制御システムユーザ企業の実態調査報告書

2016 年 3 月

IPA 独立行政法人情報処理推進機構
Information-technology Promotion Agency, Japan

目　次

1. 調査概要

1.1. 調査目的

昨年度調査において、独立行政法人情報処理推進機構（以下、IPA）では、公表された脆弱性情報への対応など制御システムユーザ企業（大手～中堅）がどのように対応すべきかを解説した啓発資料「制御システム利用者のための脆弱性対応ガイド」を策定した。

しかし、制御システムユーザ企業の多くが制御システムの脆弱性に関するリスクを十分に把握しておらず、自ら積極的にこの啓発資料にアクセスする可能性は低いと考えられる。また、制御システム分野では、セキュリティの脅威に関する意識が乏しいケースや脆弱性の存在を把握しても迅速に対応することが困難なケースもあるため、JVN による公表モデルが必ずしも有効に機能しない可能性がある。

そこで、どのような形であれば制御システムユーザ企業に有益な情報提供を実現できるかを探るため、制御システム利用の実情とセキュリティ意識について把握する必要がある。より具体的な実態把握と啓発を目指して、制御システムユーザ企業を対象としたアンケート調査とヒアリング調査を実施し、その結果をもとに、内容をまとめ、「制御システム利用者のための脆弱性対応ガイド」に反映する。

1.2. 調査方針

本年度の調査方針を図 1-1 に示す。

本年度は制御システムユーザ企業を対象とした郵送でのアンケート調査及び、アンケート回答者または有識者を対象としたヒアリング調査を実施する。

調査結果をもとに、本報告書を取りまとめ、調査結果を「制御システム利用者のための脆弱性対応ガイド」へ反映する。

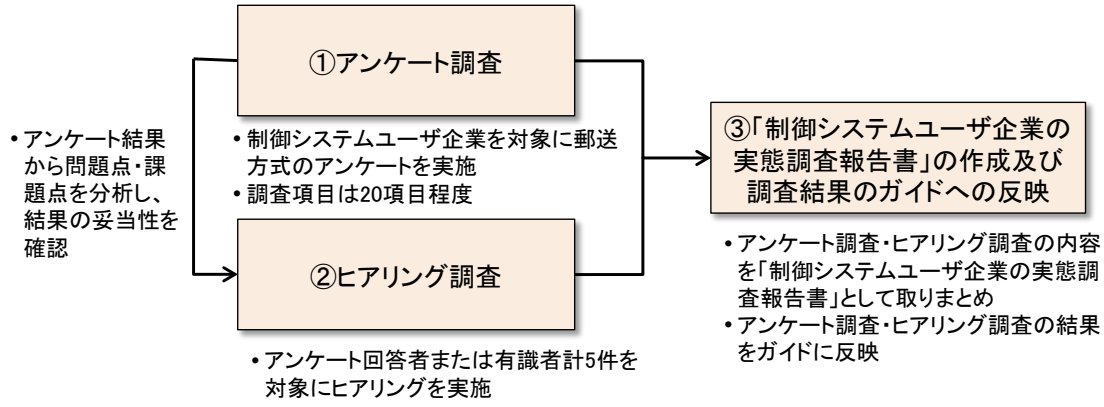

①アンケート調査
・制御システムユーザ企業を対象に郵送方式のアンケートを実施
・調査項目は20項目程度
・アンケート結果から問題点・課題点を分析し、結果の妥当性を確認
②ヒアリング調査
・アンケート回答者または有識者計5件を対象にヒアリングを実施
③「制御システムユーザ企業の実態調査報告書」の作成及び調査結果のガイドへの反映
・アンケート調査・ヒアリング調査の内容を「制御システムユーザ企業の実態調査報告書」として取りまとめ
・アンケート調査・ヒアリング調査の結果をガイドに反映

図 1-1　調査方針

2.アンケート調査

2.1.調査概要

制御システムユーザ企業を対象に、制御システムセキュリティに対する意識や被害状況、取組状況等に関するアンケート調査を実施した。

アンケート調査対象企業は PA（Process Automation）及び FA（Factory Automation）ユーザ企業のうち、上場企業（東証 1 部・2 部、マザーズ、大証 1 部・2 部、JASDAC、ヘラクレス、地方市場）から抽出した。

調査は郵送方式で実施し、有効回答 100 件の回答を得た。

表 2-1 アンケート調査の概要

調査対象	PA（食品、化学、医薬品、石油・石炭製品、ゴム製品、ガラス・土石製品、鉄鋼、非鉄金属、金属製品、電気・ガス）及び FA（機械、電気機器、輸送用機器、精密機器）ユーザ企業のうち上場企業（東証 1 部・2 部、マザーズ、大証 1 部・2 部、JASDAC、ヘラクレス、地方市場）
回答者層	・　経営企画、リスク管理部門等のリスク管理ご担当の方 ・　現場部門の制御システムの導入及び調達ご担当の方 ・　制御システムの運用に携わる管理者の方 ・　情報通信システム部門のセキュリティご担当の方
調査方法	郵送方式（1140 件発送）
回収件数	有効回答 100 件
主な設問	・　制御システムセキュリティに対する意識 ・　制御システムセキュリティの被害経験 ・　制御システムセキュリティの取組状況　等

2.2.調査結果

アンケート調査の結果について、主な調査項目ごとに整理する。なお、アンケート回答企業・回答者の属性情報に関しては参考資料 2 を参照。

2.2.1.制御システムセキュリティリスクに対する認識

制御システムセキュリティリスクを「認識して対策済み」と回答した企業は 23.0%、「認識して対応中」と回答した企業は 39.0%で、対策を開始している企業は約 6 割となっている。

また、セキュリティリスクを「認識していない」と回答した企業は 7.0%で、多くの企業で制御システムのセキュリティリスクは認識されている。

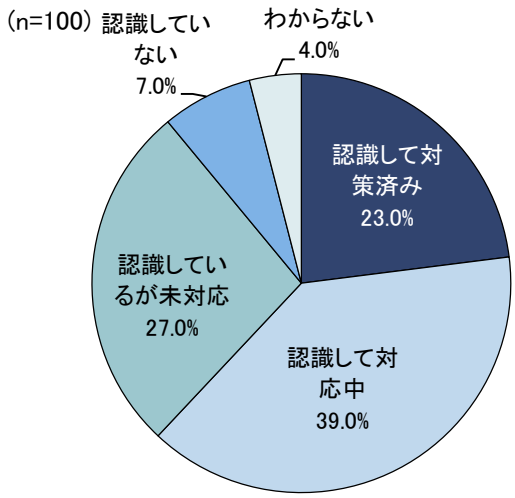


図 2-1 制御システムセキュリティリスクに対する認識

重要インフラ（電気・ガス業、化学、石油）とその他の業種を比較したところ、重要インフラのほうが「認識して対策済み」「認識して対応中」の回答割合が高く、制御システムセキュリティリスクに対する意識が高い。

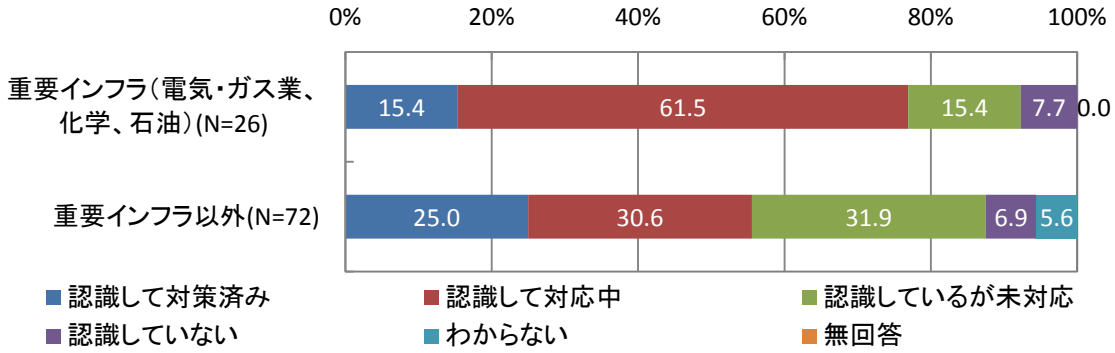


図 2-2 制御システムセキュリティリスクに対する認識（重要インフラとその他業種）

2.2.2. 制御システムセキュリティインシデントの発生・対応状況

(1) 制御システムセキュリティ上の事件・事故・ヒヤリハット発生状況

過去 5 年間で制御システムセキュリティ上の「事件・事故の経験あり」と回答した企業は 4.0%、「事件・事故はないがヒヤリハットの経験あり」との回答は 12.0%となっている。

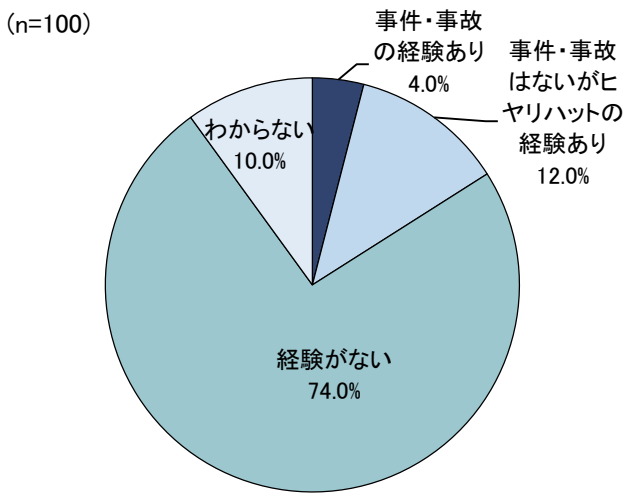


図 2-3 過去 5 年間の制御システムセキュリティ上の事件・事故・ヒヤリハット発生状況

(2) 制御システムセキュリティ上の事件・事故やヒヤリハットの発覚経緯

事件・事故・ヒヤリハットの発覚経緯は、「ウイルス対策ソフトで検出した」が最も多い。

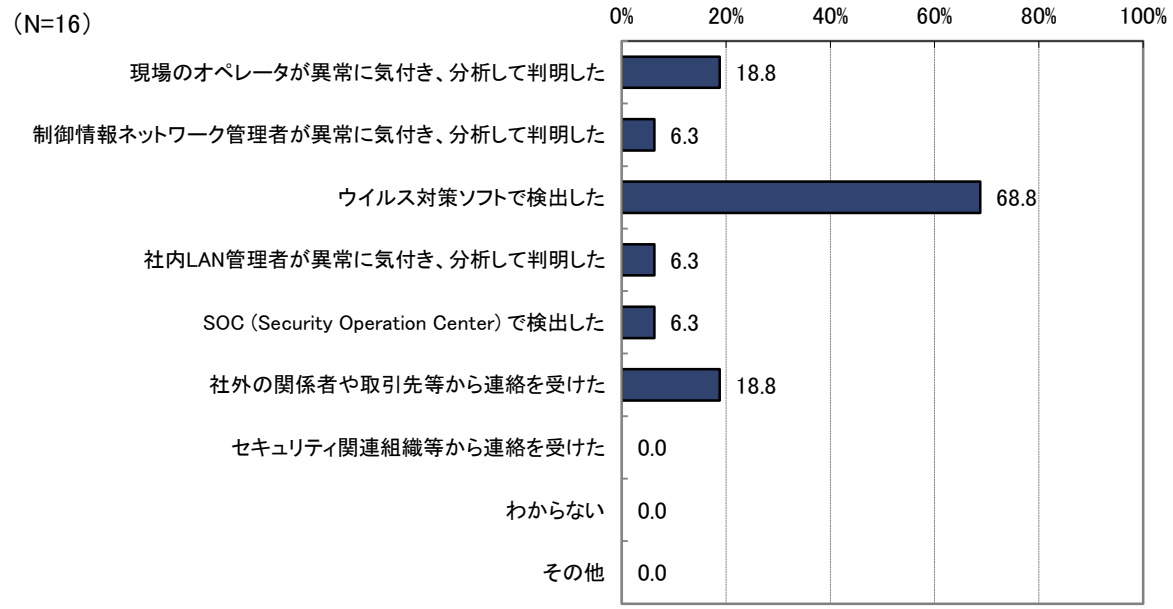


図 2-4 制御システムセキュリティ上の事件・事故・ヒヤリハットの発覚経緯

(3) セキュリティ上の事件・事故・ヒヤリハットの発生時の対応

インシデント発生時の対応として、制御システムベンダに依頼する場合よりも、自社で対応する割合のほうが高い。

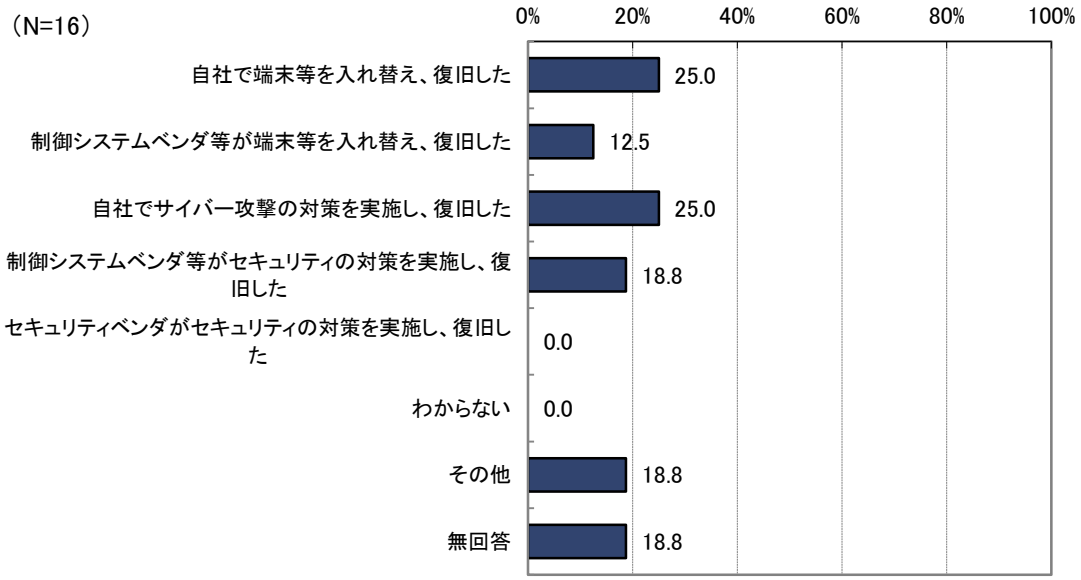


図 2-5 セキュリティ上の事件・事故・ヒヤリハットの発生時の対応

(4) セキュリティ上の事件・事故による制御システム停止期間

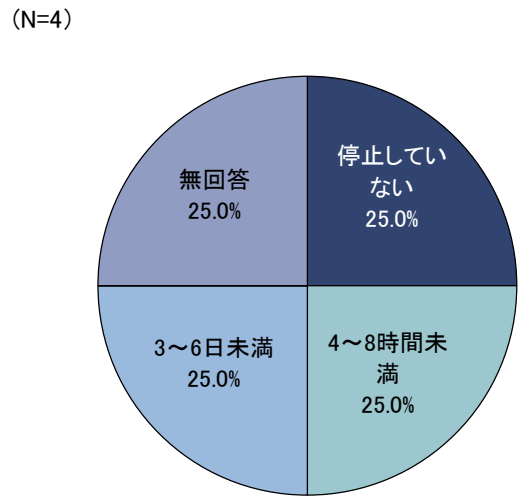


図 2-6 セキュリティ上の事件・事故による制御システム停止期間

2.2.3. 制御システムセキュリティ対策に必要な予算・人員確保状況

必要な人員を「十分に確保できている」「おおむね確保できている」と回答した企業は 25.0%で、必要な人員・予算を確保できている企業はまだ多くない。「特に確保していない」と回答した企業は 41.0%となっており、制御システム

セキュリティのための予算・人員を確保していない企業の割合が高い。

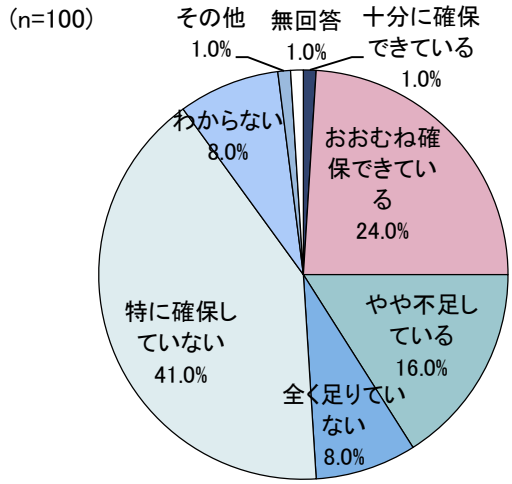


図 2-7 制御システムセキュリティ対策に必要な予算・人員確保状況

予算・人員確保状況を売上高別にみると、売上高 1,000 億円未満の企業では、「特に確保していない」との回答が半数を超えている。

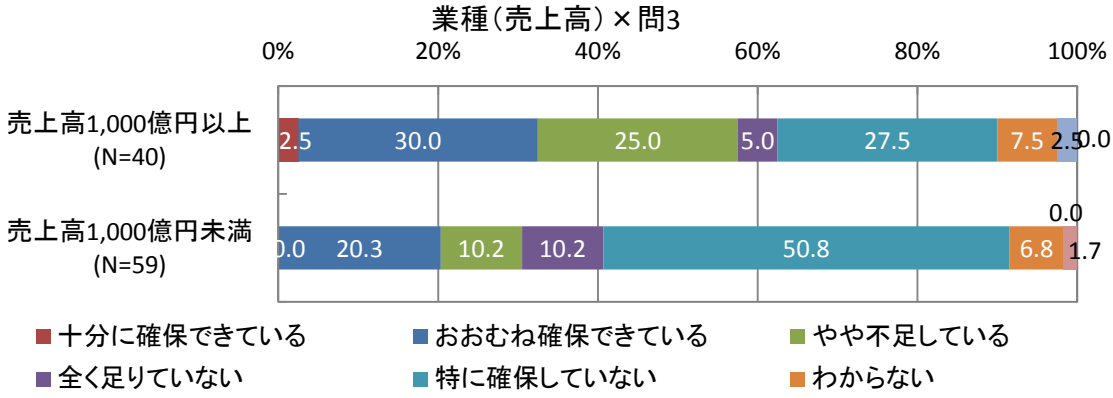


図 2-8 制御システムセキュリティ対策に必要な予算・人員確保状況（売上高別）

2.2.4. 制御システムセキュリティ担当組織の設置状況

制御システムセキュリティの担当組織（担当者）を設置している企業は 23.0%となっており、担当組織（担当者）はないが事実上対応しているとの回答は 42.0%となっている。

また、担当組織(担当者)を設置している割合は重要インフラのほうが高く、重要インフラ以外の業種では、担当組織（担当者）がいない割合が高い。

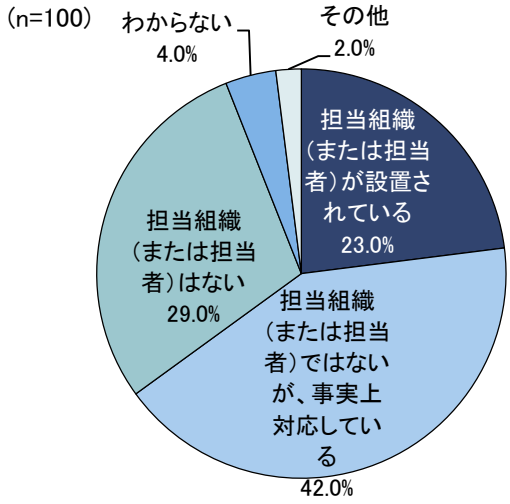


図 2-9 制御システムセキュリティ担当組織の設置状況

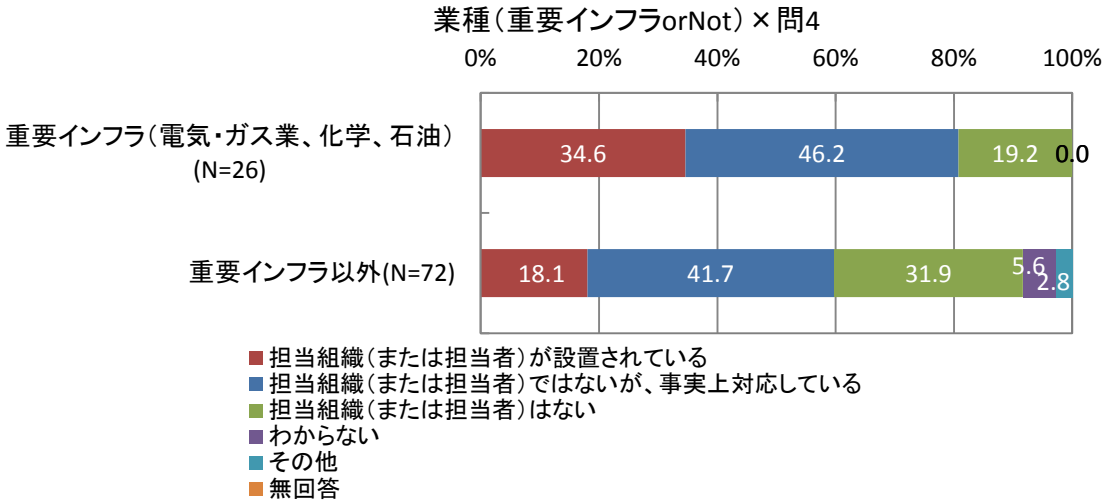


図 2-10 制御システムセキュリティ担当組織の設置状況（重要インフラとその他業種）

2.2.5. 制御システムのセキュリティ対策把握状況

制御システムのセキュリティ対策を「十分に把握できている」「ある程度把握できている」と回答した企業は 56.0%となっている。一方で、「あまり把握できていない」「全く把握できていない」と回答した企業は 39.0%となっており、対策状況を十分に把握できていない企業の割合は高い。

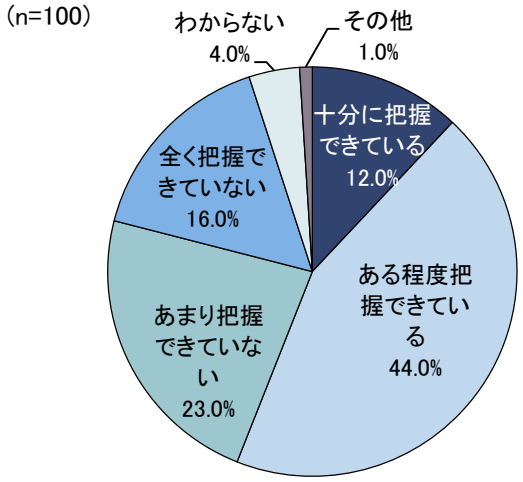


図 2-11 制御システムセキュリティ対策の把握状況

2.2.6. 制御システム調達時のセキュリティ要件の有無

制御システム調達時に、「通常、セキュリティ要件が含まれている」と回答した企業は 27.0%、「セキュリティ要件が含まれることもある」と回答した企業は 24.0%である。

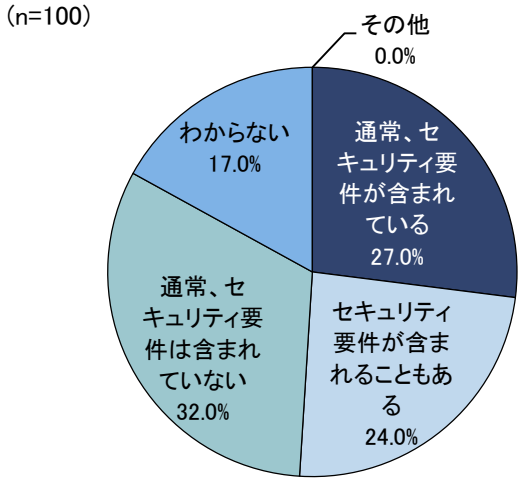


図 2-12 制御システム調達時の要求仕様におけるセキュリティ要件の有無

2.2.7. 制御システム保守業務

(1) 制御システム保守業務の外部（子会社を含む）への委託状況

制御システム保守業務の外部（子会社を含む）への委託状況について、「基本的に外部業者に委託している」と「自社で保守しているものと外部事業者に委

託しているものが混在している」を合わせると 60.0%となっており、外部へ委託しているケースが多い。「基本的に自組織で保守している」と回答した企業は 36.0%で、自社で保守を行っている企業の割合も高い。

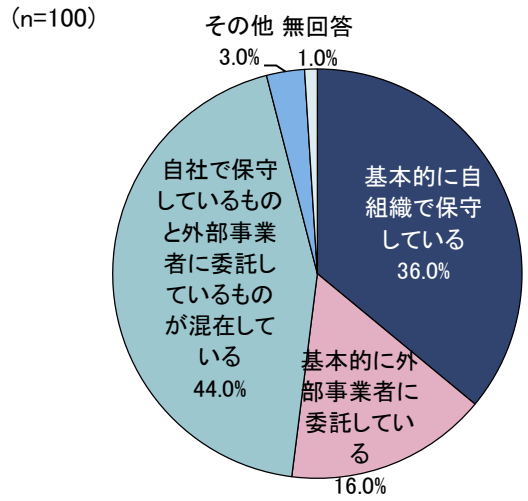


図 2-13 制御システム保守業務の外部（子会社を含む）への委託状況

(2)制御システム保守契約にセキュリティに関する項目が含まれているか

制御システムの保守契約に「通常、セキュリティ項目が含まれている」は 25.4%、「セキュリティ項目が含まれることもある」と回答した企業は 31.7%となっている。

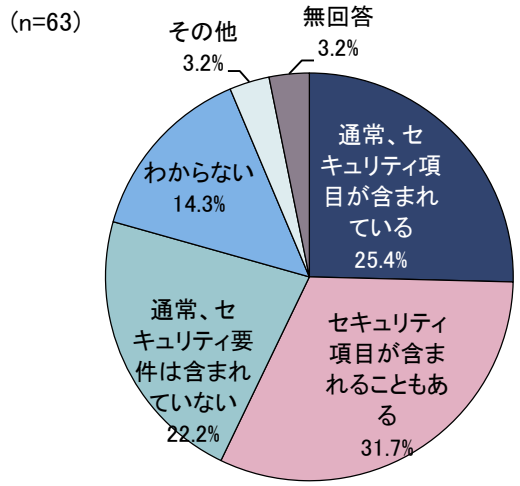


図 2-14 制御システム保守契約にセキュリティに関する項目が含まれているか

2.2.8. 制御システムに対する脅威を抑制する対策の実施状況

（1）USB メモリ（2）操作端末の入れ替え/保守用端末の管理（3）リモート

メンテナンス回線に関する対策は、現在の「制御システム利用者のための脆弱性対応ガイド」で記載した項目である。ガイドに記載した項目に関しては、対策をとっている企業の割合が高い。また、どの対策も売上高が 1,000 億円以上の企業のほうが、何らかの対策をとっている割合が高い。

(1)USB メモリ

USB メモリ対策としては、利用規約の策定や利用可能な USB メモリを特定し管理している回答の割合が高い。「USB ポートを取り外す/ロックする」まで実施している企業は 19%である。

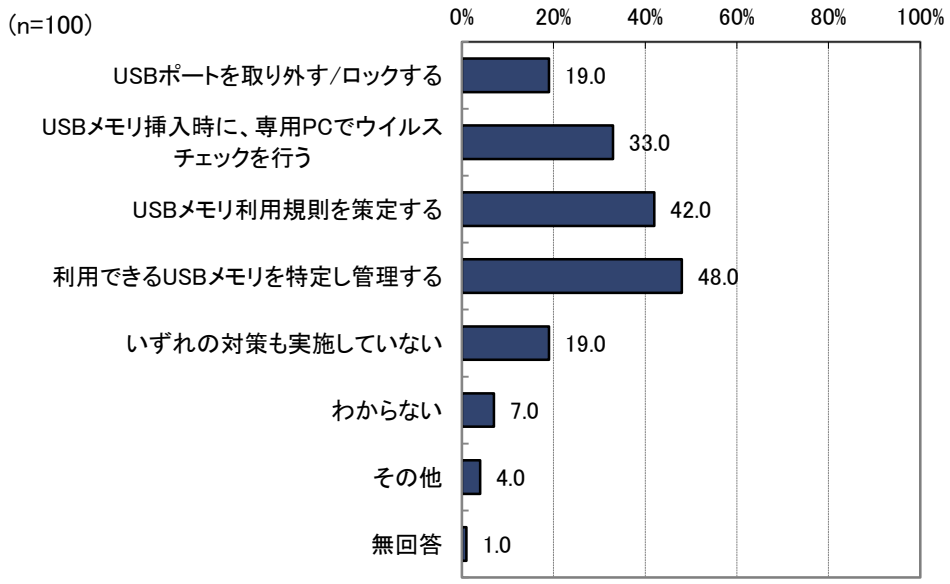


図 2-15 USB メモリ

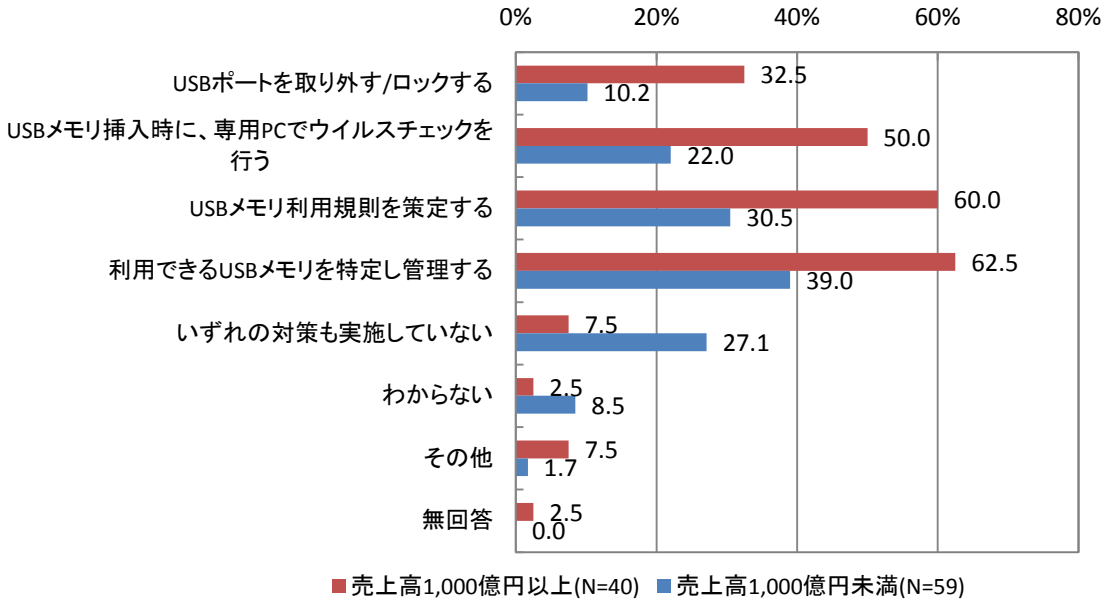


図 2-16 USB メモリ（売上高別）

(2) 操作端末の入れ替え/保守用端末の管理

「操作端末の入れ替え時にウイルスチェックを行う」との回答は 48.0%、「保守用端末等の機器の管理（持ち込み禁止等）を行う」は 52.0%となっている。

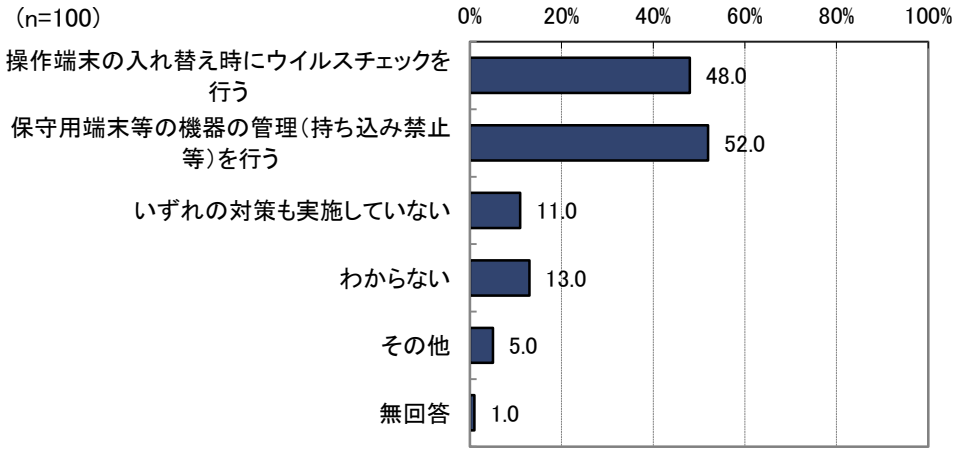


図 2-17 操作端末の入れ替え/保守用端末の管理

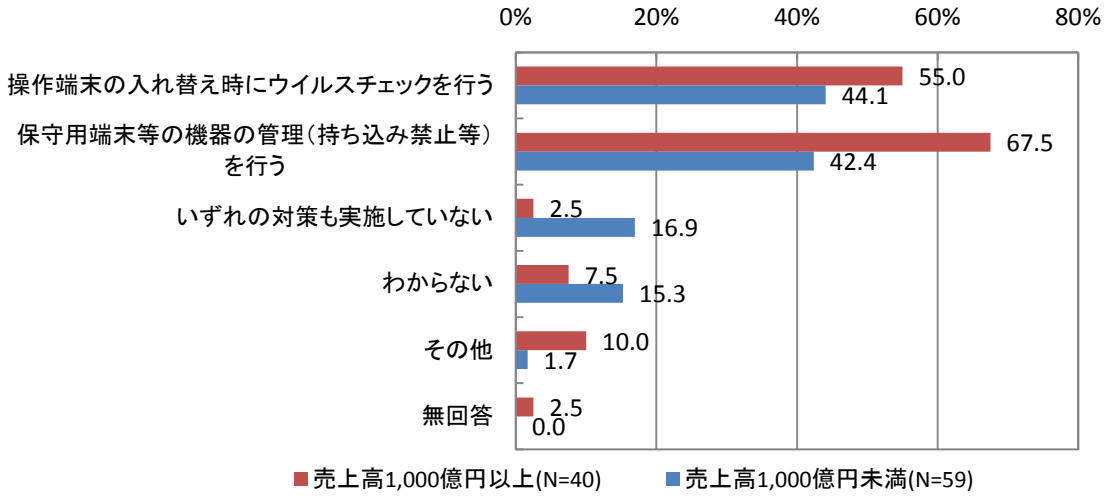


図 2-18 操作端末の入れ替え/保守用端末の管理（売上高別）

(3) リモートメンテナンス回線

リモートメンテナンス回線に対する対策としては、「利用時のみ接続させる」が 46.0%、「接続させる端末の認証を行う」が 39.0%となっている。

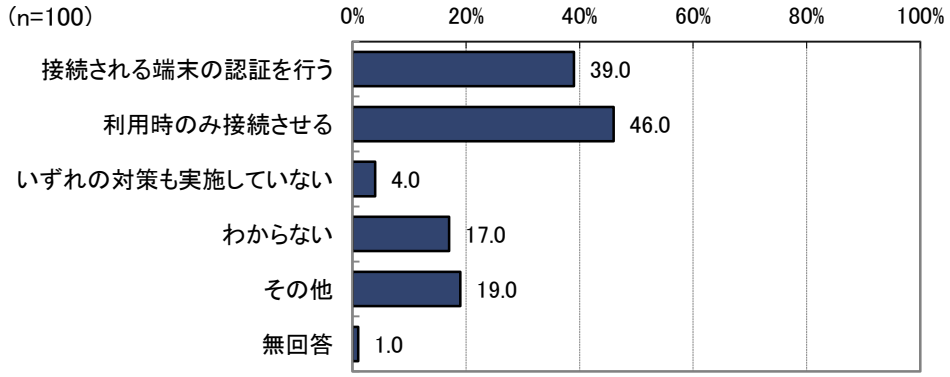


図 2-19 リモートメンテナンス回線

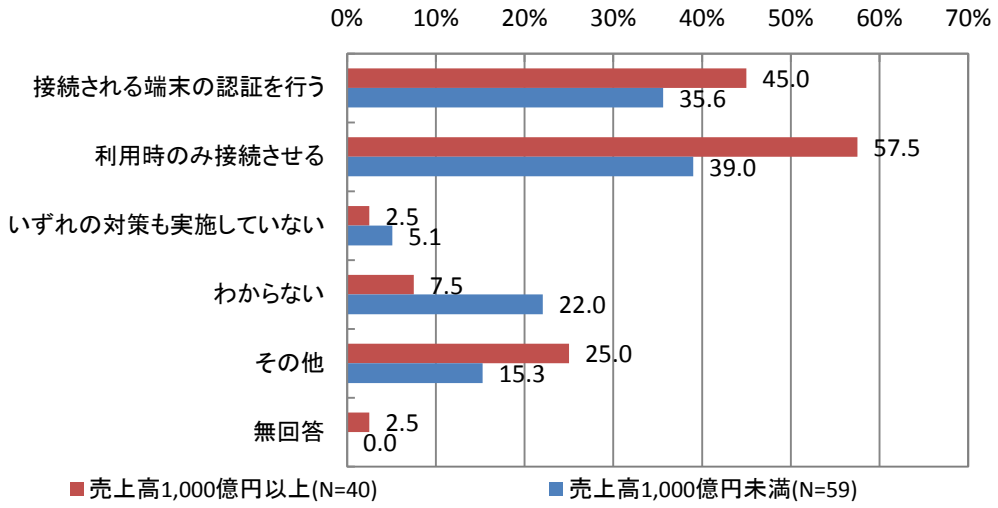


図 2-20 リモートメンテナンス回線（売上高別）

(4) 制御システム・ネットワークの監視

制御システムのネットワーク監視は、「いずれの対策も実施していない」が30.0%で、対策を実施していない企業の割合が高い。監視を行っている企業では、制御システムにもともと組み込まれているログ管理機能を利用している割合が高い。

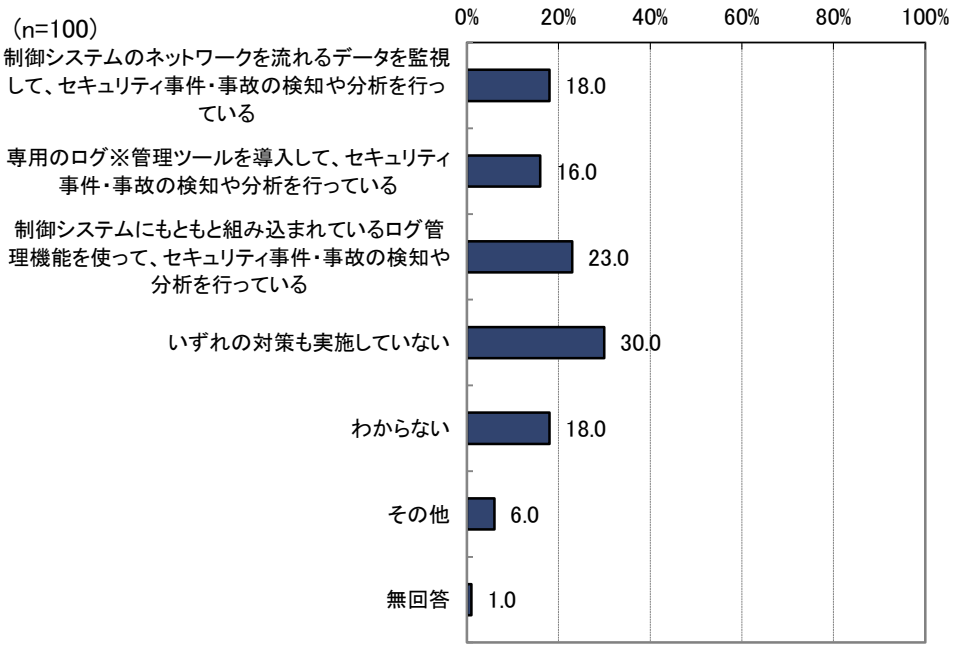


図 2-21 制御システム・ネットワークの監視

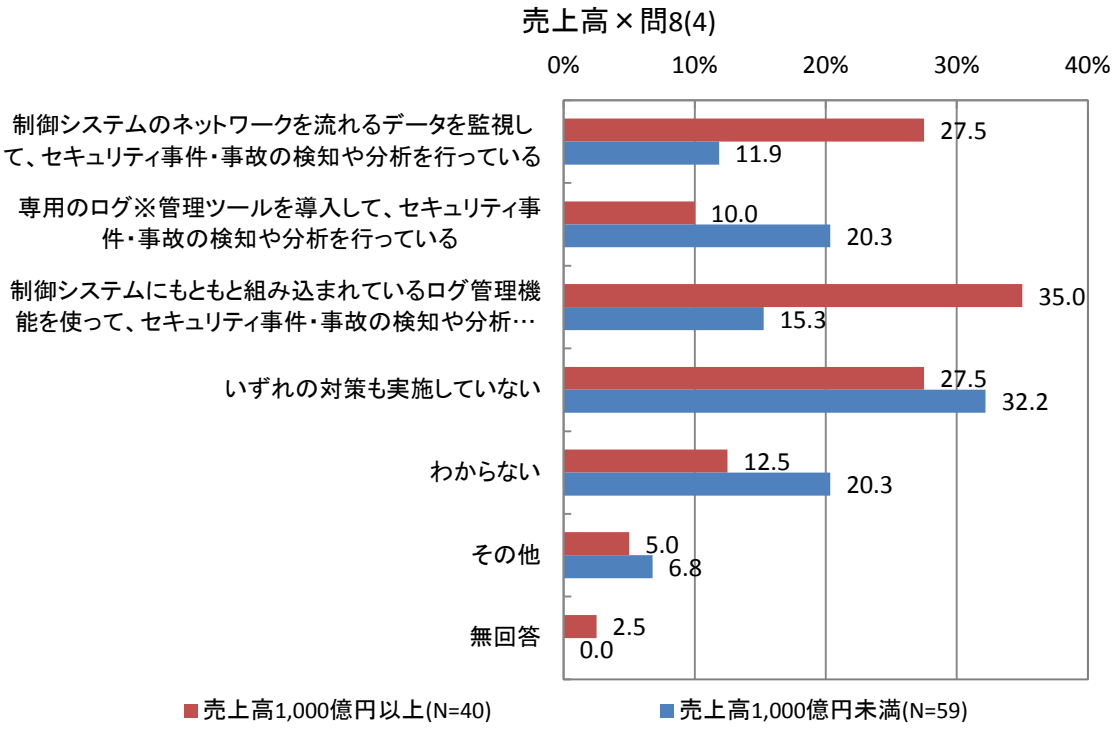


図 2-22 制御システム・ネットワークの監視（売上高別）

(5)制御系ネットワークへのタブレット・PC 等端末の接続

制御系ネットワークへのタブレット・PC 端末の接続対策は、「接続できる端末をシステムで制限している」が 50.0%で最も多い。

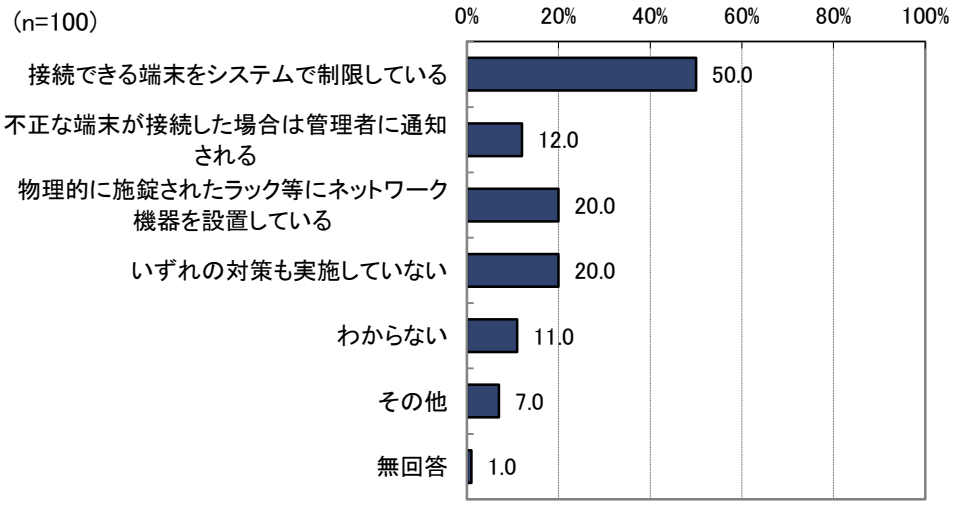


図 2-23 制御系ネットワークへのタブレット・PC 等端末の接続

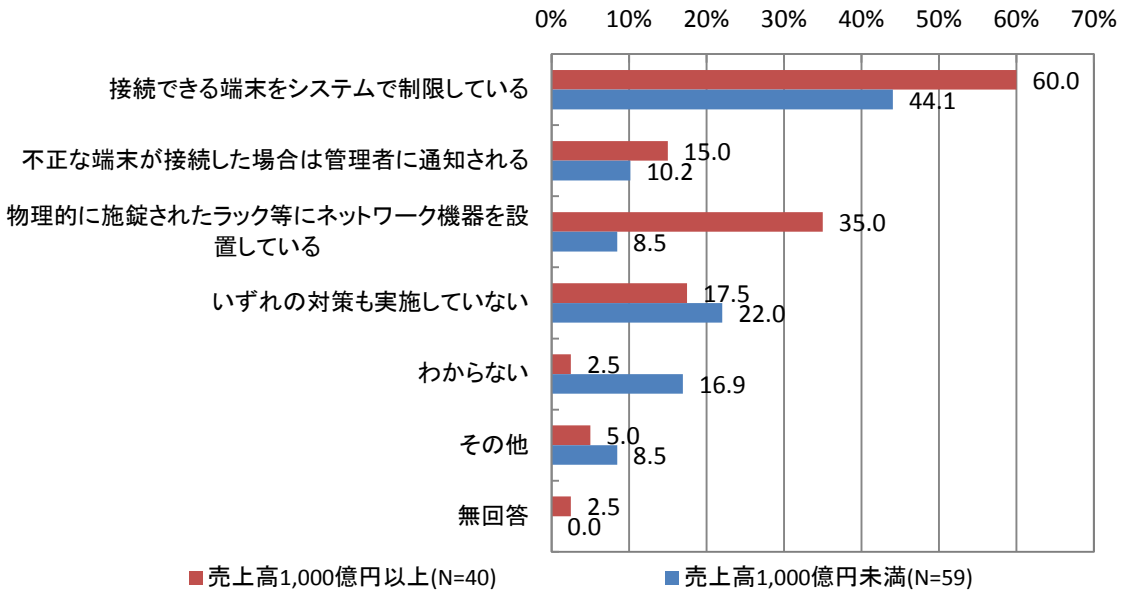


図 2-24 制御系ネットワークへのタブレット・PC 等端末の接続（売上高別）

(6)（1）から（5）のいずれかの対策を実施していない理由

対策を実施していない理由としては、「インターネットにつながっていないため、特に問題を感じていない」が最も多く、次に「人材が不足している」が挙げられている。

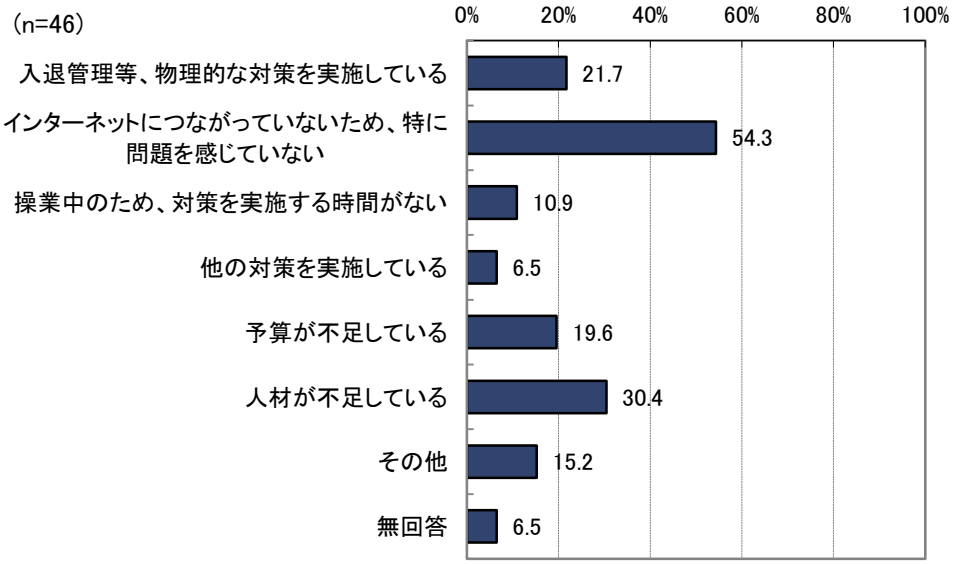


図 2-25 問 8 の対策を実施していない理由

2.2.9. 制御システムセキュリティに関する情報の入手先・入手経験

関係機関からの情報の入手先・入手経験は、IPA の割合が最も高く、JPCERT/CC、NISC の順となっている。

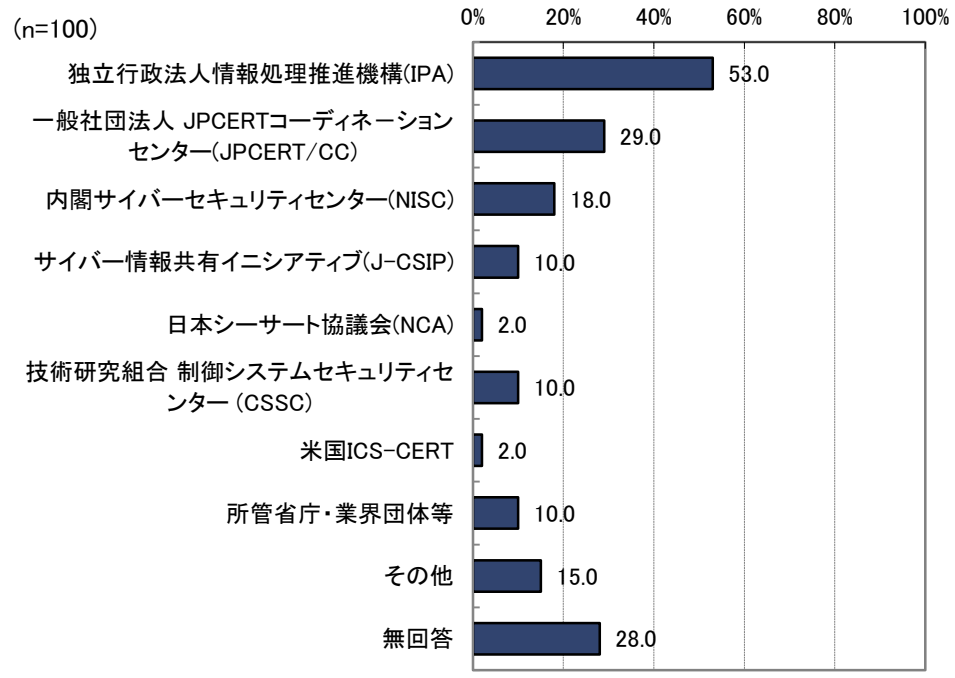


図 2-26 制御システムセキュリティに関する情報の入手先・入手経験

2.2.10. 制御システムに関する脆弱性情報の入手

(1)　制御システムに関する脆弱性情報の必要性

脆弱性情報の必要性を「感じており入手している」と回答した企業の割合は、44.0%である。一方で、「入手したいが方法がわからない」との回答が、24.0%となっており、脆弱性情報に対するニーズがあるが入手できていない企業が一定割合存在する。

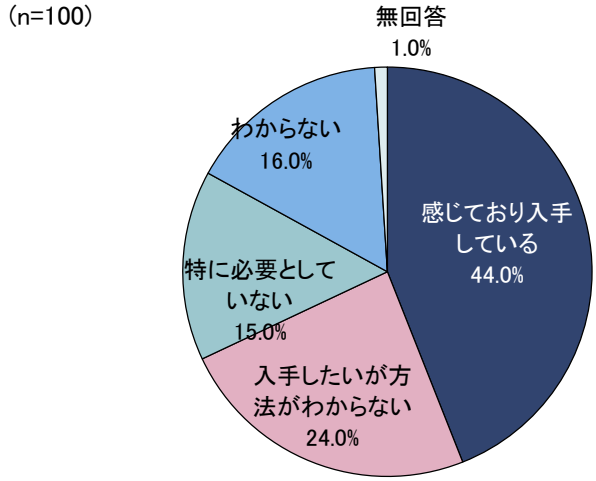


図 2-27 制御システムに関する脆弱性情報の必要性

(2)制御システムの脆弱性に関する情報の主な入手先

脆弱性情報の入手先は、IPA 等の「セキュリティ関係組織」が最も多く、次に「制御システムベンダ」となっている。

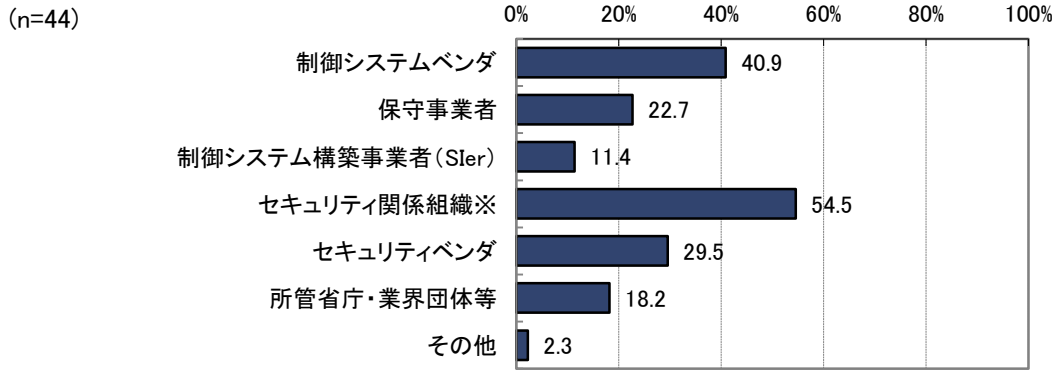


図 2-28 制御システムの脆弱性に関する情報の主な入手先

(3)制御システムの脆弱性情報を入手している部署

脆弱性情報の入手先は「情報システム部門」の割合が最も高く、次に「情報

システムのオーナー部門」となっている。

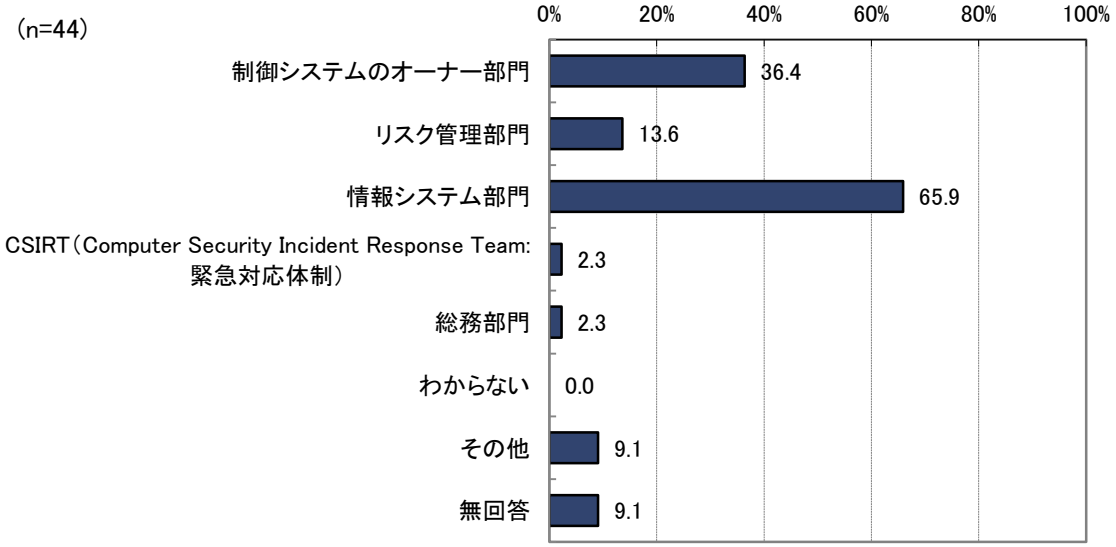


図 2-29 制御システムの脆弱性に関する情報を入手している部署

(4)制御システムの脆弱性情報を必要としていない理由

脆弱性情報を必要としない理由としては、「制御システムが攻撃される可能性は低いと思われるため」が 53.3%となっている。

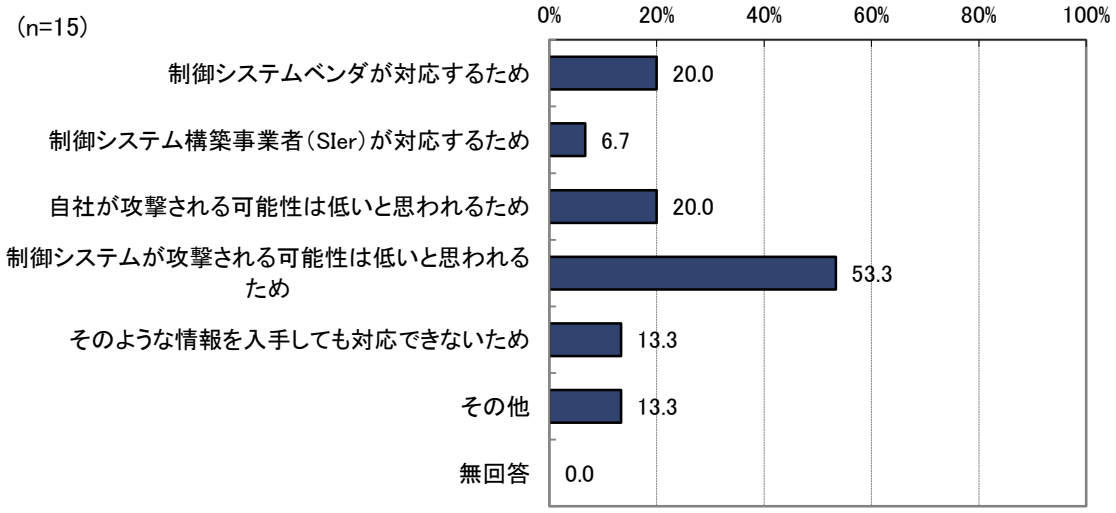


図 2-30 制御システムの脆弱性情報を必要としていない理由

2.2.11. 制御システムの脆弱性対策

(1)制御システムの脆弱性対策取組状況

「自社の保有するすべての制御システムの脆弱性対策に取組んでいる」と回

答した企業は 21.0%となっている。

一方で、「制御システムの脆弱性対策に取組んでいない」と回答した企業は 43.0%である。重要インフラ企業でも 26.9%は脆弱性対策に取組んでおらず、重要インフラ以外の業種ではその割合は 48.6%である。

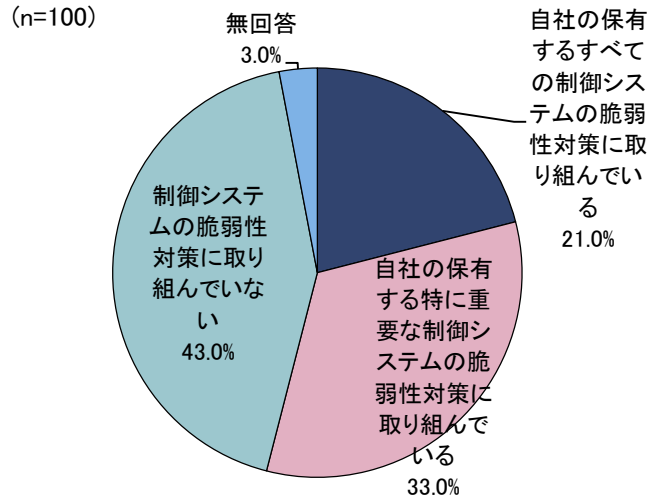


図 2-31 制御システムの脆弱性対策取組状況

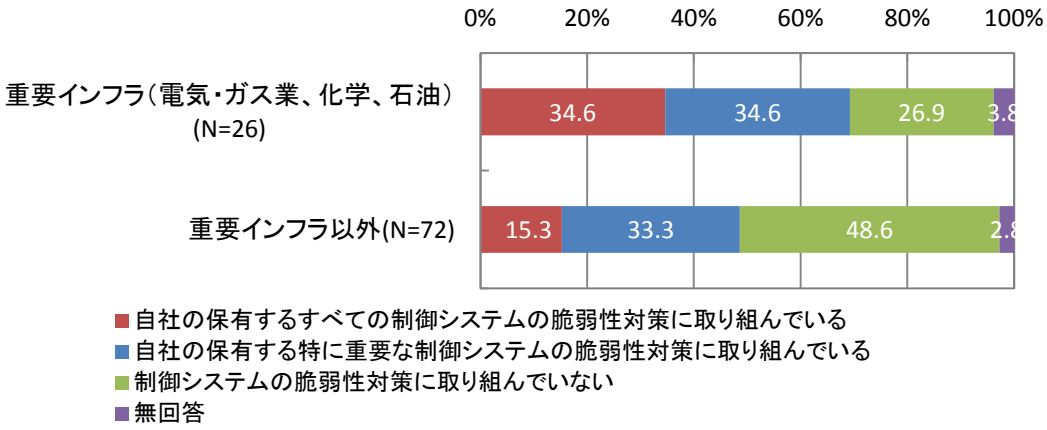


図 2-32 制御システムの脆弱性対策取組状況（重要インフラとその他業種）

(2) 制御システムにおいて脆弱性対策を始めたきっかけ

脆弱性対策を始めたきっかけは、「脆弱性が公表されていると聞いて」が一番多く、次に「新たにセキュリティポリシー等を策定し具体的な対策を合わせて実施する」が多い。

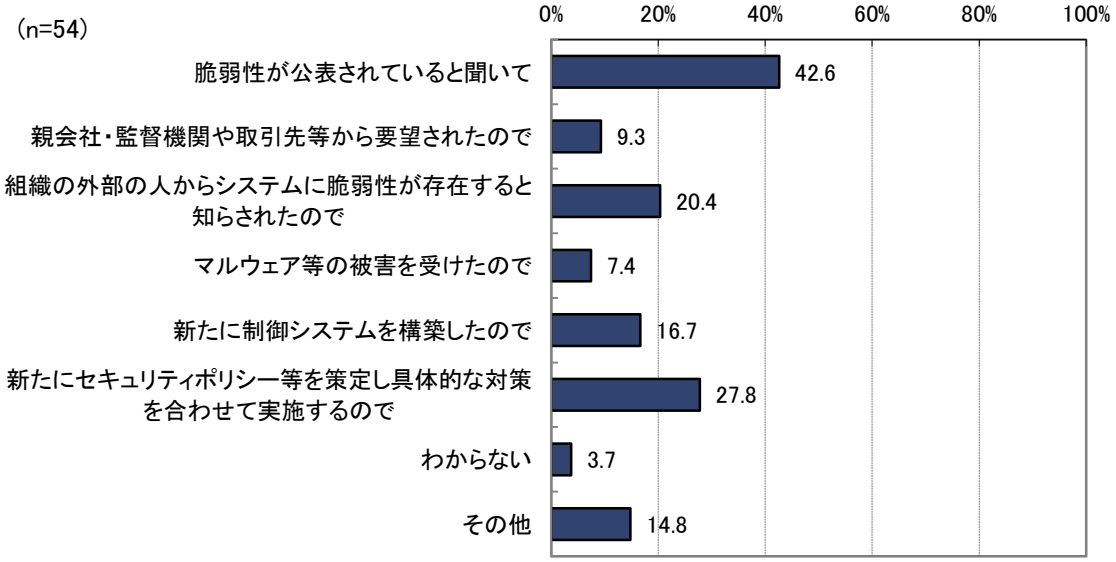


図 2-33 制御システムにおいて脆弱性対策を始めたきっかけ

(3) 制御システムの脆弱性対策の要否を判断し、指示を出す主な主体

脆弱性対策の要否の判断、指示を出す主体は「自社スタッフ」が大半を占め

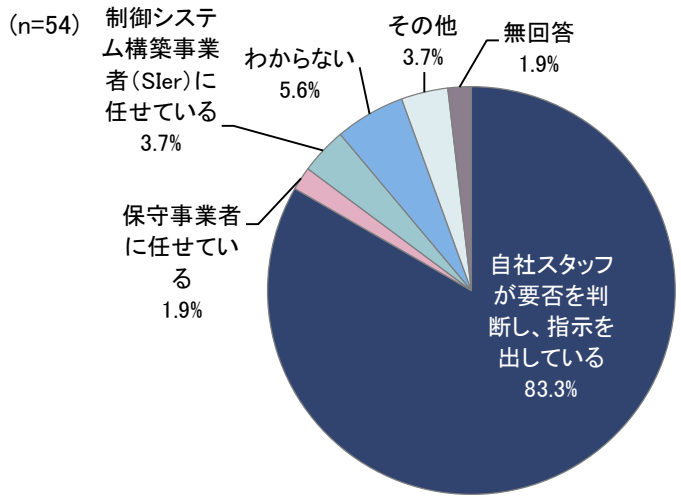


図 2-34 制御システムの脆弱性対策の要否を判断し、指示を出す主な主体

(4) 制御システムの脆弱性対策の要否の判断基準

脆弱性対策の要否を判断基準は、「予想される損失額」・「顧客の業務に影響するか」・「高機密を要する特殊な情報を扱っているか」の割合が高い。

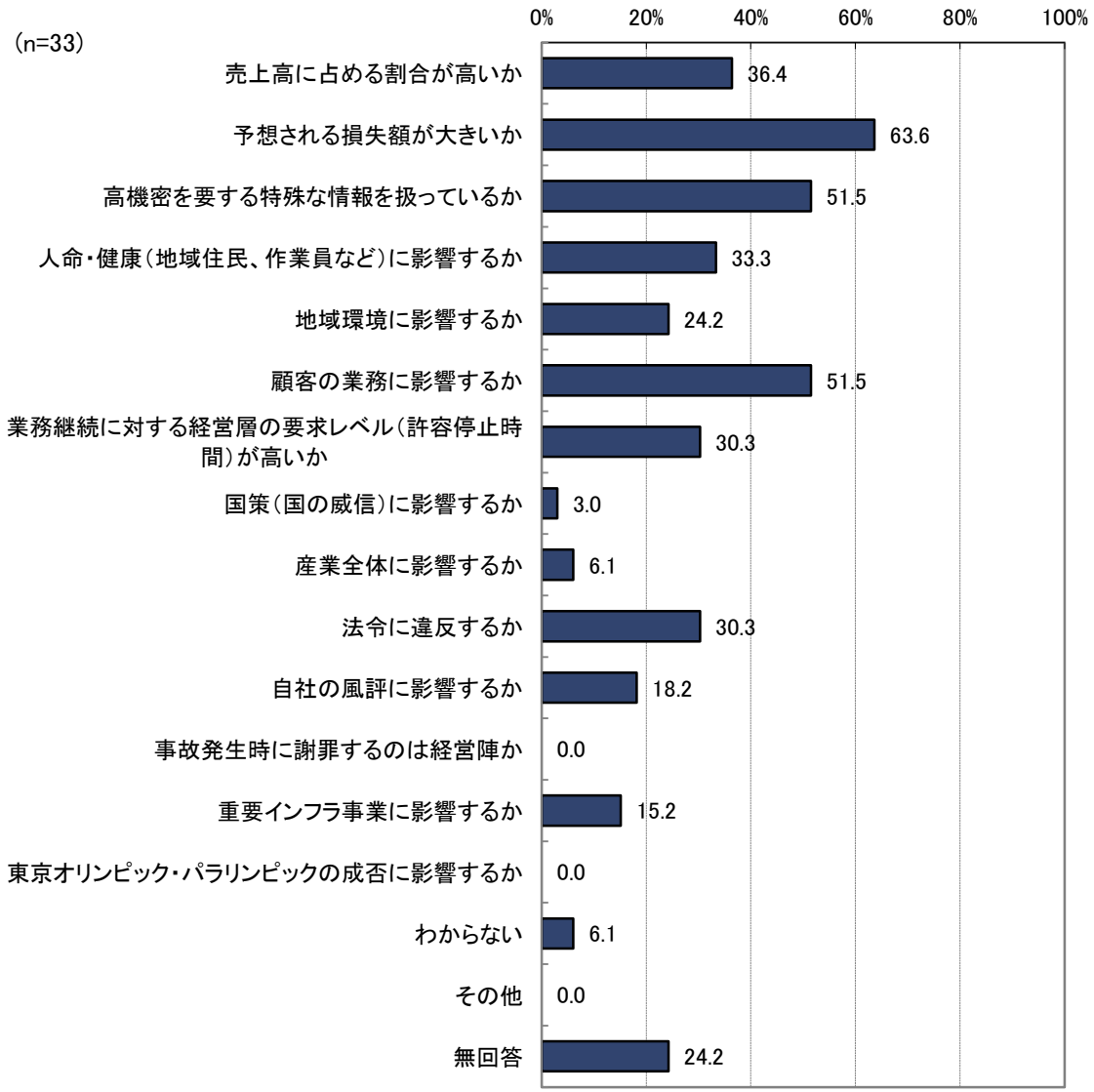


図 2-35 制御システムの脆弱性対策の要否の判断基準

(5) 制御システムの脆弱性対策を行わない主な理由

脆弱性対策を実施しない理由としては、「インターネットとの接続が無い」をあげる割合が高く、次に「同種の制御システムの被害事例が無い」が高い。

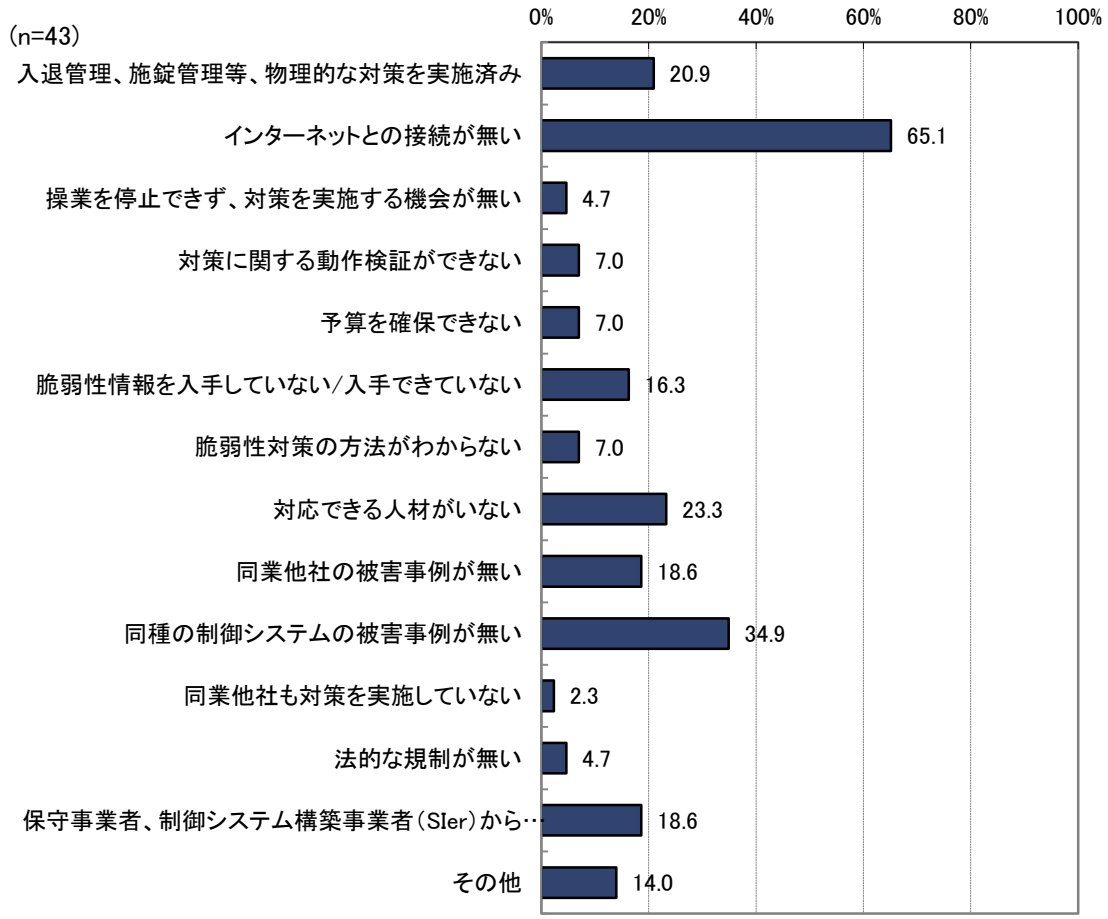


図 2-36 制御システムの脆弱性対策を行わない主な理由

2.2.12. 制御システムに深刻な脆弱性が見つかった場合の対応方針

深刻な脆弱性が見つかった場合の対応では、「セキュリティ更新プログラム（パッチ）をすみやかに適用する」が 32.0%、「メンテナンス時や操業停止時などに計画的にパッチを適用する」が 27.0%で、制御システムでもパッチを適用すると回答した企業は 59.0%となっている。

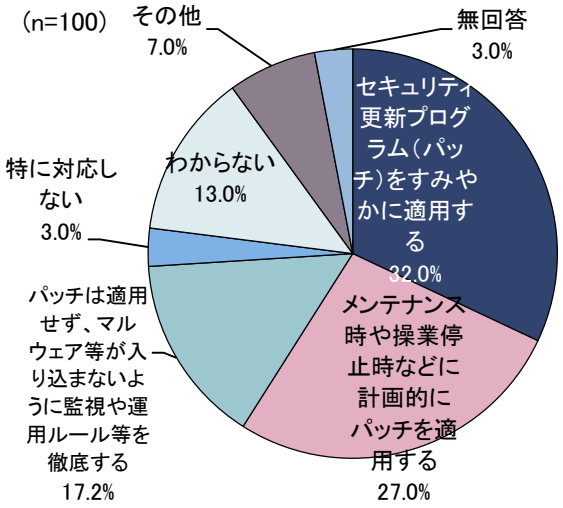


図 2-37 制御システムに深刻な脆弱性が見つかった場合の対応方針

2.2.13. 制御システムの脆弱性対策を進める上での課題

脆弱性対策を進める上での課題としては、「脆弱性対策にコストを要する」・「社内外の脆弱性対策の体制・人員の不整備」・「脆弱性対策を適用できない」をあげる回答割合が高い。

一方、「経営層の理解不足」・「制御システムオーナ部門の理解不足」・「脆弱性の情報がどこにあるかわからない」を課題にあげる回答の割合は低い。

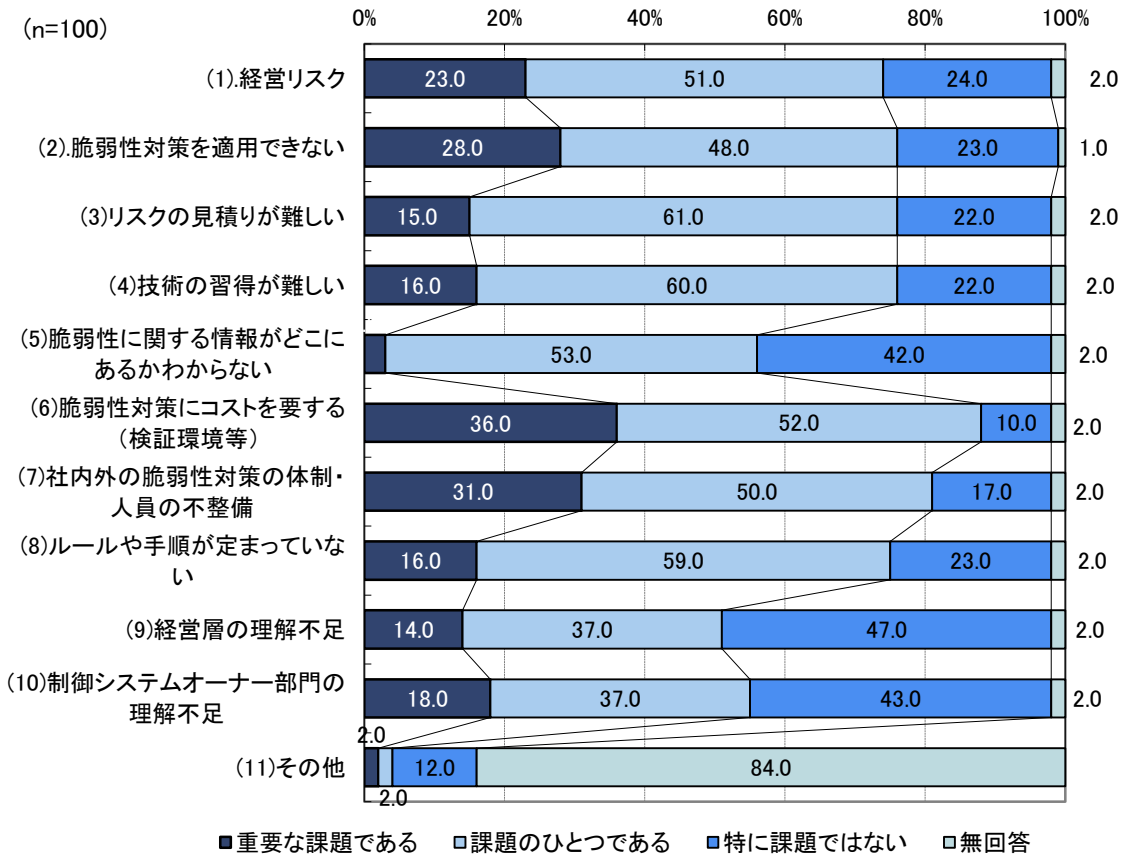


図 2-38 制御システムの脆弱性対策を進める上での課題

2.3. まとめ

アンケート調査結果から得られた知見は次のとおりである。

(1) 制御システムセキュリティに対する認識

制御システムのセキュリティリスクに関しては、多くの企業で認識しているが、実際の対策まで取組んでいる企業の割合は高くない。特に、重要インフラ以外の業種では認識しているが対応していない企業の割合が高い（図 2-2、図 2-32）。

また、制御システムのセキュリティリスクは認識されつつあるが、対策のために必要な予算や人員は十分確保されていない（図 2-8）。

(2) ガイド記載の対策項目の実施状況

「制御システム利用者のための脆弱性対応ガイド」に記載した、（1）USB メモリ（2）操作端末の入れ替え/保守用端末の管理（3）リモートメンテナンス回線

に関する対策項目に関しては、売上高 1,000 億円以上の企業では対策をとっている割合が高かった(図 2-16、 図 2-18、 図 2-20)。

売上高が 1,000 億円未満の企業では対策が未実施のところも多く、どのように対策を進めてもらうかが課題である。

また、対策を実施しない理由では「インターネットに接続していない」が挙げられている(図 2-25)。

(3)脆弱性情報の入手先

脆弱性情報の入手先としては、IPA 等のセキュリティ関係機関や制御システムベンダの割合が高かった(図 2-28)。また、脆弱性情報を入手している部門は情報システム部門、制御システムのオーナー部門の割合が高い(図 2-29)。

制御システムに関する脆弱性情報の展開や普及啓発を考えた場合、これらのルートを活用することが考えられる。

3. ヒアリング調査

3.1. 調査概要

アンケート回答者を対象にヒアリング調査を実施した。

ヒアリング調査では、アンケート調査の分析から得られた結果の妥当性の確認やセキュリティ対策の取組状況､「制御システム利用者のための脆弱性対応ガイド」に関する意見を伺った。

表 3-1 ヒアリング調査概要

調査対象	アンケート回答者
ヒアリング件数（予定）	5 件（PA3 件、FA2 件）
主な質問項目	・ 制御システムにおけるセキュリティ対策状況 ・ 脆弱性情報の収集・対応状況について ・ 「制御システム利用者のための脆弱性対応ガイド」について 等

3.2. 調査結果

ヒアリング調査でいただいた主なご意見について、項目別に整理したものを以下に示す。

(1)制御システムにおけるセキュリティ対策状況について

- 親会社を中心に制御系のセキュリティについて 2 年ほど前から検討している。グループとしてどのように取り組むかの方針は決まっており、グループのセキュリティレベルが一定の水準を満たすように取組んでいる。
- 制御系はOSのパッチを適用することによりラインが停止する可能性を考えると、恐怖感がありできない。仮に停止した場合、復旧までにどの程度の時間がかかるかがわからず、経営への影響も大きい。
- セキュリティへの投資は、現場への投資に比べると優先順位は低くなる。セキュリティ対策メンバーも潤沢にいるわけではない。
- グループで目指すセキュリティレベルの中には保守契約時の基準もある。
- 親会社が策定するガイドラインを満たさない企業は、グループ会社であっても取引の優劣のランクが低くなる。親会社は、グループ会社に対して厳格にセキュリティ対策を進めている。
- データベースのメンテナンスは関係会社に委託しているが、通常の保守は

自社で実施している。自社で対応できないものに関してはベンダに依頼している。高度な技術が使用されるようになり自社だけでは対応が難しいケースも増えているが、可能な限り自社で取り組むようにしている。

- 情報通信の担当役員は形式的にいるが、制御系を担当する役員はいない。制御系に関しては部門ごとに担当し、部長を中心に方針を決定している。
- SIer のリモート回線が一番の脅威だと感じている。ベンダの管理者権限の管理にユーザが参画する必要があるのではないか。リモート管理の状況を確認させてもらえないため、実態は不明である。
- サイバーセキュリティ基本法が制定され、化学分野は重要インフラとして認定されていることから、経営も重要性を理解している。
- 制御系は OA 系から独立しているとして安心していたが、検査したところ色々なネットワークと接続されていることがわかった。
- 制御システムにパッチをあてるのは定期修理など、プラントが停止しているときしか対応できない。社員が最終的にスケジュールを含め判断せざるをえない。
- 教育資料や報道から、制御システムセキュリティの認識を持っている部署もある。他工場でのヒヤリハットの情報は共有されるので管理者レベルは危機感を持つが、担当者レベルの意識向上に繋がりにくい。
- セキュリティ関連予算や人員は、全体として十分ではない。組織的に会社として取り組む必要があるが、どのような体制とすべきか検討段階である。制御系は設備の中に入るため目に見えない。OA 系と同等には考えてもらえず、「機械」と捉えられている。
- 大型装置は金額も大きいため、セキュリティ関連予算規模は全体の一部になり、詳細が見えない。装置では様々なテストは行うが、セキュリティの項目は欠けている。
- FA-LAN 構築基準を現在作成している。DMZ がきれいに分かれていない場合や、DMZ がないケースもある。すべてを網羅するのは難しいが、いくつかケースを分けて指針を示す予定である。
- 以前は、情報システムグループが把握していないシステム導入があった。システム投資案件に関しては、各工場のシステム担当者が入るようにし、事前相談を必ず実施するよう依頼している。
- 制御システムの管理は工場ごとであるが、セキュリティに対する認識は低い。しかし、インターネットに接続してはダメという認識は浸透しつつある。

(2)脆弱性情報の収集・対応状況について

- IPA 等様々なところから収集しているが､一番情報提供のパイプとして太いのは親会社である。
- IT 推進グループでは全社に対して情報を発信し、対応の有無は各事業部が判断している。重要なものに関してはフィードバックしている。
- 自社のシステム構成はベンダのほうが詳しい。脆弱性対応等はベンダの SE に依頼している。IT 推進グループで指示することもあるが、多くのケースでは SE が既に対応している。
- 脆弱性情報について担当者を決めて収集はしていない。必要性はあるかもしれないが、時間や人の確保等現実的には難しい。
- 脆弱性情報が多数提供されるため作業負荷はかかるが、何があるかわからないため内容は確認するようにしている。
- 重要な脆弱性情報は業界団体から提供される。制御系の情報に関しては部門横断的な取り組みをしており、該当する部門で情報を共有している。
- 脆弱性情報は､制御システムベンダの情報を SIer が取りまとめてから自社に提供される。システム構成を一番理解しているのは SIer である。
- 有名な脆弱性は各部門に注意喚起しているが、この装置のこの脆弱性といったやり取りはしていない。

(3)「制御システム利用者のための脆弱性対応ガイド」について

- 経営者層に伝えるにはまだメッセージが弱いのではないか。
- ガイドは当たり前の内容を記載しているが、大げさに書かれている印象を受ける。リスク評価やセキュリティ対策という記載では、大変な取組と捉えられる可能性がある。
- FW や IDS・IPS で何ができるかを十分に理解していない可能性がある。FW や IDS を設置すれば安全だと考えている人がいるのではないか。
- 最大のリスクは人である。現在のガイドはモノの対策が中心である。人の対策に関する内容があったほうがよい。
- 現場にガイドを回覧してもほとんど読まない可能性がある。現場に周知するためには、エッセンスを抽出して研修等で伝えるとよいのではないか。
- 経営トップは忙しいため、開いて読んでもらうにはハードルが高い。
- 製造所長／工場長は読者として狙い目ではないか。安全について現場で守るというモチベーションを持っている。
- 制御系のシステムは分かりにくい。体系的に理解したうえで制御システムの具体的なシステムとそのどの部分に脆弱性があり、という情報までおち

るとはっとするのではないか。
- 生産部門の上の人に読ませるには、Industry4.0 や IoT といったキャッチーなキーワードを入れて関心を持ってもらうとよい。競争環境のなかの一部といわれると響くのではないか。
- 内容は理解できると思うが、自社にとって何が危険であるかがピンとこないのではないか。
- 研修の中に制御セキュリティを入れるのは難しい。ネットワークの知識等が必要であり、工場のシステム担当者に教えるのが限界である。
- ワークシートがあるとよい。自社に置き換えて考えることができるのではないか。システムの棚卸を実施し、どこにリスクがあるかを考えてもらうことができる。

3.3. まとめ

(1)制御システムにおけるセキュリティ対策状況について

グループや部門横断的に制御システムのセキュリティ対策に取り組み始めたという意見があった。グループで目標とするセキュリティレベルを定め、それを満たさない場合、グループ会社であっても取引の優劣のランクが低くなるといった、厳格な運用がなされているところもある。

また、自社で可能な限り保守を行っている企業では、新たな技術に今後どのようにキャッチアップするかが課題との意見があった。

SIer リモートメンテナンスの状況に関しては、事業者で状況を確認することができず、脅威になりうるとの意見もあった。

(2) 脆弱性情報の収集・対応状況について

今回ヒアリングした企業はいずれも積極的に脆弱性情報を収集していた。様々な機関から情報が提供されているが、その数が多く自社にとってどれが重要かを判断するのに苦労しているとの意見があった。

また、自社のシステム構成に関しては SIer が一番理解しているとの意見もあり、脆弱性情報の対応判断には SIer が重要な役割を担っている。

(3)「制御システム利用者のための脆弱性対応ガイド」について

現在のガイドに対しては、経営層へのメッセージが不十分や当然の内容を大げさに書いている印象を受け、セキュリティ対策が大変な取組みと捉えられる可能性があるとの意見をいただいた。また、人的側面の視点が抜けているとの指摘もあった。

ガイドを活用した普及啓発方策としては、従業員向けの研修でガイドからエッセンスを抽出して利用するとよいのではないかとの意見があった。

参考資料 1　制御システムユーザ企業におけるセキュリティリスクの実態調査 調査票

Ⅰ. 制御システムセキュリティの状況

制御システムとは、プラントにおけるプロセスの監視・制御、および機械・食品等の工場の生産・加工ラインなどで、多くの企業に利用されているシステムです。

制御システムにトラブルが生じると、生産ラインの停止や設備損壊、環境汚染等を引き起こし、企業に甚大な損失を与える可能性があります。そうしたトラブルの大半はシステムの不具合や障害が原因でしたが、今後はサイバー攻撃や悪意のあるソフトウェア（マルウェア）がトラブルを引き起こすリスク（**セキュリティリスク**）が懸念されています。

そこで、こうした問題を防ぐ対策として、**制御システムセキュリティ**の取組みが重要となります。

問1　貴社の制御システムのセキュリティリスクに関するご認識について、お答えください。（1 つだけ選択）

1. 認識して対策済み
2. 認識して対応中
3. 認識しているが未対応
4. 認識していない
5. わからない

問2　貴社では、過去 5 年のうちに経験した制御システムのトラブルのうち、セキュリティ上の事件・事故※1 やヒヤリハット※2 であったことが判明したケースがありますか。（1 つだけ選択）

※1 セキュリティ上の事件・事故：本調査では、制御システムの不具合や障害ではなく、サイバー攻撃や悪意のあるソフトウェアが原因で発生した、制御システムの停止や暴走、情報の漏えいや消失等の事件・事故とする

※2 ヒヤリハット：事件・事故には至らなかったが、場合によっては事件・事故に直結したかもしれない問題

1. 事件・事故の経験あり
2. 事件・事故はないがヒヤリハットの経験あり
3. 経験がない
4. わからない

問 2-S1［問 2 で 1 または 2 を回答した方にお尋ねします］

セキュリティ上の事件・事故やヒヤリハットにはどのようにして気づきましたか。（複数選択可）

1. 現場のオペレータが異常に気付き、分析して判明した
2. 制御情報ネットワーク管理者が異常に気付き、分析して判明した
3. ウイルス対策ソフトで検出した
4. 社内 LAN 管理者が異常に気付き、分析して判明した
5. SOC（Security Operation Center）で検出した
6. 社外の関係者や取引先等から連絡を受けた
7. セキュリティ関連組織等から連絡を受けた
8. わからない
9. その他（具体的に：　　）

問 2-S2［問 2 で 1 または 2 を回答した方にお尋ねします］

セキュリティ上の事件・事故やヒヤリハットを受けて、どのように対応しましたか。（複数選択可）

1. 自社で端末等を入れ替え、復旧した
2. 制御システムベンダ等が端末等を入れ替え、復旧した
3. 自社でサイバー攻撃の対策を実施し、復旧した
4. 制御システムベンダ等がセキュリティの対策を実施し、復旧した
5. セキュリティベンダがセキュリティの対策を実施し、復旧した
6. わからない
7. その他（具体的に：　　）

問 2-S3［問 2 で 1 を回答した方にお尋ねします］

セキュリティ上の事件・事故を受けた影響によって貴社の制御システムが停止した期間（複数ある場合はそのうち最長の期間）はどのくらいですか。（1 つだけ選択）

1. 停止していない
2. 4 時間未満
3. 4～8 時間未満
4. 8～12 時間未満
5. 12～24 時間未満
6. 24 時間～3 日未満
7. 3～6 日未満
8. 6 日以上
9. わからない

問3　制御システムのセキュリティ対策に必要な予算や人員はどの程度まで確保されていますか。（1 つだけ選択）

1. 十分に確保できている
2. おおむね確保できている
3. やや不足している
4. 全く足りていない
5. 特に確保していない
6. わからない
7. その他（具体的に：　　）

問4 制御システムのセキュリティの現状を把握し、対策を推進する担当組織（または担当者）が設置されていますか。（1 つだけ選択）

1. 担当組織（または担当者）が設置されている
2. 担当組織（または担当者）ではないが、事実上対応している
3. 担当組織（または担当者）はない
4. わからない
5. その他（具体的に：　　）

問5　現在の制御システムのセキュリティ対策状況について把握していますか。（1 つだけ選択）

1. 十分に把握できている
2. ある程度把握できている
3. あまり把握できていない
4. 全く把握できていない
5. わからない
6. その他（具体的に：　　）

問6 制御システムの調達にあたって、要求仕様にセキュリティ要件が含まれていますか。（1 つだけ選択）

1. 通常、セキュリティ要件が含まれている
2. セキュリティ要件が含まれることもある
3. 通常、セキュリティ要件は含まれていない
4. わからない

5. その他（具体的に：　　）

問7　制御システムの保守業務を外部（子会社を含む）に委託していますか。（1つだけ選択）

1. 基本的に自組織で保守している
2. 基本的に外部事業者に委託している
3. 自社で保守しているものと外部事業者に委託しているものが混在している
4. その他（具体的に：　　）

問 7-S1［問 7 で 2～4 を回答した方にお尋ねします］
制御システムの保守契約に、セキュリティに関する項目が含まれていますか。（1 つだけ選択）

1. 通常、セキュリティ項目が含まれている
2. セキュリティ項目が含まれることもある
3. 通常、セキュリティ要件は含まれていない
4. わからない
5. その他（具体的に：　　）

問8 制御システムに対する脅威を抑制する対策として、以下のものを実施していますか。

(1) USB メモリ（複数選択可）

1. USB ポートを取り外す/ロックする
2. USB メモリ挿入時に、専用 PC でウイルスチェックを行う
3. USB メモリ利用規則を策定する
4. 利用できる USB メモリを特定し管理する
7. いずれの対策も実施していない
8. わからない
9. その他（具体的に：　　）

(2) 操作端末の入れ替え/保守用端末の管理（複数選択可）

1. 操作端末の入れ替え時にウイルスチェックを行う
2. 保守用端末等の機器の管理（持ち込み禁止等）を行う
7. いずれの対策も実施していない
8. わからない

9. その他（具体的に：　　）

(3) リモートメンテナンス回線（複数選択可）

1. 接続される端末の認証を行う
2. 利用時のみ接続させる

7. いずれの対策も実施していない

8. わからない
9. その他（具体的に：　　）

(4) 制御システム・ネットワークの監視（複数選択可）

1. 制御システムのネットワークを流れるデータを監視して、セキュリティ事件・事故の検知や分析を行っている
2. 専用のログ※管理ツールを導入して、セキュリティ事件・事故の検知や分析を行っている
3. 制御システムにもともと組み込まれているログ管理機能を使って、セキュリティ事件・事故の検知や分析を行っている

7. いずれの対策も実施していない

8. わからない
9. その他（具体的に：　　）

※ 制御システムのログ：オペレータの操作記録、ネットワーク装置の記録、制御システム内の OS のイベントログを含むデータ

(5) 制御系ネットワーク※へのタブレット、PC 等端末の接続（複数選択可）

1. 接続できる端末をシステムで制限している
2. 不正な端末が接続した場合は管理者に通知される
3. 物理的に施錠されたラック等にネットワーク機器を設置している

7. いずれの対策も実施していない

8. わからない
9. その他（具体的に：　　）

※ 制御系ネットワーク： 図 39 における『小規模な制御システム』では図中のいずれかの個所、および『大規模な制御システム』では図中の「制御システム(DCS)」内を想定します。

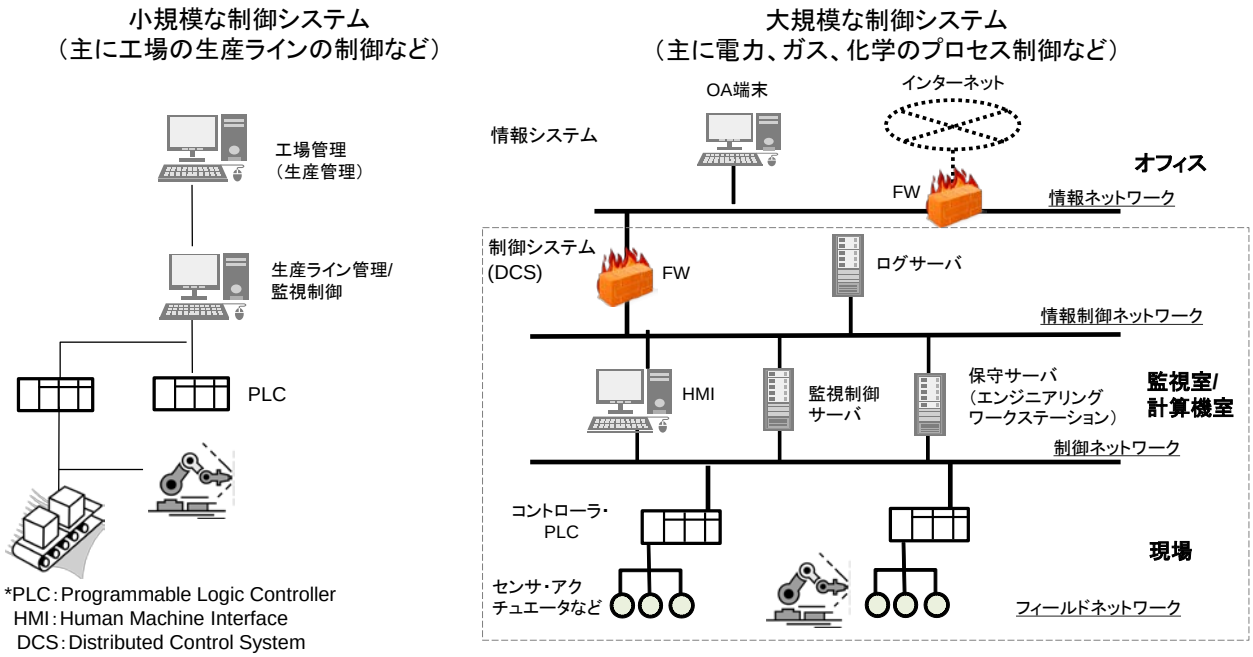


図 39 制御システムの構成（「制御システム利用者のための脆弱性対応ガイド」 3.1. 制御システムの構成より抜粋）

問 8-S1 ［問 8］ (1) (2) (3) (4) (5)のいずれか一つ以上で 7. を回答した方にお尋ねします］

問 8 の対策を実施していない理由は何ですか。（複数選択可）

1. 入退管理等、物理的な対策を実施している
2. インターネットにつながっていないため、特に問題を感じていない
3. 操業中のため、対策を実施する時間がない
4. 他の対策を実施している（具体的に：　　）
5. 予算が不足している
6. 人材が不足している
7. その他（具体的に：　　）

問9 制御システムのセキュリティに関する情報を以下のいずれかの組織から入手したことがありますか。（複数選択可）

1. 独立行政法人情報処理推進機構(IPA)
2. 一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)
3. 内閣サイバーセキュリティセンター(NISC)
4. サイバー情報共有イニシアティブ(J-CSIP)
5. 日本シーサート協議会(NCA)
7. 米国 ICS-CERT
8. 所管省庁・業界団体等
（具体的に：　　）
9. その他
（具体的に：　　）

6. 技術研究組合 制御システムセキュリティセンター（CSSC）

Ⅱ. 制御システムの脆弱性（ぜいじゃくせい）※対応

※脆弱性：セキュリティ上の弱点。同封の「制御システム利用者のための脆弱性対応ガイド」18-19 頁をご参照ください。

問10　制御システムの脆弱性に関する情報について、必要性を感じていますか。（1 つだけ選択）

1. 感じており入手している
2. 入手したいが方法がわからない
3. 特に必要としていない
4. わからない

問 10-S1　[問 10 で 1 を回答した方にお尋ねします]
制御システムの脆弱性に関する情報を主にどこから入手していますか。（複数選択可）

1. 制御システムベンダ
2. 保守事業者
3. 制御システム構築事業者（SIer）
4. セキュリティ関係組織※
5. セキュリティベンダ
6. 所管省庁・業界団体等
7. その他（具体的に：　　）

※セキュリティ関連組織の例：
- 独立行政法人情報処理推進機構(IPA)　・サイバー情報共有イニシアティブ(J-CSIP)
- 一般社団法人 JPCERT コーディネーションセンター(JPCERT/CC)　・米国 ICS-CERT
- 内閣サイバーセキュリティセンター(NISC)　・日本シーサート協議会(NCA)
- 技術研究組合 制御システムセキュリティセンター（CSSC）

問 10-S2 [問 10 で 1 を回答した方にお尋ねします]
貴社において制御システムの脆弱性に関する情報を入手しているのはどちらの部署ですか。（複数選択可）

1. 制御システムのオーナー部門
2. リスク管理部門
3. 情報システム部門
4. CSIRT（Computer Security Incident Response Team: 緊急対応体制）

5. 総務部門
6. わからない
7. その他（具体的に：　　）

問 10-S3［問 10 で 3 を回答した方にお尋ねします］
特に必要としていない理由は何ですか。（複数選択可）

1. 制御システムベンダが対応するため
2. 制御システム構築事業者（SIer）が対応するため
3. 自社が攻撃される可能性は低いと思われるため
4. 制御システムが攻撃される可能性は低いと思われるため
5. そのような情報を入手しても対応できないため
6. その他（具体的に：　　）

問11　貴社では制御システムの脆弱性対策に取り組んでいますか。(1 つだけ選択)

1. 自社の保有するすべての制御システムの脆弱性対策に取り組んでいる
2. 自社の保有する特に重要な制御システムの脆弱性対策に取り組んでいる
3. 制御システムの脆弱性対策に取り組んでいない

問 11-S1［問 11 で 1,2 を回答した方にお尋ねします］
貴社の制御システムにおいて脆弱性対策を始めたきっかけはどのようなものですか。あてはまるものをすべてお答えください。（複数選択可）

1. 脆弱性が公表されていると聞いて
2. 親会社・監督機関や取引先等から要望されたので
3. 組織の外部の人からシステムに脆弱性が存在すると知らされたので
4. マルウェア等の被害を受けたので
5. 新たに制御システムを構築したので
6. 新たにセキュリティポリシー等を策定し具体的な対策を合わせて実施するので
7. わからない
8. その他（具体的に：　　）

問 11-S2［問 11 で 1,2 を回答した方にお尋ねします］
貴社において、制御システムの脆弱性対策の要否を判断し、指示を出すのは主に誰ですか。（1 つだけ選択）

1. 自社スタッフが要否を判断し、指示を出している
2. 保守事業者に任せている
3. 制御システム構築事業者（SIer）に任せている

4. わからない
5. その他（具体的に：　　）

問 11-S3 [問 11 で 2 を回答した方にお尋ねします]
貴社における制御システムの脆弱性対策の要否を判断する基準は何ですか。（複数選択可）

1. 売上高に占める割合が高いか
2. 予想される損失額が大きいか
3. 高機密を要する特殊な情報を扱っているか
4. 人命・健康（地域住民、作業員など）に影響するか
5. 地域環境に影響するか
6. 顧客の業務に影響するか
7. 業務継続に対する経営層の要求レベル（許容停止時間）が高いか
8. 国策（国の威信）に影響するか
9. 産業全体に影響するか
10. 法令に違反するか
11. 自社の風評に影響するか
12. 事故発生時に謝罪するのは経営陣か
13. 重要インフラ事業に影響するか
14. 東京オリンピック・パラリンピックの成否に影響するか
15. わからない
16. その他（具体的に：　　）

問 11-S4 [問 11 で 3 を回答した方にお尋ねします]
貴社における制御システムの脆弱性対策を行わない主な理由は何ですか。（複数選択可）

1. 入退管理、施錠管理等、物理的な対策を実施済み
2. インターネットとの接続が無い
3. 操業を停止できず、対策を実施する機会が無い
4. 対策に関する動作検証ができない
5. 予算を確保できない
6. 脆弱性情報を入手していない/入手できていない
7. 脆弱性対策の方法がわからない
8. 対応できる人材がいない
9. 同業他社の被害事例が無い
10. 同種の制御システムの被害事例が無い
11. 同業他社も対策を実施していない
12. 法的な規制が無い
13. 保守事業者、制御システム構築事業者（SIer）からの提案が無い
14. その他
（具体的に：　　）

問12　貴社の制御システムに深刻な脆弱性が見つかった場合、通常どのように対応しますか。（1 つだけ選択）

1. セキュリティ更新プログラム（パッチ）をすみやかに適用する
2. メンテナンス時や操業停止時などに計画的にパッチを適用する
3. パッチは適用せず､マルウェア等が入り込まないように監視や運用ルール等を徹底する
4. 特に対応しない
5. わからない

6. その他（具体的に：　　）

問13　貴社の制御システムの脆弱性対策を進める上での課題について、あてはまるものを選択してください。

（それぞれ１つ選択）		重要な課題である	課題のひとつである	特に課題ではない
(1)	経営リスクとしてとらえていない	1.	2.	3.
(2)	システムに不具合が生じる恐れがあるため脆弱性対策を適用できない	1.	2.	3.
(3)	脆弱性を修正しないと判断した場合のリスクの見積りが難しい	1.	2.	3.
(4)	脆弱性に関する技術の習得が難しい	1.	2.	3.
(5)	脆弱性に関する情報がどこにあるかわからない	1.	2.	3.
(6)	脆弱性対策にコストを要する（検証環境等）	1.	2.	3.
(7)	社内外に脆弱性対策の体制・人員が整っていない	1.	2.	3.
(8)	脆弱性対策に関するルールや手順が定まっていない	1.	2.	3.
(9)	脆弱性対策について経営層の理解が乏しい	1.	2.	3.
(10)	脆弱性対策について制御システムのオーナー部門の理解が乏しい	1.	2.	3.
(11)	その他（具体的に：　　）	1.	2.	3.

Ⅲ. 貴社及び回答者情報

問14　貴社の主な業種をお答えください。（1 つだけ選択）

1. 食品　2. 化学　3. 医薬品　4. 石油・石炭製品
5. ゴム製品　6. ガラス・土石製品　7. 鉄鋼　8. 非鉄金属
9. 金属製品　10. 電気・ガス　11. 機械　12. 電気機器
13. 輸送用機器　14. 精密機器　15. その他（　　）

問15　貴社の直近年度の総売上高（単体）をお答えください。（1 つだけ選択）

1. 5,000 万円未満　2. 5,000 万円～1 億円未満　3. 1 億円～5 億円未満
4. 5 億円～10 億円未満　5. 10 億円～100 億円未満　6. 100 億円～1,000 億円未満
7. 1,000 億円～1 兆円未満 8. 1 兆円以上

問16　貴社の事業所数をお答えください。（1 つだけ選択）

1. 1 箇所のみ　2. 2 箇所～10 箇所　3. 11 箇所～50 箇所
4. 51 箇所～100 箇所　5. 101 箇所以上

問17　貴社の総従業員数※（単体）をお答えください。（1 つだけ選択）

※ 総従業員数：有給役員、正社員・正職員、準社員・準職員、アルバイト等を含む

1. 9 人以下　2. 10～49 人　3. 50～99 人　4. 100～499 人
5. 500 人～999 人6. 1,000 人～4,999 人 7. 5,000 人～9,999 人 8. 10,000 人以上

問18　あなたのお立場をお答えください。（複数選択可）

1. 経営企画、リスク管理部門等のリスク管理ご担当の方
2. 現場部門の制御システムの導入及び調達ご担当の方
3. 制御システムの運用・管理に携わる管理者の方
4. 情報通信システム部門の IT セキュリティご担当の方
5. その他（具体的に：　　）

問19　あなたは、ソフトウェア等の脆弱性関連情報の届出や調整、公表を行う「情報セキュリティ早期警戒パートナーシップ」の枠組みや活動について御存知ですか。（それぞれ 1 つだけ選択）

		1. 名前も概要も知っている	2. 名前は知っているが、概要は知らない	3. 知らない
(1)	情報セキュリティ早期警戒パートナーシップ	1	2	3
(2)	独立行政法人情報処理推進機構（IPA）	1	2	3
(3)	一般社団法人 JPCERT コーディネーションセンター（JPCERT/CC）	1	2	3

問20　本調査に関連して、インタビュー調査にご協力いただくことは可能ですか。（1 つだけ選択）

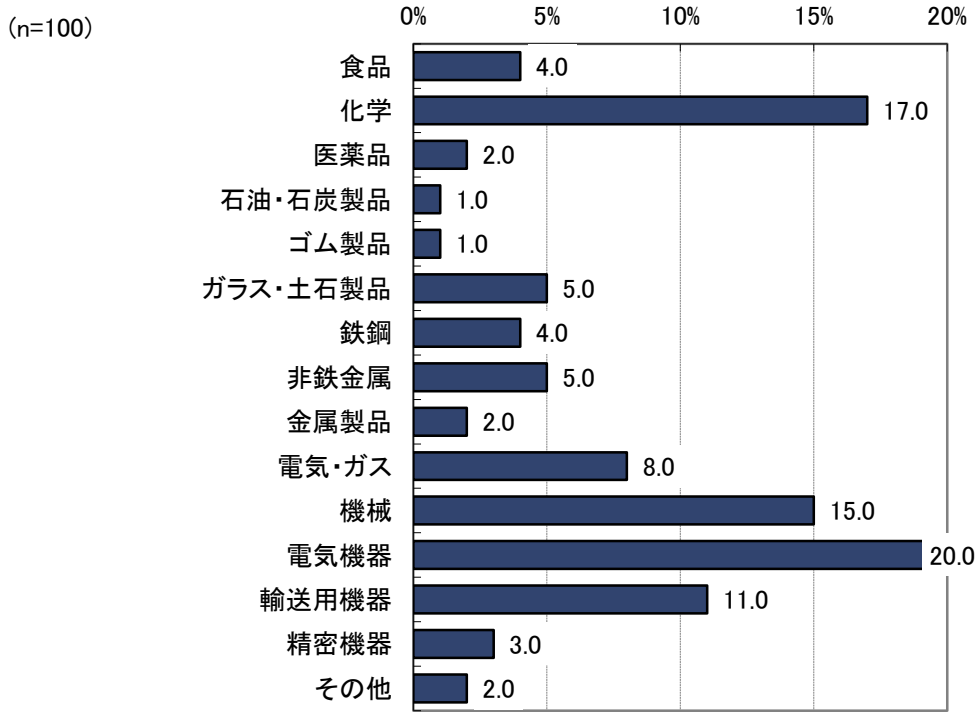
1. 協力してもかまわない　　2. 協力はできない

次のページの「個人情報のお取り扱いについて」にご同意の上、差支えない範囲でご記入をお願いします。

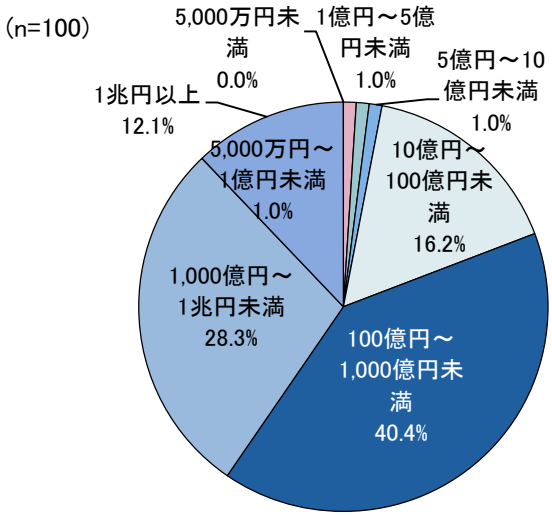
貴社名・貴事業所名	
ご所属・お役職	
お名前	
電話番号	
E-mail	

参考資料２　アンケート回答企業の属性情報

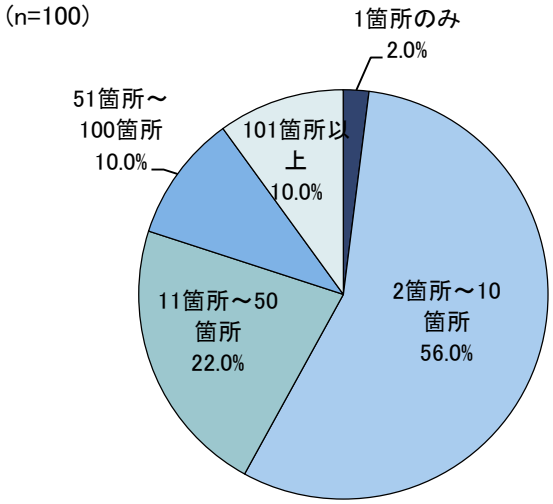
（1）業種



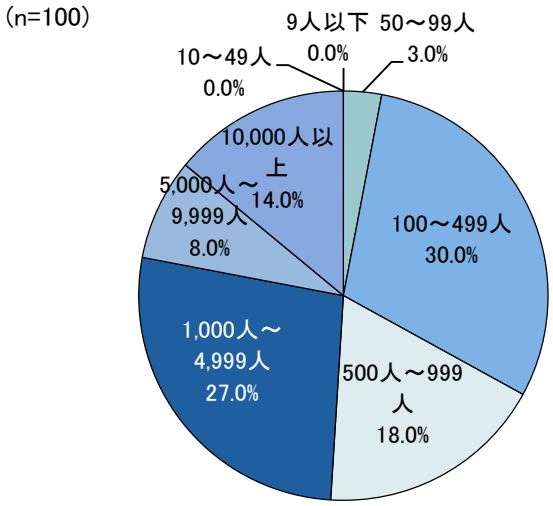
（2）売上高



（3）事業所数



（4）従業員数



（5）回答者の役職