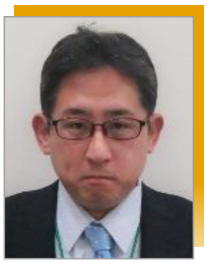
特集
Special Feature

［DX（デジタル・トランスフォーメーション）時代のサプライチェーン・セキュリティ］

6 米国を中心とした第三者機関によるセキュリティ評価の動向

基 応 専 般

―製品リスク評価のためのセキュリティ認証―



吉岡俊郎 （株）UL Japan

サプライチェーンセキュリティ

近年，製品開発時に外部委託先を含めたサプライチェーン全体でセキュリティを考慮することは，IoT 時代においてますます重要となってきている．また，IoT の普及によりネットワークに接続されるデバイスが増え，それらが相互に接続される場合もある．1 台のデバイスのセキュリティが破られることで，ほかのデバイスにも不正にアクセスされる恐れがある．IoT には利点も多い反面，攻撃者にとっては IoT 機器がエントリーポイントともなり得るものである．

そのような中，米国では 2016 年 2 月 9 日，サイバーセキュリティ対策の方針としてオバマ政権（当時）より「Cybersecurity National Action Plan (CNAP)」が発表された．発表内容には外部の有識者などで構成する委員会の設置や，190 億ドルの予算確保などが含まれる．

また同発表の中では，「国土安全保障省は，サイバーセキュリティ保証プログラムを開発するために IoT 製品分野における規格策定機関として，米国 Underwriter Laboratories Inc.（以下，UL）および他の業界パートナーと協力しており，冷蔵庫であれ医療用輸液ポンプであれ，“モノのインターネット”内のネットワークデバイスを試験・認定し，新製品を購入時にセキュリティ基準を満たしていることが認定されていることを確認できるようにする」とも述べられている[☆1]．

UL CAP と UL 2900 規格

このような背景で開発されたセキュリティ認証制度が UL CAP（Cybersecurity Assurance Program）であり，UL および連邦政府・学会・産業界を代表する関係者により開発された．UL は，1894 年に米国で設立された安全認証機関で，家電製品・自動車・産業機器・電子部品・エネルギー関連機器等の分野でサービスを展開し，2020 年 11 月現在では 143 カ国以上に拠点を構えている．また，UL は安全規格策定機関として規格作成能力を保有し，これまでに約 1,600 の UL 規格が策定され，うち 50% 以上が ANSI 規格（米国国家規格）として採用されている．

UL CAP は，IoT のサプライチェーンにおけるコネクテッド製品を試験・認証するための制度であり，コネクテッド製品のセキュリティに関するベストプラクティス等を規定した「UL 2900」規格群を基に実施される．本制度には，網羅的に脆弱性を検査する「脆弱性診断」，攻撃者の観点から攻撃が成功するかどうかを確認する「ペネトレーション試験」，さまざまな入力を行うことで脆弱性を検査する「ファジング試験」，ソースコードや実行コードを実行せずに構文や処理フローなどの解析を行う

☆1 https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan

© 2021 Information Processing Society of Japan

「静的コード解析・バイナリ解析」といった製品に対する試験に加え，「開発プロセス」「リリース後のパッチ管理プロセス」の確認といったソフトウェアの設計開発や運用体制に対する評価も含まれる．これらの検証をクリアした製品には1年間有効の認定書が発行される．認定書には評価実施時に参照されたNIST脆弱性データベース☆2の日付も記載されるため，どの時点での脆弱性の情報を基に上記の検査が行われたかが分かるようになっている．

UL 2900規格はソフトウェアのセキュリティに一般的に求められる事項（一般要求事項）を含むPart1，および特定分野の製品要求事項を含むPart2で成り立っている．このうちUL 2900-1（一般要求事項），UL 2900-2-1（ヘルスケアシステム），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）は米国国家規格協会（ANSI）およびカナダ標準審議会（SCC）により承認されている．またUL 2900-2-1は米国食品医薬品局（FDA）によりRecognized Consensus Standardに認定されている．これにより，ネットワーク接続型の医療機器を製造・開発し，米国FDAへの申請を行う際には，同規格を参照することができる．

☆2 https://nvd.nist.gov/

■図-1 UL2900-1:2020規格

UL 2900要求事項

例としてUL 2900-1規格の要求事項を取り上げる．

序文において，本規格の趣旨として3点が述べられている．

a）製品に対するソフトウェア開発者（ベンダもしくはその他サプライチェーン）のリスクマネジメントプロセス要求事項．表-1の「リスクマネジメント」のカテゴリがこれに相当する．

b）脆弱性・ソフトウェアの弱点・マルウェアの存在に対する製品評価･試験方法．表-1の「脆弱性･エクスプロイト」と「ソフトウェア脆弱性」のカテゴリがこれに相当する．

c）製品アーキテクチャ･設計におけるセキュリティリスクコントロールに関する要求事項．表-1の「リスクコントロール」，「製品および使用に関するドキュメンテーション」のカテゴリがこれに相当する．

さらに，医療分野を対象とする規格であるUL

■表-1 UL 2900-2-1規格 主な要求事項

カテゴリ	項目
製品および使用に関するドキュメンテーション	製品設計ドキュメンテーション
	製品使用時ドキュメンテーション
リスクコントロール	リスクコントロール
	アクセスコントロール・ユーザ認証
	リモート通信プロトコル
	機密情報
	製品マネジメント
リスクマネジメント	ベンダ製品リスクマネジメントプロセス
脆弱性・エクスプロイト	公知脆弱性試験
	マルウェア試験
	不正入力試験（ファジング）
	ペネトレーションテスト
ソフトウェア脆弱性	ソフトウェアの弱点の分析
	静的ソースコード解析
	静的バイナリ―・バイトコード解析

© 2021 Information Processing Society of Japan

2900-2-1（ヘルスケアシステム）においては，組織観点でのセキュリティ要求事項として「品質マネジメントシステム」「購買プロセス・購買におけるリスクマネジメントプロセス」「製品アップデートリリース・パッチマネジメントプロセス」「廃棄プロセス」に関する内容が盛り込まれている．

このように，IoT 製品に関するセキュリティ試験やソースコード・設計文書・リスクマネジメントプロセス等を含めたレビューを第三者の立場で行うことで，製品が適切に設計され，かつその設計が正しく実装されているかどうかを確認することができる．

第三者評価により得られるメリット

このような第三者機関によるセキュリティ評価を実施し認証を取得することで，製品のセキュリティレベルに対する客観的な評価を得ることができる．これは市場における製品展開上の差別化要因となり得る．また，製品内の一部コンポーネントに対する評価ではなく機器全体に対する評価を行うこととなるため，包括的なセキュリティ評価が可能となっている．

（2020 年 11 月 4 日受付）

■吉岡俊郎　toshiro.yoshioka@ul.com

法政大学卒業．システムエンジニア・プロジェクト管理業務を約 10 年経験後，Gemalto（現・タレス DIS）などを経て 2020 年より UL Japan にてプログラムマネージャとしてサイバーセキュリティ業務に携わる．

© 2021 Information Processing Society of Japan