経済産業省

資料9

サイバーセキュリティ対策の推進について

２０１６年３月３１日

経済産業省商務情報政策局

日本再興戦略2015

第二　３つのアクションプラン

４．世界最高水準のＩＴ社会の実現
（３）新たに講ずべき具体的施策
ⅰ）国民・社会を守るサイバーセキュリティ

③民間企業における対策の推進

④サイバーセキュリティの確保に向けた基盤強化

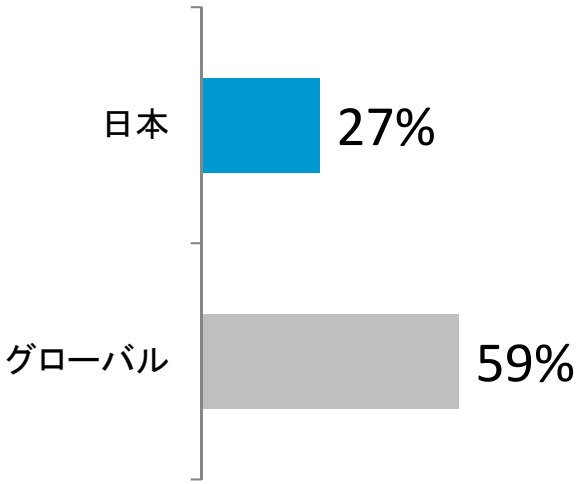
ア）技術力の強化・産業育成

イ）人材育成

民間企業における対策の促進

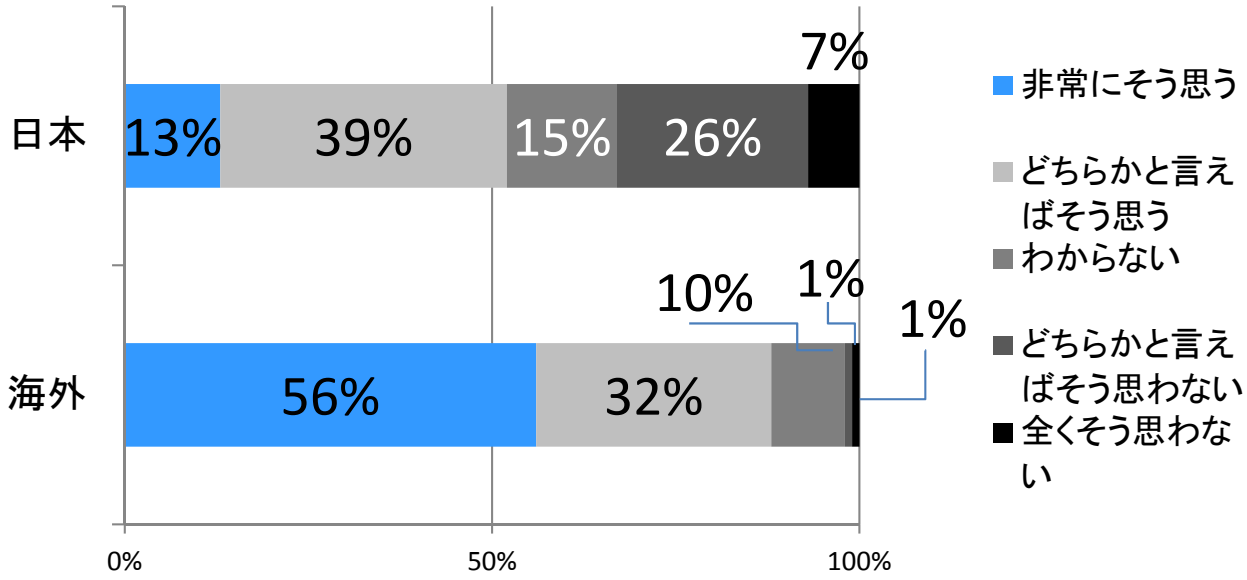
- 我が国では、サイバーセキュリティ対策において、必ずしも経営者が十分なリーダーシップを発揮していない可能性がある。
- 昨年１２月、経営者のリーダーシップによってサイバーセキュリティ対策を推進するため、経営者が認識すべき原則と、経営者がセキュリティの担当幹部（ＣＩＳＯ等）に指示をすべき重要事項をまとめた「**サイバーセキュリティ経営ガイドライン**」を策定。

（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） プライスウォーターハウスクーパース（株）「グローバル情報セキュリティ調査2014」より経済産業省作成

（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ジャパン「KPMG Insight 日本におけるサイバー攻撃の状況と課題ーセキュリティサーベイ2013からー」より経済産業省作成

（参考）サイバーセキュリティ経営ガイドライン概要

１．経営者が認識すべき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．経営者がＣＩＳＯ等に指示をすべき１０の重要事項

リーダーシップの表明・体制構築
- （１）組織全体での対策方針を策定すること
- （２）方針を実装するための体制を構築すること

ＰＤＣＡ策定
- （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

攻撃を防ぐ事前対策
- （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

攻撃を受けた場合に備えた準備
- （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

サイバーセキュリティ経営ガイドライン
http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

技術力の強化・産業育成

- 戦略的イノベーション創造プログラム（SIP）の枠組みで、「重要インフラ等におけるサイバーセキュリティの確保」事業を実施。
- 産業革新機構（INCJ）が最先端のセキュリティ技術の開発を行う企業に成長資金を出資。

重要インフラ等における
サイバーセキュリティの確保（SIP事業）

コア技術

- ◆ 制御システムの動作監視・解析技術
- ◆ 制御システムの防御技術　　等

社会実装技術

- ◆ 情報共有プラットフォーム技術
- ◆ セキュリティ人材育成　　等

東京オリンピックを支える主要な重要インフラ向けプラットフォーム

F.TRONの事業
（INCJから9億円を上限とする出資）

現状

現在の防御は既知の攻撃のパターンをマッチングして対応することが中心であり、未知の攻撃に対して完全な保護を提供できる技術はない。

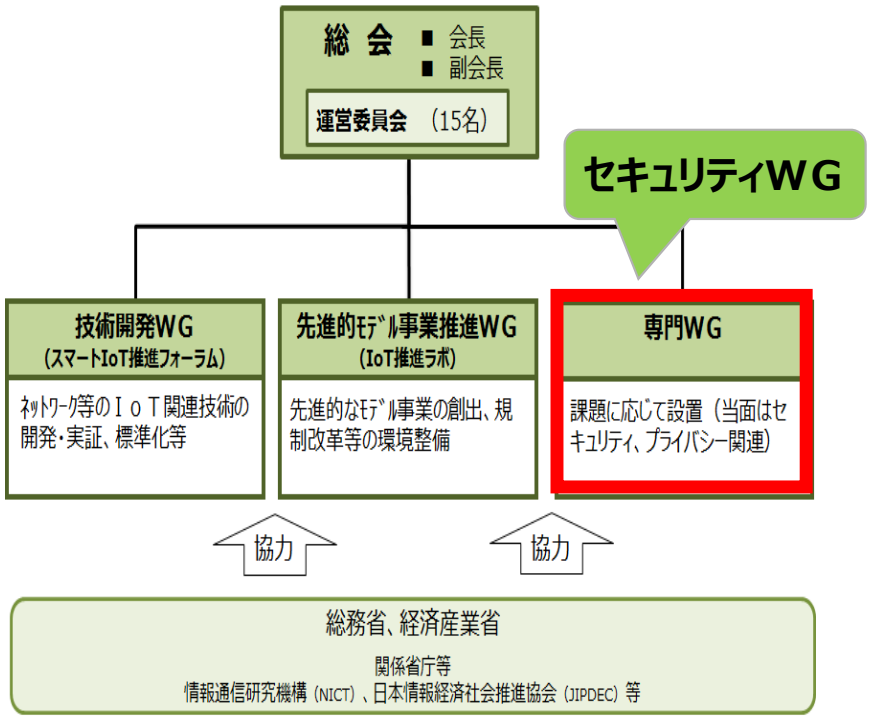
F.TRONが開発した技術

PC端末の全機能を掌握し、第三者による処理の実行を100%許さない新しいサイバーセキュリティ対策製品等を開発。

技術力の強化・産業育成

- 「IoT推進コンソーシアム」の下に、**IoTのセキュリティに関するWGを設置**。リスクの共通認識を図った上で、各分野において必要な対策を検討し役割分担を検討することを促すための**ガイドラインを策定中**（本年5月目途）。

＜ IoTセキュリティＷＧ組織構成＞



＜ IoTセキュリティの検討の方向性＞

理念	IoTシステムの普及により、サイバー空間と実空間の融合が進むとともに、IoTシステムによる新たな価値の創造が期待される。IoTのセキュリティリスクを許容しうる程度まで低減し、セキュリティ品質を企業価値として競争力につなげていくことが必要。
目的	様々なIoT機器やシステムがつながる世界において、IoT機器等がつながることのリスクを認識し、関係者（供給者・利用者）に対策の必要性や役割の認識を促す。
内容	IoT機器等の設計・構築・運用・ネットワークへの接続等にあたって、IoT関係者が注意すべきポイントをまとめたもの （※サプライチェーン上のリスクも考慮）

ガイドラインで記載

今後、守るべき対象やリスクの大きさを踏まえて分野別の検討を期待

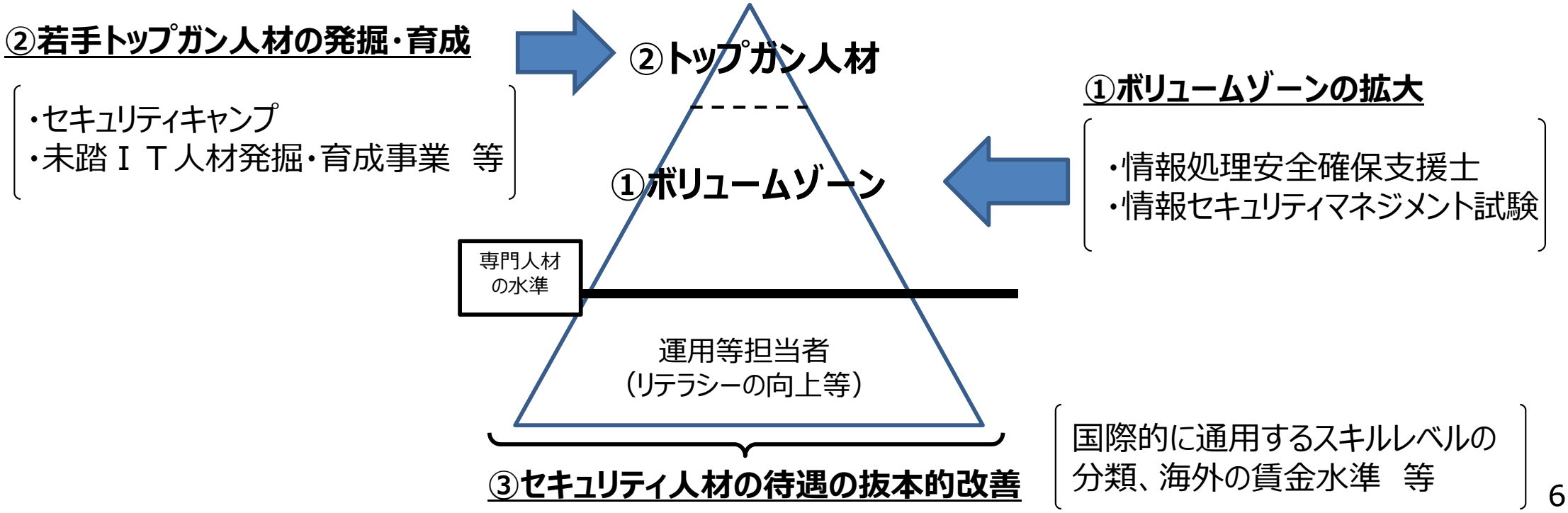
人材育成

●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。

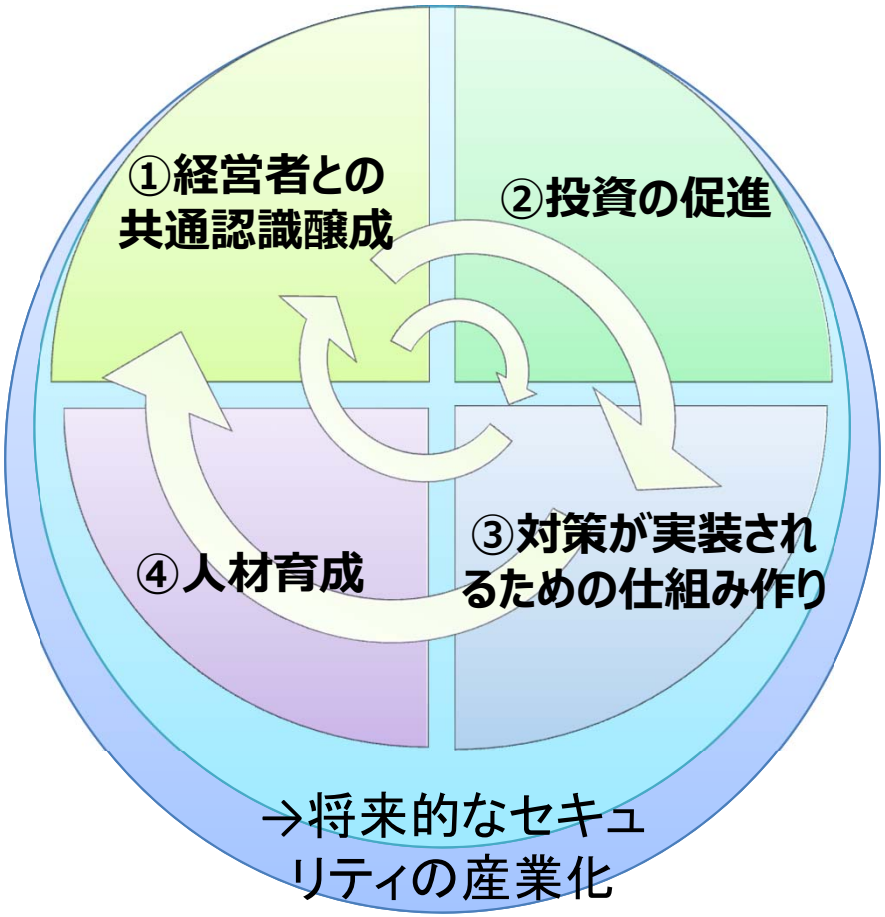
③セキュリティ人材の待遇改善に向けた方策について検討。



今後の進め方

- 国とともに**エネルギーや自動車、素材等の基幹ユーザー産業が中心となって、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**が必要。
- 具体的には、①経営者との共通認識醸成、②セキュリティ投資の促進、③対策が実装されるための仕組み作り、④人材育成という循環を通じて、**エコシステムを形成**していくことが重要。

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