Kaspersky Industrial CyberSecurity NLMK の産業用インフラストラクチャ向けパイロットテストに合格

https://www.nlmk.com/en/

NLMK

鉄冶金

- 1934 年に設立
- NLMK 企業グループの 1 社
- リペツク（ロシア）
- ロシアの鉄鋼生産シェア：**18%**
- 生産能力：**1 年あたり 1,300 万トン以上の鉄鋼生産**

Novolipetsk Steel（NLMK）は、国際的な企業グループである NLMK Group の主要生産拠点であり、世界中で最もコスト効率に優れた冶金企業の 1 つです。ロシア、欧州、北米で、垂直統合されたビジネスモデルや資産を展開しています。

基本的な原料、エネルギー、および高度な技術を自給できる NLMK Group は、ロシアの冶金業界におけるトップ企業であり、世界の製鋼業者の上位 20 社の中で唯一のロシア企業でもあります。同グループの鉄鋼生産能力は、1 年あたり 1,700 万トンを超えています。

NLMK の工場では、NLMK Group の鉄鋼の総生産量の約 80% を担っています。Novolipetsk Steel での生産工程には、原料の加工から高級鋼材の製造まで、産業プロセスの全段階が含まれています。NLMK の高品質な鉄鋼製品は、建築、エンジニアリング、電力設備、洋上風力発電所などの幅広い業界で利用されています。

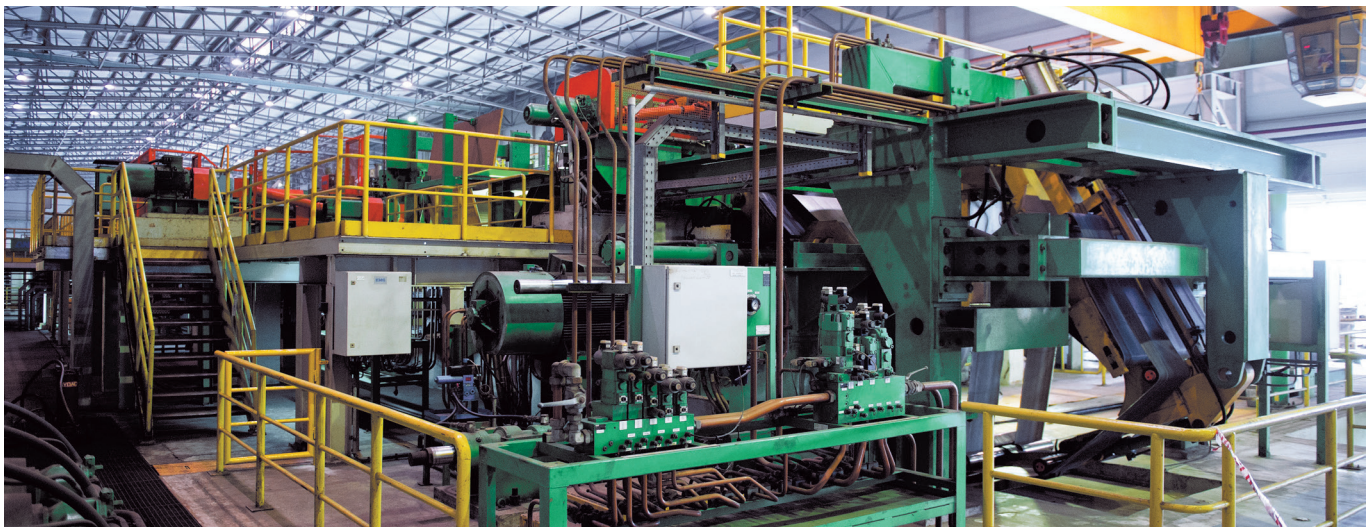
「私たちにとって、この NLMK のインフラストラクチャを保護するプロジェクトは、他では得られない価値ある経験でした。ICS の上層で仮想化が利用されていることから、興味深い技術的課題が複数発生しました。カスペルスキーのエキスパートは発生した課題に適切に対処しました。これらの課題は間違いなく、当社のソリューション開発に良い影響を与えてくれることでしょう。」

Georgy Shebuldayev、
Kaspersky Industrial CyberSecurity 責任者

課題

NLMK は Kaspersky Lab と共に、電磁鋼板の製造所で産業用制御システム（ICS）をサイバー攻撃から効果的に保護するためのパイロットプロジェクトを立ち上げました。

このプロジェクトで、NLMK は、地域的に分散された複数のデータセンターにある産業用制御システム（ICS）のコンピューティングリソースを統合して、1 つの最新のオートメーションインフラストラクチャを構築するタスクを実施しました。このアプローチによって、オートメーションシステムの信頼性が向上し、保守費用が削減されます。同時に、このアーキテクチャでは、明確なネットワーク境界を敷いて、オートメーションシステムから企業ネットワークへのデータ転送をセキュアに行うことが可能になり、ICS のサイバー攻撃に対する耐性が強化されます。



非侵入型ソリューション
Kaspersky Industrial CyberSecurity は事業継続性や産業プロセスの一貫性に影響を及ぼしません。

現実の攻撃シナリオ
Kaspersky Industrial CyberSecurity に統合されている技術は、さまざまな業界における、サイバー攻撃から物理攻撃までの実際のシナリオに基づいて開発されました。

リスク管理
産業環境に包括的なサイバーセキュリティソリューションを導入することは、企業のリスク管理システムの強化につながります。

ソリューション

この境界内部でのサイバーセキュリティを確保するために、NLMK は 、仮想化サーバー、エンジニアリング用ワークステーション、PLC を含む、運用技術層やその他の組織の構成要素を保護するように設計された一連の技術とサービスである Kaspersky Industril CyberSecurity を選択しました。

Kaspersky Industrial CyberSecurity の基盤となる各種技術によって、エンドポイントの保護に加えて、受動監視による産業用ネットワーク内への侵入や異常検知も行われます。

Kaspersky Industrial CyberSecurity 責任者の Georgy Shebuldayev は次のように述べています。「私たちにとって、この NLMK のインフラストラクチャを保護するプロジェクトは価値があり、ある意味で他では得られない経験でした。ICS の上層で仮想化が利用されていることから、いくつかの興味深い技術的問題が浮かび上がったのです。たとえば、複数の仮想サーバーを 1 つの物理ハイパーバイザーにデプロイすると、セキュリティと負荷分散の観点から、さらに追加の要件が必要になります。アンチウイルススキャンが複数の仮想サーバーで開始されると、ハイパーバイザーに対する負荷の総量が増え、他の仮想マシン、最終的には産業プロセス全体のパフォーマンスに影響を及ぼす可能性があるのです。カスペルスキーのエキスパートはこのインフラストラクチャが提示する課題のすべてに適切に対処しました。」

これまでに、Kaspersky Industrial CyberSecurity のすべてのコンポーネントのテストが成功し、現在は鋼板の製造所内でユーザーテストが実施されています。

「NLMK と Kaspersky Lab の協業はこのパイロットプロジェクト限定のものではありません。このプロジェクトは、この先に期待できる技術提携の第一歩と言えます」

Sergey Slauta氏、NLMK 産業プロセス
オートメーション担当ディレクター

評価結果

NLMK の産業プロセスオートメーション担当ディレクターである Sergey Slauta 氏は次のように述べています。「最新のインテリジェントオートメーションシステムを生産工程に導入すると、潜在的なサイバー攻撃のリスクが増加します。これが産業プロセスに影響を及ぼす可能性があります。NLMK ではそのような事態の発生を防ぐために、オートメーションインフラストラクチャレベルで、統合された多層型防御を導入しようとしています。Kaspersky Industrial CyberSecurity は当社の真のニーズに応えており、産業プロセスの主要なサイバーセキュリティ要件を満たしています。NLMK と Kaspersky Lab の協業はこのパイロットプロジェクト限定のものではないでしょう。このプロジェクトは、この先に期待できる技術提携の第一歩と言えます」

Kaspersky® Industrial CyberSecurity

Kaspersky Industrial CyberSecurity は、運用技術層および組織の構成要素（SCADA サーバー、HMI、エンジニアリング用ワークステーション、PLC、ネットワーク接続のほか、さらにエンジニアも含む）を保護するよう設計された技術とサービスのポートフォリオであり、事業継続性や産業プロセスの一貫性に影響を及ぼさないよう設計されています。詳細情報はこちら：
www.kaspersky.co.jp/enterprise-security/industrial

ICS サイバーセキュリティについて：
https://ics-cert.kaspersky.com
サイバー脅威に関する最新情報：
www.securelist.com

#truecybersecurity

www.kaspersky.co.jp

IIC MEMBER industrial internet CONSORTIUM

OPC® FOUNDATION MEMBER

CYBER SECURITY EXCELLENCE AWARDS ★ WINNER ★ 2018

* 第 3 回 World Internet Conference の「World Leading Internet Scientific and Technological Achievement Award」

** 2016 年 China International Industry Fair（CIIF）特別賞