株式会社日本触媒

重要インフラ事業者としての
社会的責任を果たすため
Network IPS+MSSを導入して
制御系システムのセキュリティーを強化

お客様情報

株式会社日本触媒 姫路製造所

株式会社日本触媒

●本社所在地
〒541-0043 大阪市中央区高麗橋4-1-1 興銀ビル
http://www.shokubai.co.jp/ja/

1941年の創業以来、自社開発の触媒技術を核に事業を拡大。化学メーカーとして、酸化エチレンやアクリル酸、自動車用・工業用触媒など、生活の身近なところで使われる製品や素材を世の中に送り出し、現在では、紙おむつに使われる高吸水性樹脂で世界1位のシェアを誇っている。また、グループ企業理念「TechnoAmenity:私たちはテクノロジーをもって人と社会に豊かさと快適さを提供します」を掲げ、グローバルな活動を展開している。

2014年5月に内閣サイバーセキュリティセンター（以下、NISC）が「重要インフラの情報セキュリティ対策に係る第3次行動計画」を決定し、化学分野が重要インフラ分野に追加されたことによって、新たに重要インフラ事業者となった株式会社日本触媒（以下、日本触媒）は、生産活動を司る制御系システムをサイバー攻撃の脅威から守るべく、IBM® Security Network Intrusion Prevention System（以下、Network IPS）およびIBM Managed Security Services（以下、MSS）を導入。社会に重大な影響を及ぼしかねないシステム停止のリスクを最小化しました。

国としての重要インフラを サイバー攻撃から守る責務を負う

独自開発の触媒技術を中心に事業を拡大する日本触媒の製品は電子情報材料や新エネルギーなどの分野にも広がるほか、特に紙おむつに使われる高吸水性樹脂では世界1位のシェアを誇っています。

そうした中で日本触媒が重視しているのが、1973年以来、社是として掲げている「安全が生産に優先する」という精神を受け継いだCSR（企業の社会的責任）の徹底です。同社のIT統括室長を務める野原　利夫氏は、「万が一、弊社の生産ラインが事故や過失などで停止した場合、紙おむつは言うまでもなく、サプライチェーンでつながっているハイテク製品や生活用品の市場に大きな混乱を招いてしまいます」と、その背景を話します。

そして2014年、NISCから示された「重要インフラの情報セキュリティ対策に係る第3次行動計画」に対応するため、日本触媒では安全対策のさらなる強化が急務となりました。

同行動計画は、国の重要インフラをサイバーテロなどの脅威から守るために、対象事業者が取り組むべき施策をとりまとめたものです。今回の第3次行動計画では、従来からの通信、電力、鉄道などに加え、化学や石油といった分野もその対象となりました。「こうした動きを察知して重要インフラ事業者となる1年前から、生産設備や装置を司る制御システムのセキュリティーを強化する準備を進めました」と野原氏は話します。

例えば、日本触媒の各製造所では、生産設備や装置の運転状況をヒューマン・マシーン・インターフェース（以下、HMI）と呼ばれるコンピューターによって常時モニタリングしているのですが、そこにもセキュリティー・リスクは存在します。同社エンジニアリング本部　エンジニアリング統括部の主任部員である青田　雅弘氏は、このように話します。

事例概要

課題

- 化学分野の重要インフラ事業者として、生産設備や装置を司る制御システムのセキュリティーを強化し、システム停止のリスクを最小化

ソリューション

- IBM Security Network Intrusion Prevention System
- IBM Managed Security Services

期待される効果

- サイバー攻撃による生産設備の全面停止のリスクを最小限に抑制
- マルウェア感染や不正侵入に対する防御の状況が「見える化」されたことで、明確な根拠を持って、安全性を立証

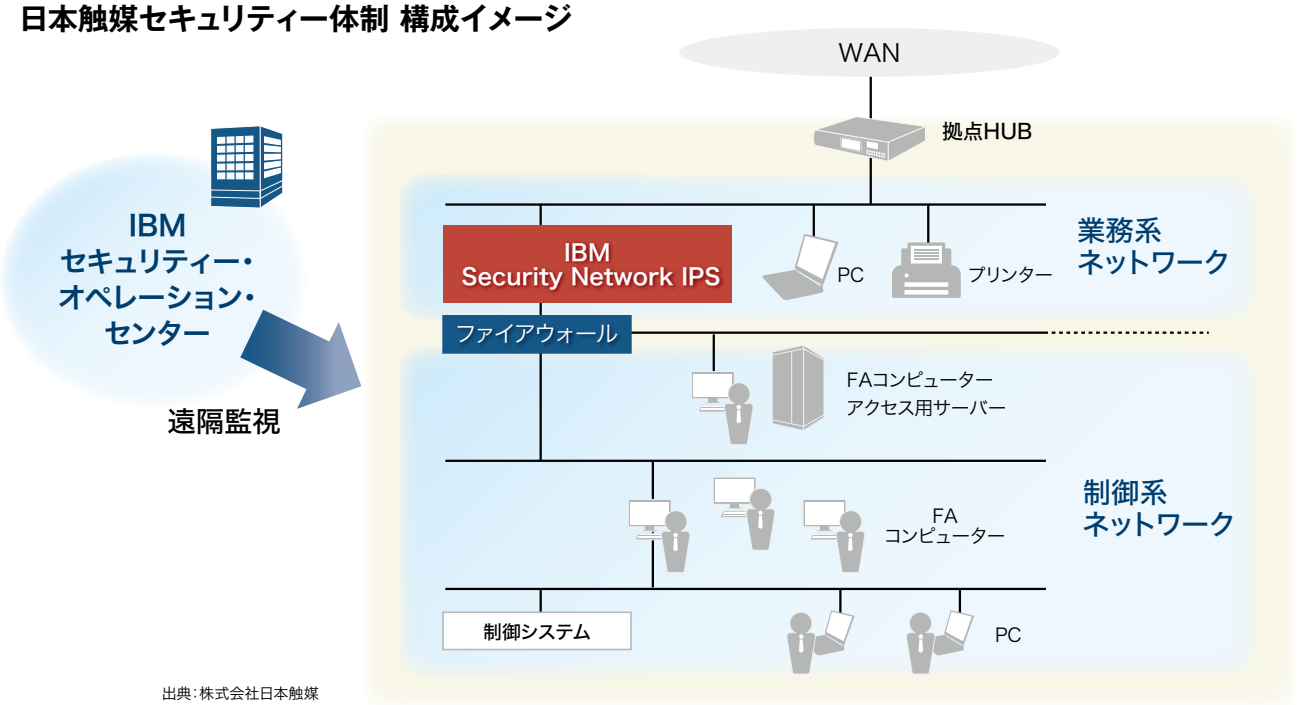
「一見すると専用機のHMIですが、実はその中身はWindowsベースの汎用的なコンピューターなのです。制御系システムのネットワークは業務系システムのネットワークから論理的に分離されており安全性を担保していますが、それでも外部からのサイバー攻撃は絶対にありえないとは言い切れません。仮にHMIがマルウェアに感染して正常なモニタリングを行えなくなった場合、生産設備や装置の電源を落としてシャットダウンせざるを得ない緊急事態となり、多大な被害が発生してしまいます」

セキュリティーの専門家による監視や集中管理が欠かせない

制御系システムのセキュリティー対策においても業務系システムと同様に「多層防御」の考え方が基本となります。日本触媒は当初、このソリューションを制御系システムのインテグレーションを手がけているベンダーに求めました。しかし、そこから得られた提案内容は同社の要件を十分に満たすものでありませんでした。「ファイアウォールやアンチ・ウィルスなどのセキュリティー対策製品については、制御系システムのベンダーからも調達することが可能です。ただし、それらの要素技術の効果を最大限に発揮させ、起こっているリスクを機械的に判断できないような困難な事象にも対処していくには、運用面のサポートが欠かせません。そうしたもうひとつの軸となる、セキュリティーの専門家による監視や集中管理といったサービスが十分ではなかったのです」と野原氏は話します。

そこで日本触媒が目を付けたのが、IBM Security Network Intrusion Prevention System（以下、Network IPS）とIBM Managed Security Services（以下、MSS）を利用したIBMのセキュリティー対策ソリューションです。

日本触媒セキュリティー体制 構成イメージ



出典：株式会社日本触媒

“重要インフラ事業者となる1年前から、生産設備や装置を司る制御システムのセキュリティーを強化する準備を進めました”

株式会社日本触媒
IT統括室長
野原 利夫氏

“IBMには、第三者としての視点に立った現状把握と評価、今後の社内規定に盛り込むべき項目の示唆、それを社内に定着させていくための施策の提案など、情報セキュリティー基準策定の幅広いコンサルティングをお願いできればと考えています”

株式会社日本触媒
エンジニアリング本部
エンジニアリング統括部
主任部員
青田 雅弘氏

“収集したデータの解析や分類を、IBMのセキュリティー・コンサルタントが的確にサポートしてくれたおかげで、短期間かつスムーズな正式運用への移行を実現することができました”

株式会社日本触媒
IT統括室
課長代理
奥山 忠士氏

Network IPSは、ワームからボットネット、データ・セキュリティー、Web アプリケーションまで、幅広く対応する先進機能を備えた侵入防御のアプライアンス機器。一方のMSSは、セキュリティー・オペレーション・センター（以下、SOC）において、24時間365日体制でサイバー攻撃の脅威から対象のシステムを守る監視サービスです。

これらのセキュリティー対策ソリューションの導入に至った経緯を、同社 IT統括室の課長代理である奥山 忠士氏は、次のように話します。

「防衛産業や個人情報を狙い撃ちにしたサイバー攻撃の脅威が大きな社会問題として顕在化した2011年に、弊社は業務系システムで先行してNetwork IPSとMSSを導入していました。以降3年以上にわたる高品質の運用実績を高く評価しており、制御系システムについてもやはりIBMに任せるのが安心という結論に至りました」

なかでも日本触媒が高く評価しているのが、Network IPSやMSSを背後から支えているIBM X-Forceの存在です。「最新のサイバー攻撃から未知の脅威までを分析する世界最大規模のセキュリティー研究開発チームであるIBM X-Forceの知見とノウハウで守られていることに、非常に大きな安心感があります」と奥山氏は話します。

高い安全性が維持されていることを明確な根拠を持って立証

こうして2015年1月に日本触媒の制御系システムに導入されたNetwork IPSは、MSSと合わせて同年3月より正式運用を開始しました。

「導入から最初の1カ月程度は、Network IPSをインライン・シミュレーション・モードで運用し、制御システムが外部とやりとりしても問題のないデータ、内部にとどめて保護しなければならないデータの切り分けを行いました。収集したデータの解析や分類を、IBMのセキュリティー・コンサルタントが的確にサポートしてくれたおかげで、短期間かつスムーズな正式運用への移行を実現することができました」と奥山氏は話します。

そして現在もNetwork IPSとMSSは、ますます悪質化するサイバー攻撃の脅威から、日本触媒の業務系システムおよび制御系システムを守り続けています。そうした中で野原氏は、次のような側面からもNetwork IPSとMSSの導入効果を話します。

「重要インフラ事業者としての責任を果たし、マルウェア感染や不正侵入をしっかり防御できているかどうか、先般も経済産業省から問い合わせを受けました。その際にも、高い安全性が維持されていることを、明確な根拠をもって説明することができました。もしNetwork IPSやMSSの仕組みがなかったとしたら、たとえサイバー攻撃は受けていないとしても立証することは困難で、社内的に大きな混乱が起こっていたかもしれません」

「制御系システムへのサイバー攻撃は生産活動の全面停止につながる危険性があります。仮にそのような事態が発生した場合、原因の追究、システムの復旧などで生産を再開するまでに3～7日といった長い時間がかかる可能性があります。Network IPSとMSSが運用を開始した現在は、サイバー攻撃によって、生産設備を停止するような重大なリスクがより一層低くなりました」と青田氏は話します。

全社的な課題意識を醸成すべく
情報セキュリティー基準の策定にあたる

「重要インフラの情報セキュリティ対策に係る第3次行動計画」では、重要インフラ事業者に対してサイバー攻撃への防御策の導入はもとより、情報セキュリティーに対するより高い課題意識と社内風土を醸成し、PDCAサイクルに基づいた継続的なリスクマネジメントの改善を求めています。
この要件に対応すべく日本触媒では現在、2015年度内を目標として全社的な情報セキュリティー基準（社内標準のセキュリティー・ポリシー）の策定を進めています。
野原氏が「経営者をはじめ、従業員一人一人の情報セキュリティー意識を変えていくことは簡単なことではなく、とても苦労しています」と話す一方で、「IBMには、第三者としての視点に立った現状把握と評価、今後の社内規定に盛り込むべき項目の示唆、それを社内に定着させていくための施策の提案など、情報セキュリティー基準策定の幅広いコンサルティングをお願いできればと考えています」と青田氏は話します。
野原氏と青田氏は「身近な相談役として、情報セキュリティーに関する多様な課題の解決に共にあたっていただければ」と、IBMに対する期待を寄せています。
情報セキュリティー対策は一過性のものであってはなりません。パートナーシップで強く結ばれた日本触媒とIBMは、さらなる安全を目指した取り組みを重ねています。

日本アイ・ビー・エム株式会社
〒103-8510　東京都中央区日本橋箱崎町19番21号

© Copyright IBM Japan, Ltd. 2015
All Rights Reserved
10-15 Printed in Japan

IBM、IBMロゴ、ibm.comおよびX-Forceは、世界の多くの国で登録されたInternational Business Machines Corporationの商標です。他の製品名およびサービス名等は、それぞれIBMまたは各社の商標である場合があります。現時点でのIBMの商標リストについては、www.ibm.com/legal/copytrade.shtmlをご覧ください。
Windowsは Microsoft Corporationの米国およびその他の国における商標です。
他の会社名、製品名およびサービス名等はそれぞれ各社の商標です。

このカタログに掲載されている情報は2015年10月のものです。事前の予告なしに変更する場合があります。
本事例中に記載の肩書きや数値、固有名詞等は初掲載当時のものであり、閲覧される時点では変更されている可能性があることをご了承ください。
事例は特定のお客様での事例であり、すべてのお客様について同様の効果を実現することが可能なわけではありません。
製品、サービスなどの詳細については、弊社もしくはIBMビジネスパートナーの営業担当員にご相談いただくか、以下のWebサイトをご覧ください。
ibm.com/security/jp