# 表1

## システム管理についてお聞きします

| | | | |
|---|---|---|---|
| 1 | 情報セキュリティポリシーや情報セキュリティ管理に関する規程を定めていますか。 | 1．定めていない<br>2．作成中である<br>3．一部定めている<br>4．定めている<br>5．その他（ ） | → a.考えている<br>b.考えていない |
| 2 | 患者データ（画像を含む）など重要な個人情報については、取得、利用、保管、開示、消去などの一連の業務工程ごとに指置（責任者、手順の明確化、取り扱い者限定、処理の記録、確認など）を講じていますか | 1．講じていない<br>2．計画中である<br>3．一部講じている<br>4．講じている<br>5．その他（ ） | → a.考えている<br>b.考えていない |
| 3 | 施設外の組織に業務を委託する際の契約書に、セキュリティ上の理由（データの漏洩や消失、情報あるいは情報システムの誤用など）から相手方に求めるべき事項を記載していますか | 1．記載してない<br>2．記載している<br>3．その他（ ） | → a.契約書はある<br>b.契約書はない |
| 4 | 従業者（派遣を含む）に対し、採用、退職の際に機密保持に関する書面を取り交わすなどして就業上のセキュリティに関する義務を明確にしていますか | 1．していない<br>2．計画中である<br>3．している<br>4．その他（ ） | |
| 5 | 施設に出入りする外部の人（ベンダーや清掃業者など）に対するセキュリティ上のルールを定めていますか | 1．定めていない<br>2．作成中である<br>3．一部定めている<br>4．定めている<br>5．その他（ ） | → a.考えている<br>b.考えていない |
| 6 | 特にセキュリティを強化したい建物や区画について、必要に応じたセキュリティ対策（部とのセキュリティ上の境界を明確に意識した入退館・入退室管理や警報装置の設置など）を実施していますか | 1．実施していない<br>2．計画中である<br>3．実施している<br>4．その他（ ） | |
| 7 | 患者情報や記憶媒体の適切な管理（サーバーの管理、キャビネットの施錠やプリント出力の放置禁止、記憶媒体の粉砕廃棄など）を行っていますか | 1．行っていない<br>2．計画中である<br>3．行っている<br>4．その他（ ） | |
| 8 | 情報システムの運用に必要なセキュリティ対策（セキュリティ要件の明確化、各種手順書の策定、セキュリティログの記録とチェックなど）を実施していますか | 1．実施していない<br>2．計画中である<br>3．実施している<br>4．その他（ ） | |
| 9 | 不正ソフトウェア（ウイルス、ワーム等）に対する対策（コンピュータウイルス対策ソフトを導入し、パターンファイルのアップデートを適時行うことなどを含む）を実施していますか | 1．実施していない<br>2．計画中である<br>3．実施している<br>4．その他（ ） | |
| 10 | 導入しているソフトウェアに対して適切な脆弱性対策（セキュリティを考慮した設定や、脆弱性修正プログラムの適用、定期的な脆弱性検査など）を実施していますか | 1．実施していない<br>2．計画中である<br>3．実施している<br>4．その他（ ） | |
| 11 | 通信ネットワークに流れるデータに関して、暗号化などの適切な保護策（ＶＰＮの使用や、重要な情報のＳＳＬ等での暗号化を含む）を実施していますか | 1．実施していない<br>2．計画中である<br>3．実施している<br>4．その他（ ） | |
| 12 | 画像や患者情報を含んだ、携帯PC や記憶媒体に対して、盗難、紛失等を想定した適切なセキュリティ対策を実施していますか（携帯PC や記憶媒体の使用場所は、施設外のすべての場所を含む） | 1．実施していない<br>2．計画中である<br>3．実施している<br>4．その他（ ） | |
| 13 | 画像や患者情報（データ）へのアクセスを制限するためのユーザ管理（不要なユーザＩＤの定期的な見直しや共用ＩＤの制限、単純なパスワードの設定禁止など）や認証を適切に実施していますか | 1．実施していない<br>2．計画中である<br>3．実施している<br>4．その他（ ） | |
| 14 | ネットワークのアクセス制御（例えばネットワークの分離や社外からの接続時の認証など）を実施していますか | 1．実施していない<br>2．計画中である<br>3．実施している<br>4．その他（ ） | |
| 15 | 情報システムの障害発生を想定した適切な対策（システムの冗長構成やバックアップ、障害対応手順書の策定、運用記録の取得、社外委託先とのサービスレベルの合意などを実施していますか | 1．実施していない<br>2．計画中である<br>3．実施している<br>4．その他（ ） | |
| 16 | 情報セキュリティに関連する事件や事故が発生した際の行動や報告、判断の基準を定めた対応手続を準備していますか | 1．準備してない<br>2．計画中である<br>3．準備してある<br>4．その他（ ） | |
| 17 | 何らかの理由で情報システムが停止した場合でも業務を継続するための取り組みが、組織全体を通じて検討されていますか | 1．検討してない<br>2．計画中である<br>3．検討してある<br>4．その他（ ） | |
| 18 | 現状のセキュリティ対策の全体としての評価 | 1．十分である<br>2．やや不安がある<br>3．かなり不安がある<br>4．その他（ ） | |

19 セキュリティ対策に関してご意見があればお聞かせください

# 表2

**遠隔画像診断をされる先生にお聞きします。**
**該当しない設問は無視してください。**

| | | |
|---|---|---|
| 1 | 依頼施設からの画像伝送について（複数回答可） | 1．一般のインターネットで伝送<br>2．インターネットであるがＶＰＮを利用<br>3．専用回線で伝送<br>4．そのほか（　　） |
| 2 | 依頼施設側のシステムの利用について実際に行っている項目があれば○をしてください。（複数回答可） | 1．PACSをオンラインで共有（一方向・双方向）<br>2．医療情報システムをオンラインで共有（一方向・双方向）<br>3．電子カルテシステムをオンラインで共有（一方向・双方向）<br>4．該当なし |
| 3 | 今は行えていないが行えたら良いと考えられる項目があれば○をしてください。（複数回答可） | 1．PACSをオンラインで共有（一方向・双方向）<br>2．医療情報システムをオンラインで共有（一方向・双方向）<br>3．電子カルテシステムをオンラインで共有（一方向・双方向）<br>4．該当なし |
| 4 | 診断レポートの作成方法について | 1．すべて電子的に作成している<br>2．電子的に作成するものと手書きとを併用→ a.手書き　％ b.電子的　％<br>3．すべて手書きで作成<br>4．そのほか（　　） |
| 5 | 検査依頼情報（患者の基本情報および臨床情報）の受け取りについて | 1．オンラインで電子的に受け取る<br>2．文書で受け取る<br>3．そのほか（　a.ＦＡＸ　b.郵送→　c.宅配　） |
| 6 | 電子的に検査依頼情報を受け取る場合，依頼情報の読影後の保管状況について該当するものを選んでください | 1．電子的レポートに組み込んで保存される<br>2．電子的レポートに臨床情報を書き込まないが，読影後も臨床情床情報を閲覧することができる<br>3．電子的レポート作成完了後は一切閲覧できない<br>4．そのほか（ |
| 7 | 手書き文書で依頼情報を受け取る場合，依頼情報の読影レポート完成直後の保管状況について該当するものを選んでください | 1．レポートと共に依頼箋をファイルし保管する<br>2．レポートとは別に依頼箋をファイルし保管する<br>3．レポート作成後，直ちに裁断・廃棄する<br>4．そのほか（ |
| 8 | 診断レポートの送付（返信）について | 1．オンラインで電子的に返信<br>2．文書で返信<br>3．そのほか（　a.ＦＡＸ　b.郵送　c.宅配　） |
| 9 | レポートの保存方法について該当するものをお答えください | 1．すべて電子的に保存し，印刷した文書は残さない<br>2．電子的データ及び印刷した報告書を保存する<br>3．電子的に保管せず，印刷したものを保存する<br>4．一切保存しない<br>5．そのほか（ |
| 10 | 貴施設における電子的レポートの保管期間について該当するものを選んでください | 1．永久保管を想定している<br>2．保管年限を定めている（　　年）<br>3．運用上，特に定めていない<br>4．そのほか（ |
| 11 | 問１０で保管期間に年限を定めている場合，データの廃棄方法について該当するものを選んでください | 1．ある年限を経過したレポートは自動的にサーバーから削除<br>2．管理者が削除する文書を指定する<br>3．データの削除方法を運用上，定めていない<br>4．そのほか（ |
| 12 | 印刷されたレポートの保管期間について該当するものを選んでください | 1．永久保管を想定している<br>2．保管年限を定めている（　　年）<br>3．運用上，特に定めていない |
| 13 | 依頼箋，レポートなど印刷された文書又は電子的な文書の施設内での閲覧状況について該当するものを選んでください | 1．職員であれば自由に閲覧可能である<br>2．医師のみ自由に閲覧可能である<br>3．管理者の許可を得たもの以外は閲覧できない<br>4．そのほか（ |
| 14 | 遠隔読影で使用しているモニタについてお答えください。複数回答可 | 1．高精細CRT（サイズ：　インチ，　解像度：　M）<br>2．汎用CRT（サイズ：　インチ，　解像度：　M）<br>3．高精細LCD（モノクロ）（サイズ：　インチ，　解像度：<br>4．高精細LCD（カラー）（サイズ：　インチ，　解像度：<br>5．汎用カラーLCD（サイズ：　インチ，　解像度：　M）<br>6．そのほか（ |
| 15 | ノートパソコンによる読影についてお答えください。複数回答可 | 1．ノートパソコンは使用しない<br>2．ノートパソコンを使用することがある<br>a.画像観察専用に限定　b.多目的なパソコンで兼用<br>3．ノートパソコンに外部モニタを接続し，画像は外部モニタで読影している<br>4．ノートパソコンに画像を表示し，読影している<br>5．そのほか（ |
| 16 | 遠隔読影で使用しているモニタの精度管理についてお答えください。ここでいう精度管理はモニタの劣化の有無を確認し，輝度，階調特性などの経時的変化に対して適切な補正を加える作業をいいます | 1．モニタ管理者を定め，管理者の責任で定期的に実施している<br>2．運用管理規定は定めず，ユーザーが自主的に実施している<br>3．精度管理は特に行っていない<br>4．そのほか（ |
| 17 | 問１６で何らかの精度管理を行っていると答えた方にうかがいます。精度管理の内容について，該当するものを選んでください | 1．JESRA0093-2005にしたがった不変性試験を実施している<br>2．ガイドラインとは無関係な方法で定期的（　ヶ月間隔）に点検している<br>3．まったくの不定期にユーザーの自主的判断で実施している<br>4．そのほか（　　） |
| 18 | **最後に遠隔画像診断に関してセキュリティーを含めてご意見があればご自由にお願いします** | |

図1

情報セキュリティポリシーや情報セキュリティ管理に関す

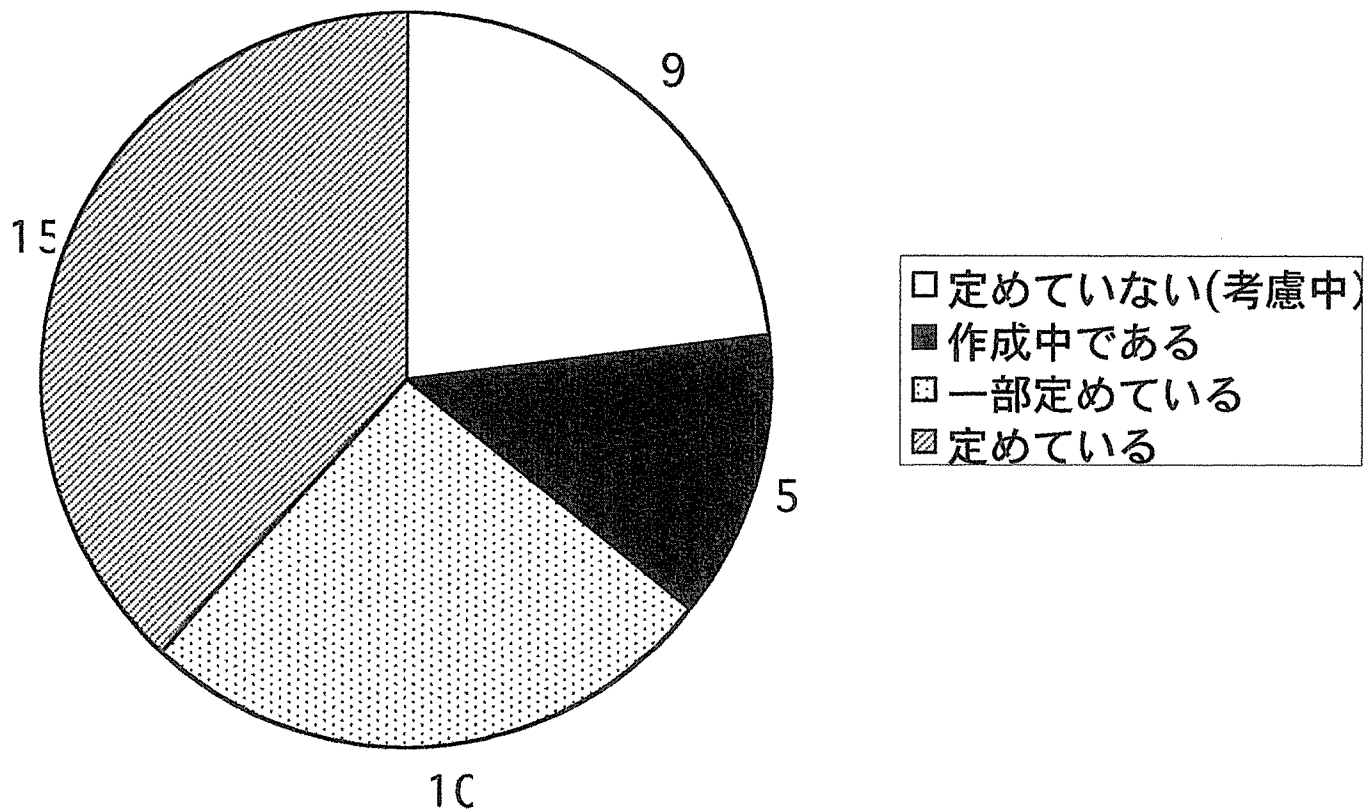

図２

患者データ（画像を含む）など重要な個人情報については、
取得、利用、保管、開示、消去などの一連の業務工程ごとに措置（責任
手順の明確化、取り扱い者限定、処理の記録、確認など）を講じてい

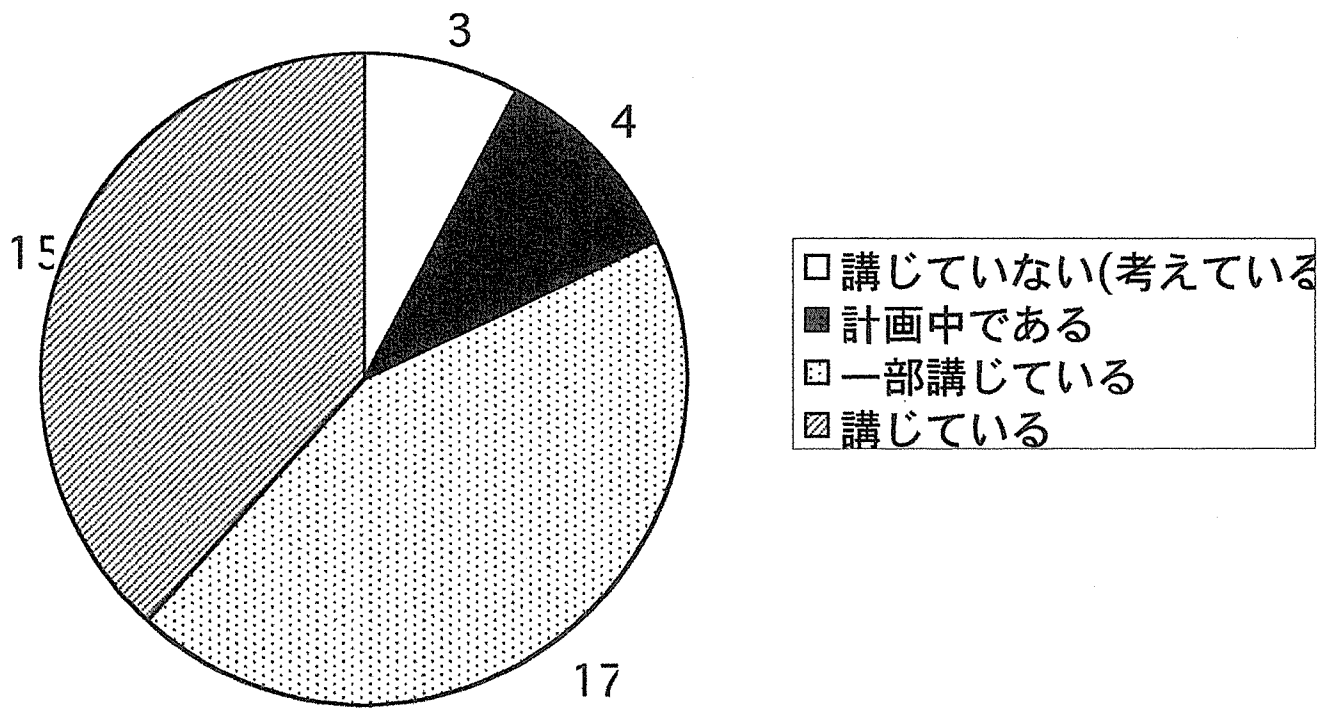

図 3

施設外の組織に業務を委託する際の契約書に、セキュリティ上の理由（
タの漏洩や消失、情報あるいは情報システムの誤用など）から相手方に
めるべき事項を記載しているか

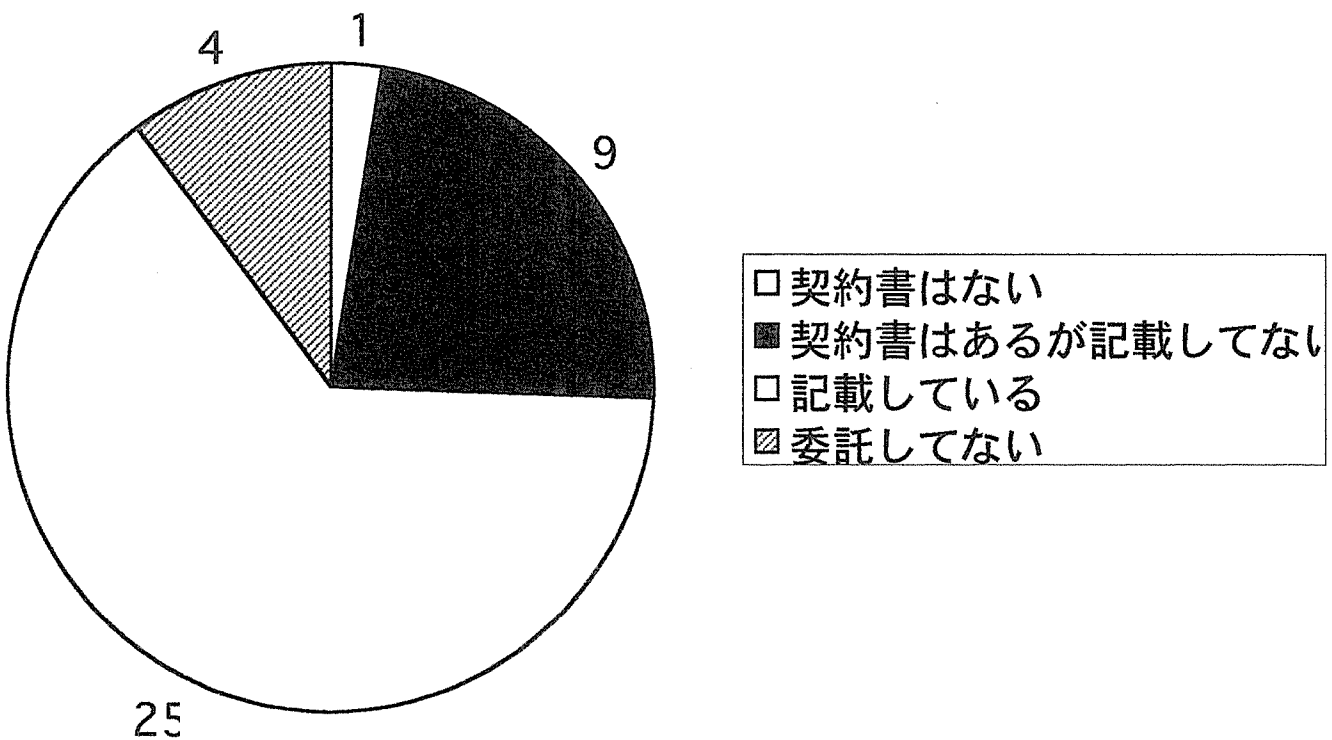

図 4

従業者（派遣を含む）に対し、採用、退職の際に
機密保持に関する書面を取り交わすなどして
就業上のセキュリティに関する義務を明確にしてい

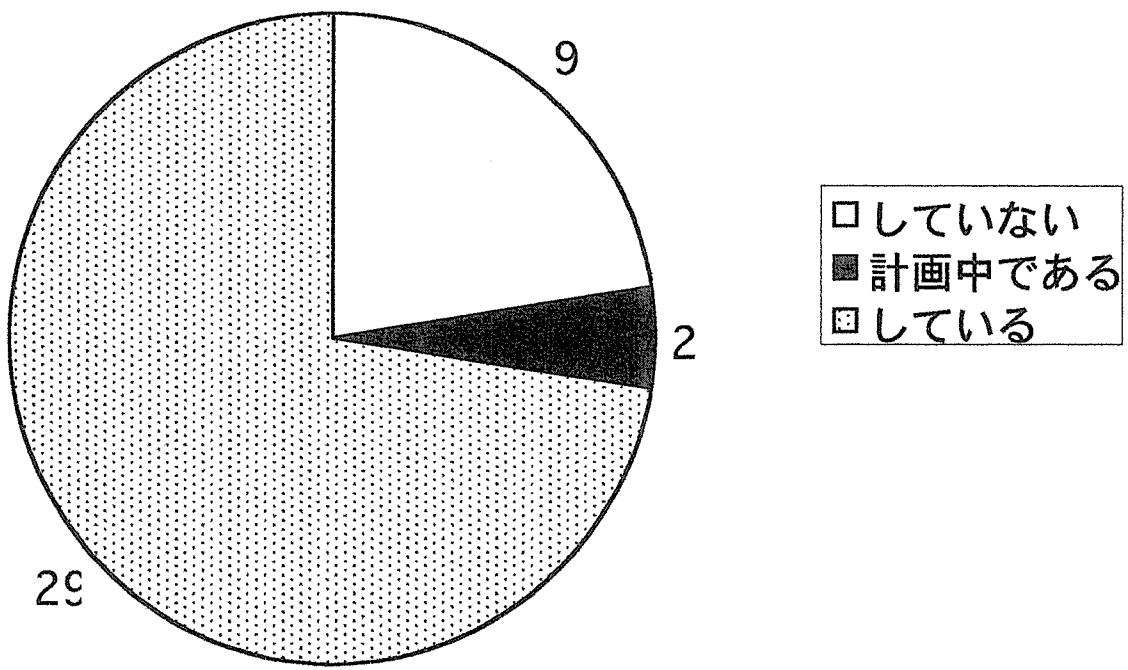

図5

施設に出入りする外部の人（ベンダーや清掃業者など）に対
セキュリティ上のルールを定めているか

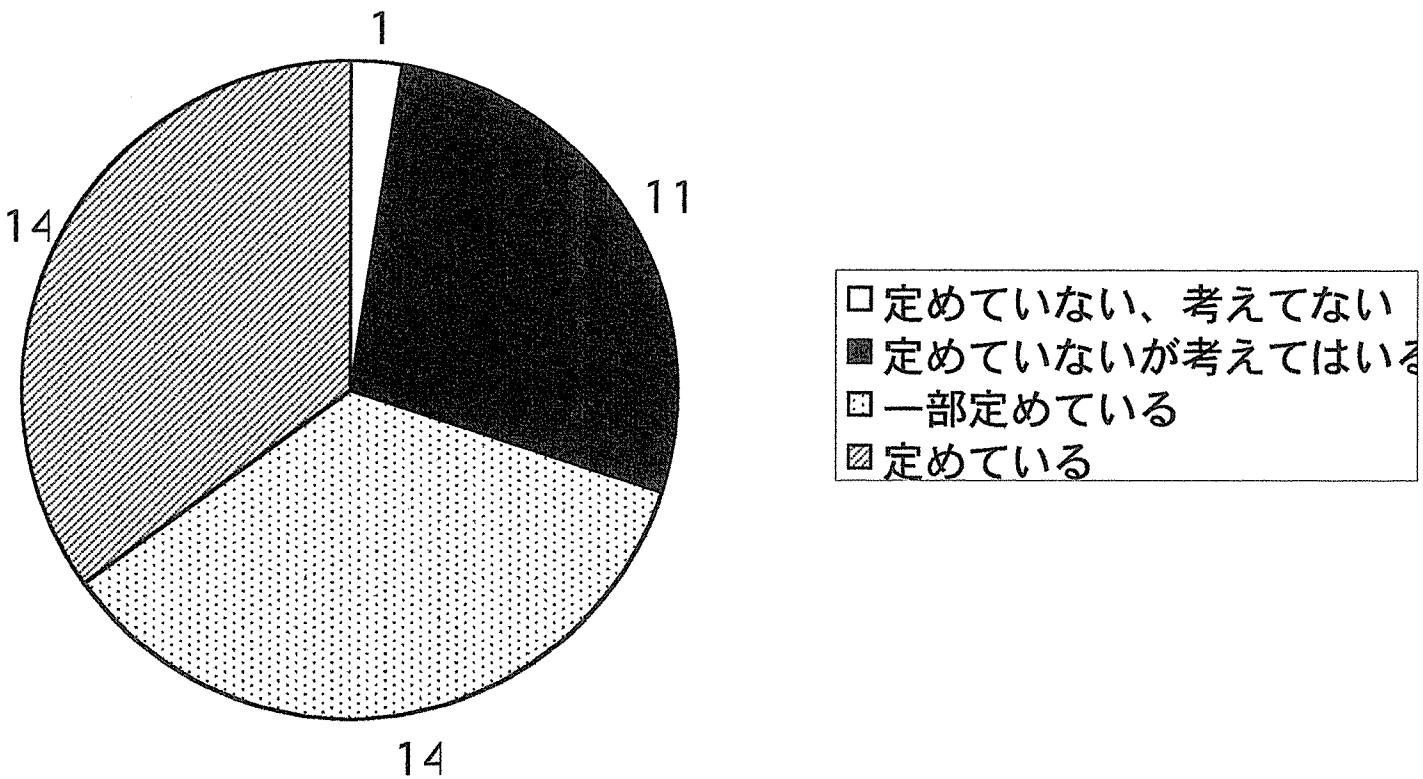

図６

特にセキュリティを強化したい建物や区画について、必要に応じたセティ対策（外部とのセキュリティ上の境界を明確に意識した入退館・管理や警報装置の設置など）を実施しているか

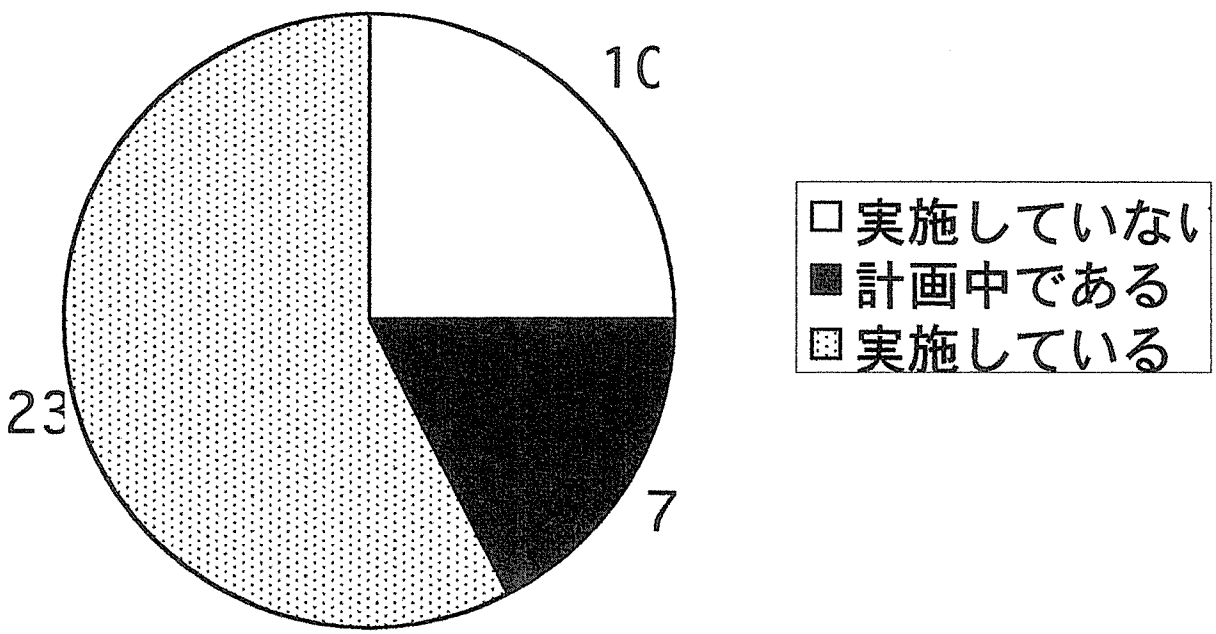

図 7

患者情報や記憶媒体の適切な管理
（サーバーの管理、キャビネットの施錠やプリント出力の放置禁止、
体の粉砕廃棄など）を行っているか

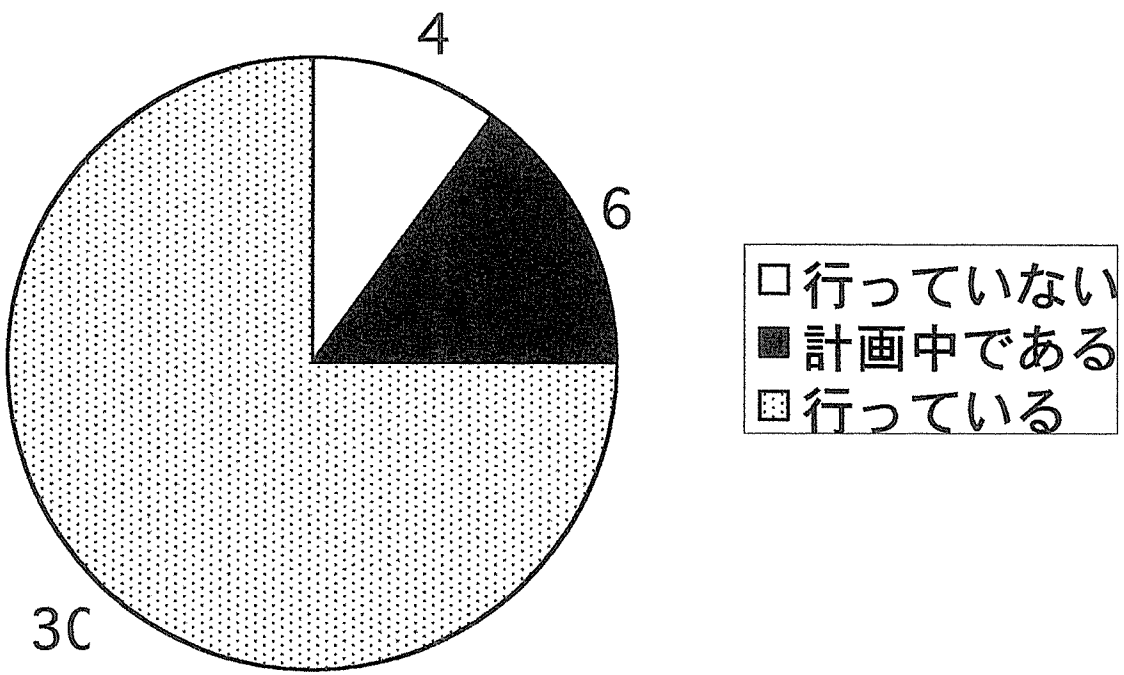

図 8

情報システムの運用に必要なセキュリティ対策
（セキュリティ要件の明確化、各種手順書の策定、
セキュリティログの記録とチェックなど）を実施して

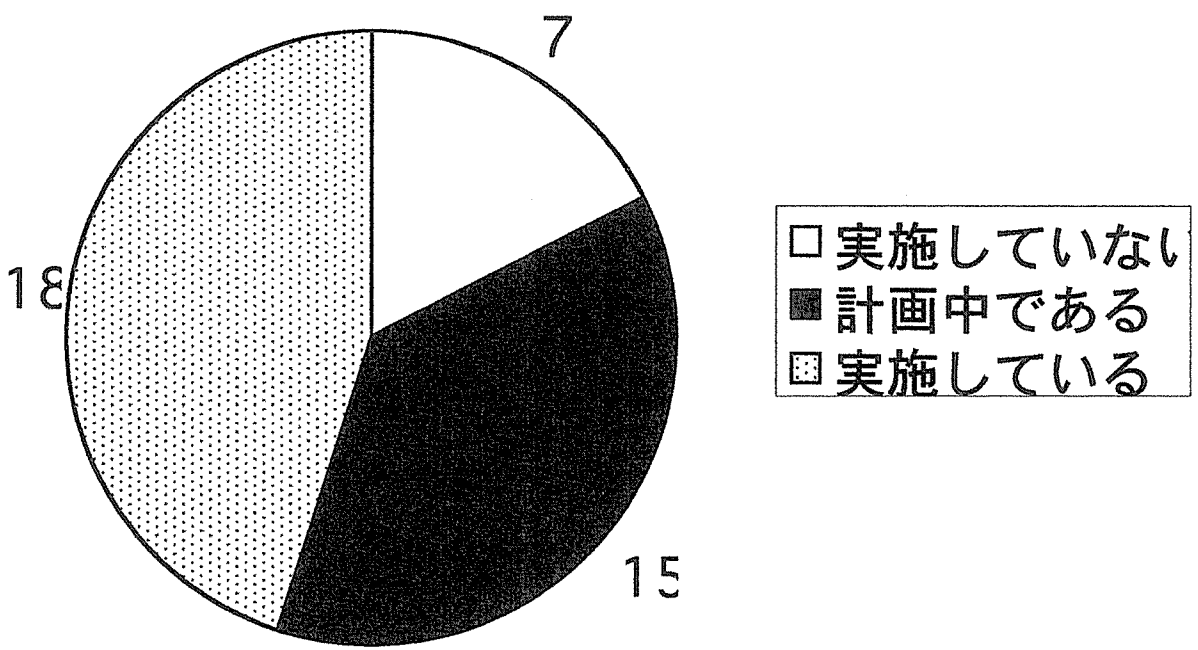

図９

不正ソフトウェア（ウイルス、ワーム等）に対する対策
（コンピュータウイルス対策ソフトを導入し、パターンファイルのアップデート
ことなどを含む）実施しているか

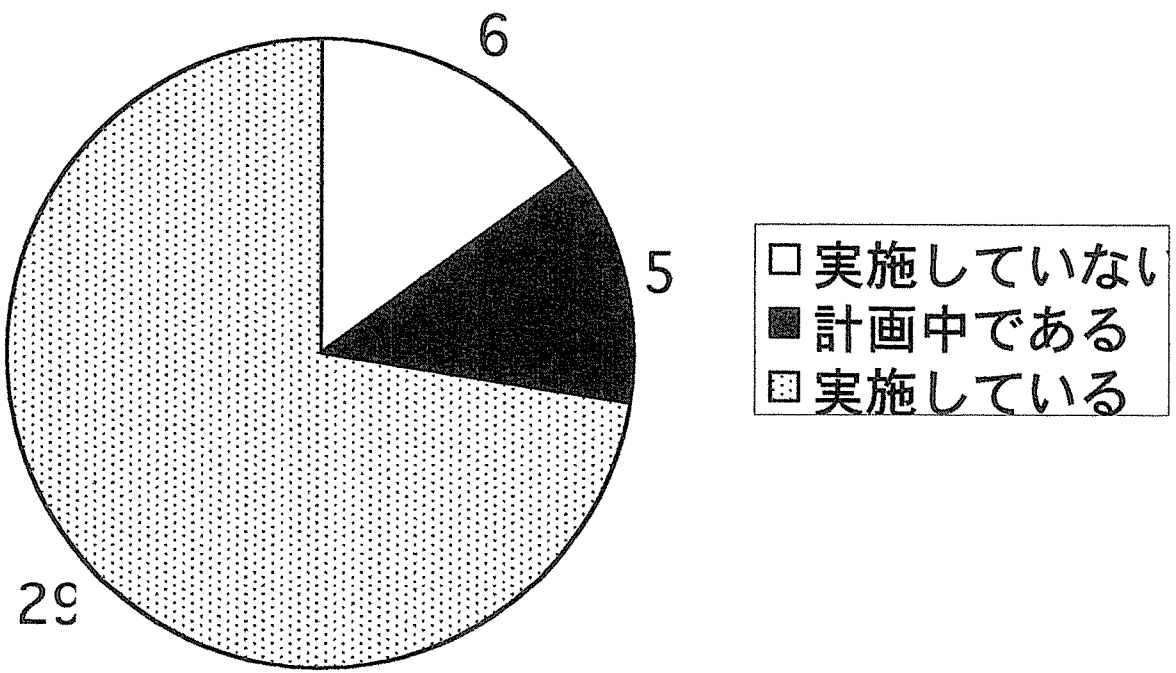

図10

導入しているソフトウェアに対して適切な脆弱性対策（セキュリティを考慮した設定や、脆弱性修正プログラムの適用、定脆弱性検査など）を実施しているか

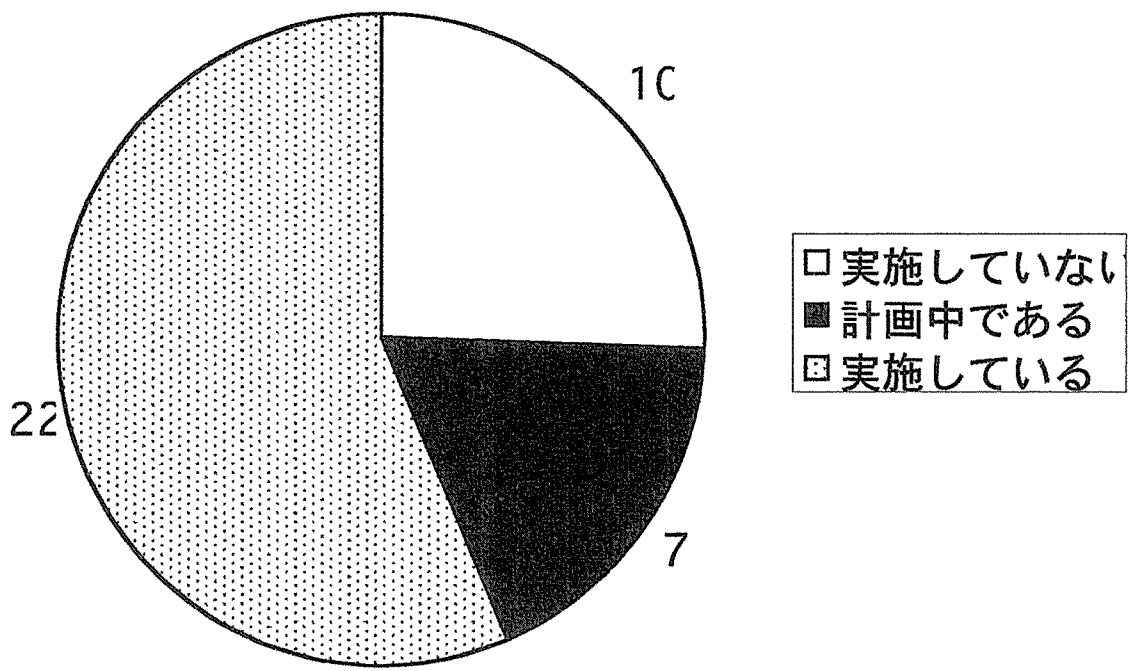

図11

通信ネットワークに流れるデータに関して、暗号化な適切な保護策（ＶＰＮの使用や、重要な情報のＳＳＬ暗号化を含む）を実施しているか

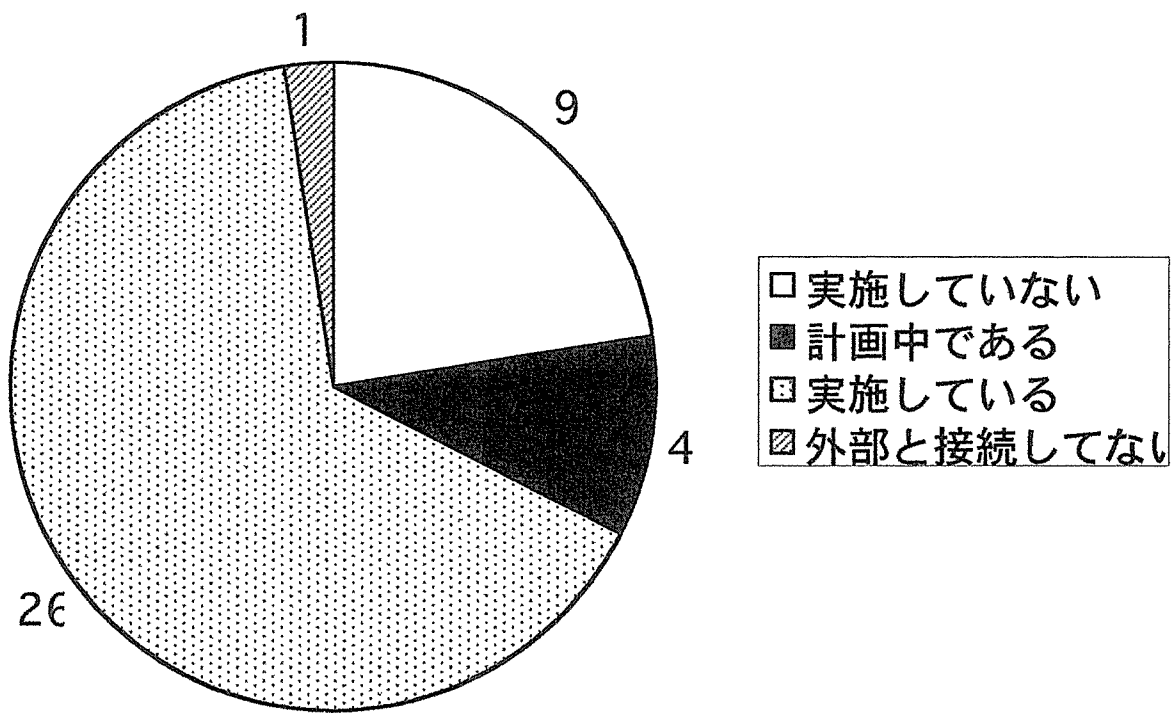

図12

画像や患者情報を含んだ、記憶媒体に対して、盗難、紛失等を想定し
切なセキュリティ対策を実施しているか
（携帯PC や記憶媒体の使用場所は、施設外のすべての場所を含む）

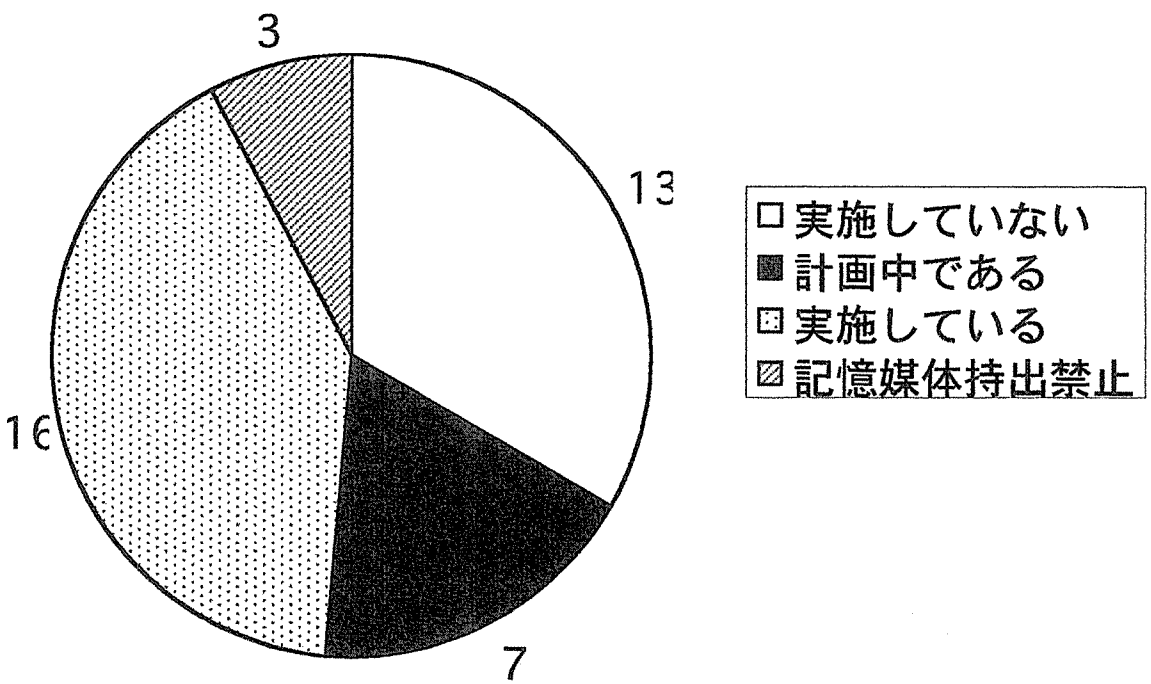

図13

画像や患者情報（データ）へのアクセスを制限するための
ユーザ管理（不要なユーザＩＤの定期的な見直しや共用ＩＤの制限、
スワードの設定禁止など）や認証を適切に実施しているか

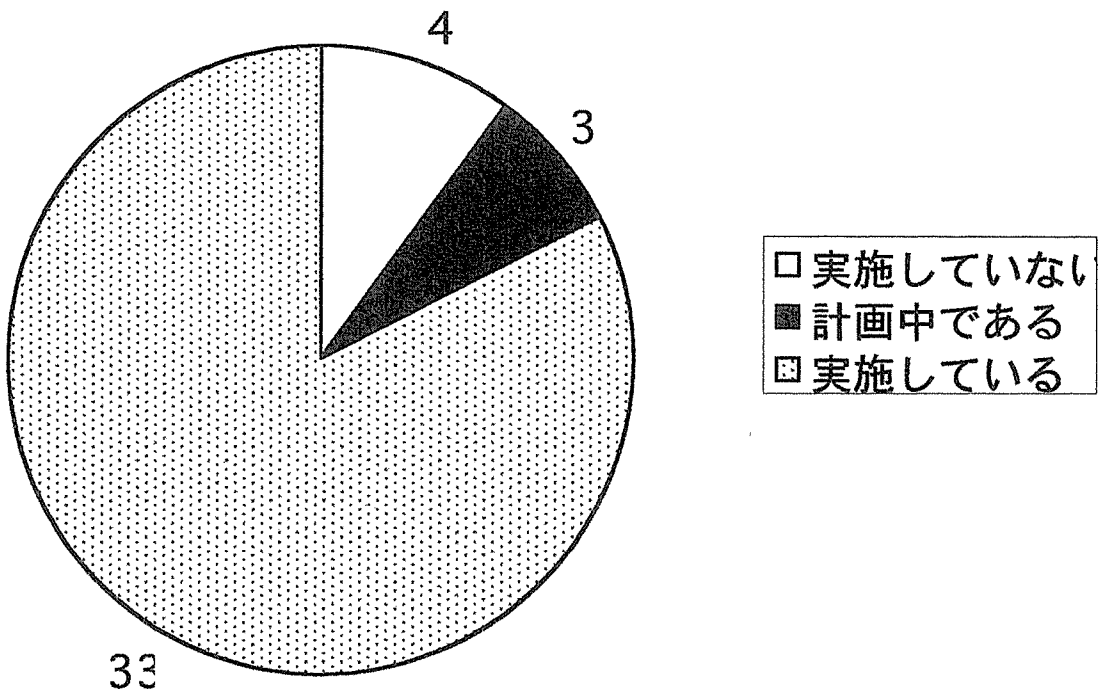

図14

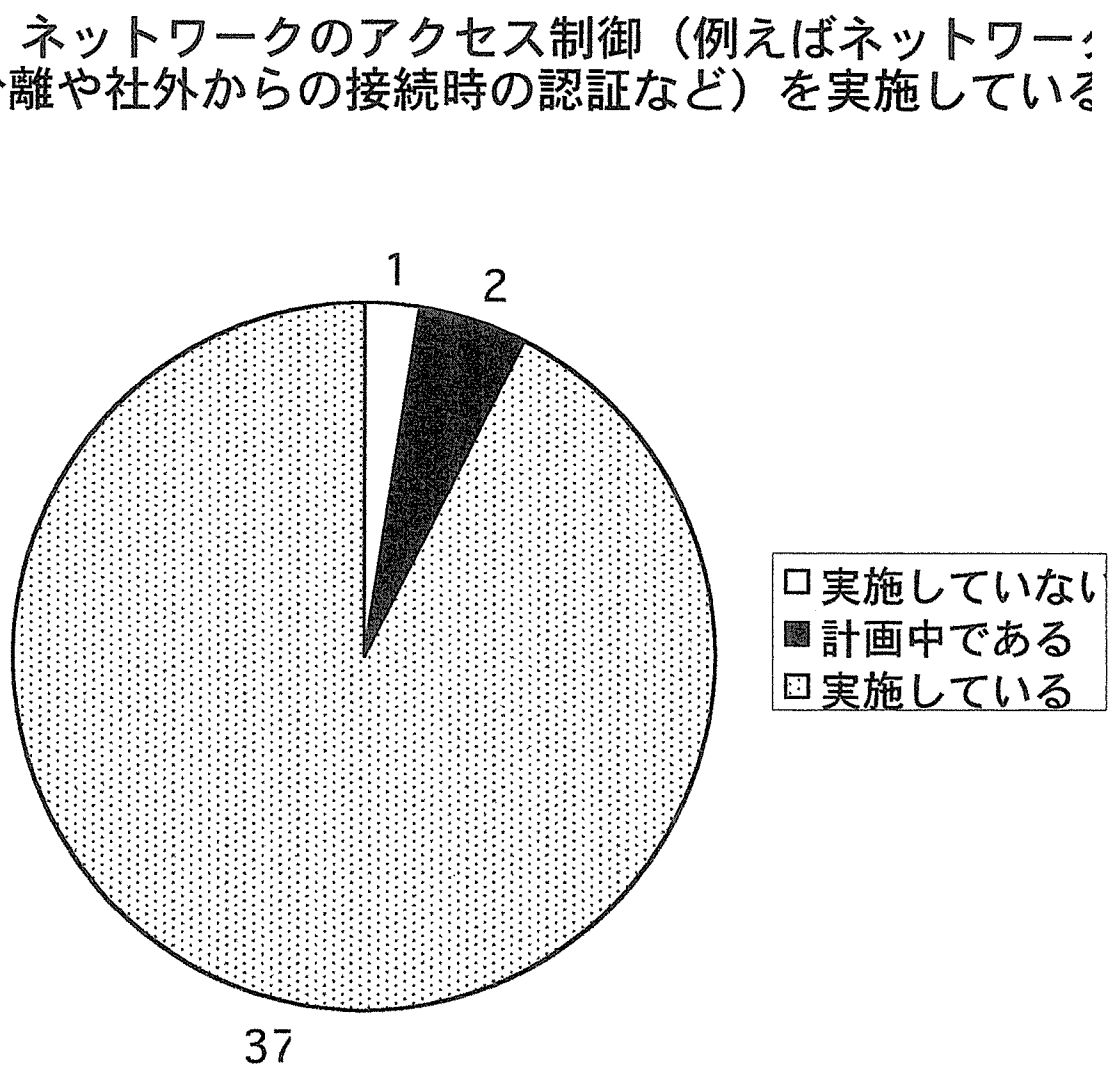
ネットワークのアクセス制御（例えばネットワー
分離や社外からの接続時の認証など）を実施してい
1
2
37
実施していない
計画中である
実施している

図15

情報システムの障害発生を想定した適切な対策（システムの冗長構成
バックアップ、障害対応手順書の策定、運用記録の取得、
社外委託先とのサービスレベルの合意など）を実施しているか

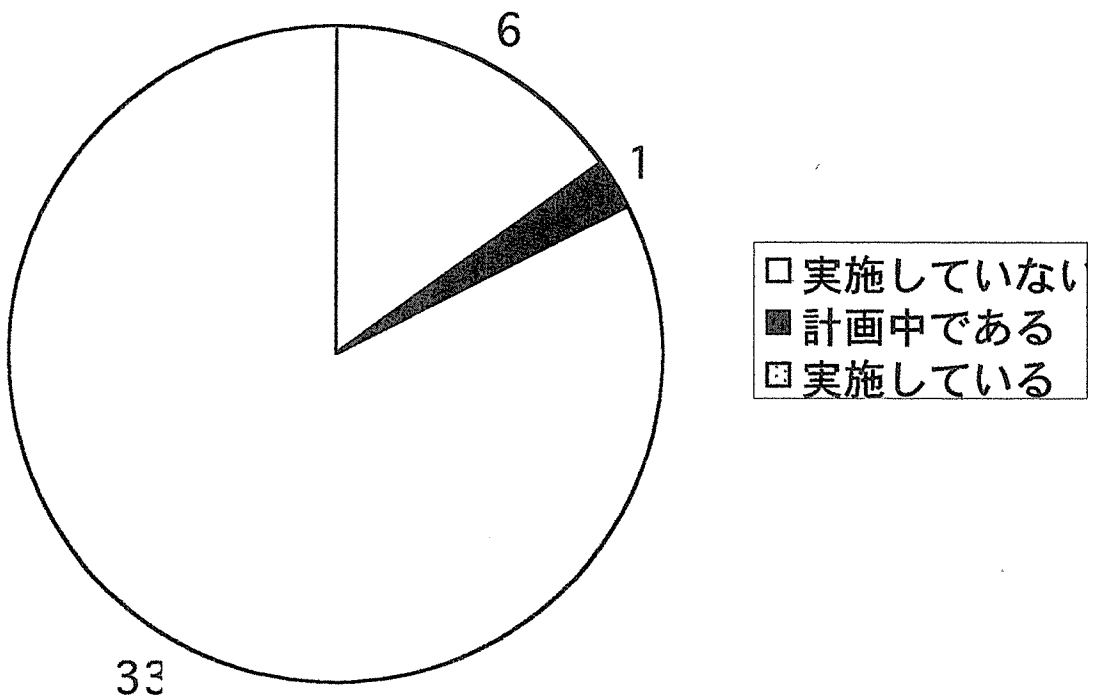

図16

情報セキュリティに関連する事件や事故が発生した際の行動
報告、判断の基準を定めた対応手続を準備しているか

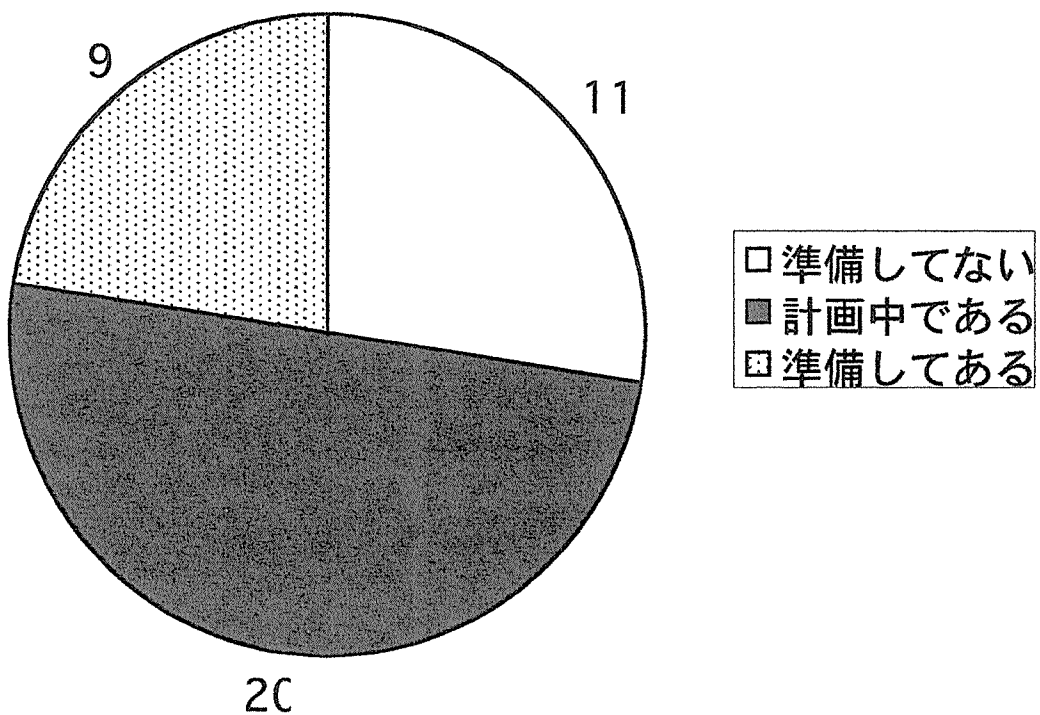

図17

何らかの理由で情報システムが停止した場合でも業務を継
するための取り組みが、組織全体を通じて検討されていま

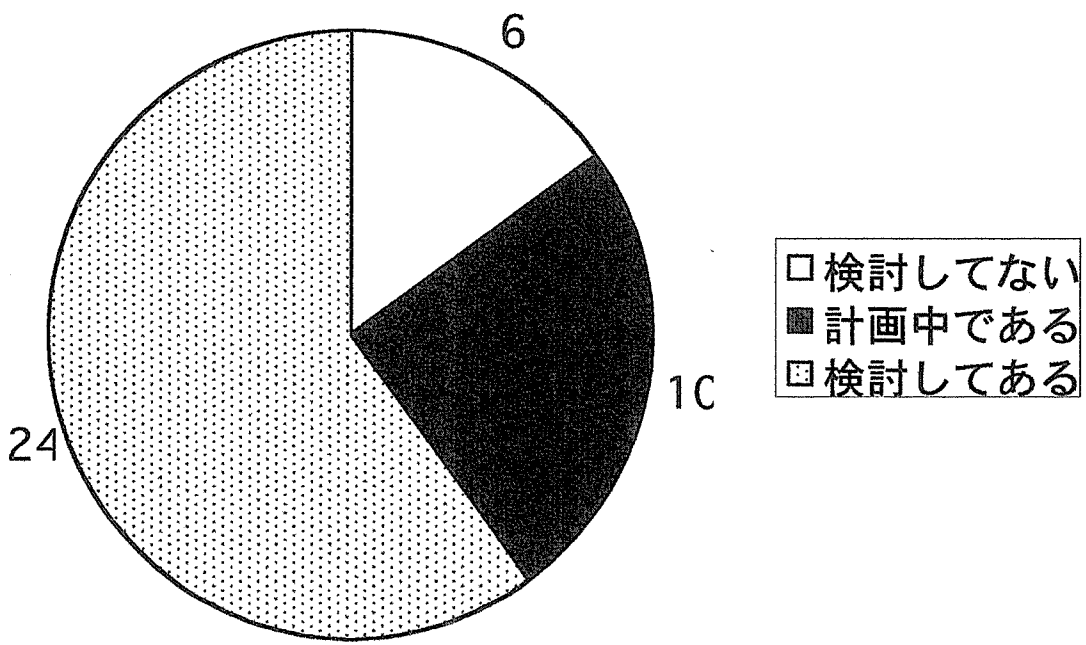

図18

現状のセキュリティ対策の全体としての評