事件駆動型セキュリティを脱却するためのリスク対応法

東京電機大学
佐々木良一

自己紹介

＜現職＞
佐々木良一
東京電機大学
名誉教授
同大学サイバーセキュリティ研究所
客員教授

＜略歴＞
1971年日立製作所入社。システム開発研究所にて、システム高信頼化技術やセキュリティ技術（1984年より）等の研究開発に従事　同研究所部長や主管研究長兼セキュリティシステム研究センタ長を歴任

2001年4月から2018年3月まで東京電機大学教授、2018年4月より2020年3月特命教授、2020年4月より現職

日本セキュリティ・マネジメント学会会長，
デジタル・フォレンジック研究会会長
内閣官房サイバーセキュリティ補佐官
などを歴任

目次

はじめに

１．セキュリティ対策の歴史を振り返り、事件駆動型セキュリティだったことを示す。

２．事件駆動型セキュリティを排し、適切なセキュリティ対策を実施するためには、ゼロリスクはないという認識の下、リスクベースアプローチが必要であることを示す。

３．そのためのアプローチとして、講演者らが開発したITリスク学や、多重リスクコミュニケータを解説する。

目次

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

2000年　　不正アクセス禁止法施行

2000年　　JNSA発足（2001年NPO化）

2001年　Code　Red、Sircumによる被害

2001年　　電子署名法施行

2001年　　CRYPTREC（暗号技術検討会）発足

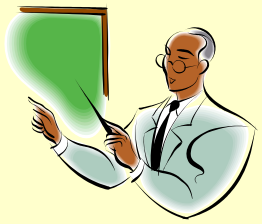
＜セキュリティにとっての第二のターニングポイント＞

2010年　Stuxnetの出現(遠心分離機への攻撃)

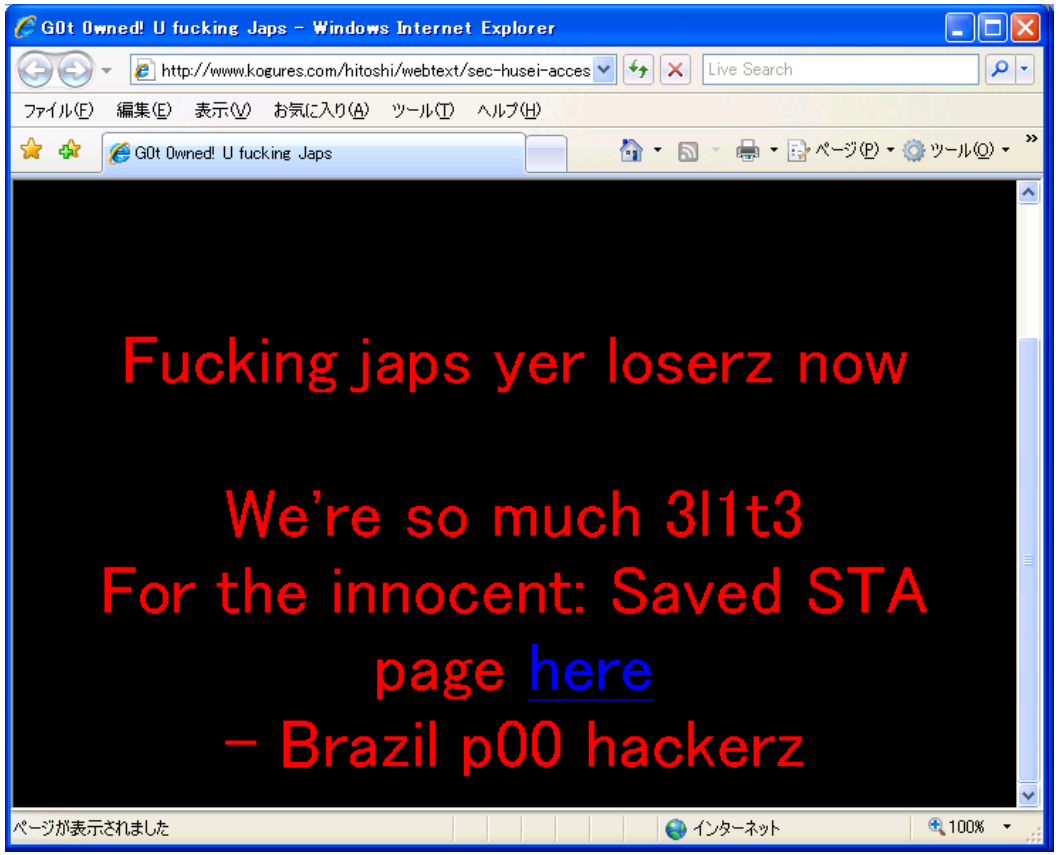
2011年　　ウイルス作成罪施行

2011年　三菱重工などへの標的型メール攻撃

2015年　日本年金機構への攻撃



科学技術庁ホームページ改ざん事件



2000年1月

Reference：http://www.kogures.com/hitoshi/webtext/sec-husei-access/homepage.html

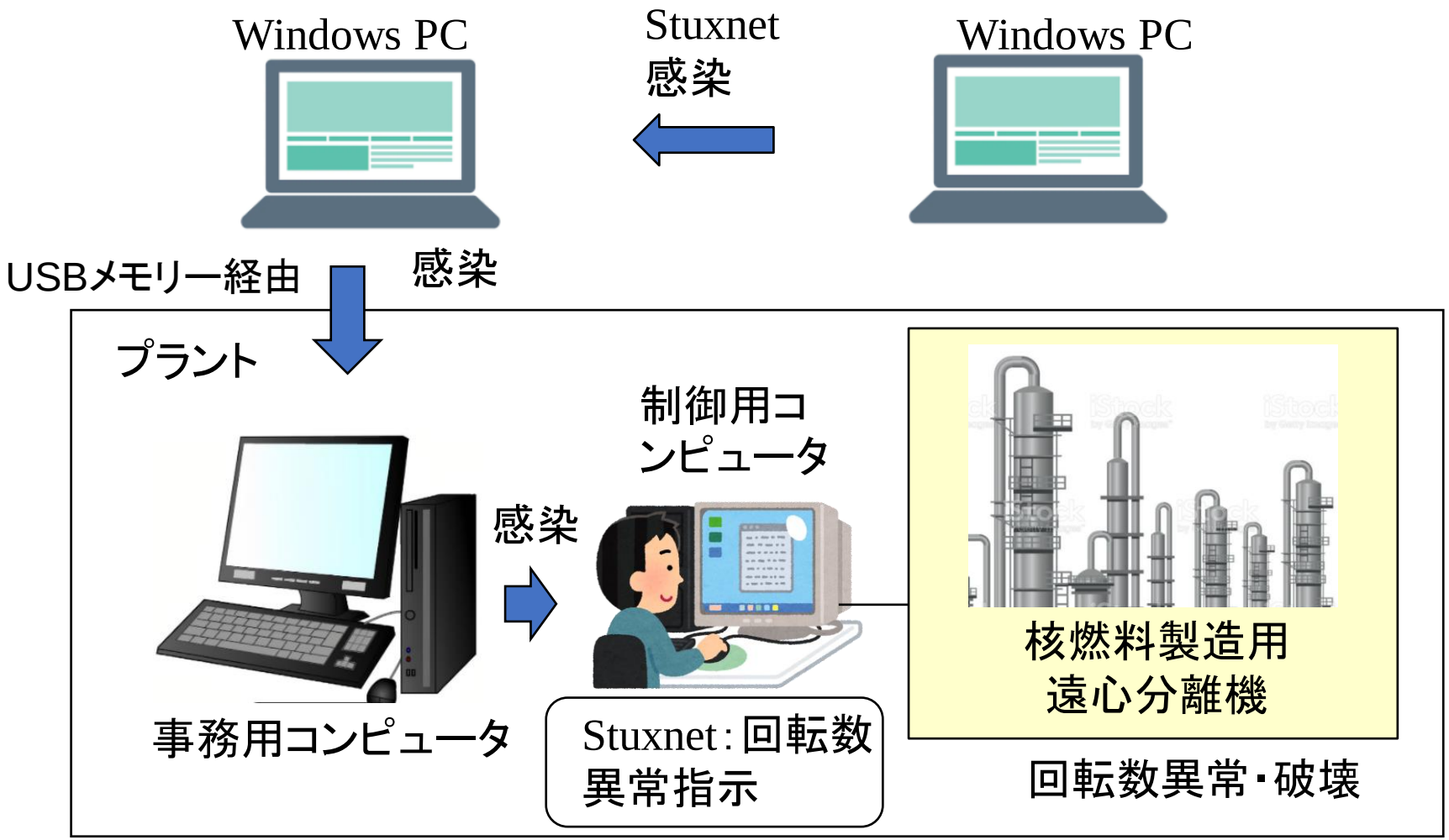
サイバー攻撃の歴史

＜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
2000年　　不正アクセス禁止法施行
2000年　　JNSA発足（2001年NPO化）
2001年　Code　Red、Sircumによる被害
2001年　　電子署名法施行
2001年　　CRYPTREC（暗号技術検討会）発足

＜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)
2011年　　ウイルス作成罪施行
2011年　三菱重工などへの標的型メール攻撃
2015年　日本年金機構への攻撃

Stuxnetの概要

Stuxnet：Windows上で動くマルウエア



２つのターニングポイントの比較

	第一次ターニングポイント後（2000年ごろ）	第二次ターニングポイント後（2010年以降）
攻撃目的	面白半分	多様化（面白半分、主義主張、お金儲け、国家の指示）
攻撃者	ハッカー（クラッカー）	ハッカー、ハクティビスト、犯罪者、スパイ、軍人
攻撃対象	WEBなどの一般IT	重要情報インフラも＜Stuxnet＞
攻撃パターン	不特定多数	標的型＜Stuxnet、ソニー、三菱重工、日本年金機構＞
セキュリティタイプ	完全な事件駆動型セキュリティの時代	新しい事件が発生し種々のリスクにバランスよく対応が必要なノー「ゼロリスク」時代

リスクベースアプローチが必要に

目次

リスクとは（1）

1．リスク とは，英語のRiskの訳であり，危険と訳される場合もある．「**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いて常に**不確実性**を伴う。

2．リスクという言葉には
（1） 損失をもたらす「純粋リスク」だけを考える場合と
（2） 損失がある一方で利得の可能性もある「投機的リスク」も含めて考える場合がある

3．（2）に基づくものとして、ISO31000:2018では次の定義
「目的に対する不確かさの影響」 経営リスクなどはこの立場

4．サイバーセキュリティの分野では（1）の立場を採用することが多い

リスクとは（2）

① 工学分野の確率論的リスク評価では通常次のように定義することが多い。
リスク＝損害の大きさ　×損害の発生確率

② 「ISO/IEC 27005：2008」ではITのリスクを以下のように定義している

リスク＝資産 × 脅威 × 脆弱性

資産　×　脅威 × 脆弱性　　対応付け

損害の大きさ　×損害の発生確率

リスク社会

ドイツの社会学者ウルリヒ・ベック
「かつて人類は地震などの自然災害や病気などを恐れていたが，現在ではそれらのリスクをコントロールするために開発した科学技術そのものが新たなリスクとして問題になってきている．」と指摘．
「このような新たなリスクに覆われた社会を「リスク社会（翻訳では危険社会）」」と呼んだ．

ウルリヒ・ベック（東廉／伊藤美登里訳）「危険社会　新しい近代への道」法政大学出版局，1998年

セキュリティリスクは新たなリスクの1つ

誤ったリスク認識の例

2001年の９．１１後、飛行機が危険という認識から1年間自動車の利用者が増えた。

それによって1年間で米国で1595人の自動車事故の死亡者が増加（これは９．１１の不幸なフライトの総死亡者の約6倍）

ベルリンのマックス・ブランク研究所の心理学者ゲルド・ギレンザーの調査結果

ダン・ガードナー「リスクにあなたは騙される」早川書房、2009、p11

日本人のリスク感の特徴

＜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

①②と③は矛盾するがこのようなリスク感を形成する要因として、日本人は不可実性を回避する傾向が高い、現状肯定的心情があるとしている。

奈良由美子「生活とリスク」放送大学教育振興会、2007　（林ほか「セキュリティ経営」勁草書房、2011より）

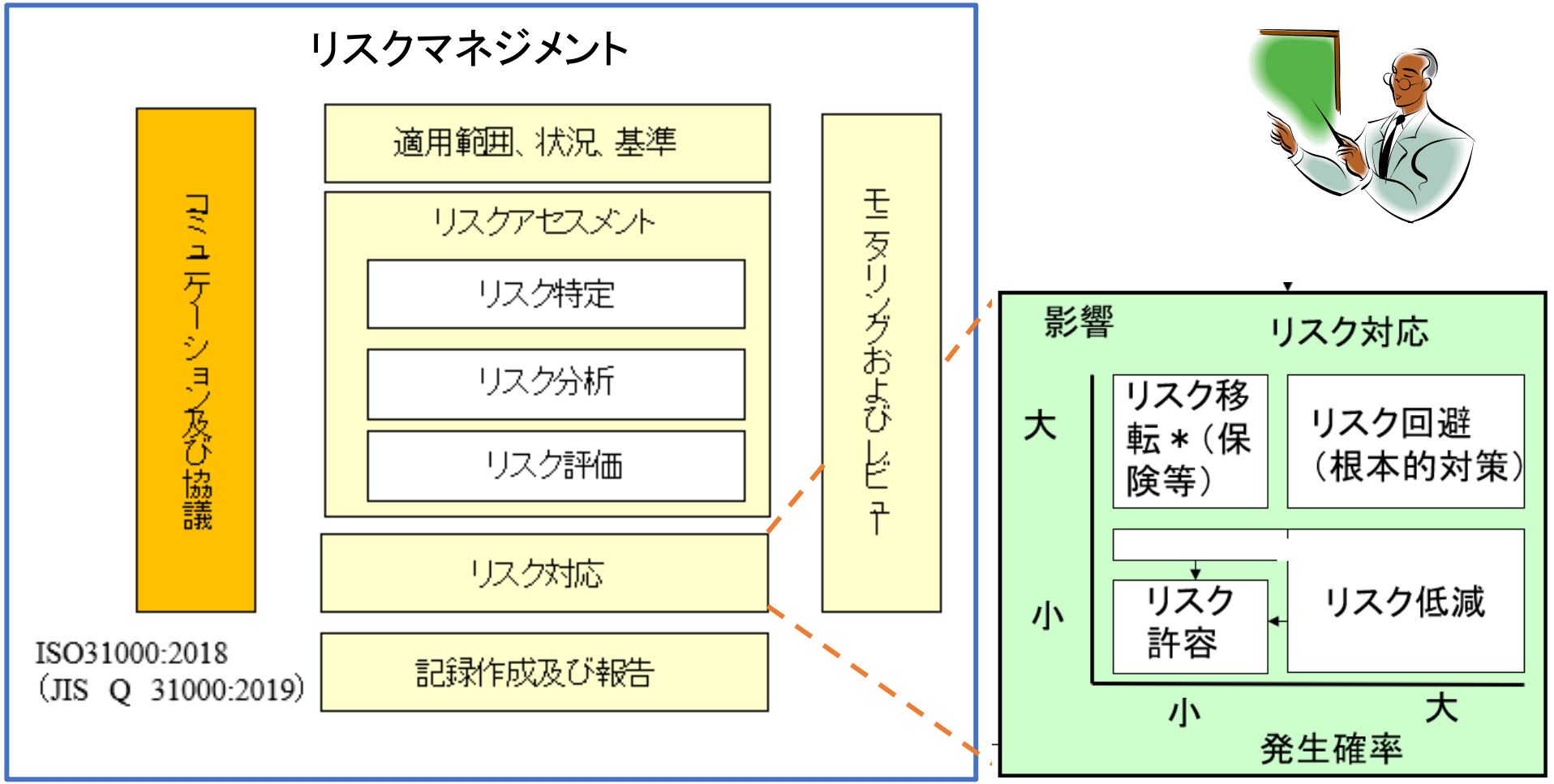
私たちの基本スタンス

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と思う。

そのため情報システムのリスクに応じてどう対応すべきかを明確化していく。

リスクマネジメントの要素と相互関連



リスク分析法

アプローチ法	長所	欠点
定量的	費用対効果分析を最も効果的に支援	得られた数値または結果に関する信頼性の説明が必要
準定量的	比較的少ないコストで相互比較が可能に	厳密性が不足
定性的	分析にコストがかからない	経験により結果が異なる場合もある

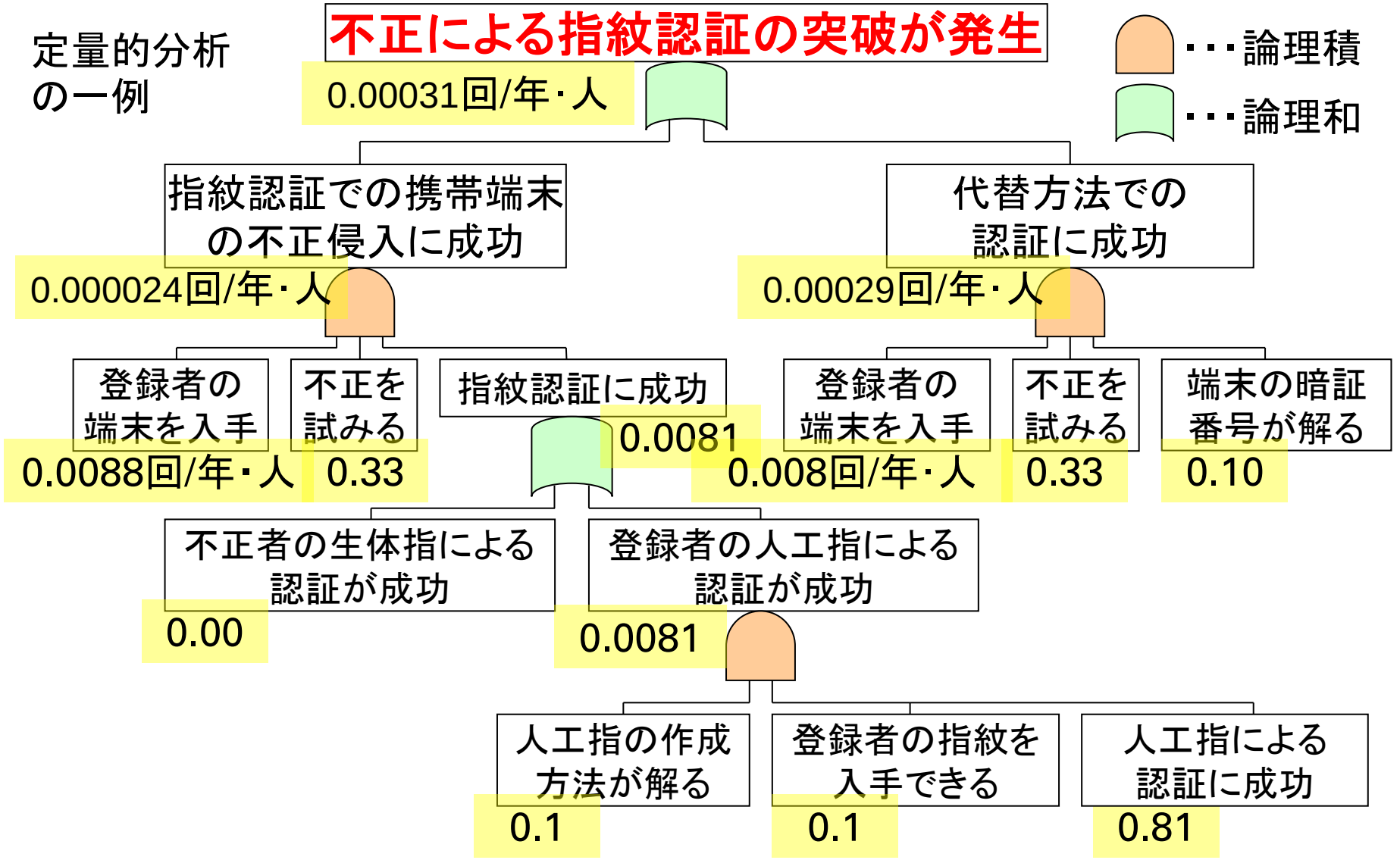
FIPS SP 800-30

定量的リスク分析法

1. アタックツリー法
   （トップダウン型インシデント原因分析用）
2. イベントツリー法
   （シーケンスが深いシステム向け）
3. FMCA法＊
   （ボトムアップ型結果推定用）
4. STAMP/STPA法＊
   （フィーバック系を含むシステム向け）
5. イベントツリー・ディフェンスツリー結合法
   （シーケンスが深いシステムで、対策案の評価も含むシステム向け）

＊準定量的リスク分析法になることもあり

指紋認証に関するアタックツリー分析法



リスク分析法

アプローチ法	長所	欠点
定量的	費用対効果分析を最も効果的に支援	得られた数値または結果に関する信頼性の説明が必要
準定量的	比較的少ないコストで相互比較が可能に	厳密性が不足
定性的	分析にコストがかからない	経験により結果が異なる場合もある

FIPS SP 800-30

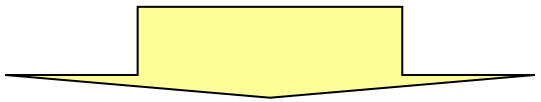
準定量的方法
ーJIPDECのリスク算出式ー

＜リスク値の計算式＞

リスク値＝情報資産の価値　X　脅威　X　脆弱性

＜適用例＞

情報資産	資産価値	脅威レベル	脆弱性レベル	リスク値
A	4	3	3	３６
B	2	4	5	４０



リスク値の大きい情報資産Bに対する対策を優先

25マスによる準定量的分析方法

	インシデントシナリオの発生可能性	きわめて低い（ほとんど発生しない）	低い（まず発生しない）	中程度（発生の可能性がある）	高い（発生の可能性が高い）	きわめて高い（頻繁に発生する）
事業影響	きわめて低い	0	1	2	3	4
	低い	1	2	3	4	5
	中程度	2	3	4	5	6
	高い	3	4	5	6	7
	きわめて高い	4	5	6	7	8

ENISA（European Network and Information Security Agency）等で利用

リスク分析法

アプローチ法	長所	欠点
定量的	費用対効果分析を最も効果的に支援	得られた数値または結果に関する信頼性の説明が必要
準定量的	比較的少ないコストで相互比較が可能に	厳密性が不足
定性的	分析にコストがかからない	経験により結果が異なる場合もある

FIPS SP 800-30

情報システムのリスク分析・評価技法

- 定性的手法
  - チェックリスト利用方法
    - 情報資産や利用環境についてチェックポイントを上げたリストを用いて調査分析（通産等の基準・ガイドを参考にリスト作成）
  - 質問表利用方法
    - 職務担当別、階層別に質問表で調査し、脆弱性を洗い出し、回答のウエイト付けと相対評価で優先対策を決定
  - シナリオ分析法
    - 脅威と影響・損失の多岐のシナリオを作成・評価して対応策を示す

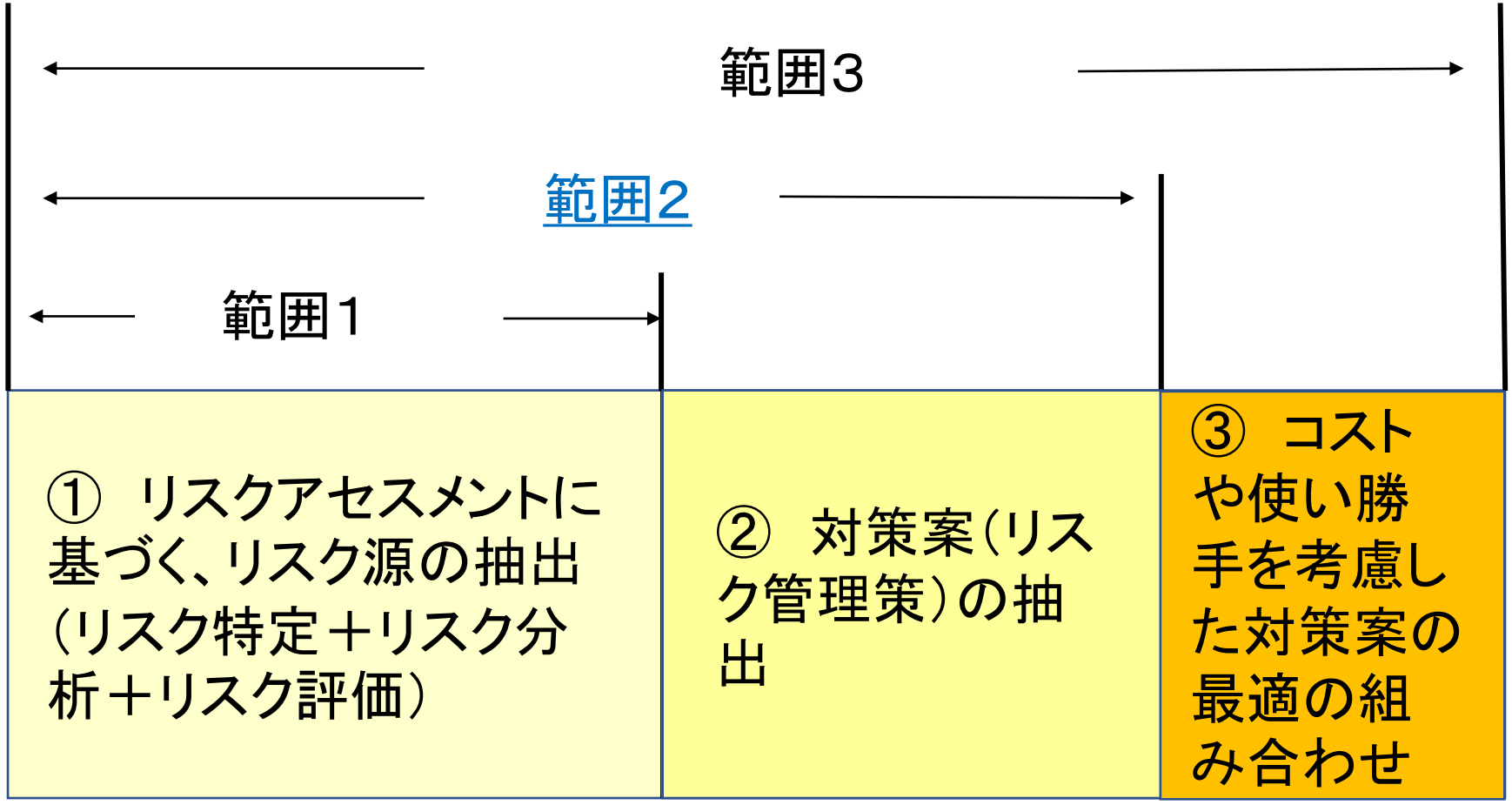
参考となる準定量的リスクアセスメント法

「制御システムのセキュリティ分析ガイド　第2版　～セキュリティ対策におけるリスクアセスメントの実施と活用～」IPA 2023年3月バージョン

https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf

比較的よくできた方式

リスクアセスメントが扱う範囲



詳細リスク分析法

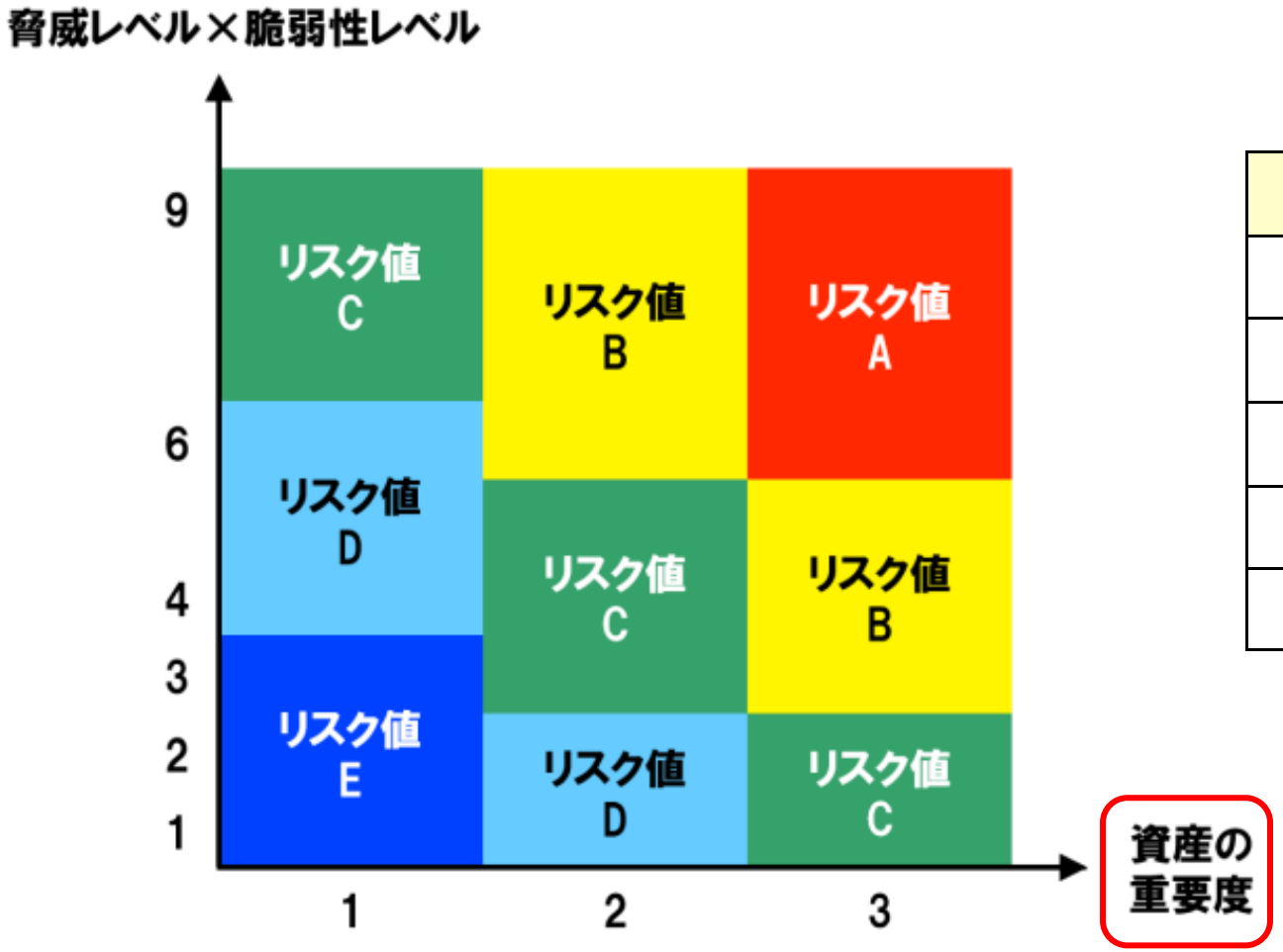
1．資産ベースのリスク分析は必ず実施する
　　保護資産を網羅的に把握、評価する上で不可欠
2．事業被害ベースのリスク分析は対象を絞って実施
　　事業被害を回避できるかを検証する上で不可欠

表 2-2 リスク分析手法と評価指標の関係

リスク分析手法	評価指標			
	資産の重要度	事業被害	脅威	脆弱性
資産ベースのリスク分析	○	－	○	○
事業被害ベースのリスク分析	－	○	○	○

https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf

資産ベースにおける脅威レベル・脆弱性レベル・資産の重要度とリスク値の関係



リスク値	意味
A	リスクが非常に高い。
B	リスクが高い。
C	リスクが中程度。
D	リスクが低い。
E	リスクが非常に低い。

https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf

資産の重要度の判断基準の例

重要度

高

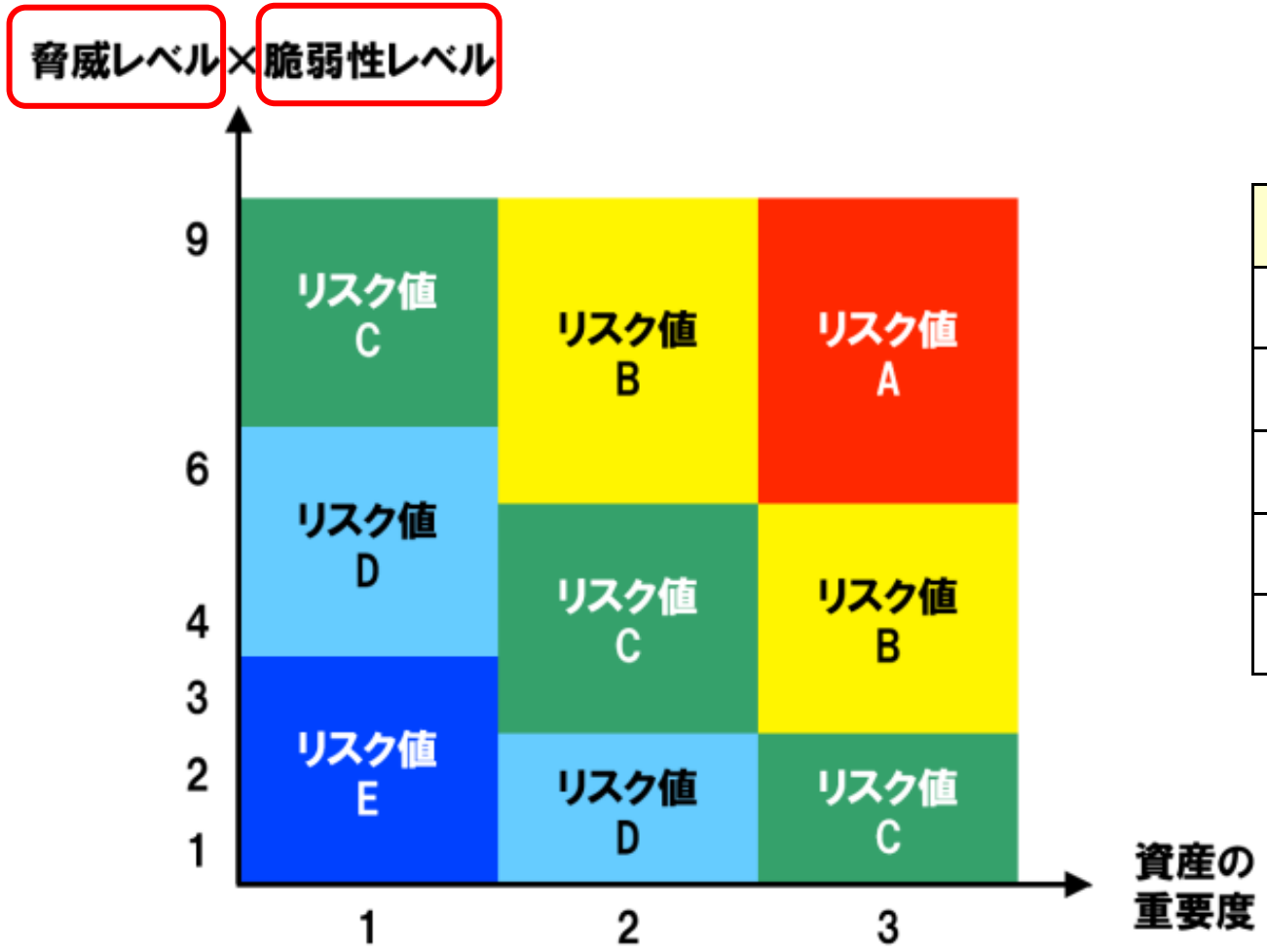
低

表 4-7 資産の重要度の判断基準の定義例(2)

評価値	判断基準
3	・資産が攻撃された場合、システムが 1 週間以上停止する恐れがある。 ・資産から情報が漏えいした場合、5 億円以上の損失が発生する恐れがある。 ・資産が攻撃された場合、従業員の死亡事故が発生する恐れがある。
2	・資産が攻撃された場合、システムが 24 時間以上 1 週間未満停止する恐れがある。 ・資産から情報が漏えいした場合、500 万円以上 5 億円未満の損失が発生する恐れがある。 ・資産が攻撃された場合、従業員の重傷事故が発生する恐れがある。
1	・資産が攻撃された場合でも、システムが 24 時間以上停止する恐れはない。 ・資産から情報が漏えいした場合でも、500 万円以上の損失が発生する恐れはない。 ・資産が攻撃された場合でも、従業員の重傷事故が発生する恐れはない。

https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf

資産ベースにおける脅威レベル・脆弱性レベル・資産の重要度とリスク値の関係



リスク値	意味
A	リスクが非常に高い。
B	リスクが高い。
C	リスクが中程度。
D	リスクが低い。
E	リスクが非常に低い。

https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf

脅威の簡易評価法

悪意ある第三者が代表的な経路で当該資産までネットワーク経由で侵入する脅威（攻撃手法）に対しては、

- インターネットに直結している場合： 脅威レベル＝3
- ファイアウォールを介している場合： 脅威レベル＝2
- 複数の異機種のファイアウォールを介している場合：
  脅威レベル＝1

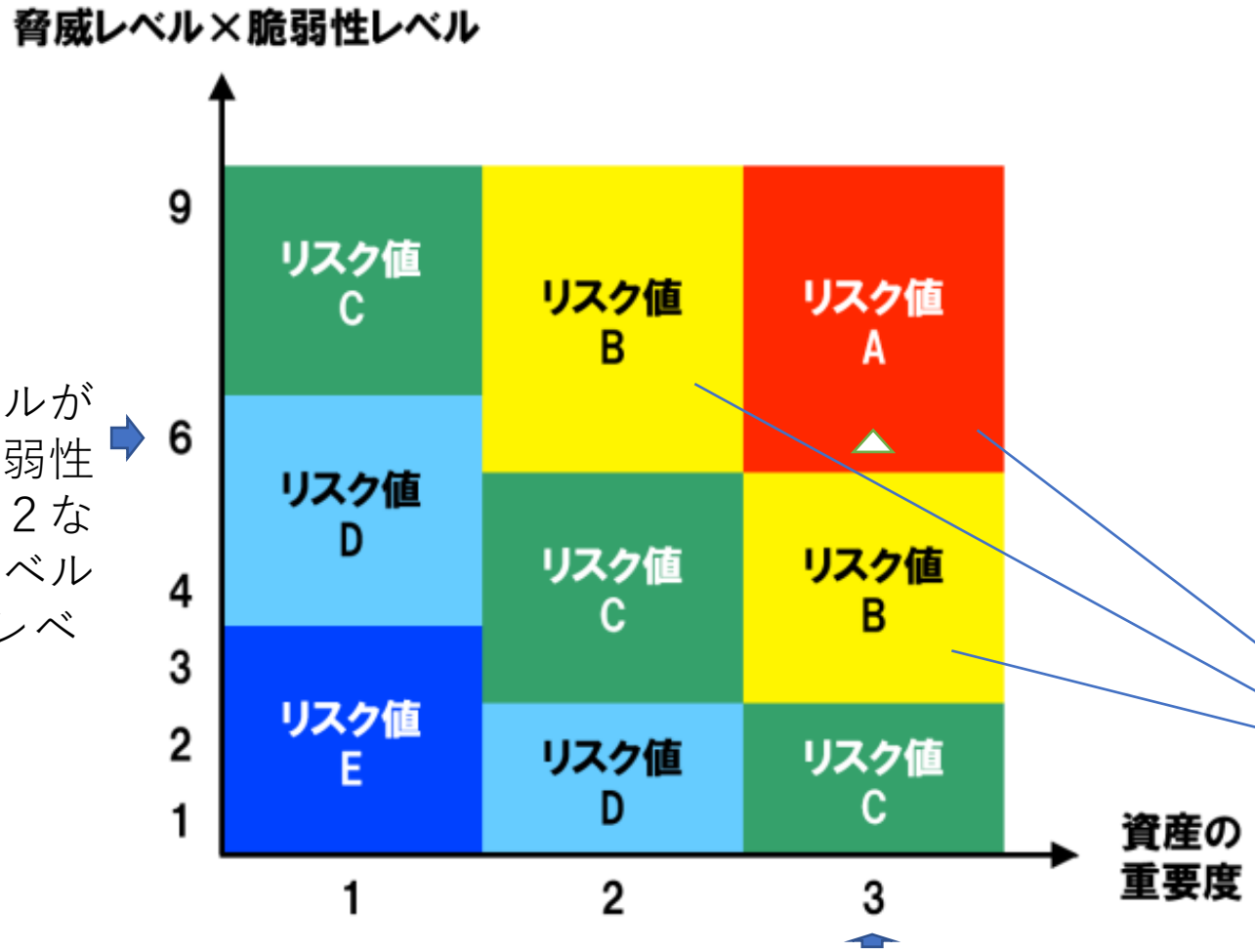
https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf

脆弱性レベルの定義

対策レベルが高い→脆弱性レベルが低い
対策レベルが低い→脆弱性レベルが高い

脆弱性レベル	対策レベル	判断基準例
3	1	防御可能な対策を実施してない
2	2	防御可能な対策を部分的に実施している
1	3	防御可能な対策を網羅的に実施している

資産ベースにおける脅威レベル・脆弱性レベル・資産の重要度とリスク値の関係



脅威レベルが３で、脆弱性レベルが２なら脅威レベルX脆弱性レベルは６

資産の重要性が３

リスク値	意味
A	リスクが非常に高い。
B	リスクが高い。
C	リスクが中程度。
D	リスクが低い。
E	リスクが非常に低い。

対応例：リスク値がA並びにBの資産に対しては対策することにしているオデ対策を実施

https://www.ipa.go.jp/security/controlsystem/ssf7ph00000098vy-att/000109380.pdf

目次

ITリスク問題が重要になった背景

社会全体のITシステムへの依存の増大によりITシステムの安全が重要に

従来よりも広い統一的アプローチが必要に

故意の不正

天災・故障・
ヒューマンエラー

①ITシステムの扱う情報の安全

②ITシステムそのものの安全
③ITシステムが行うサービスの安全

Security

Privacy・Reliability
Safety・Usability等

工学的アプローチ

心理学的・社会科学的アプローチ

新しいアプローチ法の名称例

①トラスト
②ニューディペンダビリティ　など

採用した名称

ITリスク（学）
＜確率論的扱いが不可欠＞

ＩＴシステムの安全の階層化

階層	対象	扱う事故・障害	従来の学問・技術分野	指標
３	ITシステムが行うサービスの安全	発券サービスの停止、プライバシーの喪失など	システム工学 リスク学 社会科学など	プライバシー、ユーザビリティ
２	ITシステムが扱う情報の安全	情報のCIAの喪失	セキュリティ	セキュリティ（機密性、完全性、可用性）
１	ITシステムそのものの安全	コンピュータや通信機器の故障	信頼性工学 セキュリティ	リライアビリティ、アベイラビリティ

＊

＊　従来情報セキュリティが扱っていた範囲

ITリスク問題が重要になった背景

社会全体のITシステムへの依存の増大によりITシステムの安全が重要に

従来よりも広い統一的アプローチが必要に

故意の不正

天災・故障・
ヒューマンエラー

①ITシステムの扱う情報の安全

②ITシステムそのものの安全
③ITシステムが行うサービスの安全

Security

Privacy・Reliability
Safety・Usability等

工学的アプローチ

心理学的・社会科学的アプローチ

新しいアプローチ法の名称例

①トラスト
②ニューディペンダビリティ　など

採用した名称

ITリスク(学)
＜確率論的扱いが不可欠＞

ITリスク学の確立に向けての活動

① 2008年5月に日本セキュリティ・マネジメント学会の中に「ＩＴリスク学」研究会を立ち上げ

② ITリスク学の定義

③ ITリスク学の全体像と構成要素の明確化

④ 構成要素の概要と研究課題の明確化

⑤ 研究課題の解決に向けての活動

⑥ 本の出版（２０１３年1月）

ITリスク学の定義

「不正によるものだけでなく，天災や故障ならびにヒューマンエラーによって生ずるITシステムのリスクならびにITシステムが扱う情報やサービスに関連して発生するリスクを，リスク対策の不確実性や，リスク対リスクの対立，関与者間の対立などを考慮しつつ学際的に対処していくための手段に関する学問」

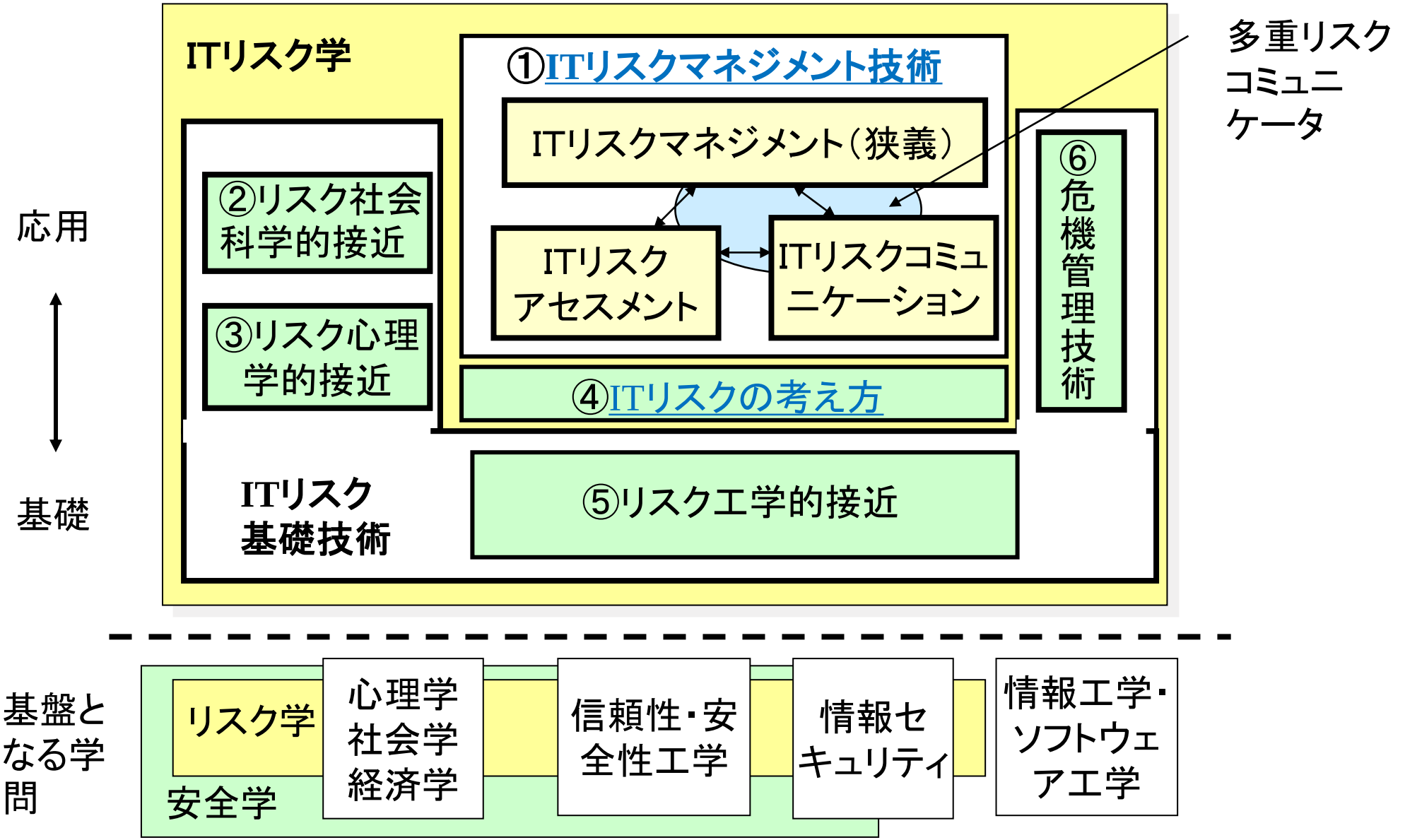
（注1）ITシステムのサービスに関するリスクを含むので、セキュリティだけでなく，プライバシーユーザビリティなども含む

（注2）一般的に扱うとあまりにも広くなるので，ITリスクの特徴である「リスク対リスクの対立，関与者間の対立を考慮しつつ」を入れることにより研究範囲を明確にした

（注3）「制御する」ではなく「対処していく」にしたのはリスクの完全な制御は不可能であるとの認識に基づく

（注4）「手段に関する学問」としたが，手段を考える上での前提となるとなる周辺の学問も含むものとする

ＩＴリスク学の構成（Version3）



ITリスク学の確立に向けての活動

① 2008年5月に日本セキュリティ・マネジメント学会の中に「ＩＴリスク学」研究会を立ち上げ

② ITリスク学の定義

③ ITリスク学の全体像と構成要素の明確化

④ 構成要素の概要と研究課題の明確化

⑤ 研究課題の解決に向けての活動

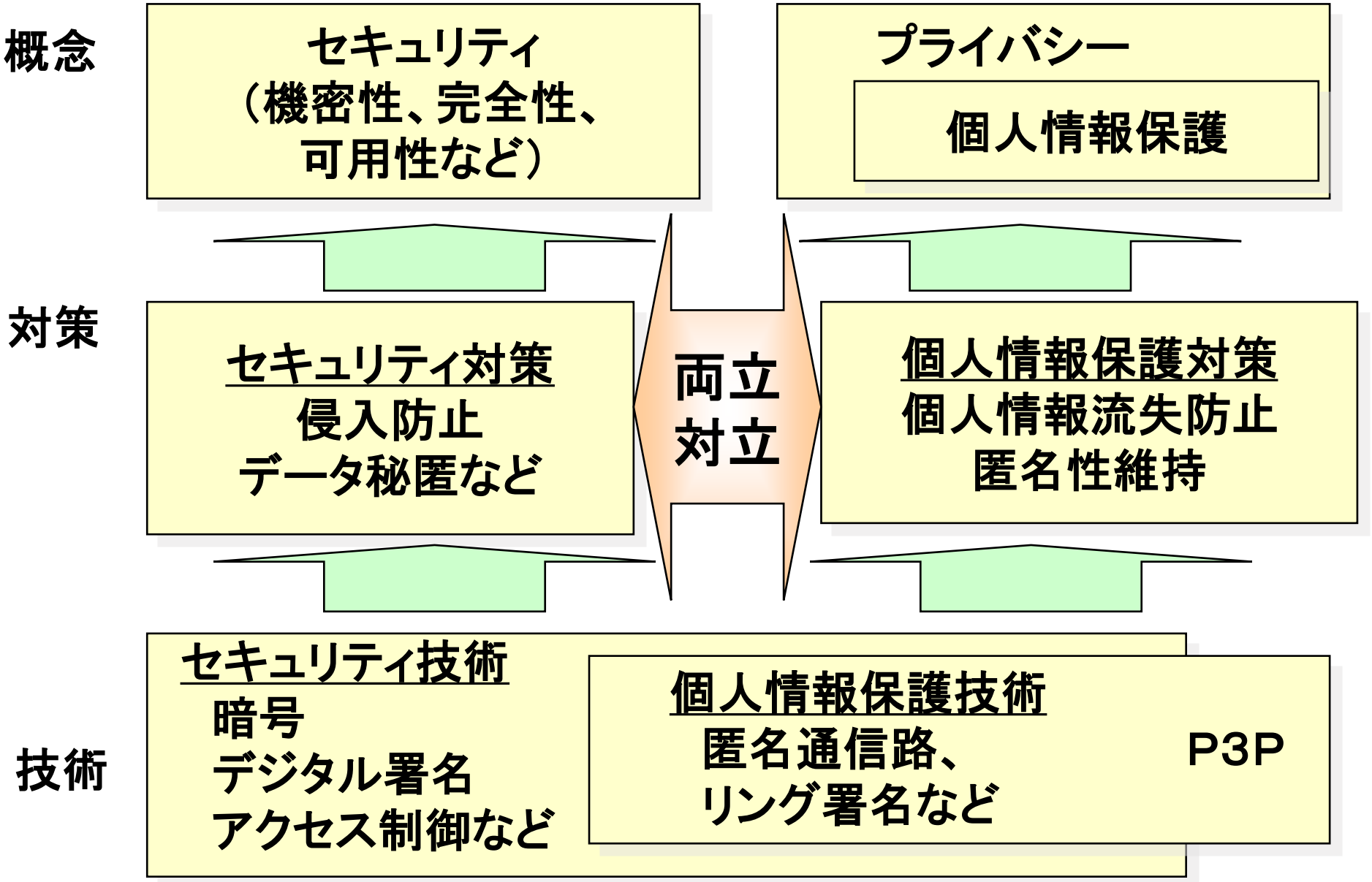
⑥ 本の出版（２０１３年1月）

代表的ITリスクの現状の調査

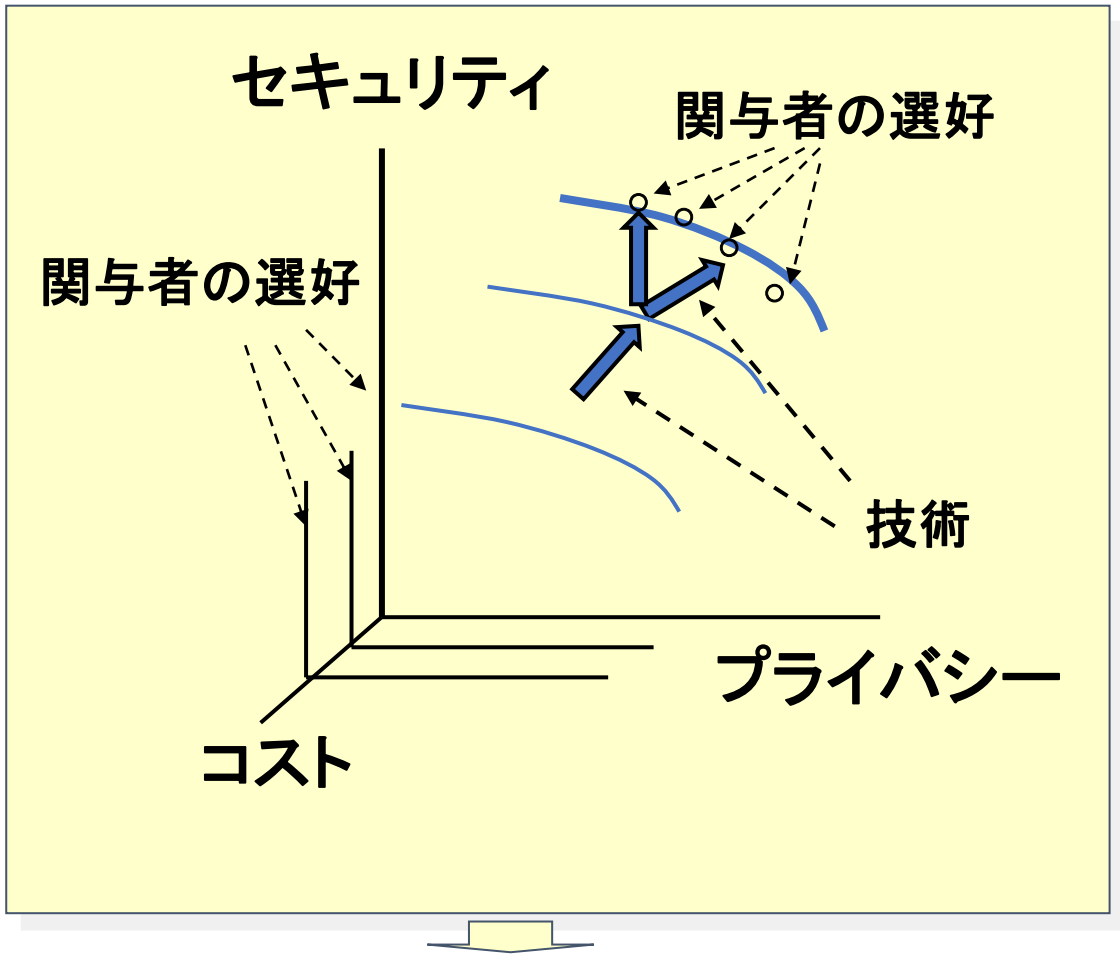
佐々木良一「ITリスクの考え方」岩波新書、2008年

佐々木良一編著 「ITリスク学」共立出版2013年

セキュリティとプライバシの関連



多重リスクへの対応法



多くの関与者が異なる選好を持つ
（リスクコミュニケーションが重要に）

技術による解決

＜例＞

公開鍵証明書の利用

属性証明書の利用など

多重リスクコミュニケータ（MRC）の対応

＜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、使い勝手など）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

専門家

対策案
①②③④

定式化結果

多重リスクコミュニケータ MRC

最適解
対策案
①③の組合せ

満足

Y

END

N

制約条件などの変更

ファシリテータ　関与者

組み合わせ最適化問題としての定式化結果

Minimization on: $\{損害額*(P_{\alpha 1}+P_{\alpha 2}+P_{\beta})+\sum_{i=1}^{8} Ci*Xi\}$

（トータルコスト）

Subject to $\sum_{i=1}^{8} C_i X_i \le Ct$ （対策コスト） 経営者向け

専門家が設定

$\sum_{i=1}^{8} D_{1i} X_i \le D_1$ （プライバシー負担度） 授業員向け

アンケートなど

$\sum_{i=1}^{8} D_{2i} X_i \le D_2$ （利便性負担度） 授業員向け

専門家や関与者が設定

$P_{\alpha 1}+P_{\alpha 2}+P_{\beta} \le Pt \quad (X_i = 0,1)$

（漏洩確率） 顧客向け

アタックツリー分析法などによりにより計算

リスクコミュニケーションの例

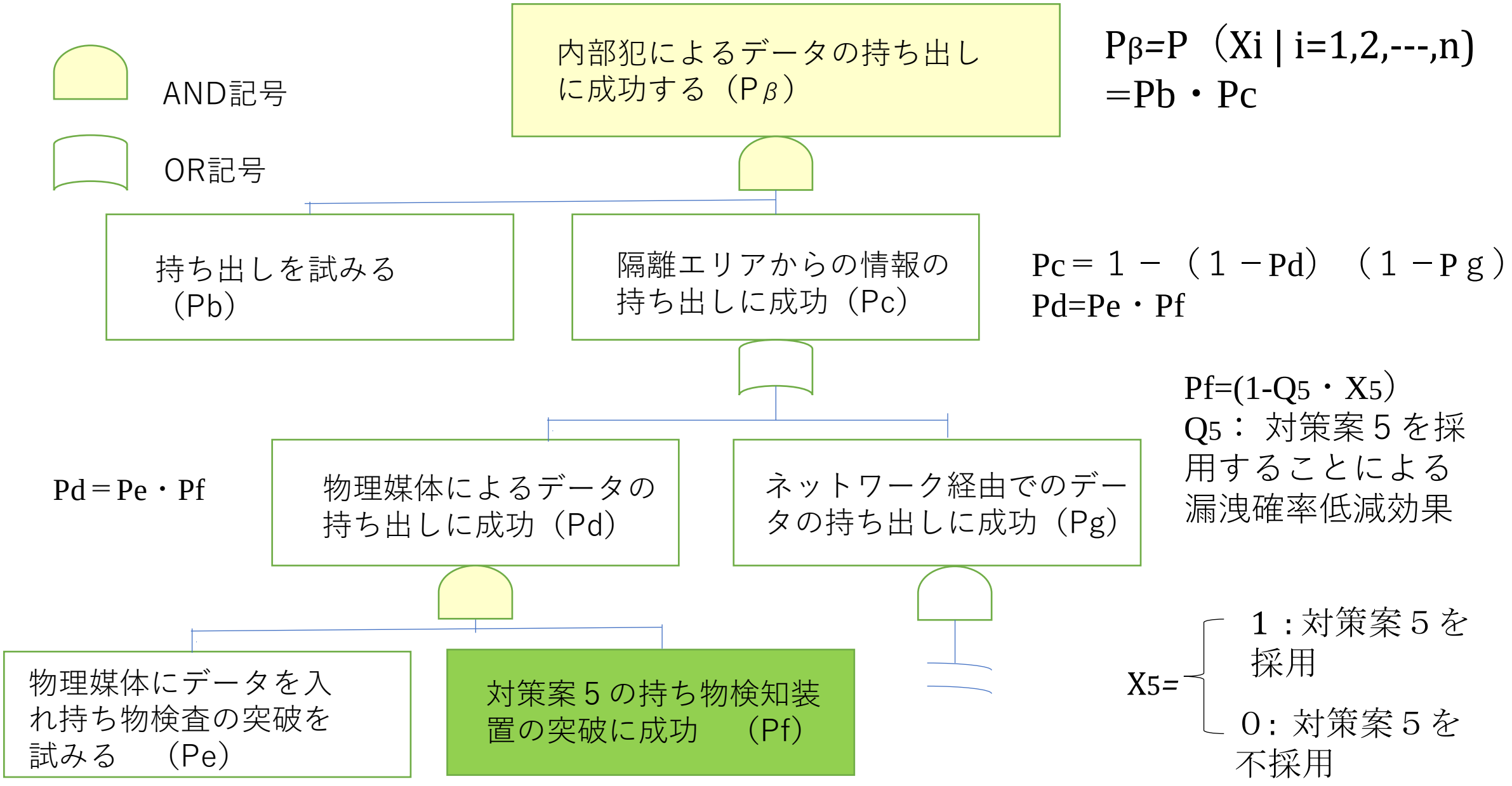
①もっと対策コストをかけてもよいのではないか

② 対策iは利便性負担度が大きく採用は絶対反対など

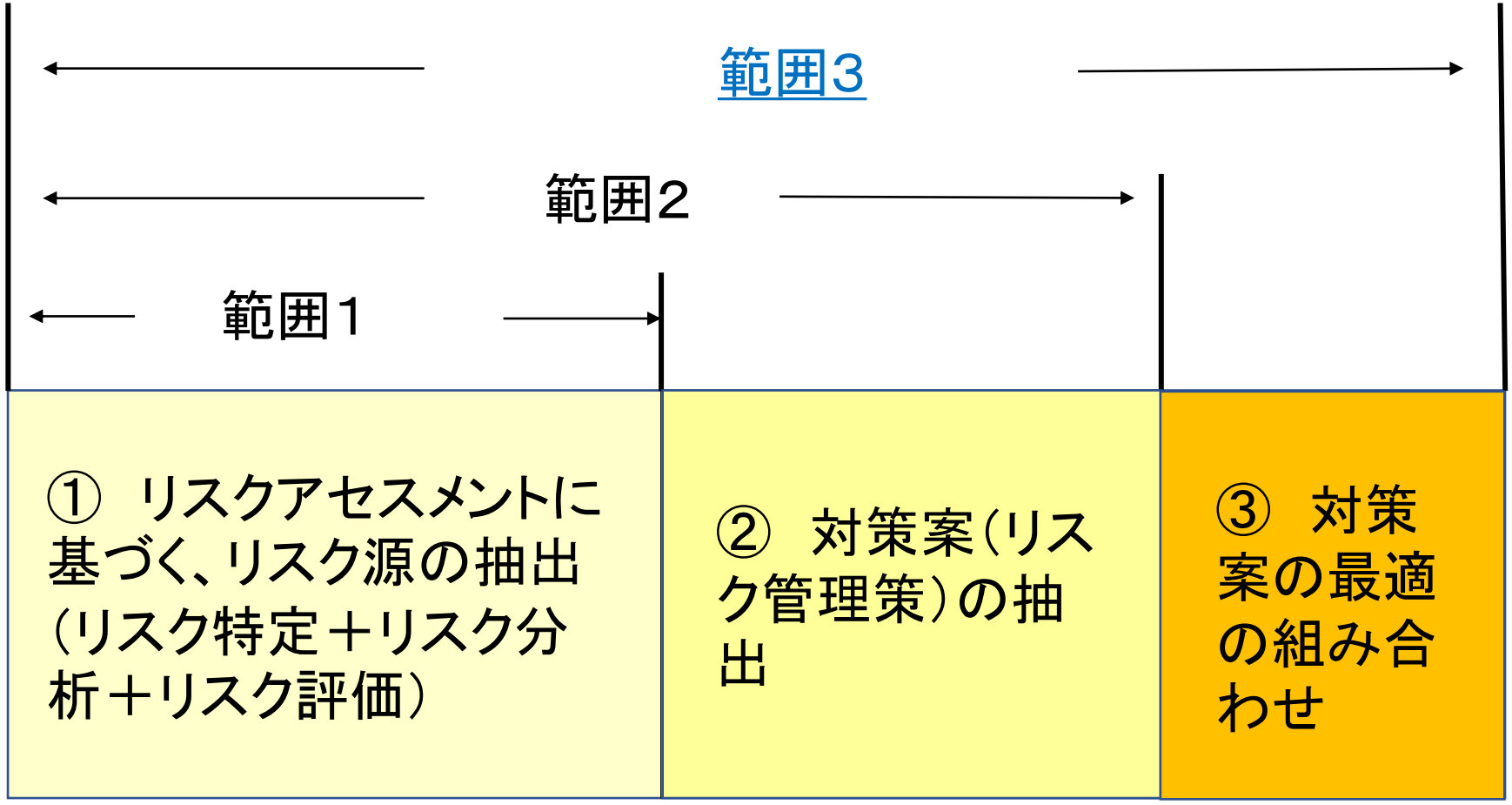
Xi＝１：対策案iを採用

Xi＝０：対策案iを不採用

解析に用いたアタックツリーの一例



リスクアセスメントが扱う範囲



リスクコミュニケーションが必要になった背景

＜リスク対応の困難性＞

（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.

（a）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。

①従って、人知を集める手段としてのリスクコミュニケーションが大切に（リスクコミュニケーションベースアプローチ）

（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.

（b）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

2つのタイプのリスクコミュニケーションの比較

	一般的リスクコミュニケーション	著者らのリスクコミュニケーション
目的	住民などに対象の安全性を理解してもらう	組織としてどういう対策をとるべきか、住民や従業員などの意見も入れて合意形成をする
主な研究課題	リスク認知 リスク心理学など	組み合わせ最適化法 合意形成法など
主な用途	社会的合意 個人の行動変容	（関係者の意見を反映した） 組織内合意
リスクアセスメントとの関係	通常なし	リスクアセスメントが主でその結果の組織内合意のためにリスクコミュニケーションを利用

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
（1）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
（1）この対策はそんなに効果はないと思う

多重リスクコミュニケータシリーズ

＜ リスクコミュニケーション法の展開＞

②1000人を超える関与者間の合意形成用
Social-MRC

＜ リスクアセスメント法の展開＞

⑤メタバースに適した準定量的リスクアセスメント法　MRC-QQ
⑥Attack byAIに適した定量・準定量結合型リスクアセスメント法　改良MRC-EDC

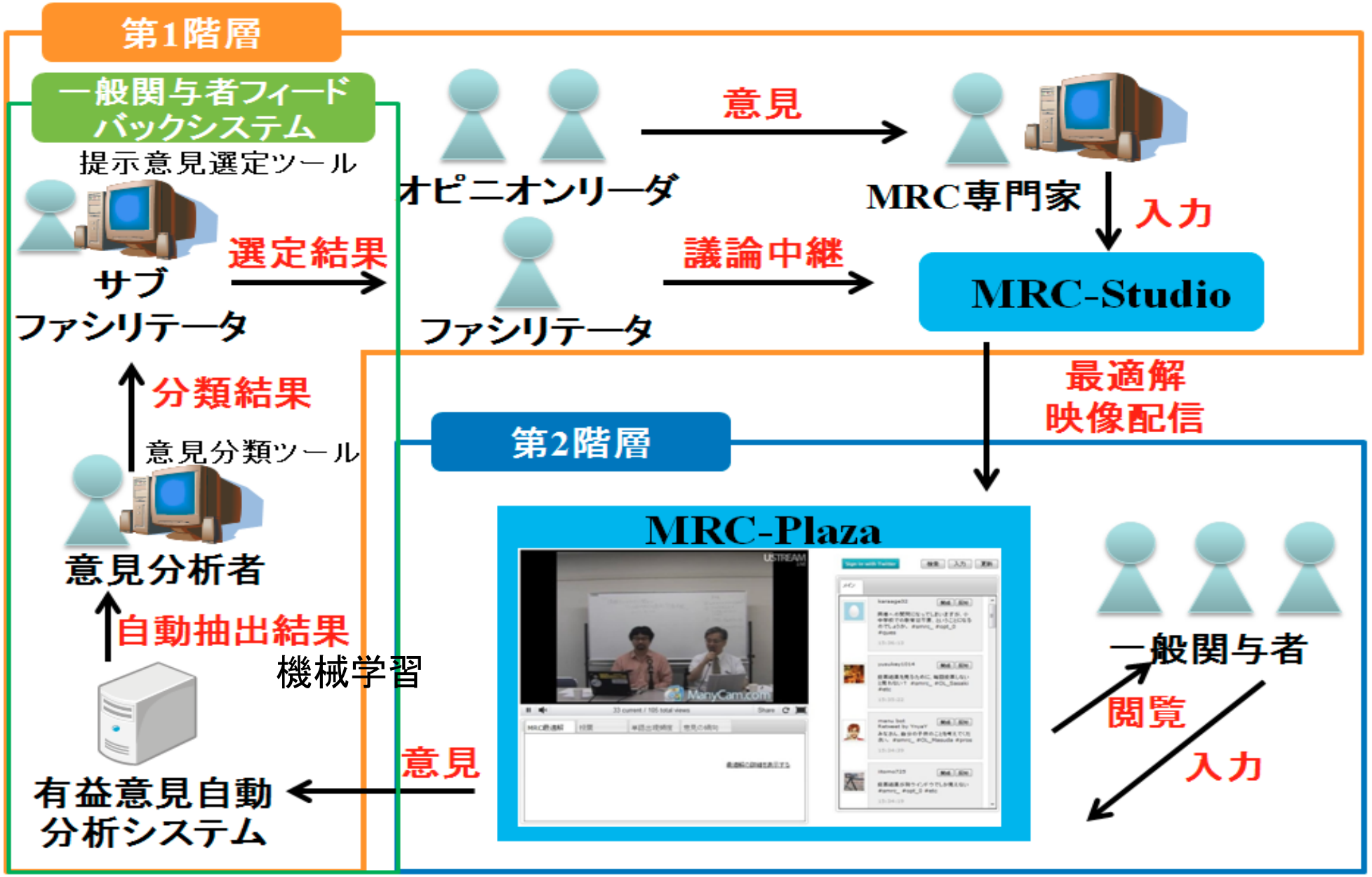
③多段階の攻撃に適したリスクアセスメント法
MRC-EDC

④フィードバックやリモートメンテナンス機能を持つIoTシステムに適したリスクアセスメント法
MRC-IoT

①基本的多重リスクコミュニケータ　Basic MRC
佐々木良一他「多重リスクコミュニケータの開発と適用」
情報処理学会論文誌第49号第９号pp3180-3190　2008

EDC method (Event Tree and Defense Tree Combined method)

Social-MRCの概要

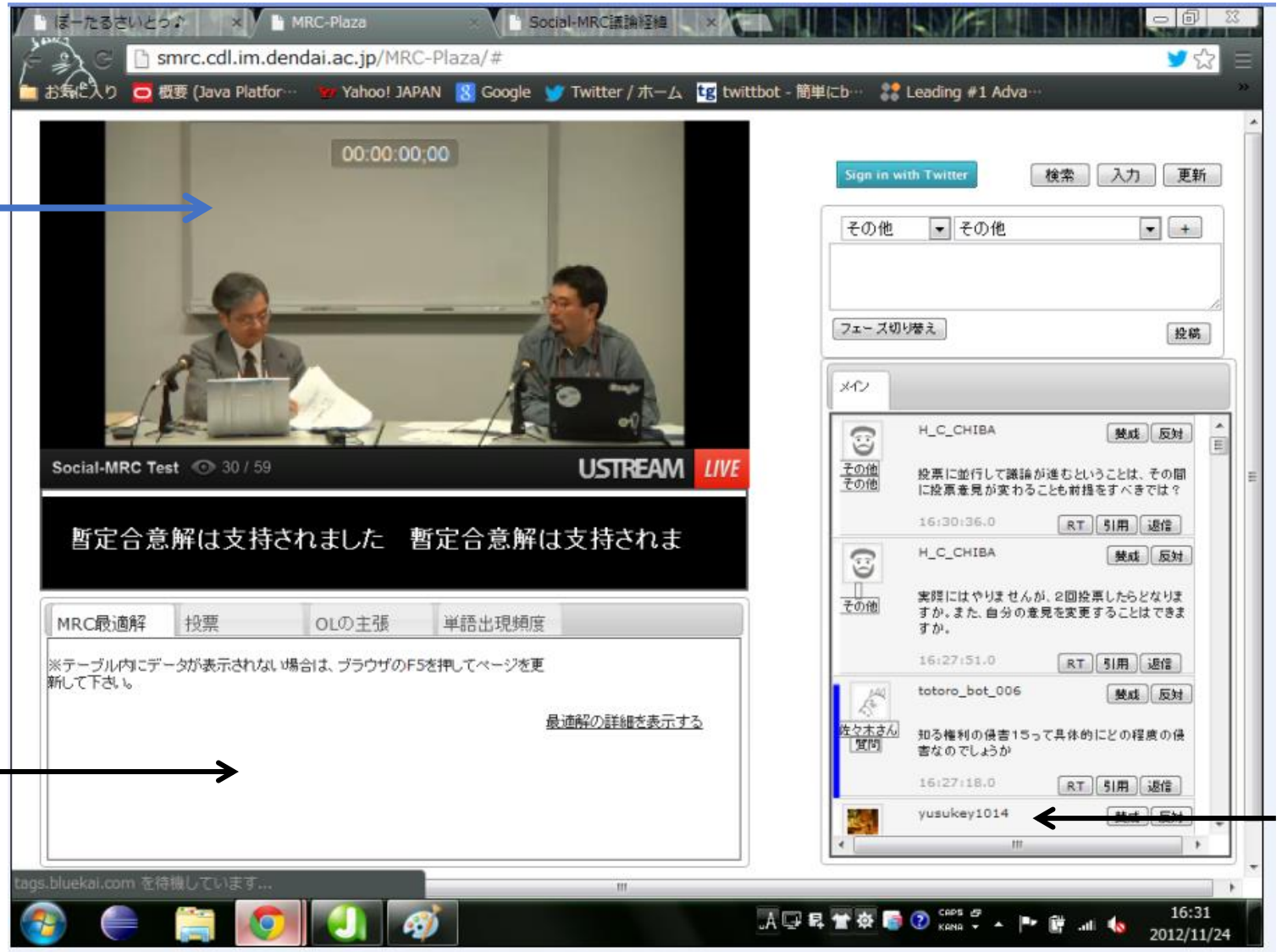


2階層アプローチ
① オピニオンリーダ
② 一般関与者

Social-MRCの出力画面の一例

Ustream表示部

Social-MRC固有部



Twitter用入力部

青少年への情報フィルタリング問題に適用

適用結果

（1）青少年への情報フィルタリング問題に適用

(2) 一般関与者の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

(3) 一般関与者の85%が最終解は合理的なものであると回答

佐々木良一他「ITリスク対策に関する社会的合意形成支援システムSocial-MRCの開発構想」情報処理学会論文誌
VOL.52,No.9、pp 2562-2574　2011

別テーマに力を入れたため中断したが、再開すべきテーマかもしれない

多重リスクコミュニケータシリーズ

＜ リスクコミュニケーション法の展開＞

②1000人を超える関与者間の合意形成用
Social-MRC

＜ リスクアセスメント法の展開＞

⑤メタバースに適した準定量的リスクアセスメント法　MRC-QQ
⑥Attack by AIに適した定量・準定量結合型リスクアセスメント法　改良MRC-EDC

③多段階の攻撃に適したリスクアセスメント法
MRC-EDC

④フィードバックやリモートメンテナンス機能を持つIoTシステムに適したリスクアセスメント法
MRC-IoT

①基本的多重リスクコミュニケータ
Basic MRC

2024年ITリスク学研究会リスクアセスメント試行WGを設置

目次

今後の対応

１．ITリスク学、特にリスクアセスメントやリスクコミュニケーションは、今後ますます重要になっていくと考えられる。

２．引き続き、リスクアセスメントやリスクコミュニケーションを中心に研究を続けていきたい。

３．特に、Attack by Generative AI　のリスクアセスメント、リスクコミュニケーションについては注力したい。


END

質問など

講演について
---
①セキュリティ・クリアランス制度がまだない日本では、
　内部犯行・内部不正対策として、どのような対策が考えられるでしょうか?
②ITに詳しくない人でも、特権管理者の方による不正に気付くことが
　できるようにするには、どうするのが現実的で・効果的でしょうか。

パネルディスカッションについて
---
①ランサムウェア対策の観点からもご議論いただけるとありがたいです。
②技術対策だけで内部不正を防ぐことは、なかなか難しいと最近良く感じます。
　ベスプラがある訳ではないと思いますが、技術対策以外でどの様な対策が
　考えられるのでしょうか。また、技術対策をガチガチにしてしまうと、
　利用者が端末出来る事が限られてしまって心情的にも業務的にも
　モチベーション低下（特に開発者や技術者）に繋がる様に感じます。
　セキュリティと利便性のバランス感覚についてもお話が聞けると嬉しいです。

セキュリティクリアランス

セキュリティ・クリアランスとは、安全保障などに関わる機密情報にアクセスできる資格者を政府が認定する制度です。この制度は人を対象とする場合と施設を対象とする場合があります。この記事では人を対象にするセキュリティ・クリアランスについて、解説します。人を対象にするセキュリティ・クリアランスは、機密情報にアクセスできる人を限定することで、その情報の漏洩を防ぐことが主な目的とされています。

セキュリティ・クリアランスは
1. 情報指定：政府が保有する安全保障上重要な情報の指定
2. 政府の調査によるセキュリティ・クリアランスの付与：該当の情報にアクセスする必要性がある人の信頼性確認
3. 情報漏えい時の厳罰を含む特別の情報管理ルール：万が一セキュリティ・クリアランス保持者から情報が漏洩した際の厳罰を含むルール

の3つの機能がセットになっています。

https://www.trendmicro.com/ja_jp/jp-security/23/d/securitytrend-20230410-01.html

内部不正対策

適切な内部統制の確立：組織内での権限と責任を明確にし、職務分掌や二重管理を防止するための仕組みを整える。

監査と検査：内部監査を通じて業務プロセスや取引の透明性を確保し、不正や違反を発見する仕組みを構築する。

教育と啓発：従業員に対して倫理観やコンプライアンスの重要性を啓発し、不正行為を防止する文化を醸成する。

報告と通報システム：不正や違反を発見した場合に匿名で報告できる仕組みを整え、適切な対応を行う。

アクセス制御とセキュリティ：情報システムや資産へのアクセスを制限し、不正行為や情報漏洩を防止するための対策を講じる。

ChatGPT

特権管理者の不正の発見・防止

1.ログの監視と分析：特権管理者が行った操作のログを監視し、不審なアクティビティを検出するためのツールを使用します。異常なパターンや頻度の高い変更などに注意を払います。
2.アクセス権の適切な管理：特権管理者に与えられる権限は最小限に留め、業務に必要な範囲内でのみ権限を付与します。また、権限の付与や変更には、複数人の承認が必要となるようにします。
3.セグリゲーション（分離）：特権管理者には、通常のユーザーとは別のアカウントを使用させ、通常の業務と特権操作を分離します。これにより、不正行為を隠すのが難しくなります。
4.異常検知システムの導入：異常検知システムを導入し、通常のパターンから外れたアクティビティを検出します。特に、特権管理者のアカウントでの異常な操作を検知することが重要です。
5.教育と啓発：組織全体での情報セキュリティに関する教育を行い、特権管理者も含めた全ての従業員がセキュリティ意識を高めるよう努めます。

ランサムウエア

ランサムウェア（Ransomware）とはマルウェアの一種である。これに感染したコンピュータはシステムへのアクセスを制限される。この制限を解除するため、マルウェアの作者へ身代金の支払いが要求される。

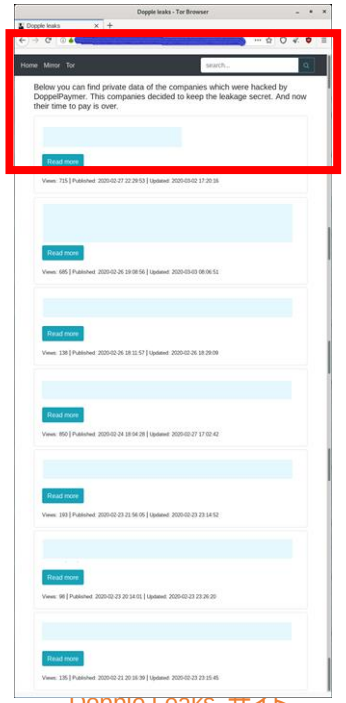
＜手順＞

① 攻撃者がマルウエアを仕掛ける
② 利用者のPCやサーバが感染し、データなどが暗号化
③ 利用者は業務が不可能に
④ 攻撃者は身代金を要求
⑤ ビットコインなどで身代金を支払うとデータなどが復元

＜データの暗号化という意味では完全性の喪失
データを使えないという意味では可用性の喪失＞

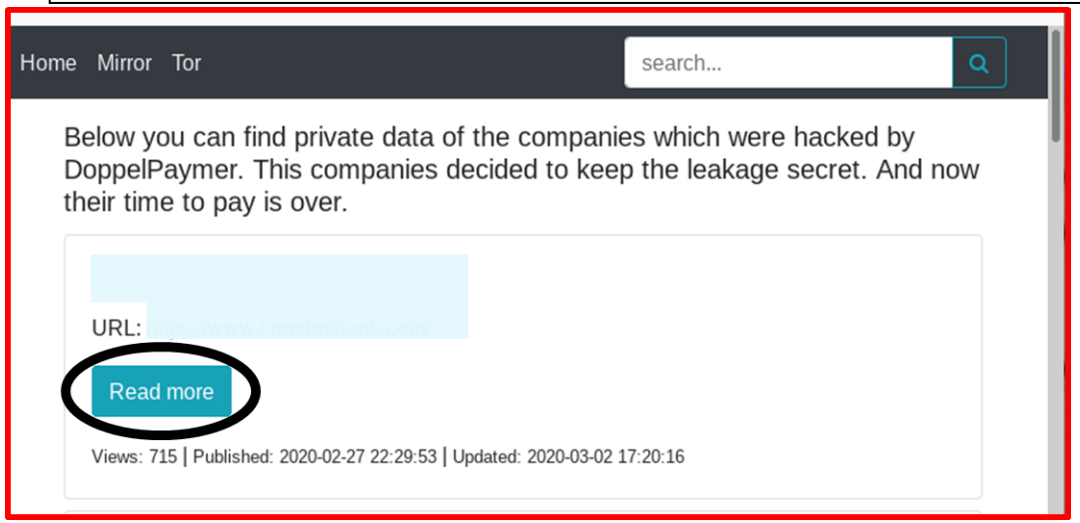
最近のランサムウエア

① 標的型化（目的とする特定少数の組織への攻撃）
② 2重脅迫型化（暗号化による業務妨害＋データ公開）



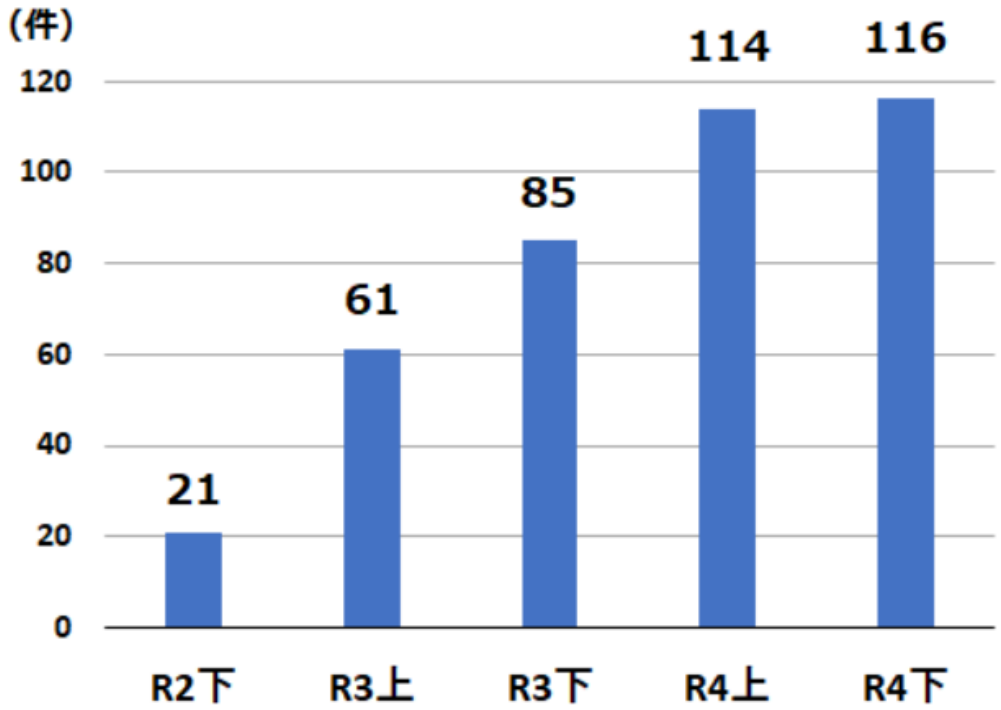
Dopple Leaks サイト
(3/6現在)

Dopple Leaks
DoppelPaymer Ransomwareで盗み出した情報を公開することで、身代金支払いを促す効果がある



類似のものに「Maze」、「DarkSide」などがある。

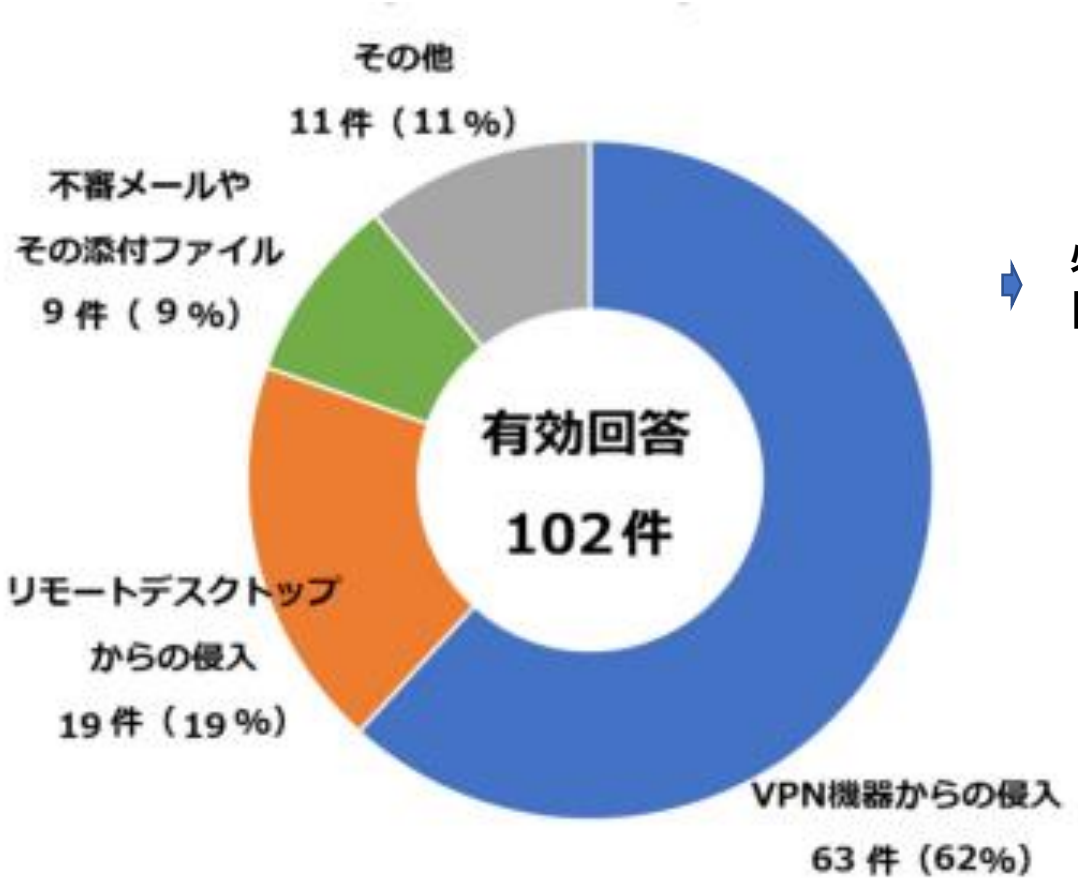
ランサムウエア被害報告件数



アンケート結果（R4下）
① 2重脅迫が65%
② 暗号資産による支払い要求が93%
③ 復旧に多大な時間が

「令和４年におけるサイバー空間をめぐる脅威の情勢等について」（警察庁）（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf）を加工して作成

感染経路



必要な対策：VPNソフトのバージョンアップ

VPN: Virtual Private Network
通信路暗号を実現するための一手段

「令和４年におけるサイバー空間をめぐる脅威の情勢等について」（警察庁）（https://www.npa.go.jp/publications/statistics/cybersecurity/data/R04_cyber_jousei.pdf）を加工して作成

ランサムウェアの被害を防ぐために必須の対策

＜感染防止対策＞

（１）　OSやソフトの脆弱性を修正する

（２）　メールのリンクや添付ファイルを安易に開かない

（３）　セキュリティソフトを最新の状態で利用する

＜データ復旧準備対策＞

（１）　こまめにバックアップする

＜できればネットワークから切り離した保管も＞

ランサムウエアへの対応法

＜データ復元法＞

1．バックアップやクラウドストレージから戻す方法

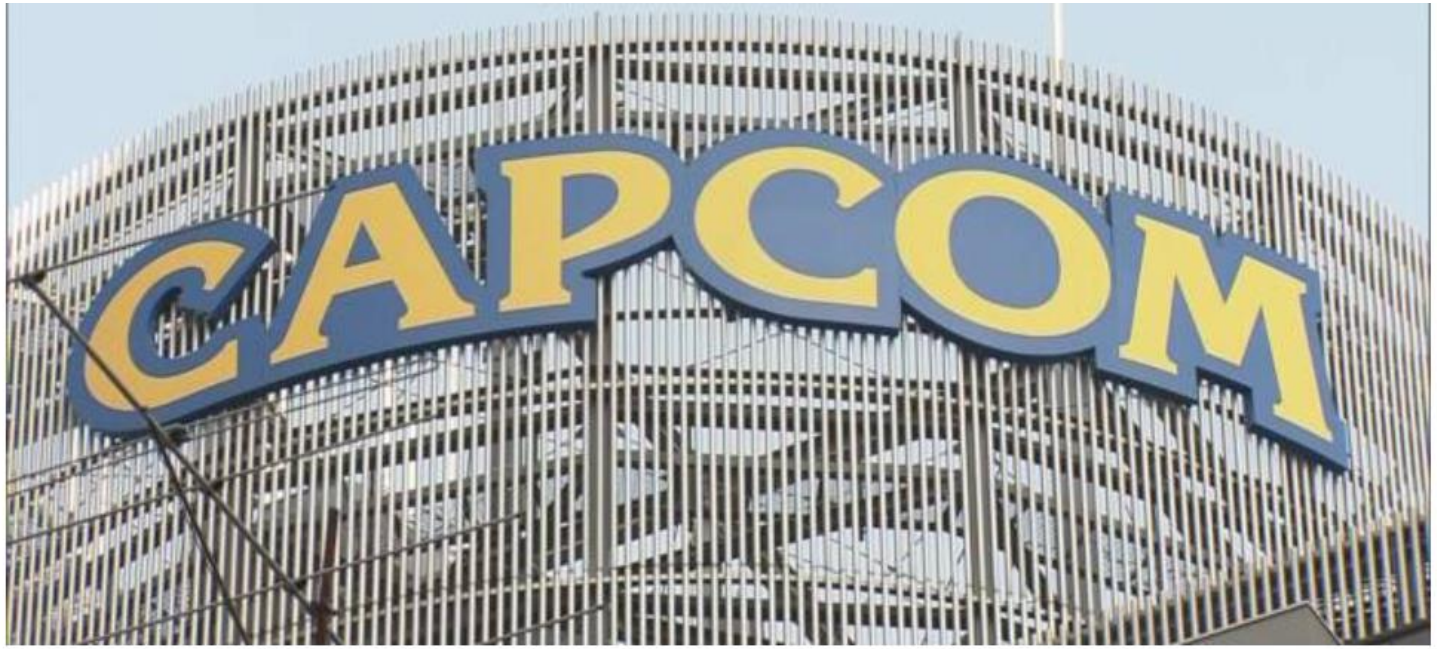
2．ボリュームシャドウコピーで復元させる方法

3．削除ファイルの復元ツールを使う方法

平文を暗号化した後、平文フアイルを単純消去するだけなら復元ツールで復元可能（単純消去だけの可能性は低い）

4．メモリー上のデータのダンプをとることによる暗号かぎの取り出し（可能性は低い）

ランサムウエアの被害



カプコン サイバー攻撃 金銭要求の「ランサムウェア」

2020年11月12日 18時19分　IT・ネット

1100万ドル（11億円ほど）の身代金を支払うように要求

https://www3.nhk.or.jp/news/html/20201112/k10012708311000.html

支払いを容認する考え方

- 支払いは最も費用のかからない選択である
- 支払いは利害関係者の最善の利益になる（例えば、即時の手術を切実に必要としている入院患者）
- 支払いにより、重要なデータを失ったことによる罰金を回避できる
- 支払いは、機密性の高い情報を失わないことを意味する
- 支払いは、データ侵害で公開されないことを意味する場合がある

ブルースシュナイアーのブログ
https://www.schneier.com/blog/archives/2020/09/negotiating-with-ransomware-gangs.html

支払いに否定的な考え方

- 支払いは、復号のためのキーが提供されることを保証するものではない
- 支払いは、攻撃者に資金を提供し、さらなる攻撃を可能としてランサムウェア犯罪サイクルを維持する
- 支払いは、企業ブランドの毀損に繋がる可能性がある
- 支払いによって、攻撃者による次なる攻撃を防げない
- 被害者がランサムウェアの支払わなかったら、攻撃者は別の手法を使わざるを得なくなる
- ビットコインによる支払いは、組織を別の危険に晒す可能性がある。ほとんどの被害者は、ハッキングされる可能性のある取引所でビットコインを購入する必要があり、これらの取引所に保存されている購入者の銀行口座情報は脆弱なままだからである

ブルースシュナイアーのブログ
https://www.schneier.com/blog/archives/2020/09/negotiating-with-ransomware-gangs.html

米国の対応状況

1．米国ではサイバー保険で身代金を支払っている例も
　　＝＞逆に保険に入っている企業は、攻撃を受けやすいという説も

2．FBIなどは、身代金を払ってもよいので情報を流してほしいというポジションか

3．身代金の支払いを禁止すべきであるという意見も
　フロリダ州などでは州法で、州立病院などの組織が身代金を払うのを禁止

主な調査結果(2022年度)

項目	日本	世界
①　ランサムウエアの被害を受けた企業の割合	61%　（前年は１５％）	６６％
②　暗号化された割合	６９％　（前年は４７％）	６５％
③　何らかのデータデータを復元	９５％	９９％
④　身代金支払い	５０％	４６％
⑤　身代金による復元	５４％	６５％
⑥　身代金平均額	４３３万ドル	81万ドル

ソフォス ホワイトペーパー2022年 4月より
ソフォスが調査会社 Vanson Bourne 社に委託して実施
世界31か国の中規模組織（従業員数100-5000人） 2021年対象

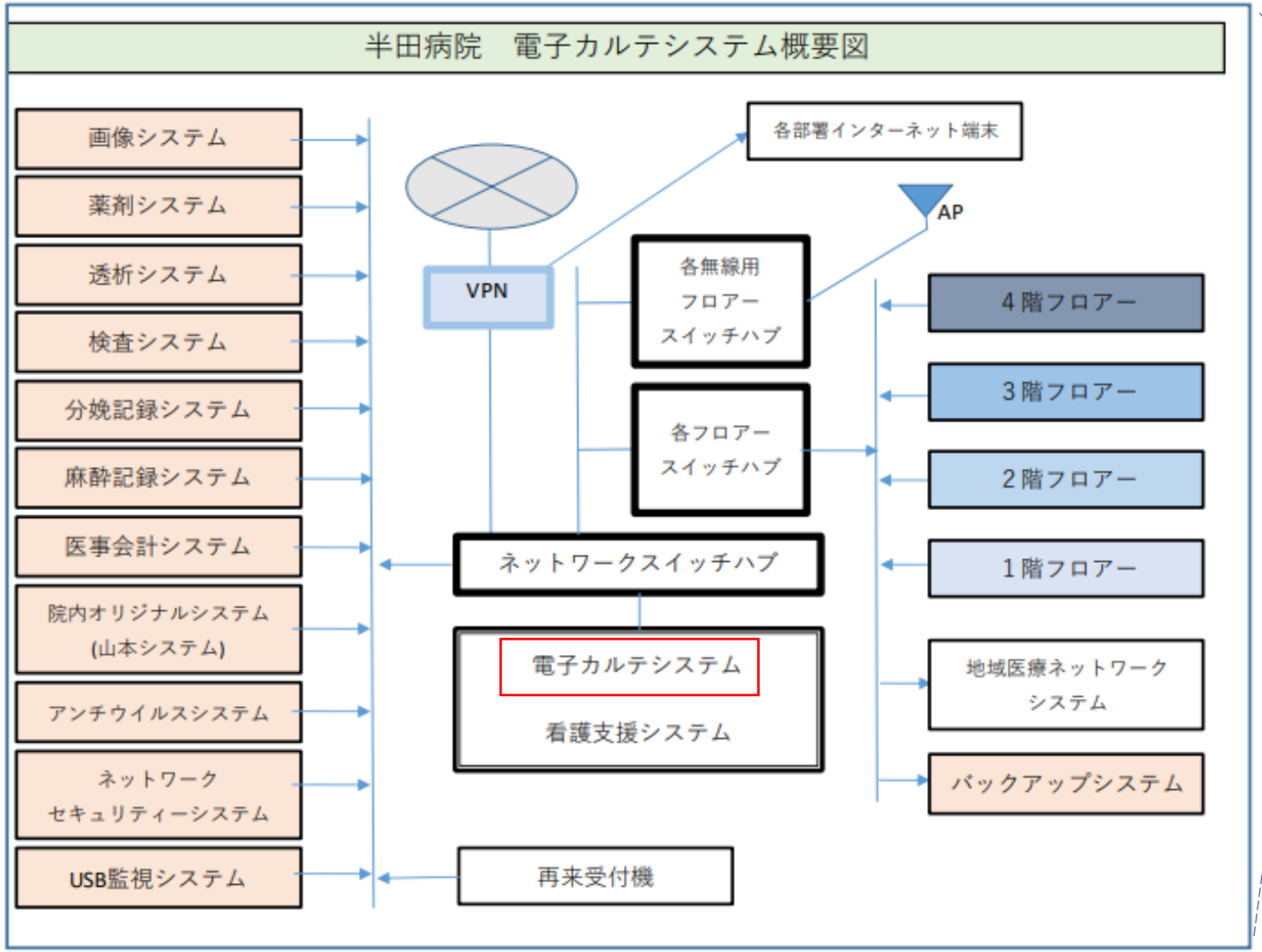
トレンドマイクロの調査結果では身代金の支払い比率は
世界41.7%に対し日本11.4%

徳島の半田病院事案概要 1

- 令和 3 年 10 月 31 日未明、病院内に設置されていた複数台のプリンタが、一斉に犯行声明を印字し始めた ことでインシデントが発覚した。
- Lockbit2.0 によるランサムウェア（身代金要求型ウイルス）に感染し、患 者の診察記録を預かる電子カルテなどの端末や関連するサーバーのデータが暗号化され、データが使用でき ない甚大な被害が生じた。
- 侵入経路としては導入している仮想プライベートネットワーク（Virtual Private Network、以下、「VPN」という。）装置の脆弱性を悪用して侵入したものと思われる。

https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf

病院のシステム構成



全体はHIS（Hospital Information System）ともいう

https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf

徳島の半田病院事案概要 2

- 全容解明や情報漏えい有無の特定よりも、病院としての機能を一日も早く取り戻すために、患者のデータ をいかに復元させるか、端末を利用できる状況に戻すかに焦点を当てインシデント対応を行っていた。
- 病院側は身代金要求に応じない方針。
- 幸い にして、フォレンジックを請け負った事業者が、（データを確認できる範囲で）元の通り復元をすることが できたと考えられる。その後、端末の初期化対応を行い、端末を再利用したり、システムやネットワークを 最低限見直したりした上で、令和 4 年 1 月 4 日の通常診療の再開にこぎつけることができた。

https://www.handa-hospital.jp/topics/2022/0616/report_01.pdf

RAASサイトのテイクダウン法

- 情報収集：まず、RaaSサイトのホスティング情報やドメイン情報、運営者の情報などを収集します。WHOISデータベースやウェブホスティングサービスの情報などを利用します。
- 法的手段の検討：収集した情報を元に、違法な活動を行っているRaaSサイトに対して法的手段を検討します。著作権侵害やサイト利用規約違反などの違反行為があれば、これを根拠にしてテイクダウンを要求することができます。
- ホスティングサービスへの報告：RaaSサイトが利用しているホスティングサービスに対して、違法な活動を行っているサイトであることを報告し、テイクダウンを要求します。ホスティングサービスは、違法な活動を行っているサイトをホスティングすることに対して法的責任を負う可能性があるため、要求が受け入れられることがあります。
- ドメインレジストラへの報告：RaaSサイトのドメインを管理しているドメインレジストラに対して、違法な活動を行っているサイトであることを報告し、ドメインの停止を要求します。ドメインレジストラも、違法な活動を行っているサイトをドメイン登録することに対して法的責任を負う可能性があるため、要求が受け入れられることがあります。
- 協力機関や専門家の支援：RaaSサイトのテイクダウンには専門知識が必要な場合があります。情報セキュリティ機関や法律専門家などの支援を受けることで、効果的なテイクダウンを行うことができます。