NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

資料6
（一部非公開）

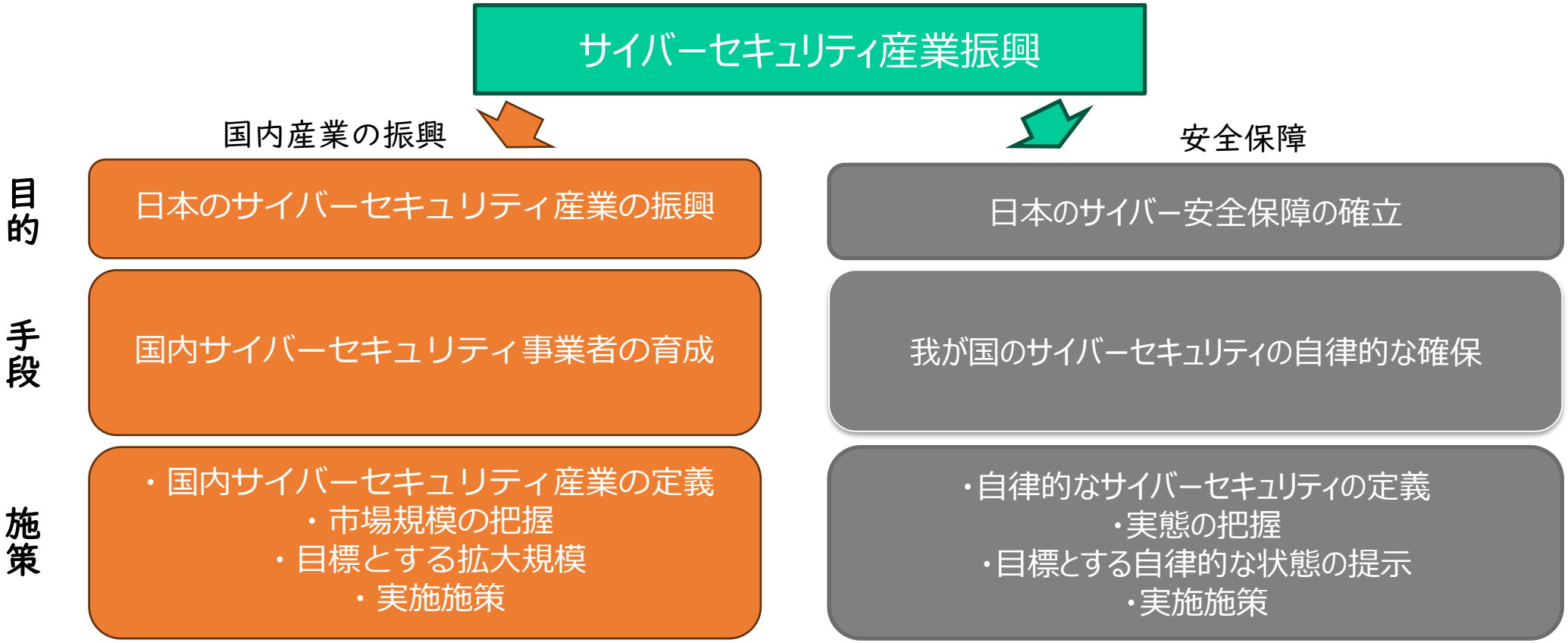
サイバーセキュリティ産業振興
ベンダー意見取りまとめ

NPO日本ネットワークセキュリティ協会
2024/10/29

論点の整理

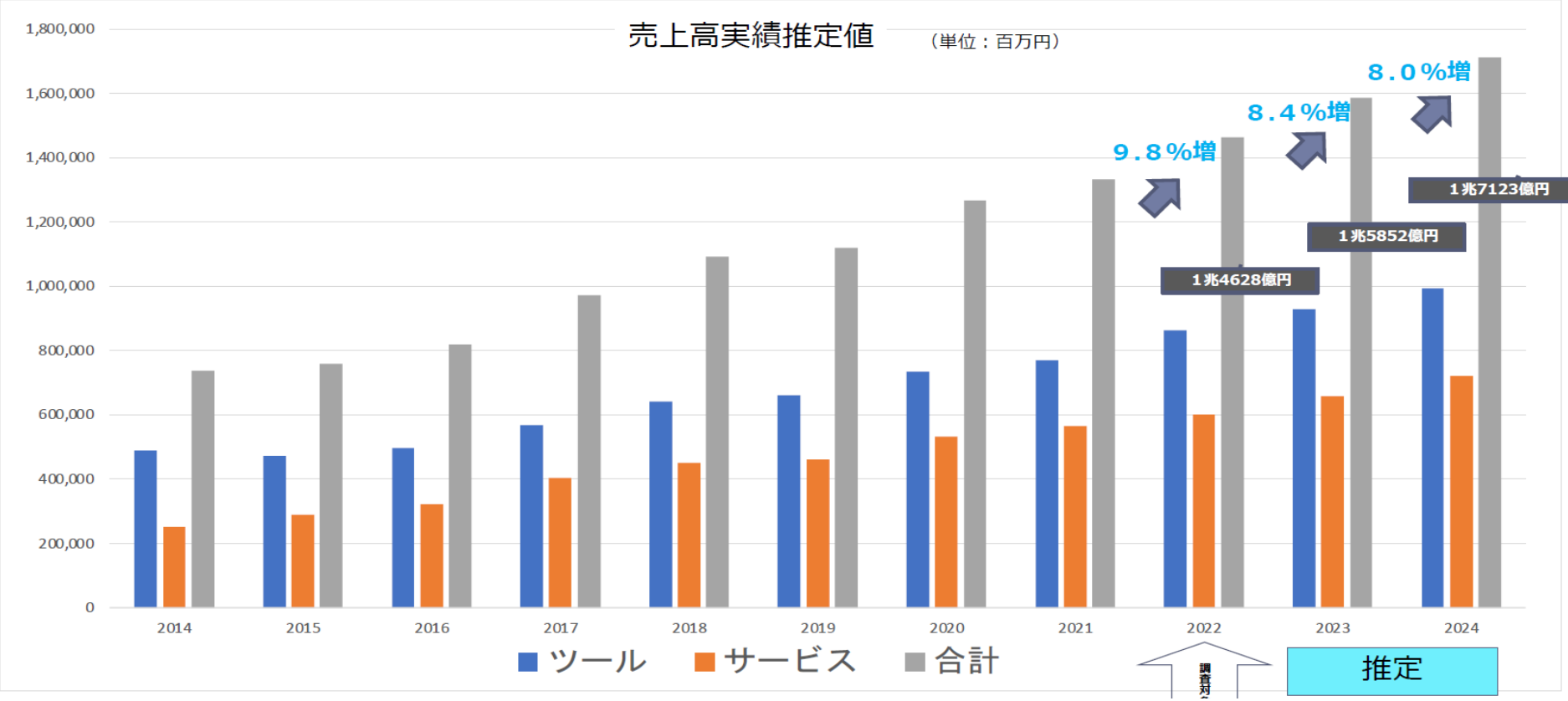
1. サイバーセキュリティ産業振興
2. 日本サイバー市場の現状
3. 日本のサイバーセキュリティ産業の課題
4. 政策要望案
5. 参考資料１ 会員意見取りまとめ
6. 参考資料２ 政策提言（2024年5月版）

Ⅰ．サイバーセキュリティ産業振興



産業振興と安全保障は分けて議論すべきではないか
（マーケットもプレイヤーも違うはず）
結果的に重なる部分があるとしても

２．情報セキュリティ市場の推移



情報セキュリテイ市場規模は、１兆７千億円と推計される

JNSA「2023年度 国内情報セキュリティ市場調査報告書」より

調査対象企業数と分布（2024年3月期）

区分	有効対象企業数	エンドポイント保護管理製品	ネットワーク防御・検知／境界線防御製品	コンテンツセキュリティ対策製品	アイデンティティ・アクセス管理製品	セキュリティツール	コンサルティング／診断サービス	マネージド・運用サービス	周辺サービス	セキュリティサービス
A	112	56	78	57	32	97	62	60	35	83
B	122	53	70	52	39	104	66	48	38	82
C	56	33	42	32	27	48	29	26	22	37
D	135	81	99	89	65	118	93	66	61	106
E	50	37	39	39	31	44	37	36	31	49
F	31	13	16	13	10	18	23	17	11	25
G	158	61	77	65	50	109	108	90	64	134
H	17	5	2	5	4	6	8	3	8	14
計	681	339	423	352	258	544	426	346	270	530

※黄色文字部分は兼業を含むため重複カウントあり。

区分		ツール専業	サービス専業	ツール・サービス兼業	有効対象企業数	分布割合
A	海外メーカまたはその日本法人	29	15	68	112	16.2%
B	国内のセキュリティツールメーカ	40	18	64	122	17.5%
C	販売店･商社等主として流通機能の企業	18	7	30	56	7.6%
D	SI・NI機能を有する二次･三次販売店	29	17	89	135	16.8%
E	SIが主たる付加価値の大手システムインテグレータ	1	6	43	50	5.7%
F	コンサルティング企業	6	13	12	31	4.8%
G	セキュリティサービス提供事業者	24	49	85	158	25.5%
H	その他　（サイバー保険・その他異業種）	3	11	3	17	5.9%
	計	150	136	394	681	100%

国内セキュリティビジネスの定義を行い、具体的にどの領域の市場規模を、どのくらい増やすのか目標値が必須

JNSA「2023年度 国内情報セキュリティ市場調査報告書」より

サイバー安全保障（サイバーセキュリティの自律）

IPA「重要情報を扱うシステムの要求策定ガイド」自律性確保の要件（一部抜粋）

運用	運用体制への国内法の強制
	運用体制の国内確保
	資本・支配関係の比較法的チェック
	人に対するセキュリティチェック
	データ持ち出しの可能性の確保（コスト面含む）
	運用操作の記録・監査・保全
	国内体制での障害および再発防止の対応
ソフトウエア	開発体制のセキュリティチェック
	サプライヤーのセキュリティチェック
	商用ソフトウェア（商用OSSを含む）への技術情報アクセスの確保
	自社開発ソフトウェア・OSSに対する自社でのメンテナンス体制確保
	メンテナンス処理の調整機構
データセンター・通信	機器の国内設置
	日本法と抵触する法体系の設置箇所への適用の排除
	運用操作の記録・監査・保全
	通信経路の信頼性確保
	データセンター・通信の冗長性の確保
	電力供給の継続性確保
	実地での立ち入り監査による実効性確保

防衛的側面において
他国依存性の低下（排除）

自律的なサイバーセキュリティの定義と具体的な**評価指標、目標値**の設定が必須

３．日本のサイバーセキュリティ産業の課題

- 政府機関や企業のITやサイバーセキュリティ対策の実装手段を海外製品・ツール・サービス等に依存している
- 公共性の観点から海外製の製品を真っ向から除外することが難しい
- 海外プラットフォーマーが国内スタートアップの参入障壁
- 独自製品の開発に取り組んだが、海外販売において数万台という検証規模の要求に答えられなかった
- ユーザやSIerの傾向として実績重視で製品やサービスを選択する傾向があり、新規参入のハードルが高い
- クラウドサービスにおいて、ISMAP(ーLIU)の存在が大きく、官公庁への参入においてはこの取得が大きいなハードル
- 国策の融資制度について、赤字の許容範囲が少なく利用しにくい
- 脆弱性検査ツールの開発など、攻撃手法の研究を意図的に避けている

４．政策における期待

■ 政府として、具体的にどの領域のビジネス規模をどの程度拡大するのか具体的な（数値として）目標をさだめていただきたい。

- ➢ 売上規模、市場占有率、サイバー自給率

■ 海外ベンダーと競合する領域で勝負することは極めて困難であり、戦える領域に注力いただきたい。

- ➢ 未開拓領域
  - 例）OT分野、SaaS、生成AI活用、データ連携
- ➢ 日本独自（強み）領域
  - 例）暗号、量子IT技術、日本の商習慣や法律が影響を与える分野
- ➢ 海外向けの参入障壁を設ける領域
  - 例）情報開示、報告義務化・・・・

4．政策要望（2025年候補案＝検討中）

1. 国内セキュリティ産業の振興:
   - 国産サイバーセキュリティ産業の定義と、市場の実態調査
   - 検証環境の整備: 新製品・サービスの検証環境を整備し、評価結果を公開することで、国内製品の信頼性向上を図る。
   - 政府調達の改善: 国産製品の優遇措置を検討し、国内産業の育成を促進する。
   - プラットフォーマー規制の強化: 基盤サービスとセキュリティ機能の抱き合わせ販売を禁止し、競争を促進する。
2. 人材育成:
   - 教育改革: 中学校・高校でのプログラミング教育の拡充、大学・高専でのセキュリティ教育の強化。
   - 人材育成支援: 海外人材の受け入れ促進、セキュリティ人材育成プログラムの拡充。
   - 産学連携: 企業と大学が連携し、実践的な人材育成を行う。
3. 法規制の強化:
   - リスクベースのアプローチ: リスクアセスメントに基づいた対策を義務化する。
   - 情報開示の義務化: 特定の規模以上の企業に対して、セキュリティに関する情報開示を義務化する。
   - インシデント対応の義務化: 重大なインシデント発生時の報告義務を課す。

4．政策要望（2025年候補案＝検討中）

4. 中小企業への支援:
   - 補助金制度の拡充: 中小企業向けのセキュリティ対策補助金を拡充する。
   - コンサルティング支援: 中小企業に対するセキュリティコンサルティングを支援する。
5. OTセキュリティの強化:
   - 国産ソリューションの開発: OT分野における国産ソリューションの開発を促進する。
   - 標準化の推進: OTセキュリティの標準化を推進し、相互運用性を高める。
6. 脅威インテリジェンスの強化:
   - 国産脅威インテリジェンスの開発: 自国の脅威インテリジェンスを開発し、共有を促進する。
   - 情報共有プラットフォームの構築: 官民連携による情報共有プラットフォームを構築する。

参考資料１：会員意見とりまとめ

非公開

参考資料２：2024年度JNSA政策提言

2024年5月にIT団体連盟より提言したもの

参考資料２：2024年度JNSA政策提言（重点要望）

1. 上場企業のセキュリティ投資・インシデント報告義務化及び優遇策

- 有価証券報告書に、当該企業のサイバーセキュリティ対策について詳細を記したホームページのURLを記載することを義務付けるとともに、その記載内容の成熟度に応じて「サイバーセキュリティ経営銘柄」として評価・選定する。
- 適時開示の対象に「サイバー攻撃の発生」を入れる。

2. 中小企業における情報セキュリティ対策強化支援の推進

- セキュリティリスクの現状評価（アセスメント）、導入計画策定業務
- セキュリティ対策システムの導入、および、運用（監視・保守）業務
- 運用評価業務（次年度以降の運用計画策定を含む）

3. 経済安全保障に資するサイバーセキュリティ自給率の向上

- 国産のセキュリティ製品、サービス、インフラへ依存度を計測する国産化率の指標（サイバー自給率）を整備するとともに、目標値を設定し海外への依存度の軽減を図る。
- 安全保障の観点から海外製品を使える領域使えない領域を明確にする。
- 国産セキュリティ対策製品・サービスの開発支援、例えば国産サービスに対する（単年度でない）複数年契約可能なクーポンや補助金の設定。
- 政府機関における、国産セキュリティ対策製品・サービス採用促進。
- 国内マーケットにおける、国産セキュリティ対策製品・サービス採用促進。
- 海外マーケットにおける、日本製セキュリティ対策製品・サービス販売促進。

参考資料２：2024年度JNSA政策提言（2）

4. 政府機関セキュリティ情報共有及び公開

- 全省庁を網羅したサイバーセキュリティのアニュアルレポートを発行していただきたい。
- 政府主導で民間のインシデント事例を収集し公開していただきたい。

5. 小・中・高　セキュリティ教育の必須化

- 学習指導要領の情報教育において、「サイバーセキュリティ教育」を追加
- 大学入試共通テストの「情報」科目において、サイバーセキュリティを追加
- 「サイバーセキュリティ教育」では、現実社会において発生しているサイバーセキュリティリスクとその対策を必須化
- 「サイバーセキュリティ教育」を実施できる教育者の育成および当面不足する教育者を充当するための外部委託制度の創設

6. セキュリティ知識習得・維持にかかる個人の負担軽減

- サイバーセキュリティ知識・技術習得に対する国民の自助努力を促すため、自己負担額を対象とした所得控除制度を創設し、自発的に取組む環境整備を行うべきである。

参考資料２：2024年度JNSA政策提言（３）

7. サイバー犯罪対応能力の強化

- ボットネットのテイクダウン等、国際的なオペレーションに積極的に協力すべきである。
- シンクホールやおとりアカウントを利用した調査、民間のリサーチャーと契約した調査等、積極的に犯罪者の情報を収集し、捜査に生かしていただきたい。

8. サイバー防火管理制度

- 現在企業に課されている防火管理制度に倣った「サイバー防火管理制度（仮称）」を中小企業に対し実施することを要望する。