2023.07.03

サイバーセキュリティニュース ＜2023 No.001＞

サイバーリスク対策および攻撃被害発生時における「情報共有」のポイント

【要旨】
- サイバー攻撃の手法は高度化しており、攻撃を受けた企業・組織が単独で攻撃の全容を解明することは困難である。攻撃被害を未然に防止し、被害を最小限に抑えるためには、平時・有事ともに他の企業・組織との有益かつ適切な情報共有が肝要である。
- 平時においては、外部から把握できる情報を用いて IT 資産を適切に管理する手法を活用して、自社だけでなく、子会社・関連会社・サプライヤーとの対話を推奨する。
- 迅速かつ効果的な有事対応をするために、予め「何のために」「どのような情報を」「どのタイミングで」「どのような主体に対して」情報共有すべきか整理しておくことが必要である。

１．単一企業による対応の限界

サイバー攻撃の手法は高度化しており、攻撃を受けた企業・組織が単独で攻撃の全容を解明することは困難になっている。攻撃者は、取引先やサプライヤーも含めて攻撃対象として偵察活動を行い、脆弱性を発見した上で攻撃手法を確立するといわれている。サイバー攻撃被害を未然に防止、または侵害を早期に検知し、被害を最小限に抑えるためには、攻撃に関する情報、特に「脅威情報」の入手が必要だが、その範囲は自社に限らず取引先やサプライヤーまで拡がるため、単一企業で得られる情報には限界がある。

また、攻撃を受けた際の被害の影響の大小は、インシデント対応の巧拙、すなわち攻撃開始から検知（発覚）および検知（発覚）から復旧までに要する時間によるため、他の企業・組織で発生した同様の攻撃被害情報や技術的な情報がスムーズに共有・活用できることが望まれる。しかし、被害が発生した組織は情報共有に消極的であり、共有されてもそのタイミングは調査後となるケースが多く、有益な情報共有ができていないのが実態である。

現状の課題を解消するために、政府は「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～」と「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を公表した。本稿ではこれらのガイダンスの概要と、有益かつ適切な情報共有のポイントについて解説する。

２．ASM（Attack Surface Management）導入ガイダンスの概要

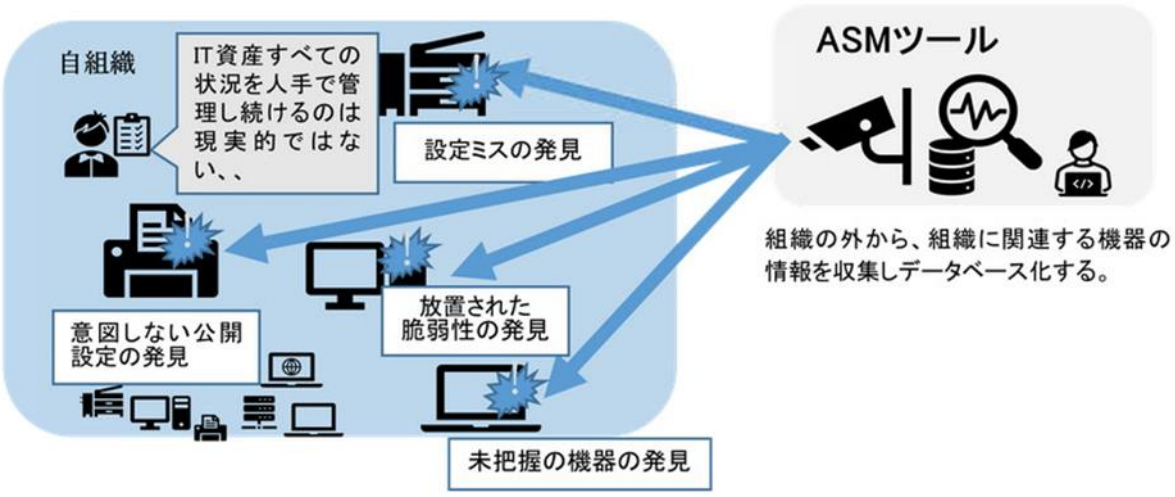
「ASM（Attack Surface Management）導入ガイダンス～外部から把握出来る情報を用いて自組織の IT 資産を発見し管理する～」は 2023 年 5 月 29 日に経済産業省から公表された。

高度化するサイバー攻撃の脅威に対して、自社が保有する IT 資産を適切に管理し、リスクを洗い出すことが求められるが、人手を介した管理の下では、システム管理部門の把握しきれないシステムが生じやすく、機器の実際の設定も見えづらいことなどから、自社の全ての IT 資産を管理するのは必ずしも容易ではない。本ガイダンスでは、サイバー攻撃から自社の IT 資産を守るための手法として注目されている ASM について、自社のセキュリティ戦略に組み込んで適切に活用してもらえるよう、ASM の基本的な考え方や特徴、留意点などの基本情報とともに取組事例などを紹介している。

本ガイダンスでは ASM を「組織の外部（インターネット）からアクセス可能な IT 資産を発見し、それらに存在する脆弱性などのリスクを継続的に検出・評価する一連のプロセス」と定義している。具体的には、外部（インターネット）に公開されているサーバやネットワーク機器、IoT 機器の情報を収集・分析することにより、不正侵入経路となりうるポイントを把握する。ASM を行うことで、以下が

可視化されることが期待される。

- 情報システムを管理している部門が把握していない IT 資産を発見できる
  （例）キャンペーン活動などに利用する Web サイトなど、情報システムを管理している部門以外が構築・運用している IT 資産を発見する
- 情報システムを管理している部門の想定と異なり、公開状態となっている IT 資産を発見できる
  （例）設定ミスなどにより、外部（インターネット）からアクセス可能な状態となっている社内システムなどを発見する
  （例）グループ企業における統制上の課題や地理的な要因によって、本社で一元的に管理できていない IT 資産を発見する



【図１】一般的な ASM の特徴とイメージ
（出典：経済産業省 HP　https://www.meti.go.jp/press/2023/05/20230529001/20230529001.html）

ASM は、主に「（１）攻撃面の発見」「（２）攻撃面の情報収集」「（３）攻撃面のリスク評価」の３つのプロセスで構成される。

（１） 攻撃面の発見
はじめに、企業が保有または管理し、外部（インターネット）からアクセス可能な IT 資産を発見する。具体的には IP アドレス・ホスト名のリストが本プロセスのアウトプットとなる。一般的には以下のような手順で行われる。

① 組織名をもとに、当該組織が管理者となっているドメイン名を特定する。これは、例えば社外に公開している Web サイトや WHOIS（IP アドレスやドメイン名の登録者等に関する情報を参照できるサービス）を利用して特定する。

② 上記①で特定したドメイン名に対して、DNS による検索や、ツールなどを活用して IP アドレス・ホスト名の一覧を取得する。

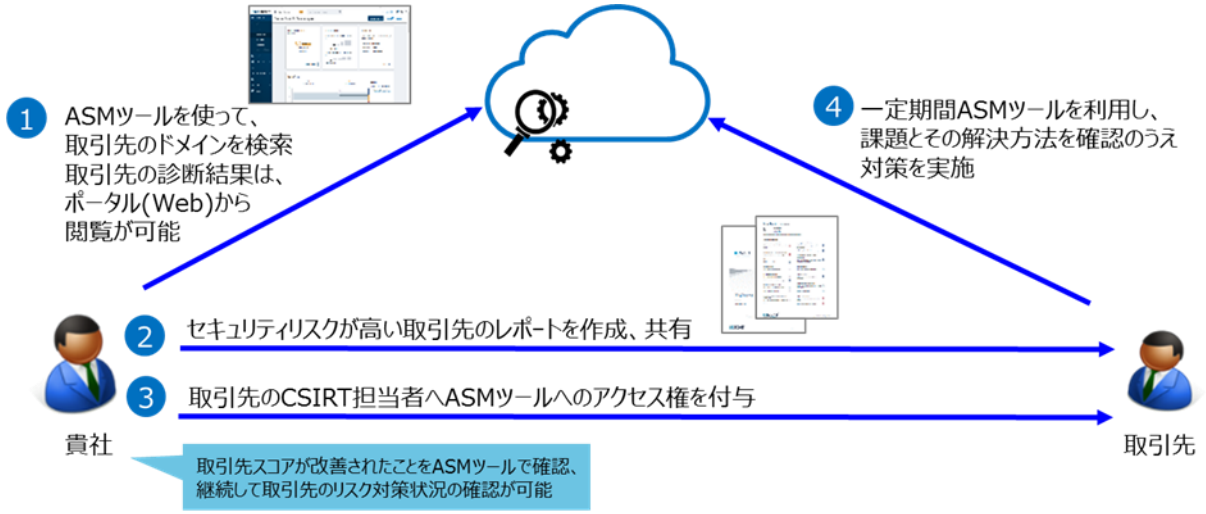
（２）攻撃面の情報収集
上記（１）で発見した IT 資産の情報を収集する。このプロセスで収集する情報には、攻撃面を構成する個々の IT 資産における OS、ソフトウェア、ソフトウェアのバージョン、オープンなポート番号などがある。一般的にこのプロセスは、調査対象に影響を及ぼさないよう、Web ページの表示など通常のアクセスの範囲で行われる。

（３）攻撃面のリスク評価

上記（２）で収集した情報をもとに攻撃面のリスクを評価する。一般的には、公開されている既知の脆弱性情報と、（２）で収集した情報を突合し、脆弱性が存在する可能性を識別する。

上記のプロセスを経て、そのリスクが顕在化した場合に想定される被害と修正にかかるコストを考慮して、パッチ適用（リスクの低減）や対策見送り（リスクの受容）など、脆弱性管理と同様のことを実施する。

ASM はドメイン名が分かればリスク評価ができることから、自社のみならず子会社・関連会社・サプライヤーのセキュリティ対策状況の把握・管理が可能となる。サプライチェーンへのサイバー攻撃によるビジネス中断など、サプライチェーン全体のサイバーリスク対策が企業活動の喫緊の課題となっているなか、ASM ツールを活用した企業間の対話とサプライチェーン全体のセキュリティ向上に活用されたい。



【図２】ASM ツールを活用した取引先との対話のイメージ
（ＭＳ＆ＡＤインターリスク総研が作成）

３．サイバー攻撃被害に係る情報の共有・公表ガイダンスの概要

総務省、内閣サイバーセキュリティセンター（NISC）、警察庁、および政令指定法人 JPCERT コーディネーションセンターが事務局として運営する「サイバーセキュリティ協議会」は、2022 年 5 月に「サイバー攻撃被害に係る情報の共有・公表ガイダンス検討会」を設置し、討議・検討を踏まえて 2023 年 3 月 8 日に「サイバー攻撃被害に係る情報の共有・公表ガイダンス」を公表した。

本ガイダンスは、冒頭で「情報共有」「被害の公表」「行政機関への報告／届出、警察への通報」「取引先や顧客への連絡」を定義、それぞれの持つ意味の違いを解説した上で、速やかな情報共有や被害公表を行うために、予め「何のために」「どのような情報を」「どのタイミングで」「どのような主体に対して」情報共有すべきか、実務上のポイントをまとめている。

【表１】用語の定義

用語	解説
情報共有	サイバー攻撃に関する情報共有のことであり、被害組織で見つかった攻撃技術情報を中心に、非公開の方法で情報共有活動参加組織との間で共有し、そのフィードバックを得ること。 不特定多数の者がまだ認知していなかったり、被害が未公表であったりする個別の攻撃（被害）を特定・調査するために必要なインディケータ情報や、被

	害予防に必要な侵入経路などの TTP 情報[1]を共有する 。
被害の公表	サイバー攻撃被害があったことやどのようなインシデント対応を行ったのかについて公開情報として被害組織が情報発信すること。 法令／ガイドラインに基づく公表のほか、法令等の定めはないものの被害組織自身の判断で行われる公表があり、後者の判断に至る事情は様々で、例えば、以下のようなものがある。 ・　二次被害拡大防止のため注意喚起として行われる公表 ・　サービス停止時など対外的な説明を行う場合の速報的な公表 ・　広報／リーガルリスク対応としての公表
報告	法令に基づき、または任意により、被害事実や対応状況について行政機関に伝えること。
連絡	取引先や顧客等、なんらかの利害関係者に対して攻撃被害が発生したことや、調査結果等を伝えること。個人情報漏えいなどで顧客や取引先に二次被害が発生するおそれがある場合や、調査がある程度終わり、被害内容や取引先へ影響の有無などを伝えるために行う。

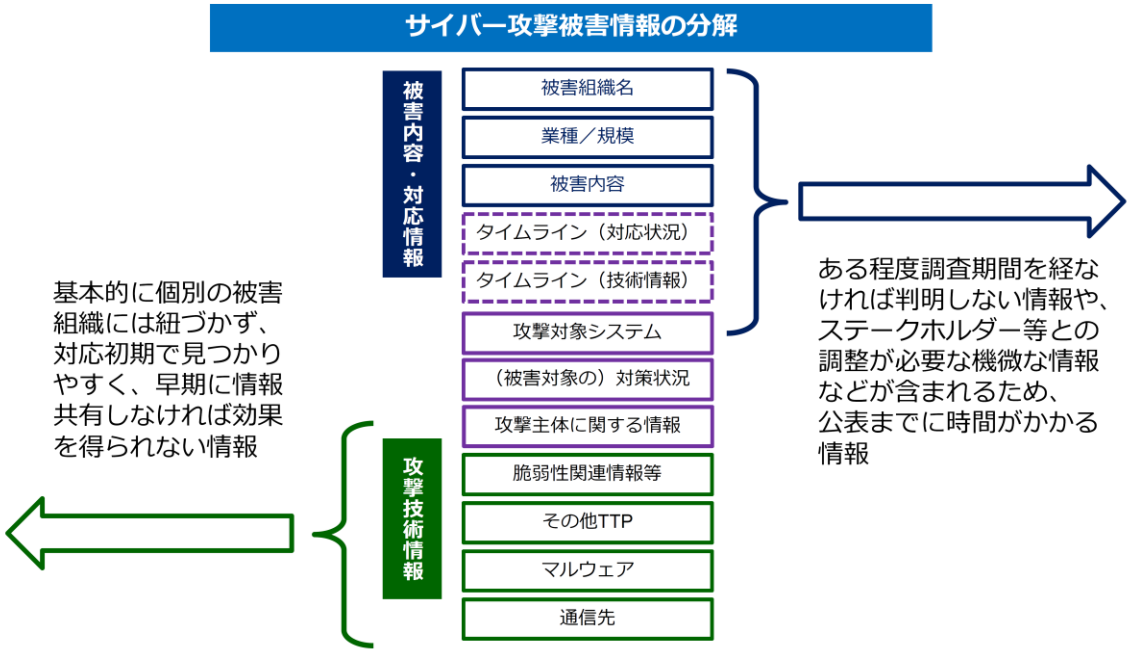
※「サイバー攻撃被害に係る情報の共有・公表ガイダンス」をもとにＭＳ＆ＡＤインターリスク総研が作成

被害組織とサイバーセキュリティ専門組織などとの情報共有は、被害組織にとっても社会全体にとっても非常に有益である一方、被害組織にとっては自組織のレピュテーション（風評）に影響しかねないため、慎重になるケースも多い。情報共有に消極的になる原因は、サイバー攻撃被害に係る情報を外部に知られることで風評リスクなどが想定される「被害そのものを示す情報」と、そうではない「攻撃／攻撃者の活動を示す情報」を切り分けられていないことにある。

本ガイダンスの重要なポイントは、サイバー攻撃に関する情報について、「攻撃／攻撃者の活動を示す情報（攻撃技術情報）」と、「被害そのものを示す情報（被害内容・対応情報）」の２つの情報に切り分けることにある。前者を早期に情報共有することで、被害組織自身の早期の全容解明や、他の組織の被害予防、被害の早期認知、攻撃被害拡大防止に役立てることを意図している。

例えば、攻撃者は一定期間において、攻撃手法や攻撃インフラを使いまわす傾向があるが、被害組織単独による調査だけではそれらの特定は困難である。情報共有活動により「自組織だけでは見つけられなかった情報」を得ることを通じて被害の抑止や拡大防止ができる。

[1] 攻撃者が用いた攻撃手法に関する情報。
「Tactics（戦術）、Techniques（技術）、Procedures（手順）」の略。



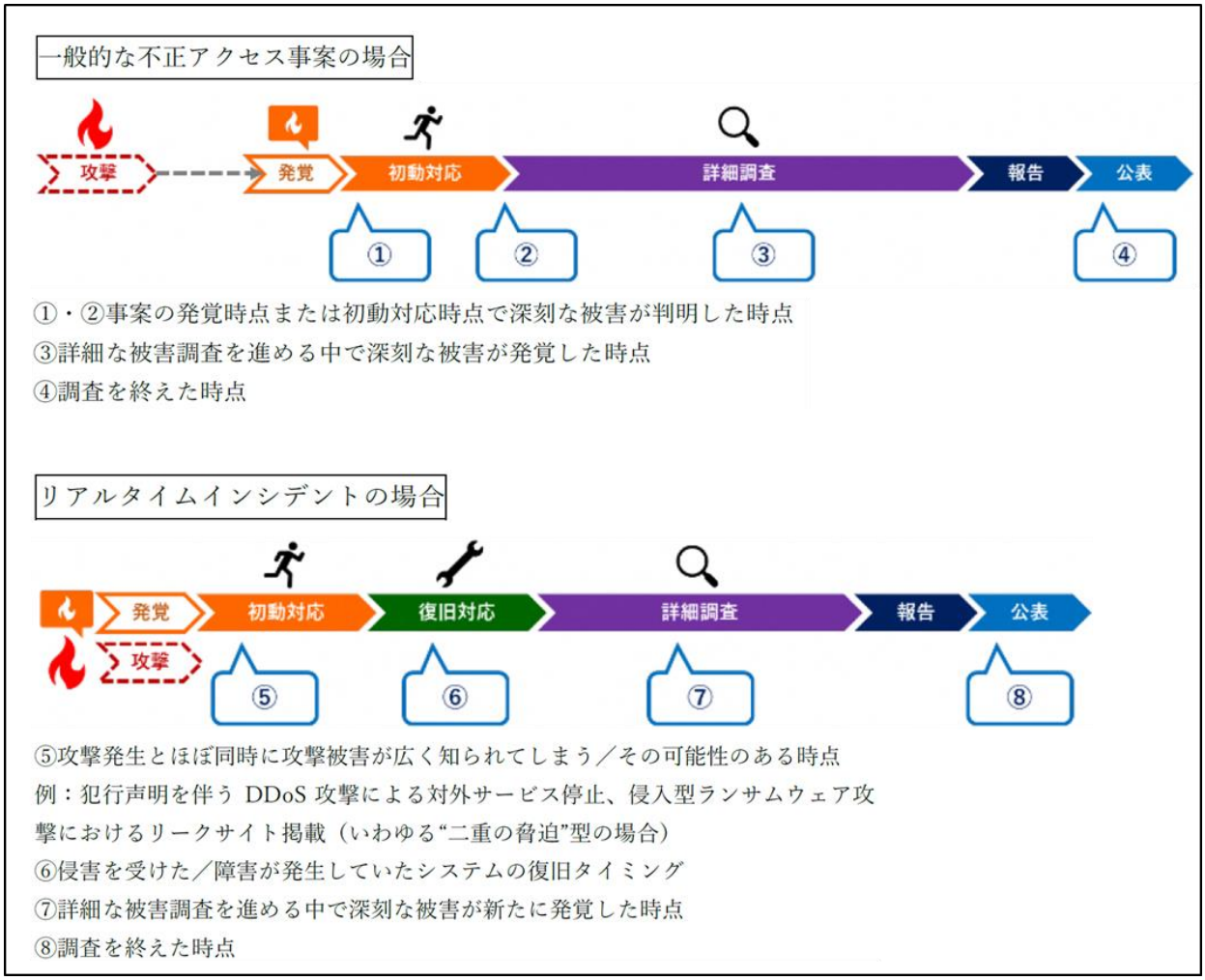
【図３】攻撃技術情報と被害内容・対応情報の分離

（出典：経済産業省「サイバー攻撃被害に係る情報の共有・公表ガイダンス（概要）」）

本ガイダンスでは、公表のあり方や具体的方法については主たる検討対象としていないが、

- 被害組織の公表は、サイバー攻撃被害の実態を目に見える形で社会に示すことによって、脅威の度合いを測るものさしとなり、日本が置かれているサイバー攻撃被害の現状を社会が正しく理解する助けになる
- どのような脅威度合いの攻撃を受け、どのような被害が発生し、どのように対処したのか、被害組織が公表したインシデント対応の内容が正しく評価されるためには、日頃から社会全体においてサイバー攻撃やインシデント対応に関する理解が必要
- サイバー攻撃被害に係る情報の公表により社会全体に対して情報が提供されることで、積極的に被害公表を行った組織に対して、より適切な評価がなされるようになる

と、公表の社会的意義を訴えている。FAQ では、公表の目的のほかにタイミングや公表内容、留意点について実務運用を想定して解説している。



【図４】公表のタイミング
（出典：経済産業省「サイバー攻撃被害に係る情報の共有・公表ガイダンス」）

４．情報共有の活性化に向けた推奨事項

本稿で紹介した２つのガイダンスのほかに、警察庁の有識者検討会は、「サイバー事案の被害の潜在化防止に向けた検討会報告書[2]」において、被害報告の窓口が所管省庁、個人情報保護委員会、警察等多岐にわたっており、報告様式・内容等も異なるため、被害組織等の負担軽減や関係機関等における迅速な情報の把握・共有の観点から、ポータルサイトを設けるなど窓口を一元化（統一化）すべきであると述べている。また、内閣官房が設置するサイバー安全保障体制整備準備室と経団連サイバーセキュリティ委員会は、サイバー安全保障の今後の方向性等について意見交換会を開催、「能動的サイバー防御[3]」導入や民間および政府機関のサイバーセキュリティ強化に向けて、サイバー攻撃を受けた企業の被害情報を官民で共有する仕組み作りの検討を始めた。

本稿で紹介したガイダンスおよび政府の動向を踏まえた、自社および取引先、ひいてはサプライチェーン全体のサイバーセキュリティ強靭化に向けた推奨事項を以下に紹介する。

[2] サイバー事案の被害の潜在化防止に向けた検討会　報告書　2023
https://www.npa.go.jp/bureau/cyber/pdf/20230406_2.pdf
[3] 2022 年末に閣議決定された「国家安全保障戦略」において、導入が宣言されたサイバーセキュリティ政策。今夏以降に有識者会議を設置し、必要な法整備を検討する予定。

（1）リスク管理体制と緊急時対応体制の見直し

組織の内外の関係者間のコミュニケーションは、平時のリスク管理およびインシデント発生を検知した緊急時のいずれにおいても欠かせないものである。国内企業においてもサイバー事故が頻発している近年、インシデント対応手順の整備が進んできているが、この手順に「誰が」「何のために」「どのような情報を」「どのタイミングで」「どのような主体に対して」を着実に落とし込むことが肝要である。

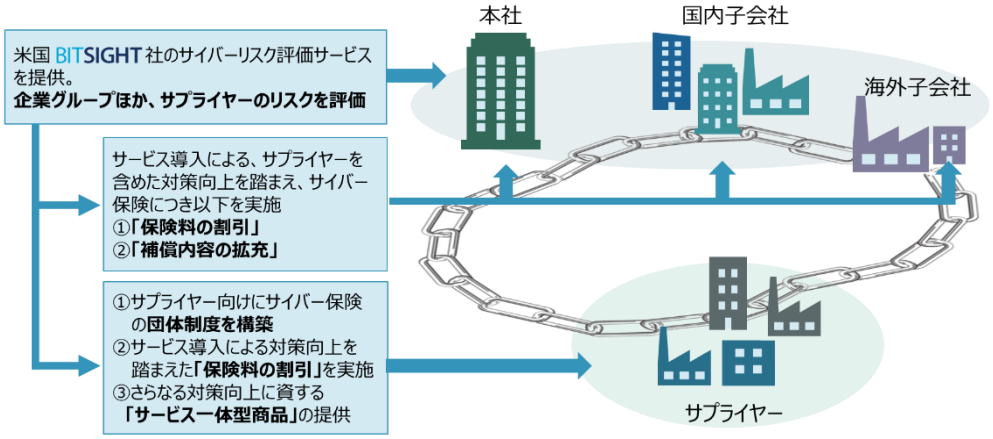
（2）サプライヤーも巻き込んだインシデント対応演習の実施

演習の目的と効果に①基本的なインシデント対応の習得があるが、サプライヤーも演習に参加することで、②演習参加者におけるリスク対策の現状と課題、悩みの共有③「顔が見える」ことにより、有事の連絡・情報共有がよりスムーズになることが期待される。

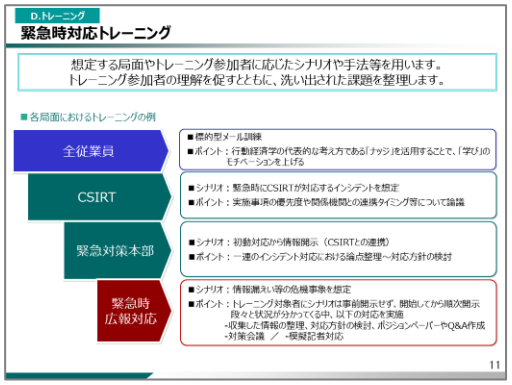
本稿が組織内外における情報共有の必要性への気づきと、実務運用の参考となれば幸いである。

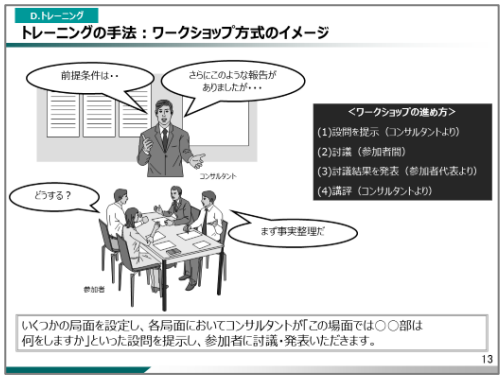
ＭＳ＆ＡＤインターリスク総研株式会社
リスクマネジメント第三部 サイバーリスクグループ
上席コンサルタント　五十嵐　大

ＭＳ＆ＡＤインシュアランス グループの三井住友海上火災保険株式会社、あいおいニッセイ同和損害保険株式会社ならびにＭＳ＆ＡＤインターリスク総研株式会社の３社は、サプライチェーンを取り巻くサイバーリスクに対するソリューションとして、サプライチェーンへのサイバー攻撃対策を包括的に支援するメニューの提供をしています。保険商品・サービスの両面からサプライチェーンのサイバー攻撃対策支援を行うことで、社会課題の解決に取り組んでおります。



また、ＭＳ＆ＡＤインターリスク総研株式会社では、危機発生時において求められる、事実確認、情報共有化、意思決定、対策実行、情報開示に関するトレーニングを企画、お客さまの実践力を検証します。





ＭＳ＆ＡＤインターリスク総研株式会社は、ＭＳ＆ＡＤインシュアランスグループに属する、リスクマネジメントについての調査研究及びコンサルティングに関する専門会社です。
情報セキュリティに関するコンサルティング・セミナー等を実施しております。
コンサルティングに関するお問い合わせ・お申込み等は、下記の弊社お問合せ先、またはあいおいニッセイ同和損保、三井住友海上の各社営業担当までお気軽にお寄せ下さい。

お問い合せ先
ＭＳ＆ＡＤインターリスク総研㈱
リスクマネジメント第三部 サイバーリスクグループ
東京都千代田区神田淡路町2-105 **TEL.03-5296-8932**
https://www.irric.co.jp/