Keidanren
Policy & Action

Society 5.0 実現に向けた

サイバーセキュリティの強化を求める

2018年 8月21日

一般社団法人　日本経済団体連合会

Society 5.0の実現に向けた
サイバーセキュリティの強化を求める

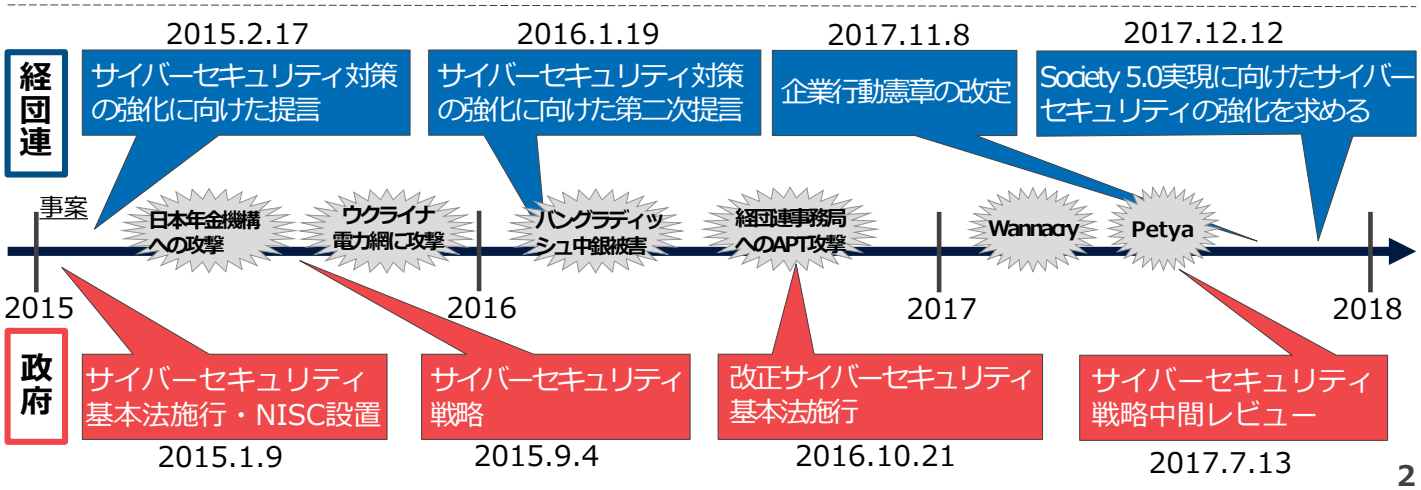
経緯とねらい

Keidanren Policy & Action

経団連は過去２度、サイバーセキュリティ対策の強化を提言
企業行動憲章を改定し社会的責任として取り組むことも明言

サイバー攻撃の被害は世界中で拡大し、新たな段階に突入

あらゆる企業や組織における具体的な取り組みと
関係者の連携をさらに推し進めるため、改めて提言



Society 5.0 時代のサイバーセキュリティの重要性

Keidanren Policy & Action

あらゆるモノ・ヒト・コトがデータでつながる社会「Society 5.0」が到来
技術とデータで課題を解決する社会に向け、サイバーセキュリティ確保は重要

サイバーセキュリティを考える際の基本的な視点

Keidanren Policy & Action

Society 5.0によって価値を創出する前提という視点と危機管理の視点の両面から、サイバーセキュリティ確保に積極的に取り組むことが重要

価値創造

Society 5.0時代にサイバー空間で価値を創造する際の前提としてセキュリティ確保は必要

- ◆ サイバーセキュリティが確保された安心・安全な商品・サービスを提供することで、競争力を維持・強化。
- ◆ グローバル市場でのビジネス環境確保や、セキュリティ自給率の向上も必要な観点。

危機管理

サイバー攻撃対策を怠れば事業継続が困難となり、関係者・市民に大きな影響を与えかねない

- ◆ 企業の社会的責任として主体的に対策を講じる必要。
- ◆ 一方、完璧な防御は不可能であり、サイバー攻撃を自然災害と同様に避けられないリスクと捉えるべき。
- ◆ 事業継続の観点から、攻撃の早期の検知や被害拡大の阻止、対応復旧を重視。

サイバーセキュリティ対策の全体像

Keidanren Policy & Action

取り組む姿勢

自助	共助	公助	国際連携
まずは企業自らが主体的に	一組織では限界がある業界を越えて連携を	政府からの情報提供・支援も必要	国境を越えた連携を

意識改革とリソースの確保

意識改革

- ✓ 国民全体の意識向上
- ✓ 経営者の意識改革

＋

- ✓ リテラシー向上
- ✓ 専門人材育成
- ✓ 情報の類型整理
- ✓ 共有の場を拡大
- ✓ 官民で資金投入
- ✓ 税制上の支援
- ✓ 研究開発
- ✓ 社会実装

基盤となる体制整備

政府体制	企業体制	法制度・規範
✓ 政府施策の一体化	✓ 企業内体制整備 ✓ サプライチェーン管理	✓ 法制度・技術標準整備 ✓ 国際規範の策定

意識改革

サイバーセキュリティに対する意識を国全体で向上させることが必要
とりわけ各組織においては経営者の意識改革が鍵を握る

セキュリティ・バイ・デザイン

✓ 商品・サービスの**企画・設計段階から**セキュリティを意識

経営者の意識改革

✓ 経営者がサイバーセキュリティを**経営の最重要課題と認識**

✓ 取締役会等で定期的に報告・討議、経営者の責任で判断

✓ **人員・予算等のリソースを適切に確保**

完全な防御は不可能という認識の拡大

ベースラインの対策を行っていても、サイバー攻撃を完全に防御することは不可能。

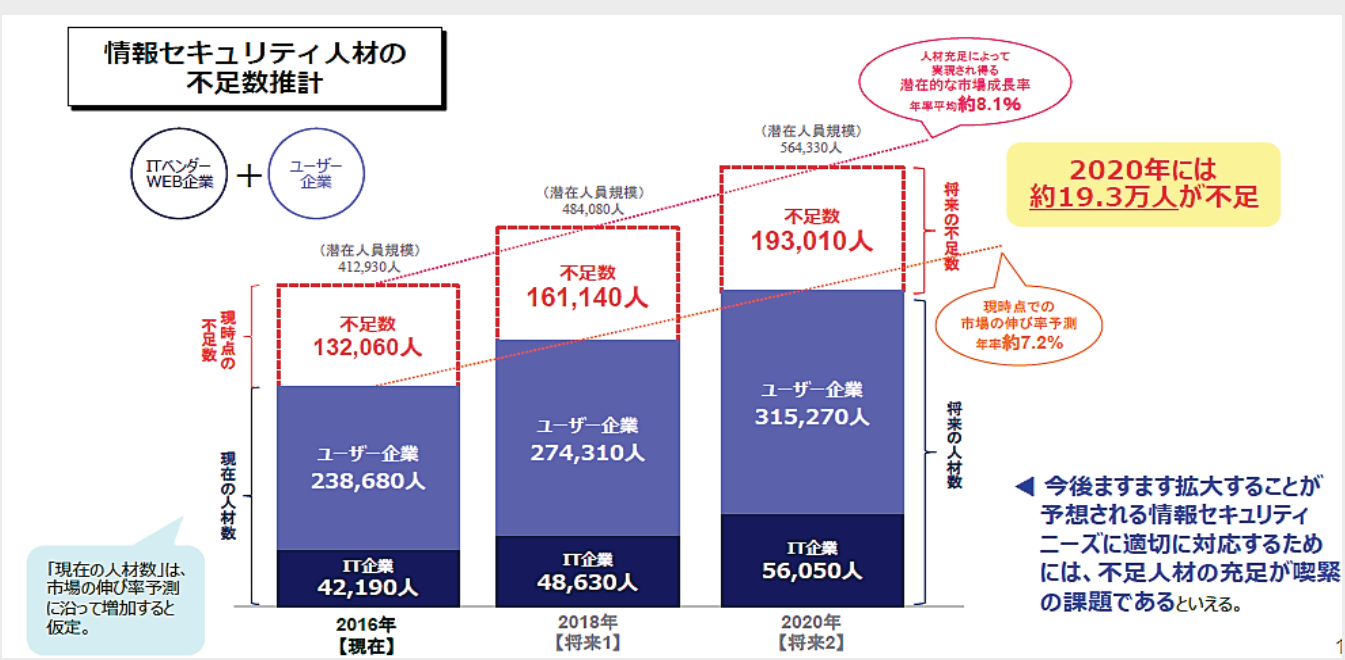
✓ 攻撃を受けた後の**被害最小化に向けた取り組み**を重視

✓ 対策に努めていたのに被害を受けた企業をいたずらに責めず、
むしろ積極的な情報公開を促す**社会風土の醸成**

人材育成（１）

サイバーセキュリティ事故の多くは人的要因に起因しており、
社会全体のリテラシーを向上させることが重要
対策を担う人材も質・量ともに大幅に不足しており、人材育成・維持のエコシステムを構築することが必要

【図　情報セキュリティ人材の人材数・不足数に関する推計（2016年）】



出典：経済産業省「IT人材の最新動向と将来推計に関する調査結果　報告書概要版」（2016.6.10）

人材育成（2）

Keidanren Policy & Action

社会全体のリテラシー向上

学校

- ✓ **小中学校からリテラシー教育**
- ✓ 教えられる教員の増強

各組織

- ✓ 職員・従業員への**継続的な教育・研修**

経営者

- ✓ **経営者自身**がITやサイバーセキュリティへの理解を深める

若年層の優秀な人材の発掘

競う場の提供 ＋ **倫理観の教育**

- ✓ セキュリティコンテスト・CTFなどの腕を試す場の提供が必要。
- ✓ 若い優秀な人材が悪事に手を染めないよう倫理観の教育が必要。

人材育成（3）

Keidanren Policy & Action

専門・高度人材の育成・維持のためのエコシステム構築

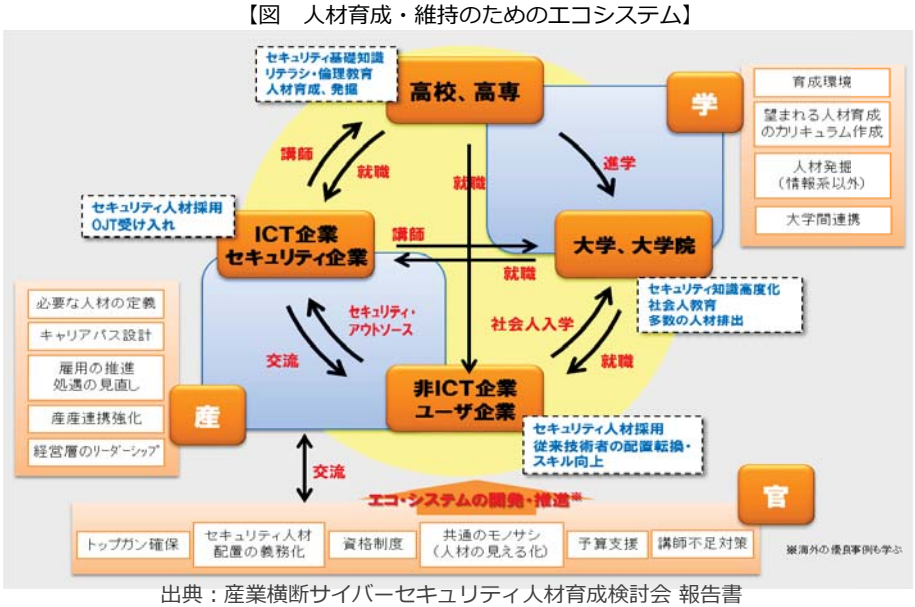
教育・研修

- ✓ 産業界が求める人材像を育成施策・教育課程に反映
- ✓ 社会人の研修や学び直し、リカレント教育
- ✓ 資格の普及やグローバル連携

キャリアパス

- ✓ **待遇改善・国内外の高度人材の積極採用**
- ✓ 官民の**既存の人事制度の突破**
  （年齢や経歴に関わらず特別な待遇で活躍できる制度）

【図　人材育成・維持のためのエコシステム】



出典：産業横断サイバーセキュリティ人材育成検討会 報告書

情報共有（1）

Keidanren Policy & Action

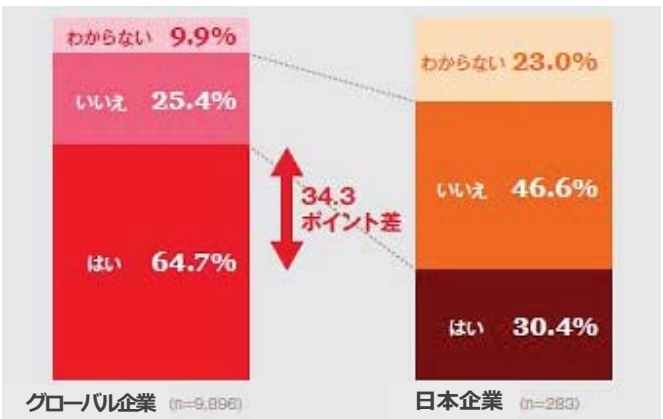
攻撃に備えるため、情報収集・共有・活用を率先して行うことが重要
企業・業界・官民・国境を越えて迅速な情報を共有する仕組みが必要

情報の５W1Hの整理

課題
- 情報共有の重要性は理解されつつあるが、具体的な枠組みの構築が進んでいない。
- 情報といっても「ノウハウ・ベストプラクティス」から「脆弱性・技術情報」、「分析情報」、「脅威情報」などさまざまあり、受け取る階層によっても必要な情報や対応の仕方は異なる。

✓ 共有・活用する情報の**５W１H（目的、類型、共有の場、階層、タイミング、手法等）の整理・標準化**を官民・各組織で行う必要。

【図　サイバーリスクに関する情報共有を行っているか？】



【図　他組織と情報共有を行わない理由】

出典：PwC「グローバル情報セキュリティ調査2016：サイバーセキュリティの転換と変革」

情報共有（2）

Keidanren Policy & Action

情報共有の枠組み拡大

一部の業界ではISAC（Information Sharing and Analysis Center、情報共有・分析機関）が設立されるなど情報共有の場の構築も進みつつあるが、より一層の拡大が必要。

✓ **ISACの分野拡大**、既存のISACの機能改善
✓ 業界を横断するISAO(Information Sharing and Analysis Organization）の設立
✓ 情報共有を行うメーリングリストやポータル等の媒体整備

公助の仕組み

民間企業のみでの情報収集・共有には限界があるため、政府による「公助」が必要。

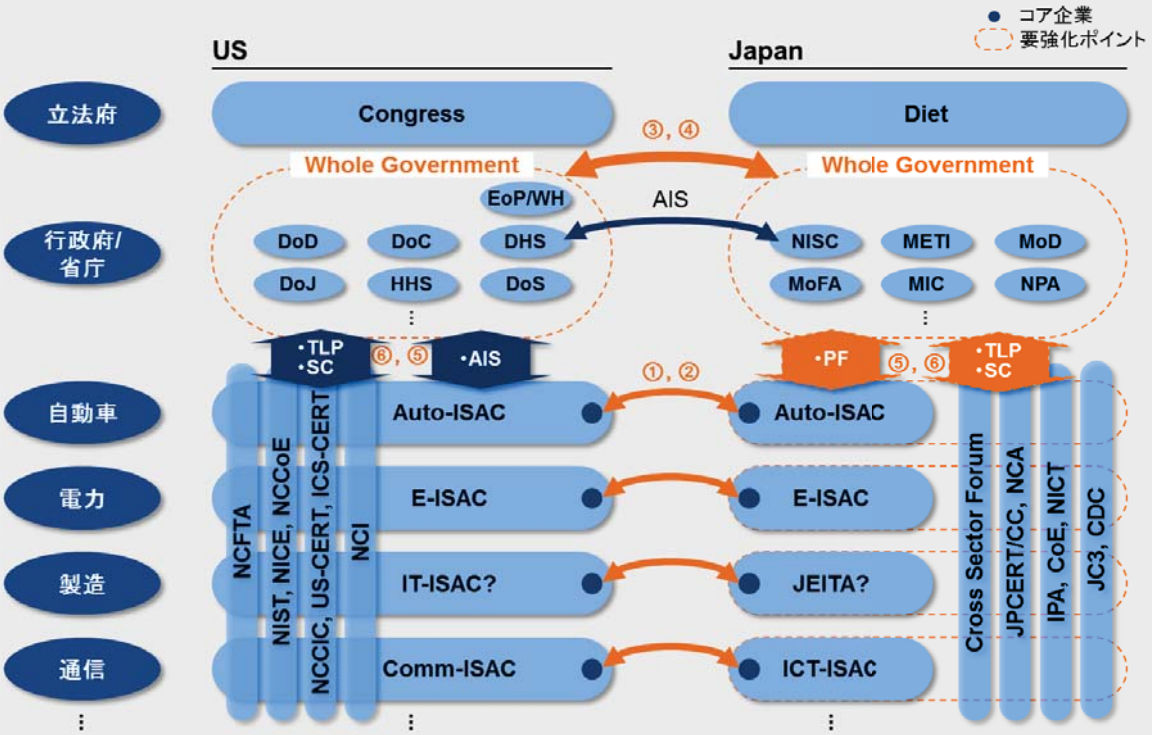
✓ 情報類型の主導、情報共有組織への支援
✓ 一定の条件を課した上で**横断的な脅威情報を民間に提供する仕組み**
✓ 既存TLP（Traffic Light Protocol） の統一化・活用推進
✓ 情報を取り扱える者の認定制度(セキュリティクリアランス)等の範囲・条件を検討
✓ 情報提供者が共有範囲を限定できる仕組み

情報共有（3）

国際連携

- ✓ 米国など**関係諸国との間でリアルタイムに官民で情報共有**できる仕組み
- ✓ **政府間・企業間の情報共有やISAC同士の国際連携**を目指すべき

【図　日米間の情報共有の将来イメージ】



技術対策

人材やリテラシー不足を補うためにも、技術的な対策強化が不可欠
官民を挙げて技術の研究開発を進めると共に、社会実装を急ぐべき

各組織での対策

- ✓ **OSやソフトウェアのアップデート**
- ✓ ウイルス対策ソフト導入
- ✓ パスワードや暗号化技術の活用
- ✓ アクセス権限管理
- ✓ 物理的セキュリティも含めた多重防御

中小企業対策

中小企業は、自社単独でのリソース確保が難しいため、技術・人材の共助的な活用が必要

- ✓ **中小企業でのクラウド化**の促進
- ✓ 利便性が高いクラウドサービス普及

技術開発等

- ✓ セキュリティ技術（予兆検知、匿名化、暗号技術等）の**研究開発の拡大**
- ✓ OT（制御技術）とIT（情報技術）や多様な機器が連携することへの対策
- ✓ AI（人工知能）やブロックチェーンなど最新技術の活用
- ✓ 攻撃側の研究推進

商品・サービスの提供

- ✓ 各種ガイドラインを踏まえて対策
- ✓ 脆弱性情報の発見者へ報奨金を支払うプログラム等の有効活用

国際標準化

- ✓ 技術標準の仕様を主体的に提案
- ✓ 認証制度を欧米諸国と相互認証

投資促進（１）

Keidanren Policy & Action

Society 5.0実現に向けて、人材、情報、技術に重点的に資金を投入、その資金が効率的に循環する仕掛けや制度を作ることが不可欠

企業での投資

- ✓ **人材・技術・体制整備等に十分に資金**を投入
- ✓ リスクを保険等でカバー
- ✓ 子会社や取引先等の対策支援
- ✓ ISACやシンクタンク等の組織設立

中小企業での対策

- ✓ 中小企業が小額の掛け金によって情報共有が行える**共済を創設**
- ✓ サイバーセキュリティ対策、監査、情報共有、事故処理、保険対応等を**総合的に支援できる全国的組織**の設置

投資促進（２）

Keidanren Policy & Action

政府による公助

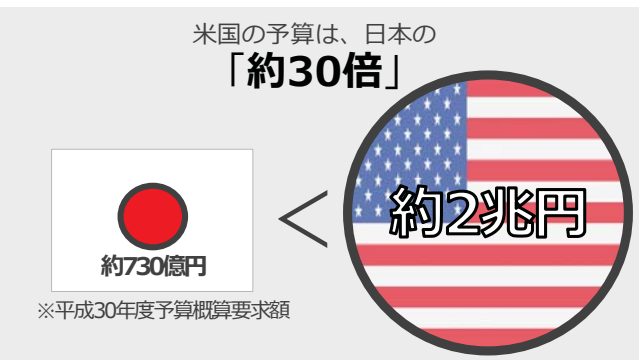
組織や団体の設立・維持には少なからぬ負担がかかる。中小企業も自社のリソースのみので対策は困難。
→政府の支援による企業の取り組み促進が必要。

- ✓ システムやサービスの購入等に関する**税制措置の創設**、**中小企業投資促進税制の拡充**、補助金支援
- ✓ 親会社負担の国内子会社の対策費への税制上の支援
- ✓ 組織（ISACやシンクタンク等）の設立・運営費用への助成

政府予算

- ✓ サイバーセキュリティを公共インフラ整備に準じた位置づけ
- ✓ **政府予算の大幅な拡充**により、人材や技術等に重点的に投資

【図　サイバーセキュリティ関連予算日米比較】



政府関連組織の整備・連携

Keidanren Policy & Action

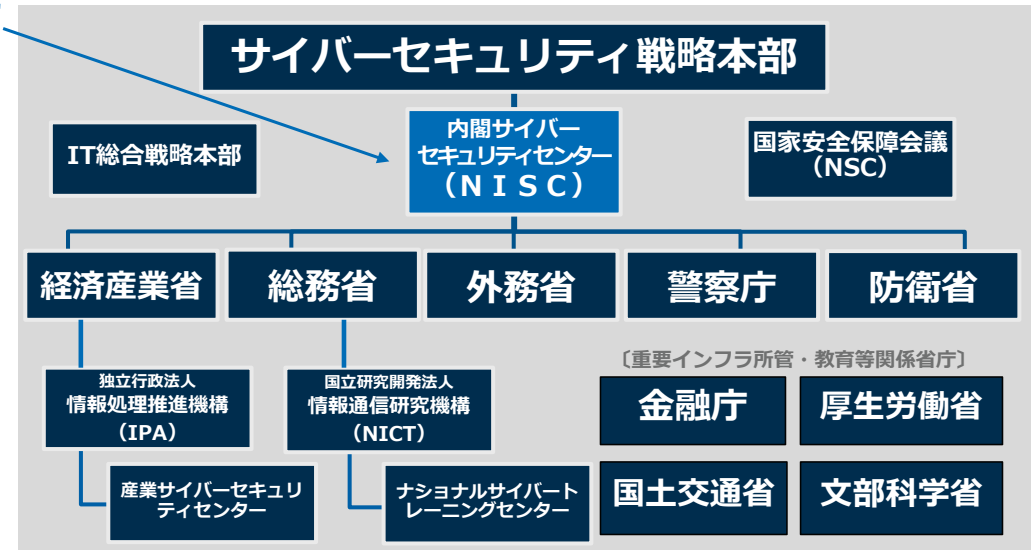
政府戦略はサイバーセキュリティ戦略本部が策定し、各府省が予算確保・施策実行
縦割りで重複・分散する施策も見られ、各府省の役割分担は不明確

✓ 関連府省・組織の役割明確化、**施策の一体化と優先順位の共有**が必要

司令塔組織としてNISCの機能強化

- ✓ 各府省施策の新設・統廃合の提案・決定権限
- ✓ **人員・予算の拡大**
- ✓ 人材育成、情報収集・分析・共有、国際標準・連携等に関する**監督・管理・監修**
- ✓ 普及啓発活動の拡大
- ✓ 攻撃の報告先や相談窓口の一本化
- ✓ 物理的セキュリティとの連携

【図　サイバーセキュリティに関連する政府関連組織】



今後の課題

✓ 将来的には、各省に散在する**関連政策を一元的に所管する機関の創設**
✓ **政治のリーダーシップ**による一体的対策強化

企業内の体制

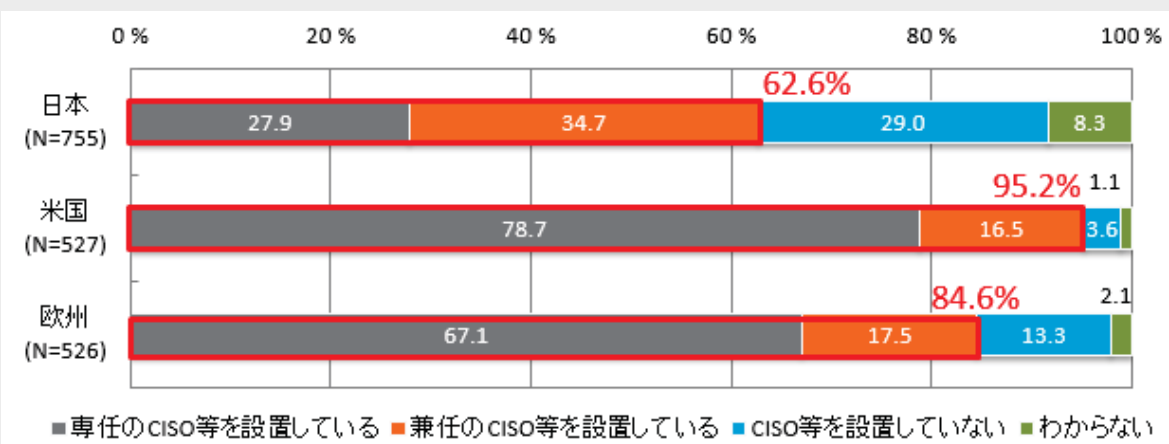
Keidanren Policy & Action

CISOや対応組織を設置するなど企業内の体制を整備するとともに、
BCP（事業継続計画）等も重要

企業内体制の整備

- ✓ セキュリティ対策に責任を持つ**CISO等の設置**およびスタッフの充実
- ✓ **対応組織**（CSIRTやPSIRT、SOC等）**の設置および経営層との橋渡し**
- ✓ 従業員への研修や演習を通じた持続的な啓発・教育
- ✓ 早期回復に向けた**BCP(事業継続計画）等の策定**および定期的な訓練

【図　企業のCISO任命率】



出典：IPA「企業のCISOやCSIRTに関する実態調査2017」(2017年4月13日)

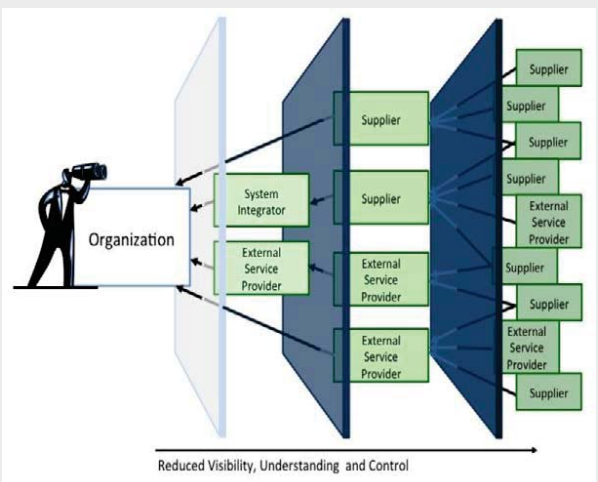
サプライチェーン管理

あらゆる業種・規模の企業がITでつながるなか、委託先や取引先も含めたサプライチェーン全体のサイバーセキュリティの管理徹底が必要

サプライチェーンのサイバーセキュリティ確保

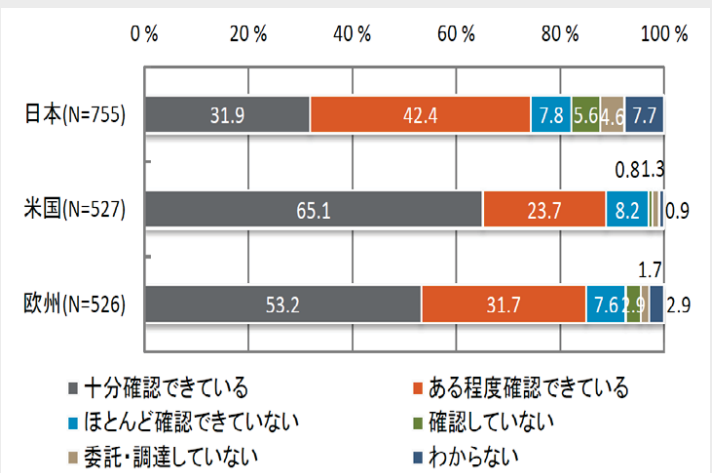
- ✓ デジタルサプライチェーンISAO設立
- ✓ 各段階におけるプロセス管理の適用
- ✓ 委託先・取引先のチェックの際にSOCレポートや各種報告書の活用

【図　ITサプライチェーンの構造】



出典:NIST SP 800-161, “Supply Chain Risk Management Practices for Federal Information Systems and Organizations”

【図　委託先のセキュリティ対策状況把握（業務委託先）】



出典：IPA「企業のCISOやCSIRTに関する実態調査2017」(2017年4月13日)

法制度・規範の整備

技術の急速な進歩に、法制度・規範の対応が追いついていないのが現状
安全･安心なサイバー空間の構築に向けて、法制度・規範の整備が必要

国内法制度

サイバーセキュリティの強化には、攻撃に関する研究や攻撃元の特定等が必要不可欠。

しかし → **不正アクセス禁止法や著作権法、電気通信事業法**等に抵触する恐れがあり、逆にセキュリティ強化に向けた研究や対策の障壁に。

- ✓ **参考とすべきガイドラインの整備や法律の必要十分な見直しが必要**

技術基準

米国は、サイバーセキュリティ技術に関するフレームワークや認証(NIST SP800 ・FedRAMP等)を導入、国家全体のクラウド化推進にも寄与。

- ✓ これらの取り組みを運用も含めて参考にし、民間の意見も取り入れながら、**国際的に通用する技術標準や対策ガイドラインを早期に策定すべき**

国際規範

安心・安全なサイバー空間の構築に向け、国連等において国際的な枠組みや規範を作る動きがある。

- ✓ わが国でも、あらゆる関係省庁や民間組織も含めた関係者による対話を重ね、**産学官で国際規範の策定の動きに積極的に参画・主導**していく必要

経団連アクションプラン

Keidanren Policy & Action

経団連自身も、サイバーセキュリティ対策の強化をSociety 5.0 実現に向けた最重要課題と捉え、自ら変革を促す取り組みを進めていく

1 経営層の理解促進に向けたAction

- 『経団連サイバーセキュリティ経営宣言』の策定
- 経営者向けセミナー・研修・合宿の実施

2 周知・広報に関するAction

- 各社のサイバーセキュリティ対策の実態調査、事例集等の公開
- 機関誌や説明会・講師派遣等を通じた広報・周知
- 政府・各団体におけるイベントへの協力
- 国内外のステークホルダーへの情報発信

3 国際連携の推進に向けたAction

- 日米サイバー対話、インターネットエコノミーに関する日米政策協力対話、日EU・ICT戦略ワークショップ等の国際会合への参加
- 世界経済フォーラム（WEF）等との連携

おわりに

Keidanren Policy & Action

**2020年の東京オリンピック・パラリンピックに向けて、
サイバーセキュリティの強化は喫緊の課題。**

**企業・団体、政治家、政府・地方公共団体、
大学・教育機関・研究機関、メディア、投資家、市民など
あらゆるステークホルダーの団結が必要不可欠。**

**わが国の基礎技術力、品質重視、
仕事に真面目に取り組む国民性は、
世界のサイバーセキュリティ強化にも貢献できる。**

**経団連としても政府や各団体と連携しながら、
具体的な取り組みを進めていく。**

参　考

サイバー攻撃の現状

Keidanren
Policy & Action

■WannaCry（ワナクライ）

・Microsoft Windowsの脆弱性をついたワーム型ランサムウェア（感染したパソコンに特定の制限をかけ、その制限の解除と引き換えに金銭を要求）。
・2017年5月12日から大規模なサイバー攻撃が開始され、150か国の23万台以上のコンピュータに感染し、身代金として暗号通貨ビットコインを要求。

■イラン核施設へのStuxnet（スタックスネット）攻撃

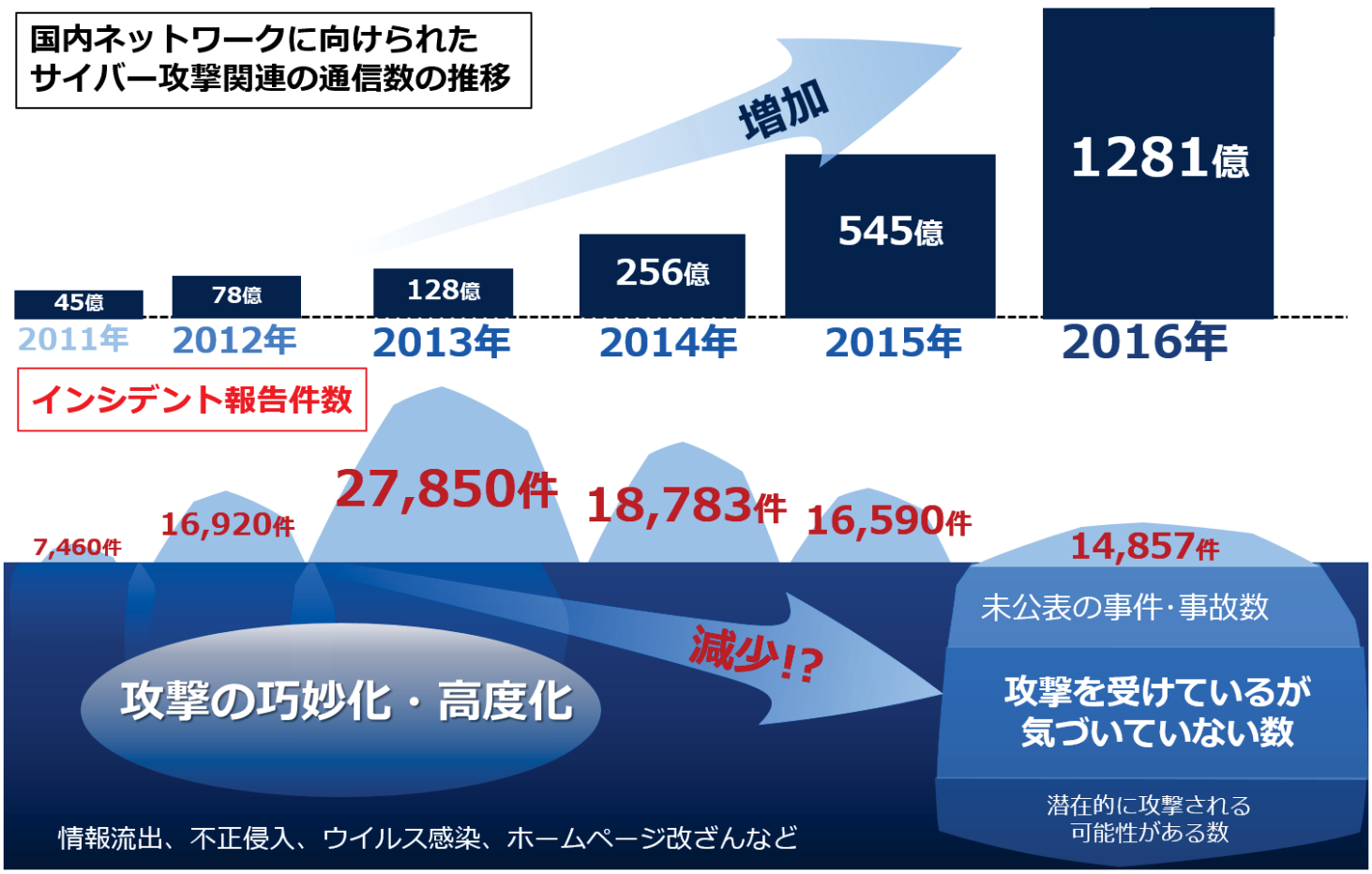
・「スタックスネット」というマルウェアによるサイバー攻撃により、2009年にイランにある核燃料施設で多数の遠心分離機が制御不能となった。
・USBメモリにマルウェアを仕掛け、インターネットなどに繋がっていない核施設の制御装置を不正操作し、遠心分離機の回転速度を急速に上げ下げして破壊が行われた。
・アメリカとイスラエルが関与したと指摘されているが、公式には関与を認めていない。
・重要インフラへの物理的な破壊が行われた初めてのサイバー攻撃と言われている。

■経団連事務局コンピュータのマルウェア感染

・2016年11月、経団連事務局のコンピュータがマルウェア感染により、外部との不審な通信を行っていたことが判明、公表した。
・PlugX(プラグエックス)、Elirks(エリクス)というマルウェアが発見された。

サイバー攻撃の件数の推移

Keidanren Policy & Action



出典:国立開発研究法人　情報通信研究機構（NICT） JPCERT/CC レポートより NEC作成資料

オリンピック・ロンドン大会とリオ大会

Keidanren Policy & Action

ロンドン大会（2012年）で観測されたサイバー攻撃

- 初のデジタルオリンピックと言われる2012年ロンドン大会では、英国政府は数兆円規模の政府予算をつけて英国全体の総合的なセキュリティ対策を実施。
- 公式サイトへ2億回以上のサイバー攻撃、全体で23億5000万件のセキュリティイベントが発生したと言われている。
- 開会式前日に、東欧からのサイバー攻撃があった。開会式当日には、電力システムを狙った攻撃や北米や欧州の90のIPアドレスから1,000万件のDDoS攻撃が40分間にわたって続いた。
- 大会終了間近には、１秒間に30万パケットのDDoS攻撃が同じIPアドレスから送られてきた。
- ロンドン大会では十分な準備も行われていたこともあり、上記攻撃により大会運営に支障をきたすほどの影響はなかったとも言われる。

リオ大会（2016年）で観測されたサイバー攻撃

- 大会開始前からネットのSNS等でサイバー攻撃の予告や呼びかけが見られた。
- 開会当初は大会関連Webサイトを標的とした攻撃が多く確認されたが、徐々に攻撃の対象が周辺のWebサイトへと移行。公共事業を請け負った建設会社のWebサイトから個人情報が漏洩した。
- オリンピック期間中に4,000万回のセキュリティ脅威を観測、2,300万回の攻撃をブロック、大規模なDDoS攻撃は223回ほどあった（Cisco）。
- オリンピック開会直後に攻撃のピークを迎えたが、事前の対策や演習等の備えにより迅速に対処できたため、大きな問題は発生しなかったと言われている。

出典:"BT reveals over 200 million hack attempts on London Olympics 2012 website"
https://www.v3.co.uk/v3-uk/news/2279265/bt-reveals-over-200-million-hack-attempts-on-london-olympics-2012-website
"Cisco's Digital Network Shines at Rio 2016"　https://blogs.cisco.com/news/ciscos-digital-network-shines-at-rio-2016
内閣サイバーセキュリティセンター（NISC）　資料

「情報セキュリティ10大脅威 2017」

新たな脅威として、IoT機器の脆弱性が顕在化

■「情報セキュリティ10大脅威 2017」

昨年順位	個人	順位	組織	昨年順位
1位	インターネットバンキングやクレジットカード情報の不正利用	1位	標的型攻撃による情報流出	1位
2位	ランサムウェアによる被害	2位	ランサムウェアによる被害	7位
3位	スマートフォンやスマートフォンアプリを狙った攻撃	3位	ウェブサービスからの個人情報の窃取	3位
5位	ウェブサービスへの不正ログイン	4位	サービス妨害攻撃によるサービスの停止	4位
4位	ワンクリック請求等の不当請求	5位	内部不正による情報漏えいとそれに伴う業務停止	2位
7位	ウェブサービスからの個人情報の窃取	6位	ウェブサイトの改ざん	5位
6位	ネット上の誹謗・中傷	7位	ウェブサービスへの不正ログイン	9位
8位	情報モラル欠如に伴う犯罪の低年齢化	8位	IoT機器の脆弱性の顕在化	ランク外
10位	インターネット上のサービスを悪用した攻撃	9位	攻撃のビジネス化（アンダーグラウンドサービス）	ランク外
ランク外	IoT機器の不適切な管理	10位	インターネットバンキングやクレジットカード情報の不正利用	8位

出典：情報処理推進機構(IPA) 2017.5.30　https://www.ipa.go.jp/security/vuln/10threats2017.html

Keidanren
Policy & Action