修士論文等審査会
【特定課題研究】

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

業務の電子化におけるガイドワードを利用したリスク特定手法の提案

2023/2/18

後藤研究室
博士前期課程1年（1年制）
5524701 稲田 陽一

概要

■ 取り組んだ課題

- 企業での業務電子化において，「リスクおよび情報システムの非専門家」によるリスク特定が行われているが，網羅性に欠けるため運用段階において想定しないリスクが顕在化している

■ 成果

- リスクおよび情報システムの非専門家でも実施できるリスク特定手法を提案した
- 提案手法をツール化し，非専門家が実際に利用できるようにした
- 従来手法およびリスク専門家によるリスク特定との比較を実施し，提案手法の検証を行った
- 検証の結果，従来手法と比してリスク特定の網羅性向上が示唆された

目次

①業務の電子化におけるリスク特定の課題

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

【網羅性の欠如】
• 業務所管部署の役職員が実施
→知識や体系的な特定手法の不在

【本提案が想定する業務の電子化の例】

- 対象業務例：
  社内研修への対象者アサイン
- 企画者：
  社内での当該業務所管部署の要員
- 予算/プロセス：
  部内or本部内で完結
- 利用ツール：
  RPAなど

※業務所管部署：組織において業務を担い，その業務を所管する部署
※リスク特定：ハザードおよびそれによって引き起こされる望ましくない動作の特定
※ハザード：望ましくない動作を引き起こしうる現象

②先行研究

① 非専門家によるリスク特定に関する先行研究

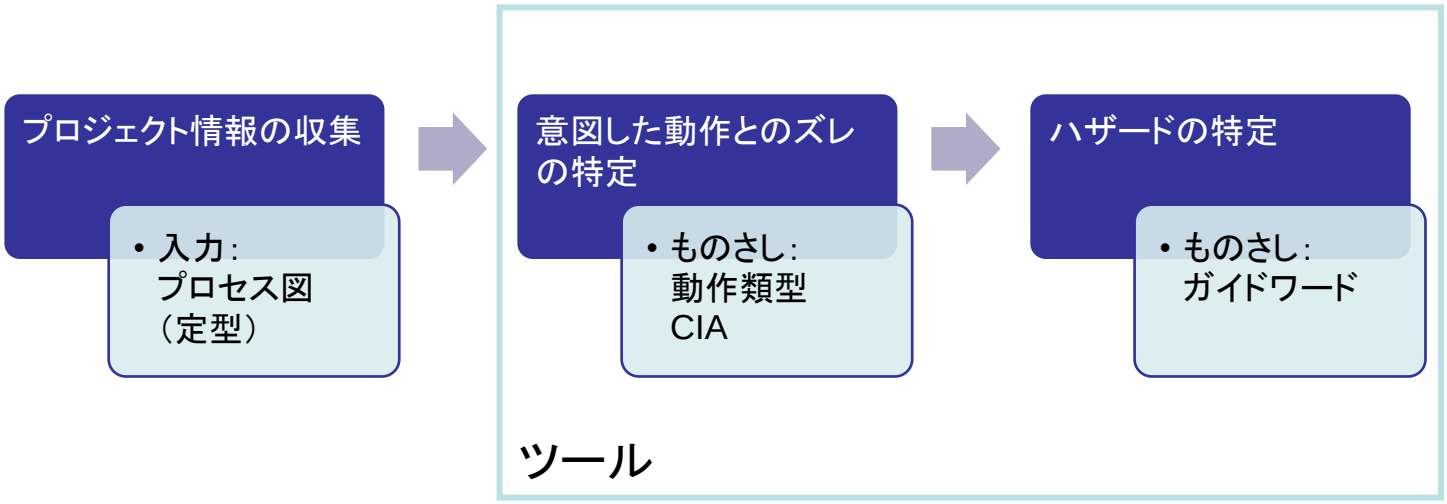
- 特定の軸（ものさし）が必要（土井ほか）
- 自動化（ツール化）が必要（宍戸ほか）

② 網羅的なリスク特定に関する先行研究

- 既存電子化プロセスに適用可能であること
  →プロセス図を利用し相互作用に対し意図した動作とのズレを特定（Catmurほか）
- 網羅的なリスク特定であること
  →ガイドワードを利用したハザード特定（Wintherほか）

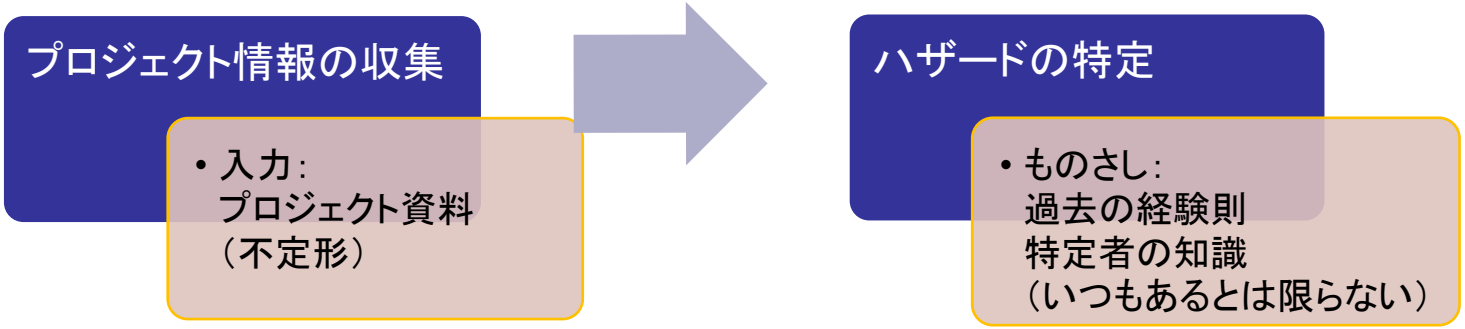
③提案手法の概要

■ 提案手法



定型のインプット
定型のものさし
→ブレないリスク特定

■ 従来手法

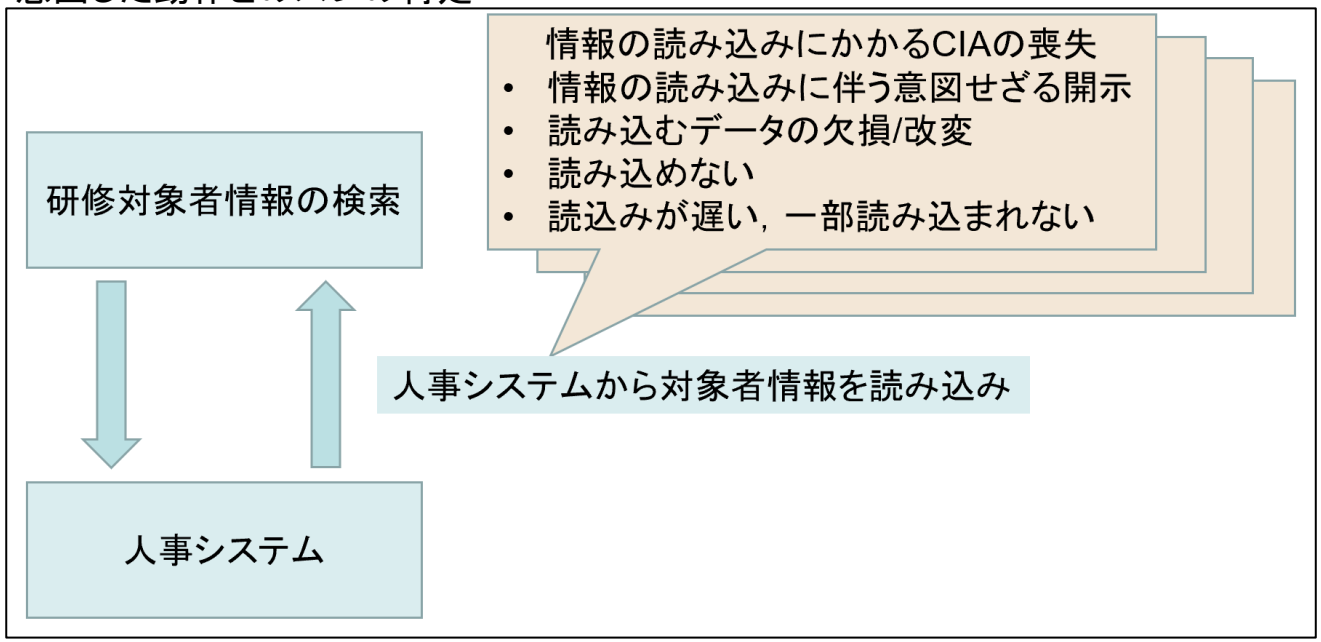


不定形のインプット
不定形のものさし
→網羅性のブレ

③意図した動作とのズレの特定

- 動作種別ごとの機密性/完全性/可用性の喪失

意図した動作とのズレの特定



動作の類型

動作の類型	定義
読み込み	既存ファイルに変更を加えず，その内容を読み取ること
書き込み	既存ファイルに編集を行うこと
作成	新たにファイルを作成すること
保存	書き込みを行ったファイルを保存し，更新すること
制御	対象システム以外のシステムを動作せしめること
移動	既存ファイルを元の場所から別の場所に移動すること
削除	既存ファイルを削除すること

③意図した動作とのズレを引き起こすハザードの特定

- Wintherらの先行研究で編み出されたガイドワードの利用

ハザードの特定

- 特定したズレ
  - 情報の読み込みに伴う意図せざる開示
- ガイドワード

情報の読み込みにおける漏洩のガイドワード

Post-Guideword（要因）	Attribute（手段）
Insider（内部者） Outsider（外部者） Technical Failure（技術的故障） Configuration fault（設定ミス） Social manipulation（ソーシャルエンジニアリング）	暴露 操作 切断 偽造
…	
…	
…	
…	

- 特定されたハザード
  - 内部者による暴露

③意図した動作とのズレを引き起こすハザードの特定

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- Wintherらの先行研究で編み出されたガイドワードの利用

Pre-Guideword	Attribute（手段）		Post-Guideword（要因）
意図的に 意図せずして	Disclosure（暴露） Manipulation（操作） Disconnection（切断） Fabrication（偽造） Delay（遅延） Corruption（欠落） Deletion（消去） Removal（持ち去り） Stopping（停止） Destabilization（不安定化） Capacity Reduction（許容量の減少） Destruction（破壊） Denial（拒否）	動作を受ける対象	Insider（内部者） Outsider（外部者） Technical failure（技術的故障） Virus（マルウェア） Ignorance（無知） Fire（火災） Faulty Auxiliary Equipment（予備機器の故障） Sabotage（怠業） Broken cable（ケーブル故障） Logical problems（ロジック問題） Logical attack（論理攻撃） Planned work（計画作業） Configuration fault（設定ミス） Spamming（スパム） Social manipulation（ソーシャルエンジニアリング）

Winther他より作成

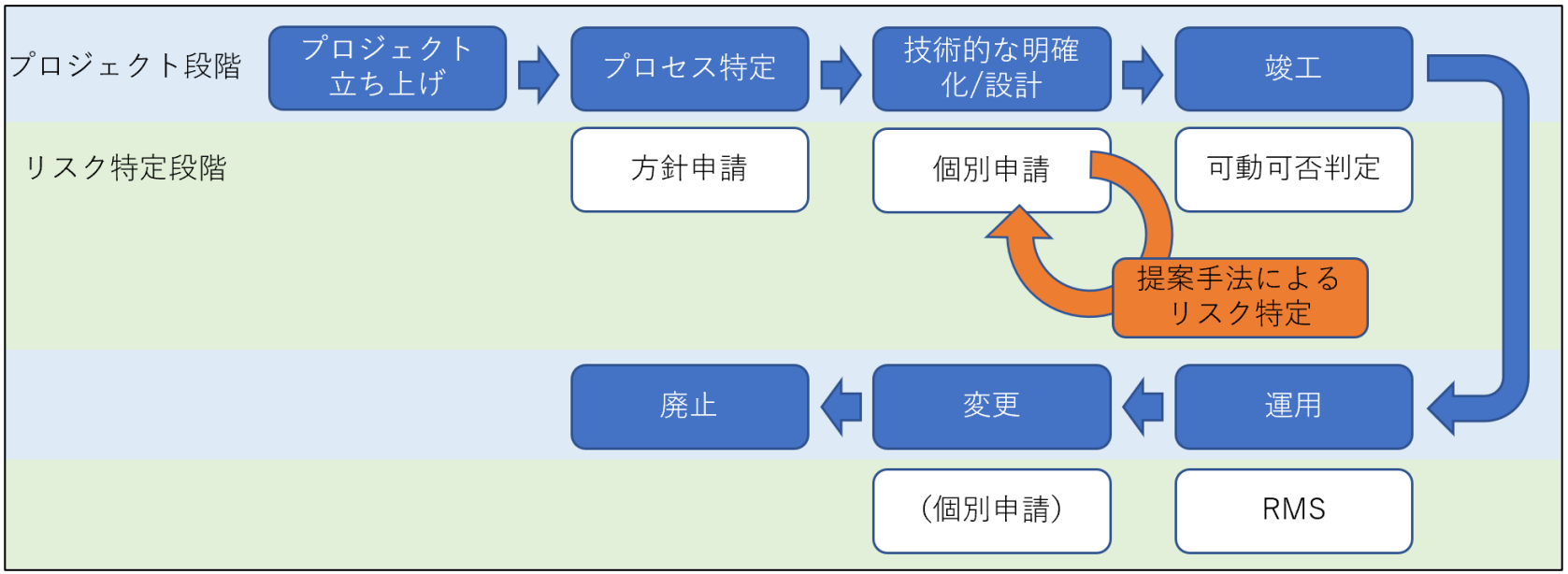
③ハザード候補の絞り込み

- **他と重複するハザードの排除**
  （例：火災による持ち去り→持去主体は内部者/外部者のため重複）
  AttributeとPost-Guidewordの組み合わせ195種→163種
- **当該の動作で発生し得ないハザードを排除**
  （例：削除した情報の消去→意図した動作とのズレではない）
  19意図した動作とのズレ×163ハザード=3097種→2476種
- **ハザード発生を抑止する要因によるハザード候補の排除**
  （例：予備機器がない→予備機器に起因するハザードの除外）
  システム構成や要件上発生し得ないハザードの除外
- **システム重要度に応じた特定ハザードの絞り込み**
  機密性/完全性/可用性への対策有無に応じたハザード候補の絞り込み
  - ◆システムが停止した場合の代替手段の有無，データバックアップの有無，扱う情報の重要性
    →デフォルトの重要度「3」
    →代替手段orデータバックアップが存在→重要度「-1」
    →扱う情報が公開情報or社外秘→重要度「-1」

③実施フェーズと実施者

■ 提案手法の実施フェーズ

システム要件がある程度明確&竣工前である「設計」段階で実施



モデル企業での申請プロセスにおける本提案手法の実施タイミング

■ 実施者

- 電子化企画部署(業務所管部署)の役職員

④提案手法のツール化

- Excelツールにて実装
  - 事前質問シートに「システムが有する動作」,「ハザード抑止要因の有無」,「システムの重要性」を入力.
    - ◆ハザード抑止要因の有無
      →存在しない動作に起因するハザードを除外
      →システム構成や要件上発生し得ないハザードの除外
      （e.g.予備機器がない→予備機器に起因するハザードの除外）
  - システムにおいて起こり得る「意図した動作とのズレ」およびハザードの表示

④提案手法の実装−画面イメージ①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 事前質問シート

A1

	A	B
1		↓この列に入力（当てはまる場合は1，当てはまらない場合は0）
2	**機器構成に関する質問**	**当否**
3	内部者が操作できない	0
4	外部からアクセスできない	1
5	予備機器が存在しない	1
6	内部者による設定変更ができない	1
7	外部者が設置個所に立ち入りできない	1
8	物理筐体が存在しない	1
9	メールを利用しない	0
10	内部者と外部者がデータ量を制御できない	1
11	バックアップが行われている	1
12	データの抽出ができない&データの送信が制限されている	0
13	内部者による停止が制限されている	1
16	**動作種別に係る質問**	**当否**
17	読込みに当たる動作が存在するか	1
18	書込みに当たる動作が存在するか	1
19	作成に当たる動作が存在するか	1
20	保存に当たる動作が存在するか	1
21	制御に当たる動作が存在するか	0
22	移動に当たる動作が存在するか	0
23	削除に当たる動作が存在するか	1
25	**システム重要度に関する質問**	**選択**
26	システムが停止した際に代替手段が存在するか	存在する
27	扱う情報の情報区分は何か	社外秘
31		

1 ページ　2 ページ

④提案手法の実装-画面イメージ②

■ 意図した動作とのズレ一覧シート

L16

	C	D	E
1	システムにおいて考えられるリスクの一覧		
2	動作	考えられるリスク	ハザードの件数
3	読込み	情報の読込みに伴う意図せざる開示	27
4		読み込むデータの欠損/改変	132
5		読み込めない	111
6		読み込みが遅い/一部読み込まれない	105
7	書込み	情報の書込みに伴う意図せざる開示	27
8		書き込まれたデータの欠損/改変	132
9		書き込めない	111
10		書き込みが遅い/一部書き込まれない	105
11	作成	作成物の意図せざる開示	27
12		作成されたデータの欠損/改変	132
13		作成されない	111
14		作成が遅い/一部作成されない	105
15	保存	保存した情報の意図せざる開示	27
16		保存したデータの欠損/改変	132
17		保存されない	111
18		保存が遅い/一部保存されない	105
19	制御	#N/A	0
20		#N/A	0
21		#N/A	0
22	移動	#N/A	0
23		#N/A	0
24		#N/A	0
25		#N/A	0
26	削除	削除した情報の意図せざる開示	27
27		削除されない	111
28		削除が遅い/一部削除されない	99

④提案手法の実装−画面イメージ③

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ ハザード一覧シート

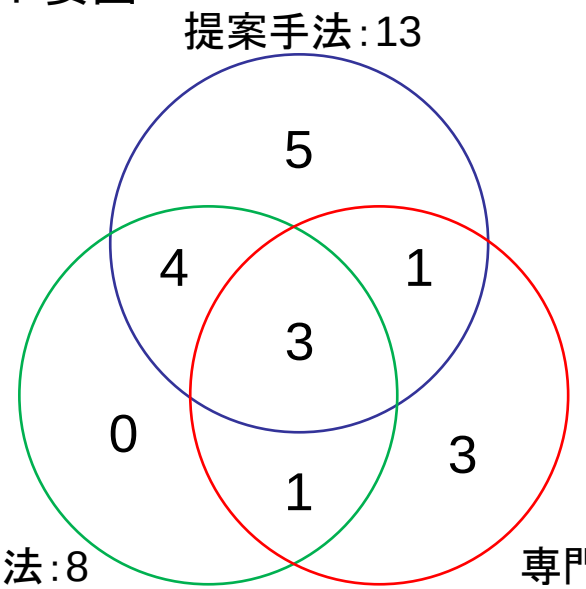
ES15

	C	N
4		↓この列をFALSEでフィルタする
5	ハザード候補	阻害条件に該当する
6	**Insider（内部者）によるDisclosure（暴露）**	FALSE
7	**Outsider（外部者）によるDisclosure（暴露）**	TRUE
8	Technical failure（技術的故障）によるDisclosure（暴露）	FALSE
9	**Virus（マルウェア）によるDisclosure（暴露）**	FALSE
10	Ignorance（無知）によるDisclosure（暴露）	FALSE
11	Faulty auxiliary equipment（予備機器の故障）によるDisclosure（暴露）	TRUE
12	Sabotage（怠業）によるDisclosure（暴露）	FALSE
13	Logical problems（ロジック問題）によるDisclosure（暴露）	FALSE
14	Logical attack（論理攻撃）によるDisclosure（暴露）	FALSE
15	**Configuration fault（設定ミス）によるDisclosure（暴露）**	TRUE
16	Social manipulation（ソーシャルエンジニアリング）によるDisclosure（暴露）	FALSE
17	**Insider（内部者）によるManipulation（操作）**	FALSE
18	**Outsider（外部者）によるManipulation（操作）**	TRUE
19	**Virus（マルウェア）によるManipulation（操作）**	FALSE
20	**Ignorance（無知）によるManipulation（操作）**	FALSE
21	Sabotage（怠業）によるManipulation（操作）	FALSE
22	Logical problems（ロジック問題）によるManipulation（操作）	FALSE
23	Logical attack（論理攻撃）によるManipulation（操作）	FALSE
24	**Planned work（計画作業）によるManipulation（操作）**	FALSE
25	**Configuration fault（設定ミス）によるManipulation（操作）**	TRUE
26	**Social manipulation（ソーシャルエンジニアリング）によるManipulation（操作）**	FALSE
27	**Insider（内部者）によるRemoval（持ち去り）**	FALSE
28	**Outsider（外部者）によるRemoval（持ち去り）**	FALSE
29	**Virus（マルウェア）によるRemoval（持ち去り）**	FALSE
30	**Ignorance（無知）によるRemoval（持ち去り）**	FALSE
31	**Logical attack（論理攻撃）によるRemoval（持ち去り）**	FALSE
32	**Social manipulation（ソーシャルエンジニアリング）によるRemoval（持ち去り）**	FALSE
33	**Insider（内部者）によるDisconnection（切断）**	FALSE
34	**Outsider（外部者）によるDisconnection（切断）**	TRUE
35	**Technical failure（技術的故障）によるDisconnection（切断）**	FALSE
36	**Virus（マルウェア）によるDisconnection（切断）**	FALSE
37	Ignorance（無知）によるDisconnection（切断）	FALSE
38	Fire（火災）によるDisconnection（切断）	FALSE
39	Faulty auxiliary equipment（予備機器の故障）によるDisconnection（切断）	TRUE
40	**Sabotage（怠業）によるDisconnection（切断）**	FALSE
41	Broken cable（ケーブル故障）によるDisconnection（切断）	TRUE
42	**Logical problems（ロジック問題）によるDisconnection（切断）**	FALSE
43	**Logical attack（論理攻撃）によるDisconnection（切断）**	FALSE
44	**Planned work（計画作業）によるDisconnection（切断）**	FALSE
45	**Configuration fault（設定ミス）によるDisconnection（切断）**	TRUE

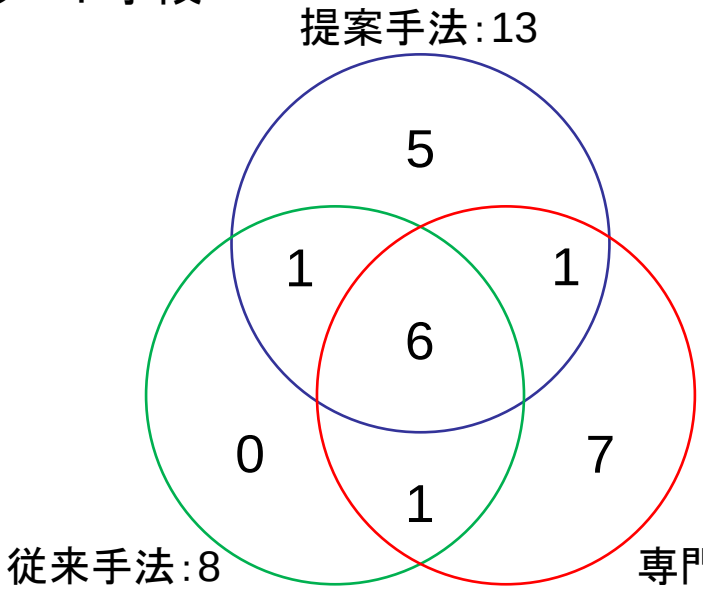
⑤検証と結果

特定手法	特定された ハザード要因	特定された ハザード手段
提案手法（業務部署）	13	13
従来手法（業務部署）	8	8
専門家	8	15

ハザード要因



ハザード手段



※従来手法と提案手法のリスク特定は業務部署役職員により2時間で実施

⑤検証と結果

■ 提案手法でのハザード特定の特性

- 提案手法で特定されたハザードは従来手法で特定された，
  手段&要因をおおむね含み，従来手法より網羅的であった.
  →提案手法により利用者の事前知識を補完できることが示唆された

- 提案手法と専門家によるハザード特定では，相互に特定されない手段，要因が存在した.
  →ツールの特定分野に課題があることが示唆された

ハザード特定の特性	手段（Attribute）	要因（Post-Guideword）
提案手法	可用性に影響を及ぼす手段を多く特定	外部的/偶発的な要因を多く特定
専門家	意図せぬ誤りについて多く特定	内発的な要因を多く特定

⑥提案手法で実現できたこと

- 従来手法と比して網羅性が向上した
  - 2段階での特定により「意図した動作とのズレ」とハザードの紐づけが容易になった（従来手法では1つのズレに一つのハザードが対応）
  - Wintherらの具体的なガイドワードを利用することによりリスク特定者の知識と想像力を補完できた（従来手法では提案手法と比較してより少ない手段および要因の特定に留まる）
- リスク特定粒度が均一化できた
  - 「意図した動作とのズレ」にCIAを用いることにより一定粒度のズレの抽出を実現した（従来手法および専門家ではCIAの全てを包含するズレが散見）
- 非専門家でも容易に利用が可能であった
  - 9種の動作類型の採用により情報システムの非専門家にも比較的理解しやすい
  - 提示するハザードの絞り込みにより単純な組み合わせと比してリスク特定者の負担軽減を実現した
  - Excelの利用により容易な操作を実現した
- ツール化が容易であった
  - 組合せ件数がハザード件数の大枠となるため，ツール化が容易であった

⑥検証で明らかになった課題

- CIAで測りづらい「意図した動作とのズレ」が特定されない
- ガイドワードに記載されていない事柄のハザード特定は手薄になる
- ガイドワードを用いる他のリスク特定手法（STPA/STRIDEなど）との優位性が不明
- 動作類型に重複および抜けもれが存在

動作種別

動作の類型	定義
読み込み	既存ファイルに変更を加えず，その内容を読み取ること
書き込み	既存ファイルに編集を行うこと
作成	新たにファイルを作成すること
保存	書き込みを行ったファイルを保存し，更新すること
制御	対象システム以外のシステムを動作せしめること
移動	既存ファイルを元の場所から別の場所に移動すること
削除	既存ファイルを削除すること

- **読み込みにおける喪失**
  機密性：情報の移動に伴う意図せざる開示
  可用性：読み込めない
  完全性：正しい情報が読み込めない
- **書き込みにおける喪失**
  機密性：情報の移動に伴う意図せざる開示
  可用性：書き込めない
  完全性：正しい情報が書き込めない
- **作成における喪失**
  機密性：作成物の意図せざる開示
  可用性：作成されない
  完全性：作成された情報が欠損/改変する/される
- **保存における喪失**
  機密性：保存した情報の意図せざる開示
  可用性：保存されない
  完全性：保存したデータが欠損/改変する/される
- **制御における喪失**
  機密性：（存在しない）
  可用性：制御対象が動作しない
  完全性：制御対象が不正な動作をする
- **移動における喪失**
  機密性：情報の移動に伴う意図せざる開示
  可用性：情報が移動しない
  完全性：移動した情報が改変される
- **削除における喪失**
  機密性：削除した情報の意図しない開示
  可用性：削除されない
  完全性：（存在しない）

Wintherらによるガイドワードの解釈①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

ハザード種別	説明
Disclosure（暴露）	利用者の意図に反して機密情報が公開されること
Manipulation（操作）	悪意ある操作によってCIAの喪失が起こされること
Disconnection（切断）	システム内/間の通信が切断され，意図する操作が行えないこと
Fabrication（偽造）	システム内/間の入出力が偽装され，正しくないデータになること
Delay（遅延）	システム内/間の応答が想定より遅延すること
Corruption（欠落）	システム内/間の入出力/保存データが一部欠落すること
Deletion（消去）	人為的な要因によりデータが消去されること
Removal（持ち去り）	悪意ある操作によって外部へのデータの移動が行われること
Stopping（停止）	利用者の意図に反してシステムが停止すること
Destabilization（不安定化）	システムの応答が不安定になり，利用者の意図に応じたり応じなかったりすること
Capacity Reduction（許容量の減少）	システムが毀損され，処理能力が平時より減少すること
Destruction（破壊）	利用者の意図に反してシステムが破壊され機能を果たさなくなること
Denial（拒否）	利用者の意図に反してシステムが利用を拒否すること

Wintherらによるガイドワードの解釈②

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

主体	CIAへの該当
Insider（内部者）	全てに該当
Outsider（外部者）	全てに該当
Technical failure（技術的故障）	全てに該当
Virus（マルウェア）	全てに該当
Ignorance（無知）	全てに該当
Fire（火災）	完全性/可用性
Faulty Auxiliary Equipment（予備機器の故障）	可用性
Sabotage（怠業）	完全性/可用性
Broken cable（ケーブル故障）	可用性
Logical problems（ロジック問題）	全てに該当
Logical attack（論理攻撃）	全てに該当
Planned work（計画作業）	全てに該当
Configuration fault（設定ミス）	全てに該当
Spamming（スパム）	全てに該当
Social manipulation（ソーシャルエンジニアリング）	機密性/完全性/可用性に該当

ハザード発生の抑止要因①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

抑止する要因	排除するハザード
内部者が操作できない	要因:内部者 手段:暴露，操作，偽造，欠落，消去，不安定化，許容量の減少 要因:無知 手段:暴露，操作，欠落，消去，不安定化，許容量の減少，破壊 要因:怠業 手段:暴露，操作，遅延，欠落，消去，許容量の減少
外部からアクセスできない	要因:外部者 手段:暴露，操作，偽造，欠落，消去，停止，不安定化，許容量の減少
予備機器が存在しない	要因:予備機器の故障 手段:暴露，切断，遅延，欠落，消去，停止，不安定化，許容量の減少，破壊，拒否
内部者による設定変更ができない	要因:設定ミス 手段:暴露，操作，切断，遅延，欠落，停止，不安定化，許容量の減少，拒否 要因:怠業 手段:不安定化，拒否 要因:ソーシャルエンジニアリング 手段:不安定化，拒否 要因:無知 手段:拒否
物理筐体が存在しない	要因:ケーブル故障 手段:切断，遅延，欠落，停止，不安定化，許容量の減少，拒否 要因:火災 手段:不安定化，許容量の減少，破壊，拒否
メールを利用しない	要因:スパム 手段:切断，遅延，欠落，停止，不安定化，許容量の減少，拒否
内部者と外部者がデータ量を制御できない	要因:内部者 手段:遅延 要因:外部者 手段:遅延 要因:無知 手段:遅延 要因:ソーシャルエンジニアリング 手段:遅延

ハザード発生の抑止要因②

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

抑止する要因	排除するハザード
データの抽出ができない&データの送信が制限されている	要因:内部者 手段:持ち去り 要因:外部者 手段:持ち去り 要因:マルウェア 手段:持ち去り 要因:無知 手段:持ち去り 要因:論理攻撃 手段:持ち去り 要因:ソーシャルエンジニアリング 手段:持ち去り
内部者による停止が制限されている	要因:内部者 手段:停止 要因:無知 手段:停止 要因:怠業 手段:停止 要因:ソーシャルエンジニアリング 手段:停止
内部者が操作できない&外部からアクセスできない	要因:ソーシャルエンジニアリング 手段:暴露，操作，消去
外部からアクセスできない&外部者が設置個所に立ち入りできない	要因:外部者 手段:切断，破壊，拒否
物理筐体が存在しない&バックアップが行われている	要因:火災 手段:消去
物理筐体が存在しないor予備機器が存在する	要因:火災 手段:停止

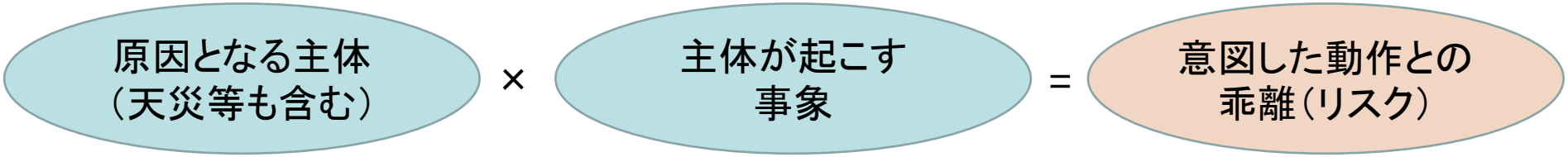
検証実施事項@検証説明資料より

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

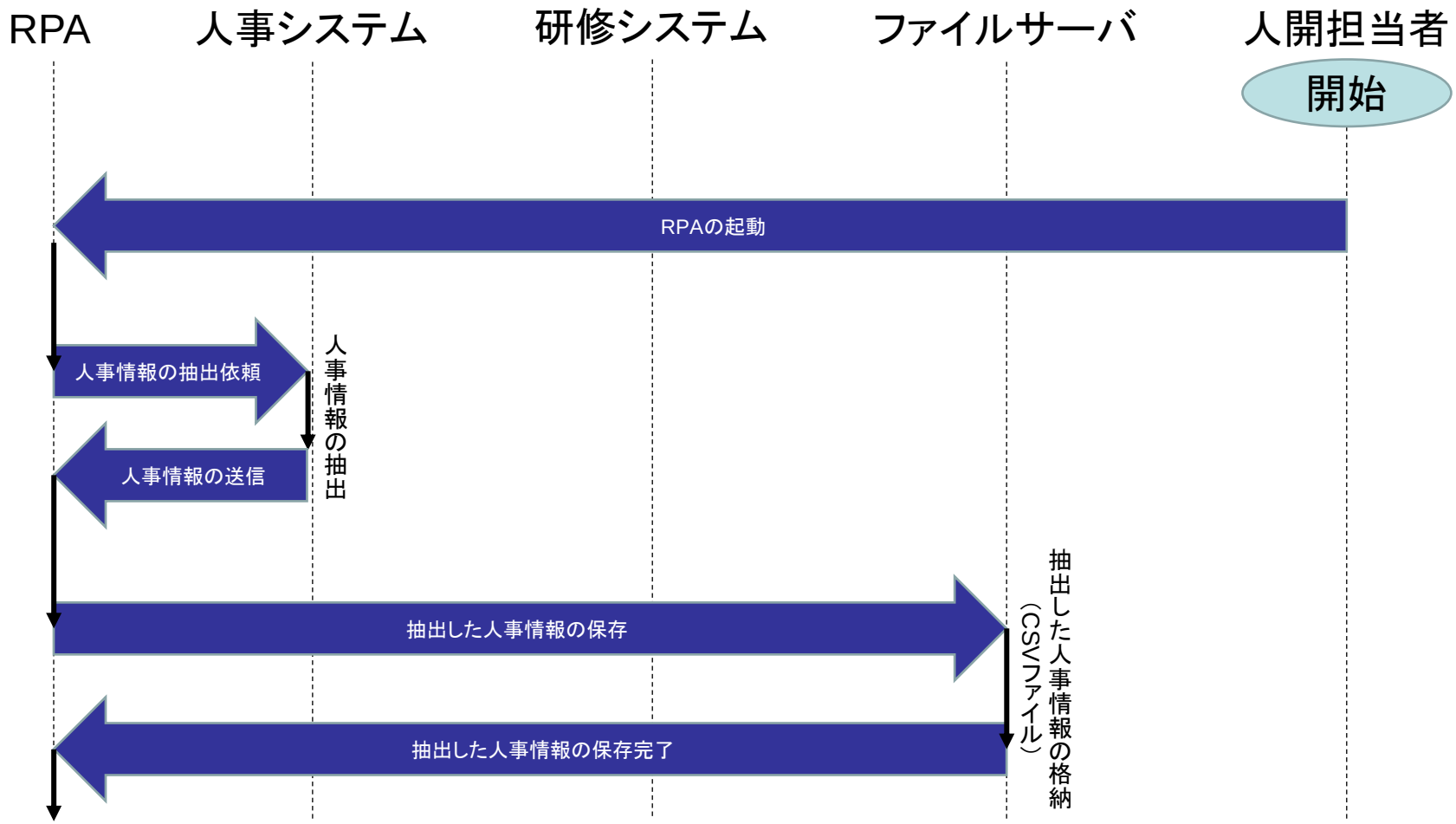
- 本稿に記載されているモデルケースを読んで，当該システムについて考えられるリスクと，それを引き起こす要因（ハザード）をすべて記載してください．
（実際のリスク対応においては頻度・影響に応じた評価を行いますが，今回は頻度&影響の多寡に関わらず，なるべく多くのリスクと要因を特定します．）

  - リスクはシステムが本来の意図と離れた動作を行うことを示します．
（例：書き込んだデータが意図せず開示される）

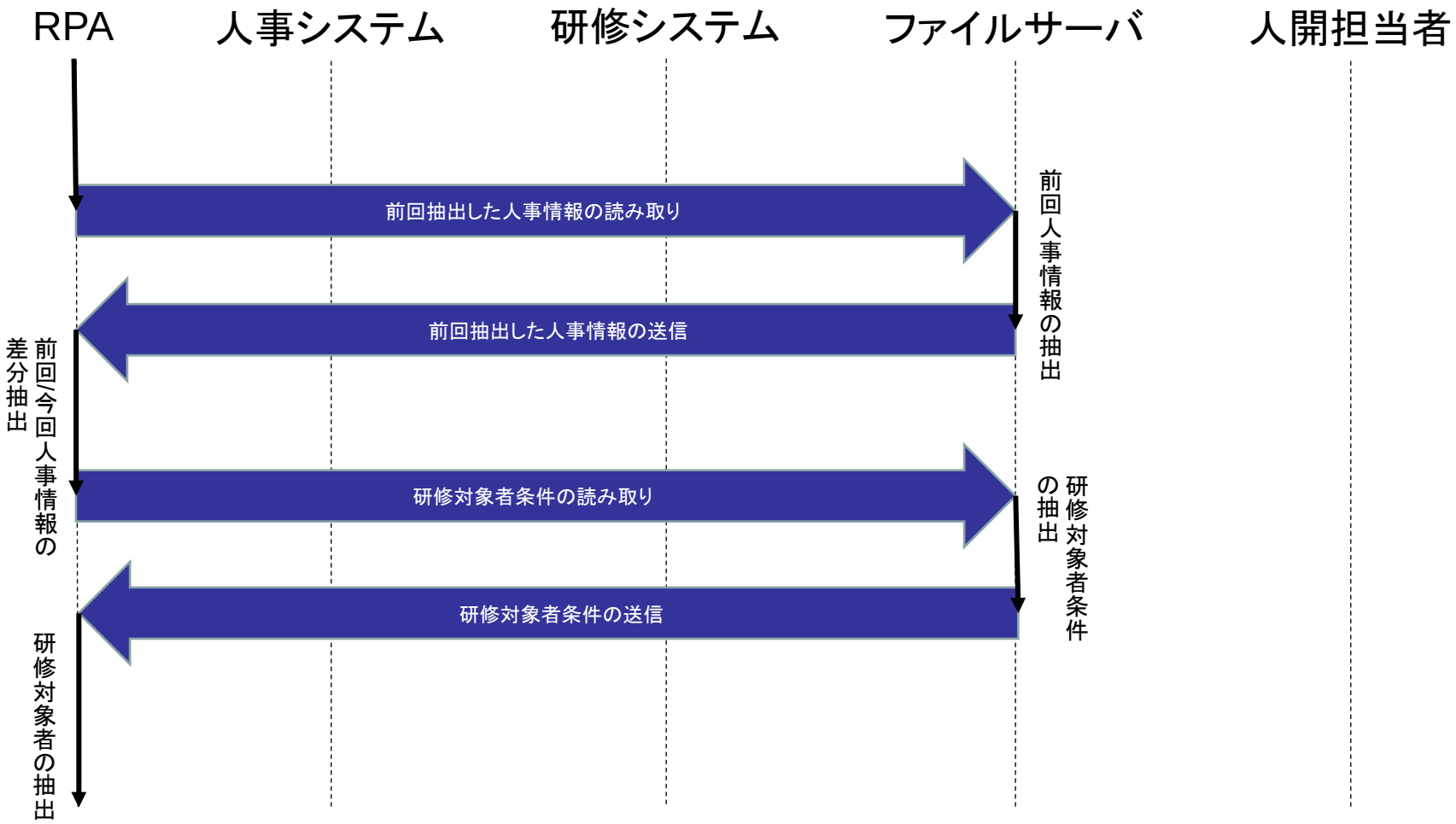
  - ハザードは「〇〇による△△」という形で，〇〇に原因となる主体を，△△に主体によって起こる事象を記載します．
（例：内部者の持出（により書き込んだデータが意図せず開示される））



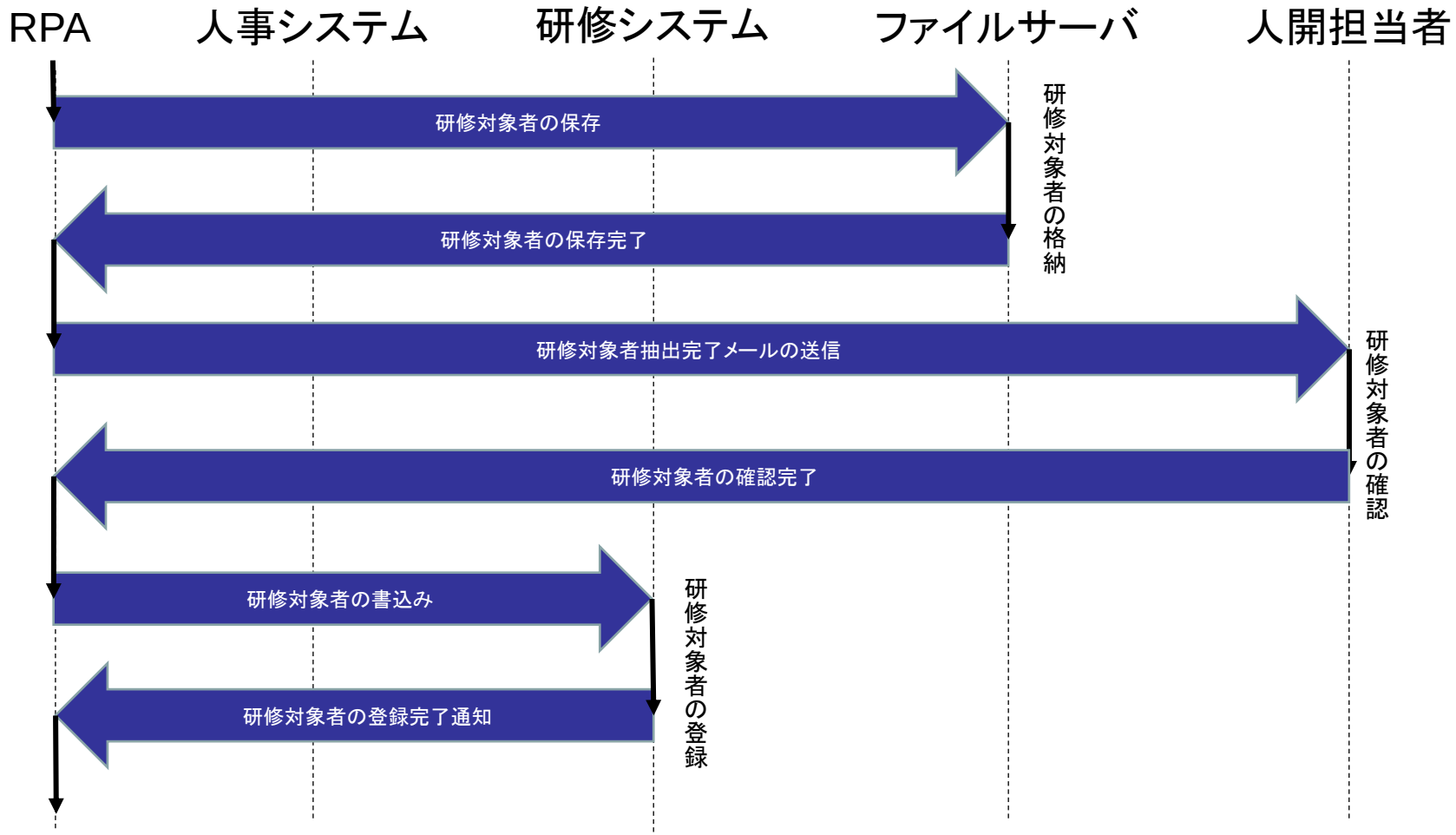
モデルケース
システム連携フロー①



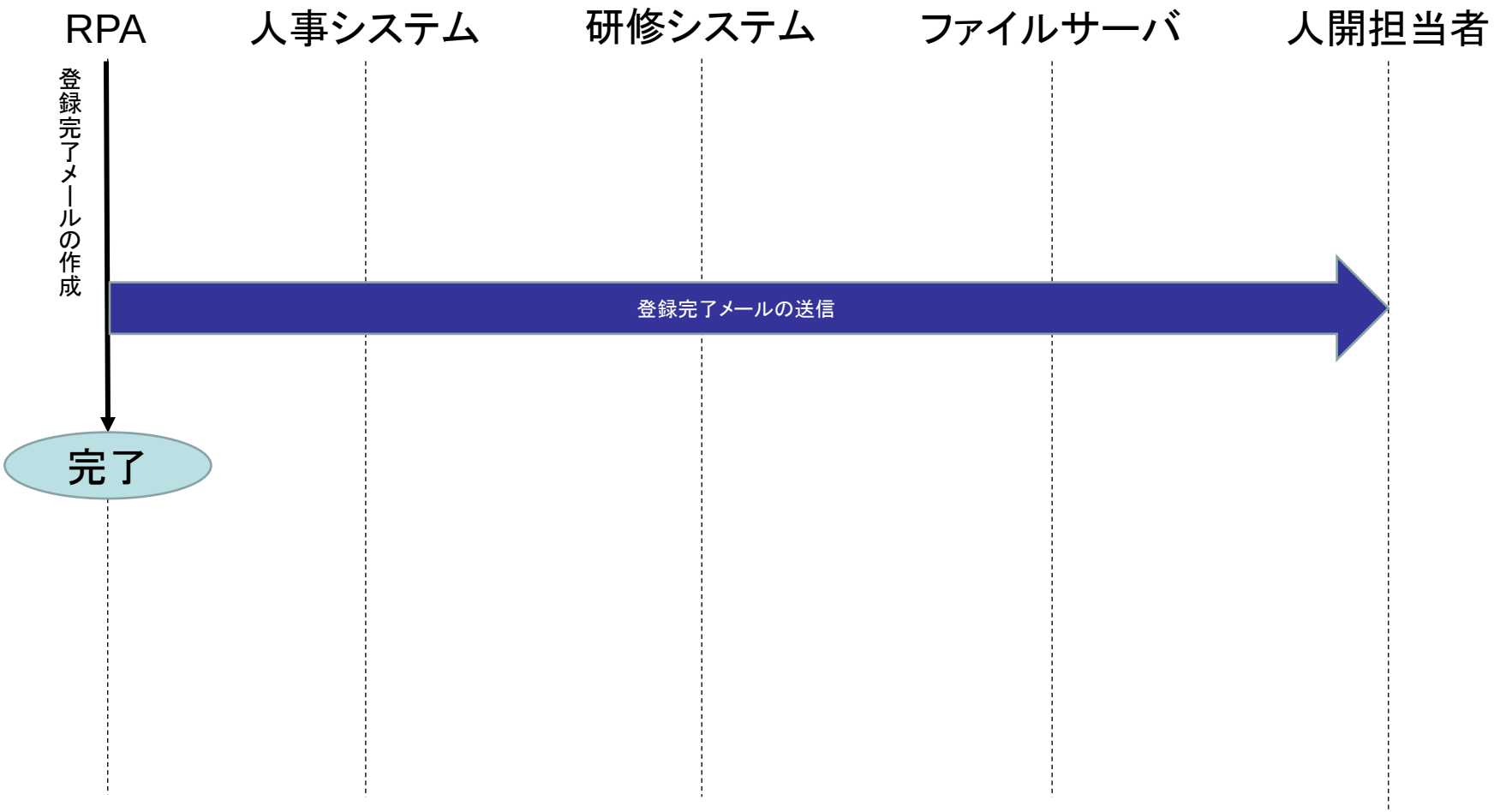
モデルケース
システム連携フロー②



モデルケース
システム連携フロー③



モデルケース
システム連携フロー④



検証における特定結果

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

従来手法によるリスク特定①

特定されたリスク
想定外のデータ抽出・登録されてしまう
意図しない人や場所へ情報が開示されてしまう
意図しない人でも共有サーバーが見えてしまう
関係者に情報を持ち出されてしまう
ウイルスに感染させられる
手動アサインを間違ってしまう
RPA改修などによって意図しない動作が発生してしまう
担当者変更時に引継ぎが困難になる
CSVファイル破損，文字化けして意図しないデータ抽出が発生する
Eメールが意図しない人に送信されてしまう
第三者からリモートアクセスされてしまう
サーバーが破損してしまう
データが消失してしまう

特定されたリスクを引き起こす要因（ハザード）
データのご登録により想定外のデータ登録・抽出
関係者のミスにより情報開示をしてはいけないところに開示をしてしまった.
サーバー閲覧権限の設定ミスにより共有サーバーが見えてしまった
関係者の個人情報を持ち出しによる漏洩リスク
第三者のサイバー攻撃による感染リスク（DDoS攻撃）
関係者のヒューマンエラーによる手動アサインリスク
設計・開発担当者の設計・開発ミスにより誤作動・登録
人事異動や退職による運用パフォーマンスの低下
関係者のCSVファイル破損を認知できなかったことによるファイルサーバーへの誤作動リスク
情報登録担当者の通知先emlご登録による情報漏洩
BEC攻撃によりリモートアクセス権限を乗っ取られる
ソフトウェアの不具合やハードウェアの故障によるサーバー障害リスク
災害によるデータの消失リスク

検証における特定結果

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

リスク特定支援ツールによるリスク特定①

特定されたリスク
情報の読込みに伴う意図せざる開示
読み込むデータの欠損/改変
読み込めない
読み込みが遅い/一部読み込まれない
情報の書込みに伴う意図せざる開示
書き込まれたデータの欠損/改変
書き込めない
書き込みが遅い/一部書き込まれない
作成物の意図せざる開示
作成されたデータの欠損/改変
作成されない
作成が遅い/一部作成されない
保存した情報の意図せざる開示
保存したデータの欠損/改変
保存されない
保存が遅い/一部保存されない
削除した情報の意図せざる開示
削除されない
削除が遅い/一部削除されない

特定されたリスクを引き起こす要因（ハザード）
Insider（内部者）によるDisclosure（暴露）
Technical failure（技術的故障）によるDisclosure（暴露）
Virus（マルウェア）によるDisclosure（暴露）
Ignorance（無知）によるDisclosure（暴露）
Sabotage（怠業）によるDisclosure（暴露）

検証における特定結果

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

リスク特定支援ツールによるリスク特定②

Logical problems（ロジック問題）によるDisclosure（暴露）
Logical attack（論理攻撃）によるDisclosure（暴露）
Social manipulation（ソーシャルエンジニアリング）による Disclosure（暴露）
Insider（内部者）によるManipulation（操作）
Virus（マルウェア）によるManipulation（操作）
Ignorance（無知）によるManipulation（操作）
Sabotage（怠業）によるManipulation（操作）
Logical problems（ロジック問題）によるManipulation（操作）
Logical attack（論理攻撃）によるManipulation（操作）
Planned work（計画作業）によるManipulation（操作）
Social manipulation（ソーシャルエンジニアリング）による Manipulation（操作）
Insider（内部者）によるRemoval（持ち去り）
Outsider（外部者）によるRemoval（持ち去り）
Virus（マルウェア）によるRemoval（持ち去り）
Ignorance（無知）によるRemoval（持ち去り）
Logical attack（論理攻撃）によるRemoval（持ち去り）
Social manipulation（ソーシャルエンジニアリング）によるRemoval （持ち去り）
Insider（内部者）によるDisconnection（切断）
Technical failure（技術的故障）によるDisconnection（切断）
Virus（マルウェア）によるDisconnection（切断）
Ignorance（無知）によるDisconnection（切断）
Fire（火災）によるDisconnection（切断）
Sabotage（怠業）によるDisconnection（切断）
Logical problems（ロジック問題）によるDisconnection（切断）
Logical attack（論理攻撃）によるDisconnection（切断）

検証における特定結果

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

リスク特定支援ツールによるリスク特定③

Planned work（計画作業）によるDisconnection（切断）
Spamming（スパム）によるDisconnection（切断）
Social manipulation（ソーシャルエンジニアリング）による Disconnection（切断）
Insider（内部者）によるFabrication（偽造）
Virus（マルウェア）によるFabrication（偽造）
Logical problems（ロジック問題）によるFabrication（偽造）
Social manipulation（ソーシャルエンジニアリング）による Fabrication（偽造）
Insider（内部者）によるDelay（遅延）
Outsider（外部者）によるDelay（遅延）
Technical failure（技術的故障）によるDelay（遅延）
Virus（マルウェア）によるDelay（遅延）
Ignorance（無知）によるDelay（遅延）
Fire（火災）によるDelay（遅延）
Sabotage（怠業）によるDelay（遅延）
Logical problems（ロジック問題）によるDelay（遅延）
Logical attack（論理攻撃）によるDelay（遅延）
Planned work（計画作業）によるDelay（遅延）
Spamming（スパム）によるDelay（遅延）
Social manipulation（ソーシャルエンジニアリング）によるDelay（遅延）
Insider（内部者）によるCorruption（欠落）
Technical failure（技術的故障）によるCorruption（欠落）
Virus（マルウェア）によるCorruption（欠落）
Ignorance（無知）によるCorruption（欠落）
Fire（火災）によるCorruption（欠落）
Sabotage（怠業）によるCorruption（欠落）
Logical problems（ロジック問題）によるCorruption（欠落）

検証における特定結果

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

リスク特定支援ツールによるリスク特定④

Logical attack（論理攻撃）によるCorruption（欠落）
Planned work（計画作業）によるCorruption（欠落）
Spamming（スパム）によるCorruption（欠落）
Social manipulation（ソーシャルエンジニアリング）による Corruption（欠落）
Insider（内部者）によるDeletion（消去）
Technical failure（技術的故障）によるDeletion（消去）
Virus（マルウェア）によるDeletion（消去）
Ignorance（無知）によるDeletion（消去）
Sabotage（怠業）によるDeletion（消去）
Broken cable（ケーブル故障）によるDeletion（消去）
Logical problems（ロジック問題）によるDeletion（消去）
Logical attack（論理攻撃）によるDeletion（消去）
Planned work（計画作業）によるDeletion（消去）
Social manipulation（ソーシャルエンジニアリング）によるDeletion （消去）
Technical failure（技術的故障）によるStopping（停止）
Virus（マルウェア）によるStopping（停止）
Logical problems（ロジック問題）によるStopping（停止）
Logical attack（論理攻撃）によるStopping（停止）
Planned work（計画作業）によるStopping（停止）
Spamming（スパム）によるStopping（停止）
Insider（内部者）によるDestabilization（不安定化）
Technical failure（技術的故障）によるDestabilization（不安定化）
Virus（マルウェア）によるDestabilization（不安定化）
Ignorance（無知）によるDestabilization（不安定化）
Logical problems（ロジック問題）によるDestabilization（不安定化）
Logical attack（論理攻撃）によるDestabilization（不安定化）
Planned work（計画作業）によるDestabilization（不安定化）
Spamming（スパム）によるDestabilization（不安定化）

検証における特定結果

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

リスク特定支援ツールによるリスク特定⑤

Insider（内部者）によるDestruction（破壊）
Technical failure（技術的故障）によるDestruction（破壊）
Virus（マルウェア）によるDestruction（破壊）
Ignorance（無知）によるDestruction（破壊）
Sabotage（怠業）によるDestruction（破壊）
Logical problems（ロジック問題）によるDestruction（破壊）
Logical attack（論理攻撃）によるDestruction（破壊）
Planned work（計画作業）によるDestruction（破壊）
Social manipulation（ソーシャルエンジニアリング）による Destruction（破壊）
Technical failure（技術的故障）によるDenial（拒否）
Virus（マルウェア）によるDenial（拒否）
Logical problems（ロジック問題）によるDenial（拒否）
Logical attack（論理攻撃）によるDenial（拒否）
Planned work（計画作業）によるDenial（拒否）
Spamming（スパム）によるDenial（拒否）
Insider（内部者）によるCapacity Reduction（許容量の減少）
Technical failure（技術的故障）によるCapacity Reduction（許容量の減少）
Virus（マルウェア）によるCapacity Reduction（許容量の減少）
Ignorance（無知）によるCapacity Reduction（許容量の減少）
Sabotage（怠業）によるCapacity Reduction（許容量の減少）
Logical problems（ロジック問題）によるCapacity Reduction（許容量の減少）
Logical attack（論理攻撃）によるCapacity Reduction（許容量の減少）
Planned work（計画作業）によるCapacity Reduction（許容量の減少）
Spamming（スパム）によるCapacity Reduction（許容量の減少）

検証における特定結果

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

専門家によるリスク特定①

特定されたリスク
共有サーバのリソースが枯渇する
共有サーバの更新（バージョンアップ、脆弱性対応）が遅れる
旧担当者からのID/PWの漏えい
連携システム経由での侵害
連携システムを侵害（担当者PC、研修システム、ファイルサーバ）
人事情報が漏えいする
研修対象条件の漏えい、改ざん
研修対象者の漏えい、改ざん
抽出完了メールの誤送信
登録完了メールの誤送信
プログラムに不備が多い
障害に気づけない
障害対応に時間がかかる
セキュリティ侵害に気づけない
RDPによる仮想PCへの不正アクセス
バックアップからの復旧ができない
重複受講依頼

特定されたリスクを引き起こす要因（ハザード）
共有サーバのリソース管理ができていないことにより、仮想PCを立ち上げ過ぎる
一部の仮想PCがリソースを消費する（利用量増、バグ等）
仮想PCの停止調整がうまくいかず、メンテナンススケジュールが決められない
業務変更、異動、退職により、担当が外れた際にPW変更を実施しない
ファイルサーバ（共有用）、担当者利用PC等にID/PWが残される
担当者PCがマルウェアに感染している

検証における特定結果

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

専門家によるリスク特定①

人事システムがマルウェアに感染している
ファイルサーバがマルウェアに感染している
仮想PCがマルウェアに感染している
仮想PCのアクセス権が適切でない
ファイルサーバのアクセス権が適切でない
特権管理が適切でない
仮想PCに人事情報が保存される（永続、一時）
ファイルサーバに人事情報が保存される
ファイルサーバ上に前回抽出した人事情報が保存されている
仮想PCに前回抽出した人事情報が保存される（永続、一時）
ファイルサーバのアクセス権が適切でない
ファイルサーバ上に研修対象条件が保存されている
特権管理が適切でない
仮想PCに研修対象条件が保存される
ファイルサーバのアクセス権が適切でない
ファイルサーバ上に研修対象者が保存される
仮想PCに研修対象者が保存される
送信先が適切に管理されていない（担当者変更）
MLメンバが適切に管理されていない（メンバ変更）
送信先が適切に管理されていない（担当者変更）
開発担当者のスキル不足（不十分な開発（特に例外処理））
運用担当者のスキル不足
運用担当者のスキル不足
運用担当者のスキル不足
運用担当者による監視が不十分
アクセス制御の不備
ログが適切に取得・保存されていない
復旧試験を定期的に実施していない
過去の受講履歴を確認していない