NTT DATA
Trusted Global Innovator

令和３年度サイバー・フィジカル・セキュリティ対策促進事業
（企業におけるサプライチェーンのサイバーセキュリティ対策に関する調査）

調査報告書

2022年３月
株式会社NTTデータ経営研究所

目次

１．調査実施の背景、目的

1．調査実施の背景、目的
背景、目的

【サプライチェーン全体でのサイバーセキュリティ対策の必要性】

- 近年、中小企業を対象とするサイバー攻撃が多く観測されており、また、サイバー攻撃の影響が、攻撃を直接受けた企業への影響にとどまらず、それらの企業とサプライチェーンを共有する大企業等にも影響を及ぼすケースが顕在化してきている
- こうした背景から、**取引先企業を含むサプライチェーンのサイバーセキュリティ対策は、自社組織のセキュリティ対策に並び重要な要素**となっている

【サプライチェーンのサイバーセキュリティ対策を進める上での課題】

- 取引先企業へのサイバーセキュリティ対策に係る要請は、費用負担に係る問題や、独占禁止法等の法・規制等への抵触への懸念からハードルが高いとの見解もあり、これが対策を推し進める上での課題となっている可能性もある
- サイバー攻撃を受けた場合に、被害状況や攻撃に関する情報が共有されることにより、サイバー攻撃に関する理解が進み、実効性のある対策が講じられることで、サプライチェーン全体のサイバーセキュリティ対策の向上が期待される。他方で、**効果的な情報共有の時期、内容、手段について十分な共通認識は得られていない**

- 大企業・中堅企業から取引先企業へのセキュリティ対策要請の実態、課題、優良事例等や、サイバー攻撃の被害情報の共有のあり方について、調査（アンケート調査及びヒアリング調査）を行うことにより、**各企業におけるサプライチェーンのサイバーセキュリティ対策を促進するために、企業、国、民間団体等が講ずべき措置の方向性を明らかにする**

1．調査実施の背景、目的
調査の実施内容

- 前ページに示した背景、目的を踏まえ、企業におけるサプライチェーンのサイバーセキュリティ対策の実態、課題、優良事例を把握・分析するために、幅広い業種の大企業・中堅企業を対象とした「アンケート調査」を実施
- また「アンケート調査」で確認された優良事例について、詳細を確認するための「ヒアリング調査」を実施
- これら結果を分析のうえ、サプライチェーンのサイバーセキュリティの確保に関して、「広く普及させるべき取組の優良事例」、「企業における情報共有の認識、今後の在り方」、及び「企業、国、民間団体等が講ずべき措置の方向性」をとりまとめた

調査の実施概要

調査項目	実施概要
アンケート調査	● 幅広い業種の大企業・中堅企業を対象に、サプライチェーンのサイバーセキュリティ対策にかかるアンケート調査を実施（回答数1,878件） ● サプライチェーンに関連するサイバー攻撃被害、取引先等への要請、情報収集・共有等の課題や、支援制度の利用等取組みの実態を調査
ヒアリング調査	● 幅広い業種の大企業・中堅企業（11社）を対象に、インタビュー調査を実施 ● 取引先等への要請等サプライチェーンのサイバーセキュリティ対策の具体事例、国、自治体、公的機関等への具体的な要請内容等を調査
優良事例、課題のとりまとめ及び、今後の対応措置の検討	● アンケート調査及びヒアリング調査の結果から、優良事例や今後の課題、企業、国、民間団体等が講ずべき措置の方向性を整理

２．アンケート調査

2．アンケート調査
調査概要

- 幅広い業種の大企業・中堅企業9,800社を対象に、サプライチェーンのセキュリティ対策にかかるアンケート調査（Web及び、メール）を実施し、1,878社より回答を得た

実施概要

項目	内容
対象企業の選定	● 商用データベース(東洋経済新報社) より、我が国の大企業・中堅企業(中小企業基本法の定義する中小企業者及び小規模企業者を除く企業)9,800社を抽出
配布・回収方法	● 配布：9,800社へ郵送 ● 回収：専用のWebサイトまたはメール
回収件数	● 1,878社（回答率:19.2%） （Web:1778件、メール100件）
実施スケジュール	(2022年) 1月6日:アンケート依頼状送付 1月14日:御礼状兼催促はがき送付 1月28日：アンケート回収〆切

アンケート調査項目の概要

No	分類	内容
-	属性情報	● 業種、従業員数、売上高
1	攻撃被害	● 取引先等※を経由した攻撃被害の経験の有無、内容
2	取引先等への要請	● 取引先等に対するセキュリティ対策の要請や取決めの内容 ● 取引先等への支援の実施有無、内容 ● 取引先等への要請の実施主体(部門) ● 取引先等へ要請を行ううえでの課題
3	情報収集・共有、対外公表	● 取引先等が攻撃をうけた場合の対応 ● 情報収集及び取引先等との情報共有 ● サイバー攻撃被害の対外公表
4	支援制度の利用、国等への要請	● 各種支援制度の認知、利活用の実態 ● 国、自治体、公的機関等に求める施策、取組み

※ 取引先等の類型として、「仕入・外注・委託先等の取引先」「グループ会社」「海外拠点」の３つに分類し、それぞれに対して同様の設問を設定

2．アンケート調査
調査結果・・・１．攻撃被害（①仕入・外注・委託先等の取引先）

- 仕入・外注・委託先等の取引先を経由したサイバー攻撃被害の経験の内容として、「Emotet」、「ランサムウェア」、「ファイル転送サービスの侵害」や「ホームページの改ざん」等があげられた

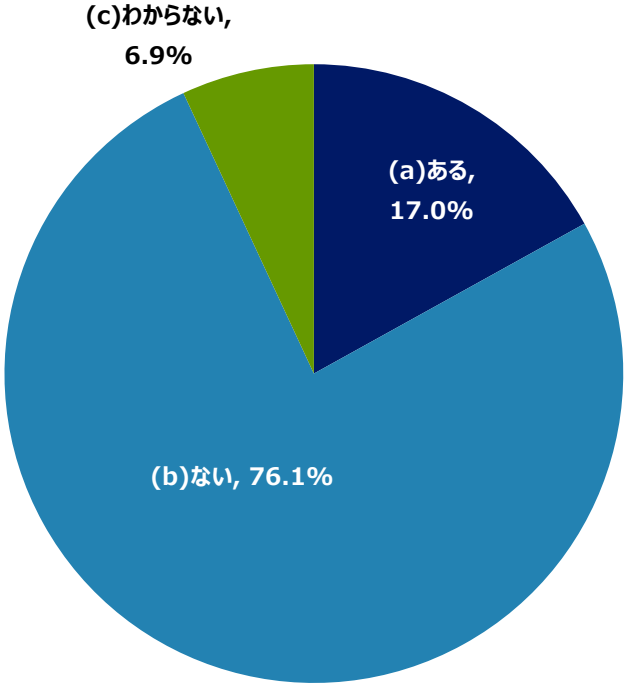
取引先等を経由したサイバー攻撃被害の主な内容 ＜①仕入・外注・委託先等の取引先＞

分類	内容
Emotet	● 取引先がEmotetに感染し、不正なメールを受信
ランサムウェア	● 取引先がランサムウェアに感染し、自社関連情報が暗号化／外部漏洩 ● 取引先がランサムウェアに感染、業務停止し、自社業務に影響
不正アクセス	● 取引先のシステムが不正アクセスをうけ、自社関連の情報が漏洩
DDoS攻撃	● 委託先のシステムや利用するクラウドサービスがDDoS攻撃を受け、自社業務に影響
その他	● 取引先と情報共有を行うために利用するツール（ファイル転送サービス）が侵害を受け、情報が流出 ● 取引先のホームページの改ざんによる、不正サイトへの誘導、自社業務への影響 ● 取引先が提供する電子決済サービスの悪用による顧客口座の不正送金　等

取引先等を経由したサイバー攻撃被害の経験 ＜①仕入・外注・委託先等の取引先＞

➢ 過去に取引先等がサイバー攻撃の被害を受け、それが貴社に及んだ経験がありますか（仕入・外注・委託先等の取引先）

(N=1876)



※「仕入・外注・委託先等の取引先を有していない」回答先を除く

2．アンケート調査
調査結果･･･１．攻撃被害（②グループ会社）

- グループ会社を経由したサイバー攻撃被害の経験の内容として、仕入・外注・委託先等と同様「Emotet」や「ランサムウェア」が多くあげられた。グループ会社の特徴として、「ビジネスメール詐欺」や、「VPNの脆弱性を利用したネットワークへの侵害」等が見られた

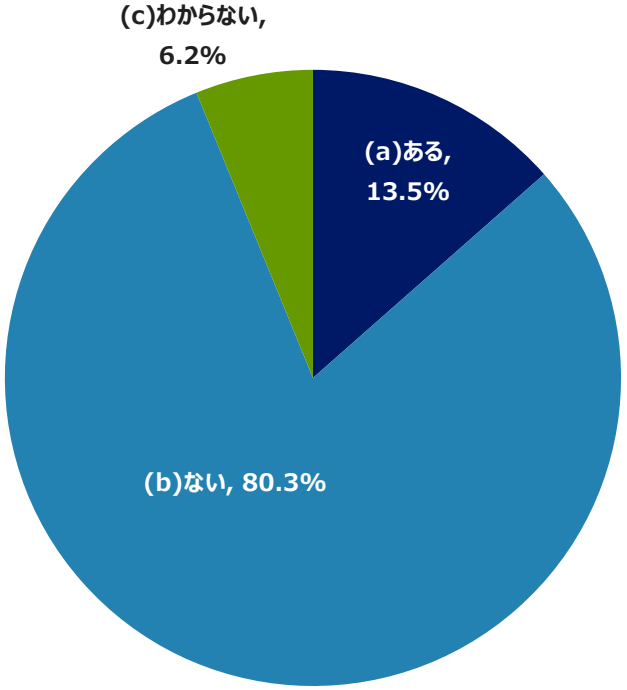
取引先等を経由したサイバー攻撃被害の主な内容 ＜②グループ会社＞

分類	内容
Emotet	● グループ会社がEmotetに感染し、不正なメールを受信
ランサムウェア	● グループ会社がランサムウェアに感染し、自社関連情報が暗号化／外部漏洩 ● グループ会社がランサムウェアに感染、業務停止し、自社業務に影響
不正アクセス	● グループ会社のシステムが不正アクセスをうけ、自社関連の情報が漏洩 ● グループ会社がVPNの脆弱性をついた不正アクセスによりネットワーク侵害をうけ情報が漏洩
ビジネスメール詐欺	● グループ会社を装い金銭を要求する詐欺メールを受信
その他	● グループ会社と情報共有を行うために利用するツール（ファイル転送サービス）が侵害を受け、情報が流出 ● グループ会社のホームページの改ざんによる、不正サイトへの誘導、自社業務への影響

取引先等を経由したサイバー攻撃被害の経験 ＜②グループ会社＞

➢ 過去に取引先等がサイバー攻撃の被害を受け、それが貴社に及んだ経験がありますか（グループ会社）

(N=1718)



※「グループ会社を有していない」回答先を除く

2．アンケート調査
調査結果･･･１．攻撃被害（③海外拠点）

- グループ会社を経由したサイバー攻撃被害の経験の内容として、グループ会社と同様に、「Emotet」や「ランサムウェア」に加え、「ビジネスメール詐欺」や「VPNの脆弱性を利用したネットワークへの侵害」が多くあげられた

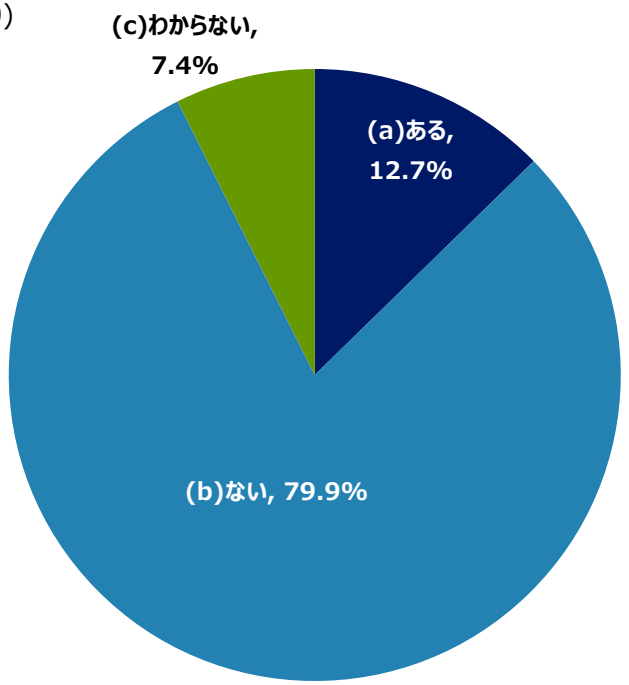
取引先等を経由したサイバー攻撃被害の主な内容＜③海外拠点＞

分類	内容
Emotet	● 海外拠点がEmotetに感染し、不正なメールを受信
ランサムウェア	● 海外拠点がランサムウェアに感染し、自社関連情報が暗号化／外部漏洩 ● 海外拠点がランサムウェアに感染、業務停止し、自社業務に影響
不正アクセス	● 海外拠点のシステムが不正アクセスをうけ、自社関連の情報が漏洩 ● 海外拠点がVPNの脆弱性をついた不正アクセスによりネットワーク侵害をうけ情報が漏洩
ビジネスメール詐欺	● 海外拠点を装い金銭を要求する詐欺メールを受信

取引先等を経由したサイバー攻撃被害の経験＜③海外拠点＞

➢ 過去に取引先等がサイバー攻撃の被害を受け、それが貴社に及んだ経験がありますか（海外拠点）

(N=1190)



※「海外拠点を有していない」回答先を除く

2．アンケート調査

調査結果･･･2．取引先等への要請（取引先等に対するセキュリティの要求/取決め ①仕入・外注・委託先等の取引先）

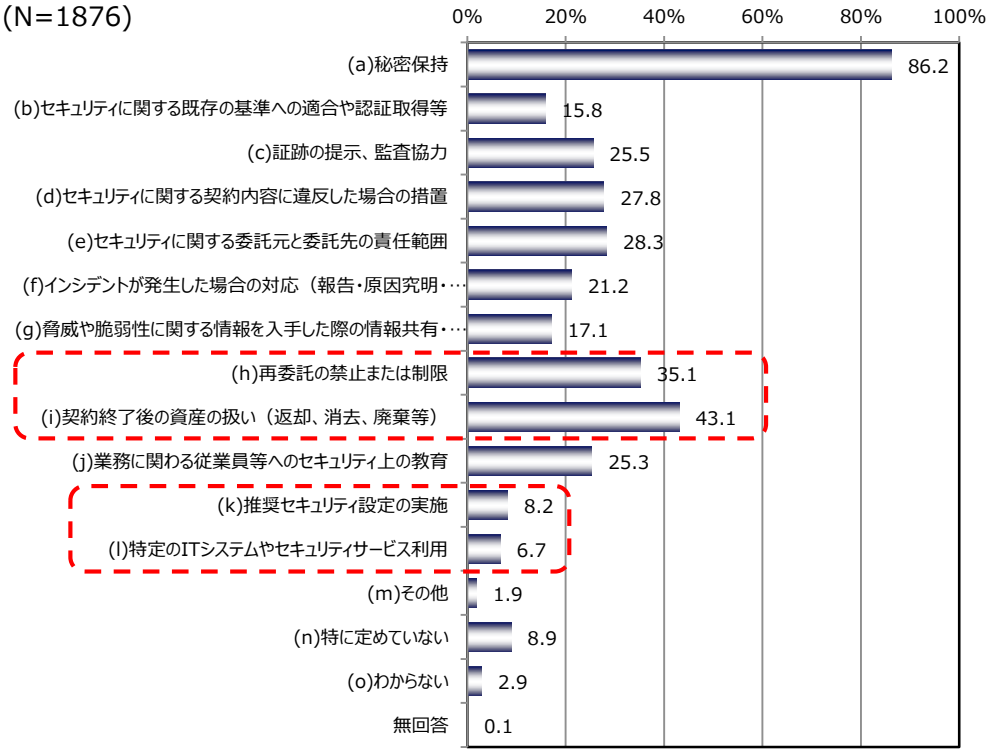
- 仕入・外注・委託先等の取引先への要請について、一般的となりつつある「秘密保持」を求めるほか、「推奨セキュリティ設定の実施」「特定のITシステムやセキュリティサービス利用」「国際セキュリティ認証(SOC2/SOC3)」が挙げられたほか、「第三者が提供するアセスメントサービス」を利用する取組みも見られた

セキュリティの要求/取決めの内容（取組事例）<①仕入・外注・委託先等の取引先>

分類	内容
(b) セキュリティに関する既存の基準への適合や認証取得等	● 自社で定めるセキュリティ基準・チェックシート ● Pマーク、ISMS ● クラウドサービスセキュリティ管理策 ● SOC2/SOC3（監査法人によるセキュリティ等の内部統制に係る保証報告書）
(f) インシデントが発生した場合の対応	● 契約にもとづき、報告、原因調査、再発防止を要請 ● 損害賠償について契約書等で規定
(k) 推奨セキュリティ設定の実施	● 以下の各種対策 ✓ ウイルス対策ソフトの導入/適時の更新、セキュリティパッチの適用、アクセス管理、端末画面のロック、暗号化通信、パスワードの定期的な再設定、記憶媒体の使用や持ち出しの制限 等 ● リスクに応じ、PCやVDI環境の貸与
(l) 特定のITシステムやセキュリティサービス利用	● 以下の各種対策 ✓ ウイルス対策ソフト、ファイル転送サービス、Web会議システム、クライアント運用管理ソフト 等 ● サイバーセキュリティお助け隊の利用勧奨
(m) その他	● 第三者が提供するアセスメントサービスを利用し、取引先のセキュリティリスクを評価（次ページ参照）

取引先等に対する、セキュリティの要求/取決め<①仕入・外注・委託先等の取引先>

➢ 取引先等に対し、セキュリティに関してどのような要求事項または取決めを定めていますか（仕入・外注・委託先等の取引先）



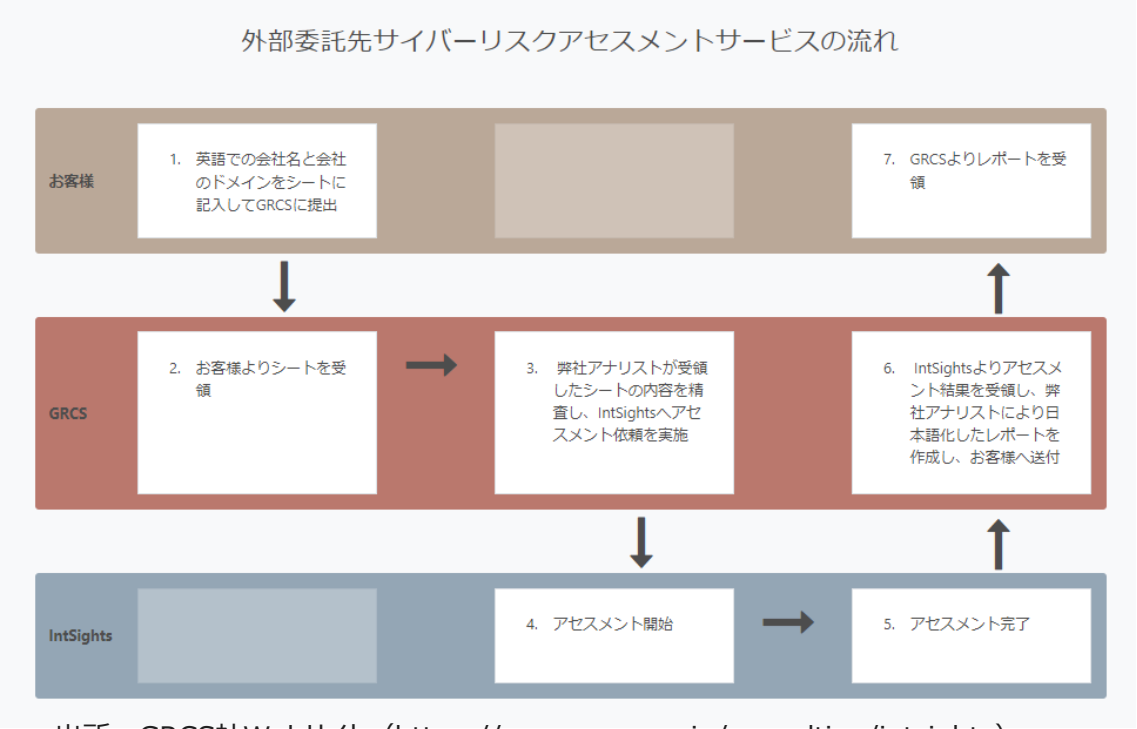
※「仕入・外注・委託先等の取引先を有していない」回答先を除く

（参考）第三者が提供するアセスメントサービス

- 取引先やグループ会社等に関し、当該企業からの情報漏洩の状況やサイバー攻撃の標的になっているか等を調査し、リスクスコアを提供するサービスが提供されており、取引先等のアセスメントに、こうしたサービスを活用する企業が見られた

事例：GRCS社が提供する外部委託先サイバーリスクアセスメントサービス

➢ 取引先やグループ会社等に関する情報漏洩や、サイバー攻撃の標的になっているかなどを調査し、その結果をリスクスコア付きのレポートとして出力



出所：GRCS社Webサイト（https://www.grcs.co.jp/consulting/intsights）

2．アンケート調査
調査結果･･･2．取引先等への要請（取引先等に対するセキュリティの要求/取決め ②グループ会社）

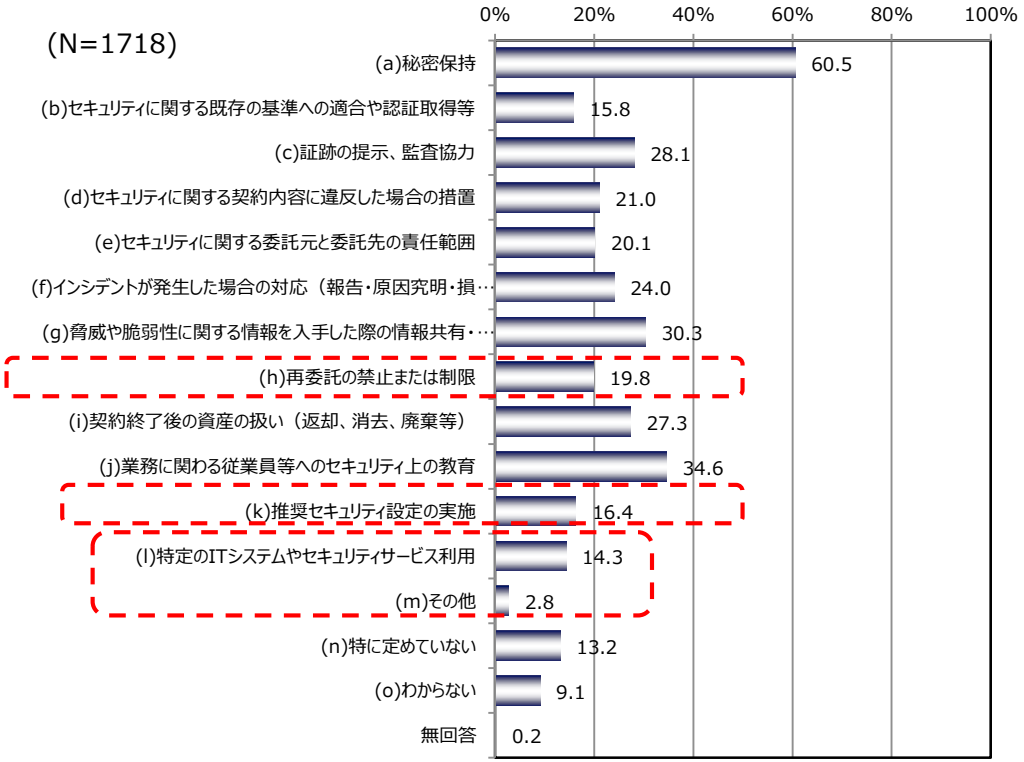
- グループ会社への要請について、グループ会社共有のポリシーを適用し、「脅威情報等の共有」「推奨セキュリティ設定の実施」「特定のITシステムやセキュリティサービス利用」を定めているケースが多く見られた

セキュリティの要求/取決めの内容（取組事例）<②グループ会社>

分類	内容
(b) セキュリティに関する既存の基準への適合や認証取得等	● ①仕入・外注・委託先等の取引先と同様の事例 ● グループ共通のセキュリティガイドラインへの準拠 ● 米国NISTのセキュリティフレームワークへの準拠
(f) インシデントが発生した場合の対応	● グループ全体で定められたインシデント対応規定等にもとづき、報告、原因調査、再発防止を要請
(k) 推奨セキュリティ設定の実施	● ①仕入・外注・委託先等の取引先と同様の事例 ● Webフィルタリング ● グループ共通のポリシーの適用
(l) 特定のITシステムやセキュリティサービス利用	● 自社の情報教育サービスのグループ会社への提供
(m) その他	● 自社の規程、基準、IT基盤、運用をグループ会社に展開

取引先等に対する、セキュリティの要求/取決め<②グループ会社>

➢ 取引先等に対し、セキュリティに関してどのような要求事項または取決めを定めていますか（グループ会社）



※「グループ会社を有していない」回答先を除く

2．アンケート調査
調査結果･･･2．取引先等への要請（取引先等に対するセキュリティの要求/取決め ③海外拠点）

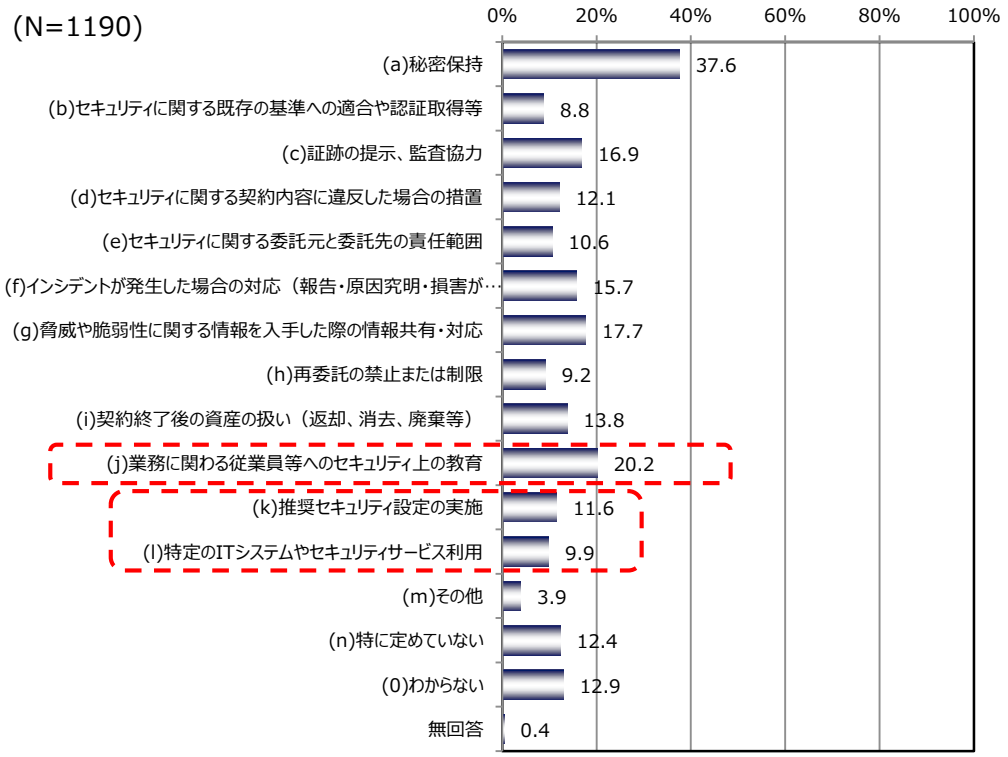
- 海外拠点への要請について、国内と同じシステムを利用できない場合には、同等のセキュリティ基準を満たすシステムの利用や、グループ共通ポリシーをベースに現地事情に合わせた対策を適用するケースが見られた

セキュリティの要求/取決めの内容（取組事例）＜③海外拠点＞

分類	内容
(b) セキュリティに関する既存の基準への適合や認証取得等	● 自社で定めたグローバルセキュリティポリシーの適用 ● 国内と同じシステムを利用できない場合、同等のセキュリティ基準を満たすシステムを利用
(f) インシデントが発生した場合の対応	● インシデント対応規定等にもとづき、報告、原因調査、再発防止を要請
(k) 推奨セキュリティ設定の実施	● グループ共通のポリシーに基づき基本的なルール・手順は変更せず、実施手段・運用形態を、現地事情（法規制、IT・ビジネス環境等）を踏まえてローカライズして適用 ● 専用のリモート端末を使用し、国内で管理されている環境へリモートアクセスして業務を実施
(l) 特定のITシステムやセキュリティサービス利用	● 直接的なデータのやり取りは決められたシステム経由のみに制限
(m) その他	● 海外拠点とネットワークを接続しない

取引先等に対する、セキュリティの要求/取決め＜③海外拠点＞

➢ 取引先等に対し、セキュリティに関してどのような要求事項または取決めを定めていますか（海外拠点）



※「海外拠点を有していない」回答先を除く

2．アンケート調査

結果概要・・・2．取引先等への要請（取引先等に対する支援の実施 ①仕入・外注・委託先等の取引先／②グループ会社）

- いずれの取引先類型においても、「費用・備品の一部負担」、「教育の実施」に関連する回答が見られた
- 資本関係のない、仕入・外注・委託先等に対しては、監査やアンケートを通じた「対応状況確認」が行われており、グループ会社、海外拠点に対しては、「稼働提供」や「設備の提供」等の支援が多く見られた

取引先等への支援（取組事例）<①仕入・外注・委託先等の取引先>

分類	内容
費用・備品の一部負担	● セキュリティ強化を目的としたIT環境の整備費用の一部を負担 ● 協力会社同士で費用を分担 ● セキュリティ強化のための備品を貸与 ● 脆弱性診断に係る費用の負担と対応策の共有
教育の実施	● セキュリティ教育の実施 ● 着任時教育（e-Learning）の実施
対応状況の確認	● セキュリティ強化を目的とした現地監査 ● 定期的なアンケート調査 ● セキュリティ水準を確認するための当社チェックシートによる実態調査

取引先等への支援（取組事例）<②グループ会社>

分類	内容
費用・備品の一部負担	● IT環境の整備費用の一部負担 ● セキュリティ製品の運用費用（SOC対応含）について、本体での負担
教育の実施	● セキュリティ教育資料の展開 ● グループ会社も対象にした、セキュリティ教育の本社主体での定期的な実施
脅威、脆弱性情報の共有	● 脅威、脆弱性情報の共有 ● 従業員等のセキュリティに関する注意喚起
稼働提供	● 共通で利用しているクラウドサービスにおける、必須・推奨に分けた設定の提示とサポートの実施 ● 新規案件に関する、本社からの情報セキュリティチェックの実施
設備の提供	● 従来から弊社が構築した環境を利用させており、個社インフラは無い ● インフラ、セキュリティ環境の提供

2．アンケート調査
結果概要･･･２．取引先等への要請（取引先等に対する支援の実施 ③海外拠点）

- （続き）

取引先等への支援（取組事例）<③海外拠点>

分類	内容
費用・備品の一部負担	● IT機器、社内情報ツール、ウイルス対策ソフト等の提供 ● インテリジェントルータや高度なウイルス対策ソフトを導入し、運用費用を本社で負担
教育の実施	● 海外現地法人における経営層のセキュリティー教育について、自社経営層に対する教育に包含して実施 ● 従業員向けのトレーニングプログラムの提供
脅威、脆弱性情報の共有	● 脅威、脆弱性情報の共有 ● 従業員へのセキュリティーに関する注意喚起
稼働提供	● セキュリティインシデント発生時における、調査・対処等の支援 ● 本社からの出向者派遣による現地スタッフの育成
設備の提供	● 情報資産の貸与および専用線（VPN）の提供

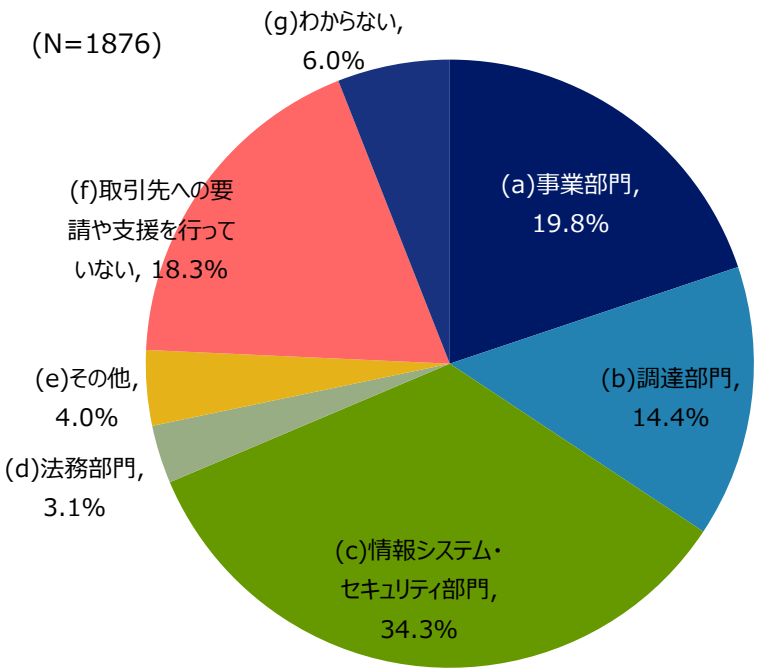
● 仕入れ・外注・委託先等への要請・支援を実施する部門として、IT全般またはサイバーセキュリティを管理する「情報システム・セキュリティ部門」、取引先との契約・折衝等を行う「事業部門」「調達部門」が多く見られた

取引先等への要請・支援を実施する部門と考え方 ＜①仕入・外注・委託先等の取引先＞

部門	内容
事業部門	● 取引先との折衝を一元的に担う部門であるため ● 取引先と契約を締結する主体であるため ● 業務上、取引先と最も頻繁にコミュニケーションをとる部門であるため
調達部門	● 取引先との折衝を担う事業部門が窓口となり、適時、情報システム・セキュリティ部門がサポートを実施 ● 調達部門が委託する内容に応じ、法務コンプライアンス、セキュリティ対策室の支援を得て対応
情報システム・セキュリティ部門	● IT全般の管理を行う部門であるため ● サイバーセキュリティを所管する部門であるため ● ITやサイバーセキュリティに関する知識を有する部門であるため ● 他に対応できる部門がないため
法務部門	● セキュリティや個人情報の管理を所管する部門であるため ● 外部委託管理を統括する部門であるため

取引先等への要請・支援を実施する部門 ＜①仕入・外注・委託先等の取引先＞

➢ 取引先等のセキュリティ強化を実現するにあたり、取引先等への要請や支援を担う主たる実施主体（部門）はどこですか（仕入・外注・委託先等の取引先）



※「仕入・外注・委託先等の取引先を有していない」回答先を除く

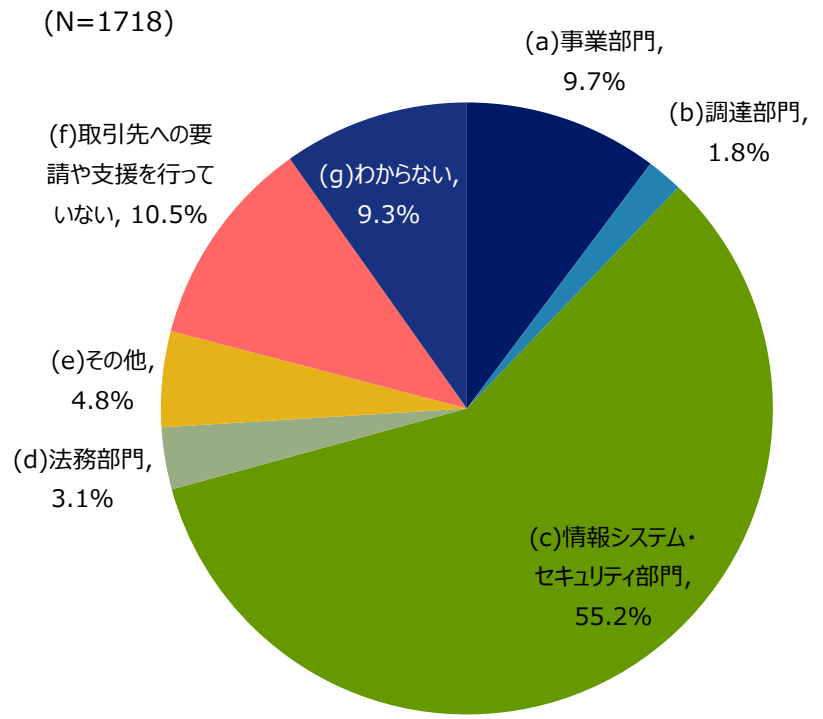
- グループ会社への要請・支援を実施する部門として、IT全般またはサイバーセキュリティを管理する「情報システム・セキュリティ部門」が多く見られた

取引先等への要請・支援を実施する部門と考え方 <②グループ会社>

部門	内容
事業部門	● グループ会社を統括・管理する部門であるため ● 業務上、グループ会社と最も頻繁にコミュニケーションをとる部門であるため ● グループ会社との折衝を担う事業部門が窓口となり、適時、情報システム・セキュリティ部門がサポートを実施
情報システム・セキュリティ部門	● 本社/グループ全体のセキュリティに責任を負う部門であるため ● IT全般の管理を行う部門であるため ● サイバーセキュリティを所管する部門であるため ● ITやサイバーセキュリティに関する知識を有する部門であるため
法務部門	● グループ会社を統括・管理する部門であるため ● セキュリティや個人情報の管理を所管する部門であるため

取引先等への要請・支援を実施する部門 <②グループ会社>

➢ 取引先等のセキュリティ強化を実現するにあたり、取引先等への要請や支援を担う主たる実施主体（部門）はどこですか（グループ会社）



※「グループ会社を有していない」回答先を除く

2．アンケート調査
結果概要･･･２．取引先等への要請（取引先等への要請・支援を実施する部門 ③海外拠点）

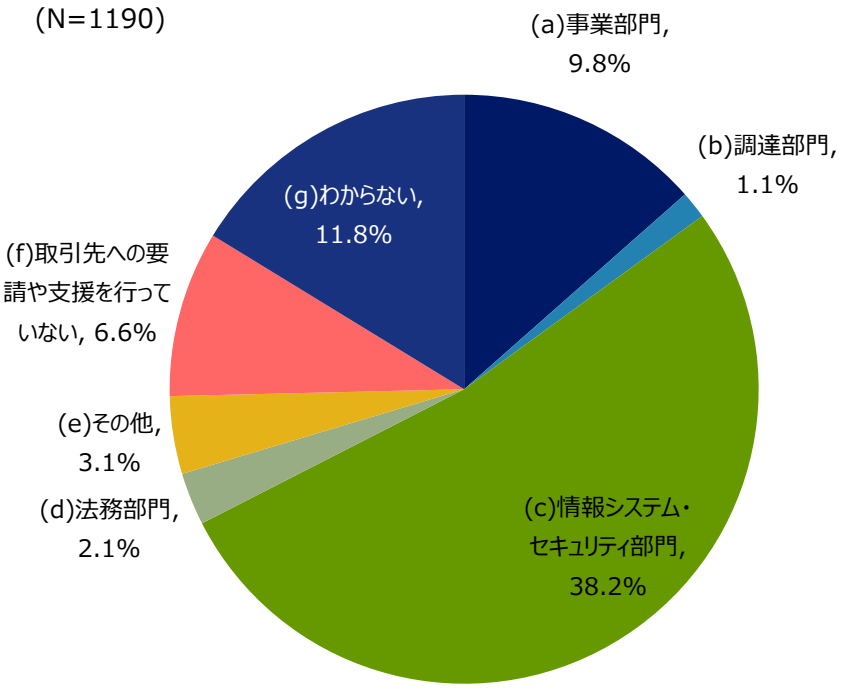
- 海外拠点への要請・支援を実施する部門として、IT全般またはサイバーセキュリティを管理する「情報システム・セキュリティ部門」が多く見られた

取引先等への要請・支援を実施する部門と考え方 ＜③海外拠点＞

部門	内容
事業部門	● 海外拠点を統括・管理する部門であるため ● 業務上、海外拠点と最も頻繁にコミュニケーションをとる部門であるため ● 海外拠点との折衝を担う事業部門が窓口となり、適時、情報システム・セキュリティ部門がサポートを実施
情報システム・セキュリティ部門	● 本社/グループ全体のセキュリティに責任を負う部門であるため ● IT全般の管理を行う部門であるため ● サイバーセキュリティを所管する部門であるため ● ITやサイバーセキュリティに関する知識を有する部門であるため
法務部門	● 海外拠点を統括・管理する部門であるため ● セキュリティや個人情報の管理を所管する部門であるため

取引先等への要請・支援を実施する部門 ＜③海外拠点＞

➢ 取引先等のセキュリティ強化を実現するにあたり、取引先等への要請や支援を担う主たる実施主体（部門）はどこですか（海外拠点）



※「海外拠点を有していない」回答先を除く

2．アンケート調査
結果概要・・・2．取引先等への要請（取引先等へ要請を行う上での課題や足かせ）

- 取引先等への要請を行う上での課題は、小規模事業者への過度な負担や取引先の環境等を考慮した「業種や規模の違い」、及び取引関係に影響することを懸念した「自社と取引先との関係性」に大別された

取引先等へ要請を行ううえでの課題や足かせの具体的な内容

分類	内容
業種、環境、 人員・体力、 意識レベル等の違い	【業種】 ● 自社と業種が異なる企業に、自社の要請に応えてもらうことが難しい場合が多い ● 小規模事業者（個人事業主等）に高いレベルのセキュリティを要求しづらい 【環境】 ● 取引先の環境等が不明、または自社と異なるため、自社の条件をそのまま当てはめることができない 【人員・体力】 ● 規模の小さい企業においては、PCスキルすら満足でないケースがあり、依頼内容を理解できない 【意識レベル】 ● 契約において、「個別対応不可」と回答され修正要求を受け入れない企業がある ● コロナや部材不足で自社も取引先も疲弊しておりセキュリティどころでない 【その他】 ● グループ企業が多い為、徹底まで時間を有する
自社と取引先との関係性	【自社と取引先との関係性】 ● 業界上位の組織が委託先の場合、自社との力関係からお願いレベルでの要請となる ● 取引関係により（取引への影響を懸念し）、取引先への要請や費用負担を要求しづらい ● 取引先ごとに自社との関係性が様々であり、個々の取引先に対してどこまで求めることが出来るのか簡単に判断できない ● SaaS※提供元への要請の限界（個別契約がなく要請そのものがしにくい、SaaS※提供元の反応も鈍い）

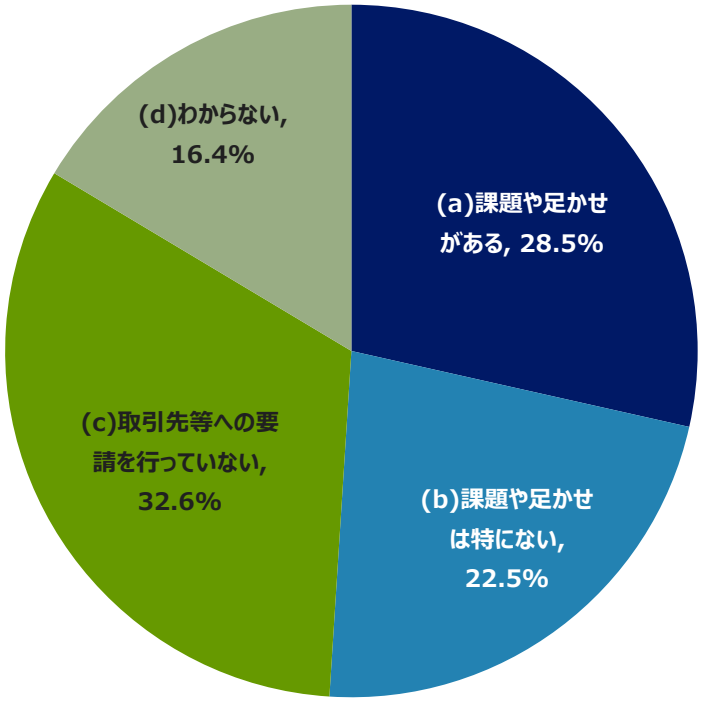
※Software as a Serviceの略。ソフトウェアやアプリケーションの機能をネットワーク経由で提供(利用)するサービス

2．アンケート調査
結果概要・・・2．取引先等への要請（取引先等へ要請を行う上での課題や足かせ）

- 取引先等への要請を行う上での課題や足かせとして、「対策費用の負担」と「取引先等の意識・リテラシーが低い」といった回答が多く見られた

取引先等へ要請を行ううえでの課題や足かせの有無

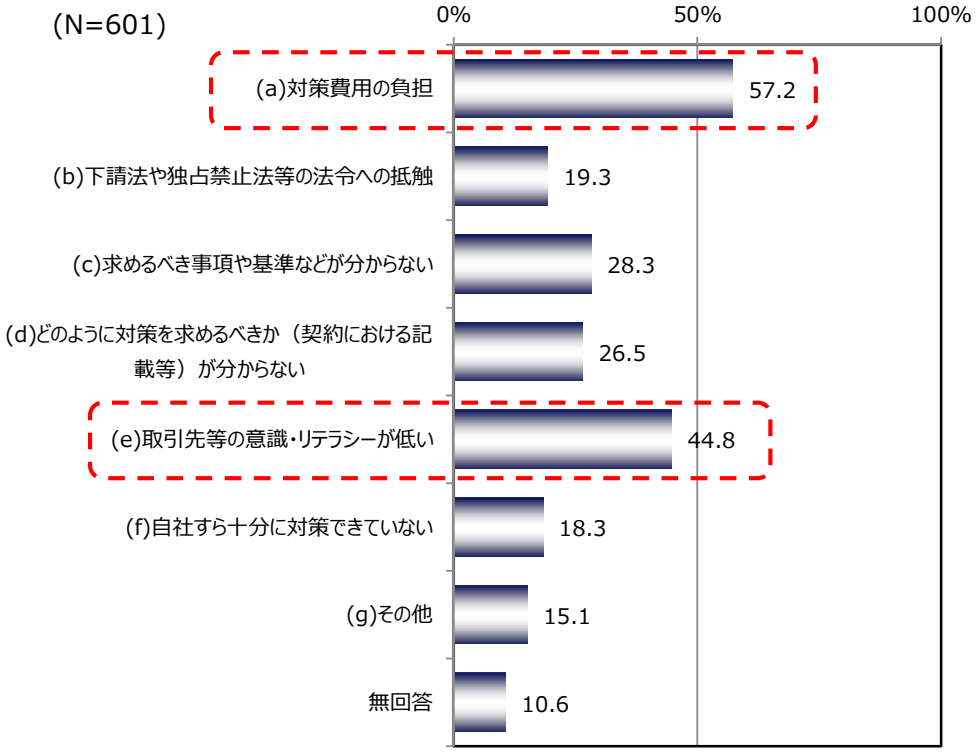
➢ 取引先等に対しセキュリティ対策強化の要請を行うにあたり、課題や足かせはございますか
(N=1876)



※「仕入・外注・委託先等の取引先を有していない」回答先を除く

取引先等へ要請を行ううえでの課題や足かせの内容

➢ 取引先等に対して要請を行うにあたっての課題や足かせの内容として、当てはまるものを全てお選びください



※「課題や足かせがある」回答先のみ

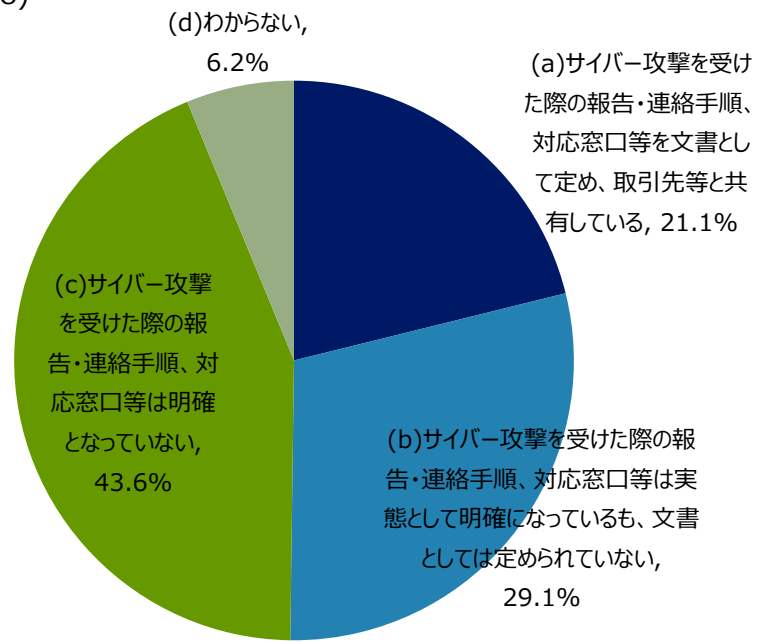
2．アンケート調査
結果概要・・・3． 情報収集・共有、対外公表（サイバー攻撃の報告、情報収集・共有）

- 取引先等からのサイバー攻撃に関する報告・連絡手順、対応窓口等について、明確にされていないケースが多い
- 利用しているサービスやシステムに関する脆弱性やセキュリティ対策等の情報は、自社単独での情報収集に留まらず、グループ会社や取引先等と情報共有されているケースが多く見られた

取引先等からのサイバー攻撃に関する報告

➢ 取引先等がサイバー攻撃を受けた際の貴社への報告・連絡の手順、また、貴社における対応の窓口は定められていますか

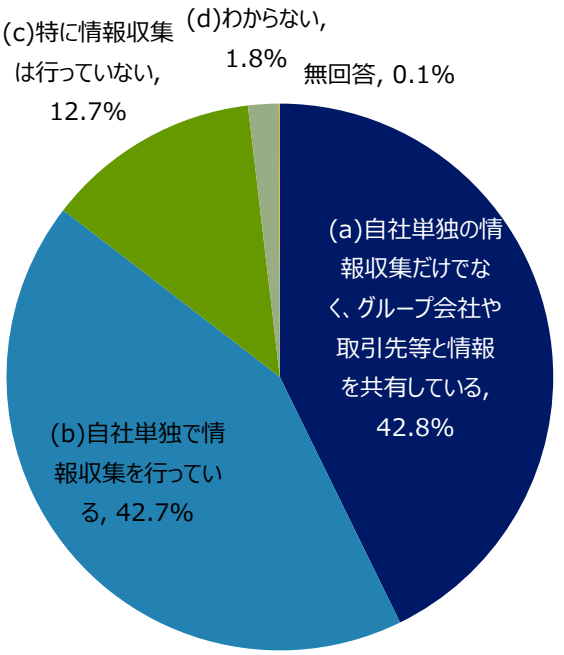
(N=1878)



利用サービス・システムに関する情報収集

➢ 貴社で利用しているサービスやシステムにおける、脆弱性やセキュリティ対策等の情報を定期的に収集していますか

(N=1878)



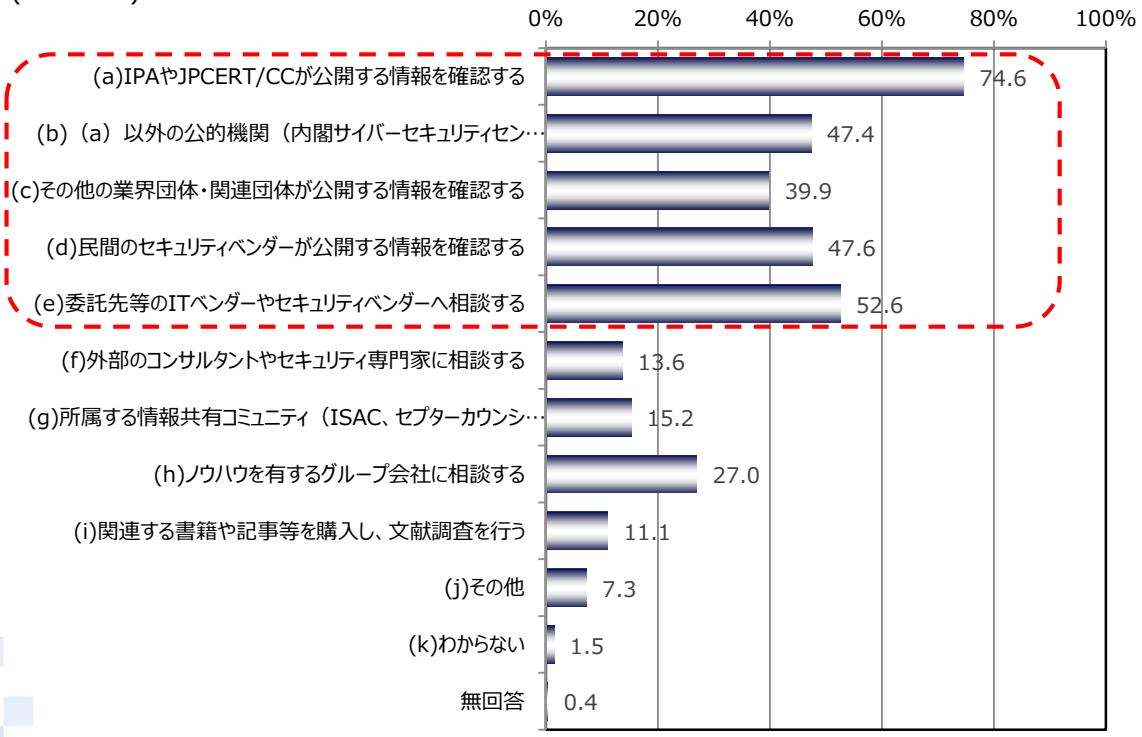
2．アンケート調査
結果概要･･･3．情報収集･共有、対外公表（サイバー攻撃の報告、情報収集･共有）

- 「IPA、JPCERT等の機関」、「民間のセキュリティベンダー等が公開する情報の収集」、「ITベンダー等への相談」による情報収集が多く見られた
- ネットニュース、SNS等、バグバウンティプログラムの活用も見られた

情報収集方法

➢ 情報の収集方法について、当てはまるものを全てお選びください

(N=1611)



※「セキュリティ対策等の情報を定期的に収集している」回答先のみ

情報収集方法（その他）

分類	回答例
親会社等からの支援	● 親会社 ● グループ会社
公知情報	● ネットニュース/TV/新聞 ● メルマガ ● Web記事（官公庁･専門誌等） ● ネット情報検索 ● SNS
その他	● 地元警察との連携 ● バグバウンティプログラム（バグ報奨金サービス）の活用（次ページ参照） ● 脅威インテリジェンスサービスの利用 ● 脆弱性診断ツールの活用 ● 米国CISAのWebサイトの活用 ● TwitterやRSSによる積極的脅威インテリジェンスの収集 ● ウイルス対策ソフトの総合リスクレポートの活用 ● グループ会社間での脆弱性情報共有スキームの活用

（参考）バグバウンティプログラム

- 自社が公開するプログラムに脆弱性があることを想定して報奨金をかけて公開し、脆弱性を発見・報告した外部のホワイトハッカー等に報奨金を授与する制度であり、サイバー攻撃の報告、情報収集・共有に、こうしたサービスを活用する企業が見られた

事例：サイボウズ社のサイボウズ脆弱性報奨金制度

- サイボウズ社が提供するサービスに存在するゼロデイ脆弱性の早期発見を目的とし、実施時期を区切って報奨金制度を実施
- 報奨金は1件あたり20,000円～300,000円（2021年4月28日（水）～ 2021年12月17日（金）実施分）

参加方法

報奨金制度に参加したい場合は、報告用サイト経由でご報告ください。

報告用サイト経由で報告するには、アカウントの申請が必要です。申請はこちらから行うことができます。

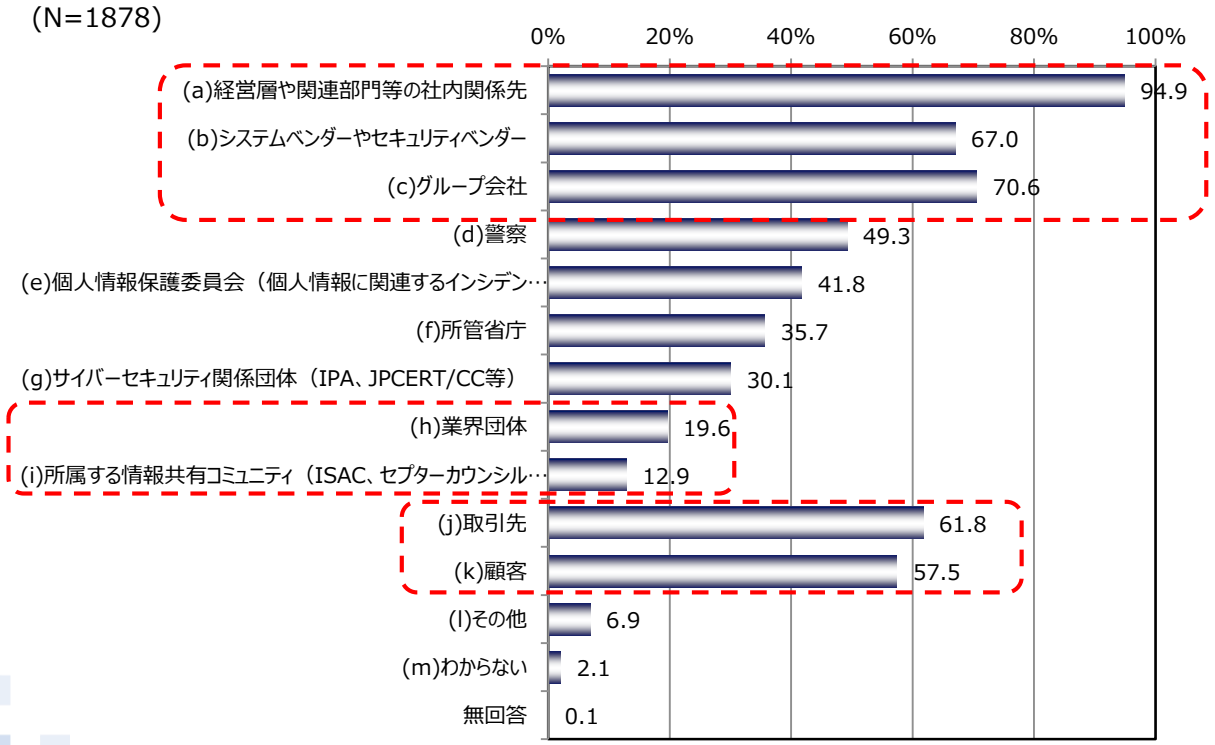
出所：サイボウズ社Webサイト（https://cybozu.co.jp/products/bug-bounty/）

2．アンケート調査
結果概要・・・3．情報収集・共有、対外公表（対外公表）

- サイバー攻撃の被害が発覚した場合に想定される報告・共有・公表先として、経営層や関連部門等の社内関係先、システムベンダーやセキュリティベンダー、グループ会社、取引先、顧客が多く見られた
- 地域に拠点を有する同業他社、共同の基幹系システムを利用する他社等も見られた

サイバー攻撃の被害が発覚した場合に想定される報告・共有・公表先

➢ 貴社においてサイバー攻撃の被害が発覚した場合に想定される報告・共有・公表先に該当するものを全てお答えください



その他

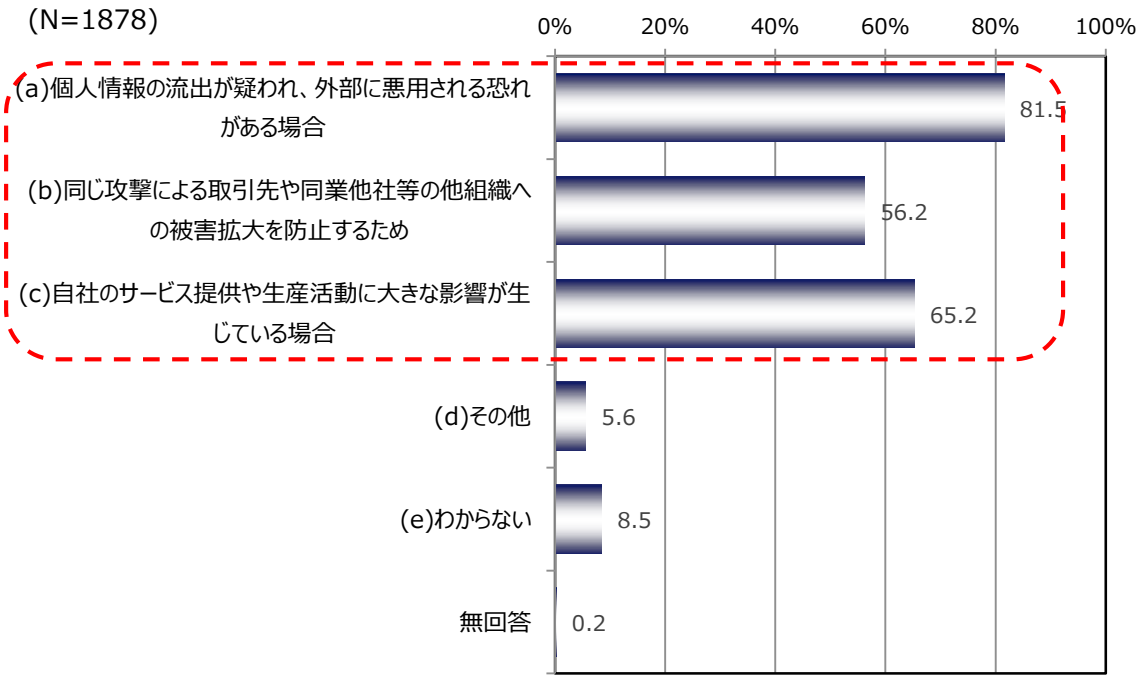
分類	回答例
親会社等との相談、指示	● 親会社 ● グループ本社 ● グループ会社の指示先
その他	● 地域に拠点を有する同業他社 ● 株主等のステークホルダー ● 保険会社（サイバー保険） ● 被害の影響がある取引先および顧客 ● 情報を得るために外部のコンサルタントへ被害情報を連携 ● 顧問弁護士の指導を踏まえて適切に対応 ● 共同の基幹系システム（金融機関向けのシステムベンダーが提供）を利用する他社 ● 対外報告に関する取扱い規定がないため不明

2．アンケート調査
結果概要・・・3．情報収集・共有、対外公表（対外公表）

- サイバー攻撃の被害について対外的に共有・公表を行う理由として、「個人情報の流出が疑われ、外部に悪用される恐れがある場合」、「同じ攻撃による取引先や同業他社等の他組織への被害拡大防止を望む場合」、「自社のサービス提供や生産活動に大きな影響が生じている場合」が多く見られた

サイバー攻撃の被害について対外的に共有・公表を行う理由

➢ 今後仮に貴社においてサイバー攻撃の被害が発覚した場合、対外的に共有・公表を行う場合との理由として想定されるものを全てお選びください



※「対外的な共有・公表」については、各業法等に基づく所管省庁への報告、及びセキュリティ専門事業者等への相談等を除く

その他

分類	回答例
親会社等の指示・判断	● 親会社の指示・判断に従う（親会社に報告する）
ルールに準拠した判断	● 事前に定めた基準に従う ● 重要情報が流出した場合、関係取引先や顧客に共有する ● サイバー保険に加入しているため（保険金支払に公表要件があるケース）
都度判断	● 状況を踏まえ、経営層や内部会議にて判断する ● 専門家・顧問弁護士と相談して対応 ● 被害の規模により、連絡すべき先が多いケース等で、連絡に時間を要する場合、一般に公表

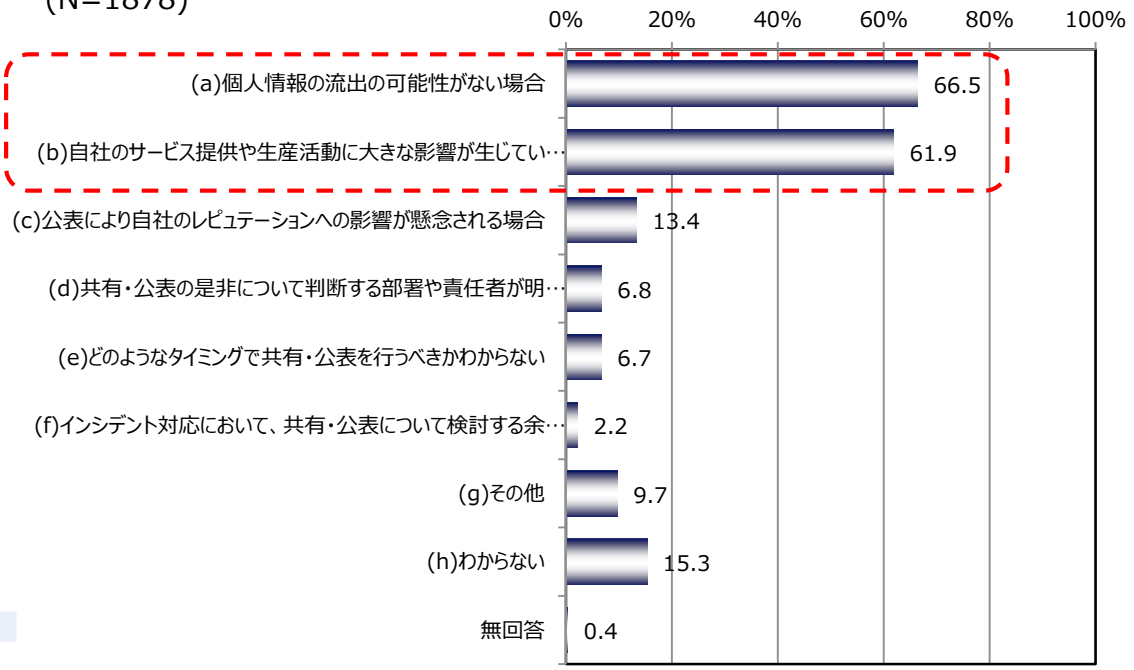
2．アンケート調査
結果概要・・・3．情報収集・共有、対外公表（対外公表）

- サイバー攻撃の被害について対外的に共有・公表を行わない理由として、「個人情報の流出の可能性がない場合」、「自社のサービス提供や生産活動に大きな影響が生じていない場合」が多く見られた
- 「必ず共有・公表する」「公表により二次被害を誘引する可能性がある場合は公表しない」との回答も見られた

サイバー攻撃の被害について対外的に共有・公表を行わない理由

➢ 今後仮に貴社においてサイバー攻撃の被害が発覚した場合、対外的に共有・公表を行わない場合との理由として想定されるものを全てお選びください

(N=1878)



※「対外的な共有・公表」については、各業法等に基づく所管省庁への報告、及びセキュリティ専門事業者等への相談等を除く

その他

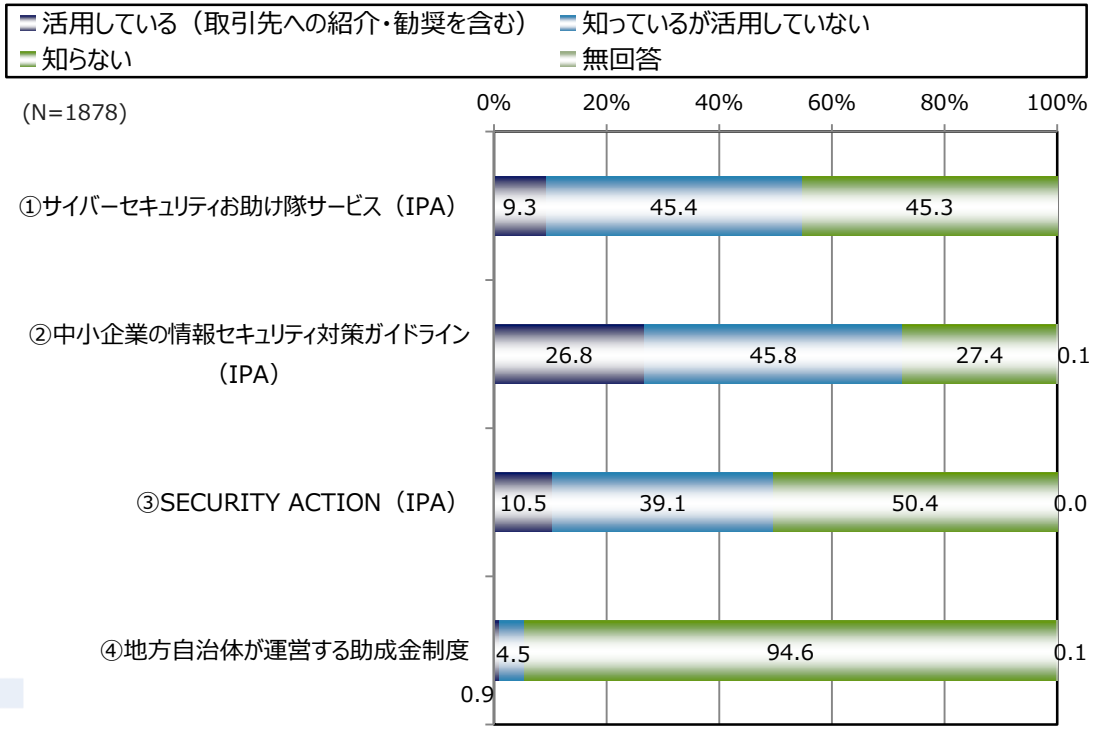
分類	回答例
親会社等の指示・判断	● 親会社の指示・判断に従う（親会社に報告する）
ルールに準拠した判断	● 事前に定めた基準に従う ● 顧客や取引先への影響がない場合 ● インシデントが発生した場合は、必ず共有・公表を行う ● 同業他社等の他組織への被害拡大防止の観点から、情報共有・公表は積極的に実施するよう対応手順を定めている。
都度判断	● 状況を踏まえて（経営層や内部会議にて）判断する ● 公表によって二次被害を誘引する場合など個人の権利利益を保護の観点で公表しない方が望ましいと認められるような場合

2．アンケート調査
結果概要･･･４．支援制度の利用、国等への要請（支援制度の活用･認知）

- 「中小企業の情報セキュリティ対策ガイドライン（IPA）」の活用･認知は比較的進んでいる一方、「サイバーセキュリティお助け隊サービス（IPA）」「SECURITY ACTION（IPA）」の認知はあまり進んでいない
- 「親会社からの支援」や「業界団体が公表している情報やガイドライン」の活用も見られた

支援制度の活用･認知の状況

➢ 下記①～④に挙げた国や自治体、関係機関による中小企業向けのサイバーセキュリティ対策支援活動の活用、認識状況について、あてはまるものをそれぞれお答えください



左記以外で活用･認知している支援制度

分類	回答例
親会社からの支援	● 親会社が定めるITセキュリティ基準に準拠 ● 親会社のセキュリティ部門のサービスを利用している
業界団体が公表している情報やガイドライン	● 業界団体等が策定し、業界の企業向けに発出するサイバーセキュリティガイドライン
JPCERTからの情報	● JPCERT CISTA等の情報共有プラットフォーム 各種ガイドライン
セキュリティ･システムベンダーからの情報	● 各ベンダの発信する注意喚起情報や啓蒙に使える資料

2．アンケート調査
結果概要・・・４．支援制度の利用、国等への要請（国等への要請）

- 「補助金の拡充」や「ガイドラインの提供」を求める声が多い
- 企業に対する「強制力を伴うセキュリティ対策実施制度の導入」や「相談・情報窓口一元化」に関する要請も確認された

国等への要請

分類	内容
補助金の拡充	● 法改正については規制の多い状況下でさらに制度変更などにより追加コストや社内外の対応が増加する傾向が強く、補助金などの拡大や制度変更とあわせて利用できるスポット的な補助も含め拡充してほしい ● 補助金については設備投資など短期で計画から実行までを行えないため期間の長期化や制度利用可否を簡易的に確認できるツールなどを準備を希望 ● ランサムウェア対策に係る費用が自己責任となっている現状に対し、予防策を講じる際の公的支援（補助金等）があれば助かる
ガイドラインの提供	● サプライチェーンに関するガイドラインを企業規模別に定め順守させる等の官民一体のガイドラインを制定し順守させる仕組み ● 現行業界団体がガイドラインを定めているケースがあるが、企業規模として資本が大きい会主向けの内容が多く、企業規模が30人程度の中小企業向けには向いていないと考える ● IT関連ではない一般の中小企業が取り組むべきセキュリティ対策のガイドラインを示してもらえると目標が明確化されやすい。現状どの程度セキュリティ対策投資すればいいのか目安がわからない ● テレワーク実施時におけるセキュリティ確保のための費用について、企業と個人の費用負担に関するガイドライン
強制力を伴う制度の導入	● 公的機関等による定期的な監査、または定期的な活動報告の徴求 ● 脆弱性診断を補助金を利用して受けられるようにする。又は、強制的に診断を受けることを義務化する ● セキュリティへの取り組みにレベル認定制度を導入し、格付けを行う。特に公共事業への入札向けの必須要件とする
相談・情報提供等の窓口の一元化	● 相談や助成金、ガイドライン、情報提供などの窓口の一本化
その他	● 攻撃被害に遭い、且つ加害者となった場合、様々な面で制裁が加わるのは致し方ないにせよ、純粋に被害者で留まった場合でも報道等により社会的制裁がなされる風潮を是非是正して欲しい。事例は他社にも価値がある筈だが、誰も公表したくなくなる ● 子会社のサイバーセキュリティ対策を親会社の支出で実施した際に、一定の範囲で利益供与にあたらなくなるような税制上の対策を講じてほしい

３．ヒアリング調査

3．ヒアリング調査
調査概要

- 組織のサプライチェーン・サイバーセキュリティ対策や情報共有の具体事例、国等へ要請の把握を目的に、様々な業種の民間事業者を対象に、インタビュー調査を実施

実施概要

項目	内容
対象企業の選定	● アンケート調査結果、ならびに各社のIR資料等より、サプライチェーンのサイバーセキュリティについて、特徴的な(または他社が参考となる)取組みが想定される事業者を選定
実施方法	● Web会議(Microsoft Teamsを利用)
実施件数	● 多様な業種から、大手企業を中心に11社に対してヒアリングを実施
実施スケジュール	● 2022年1月17日～3月10日

インタビュー項目の概要

No	分類	内容
1	リスク認識	● 取引先等を経由した攻撃被害等のサプライチェーン・サイバーセキュリティに係るリスク認識
2	対策	● 取引先等に対するセキュリティ対策の要請や取決めの内容 ● 対策を進めるにあたっての課題、解決方法 ● 取引先等への支援の実施内容
3	情報収集・共有、対外公表	● 情報収集及び取引先等との共有 ● サイバー攻撃被害の対外公表
4	支援制度の利用、国等への要請	● 各種支援制度の認知、利活用の実態 ● 国、自治体、公的機関等に求める施策、取組み

3．インタビュー調査
結果概要･･･１．リスク認識（１／５）

- サプライチェーンのサイバーセキュリティリスクは、企業のビジネスやサービス・商材の特性等に応じ、取引先等との関係性、自社と取引先等とのやりとり、自社のサプライチェーンの特性等の観点から認識されている

サプライチェーンのサイバーセキュリティに関して認識するリスク（１／２）

自社と取引先等との関係性	● 「保守・運用」、「調達」、「委託」についてそれぞれリスクを認識している • ITシステムの保守・運用の委託先 ネットワークを経由したマルウェア感染（取引先とネットワーク接続されているケース、外部からPCを持ち込み、ネットワークに接続するケース） • システムや設備の調達先 システムや設備の調達の際、納入時にマルウェアが混入、または脆弱性が含まれていることをきっかけとしたマルウェア感染 • 業務委託先委託 当社保有データを連携した委託先の情報管理が脆弱なことによる情報漏洩 ● 自社と取引先等との関係性ごとにリスクを認識している • 業務委託先（協力会社） お客様から預かった情報を提供した協力会社が標的型攻撃等を受けることによる情報漏洩 • 保有システム、サーバーの運用・保守・監視の委託先 当社内のネットワークに接続している委託先が攻撃、侵入を受けて感染することによる被害 • SaaSの運営企業 相手先が運用するサービスが攻撃を受けることによるサービスの利用不可や情報漏洩 • 上記以外の委託先 相手先が攻撃を受けることによる情報漏洩 • 国内グループ会社 グループ会社が攻撃を受けることによる情報漏洩（グループ間でネットワークやインフラとなるクラウドサービスを共同運用） • 海外グループ会社 レピュテーションリスク等（ネットワークは分離しているため直接攻撃が波及することはない）

3．インタビュー調査
結果概要･･･1．リスク認識（2／5）

サプライチェーンのサイバーセキュリティに関して認識するリスク（2／2）

自社と取引先等とのやりとり	● 自社と取引先等とのやりとりの内容に応じてリスクを認識している • メール等のやり取りを介した情報漏洩やマルウェア感染のリスク • 取引先自身が物品・ソフト等を調達し、製品を開発・製造するプロセスの中でマルウェア等に感染し、ソースコードなどが流出してしまうリスク • 自社が取引先から調達する物件（OS、商用ソフトウェア等）がセキュアなものでないリスク
自社が提供する商材を利用する組織の特性	● 自社が生産する商材がどの領域で利用されるか（例：重要インフラ事業等）を1つの指標として捉え、それらに関係する取引先のリスクを認識している
サプライチェーンの特性	● サプライチェーンを類型化してそれぞれのリスクを認識している • 自社の商品・サービスを提供するためのサプライチェーンの特徴に応じたリスク • 自社が製造するハードウェアの部品を仕入れるためのサプライチェーンの特徴に応じたリスク • 自社の製品に組み込むソフトウェアを仕入れるためのサプライチェーンの特徴に応じたリスク ● 自社の事業内容ごとにサプライチェーンの特性を踏まえてリスクを認識している • 受託事業を担うサプライチェーンの特徴に応じたリスク • 販売事業を担うサプライチェーンの特徴に応じたリスク ● サプライチェーンを通じて取引を行う資材等の重要度を踏まえてリスクを認識している • 原材料、部品、包装資材等、自社が提供する製品に関わる直接材を扱う取引先のリスク • 工具、ごみ袋等の生産補助品を扱う取引先のリスク

3．インタビュー調査
結果概要･･･1．リスク認識（3／5）

- 懸念しているリスクの種類として、サプライチェーン上の取引先等と繋がることによる顧客情報流出、重要情報窃取、クラウドベースでの取引によるリスク等が挙げられた

懸念しているリスクの種類

懸念しているリスクの種類	● 製品加工を担う取引先に顧客の製品図面等を連携することによる情報流出リスク ● 協力企業とサイバー空間でつながることによるリスク ・ セキュリティ対策の脆弱な取引先がサイバー攻撃を受けることによる機密情報の漏洩 ・ 同じネットワークに接続している協力企業や工場が攻撃を受けることによるネットワーク接続設備の停止、部品生産、供給への影響 ● クラウドベースで取引を行うことも多いため、メールや物理媒体と同様、クラウドも攻撃の入り口となり得る外部接点として留意している ● 国内では非上場の取引先、海外ではアジア地域の取引先のサイバーセキュリティリスクが高いと認識。比較的規模の小さい非上場の取引先については、秘密保持・情報セキュリティに関する意識が高くない傾向 ● 攻撃被害は、標的型攻撃メール、ビジネスメール詐欺に加え、ホームページのデータ改ざんを特に懸念している。自社のホームページでは、製品に関する情報を公示しているが、その情報を改ざんされてしまうと、消費者に大きな影響が生じ得る ● 技術に関する重要情報窃取のリスクを想定 ● 昨今、国内・海外共に増加している標的型メール、不正な送金先変更を指示するビジネス詐欺メールや、不正アクセスによる情報漏洩、ランサムウェア攻撃による身代金請求やシステム・業務の停止等についてリスクを認識

3．インタビュー調査
結果概要･･･１．リスク認識（４／５）

- 過去に受けた攻撃として、標的型攻撃メール、ビジネスメール詐欺、ランサムウェアが挙がっており、実際に被害が発生したケースも見られた

過去に受けた攻撃内容と被害状況

	攻撃内容	被害状況
グループ会社・海外拠点における攻撃	● 十年以上前から標的型攻撃メールが送られてきているほか、ビジネスメール詐欺、ランサムウェア感染が挙げられる	● ビジネスメール詐欺では金銭を支払った事案、ランサムウェア感染ではグループ会社で被害が発生し、対応に多額の費用を要したケースもある ● 最近ではランサムウェアの被害によりシステムが停止する、破壊するといったものが多く、グループ会社や海外のブランチで影響が出ているが、本体への影響は出ていない
委託先を経由した攻撃	● 委託先のメールシステムが乗っ取られ、支払先口座を変更してほしいという詐欺メールが委託先メールアドレスから当社に送信されたことがあった ● 設備業者がメンテナンスのために持ち込んだPCから当社環境にウイルスが侵入してきた事例もある ● 取引先企業がEmotet等に感染し、ウイルスメールが当社に送り付けられるような事象は発生している	● いずれのケースも大事には至っていない
	● 人事サービスを提供している企業がランサムウェア攻撃を受けた際、当社は当該企業の子会社の人事サービスを使っていた。サイバー攻撃を受けた親会社のIT基盤を子会社でも使っており、当社が連携した人事データはそのIT基盤内に格納されていた	● ランサム攻撃を受けた旨の一報は受けたが、当社のデータが影響を受けたかに関する適切な回答は受けていない。ある程度、被害範囲は特定できており情報は漏えいしていないと聞いているが、本当に漏えいしていないかについては不明である

3．インタビュー調査
結果概要･･･１．リスク認識（５／５）

過去に受けた攻撃内容と被害状況

	攻撃内容	被害状況
PPAPを利用したメールでの攻撃	● SOC（Security Operation Center）にて当社に対する外部からの攻撃や不正アクセスの状況を監視しているが、最近禁止したPPAP（パスワード付添付ファイルのEメールによる送付）の手法を利用した攻撃が多い。同様の傾向は取引先にもあるものと想定しており、注意が必要	● 監視段階にて発見

3．ヒアリング調査
結果概要･･･2．対策（1／2）

- 業界により、業界団体や協議会が関係する中小企業等の普及啓発を担う取組みが確認された
- 個々の企業として、取引先等とプラットフォームを共有し、情報提供やアセスメントを実施する取組みもみられた
- また、課題として、取引先等との関係性により、強い要請を実施しづらいとの意見もあげられた

取組み事例等	
業界団体が主導する啓発	● 業界団体が主導して委託先事業者向けのチェックシートや教育資料等を作成・提供し、それが業界のスタンダードとなっている。これにより、業界全体の対策レベルの向上につながるとともに、委託先事業者が複数の委託元事業者より同様のチェックや対策を求められ、それに対応する負担の圧縮ができている
協議会による連携	● 業界に関連する様々なステークホルダーが参加してサイバーセキュリティを目的とした協議会を設立し、情報共有、訓練、従業員教育等を実施している。将来的には、参加者間でのサイバーセキュリティに係る連携・調整を図る機能を志向している
取引先等への要求	● 基本契約において秘密保持やインシデント対応等の条項を設定しているが、取引内容によってはより詳細な要求項目を設定する必要を認識している。これを踏まえ、取引内容に応じ、調達部門がより具体的な要求事項を提示できるようにするためのガイドラインを検討している ● ISO27001/27002に基づく約100項目の独自の要求事項をリスト化し、これをもとに取引先に対して対策の有無を確認している ● 再委託については、自社と委託先の双方で合意ができれば認めているが、自社から委託先に求める対策水準を委託先から再委託に徹底することを求めている。加えて、これに不備があった場合は委託先が責任を負うことを明確化している ● インシデントの発生を契機に社長名で通達を行いEDR※を全グループに導入した ● 個人情報、財務情報、社外秘情報等を扱うITベンダーに対しては、海外本社の方針により外部の第三者によるアセスメントへの協力を依頼している ● 取引先に対し、ウイルスメールの危険性を説明しているが具体的な対策要請まではできていない ● 取引先に対し、ランサムウェアの身代金が高額にもなることを伝え、事前対策の必要性を説いている

※Endpoint Detection and Responseの略。ユーザーが利用するパソコンやサーバー（エンドポイント）における不審な挙動を検知し、迅速な対応を支援するソリューション

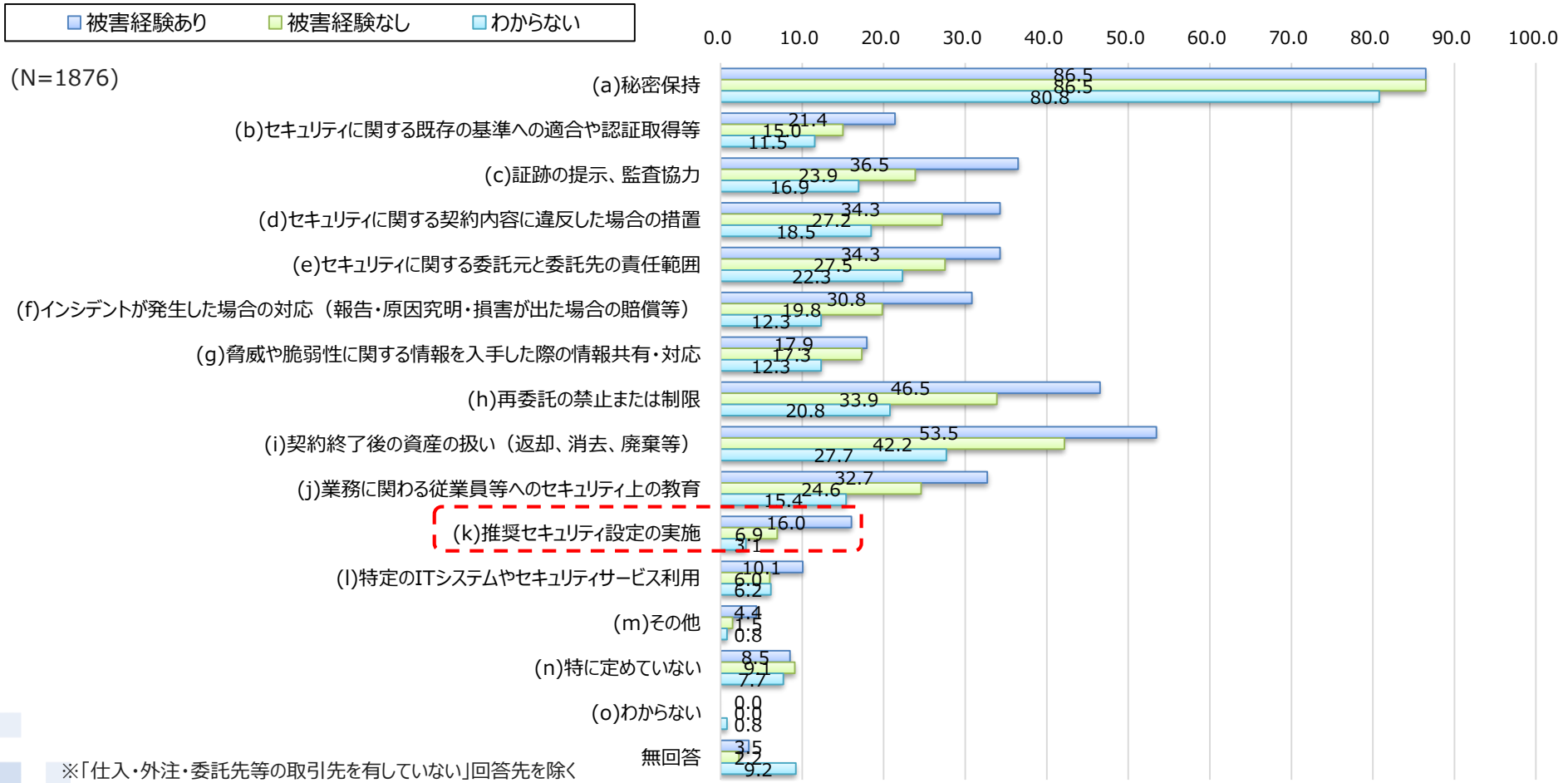
3．ヒアリング調査
結果概要･･･2．対策（2／2）

取組み事例等（続き）	
（続き） 取引先等への要求	● 取引先へのアンケートを毎年実施し、現状把握と改善指導を行っている ● 中小企業の取引先に対して、訪問や電話会議にて自社が行っているサイバーセキュリティ対策の紹介やアドバイスを実施している。他方で、取組みを強制することはできないため、情報を提供して対策を促すレベルの支援となる
取引先等への支援	● 委託元である自社が主導して取引先企業同士のコミュニティを組成し、そのコミュニティを通じて、ガイドラインやチェックシート、教育資料等を共有している。チェックシートの活用により、取引先の対応レベルの見える化が可能となり、個別ヒアリング等自社からのアプローチに活用している ● CSR活動の一部として、取引先と共有で利用するプラットフォームシステムを介し、情報セキュリティに関するアセスメントを実施している ● 取引先からセキュリティに関して個別に相談があればそれに応じている ● 取引先は自社とだけ取引しているわけではなく、同業他社とも同様に取引しているケースが多い。そのため、自社だけがセキュリティ対策を強く要請した際に、自社との取引を敬遠されてしまうことを危惧している ● 自社の資本が入ってない取引先に対してサイバーセキュリティ対策を求めることは難しい。費用負担については寄付金や交際費に該当してしまう懸念ある。また、強く要請すると、優越的地位の乱用ととられかねないことを危惧している。セキュリティの懸念から重い要請を行うこともできなくはないとは考えるが、どこまでが許容されうる範囲なのかはわからない ● 自社の資本が50%以上のグループ会社に対しては、海外も含め、セキュリティ対策に関する導入やレビュー等の支援を実施し始めているが、それ以外の取引先については特に支援等は実施していない
グループ一体のガバナンス	● 年に複数回本社とグループ会社によるセキュリティ部会を開催し、セキュリティの活動方針やKPIの検証を実施 ● グループ会社には、業務上の制約等により、自社と同様の対策を適用したくないという要望もある ● グループ会社を集めて定期的にセキュリティに関する連絡会を実施している ● 海外拠点と情報交換を行う際に、必ずセキュリティに関する連絡を実施している ● 日本及び海外拠点のセキュリティ担当者間で週に1回ミーティングを行い、セキュリティ対策の状況等について情報共有を実施している

（参考）攻撃被害をうけた取引先等への要求/取決め（アンケート調査結果より）

- インタビュー調査では、攻撃被害を踏まえ、対策が進められたケースも確認された
- アンケート調査においても、取引先を経由した攻撃被害の経験を有する企業ほど、取引先への要求事項を設けている割合が高い傾向が見られた

攻撃被害の経験有無×取引先等への要求/取決め ＜①仕入・外注・委託先等の取引先＞

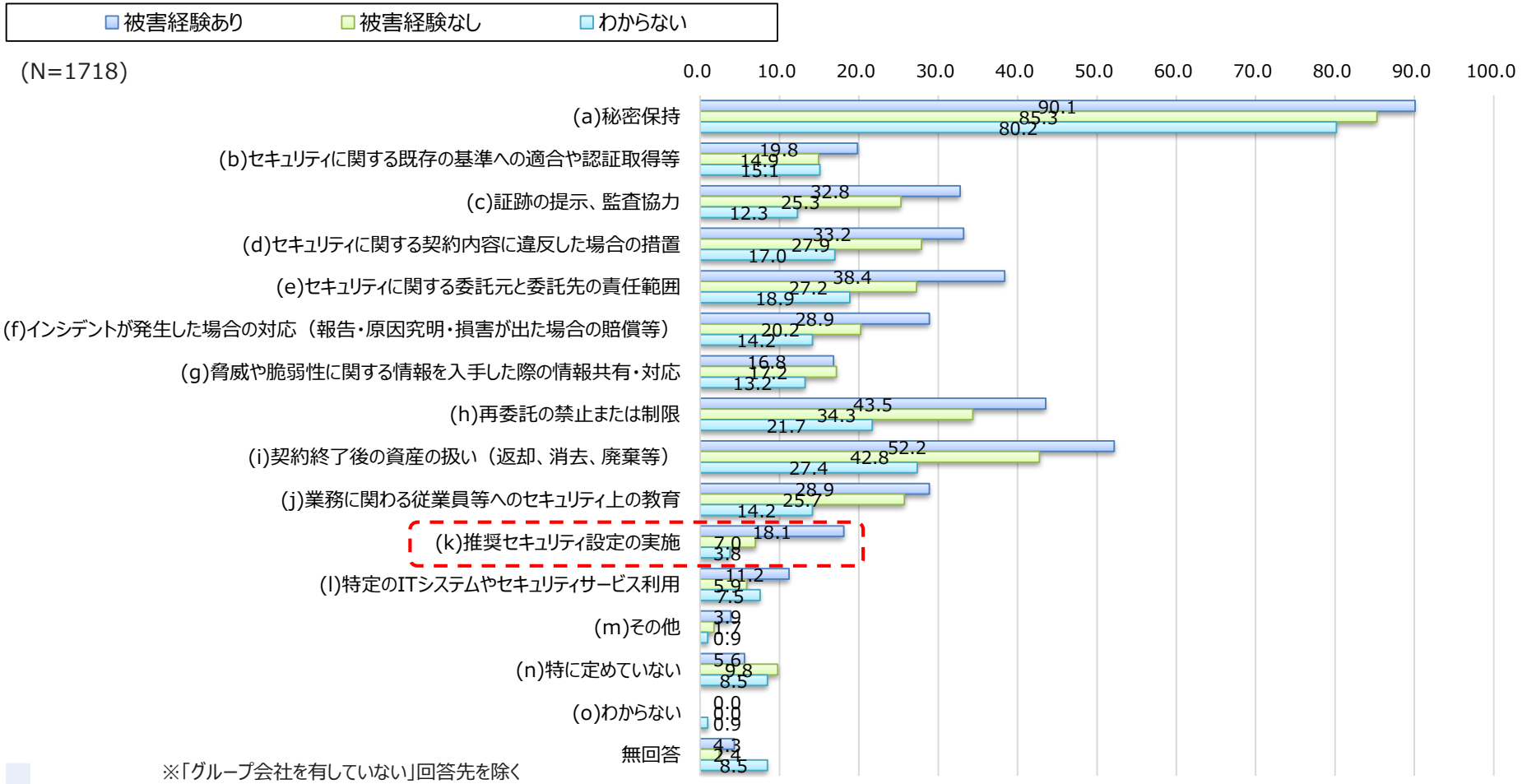


※「仕入・外注・委託先等の取引先を有していない」回答先を除く

（参考）攻撃被害をうけた取引先等への要求/取決め（アンケート調査結果より）

- グループ会社も同様に、攻撃被害の経験を有する企業ほど、「推奨セキュリティ設定の実施」等の要求事項を設けている企業が多い

攻撃被害の経験有無×取引先等への要求/取決め ＜②グループ会社＞

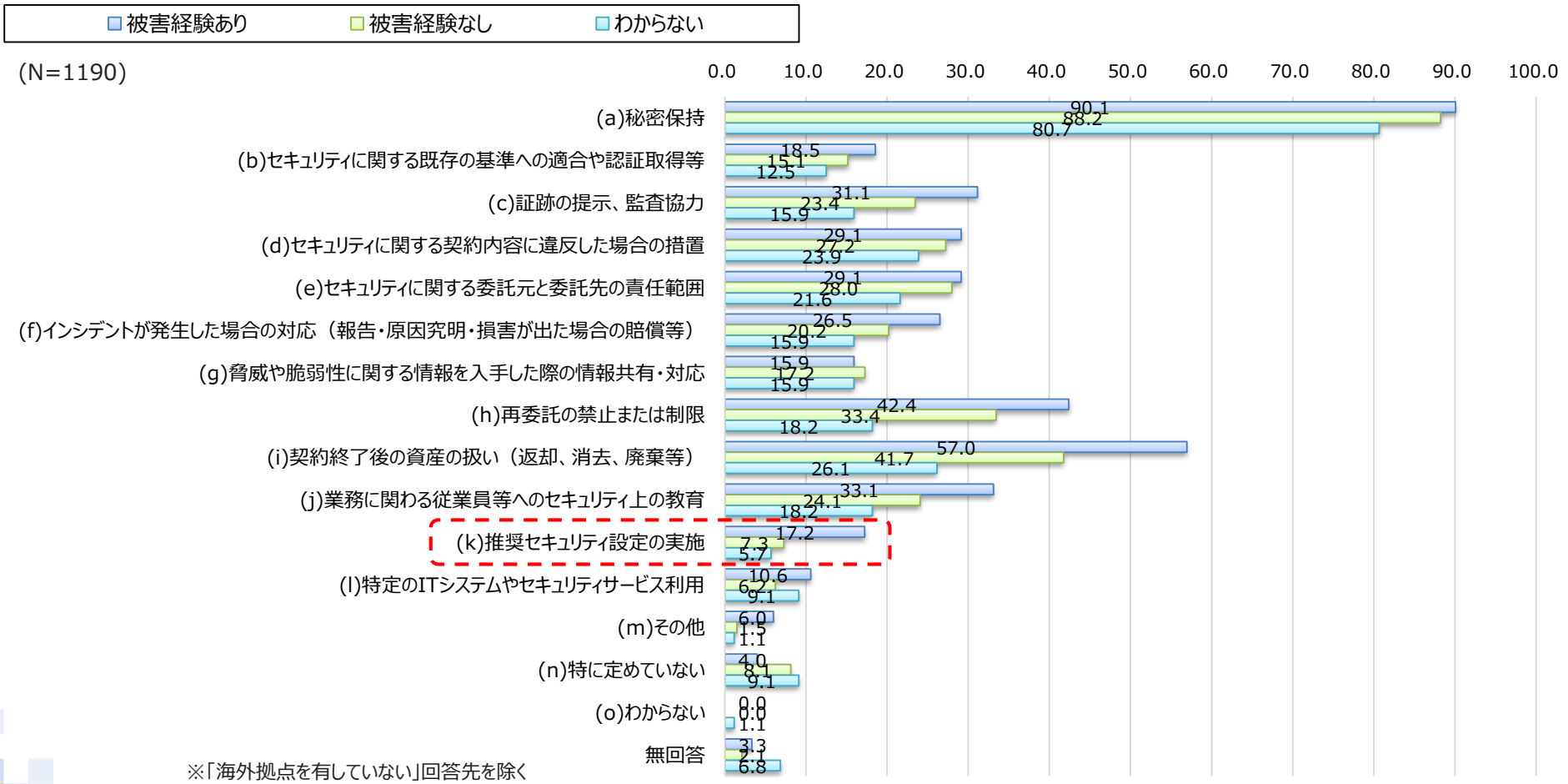


※「グループ会社を有していない」回答先を除く

（参考）攻撃被害をうけた取引先等への要求/取決め（アンケート調査結果より）

- 海外拠点も、攻撃被害の経験を有する企業ほど、「推奨セキュリティ設定の実施」等の要求事項を設けている企業が多い
- また、グループ会社と比較して各要求事項を定めている割合が低い傾向。他方で、被害経験を有する企業の場合、「資産の扱い」や「従業員等へのセキュリティ教育」については、グループ会社よりも定めている企業が多い

攻撃被害の経験有無×取引先等への要求/取決め ＜③海外拠点＞



※「海外拠点を有していない」回答先を除く

3．ヒアリング調査
結果概要・・・3．情報収集・共有、対外公表（1/2）

- 各社JPCERT等から情報収集活動を実施しているが、取引先への情報共有を行っている場面は限定的である
- 対外公表については、顧客・取引先への影響や監督官庁と調整を鑑み、個々に判断されるケースが多い

取組み事例	
情報収集活動	● 情報収集先となる外部機関 　• IPA、JPCERT/CC、J-CSIP、日本CSIRT協議会、ISAC、NISCの情報共有システムJISP、ITメディア等のセキュリティニュース、警視庁などから情報を収集 　• セキュリティベンダー、ITシステムの業務委託先から情報を収集 ● 親会社・海外本社や関連組織が中心となり情報収集を実施 　• 親会社のセキュリティチームから情報受領、海外本社主導によるバグバウンティプログラムの実施 　• 会社内のPSIRT、IRT(Incident Response Team)が中心となり情報収集を実施
業界としての取り組み	● 業界単位で組織しているISACから、NISCやJPCERTの情報をまとめて受領 ● 所属する業界団体のセキュリティに関する部会で定期的に会合を開き情報共有を実施
取引先・グループ会社への共有の仕組み	● インシデント情報、リスク、脆弱性情報等、緊急対応が必要な場合は、国内・海外グループ会社に情報共有を実施 　• グループ掲示板やメール、社内のコミュニケーションツールによってグループ会社等と情報共有を実施 　• CSIRTが主体となって情報収集・グループ企業への展開を実施 　• 国内外のグループ会社で共通で設置しているCSIRTの枠組みの中で未然防止の検討や攻撃分析、演習・訓練を実施 ● 必要に応じ、取引先への情報共有を実施 　• Emotet等のメールについて注意が必要なケースについては、協力会社も含めて情報共有するケースあり 　• 当社の製品に影響があると判断した場合、調査を行うため、取引先にも情報共有するケースがあり 　• 本部や総務部が取引先にも影響のある情報を調達本部に連携し、取引先企業に通知 ● セキュリティソリューションの提供を受けている企業で開催しているユーザー会で取引先と互いの課題等情報共有を実施

3．ヒアリング調査
結果概要・・・3．情報収集・共有、対外公表（2/2）

取組み事例

対外公表についての考え方	● 対外公表については個々事象の影響を鑑みて個別に判断を実施 • お客様に広くお知らせする必要があるものについては、報道発表を行うが、個別対応ができる範囲のものは、個別対応を実施 • 国家事業に関する情報の漏洩時には、会社単独での判断ができないため、監督官庁と連携したうえで、対応を検討 • 単純な基準は設けておらず、経営への影響の大きさや顧客への被害状況を元に判断（インシデントについては、その重大性からいくつかのレベルに分類の上、その分類に従って管理） • 事業部ごとに、会社・グループHPから公表するかを案件ごとに検討 • 攻撃被害の社外公表は、広報、IR部門と相談して個別に判断 • サイバーセキュリティに限定したものではない、グループ全体の基準に則って都度判断 ● 何かしらの基準に沿って判断を実施（予定含む） • 経営層へのエスカレーションや外部公表の判断について、CSIRT立ち上げやサイバーBCP構築を合わせ基準策定を検討中 • インシデント生じた場合、HPで公表、個人情報が流出した際には、所管省庁に報告ののち、個人情報保護委員会に報告
その他課題	● 業界内で課題になっている事項として、具体的な被害が発生していないヒヤリハットのような事象をどこまで共有するべきかが不明確な状況 ● 次年度からCSIRTを立ち上げる予定となっており、IPAやJPCERT/CC等の第三者から情報のパスの整理も今後の課題 ● 個人情報漏洩が海外子会社で発生した場合は、海外の警察への通報が必要であるが、国内の警察にも通報した際、事情聴取等に手間が取られ、犯人への対応、システムへの対応が困難になる可能性あり

（参考）業種ごとの情報収集方法（アンケート調査結果より）

- インタビュー調査では、特定の業種・業界において、業界団体等コミュニティから情報収集する事例が確認できた
- アンケート調査でも、「電気・ガス・熱供給・水道業」「金融業務、保険業」等重要インフラ事業者は、業界団体やISAC等の情報共有コミュニティを通じた情報収集が活発であることが確認できた

業種×情報収集方法

	N	(a)IPAやJPCERT/CCが公開する情報を確認する	(b)（a）以外の公的機関（内閣サイバーセキュリティセンターや警察庁、地方自治体等）が公開する情報を確認する	(c)その他の業界団体・関連団体が公開する情報を確認する	(d)民間のセキュリティベンダーが公開する情報を確認する	(e)委託先等のITベンダーやセキュリティベンダーへ相談する	(f)外部のコンサルタントやセキュリティ専門家に相談する	(g)所属する情報共有コミュニティ（ISAC、セプターカウンシル等）に相談する	(h)ノウハウを有するグループ会社に相談する	(i)関連する書籍や記事等を購入し、文献調査を行う
(a)農業、林業、漁業	2	100.0	50.0	50.0	50.0	100.0	50.0	0.0	50.0	50.0
(b)鉱業、採石業、砂利採取業	7	71.4	57.1	28.6	28.6	57.1	28.6	14.3	14.3	42.9
(c)建設業	168	52.4	25.6	21.4	41.7	41.7	8.9	3.6	17.9	6.0
(d)製造業	623	62.9	36.4	28.6	39.6	40.6	10.8	5.9	19.3	9.6
(e)電気・ガス・熱供給・水道業	40	85.0	72.5	60.0	60.0	52.5	27.5	35.0	40.0	12.5
(f)情報通信業	133	85.0	57.9	50.4	48.1	28.6	11.3	10.5	20.3	9.8
(g)運輸業、郵便業	90	60.0	44.4	31.1	40.0	44.4	10.0	15.6	33.3	10.0
(h)卸売業、小売業	298	47.0	23.2	24.2	32.2	46.6	6.4	5.4	23.2	5.7
(i)金融業務、保険業	215	87.9	80.5	75.3	54.9	69.3	24.2	60.0	30.2	19.1
(j)不動産業、物品賃貸業	33	78.8	42.4	21.2	39.4	66.7	15.2	3.0	24.2	9.1
(k)学術研究、専門・技術サービス業	14	78.6	57.1	28.6	42.9	35.7	28.6	0.0	35.7	0.0
(l)宿泊業、飲食サービス業	34	38.2	20.6	14.7	29.4	41.2	8.8	0.0	17.6	2.9
(m)生活関連サービス業務、娯楽業	15	46.7	26.7	6.7	20.0	26.7	13.3	0.0	33.3	6.7
(n)教育、学習支援業	1	100.0	0.0	0.0	100.0	100.0	0.0	0.0	0.0	0.0
(o)医療、福祉	6	33.3	0.0	0.0	16.7	50.0	0.0	0.0	0.0	0.0
(p)サービス業（他に分類されないもの）	162	64.2	35.2	29.0	39.5	41.4	7.4	7.4	27.2	8.0
(q)その他	37	56.8	29.7	21.6	29.7	40.5	5.4	2.7	21.6	5.4
全業種平均	1878	64.0	40.7	34.2	40.8	45.1	11.7	13.0	23.2	9.5

（参考）業種ごとの情報収集方法（アンケート調査結果より）

- インタビュー調査では、特定の業種・業界において、業界団体等コミュニティへ報告・共有する事例が確認できた
- アンケート調査においても、重要インフラ事業者のうち、特に「電気・ガス・熱供給・水道業」及び「金融業務、保険業」は、業界団体やISAC等への報告・共有を積極的に実施していることが確認できた

業種×攻撃被害発覚時の報告・共有・公表先

	N	(a)経営層や関連部門等の社内関係先	(b)システムベンダーやセキュリティベンダー	(c)グループ会社	(d)警察	(e)個人情報保護委員会（個人情報に関連するインシデントが発生した場合のみ）	(f)所管省庁	(g)サイバーセキュリティ関係団体（IPA、JPCERT/CC等）	(h)業界団体	(i)所属する情報共有コミュニティ（ISAC、セプターカウンシル等）	(j)取引先	(k)顧客
(a)農業、林業、漁業	2	100.0	100.0	100.0	100.0	50.0	0.0	50.0	0.0	0.0	50.0	100.0
(b)鉱業、採石業、砂利採取業	7	100.0	57.1	100.0	28.6	14.3	28.6	28.6	28.6	14.3	85.7	28.6
(c)建設業	168	89.9	63.7	61.9	35.1	23.2	23.8	21.4	8.3	3.0	57.1	48.2
(d)製造業	623	94.4	61.8	69.5	40.9	31.3	22.0	23.0	9.6	3.7	58.1	49.0
(e)電気・ガス・熱供給・水道業	40	97.5	67.5	82.5	75.0	70.0	75.0	42.5	62.5	37.5	72.5	72.5
(f)情報通信業	133	98.5	50.4	68.4	54.1	73.7	47.4	46.6	21.1	14.3	65.4	70.7
(g)運輸業、郵便業	90	92.2	75.6	77.8	58.9	32.2	35.6	28.9	15.6	18.9	61.1	63.3
(h)卸売業、小売業	298	94.6	68.5	71.5	43.6	37.2	22.5	18.1	14.1	2.0	63.1	52.0
(i)金融業務、保険業	215	99.5	91.2	73.0	89.3	60.9	92.6	69.8	66.0	64.7	69.8	83.3
(j)不動産業、物品賃貸業	33	100.0	84.8	78.8	45.5	69.7	39.4	30.3	18.2	0.0	72.7	75.8
(k)学術研究、専門・技術サービス業	14	100.0	64.3	78.6	57.1	64.3	50.0	35.7	7.1	7.1	42.9	57.1
(l)宿泊業、飲食サービス業	34	88.2	73.5	67.6	35.3	32.4	17.6	11.8	5.9	2.9	41.2	44.1
(m)生活関連サービス業務、娯楽業	15	93.3	66.7	60.0	40.0	60.0	33.3	53.3	20.0	0.0	53.3	53.3
(n)教育、学習支援業	1	100.0	100.0	100.0	100.0	100.0	100.0	100.0	100.0	0.0	100.0	100.0
(o)医療、福祉	6	100.0	83.3	50.0	50.0	50.0	33.3	0.0	0.0	16.7	66.7	66.7
(p)サービス業（他に分類されないもの）	162	92.6	63.6	75.3	44.4	50.0	32.7	24.1	17.3	7.4	69.8	60.5
(q)その他	37	100.0	48.6	56.8	35.1	40.5	35.1	18.9	0.0	5.4	43.2	43.2
全業種平均	1878	94.9	67.0	70.6	49.3	41.8	35.7	30.1	19.6	12.9	61.8	57.5

3．ヒアリング調査
結果概要･･･４．支援制度の利用、国等への要請（１/２）

- IPA等が公開している情報を有効活用していることが確認できた
- 監査の簡略化の実現や、対応事項の整理といった観点で、国としての統一的な対応を望む声があった

支援制度の利用、国等への要請の事例

既存支援制度の活用の事例	● IPA提供の中小企業の情報セキュリティ対策ガイドライン、プラクティス集、チェックシート等を活用 • 中小企業の情報セキュリティ対策ガイドラインは、グループ会社におけるセキュリティのチェックに活用 • 中小企業向けのガイドライン、ベストプラクティス、チェックシート等は、中小企業に指導する際に活用。各種セキュリティ部門のメンバーの勉強にも有益
中小企業の企業規模を意識した対応	● セキュリティ部門やIT部門が無いケースもあり、中小企業向けの情報理解促進に向けた無料の相談窓口があると良い ● 中小企業が安価に利用可能な施策の立案 • 中小企業がセキュリティに支出可能なコストを把握した上での施策立案が必要 • 情報セキュリティベンダーのサービスをもっと安価に利用可能となるよう、国家レベルでの取り組みが必要と思料 ● 中小企業においてセキュリティ対策実施の必要性を認識してもらうための取り組み • 社会インフラを守るという意味で、国からトップダウンで各社でのセキュリティ対策実施の必要性を具体的に示すとともに、税制の優遇や、各種施策を手軽に利用できるよう周知していくことが重要 • 中小企業からすると、そもそも各種補助施策を使う必要があるのか判断できないケースも考えられ、中小企業自身が施策利用の必要性を判断できるような形で施策を紹介してもらう必要がある ● 情報セキュリティ分野の補助金について、取引先に対して活用するようにアドバイスできるとよい
サイバーセキュリティに関する監査の簡略化	● 取引先のサイバーセキュリティ対応状況を簡易に判断可能な仕組みの必要性 • サイバーセキュリティの対応状況を判断できる認証制度を設け、ベースラインを達成していなければ取引に参画できない、認証を受けてなければ補助金を受けられないというような、インセンティブとセットでセキュリティが向上するような施策があると良い • RBA※1のサイバーセキュリティ版のような仕組みがあれば、委託側は監査実施の手間を省略でき、受託側は取引をしている複数先から監査を受ける手間を省略することが可能

※1 Responsible Business Allianceの略。加盟する企業が協力し、先進的な基準や手法を用いて労働環境やビジネス活動の向上を図ることを目指す団体

3．ヒアリング調査
結果概要･･･４．支援制度の利用、国等への要請（２/２）

支援制度の利用、国等への要請の事例（続き）

サイバーセキュリティに関する対応事項の整理	● サプライチェーン最上位の企業における、サーバーセキュリティのアシュアランス（何が実現できればセキュリティが担保できるか）や、プラクティス集の提示があると対応がしやすい ● また、アシュアランスの提示やプラクティス集以外にも、動的に変化するリスクへの対応方針を示す必要あり ● 取引先への支援や要請に関して、下請法や独禁法への抵触有無が判断可能となるようなガイドラインや支援の実例を集めたプラクティス集があると望ましい
その他	● サプライチェーン全体での情報公開の仕組みが必要 　• 特定のライブラリの脆弱性が判明した際に、どの製品に当該ライブラリが導入されているかを確認するのには大きな労力とコストを要する 　• サプライチェーンの中でSBOM※2が公開されていれば、容易に対応可能となる ● 人材の流動化によりノウハウが他国に流出するリスクへ対応もあり、不正競争防止の観点で、サイバー攻撃につながるような情報流出を取り締まるような法制度があっても良い ● 公共事業等の入札要件へのセキュリティ要件の組込み ● クラウドサービスの導入により起こり得る問題、サービス水準の合意レベル、運用における責任分界点等についての法制度による明確化

※2 Software Bill Of Materialsの略。特定の製品に含まれるすべてのソフトウェアコンポーネント、ライセンス、依存関係を一覧化したもの

４．調査結果のまとめ

４．調査結果のまとめ
現状の課題

1	企業における リスク認識・対策	**【リスク認識、攻撃被害の状況】** ● 企業は取引先等を経由したサイバー攻撃（Emotet、ランサムウェア、不正アクセス等）の被害影響のリスクを認識しており、実際に影響を受けているケースも多い ● 業界・企業ごとにサプライチェーンの構造・特徴（商材、顧客、活動地域、利用するITサービス等）は異なり、特定・対処するリスクも様々 **【取引先等への要請】** ● 多くの企業は、秘密保持、資産の取扱い、再委託の禁止等、自社で定める基準の適合を求めているが、推奨セキュリティ設定や、特定のサービス導入まで要求しているケースは少ない ● 対策費用の負担、業種・規模・環境・意識レベル等の違い、自社と取引先等との関係性（力関係、取引への影響の懸念）から、サイバーセキュリティに関する要請を行いにくいと考える企業が多い ● 取引先が多岐に渡り個別に対応する負荷が大きいため、各社への対応が十分に実施できない
2	企業における 情報共有、攻撃被害の報告・公表	● 取引先等がサイバー攻撃の被害を受けた際の報告・連絡手順、対応窓口が明確化されていない企業も多い ● IPAやJPCERT/CC等の公的機関から情報収取を実施する企業は多いが、専門家の活用や、情報収集コミュニティを通じた情報取得を実施する企業は一部に留まる ● サイバー攻撃の被害について、個人情報の流出や事業停止といった重大な影響が生じない場合、外部に公表しない企業が多い
3	国等の支援制度	● 「中小企業の情報セキュリティ対策ガイドライン」の活用・認知は比較的進んでいる一方、「サイバーセキュリティお助け隊サービス」「SECURITY ACTION」は5割前後の認知に留まる ● 補助金制度の拡大、強制力を伴う制度の導入、規模の小さい企業向けや特定のテーマに焦点化したガイドラインの提供等のニーズがある

４．調査結果のまとめ
優良事例・取組みの方向性

1	**普及させるべき取組みの優良事例**	**【共通】** ● 取引先等の実態や調達するサービス・商材に応じたリスク評価と対策（自社基準、認証制度等の活用） **【仕入・外注・委託先等】** ● 業界団体・協議会等による、基準の策定やプラクティスの収集とその普及・啓発 ● 委託先等に提供する業務システム（プラットフォーム）を通じた情報提供、教育、アセスメント ● セキュリティ強化のための費用の一部負担 **【グループ会社/海外拠点】** ● グループポリシーの適用（海外拠点の場合等、実態に応じた適用） ● KPIの制定と経営層を含む定期的な会議体運営を通じたPDCA ● 対策費用の一部負担、本社からの稼働提供によるサポート ● 本社経営層主導での対策の強化
2	**企業における情報共有の認識、今後の在り方**	**【情報収集・共有】** ● IPA、JPCERT等の専門機関、業界団体・コミュニティ（ISAC等）を通じた情報収集・共有 ● 取引先等への情報共有の方針の検討 **【攻撃被害の公表】** ● 平時における、攻撃被害の外部公表方針の検討、及びステークホルダーとの共有
3	**企業、国、民間団体等が講ずべき措置の方向性**	**【企業等】** ● 業界団体・協議体等の働きかけによるベースラインの構築と定着 **【国、自治体、関係機関等】** ● 補助金の拡充 ● ガイドラインの提供 ● 相談・情報提供等の窓口の一元化

NTT DATA

Trusted Global Innovator