ＮＴＴアドバンステクノロジ
組織内CSIRT向け「インシデント対応リモート支援サービス」

駆け付け時間が不要なリモート支援により インシデント被害の収束をより迅速にサポート

NTTアドバンステクノロジ（以下、NTT-AT）は、昨今のサイバー攻撃による被害の増加に伴い、
各企業や団体において体制整備が進むセキュリティインシデント対応の専門チームCSIRT向けに、
エンドポイントのログ解析とSOCや外部組織への報告に関し、
専門家がリモートで支援する「インシデント対応リモート支援サービス」を提供しています。

組織内CSIRTで想定される課題の解決を支援する「インシデント対応リモート支援サービス」

現代のビジネスシーンにおいては、業種・業態を問わずネットに頼らざるを得ない状況になっており、サイバー攻撃に遭わない確率は、ほぼ皆無といえます。このような状況を考慮し、セキュリティインシデント発生時の対応を専門とするCSIRT（Computer Security Incident Response Team）を設立する企業が相次いでいます。

CSIRTの最大の役割は、「被害極小化のための迅速な対応（レスポンス）」、および「収束までのインシデントハンドリング」ですが、実際にインシデントが発生した場合、CSIRTには次のような懸念事項が想定されます。

- どのように初動対応すればよいのか分からない…
- インシデント調査の技術力に不安…
- 技術力のある要員確保ができない…
- 技術者の養成には時間がかかる…
- どのように報告すればよいのか分からない…
- 研修しても実際に起きたら役に立たないのでは…
- 現場駆け付け対応では手遅れではないか…

NTT-ATが本年3月から提供開始した組織内CSIRT向け「インシデント対応リモート支援サービス」は、このような課題を踏まえながら、NTT研究所の支援で培った高度な技術を用いて、組織内CSIRTに求められる専門的なエンドポイントのログ分析と外部組織への報告をリモートで支援するサービスです。

インシデント対応スペシャリストが状況の解析をリモートで支援

NTT-ATでは、これまで企業・自治体のインシデント対応を実際に行ってきた実績とICT-24SOCに高度なセキュリティ技術を備えた技術者を有してきました。これらの技術やノウハウを生かし、組織内CSIRTに求められる専門的なエンドポイントのログ解析と外部組織に対して必要な報告を

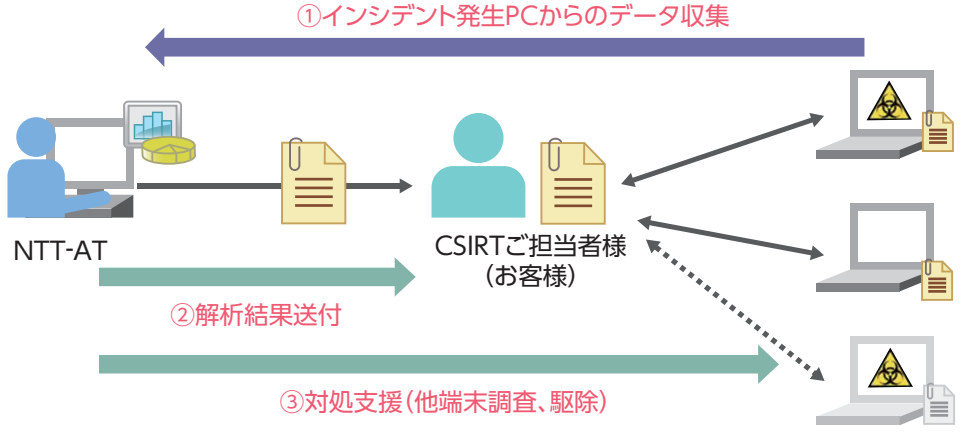

図1　支援サービスの流れ

インシデント対応スペシャリストがリモートで支援する「インシデント対応リモート支援サービス」の提供を開始しました。

本支援サービスは、SOC や外部組織からインシデント通知や指摘があった後、お客様の CSIRT の役割である分析・報告に関して NTT-AT のインシデント対応スペシャリストがリモートから支援していくサービスです。弊社指定のインシデントレスポンス支援ツール（EDR 製品）をお客様の PC に事前に導入していただくことにより、SOC や外部組織から連絡後、迅速な CSIRT リモート支援が可能になります。支援ツールとなる EDR（Endpoint Detection and Response）製品とは、エンドポイント（= PC）がマルウェアに感染した場合を想定した対策として昨今注目されている製品で、感染後の対応を迅速に行うために必要なインシデントレスポンスを支援するさまざまな機能を備えています。

図 1 は本支援サービスの流れを示しものです。①お客様にネットワークの監視拠点などの外部拠点から異常検知の連絡があった後、EDR 製品を通じて PC からログやメモリなどのデータを取得します。②取得したデータからウイルスの特定や被害状況を解析し、その結果をお客様に送付します。③お客様に報告した結果に基づき、対処方法を支援します。

駆け付け時間がゼロ！ インシデント状況を迅速に解析してレポートを提供

本支援サービスの特徴として次の 2 点があげられます。

・インシデント状況を迅速に解析しレポートを提供
・解析に必要なログを簡単に取得できるツールを提供

また、必要に応じてオンサイト支援も行えるよう、オプションサービスも用意しています。

「現地駆け付け支援サービス」は、インシデント発生直後に専門スタッフが現地に駆け付け、ログ分析・データ保全・簡易フォレンジック等を迅速に実施し、証拠の保全と二次被害を防止するサービスです。

「デジタルフォレンジック解析サービス」は、インシデント発生直後、該当する HDD 等をフォレンジック専用の解析装置で保全・分析し、インシデント発生時の技術的詳細を明らかにするサービスです。

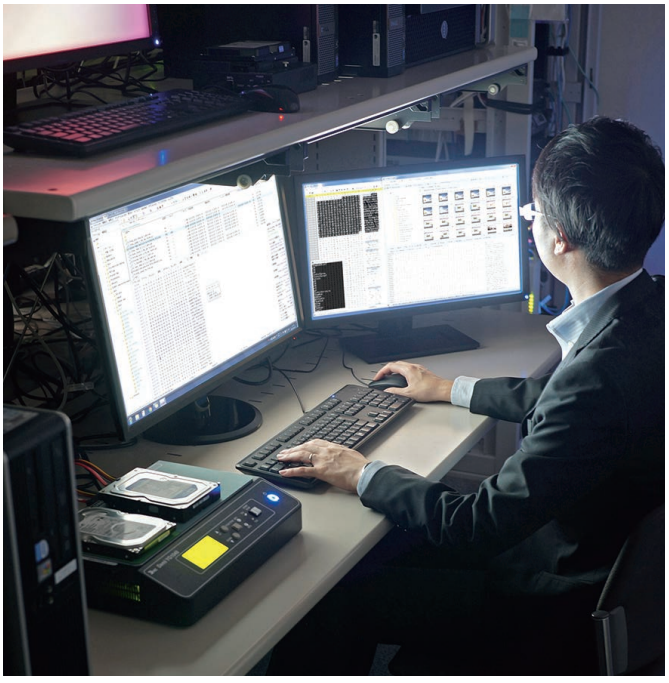
図2　支援サービスの提供イメージ

「インシデント対応リモート支援サービス」の価格は、1,000 クライアントの場合、初期費用は 125,000 円～（税抜）、サービス利用料金は月額 225,000 円～（税抜）です。契約期間は年単位となります。

近年のサイバー攻撃によるセキュリティインシデントは自然災害と同様、いつ被害に遭っても不思議ではない状況です。本サービスは、専門家による解析を即時提供することで、今まで時間を要していたマルウェアの拡散状況などもいち早く把握することができ、お客様の一刻も早いインシデント終息をご支援します。

ＮＴＴアドバンステクノロジ
セキュリティ事業本部　マネージドサービスビジネスユニット
サイバークライムアナリスト　**越谷 淳平**

お問い合わせ先

NTTアドバンステクノロジ株式会社　商品お問い合わせセンタ
TEL：0120-057-601　E-mail：sales@ml.ntt-at.co.jp

※http://www.bcm.co.jp/でも閲覧できます。