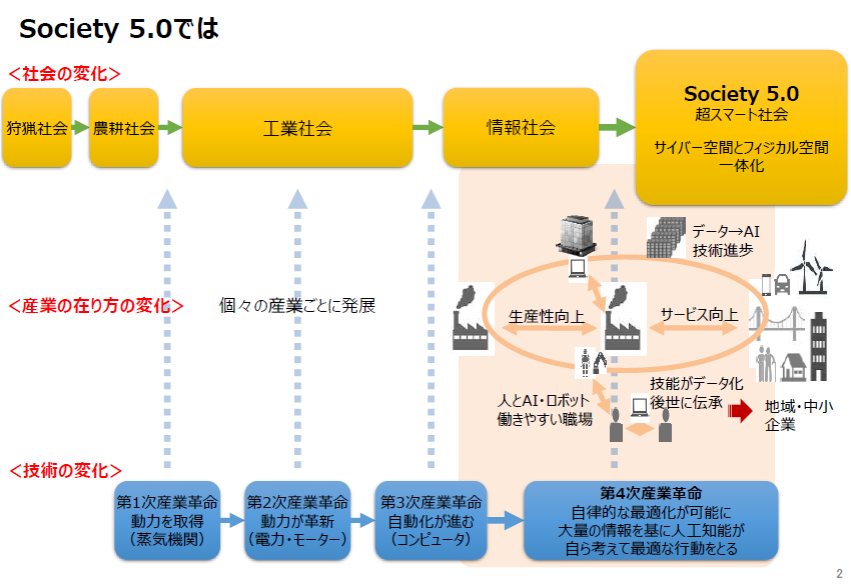
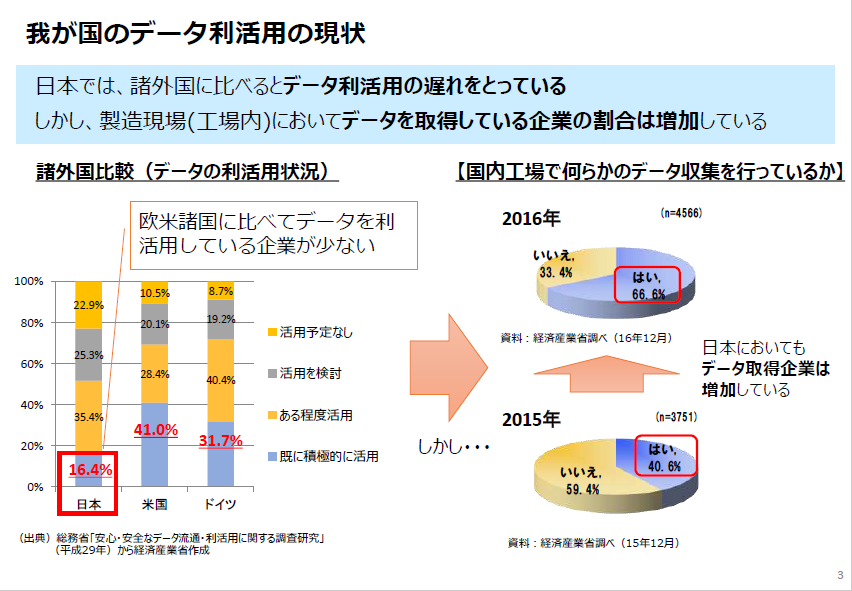
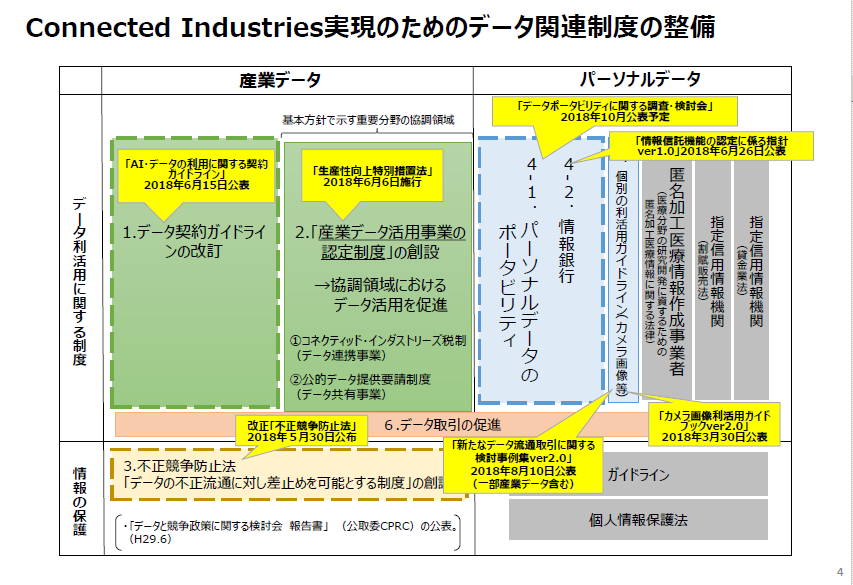
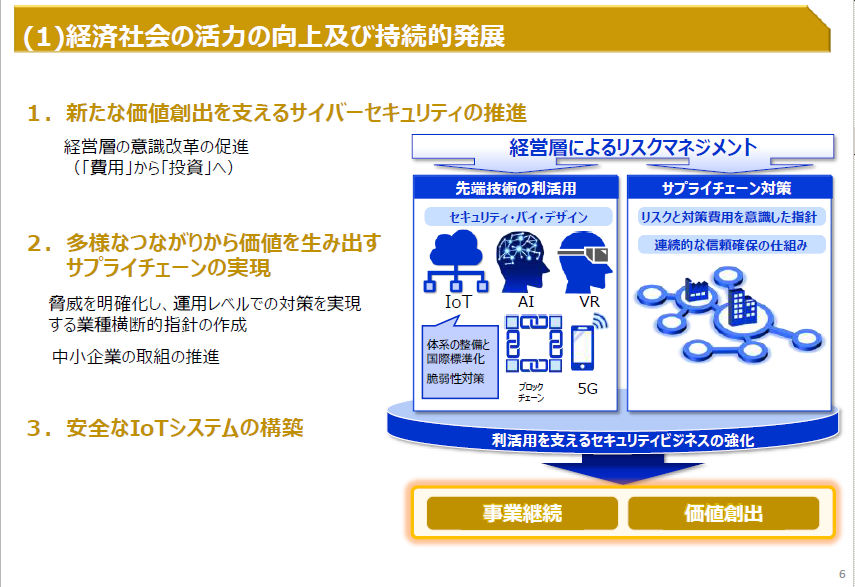
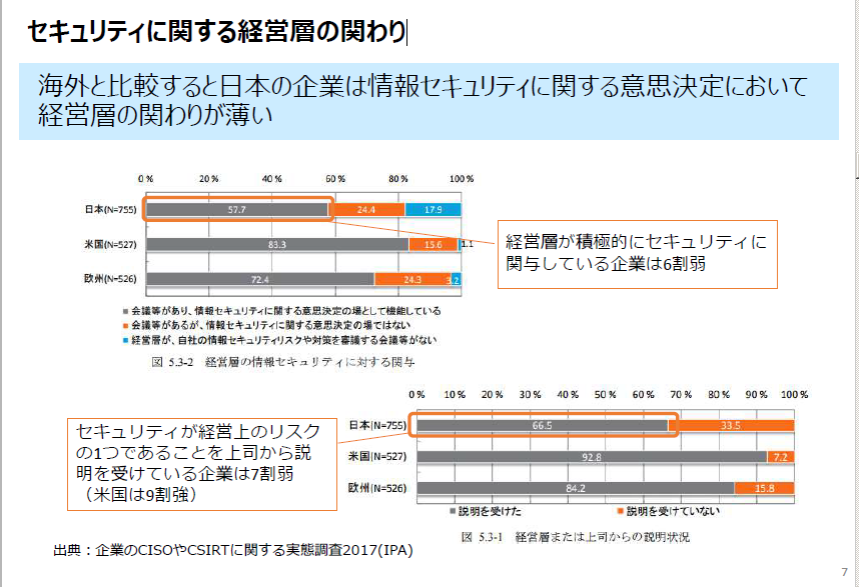
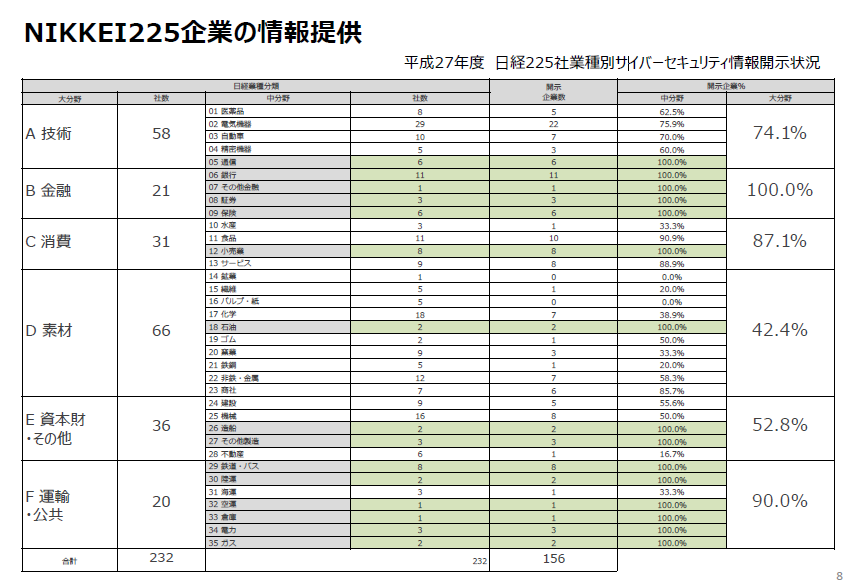
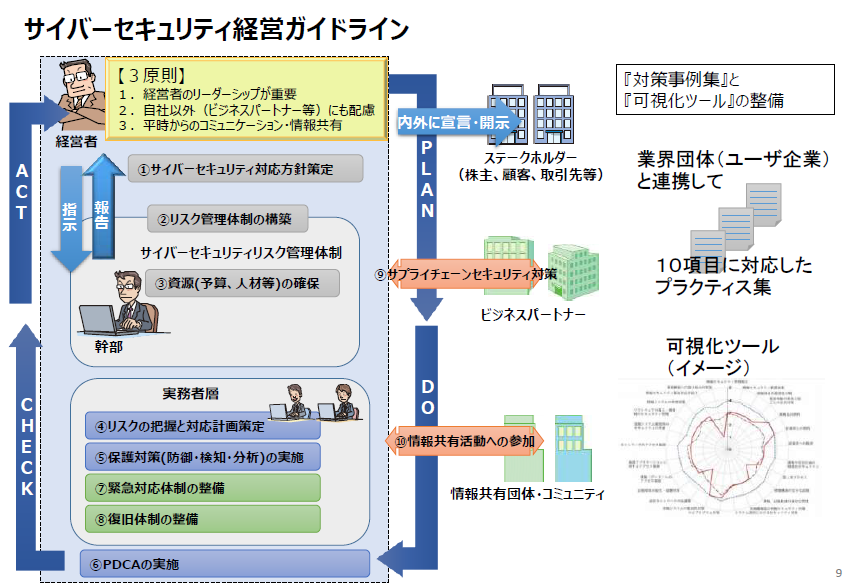
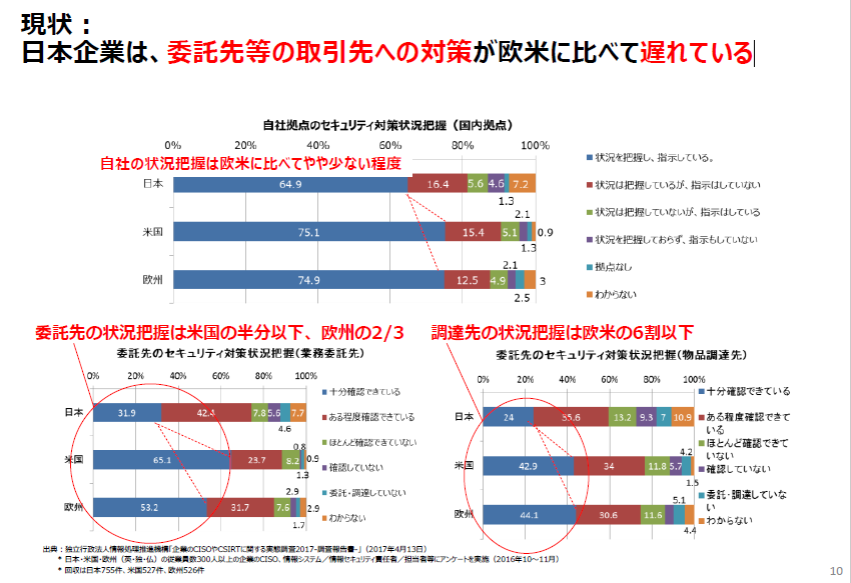
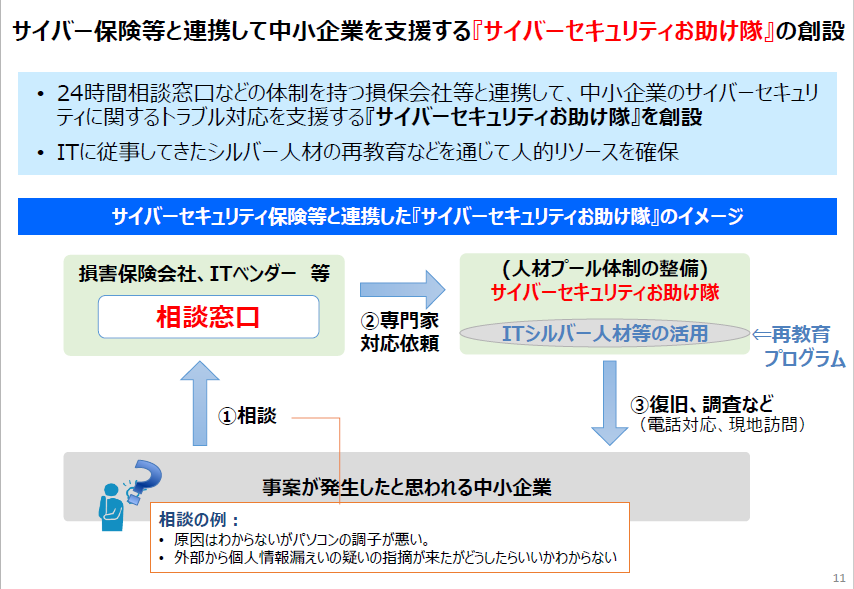
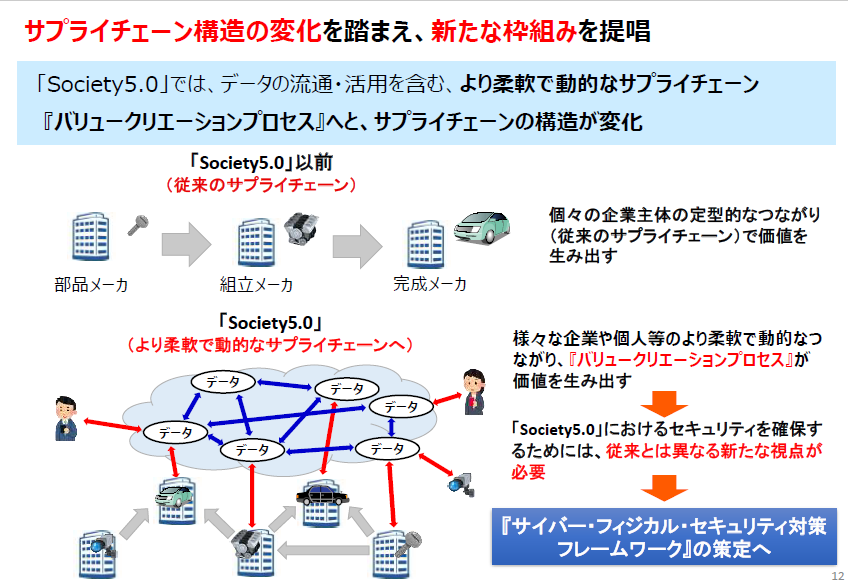
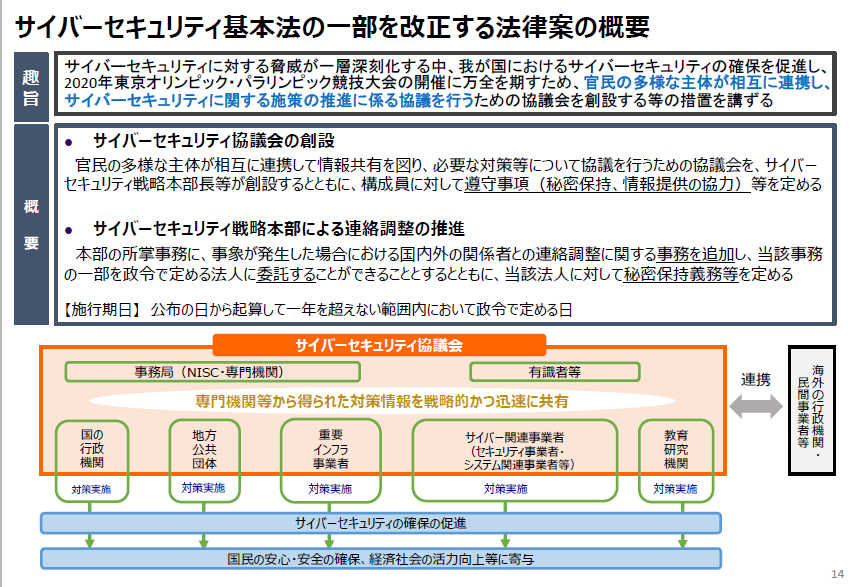
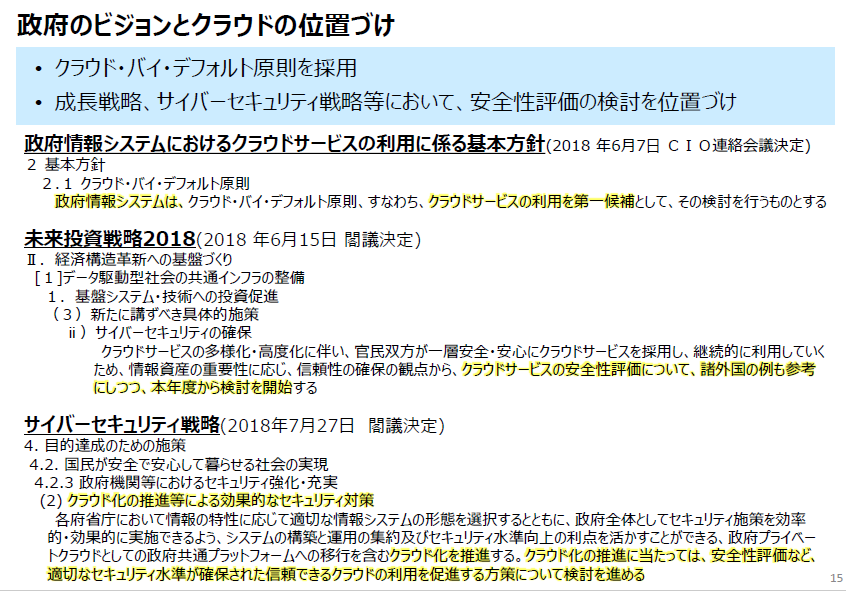
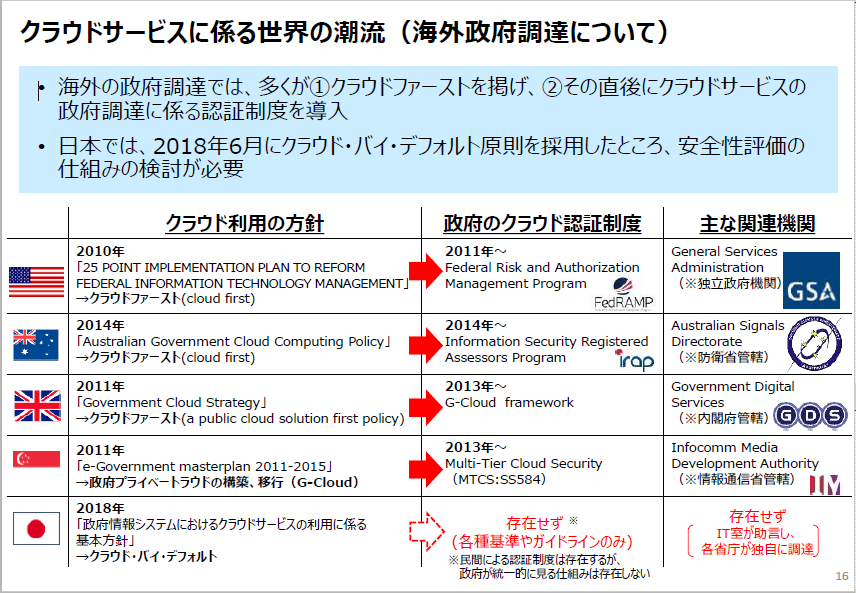
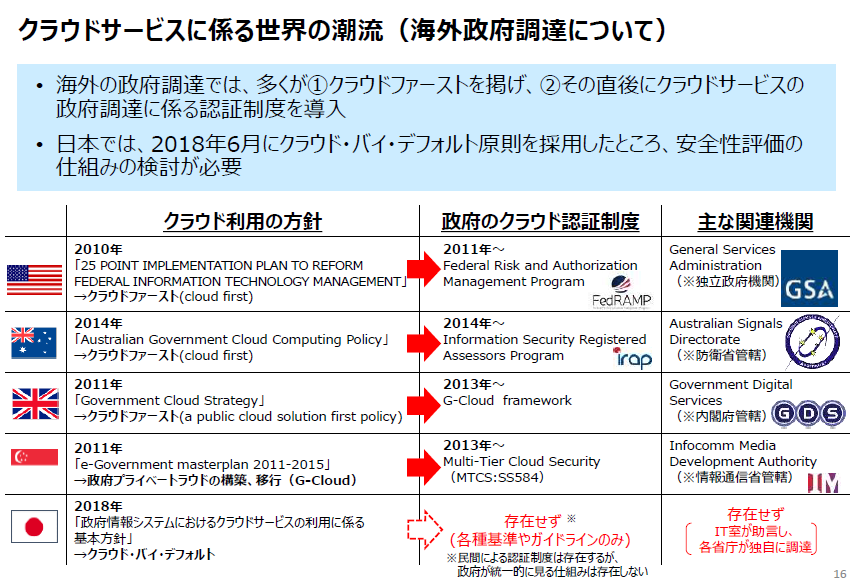
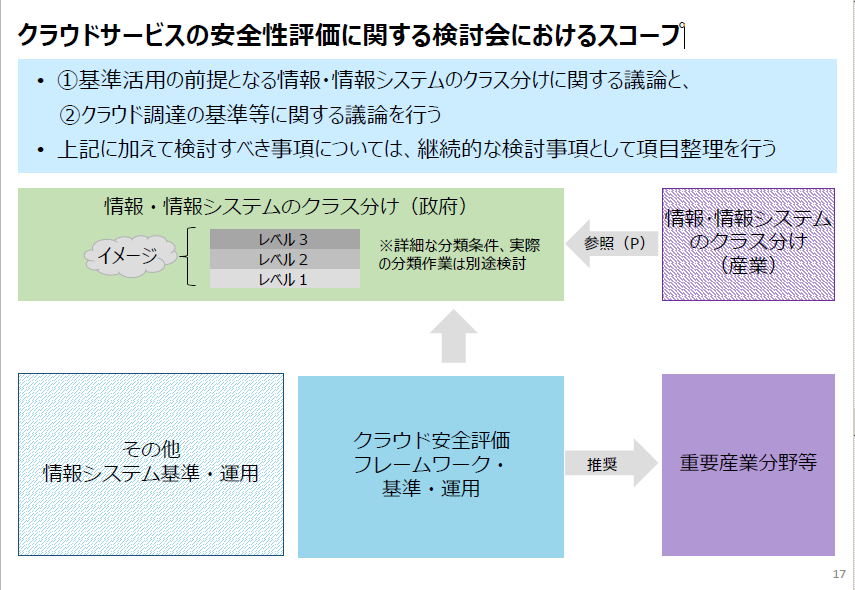
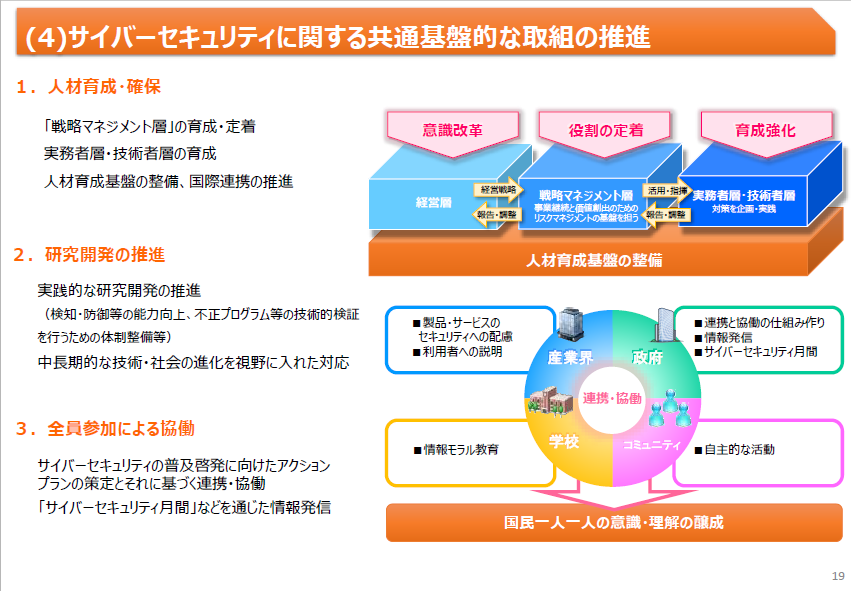
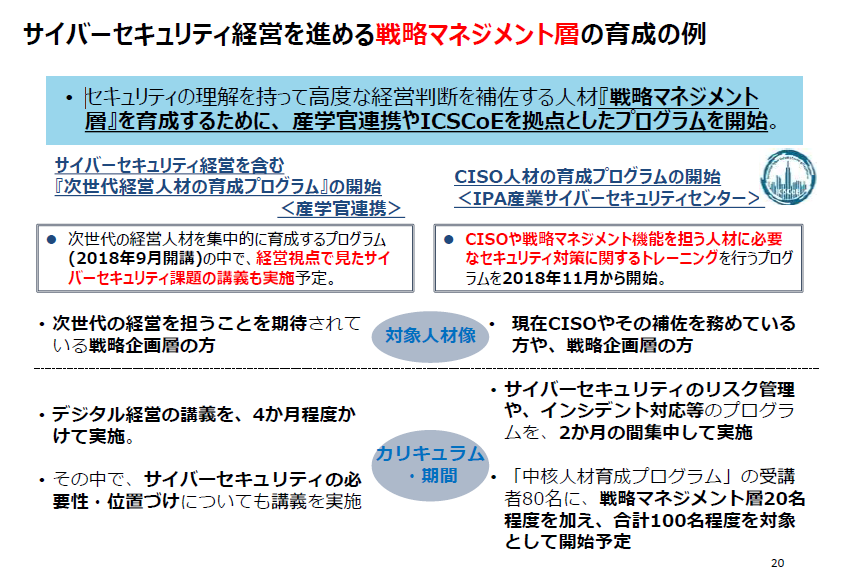
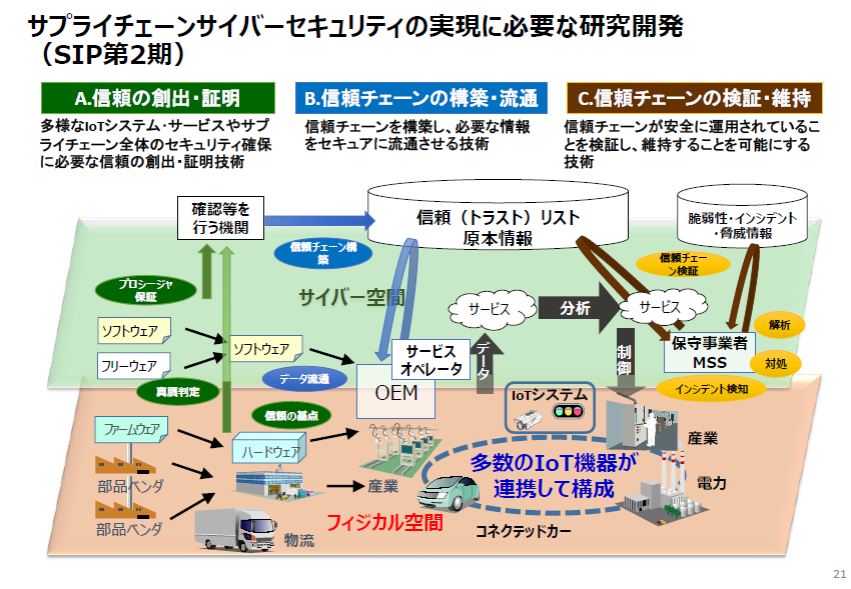
Sec01-03-01【スライド】クラウド化推進社会と我が国のサイバーセキュリティ戦略

1. 内閣官房内閣サイバーセキュリティセンター(NISC) 内閣審議官 経済産業省(METI) サイバーセキュリティ・情報化審議官 三角育生
2. トップ
   1. Subtopic  
      
3. Society 5.0では
   1. Subtopic  
      
4. 我が国のデータ利活用の現状
   1. Subtopic  
      
   2. 日本では、 諸外国に比べるとデータ利活用の遅れをとっている
   3. しかし、 製造現場(工場内)においてデータを取得している企業の割合は増加している
5. Connected Industries実現のためのデータ関連制度の整備
   1. Subtopic  
      
6. サイバーセキュリティ戦略
   1. Subtopic  
      
   2. １ 策定の趣旨・背景
      1. • Society5.0
      2. • サイバー空間と実空間の一体化の進展
   3. ２ サイバー空間に係る認識
      1. • 人工知能（AI)、 IoTなど→人々に豊かさ
      2. • 多大な経済的・社会的損失が生ずる可能性は指数関数的に拡大
   4. ３ 本戦略の目的
      1. • 自由、 公正かつ安全なサイバー空間
      2. • 持続的な発展のためのサイバーセキュリティ（サイバーセキュリティエコシステム）
      3. ← ①サービス提供者の任務保証、 ②リスクマネジメント、 ③参加・連携・協働
7. (1)経済社会の活力の向上及び持続的発展
   1. Subtopic  
      
8. セキュリティに関する経営層の関わり
   1. Subtopic  
      
9. NIKKEI225企業の情報提供
   1. Subtopic  
      
10. サイバーセキュリティ経営ガイドライン
    1. Subtopic  
       
11. 現状：日本企業は、 委託先等の取引先への対策が欧米に比べて遅れている
    1. Subtopic  
       
12. サイバー保険等と連携して中小企業を支援する『サイバーセキュリティお助け隊』の創設
    1. Subtopic  
       
13. サプライチェーン構造の変化を踏まえ、 新たな枠組みを提唱
    1. Subtopic  
       
14. (2)国民が安全で安心して暮らせる社会の実現
    1. Subtopic  
       
15. サイバーセキュリティ基本法の一部を改正する法律案の概要
    1. Subtopic  
       
16. 政府のビジョンとクラウドの位置づけ
    1. Subtopic  
       
    2. • クラウド・バイ・デフォルト原則を採用
    3. • 成長戦略、 サイバーセキュリティ戦略等において、 安全性評価の検討を位置づけ
    4. 政府情報システムにおけるクラウドサービスの利用に係る基本方針(2018 年6月7日ＣＩＯ連絡会議決定)
    5. 未来投資戦略2018(2018 年6月15日閣議決定)
    6. サイバーセキュリティ戦略(2018年7月27日閣議決定)
17. クラウドサービスに係る世界の潮流（海外政府調達について）
    1. Subtopic  
       
    2. • 海外の政府調達では、 多くが①クラウドファーストを掲げ、 ②その直後にクラウドサービスの政府調達に係る認証制度を導入
    3. • 日本では、 2018年6月にクラウド・バイ・デフォルト原則を採用したところ、 安全性評価の仕組みの検討が必要
18. クラウドサービスの安全性評価に関する検討会におけるスコープ
    1. Subtopic  
       
19. クラウドサービスの安全性評価に関する検討会におけるスコープ
    1. Subtopic  
       
    2. • ①基準活用の前提となる情報・情報システムのクラス分けに関する議論と、 ②クラウド調達の基準等に関する議論を行う
    3. • 上記に加えて検討すべき事項については、 継続的な検討事項として項目整理を行う
20. (3)国際社会の平和・安定及び我が国の安全保障への寄与
    1. Subtopic  
       
    2. １．自由、 公正かつ安全なサイバー空間の堅持
    3. ２．我が国の防御力・抑止力・状況把握力の強化
    4. ３．国際協力・連携
21. (4)サイバーセキュリティに関する共通基盤的な取組の推進
    1. Subtopic  
       
    2. １．人材育成・確保
       1. 「戦略マネジメント層」の育成・定着
       2. 実務者層・技術者層の育成
       3. 人材育成基盤の整備、 国際連携の推進
    3. ２．研究開発の推進
       1. 実践的な研究開発の推進
       2. （検知・防御等の能力向上、 不正プログラム等の技術的検証を行うための体制整備等）
       3. 中長期的な技術・社会の進化を視野に入れた対応
    4. ３．全員参加による協働
       1. サイバーセキュリティの普及啓発に向けたアクション
       2. プランの策定とそれに基づく連携・協働
       3. 「サイバーセキュリティ月間」などを通じた情報発信
22. サイバーセキュリティ経営を進める戦略マネジメント層の育成の例
    1. Subtopic  
       
    2. • セキュリティの理解を持って高度な経営判断を補佐する人材『戦略マネジメント層』を育成するために、 産学官連携やICSCoEを拠点としたプログラムを開始。
    3. サイバーセキュリティ経営を含む『次世代経営人材の育成プログラム』の開始＜産学官連携＞
    4. CISO人材の育成プログラムの開始＜IPA産業サイバーセキュリティセンター＞
23. サプライチェーンサイバーセキュリティの実現に必要な研究開発（SIP第2期）
    1. Subtopic  
       
    2. A.信頼の創出・証明
       1. 多様なIoTシステム･サービスやサプライチェーン全体のセキュリティ確保に必要な信頼の創出・証明技術
    3. B.信頼チェーンの構築・流通
       1. 信頼チェーンを構築し、 必要な情報をセキュアに流通させる技術
    4. C.信頼チェーンの検証・維持
       1. 信頼チェーンが安全に運用されていることを検証し、 維持することを可能にする技術