

防災・身体保護システムのための ULサイバーセキュリティ認証プログラム (UL CAP)

UL CAPの試験、評価、認証サービスは、 防災・身体保護セキュリティシステムのリスクを軽減します

モノのインターネット (IoT) により、製品やシステムがネットワークに接続されることで、高度な機能が利用できるようになってきました。これにより相互接続やネットワークへの接続が可能な防災・身体保護デバイス/システムが増えています。このような技術革新が進むことにより、防災・身体保護が確実に強化される一方で、新たなリスクも生まれ、対処が必要になっています。一方、多くの業界レポートや米国政府の発表によれば、接続されたネットワークへの侵入攻撃件数は急激に増加しています。結果として、これらシステムの安全性、個人/機密情報管理、パフォーマンスの維持や向上を確保するためには、ソフトウェアのサイバーセキュリティ対策が重要になってきています。ソフトウェアの既知の脆弱性とエクスプロイトの可能性のある弱点を検証することで、システムがサイバー攻撃の対象となるリスクを軽減できます。

ULサイバーセキュリティ認証プログラム (UL CAP) では、新規格 UL 2900-1 に基づき、防災・身体保護システム向けに検証可能なサイバーセキュリティ評価基準を提供し、ソフトウェアの脆弱性や弱点の評価、エクスプロイトの最小化、既知のマルウェアへの対処、セキュリティ制御機能の見直し、セキュリティ意識の向上に取り組んでいます。

防災・身体保護システムに対する サイバーセキュリティ評価の必要性

サイバー攻撃は、発生件数が増加しているだけでなく攻撃方法も高度になってきています。ネットワークへのデバイス接続が急激に増加していることから、防災・身体保護システムをサイバーセキュリティの面から評価し、パフォーマンスと信頼性の確保、ダウンタイムの軽減、資産への損害防止、リスクの削減、セキュリティの改善、健全性と安全性の維持を図ることは必須です。

防災・身体保護システムのためのUL CAP

UL CAPは、ネットワークに接続する製品/システムのセキュリティ、および、製品やシステムを開発/保守するベンダーのプロセスのセキュリティの2つの側面からの評価が可能です。UL は信頼できる第三者機関としてのサポートを提供いたします。UL CAPを活用することでお客様は、市場ニーズに応える機能や性能の導入、または新たなテクノロジーを駆使した製品の開発に集中していただけます。市場要求の多様化が進む中、UL CAPは、企業の現在のニーズに最も即したサービスとして選ばれています。

防災・身体保護製品は、*UL 2900-1* (ネットワーク接続型デバイスのための ソフトウェアのサイバーセキュリティ規格) に準じて試験、評価、認証を 受けます。この規格では、防災・身体保護コンポーネントのデータセキュ リティ関連機能を製品レベルで評価し、既知の脆弱性に対する試験を行う と同時に、コンポーネントに影響する可能性のあるゼロデー脆弱性の発生 率を軽減するため、最小セットの検証活動を規定する方法を明らかにしま す。



防災・身体保護製品/システム向けULサイバーセキュリティ・サービスの概要



- UL 2900-1または指定された要件に基づくセキュリティ基準の試験
- UL 2900-1サイバーセキュリティ規格に準じた認証
- ・ 防災・身体保護製品/システムの開発/保守のベンダープロセスの評価とリスクアセスメント
- 製品設計時および部品を調達する際のセキュリティ整備に関するトレーニング

UL 2900-1規格は以下のコンポーネント対象ですが、この他にも適用可能です。

- 火災警報制御パネル
- ・ 煙/ガス検知機器
- ビデオカメラ
- アクセス制御
- ネットワーク機器対応の防災・身体保護システム
- 侵入検知
- ・ ネットワーク接続型ロック装置
- 警報受信機器
- PSIMシステム

- ATM
- 盗難防止機器
- 緊急通信
- 排煙設備

ネットワークに接続可能な製品/システム



防災・身体保護製品の試験に伴う成果物

サービス 成果物

認証 UL 2900-1準拠の認証書 (UL 2900準拠と記載)

試験 UL 2900-1の要件の一部または全部、または指定された要件に基づく試験レポート

トレーニング 防災・身体保護機器に関するUL 2900規格

ソフトウェアの脆弱性に関連したリスクの認識、軽減のためのベストプラクティス

UL選択のメリット

UL CAPは、重要な公共インフラのサプライチェーンに導入されているセキュリティ対策を向上したいという米国連邦政府、学会、産業界を代表する関係者からの意見をもとに開発されました。事実、ULのCAPとソフトウェアセキュリティへの取り組みは、連邦政府のサイバーセキュリティ・ナショナルアクションプラン(CNAP)で、IoTのサプライチェーンに含まれるネットワーク接続型機器を試験、認証する方法として認められています。

UL CAPを早期に導入いただくことで、市場競争における優位性の確保、およびサイバー攻撃が発生した場合に生じうる潜在的リスクの軽減が可能になります。

問い合わせ先 ul.com/jp

株式会社UL Japan カスタマーサービス E-mail: customerservice.jp@jp.ul.com T: 03-5293-6200 F: 03-5293-6201