します。

※注：導入期間終了後はマルウェア対策機能をノンブロックモードかブロックモードを選択いただけます。
ノンブロックモード：マルウェア対策機能で不審なファイルを検知しても、検知されたファイルは実行可能です。
ブロックモード：マルウェア対策機能で不審なファイルを検知すると、検知されたファイルは実行不可です。
例外リストに登録し設定が反映されると、検知されたファイルは実行可能になります。

4. 運用レポート提供サービス

検知アラート発生後、ファイル情報、セキュリティログの内容から危険度を「ブラック」「グレー」「ホワイト」の三段階で判定し、レポートとしてご報告します。

4-1. 速報レポートの提供（24 時間 365 日対応）

- 検知アラートをサービスシステムで受信後 2 時間以内を目安に提供し、以下の内容を速報レポートとしてポータルサイトにアップロードします。明らかな脅威であるブラック判定の場合は、担当者にメールにてご連絡します。
  ① ファイルの生成経緯
  ② 検知ファイルが実行されるまでのプロセス
  ③ 検知ファイルが実行したプロセス
  ④ 書き込まれたファイル
  ⑤ 編集されたレジストリ
  ⑥ 読み込まれたファイル
  ⑦ 通信
  ⑧ ファイル属性
- セキュリティログの調査対象期間は検知アラート発生時から遡って 7 日以内までとします。
- ヒアリングシートで「直ちに隔離登録する」をご希望の場合は、検知アラートの判定結果により直ちにネットワーク隔離を実施します。
- ヒアリングシートで「例外リストに登録する」をご希望の場合かつ過検知の可能性が高いホワイト判定の場合は、当社営業時間内に例外リストに登録します。
- 検知アラートをサービスシステムで受信後、72 時間以内に同一サービス利用端末で同一ファイル(同一ハッシュ値)を検知した場合は、メールによる連絡含めレポート提供の対象外です。

4-2. 解説レポートの提供（当社営業時間対応）

・速報レポートの内容をもとに当社で追加調査が必要と判断した検知アラートに対して、担当アナリストがセキュリティログを分析した結果をご報告します。
・検知アラートをサービスシステムで受信後、5 営業時間以内を目安に分析結果を解説レポートとしてポータルサイトにアップロードします。明らかな脅威であるブラック判定、要調査であるグレー判定の場合は、担当者にメールにてご連絡します。
　例）正午までの検知アラート：　当日中を目安に報告
・セキュリティログの調査対象期間は検知アラート発生から遡って 7 日以内までとします。
・分析の結果、本レポートの判定結果が速報レポートの判定結果から変わることがあります。
・同一端末で複数の検知アラートが発生した場合や多数の同一事象が発生している場合は、複数の速報レポートを 1 つの解説レポートに集約したうえでご報告することがあります。

ブラック判定の場合（明らかな脅威）

・検知されたファイルについて、ファイルおよび関連するセキュリティログの内容をご報告します。
・サービス管理者の依頼に基づくネットワーク隔離や検知されたファイルの駆除も可能です。

グレー判定の場合（要調査）

・マルウェアか過検知かを判断するために、検知された端末のサービス利用者に対しサービス管理者にて確認すべきセキュリティログの内容をご報告します。
・サービス管理者の依頼に基づくネットワーク隔離や検知されたファイルの駆除も可能です。
・サービス利用者、サービス管理者で検知ファイルを意図して保存もしくは実行していたか否かなど、解説レポートを参照の上、ご返信ください。
3 営業日以内に返信が無い場合 はホワイト判定と同様の対応を実施します。

ホワイト判定の場合（過検知、誤検知）

・検知されたファイルについて、ファイルおよび関連するセキュリティログの内容をご報告します。
・ヒアリングシートで「例外リストに登録する」をご希望の場合かつ過検知の可能性が高いホワイト判定の場合は、当社営業時間内に例外リストに登録します。

4-3. ネットワーク隔離の実施（当社営業時間対応）

・本サービスにおけるネットワーク隔離とは論理抜線です。
・ヒアリングシートで「直ちに隔離登録する」をご希望の場合は、検知アラートの判定結果により直ちにネットワーク隔離を実施します。
・ネットワーク隔離実施後は、ヒアリングシートの通信許可設定以外の宛先には接続できません。
・通信許可設定は宛先 IP アドレス、ポート番号による指定が可能です。
・サービス管理者の依頼に基づくネットワーク隔離および隔離の解除は当社営業時間内のみ対応可能です。
※注：サービス利用端末がサービスシステムと通信可能であることが必要です。

4-4. 検体削除と調査（当社営業時間対応）

・サービス管理者の依頼に基づき検知されたファイルの削除も可能です。
・検知の原因の調査をサービス管理者がご希望される場合、調査可能な範囲で追加情報を提供します。
・ファイルの削除および調査のためのファイルの取得は当社営業時間内に行います。
※注：サービス利用端末がサービスシステムと通信可能であることが必要です。

4-5. 問合せ対応（24 時間 365 日受付/当社営業時間対応）

・レポートへのお問合せは受信したメールに直接返信ください。
・お問合せ対応は、専門アナリストが当社営業時間内に行います。
・レポート以外の各種お問合せは専用 web フォームにご入力ください。

5. 運用管理サービス

5-1. 月次レポートの提供

1 ヶ月の対応状況を集計し、翌月 5 営業日を目安に月次レポートとしてポータルサイトにアップロードしメールにてサービス管理者へご連絡します。

1. 1 ヶ月のエグゼクティブ・サマリー
   ① 当月のサービスサマリー
   ② 当月の脅威判定結果
   ③ 検知アラート月次推移分析
   ④ 補足事項
2. 1 ヶ月のサービス稼動状況
   ① 検知アラート毎レポート
   ② サービス利用端末
   ③ マネージドサービス停止時間
3. 別紙と用語
   ① 別表一覧
   ② 用語の解説

5-2. 管理コンソールの提供

・サービス利用端末の情報やエラー情報を確認可能です。
・サービス利用端末の登録台数、最終通信日時を確認可能です。
・ネットワーク隔離されたサービス利用端末の隔離解除が可能です。

5-3. サービス用クライアントのバージョンアップ

・サービス利用端末にインストールする サービス用クライアントをバージョンアップします。
・サービス用クライアントのバージョンアップは、以下の手順で行います。
   ① バージョンアップ実施日を事前にご連絡します。ご都合が悪い場合は、サービス管理者との調整を行います。
   ② 新しいバージョンの サービス用クライアントをサービス管理者に提供します。サービス管理者はインストールの事前検証が可能です。
   ③ 新しいバージョンをサービスシステムに適用後、サービスシステムと同期したサービス利用端末からバージョンアップされます。
   ④ サービス利用端末のバージョンアップ状況は、ポータルサイトの管理コンソールより確認可能です。

6. オプションサービス

必要に応じて以下オプションサービスをご利用可能です。オプションサービスには別途料金が発生します。

6-1. 定例会の実施

- サービス管理者指定の場所で月次レポートを報告します。
- 国内外の情報セキュリティ動向、および脅威トレンドなどの情報を提供します。
- 月 1 回、1 ～2 時間程度の報告です。

6-2. プロフェッショナルサービス

- 基本的な範囲を超え、当社の通常運用では対応できない調査等の専門サービスを実施します。
  例：システム監査対応、電磁的記録の証拠保全、法的紛争や訴訟対応、フォレンジック調査

7. 制限事項

7-1. レポート保持期間

- 月次報告書含め各種レポートは最大で過去 13 ヶ月分が保持されます。

7-2. レポート提供の対象制限

- ファイル情報から無害なアプリケーションと判断した場合、例外リストに登録し、レポート提供は実施しません。

7-3. サービス対象外事項

以下事項は、本サービスの対象外です。

- 機器の貸出
- サービス管理者から提供された資料、設定情報等の維持保管
- サービス利用端末へのサービス用クライアントインストール作業
- サービス管理者指定の条件下におけるサービス用クライアントの動作検証、動作保証など
- オンサイト作業でのサービス用クライアントの障害報告、および調査

以上