小規模地方自治体職員の情報セキュリティインシデント報告行動を促進する要因の分析

岡 佳伸[1]　島 成佳[1]

概要：著者らが所属する町村のような小規模な地方自治体では，一般的に専門人材の不在や限られた予算等によって，理想的な情報セキュリティ対策を実施することが難しい．標的型攻撃メールをはじめとした様々なサイバー攻撃を受けているが，前述の制約により情報セキュリティインシデント時の検知を目的とする技術的対策の導入は一部に留まっている．本研究では，この情報セキュリティインシデントの早期検知を目的として，職員からの報告行動を促すための施策に注目する．具体的には，情報セキュリティ対策の中で，専門人材や予算を必要としない制度的セキュリティである情報セキュリティポリシーの策定や運用を対象とする．情報セキュリティポリシーにより職員からの報告を促すため，報告行動に関係する仮説を設定し，著者らが所属する地方自治体で実施した研修とアンケート調査結果を用いて分析・考察した結果を報告する．

キーワード：情報セキュリティインシデント，報告行動，地方公共団体，小規模自治体

An analysis of factors to Encourage Information Security Incident Reporting Behavior of officials in Small Local Governments

YOSHINOBU OKA[1]　SHIGEYOSHI SHIMA[1]

Abstract: Small local governments, such as the towns and villages to which the authors belong, generally lack expert personnel and have limited budgets, making it difficult to implement ideal information security measures. In addition, despite being exposed to various cyber attacks including targeted e-mail attacks, the above limitations limit the implementation of technical measures for the purpose of detecting information security incidents when they occur. This study focuses on measures to promote staff reporting behavior for early detection of such information security incidents. The authors developed a hypothesis on reporting behavior to promote reporting from employees through the formulation and operation of information security policies, which are institutional security measures that do not require specialized personnel or budget, and analyzed and discussed the results of training and questionnaire surveys conducted in the local government to which the authors belong. The results are reported here.

Keywords: Information Security Incident, Reporting Behavior, local public entity, Small local governments

1. はじめに

地方自治体では，法令等に基づき，住民の個人情報や企業の経営情報等の重要情報を多数保有しており，地方行政のデジタル化が進んだことで，この重要情報を扱う業務も情報システムで処理されるようになった．このことから，情報セキュリティの重要性も増しており，地方自治体の情報セキュリティ方針策定の推進のため，総務省の主導のもと，情報システムの状況や利用実態，パブリックコメント等から「地方公共団体における情報セキュリティポリシーに関するガイドライン」が平成 15 年 12 月に策定された．その後，継続的に改定が行われており，現状令和 5 年 3 月版が最新である[1].

多くの地方自治体は，「地方公共団体における情報セキュリティポリシーに関するガイドライン」に基づいて情報セキュリティポリシーを策定している[1]. 情報セキュリティポリシーでは，技術的セキュリティの他にも人的セキュリティ・制度的セキュリティとして職員への研修や適切な情報機器の取り扱い，インシデント報告等を求めており，職員は策定された情報セキュリティポリシーに遵守して業務を行わなければならない.

さらに, 政府は地方公共団体の行政サービスを含む 14 分野を，重要インフラ分野と特定し，サイバーセキュリティに係る行動計画を策定しており[2]，これに沿って自治体等に防護強化を求めている．自治体は住民サービスに影響がないよう事業継続するためのサイバーセキュリティが求められている.

このように情報セキュリティに関係する施策が実施されているにも関わらず，業種別の個人情報漏洩件数は公務が最も多いという事例が 2018 年に示されている[3]. また，インシデントの内容と発生した場所をまとめているサイトによると a，2023 年においても地方自治体は，メールの誤送信や，紛失，持ち出し等の情報セキュリティインシデン

1 長崎県立大学
University of Nagasaki

a Cyber Security.com の「 個人情報漏洩事件・被害事例一覧 」より.
https://cybersecurity-jp.com/leakage-of-personal-information#content2023

ト（以下「インシデント」という）を発生させており．全体 120 件中 8 件で約 6%が地方自治体である．令和 3 年度経済センサスによると国内の企業等数は 3,674,058 あり[4]，市町村数が 1,718（792 市，743 町，183 村）で占める割合が約 0.05%であることから，地方自治体が発生させたインシデント件数の割合（約 6%）は高いと考える．

インシデントが発生した際には，早期の対応が求められる．早期に対応を開始できれば，アクシデント（被害）に至らずにすむ可能性が高くなる．また，アクシデントに至ったとしても，被害拡大防止や迅速な復旧が期待できる．インシデントの早期発見のため，インシデントを発生させた職員が直ちにインシデントの「報告」を行う必要がある．しかし，インシデントを発生させた職員が「報告」せずに，外部からの通報によりインシデントが発覚することもあり，早期対応のタイミングを逃してしまう．

本研究では，インシデント時の職員の報告行動をはじめとする情報セキュリティ行動促進の要因について，著者らが所属する地方自治体で，研修とアンケート調査，テスト，インタビューにより調査・分析する．

本論文は，第 2 節で研究対象，第 3 節で研究課題，第 4 節で仮説設定，第 5 節でアンケート・テスト設計，第 6 節で分析，第 7 節で考察を述べる．

2. 研究対象

本研究では，総務省の示す地方公共団体の区分で示されている人口 5 万人以下の町村レベルにある地方自治体を対象としており[5]，著者らが所属する約人口 1 万人の地方自治体における現状の情報セキュリティの課題を抽出し，その課題に対して一助となる研究成果創出を目的としている．

小規模な地方自治体では，一般的に情報セキュリティ専任の担当者がおらず，情報セキュリティ業務を担う情報システム管理者でさえ，十分な知識を保有しているとは言い難い状況である．また，いわゆる「ひとり情シス」に代表される人員不足が問題となっており，約 10%の自治体が一人で情報システムを管理している [6] ．このことから，小規模な地方自治体では情報セキュリティ人材が質・数ともに不足している現状がある．

1 節で述べた通り多くの地方自治体は情報セキュリティポリシーを作成しているが，小規模な地方自治体では，ポリシーや実施ルールを設定していても，情報セキュリティの技術的な知識が不足しているために，実施が困難な内容もある．実際にインシデントレスポンスでログを確認することが必要だが，担当者の技術的な側面から実施が困難な可能性がある．また，このような状況から，情報システム管理者のみでなく，一般職員も十分に実施ルールを順守できているか疑問である．実際に，私が入庁してから，情報セキュリティの研修は実施されているが，一度も情報セキュリティポリシーの説明や研修は行われておらず，一般職員は情報セキュリティポリシーに触れる機会がない．

また，筆者らが所属する地方自治体では，役場のメールフィルターをすり抜けてマルウェア付きのメールが職員の PC にまで到達している．すり抜けた不審なメールを参考に自治体側のメールフィルターの設定を見直すことで不審なメールを防ぐことができるが，職員の技術的知識の不足により対応ができない．設定の見直しを適宜行うことで不審なメールの受信を減らすことは可能だが，完全に防ぐことは難しく，多層の防御対策が求められる．

このため，筆者らは，費用をかけずに多層の防御対策を実施することを考慮し，制度的セキュリティの情報セキュリティポリシーの策定に注目した．

この情報セキュリティポリシー策定の助けとするため，総務省は「地方公共団体における情報セキュリティポリシーに関するガイドライン」を策定・改定している．このガイドラインを活用することで，情報セキュリティの技術的な知識が不足している職員でも，策定・改定が可能である．実際に，多くの自治体はこのガイドラインを基に情報セキュリティポリシーの策定・改定を行なっている．

筆者らは，このガイドラインにおいて，職員は「情報セキュリティインシデントを認知した場合，速やかに情報セキュリティ管理者及び情報セキュリティに関する統一的な窓口に報告しなければならない」とされている点に注目している．

インシデント時の職員の報告行動は，早期のインシデント発見による早期のインシデント対応が可能となり，アクシデント（被害）に至らずにすむ可能性が高くなる．しかし，先に述べたが実施ルールである報告行動を一般職員が十分に遵守できているか疑問がある．

アクシンデントの中でも個人情報の漏洩は，漏洩した情報を使った 2 次被害等住民の影響も大きく，漏洩した自治体も，各機関への報告や，マスコミ対応などへの対応等影響が大きいため，優先し防ぐべきアクシデントである．

これまでの研究で，インシデント時の職員の報告行動の促進要因として，職員の予防能力と情報セキュリティポリシーの整備が重要であることが分かった[7]．しかし，情報セキュリティポリシーの整備とは，策定のみで効果があるのか，職員が理解する必要があるのか等の具体的な要素の特定ができていない．

このため，本研究では情報セキュリティポリシーの運用について注目し，情報セキュリティポリシーのどのような要素がインシデント時の職員の報告行動に影響を与えるか明らかにする．

3. 研究課題

本説では，2 節で示した研究対象に基づいて，課題分析を行い，本研究の研究課題について述べる．

職員の報告行動への影響として，情報セキュリティーポ

リシー運用の観点と，情報セキュリティポリシーの研修効果の観点から報告行動を促進する要因を分析する．

(1) 情報セキュリティポリシーのどのような要素が報告行動へ影響を与えているか.

情報セキュリティ行動の一つであるインシデント時の報告行動を促進する要因として情報セキュリティポリシーの整備があることが分かっている[7]．しかし，具体的にどのような要素が促進要因なのか研究ができていない．

このことから本研究では，情報セキュリティポリシーの策定や職員理解度等のどの要素が「報告行動」に影響があるか確認する．

(2) 情報セキュリティポリシーの研修が, 報告行動等へ影響を与えるか.

諏訪らは，情報セキュリティの知識が情報セキュリティ行動に影響を与えていることを示す情報セキュリティ行動モデルを構築している[8].

このことから本研究では，情報セキュリティポリシーの内容説明を中心とした職員向けのセキュリティ研修を実施することにより，「報告行動」等に影響があるか確認する．

以上 2 点を研究課題として，仮説を設定する．

4. 仮説設定

3 節で示した 2 点の研究課題について明らかにするために，H1 から H6 の仮説を作成した．

(1) 情報セキュリティポリシーのどのような要素が報告行動へ影響を与えているか.

H1 : 所属する自治体に情報セキュリティポリシーが整備されていることを知っている職員が報告する傾向にある．

H2 : 情報セキュリティポリシーに詳しい職員が報告する傾向にある．

また，報告行動を取るためには，インシデントにつながる事象を認識する必要があることから，この事象を認識する能力と情報セキュリティポリシーの運用，報告行動意図それぞれが影響を与えているか検証する．

H3 : インシデントにつながる事象を認識できる職員が報告する傾向にある．

H4 : 所属する自治体に情報セキュリティポリシーが整備されていることを知っている職員が，インシデントにつながる事象を認識できている．

H5 : 所属する自治体の情報セキュリティポリシーを理解している職員が，インシデントにつながる事象を認識できている．

(2) 情報セキュリティポリシーの研修が, 報告行動等へ影響を与えるか.

H6 : 情報セキュリティポリシーに関係する研修を受講した職員が報告する傾向にある．

5. アンケート・テスト設計

本節では，アンケート・テスト設計について述べる．

本研究の対象は町村レベルの小規模地方自治体としており，4 節で示した仮説を検討するため，筆者が勤務する地方自治体の職員を対象に，情報セキュリティポリシーに関連する対面の集合研修とアンケート調査・テストを実施する．

正規職員数が 112 名（令和 5 年 4 月 1 日時点）であり，対象に出来る人数が限られており, 対象人数を増やすため, パソコンを利用する会計年度任用職員を含めた全職員を対象にアンケート･テストを実施することとする. このため, 正規職員ではあるがパソコンを業務で利用しない調理員等を除いた．また，研修準備等で協力を得た情報システム担当職員も除き，約 140 名を対象とした．

5.1 仮説の検証方法

各仮説について検証方法を述べる．

(1) 情報セキュリティポリシーのどのような要素が報告行動へ影響を与えているか.

H1 は，研修の影響を受けていない，研修前のアンケートを使い，情報セキュリティポリシーを知っている群と知らない群について，報告行動意図の差を比較する．

H2 は，研修後，全員が情報セキュリティポリシーを知っている状況で，次の 2 点から検証する．

① 情報セキュリティポリシーについてアンケートでの主観の理解度の高い群と低い群で，報告行動意図の有無を比較する．

② 情報セキュリティポリシーの理解度テストでの理解度の高い群と低い群で， 報告行動意図の有無を比較する．

H3 は，研修の影響を受けないよう，研修前のアンケートとテストを用いて，次の 2 点から検証する．

① アンケートでの情報セキュリティについて主観の理解度の高い群と低い群で，報告行動意図の有無を比較する．

② インシデントにつながる事象を認識できるか測るテストにて理解度の高い群と低い群で，報告行動意図の有無を比較する．

H4 は, 研修前に情報セキュリティポリシーが組織にあることを知っている群と知らない群で，インシデントにつながる事象を認識できるか測るテストの結果を比較する．

H5 は，研修後に情報セキュリティポリシーの理解度を測るテストの結果と，インシデントにつながる事象を認識できるか測るテストの結果の関連を検討する．

(2) 情報セキュリティポリシーの研修が, 報告行動等へ影響を与えるか.

H6 は，次の 4 点から検証する．

① 情報セキュリティポリシーを知らなかった群に対し，

研修により情報セキュリティポリシーを知ったことで，報告行動意図が変化するか確認する．

② 研修を受けていない群と，受けた群で，報告行動意図に差があるか確認する．

③ 研修前に報告しなかった群が研修後，報告行動意図に変化があるか確認する．

④ 研修前後で報告行動意図に差があるか．

5.2 アンケート・テスト設計

研修とアンケート，テストは図 1 の流れとした．

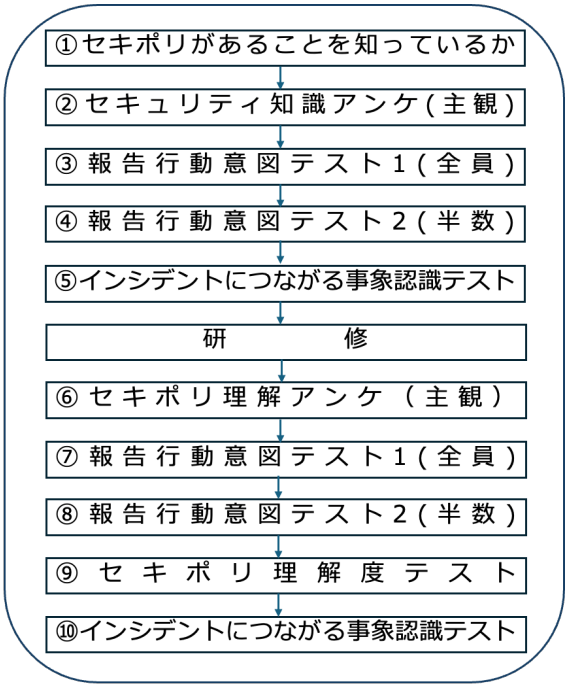

図 1 実験の流れ

なお，調査対象となる人数に限りがあるため，少ない人数で，複数の仮説を検証するため次の工夫を行なっている．

- 研修を受けた群と受けていない群の比較を行う際に，実際に半数に分けてしまうと，他のアンケートやテストの対象者が半減してしまうため，今回は研修を受ける前に該当のアンケートを回答した群を．研修を受けなかった群として整理した．

2 つ実施するテストの設問は次のとおり作成した．

① インシデントにつながる事象の認識テスト
JNSA の「知っておきたい情報セキュリティ理解度セルフチェック」から関連する 7 問を利用した[9].

② 情報セキュリティポリシー理解度テスト
総務省の「地方公共団体における情報セキュリティポリシーに関するガイドライン」から研修で説明する内容に関連する 7 問を作成した．

また，今回のインシデント事例は次の 6 つとした．なお，実際には報告を求めていない事例をダミー設問として 2 つ含めており，ダミー設問は分析しないこととする．

表 1 インシデントケース一覧

略称	インシデント事例
インシデントケース1	業務中，不審なメールの添付ファイルを開封した時，電算情報班に報告しないといけませんか？
インシデントケース2	個人情報を取り扱うシステムの個人のログインIDとパスワードを，他の職員に教えている所を見た時，電算情報班に報告しないといけませんか？
インシデントケース3	業務中，個人情報を含んだ電子メールの送信先を間違いました．電算情報班に報告しないといけませんか？
インシデントケース4	役場で利用しているUSBを紛失しました．電算情報班に報告しないといけませんか？
インシデントケース5	自宅のパソコンがウイルス感染した時，電算情報班に報告しないといけませんか？ **※報告求めていない　ダミー設問**
インシデントケース6	業務中，不審なメールが届きました．電算情報班に報告しないといけませんか？ **※報告求めていない　ダミー設問**

なお，アンケートとテストの設問は付録に示す．

6. 分析

本節では，仮説毎にアンケートとテストの集計結果を基とした分析について述べる．分析には，IBM SPSS Statistics28.0 を使用した．

(1) 情報セキュリティポリシーのどのような要素が報告行動へ影響を与えているか．

H1 から H5 について順に述べる．

H1 は，研修前アンケートの「情報セキュリティポリシーがあることを知っているか」と「インシデント時報告するか」の設問についてクロス集計を行ったが，差は見られなかった．

表 2 セキポリ整備とインシデントケース 1 の報告

組織に情報セキュリティポリシーがあることを知っている	報告無	報告有	合計	報告割合
はい	1	95	96	99%
いいえ	0	31	31	100%
合計	1	126	127	99%

表 3 セキポリ整備とインシデントケース 2 の報告

組織に情報セキュリティポリシーがあることを知っている	報告無	報告有	合計	報告割合
はい	10	86	96	90%
いいえ	3	28	31	90%
合計	13	114	127	90%

H2 は 2 つの方法で検証した．

① 研修後アンケートの「情報セキュリティポリシーは理解できましたか？」により主観の情報セキュリティポ

リシーの理解度による報告行動の差を見るため，クロス集計を行ったが，差は見られなかった．

表 4　セキポリ理解度（主観）とインシデントケース 1 の報告

情報セキュリティポリシー理解度（主観）	報告無	報告有	合計	報告割合
1(理解できた)	1	66	67	99%
2	2	51	53	96%
3	0	6	6	100%
4(理解できなかった)	0	1	1	100%

表 5　セキポリ理解度（主観）とインシデントケース 2 の報告

情報セキュリティポリシー理解度（主観）	報告無	報告有	合計	報告割合
1(理解できた)	2	65	67	97%
2	2	51	53	96%
3	0	6	6	100%
4(理解できなかった)	0	1	1	100%

② 研修後テストによる客観の情報セキュリティポリシー理解度による報告行動の差を見るため，クロス集計を行ったが，差は見られなかった．

表 6　セキポリ理解度（客観）とインシデントケース 1 の報告

情報セキュリティポリシー理解度テスト正答数	報告無	報告有	合計	報告割合
7	3	106	109	97%
6	0	17	17	100%
4	0	1	1	100%

表 7　セキポリ理解度（客観）とインシデントケース 2 の報告

情報セキュリティポリシー理解度テスト正答数	報告無	報告有	合計	報告割合
7	3	106	109	97%
6	1	16	17	94%
4	0	1	1	100%

H3 は 2 つの方法で検証した．

① 研修前アンケートの，「あなたは情報セキュリティに詳しいですか？」により主観の情報セキュリティの理解度による報告行動の差をみるためクロス集計を行ったが，差は見られなかった．

表 8　セキュリティ知識量（主観）とインシデントケース 1 の報告

情報セキュリティ知識量（主観）	報告無	報告有	合計	報告割合
1(詳しい)	0	2	2	100%
2	0	17	17	100%
3	0	48	48	100%
4(詳しくない)	1	59	60	98%

表 9　セキュリティ知識量（主観）とインシデントケース 2 の報告

情報セキュリティ知識量（主観）	報告無	報告有	合計	報告割合
1(詳しい)	0	2	2	100%
2	3	14	17	82%
3	5	43	48	90%
4(詳しくない)	5	55	60	92%

② 研修前のインシデントにつながる事象の認識テストの正答数による報告行動の差をみるため，クロス集計を行った．インシデントケース 2 で正答数が多い方が報告する傾向が見られた．このため，まずテストの正答数についてシャピロウィルク検定で正規性を確認し，正規分布でなかったことから，U 検定を実施したが有意確率が.282 であり，有意な差は見られなかった．

表 10　インシデントにつながる事象の認識テストとインシデントケース 1 の報告

インシデントにつながる事象の認識テスト正答数	報告無	報告有	合計	報告割合
7	0	25	25	100%
6	1	49	50	98%
5	0	29	29	100%
4	0	14	14	100%
3	0	6	6	100%
2	0	2	2	100%

表 11　インシデントにつながる事象の認識テストとインシデントケース 2 の報告

インシデントにつながる事象の認識テスト正答数	報告無	報告有	合計	報告割合
7	2	23	25	92%
6	4	46	50	92%
5	3	26	29	90%
4	3	11	14	79%
3	1	5	6	83%
2	0	2	2	100%

H4 は研修前アンケートの，「あなたは情報セキュリティポリシーがあることを知っていますか？」と研修前のインシデントにつながる事象の認識テストの正答数の関連をみるため，クロス集計を行った．あることを知っている群の平均点が高い傾向にあった．テストの正答数については正規分布でなかったことから，U 検定を実施したが有意確率が.150 であり，有意な差は見られなかった．

表 12　情報セキュリティポリシーがあることを知っていることとインシデントにつながる事象の認識の相関

組織に情報セキュリティポリシーがあることを知っている		インシデントにつながる事象の認識テスト正答数 2	3	4	5	6	7	合計	平均点
はい	人数	2	1	10	24	37	21	95	
	点数	4	3	40	120	222	147	536	5.64
いいえ	人数	0	5	4	5	13	4	31	
	点数	0	15	16	25	78	28	162	5.23

H5 は研修後テストによる情報セキュリティポリシーの理解度と，インシデントにつながる事象の認識テストの正答数の関連をみるため，クロス集計を行った．

情報セキュリティポリシーを理解している群の平均点が高い傾向にあった．テストの正答数については正規分布でなかったことから，U 検定を実施するため，表 14 の通り情報セキュリティポリシー理解度のテストの全問正答群とそれ以外の 2 群に分けたが，有意確率が.223 であり，有意な差は見られなかった．

表 13　情報セキュリティポリシーの理解度と情報セキュリティ理解度の相関

情報セキュリティポリシー理解度テスト正答数		インシデントにつながる事象の認識テストの正答数 3	4	5	6	7	合計	平均点
7	人数	3	8	17	49	32	109	
	点数	12	32	85	294	224	647	5.94
6	人数	1	2	3	7	4	17	
	点数	4	8	15	42	28	97	5.71
4	人数	1	0	0	0	0	1	
	点数	4	0	0	0	0	4	4

表 14　情報セキュリティポリシーの理解度と情報セキュリティ理解度の相関

情報セキュリティポリシー理解度テスト		インシデントにつながる事象の認識テストの正答数 3	4	5	6	7	合計
全問正答	人数	3	8	17	49	32	109
誤答有り	人数	2	2	3	7	4	18

(2) 情報セキュリティポリシーの研修が，報告行動等へ影響を与えるか．

H6 は 4 つの方法で検証した．

① 研修前アンケートで，セキポリがあることを知らなかった群が，研修でセキポリがあることを知ったことでの報告行動の変化を見るため，クロス集計を行ったが，差は見られなかった．

表 15　情報セキュリティポリシーを知らなかった者の研修前後でのインシデントケース 1 の報告行動意図

	報告無	報告有	合計	報告割合
研修前	0	31	31	100%
研修後	1	30	31	97%

表 16　情報セキュリティポリシーを知らなかった者の研修前後でのインシデントケース 2 の報告行動意図

	報告無	報告有	合計	報告割合
研修前	3	28	31	90%
研修後	0	31	31	100%

② 研修受けていない群と研修を受けた群で報告行動の差をみるため，クロス集計を行ったが，差は見られなかった．

表 17　インシデントケース 3 の研修前後の報告行動意図

	報告無	報告有	合計	報告割合
研修無し	2	58	60	97%
研修有り	2	65	67	97%

表 18　インシデントケース 4 の研修前後の報告行動意図

	報告無	報告有	合計	報告割合
研修無し	0	60	60	100%
研修有り	1	66	67	99%

③ 研修前に報告しなかった群が，研修を受けた後，報告行動に差を見る予定であったが，研修前に報告しなかった群の対象数が少なすぎたため分析できなかった．

④ 研修前後で報告行動の差をみるため，クロス集計を行った．インシデントケース 3 では報告する者が増加する傾向にあったが，ケース 1 では報告しない者が増加した．

表 19　インシデントケース 1 の研修前後の報告行動意図

	報告無	報告有	合計	報告割合
研修前	1	126	127	99%
研修後	3	124	127	98%

表 20　インシデントケース 2 の研修前後の報告行動意図

	報告無	報告有	合計	報告割合
研修前	13	114	127	90%
研修後	4	123	127	97%

研修前も高い報告割合であったが，研修後さらに報告割合が高くなり研修の効果が見られた．しかし，インシデントからのアクシデントを職員の誰かが 1 件でも発生させてしまうと組織として大きな問題となるため，研修後も報告しなかった者についてさらに分析を行う．

報告しなかった者はケース 1 とケース 2 を合わせると 7 名であった．ただし，ケース 1 とケース 2 両方で報告をしない職員が 2 名おり，分析すべき職員は実質 5 名である．

その 5 名について，研修前と研修後の違いを比較してみると表 21 のようになる．

表 21　報告しない者の人数

No	研修前	研修後	人数
1	報告する	報告しない	3
2	報告しない	報告しない	2

大きく分けて No.1（研修前に報告するが研修後に報告しないに変化）と No.2（研修前・研修後とも報告しない）の職員がいる．この 5 名にインタビューを試み，考察するこ

とにした．

No.1 では報告するとしていたのに，報告しないにしたことの理由を 3 名にインタビューした．回答は以下である．

① 設問では報告先が情シス部門となっていたが，研修では，情シス部門と所属長への報告が求められていたため，報告先が不足していると誤解をし，報告しないに変更した．

② 今，設問を読むと報告しなければいけないと答えるが，研修後の設問を誤って解釈したのではないかと思う．（2 名）

No 2 はなぜ，研修前後ともに報告しないことを選択した理由を 2 名に確認することにした．回答は次の通り．

③ 現状 ID とパスワードを同僚に教えており，報告することでパスワード共有ができなくなり業務に影響が出ると考えた．

④ 不審なメールの着信が多く，全て報告すると報告を受ける情シス部門の負担になると考えた．

7. 考察

6 節の分析結果と，その結果の活用について述べる．

7.1 分析結果

3 節で示した 2 点の研究課題に対し，4 節で示した 6 個の仮説を検証した．

仮説全てで統計的に有意な差を見つけることができなかった．これは報告行動意図について，以前実施したアンケートでは[5]，同様のインシデントに対し報告する割合が 83.4%(1,000 人中 834 人)であり，著者が所属する団体でも同程度の割合を見込んだが，結果は 99.2%と大きく偏ってしまい分析が困難となってしまったことが理由にあげられる．

以前の調査では正規職員を対象としたが，職種を絞っていなかった．住民の情報を多く取り扱う公務員は報告行動意図が高いと考えられる．

また，今回は著者が所属する小規模自治体を対象に調査を実施したが，統計分析にあたってはサンプル数が不足している．

ただし，今回のアンケートとテストは職場の約 9 割が実験に参加しており，自身が所属する自治体のみでの調査は限界がある．対象者数を増やすためには，他自治体への協力依頼が必要であるが，組織文化が異なる等，他自治体を含めての分析には課題もあるため，十分な検討が必要である．

7.2 研修の効果

統計的に有意な差を見つけることはできなかったが，クロス集計で見た中では，インシデントにつながる事象の認識テストの点数が高い者が，報告行動意図が高い傾向にあった．研修前後で実施したインシデントにつながる事象の認識テストでは次の表の通り平均値が向上しており，報告行動促進の効果が期待できる．

表 22　インシデントにつながる事象の認識テストの研修前後の差

	有効人数	欠損値	平均値	標準偏差
研修前	126	1	5.54	1.164
研修後	127	0	5.85	1.047

次に，インタビューで判明した報告しない 4 つの理由について考察する．

No.1 の①は，研修内容と設問の報告先の違い（情シス部門のみ，情シス部門と所属長）が原因であった．今後研修やテストする際には誤解がないよう整合性をとり資料を作成すべきであると考える．

No.1 の②は，インシデントにつながる事象について正しく認識できていなかった，または，正しく理解できていなかったと考える．具体的な事象を示すなど研修内容を見直し理解しやすく，また，それが薄れないように定期的に研修を行うことで，職員が正しく事象を認識できるようにしたい．

No.2 の③は，現状行っている業務のやり方がこれまでアクシンデントを起こさなかったからと良いわけではなく，安全ではないことを研修等で引き続き教育する．改善が見られない場合は，上司から注意喚起する等の対応を検討したい．さらに，ポリシーに準拠より業務効率を優先すべきでないことをトップ層から周知してもらうことも必要かもしれない．

No.2 の④は，研修でアクシデント対応よりも報告を受けての対応が情シス部門や組織として望ましいことの認識の定着や，報告しやすい環境作りを検討したい．

8. おわりに

地方自治体職員は緊急性の高い連絡を受けるため，表題が多少怪しかろうがメールを開かざるを得ない場面があり，インシデントに対峙するケースも多いと考えられる．住民の生命と財産を守ることが最大の使命であることから，このようなインシデント時に早期対応ができるよう速やかな報告が求められる．

情報セキュリティポリシーが多くの団体で整備済みではあるが，定期的なポリシーや実施ルールの見直し，研修による職員の理解の向上等継続しての取組みが求められている．今後の研修等に今回の研究が参考になることを期待する．

なお，著者が所属する団体は報告行動意図が非常に高い割合であったが，意図があっても行動をとるかわからない．今後訓練で意図と行動が一致するか検証したいと考えている．

参考文献

[1] “地方公共団体における情報セキュリティポリシーに関するガイドライン”．
https://www.soumu.go.jp/main_content/000805453.pdf, (参照

2024-02-12).
[2] “重要インフラサイバーセキュリティに係る行動計画“. https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf, (参照 2024-02-12).
[3] “2018 年情報セキュリティインシデントに関する調査結果～個人情報漏えい編～(速報版)”. https://www.jnsa.org/result/incident/2019/2019-005.pdf, (参照 2024-02-12).
[4] “令和 3 年経済センサス-活動調査 調査の結果”. https://www.stat.go.jp/data/e-census/2021/kekka/index.html, (参照 2024-08-18).
[5] “地方自治制度　地方公共団体の区分”. https://www.soumu.go.jp/main_sosiki/jichi_gyousei/bunken/chihou-koukyoudantai_kubun.html, (参照 2024-08-23).
[6] “地方自治体における業務プロセス・システムの標準化及び AI・ロボティクスの活用に関する研究会（スマート自治体研究会）”. https://www.soumu.go.jp/main_sosiki/kenkyu/process_ai_robo/index.html, (参照 2024-08-16).
[7] 岡佳伸，藤本恵莉華，島成佳，小松文子. 情報セキュリティインシデントの初期発見につながる「報告」行動の要因分析. SPT, 2024, vol. 54, no. 26, p. 1-8.
[8] 諏訪博彦，原賢，関良明. 情報セキュリティ行動モデルの構築―人はなぜセキュリティ行動をしないのか. 情報処理学会論文誌,2012, vol. 53, no. 9, p. 2204-2212
[9] “知っておきたい情報セキュリティ理解度セルフチェック”. https://slb.jnsa.org/slbm/benchmark, (参照 2024-08-01).

付録

アンケートとテストの設問は次のとおりである.

表 23　研修前アンケート（全職員対象）設問

No	設問	回答群
1	本町に情報セキュリティポリシーがあることを知っていますか？	はい・いいえ
2	あなたは情報セキュリティに詳しいですか？	4段階（詳しい-詳しくない）

表 24　研修後アンケート（全職員対象）設問

No	設問	回答群
1	情報セキュリティポリシーは理解できましたか？	4段階（理解できた-理解できなかった）

表 25　報告行動意図テスト 1（全職員対象）設問

No	設問	回答群
1	業務中，不審なメールの添付ファイルを開封した時，電算情報班に報告しないといけませんか？	はい・いいえ
2	自宅のパソコンがウイルス感染した時，電算情報班に報告しないといけませんか？	はい・いいえ
3	個人情報を取り扱うシステムの個人のログインIDとパスワードを，他の職員に教えている所を見た時，電算情報班に報告しないといけませんか？	はい・いいえ

表 26　報告行動意図テスト 2（半数）設問

No	設問	回答群
1	業務中，不審なメールが届きました．電算情報班に報告しないといけませんか？	はい・いいえ
2	業務中，個人情報を含んだ電子メールの送信先を間違いました．電算情報班に報告しないといけませんか？	はい・いいえ
3	役場で利用しているUSBを紛失しました．電算情報班に報告しないといけませんか？	はい・いいえ

表 27　インシデントにつながる事象認識テスト設問

No	設問	回答群
1	社長から「添付ファイルの情報に基づき、取引先に至急お金を振り込むよう」メールで指示がありました。この時の行動で最も適切な行動はどれでしょうか？	4択
2	企業のITセキュリティを高める上で適切でない考え方はどれでしょうか？	4択
3	USBメモリーを執務室で拾った場合、最も適切な対応はどれでしょうか？	4択
4	SNS/クラウドサービスを利用する際の注意点として間違っているものはどれでしょうか？	4択
5	電子メールの安全性や信頼性に関する記述のうち、適切なものはどれでしょうか？	4択
6	ファイルを開くパスワードを忘れてしまったので教えてほしいと電話がありました。そのときの対応として最も望ましくないものはどれでしょうか？	4択
7	電子メールを送る際、鈴木さんをメインの宛先とし、山本さん、田中さんには「参考までに知っていて欲しい」というかたちでメールを送りたいと思います。また、田中さんにメールを送っていることを他の人に知らせたくないような場合のTo.Cc.Bcc設定方法として適切なものはどれでしょうか？	4択

表 28　情報セキュリティポリシー理解度テスト設問

No	設問	回答群
1	情報セキュリティの対象に印刷物は含まれない.	はい・いいえ・わからない
2	情報セキュリティポリシーに違反すると役場から処分される.	はい・いいえ・わからない
3	情報セキュリティに関する研修・訓練は定期的に実施しなければならない.	はい・いいえ・わからない
4	情報セキュリティインシデントを認知したが，電算情報班が不在なら報告しなくても良い.	はい・いいえ・わからない
5	緊急の対応が発生する可能性があるため，IDとパスワードを同僚に教えても良い.	はい・いいえ・わからない
6	ソフトウェアのサポートが終了したが，動作に問題がないため利用し続けても問題ない.	はい・いいえ・わからない
7	電子メールで個人情報を送信する場合は，暗号化しなければならない.	はい・いいえ・わからない