製品分野別セキュリティガイドライン
IoT-GW編　別冊

–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–

平成29年5月29日

CCDS セキュリティガイドラインWG
ホームGW SWG

IoT-GWガイドライン別冊の目次

1.リスク評価手法

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為である。

２．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	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。
4	情報セキュリティ マネジメントシステム(ISMS)	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	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	OWASP(Open Web Application Security Project)によって開発された手法。
7	FAIR	RISK Management Insight LLCによって開発されたリスク評価方法。

2.各種リスク評価手法詳細-その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)

■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。

2.各種リスク評価手法詳細-その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

2.各種リスク評価手法詳細-その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

2.各種リスク評価手法詳細-その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

2.各種リスク評価手法詳細-その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。

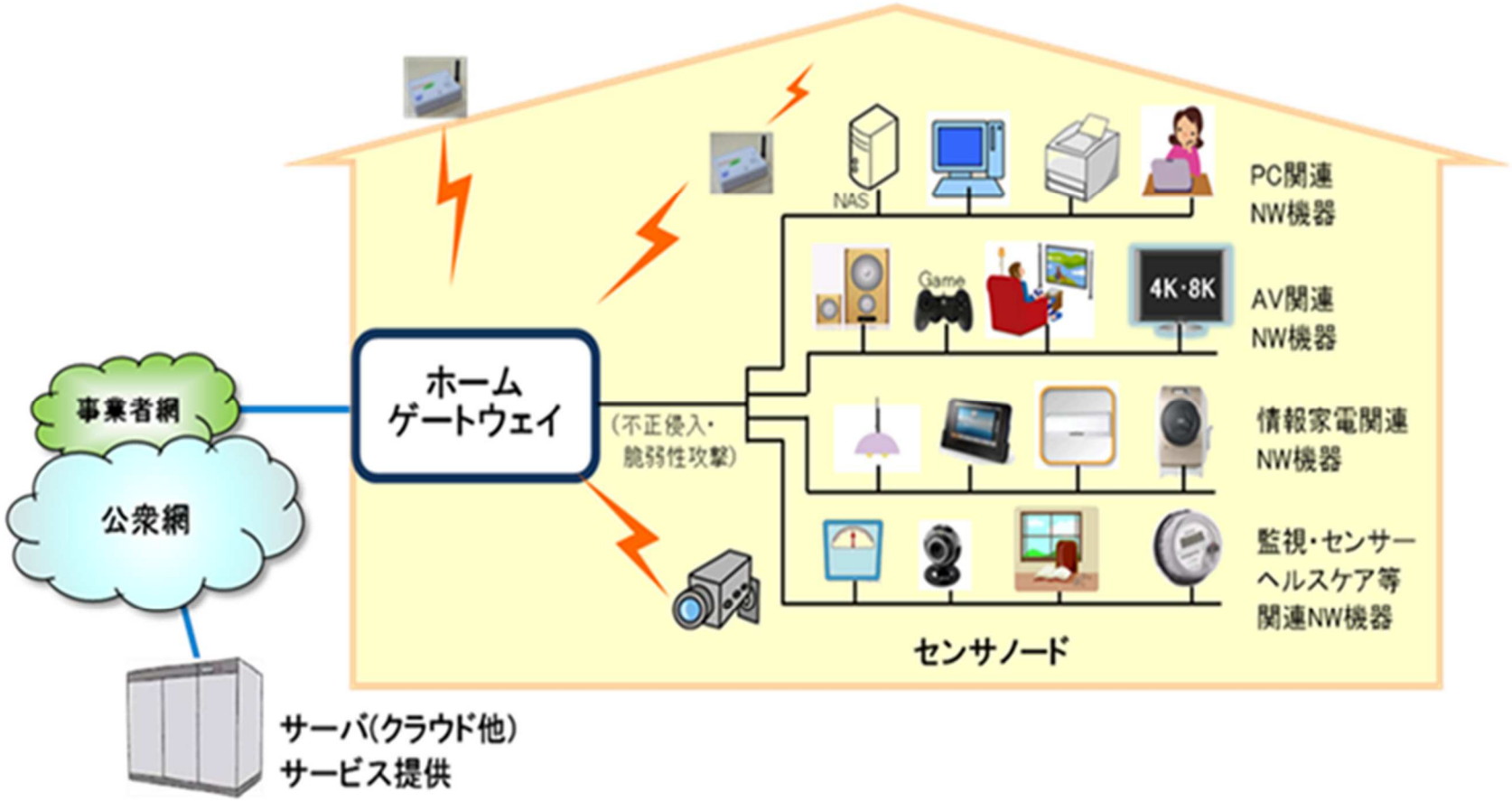
- ステップ1：リスクの明確化
- ステップ2：頻度(Likelihood)を見積もる為のファクタ
- ステップ3：影響度(Impact)を見積もる為のファクタ
- ステップ4：リスク影響度の決定
- ステップ5：対策内容の決定
- ステップ6：リスク評価方法のカスタマイズ

■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。

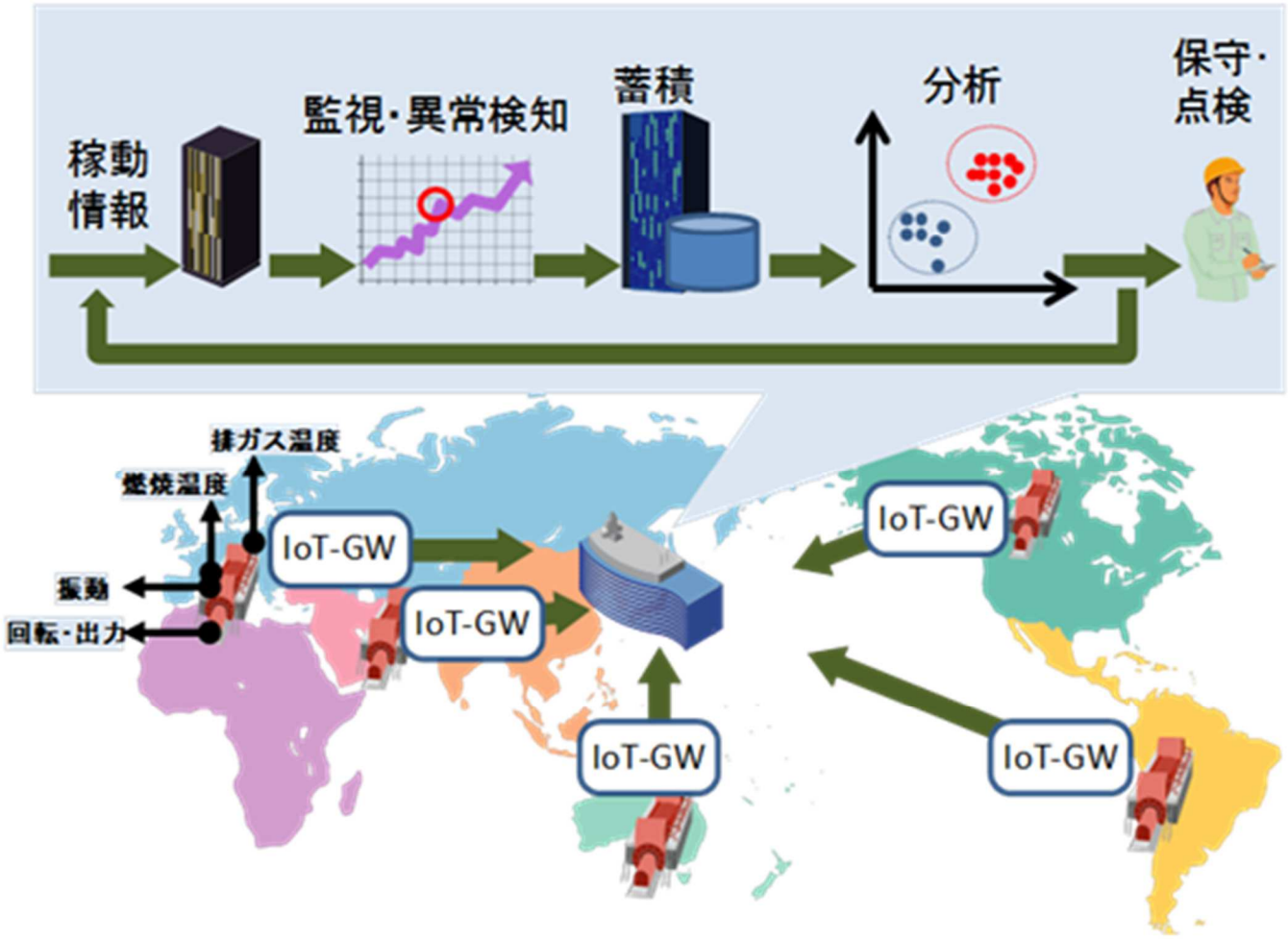
3.ケーススタディ–その1–

■ホームゲートウェイ
　守るべき資産：金融資産、評判



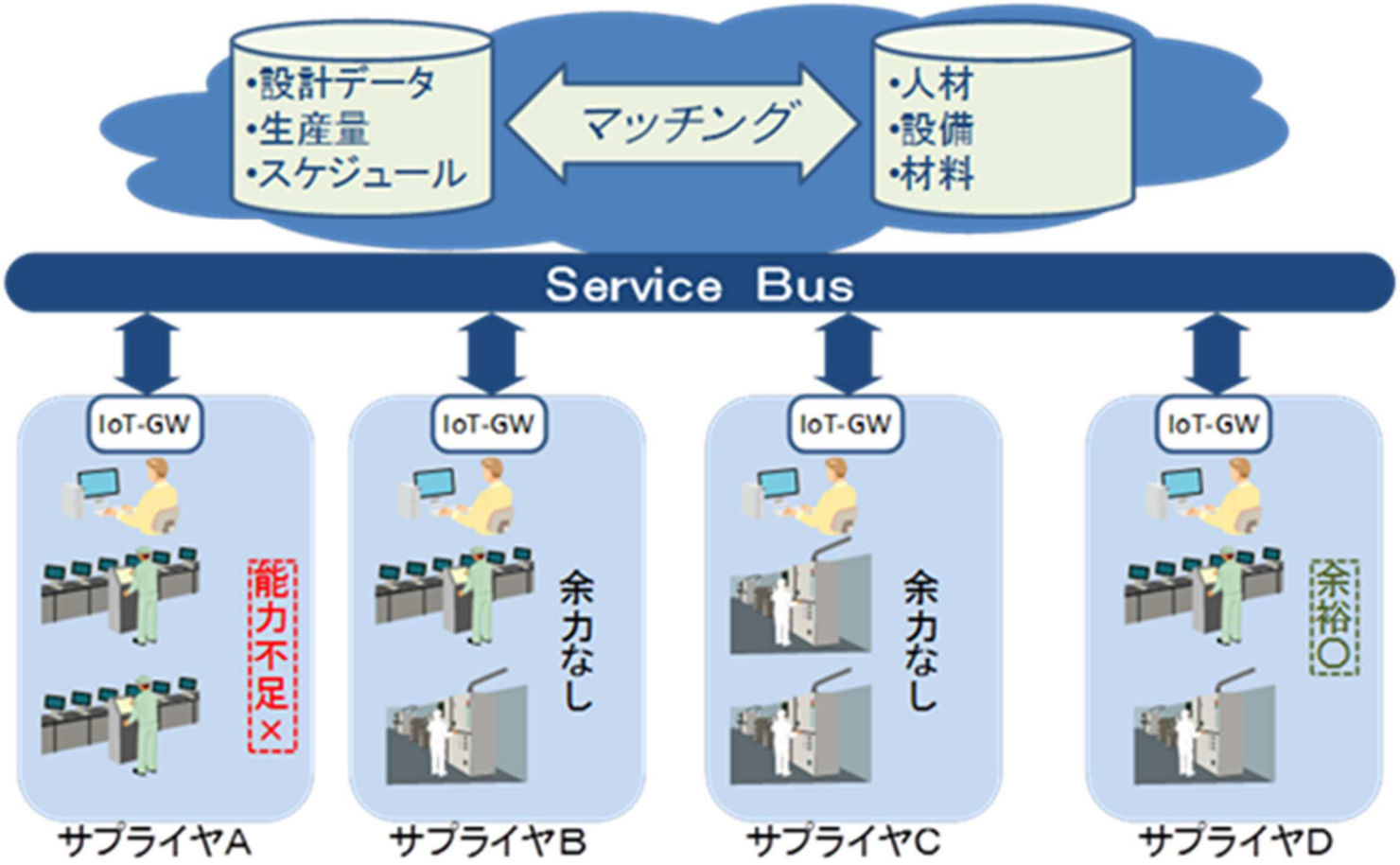
3.ケーススタディ–その2–

■スマートメンテナンス
守るべき資産：人命(アクチュエータの暴走)、評判



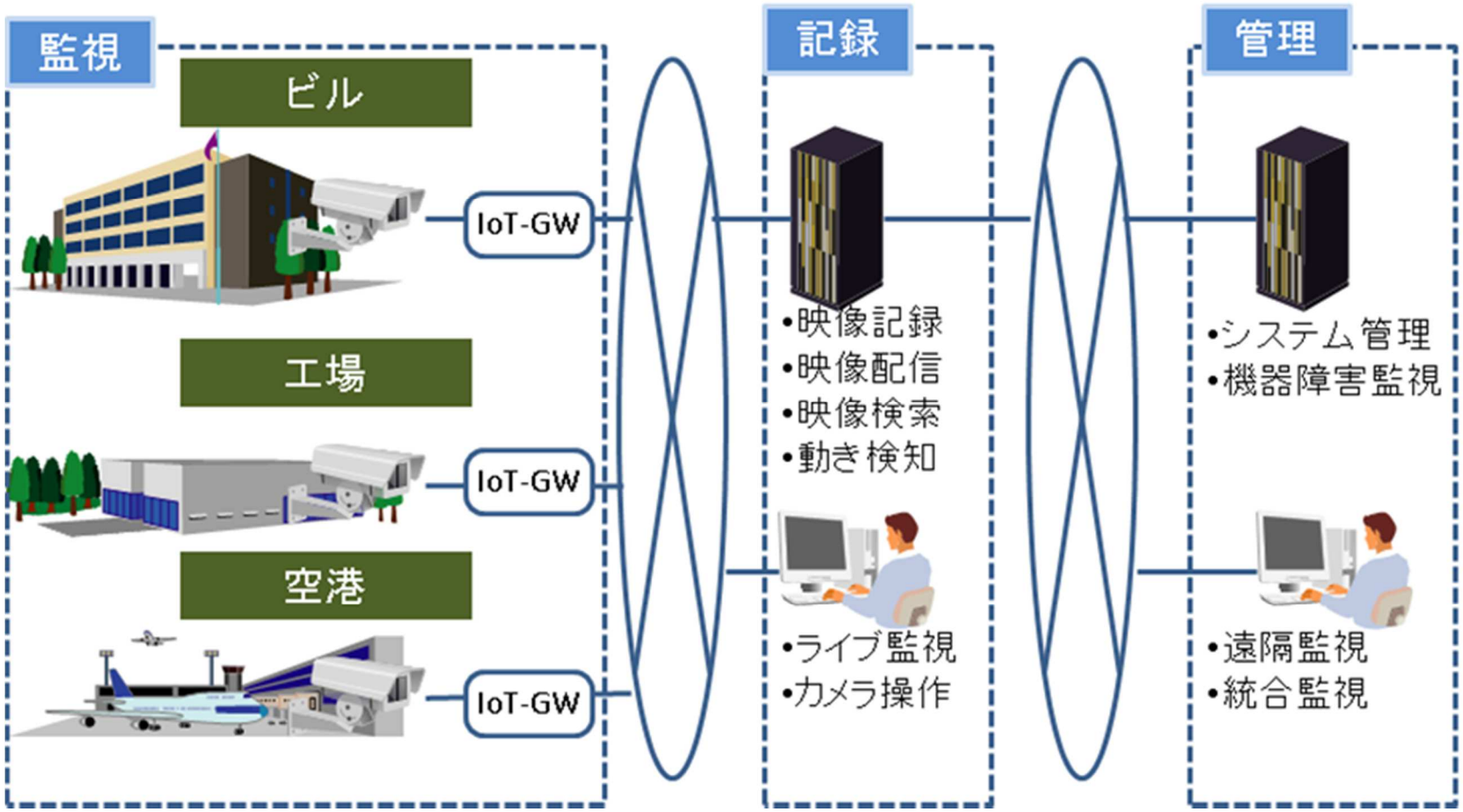
3.ケーススタディ–その3–

■サプライチェーン管理および生産ライン最適化
守るべき資産：生産設備、評判



3.ケーススタディ–その4–

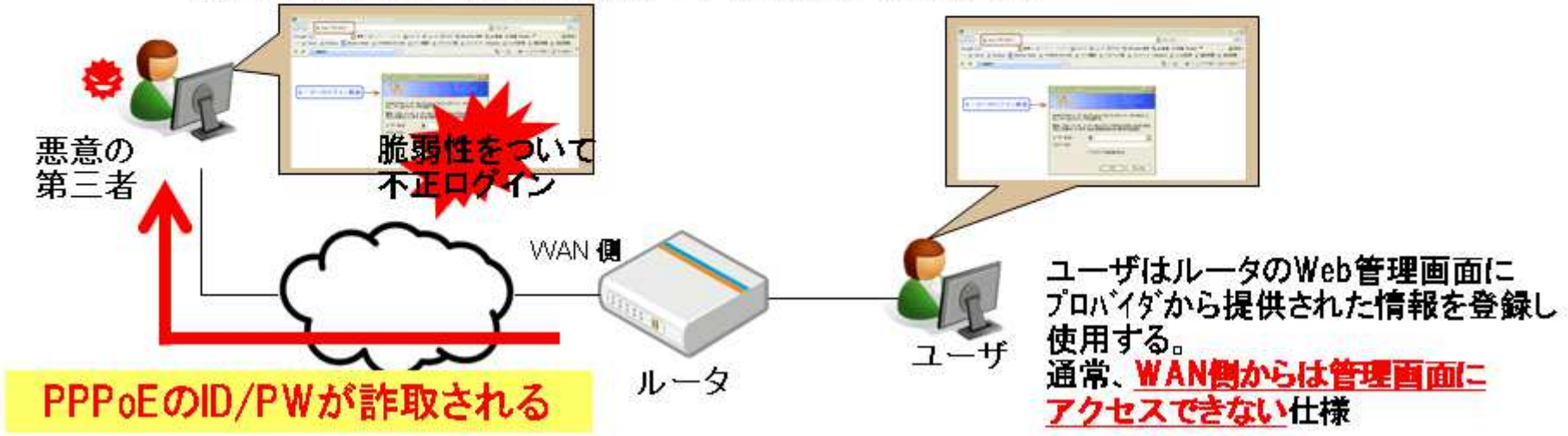
■映像監視
守るべき資産：映像情報(プライバシ)、評判



4.脆弱性、懸念されるリスクの定義

■脆弱性

脆弱性：①WAN(インターネット)側からルータのWeb管理画面へアクセス可能。
②ルータのWeb管理画面の初期ID/PWが単純である。
（初期ID/PWは製品によらず、同一。マニュアルに記載有。）
③ルータのWeb管理画面において、設定されているISP提供情報(PPPoE)が簡単に読取り可能な状態(平文)保存されている。



■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

5.ケーススタディ結果比較

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

6.各リスク評価手法の特徴-その1-

- 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。

6.各リスク評価手法の特徴-その2-

- 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。

6.各リスク評価手法の特徴-その3-

- 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。