特集論文

IoT時代のセキュリティリスクアセスメントへの取組み

佐藤明行*　細川智洋*
猿渡新路*
植田　武**

Approach to Security Risk Assessment in IoT Era

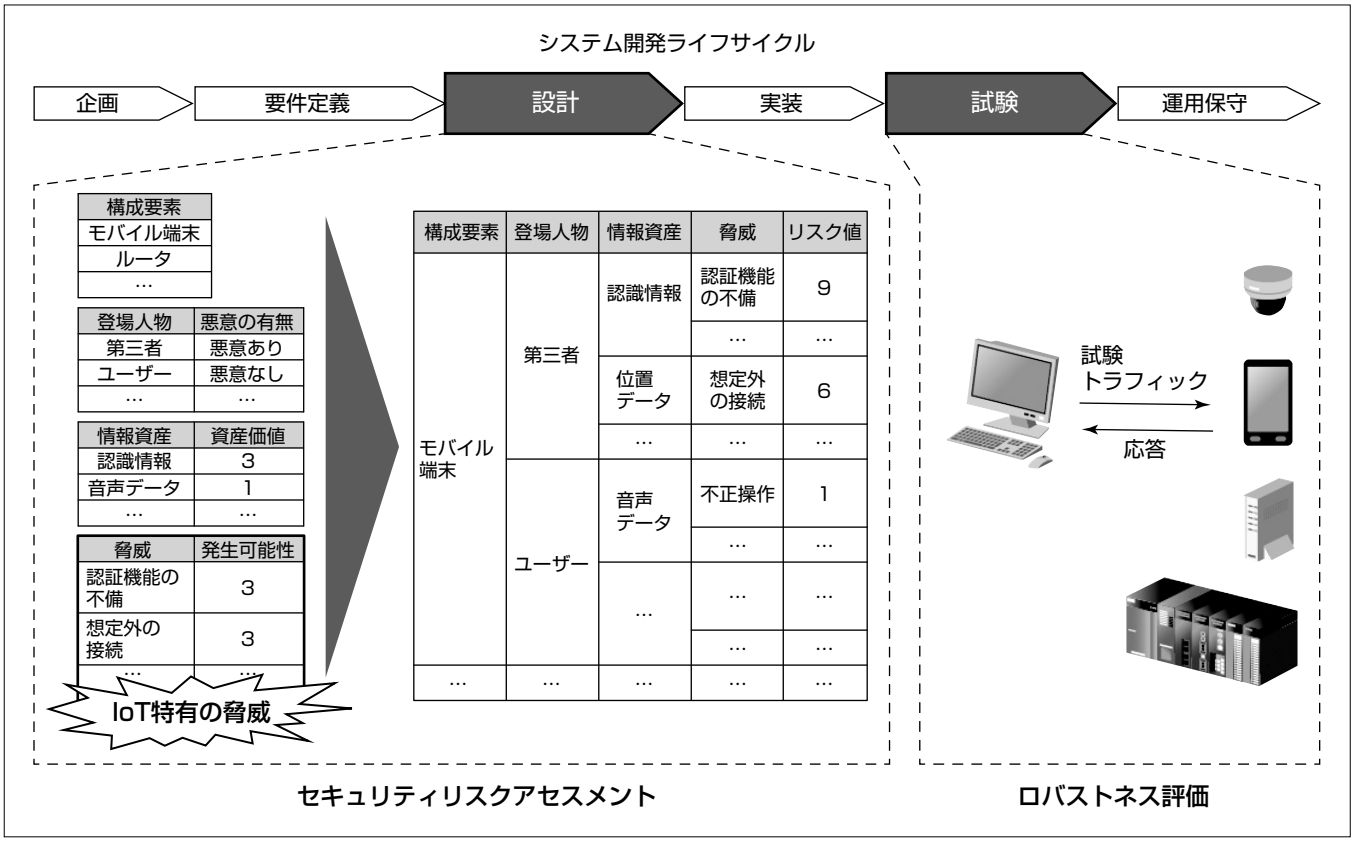
Akiyuki Sato, Shinji Saruwatari, Takeshi Ueda, Tomohiro Hosokawa

要　旨

IoT(Internet of Things)は，エアコン等の家電機器や監視カメラ等の防犯機器はもとより，住宅，製造業，医療，農業，自動車等の様々な分野への適用が期待されている。その一方で，今までインターネットに接続されてこなかったモノがネットワークにつながることで，マルウェア“Mirai”に代表されるような外部からの攻撃にさらされるおそれがある。このような状況にあるIoTでは，従来の機器やソフトウェアのバージョン管理，セキュリティ設計チェックだけでは予測できない新たな脅威・脆弱(ぜいじゃく)性の存在が危惧される。

新たな脅威や脆弱性を低減するためには，システム開発のライフサイクル全体にわたるセキュリティ対応プロセスが重要と考え，三菱電機インフォメーションシステムズ㈱(MDIS)と三菱電機の情報技術総合研究所と連携して設計段階でのセキュリティリスクアセスメント，試験段階でのロバストネス評価など，システム開発ライフサイクル全体でのセキュリティ対応プロセスの構築を行う取組みを行った。セキュリティリスクアセスメントは五つの作業ステップで，情報資産価値と脅威の発生可能性からリスクの度合いを明確にする。それに基づいてセキュリティ対策を適用し，ファジングテストなどでシステムのロバストネスを評価する。

今後の課題であるアセスメント作業の効率化と属人性排除に向けて，セキュリティリスクアセスメント用ツールとアセスメントに関するノウハウなどの情報を集めた社内共有データベースの充実化を図っていく。



セキュリティリスクアセスメントとロバストネス評価

IoT機器が攻撃対象となるセキュリティ事故が急増している。サイバー攻撃などのセキュリティリスクへの対策として，システム開発ライフサイクルの設計段階で実施するセキュリティリスクアセスメントと試験段階で実施するロバストネス評価が重要になっている。前者は守るべき情報資産，想定されるIoT特有なものを含めた脅威，脅威による影響度合いを明確にする。後者はアセスメント結果から行った対策の効果を確認するため試験段階で開発システムに通信データとして問題を引き起こしそうなテストデータを送信し，脆弱性が存在しないかを評価する。

*三菱電機インフォメーションシステムズ㈱　**三菱電機㈱ 情報技術総合研究所

1. まえがき

従来，インターネット等の通信環境とは無縁であった機器が通信機能を持ち，インターネット等の通信環境に接続されて動作するIoTシステムが市場で急速に拡大しており，近い将来にはインターネット等の通信環境に接続される機器が爆発的に増加すると予測されている。一方で接続された機器へのサイバー攻撃の脅威や未知の脆弱性による脅威が増大することが懸念されている。

IoTシステムは工場や公共インフラに使用される機器のように長期間利用されるものや，センサデバイスのようにコンピューティングリソースに制約があるもの等，多様な特性を持った機器で構成されており，IoT機器やIoTシステムの特性を踏まえたセキュリティ対策の検討が急務となっている。

MDISと三菱電機の情報技術総合研究所は連携してIoTのセキュリティ対策に取り組んでいる。

本稿ではセキュリティリスクアセスメントの進め方，及び，アセスメント結果から行った対策の効果を確認するロバストネス評価について述べる。

2. IoTのセキュリティ事故事例

昨今注目を浴びているIoTは，センサと通信機能が組み込まれた様々な“モノ(物)”がインターネットに接続され，それぞれが情報交換することで相互に制御させる仕組みのことである。監視・管理対象下にあるそれらの機器のデータを収集することで各機器の状態を把握し，その状態に応じて各機器の最適な制御を行うことができる。また，蓄積したデータを分析し，新たな知見が得られることも期待されている。IoTは，エアコン等の家電機器や監視カメラ等の防犯機器を接続したシステムを始めとして，住宅，製造業，医療，農業，自動車等の様々な分野への適用が期待されている。

一方，今までインターネットに接続されてこなかったモノがネットワークにつながることで，新たに外部からの攻撃にさらされるおそれがある。IoT機器は，廉価な機器で十分なセキュリティ対策が施されていない場合が多く，攻撃者に狙われることが懸念されている。事実，最近ではIoT機器を狙ったサイバー攻撃が増加しているとの報告がある[1]。

2016年10月には米国で，マルウェア“Mirai”に感染した監視カメラ等のIoT機器を踏み台にしたサイバー攻撃が発生した。Miraiに感染した複数のIoT機器は，特定のDNS(Domain Name System)サーバや企業サイトに対して大量にメッセージを送信するDDoS(Distributed Denial of Service)攻撃を行った。これによって，当該DNSの停止による関連サイトの閲覧不能や企業サイトの停止等の被害に至った。このMiraiで行われたDDoS攻撃では，過去に例を見ない100Gbps超の攻撃が複数回行われ，最大623Gbpsの史上最悪の規模に達したと言われている[2]。

他にも，SOAP(Simple Object Access Protocol)通信ライブラリのgSOAP(generic XML and SOAP)の脆弱性を悪用したマルウェア“Devil's Ivy”も登場した。これは攻撃者によって遠隔から工場出荷状態に戻されて，ネットワークカメラの乗っ取りや不正な制御が行われる危険性があると報告されている[3]。また，IDとパスワードが初期設定のままのネットワークカメラを勝手にのぞき見できるサイト“Insecam”が現在も公開されている。

また，“BlueBorne”と呼ばれるBluetooth(注1)の実装上の脆弱性が複数見つかっている[4]。この脆弱性が悪用されると，攻撃者によって遠隔から情報が窃取されたり，機器が操作されたりする等の問題につながるおそれがある。大々的な攻撃の報告はないものの，IoT機器ではBluetoothを利用している場合が多く，多くの機器が影響を受けると推測されている。

このように，近年では，IoT機器が攻撃対象となるサイバー攻撃の事例が増加している。

(注1) Bluetoothは，Bluetooth SIGの登録商標である。

3. IoTセキュリティ対応の必要性

3.1 IoT特有のセキュリティリスク

IoTシステムでは，従来ネットワークに接続することすら想像しなかったモノが多数つながり，相互に通信可能となる。このため，IT(Information Technology)システムでは発生しなかったIoT特有のセキュリティリスクが生じるおそれがある。先に述べたようにマルウェアMiraiによる攻撃はかつてない規模のDDoS攻撃に発展した。また，IoTのシステム設計・実装・試験・運用保守等に関わる多種多様な人々，IoTで取り扱われる多種多様な情報資産が存在している。このような多種多様な状況による未知のものも含めた注意すべき脅威・脆弱性は個々のIoTシステムによって全く異なってくる。

IoT推進コンソーシアムのIoTセキュリティガイドラインでは，**表1**に示すようにIoT機器特有のセキュリティに関わる性質を六つあげている[5]。

また，インターネットに接続しないシステムでも，様々

表1．IoT機器特有のセキュリティに関わる性質

No	IoT機器特有のセキュリティに関わる性質
1	脅威の影響範囲・影響度合いが大きいこと
2	IoT機器のライフサイクルが長いこと
3	IoT機器に対する監視が行き届きにくいこと
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であること
5	IoT機器の機能・性能が限られていること
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こと

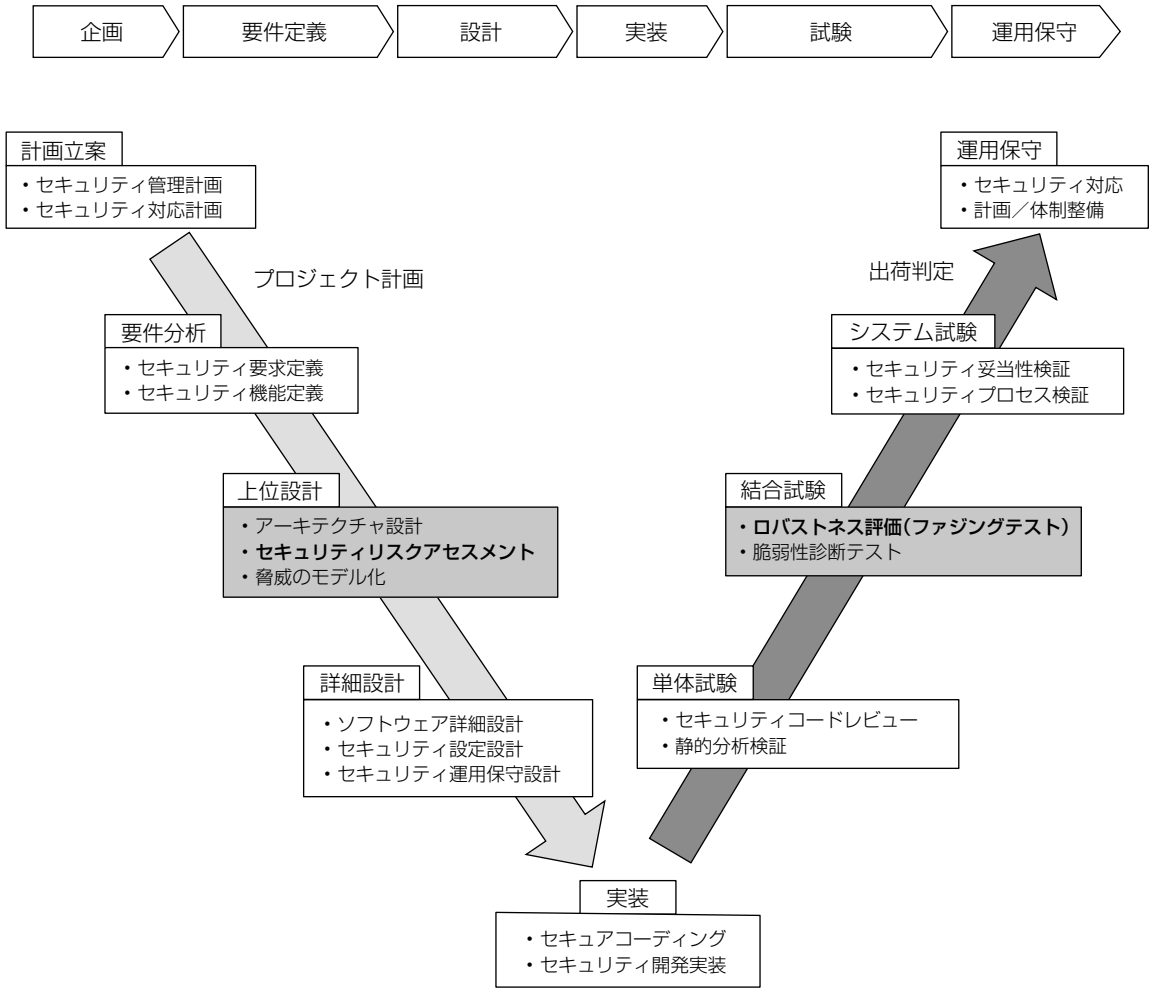


図1．システム開発ライフサイクルでのセキュリティ対応プロセス

なモノを利用する場合や，USB(Universal Serial Bus)メモリやスマートフォン等の持込み機器の接続によるマルウェア感染に伴う攻撃も考えられる。さらに，関連する技術の革新によって，巧妙化・高度化している脅威に対応するためには，情報セキュリティリスク対応が必要である。

3.2　IoT機器の性質を考慮したセキュリティ対策への取組み

表1のようなIoTの性質から，従来の機器やソフトウェアのバージョン管理，セキュリティ設計チェックだけでは予測できない新たな脅威・脆弱性の存在が危惧されることとなり，これらリスクへの対応について具体的な対応策を用意していくことが必須となる。

新たな脅威や脆弱性を低減するためには，EDSA(Embedded Device Security Assurance)認証[6]のSDLA(Security Development Lifecycle Assurance)やIEC62443-4-1[7]で定義されているように製品開発のライフサイクル全体にわたるセキュリティ対策への取組みが重要である。

図1に示すようにシステム開発のライフサイクルには，設計段階でのセキュリティリスクアセスメント，試験段階でのロバストネス評価などが含まれ，それらについての手順書などを資料化して，システム開発ライフサイクルのセキュリティ対応プロセスの強化を推進している。

4.　セキュリティリスク対応のプロセス

4.1　セキュリティリスク対応の作業ステップ

セキュリティリスク対応には，**表2**に示すように“ステップ1　分析対象の定義”から“ステップ7　実施した対策の効果確認”まで七つの作業ステップがある。

セキュリティリスクアセスメントは，このうちの“ステップ1　分析対象の定義”から“ステップ5　リスクの判断”までの作業である。

セキュリティリスクアセスメントを行った後，“ステップ6　対策の検討と適用”を行い，“ステップ7　実施した対策の効果を確認”で実施するのがロバストネス(堅牢(ろう)性)評価である。

4.2　セキュリティリスクアセスメント

セキュリティリスクアセスメントは対象とするシステムに対し，**表2**に示した準備・分析段階の作業ステップ1～5を実施する。その後に対策段階の作業ステップ6を実施する。

(1)　分析対象の定義(ステップ1)

対象とするシステムから分析の対象とする構成要素と設置場所を抽出して定義する(**表3**)。

表2．セキュリティリスク対応の作業ステップ

作業ステップ		
準備	1	分析対象の定義
	2	登場人物(役割)の明確化
	3	情報資産の洗い出し
分析	4	脅威の明確化
	5	リスクの判断
対策	6	対策の検討と適用
	7	実施した対策の効果を確認

表3．ステップ1 分析対象の定義例

構成要素	設置場所
モバイル端末	構外
ルータ	サーバルーム
管理端末	事務所

表4．ステップ2 登場人物の明確化例

登場人物	悪意の有無
第三者(攻撃者)	悪意あり
管理者	悪意なし
ユーザー	悪意なし

表5．ステップ3 情報資産の洗い出し例

情報資産	特性	資産価値
ウェアラブル・デバイス認証情報	機密性	3
	完全性	2
	可用性	2
位置データ	機密性	2
	完全性	2
	可用性	2
音声データ	機密性	2
	完全性	2
	可用性	1

(2) 登場人物の明確化(ステップ2)

定義した構成要素に関わる人物と人物の悪意の有無を定義する(**表4**)。

(3) 情報資産の洗い出し(ステップ3)

構成要素に含まれる情報資産の特性(機密性，完全性，可用性)を資産価値(例えば3段階で評価)とともに定義する(**表5**)。

(4) 脅威の明確化(ステップ4)

構成要素にある情報資産に対して，システムの前提条件を考慮して発生する可能性のある脅威の種類と内容，その発生可能性(例えば3段階で評価)を定義する(**表6**)。

(5) リスクの判断(ステップ5)

情報資産価値と脅威の発生可能性からリスク値(リスクの度合い)を求める。リスク値は，“資産価値×発生可能性”によって計算できる。**表7**は，ステップ5までのセキュリティリスクアセスメントを行い，リスク値を算出した例の一部を示す。

(6) 対策の検討と適用(ステップ6)

セキュリティポリシー，構成要素の機能，対策にかかるコスト，対策に要する期間などの各要素を勘案して実施すべき対策を判断する。判断した結果，製品やシステムにセキュリティ対策を適用する。

4.3 ロバストネス評価

ロバストネス評価は**表2**に示した対策の作業ステップ7を実施する。

ロバストネス評価ツールによって対策の効果の度合い，他に脆弱性がないことを確認する。例えば，入力処理の実

表6．ステップ4 脅威の明確化の例

分析対象の定義		登場人物の明確化		情報資産の洗い出し			脅威の明確化		
構成要素	場所	登場人物	悪意の有無	情報資産	特性	資産価値	脅威		発生可能性
							種類	内容	
モバイル端末	構外	第三者(攻撃者)	悪意あり	ウェアラブル・デバイス認証情報	機密性	3	意図的	認証機能の不備	3
モバイル端末	構外	第三者(攻撃者)	悪意あり	位置データ	完全性	2	意図的	想定外の接続	3
モバイル端末	構外	ユーザー	悪意なし	音声データ	可用性	1	非意図的	不正操作	1

表7．ステップ5 リスク値の算出例

分析対象の定義		登場人物の明確化		情報資産の洗い出し			脅威の明確化			リスクの判断
構成要素	場所	登場人物	悪意の有無	情報資産	特性	資産価値	脅威		発生可能性	リスク値
							種類	内容		
モバイル端末	構外	第三者(攻撃者)	悪意あり	ウェアラブル・デバイス認証情報	機密性	3	意図的	認証機能の不備	3	9
モバイル端末	構外	第三者(攻撃者)	悪意あり	位置データ	完全性	2	意図的	想定外の接続	3	6
モバイル端末	構外	ユーザー	悪意なし	音声データ	可用性	1	非意図的	不正操作	1	1

表8．ファズのパターン例

ファズのパターン	ファズの例	説明
正常値	GET / HTTP/1.0	
リクエストURIに極端に長い文字列を設定	GET AAAAAAAAAAAAAAAAAA…	スタック・ヒープオーバーフローにつながる可能性がある
リクエストURIに書式文字列を設定	GET %s%s%s%s HTTP/1.0	書式文字列の問題につながる可能性がある
HTTPバージョンに数値の上限を超える値を設定	GET / HTTP/65537	整数オーバーフローにつながる可能性がある

URI：Uniform Resource Identifier，HTTP：HyperText Transfer Protocol

装に関する脆弱性については通信データとして問題を引き起こしそうなテストデータ(ファズ)を送り込むファジングテストツールを使用して評価を行う。他には脆弱性診断テスト，**図1**のシステム試験プロセスで評価，検証を行う。**表8**にファジングテストのファズのパターン例を示す[8]。

5. 課題と今後の対応

5.1 課　題

セキュリティリスクアセスメントを進める上での課題が二つある。一つ目は，セキュリティリスクアセスメントの所要時間である。分析対象の条件等にもよるが，現状の手順で進めた場合，3か月程度を要する場合がある。二つ目は，セキュリティリスクアセスメントによるリスク抽出・判断結果のばらつきである。分析作業者の習熟度によって，抽出漏れや影響評価，及び所要時間にばらつきが生じる場合がある。

5.2 課題に対する考察

セキュリティリスクアセスメントの所要時間が長くなる原因は，リスク分析者が対象システムを理解・把握して情報資産の洗い出しなどの準備作業に時間を要すること，発生する脅威の明確化の作業が多岐・多数にわたることにある。リスク抽出・判断結果にばらつきが生じる原因としては，リスク分析者のセキュリティリスクアセスメントの経験，習熟度によって脅威による影響の及ぶ範囲についての考え方に個人差が出ることが挙げられる。

前者に対しては，情報資産の洗い出しから脅威の明確化が速やかに行えるように作業効率を向上させる必要がある。後者に対しては，リスク分析者の経験，習熟度によらずに脅威の影響を導けるように属人性を排除することが必要と考える。

5.3 今後の対応

先に述べた作業効率向上と属人性排除に向け，今後コンセプトブック(セキュリティリスクアセスメント用ツール，知見・ノウハウ・事例・対策例の社内共有データベース)の充実を図っていく。また並行してシステム設計者に対してもセキュリティリスクアセスメントの教育やセキュリティリスクアセスメント用ツール，ロバストネス評価ツール等の操作・活用教育を更に推し進めていく。

6. むすび

情報セキュリティは社会問題であること，IoTが一般化して市場に浸透するまでに長期間かかることが見込まれることなどから，未知の脅威への新たなセキュリティ対策が必要になることが予測される。

今回は三菱電機の情報技術総合研究所との連携によって技術展開を進めてきたが，今後は三菱電機のグループ会社とも連携し，共創を進めていく。これらによって，高度なセキュリティソリューションの具体化を図り，グループ全体での新たな価値を創出し，社会貢献を目指していく。

参考文献

(1) 国立研究開発法人 情報通信研究機構(NICT) サイバーセキュリティ研究所：NICTER観測レポート2016 (2016)
http://www.nict.go.jp/cyber/report/NICTER_report_2016.pdf
(2) Akamai Technologies. Inc.：MIRAIボットネットが今日の最大規模評価かつ破壊的なZDDOS攻撃を生み出す理由 (2016)
https://www.akamai.com/jp/ja/multimedia/documents/white-paper/akamai-mirai-botnet-and-attacks-against-dns-servers-white-paper.pdf
(3) Senrio Inc.：Devil's Ivy：Flaw in Widely Used Third-party Code Impacts Millions (2017)
http://blog.senr.io/blog/devils-ivy-flaw-in-widely-used-third-party-code-impacts-millions
(4) 独立行政法人情報処理推進機構：Bluetoothの実装における複数の脆弱性について (2017)
https://www.ipa.go.jp/security/ciadr/vul/20170914_blueborne.html
(5) 総務省／経済産業省 IoT推進コンソーシアム：IoTセキュリティガイドラインver 1.0 (2016)
http://www.soumu.go.jp/main_content/000428393.pdf
(6) CSSC認証ラボラトリー：ISASecure® EDSA認証とは (2014)
http://www.cssc-cl.org/jp/about_edsa/index.html
(7) IEC：Security for industrial automation and control systems-Part 4-1: Secure product development lifecycle requirements, IEC 62443-4-1:2018 (2018)
(8) 独立行政法人 情報処理推進機構：ファジング活用の手引き (2017)
https://www.ipa.go.jp/files/000057652.pdf