DIR SOC Quarterly vol.3

2023 ❄ winter

大和総研
Daiwa Institute of Research

目次

はじめに

本冊子は、サイバー攻撃の状況と対策の動向をタイムリーにお伝えすることを目的としています。今回は、2022 年度第 3 四半期の話題を取り上げます。

本冊子は三部構成となっています。第 1 部はサイバー攻撃対策が国家主導の下に行われており、それを指揮する行政機関の動向をウォッチすることが不可欠であるため、この点にフォーカスしています。また実際のインシデント事例は、組織がさらされているサイバー攻撃の状況を端的に示すと同時に、組織の対策のあるべき姿を浮かび上がらせるものです。第 2 部はこの点に注目しています。また第 3 部では、注目度の高いサイバーセキュリティ関連の話題をトピックスとして詳しく説明します。

今回の第 1 部では第 3 四半期におけるわが国の政策・法制度の動向を取り上げます。クラウド化、IoT 活用など、外部サービスとの接続機会が増加し、「Society 5.0」に向けて急速にその姿を変えつつある産業界の取り組みとして、ビルシステムおよび工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインが公開されました。これにより、産業界のサプライチェーン・サイバーセキュリティ確保のための枠組みを整理したと言えます。また昨今サプライチェーンが狙われ、業務停止に追い込まれた事例を受け、『サイバーセキュリティ経営ガイドライン Ver3.0（案）』等を通して、経営者に対するサプライチェーンのセキュリティ対策への関与の必要性が強く示されています。加えて金融庁「企業内容等の開示に関する内閣府令」等の改正案から見えるサステナビリティ情報の開示では、議論の俎上にあがっているサイバーセキュリティ情報の有用性と課題について紹介します。

第 2 部では第 3 四半期に注目を集めたインシデント事例を取り上げます。今回紹介する事例は、多発している医療機関に対するサイバー攻撃において、サプライチェーン上の脆弱性を悪用された典型的なインシデントであるととらえています。

最後に第 3 部では国内で広がりを見せている「セキュリティインシデント対応を行う組織である xSIRT」等について解説します。わが国では PSIRT、FSIRT、DSIRT 等を構築する取り組みがある中で、『サイバーセキュリティ経営ガイドライン』の中で、経営層主導の下、CSIRT 等の構築を強く促しています。

上記トピックスのいずれかが皆様の日々の活動に関連する何らかの「気づき」や「きっかけ」となれば幸いです。

2023 年 1 月　株式会社大和総研執筆者一同

1. ビルシステムおよび工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドラインの公開

二つのサイバー・フィジカル・セキュリティ対策ガイドラインの公開

現在、サイバー空間とフィジカル空間が密接にかかわりあい、高度に融合する社会「Society 5.0」(*1)が到来しつつあります。この結果、すべての業界・業種・組織にてこのようなサイバー空間とフィジカル空間をまたいだセキュリティ対策を検討すべき状況が発生しつつあります。「サイバー・フィジカル・セキュリティ」は、「Society 5.0」において増大するサイバー攻撃の脅威に対応するために政府が推進しようとしている施策のキーワードとなっています。政府のサイバーセキュリティ戦略本部が 2022 年 6 月に決定した『サイバーセキュリティ 2022（2021 年度年次報告・2022 年度年次計画）』でも政府が特に強力に取り組むべき施策の一つとしてサイバー・フィジカル・セキュリティ対策があげられています。

経済産業省は 2022 年 10 月 24 日、『ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（個別編：空調システム）第 1 版』を公開し、2022 年 11 月 16 日には『工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.0』を公開しました。

本記事では、サイバー・フィジカル・セキュリティについて検討している経済産業省の産業サイバーセキュリティ研究会やそのサブワーキンググループが公開するガイドラインの位置づけなどに触れた上で、今回公開された前述の二つのガイドラインについて紹介します。

産業サイバーセキュリティ研究会とその構成

「産業サイバーセキュリティ研究会」（以下研究会）は、産業界が直面するサイバーセキュリティの課題を洗い出し、関連政策を推進していくため、産業界を代表する経営者、インターネット時代を切り開いてきた学識者等から構成されています(*2)。

また、研究会内にはワーキンググループやサブワーキンググループ、タスクフォースなどが存在しています。今回、前述の二つのガイドラインを策定したビルサブワーキンググループと工場サブワーキンググループは図 1 の赤枠の部分に位置しています。

(*1) 内閣府「Society 5.0 とは」（https://www8.cao.go.jp/cstp/society5_0/index.html）

(*2) 第 1 回 産業サイバーセキュリティ研究会　資料 3　産業サイバーセキュリティ研究会の設置について
（https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/pdf/001_03_00.pdf）

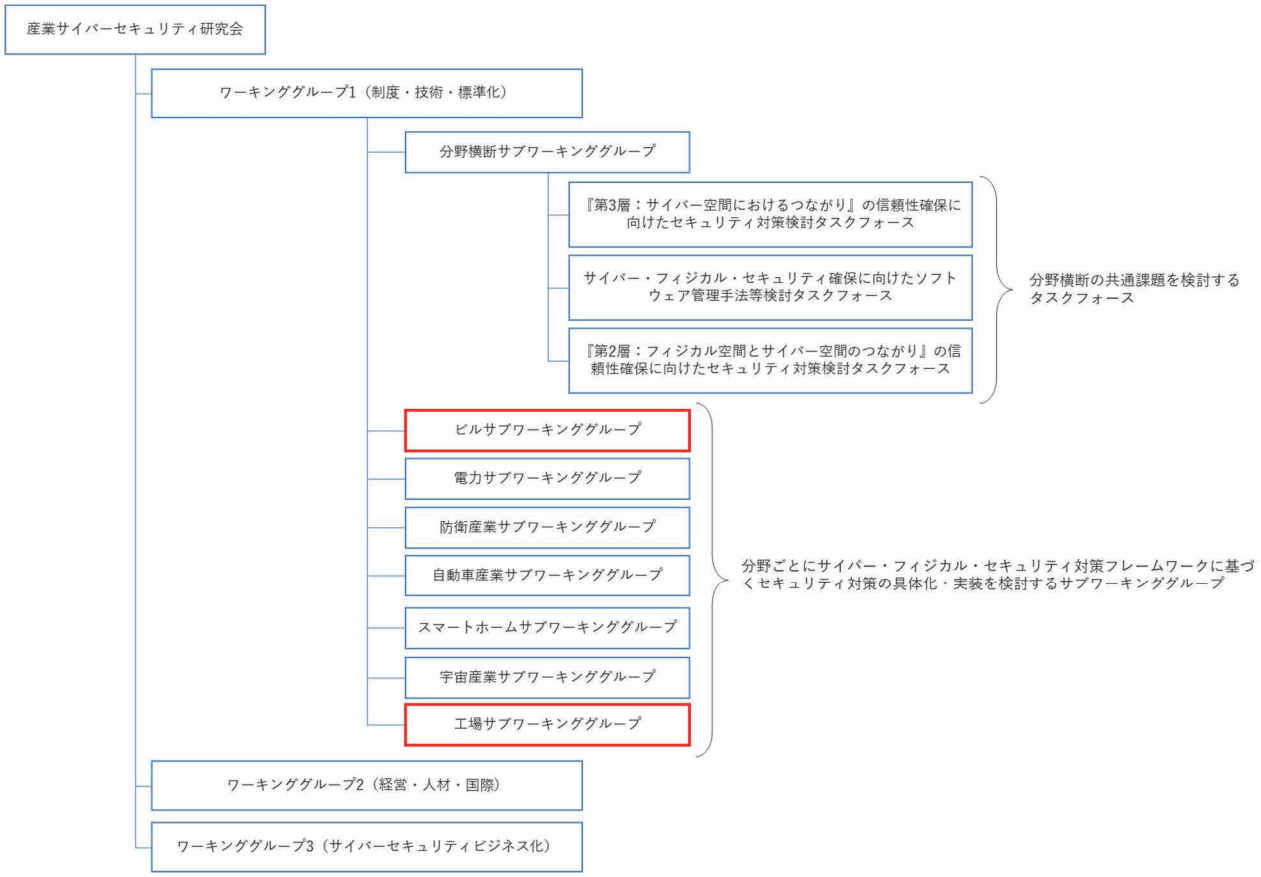


図 1：産業サイバーセキュリティ研究会の構成

出典：第 9 回 産業サイバーセキュリティ研究会 ワーキンググループ 1（制度・技術・標準化）第 7 回 WG1 分野横断サブワーキンググループ 合同会議　資料 4　事務局説明資料 (*1) に掲載の図を基に大和総研作成

なお、前掲の図 1 中の分野横断サブワーキンググループ内のタスクフォース名称にある「第 2 層」や「第 3 層」とは、『サイバー・フィジカル・セキュリティ対策フレームワーク Ver1.0』（以下 CPSFv1.0）で提唱されている「三層構造モデル」における第 2 層と第 3 層のことです。CPSFv1.0 は「Society 5.0」、「Connected Industries」における新たなサプライチェーン全体のセキュリティ確保のため、前掲の図 1 中のワーキンググループ 1 で検討した結果を踏まえて経済産業省が 2019 年 4 月に策定したものであり、産業社会を三つの層（三層構造モデル）でとらえてセキュリティを確保していくアプローチを提示しています。詳細は研究会の Web サイト(*2)もしくは DIR SOC Quarterly 2022 the first issue(*3)でも取り上げていますのでご参照ください。

(*1) https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/009_04_00.pdf

(*2) https://www.meti.go.jp/policy/netsecurity/wg1/cpsf.html

(*3) https://www.dir.co.jp/publicity/publication/socquarterly2210.html

経済産業省が公開するガイドライン類

研究会およびその他の経済産業省関連組織が公開したガイドライン類は数多くありますが、下図のような関係になっています。前述の CPSFv1.0 は経営層から実務層まで幅広い読者に対して抽象的なコンセプトを提示しているのに対して、各サブワーキンググループが策定するサイバー・フィジカル・セキュリティ対策ガイドラインは産業分野個別の実務層向けに、より具体的な対策を提示していることが分かります。

図 2：経済産業省が公開するガイドラインの関係

出典：第 9 回 産業サイバーセキュリティ研究会 ワーキンググループ 1（制度・技術・標準化）第 7 回 WG1 分野横断サブワーキンググループ 合同会議　資料 4　事務局説明資料 (*1)

ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（個別編：空調システム）第 1 版

ビルシステムにおけるガイドラインはこれまで共通編の位置づけとして『ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン第 1 版』(*2)がありましたが、今回は空調システムに特化した個別編として『ビルシステムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン（個別編：空調システム）第 1 版』(*3)が公開されました。今後、これ以外の個別システムについても個別編を公開していく予定のようです。

(*1) https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/pdf/009_04_00.pdf

(*2) https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20190617_report.html

(*3) https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_building/20221024_report.html

今回公開された個別編では、空調システムの特徴や実際のサイバー攻撃事例を記載した後に、空調システムにおけるセキュリティ対策の考え方、リスクとそのリスクに対応するためのセキュリティポリシー、設備のライフサイクル（設計、建設、運用、改修・廃棄など）を考慮した具体的なセキュリティ対策などを記載しています。なお、空調システムに特化した記載にはなっていますが、サイバーセキュリティ対策の初歩的な対策をまとめたものである点や検討の糸口であってマストではない点から、これをもとにそれぞれの状況や立場に応じて工夫・改善をして欲しいという点が強調されています。

工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.0

工場における産業制御システム(ICS/OT)を対象としたガイドラインが『工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.0』(*1)です。このガイドラインでは、セキュリティ対策を企画・導入する際の進め方として、事業環境や技術動向の変化等に応じて次の各ステップについて不断の見直しを行いながら継続的に PDCA サイクルを回していくことが重要であるとしています。

ステップ 1：内外要件（経営層の取組や法令等）や業務、保護対象等の整理

ステップ 2：セキュリティ対策の立案

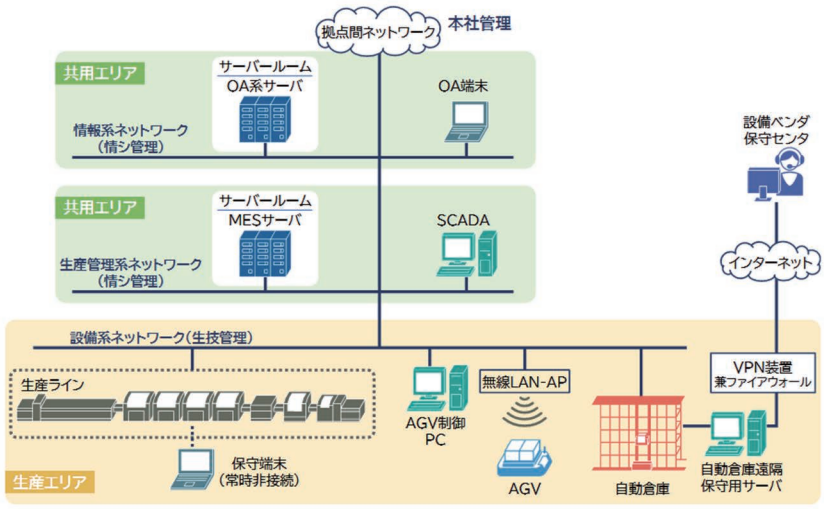
ステップ 3：セキュリティ対策の実行、及び計画・対策・運用体制の不断の見直し

特徴的な点としては、分かりやすさを考慮して想定工場を設定し、対策や取り組みの具体例として随所に記載している点があげられます。ただし、読者の置かれた環境と想定工場とが必ずしも一致しない部分もあると考えられるため、読者の環境に応じて適宜読み替えることが求められます。

想定されている工場は電子機器メーカーのものであり、スマートファクトリーのレベル 1 (*2)相当とされています。設備系ネットワーク、生産管理系ネットワーク、情報系ネットワークが相互に接続され、さらには設備ベンダーがインターネット経由で VPN 接続する構成となっており、サイバーセキュリティのリスクが少なからず存在する典型的な工場が想定されていると言えます。（図 3）

(*1) https://www.meti.go.jp/policy/netsecurity/wg1/factorysystems_guideline.html

(*2) 第 1 回 産業サイバーセキュリティ研究会　ワーキンググループ 1（制度・技術・標準化） 工場サブワーキンググループ　参考資料 2　令和 2 年度スマートファクトリーにおけるサイバーセキュリティ確保に向けた調査報告書
(https://www.meti.go.jp/shingikai/mono_info_service/sangyo_cyber/wg_seido/wg_kojo/pdf/001_s02_00.pdf)



左図の略語について

- MES(Manufacturing Execution System): 製造実行システム
- SCADA(Supervisory Control And Data Acquisition): 監視制御
- AGV(Automatic Guided Vehicle): 無人搬送車

図 3：想定工場のシステム例

出典：『工場システムにおけるサイバー・フィジカル・セキュリティ対策ガイドライン Ver 1.0』

二つのサイバー・フィジカル・セキュリティ対策ガイドラインからの示唆

サイバー空間とフィジカル空間の融合は至る所で進行しています。たとえば農場もハッキングされる時代になったとの報告(*1)もあります。このような状況やサイバー攻撃の種類が多様になってきていることに鑑み、政府も「サイバー・フィジカル・セキュリティ対策」を推進しています。経済産業省はこれまで複数の分野で「サイバー・フィジカル・セキュリティ対策ガイドライン」を策定していますが（5 ページの図 2）、このようなガイドラインが策定されていないような業界・業種についても、サイバー攻撃によるサイバー空間とフィジカル空間の双方に対する影響や被害を想定し、セキュリティ対策を検討しておくべきと言えるでしょう。たとえばキーボードに残った「指の熱」でパスワードを盗む攻撃手法についての論文が発表される(*2)などしていますので、オフィス空間については今までとは異なった考慮が必要になってくるかもしれません。今後は、これまでフィジカル空間とのつながりがあまりなかった業態においても、自社の環境についてセキュリティ対策を見直していく必要があるでしょう。

(*1) 『Tractors vs. threat actors: How to hack a farm』(https://www.welivesecurity.com/2022/12/05/tractors-threat-actors-how-hack-farm/)

(*2) 日経クロステック「キーボードに残った『指の熱』でパスワードを盗む、6 文字なら 100％的中」
https://xtech.nikkei.com/atcl/nxt/column/18/00676/101500117/

2. 『サイバーセキュリティ経営ガイドライン Ver3.0(案)』に対する意見募集

サイバーセキュリティ経営ガイドライン

経済産業省と独立行政法人情報処理推進機構（IPA）は 2022 年 10 月 26 日、「サイバーセキュリティ経営ガイドライン Ver3.0（案）」(*1)に対する意見公募手続（パブリックコメント）を開始しました（12 月 5 日終了）。今後、パブリックコメントの結果を踏まえた内容が公表されることが予想されます（初版は 2015 年、Ver2.0 が 2017 年に公開）。

近年、企業のサイバーセキュリティ対策では「テレワークを代表とするデジタル環境の活用を前提とした働き方の多様化」、「サイバー攻撃による事業活動停止にまで及ぶ影響の拡大化」、「サプライチェーンを介して連鎖する被害の甚大化」等の大きな変化への対応を迫られていることが議論されています。これらを踏まえ、最新の状況へ記載内容の見直しが行われました。

ガイドラインの構成

このガイドラインは経営者を想定読者としており、「経営者が認識すべき 3 原則」と経営者がセキュリティ担当幹部などへ向けて指示すべき「サイバーセキュリティ経営の重要１０項目」で構成されています。以降では、改定のポイントであり国内外で急速に関心が高まっている「サプライチェーン」と、事業活動の継続のためインシデント発生時の対応に結び付く「CSIRT の整備」を取り上げます。

【経営者向け】3 原則	
原則 1	サイバーセキュリティリスクを重要課題と認識し、経営者のリーダーシップが重要
原則 2	サプライチェーン全体にわたる自社以外（ビジネスパートナー）にも配慮
原則 3	平時から関係者との積極的なコミュニケーション・情報共有
【担当者向け】重要 10 項目	
指示 1	サイバーセキュリティリスクの認識、組織全体での対応方針の策定
指示 2	サイバーセキュリティリスク管理体制の構築
指示 3	サイバーセキュリティ対策のための資源（予算、人材等）確保
指示 4	サイバーセキュリティリスクの把握とリスク対応に関する計画の策定
指示 5	サイバーセキュリティリスクに効果的に対応する仕組みの構築
指示 6	PDCA サイクルによるサイバーセキュリティ対策の継続的改善
指示 7	インシデント発生時の緊急対応体制の整備
指示 8	インシデントによる被害に備えた事業継続・復旧体制の整備
指示 9	ビジネスパートナーや委託先等を含めたサプライチェーン全体の状況把握及び対策
指示 10	サイバーセキュリティに関する情報の収集、共有及び開示の促進

表：『サイバーセキュリティ経営ガイドライン Ver3.0（案）』から抜粋して大和総研が作成。下線は変更が加わった主な箇所。

(*1) 経済産業省、独立行政法人 情報処理推進機構 「サイバーセキュリティ経営ガイドライン Ver3.0 (案)」（https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000242524）

サプライチェーンにおけるサイバーセキュリティの強化

改定の主な点として、サプライチェーン関係者または全体を考慮する必要性が、原則 2、指示 7、指示 8、指示 9 に追記されました。また「サプライチェーン」という単語は 36 回登場し、Ver2.0 の 22 回と比較すると約 1.6 倍に増えており、政府および民間がサプライチェーンリスクへの“懸念”から社会全体で取り組む“課題”として認識すべきと示唆しています。

サプライチェーンは一般に製品やサービスが消費者の手元に届くまでの、調達、製造、配送、販売といった一連の流れのことをいいますが、それぞれの工程を系列企業やビジネスパートナーなどに委託や業務提携することで実現します。この形態では、自社と異なり、他社に対してセキュリティルールや運用方法、対策手法を統制する権限がない点に管理の難しさがあります。しかし、特に昨年は、トヨタ自動車の仕入れメーカー小島プレス工業への攻撃により、事業活動の停止まで至った事例もありました。10 月には、大阪急性期・総合医療センターの給食事業者への攻撃も発生するなど、サプライチェーンリスクは急速に高まっています。サプライチェーンリスクに目を向けず、安定した事業活動を継続することは困難な状況になったと言えるでしょう。

経団連サイバーセキュリティ経営宣言 2.0

注目したいのは、同時期に経団連（一般社団法人 日本経済団体連合会）からもサプライチェーン全体を俯瞰したサイバーセキュリティの強化を強調した「経団連サイバーセキュリティ経営宣言 2.0」が発表されたことです（2022 年 10 月 11 日改定）。

経団連サイバーセキュリティ経営宣言は、経済界が全員参加でサイバーセキュリティ対策を推進し、安心・安全なサイバー空間の構築に貢献することを目的として 2018 年 3 月に策定されました。経営層の危機意識を高める観点から、国内外の最新情勢を踏まえ、この度、本経営宣言が改定されました。

「経団連サイバーセキュリティ経営宣言 2.0」では、経営者が取り組むべき 5 項目のうち、「経営課題としての認識」と「安心・安全なエコシステムの構築への貢献」の 2 項目について、それぞれ「サプライチェーン全体を俯瞰したサイバーセキュリティの強化」、「サプライチェーン全体」が明記されました。これは、経営者がサイバーセキュリティ対策を講じ責任をもって取り組む内容として、ビジネスパートナーを含めたサプライチェーンリスクへの対策の必要性をメッセージとして強く打ち出したということです。

このように、経団連の「経団連サイバーセキュリティ経営宣言 2.0」と「サイバーセキュリティ経営ガイドライン」は、経営者の強い関与をもってサイバーセキュリティ全体を俯瞰し総合的なセキュリティを徹底する点で方向性が一致していることが読みとれます。

サプライチェーンにおける CSIRT への期待

本ガイドラインの改定では、前述したようにサプライチェーン全体への対応の必要性が明記されました。さらに注目したいのは、サイバー攻撃から社会全体を守るための社外とのコミュニティネットワークとそれを支える CSIRT（第 3 部 トピックス「xSIRT」で取り上げて説明します）の役割です。

「指示 7」では、内容は大きく見直されていないものの、CSIRT を代表としたサプライチェーン全体のインシデントに対応可能な体制の整備、「指示 10」では、情報を入手するのみならず、サイバー攻撃に関する情報やインシデントに備えた日頃の取り組みなどを積極的に発信することを経営者がセキュリティ幹部に対して指示すべきだと推奨しています。

この情報連携は、日本シーサート協議会などのコミュニティ活動への参加を通じて行うことができますが、CSIRT 間の直接的な連携も期待され、今後重要な役割を担っていくと考えられます。

「サイバーセキュリティ経営ガイドライン Ver3.0 (案) 」の内容(*1)

> 指示 7　インシデント発生時の緊急対応体制の整備
>
> 影響範囲や損害の特定、被害拡大防止を図るための初動対応、再発防止策の検討を適時に実施するため、制御系を含むサプライチェーン全体のインシデントに対応可能な体制（CSIRT 等）を整備させる。
>
> 指示 10　サイバーセキュリティに関する情報の収集、共有及び開示の促進
>
> 有益な情報を得るには自ら適切な情報提供を行う必要があるとの自覚のもと、サイバー攻撃や対策に関する情報共有を行う関係の構築及び被害の報告・公表への備えをさせる。

(*1) 経済産業省、独立行政法人 情報処理推進機構 「サイバーセキュリティ経営ガイドライン Ver3.0 (案) 」（https://public-comment.e-gov.go.jp/servlet/PcmFileDownload?seqNo=0000242524）

セキュリティインシデントは日々高度化・巧妙化しています。また、複雑化する技術の利用にともなって発生する脆弱性、未知のサイバー攻撃（ゼロデイ攻撃）などにも注意を払う必要があります。もはや自社内で閉じた情報収集やセキュリティ対策では不十分である可能性が高く、既に限界に来ていると言えます。サイバーセキュリティ分野は競争分野ではなく、非競争分野・“共助”の分野であることに意識を変えていく必要があるでしょう。それには、情報を集約・発信する役割を担う CSIRT などの組織的な専門部隊をつくることから始めることが有効だと考えます。

本ガイドラインからの示唆

いまやサプライチェーンは企業や国境を越えてつながり、情報とモノが行き交います。これは、その分だけ攻撃対象が増えることを意味します。セキュリティ対策において、「鎖は一番弱い輪以上に強くなれない(*1)」や「セキュリティ桶の理論(*2)」という言葉があります。両者が意味していることは同様で、前者はどれだけ一部のセキュリティを強化しても脆弱な部分があると全体としてセキュリティが弱くなってしまうことを表しており、後者は桶に溜まる水のように、セキュリティは一番弱いところから破られる（水が漏れてしまう）ことを表しています。自らの目が届く範囲だけ強化しても全体のセキュリティとしては不十分だと言え、いかにサプライチェーンに連なる組織（一番弱い輪）を適切に可視化するか、問題があればどう改善・支援していくのかをきちんとプロセス化できるかが重要です。

このように、サイバーセキュリティ対策について経営者に係る責任やセキュリティ担当者の負担が拡大していくことが見込まれます。前号のトピックスでも触れた「SBOM」を例として、サプライチェーンに関する組織、モノ、ヒトを管理するツールの積極的な活用が必要になる時期に来ていると言えるでしょう。

(*1)(*2) 日経 XTEC 情報セキュリティ・マネジメントと ISMS
（https://xtech.nikkei.com/it/article/COLUMN/20070522/271848/）

3. 『サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて』の公表

サプライチェーン全体のサイバーセキュリティ向上

公正取引委員会と経済産業省は 2022 年 10 月 28 日、「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」と題したガイドラインを公表しました。昨今、サイバーセキュリティ対策が不十分な中小企業が踏み台としてサイバー攻撃に狙われ、サプライチェーン全体に問題が波及する事態が発生しています。サイバーインシデントによってサプライチェーンが分断され、物資やサービスの安定供給に支障が生じることのないよう、中小企業等におけるサイバーセキュリティ対策を支援するための施策と、取引先への対策の支援・要請に係る独占禁止法および下請法の考え方について上記ガイドラインでは整理されています。

中小企業等におけるサイバーセキュリティ対策

経済産業省及び独立行政法人情報処理推進機構（IPA）は、中小企業等がサイバーセキュリティ対策を講じることを支援するため、以下の施策を整備しています。政府としても、IT 導入補助金(*1)の対象とするなど普及を後押ししています。また、一民間の取引において、発注側が取引先にこうした施策の活用を促していくことを期待しています。

サイバーセキュリティ対策に関する支援策	支援策の概要
サイバーセキュリティお助け隊サービス	中小企業等に対するサイバー攻撃への対処として不可欠なサービスをワンパッケージで安価に提供するサービス。サービス内容としては見守り（24 時間監視し攻撃を検知）、駆付け（問題が発生した際に IT 事業者が対応）、保険（サイバー攻撃による被害対応コストを補償）などがある。
セキュリティアクション	中小企業等が、自ら情報セキュリティ対策に取り組むことを自己宣言する制度。本宣言を通じて、中小企業等がサイバーセキュリティ対策に積極的に取り組んでいることを広く社会にアピールすることが可能になる。
中小企業の情報セキュリティ対策ガイドライン	本ガイドラインは、中小企業等を対象に、情報セキュリティ対策に取り組む際の、経営者が認識し実施すべき指針と社内において対策を実施する際の手順や手法をまとめたもの。
サプライチェーン・サイバーセキュリティ・コンソーシアム	中小企業等のサイバーセキュリティ対策やインシデント対応について、経営者へのインタビュー形式でまとめた事例集を作成し、中小企業等の経営者の意識改革に取り組んでいる。本コンソーシアムには 2022 年 9 月時点で 175 の業界団体等が参加する。
パートナーシップ構築宣言	サプライチェーンの取引先や価値創造を図る事業者の皆様との連携・共存共栄を進めることで、新たなパートナーシップを構築することを、発注者側の立場から宣言するもの。宣言に際し、取引先に対するサイバーセキュリティ対策の助言・支援等は、サプライチェーン全体の共存共栄と規模・系列等を超えた新たな連携の一つとして例示されている。

表：「サプライチェーン全体のサイバーセキュリティ向上のための取引先とのパートナーシップの構築に向けて」を基に大和総研作成

(*1)中小企業等が IT ツールを導入する経費の一部を補助することで業務効率化をサポートする補助金

取引先への対策の支援・要請についての考え方

中小企業等との取引において、発注側は取引先へのサイバーセキュリティ対策の実施（例：有償のセキュリティサービスの利用、セキュリティ認証の取得、セキュリティ体制の構築）を要請することについて、独占禁止法の優越的地位の濫用や下請法上、問題とならないかといった点に注意する必要があります。そのため、本ガイドラインでは、取引先への対策の支援・要請にあたっての独占禁止法および下請法の考え方を整理しています。

サプライチェーン全体としてのサイバーセキュリティ対策の強化は、重要な取り組みであるため、サイバーセキュリティ対策の実施を要請することは、直ちに独占禁止法や下請法上の問題となることはありません。ただし、要請の方法や内容によっては、強要とみなされ、問題となることもあるため注意が必要です。本ガイドラインでは、問題となるおそれがある三つのケースが示されています。

（1） 取引の対価の一方的決定

発注側が取引先に対してサイバーセキュリティ対策の要請を行い、取引先に生じるコスト上昇分を考慮することなく、価格改定に応じない場合

（2） セキュリティ対策費の負担の要請

発注側が取引先に対してサイバーセキュリティ対策の要請を行い、当該セキュリティ対策費の算出根拠、使途などについて取引先との間で明確にしないで、発注側が取引先に対し合理的な範囲を超えた作業を求める場合

（3） 購入・利用強制

発注側が取引先に対してサイバーセキュリティ対策の要請に際して、取引先が同等またはそれ以上の対策を実施しているにもかかわらず、発注側が指定するセキュリティサービスの利用を強制する場合

本ガイドラインからの示唆

中小企業等では、IT 導入補助金を活用し、サイバーセキュリティ対策を講じることができます。これら政府の施策を賢く活用し、まずはできるところからサイバーセキュリティ対策を進めていくことが大切です。ただし発注側においては、取引先に対しサイバーセキュリティ対策の実施を要請する場合、独占禁止法や下請法に抵触しないよう十分に注意する必要があります。

4. サイバーセキュリティを含むサステナビリティ情報の開示

「企業内容等の開示に関する内閣府令」等の改正案の公表

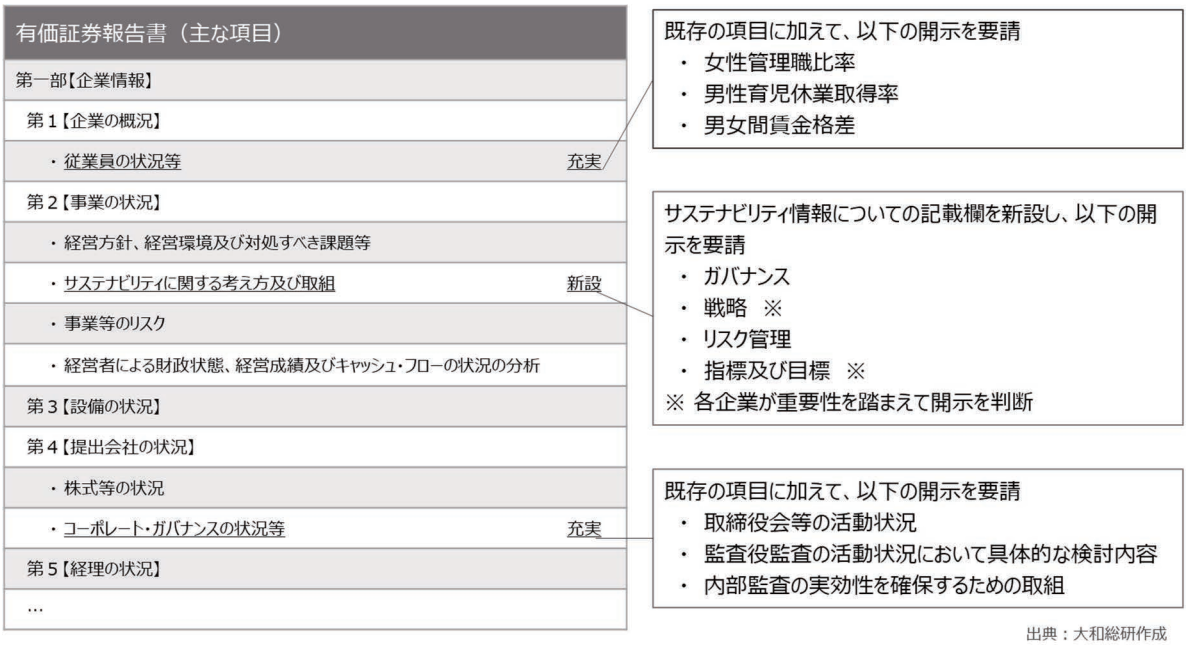
金融庁は有価証券報告書において、サステナビリティ・コーポレートガバナンス情報の開示を追加した「企業内容等の開示に関する内閣府令」等の改正案(*1)に対する意見公募手続（パブリックコメント）を行いました（2022 年 11 月 7 日開始、12 月 7 日終了）。

これは、6 月 13 日の金融審議会 ディスクロージャーワーキング・グループ報告（以降、ディスクロージャーWG 報告）の提言を踏まえたもので、改正案では、3 月期決算企業に対して 2023 年 3 月 31 日以後に終了する事業年度に係る有価証券報告書等から開示を求めています。

【有価証券報告書の記載事項についての主な改正案】

1. サステナビリティに関する企業の取組みの開示
   - サステナビリティ全般に関する開示
   - 人的資本、多様性に関する開示
2. コーポレートガバナンスに関する開示
   - 取締役会や指名委員会の活動状況等の開示

【改正案の概要】



出典：大和総研作成

(*1) 金融庁 「企業内容等の開示に関する内閣府令」等の改正案の公表について
（https://www.fsa.go.jp/news/r4/sonota/20221107/20221107.html）

サステナビリティ情報に含まれるサイバーセキュリティ

改正案では、サステナビリティ情報は環境、社会、従業員、人権の尊重などといった、いわゆる ESG の基本的な内容に加えて、「サイバーセキュリティ、データセキュリティ」も含まれ得る、との見解が示されています。元々、サステナビリティ情報に明確な定義はなかったのですが、SASB（Sustainability Accounting Standards Board, サステナビリティ会計基準審議会）及びその後継である ISSB（International Sustainability Standards Board, 国際サステナビリティ基準審議会、2021 年 11 月 3 日設立）がサステナビリティ情報の大枠を整理したことから踏み込んだ記述になりました。

SASB のマテリアリティマップ(*1)には、サイバーセキュリティではなく、データセキュリティの項目があります。データセキュリティが注目された背景は、中国やロシアなどによる大規模なハッキングが社会問題化したことだと考えられます。また、個人情報が人権問題として取り扱われ、EU で GDPR（General Data Protection Regulation,一般データ保護規則、2016 年制定、2018 年施行）が施行された時期から論点として注目されました。

ISSB ではサイバーセキュリティが議論の俎上に上がっていますが、経済産業省の資料(*2)によると下記のような課題があり、継続的な議論がされている状況です。ただし、経営基盤の強化の観点からもサイバーセキュリティはサステナビリティ情報の項目に含まれていると言えるでしょう。

「経済産業省　ISSB 開示基準の審議状況について（事務局資料①）」の抜粋

【サイバーセキュリティ、データセキュリティ、顧客のプライバシー】

<市場ニーズへ対応するための課題>

- ✧ サイバーセキュリティリスクに関する**将来を見越した分析は定量化及び比較が困難**であること
- ✧ 法律や枠組みが多様であるため、**規制リスクエクスポージャーを法域間で比較することは困難**であること
- ✧ 企業が、**サイバーセキュリティの実務や過去の事故に関する情報を開示することをためらう可能性**があること

(*1) SASB Materiality Map Screenshot（https://www.sasb.org/standards/materiality-map/）

(*2) 経済産業省 第 10 回 非財務情報の開示指針研究会 資料 3　ISSB 開示基準の審議状況について（事務局資料①）（https://www.meti.go.jp/shingikai/economy/hizaimu_joho/pdf/010_03_00.pdf）

改正案からの示唆

近年、サイバー攻撃により情報漏洩に留まらず事業の停止まで追い込まれるケースが発生しており、持続可能な経営基盤の強化の観点からもサステナビリティ情報にサイバーセキュリティへの取り組みが含まれることは受け入れられるのではないでしょうか。また、サイバーセキュリティへの取り組みが投資家の投資判断にとって有用な情報であることは疑いもありません。

その一方、課題もあります。ディスクロージャーWG 報告(*1)の提言にあるように、サステナビリティ情報をはじめとした将来情報の記載について、事後に事情が変化した場合に虚偽記載の責任が問われることを懸念して企業の開示姿勢が委縮することが想定されます。

しかし企業の持続可能性の観点から、いわゆる ESG 要素（ Environment（環境）、Social（社会）、Governance（企業統治））に加え、対株主、対投資家、対市場の観点からも重要となっていくと思われる「サイバーセキュリティ」に関する開示が求められる時期は確実に近付いていると言えるでしょう。

(*1) 金融審議会「ディスクロージャーワーキング・グループ報告」 －中長期的な企業価値向上につながる資本市場の構築に向けて－（https://www.fsa.go.jp/singi/singi_kinyu/tosin/20220613/01.pdf）

1. 大阪急性期・総合医療センターにおけるセキュリティインシデント

概要

2022 年 10 月 31 日午前、大阪急性期・総合医療センター（以下、医療センター）はランサムウェアと呼ばれる身代金を要求するウィルスによるサイバー攻撃を受けて電子カルテシステムに障害が発生し、緊急以外の手術や外来診療、救急患者の受け入れを停止せざるを得ない状況となりました。政府から派遣された専門家チームの調査によると、ウィルスは給食委託事業者を経由して医療センターに侵入し、データを暗号化した可能性が高いとみられています。関係者のその後の対応により、医療センターのシステムは 2023 年 1 月 11 日に復旧しました。

本インシデントは、医療機関に対するサイバー攻撃が多発する中で発生している点や、サプライチェーン上の脆弱性を悪用されている点など、典型的かつ象徴的なインシデントであり、学ぶべきことが多いと言えます。

被害状況

この医療センターは、36 診療科、病床数 865 床という大規模な総合病院であり、診療停止の影響も大きかったため、多くの報道機関で連日のように取り上げられました。公開されている主な被害や影響には以下のようなものがあります(*1)(*2)(*3)。

- 院内のサーバー31 台がランサムウェアに感染
- 電子カルテの閲覧不可
- 緊急以外の手術や外来診療、救急患者の受け入れを停止
- 患者の健康状態に直接の影響はないものの、過去の詳細な治療歴の照会不可
- 会計や薬の処方のためのシステムも使用不可
- 11 月 7 日までに予定していた手術のうち 77 件が中止
- 11 月 7 日までに外来診察や検査を受けた患者延べ約 2700 人弱に影響
- 個人情報の流出は確認されていない

(*1) 2022 年 10 月 31 日の記者会見（https://www.youtube.com/watch?v=HbiDVovNt5w）

(*2) 2022 年 11 月 07 日の記者会見（https://www.youtube.com/watch?v=z8sfezpBGfs）

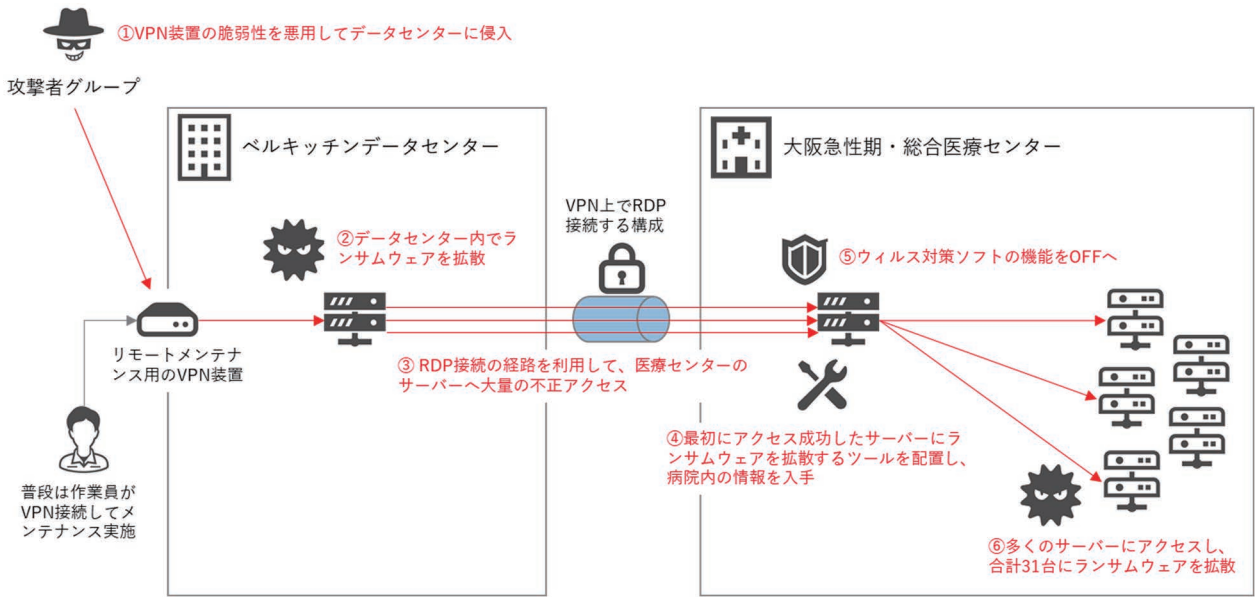
(*3) 朝日新聞デジタル「サイバー攻撃被害の病院、手術 77 件を中止　完全復旧は来年 1 月めど」（https://www.asahi.com/articles/ASQC771NXQC7OXIE023.html）

原因

政府から派遣された専門家チームが原因調査を行った結果、ウィルスは医療センターの給食委託事業者を経由して医療センターに侵入し、データを暗号化した可能性が高いことが分かりました(*1)。

この給食委託事業者が運営する給食提供施設（ベルキッチン）のデータセンターではリモートメンテナンス用に VPN 装置を使用していましたが、この VPN 装置は 2021 年 10 月にサイバー攻撃を受けた徳島県の「半田病院」と同一のもの（FortiGate 60E）であり、ソフトウェア更新がされていませんでした。また食事数や「糖尿病患者向け」などのオーダー内容についてベルキッチン側へ情報提供するため、ベルキッチンのデータセンターから医療センターのサーバーへリモートデスクトップ（RDP）接続する構成になっていました。ウィルスはこの RDP 接続の経路を利用して医療センターに侵入したものと推定されています。

医療センター側では外部との通信にファイアウォールを利用し、ウィルス対策ソフトやファームウェアの更新も実施していたようですが、結果的に取引先システムの脆弱性を悪用される「サプライチェーン攻撃」の被害を受ける格好になってしまいました。



図：医療センターへのサイバー攻撃経路

出典：2022 年 11 月 07 日の記者会見(*1)の内容を基に大和総研作成

(*1) 2022 年 11 月 07 日の記者会見（ https://www.youtube.com/watch?v=z8sfezpBGfs ）

頻発する医療機関へのサイバー攻撃

近年、医療機関へのサイバー攻撃が相次いでいます。国内で発生した医療機関へのサイバー攻撃の事例としては、下表のようなものがあります。

発生時期	医療機関	事例内容
2021 年 5 月	大阪府　東大阪医療センター	不正アクセスにより、医用画像参照システムが使用不可
2021 年 10 月	徳島県　半田病院	ランサムウェアに感染し、電子カルテや会計システムが使用不可
2022 年 1 月	東京都　日本歯科大学附属病院	コンピュータウィルスに感染し、電子カルテや会計システムが使用不可
2022 年 1 月	愛知県　春日井リハビリテーション病院	ランサムウェアに感染し、電子カルテが使用不可
2022 年 4 月	大阪府　青山病院	ランサムウェアに感染し、電子カルテが使用不可
2022 年 6 月	徳島県　鳴門山上病院	ランサムウェアに感染し、電子カルテ、院内 LAN システムが使用不能
2022 年 10 月	静岡県　田沢医院	ランサムウェアに感染し、電子カルテシステムに障害発生

このように医療機関でサイバー攻撃が相次いでいる大きな理由の一つとして、セキュリティ対策の不足があげられています。

厚生労働省が公開している資料『医療機関を取り巻く情報セキュリティ対策の現状』(*1)では、医療機関における情報化の進展により様々な情報システムの導入や組織外のネットワークとの接続を行っているにかかわらず、十分なセキュリティ対策が取られておらず、攻撃手法の進歩とも相まってサイバー攻撃の増加につながっている旨が記載されています。

また、一般社団法人医療 ISAC が実施したアンケート調査では、年間のセキュリティ予算が 500 万円未満と回答した病院の割合は 5 割強もあり、医療 ISAC は予算の制約上、実施すべきセキュリティ対応が行えなくなっているのではないかと分析しています(*2)。

(*1) https://www.mhlw.go.jp/content/10808000/000644753.pdf

(*2) 一般社団法人　医療 ISAC「四病院団体協議会の加盟病院を対象としたセキュリティアンケートの調査結果」(https://m-isac.jp/wp-content/uploads/2022/04/FinalReport_202220331.pdf)

政府の施策

このような状況の中、医療分野のサイバーセキュリティ対策に関する厚生労働省の施策として、最近では下表のようなものが打ち出されました。

日付	施策
2022 年 3 月 31 日	『医療情報システムの安全管理に関するガイドライン　第 5.2 版』の策定(*1)
2022 年 11 月 10 日	医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）(*2)
2022 年 12 月 8 日	『医療機関向けセキュリティ教育支援ポータルサイト』の開設(*3)

また、厚生労働省が開催している健康・医療・介護情報利活用検討会の医療等情報利活用ワーキンググループでは、医療機関におけるサイバーセキュリティ対策のさらなる強化策が議論されており、今後の基本方針として以下のような方針が提案(*4)されています。ワーキンググループではこれらの方針についてさらに議論が深められていくと思われ、今後の展開が注目されます。

（1） 短期的なサイバーセキュリティ対策

1. 平時の予防対応（ソフトウェアアップデート、検知機能強化など）
2. インシデント発生後の初動対応（駆けつけ機能の確保、行政機関への報告徹底など）
3. 日常診療を取り戻すための復旧対応（緊急対応手順の作成と訓練の実施など）

（2） 中・長期的なサイバーセキュリティ対策

1. バックアップデータの暗号化・秘匿化
2. 保健医療分野における SOC の構築

(*1) https://www.mhlw.go.jp/stf/shingi/0000516275_00002.html

(*2) https://www.mhlw.go.jp/content/10808000/001011666.pdf

(*3) https://www.mhlw.go.jp/stf/newpage_29579.html

(*4) 第 12 回健康・医療・介護情報利活用検討会　医療等情報利活用ワーキンググループ　【資料２－２】医療機関におけるサイバーセキュリティ対策の更なる強化策　（ https://www.mhlw.go.jp/content/10808000/000985159.pdf ）

インシデントからの示唆

今回の医療センターのインシデントで注目すべきことの一つに、医療センターはウィルス対策ソフトやファームウェアの更新をきちんと実施していたという点があげられます。もちろん、これは正しいセキュリティ対策ですが、攻撃手法は常に進化しており、これらのセキュリティ対策だけではサイバー攻撃を防ぎきれなくなっているということを示しています。

攻撃者は今回のように脆弱な取引先企業のシステムに侵入後、その企業とネットワーク接続されている自組織に侵入してきます。侵入方法は様々であり、たとえソフトウェアを最新状態にしていたとしても、セキュリティパッチが公開されていない「ゼロデイ脆弱性」を悪用されてしまう場合もあるでしょうし、管理者パスワードとして脆弱なものを設定していたといったパスワード運用上の問題点を突かれてしまう場合もあるでしょう。

それではどのような対策が考えられるでしょうか。一つには前述の厚生労働省の『医療機関等におけるサイバーセキュリティ対策の強化について（注意喚起）』に記載してあるような「サプライチェーンリスク全体の確認」です。しかし、これは取引先企業のセキュリティ管理体制に関わることにもなり、対策に長期間を要します。

そこで並行して、「侵入されること」を前提としたセキュリティ対策に方向転換することが考えられます。「侵入されること」を前提とする考え方として代表的なものに「ゼロトラスト」があります。ゼロトラストでは「すべての通信を信頼せず、常に動的かつ最小限のアクセス権限を付与することを原則」とします。前述の「健康・医療・介護情報利活用検討会　医療等情報利活用ワーキンググループ」では、早くも『医療情報システムの安全管理に関するガイドライン』の第 6.0 版策定に向けた議論が進んでおり、第 6.0 版では「ゼロトラスト」の考え方が取り入れられようとしています(*1)。

また、侵入されることを前提とした、24 時間 365 日体制で不審な通信やアプリケーションの挙動を監視する SOC（Security Operation Center）を構築することも有効です。ただし、前述のようにセキュリティ対策予算が限定される医療機関が多いのも事実です。そのような医療機関にとっては SOC をサービスとして提供する SOCaaS（SOC-as-a-Service）を利用するという選択肢もあります。SOC や SOCaaS については、第 3 部のトピックス「xSIRT」でも触れていますのでご参照ください。

(*1) 第 13 回健康・医療・介護情報利活用検討会　医療等情報利活用ワーキンググループ　【資料２－１】「医療情報システムの安全管理に関するガイドライン」について（https://www.mhlw.go.jp/content/10808000/001024397.pdf）

1. xSIRT

xSIRT とは

セキュリティインシデントには、組織で利用している IT インフラにおけるインシデントはもとより、自社で販売した製品に関わる販売先で起きたインシデントや、自社で提供するサービスに関わるインシデントも含まれます。このようなインシデント対応を行う組織を総称して xSIRT（エックスサート）と呼びます。“x”には Computer の C や Product の P、Service の S など組織が守るべき対象を指す頭文字が入ります。以下の表は、各 xSIRT の主な活動や設置部署を整理したものです。

xSIRT	対象	主な活動	設置部署
CSIRT（組織内CSIRT）（Computer Security Incident Response Team）	組織内CSIRTは、組織内の業務運営に用いるコンピュータやネットワークといった情報システムの安定稼働とそこで取り扱われる情報保護を対象として、セキュリティ・インシデントに対処する。 ※全組織的なセキュリティ統括機能が設置される場合はその機能の1つとして上記を担う。	インシデントの検知や受付を経て、その原因分析や影響範囲の調査、問題への対応、復旧を行う。あるいは、そのための技術支援を関係部署に提供する。 経営層や関係部署との連絡調整や情報共有なども行う。 平常時には、パッチ適用などの脆弱性対応、従業員への普及啓発・注意喚起なども担う。	情報システム部門やIT部門と呼ばれる部署に設置されることが多い。 なお、なお、インシデントの検知や深堀分析をSOC（Security Operation Center）と呼ばれる専門組織が担い、CSIRTと連携する場合が多い。自組織CSIRTと外部の専門組織の役割分担は組織によって異なる。
PSIRT（Product Security Incident Response Team）	PSIRTは、顧客に販売されネットワークに接続された製品および顧客の安全確保・情報保護を対象として、セキュリティ・インシデントに対処する。 ここでいう製品にはハードウェア製品とソフトウェア製品がある。	インシデントの検知や受付を経て、CSIRTが設置されている場合はCSIRTと分担・連携しつつ、製品に係る原因分析や影響範囲の調査、問題への対応、復旧を行う。 更に、製品の顧客へのパッチ提供や対策支援等の脆弱性対応なども行う。 活動の際には、製品開発や品質管理を担う部署と協調することが求められる。	事業部門ごとに、製品開発や品質管理を担う部署と連携する部署として設置されることが多い。 その際、製品開発プロセスにおけるセキュリティ・バイ・デザインの管理を兼ねる場合もある。また、複数の事業部門がある場合は、全組織的に統括的なPSIRTが置かれる場合がある。
DSIRT/SSIRT（Digital Service Security Incident Response Team）	Service SIRTは、顧客が利用するデジタル・サービスの継続的提供・品質維持および顧客の資産保護・情報保護を対象として、セキュリティ・インシデントに対処する。	インシデントの検知や受付を経て、デジタル・サービスを提供する事業部門が原因分析や影響範囲の調査、問題への対応、復旧を行うが、Service SIRTは、各事業部門を横断的・俯瞰的に確認し、事業部門に対して実務的な助言・支援を行う。 主に、サービス企画時のサービスリスク分析、サービスの不正を検知する監視ロジックの設計・更新支援、大規模サービスインシデント発生時の対応が挙げられる。 全組織的なCSIRTがある場合は必要に応じ連携する。	デジタル・サービスを提供する事業部門と横並びの独立部署、もしくは、各事業部門のセキュリティ担当を集めたバーチャル組織として設置されることが多い。

出典：NISC「DX with Cybersecurity 実践に向けた人材の確保、育成、活躍促進に係る主な政策課題と方向性」（https://www.nisc.go.jp/pdf/council/cs/jinzai_houkousei.pdf）

上記以外に、製造業などにおいて自社の工場や生産ラインの安定稼働や作業員の安全確保のために、サイバー攻撃の監視・対処を行う FSIRT(Factory Security Incident Response Team)と呼ばれる組織が生産管理部門に設置される場合があります。

xSIRT と SOC の相違点

セキュリティインシデント対応を行う組織として、xSIRT のほかに SOC があげられます。セキュリティインシデント対応には、通常時の活動と、インシデント発生後の活動があります。一般的に通常時における活動を SOC、インシデント発生後の活動を xSIRT（CSIRT、PSIRT など）と呼んでいます。しかし、昨今のサイバー攻撃の増加にともなうセキュリティ対応への意識の高まりやニーズにより、SOC は活動範囲をインシデント対応まで広げたり、xSIRT は基本的な分析を行えるように技術レベルを上げたりと、その境界線は組織の規模や技術習熟度によって多様化してきています。しかしいずれにせよ、サイバー攻撃に対応するためには、SOC と xSIRT の密な連携が必須です。

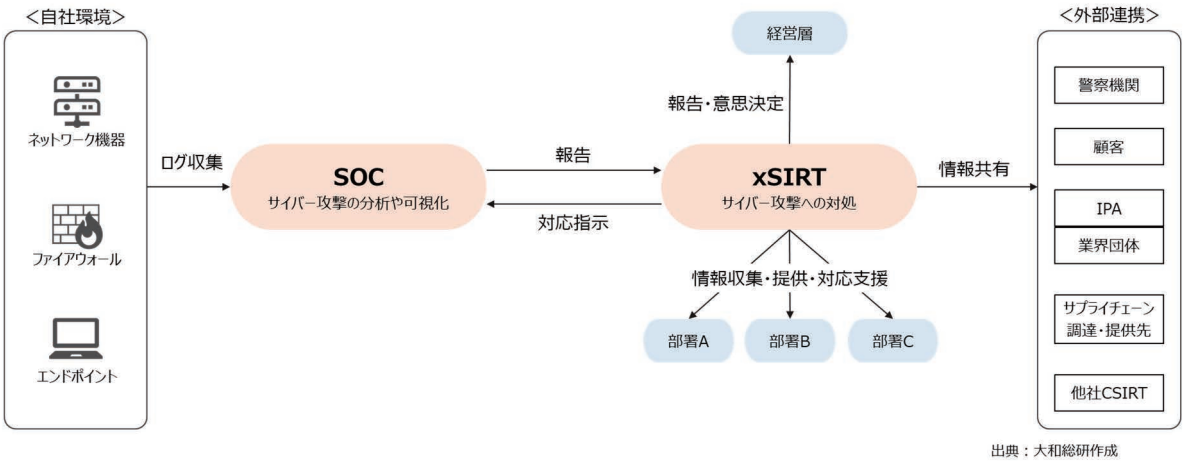
SOC

ネットワークやデバイスなどのログを取得し、サイバー攻撃の兆候を早期段階で検知する組織です。サイバー攻撃の分析や可視化（レポーティング）も行います。サイバー攻撃は日々進化しており、検知するのが困難になってきています。高度化したサイバー攻撃を検知して適切に対応するには様々なセキュリティ製品を使いこなす必要があり、高い専門知識や経験が求められます。このような状況を踏まえ、自組織の弱点を補完すべく、SOC をサービスとして提供する SOCaaS（SOC-as-a-Service）を利用する組織も増えています。

xSIRT

SOC が検知したサイバー攻撃の兆候をもとに、インシデントの詳細調査や対処を行う組織です。被害の封じ込め・復旧、脆弱性や脅威情報の収集と対応、セキュリティ人材の育成、経営層や監督官庁への報告・連携など多岐にわたります。

情報セキュリティ組織の体制イメージ



出典：大和総研作成

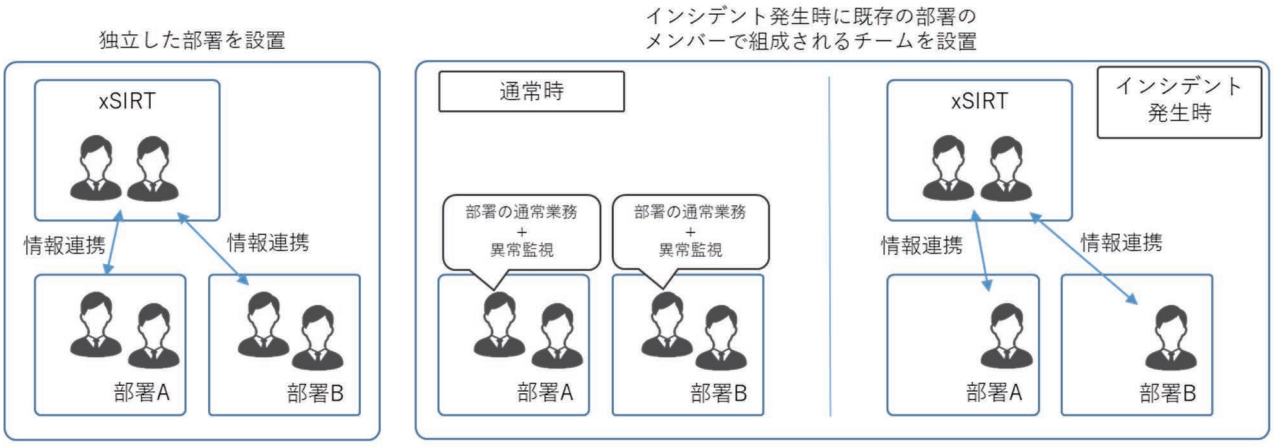
xSIRT の目的

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」が経営課題として CSIRT 構築の必要性に言及し、体制の整備を求めたことで、CSIRT を構築する企業は増加しました。その一方で業務のデジタル化（DX）の進展にともない、あらゆる業務に IT が組み込まれ、CSIRT の業務範囲が広がっています。その結果、CSIRT だけですべてのセキュリティインシデントに対応することが困難になってきました。

また顧客に提供している製品やサービスに脆弱性が含まれていた場合、顧客に多大な被害を与えてしまう可能性があります。最悪の場合、社会的信用の失墜などにつながり、取引が停止されることもあります。このような状況に対して、事業部門ごとに目的別の xSIRT を構築することで、CSIRT の負担を軽減するとともに製品やサービスの企画や設計の段階からセキュリティ対策を組み込むことができます。

xSIRT の組織モデル

xSIRT の組織モデルについては、新たに独立した部署を設置する場合と、インシデント発生時に既存の部署に属するメンバーで組成されるチームを設置する場合の 2 通りが存在します。後者の場合、異常の監視などのようなインシデント発生にかかわらず行う活動は、通常業務の一部として実施します。いずれの組織モデルにあたっても、事業内容とサイバーセキュリティの知識を備えた人材の確保、関係部署間の連携、取引先など他社との組織をまたいだ連携などがポイントになります。



出典：大和総研作成

まとめ

デジタルサービスの開発や連携などが増加する中で、製品やデジタルサービスの企画や設計の段階からセキュリティ対策を組み込む「セキュリティ・バイ・デザイン(*1)」の考え方が重要になってきています。インシデント発生後の対応だけでなく、セキュアな開発プロセスを構築・管理あるいは構築・牽制することも xSIRT の重要な役割の一つです。

NISC（内閣サイバーセキュリティセンター）では、xSIRT の普及に向けた取り組みを行っています。取り組みとしては、xSIRT の構築や普及にあたっての課題の議論や xSIRT の構築事例の公開などを行っています。このように PSIRT や DSIRT/SSIRT を製品やサービスを提供している事業部門に設置する取り組みが進められています。一方で組織内にインシデント発生時に対応する体制が整備されていない場合は、まずは CSIRT を構築することが必要です。組織全体のインシデントに対応する CSIRT を構築し、体制やルールを整備するところから始める必要があります。

CSIRT 構築支援サービス

大和総研では、大和証券の CSIRT 構築・運用で培ったノウハウを活かし、お客様の CSIRT 構築や見直し・強化を支援する CSIRT 構築支援サービスを提供しています。サービスの詳しい内容については、下記のサイトをご参照ください。

https://it-solution.dir.co.jp/l/973193/2022-12-14/31n5q

(*1)システム導入・運用後ではなく、製品やデジタルサービスの企画・設計の段階でセキュリティ対策を組み込むことで、サイバーセキュリティを確保する考え方

バックナンバーはこちら

DIR SOC Quarterly 2022 the first issue （2022 年 9 月 29 日発行）

https://www.dir.co.jp/publicity/publication/socquarterly2210.html

DIR SOC Quarterly 2022 vol.2 （2022 年 11 月 21 日発行）

https://www.dir.co.jp/publicity/publication/socquarterly2211.html

DIR SOC Quarterly 2023 winter vol.3
2023 年 1 月 30 日発行

著者　大和総研
発行所　株式会社大和総研　フロンティア研究開発センター
印刷・製本　セキ株式会社

お問い合わせ先　https://www.dir.co.jp/contact/solution/input.php

大和総研が運営する、AI・データサイエンスなど先端技術に特化した用語解説サイト「WORLD」（ワード）を開設しました。

大和総研の用語解説サイト

WORLD

キーワードから、みえる、つながる、未来の日常（Life）

「WORLD」（ワード）は、大和総研が運営する、AI・データサイエンスなど先端技術に特化した用語解説サイトです。
大和総研にはシステム、リサーチ、コンサルティング分野のスペシャリストが連携して、多くのお客様の幅広いニーズに応えてきた実績があります。用語解説サイト「WORLD」では、大和総研がこれまでに培ってきた豊富な経験をもとに、未来を築く新ソリューション創出の礎となる情報を、わかりやすく、深くご紹介していきます。
大和総研は先端テクノロジーやAI・データサイエンス技術を駆使し、デジタル社会を牽引するビジネスパートナーであり続けます。

CONTENTS

キーワードから　旬のIT用語が一目でわかるトレンドワードクラウド

国内約50のIT関連ニュースサイトで掲載された記事の中から、トレンドのワードをピックアップして視覚化。今押さえるべきIT用語が一目でわかるトレンドワードクラウドです。

みえる　AI・データサイエンスなど4分野の用語を解説

よく耳にする頻出用語から最新の用語まで、先端技術の研究・開発を通じてテクノロジーの可能性を追求しつづける大和総研の知見を活かした用語解説ページです。

解説用語例	AI・データサイエンス	セキュリティ	IT全般	ブロックチェーン
	●MLOps ●マルチモーダルAI ●ニューラルネットワーク	●eKYC ●ゼロトラスト	●マルチクラウド ●データマネジメントプラットフォーム ●ノーコード開発/ローコード開発	●暗号資産（仮想通貨） ●セキュリティ・トークン・オファリング（STO）

つながる　IT技術とビジネスをつなぐ深掘り解説

ビジネスでの活用が見込まれる技術を深掘り。技術発展の背景、関連技術の紹介や導入における注意点など、未来を築く新ソリューション創出の礎となる情報をわかりやすく解説します。

大和総研の用語解説サイト
WORLD

https://www.dir.co.jp/world/

大和総研
Daiwa Institute of Research