サプライチェーンにおけるサイバーセキュリティのリスクを管理

ULサプライヤー・サイバートラストレベル

サイバーセキュリティは、製造者、サプライヤー、最終製品のエコシステムに影響を及ぼす、大きな関心事項です。調達メカニズムを確立し、サプライヤーやベンダーが各自のセキュリティ対策の信頼性を実証できるようにする必要があります。グローバルなサプライチェーンはますます多様化・複雑化しており、サイバーセキュリティの脅威は増大しています。サイバーセキュリティの要件に準拠し、サードパーティと緊密な連携を行うことが不可欠になっています。

製造者、サプライヤー、最終製品のエコシステムの健全性は、最も脆弱な箇所によって決まります。ULでは、調達メカニズムを支援し、全体的なサプライチェーンを強化するために、サプライヤー・サイバートラストレベルを開始しました。このソリューションでは、工業、自動車、医療機器の製造企業が、最終製品でセキュリティ上の問題が発生するリスクを最小限に抑え、顧客が最終製品の使用時にソフトウェアやシステムの脆弱性が露呈するような状況の回避を支援します。

サプライヤー・サイバートラストレベル

ULのサプライヤー・サイバートラストレベルでは、以下の主な信頼性カテゴリにおけるセキュリティ対策の信頼性を実証することにより、サプライヤーやベンダーが調達/品質保証プロセスをより適切に実施できるようサポートします。

- ソフトウェア開発における対策
- ソフトウェア開発の環境およびインフラストラクチャ
- ハードウェア開発における対策
- 製品の文書化
- 安全な製造プロセスと配送管理
- セキュリティ問題の管理
- ホストするソフトウェア
- 品質管理システム
- エンタープライズセキュリティ
- サプライヤー管理

サプライヤーやベンダーは、実績のある審査/評価プロセスを通して単一のセキュリティレベルの認証を受けることで、メリットが得られます。また、サプライヤー・サイバートラストレベルは、文書化され独立したサプライヤーのトラスト・レベル・レーティングによって、競合上の差別化を許可するためにも役立ちます。

サプライヤーのトラストレベルレーティング：

- レベル1：Nascent（初級）
  一時的なセキュリティ対策がまったく、あるいはほとんど実施されていない。顧客に提供する製品/サービスに関連するすべてのプロセスで、セキュリティを検討する必要がある。
- レベル2：Challenger（チャレンジャー）
  一部のプロセスで基本的なセキュリティ対策が実施されている。顧客に提供する製品/サービスに関連するすべてのプロセスで、セキュリティを検討する必要がある。
- レベル3：Contender（中級）
  一部のプロセスで中程度のセキュリティ対策が実施されている。顧客に提供する製品/サービスに関連するすべてのプロセスで、セキュリティを検討する必要がある。
- レベル4：Strong performer（上級）
  大半のプロセスで高度なセキュリティ対策が実施されている。一部のプロセス改善により、最高レベルの信頼性を達成できる。
- レベル5：Leader（リーダー）
  最高レベルの信頼性が達成されている。すべての信頼性カテゴリで、期待されるレベルのセキュリティ対策が実施されている。

独立した信頼できる第三者機関としてULは、サプライチェーンのセキュリティリスクを評価するための時間効率とコスト効率の高いプロセスとして、組織に代わって、サプライヤー・サイバートラストレベルの管理を支援します。

ULのサプライヤー・サイバートラストレベルは、以下のような既知の主要な業界ベストプラクティス、規格、フレームワークのセキュリティ管理対策をマッピングおよび活用することで、現在の世界的なサイバーセキュリティの複雑さに対処するために支援します。

- NISTサイバーサプライチェーンリスク管理
- ENISAサプライチェーン攻撃
- 経済産業省Society 5.0
- NERC CIP-013-1UKサプライヤー保証
- ISO/IEC 20243-1
- IEC 62443-4-1および62443-2-4
- ISO 27001
- NERC

ソリューションの主な目標

サプライチェーン内のサイバーセキュリティのリスクを理解する

- 調達メカニズムを活用して、サプライチェーンにサイバーセキュリティのリスク管理を組み込む
- 業界で認知された規格、フレームワーク、ベストプラクティスを使用して、セキュリティ開発ライフサイクル（SDL）基準に対応する
- サプライヤーやベンダーのセキュリティ対策の信頼性を実証する

IoTサプライヤーおよびベンダーに向けた質問と評価対象の対策

ULのサプライヤー・サイバートラストレベルでは、10個の信頼性カテゴリにわたって詳細な分析を行い、サプライヤーやベンダー対策を以下のように審査します。

- 情報セキュリティ、およびソフトウェア/ハードウェア製品またはコンポーネントの開発、導入、使用に関連付けられたサイバーセキュリティのリスクを最小限に抑えるために、適切な安全対策を講じているか？また、定期的なフォローアップを行っているか？
- すべての社内開発/サードパーティ製のソフトウェア/ハードウェア製品およびコンポーネントについて、組織内のサイバーセキュリティ基準/要件（規格やフレームワークの要件を含む）を活用しているか？
- すべてのソフトウェア/ハードウェアについて、セキュリティ上の欠陥および脆弱性に対する十分な保護対策を講じているか？
- セキュリティ侵害を招く可能性のある潜在的なソフトウェア脆弱性を定期的に特定しているか？
- ソフトウェア/ハードウェア製品およびコンポーネントについて、組織内のサイバーセキュリティ基準/要件の準拠を継続的に評価および検証しているか？
- 新たなセキュリティ上の脅威やリスクから継続的に保護するために、潜在的なソフトウェア脆弱性を特定し、適宜、ソフトウェアを更新したり、パッチアップデートを適用したりする正式なプロセスはあるか？
- 社内開発/サードパーティ製のソフトウェア/ハードウェアのセキュリティを検証するための、独立した第三者による評価を活用しているか？

ソリューションの主な目標

弊社は、決済や連邦調達などのセキュリティ規制が設けられた市場において、セキュリティに関連するアドバイザリー、試験、監査、認証の各種サービスを提供する、認知されたリーダーです。弊社の提供するIoTセキュリティソリューションは拡大し続けています。これには、ULのIoTセキュリティレーティング、UL Cybersecurity Assurance Program（CAP）、IEC 62443、およびその他のトレーニング、アドバイザリーサービスが含まれ、安全な製品開発、スマートエコシステムにおけるサイバーセキュリティ、サプライチェーンのリスク管理に対処しています。

主にITやリスク管理の経験を持つ大半のセキュリティ企業とは異なり、ULは長年にわたり、ハードウェアベースとソフトウェアベースの両方の製品のセキュリティ評価や、業界ベストプラクティスに基づいた開発プロセスの審査を実施してきた実績があります。

ULのサプライヤー・サイバートラストレベルでは以下をご提供します：

- IoTサプライチェーンに関連付けられたセキュリティ上のリスクに対処し、これを軽減する
- 業界と利害関係者の間の連携を促進し、サイバーセキュリティに関する知識やベストプラクティスを共有する
- IoTサプライチェーンのサイバーセキュリティ保証を行うために、適切な指標や評価方法を開発し、利用する
- 組織の調達ニーズをサポートし、サプライヤーやベンダーが各自のセキュリティ対策の信頼性を実証しやすくする
- サイバーセキュリティの専門知識と組織リソースのサポートを外部から提供する

ULのサプライヤー・サイバートラストレベルの詳細については、imsecurity@UL.comにメールでお問い合わせください。または、ims.UL.com/Supplier-Cyber-Trust-Levelをご参照ください。

Empowering Trust®