



JIRA セキュリティ委員会
リモートサービスに関するセキュリティアンケート調査報告書

2012 年 3 月

社団法人 日本画像医療システム工業会
医用画像システム部会 セキュリティ委員会
JIRA/ JAHIS 合同リモートサービスセキュリティ WG

調査設計

【調査要綱】

1. 調査目的

リモートサービスの実施状況や契約形態を把握するため。

2. 調査対象

- ・ JIRA 医用画像システム部会登録会員各社
- ・ JAHIS 会員各社

3. 調査項目

別紙添付アンケート用紙参照

4. 調査方法

電子メール通知アンケート形式

(対象の選定) JIRA 医用画像システム部会登録会員、JAHIS 会員

5. 調査スケジュール

アンケート期間：2011 年 12 月 01 日（木）～12 月 28 日（水）

実査期間：2011 年 12 月 01 日（木）～2012 年 2 月 29 日（水）

集計・分析期間：2011 年 12 月 29 日（木）～2012 年 2 月 29 日（水）

6. 回収数

有効回収数：67 社

7. 集計方法

各質問項目別の単純・クロス集計

【調査設計・実施】

- ・ JIRA セキュリティ委員会
JIRA/JAHIS 合同リモートサービスセキュリティ WG
- ・ JAHIS セキュリティ委員会
JAHIS/JIRA 合同リモートサービスセキュリティ WG

セキュリティアンケート集計結果

アンケート対象.....	4
1 リモートサービスについて	6
2 厚生労働省「医療情報の安全管理に関するガイドライン」について	7
3 JESRA・JAHIS 標準の「リモートサービスセキュリティガイドライン」について	10
4 実施しているリモートサービスについて	12
5 質問間クロス集計結果①：対象システム間集計	21
6 質問間クロス集計結果②：資本金間集計	30
7 質問間クロス集計結果③：資本金と対象システム間集計	39
8 総括	40

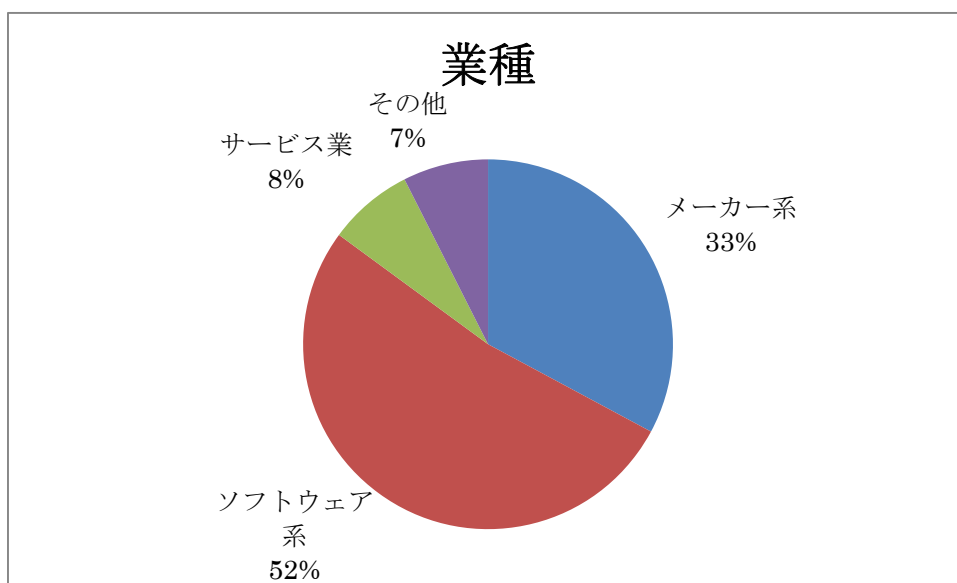
アンケート対象

<アンケート対象の業種>

業種 : メーカー系／ソフトウェア系／サービス系／その他

<集計結果>

メーカー系 33%、ソフトウェア系 52%、サービス系 8%、その他 7%であった。



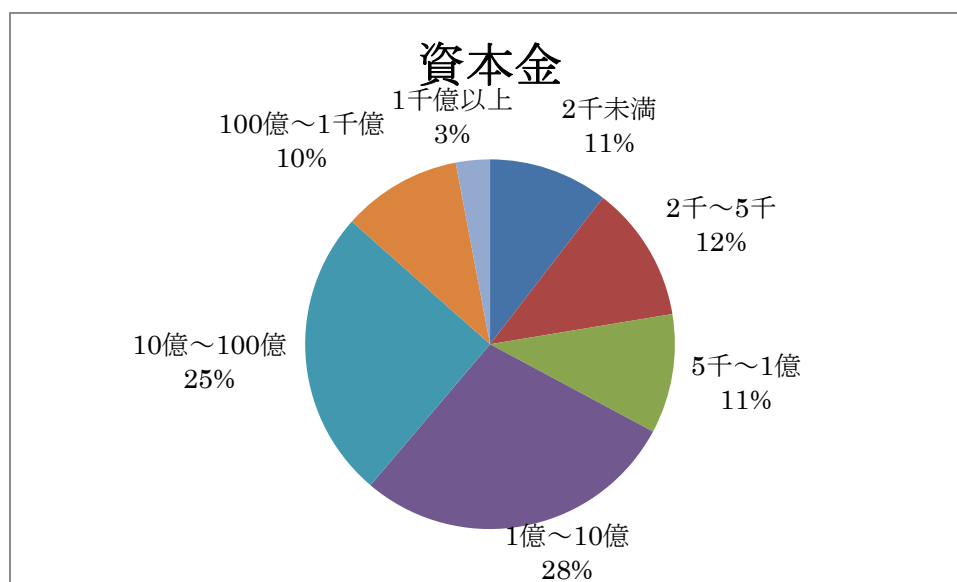
※アンケート本体では「職種」と記載。

<アンケート対象の資本金>

資本金：2 千万円未満／2 千万円～5 千万円／5 千万円～1 億円／1 億円～10 億円
／10 億円～100 億円／100 億円～1 千億円／1 千億円以上

<集計結果>

2 千万円未満 11%、2 千万円～5 千万円 12%、5 千万円～1 億円 11%、1 億円～10 億円 28%、10 億円～100 億円 25%、100 億円～1 千億円 10%、1 千億円以上 3%であった。



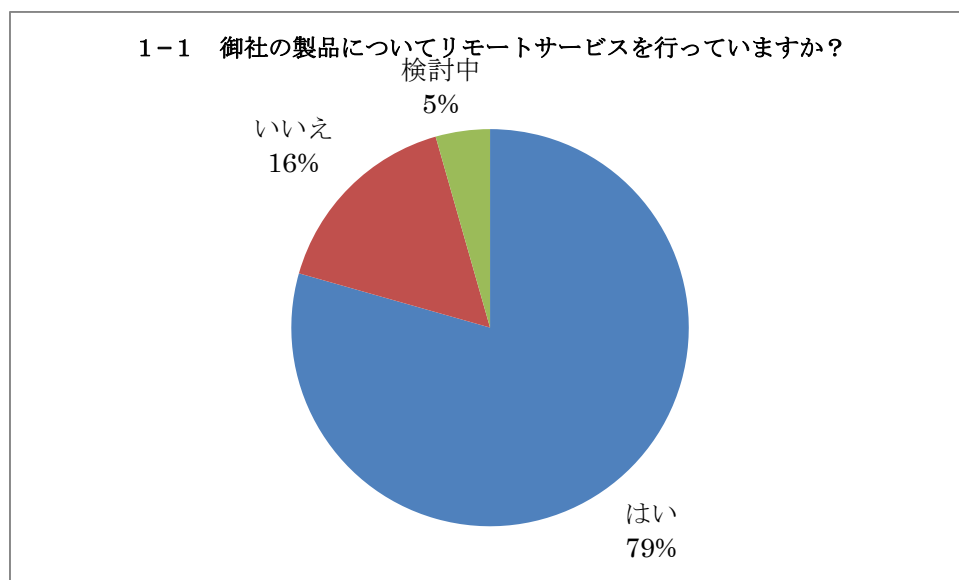
1 リモートサービスについて

1-1 御社の製品についてリモートサービスを行っていますか？

※上記の質問に「はい」または「検討中」と回答された方は、以下の設問に回答願います。

<集計結果>

はい 79%、いいえ 16%、検討中 5%となった。



2 厚生労働省「医療情報の安全管理に関するガイドライン」について

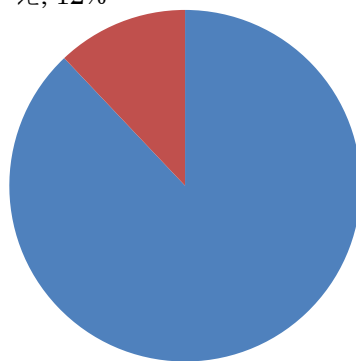
2-1 安全管理ガイドラインにリモートサービスに関する要求事項があることをご存知ですか？

<集計結果>

はい 88%、いいえ 12%となり、安全管理ガイドラインにリモートサービスに関する要求事項が記載されていることの認識が高いことが分かった。

2-1 安全管理ガイドラインに、リモートサービスに関する要求事項があることをご存知ですか？

いいえ, 12%



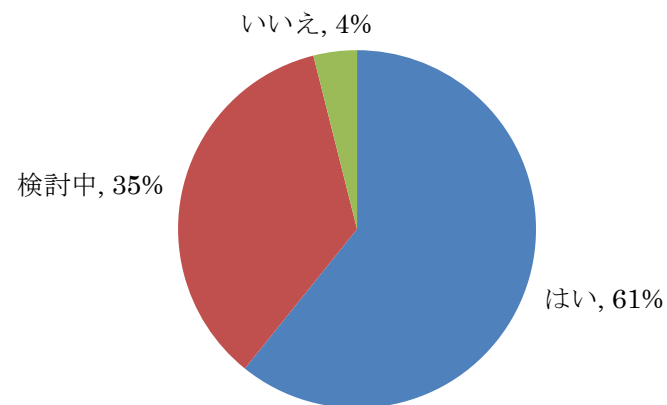
はい, 88%

2-2 2-1 が「はい」の方にお伺いします。リモートサービスの自社ルールに、その内容を盛り込んでいますか？

<集計結果>

はい 61%、いいえ 4%、検討中 35%となり、自社サービスへ展開済みが半数以上を占めたが、3 割以上の企業では検討中となっている。各企業の前向きな対応が見てとれる。

2-2 2-1が「はい」の方にお伺いします。リモートサービスの自社ルールに、その内容を盛り込んでいますか？

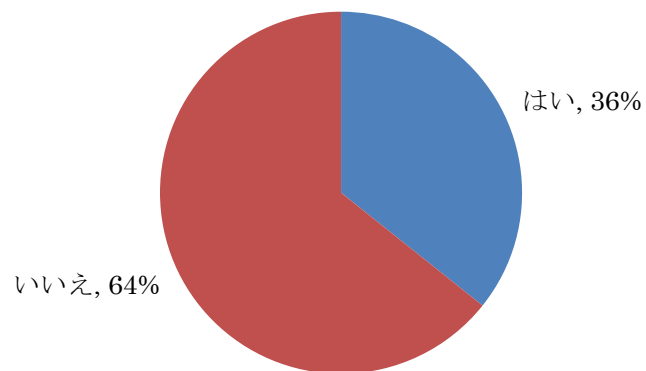


2-3 リモートサービスに関して安全管理ガイドラインの要求事項の遵守を顧客から要求されたことはありますか？

＜集計結果＞

はい 36%、いいえ 64%となり、顧客からの対応要求は過半数を満たしてはいないが、医療機関からの安全管理ガイドラインに対する準拠要請はあったことが確認できる。

2-3 リモートサービスに関して、安全管理ガイドラインの
要求事項の遵守を顧客から要求されたことはありますか？



3 JESRA・JAHIS 標準の「リモートサービスセキュリティガイドライン」

について

3-1 RSS ガイドラインが策定されていることをご存知ですか？

3-2 RSS ガイドラインの内容をご存知ですか？

3-3 3-2 が「はい」の方にお伺いします。リモートサービスの自社ルールに、その内容を盛り込んでいますか？

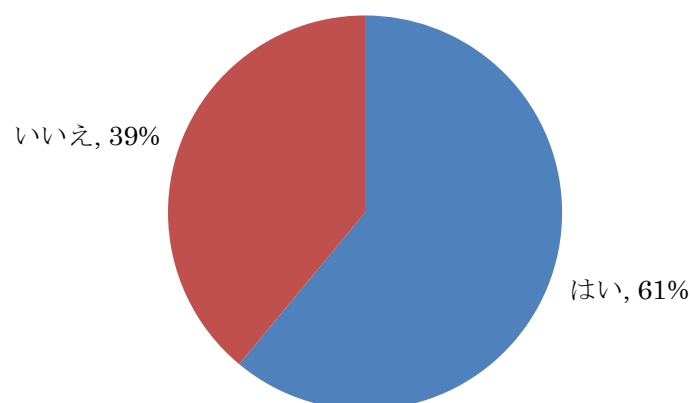
<集計結果>

3-1 では、はい 61%、いいえ 39%となり、過半数以上の企業にリモートサービスセキュリティガイドライン（以下、RSS ガイドライン）の存在が認識されていることが分かった。

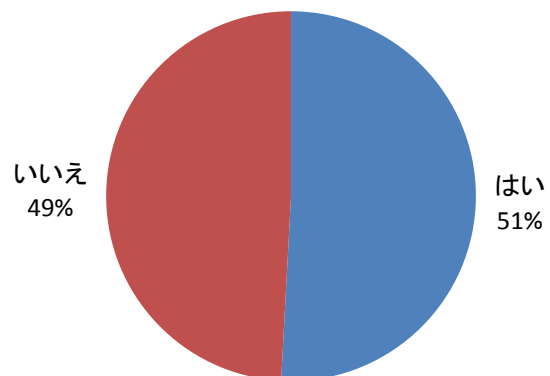
3-2 では、はい 51%、いいえ 49%となり、RSS ガイドラインの内容に対して今後の啓発の必要性が見てとれる。

3-3 では、はい 53%、いいえ 10%、検討中 37%となり、約 3 割の企業が RSS ガイドラインを自社サービスのリスクアセスメント時に参考いただけたことが分かった。

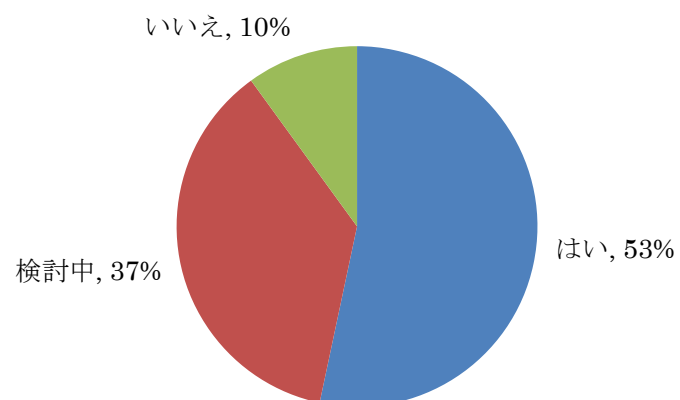
3-1 RSSガイドラインが策定されていることをご存知ですか？



3-2 RSSガイドラインの内容をご存知ですか？



3-3 3-2が「はい」の方にお伺いします。リモートサービスの自社ルールに、その内容を盛り込んでいますか？

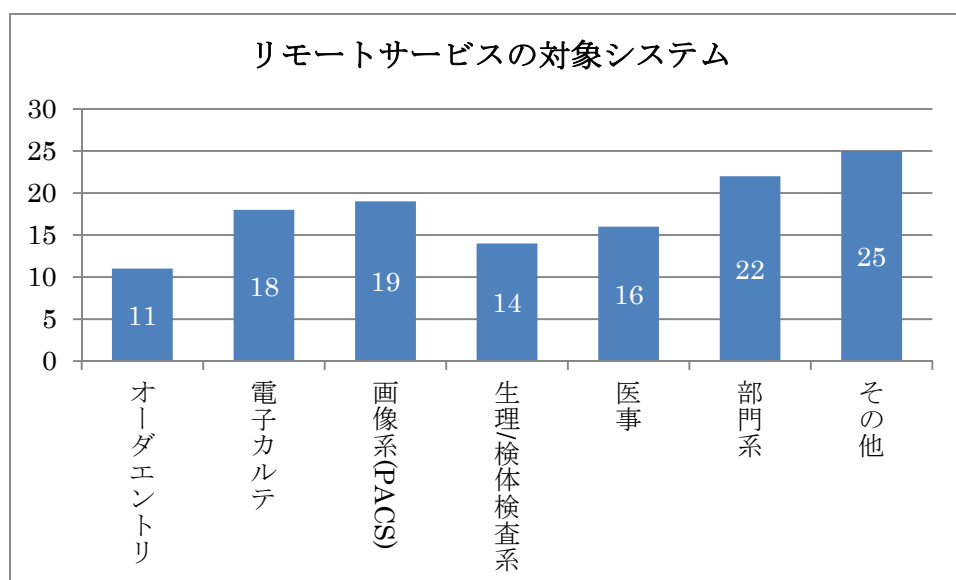


4 実施しているリモートサービスについて

4-1 リモートサービスを行っている対象システムは何ですか？（複数回答可）

＜集計結果＞

オーダエントリ 11 件、電子カルテ 18 件、画像系 19 件、生理・検体検査系 14 件、医事 16 件、部門系 22 件、その他 25 件となった。

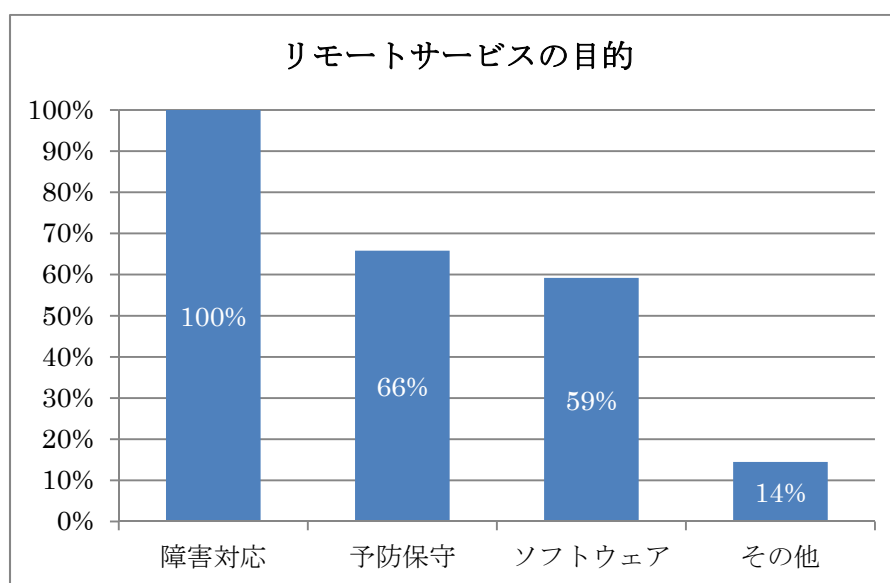


4・2 行っているリモートサービスの目的は何ですか？（複数回答可）

＜集計結果＞

リモートサービスの共通の目的としては障害対応が 100%となった。続いて予防保守 66%、ソフトウェア（更新など）59%、その他 14%となった。RSS ガイドラインが提示している 3 つの目的（障害対応・予防保守・ソフトウェア管理）に合致した回答となっていることが分かった。

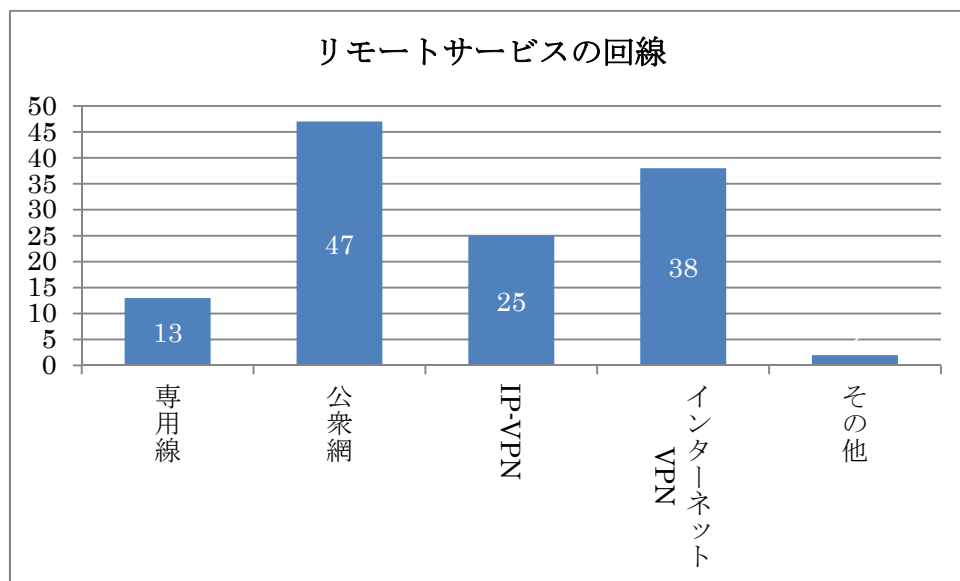
その他の内容は、Q&A、操作指導、マスタ更新などであった。



4・3 リモートサービスの回線は何ですか？（複数回答可）

<集計結果>

専用線 13 件、公衆網 47 件、IP-VPN25 件、インターネット VPN38 件、その他 2 件となった。



※アンケート本体では 4-4 と記載。

4-4 リモートサービスの回線は常時接続ですか？

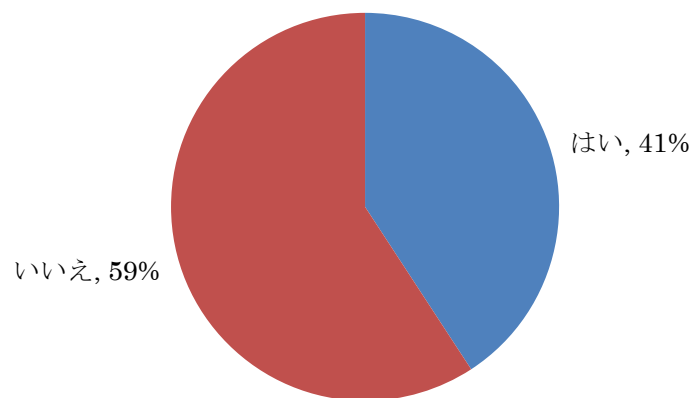
4-5 リモートサービスの接続時に相手先に承諾を得ていますか？

<集計結果>

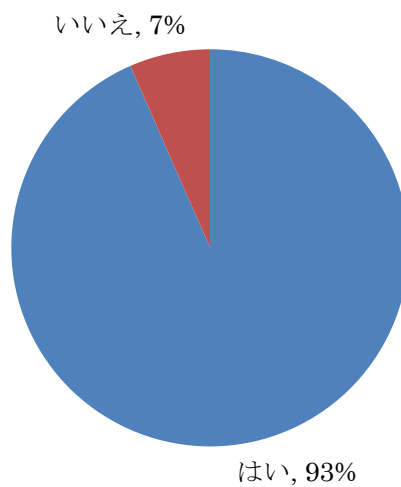
4-4 では、はい 41%、いいえ 59%となった。

4-5 では、はい 93%、いいえ 7%となった。常時接続が約過半数の中で、やはりリモートサービスの開始時には医療機関の承諾を得ていることが見てとれる。

4-4 リモートサービスの回線は常時接続ですか？



4-5 リモートサービスの接続時に相手先に承諾を得ていますか？



※アンケート本体では 4-4 を 4-3 と記載。

4－6 リモートサービス作業中に患者個人情報にアクセスすることがありますか？

4－7 リモートサービス作業中に患者個人情報をダウンロードすることがありますか？

4－8 リモートサービス作業中に患者個人情報を変更することがありますか？

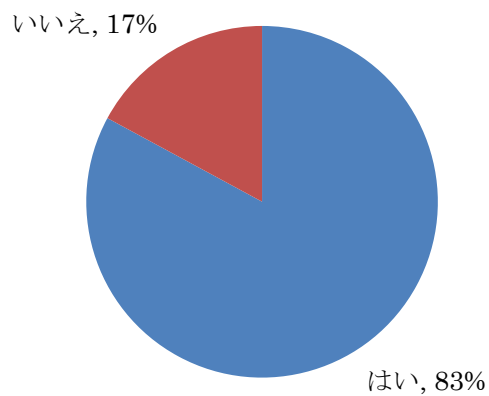
<集計結果>

4-6 では、はい 83%、いいえ 17%となった。

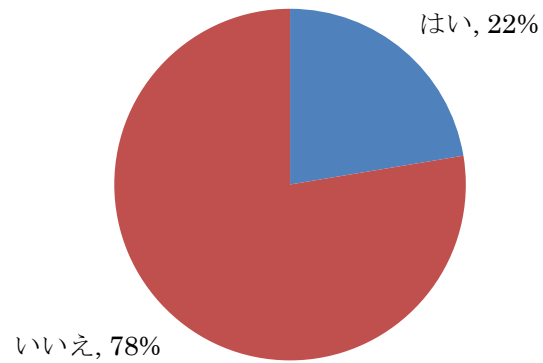
4-7 では、はい 22%、いいえ 78%となった。

4-8 では、はい 16%、いいえ 84%となった。

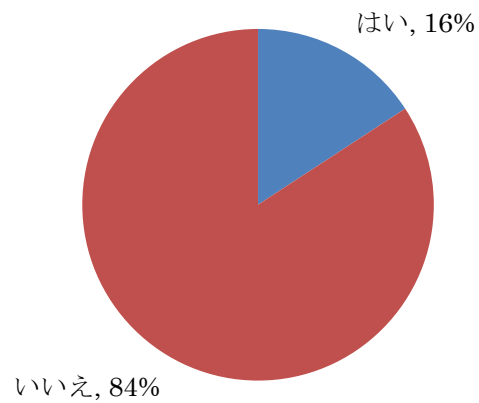
4-6 リモートサービス作業中に患者個人情報にアクセスすることがありますか？



4-7 リモートサービス作業中に患者個人情報をダウンロードすることがありますか？



4-8 リモートサービス作業中に患者個人情報を変更することがありますか？

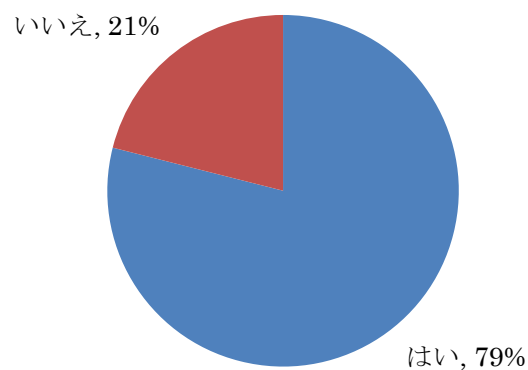


- 4-9 締結した保守契約の中にリモートサービス専用項目を含んでいますか？
- 4-10 SLA(サービス・レベル・アグリーメント)の中にリモートサービスに関する条項はありますか？
- 4-11 守秘義務に関する契約を締結していますか？
- 4-12 リモートサービスに関する標準契約書を用意していますか？

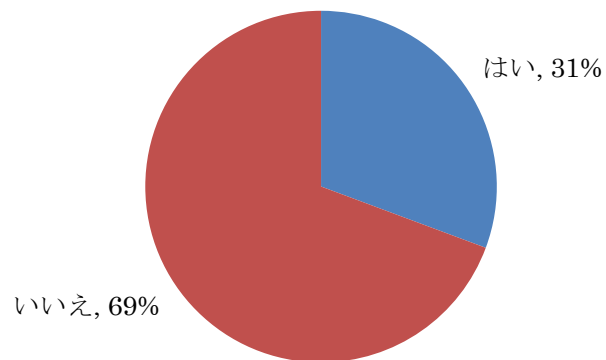
<集計結果>

- 4-9 では、はい 79%、いいえ 21%となった。
- 4-10 では、はい 31%、いいえ 69%となった。なお、本設間においては、本アンケートにおける SLA に関する説明が明記されておらず、保守契約の中に合意レベルの設定がある場合でも「いいえ」を選択された回答があったと想定される。
- 4-11 では、はい 88%、いいえ 12%となった。
- 4-12 では、はい 64%、いいえ 36%となった。

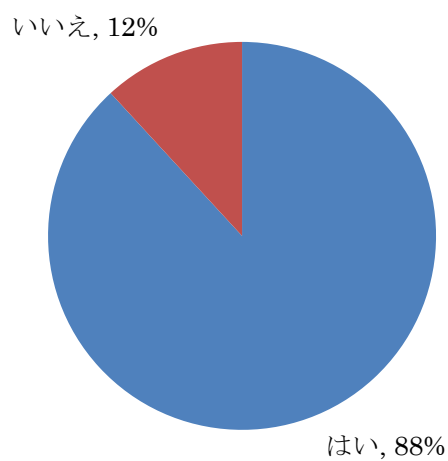
4-9 締結した保守契約の中にリモートサービス専用項目を含んでいますか？



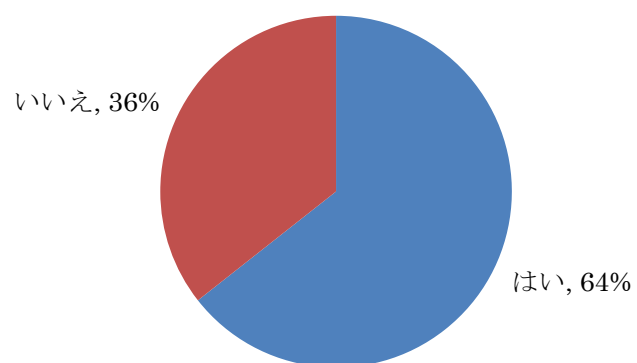
4-10 SLA(サービス・レベル・アグリーメント)の中にリモートサービスに関する条項はありますか？



4-11 守秘義務に関する契約を締結していますか？



4-12 リモートサービスに関する標準契約書を用意していますか？



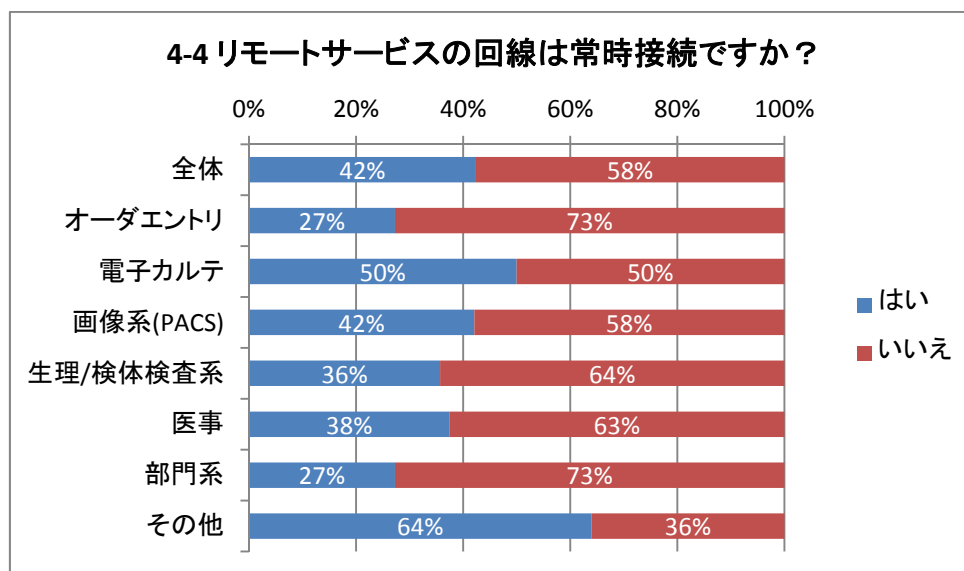
5 質問間クロス集計結果①：対象システム間集計

＜対象システム集計＞

（設問 4-4）リモートサービスの回線は常時接続ですか？

＜質問間クロス集計結果＞

電子カルテ 50%、画像系 42%で常時接続をリモートサービスの回線として利用していることが分かった。オーダーエントリをはじめ、常時接続以外の回線を利用したリモートアクセスが過半数を占めている。

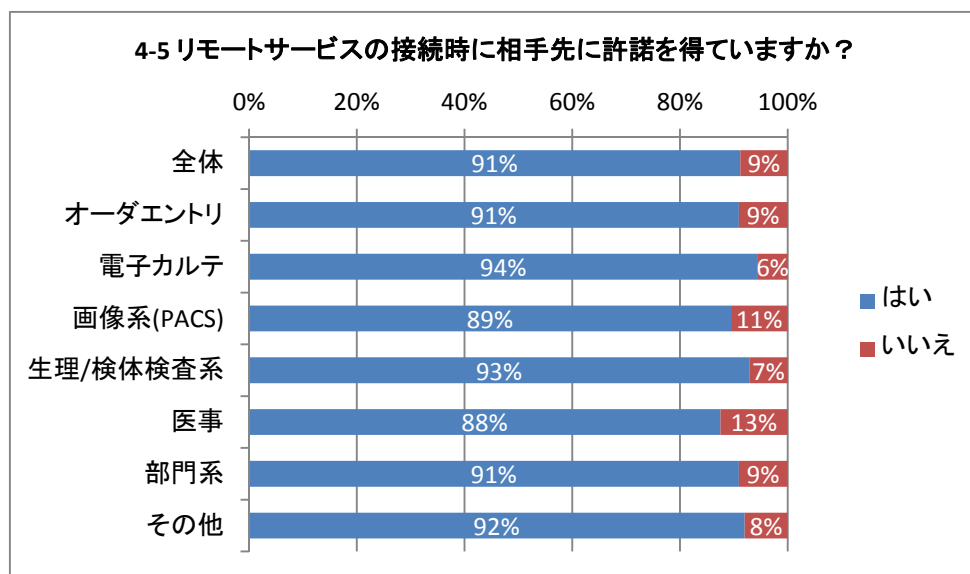


<対象システム集計>

(設問 4-5) リモートサービスの接続時に相手先に許諾を得ていますか？

<質問間クロス集計結果>

全体の 91%が医療機関からの許諾を得ていることから、どのシステムもリモートサービスの接続時に事前の作業申請を行っていることが分かった。

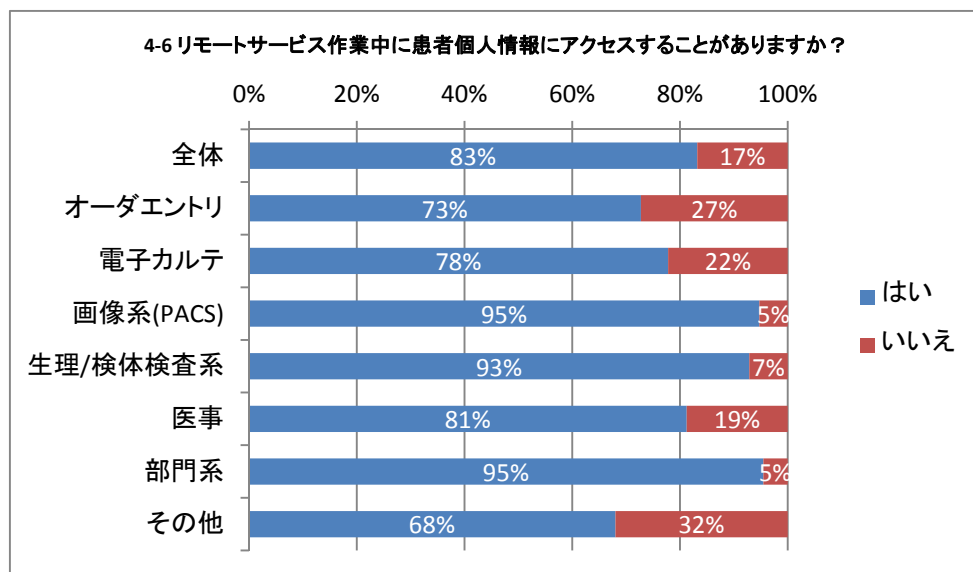


<対象システム集計>

(設問 4-6) リモートサービス作業中に患者個人情報にアクセスすることがありますか？

<質問間クロス集計結果>

リモートサービス対象の大半のシステムが、患者の個人情報にアクセスすることが見てとれ、特に PACS 等の画像系と生理／検体検査系で顕著に表れている。

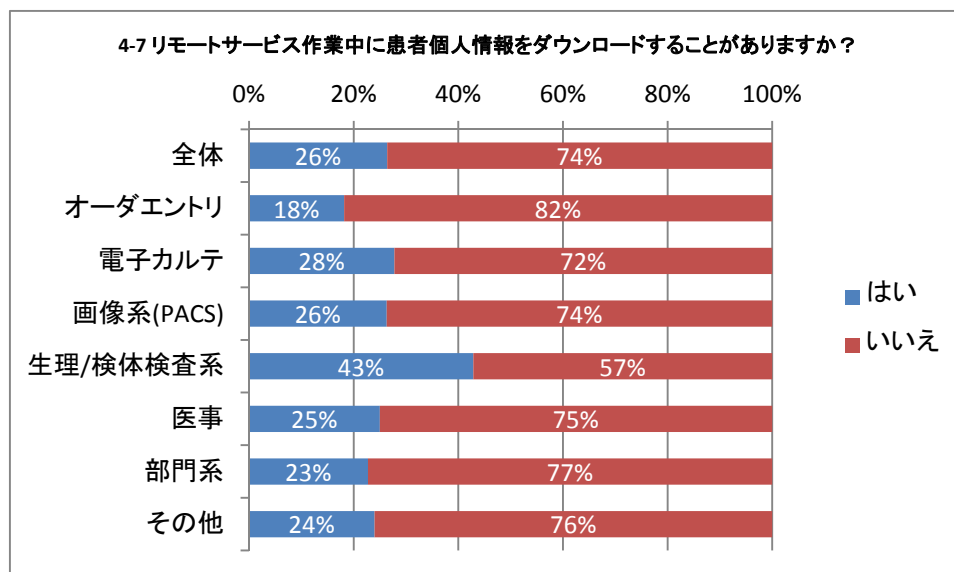


<対象システム集計>

(設問 4-7) リモートサービス作業中に患者個人情報をダウンロードすることがありますか？

<質問間クロス集計結果>

設問 4-6 で全体の 83%が患者の個人情報にアクセスすることに対して、システムの種類によらず患者の個人情報をダウンロードしてリモートサービスを行うケースは比較的少ないことが分かった。

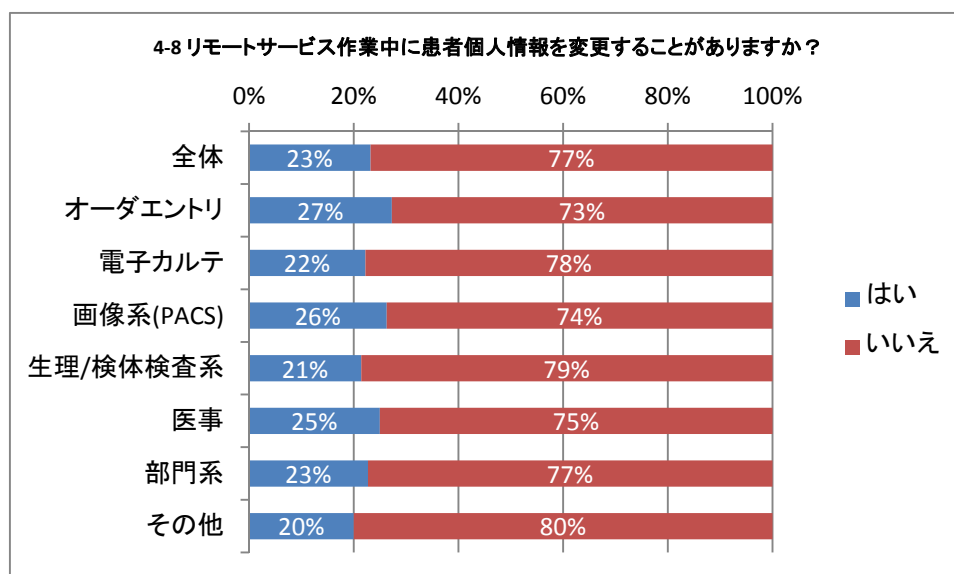


＜対象システム集計＞

（設問 4-8）リモートサービス作業中に患者個人情報を変更することがありますか？

＜質問間クロス集計結果＞

オーダエントリ、電子カルテに関してはリモートメンテナンスで患者の個人情報を変更する作業が比較的多いことが分かった。

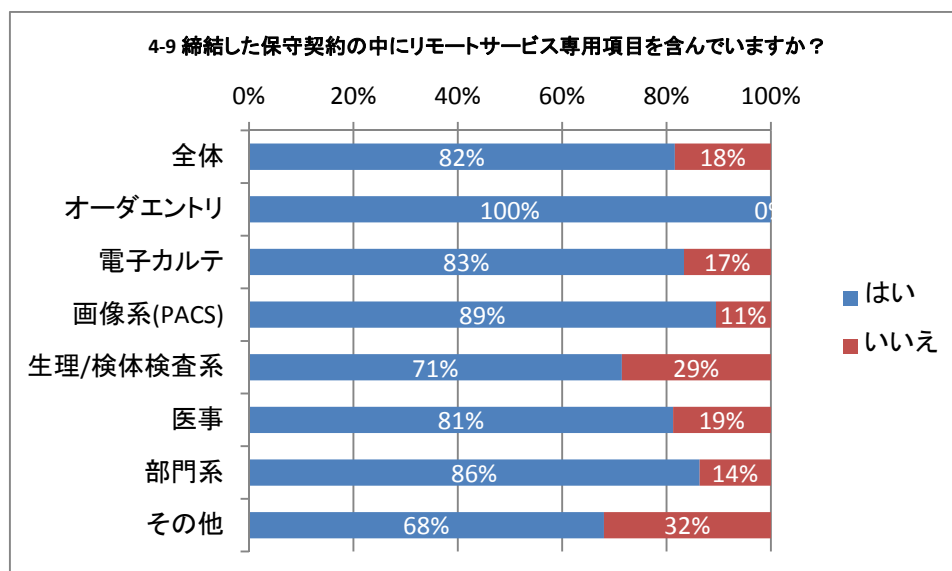


＜対象システム集計＞

（設問 4-9）締結した保守契約の中にリモートサービス専用項目を含んでいますか？

＜質問間クロス集計結果＞

ご回答いただいた全てのオーダーエントリシステムでは、リモートサービス専用項目が保守契約に含まれていることが分かった。生理／検体検査系システムでは約3割のシステムが保守契約にリモートサービス専用項目が含まれていないことから、安全管理ガイドラインの認知度とのクロス集計を後述してみることにした。

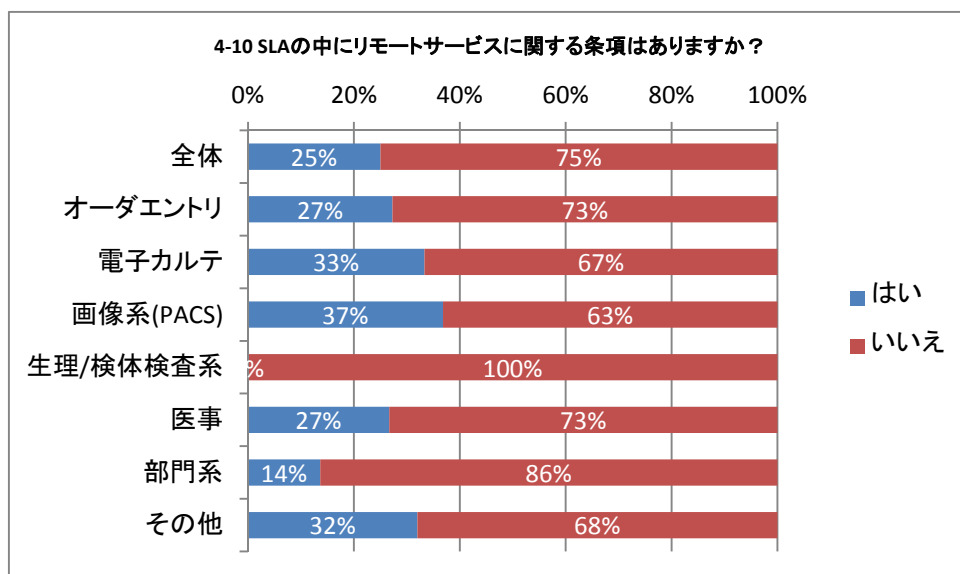


<対象システム集計>

(設問 4-10) SLA の中にリモートサービスに関する条項はありますか？

<質問間クロス集計結果>

画像系システムでは4割弱のシステムでSLAにリモートサービスの条項を含んでいることが分かったが、生理／検体検査系システムでは顕著な数値を得た。

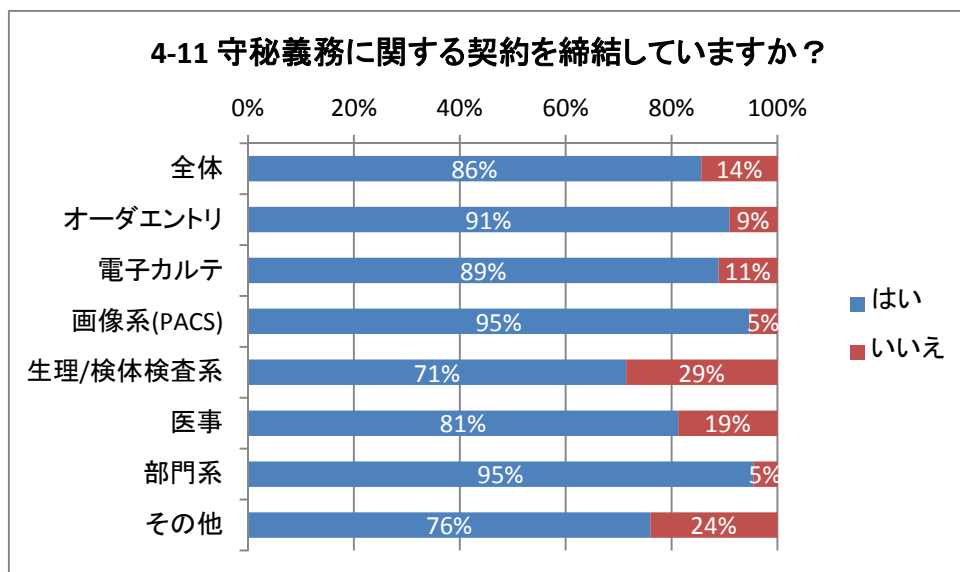


＜対象システム集計＞

（設問 4-11）守秘義務に関する契約をしていますか？

＜質問間クロス集計結果＞

全体として守秘義務に関して高い数値が見てとれるが、生理／検体検査系システムと医事システムでは守秘義務に関する締結がないものが 3 割前後あるようである。

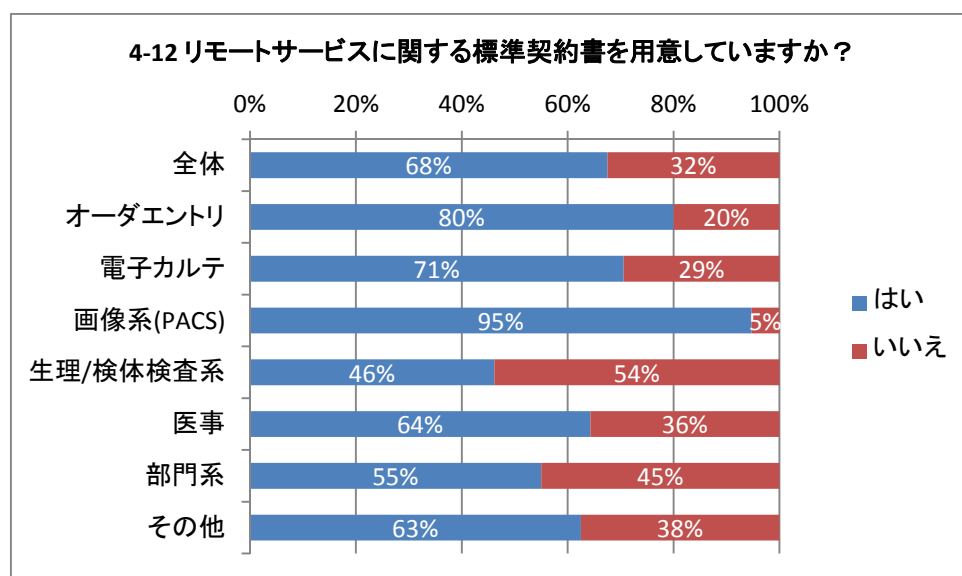


＜対象システム集計＞

（設問 4-12）リモートサービスに関する標準契約書を用意していますか？

＜質問間クロス集計結果＞

システムの種類により差が出る結果となったが、生理／検体検査系システムと部門系システムではリモートサービスに関して標準契約書を用意していないことが見てとれる。ただし、標準契約書ではなく都度の契約を締結していることも考えられる。



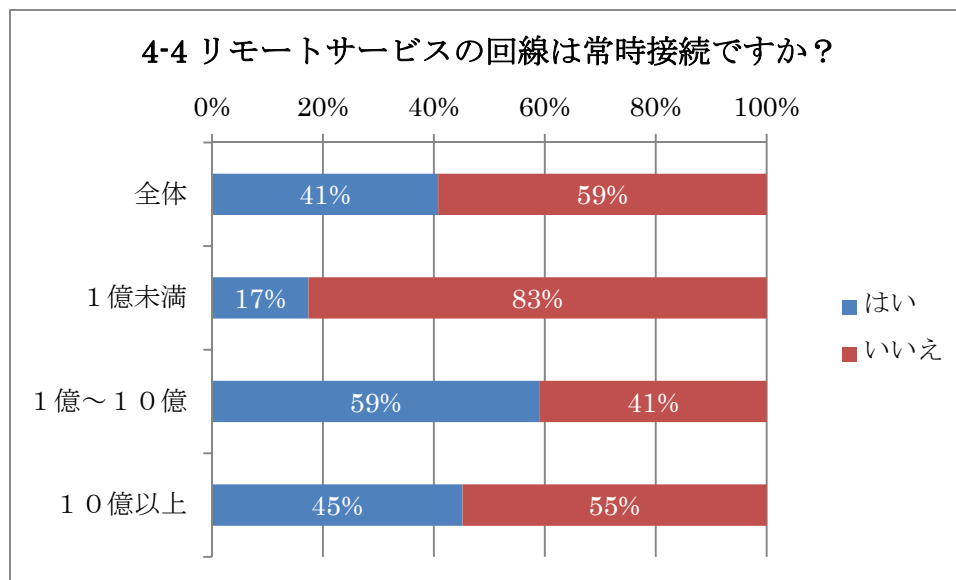
6 質問間クロス集計結果②：資本金間集計

<対象システム集計>

(設問 4-4) リモートサービスの回線は常時接続ですか？

<質問間クロス集計結果>

資本金 1 億未満のベンダでは 8 割強が常時接続の回線を利用していないことが顕著に表れた。また、回線種別との質問間クロス集計では、専用線とインターネット VPN で約 50%が常時接続となっていることが分かった。

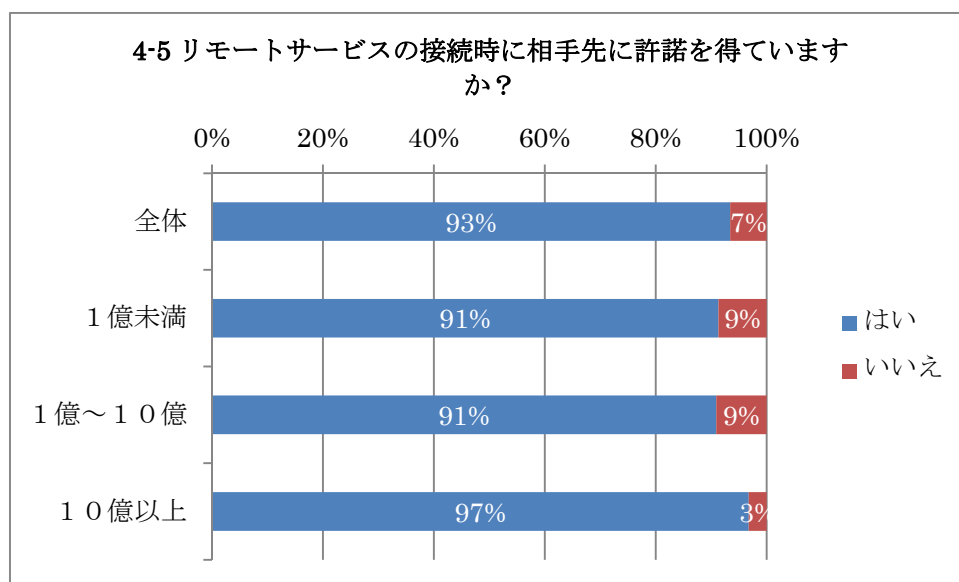


＜対象システム集計＞

（設問 4-5）リモートサービスの接続時に相手先に承諾を得ていますか？

＜質問間クロス集計結果＞

リモートサービスの接続時に医療機関に承諾を得ることに対し、ベンダの資本金に起因する差はないようである。また、回線種別との質問間クロス集計では、特段大きな差は見えてとれない。

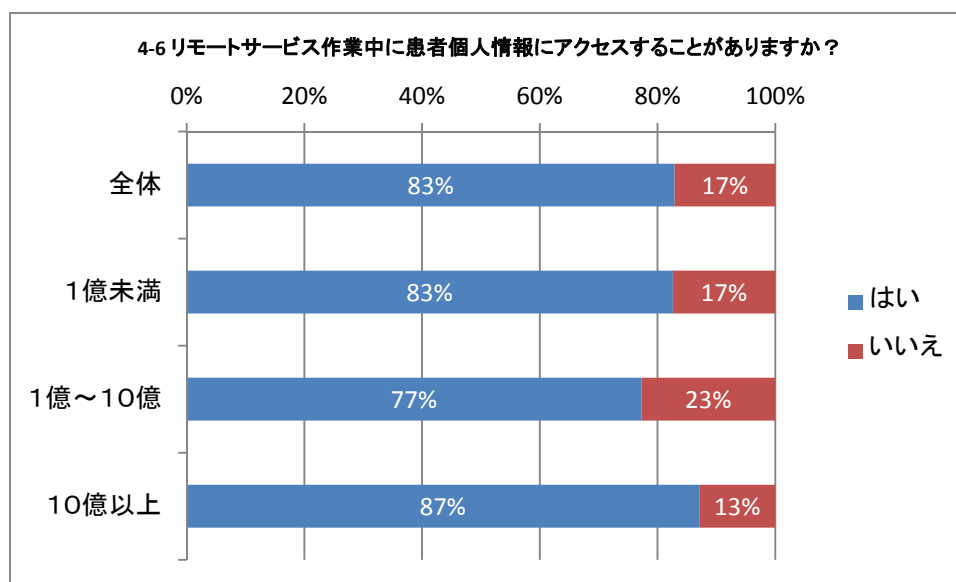


＜対象システム集計＞

(設問 4-6) リモートサービス作業中に患者個人情報にアクセスすることがありますか？

＜質問間クロス集計結果＞

リモートサービス時に患者の個人情報にアクセスすることに対しては、若干ではあるが、資本金 1 億～10 億のベンダで全体に対して小さな値となった。

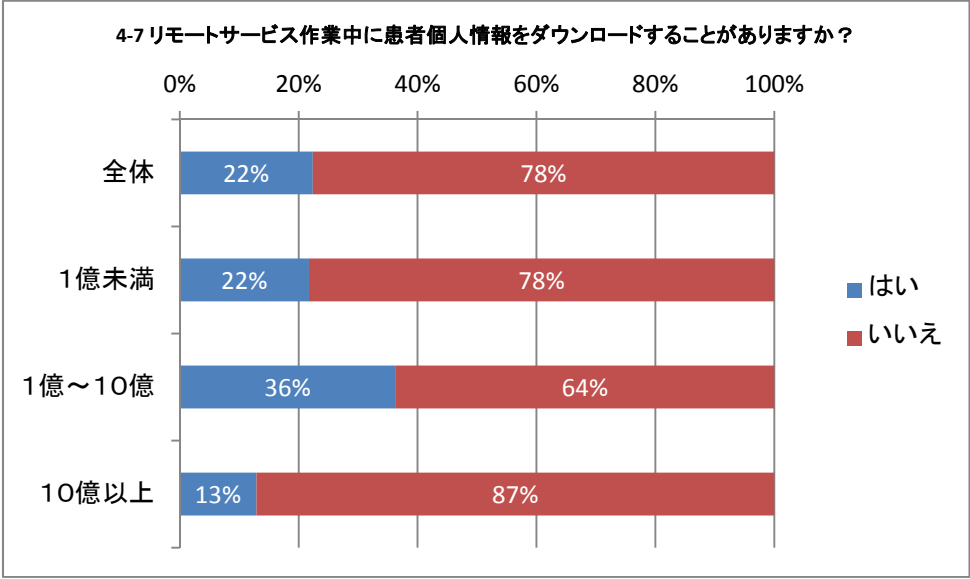


＜対象システム集計＞

(設問 4-7) リモートサービス作業中に患者個人情報をダウンロードすることがありますか？

＜質問間クロス集計結果＞

資本金 10 億以上のベンダでは、大半がリモートサービス作業中に患者の個人情報をダウンロードすることなく、資本金 1 億～10 億のベンダでは 3 割強がダウンロードを含む作業を行っていることが分かった。

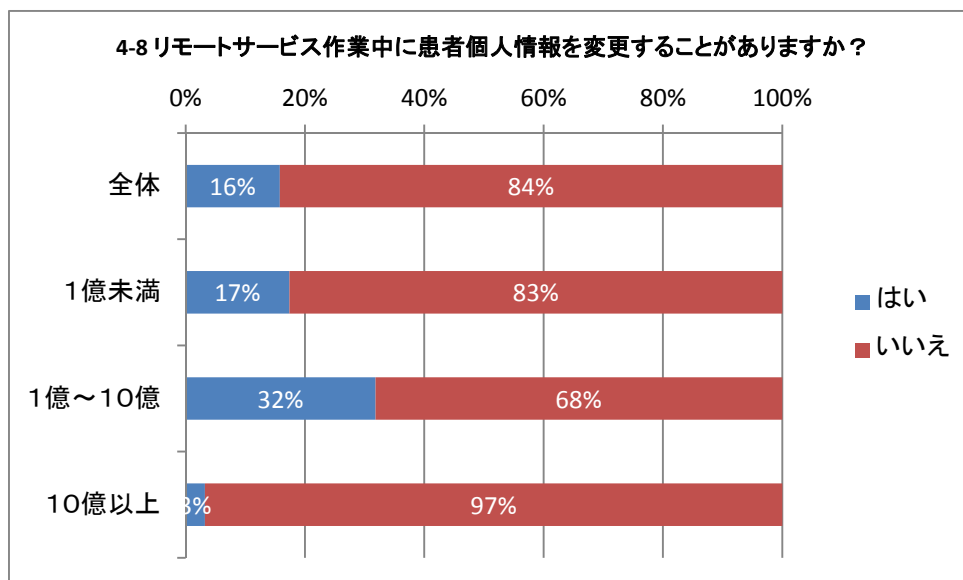


＜対象システム集計＞

（設問 4-8）リモートサービス作業中に患者個人情報を変更することがありますか？

＜質問間クロス集計結果＞

ほとんどの資本金 10 億以上のベンダでは、ガリモートサービス作業中に患者の個人情報を変更することなく、資本金 1 億～10 億のベンダでは 3 割強が患者の個人情報の変更を含む作業を行っていることが顕著に表れている。

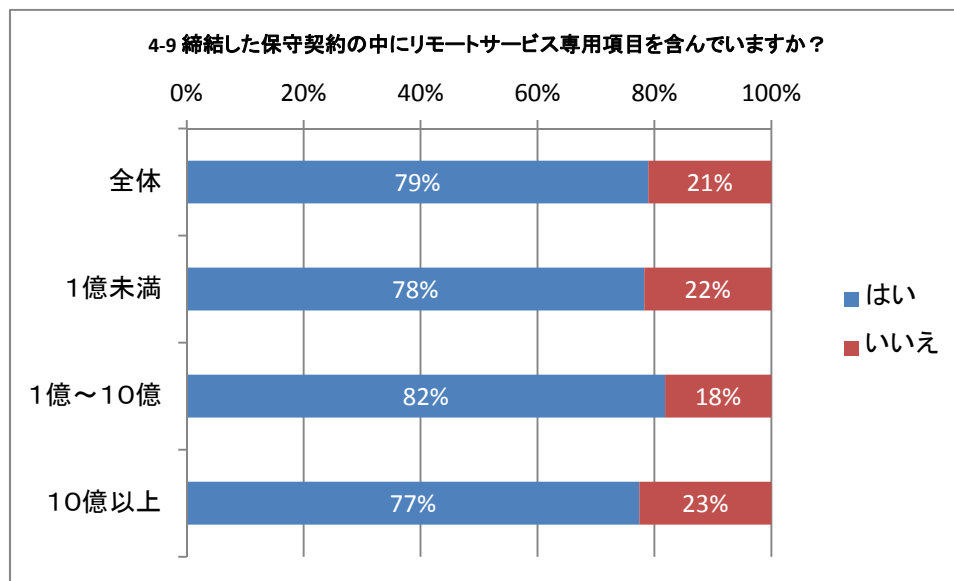


＜対象システム集計＞

（設問 4-9）締結した保守契約の中にリモートサービス専用項目を含んでいますか？

<質問間クロス集計結果>

保守契約の中にリモートサービス専用項目を含んでいることに対し、ベンダの資本金に起因する差はないようである。

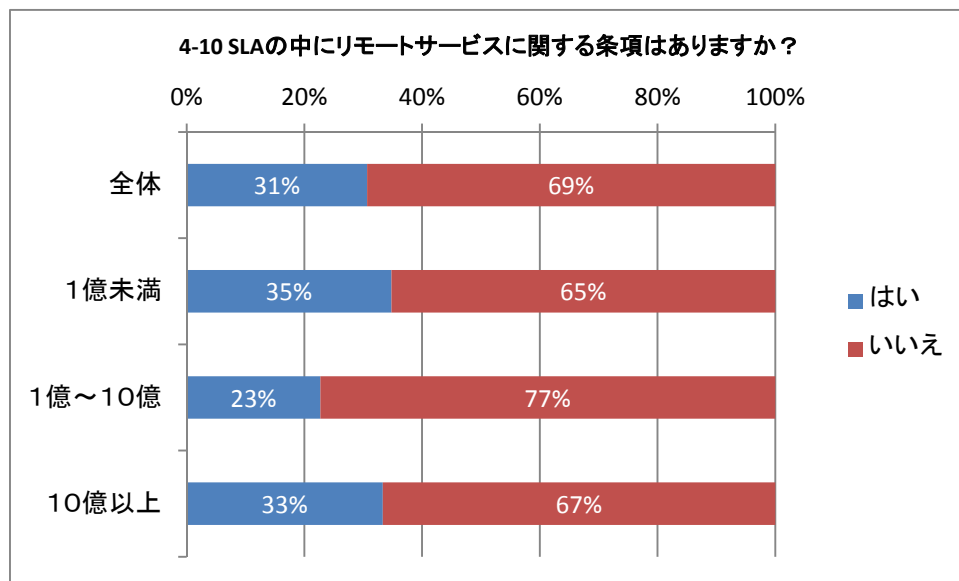


＜対象システム集計＞

（設問 4-10）SLA の中にリモートサービスに関する条項はありますか？

＜質問間クロス集計結果＞

資本金 1 億～10 億のベンダでは、8 割弱が SLA の中にリモートサービスに関する条件を含んでいないことが分かったが、全体として大きな差はないようである。

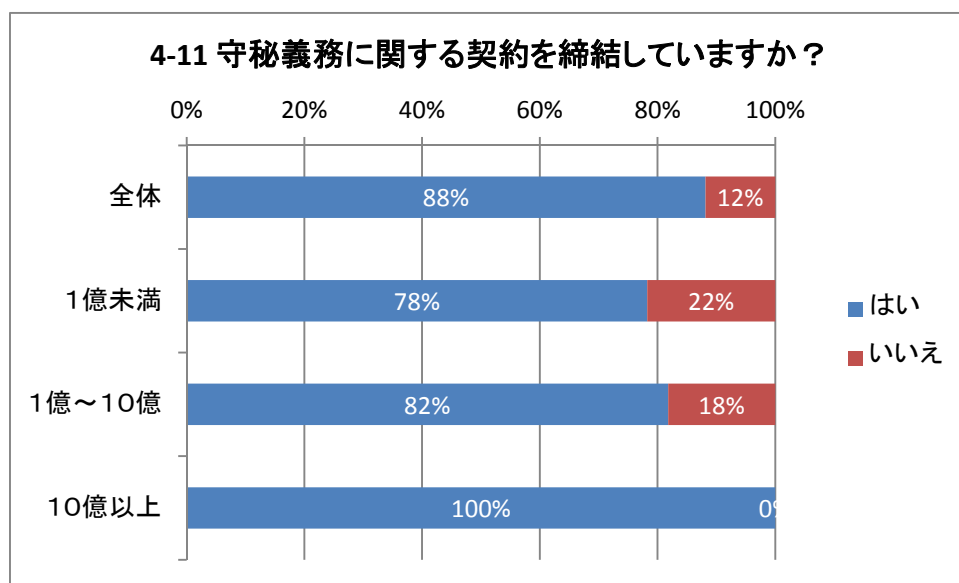


＜対象システム集計＞

（設問 4-11）守秘義務に関する契約をしていますか？

＜質問間クロス集計結果＞

ご回答いただいた資本金 10 億以上の全てのベンダでは、医療機関に対して守秘義務を締結していることが分かった。資本金 1 億未満のベンダへの啓発の必要性が見てとれる。

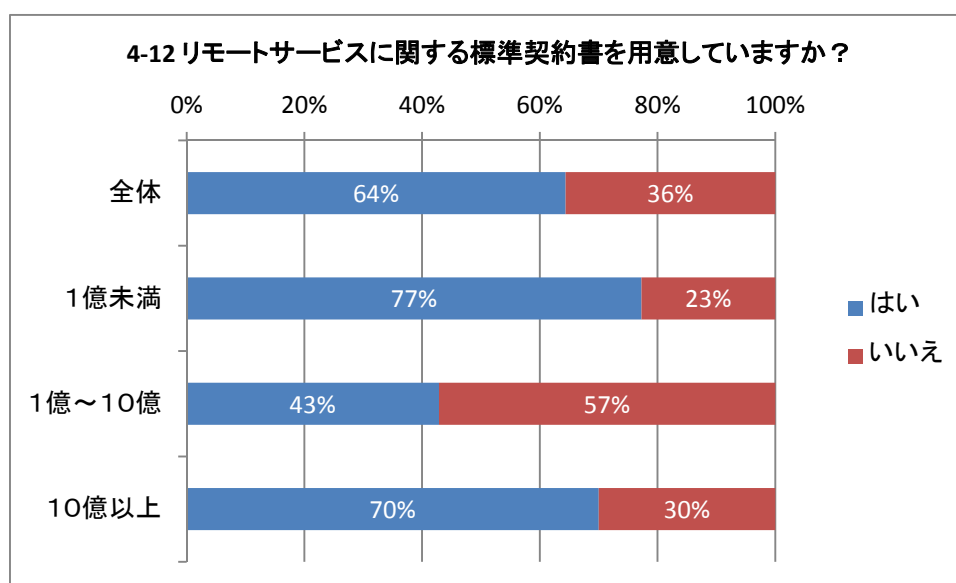


＜対象システム集計＞

（設問 4-12）リモートサービスに関する標準契約書を用意していますか？

＜質問間クロス集計結果＞

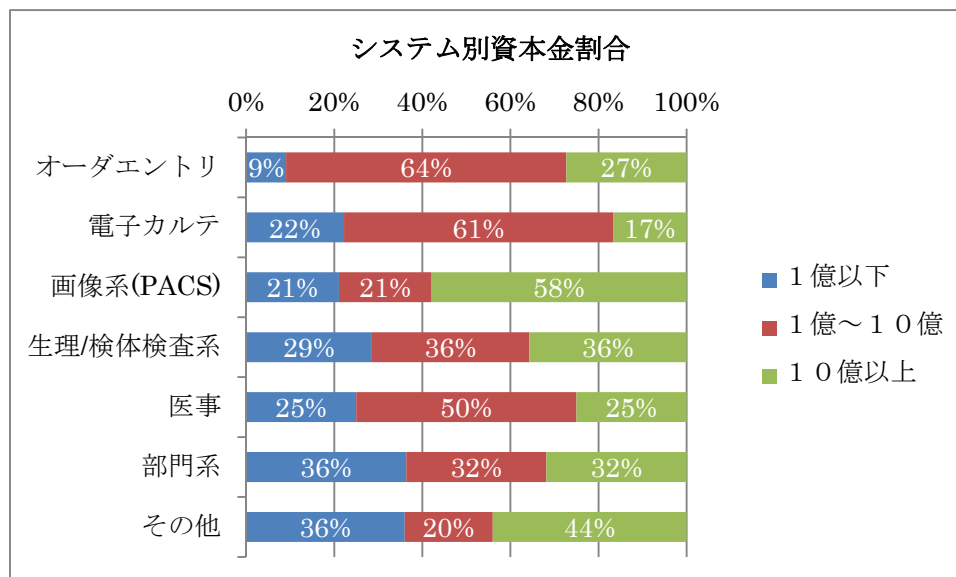
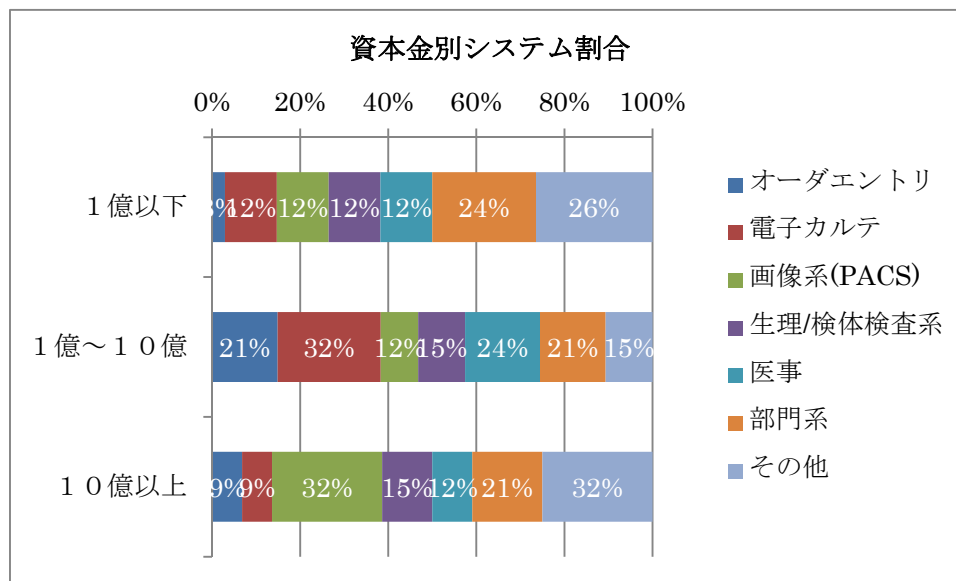
リモートサービスに関する標準契約書の有無に関して、資本金 1 億～10 億のベンダでは半数以下となった。逆に資本金 1 億未満のベンダと、資本金 10 億以上のベンダは 7 割以上が標準契約書を用意しており、顕著である。



7 質問間クロス集計結果③：資本金と対象システム間集計

< 質問間クロス集計結果 >

資本金と対象システムの関係について、質問間クロス集計を以下に示す。



8 総括

今回、JIRA/JAHIS 合同リモートサービスセキュリティ WG では、医療機関向けのリモートサービスの実施状況を把握するとともに、リモートサービスセキュリティガイドラインの普及推進を目的として、JIRA および JAHIS の会員様を対象にアンケートを行った。

回答をいただいた結果からは、「障害対応」「予防保守」「ソフトウェア改訂」の目的でリモートサービスを利用するケースは非常に高いことが分かった。リモートサービスを実施するための基本的なセキュリティ要件は、厚生労働省の安全管理ガイドラインが示している。今回のアンケート調査では、この安全管理ガイドラインの認知度が 90%近くと高く、かつ、その内 95%の医療ベンダがその要求事項を自社のルールに盛り込んでいるか盛り込むことを検討中であることが分かった。リモートサービスを行う際のルール作りは、かなりのところまで整備されてきていると思われる。しかしながら、両工業会制定のリモートサービスガイドラインの認知度は 61%、内容については 51%の認知度に留まっている。これについても自社のルールに盛り込んでもらえるように今後さらなる啓発活動が必要である。

また、標準契約や SLA にリモートサービスに関する項目を含んでいるかの設問に対しては、高い数値を得ることができなかった。当 WG では、工業会として、これらの要件を整理し啓発していくことが大切であると認識している。

今回のアンケート調査では、設問によっては調査特有の隔たりが顕著に表れたものもあり、場合によっては追加調査の必要性も検討する余地があると考えられる。当 WG では、引き続き安全で安心できるリモートサービスの実現に向けた啓発活動を行っていく。

2012 年 3 月 JIRA/JAHIS 合同リモートサービスセキュリティ WG