第 6 回特別講義　レポート

日時	2019 年 11 月 15 日（金）10:00 ～ 12:00
会場	（一財）日本科学技術連盟・東高円寺ビル　2 階講堂
テーマ	IoT 時代のリスク評価・リスクコミュニケーション
講師名・所属	佐々木 良一氏 （東京電機大学 総合研究所 特命教授／サイバーセキュリティ研究所長／本研究会 セーフティ&セキュリティ アドバイザー）
司会	金子 朋子 氏（情報セキュリティ大学院大学／本研究会 セーフティ&セキュリティ 主査）
アジェンダ	1. サイバー攻撃の動向 2. 従来のリスク評価・リスクコミュニケーション 3. 多重リスクコミュニケータ MRC の基本方式 4. 多重リスクコミュニケータ MRC の拡張 5. IoT 時代のリスク評価・リスクコミュニケーション 6. おわりに
アブストラクト	IT システムは、社会の重要基盤の一つとなっており、その安全性が失われる影響は非常に大きなものになってきた。講演者らは、IT システムに対する適切なリスク対策を可能とするため IT リスク学の名のもとに、リスク評価・リスクコミュニケーション支援手法や支援システムの開発を行うとともにいろいろな実適用を行ってきた。IoT 時代を迎え、従来の方式だけでは不適切であると考え、IoT 時代に適したリスク評価・リスクコミュニケーション支援手法・ツールを開発するとともに、医療用 IoT システムなどへ適用した。本講義では、これらの研究結果について解説する。

講義の要約

◆講師紹介

佐々木 良一 氏

1971 年３月　東京大学卒業。
1971 年４月　株式会社日立製作所 入社
　　システム開発研究所にてシステム高信頼化技術、セキュリティ技術、ネットワーク管理システム等の研究開発に従事。
2001 年４月～2018 年３月　東京電機大学教授。
　　情報セキュリティの研究と教育に従事。
2018 年４月　現職。

1. サイバー攻撃の動向

サイバー攻撃の歴史

◆セキュリティにとっての第一のターニングポイント：2000 年 科学技術庁などのホームページの改ざん事件。

◆セキュリティにとっての第二のターニングポイント：2010 年 Stuxnet の出現（遠心分離機への攻撃）

◆第一と第二では攻撃目標が異なり、第二からは標的型に移ってきており、攻撃技術も高くなっている。

今後、増加が予想される攻撃

１．被害の大型化

仮想通貨 580 億円相当の不正流出する事件

２．被害形態の多様化：機密性の喪失から完全性や可用性の喪失へ

脅威の分類

(1)機密性（Confidentiality）の喪失: 表法を不当にみられる

(2)完全性（Integrity）の喪失：情報を不当に破壊、改ざんされる

(3)可用性（Availability）の喪失：不当な利用によりデータやコンピュータパワーが使えなくなる

３．攻撃対象の多様化： PC などから IoT などへ

IoT の特徴とセキュリティへの影響: IoT には、

（１）脅威の影響範囲・影響度合いが大きい

（２）IoT 機器のライフサイクルが長い

（３）IoT 機器に対する監視が行き届きにくい

（４）IoT 機器側とネットワーク側の環境や特性の相互理解が不十分

（５）IoT 機器の機能・性能が限られている

（６）開発者が想定していなかった接続が行われる可能性がある、という性質があり、セキュリティ対策がより重要になっている。また、IoT ではセキュリティがセーフティに及ぼす影響を考えていく必要性が出てきている。

例）「制御装置: 電力会社へのサイバー攻撃で 140 万世帯が停電」、「自動車: Blackhat での自動車の遠隔操作法の発表」、「電子掲示板: 交通標識が『ゴジラ来襲』と警告」

また、製造工程からバックドアが設置されるなどのサプライチェーンにおける脅威もある。

４．愉快犯から経済犯・組織犯へ：犯罪組織の高度化

昔は個人（愉快犯）が多かったが、今一番多いのは金銭入手である。サイバー犯罪者組織では役割の分化も行われている。

2. 従来のリスク評価・リスクコミュニケーション

◆社会の IT システムへの依存: IT システムへの依存は増大しており、情報セキュリティの問題が重要

◆ISMS と PDCA: リスクマネジメントの仕組みとして ISMS（Information Security Management System）がある。ISMS とは、組織のマネジメントとして、自らのリスクアセスメントにより必要なセキュリティレベルを決め、プランを持ち、資源を配分して、システムを運用することである。（https://isms.jp/isms/）

◆リスクとは「将来の帰結に対する現在における予測」という見方が下敷きになっており、常に不確実性とをもなう。工学分野ではリスク＝損害の大きさ×損害の発生確率で定義されるが、情報分野ではリスク＝資産価値×脅威×脆弱性で定義される。

◆リスク社会: 自然災害などをコントロールするためのシステムが新たなリスクとして問題になってきている。

◆誤ったリスク認識の例: 2001 年の 9・11 後、飛行機が危険との認識で、自動車の利用者が増えたが、それによって、自動車事故の死亡者数が増加。飛行機による事故の約 6 倍であった。

◆日本人のリスク感の特徴: ①リスクに極めて敏感でゼロリスクを求める傾向、②安全よりも安心を重視する傾向、③リスクに対しあきらめてしまう傾向

◆リスク社会学者などが指摘するようにリスクを制御するのは限りなく難しい。しかし、そこにリスクがある以上、当事者は万全の注意を払ってリスクに対応し続けるしかない。そのため IT リスクに応じてどう対応すべきかを明確化していく必要がある。

◆リスク評価法の分類

１．リスク分析のアプローチの方向

①ボトムアップ型（情報資産の洗い出し）：チェックリスト法など

②トップダウン型（情報システム上の脆弱性の洗い出し）：アタックツリー法など

２．リスク分析における量的扱い

①定量的アプローチ：例）指紋認証に関するアタックツリー分析法

②準定量的アプローチ：例）JPDEC のリスク算出式、25 マスによる準定量的分析方法

③定性的アプローチ：例）チェックリスト利用法、質問票利用法、シナリオ分析法

3．リスク評価の目的と範囲

①リスクの大きな情報資産やシステムの明確化

②上記＋必要なリスク対策の明確化：こちらが望ましい

3. 多重リスクコミュニケータ MRC の基本方式

◆基本的認識とアプローチ

1．ゼロリスクはないので定量的リスク評価が不可欠である。

2．IT システムのリスクは多様であるので、ＩＴシステムが扱う情報の安全だけでなく、ＩＴシステムそのものの安全や、ＩＴシステムが行うサービスの安全も同時に扱う必要がある。

3．リスク対策が別のリスクを引き起こすことがあるので「リスク対リスク」「多重リスク」への考慮が不可欠である.

4．多くの関与者がおり、パラメータの設定などに不確実性を伴うのでリスクコミュニケーションの導入が不可欠である

◆リスクコミュニケーションが必要になった背景

（1）人はリスクの存在そのものを認識できないのではないか。

人はリスクに直面し判断せざるを得ない場合は少なくないが人知を超える判断はいずれにしろできない。

（2）リスクの存在を認識できたとしてもフランク・ナイトが指摘するようにその事象の発生確率は測定できない場合が多い

（3）事象の発生確率やその損害の大きさを推定できたとしてもそれらの値そのものに不確実性が残る。

ナシーム・タレブが指摘するようにすべての確率は主観確率。よって、各人の主観を明確にしそれらのあいだの合意形成を図るしかない

◆リスクコミュニケーションの分類と目的

・リスクコミュニケーションのフェーズ分類

（フェーズ１）そのリスクに関連する情報を提供するフェーズ

（フェーズ２）対象となる事象や対象システムが受け入れられうるものかどうかの検討のためのフェーズ

（フェーズ３）そのままでは受け入れられないとすれば、どのような対策をとるべきかを決めるフェーズ

・リスクコミュニケーションの目的

目的① 個人的選択：例）禁煙の実施、インフルエンザワクチンの接種

目的② 組織内合意形成：例）工場の環境対策、オフィスの省エネ対策

目的③ 社会的合意形成：例）原発再稼働の可否、BSE 対策のための全頭検査

◆多重リスクコミュニケータ MRC の対象は目的②の組織内合意形成である。

◆MRC の背景

背景１．多くのリスク（セキュリティリスク、プライバシーリスクなど）が存在＝＞リスク間の対立を回避する手段が必要

背景２．ひとつの対策だけでは目的の達成が困難＝＞対策の最適な組み合わせを求めるシステムが必要

背景３．多くの関与者（経営者・顧客・従業員など）が存在＝＞多くの関与者間の合意が得られるコミュニケーション手段が必要

◆MRC における対応

①多くのリスクやコストを制約条件とする組み合わせ最適化問題として定式化

②関与者の合意が得られるまでパラメータの値や制約条件値を変えつつ最適化エンジンを用い求解

◆関与者間のリスクコミュニケーションの一例

１．制約条件に関するもの

（１）もっとコストをかけてもいいのではないか　（従業員代表の意見）

（２）情報の漏洩確率は、半分ぐらいにできないか　（顧客代表や経営者の意見）

（３）プライバシー負担度をもっと小さくしてほしい　（従業員代表の意見）

（４）利便性負担度をもっと小さくしてほしい　（従業員代表の意見）

２．対策案に関するもの：この対策案は使いにくくて困る。外した場合の対策案最適組あわせを求めてほしい　（従業員の意見）

３．対策効果などに関するもの：この対策はそんなに効果はないと思う

◆納得のプロセス

①説明を聞くことによる納得（確かにそういうような対策案はあるな、確かにそういうような制約条件はあるな）

②条件を変えて再計算を行った結果による納得（パラメータの値を変えても最適の対策案はあまり変わらない）

③相手に対する信頼による納得（彼の言うことだから間違いないだろう）

4. 多重リスクコミュニケータ MRC の拡張

１．リスクコミュニケーション法の拡張

（１）合意形成対象者が 1000 人を超すような問題への適用

・合意形成対象者が 1000 名を超すような社会的合意形成問題には従来の MRC は適用できない。

・オピニオンリーダ向けの従来 MRC 支援システムである MRC-Studio と一般関与者の意見を導入するための MRC-Plaza からなる Social-MRC を開発

・Social-MRC を青少年への情報フィルタリング問題に試適用。一般関与者 20 名のうち 75%が Social-MRC はこの問題に関する対策案の合意を形成するのに有効と回答。一般関与者の 85%が最終回は合理的なものであると回答

（２）経営者とのリスクコミュニケーションも考慮した多重リスクコミュニケータ

２．リスク評価法の拡張

（１）標的型攻撃等多段にわたる攻撃のリスク評価のためのリスク解析法（EDC 法）の開発

・・従来はアタックツリーを用いてリスク分析を行っていたが、EDC 法を開発。

・・イベントツリー分析とは、標的型攻撃メールなどの初期事象から時系列順に攻撃事象の成功・失敗を追うことでそれぞれのシーケンスの発生確率を求める分析手法。またそれぞれの発生確率にその影響度をかけることで定量的にリスクを求めることができる。

・・発生確率を求めるために、ディフェンスツリー分析を用いる。

・東京電機大学の次期セキュリティ対策に対して EDC 法を実適用し、リスクとコストが最少となる対策案を最適解として適用。

（２）被害発生防止対策と復元対策の両方を考慮した対策案最適組合せ法

・・イベントツリー分析法を採用することにより、確率と影響の大きさの両方の扱いを可能化

・・PERT 手法を用いることにより影響の大きさの推定を可能に

（３）動的リスクを考慮した多重リスクコミュニケータ

（４）発生確率の不確実性を考慮した多重リスクコミュニケータ

・・発生確率をあいまいであると考えて、最適な組み合わせを求める。

5. IoT 時代のリスク評価・リスクコミュニケーション

◆Society5.0:サイバー空間（仮想空間）とフィジカル空間（現実空間）を高度に融合させたシステムにより、経済発展と社会的課題の解決を両立する、人間中心の社会。IoT が中心となって入ってくる。

◆IoT の特徴とセキュリティへの影響: IoT には、

（１）脅威の影響範囲・影響度合いが大きい

（２）IoT 機器のライフサイクルが長い

（３）IoT 機器に対する監視が行き届きにくい

（４）IoT 機器側とネットワーク側の環境や特性の相互理解が不十分

（５）IoT 機器の機能・性能が限られている

（６）開発者が想定していなかった接続が行われる可能性がある

という性質があり、セキュリティ対策がより重要になっている。また、IoT ではセキュリティがセーフティに及ぼす影響を考えていく必要性が出てきている。

◆IoT システムでは対象によってセキュリティ対策が大幅に異なる。

◆IoT システムのリスク評価法の開発

・・方式１：制御型ＩｏＴシステムに対するセキュリティとセーフティを考慮したリスク評価法

例）インスリン注射システム

・　・フィードバックがあるので従来のアタックツリーのようなものだけではアンセーフな事象の適切な抽出が困難 -> STPA 手法によりハザードを導き出す

・　・従来の STPA にはサイバー攻撃が入っていない -> STPA 手法にサイバー攻撃を追加

・STPA では対策案までは対象としていない -> 多重リスクコミュニケータを改良し、対策案の最適な組み合わせを求められるようにする

・・方式２：センサー型ＩｏＴシステムに対するＭＳＳを考慮したリスク評価法

例）敷布型マルチバイタル IoT モニタ

・システム導入によるメリットとデメリットを考慮する

6．おわりに

まとめと今後の方向

1.リスク評価方法の推移と最近の動向を紹介

2.特に、定量的リスク評価に基づき、対策案の最適組み合わせを求める多重リスクコミュニケータとその改良版について詳しく紹介

3.最近は IoT システムのリスク評価方法や、サプライチェーンを考慮したリスク評価方法が大切になってきている

4.今後は AI システムのリスク評価も重要に

質疑応答

1. EDC 法の東京電機大学への適用にかんして、セキュリティをどれだけのコストをかけるか:コスト試算について、どのように一般化していくらと分配したのか？

→実際の分析は一回では終わらず、複数回行う。一回目はざっくりおこない、2 回目以降はベンダーも決まってくるので、コストや効果が細かくわかってくる。

以上