情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

クラウド時代における情報セキュリティ
～アンケート調査結果を踏まえて～

2010年11月17日

林　紘一郎

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

目次

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

1　はじめに

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

クラウドに対する注目は大きいが導入への不安も大きい

順位	キーワード
1	クラウド・コンピューティング
2	プライベート・クラウド
3	国際会計基準（IFRS）
4	見える化
5	SaaS（Software as a Service）
6	Twitter
7	環境経営/グリーン経営
8	PaaS/IaaS （Platform as a Service/Infrastructure as a Service）
9	コスト最適化
10	排出量取引

2010年に注目したい
マネジメント/情報システム分野のITキーワード
出典：ITPro

パブリッククラウドサービスの阻害要因
出典：IDC Japan

セキュリティへの不安の払拭はクラウドでの重要な課題
具体的にどのような課題があるのか？

2 アンケート調査概要

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

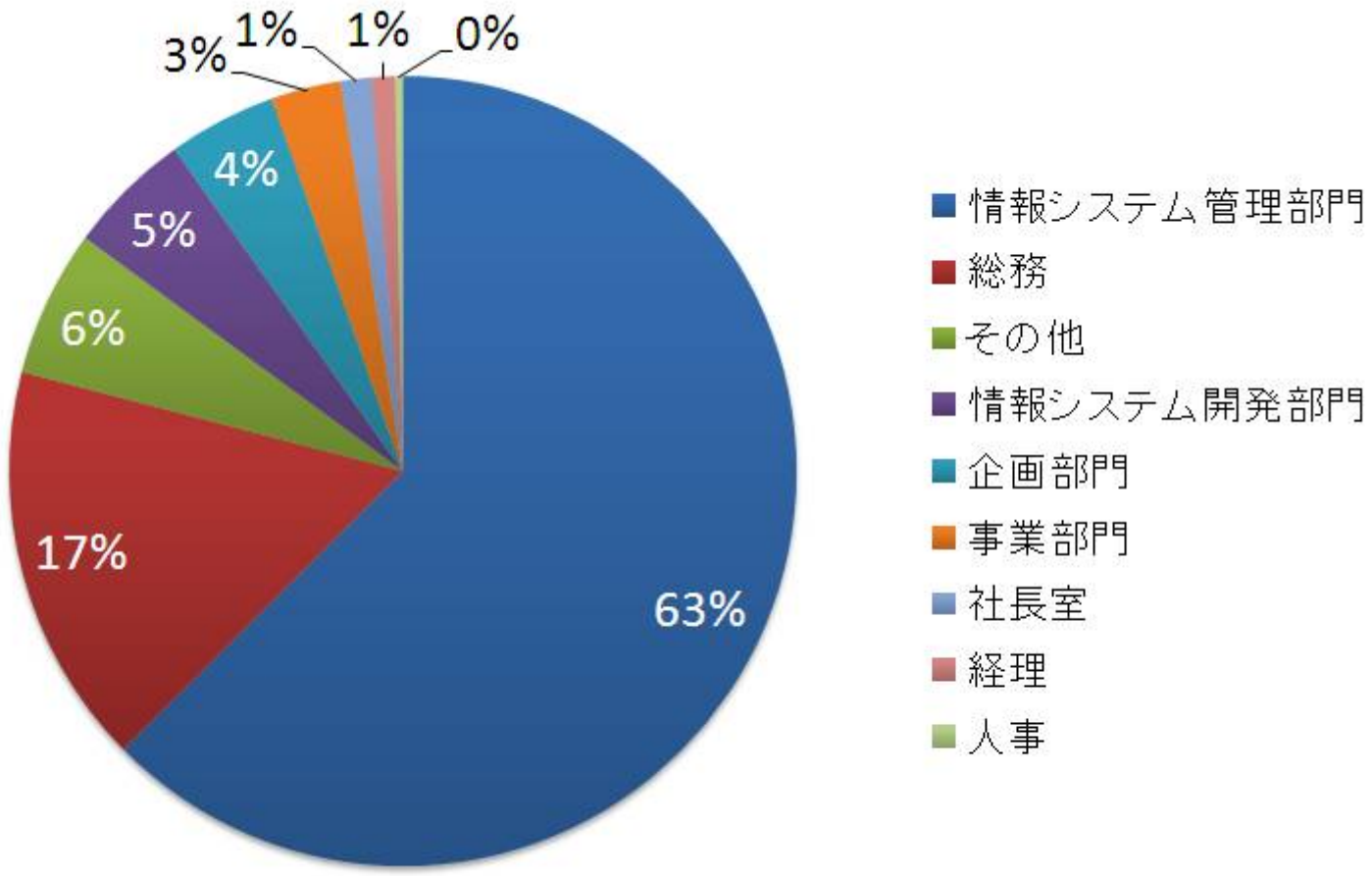
情報セキュリティ大学院大学 原田研究室にてアンケート調査を実施。
クラウドに対する企業の意識動向の実態を明らかにすることを目的。
ENISA「Cloud Computing Risk Assessment」のリスク評価項目、
経済産業省「SaaS向けSLAガイドライン」等を参考に設問を検討。

実施期間： 2010年8月1日～8月31日
実施方法： 郵送
調査対象： 企業・行政機関・大学を中心とする4500組織の
情報セキュリティ担当者
有効回答： 316（7%）
調査項目： 主に以下の通り
① 組織の概要
② クラウドの利用動向
③ クラウドのリスク評価
④ クラウド事業者の選定要因

2.1　回答組織の概要①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

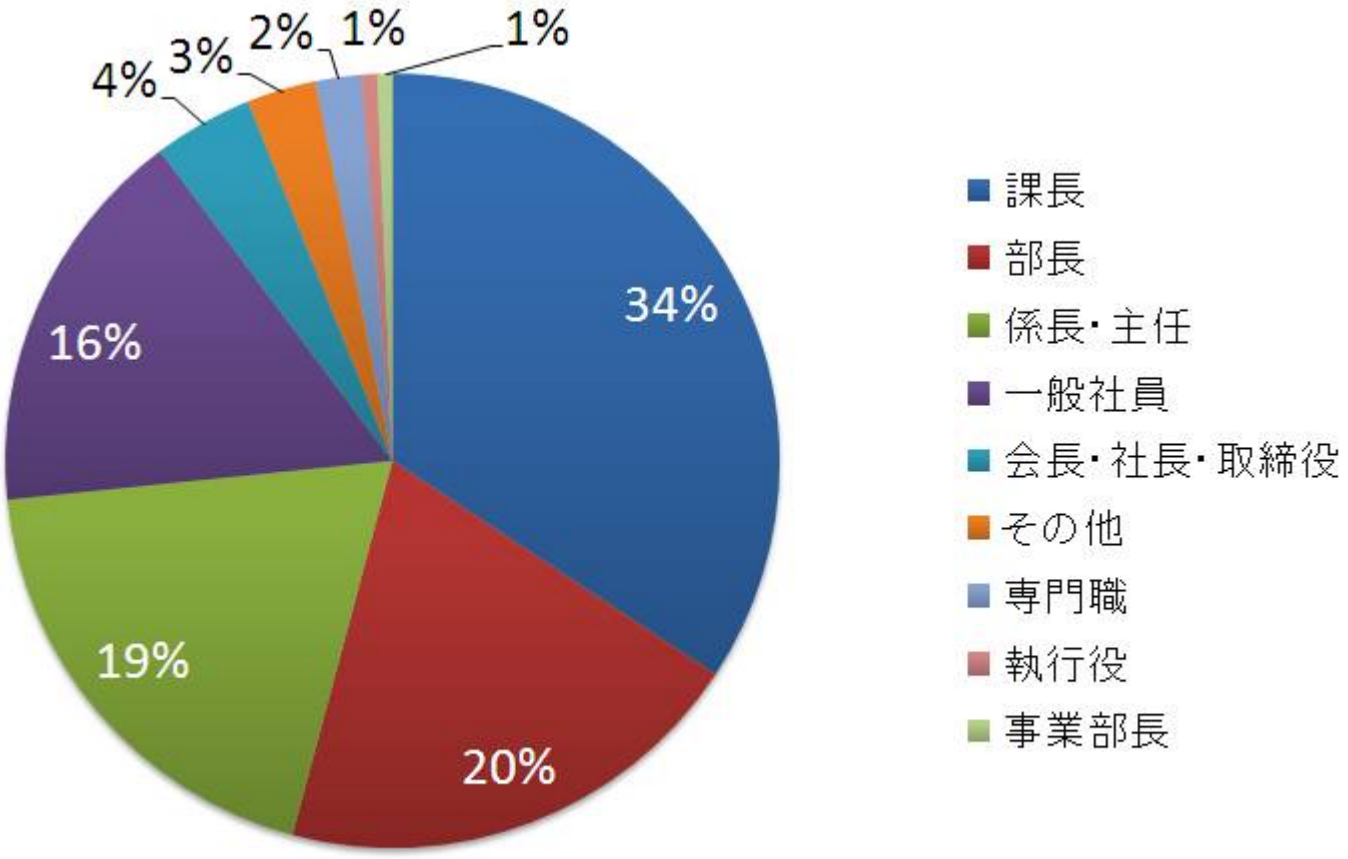
回答者の所属　（N=315）



2.1　回答組織の概要②

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

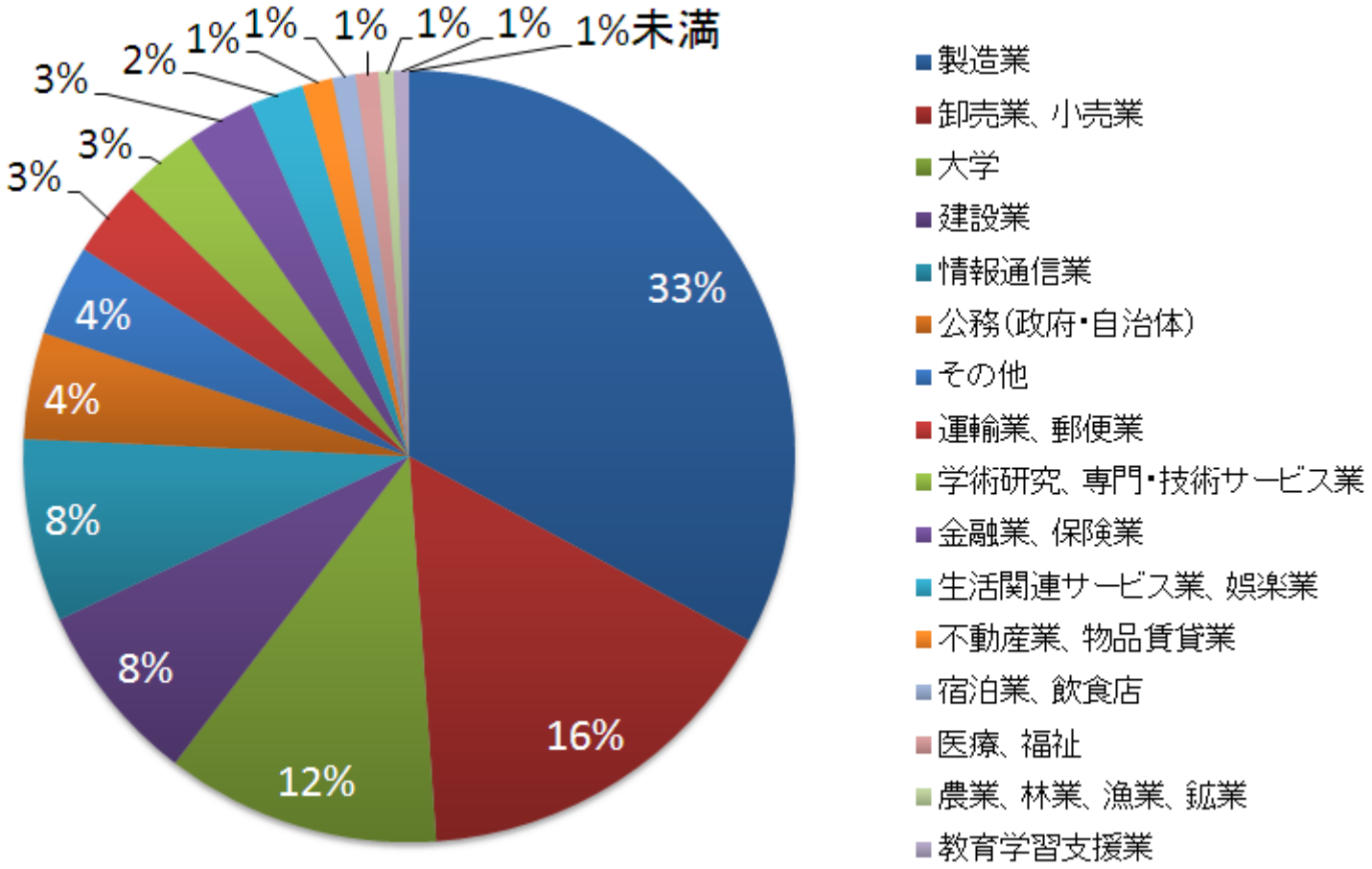
回答者の役職　（N=312）



2.1　回答組織の概要③

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

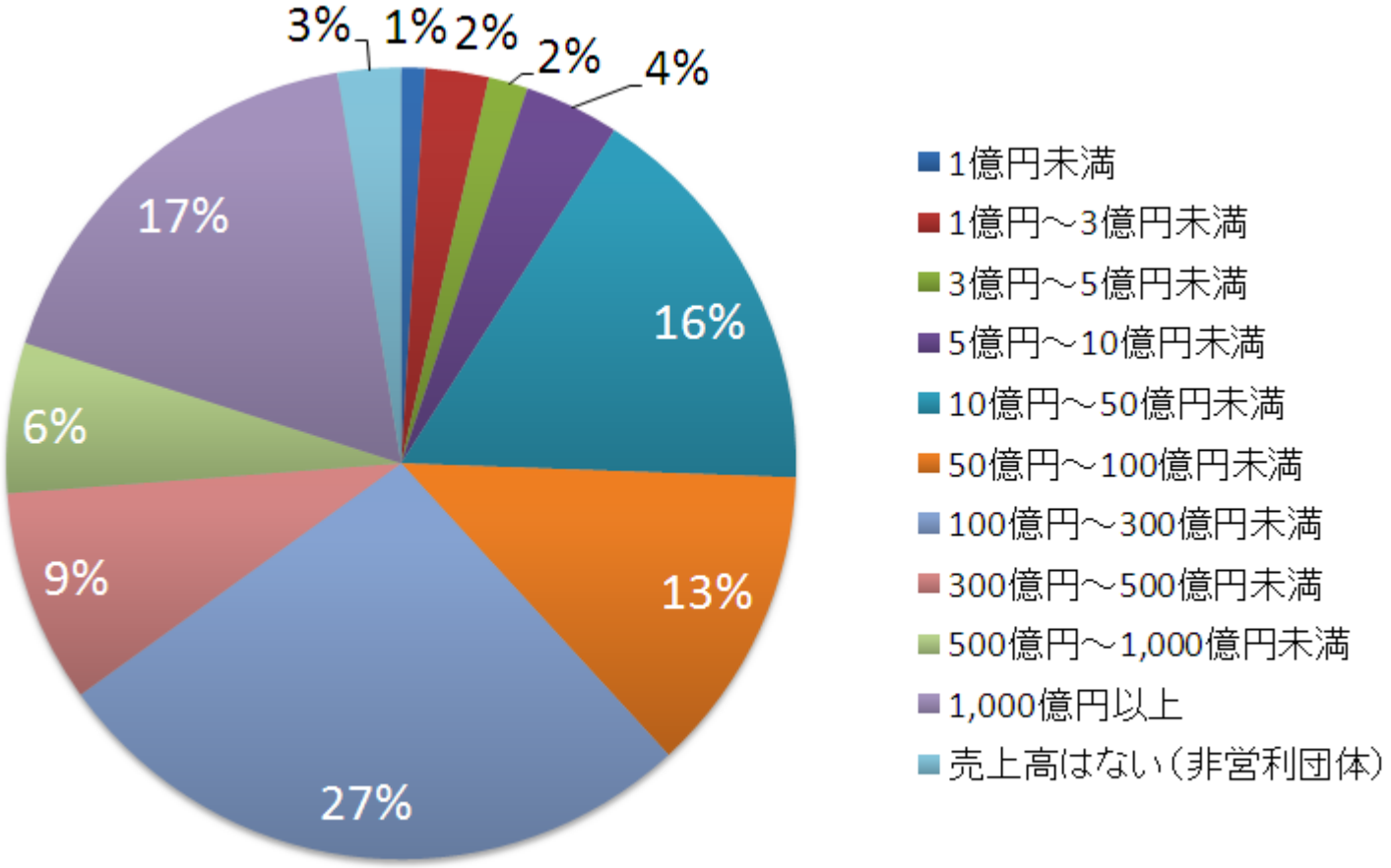
回答組織の業種　（N=313）



2.1　回答組織の概要④

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

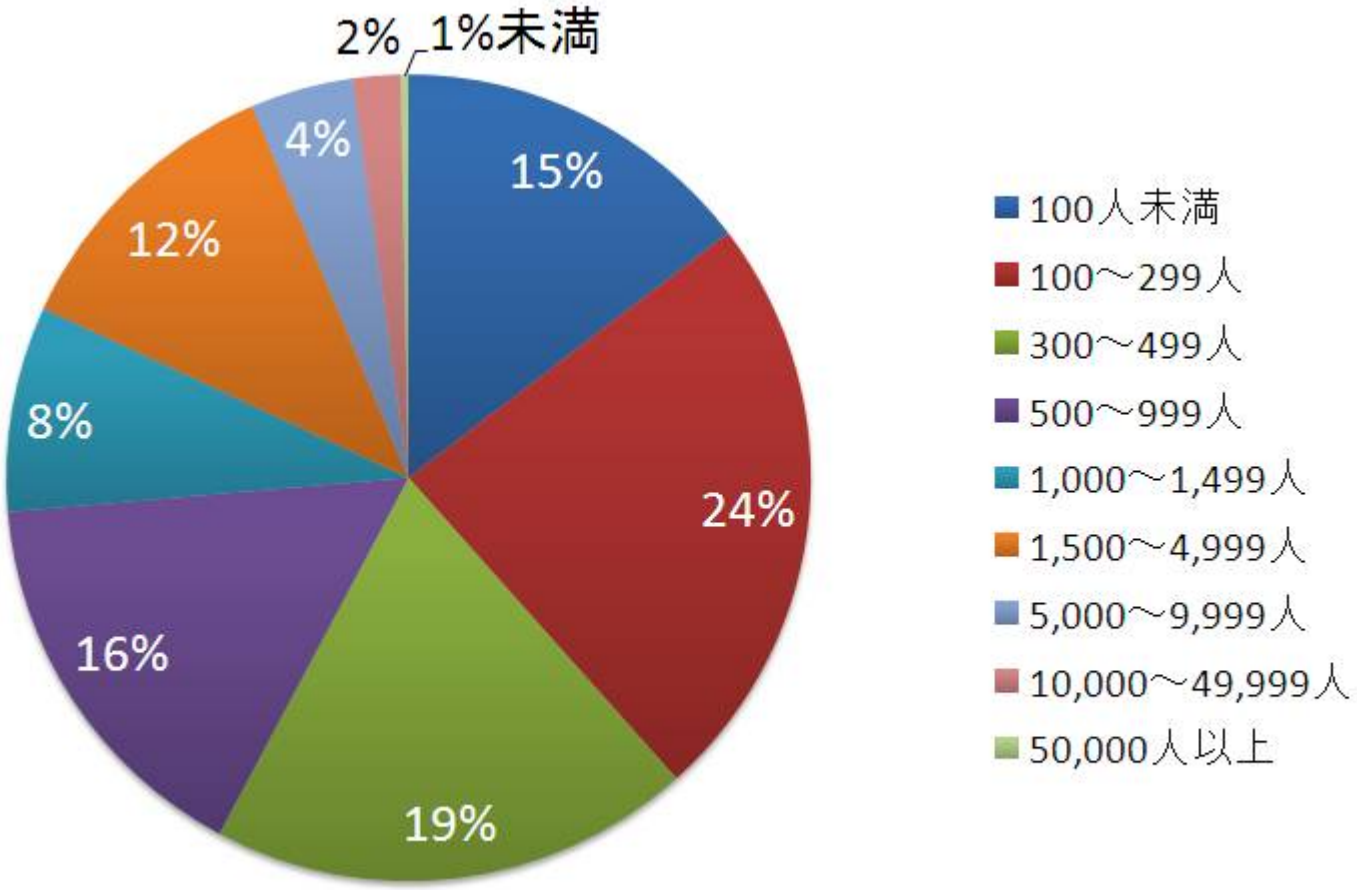
回答組織の年間売上高　（N=309）



2.1　回答組織の概要⑤

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

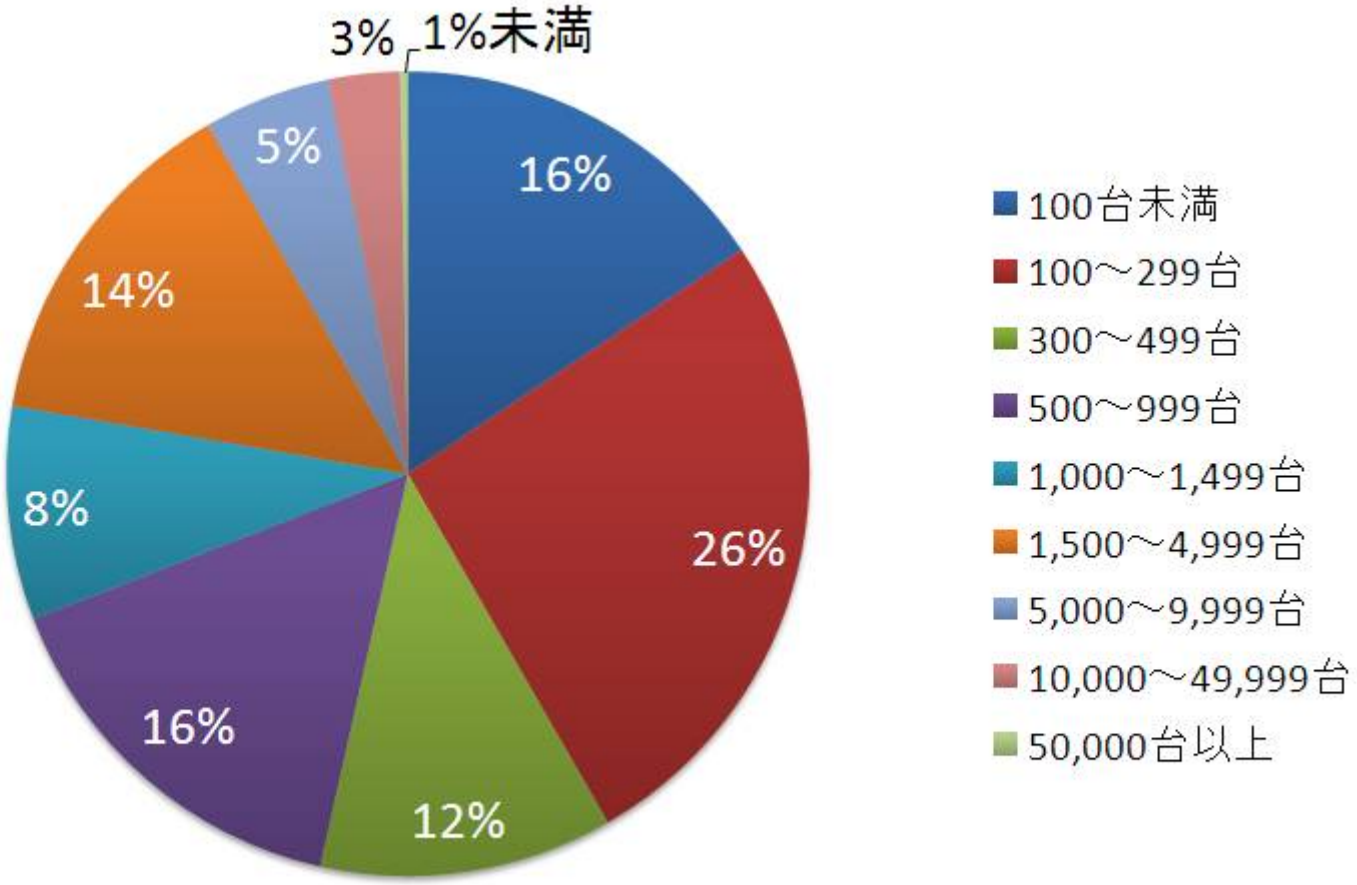
回答組織の全従業員数　（N=315）



2.1　回答組織の概要⑥

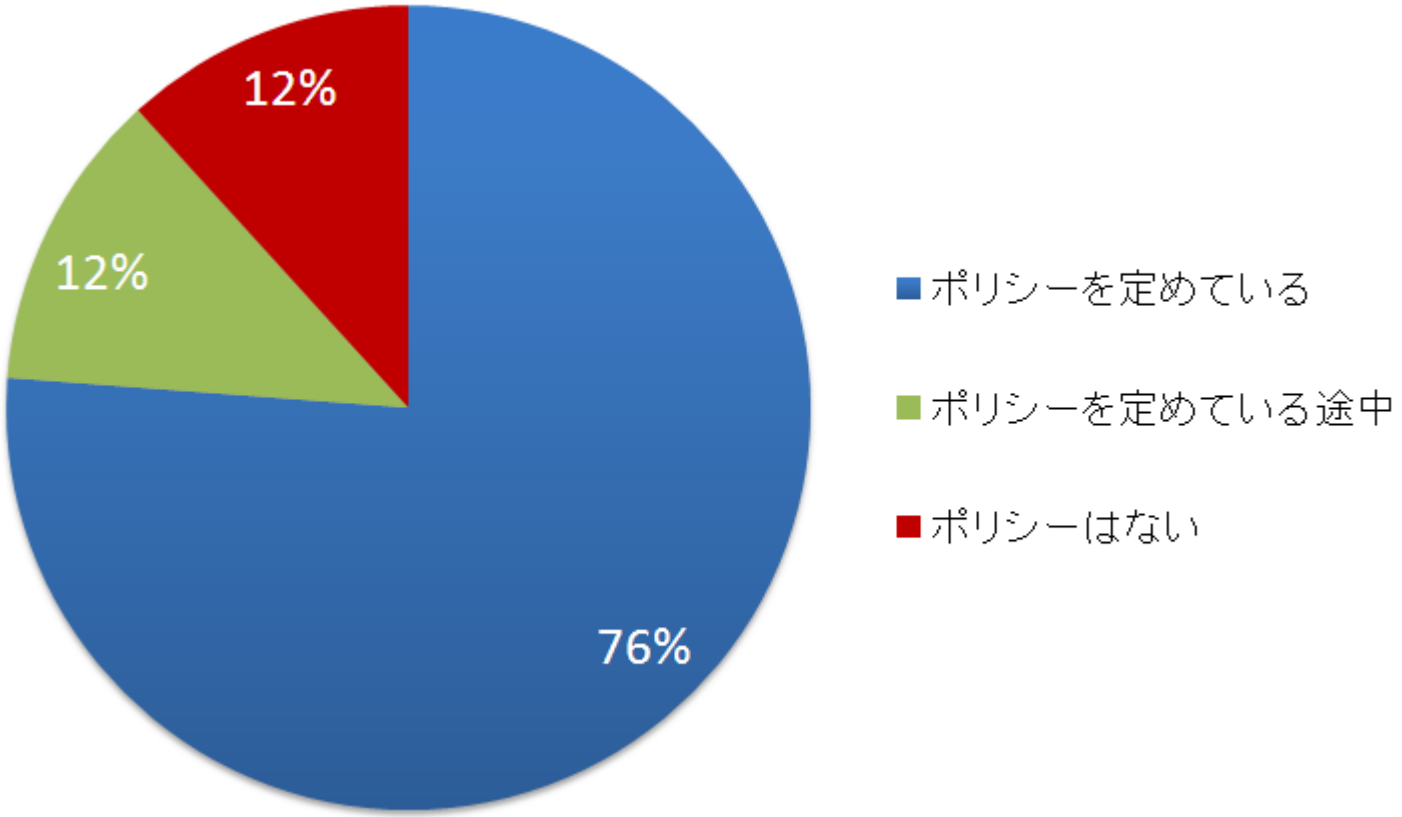
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

回答組織の保有PC台数　（N=314）



2.1　回答組織の概要⑦

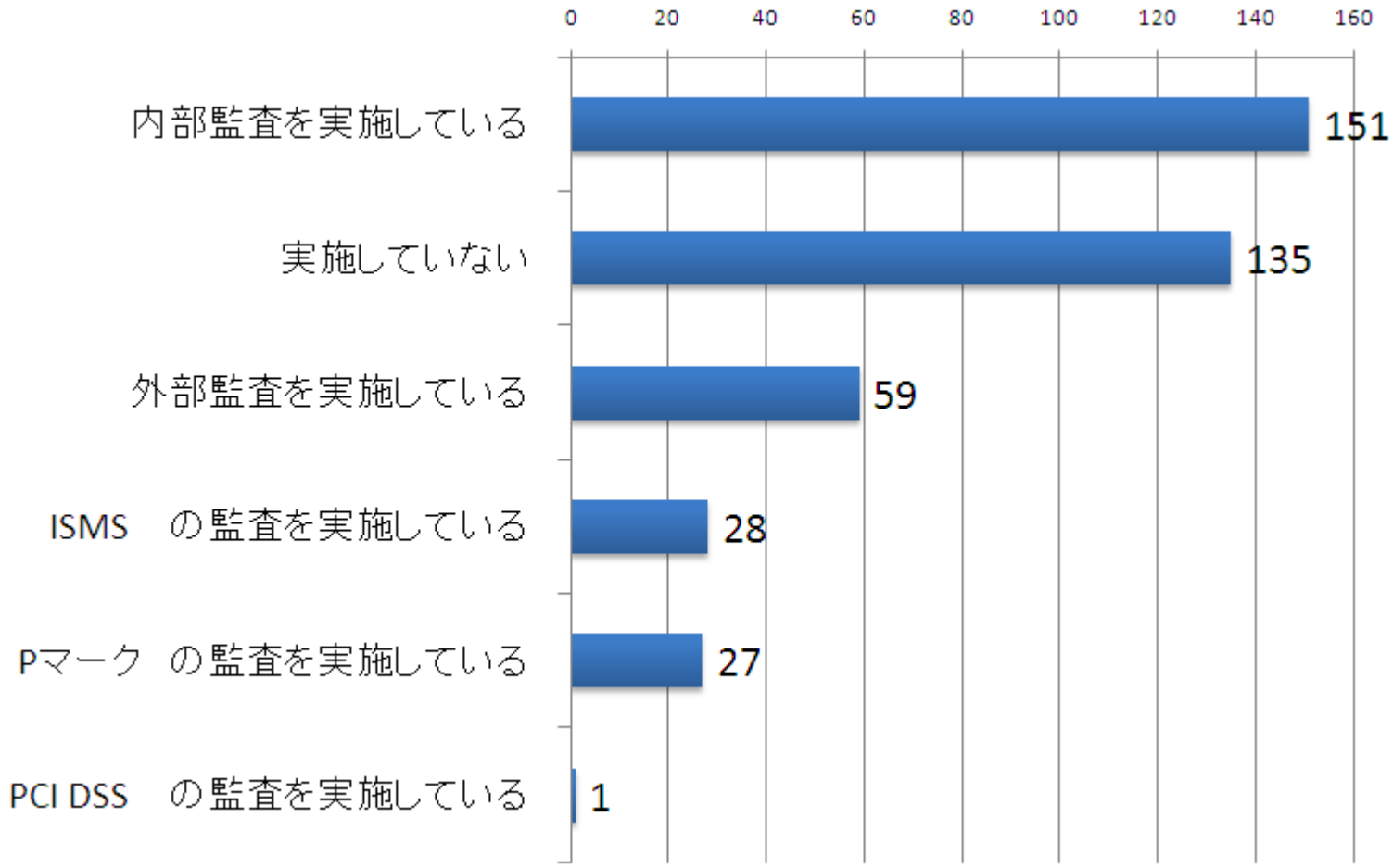
情報セキュリティポリシーの有無　（N=315）



2.1　回答組織の概要⑧

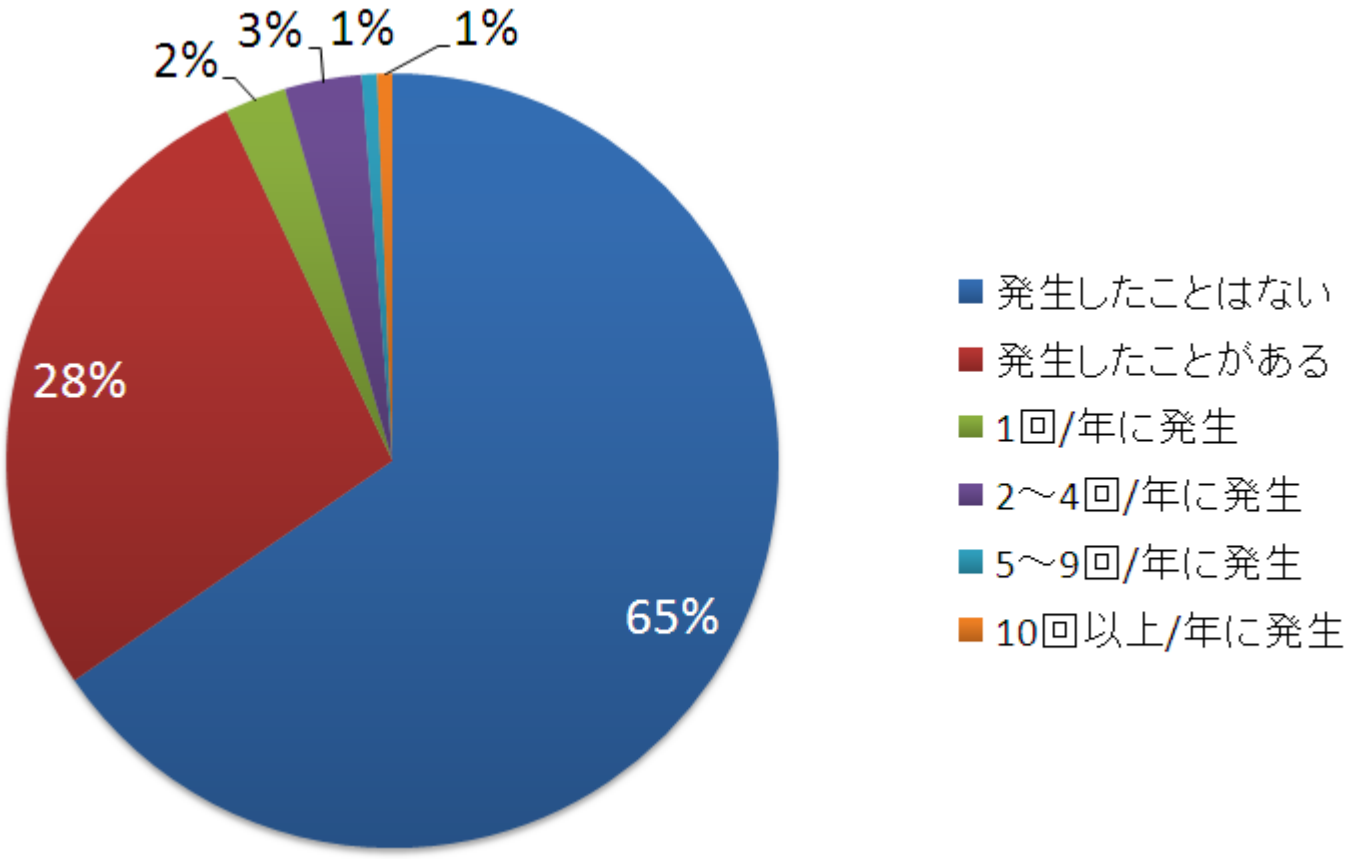
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティ監査の実施状況　（N=316）複数選択



2.1　回答組織の概要⑨

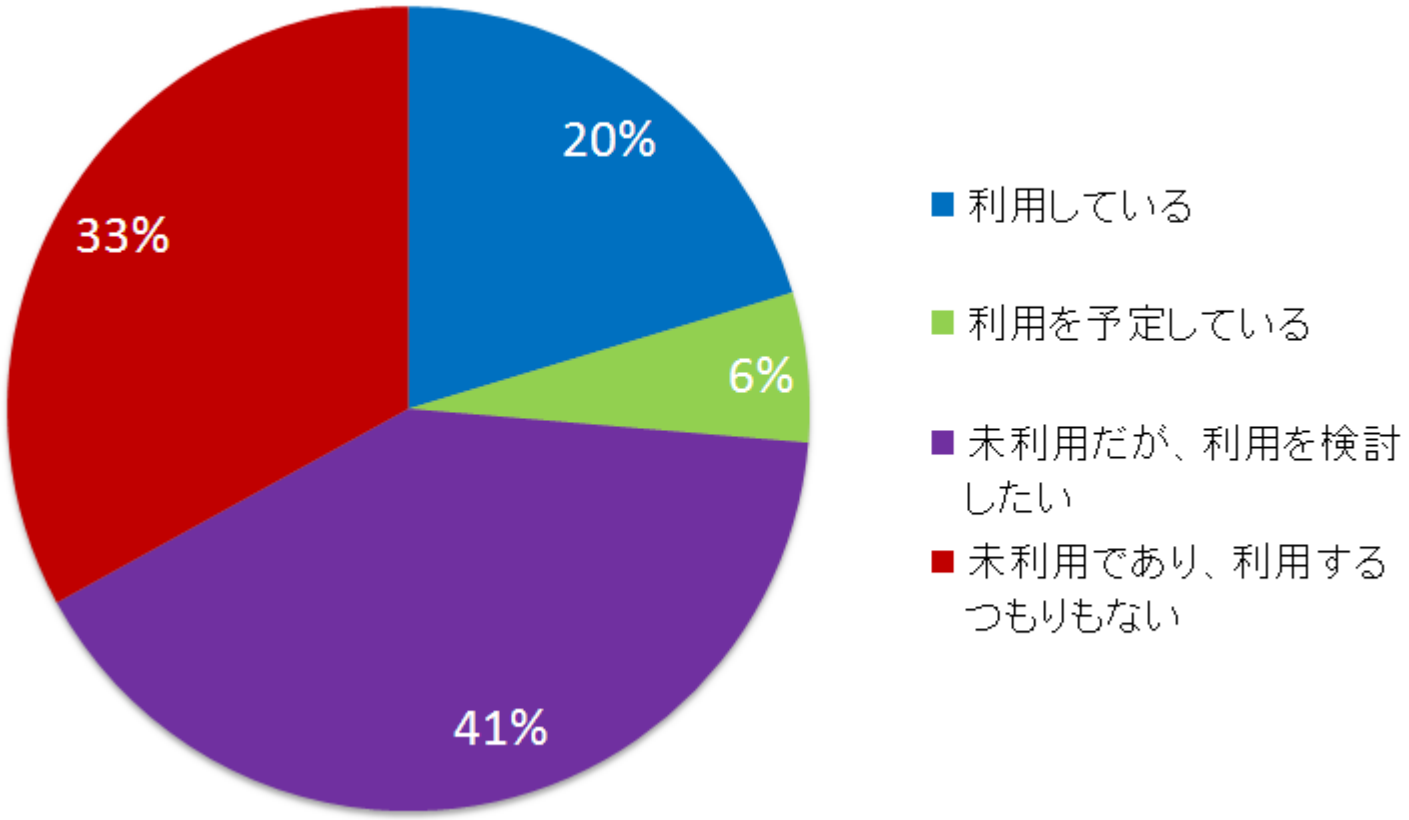
情報セキュリティ事故/事件の発生状況　（N=312）



2.2　クラウドの利用動向①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

クラウドを利用していますか？　（N=315）

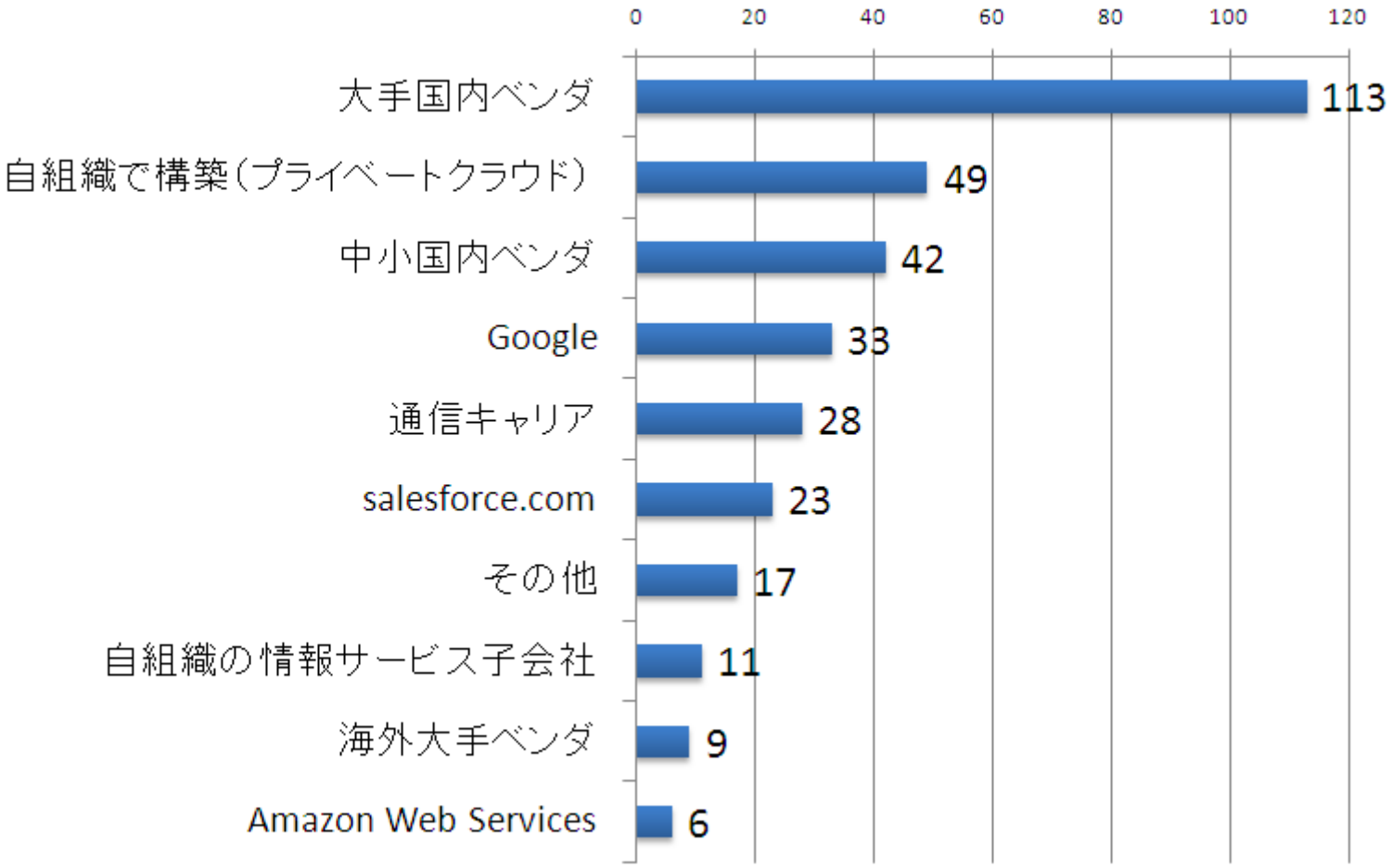


2/3の企業にクラウドの利用意向がある

2.2 クラウドの利用動向②

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

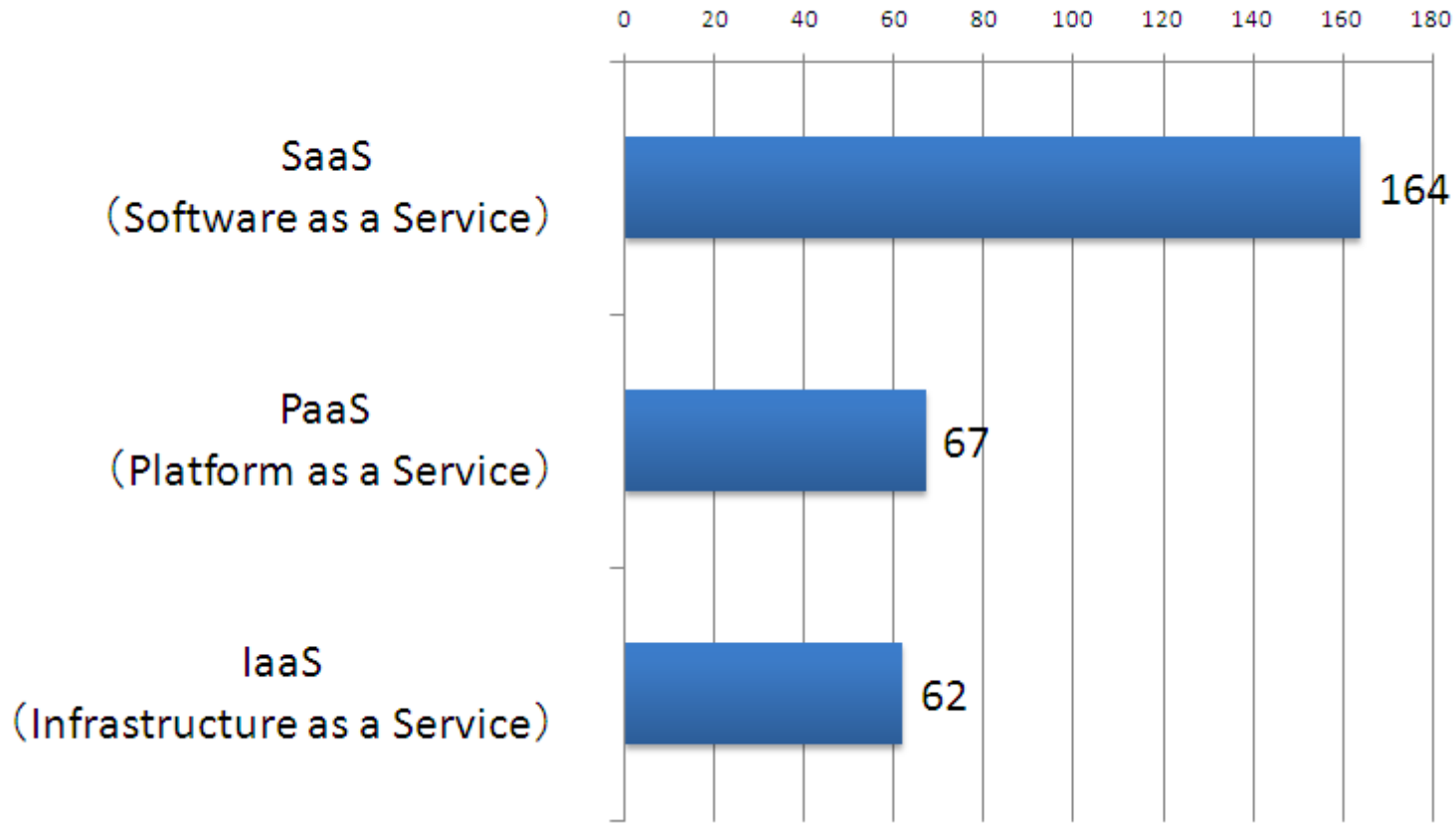
どのような事業者を利用(予定含む)していますか？ (N=316)複数選択



2.2 クラウドの利用動向③

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

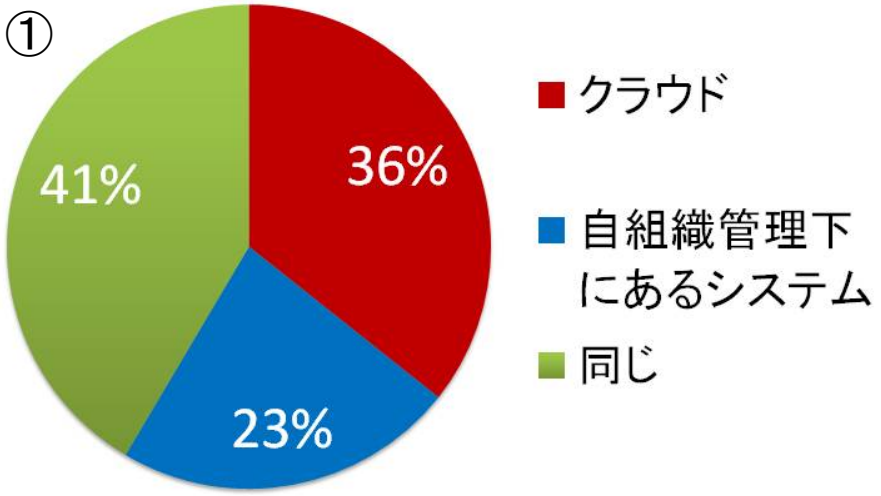
どのようなサービスを利用（予定含む）していますか？ （N=316）複数選択

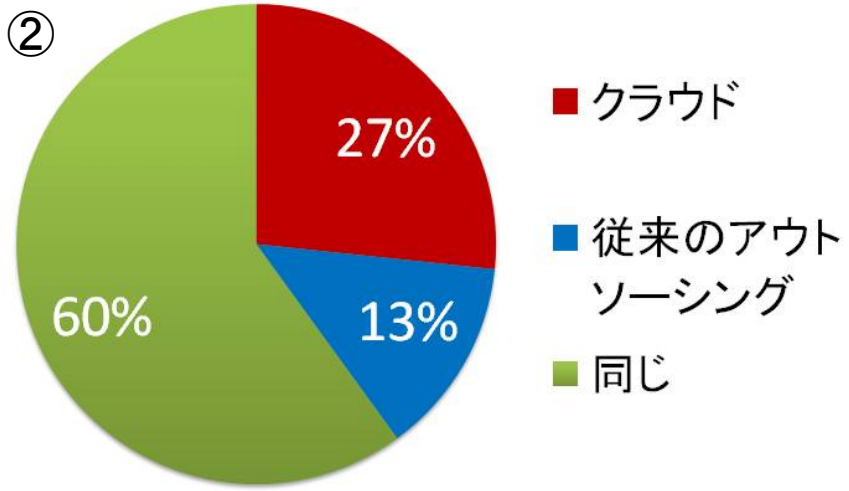


2.2 クラウドの利用動向④

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

①クラウドと自組織管理下にあるシステム
②クラウドと従来のアウトソーシング（ホスティング）
セキュリティ上の脅威は、どちらが大きいと感じますか？ （N=311）





どちらもクラウドの脅威の方が大きい。
一方で、「同じ」と感じる方も多数。特に従来のアウトソーシングとクラウドを比較するとその傾向が強い。

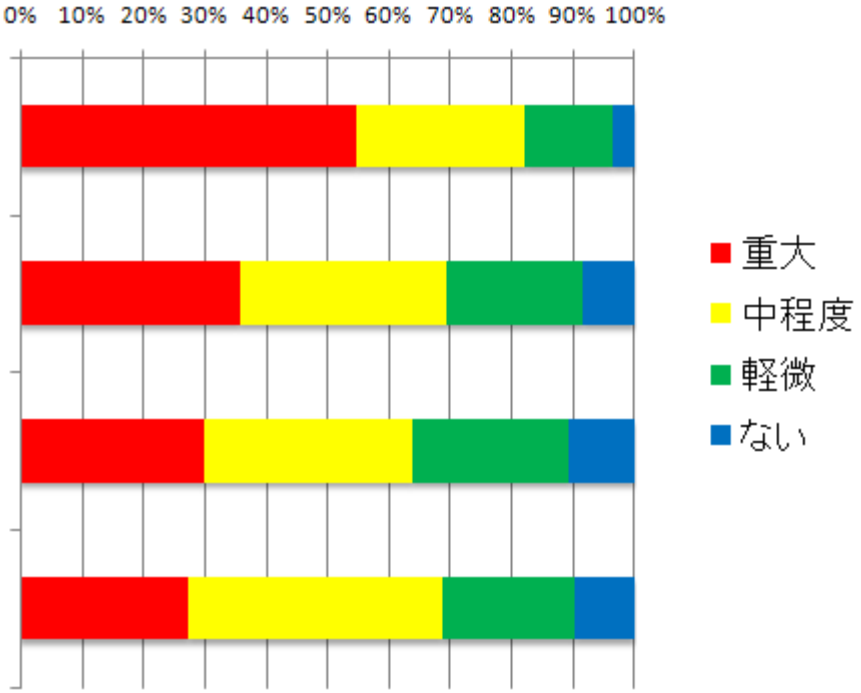
2.3　クラウドのリスク評価①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

組織的リスク

「重大」と回答した件数が多かったリスク　1～4位　（N=316）

1. 事業者がサービスを中断したときに、自組織のビジネスへのリスク
2. 事業者の一方的な都合で、サービス内容が変更されるリスク
3. 事業者が利用している他のクラウド事業者のトラブルの影響を受けて、サービス提供が中断したり、サービス内容が変更されるリスク
4. 事業者にすべてを任せてしまい、自組織で対応できなくなるリスク



2.3　クラウドのリスク評価②

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

組織的リスク

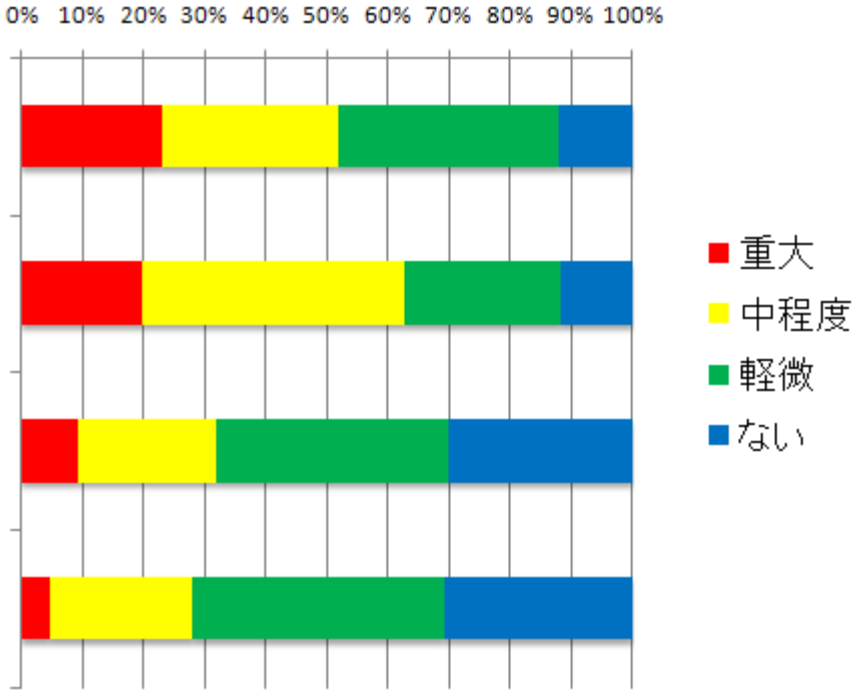
「重大」と回答した件数が多かったリスク　5～8位　（N=316）

5. 事業者のコンプライアンス違反で、自組織も違反になってしまうリスク

6. 事業者に囲い込まれて、後日、事業者を変更できなくなってしまうリスク

7. 事業者が買収されて、競合相手の傘下に入ってしまうリスク

8. 同じ事業者を利用する競争相手との差別化ができなくなるリスク



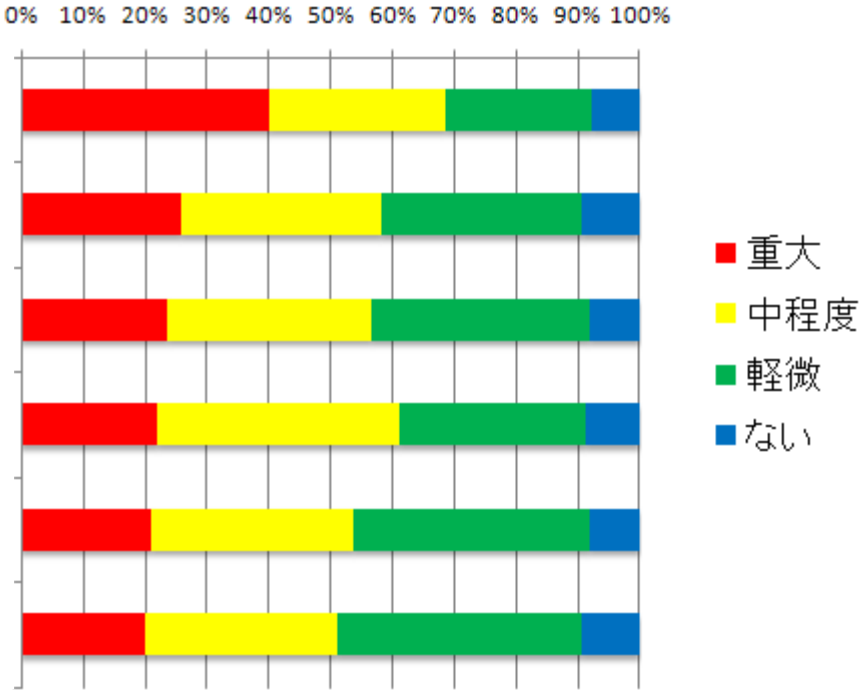
2.3　クラウドのリスク評価③

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

技術的リスク

「重大」と回答した件数が多かったリスク　1～6位　（N=316）

1. 事業者の内部者によるセキュリティ違反（不正アクセスなど）で自組織の機密情報が見られ、その事実が分からないリスク
2. 事業者が意図的に自組織の機密情報を盗み見するリスク
3. 事業者へのDDoS攻撃でサービスが中断したり品質低下するリスク
4. 事業者のリソース（サーバのCPU能力やストレージの容量）が不足して、その影響を受ける（処理速度が遅い、ファイルが保存できないなど）リスク
5. 事業者へのデータ転送の際に機密情報が漏えいするリスク
6. 事業者の提供するサービスに欠陥や問題があるリスク



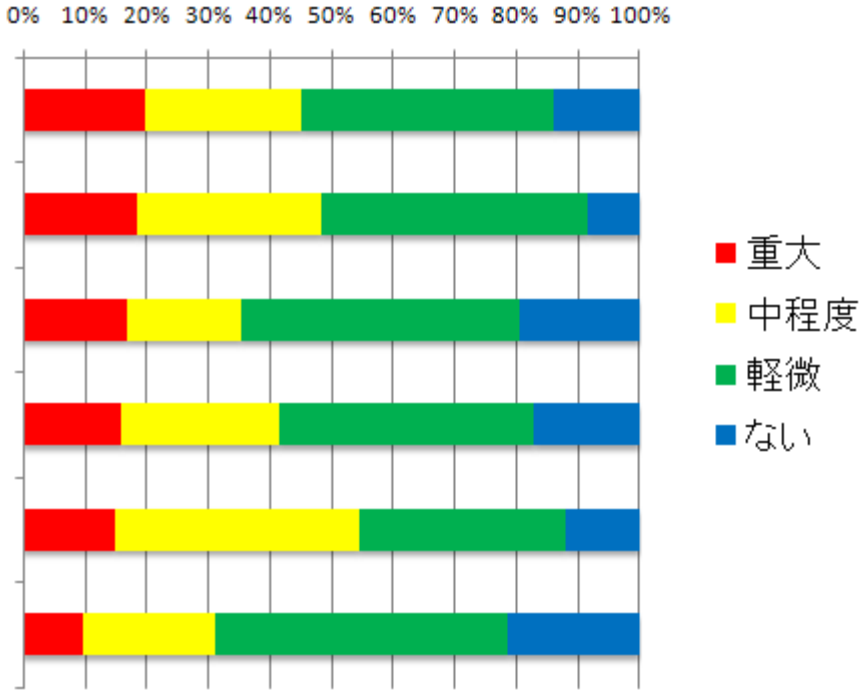
2.3　クラウドのリスク評価④

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

技術的リスク

「重大」と回答した件数が多かったリスク　7～12位　（N=316）

7. 事業者の提供するセキュリティ水準が低いため、結果として自組織のセキュリティが低くなるリスク
8. 事業者が不要になったデータを消去しないリスク
9. 事業者が暗号かぎを紛失して復号できなくなるリスク
10. 事業者を利用して提供している自組織のWebサービスなどへのDDoS攻撃を受けて、増えたアクセスに対する使用料を事業者に請求されるリスク
11. リソースを共用する他の利用者の影響で自組織のサービス品質が低下するリスク
12. 事業者が、自組織にスキャン（空いているポートを探すなど）をかけるリスク



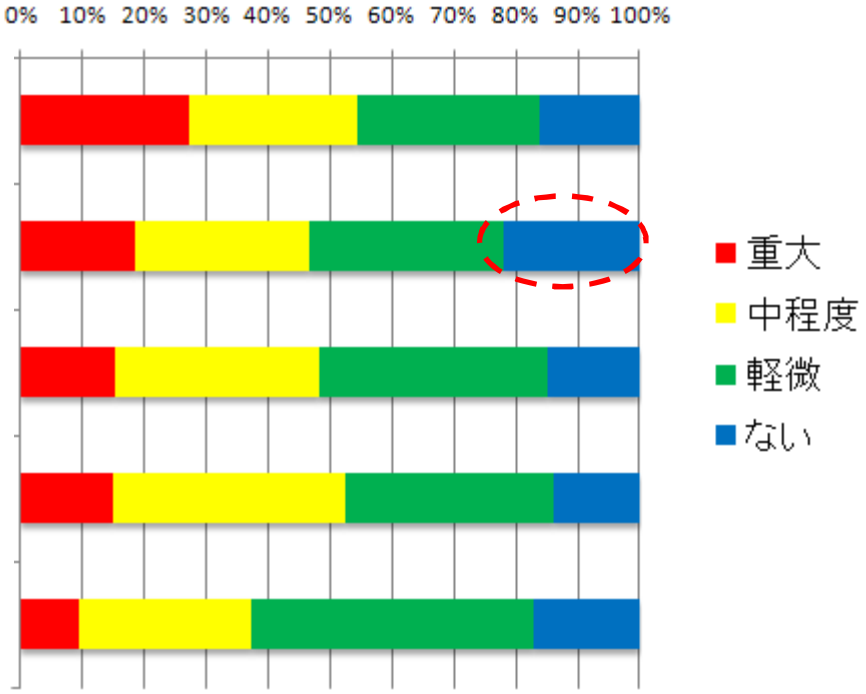
2.3　クラウドのリスク評価⑤

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

法的リスク

「重大」と回答した件数が多かったリスク　1～5位　（N=316）

1. 事業者の違反や倒産などで、自組織のデータが差し押さえられるリスク
2. 事業者と自組織の所在地（国）が異なり、裁判の管轄や適用される法令（例えば個人情報保護法など）が異なるリスク
3. 事業者への法的な命令で証拠保全が必要となる（例えば法的機関へ自組織の情報が提出される）リスク
4. 自組織への法的な命令で証拠保全が必要となる場合、事業者側で証拠保全ができないリスク
5. 事業者が受けているソフトウェアのライセンス条件と自組織に必要となる条件が異なるリスク



裁判の管轄・適用法令が異なるリスク・・・「ない」が多い
国内クラウド事業者の利用（予定）が多数のためか

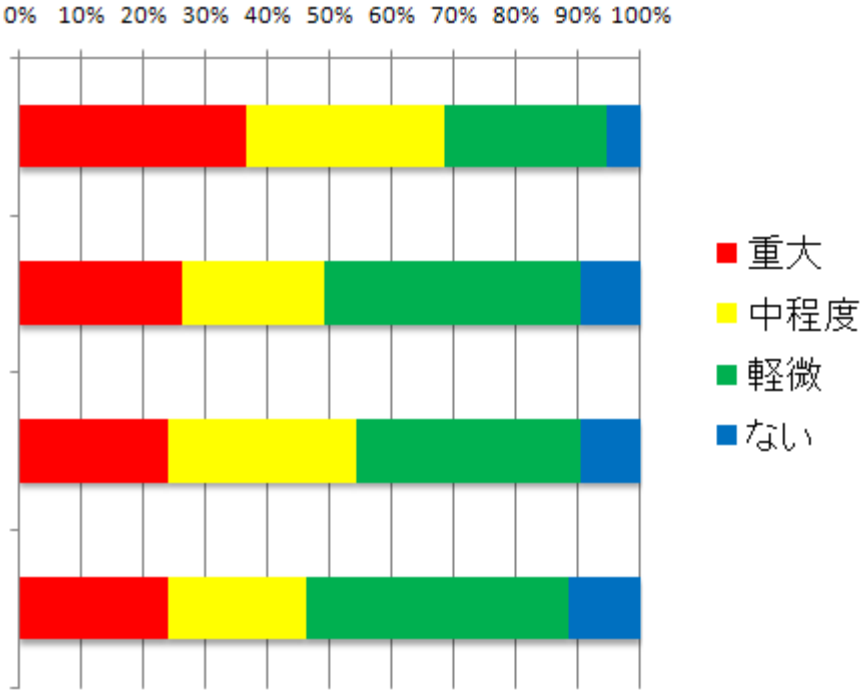
2.3　クラウドのリスク評価⑥

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

共通事項

「重大」と回答した件数が多かったリスク　1～4位　（N=316）

1. 事業者と自組織を結ぶネットワークがダウンするリスク
2. 事業者のルート権限を奪取されて、自組織情報が盗まれたり、改ざんされるリスク
3. 事業者の運用管理体制が悪く、容量不足や、接続ミスなどが起きるリスク
4. 事業者がバックアップファイルを毀損させたり、漏えいさせるリスク



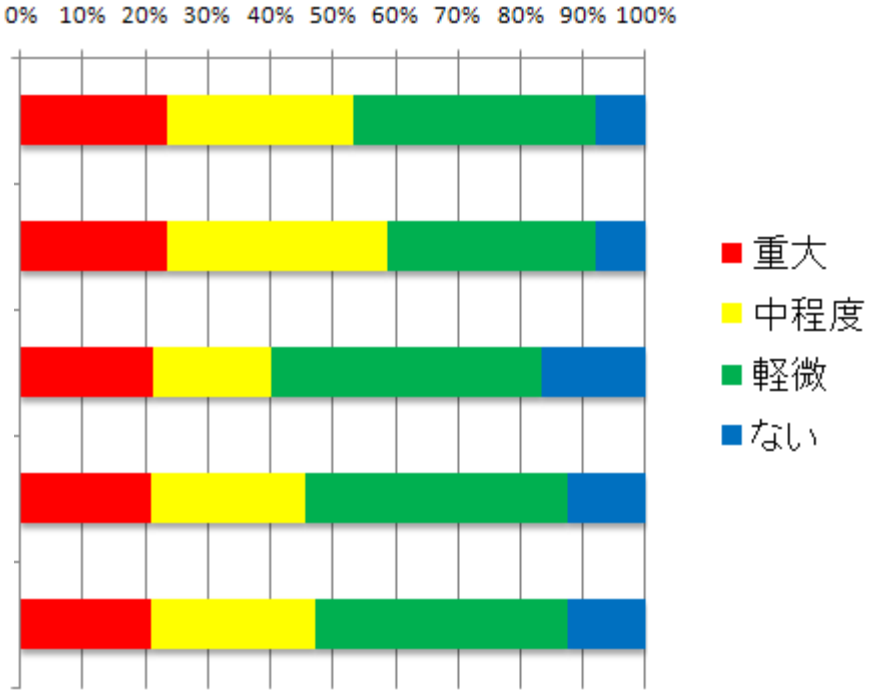
2.3　クラウドのリスク評価⑦

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

共通事項

「重大」と回答した件数が多かったリスク　5～9位　（N=316）

5. 事業者が自然災害を受けてサービスが停止するリスク
6. ネットワーク障害の場合、事業者と自組織間の経路変更できないリスク
7. 事業者の施設に簡単に侵入でき、機器にもアクセスできるリスク
8. 事業者がソーシャルエンジニアリング攻撃を受けて、自組織に関する情報を開示するリスク
9. 事業者が認証などのセキュリティログを紛失したり、漏えいさせるリスク



2.3　クラウドのリスク評価⑧

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

共通事項

「重大」と回答した件数が多かったリスク　10～14位　（N=316）

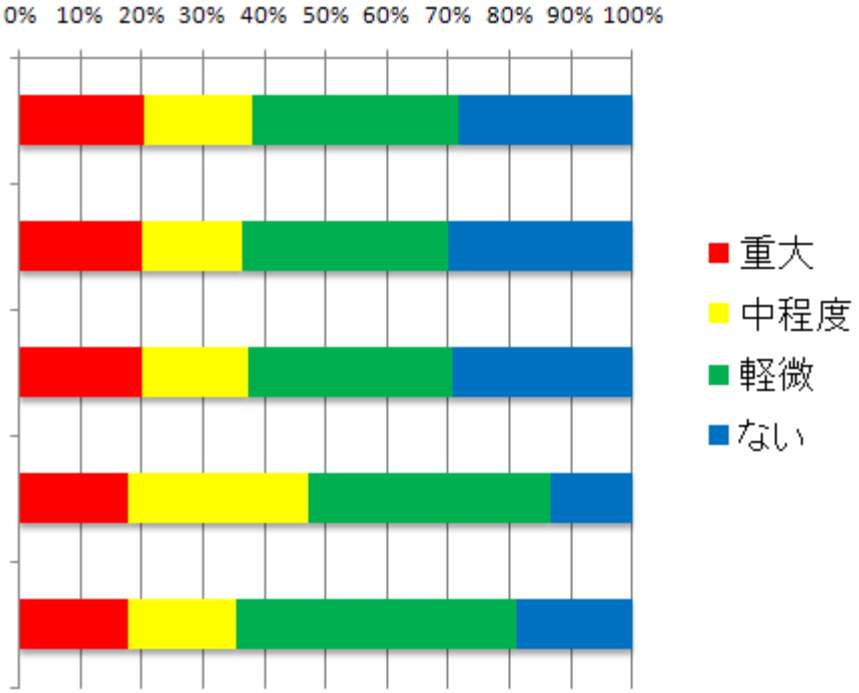
10. 事業者が情報セキュリティ監査を実施していない

11. 事業者が情報セキュリティポリシーを制定していない

12. 事業者が従業員に情報セキュリティ教育を実施していない

13. 自組織サービスが取得しているログを紛失したり、漏えいさせるリスク

14. 事業者の機器（サーバ、ストレージなど）が盗まれるリスク



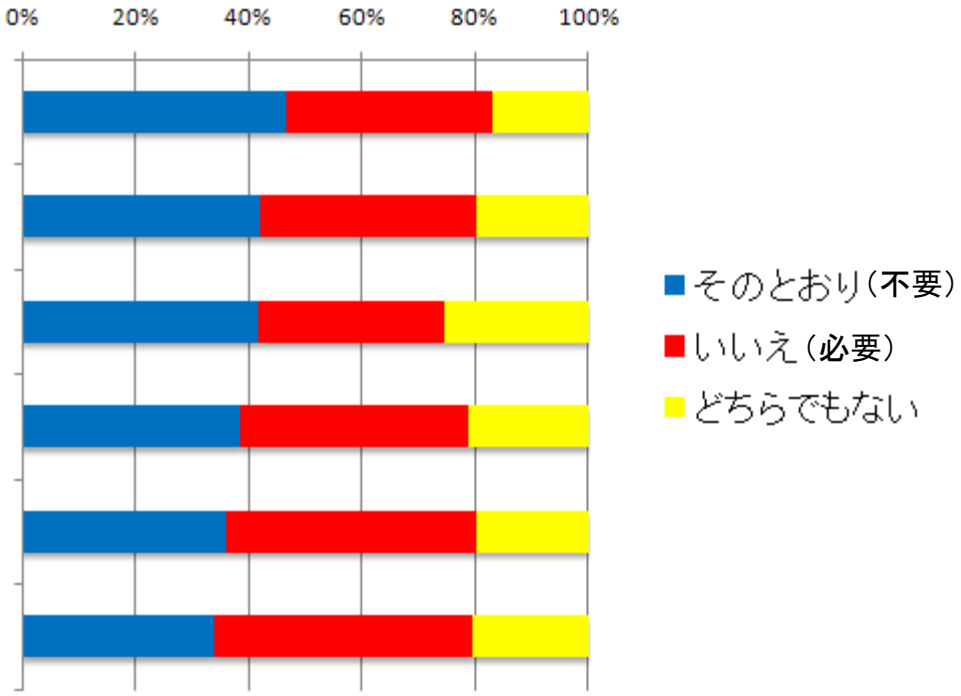
2.3　クラウドのリスク評価⑨

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

クラウドの導入により不要となるセキュリティ対策

「そのとおり」と回答した件数が多かった対策　1～6位　（N=316）

1. サーバ室の入退室管理
2. OSやアプリケーションのセキュリティパッチ
3. サーバでの情報セキュリティ対策
4. 定期的なバックアップ
5. ウィルスパターンファイル更新
6. ネットワークの侵入検知（不正侵入の監視）



2.3　クラウドのリスク評価⑩

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

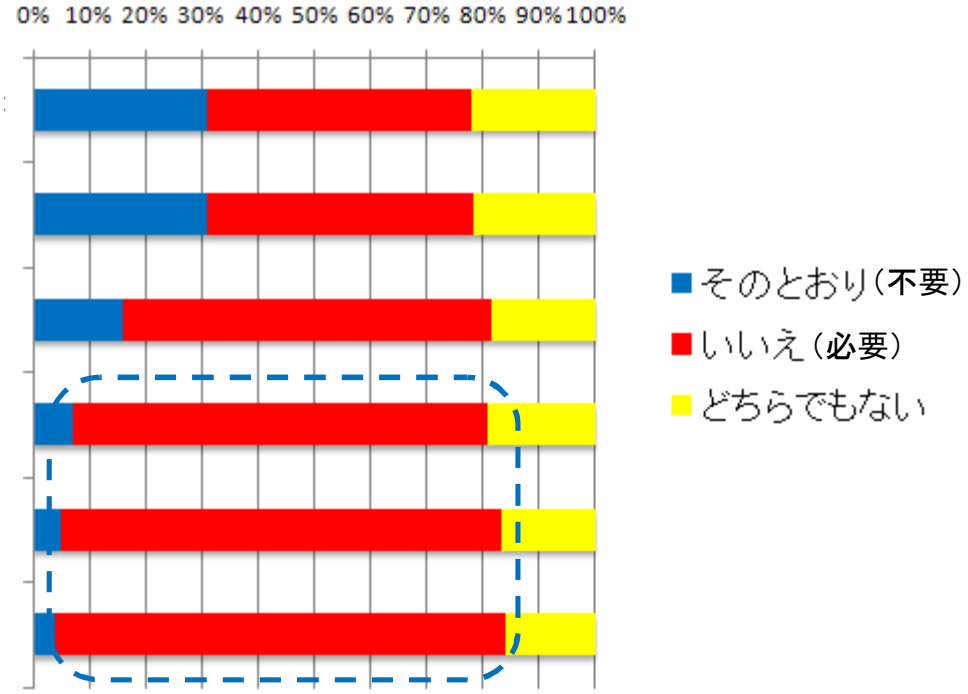
クラウドの導入により不要となるセキュリティ対策

「そのとおり」と回答した件数が多かった対策　7～12位　（N=316）

7. ログの取得と保存

8. ネットワークのセキュリティログの取得と保存
9. アクセス管理（ユーザの設定、維持、退職などによる削除）
10. 情報システムのインデント管理

11. 情報セキュリティポリシーの策定および定期的な維持管理
12. 情報セキュリティ教育



インシデント管理や情報セキュリティポリシーの維持管理および情報セキュリティ教育等は、今後も必要

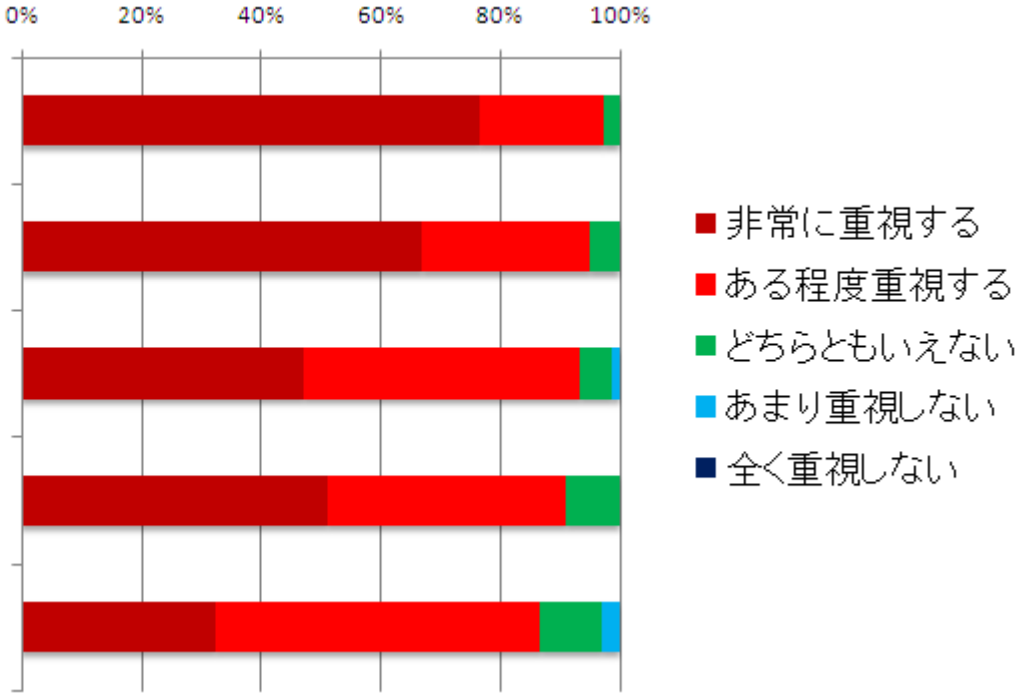
2.4 クラウド事業者の選定要因①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

クラウド事業者の選択で重視する項目

「重視する」と回答した件数が多かった項目　トップ5　（N=316）

1. 障害が起きた時の対応が早い
2. 月額（ランニング）費用が安い
3. 技術力が高い
4. 導入（イニシャル）費用が安い
5. 会社の実績が豊富である



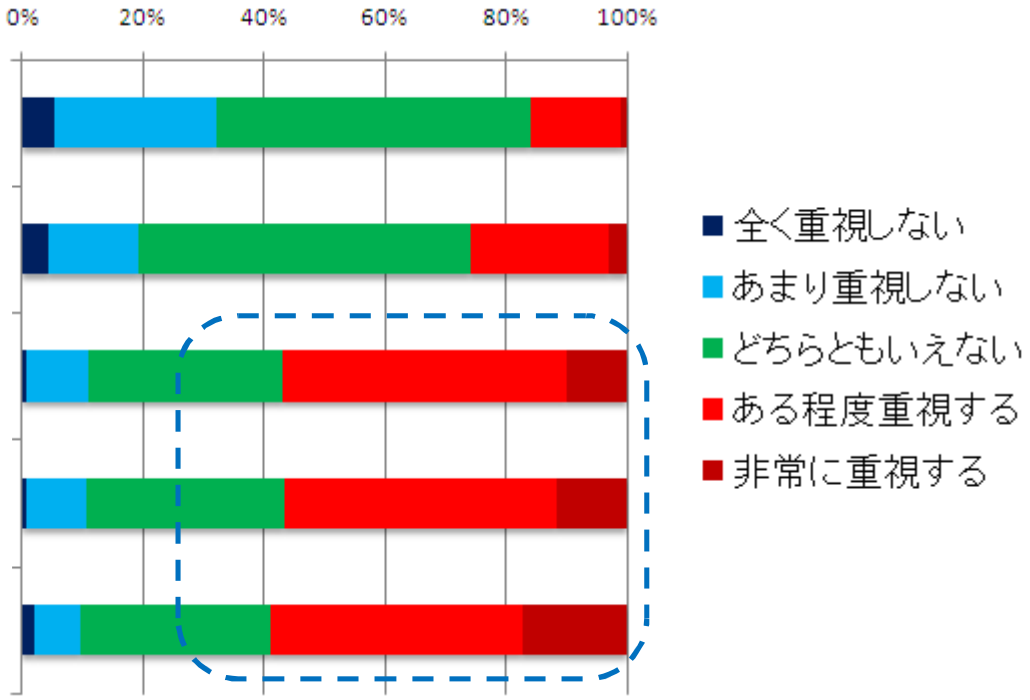
2.4 クラウド事業者の選定要因②

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

クラウド事業者の選択で重視する項目

「重視しない」と回答した件数が多かった項目　トップ5　（N=316）

1. 広告、宣伝を良く見る
2. セミナーなどを頻繁に開催している
3. 会社の知名度が高い
4. 営業の提案力が高い
5. 仮想化技術を選択できる



広告宣伝やセミナよりも、知名度や提案能力、技術の選択などを重要としている

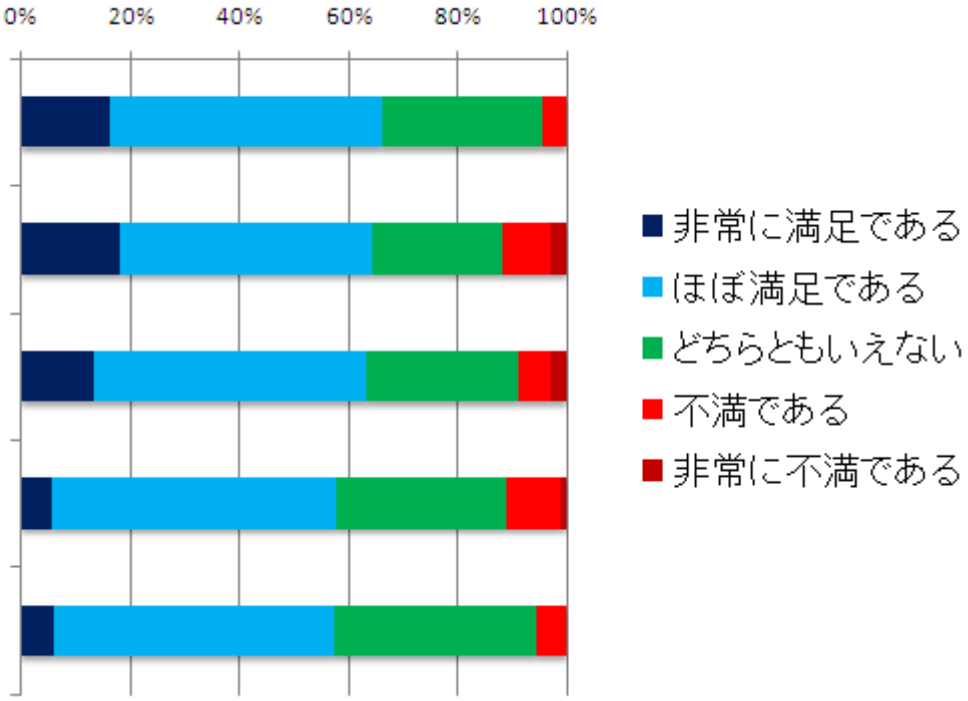
2.4 クラウド事業者の選定要因③

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

現在利用中のクラウドサービスの満足度

「満足である」と回答した件数が多かった項目　トップ5　（N=70）

1. 会社の知名度が高い
2. 導入（イニシャル）費用が安い
3. 会社の実績が豊富である
4. 障害が起きた時の対応が早い
5. 技術力が高い

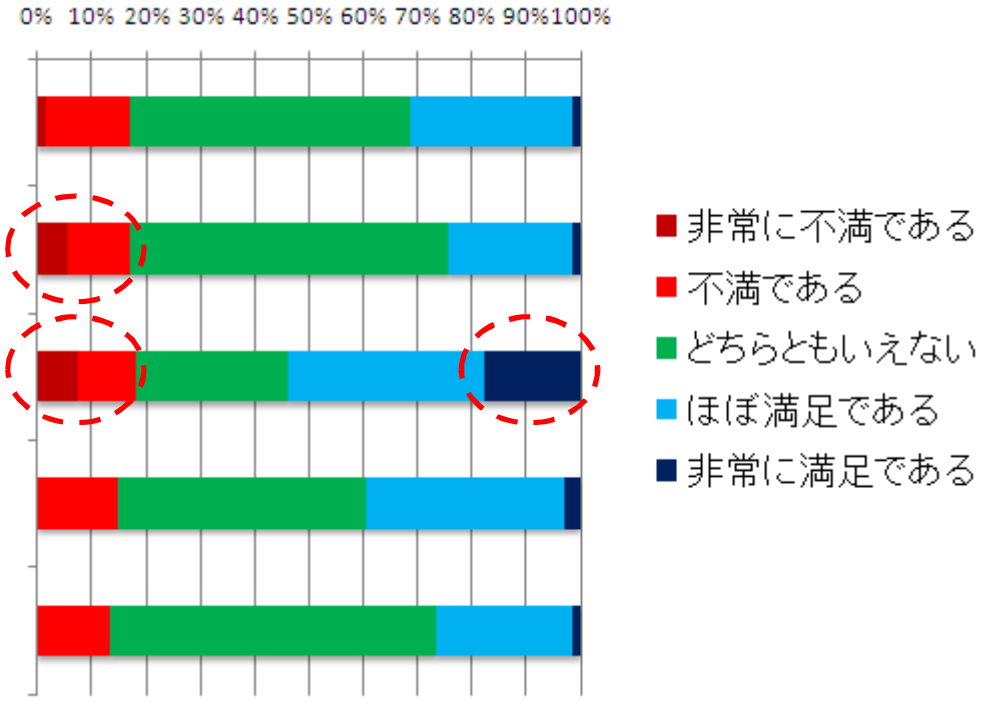


2.4 クラウド事業者の選定要因④

現在利用中のクラウドサービスの満足度

「不満である」と回答した件数が多かった項目　トップ5　（N=70）

1. カスタマイズ等の実現スピードが早い
2. 営業の提案力が高い
3. 月額（ランニング）費用が安い
4. サービス提供状況を報告・可視化している
5. 監査できる



クラウドでも営業力は求められる
ランニング費用に対する満足の一方、不満も多い

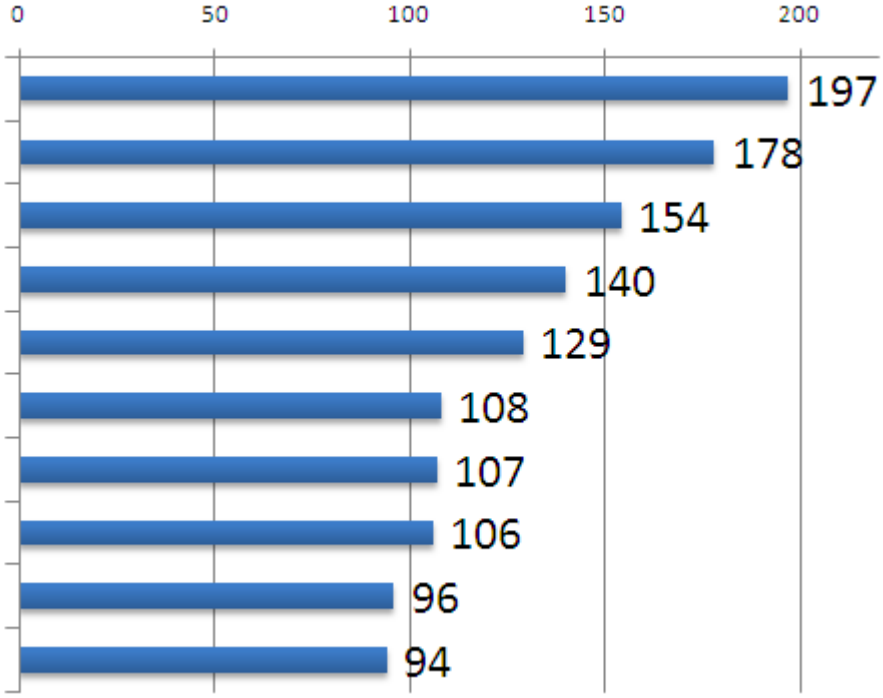
2.4 クラウド事業者の選定要因⑤

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

クラウド事業者とのSLAで特に重視する項目トップ10

（N=316）複数選択

1. 重大障害時の代替手段
2. サービス時間
3. 平均復旧時間
4. サービス稼働率
5. サポート時間帯
6. バックアップの方法
7. バックアップデータの保存期間
8. オンライン応答時間
9. ログの取得
10. 障害通知プロセス



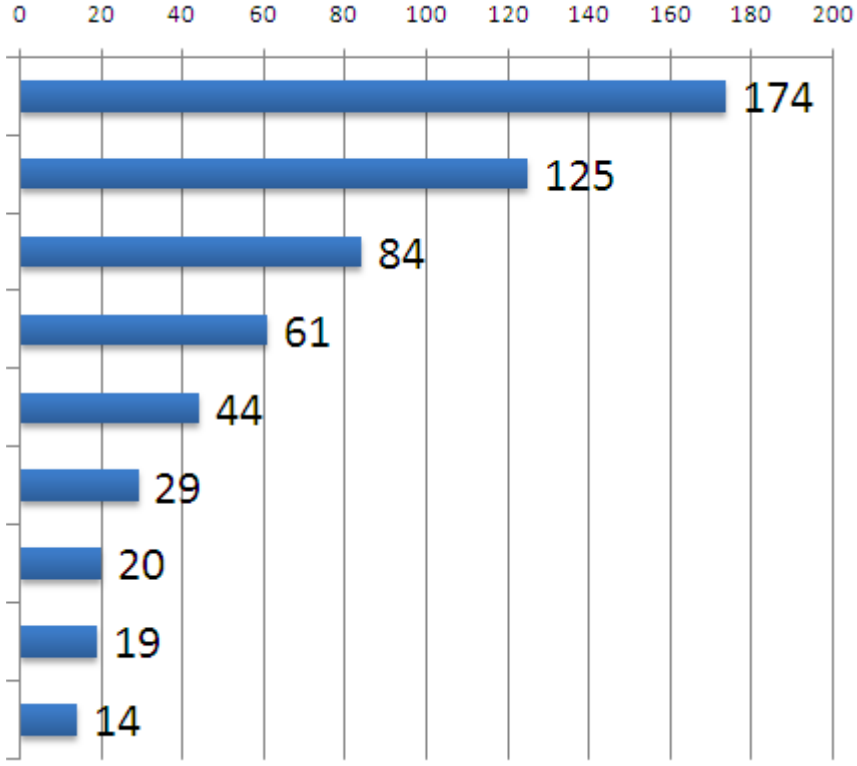
2.4 クラウド事業者の選定要因⑥

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

クラウド事業者に備えていて欲しい第三者評価

（N=316）複数選択

1. ISMSの認定取得
2. Pマークの認定取得
3. BS25999（BCM/BCP）の認定取得
4. ASP・SaaS情報開示認定の取得
5. SAS70type2/18号監査の認定取得
6. PCI DSSの認定取得
7. SysTrustの取得
8. CSAへの参加
9. その他



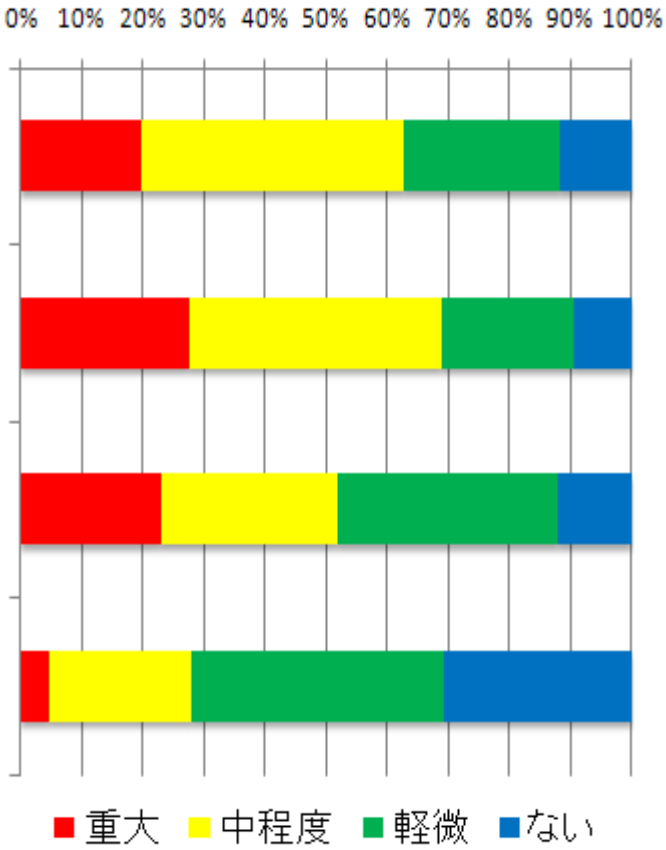
3　ENISAのリスク評価結果との比較①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

組織的リスク①

リスク	ENISA
LOCK-IN 事業者に囲い込まれて、後日、事業者を変更できなくなってしまうリスク	High
LOSS OF GOVERNANCE 事業者にすべてを任せてしまい、自組織で対応できなくなるリスク	High
COMPLIANCE CHALLENGES 事業者のコンプライアンス違反で、自組織も違反になってしまうリスク	High
LOSS OF BUSINESS REPUTATION DUE TO CO-TENANT ACTIVITIES 同じ事業者を利用する競争相手との差別化ができなくなるリスク	Medium

アンケート結果



日本企業は、囲い込み、ガバナンスのリスクは欧州ほど強く感じていない。

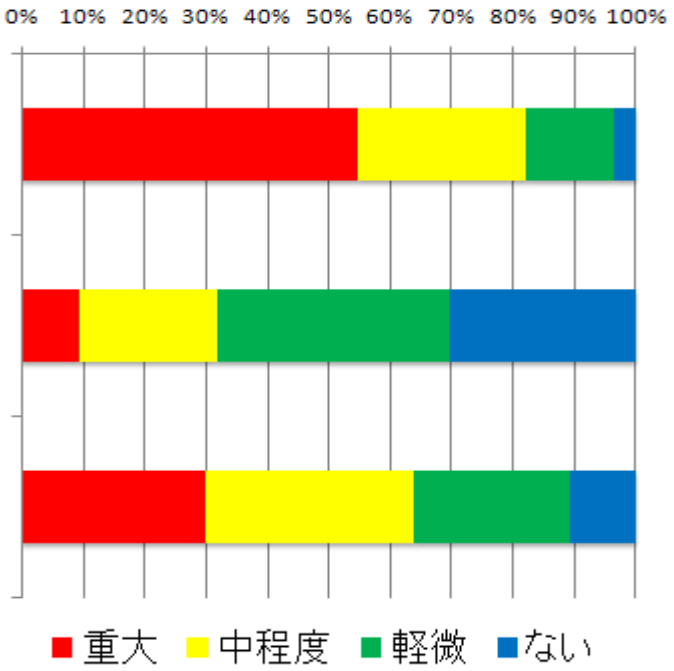
3　ENISAのリスク評価結果との比較①

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

組織的リスク②

リスク	ENISA
CLOUD SERVICE TERMINATION OR FAILURE 事業者がサービスを中断したときに、自組織のビジネスへのリスク	Medium
CLOUD PROVIDER ACQUISITION 事業者が買収されて、競合相手の傘下に入ってしまうリスク	Medium
SUPPLY CHAIN FAILURE 事業者が利用している他のクラウド事業者のトラブルの影響を受けて、サービス提供が中断したり、サービス内容が変更されるリスク	Low

アンケート結果



日本企業は、ビジネスの継続性を重んじているため、欧州より、サービス中断にうるさい
しかし、買収されるリスクはあまり感じていない

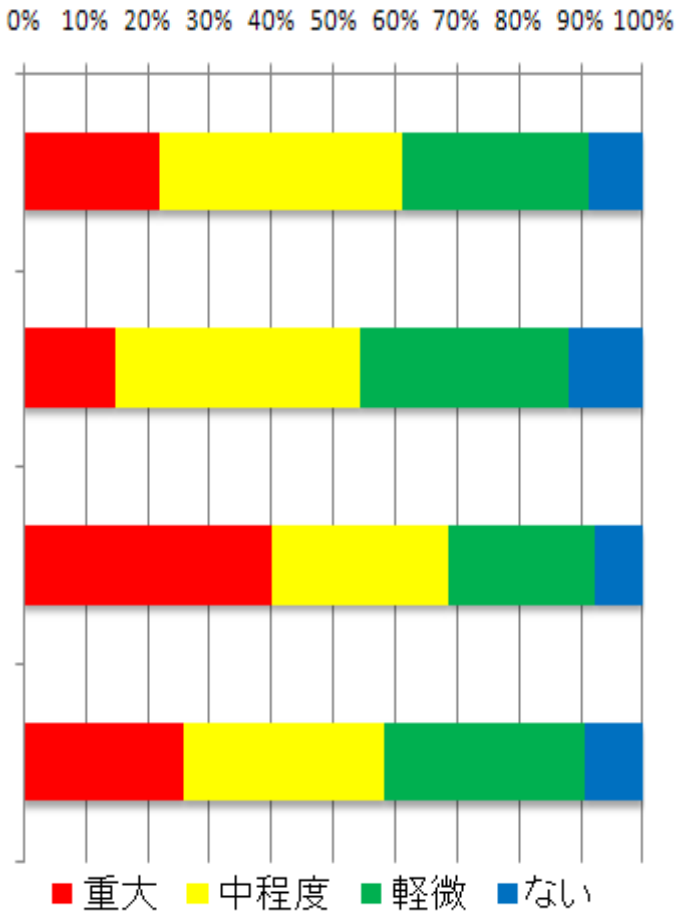
3　ENISAのリスク評価結果との比較②

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

技術的リスク①

リスク	ENISA
RESOURCE EXHAUSTION 事業者のリソース（サーバのCPU能力やストレージの容量）が不足して、その影響を受ける（処理速度が遅い、ファイルが保存できないなど）リスク	Medium
ISOLATION FAILURE リソースを共用する他の利用者の影響で自組織のサービス品質が低下するリスク	High
CLOUD PROVIDER MALICIOUS INSIDER - ABUSE OF HIGH PRIVILEGE ROLES 事業者の内部者によるセキュリティ違反（不正アクセスなど）で自組織の機密情報が見られその事実が分からないリスク	High
MANAGEMENT INTERFACE COMPROMISE 事業者が意図的に、自組織の機密情報を盗み見するリスク	Medium

アンケート結果



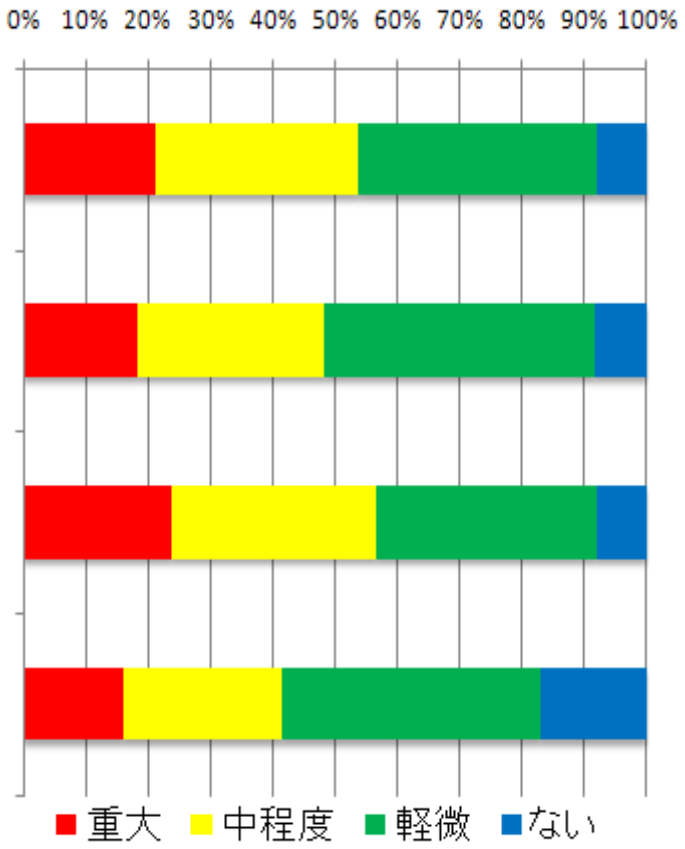
セキュリティ違反は強く感じているものの、リソース共有によるサービス低下については強く感じていない

3　ENISAのリスク評価結果との比較②

技術的リスク②

リスク	ENISA
INTERCEPTING DATA IN TRANSIT DATA LEAKAGE ON UP/DOWNLOAD, INTRA-CLOUD 事業者へのデータ転送の際に機密情報が漏えいするリスク	Medium
INSECURE OR INEFFECTIVE DELETION OF DATA 事業者が不要になったデータを消去しないリスク	Medium
DISTRIBUTED DENIAL OF SERVICE (DDOS) 事業者へのDDoS攻撃でサービスが中断したり品質低下するリスク	Medium
ECONOMIC DENIAL OF SERVICE (EDOS) 事業者を利用して提供している自組織のWebサービスなどへのDDoS攻撃を受けて、増えたアクセスに対する使用料を事業者に請求されるリスク	Medium

アンケート結果



日本企業は、一般的な技術的なリスクについては、欧州企業とあまり変わらない

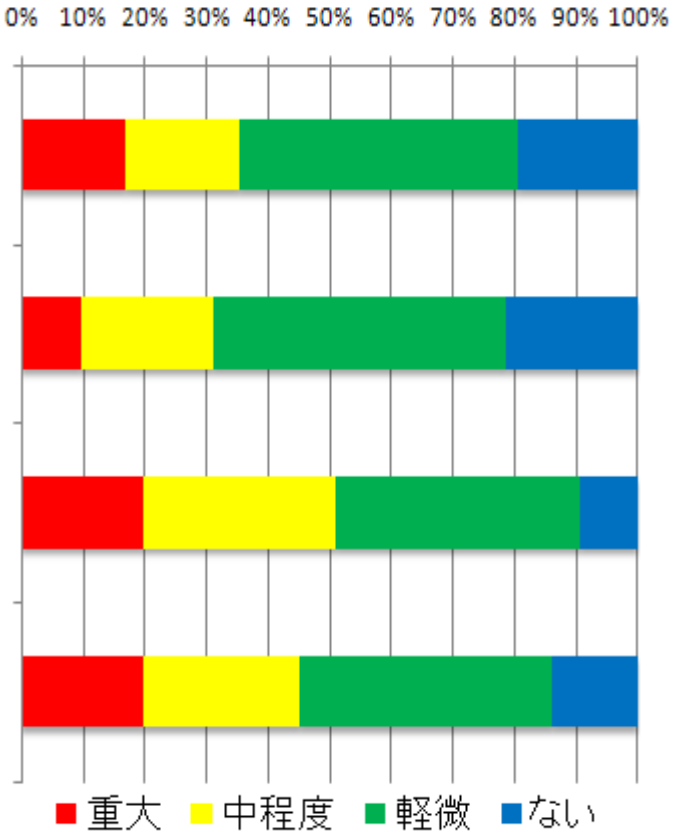
3　ENISAのリスク評価結果との比較②

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

技術的リスク③

リスク	ENISA
LOSS OF ENCRYPTION KEYS 事業者が暗号かぎを紛失して復号できなくなるリスク	Medium
UNDERTAKING MALICIOUS PROBES OR SCANS スキャン（空いているポートを探すなど）のリスク	Medium
COMPROMISE SERVICE ENGINE 事業者の提供するサービスに欠陥や問題があるリスク	Medium
CONFLICTS BETWEEN CUSTOMER HARDENING PROCEDURES AND CLOUD ENVIRONMENT 事業者の提供するセキュリティ水準が低いため、結果として自組織のセキュリティが低くなるリスク	Low

アンケート結果

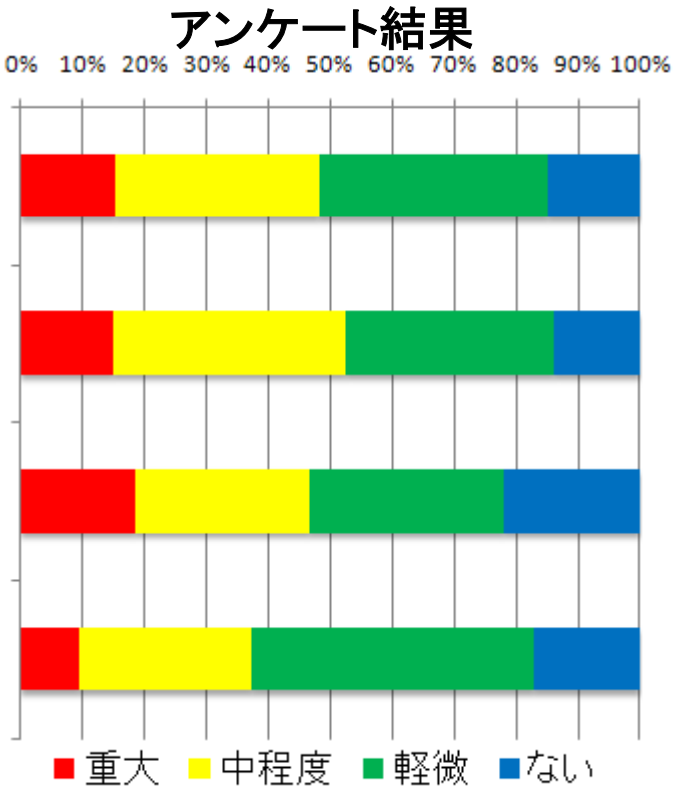


3　ENISAのリスク評価結果との比較③

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

法的リスク

リスク	ENISA
SUBPOENA AND E-DISCOVERY 事業者への法的な命令で証拠保全が必要となる（例えば法的機関へ自組織の情報が提出される）リスク	High
自組織への法的な命令で証拠保全が必要となる場合、事業者側で証拠保全ができないリスク	High
RISK FROM CHANGES OF JURISDICTION 事業者と自組織の所在地（国）が異なり、裁判の管轄や適用される法令（例えば個人情報保護法など）が異なるリスク	High
LICENSING RISKS 事業者が受けているソフトウェアのライセンス条件と自組織に必要となる条件が異なるリスク	Medium



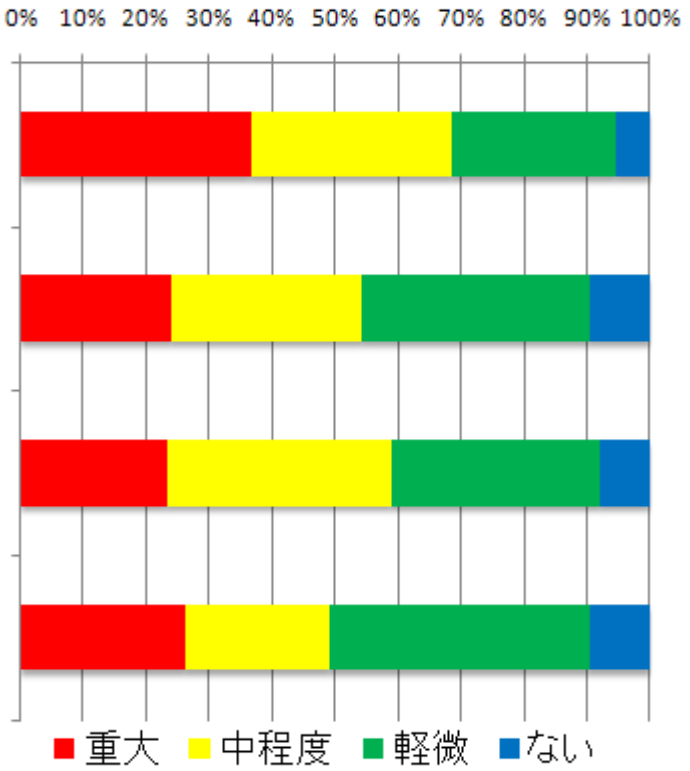
欧州企業は、日本企業と比べて、法的なリスクを強く感じている。
日本企業がクラウドでグローバル展開するときには、避けて通れない問題であることを周知する必要がある

3　ENISAのリスク評価結果との比較④

共通事項①

リスク	ENISA
NETWORK BREAKS 事業者と自組織を結ぶネットワークがダウンするリスク	Medium
NETWORK MANAGEMENT 事業者の運用管理体制が悪く、容量不足や、接続ミスなどが起きるリスク	High
MODIFYING NETWORK TRAFFIC ネットワーク障害の場合、事業者と自組織間の経路変更できないリスク	Medium
PRIVILEGE ESCALATION 事業者のルート権限を奪取されて、自組織情報が盗まれたり、改ざんされるリスク	Medium

アンケート結果



日本企業は、ネットワークの管理などについては、既存のサービス品質が高いため、あまり真剣に考えていない。
今後、グローバルな展開で海外ベンダを使うときには問題となる。

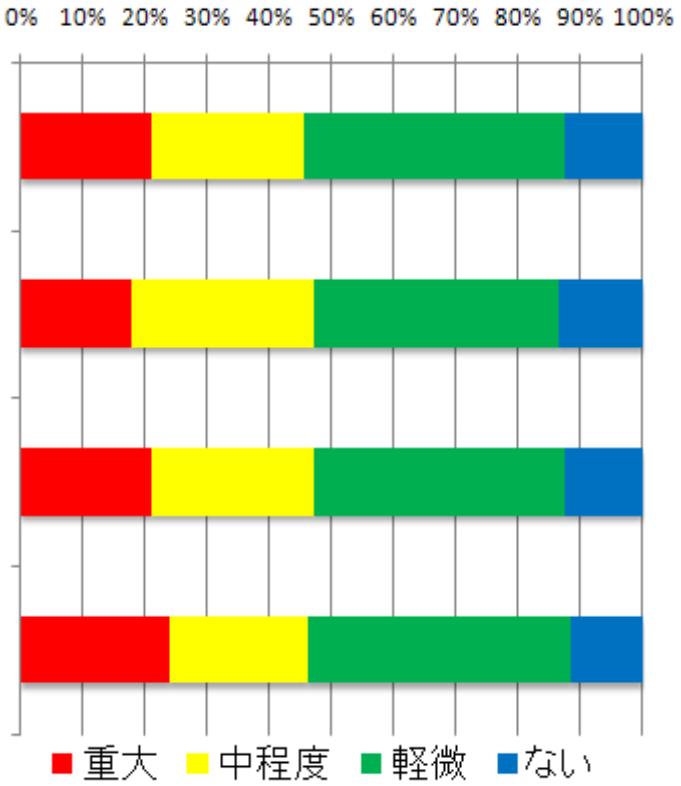
3　ENISAのリスク評価結果との比較④

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

共通事項②

リスク	ENISA
SOCIAL ENGINEERING ATTACKS 事業者がソーシャルエンジニアリング攻撃を受けて、自組織に関する情報を開示するリスク	Medium
LOSS OR COMPROMISE OF OPERATIONAL LOGS 自組織サービスが取得しているログを紛失したり、漏えいさせるリスク	Low
LOSS OR COMPROMISE OF SECURITY LOGS 事業者が認証などのセキュリティログを紛失したり、漏えいさせるリスク	Low
BACKUPS LOST, STOLEN 事業者がバックアップファイルを毀損させたり、漏えいさせるリスク	Medium

アンケート結果



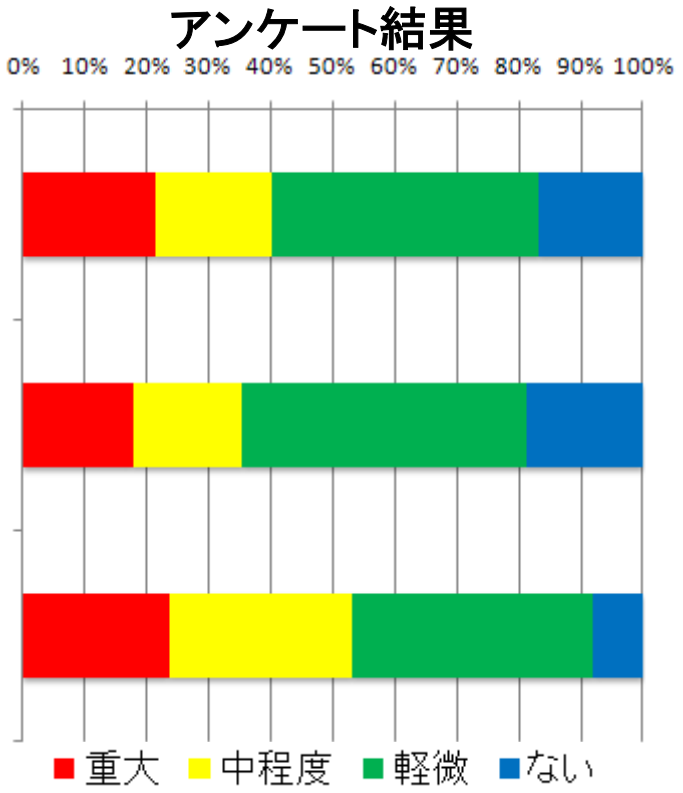
日本企業は、共通的なリスクについては、欧州企業とあまり変わらない

3　ENISAのリスク評価結果との比較④

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

共通事項③

リスク	ENISA
UNAUTHORIZED ACCESS TO PREMISES 事業者の施設に簡単に侵入でき、機器にもアクセスできるリスク	Low
THEFT OF COMPUTER EQUIPMENT 事業者の機器（サーバ、ストレージなど）が盗まれるリスク	Low
NATURAL DISASTERS 事業者が自然災害を受けてサービスが停止するリスク	Low



日本企業は、自然災害については、欧州企業よりも、重視している

4 おわりに

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- クラウドに対する懸念
  - 日本企業は、日本のガラパゴス的な高品質サービスをクラウドにもとめるようにみられる。
  - 欧州は企業は、安いサービスをリスクをにらみながら利用しようと考えている。
- クラウドに対する期待
  - 企業は、既存サービスの置き換えとして日本型の高品質サービスを求めているがグローバルとずれてしまう可能性がある

- 第51回CSEC研究発表会で情報セキュリティ大学院大学

  原田研究室　服部真　が分析結果を発表予定
- アンケート調査票・集計結果はウェブで公開予定。

  http://lab.iisec.ac.jp/~harada_lab/

ご清聴ありがとうございました