IoTセキュリティ品質保証部門担当者がすべきことチェックリスト

「IoTセキュリティガイドラインVer1.0」に基づき、品質保証部門担当者がすべきことをピックアップしました。
「IoTセキュリティガイドラインVer1.0」と併せてご活用ください。

	確認項目	ガイドラインVer1.0 該当個所
☐	**守るべき機能や情報が洗い出されているか確認**	指針２、要点３
☐	**インターネットに繋がる機能があるか確認**	指針２、要点４
☐	**インターネットにつながる機能がある場合、ペネトレーションテストを実施**	指針２、要点４
☐	**つながりで波及するリスクを想定するため、以下のケースやリスクの想定がなされているかを確認** ☐機器やシステムの異常が他のIoT機器・システムに影響を与えるケース ☐ウイルスなどがつながりを介してIoT全体に波及するケース ☐機能停止することで連携する機器やシステムに影響を与えたり、ウイルス感染で踏み台にされたりすることで被害者から加害者に転じるケース ☐機器やシステムが自分自身の異常状態や他の機器を攻撃していることを認識できないケース ☐共同利用の機器やシステムを介して波及するリスク ☐対策のレベルが異なるIoT機器・システムがつながることで、対策レベルが低いIoT機器・システムが攻撃の入り口になるリスク ☐対策レベルが低いIoT機器・システムが接続されたIoTが別のIoTと接続することで全体的にリスクが波及するリスク	指針２、要点５
☐	**物理的なリスクを認識するため、以下のケースやリスクを想定する必要性を社内に提言** ☐盗まれた機器が不正操作されたり、紛失して拾われた機器が操作されIoTサービスが誤動作するようなリスク ☐駐車場の自動車や庭に置かれた機器のカバーが開けられ、不正な機器をつなげられて遠隔操作されるリスク ☐留守宅に侵入して家電の設定を変更し、不正なサイトに接続されるリスク ☐廃棄されたIoT機器のソフトウェアや設定を読み出して、つながる仕組みを解析してIoT機器の攻撃に利用したり、個人情報を読み出し、なりすましにより不正アクセスをされるリスク ☐IoT機器のソフトウェアを不正なサイトに接続させるように書き換えてオークションに出したり、中古店に販売されるリスク	指針２、要点６
☐	**個々でも全体でも守れる設計をするため、以下の対策が実装されているかを確認** ☐盗難、紛失時に遠隔から端末をロックする機能の実装 ☐ソフトウェアの難読化、暗号化 ☐機密データの暗号化、使用時のメモリなど在中時間の短縮 ☐実行時のメモリ上でのプログラムやデータの改ざんの防止	指針３、要点８
☐	**（製品の仕様上の制約等により十分な対策をとれない場合）当該IoT機器・システム使用時のリスクへの対策で考慮すべき事項がマニュアルや使用手引書等で明示されているか確認**	指針３、要点８
☐	**安心安全を実現する設計の整合性を取るため、設計の「見える化」（設計における分析、設計、評価などのプロセスを経緯や根拠も含めて可視化すること）がなされているか確認**	指針３、要点10

ネットエージェント株式会社ではIoT機器のペネトレーションテストのご相談を受け付けております。お気軽にご相談ください。