２２－Ｈ００１

平成２２年度
IT サービスマネジメントの利活用による
システム構築・運用環境の改善に向けた調査研究
成果報告書

平成 23 年 3 月

財団法人　日本情報処理開発協会

この事業は、競輪の補助金を受けて実施したものです。
http://ringring-keirin.jp/

はじめに

本報告書は、財団法人日本情報処理開発協会が財団法人JKAの補助金を受けて実施した平成22年度情報化推進に関する調査研究等補助事業「ITサービスマネジメントの利活用によるシステム構築・運用環境の改善に向けた調査研究」の事業の一環として取りまとめたものである。

IT の発展と IT サービスの利活用は、ビジネスの効率化を目的とした導入からはじまり、社会システム構築・運用の基盤となりつつある。特に IT への依存度が高まっている状況では、IT サービスを一定の品質でどのように提供するかが IT サービスマネジメントの利活用の観点から重要となっている。

最近のように IT 環境が大きく変化する中では、システムのアウトソーシングが進み、必要なシステム機能を取り込むことができるクラウドコンピューティングの利活用が、さらに進展するものと考えられる。クラウドコンピューティングは、ソフトウェアの利用方法の一形態として考えられるため、何をどう管理すればいいのか、どのような点に留意する必要があるのか、IT サービス利用の側面における喫緊の課題となっている。

本事業は、企業・組織における IT 資産、とりわけソフトウェア資産のライフサイクルを通じた、効果的なソフトウェア資産管理及び保護を実現するため、国際規格 ISO/IEC 19770-1（JIS X 0164-1）（Information technology-Software Asset management-Part1）に基づいた比較検討、及び SAM ユーザーズガイドを活用するための実証評価をした。また、IT サービスマネジメントの利活用の観点から企業の効果的な SAM の導入を促進するための説明会を全国４ヶ所で実施した。

本調査研究の成果については、昨年度に引き続き情報セキュリティに取組む様々な団体が協力して開催する「情報セキュリティに関する総合的普及啓発シンポジウム」で報告された。今回は、「クラウド時代における情報セキュリティとソフトウェア資産管理」をメインテーマに、「クラウド時代における政策及び情報セキュリティの側面」（１日目）及び「クラウド時代におけるソフトウェア資産管理の側面」（２日目）をサブテーマとして取り上げた。

このような検討やシンポジウムの実施に当っては、関連する団体の皆様のご協力により実現したもので、この場を借りて講師の方々、委員をはじめ原稿をご執筆頂いた関係各位に対し厚く御礼を申し上げる。

最後になりますが、本事業にご支援いただいた財団法人 JKA ならびに日頃からご指導いただいている関係官庁に対して厚く御礼を申し上げる。

平成 23 年 3 月

財団法人　日本情報処理開発協会

目　　次

1. 事業の概要及び背景

1.1 概要

本事業では、組織内の効果的なソフトウェア資産管理（SAM：Software Asset Management）及び保護を実現するための調査研究を実施するとともに、国内外における企業や団体などのSAMに関する動向調査を行った。本事業の目的は、わが国における企業や団体における情報セキュリティ強化の促進と適切なソフトウェア資産管理を推進させるとともに、わが国の企業・組織におけるITサービスマネジメントの利活用によるシステム構築の普及・推進活動に資する情報を提供することにある。

ソフトウェア資産管理及びITサービス継続管理に関しては、本報告書の別冊である「ソフトウェア資産管理及びITサービス継続管理に関する国際動向調査研究報告書」にて参照されたい。また、本調査研究の成果については、昨年度に引き続き実施した情報セキュリティに関する総合的な普及啓発シンポジウムで報告された。

特に、情報セキュリティに関連する取り組みは、国をはじめ団体あるいは特定非営利法人（NPO）において、それぞれの視点、立場から行われているが、企業においては、これらの活動や成果に関する情報が個別に提供されるため、相互の関係や位置付けなどが十分理解されない面もある。

今後はこれらの活動の相互連携も必要とされているため、情報セキュリティに取り組む様々な団体等が協力して、情報セキュリティに関する総合的なシンポジウムを開催することとし、そのテーマや内容について検討した。今年度は、「クラウド時代における情報セキュリティとソフトウェア資産管理」をメインテーマに、「クラウド時代における政策及び情報セキュリティの側面」（１日目）及び「クラウド時代におけるソフトウェア資産管理の側面」（２日目）をサブテーマとして取り上げて、専門家の方々をお招きしご講演いただいた。

事業の実施にあたっては、学識経験者並びに情報セキュリティ・ソフトウェア関連分野の業界知識者をもって構成する「情報セキュリティ普及実行評価検討委員会」、「ソフトウェア資産管理評価検討委員会」を設置して調査研究を実施した。また、ソフトウェア資産管理及びITサービス継続管理に関する国際動向調査、並びにセキュリティ関連団体が連携して実施する情報セキュリティに関する総合的普及啓発シンポジウムの会場運営などについては、専門機関又は事業者を選定、委託して実施した。

本事業の実施体制は、図1.1の通りである。

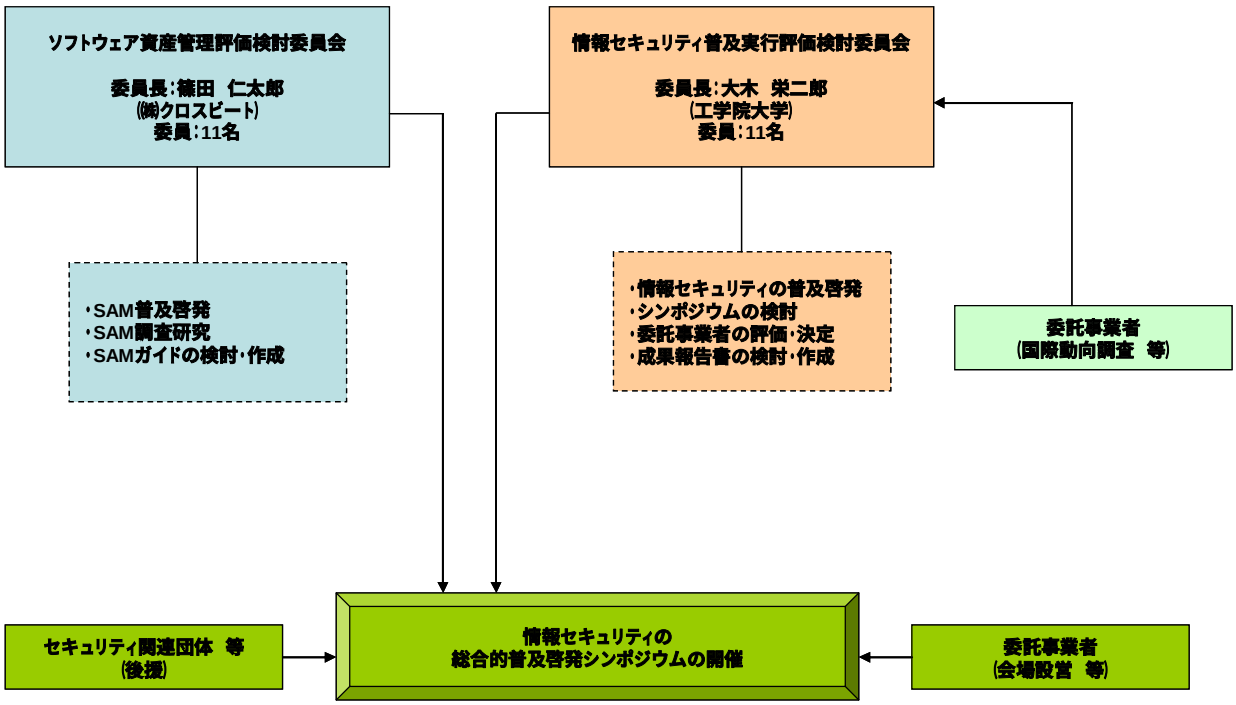


図1.1　実施体制

1.1.1　情報セキュリティ普及実行評価検討委員会

(1)委員構成

本事業の全体的な推進を主な役割とした委員会である。メンバー構成は次の通りである。

表 1.1　委員構成

ー	団体名	委員名
委員長	工学院大学	大木　栄二郎
委　員	NPO 日本ネットワークセキュリティ協会(JNSA)	安田　直
委　員	NPO 日本セキュリティ監査協会(JASA)	永宮　直史
委　員	独立行政法人情報処理推進機構(IPA)	菅野　泰子
委　員	㈱ラック内　ISOG-J (日本セキュリティオペレーション事業者協議会 ：Information Security Operation provider Group Japan)	西本　逸郎
委　員	(社)電子情報技術産業協会(JEITA)	馬場　敬博
委　員	(財)インターネット協会(IAjapan)	人見　庸
委　員	情報ネットワーク法学会(IN-Law)	早貸　淳子
委　員	BCI 日本支部	小林　誠
委　員	日本セキュリティ・マネジメント学会(JSSM)	井上　克至
委　員	特定非営利活動法人　*it*SMF Japan	若山　郁夫

(2)検討内容

情報セキュリティ普及実行評価検討委員会の検討状況は、表 1.2 に示す通りである。

表 1.2　検討状況

回数	開催日	主要テーマ
第 1 回	2010.6.24	・本委員会での目標・計画・成果物について ・本年度の情報セキュリティ総合的普及啓発シンポジウムのテーマについて ・委託調査研究に関する公募の実施について
第 2 回	2010.8.26	・委託調査研究応募企業の評価・選定 ・シンポジウムプログラム内容の検討
第 3 回	2010.9.16	・委託調査研究応募企業の評価・選定 ・シンポジウム運営業務委託応募企業の評価・選定 ・シンポジウムプログラム内容の検討
第 4 回	2010.12.13	・委託調査（IT サービス継続管理）の進捗状況報告 ・情報セキュリティ総合的普及啓発シンポジウムの進捗状況報告及びアンケート内容の検討
第 5 回	2011.3.18	・情報セキュリティ総合的普及啓発シンポジウム実施報告 ・IT サービスマネジメントの利活用によるシステム構築・運用環境の改善に向けた調査研究成果報告書（案）の検討 ・国際動向調査研究の最終報告

1.1.2　ソフトウェア資産管理評価検討委員会

(1)委員構成

ソフトウェア資産管理（SAM）のユーザーズガイド作成を主な役割とした委員会である。メンバー構成は次の通りである。

表 1.3　委員構成

ー	所属機関名	委員名
委員長	㈱クロスビート	篠田　仁太郎
委　員	日本電気㈱	岩下　健久
委　員	オートデスク㈱	片岡　伸吉
委　員	有限責任あずさ監査法人	薩摩　貴人
委　員	ダイヤモンドレンタルシステム㈱	島田　篤
委　員	富士通㈱	高橋　快昇
委　員	㈱CMDB Consulting	武内　烈
委　員	有限責任監査法人トーマツ	田村　仁一
委　員	マイクロソフト㈱	手島　伸行
委　員	ウチダスペクトラム㈱	中村　大造
委　員	㈱シルクロード テクノロジー	中村　究

(2)検討内容

ソフトウェア資産管理評価検討委員会の検討状況は、表 1.4 に示す通りである。

表 1.4　検討状況

回数	開催日	主要テーマ
第 1 回	2010.6.23	・平成 22 年度　本委員会での目標・計画・成果物について ・ソフトウェア資産管理（SAM）に関する説明会の実施について ・ソフトウェア資産管理に関する委託調査研究について
第 2 回	2010.8.6	・各グループにおける作業内容の検討 -JIS X 0164-1 マッピング -SAM における SaaS、OSS 利用時の留意点 ・SAM 説明会（札幌）の実施報告 ・ソフトウェア資産管理に関する調査研究の公募状況について
第 3 回	2010.9.14	・各グループにおける作業の進捗状況の報告 -JIS X 0164-1 マッピング -SAM における SaaS、OSS 利用時の留意点 ・SAM 説明会（大坂）の実施報告 ・ソフトウェア資産管理に関する調査研究の公募状況について ・シンポジウムプログラム内容の検討について
第 4 回	2010.10.22	・各グループにおける作業の進捗状況の報告 -JIS X 0164-1 マッピング -SAM における SaaS、OSS 利用時の留意点 ・SAM 説明会（東京）の実施報告 ・ソフトウェア資産管理に関する調査研究について ・シンポジウムプログラム内容の報告
第 5 回	2010.12.1	・各グループにおける作業の進捗状況の最終報告 -JIS X 0164-1 マッピング -SAM における SaaS、OSS 利用時の留意点 ・SAM 説明会（福岡）の実施報告 ・ソフトウェア資産管理に関する調査研究の進捗状況報告
第 6 回	2011.3.17	・情報セキュリティ総合的普及啓発シンポジウム実施報告 ・IT サービスマネジメントの利活用によるシステム構築・運用環境の改善に向けた調査研究成果報告書（案）の検討 ・SAM 調査研究の最終報告

2. 情報セキュリティ総合的普及啓発シンポジウム

2.1 実施概要

本シンポジウムを「情報セキュリティ総合的普及啓発シンポジウム」と題し、次の概要にて実施した。

① タイトル

－情報セキュリティ総合的普及啓発シンポジウム

② 主催

－財団法人日本情報処理開発協会

③ 後援（順不同）

－経済産業省
－情報セキュリティ政策会議
－工学院大学
－特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）
－特定非営利活動法人 日本セキュリティ監査協会（JASA）
－社団法人電子情報技術産業協会（JEITA）
－独立行政法人情報処理推進機構（IPA）
－日本セキュリティ・マネジメント学会（JSSM）
－財団法人インターネット協会（IAjapan）
－日本セキュリティオペレーション事業者協議会（ISOG-J）
－BCI 日本支部
－情報ネットワーク法学会（IN-Law）
－特定非営利活動法人 *it*SMF Japan
－特定非営利活動法人 ソフトウェア資産管理コンソーシアム（SAMCon）
－ビジネス ソフトウェア アライアンス（BSA）

④ 開催日時

－1 日目：2011 年 1 月 27 日（木）11 時 00 分～17 時 00 分
－2 日目：2011 年 1 月 28 日（金）10 時 00 分～17 時 00 分

⑤ 会場

－有楽町朝日ホール（東京都千代田区有楽町 2-5-1　有楽町マリオン 11F）

⑥ プログラム概要

情報セキュリティ総合的普及啓発シンポジウム

メインテーマ ：「クラウド時代における情報セキュリティとソフトウェア資産管理」

【１月２７日】　「クラウド時代における政策及び情報セキュリティの側面」

ｔｉｍｅ	講演時間	内　容	講　師
11：00～11：05	（5 分）	開催挨拶	司会者
11：05～11：15	（10 分）	開会ご挨拶	挨拶： 財団法人　日本情報処理開発協会 常務理事 小林　正彦
11：15～12：05	（50 分）	基調講演 1： 「クラウドコンピューティングと 日本の競争力について」	講演者： 経済産業省 商務情報政策局　情報処理振興課 課長補佐 下田　裕和　氏
12：05～13：15	（70 分）	昼食休憩	
13：15～14：05	（50 分）	講演 1： 「クラウドサービスの 安全利用におけるチェック事項」	講演者： 独立行政法人　情報処理推進機構（IPA） セキュリティセンター 研究員 河野　省二 氏
14：05～14：55	（50 分）	講演 2： 「クラウドのリスクと セキュリティにおける法律面での 留意点」	講演者： 情報ネットワーク法学会(IN-Law) (英知法律事務所) 弁護士 岡村　久道　氏
14：55～15：10	（15 分）	休憩	
15：10～16：00	（50 分）	講演 3： 「クラウド利用と セキュリティオペレーション」	講演者： 情報セキュリティ 普及実行評価検討委員会 （日本セキュリティオペレーション 事業者協議会(ISOG-J)） 西本　逸郎　氏
16：00～17：00	（60 分）	パネルディスカッション (テーマ： クラウド時代の情報セキュリティ)	コーディネーター： 情報セキュリティ 普及実行評価検討委員会　委員長 （工学院大学　教授） 大木　栄二郎　氏 パネラー： ・河野　省二 氏 ・岡村　久道　氏

			・西本　逸郎　氏

【１月２８日】　「クラウド時代におけるソフトウェア資産管理の側面」

ｔｉｍｅ	講演時間	内　容	講　師
10：00～10：05	（5 分）	開催挨拶	司会者
10：05～10：55	（50 分）	基調講演 2： 「政府機関における 情報セキュリティの取組と ソフトウェア資産管理について」	講演者： 内閣官房情報セキュリティセンター 主査 渡邉　雅士　氏
10：55～11：45	（50 分）	講演４： 「IT サービスマネジメントと SAM の関係」	講演者： 特定非営利活動法人 *it*SMF Japan 理事 （日本ヒューレット・パッカード㈱ プロフェッショナル・サービス事業本部 コンサルタント） 塩田　貞夫　氏
11：45～13：00	（75 分）	昼食休憩	
13：00～13：50	（50 分）	講演 5： 「クラウド・コンピューティング 時代の SAM の考え方」	講演者： ソフトウェア資産管理評価検討委員会 （㈱シルクロード テクノロジー 執行役 コンサルティング＆サービス） 中村　究　氏
13：50～14：40	（50 分）	講演 6： 「JIS X 0164-1 から見た SAM ユーザーズガイド活用方法」	講演者： ソフトウェア資産管理評価検討委員会 （マイクロソフト㈱ ライセンスコンプライアンス推進本部 IT 資産管理推進部　部長） 手島　伸行　氏
14：40～14：55	（15 分）	休憩	
14：55～15：55	（60 分）	講演７： ・SAM 導入事例（自治体） 「宮崎県におけるソフトウェア 資産管理の取組みについて」	講演者： 宮崎県 県民政策部　情報政策課 課長 金丸　裕一　氏
		・SAM 導入事例（一般企業） 「富士通における SAM の事例」	富士通㈱ フィールド・イノベーション本部 第一 FI 統括部 ディレクタ 高橋　快昇　氏

15：55～17：00	（60 分）	パネルディスカッション （テーマ： ソフトウェア資産管理とクラウド）	コーディネーター： ソフトウェア資産管理評価検討委員会 委員長 （㈱クロスビート　取締役） 篠田　仁太郎　氏 パネラー： ・金丸　裕一　氏 ・高橋　快昇　氏 ・アドビシステムズ㈱ ライセンスコンプライアンス管理部 シニアマネージャー 宮澤　啓一郎　氏 ・マイクロソフト㈱ ライセンスコンプライアンス推進本部 本部長 相田　雄二　氏 ・有限責任監査法人トーマツ エンタープライズリスクサービス部 パートナー 田村　仁一　氏

⑦　申込者数

1,050 名

⑧　参加者

日　程	申込者数(A)	参加者数(B)	参加率(B÷A)
1 月 27 日(木)	600 名	396 名	66%
1 月 28 日(金)	450 名	298 名	66%
合　計	1,050 名	694 名	66%

2.2 アンケート集計

2.2.1　概要

本シンポジウムの参加者数 694 名のうちアンケート回答数は、452 名（全体回答率：65%）であった。アンケート項目の集計結果を「2.2.2 集計結果」に示す。

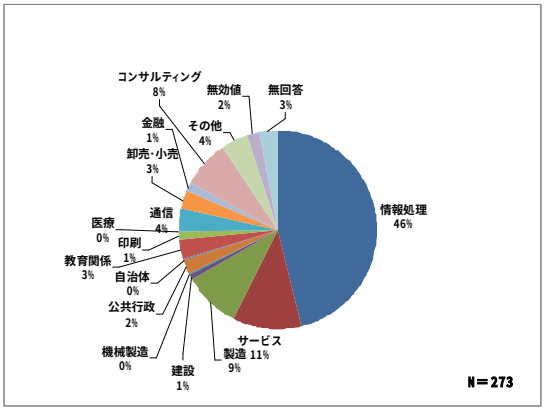
2.2.2　集計結果

(1) 業種及び参加日

①業種

最も多い参加業種は共に「情報処理」で１日目（46%）、２日目（44%）となっており、次いで「サービス」が１日目（11%）、２日目（7%）と続いている。

１日目（1/27）



２日目（1/28）

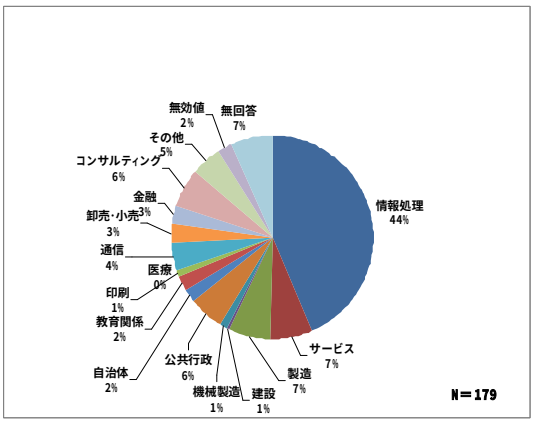


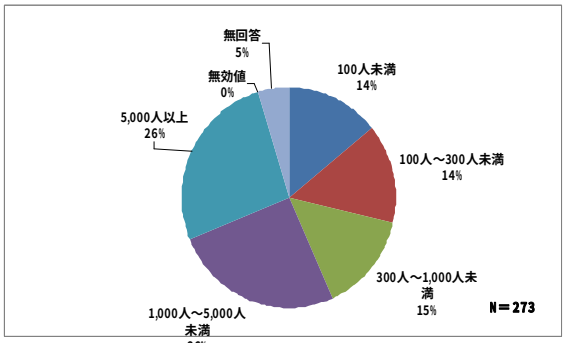
図 2.1　業種

その他の例：物流、出版、エネルギー、ソフトウェア開発　等（１日目）
ソフトメーカー、審査・検査　等（２日目）

②従業員数

１日目は「5,000 人以上」が 26%と最も多く、大規模企業からの参加が多いといえる。また、２日目は「1,000 人～5,000 人未満」が 31%と最も多い。

１日目（1/27）



２日目（1/28）

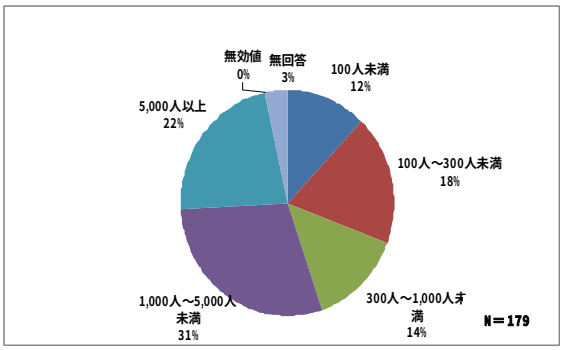
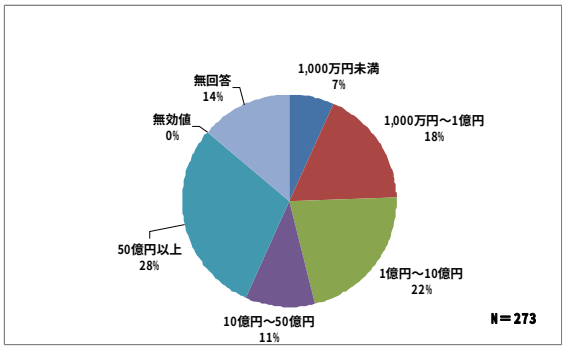


図 2.2　従業員

③資本金

１日目は「50 億円以上」が 29%と全体の３割を占め、２日目は「1,000 万円～1 億円未満」が 25%と最も多く、②の結果からも分かるように大規模企業の方がクラウド及び SAM に関心があることがわかる。

１日目（1/27）



２日目（1/28）

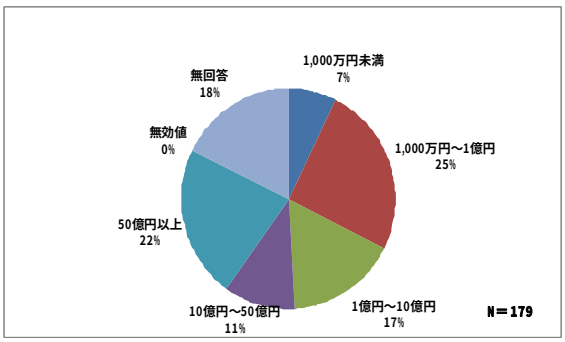
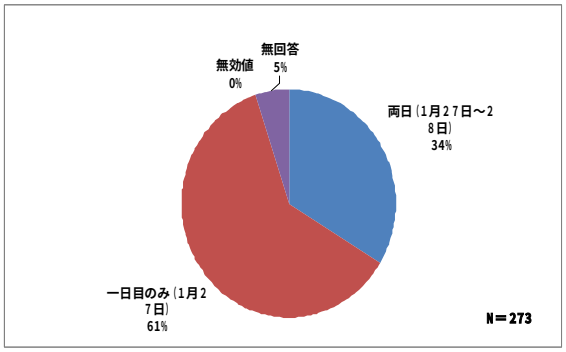


図 2.3　資本金

④参加日

「27 日のみ」が 61%、「28 日のみ」が 53%であった。このことから、クラウドに関心が高いことがわかる。

１日目（1/27）



２日目（1/28）

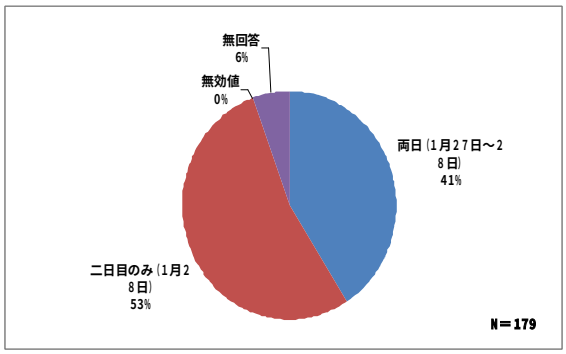


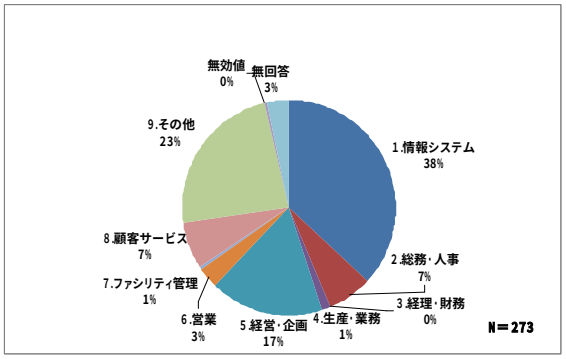
図 2.4　参加日

(2) 参加者について

①職種

両日共に「情報システム」が最も多く、それぞれ 38%、45%となっている。次いで「その他」が 23%、16%と続いている。

１日目（1/27）



２日目（1/28）

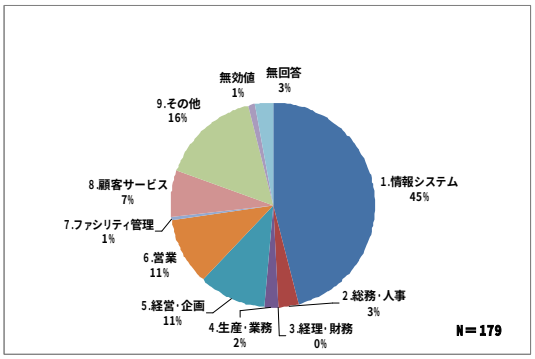


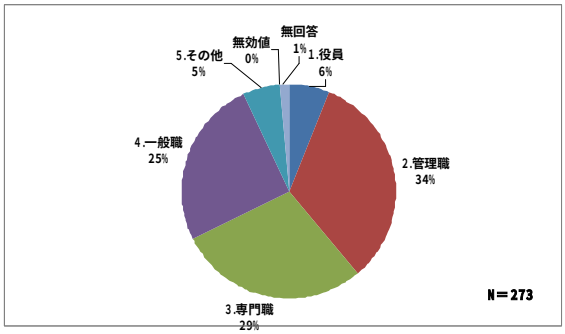
図 2.5　職種

その他の例：品質管理・人材育成、生産技術、広報宣伝、法務　等（１日目）
技術統括、教育、セキュリティ推進、リスク管理　等（２日目）

②役職

１日目は「管理職」が 34%で最も多く、２日目は「一般職」（33%）と「管理職」（32%）で全体の６割を占めている。

１日目（1/27）



２日目（1/28）

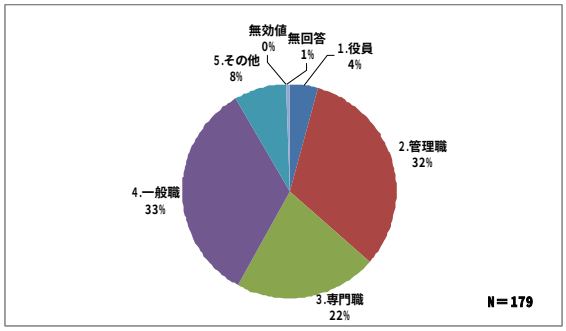
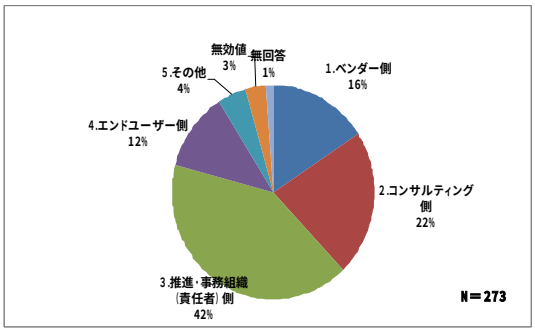


図 2.6　役職

③情報セキュリティに対する立場

両日共に「推進・事務組織（責任者）側」がそれぞれ 42%、36%と最も多くなっている。

１日目（1/27）



２日目（1/28）

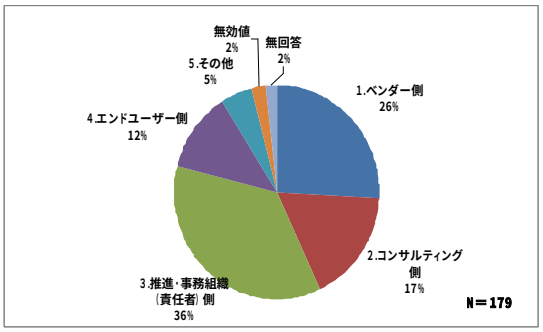


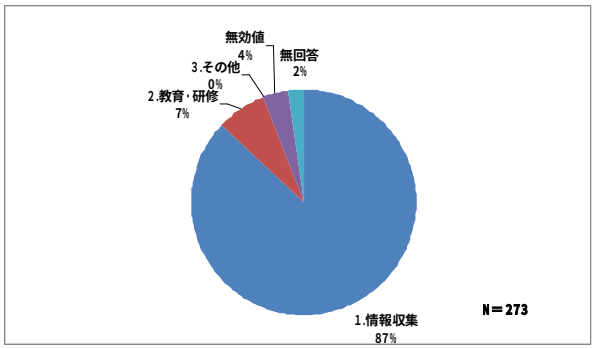
図 2.7　情報セキュリティに対する立場

その他の例：パートナー向け教育（指導を含む）、監査部門　等（１日目）
経営支援、監査側　等（２日目）

④本シンポジウムの参加目的

両日共に「情報収集」が 8 割以上を占めている。また、2 日目の参加者で「リスク把握」という意見もあった。

１日目（1/27）



２日目（1/28）

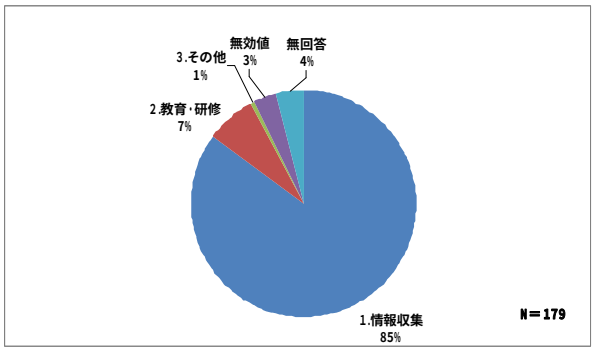


図 2.8　参加目的

(3) クラウド・コンピューティングについて（１日目（1/27））

①クラウドの利用状況

「利用を検討中」が 31%と最も多く、次いで「利用している」が 30%と続いている。

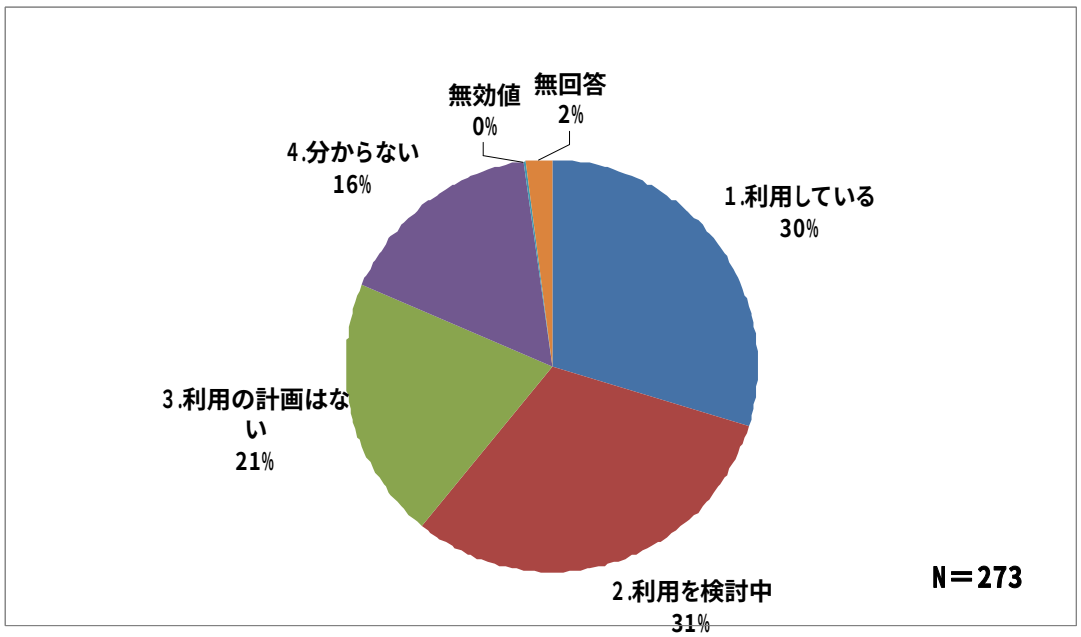


図 2.9　クラウドの利用状況

②利用したい（検討中の）クラウドサービスについて

クラウドを「１.利用している、２.利用を検討中」のいずれかの回答者に対して質問したところ、「グループウェア」（20%）と「アプリケーション」（20%）が最も多く、次いで「電子メール」が 16%と続いている。

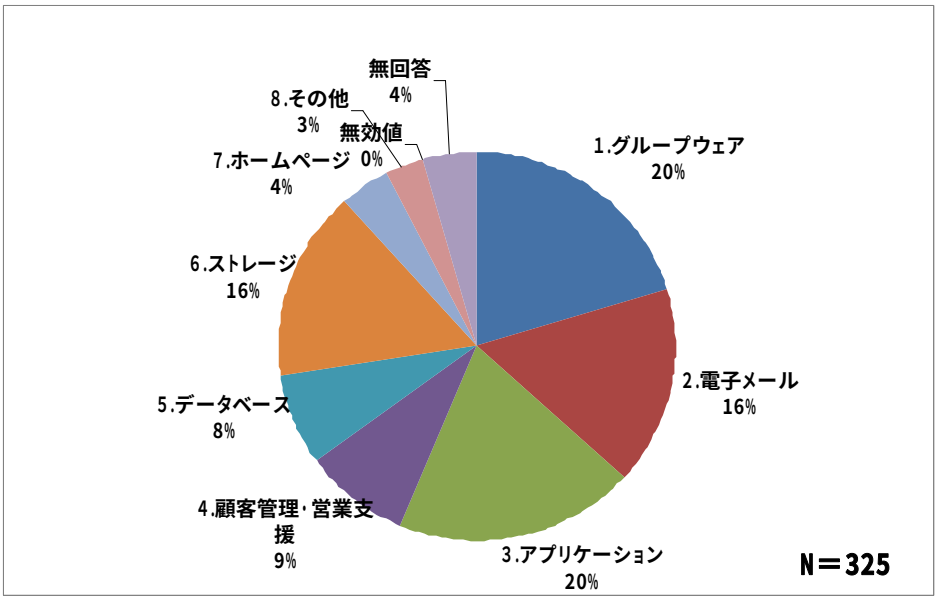


図 2.10　利用したい（検討中の）クラウドサービス

③クラウドを利用する際の利点について

クラウドを「１.利用している、２.利用を検討中」のいずれかの回答者に対して質問したところ、最も多いのが「運用コストの削減」で 24%となっている。次いで「IT 資産の保有の削減」が 19%と続いている。

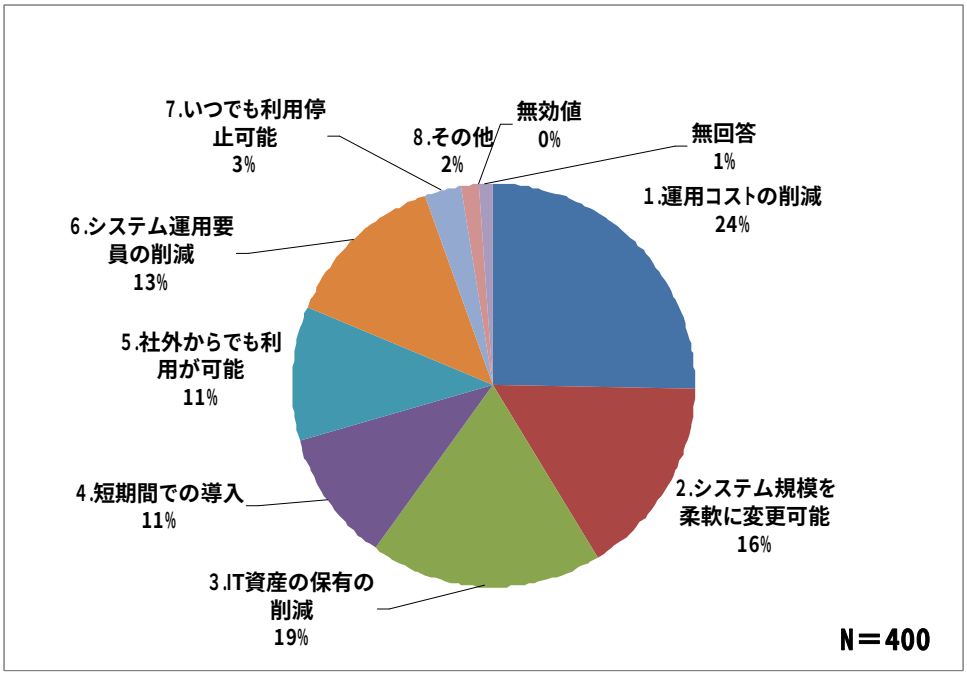


図 2.11　クラウドを利用する際の利点

その他：社内サーバー障害時の負荷低減、IT 関係要因の削減（開発・保守）等

④クラウドを利用する上での懸念事項

「サービスのセキュリティレベル」が 29%と最も多く、全体の３割となっている。

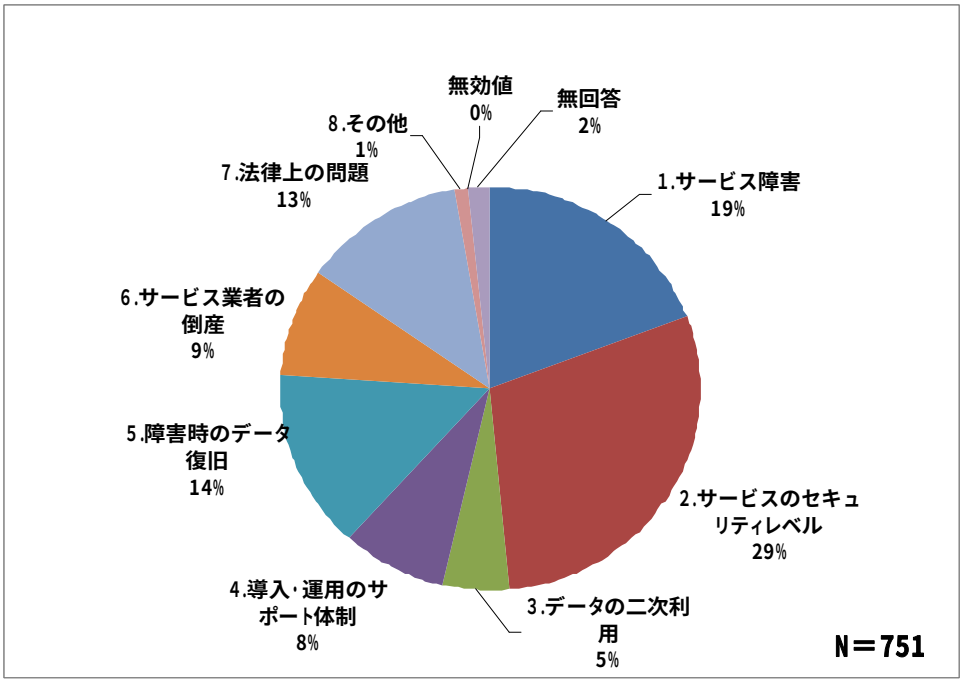


図 2.12　　クラウドを利用する上での懸念事項

その他：オンプレミス例のシステムとの連携、個人情報の保護が不安　等

⑤クラウドと情報セキュリティについて

「サービス障害時の対応体制」が 23%、「SLA の締結」と「サービス提供者の事業継続性」が 18%と、サービスの安定提供に考慮していることがわかる。

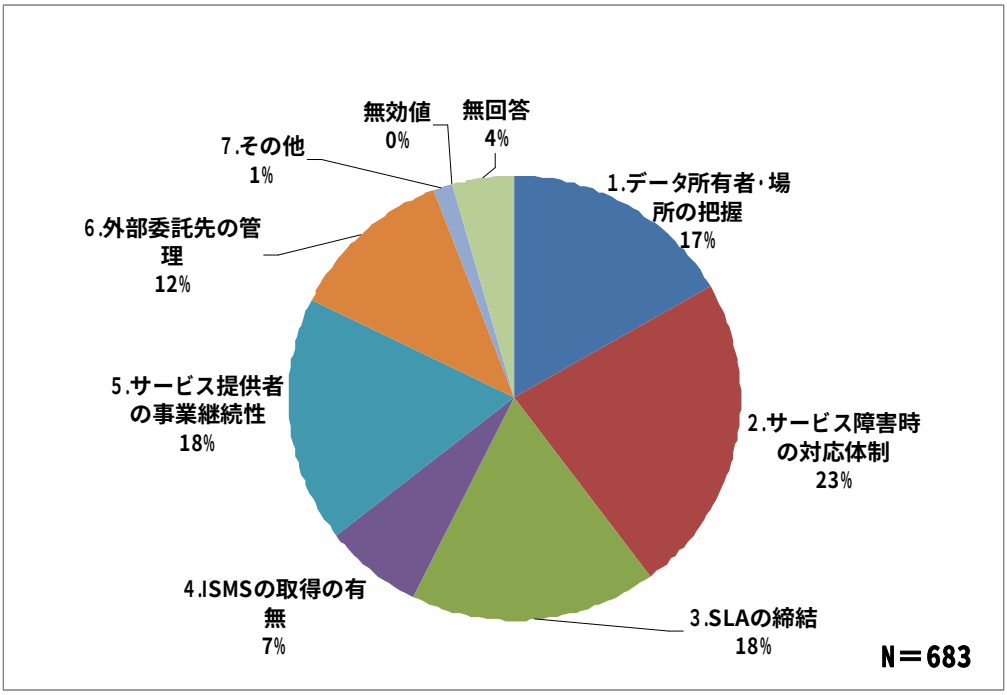


図 2.13　クラウドを利用する際情報セキュリティ管理体制上、留意・考慮している点

その他：運用手順、ルールの策定、内部統制対応（監査 18 号、SAS70 など）　等

⑥クラウドと IT サービスマネジメントについて

クラウドサービスを提供するにあたって、留意・考慮している点について質問したところ「サービスの可用性」が 33%と３割を占めている。

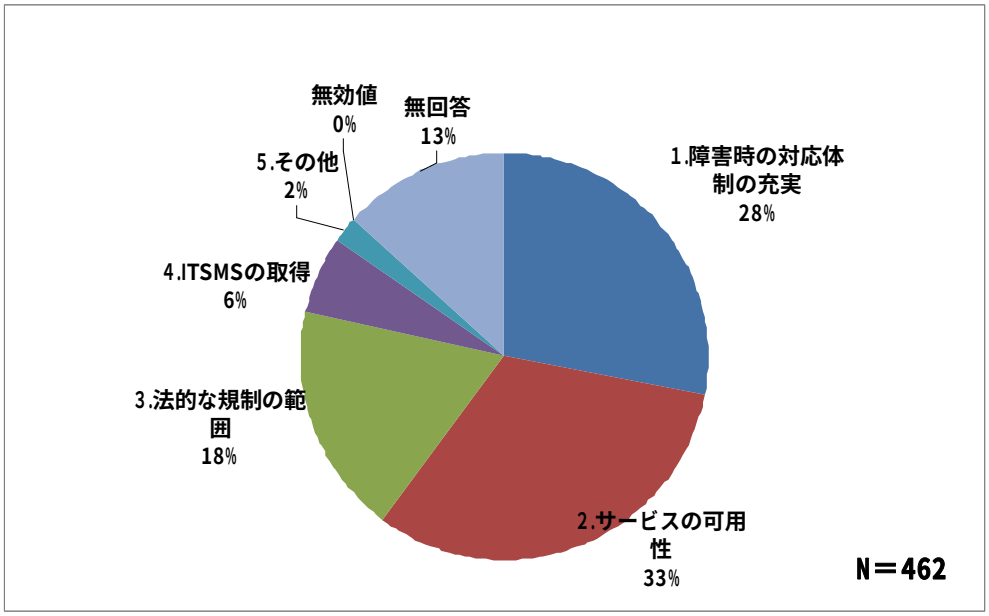


図 2.14　　クラウドサービスを提供するにあたって、留意・考慮している点

⑦クラウドサービスを利用する分野についてお聞かせ下さい。

内部情報系
ISO50001 とリンクしたビジネスの創出
通常業務で作成するデータ等の保管、共有
アプリケーション、グループウェア、メール等
サブシステム系が初期と考えるが、いずれ基幹含めたすべてが対応せざるを得ないと考える。
機密情報を扱わない業務
自社への管理系システムでの利用、顧客への提案（アプリケーションの運用）
業務システム（アプリケーション）
トライ＆エラー用新サービス（小規模）　資産をもたずすぐ止められるもの
資産管理（SAM を含めて）、セキュリティ（ログ･デバイスの禁止）
可用性、機密性が低い分野（匿名アンケートなど）、公開情報（会社のホームページなど）
製造業、物流系、公共
フロントオフィス系業務アプリ
ストレージ、ＤＢ、アプリ
顧客データ管理
地域の電子カルテ
情報共有を安く安全で早くどこからでも対応できる環境として利用したい ソフト開発環境のクラウド化によるＢＣＰの確保と、有休人材の活用を考えたい。
社内ワークフローや情報の共有
社内情報システム全般
開発（システム）、新規事業

⑧クラウドサービス提供事業者の選択基準として考慮している点

最も多かったのが「セキュリティ」で 28%、次いで「信頼」が 26%と続いている。

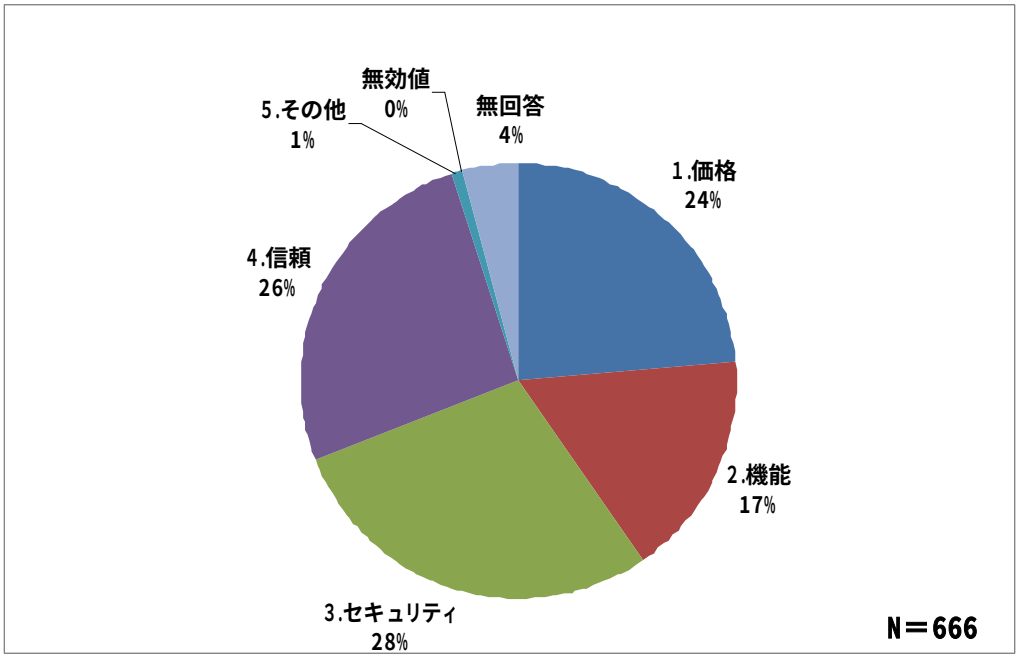


図 2.15　　クラウドサービス提供事業者の選択基準として考慮している点

その他：サービス提供事業者の事業状況、信頼性等。他業者への移行が容易　等

(4) ソフトウェア資産管理（SAM）について（２日目（1/28））

①SAM の実施状況について

SAM の実施状況について質問したところ、「実施している」が 32%と最も多い。次いで「検討中」（24%）、「構築中」（14%）と続き、「実施している」と併せると７割となっている。

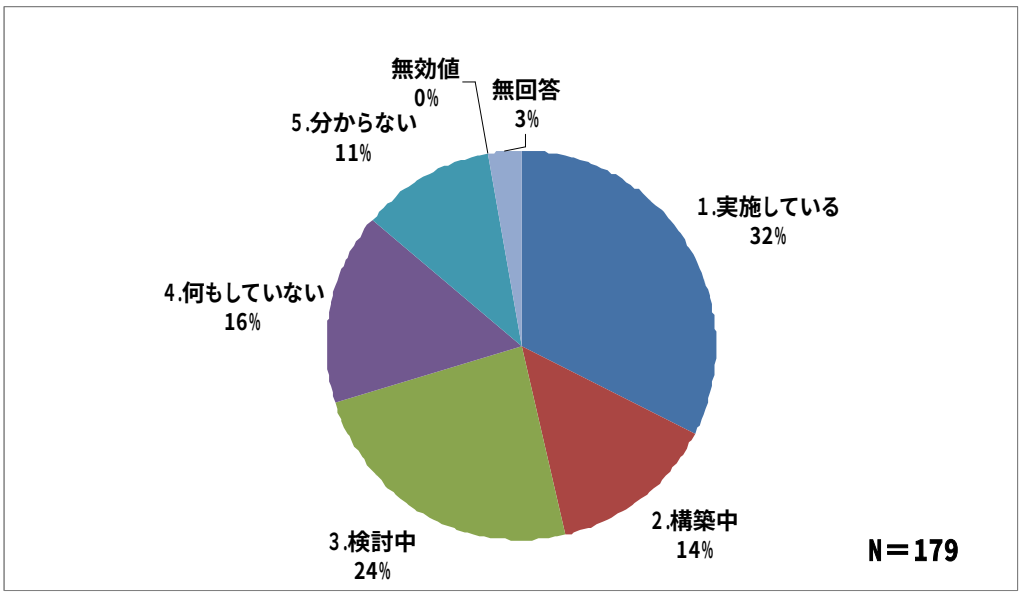


図 2.16　　SAM の実施状況

②外部組織のアドバイスや支援

SAM を「１.実施している、２.構築中、３.検討中」のいずれかの回答者に対して質問したところ、約４割が「受ける予定はない」と回答している。

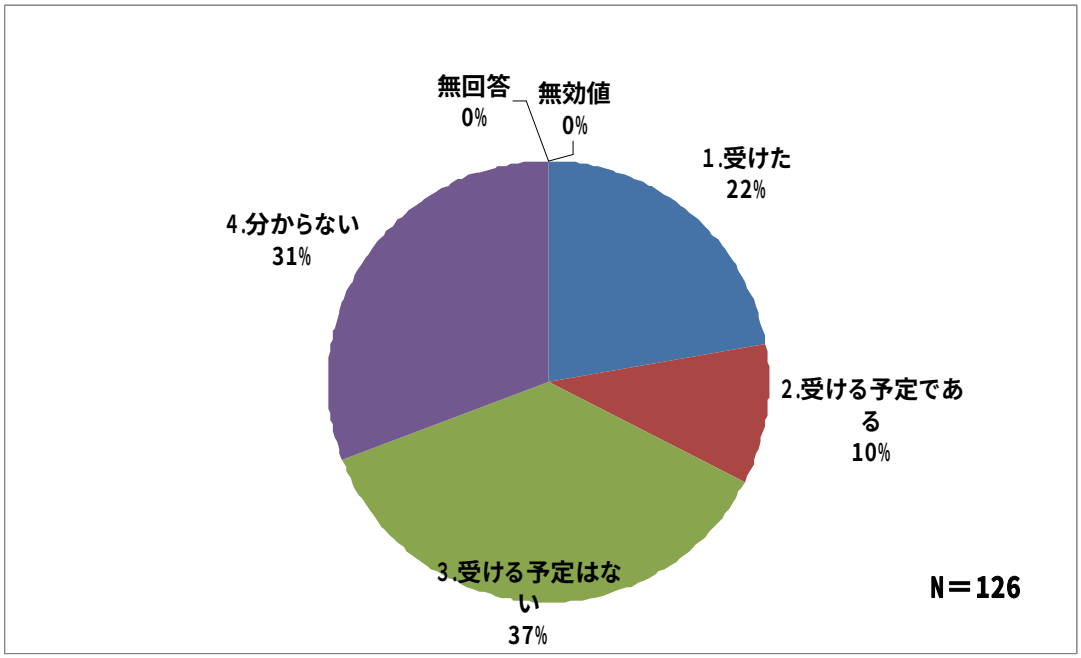


図 2.17　外部組織のアドバイスや支援

③外部組織のアドバイスの種類

外部組織のアドバイスを受けた回答者に対して質問したところ、約５割が「SAM のコンサルティング会社」（47%）からアドバイスを受けたと回答している。

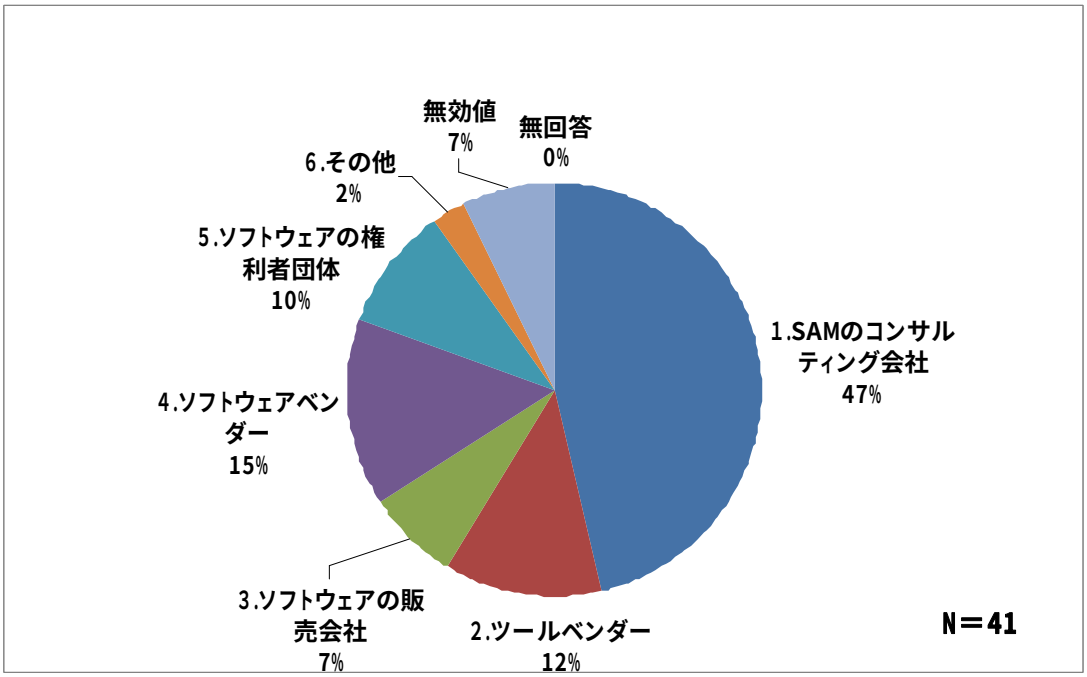


図 2.18　外部組織のアドバイスの種類

④外部組織のアドバイスの満足度

外部組織のアドバイスを受けた回答者に対して質問したところ、「満足だった」が 29%となっている。

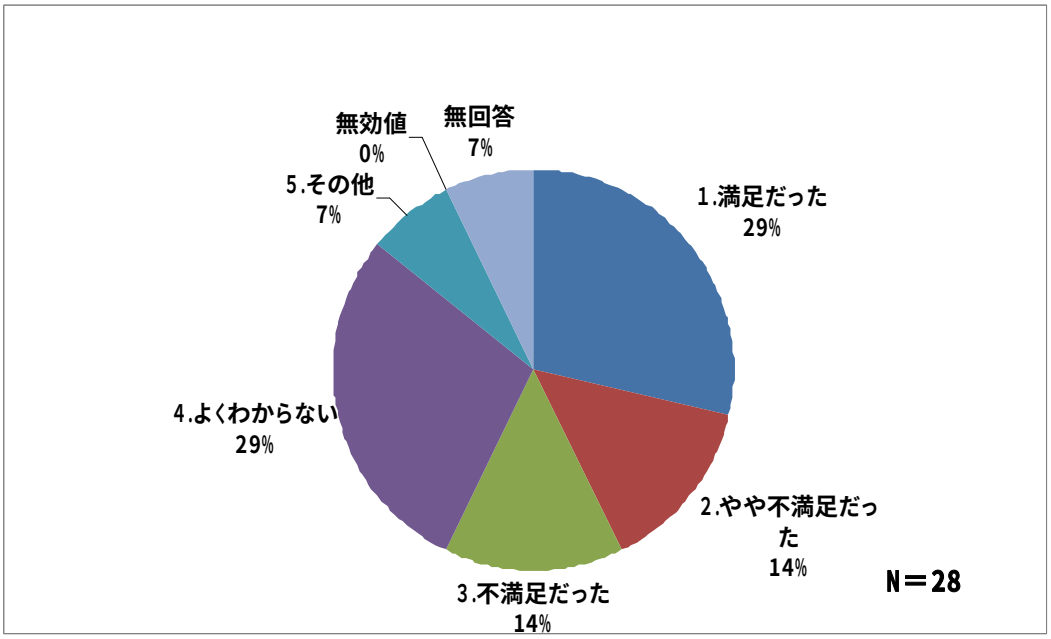


図 2.19　外部組織のアドバイスの満足度

⑤SAM の導入期間

SAM を「１.実施している、２.構築中、３.検討中」のいずれかの回答者に対して質問したところ、「一年 ～ 二年未満」が 25%と最も多く、「六ヶ月 ～ 一年未満」が 19%と続いている。

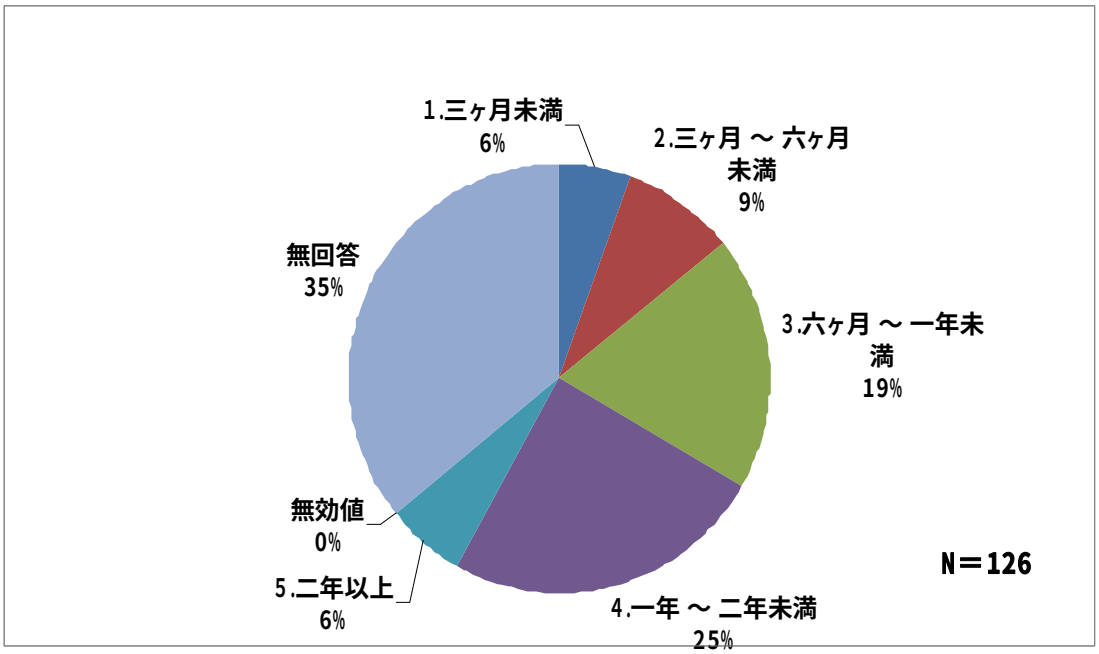


図 2.20　SAM の導入期間

⑥SAM を導入したきっかけ

SAM を「１.実施している、２.構築中、３.検討中」のいずれかの回答者に対して質問したところ、「組織内上層部からの要請」21%、「社内管理担当部門からの要請」17%と約４割が社内での要請で SAM を実施していることがわかる。

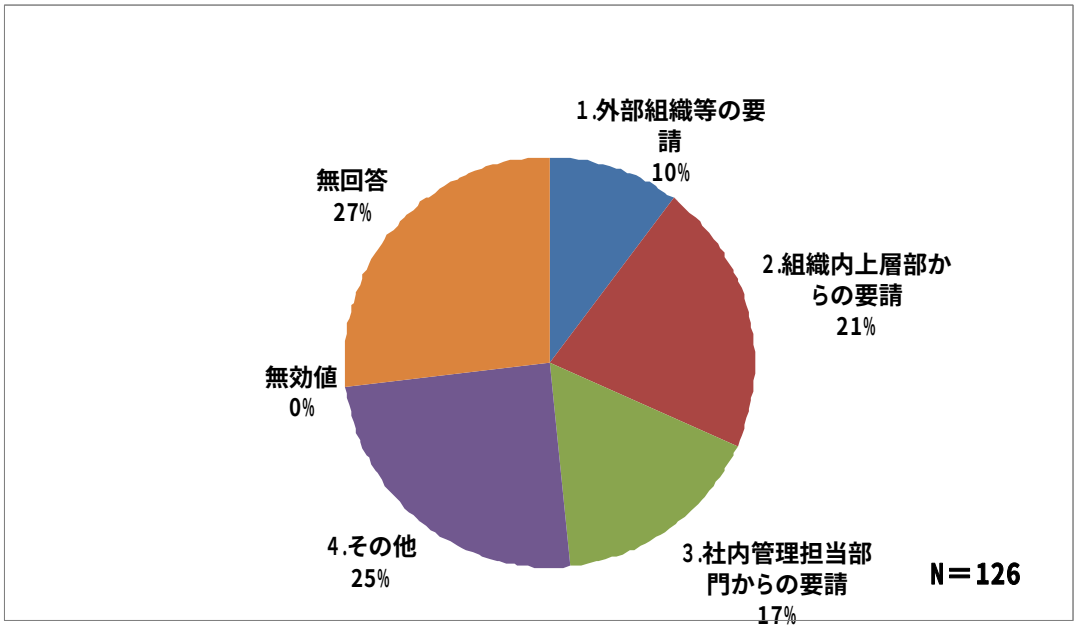


図 2.21　　SAM 導入のきっかけ

⑦SAM 導入時の予算

SAM を「１.実施している、２.構築中、３.検討中」のいずれかの回答者に対して導入予算について聞いたところ「不明」が 36%と最も多く、導入予算を明確にすることができないものといえる。回答された金額では「100 万円～500 万円未満」が 14%となっている。

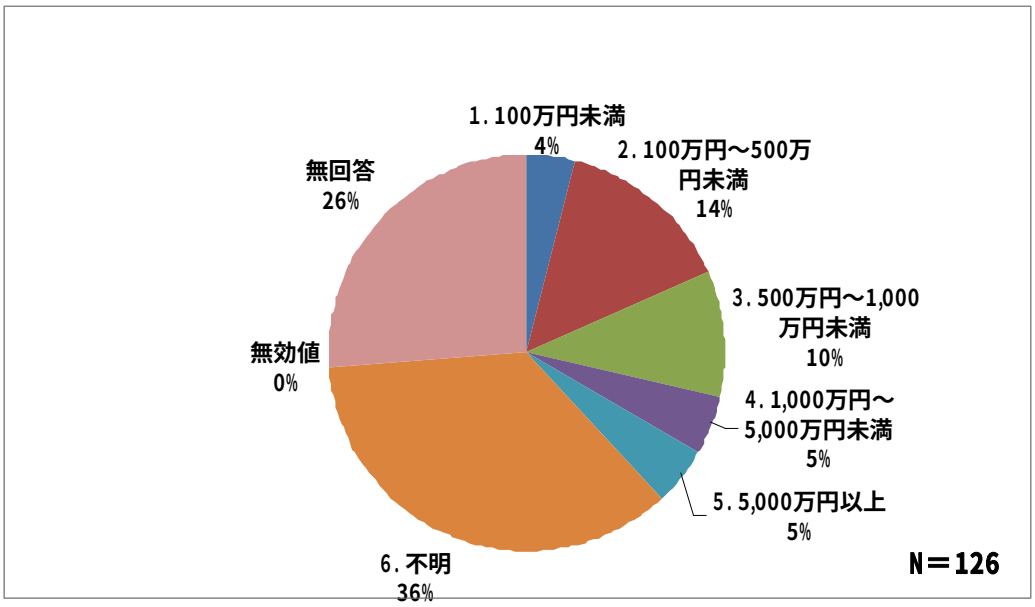


図 2.22　　SAM 導入時の予算

⑧SAM の対象組織（社内組織）

SAM を「１.実施している、２.構築中、３.検討中」のいずれかの回答者に対して質問したところ「全社」が６割以上という結果となった。

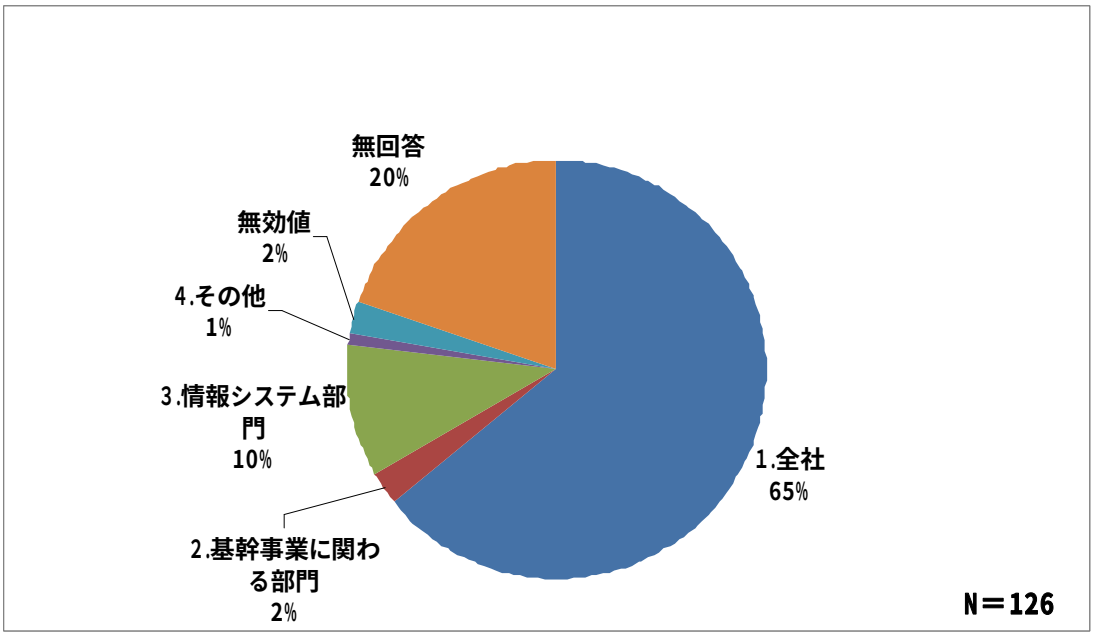


図 2.23　　SAM の対象組織（社内組織）

⑨SAM の推進組織（社内組織）

SAM を「１.実施している、２.構築中、３.検討中」のいずれかの回答者に対して質問したところ「情報システム部門」が５割以上という結果となった。

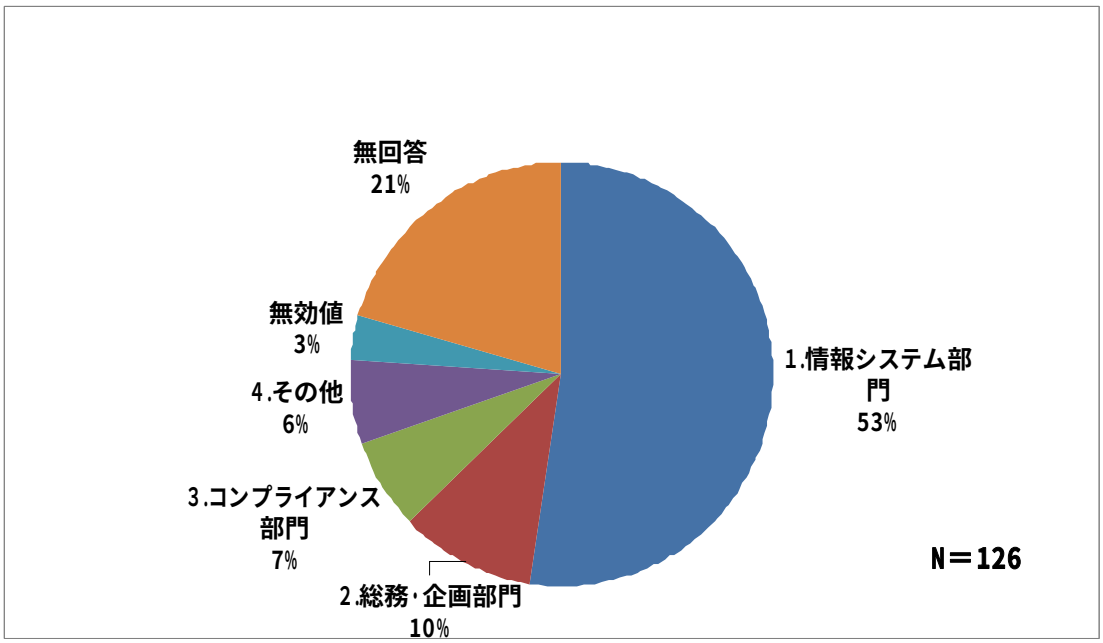


図 2.24　　SAM の推進組織（社内組織）

その他：情報セキュリティ管理、監査部内および各事業部内のＳＡＭ担当者　等

⑩SAM を導入した(導入する)目的

SAM を「１.実施している、２.構築中、３.検討中」のいずれかの回答者に対して質問したところ「コンプライアンス」が最も多かった。

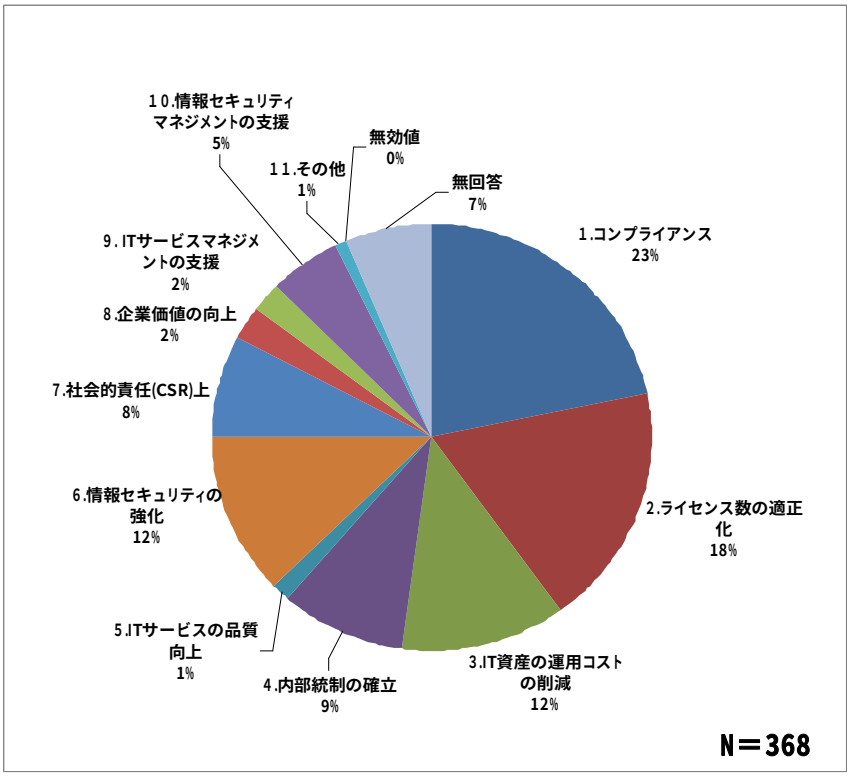


図 2.25　　SAM を導入した(導入する)目的

⑪SAM と ISMS、ITSMS、ITIL の関連

「ISMS 認証を取得している」が 32%で最も多かった。

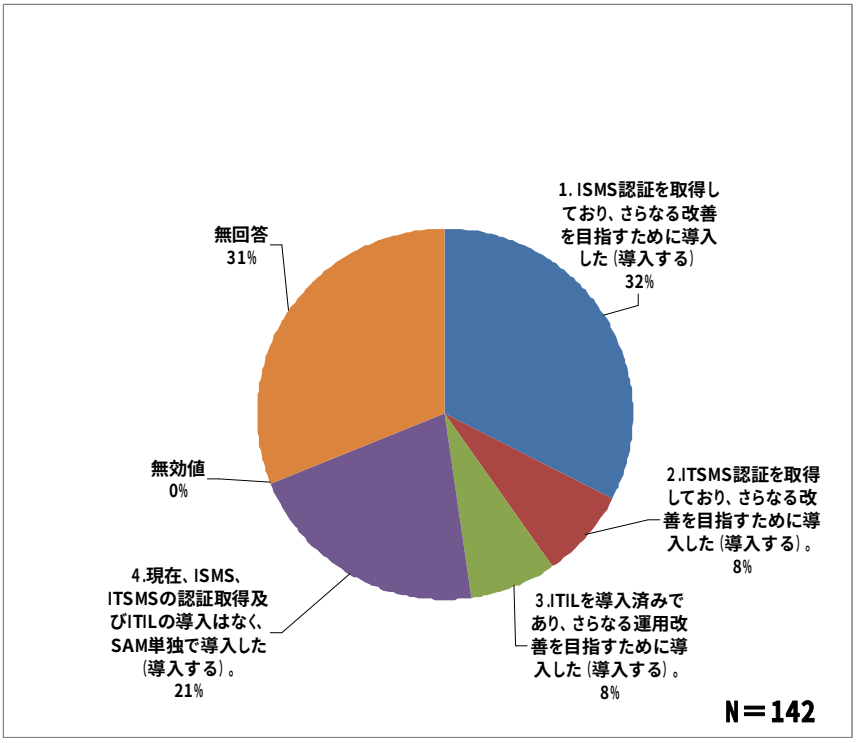


図 2.26　　SAM と ISMS、ITSMS、ITIL の関連

⑫SAM を導入するにあたり参考にした(する予定の)ガイドライン

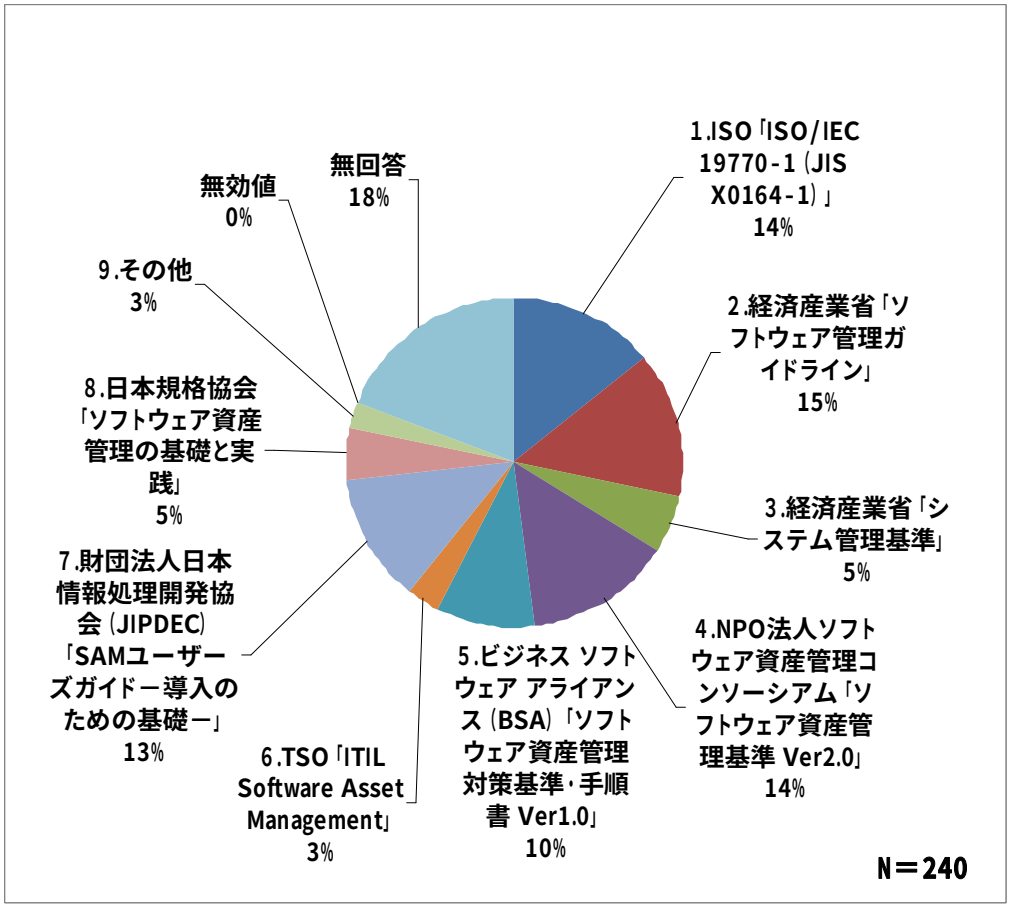


図 2.27　　SAM を導入するにあたり参考にした(する予定の)ガイドライン

⑬SAM の内部監査の実施

SAM を「１.実施している」を選択された方に質問したところ、4 割の企業・組織が内部監査を実施しているという結果になった。

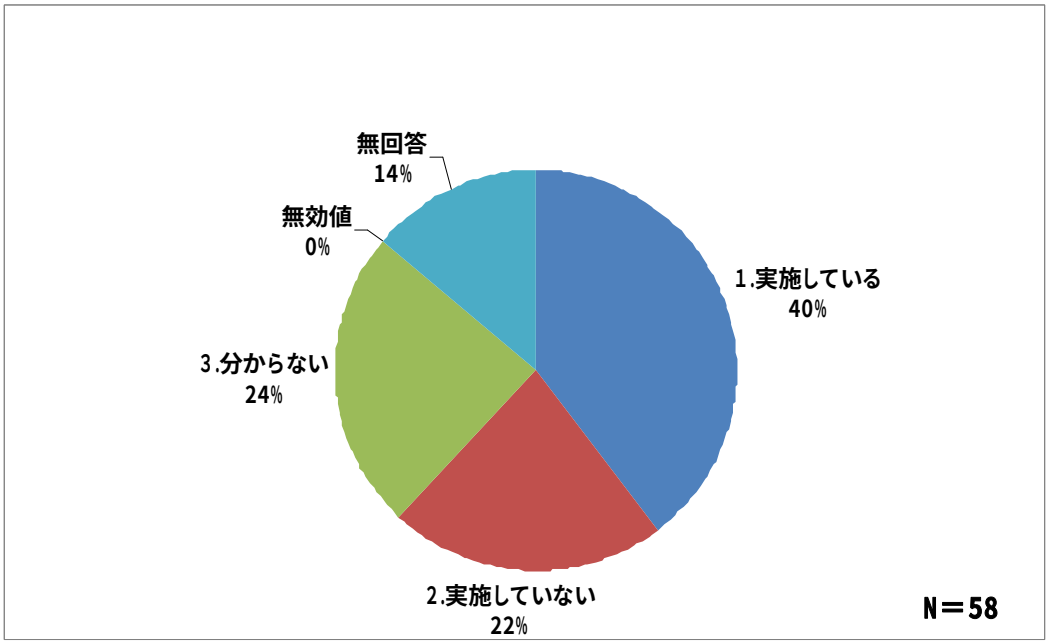


図 2.28　　SAM の内部監査の実施

⑭SAM の内部監査の実施部門（内部監査を実施している組織）

57%と半数以上で「監査部門」が内部監査を実施している。

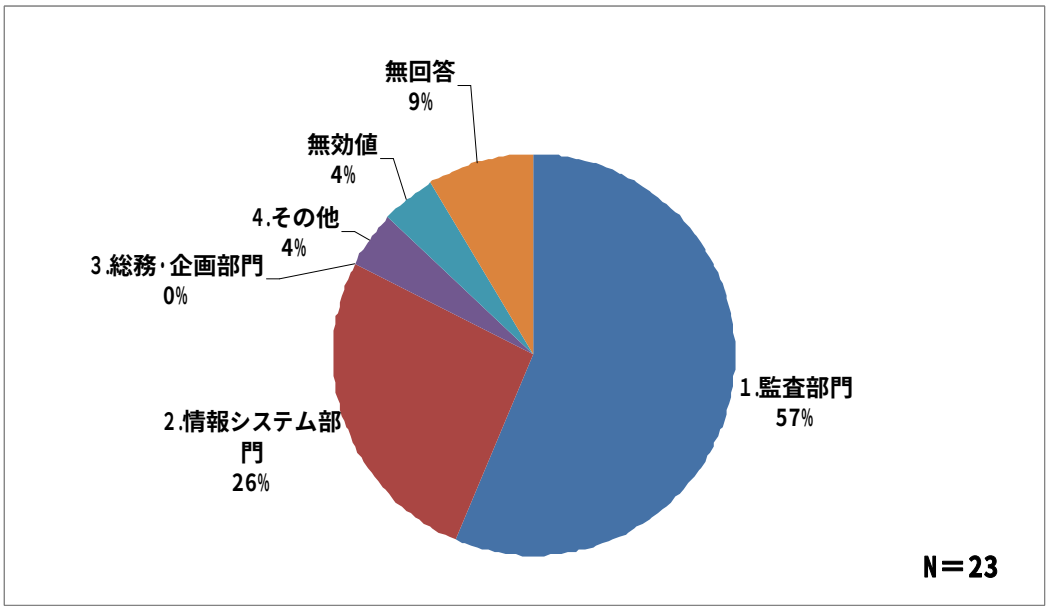


図 2.29　　SAM の内部監査の実施部門

⑮SAM の外部監査

「受けている」の 5%に対して、「受けていない」が 31%となっており、大きく開きがあった。

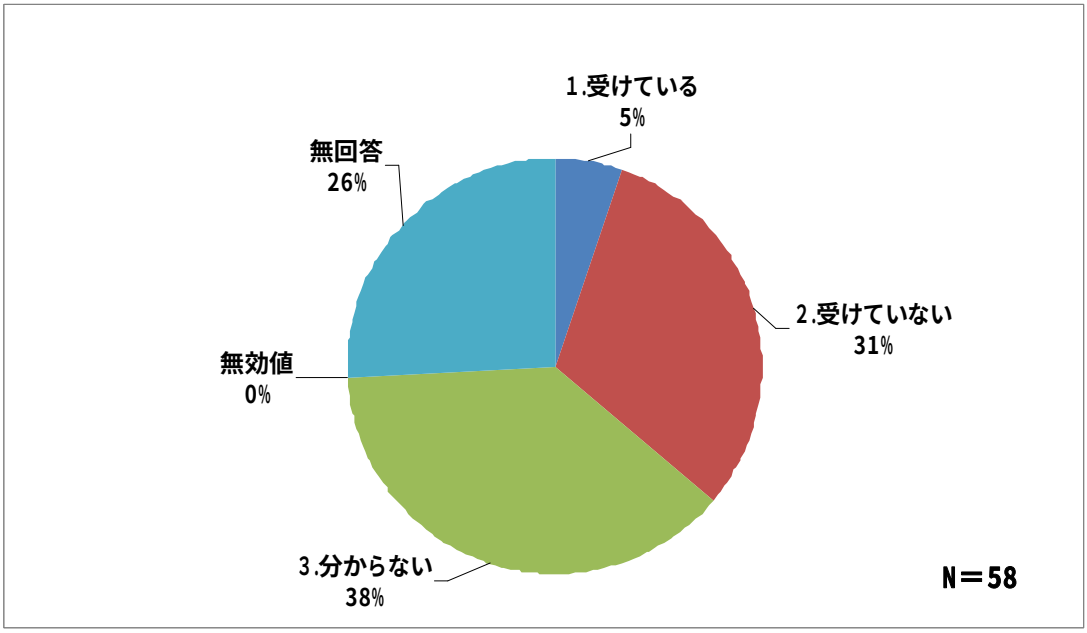


図 2.30　　SAM の外部監査の実施

受けていない理由：BSA の簡易監査のみ、現在 SAM 推進中のため SAM の内容がまだよくわからない　　等

⑯SAM を導入するにあたり障害となったもの

「他部門・現場の協力不足」が 16%で最も多く、「SAM そのものの基本的情報不足」が 15%、「人材不足」が 13%と続いている。

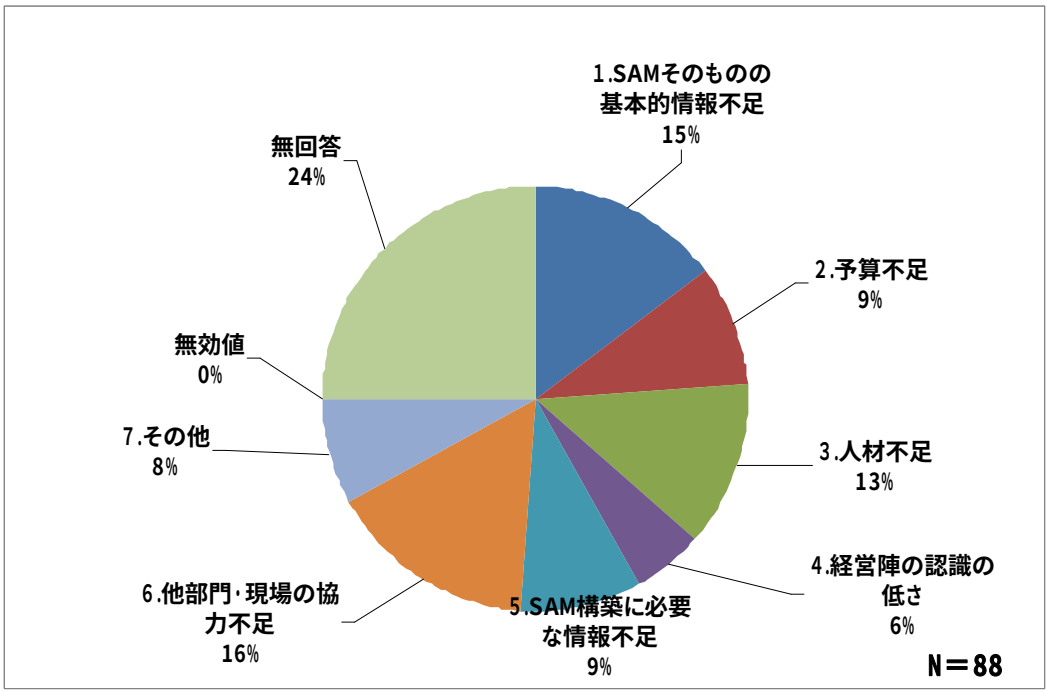


図 2.31　　SAM 導入時の障害

その他：複雑な環境となって来ている、規模の大きさ、多さ　等

⑰SAM 実施後の課題

最も多かったのが「人材がいない」で 14%、次に「必要な情報不足」が 10%と続いている。

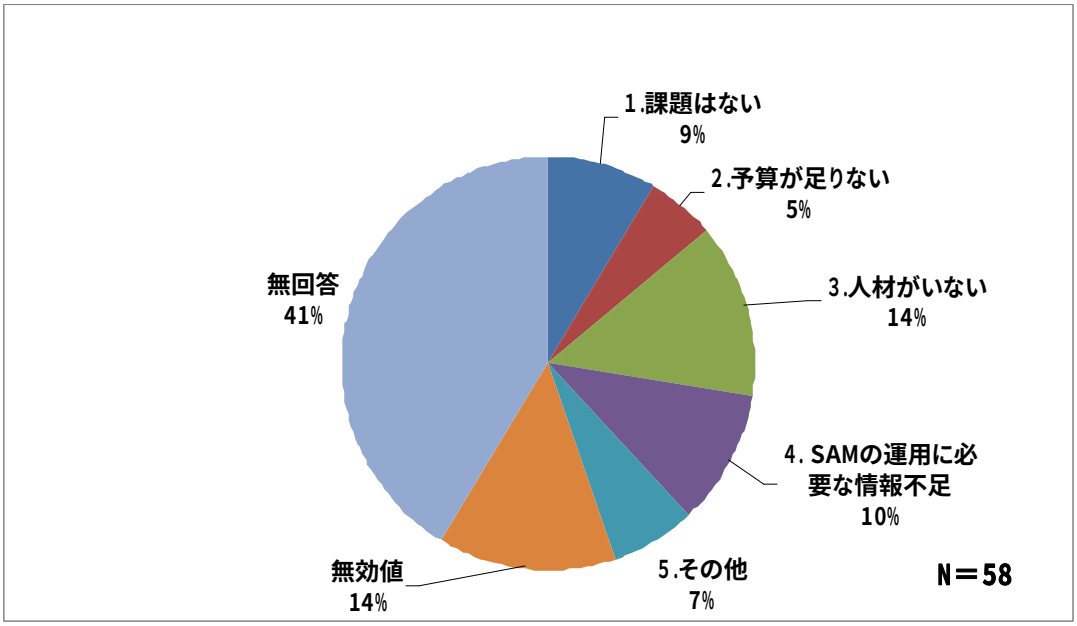


図 2.32　　SAM 実施後の課題

その他：SI ベンダーでもユーザー資産などが流入し、管理がむずかしい。　等

⑱SAM を導入して良かった点は何ですか。

基本的インベントリが収集できるようになった
余剰ソフトウェアライセンスの有効活用→ITコストの適正化、従業員のモラル向上。
業務に必要なソフトウェアのみを導入できるようになった。 部門担当者の好みによる不必要な導入がなくなった。
コンプライアンス、コストの低減
software 資産の把握は今後必須
IT資産の運用コストを削減できた
管理コストが削減できた。管理部内の対応速度が上がった。
確一的に情報を把握できるようになった。
余剰ライセンスの有効活用

⑲SAM 導入を今後どのようにしたいと思いますか。

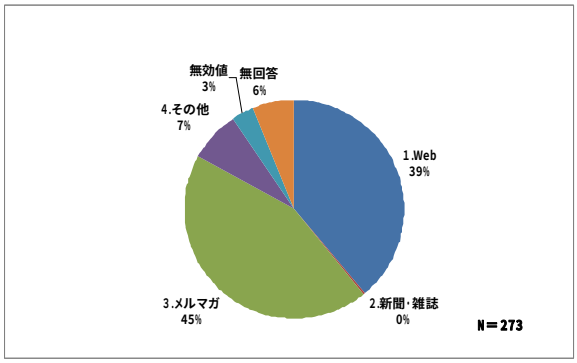
管理の対象がせまい範囲であることと、棚々まで管理できていない。今後徐々に整備、改善していく。
実運をしっかりと確立していきたい
ＳＡＭＡＣ認定レベルまでの成熟度向上
正直に言えばMは行っていてもＭＳには至っていない。 漏れや対象外がどれだけあるか、精度を把握する仕組みを考えたい。
情報収集の自動化

(5) 本シンポジウムについて

①本日の情報セキュリティ総合的普及啓発シンポジウムを知った媒体

１日目が「メルマガ」（45%）、２日目が「Web」（32%）と最も多く、ほとんどの参加者は電子媒体で知ったこととなる。

１日目（1/27）



２日目（1/28）

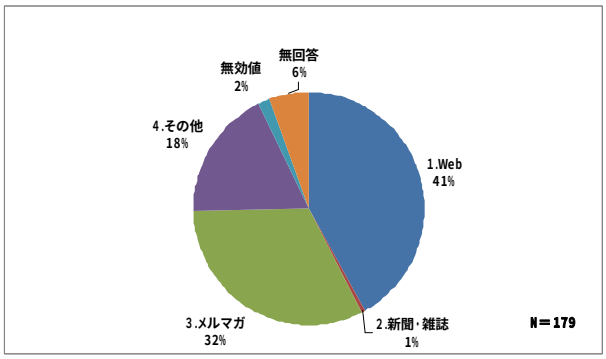


図 2.33　　シンポジウムを知った媒体

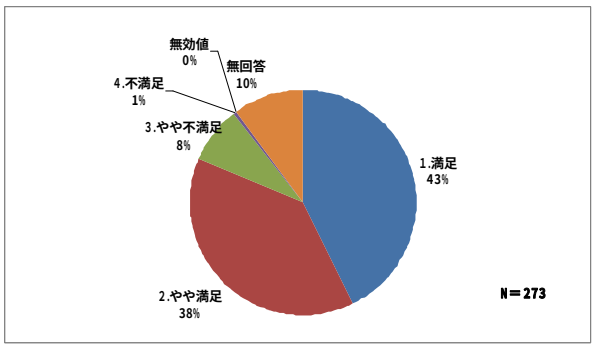
その他の例：職場の上司、社内掲示、会員案内、関係者からの通知　等（１日目）
ソフトウェアベンダーから紹介、協力会社からの案内　等（２日目）

②本日の情報セキュリティ総合的普及啓発シンポジウムの総合評価

・講演内容

１日目、２日目とも「満足」、「やや満足」を合わせると８割を超えており、ほとんどの参加者が満足だったと言える。

１日目（1/27）　　２日目（1/28）



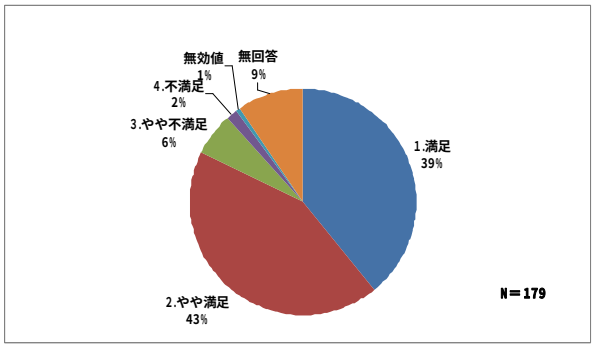


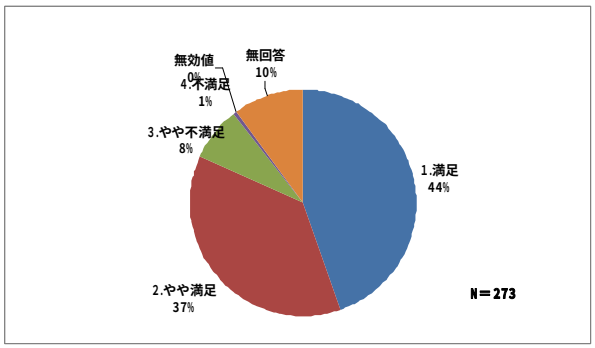
図 2.34　情報セキュリティ総合的普及啓発シンポジウムの総合評価（講演内容）

③本日の情報セキュリティ総合的普及啓発シンポジウムの総合評価

・講演時間

１日目、２日目とも「満足」、「やや満足」を合わせるとこちらも８割を超えている。

１日目（1/27）　　２日目（1/28）



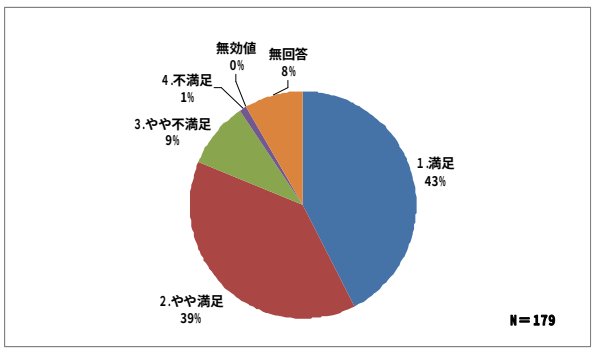


図 2.35　情報セキュリティ総合的普及啓発シンポジウムの総合評価（講演時間）

④本日の情報セキュリティ総合的普及啓発シンポジウムの総合評価

・講演会場

１日目（1/27）　　２日目（1/28）

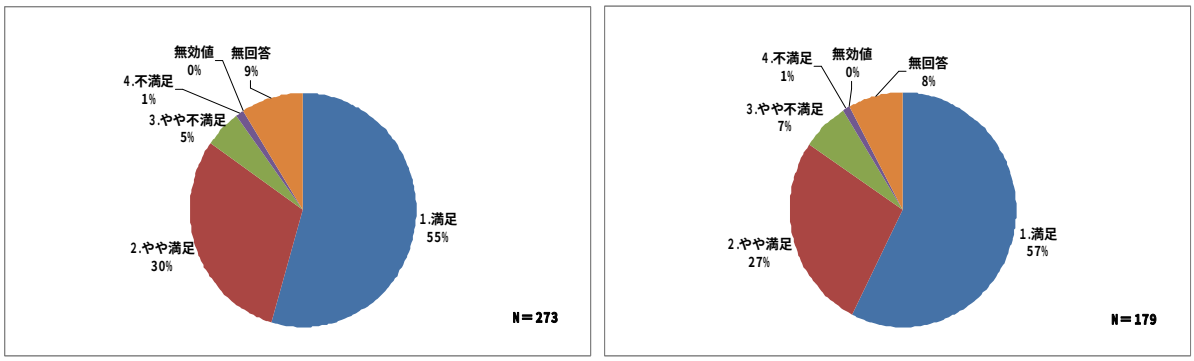


図 2.36　情報セキュリティ総合的普及啓発シンポジウムの総合評価（講演会場）

⑤今後も情報セキュリティ総合的普及啓発シンポジウムの開催を期待しますか。

１日目、２日目とも「はい」が９割を超えており、今後も開催を期待していることがわかる。

１日目（1/27）　　２日目（1/28）

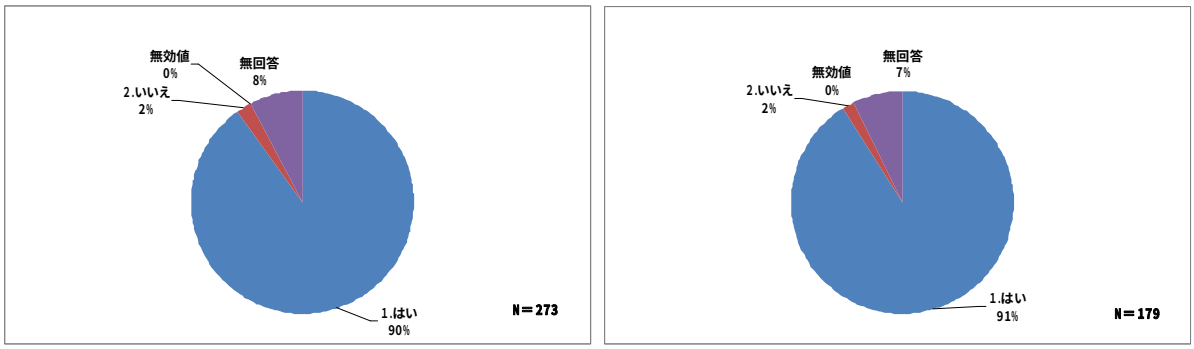


図 2.37　今後の情報セキュリティ総合的普及啓発シンポジウムへの期待

⑥今後、取り上げて欲しいソフトウェア資産管理に関するテーマやその他ご意見

１日目（1/27）

・IT 人材育成、セキュリティの海外事情
スマートフォン関係
ISO50001 と連携した情報セキュリティ分野
今回の会場は便利だが、メモを取る上で机がないのがやや不便であった。
BCMS の構築プロセスについて
リスク分析とリスクの定量化手法及び具体例の紹介
社員に対する情報セキュリティ意識の向上に向けた対策
ISO/IEC27000 シリーズの最新情報、国の取り組みの最新情報
講演者の方は、時間内に話せる内容で願いたいと感じました。 最後がかけ足になるので、消化不良の感がします。
ISMS,PMS,ISO20000 も、QMS の連携（効率的な運用をどうすればできるか） ※プレゼン資料の字が小さく見にくいページが多かったので、次回より考慮願います （冊子見ればよいのですが…）
個人情報管理
情報セキュリティガバナンス
デバイスなどのストレージ管理、Xen などの仮想環境
業務のグローバル化に対応した ISMS の対応
①クラウドでのセキュリティリスクと対策。個人情報の扱い方など ②スマートフォン活用でのセキュリティリスクと対策
ＢＣＰ
情報ろうえい（内部から）対策
セキュリティと利便性のリスクアセスメント事例
いつも時事に即したセミナーを開催され、参考にさせて頂いています。 クラウド（＆スマートフォン等端末）関連の動向については継続して情報発信いただきたいです
（グローバル対応に関する課題…）
ＩＳＭＳとＰマークの統合運用
ＩＳＭＳ、個人情報運用時の事例…良い点、悪い点、困っている点など身近な事物についてお願いしたい。
ＩＳＭＳについての不満点とその改善について ・不満はありませんか。ＩＳＭＳの要求事項についても、制度（運用）についても。 ・どの位の数の事業者がＩＳＭＳを構築するのが理想なのですか。
ＳＡＭ
・スマートフォン等のモバイルセキュリティ ・スマートシティ/スマートグリッドにおけるセキュリティ
ＩＤ共通化の動向とセキュリティ
アンドロイド、シンクライアント等…

パネルディスカッションはとても参考になった。 司会者がパネラーの特質をひき出していた。
情報セキュリティガバナンス
クラウド時代におけるデータセンター運営のあり方 （設備、機能、顧客とのとり決め要件の境界、監査対応/体制、開示の限界…等）
クラウドサービスの第三者監査、各サービスの連携と標準化の動向
今回のセミナーに対して2～3月後に同じタイトルで、変化を教えて欲しい。
業務に係りそうな法的な規制等のテーマ 「輸出貿易禁止令」による暗号化技術の輸出について。
もう少しスライドの情報量や話す内容をシンプルにしていただけると良いと思いました。 ポイントが今一つつかみにくい感じがしました。
・海外動向もっと詳しく、特にインシデント事例やユーザ評価など ・コンプライアンス、法令対応問題は面白かった。もっと実際の運用の観点でもっと教えて欲しい。
・サービス提供者の事業継続性 ・法律について、もう少し具体例を混えながら
・今後もクラウドに関する取り込み方や方向性については情報がほしい。 クラウドの展開とセキュリティでの考え方やおりあいの付け方など。
・スマートフォン ・内部犯行への対策が興味あります。
公開カギの具体的活用分野、とくに、サービス業と金融系
IPv6
海外、特に新興国における情報セキュリティ
インシデント事例の詳設
国家、政府、地方自治体の情報 Security 情報 Security 法整備
クラウド、ＳＮＳ
大阪方面でのセミナー開催をお願いします。

２日目（1/28）

日本企業の海外グループ会社におけるソフトウェア資産管理の成功例
クラウドにおける具体的なＳＡＭの構築
事例多めにしてほしい。
ＩＳＭＳとＰマークの統合について
幅広い分野の導入事例紹介
ソフトウェア資産管理の実例紹介、使用許諾事件の読み方（ポイント）解説
ライセンス形態の規格の制定

取り上げて欲しいテーマ ・今回の宮崎県のような生々しい経験に基づいた報告 避けて欲しいテーマ ・形だけの話。
ISO関連実装事例。
導入事例の中で、失敗談、成功談等
クラウド環境でのSAMの具体的な手法について取り上げて欲しい（オンプレミスとの違い）
認証・認定制度について。
世界でのSAMの状況
ソフトウェア資産管理の導入する際の注意点やなぜ必要か、未導入の際のリスク等、基本的な部分先知したい。
事前申込みにて満員の事だったが、来場者が少なく感じた。 他に出席したかった方もいると思うので、もう少し方法を考えてほしい（課金1社○名 etc） 内容としてはとても参考になった。（トレンド）
都合で全て聴講できなかったので聴講内容については評価していません
SAMの必須性（便益）、メリットの周知
保守契約との関連と資産管理との連動した管理
H/Wを含めた考え方
導入事例を具体的な帳表等まじえて時間を取って説明頂くともっと普及啓発につながるのではと思います。
クラウドに関するテーマを取り上げた講演もありましたが、内容としてはクラウド環境下におけるSAMをどのようにすべきか不明だった為、クラウド環境下のSAMについて具体的な内容をテーマにして頂きたい。
二日間参加させていただきました。特に本日の内容は参考になりました。 今後も継続開催により新しい情報提供を希望します。 ※普及活動という点ではもう少し初級者向けにターゲットを絞った内容があってもよいと思いました。
クラウド時代に向けてソフトベンダ自身が"ライセンスアクティベーション"などの技術を使って、クラウド自身で機械的に契約内容と照合して、速度をとるようなテーマを取上げてほしい。

2.2.3 アンケート調査票

情報セキュリティ総合的普及啓発シンポジウムアンケート
1日目（2011/1/27） 「クラウド時代における政策及び情報セキュリティの側面」

本日は、お忙しい中、「情報セキュリティ総合的普及啓発シンポジウム」にご参加いただきありがとうございます。お手数ですが、下記のアンケートにご協力をお願いします。なお、ご回答は、該当番号に○印をお付けいただくか、もしくは記入欄にご記入ください。

業種：□情報処理 □サービス □製造 □建設 □機械製造 □公共行政 □自治体 □教育関係 □印刷 □医療 □通信 □卸売･小売 □金融 □コンサルティング □その他（ ） 複数業種に関連する場合は、主力業種1つのみレ印をつけて下さい。
従業員数：□100人未満 □100人～300人未満 □300人～1,000人未満 □1,000人～5,000人未満 □5,000人以上
資本金：□1,000万円未満 □1,000万円～1億円 □1億円～10億円 □10億円～50億円 □50億円以上
参加日：□両日（1月27日～28日） □一日目のみ（1月27日） 1つのみレ印をつけて下さい。

■質問1．あなたの職種、役職等ついてお聞かせ下さい。

質問1-1 職種

1.情報システム	2.総務・人事	3.経理・財務	4.生産・業務	5.経営・企画
6.営業	7.ファシリティ管理	8.顧客サービス	9.その他( )	

質問1-2 役職

1.役員	2.管理職	3.専門職	4.一般職	5.その他

質問1-3 情報セキュリティに対する立場

1.ベンダー側	2.コンサルティング側	3.推進・事務組織（責任者）側
4.エンドユーザー側	5.その他（ ）	

質問1-4 本シンポジウムの参加目的

1.情報収集	2.教育・研修	3.その他（ ）

■質問2．クラウド・コンピューティングについてお聞かせ下さい。

質問2-1 御社のクラウドの利用状況についてお聞かせください。

1．利用している	2.利用を検討中	3．利用の計画はない	4.分からない

質問2-2 質問2-1で「1.利用している、2.利用を検討中」のいずれかを選択された方に伺います。

① 利用したい（検討中の）クラウドサービスについてお聞かせください。(複数回答可)

1.グループウェア	2.電子メール	3.アプリケーション	4.顧客管理・営業支援
5.データベース	6.ストレージ	7．ホームページ	
8.その他（ ）			

② クラウドを利用する際の利点についてお聞かせください。(複数回答可)

1.運用コストの削減	2.システム規模を柔軟に変更可能	3.IT資産の保有の削減
4.短期間での導入	5.社外からでも利用が可能	6.システム運用要員の削減
7.いつでも利用停止可能	8.その他（ ）	

質問2-3　クラウドを利用する上での懸念事項はありますか。(複数回答可)

1.サービス障害	2.サービスのセキュリティレベル	3.データの二次利用
4.導入・運用のサポート体制	5.障害時のデータ復旧	6.サービス業者の倒産
7.法律上の問題	8.その他（　　）	

質問2-4　クラウドと情報セキュリティについてお聞かせ下さい。

①　クラウドを利用するにあたって、情報セキュリティ管理体制上、留意・考慮している点はどれですか。(複数回答可)

1.データ所有者・場所の把握	2.サービス障害時の対応体制	3.SLAの締結
4.ISMSの取得の有無	5.サービス提供者の事業継続性	6．外部委託先の管理
7.その他（　　）		

質問2-5　クラウドとITサービスマネジメントについてお聞かせ下さい。

①　クラウドサービスを提供するにあたって、留意・考慮している点はどれですか。(複数回答可)

1.障害時の対応体制の充実	2.サービスの可用性	3.法的な規制の範囲
4.ITSMSの取得	5.その他（　　）	

質問2-6　クラウドサービスを利用する分野についてお聞かせ下さい。

質問2-7　クラウドサービス提供事業者の選択基準として、考慮している点はどれですか。(複数回答可)

1.価格	2.機能	3.セキュリティ
4.信頼	5.その他（　　）	

■質問3．本シンポジウムについてお聞かせ下さい。

質問3-1　本日の情報セキュリティ総合的普及啓発シンポジウムは、どのような媒体で知りましたか

1．Web	2．新聞・雑誌	3．メルマガ	4．その他（　　）

質問3-2　本日の情報セキュリティ総合的普及啓発シンポジウムの総合評価はどれですか。

①講演内容	1．満足	2．やや満足	3．やや不満足	4．不満足
②講演時間	1．満足	2．やや満足	3．やや不満足	4．不満足
③講演会場	1．満足	2．やや満足	3．やや不満足	4．不満足

質問3-3　今後も情報セキュリティ総合的普及啓発シンポジウムの開催を期待しますか。

1．はい	2．いいえ

質問3-4　今後、取り上げて欲しい情報セキュリティに関するテーマやその他ご意見をお聞かせ下さい。

御協力いただきありがとうございました。皆様からいただいたコメントやご要望につきましては、今後の検討材料のひとつとして活用させていただきます。

以上

KEIRIN

この事業は、競輪の補助金を受けて実施するものです。
http://ringring-keirin.jp/

情報セキュリティ総合的普及啓発シンポジウムアンケート
2日目（2011/1/28）　「クラウド時代におけるソフトウェア資産管理の側面」

本日は、お忙しい中、「情報セキュリティ総合的普及啓発シンポジウム」にご参加いただきありがとうございます。お手数ですが、下記のアンケートにご協力をお願いします。なお、ご回答は、該当番号に○印をお付けいただくか、もしくは記入欄にご記入ください。

業種：□情報処理　□サービス　□製造　□建設　□機械製造　□公共行政　□自治体　□教育関係　□印刷　□医療 □通信　□卸売･小売　□金融　□コンサルティング　□その他（　　） 複数業種に関連する場合は、主力業種1つのみレ印をつけて下さい。
従業員数：□100人未満　□100人～300人未満　□300人～1,000人未満　□1,000人～5,000人未満　□5,000人以上
資本金：□1,000万円未満　□1,000万円～1億円　□1億円～10億円　□10億円～50億円　□50億円以上
参加日：□両日（1月27日～28日）　□二日目のみ（1月28日） 1つのみレ印をつけて下さい。

■質問1．あなたの職種、役職等ついてお聞かせ下さい。

質問1-1　職種

1.情報システム	2.総務・人事	3.経理・財務	4.生産・業務	5.経営・企画
6.営業	7.ファシリティ管理	8.顧客サービス	9.その他(　　)	

質問1-2　役職

1.役員	2.管理職	3.専門職	4.一般職	5.その他

質問1-3　情報セキュリティに対する立場

1.ベンダー側	2.コンサルティング側	3.推進・事務組織（責任者）側
4.エンドユーザー側	5.その他（　　）	

質問1-4　本シンポジウムの参加目的

1.情報収集	2.教育・研修	3.その他（　　）

■質問2．ソフトウェア資産管理（SAM）についてお聞かせ下さい。

質問2-1　御社のSAMの実施状況についてお聞かせください。

1．実施している	2．構築中	3．検討中	4．何もしていない	5.分からない

質問2-2　質問2-1で「1.実施している、2.構築中、3.検討中」のいずれかを選択された方に伺います。

<u>なお、「4．何もしていない、5．分からない」を選択された方は、質問3へお進み下さい。</u>

①　SAMの構築にあたって、外部組織のアドバイスや支援を受けましたか。または受ける予定ですか。

1.受けた	2．受ける予定である	3．受ける予定はない	4.わからない

②　①で「1．受けた、2．受ける予定である」のいずれかを選択された方に伺います。どういった外部組織のアドバイスや支援を受けましたか。

1.SAMのコンサルティング会社	2.ツールベンダー	3.ソフトウェアの販売会社
4.ソフトウェアベンダー	5ソフトウェアの権利者団体	6．その他（　　）

③ ①で「1．受けた」を選択された方に伺います。外部組織のアドバイスや支援の内容は、満足のいくものでしたか。

1.満足だった	2.やや不満足だった	3.不満足だった
4.よくわからない	5．その他（　　）	

④ SAM の導入にはどのくらいの期間がかかりましたか。(かける予定ですか)

1.三ヶ月未満	2.三ヶ月～六ヶ月未満	3.六ヶ月～一年未満	4.一年～二年未満	5.二年以上（　　年)

⑤ SAM を導入したきっかけをお聞かせ下さい。(導入予定含む)

1.外部組織等の要請	2.組織内上層部からの要請	3.社内管理担当部門からの要請	4.その他

⑥ SAM の導入にはどのくらいの予算が組まれていますか。(組まれる予定ですか)

1.100 万円未満	2.100 万円～500 万円未満	3.500 万円～1,000 万円未満
4.1,000 万円～5,000 万円未満	5.5,000 万円以上（　　万円)	6．不明

⑦ SAM の対象組織（社内組織）についてお聞かせください。

1.全社	2.基幹事業に関わる部門	3.情報システム部門	4.その他（　　）

⑧ SAM の推進組織（社内組織）についてお聞かせください。

1.情報システム部門	2．総務・企画部門	3.コンプライアンス部門
4．その他（　　）		

⑨ SAM を導入した(導入する)目的についてお聞かせください(複数回答可)

1．コンプライアンス	2．ライセンス数の適正化	3．IT 資産の運用コストの削減
4．内部統制の確立	5．IT サービスの品質向上	6．情報セキュリティの強化
7．社会的責任(CSR)上	8.企業価値の向上	9．ITサービスマネジメントの支援
10．情報セキュリティマネジメントの支援	11．その他（　　）	

⑩ SAM と ISMS、ITSMS、ITIL の関連についてお聞かせください(複数回答可)

1．ISMS 認証を取得しており、さらなる改善を目指すために導入した（導入する)。
2．ITSMS 認証を取得しており、さらなる改善を目指すために導入した（導入する)。
3．ITIL を導入済みであり、さらなる運用改善を目指すために導入した（導入する)。
4．現在、ISMS、ITSMS の認証取得及び ITIL の導入はなく、SAM 単独で導入した（導入する)。

⑪ SAM を導入するにあたり参考にした(する予定の)ガイドラインは何ですか。(複数回答可)

1．ISO「ISO/IEC 19770-1（JIS X0164-1)」	2.経済産業省「ソフトウェア管理ガイドライン」
3．経済産業省「システム管理基準」	4．NPO 法人ソフトウェア資産管理コンソーシアム「ソフトウェア資産管理基準 Ver2.0」
5．ビジネス ソフトウェア アライアンス（BSA)「ソフトウェア資産管理対策基準・手順書 Ver1.0」	6．TSO「ITIL Software Asset Management」
7．財団法人日本情報処理開発協会（JIPDEC)「SAM ユーザーズガイドー導入のための基礎ー」	8．日本規格協会「ソフトウェア資産管理の基礎と実践」
9．その他（　　）	

質問2-3　質問2-1で「1.実施している」を選択された方に伺います。

①　SAM の内部監査を実施していますか。

1.実施している	2.実施していない	3.分からない

②　①で「1．実施している」を選択された方に伺います。SAM の内部監査の実施部門（内部監査を実施している組織）についてお聞かせ下さい。

1.監査部門	2.情報システム部門	3.総務・企画部門
4．その他（　　）		

③　SAM の外部監査を受けていますか。

1.受けている	2.受けていない	3.分からない
理由：	理由：	

④　SAM を導入するにあたり障害となったものは何ですか。(複数回答可)

1.SAM そのものの基本的情報不足	2.予算不足	3.人材不足	4.経営陣の認識の低さ
5.SAM 構築に必要な情報不足	6.他部門・現場の協力不足	7.その他（　　）	

⑤　SAM の実施後に出た課題がありましたらお聞かせ下さい。

1.課題はない	2．予算が足りない	3.人材がいない
4．SAM の運用に必要な情報不足	5．その他（　　）	

⑥　SAM を導入して良かった点は何ですか。

⑦　SAM 導入を今後どのようにしたいと思いますか。

■質問3．本シンポジウムについてお聞かせ下さい。

質問3-1　本日の情報セキュリティ総合的普及啓発シンポジウムは、どのような媒体で知りましたか。

1．Web	2．新聞・雑誌	3．メルマガ	4．その他（　　）

質問3-2　本日の情報セキュリティ総合的普及啓発シンポジウムの総合評価はどれですか。

①講演内容	1．満足	2．やや満足	3．やや不満足	4．不満足
②講演時間	1．満足	2．やや満足	3．やや不満足	4．不満足
③講演会場	1．満足	2．やや満足	3．やや不満足	4．不満足

質問3-3　今後も情報セキュリティ総合的普及啓発シンポジウムの開催を期待しますか。

1．はい	2．いいえ

質問3-4　今後、取り上げて欲しいソフトウェア資産管理に関するテーマやその他ご意見をお聞かせ下さい。

御協力いただきありがとうございました。皆様からいただいたコメントやご要望につきましては、今後の検討材料のひとつとして活用させていただきます。

以上

この事業は、競輪の補助金を受けて実施するものです。
http://ringring-keirin.jp/

3. クラウド時代における政策及び情報セキュリティの側面

3.1 クラウドサービスにおける情報セキュリティ管理とセキュリティチェック

3.1.1 クラウドサービスによるシステム環境の変化

ネットワークの高速化や安全確保、そして高機能の CPU やメモリ、ハードディスクの低価格化にともなってインターネットサービスが普及し、アプリケーションだけではなく、システム環境そのものまでがサービスとして提供されるようになった。

これらをクラウドサービスといい、提供されるコンピュータリソースによって、SaaS、PaaS、IaaS というサービスモデルが定義されている。また、これらのサービスを提供する環境をクラウドコンピューティングといい、仮想化や分散処理といった技術を活用して、低コストで拡張性の高いシステム環境を構築できるようになった。

また、インターネットを含めた広範囲なネットワーク上でサービスが提供されることから、クライアント環境も多様化しており、スマートフォンや携帯電話などもシステム環境の一部として考慮する必要が出てきた。公衆無線 LAN や 3G 回線を利用したサービス利用についても、クラウドサービス利用におけるシステム環境の変化ととらえることができるだろう。

3.1.2 クラウドサービスの利用におけるリスク管理

クラウドサービスの利用におけるリスクを考慮する際に注目すべき事項の一つに、クラウドサービスが提供される場所が挙げられる。これをクラウドサービスの運用モデルといい、自らの管理下にあるクラウドサービス環境をプライベートクラウド、管理外にあるクラウドサービス環境をパブリッククラウドという。

プライベートクラウドにおいては、クラウドコンピューティングに活用される技術におけるリスクを主に検討すればよい。運用については、ネットワーク環境の変化、クライアント環境の変化を主としてリスク分析を行えば良いだろう。リスク変化の多くは技術面にあり、これらはその技術やデバイスを提供するメーカーやベンダーと情報交換をすることによって解決ができるのではないかと考えられる。

パブリッククラウドにおいては、技術面において懸念されるリスクについて、クラウドサービスプロバイダーが適切な対応をしているかなど、主に運用面についてリスク分析を行う必要がある。しかし、パブリックにサービスを提供しているプロバイダーにとっては、技術的な情報を開示することが、新たなぜい弱性を生むこととなり、システム環境における情報提供は望まないかもしれない。現状では、システム環境における情報開示ではなく、システムの運用状況における情報開示によって、利用者に対して安全性や安定性の確認を促すことが多いようだ。また、ISMS 認証や情報セキュリティ監査によって、運用における客観性を示しているプロバイダーも多い。

3.1.3 クラウドサービスの利用と情報セキュリティマネジメントシステム

情報セキュリティマネジメントシステム（ISMS）では、運用において様々な情報を必要とする。たとえば、イベントやインシデントの発生における原因究明や対応策の選択において、情報システムや業務プロセスのログを確認し、判断を実施するという手順を構築していることだろう。

しかしながら、クラウドサービスを利用した場合には、これらのログを自由に取得することが難しいという問題が発生する。

IaaS や PaaS など、システム環境に近いサービスを利用している場合には、自らが設定したログを閲覧することが可能だが、ログのサイズによってはこれらをネットワーク経由で取得するために膨大な時間を要することがある。即時の判断が求められる場合に情報を活用できないだけではなく、ログを長期間保存しておくために追加のサービス利用料がかかることもある。

SaaS においては、ログを自由に設定できずに、イベントやインシデントのハンドリングができないという問題が発生する可能性がある。システムに関するログは必要ないとしても、ID 管理が統合化できていない場合にプロセスにおけるトレーサビリティが確保できないという問題もあろう。

ISMS の維持のために、以下の項目について考慮することが望ましい。

・ 情報セキュリティマネジメントに必要なシステム情報

・ これらの情報がサービスとして提供されているか

また、ISMS においては、マネジメントレビューに必要なさまざまな情報のインプットも考慮しなければならない。情報セキュリティ監査や第三者の提供するサービスの管理など、JIS Q 27001 などを参考に ISMS の維持管理とクラウドサービスの利用について検討してほしい。

3.1.4 クラウドサービス利用における情報セキュリティ上のメリットとデメリット

クラウドサービスの利用において、情報セキュリティ上の懸念事項ばかりが注目されているが、メリットも少なくない。これらを明確にするためには、情報セキュリティの三つの要素についてもう一度見直してみると良い。

情報セキュリティ対策のひとつである「バックアップ」について、クラウドサービス利用のメリット、デメリットを考えてみる。

バックアップの目的は大きく分けて、以下の二つだろう。

① 情報システムの可用性確保

② 情報システムで利用される情報の完全性確保

可用性の確保という面では、クラウドサービスの利用はメリットと考えられる。自らの環境でシステムを構築する場合、システムにかかる費用の償却期間などを考慮して、数年先までのシステム関連費用を確保しておく必要があった。また、環境を維持するために保

守費用などを別途検討する必要があり、コストだけではなく、システム導入までの計画において多くの時間を要していた。

クラウドサービスの利用によって、システムの可用性について利用者が考慮すべき事項が減少し、システムの可用性確保に関する費用や計画にかかる時間を短縮することができる。トラブルが発生した場合においても、対応をサービスプロバイダが実施するために、予算外の対応費用などを計上する必要がないというのも大きなメリットとなるだろう。
また、クライアント上にデータをおかないことで、ウイルススキャンなどにかかる時間も大幅に短縮される。クライアント上のデータの多くがオフィスソフトで作成したデータやメールでやり取りするデータであることを考えると、これらのサービスをクラウドに移行することで、全体的なシステムの可用性に貢献すると考えられる。

一方で完全性確保についてはデメリットが挙げられる。これは、システムの不備によってデータが滅失する可能性があるということではない。利用者が誤ってデータを書き換えてしまったり、削除してしまった場合に復旧することができるかどうかという点で、自由度が損なわれる可能性がある。

クラウドサービス上に保管しているデータをローカルにバックアップするには、ネットワーク経由で行わなければならない。ネットワークの速度がいくら高速になったからとはいえ、データのバックアップをリアルタイムに行うには十分ではないだろう。
クラウドサービス上に保管するデータにおいて、個人情報や機密情報が大きく注目されているが、もう一つの視点としてアクティブなデータかどうかという点についても考慮する必要がある。すでに終了したプロジェクトのデータや、共有管理を行う必要がないデータについては、クラウド上ではなくローカルの書き換え禁止メディア（ライトワンス）に保管しておくことで、クラウドサービス上のデータのバックアップを容易にすることができる。

このように、情報セキュリティの目的を明確にし、可用性、完全性、機密性のどれを高めるために実施するのか、クラウドサービスを利用することで向上する要素と低下する要素を明確にして、情報セキュリティ対策の選択を行ってほしい。

3.1.5 クラウドサービス利用における情報セキュリティ対策の選択

前述したとおり、クラウドサービスの利用において、環境の変化を明確にし、情報セキュリティの 3 要素についてそれぞれ考察することで、情報セキュリティ対策を選択することができる。しかしながら、クラウドサービスは黎明期であり、経験則による対策の選択を行うことが難しい。

このような事態を予測し、経済産業省では「クラウドサービス利用のための情報セキュリティマネジメントガイドライン[1]」を提供している。

ISMS における情報セキュリティ対策の選択に利用される JIS Q 27002 をベースに、クラウドサービス利用における実施策や新たな考慮事項、関連する情報などをまとめている。また、附属書には国内外の団体が言及しているクラウドサービス関連のリスク一覧やクラ

[1] クラウドサービス利用のための情報セキュリティマネジメントガイドライン（案）に対する意見募集について
（http://search.e-gov.go.jp/servlet/Public?CLASSNAME=PCMMSTDETAIL&id=595210034&Mode=0）

ウドサービスにおけるリスクアセスメントの考え方、ツールなどが提供されている。

国内でクラウドサービスが提供され始めて間もない現在は、経験則による対策を実施することが難しい。多くの情報を入手して、自らの環境と照らし合わせることで、よりよい情報セキュリティ対策を実施するとともに、クラウドサービスを有効活用していただきたい。

独立行政法人 情報処理推進機構 セキュリティセンター（IPA/ISEC）では、ENISA（European Network and Information Security Agency：欧州 ネットワーク情報セキュリティ庁）が作成したクラウドセキュリティに関する文書を翻訳して提供している（http://www.ipa.go.jp/security/publications/enisa/）。こちらもぜひ参考にしていただきたい。

3.2 クラウドのリスクとセキュリティにおける法律面での留意点

3.2.1 クラウドコンピューティングについて法的側面からの検討作業が必要な理由

従来において、ユーザー企業は、自前の情報処理システムを構築・運用することが通常であった。データセンターを利用する場合でも、ユーザー企業との専用線接続が一般的であり、このモデルでは、選択すべきデータセンターは、通信費用との関係で、必然的に近隣の国内に所在するものとならざるをえなかった。

これに対し､クラウドではインターネット回線を用いることが一般的である｡このため、通信費用を考慮しなくてもよいから、必ずしも国内である必要はない。それゆえ、国外事業者の日本国内市場への参入が容易となるので、サービスやデータをめぐって国際的な問題が生じる。これを「データの越境」と呼ぶことができる。

次に、全世界に広がったインターネット上に、無数のサーバ群が接続され、しかも仮想化されていることから、どこに所在する、どのようなサーバ群からサービスの提供を受けているのか、ユーザー企業側が把握困難になるケースすら存在する。これを「データの所在の不明確性」と呼ぶことができる。

これらの点が、従来における自前の情報処理システムの利用、そしてデータセンターの利用と比べて、クラウドを、改めて法律的に分析すべき理由となる[2]。

3.2.2 クラウド提供事業者とユーザー企業間の法律関係

自前の情報処理システムをベンダに依頼して構築してもらう場合と異なり、クラウドコンピューティングでは、具体的なハードやソフトが完成・納入されることなく、提供されたコンピュータリソースを利用しうるだけである。したがって、請負契約ではなく、サービス提供契約とでもいうべきものとなる。それに加えて、個々のクラウドごとにサービスは多様であるから、その内容は基本的に契約内容のみによって決定される。しかも、一般にクラウドコンピューティングは多数のユーザー企業を相手に提供されるものであるから、ユーザー企業としては、クラウド提供事業者から提示された契約約款を受け入れて契約を締結するかしないか、二者択一関係である場合が多い。

なお、契約内容については、提供するサービスの水準を示した SLA（Service Level Agreement）と呼ばれる契約で、別途、サービス内容の詳細が定められることが多い。しかし、これはサービス内容の詳細を定めたものであるから、契約約款の一部であるとみてよい。

ところで、個々のクラウドの内容如何では、さらに特定のユーザー企業に最適化するためのカスタマイズを要する場合がある。パラメータの設定だけで足りる場合はともかく、そのために専用のソフトウェアを構築することを依頼する場合には、当該構築部分は請負契約となろう。クラウドの利点として、迅速なリリースやスケーラビリティと並んで低価格性が指摘されることが多いが、いくらサービス提供費用が安価でも、カスタマイズ費用が高額になれば、利点が帳消しになるので、カスタマイズの要否と費用について事前確認

[2]本稿は、岡村久道「クラウドコンピューティングと法律」情報通信ジャーナル 2009 年 12 月号をベースにした講演原稿に、加筆修正を加えたものである。詳細は、この論考を参照されたい。

が重要となる。
　以上のように、サービス提供と、カスタマイズのためのソフトウェア構築とは、分けて考える必要がある。

3.2.3 裁判管轄、準拠法と法令の執行

　クラウドに関連する法律紛争は、どこの国の裁判所で、どこの国の法律を適用して裁かれるか。一般にサービス提供契約の中に、合意裁判管轄と、準拠法の指定を定めた規定が置かれることが多く、クラウド提供事業者とユーザー企業間の紛争は、基本的に、この規定内容に従うことになる。
　といっても、外国の裁判所で、外国法に従って裁判を遂行することは、ユーザー企業にとって負担が重い。そのため、これらの条項について、事前に関係箇所を確認し、不都合である場合には、変更を求めるか、それが無理なら他のクラウドを選択することが考えられる。
　これらの契約約款は両当事者を拘束するが、それ以外の第三者との関係では拘束力がない。第三者との関係では、国際民事訴訟法によって裁判管轄が決せられ、それによって法定地となった国が制定する国際私法によって、どこの国の法律によって裁かれるか、選択されるという仕組みになっている。
　以上は私法関係である。これに対し、刑法のような公法関係については、一般に属地主義の原則が採用されている。これは、その国の領土内に限って公法が及ぶという原則である。この点も当事者間の提供契約では左右できない。
　この原則には例外がある。例えば、我が国の刑法の中には国外で行われた行為も処罰の対象にする規定がある。とはいっても、日本の領土内でなければ、犯人を逮捕することができず、捜索差押を行うこともできない。このように、法令の執行はその国の主権が届く範囲に限られる。例えば、A 国に設置されたクラウド用データセンターを捜索差押できるのは、A 国の捜査機関であって、我が国のそれではない。データセンター所在地国等が変更されるたびに、どこの国の公法がクラウドに適用されるかについても変化する。諸外国の中には、犯罪捜査等のために、極めて緩やかな要件で捜査機関に通信傍受を認める国もあるから、それによって営業秘密が漏示しないよう、注意が必要である。

3.2.4 契約の終了－ポータビリティ等の問題

　ユーザーが、すでに契約しているサービスから、別のクラウドベンダが提供する新サービスへと乗り換えようとする場合、旧サービス提供契約を解約して、データを新サービスに移行する必要がある。ところが、旧サービスのデータ形式が独自、もしくはデータの書き出しが困難な場合には、事実上、新サービスに移行できなくなる。データ移行に多額の費用を要求される場合もある。ベンダロックイン（ベンダによる顧客の囲い込み）と呼ばれる問題である。
　ユーザー企業がデータのポータビリティを保つためには、契約期間中に入力、集計、加工したデータをユーザーが契約終了時に出力して受領する権利の有無と条件、どのようなデータ形式での出力の可否、その容易性はどうか等の点が、どのように定められているかについて、契約締結時に検討しておく必要がある。併せて、漏えい防止のため、提供事業者側に契約終了時のデータ消去義務が定められているか等についてもチェックが必要とな

る。

3.2.5 契約違反と救済の問題

サービス提供事業者側に責任減免条項が定められているケースが多い。そのため、現実に障害が発生した場合に、ユーザー側で原因を特定することが困難となるおそれがある。クラウドは、ブラックボックス化、多層化された「雲」であるため、責任の切り分けが困難であり、データセンター所在地国すら不明な場合がある。いきおいサービス提供事業者側が示した説明を鵜呑みにするほかない状況へ追いやられ、SLA 上の責任追及が困難になるおそれがある。原因が特定された場合には、クラウド側で発生したインシデントは、たとえ提供事業者が当該サービスの運用の一部を委託しているサードパーティに起因するものであっても、当該サードパーティは提供事業者の履行補助者として、提供事業者の責任となる。

3.2.6 契約によるリスクコントロールの限界

以上に述べた点に加えて、データセンター所在地国のカントリーリスクが生じる場合があるだけでなく、その国の法令によって、当該国の政府に対して通信のデータ内容等の開示義務が課されているような場合には、データの機密性は保たれない。海外のクラウドベンダの中には、サーバ所在地を明らかにしていないケースもあり、そうなれば、どのような国の法令に服するのかを含め、カントリーリスクについてリサーチすらできない。この点、クラウドサービスに用いられるべきデータセンターの所在地を、提供契約によって日本国内に限定することは可能である。これに対し、情報セキュリティを理由に、データセンター所在地を明らかにしようとしない提供事業者もあるが、「中部地方」「福島県内」のような限定であれば、情報セキュリティを害するおそれはないはずである。しかし、データセンター所在地国を明らかにしているケースであっても、サーバ所在地の移転が自由に認められていれば、契約時に想定していなかった国のカントリーリスクに、新たに服することになるリスクがある。これを避けようと思えば、サーバ所在地の移転についても、契約で縛っておく必要がある。

3.2.7 情報セキュリティとコンプライアンス

クラウドは、その構造上、漏えいをはじめ、預けているデータ、サーバのハード・ソフト等の安全性が、主としてサービス提供事業者側のセキュリティレベルに依存せざるを得ない点に特徴がある。それだけに、SLA 等の関連契約条項で、どのように定められているか、導入決定前に検討が必要となる。

法令でデータの取扱いに関する責任を定めているケース（例：個人情報保護法）がある。ユーザー企業がクラウド上に個人データを置く行為は、第三者提供（同法 23 条）に該当する可能性があるが、少なくとも「委託」に該当するので、本人の事前同意は不要であるが、その代わりとして、ユーザー企業はクラウドベンダに対する監督義務を負う（同法 22 条）。クラウドを利用した場合に、どのような管理策を講じれば監督義務を果たしたといえるか、解釈は未確立の状態である。個人データの越境流通として、EU 個人データ保護指令への適合性を要するケースも想定される。

他にも、不正競争防止法上の「営業秘密」として認められるための要件である秘密管理

性との関係でも、同様の問題が生じる。システム監査との関係も不明であり、これらの点が、コンプライアンスとの関係で、解決を急ぐべき課題となっている。

3.2.8 おわりに

クラウドには多様な利点がある半面、法的側面からみた課題は多い。現時点では、少なくともユーザー企業は、こうしたリスクをわきまえた上、クラウドの導入決定に先立ち、契約内容を精査しておき、採否・利用範囲を決定することが重要となる。

他方、サービス提供事業者としては、こうしたリスクを可能な限り解決することによって、市場で競争力を有するクラウドサービスを検討する必要があろう。

3.3 クラウドの浸透と情報セキュリティ管理～技術変革と利用環境変化を踏まえて～

3.3.1 はじめに

ISOGJ（Information Security Operation provider Group Japan:日本セキュリティオペレーション事業者協議会）は、情報セキュリティ運用管理を行う組織が主体となって活動している団体である。活動そのものは JNSA（NPO 日本ネットワークセキュリティ協会）の下で実施している。

現在、セキュリティ運用管理を委託するにも「セキュリティ運用管理」という定義や内容が確立しておらず、必要な技術や関連法令なども明確になっていない状況であり、各社が各個に実施しているのが実態である。我国においては、多くの組織で IT 環境を活用し事業を継続し成長していかなければならず､そういう背景からも情報セキュリティの運用管理もアウトソースへの需要が高まることは必須と考えられる。そのためには、セキュリティ運用管理の各種定義、必要技術、法的な課題などを洗い出し、委託者が安心して適切に委託できるようにするとともに、サービス提供者側のレベル向上を図り、日本の IT 活用の促進と成長を支える目的で活動している。

3.3.2 昨今の発生事件から

昨年の 9 月になるが、印象的な事件として、フロッピーディスクの日付改ざん事件があった。筆者が驚愕したのは、証拠のフロッピーディスクの原本を、個人のパソコンで閲覧などしていたという報道である。調査すべき対象の媒体も紙ばかりではなく、電子データが増えてきていると想像される中で、関係する多くの方々が、ひょっとすると原本を自分のパソコンで閲覧などしているのではないかという、疑問がふつふつと湧いたのである。原本に手を入れられる状態で、大切な証拠に触れているということがどういうことかを含め、考えて頂かなければならない。ある面、人々の活動の場が、リアル空間からサイバー空間に移った結果、生成したドキュメントなどの活動記録の多くもサイバー空間に移っているということを認識しなければならないということだ。逆にいえばハードディスクやメモリーなどのサイバー空間にのみ記録が残る時代がすぐそこに来ているということかもしれないが、それを取り扱う人間が理解できていない状態だと思う。

次に、印象的な事件は、ビデオ流出事件である。この事件では、文章とは異なる性質が映像にはあるということが分かった。文章は、そもそも目的がはっきりしており、作成時に機密レベルを決められる。しかも、データ容量は極めて小さい。一方、映像情報自身に

は目的がない。考えてみると、見た人が意味を感じ利用目的を決めていくのが一般的だ。テレビ番組で見かける監視カメラの記録映像は、ある時にはお笑いに、ある時には衝撃映像としてバラエティー番組に、ある時は犯罪の捜査などに使用されていることからもわかる。つまりは、映像データは機密管理の鉄則である作成時に機密レベルを決めることが極めて難しいのである。しかも大容量であり、記録される機器、記録媒体、編集機材などを考慮すると管理の徹底も極めて難しいことも分かる。これも、急速なデジタル技術の変革に、我々が適応できていないと考えられる。

さらに、機密情報流出事件報道にもびっくりした。何に対してびっくりしたかということは、筆者自身、メディアや世間の方々も、「あってはならぬことが起こった時に、どう反応すれば良いかが分かっていない」ことが判明したことだ。デジタル化した情報の場合、以前のように少しずつ漏れるということは基本的には無い。少量であろうが大量であろうがほとんど変わらないコストと時間で実行できるため、IT 化すればするほど、あってはならないことが起こりえるということを、改めて認識しなければならない。これまた、我々が時代に適応できていない証左の一つであろう。

以上のことから、道具から社会基盤へと急速に変革している IT 環境に、私たちが対応できていないという事実が改めて理解できると思う。

一方、Wikileaks の 25 万件もの米国外交機密文書の暴露という事件も起きている。この中での着目点は三つある。一つ目は、25 万件という数量は、紙だと 1 件 1 ページと換算し積み上げると 25m 以上になると推測される量である。 12 月時点で公開されていたデータから推測すると、1 件当たり平均約 13,000 文字であった。つまり、高々約 3.3GB 程度の情報量であることが推測できる。現在、数千円程度で市販されている 1 ㎠程度の MicroSD カードは 32GB 程度の容量があり、まったく余裕で格納可能な量である。 さらに、ZIP などで圧縮すると 200MB 程度となることも推測され、現在、無数にある無料のオンラインストレージへも余裕で送れる程度のデータ量であるということ。二つ目は、サイトを潰されないために、本家のミラーを行うサイトが募集され千数百程度が動作している。ある面、wikileaks クラウドと呼べるような状態になりつつあること。三つ目は、TOR（The Onion Route:トーア）と呼ばれる匿名プロクシクラウドサービス（千数百のリレーサーバーで構成されている。）を利用して投稿させていると言われていることである。これは、先程の機密情報が TOR を使用されて様々な機関に送付されていたという報道からも、世界中の告発したい人間に対して、簡単に匿名で告発が出来ることを知らしめてしまった点がインパクトとしては見逃せない。

同時に、ソーシャルメディアの浸透は、想像以上に大きな影響を持ちつつある。日本でも、レストランなどの従業員がツイッターで、お客様の情報をつぶやくことで、ちょっとした事件となることが発生している。先程のビデオ流出もソーシャルメディアである Youtube に投稿され、その後の議論もツイッターで主に行われていた。海外では、Facebook やツイッターなどでの情報共有や議論がトリガーになり、独裁政権を覆すだけではなく、同じような国や地域へ連鎖するような事象にまで発展しているという報道もある。ある面、

ソーシャルメディアは企業においても販売促進の目的などで多くの活用され始めている半面、多くの組織では逆に「使用禁止」としていることも多い。今後、私たちのソーシャルメディアリテラシーの向上は、事業継続や成長の観点で極めて重要なテーマとなると予測される。

一方、組織内で発生している事件に目を移すと、一つの傾向がみられる。これは、組織内に侵入する方法と、侵入させる脅威（侵入目的）を分離して考えると分かりやすい。つまり、侵入させる主な手段は、最近あまり変化はしておらず USB メモリ、改ざん Web 閲覧、標的メールの三つである。重要なことは、侵入後の脅威が、通常の一般的なマスに対する脅威だけではなく、「標的型サイバー攻撃」は既に身近で発生しているということが看過できない点である。特に、公共の組織や当該組織に関係した組織などを装ったメールに添付された悪性プログラムを使用し、組織内に侵入、その後、管理者権限を窃取し、さらに深く潜入。多くのパソコンを乗っ取り、必要な情報を盗み出していくような事例が観測されている。米国などで数年前から報道されていることは、遠い国の事ではなく、現実に我々の身近で発生しているということを認識すべきである。

3.3.3 昨今の環境変化

これまで、最近発生している事件を語ってきたが、こういった状況の中で、さらに、大きな変化が発生している。それは、クラウドとスマートフォンである。クラウド自体は多くの方が語っているので割愛するが、筆者はクラウド活用へのトリガーはスマートフォンがカギを握っていると考えている。今回のシンポジウムの中でも口頭で尋ねてみたが、組織でのクラウドやスマートフォンの活用はほとんど図られていない。しかし、個人の活用は急速に進みつつある現実が、確認された。実際、数年前から進歩的な個人からブレークしつつあったスマートフォンに火がついたのは、国産メーカがアンドロイド端末を投入し始めたここ半年であると思う。あまりにも急激な浸透である。

一方、スマートフォンの特徴は、スマートフォンの実力を最大限に引き出す自由で魅力的なアプリケーションにある。また、その魅力的なアプリケーションの大半は背後のクラウドと連携することで成り立っているのだ。つまりは、企業におけるクラウド活用は、スマートフォンを活用したワークプレースの提供から起きてくると推測される。

ところが、日本においては、ファイル共有ソフトなどによる情報流出事件の多発を受け、自宅パソコンでの業務や職場のデータの持ち出しを禁止にしているところも多い。この状態で、個人に対して急速にスマートフォンが普及している。個人の生活の用途だけでスマートフォンを活用したいと考える人はどの程度存在するだろうか。同時に、ソーシャルメディアも歩調を合わせるかのごとく急速に普及している。つまりは、スマートフォンは、職場と個人が同居する場所であり、そのかかわりに関して何らかの解を持つ必要もあると考えられる。

3.3.4 まとめ

ISOGJ では、以下の 4 つのワーキンググループ活動を行っている。

１）　【WG1】セキュリティオペレーションガイドライン WG

２）　【WG2】セキュリティオペレーション技術 WG
３）　【WG3】セキュリティオペレーション関連法調査 WG
４）　【WG4】セキュリティオペレーション認知向上・普及啓発 WG

今年度は、WG１にて「マネージドセキュリティサービス（MSS）選定ガイドライン」の制定をおこなった。
http://www.jnsa.org/isog-j/activities/result.html

その目的は、サービスを利用したい方々へのガイドラインとなる為に、利用すべきサービスの理解と、どのようなサービスが利用できるかを理解し、調達をかける場合の RFP への参考となること。さらに、業者選定や利用における注意点やチェックポイントへの理解や各社のサービスを比較・評価するためのポイントも盛り込み、マネージドセキュリティサービス（MSS）の使い方のノウハウ集としても活用いただけるように、整えて来た。是非、ご活用を頂き、意見なども頂戴したいと考えている。ただし、これまで述べてきたように、環境が急速に変革しており、スマートフォンやクラウドの活用をベースとした内容にはなっていない。

しかしながら、冒頭で説明したような現在の IT 環境変化を理解し、適応しながら、さらにスマートフォンをとり入れクラウドを活用していくということは、当然のことながら最低限、責任分解点を意識して IT 活用を図っていかなければならない。その道を、どう歩んでいくかは様々だが、一つの道標としては、クラウド活用と同時に MSS アウトソースの活用も検討することは、これからのクラウド時代を乗り切って事業継続を行っていくための一里塚になる可能性は極めて高い。

3.4 「クラウド時代の情報セキュリティ」パネルディスカッション報告

3.4.1 パネルメンバー

コーディネータ:

情報セキュリティ普及実行評価検討委員会 委員長（工学院大学　教授）大木　栄二郎

パネラー:

独立行政法人　情報処理推進機構（IPA）セキュリティセンター研究員　河野　省二 氏

情報ネットワーク法学会（IN-Law）（英知法律事務所）弁護士　　岡村　久道 氏

情報セキュリティ普及実行評価検討委員会（日本セキュリティオペレーション事業者協議会（ISOG-J））西本　逸郎 氏

3.4.2 パネルの進め方

最初にコーディネータから、「クラウド時代とは」と題して、時代の見方を提供し、そのうえでディスカッションに入ることとした。ディスカッションは、コーディネータからパネラーに質問する形で進め、フロアからも 2，3 質問を受ける予定である。

3.4.3 「クラウド時代とは」

ディスカッションの前提として、テーマであるクラウド時代について、共通の理解を得るために、コーディネータからクライド登場の時代背景やその影響についての大まかな捉え方を紹介した。

まず、技術と社会の変革の関係に注目した増田米二氏の「原典情報社会」で示されている社会的技術法則によって、技術が社会を大きく変革させてきた過去の人類の歴史と、いま現在起きていると考えられる情報革命、つまり情報技術が工業社会から情報社会へ大きく変革させるという捉え方を紹介した。次に、段階的社会変革法則を取り上げ、このような大きな社会の変革は、一朝一夕に実現するのではなく、大きく三つの段階で変革が進むという見方を示した。

第一段階は、新たな技術がそれまでの人間労働にとって代わる段階、第二段階は新たな技術がそれまで不可能だったことを可能にする段階、それらを経て伝統的な社会の仕組みが新しい仕組みに根本的に変わるのが第三段階である。

こう考えると、現在はまさしく工業社会から情報社会への変革の第三段階へ入ってきたと言えるのではないだろうか。そうだとすると、これから社会的な仕組みが大きく変わり始める時期にあるということになる。その仕組みとは、現在の我々の社会を支えている大きな原理原則に関わるものではないかと考える。一つは、民主主義の原則である。現在の選挙制度や代議士制は、情報ネットワークが発達する前に形作られてきた。もう一つが資本主義であり市場原理である。

どちらも、情報の流通が不自由な時代にその原型が形作られてきたが、これからの情報時代にあっては、情報ネットワークの存在を前提とした別の形にさらに進化しなければならないだろう。また、同時に我々の生活を支える農業社会や工業社会の成果もさらに洗練されていかなければ、人類は情報だけでは命をつなぐことはできない。IT を活用した農林

漁業の再生なども、大きな仕組みの変化の一つと考えることができよう。今騒がれているTPPなどの取り組みも、このような大きな時代認識の中でとらえて議論する必要があるのではないかと考える。

このような時代背景の中で登場したのがクラウドコンピューティングであり、社会の仕組みの大きな変革を加速させるものと位置付けることができるというものの見方をしている。つまり、このような情報技術による社会の変革を、逆に「クラウド時代」と名付けていると言ってもいいかもしれない。

このような変化を、企業経営の立場から捉えてみると、特徴的な変化が企業価値に表れている。鮫島正洋氏の「特許戦略ハンドブック」によれば、1950年には、企業価値の75%を占めていた有形資産（土地建物機械部品などの物理資産）は2010年には20%に後退し、知的財産を中心とする無形資産の割合が、25%から80%へと劇的に増加するとされている。この80%を占める無形資産は、そのほとんどがデジタル化されコンピュータに記憶されているのが実態である。

このような企業価値の構成の劇的な変化が､企業が直面するリスク管理にも表れてくる。かつて75%を占めていた物理資産に関わるリスクをアトムリスク､すでに80%を占めるようになった無形資産に関わるリスクをビットリスクと名付けると、リスクの特性が大きく変化してきたことが分かる。経営者は大きくなってきたアトムリスクに対応していかなければならない。

アトムリスクは、局所的に激烈な被害を与えかねず場合によっては人命を失いかねない事故と被害が直結するもので、隔離を中心とするリスク対応に豊富な経験がある。一方、ビットリスクは何もしなくても今日すぐに激烈な被害が明らかになるわけではないが、被害認識の遅れがボディーブローのようにじわじわと企業経営に深刻な影響をおよぼすタイプのリスクである。企業経営者は、このようなリスクの変質に真摯に対応していかなければならない。

リスク対応の考え方も大きく変化する。工業社会の基本的な考え方の一つに有限な資源を配分し合う、つまり質量保存の法則やエネルギー保存の法則に支配された有限な資源のうち、如何に自社に配分される資源を得て事業に活用できるかが主たる経営戦略であり、そこには配分された資源に関するリスクは自社が負う、つまりリスク分担の考え方が基礎にあることになる。言い換えれば、アトムリスク対応は、分担しあうことが中心の概念である。ところが、情報社会においては、情報は無限のコピーや伝搬が可能で際限がない。情報は共有し活用するという概念が基本であるから、経営戦略も如何に適者と適切に情報共有関係を結んで事業を発展させるかに気を配らなければならない。したがって、情報共有関係の間柄では、必然的にビットリスクを共有しなければならない。アトムリスクを分担するという考え方から、ビットリスクを共有するという考え方への大きな転換が求められているのである。

さらに、ビットリスクを分解すると、情報そのものに関わるリスク（純粋なビットリスク）と、その情報を取り扱う器に関わるテクノロジーリスクとに分解することができる。これから企業が取り組まなければならないビットリスクのマネジメントは、この二つに大別できるが、企業により、情報そのものの活用に関わる純粋ビットリスクのマネジメント

が中心の一般企業と、情報を取り扱うシステムのテクノロジーリスクのマネジメントを担当するインフラ企業とに大きく分かれていくことも想定される。これが、IT の所有から利用へという、クラウドコンピューティングのもう一つの本質を示しているということができよう。

クラウド時代というものを、以上のような時代背景の中で理解し、クラウドコンピューティングが持つ様々な利点や課題、あるいは所有から利用への変化などをこの時代認識にあてはめて考えることによって、今後の対応策の基軸を定めるヒントが得られるのではないかと思う。これらも踏まえて、議論していただければ幸いである。

3.4.4 ディスカッション

ディスカッションでは、コーディネータからパネラーに質問する形で進められた。

テーマ１．クラウドは 1,2 年後どのようになっているか

最初の質問は、短期的にここ 1，2 年で、クラウドはどのように変化するのか、どういう風になっていくのかについてパネラーの個人的な見通しを尋ねた。

河野氏からは、現在の Saas，Paas，Iaas など、プラットフォームに近いサービスから、それらに情報が集まってくることにより、集まった情報が新たな価値を生み、新たなサービスの核になっていく、いわば Contents Cloud みたいなものが出てくるのではないかと予想する考えが示された。cookpad みたいに利用者から集まってきた情報が二次的な価値を生み、それが再利用される仕組みを例に挙げ、そのためにはデータ構造などが再利用されやすいようにする必要があることにも触れた。今はその準備段階ではないかと位置付けた。

岡村氏からは、ある法科大学院での例を取り上げ、レジメの受け渡しはメーリングリストで、日程調整はスケジューリングサイトでなど無料サービスを活用している、某学会でのパネルディスカッションも You Stream で中継する等、気がつけばこれらのサービスを当たり前のように使っているという実態が示された。そのうえで、たとえば財政的に苦しい状況にある自治体にあっても、同じように利用が進んでいくと考えるべきだ、この流れは止められない、ごく当たり前のことになるのではと、いまの延長線上で利用が進むという予測が示された。

西本氏は、正直言って分からないと前置きしながら、カンブリア時代と言えるのでないかとの考え方を示した。つまり、進化の実験の期間ではないか、Facebook が日本で定着するのか、デバイスやサービスもまだまだ使えない中途半端である、キラーアプリが出現してくるかが一つのキーと考えられる。この 1，2 年でその種のものが出てくるかどうかを見てみたい。仮想化技術がどこまで枯れるか、IPv6 がどういう世界になるか、HTML5 がどこまで基盤になるか、などにも注目していく必要がある。まとめると、良くわからないが、この 1，2 年はワクワクすることは間違いないと締めくくった。

この 1，2 年で、企業が基幹業務をクラウドに載せることはおそらくあまり進まないであ

ろう。基幹業務ではない部分、付帯業務というか、企業固有の付加価値が生まれるわけではない部分については､ビジネスプロセスと IT プロセスがともにクラウド化していくのがこれからの期間ととらえられるのではないだろうか。その意味では、これまでの延長線上にありながら、様々な進化の実験が行われ、そのような中から、Contents Cloud が登場する、あるいはキラーアプリが出てくるなどを期待したい。

テーマ２．あるべき(to be)クラウドサービスとは

クラウドにはいろいろな課題が指摘されているが、それらに対してあるべきクラウドサービスの姿、見通しや期待などを専門的な立場から描いていただいた。

河野氏は、すべてのサービスを１社が提供するのではなく、いろいろな事業者の提供するクラウドサービスを融合して提供するような考え方が望ましいという考え方を示した。例えば、SalesForce のユーザー管理は GoogleApps を使うなど、すでにサービスとしてあるものを作らない、あるものを使うという態度が大事ではないか、日本の事業者もすべてを自分で作ろうとせず、良いものを使うというスタンスで、サービスをインテグレートするべきであるとまとめた。

岡村氏は、医療用語の Informed Consent を例に、クラウドサービスにおいても選択の前提条件として十分な説明がなければならないことを取り上げた。利用者は自己責任でクラウドサービスを選択する。この選択が的確に行えるには、クラウド提供者からの十分な Disclosure、つまりサービス内容とともにどんな分野に使えるかなどが判断できる情報の提供がなければならない。利用者の立場からすれば、的確に選択できるためには、クラウド事業者の比較検討ができる必要がある。そのためには、株式投資も引き合いに出しながら、比較検討の新たなサービス、例えば格付けなども必要であろうと締めくくった。

西本氏は、誠実であること、信頼されることに注目した。クラウドは電気、ガス、水道のような社会インフラになるであろうから、信頼されるところが提供すべきだ。生産システム、POS システム、食材デリバリー、工場制御システム、銀行などを取り上げ、クラウドに行くべきかどうかの検討項目を例に挙げながら、基盤となるクラウドに必要なのは、誠実であること信頼されることの意味を強調した。次に、facebook を例に取り上げながら、Private をフリーにオープンにする部分と、徹底的に匿名性を担保すべき部分とが両方必要で、幅を広げていく必要がある。そのような幅の広いトータルの社会システムがクラウドのあるべき姿ではないかと締めくくった。

クラウドサービスが融合し合う、いわゆるサービスの入れ子構造がクラウドサービスのもう一つの特徴である。この場合、融合が進んで複雑な入れ子構造になったサービスを、利用者が自己責任で選択するというのはかなり難しいことになる。この意味から言うと、電気、ガスなどと同じインフラとして、誠実で信頼できる主体が提供するサービスとして国などの公的な機関が提供するということも、理想的には一つの選択肢であろう。

この点について、さらにパネラーに意見を聞いた。

現実には、ボーダーレスの世界で、一つの国がコントロールするというのも効果が薄く、現実的ではない。サービスの特性を示すデファクトスタンダード、あるいは ISO 化などが一つの答えになるかもしれない。

利用者が入れ子構造のサービスを的確に選択する手段は、現状ではあまり機能していない。多くの人が使っているなどが今の現実的なところ判断材料であろう。これから選択基準を整備して、情報開示ガイドラインなどをブラッシュアップして、信頼モデルなど監査なども含めて考えていく必要があろう。

安全マークなどのような考え方もあろうが、もう一つの考え方は、セキュリティにいつまで利用者が対価を払うのか、という視点で考える必要があるのではないか。つまり、セキュリティは利用者から見えない当たり前の機能として基礎に入っている。セキュリティコストが表に出ない形にするという考え方もあろう。セキュリティが公的機関からの強制でなければ、マークなどの方法はあまり機能しないのではないか。

ここで、フロアからの意見を求めたが、質問はなかった。

テーマ３．落とし穴にはまらない為にどのような点に気をつけたらいいのか

改めて、いままでの二つのテーマでの討論を踏まえて、落とし穴にはまらない為にどのような点に気をつけたらいいのかについて、パネラーの意見を求めた。

河野氏は、クラウドを使うとセキュリティポリシーが守れなくなることがあることを例をあげて紹介した。つまり、ポリシーを策定した状況と現状とが異なってきている、あるいは以前のリスクアセスメントが実情に合わなくなってきている、などを指摘した。まとめると、情報セキュリティポリシーを見直せということになる。

岡村氏は、ポリシーについて触れたのち、契約について取り上げた。例えば、契約書の中に記載された「データセンターの立ち入り条項」などが、実効的に意味がなくなることを指摘した。また、国土交通省の ITS の例を取り上げ、いろんなプレーヤーが集まってサービスが構成されている場合の責任分担の在り方に問題があることを指摘し、責任の所在と切り分けを明確にするとともに、一旦事故が起きた後に、対策をして再開するに当たっては、誰かが責任を持って安全宣言をしてあげる必要があるのではないかと指摘した。

西本氏は、ベンダーにあまり要求しないようにという考え方を示した。あまり要求すると、アウトソースと同じであり、クラウドではないだろう。クラウドはベンダー側が決めるのだろう。また、目的が変化することも考えなければならない。最初はコスト削減で使い始めたものが、成長戦略に切り替わることはよくある。また、自己責任の部分とベンダー責任の部分の切り分けも時間とともに変化するはずだ。その意味でも定期的に責任分担を見直すことが求められる。変化を前提として、自分たちがどう使うのかを常に見極めながら行くことが大事だと締めくくった。

いずれも非常に示唆に富んだ意見を聞かせていただくことができた。

3.4.5 ディスカッションのまとめ

新しいフロンティア

冒頭で紹介した歴史的な見方から言うと、IT を基軸にしていろいろな新しいことが起きている。これは一つのフロンティア、未開の地である。これまでの制約や規制があまり及ばない、何をやってもよいがその代わり自己責任で取り組まなければならない、そのような部分が大きい分野である。そのような見方でこれまでのディスカッションを進めてきた。

ここでもう一つの見方として、新しいフロンティアで新しい事業が生まれる、新たな雇用が生まれるなどのプラスの部分に焦点を当てて、見通しなどをお伺いした。

情報提供

例えば、セキュリティのクラウドサービスも結構使われている。ウイルスとか脅威に関する情報を、これまでのように自分たちのところだけで考えるのではなく、自分たちの経験を提供することで、全体の情報がフィードバックされるようになり、より良い対策が可能になる。自分たちの情報を出すと集約された形で帰ってくる、このような形で中小企業でも大企業と同じレベルで情報が即時に入ってくる。中小規模の企業にとって有利な状況と言える。

ネット家電

前向きな明るい話としては、日本型クラウドの次の発展形はネット家電だと思う。レシピが空から降ってくることになるから、新たなサービスが生まれる、ネットサービスが使われる。さらに IP v6 が加速されると家電にそれぞれ IP アドレスが割り当てられ、そこに様々なサービスが可能になる。家電そのものも韓国などのメーカーとの競争に優位性を発揮できるようになる、日本経済も上向きになるのではないか。

信頼ブランド

日本はセキュリティは全く遅れていない。遅れているのは IT の活用だ。標準化や監査をどうするかなど非常に進んでいる。セキュリティについては、世界に冠たるフレームワークもあり、洗練された Operation もまとめて Package にし、「信頼ブランド Japan」みたいにして国をあげて輸出していくような取り組みができるはずだ。そこに重要なのがセキュリティなのだ。

これにてパネルディスカッションを終了した。

4. クラウド時代におけるソフトウェア資産管理の側面

4.1 IT サービスマネジメントと SAM の関係

(注：SAM はソフトウェア資産管理 (Software Asset Management)を表す)

4.1.1 はじめに

ITIL® (Information Technology Infrastructure Library、以下 ITIL とする) と SAM の関係について紹介する。ITIL は誕生以来、IT サービスマネジメントのデファクトスタンダード (事実上の標準) として広く周知され、V1、V2、V3 と版を重ねて来た。SAM は ITIL V2 の中核書籍として扱われず､フレームワークに対する補完書籍としての位置付けであった。最新版の ITIL V3 では、構成するプロセス群の中に、SAM を構築する上で必要とされるプロセスが包含された形で存在していることを示す。

SAM の国際規格として、ISO/IEC19770-1 が 2006 年に制定され、国内では対応する JIS 規格として JIS X 0164 が 2010 年に発行された。一方、ITIL をルーツとする IT サービスマネジメントの国際規格 ISO/IEC20000 は 2005 年に発行されている。ISO/IEC20000 規格と SAM 規格は密接な関係を持っている。ITIL、SAM、規格の関係を明らかにしてゆくことで、IT サービスマネジメントの実践が、SAM のプロセスを構築する上でも有効であることが理解できるだろう。

4.1.2 ITIL

ITIL には、IT サービスを管理してゆく上で必要となるプロセスに関する包括的なガイドラインが含まれている。英国政府の CCTA (Central Computer & Telecommunications Agency) が中心となり、1980 年代後半に第一版の ITIL V1 として誕生した。ITIL V1 の制定には、政府関連の機関に加えて、様々な組織が協力して開発された。ITIL の所有権は現在も英国政府にあり、CCTA を統合した OGC (Office of Government Commerce) が所管している。

1991 年には ITIL を普及・促進する目的で、グローバルなユーザーフォーラムとして、*it*SMF が設立された。ITIL は ITIL V1 の発表以来、IT サービスマネジメントのベストプラクティスの向上を目的としたグローバルな組織である *it*SMF によって改善され続けている。

Library という名が示すように ITIL は書籍群である。最初に制定された ITIL V1 は 40 冊を超える冊子から構成されていた。1990 年代の後半に入ると，書籍間の重複部分の整理，改訂が計画され，書籍の統合化がすすめられた。結果として 7 冊のコア書籍にまとめられた。(図 4.1 を参照) これが ITIL の第二版（以下“ ITIL V2 ”と略す.）である。中核となる書籍は 7 冊(注:『ビジネスの観点』は Part 1 と Part 2 に分冊で発行された。) であり、各書籍の概要は以下のような内容である。

- 『サービスサポート』日常における IT サービスの運用とサポートに不可欠とされるプロセスを中心にまとめられている。機能としてのサービスデスクに加えて，インシデント管理，問題管理，変更管理，リリース管理および構成管理の 5 つプロセスから構成されている。
- 『サービスデリバリ』中長期的な IT サービスの提供に関連するプロセスを扱う。サービ

スレベル管理，キャパシティ管理，可用性管理，IT サービス継続性管理および IT サービス財務管理のプロセスが含まれている。

•『サービスマネジメント導入計画立案』組織における IT サービスマネジメントの成熟度評価を 5 段階で定義し、プロセスの導入計画立案と改善のガイダンスを含んでいる。

•『セキュリティ管理』IT サービスマネジメントに関わるセキュリティをプロセスの観点から説明している。ISO/IEC19970 との比較も掲載している。

•『ビジネスの観点 Part1＆2』顧客とのビジネス関係およびサービス提供者におけるサプライヤ管理について述べている。

•『ICT インフラストラクチャ管理』インフラストラクチャのライフサイクル管理を扱う。

•『アプリケーション管理』アプリケーションのライフサイクル管理を扱う。

2007 年に ITIL V2 が改訂され ITIL V3 が発表された。ITIL V3 では、ITIL V2 の運用のプロセスアプローチ中心から、サービスのライフサイクルに焦点をあてることで、IT サービスの戦略から運用までに至る幅広いスコープを持っている。ITIL V3 は 5 冊の書籍として刊行され、それぞれの書籍の特徴は次のようになっている。

•『サービスストラテジー』

サービスマネジメントを戦略的資産として開発、導入するための手引き。IT サービスおよび IT サービスマネジメントに対する全体的な戦略を確立する。

•『サービスデザイン』

事業の要求を満たすサービスとプロセスを設計するための手引き

•『サービストランジション』

新規または変更されたサービスを運用に移行させる手引き。

•『サービスオペレーション』

サービスの提供における有効性と効率性を達成するための手引き

•『継続的サービス改善』

サービスの品質や運用上の効率性を維持し改善するための手引き。

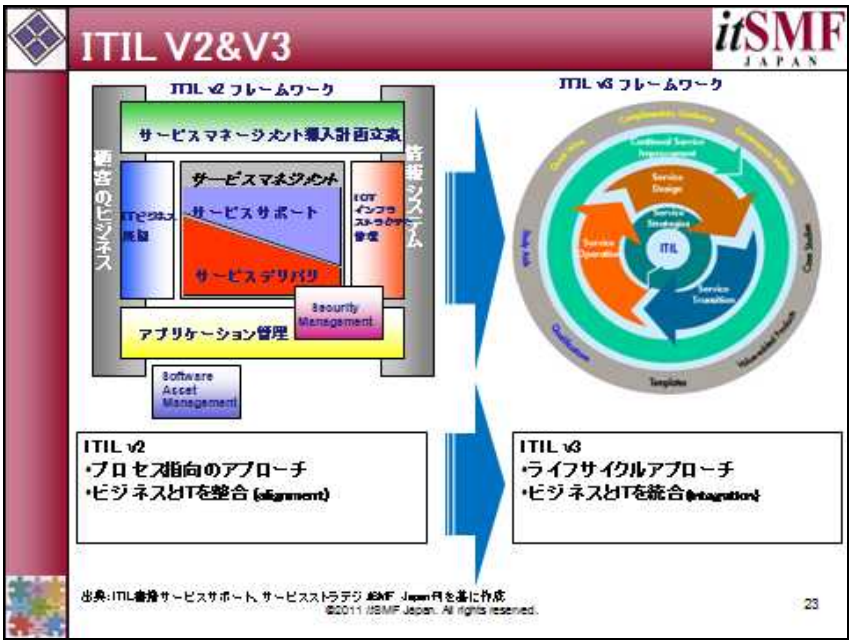


図 4.1　ITIL V2＆V3 フレームワーク

ITIL は V2 であれ、V3 であれ、IT サービスマネジメントに関する、数多くのベストプラクティスを含んでいる。ベストプラクティスとは、複数の組織で成功している、実績のある活動またはプロセスのことである。

現実に IT サービスを提供している組織においては、ITIL を意識しなくとも IT サービスマネジメントのプロセスに該当する何らかの活動を実践しているであろう。従って、ITIL を導入しようとする活動は、組織が元々実践している改善活動の一つとして捉えることも可能である。ITIL のプロセス群を、適応しやすい所から順次導入してゆくことも可能である。ITIL は特定のハードウェア、ソフトウェア、プラットフォーム及びテクノロジ（ツール等）に依存しないために、あらゆる IT 環境で役立てることができる。IT サービスを提供している組織の規模に関係なく､身の丈に合った IT サービスマネジメントが構築できるのである。

4.1.3 ソフトウェア資産管理

ソフトウェア資産をプロセスのもとで管理しようとする考え方は目新しいものではない。明示的にソフトウェアアセット管理(SAM: Software Asset Management、以下 SAM とする。)という形では、ITIL V2 の中核書籍に対する補完書籍という位置付けで、SAM 書籍が存在していた。SAM 書籍は ITIL V2 フレームワークを補完する書籍としながらも、ITIL の中核書籍であるサービスサポート（2000 年発行)、サービスデリバリ（2001 年発行)、アプリケーション管理(2002 年発行)､サービスマネジメント導入計画立案(2002 年発行)の中核書籍に遅れることなく、2003 年に発行されている。ITIL の SAM 書籍では、ソフトウェア資産管理を次のように定義している。

SAM の定義

SAM（ソフトウェア資産管理）は、組織内のソフトウェア資産のライフサイクル全ステージを通じて、効果的な管理、制御、および保護のために必要なインフラストラクチャとプロセスの全てである。

出典：ITIL 書籍 『Software Asset Management』 TSO 刊を基に作成

定義における管理、制御、および保護の意味するところは、ソフトウェア資産の持っている特徴をよく表しているだろう。すなわち、ソフトウェア資産を管理する上での重要なテーマの一つであるライセンス管理を想起させる。ライセンス管理を実践することはコンプライアンス(法令遵守)につながることから、ソフトウェア資産を管理、制御、および保護することは必須である。

ITIL V2 のコア書籍においては、IT サービスを顧客/利用者に提供するために必要なプロセス群のベストプラクティスが中心であり、ソフトウェア資産をライフサイクルを通じて管理、制御、および保護するためのプロセスは扱われていない。SAM の定義では、必要なインフラストラクチャも含まれるので、SAM はソフトウェア資産に係るハードウェアとソフトウェア（ライセンスを含んだ）を扱うプロセス群のすべてを指している。

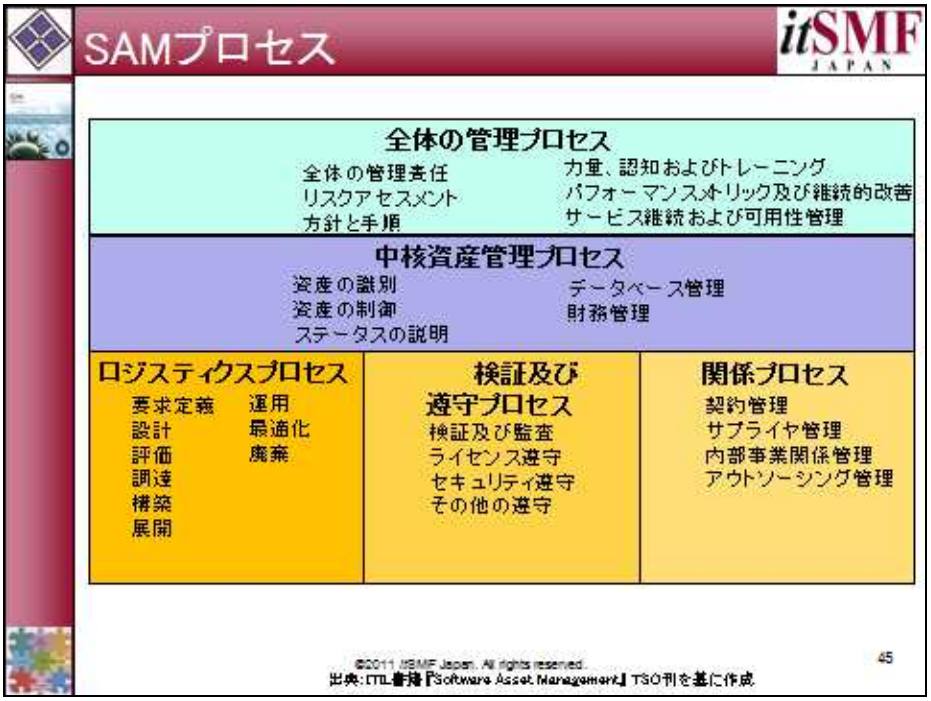


図 4.2　ITIL 書籍における SAM プロセス

（１）SAM の国際規格

SAM の国際規格である ISO/IEC19770-1（以下 SAM 規格とする）は 2006 年に制定された。SAM 規格は、ソフトウェア管理に必要とされる一連のプロセス群を規定している。ソフトウェア資産をプロセスのもとで管理する ITIL V2 の SAM 書籍と目的は同じである。SAM 規格の発行を受けて、JIS 化が推進され、2010 年に JIS X 0164-1 の国内規格として発行されている

SAM 規格の序文の中には次のような表現がある。

この規格は，JIS Q 20000 規格群と緊密な整合をとり，また，それを支援するように意図されている。

出典：JIS X 0164-1 ソフトウェア資産管理：2010

独立した規格が他の規格を支援するというのは、違和感を覚えるが、規格の箇条において、次のように上記の序文を補足している。

4.1.1 定義及びサービスマネジメントとの関係

ソフトウェア資産管理とは，組織内のソフトウェア資産の有効な管理，制御及び保護をいう。

この規格が定義する SAM のプロセスは，JIS Q 20000 規格群が定義している情報技術（IT）サービスマネジメントとよく両立するように構成されており，それを適切に支援することを意図している。

出典：JIS X 0164-1 ソフトウェア資産管理：2010

注：下線部は筆者による

SMA のプロセスが 、JIS Q 20000 規格の定義する IT サービスマネジメントとよく両立するように構成されており，それを適切に支援することを意図していると明言している。

JIS Q 20000 は ISO/IEC20000 を基に制定された国内規格である。また、ISO/IEC20000 は ITIL と整合し、補完している規格である。

SAM 規格で定義されるプロセス群が JIS Q 20000 規格で定義している IT サービスマネジメントのプロセスと緊密に整合する事は、ITIL にも整合していると考えても良いだろう。

とりわけ、下記の箇条 4.7 の 4.7.1 一般では、SAM 規格の中で定義されている SAM のライフサイクルプロセスインターフェイスは、明示的に JIS Q 20000 のプロセスと整合が取られているとしている。

4.7 SAM のライフサイクルプロセスインタフェース

4.7.1 一般

“SAM のライフサイクルプロセスインタフェース”は，SAM との関連では，JIS X 0160 での主ライフサイクルプロセス及び JIS Q 20000 規格群のプロセスとほぼ整合がとられている。

出典：JIS X 0164-1 ソフトウェア資産管理：2010

注：下線部は筆者による

SAM 規格でのライフサイクルプロセスとは、次のプロセス群である。

a) 変更管理プロセス
b) 取得プロセス
c) ソフトウェア開発プロセス
d) ソフトウェアリリース管理プロセス
e) ソフトウェア展開プロセス
f) 事件・事故管理プロセス
g) 問題管理プロセス
h) 廃棄プロセス

変更管理、リリース管理、展開、問題管理などのプロセスと JIS Q 20000 の同名のプロセス群が緊密に整合する関係があることは容易に想像できるだろう。

SAM 規格は Asset（資産）を扱う事から、IT サービスマネジメントのプロセスの中で最も関連が深いプロセスは構成管理であることは明白だが、SAM 規格では構成管理との関係について、次のように述べている。

“SAM の在庫プロセス”は，SAM の基本であるだけでなく，すべての構成管理の基本である。すべての IT 資産（ソフトウェア及び関連資産だけではない。）及びこれらの資産すべての間の関係を対象にする限りにおいて，更に非 IT 資産も含んでよいことから，構成管理は，SAM の適用される範囲を超える。IT サービスマネジメントのすべてを含むプロジェクトでは，“SAM の在庫管理プロセス”が構成管理の一部とみなされることもある。

出典：JIS X 0164-1 ソフトウェア資産管理：2010

注：下線部は筆者による

構成管理の適用範囲は“SAM 在庫プロセス”における適用範囲を包含することを述べているのである。“SAM の在庫プロセス”とは、次のプロセスで構成されている。

a) ソフトウェア資産の識別
b) ソフトウェア資産の在庫管理
c) ソフトウェア資産の管理

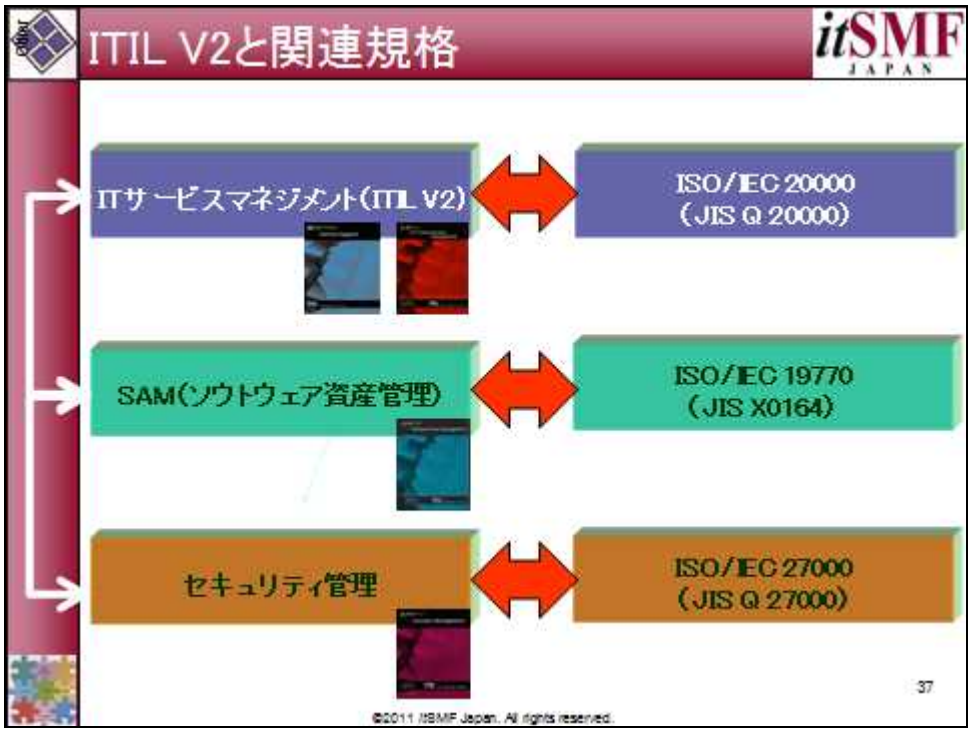


図 4.3　ITIL V2 と関連規格

（2）SAM と ITIL V3

2007 年に ITIL V2 はそれまでのプロセスベースのガイダンスから、サービスのライフサイクルに焦点を当てた ITIL V3 へアップデートされた。ITIL V3 はライフサイクルアプローチを取ることで、SAM に必要なプロセスの多くを抱合した形となっている。

ITIL V2 では、セキュリティ管理は別の書籍として存在していたが、ITIL V3 ではプロセスの一つとして取り込まれている。

ITIL V3 のプロセス群で SAM に密接に関連するプロセスは、IT 財務管理、リリース管理および展開管理、サービス資産および構成管理である。

注目すべきはサービス資産および構成管理(Service Asset and Configuration Management: 以下 SACM とする）であろう。ITIL V3 用語集によれば、サービス資産は次のように定義されている。

サービス資産
サービス・プロバイダのあらゆる能力またはリソース。サービスの提供に寄与する可能性があるすべてのものが含まれる。

資産
任意のリソースまたは能力。資産は、マネジメント、組織、プロセス、知識、人材、情報、アプリケーション、インフラストラクチャ、金融資本のいずれかのタイプになりうる。

出典：ITIL V3 用語集

ITIL V3 でのサービス資産および構成管理プロセスは、“サービス資産”を“あらゆる資産”と読み替えれば、“SAM の在庫プロセス”の適用範囲を超えるものであることが理解できる。

ITIL V3 のサービス資産および構成管理は次のような特徴を持っている。

- **SACM はサービストランジションの主要プロセスのひとつ。資産とそれに関連するライフサイクルを管理するだけではなく、資産間のリンクと関係も管理する。**
- **インシデント、問題と変更、サービスと SLA のような、他のサービス管理に関連する問題と資産との関連を管理する。**
- **SACM の主要な役割は物理的なソフトウェア資産の管理である。**
- **メディア、ライセンス及び真正性を示す文書類の制御。資産管理の財務の側面は IT 財務管理に任せられる。**

ITIL V3 の SACM プロセスでは SAM を抱合している事が、より明白に述べられていることが理解できるだろう。

4.1.4 IT サービスマネジメントと SAM の関係

IT サービスマネジメントを実践しているサービス提供者にとって、SAM を構築する事は新たにプロセスを導入する必要はないだろう。既存のプロセスを SAM に合わせて変更し、改善を加えてゆけば良い。ITIL V2 での基本的な原則とプロセスは ITIL V3 に包含されている。ITIL V2 の SAM 書籍から SAM 規格にいたるまで、一貫して IT サービスマネジメントと SAM のプロセス群は密接に関係し、整合しているのである。

- ❑ SAM は IT サービスマネジメントと緊密に整合が取られている。（ITIL V2＆V3）
- ❑ SAM が対象とする適応範囲は、IT サービスマネジメント（ITIL V3）のサービス資産および構成管理プロセスにおける対象範囲に含まれる。
- ❑ SAM を実践・構築する事は、ソフトウェアの管理性を高めると共に、IT サービスマネジメントへの貢献となる。

紙面の関係上、SAM のプロセス群と IT サービスマネジメントのプロセス群を全て網羅できていないが、IT サービスマネジメントを実践されているサービス提供者の方々にとって、

SAM がより身近なプロセスとして感じていただけたのではないだろうか。また、SAM のプロセス群を構築しようとする方にとって、一助となれば幸いである。

4.2 クラウド・コンピューティング時代の SAM の考え方

4.2.1 はじめに

クラウド・コンピューティング（以下「クラウド」と呼ぶ。）とは、ユーザーがインターネットを経由して様々な IT サービスを利用する仕組みの総称である。クラウドはシステム管理負荷の軽減、初期投資の平準化など多くのメリットが得られるため、現在急速に普及し始めている。

一方、クラウドの普及に伴い、企業の IT ガバナンス上の問題が指摘され始めた。クラウドを導入するためには、ユーザーは用意されたメニューを選択するだけでよく、この間に企業の IT 部門が関与することはほとんどない。またビジネスの規模拡大に伴う IT リソースの拡張も容易である。そのため企業内のユーザーが自らの判断で業務用にクラウドを導入し始めた場合、企業側がそれを逐一把握することは非常に困難になる。

全社 IT の運営管理に支障が生じ、情報セキュリティやソフトウェアライセンス管理上のリスクも高まる。現在、クラウド・コンピューティングは急速に普及しつつあるため、これらの問題を放置するとクラウド・コンピューティングは将来 IT ガバナンス上の大きな穴になる可能性がある。

我々は今回こうした問題意識に基づき「クラウド・コンピューティング時代の SAM の考え方」について調査研究を行った。本稿はその報告書であり、クラウド・コンピューティングの特徴である仮想化技術や、クラウド・コンピューティングを支える OSS（Open Source Software）を利用する際の IT ガバナンス上の留意点を「ソフトウェア資産管理（SAM; Software Asset Management）」の観点から指摘することを目的としている。

本稿の構成は、まず 4.2.2 でクラウド・コンピューティングの特徴である仮想化技術に着目し、仮想化環境における SAM の留意点について述べる。続く 4.2.3 で IT サービス提供形態としてのクラウド・コンピューティングに着目し、クラウド環境における SAM の留意点について述べる。最後の 4.2.4 ではクラウド・コンピューティングにおいて広く利用されている OSS（Open Source Software）に着目し、OSS 利用時の SAM の留意点について述べる。

4.2.2 仮想化環境における SAM の留意点

(1)仮想化の定義

仮想化（Virtualization）とは IT リソースの物理的特性をユーザー等から隠蔽する技法である。この技法により単一の物理リソースを複数の論理リソースに見せかけたり、逆に複数の物理リソースを単一の論理リソースに見せかけたりすることができる。仮想化の歴史は古く、1960 年代に遡ることができる。初期のコンピュータはメモリー上に１つのプログラムしか呼び出せず、そのため１つのプログラムがリソースをすべて占有していた。これでは高価なコンピュータの利用効率が上がらないため１台のコンピュータを複数のユーザーで同時利用するための技術、すなわちタイム・シェアリング・システム（TSS：Time Sharing System）や仮想記憶などの技術が登場した。これらの技術はその後オペレーティングシステム（OS：Operating System）へと発展し、現在では OS の標準機能となっている。

近年ハードウェアの性能向上と共に新たな仮想化技術が登場し、クラウド・コンピュー

ティング時代の到来と共にこの歴史ある概念が再び注目されている。本稿では仮想化技術を大きく、サーバー仮想化、ストレージ仮想化、ネットワーク仮想化、クライアント仮想化（デスクトップ/アプリケーション仮想化）の４つに分類し、仮想化環境における SAM の留意点について検討した。

(2)サーバー仮想化

サーバー仮想化とは、単一のサーバーをあたかも複数のサーバーであるかのように論理的に分割し、それぞれ別の OS やアプリケーションソフトウェアを動作させる技術である。各々の仮想サーバーは、お互いに悪影響を及ぼすことがないように設計・設定されているので、ある仮想サーバーがダウンしても他の仮想サーバーは稼動し続けることができる。サーバー仮想化の導入メリットとしては、サーバー統合によるコスト削減効果、プロビジョニングとリソース共有化による安定稼動効果、コンピューティング環境整備の短工期化の効果などが挙げられる。

(3)ストレージ仮想化

ストレージ仮想化とは、複数のストレージ装置を論理的に集約する技術である。ストレージ仮想化はサーバー仮想化のストレージ機器版とも考えられ、そのメリットもサーバー仮想化とほぼ共通している。

(4)ネットワーク仮想化

ネットワーク仮想化という用語はまだ一般的ではないが、一台の大型ネットワークサーバーの内部に論理的に（ルーター／スイッチ、セキュリティアプライアンス等の）ネットワーク関連機器を設定し、利用する技法である。ネットワーク仮想化もサーバー仮想化のネットワーク機器版とも考えられ、そのメリットはネットワーク環境構築と変更管理の柔軟性確保である。

(5)クライアント仮想化（デスクトップ仮想化）

クライアント仮想化（デスクトップ仮想化）という用語もまだ一般的ではないが、サーバー側でソフトウェアを実行し､クライアント PC はその結果画面を表示するという技法である。旧来のメインフレームコンピュータにおけるダム端末の現代版とも考えられるが、近年ネットワークの高速化と共に新たなクライアント仮想化技術が登場し､PC 運用管理負荷の軽減、情報漏洩対応策として注目されている。

(6)仮想サーバー上のライセンス

仮想サーバー上のソフトウェアのライセンス料は仮想サーバー単位で発生する。仮想サーバーは容易に追加・削除が可能なのでライセンス管理が甘くなりがちである。そのため仮想サーバーの変更管理に連動したライセンス変更管理が求められる。ソフトウェアベンダー各社のライセンス体系（CPU 課金体系）は様々であるが、仮想サーバーに割り当てられた CPU 数に応じて課金する方式が現状では多数派である。例えば、代表的な基本ソフトウェアである Microsoft Windows Server 2008 では、ライセンスの種類により実行可能な仮想マシン数が定められている。すなわち、Windows Server 2008 Standard は最大 1 つ、

同 Enterprise は最大 4 つ、同 Datacenter は無制限となっている。

(7)仮想化環境における SAM の留意点

仮想化の“肝”は、「物理的実装を隠蔽しつつ、使い勝手のよいインターフェースを提供すること」である。一方、ソフトウェア資産管理（SAM：Software Asset Management）を実施するためには、ソフトウェアが稼働するハードウェア機器の所在と構成を把握する必要がある。つまり「仮想化」と「SAM」は端から相性が悪いのである。

仮想化環境において想定される SAM の留意点として、CPU 数の動的再配置への対応が挙げられる。CPU 数に応じて課金するソフトウェアの場合、仮想サーバーの負荷変動に応じて CPU 数が適宜変動すると、課金も変動することになる。その場合、どのように割当 CPU 数の変動を把握し課金に反映するのか、技術的な方策も含めて今後の活発な議論が期待される。

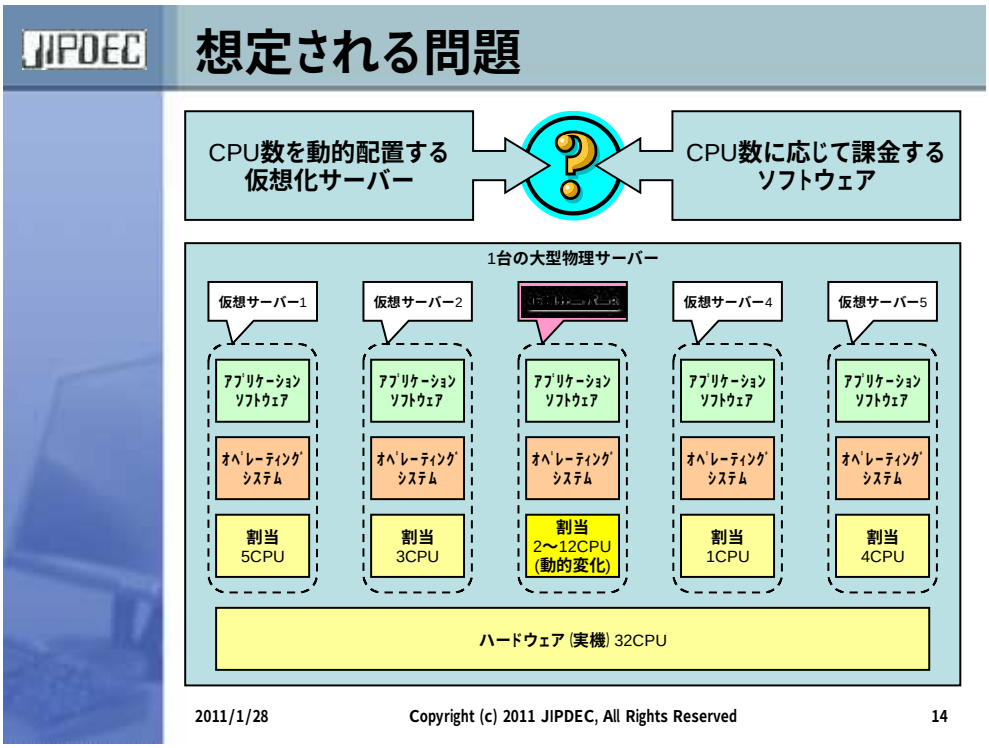


図 4.4　仮想化環境において想定される問題

4.2.3 クラウド環境における SAM の留意点

(1)クラウドの定義

クラウド・コンピューティング（Cloud Computing）とはネットワークを介してハードウェアやソフトウェアなどの IT リソースを利用するコンピューティング形態である。ユーザーはインターネットの先に用意されている IT リソースの実装状況を知らないまま（あるいは気にせずに）それらを利用する。。

(2)クラウドの分類

クラウドは、向先別で２つ、提供されるリソース階層で４つに分類される。

表 4.1　クラウドの分類

分類法	分類
向先別	パブリッククラウド
	プライベートクラウド
階層別	SaaS (Software as a Service)
	PaaS (Platform as a Service)
	IaaS (Infrastructure as a Service)
	DaaS (Desktop as a Service)

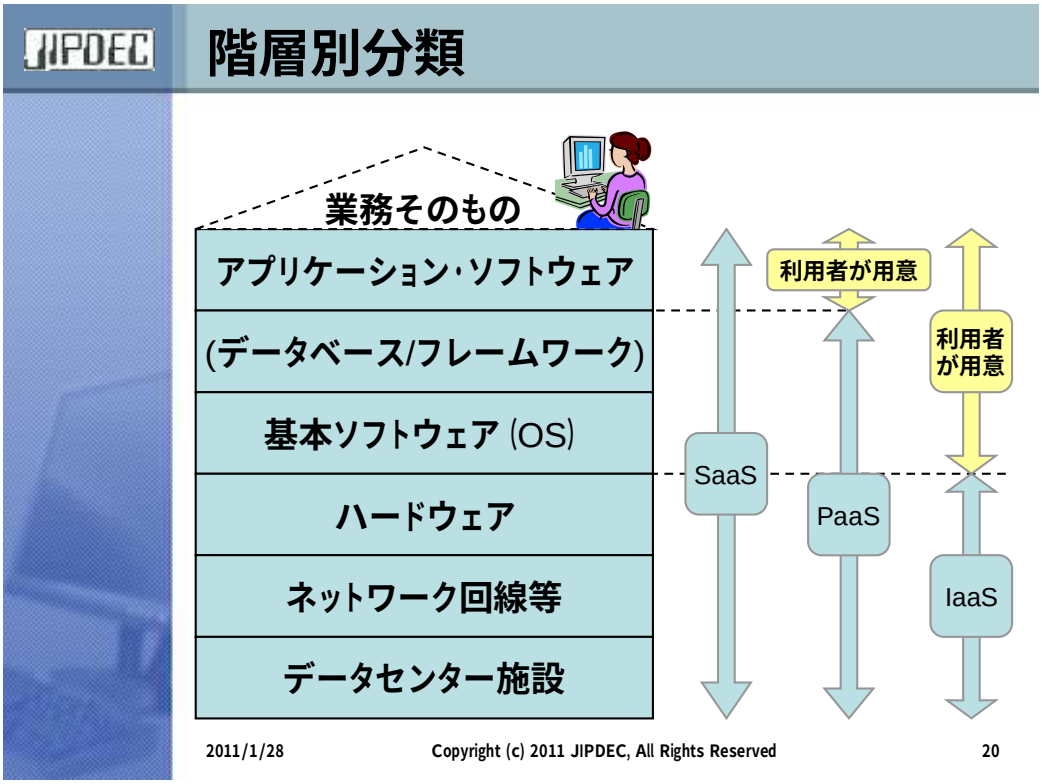


図 4.5　クラウドの分類（階層別）

(3)クラウド環境における SAM の留意点

クラウドの普及に伴い、人々の情報システムの利用スタイルが「所有」から「利用」へ大きく変化してきた。クラウドではサービスインのスピードが注目される一方、IT 部門の関与の薄さに起因する様々なマネジメントリスクが指摘されている。

- 　　/　　/
-
-

そこで我々は、業務アプリケーションを SaaS の形態で利用する場合の「SAM の留意点」について、以下の４つの側面から検討した。

-

- SLA　EULA
-
- SLA　SLM

(4)組織面での留意事項

業務アプリケーションが SaaS で提供されている場合、サービスを利用する利用部門（契約部門）は、「SAM の業務アプリケーションを SaaS で利用する場合の規程」に則ってサービスを利用し、管理者はその運用状態が規程に則って利用されているかどうかを管理しなければならない。各組織の役割は以下の通りである。

①総務・法規部門

SAM 規程を作成・管理・監督する部門は、契約書（サービスレベル契約及び、ソフトウェア使用許諾契約）の内容に基づき、利用部門と運用管理部門の連携に関する規程を作成しなくてはならない。

この規程には「利用」するサービスとして提供される SaaS の性質から、サービス利用部門が利用可能なサービスの範囲、サービス提供者としての適格性の基準、SLA（Service Level Agreement：サービスレベル合意）で網羅すべき項目および課題、SLM（Service Level Management：サービスレベル管理）などが定義されていることが望ましい。

② SaaS 利用部門

SaaS 利用部門は、同じく契約書の内容に基づき SaaS を利用する必要がある。具体的には、スピード、コスト、利便性などのバランスを考慮し、規程に則り利用サービスを決定する。SLA／SLM の成功には利用部門の参画が必須であるため、早期に関係各部門との共通認識を形成することが肝要である。

③運用管理部門

SaaS 運用管理部門（情報システム部門）は、同じく契約書の内容に基づき SaaS が利用されているかどうかを管理する必要がある。具体的には、SaaS の実行環境となるクライアント環境を提供し、規程に則りサービス利用部門の利便性を損ねることなく、利用部門を支援する体制を整備する。

(5)契約面での留意事項

SaaS 提供者とサービス契約や SLA を締結する際には、以下の点に留意する必要がある。

- SaaS
-
-
-
-
-
- SLA
-

(6)セキュリティに関する留意事項

SaaS 提供者の選定には、JIS Q 27001：2006（ISO/IEC27001:2005）の要求事項を基本としたセキュリティ対策が求められる。更に Web 脆弱性検査など、第三者による安全性検証試験／セキュリティ診断も必要である。具体的な施策策定においては、以下の点に留意すべきである。

-
-
-

(7)運用管理面の留意事項

SaaS の運用管理部門は、サービスの導入に際して以下の手順で管理監督を行う責任がある。

① 導入のための事前検討、デモ版試用段階

SaaS 導入の事前準備として、以下の項目について検討を行う。

-
-
-
-
-

② 小規模導入段階

SaaS を小規模に導入するために、以下の項目を実施する。

-
-
-
-
-

③ 利用開始／全社展開

SaaS の利用開始、全社展開を行う。更に必要に応じてカスタマイズを行う。

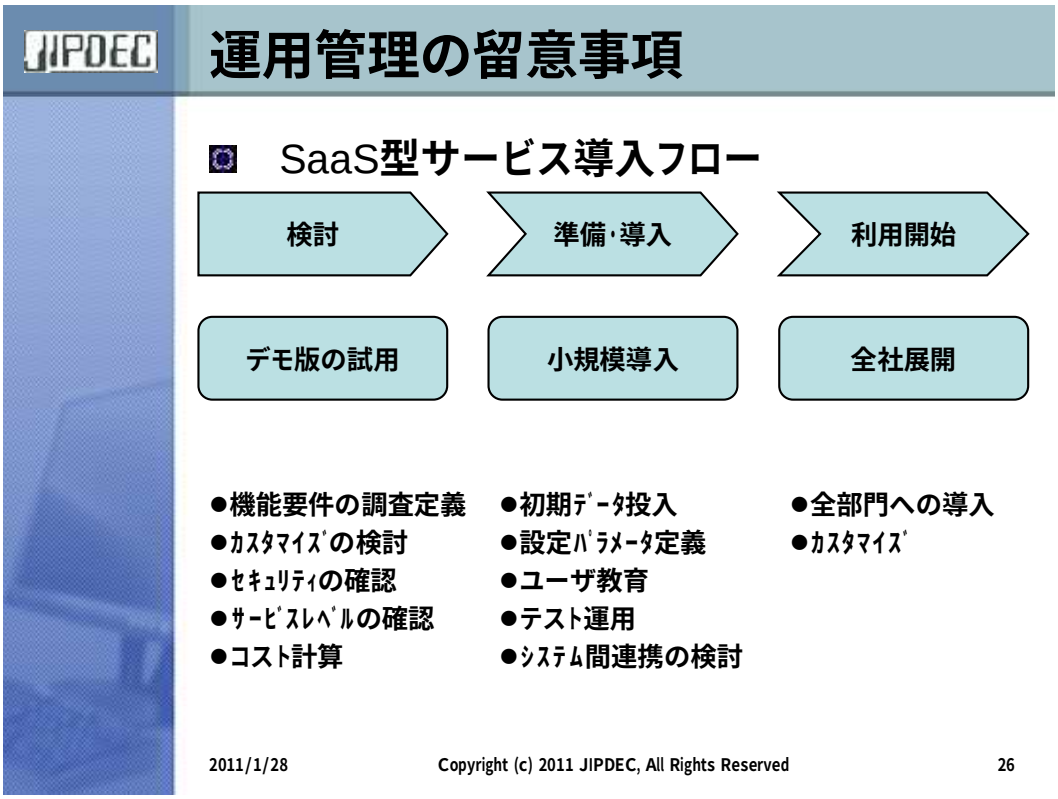


図 4.6　SAM 運用管理の留意事項

(7)クライアントが仮想化デスクトップサーバー（DaaS）を利用する場合

　業務で仮想化デスクトップサーバー（DaaS）を利用する場合、サーバー上に集約されたデスクトップ環境をクライアントに配信することになる。その際の基本的な留意点についても検討したが、結果は SaaS とほぼ同様であった。

●
●
●
●

(8)まとめ

　クラウドは多くのユーザーメリットが見込まれる反面､企業の IT 部門の関与の薄さから、全社の IT 管理が疎かになり、企業の IT が以下のようにサイロ化するおそれがある。

● IT
●
● IT

SaaS 導入における手順を疎かにすることにより、再び企業 IT をサイロ化することは許されない。

4.2.4 OSS 利用時の SAM の留意点

(1)OSS の定義

OSS とは、「ソフトウェア著作者の権利を守りながらソースコードを公開することを可能にする」というオープンソースの概念に基づき、ソフトウェアのソースコードが無償で公開され、改良や再配布を行うことが誰に対しても許可されているソフトウェアのことである。

Open Source Initiative（OSI）では、「オープンソースの定義」（OSD：Open Source Definition）と呼ばれるライセンス文書を策定、公開しており、当ライセンスに準拠していると認められたソフトウェアに対して「OSI 認定マーク」を与える活動を行っている。

［オープンソース・ライセンスの要件（出典：The Open Source Initiative)］

-
-
-
-
-
-
-
-
-
-

本来ソースコードは著作者の知的財産であるため、内容は秘匿され、アクセスは制限される。これに対して、OSS ではソフトウェア著作者の権利保護とソースコード公開の両立を理念としている。すなわち、OSS では誰もが改良や再配布を行うことができる。そして、ソースコードはみんなの共有財産であり、改良を重ねて、よりよいソフトウェアを育むことを理念としている。

(2)代表的な OSS

代表的な OSS としては Linux を挙げることができる。Linux は改良が進められ、現在では幅広い領域で高い市場占有率を獲得するに至っている。また Linux ディストリビューションと呼ばれる商用パッケージソフトウェアとしての応用も活発に行われている。

Linux の他にも、Web サーバーの Apache、データベース管理システムの MySQL、プログラミング言語の Java、統合開発環境（IDE）の Eclipse、スクリプト言語の Perl、PHP、Python、Web ブラウザーの Firefox、といったソフトウェアが OSS として提供されている。近年では、IT ベンダーが OSS のコミュニティに参加し、開発活動に参画する例も増えている。

表 4.2　OSS の分類

分野・領域	ソフトウェア名称
オペレーティングシステム	Linux
ウェブサーバーソフトウェア	Apache
データベース管理システム	MySQL
プログラミング言語	Java
統合開発環境	Eclipse
スクリプト言語	Perl
ウェブブラウザー	FireFox

(3)クラウド育ちの OSS

近年クラウドの世界で新型 OSS が広く活用され始めている。過去の OSS が各分野の代表的な商用ソフトウェアをキャッチアップすべく機能強化してきたのに対し、これらの新型 OSS はクラウド技術（仮想化、システム監視、認証基盤、分散処理等）のベースとなっていることが特徴である。代表的なものを以下に示す。

表 4.3　新型 OSS の分類

分野・領域	ソフトウェア名称
仮想化機構	Oracle VM VirtualBox, KVM, Xen, Citrix Xen Server
システム監視・管理	Groundwork Monitor, ZABBIX, Hinemos, Nagios, Xymon, Virt-manager, oVirt, Eucalyptus, Proxmox Virtual Environment, ConVirt, OpenNebula, Nimbus
利用者向け認証基盤	OpenSSO, Shibboleth Higgins, SimpleSAMLpho, OpenDS, OpenLDAP
分散処理基盤	Hadoop, SkyNet, Gfram, CouchDB, Hbase, Hypertable, Voldemort, Cassandra

(4)OSS のライセンス概念

OSS のライセンスは、一定の条件下でソフトウェアの使用、複製、改変、再頒布を認めている他、以下の二点がほぼ共通している。

①無保証であること

オープンソースのソフトウェア（複製物、二次的著作物）は元の著作者も制御できない形で流通するため､著作者は当該ソフトウェアについて動作保証をしないのが通例である。また、その動作の結果何らかの損害をもたらしたとしてもそれを保障しないものと定めている。

②著作権表示を保持すること

オープンソースの著作者は一定の条件下で自由な利用を認めているのであり、著作権を放棄している訳ではない。そのため多くのライセンスは適切な形でソースコードや付属文

書に含まれる著作権表示を保持することを定めている。

(5)OSS 利用企業の増加と OSS ライセンスに関する誤解

OSS 利用企業は全体の 7 割弱に達しており、いまや OSS はビジネスに広く利用されている。そして従来は OS やサーバー系ミドルウェア中心であったが、近年は ID 認証、シングルサインオン、オフィスソフトウェアといったアプリケーション領域で OSS が本格化してきている。また前述のようにクラウド育ちの OSS が増加しており、仮想化技術や SaaS の提供において広く OSS が活用されている。

その一方で、OSS について著作権を放棄したソフトウェアであるという誤った考えから、ソフトウェア資産管理（SAM）の管理対象ではないと誤解しているケースが多く見受けられる。

(6)OSS におけるライセンス違反の例

一般的なソフトウェアにおけるライセンス違反例としては、著作者（多くはソフトウェアベンダー）の許諾なく、複製、譲渡、貸与等されたソフトウェアを使用する行為を指す。

これに対して OSS では、組織が OSS のソースコードを入手し、自社のコンピュータ上で使用することは合法である。そして、組織が入手した OSS の複製物を、「受け取った通りの形」で複製・再頒布することも可能である。しかしながら、OSS が定めた複製条件に従わず、複製した OSS を外部の組織に再頒布することは禁止されている。

(7)OSS 利用時におけるその他の留意点

ライセンス違反以外の OSS 利用時における SAM の留意点をについて述べる。

① OSS には管理者権限がなくてもインストールできるものがある。

組織が、従業員によるインストール行為を制限するために管理者権限を限定している場合であっても、当該 OSS はインストールできてしまう。

② インベントリー情報収集ツールで情報が取れないものがある。

OSS の中には、OS のインストーラーを介さずインストールされるものがあり、その場合はインベントリー情報収集ツールによるソフトウェアの棚卸に支障が生じる可能性がある。

4.2.5 まとめ

以上が、クラウド・コンピューティング時代の SAM の考え方に関する検討結果である。以下、本稿の要点をまとめる。

●

●

- IT
  IT

-

4.3 JIS X 0164-1 から見た SAM ユーザーズガイド活用方法とクラウド時代のソフトウェア資産管理

4.3.1 はじめに

2009 年から財団法人日本情報処理開発協会（JIPDEC）の「ソフトウェア資産管理評価検討委員会」において SAM ユーザーズガイドの作成や来るべくクラウドや仮想化時代に向けてのソフトウェア資産管理の在り方など様々な議論および研究を行ってきた。また、全国各地における SAM の普及啓発活動の一環としてシンポジウムやセミナー等も開催し、委員一同「ソフトウェア資産管理（SAM）」という側面から、日本の IT サービスマネジメントおよび情報セキュリティの発展向上に寄与できればと考えている。

この度、筆者が平成 23 年 1 月 28 日に行われた「JIPDEC 情報セキュリティ総合的普及啓発シンポジウム」にて発表する機会をいただいたので、その内容およびクラウド時代のソフトウェア資産管理と絡めていくつかの提言をさせていただきたい。

4.3.2 近年における SAM の動向

まず近年における SAM の動きを簡単に振り返ってみると、日本では 1995 年の経済産業省によるソフトウェア管理のガイドライン策定に始まっている。一方、欧米においても 2000 年に ISO/IEC の SC7[3] にて SAM の標準化が提案された。翌年 2001 年には SAM のプロセスを審議する WG 21 が SC7 配下に設立され、本格的な SAM 標準化への議論が始まった。2003 年には ITIL の基本プロセスの中に SAM が定義されるなど、横断的にその動きは徐々に拡大していき、2006 年 5 月についに ISO/IEC 19770-1 として SAM プロセスが国際標準として規格化された。日本においても、ソフトウェア資産管理コンソーシアムにおいて SAM の管理基準や、評価規準をいち早く策定しており、ISO/IEC 19770-1:2006 の発表後、ISO に対応する形で 2007 年に管理基準 Ver 2.0 を、2008 年に評価規準 Ver 2.0 をそれぞれ発表した。その後、BSA や ACCS といった団体の SAM の普及啓発活動もあり、現在の日本の企業や組織において、ソフトウェア資産管理コンソーシアムの管理基準を参考に SAM の体制構築を実施しているところは多い。

そして、2009 年には JIPDEC ソフトウェア資産管理 評価検討委員会が発足し、有識者メンバーによる本格的な SAM の普及にむけての議論と SAM 事業者の成熟度評価へ向けての在り方などが研究されてきた。また同年 11 月には ISO/IEC 19770-2 ソフトウェア識別タグの標準化提案が規格化され ISO の活動も広がりを見せてきている。さらに 2010 年 1 月に JIPDEC の SAM ユーザーズガイド[4]の発行、5 月には待望の日本工業規格 JIS X 0164-1:2010[5] が制定され今日に至る。また、同年 12 月には、ソフトウェア資産管理 評価認定協会（通称：SAMAC）という SAM の成熟度評価や SAM のコンサルタントおよび SAM 事業者を評価認定する事業を行う一般社団法人も設立され、日本は欧米にも引けを取らない SAM における先進的な取り組みを行っている国となっている。

---

[3] SC7 は、ISO/IEC JTC1 のもとで、ソフトウェアエンジニアリング（ソフトウェア工学、ソフトウェア技術）の規格を担当している専門委員会

[4] SAM ユーザーズガイド – 導入のための基礎 - 日本情報処理開発協会 2010 年 発行 ISO/IEC 19770-1 をベースに、より実践的な解説を踏まえ、SAM 導入におけるポイントを説明しているガイド

[5] ISO/IEC 19770 - 1:2006 国際規格の構成および内容に一致した、SAM の統合されたプロセスを定めた日本工業規格

4.3.3 ISO/IEC 19770 シリーズ

ここでは SAM の国際標準規格である ISO/IEC 19770 シリーズ[6]について、少しおさらいしておく。情報は 2011 年 1 月現在のもので、まだ規格化されておらず未確定のものについては今後変更される可能性があることをあらかじめご了承いただきたい。

- **ISO/IEC 19770-1:2006**

  SAM における統合されたプロセスのベースラインを定める国際規格。ISO/IEC 20000 と緊密な整合がとられている
- **ISO/IEC 19770-2:2009**

  インストールされているソフトウェアを識別するための「ソフトウェア識別タグ」についての規格
- **ISO/IEC 19770-3（策定中）**

  Information technology -- Software asset management -- Part 3: Software entitlement tag
  インストールされているソフトウェアの使用権を識別するための標準化規格（2012 年 発行予定）
- **ISO/IEC CD 19770-1（ISO/IEC 19770-4）**[7]

  Information technology -- Software asset management -- Part 1: Processes and tiered assessment of conformance
  SAM におけるプロセスと適合の段階的評価
- **ISO/IEC 19770-5（策定中）**

  Information technology -- Software asset management -- Part 5: Overview and Vocabulary
  SAM の概要と用語の定義

4.3.4 JIS X 0164-1 から見た SAM ユーザーズガイド活用方法

今回発表したものは、JIS X 0164-1 の規格（表 4.4 を参照）と SAM 導入の実践ガイドである SAM ユーザーズガイドとの間を埋めるための活用ガイド（マッピングガイド）となる。SAM ユーザーズガイドだけでは、JIS 規格の内容を完全には網羅しておらず、規格に準拠した体制構築をするということは難しい。また規格書だけでは、実際にどのように SAM の導入・構築を実施していくのかが分からない。という問題点があるので、今回のガイドは JIS X 0164-1 の規格と SAM ユーザーズガイドの関連を明確にし、規格の要求事項を実現するために、どのようにガイドを活用していけばいいかということを検討し、取りまとめたものとなる。

---

[6] ソフトウェア資産管理（SAM）のための統合されたプロセス群のベースラインを定める国際規格。ISO/IEC 20000 と緊密な整合がとられており、ISO/IEC 20000 の IT サービスマネジメントを支援することを意図している。

[7] ISO/IEC 19770 – 1:2006 に ISO/IEC 19770 – 4 として計画されていた Tired Approach（適合の段階的評価）を統合し、あらたに ISO/IEC 19770 – 1:20XX として規格化することが検討されている

表 4.4　JIS X 0164-1 の構成

4.3.6 マッピングガイドの使い方

マッピングガイドの想定する利用者としては、SAM の基本的知識をもち、規格および SAM ユーザーズガイドの内容理解ができて、JIS 規格に準拠した SAM を構築または改善しようとしている人で、利用方法としては、JIS 規格の要求事項およびポイントの理解や、SAM ユーザーズガイドの項目と合わせた活用を想定しており、まさに JIS 規格に対応した SAM ユーザーズガイドを活用するための手引き書的な位置づけとして作成されている。ただし、JIS 規格に関する要求事項は必ず JIS 規格本文を参照するようにして欲しい。尚、このマッピングガイドを参照し SAM の体制構築を実施しても JIS 規格に準拠していることを保証するものではないことはご承知おき願いたい。

4.3.7 従来の資産管理とソフトウェア資産管理のあるべき姿

先進的な組織はすでに SAM の体制構築をすませ、運用管理を回している段階になっているところもあるだろう。しかし、SAM をまだ従来型の資産管理と混同している組織も少なくない。従来型の資産管理とは、いわゆるハードウェアがコストの中心であり、ソフトウェアはハードウェアに付属（バンドル）されている時代の管理方法を指す。TCO（Total Cost of Ownership：総所有コスト） の中心は当然ハードウェアとその運用管理・保守という観点となり、SAM の各プロセスについては必要最低限のものをアドホックに対応している形が多い。しかし、現在の TCO は実はハードウェアよりソフトウェアの価格の方が高くなっており、さらにハードウェアとソフトウェアを合わせたコストより、それら IT 資産に関わる導入・運用管理・保守・教育といった間接コスト全般にかかる方が多くなっている。本来の SAM を実施している組織は、その事実を的確に受け止め、理解しているからこそ、取得・展開・教育・変更・廃棄といったソフトウェアのライフサイクルを軸とした管理を行っている。CIO など経営層がそのことをいち早く理解し適切な SAM の体制構築を行うことで、IT 資産全体が戦略的に利活用され、結果競争力も高めることができる。

4.3.8 組織における重要課題と SAM の関連性

SAM は組織おける重要課題である、情報セキュリティや IT ガバナンス、コンプライアンスといった重要事項と密接関わっていることを忘れてはいけない。例えば、情報セキュリティという面では、普段はオフラインとなっているために把握していなかった PC がいつの間にか紛失してしまっていたり、管理しきれていないフリーウェアやシェアウェアなどのソフトウェアから情報漏えいが発生したり、情報セキュリティ上の問題と SAM は深く関わっている。また、IT ガバナンスという面では、誰がどの PC で何のソフトウェアを利用しているのかもわからない状態で IT 統制できているということは言えないだろう。

その他にも、組織における最適な調達が行われているかどうかという視点や、ソフトウェアや IT 資産の標準化によりサポートコストやトラブル対応コストを最小限に抑えるという部分にも SAM は密接に関わっている。

4.3.9 これからのソフトウェア利用形態

図 4.7 は、ソフトウェアの利用形態における過去・現在・未来を表したもので、ステージ 1 としては、ソフトウェアは PC と一体で管理するプレインストール型やパッケージソフトウェア型の利用形態を表している。次のステージ 2 は、組織など多数の PC で利用す

ることを前提としたボリュームライセンス型の利用形態を表す。現在の多くの組織においては、このステージ 2 の段階にあると考えられる。そして今後の利用形態として、クラウドやソフトウェアをサービスとして利用する形態が今後増加することを考えると、既存のソフトウェアの利用形態とクラウドなどサービスとしてのソフトウェアの利用形態が混在するステージ 3 に多くの組織が置かれることになる。ステージ 4 については、従来型の利用形態をなくし、クラウドまたはサービスとしての利用形態のみの状態を想定している。組織で利用するソフトウェアがすべてクラウド上もしくはサービスとして提供されるインフラが整ってからの話ではあるが、ソフトウェア（サービス）が電気やガスのように組織運営のインフラとして必須のものとなると仮定すれば、ソフトウェアを保有するという形から、利用するという形だけで運用する組織も、そう遠くない未来に出てくるだろう。

図 4.7　ソフトウェア利用形態（過去、現在、未来）

4.3.10 まとめ

最後に提言事項としていくつかの内容を記載したい。今後、ソフトウェアはクラウド化、仮想化での利用が急速に進むことで利用形態がより複雑に多様化することが考えられる。すでに IT 資産の可視化を適切に行い、その管理プロセスも構築できている組織はまだ対応する方法があるが、現時点で従来型の運用管理しかしておらず、本来の SAM を実施していないことによる潜在的なリスクを抱えている組織は、クラウド化や仮想化が本格的に浸透する前に、まずは正確かつ網羅的な IT 資産の把握・可視化および管理体制の構築を実施することが必要となる。

また、SAM の認証という面でも、欧米をはじめ（日本においても SAMAC という団体の設立もあり）徐々にその動きが見られる。国際規格の要求事項を満たす管理体制を構築している組織がその認証を受けられる可能性も大いに出てきた。SAM という概念が情報セキュ

リティや IT サービスマネジメントと同じく、正しく運用され、適切に認証されることで、これまで以上に IT を利活用する組織が競争力をつけ、世界においても信頼されリーダーシップを発揮する時代がもうそこまで来ている。

4.4 富士通における SAM の事例

4.4.1 はじめに

ソフトウェア資産管理（SAM）の一般企業における取組ということで富士通の事例を紹介する。富士通では、1990 年代の後半から、全社的なソフトウェア資産管理に取り組んでおり、一定の成果をあげた。以下でその取り組みの概要を説明する。また、近年のソフトウェア資産管理に対する問題点について、特にクラウド・コンピューティングに伴うものについて説明する。

4.4.2 経緯

社内に散らばっているパーソナルコンピュータ(以下、PC と呼ぶ)の全社的な管理の必要性が特に叫ばれたのは、1990 年代のことである。

当時、全社システムはクライアントとホストコンピュータが分散して処理する、いわゆる、クライアントサーバシステムが全盛の時代であり、情報システム部門が各職場に数台の PC を専用の端末として配置していた。これらの端末には、クライアントサーバーのためのソフトウェアの他に OA 業務を支援する表計算や文書作成用のソフトウェアが一緒に展開された。一方、部門では、ホワイトカラーの業務を支援するために PC が独自に導入され、多くの従業員が一人一台の利用を行い始めていた。必然として、個人の利用している PC からも全社システムを利用したいということが要求されたが、情報システム部門は、一人一台で利用されている PC がどんなソフトウェアを利用していて、全社システムとの互換性が保証されているのかどうか、また、いったい何台の PC が利用されているのかも分からないといった状況であった。

このような環境で、1997 年にコンピュータウィルスによる感染と Microsoft Word のバージョンアップによる非互換問題が発生した。CIO を中心とした委員会でこの問題が報告され、この際、コンピュータウィルス対応のソフトウェアと Microsoft Office の最新バージョンのライセンスを全社の PC 台数分購入して配布しようということが審議された。

購入に際して、先ずは現状のライセンス購入状況を調査しようということで調べてみると、既に数量的には十分な数のライセンスがあることが分かった。ところが、現場にはそれらがインストールされていない PC が沢山散見された。原因を調べると、各部門、各業務システム（人事、総務、経理、生産管理など）の主管元ごとにライセンスが購入され、購入していない部門もあるが多めに買っている部門がある。また、ライセンスは購入したものの実際の展開は数か月先という有様であった。この経験から、導入されている PC の実情を全社的に把握することが重要であるとの認識に至った。

ことの発端は、全社システムとの互換性や現場の PC の問題に起因するものであるが、結果として、ライセンスコンプライアンスや無駄の解消にもつながる重要な取り組みとなった。

4.4.3 現状の SAM の仕組み

さて、SAM に取り組み始めて十数年になるが、年々、レベルが上がってきている。ポイントとなるのは、やはり利用者の意識であり、特に、セキュリティとか情報漏えいに関す

る従業員教育とともにライセンスに関するコンプライアンスの意識が常識になりつつあることがあげられる。ここで、当社の SAM の仕組みについて簡単に触れておく。

PC の状況を把握する方法としては、その都度手動で調査する方法とツールで PC の状況を自動的に調べ、ネットワークを経由してサーバーに送信し、サーバーで調査する方法がある。数万台という PC を手動で調査することは無理であり、その労力と即時性を考慮し、ツールによる自動収集が採用された。いわゆるインベントリ収集である。インベントリは、レジストリの情報だけでなく、ファイルやファイルヘッダー情報も必要であった。これは、当時(現状もそうであるが,ISO/IEC 19770-2:2009 で世界標準としての規格は制定された。)PC にインストールされているソフトウェアを識別する共通のルールが定められていなかったことが原因である。とにかく、インベントリを集めたサーバーでソフトウェア毎に識別する必要があった。その方法を記述した辞書をサーバーに持ち、自動的に突合せが行えるようにすることは、労力を削減するための必然的な防衛手段であった。インベントリが自動収集できないコンピュータに対しては、オンラインで利用ソフトウェアを登録できる仕組みを提供した。

一方、購入するライセンスは、部門でばらばらに購入すると以前と同様な状態になってしまうので、これを禁止している。稟議取扱い部門や購買部門の協力を得て、個別購入を原則禁止とし、その代わり、年 2 回、知的財産費用（OA 関連のソフトウェア購入費）を全社稟議とし、利用部門は、部門の承認で直ちにソフトウェアを導入できるようにした。ソフトウェアベンダーに対しては、月次で使用しているソフトウェアの数と保有しているライセンス数の差で購入できるような契約にしてもらった。こうすることで、月次の集計による実績ベースの購入が可能となる。各利用者（利用部門）には、購入金額をライセンスの不足数で割った単価で費用を計算し自動的に月次で配賦している。

これらの試みは、ライセンスのコンプライアンスとソフトウェア購入費用、事務手続きを大幅に改善した。センターサーバーにクライアントの情報がリアルタイムで収集されていることは、PC のセキュリティ向上に対しても多大な貢献をしている。

これらの前提となるのは、センターサーバーに社内の全クライアントの情報が正確に記録されていることである。このために、SAM に関する規定や運用についての告知と公開（当社では WEB システムで公開されている）が行われ、インベントリ更新状況の公開、部門管理者又は幹部への通知、各期の棚卸と監査、利用者のコンプライアンスに関する教育の徹底などが行われている。

4.4.4 クラウド・コンピューティングの心配

さて、現状の PC の利用に対して紆余曲折はあるものの曲がり形にも SAM に通じる取り組みを行ってきたが、最近のクラウド・コンピューティングの進展について心配がある。

スピーディに導入できることから、クラウド・コンピューティングの業務システムへの浸透は予想以上に早くなると予想される。もう一つ、クラウド・コンピューティング環境を利用して、数十 GB のディスクを無償でサービスするところも出てきている。SAM の観点でこの状況をどうするかということが問題になる。

先ず、業務システムへの浸透についてだが、内部統制に関係のない業務システムは、パブリックなクラウド・コンピューティングを利用されるかもしれない。通常のシステムは、サーバーやネットワークが特定できるようなプライベートなクラウド・コンピューティン

グが利用されるであろう。少なくとも現行の規制では、データがどこの国のサーバーに格納されているかわからないようなクラウドサービスを利用することはできないのである。こう考えると ICT のハードウェアインフラについては、運用を信頼のおけるクラウド業者に任せることで、情報システム部門は、インフラの運用という非常に労力のかかる仕事から解放されるであろう。

ソフトウェアに関してはどうであろうか。現状のクラウド業者の殆どはソフトウェアのライセンスに関して利用者責任にしている場合が多い。ミドルウェアソフトなどは特に管理が難しく、ユーザーの知らないうちにライセンス違反を起こしている場合が多々ある。SaaS 費用の中に全てのアプリケーションのライセンスが含まれているのであれば良いが、利用者任せということになれば簡単ではない。クラウド・コンピューティング環境では、その特徴であるプロビジョニング機能により、使用 CPU が変化する。利用者が持ち込んだアプリケーションはこういったことを想定して管理されなくてはならない。また、クラウド・コンピューティングの世界では OSS（Open Source Software ）を利用することも多くなるが、これらも自己責任で管理しなければならない。結局、サーバーのソフトウェアの管理が非常に複雑で難しいものになる。

クライアントのコンピュータに関しても大きく様変わりする。現在、情報漏えいを防止するため、PC の持ち出しが制限されている。置き忘れや盗難の可能性を考えるとこういった規制に走りやすいのだが果たして妥当な策と言えるのだろうか？ SNS が提供する大規模なディスクスペースを利用して情報交換し始めた利用者もいるのではないか。

このような問題を解決する手段として、シンクライアントの形態、DaaS を導入することや大規模なプライベートなディスクスペースを導入することは非常に有効である。ただ、この場合も殆どが、OS も含め利用者責任でソフトウェアのライセンスを管理しなければならない。ましてや一挙にシンクライアント化する筈はなく、当面、ディスクを持った PC とシンクライアントが共存する。

IT 資産の管理がやっと落ち着いたと思ったら、今度は、クラウドサービスの管理と利用者の管理、ユーザーと業務システムのインタフェースとなる各種デバイスの管理が必要になる。本当にクラウド・コンピューティングの導入で SAM が楽になるのであろうか？

4.4.5 クラウドサービスに期待すること

原点に返り、何故、SAM に取り組むのかということをもう一度考えてみよう。企業としては ICT をビジネスの世界にうまく利用して、最大の効果を挙げたいと思っている。色々な革新的なビジネスチャレンジや企業改革は、トップ又は組織のアイディアが如何に早く組織全体に伝わり、ビジネスのプロセスに定着していくかが重要な成功要因となる。この点を最も効果的に支援するのがこれからの ICT であると考える。そのためには、誰が（どの組織が）、どこで、何のために、何を使っているかということを正確に掴んで利用者（組織）を支援する組織として情報システム部門が重要な役割を果たす。このように考えると SAM への積極的な取り組みは、単にライセンスコンプライアンスのためにだけあるのではないことは明白な事実である。

クラウド・コンピューティングがこれからの ICT の本命になるために期待することを最後に上げておく。

- クラウドサービスは同時アクセスを許さない ID 単位ですべてのサービスを取り込

んだ課金にすること。

- サービス業者は ID 単位にどういったサービス（アプリケーション）をいつどれだけ使ったかをリストとして顧客に提示すること。
- サービス業者がすべての権利（サービス）を最も安価で提供できるようにソフトウェアベンダー，その他と交渉すること。
- OSS を利用する場合には，注意事項を明確にし、利用者に提供すること。
- サービス業者は、常にユーザーへのサービスが最大の投資効率を発揮できるようにユーザを支援すること。

4.5 ソフトウェア資産管理とクラウド～パネルディスカッションから～

4.5.1 はじめに

IT 資産管理の基盤プロセスであるソフトウェア資産管理は、従来の目的である単なるライセンスコンプライアンスへの対応だけでなく、情報セキュリティの維持向上、IT 統制の基盤強化へつながるものであるとの認識が広がりつつある。

しかしながら、こういった観点でのソフトウェア資産管理への取り組みは、まだ緒に就いたばかりであり、従来の、単なるライセンスの数合わせにとどまっている組織は少なくない。

一方で組織には、SaaS や PaaS などのクラウドサービスや仮想化という新しい仕組みが導入されつつある。

このような状況下、ユーザーからは、ソフトウェア資産管理に関連する団体や専門家に対し、「どのようにソフトウェア資産管理に取り組んでゆくべきなのか？」、「クラウドになれば、ユーザーとしての管理義務は大幅に削減されるのではないか？」といった問い合わせが非常に多く寄せられるようになってきている。

今回のパネルディスカッションでは、ソフトウェア資産管理を組織が導入する際のメリットを改めて考えるとともに、クラウド時代を迎えるにあたって、どのようなことを考えていくべきなのかについて、SAM に造詣の深いユーザー、ベンダー、監査会社をパネリストに招き、全方位的に意見交換を行った。

これまで、このように立場の異なる人々が一堂に会し、ソフトウェア資産管理に関する意見を述べたことはなく、立場の違いを超えた、ソフトウェア資産管理の普遍的なメリットについて、また、クラウド時代におけるソフトウェア資産管理の注意点や有効性について、指針となる意見が出されたように思う。

（パネリスト）
・宮崎県 県民政策部 情報政策課 課長 金丸 裕一氏
・富士通株式会社 フィールド・イノベーション本部 第一 FI 統括部
ディレクタ 高橋 快昇氏
・アドビシステムズ株式会社 ライセンスコンプライアンス管理部
シニアマネージャー 宮澤 啓一郎氏
・マイクロソフト株式会社 ライセンスコンプライアンス推進本部 本部長 相田 雄二氏
・有限責任監査法人トーマツ エンタープライズリスクサービス部
パートナー田村 仁一 氏
（モデレーター）
SAM 評価検討委員会委員長 篠田 仁太郎（株式会社クロスビート）

パネリストとして貴重なご意見をいただいた皆様には、ここで改めてお礼を申し上げたい。

今回のパネルディスカッションのアジェンダは次のとおり。
1）それぞれの立場から見たソフトウェア資産管理とは？
2）ソフトウェア資産管理の現状
3）ソフトウェア資産管理の動向
4）ソフトウェア資産管理の導入と運用のポイント
5）クラウドにおける SAM

以下に詳細を記載する。

4.5.2 ディスカッションの内容

１）それぞれの立場から見たソフトウェア資産管理とは？

ユーザーの立場では、上述の通り、未だに「ソフトウェア資産管理は、ライセンスコンプライアンスに対応するための施策であり､ベンダーの権利保護のために行うものである」とする人は多い。

しかしながら実際にソフトウェア資産管理に取り組んだユーザーであれば、ソフトウェア資産管理を行った後にもたらされる利益は単なるライセンスコンプライアンスにとどまるものではなく、金丸氏や高橋氏のいうところの「コストや資源の最適化」であったり、「情報セキュリティの向上」というものに寄与するものだということが理解されるようになる。

これについては、昨年の事例紹介にもあったヤマハ発動機も同様の意見だった。また、田村氏からは、IT ガバナンスのためにも、ソフトウェア資産管理は有効だとの指摘もあった。

IT 資産の管理は、IT ガバナンスの基盤であり、その基盤を盤石なものにするためにソフトウェア資産管理のプロセスは、非常に有効なものとして認識されているという。

一方で、ベンダーがソフトウェア資産管理を促す理由は、相田氏、宮澤氏によれば､「著作権の保護に対する意識の醸成」と「コストの削減」ということになる。「著作権の保護に対する意識の醸成」は、単にベンダーの利益を守ることを指しているのではなく、日本として､知的財産を生み出し守ってゆく社会を築くという､社会的意義を持ったものである。

また、実際にソフトウェア資産管理を進めていくと、適切なライセンスプログラムの導入や、資源配分が促進されることになり、無駄なライセンス投資やハードウェア投資は削減され、結果として「コスト削減」が実現されることになるとしている。実際にソフトウェア資産管理を導入した組織では､特にライセンスへの投資は大きく減少する傾向にある。

以上、立場の違いによるソフトウェア資産管理のメリットについてまとめたが、ここで留意して欲しいのは、ユーザーの立場にせよ、監査会社の立場にせよ、ベンダーの立場にせよ､上述したメリットを得るためには､「ライセンス管理」という狭い範囲での取り組みとはせず、適切に「ソフトウェア資産管理」を行うことが重要だということである。

２）ソフトウェア資産管理の現状

次に、実際にソフトウェア資産管理への取り組みはどのような状況にあるかについて、一般企業、自治体、大学の状況についてそれぞれ伺った。

一般企業の一例として高橋氏からは､「富士通ではかなり効率的で且つ厳しい管理体制が敷かれており、今後は可用性をもう少し意識した仕組みを検討するようなレベルに来ている」との話があったが、残念ながらこのような先進的な取り組みをしている組織は、まだそれほど多くはないであろう。

もちろん、ソフトウェア資産管理に対する意識は、ここ 2 年くらいで急激に高まってきており、これまで以上に管理精度を上げようとする企業も増えては来ている。

しかしながら、ソフトウェア資産管理への取り組みが増えてきたことを目にし、耳にするようになって、ようやくこれから取り組もうとする企業はまだまだ多い。

一方自治体では、いくつかの自治体による損害賠償事件などがあった関係から、ソフトウェア資産管理への注目は一般企業よりも高いようである。

金丸氏によれば、宮崎県ではそういった事件が流れる前からソフトウェア資産管理の強化に取り組もうとしていたとのことだが､当初は､「なぜ使用者が管理しなければならないのか？」という意見も出たほど、自分たちで使用しているソフトウェアの「管理」に対する意識は全庁的に低かったという。

それは､「改めて管理強化をせずとも、十分に管理はできているはずだ」という意識があったことにもよるそうである。

しかしながら、実際にソフトウェア資産管理の導入を始めてみると、様々な事象が発見され、管理状態は残念ながら想定していたレベルには程遠いものだった。そういったこと

が可視化されたことで、県の中でも、ソフトウェア資産管理は重要だとの認識は高まり、プロアクティブに取り組むべきものとの意識が高まっているという。最近では宮崎県のこういった取り組みは、他の自治体にも注目され、現在、多くの問い合わせを受けている。

大学については、宮澤氏より、「職員・学生・共有 PC についての管理はだいぶ進んでいるものの、研究室で利用されているものについては、管理が行き届かないケースがまだ多いようだ。」との話があった。研究室で利用されているソフトウェアや PC は多岐にわたっており、且つ試験的に使用されるものも多いため、そこにソフトウェア資産管理を浸透させることは、これまでのところは難しかったのではないかとのことだった。
しかしながら、研究室こそ、情報セキュリティ上も、知的財産の保護のためにも、ソフトウェア資産管理の導入は必須であり、大学側にもこういった意識は醸成されつつあり、現在、複数の大学で、学校を上げての取り組みが始まってきている。

３）ソフトウェア資産管理の動向
ISO/IEC19770 を検討する WG21 の主査も務める高橋氏によれば、ISO/IEC19770-1 は現在、ソフトウェア資産管理の構築を 4 段階に分けて検討できるプロセスに改変中とのことであり、今後は、この 4 段階に分けた形で認証していく仕組みを検討している国もあるという。
また、2009 年 12 月 1 日には、インストールされているソフトウェアのベンダーや名称、バージョンなどを明確にするためのタグ標準となる ISO/IEC19770-2 が発行しており、現在はさらに、ISO/IEC19770-3 として、どのようなライセンスに基づくものがインストールされているのかを明確にするためのタグ標準も検討されている（アドビシステムズではすでに新しいバージョンでは、ISO/IEC19770-2 に対応しているとのこと）。

こういった動きは、ユーザーのソフトウェア資産管理を効率化するものであり、歓迎される動きであろう（ISO/IEC19770-2 については、対応しているソフトウェアベンダーはまだ少ないものの、米国の軍にて採用が決定したとのことであり、今後、対応するソフトウェアベンダーが増えてくることが予想される）。

このようにソフトウェア資産管理に関する規格が整理・整備されつつある中、米国の団体である IAITAM や IBSMA、イギリスに本部を置く *it*SMF、米国に本部を置く BSA など、様々な団体が、ソフトウェア資産管理に関連する第三者認証を始めている。日本でも、2010 年 12 月に、一般社団法人ソフトウェア資産管理評価認定協会（以下「SAMAC」）が設立され、組織におけるソフトウェア資産管理の成熟度レベルに対する第三者認定制度や、ソフトウェア資産管理の導入知識を保持していることを認定するための仕組みが本格的に動き始めている。

金丸氏によれば、実際に地方自治体でソフトウェア資産管理の導入作業に関する委託業務の入札をかけた場合、どの組織がそういった知識やノウハウを持っているのかを確認することは非常に困難であり、場合によっては、なんらノウハウを持たない組織が落札し、失敗してしまうケースも考えられるという。特に地方自治体においては地場業者に発注するケースが多く、広く日本全体で、その能力を持っている業者を探すことはできない状況にあるため、地場業者にそういった知識を持たせる、または持っていることを証明できるような仕組みを確立してもらえたら良いのではないかとの意見もあった。

先述した、SAMAC による活動も待たれるところだが、当ソフトウェア資産管理評価検討委員会としても、こういったユーザーの声に応えられるようなガイドラインの作成、制度の構築について引き続き検討していきたい。

４）ソフトウェア資産管理の導入・運用の際の注意点
次に、実際にソフトウェア資産管理を導入する場合また、運用をしていく場合にどのような点に注意をする必要があるのかについて、話を伺った。

金丸氏によれば、導入で最も注意をしなければならないのは、現状把握の準備であるという。当初宮崎県では２か月の準備期間を設けていたが、実際に始めてみると、想定外の

事象が多数発現、発見され、十分と考えていた準備期間は、1 か月程度足りなかった。その結果、準備が整いきらず、作業の手順やスケジュールを修正しながらの現状把握となってしまったとのことだ。そして、現状把握の作業の中で最も大変だったのは、保有ライセンスの確認であったという。

特にパッケージソフトウェアについては、どのようなライセンス媒体が組織に存在しており､何を保有していればライセンスされていることを証するのかなどを確認する作業は、非常に手間がかかるだけでなく、調査のレベルを均質にする（調査者による“ゆらぎ”を生じないようにする）ことが難しかったとのことである。

また、現状把握の作業開始前に、サンプリングでいくつかの部門に対し、想定した調査手順を実施し、修正をしておくことが重要だという。金丸氏のこれらのコメントは、どのような組織にも言えることで、現状把握を始めようとする組織には、是非参考にしていただきたい。

また、運用において金丸氏は､「初めから 100 点を目指すべきではない」という。0 から 100 点を目指したのでは、運用の負荷もコストもかかりすぎてしまう可能性がある。100 点はゴールであり、まずはその手前に及第点を設定し、そこに向かうことが必要ということである。これには田村氏も同様の意見であり、現状やりうる、またやるべきレベルから運用を開始するのが良いとしている。ただしここで注意しなければならない点は、現状把握においては 100 点を目指すということである。現状が正しく把握され、認識されなければ、その先のスコープや管理方針、運用施策を策定することはできない。

ここで特に気を付けたいのは、有償ソフトウェアだけを先に把握しようという考え方である。組織で使用されている数千種類、数万種類のソフトウェアから有償ソフトウェアだけを抜き出すことは難しく、結局一部のソフトウェアだけを対象にすることになってしまう。その結果、本来セキュリティ上も著作権法上も厳しく管理されるべきソフトウェアが管理対象から漏れてしまっていることにも気づけないという事態が容易に起こりうることになる。現状把握では確実に 100 点を取ることをめざし、さらにその先の運用をどのように行うかを検討しておくことが重要である。

高橋氏は運用を効率的に行うための施策として重要なのは､管理部門に任せきりにせず、常に見直し、改善するための仕組みを構築することだという。

そのためには､SLM を導入しやすい外部委託を検討することも一つの方法であるとした。

マイクロソフトの相田氏からは、ライセンスの調達に関し、調達先（パートナー）任せにしてしまうのはよくないとの話があった。パートナーにすべてを任せきりにしてしまうことで、パートナーによるオーダーミスやキッティングミスによる発注内容とは異なるライセンスやソフトウェアが納品されてしまう事象も起こっているという。発注したライセンスが正しく納品されているかについては、自らが確認するプロセスを持つことが重要であり、さらに、パートナーの能力を見極める知識も、ユーザーは持った方が良いということである。

以上から、ソフトウェア資産管理の導入と運用のポイントは、

・余裕をもって 100 点を撮るための現状把握を行うこと。
・組織の現状に見合った管理レベルを設定し、運用を始めること。
・改善するための仕組みを持つこと。
・他人任せにせず、自らが実施内容を確認する仕組みを持つこと。

という 4 点にまとめられる。

５）クラウドにおける SAM

これまでは、どちらかというとオンプレミス型に対するソフトウェア資産管理の話をしてきた。これに対し、クラウドとなった場合には、どのようなソフトウェア資産管理が必要になるのか？また、ユーザーのソフトウェア資産管理業務自体は、簡単になるのか？について話を伺った。

高橋氏からは、企業が一般的に利用しているクラウドは「プライベートクラウド」と呼ばれているものであり、ハードウェアについては借りているものが多いものの、ライセンスについてはほとんどがユーザーが保有しているものであり、(「プライベートクラウド」においては）現時点ではユーザー自身が管理、コントロールしなければならないという。

金丸氏は、自治体においては、国内法が適用される IDC を利用しなければならないため現時点では利用できるサービスが限定されること、また、すべてのシステムがクラウド化できるものではないということから､混在環境となり､管理はより複雑化するとみている。

相田氏もソフトウェアベンダーとして、クラウド型とオンプレミス型のミックスが続くと話しており、そこにクライアントやサーバーの仮想化技術が加わってくるために、現状把握はより難しくなっていくのではないかという。これらはクラウドに移行することを考えた場合に、非常に重要なポイントであり、組織の IT 環境がより複雑化する前に、現状把握を進めておくことが望まれるということである。

田村氏からは、クラウド化や仮想化は、IT 利用の選択肢を広げるものであり、組織にとって好ましいものではあるが、やみくもに導入するのではなく、組織の状態を見、どこに何をどのように適用していくかについて、リスク分析した上で考えることが重要との話があった。

また、SaaS ベンダーが、すべてを管理すべきであり、ユーザーに負担をかけさせないことが重要との意見も出された。

いずれにせよこういった混在環境は間違いなくここ数年は続くものであり､IT ガバナンスの面からも、混在環境が複雑化する前に、ソフトウェア資産管理に取り組んでおくことが重要であるといえる。

5. ソフトウェア資産管理（SAM）に関する説明会

5.1 実施概要

ソフトウェア資産管理（SAM）に関する説明会を次の概要にて全国４ヶ所で実施した。

① タイトル

－ソフトウェア資産管理（SAM）に関する説明会

② 主催

－財団法人日本情報処理開発協会

③ 後援（順不同）

－特定非営利活動法人　ソフトウェア資産管理コンソーシアム（SAMCon）

－ビジネス ソフトウェア アライアンス（BSA）

④ 開催日時及び開催場所

－札幌：2010 年 7 月 5 日（月）

TKP 札幌ビジネスセンター　カンファレンスルーム 5B（5 階）

（札幌市中央区北三条西 3-1-44）

－大阪：2010 年 9 月 3 日（金）

TKP 大阪梅田ビジネスセンター（大阪府大阪市福島区福島 5-4-21 TKP ゲートタワービル）

－東京：2010 年 10 月 14 日（木）

内幸町ホール（千代田区内幸町 1-5-1）

－福岡：2010 年 11 月 24 日（水）

TKP 博多シティセンター　阿蘇１

（福岡市博多区博多駅前 3 丁目 4 番 8 号 サットンプレイスホテル博多内 5 階）

⑤ プログラム概要

時　間	内　容	講　演　者
13：30～13：35	開催挨拶	財団法人日本情報処理開発協会
13：35～14：05	ソフトウェア資産管理に関する 調査研究の概要	財団法人日本情報処理開発協会 情報マネジメント推進センター 副センター長 高取　敏夫
14：05～14：55	講演 1： 「法律/コンプライアンス面から見た ソフトウェア資産管理(SAM)の必要性」	BSA 日本担当顧問 弁護士 石原　修　氏
14：55～15：10	休　　憩	
15：10～16：00	講演 2： 「SAM 概論／SAM ユーザーズガイドの概説」	ダイヤモンドレンタルシステム株式会社 開発業務部　IT サービス課 課長 島田　篤　氏 --- 有限責任監査法人トーマツ エンタープライズリスクサービス部 パートナー 田村　仁一　氏
16：00～16：50	講演 3： 「事例に基づく SAM 構築の実際」	ソフトウェア資産管理評価検討委員会 委員長 （株式会社クロスビート） 篠田　仁太郎　氏

⑥ 申込者数

460 名

⑦ 参加者

会場/日程	申込者数(A)	参加者数(B)	参加率(B÷A)
札幌　7 月 5 日（月）	113 名	101 名	89%
大坂　9 月 3 日（金）	109 名	98 名	90%
東京　10 月 14 日（木）	191 名	148 名	77%
福岡　11 月 24 日（水）	47 名	43 名	91%
合　計	460 名	390 名	85%

5.2 アンケート集計

5.2.1 概要

本説明会の参加者数 390 名のうちアンケート回答数は、4 ヶ所合計で 322 名（全体回答率：83%）であった。アンケート項目の集計結果を「5.2.2 集計結果」に示す。

5.2.2　集計結果

(1) 業種及び資本金

①業種

最も多い参加業種は全会場で「情報処理」となっており、地域によって「自治体」や「卸売・小売」も続いている。

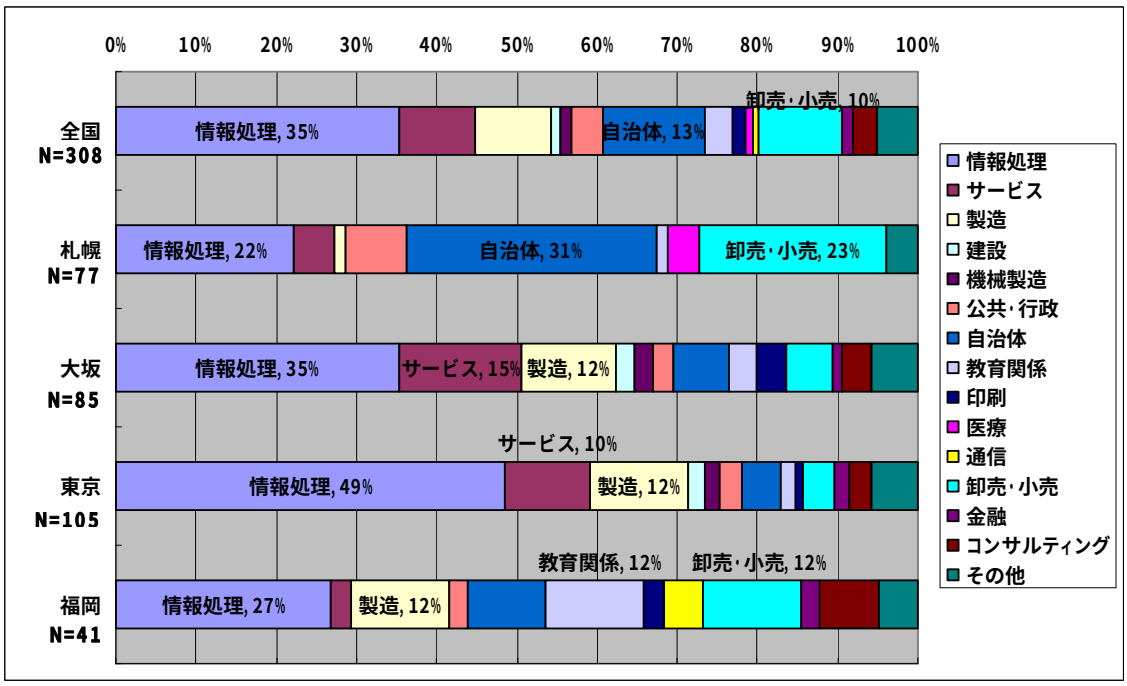


図 5.1　業種

②従業員数

全国的に見ると「300～1,000 人未満」が最も多くなっているが、札幌では「5,000 人以上」が 25%、福岡では「100 人未満」が 32%と地域によって異なっている。

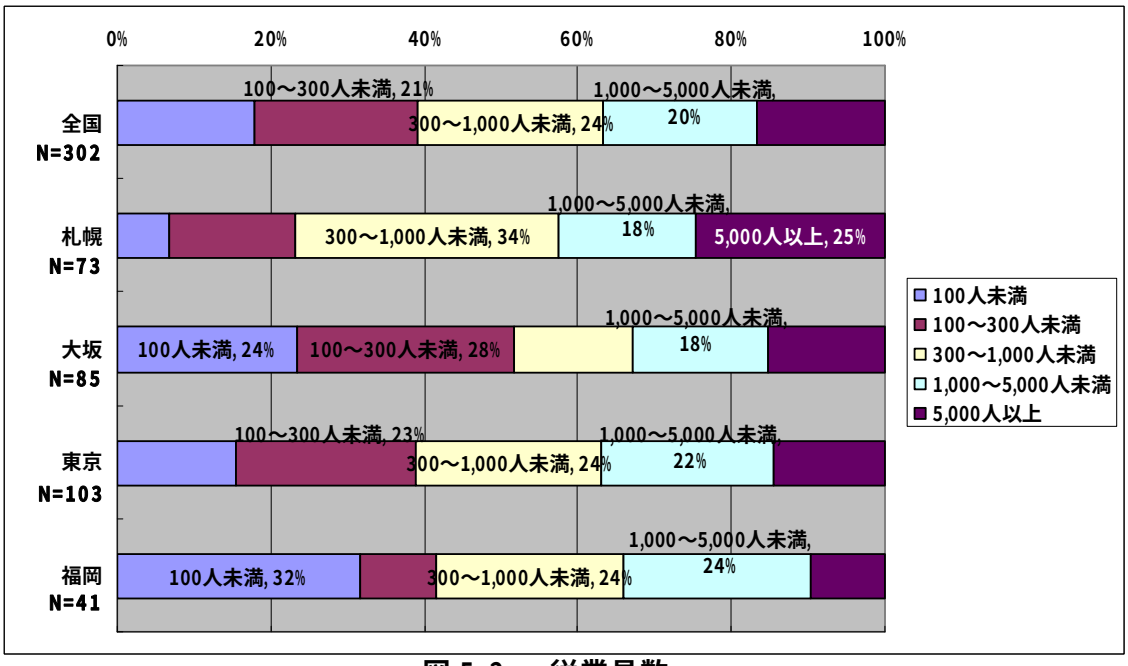


図 5.2　従業員数

③資本金

札幌以外の会場では、「1,000 万円～1 億円」の企業が最も多く参加している。また、ほとんどの会場で「50 億円以上」の企業も１割を超えている。

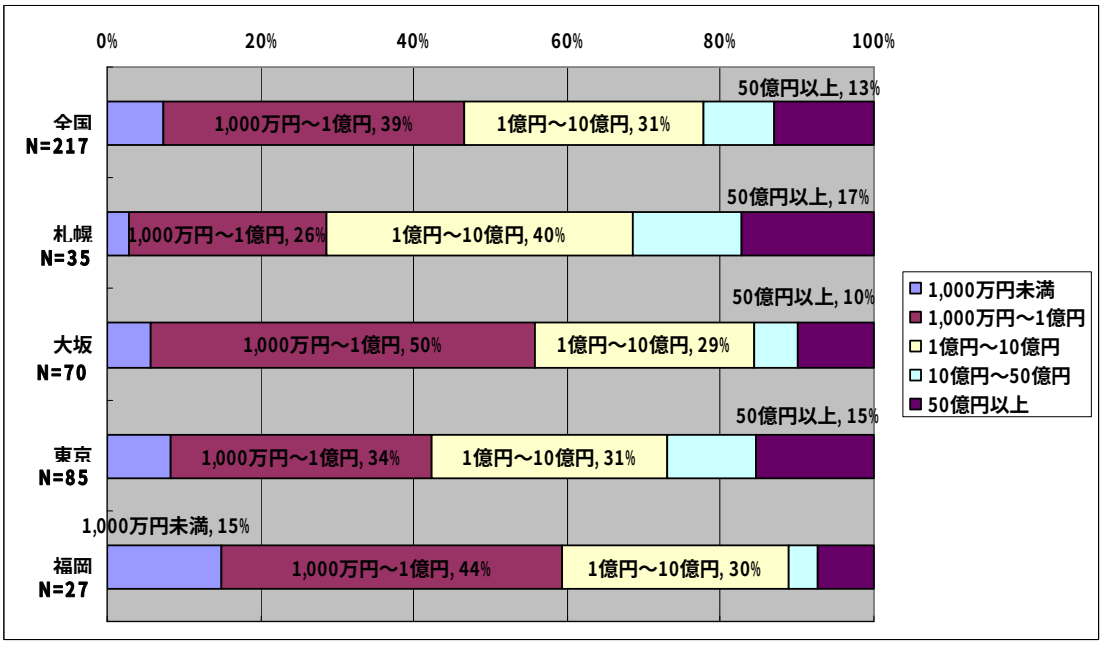


図 5.3　資本金

(2) 参加者について

①職種

全会場で「情報システム」が 5 割を超えて最も多く、「営業・販売」が続いている地域が多い。

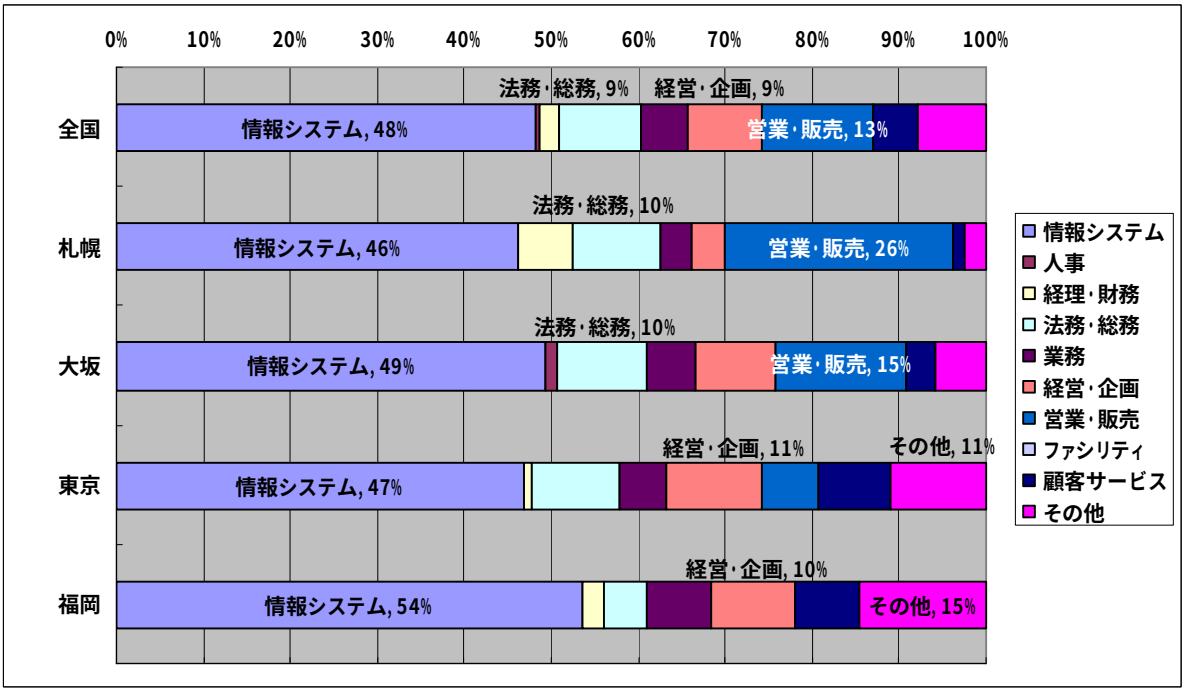


図 5.4　職種

②役職

大坂以外の会場で、「一般職」、「管理職」の順で参加者が多くなっている。

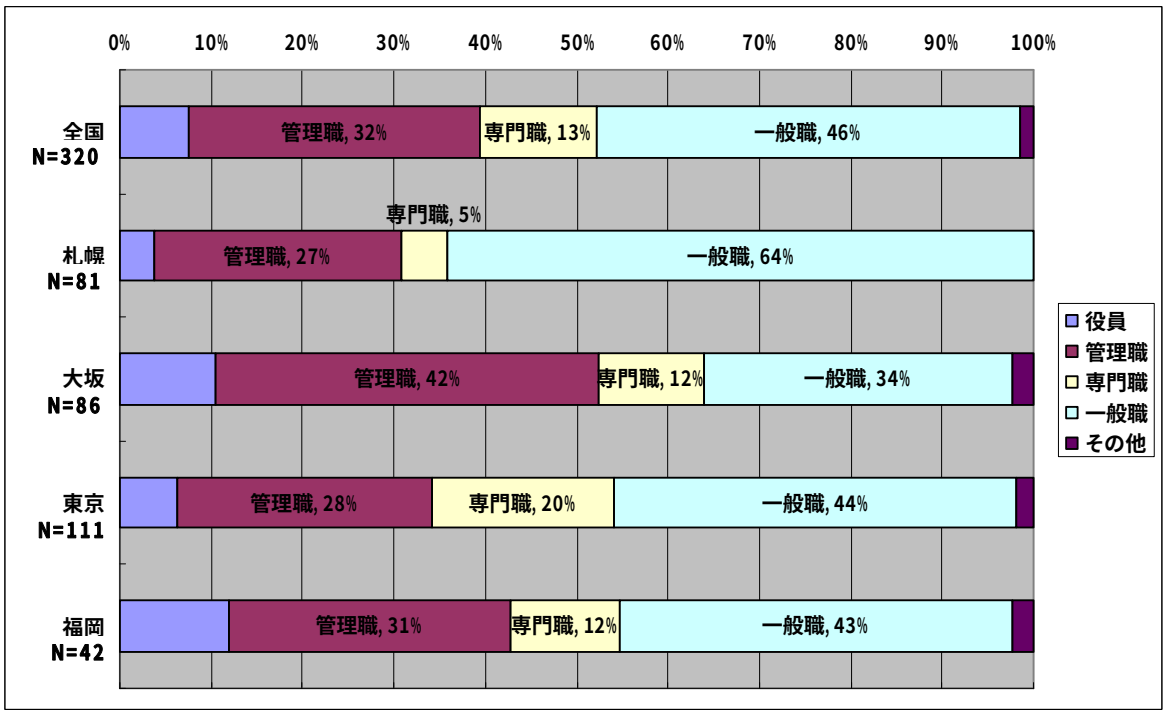


図 5.5　役職

③SAM に対する立場

全会場において、「推進・事務組織（責任者）側」と「エンドユーザー側」に集中している。

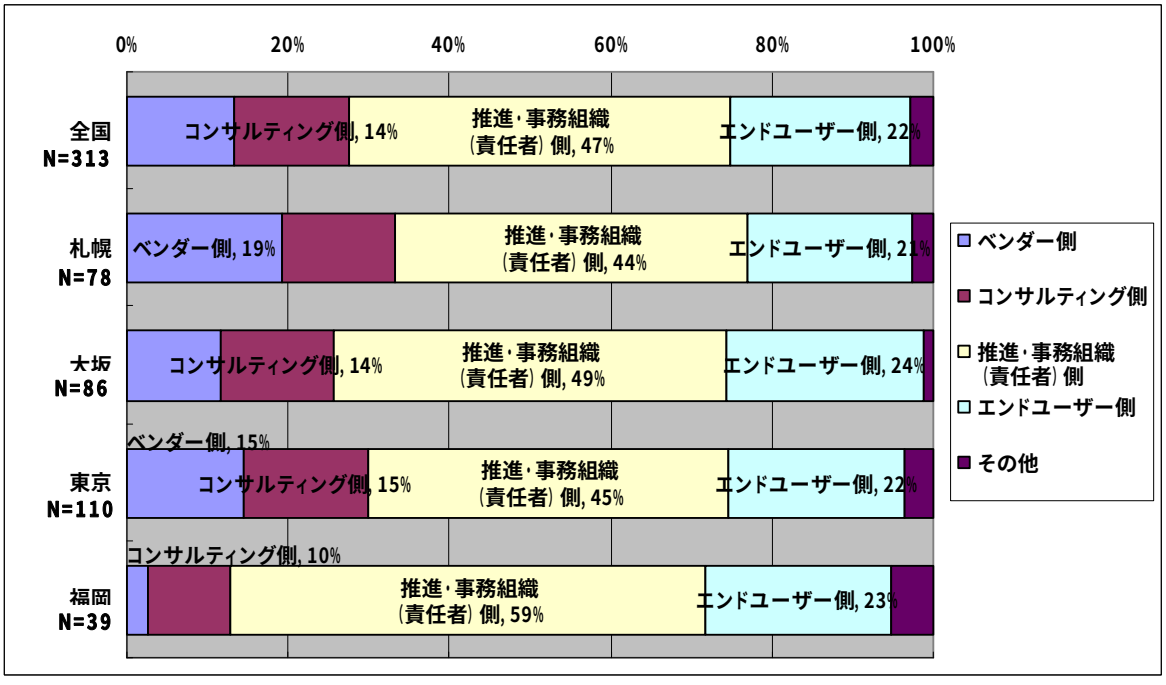


図 5.6　SAM に対する立場

④参加目的

全会場においてほぼ８割が、「情報収集」の目的で参加していることがわかる。

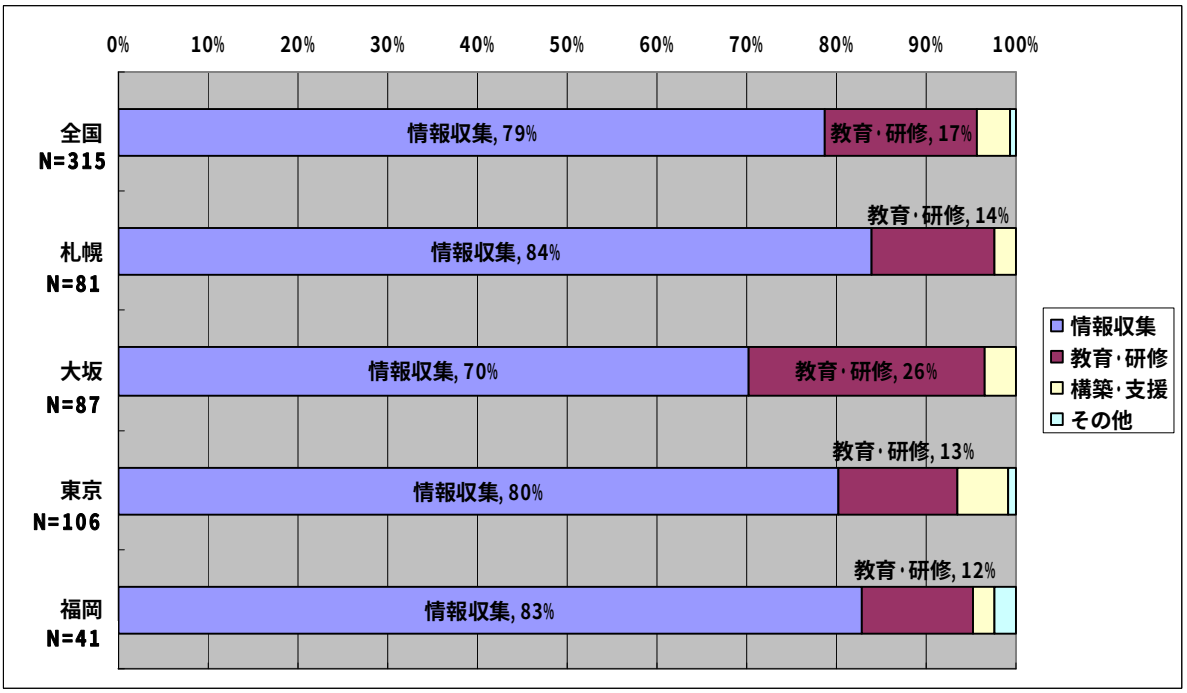


図 5.7　参加目的

(3) ソフトウェア資産管理（SAM）について

①SAM の実施状況

福岡会場では「検討中」が最も多く、その他の地域では「実施している」が最も多くなっている。

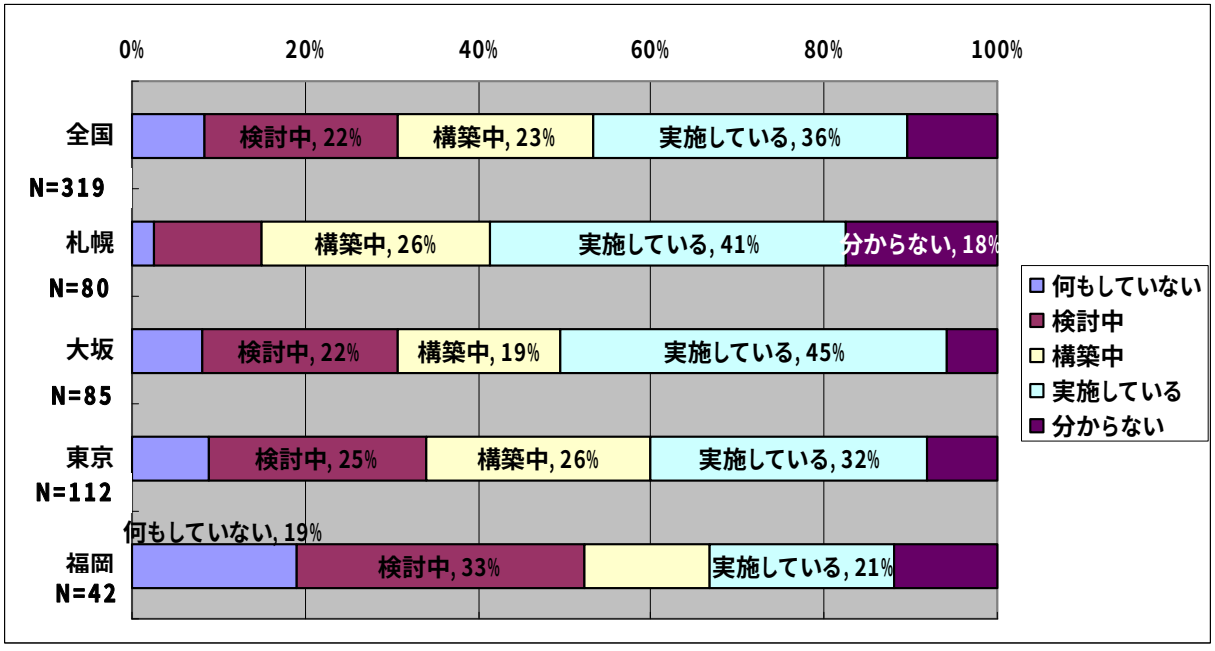


図 5.8　SAM の実施状況

②SAM 構築時の外部組織のアドバイス状況

SAM を「検討中」、「構築中」、「実施している」と回答した参加者のうち、ほとんどが「受ける予定はない」としている。

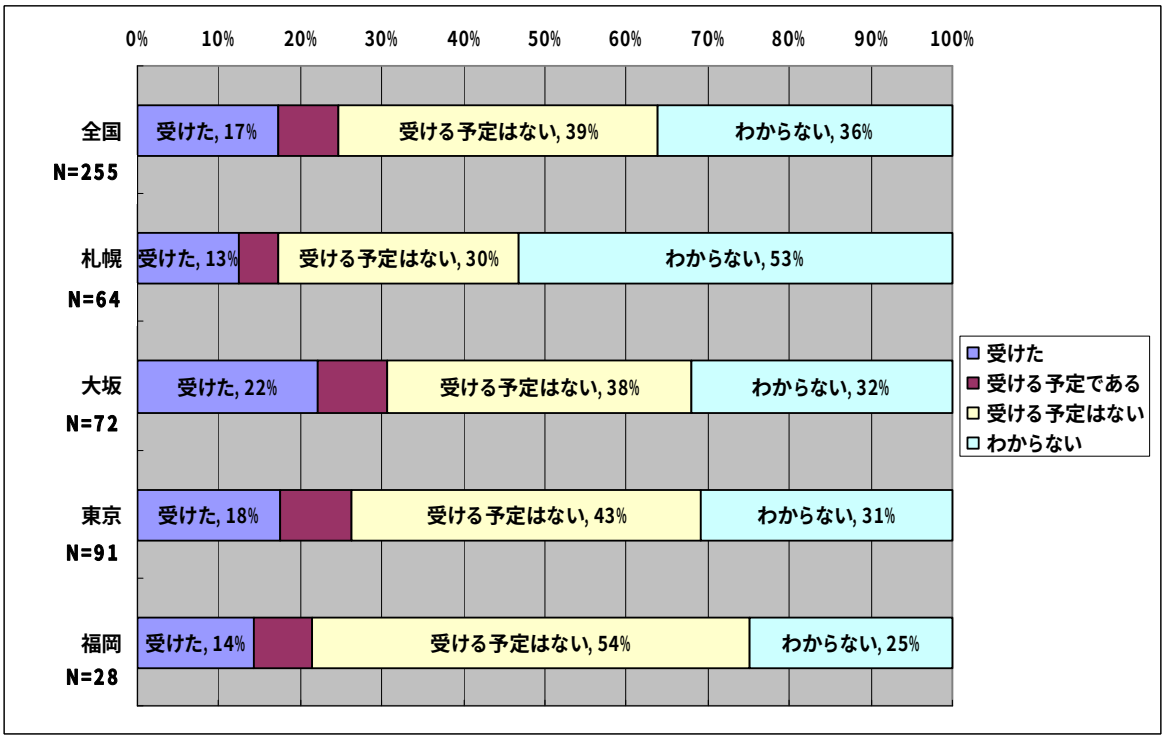


図 5.9　SAM 構築時の外部組織のアドバイス状況

③外部のアドバイス内容

「外部組織のアドバイスを受けた（受ける予定）」と回答した参加者のうち、ほとんどが「コンサルティング会社」を選んでいる。

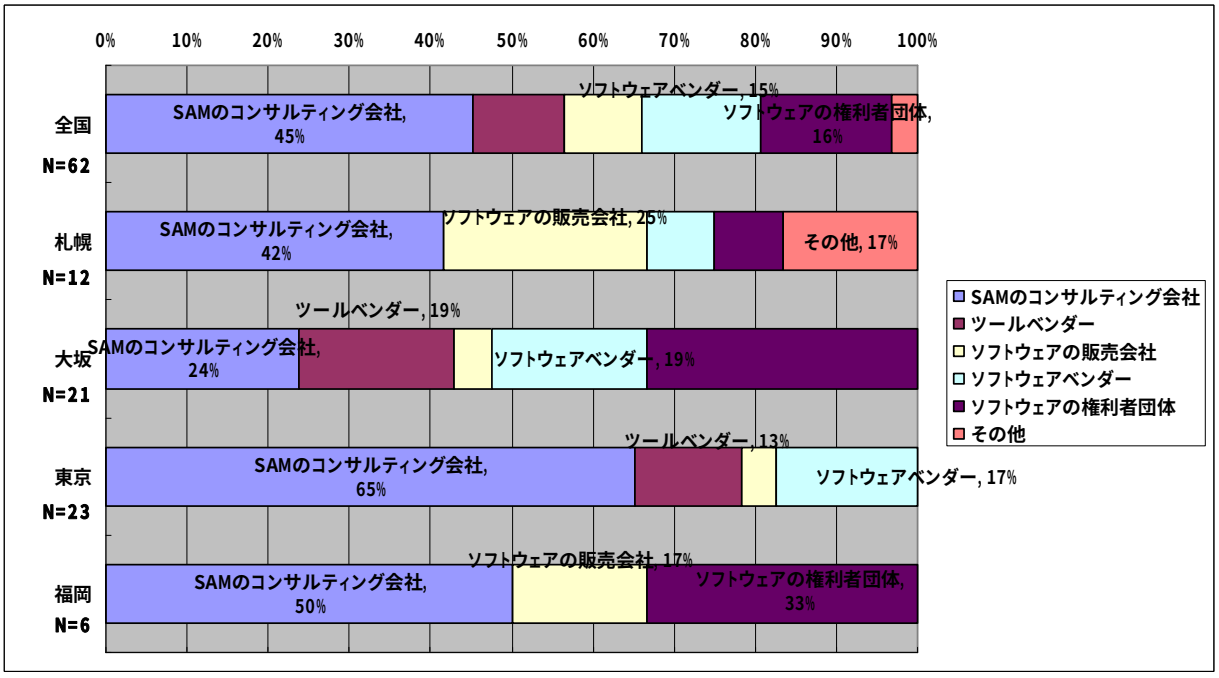


図 5.10　外部組織のアドバイス状況

④外部のアドバイスの満足度

「外部組織のアドバイスを受けた（受ける予定）」と回答した参加者のうち、ほとんどが「満足だった」としている。

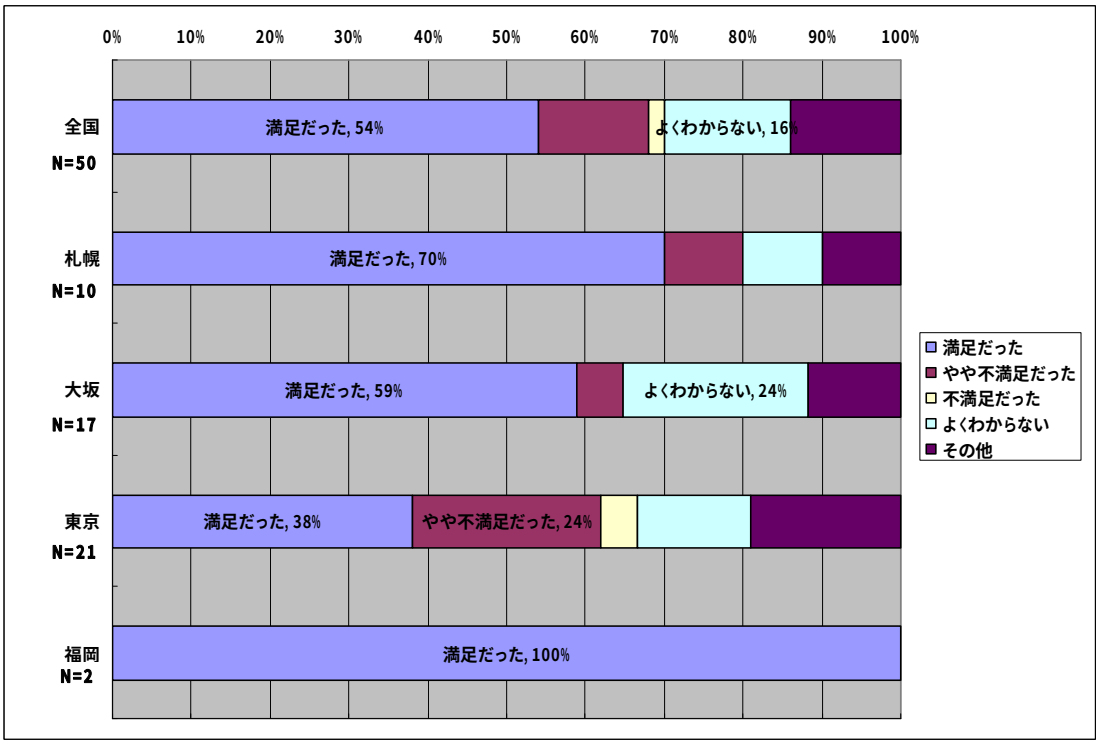


図 5.11　外部組織のアドバイスの満足度

⑤策定期間

SAM の策定期間としては、「6 ヶ月～1 年未満」が最も多くなっている。

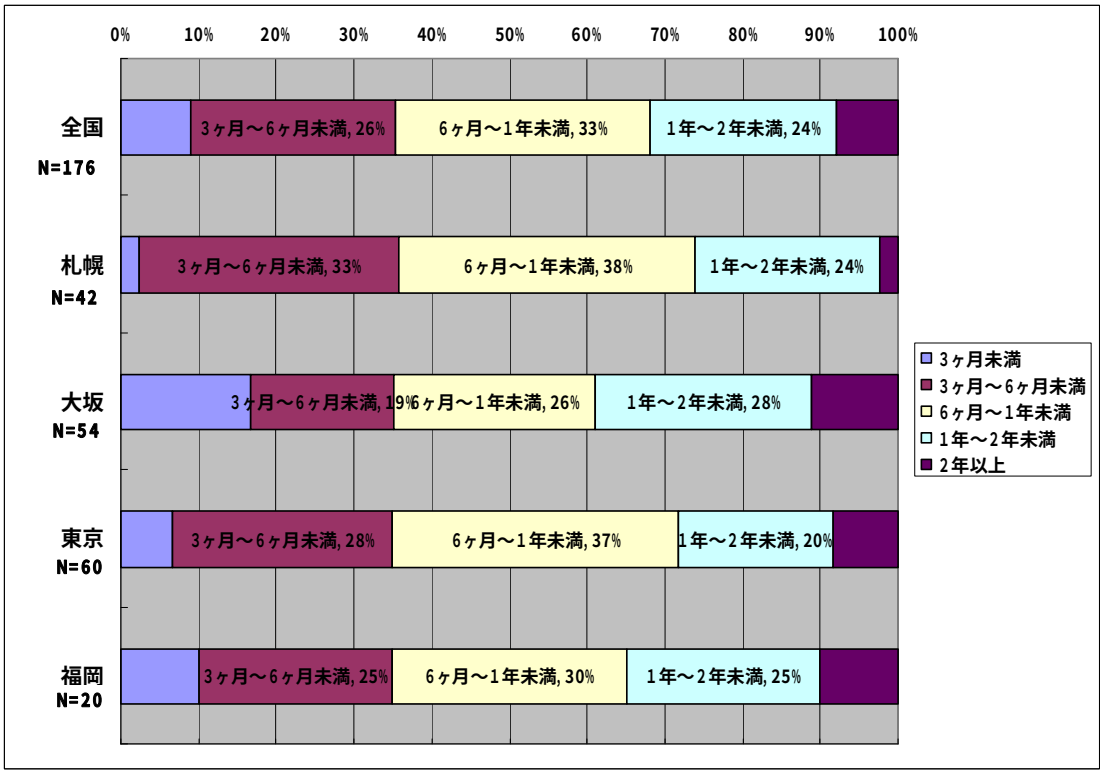


図 5.12　策定期間

⑥SAM 導入のきっかけ

全会場において「組織内上層部からの要請」が最も多くなっている。

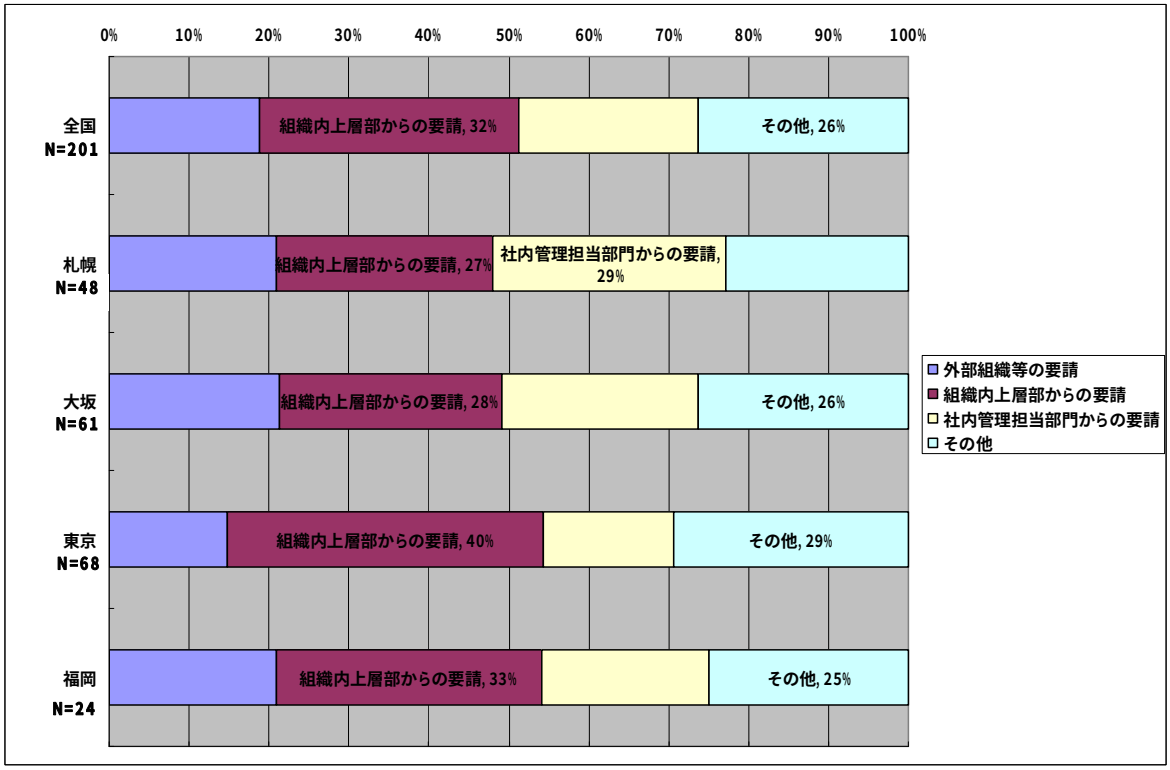


図 5.13　SAM 導入のきっかけ

⑦予算

SAM を構築する際の予算に対しては、全会場で「不明」との回答が最も多く、ほとんどは「100 万円未満」、「100 万円～500 万円未満」となっている。

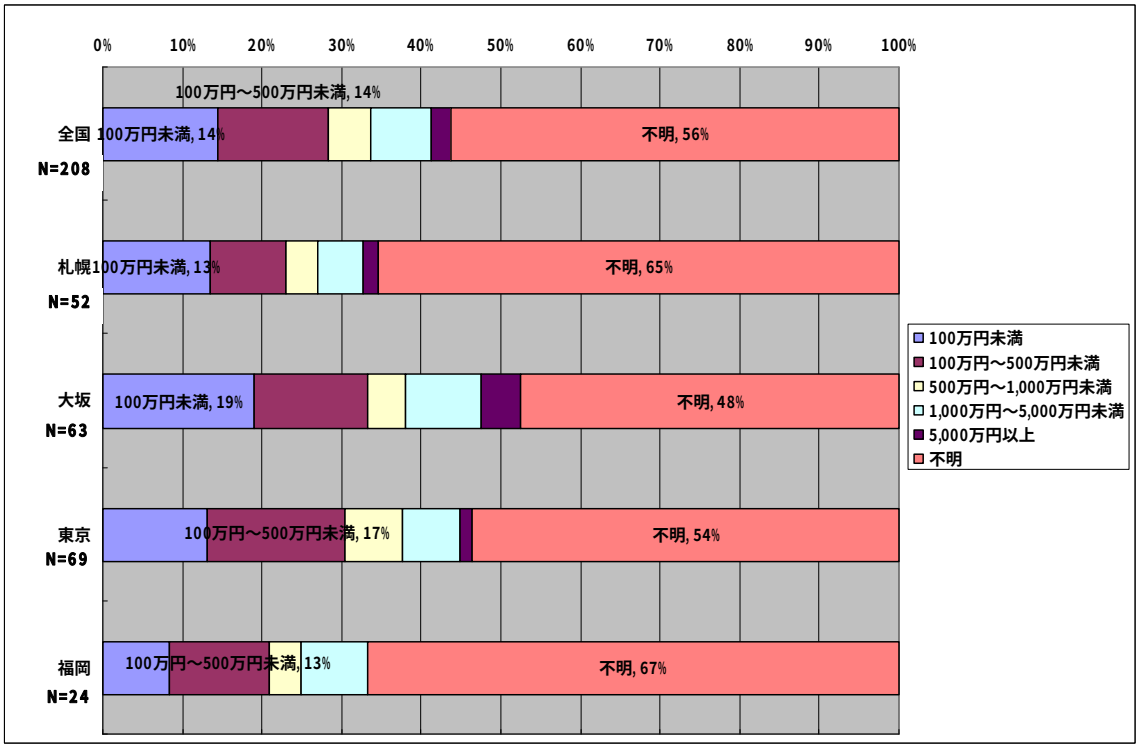


図 5.14　予算

⑧SAM の対象組織（社内組織）

全会場において「全社」（約８割）が SAM の対象組織（社内組織）となっている。

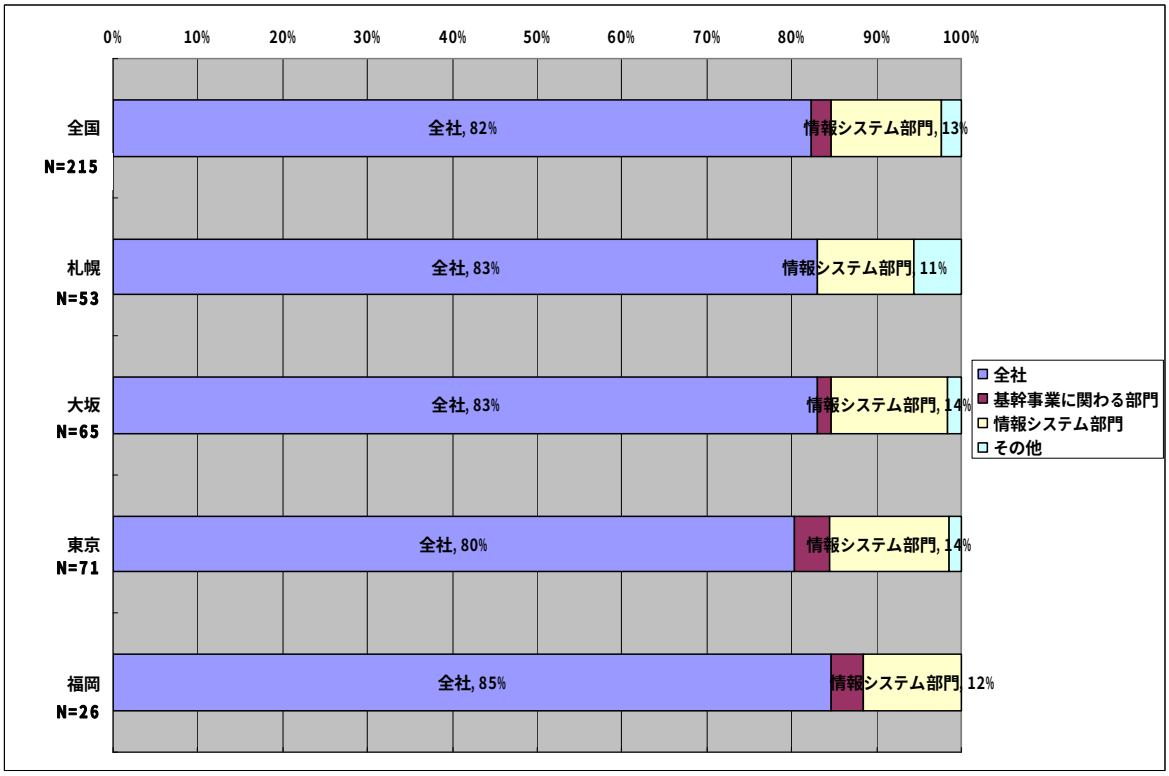


図 5.15　SAM の対象組織（社内組織）

⑨SAM の推進組織（社内組織）

SAM の推進組織（社内組織）については、「情報システム部門」が最も多くなっている。

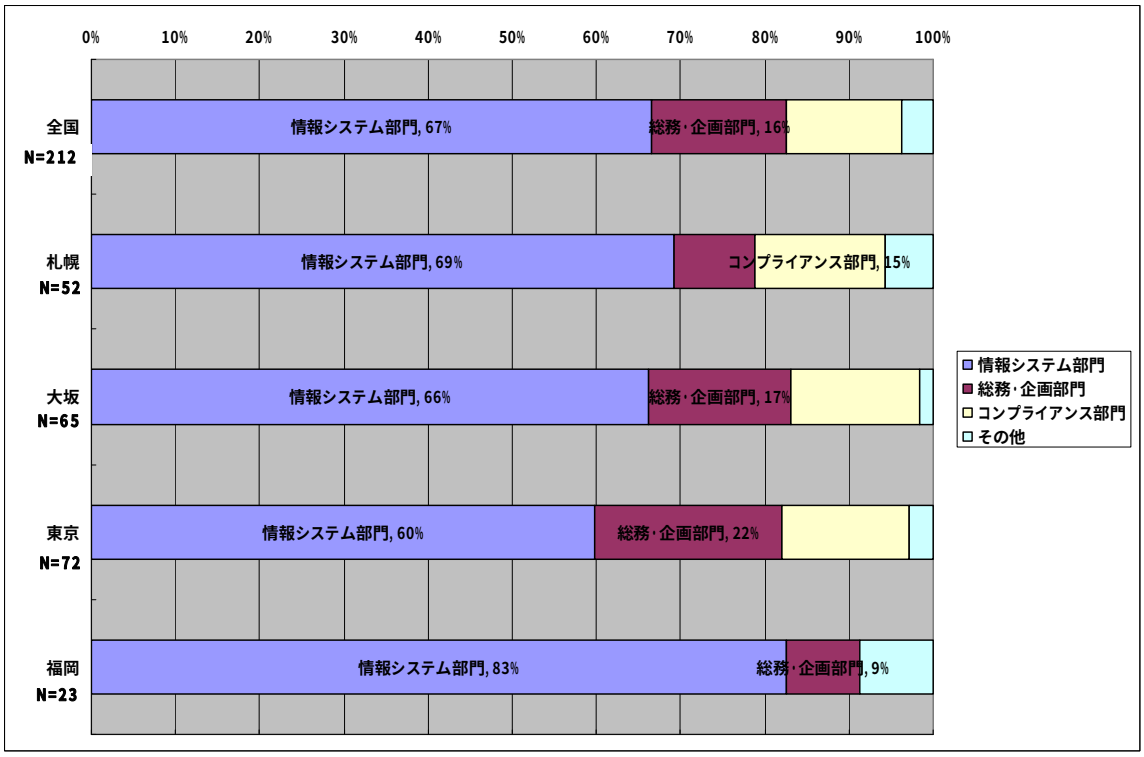


図 5.16　SAM の推進組織（社内組織）

⑩SAM 導入の目的

全会場で最も多いのが「コンプライアンス」、続いて「ライセンス数の適正化」となっている。

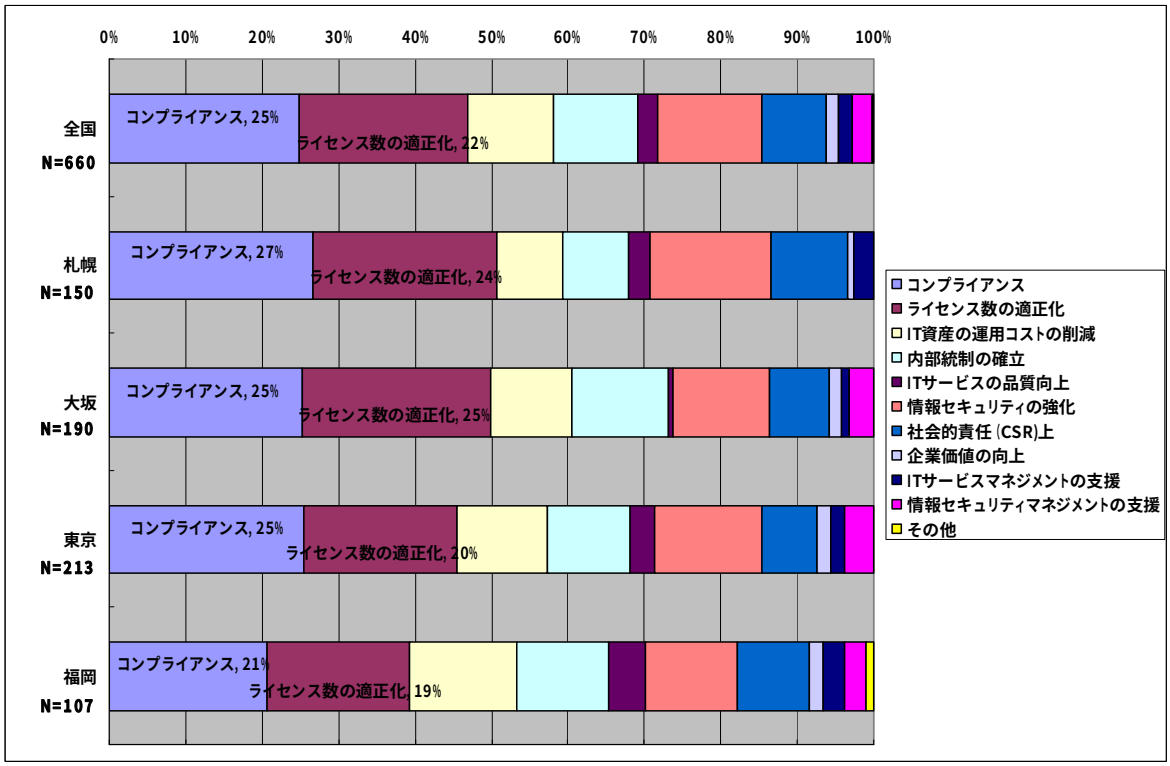


図 5.17　SAM 導入の目的

⑪SAM と ISMS、ITSMS、ITIL の関連

全会場においてほとんどが「SAM 単独で導入」となっている。

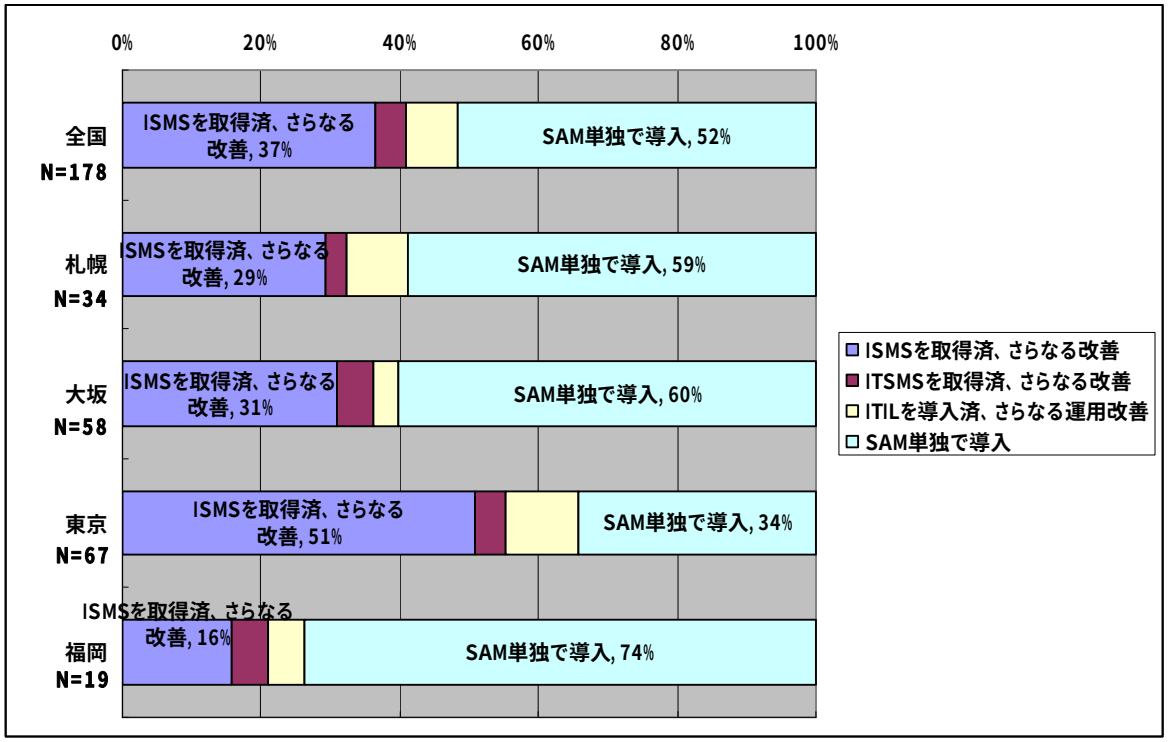


図 5.18　SAM,ISMS,ITSMS,ITIL の関連

⑫SAM 導入するにあたり参考にしたガイドライン

ほとんどの企業・組織が「ソフトウェア資産管理対策基準・手順書 Ver.1.0」、「ソフトウェア管理ガイドライン」を参考としている。

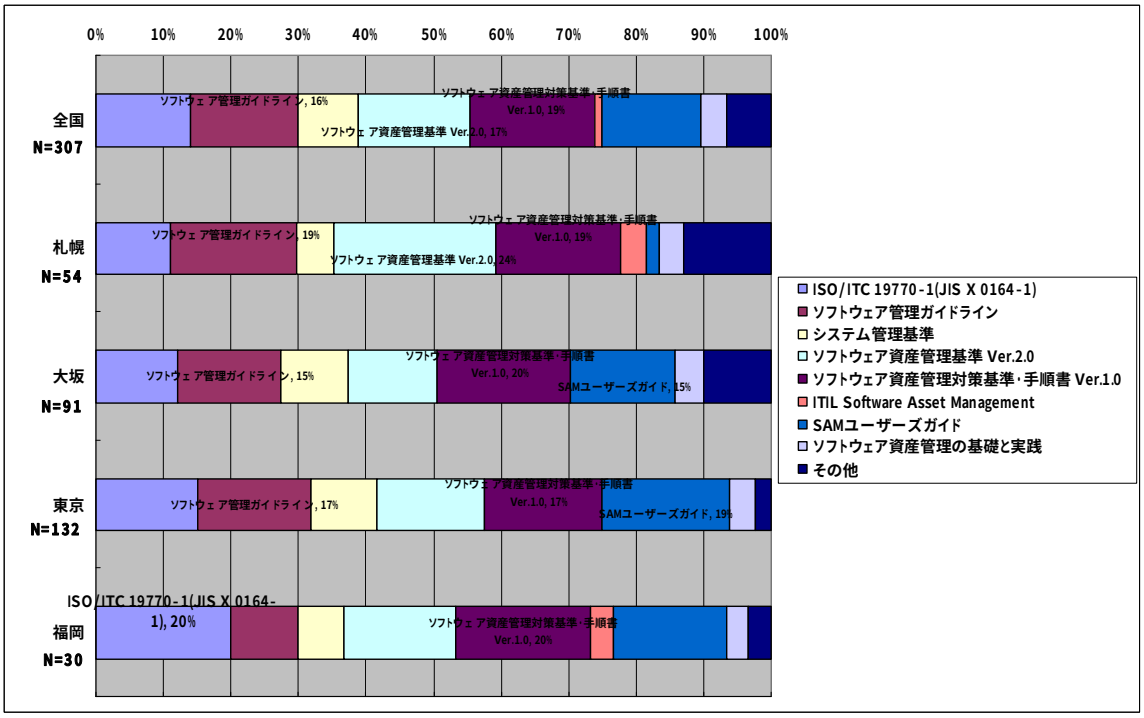


図 5.19　SAM を導入するにあたり参考にした(する予定の)ガイドライン

⑬SAM 内部監査の実施

SAM を「実施している」と回答した参加者のうち、内部監査を「実施している」が「実施していない」を上回っている。

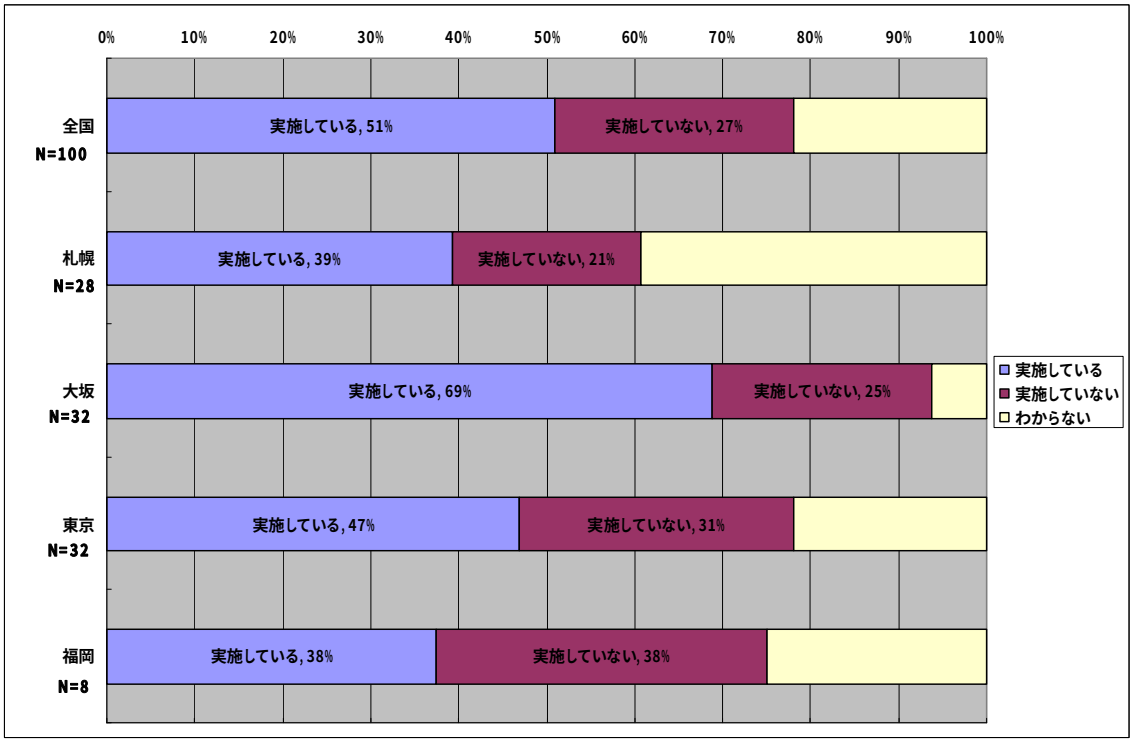


図 5.20　SAM 内部監査の実施

⑭内部監査の実施部門

内部監査を「実施している」と回答した参加者のうち、福岡会場以外は「監査部門」が約半分を占めている。

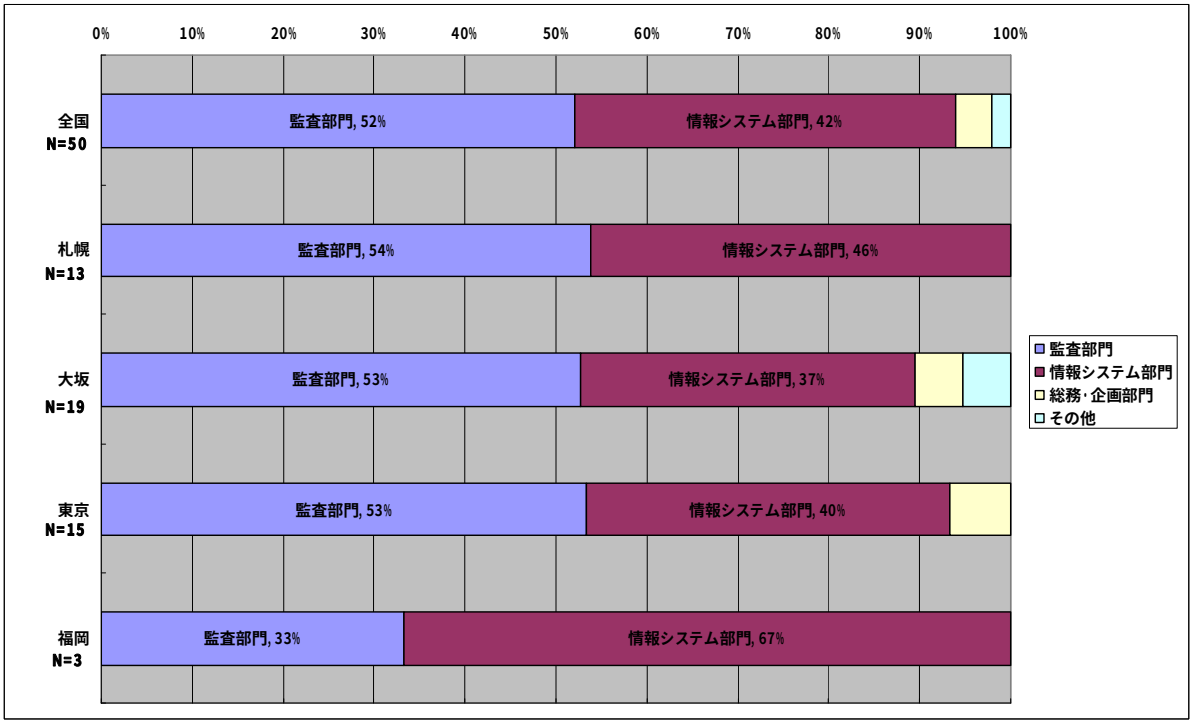


図 5.21　内部監査の実施部門

⑮SAM の外部監査の実施

SAM を「実施している」と回答した参加者のうち、外部監査を「受けていない」が「受けている」を大きく上回っている。

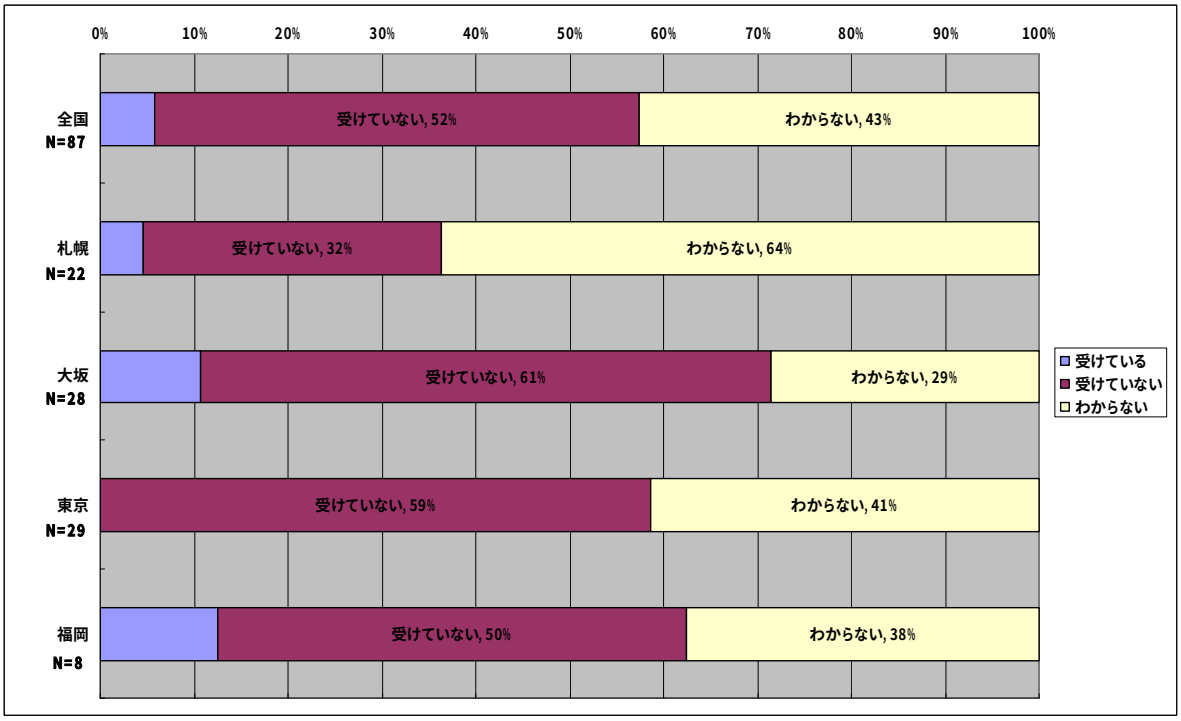


図 5.22　外部監査の実施

⑯SAM 導入にあたり障害となったもの

導入にあたり障害となったものは、ほとんどの会場で「人材不足」、「予算不足」をあげている。

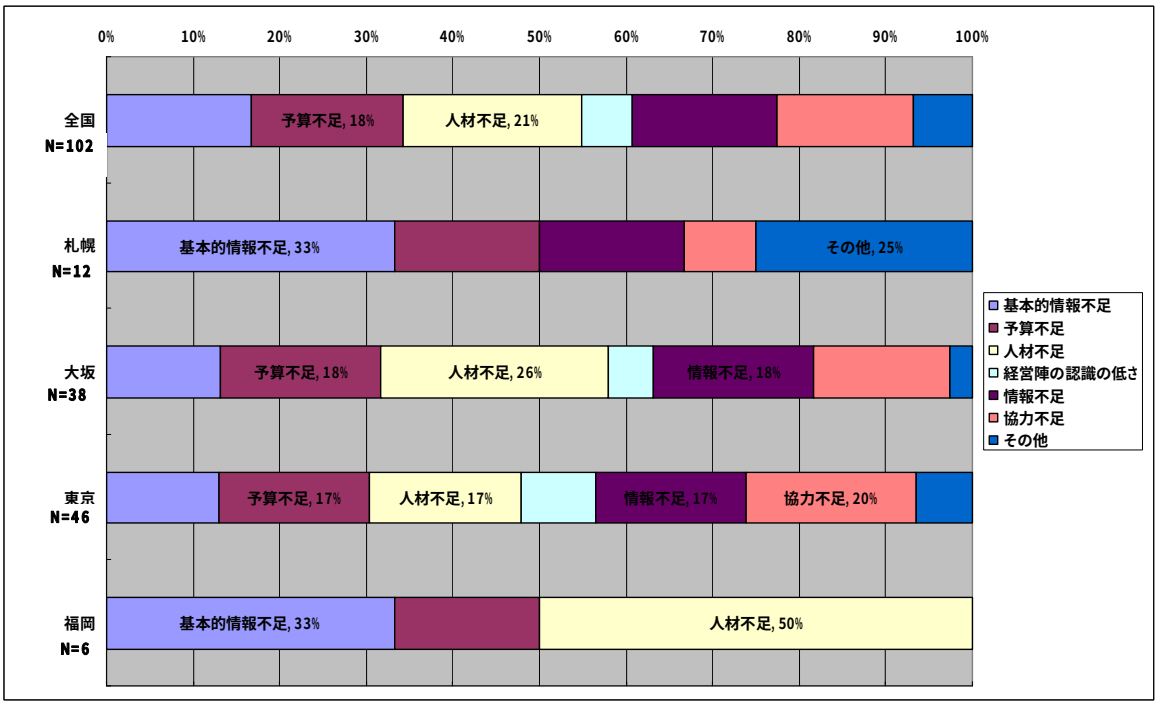


図 5.23　SAM 導入にあたり障害となったもの

⑰SAM 実施後の課題

実施後の課題に関しては、全会場において「人材がいない」、「運用に必要な情報不足」をあげている。

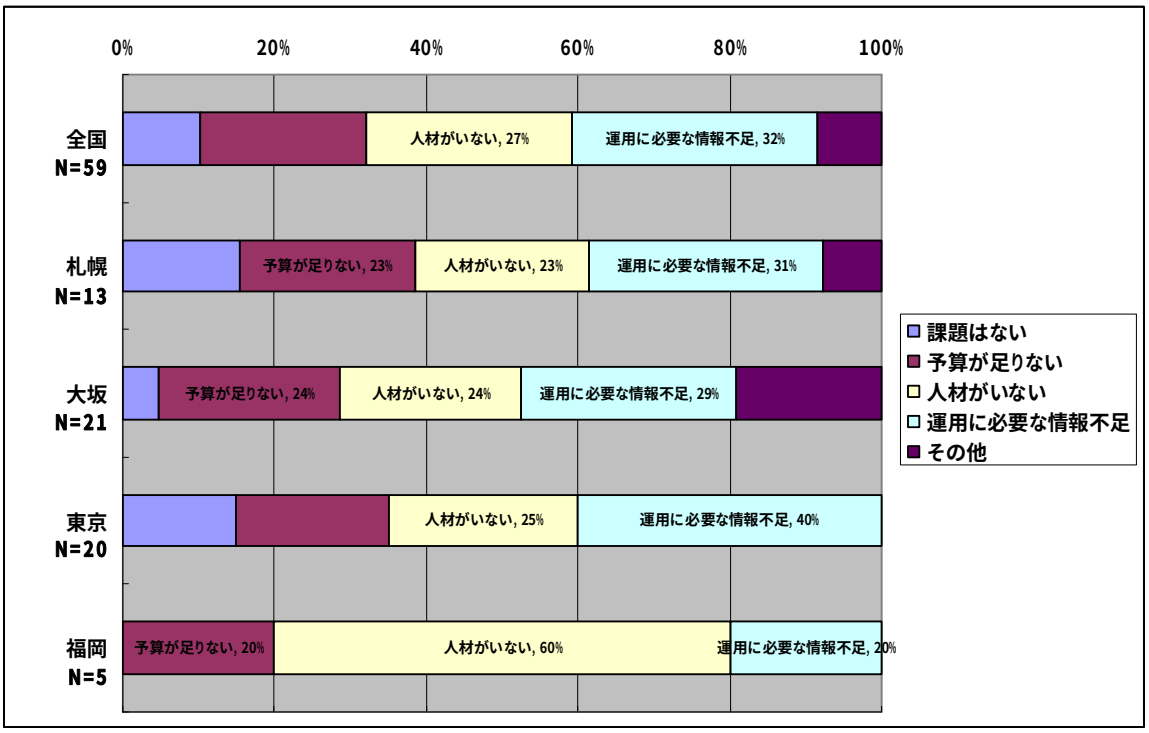


図 5.24　SAM 実施後の課題

⑱SAM を導入して良かった点は何ですか。

札幌会場（7/5）

・不正コピーの使用がなくなった。
・違法コピーを止める規定が確立された。
・まだ導入後間がないため、具体的なメリットは出ていないが、職員が「ライセンス管理は重要」という最低限度の認識を持ち始めたことは実感できる。
・ソフトウェアの全体状況を把握することができた。
・導入途中ではあるが、整備・管理を行い、コンプライアンス及びライセンス数の適正化を実施できる。

大坂会場（9/3）

・ソフトウェア資産の適正管理ができるようになった。
・訴訟リスク軽減、不正ソフト利用なし。
・社員のコンプライアンスへの意識の高まり。
・機器ソフトの移動の管理がしやすい。
・ソフトウェアのインストール確認、クライアント PC 使用者の認識。
・全社員の意識が高まったこと。
・ライセンス数の把握、異動管理、社員の意識の向上が図られた。
・コンプライアンス意識が高まった？
・従業員のコンプライアンスに対する意識が向上した。不必要なライセンス購入費用が削減できた。

東京会場（10/14）

・コンプライアンスが向上した。
・ソフトウェア資産の整理ができた点。
・コンプライアンスの意識が高くなった。
・ソフトウェア資産を明確に把握できるようになった。
・ライセンスの適正化管理向上。
・コンプライアンス、情報セキュリティ。

福岡会場（11/24）

・見える化により、遊休資産の利用と剰余資産の削減。
・ソフトウェア管理の適正化。

⑲SAM 導入を今後どのようにしたいと思いますか

札幌会場（7/5）

・適切な資産管理を、システム化して実施したい。
・現在手作業により実施している業務をシステム化できれば、大幅に省力化できるものと期待している。
・社員はもとより、お客様へのコンサルへ活用したい。

大坂会場（9/3）

・SAM の全要求内容を展開しているわけではなく、SAM 自体には上層部の理解を得られていない。社会の標準化の流れをキャッチして、いかにそれに合わせて上を説得するか。効率的な管理ができるか。

・IT 資産に関する予算の削減。
・コンプライアンス面で機能するようにして行きたい。
・内部統制、コスト削減
・ライセンス管理を行うツールと資産台帳の運用
・最小限の管理（労力）で、高いパフォーマンス（目的達成）を得る。
・着実な運用
・今までは社内で独自に検討してフレームを作り実施していたが、今回 SAM の説明を聞き参考になった部分を生かして行きたいと思います。

東京会場（10/14）

・まだ十分な状態ではないので、ガイドライン等を参考にして充実していく必要がある。
・もっと完全な SAM にしていきたい。
・運用がまわっていない。改善したい。
・継続したい。
・ソフトウェア資産の適切な識別がまだ不十分である。改善が必要。
・ライセンスマネジメントの拡充。

福岡会場（11/24）

・さらに高い管理を行う。

(4) その他

①説明会を知った媒体

ほとんどの参加者は、「電子メール」、「Web」で説明会を知ったことがわかる。

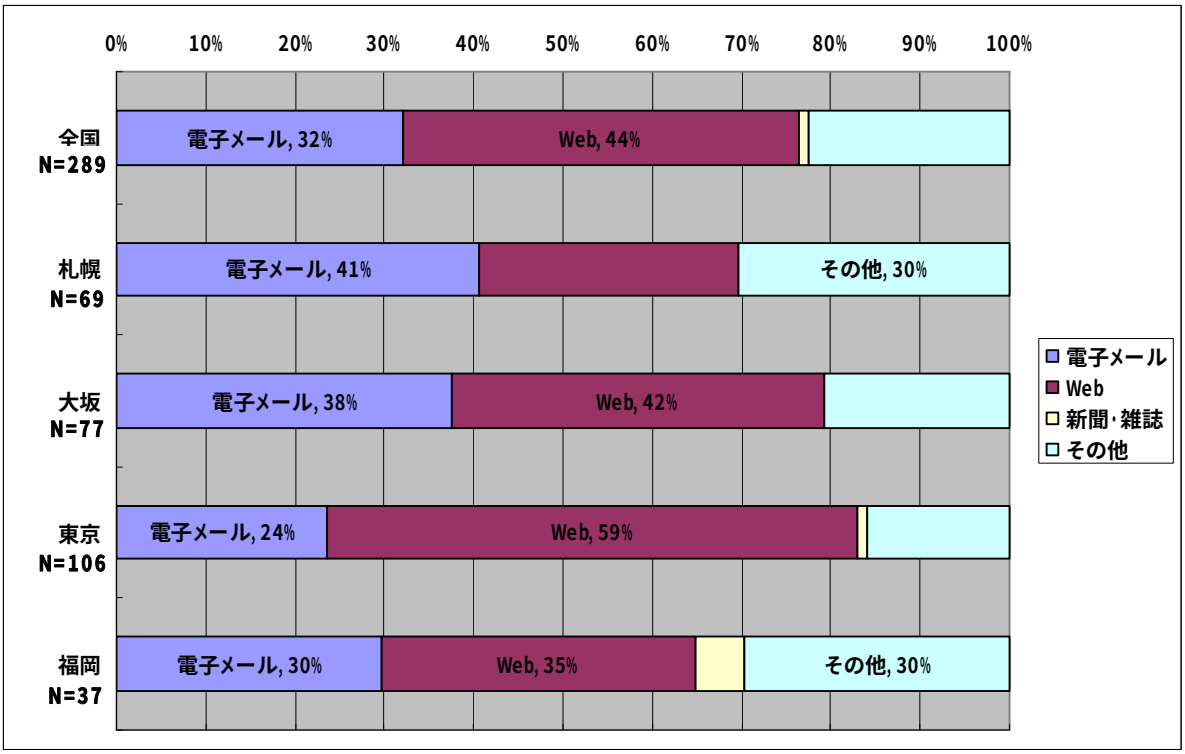


図 5.25　説明会を知った媒体

②説明会の評価（講演内容）

講演内容に関しては、「満足」、「やや満足」を合わせるとほぼ 9 割の参加者が満足だったことがわかる。

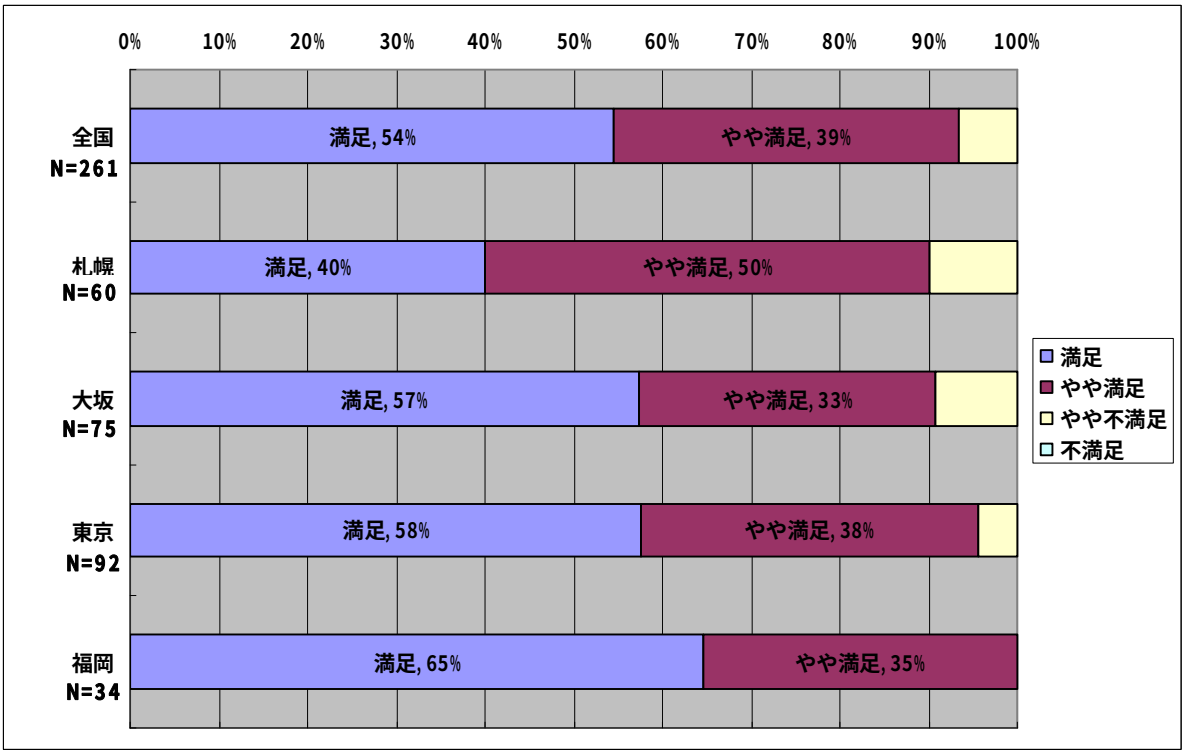


図 5.26　説明会の評価（講演内容）

③説明会の評価（講演時間）

講演時間に関しても、8 割以上の参加者がほぼ満足だったことがわかる。

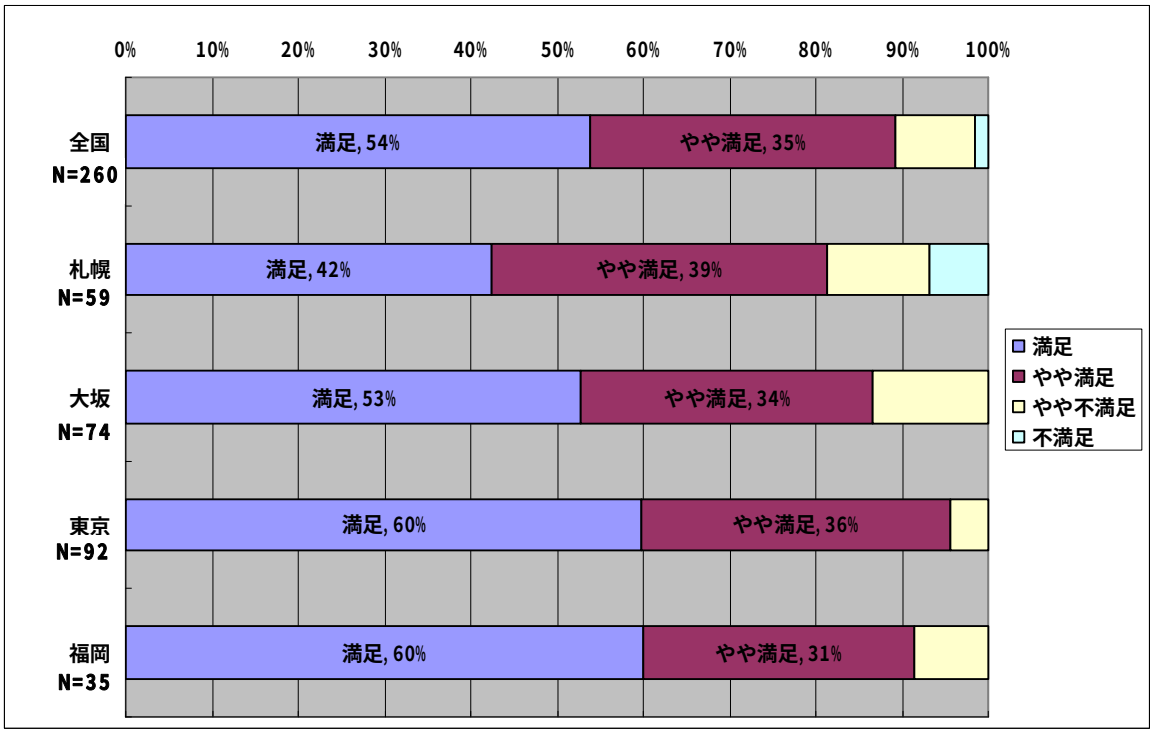


図 5.27　説明会の評価（講演時間）

④説明会の評価（講演会場）

講演会場についても、大坂会場以外は「満足」、「ほぼ満足」が多かった。

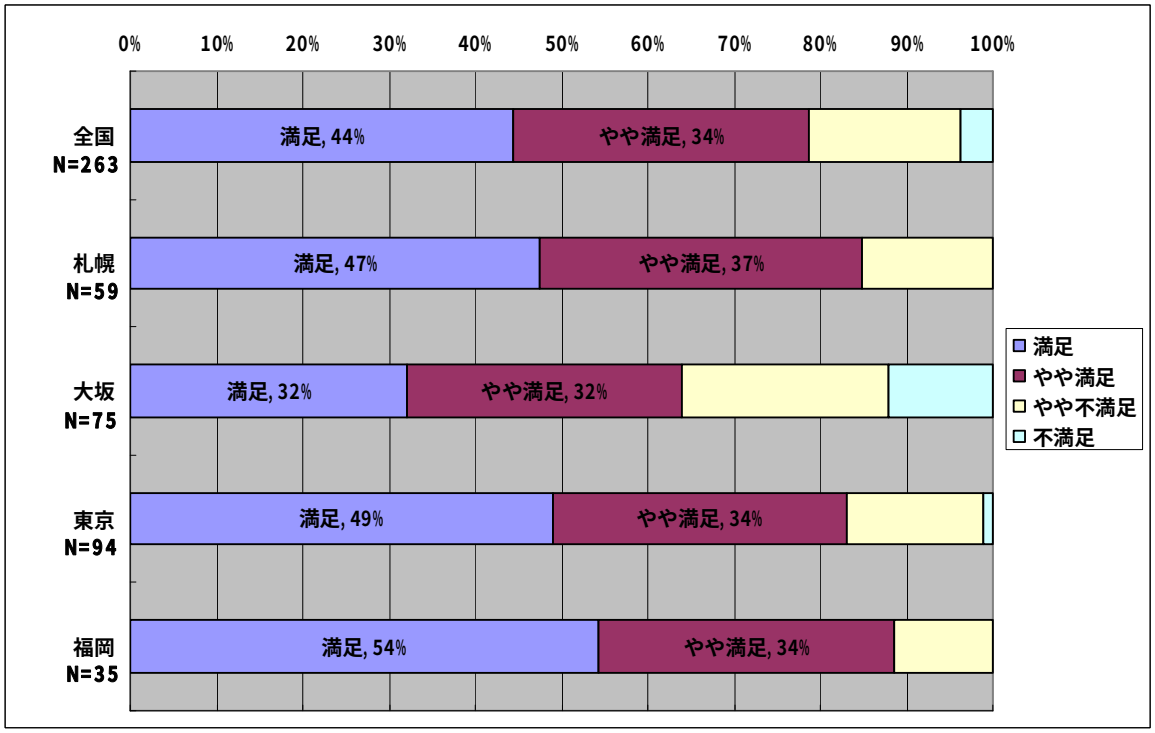


図 5.28　説明会の評価（講演会場）

⑤今後の説明会開催

今後の説明会の開催については、全会場において開催を期待しているという結果となっている。

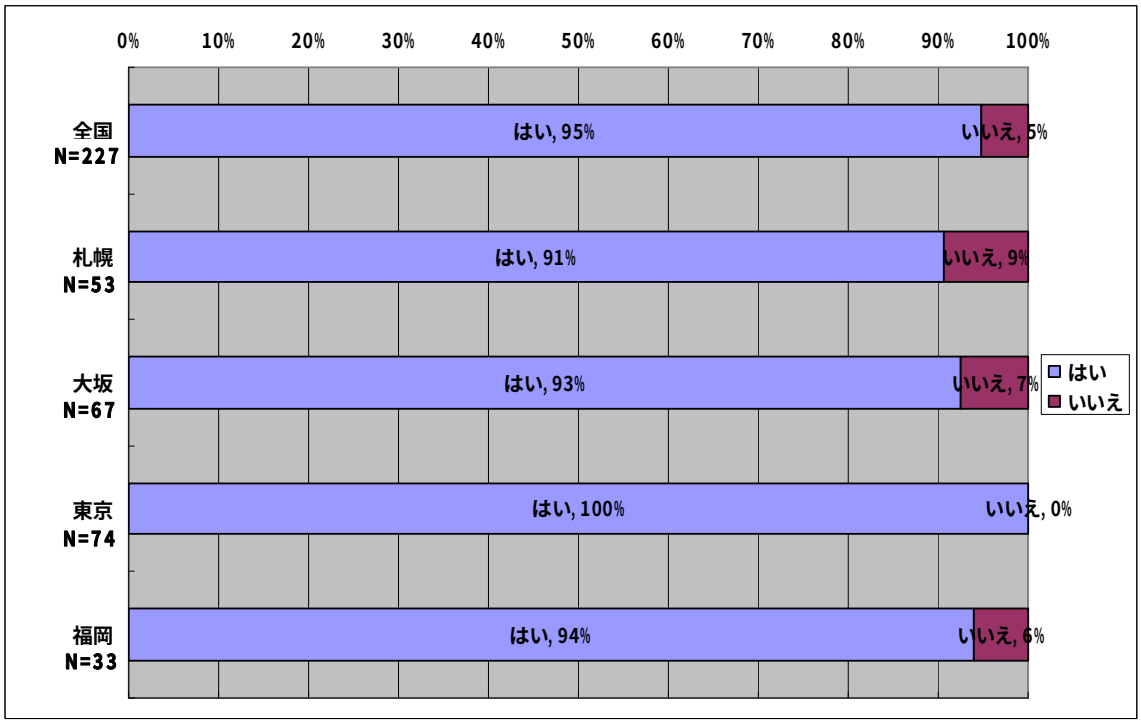


図 5.29　今後の説明会の開催

⑥今後取り上げて欲しいテーマあるいはその他ご意見

札幌会場（7/5）

・無線 LAN の企業利用とセキュリティ
・SAM を構築した企業、自治体の実践事例、発表等。
・特になし。
・インベントリーツールは何がいいか。
・全体的にもっと詳細に掘り下げた内容の説明会（セミナー）があれば参加したい。

大坂会場（9/3）

・大学事例（教員、情報、資産、管理）
・ソフトウェア提供者のルール化を望む。インベントリ名の統一化、バージョンアップ方法の統一化。
・CSR、BS 7799。
・講師がそれぞれの立場に立ってディスカッションをしていただくのも今後良いのではないでしょうか？
・ライセンス形態に基づいた具体的な管理の方法。
・具体的な SAM 方法論を重点に実施事例を知りたい。
・クラウドのセキュリティとリスク。
・もっと具体的に S/W を全て洗い出す手順(PC の中の全ての S/W はどう確認するか？exe?)、ライセンス体系による管理手法。
・情報漏えい関係
・SAM に関する最新の情報、状況等についてタイムリーに取り上げてもらいたい。(19770-2、3 や認証など)
・有償ソフトと無償ソフトの管理方法の違い等、運用上の注意点。
・ソフト資産管理と会計との関係。
・ISMS（JIS Q 27001）とのリンク、あるいは CSR、コンプライアンスとの関連づけたテーマ

東京会場（10/14）

・具体的な立ち上げ～運用の方法。
・企業の導入事例、SAM ツールの具体的な比較。
・クラウド時代の SAM 運用について(シンポジウムのご紹介の時にもありましたが。)。ITSMS の概説。
・HW に対して SAM の支援を受けたユーザー。
・もっと具体的な話が聞きたい。
・ASSET と全管理
・導入事例、失敗例。
・訴訟事例として、外部委託先監督義務違反（発注先）が問われた事例の紹介。外部先（ex. 指定したインストールソフトの edition 誤りに気づかず結果として違法なソフト使用を行っていた。
・ツールを使わずにすむ方法はないか。
・自分達でできる SAM の動向についても聞きたい。

福岡会場（11/24）

- ITIL/ITSMS
- ITIL/ITSMS とシステム管理基準との関連性のガイド
- QMS→ITSMS への移行ガイド
- データセンター/クラウド事業者以外の事例の公表
- 管理ツールの説明（おすすめ）。
- 大変勉強になりました。ありがとうございました。
- ITSMS について
- 統合マネジメントについて

5.2.3 アンケート調査票

ソフトウェア資産管理（SAM）に関する説明会アンケート

本日は、お忙しい中、「ソフトウェア資産管理（SAM）に関する説明会」にご参加いただきありがとうございます。お手数ですが、下記のアンケートにご協力をお願いします。なお、ご回答は、該当番号に○印をお付けいただくか、もしくは記入欄にご記入ください。

業種：□情報処理　□サービス　□製造　□建設　□機械製造　□公共行政　□自治体　□教育関係　□印刷　□医療 □通信　□卸売･小売　□金融　□コンサルティング　□その他（　　） 複数業種に関連する場合は、主力業種1つのみレ印をつけて下さい。
従業員数：□100 人未満　□100 人～300 人未満　□300 人～1,000 人未満　□1,000 人～5,000 人未満　□5,000 人以上
資本金：□1,000 万円未満　□1,000 万円～1 億円　□1 億円～10 億円　□10 億円～50 億円　□50 億円以上
参加日：□札幌（7月5日）　□大阪（9月3日）　□東京（10 月 14 日）　□福岡（11 月 24 日）　□ 1つのみレ印をつけて下さい。

■質問1．あなたの職種、役職等ついてお聞かせ下さい。

質問1-1　職種

1.情報システム	2.人事	3.経理・財務	4．法務・総務	5.業務	6.経営・企画
7.営業・販売	8.ファシリティ	9.顧客サービス	10.その他 （　　）		

質問1-2　役職

1.役員	2.管理職	3.専門職	4.一般職	5.その他

質問1-3　SAM に対する立場

1.ベンダー側	2.コンサルティング側	3.推進・事務組織（責任者）側
4.エンドユーザー側	5.その他（　　）	

質問1-4　説明会の参加目的

1.情報収集	2.教育・研修	3．構築・支援	4.その他（　　）

■質問2．ソフトウェア資産管理（SAM）についてお聞かせ下さい。

質問2-1　御社の SAM の実施状況についてお聞かせください。

1.何もしていない	2.検討中	3.構築中	4.実施している	5.分からない

質問2-2　質問2-1で「2．3．4.」のいずれかを選択された方に伺います。<u>なお、「1．5.」を選択された方は、質問3へお進み下さい。</u>

①　SAM の構築にあたって、外部組織のアドバイスや支援を受けましたか。または受ける予定ですか。

1.受けた	2．受ける予定である	3．受ける予定はない	4.わからない

②　①で「1．2.」のいずれかを選択された方に伺います。どういった外部組織のアドバイスや支援を受けましたか。

1.SAM のコンサルティング会社	2.ツールベンダー	3.ソフトウェアの販売会社
4.ソフトウェアベンダー	5ソフトウェアの権利者団体	6．その他（　　）

③　①で「1．2.」のいずれかを選択された方に伺います。外部組織のアドバイスや支援の内容は、満足のいくものでしたか。

1.満足だった	2.やや不満足だった	3.不満足だった
4.よくわからない	5．その他（　　）	

④ SAM の導入にはどのくらいの期間がかかりましたか。(かける予定ですか)

1.三ヶ月未満	2.三ヶ月～六ヶ月未満	3.六ヶ月～一年未満	4.一年～二年未満	5.二年以上（　　年)

⑤ SAM を導入したきっかけをお聞かせ下さい。(導入予定含む)

1.外部組織等の要請	2.組織内上層部からの要請	3.社内管理担当部門からの要請	4.その他

⑥ SAM の導入にはどのくらいの予算が組まれていますか。(組まれる予定ですか)

1.100 万円未満	2.100 万円～500 万円未満	3.500 万円～1,000 万円未満
4.1,000 万円～5,000 万円未満	5.5,000 万円以上（　　万円)	6．不明

⑦ SAM の対象組織（社内組織）についてお聞かせください。

1.全社	2.基幹事業に関わる部門	3.情報システム部門	4.その他（　　）

⑧ SAM の推進組織（社内組織）についてお聞かせください。

1.情報システム部門	2．総務・企画部門	3.コンプライアンス部門
4．その他（　　）		

⑨ SAM を導入した(導入する)目的についてお聞かせください(複数回答可)

1．コンプライアンス	2．ライセンス数の適正化	3．IT 資産の運用コストの削減
4．内部統制の確立	5．IT サービスの品質向上	6．情報セキュリティの強化
7．社会的責任(CSR)上	8.企業価値の向上	9．IT サービスマネジメントの支援
10．情報セキュリティマネジメントの支援	11．その他（　　）	

⑩ SAM と ISMS、ITSMS、ITIL の関連についてお聞かせください(複数回答可)

1．ISMS 認証を取得しており、さらなる改善を目指すために導入した（導入する)。
2．ITSMS 認証を取得しており、さらなる改善を目指すために導入した（導入する)。
3．ITIL を導入済みであり、さらなる運用改善を目指すために導入した（導入する)。
4．現在、ISMS、ITSMS の認証取得及び ITIL の導入はなく、SAM 単独で導入した（導入する)。

⑪ SAM を導入するにあたり参考にした(する予定の)ガイドラインは何ですか。(複数回答可)

1．ISO「ISO/IEC 19770-1（JIS X0164-1)」	2.経済産業省「ソフトウェア管理ガイドライン」
3．経済産業省「システム管理基準」	4．NPO 法人ソフトウェア資産管理コンソーシアム「ソフトウェア資産管理基準 Ver2.0」
5．ビジネス ソフトウェア アライアンス（BSA)「ソフトウェア資産管理対策基準・手順書 Ver1.0」	6．TSO「ITIL Software Asset Management」
7．財団法人日本情報処理開発協会（JIPDEC)「SAM ユーザーズガイドー導入のための基礎ー」	8．日本規格協会「ソフトウェア資産管理の基礎と実践」
9．その他（　　）	

質問2-3　質問2-1で「4.実施している」を選択された方に伺います。

① SAM の内部監査を実施していますか。

1.実施している	2.実施していない	3.分からない

② ①で「1．実施している」を選択された方に伺います。SAM の内部監査の実施部門（内部監査を実施している組織）についてお聞かせ下さい。

1.監査部門	2.情報システム部門	3.総務・企画部門
4．その他（　　）		

③ SAM の外部監査を受けていますか。

1.受けている	2.受けていない	3.分からない
理由：	理由：	

④ SAM を導入するにあたり障害となったものは何ですか。(複数回答可)

1.SAM そのものの基本的情報不足	2.予算不足	3.人材不足	4.経営陣の認識の低さ
5.SAM 構築に必要な情報不足	6.他部門・現場の協力不足	7.その他（　　）	

⑤ SAM の実施後に出た課題がありましたらお聞かせ下さい。

1.課題はない	2．予算が足りない	3.人材がいない
4．SAM の運用に必要な情報不足	5．その他（　　）	

⑥ SAM を導入して良かった点は何ですか。

⑦ SAM 導入を今後どのようにしたいと思いますか。

■質問3．その他

質問3-1　今回のソフトウェア資産管理（SAM）に関する説明会は、どのような媒体で知りましたか。

1．電子メール	2．Web	3．新聞・雑誌	4．その他（　　）

質問3-2　今回のソフトウェア資産管理（SAM）に関する説明会の評価はどれですか。

①講演内容	1．満足	2．やや満足	3．やや不満足	4．不満足
②講演時間	1．満足	2．やや満足	3．やや不満足	4．不満足
③講演会場	1．満足	2．やや満足	3．やや不満足	4．不満足

質問３-３　講師についてお聞かせ下さい。

①今回のソフトウェア資産管理（SAM）における講師の評価はどれですか。

講演 1:「法律/コンプライアンス面から見たソフトウェア資産管理（SAM）の必要性」			
1．満足	2．やや満足	3．やや不満足	4．不満足
講演に関するご感想、ご要望等ございましたらお聞かせ下さい。			
講演 2:「SAM 概論／SAM ユーザーズガイドの概説」			
1．満足	2．やや満足	3．やや不満足	4．不満足
講演に関するご感想、ご要望等ございましたらお聞かせ下さい。			
講演 3:「事例に基づく SAM 構築の実際」			
1．満足	2．やや満足	3．やや不満足	4．不満足
講演に関するご感想、ご要望等ございましたらお聞かせ下さい。			

質問３-４　今後もソフトウェア資産管理（SAM）に関する説明会の開催を期待しますか。

１．はい	２．いいえ

質問３-５　今後取り上げて欲しいテーマあるいはその他ご意見をお聞かせ下さい。

ご協力いただきありがとうございました。皆様からいただいたコメントやご要望につきましては、今後の検討材料のひとつとして活用させていただきます。

以上

この事業は、競輪の補助金を受けて実施するものです。
http://ringring-keirin.jp/

おわりに

近年、ビジネスにおけるコスト削減、効率化などが厳しく求められる一方で、仮想化技術やクラウドコンピューティングなどの利用が浸透している状況である。それに伴ってITシステムの継続性が企業・組織の事業継続に与える影響は増大している。特に、ソフトウェア資産管理を適切に管理することで、利用ソフトウェアのライセンス管理やオペレーションコストの削減にもつなげることができる。組織内のソフトウェア資産のライフサイクルを通じた効果的なソフトウェア資産管理及び保護を実現することにより、情報セキュリティ強化の促進、ITサービスの品質を向上させることができ、システム構築・運用環境の改善を図ることができる。

今後は、このような経営環境の変化に対応した組織変革が必要であり、組織に対応したリスクマネジメントの重要性を認識させる必要がある。

企業・組織にとって、IT システムを抜きにしては事業継続を語ることができない状況であり､情報セキュリティとソフトウェア資産管理及び IT システムとも不可分の関係である。すなわち、経営者が組織全体の観点からどの事業戦略が重要であり、必要な経営資源を確保するため、その事業を優先する度合いを決めた上で、いかにリスクマネジメントするかが求められている。

最後になりますが、皆様にとっても情報セキュリティ意識を相互に向上させることが重要であり、今後とも様々な課題解決のためにご協力ご支援をお願いすると共に、忌憚のないご意見をいただければ幸甚である。

平成 23 年 3 月
情報セキュリティ普及実行評価検討委員会
財団法人　日本情報処理開発協会

平成 23 年 3 月発行

発行者：財団法人　日本情報処理開発協会
〒105-0011　東京都港区芝公園 3-5-8
機械振興会館内
TEL:03-3432-9386
URL：http://www.isms.jipdec.or.jp/

印刷所：山陽株式会社
東京都千代田区神田神保町 1-30
TEL:03-3293-5412

２２－Ｈ００１