NRI グループからのお知らせ
Notification from NRI Group

Nomura Research Institute Group

2021 年 2 月 10 日
NRI セキュアテクノロジーズ株式会社

NRI セキュア、「マネージド EDR サービス」を拡充し、マルウェアに感染した PC やサーバの復旧をリモートで支援可能に

～「復旧支援対応」と「ログ長期保存対応」の 2 機能を追加～

NRI セキュアテクノロジーズ株式会社（以下「NRI セキュア」）は、エンドポイント端末などを監視し情報システムのセキュリティ向上を図る「マネージド EDR サービス（以下「本サービス」）」に「復旧支援対応」「ログ長期保存対応」機能を追加し、本日提供を開始します。

本サービスは、PC やサーバ等のエンドポイント端末に導入した EDR 製品[1]を、NRI セキュアが企業に代わって管理・運用し、マルウェア[2]感染をはじめとするセキュリティインシデント（事故・事案）の予防や早期検知、インシデント対応までを一気通貫で提供します。

コロナ禍でリモートワークが拡大する一方、国内外の移動が困難な状況が続いています。「インシデント発生後の復旧まで支援してほしい」という多くのニーズに応え、感染した端末をリモートで復旧させる「復旧支援対応」機能を実装しました。さらに、金融情報システムセンター（FISC）、PCI SSC[3]、政府機関等のガイドラインや法制度に基づく各社のセキュリティ要件に対応するため、EDR 製品が取得した、ユーザの操作や端末の挙動に関するログを長期間保存できる「ログ長期保存対応」機能を追加しました。

2 つの機能の概要と特長は、下記の通りです。

■ 端末に残存する脅威をリモートで除去する「復旧支援対応」

従来、本サービスの提供範囲は平時のログ監視から、マルウェアなどに感染した端末をネットワークから隔離し、被害状況などの詳細を調査する「ファスト・フォレンジック」[4]までででした。

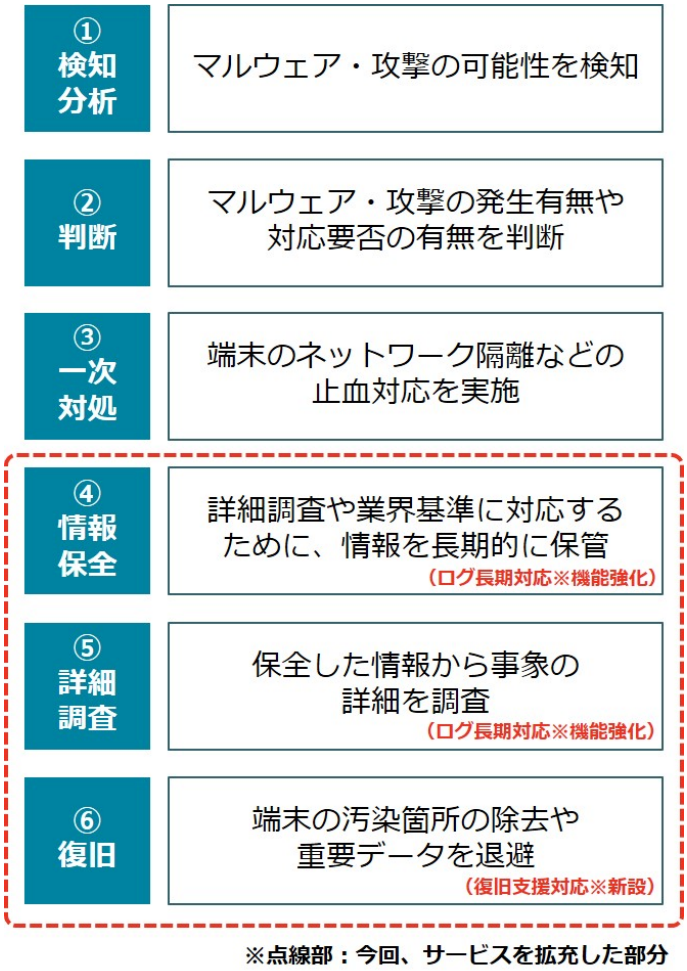
新たに実装した「復旧支援対応」機能では、NRI セキュアのインシデント対応の専門家が、感染した端末に残存する悪性ファイルの除去や改ざんされたレジストリの修正等を、リモートで実施します。これにより、不正アクセスをはじめとするサイバー攻撃の被害に遭い、マルウェアなどに感染してしまった場合にも、感染端末の速やかな利用再開を期待でき、迅速な業務復旧につなげられます。

■ 各種基準に対応した「ログ長期保存対応」

通常、EDR 製品の膨大なログはクラウド上の管理コンソールで保管され、契約している製品ライセンスごとに定義された期間が経過すると自動的に削除されます。一般的な保管期間は、おおよそ 3 か月以内で、政府機関などが推奨する基準や各社のセキュリティ要件を満たさない場合もあります。

この機能を用いることで、EDR 製品のログをダウンロードし、任意の期間の個別保管を可能にします。これにより、各種の基準や要件に対応できるようになります。また、ログ情報を活用して、過去に発生したインシデントを調査することも可能です（調査料金は、別途個別見積となります）。

図：2 つの機能を追加した本サービスの全体像



※点線部：今回、サービスを拡充した部分

本サービスの詳細については、次の Web サイトをご参照ください。

https://www.nri-secure.co.jp/service/mss/edr

NRI セキュアは今後も、企業・組織の情報セキュリティ対策を支援するさまざまな製品・サービスを提供し、グローバルな規模で安全・安心な情報システム環境と社会の実現に貢献していきます。

1 EDR 製品：
Endpoint Detection and Response の略。主にエンドポイント端末におけるインシデント発生後の対応を、明確化・迅速化する機能を持つセキュリティ対策製品のことです。

2 マルウェア：
不正かつ有害な動作を行う意図で作成されたソフトウェアや悪質なコードの総称で、ウイルス、トロイの木馬などを含みます。

3 PCI SSC：
PCI Security Standards Council の略。国際カードブランドである JCB、Visa、MasterCard、American Express、Discover の 5 社によって 2006 年に設立された団体のことです。

4 ファスト・フォレンジック：
フォレンジックとは、元々「鑑識」「科学捜査」の意味で使われる言葉ですが、情報セキュリティ分野では、セキュリティ事故や犯罪が起きた際に、端末やネットワーク内の情報を収集し、被害状況の解明や犯罪捜査に必要な法的証拠を明らかにする取り組みを指します。NRI セキュアの「ファスト・フォレンジック」では、従来型の調査よりも、迅速なフォレンジック調査を提供しています。

【お知らせに関するお問い合わせ先】
NRI セキュアテクノロジーズ株式会社　広報担当
TEL：03-6706-0622　E-mail：info@nri-secure.co.jp