

2016年9月21日

## 「WideAngle」のセキュリティインシデント対応メニューを強化

～日本初<sup>\*1</sup>の24時間以内の「インシデント対応駆付け保証」、  
「標的型マルウェア感染端末調査」を提供開始～

NTTコミュニケーションズ株式会社（略称：NTT Com）は、2016年10月3日より、統合セキュリティサービス「WideAngle」において、以下2点の新たなセキュリティインシデント対応メニューを開始します。

- ・インシデント発生後24時間以内<sup>\*2</sup>に、高スキルのエンジニアがお客さま拠点へ駆付け、被疑端末の証拠保全、マルウェア感染判定などを行う「インシデント対応駆付け保証」によりセキュリティ被害の範囲を最小化します。
- ・お客さま ICT 環境において、標的型マルウェアに感染している端末がないかを事前に調査する「標的型マルウェア感染端末調査」により、予防保全の強化をサポートします。

### 1. 背景

標的型攻撃などのサイバー攻撃において、従来のウイルス対策のパターンファイルでは検知できない未知のマルウェアなども多く、企業には侵入されることを前提とした対処策が求められております。マルウェアは機密情報を摂取するもの、または時間に乗じて拡散・潜伏し、影響範囲を広げていくものなど様々な行動をおこします。そのため、セキュリティインシデント対応においては、証拠情報の保全、感染端末の特定、マルウェアの特定などの初動対応、利害関係者への事故報告を早急に行うことが、原因究明の複雑化とコストの増加を抑えることにつながります。また、お客さま ICT 環境のエンドポイントにおける未知のマルウェアの侵入や、感染状況を網羅的に把握することが今後のセキュリティ対策を検討・実施する上で、非常に重要です。

### 2. 概要

NTT Com では、2013年11月より、「インシデントレスポンス（旧名称：レスキューサービス）<sup>\*3</sup>」を提供していますが、今回、以下のとおり、メニューを拡充します。※詳細は別紙参照

サービスメニュー	メニュー	概要
インシデントレスポンス	総合インシデントレスポンス	セキュリティインシデントの判定、原因の特定、情報漏えいの有無など、インシデントレスポンスに関わるフルサービス
	インシデント初動対応パック	ネットワークログなどの分析によるセキュリティインシデント判定、初動対応、今後の対応アドバイス
	インシデント対応駆付け保証	インシデント発生後24時間以内に駆付け、マルウェア感染判定を即日実施することを保証
	標的型マルウェア感染端末調査	標的型マルウェアに感染している端末がないか調査するサービス (対象はお客さま管理の全 Windows 端末)

### (1) 「インシデント対応駆付け保証」

お客さまの依頼連絡から、お客さま拠点まで駆付ける所要時間を以下のとおり保証する「インシデント初動対応パック」のオプションサービスです。

- ・東京都 23 区内並びに主要都市（大阪市、名古屋市、横浜市、千葉市、さいたま市など）：24 時間以内
- ・上記エリアおよび都市以外：翌日中\*<sup>2</sup>

駆付け後、お客さま ICT 環境のネットワークログや被疑端末ログを収集・分析し、マルウェア感染の有無を即日判定します。

従来の「インシデント初動対応パック」では、同様のサービスをリモート環境より 3 日以内に行っておりました。本メニューの利用により、お客さまは更に早くインシデント原因の究明や感染端末の拡大を防ぐ対応が可能となり、被害範囲の最小化、的確な影響判定、状況把握と再発防止策実行の迅速化が可能となります。

### (2) 「標的型マルウェア感染端末調査」

お客さま ICT 環境のエンドポイントにおいて、標的型マルウェアに感染している端末がないか全端末を調査します。

本サービスにより、お客さまは、従来把握が困難であったエンドポイントでの未知のマルウェアの潜伏・感染について、事前に認識した上で、予防保全策を講じることが可能です。また、セキュリティインシデント発生後に利用することで、確実な根拠に基づいた復旧宣言に資することが可能です。

## 3. 提供価格（税抜）

(1) 「インシデント対応駆付け保証」：100 万円/駆付け

※有効期間は本サービス申込みより 1 年間です。

※駆付けを実際に行った時のみ料金が発生します。

※別途「インシデント初動対応パック」の料金が必要です。

(2) 「標的型マルウェア感染端末調査」：100 万円/回

※調査対象端末 500 台（Windows 端末）の場合。

## 4. 提供範囲および提供開始日

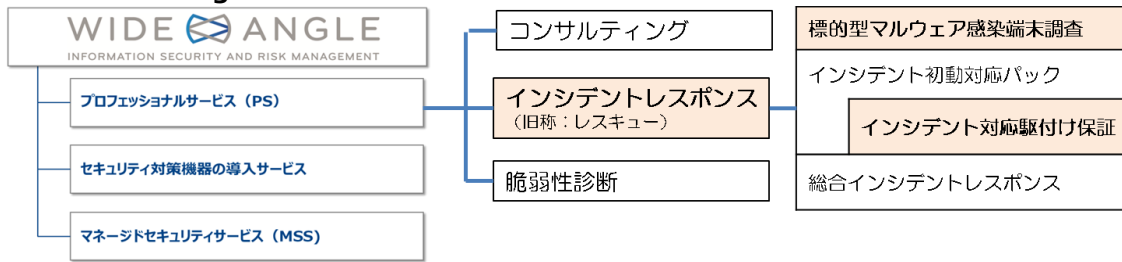
日本国内にて、2016 年 10 月 3 日より提供開始予定

(記載されている会社名および商品名は、各社の登録商標または商標です)

- \*1：当社調べ。人工知能を搭載の SIEM エンジンを活用したマネージドセキュリティサービスと連携した 24 時間以内駆付け保証サービスの提供は日本初。
- \*2：お客さまからの申告を当社が受けたタイミングが起点となります。
- \*3：「WideAngle プロフェッショナルサービス」における「レスキューサービス」について、2016 年 10 月より、サービス名を「インシデントレスポンス」に変更します。

<別紙>

(1) 「WideAngle」サービスの概要



(2) 「インシデントレスポンス」サービスのメニュー拡充について

