2018年4月25日
三菱重工業株式会社
日本電信電話株式会社
株式会社NTTデータ
NTTコミュニケーションズ株式会社

制御システムの安心・安全な運用を実現する サイバーセキュリティ技術「InteRSePT®」の販売を開始

～運転状態ごとの高機能セキュリティ対策が低コスト・省スペースで可能に～

三菱重工業株式会社（本社：東京都港区、代表取締役社長 宮永 俊一、以下 三菱重工）と日本電信電話株式会社（本社：東京都千代田区、代表取締役社長 鵜浦 博夫、以下 NTT）、株式会社NTTデータ（本社：東京都江東区、代表取締役社長：岩本 敏男、以下 NTTデータ）、およびNTTコミュニケーションズ株式会社（本社：東京都千代田区、代表取締役社長：庄司 哲也、以下 NTT Com）は、三菱重工とNTTが共同開発を進めてきた重要なインフラ（社会基盤）などの制御システム向けサイバーセキュリティ技術「InteRSePT®」※1を製品化し、2018年5月より販売を開始します。未知のサイバー攻撃に対するリアルタイムの異常検知および対処を可能とし、安心・安全なシステム運用を実現に貢献します。火力発電設備や化学プラントなどの可用性※2が重視される民需分野を積極開拓していきます。

1. これまでの経緯

これまで発達してきたマルウェア※3やDDoS攻撃※4のようなサイバー攻撃に対するセキュリティ対策であるIDS・IPS※5、FW※6に加え、近年は、攻撃対象機器の動作特性や制御指令を監視し、指令送信のタイミングや指令内容の一部を改変して、対象機器を故障させる高度なサイバー攻撃への新たな対策が求められています。

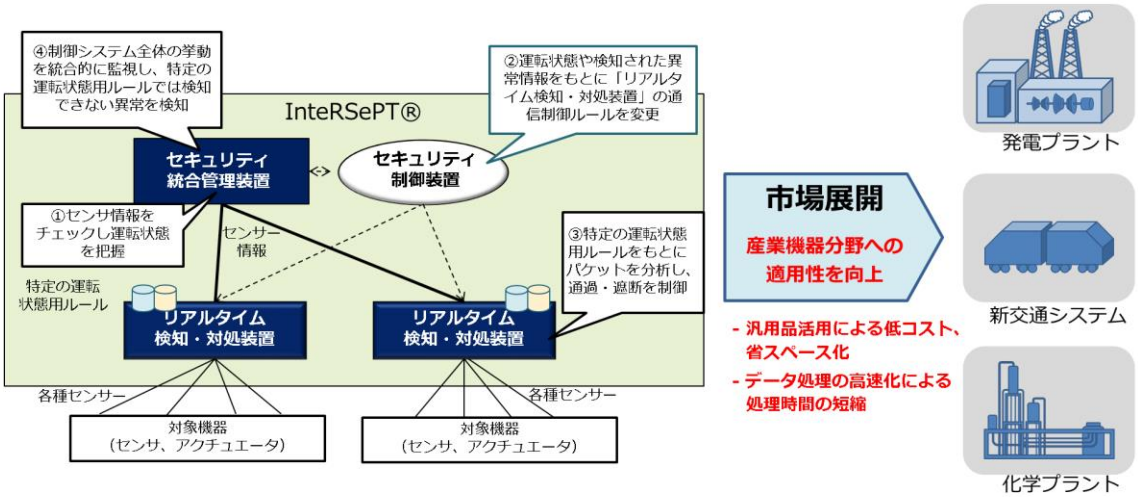
三菱重工とNTTグループは、このようなニーズの高まりに対応するため、2016年3月にセキュリティ技術の研究開発を開始、同年11月には、三菱重工が防衛・宇宙分野で培った信頼性および安全性の高い制御技術と、NTT研究所が保有するセキュリティ統合管理・制御技術研※7を組み合わせることにより、「InteRSePT®」の試作を完成させました。

その後、東京都内にある三菱重工のセキュリティ開発・実証拠点「サイバーラボ」で試作の評価および制御システムへの適合性検証を行い、「InteRSePT®」のさらなる高度化およびO&M（運用およびメンテナンス）ビジネスへの適用範囲の拡大をはかった結果、今回の製品化、ならびに販売開始に至ったものです。

2. 「InteRSePT®」の特徴

「InteRSePT®」は、「リアルタイム検知・対処装置」と「セキュリティ統合管理装置」で構成され、ネットワークに流れるリアルタイムのデータを統合的に監視し、従来の技術では対応が困難だった制御指令を悪用したサイバー攻撃を検知します。対象機器の運転状態ごとにリアルタイムに適用するセキュリティルールを変更することで異常を早期に発見し、可用性を維持しながら未知のサイバー攻撃にも迅速に対応可能になります（共同特許出願中）。

また、「InteRSePT®」はネットワークの細部まで確認することができ、多様な産業設備・機器に対する適合性に優れています。



「InteRSePT®」イメージ図

①制御システムのネットワークに流れるセンサー情報などのパケットを収集・分析して運転状態を把握。
②運転状態などに応じて「リアルタイム検知・対処装置」における通信制御ルールを変更。
③ルールにもとづいてパケットを分析し、通過・遮断を制御。
④複数のセンサー情報を「セキュリティ統合管理装置」に集約し、制御システム全体の挙動を統合的に監視（ふるまい検知処理※8）することで異常を早期発見し、未知のサイバー攻撃にも迅速に対応。

3. 製品化にあたり

リアルタイム検知・対処装置には汎用ハードウェアを採用し、併せてネットワークスイッチと一体化することにより、低コスト・省スペース化を実現し、システム導入を容易にしました。併せて、セキュリティ統合管理装置の処理を並列化することにより、ふるまい検知処理の高速化が可能となりました。

4. 各社の役割

三菱重工	「InteRSePT®」の販売/制御システムに応じたデータ分析・運転状態推定/異常検知手法、対処・復旧手法の開発および最適化設計。
NTT	NTT研究所が保有するセキュリティ統合管理・制御技術、およびリアルタイム検知・対処技術の提供。
NTTデータ	三菱重工とNTTグループで開発した「InteRSePT®」をベースとしたセキュリティ対策ソリューションの市場展開を支援。
NTT Com	「InteRSePT®」の製品化に向けて、NTT研究所のコア技術を市場に適用するために必要なデータ集積や異常検知に関する技術開発、およびセキュリティ対策ソリューションの商用化を実施。

5. 今後について

今後は、三菱重工とNTT、NTTデータおよびNTT Comの協業により「InteRSePT®」の低コスト・高機能性および高速処理能力、ならびに導入容易性をさまざまな業界に訴求し、個別のセキュリティ対策ソリューションを提案するとともに市場開拓を進めていきます。

さらに「InteRSePT®」で集約・解析したセンサー情報を、セキュリティ対策に加えて運転パラメータ最適化や故障予知による維持整備期間短縮などに有効活用し、顧客オペレーション効率向上に貢献するO&Mトータルソリューションビジネスとして展開を進めていきます。

※1 「InteRSePT®」は、Integrated Resilient Security and Proactive Technologyの略で、三菱重工の登録商標。
※2 可用性は、システムを停止することなく継続して稼働できる状態のこと。
※3 マルウェアは、Malware, Malicious Softwareの短縮語で悪意のあるソフトウェア。
※4 DDoS攻撃は、Distributed Denial of Service attack、分散型サービス拒否攻撃のこと。
※5 IDS・IPSは、Intrusion Detection System／Intrusion Protection Systemの短縮語で、侵入検知・防御システムのこと。
※6 FWは、FireWall、不正アクセス判別・遮断システム。
※7 セキュリティ統合管理・制御技術は、対象機器／システムの状態や異常発生のイベントなど、攻撃の検知にまつわる情報を収集・分析し、対処装置群を統合制御して多層的な防御を実現する技術のこと。
※8 ふるまい検知処理は、対象機器／システムのいつもの運転状態と異なる挙動を検知する処理のこと。