News Release

2017 年 7 月 19 日

サイバーセキュリティに関する情報分析など
専門性の高い業務を支援する「アドバイザリーサポート」を提供開始

～「WideAngle」の「プロフェッショナルサービス」において、
お客さま企業の CSIRT への総合支援を強化～

NTT コミュニケーションズ株式会社(以下：NTT Com)は、2017 年 7 月 19 日より、総合リスクマネジメントサービス「WideAngle」の「プロフェッショナルサービス」において、新メニュー「アドバイザリーサポート」の提供を開始します。

本メニューにて、お客さま企業の CSIRT※1 における重要な役割である、サイバーセキュリティに関する情報収集/調査/分析などの専門性の高い業務を、NTT Com がサポートすることで、人材不足の解消や、巧妙かつ悪質なサイバー攻撃に対して迅速に対応可能なリスクマネジメント体制の実現ができます。

1.背景

世界中で報道されたランサムウェア※2「WannaCry」※3 など、サイバー攻撃の巧妙化・悪質化とセキュリティインシデント発生による事業影響度の増大に伴い、お客さま企業内では CSIRT を設置し、リスクマネジメントを強化しています。

多岐にわたる CSIRT の役割の中でも特に重要なポイントは、自社の情報セキュリティ対策の弱点把握・強化方針決定をはじめ、次々と顕在化するサイバー脅威への事前準備や、セキュリティインシデント発生時の迅速かつ的確な初動対応などセキュリティインシデントの発生を未然に防ぎ、被害を最小化することです。そのため、サイバーセキュリティに関する情報を収集・調査し、分析する業務が鍵となってきます。（別紙 1）

一方、それらの業務において、さまざまな情報が混在するインターネットなどから、有用かつ信頼性の高い情報ソースを抽出し、タイムリーに分析するには、高度な専門知識やノウハウに加えて、迅速かつ的確な対応スキルが求められます。こうした中、お客さま企業では、自社で対応するためのスキル習得や人材確保など、リソース不足が課題となっていました。

2.概要

NTT Com は、お客さま企業の CSIRT 運用支援をさらに強化するため、「WideAngle」の「プロフェッショナルサービス」を再構成し、「CSIRT 運用支援ソリューション」を新設します。

本ソリューションの新メニューとして、国内外合わせて約 30 年間で約 10,000 件の企業およ

NTT コミュニケーションズ株式会社　広報室
NTT Communications Corporation　Public Relations Office
〒100-8019　東京都千代田区内幸町 1-1-6
1-1-6 Uchisaiwai-cho, Chiyoda-ku, Tokyo 100-8019, Japan
Tel (03)6700-4010 International +81 3 6700 4010

び公共団体などのセキュリティ管理体制への支援実績を活かした「アドバイザリーサポート」の提供を開始します。

（別紙 2）

アドバイザリーサポートにおけるお問い合わせ対応例：

・セキュリティイベント/セキュリティトピック/セキュリティトレンドの調査
・脅威情報/脆弱性情報/攻撃者のプロファイル情報/スレットインテリジェンス※4 の把握
・国際情勢やメディア情報の分析
・お客さま企業のシステム内で検知した不審なメールや、お客さま企業の Web サイトのセキュリティに関するお問い合わせ

3. 提供価格（税別）

初期費用：0 円、年間費用 300 万円（年間 24 チケットの場合）
※平日日勤帯にメールや電話などで、受付および回答を実施し、月次報告書を別途提供。
※お客さまのご要望による報告会を実施する場合は別途有償。

4. 提供範囲および提供開始日

日本国内にて 2017 年 7 月 19 日より提供開始

5.今後の予定

NTT Com は、お客さま企業 CSIRT の高度化を実現するため、「CSIRT 運用支援ソリューション」を、より一層拡充していきます。また、開発中の「脆弱性マネジメントプラットフォーム（仮称）」では、お客さま企業内の様々な組織で設置している ICT システムの情報をあらかじめデータベース化しておき、脆弱性情報が公開された際、該当するシステムを自動抽出し、システム管理者に随時通知する機能を提供予定です。

NTT Com は、引き続き、脆弱性情報への対応状況を一元的かつ効率的に管理できる仕組みを実現していきます。

※1　CSIRT：Computer Security Incident Response Team の略。コンピューターシステムなどに保安上の脅威（セキュリティインシデント）が発生した際に対応する組織。

※2　ランサムウェア：コンピューターウイルスの一種。感染したコンピューターを復旧するためとして、不当な料金請求をするソフトウエア。身の代金型ウイルス。

※3　WannaCry：一般的なランサムウェアの機能に加え、SMBv1 の脆弱性（MS17-010）を悪用することでネットワーク上のほかの PC に感染する機能を有する。

※4　スレットインテリジェンス:サイバーリスクの分析において得られる価値ある洞察およびそれを収集するプロセス

【別紙1】お客さま企業のCSIRTによるセキュリティ管理体制（参考モデル）

◆ インシデント発生を前提としたセキュリティ管理体制

情報収集

- 自社システムの構成情報(インターネット接続の有無など)をデータベース化
- セキュリティインシデント、脆弱性情報やその影響範囲などを情報収集

脆弱性管理などの事前対策

- 自社システムの防御機能や、監視強化すべきポイントの確認
- 自社システムに対して、定期・随時で脆弱性診断を行い、脆弱性を発見した場合は、マルウェア感染の調査や、システム改修を実施

インシデント発生

事実の把握と迅速対応

- 事実に基づく正確な情報を再調査し、経営層に状況報告
- 自社システムへの影響有無を判断し、迅速に対策を講じる
- 自社システムの構成情報に基づき、再点検の実施

CSIRT運用支援ソリューション

WIDE ANGLE
INFORMATION SECURITY AND RISK MANAGEMENT

アドバイザリーサポート

脆弱性診断

インシデント
レスポンス

脆弱性マネジメントプラットフォーム(仮称)

【別紙2】WideAngle プロフェッショナルサービス 各メニューの詳細

サービス	サービスメニュー	メニュー	内容	提供状況
プロフェッショナルサービス	総合コンサルティング		お客様ICT環境の「ガバナンス」「リスク」「コンプライアンス」に関わる各種サポートを提供 ・セキュリティポリシー作成支援 ・システムリスクアセスメント ・セキュリティプランニング支援 ・CSIRT/SOC 構築支援 ・インテリジェンス導入支援　など	提供中
	CSIRT運用支援ソリューション	インシデントレスポンス	総合インシデントレスポンス	緊急事態にエンジニアが調査・分析を実施初動対応、調査分析、改善提案まで提供	
			インシデント初動対応パック	情報の整理、事象の把握と調査、被害の拡大防止までを実施	
			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	
		脆弱性診断	プラットフォーム脆弱性診断	OSやミドルウェアなどの脆弱性を検出、リスクを可視化	
			Webアプリケーション脆弱性診断	Webアプリケーションの脆弱性を検出、リスクを可視化	
			セルフ脆弱性診断	脆弱性診断をお客様自身で行う環境を提供	
	アドバイザリーサポート			WideAngleで蓄積された高度な専門知識や調査分析のノウハウを活かし、サイバー情報収集/調査/分析を代行	2017/7/19 提供開始
	脆弱性マネジメントプラットフォーム(仮称)			社内/NTTグループのシステム脆弱性管理業務のノウハウを展開し、システム情報管理、脆弱性検出/通知/診断、対策/リスク管理機能をプラットフォームサービスとして提供	開発中

凡例：

提供中
メニュー再構成
新メニュー