Nomura Research Institute Group

NEWS RELEASE

2020 年 6 月 25 日

NRI セキュアテクノロジーズ株式会社

NRI セキュア、工場向けに特化したセキュリティ教育・インシデント対応訓練プログラムを提供開始

NRI セキュアテクノロジーズ株式会社（本社：東京都千代田区、社長：小田島 潤、以下「NRI セキュア」）は、「工場向けセキュリティ教育・インシデント対応訓練プログラム（以下「本プログラム」）」の提供を、本日開始します。各工場の事情に合わせて作成したシナリオを用いて、現場従業員のセキュリティ意識と、サイバー攻撃によって発生するセキュリティインシデント（事故・事案）への対応力の向上を支援します。

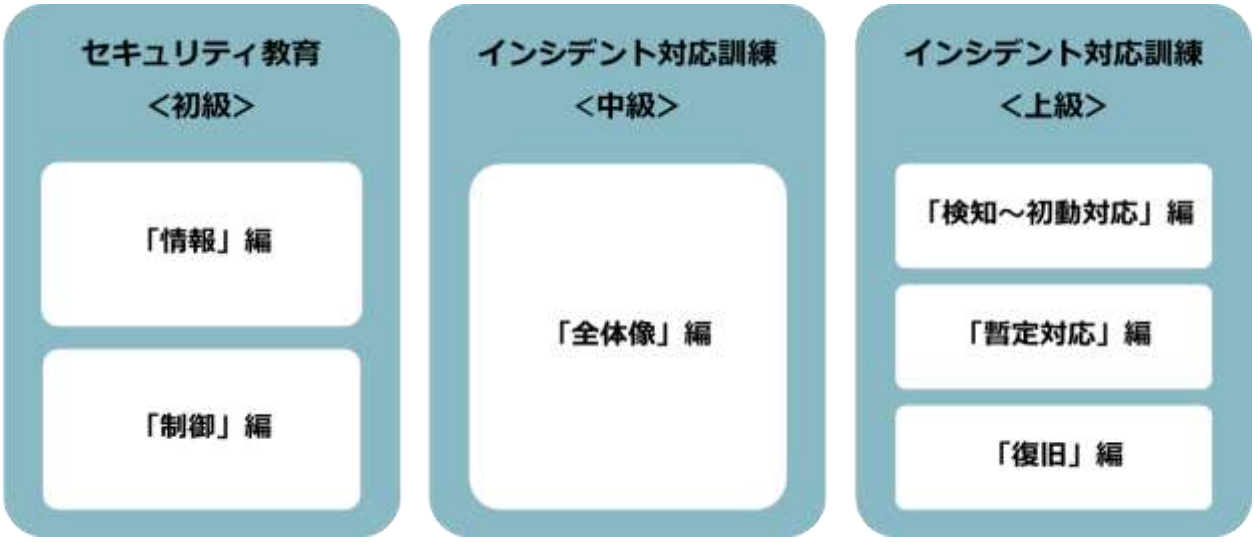
スマートファクトリー[1]の登場や IoT（モノのインターネット）の進展により、工場の制御システムが、サイバー攻撃の標的となる危険性が高まっています。実際、生産設備を狙ったマルウェア[2]に感染した結果、工場の稼働が停止してしまう事案などが、国内外で増加傾向にあります。

そのため、工場のサイバーセキュリティ対策を検討する企業が増えていますが、サイバー攻撃に対する問題意識には、工場や本社のセキュリティ管理部門と生産現場の間に差があり、生産現場におけるセキュリティ体制の整備や従業員への教育が不十分な状況が見られます。工場でセキュリティインシデントが発生した際に、いかに被害の拡大を極小化し、迅速な復旧につなげられるように準備しておくかが、企業の事業継続を左右します。このような背景から、NRI セキュアはこれまでの経験やノウハウをもとに、本プログラムを開発しました。

■本プログラムの概要

本プログラムは、初級・中級・上級と 3 つのレベルに分かれています。初級は従業員への「セキュリティ教育」、中級・上級は「インシデント対応訓練」で構成されており、各工場の実情や要望に合ったレベルを選択することが可能です（図 1）。

図１：「工場向けセキュリティ教育・インシデント対応訓練プログラム」の構成



現場担当者向けセキュリティ教育（初級）

生産現場の担当者向けのセキュリティ教育プログラムです。情報セキュリティの基礎知識や工場設備を狙った最新のサイバー攻撃動向などについて、インシデント対応訓練を実施する前に学ぶことで、訓練の理解度が向上し、インシデント発生時の対応力の強化を図ることができます。また、社内のセキュリティポリシーや規程などで定める手順について教育コンテンツを作成することも可能です。なお、このセキュリティ教育プログラムは、中級・上級のプログラムを導入される企業へのオプションサービスです。

工場特化型インシデント対応訓練（中級・上級）

訓練対象となる工場の特性を踏まえ、発生可能性の高いサイバー攻撃手法を選定した上で訓練シナリオを作成します。シナリオをもとに、セキュリティインシデントが発生した際の対応について、机上訓練を中心に学ぶことができます。なお、インシデント対応の全体像を把握することに主眼を置いた中級の訓練を行った後、個別の部署単位で、インシデントの検知や初動対応、暫定対応、復旧など、より具体的な対応について定期的に訓練を実施することを推奨しています。

インシデント対応訓練のおもな特長は、以下の３点です。

① 各工場の特性に合わせ、発生しうるサイバー攻撃を机上訓練で再現

シナリオには、インシデントの発生原因が、装置の故障かサイバー攻撃によるものかについての判断や、生産ラインの停止要否の判断、本社機構との連携、復旧見込みと在庫の調整など、工場特有の事情に合わせた要素が盛りこまれています。さらに、シナリオは各工場の生産設備やネットワークの特性に合わせてカスタマイズできるほか、開発環境や模擬環境を用いた実機訓練についても対応が可能です。

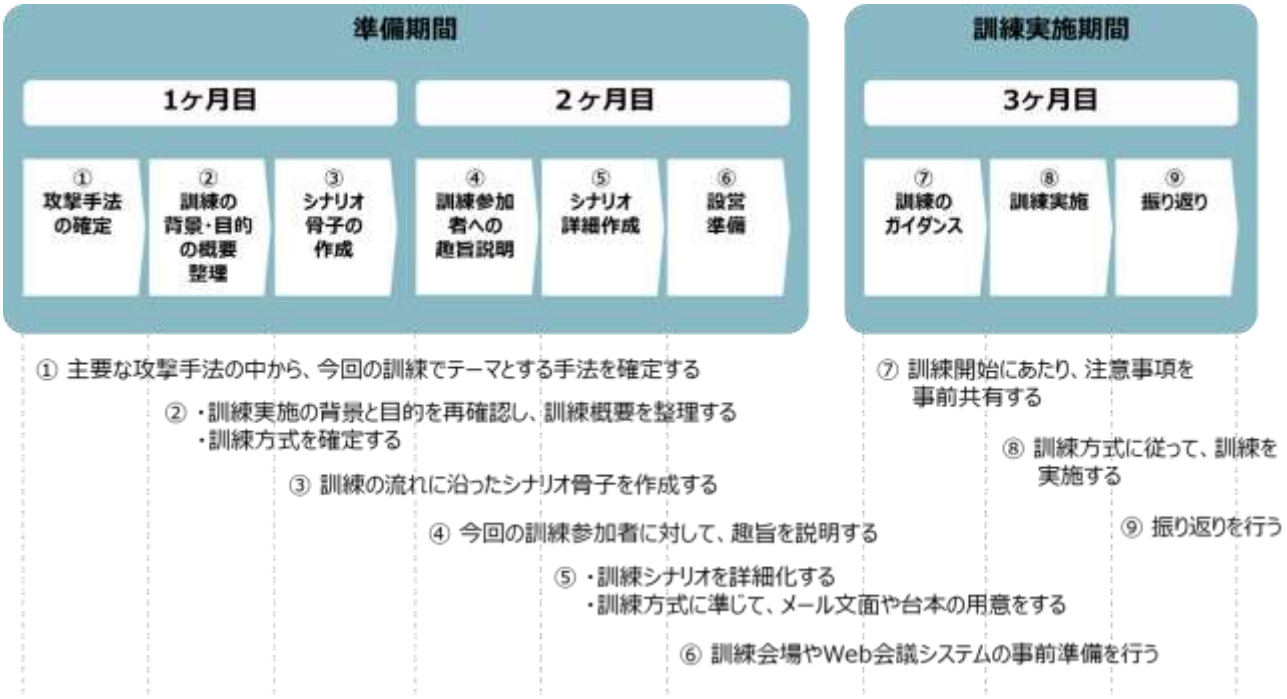
② リモートワークに対応

Web 会議システムやメール等を利用して、訓練を実施することが可能です。参加者全員が一堂に集まらずに、複数の拠点や在宅で訓練を実施することができます。

③ 訓練後の振り返り

訓練後に行う振り返りでは、訓練で浮き彫りになった課題を抽出し、実際にインシデントが発生した場合に、迅速かつ正確に対応するため、ベストプラクティスとして期待される行動を解説します。ご要望に応じて、経営層に報告することも可能です（図 2）。

図 2 ：インシデント対応訓練の流れ



おおよそ 2 カ月間を準備期間として想定しています。本プログラムの費用は、インシデント対応訓練 1 回あたり、200 万円からです（税抜）。なお、初級のセキュリティ教育については、個別にお見積りをします。

本サービスの詳細については、以下の Web サイトをご参照ください。

https://www.nri-secure.co.jp/service/consulting/factory-training

NRI セキュアは、これまでも工場や IoT のセキュリティの確保・向上に特化したサービスを提供してきました（サービス一覧は、末尾の「ご参考」を参照）。今後も、企業・組織のサイバーセキュリティ対策を支援することで、安全・安心な社会基盤・産業基盤の実現に貢献していきます。

[1] スマートファクトリー：工場内のあらゆる機器や設備、工場内で人が行う作業のデータを、センサーなどを活用して取得・収集し、それらのデータを分析・活用することで新たな付加価値を生み出せるようにする工場のこと。

[2] マルウェア：悪意のあるプログラムのこと。

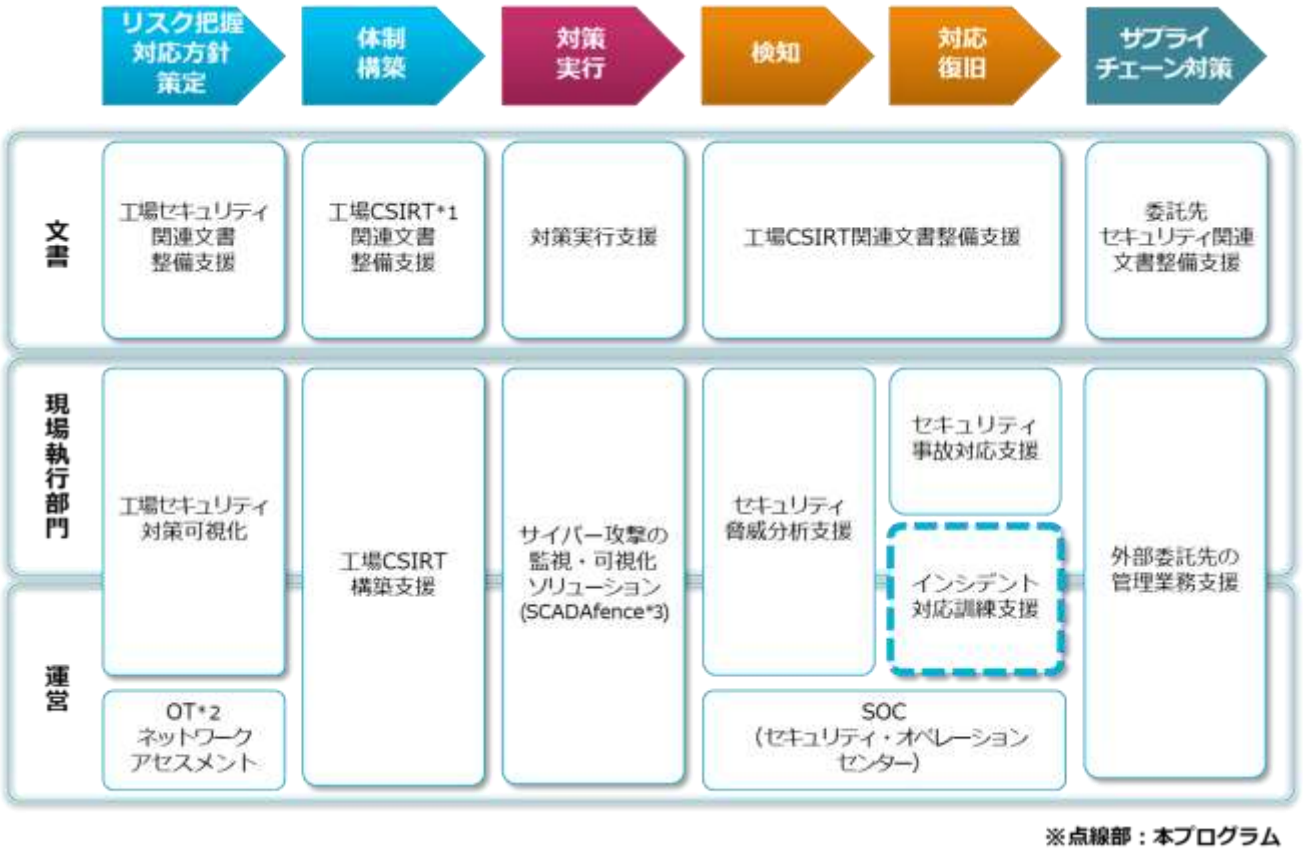
【ニュースリリースに関するお問い合わせ先】

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

【ご参考】

■ NRI セキュアが提供する、工場向けサイバーセキュリティ対策支援サービスの一覧



※点線部：本プログラム

*1　CSIRT：Computer Security Incident Response Team の略。サイバー攻撃に対応するための専門チームのこと。支援内容の詳細については、「CSIRT 総合支援サービス」の Web サイトをご参照ください。https://www.nri-secure.co.jp/service/consulting/csirt

*2　OT：Operational Technology の略。工場やビルなどの制御システムのこと。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/assessment/ot_network

*3　SCADAfence：イスラエルのサイバーセキュリティ企業 SCADAfence, Ltd.が開発した、工場やビル内のネットワークを監視し、不審な通信を検知してセキュリティ担当者に通知するソリューション「SCADAfence プラットフォーム」のこと。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/solution/scadafence