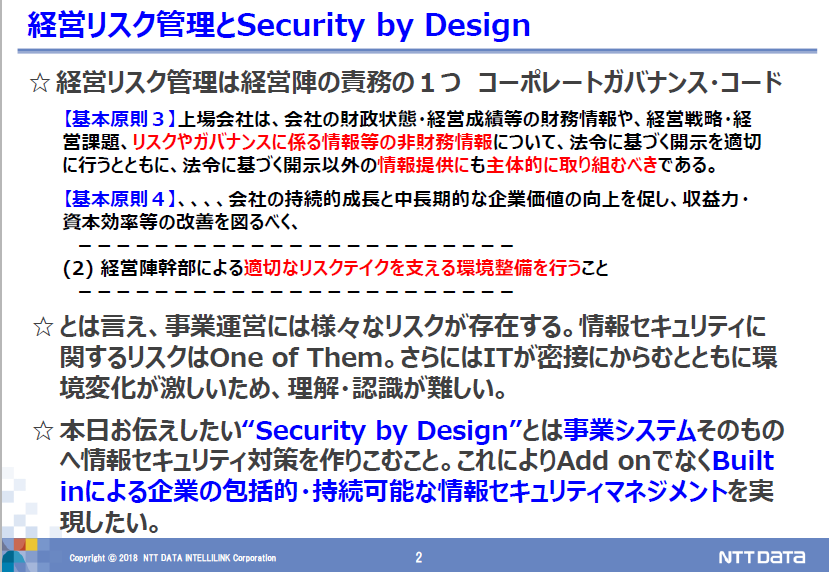
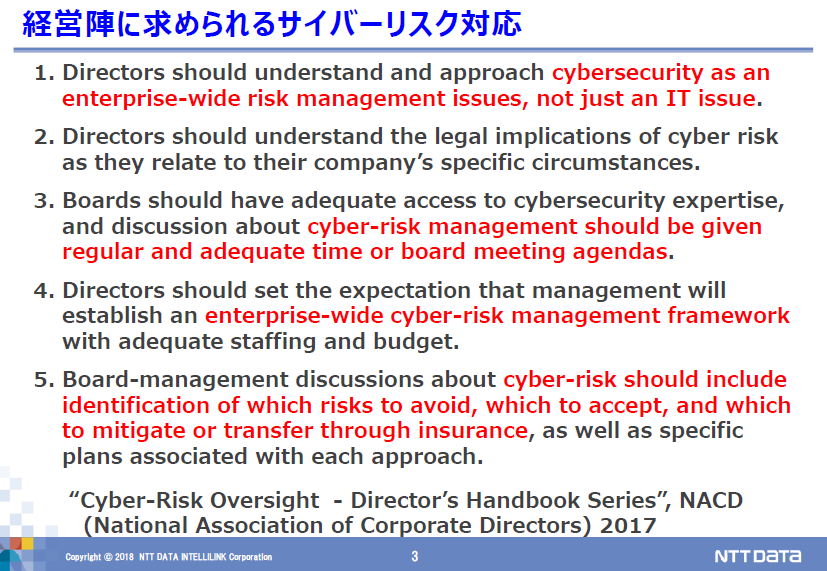
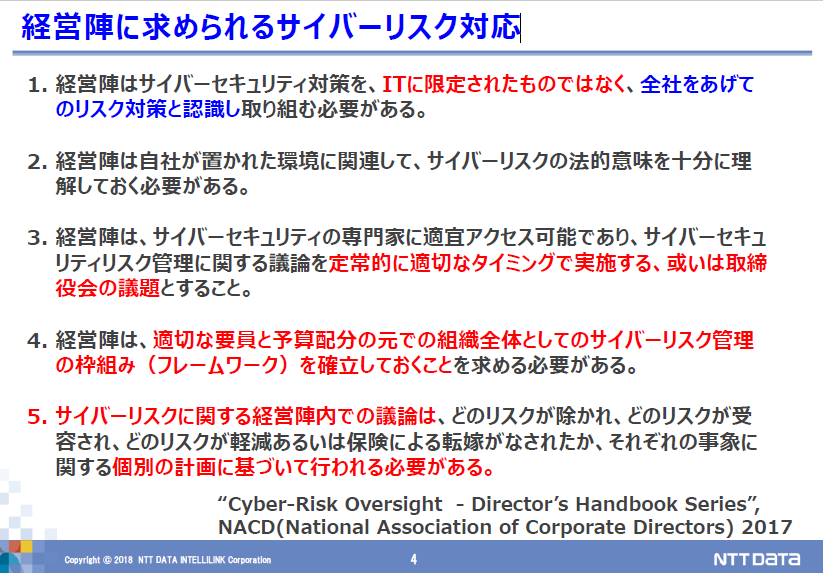
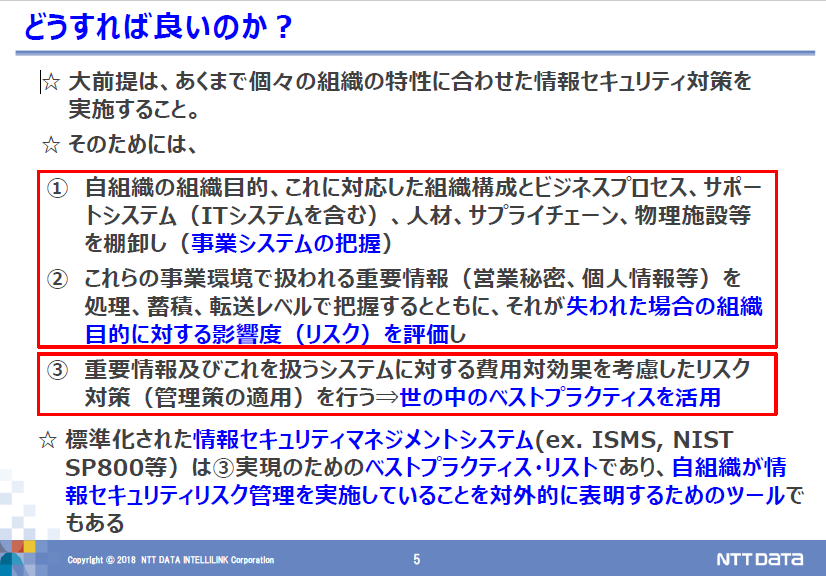
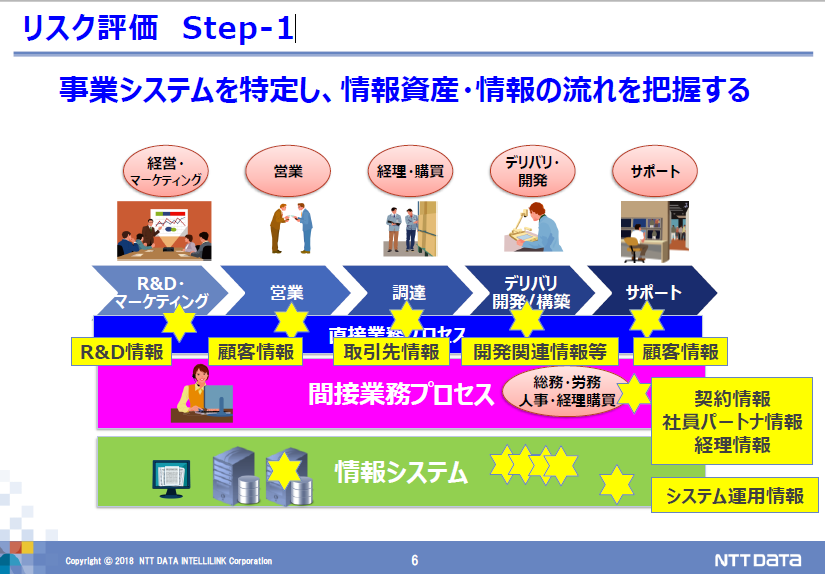
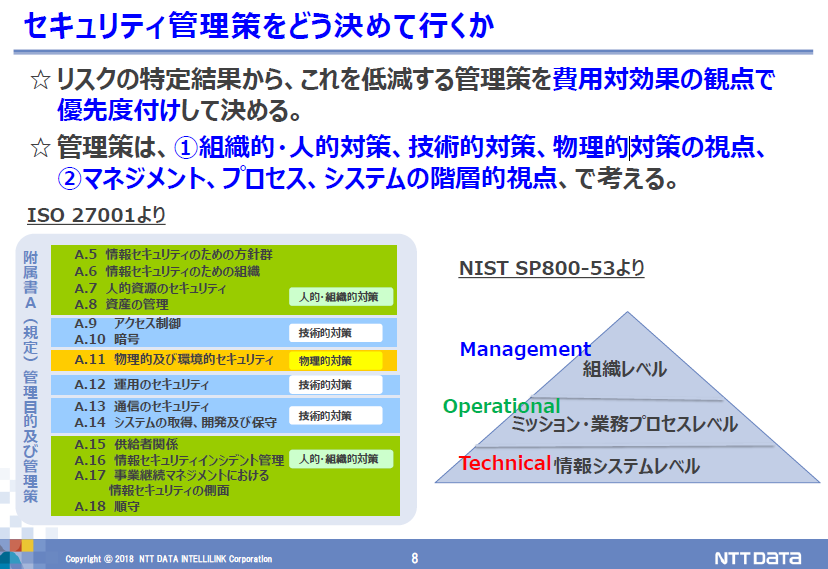
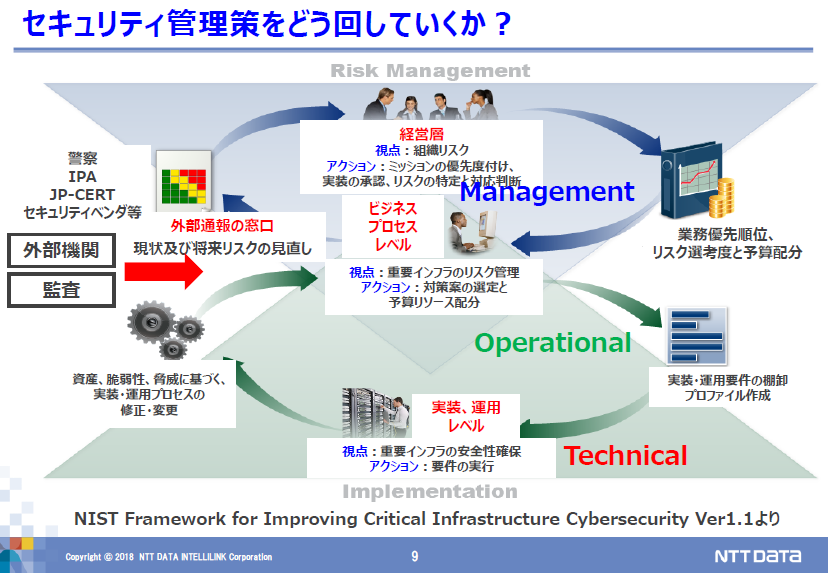
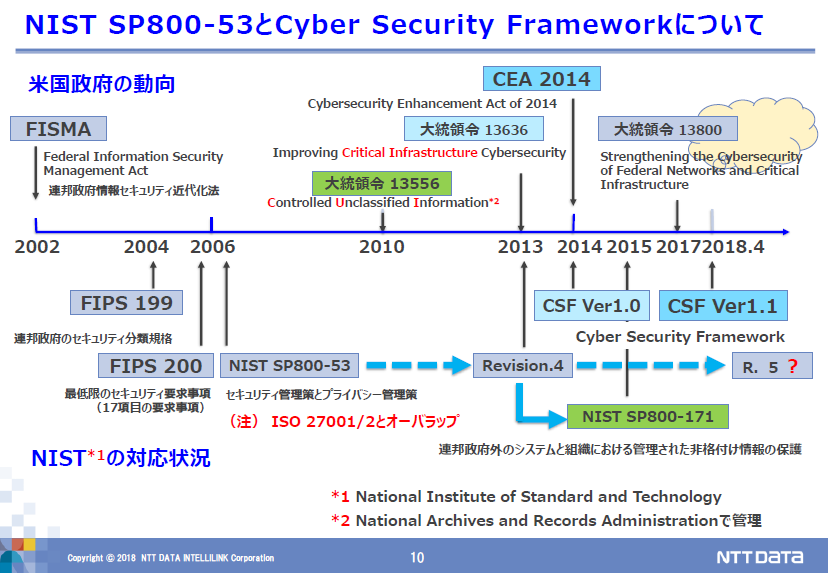
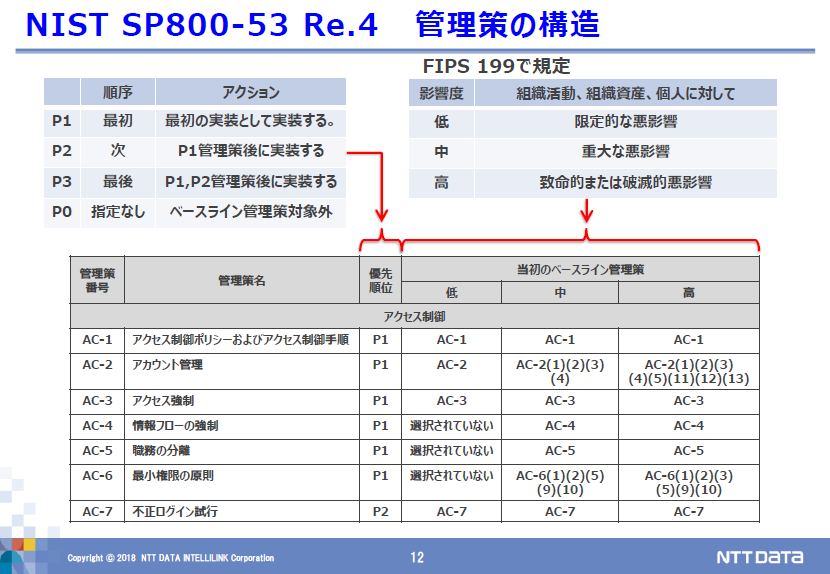
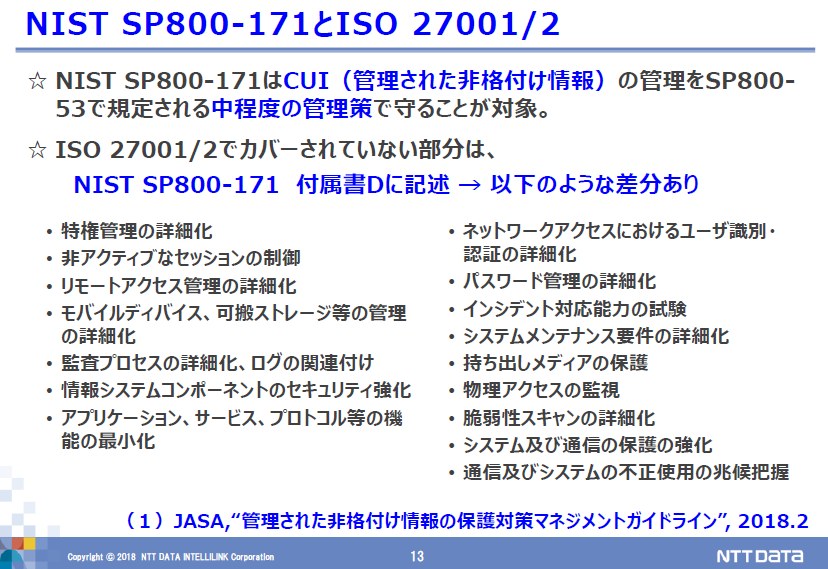
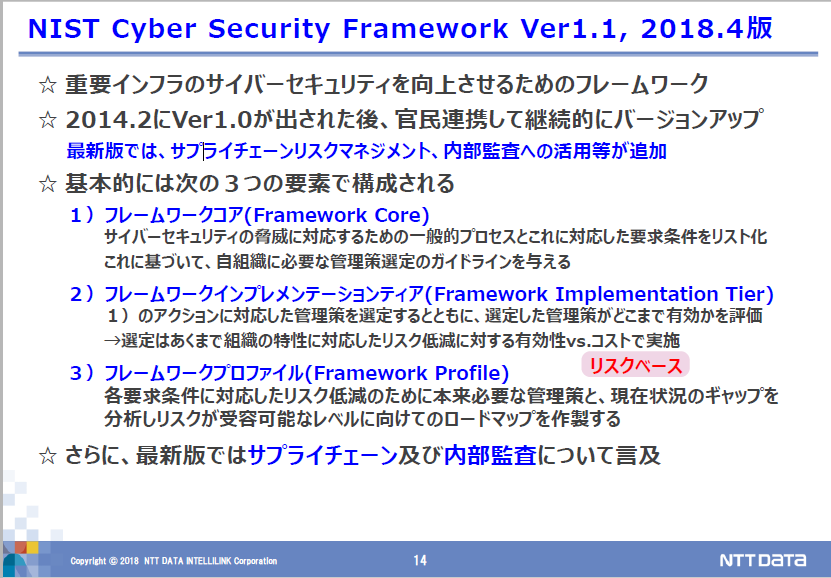
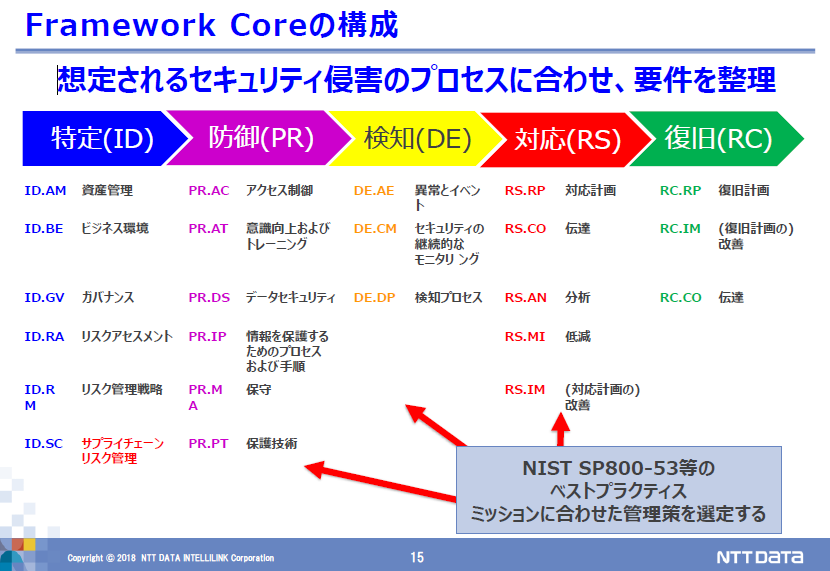
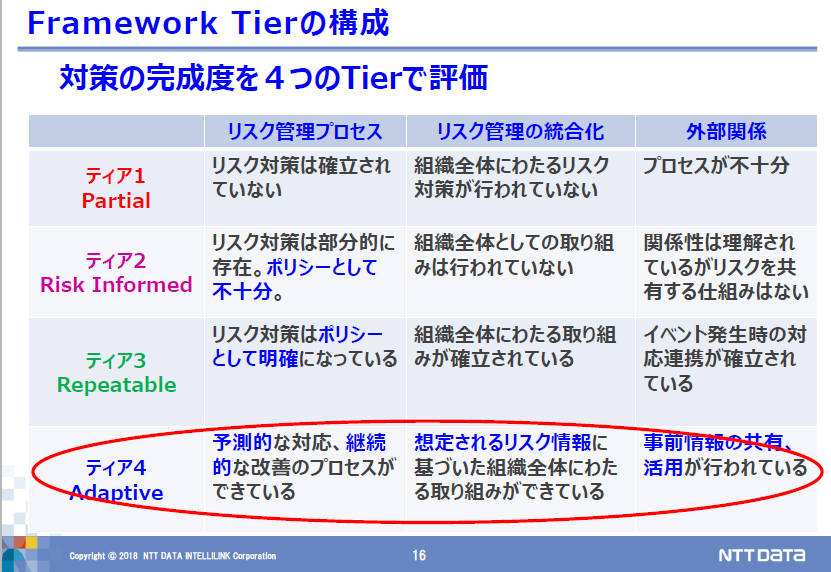
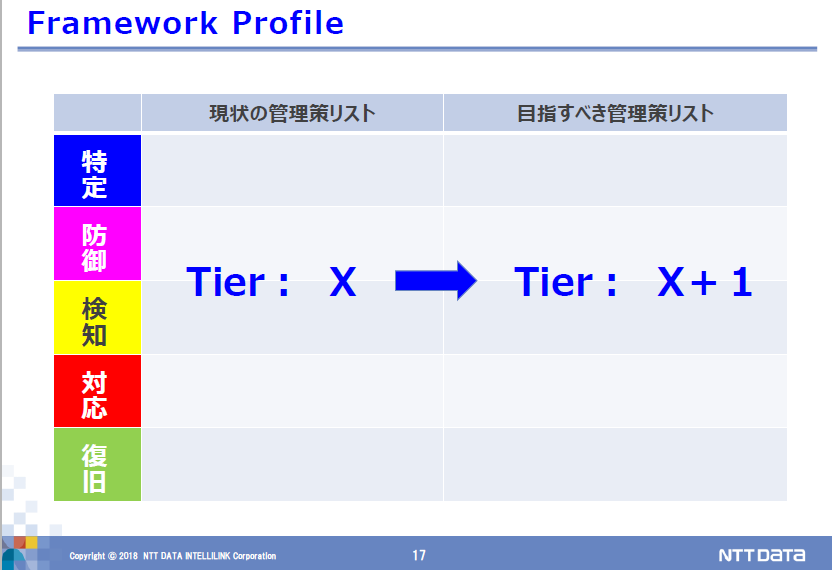
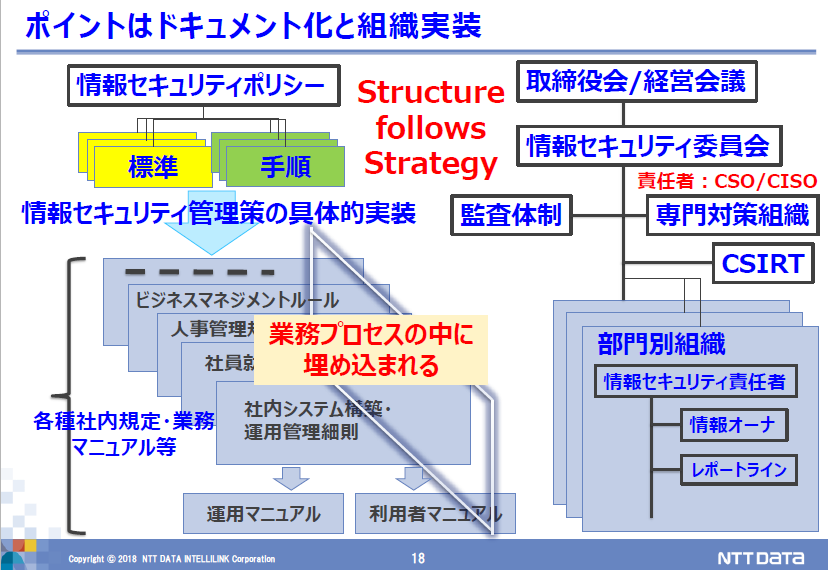
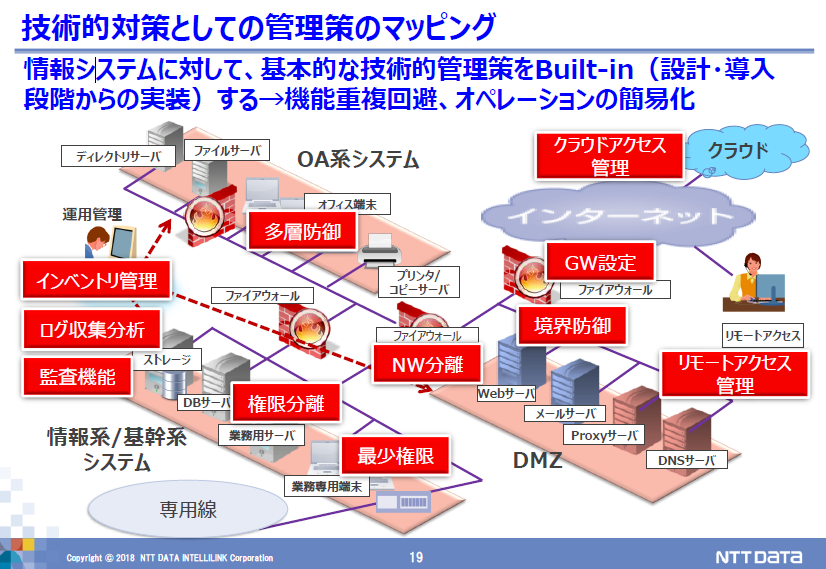
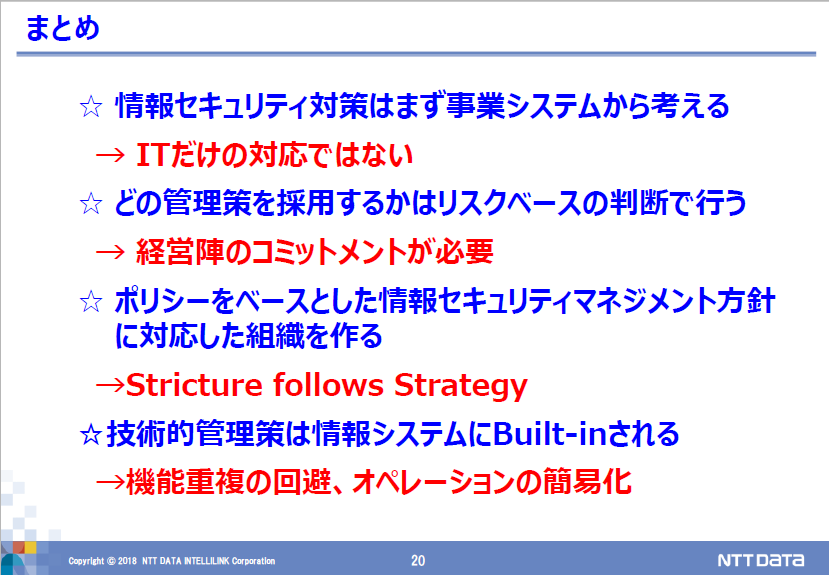
Sec01-03-05【スライド】経営リスク管理から考えるSecurity by Design

1. 2018年11月8日 NTTデータ先端技術株式会社 三宅功
2. タイトル
   1. Subtopic  
      
3. 経営リスク管理とSecurity by Design
   1. Subtopic  
      
   2. ☆ 経営リスク管理は経営陣の責務の１つコーポレートガバナンス・コード
      1. 【基本原則３】上場会社は、 会社の財政状態・経営成績等の財務情報や、 経営戦略・経営課題、 リスクやガバナンスに係る情報等の非財務情報について、 法令に基づく開示を適切に行うとともに、 法令に基づく開示以外の情報提供にも主体的に取り組むべきである。
      2. 【基本原則４】、 、 、 、 会社の持続的成長と中長期的な企業価値の向上を促し、 収益力・資本効率等の改善を図るべく、
         1. (2) 経営陣幹部による適切なリスクテイクを支える環境整備を行うこと
      3. ☆ 本日お伝えしたい“Security by Design”とは事業システムそのものへ情報セキュリティ対策を作りこむこと。 これによりAdd onでなくBuiltinによる企業の包括的・持続可能な情報セキュリティマネジメントを実現したい。
4. 経営陣に求められるサイバーリスク対応
   1. Subtopic  
      
   2. 1. Directors should understand and approach cybersecurity as anenterprise-wide risk management issues, not just an IT issue.
   3. 2. Directors should understand the legal implications of cyber riskas they relate to their company’s specific circumstances.
   4. 3. Boards should have adequate access to cybersecurity expertise,and discussion about cyber-risk management should be given regular and adequate time or board meeting agendas.
   5. 4. Directors should set the expectation that management willestablish an enterpise-wide cyber-risk management framework with adequate staffing and budget.
   6. 5. Board-management discussions about cyber-risk should include identification of which risks to avoid, which to accept, and whichto mitigate or transfer through insurance, as well as specific plans associated with each approach.“Cyber-Risk Oversight - Director’s Handbook Series”, NACD (National Association of Corporate Directors) 2017
5. 経営陣に求められるサイバーリスク対応
   1. Subtopic  
      
   2. 1. 経営陣はサイバーセキュリティ対策を、 ITに限定されたものではなく、 全社をあげてのリスク対策と認識し取り組む必要がある。
   3. 2. 経営陣は自社が置かれた環境に関連して、 サイバーリスクの法的意味を十分に理解しておく必要がある。
   4. 3. 経営陣は、 サイバーセキュリティの専門家に適宜アクセス可能であり、 サイバーセキュリティリスク管理に関する議論を定常的に適切なタイミングで実施する、 或いは取締役会の議題とすること。
   5. 4. 経営陣は、 適切な要員と予算配分の元での組織全体としてのサイバーリスク管理の枠組み（フレームワーク）を確立しておくことを求める必要がある。
   6. 5. サイバーリスクに関する経営陣内での議論は、 どのリスクが除かれ、 どのリスクが受容され、 どのリスクが軽減あるいは保険による転嫁がなされたか、 それぞれの事象に関する個別の計画に基づいて行われる必要がある。
   7. “Cyber-Risk Oversight - Director’s Handbook Series”, NACD(National Association of Corporate Directors) 2017
6. どうすれば良いのか？
   1. Subtopic  
      
   2. ☆ 大前提は、 あくまで個々の組織の特性に合わせた情報セキュリティ対策を実施すること。
   3. ☆ そのためには、
   4. ① 自組織の組織目的、 これに対応した組織構成とビジネスプロセス、 サポートシステム（ITシステムを含む）、 人材、 サプライチェーン、 物理施設等を棚卸し（事業システムの把握）
   5. ② これらの事業環境で扱われる重要情報（営業秘密、 個人情報等）を処理、 蓄積、 転送レベルで把握するとともに、 それが失われた場合の組織目的に対する影響度（リスク）を評価し
   6. ③ 重要情報及びこれを扱うシステムに対する費用対効果を考慮したリスク対策（管理策の適用）を行う⇒世の中のベストプラクティスを活用
   7. ☆ 標準化された情報セキュリティマネジメントシステム(ex. ISMS, NIST SP800等）は③実現のためのベストプラクティス・リストであり、 自組織が情報セキュリティリスク管理を実施していることを対外的に表明するためのツールでもある
7. リスク評価Step-1
   1. Subtopic  
      
   2. 事業システムを特定し、 情報資産・情報の流れを把握する
8. リスク評価Step-2 リスクの特定
   1. Subtopic  
      
   2. 特定された情報資産・情報が侵害された場合の影響度からその重要度を決定する。
9. セキュリティ管理策をどう決めて行くか
   1. Subtopic  
      
   2. ☆ リスクの特定結果から、 これを低減する管理策を費用対効果の観点で優先度付けして決める。
   3. ☆ 管理策は、 ①組織的・人的対策、 技術的対策、 物理的対策の視点、 ②マネジメント、 プロセス、 システムの階層的視点、 で考える。
   4. ISO 27001より
   5. NIST SP800-53より
10. セキュリティ管理策をどう回していくか？
    1. Subtopic  
       
    2. NIST Framework for Improving Critical Infrastructure Cybersecurity Ver1.1より
11. NIST SP800-53とCyber Security Frameworkについて
    1. Subtopic  
       
    2. FISMA(Federal Information Security Management 連邦政府情報セキュリティ近代化法)
    3. CEA 2014(Cybersecurity Enhancement Act of 2014)
    4. FIPS 199(連邦政府のセキュリティ分類規格)
    5. FIPS 200(最低限のセキュリティ要求事項（17項目の要求事項）)
    6. NIST SP800-53(セキュリティ管理策とプライバシー管理策)
    7. NIST SP800-171(連邦政府外のシステムと組織における管理された非格付け情報の保護)
12. NIST SP800-53 Re.4 管理策ファミリ
    1. Subtopic  
       
    2. ☆ISO 27001/2の管理策とかなり重複するが、 より詳細に規定
13. NIST SP800-53 Re.4 管理策の構造
    1. Subtopic  
       
14. NIST SP800-171とISO 27001/2
    1. Subtopic  
       
    2. ☆ NIST SP800-171はCUI（管理された非格付け情報）の管理をSP800-53で規定される中程度の管理策で守ることが対象。
    3. ☆ ISO 27001/2でカバーされていない部分は、 NIST SP800-171 付属書Dに記述→ 以下のような差分あり
    4. ・特権管理の詳細化
    5. ・非アクティブなセッションの制御
    6. ・リモートアクセス管理の詳細化
    7. ・モバイルディバイス、 可搬ストレージ等の管理の詳細化
    8. ・監査プロセスの詳細化、 ログの関連付け
    9. ・情報システムコンポーネントのセキュリティ強化
    10. ・アプリケーション、 サービス、 プロトコル等の機能の最小化
    11. ・ネットワークアクセスにおけるユーザ識別・認証の詳細化
    12. ・パスワード管理の詳細化
    13. ・インシデント対応能力の試験
    14. ・システムメンテナンス要件の詳細化
    15. ・持ち出しメディアの保護
    16. ・物理アクセスの監視
    17. ・脆弱性スキャンの詳細化
    18. ・システム及び通信の保護の強化
    19. ・通信及びシステムの不正使用の兆候把握
15. NIST Cyber Security Framework Ver1.1, 2018.4版
    1. Subtopic  
       
    2. ☆ 重要インフラのサイバーセキュリティを向上させるためのフレームワーク
    3. ☆ 2014.2にVer1.0が出された後、 官民連携して継続的にバージョンアップ
       1. 最新版では、 サプライチェーンリスクマネジメント、 内部監査への活用等が追加
    4. ☆ 基本的には次の３つの要素で構成される
       1. １）フレームワークコア(Framework Core)
          1. サイバーセキュリティの脅威に対応するための一般的プロセスとこれに対応した要求条件をリスト化
          2. これに基づいて、 自組織に必要な管理策選定のガイドラインを与える
       2. ２）フレームワークインプレメンテーションティア(Framework Implementation Tier)
          1. １）のアクションに対応した管理策を選定するとともに、 選定した管理策がどこまで有効かを評価
          2. →選定はあくまで組織の特性に対応したリスク低減に対する有効性vs.コストで実施
       3. ３）フレームワークプロファイル(Framework Profile)
          1. 各要求条件に対応したリスク低減のために本来必要な管理策と、 現在状況のギャップを分析しリスクが受容可能なレベルに向けてのロードマップを作製する
    5. ☆ さらに、 最新版ではサプライチェーン及び内部監査について言及
16. Framework Coreの構成
    1. Subtopic  
       
    2. 想定されるセキュリティ侵害のプロセスに合わせ、 要件を整理
    3. 特定(ID)
    4. 防御(PR)
    5. 検知(DE)
    6. 対応(RS)
    7. 復旧(RC)
17. Framework Tierの構成
    1. Subtopic  
       
    2. 対策の完成度を４つのTierで評価
18. Framework Profile
    1. Subtopic  
       
19. ポイントはドキュメント化と組織実装
    1. Subtopic  
       
20. 技術的対策としての管理策のマッピング
    1. Subtopic  
       
    2. 情報システムに対して、 基本的な技術的管理策をBuilt-in（設計・導入段階からの実装）する→機能重複回避、 オペレーションの簡易化
21. まとめ
    1. Subtopic  
       
    2. ☆ 情報セキュリティ対策はまず事業システムから考える
       1. → ITだけの対応ではない
    3. ☆ どの管理策を採用するかはリスクベースの判断で行う
       1. → 経営陣のコミットメントが必要
    4. ☆ ポリシーをベースとした情報セキュリティマネジメント方針に対応した組織を作る
       1. →Stricture follows Strategy
    5. ☆技術的管理策は情報システムにBuilt-inされる
       1. →機能重複の回避、 オペレーションの簡易化