サイバーセキュリティ、
早めの対策で経営リスクは軽減します

「世界初IoTサイバーセキュリティ規格」をお客様のニーズに合わせて提供、経営リスクの軽減をサポートします

つながる社会のセキュリティリスク

近年、IoT「モノのインターネット」が普及し、自動車や家電など身の回りのあらゆるモノがネットにつながる世の中になってきています。私たちの生活はより便利に、そして快適になると期待されていますが、一方でセキュリティリスクはかつてないほどに深刻化、2018年までに66%のネットワークでIoT関連のセキュリティ侵害が発生すると予測されています。*1
今やサイバー攻撃は未知のリスクとしてではなく、より身近に潜む危険として現実的な対策が不可欠です。

起こってからでは遅い、サイバー攻撃による経営リスク

事例：クライスラー、車の遠隔操作問題で140万台のリコール発表

2015年、走行中の「ジープ・チェロキー」がハッキングされ、エアコンやワイパーなどの機能を運転手の意思に反して不正に操作されてしまう動画がネット上に公開され話題を呼びました。これはセキュリティ専門家がコネクテッドカーの脆弱性に警鐘を鳴らすためにハッキングを試みた実験動画ですが、クライスラーはこの事態を受け、140万台のリコールを発表しました。*2

サイバー攻撃を受けると以下のような損害を受ける可能性があります

- 情報漏えいによる経済的な損害やブランド力の低下
- データの喪失や改ざんによる高額な資産損害
- 不測のダウンタイムや生産ロス

*1 出典：IDC Research, Inc.
*2 出典：Valsek & Miller, 2015

サイバーセキュリティ、企業の取り組みの難しさ

経済産業省からサイバーセキュリティ経営ガイドラインが発行されるなど、サイバー攻撃に対する取り組みの重要性は世間でも広く認知されはじめています。しかしネット利用の普及に伴い高度化するサイバー攻撃への防御は、製品単体としてのセキュリティだけではなく、**「接続先」を意識した対策**が必要になるなど、かつてないほどに困難で、かつコストもかかる状況となっています。

Tip:「接続先」を意識したセキュリティ対策

例えば自動車や家電、医療機器はもちろん、一見してサイバー攻撃のターゲットになりにくそうな製品でも、お互いの製品が接続されることで攻撃のエントリーポイントになってしまう可能性があります。
IoT化が進む今の社会では、製品単体では完結しない「接続先」を意識したセキュリティ対策を行い、あらゆるサイバー攻撃のリスクに備えることが重要です。

ネットにつながる製品・システム向け
セキュリティソリューション

アメリカ連邦政府から認められたサイバーセキュリティ認証プログラム（CAP*）を「第三者機関」として提供します
*CAP: Cybersecurity Assurance Program

サイバーセキュリティ規格 UL 2900の誕生

サイバーセキュリティに対する意識が高まる中、UL 2900はANSI (American National Standards Institute)、FDA (U.S. Food and Drug Administration)、その他規制当局に認められた**世界初のIoTセキュリティ評価規格**として誕生しました。UL 2900は**「ネットにつながる製品やシステム」**を対象としたシリーズ規格として**検証可能なセキュリティ基準を提供**し、製品やシステムに潜むあらゆるサイバーリスクの検知をサポートします。

ネットにつながる製品・システム向けセキュリティソリューション
サイバーセキュリティ認証プログラム（UL CAP）とは

対象製品／システム

AUTOMOTIVE　SMART TVS　SPEAKERS　SMART TOYS　LIGHTING　APPLIANCES　BABY MONITORS　ROUTERS　CAMERAS　SMART WATCHES　SMART GLASSES

- サイバーセキュリティ規格UL 2900を用い製品やシステムの**試験・認証**をご提供いたします。
- UL 2900の要求事項を満たした製品に対し、**認証書を発行いたします。**
- ご希望に合わせて、試験結果について**詳細レポート**の発行も可能です。
- UL CAPをご活用いただくことで、貴社製品の信頼性が**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るとともに、以下のようなサイバー攻撃による経営リスクの軽減が可能です。

✔ 不測のダウンタイム　✔ 生産ロス　✔ 高額な資産損害　✔ ブランド力の低下

UL CAPサービスの概要とプロセス

UL CAPではお客様のニーズに合わせて以下のサービスの提供が可能です。貴社製品・システムを安全かつ確実に市場に送り出すために提供可能なサポートをご提案させていただきます。ぜひ一度お問い合わせください。

Product and/or System →

TRAINING & ADVISORY	CAP EVALUATION & CERTIFICATION
トレーニング／アドバイザリー	CAP検証サービス
ワークショップ	ファジングテスト　静的コード　アクセス制御 脆弱性-CVE　静的バイナリ　暗号処理 侵入テスト　CWE　通信 マルウェア　ソフトウェアのアップデート
ドキュメントレビュー	

→ 試験レポート
→ 認証書

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

自動車のサイバーセキュリティについてさらに詳しく知りたい方

ホワイトペーパー（完全版）のご予約URL：QRコードからご予約いただいたお客様に自動車分野のサイバーセキュリティに関するホワイトペーパー（完全版）の配布をご案内させていただきます。また、予約受け付け中も抜粋版をダウンロードいただけます。

ご質問、ご要望も合わせてお問い合わせください。**http://connect.ul.com/DL.Cybersecurity.jp.html**

1801NS500_V1.0