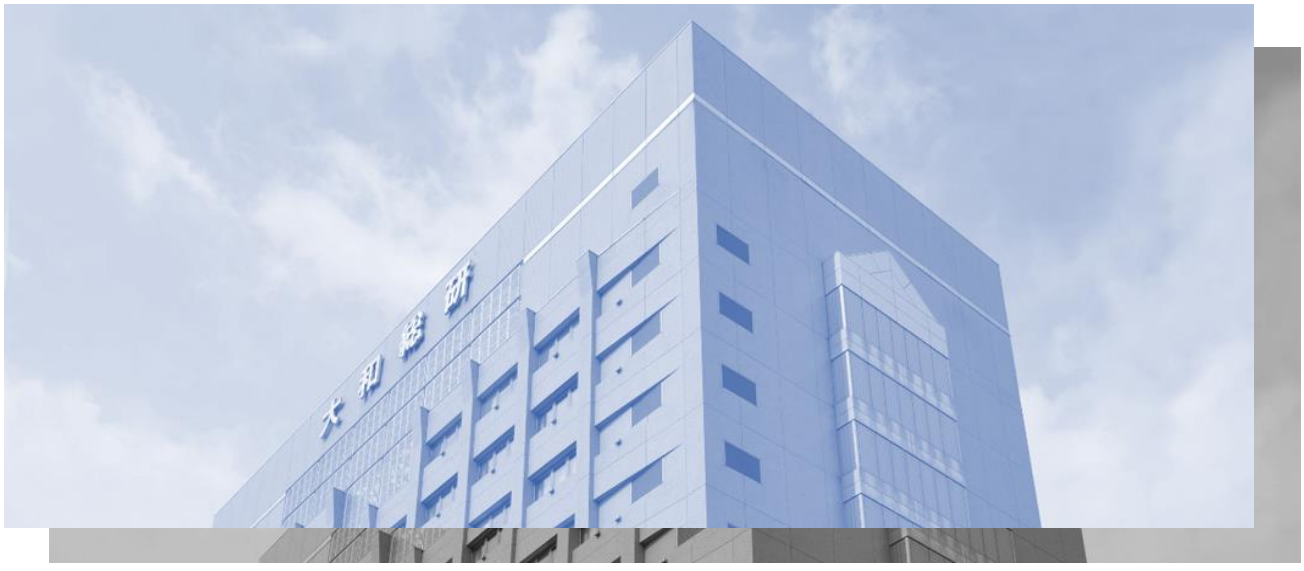
DIR SOC Quarterly
2022 the first issue



大和総研
Daiwa Institute of Research

目次

創刊にあたって

近年は、ビッグデータ、デジタルトランスフォーメーション、データマネジメントなど、データ活用の重要性が叫ばれて久しく、データを駆使して新たな付加価値を生み出せるかどうかは、競争優位を確立できるか否かの分水嶺と言えます。言い換えれば、データこそ付加価値の源泉であり、企業が守るべき最重要資産の１つということです。データを安全に扱える環境を守ることが、企業をはじめとする様々な組織にとっての生命線であると言って過言でありません。

一方、サイバー攻撃はいまこうしている間にも行われており、各企業や組織が様々な対策を講じ、これを防いでいる状況に違いありません。サイバー攻撃は激しくなる一方であり、かつ巧妙化の一途を辿っています。したがって、データを使って様々な価値を創出したり、また経営判断をしたりする以上、サイバー攻撃の状況と対策の動向は日常的に意識されるべきであり、本冊子はこれをタイムリーにお伝えすることを目的としています。

本冊子は二部構成となっています。

サイバー攻撃対策は、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り、第一部は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。第二部はこの点にフォーカスしています。

サイバー攻撃は前触れをつかむことが難しく、組織の活動を一瞬にして停止に追い込んでしまいます。であるからこそ、日ごろから抜け漏れのない備えが大切です。本冊子が、読者の皆様のサイバーセキュリティへの理解と関心を深める一助となれば幸いです。

2022 年 9 月　株式会社大和総研執筆者一同

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 年第 1 四半期におけるわが国の政策・法制度の動向、および、2022 年第 1 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。

第 1 部：わが国の政策・法制度の動向

1 『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）』の決定

1 - 1 内閣サイバーセキュリティセンター（NISC）の体制変更

1 - 2 『重要インフラのサイバーセキュリティに係る行動計画』の決定

1 - 3 サイバー・フィジカル空間の融合に対応したセキュリティ対策

2 経済安全保障推進法の成立

3 『デジタル社会推進標準ガイドライン』の公開

4 『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』の開催

5 『ISMAP-LIU クラウドサービス登録規則（案）』等に対する意見公募

6 『サイバーセキュリティ体制構築・人材確保の手引き』第 2.0 版の公開

なお、上記の 1－1 と 1－2 と 1－3 は 上記 1 で明記されている「政府が特に強力に取り組むことが必要であると考える施策」に関連する話題を取り上げたものです。

第 2 部：インシデント事例の紹介

1 ランサムウェアによる事業停止

2 マルウェア Emotet の感染拡大

2022 年度第 1 四半期に政府から公開された文書は、経営層が責任をもってサイバーセキュリティ対策をコーポレートガバナンスに組み入れることを求めるものが多い印象でした。また、2022 年度第 1 四半期に注目を集めたインシデント事例も、コーポレートガバナンスの必要性や組織に属する一人ひとりのセキュリティに対する意識の重要性を示唆するものでした。

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。

第 1 部：わが国の政策･法制度の動向

1. サイバーセキュリティ 2022 の決定

年次報告・年次計画

政府は 2022 年 6 月 17 日、『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）』を決定し、公表しました。なお、各年度の年次報告・年次計画の決定は、政府の 3 か年計画『サイバーセキュリティ戦略』（2021 年 9 月 28 日決定）に定められている取り組みです。

例年との違い

今回の年次報告・年次計画は 3 部構成で、これまでと異なり、冒頭の第 1 部にエグゼクティブサマリーを新たに配置し、政府が特に強力に取り組むことが必要であると考える施策を簡潔に示しています。（下図参照）また第 2 部と第 3 部では、サイバーセキュリティに関する情勢、昨年度の取組実績および今年度の取組について、2021 年 9 月決定の『サイバーセキュリティ戦略』の基本施策に沿った形で記載するなど、『サイバーセキュリティ戦略』との整合性に配慮していることがうかがえます。

これ以降、下表の(1)～(3)に関連した話題を取り上げます。

「自由、公正かつ安全なサイバー空間」の実現のために特に強力に取り組む施策
（1）官民連携のオールジャパンの推進体制強化（ナショナルサート機能の強化）
（2）重要インフラ事業者をはじめとする民間部門のサイバーセキュリティの強化
（3）サイバー空間とフィジカル空間の融合に対応したサイバーセキュリティ対策
（4）地域・中小企業のサイバーセキュリティ対策
（5）サイバー警察局・サイバー特別捜査隊の新設による官民連携・国際連携の推進
（6）インド太平洋地域における能力構築支援の推進

表：『サイバーセキュリティ 2022』のエグゼクティブサマリーに記載されている「政府が特に強力に取り組むことが必要であると考える施策」
出典： https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022.pdf

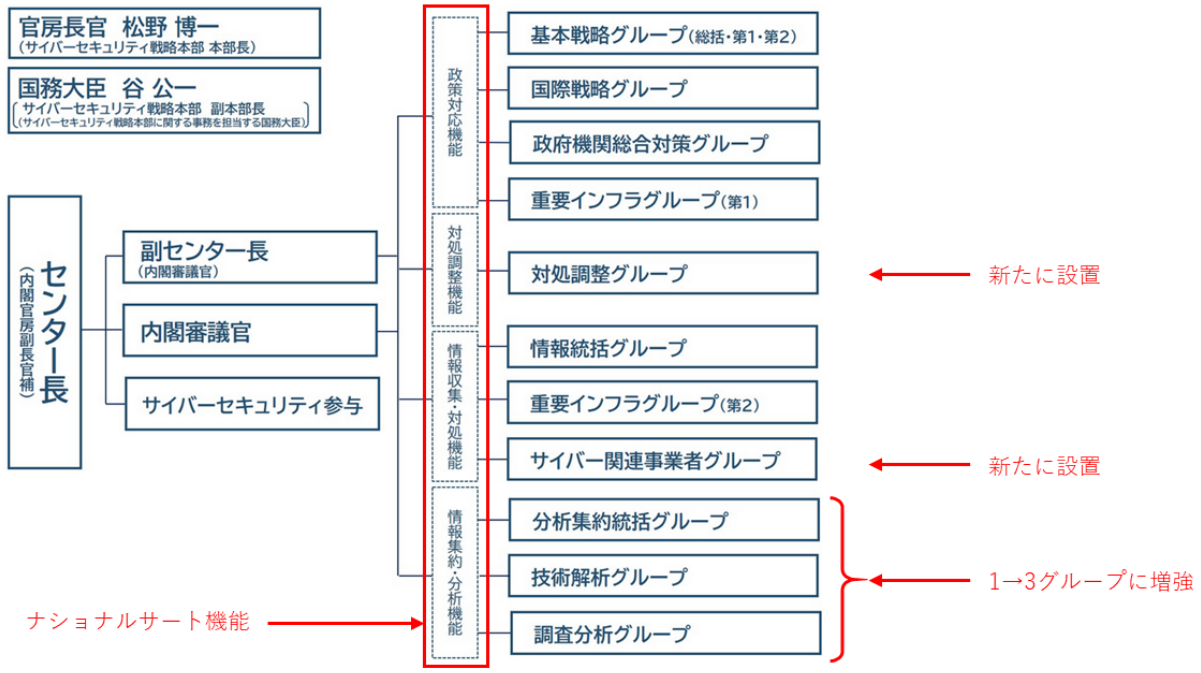
1-1. 内閣サイバーセキュリティセンター（NISC）の体制変更

ナショナルサート機能の強化

2021 年 9 月決定の『サイバーセキュリティ戦略』や 2022 年 6 月決定の『サイバーセキュリティ 2022』（本資料 4 ページ参照） では、ナショナルサート（CSIRT/CERT）(*1)の枠組みを強化する旨を施策として記載しています。

政府は、ナショナルサートを 「深刻なサイバー攻撃に対し、情報収集・分析から、調査・評価、注意喚起の実施及び対処と、その後の再発防止等の政策立案・措置に至るまでの一連の取組を一体的に推進するための総合的な調整を担う機能」 として位置づけています。(*2)

2022 年 6 月より、内閣サイバーセキュリティセンター（NISC） はこのナショナルサートの機能を具備すべく、新たなグループを設置する等、体制を変更しました。



図：2022 年 8 月 10 日現在の NISC の体制図
出典： https://www.nisc.go.jp/about/organize/index.html に掲載の図をもとに加筆

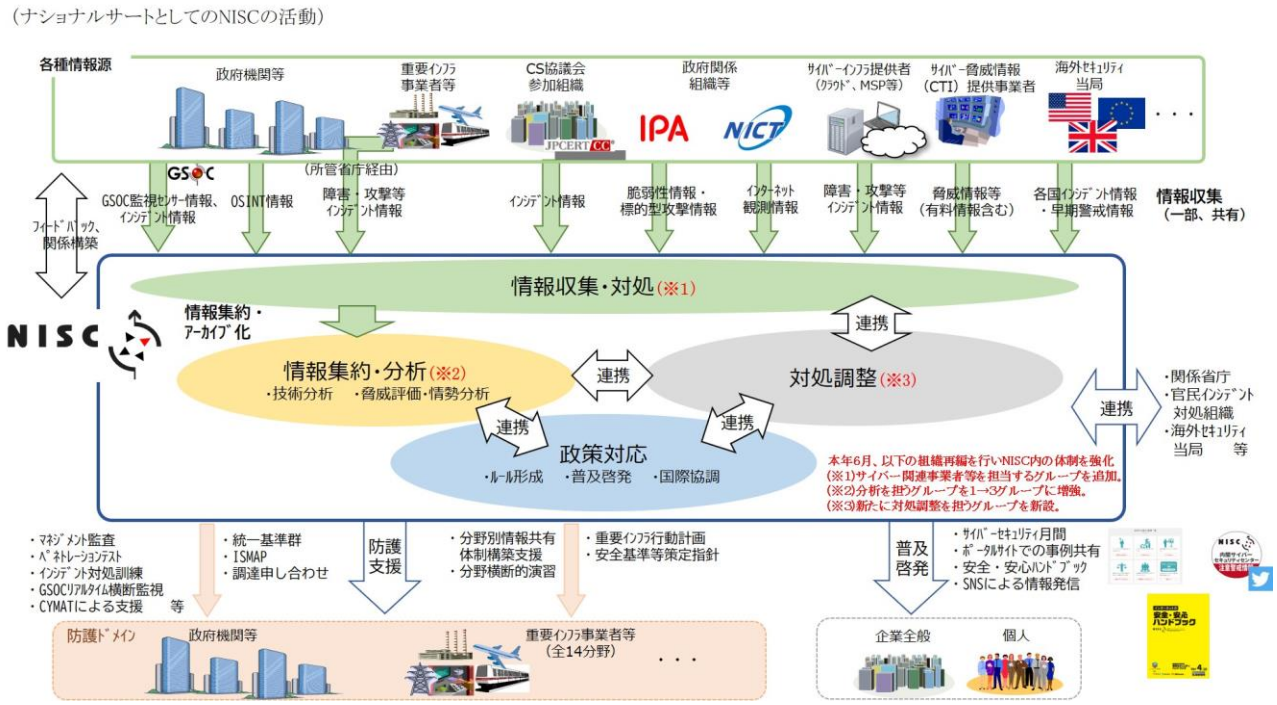
(*1) 次頁の脚注をご参照ください。
(*2) 『サイバーセキュリティ戦略』 p11（ https://www.nisc.go.jp/pdf/policy/kihon-s/cs-senryaku2021.pdf ）

（参考）ナショナルサートとしての NISC

ナショナルサートとしての NISC の活動

以下の図は、内閣サイバーセキュリティーセンター（NISC）の Web サイトに掲載されているものです。

前頁の図にある NISC が担うナショナルサート（CSIRT/CERT）(*1)の 4 つの機能「政策対応」、「対処調整」、「情報収集・対処」、「情報集約・分析」の関係性や、NISC がどのような組織・主体とどのように関わるのかが明確になっています。



図： ナショナルサートとしての NISC の活動

出典： https://www.nisc.go.jp/about/organize/kinokyoka.html

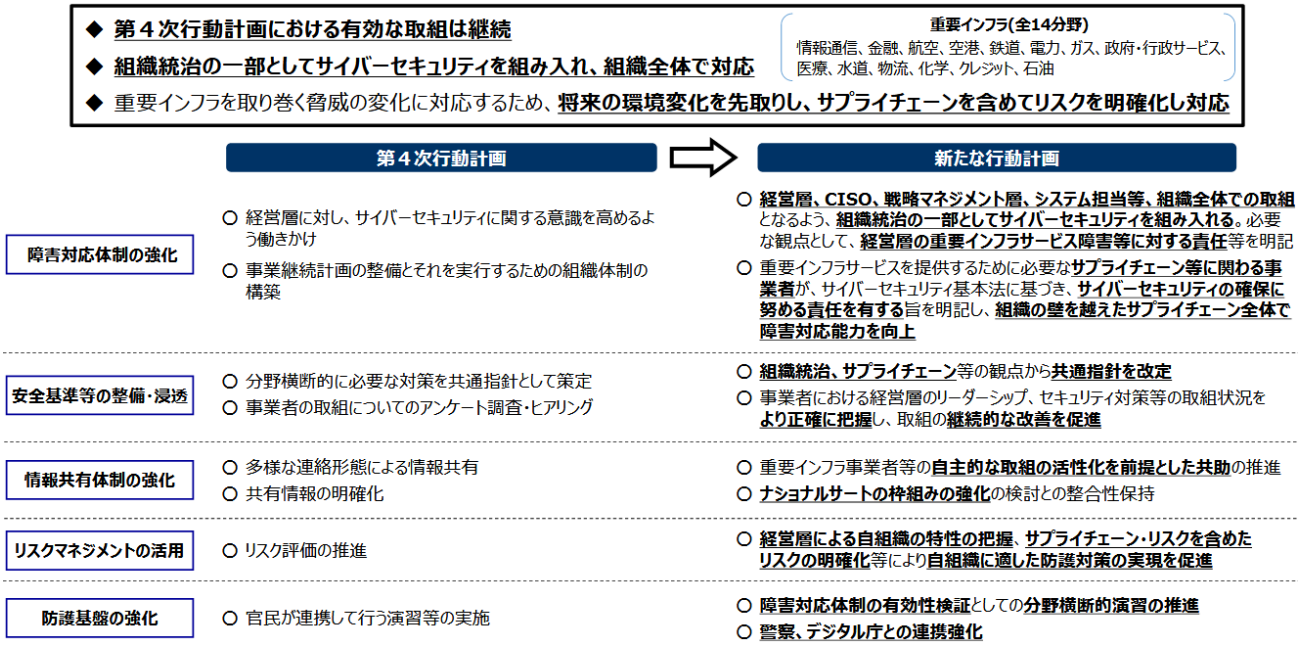
(*1) 一般に、CSIRT（シーサート）とは Computer Security Incident Response Team の略であり、CERT（サート）は Computer Emergency Response Team の略です。いずれも同義的に用いられ、「コンピュータセキュリティインシデントに対応する活動を行う組織」のことを差しますが、用いる人によって微妙にその内容が異なる場合もあり、注意が必要です。政府による「ナショナルサート」の定義は前頁に記載のとおりです。

1-2. 重要インフラ行動計画の決定

重要インフラのサイバーセキュリティ

政府は 2022 年 6 月 17 日に『重要インフラのサイバーセキュリティに係る行動計画』を決定し、公表しました。2022 年 6 月決定の『サイバーセキュリティ 2022』（本資料 4 ページ参照）では、この『行動計画』を踏まえて重要インフラのサイバーセキュリティの確保を推進していくことを強化施策の 1 つとして掲げています。

今回の行動計画では、2017 年に決定（2020 年に改訂）された『重要インフラの情報セキュリティ対策に係る第 4 次行動計画』を踏襲しつつ、今後の脅威動向や環境変化に適確に対応できるように補強・改善されています。

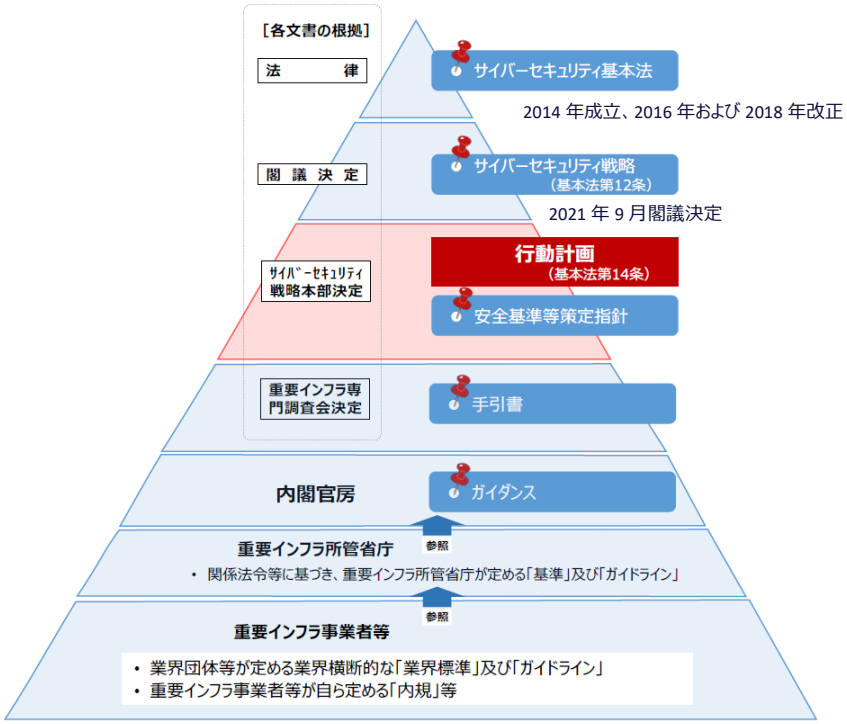


図：政府の強化施策の 1 つ「重要インフラ事業者を始めとする民間部門におけるサイバーセキュリティの強化」
出典： https://www.nisc.go.jp/pdf/policy/kihon-s/cs2022-gaiyou.pdf

サイバーセキュリティ基本法との関連付け

今回の行動計画で目を引く点として、国や重要インフラ事業者の責務等について規定しているサイバーセキュリティ基本法（2014 年成立、2016 年および 2018 年改正）や重要インフラ事業者のサイバーセキュリティ確保に関する諸施策の実施方針が示されているサイバーセキュリティ戦略（2021 年閣議決定）との関連付けが挙げられます。「行動計画」の法的根拠を明示して実効性を高める狙いが垣間見えると言えます。

例えば、今回の計画期間内の取り組みの 1 つである安全基準等の整備及び浸透の部分では、下図のように安全基準の体系や法的根拠が明示されています。(*1)



図：重要インフラ防護に関する安全基準等に係る体系
出典： https://www.nisc.go.jp/pdf/policy/infra/cip_policy_2022.pdf に掲載の図に西暦年号を加筆

(*1) 今回の行動計画の中で、安全基準は以下の種類に分類されています。

① 安全基準策定指針、手引書等を踏まえ、関係法令に基づき国（重要インフラ所管省庁）が定める強制基準
② 安全基準策定指針、手引書等を踏まえ、関係法令に準じて国（重要インフラ所管省庁）が定める推奨基準及びガイドライン
③ 関係法令や国民からの期待に応えるべく業界団体等が定める業界横断的な業界標準及びガイドライン
④ 関係法令や国民・利用者等からの期待に応えるべく重要インフラ事業者等が自ら定める内規等

いずれも最終的な根拠はサイバーセキュリティ基本法に行き着くと言えます。

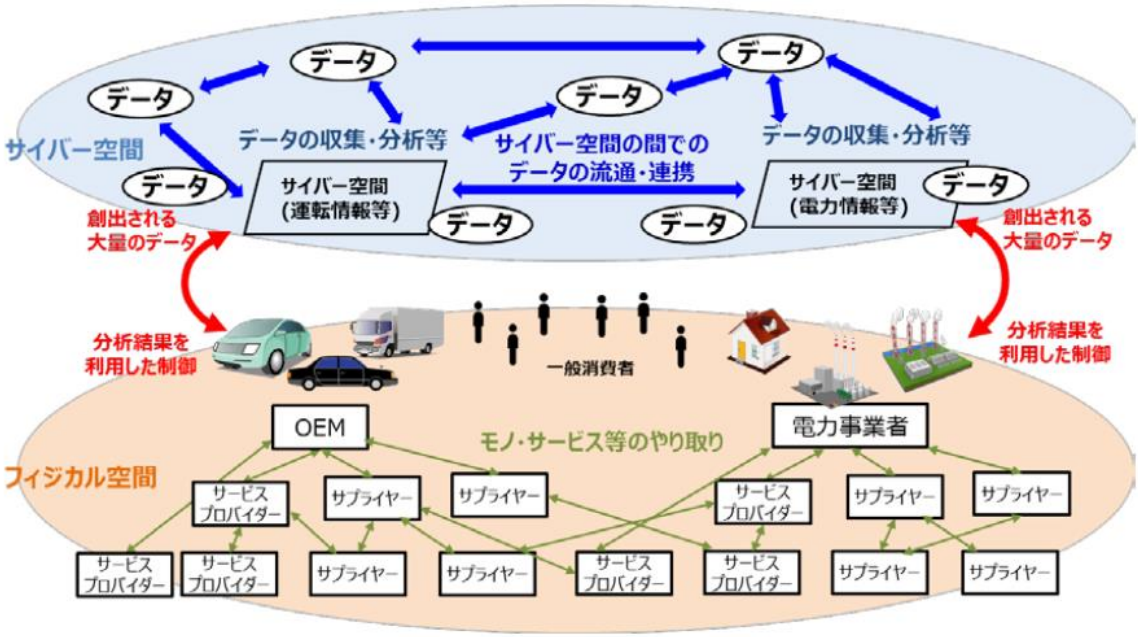
1-3. サイバー・フィジカル空間の融合に対応したセキュリティ対策

サイバー・フィジカル空間の融合に伴う脅威の増大

政府は、2016 年に閣議決定した第 5 期科学技術基本計画において、「サイバー空間（仮想空間）とフィジカル空間（物理空間）を高度に融合させたシステムにより経済発展と社会的課題の解決を両立する人間中心の社会」を、狩猟社会（Society 1.0）、農耕社会（Society 2.0）、工業社会（Society 3.0）、情報社会（Society 4.0）に続く新たな社会「Society5.0」として、提唱しました。(*1)

このような社会では、企業間・産業間のネットワーク化が進展し、サイバー空間とフィジカル空間をまたいで構成される新たな形のサプライチェーンが新たな付加価値を生み出していくことが期待されています。しかし、それは同時に以下のような懸念が新たに生まれることも意味しています。(*2)

- ネットワーク化されたサプライチェーン上にサイバー攻撃起点が広く拡散していくことになり、攻撃側が攻撃起点を得る機会が増え、防御側が守るべき範囲が急激に拡大する
- サイバー空間とフィジカル空間が相互に作用しあうことは、サイバー攻撃がフィジカル空間に及ぼす影響も増大し、サイバー攻撃による被害は甚大なものになっていく可能性がある



図：「Society5.0」社会におけるモノ・データ等のつながりのイメージ
出典：サイバー・フィジカル・セキュリティ対策フレームワーク https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf

(*1) https://www8.cao.go.jp/cstp/society5_0/index.html
(*2) https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf

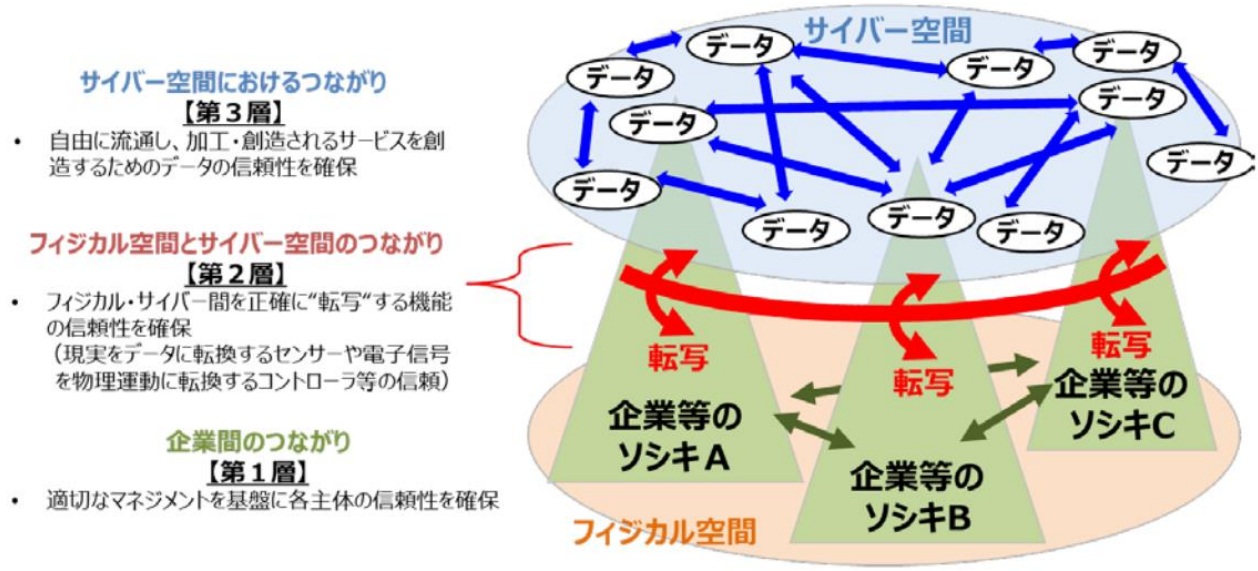
サイバー・フィジカル・セキュリティ対策フレームワーク

政府は、サイバー・フィジカル空間の融合で増大するサイバー攻撃の脅威に対応するため、フレームワークの整備や社会実装を推進していく方針です（『サイバーセキュリティ 2022』（本資料 4 ページ参照））。このための具体的な取り組みとして挙げられているのは以下の 2 点であり、これら施策により、サイバー・フィジカル・システムの理解促進、リスクへの対応力向上、データの自由な流通、新たな付加価値の増大に寄与するとしています。

① サイバー・フィジカル・セキュリティ対策フレームワーク（以後、CPSF と略記）や関連するフレームワーク等の普及啓発活動、国際標準化、関係団体・企業との協力を推進
② ソフトウェア部品表（SBOM、次頁参照）の普及に向け、効果的な活用モデルや共有に係る取引モデル、ノウハウ等の構築のための検討を推進

CPSF は、「Society5.0」におけるサプライチェーン全体のセキュリティ確保のため、経済産業省が設置する「産業サイバーセキュリティ研究会」の「ワーキンググループ 1」で検討され、2019 年 4 月に公開されたものです。

その後も同ワーキンググループ内の複数のタスクフォースで具体化・詳細化・普及促進等の検討が進められており、2022 年度第 1 四半期も複数回の検討会が開催されています。



図：CPSF が提唱する三層構造モデルと各層における信頼性
出典：サイバー・フィジカル・セキュリティ対策フレームワーク https://www.meti.go.jp/policy/netsecurity/wg1/CPSF_ver1.0.pdf

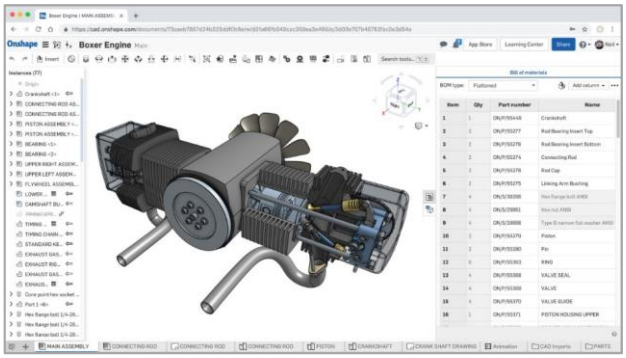
ソフトウェア部品表

ソフトウェア部品表（SBOM： Software Bill of Material、通称「えすぼむ」）とは、製造業で従来から取り入れられている BOM（Bill of Material ）という考え方をソフトウェア開発に適用したものです。

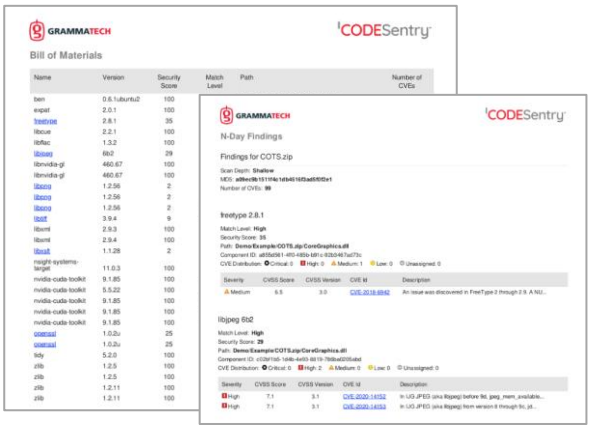
- BOM は製品をつかさどる部品の一覧であり、階層構造を示すとともに製品を構成する各部品の基本情報を含む
- 食品に成分表が示され、ハードウェア製品に部品表（BOM）が用意されているのと同じように、どのようなソフトウェアを使った製品か誰にでも分かるように管理されるべきという考え方

米国を中心にソフトウェア脆弱性情報への対応や安全なソフトウェア開発の促進を目的として活用が進んでおり、特にサイバーセキュリティを強化する大統領令（2022 年 5 月）以降、米国立標準技術研究所（NIST）にて SBOM 利用のガイドライン策定等が進められています。

日本政府も今後、SBOM の普及に向けた検討を推進していく予定であり、前述の経済産業省が設置する「産業サイバーセキュリティ研究会」にて検討や検証が進められています。



図：BOM のイメージ
出典： https://www.onshape.com/ja/features/bill-of-materials



図：SBOM のイメージ
出典： https://blogs.grammatech.com/what-is-an-sbom-a-deep-dive

2. 経済安全保障推進法の成立

経済安全保障推進法の 4 つの柱

2022 年 5 月 11 日に、経済安全保障推進法が成立しました。(*1) この法律が成立した背景としては、国際情勢の複雑化や社会経済構造の変化等が挙げられますが、安全保障を確保するための 4 つの経済施策（以下の 4 つの柱）からなっています。

1. 重要物資の安定的な供給の確保（サプライチェーン強靭化）
2. 基幹インフラ役務の安定的な提供の確保（基幹インフラのサイバーセキュリティ確保）
3. 先端的な重要技術の開発支援
4. 特許出願の非公開

このうち、基幹インフラ事業（後述）に関わる者にとっては、上記の 2. の影響が最も大きいと考えられ、今後、具体化される内容について十分注意を払う必要があります。

今後のスケジュール

この法律の施行日や具体的な方針・指針などは今後の政令・省令等で規定・策定される予定です。4 つの柱それぞれで基本方針の策定時期や施行時期が異なりますが、2 つ目の柱である基幹インフラのサイバーセキュリティに関しては以下のようなスケジュールとなっています。

日程	内容
2023 年 5 月までの政令指定日	基幹インフラ役務の安定的な提供の確保に関する基本指針の策定
2023 年 11 月までの政令指定日	特定社会基盤事業者の指定
2024 年 2 月までの政令指定日	事前審査や勧告・命令等の施策の施行

(*1) 正式名称は、「経済施策を一体的に講ずることによる安全保障の確保の推進に関する法律」です。

基幹インフラ事業者の定義

前述の 2 つ目の柱により、今後、基幹インフラ事業者は重要設備（ハードウェア、ソフトウェア、クラウドサービスなど）の導入・維持管理等の委託について政府の事前審査を受けなければならず、また審査結果に基づいて勧告・命令などを受ける可能性があります。

なお、「基幹インフラ事業」はサイバーセキュリティ基本法で触れられている「重要インフラ分野」とは異なります（下図参照）。基幹インフラ事業者や重要設備の具体的な内容は今後省令で指定される予定ですが、対象事業を行う者のうち、

① 重要設備の機能が停止・低下した場合、
② 役務の安定的な提供に支障が生じ、
③ 国家・国民の安全 （国民の生存・社会経済秩序の平穏）を損なうおそれが大きいもの

として主務省令で定める基準に該当する者が「基幹インフラ事業者」として指定されます。(*1)

重要インフラ分野（サイバーセキュリティ基本法）		基幹インフラ事業（経済安全保障推進法）	
金融	クレジット	金融	クレジットカード
情報通信	石油	電気通信	石油
政府・行政サービス	航空	放送	航空
医療	空港	郵便	空港
水道	鉄道	水道	鉄道
電力	化学	電気	外航貨物
ガス	物流	ガス	貨物自動車運送

図： 重要インフラ分野と基幹インフラ分野の比較。この図における彩色の意味は以下のとおりです。
オレンジ色：他方にない分野・事業
緑色：他方に類似の分野・事業あり
無彩色：同一の分野・事業あり

(*1) 経済安全保障推進法案の概要（ https://www.cas.go.jp/jp/houan/220225/siryou1.pdf ）より引用

3. デジタル社会推進標準ガイドライン公開

セキュリティに関するドキュメントの公開

デジタル庁は 2022 年 6 月 30 日にデジタル社会推進標準ガイドラインのうち、セキュリティに関する以下のガイドラインを公開しました。(*1)

- ゼロトラストアーキテクチャ適用方針
- 常時リスク診断・対処（CRSA）アーキテクチャ
- 政府情報システムにおけるセキュリティ・バイ・デザインガイドライン
- 政府情報システムにおける脆弱性診断導入ガイドライン

デジタル社会推進標準ガイドライン群は、サービス・業務改革並びにこれらに伴う政府情報システムの整備及び管理についての手続・手順や、各種技術標準等に関する共通ルールや参考ドキュメントをまとめたものです。(*2)

もともとは「デジタル・ガバメント推進標準ガイドライン群」という名称でしたが、デジタル庁として政府内部だけでなく社会全体のデジタル化を推進するという観点から改称したという経緯があります。したがって、場合によっては一般企業がこれらのガイドラインを参考にしたり、準拠したりすることが求められる状況が将来的に発生する可能性も考えられます。

なお、ガイドラインの位置づけには Normative と Informative がありますが、今回公開された上記ガイドラインはすべて Informative です。

- Normative（標準ガイドライン）：政府情報システムの整備及び管理に関するルールとして順守する内容を定めたドキュメント
- Informative（実践ガイドブック）：参考とするドキュメント

(*1) https://www.digital.go.jp/resources/standard_guidelines/#ds200

(*2) 2022 年 8 月時点では、デジタル社会推進標準ガイドライン群には以下の 5 つがあります。

1. 政府情報システム全般に関するドキュメント
2. セキュリティに関するドキュメント
3. クラウドに関するドキュメント
4. データ連携に関するドキュメント
5. ID・認証に関するドキュメント

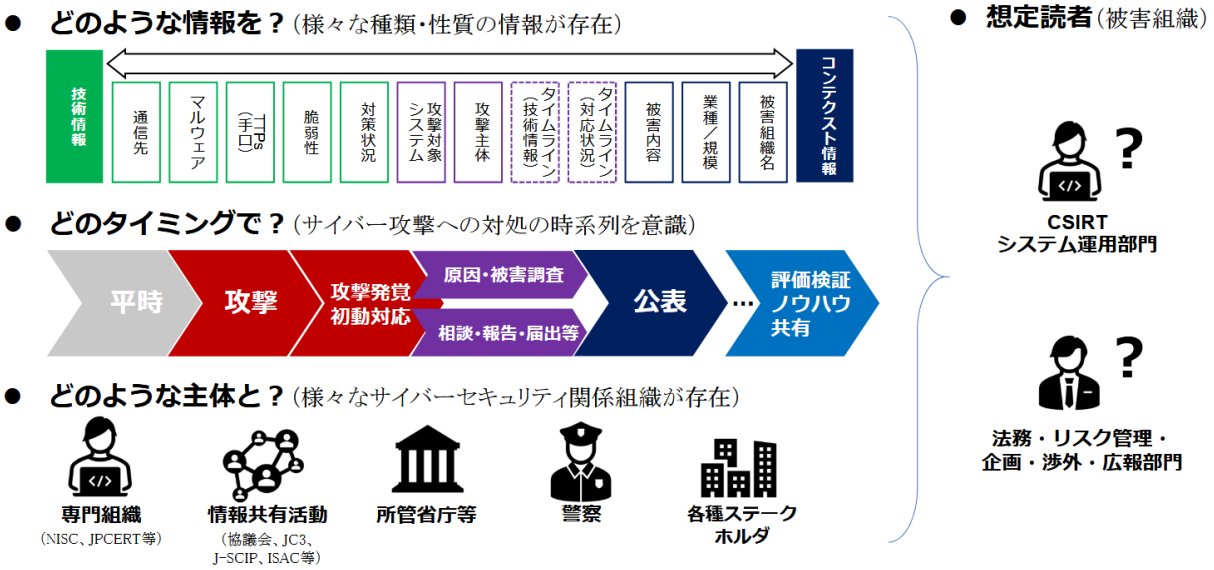
4. サイバー攻撃被害に係る情報の共有・公表ガイダンスの検討

情報共有・公表のガイダンス策定へ

政府は 2022 年 4 月 20 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（＝実務上の参考となるガイダンス文書）を策定すべく、サイバー攻撃に係る情報の共有・公表ガイダンス検討会を開催することを決定しました。この背景には、サイバー攻撃被害に係る情報を共有することは被害組織自身および社会全体にとって有益ですが、一方でどのような情報をどのようなタイミングでどのような主体と共有すべきか適切に判断することが難しいという現状があります。

本検討会の事務局は、警察庁、総務省、経済産業省及びサイバーセキュリティ協議会事務局（内閣官房内閣サイバーセキュリティセンター及び政令指定法人 JPCERT/CC）が担うことになっています。

2022 年 5 月 30 日には第 1 回検討会が開催され、事務局からの論点提示や検討委員による自由討議が行われました。



図： サイバー攻撃被害に係る情報の共有・公表ガイダンス（イメージ）
出典： https://www.nisc.go.jp/pdf/council/cs/kyogikai/dai1/GDkentoukai01_shiryou2-1.pdf

5. ＩSMAP－LIUクラウドサービス意見公募

低リスク業務のためのクラウドサービス評価

政府は 2022 年 6 月 15 日に、「ISMAP-LIU クラウドサービス登録規則（案）」等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（7 月 5 日終了）。

ISMAP（Information system Security Management and Assessment Program）は政府が求めるセキュリティ要求を満たしているクラウドサービスを予め評価・登録するセキュリティ評価制度です。しかし、セキュリティ上のリスクの小さな業務・情報の処理に用いるクラウドサービスに対しては、現行の ISMAP では過剰なセキュリティ要求となる場合も考えられるため、ISMAP for Low-Impact Use（ISMAP-LIU）の仕組みを策定する方針です。

対象とする機密情報の分類

現行 ISMAP が対象とするのは機密性 2 情報(*1)を扱うクラウドサービスのみですが、新たに策定する ISMAP-LIU が主に対象とするのは、機密性 2 情報を扱うクラウドサービスのうちセキュリティ上のリスクの小さな業務・情報の処理に用いる SaaS（Software as a Service）です。下図の 8 つの業務が現時点で ISMAP-LIU の対象となる業務の例として公表されています。

1. **公表を前提とした政策・制度の立案・調整過程等で民間と連携して作業する業務**
   有識者を招いた審議会等の運営を行うために、Web会議による会議運用や、ファイル共有による情報の保存・管理・共有を行う用途
2. **政府機関等職員の業務上の役職・氏名等情報を扱う業務**
   （業務の性質上、従事する職員の情報について厳格な秘匿が求められている場合を除く）
   政府職員の役職・氏名情報を用いて職員の人事管理やタレントマネジメントを行う用途
3. **名刺情報等の一般に広く提供する範囲の情報、及びユーザ名・パスワード・メールアドレス等の情報を扱う業務**
   企業名、役職、氏名等の名刺情報を登録・管理する業務
   政府機関等の顧客に対する映像・コンテンツ等の配信に伴う配信先の特定を目的としたユーザ登録・管理業務
4. **民間から提供される情報であり、当該情報提供者が低リスクだと判断している情報を処理する業務**
   民間企業・民間団体が利用しているWeb会議やファイル共有のためのSaaSを用いて、当該情報提供元企業が提供する情報の保存・管理を行う用途
5. **オープンソース・公知の事実・一般情報を扱う業務だが例外的に要機密扱いとする必要がある場合**
   Webサイトの公開前情報など、公開が予定されている情報であり、当該情報の公開が意思決定されている情報を扱う用途
   機械翻訳を用いて他国の政策情報や技術情報等を翻訳し調査を行う用途（政府の特定情報に対する調査傾向が要機密となる場合）
6. **災害時等に組織構成員の被災状況確認等を行う業務**
7. **組織構成員に対する組織ルールやビジネススキル等の教育を行う業務**
8. **「行政文書の管理に関するガイドライン」において保存期間１年未満に該当するもののうち、定型的・日常的な業務連絡等を扱う業務**
   政府機関等の掌握事務に対する事実関係の問合せへの応答業務

図： ISMAP-LIU の対象となる SaaS が取り扱って差し支えないと考えられる業務（黒字は具体的な参考例）
出典： https://www.soumu.go.jp/main_content/000819998.pdf

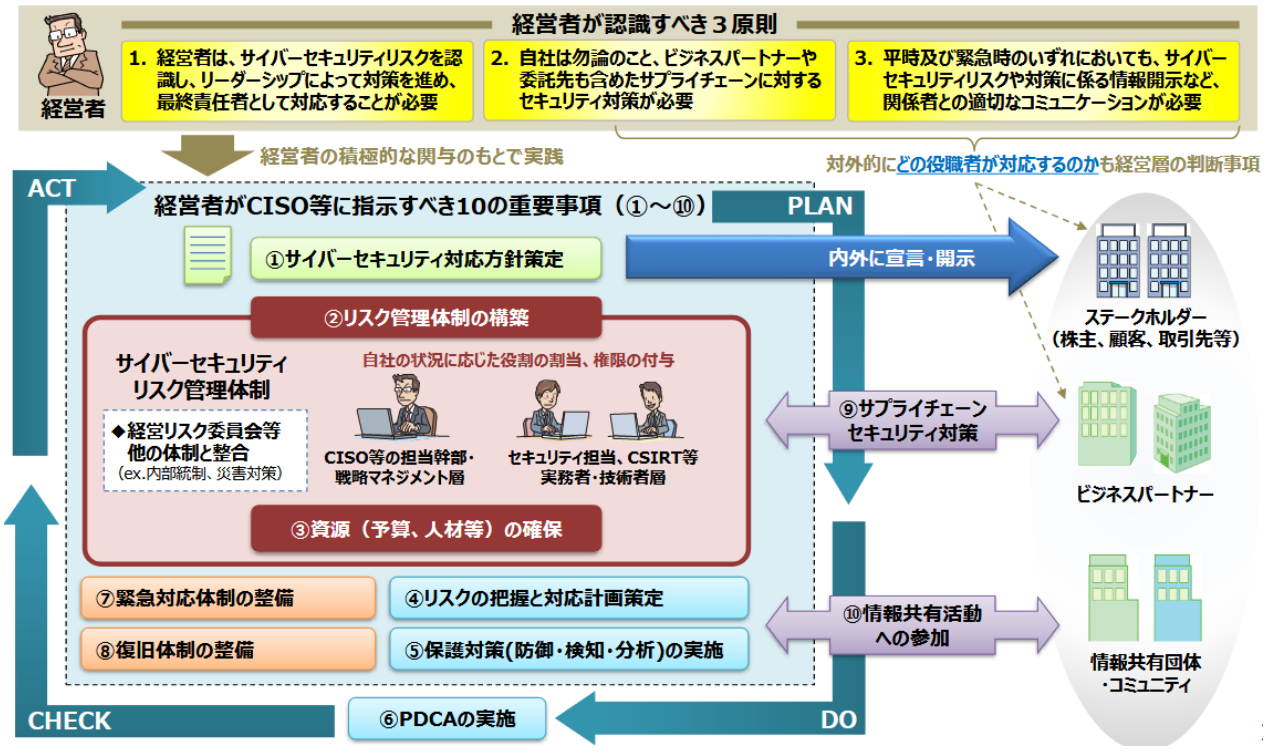
(*1) 機密性 2 情報は、非公開情報だが秘密文書に該当しない情報。なお、機密性 3 情報は、秘密文書に該当する情報、機密性 1 情報は、公開情報。

6. サイバーセキュリティ体制構築・人材確保の手引き更新

第 2.0 版の公開

経済産業省は 2022 年 6 月 15 日に、リスク管理体制の構築と必要な人材の確保するためのポイントをまとめた『サイバーセキュリティ体制構築・人材確保の手引き』を更新し、第 2.0 版として公開しました。この手引きは、経済産業省が独立行政法人情報処理推進機構（IPA）とともに策定した「サイバーセキュリティ経営ガイドライン」の付録という位置づけです。

第 2.0 版では、第 1.1 版をもとに読みやすさを重視してポイントを絞って検討手順を明確化し、「プラス・セキュリティ」の必要性を踏まえ、一部内容の更新・拡充を行っています。プラス・セキュリティとは、業務遂行にあたってセキュリティを意識し、必要かつ十分なセキュリティ対策を実現できる能力を身につけること、あるいは身につけている状態のことと定義されています。



図： サイバーセキュリティ経営ガイドラインの全体像における「手引き」の位置づけ（今回の『手引き』は左図赤枠部分（②、③）を具体的に検討するための参考文書）

出典： https://www.meti.go.jp/policy/netsecurity/tebikigaiyou2.pdf

7. サイバーセキュリティ対策への示唆

以上に述べてきた通り、この四半期の間に行政機関から多くの文書が決定、公表されてきました。これらから、我々はどのようなことを考えて対策に取り組めばよいのでしょうか。

例えば、現在ほぼすべての金融機関で、サイバー攻撃を受けたときの規程、手順書は整備されています。すなわち、サイバー攻撃を受けた際の対応は決められているのです。問題はその実効性です。決められた通りの対応をすれば、本当に被害を最小限に食い止められることを、自信を持って言える金融機関は少ないのではないでしょうか。そして、これは金融機関に限った話ではないと思います。サイバーセキュリティ対策の実効性の向上には、演習を積み重ねて、既存の対策をブラッシュアップしていく以外にありません。

そこで、本項では行政機関からの公表文書をベースに、ブラッシュアップの方向を考えてみたいと思います。望ましい方向は、大きく 3 つあると考えられます。

1 つ目はサプライチェーンを意識することです。1-2 で取り上げた『重要インフラのサイバーセキュリティに係る行動計画』で、「サプライチェーン」という言葉は 25 回登場しています。2022 年 2 月、小島プレス工業の情報システムがランサムウェアとみられるサイバー攻撃を受け、その影響で部品供給先のトヨタ自動車の国内全 14 工場が停止に追い込まれた事例は、たった一か所への攻撃であっても、いかに大きな影響を生じうるかを示しています。サプライチェーンを構成する組織は、自らの対策を講じる際に、サービスがどのようなサプライチェーンを通じてお客様の許に届くか、及び、サプライチェーンのどこがサイバー攻撃に遭ったらどのような影響があるのかをシミュレートしておくことが大切です。これを、サイバー演習のシナリオ作りや、実際のサイバー演習を通じて組織内に共有し、対策のブラッシュアップにつなげることが重要です。ここで、１つ注意しなくてはならないことは、サプライチェーンは必ずしも会社どうしのチェーンだけではない、ということです。実際には人対人、部署対部署、本部対本部、など様々なレベルでサプライチェーンは構成されています。サプライチェーンが攻撃を受けるということは、突き詰めれば端末が攻撃を受け、その影響が大きく広がっていく、ということです。その端末がどのような属性のときにどのような事態をもたらす可能性があるのか、緻密に考えておくことが重要です。10 ページに記載した「サイバー・フィジカル・セキュリティ対策フレームワーク」にある図は、サイバー攻撃がサイバー空間とフィジカル空間の双方に影響があることを示しています。この図をイメージして、影響の把握に漏れのないようにすることも有効でしょう。

2 つ目はリスクマネジメントです。『重要インフラのサイバーセキュリティに係る行動計画』で、「リスクマネジメント」という言葉は 38 回登場します。これまで、NISC や金融庁などから発表されるサイバーキュリティ関連文書には、経営層がサイバーセキュリティへの意識を高めることを促す記載が多く見られました。一方、今回発表された行動計画では、経営層がサイバーセキュリティに意識を持つことはすでに当然であり、今後はコーポレートリスクの一部としてサイバーリスクを捉え、これを管理していくことが必要だ、という姿勢が感じられます。すなわち、自らが晒されているリスクをきちんと洗い出し、それぞれのリスクに対して現在どのような対策がとられているのかをまず把握する。それをベースに、それぞれのリスクのコントロールできていない部分を把握する。そして、コントロールできていないリスクについて、それを保有するのか、移転するのか、低減するのか、回避するのかを決定して対応し、一連のプロセスの PDCA サイクルを回す。こうした基本的なリスクマネジメント活動に、サイバーリスクを対象として組み入れる、ということです。

ただし、その前提として、IT 関連資産の棚卸しが必要であることは言うまでもありません。例えば、あるソフトウェアの脆弱性情報を受け取った場合、自社でそのソフトウェアを使っているのか、さらにそのソフトウェアを構成する部品はどのようなものかがわからなければ、対応の要否の判断がつきません。11 ページに記載したソフトウェア部品表（SBOM）の話は、このような状況に役立てられることが期待されての動きです。

3 つ目はレジリエンスです。レジリエンスとは、通常ではない悪状況に陥ったあと、すばやく通常に戻れる能力のことを言います。サイバー攻撃は激しさを増す一方であり、どのような対策を打ったとしても、防ぎきれる保証はありません。ならば、マルウェアに感染したあと、あるいは不正に侵入されたあとに、いかにシステムを迅速に復旧できるかにフォーカスした対策が重要だ、ということです。ご紹介した「4　サイバー攻撃被害に係る情報共有・公表ガイダンスの検討」は、サイバー攻撃を受けた経験を相互に共有しあい、被害を最小限に抑えることが重要、との認識に基づいています。被害を最小限に抑えることは、レジリエンス能力を高めることにより実現できます。レジリエンスは、実戦さながらの演習によって高められていきます。システム的な防御だけでなく、対応にあたる人、対応マニュアルの妥当性を含めて評価することが必要です。

行政機関の決定や公表文書を活用することには、客観的に見て質の高い取組みを効率的に行えるというメリットがあります。第 1 部でご紹介した文書から、以上の 3 つの方向を意識しつつ進めることが、今後のサイバーセキュリティ対策のレベル向上を効率よく進めるうえでポイントになると考えられます。

第 2 部：インシデント事例の紹介

1. ランサムウェアによる事業停止

概要

2021 年 10 月 31 日未明、徳島県つるぎ町立半田病院が Lockbit2.0 によるランサムウェアに感染し、電子カルテなどの端末や関連するサーバーのデータが暗号化され、データが使用できない甚大な被害が生じました。侵入経路は導入している VPN（仮想プライベートネットワーク）装置の脆弱性を悪用して侵入したものと思われます。

感染確認後は、ネットワークの遮断や端末の停止、救急や新規患者の受け入れを中止、手術も可能な限り延期にするなどの対応が行われ、病院としての機能は事実上、停止する状態に陥りました。

被害状況

有識者会議調査報告書によると、幸いにして、フォレンジックを請け負った事業者が、データを確認できる範囲で元の通り復元をすることができました。その後、端末の初期化対応を行い、端末を再利用したり、システムやネットワークを最低限見直したりした上で通常診療の再開まで 2 ヶ月（2021 年 10 月 31 日未明～2022 年 1 月 4 日）かけて復旧しました。

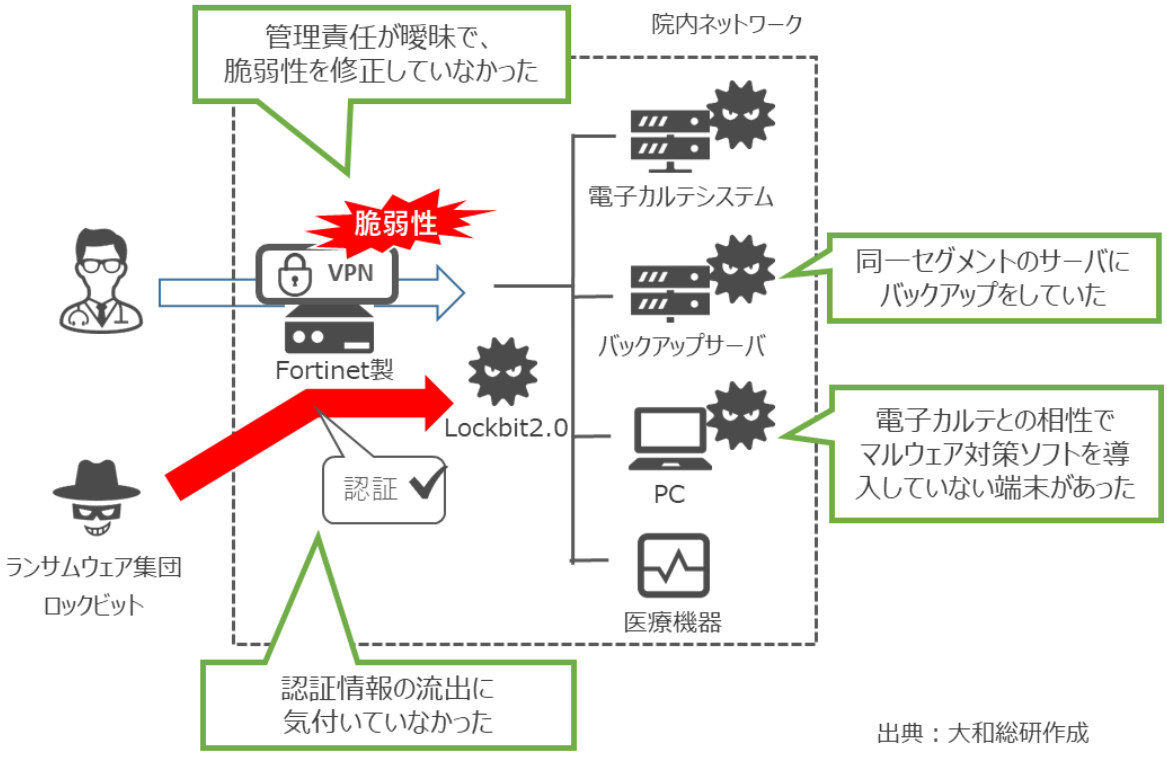
復旧までの期間、システムが使えなかったことで患者の予約状況や個人情報が分からなくなっていたため、受付で職員が患者から過去の記録を聞き取り紙のカルテに記録する等の状況が続き、病院側だけでなく患者への負担も少なからず生じることになりました。

半田病院における問題点

VPN 装置の脆弱性管理を実施していなかった点、同脆弱性を利用した認証情報が漏洩したが、ID、パスワードを変更していなかった点があげられます。

Fortinet 社の VPN 装置 FortiGate 60E の脆弱性（CVE-2018-13379※）は 2019 年 5 月に発表されており、2021 年 9 月に同脆弱性を悪用し全世界で 87,000 台の ID、パスワードが公開されました。その漏洩データに、半田病院のグローバル IP アドレス、ID、パスワードが含まれていましたが対応が取られていませんでした。

※　細工を施したデータを VPN 装置に送信することで、VPN 装置のシステムファイルがダウンロードでき、結果として、システム管理者の ID、パスワードを入手でき、インターネットから閉域網内に侵入が可能となる脆弱性



出典：大和総研作成

得られる教訓と考えられる対策（ソリューション）

半田病院のような 200 床未満(全体の 54.1％)は、一般的に IT 部門を持っていません。セキュリティ対策について医療システム事業者やサポートベンダーに頼らざるを得ない状況になるのは仕方なく、予算が限られている中の局所の対応に留まりがちです。

また、 組織の大小に依らず IT 運用のマネジメント不全は経営者の責任といえます。経営者は、サイバーセキュリティリスクを認識し、リーダーシップを発揮して、ビジネスパートナー、IT システム管理の委託先を含めたセキュリティ対策を進めることが必要です。

システムを正しく管理して運用するための仕組みである IT ガバナンスを実施する際には、NIST のサイバーセキュリティフレームワーク（CSF）等のフレームワークの利用が大いに役立ちます。本件では、セキュリティの継続的なモニタリングとなる「検知」のプロセスが不十分であったため、情報漏洩や脆弱性の情報を収集できずに認知できていませんでした。サポートベンダーから本脆弱性の説明が利用者に行き届いていないことも問題であったものの、サポートベンダーと事前に取り決めておくなど何らかの手段で情報を収集する体制を整えておくことが重要です。

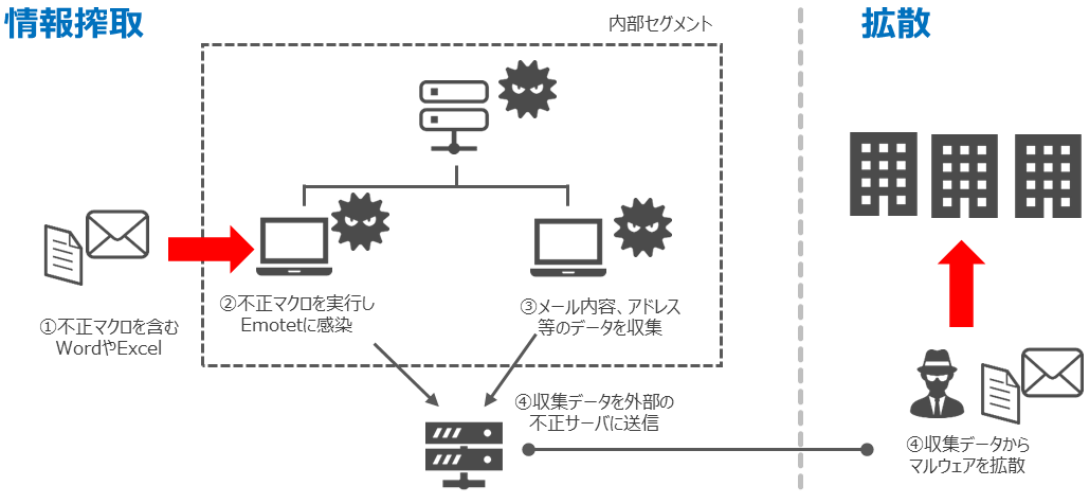
NIST サイバーセキュリティフレームワーク（CSF）

2. マルウェア Emotet の感染拡大

Emotet とは

2014 年に初めて発見されたマルウェアで、E メールの添付ファイルを感染経路とする不正プログラムです。添付された Word や Excel ファイルを開封後に「コンテンツの有効化」をクリックしてしまうと Emotet に感染する仕組みです。感染すると、メール情報やアカウント情報の流出、Emotet ばらまきの踏み台、不正送金マルウェアやランサムウェア等の二次感染などのリスクがあり、更に、金銭面だけでなく、正常化するまでに人的リソースを割かれ、システムが稼働不能になることで操業停止に陥る場合もあります。 JNSA（NPO 日本ネットワークセキュリティ協会）の調査によると、ランサムウェアによる身代金の被害金額は、平均値約 2,400 万円、中央値約 860 万円で、企業の情報漏洩事件による損害賠償は、一件あたり平均 6 億 3,000 万円となっています。

Emotet は 2021 年 1 月に、世界各国の捜査機関の連携によりマルウェアをコントロールする C&C サーバーを停止させてマルウェアを無害化するテイクダウンがされています。しかしながら、それから 1 年も経たない 2021 年 11 月に活動の再開が確認され、2022 年 1 月からは活動が活発になり、多くの企業で被害が発生しています。国内での感染も 2022 年 2 月から急速に拡大しており、警視庁や IPA なども注意を呼びかけている状況です。



出典：大和総研作成

Emotet の進化

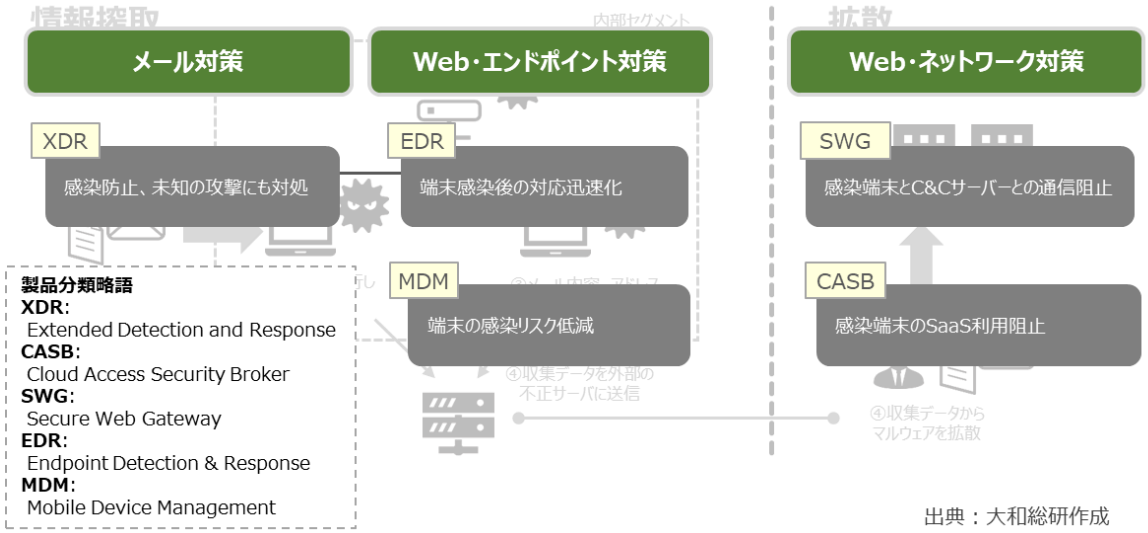
これまで Word や Excel のマクロを利用した攻撃が主流でしたが、2021 年から新しい攻撃手法や機能が確認されています。例えば、PDF のプレビュー用アプリを装った攻撃（2021 年 11 月）やショートカットファイル（.lnk）を利用した攻撃（2022 年 4 月）です。感染により、Google Chrome に保存されているクレジットカード情報を外部送信（2022 年 6 月）することも確認されています。

効果的な対策

1. 多層防御

Emotet にはエンドポイント（パソコンなどのネットワークの末端にあるデバイス）のマルウェア対策が基本であり有効と言われていますが、昨今は感染の手口は巧妙で多岐に及ぶため、単体の防御策で終わらすのではなく多層防御の考えが重要になってきています。

例えば、EDR（Endpoint Detection and Response）製品は、エンドポイント上でマルウェアやランサムウェアによる不審な動きがないかどうか、常時監視を行います。メモリ上などにおいて不審な動作を検知することで、万一ネットワーク内に侵入された場合の被害拡大を最大限抑えることができます。また、各レイヤーの対策として、侵入後のマルウェアをコントロールする C&C サーバーへのアクセスをブロックするための Web 対策に SWG（Secure Web Gateway）製品の導入などが考えられます。



出典：大和総研作成

2. 教育

Emotet は進化しており、受信した Email の送信元を確認せずに添付ファイルをすぐに開いてしまうなど従業員のサイバーセキュリティへの意識が低ければ、最新のツールや機器を導入しても感染を防ぐことは困難です。e ラーニング、メール訓練、自己点検チェックシート等を用いて、「攻撃メールが届いたらどう対処したらいいのか」「感染の疑いがある場合の対処法は」といった教育を定期的かつ継続的に実施することが重要です。

サイバーセキュリティ対策にゴールはありません。サイバーセキュリティ環境は刻々と変化しています。環境の変化に伴い教育内容をブラッシュアップし、定期的（半年、1 年程度）なフォローアップ教育が必要です。教育後にテストを行って従業員の理解度を試してみる等、教育の効果を確認しながらサイバーセキュリティ対策を継続していくのが効果的と言えます。

DIR SOC Quarterly 2022 the first issue
2022 年 9 月 29 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

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

大和総研
Daiwa Institute of Research