HITACHI
Inspire the Next

サイバー攻撃分析サービス のご紹介
（脅威判定編）

株式会社　日立ソリューションズ

1．課題と対策

HITACHI
Inspire the Next

こんな課題に

マルウェア検知製品のアラートが発生したが、
マルウェアかどうか判断できない

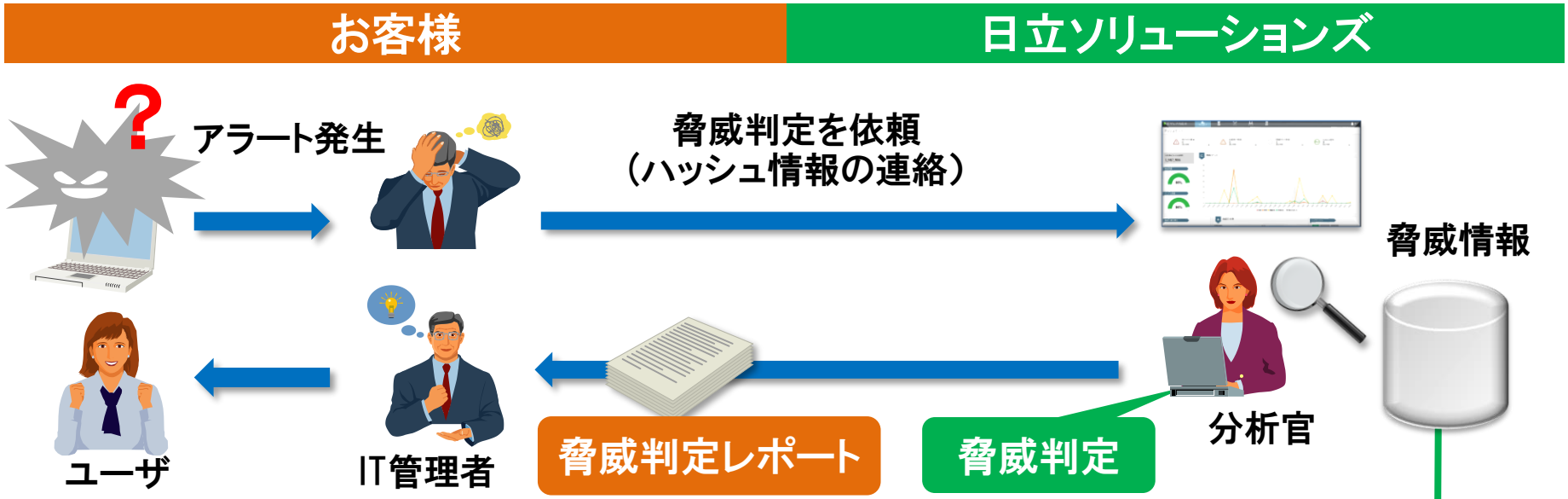
効果

- 最新の脅威情報を活用し、マルウェア検知製品のアラートがマルウェアかどうか判定

2. サイバー攻撃分析サービス　～脅威判定～

HITACHI
Inspire the Next

マルウェア検知製品が検知したアラートの脅威判定
お客様のアラート発生時の対応作業を支援



検知アラートの対応判断

マルウェア検知製品が検出したファイル（プログラム）が、マルウェアか正常ファイルか判定（白黒判定）

脅威判定レポート

脅威インテリジェンスの膨大な脅威データ

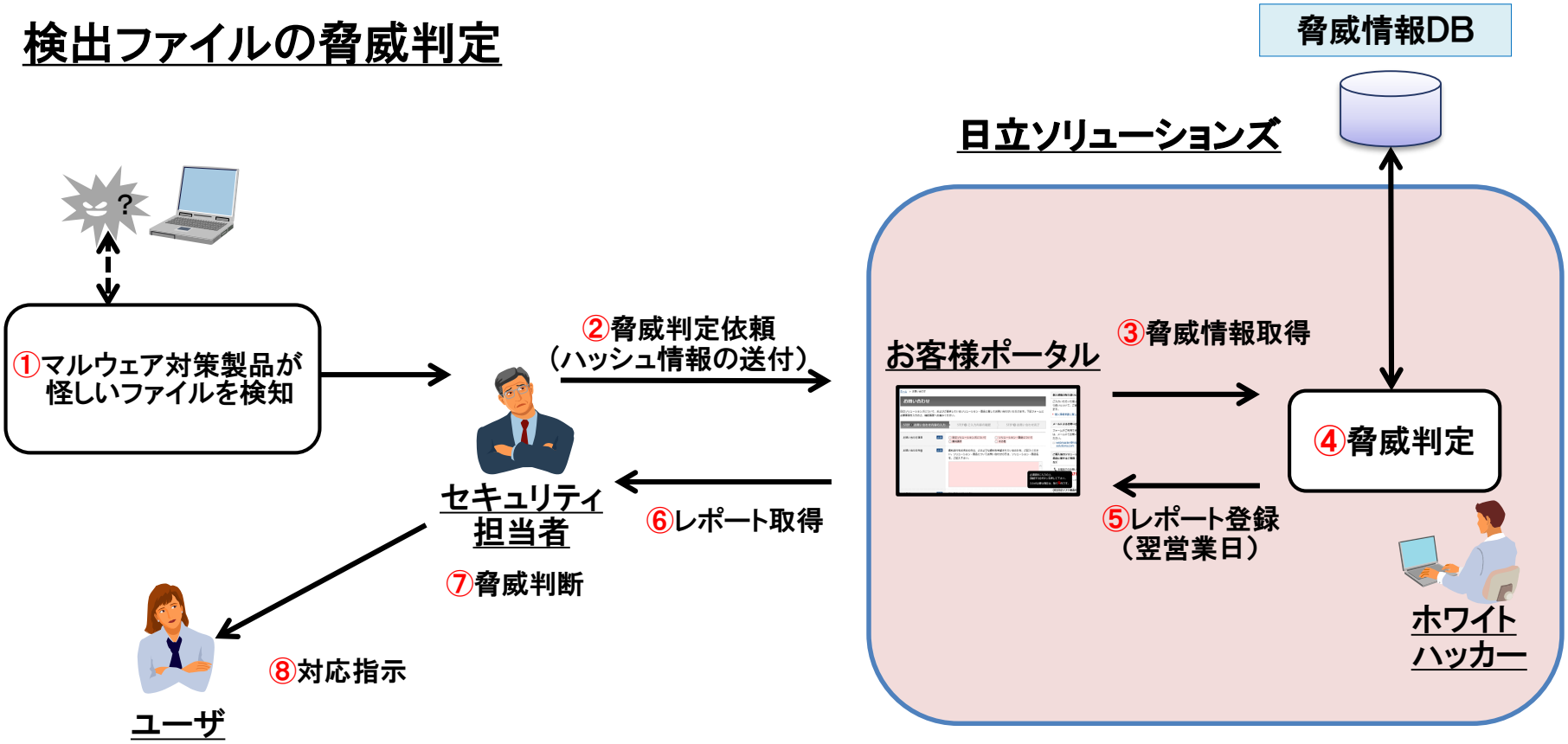
- 270億以上 URL
- 90億以上 ファイル振る舞い記録
- 6億以上 ドメイン
- 2,000万以上 モバイル・アプリ
- 40億以上 IPアドレス
- 1,000万以上 接続されたセンサー

※ 詳細なシステム構成/条件等はAppendixをご参照ください

3. サービス利用詳細

マルウェア対策製品等で検知されたファイルの脅威判定結果レポートを作成しご提供

検出ファイルの脅威判定



3. 価格表

HITACHI
Inspire the Next

■価格

No	メニュー		サービス内容	対応回数	価格	備考
1	脅威判定	新規・更新	脅威判定とレポート提供	12ファイル/年	3万円/月 (36万円/年)	
2		回数追加	対応回数の追加	1ファイル	3万円	

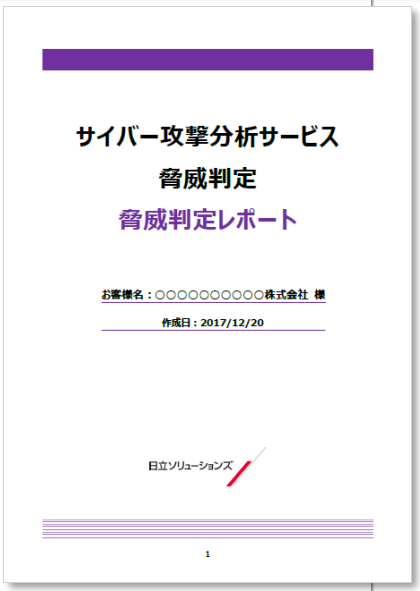
■前提条件

メニュー		サービス内容	前提条件
脅威判定			
	脅威判定	マルウェア対策製品等で検出されたファイルの脅威判定、レポート報告 (ご依頼後、翌営業日に判定結果をご提供)	・ご依頼時に対象ファイルのハッシュ値(MD5)が必要 ・判定可能なファイルの種類はWindowのPEファイル(exe、dll、sysファイル)

4. レポートサンプル

HITACHI
Inspire the Next

脅威判定（脅威判定レポート）



サイバー攻撃分析サービス

脅威判定

脅威判定レポート

お客様名：○○○○○○○○○○株式会社 様

作成日：2017/12/20

日立ソリューションズ

1

1.調査概要

調査日：2017/08/01

2.調査結果

脅威判定依頼いただきましたファイル情報の判定結果は以下となります。

ファイル名	FJK.dll
ハッシュ値	5ce24deaba037ffb761a1881770baed4a541be0e
分類	無害なファイル
区分	
推奨対策方法	本ファイルは脅威判定分析により、安全なファイルと判断されました。 以降社内の環境にて検知などが行われることがないように、ホワイトリストに登録していただく対応をお願いいたします。

ファイル名	Abc.exe
ハッシュ値	f88f94f974393a32cedc172ea3f7f4affb82f4c2
分類	**有害なファイル**
区分	ランサムウェア
推奨対策方法	本ファイルは、ランサムウェアの一種です。感染するとコンピュータをロック、あるいはファイルを暗号化することで使用不能にしたのち、元に戻すことと引き換えに金銭を要求する不正なプログラムです。 環境から削除したうえで適切な対処を行うことを推奨いたします。

ファイル名	DEF.dll
ハッシュ値	27ef11c24a1d336f46c69762b655a1495656820f
分類	**有害なファイル**
区分	不適切アプリケーション
推奨対策方法	本ファイルは、ビジネス環境では不適切と考えられるアプリケーションの一種です。 環境に悪質な影響は及ぼすことはありませんが、不適切と判断された場合は、削除されることを推奨いたします。

ファイル名	GHI.dll
ハッシュ値	c8d757246d5b7d35ba9e3f761a65e96de3101ae9
分類	**有害なファイル**
区分	不適切アプリケーション
推奨対策方法	本ファイルは、ビジネス環境では不適切と考えられるアプリケーションの一種です。 環境に悪質な影響は及ぼすことはありませんが、不適切と判断された場合は、削除されることを推奨いたします。

以上

5. FAQ

#	質問	回答
1	レポートは、どのように提供されますか？	弊社製品のサポートWEBページ「@Service24」にアップロードさせていただきます。 https://service24.hitachi-solutions.co.jp/Session
2	アップロードされたレポートの保存期間について教えてください。	登録されたレポートは、速やかにダウンロードし保存してください。 登録から1か月以上経過したレポートは、予告なく削除させていただきます。
3	ファイルのハッシュ値の取得方法について教えてください。	ファイルのハッシュ値(MD5)はWindows Vista/WindowsServer2008以降のWindowsOSに標準で付属している「certutil.exe」コマンドでご確認いただけます。コマンドプロンプトからの「certutil.exe」コマンドの実行例を次に示します。 ---------- >certutil.exe -hashfile "対象ファイルのフルパス" MD5 ----------
4	脅威判定可能なファイルの種類はWindowsのPEファイル(exe、dll、sys)であり、マクロ等のウイルスは判定できないとの事ですが、これで脅威判定として十分なのでしょうか？。	マクロを以下の2つに大別して説明します。 ①マルウェアのダウンローダーとして動作するもの。 ②マクロ自身がファイルの改ざん等を行うもの。 最近、マクロウイルスとして流行しているのは主に①のタイプになります。この場合、ダウンロードされたマルウェアは検知されます。
5	脅威データベースとは何ですか？	最新の脅威情報を日々収集している第3者機関の脅威情報データベース(＝脅威DB)を活用して、お客様から収集した情報の脅威を判定しています。脅威DBは、リアルアイムに未知の脅威を収集し更新されます。多くの製品の脅威判定にも利用されており、高い実績と信頼性を兼ね備えております。

HITACHI

Inspire the Next