シーメンスデジタルインダストリーズソフトウェア

デジタル・スレッドにおけるデータ保護

シーメンスとIdentify3Dの展望

エグゼクティブ・サマリー

シーメンスとIdentify3D社のテクノロジーにより、デジタル・マニュファクチャリング・スレッドにおけるデータの機密性と整合性を保護するとともに、知的財産の保護、製造の再現性、トレーサビリティーを提供して、常に進化するサイバーセキュリティーの脅威に対抗できます。

はじめに

インダストリー4.0やモノのインターネット (IoT) などの取り組みを通じたデジタル・マニュファクチャリングの登場により、設計、エンジニアリング、生産、プロセス制御に使用されるツール群がデジタルでリンクされるようになりました。デジタル・スレッドで情報を共有できる機能が、製品ライフサイクル全体でのコラボレーション、効率、コスト削減の進歩につながっています。しかし、システムとソフトウェアをデジタル接続する必要があるため、デジタル・マニュファクチャリング・エコシステムは深刻なサイバーセキュリティーの脅威にさらされがちです。

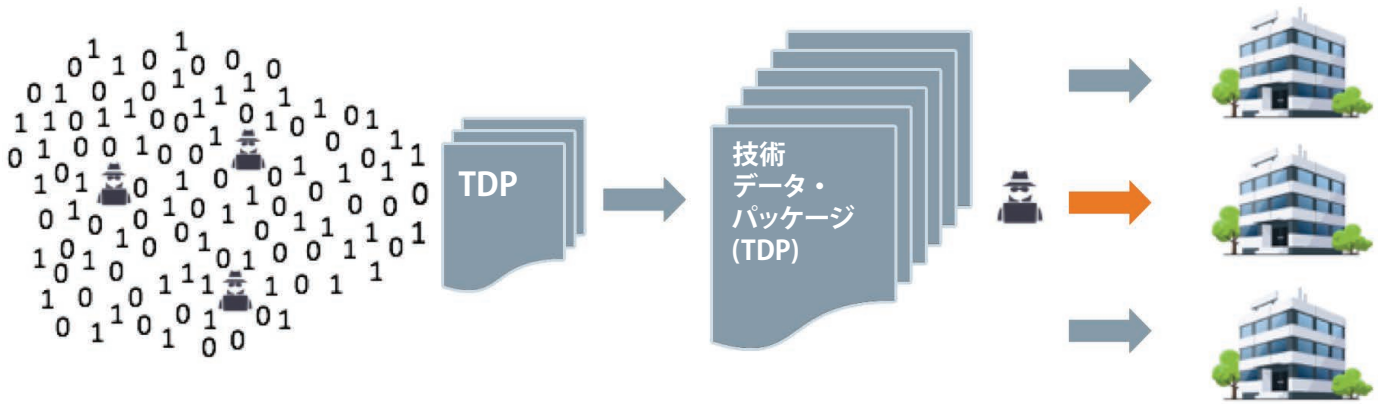
設計とエンジニアリングの面では、シーメンスデジタルインダストリーズソフトウェアのNX™ソフトウェアなどのコンピューター支援設計ツールにより、個々の部品、アセンブリ、さらには製造プロセスの設計、シミュレーション、可視化が可能になっています。多くの場合、設計プロセスではさまざまなツールが使用され、それぞれのツールは、効率を最大化するためにスレッド内の他のツールと相互運用する必要があります。

インダストリー4.0の生産および製造の面では、生産フローで使用されるデバイスとマシンの多くは、運用のための情報をデジタル化して送受信する機能と、プロセス中に収集したデータをレポートする機能を備えています。過去数十年にわたって、コンピューター数値制御 (CNC) マシンでは、マシン制御コマンドの自動化シーケンスの指示にGコード・ファイルを使用してきました。アディティブ・マニュファクチャリングにより、情報のデジタル・パッケージによって定義される多数の部品をすべて同時に作成することが可能となり、デジタライゼーションがさらに一歩進みました。その一方で、マシンに組み込まれたセンサーとスマート・デバイスは膨大な量のデータを収集しています。

製品ライフサイクル管理 (PLM) システムとコラボレーションプラットフォーム[1] (シーメンスデジタルインダストリーズソフトウェアのTeamcenter®製品など) は、エンター プライズ・リソース・プランニング (ERP)、製造オペレーション管理 (MOM)、電子設計自動化 (EDA) の各種システム間のデータ統合と、デジタル・スレッドで各システムによって作成されるデジタル情報を蓄積する製品です。さらにPLMシステムは、設計システムと製造システムをリンクして、従来は切り離されていた2つのビジネスオペレーション間でデジタル情報を共有します。

企業はシーメンスのMindSphereなどのデータ収集システムを使ってインダストリー4.0やIoTによって生成される幅広いデジタル・データを収集するほか、付属のデータ解析機能を使用して、製造プロセス・フローをより深く理解できるようになってきました。

アディティブ・マニュファクチャリングの分野では、シーメンスのアディティブ・マニュファクチャリング・ネットワークによって、設計コンサルティング・サービスおよび機能、さらにオンデマンド生産の製造サービスを実現できます。企業はこうした分散型製造プラットフォームを活用して、機能プロトタイプや連続生産部品の生産能力を手に入れています。



技術データ・パッケージ

デジタル・スレッドを構成するさまざまなシステム間で共有されるデータは通常、技術データ・パッケージ（TDP）と呼ばれます。設計から製造までの間に非常に多くの統合ツールおよびデバイスが存在しているため、システム間で交換されるTDPのサイズと複雑さは飛躍的に増大しています。それと同時に、アプリケーションとシステムの増加は、システム間の相互運用性をサポートするインターフェースの複雑化も招いています。

PLMシステムによって部品のTDPを管理しやすくなりましたが、多くの異なる企業でデータを共有している場合は、それぞれシステム間にデジタル・インターフェースがまだ必要です。また、相互運用性と複雑性が高まるデジタル・インターフェースの脆弱性は、サイバーセキュリティーの攻撃対象になりかねません。IBM Security によると、2016年、製造システムに対して行われたサイバーセキュリティー攻撃の74%は、デジタル・インターフェースに攻撃ベクトルのインジェクションを試みる攻撃でした。

製造システムへの攻撃には、知的財産（IP）の窃取が含まれます。例えば、ドイツの鉄鋼・工業製品メーカーThyssenKrupp社 は2016年、設計IPの窃取に遭いました。[2] Manufacturing Business Technologyに社によると、メーカーの21%が、サイバー攻撃によるIPの流出被害を受けたことがあるといっています。[3] 機器の物理的破壊を狙ったケースもあり、ドイツ連邦政府情報セキュリティー庁(BSI)の報告によると、製鉄所の溶鉱炉が攻撃され、その結果として、炉が過熱するという事例もありました。[4] Stuxnet[5] ワームというイランの核プログラムを標的としたも事例も有名です。L.D. Sturmをはじめとする研究者が詳述しているように、攻撃者の手口 にはIPの 窃取や物理的破壊のほか、物理パーツの改ざんもあります。[6] Cybersecurity Ventures社は、2015年には3兆ドルだった全世界のサイバー犯罪の被害額は2021年には6兆ドルに増大すると予測しています。[7] 近年、ランサムウェア攻撃が原因で、複数の製造施設が一度に数日間閉鎖に追い込まれる事態も発生しました。

「製造業は、最もランサムウェア攻撃の標的になりやすい産業です」

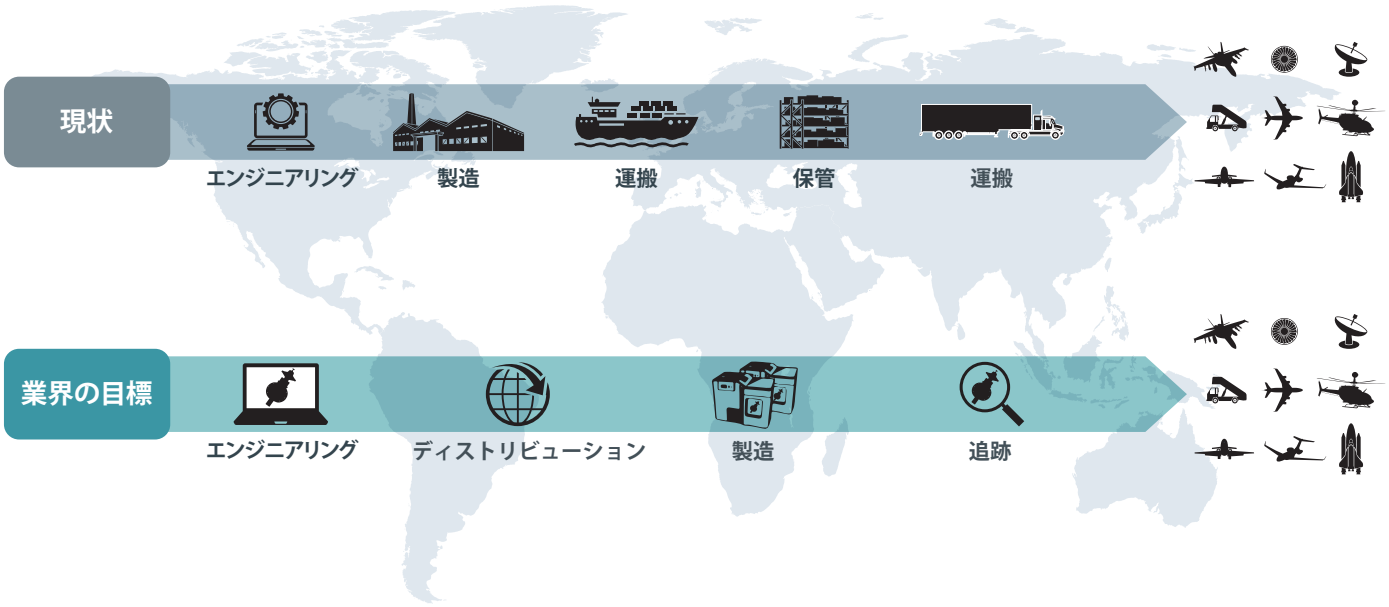
Carbon Black[8]

サイバー攻撃が増加し、製造システムと分散型サプライチェーン網の複雑さが増すなか、デジタル・マニュファクチャリング・エコシステムのセキュリティーは一層、困難を極めます。Cybersecurity Ventures社は、今後5年間（2017年～2021年)で累積1兆ドル以上が費やされると推定されています。[9] 従来、サイバーセキュリティー防御は、デバイスへの論理的および物理的アクセスの保護と、個々のデバイスの悪用防止に重点を置いてきました。確かにこうした方法は一定の効果があり、適切に実行されれば、非常に強固な防御を実現します。ただし、デジタル・マニュファクチャリング・スレッドではその性質上、異なる事業体が所有することの多い、物理的に異なる場所のデバイスとシステム間の相互運用性と通信が必要となります。そのため、デジタル・スレッド内のTDPを保護するという中心的課題に特化した優れたソリューションが求められています。

このホワイトペーパーでは、デジタル・マニュファクチャリング・スレッド内のTDPを保護するための新しいテクノロジーについて説明します。Identify3Dアプリケーション製品は、設計センターにおける作成から製造デバイスでの生産まで、TDPの機密性と完全性を保護し、デジタル・マニュファクチャリングのIP保護、製造の再現性、さらにはトレーサビリティーを実現します。TDPの保護に特化しているため、所有者が異なり、サイバーセキュリティー保護の程度も異なるさまざまなシステム間をTDPが通過する場合でも、顧客のデータを確実に保護することができます。

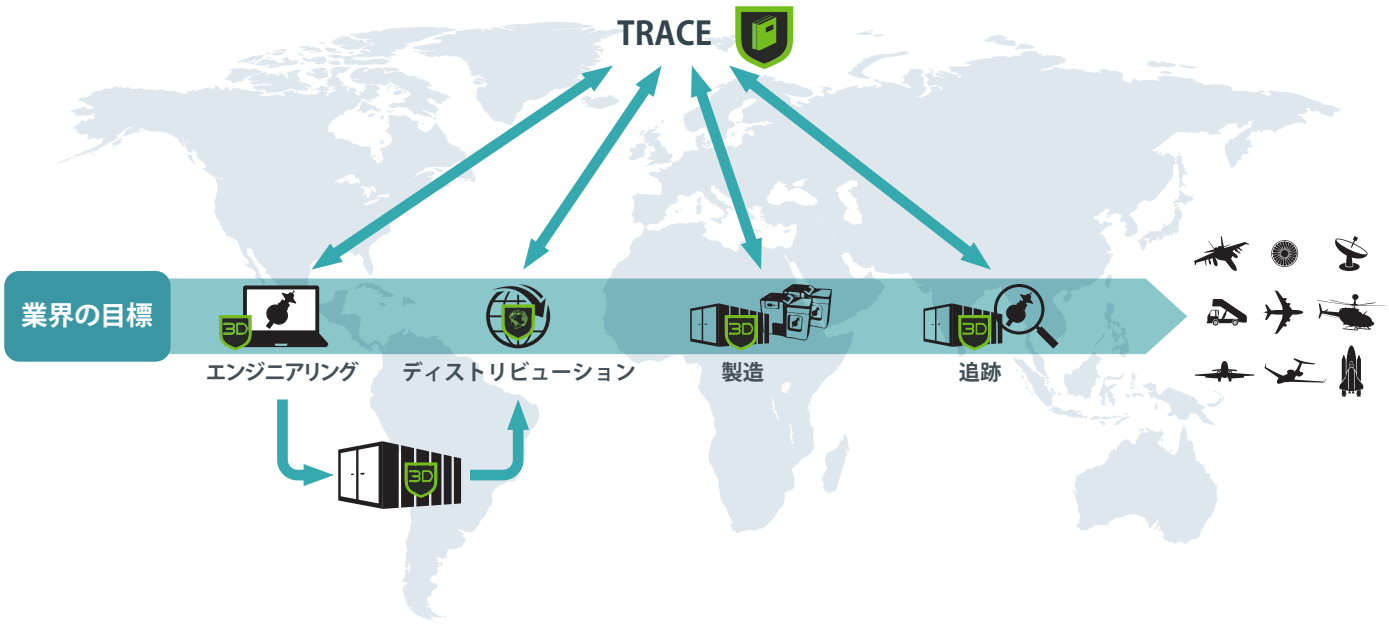
デジタル・スレッドのデータ保護に向け た新たなソリューション

製造のデジタライゼーションを進めるには、サプライチェーンを見直す必要があります。従来、サプライチェーンでは、箱やコンテナに入った物理的なアイテムの運搬を主に担ってきました。しかし現在、こうしたアイテムには長く複雑なデジタル・ライフサイクルが付きものであり、物理的パーツの製造に先立ち、データの移動と管理が発生しています。 また、 データの移動と管理には、物理的なサプライチェーンとの類似点もあり、デジタル・スレッドとして実現できるものです。輸送コンテナの発明により、商品を倉庫から港湾、電車、 トラックそして最終的に店舗まで簡単に運搬できるようになると、世界貿易に変革がもたらされました。デジタル・スレッドでは、TDPがデジタル・ワークフロー内で似たような道筋をたどります。標準化された安全な物理コンテナが商品の取引に革命をもたらし、輸送システム間で簡単かつ安価な運搬が可能になったように、デジタルコンテナも、デジタル・スレッド内のアプリケーション間のシームレスな相互運用を可能にするものであるべきです。



デジタル・スレッド

シーメンスとIdentify3D社のエコシステムは、デジタル・ワークフローを通じてTDPを移動させるためのセキュアなデジタル・コンテナを実現します。このソリューションにより、相互運用性を維持しつつ、TDPを完全に保護することができます。デジタル・コンテナでは、特殊なストレージ・リポジトリやセキュアな転送方法は不要です。Identify3D Protect™アプリケーションによってセキュアなコンテナが作成され、Identify3D　Manage™によってコンテナ内でTDPを使用するための流通ポリシーとライセンス・ポリシーの作成が可能になります。 Identify3D Enforce™を使用すると、製造デバイスとの統合により、コンテナに対して定義されたライセンス・ポリシーに基づいて、アプリケーションとデバイスがTDPにアクセスできます。セキュア・コンテナがデジタル・スレッドを移動すると、Identify3D　Trace™によってすべてのトランザクションが記録され、Identify3D Track™によって物理パーツIDがデジタル・ツインにリンクされます。CAD、コンピューター支援製造 (CAM)、アディティブ・マニュファクチャリング・ソフトウェアから機械コントローラーにいたるまで、これらの要素はすべてシーメンスのDigital Factoryツールに統合されます。

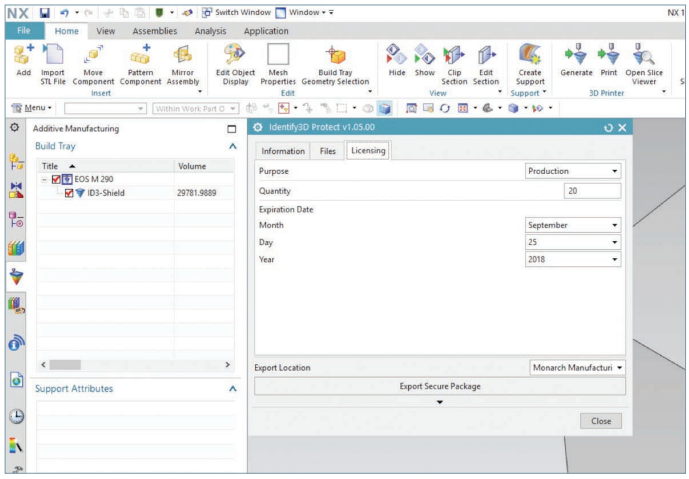


デジタル・スレッド – ソリューション

Identify3D Protectを使用することで、設計者は、デジタル・マニュファクチャリングに使用される CAD / CAM および AMファイルを、Digital Supply Item (DSI) と呼ばれる暗号化されたデジタル・コンテナに保存することができます。このコンテナはデジタル署名されており、ビジネス・ルールと製 造ルールが組み合わされています。TDPに組み込まれたすべてのデジタル・ファイルは、パッケージの製造準備が完了すると、DSIにセキュアに保存できます。DSIのライセンスの作成には、元の設計に固有の製造ルールとその他の仕様が使用されます。設計がすべて完成すると、ファイルはセキュアに暗号化された上でデジタル署名され、DSIコンテナ は配布および製造待ちのデジタル・ストレージ・システムに転送されます。デジタル・ライセンスは、Identify 3D Protect に転送されます。DSIコンテナは暗号化とデジタル署名が行われるため、DSIのデジタル・ストレージおよび配布に関するセキュリティー要件はありません。

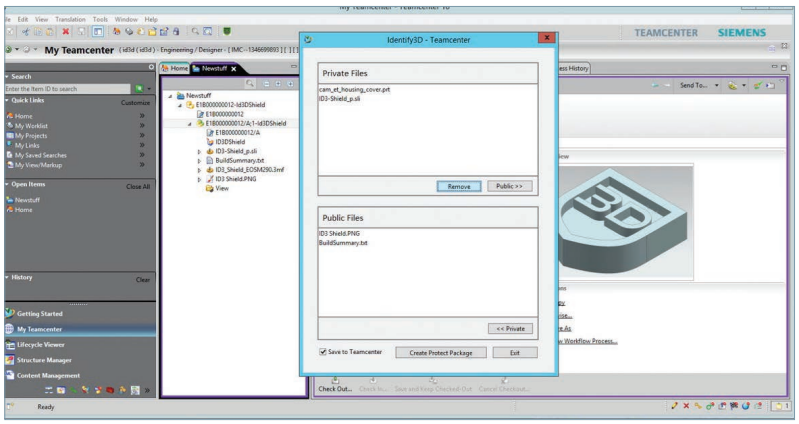
Identify3D社のエコシステム

Identify3D ProtectをNXに直接統合することで、ユーザーは、CADファイル、AMビルドファイル、またはCAM後処理ファイルが含まれる暗号化されたDSIを作成できます。この統合により、すべてのパッケージ名とファイルの説明がProtectモジュールに自動的に取り込まれるため、シームレスなユーザー・エクスペリエンスを実現できます。さらに、下流のIdentify3D Manageへの登録も、NX内で直接実行できます。



シーメンスのNXで直接動作するIdentify3D Protect

Teamcenterのユーザーは、Identify3D Protectプラグインに直接アクセスして、Teamcenterのアイテム・リビジョン内のファイルからセキュアなDSIコンテナを作成できます。作成したDSIコンテナは、Teamcenterに保存するか、シーメンスの製造実行システム （MES） などの下流のアセット・ストレージ・システムに送信できます。



Teamcenter内で直接動作するIdentify3D Protect

Identify3D ManageがIdentify3D Protect™ からライセンスを受け取ると、生産指示が出され、セキュアかつ説明可能なデジタル配布にユーザーがアクセスできるようになります。ユーザーは、DSIの配布および製造権をあらゆるディストリビューターまたはデジタルメーカーに割り当てることができます。基本的に、システム内のDSIの運用性は、ユーザー、システムの所有者、またはシステムに関連付けられたデジタル所有権に基づいて、セキュアに制御することができます。Identify3D Manage™には、生産指示のタイミングで、ライセンシーが製造可能な部品数を制限する機能があります。Identify3D Manageアプリケーションは、エンジニアリング、流通、製造向けにカスタマイズされた形式で提供されます。

例えば、シーメンスのアディティブ・マニュファクチャリング・ネットワークは流通モードで動作します。 Identify3D Manageのインスタンスはネットワークの一部として動作し、生産指示として送られてきた部品が製造に送られるまでを管理します。これにより、アディティブ・マニュファクチャリング・ワークフローのこれらの手順が実行されるときに、シーメンスのアディティブ・マニュファクチャリング・ネットワーク内で顧客のデータを確実かつセキュアに管理できます。

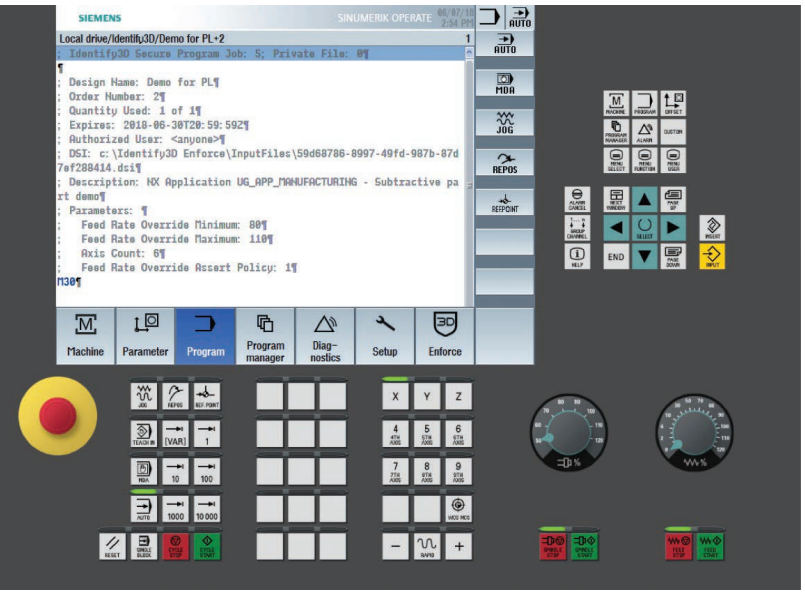
部品の製造マシンは、メーカー、モデル、または個々のマシンに応じて指定できます。部品の製造を制御するために使用するデジタル・パラメーターは、範囲または値で制限されます。一貫した再現性を保証するために必要な、デバイスに関連する認定・認証は、ライセンスで指定できます。シーメンスとIdentify3D社のエコシステムによって、部品単位で製造が許可されている製造システムを完全に制御できるため、 IP所有者は一貫した品質を確保できます。

Identify3D社のライセンス・ポリシーとして、IDの厳格な管理がサポートされます。これにより、顧客は、個別に定義するか、あるいはグループ、役割、または証明書のステータスを通じて定義するライセンス・ユーザーによってのみ、部品が製造されることを要求できます。このポリシーによって、顧客は、デジタル・スレッドのシステムのユーザーが現地のID管理システムで認証されていることを確認できるだけでなく、定義された製造システム上のDSIの保護されたファイルを使用するためのアクセス権が、適切な資格を持つ特定のユーザーに付与されるように要求することができます。

デジタル配布が完了し、部品の生産準備が完了すると、Identify3D Manageによって、Identify3D Enforceアプリケーションが組み込まれた製造デバイスに、部品の生産ライセンスが付与されます。Identify3D Enforceは、ライセンス、マシンの設定、ユーザー、DSIの完全性検証を通じて、生産中の設計のセキュリティーと完全性を保証します。完全な検証が完了した場合のみ、Identify3D EnforceによってDSIコンテナの暗号化が解除され、機械コントローラーに製造用のライセンス・ファイルが提供されます。

製造デバイスで部品を生産するプロセスは、Identify3D Enforceによって継続的に監視され、すべての設定とパラメーターがライセンスされた値と範囲に収まっていることが保証されます。さらに、最大ライセンス数量を超えて部品が生産されることのないよう、生産される部品の合計数量が追跡されます。

Identify3D Enforceは、 シーメンスのSINUMERIK 840D sl CNCコントローラーに統合されており (2018年6月現在)、暗号化されたGコード・ファイルが含まれるセキュア DSI コンテナをロードするためのシームレスなユーザー・エクスペリエンスを提供します。



シーメンスのSINUMERIK 840D slに統合されたIdentify3D Enforce

製造業のサイバーセキュリティーのベストプラクティスは、『NIST SP 800-82 publication10』とIEC 62443/ISA-99標準で概説されています。[11] これらには、製造拠点で重要かつ最も脆弱な機器の指定、必要な保護レベルに基づくセキュリティー・レベルの割り当て、分離ゾーンの作成が含まれています。さらに、ソフトウェアのパッチを最新の状態に保つ、監査証跡を作成する、アクセスを制限する、適切なウイルス対策およびファイルの整合性チェックを実装する、未使用のポートを無効にするなど、個々のシステムに対する標準的なサイバーセキュリティー・プラクティスも適用されます。システムの継続的な監視も重要です（特に侵入を検出可能な場合）。

保存中のデータの暗号化も、ベストプラクティスとして推奨されます。暗号化がデータ・セキュリティーにおいて非常に重要な側面であることは確かです。ただし、デジタル・スレッドでシステム間の相互運用性を維持するには、システム間のインターフェースでデータの暗号化を解除する要があり、ここに脆弱点が生じます。Identify3Dは、DSI の暗号化されたデータをアプリケーション間で受け渡すことにより、これを解決します。暗号化されたデータは、製造デバイスに組み込まれた Identify3D Enforce アプリケーションからアクセスされた場合にのみ、プレーン・テキスト形式で暗号化を解除できます。

従来から、暗号システムで最も複雑な課題は、必要な暗号化キーを安全に管理することです。暗号化が失敗する場合、その原因の大部分はキーが適切に保護されていないことにあります。暗号化キーを保護する方法として、ハードウェア・セキュリティー・モジュール（HSM）、スマート・カード、トラステッド・プラットフォーム・モジュール（TPM）などのいくつかの方法があります。顧客のセキュリティー・レベル要件に基づき、Identify3Dは、連邦情報処理標準（FIPS）またはコモン・クライテリア認証デバイスの使用など、暗号化キー保護のあらゆる業界標準をサポートしています。暗号化キーを利用する Identify3Dアプリケーションにはそれぞれ、ハードウェアで保護されたソースからそれらのキーにアクセスする機能があります。

Identify3D社のエコシステムを実装しても、製造におけるサイバーセキュリティーのベストプラクティスに従う必要性がなくなるわけではありません。むしろ、ベストプラクティスに従うことによって、Identify3Dの保護レベルを強化できます。ベストプラクティスの実装にあたっての最大の弱点は、相互運用性の要件と内部関係者に関連する脅威です。Identify3Dを使用すると、暗号化による相互運用が可能となり、TDPはDSI内で暗号化されるため、デジタル・スレッドのどこであっても、内部関係者がTDPにアクセスできる機会はなくなります。 Identify3Dアプリケーション製品群は、TDPの保護に重点を置いており、デジタル・スレッド全体でTDPの機密性と完全性を保証します。

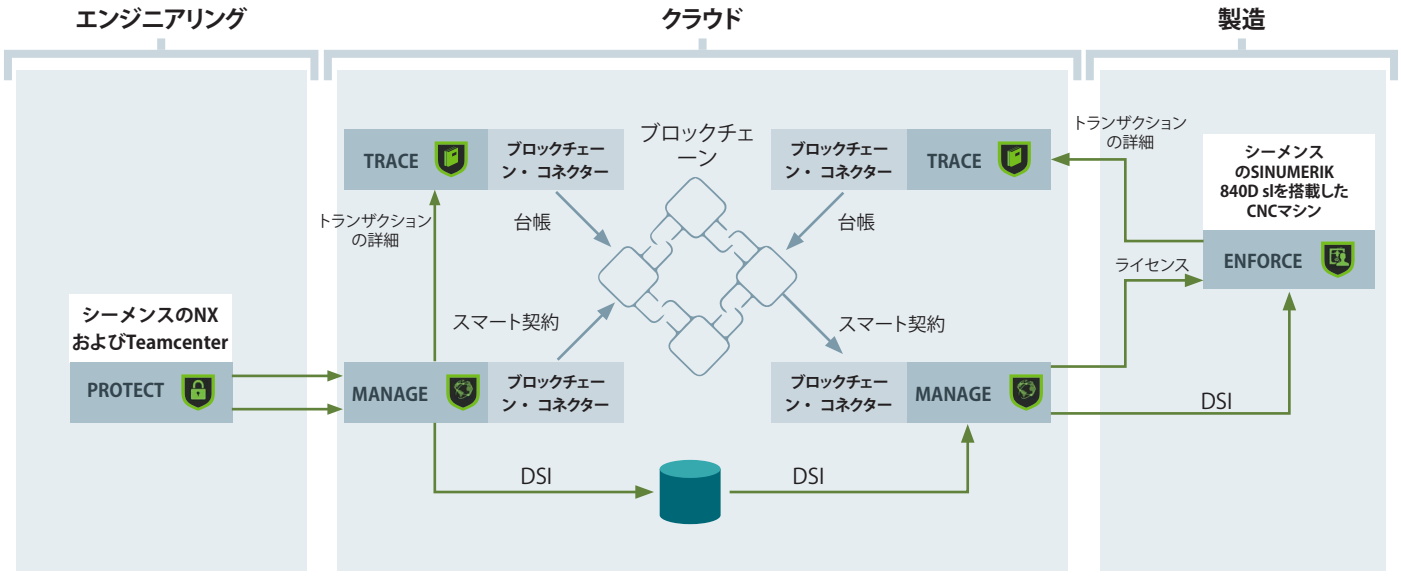
デジタル・スレッド内でのIPの保護と品質の維持に加えて、Identify3D社のテクノロジーにより、そのIPのすべてのオペレーションとトランザクションがセキュアに保存されます。 Identify3D Traceは、DSIに関わる各デジタル・トランザクションの記録を保存するアプリケーションであり、各TDPのデジタル・マニュファクチャリングとディストリビューションの監査記録が可能です。 トランザクションに保存されるすべてのデータは暗号化され、IP所有者の裁量で、TDPのデジタル・マニュファクチャリ ングに関わる事業体がアクセスできます。物理パーツが製造されると、Identify3D Trackにその識別番号が記録され、 デジタル・スレッドと物理スレッド間のリンクがTraceの台帳に保存されます。さらに、Traceに保存されたこのセキュアな データは、データ保存のため、シーメンスのMindSphereシステムなどのデジタル・データ収集システムに提供することもあります。

ブロックチェーン

ブロックチェーンは、集中管理型の専用データベースを分散型のオープン・データ・リポジトリに置き換えることができるテクノロジーです。ブロックチェーン内で、各参加ノードを継続的かつ恒常的に更新される共有台帳に追加できます。共有台帳には強力な暗号整合性保護機能があり、特定のブロックチェーン内で発生したトランザクションの履歴全体が記録されます。さらに、各ノードはトランザクションの信頼性について投票を行い、不正なトランザクションを拒否することができます。ブロックチェーンは分散型というその性質上、台帳に記録されたデータについて特定の企業が所有したり、過度の影響を及ぼしたりすることがありません。

各Identify3Dアプリケーションは独立したノードで実行されるため、サプライチェーンのブロックチェーン内でIdentify3Dエコシステムを実装するのも簡単であり、Identify3Dのコアテクノロジーを変更する必要もありません。利用するブロックチェーン・テクノロジーに応じて、複数の実装も使用することができます。デジタル契約が可能なHyperledger Fabricなど、より複雑なブロックチェーンの場合は、Identify3Dアプリケーションによって作成されるデジタル・ライセンス全体をブロックチェーンに保存し、デジタル契約をライセンスに利用する方法もあります。もっと簡単な実装の場合、ライセンスのデジタル署名されたハッシュレコードをブロックチェーンに保存します。どちらの場合においても、ライセンス・トランザクションの記録はブロックチェーンによって維持されます。ライセンス全体がブロックチェーンに組み込まれている場合においては、ブロックチェーン自体がノード間でライセンスを移動するためのメカニズムとして機能します。ライセンスの機密情報はライセンシー暗号化キーで暗号化されるため、IPの機密部分を保持したまま、トランザクションの整合性が維持されます。

Identify3Dアプリケーションは、デジタル・マニュファクチャリング・テクノロジーで作成された各物理パーツに、デジタル・ツインの記録を追加することで、サプライチェーンのブロックチェーンを強化します。これにより、最終的に組み立てられた製品には、製造オペレーションの完全な記録だけでなく、完成製品に含まれているデジタル設計とIPを含めることができます。



Identify3Dとブロックチェーンの統合例

ソフトウェア / ハードウェア接続

現在、Identify3Dソリューションはシーメンスのデジタル・エンタープライズ製品群に統合されているため、ユーザーは作成から製造まで、IPの機密性と完全性を保護することができます。

例えば、ある航空宇宙メーカーがCNCで製造する20個の交換部品を短納期で要求されたケースを考えてみましょう。部品はすでに設計済みで認定も受けているため、TDPはTeamcenterにアイテム・リビジョンとして保存されています。ユーザーは、認定を受けたマシンでのみ部品が作成されるよう制限しながら、Identify3D Protectを使用して、TDPを選択し、DSIを作成します。次に航空宇宙メーカーは、Identify3D Manage for Engineering を通じて、外部受託メーカーが20個の部品を製造することを承認します。

承認済みの受託メーカーが、別の委託先に依頼しないと要求数量を製造できないという判断に至った場合には、Identify3D Manage for Distributionを使用して、自社の作業現場で12個の部品を製造することを承認し、別の委託業者が8個の部品を製造することを承認します。

外部受託メーカーは、作業現場で実行されているIdentify3D Manage for Manufacturingで承認を受け取り、部品の製造資格がある3台のCNCマシンを認証することができます。こうして、外部受託メーカーは各マシンに4個の部品の製造を割り当てます。各マシンでIdentify3D Enforceを実行しているシーメンスのSINUMERIK 840D slコントローラーは、部品固有のGコードが含まれるDSIを受け取り、ジョブを作成します。その後、各マシンは適切な認証を取得しているため、オペレーターはジョブを選択して4個の部品のみを製造することができます。

プロセスが完了すると、航空宇宙メーカーは、Identify3D Traceやそれに接続されたシーメンスのMindSphereから、各製造マシンのレポートなど、発注が正常に完了した記録を確認します。航空宇宙メーカーはまた、下請業者が使用した2台のCNCマシンからのレポートを確認することもできます。

まとめ

インダストリー4.0は、企業の製造方法を劇的に変えつつあります。他の産業と同様に、製造業もアセットとプロセスのデジタライゼーションが進んでいるため、ある程度は将来の見通しがあります。ただし、このデジタライゼーションのメリットを存分に活用するには、デジタル・サプライチェーンを流れる膨大な量のデータを、管理、制御、追跡する必要があります。

必要なときに必要な場所で製造可能な分散型の製造モデルの実装は、厳密に管理されたセキュアなプロセスに従い、適切なデータが適切なタイミングで適切なマシンに到達することでのみ実現されます。

偽造部品、悪意を持って改変された部品、低品質の部品、未認証の部品が市場に出荷されてしまう事態を防ぐには、デジタルとリアルの両方のサプライチェーンの整合性が重要です。Identify3Dのテクノロジーのように、保存中のデータの保護、ライセンスを通じたデータフローの管理、改変できない移動記録の管理のためのテクノロジーは、こうした新しい製造ビジネスモデルをセキュアに展開する上で、これから大きな役割を果たすでしょう。

参考文献

1. https://www.plm.automation.siemens.com/en/plm/digital-manufacturing.shtml
2. https://www.reuters.com/article/us-thyssenkrupp-cyber/thyssenkrupp-secrets-stolen-in-massive-cyber-attack-idUSKBN13X0VW
3. https://www.mbtmag.com/article/2017/03/top-cybersecurity-threats-manufacturing-2017
4. http://www.bbc.com/news/technology-30575104
5. http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf
6. Sturm, L.C.ほか「Cyber-physical vulnerabilities in additive manufacturing systems: A case study attack on the .STL file with human subjects.」『*Journal of Manufacturing Systems*』第44巻、第1部: 2017年7月、154〜164ページ。
7. https://www.prnewswire.com/news-releases/cybercrime-damages-are-predicted-to-cost-the-world-6-trillion-annually-by-2021-300540158.html
8. https://www.infosecurity-magazine.com/news/nonmalware-attacks-on-the-rise
9. https://www.infosecurity-magazine.com/news/annual-cybercrime-costs-double-6
10. https://csrc.nist.gov/publications/detail/sp/800-82/rev-2/final
11. https://www.isa.org/isa99

シーメンスデジタルインダストリーズソフトウェア

本社
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 972 987 3000

アメリカ
Granite Park One
5800 Granite Parkway
Suite 600
Plano, TX 75024
USA
+1 314 264 8499

ヨーロッパ
Stephenson House
Sir William Siemens Square
Frimley, Camberley
Surrey, GU16 8QD
+44 (0) 1276 413200

アジア／太平洋
Unit 901-902, 9/F
Tower B, Manulife Financial Centre
223-231 Wai Yip Street, Kwun Tong
Kowloon, Hong Kong
+852 2230 3333

日本
〒151-8583 東京都渋谷区代々木 2-2-1
小田急サザンタワー
TEL: 03-5354-6700 (代)

siemens.com/plm

71790-81573-C7-JA 2/20 LOC

シーメンスデジタルインダストリーズソフトウェアについて
シーメンスデジタルインダストリーズソフトウェアは、シーメンスのデジタルインダストリーズのビジネス・ユニットです。製造業がイノベーションを実現するための新たな機会を創出し、産業のデジタル・トランスフォーメーションを牽引するソフトウェア・ソリューションの提供において、世界をリードするグローバル・プロバイダーです。米国テキサス州プラノを本拠地とし、これまで世界140,000社以上のお客様にサービスを提供しています。シーメンスデジタルインダストリーズソフトウェアは、あらゆる規模のお客様と協働して、アイデアの実現方法、製品の実現方法、稼働中の製品および設備資産の活用や状況把握の方法を変革できるよう支援しています。
シーメンスの製品およびサービスについての詳細は、siemens.com/plmをご覧ください。