スマートライフ分野におけるリスク評価指針

ステークホルダ分類

リスク評価のステップ

評価ステップ	サービス事業者	プラットフォーム事業者	機器メーカー
①守るべき資産の特定	● ユーザへの一次提供者として、利用するプラットフォーム、機器データなど、他のステークホルダの利用規約等に留意して資産を特定	● 機器メーカーとサービス事業者を繋ぐ立場として、自組織および機器メーカの資産を特定	—
	● サービス事業者、プラットフォーム事業者等のステークホルダごとに提供するクラウドやデータを情報資産として捉えることが必要 ● スマートライフを構成する多様な構成要素からの資産の入出力プロセスに着目し、漏れなく洗い出しを行うことが必要 ● 大分類レベルの資産の最小構成まで分解するため、サービスやシステムの項目設計書との突合せ・整合確認が必要		
②脅威・脆弱性の洗い出し	● プラットフォームを介した外部との接続において、外部における脅威により事故が発生するという前提で、脅威・脆弱性を洗い出し ● （元データの問題により）誤ったアドバイスによる健康への悪影響等、間接的なセーフティ侵害について考慮 ● スマートライフサービスに対して、誰が（Who)、いつ（When)、どこで（Where)、どのように（How)、脅威、脆弱性を顕在化させるか分析が必要	● サービス/機器など他のステークホルダーに係る脅威・脆弱性の影響も受ける可能性を考慮 ● 異常の検知や脆弱性のあるバージョン等を検知した際、アラート通知等、データ連携を円滑に継続するための対策を実施	● 機器メーカーは関連法規（電安法等）の順守違反などの脅威を洗い出し ● 脆弱性が発見された場合の利用者によるアップデートの可否を検討
	● 安全性に影響を与えるセキュリティの脅威を洗い出すことで、セーフティとセキュリティの統合的なリスク分析を行うことが不可欠		
③リスクの影響評価	● データプラットフォームの停止がサービス提供に与える影響の考慮が必要 ● サービス停止により、利用者への影響を最優先に考えてリスクの影響度合いの評価が必要	● データプラットフォームが停止した場合に他のステークホルダに与える影響の範囲と大きさの評価が必要	● 機器が停止した場合の他社への影響、復旧時の急激な通信増大の影響を評価
	● 攻撃者のインセンティブを考慮して、脅威の発生可能性と影響の大きさの高いものを把握し、対策の優先度の参考とすることが重要 ● 依存する外部のサービス、機器の停止など、「動かないことのリスク」によりどのような影響を受けるかについて考慮		
④対策の検討	● サービス事業者はプラットフォーム事業者からデータが提供されない場合のサービス継続の対処が必要（別のプラットフォーム事業者からの情報取得や既存データからの推定処理の実装等） ● システムに跨る事案の原因特定に時間がかかり対応が遅れるリスクを考慮	● 想定される脅威・脆弱性の発現時の免責について、サービス提供事業者、機器メーカーに通知・対応合意が必要	● 機器メーカーは保証する動作条件や警告・禁止表示等を必要に応じて掲示するなどの対策が必要
	● マルチステークホルダによるシステムにおいて障害が発生した場合の責任範囲の明確化、エビデンスに基づく説明責任の確保 ● 事案に対し迅速な判断を行うための情報連携（エスカレーション）フローの計画を立案 ● スマートライフ分野特有となる資産ごとの特性を勘案し、機器や機能自体で対策するもの、資産を扱うプロセス面で対策するもの、等に区別することが重要		

出所：　NEDO「IoTを活用した新産業モデル創出基盤整備事業／ライフデータの高度利用システムに資するプラットフォームのあるべき姿の検討」成果より