製品分野別セキュリティガイドライン

IoT-GW 編　別冊

ー各種リスク評価手法を用いた
守るべき資産への影響度考察ー

Ver. 1.0

CCDS　セキュリティガイドライン WG

ホーム GW SWG

改訂履歴

版数	改訂日	改訂内容
Ver.1.0	2017/05/29	新規作成

目次

1 はじめに

リスク評価手法は CVSS(Common Vulnerability Scoring System)v3.0[1]や ETSI(European Telecommunications Standards System) TS 102 165-1[2]等のように、各団体から様々な手法が提案されている。どのリスク評価手法を使用するかは、使用する組織のセキュリティポリシーによるが、本書は各種リスク評価手法を用いて複数のユースケースを想定し、ケーススタディを実施し、導き出された結果について考察を行ったものである。

各組織においてリスク評価を行う場合の一助となれば幸いである。

2 リスク評価手法とは

2.1 リスク評価の目的

リスク評価を行う目的は、発生する/発生したリスクが守るべき資産にどの程度の影響を及ぼすかを検討することであり、定量的なリスク評価を行った場合、結果は数値や High や Low のように指標で表現され、その評価の方法はリスク評価手法により様々な形がある。

2.2 代表的なリスク評価手法

代表的なリスク評価手法を表 2-1 に示す。GMITS(ISO/IEC TR 13335-3)[3]ではリスク評価手法を 4 つのアプローチに分類しており、それぞれ、ベースラインアプローチ、非形式的アプローチ、詳細リスク評価アプローチ、組合せアプローチとしている。今回紹介するリスク評価手法は、詳細リスク評価に大別され、守るべき資産を明確化し、資産価値、脅威、頻度などをファクタとしてリスクを評価する。

表 2-1 代表的なリスク評価手法

項番	リスク評価手法	概要
1	NIST SP800-30[4]	米国連邦政府の情報システムのリスクアセスメント実施方法を提供する為に、NIST SP800-39 を詳説したドキュメント。
2	GMITS(ISO/IEC TR 13335-3)	IT セキュリティマネジメントのガイドライン。 現在存在する各種リスクマネジメント手法のベースになっている規格。
3	ETSI TS102 165-1	European Telecommunications Standards Institute によって策定された詳細リスク評価アプローチ手法。

項番	リスク評価手法	概要
4	情報セキュリティマネジメントシステム(ISMS)[5]	情報資産のセキュリティを管理する為の枠組みを策定し、実施する規格。
5	OCTAVE Allegro[6]	カーネギーメロン大学(米国)により 1999 年に発行された OCTAVE をベースに作られた脆弱性評価フレームワーク。
6	The OWASP Rating Methodology[7]	OWASP(Open Web Application Security Project)によって開発された手法。
7	FAIR[8]	RISK Management Insight LLC によって開発されたリスク評価方法。

2.3 各種リスク評価手法詳細

以降に各種リスク評価手法の詳細について解説するが、本書ではリスクに対する影響度を求めるうえで考慮するファクタや計算方法にフォーカスすることとする。

2.3.1 NIST SP800-30

NIST SP800-30 は米国連邦政府の情報システムのリスクアセスメント実施方法を提供する為に、NIST SP800-39 を詳説したドキュメントであり、1 章～3 章と Appendix A～L で構成される。詳細なリスク評価手法は 3 章に以下に示すステップ 1～ステップ 4 が記載されている。

- ステップ 1:リスクアセスメントの準備(Prepare for Risk Assessment)
- ステップ 2:リスクアセスメントの実施(Conduct Risk Assessment)
- ステップ 3:リスクアセスメントの結果連絡と共有
  (Communicate and Share Risk Assessment Results)
- ステップ 4:リスクアセスメントの保持(Maintain Risk Assessment)

リスク評価における考慮すべきファクタは、ステップ 2 のリスクアセスメントの実施に以下の 5 つのファクタを認識することが実施すべきタスクとして挙げられている。

✓ リスクファクタ(5 ファクタ)

① :THREAT SOURCE(脅威源)

② :THREAT EVENT(脅威事象)

③ :VULNERABILITIES AND PREDISPOSING CONDITIONS(脆弱性と発生条件)

④ :LIKELIHOOD OF OCCURRENCE(発生の可能性)

⑤ :IMPACT(影響度)

✓ リスク計算式

リスクファクタは上記の通り 5 つ提示されているが、各リスクファクタを結合する計算式(計算アルゴリズム)は各組織において定義するリスクモデルに含むとしている。

(Organization-specific risk models include algorithms (e.g., formulas, tables, rules) for combining risk factors.)

よって、リスク値を求めるにはリスク計算の為の計算アルゴリズムを含んだ、リスクモデルを独自に定義する必要がある。

2.3.2 ISO/IEC TR 13335-3(GMITS)

ISO/IEC TR 13335 は IT セキュリティマネジメントのガイドラインであり、現在存在する各種リスクマネジメント手法のベースとなっている規格である。その中でも ISO/IEC TR 13335-3 はタイトルが Information technology - Guidelines for the management of IT Security-となっており、そのタイトルを略して GMITS とも呼ばれる。ISO13335-3 は 1 章～12 章と Annex A～E で構成され、詳細リスク評価手法は 9 章に記載さており、以下に示す 3 つのファクタを用いる。資産価値の評価、脅威の評価、脆弱性の評価を行い、全体としてリスクを評価する。

✓ リスクファクタ(3 ファクタ)

① :Asset(資産価値)

② :Threat(脅威)

③ :Vulnerability(脆弱性)

✓ リスク計算式

各ファクタを結合する計算アルゴリズムはドキュメント内に記載されていない。ただし、Annex E に表を用いた方法が 4 つ例示しているが、使用する手法は NIST SP800-30 同様に使用する組織(ユースケース)にマッチした、手法を使用するべきと記載されている。

2.3.3　ETSI TS102 165-1

ETSI TS102 165-1 は European Telecommunications Standards Institute によって策定された詳細リスク評価アプローチ手法 TVRA(Threat Vulnerability and Risk Analysis)であり、1 章～6 章と Appendix A～J で構成される。詳細な手法は 6 章にステップ 1～ステップ 10 まで記載があり、リスク評価対象の明確化から、リスクに対する対策までが記載されている。

- ステップ 1:リスク評価のゴール、目的、スコープの明確化
- ステップ 2:高度なセキュリティ要件が必要となった対象と、解決すべき問題の明確化
- ステップ 3:ステップ 2 から導き出される対象の機能的なセキュリティ要件の明確化
- ステップ 4:ステップ 1, 2, 3 で明確した資産のリスト化
- ステップ 5:システムの脆弱性、脆弱性を悪用する脅威、望まないインシデントの明確化と分類
- ステップ 6:脅威の発生頻度と影響度の定量化
- ステップ 7:リスクの確立
- ステップ 8:リスクを低減する為に必要な代替サービスや機能など対策フレームワークの明確化
- ステップ 9:代替案の中で最適なサービスや機能を明確にする為の費用対効果評価
- ステップ 10:ステップ 9 のセキュリティサービスと機能に関する詳細な要件の仕様化

リスク評価における考慮すべきファクタは、ステップ 5、6 に合計 7 のファクタが記載されている。

✓　リスクファクタ(7 ファクタ)

①Likelihood(頻度)

①-1　:Time(攻撃に要する時間)

①-2　:Expertise(攻撃者のスキル)

①-3　:Knowledge(システム知識)

①-4　:Opportunity(攻撃の機会)

①-5　:Equipment(設備)

②Impact(影響度)

②-1:Asset Impact(資産への)

②-2：Attack Intensity(攻撃の強度)

✓ リスク計算式

リスク計算式は

Risk = Likelihood*Impact

と表現され、Likelihood と Impact は以下の手順①～⑥により求めることができる。

◆ 手順①：Likelihood 詳細なファクタ「Time」、「Expertise」、「Knowledge」、「Opportunity」、「Equipment」の攻撃される可能性を定量化

表 2-2 に示す Attack Potential Value という評価指標で定量化を行う。

表 2-2 Attack Potential

Factor	Range	Value
Time (1 point per week)	≤1 day	0
	≤ 1 week	1
	≤ 1 month	4
	≤ 3 months	13
	≤ 6 months	26
	> 6 months	See note 1
Expertise	Layman	0
	Proficient	2
	Expert	5
Knowledge	Public	0
	Restricted	1
	Sensitive	4
	Critical	10
Opportunity	Unnecessary / unlimited access	0
	Easy	1
	Moderate	4
	Difficult	12
	None	See note 2
Equipment	Standard	0
	Specialized	3
	Bespoke	7
NOTE 1: Attack potential is beyond high. NOTE 2: Attack path is not exploitable.		

◆ 手順②：定量化した「Time」、「Expertise」、「Knowledge」、「Opportunity」、「Equipment」の Attack Potential Value の格付

手順①で定量化した「Time」、「Expertise」、「Knowledge」、「Opportunity」、「Equipment」の各 Attack Potential Value を合計し、表 2-3 に示す Vulnerability rating による、対応表によってよって、脆弱性の格付を行う。

表 2-3 Vulnerability Rating

Attack potential values	Resistant to attacker with attack potential of:
0 to 2	No rating
3 to 6	Basic
7 to 14	Moderate
15 to 26	High
> 26	Beyond high

◆ 手順③:「Time」、「Expertise」、「Knowledge」、「Opportunity」、「Equipment」を統合した Likelihood の指標化

手順②で行った脆弱性の格付指標を表 2-4 に示す Mapping of vulnerability rating to likelihood of attack に示す対応により、Vulnerability rating から Likelihood を指標化する。

表 2-4 Mapping of vulnerability rating to likelihood of attack

Vulnerability rating	Likelihood
Beyond high	Unlikely
High	
Moderate	Possible
Basic	Likely
No rating	
NOTE: Motivation is not considered explicitly in the vulnerability rating.	

◆ 手順④:Likelihood の定量化

Likelihood は表 2-5 の Occurrence likelihood により、手順③で求めた指標から定量化を行う。(Occurrence Likelihood Value を求める)

表 2-5 Occurrence likelihood

Value	Likelihood of occurrence	Explanation
1	Unlikely	According to up-to-date knowledge, a possible attacker needs to solve strong technical difficulties to state the threat or the motivation for an attacker is very low.
2	Possible	The technical requirements necessary to state this threat are not high and could be solved without significant effort; furthermore, there is a reasonable motivation for an attacker to perform the threat.
3	Likely	There are no sufficient mechanisms installed to counteract this threat and the motivation for an attacker is quite high.

◆ 手順⑤:「Asset Impact」と「Attack Intensity」から Impact を数値化

表 2-6 の Asset Impact に示す、資産への影響度から資産に対する攻撃の影響度を定量化する。また、表 2-7 の Attack intensity levels から攻撃の強度を定量化する。定量化された Asset Impact 値と Attack intensity 値を元に表 2-8 に示す Result on overall impact of varying attack intensity によりに示す組合せにより、Asset Impact と Attack Intensity から Impact を数値化する。なお表 2-8 で示すように最終的な影響度(Resulting Impact)は Asset Impact と Attack Intensity

の合計値になるが上限は 3 である為、仮に Asset Impact と Attack Intensity を加算した合計が「5」になったとしても、最終的には「3」に値が丸められる。

表 2-6 Asset Impact

Impact	Explanation	Value
Low	The concerned party is not harmed very strongly; the possible damage is low.	1
Medium	The threat addresses the interests of providers/subscribers and cannot be neglected.	2
High	A basis of business is threatened and severe damage might occur in this context.	3

表 2-7 Attack intensity levels

Attack intensity	Value
Single instance of attack	0
Moderate level of multiple instances	1
Heavy level of multiple instances	2

表 2-8 Result on overall Impact of varying attack intensity

Asset Impact	Attack Intensity	Resulting Impact
1	0	1
1	1	2
1	2	3
2	0	2
2	1	3
2	2	3 (note)
3	0	3
3	1	3 (note)
3	2	3 (note)
NOTE: The Asset Impact Is assigned a value in the range of 1 to 3. Consequently, any Resulting Impact value calculated to be greater than 3 is given the value of 3.		

◆ 手順⑥:リスクを求める

最後に手順④で数値化した Occurrence likelihood Value と手順⑤で数値化した Resulting Impact Value を掛け算し、その結果を表 2-9 に示す「Critical」、「Major」、「Minor」という 3 指標でリスクを表現する。

表 2-9 Risk

Value	Risk	Explanation
1, 2	Minor	No essential assets are concerned, or the attack is unlikely. Threats causing minor risks have no primary need for counter measures.
3, 4	Major	Threats on relevant assets are likely to occur although their impact is unlikely to be fatal. Major risks should be handled seriously and should be minimized by the appropriate use of countermeasures.
6, 9	Critical	The primary interests of the providers and/or subscribers are threatened and the effort required from a potential attacker's to implement the threat(s) is not high. Critical risks should be minimized with highest priority.
NOTE: Because risk is calculated as the product of likelihood and impact the values 5, 7 and 8 cannot occur.		

2.3.4 情報セキュリティマネジメントシステム(ISMS)

JIPDEC による解説[9]によると、情報セキュリティマネジメントシステム(ISMS)は、情報資産のセキュリティを管理する為の枠組みを策定し，実施する規格であり、1 章～9 章で構成される。ISMS の確立手順として 4 章のステップ 1～ステップ 10 の実施作業に纏められている。

- ステップ 1:ISMS 適用範囲及び境界を定義する
- ステップ 2:ISMS の基本方針を定義する
- ステップ 3:リスクアセスメントの取組方法を定義する
- ステップ 4:リスクを特定する
- ステップ 5:リスクを評価し評価する
- ステップ 6:リスク対応を行う
- ステップ 7:管理目的と管理策を選択する
- ステップ 8:残留リスクを承認する
- ステップ 9:ISMS の導入・運用を許可する
- ステップ 10:適用宣言書を作成する

リスク評価に関する内容はステップ 4 に考慮すべきファクタ、ステップ 5 にリスク値算出の為の計算式が記載されている。

✓ リスクファクタ(3 ファクタ)

①資産の価値

②脅威

③脆弱性

✓ リスク計算式

リスク値 = 資産の価値 × 脅威 × 脆弱性

計算式は JIPDEC(日本情報経済社会推進協会)による例示であり、規格自体には計算式は示されていない。

2.3.5 OCTAVE Allegro

カーネギーメロン大学(米国)により 1999 年に発行された OCTAVE をベースに作られた脆弱性評価フレームワークであり、1 章～5 章と Annex A～D で構成される。手法の概略が 3 章にステップ 1～ステップ 8 まで記載され、詳細は Annex A に記載されている。

- ステップ 1:リスク評価判断基準の確立
- ステップ 2:情報資産の定義
- ステップ 3:情報資産保管場所の明確化
- ステップ 4:情報資産に影響を与える可能性のある懸念点の明確化
- ステップ 5:脅威のシナリオの明確化
- ステップ 6:リスクの明確化
- ステップ 7:リスク評価
- ステップ 8:リスク軽減アプローチの選択

リスク評価における考慮すべきファクタは、ステップ 7 に以下に示す 5 つのファクタが記載されている。

✓ リスクファクタ(5 ファクタ)

①評判(Reputation)

②Financial(お金)

③Productivity(生産性)

④Safety & Health(安全、健康)

⑤Fines/Legal(懲罰)

✓ リスク計算式

リスク計算式は

Risk = 各 Impact Area*Value の合計

で表現され、「Impact Area」はリスクファクタに①～⑤に優先順位(1～5)の値を付与した値となり、「Value」は Impact Area に対する影響度を High(3)、Moderate(2)、Low(1)の 3 段階に分けた値となる。

表 2-10 表 2-10 に OCTAVE Allegro を用いたリスク評価の一例を示す。

表 2-10 OCTAVE Allegro を用いたリスク評価の一例

Impact Area	Ranking	Impact Value	Score
Reputation	4	Moderate(2)	8
Financial	5	Low(1)	5
Productivity	3	Low(1)	3
Safety and Health	1	Low(1)	1
Fine/Legal	2	High(3)	6
		Total(Risk)	23

2.3.6 The OWASP Rating Methodology

The OWASP Rating Methodology は OWASP(Open Web Application Security Project)によって開発された手法であり、以下のステップ 1～ステップ 6 で構成される。

- ステップ 1:リスクの明確化
- ステップ 2:頻度(Likelihood)を見積もる為のファクタ
- ステップ 3:影響度(Impact)を見積もる為のファクタ
- ステップ 4:リスク影響度の決定
- ステップ 5:対策内容の決定
- ステップ 6:リスク評価方法のカスタマイズ

リスク評価における考慮すべきファクタは、ステップ 2、3 に以下に示す合計 16 のファクタが記載されている。

✓　リスクファクタ(16 ファクタ)

・発生頻度を求める為のファクタ

①Threat Agent

②Vulnerability

・影響度を求める為のファクタ

③Technical Impact

④Business Impact

これら①～④のファクタは表 2-11 に示す詳細なファクタに細分化されリスク評価を行う場合には 16 のファクタを考慮することとなる。

表 2-11 発生頻度、影響度を求めるファクタの詳細

①Threat Agent	③Technical Impact
①-1：Skill Level	③-1：Loss of confidentiality
①-2：Motive	③-2：Loss of integrity
①-3：Opportunity	③-3：Loss of availability
①-4：Size	③-4：Loss of accountability
②Vulnerability	④Business Impact
②-1：Ease of discovery	④-1：Financial damage
②-2：Ease of exploit	④-2：Reputation damage
②-3：Awareness	④-3：Non compliance
②-4：Intrusion detection	④-4：Privacy violation

✓　リスク計算式

リスク計算式は

Risk Severity=(①+②)/2)x(③+④)/2)

で表現され、一般的なリスク計算式 Risk=Likelihood×Impact を踏襲している。

Likelihood、Impact の求め方から、最終的なリスクの求め方の具体例を表 2-12～表 2-14 に示す。

表 2-12 OWASP を用いたリスク評価の一例

Likelihood								
Threat agent factors					Vulnerability factors			
Skill level	Motive	Opportunity	Size		Ease of discovery	Ease of exploit	Awareness	Intrusion detection
4 - Advanced computer user	1 - Low or no reward	4 - Special access or resources required	5 - Partners		3 - Difficult	3 - Difficult	4 - Hidden	3 - Logged and reviewed
Overall likelihood: 3.375 MEDIUM								
Technical Impact					Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of accountability		Financial damage	Reputation damage	Non-compliance	Privacy violation
2 - Minimal non-sensitive data disclosed	0 -	0 -	9 - Completely anonymous		1 - Less than the cost to fix the vulnerability	1 - Minimal damage	0 -	5 - Hundreds of people
Overall technical impact: 2.750 LOW					Overall business impact: 1.750 LOW			
Overall impact: 2.250 LOW								

表 2-13 Likelihood と Impact 度合いの変換表

Likelihood and Impact Levels	
0 to < 3	Low
3 to < 6	Medium
6 to < 9	High

表 2-14 Likelihood と Impact レベルから求めるリスクマッピング表

Overall Risk Severity = Likelihood x Impact				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	NOTE	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

2.3.7　FAIR

FAIR(Factor Analysis for Information Risk)は合計 9 の章と、Appendix A～C で構成され Measuring Risk(リスクの測定)章に、以下に示すリスク評価で考慮すべきリスクファクタの記載がある。

✓　リスクファクタ(6 ファクタ)

①Loss Event Frequency(LEF):損失発生頻度(TEF、Vuln)

①-1:Threat Event Frequency(TEF):発生頻度

①-2:Threat Capability(Tcap):脅威難易度

①-3:Control Strength(CS):保護強度

①-4:Vulnerability(Vuln):脆弱性(Tcap、CS)

②Probable Loss Magnitude(PLM):金銭的な影響度

上記に示すリスクファクタのうち、Vuln と LEF は他のファクタの組合せにより求める。Vuln は表 2-15 に示すように Tcap と CS のマッピング表から求める。

表 2-15 Vuln を求める為の Tcap と CS のマッピング表

Vulnerability(Vuln)						
Threat Capability (Tcap)	VH	VH	VH	VH	H	M
	H	VH	VH	H	M	L
	M	VH	H	M	L	VL
	L	H	M	L	VL	VL
	VL	M	L	VL	VL	VL
		VL	L	M	H	VH
Control Strength(CS)						

また、LEF は表 2-16 に示すように TEF と Vuln の組合せから求める。

表 2-16 LEF を求める為の TEF と Vuln のマッピング表

Loss Event Frequency(LEF)						
Threat Event Frequency (TEF)	VH	M	H	VH	VH	VH
	H	L	M	H	H	H
	M	VL	L	M	M	M
	L	VL	VL	L	L	L
	VL	VL	VL	VL	VL	VL
		VL	L	M	H	VH
Vulnerability(Vuln)						

最終的にリスクは

表 2-17 に示す、PLM と LEF の組合せからリスクは求められ、Critical(C)、High(H)、Medium(M)、Low(L)の 4 種類の指標で表現される。

表 2-17 リスクを求める為の PLM と LEF のマッピング表

RISK						
Probable Loss Magnitude (PLM)	Severe	H	H	C	C	C
	High	M	H	H	C	C
	Significant	M	M	H	H	C
	Moderate	L	M	M	H	H
	Low	L	L	M	M	M
	Very Low	L	L	M	M	M
		VL	L	M	H	VH
Loss Event Frequency(LEF)						

3 ケーススタディ

3.1 ユースケースの定義

ケーススタディを実施する前提条件を定義する。ケーススタディを行うユースケースは本編に記載されている以下の 4 ユースケースとする。

■ユースケース①：ホームゲートウェイ

機器：IoT-GW(HGW)

有線 WAN/LAN 接続：PC(ネットサーフィン、ネットバンキング、ネット株取引)

無線 LAN 接続：PC、スマホ、ポータルゲーム

守るべき資産：金融資産、評判

■ユースケース②：スマートメンテナンス

機器：IoT-GW

有線 WAN/LAN 接続：センサ、アクチュエータ

無線 LAN 接続：センサ、アクチュエータ

守るべき資産：人命(アクチュエータの暴走)、評判

■ユースケース③：サプライチェーン管理及び生産ライン最適化

機器：IoT-GW

有線 WAN/LAN 接続：センサ

無線 LAN 接続：センサ

守るべき資産：生産設備、評判

■ユースケース④：映像監視

機器：IoT-GW

有線 WAN/LAN 接続：Web カメラ

無線 LAN 接続：Web カメラ

守るべき資産：映像情報(プライバシ) 、評判

3.2　4ユースケースにおける脆弱性、リスクの定義

3.2.1　脆弱性の定義

ここでは 4 ユースケースにおける共通の脆弱性を定義する。今回ケーススタディを行ううえで、前提とした脆弱性は以下の 3 つ。図 3-1 は脆弱性のイメージ図。

■脆弱性

①WAN(インターネット)側からホームゲートウェイ管理画面へアクセス可能。

②HGW 管理画面の初期 ID/PW が平易。

③HGW 管理画面上で設定されている ISP 提供情報が容易に読み取り可能な状態(平文)で保存されている。

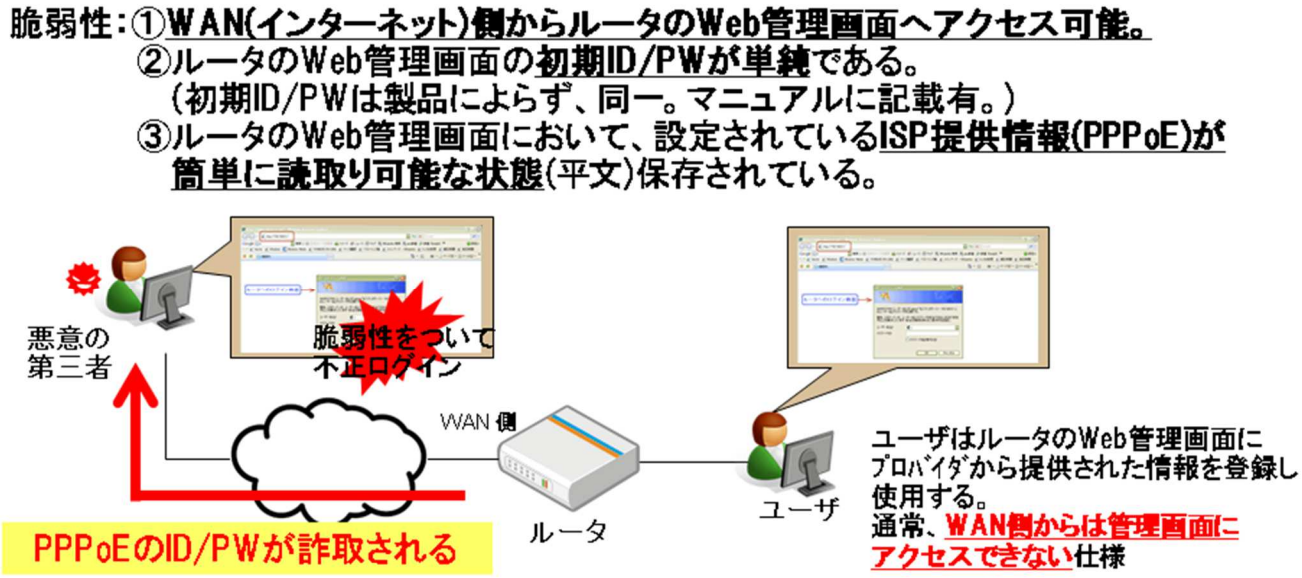

図 3-1 ケーススタディを行ううえで前提とした脆弱性

3.2.2　懸念されるリスク

3.2.1 で定義した脆弱性から引き起こされるであろうリスクを定義する。今回ケーススタディを行ううえで、前提としたリスクは以下の 2 つ。

■懸念されるリスク

・成りすまし、乗っ取りによる身元を隠蔽した各種サイバー攻撃への加担

・通信の盗聴による情報の詐取

3.3　各種リスク評価手法を用いたケーススタディ結果

通常リスク評価は一つの脆弱性に対してどれだけ影響度があるかを求めるが、今回のケーススタディにおいては複数の脆弱性を”OR”条件で考慮し影響度を求めることとし、複数ある脆弱性の一部を取り去ることで結果がどのように変化するかを確認した。また、使用するリスク評価方法は、定量的なリスク評価を行うことができ、計算式が規定または例示されている ETSI TS102 165-1、情報セキュリティマネジメントシステム(ISMS)、OCTAVE Allegro、The OWASP Rating Methodology、FAIR の 5 種類を使用することとした。

3.3.1　ETSI TS102 165-1 を用いたリスク評価

リスク評価手法として ETSI TS102 165-1 を使用しケーススタディを行った場合の結果を図 3-2 ～図 3-5 に示す。

ユースケース①:ホームゲートウェイ

Risk	Asset Impact	Attack Intensity	Impact Value	Knowledge Factor	Time Factor	Expertise Factor	Opportunity Factor	Equipment Factor	Likelihood Value	Risk Index
サイバー攻撃への加担＆盗聴による金銭的な被害	3	2	3	0	1	0	1	0	3	Critical

Risk	Asset Impact	Attack Intensity	Impact Value	Knowledge Factor	Time Factor	Expertise Factor	Opportunity Factor	Equipment Factor	Likelihood Value	Risk Index
サイバー攻撃への加担＆盗聴による金銭的な被害	2	2	3	0	1	0	1	0	3	Critical

図 3-2 ETSI TS102 165-1 を用いたケーススタディ(ホームゲートウェイ)

ユースケース②:スマートメンテナンス

Risk	Asset Impact	Attack Intensity	Impact Value	Knowledge Factor	Time Factor	Expertise Factor	Opportunity Factor	Equipment Factor	Likelihood Value	Risk Index
サイバー攻撃への加担＆人命への被害	3	2	3	0	1	0	1	0	3	Critical

Risk	Asset Impact	Attack Intensity	Impact Value	Knowledge Factor	Time Factor	Expertise Factor	Opportunity Factor	Equipment Factor	Likelihood Value	Risk Index
サイバー攻撃への加担	2	2	3	0	1	0	1	0	3	Critical

図 3-3 ETSI TS102 165-1 を用いたケーススタディ(スマートメンテナンス)

ユースケース③:サプライチェーン管理及び生産ライン最適化

Risk	Asset Impact	Attack Intensity	Impact Value	Knowledge Factor	Time Factor	Expertise Factor	Opportunity Factor	Equipment Factor	Likelihood Value	Risk Index
サイバー攻撃への加担&生産設備の停止	3	2	3	0	1	0	1	0	3	Critical

Risk	Asset Impact	Attack Intensity	Impact Value	Knowledge Factor	Time Factor	Expertise Factor	Opportunity Factor	Equipment Factor	Likelihood Value	Risk Index
サイバー攻撃への加担	3	2	3	0	1	0	1	0	3	Critical

図 3-4 ETSI TS102 165-1 を用いたケーススタディ(サプライチェーン管理)

ユースケース④:映像監視

Risk	Asset Impact	Attack Intensity	Impact Value	Knowledge Factor	Time Factor	Expertise Factor	Opportunity Factor	Equipment Factor	Likelihood Value	Risk Index
サイバー攻撃への加担&プライバシの侵害	3	2	3	0	1	0	1	0	3	Critical

Risk	Asset Impact	Attack Intensity	Impact Value	Knowledge Factor	Time Factor	Expertise Factor	Opportunity Factor	Equipment Factor	Likelihood Value	Risk Index
サイバー攻撃への加担	3	2	3	0	1	0	1	0	3	Critical

図 3-5 ETSI TS102 165-1 を用いたケーススタディ(映像監視)

リスク評価手法として ETSI TS102 165-1 を使用し、4 つのユースケースにおいてケーススタディを行った結果のまとめを表 3-1 に示す。

表 3-1 ETSI TS102 165-1 によるケーススタディ結果まとめ

HGW (守るべき資産:金融資産)		スマートメンテナンス (守るべき資産:人命)		ライン最適化 (守るべき資産:生産設備)		映像監視 (守るべき資産:映像情報)	
対策前	対策後	対策前	対策後	対策前	対策後	対策前	対策後
Critical	Critical	Critical	Critical	Critical	Critical	Critical	Critical

3.3.2　情報セキュリティマネジメントシステム(ISMS)を用いたリスク評価

リスク評価手法として情報セキュリティマネジメントシステム(ISMS)を使用しケーススタディを行った場合の結果を以下に図 3-6～図 3-9 に示す。

ユースケース①:ホームゲートウェイ

Risk	資産価値	脅威	脆弱性	リスク値
サイバー攻撃への加担& 盗聴による金銭的な被害	機密性:3 完全性:2 可用性:2	3	3	27

Risk	資産価値	脅威	脆弱性	リスク値
サイバー攻撃への加担	機密性:3 完全性:2 可用性:1	2	3	18

図 3-6 ISMS を用いたケーススタディ(ホームゲートウェイ)

ユースケース②:スマートメンテナンス

Risk	資産価値	脅威	脆弱性	リスク値
サイバー攻撃への加担& 人命への被害	機密性:3 完全性:2 可用性:2	3	3	27

Risk	資産価値	脅威	脆弱性	リスク値
サイバー攻撃への加担	機密性:3 完全性:2 可用性:2	2	3	18

図 3-7 ISMS を用いたケーススタディ(スマートメンテナンス)

ユースケース③:サプライチェーン管理及び生産ライン最適化

Risk	資産価値	脅威	脆弱性	リスク値
サイバー攻撃への加担& 生産設備の停止	機密性:3 完全性:2 可用性:2	3	3	27

Risk	資産価値	脅威	脆弱性	リスク値
サイバー攻撃への加担	機密性:3 完全性:2 可用性:2	2	3	18

図 3-8 ISMS を用いたケーススタディ(サプライチェーン管理)

ユースケース④:映像監視

Risk	資産価値	脅威	脆弱性	リスク値
サイバー攻撃への加担& プライバシの侵害	機密性:3 完全性:2 可用性:2	2	3	18

Risk	資産価値	脅威	脆弱性	リスク値
サイバー攻撃への加担	機密性:3 完全性:2 可用性:2	2	3	18

図 3-9 ISMS を用いたケーススタディ(映像監視)

リスク評価手法として ISMS を使用し、4 つのユースケースにおいてケーススタディを行った結果のまとめを表 3-2 に示す。

表 3-2 ISMS によるケーススタディ結果まとめ

HGW (守るべき資産:金融資産)		スマートメンテナンス (守るべき資産:人命)		ライン最適化 (守るべき資産:生産設備)		映像監視 (守るべき資産:映像情報)	
対策前	対策後	対策前	対策後	対策前	対策後	対策前	対策後
27	18	27	18	27	18	18	18

3.3.3　OCTAVE Allegro を用いたリスク評価

リスク評価手法として OCTAVE Allegro を使用しケーススタディを行った場合の結果を図 3-10 ～図 3-13 に示す。

ユースケース①:ホームゲートウェイ

Risk	Factor	Ranking	Impact Value	Score
サイバー攻撃への加担&盗聴による金銭的な被害	Reputation	5	High	15
	Financial	4	High	12
	Productivity	1	Low	1
	Safety & Health	2	Low	2
	Fines/Legal	3	High	9
			Total	39

Risk	Factor	Ranking	Impact Value	Score
サイバー攻撃への加担	Reputation	4	High	12
	Financial	2	Moderate	4
	Productivity	3	Low	3
	Safety & Health	1	Low	1
	Fines/Legal	5	Moderate	10
			Total	30

図 3-10 OCTAVE Allegro を用いたケーススタディ(ホームゲートウェイ)

ユースケース②:スマートメンテナンス

Risk	Factor	Ranking	Impact Value	Score
サイバー攻撃への加担&人命への被害	Reputation	2	High	6
	Financial	1	Moderate	2
	Productivity	3	High	9
	Safety & Health	5	High	15
	Fines/Legal	4	Moderate	8
			Total	40

Risk	Factor	Ranking	Impact Value	Score
サイバー攻撃への加担	Reputation	4	High	12
	Financial	2	Moderate	4
	Productivity	3	Low	3
	Safety & Health	1	Low	1
	Fines/Legal	5	Moderate	10
			Total	30

図 3-11 OCTAVE Allegro を用いたケーススタディ(スマートメンテナンス)

ユースケース③:サプライチェーン管理及び生産ライン最適化

Risk	Factor	Ranking	Impact Value	Score
サイバー攻撃への加担&生産設備の停止	Reputation	3	High	9
	Financial	2	Moderate	4
	Productivity	5	High	15
	Safety & Health	1	Low	1
	Fines/Legal	4	Moderate	8
			Total	37

Risk	Factor	Ranking	Impact Value	Score
サイバー攻撃への加担	Reputation	4	High	12
	Financial	2	Moderate	4
	Productivity	3	Low	3
	Safety & Health	1	Low	1
	Fines/Legal	5	Moderate	10
			Total	30

図 3-12 OCTAVE Allegro を用いたケーススタディ(サプライチェーン管理)

ユースケース④:映像監視

Risk	Factor	Ranking	Impact Value	Score
サイバー攻撃への加担&プライバシの侵害	Reputation	4	High	12
	Financial	2	Low	2
	Productivity	1	Low	1
	Safety & Health	3	Moderate	6
	Fines/Legal	5	High	15
			Total	36

Risk	Factor	Ranking	Impact Value	Score
サイバー攻撃への加担	Reputation	4	High	12
	Financial	3	Low	3
	Productivity	2	Low	2
	Safety & Health	1	Low	1
	Fines/Legal	5	High	15
			Total	33

図 3-13 OCTAVE Allegro を用いたケーススタディ(映像監視)

リスク評価手法として OCTAVE Allegro を使用し、4 つのユースケースにおいてケーススタディを行った結果のまとめを表 3-3 に示す。

表 3-3 OCTAVE Allegro によるケーススタディ結果まとめ

HGW（守るべき資産：金融資産）		スマートメンテナンス（守るべき資産：人命）		ライン最適化（守るべき資産：生産設備）		映像監視（守るべき資産：映像情報）	
対策前	対策後	対策前	対策後	対策前	対策後	対策前	対策後
39	30	40	30	37	30	36	30

3.3.4 The OWASP Rating Methodology

リスク評価手法として The OWASP Rating Methodology を使用しケーススタディを行った場合の結果図 3-14～図 3-17 に示す。

ユースケース①：ホームゲートウェイ

Risk	Threat Agent		Vulnerability		Technical Impact		Business Impact		Risk Severity
サイバー攻撃への加担&盗聴による金銭的な被害	Skill Level	3	Ease of discovery	7	Loss of confidentiality	9	Financial damage	9	High
	Motive	4	Ease of exploit	5	Loss of integrity	3	Reputation damage	9	
	Opportunity	7	Awareness	6	Loss of availability	5	Non compliance	5	
	Size	9	Intrusion detection	3	Loss of accountability	7	Privacy violation	3	

Risk	Threat Agent		Vulnerability		Technical Impact		Business Impact		Risk Severity
サイバー攻撃への加担	Skill Level	3	Ease of discovery	7	Loss of confidentiality	9	Financial damage	3	Medium
	Motive	4	Ease of exploit	5	Loss of integrity	1	Reputation damage	9	
	Opportunity	7	Awareness	6	Loss of availability	1	Non compliance	5	
	Size	9	Intrusion detection	3	Loss of accountability	7	Privacy violation	3	

図 3-14 The OWASP Rating Methodology を用いたケーススタディ(ホームゲートウェイ)

ユースケース②：スマートメンテナンス

Risk	Threat Agent		Vulnerability		Technical Impact		Business Impact		Risk Severity
サイバー攻撃への加担&人命への被害	Skill Level	3	Ease of discovery	7	Loss of confidentiality	9	Financial damage	3	Medium
	Motive	4	Ease of exploit	5	Loss of integrity	3	Reputation damage	9	
	Opportunity	7	Awareness	6	Loss of availability	5	Non compliance	5	
	Size	9	Intrusion detection	3	Loss of accountability	7	Privacy violation	3	

Risk	Threat Agent		Vulnerability		Technical Impact		Business Impact		Risk Severity
サイバー攻撃への加担	Skill Level	3	Ease of discovery	7	Loss of confidentiality	9	Financial damage	3	Medium
	Motive	4	Ease of exploit	5	Loss of integrity	1	Reputation damage	9	
	Opportunity	7	Awareness	6	Loss of availability	1	Non compliance	5	
	Size	9	Intrusion detection	3	Loss of accountability	7	Privacy violation	5	

図 3-15 The OWASP Rating Methodology を用いたケーススタディ(スマートメンテナンス)

ユースケース③：サプライチェーン管理及び生産ライン最適化

Risk	Threat Agent		Vulnerability		Technical Impact		Business Impact		Risk Severity
サイバー攻撃への加担&生産設備の停止	Skill Level	3	Ease of discovery	7	Loss of confidentiality	9	Financial damage	7	High
	Motive	4	Ease of exploit	5	Loss of integrity	3	Reputation damage	9	
	Opportunity	7	Awareness	6	Loss of availability	5	Non compliance	5	
	Size	9	Intrusion detection	3	Loss of accountability	7	Privacy violation	3	

Risk	Threat Agent		Vulnerability		Technical Impact		Business Impact		Risk Severity
サイバー攻撃への加担	Skill Level	3	Ease of discovery	7	Loss of confidentiality	9	Financial damage	3	Medium
	Motive	4	Ease of exploit	5	Loss of integrity	1	Reputation damage	9	
	Opportunity	7	Awareness	6	Loss of availability	1	Non compliance	5	
	Size	9	Intrusion detection	3	Loss of accountability	7	Privacy violation	5	

図 3-16 The OWASP Rating Methodology を用いたケーススタディ(サプライチェーン管理)

ユースケース④:映像監視

Risk	Threat Agent		Vulnerability		Technical Impact		Business Impact		Risk Severity
サイバー攻撃への加担&プライバシの侵害	Skill Level	3	Ease of discovery	7	Loss of confidentiality	9	Financial damage	3	High
	Motive	4	Ease of exploit	5	Loss of integrity	3	Reputation damage	9	
	Opportunity	7	Awareness	6	Loss of availability	5	Non compliance	5	
	Size	9	Intrusion detection	3	Loss of accountability	7	Privacy violation	7	

Risk	Threat Agent		Vulnerability		Technical Impact		Business Impact		Risk Severity
サイバー攻撃への加担	Skill Level	3	Ease of discovery	7	Loss of confidentiality	9	Financial damage	3	Medium
	Motive	4	Ease of exploit	5	Loss of integrity	1	Reputation damage	9	
	Opportunity	7	Awareness	6	Loss of availability	1	Non compliance	5	
	Size	9	Intrusion detection	3	Loss of accountability	7	Privacy violation	5	

図 3-17 The OWASP Rating Methodology を用いたケーススタディ(映像監視)

リスク評価手法として The OWASP Rating Methodology を使用し、4 つのユースケースにおいてケーススタディを行った結果のまとめを表 3-4 に示す。

表 3-4 The OWASP Rating Methodology によるケーススタディ結果まとめ

HGW (守るべき資産:金融資産)		スマートメンテナンス (守るべき資産:人命)		ライン最適化 (守るべき資産:生産設備)		映像監視 (守るべき資産:映像情報)	
対策前	対策後	対策前	対策後	対策前	対策後	対策前	対策後
High	Medium	Medium	Medium	High	Medium	High	Medium

3.3.5 FAIR

リスク評価手法としてFAIRを使用しケーススタディを行った場合の結果図 3-18～図 3-21 に示す。

ユースケース①:ホームゲートウェイ

Risk	Loss Event Frequency Factor	Value	LEF	PLM	Risk
サイバー攻撃への加担& 盗聴による金銭的な被害	Threat Event Frequency	VH	VH	High	Critical
	Threat Capability	M			
	Control Strength	L			
	Vulnerability	H			

Risk	Loss Event Frequency Factor	Value	LEF	PLM	Risk
サイバー攻撃への加担	Threat Event Frequency	VH	VH	Significant	Critical
	Threat Capability	M			
	Control Strength	L			
	Vulnerability	H			

図 3-18 FAIR を用いたケーススタディ(ホームゲートウェイ)

ユースケース②:スマートメンテナンス

Risk	Loss Event Frequency Factor	Value	LEF	PLM	Risk
サイバー攻撃への加担& 人命への被害	Threat Event Frequency	VH	VH	High	Critical
	Threat Capability	M			
	Control Strength	L			
	Vulnerability	H			

Risk	Loss Event Frequency Factor	Value	LEF	PLM	Risk
サイバー攻撃への加担	Threat Event Frequency	VH	VH	Significant	Critical
	Threat Capability	M			
	Control Strength	L			
	Vulnerability	H			

図 3-19 FAIR を用いたケーススタディ(スマートメンテナンス)

ユースケース③:サプライチェーン管理及び生産ライン最適化

Risk	Loss Event Frequency Factor	Value	LEF	PLM	Risk
サイバー攻撃への加担& 生産設備の停止	Threat Event Frequency	VH	VH	High	Critical
	Threat Capability	M			
	Control Strength	L			
	Vulnerability	H			

Risk	Loss Event Frequency Factor	Value	LEF	PLM	Risk
サイバー攻撃への加担	Threat Event Frequency	VH	VH	Significant	Critical
	Threat Capability	M			
	Control Strength	L			
	Vulnerability	H			

図 3-20 FAIR を用いたケーススタディ(サプライチェーン管理)

ユースケース④:映像監視

Risk	Loss Event Frequency Factor	Value	LEF	PLM	Risk
サイバー攻撃への加担& プライバシの侵害	Threat Event Frequency	VH	VH	Significant	Critical
	Threat Capability	M			
	Control Strength	L			
	Vulnerability	H			

Risk	Loss Event Frequency Factor	Value	LEF	PLM	Risk
サイバー攻撃への加担	Threat Event Frequency	VH	VH	Significant	Critical
	Threat Capability	M			
	Control Strength	L			
	Vulnerability	H			

図 3-21 FAIR を用いたケーススタディ(映像監視)

リスク評価手法として FAIR を使用し、4 つのユースケースにおいてケーススタディを行った結果のまとめを表 3-5 に示す。

表 3-5 FAIR によるケーススタディ結果まとめ

HGW（守るべき資産：金融資産）		スマートメンテナンス（守るべき資産：人命）		ライン最適化（守るべき資産：生産設備）		映像監視（守るべき資産：映像情報）	
対策前	対策後	対策前	対策後	対策前	対策後	対策前	対策後
Critical	Critical	Critical	Critical	Critical	Critical	Critical	Critical

4 まとめ

4.1 結果比較及び考察

表 4-1 に 5 つのリスク評価方法を用いたケーススタディの結果を示す。

表 4-1 5 つのリスク評価方法を用いたケーススタディ結果

手法	HGW（守るべき資産：金融資産）		スマートメンテナンス（守るべき資産：人命）		ライン最適化（守るべき資産：生産設備）		映像監視（守るべき資産：映像情報）	
	対策前	対策後	対策前	対策後	対策前	対策後	対策前	対策後
ETSI	Critical	Critical	Critical	Critical	Critical	Critical	Critical	Critical
ISMS	27	18	27	18	27	18	18	18
OCTAVE	39	30	40	30	37	30	36	30
OWASP	High	Medium	Medium	Medium	High	Medium	High	Medium
FAIR	Critical	Critical	Critical	Critical	Critical	Critical	Critical	Critical

表 4-1 に示す通り、使用するリスク評価手法によっては対策前、対策後での影響度に差が出ない結果となった。これは、数値を High、Low のようなレンジで表現していることによるとも考えられるが、それぞれのユースケースにおける守るべき資産や考慮すべき内容が、リスク評価手法の中に考慮すべきファクタとして用意されていない場合もあるということも要因として考えられる。

- ETSI TS 102 165-1：

複数のファクタを用いてリスクに至る攻撃の難易度から Likelihood 算出に重点を置いている。CIA(Confidentiality、Integrity、Availability)などを考慮して Likelihood を算出するかは、リスク評価者の技量次第。最終結果は数値レンジと指標の組合せによる High、Medium、Low 表現の為、レンジ境界付近の同じような数字でも結果に差分が出てしまう。

- 情報セキュリティマネジメントシステム(ISMS)：

リスク値算出の為のファクタが少なく、各ファクタの重み付けの範囲が狭い(1～3)ので、評価者の主観によってスコアにばらつきが出る。また、算出に使用するファクタに含む詳細なファクタは評価者の熟練度によって差が出てしまう為、簡易的に用いることができるが、正確に評価するにはリスク評価に対する知識が必要になる。

- OCTAVE Allegro：

考慮すべきファクタが 5 つあり、その 5 つ毎にインパクトを考慮する。考慮すべきファクタが多い為、リスク評価初心者にとっては使いやすい。影響を受ける領域をランキング付けするという方法は他の手法にはなく、守るべき資産とその領域が合致する場合には正確にリスク評価が可能。ユースケース(守るべき資産)によっては不要と思われるファクタを独自のファクタに置き換えて実施することも有効な手段。(独自のファクタに置き換えることは、手法の中で紹介されているわけではない。)

- The OWASP Rating Methodology：

リスクファクタが多い為、どれかひとつの要素に対するリスクを排除したとしても、排除した結果が反映されにくい。複数の要素のリスク排除が必要。しかしながら、OCTAVE Allegro 同様考慮すべきファクタあらかじめ多く(16 個)用意されており、リスク評価初心者にとって使い。また、守るべき資産に直結するファクタが用意されている為、脆弱性に対する対策前後で差分が見えやすい。また、各ファクタの重み付けの範囲が(0～9)の為、評価者毎の主観に差があったとしても、結果には大きく差は出ない。最終結果は数値レンジを Critical、High、Medium、Low で表現する為、レンジ境界付近の同じような数字でも結果に差分が出てしまう。OCTAVE Allegro 同様ファクタの入替えも有効。

- FAIR：

ETSI 同様複数のファクタを用いて、リスクに至る攻撃の難易度から頻度(Frequency)算出に重点を置いている。インパクトに関するファクタは 1 つ(ETSI は 2 つ)であり、且つインパクト強度を金銭的に換算しなければならない為、様々なインパクトファクタ(人命等)を纏めて金額に換算するのが難しい。考慮すべきインパクトが用意されていないので抜けが生じる可能性あり。

引用/参考文献

[1] CVSS v3.0: Common Vulnerability Scoring System v3.0: Specification Document V1.7.

[2] ETSI TS 102 165-1: “Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Methods and protocols; Part 1: Method and proforma for Threat, Risk, Vulnerability Analysis,” V4.2.3 (2011-03).

[3] ISO/IEC TR 13335-3(GMITS): Information technology – Guidelines for the management of IT Security

[4] NIST SP800-30: Guide for Conducting Risk Assessments

[5] 情報セキュリティマネジメントシステム(ISMS): Information Security Management System

[6] OCTAVE Allegro: Operationally Critical Threat, Asset, and Vulnerability Evaluation

[7] The OWASP Rating Methodology:

https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology

[8] FAIR: Factor Analysis of Information Risk

[9] 財団法人 日本情報処理開発協会による ISMS の解説

https://www.isms.jipdec.or.jp/doc/JIP-ISMS111-21_2.pdf