経済産業省

資料４－２

今後のサイバーセキュリティ政策について

平成２８年３月

商務情報政策局

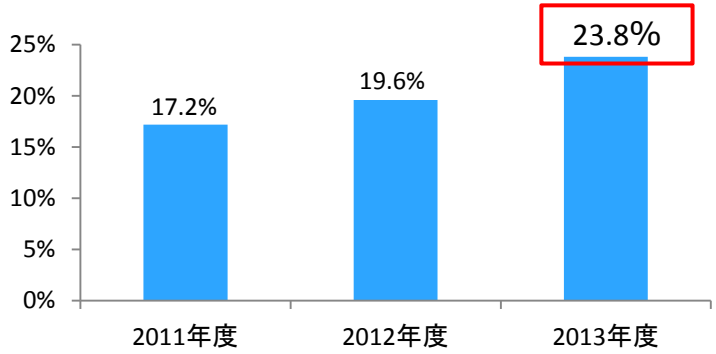
１．現状と課題

サイバー攻撃の現状

○政府関係機関や企業への標的型サイバー攻撃により、多くの重要情報漏洩事案が発生。

○情報漏えいに留まらず、**社会インフラやIoTシステムを標的として物理的なダメージを与えるサイバー攻撃のリスクが高まりつつある。**今後、2020年オリンピック・パラリンピック東京大会の開催により、リスクは更に拡大。

【標的型攻撃による情報漏洩等が確認された割合】



（出典）ＩＰＡ「情報セキュリティ事象被害状況調査」2013年度、2012年度、2011年度より経済産業省作成

【IoTシステムへのサイバー攻撃事例】

- 2015年7月、セキュリティの研究者がクライスラー社の「コネクテッドカー」システム（スマホを使ってエンジン起動やGPSで車の現在位置を把握することができるシステム）の脆弱性を突いてハッキングできることを証明。
- 具体的には、第三者がスマホを使って遠隔操作でエンジンを切ったり、ブレーキ操作が可能。
- 同社は、約140万台をリコール。

出典：Wired Magazine

【インフラ・産業基盤への攻撃の海外事例】

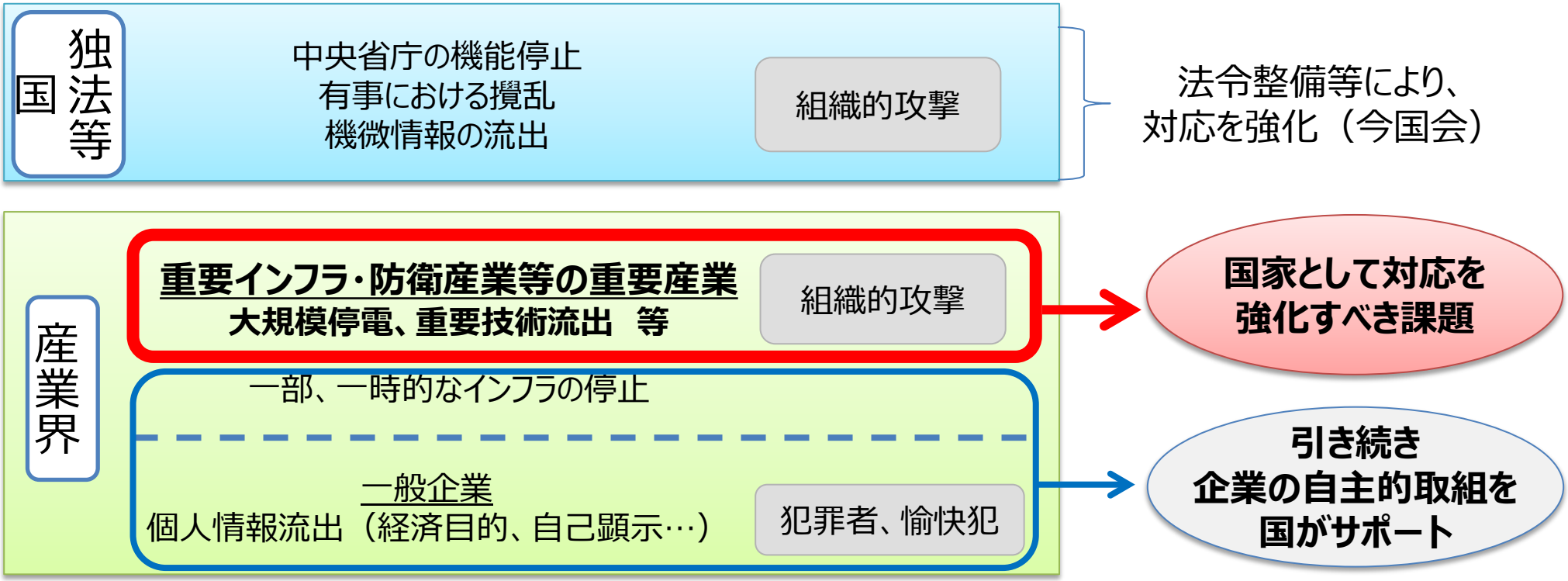
製鉄所の溶鉱炉損傷(ドイツ、2014年)
標的型攻撃により、製鉄所の制御システムを不正操作。
溶鉱炉が損傷。

ウクライナの大規模停電(2015年)
標的型攻撃により、制御系システムを不正操作。
ウクライナ西部数万世帯で、3~6時間にわたる大規模停電が発生。

サイバーセキュリティ対策の基本的考え方

○これまでのサイバーセキュリティは、個人情報や企業情報といった財産を守る観点から、企業や政府機関等の自主的なセキュリティ強化を国がサポートしてきており、引き続き実施する。

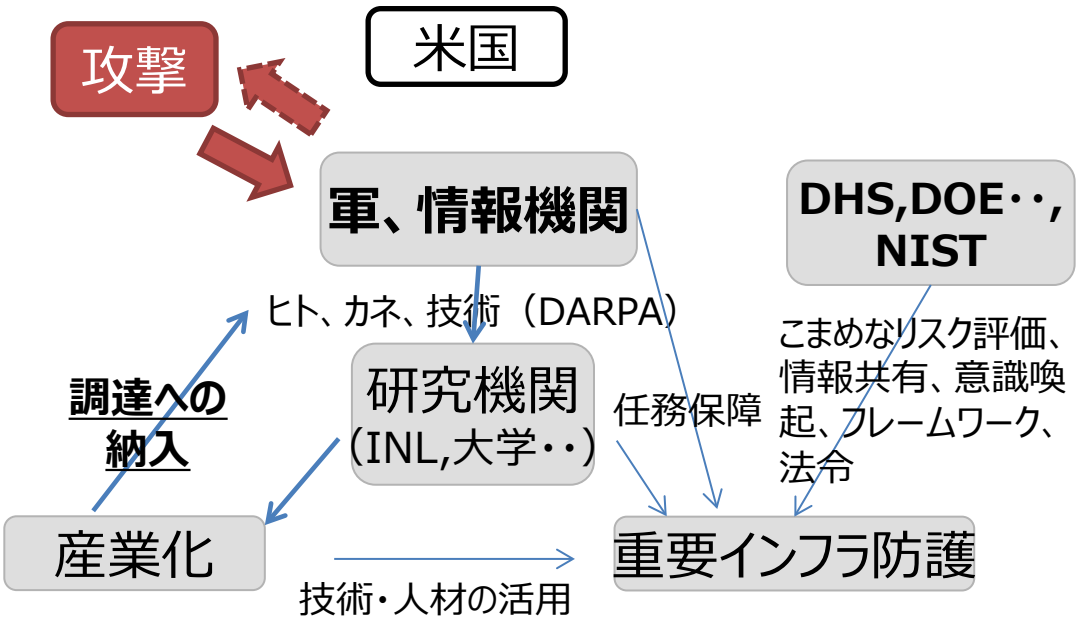
○**重要インフラ事業者や、国家安全保障にかかわる重要技術を持つ企業**へのサイバー攻撃は、ひとたび発生すれば、国民の生命や社会システム全体に甚大な被害が発生する可能性があり、**国家として対応を強化すべき課題**。



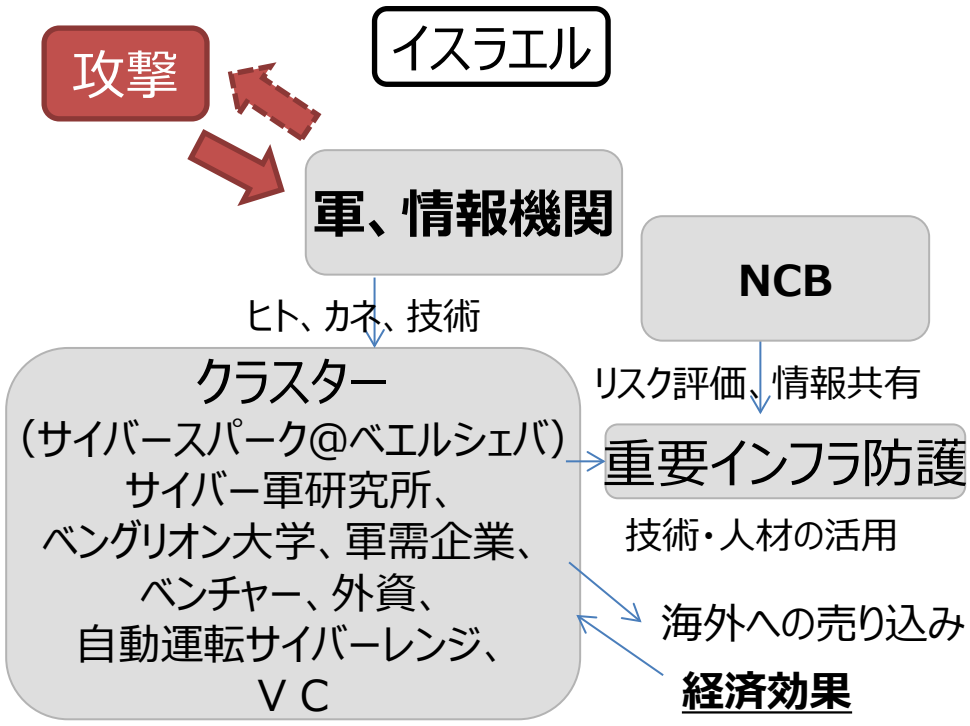
米国やイスラエルのサイバーセキュリティのエコシステム

○米国・イスラエルでは、膨大な軍事予算と、日々攻撃にさらされている**実戦経験**を通じ、**軍や情報機関のニーズに基いた極めて高度な技術と人材が養成**され、民間企業に**スピルオーバー**している。

○こうした知見は民間において**産業化**され、米国であれば**国防総省、情報機関への納入**、イスラエルであれば**グローバルマーケットへの売込み**を通じ、ヒト、カネ、技術が循環する**エコシステムが機能。**



DHS:国土安全保障省
DOE:エネルギー省
DARPA：国防高等研究計画局
NIST：アメリカ国立標準技術研究所
INL：アイダホ国立研究所



NCB：国家サイバー局

我が国のサイバーセキュリティにおける課題

○我が国の重要インフラ・防衛産業等の重要産業を守るサイバーセキュリティは、**中核的な推進機能が欠けており、エコシステムが無い**状況。実践力のある人材も圧倒的に不足しており、各企業・機関が個別に対応することに限界がある。

○我が国においては、**国がリーダーシップをとりつつ産業界と連携し、必要な対策を特定**するとともに、**サイバーセキュリティ対策のニーズを見える化**することで、**対策の循環を生み出していく**ことが必要ではないか。

わが国の産業におけるサイバーセキュリティ対策の課題

- サイバーセキュリティに対する企業経営者の認識が必ずしも十分ではない
- ユーザー企業が保有すべきセキュリティ技術や人材を生み出す中核的な場がない
- 企業にとってサイバーセキュリティ対策の費用対効果が見えにくい
- 専門的な知識や技能を備えたセキュリティ人材の不足
- サイバーセキュリティ対策に十分な資金が流れていない

これらの課題を解消し、セキュリティ対策が実装されていく循環が必要

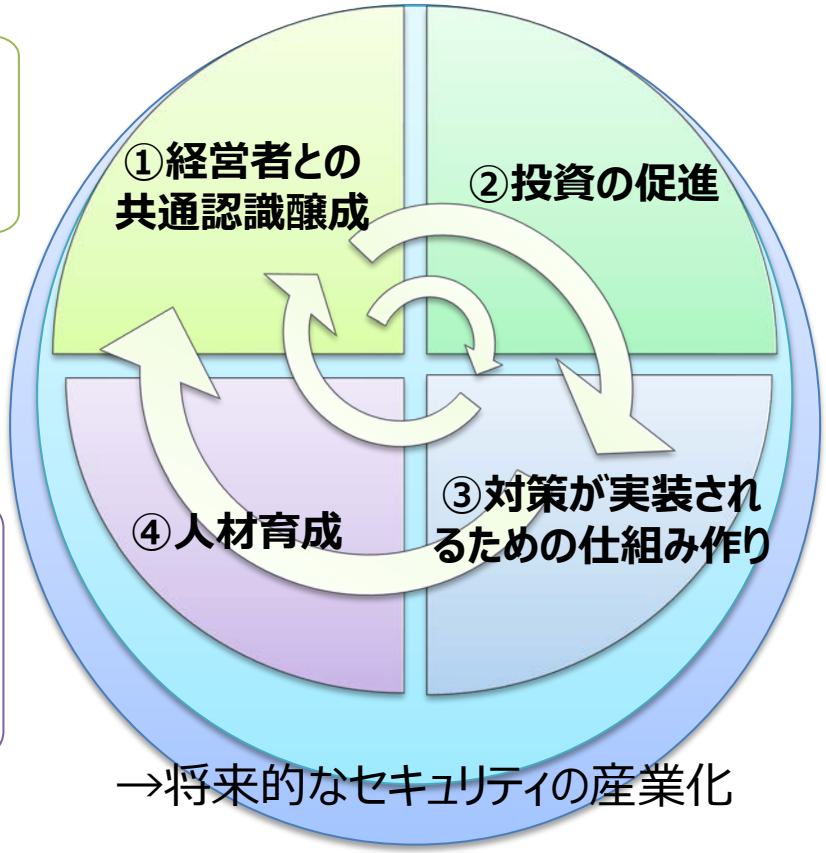
２．政策の方向性

日本型のサイバーセキュリティのエコシステムのあり方

○我が国では、国がリーダーシップをとって、**エネルギーや自動車、素材等の対策強化が喫緊の課題**となっている。**産業界と連携し、セキュリティの産業化**が図られていくような**エコシステムを形成していくこと**が必要ではないか。

○こうした取組により、一般企業や個人も含めた**我が国全体のサイバーセキュリティ強化に繋がる**のではないか。

官民で国を守っていく共通認識が醸成されるよう
リスク分析・防衛力の確認等



セキュリティ投資に繋がるような基盤の整備

対策を確実に実施するための人材が確保されるよう
資格制度による質の担保、
高度なセキュリティ人材の発掘等

対策を行う企業が市場から評価される仕組みなどを検討

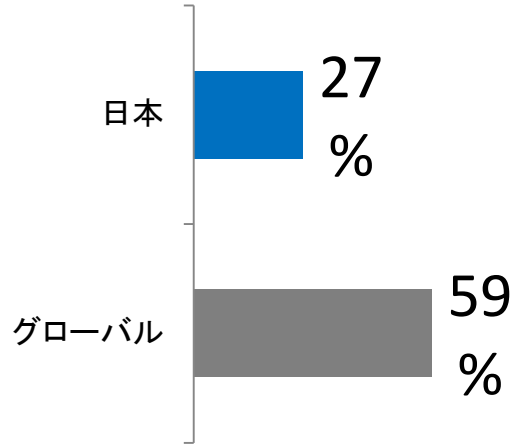
→将来的なセキュリティの産業化

①経営者と政府での共通認識の醸成

○重要産業においては、国と事業者において、**サイバー攻撃のリスクに対する共通認識を醸成する必要がある。**

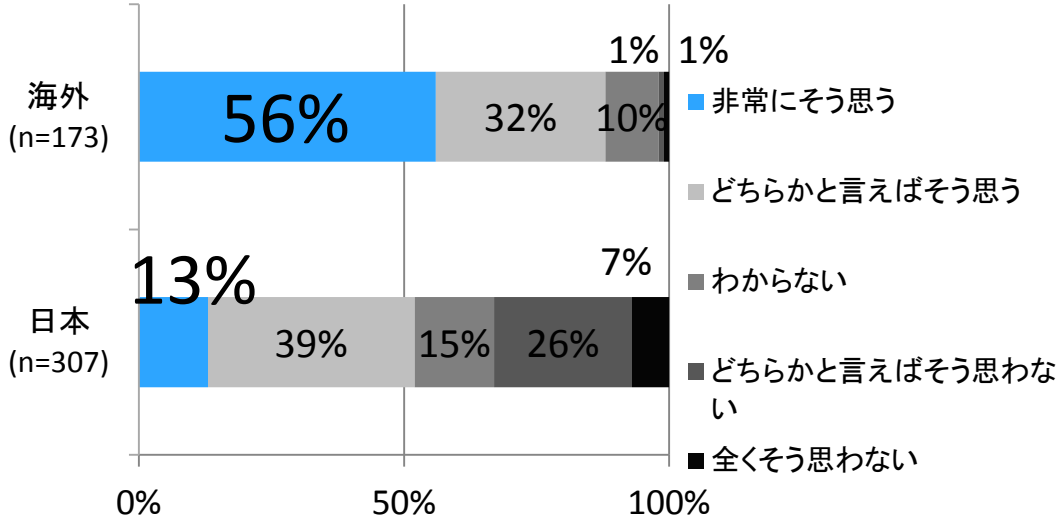
○また、一般的な企業の経営者においても、**セキュリティ対策の必要性の意識を持つことが重要。**

（参考）積極的にセキュリティ対策を推進する経営幹部がいる企業



（出典） PwC,2014 Global State of Information Security Survey

（参考）サイバー攻撃の予防は取締役レベルで議論すべきか



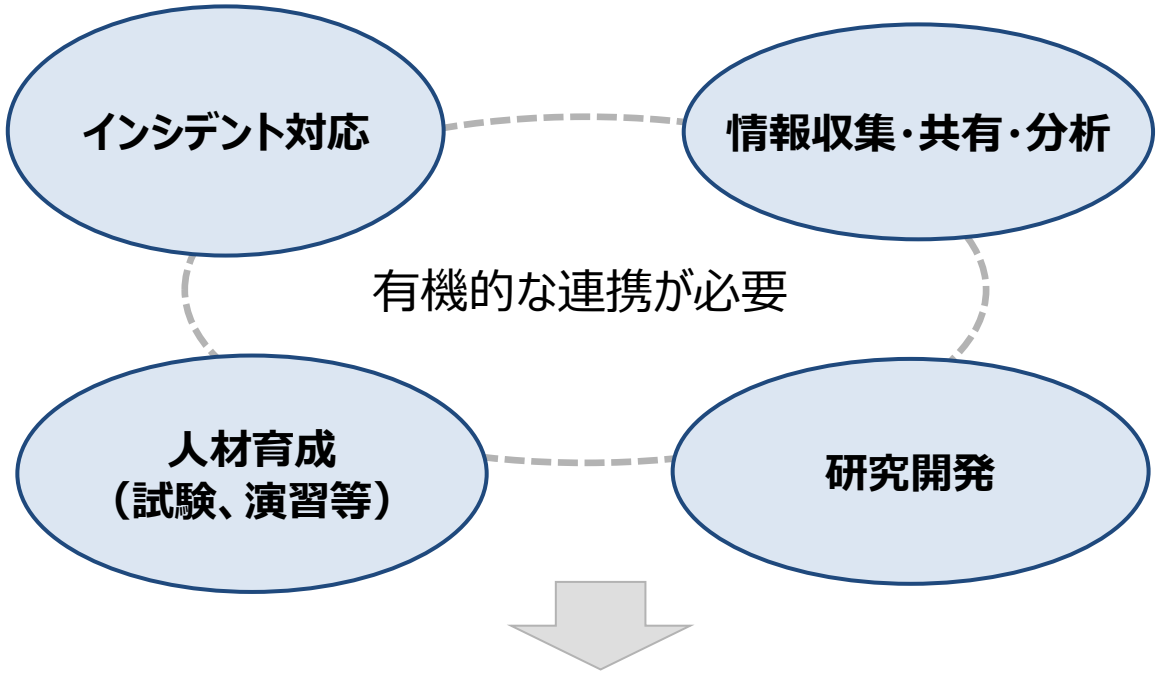
（出典） KPMG, セキュリティサーベイ2013

②セキュリティに対する投資の促進

○我が国におけるエコシステム形成のためには、国が率先してサイバー攻撃・防御の実践を促すことで、技術や人材を研鑽し、**投資につながる具体的なセキュリティ対策のニーズを生み出すことが必要。**

○セキュリティのユーザー産業のニーズを生み出すためには、**実際のインシデント対応、最新の攻撃情報とその分析、それらをふまえた研究開発、実践を通じた人材育成が連携して行われることが必要。**

◆ これまでバラバラに行われてきた機能の有機的な連携
◆ 我が国の重要産業を守るためのサイバーセキュリティの高度な技術の研究や人材育成の機会の創出



具体的なセキュリティ対策へのニーズの見える化を目指す

③対策が実装されるための仕組み作り

○企業にとって、サイバーセキュリティ対策の費用対効果は見えにくい。対策実装の推進には、どのような対策を行うべきかの**基準の明確化**や、**対策を行う企業が市場から評価されるような仕組み**が必要。

○業法によってサービスの維持や安全確保に係る水準が求められている分野については、**規制の枠組みを活用**することも考えられる。

【海外の対策実装のための仕組みの事例】

米国

- **重要インフラのサイバーセキュリティ強化のためのフレームワーク（2014年）**を、国立標準技術研究所（ＮＩＳＴ）が対策基準として策定。
- 消費者保護などのテーマ別に**官民フォーラム**により課題等を共有し、フレームワーク採用を促進。
- 国土安全保障省等が**サイバー保険の活用等のインセンティブ策**を検討。
- **米国の保険会社**ではフレームワークを利用して企業等の**リスク評価に活用**。

ドイツ

- 重要インフラ事業者が講ずべき**サイバーセキュリティ対策に関する新たなサイバーセキュリティ法**（Act for increasing the security of information technology systems (2015)を策定。
- **各業界が最低限の対策の案を提示**し、政府が基準として了承し、監督を行うもの。
- 重要インフラ事業者は、対策基準を満たしていることを監査、テスト、認証等の手段により証明する義務を負う

④人材育成

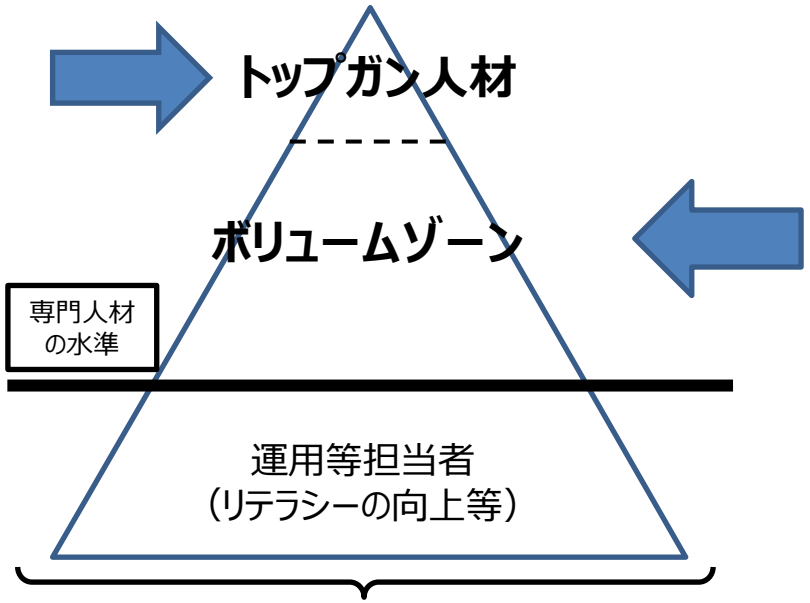
○エコシステムを担うそれぞれの人材の層の拡大のため、ユーザー・ベンダーにおける人材育成のために国が基盤を整備、将来的なキャリアパスの創出や人材市場の形成（雇用の流動化）を図ることが必要。

①**ボリュームゾーン人材**：ユーザー産業やベンダーで対策の中核を担う情報システムや施設・設備のオペレーションを担う人材の確保・育成のため、国家資格制度等を通じた**人材の見える化などが必要**。

②**トップガン人材**：**若手からの発掘・育成**を図るため、ハッカーコンテストや演習などの実戦を模擬したスキルアップが必要

③待遇の改善：セキュリティ人材の待遇を改善し、人材の流動性を確保することも重要。

②若手トップガン人材の育成
サイバー攻撃に対する防御思想等を設計できるセキュリティのトップガンを若手から育成



①ボリュームゾーンの拡大
国家資格保有者やそれに匹敵する現場の専門家

③セキュリティ人材の待遇改善

３．当面の具体的な対応策

①経営者と政府での共通認識の醸成

○サイバー攻撃によって人命への影響が生じうる分野の主要事業者において、サイバー攻撃リスクを認識するため、**リスク分析を行うための防衛力の確認**を行う。

○企業全般については、経営者のリーダーシップの下でセキュリティ対策を推進するためのツールとして、**「サイバーセキュリティ経営ガイドライン」**（平成27年12月公表）を普及する。

【重要インフラ分野】

重要インフラ事業者の
リスク分析・防衛力の確認

以下のような取組に繋がることを期待

- ◆ 事業者における改善計画の策定、対策の実施
- ◆ 業界内における他の事業者や他の重要インフラ分野への展開
- ◆ 業法におけるサイバーセキュリティ基準の策定、見直し

【企業全般】

サイバーセキュリティ経営ガイドライン

普及のための取組

- ◆ 経営者への直接的な働きかけ
- ◆ 中小企業も活用できる解説の策定・普及

（参考）サイバーセキュリティ経営ガイドラインの概要

○サイバー攻撃対策は、ＩＴを利活用する限り避けて通れない経営課題。

○昨年１２月、経営者のリーダーシップによってサイバーセキュリティ対策を推進するために、経営者が認識すべき３原則と、経営者がセキュリティの担当幹部（ＣＩＳＯ等）に指示をすべき重要１０項目をまとめた「サイバーセキュリティ経営ガイドライン」を公表。

１．サイバーセキュリティ経営の３原則

（１）経営者は、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要
（２）自社のみならず、ビジネスパートナーを含めた対策が必要
（３）平時及び緊急時のいずれにおいても、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

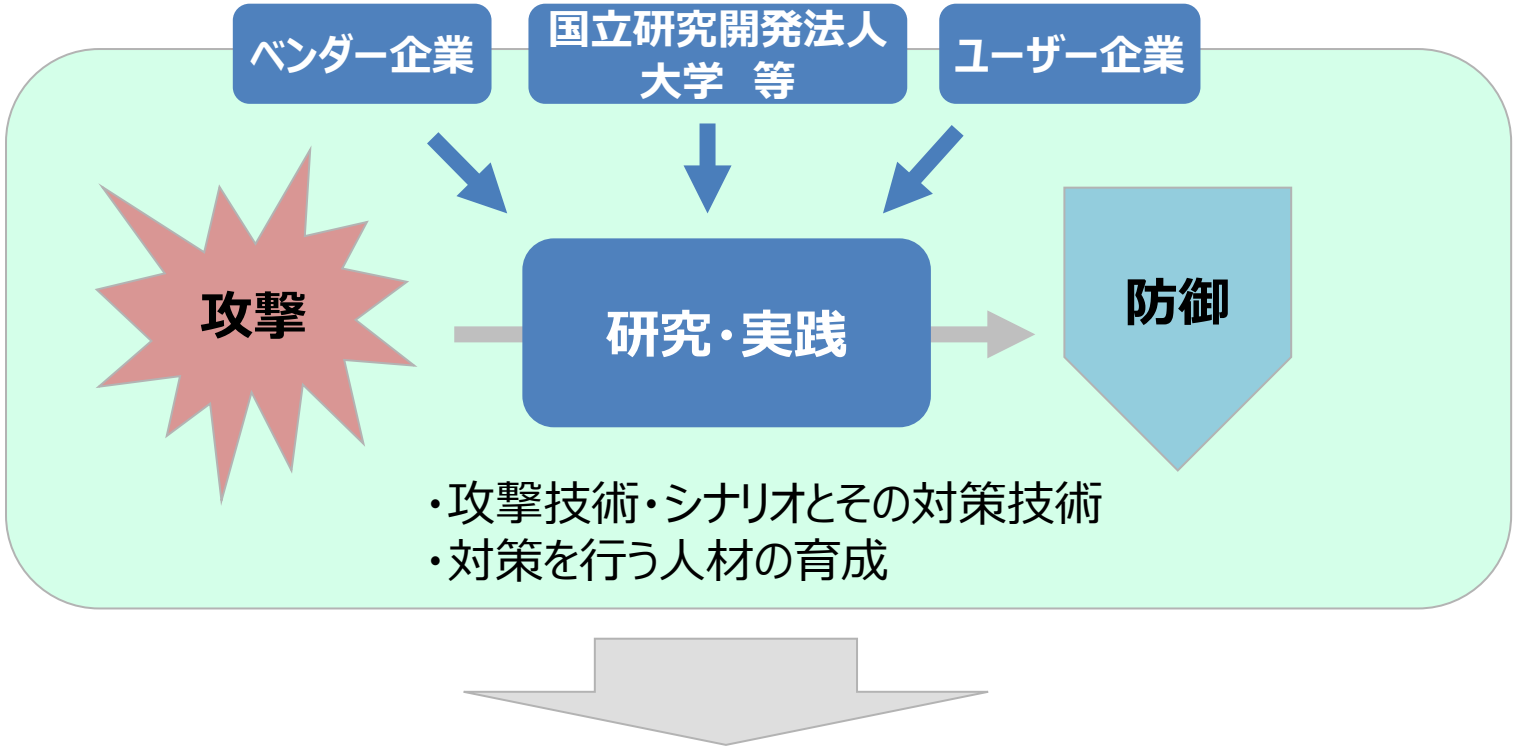
２．サイバーセキュリティ経営の重要１０項目の概要

（１）組織の内外に対策の方針を宣言すること
（２）方針を実装するための体制を構築すること
（３）リスクを洗い出し、計画を策定すること
（４）ＰＤＣＡを実施し、状況報告をすること
（５）ビジネスパートナーを含めＰＤＣＡを実施すること
（６）予算・人材などリソースを確保すること
（７）ＩＴシステムの委託先対策も確認すること
（８）最新状況を対策に反映し、被害拡大を防ぐため、情報収集・共有活動に参加すること
（９）迅速な初動対応を行うため、ＣＳＩＲＴ整備や訓練を実施すること
（10）情報開示や経営者がスムーズな説明が出来るよう事前に準備すること

②セキュリティに対する投資の促進

○我が国の**電力・ガスなどの重要インフラ、自動車・素材等の重要産業**をサイバー攻撃から守るため、**国、守る対象となるセキュリティのユーザー企業、守る製品・サービスを供給するベンダー企業が連携。**実際の施設・システムの防護に必要な最先端のサイバーセキュリティ技術の研究や、実践を通じた人材育成の機会を創り、**セキュリティ対策ニーズを見える化することで、投資を促していく**ことが必要。

【研究・実践のイメージ】



ユーザー企業等による、対策や人材への投資

③対策が実装されるための仕組み作り

○重要インフラについては、業法の枠組みを活用した対策を検討中。電力分野では、**スマートメーターや制御系システムにおけるサイバーセキュリティ対策**をガイドラインとして示し、**電気事業法の保安規制に位置付け**るべく調整中。

○企業全般の対策を後押しするため、攻めのＩＴ経営銘柄の選定基準の一部へのサイバーセキュリティ経営ガイドラインの取り入れ、サイバー保険料率のセキュリティ対策との連動等、**対策をとった企業が評価される仕組みを普及**する。

○さらに、今後多くの企業で進展が見込まれるIoTのセキュリティについては、専門WGにおいて、IoTシステムの設計者等に具体的な対策の検討を促すためのガイドラインを策定中（本年５月目途）。

【電力・クレジット分野における先行的な取組事例】

・スマートメーターシステムのセキュリティ

スマートメーターシステムの設計調達段階から保守運用段階までの一連の工程における、セキュリティ対策の要求事項を定めた民間ガイドラインを策定。今後、当該ガイドラインを電気事業法の保安規制に組み込んでいく予定。

・電力制御システムのセキュリティ

電力の安定供給や電気工作物の保安の確保に支障をきたす可能性のある電力制御システム等のセキュリティ対策の要求事項を定めた民間ガイドラインを策定中　（平成28年夏を目途に策定予定）。今後、当該ガイドラインを電気事業法の保安規制に組み込んでいく予定。

・クレジット決済システムのセキュリティ

2020年までの決済端末のIC対応化100%等、クレジット取引セキュリティ協議会（官民の約４０事業者で構成）が策定した実行計画の円滑な実施を促進するとともに、その実効性を確保するため、割賦販売法を見直し、加盟店等における必要なセキュリティ対策を求める予定。

④人材育成

○我が国産業全体のセキュリティ人材育成・確保のために、産業界と連携しつつ、以下の措置を講じる。

①ユーザー産業やベンダーで対策の中核を担う人材を育成するため、**資格制度（今通常国会の法改正により情報処理安全確保支援士制度を新設）により、人材の見える化と質の担保を図る。**また、ユーザー企業におけるセキュリティマネジメント人材育成のため、**「情報セキュリティマネジメント試験」**を実施。

②「セキュリティキャンプ」や「未踏ＩＴ人材発掘・育成事業」を継続して実施するほか、**教育機関との連携**（セキュリティ専門の大学院等）や**ハッカーコンテスト**等を通じ、若手トップガンを発掘・養成。

③セキュリティ人材の待遇改善に向けた方策について検討。