32SQiP 研究会　特別講義　レポート

作 成 日：　2017 年 1 月 16 日
書記氏名：　大島　修

日時	2017 年 1 月 13 日（金）　10:00 ～ 12:00
会場	(一財) 日本科学技術連盟・東高円寺ビル　地下 1 階講堂
テーマ	「IoT 時代」のセーフティ&セキュリティ by デザイン ～アシュアランスケースとコモンクライテリア(ISO/IEC15408)によるセキュリティの品質保証を考える～
講師名・所属	金子　朋子　氏（情報セキュリティ大学院大学　客員研究員　公認情報セキュリティ監査人）
司会者	栗田　太郎　氏（ソニー株式会社）
アジェンダ	１．つながる世界の開発指針～安全安心な IoT の実現に向けて～ ２．IoT の特徴と開発の課題 ３．セキュリティ・バイ・デザイン ４．セキュリティ設計　主な分析技法・リスク評価手法 ５．セキュリティ設計の評価・認証 ６．ロジカルな設計品質の説明 ７．アシュアランスケースによるセキュリティ要件の見える化
アブストラクト	『「IoT 時代」のセーフティ&セキュリティ by デザイン～アシュアランスケースとコモンクライテリア(ISO/IEC15408)によるセキュリティの品質保証を考える～』と題して、昨今のセキュリティ問題に対する対策について、御講演頂きました。 その中で、セキュリティ設計の重要性に触れ、セキュリティ・バイ・デザインの考え方のもと、主な分析技法・リスク評価手法、評価・認証、Protection Profile の適用、見える化のためのアシュアランスケース等について、御教示頂きました。 これまで、セキュリティ対策は必須であるとの漠然とした認識はありましたが、具体的に、どのような方法で品質保証をするかまでは確立されていなかったため、今回大変貴重な情報を御教示頂きました。 尚、第 33 年度ソフトウェア品質管理研究会から、「演習コースⅢ：セーフティ&セキュリティ開発」が新設されるため、興味のある方は是非とも参加して頂きたいと思います。 ありがとうございました。

第 8 回の特別講演では、『「IoT 時代」のセーフティ&セキュリティ by デザイン～アシュアランスケースとコモンクライテリア(ISO/IEC15408)によるセキュリティの品質保証を考える～』と題して、金子さんから御講演を頂きました。
金子さんは、10 年ほど前から情報セキュリティ大学院大学で学んでおり、公認情報セキュリティ監査人(CAIS)でもあります。又、産官学の組織に同時に所属している貴重な存在であり、多方面で御活躍されております。
以前、ソフトウェア品質管理研究会の特別コースに参加した経験もあり、研究者視点で丁寧に御説明頂きました。
ありがとうございました。

１．つながる世界の開発指針～安全安心な IoT の実現に向けて～
<ビデオ講義>
◆IoT：Internet of Things（インターネットオブシングス）の略。
◆17 の指針
例）
・保守：アップデートを自動的に実施。ログの分析・保管。
・運用：パスワードが出荷時のまま、アップデートされていなかった。つながるリスクへの周知。
◆IPA において、17 の指針の続編を策定中であり、2017 年 3 月以降に発行予定。

２．IoT の特徴と開発の課題
◆設計がまとまってからセキュリティの対処を検討するのではなく、もっと企画・設計の前段階から考えることが重要である。
◆米国で 14 歳の少年が ATM のハッキングをした事件があったが、幸いにもホワイトハッキングであり、脆弱性を発見してもらったこともあって後で表彰された。
◆IoT ハッキング技術を身につけ、実践を始めるハッカーが増加する一方で、ハッキングコンテストを実施して脅威に対応している組織もある。
◆IoT セキュリティの対象となる機器やシステムに対する脅威には様々なものが想定されるが、全て洗い出されていない。更に、業界、製品、システムごとに要件が異なるため、セキュリティ対応レベルが異なり、標準化の動向も異なっている。
→故に、IoT のセキュリティを確保するための技術や手法、標準、基準はまだ確立されていない。

３．セキュリティ・バイ・デザイン
◆セキュリティ・バイ・デザインとは、「情報セキュリティを企画・設計段階から確保するための方策」である。
◆平成 28 年 8 月 26 日に内閣府サイバーセキュリティセンターから発表された「安全な IoT システムのためのセキュリティに関する一般的枠組」は IoT の憲法と言われている。
◆セキュリティ・バイ・デザインのメリットは、以下である。
①手戻りが少なく納期を守れる
②コストも少なくできる（運用時のセキュリティ対策コストは、設計時を 1 とした場合の 100 倍）
③保守性の良いソフトウェアができる
セーフティの観点だけでなく、セキュリティの観点も追加して、総合的観点で問題の解決にあたることが重要。

４．セキュリティ設計　主な分析技法・リスク評価手法
◆そもそも、セキュリティ設計ができていないのではないか？
→セキュリティ設計の基本方針・設計ルールを明文化している組織は多くない。分母は少ないが、調査対象の約半分が「明文化されたものはない」というデータがある。
◆セキュリティ設計プロセスは、要件定義、設計の各フェーズで脅威分析（セキュリティ要求分析）を実施して、随時反映する。
◆セキュリティ機能は「非機能要件」であり、お客様に納得していただき、ギャップを埋めることが難しい。
◆セキュリティ特有の課題として攻撃者の存在があるが、世の中には良い人しかいない訳ではなく、悪い人もいる前提で考える。

◆脅威の特定・分析手法として、以下の例がある。
・STRIDE：マイクロソフトが定義する脅威モデル
・ミスユースケース：ユースケースに攻撃者を追加したミスユースケース図
・Attack Tree：攻撃者のゴールを設定し、ゴールに至る攻撃手順をツリー上に展開
◆脅威に対するリスクの見積もり及び評価には、以下の例がある。
・ハザード分析を利用したリスク評価：FTA、FMEA、HOZAP などのセーフティ手法
・CVSS：情報システムの脆弱性に対するオープンで汎用的な評価方法
・i＊（LIU 法）：ゴール指向要求分析の 1 つである i＊手法を拡張したセキュリティ要求分析手法
・SARM：攻撃と通常のシステム機能との間のセキュリティ上の関係を分析するための要求分析手法

５．セキュリティ設計の評価・認証
◆「保証」を英語で言うと、「assurance（アシュアランス）」である。
◆汎用的で広く認知されたセキュリティ基準として 2 つの国際規格がある。
・CC（ISO/IEC15408）=IT セキュリティ評価標準　→セキュリティ機能を評価する規格である
・ISMS（ISO/IEC27001）=セキュリティ・マネジメント規格　→セキュリティ機能を評価する規格ではない
◆一般の IT 機能は実際に利用してみることで保証されていることを確認できるが、セキュリティ機能は不測の事態を発生させて正確かつ有効に動くことを確認することは困難である。
◆開発者がセキュリティ保証を検証しなければならない。このセキュリティ保証を確認するのが第三者によるセキュリティ評価である。
→セキュリティ評価の国際規格：コモンクライテリア（CC）の保証
◆具体的には CC（IT セキュリティ評価の国際標準）を基にセキュリティ仕様を書いて、評価する。
◆CCRA：セキュリティ評価における相互認証を実現しており、日本を含む 17 カ国が認証書生成国、8 カ国が認証書受入国となっている。
◆CC は日本においては、電子複合機などの特定の製品の認証が多く、広く普及しているとは言えず、コストが掛かることを批判する人もいるが、認証制度運用方法と認証の方式や参照とする基準は分けて考えるべきである。
又、セキュリティ機能要件というツールボックスと保証要件の規定という優れた点がある。
◆PP（Protection Profile）とは、特定の製品分野のために用意されるセキュリティ要件であり、想定されるセキュリティ課題、機能要件を定義し、調達者、業界団体等が開発し、調達要件として活用するものである。
→実際の PP は IPA のサイトから参照可能であり、誰でも見ることができる。
◆PP は評価対象のタイプ（OS、ファイアウォール、スマートカード等）に対するセキュリティの設計仕様書であり、具体的な実装方法に依存しないため、多数の製品・システムの ST（セキュリティターゲット）で再利用可能である。

６．ロジカルな設計品質の説明
◆セーフティとセキュリティの概念：セキュリティはセーフティを含む。
◆セキュリティ・バイ・デザインの考え方はセキュリティだけのものではない。セキュリティで脅かされるセーフティも守ることができる。
◆セキュリティ設計プロセスの「脅威分析（セキュリティ要求分析）」とセーフティ設計プロセスの「ハザード分析」は一緒にやる。
→双方が“設計品質を見える化”して、持ち寄ってすり合わせを行う。

７．アシュアランスケースによるセキュリティ要件の見える化
◆アシュアランスケース（ISO/IEC15026）とは、テスト結果や検証結果をエビデンスとしそれらを根拠にシステムの安全性、信頼性を議論し、システム認証者や利用者などに保証する、あるいは確信させるためのドキュメントである。
◆GSN は代表的なアシュアランスケースの表記法であり、保証のための構造化された議論の記述ができる。
◆日本で主流のウォーターフォールモデルはイテレーションがないため、セキュリティ・バイ・デザインを実現しにくい。

→外注によってソフトウェアを作ると、ウォーターフォールになりがちであり、要件が頻繁に変わることに対応し辛い。

◆設計、QA の双方でセキュリティに関するケースを作成し、それをぶつけることによって脆弱性を発見する。

<全体的な Point！>

・セキュリティ・バイ・デザインは企画・設計段階から！
・セーフティ設計とセキュリティ設計の擦り合わせ！
・その設計によって目標が達成されることが事実に基づき論理的に説明されていること！
・設計の見える化、変化するリスクへの対応、セーフティとセキュリティの擦り合わせ！

<ソフトウェア品質管理研究会新設コースの案内>

◆第 33 年度ソフトウェア品質管理研究会（2017 年 5 月～2018 年 2 月）から、演習コースⅢ：セーフティ&セキュリティ開発が新設される。

主査：金子 朋子（情報セキュリティ大学院大学）
副主査：高橋 雄志（株式会社トレドシステム）
アドバイザー：勅使河原 可海（東京電機大学）

<質疑応答>

◆「セーフティとセキュリティの特徴の比較」の発生頻度において、脅威の洗い出しをするが、それに対してどのような優先順位で対策を取捨選択するのか?

→現在基準がないが、確立しようと研究中の人もいる。発生頻度よりも、重要度の方が重要と考えており、そちらに重み付けをして対処することも考えられる。

→現場では、たくさんリスクを洗い出すが論理的に洗い出せない。又、やりっ放しで定着しない傾向が強いため、合理的な選択基準があると良い。

◆セキュリティとセーフティは全く考え方の空間が異なる。リスクを全て洗い出すことができない。そもそも、リスク認識ができないのではないか?

→総当りでやらなければいけないのは事実。システムエンジニアリングの技法等で全体の構造を書いていかなければならない。AI に頼るべきという人も居る。

攻撃側の心理が解っていないと対策が出来ない。心理学的ところではないか?

→何が目的でこういう攻撃をするのかの意図を把握することが重要でそれに対して対策を確実に実施できるのが理想である。攻撃者は脆弱性の穴を 1 つ見つければ良いが、守る方は全てに対応するので大変である。そうは言っても、悪意のない人間の方が多い。またセーフティに比べ、セキュリティは機能がはっきりしているという利点もある。

以上