サイバーセキュリティの概念
－ 国際標準化の動向を背景に －

2018年12月

国立研究開発法人　情報通信研究機構 (NICT)
山下　真
ISO/IEC JTC1 SC27 WG1, WG4 国際エキスパート

目次

- **はじめに**
- サイバーセキュリティのさまざまな定義
- インシデントと原因・結果の連鎖
- 情報セキュリティとサイバーセキュリティ
- サイバーセキュリティの類型
- サイバーセキュリティに関連するISMSの役割
- サイバーセキュリティに関連する JTC 1/SC 27の国際標準
- まとめ

セキュリティ事案の状況

- SNSやウェブサービスからの個人情報漏洩、最大8700万人分（2018.10）
- 仮想通貨流出、数百億円相当（2018.1, 2018.9）
  - 取引所における管理の課題
- IoT機器を踏台にするDoS攻撃
  - 広範なIoT機器に脆弱性
- カード偽造、カード情報売買
- ランサムウェア　WannaCry（2017.5）

参考資料：

『JNSA 2017 セキュリティ十大ニュース』　JNSA

『情報セキュリティ 十大脅威 2018』　情報処理推進機構 (IPA)

国際標準化における悩み

- ISO/IEC JTC 1/SC 27 において、情報セキュリティマネジメント分野にISO/IEC 27000ファミリーを整備してきた。
- その間に「サイバーセキュリティ」が浸透。
- 両者の共通性や相違についての説明は未整備。
  - リスクマネジメントの考え方やISO/IEC 27002の管理策は、どちらにも有効に思われるが。
- 「サイバーセキュリティ」の意味が2010年頃から流動し、共通した理解の定着も今後。

2016年にサイバーセキュリティに関する標準化の事前検討に着手：検討期間(Study Period)を設置

目次

- はじめに
- **サイバーセキュリティのさまざまな定義**
- インシデントと原因・結果の連鎖
- サイバーセキュリティの類型
- 情報セキュリティとサイバーセキュリティ
- サイバーセキュリティに関連するISMSの役割
- サイバーセキュリティに関連する
  JTC 1/SC 27の国際標準
- まとめ

サイバーセキュリティの定義

- 定義の例として以下を取り上げる。

  - 日本
    サイバーセキュリティ基本法における定義

  - 米国 NIST
    Cybersecurity Framework における定義

  - 国際標準（例）
    SC 27において検討中の定義

サイバーセキュリティ基本法における定義

1. 出典：サイバーセキュリティ基本法（平成二十六年法律第百四号）
   第二条

2. 定義
   この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。）が講じられ、その状態が適切に維持管理されていることをいう。

サイバーセキュリティ基本法における定義

- 定義を読みやすく箇条書きに変えると・・・

この法律において「サイバーセキュリティ」とは、

a. 電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され伝送され若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該**情報の安全管理のために必要な措置**

並びに

b. **情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置**

(情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体(以下「電磁的記録媒体」という。)を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む。)

が講じられ、その状態が適切に維持管理されていることをいう。

サイバーセキュリティ基本法における定義

3. 定義の特徴

i. 「措置」

a. 「情報の安全管理のために必要な」措置：
言葉は違うが、情報セキュリティと同じ。

b. 「情報システム及び情報通信ネットワークの**安全性及び信頼性の確保**のために必要な」措置
情報セキュリティとは別の要件を含む。

ii. インターネットやネットワークは必須の前提にしていない。電磁的記録媒体での情報の抜出しも対象。

iii. 原因を意図的な攻撃に限定していない。

米国 NIST Cybersecurity Framework における定義

1. 出典：Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, National Institute of Standards and Technology, April 16, 2018
   https://www.nist.gov/cyberframework/framework
2. Cybersecurityの定義
   The process of protecting information by preventing, detecting, and responding to attacks.
   攻撃を防止し、検知し、対応することによって情報を守るプロセス
3. 定義の特徴
   a. 「プロセス」
   b. 定義の基本的な要素は、「情報を守る」「攻撃から守る」
   c. 重要インフラを対象とする文書であるが、定義では重要インフラには触れていない。
   d. 前提としてインターネットやネットワークを明示していない。

SC 27 において検討中の定義

1. 出典：ISO/IEC TS 27100, Information technology – Cybersecurity – Overview and concepts のドラフト
2. cybersecurity の定義 [検討中]
   safeguarding of society, people, organization and nation from digital risks
   デジタルリスクから社会、人々、組織及び国を守ること
3. 定義の特徴
   a. 情報に言及していない。
   b. “digital platform”, “digital age” 等に感じられる “digital” な環境の危うさを意識。
   c. デジタルリスクが顕在化するとき、その原因が情報の機密性・完全性・可用性の棄損以外にある場合も除外しない。機器の品質問題や人の誤操作も視野に入れている。

対照： 情報セキュリティの定義

1. 出典：ISO/IEC 27000, Information technology – Security techniques – Information security management systems – Overview and vocabulary
2. Information security の定義
   preservation of confidentiality, integrity and availability of information
   情報の機密性、完全性及び可用性を維持すること
3. 定義の特徴
   a. 情報の管理における要件だけに言及している。情報に着目。
   b. 汎用の定義であり、以下の要素はこの語を使う文書や文脈で補われる場合がある。
      ✓適用場面の特定、例えば組織、国など。
      ✓機密性、完全性又は可用性が損われた場合のシナリオと結果の想定
   c. したがって、安全や品質とのつながりは定義からは見えない。

定義の比較

	サイバーセキュリティ基本法	米国　NIST Cybersecurity Framework	SC 27 において検討中の定義
守るものは情報か？	△ 情報システム等も	○	ー　社会、人、組織、国
情報セキュリティとの関係は	情報セキュリティより広い（除紙媒体）	情報セキュリティの一部	情報セキュリティとは視点が異なる
場面はネットワークが必須の前提か？	× より広い。 記録媒体での情報抜出しも対象	?	× より広い。 ネットワークに限定しない
原因は意図的な攻撃が前提か？	× 誤りや故障による例も対象。	○	× 誤りや故障による例も対象
安全の側面があるか？	○	△ 明示なし。	○

補足：　定義を読むときに注意すべきこと

- 定義では、意図した内容の一部を明記していない可能性がある。
  - 執筆者には自明のことが省かれている可能性
    - 例：インターネット環境を前提とすること、あるいは重要な要件とすることは、自明であるのかもしれない
  - 意味の限定を文脈に任せて、広く定義する可能性
    - 例：文書は重要インフラが前提、定義は汎用

目次

- はじめに
- サイバーセキュリティのさまざまな定義
- **インシデントと原因・結果の連鎖**
- サイバーセキュリティの類型
- 情報セキュリティとサイバーセキュリティ
- サイバーセキュリティに関連するISMSの役割
- サイバーセキュリティに関連する
  JTC 1/SC 27の国際標準
- まとめ

異なるサイバーセキュリティを理解する鍵

- サイバーセキュリティの理解やイメージは、場面や立場によって異なり、一つではない。このことは、今後も変わらない。

- 話題にしているサイバーセキュリティが何であるかを理解する鍵を、**インシデントの捉え方**に求めてはどうか。これは様々な**リスクシナリオ**を認識することにつながる。

- **リスクシナリオと重視するリスクを知ること**が、それぞれのサイバーセキュリティの理解に繋がるのではないか。

インシデントの見方

- **インシデント（情報セキュリティインシデント）とは、一連の事象と結果を連鎖として把握したシナリオ**
  - ISO/IEC 27000:2018 における情報セキュリティインシデント定義では、「単独若しくは一連の情報セキュリティ事象」であることを要件としている。

インシデントはリスクシナリオに密接に関係

リスクアセスメントにおける
リスクシナリオの網羅的な記述

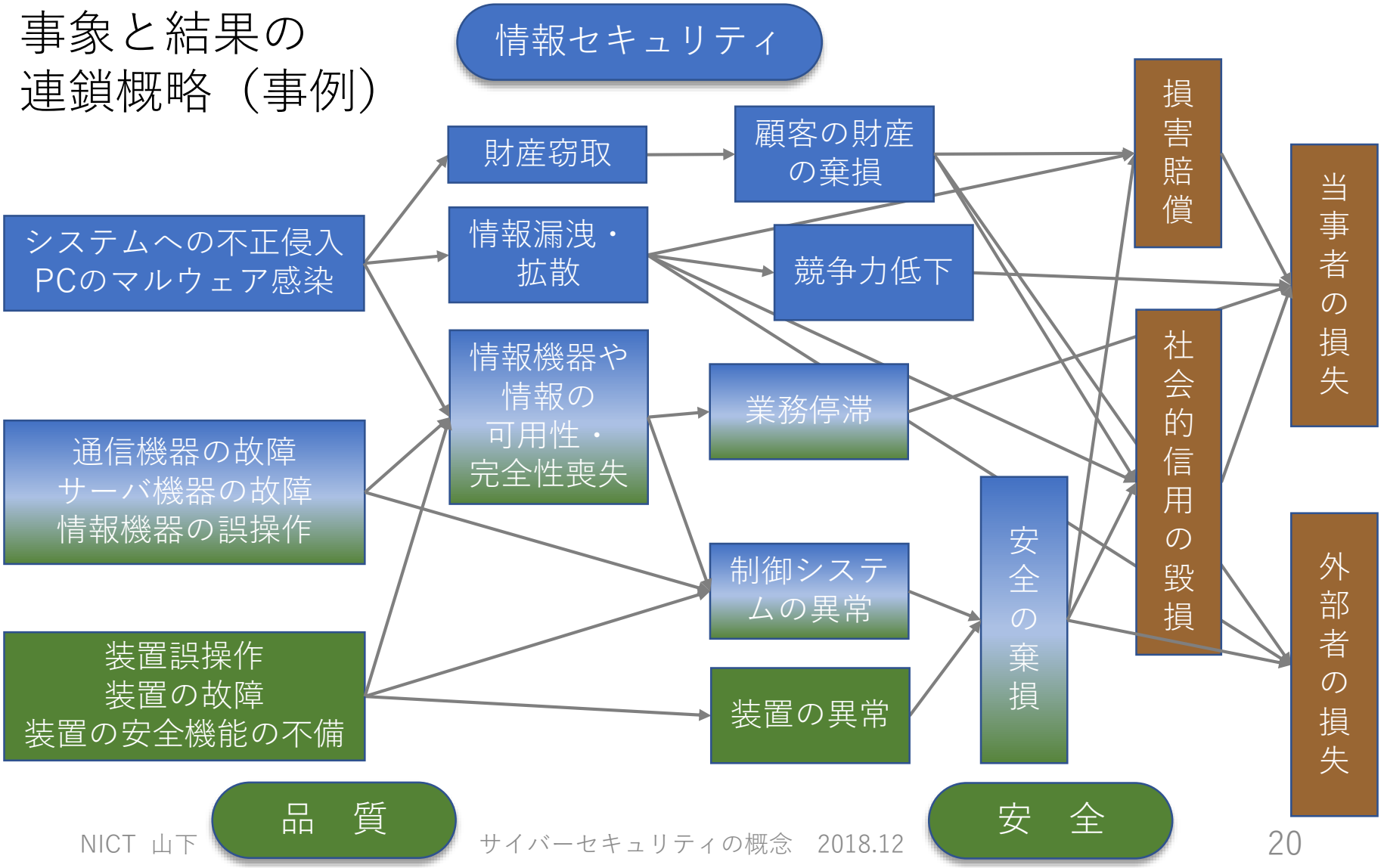
≒　起こりうる様々なインシデント
の描写

ISO/IEC 27001:2013 より　事象・結果への言及

- 情報セキュリティリスクアセスメントの要求事項 [6.1.2]から
  - リスクの特定：
    情報の機密性、完全性及び可用性の喪失に伴う情報セキュリティリスクを特定する[c) 1)]。
  - リスクの分析：
    特定した情報セキュリティリスクについて、**事象が発生した場合に起こりうる結果を想定する**[d) 1)]。

さまざまなインシデントを想定する

事象と結果の
連鎖概略（事例）



原因・結果の連鎖から読み取れること

1. **インシデントの記述やリスクシナリオは、情報セキュリティの中で完結しない。**
   - 社会的な結果や事業上の結果を起点にして連鎖を遡ると、原因は情報セキュリティに閉じない。
   - 賠償や信用毀損という結果は、組織活動の中で、情報セキュリティを越えた枠組みで扱われる。

2. **サイバーセキュリティにおいては、**
   - **原因・結果の連鎖と、結果の重大性を強く意識し、**
   - **「安全」を目標に含める傾向があるのではないか。**

安全 (safety) とは

- ISO/IEC Guide 51:2014, Safety aspects — Guidelines for their inclusion in standards (JIS Z 8051 安全側面 ー 規格への導入指針) において 用語 safety を定義している。その主旨は、次のとおり。

> 対象： ① 人の傷害　② 人の健康障害
> ③ 財産の損害　④ 環境の棄損
> これらの対象について、発生確率と程度の組合せが許容できる状態にあること。

- 詳しくは上記文書を参照。
  - ISOのウェブサイト
    https://www.iso.org/store.html
    から文書を検索し、用語定義を参照することができる。

目次

- はじめに
- サイバーセキュリティのさまざまな定義
- インシデントと原因・結果の連鎖
- **情報セキュリティとサイバーセキュリティ**
- サイバーセキュリティの類型
- サイバーセキュリティに関連するISMSの役割
- サイバーセキュリティに関連する
  JTC 1/SC 27の国際標準
- まとめ

情報セキュリティとサイバーセキュリティの対比

	情報セキュリティ	サイバーセキュリティ
当事者・立場	1) 情報セキュリティ(CIAを維持すること)：**多様なエンティティ**に個別に適用可能。 2) 情報セキュリティマネジメント：　**組織**の活動。	**多くのエンティティ。** 国、重要インフラ、産業、個人。 **管理責任の所在が明確にしにくい場面もある。**
インシデントの原因	意図した攻撃に限定しない。	1) **意図した攻撃への対処とする例がある。** 2) 誤りや機器等の不具合も除外しない例もある。
目標	**情報に価値があり、これを保護する。** 特に、**機密性の維持**が重要な例が多い。	自身及び他者の**損失防止と安全。** 情報の機密性のほか、**完全性と可用性の維持**を重要な要件とする例が多い。

目次

- はじめに
- サイバーセキュリティのさまざまな定義
- インシデントと原因・結果の連鎖
- 情報セキュリティとサイバーセキュリティ
- **サイバーセキュリティの類型**
- サイバーセキュリティに関連するISMSの役割
- サイバーセキュリティに関連する JTC 1/SC 27の国際標準
- まとめ

特定の「サイバーセキュリティ」について位置づけを知るためのチェックポイント

定義、インシデント／リスクシナリオの検討及び情報セキュリティとの対比から、サイバーセキュリティの概念を理解するための要素として、

1. 当事者・立場

- 国の行政、重要インフラ、産業活動、ネットワーク事業者、個人
- 管理責任を特定のエンティティに求めにくい場面もある

2. 目標

- サイバー空間における攻撃への対処
- 重要インフラの安定稼働
- 産業活動の維持・安全
- 多くのエンティティが関係するサイバー空間におけるエンティティの安全・保護

立場によって異なる関心や目標

- **ネットワーク事業者**：安全なネットワークインフラやネットワークサービスの提供
- **重要インフラ**：社会活動や生活の基礎となる仕組みの維持
- **産業分野**：産業IoT、サプライチェーン、サイバーフィジカルシステムの安全
- **個人**：IoT機器利用におけるセキュリティ

立場や場面によってそれぞれの関心、理解やサイバーリスクシナリオが存在

サイバーセキュリティの典型的な類型

類型Ⅰ：サイバー空間における攻撃への対処

- インターネットの基盤・サービスの保全
- この語の初期から存在した意味

類型Ⅱ：産業分野のサイバーセキュリティ

- 重要インフラの維持・保全
- サイバーフィジカルセキュリティ

類型Ⅲ：個人の生活におけるIoTセキュリティ

- IoT端末の普及における管理の課題への取組み

類型Ⅳ：デジタルリスクへの対応としてのサイバーセキュリティ

- 国・社会の仕組みや人の生活の基礎にICTが遍在する状況における安全確保

「サイバーセキュリティ」の意味

「サイバーセキュリティ」という語は、一つの類型をイメージして使われたり、その中のある場面を前提に使われたりしている。

また、これらの類型の全体を指す言葉でもある。

目次

- はじめに
- サイバーセキュリティのさまざまな定義
- インシデントと原因・結果の連鎖
- 情報セキュリティとサイバーセキュリティ
- サイバーセキュリティの類型
- **サイバーセキュリティに関連するISMSの役割**
- サイバーセキュリティに関連する JTC 1/SC 27の国際標準
- まとめ

サイバーセキュリティに関連するISMSの役割

組織の活動であるISMSは、サイバーセキュリティに関連して次の役割がある。

1. 組織の情報セキュリティマネジメント

2. 重要インフラの維持に貢献するISMS

3. エコシステムの安全に関わるISMS

1. 組織の情報セキュリティマネジメント

- 場面・関心 ＝ 組織
- **サイバー空間の中にあってサイバーセキュリティの課題に対応する組織の情報セキュリティマネジメントにISMSを採用する。**
  - 関心の対象は、組織自身の情報と預り情報：ISMSの基本形
    - ISO/IEC 27001:2013, 6.1.2 c) 1) において、情報セキュリティリスクアセスメントの目的について規定：「ISMSの適用範囲内における情報の機密性、完全性及び可用性の喪失に伴うリスクを特定するために」

2. 重要インフラの維持に貢献するISMS

- 場面・関心 ＝ 国の重要インフラ
- **重要インフラを担うICTの安定稼働を維持する活動にISMSを活用する。**
- 安定稼働と安全を目的として、情報及びICTについて完全性・可用性を維持する。
  - 関心の対象： 国、社会、経済、生活、命・健康、財産
- 関係する標準（例）
  - ISO/IEC 27019:2017, Information technology – Security techniques – Information security controls for the energy utility industry

3. エコシステムの安全に関わるISMS

- 場面・関心
  ＝ サイバー空間に共存する多くの組織や人

- **サイバー空間上で自身と他者の利益を守る。**
  サイバー空間の安全に対して役割を持つ。
  - ISMSの適用においては、外部者への影響も重視する。
    1. 組織の目的 (ISO/IEC 27001:2013, 4.1) や利害関係者 (4.2) を広い視点で設定する。
    2. 「ISMSの適用範囲内における情報の機密性、完全性及び可用性の喪失に伴うリスクを特定するために」(6.1.2 c) 1)) という限定的な要求事項に縛られることなく、組織が自ら設定する目的に外部者の利益も含める。

目次

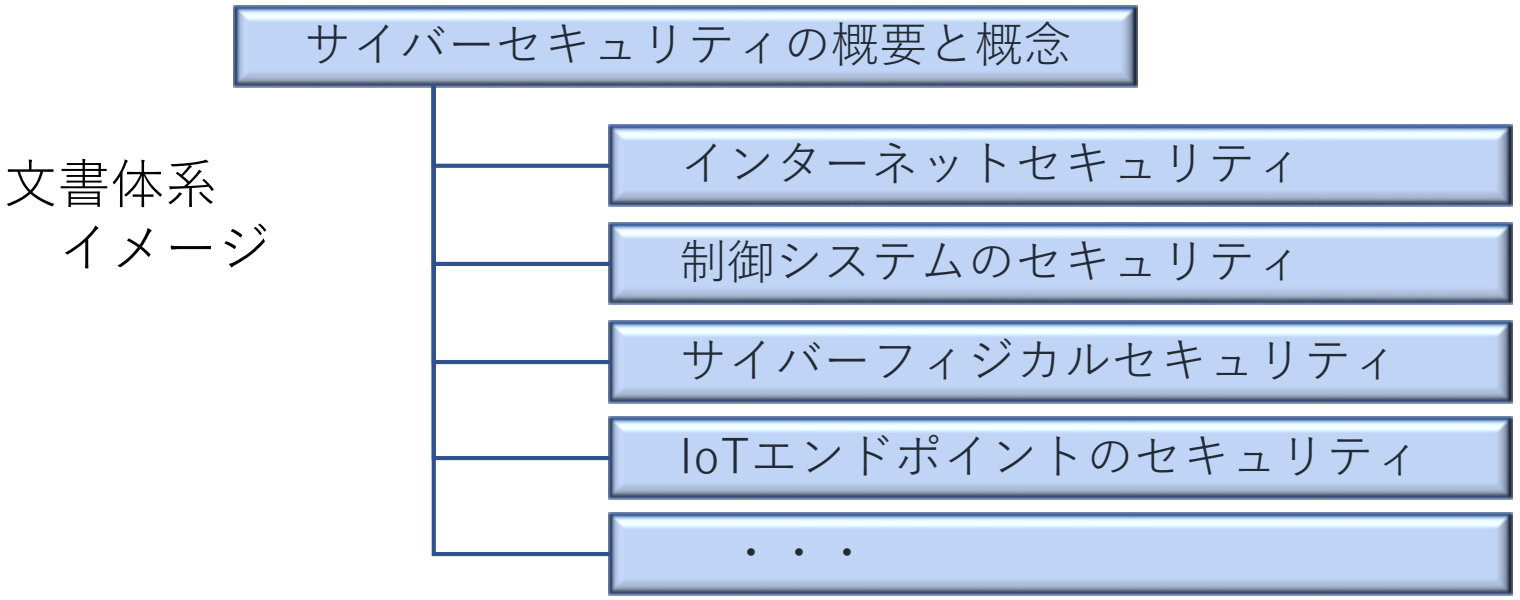
- はじめに
- サイバーセキュリティのさまざまな定義
- インシデントと原因・結果の連鎖
- 情報セキュリティとサイバーセキュリティ
- サイバーセキュリティの類型
- サイバーセキュリティに関連するISMSの役割
- **サイバーセキュリティに関連する JTC 1/SC 27の国際標準**
- まとめ

サイバーセキュリティに関連する国際標準等

国際標準等	内容	現状
ISO/IEC TS 27100	サイバーセキュリティの概要、概念、用語定義	開発中
ISO/IEC TS 27101	サイバーセキュリティフレームワーク策定のための指針	開発中
ISO/IEC 27102	サイバー保険の指針	開発中
ISO/IEC TR 27103:2018	サイバーセキュリティフレームワークとISO/IEC文書等の対応	出版済
ISO/IEC 27030	IoTにおけるセキュリティ及びプライバシーの指針	開発中
ISO/IEC 27032	サイバーセキュリティにおけるインターネットセキュリティ	改定に着手
ISO/IEC 27019:2017	エネルギー産業における制御システムセキュリティの指針	出版済

国際標準化活動が目指すもの

- 国際標準化活動においては、サイバーセキュリティについてさまざまな見方が存在することを認識し、このことを反映した文書群を整備していくことが想定される。



- この活動は、国際標準の目的である概念や指針の国際的な共有に貢献するものにしたい。

目次

- はじめに
- サイバーセキュリティのさまざまな定義
- インシデントと原因・結果の連鎖
- 情報セキュリティとサイバーセキュリティ
- サイバーセキュリティの類型
- サイバーセキュリティに関連するISMSの役割
- サイバーセキュリティに関連する JTC 1/SC 27の国際標準
- **まとめ**

サイバーセキュリティの概念　まとめ

1. **サイバーセキュリティの当初からの意味は「サイバー空間において攻撃に対処する活動」であると思われるが、異なる意味でも使われ、それぞれのサイバーセキュリティがある。**

2. **情報セキュリティと対比して、インシデントの結果に強い関心がある例が多い。リスクシナリオの下流に注目する傾向がある。**

3. **リスクシナリオは情報セキュリティに閉じるものではなく、品質や安全にも関係する。**

サイバーセキュリティの概念　まとめ

4. **組織を越えて他者に影響が及ぶ状況 －エコシステム－ の視点を持つこともある。**

5. **組織のISMSは、サイバーセキュリティとの関わりにおいてもその役割がある。**

6. **サイバーセキュリティの概念の展開は、リスクマネジメントのカテゴリを今一度整理する契機にもなるかもしれない。**

   参考：　この観点の検討に、例えば trustworthiness (security, privacy, safety, reliability, resilience) の概念の検討がある。

サイバーセキュリティの概念
－ 国際標準化の動向を背景に －

2018年12月

国立研究開発法人　情報通信研究機構 (NICT)
山下　真
ISO/IEC JTC1 SC27 WG1, WG4 国際エキスパート