NISC National center of Incident readiness and Strategy for Cybersecurity

資料４

サイバーセキュリティの強化について

平成27年4月20日

内閣官房

内閣サイバーセキュリティセンター

IoTと成長戦略

IoTは成長戦略のkeyの１つ

○成長戦略進化のための今後の検討方針　（平成27年１月29日産業競争力会議決定）

（略）「ロボット革命」の実現に加え、ビッグデータ、人工知能やモノのインターネット（IoT）等の急速な発展により生産・流通・販売、交通、健康・医療、公共サービス等の幅広い分野で想定される産業構造の変革に対応するため、今後のビジネスモデルの在り方を見据えた産業横断的な課題及び対応策の検討を進めるとともに、人材育成やセキュリティ対策、グローバル市場を念頭に置いた国際標準化対応などの環境整備を加速化する。

背　景

- ハードウェアデバイスの進化
  （センサー等の小型化・低価格化が進展）
- 低廉・高速なインターネットの普及
- ビッグデータ解析技術の進歩

- あらゆるモノがネットワークでつながり、リアルタイムでのデータ化・自動制御が進展。あらゆる産業でデータの利活用、高度な判断サービスや自動制御が可能に。

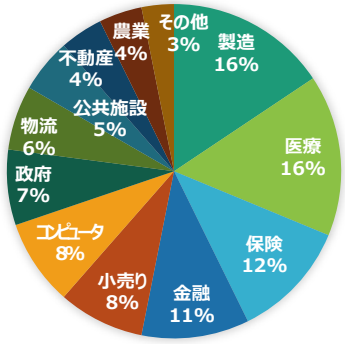
（出典：産業構造審議会 情報経済小委員会第1回（2014年12月）経産省資料等）

市場規模・対象範囲の拡大

- 創出する経済価値：
  1.9兆ドル（約228兆円）
- 全体のサービス投資：
  2630億ドル（約32兆円）
- 対応製品は約250億台
  （PC、スマートフォン、タブレット以外の端末が過半数）

※ 数字は2020年時点の予測、1ドル＝120円で計算

多様な市場



（出典：Gartner）

諸外国も国家レベルで推進

ドイツ政府は、2011年、独製造業の競争力強化のための構想“Industry4.0” を提示し、IoTによるさらなる効率化を国全体で強化。
メルケル首相の強力なリーダーシップにより推進。

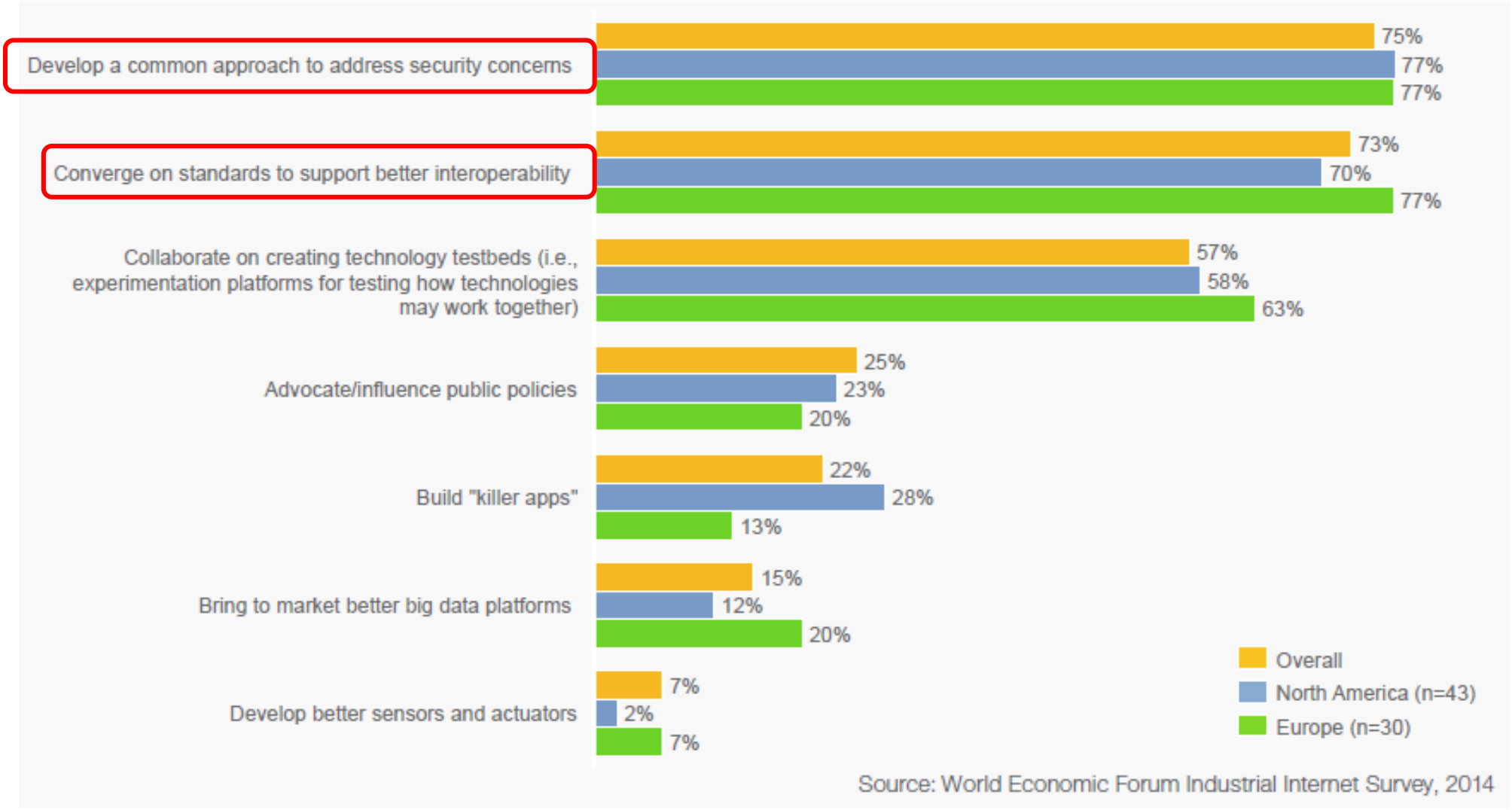
（出典：サイバーセキュリティ戦略本部研究開発戦略専門調査会第1回（2015年4月）経産省資料）

米国政府は、2012年、ビッグデータを活用し、国家の喫緊の課題解決を図るため「BigData R&D Initiative」を発表。民間では、GEが、「インダストリアル・インターネット」を提唱。60社以上でコンソーシアムを形成。

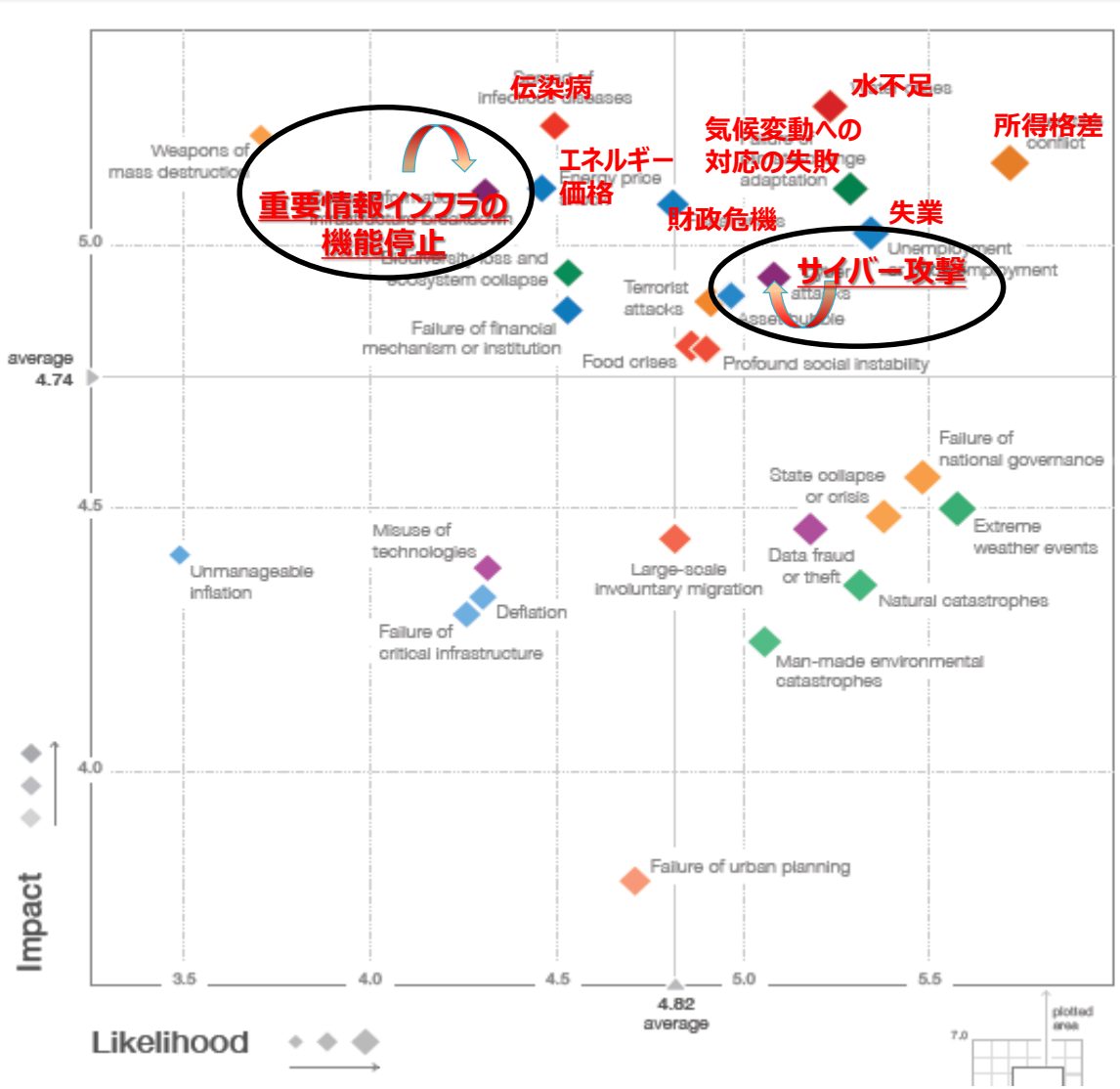
（出典：産業構造審議会 情報経済小委員会第1回（2014年12月）経産省資料）

IoT促進のカギとなるセキュリティ

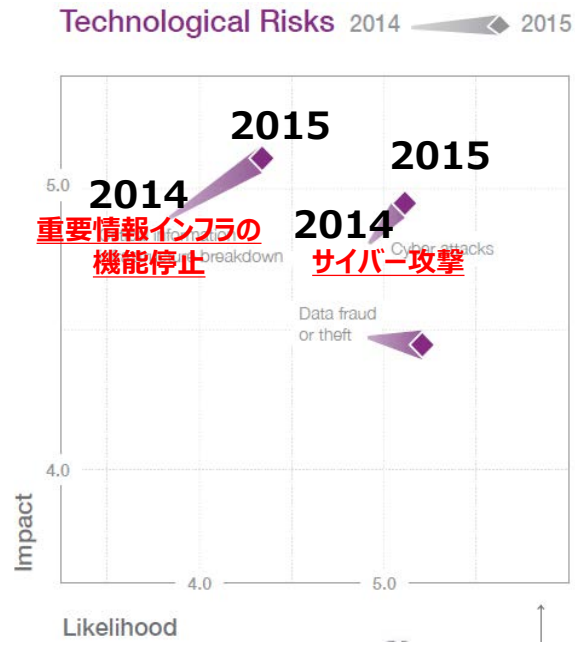
IoTの適用を加速させる重要なアクション ⇒ セキュリティと相互接続を促進する標準化が２大アクション



世界が直面するグローバルリスク



“大規模サイバー攻撃のリスクは、発生確率、発生時の影響度のいずれの側面からみても平均的リスクを上回る。これはサイバー攻撃がますます洗練化されていることに加え、インターネットに接続されるモノが急増し、企業によってクラウドにより多くの機微性を有するパーソナルデータが蓄積されるようになってきていることによるものである。”



備考：全世界及び全産業界に対して重大な悪影響を及ぼす可能性のあるものとして抽出した28のリスクに関する今後10年間の展望について、世界各地の約900名の専門家に対する調査結果をとりまとめたもの。

(Source)World Economic Forum “Global Risks 2015 : 10th edition”

サイバーセキュリティをめぐる状況の変化

IT依存度の高まり

ＰＣ 
多くの職場・家庭に普及し、インターネットに接続
（2013年末：PC普及率 81.7%、インターネット普及率 82.8%）
※2014年版情報通信白書（総務省）

スマートフォン 
世帯保有率が６倍に急増
（2010年末：9.7%→2013年末：62.6%）
※2014年版情報通信白書（総務省）

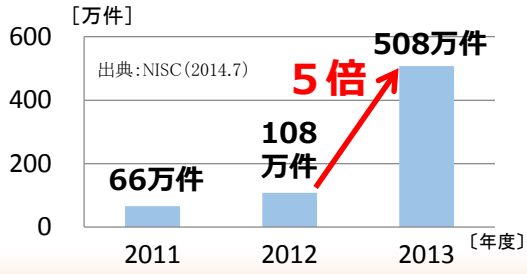
自動車 
一台に搭載される車載コンピュータは100個以上、
ソフトウェアの量は約1000万行
※自動車の情報セキュリティへの取組みガイド（2013.8 IPA）

スマートメーター（次世代電力量計） 
電力会社による開発・導入の開始
［主な予定］・東京：2020年度までに2700万台の導入完了
・関西：2022年度までに1300万台の導入完了

サイバー攻撃の増加

⇒ **６秒に１回**攻撃が発生

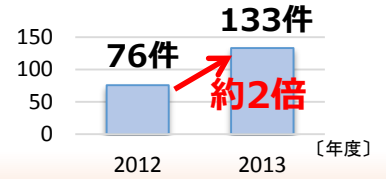
センサー監視等による脅威件数



⇒ **重要インフラ**への攻撃も増加

重要インフラへの攻撃件数

【重要インフラ分野】
情報通信、電気、鉄道、航空など13分野



国家関与の疑われる攻撃


韓国（2013年4月）

重要ｲﾝﾌﾗ（金融・放送等）に対する大規模サイバー攻撃が発生。韓国当局は北朝鮮の所業と発表。


米国（2014年12月）

ｿﾆｰ・ﾋﾟｸﾁｬｰｽﾞ・ｴﾝﾀｰﾃｲﾝﾒﾝﾄ社に対するサイバー攻撃が発生。 米国政府は北朝鮮に責任ありとし、国家安全保障上の問題として対応。

東京五輪へ向けた準備

- 世界の注目を集める祭典。「ダウンタイム」は許されない。
- 2012年のオリンピック・パラリンピックロンドン大会では、開催期間中、約２億件のサイバー攻撃が発生。
- 英国政府は、6年前からサイバー攻撃対策を準備。

サイバー脅威に対応し、サイバーセキュリティを強化するため、サイバーセキュリティ基本法が成立、施行。

（平成26年11月12日公布。平成27年１月９日全面施行）