SIセキュリティ認定制度について

～事業者責任の時代にどう対応するのか～

IT連
日本IT団体連盟

本日のAgenda

- 政策の流れとその影響
- SIセキュリティ認定制度について

政策の流れとその影響

病院におけるランサムウェア事案からの学び

日本経済新聞

朝刊・夕刊　LIVE　Myニュース

トップ　速報　オピニオン　経済　政治　ビジネス　金融　マーケット　マネーのまなび　テック　国際　スポーツ　社会・調査　地域

ランサム攻撃でカルテ暗号化　徳島の病院、インフラ打撃

事件・司法　＋フォローする

2021年11月12日 11:30

保存

サイバー攻撃で電子カルテによる診療が中断されている半田病院（2日、徳島県つるぎ町）＝共同

徳島県つるぎ町の町立半田病院を10月末、サイバー攻撃が襲った。病院のシステムに侵入して情報を暗号化し、復旧と引き換えに金銭を要求するコンピューターウイルス「ランサムウエア」に感染した。約8万5千人分の電子カルテが閲覧できなくなり新規患者の受け入れを停止。復旧のめどは立っていない。命を守る地域の重要インフラは大打撃を受けた。

NHK

NHKについて　コロ

NEWS WEB　新着　天気　動画　特集　社会　気象・災害　科学・文化　政治　ビジネス　国際

関西 NEWS WEB　◀ 大阪の

大阪急性期・総合医療センター サイバー攻撃で診療影響続く

11月01日　15時55分

「ランサムウエア」と呼ばれる身代金要求型のウイルスによるサイバー攻撃を受けた大阪急性期・総合医療センターでは、１１月１日も緊急以外の手術を停止するなど影響が続いています。
病院を訪れた患者からは「どこかに情報が流出してしまったら怖い」などと不安の声が聞かれました。

大阪・住吉区の大阪急性期・総合医療センターでは、１０月３１日、「ランサムウエア」とよばれる身代金要求型のウイルスによるサイバー攻撃を受け、電子カルテなどのシステムに障害が発生して閲覧などができなくなっています。
このため、病院では３１日に続き、１日も朝から通常の外来診療や緊急以外の手術を停止しているほか、救急患者の受け入れもできない状況だということです。
病院には１日午前中から、診察の予約をしていた患者が訪れ、職員から説明を受けたりしていました。

調査報告書が指摘する事業者の責任

- **専門家のセキュリティの知識や経験**が乏しければ、問題を抱えながら運用していることになる。
- 各地域の情報技術を生業とする**事業者の セキュリティ教育と強化が必要**である。
- **事業者としての信頼性を証明するための評価制度**などを設けて、セキュリティレベルの持続的な向上に努めていく必要もある。


徳島県つるぎ町立半田病院
コンピュータウイルス感染事案
有識者会議調査報告書

2022年6月7日

徳島県つるぎ町立半田病院　コンピュータウイルス感染事案有識者会議調査報告書　2022年6月7日　より抜粋

調査報告書が指摘する社会的課題

調査委員会としての気付き事項と国に期待する事項　（調査報告書20～21頁）

契約時の責任分界の合意が問題に

① **地域医療への脅威からの保護**
- 今回の事案はどの医療機関でも起こりうる大きなリスク
- 医療分野のネットワーク化が推進される中で、セキュリティ向上は必須課題
- 国においては、ガイドラインや法整備、財源の確保など、その役割はますます重要

② **役割と責任分界点の明確化**
- ステークホルダーそれぞれの責任分界点や役割分担が非常に曖昧
- 発注者と受注者の間で「情報の非対称性」が存在する中で、ガイドラインに基づく契約時の文書による役割の明確化が必須
- 国においては、ガイドラインの運用推進および周知徹底により、情報セキュリティに係る各契約の役割や責任分界点の明確化を推進していくことが必要

③ **閉域網意識の見直し**
- 医療情報を扱うシステムベンダーや医療機器メーカーのセキュリティ意識は、閉域網神話から決して高いない
- 医療分野において高度かつ複雑な様相を呈するシステム化やネットワーク化が推進される中で、医療系セキュリティ意識及び見識の向上は早急に必要
- 国においては、セキュリティ対策向上に資するレギュレーションの策定や整備とともに、それらを業界く取り組みが求められる

④ **医療継続支援への更なる取り組み**
- 情報システムに依存している医療においては、大規模システム障害が起こりうる状況にあるという前提想定した対策が必要
- 国においては、医療機関へのサイバー攻撃を災害の一つとして捉え、その支援対策を充実させるなど、に医療を受けられるよう、更なる取り組みの推進が必要

調　査　報　告　書

2023年3月28日

地方独立行政法人大阪府立病院機構
大阪急性期・総合医療センター
情報セキュリティインシデント調査委員会

大阪急性期・総合医療センター 情報セキュリティインシデント調査報告書 概要 2023.3.28 調査委員会　より抜粋

調査報告書が指摘する社会的課題

課題解決のための提言　（調査報告書65～66頁）

① **医療継続のための取り組み支援**
- 自助（病院の）努力は必要性を理解した上で、国や地方公共団体は医療機関のサイバーセキュリティの継続的な向上のために、また地域医療を安定的に持続するために、以下のような支援や対応を願いたい。
  - ✓ 「財政的」「人的」「物的」、そしてスキルなどの「情報的」視点の支援
  - ✓ 厚生労働省の初動対応支援・調査事業は可能な限り継続
  - ✓ 診療録管理体制加算とは別建ての医療情報システムの管理およびセキュリティ強化や
    酬の評価が必要

② **セキュリティ機能の集中・集約化**
- すべての医療機関でのセキュリティ責任者の設置を目指し、サイバーセキュリティ
  すべての医療機関にセキュリティ支援が行えるような人材共有の枠組みが必要
- 医療機関におけるSOCを含めたセキュリティの集約を都道府県や国レベルで整備し、セキュリ
  フォーム化を検討するなど、個別医療機関のセキュリティ負荷を軽減が必要

③ **脆弱なシステムや機器を生み出さないための根本的な仕組み**
- 国において現状の医療機関でも適用可能な現実的かつ実践的なガイドラインの整備が必要
- 国においてシステムや機器の根本的な設計思想の転換を促す薬事法・薬機法の解釈や改正の議論が必要
- セキュリティにおける共通の考え方や枠組み、またセキュリティ運用を踏まえた現実的かつ具体的な規格が必要

④ **インシデント情報等の共有の場**
- 医療機関同士がセキュリティインシデントの情報共有などで連携できる枠組みについて、早期立ち上げ、運用開始が必要

脆弱性を防ぐ、国としての取り組みが求められている

大阪急性期・総合医療センター 情報セキュリティインシデント調査報告書 概要 2023.3.28 調査委員会　より抜粋

セキュリティバイデザインに対する政府の取り組み

経済産業省

資料3　サイバーインフラ事業者に求められる役割等の検討の方向性

ガイドライン等の実効性の強化

（セキュアなIoT製品及びソフトウェアの流通に向けた取組等）

実効性強化

ベンダーの取り組みを強化する流れ

- セキュリティ対策レベルを評価し、それを可視化する取組の**先行例として、IoTセキュリティ適合性評価制度を検討中。米欧等の諸外国との制度調和を図るための議論も継続中。**
- また、**SBOM（ソフトウェア部品構成表）**導入時の課題検証のための実証や企業向けの手引書を策定。
- IoTセキュリティ適合性評価制度の実効性強化やSBOMの導入促進に向けては、**産業界との連携のほか、政府調達等の要件化等に向けて関係省庁と議論も開始。**
- さらに、米国が策定し、我が国政府も共同署名をしたセキュア・バイ・デザインのガイダンスも踏まえ、**ソフトウェア開発者が行うべき取組整理**や**安全なソフトウェアの自己適合宣言の仕組みの検討**を行っていく。

IoTセキュリティ適合性評価制度

- 幅広い**IoT製品を対象**として、一定のセキュリティ基準を満たすものを認証し、ラベルを付与する制度の整備に向けて、検討を実施。その結果を2024年３月に取りまとめ、**2024年度中に一部運用を開始**予定。

SBOMのイメージ

- **SBOM（ソフトウェア部品構成表）**がソフトウェアのセキュリティの脆弱性を管理する手法の一つとして着目。

サプライヤ名	コンポーネント名	バージョン	製品URLなど	…
A会社	ソフトウェアA	Ver1.0	……	…
A会社	└…ソフトウェアa	Ver2.1	……	…
B会社	└…ソフトウェアb	Ver5.3	……	…
C会社	└…ソフトウェアc	Ver1.2	……	…

セキュアバイデザイン・セキュアバイデフォルト

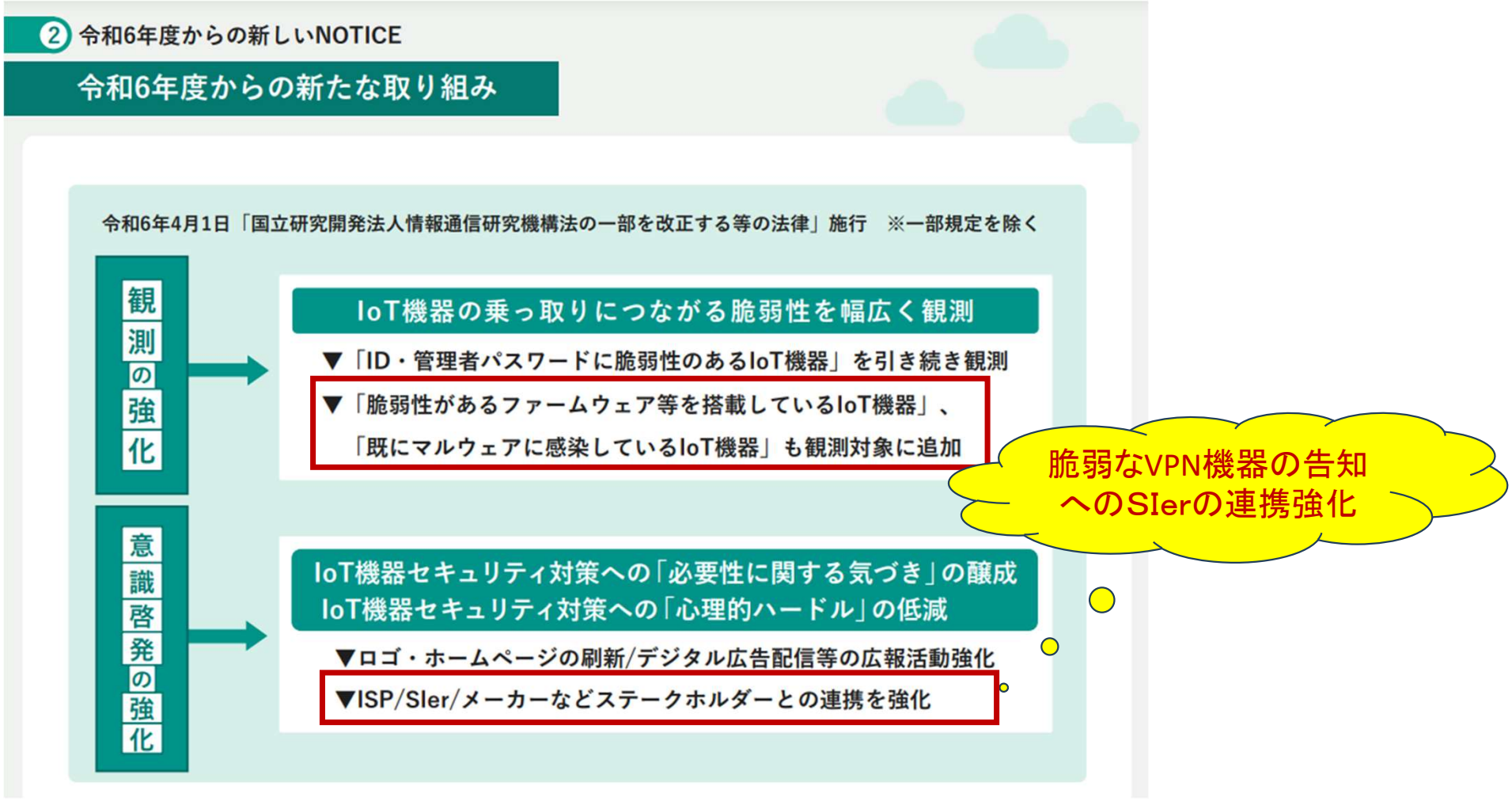
- **セキュア・バイ・デザイン**：IT製品（ソフトウェア等）が、設計段階から安全性を確保されていること。
- **セキュア・バイ・デフォルト**：ユーザーが、追加の手間をかけることなく、購入後すぐにIT製品（ソフトウェア等）を安全に利用できること。

（出典：国際共同ガイダンス「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」）（2023年10月28日署名）

サイバー攻撃に悪用されるIOT機器の調査(NOTICE)

総務省

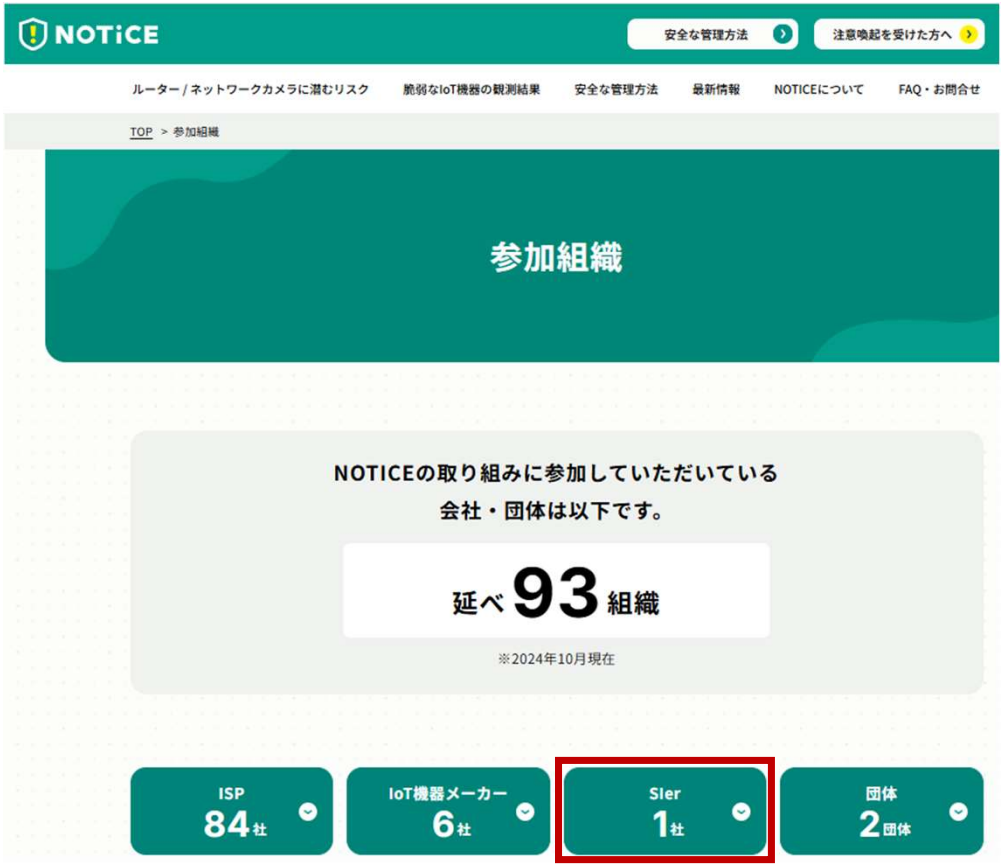
ICTサイバーセキュリティ政策分科会（第7回）NOTICEの活動について（事務局）



サイバー攻撃に悪用されるIOT機器の調査(NOTICE)

総務省

https://notice.go.jp/org

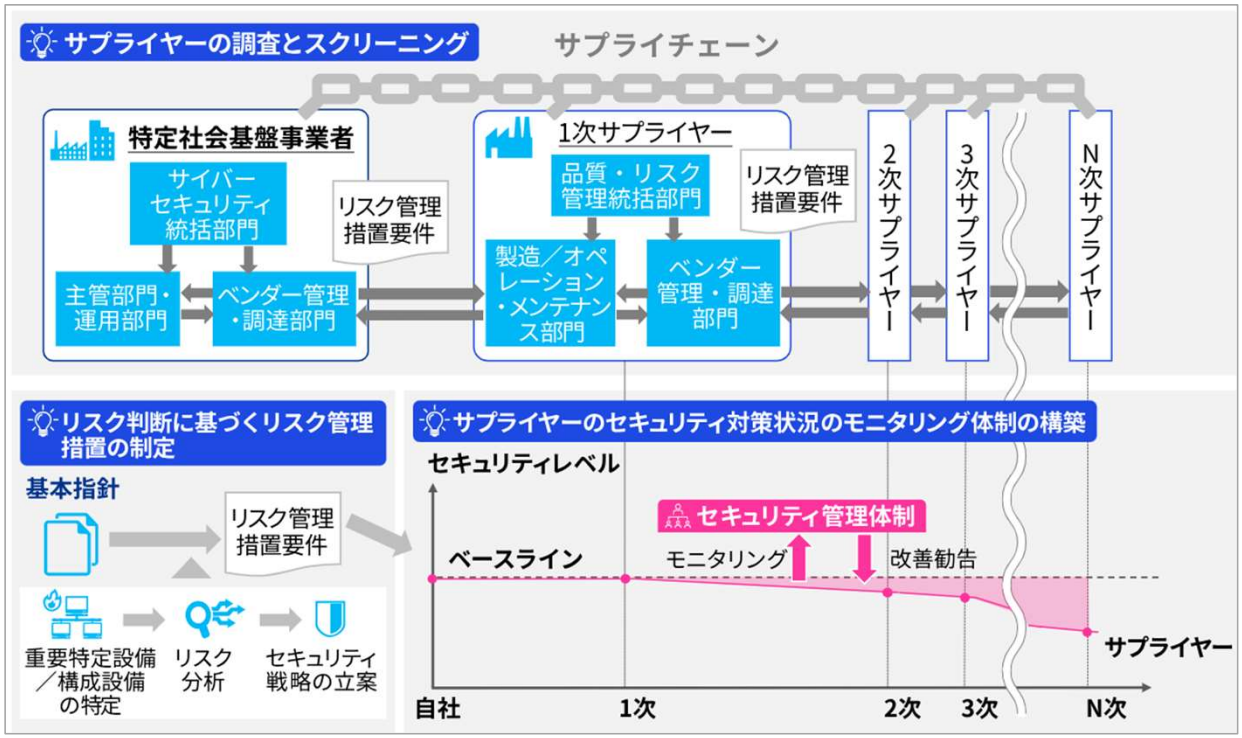


サプライチェーンセキュリティへの対策の先行事例

内閣府
所管省庁

■「基幹インフラ役務の安定的な提供の確保に関する制度」においてやるべきこと

本制度は、特定重要**設備の導入、維持管理のサプラチェーンにおけるリスクを特定**し、経済・社会秩序の平穏を損なう恐れのあるサイバー攻撃をはじめとした外部からの妨害行為に対して、継続的にリスクを低減、または排除する仕組みを各事業者が作ることを求めています。



★国が、発注者である基幹インフラ企業（エンドユザー）に求める事項

✓ 委託先に関する届出事項例
⇒**委託の相手方の名称他**

✓ **サプライヤーの調査とスクリーニング**
⇒「リスク管理措置要件～モニタリング～改善勧告」

※対象業種：基幹インフラ
金融、クレジットカード、電気、ガス、石油、水道、鉄道、物流、貨物、航空、空港、電気通信、放送、郵便、港湾、
（**医療、防衛**、政府・**行政サービス（地方公共団体を含む）**）
※この他、「ビジネスを欧米市場展開されている企業」では、EUの規制等で既に影響を受ける顧客企業もあります。

貴社の顧客に対象はありませんか？

「認定」や「要件」を業界の自助努力として建付け、
👉「認定」や「要件」を、きちんと制度化することにより、ビジネスの上でも大きな施策として活用することができるはず!!

サイバー対処能力強化法案※1
及び同整備法案※2について

※1　重要電子計算機に対する不正な行為による被害の防止に関する法律案
※2　重要電子計算機に対する不正な行為による被害の防止に関する法律の施行に伴う関係法律の整備等に関する法律案

令和７年２月
内閣官房
サイバー安全保障体制整備準備室

新法①【官民連携の強化】

基幹インフラ事業者が*サイバー攻撃を受けた場*…*民間事業者等への情報共有、対処支援等の取組を強化*

基幹インフラ事業者の
インシデント報告義務化

基幹インフラ事業者によるインシデント報告等

（新法第２章関係）

- 基幹インフラ事業者は、特定重要電子計算機を導入したときは、その製品名等を事業所管大臣に届出（当該事業所管大臣は当該届出に係る事項を内閣総理大臣に通知）
- 基幹インフラ事業者は、特定重要電子計算機のインシデント情報やその原因となり得る事象を認知したときは、事業所管大臣及び内閣総理大臣に報告

情報共有・対策のための協議会の設置

（新法第９章関係）

- 内閣総理大臣は、サイバー攻撃による被害の防止のため、関係行政機関の長により構成される「情報共有及び対策に関する協議会」を設置
- 協議会には、基幹インフラ事業者、電子計算機等のベンダー等をその同意を得て構成員として加える
- 構成員に対しては、守秘義…情報を共有するとともに…が可能

ベンダーに対する脆弱
性対策の要求の強化

脆弱性対応の強化

（新法第８章第42条, サイバーセキュリティ基本法第７条関係）

- 内閣総理大臣・事業所管大臣（※）が重要電子計算機に用いられる電子計算機等の脆弱性を認知
  → 電子計算機等のベンダー等に対して情報提供、対応方法の公表・周知
- 基幹インフラ事業者が使用する特定重要電子計算機に用いられる電子計算機等に関連する脆弱性の場合
  → 事業所管大臣（※）は、その電子計算機等のベンダー等に対し、必要な措置を講ずるよう要請　　等

（※）電子計算機やそれに組み込まれるプログラムの供給を行う事業を所管する大臣

産業界へのメッセージ

経済産業省

産業界へのメッセージ（６）（ＩＴサービス等提供事業者向け）

- **自らの製品・サービスのセキュリティ対策に責任を持ち、「セキュア・バイ・デザイン」**（※１）**や「セキュア・バイ・デフォルト」**（※２）**の考え方に沿った一層の対応**（「顧客だけにセキュリティの責任を負わせない」、「トップ主導での実施」等の基本原則の遵守、SBOMの採用、メモリに安全なプログラミング言語の採用等）をお願いしたい。

※１「セキュア・バイ・デザイン」：IT 製品（特にソフトウェア）が、設計段階から安全性を確保されていること。前提となるサイバー脅威
スク評価が不可欠。

※２「セキュア・バイ・デフォルト」：ユーザー（顧客）が、追加コストや手間をかけることなく、購入後すぐに IT 製品（特にソフト
利用できること。

事業者の責任のリバランス

趣旨・背景

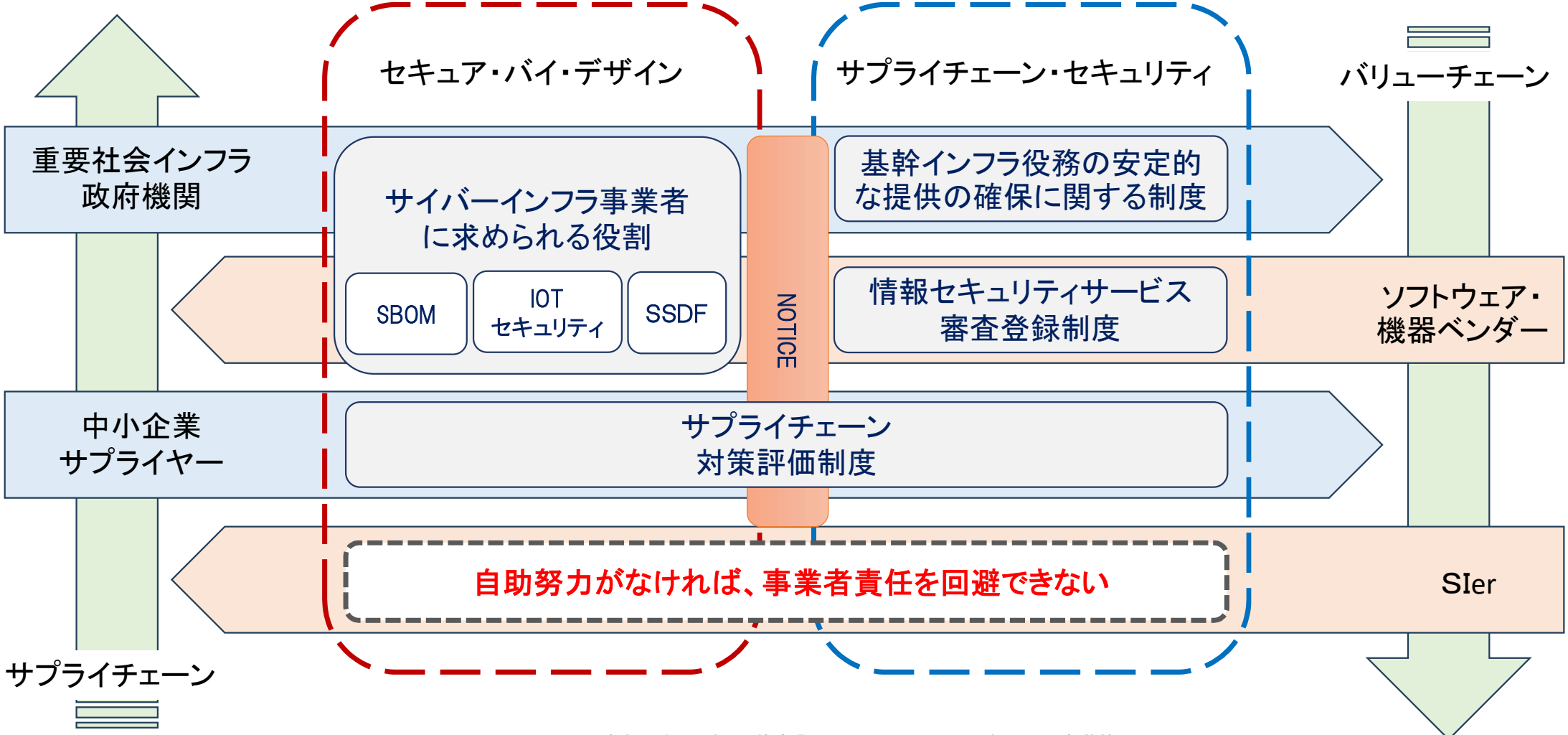
- 「セキュア・バイ・デザイン」は、**セキュリティの責任は製造者等が追うべきである（「責任のリバランス」）**、という**欧米諸国を中心に提唱されている概念**。
- 2023年4月に米国サイバーセキュリティー・インフラセキュリティー庁（CISA）が一部有志国と共に**セキュアバイデザイン・セキュアバイデフォルトの実践に向けた推奨事項をまとめたガイダンスを作成**し、**ソフトウェア開発者に対し、安全な製品を出荷するために必要な措置を講じるよう**促した。同年10月に本文書が改訂され、我が国を含む13か国が共同署名。その中でも、組織の変革を実行できる**経営層の意思決定者による**、製品開発の重要な要素としてセキュリティを優先させるという**コミットメントの重要性**が言及されている。**今後、当該提言を踏まえた対応が全世界レベルで求められていくことが想定される**。
- 今後、経済産業省としても、本文書も踏まえ、**ソフトウェア開発者が行うべき取組整理など推進のための取組を検討**していく予定。それにより、ITサービス等提供事業者が上記メッセージをより具体的に理解し、実践しやすい環境を整備していく。

関係する政府文書・窓口等

– 内閣サイバーセキュリティセンター「国際共同ガイダンス「Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Security by Design and Default」に署名しました」（令和５年10月）

SIセキュリティ認定制度について

政府の取り組みとステークホルダーの紐づけ



SIセキュリティ認定制度導入検討の背景

政策・市場環境

- セキュリティバイデザインを起点とした事業者責任追及の流れ
- サプライチェーンにおける中小企業リスク対策強化の具体化

ビジネス阻害要因

- 一定の事業者責任を果たさないことによる善管注意義務違反・訴訟リスク
- 必要以上に厳しい認定制度導入によるサプライチェーン、調達からの排除

ビジネス促進要因

- 認定制度により、安心安全を訴求し、競合優位を獲得
- 公共調達や補助金における優遇を目指す。

サイバーセキュリティ委員会の打ち手として

- 政府のガイドラインや認定制度を待つのではなく、自発的取り組みにより社会的課題の解決を目指したい。
- IT事業者のリスク回避だけでなく、サイバーセキュリティの伴走者として、安心できるIT環境やDX推進をしていきたい。
- 信頼できるIT事業者の団体としてのブランドイメージを確立する事によって、加盟企業の事業環境の改善を目指したい。

SIセキュリティ認定制度の導入検討を開始

SIセキュリティ認定制度要求事項（案）

大項目	中項目	内容	要求事項（レベル１）自己適合宣言	要求事項（レベル２）認定審査
① 企業の体制	管理体制の整備	経営者はセキュリティ管理体制を宣言している	中項目の徹底を供給者として宣言する	中項目の徹底を供給者として宣言する
	社内教育・指導	継続的にセキュリティ教育を行っている	セキュリティ基礎教育の定期実施	SecBokを元にセキュリティ資格取得の推進
	情報収集体制	平時・有事に外部と連携できる体制を持っている	団体、ISAC参加 により情報を入手するルートを持っている	団体、ISAC参加 により情報を入手するルートを持っている
	継続性の担保	PDCAが機能するように チェック体制を持っている	定期的レビューの実施	定期的レビューの実施
② 構築	セキュリティリスク評価	リスクに基づくセキュリティ要件を お客様と合意している	製品のセキュリティリスクの説明	情報セキュリティリスクアセスメント実施
	完成検査	導入時の脆弱性を低減する	設定のチェックリスト	標準に従った脆弱性検査の実施
	構成管理	ＩＴ資産を棚卸し、可視化している	顧客ネットワークへの影響度の確認	納入システムの構成管理表を提供する
	サプライチェーン管理	委託先を起点としたリスクを低減する	仕入れ先との情報セキュリティ合意	外部委託に対するセキュリティ管理体制
③運用	インシデント対応	ログ分析の重要性を認識し、 リスク評価を元に判断している	トラブル対応窓口の設置	セキュリティインシデントの処理・エスカレーションプロセス・対応手順があること
	脆弱性対応	継続的対応の必要性を認識している	脆弱性情報の提供プロセスがある事	構成管理を元にした運用体制の提供
	保守・保全	サポート範囲、条件を明文化している	サポート範囲を合意する手続きがある事	サポート範囲を合意する手続きがある事
④契約	Life Time Value への責任分解意識	有償・無償の責任範囲とリスクを 顧客と合意している	「重要事項説明書活用型」モデル取引・契約書	情報システム・モデル取引・契約書

SIセキュリティ認定制度の概要

- 網羅性よりも必要な項目に絞って適合性を評価します。
  - 大項目においては、①企業の体制、②構築、③運用、④契約に分け中項目に適合要件を定義し、内容を今後議論して行きます。
- 最低限必要なレベルから、あるべき姿を目指す2段階で構成しています。
  - セキュリティを提案・構築・運用する事業者を大きく2つにレベル分けし、それぞれ自己適合宣言と認定審査でカテゴライズしています。
    - 要求事項（レベル1）自己適合宣言（個別ソリューション納入事業者）
    - 要求事項（レベル2）認定審査（システム基盤構築事業者）
- 積極的に参加できる自己適合から始め、第三者認証を目指します。
  - 自己適合宣言においてはチェックリスト、認定審査においては審査書類の提出（今後詳細検討）を行う等、今後議論をしていきます。
  - 認定の信頼性を高めるための事後の抜き打ち検査や外部認証の利用、審査リソースの外注なども今後検討していく予定です。

SIセキュリティ認定制度詳細要件（案）企業の体制

大項目	中項目	内容	要求事項（レベル１）自己適合宣言	詳細要件(アクション詳細を今後検討)
①企業の体制	管理体制の整備	経営者はセキュリティ管理体制を宣言している	中項目の徹底を供給者として宣言する	法令を遵守し、サービス運用インフラ及びプロセスに関するすべての**セキュリティポリシーを文書化し、維持する。** ポリシーに基づいてセキュリティを確保するために必要な人員及び予算を確保する。
①企業の体制	社内教育・指導	継続的にセキュリティ教育を行っている	セキュリティ基礎教育の定期実施	全要員に対して情報セキュリティに対する経営層のコミットメントを周知し、**組織にとっての情報セキュリティの重要性を教育する。** 各役割のトレーニング計画を作成し、**全要員が習熟度と役割に応じてトレーニングを実施**できるように提供する。
①企業の体制	情報収集体制	平時・有事に外部と連携できる体制を持っている	団体、ISAC参加により情報を入手するルートを持っている	提供するソフトウェア製品及びサービスのセキュリティを改善するために、**民間企業同士、関係当局、専門組織との情報連携のための組織体制を構築**する。 コミュニティや協力体制に参加する場合には、**積極的に活動に関与し、協力体制に対して貢献**する。
①企業の体制	継続性の担保	PDCAが機能するようにチェック体制を持っている	定期的レビューの実施	ポリシーに基づくガバナンスにより、サービス運用インフラ及びプロセスの保護、及びサービスの**セキュリティ要件が全体にわたって維持されていることを定期的に見直し、継続的な改善を確認**する。

SIセキュリティ認定制度詳細要件（案）構築

大項目	中項目	内容	要求事項（レベル１）自己適合宣言	詳細要件(アクション詳細を今後検討)
②構築	セキュリティ リスク評価	リスクに基づくセキュリティ要件をお客様と合意している	製品のセキュリティリスクの説明	顧客の取組と契約に基づく取組を統合した**リスク管理を文書化し、合意する。** 開発するシステムのリスクを分析・評価し、**リスク対応、セキュリティ要件、設計上の決定事項を追跡し、対策を維持**する。
②構築	完成検査	導入時の脆弱性を低減する	設定のチェックリスト	ソフトウェアのセキュアな導入・設定の**情報を文書化し、ソフトウェアの取得者（ユーザー）が利用できるようにする。** 文書及びチェックリストは**平易で理解しやすく、スキルが低いエンジニアでも理解が出来るものにする。**
②構築	構成管理	ＩＴ資産を棚卸し、可視化している	顧客ネットワークへの影響度の確認	ネットワーク構成図、重要IT資産台帳の存在を確認し、**提案するセキュリティシステムに内包するリスクとその影響を分析**するとともに、明文化した上で**顧客に理解できるコミュニケーションに努める。**
②構築	サプライチェーン 管理	委託先を起点としたリスクを低減する	仕入れ先との情報セキュリティ合意	**委託先における情報セキュリティポリシー及びマネジメントシステムを確認し、契約の条件として合意する。** 情報管理上重要な委託先については、**必要に応じて監査を行う事が望ましい。**

SIセキュリティ認定制度詳細要件（案）運用

大項目	中項目	内容	要求事項（レベル１）自己適合宣言	詳細要件(アクション詳細を今後検討)
③運用	インシデント対応	ログ分析の重要性を認識し、リスク評価を元に判断している	トラブル対応窓口の設置	情報セキュリティインシデントが発生した場合に問い合わせることが出来る窓口を契約時に明確にするとともにWebでの明示や問い合わせシステムを使って**容易にコンタクトが出来るように努める。** **自社の対処能力を継続的に高める**と共に、自社での解決が困難な場合には**外部委託やベンダーへのエスカレーションプロセスを常に確認**しておく
③運用	脆弱性対応	継続的対応の必要性を認識している	脆弱性情報の提供プロセスがある事	すべての利害関係者に対するコミュニケーション計画を定め、**情報流通の実効性を担保するための情報の内容及びプロセスの改善を継続的に行う。** 公知情報の探索、ソフトウェア取得者からの通知、外部脅威情報の取得、システム構成データのレビュー、その他の方法を通じて、**新たな脆弱性情報を収集する。**
③運用	保守・保全	サポート範囲、条件を明文化している	サポート範囲を合意する手続きがある事	自社が提供したシステム及びソリューションを明確にし、**対応できるサポート範囲を可能な限り明確にする。** 複数のベンダーが関与したシステムにおいて、**自社がサポート出来ない部分に関しても、問題が発生した際の問い合わせ先を可能な限り明らかにする。** 製品に付随する無償の製品問い合わせと有償で提供する**サポートの区分けを明確にし、文書化し、顧客に明示的に説明を行い、合意の証拠を残す。**

SIセキュリティ認定制度詳細要件（案）契約

大項目	中項目	内容	要求事項（レベル１）自己適合宣言	詳細要件(アクション詳細を今後検討)
④契約	Life Time Value への責任分解意識	有償・無償の責任範囲とリスクを顧客と合意している	「重要事項説明書活用型」モデル取引・契約書	関係者間で**合意すべきセキュリティ要件を確立し、契約に盛り込んでいる。** 顧客の責任範囲も含めたシステム全体のセキュリティの責任を明確にするとともに、**適切に責任を果たさない場合のリスク及びその影響を明示的に説明を行い、合意の証拠を残す。**

最後に

- 本認定制度はまだ検討を始めたばかりです。
- 制度や詳細要件の詰めを行う為には、皆様の意見が不可欠です。
- 是非、趣旨にご賛同いただき、積極的な参画をお願いいたします。

ご清聴ありがとうございました。