FUJITSU Infrastructure Service

自治体様向けふるまい検知サービス

マイナンバー対策にも最適！「ふるまい検知サービス」のご紹介

2016年1月　マイナンバー制度　開始

マイナンバー制度の運用開始により、所轄官庁より、中間サーバのセキュリティ対策として**サンドボックス装置**を使ったマルウェア対策が「重要」と定義されています。

本サービスは、サンドボックス装置を活用した、通信の監視による**未知のマルウェアの「検知」**から、**富士通のセキュリティエキスパートによる経験と知見を基にした「解析」**までを、自治体様にご提供するサービスです。

サービスの特長

- LGWAN網を使用することにより、**セキュアな監視を実現**
- メール添付ファイルや通信パケットを24時間・365日の体制で監視・分析することで、マルウェアやウイルス感染などの脅威を**早期発見**
- ふるまい検知ツールをサービスとして月額利用することができ、**初期投資を抑止**
- 別サービス「ウイルス拡散防止サービス」をご契約いただければ、検知だけではなく、サービスエンジニアが駆除用ツールを持参し、マルウェア駆除を代行

サンドボックス（動的解析）装置とは

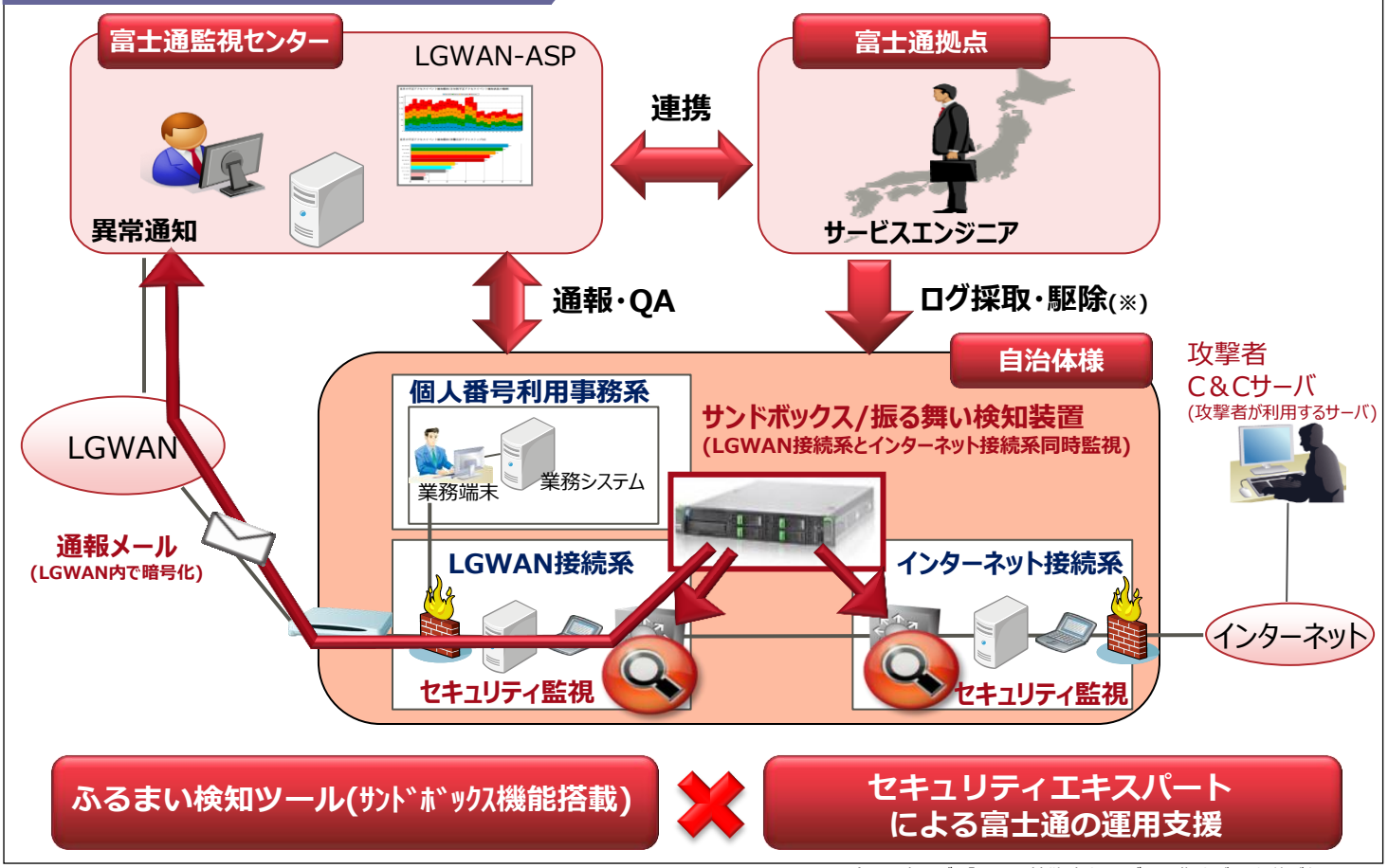
ウイルス対策ソフトでは検知できない、巧妙に作りこまれた未知のマルウェアを、通信のふるまいから検出する装置です。

■サンドボックス機能による、未知のマルウェアの解析イメージ

主に検出するもの

- ・不正なURLへのアクセス
- ・既知のC&Cサーバへのセッション確立
- ・頻繁なログイン失敗
- ・不正なアプリケーションの通信
- ・疑わしい拡張子のついた実行ファイルの転送（各種通信プロトコル）
- ・不審なDNSクエリ
- ・不正なUser-Agent によるWebアクセス
- ・IRC ボットによるコマンド
- ・不正なURLを本文に含むメールの検出
- ・外部サイトへのファイルアップロード

サービス提供イメージ



※駆除には別サービス「ウイルス拡散防止サービス」の拠点ごとの契約が必要です。

サービス実施内容

サービス名称				サービス概要
ふるまい検知サービス	導入支援サービス			■運用サービスに必要な要件のヒアリング（運用手順の取り決め 等） ■運用条件書の作成 ■検知ツールの設置
	運用サービス	基本サービス		■未知のマルウェアによる脅威イベントの監視・通報 ■インシデント管理・月次報告（通報履歴） ■通報内容に関するQA
		オプション	ログ分析レポート	■検知ツールのログを分析し、潜在的な脅威および、対策に関するアドバイスを月次レポートでご報告
			周辺機器ログ分析	■危険度が高いアラート発生時の詳細分析 (FW/Proxy等の周辺機器ログと振る舞い検知装置ログの相関分析調査：月２回まで)
			検体解析	■未知のマルウェアを検知した場合の検体分析（年2回まで）
			オンサイト支援	■サービスエンジニアが検知ツールのログ採取の現地作業を代行
ウイルス拡散防止サービス				■サービスエンジニアがお客様先へご訪問させて頂き、USB型ツールを使用してウイルスチェック・駆除代行を行います。

【問合わせ先】お近くの弊社又は代理店の担当営業までお問合わせ願います。