サイバーセキュリティ対策
経営リスク軽減

狙われるIoT機器

IoT「モノのインターネット」が普及する中、サイバー攻撃は年々高度化、複雑化しています。

NICTの観測*によると、2016年のサイバー攻撃のうち約64%がWebカメラやルーターなどのIoT機器を狙った攻撃であることが判明しています。

*出典: 国立研究開発法人情報通信研究機構

IoT向けサイバーセキュリティ規格 UL 2900

UL 2900は「ネットにつながる製品やシステム」を対象とした**業界初のセキュリティ規格**です。

シリーズ規格であるUL 2900はアメリカ連邦政府からの要請で策定され、
ANSI* (米国規格協会)、FDA* (米国食品医薬品局)、その他規制当局に認められています。

✔ UL 2900の規格構成

一般要求事項	産業別要求事項	プロセス要求事項
UL 2900-1 ネットワーク接続製品SW	UL 2900-2-1 ヘルスケアシステム	UL 2900-3-1 一般プロセス要求事項
	UL 2900-2-2 産業用制御システム	UL 2900-3-2 SDLC
	UL 2900-2-3 セキュリティ・ライフセーフティシグナリングシステム	
凡例: 発行済み 開発中	UL 2900-2-X * TBD	

*ANSI: American National Standards Institute / *FDA: U.S. Food and Drug Administration
*副通則は随時策定中です。産業別要求事項が該当しない場合、UL 2900-1が適用されます。

業界初！ IoT向け
サイバーセキュリティ規格 UL 2900

サイバーセキュリティ認証プログラム (UL CAP)とは？

UL Japanは、業界初のセキュリティ規格UL 2900に基づいた「ネットにつながる製品・システム」向けの認証プログラム**UL CAP (UL Cybersecurity Assurance Program)** を提供しています。

UL CAPご利用のメリット

✔ 競合優位性

製品の信頼性が第三者による試験・認証によって証明され、市場競争で優位に立つことができます。

✔ リスクの軽減

サイバー攻撃によって、顧客情報が悪質なハッカーのもとに晒される可能性があります。予防措置を実施することによって、貴社のブランドをセキュリティリスクから守ります。

✔ イノベーション

IoTのセキュリティ対策を品質保証プログラムに組み込み、パートナーやサプライヤーが遵守すべき基本的なセキュリティ基準を確立することができます。

UL CAPサービスのプロセス

お問い合わせ

UL.com/jp

株式会社UL Japan コンシューマーテクノロジー事業部　E-mail: ConsumerTechnology.JP@ul.com

1801NS500_V1.0