身の回りにあるミニマムなシステム監査の検討

Research on system auditing for minimal information systems around us

「監査の適合性チェックとコンサルティング機能の実効性・有効性の達成」
研究プロジェクト（2023年度）

木村 裕一、赤尾 嘉治、稲留 和紀、 尾崎 孝章、仁井 健友、 深瀬 仁、 月見 典史

目次

別途報告書を作成中。

第一編　1．プロジェクト発足の経緯

1．1研究の経緯

- ・どの企業も実施がしやすい身近なテーマから、監査を知ってもらう。
- ・IPAの10大脅威への対策の度合いを確認し、セキュリティ対策の一環として考える。
- ・バックアップを切り口に、他のセキュリティ項目への関心を持ってもらう。

1．2　プロジェクトの内容

種類	内容
テーマ	身の回りにあるミニマムなシステム監査の検討 ランサムウェア対応のミニマム監査チェックリスト作成と実践
研究の狙い	身近な課題に対してシステム監査を実施し意義を実感してもらう、普及啓発活動の一環 ランサムウェアによる被害を想定した場合に備えた、適切なバックアップが取得できているか。 取得したバックアップを利用しての情報システム復旧の手順は確認しているか。
研究報告	研究報告書を作成　　随時内容を集約し、まとめる ミニマム監査の実践　　内部監査用手順としてまとめる
成果発信	研究大会へ参加・発表　　ｽﾗｲﾄﾞを作成、発表、ニュース記事作成
研究成果活用	研究成果の普及啓発　　監査を必要としている組織にどのようにして届けるのかの方法

1．3 検討過程での研究テーマの絞り込み

検討項目	検討内容
セキュリティ脅威への対策	IPAの「情報セキュリティ10大脅威」にあるように、セキュリティ脅威への対策の見直し・レベルアップの必要性を感じている。
事業継続（BCP）	ランサムウェア対応、情報BUの究極の目的は事業継続であり、それが実現できるかの確認が必要
情報システムへの要求事項	情報システムで提供するサービスが顧客に浸透するに従って、信頼性への客観的評価を提示する必要性が生まれてきた。
内部監査の役割	実際に情報システムの監査をするのに、システム技術の人材はいるが監査のスキルを持っている者が少ない。監査がチェックや診断としての役割を果たせないのか
監査員のスキル	ミニマム監査では、監査員には一般的な監査以上にスキルや品質が必要である。人材で適任者がいないことが課題となる。
身の回りにあるミニマムなシステム監査	上記のニーズや課題に対応できる情報システム監査を考えたときに、現状の監査では監査対象組織の負荷が大きく躊躇することも考えられる。そのため、「ミニマム監査」を提示することを試みる。

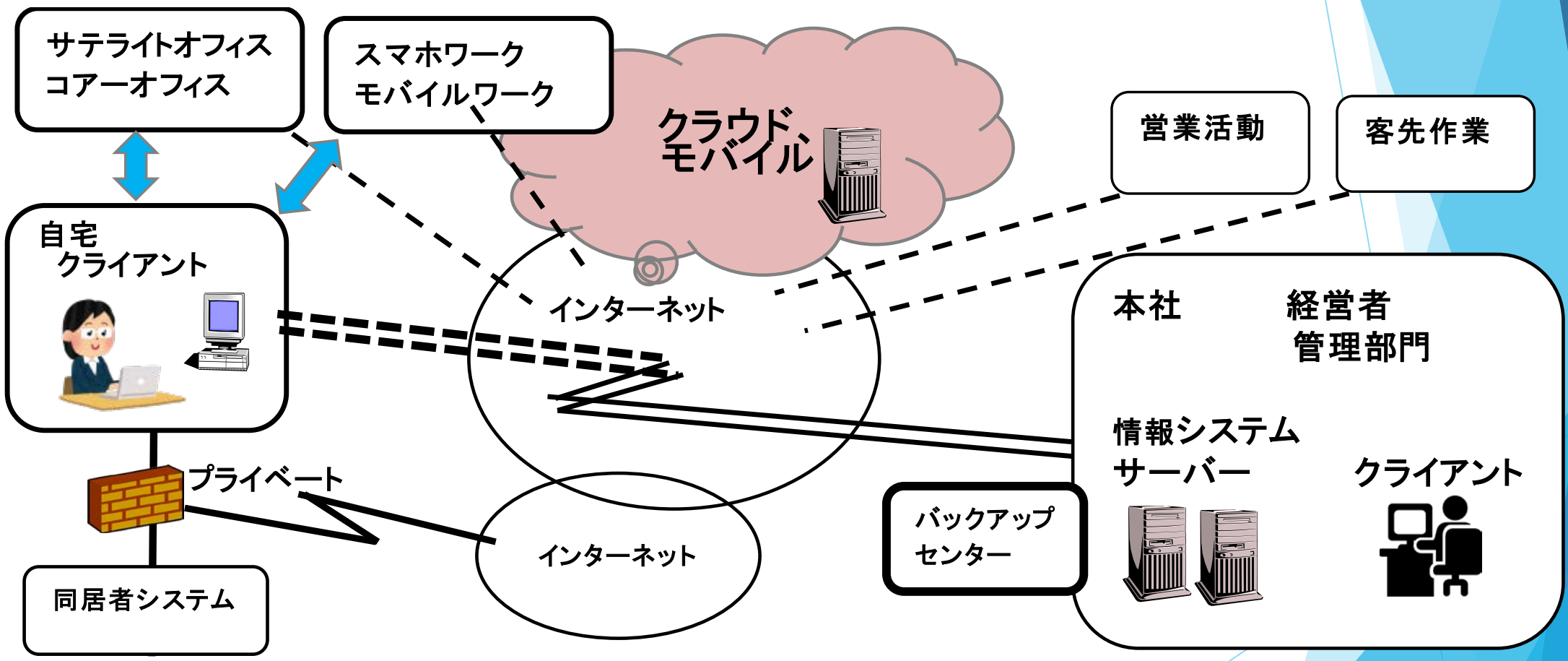
第二編　検討課題

1．セキュリティ脅威への対応　　IPA情報セキュリティ10大脅威

情報セキュリティ10大脅威 2023とバックアップのリスク対応への効果

順位	個人	効果	組織	効果
1位	フィッシングによる個人情報等の詐取	無	ランサムウェアによる被害	有
2位	ネット上の誹謗・中傷・デマ	無	サプライチェーンの弱点を悪用した攻撃	無
3位	メールやSMS等を使った脅迫・詐欺の手口による金銭要求	無	標的型攻撃による機密情報の窃取	無
4位	クレジットカード情報の不正利用	無	内部不正による情報漏えい	無
5位	スマホ決済の不正利用	無	テレワーク等のニューノーマルな働き方を狙った攻撃	無
6位	不正アプリによるスマートフォン利用者への被害	多少	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）	無
7位	偽警告によるインターネット詐欺	無	ビジネスメール詐欺による金銭被害	無
8位	インターネット上のサービスからの個人情報の窃取	無	脆弱性対策の公開に伴う悪用増加	無
9位	インターネット上のサービスへの不正ログイン	多少	不注意による情報漏えい等の被害	無
10位	ワンクリック請求等の不正請求による金銭被害	無	犯罪のビジネス化（アンダーグラウンドサービス）	無

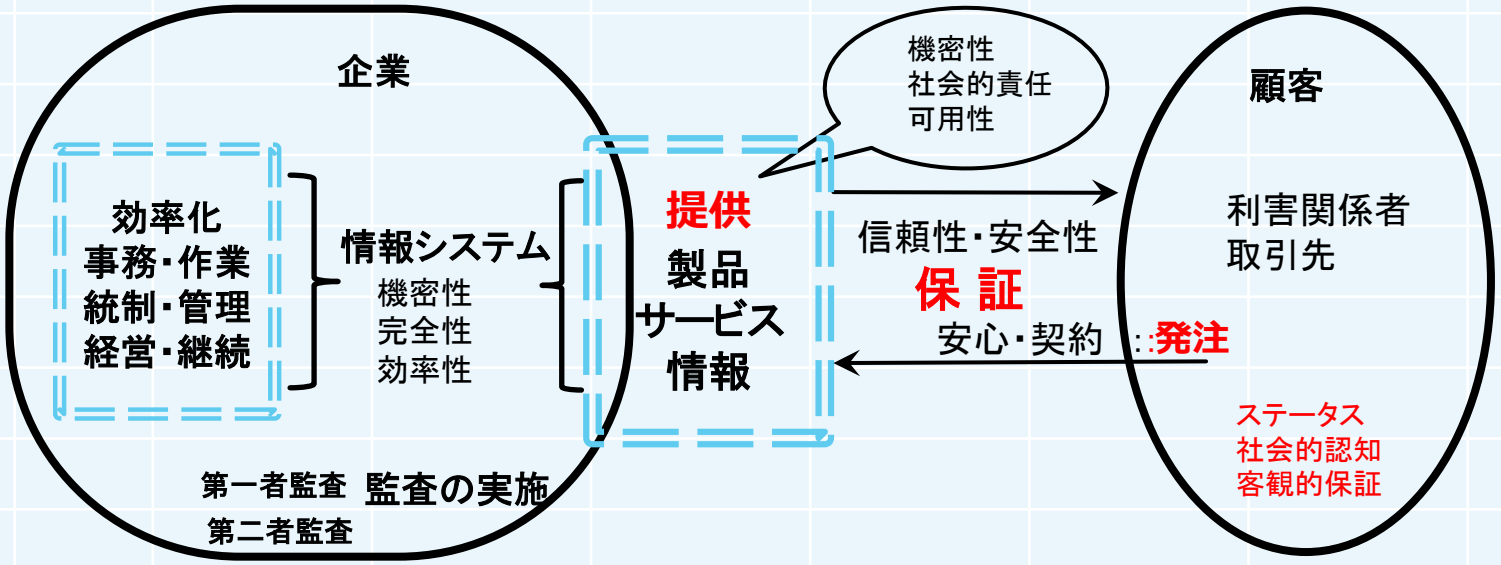
２．情報システムの形態のイメージ　監査対象



３．監査対象組織の情報システム形態とリカバリー

システムの形態	トラブル原因	主要なリカバリー法
クラウド	サービス停止	自社でのリカバリー手段は難しい バックアップサイトの契約、随時情報のバックアップ取得
自社サーバ	システム、情報の障害	バックアップ・リカバリー
PC	システム、情報の障害	シンクライアント化、リストアー
スマホ、モバイル端末	原因の特定が困難	設定内容の見直し、買い替える

4. 情報サービスの信頼性　客観的評価を顧客に提示する必要性



5．既存の監査の種類と狙い

監査の要求	監査の種類	監査を通しての本音の狙い
法規制	会計監査 内部統制監査 業務監査	会社法、金融商品取引法　**遵法** 内部統制報告制度（J-SOX）会社法第381条1項、監査役、e-文書法
ISO・JIS 認証取得	ISO等の監査 QMS、ISMS、EMS等 Pマークの監査（審査）	JIS Q 19011 マネジメントシステム監査のため、 プライバシーマーク付与適格性審査基準、JIS Q 15001　等 **認証維持管理**
告示等	システム監査 情報セキュリティ監査	信頼性、安全性、効率性。それ以外認証などは他の監査でカバーしている お付合い　役所向けアピール
契約上の要求	取引先監査	契約に基づき、顧客・取引先が実施する **取引優先**、顧客満足度の向上
自社での業務改善	規程・手順の執行監査 是正・改善処置	社内規程類、手順書、マニュアル　の**妥当性** 隘路、生産性などの**改善**
自社内情報共有 相互理解	部門間相互監査	**情報共有**、相互啓発、切磋琢磨、
社員教育 社内啓発	名目的監査	必要性教育、担当者育成、社内啓発 実際の監査を通じてOJT実施がほとんど

6. 監査員のスキル（抜粋）

ヒアリング対応者を理解できるスキル

対応者	主要な職務上の観点
社長（経営者） 取締役 経営幹部	・現状把握、経営の観点　・企業存続 ・ランサムウェアへの方針 ・ランサムウェアへのリスクの認識度合いと対応方針 ・該当項目の認識度合い関与度合い
担当役員 （業務部門長）	・対顧客の観点　・事業継続 ・業務部門長としての責任範囲と関与度合い
業務管理者 業務担当者	・業務管理完遂の観点　・セキュリティ管理 ・実業務での関連と規程等の周知状況
情報システム管理者等	・セキュリティ対策　・情報システムの復旧 ・構成管理、運用管理、安全確認　事故、障害管理 ・対策の技術面については被監査外
情報システム利用者	・日常のルーチンワーク　・異常の早期発見対応
新入社員	・教育・訓練的　・情報システム利用者と同じ
協業の社員	・日常のルーチンワーク　・情報システム利用者と同じ

第三編　ミニマム監査へのアプローチ

1．ミニマム監査の導入組織のニーズ例

★自社防衛のため、IPAの「情報セキュリティ10大脅威」などセキュリティ脅威へ対応することを意識している。

★情報システムで提供するサービスが顧客に対する、信頼性への客観的評価の必要性を意識している。

★情報システム監査の試行に当たってシステム技術と監査のスキルを持った適任者がいないことを意識している。

★上記のニーズや課題に対応できる情報システム監査を体験してもらいたいと考えている。

２．ミニマムなシステム監査研究の成果物

研究結果		内容
成果物	ベースチェックリスト	ミニマム監査時に使うカスタマイズ可能なチェックリストを作成
	個別の監査計画書（ひな型）	監査の計画段階で明らかにするべき事項を整理する資料
	監査報告書（ひな型）	監査対象組織への確認、目的、監査範囲、運用の把握 報告の内容にレーダーチャートなどを導入

３．ミニマム監査と普通の監査との違い

以下のような違いがある

①啓発が主眼であるので、監査対象をミニマムに、要求事項・条件を最小限にする。
②基準文書といわれるものが存在しないので、本報告書のベースチェックリストを作成し利用する。
③ミニマムなので監査対応者に社長（経営者）は含めない。
④監査範囲は規模の拡大を抑えるためサンプリングも考慮する。

・監査目的の達成により、監査体験から得られる監査の必要性や有効性を明確にして効果をアピール

４．実施に向けての前提条件

バックアップの目的

システム管理基準では、バックアップ活動として、①バックアップ手順の策定、②バックアップ手順の検証を要求している。

ランサムウェアによる被害を想定すると、バックアップの取得は情報システムの復旧に役立ってこそ意味がある。そのため、バックアップが有効であるかは、復旧までを評価して成果をアピールする必要がある。

最終的にはバックアップ取得に限定せず、被害防止対策に焦点を当てたシステム監査を考えることになる。

４．実施に向けての前提条件

ベースチェックリスト

既存の基準文書では対応するものが見当たらない。よって基準文書となる「ベースチェックリスト」を策定することにした。チェックリストは汎用性を高くして、監査に当たってカスタマイズする。

① 監査対象企業の情報システム環境、監査対象組織体制によってカスタマイズする。

② チェックリストはシステム形態別に考える。

③ カスタマイズした「個別チェックリスト」を準備する。

カスタマイズには、例えば外部委託、業務優先順位、リソース状況などの考慮要素がある。

このチェックリストは内部監査の利用が前提ですが、外部監査や監査の形態でなくシステムチェック・確認での利用も可能としている。

４．実施に向けての前提条件

監査結果に対する保証

経営者が期待する事は、“ランサムウェアの被害に遭わないこと”である。しかし、システム監査実施の結果、「ランサムウェアの被害に遭わないと言えるか」の問いには保証はできない。

①ランサムウェア対策に関して高度な技術を持って監査をしても、被害に遭わない保証はできないと考える。

②当チェックリスト及び当研究の範囲での監査では、情報システム管理に対する対策の技術面はこのチェックリストの監査対象外とした。

③当監査は助言型である。

当監査は最終的に、システム管理基準に即したシステム監査基準で実施されることを目指している。

５．ミニマム監査の実践効果

（１）良い点　　情報システム管理の基本の確認

- セキュリティ対策の一環として、監査を知ってもらう。
- バックアップを切り口に、他のセキュリティ項目やランサムウェア対応への関心を持ってもらう。
- 企業としての事業継続計画の充実へテーマを拡げることが出来る。
- 情報システムの技術的統制のチェック、自社サーバとクラウドの活用のバランスを見直すことに寄与できる。
- 情報資産と管理方法の見直しへの機会となる。
- 情報システム管理、運用体制の改善や改革のきっかけとなる可能性がある。

５．ミニマム監査の実践効果

（２）不十分な点

- ランサムウェア対策の技術面には保証が出来ないことから、技術面の欠点を指摘してもらいたい要望の企業の期待に応えられない。
- 監査対象組織のセキュリティ対策の成熟度が監査成功のカギとなる。
- 監査対象組織の情報システムによっては、簡単にすぎる内容となる。
- 監査対象組織への適応に際しての監査員の事前準備がかなりの労力を必要とする。

５．ミニマム監査の実践効果

（３）発展的計画

ミニマムであることの制約があり、それを次回以降の監査で補ってゆく。例えば、

１回目情報システム形態別に考えたが、

２回目管理プロセス、

３回目以降はシステム監査基準により選別したテーマなどを計画する。

第四編　ランサムウェア対応のミニマム監査の実践

監査業務の実践手順

- 監査の実施の経営判断　⇒　ミニマム監査の準備活動開始
- 本研究のチェックリストを基に　⇒　**個別チェックリストを作成**
- 個別監査計画書を作成
- 監査の実施　⇒　監査報告書
- 監査のトップレビュー　⇒　改善計画　⇒　改善
- 改善結果のフォローアップ監査　⇒　トップに報告と監査効果のレビュー
- 次回監査のための記録等の文書管理
- 次年度以降の年度監査計画書作成

⇒　２回目以降の監査の準備活動開始

２．個別チェックリスト例　対象システムの数だけ準備

No.	バックアップ監査項目 （〇：実施、△：一部実施、×：未実施）	選択肢、設問に対する確認内容	クラウドサービスA	〇：適合 △：観察 ×：指摘	点数
1	保護が必要な情報のバックアップを実施しているか	（実データ、設定情報、法定保管年限が求められるデータなど）	〇		1
2	バックアップは決められたスケジュールで実施しているか	（頻度の決定、未完了の確認）	〇		1
3	取得したバックアップを安全に保管しているか	（ウイルス感染チェック、アクセス制限、施錠保管など）	〇		1
4	直近取得のバックアップが破損していても、他のバックアップデータを確保しているか	（2世代以上の世代管理）	〇		1
5	上記バックアップ及び復元の手順を定めているか	（訓練結果に基づく手順の改善、改訂がなされているか）	〇		1
6	バックアップ及び復元に対する演習や訓練をしているか	（必要データの復元確認、復旧時間の確認、DB等のシステム間の整合など）	〇		1
—	サービスA点数				6

3．個別監査計画書（ひな型）

配布先	**個別監査計画書**	システム監査学会	
		研究プロジェクト	
		日付	監査責任者

〇〇　取締役社長　殿

標記の監査を以下のように計画・提示いたします.

1. 種　別: □ 定期　□ 臨時　□ その他、　形 態: □ 対面式　□ オンライン

2. 監査方針: 業務運用において従来行われている対応などが、ランサムウェアなどの最近の脅威・リスクに対して、客観的に確実であるかどうかの監査を行う

3. 監査範囲及び監査対象組織

3. 1監査範囲

チェックリストにあるクラウドサービスの被監査（サービス A,・・）、社内サーバ（サーバ A,・・）、パソコン（業務 A,・・）、スマホ等の監査範囲の中で、監査チームの検討結果に基づき決定させていただきます。

3. 2被監査者: 以下の方々へのヒアリングを希望します。監査対応に関わる方を選定し対応してください。

監査対象組織、役職	主な監査範囲、確認事項等	監査対応者名　複数名可
①　担当役員	セキュリティ対策体制、インシデントの状況、事業継続計画、利害関係者への対応	
②　業務管理者	リスク対策の整備、情報の管理、日常の管理活動、復旧への要求事項、活動	
③　情報システム管理者等	情報システムの管理、運用管理 リスク対策の整備、資産の管理、 日常の管理活動、復旧への活動	
④　情報システム利用者	日常の管理活動、復旧への活動	

対応いただける対応者の範囲で十分な確認ができないと考えられる場合に、監査範囲が限定されることが有ります。

4. 監査基準文書:

監査チームとしては**「ランサムウェア対応のミニマム監査の個別チェックリスト」**をベースにしたもので進めてまいります。

必要に応じて、手順書、規程類は下記に該当する文書等を想定して監査を行います。

・情報システム管理の文書・規程・マニュアル等

・セキュリティ対策の文書・規程・マニュアル等

・インシデント発生時の対応の文書・規程・マニュアル等、

5. 監査チームの構成

監査リーダ：

メンバー　：

6. 実施日時: 事前準備　月　日（ ）、

監査　　月　日（ ） 監査スケジュールは下記監査スケジュールのとおり

7. 会　場:: 会議室又は各部門の執務室　他、

8. 監査スケジュール （サンプル）

〇月〇日（〇

	項目、監査内容	被監査者	監査員
9:00	集合	監査の窓口管理者	
9:00～9:10	オープニングミーティング 監査方法、前提条件の確認 計画全体、及び監査結果報告の実施方法を確認	社長、担当役員 関係者	
9:10～11:30	・被監査者へのヒアリング、実地検証 ・実地検証、現地、現物確認の被監査 ・クラウド、自社サーバ、PC、スマホ、等 ＊監査範囲が増えた場合は時間を延長いたします	対応者	
11:45～12:00	監査結果の要点報告	社長、担当役員 関係者	

9. 結果報告

監査結果は監査報告書としてまとめ、後日提出の予定

また、改善結果のフォローアップ監査等の目途が立った時点で、トップへの報告と監査レビューを予定

以上

3．個別監査計画書（スケジュール (例) ）

ミニマムな監査のイメージ

	項目、監査内容	被監査者	監査員
9:00	集合	監査の窓口管理者	
9:00～9:10	オープニングミーティング 監査方法、前提条件の確認 計画全体、及び監査結果報告の実施方法を確認	社長、担当役員 関係者	
9:10～11：30	・被監査者へのヒアリング、実地検証 ・実地検証、現地、現物確認の被監査 ・クラウド、自社サーバ、PC、スマホ、等 ＊監査範囲が増えた場合は時間を延長いたします	対応者	
11:45～12：00	監査結果の要点報告	社長、担当役員 関係者	

４．監査報告書

（１）システム監査報告書は、報告書ひな型「A-05ミニマム監査報告書」を参考に作成

- ①本テーマについて、関係者に「これだけのことを得られた」と有益な効果をもたらせること。
- ②当システム監査の結果を踏まえて、継続して監査を実施することの有効性の理解を得ること。

- **（２）監査結果をシステム形態別の観点から評価（報告書A-03レーダーチャート作成　参照）**
  ①情報システム評価の集計表に今回のチェックリストをコピーして集計用の準備をする。
- ②監査結果に対し　〇：適合,１点　△：観察、0.5点　×：不適合,0点　を配点する。
- ③評価集計表に質問項目として選択したすべての質問数（X）を集計する。
- ④評価集計表に監査結果で適合だった項目のすべての適合数及び観察の配点を集計（Y）する。

４．監査報告書（ひな型）

配布先	**個別監査報告書**	システム監査学会	
		研究プロジェクト	
		日付	監査責任者

〇〇　取締役社長殿

情報システムの関係部署に対して標記のシステム監査を実施いたしましたので、ご報告いたします。

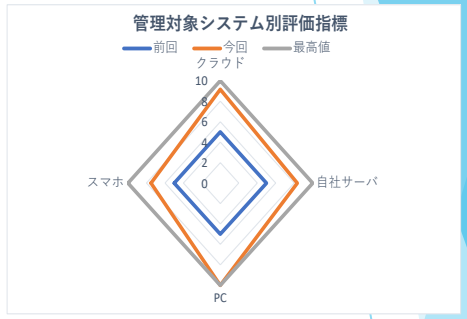
監査対象部門　：　　対象システム：
監査範囲　：
実施日：
対応者：担当役員、業務部長　　〇〇氏
　　情報システム管理者　　〇〇氏
　　口部口課係　　〇〇氏
監査員：

監査基準文書：
・ランサムウェア対応のミニマム監査個別チェックリスト
・貴社作成の手順書、規程類、
・情報システム管理、セキュリティ対策、インシデント対応、等に関する文書・規程・マニュアル等

監査結果
早急に対応の必要な事項は以下の通りです。
① 顧客に関連することで、早急に対応が必要である事項
a1）
a2）
② 事業継続に関連して、対応が必要である事項
b1）
b2）

情報システムの形態に関連する観点からの事項

管理対象システム	前回	今回	最高値
クラウド	5	9.2	10
自社サーバ	5	8.3	10
PC	5	10.0	10
スマホ	5	7.5	10



レーダーチャートからの所見
①各管理プロセスは前回の監査より改善がみられる。
②しかし、「スマホ」においては対応の改善を更に進める必要がある。
① クラウドの安全性が高いので、サービスをクラウドか自社かの選択をリスクベースで検討する必要と思われる。
また、クラウドサービス側で行うバックアップと、自社として手元にデータを残すバックアップの 2 種があるため、被監査ごとにリスクを精査する必要があると感じます。

情報システムの形態別の観点からの事項
（1）クラウド利用
（2）自社管理サーバ
（3）PC 関連
（4）スマホ、携帯端末等

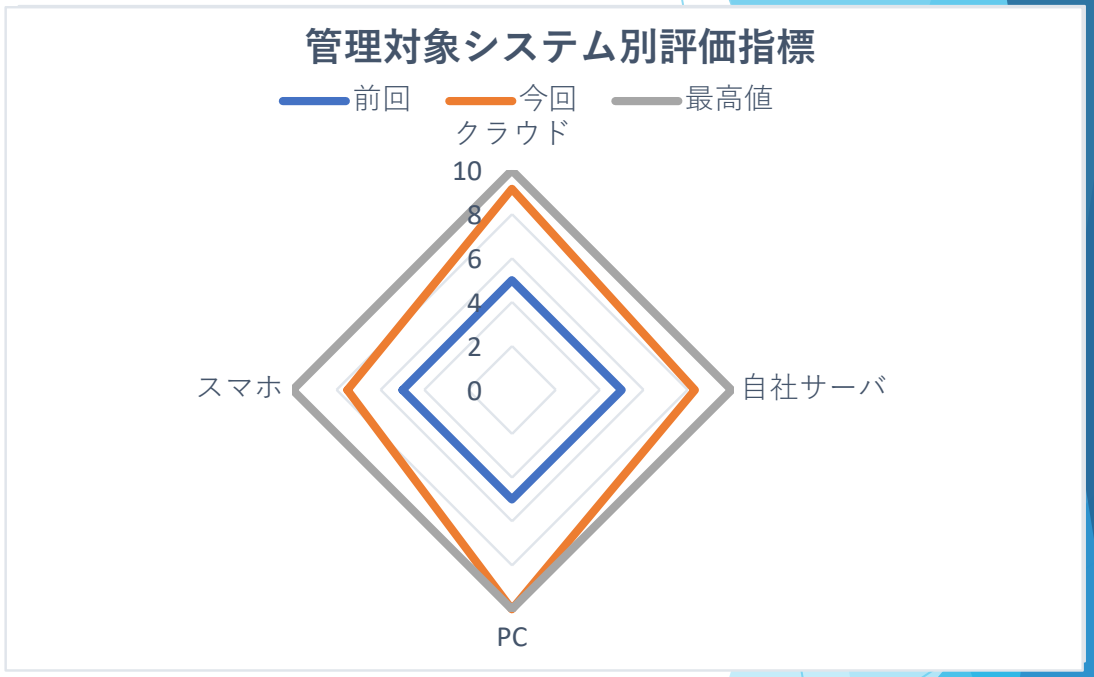
推奨事項
（1）インシデント対応、事業継続計画等の文書が丁寧に現場でも分かりやすく作成されていた。
（2）教育、訓練が新入社員及び協業の社員にまで徹底して実践されていて安全意識の高さが感じられた。

以上

４．監査報告書（一部拡大）

情報システムの形態に関連する観点からの事項

管理対象システム	前回	今回	最高値
クラウド	5	9.2	10
自社サーバ	5	8.3	10
PC	5	10.0	10
スマホ	5	7.5	10



レーダーチャートからの所見

①各管理プロセスは前回の監査より改善がみられる。

②しかし、「スマホ」においては対応の改善を更に進める必要がある。

③クラウドの安全性が高いので、サービスをクラウドか自社かの選択をリスクベースで検討する必要と思われる。

また、クラウドサービス側で行うバックアップと、自社として手元にデータを残すバックアップの 2 種があるため、被監査ごとにリスク精査する必要があると感じます。

５．監査後のフォローアップ

（１）監査のトップレビュー

監査報告書の提出時にフォローアップのためトップレビューを行うことを推奨する。

（２）改善結果のフォローアップ監査

監査結果に基づく是正・改善計画を作成して実施する。フォローアップ監査を行う。

フォローアップ監査の結果は必要に応じて、トップに報告と監査効果のレビューを行う。

レビューでは監査対象組織の疑問や課題をクリアーにすることに心がける。

（３）次回監査のための記録等の文書管理

文書管理は監査関連文書、是正・改善した業務の改訂したマニュアル、手順書、規程類も含まれる。

（４）次年度以降の年度監査計画書作成

初回の監査効果のレビューに基づいて、２回目以降の監査の準備活動や各種計画書

ここでは、システム監査基準に基づいて、次回以降の監査までの組織の方向性やシステム改善のスケジュール等の内容も含まれる。

おわりに　研究のまとめ

(1)システム監査の普及、実施の促進を狙いとして、どの企業も関心、ニーズのあるテーマを選択した。
(2)実際はランサムウェア対策と、バックアップのリカバリー処理までを考える必要があり、テーマの範囲が広がることになったが、当初の狙いのとおり、何処の企業においても必要な内容と考える。
(3)監査対象組織にとって、受査がミニマムな監査であっても、システム監査員に要求されるレベルは高いものになる。また、システム監査員は監査対象組織の情報システムの状況をよく把握し、監査対応者に応じて、チェックリストのヒアリングする必要がある。
(4)今回身近なリスクに対する適切な管理策を実施するきっかけの、システム監査実施のツールができた。
監査対象組織の情報システムの実態を把握して、見える化する成果物を得た。

おわりに

監査活動での課題

（1）当研究成果の活用で、どの企業がこのミニマム監査を希望しているか、具体的な実施への計画はない。

（2）自社内で実施する場合にシステム監査員のレベルがある程度情報システムに精通しているなどの要件があり、チーム編成にも制約があることが考えられる。

（3）研究会として危惧は、このようなツールを使いこなす卓越した監査技術を持った監査チームが実施しなければ、監査対象組織が満足できる成果を享受できない可能性があることも事実である点である。

（4）従って、自社での監査が困難な場合は、形態として専門家のサポートを含め、外部による監査の実施も検討する必要がある。

参考資料

（1）クラウドサービスの安全性評価に関する検討会 とりまとめ
https://www.meti.go.jp/shingikai/mono_info_service/cloud_services/pdf/20200130_report.pdf
（2）IPA中小企業の情報セキュリティ対策ガイドライン
付録5　情報セキュリティ関連規程（サンプル）　www.ipa.go.jp › security › guide › sme
（3）IPA 中小企業のための クラウドサービス 安全利用の手引き
https://www.ipa.go.jp/archive/files/000002661.pdf
（4）情報システム基盤の復旧に関する 対策の調査 報告書
https://www.ipa.go.jp/archive/files/000004636.pdf
（5）クラウドコンピューティングの　概要と推奨事項　米国国立標準技術研究所による推奨　Special Publication 800-146https://www.ipa.go.jp/security/reports/oversea/nist/ug65p90000019cp4-att/000025367.pdf　NIST Special Publication 800-146　IPAサイトのNIST資料各種
（6）コンピュータセキュリティログ管理ガイド　www.ipa.go.jp > security > reports > oversea > NIST
（7）マルウェアによるインシデントの防止と 対応のためのガイド　www.ipa.go.jp > security > reports > oversea > NIST
ファイル形式: PDF/Adobe Acrobat
NIST SP 800-61『コンピュータセキュリティインシデント対応ガイド（Computer Security Incident . NIST SP 800-61 で定義されているように、インシデント対応プロセス
（8）NIST SP800 シリーズに見る情報セキュリティと事業継続計画　www.ipa.go.jp > security > reports > oversea > NIST
（9）ランサムウェアとは？分かりやすく解説 | 感染経路や具体的な予防策　https://insights-jp.arcserve.com/ransomware
（10）ランサムウェアのデータ復旧方法とは？感染したらすぐにやるべきことも解説　https://insights-jp.arcserve.com/ransomware-data-recovery
（11）ランサムウェア対策 実践ガイド (Compass Booksシリーズ) 単行本（ソフトカバー） – 2023/9/22
（12）IPA 情報セキュリティ10大脅威
（13）JSSM 日本セキュリティマネジメント学会　セキュリティ法と経営研究会　なぜ中小企業のサイバー攻撃対策支援が必要なのか
古川佳和　2024/1/29

ご清聴ありがとうございました

- 研究プロジェクトの内容を、ここでは十分に報告できませんでした。
  詳細については、当研究の報告書をご覧ください。
- 報告書：「身の回りにあるミニマムなシステム監査の検討」をご希望の方は
  （kimura-yuu1@jg8.so-net.ne.jp、akao.y@canvas.ocn.ne.jp）
  へご連絡ください。
- 当報告についての問い合わせは、学会事務局経由にてお願いいたします。
- 当研究プロジェクトは月1-2回、オンラインまたは対面で実施しております。
- 2024年度計画は下記の研究テーマ予定しております。
  「システム監査におけるAIの活用に際しての課題の考察」
- 研究プロジェクトにご関心のある方は、学会事務局経由にてお問い合わせください。

以上