2019.6.7.JSSA大会

ひとり情シスとガバナンス

「The system administrator of only one person and his IT governance」

2019年06月07日

情報セキュリティ合同研究会

研究内容

【テーマ】

ひとり情シスとガバナンス

【目次】

１．本研究の背景と狙い
２．先行研究の整理
３．研究の仮説
４．研究手法
５．分析結果の提示（情報システム監査面）
６．考察（情報システム監査面）
７．研究手法（情報セキュリティ面）
８．分析結果の提示（情報セキュリティ面）
９．考察（情報セキュリティ面）
１０．まとめ・結論

1．本研究の背景と狙い

【背景】

中小企業を中心に多くの企業において、人材不足等の要因により、ひとり情シス状態（情報システム担当者がひとりしか居ない）、兼任情シス状態（他業務担当者が情報システム担当者を兼任している）が散見される。

しかしながら、ITガバナンスの観点から見た場合、**ひとり情シス状態や、兼任情シス状態を選択することによって生じる、組織全体のリスクをモニタリング、評価されていないという懸念がある**。

【狙い】

本研究は、ひとり情シスや兼任情シスを選択するにあたって、**経営として認識すべきリスクを提示する**とともに、ひとり情シスを選択せざるを得ない場合に実施すべき**補完的コントロールを提案する**ことで、**ひとり情シス・兼任情シスの選択を余儀なくされる企業においても、リスクを認識し、適切なコントロールを実施できるための一助となることを狙いとする。**

2．先行研究の整理

中堅企業IT投資動向調査（※）によると、以下のような状況であることがわかった。

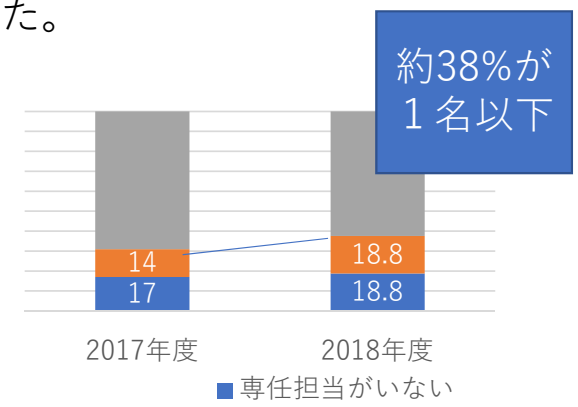
1．ひとり情シス状況

中堅企業の**約38%が情報システム担当者１名以下**

（18.8%：専任担当者１人、18.8%：専任担当者なし）

→　2016年度調査時27%、2017年度調査時32%と毎年増加傾向

また、クラウドの普及により、ひとり情シスでもシステム導入・運用可能な状況が拡大している。



2．セキュリティ事故状況

→　中堅企業の**35.7%が直近３年間にセキュリティ事故の経験あり**。

→　昨年度の30.2%から５％の増。

→　社員によると思われる不正行為からのインシデントが4.9%に達し、**ユーザーのガバナンスに起因するインシデントが急上昇している。**

3．セキュリティ対策状況

→　2017年度の調査では、**IPAガイドライン準拠率は４％、CSIRT活動は１．５％**

（※）中堅企業IT投資動向調査
調査者　DELL,EMCジャパン
調査期間　2017年度：2017年11月~2018年1月、2018年度：2018年12月~2019年1月
調査対象　国内の中堅企業（従業員100名以上1,000名未満）　2017年度：700社以上、2018年度：868社

3．研究の仮説

【仮説】

・ひとり情シスは、要員不足等の**ひとり情シスにせざるを得ないという状況のみ焦点が当てられて選択**されており、**リスクを評価した結果として選択されたものではない**。

・ひとり情シスを選択したことによるリスクについて、**補完的コントロールが実施されていない**。

４．研究手法

【情報システム監査面】

情報システム監査面において実際に発生している事例を調査し、原因を特定するとともに、各企業での実態を把握することで、改善策を検討・提案する。

【情報セキュリティ面】

情報セキュリティの観点から、以下のような視点でアンケートを行い、類型化したうえで、注力すべき補完的コントロールを提案する。

項目	視点
事業環境	事業属性、財務、投資規模、計画、プロジェクトなど
計画	ガバナンス、計画、プロジェクトなど
組織・体制	IT組織、IT人材、企画体制、開発体制、運用体制など
システム	取扱いシステムや、管理状況など
インフラ環境	サーバの構成や、クラウドサービス、ネットワークなど

・上記５分類、１１３問のアンケートを実施。

・４３社からの回答を受領し、全社から回答のあった８０問について分析。

情報システム監査面

5．分析結果の提示（情報システム監査面）(1)

発生した事例につき、原因を特定し、改善策を検討した。

発生事例	発生事象の原因	改善策
業者選定に関する問題 • RFPを作成せず、口頭発注 • 見積書内訳を精査せず • 候補となる業者選定の根拠が不透明	• 内部統制上の不備（システム導入時の業者選定のルールがない。）	⇒信頼できる会社（親会社、関連する子会社等）に、システム開発、もしくは業者選定等を委託。 ⇒RFPやRFIの書式、システム導入時の業者選定ルールなどを明確に定める。
要件定義に関わる問題 • 能率が悪いフローを踏襲	• システム開発を担当者に任せきり。（経営者は無関心） • 担当者は経営者、実務担当者との意思疎通が不十分。	⇒経営者が、適切なプロジェクト開発チームを設置する。 ⇒業務フローの見直しにもしっかり踏み込む

5．分析結果の提示（情報システム監査面）(2)

発生した事例につき、原因を特定し、改善策を検討した。

発生事例	発生事象の原因	改善策
情報セキュリティの確保が不適切 • AD（Active Directory)等を導入したが、権限設定が不適切であった • 外部媒体出力制御が実施できていなかった	• 設定担当が不明確、予算が不十分。 • 会社としてのポリシの議論が不十分	⇒セキュリティポリシ等を明確に定める ⇒要員、システムが抱えるリスク等を考慮した予算措置 ⇒セキュリティの設定等のレビューの徹底
ソフトウエアの問題 ・サポート期限切れ ・ライセンス管理が不適切	• 資産管理が不徹底（台帳を作成しない、内容の修正等を怠る） • セキュリティに関する社員の意識が低い	⇒情報資産管理ソフトなどの活用（PDCAの徹底） ⇒備品管理ルールとの紐付け（パソコンを購入する際には、経理およびシステム部門の両方に伝達。もしくはシステム部門が機種を選定） ⇒社員向けの研修（計画を策定、理解度を測定

6．考察（情報システム監査面）

◎「ひとり情シス」状態の組織の最大のリスクとは？

- 組織拡大に伴い、情報の価値（個人情報や取引先情報などを大量に保有）が高まり、管理するためのIT投資も増大
- 企業経営における情報システムの位置づけが大きくなれば、システムが不具合を起こしたときの影響も大きくなる
- 情報が漏洩すれば、会社の信用失墜、損害賠償等の対応が必要なケースあり。オンライン販売システムなどが停止すれば、会社の収入減少等の損害も発生する
- 以下の通りの手順で、計画的にシステム部門を整備していく必要がある

◎小規模組織におけるシステム部門の整備

①管理者の統制やサポートがないひとり情シス状態（スタート）

②リスク管理の定着、徹底により、管理者の統制やサポートが機能（単純業務などの委託等が可能に）

③業務量が多くなり、担当者を複数に（ひとり情シス状態からの脱却）

④独立したシステム部門の設置（権限も責任も明確に）。情報システム監査等も導入

6．考察（情報システム監査面）

◎「ひとり情シス」状態の組織のリスクを適切に管理するために

- 重要性に見合った、「ヒト」「モノ」「カネ」の措置
  - ✓ 「ヒト」…IT担当者の増員、能力向上
  - ✓ 「モノ」…合理的なITに関わる設備投資計画の策定
  - ✓ 「カネ」…十分な経費措置（ソフトウエアの購入、保守費の措置等）
- 独立したシステム部門の設置
  - ✓ 「ヒト」「モノ」「カネ」を要求するためには、明確な権限、責任を有する部署、担当者の配置が重要
  - ✓ （子会社である場合）親会社の関与のあり方を検討
    - ◆ 親会社が情報システムの基盤を整備し、合理的な使用料で業務に活用
    - ◆ 子会社に親会社のシステム担当者を派遣、もしくはグループ内のシステム関係の子会社が支援

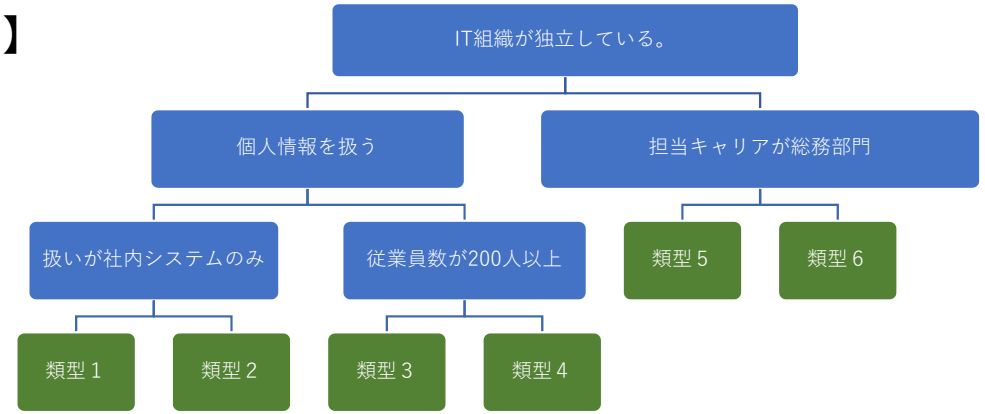
情報セキュリティ面

7．研究手法（情報セキュリティ面）

アンケート結果をもとに、ひとり情シスの類型化を行う。

類型化にあたっては、以下の特徴を有する「決定木」を利用して類型化することとした。

【決定木による分類イメージ】



【決定木の特徴】

1．解釈が容易。

決定木での分類においては、データが分割されていく流れが把握しやすく、処理内容も理解しやすい。

2．数値、カテゴリデータが混在していてもよい。

分類の視点には、数値データ（大小比較が可能な連続的なデータなど）、カテゴリデータ（区分など）のいずれも採用することができる。

3．必要な前処理が少ない。

決定木では、データを分割するための指標として、特徴量を利用するので、スケーリング等の前処理が少ない。

8．分析結果の提示（ひとり情シスの類型化）～分類手順～

決定木を用いた分類について、以下の手順に基づいて進める。

1．データを分割する基準を決定する。

まずは、データを分割する基準を決定します。ここでは、最も「きれいにデータを分割できる」基準を選びます。

「きれいにデータを分割」とは、今回の場合、「A：情報事故を起こす」「B：情報事故を起こさない」に分割するに際し、分割した際に、AとBの混在具合が最も小さいように分割する基準を選定します。

（※「情報利得が最大（不純度が最小）」（後述）となる基準を選定します。）

2．データを分割する。

1にて選定した基準に基づいて、データを分割します。

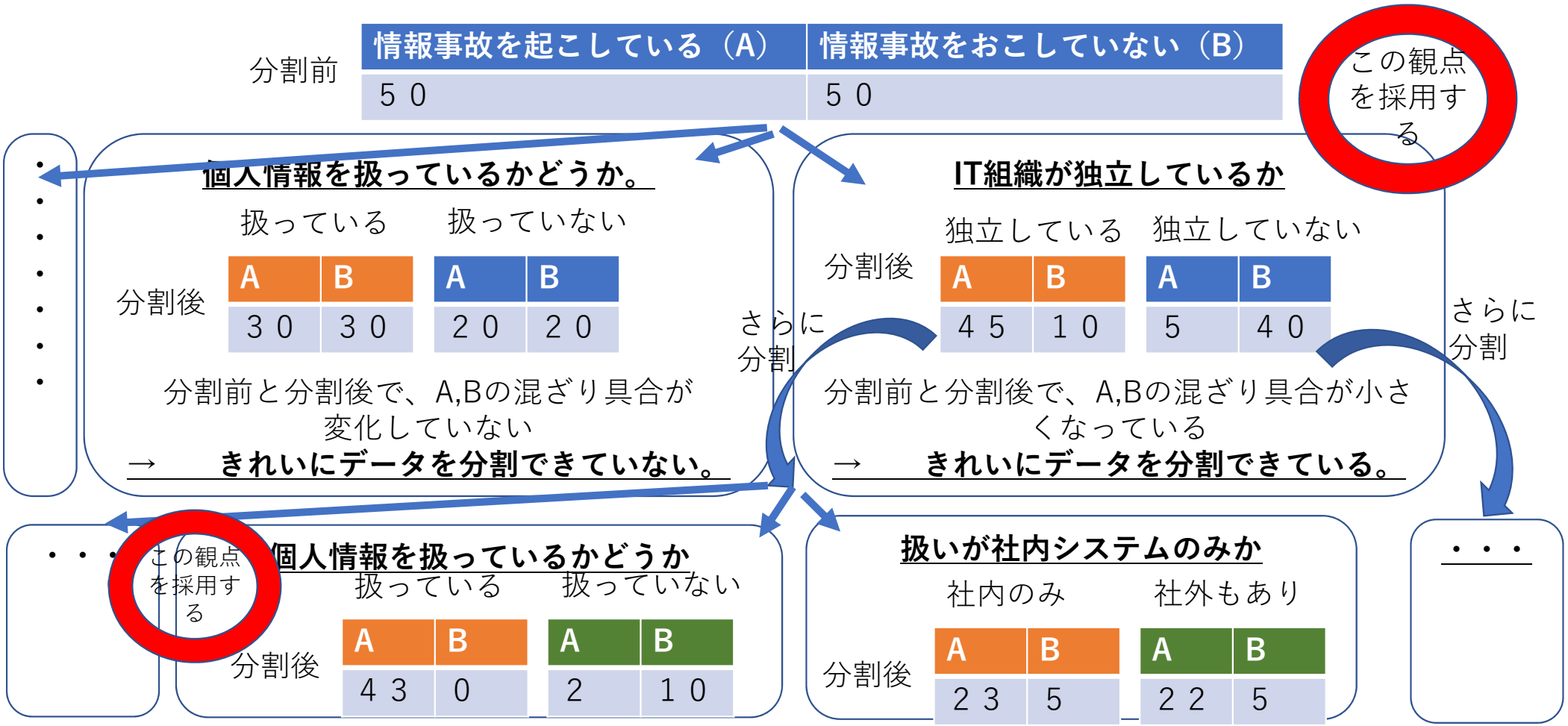
3．設定した基準になるまで、1、2を繰り返す。

決定木分析では、「どれだけの階層まで分割するか」を考慮して、類型化を行います。

あまり、細かく分割されてしまわないように、適切な階層までの類型化とします。

8．分析結果の提示（ひとり情シスの類型化）～情報利得及び不純度～

◎「情報利得」とは、「データ分割の前後を比較して、どれだけきれいにデータを分割できたか」という度合になります。例えば、以下のようなデータとなる場合は、「IT組織が独立しているか」を最初の分割の基準とすることになります。以降、分割後のそれぞれの分類に対して、同様に次の基準を適用していく。



8．分析結果の提示（ひとり情シスの類型化）～アンケート結果～

1．アンケート内容

5分類、１１３問のアンケートを実施。

2．回答結果

１１３問のアンケートのうち、全社から回答のあった８０問において、決定木による類型化を行った。

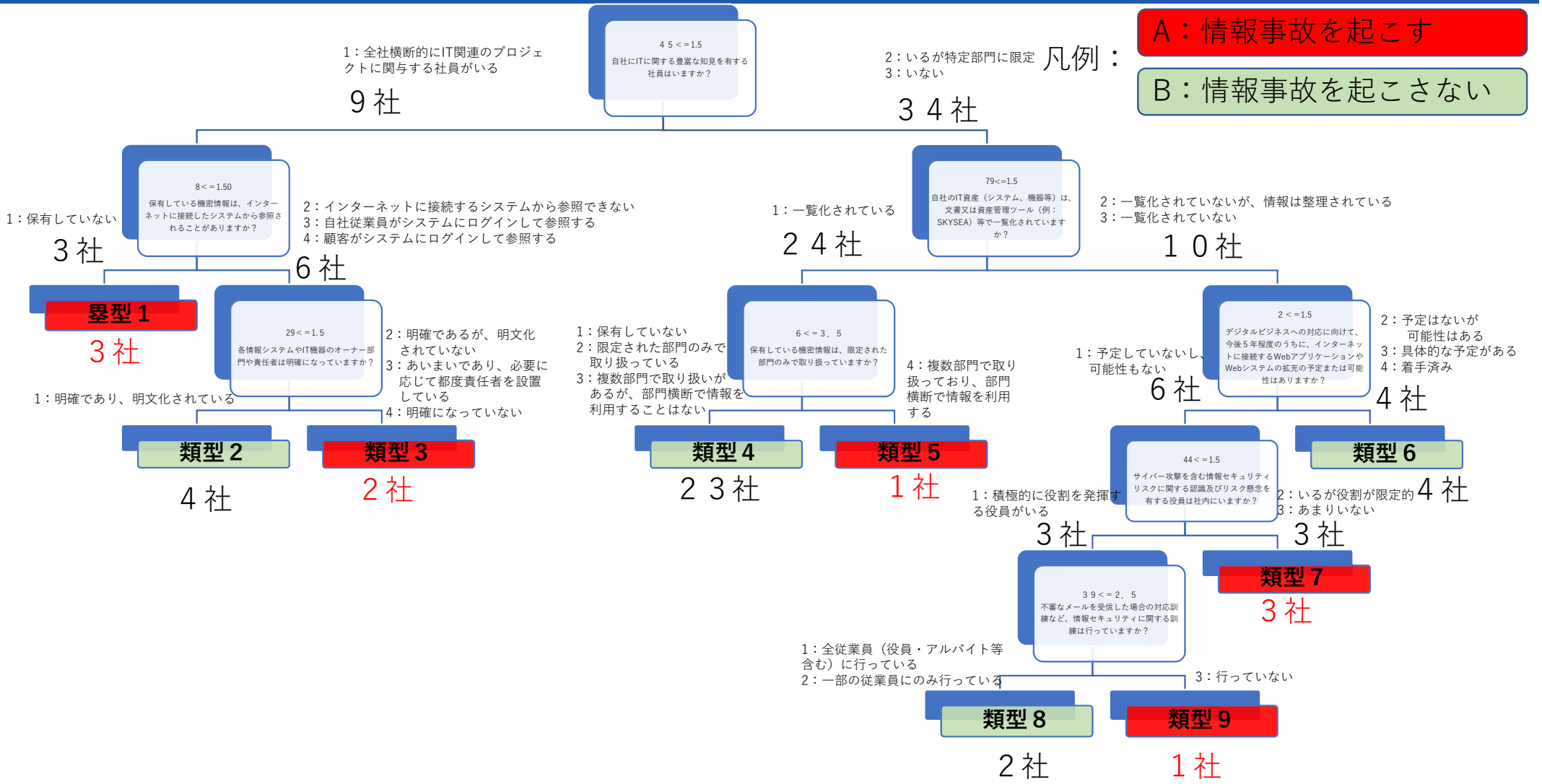
3．決定木による類型化

決定木を利用して、類型化を行った結果、以下のような９つの類型が特定された。（各類型の詳細は後述）

類型パターン	セキュリティ問題危険性
類型１	A：情報事故を起こす
類型２	B：情報事故を起こさない
類型3	A：情報事故を起こす
類型4	B：情報事故を起こさない

類型パターン	セキュリティ問題危険性
類型５	A：情報事故を起こす
類型６	B：情報事故を起こさない
類型７	A：情報事故を起こす
類型８	B：情報事故を起こさない
類型９	A：情報事故を起こす

8．分析結果の提示（ひとり情シスの類型化）～決定木による類型化結果～



8．分析結果の提示（ひとり情シスの類型化）～情報事故を起こした類型～

1．以上の分析の結果、情報事故を起こした類型は以下の通りであった。

一人情シス	類型	アンケート回答	企業数
全社横断情シス型	類型１	全社横断的にIT関連のプロジェクトに関与する社員がいるが、機密情報を**「保有していない」と認識**している。	３社
	類型３	全社横断的にIT関連のプロジェクトに関与する社員がいるかつ、機密情報が「インターネットから参照される」ことを認識しているが、**システムのオーナー部門・責任者が明文化されていない**。	２社
ひとり情シス・兼任情シス型	類型５	ITに関する知見を有する社員がいないか、特定の部門に限定されており、システムの一覧は作成されているものの、**機密情報が複数部門で取り扱っており、部門横断で情報を利用している**。	１社
	類型７	ITに関する知見を有する社員が特定の部門に限定されており、**システムの一覧も作成されておらず**、**情報セキュリティリスクに関する認識及びリスク懸念を有する役員が、いないか、限定的である**。	３社
	類型９	情報セキュリティリスクに関する認識及びリスク懸念を有する役員が明確になっているものの、ITに関する知見を有する社員が特定の部門に限定されており、**システムの一覧も作成されておらず**、**不審なメールを受信した場合の対応訓練など、情報セキュリティに関する訓練が行われていない**。	１社

9．考察（情報セキュリティ面）

◎「ひとり情シス」の組織が情報事故を起こす状態とは。

アンケートの分析結果より、以下のようなひとり情シス・兼任情シスの場合は、以下のような状態のときに情報事故を起こしているという事実が確認された。

- 情報セキュリティリスクに関する認識及びリスク懸念を有する役員が、いないか、限定的である。
- システムの一覧が作成されていない。
- 機密情報が複数部門で取り扱っており、部門横断で情報を利用している。
- 不審なメールを受信した場合の対応訓練など、情報セキュリティに関する訓練が行われていない。

◎分析結果を踏まえ注力すべき補完的コントロールとは。

①情報セキュリティリスクに関して積極的に役割を発揮する役員を明確にする。

②システムの一覧を作成する。

③機密情報は限定された部門だけで取り扱う。

④社員に対する情報セキュリティに関する訓練が行う。

【補足】全社横断情シスでも気を付けるべき事項とは。

今回のアンケートにて、全社横断情シスが存在していても以下の状態である場合は、注意する必要があることがわかった。

- 機密情報を保有していないと認識している。（保有情報を認識できていない可能性がある。）
- 各情報システムやIT機器のオーナー部門や責任者が明文化されていない。

まとめ・結論

１０．まとめ・結論

クラウド化の進展によって「ひとり情報シスの状況」はさらに増えると想定できる中で、実際に毎年ひとり情報シスが増えている状況を資料により確認し、本研究を通して以下のような内容が確認できた。

【情報システム監査面】

- 業務実態（例えば、個人情報をどの程度保有しているか？BCPが明確になっているか）、システム管理の課題、経営上重要なシステムの有無等を把握するために、実態調査は有効であることを確認した。
- 重要情報をシステム管理するようになった時点で、システムに関わるリスクが増大し、適切な管理が必要となるという仮説も確認できた。
- 今後の研究において、「ひとり情シス状態」を脱却すべきタイミング、予兆などを具体的に示し、小規模組織におけるITガバナンスの確立に貢献することとしたい。

【情報セキュリティ面】

- ひとり情シス・兼任情シスにおいては、情報セキュリティに関する役員の役割を明確化、システム一覧の作成、機密情報の限定された部門での利用、社員に対する情報セキュリティ訓練の実施が重要であることを確認した。
- また、全社横断情シスが存在する企業においても、機密情報を保有していないと認識していたり、システムのオーナー部門が明文化されていない場合は注意が必要であることを確認した。
- 今後の研究においては、分析結果の信頼性を高めるために、更に多くの企業に対して、アンケートを行い、ひとり情シス・兼任情シスの情報事故防止に貢献することとしたい。

ご清聴ありがとうございました。

研究会は、さらに情報セキュリティとシステム監査の有効性と効率性を掘り下げてまいります。 研究会への参画をお待ちしております。

情報セキュリティ合同研究会

＜２０１８年度　研　究　会　参　加　メ　ン　バ ー　（敬称略）＞
川辺 良和：主査
芳仲　宏
長野 加代子
浅野　卓　：発表者
鈴木　淳哉　：発表者