

平成 26 年度
CSMS 適合性評価制度に関する説明会
実施報告書

平成 27 年 3 月



一般財団法人日本情報経済社会推進協会

目 次

1. 実施概要	1
2. アンケート集計結果	5
3. 参考	19

1. 実施概要

(1) 目的

従来、制御システムは、独立した固有システムで構成され、外部ネットワークや共用システムとは接続されていない等の認識で、セキュリティの脅威は殆ど意識されていませんでした。しかし、ここ数年、企業内の情報システムとのネットワーク接続、Windows や UNIX などの汎用プラットフォームでの利用が進んでおり、環境の変化や脅威の増大を背景に、セキュリティ対応の必要性が非常に高まっています。

本説明会では、制御システムを利用する組織、又は、制御システムを構築する組織を対象に、CSMS(Cyber Security Management System)認証の社会的位置づけ、CSMS 認証基準(IEC 62443-2-1)及び ユーザーズガイド等について解説致します。

本説明会を開催することにより、制御システムにおけるセキュリティマネジメントの必要性について、これまで以上にご理解いただくとともに、CSMS に対する取り組みを検討する上での一助になることを期待しております。

(2) 開催日時及び開催場所

・東京①:平成 26 年 11 月 28 日(火)

グランパーク 401 ホール(東京都港区芝浦 3-4-1)

・東京②:平成 27 年 2 月 17 日(火)

グランパーク 401 ホール(東京都港区芝浦 3-4-1)

・大阪:平成 27 年 2 月 26 日(木)

大阪大学中之島センター 講義室 703(大阪市北区中之島 4-3-53)

(3) 主催

一般財団法人日本情報経済社会推進協会

(4) 後援

経済産業省

技術研究組合 制御システムセキュリティセンター

独立行政法人 情報処理推進機構

一般社団法人 JPCERT コーディネーションセンター

(5) 参加費

無料

(6)プログラム

○平成 26 年 11 月 28 日-東京会場(グランパーク 401 ホール)

time	内 容	講 師
13:30～ 13:35	開催挨拶	—
13:35～ 14:05	基調講演: 「CSMS に関連する 情報セキュリティ政策について」	経済産業省 商務情報政策局 情報セキュリティ政策室 室長補佐 上坪 健治 氏
14:05～ 14:45	講演 1: 「サイバー攻撃対策における 制御システムセキュリティの課題」	技術研究組合 制御システムセキュリティセンター 理事長 新 誠一 氏 (電気通信大学 教授)
14:45～ 15:15	講演 2: 「CSMS 適合性評価制度の概要」	一般財団法人日本情報経済社会推進協会 情報マネジメント推進センター センター長 高取 敏夫
15:15～ 15:30	休 憩	
15:30～ 16:00	講演 3:(CSMS 技術専門部会) 「CSMS の確立に向けて ～CSMS ユーザーズガイド解説～」	株式会社三菱総合研究所 情報通信政策研究本部 サイバーセキュリティグループ 主席研究員 川口 修司 氏
16:00～ 16:25	講演 4:(CSMS 技術専門部会) 「CSMS 認証取得時の成果と その後の改善活動事例」	横河ソリューションサービス株式会社 ソリューションビジネス本部 コンサルティング 3 部 制御セキュリティコンサルタント 新井 保廣 氏
16:25～ 16:50	講演 5:(CSMS 技術専門部会) 「CSMS 活動による効果」	三菱化学エンジニアリング株式会社 鹿島事業所 エンジ1部 制御情報システムグループ 次長 島廻 昭朗 氏
16:50～ 17:00	質疑応答	講演者全員

○平成 27 年 2 月 17 日-東京会場(グランパーク 401 ホール)

○平成 27 年 2 月 26 日-大阪会場(大阪大学中之島センター 講義室 703)

time	内容	講師
13:30～ 13:35	開催挨拶	—
13:35～ 14:05	基調講演: 「生産制御に関連する 情報セキュリティ政策 ～CSMSを中心に～」	経済産業省 商務情報政策局 情報セキュリティ政策室 室長補佐 上坪 健治 氏
14:05～ 14:45	講演 1: 「サイバー攻撃対策における 制御システムセキュリティの課題」	技術研究組合 制御システムセキュリティセンター 理事長 新 誠一 氏 (電気通信大学 教授)
14:45～ 15:15	講演 2: 「CSMS 適合性評価制度及び 認証基準の解説」	一般財団法人日本情報経済社会推進協会 情報マネジメント推進センター センター長 高取 敏夫
15:15～ 15:30	休 憩	
15:30～ 16:00	講演 3:(CSMS 技術専門部会) 「CSMS の確立に向けて ～CSMS ユーザーズガイド解説～」	株式会社三菱総合研究所 情報通信政策研究本部 サイバーセキュリティグループ 主席研究員 川口 修司 氏
16:00～ 16:25	講演 4:(CSMS 技術専門部会) 「CSMS 改善の取り組みと 今後の制度への期待」	横河ソリューションサービス株式会社 ソリューションビジネス本部 コンサルティング 2 部 制御セキュリティコンサルタント 新井 保廣 氏
16:25～ 16:50	講演 5:(CSMS 技術専門部会) 「CSMS 活動による セキュリティ改善成果」	三菱化学エンジニアリング株式会社 技術本部 電計情報システム部 情報グループ 次長 島廻 昭朗 氏
16:50～ 17:20	講演 6: 「制御システムセキュリティの 最新動向」	独立行政法人情報処理推進機構 技術本部 セキュリティセンター 情報セキュリティ技術ラボラトリー 主任 中野 学 氏
17:20～ 17:30	質疑応答	講演者全員

(7)参加者数

	日程	会場	定員	申込人数	参加人数	参加率
1	2014年11月28日	東京会場 (グランパーク 401ホール 東京都港区芝浦3-4-1)	100	79	58	73%
2	2015年2月17日	東京会場 (グランパーク 401ホール 東京都港区芝浦3-4-1)	100	117	79	68%
3	2015年2月26日	大阪会場 (大阪大学中之島センター 講義室703 大阪市北区中之島4-3-53)	100	61	43	70%
			計	257	180	70%

2. アンケート集計結果

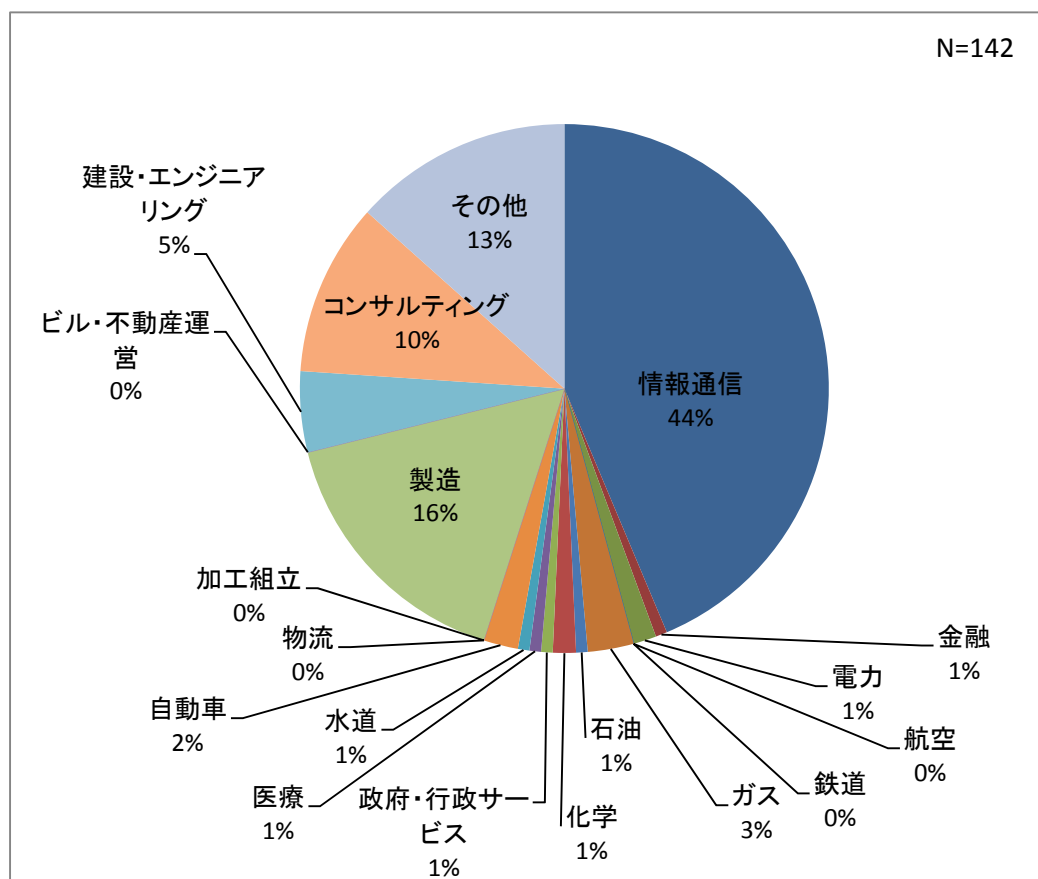
本説明会の参加者合計 180 名のうち、アンケート回答者は 145 名 (81%) であった。アンケート項目の集計分析結果を以下に示す。

なお、無回答を除いた集計としているため、設問により母数が異なっている。

2.1 参加者について

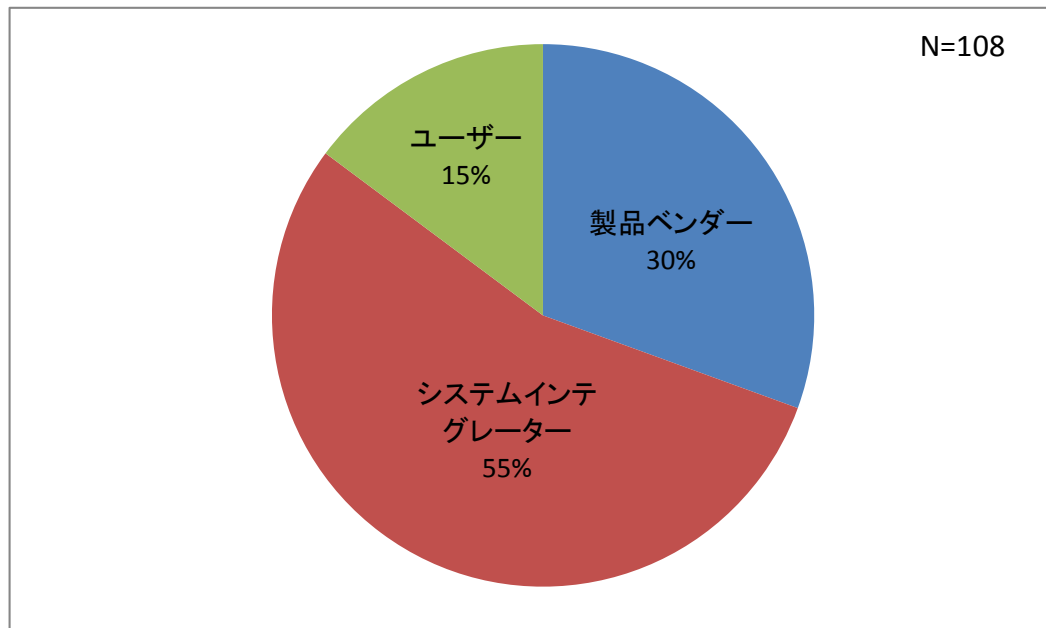
(1)業種

最も多い参加業種は「情報通信 (44%)」で半数近くを占めており、「製造 (16%)」、「コンサルティング (10%)」と続いている。今後製造業が増えることが課題となる。



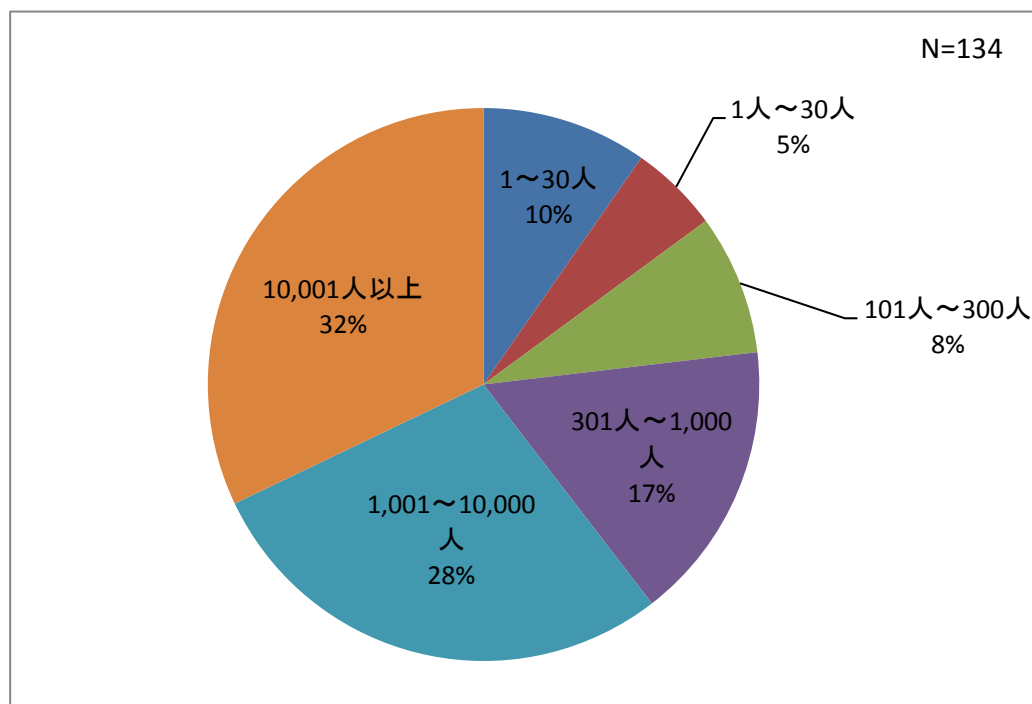
(2) 業態

業態別にみると、「システムインテグレーター(55%)」が半数以上となっており、関心が強いことがうかがわれる。



(3) 従業員

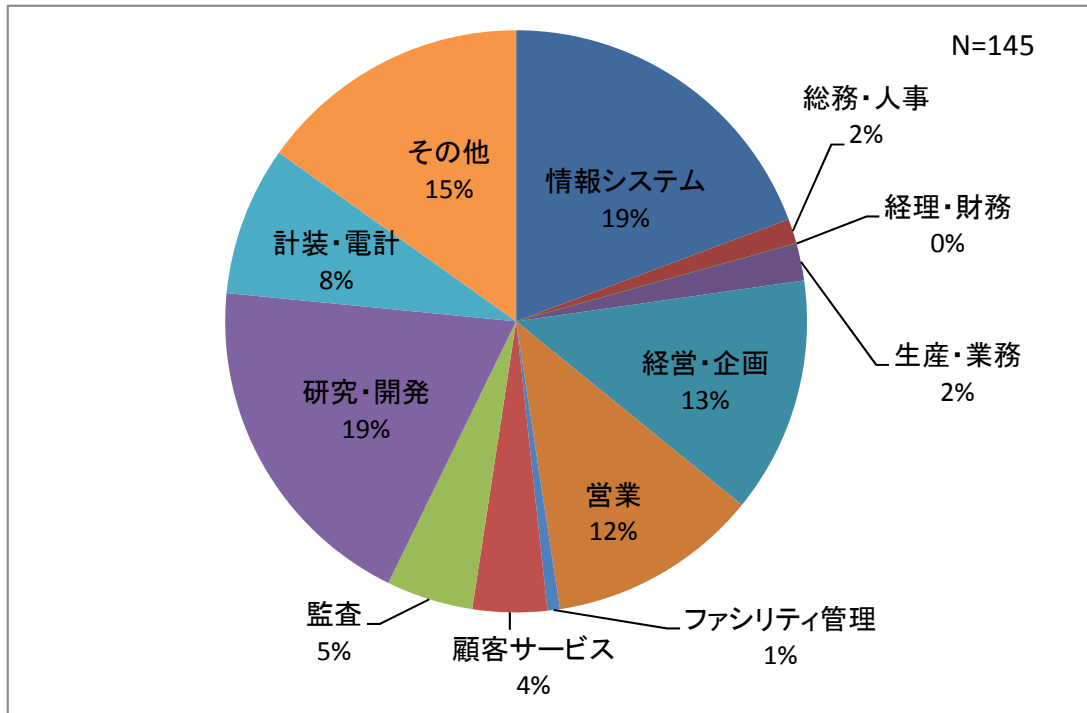
全体的にみると、「1,001人～10,000人(28%)」、「10,001人以上(32%)」となっており、1,000人以上の大規模組織が6割を占めている。



■質問1. あなたの職種、役職等についてお聞かせ下さい。

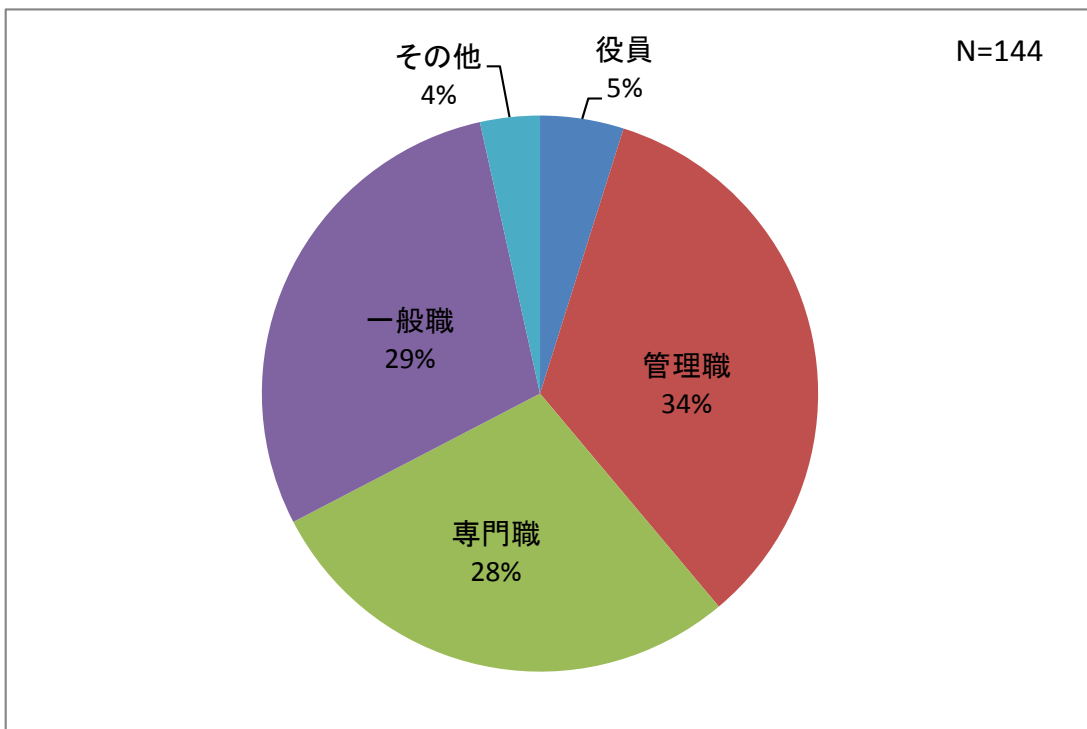
質問1-1 職種

「情報システム」と「研究・開発」がともに19%で、最も多い参加職種となっている。



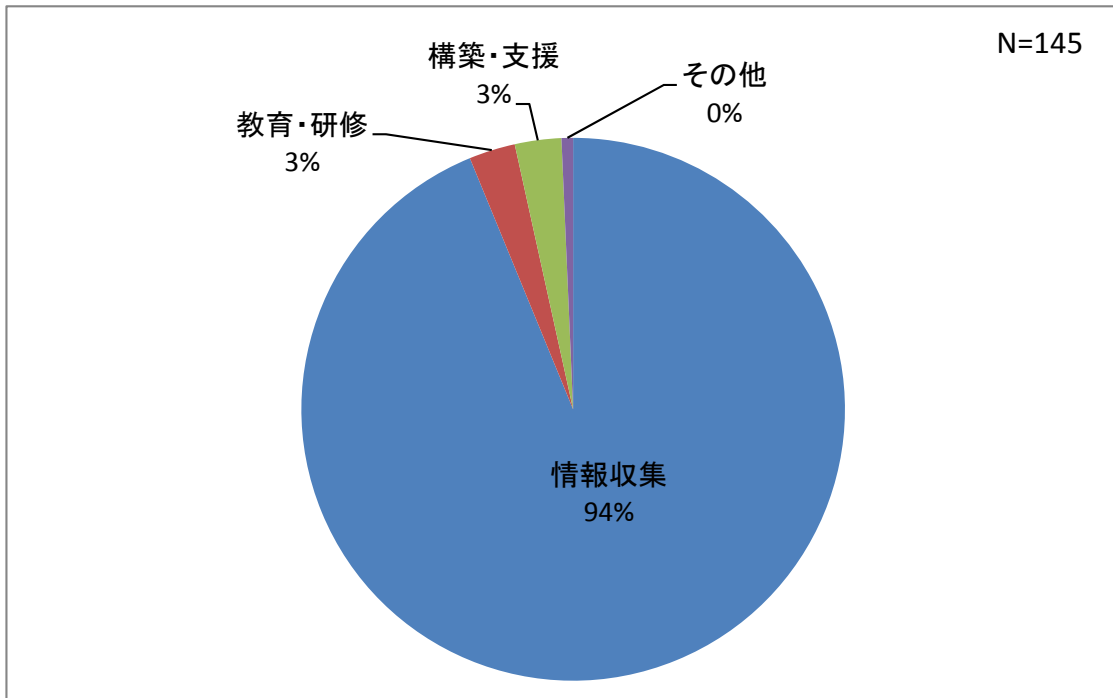
質問1-2 役職

「管理職」、「一般職」、「専門職」がそれぞれ3割前後となっている。



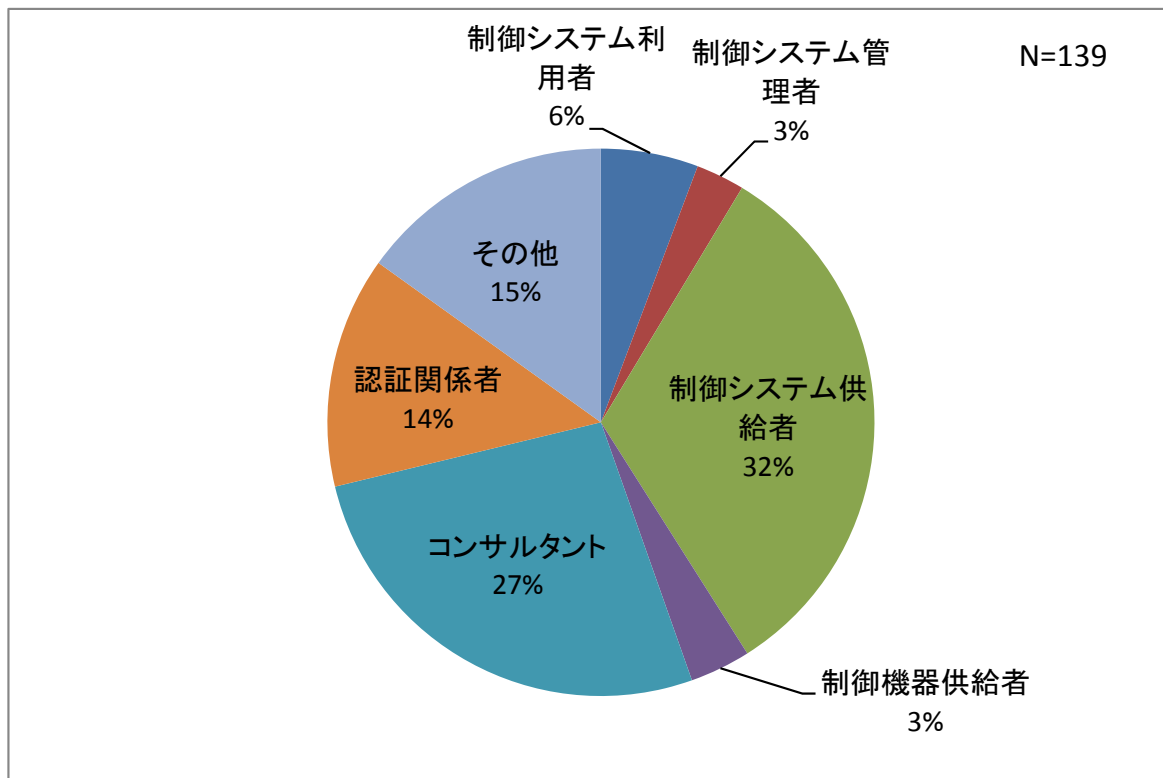
質問1-3 参加目的

9割の方が「情報収集(94%)」を目的として説明会に参加していた。



質問1-4 説明会の参加の立場

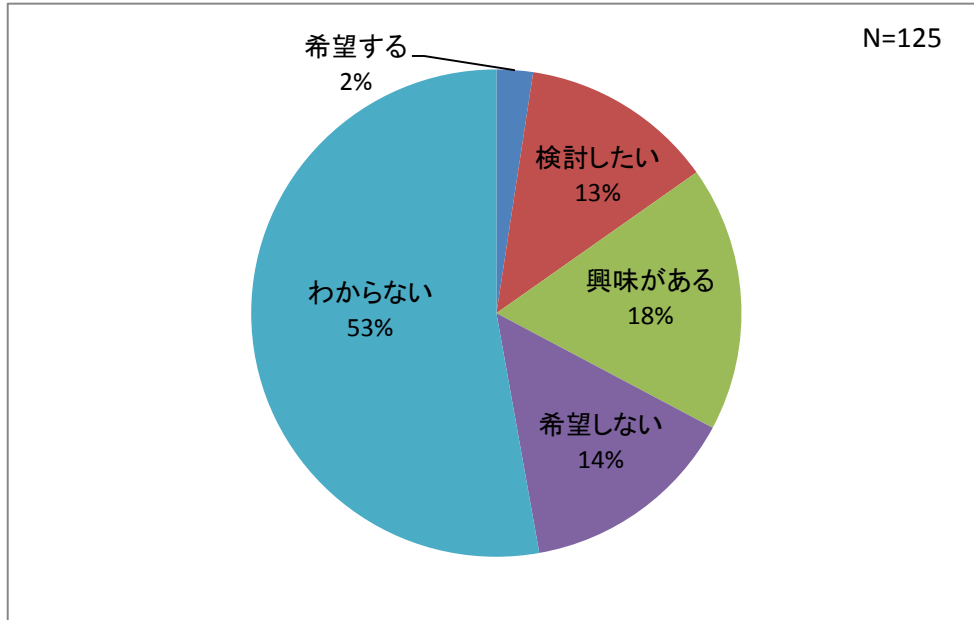
説明会への参加の立場は、「制御システム供給者(32%)」、「コンサルタント(27%)」の順となっている。



■質問2. CSMS 適合性評価制度 (IACS(Industrial Automation and Control System)を対象とした第三者認証制度)の運用が正式に開始されましたが、CSMS 認証等についてお聞かせ下さい。

質問2-1 今後 CSMS 認証取得を希望されますか？

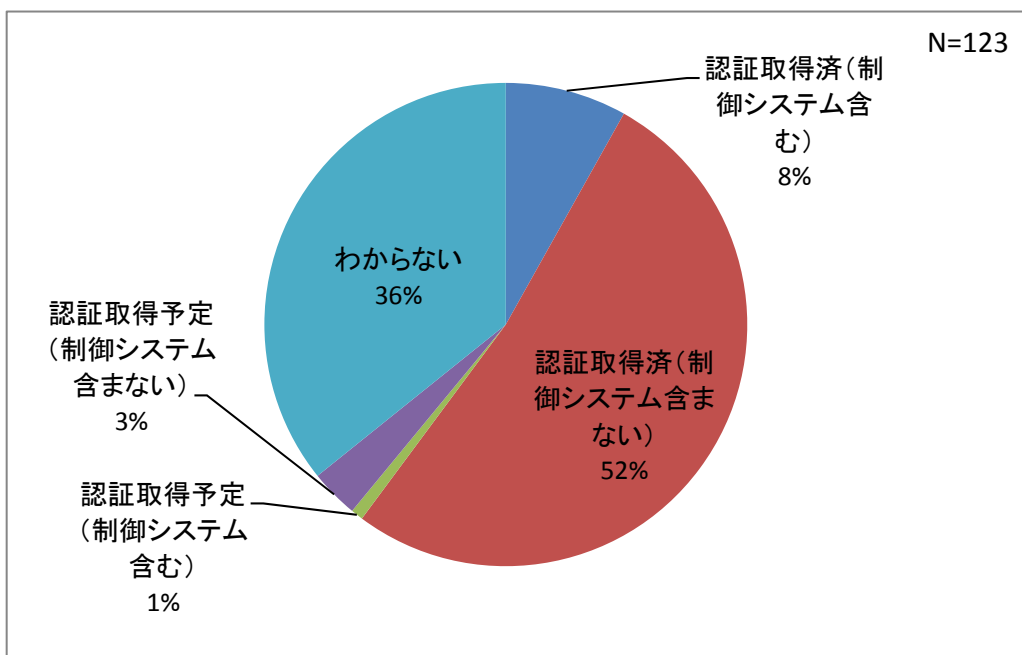
認証取得に対しては「わからない」が半数以上を占めており、「興味がある(18%)」と「検討したい(13%)」に対してもっと普及していきたいところである。



質問2-2 ISMS 認証取得状況についてお聞かせ下さい。

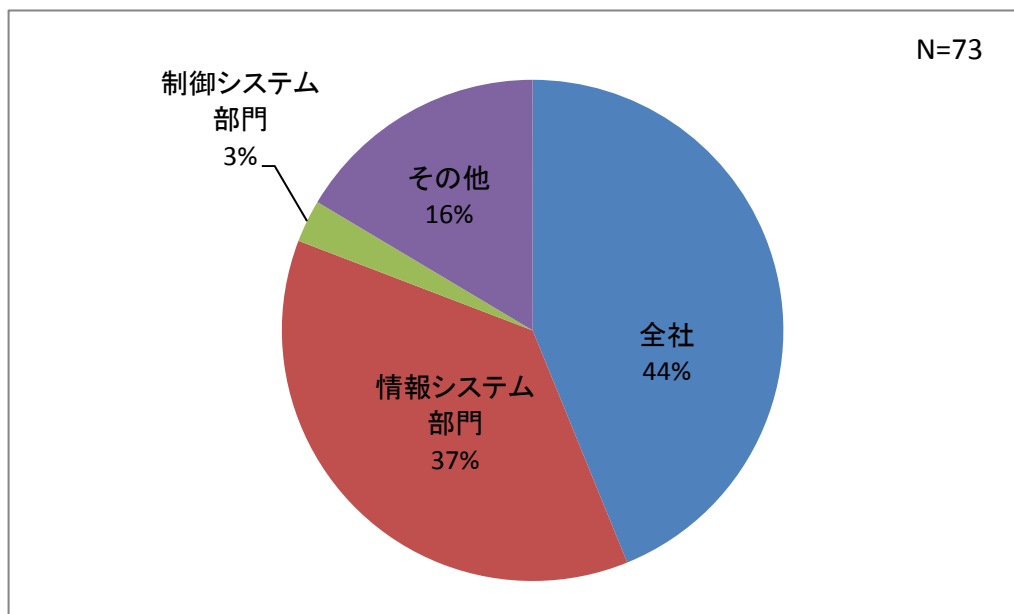
① 組織では ISMS 認証 (ISO/IEC 27001) を取得されていますか？

現状では、ISMS 認証取得済組織が 60%となっているが、ほとんどは「制御システムを含まない(52%)」となっている。



②①で「1. 及び 2.の認証取得済」を選択された方に伺います。認証取得された適用範囲に○を付けて下さい。

「制御システム部門」は 3%となっている。



質問2-3 貴組織の CSMS 構築・運用に関する今後の課題について、差支えない範囲でお聞かせ下さい。

2014/11/28 東京会場－6件

- ・ISMS 適用範囲外については、他部門/他社に依存する。上位組織のため従わざるを得ない。(環境条件)(NW、基幹システム、DC などにおけるセキュリティ対策)
- ・安全保障分野の装備品の CSMS 認証を行う場合の機密保全の問題。既存の ISMS の見直し/追加の検討。
- ・CSMS と QMS の関係(QMS でカバーできないのか?の質問に対する対応)
- ・要求事項に対してリスクとしては把握しているが、コスト等で未対応。
- ・ISMS との統合等について。(重複した運用をなくす。)
- ・受査対象者(組織)への啓蒙、国として、業界団体として。

2015/2/17 東京会場－9件

- ・何がどこまで対象となるか?すべきか?不明確
- ・当社は「サービス業」なので、「CSMS」を取得することはないが、顧客に有力企業があるので取得をおおいに勧めたい。
- ・自社が取得足りうる会社かどうかよく分かりません。
- ・考え方は参考にしたいと思うが、SI 業務においてどこまで CSMS が求められているか判断できない。(質問 2-4 の回答でもある)
- ・CSMS ではないが、サイバーセキュリティ対策として、パッチの適用方法と適用時のバリデーションについて情報漏えい対策(個人情報)

- ・運用するための要員の確保、費用
- ・ルール策定中
- ・担当外のため不明
- ・インフラの制御システムの構築部門があり、構築事業者として CSMS にどう向きあっていくのかを考える必要がある。

2015/2/26 大阪会場－5件

- ・人材育成と組織としての取り組みがカギと認識している。
- ・システムを開発する際にデザインレビューを実施しているが、CSMS と重複する項目の効率化が必要。
- ・経営層の理解、運用者・組織をまたがる教育
- ・別部門の理解と必要性の明確化
- ・特になし

質問2-4 CSMS 適合性評価制度全般に対してご意見・ご要望等ございましたらご意見をお聞かせ下さい。

2014/11/28 東京会場－7件

- ・広く普及ができたと思います。
- ・ISMS との整合性をもう少し明確にして欲しい。
- ・ISMS との関連・位置づけにて、9001 に対する AS(航空宇宙の QMS)の様な関連付けが必要かもしれません。[より高度なセキュリティ、分野固有のセキュリティへの対応]
- ・社会インフラにとって CSMS は社会のセキュリティ上重要なものと思います。マスコミ等による PR もご検討いただければと思います。ISMS と異なり世論の後押しが普及につながると思います。
- ・世界での有効性はどれほどなのでしょう？
- ・CSMS の認知向上が必要。
- ・特にありません。

2015/2/17 東京会場－11件

- ・市場性が不透明です。(認証機関として)
- ・プレゼン早くて、ついて行けず……。
- ・グローバル標準に発展することを期待します。
- ・制度の認知が高まり、認証取得組織が増加してほしい。
- ・ISMS を取得していればかなり「CSMS」認証はたやすい様に聞こえたが、これで間違いはないか逆に心配となった。ISMS と CSMS の差分と CSMS の特長(個別要求事項)をしっかり説明して欲しかった。
- ・ISMS との差異を事例から知りたい。
- ・なぜ取得数が拡大していないのか、その理由など。
- ・他の MS との関係
- ・アセットオーナー、保守運用事業者、システムインテグレーター、それぞれの要求事項をどう解釈するかガイドがあると良いと思います。

- ・普及に向けて活動して下さい。

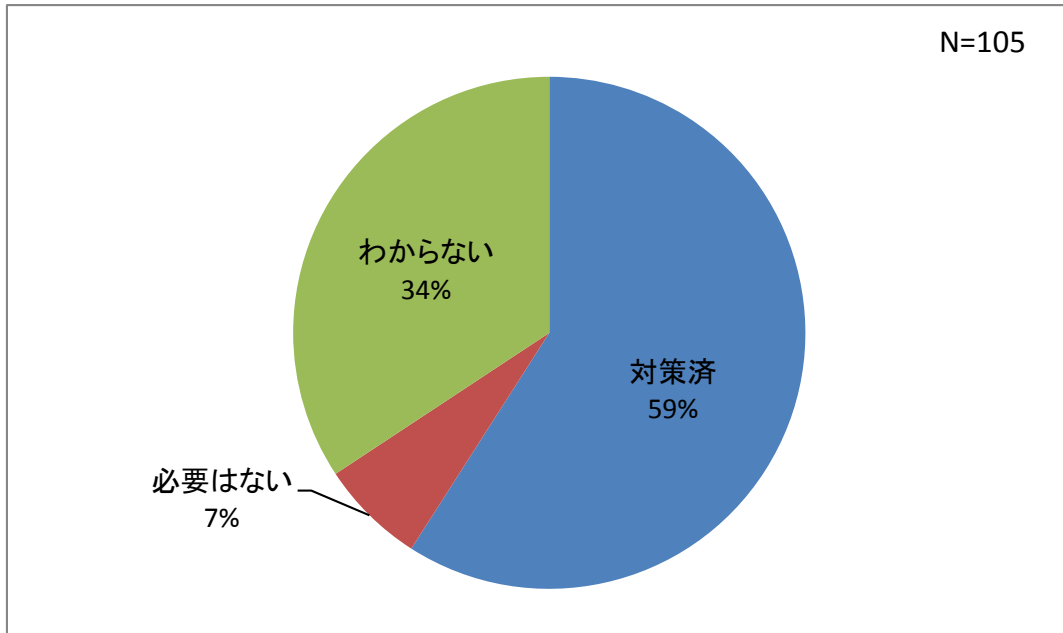
2015/2/26 大阪会場－3件

- ・認証取得のメリットを明確にする。
- ・これが、事業メリット(政治的な要請や税的な優位性など)があるとより推進するのでは？
- ・特になし

■質問3. 制御システムにおけるセキュリティの状況についてお聞かせ下さい。

質問3-1 貴組織ではサイバー攻撃等に対してどのような対策※1を講じていますか？

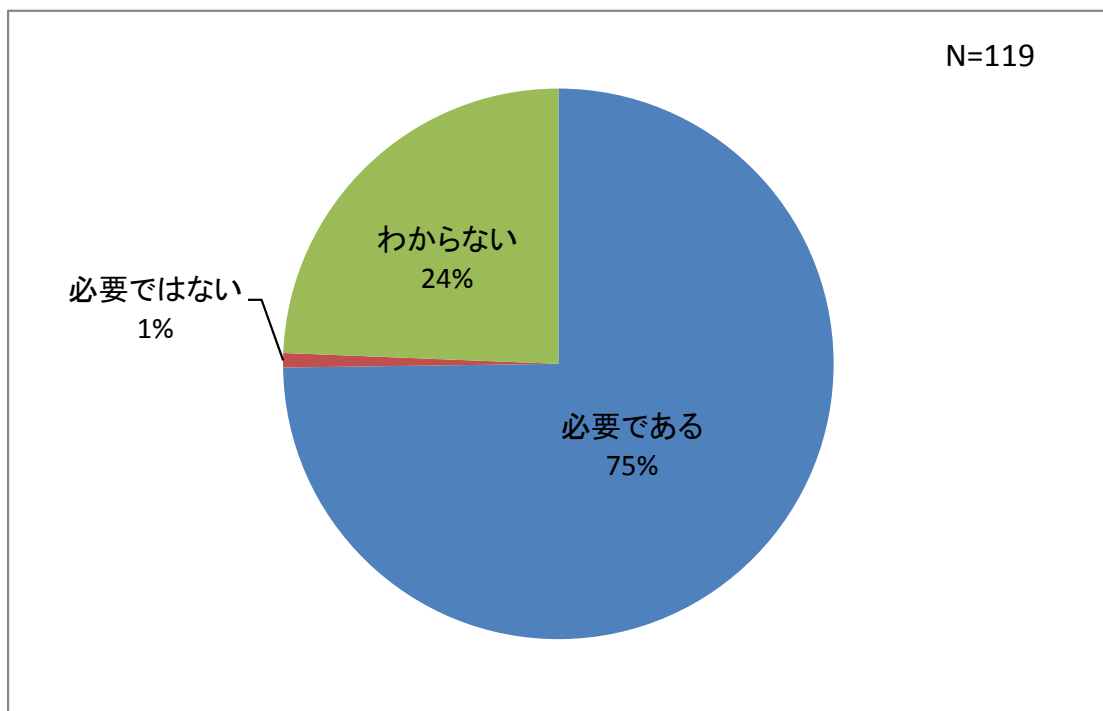
6割の組織がサイバー攻撃等に対して、何らかの対策をしていることがうかがえる。



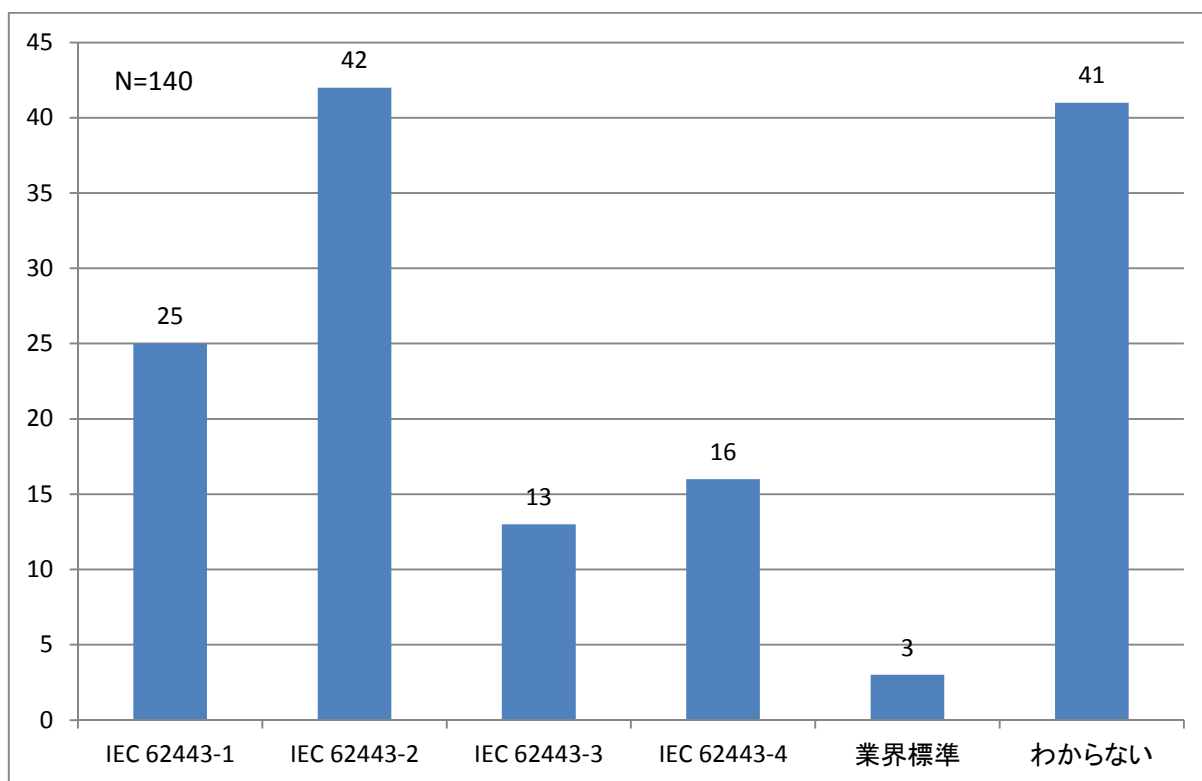
※1 サイバー攻撃等に対する対策:パッチの適用、セキュリティ教育、入退管理、装置の停止、ネットワーク分離、侵入検知装置など

質問3-2 制御システムを運用するにあたって、サイバーセキュリティマネジメントシステム (CSMS)の必要性についてお聞かせ下さい。

7割以上の参加者が、制御システムを運用するにあたってCSMSは必要であると考えている。



質問3-3 制御システムのセキュリティを実現するための基準の一つとして IEC 62443^{※2}シリーズが挙げられますが、どの規格の内容について理解していますか？該当番号に○印をお付け下さい。(複数回答可)



※2 上記に示した IEC 62443 シリーズの規格番号は、数多くのパートから構成されている。

質問3-4 制御システムを運用する上で、セキュリティについて気になる課題あるいは不安要素があればお聞かせ下さい。

2014/11/28 東京会場－6件

- ・安全保障分野の装備品のセキュリティ
- ・どんなシステムを導入し、どのような検証を行えばセキュリティの担保を得られるのか、という点が課題。
- ・実際にインシデントが発生しているのか知りたい。
- ・セキュリティ対策をすべての装置に行うことはコスト面から無理である。
- ・該当しない。
- ・インシデントに関する情報公開が進んでいないと感じる。

2015/2/17 東京会場－9件

- ・新旧多数の制御システムが様々な設備に組み込まれている状況でリスクをどこまで低減できるか不安である。
- ・ISMS との差異があまり明確でなかったところが、今後の課題と感じます。
- ・ISMS 認証取得している組織が、「CSMS」認証取得への早道ですが、製造業の生産部門や建設

業が ISMS を殆ど取得していない現状からすると、いきなり「制御システム(CSMS)を取ろうとは言えない問題がある。もっと「製造業」の生産部門が ISMS を取得するよう促進すべきと思う。

- ・OS の古さなど。
- ・長期間の保守対応(10 年)、パッチ更新・ウイルス対策方法
- ・情報処理サービス業は適用する対象が何になるかわからない。開発が終わると運用に移ります。適用範囲が変更する場合、その都度変更が必要か？
- ・IEC 62443-2 の更新の予定
- ・ISMS との違いをわかるようにして欲しい。
- ・特になし

2015/2/26 会場-7 件

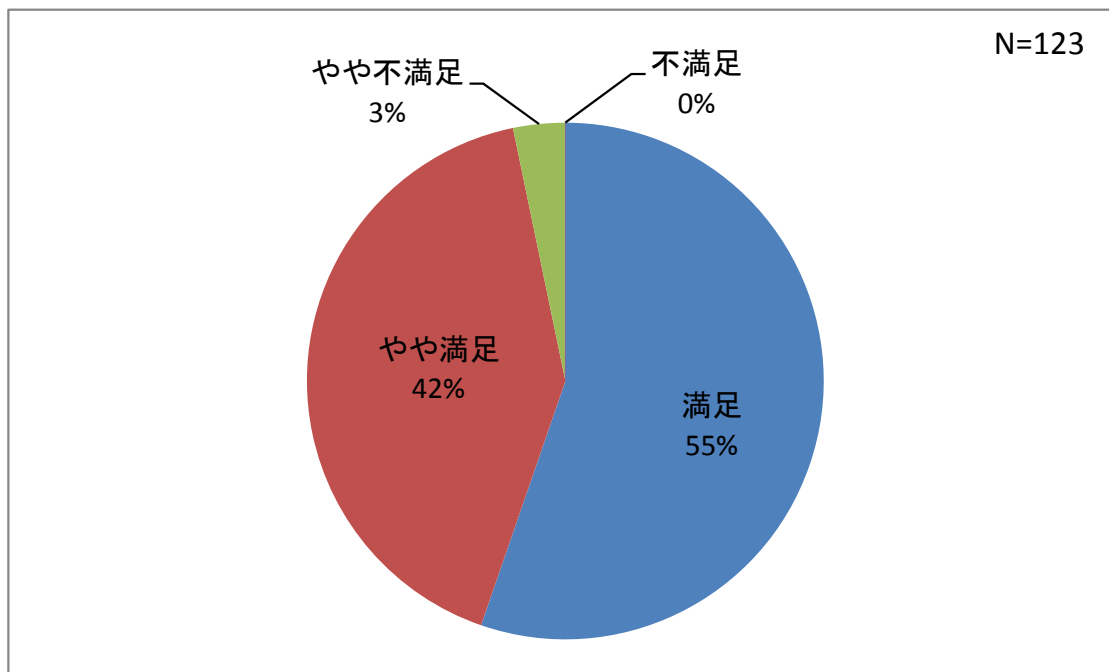
- ・事業者(アセットオーナー)の説得
- ・制御システムが汎用の OS で動作させ、汎用のプロトコルで通信していること。
- ・制御システムの脆弱性情報がわからないので、どういう課題があるのかわからない。
- ・分離されたネットワーク間をつなぐ方法。可搬的ストレージでつなぐのか？その安全性は？
- ・汎用ソフト部品、ツールの安全性
- ・特にない。

■質問4. 今回及び今後のCSMSに関する説明会についてお聞かせ下さい。

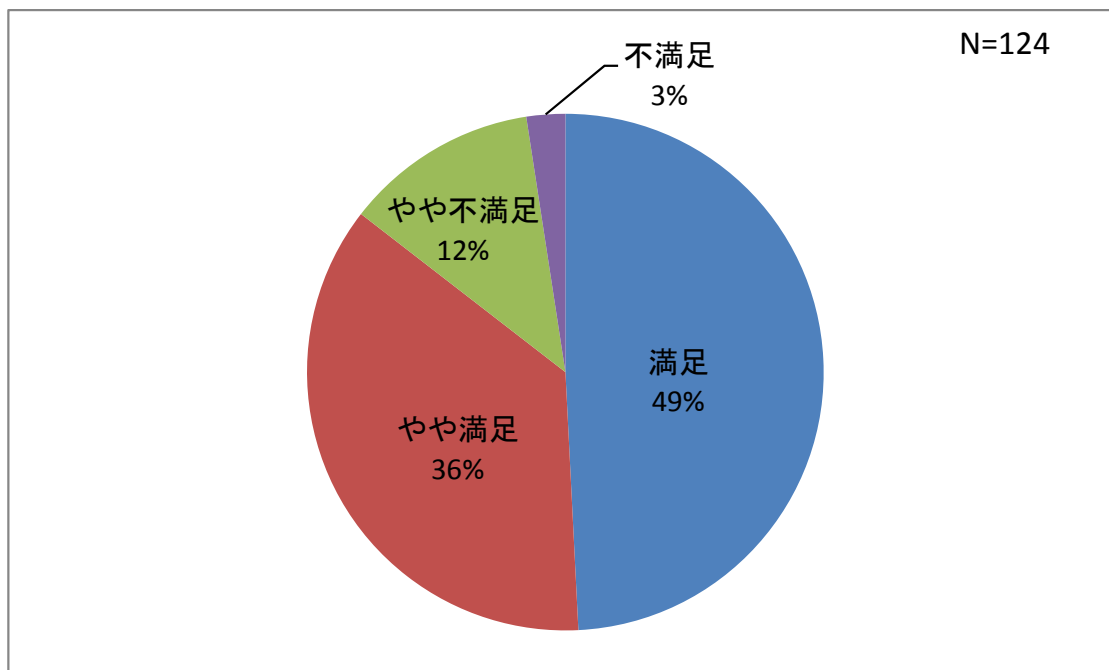
質問4-1 全体の総合評価について

今回の説明会についての総合的評価としては、半数以上の参加者が満足だったとしている。

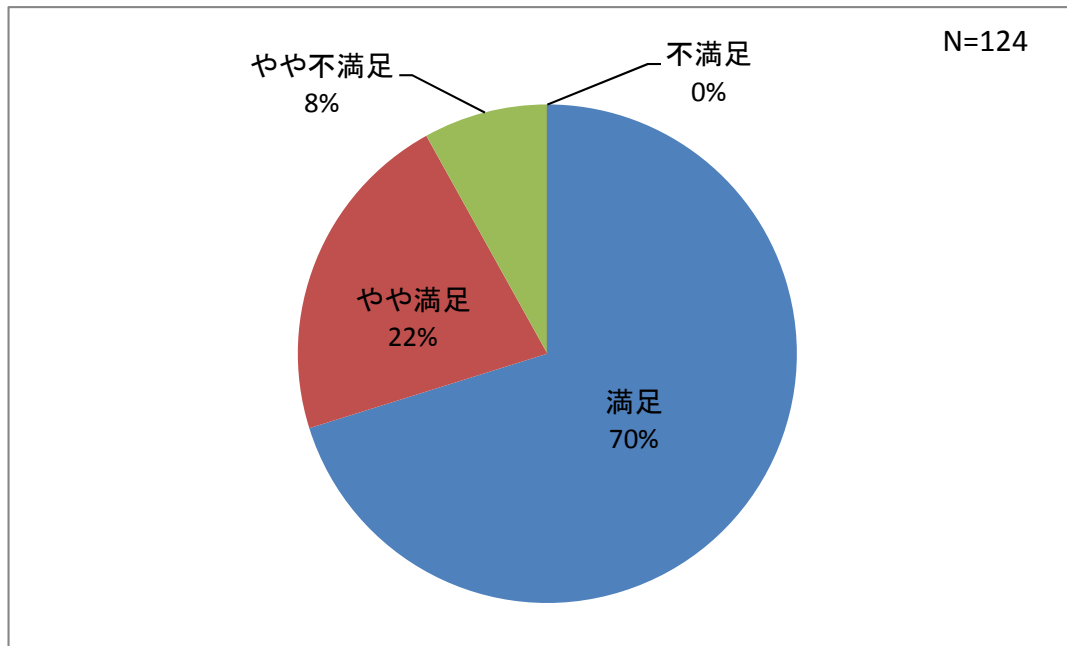
①講演内容



②講演時間



③講演会場



質問4-2 関心のあるセキュリティテーマ、あるいは講演に関するご感想、ご要望(開催希望地域)等ございましたらご意見をお聞かせ下さい。

2014/11/28 東京会場－8件

- ・ISMSとの関係が良く分からなかった。SIerや構築者のイメージはあるが、運用ではISMSにて「システム」として重要資産として位置づけられている？システムの深掘り？
- ・主たる脅威は、テロリズムや国家的規模の攻撃(Information Warfare)があるように思われます。これに対するリスク、管理策があつかわれていることが考慮されます。
- ・制御システムセキュリティ対策に有効な既存のセキュリティ対策、事例。
- ・サイバーセキュリティにおける事故事例、損害、その後の対策、費用などの具体事例を知りたい。
- ・特にありません。
- ・現場(CSMSを運用している)の方の苦労話などがあるとうれしいです。
- ・今後もよろしく願います。ありがとうございました。
- ・セキュリティに関する専門ノウハウや要員体制が不足しているため、CSMS構築を手助けしてくれる外部のコンサルティングサービスが欲しい。

2015/2/17 東京会場－10件

- ・業界別の規格についての講演の開催も希望します。(ex.鉄道)
- ・なし
- ・(1)講演 1:わかりやすかった。(2)講演 2:おもしろかったが、OS イコール 2000 とはあきれた。(3)講演 3:わかりやすい。ただし、上位レベルのリスクアセスはないと言われたが、MSS/ISMS: 2014では、あります。CSMSもISMS:2014年版に移行すべきです。(4)講演 4:わかりやすいが、得るところなし。(5)講演 4-1:事例は参考度高い。(多謝)(6)講演 4-2:参考度高い。(正直ベースで有効度高い)(7)講演 7:(IPA)これからのサイバー攻撃の対策参考度高し。(自動車、医療

機器)

- ・制御セキュリティについて次回企画を期待します。
- ・勉強になりました。ありがとうございます。
- ・認証制度については、複雑な部分が多いので事例を交えた説明があるとうれしく思います。また、CSMS 適用の具体的メリットがあるとうれしいです。
- ・①医療機器に関するサイバーセキュリティ対応について。②セキュリティ対策事例の紹介(医療機器、制御システム)東京近辺での開催を希望
- ・CSMS を適用することのデメリット(課題)についても知りたかった。生産性について、プロセス(工数)が増えたりするのではないのでしょうか？EDSA に対応している製品が市場にまだ少ないのではないのでしょうか？CSMS を構築・運用を支援する商品が増えないと導入は難しく感じる。
- ・ISMS の簡素化や効率化の事例
- ・1 つの講演時間が 30 分と短い。1 件をもう少し長くして欲しい。

2015/2/26 大阪会場－10 件

- ・EDSA 認証の勉強会もあれば参加したい。
- ・セキュリティはいろいろな視点を持たなければ、回避することができないのだと感じました。そして、完全に防ぐことができないんだと教えられました。
- ・EDSA、SSA
- ・短時間に少し詰め込みすぎではないかと思う。
- ・車や IOT のセキュリティ(家電やその他の機器を含む)。
- ・IOT など組込みシステム/機器のセキュリティについて。
- ・体験をまじえたお話、興味深く聞かせていただきました。
- ・EDSA についての説明会の開催を希望します。
- ・単純にベストプラクティス等の講演があればよい。
- ・セキュリティに関する動向を知りたく受講しました。講演 1.5.6 は、特に参考になりました。
- ・特になし。

3. 参考

CSMS に関する説明会アンケート

本日はお忙しい中、本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：□情報通信 □金融 □電力 □航空 □鉄道 □ガス □石油 □化学 □政府・行政サービス □医療 □水道 □自動車 □物流 □加工組立 □製造 □ビル・不動産運営 □建設・エンジニアリング □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つのみ印をつけて下さい。
業態：制御システムに関連する □製品ベンダー □システムインテグレーター(構築事業者) □ユーザー(運用事業者/所有者)
従業員数：□1～30人 □31人～100人 □101人～300人 □301人～1,000人 □1,001人～10,000人 □10,001人以上

■質問1. あなたの職種、役職等に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. 監査	10. 研究・開発
11. 計装・電計	12. 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 本説明会の参加目的をお聞かせ下さい。

1. 情報収集	2. 教育・研修	3. 構築・支援	4. その他（ ）
---------	----------	----------	-----------

質問1-4 本説明会参加の立場をお聞かせ下さい。

1. 制御システム利用者	2. 制御システム管理者	3. 制御システム供給者	4. 制御機器供給者
5. コンサルタント	6. 認証関係者	7. その他（ ）	

■質問2. CSMS 適合性評価制度 (IACS (Industrial Automation and Control System) を対象とした第三者認証制度) の運用が正式に開始されましたが、CSMS 認証等についてお聞かせ下さい。

質問2-1 今後 CSMS 認証取得を希望されますか？

1. 認証取得を希望する	2. 認証取得を検討したい	3. 興味があり詳細を聞いてみたい
4. 認証取得を希望しない	5. わからない	

質問2-2 ISMS 認証取得状況についてお聞かせ下さい。

①貴組織では ISMS 認証 (ISO/IEC 27001) を取得されていますか？

1. 認証取得済 (制御システムを含む)	2. 認証取得済 (制御システムを含まない)	3. 認証取得予定 (制御システムを含む)	4. 認証取得予定 (制御システムを含まない)
5. わからない			

②①で「1. 及び2. の認証取得済」を選択された方に伺います。認証取得された適用範囲に○を付けて下さい。

1. 全社	2. 情報システム部門	3. 制御システム部門	4. その他（ ）
-------	-------------	-------------	-----------

質問2-3 貴組織の CSMS 構築・運用に関する今後の課題について、差支えない範囲でお聞かせ下さい。

--

質問2-4 CSMS 適合性評価制度全般に対してご意見・ご要望等ございましたらご意見をお聞かせ下さい。

--

■質問3. 制御システムにおけるセキュリティの状況についてお聞かせ下さい。

質問3-1 貴組織ではサイバー攻撃等に対してどのような対策^{※1}を講じていますか？

1. すでに対策済 (対策概要:)	2. 対策の必要はない (理由:)
3. わからない(理由:)	

※1 サイバー攻撃等に対する対策: パッチの適用、セキュリティ教育、入退管理、装置の停止、ネットワーク分離、侵入検知装置など

質問3-2 制御システムを運用するにあたって、サイバーセキュリティマネジメントシステム (CSMS) の必要性についてお聞かせ下さい。

1. 必要である	2. 必要ではない	3. わからない
上記回答の理由:		

質問3-3 制御システムのセキュリティを実現するための基準の一つとして IEC 62443^{※1} シリーズが挙げられますが、どの規格の内容について理解していますか？該当番号に○印をお付け下さい。(複数回答可)

1. IEC 62443-1	この規格全体の用語・概念等の定義
2. IEC 62443-2	組織に対するセキュリティマネジメントシステム
3. IEC 62443-3	システムのセキュリティ要件や技術概説
4. IEC 62443-4	部品 (装置・デバイス) 層におけるセキュリティ機能や開発プロセス要件
5. 業界標準 ()	
6. わからない	

※1 上記に示した IEC 62443 シリーズの規格番号は、数多くのパートから構成されている。

質問3-4 制御システムを運用する上で、セキュリティについて気になる課題あるいは不安要素があればお聞かせ下さい。

--

■質問4. 今回及び今後の CSMS に関する説明会についてお聞かせ下さい。

質問4-1 全体の総合評価について

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

質問4-2 関心のあるセキュリティテーマ、あるいは講演に関するご感想、ご要望 (開催希望地域) 等ございましたらご意見をお聞かせ下さい。

--

アンケートに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、CSMS 適合性評価制度の普及活動の参考とさせていただきます。

以上