システム監査学会
第３２回研究大会
2018年６月８日

テレワーク(在宅勤務)のセキュリティ監査

2017年度「情報セキュリティ対策の診断」研究プロジェクト
主査　木村裕一、メンバー　尾崎孝章、赤尾嘉治
オブザーバー　西澤 利治 、 桜井由美子

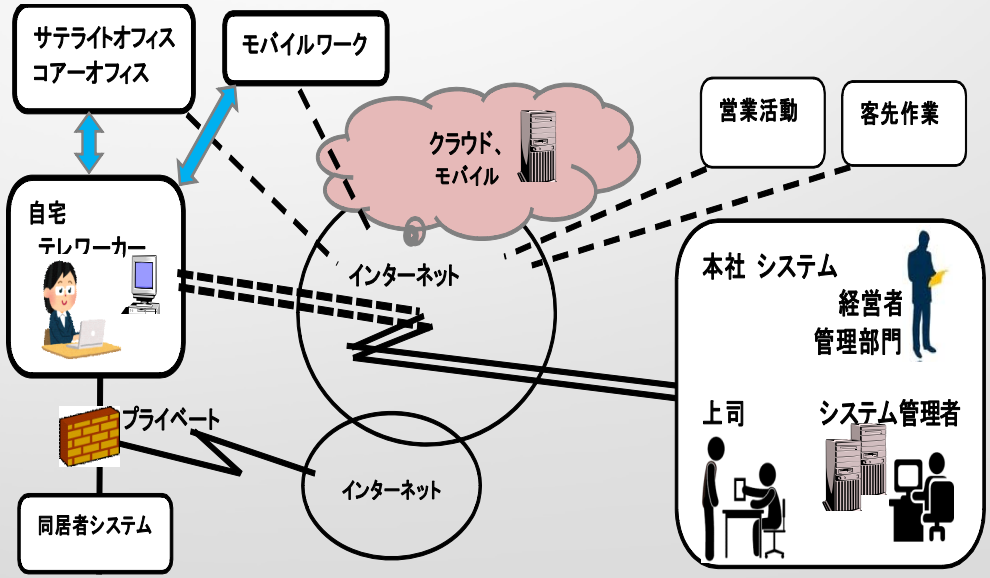
目次

1．研究の考え方と位置づけ

テレワーク（在宅勤務）の普及

- テレワークとは勤務形態の一種で、「ICT（情報通信技術）を活用し、時間や場所を有効に活用できる柔軟な働き方」とされている。これは働く人の高齢化の進展、人手不足等を背景とした、人材確保、女性の戦力化、経験者の退職防止などを要請する社会情勢に応えるものであり、また業務の効率化などの要請に応えるものでもある。

- 本研究は導入され運用されているテレワークの安全性の検証を対象にした。企業は導入の狙いとして、テレワーク導入の有効性、効率性の目標設定も行なうが、ここでは主テーマとしない。



2．研究プロジェクトのテーマと検討内容

テレワーク制度実施の課題

- 実施するテレワーク業務の(業務で取り扱う情報の重要度に応じた）安全性確保が必要である。
- 自社が管理する事務所の環境外で、新たに業務を行い情報を取り扱うため、その環境整備が必要となる。

企業が何も対処しないことは考えられないが、ややもすると安全管理が手薄になりがちである。しかし、テレワーク導入によってその業務遂行の安全レベルが下がることは許されない。リスク見合いの安全対策が必要になる。

企業が必要な対応について、総務省をはじめとしてガイドラインが公表されている。企業はそれらに沿って本当に必要なセキュリティ対策を実施しているか、選択した対策は妥当か、対策の実現状況に不備がないか確認する必要がある。例えば、**在宅業務の環境の安全性、情報通信の安全性、クラウドサービス利用方法の安全性など**が新しい視点である。

本研究のテーマと前提事項

- テレワークでは、業務管理者が事業所において仕事の指示や成果、就業時間、勤務状況を直接把握し、管理することが出来ない。しかし、その成果の品質、安全性、生産性等を確保しなければならない。
- 上記の課題対応に不備がないかの確認のために、テレワーク業務に関する内部監査を実施して前記課題に応えることを研究テーマとした。
- 国（厚生労働省）、自治体による「働き方改革助成金」など、働き方改革制度導入に対する助成金制度がある。
  ・テレワーク用通信機器の導入・運用、・就業規則・労使協定等の作成・変更、労務管理担当者に対する研修、及びこれらに関して、労働者に対する研修、周知・啓発、外部専門家によるコンサルティング等が助成の対象である。
  助成された結果が安全なテレワーク運用を行えるものになっていることは重要であり、これを担保できる監査は重要である。

研究方法

- テレワークのセキュリティ監査の実施方法を、システム監査の観点、監査方法を当てはめて検討する。実際にテレワークを導入する企業への監査の実施は、この結果の活用の課題であるが、今回の研究では範囲外とする。

a. 対象とする企業

テレワークを実施する対象企業として、次のような中小規模事業者を前提とした。

- 規模・勤務形態
  中小企業。従業員30名—50名程度。また、テレワーク勤務形態はテレワーク業務の中で基本的なパターンである“常時在宅勤務”とする。
- 適応業務
  テレワークを実施するメリットを持つ業務・業種
  対面の接客を必要としない業務。入力作業、情報に基づく事務処理、情報処理、創造的思考を行う業務等
- 管理体制（人材）
  情報システムを管理する担当者が存在する企業（兼務可）
- 技術レベル
  情報システムに関する担当者が任命され、ベンダー等の窓口として関連事項の会話ができること。自社の情報システムに関する技術保有は必須ではない。
  なお、保有する情報システムは次のどのような形であってもよい。
  - 全て自社保有している
  - 自社保有とクラウドサービスを利用している
  - クラウドを利用して社内には端末のみ保有している。

b. 対象とする企業のテレワーク業務における管理事項

- 在宅勤務に関わるセキュリティ対策
- 発生する（発生した）インシデントの対応状況
- テレワーク業務の成果、テレワーカーの勤務実績把握
  （管理対象ではあるが、今回の監査対象にはしない）

c. テレワーク監査の必要性

- テレワーク監査は次のような場面で必要になる。
  「顧客の眼」を意識する場合。
  具体的には、顧客からの要求時、受注活動や、委託元への業務説明、また事故や障害発生時の説明など
  ISMSやPマーク取得企業は定期的な監査時にテレワークに関する監査の視点を加えて実施することが必要
  個別の項目としては、例えばクラウド利用の課題対応に不備がないか、確認することなど

本研究で作成する成果物

a. テレワーク監査チェックリスト

- 何を監査するかを明らかにする「監査チェックリスト」を作成。経営者、システム管理者、テレワーク勤務者を監査対象者にし、対象別に区分してチェック項目を作成。

b. 監査計画書

- 監査目的の設定、そのスケジュール、社内関係部署との調整、監査人の任命、実施方法などを計画書の雛形により例示。

c. 監査報告書

- 報告書の様式雛形により、どのレベルまで記述するか、例示する。また、監査結果をどのように経営者に報告し、現場に改善させるかなどを示す。

d. テレワーク監査の手引き

- 監査の実施体制、監査で確認する監査証拠の例などを示す。

３．テーマ別の研究内容と検討結果

- テレワーク監査チッェクリストは「テレワークセキュリティガイドライン（第４版）(案）」（総務省平成３０年２月意見募集）の“テレワークセキュリティ対策のポイント”をベースに作成し、研究プロジェクトでの検討結果を反映した。なお、総務省では「同（第３版）」（平成２５年３月総務省）を公表しており、研究の過程ではこれをもとに検討した。
- 研究において、次のテーマを検討し結果を反映した。
  - インシデント発生への備えと対応
    テレワーク従業者がインシデントに気づかず、見過ごしてしまうと重大な事故、悪影響をもたらす恐れが高まる。それに対して予め備えておくことが必要で、そのための考え方、対処を確認することを監査チェックリストに取り込む。
  - クラウドサービスの利用
    テレワークの導入と運用は、クラウドサービスを利用することにより運営が負担軽減される。利用時に、安全性確保の点から、確認するべき事項などを監査チェックリストに取り込む。
  - テレワーク規程類の整備
    テレワーク業務に関して規程の策定が重要であり、その策定には、国（厚生労働省）、自治体（東京都など）等のテレワーク制度推進の助成金の対象にもなっている。規程の整備に参考となる公表事項を「テレワーク監査の手引き」に示す。

４．２０１７年度の研究成果

- 成果
  - ✓テレワーク監査チェック項目からなる「テレワーク監査チェックリスト」を作成した。
  - ✓監査実施方法の例示として、「監査計画書」（雛形）を作成した。
  - ✓監査結果のまとめ方の例示として、「監査報告書」（雛形）を作成した。
  - ✓監査の実施体制、監査対象者、監査証拠などについて「テレワーク監査の手引き」を作成した。

テレワーク監査計画書

テレワーク監査計画書　　例示

代表取締役　○○　○○　社長殿

承認者：(代表者)	作成者：(監査責任者) 2018 年 2 月 15 日

2017 年度監査計画に基づき、テレワーク業務に関するセキュリティ監査を以下のとおり計画いたします。

項目	内容	備考
目的	① テレワーク業務実施に関して情報システムおよび業務環境の安全対策が出来ているか確認する。 ② テレワーク勤務者の業務環境ならびにその運用の安全性を確認する。 （顧客からの委託業務を遂行するに必要なテレワーク業務実施環境の安全性が、テレワークに関連する社内規定、及び総務省「テレワークセキュリティガイドライン」(第 4 版)(案) "テレワークセキュリティ対策のポイント" に準拠して確保できているか確認する）	
監査対象 監査範囲	① 代表者（経営者） ② 管理者（情報システム部門の管理者、業務管理部門の管理者） ③ テレワーク勤務者　（テレワーク勤務者 2 名／全 5 名）	
実施場所	社内（監査対象者の執務場所、施設） テレワーク勤務者の(在宅)就業場所	
監査期間・日程	2018 年 3 月 11 日～3 月 19 日 （情報システム管理者、業務管理者へのヒアリング、及び実査） 3 月 12 日～3 月 14 日 （テレワーク勤務者へのヒアリング、及び実査）　3 月 14 日 （経営者へのヒアリング、及び実査）　3 月 15 日 （監査報告）　3 月 19 日	予備調査は 2018 年 2 月中に実施
基準	① テレワークに関連する当社社内規程 ② 「テレワーク監査チェックリスト」　（総務省「テレワークセキュリティガイドライン」(第 4 版)(案)テレワークセキュリティ対策のポイントに準拠したもの）	
監査方法	机上での規程、及び運用関連資料・記録の確認 関係者へのヒアリング、及び業務現場の実査	
監査体制 （役割）	（監査責任者）□□　□□ （監査人）　△△　△△、△△　△△	
監査工数	8 人日　内訳は下記 3 人日（予備調査：準備、検討）（準備資料作成を含む） 3 人日（対象部署の監査実施） 2 人日（対象：整理、まとめ、報告）（報告書作成を含む）	
監査報告	監査報告：2018 年 3 月 19 日	
前回監査	フォロー事項なし	

1

監査対象と監査の主要観点

対象	主要観点	監査内容	方法
代表者 （経営者）	・テレワーク業務で取り扱う情報の重要度レベル分けと取扱い方法の規程運用 ・セキュリティ事故発生時の対応 ・テレワーク業務への適用業務の妥当性（リスクの認識）	・テレワーク業務で取り扱う情報の重要度設定に伴うリスク認識の周知と徹底 ・インシデント発生時の対応体制と対応内容 ・テレワーク勤務の適用業務の妥当性	ヒアリング 資料・記録確認
管理者 （情報システム管理者） （業務管理者） （規定、運用）	・当社指定のテレワーク業務用の情報システム環境の安全性、信頼性 ・テレワーク勤務者が利用する情報システムのセキュリティルールの妥当性 ・アクセス可能情報の範囲 ・アクセスログ等の管理	・テレワーク勤務者が利用する情報システム環境の安全性、信頼性の状況 ・情報システム管理規定の妥当性 ・情報システムのセキュリティルールの妥当性 ・アクセス可能情報の範囲 （必要な範囲に限定しているか） ・ ・アクセスログ等の取得と監視分析状況	ヒアリング 情報システムの環境確認 運用記録の確認 運用規程の確認
テレワーク勤務者 （運用）	・業務実施環境の安全性 ・運用報告事項の正確性、妥当性	・業務実施環境の安全性 ・運用報告とその内容の妥当性 ・現場環境とその運用状況、及び物理的安全性 （現地視察＊2 名）	ヒアリング 実査 運用記録の確認

以上

2

テレワーク監査チェックリストの案

- 本チッェクリストはプロジェクトチームが、下記出典のガイドラインより箇条書きにリライトした。
  出典; 総務省 テレワークセキュリティガイドライン（第４版）（案）「２．テレワークセキュリティ対策のポイント」（平成30年パブリックコメント版）
- チェック内容の根拠規程・規定する確認する根拠資料等欄には参考となる文書名を例示した
- 確実性を担保するため、記録や分析・評価等を追記した項番もある

経営者が実施すべき対策

通番	チェック内容	チェック内容の根拠規程 規定する確認する根拠資料等	適否	チェック状況のコメント	備考
1	情報セキュリティポリシーに関する実施事項 ①経営者はポリシーを策定 ②定期的に監査 ③内容に応じて見直し	セキュリティポリシー、 監査報告書、 見直し記録			
2	情報の重要度に応じたレベル分けに関する実施事項 ①重要度に応じたレベル分けを実施 ②情報のテレワークでの利用可否を策定 ③利用の場合の取扱方法を定める	資産目録 資産利用者 情報資産の取扱規程			
3	情報セキュリティ理解に関する実施事項 ①情報セキュリティ対策の重要性を認識 ②定期的に教育・啓発活動を実施	教育計画、教育内容資料、 教材、教育実施記録、			
4	情報セキュリティ事故への対応に関する実施事項 ①事故の発生時の連絡体制 ②事故対応の訓練を実施	連絡体制・報告ルール インシデント対応規程、訓練、			
5	情報セキュリティ対策に適切な資源に関する実施事項 ①必要な人材・資源 ②必要な予算	年度事業計画書 年度事業計画書			

システム管理者が実施すべき対策

通番	チェック内容	チェック内容の根拠規程 規定する確認する根拠資料等	適否	チェック状況のコメント	備考
6	セキュリティ技術的対策に関する実施事項 ①システム全体を管理することを自覚 ②テレワークのセキュリティ技術的対策を実施 ③実施状況の定期的確認	 リスク対策一覧 監査報告書、査察			
7	情報の管理の設定に関する実施事項 ①情報のレベル分け ②アクセス制御、暗号化の要否や印刷可否	 資産目録 情報資産の取扱規程			
8	テレワーカーの情報セキュリティ認識に関する実施事項 ①テレワーカーの情報セキュリティ認識 ②定期的に教育・啓発活動を実施	 教材 教育実施記録			
9	情報セキュリティ事故に関する実施事項 ①事故の発生時の連絡体制 ②事故対応の規程・マニュアル ③対応訓練の実施	 連絡体制ルール インシデント対応規程、 訓練計画、対応評価、見直し			
10	アクセス管理対策に関する実施事項 ①フィルタリング等のアクセス管理設定 ②アクセス管理の遵守確認	 情報システムアクセス管理規程 アクセスログの運用確認			
11	アプリケーション管理に関する実施事項 ①端末アプリケーションは指定されたものに設定 ②例外は申請、リスク確認後に承認	 アプリソフト管理規程 申請書、決済状況確認			
12	ウイルス対策ソフトに関する実施事項 ①端末（貸与・自前）に対策ソフトをインストール ②最新の定義ファイルの適用を確認	 アプリソフト管理規程 パターンのバージョン確認			
13	端末のＯＳ・アプリケーションに関する実施事項 ①端末ＯＳをアップデートで最新の状態 ②端末アプリケーションは最新の状態	 バージョン確認 バージョン確認			
14	私用端末をテレワークに利用に関する実施事項 ①私用端末利用はリスク確認後に承認 ②申請通りの内容で対策が維持されているか	 私用機器管理規程 機器の運用確認			
15	ランサムウェアへの対策に関する実施事項 ①重要な電子データのバックアップ ②バックアップデータのオフライン保存	 情報システム運用規程 バックアップデータの確認			
16	金融機関や物流業者からのメールに関する実施事項 ①事務連絡を装う不審なメールの検出 ②メールを不振として分離する設定	 教材 メール機能の設定			
17	使用端末の管理に関する実施事項 （スマートフォン、タブレット等） ①台帳等を整備し、端末の所在や利用者等を管理	 私用機器管理規程、機器管理台帳			
18	無線 LAN の脆弱性対策に関する実施事項 ①無線 LAN の脆弱性対策が適切か	 無線 LAN 設計・設定書			
19	利用者認証に関する実施事項 ①利用者認証の技術的対応を実施 ②ＩＤ、パスワード、ＩＣカード等の適正な運用管理	 実物の動作確認 情報システム運用規程			
20	社内システムへのアクセスに関する実施事項 ①社内システムへのアクセス方法を制定 ②システム境界にはファイアウォールやルータ等を設置 ③アクセス状況の監視・測定の実施 ④不必要なアクセスを遮断 ③アクセスに関するログ情報の分析評価	 情報システム運用規程 実物の動作確認 監視ログ・測定記録 リジェクト記録 ログの分析評価結果			
21	パスワード管理に関する実施事項 ①アクセス用のパスワードは強度の高いものとする ②強度の低いものを阻止するように設定	 情報システム運用規程、パスワードＦ システムロジックの確認			
22	ＳＮＳの利用ルールやガイドラインに関する実施事項 ①ＳＮＳに関する利用ルールやガイドラインを整備 ②テレワーク時の利用上の留意事項を明示	 情報システム運用規程 情報システム運用規程			
23	クラウドサービスの利用ルールに関する実施事項 ①クラウドに関するリスク確認と利用ルールを整備 ②情報漏えいの恐れがある利用方法の禁止	 クラウドサービス利用規程 クラウドサービス利用規程			

テレワーク勤務者が実施すべき対策

通番	チェック内容	チェック内容の根拠規程 規定する確認する根拠資料等	適否	チェック状況のコメント	備考
24	テレワーク作業での環境に関する実施事項 ①利用する情報資産の管理責任を自らが負う ②セキュリティの技術的対策を実施 ③物理的対策を実施 ④人的対策を実施 ⑤定期的に実施状況を自己点検	 テレワーク業務管理規程 情報システム運用規程 地震等の自然災害、火災、テロ等 家族等勤務者以外の者への対応 自己点検表の記録			
25	情報の取扱いに関する実施事項 ①情報のレベル分け内容の確認 ②レベル毎の利用ルールに従って取扱う	 情報・文書管理規程 情報・文書管理規程			
26	情報セキュリティ教育・啓発活動に関する実施事項 ①定期的に実施される教育・啓発活動に参画 ②情報セキュリティに対する認識の向上	 教育記録 自己点検表の記録、			
27	情報セキュリティ事故への対応に関する実施事項 ①事故の発生時の連絡体制 ②事故対応の訓練を実施	 連絡体制ルール インシデント対応規程、訓練、			
28	端末のＯＳ・アプリケーションに関する実施事項 ①端末ＯＳ・ブラウザをアップデートで最新の状態 ②未実施の状態ではアクセス禁止	 バージョン確認 禁止内容の遵守確認			
29	アプリケーション管理に関する実施事項 ①端末アプリケーションは指定されたものに設定 ②例外は申請、リスク確認後に承認	 情報システム運用規程 情報システム運用規程			
30 31	作業開始前の確認作業に関する実施事項 ①ウイルス対策ソフトが最新の定義ファイルである ②ＯＳのアップデートが最新の状態である ③ソフトウェアのアップデートが最新の状態である	 作業前チェック表の確認記録 作業前チェック表の確認記録 作業前チェック表の確認記録			
32	スマートフォン、タブレット等に関する実施事項 ①テレワークには情報セキュリティ対策済の機器を使用 ②不正な改造（脱獄、root 化等）を禁止	 情報システム運用規程 情報システム運用規程			
33	マルウェアに感染した場合の対応に関する実施事項 ①感染した場合の報告、被害拡大への自覚 ②不審メールの見分け方、技術的対応の実施 ③添付ファイルの開封やリンク先のクリック ④不審メール管理の状況の確認	 情報システム運用規程 情報システム運用規程 情報システム運用規程 情報システム運用規程			
34	情報資産の持ち出すときの管理に関する実施事項 ①原本を安全な場所に保存 ②セキュリティ対策を施す	 テレワーク業務管理規程 テレワーク業務管理規程			
35	機密性が高い電子データに関する実施事項 ①機密性が高い電子データを極力使用しない業務の工夫 ②機密性が高い電子データは暗号化 ③暗号化、保管レベルの確認 ④記録媒体（ＵＳＢメモリ等）等の紛失・盗難	 情報システム運用規程 情報システム運用規程 情報システム運用規程 情報システム運用規程			
36	機密性が高い電子データの送信に関する実施事項 ①電子データを送信する際には必ず暗号化 ②宛先の正確性チェック ③相手先と授受の確認	 テレワーク業務管理規程 作業前チェック メールで確認			
37	無線 LAN 利用に関する実施事項 対策が可能な範囲で利用する。 ①無線 LAN 利用に伴うリスクを確認 ②セキュリティレベルに応じた対策を実施	 情報システム運用規程 情報システム運用規程			
38	第三者と共有する環境で作業に関する実施事項 ①画面にプライバシーフィルターを装着 ②作業場所の選択等、画面の覗き防止に努める	 作業前チェック表の確認記録 作業前チェック			
39	社内システムへのアクセスに関する実施事項 ①社内システムへのアクセス方法の確認 ②ＩＤ、パスワード、ＩＣカード等の適正な運用管理	 情報システム運用規程 情報システム運用規程			
40	社内システムにアクセスに関する実施事項 ①システム管理者が指定したアクセス方法のみ	 情報システム運用規程			
41	パスワード管理に関する実施事項 ①使い回しを避ける ②一定以上の長さにする ③他人に推測されにくいものを用いる	 自己点検表の記録 情報システム運用規程 情報システム運用規程			
42	ＳＮＳの利用ルールやガイドラインに関する実施事項 ①ＳＮＳに関する利用ルールやガイドラインの遵守	 情報システム運用規程			
43	クラウドサービスの利用に関する実施事項 ①クラウドサービス利用は社内ルールの範囲で利用	 情報システム運用規程			

テレワーク監査報告書

テレワーク監査報告書　　例示

代表取締役　　○○　○○　社長殿

承認者：(代表者)	監査責任者□□　□□ 2018年3月19日
配布先1	配布先2

2017年度監査計画に基づき実施した、テレワーク業務に関するセキュリティ監査の結果を報告いたします。

項目	内容	備考
監査目的	① テレワーク業務実施に関して情報システムおよび業務環境の安全対策が出来ているか確認する。 ② テレワーク勤務者の業務環境ならびにその運用の安全性を確認する。 （顧客からの委託業務を遂行するに必要なテレワーク業務実施環境の安全性が、テレワークに関連する社内規定、及び総務省「テレワークセキュリティガイドライン」(第4版)(案)"テレワークセキュリティ対策のポイント"に準拠して確保できているか確認する）	
監査範囲　監査対象部門	① 代表者（経営者） ② 管理者（情報システム部門の管理者、業務管理部門の管理者） ③ テレワーク勤務者　　（テレワーク勤務者2名／全5名）	
監査計画、監査日程	2018年3月11日～3月19日 （情報システム管理者、業務管理者へのヒアリング） 3月11日～3月14日 （テレワーク勤務者への実査、及びヒアリング）3月14日 （経営者への実査、及びヒアリング）3月15日 （監査報告）　3月19日	予備調査は2018年2月中に実施
場所	社内（関係者の執務場所、施設） テレワーク勤務者の(在宅)就業場所	
対象プロセス	・テレワーク業務に関する規程の妥当性確認 ・テレワーク業務システムの業務管理、安全管理に係る規程、及びその周知・徹底状況の確認 ・テレワーク業務の運用状況確認 ・情報システムのテレワーク勤務業務に係る範囲について、業務処理の上流から、結果を得る下流までのプロセスの確認	
監査体制（役割）	監査責任者　□□　□□ （規定及び業務実施状況の精査、判断） （監査対象部門へのヒアリング、問題点、指摘事項の評価） 監査人　　△△　△△、△△　△△ （規定及び業務実施状況の精査、判断） （監査対象部門へのヒアリング、問題点の指摘）	

1

監査所見、関連する証拠	・経営者に関して： テレワーク業務の情報システムおよび運用に関する経営資源が割り当てられ、社内で認識の齟齬はない。しかし、○○業務の情報の重要度評価をせずテレワーク業務で取り扱っている。取扱情報の重要度レベル分け及び取扱い方法の周知・徹底が不十分である。 ・管理者に関して： テレワーク勤務者からの業務及び点検報告書が所定期間ごとにきちんと提出されていない例があり、これに対するフォローがされていない。 テレワーク勤務業務の安全対策において一部○○、△△に関して不十分な点がある。○○について早期に対応が必要である。 また、□□については規定が不十分であり、全テレワーク勤務者に安全対策が周知できているか不明。規定を明確にして周知・確認が必要である。 ・テレワーク勤務者に関して： テレワーク勤務環境(自宅)において、テレワーク業務中にも執務場所に家族が自由に出入りできる。 テレワーク端末をテレワーク勤務者以外の者が利用した痕跡があった。なお、監査した2名に上記□□は周知されていた。	(証拠) テレワークにおける○○業務の取扱情報 業務点検報告書 執務場所の見取り図
監査結論	・テレワーク業務の規程に関して： □□について規定が不十分である。見直しが必要である。 ・経営者に関して：情報の重要度の規程はあるが、運用に漏れがある。その周知徹底が必要である。 ・管理者、テレワーク勤務者に関して： テレワーク業務の運用は、上記の問題事項があり、指摘とした。改善が必要である。 不十分な規定の見直しをする必要がある。 ・テレワーク勤務者に関して： テレワーク勤務者の執務環境の安全性確保、業務端末のアクセス管理の運用を明確にし、徹底する必要がある。	
監査基準が満たされた程度に関する記述	テレワーク業務の運用で、社内規程については規定が遵守されていた。しかし、「テレワーク監査ちぇっくりすと」(総務省「テレワークセキュリティガイドライン」(第4版)(案)"テレワークセキュリティ対策のポイント"準拠）に関しては、いくつかの項目で遵守出来ていない。当社の規程に反映させる見直しの検討が必要である。	

以上

2

5．今後の課題と進め方

1. 成果の活用

監査チェックリストの活用は、テレワーク業務を実施する企業に対して監査実施の場面で、その有効性を確認することである。しかし、今回の研究範囲では監査の実施まで進めることができず、今後の課題である。

2. 監査チェック項目のブレークダウン

今回作成した監査チェックリストは対象企業を設定しているが、具体的な業務を設定していない。対象とする企業が決まった段階で各チェック項目のブレークダウンが必要な場合がある。また、求める根拠資料を例示しているが、名称も社内規程に即して読み替える。これは監査実施に当たっての準備事項（予備調査事項）である。

3. 監査計画書、報告書の作成

雛形で示した検査計画書、報告書は、対象とする企業を決めた段階で、その企業の経営者等関係者と監査目的、監査対象等を協議の上作成する。

4. テレワークの有効性、効率性の監査

今回主テーマとして検討していないテレワークの有効性、効率性については、今後の課題である。

有効性、効率性を考える場合、監査の指標には評価に利用できる下記の項目が考えられる。各項目は定量化可能な項目、段階的な評価をする項目に分けられる。

定量化可能な項目（指標）の例

顧客対応（顧客対応回数、対応時間、顧客訪問時間）、事務工数（伝票等の処理件数、月例報告等の作成時間、企画書等の作成件数、時間）、オフィスコスト（面積、賃貸料、オフィス付随費用）、移動コスト、情報通信コスト、人材確保（応募者、退職者）、オフィス改修コスト

段階的な評価をする項目の例

業務プロセス（情報共有度、顧客サービス（顧客満足度））、コミュニケーション（垂直・水平方向のコミュニケーション頻度、質）、情報通信システム（システムの機能・能力の満足度）、情報セキュリティ（セキュリティ意識、ルールの整備度）、業務評価（満足度）、働き方の質（仕事の満足度、疲労度）

※今回のチェックリストでは、情報セキュリティ以外は段階的な評価をする項目として含めておらず、監査の見直しにおいて考量するべき事項である。

参考資料

[1]「テレワークではじめる働き方改革　テレワークの導入・運用ガイドブック」　厚生労働省
「テレワークモデル実証実験」　平成２８年１２月

[2]「情報通信機器を活用した在宅勤務の適切な導入及び実施のためのガイドライン（在宅勤務ガイドライン）」（改訂）　厚生労働省労働基準局　平成２０年７月

[3]「テレワークセキュリティガイドライン（第３版）」　総務省　平成２５年３月

[4]「テレワークセキュリティガイドライン（第４版）(案）」　総務省　平成３０年２月

[5]「職場意識改善助成金（テレワークコース）　申請マニュアル」
厚生労働省労働基準局　勤労者生活課　（Ｈ２９．４）

添付資料１　テレワーク監査チェックリスト

添付資料２　監査計画書、監査報告書　(雛形）

添付資料３　テレワーク監査の手引き

募集

- 今年度の当研究プロジェクトへの参加を募集しています。
  - 課題に対する研究を通じた、セキュリティ監査の勉強。
  - 実証実験を通じた企業とのコミュニケーションの勉強。
  - 原則月１回、研究会合により様々な立場からの意見交換。

当研究プロジェクト（連絡先）
　主査　　木村　裕一　まで

研究プロジェクトへの参加・お問い合わせは、システム監査学会 HP
「問合せフォーム」からお願いします。

http://www.sysaudit.gr.jp/toiawase/index.html

2018年度研究テーマ

- メンバーの募集（次の２本立てとする）

１．業務フローと業務リスクの把握に関して、システム監査人と被監査部門の情報共有の方法として研究　（プロジェクト成果物を求める）

- 様々な事業や業務を業務フローに展開すること、業務リスクを見落としなく把握し管理する方法を検討する
- システム監査で、この方法を情報共有のツールとしての活用を検討する

２．個人情報保護におけるグローバル化への対応に関する研究（システム監査人としての勉強会）

- 個人情報保護法の改正やGDPR等の国際動向に対して、主に国内市場を対象とする一般企業への影響やあるべき取組の基本を理解する
- 毎月の検討結果を整理し、システム監査に有効な資料として蓄積する