HITACHI
Inspire the Next

パネル討論:「ITリスク学はいかにすれば有益なものになりうるか」

～相互理解のためのモデリングアプローチの提案～

2008/6/28

株式会社 日立製作所

千葉　寛之　P.E.Jp, CISSP, CISA

uVALUE

1. そもそもセキュリティの定義は！？

HITACHI
Inspire the Next

「情報セキュリティ」に関して一般的に知られている定義：

組織にとって価値ある情報資産を，機密性、完全性、可用性の観点において維持するもの

- そもそもセキュリティの意味は広い。防犯も広義のセキュリティに含まれる。
- 「情報セキュリティ」をおおざっぱにいえば、「情報および情報システムを健全な状態で利用できること」
- 上記、「CIA」による定義は、広く認知されている。
- ただし、信頼性、責任追跡性、真正性、否認防止といった概念も提示されている。

セキュリティの定義は複数存在してよいが、それらの観点の違い、対象領域による適不適等を、整理できないか？

2. 情報セキュリティの定義いろいろ(参考)

HITACHI
Inspire the Next

OECDガイドライン(1992年11月26日※1):

「情報システムセキュリティの目的は、情報システムに依存する者を、可用性、機密性、完全性の欠如に起因する危害から保護することである。」[IPA OECDセキュリティガイドライン研究会訳]

BS7799-2:2002

情報セキュリティ:
情報の機密性、完全性及び可用性の(セキュリティ)維持。(英和対訳版)

JIS Q 27001:2006(ISO/IEC 27001:2005)

情報セキュリティ:
情報の機密性、完全性及び可用性を維持すること。さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めても良い。

GMITS[TR X 0036-1:2001(ISO/IEC TR 13335-1:1996)]

ITセキュリティ:
機密性、完全性、可用性、責任追跡性、真正性、及び信頼性の定義、達成、維持に関するすべてのセキュリティ。

MICTS[JIS Q 13335-1:2006(ISO/IEC 13335-1:2004)]

ICT(Information and Communications Technology)セキュリティ:
ICTにかかわる機密性、完全性、可用性、否認防止、責任追跡性、真正性並びに信頼性の定義づけ、達成及び維持に関連したすべての側面。

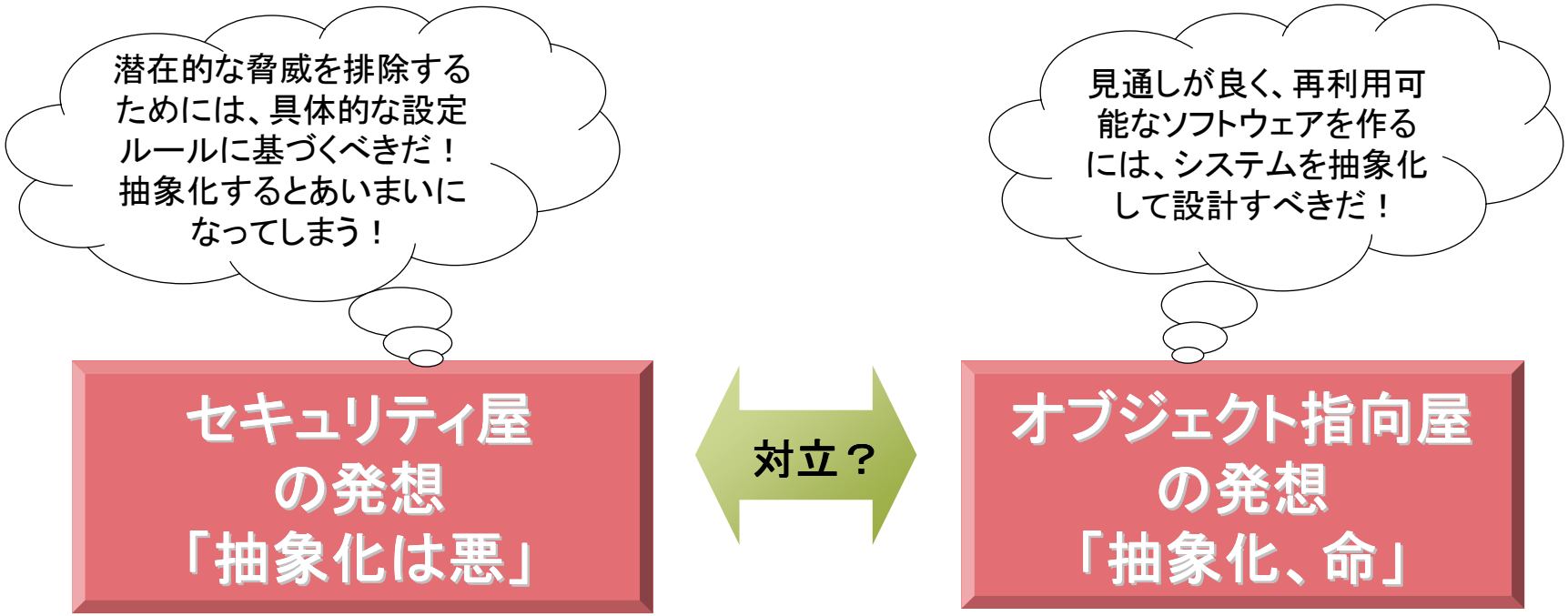
情報セキュリティ:
情報にかかわる機密性、完全性、可用性、否認防止、責任追跡性、真正性並びに信頼性の定義づけ、達成及び維持に関連したすべての側面。

CIAによる定義

6～7特性による定義

※1:2002年のOECDガイドライン「セキュリティ文化の普及に向けて」では、セキュリティの定義は明に示されていない

3. セキュリティとソフトウェア工学



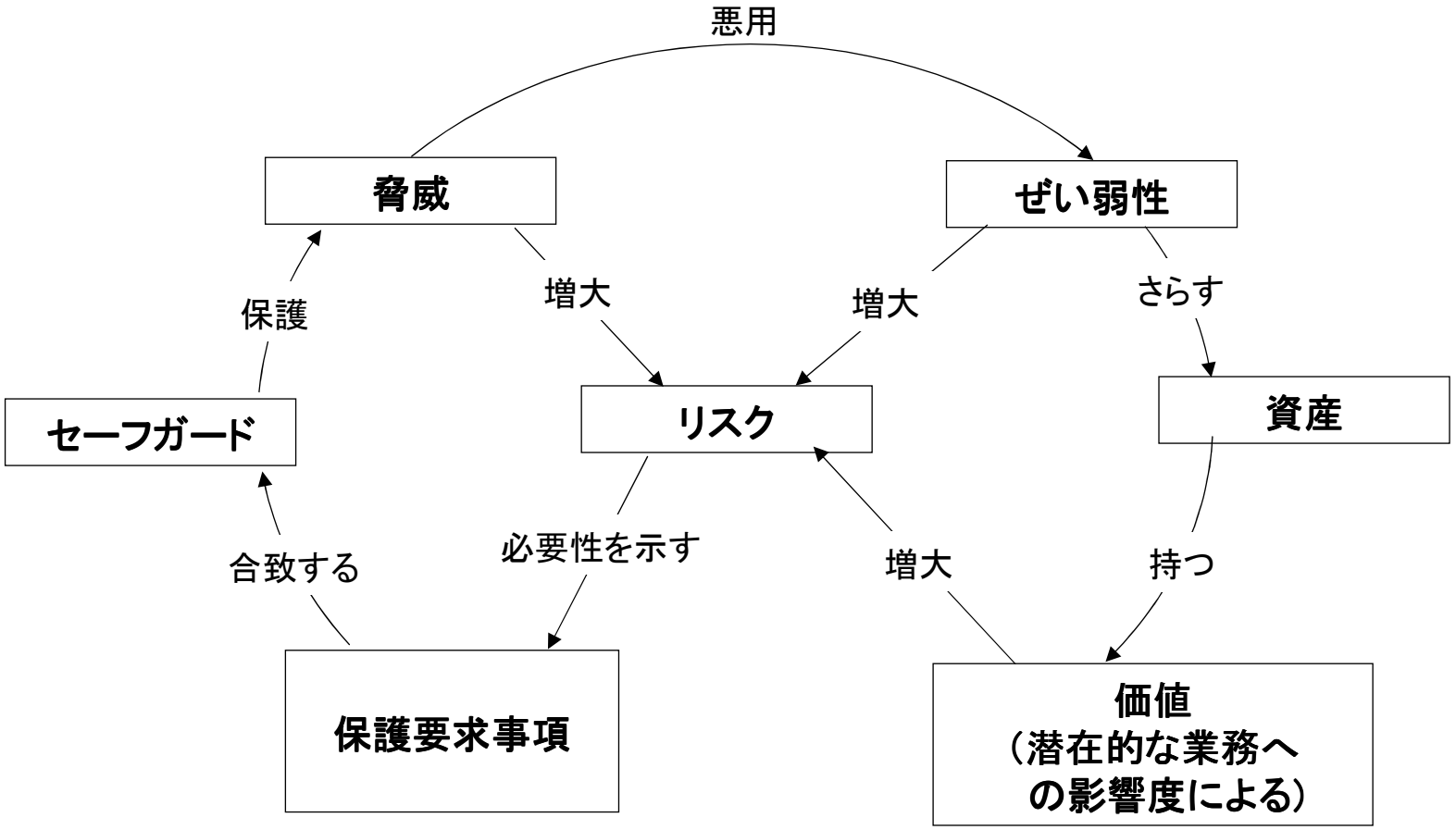
どちらの発想も、間違っていないはず．．．．．

・セキュリティの世界において（概念的な）モデル化を行うことで、脅威や対策の有効性や網羅性等を「見える化」し、理解を進めるために役立てることができるのではないか？

4. セキュリティに関する既存モデル(例1)

HITACHI
Inspire the Next

ISO/IEC TR 13335-1:1996(GMITS)の「リスクマネジメントにおける関係」

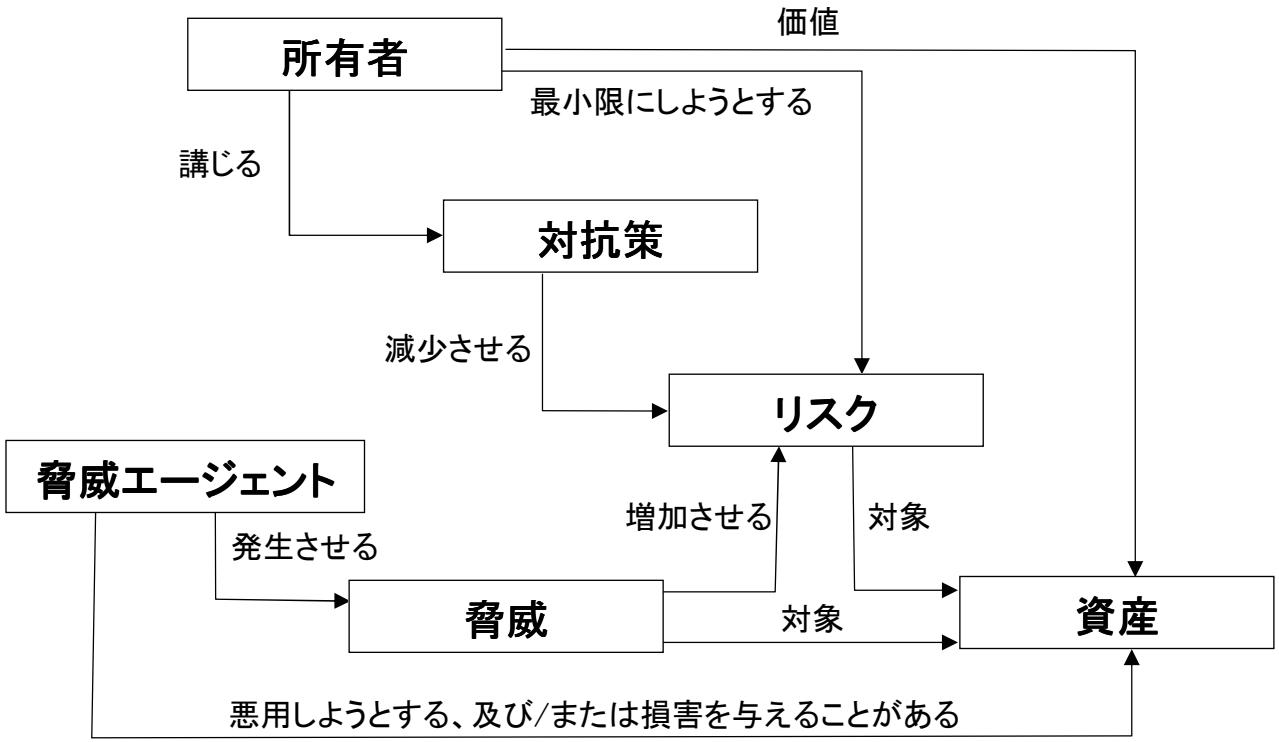


出典:TR X 0036-1:2001(ISO/IEC TR 13335-1:1996)

5. セキュリティに関する既存モデル(例2)

HITACHI
Inspire the Next

Common Criteria/ISO15408の「セキュリティの概念と関係」



出典:Common Criteria 情報技術セキュリティ評価のためのコモンクライテリア　パート1
2006年9月バージョン3.1改訂第1版　CCMB-2006-09-001(IPA翻訳第1.2版)

uVALUE

6. モデル化できていない(!?)概念いろいろ(1)

HITACHI
Inspire the Next

マーフィの法則(一般形)
「起きて欲しくないことは、必ず起きる」

＜証明＞
（1） いやな事が起きる確率をp(一般に低い)とする
（2） 1度の試行で起きない確率は、「1－p」である
（3） n回の試行で一度も起きない確率は、(1－p)のn乗となり、nが十分大きい時、0に収束する
（4） すなわち、起きて欲しくないことがずーっと起きない確率は、ゼロに収束する

ゆえに、
十分多い試行回数において、
起きて欲しくないことが1回でも起きる確率は1に収束する(＝必ず起きる)

注:なんちゃって心理学的補足: 「人間、いやなことは忘れない」

教訓: 中学、高校で習った(1回の試行に対する)確率と、ある期間における想起率は違う。

(リスクを考える際に、脅威の発生確率を考える上で重要)

7. モデル化できていない(!?)概念いろいろ(2)

HITACHI
Inspire the Next

「セキュリティ芝居(Security Theater)」

出典:ブルースシュナイアー「セキュリティはなぜやぶられたのか」

・まったく意味がないなら、対策として無視すれば良いのだが. . .
・意外と意味を成すこともあるのでは？
　→　副次効果として、従業員のセキュリティ意識が向上
　→　賢い攻撃者には意味を成さないが、お馬鹿な攻撃者には有効

セキュリティ対策の「セキュリティ芝居度」を計る手立てはないか？
セキュリティ芝居が、有効な場合、逆効果な場合を把握することはできるのか？

8. モデル化できていない(!?)概念いろいろ(3)

HITACHI
Inspire the Next

「無知のセキュリティ」

出典：ケビン・ミトニック、ウィリアム・サイモン「欺術一史上最強のハッカーが明かす禁断の技法」

・セキュリティ芝居の１種
・永遠に隠すことができない（マーフィーの法則の応用)ことを考えるべき。
・一般に、外部攻撃者と内部攻撃者は別に考えて対策するが、退職者等を考慮すると、外部攻撃者が、内部者同様の知識を持つ可能性がある。
・でも、通常よく行われている方法の一つである。

「無知のセキュリティ」が有効な局面を、モデル化できるか？

9. モデル化のためのアプローチ

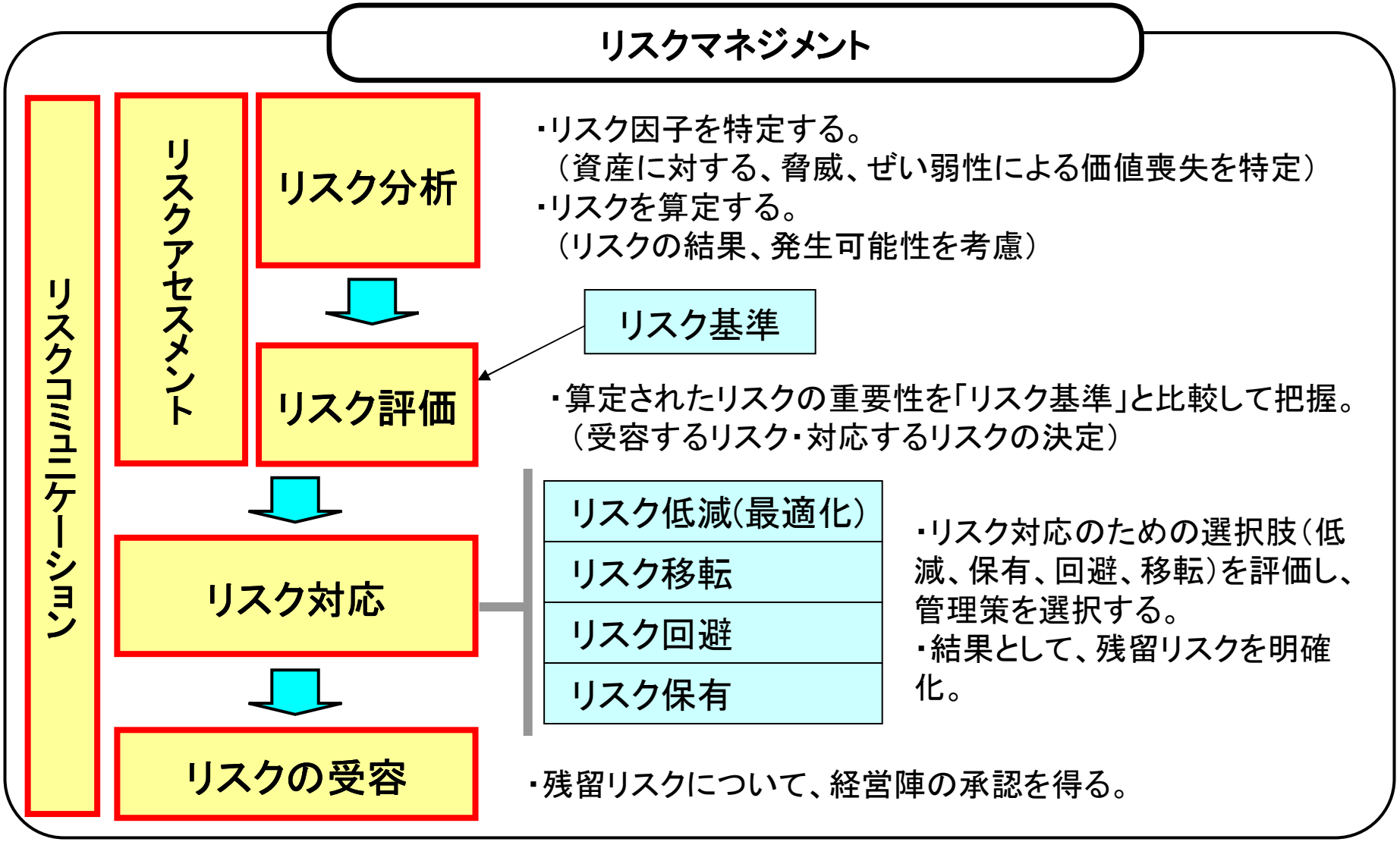
HITACHI
Inspire the Next

セキュリティおよび関連するリスクについて、より深く理解するためのモデルを整備するには？

・セキュリティに関するリスク分析はよく行われているが、心理学的な要因等まで考慮されたモデルはたぶん存在していない。
・リスクマネジメントにおいては、リスクアセスメント～リスク対応といった領域は、確立しつつある。ただし、リスクコミュニケーション、特にそのあいまい性については、うまくモデル化されたものは存在していない。
・セキュリティは、まだ日が浅く未成熟な分野であり、発展の過程を同時代史として捉える考え方も有効。

「セキュリティ」を理解するための、多面的、学際的観点から、理解モデルの整理することが有効ではないか！？

参考 リスクマネジメント



出典：TR Q 0008:2003(ISO/IEC GUIDE73:2002)より作成

uVALUE

HITACHI

Inspire the Next