2017 年度 CSIRT 構築および運用における実態調査

一般社団法人 JPCERT コーディネーションセンター

2018 年 12 月 18 日

[目次]

1. はじめに

1.1. 調査の目的

2017 年に「日本シーサート協議会（以下、NCA）」は発足から 10 周年を迎えた。発足時 6 組織だった会員数は、296 組織（2018 年 6 月 25 日現在）まで増加しており、国内の多くの組織で「Computer Security Incident Response Team（CSIRT）」の構築や運用が進められている。このような組織の動きの背景には、影響の大きなサイバー攻撃の発生があるとみられる。特に、2017 年は、ランサムウエア WannaCrypt の流布、Armada Collective による脅迫型 DDoS 攻撃、リスト型攻撃や標的型攻撃など、複数のサイバー攻撃が確認された。さらに、2017 年 11 月に経済産業省が公開した「サイバーセキュリティ経営ガイドライン ver2.0 [1]」が、経営課題として CSIRT 整備の必要性に言及し体制の整備を求めたことも、CSIRT 構築や運用の後押しとなった。

組織内 CSIRT の構築および運用については、組織文化や組織体制、メンバーの技術的背景などによって、複数の形態や構成が考えられる。JPCERT/CC では、組織内 CSIRT の構築を支援する目的にて「CSIRT マテリアル [2)]」を公開し、組織の性格にあった組織内 CSIRT を構築・運用する上でのポイントを解説している。一方で、組織内 CSIRT は、必ずしも設立の当初からすべての機能・役割が揃っているということではなく、必要な機能・役割を段階的に付与していったり、改善していったりするなどして、活動範囲や機能が次第に成熟していく面もある。2015 年度に実施した「2015 年度 CSIRT 構築および運用における実態調査 [3]」では、複数の CSIRT が設立後に要員の拡充を行うなど、設立後に最適化を試みるような傾向が見られた。この調査結果を参考に CSIRT の構築に携われた組織も多いことと思う。

前回調査から 2 年が経過する間に、上述のとおり CSIRT を備える組織が増え、サイバー攻撃の手法も高度化するなど、CSIRT を取り巻く環境も大きく変化している。こうした変化の中に置かれた CSIRT 構築および運用について、その動向を定期的に把握し、柔軟に対応することが重要である。そのような状況認識に立って、本調査は、前回も調査した CSIRT 構築および運用の実態を確認することに加え、既に構築済の CSIRT が成熟した組織となるために取り組むべき課題を把握することを目的として実施した。

新たに CSIRT を構築する際や、既に CSIRT を運用している組織が次の段階に向けた施策を検討する際に役立てていただける調査結果が得られたと信じている。

CSIRT の構築や活動の改善に関心をもっておられる方々に本報告書を参考としていただけることを願っている。

1.2. 本報告書が想定している読者

本報告書は次のような方々を読者として想定している。

- CSIRT の構築を検討している担当者・責任者
- CSIRT を構築中の担当者・責任者
- CSIRT を運用中の担当者・責任者

---

[1] サイバーセキュリティ経営ガイドライン ver2.0:http://www.meti.go.jp/policy/netsecurity/downloadfiles/CSM_Guideline_v2.0.pdf

[2] CSIRT マテリアル: https://www.jpcert.or.jp/csirt_material/

[3] 2015 年度 CSIRT 構築および運用における実態調査:https://www.jpcert.or.jp/research/2015_CSIRT-survey.html

2. CSIRT の構築および運用の実態 (調査結果)

本調査では、2017 年 10 月末に NCA の全加盟組織に対して Web によるアンケート回答を求め、このうち 187 社から同年 11 月中旬にかけて回答を得た。なお、質問項目および回答の集計結果は文末の付録に示す。

実施期間	2017 年 10 月 30 日 ~ 2017 年 11 月 13 日
実施対象	日本シーサート協議会（NCA）加盟組織（262 社：10/30 時点）
方法	Web フォーム
調査名	「2017 年度加盟組織アンケート」
調査概要	各組織におけるサービス提供範囲や運用状況　など
回答組織数	187 組織（回答率：71%）

本章では、この集計結果を前回の調査結果と対比しつつ、CSIRT の構築および運用の実態の現状を明らかにする。本章では、CSIRT の現状について、組織体制、構築時に考慮される 6 つの項目、活動内容の順に述べる。

2.1. 組織体制

前回調査時（2015 年）では NCA 加盟組織が 66 組織であったのに対し、今回は 187 組織に増加している。このことは多くの組織で CSIRT を構築し、他の CSIRT との情報共有など活動の範囲を広げていこうとする動きが背景にあるのではないかとみられる。

CSIRT の構築に注目すると、設立までには概ね 1 年程度の期間を要する場合が多い。「設立準備期間」の設問に対して「6 ヶ月以上～1 年以内」と回答した組織が、前回調査では 2 割程度だったが、今回の調査では 5 割強に増えた。より十分な期間をかけて構築する傾向にあると言える。構築した直後には多くの組織が 10 名以下の人数で部門横断型の形態をとっており、専任者を配置するケースは少ない。この状況は前回調査から変わっていない。
構築にあたっては「情報システム管理部門系」が主導している場合が最も多く、次いで「セキュリティ対策部門系」が主導するケースが多い。いずれにせよ、これら両部署がともに構築に関与し中心となっていることがうかがえる。警察や監督省庁との折衝時に関連のある法務部門や経営企画部門、総務部門が関連部門とし関わっている点に変化は見られなかったが、リスク管理部門の関与が増えつつある傾向が今回の調査結果の特徴である。

CSIRT 構築後も運用形態としては多くの組織が部門横断型を採用しており、「情報システム管理部門系」が取り纏め部署を務めているケースが多い。また、構成メンバーは専任者ではなく兼任者を配置する場合が多く、そうした体制は構築後も継続している。一方、構成人数は「10 名以下から 20 名以上」が多くを占め、構築後に増員しているケースが多い。

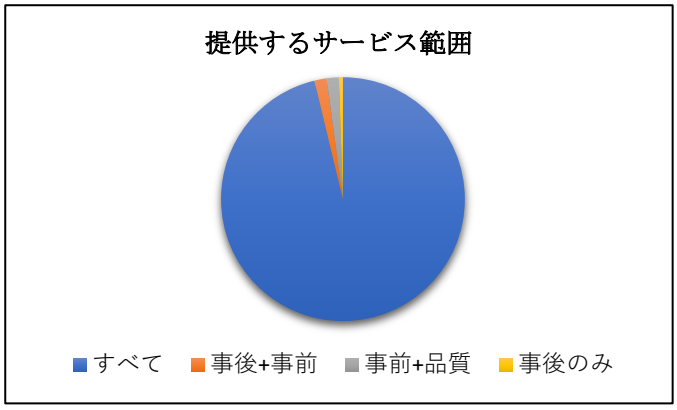
2.2. CSIRT の構築時に考慮される 6 つの項目

2015 年に実施した「CSIRT 構築および運用における実態調査」では、多くの組織が次の 6 つの項目（本報告書では、「CSIRT の構築時に考慮される 6 つの項目」と書く）を定めた上で CSIRT 構築に取り組んでいることを検証し、各項目をどのように定めているかに関する傾向を明らかにした。

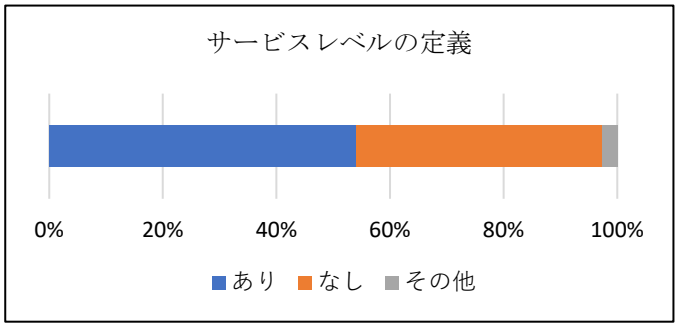
1. CSIRT が提供するサービス範囲
2. CSIRT が持つ権限
3. CSIRT を配置する部署や構成メンバー
4. 連絡窓口（Point of Contact：PoC）
5. 社内に対して CSIRT の活動効果が伝わるような報告体制
6. 定期的な CSIRT 活動の見直し

今回の調査では、これらの項目の中身についても、アンケートを通じて調査し前回の結果との対比を試みた。

2.2.1. CSIRT が提供するサービス範囲



NCA が提供している「CSIRT スタータキット[4]」では、CSIRT の提供サービスを、「事後対応型サービス」、「事前対応型サービス」、「セキュリティ品質管理サービス」の 3 つに大別しており、CSIRT 構築時には提供するサービス範囲を意識しながら体制を整えることが推奨されている。詳細は「2.3. 提供サービス」で触れる。
今回の調査ではいずれかのサービスに絞り込むのではなく、すべてのサービスを提供対象とする組織が大半を占めていることがわかった。なお、サービスレベルを定めている組織はおよそ半分(54%)であった。



2.2.2. CSIRT が持つ権限

セキュリティインシデントの対応では、組織として迅速かつ的確な意思決定が求められる。そのためにはあらかじめ意思決定に責任を持つ部署もしくは人物を決めておくことが肝要である。
インシデント発生時にシステム停止の権限を CSIRT に与えられている組織は 11%であり、81%の組織では

[4] CSIRT スタータキット:http://www.nca.gr.jp/imgs/CSIRTstarterkit.pdf

システム停止の必要性を助言するにとどまっている。システムを停止する決定権は経営者、または CSIRT よりも上位の組織が有していると推測され、CSIRT には、それらの決定者が判断を下すために資する情報を提供することや、組織内における現場対応、技術アドバイス、コーディネーション等の機能を備えていることが期待されていると考えられる。

2.2.3. CSIRT を配置する部署や構成メンバー

前回調査では、「情報システム管理部門系」や「セキュリティ対策部門系」に CSIRT を配置し、構成メンバーもインシデントハンドリングのスキルを有する同部署のメンバーを所属させる組織が多かった。今回の調査でも同様の結果だった。

2.2.4. 連絡窓口 (Point of Contact : PoC)

連絡窓口（Point of Contact: PoC）には外部から自組織に関するインシデント関連情報等を受取り、適切な部署へエスカレーションする機能に加え、類似した組織使命をもつグループと情報共有を図る役割が求められる。
社内のエスカレーション先に関しては各組織とも経営層や広報、法務部門を対象として定義している。一方で、外部組織との連携（報告・相談）については、十分に定義されていない組織が半数程度存在している。このことは、組織外部から情報を得ることができる機会を失う可能性が懸念される。

2.2.5. CSIRT の活動効果が伝わる報告体制

現状は 80%の組織において、経営層（あるいは経営層を含む情報セキュリティ委員会等）へ定期的に報告する機会が設けられており、3 分の 2 の組織が社内に向けたレポートを発行している。

2.2.6. 定期的な CSIRT 活動の見直し

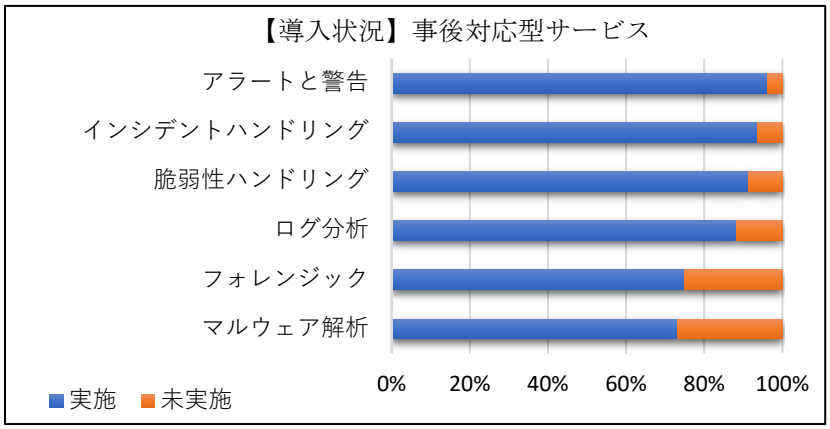
多くの組織が年 1 回の見直しを行っており、数年に 1 回見直しを行っている組織を含めるとおよそ 80%以上の組織で定期的に CSIRT の活動内容を見直していることが分かった。

2.3. 提供サービス

総じて多くの組織がすべてのサービスを実施しているのではなく、自組織の状況にあわせてスモールスタートで活動を開始していることがうかがえる。
本節では「2.2.1. CSIRT が提供するサービス範囲」で提供しているとされたサービスを 3 つのサービス分類ごとに示す。

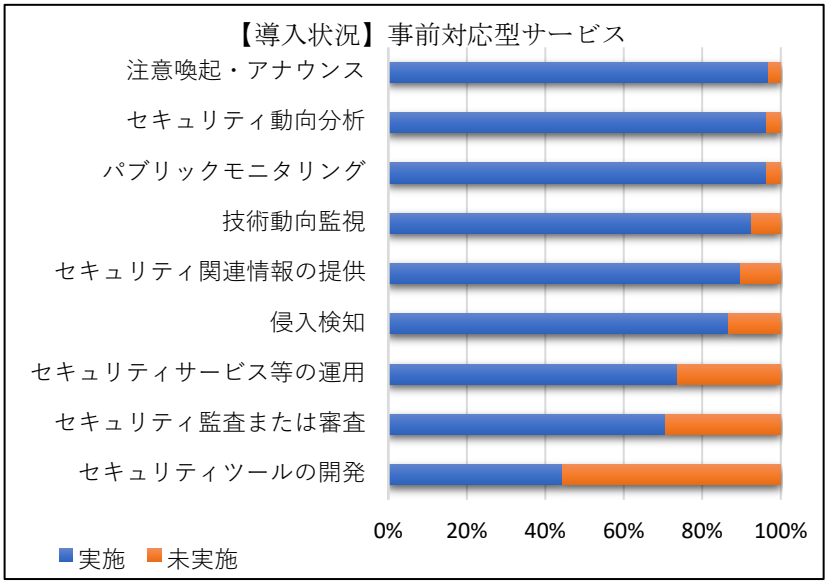
2.3.1. 事後対応型サービス

「脆弱性ハンドリング」、「インシデントハンドリング」「アラートと警告」「ログ分析」といった業務は 9 割以上の組織で実施しているものの、特殊なスキルが必要になる「フォレンジック」、「マルウエア解析」は機能を有してない組織の割合が高くなる。



2.3.2. 事前対応型サービス

組織内外の情報共有の軸となる、「注意喚起・アナウンス」、「セキュリティ関連情報の提供」、「技術動向監視」、「セキュリティ動向分析」、「パブリックモニタリング」は大半の組織で実施しており、CSIRT の基本サービス・メニューとして定着しつつある。

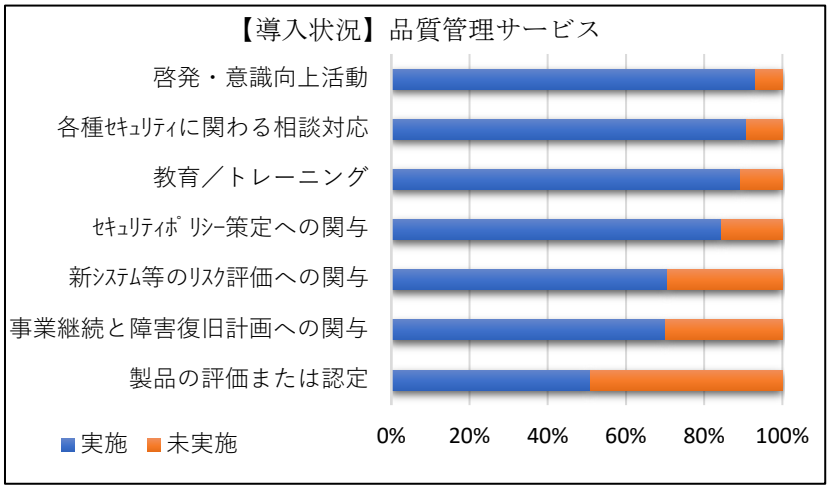


収集した情報の管理・活用という観点から、「IT 資産管理状況」と「セキュリティ関連情報を集約するプラットフォームの導入状況」についてみると、平時は IT 運用管理部門など他部門が管理し、脆弱性対応やインシデント調査時に CSIRT が利用するケースの多い「IT 資産管理」は精粗の違いこそあるものの 96%の組織で実施している（付録 B 8.1.1 参照）。このことから、自組織の IT 資産の情報を活用する仕組みづくりが進みつつあることがわかる。一方で、「パブリックモニタリング」など CSIRT が平時の活動において収集した情報の管理を容易にするための「プラットフォームの導入」は 52%に留まっている（付録 B 8.1.3 参照）。

その他、ソリューションの導入が必要な「セキュリティツールの開発」や「侵入検知」、ノウハウの入手とスキームの設定が必要な「セキュリティツール、アプリケーション、インフラ、およびサービスの運用」や「セキュリティ監査または審査」の実施率は低い。

2.3.3. セキュリティ品質管理サービス

体制整備・人材育成に係る「セキュリティポリシー策定への関与」、「教育/トレーニング」、「啓発・意識向上活動」などのサービスは積極的に実施されている様子がうかがえるが、「製品の評価または認定」、「事業継続と障害復旧計画への関与」など、評価基準の策定や他部署との調整が必要なサービスに関しては、未実施の組織も多くみられる。



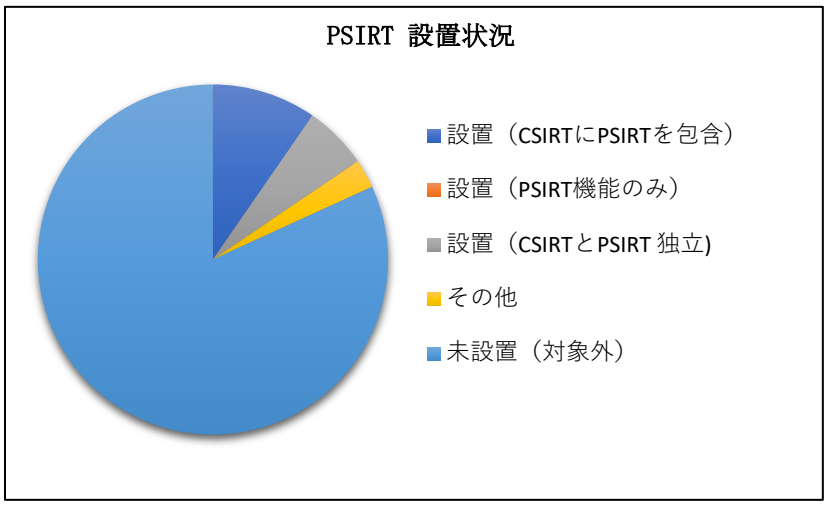
2.4. 社外との連携

過去一年間で、およそ半分程度の組織がインシデントに関する問合せを、2 割～3 割程度の組織が脆弱性に関する報告を、それぞれ組織外から受けている。報告元は、組織により多少のばらつきはあるものの、JPCERT/CC や警察庁、IPA などの専門機関だけでなく、一般ユーザやセキュリティ研究者など幅広くに渡っている。

一方、JPCERT/CC の WAISE(現在は CISTA)には多くの組織が参加しているものの、それ以外の外部コミュニティへの参加は、全体の 2 割弱に留まっている。

2.5. PSIRT 機能

自社製品の脆弱性への対応、製品のセキュリティ品質管理・向上を目的とした PSIRT（Product Security Incident Response Team）の設置が国内の製品開発者においても徐々に進んでいることを踏まえ、今回の調査では PSIRT に関する項目を設けた。



PSIRT 機能を有している組織は全体の 22% 程度であり、そのうち、実際に窓口を設けている組織および脆弱性対応までのプロセスが確立している組織はいずれも 65% 程度、実際に対応経験がある組織はおよそ 50% 程度であった。また、PSIRT の機能を保有する組織のうち、半数程度の組織が CSIRT に PSIRT の機能を持たせており、CSIRT から独立したチームとして PSIRT が存在する組織は 30% 程度だった。

2.6. 現状のまとめ

今回の調査結果を 2015 年の調査結果と比較すると、「2.2. CSIRT の構築時に考慮される 6 つの項目」から「2.4. 社外との連携」までで述べたように、CSIRT 構築および運用についても、組織体制、構築時に考慮される 6 つの項目、活動内容についても大きな変化は見当たらなかった。

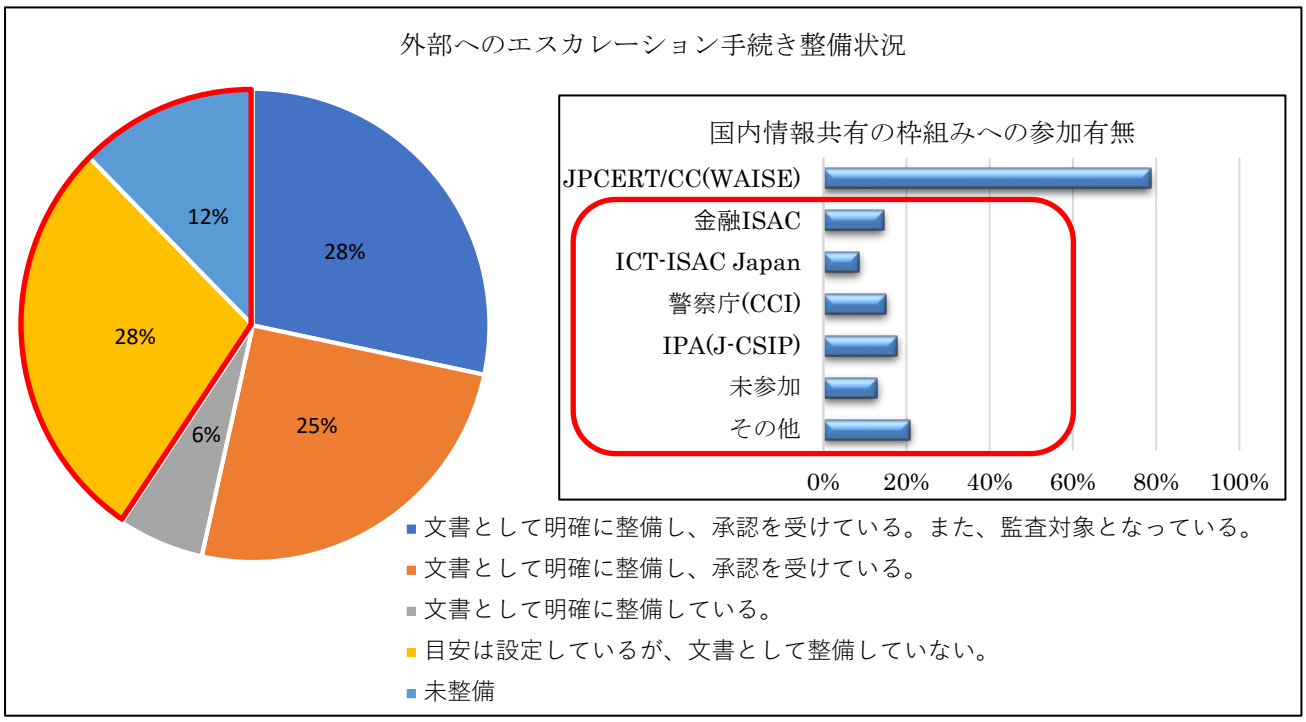
また、「2.1. 普及状況」で述べた CSIRT 構築後の増員についても、「2.3.社内活動」で述べた取り組みやすいサービスを優先的に導入しているケースが多くみられた点についても、設立当初から完成された組織を目指すのではなく、スモールスタートで構築後に組織力の強化を図っていて、2015 年の調査結果と共通している。

一方、実施するサービスに偏りが生まれていることや、社外コミュニティへの参加率が低いという課題があることが分かった。このような状況は、CSIRT が必要なサービスを提供できないことにより十分な情報が得られず、インシデントの根本的な原因を特定できない、あるいは他社でも起きているような標的型攻撃への対応が遅れてしまうなど、インシデント対応を阻む原因となる可能性がある。次章では、これらの課題を克服して、CSIRT がより成熟した組織となるために取り組むべき方策について記す。

3. ステップアップに向けた課題

様々な業界団体において ISAC[5]設立に向けた機運が見られるようになっている。同じ業種の組織は、類似した脅威にさらされていると考えられるため、新たな脅威にいち早く気づき対策を検討するために、業界内での情報共有が役立つと期待されているためであろう。ISAC が設立されるなど、CSIRT を取り巻く組織外の環境の整備が進む状況を踏まえると、今後の CSIRT の活動の方向性として、「外部コミュニケーション」の活動の比重や必要性が高まると考えられる。今回の調査でも、「2.2.4 連絡窓口 (Point of Contact : PoC)」や「2.4 社外との連携」で述べたとおり、多くの CSIRT が外部との情報共有に本格的に取り組めていない。こうした状況から、「外部コミュニケーション」の強化が今後取り組むべき課題の一つと言えるだろう。

[5] Information Sharing and Analysis Center の略称。
同一業界の事業者がサイバーセキュリティに関する情報を共有し、サイバー攻撃への防御力を高めることを目指して活動する組織。



JPCERT/CC では、2017 年度に複数の組織に対して Active Directory のログ分析の技術的な観点について説明するとともに、組織でのログ分析の実情を尋ねたことがあった。その際のヒアリングでは、回答をいただいた組織の 75%が、現状ではインシデント発生時に原因を十分に特定できない可能性が高く、ログの出力項目や分析方法などの見直しまたは、実施状況の確認が必要であると回答している。
このことから、今回の調査では 88%の組織が「ログ分析」を導入していると回答しているものの、取組み内容に改善の余地がある組織が多く存在しているのではないかと推測される。CSIRT 構築に向けた基本的な取組みとして、「原因特定に向けたサービス」に必要な「フォレンジック」、「マルウエア解析」の機能を有してない組織の割合が高いことも軽視できないが、今後は導入済みサービスの取組み内容の充実を図ることが CSIRT として成熟するために重要だと考えられる。

これら 2 つに加えて、多くの CSIRT で改善に向けた努力が期待されることが「事業継続と障害復旧計画への関与」の度合いの向上である。自然災害等の緊急事態を念頭に、近年では、多くの組織において事業継続計画（BCP : Business continuity planning）やシステム障害対応手順（SCP : System Contingency Plan）の検討がなされている。しかし、これらの計画・手順が想定する緊急事態に、サイバー攻撃が含められていない可能性がある。2017 年に世界的に発生したマルウエア WannaCrypt への感染では、一部の工場や事業所で業務が大きく混乱した事例が報じられており、こうした事案などからもサイバー攻撃にも配慮した計画・手順を整備することが望ましい状況になっているといえる。つまり、CSIRT が「事業継続と障害復旧計画への関与」の程度を高めていく必要性があると考える。今回の調査では「2.3.3. セキュリティ品質管理サービス」で確認したとおり、BCP・SCP に未関与の組織が 3 割程あった。このことは、サイバー攻撃にも配慮した計画・手順が検討されていない組織が残っていることを意味する。また、今回の調査では既に関与していると回答している組織でもその関与度合いは不明である。そのため、まだ改善する余地が残っている可能性は否定できない。

こうした状況認識から、次の３つのポイントが多くの CSIRT においてさらに成熟した CSIRT に成長するために優先的に取り組むべきポイントであると考えた。本章では各ポイントの達成に向けた方策等について考察する。

1. 外部コミュニケーションの強化
2. 原因特定に向けたサービスの拡充
3. 事業継続と障害復旧計画への関与

3.1. 外部コミュニケーションの強化

近年、標的型攻撃をはじめとしたサイバー攻撃は巧妙さを増しており、例えば、攻撃者が取引先や組織内の経営層になりすまして送金を指示するメールを担当者に送信する、あるいは、組織内に実際に存在する文書ファイルにマルウエアを組み込んで送り付けるなど、攻撃者の手口が複雑化かつ多様化の一途をたどっている。それらに的確に対処するためには、典型的な攻撃の手口や狙われている業種などの動向情報を把握できていることがきわめて重要である。
また、CSIRT を運営していく上では、「同業他社がセキュリティにどのくらいの予算を投じているか」、「セキュリティ人材の育成をどのように行っているか」など、他社とのベンチマークや他社のグッド・プラクティスから学ぶことも必要になる。
こうした必要性があるにも関わらず、多くの CSIRT が他の組織の CSIRT をはじめとする外部とのコミュニケーションに踏み出せていないことは極めて残念な状況と言わざるを得ない。

外部組織とのコミュニケーションが活発化しない理由としては次の 3 つが考えられる。
① CSIRT 構築段階にあたり外部組織とのコミュニケーションにリソースを割けない
② 情報共有を行う外部コミュニティとのコネクションが少ない
③ 自組織の情報開示に不安（抵抗）がある

①に関しては、CSIRT の構築が一段落した組織や要員が増加している組織は改善に向かうと思われる。

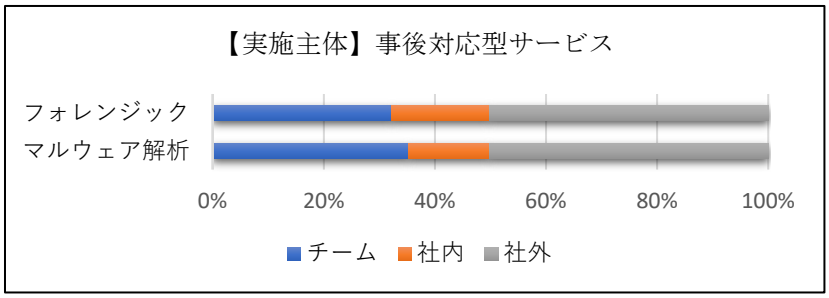
②は既に ISAC が立ち上がっている業界に属す組織であれば、これを活用することが、外部コミュニティとのコネクションを拡大するための近道である。まだ ISAC が立ち上がっていない業界に属す組織については、セキュリティ関連のセミナー等に参加し、参加者と積極的なコミュニケーションを図ることにより、より多くの人脈を形成し、同業あるいは関連業界のセキュリティ担当者とのコネクションを増やすことができるだろう。

③については、TLP(Traffic Light Protocol)など「共有情報の取扱ルール」が整備されたコミュニティに参加することにより情報開示に対する不安が払拭されると考える。インシデントに関する情報の多くは秘密にあたる場合が多い。「CSIRT マテリアル」では「インシデント関連情報を他者と共有するためには、まず何より、関係者以外に情報を漏らさないという『信頼』がお互いに必要です。そして、このような『信頼関係』に基づくコミュニティ＝『信頼の輪』によって共有できる情報の幅が広がり、結果として、CSIRT

の活動に大きな効果を生むのです。」と記している。つまり、情報共有に際しては、お互いに情報の秘匿性を保つこと（信頼）が前提にある。例えば、TLP では情報の機密レベルに応じて発信者が共有可能な範囲を決定する。受信者は決められた範囲に応じて情報を管理することにより情報の秘匿性が保たれる仕組みである。他組織への情報開示に抵抗がある組織においては、参加コミュニティの選定条件に「共有情報の取扱ルール」の整備状況を加えることも一つの手段である。

3.2. 原因特定に向けたサービスの拡充

かつては、ファイアウォールなどを境界線に配備して、ウイルスや不正な通信を自組織のネットワークに侵入させないことが主なセキュリティ対策だと考えられていた。しかし今では、攻撃手法の巧妙化により、境界線での対策をかいくぐって侵入してくる攻撃者がいることを想定して、侵入の早期検知や被害範囲の局所化等に重きを置いた対策が重視されるようになってきている。
また、サイバー攻撃の場合には、被害を受けたシステムを復旧するだけでなく、被害を引き起こしたインシデントの根本的な原因を明らかにし、それを取り除かなければ、同じインシデントが再発する可能性がある。
したがって、被害が顕在化する以前に侵入されていることをできるだけ早く検知できるようにし、さらに、顕在化した被害について原因を特定できるようにすることが強く求められている。こうした要求に応えるためには、情報漏えい発生の有無等を明らかにするための「フォレンジック」やマルウエアの特徴や影響度合いなどを明らかにするための「マルウエア解析」が欠かせないサービスであるが、今回の調査では「2.3.1.1 事後型対応サービス」で述べたように、これらのサービスを提供している率が 7 割前後にとどまっていた。右図はこれらのサービスを提供している組織について、実施主体の内訳を示したものである。社外サービスを利用している組織が多いことがわかる。



「フォレンジック」や「マルウエア解析」には特殊な知見や技術が必要である。それを自組織で獲得し保有することは困難な場合もあり、約半数の組織は社外サービスを利用している。それも 1 つの方法である。

また、88%の組織が導入済みであると回答した「ログ分析」についても、改善の可能性が指摘できないわけではない。例えば、目的に応じて取得すべきログ種目・項目が異なることや、機器の標準設定では出力されない項目があること、ログ種別に応じて確認ポイントが異なることなどを意識して取り組んでいる組織はどのくらいあるのだろうか。意識して取り組んでいる場合も、攻撃手法の変化に応じて、分析する観点を定期的に改善している組織はどのくらいあるのだろうか。サービスは導入しているものの、期待する効果が得られないというような形骸化した状況は避けたいところである。こうした状況を回避するためには、各種セミナーや講習への参加などによる知識習得や、セキュリティベンダとコミュニケーションを密に図ることなどサービス導入後の取組みも疎かにしてはならない。

これら導入済みサービスの取組み内容の充実は CSIRT が成熟するための一つの取組みとして考えられる。

3.3. 事業継続と障害復旧計画への関与

インシデント発生時には自組織のシステムの一部またはすべて停止させる場合も想定される。その際に事業へどのような影響を及ぼすのか、関連部門がどのように対応し、事業を継続するのか、停止したシステムは誰が何にもとづき復旧を指示するのかなどをあらかじめ定めておくことにより被害拡大や混乱を未然に防ぐことができる。

3.3.1. 積極的な関与

事業継続性の観点からインシデント対応において求められるのは「いかにして被害を最小限に食い止めるか」、そして発生後「いかにして速やかに復旧するか」といった点である。被害は自組織だけではなく、顧客等、多くのステークホルダーに及ぶ可能性も意識しなければならない。例えば、工場内の端末がマルウエアに感染し、基幹システムを停止しなければならない状況において、それにより通常の出荷も停止し、顧客に対して十分な商品供給ができなくなる場合などである。

インシデントが発生した際には、判断が遅れれば遅れるほど被害が拡大することから、可能な限り迅速に判断し対策を講じたい。CSIRT の立場からは、状況把握や対策の検討・実施、報告等に主たる時間を割くことになる。こうした緊迫した状況下において関係部門やステークホルダーとの調整を基本的なスタート・ポイントから始めることは時間的にも困難であると考えられる。事前に準備することで対応できることはあらかじめ備えておくことが望ましい。実際には、計画策定には関連部門との調整や手順書、場合によってはバックアップシステムの構築など、時間と費用を要する。だからこそ、あらかじめ BCP や SCP を策定しておくことに意義があり、早急に整備する必要があると考えられる。

3.3.2. 訓練の実施

BCP、SCP を策定した際には、「有事における円滑な対応」や「計画・手順のブラッシュアップ」などの効果を期待することができるため、計画にもとづく定期的な訓練の実施を伴うと、より有効となると考えられる。

サイバー攻撃は繰り返し攻撃が行われる場合もあり、自然災害やパンデミックなどの事象に比べて事態が長期化する恐れがある。被害範囲の特定においては「ログ分析」や「フォレンジング」などの分析結果を参考にしつつ対応することから従来の BCP、SCP とは対応手順が大きく異なる。加えて、原因が特定できない場合は多くのシステムを停止させることも想定され、実務部門においては代替手段としてアナログな手順を用いる場合があることも認識しなければならない。
組織の BCP や SCP を机上の空論ものとしないためにも、自然災害時への対応と同様に、サイバー攻撃によるインシデントを想定した訓練を定期的に実施することを検討されたい。そのためには、CSIRT が訓練に対して主体的に参画し計画の段階から、組織のインシデント対応体制について検討することが望ま

しい。あわせて、訓練目的を明確にし、スキル向上を目的とする場合は実務者を集めたハンズオン形式、経営判断を含めた全社的な対応手順の確認であれば幹部を集めた演習形式など、目的に応じて訓練対象者や内容に考慮する必要もある。

インシデント発生時には限られた時間の中で様々な対応をしなければならない。こうした中で、あらかじめ準備できる「事業継続と障害復旧計画」の策定は優先的に対応すべき事項である。また、計画は策定することがゴールではなく、策定した計画にもとづく定期的な訓練・見直しが重要である。

4. まとめ

CSIRT 構築および運用の実態について、2015 年に実施された前回の調査以降の変化を明らかにするとともに，より成熟した CSIRT になるために取り組むべき課題を把握することを目的として本調査を実施した。

前回の調査では、CSIRT の組織定義に含めるべき 6 項目があることが明らかにされた。今回の調査では、この 6 項目に沿って CSIRT 構築および運用の実態を分析した。その結果、設立当初から完全なメニューでのサービス提供を目指すのではなく、スモールスタートで CSIRT を立ちあげた後に徐々にサービスや組織力の強化を図っていること等において、前回の調査結果から大きな傾向の変化がないことが確認できた。

一方、JPCERT/CC が日常業務の中で交流する機会のある CSIRT の多くが、さらに成熟した CSIRT にステップアップしようとしつつ、それを果たせないでいるように感じられる。ステップアップの契機になり得るものとして、1) 他の組織の CSIRT との交流、2) インシデントの原因特定を可能にするサービスの保有、3) 事業継続と障害復旧計画への CSIRT としての関与、の 3 項目に JPCERT/CC では着目している。

今回の調査結果の分析にあたり、上記の 3 項目に沿って CSIRT の実態を分析し、ステップアップに挑戦する CSIRT が取り組むべき方向性を考察した。

新たに CSIRT の構築を検討している方々にとって、本報告書が現実の CSIRT の実態を理解するための助けとなることを願っている。前回の「2015 年度 CSIRT 構築および運用における実態調査」や NCA が提供している「CSIRT スタータキット」と併せて参考にして、CSIRT の構築に取り組んでいただきたい。

また、既に活動中の CSIRT のステップアップを目指している方々にとっては，本報告書の第 3 章が、そのための手掛かりを与えるヒントとなることを願っている。留意いただきたいポイントは、最新のセキュリティ動向を把握し、脅威に対して的確に対応していくことであり、本書で論じたことがすべてではないことは勿論である。情勢は刻々と変化しており、何が脅威となるかは事業内容によって異なるところである。また、具体的な手順に落とし込む場合は組織形態や社風などを考慮し、自組織に適応したものに落とし込む必要がある。そのかなめとなっているのが CSIRT 担当者である。日々の業務で大変かもしれない

が、現状に満足することなく、自組織のインシデントマネジメント力向上に向け、改善に取り組んでいただきたい。

5. 謝辞

日々の業務で忙しい中、本調査におけるアンケートにご協力いただいた各組織の CSIRT の皆様には厚く感謝を申し上げたい。
今後とも、ご協力のほどよろしくお願いしたく、本報告書の締めとさせていただく。

付録 A　~アンケート項目~

[表 1.3.1 アンケート項目]

アンケート項目
1. 基本情報
1.1 年度
(a) 2016 年度
(b) 2017 年度
1.2 業種
(a) 水産
(b) 鉱業
(c) 建設
(d) 食品
(e) 繊維
(f) パルプ・紙
(g) 化学工業
(h) 医薬品
(i) 石油
(j) ゴム
(k) 窯業
(l) 鉄鋼業
(m) 非鉄金属・金属製品
(n) 機械
(o) 電気機器
(p) 造船
(q) 自動車・自動車部品
(r) その他 輸送機器
(s) 精密機器
(t) その他 製造業
(u) 商社
(v) 小売業
(w) 銀行
(x) 証券
(y) 保険
(z) その他 金融業
(aa)不動産
(bb)鉄道・バス
(cc)陸運
(dd)海運
(ee)空運

(ff) 倉庫・運輸関連
(gg)通信
(hh)電力
(ii) ガス
(jj) サービス業(IT 関連)
(kk) サービス業(非 IT 関連)
(ll) 学術(大学・研究機関)

1.3 会社規模

(a) 50 名以下
(b) 50～100 名
(c) 100 名～500 名
(d) 500 名～1,000 名
(e) 1,000 名～5000 名
(f) 5,000～10,000 名
(g) 10,000 名以上

2. CSIRT の活動範囲

2.1 対象とする利用者(複数回答可)

(a) 顧客
(b) 社員
(c) グループ会社
(d) その他

2.2 対象とする分野(複数回答可)

(a) 社内向けインフラ：社員が自社で利用するネットワークで発生したインシデントに対応
(b) 顧客向けサービスのシステム：社外の利用者に対して提供しているサービスで発生したインシデントに対応
(c) 顧客納入済システム(SI 事業など)
(d) 顧客サイト(インシデントレスポンスサービス)
(e) 自社製品(ハードウェア、ソフトウェア)の脆弱性対応
(f) その他

2.3 自社で製造・出荷している製品の脆弱性を取り扱う PSIRT(Product Security Incident Response Team)機能を有しているか

(a) はい
(b) いいえ

2.4 PSIRT として行っている対応(複数回答可)

(a) 自社製品の脆弱性受付窓口（POC : Point of Contact)を設置している
(b) 自社製品の利用によって発生したインシデントに対応している
(c) 脆弱性の報告を受けてから修正バージョンリリースまでのプロセスが確立している
(d) その他

(e) 非該当

2.5 PSIRT の位置付け

(a) CSIRT は、組織 CSIRT、PSIRT などを包含している
(b) CSIRT は、PSIRT 機能のみを有する
(c) CSIRT と PSIRT は、それぞれが独立した部署が存在しており、連携している
(d) その他
(e) 非該当

3. CSIRT 構築までの体制

3.1 組織体制

3.1.1 構築を主導した部署

(a) 情報システム管理部門系
(b) 経営企画部門系
(c) 法務部門系
(d) 監査部門系
(e) 開発部門系
(f) 総務部門系
(g) リスク対策部門系
(h) セキュリティ対策部門系
(i) 品質保証部門系
(j) その他

3.1.2 構築に関わった部署(複数回答可)

(a) 情報システム管理部門系
(b) 経営企画部門系
(c) 法務部門系
(d) 監査部門系
(e) 開発部門系
(f) 総務部門系
(g) リスク対策部門系
(h) セキュリティ対策部門系
(i) 品質保証部門系
(j) その他
(k) 特になし

3.1.3 構築時に調整が必要であった部署(複数回答可)

(a) 情報システム管理部門系
(b) 経営企画部門系
(c) 法務部門系
(d) 監査部門系
(e) 開発部門系

- (f) 総務部門系
- (g) リスク対策部門系
- (h) セキュリティ対策部門系
- (i) 品質保証部門系
- (j) その他
- (k) 特になし

3.2 メンバー

3.2.1 設立時のメンバー数(構築に携わった人数(外注も含む))

- (a) 5 名未満
- (b) 5 名以上 10 名未満
- (c) 10 名以上 20 名未満
- (d) 20 名以上

3.2.2 設立時の正社員と外部委託のメンバーの割合

- (a) すべて外部委託
- (b) 正社員 2 割以下
- (c) 正社員 2～4 割
- (d) 正社員 4～7 割
- (e) 正社員 8 割以上
- (f) すべて正社員

3.2.3 設立時の実装の形態

- (a) 独立部署(専任型)
- (b) 部署横断(専任+兼務型)
- (c) 部署横断(兼務型)
- (d) その他

3.3 期間

3.3.1 設立準備期間

- (a) 3 ヶ月以内
- (b) 6 ヶ月以内
- (c) 1 年以内
- (d) 1 年以上

3.3.2 設立年月(構築完了時期)

- ○○年○○月

4. 現在の CSIRT の体制

4.1 組織体制

4.1.1 現在の取り纏め部署(組織内のどの部署に配置されているか)

- (a) 情報システム管理部門系
- (b) 経営企画部門系
- (c) 法務部門系

(d) 監査部門系
(e) 開発部門系
(f) 総務部門系
(g) リスク対策部門系
(h) セキュリティ対策部門系
(i) 品質保証部門系
(j) その他

4.2 メンバー

4.2.1 現在の人数(概数)

(a) 5 名未満
(b) 5 名以上 10 名未満
(c) 10 名以上 20 名未満
(d) 20 名以上

4.2.2 現在の正社員と外部委託のメンバーの割合

(a) すべて外部委託
(b) 正社員 2 割以下
(c) 正社員 2～4 割
(d) 正社員 4～7 割
(e) 正社員 8 割以上
(f) すべて正社員

4.2.3 現在の実装の形態

(a) 独立部署(専任型)
(b) 部署横断(専任+兼務型)
(c) 部署横断(兼務型)
(d) その他

4.2.4 現在の専任の割合

(a) すべて兼務
(b) 専任 2 割以下
(c) 専任 2～4 割
(d) 専任 4～7 割
(e) 専任 8 割以上
(f) すべて専任

4.3 活動全般

4.3.1 インシデント対応時の CSIRT の位置づけ(複数回答可)

(a) 現場で対応作業を実施または支援
(b) 技術的アドバイザ
(c) コーディネーター(調整役)
(d) その他

4.3.2a 過去 1 年間に外部から CSIRT に対しての連絡、問合せの有無(複数回答可)

(a) 問合せ有 : Web サービスの脆弱性
(b) 問合せ有 : 製品の脆弱性
(c) 問合せ有 : インシデント
(d) 問合せ無
(e) その他

4.3.2b CSIRT への連絡、問合せ元(複数回答可)

(a) セキュリティベンダ
(b) IPA
(c) JPCERT/CC
(d) 警察
(e) セキュリティ研究者
(f) 一般ユーザ
(g) その他

4.3.3 サイバー攻撃に関連する国内の情報共有の枠組みへの参加有無(複数回答可)

(a) 参加済 : JPCERT/CC(WAISE)
(b) 参加済 : 金融 ISAC
(c) 参加済 : ICT-ISAC Japan
(d) 参加済 : 警察庁(CCI)
(e) 参加済 : IPA(J-CSIP)
(f) 未参加
(g) その他

4.3.4 他組織とのサイバー攻撃情報の通知/受領で主に利用する記述形式(複数回答可)

(a) テキスト
(b) リッチテキスト(PDF/ワード文書など)
(c) HTML
(d) Open IOC
(e) STIX
(f) その他

4.3.5 緊急度の高いインシデント発生時に委譲されている権限

(a) システムを停止する権限がある(命令指示できる権限がある)
(b) システムを停止する必要性について助言ができる
(c) システムを停止する権限はない
(d) その他

4.4 インシデントを防止、検知、解決するためのプロセスが定められているか

4.4.1 サービスレベルの定義

(a) ある
(b) ない

(c) その他

4.4.2 インシデントの分類と定義

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.4.3 セキュリティポリシーの定義

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.4.4 経営層（あるいは経営層を含む情報セキュリティ委員会等）に CSIRT 活動について定期的に報告を行う体制が定められているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.4.5 CSIRT の目的やサービスについて説明した Web ページが自社のサイト内に存在するか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.4.6 機微な内容を含むインシデントレポートや情報の取り扱い方法について定められているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.4.7 分類されたインシデントについて統計的な処理のうえ、サービス対象者等に開示するルール

等が定められているか
(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている (b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている (c) 明確に設定され、文書として存在しているが、正式に承認されていない (d) だいたいの目安になるものは設定されているが、文書として存在していない (e) 設定されておらず、発生の都度検討している
4.4.8 緊急時に備えて、CSIRT メンバーや関連する担当者間の連絡網が整備されているか
(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている (b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている (c) 明確に設定され、文書として存在しているが、正式に承認されていない (d) だいたいの目安になるものは設定されているが、文書として存在していない (e) 設定されておらず、発生の都度検討している
4.4.9 CSIRT の活動が内部評価や外部評価によって監査され、フィードバックを受ける体制が定められているか
(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている (b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている (c) 明確に設定され、文書として存在しているが、正式に承認されていない (d) だいたいの目安になるものは設定されているが、文書として存在していない (e) 設定されておらず、発生の都度検討している
4.5 インシデント対応
4.5.1 社内部門へのエスカレーション
4.5.1.1 経営層(あるいは経営層を含む情報セキュリティ委員会等)へのエスカレーションの手続きを整備しているか
(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている (b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている (c) 明確に設定され、文書として存在しているが、正式に承認されていない (d) だいたいの目安になるものは設定されているが、文書として存在していない (e) 設定されておらず、発生の都度検討している
4.5.1.2 広報部門へのエスカレーションの手続きを整備しているか
(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている (b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている (c) 明確に設定され、文書として存在しているが、正式に承認されていない (d) だいたいの目安になるものは設定されているが、文書として存在していない

(e) 設定されておらず、発生の都度検討している

4.5.1.3 法務部門へのエスカレーションを行っているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.5.1.4 監査部門へのエスカレーションを行っているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.5.2 外部組織へのエスカレーション

4.5.2.1 外部組織へのエスカレーションの手続きを整備しているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない
(d) だいたいの目安になるものは設定されているが、文書として存在していない
(e) 設定されておらず、発生の都度検討している

4.5.2.2 どのような外部組織にエスカレーションしたことがありますか

(a) JPCERT/CC
(b) 金融 ISAC
(c) ICT-ISAC Japan
(d) 警察庁
(e) IPA
(f) 顧客
(g) セキュリティベンダ
(h) その他

4.5.3 インシデント対応経験

4.5.3.1 インシデントを防止、検知、解決するための手続きを整備しているか

(a) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている
(b) 明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている
(c) 明確に設定され、文書として存在しているが、正式に承認されていない

- (d) だいたいの目安になるものは設定されているが、文書として存在していない
- (e) 設定されておらず、発生の都度検討している

4.5.3.2 CSIRT 設立以降、どのようなインシデントに対応したか (複数回答可)

- (a) 自社サイトを装ったフィッシングサイトの開設
- (b) Web サイト改ざん
- (c) DoS/DDoS
- (d) マルウエア感染(標的型攻撃)
- (e) マルウエア感染(ランサムウエア)
- (f) マルウエア感染(バンキングトロジャン)
- (g) マルウエア感染(その他)
- (h) 情報流出
- (i) 不正アクセス
- (j) その他

4.5.3.3 過去 1 年間においてどのようなインシデントに対応したか(複数回答可)

- (a) 自社サイトを装ったフィッシングサイトの開設
- (b) Web サイト改ざん
- (c) DoS/DDoS
- (d) マルウエア感染(標的型攻撃)
- (e) マルウエア感染(ランサムウエア)
- (f) マルウエア感染(バンキングトロジャン)
- (g) マルウエア感染(その他)
- (h) 情報流出
- (i) 不正アクセス
- (j) その他

4.5.4 SOC による監視体制

4.5.4.1 SOC による監視体制が構築・運用しているか

- (a) 構築・運用している
- (b) 構築・運用していない

4.5.4.2 SOC の監視体制はどのようなものか

- (a) 24 時間 365日監視
- (b) 平日日勤帯のみ
- (c) その他
- (d) 非該当(構築・運用していない)

4.5.4.3 SOC の運用体制はどのようなものか

- (a) 自組織で運用している
- (b) グループ会社に外注している
- (c) 他社に外注している
- (d) その他

(e) 非該当(構築・運用していない)

4.5.4.4 SOC と CSIRT の関係はどのような関係か

(a) CSIRT が SOC 機能を有している
(b) SOC 内に CSIRT を構築している
(c) それぞれが独立した部署として存在しており、連携している
(d) その他
(e) 非該当(構築・運用していない)

4.5.4.5 SOC の構成人数・継続年数・熟練度

<構成人数>
(a) 5 名未満
(b) 5 名以上 10 名未満
(c) 10 名以上 20 名未満
(d) 20 名以上

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施

<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

5. CSIRT の活動(提供サービス)：事後対応(未実施以外は、複数回答可)

5-2 ~ 5-7 は以下の実施単位を指定して回答する
チーム：チーム自身で実施
社内：社内の他部署に依頼
社外：社外に依頼(含む、委託)
未実施：複数回答はしないこと
その他：上記以外

5.1 事後対応に関与している CSIRT メンバーの人数

<専任>
(a) 0 名
(b) 1 名以上 3 名未満
(c) 4 名以上 5 名未満
(d) 5 名以上実施している

<兼任>
(a) 0 名
(b) 1 名以上 3 名未満
(c) 4 名以上 5 名未満
(d) 5 名以上実施している

5.2 アラートと警告
セキュリティ上の脆弱性、侵入検知アラート、コンピュータウイルスなどを検知したアラートなどを通知するとともに、発生している問題への対処に関する情報を提供する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

5.3 インシデントハンドリング(オンサイト or アドバイス)
オンサイトでのインシデント対応支援、遠隔からのインシデント対応支援、インシデント対応調整のいずれかを実施する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

5.4 脆弱性ハンドリング(自社製品 or 利用製品・サービス)
脆弱性に関する情報や報告を受領し、脆弱性の要因や影響範囲の調査、脆弱性の検知と対応策および軽減策に関する対応を実施する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

5.5 マルウエア解析
検知や通知されたマルウエアの動作解析などを実施する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

5.6 フォレンジック
インシデントが発生したときの証拠復旧や、情報漏洩などの証拠調査を実施する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している

(d) 未実施

5.7 ログ分析

<運用年数>

(a) 1 年未満

(b) 1 年以上 3 年未満

(c) 3 年以上 5 年未満

(d) 5 年以上 10 年未満

(e) 10 年以上

(f) 未実施

<熟練度>

(a) まだまだ機能していない

(b) 運用に慣れてきた程度

(c) 十分に機能している

(d) 未実施

6. CSIRT の活動(提供サービス)・・事前対応(未実施以外は、複数回答可)

6-2 ~ 6-10 は以下の実施単位を指定して回答する

チーム：チーム自身で実施

社内：社内の他部署に依頼

社外：社外に依頼(含む、委託)

未実施：複数回答はしないこと

その他：上記以外

6.1 事前対応に関与している CSIRT メンバーの人数

<専任>

(a) 0 名

(b) 1 名以上 3 名未満

(c) 4 名以上 5 名未満

(d) 5 名以上実施している

<兼任>

(a) 0 名

(b) 1 名以上 3 名未満

(c) 4 名以上 5 名未満

(d) 5 名以上実施している

6.2 パブリックモニタリング

セキュリティに関するメーリングリストやセキュリティ関連の

Web サイト等をモニタリングし、情報を収集する。

<運用年数>

(a) 1 年未満

(b) 1 年以上 3 年未満

(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

6.3 技術動向監視

将来の脅威に備え、新しい技術開発に関する動向を監視・ウォッチする。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

6.4 セキュリティ動向分析

将来の脅威に備え、サイバー攻撃やガイドラインに関する動向を監視・ウォッチし、分析する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

6.5 侵入検知

IDS ログのレビューと分析、定義した閾値に達しているイベントへの対応を行い、あらかじめ定義された連絡ルートに基づき、イベントの発生を通知し対処を促す。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

6.6 セキュリティ関連情報の提供

セキュリティの向上に寄与する各種関連情報を提供する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

6.7 注意喚起・アナウンス

新たに発見された脆弱性に対する情報や流行している攻撃手法、技術的動向などを広報や通知する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施

<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

6.8 セキュリティ監査または審査
組織または該当する他の業界標準で定義された要件に基づき、組織のセキュリティ対策状況に対する監査または審査を実施する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

6.9 セキュリティツール、アプリケーション、インフラ、およびサービスの運用 CSIRT 自身が使用するツール、アプリケーション、および一般的なコンピュータ設備を安全に設定・保守する方法に関する適切なガイダンスを提示する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

6.10 セキュリティツールの開発(CSIRT が利用するものを含む)
CSIRT 活動を推進する上で必要となるツールを開発する。

<運用年数>

(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

7. CSIRT の活動(提供サービス)：セキュリティ品質管理(未実施以外は、複数回答可)

7-2 ~ 7-8 は以下の実施単位を指定して回答する
チーム：チーム自身で実施
社内：社内の他部署に依頼
社外：社外に依頼(含む、委託)
未実施：複数回答はしないこと
その他：上記以外

7.1 セキュリティ品質管理に関与している CSIRT メンバーの人数

<専任>
(a) 0 名
(b) 1 名以上 3 名未満
(c) 4 名以上 5 名未満
(d) 5 名以上実施している
<兼任>
(a) 0 名
(b) 1 名以上 3 名未満
(c) 4 名以上 5 名未満
(d) 5 名以上実施している

7.2 新サービスまたはシステム等のリスク評価への関与
攻撃の脅威や情報資産に対するリスクの評価や評価を支援する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施

<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

7.3 事業継続と障害復旧計画への関与
事業経営に深刻な影響をもたらすインシデントが発生する可能性を鑑み、大規模インシデントが発生した際に、事業を継続するための障害復旧計画を検討する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

7.4 各種セキュリティに関わる相談対応
サイバー攻撃の発生に備え、組織運営のために実施すべきセキュリティ対策などに関する助言や相談にのる。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

7.5 啓発・意識向上活動
セキュリティの理解を高めることにより、日常業務を安全に遂行することを目的として、ガイドラインを提供する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

7.6 教育／トレーニング
セミナー、ワークショップ、チュートリアルなどの形式で、セキュリティ関連情報を提供する。具体的なテーマには、セキュリティインシデントの防止・検知・対応に必要な情報の提供などを含む。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

7.7 製品の評価または認定
CSIRT または組織のセキュリティ要件に適合していることを保証するために、ツール、アプリケーション、その他のセキュリティサービスを対象に製品評価を実施する。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない

(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

7.8 セキュリティポリシー策定への関与
組織のセキュリティポリシーの策定や策定に関わる助言や相談にのる。

<運用年数>
(a) 1 年未満
(b) 1 年以上 3 年未満
(c) 3 年以上 5 年未満
(d) 5 年以上 10 年未満
(e) 10 年以上
(f) 未実施
<熟練度>
(a) まだまだ機能していない
(b) 運用に慣れてきた程度
(c) 十分に機能している
(d) 未実施

8.その他

8.1 ツールについて

8.1.1 IT 資産の管理を組織的に実施しているか

(a) 実施しており、インシデント対応の際には迅速に棚卸が行える
(b) 実施してはいるが、一部抜け漏れがある可能性がある
(c) 実施していない

8.1.2 インシデント対応を追跡するためトラッキングシステムやワークフローを導入しているか

(a) 導入しており、予行演習や実対応にて有効性を確認している
(b) 導入しているが、実際に機能するかどうかはわからない
(c) 導入していない

8.1.3 セキュリティ関連情報(インディケータ情報も含む)を集約するプラットフォームを導入しているか

(a) 導入しており、予行演習や実対応にて有効性を確認している
(b) 導入しているが、実際に機能するかどうかはわからない
(c) 導入していない

8.2 体制やルールの見直し

8.2.1 定期的にサービスの提供範囲の見直しを実施しているか

(a) 月に 1 回以上実施
(b) 四半期に 1 回
(c) 半年に 1 回
(d) 年に 1 回

(e) 数年に 1 回 (f) 実施していない
8.2.2 定期的に連絡体制図(メールアドレスや電話番号等)の見直しを実施しているか
(a) 月に 1 回以上実施 (b) 四半期に 1 回 (c) 半年に 1 回 (d) 年に 1 回 (e) 数年に 1 回 (f) 実施していない
8.3 活動報告
8.3.1 定期的にレポートは発行しているか
(a) 月に 1 回以上実施 (b) 四半期に 1 回 (c) 半年に 1 回 (d) 年に 1 回 (e) 数年に 1 回 (f) 実施していない
8.3.2 レポートの公開範囲
(a) CSIRT 内 (b) 関連部署内 (c) 社内全体 (d) 社外(Web ページなど) (e) その他

付録 B　~アンケート結果~

ここではアンケートの結果について記載する。

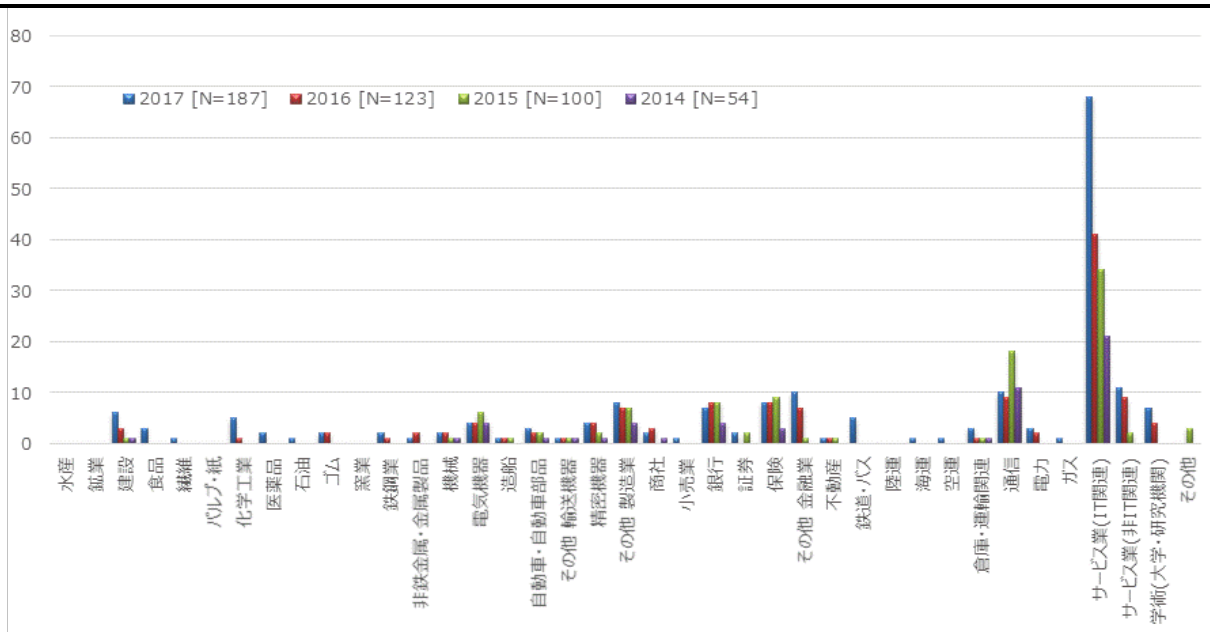
なお、表中の値は基本的に 2017 年のデータを記載する。

1.基本情報

1.1.年度

1.2.業種

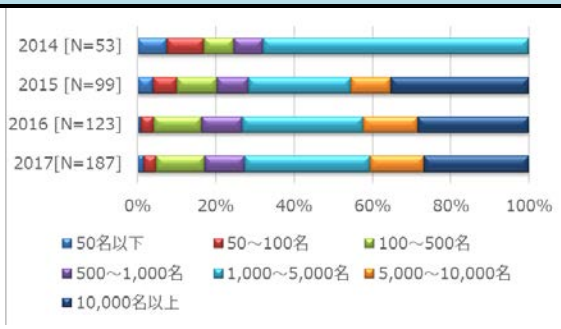
1.2. 業種					
#	項目名	回答数	#	項目名	回答数
a	水産	0	u	商社	2
b	鉱業	0	v	小売業	1
c	建設	6	w	銀行	7
d	食品	3	x	証券	2
e	繊維	1	y	保険	8
f	パルプ・紙	0	z	その他 金融業	10
g	化学工業	5	aa	不動産	1
h	医薬品	2	bb	鉄道・バス	5
i	石油	1	cc	陸運	0
j	ゴム	2	dd	海運	1
k	窯業	0	ee	空運	1
l	鉄鋼業	2	ff	倉庫・運輸関連	3
m	非鉄金属・金属製品	1	gg	通信	10
n	機械	2	hh	電力	3
o	電気機器	4	ii	ガス	1
p	造船	1	jj	サービス業(IT 関連)	68
q	自動車・自動車部品	3	kk	サービス業(非 IT 関連)	11
r	その他 輸送機器	1	ll	学術(大学・研究機関)	7
s	精密機器	4	mm	その他	0
t	その他 製造業	8			



（複数回答なし　2017 [N = 187]、2016 [N = 123]、2015 [N = 100]、2014 [N = 54]）

1.3.会社規模

1.3. 会社規模		
#	項目	回答数
a	50 名以下	3
b	50～100 名	6
c	100 名～500 名	23
d	500 名～1,000 名	19
e	1,000 名～5000 名	60
f	5,000～10,000 名	26
g	10,000 名以上	50

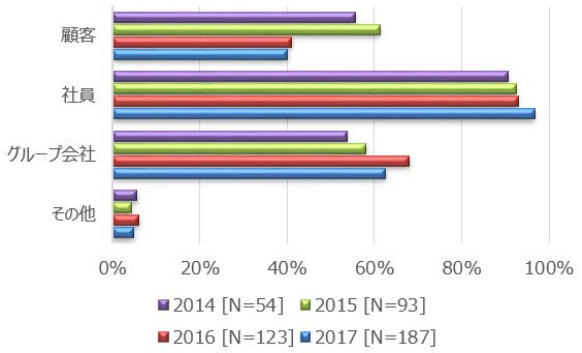


（複数回答なし 2017 [N = 187]、2016 [N = 123]、2015 [N = 99]、2014 [N = 53]）

2. CSIRT の活動範囲

2.1. 対象とする利用者(複数回答可)

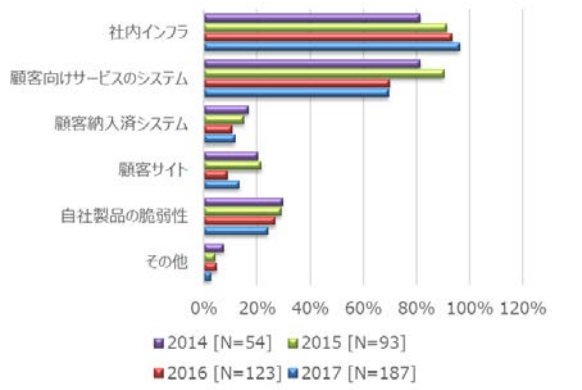
2.1. 対象とする利用者(複数回答可)		
#	項目	回答数
a	顧客	75
b	社員	181
c	グループ会社	117
d	その他	9



（複数回答あり 2017 [N = 187]、2016 [N = 123]、2015 [N = 93]、2014 [N = 54]）

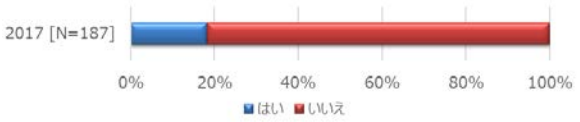
2.2. 対象とする分野（複数回答可）

2.2. 対象とする分野(複数回答可)		
#	項目	回答数
a	社向インフラ ¨社員が自社で利用するネットワークで発生したインシデントに対応	180
b	顧客向けサービスのシステム ¨社外の利用者に対して提供しているサービスで発生したインシデントに対応	130
c	顧客納入済システム(SI 事業など)	22
d	顧客サイト(インシデントレスポンスサービス)	25
e	自社製品(ハードウェア、ソフトウェア)の脆弱性対応	45
f	その他	5



（複数回答あり 2017 [N = 187]、2016 [N = 123]、2015 [N = 99]、2014 [N = 53]）

2.3.自社で製造・出荷している製品の脆弱性を取り扱う PSIRT(Product Security Incident Response Team)機能を有しているか

2.3. 自社で製造・出荷している製品の脆弱性を取り扱う PSIRT(Product Security Incident Response Team)機能を有しているか			
#	項目	回答数	
a	はい	34	
b	いいえ	153	

（複数回答なし 2017 [N = 187]）

2.4.PSIRT として行っている対応（複数回答可）

2.4. PSIRT として行っている対応(複数回答可)			
#	項目	回答数	
a	自社製品の脆弱性受付窓口（POC：Point of Contact)を設置している	23	
b	自社製品の利用によって発生したインシデントに対応している	18	
c	脆弱性の報告を受けてから修正バージョンリリースまでのプロセスが確立している	22	
d	その他	6	
e	非該当	151	

（複数回答あり 2017 [N = 187]）

2.5.PSIRT の位置付け

2.5. PSIRT の位置付け			
#	項目	回答数	
a	CSIRT は、組織 CSIRT、PSIRT などを包含している	18	
b	CSIRT は、PSIRT 機能のみを有する	0	
c	CSIRT と PSIRT は、それぞれが独立した部署が存在しており、連携している	11	
d	その他	5	

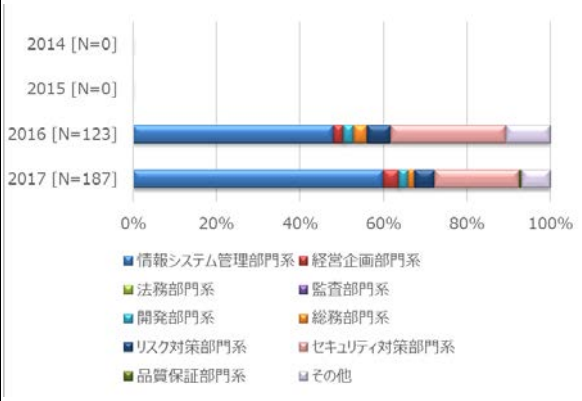
（複数回答なし 2017 [N = 34]）

3.CSIRT 構築までの体制

3.1 組織体制

3.1.1 構築を主導した部署

3.1.1 構築を主導した部署		
#	項目	回答数
a	情報システム管理部門系	112
b	経営企画部門系	7
c	法務部門系	0
d	監査部門系	0
e	開発部門系	4
f	総務部門系	3
g	リスク対策部門系	9
h	セキュリティ対策部門系	38
i	品質保証部門系	1
j	その他	13



（複数回答なし 2017 [N = 187]、2016 [N = 123]、2015 [N = 0]、2014 [N = 0]）

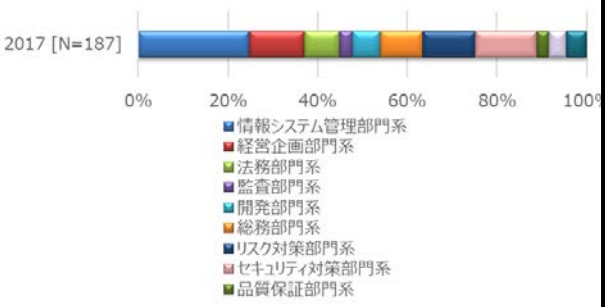
3.1.2 構築に関わった部署（複数回答可）

3.1.2 構築に関わった部署(複数回答可)		
#	項目	回答数
a	情報システム管理部門系	144
b	経営企画部門系	36
c	法務部門系	19
d	監査部門系	6
e	開発部門系	34
f	総務部門系	35
g	リスク対策部門系	51
h	セキュリティ対策部門系	87
i	品質保証部門系	11
j	その他	21
k	特になし	5

（複数回答あり 2017 [N = 187]）

3.1.3 構築時に調整が必要であった部署（複数回答可）

3.1.3 構築時に調整が必要であった部署(複数回答可)		
#	項目	回答数
a	情報システム管理部門系	128
b	経営企画部門系	63
c	法務部門系	40
d	監査部門系	15
e	開発部門系	32
f	総務部門系	49
g	リスク対策部門系	60
h	セキュリティ対策部門系	71
i	品質保証部門系	14
j	その他	20
k	特になし	23

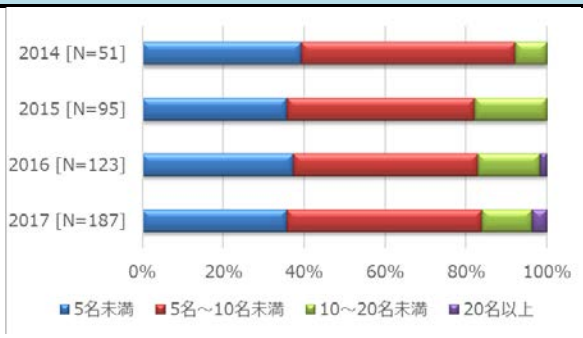


（複数回答あり 2017 [N = 187]）

3.2 メンバー

3.2.1 設立時のメンバー数（構築に携わった人数（外注も含む））

3.2.1 設立時のメンバー数(構築に携わった人数(外注も含む))		
#	項目	回答数
a	5 名未満	67
b	5 名以上 10 名未満	90
c	10 名以上 20 名未満	23
d	20 名以上	7



（複数回答なし 2017 [N = 187]、2016 [N = 123]、2015 [N = 95]、2014 [N = 51]）

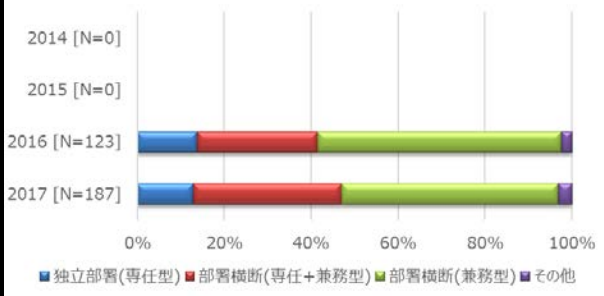
3.2.2 設立時の正社員と外部委託のメンバーの割合

3.2.2 設立時の正社員と外部委託メンバーの割合		
#	項目	回答数
a	すべて外部委託	0
b	正社員 2 割以下	4
c	正社員 2～4 割	6
d	正社員 4～7 割	12
e	正社員 8 割以上	18
f	すべて正社員	147

（複数回答なし 2017 [N = 187]）

3.2.3 設立時の実装の形態

3.2.3 設立時の実装の形態		
#	項目	回答数
a	独立部署(専任型)	24
b	部署横断(専任+兼務型)	64
c	部署横断(兼務型)	93
d	その他	6

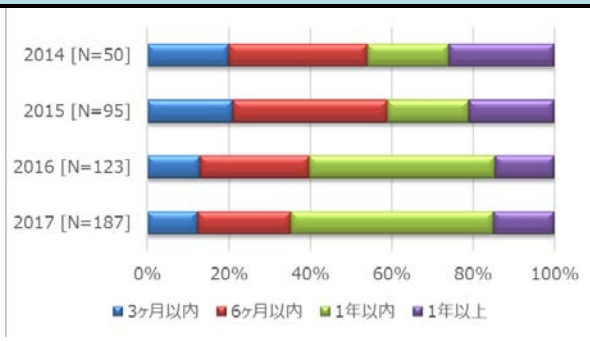


（複数回答なし 2017 [N = 187]、
2016 [N = 123]、2015 [N = 0]、2014 [N = 0]）

3.3 期間

3.3.1 設立準備期間

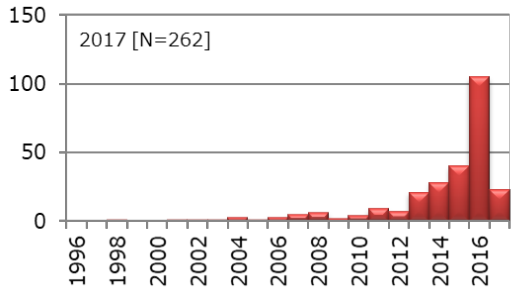
3.3.1 設立準備期間		
#	項目	回答数
a	3 ヶ月以内	23
b	6 ヶ月以内	43
c	1 年以内	93
d	1 年以上	28



（複数回答なし 2017 [N = 187]、
2016 [N = 123]、2015 [N = 95]、2014 [N = 50]）

3.3.2 設立年月（構築完了時期）

3.3.2 設立年月(構築完了時期)		
#	項目	回答数
a	2010 年以前	29
b	2011 年	6
c	2012 年	7
d	2013 年	21
e	2014 年	28
f	2015 年	40
g	2016 年	105
h	2017 年	23



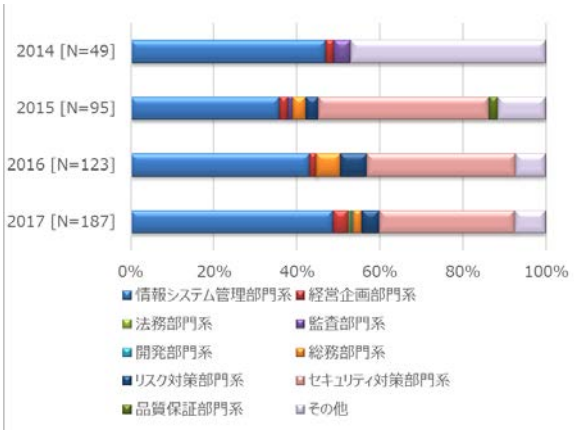
（複数回答なし [N = 262]）

4 現在の CSIRT の体制

4.1 組織体制

4.1.1 現在の取り纏め部署（組織内のどの部署に配置されているか）

4.1.1 現在の取り纏め部署(組織内のどの部署に配置されているか)		
#	項目	回答数
a	情報システム管理部門系	91
b	経営企画部門系	7
c	法務部門系	1
d	監査部門系	0
e	開発部門系	1
f	総務部門系	4
g	リスク対策部門系	8
h	セキュリティ対策部門系	61
i	品質保証部門系	0
j	その他	14

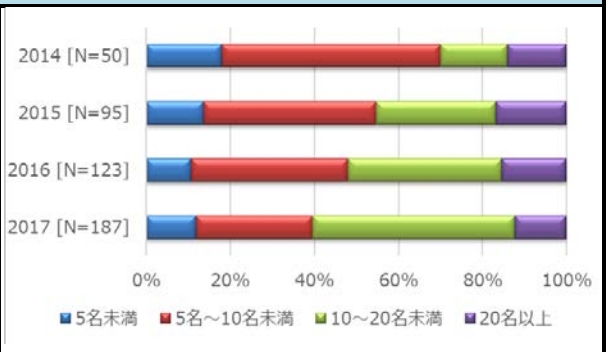


（複数回答なし 2017 [N = 187]、2016 [N = 123]、2015 [N = 95]、2014 [N = 49]）

4.2 メンバー

4.2.1 現在の人数（概数）

4.2.1 現在の人数(概数)		
#	項目	回答数
a	5 名未満	22
b	5 名以上 10 名未満	52
c	10 名以上 20 名未満	90
d	20 名以上	23



（複数回答なし 2017 [N = 187]、2016 [N = 123]、2015 [N = 95]、2014 [N = 50]）

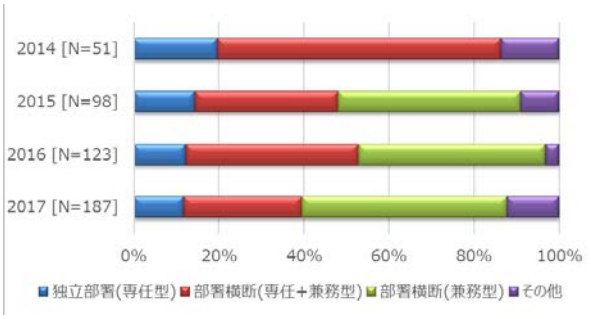
4.2.2 現在の正社員と外部委託のメンバーの割合

4.2.2 現在の正社員と外部委託のメンバーの割合		
#	項目	回答数
a	すべて外部委託	0
b	正社員 2 割以下	3
c	正社員 2～4 割	6
d	正社員 4～7 割	51
e	正社員 8 割以上	27
f	すべて正社員	100

（複数回答なし 2017 [N = 187]）

4.2.3 現在の実装の形態

4.2.3 現在の実装の形態		
#	項目	回答数
a	独立部署(専任型)	22
b	部署横断(専任+兼務型)	52
c	部署横断(兼務型)	90
d	その他	23



（複数回答なし 2017 [N = 187]、2016 [N = 123]、2015 [N = 98]、2014 [N = 51]）

4.2.4 現在の専任の割合

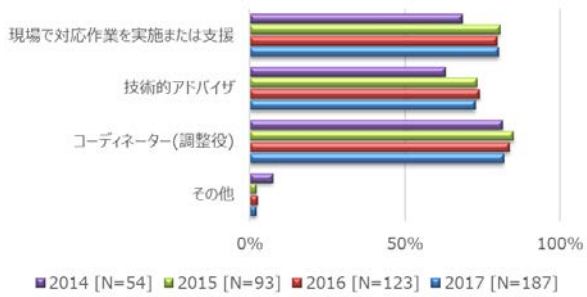
4.2.4 現在の専任の割合		
#	項目	回答数
a	すべて兼務	111
b	専任 2 割以下	25
c	専任 2～4 割	10
d	専任 4～7 割	19
e	専任 8 割以上	5
f	すべて専任	17

（複数回答なし 2017 [N = 187]、2016 [N = 123]、2015 [N = 86]、2014 [N = 41]）

4.3 活動全般

4.3.1 インシデント対応時の CSIRT の位置づけ（複数回答可）

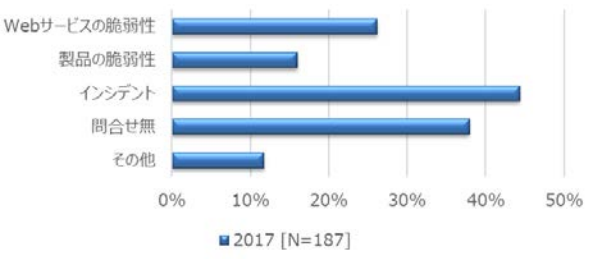
4.3.1 インシデント対応時の CSIRT の位置づけ(複数回答可)		
#	項目	回答数
a	現場で対応作業を実施または支援	260
b	技術的アドバイザ	136
c	コーディネーター(調整役)	153
d	その他	4



（複数回答あり 2017 [N = 187]、2016 [N = 123]、2015 [N = 93]、2014 [N = 54]）

4.3.2(a) 過去 1 年間に外部から CSIRT に対しての連絡、問合せの有無(複数回答可)

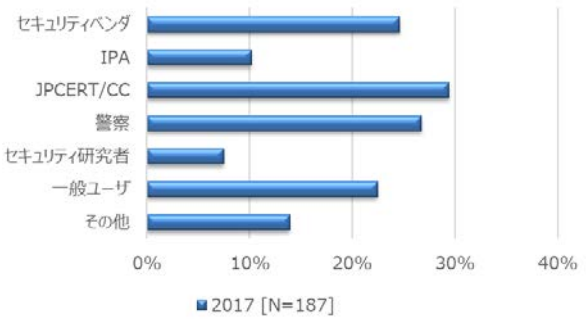
4.3.2(a) 過去 1 年間に外部から CSIRT に対しての連絡、問合せの有無(複数回答可)		
#	項目	回答数
a	問合せ有 ：Web サービスの脆弱性	49
b	問合せ有 ： 製品の脆弱性	30
c	問合せ有 ： インシデント	83
d	問合せ無	71
e	その他	22



（複数回答あり 2017 [N = 187]）

4.3.2(b) 過去 1 年間に外部から CSIRT に対しての連絡、問合せの有無(複数回答可)

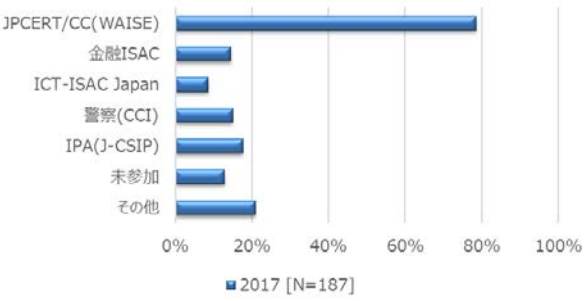
4.3.2(b) 過去 1 年間に外部から CSIRT に対しての連絡、問合せの有無(複数回答可)		
#	項目	回答数
a	セキュリティベンダ	46
b	IPA	19
c	JPCERT/CC	55
d	警察	50
e	セキュリティ研究者	14
f	一般ユーザ	42
g	その他	26



（複数回答あり 2017 [N = 187]）

4.3.3 サイバー攻撃に関連する国内の情報共有の枠組みへの参加有無(複数回答可)

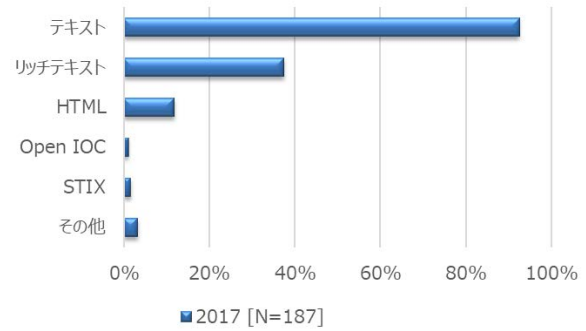
4.3.3 サイバー攻撃に関連する国内の情報共有の枠組みへの参加有無(複数回答可)		
#	項目	回答数
a	参加済 ：JPCERT/CC(WAISE)	147
b	参加済 ： 金融 ISAC	27
c	参加済 ：ICT-ISAC Japan	16
d	参加済 ： 警察庁(CCI)	28
e	参加済 ：IPA(J-CSIP)	33
f	未参加	24
g	その他	39



（複数回答あり 2017 [N = 187]）

4.3.4 他組織とのサイバー攻撃情報の通知/受領で主に利用する記述形式(複数回答可)

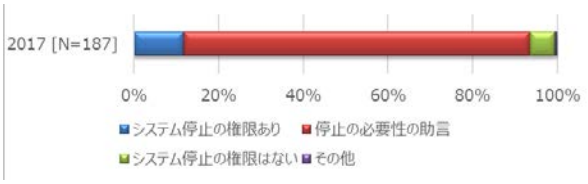
4.3.4 他組織とのサイバー攻撃情報の通知/受領で主に利用する記述形式(複数回答可)		
#	項目	回答数
a	テキスト	173
b	リッチテキスト(PDF/ワード文書など)	70
c	HTML	22
d	Open IOC	2
e	STIX	3
f	その他	6



（複数回答あり 2017 [N = 187]）

4.3.5 緊急度の高いインシデント発生時に委譲されている権限

4.3.5 緊急度の高いインシデント発生時に委譲されている権限		
#	項目	回答数
a	システムを停止する権限がある(命令指示できる権限がある)	22
b	システムを停止する必要性について助言ができる	153
c	システムを停止する権限はない	11
d	その他	1



（複数回答なし 2017 [N = 187]）

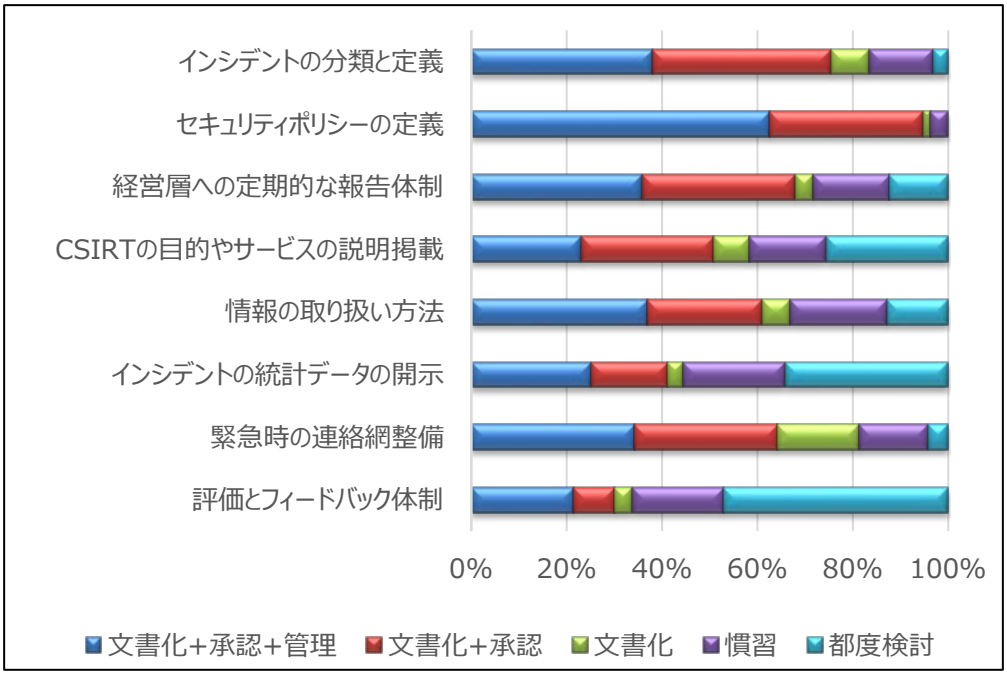
4.4 インシデントを防止、検知、解決するためのプロセスが定められているか

4.4.1 サービスレベルの定義

4.4.1 サービスレベルの定義		
#	項目	回答数
a	ある	101
b	ない	81
c	その他	5

（複数回答なし 2017 [N = 187]）

2-4-4-2 ~ 2-4-4-9 「明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている」については、項目ごとのグラフのサマリを記載し、詳細については、サービスごとに表にて記載する。



[図 2.4.4 インシデントを防止、検知、解決するためのプロセスについて]

4.4.2 インシデントの分類と定義

4.4.2.インシデントの分類と定義		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	71
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	70
c	明確に設定され、文書として存在しているが、正式に承認されていない	15
d	だいたいの目安になるものは設定されているが、文書として存在していない	25
e	設定されておらず、発生の都度検討している	6

4.4.3.セキュリティポリシーの定義

4.4.3.セキュリティポリシーの定義		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	117
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	60
c	明確に設定され、文書として存在しているが、正式に承認されていない	3
d	だいたいの目安になるものは設定されているが、文書として存在していない	7
e	設定されておらず、発生の都度検討している	0

4.4.4. 経営層（あるいは経営層を含む情報セキュリティ委員会等）に CSIRT 活動について定期的に報告を行う体制が定められているか

4.4.4.経営層（あるいは経営層を含む情報セキュリティ委員会等）に CSIRT 活動について定期的に報告を行う体制が定められているか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	67
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	60
c	明確に設定され、文書として存在しているが、正式に承認されていない	7
d	だいたいの目安になるものは設定されているが、文書として存在していない	30
e	設定されておらず、発生の都度検討している	23

4.4.5.CSIRT の目的やサービスについて説明した Web ページが自社のサイト内に存在するか

4.4.5.CSIRT の目的やサービスについて説明した Web ページが自社のサイト内に存在するか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	43
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	52
c	明確に設定され、文書として存在しているが、正式に承認されていない	14
d	だいたいの目安になるものは設定されているが、文書として存在していない	30
e	設定されておらず、発生の都度検討している	48

4.4.6. 機微な内容を含むインシデントレポートや情報の取り扱い方法について定められているか

4.4.6.機微な内容を含むインシデントレポートや情報の取り扱い方法について定められているか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	69
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	45
c	明確に設定され、文書として存在しているが、正式に承認されていない	11
d	だいたいの目安になるものは設定されているが、文書として存在していない	38
e	設定されておらず、発生の都度検討している	24

4.4.7. 分類されたインシデントについて統計的な処理のうえ、サービス対象者等に開示するルール等が定められているか

4.4.7.分類されたインシデントについて統計的な処理のうえ、サービス対象者等に開示するルール等が定められているか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	47
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	30
c	明確に設定され、文書として存在しているが、正式に承認されていない	6
d	だいたいの目安になるものは設定されているが、文書として存在していない	40
e	設定されておらず、発生の都度検討している	64

4.4.8. 緊急時に備えて、CSIRT メンバーや関連する担当者間の連絡網が整備されているか

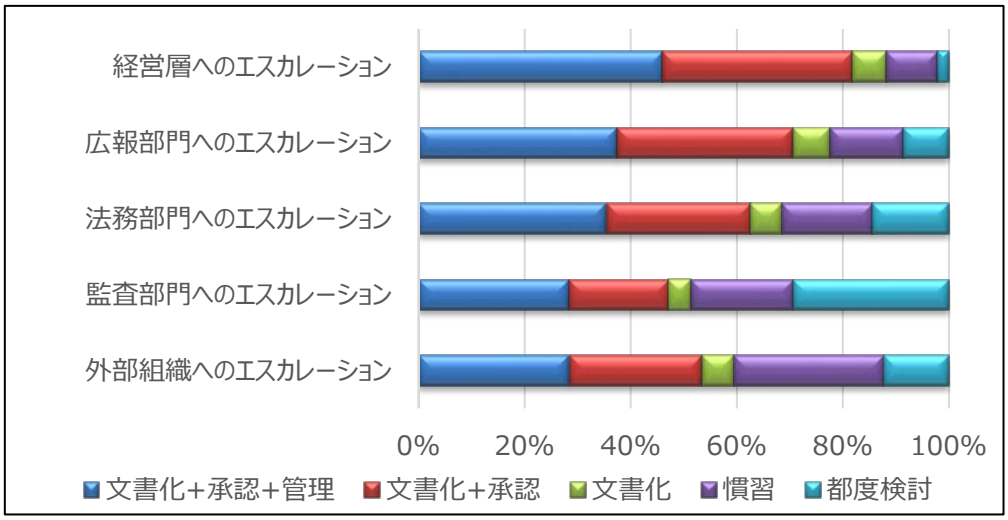
4.4.8.緊急時に備えて、CSIRT メンバーや関連する担当者間の連絡網が整備されているか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	64
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	56
c	明確に設定され、文書として存在しているが、正式に承認されていない	32
d	だいたいの目安になるものは設定されているが、文書として存在していない	27
e	設定されておらず、発生の都度検討している	8

4.4.9.CSIRT の活動が内部評価や外部評価によって監査され、フィードバックを受ける体制が定められているか

4.4.9.CSIRT の活動が内部評価や外部評価によって監査され、フィードバックを受ける体制が定められているか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	40
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	16
c	明確に設定され、文書として存在しているが、正式に承認されていない	7
d	だいたいの目安になるものは設定されているが、文書として存在していない	36
e	設定されておらず、発生の都度検討している	88

4.5 インシデント対応

2-4-5-1-1～2-4-5-2-1 「明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている」については、項目ごとのグラフのサマリを記載し、詳細については、サービスごとに表にて記載する



[図 2.4.5 インシデント対応時のエスカレーション体制について]

4.5.1 社内部門へのエスカレーション

4.5.1.1 経営層（あるいは経営層を含む情報セキュリティ委員会等）へのエスカレーションの手続きを整備しているか

4.5.1.1 経営層(あるいは経営層を含む情報セキュリティ委員会等)へのエスカレーションの手続きを整備しているか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	86
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	67
c	明確に設定され、文書として存在しているが、正式に承認されていない	12
d	だいたいの目安になるものは設定されているが、文書として存在していない	18
e	設定されておらず、発生の都度検討している	4

4.5.1.2 広報部門へのエスカレーションの手続きを整備しているか

4.5.1.2 広報部門へのエスカレーションの手続きを整備しているか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	70
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	62
c	明確に設定され、文書として存在しているが、正式に承認されていない	13
d	だいたいの目安になるものは設定されているが、文書として存在していない	26
e	設定されておらず、発生の都度検討している	16

4.5.1.3 法務部門へのエスカレーションを行っているか

4.5.1.3 法務部門へのエスカレーションの手続きを整備しているか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	66
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	51
c	明確に設定され、文書として存在しているが、正式に承認されていない	11
d	だいたいの目安になるものは設定されているが、文書として存在していない	32
e	設定されておらず、発生の都度検討している	27

4.5.1.4 監査部門へのエスカレーションを行っているか

4.5.1.4 監査部門へのエスカレーションの手続きを整備しているか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	53
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	35
c	明確に設定され、文書として存在しているが、正式に承認されていない	8
d	だいたいの目安になるものは設定されているが、文書として存在していない	36
e	設定されておらず、発生の都度検討している	55

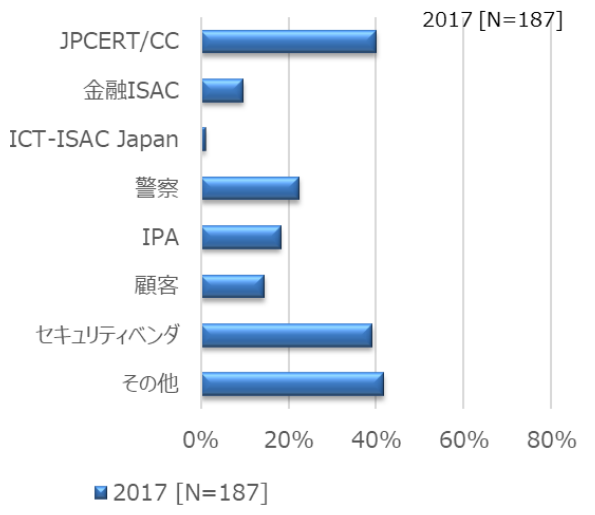
4.5.2 社内部門へのエスカレーション

4.5.2.1 外部組織へのエスカレーションの手続きを整備しているか

4.5.2.1 外部組織へのエスカレーションの手続きを整備しているか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	53
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	47
c	明確に設定され、文書として存在しているが、正式に承認されていない	11
d	だいたいの目安になるものは設定されているが、文書として存在していない	53
e	設定されておらず、発生の都度検討している	23

4.5.2.2 どのような外部組織にエスカレーションしたことがありますか

4.5.2.2.どのような外部組織にエスカレーションしたことがありますか		
#	項目	回答数
a	JPCERT/CC	75
b	金融 ISAC	18
c	ICT-ISAC Japan	2
d	警察庁	42
e	IPA	34
f	顧客	27
g	セキュリティベンダ	73
h	その他	78

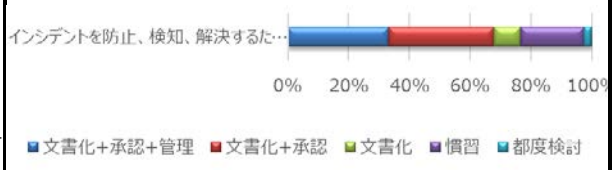


（複数回答なし 2017 [N = 187]）

4.5.3 インシデント対応経験

4.5.3.1 インシデントを防止、検知、解決するための手続きを整備しているか

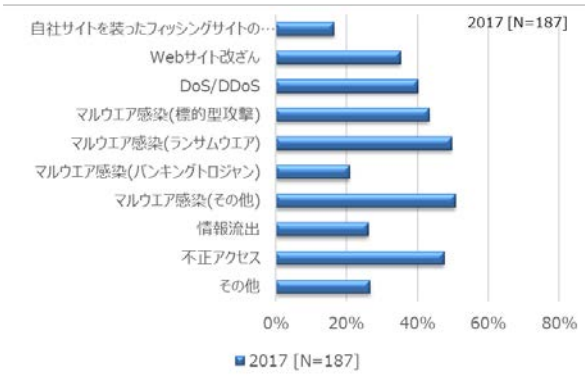
4.5.3.1 インシデントを防止、検知、解決するための手続きを整備しているか		
#	項目	回答数
a	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている、さらに業務が文書に従っているか管理(監査)されている	62
b	明確に設定され、文書として存在しており、CSIRT 責任者や CISO により承認されている	65
c	明確に設定され、文書として存在しているが、正式に承認されていない	16
d	だいたいの目安になるものは設定されているが、文書として存在していない	39
e	設定されておらず、発生の都度検討している	5



（複数回答なし 2017 [N = 187]）

4.5.3.2 CSIRT 設立以降、どのようなインシデントに対応したか (複数回答可)

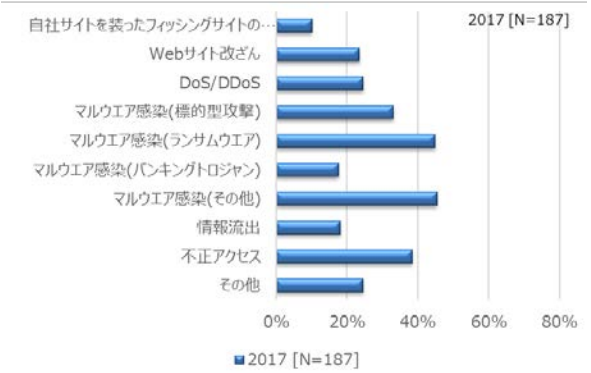
4.5.3.2CSIRT 設立以降、どのようなインシデントに対応したか (複数回答可)		
#	項目	回答数
a	自社サイトを装ったフィッシングサイトの開設	31
b	Web サイト改ざん	66
c	DoS/DDoS	75
d	マルウエア感染(標的型攻撃)	81
e	マルウエア感染(ランサムウエア)	93
f	マルウエア感染(バンキングトロジャン)	39
g	マルウエア感染(その他)	95
h	情報流出	49
i	不正アクセス	89
j	その他	50



（複数回答なし 2017 [N = 187]）

4.5.3.3 過去 1 年間においてどのようなインシデントに対応したか(複数回答可)

4.5.3.3 過去 1 年間においてどのようなインシデントに対応したか (複数回答可)		
#	項目	回答数
a	自社サイトを装ったフィッシングサイトの開設	19
b	Web サイト改ざん	44
c	DoS/DDoS	46
d	マルウエア感染(標的型攻撃)	62
e	マルウエア感染(ランサムウエア)	84
f	マルウエア感染(バンキングトロジャン)	33
g	マルウエア感染(その他)	85
h	情報流出	34
i	不正アクセス	72
j	その他	46



（複数回答なし 2017 [N = 187]）

4.5.4 SOC による監視体制

4.5.4.1 SOC による監視体制が構築・運用しているか

4.5.4.1SOC による監視体制が構築・運用しているか		
#	項目	回答数
a	構築・運用している	108
b	構築・運用していない	79

（複数回答なし 2017 [N = 187]）

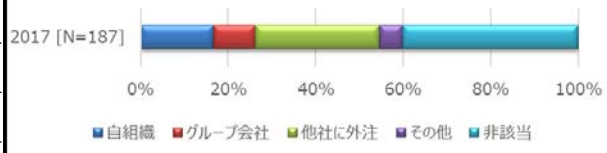
4.5.4.2 SOC の監視体制はどのようなものか

4.5.4.2SOC の監視体制はどのようなものか		
#	項目	回答数
a	24 時間 365日監視	79
b	平日日勤帯のみ	31
c	その他	3
d	非該当(構築・運用していない)	74

（複数回答なし 2017 [N = 187]）

4.5.4.3 SOC の運用体制はどのようなものか

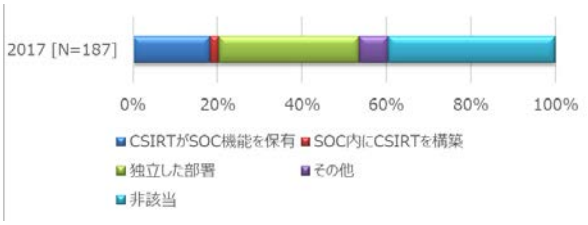
4.5.4.3SOC の運用体制はどのようなものか		
#	項目	回答数
a	自組織で運用している	31
b	グループ会社に外注している	18
c	他社に外注している	53
d	その他	10
e	非該当(構築・運用していない)	75



（複数回答なし 2017 [N = 187]）

4.5.4.4 SOC と CSIRT の関係はどのような関係か

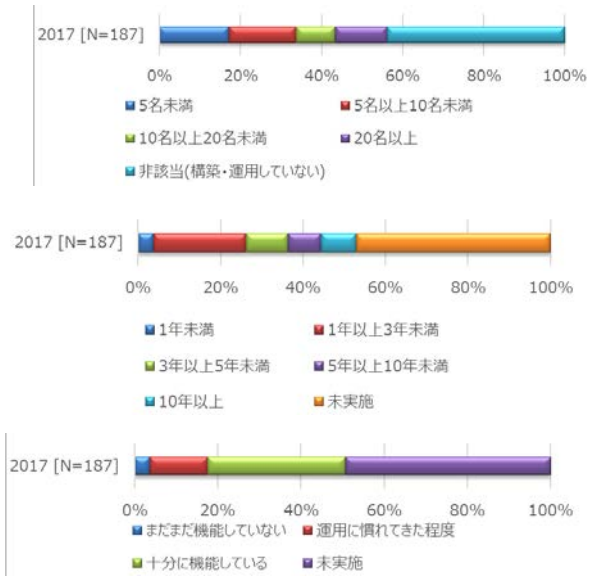
4.5.4.4SOC と CSIRT の関係はどのような関係か		
#	項目	回答数
a	CSIRT が SOC 機能を有している	34
b	SOC 内に CSIRT を構築している	4
c	それぞれが独立した部署として存在しており、連携している	62
d	その他	13
e	非該当(構築・運用していない)	74



（複数回答なし 2017 [N = 187]）

4.5.4.5 SOC の構成人数・継続年数・熟練度

4.5.4.5SOC の構成人数・継続年数・熟練度		
#	項目	回答数
<構成人数>		
a	5 名未満	32
b	5 名以上 10 名未満	31
c	10 名以上 20 名未満	18
d	20 名以上	24
e	非該当(構築・運用していない)	82
<運用年数>		
a	1 年未満	7
b	1 年以上 3 年未満	42
c	3 年以上 5 年未満	19
d	5 年以上 10 年未満	15
e	10 年以上	16
f	未実施	88
<熟練度>		
a	まだまだ機能していない	7
b	運用に慣れてきた程度	26
c	十分に機能している	62
d	未実施	92

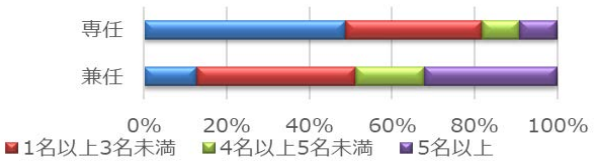


（複数回答なし 2017 [N = 187]）

5. CSIRT の活動(提供サービス)：事後対応(未実施以外は、複数回答可)

5.1 事後対応に関与している CSIRT メンバーの人数

5.1 事後対応に関与している CSIRT メンバーの人数		
#	項目	回答数
<専任>		
a	0 名	24
b	1 名以上 3 名未満	72
c	4 名以上 5 名未満	31
d	5 名以上実施している	60
<兼任>		
a	0 名	91
b	1 名以上 3 名未満	62
c	4 名以上 5 名未満	17
d	5 名以上実施している	17



（複数回答なし 2017 [N = 187]）

5-2 ~ 5-7 は以下の実施単位を指定して回答する。

ここでは、項目ごとのグラフのサマリを記載し、詳細については、サービスごとに表にて記載する。

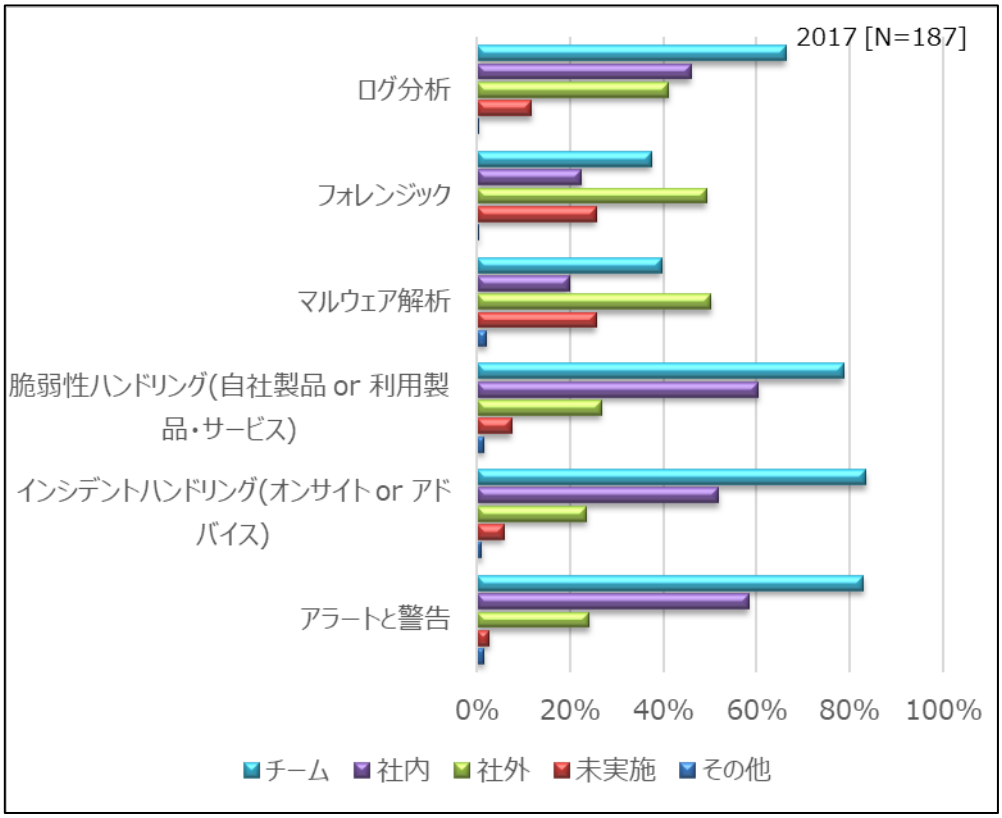
チーム：チーム自身で実施

社内：社内の他部署に依頼

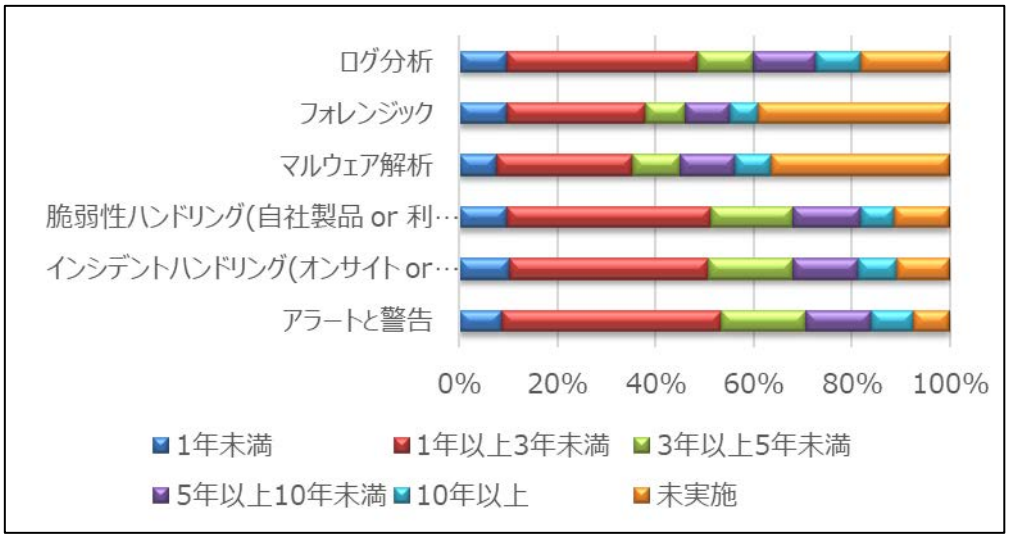
社外：社外に依頼(含む、委託)

未実施：複数回答はしないこと

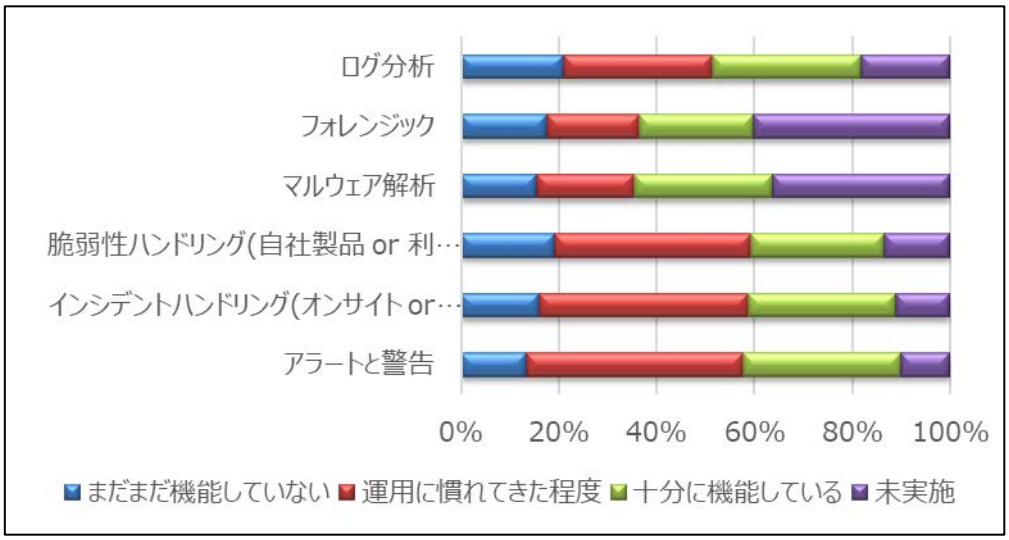
その他：上記以外



[図 2.5 a 実施単位について]



[図 2.5 b 運用年数について]



[図 2.5 c 運用年数について]

5.2 アラートと警告

5.2 アラートと警告(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	155
b	社内	109
c	社外	45
d	未実施	5
e	その他	3
<運用年数>		
a	1 年未満	16
b	1 年以上 3 年未満	84
c	3 年以上 5 年未満	32
d	5 年以上 10 年未満	25
e	10 年以上	16
f	未実施	14
<熟練度>		
a	まだまだ機能していない	25
b	運用に慣れてきた程度	83
c	十分に機能している	60
d	未実施	19

5.3 インシデントハンドリング(オンサイト or アドバイス)

オンサイトでのインシデント対応支援、遠隔からのインシデント対応支援、インシデント対応調整のいずれかを実施する。

5.3 インシデントハンドリング(オンサイト or アドバイス) (未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	156
b	社内	97
c	社外	44
d	未実施	11
e	その他	2
<運用年数>		
a	1 年未満	19
b	1 年以上 3 年未満	76
c	3 年以上 5 年未満	32
d	5 年以上 10 年未満	25
e	10 年以上	15
f	未実施	20
<熟練度>		
a	まだまだ機能していない	30
b	運用に慣れてきた程度	80
c	十分に機能している	56
d	未実施	21

5.4 脆弱性ハンドリング(自社製品 or 利用製品・サービス)

脆弱性に関する情報や報告を受領し、脆弱性の要因や影響範囲の調査、脆弱性の検知と対応策および軽減策に関する対応を実施する。

5.4 脆弱性ハンドリング(自社製品 or 利用製品・サービス) (未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	147
b	社内	113
c	社外	50
d	未実施	14
e	その他	3
<運用年数>		
a	1 年未満	18
b	1 年以上 3 年未満	78
c	3 年以上 5 年未満	31
d	5 年以上 10 年未満	26
e	10 年以上	13
f	未実施	21
<熟練度>		
a	まだまだ機能していない	36
b	運用に慣れてきた程度	75
c	十分に機能している	51
d	未実施	25

5.5 マルウエア解析

検知や通知されたマルウエアの動作解析などを実施する。

5.5 マルウエア解析(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	74
b	社内	37
c	社外	94
d	未実施	48
e	その他	4
<運用年数>		
a	1 年未満	14
b	1 年以上 3 年未満	52
c	3 年以上 5 年未満	18
d	5 年以上 10 年未満	21
e	10 年以上	14
f	未実施	68
<熟練度>		
a	まだまだ機能していない	29
b	運用に慣れてきた程度	37
c	十分に機能している	53
d	未実施	68

5.6 フォレンジック

インシデントが発生したときの証拠復旧や、情報漏洩などの証拠調査を実施する。

5.6 フォレンジック(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	70
b	社内	42
c	社外	92
d	未実施	48
e	その他	1
<運用年数>		
a	1 年未満	18
b	1 年以上 3 年未満	53
c	3 年以上 5 年未満	15
d	5 年以上 10 年未満	17
e	10 年以上	11
f	未実施	73
<熟練度>		
a	まだまだ機能していない	33
b	運用に慣れてきた程度	35
c	十分に機能している	44
d	未実施	75

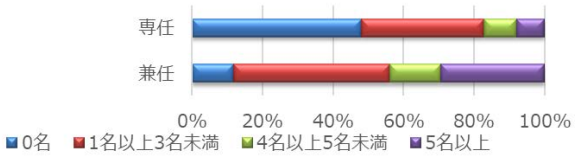
5.7 ログ分析

5.7 ログ分析(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	124
b	社内	86
c	社外	77
d	未実施	22
e	その他	1
<運用年数>		
a	1 年未満	18
b	1 年以上 3 年未満	73
c	3 年以上 5 年未満	21
d	5 年以上 10 年未満	24
e	10 年以上	17
f	未実施	34
<熟練度>		
a	まだまだ機能していない	39
b	運用に慣れてきた程度	57
c	十分に機能している	57
d	未実施	34

6.CSIRT の活動(提供サービス) ¨事前対応(未実施以外は、複数回答可)

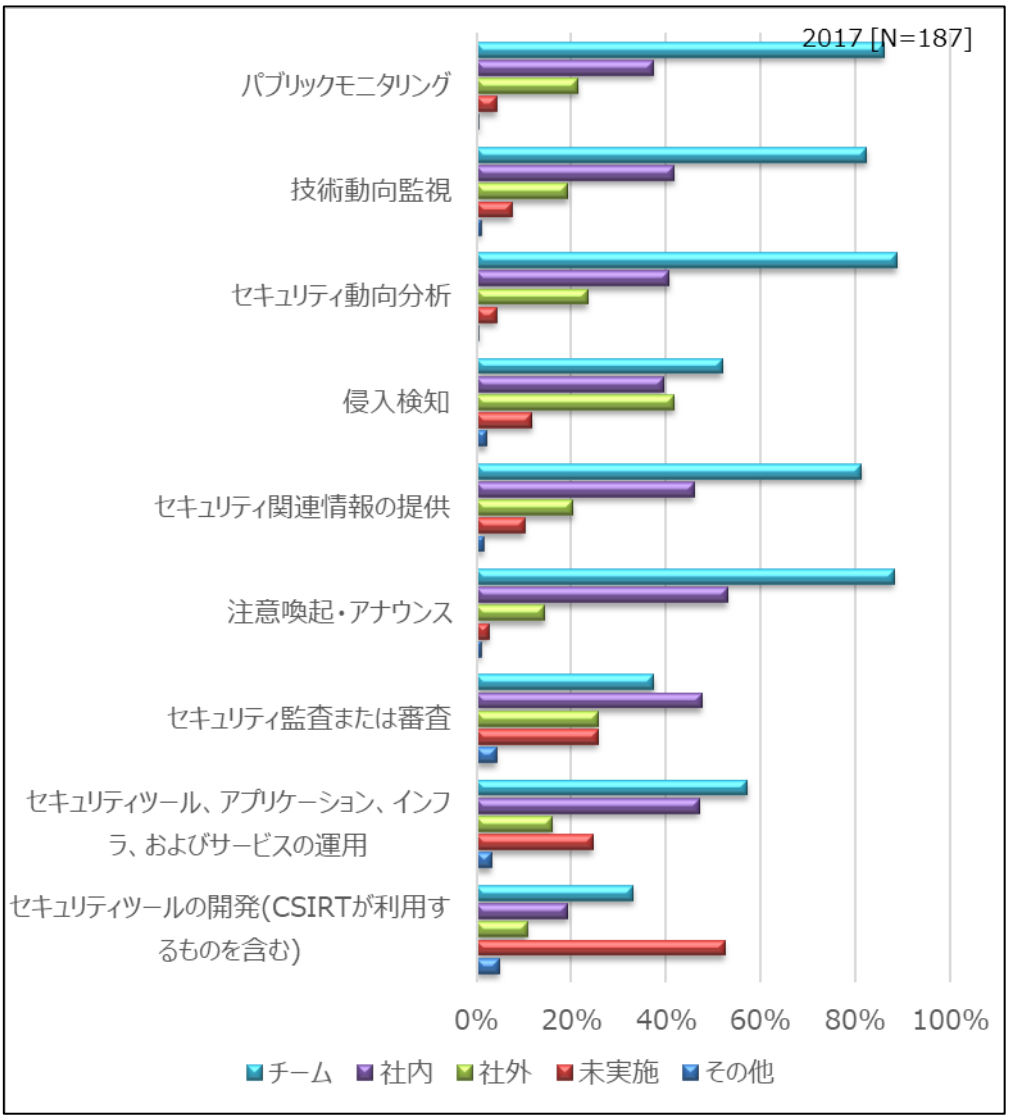
6.1 事前対応に関与している CSIRT メンバーの人数

6.1 事前対応に関与している CSIRT メンバーの人数		
#	項目	回答数
<専任>		
a	0 名	90
b	1 名以上 3 名未満	65
c	4 名以上 5 名未満	17
d	5 名以上実施している	15
<兼任>		
a	0 名	22
b	1 名以上 3 名未満	83
c	4 名以上 5 名未満	27
d	5 名以上実施している	55

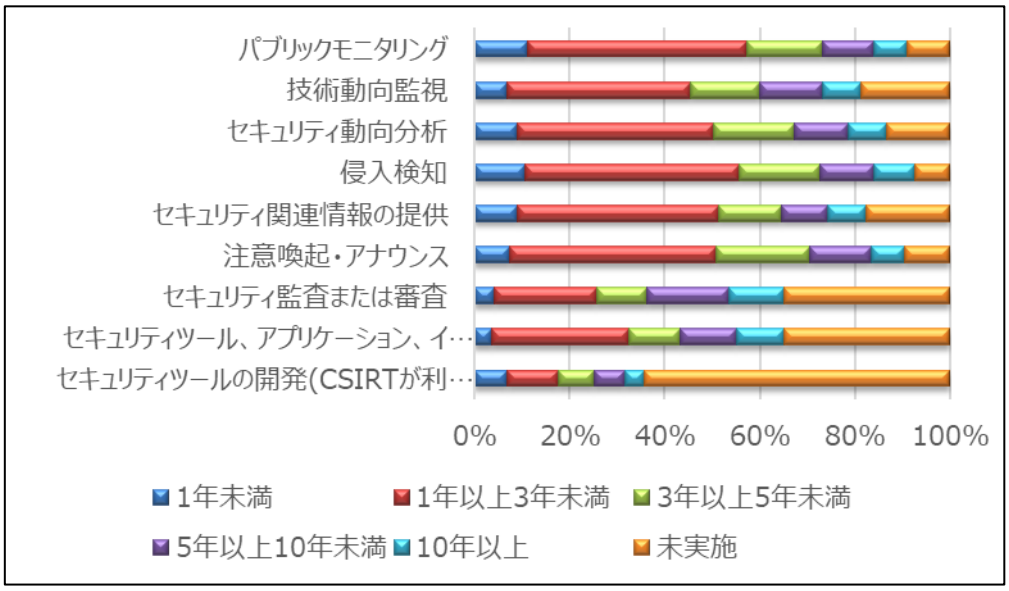


（複数回答なし 2017 [N = 187]）

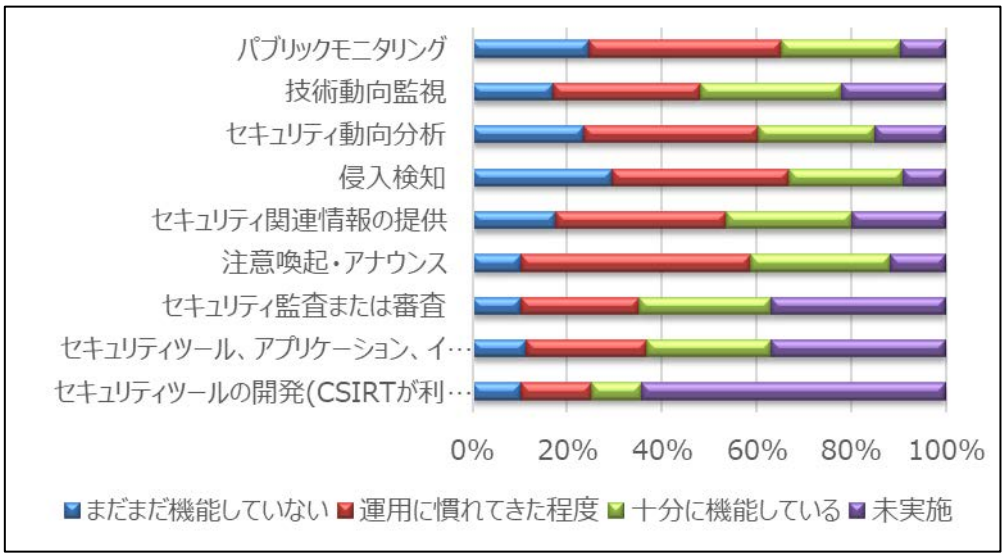
6-2 ~ 6-10 は以下の実施単位を指定して回答する。
ここでは、項目ごとのグラフのサマリを記載し、詳細については、サービスごとに表にて記載する。
チーム：チーム自身で実施
社内：社内の他部署に依頼
社外：社外に依頼(含む、委託)
未実施：複数回答はしないこと
その他：上記以外



[図 2.6 a 実施単位について]



[図 2.6 b 運用年数について]



[図 2.6 c 運用年数について]

6.2 パブリックモニタリング

セキュリティに関するメーリングリストやセキュリティ関連の Web サイト等をモニタリングし、情報を収集する。

6.2 パブリックモニタリング(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	161
b	社内	70
c	社外	40
d	未実施	8
e	その他	1
<運用年数>		
a	1 年未満	21
b	1 年以上 3 年未満	86
c	3 年以上 5 年未満	30
d	5 年以上 10 年未満	20
e	10 年以上	13
f	未実施	17
<熟練度>		
a	まだまだ機能していない	46
b	運用に慣れてきた程度	76
c	十分に機能している	47
d	未実施	18

6.3 技術動向監視

将来の脅威に備え、新しい技術開発に関する動向を監視・ウォッチする。

6.3 技術動向監視(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	154
b	社内	78
c	社外	36
d	未実施	14
e	その他	2
<運用年数>		
a	1 年未満	13
b	1 年以上 3 年未満	72
c	3 年以上 5 年未満	27
d	5 年以上 10 年未満	25
e	10 年以上	15
f	未実施	35
<熟練度>		
a	まだまだ機能していない	32
b	運用に慣れてきた程度	58
c	十分に機能している	56
d	未実施	41

6.4 セキュリティ動向分析

将来の脅威に備え、サイバー攻撃やガイドラインに関する動向を監視・ウォッチし、分析する。

6.4 セキュリティ動向分析(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	166
b	社内	76
c	社外	44
d	未実施	8
e	その他	1
<運用年数>		
a	1 年未満	17
b	1 年以上 3 年未満	77
c	3 年以上 5 年未満	32
d	5 年以上 10 年未満	21
e	10 年以上	15
f	未実施	25
<熟練度>		
a	まだまだ機能していない	44
b	運用に慣れてきた程度	69
c	十分に機能している	46
d	未実施	28

6.5 侵入検知

IDS ログのレビューと分析、定義した閾値に達しているイベントへの対応を行い、あらかじめ定義された連絡ルートに基づき、イベントの発生を通知し対処を促す。

6.5 侵入検知(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	97
b	社内	74
c	社外	78
d	未実施	22
e	その他	4
<運用年数>		
a	1 年未満	20
b	1 年以上 3 年未満	84
c	3 年以上 5 年未満	32
d	5 年以上 10 年未満	21
e	10 年以上	16
f	未実施	14
<熟練度>		
a	まだまだ機能していない	55
b	運用に慣れてきた程度	70
c	十分に機能している	45
d	未実施	17

6.6 セキュリティ関連情報の提供

セキュリティの向上に寄与する各種関連情報を提供する。

6.6 セキュリティ関連情報の提供(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	152
b	社内	86
c	社外	38
d	未実施	19
e	その他	3
<運用年数>		
a	1 年未満	17
b	1 年以上 3 年未満	79
c	3 年以上 5 年未満	25
d	5 年以上 10 年未満	18
e	10 年以上	15
f	未実施	33
<熟練度>		
a	まだまだ機能していない	44
b	運用に慣れてきた程度	69
c	十分に機能している	46
d	未実施	28

6.7 注意喚起・アナウンス

新たに発見された脆弱性に対する情報や流行している攻撃手法、技術的動向などを広報や通知する。

6.7 注意喚起・アナウンス(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	165
b	社内	99
c	社外	27
d	未実施	5
e	その他	2
<運用年数>		
a	1 年未満	14
b	1 年以上 3 年未満	81
c	3 年以上 5 年未満	37
d	5 年以上 10 年未満	24
e	10 年以上	13
f	未実施	18
<熟練度>		
a	まだまだ機能していない	19
b	運用に慣れてきた程度	91
c	十分に機能している	55
d	未実施	22

6.8 セキュリティ監査または審査

組織または該当する他の業界標準で定義された要件に基づき、組織のセキュリティ対策状況に対する監査または審査を実施する。

6.8 セキュリティ監査または審査(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	70
b	社内	89
c	社外	48
d	未実施	48
e	その他	8
<運用年数>		
a	1 年未満	8
b	1 年以上 3 年未満	40
c	3 年以上 5 年未満	20
d	5 年以上 10 年未満	32
e	10 年以上	22
f	未実施	65
<熟練度>		
a	まだまだ機能していない	19
b	運用に慣れてきた程度	47
c	十分に機能している	52
d	未実施	69

6.9 セキュリティツール、アプリケーション、インフラ、およびサービスの運用

CSIRT 自身が使用するツール、アプリケーション、および一般的なコンピュータ設備を安全に設定・保守する方法に関する適切なガイダンスを提示する。

6.9 セキュリティツール、アプリケーション、インフラ、およびサービスの運用(未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	107
b	社内	88
c	社外	30
d	未実施	46
e	その他	6
<運用年数>		
a	1 年未満	7
b	1 年以上 3 年未満	54
c	3 年以上 5 年未満	20
d	5 年以上 10 年未満	22
e	10 年以上	19
f	未実施	65
<熟練度>		
a	まだまだ機能していない	21
b	運用に慣れてきた程度	48
c	十分に機能している	49
d	未実施	69

6.10 セキュリティツールの開発(CSIRT が利用するものを含む)

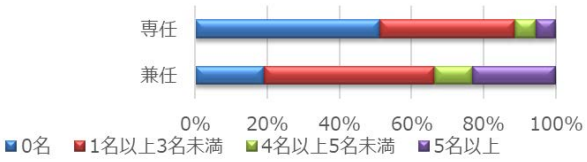
CSIRT 活動を推進する上で必要となるツールを開発する。

6.10 セキュリティツールの開発(CSIRT が利用するものを含む) (未実施以外は、複数回答可)		
#	項目	回答数
<実施単位>		
a	チーム	62
b	社内	36
c	社外	20
d	未実施	98
e	その他	9
<運用年数>		
a	1 年未満	13
b	1 年以上 3 年未満	20
c	3 年以上 5 年未満	14
d	5 年以上 10 年未満	12
e	10 年以上	8
f	未実施	120
<熟練度>		
a	まだまだ機能していない	19
b	運用に慣れてきた程度	28
c	十分に機能している	20
d	未実施	120

7.CSIRT の活動(提供サービス)：セキュリティ品質管理(未実施以外は、複数回答可)

7.1 セキュリティ品質管理に関与している CSIRT メンバーの人数

7.1 セキュリティ品質管理に関与している CSIRT メンバーの人数		
#	項目	回答数
<専任>		
a	0 名	96
b	1 名以上 3 名未満	70
c	4 名以上 5 名未満	11
d	5 名以上実施している	10
<兼任>		
a	0 名	36
b	1 名以上 3 名未満	88
c	4 名以上 5 名未満	20
d	5 名以上実施している	43



（複数回答なし 2017 [N = 187]）

7-2 ~ 7-8 は以下の実施単位を指定して回答する。

ここでは、項目ごとのグラフのサマリを記載し、詳細については、サービスごとに表にて記載する。

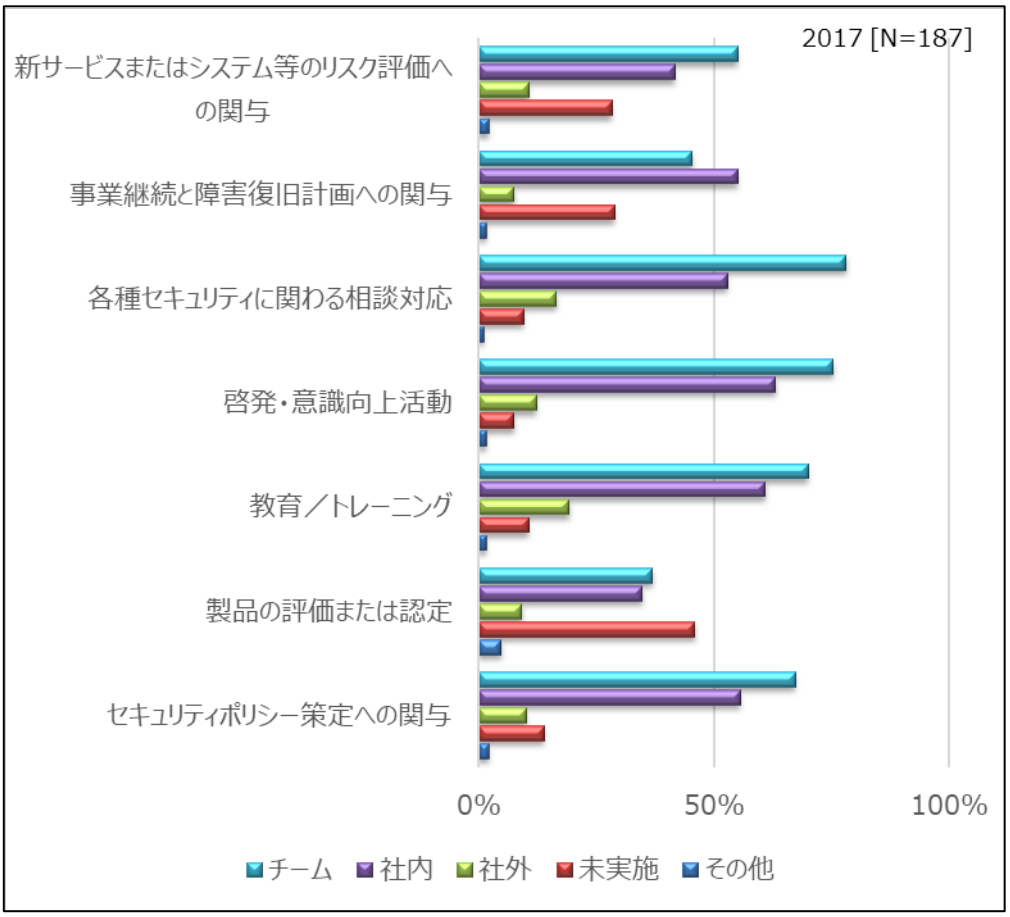
チーム：チーム自身で実施

社内：社内の他部署に依頼

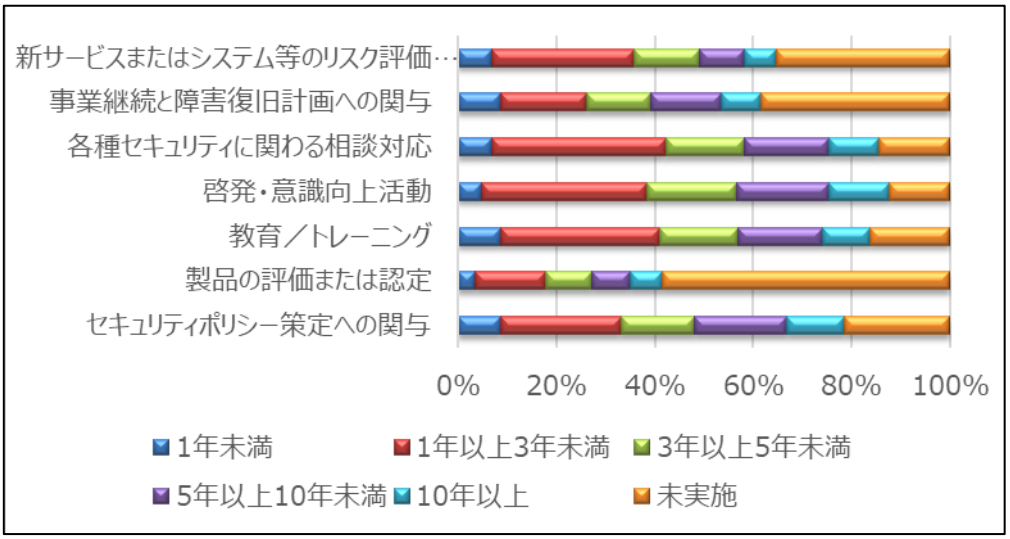
社外：社外に依頼(含む、委託)

未実施：複数回答はしないこと

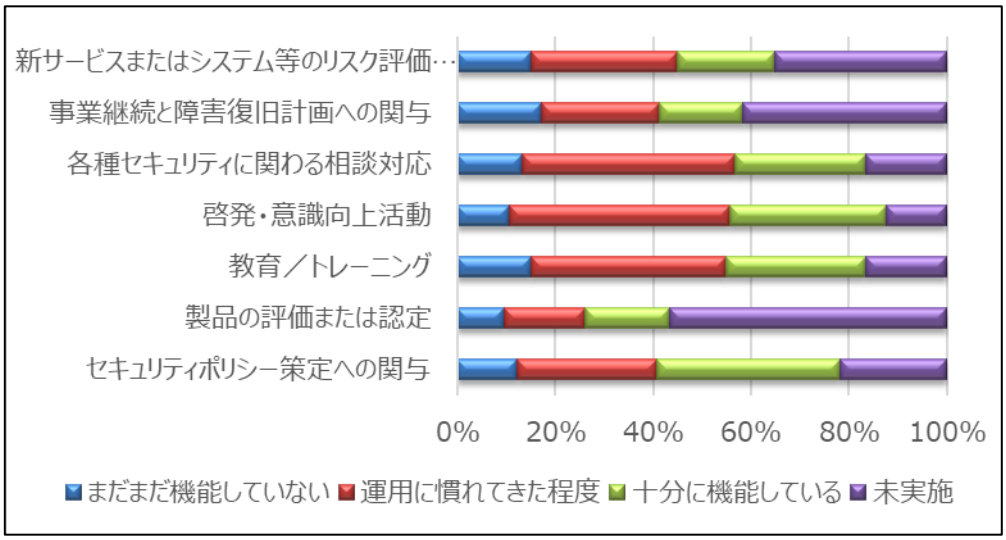
その他：上記以外



[図 2.7 a 実施単位について]



[図 2.7 b 運用年数について]



[図 2.7 c 運用年数について]

7.2 新サービスまたはシステム等のリスク評価への関与

攻撃の脅威や情報資産に対するリスクの評価や評価を支援する。

7.2 新サービスまたはシステム等のリスク評価への関与		
#	項目	回答数
<実施単位>		
a	チーム	103
b	社内	78
c	社外	20
d	未実施	53
e	その他	4
<運用年数>		
a	1 年未満	13
b	1 年以上 3 年未満	54
c	3 年以上 5 年未満	25
d	5 年以上 10 年未満	17
e	10 年以上	12
f	未実施	66
<熟練度>		
a	まだまだ機能していない	28
b	運用に慣れてきた程度	56
c	十分に機能している	37
d	未実施	66

7.3 事業継続と障害復旧計画への関与

事業経営に深刻な影響をもたらすインシデントが発生する可能性を鑑み、大規模インシデントが発生した際に、事業を継続するための障害復旧計画を検討する。

7.3 事業継続と障害復旧計画への関与		
#	項目	回答数
<実施単位>		
a	チーム	85
b	社内	103
c	社外	14
d	未実施	54
e	その他	3
<運用年数>		
a	1 年未満	16
b	1 年以上 3 年未満	33
c	3 年以上 5 年未満	24
d	5 年以上 10 年未満	27
e	10 年以上	15
f	未実施	72
<熟練度>		
a	まだまだ機能していない	32
b	運用に慣れてきた程度	45
c	十分に機能している	32
d	未実施	78

7.4 各種セキュリティに関わる相談対応

サイバー攻撃の発生に備え、組織運営のために実施すべきセキュリティ対策などに関する助言や相談にのる。

7.4 各種セキュリティに関わる相談対応		
#	項目	回答数
<実施単位>		
a	チーム	146
b	社内	99
c	社外	31
d	未実施	18
e	その他	2
<運用年数>		
a	1 年未満	13
b	1 年以上 3 年未満	66
c	3 年以上 5 年未満	30
d	5 年以上 10 年未満	32
e	10 年以上	19
f	未実施	27
<熟練度>		
a	まだまだ機能していない	25
b	運用に慣れてきた程度	81
c	十分に機能している	50
d	未実施	31

7.5 啓発・意識向上活動

セキュリティの理解を高めることにより、日常業務を安全に遂行することを目的として、ガイドラインを提供する。

7.5 啓発・意識向上活動		
#	項目	回答数
<実施単位>		
a	チーム	141
b	社内	118
c	社外	23
d	未実施	14
e	その他	3
<運用年数>		
a	1 年未満	9
b	1 年以上 3 年未満	63
c	3 年以上 5 年未満	34
d	5 年以上 10 年未満	35
e	10 年以上	23
f	未実施	23
<熟練度>		
a	まだまだ機能していない	20
b	運用に慣れてきた程度	84
c	十分に機能している	60
d	未実施	23

7.6 教育／トレーニング

セミナー、ワークショップ、チュートリアルなどの形式で、セキュリティ関連情報を提供する。具体的なテーマには、セキュリティインシデントの防止・検知・対応に必要な情報の提供などを含む。

7.6 教育／トレーニング		
#	項目	回答数
<実施単位>		
a	チーム	131
b	社内	114
c	社外	36
d	未実施	20
e	その他	3
<運用年数>		
a	1 年未満	16
b	1 年以上 3 年未満	60
c	3 年以上 5 年未満	30
d	5 年以上 10 年未満	32
e	10 年以上	18
f	未実施	30
<熟練度>		
a	まだまだ機能していない	28
b	運用に慣れてきた程度	74
c	十分に機能している	53
d	未実施	31

7.7 製品の評価または認定

CSIRT または組織のセキュリティ要件に適合していることを保証するために、ツール、アプリケーション、その他のセキュリティサービスを対象に製品評価を実施する。

7.7 製品の評価または認定		
#	項目	回答数
<実施単位>		
a	チーム	69
b	社内	65
c	社外	17
d	未実施	86
e	その他	9
<運用年数>		
a	1 年未満	6
b	1 年以上 3 年未満	24
c	3 年以上 5 年未満	16
d	5 年以上 10 年未満	13
e	10 年以上	11
f	未実施	99
<熟練度>		
a	まだまだ機能していない	18
b	運用に慣れてきた程度	31
c	十分に機能している	32
d	未実施	106

7.8 セキュリティポリシー策定への関与

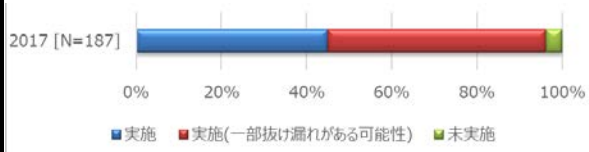
組織のセキュリティポリシーの策定や策定に関わる助言や相談にのる。

7.8 セキュリティポリシー策定への関与		
#	項目	回答数
<実施単位>		
a	チーム	126
b	社内	104
c	社外	19
d	未実施	26
e	その他	4
<運用年数>		
a	1 年未満	16
b	1 年以上 3 年未満	46
c	3 年以上 5 年未満	28
d	5 年以上 10 年未満	35
e	10 年以上	22
f	未実施	40
<熟練度>		
a	まだまだ機能していない	23
b	運用に慣れてきた程度	53
c	十分に機能している	70
d	未実施	41

8.その他

8.1.ツールについて

8.1.1.IT 資産の管理を組織的に実施しているか

8.1.1IT 資産の管理を組織的に実施しているか			
#	項目	回答数	
a	実施しており、インシデント対応の際には迅速に棚卸が行える	84	
b	実施してはいるが、一部抜け漏れがある可能性がある	96	
c	実施していない	7	

（複数回答なし 2017 [N = 187]）

8.1.2 インシデント対応を追跡するためトラッキングシステムやワークフローを導入しているか

8.1.2 インシデント対応を追跡するためトラッキングシステムやワークフローを導入しているか			
#	項目	回答数	
a	実施しており、インシデント対応の際には迅速に棚卸が行える	65	
b	実施してはいるが、一部抜け漏れがある可能性がある	33	
c	実施していない	89	

（複数回答なし 2017 [N = 187]）

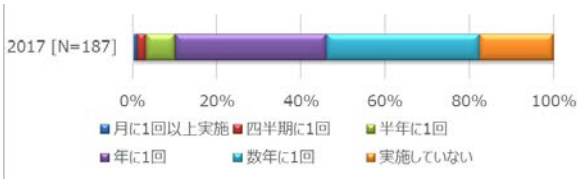
8.1.3 セキュリティ関連情報（インディケータ情報も含む）を集約するプラットフォームを導入しているか

8.1.3 セキュリティ関連情報(インディケータ情報も含む)を集約するプラットフォームを導入しているか			
#	項目	回答数	
a	実施しており、インシデント対応の際には迅速に棚卸が行える	57	
b	実施してはいるが、一部抜け漏れがある可能性がある	24	
c	実施していない	106	

（複数回答なし 2017 [N = 187]）

8.2 体制やルールの見直し

8.2.1 定期的にサービスの提供範囲の見直しを実施しているか

8.2.1 定期的にサービスの提供範囲の見直しを実施しているか			
#	項目	回答数	
a	月に 1 回以上実施	2	
b	四半期に 1 回	4	
c	半年に 1 回	13	
d	年に 1 回	67	
e	数年に 1 回	68	
f	実施していない	33	（複数回答なし 2017 [N = 187]）

8.2.2 定期的に連絡体制図（メールアドレスや電話番号等）の見直しを実施しているか

8.2.2 定期的に連絡体制図(メールアドレスや電話番号等)の見直しを実施しているか			
#	項目	回答数	
a	月に 1 回以上実施	13	
b	四半期に 1 回	18	
c	半年に 1 回	27	
d	年に 1 回	70	
e	数年に 1 回	38	
f	実施していない	21	（複数回答なし 2017 [N = 187]）

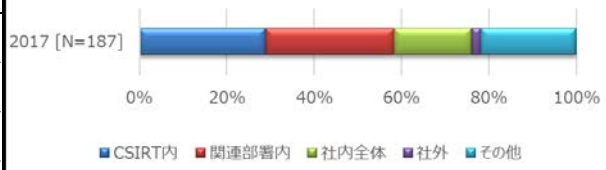
8.3 活動報告

8.3.1 定期的にレポートは発行しているか

8.3.1 定期的にレポートは発行しているか			
#	項目	回答数	
a	月に 1 回以上実施	38	
b	四半期に 1 回	38	
c	半年に 1 回	18	
d	年に 1 回	32	
e	数年に 1 回	3	
f	実施していない	58	（複数回答なし 2017 [N = 187]）

8.3.2 レポートの公開範囲

8.3.2 レポートの公開範囲		
#	項目	回答数
a	CSIRT 内	54
b	関連部署内	55
c	社内全体	33
d	社外(Web ページなど)	4
e	その他	41



（複数回答なし 2017 [N = 187]）