資料2

# 今後の取組みの方向性（案）

平成27年4月
事務局

# CPS社会に求められるサイバーセキュリティ

## 1. ネットワークでつながる主体・端末数が増加

例）ヘルスケアデータの予防医療等への活用


例）電力消費情報の流通による小売市場活性化


**求められるセキュリティ経営のポイント**

- ビジネスパートナーへの一定基準のセキュリティ対策の要求
- 第三者認証等を活用した自組織のセキュリティ対策の情報開示

## 2. 所有・分析するデータの増加

例）業務委託・クラウドの活用によるビッグデータの蓄積・解析


**求められるセキュリティ経営のポイント**

- 委託先管理の徹底
- クラウド活用におけるセキュリティチェック

## 3. 影響の大きい重要システムへのつながり

例）センサーによるインフラ管理


例）自動走行等による交通インフラの管理

**求められるセキュリティ経営のポイント**

- サイバー攻撃情報の業種横断的共有による対策のアップデート
- 攻撃を受ける前提での緊急体制の整備・リスクファイナンス等の活用

**予想されるリスク**

- ○ サイバー攻撃により窃取できる企業情報の付加価値が上がり、不正な取引の対象となるおそれ
- ○ サプライチェーンおいて、取引先企業のセキュリティホールが原因で情報が漏洩するおそれ
- ○ 重要インフラにおいて、予期せぬ機器・ネットワークの入口から致命的な攻撃を受ける懸念

# 今後の取組みの方向性（案）

○　当研究会での議論を踏まえ、今後、以下の3本柱の取組みを具体化していくべきではないか。

※　産業構造審議会情報経済小委員会中間取りまとめにおいても、概ね記載。

## 1．CPS社会に求められるサイバーセキュリティ経営ガイドラインの策定

【取組みの方向性（案）】

以下を主な内容とするガイドラインを、平成27年度に有識者委員会を設置して策定してはどうか。

- ○　CPS社会に求められるサイバーセキュリティ経営のポイント
- ○　CPS社会における経営層のリーダーシップと社内専門組織の設置・運用
- ○　サイバーセキュリティ人材の確保・育成
- ○　つながるビジネスパートナーと連携したセキュリティ対策の実施
- ○　高度なサイバー攻撃に対応するための技術的対策

  例）　検知能力の強化、侵入されても被害を最小限に抑えるネットワーク設計　など侵入を前提とした対策

- ○　ステークホルダーへの情報開示のあり方

# 今後の取組みの方向性（案）

## 2. 同ガイドラインに基づいた第三者認証制度の確立

【取組みの方向性（案）】

○　1. のガイドラインも踏まえ(注)、約4,600社が取得するISMS認証に上乗せとなる認証制度を確立。

（注） 制御システム機器に関するIEC62443やクラウドに関する国際基準等も踏まえる予定

○　また、第三者認証取得企業のリスクを算出し、保険会社と共有。サイバー保険を促進する仕組みの構築。

○　中小事業者向けの“軽量版”認証基準についても併せて検討。

## 3. 官民・業種を越えた情報共有の促進

【取組みの方向性（案）】

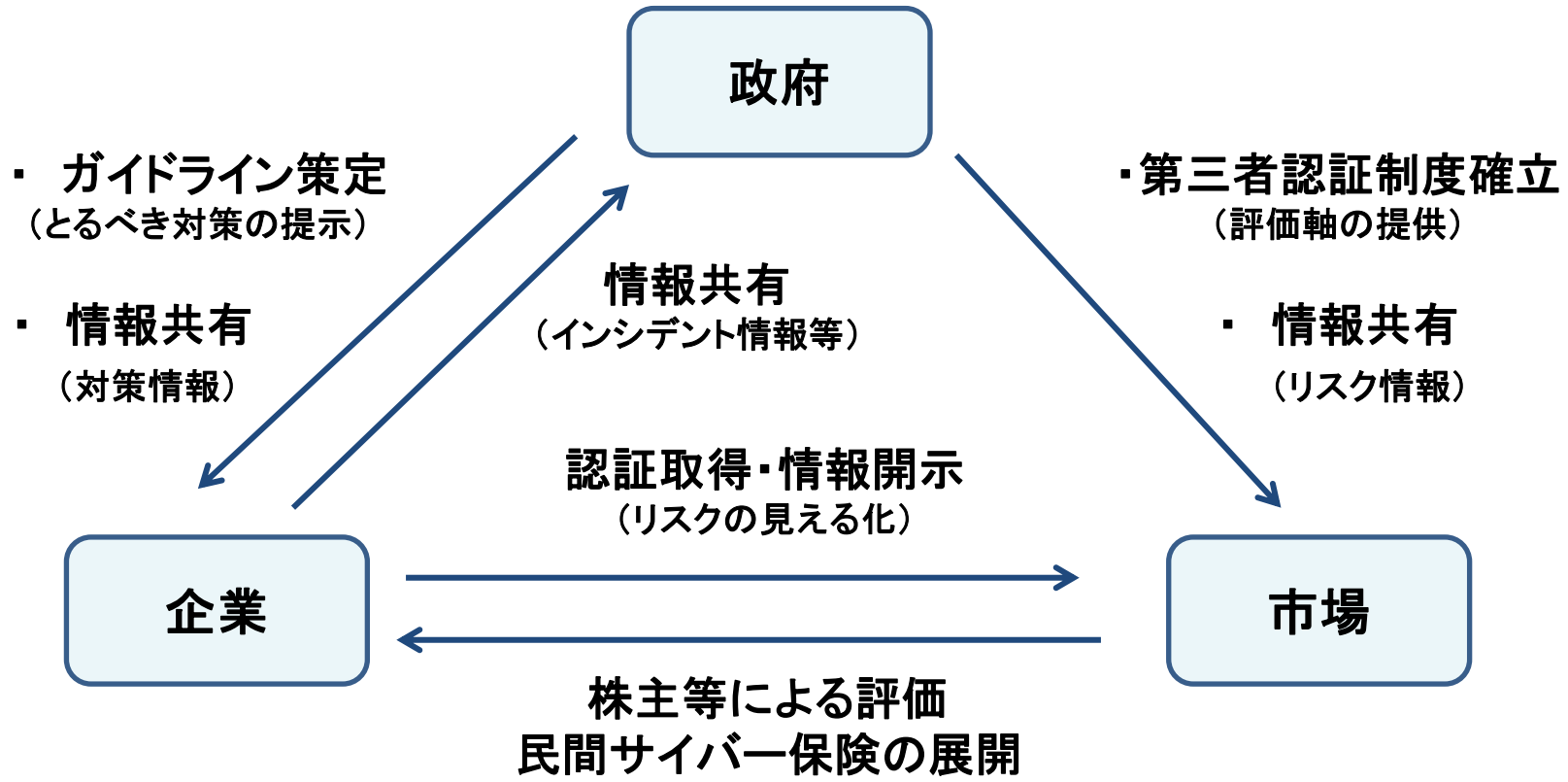
○　IPA（（独）情報処理推進機構）が分析ハブとなった情報共有活動（J-CSIP）の参加業種・参加企業等の拡大。

※　従来の5業種（重工・電力・ガス・石油・化学）に加えて、本年3月に新たに6番目の業種（資源開発）が参加。

○　対策向上のために共有する情報の種類等の充実も検討。

# （参考）今後の取組みの方向性（イメージ）

国がイニシアティブを取って、民間部門における
自主的な取組みを促進する枠組みを構築。



# （参考） 諸外国の取組み

諸外国では、政府主導により、民間企業の自主的な取組みを促進する動きあり。

## 米国

**① 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2月）

- **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**。

**② 民間部門によるサイバーセキュリティ情報の共有強化**（2015年2月）

- サイバー攻撃情報と脆弱性情報を共有する業種別の**官民情報共有網の構築**促進に関する**大統領令を発出**。
- 国土安全保障省が、当該官民情報共有網の構築を支援する予定。
- また、サイバー攻撃情報の共有促進のため、**ホワイトハウスに新たな組織**を設置する予定。

## ドイツ

○ 重要インフラ事業者に対して**基準に基づく対策を義務づける法案の政府案を公表**。

○ **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。

○ また、BSI（情報セキュリティ庁）の分析能力を強化し、BSIをハブとした情報共有網を強化。

## 英国

○ ロンドンオリンピック開催にあたって、重点的に対策を講じるべき重要インフラ8分野を特定。

○ **官民のCIOｸﾞﾙｰﾌﾟと実務者ｸﾞﾙｰﾌﾟ**を大会4年前に構成し、**官民における対策の進捗管理**。

○ 大会直前には、官民合同のサイバー演習等を実施。

# （参考）情報セキュリティマネジメント認証制度（ISMS認証）

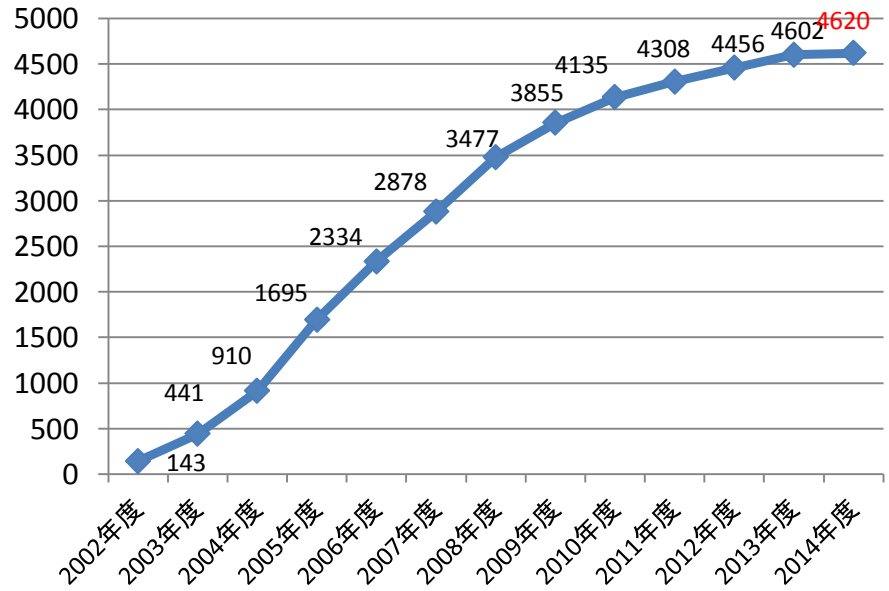
## ○ ISMS認証制度の経緯

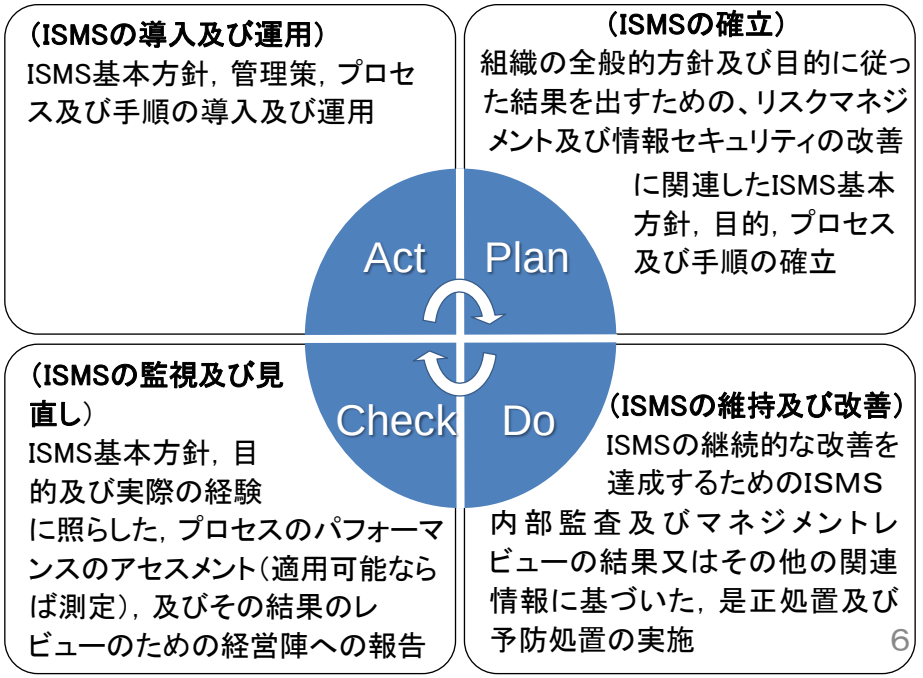
- ISMS（Information Security Management System 情報セキュリティマネジメント）認証制度は、組織における情報セキュリティを管理するための手順・体制を認証する制度。
- 1995年に英国にて規格化された後、国際規格ISO/IEC 27001により国際的な標準を規定。
- 国内では、2002年4月より、経済産業省委託事業により一般財団法人日本情報経済社会推進協会（JIPDEC）が制度を開始。2014年度までで、4,620組織が取得。

## ○ ISMS認証のポイント

- セキュリティ対策のPDCAを繰り返す管理体制が構築されているのかをドキュメントベースで確認。

### ISMS認証取得者数の推移



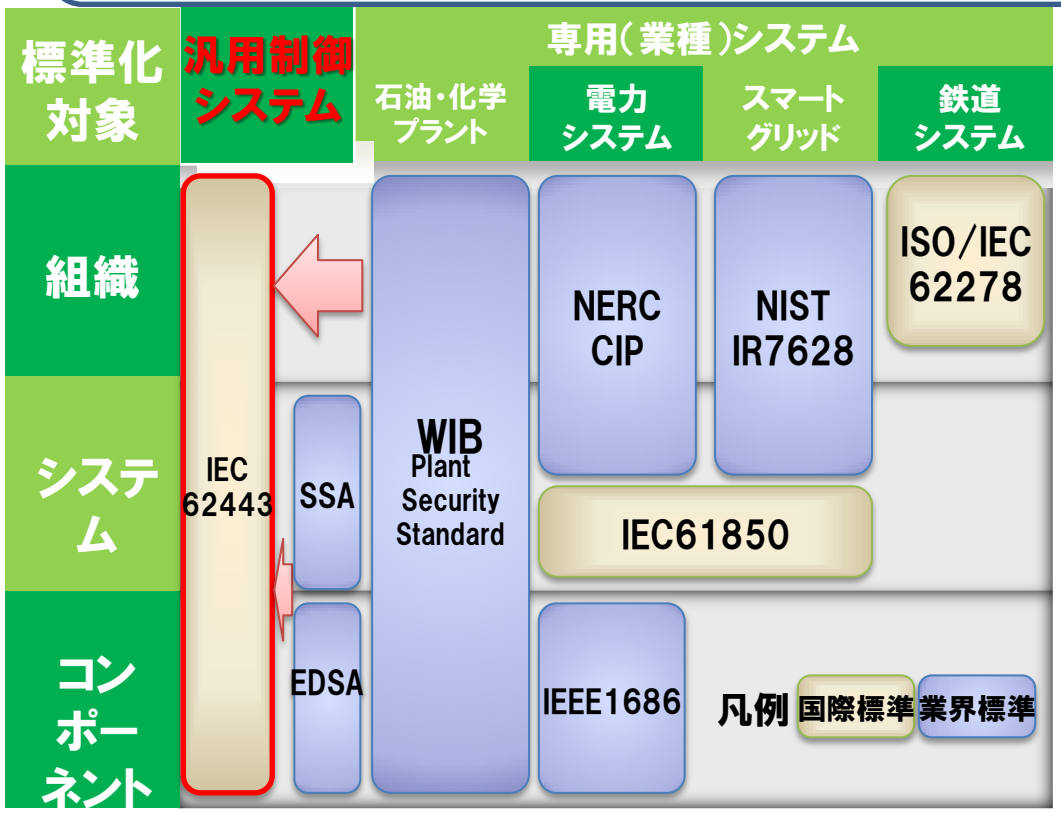



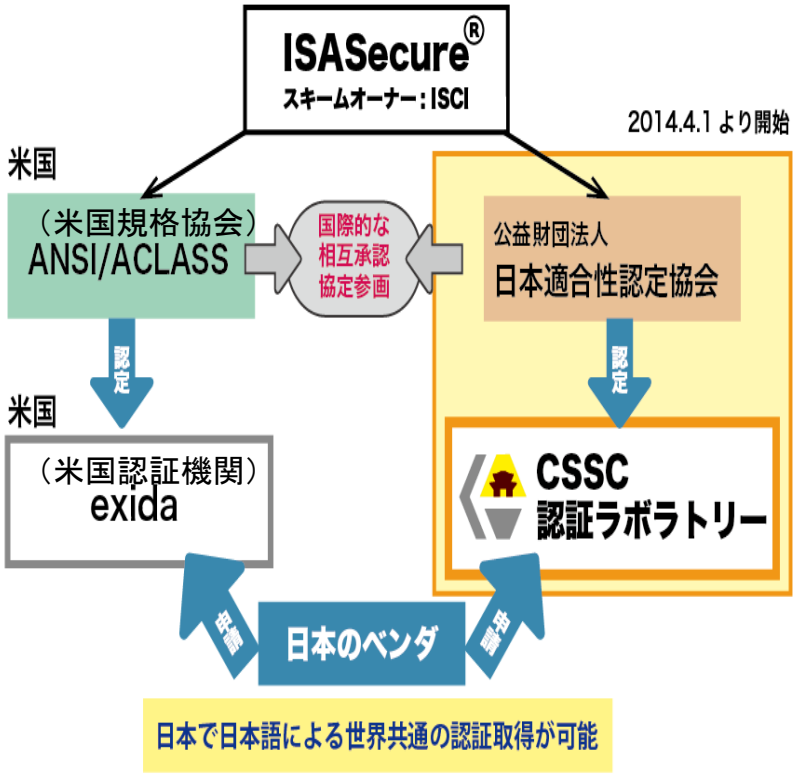
# （参考） IEC62443について

○ CSSCで実施している制御機器向けセキュリティ認証（EDSA認証）は、ISA（国際計測制御学会。CSSCも会員）で議論され、策定された基準。

○ 日米両国でこの基準に基づく認証が行われており、日本での認証が米国でも自動認証されるスキームとなっている。

○ この基準は、IEC（国際電気標準学会）において、日米両国により制御システム一般に適用される国際基準に提案されている（2017年に国際標準化予定）。




ISA（The International Society of Automation）：国際計測制御学会。
ISCI（ISA Security Compliance Institute）： ISA内の産業機械等のセキュリティの認証基準の策定及び認証制度を推進する機関

# （参考）クラウドの安全指針策定と国際標準化の流れ