サイバーセキュリティにおける ISMSの役割

2020年12月18日

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 エキスパート

講演骨子

1. ISMS に関わる人や組織にとって、サイバーセキュリティは重要な関心事であると共に、関わりについて整理することも必要であると感じられるのではないか。
2. サイバーセキュリティの概要・概念について SC 27 の視点でまとめた文書である ISO/IEC TS 27100 が、ISMS との関係を考えるためにも参考になる。
3. ISMSが組織の視点に基づく情報セキュリティマネジメントの仕組みであるのに対し、サイバーセキュリティの基礎にはサイバー空間を場とするリスクの特定と対応という視点がある。
4. 組織は、サイバー空間にあって、ISMSの基本的な仕組みである外部の状況と利害関係者の認識を通してサイバーセキュリティに対処し、貢献する。

目　次

1. サイバーセキュリティの概念
　　― ISO/IEC TS 27100 を参考にして　―

2. サイバーセキュリティの現場と
　　サイバーリスクの類型

3. ISMSの基本的な関心

4. サイバーセキュリティにおけるISMSの役割

国際標準化組織

JTC 1: 情報技術 (Information technology)

SC 27: 情報セキュリティ、サイバーセキュリティ
及びプライバシー保護

WG 1: 情報セキュリティマネジメントシステム

WG 4: セキュリティ・コントロールと
セキュリティ・サービス

サイバーセキュリティ関連規格群　一般 (1/2)

文書番号	内容	備考
ISO/IEC TS 27100	サイバーセキュリティの概要及び概念	近く出版予定
ISO/IEC 27102:2019	情報セキュリティリスクマネジメントにおけるサイバー保険活用の説明	
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 27001、ISO/IEC 27002 その他の文書との対応関係	

TS: Technical Specification, 技術仕様書
TR: Technical Report, 技術報告書
*　Framework for Improving Critical Infrastructure Cybersecurity, NIST, 2018

サイバーセキュリティ関連規格群　一般 (2/2)

文書番号	内容	備考
PWI (ISO/IEC TR 27109 予定)	サイバーセキュリティの教育・訓練	プロジェクト開始前検討中
ISO/IEC 27110	サイバーセキュリティ・フレームワーク策定指針*（規格開発者向け）	近く出版予定
PWI 5689	サイバー・フィジカル・システムの概要と参照アーキテクチャ **	プロジェクト開始前検討中

* Framework for Improving Critical Infrastructure Cybersecurity, NIST, 2018 の内容と整合性がある。
** 「サイバー・フィジカル・セキュリティ対策フレームワーク Version 1.0」（経済産業省、2019年4月）を基礎に日本から提案したプロジェクト。

サイバーセキュリティ関連規格群　IoT関連

文書番号	内容	備考
ISO/IEC 27400	IoTにおけるセキュリティ及びプライバシーに関する指針* Cybersecurity – IoT security and privacy – Guidelines	作成中
ISO/IEC 27402	IoT機器のセキュリティ対策基本要求事項 Cybersecurity – IoT Security and Privacy–Device baseline requirements	作成中
ISO/IEC 27403	居住環境におけるIoTセキュリティ・プライバシーの指針 Cybersecurity – IoT security and privacy – Guidelines for IoT–domotics	作成中

* 「IoT セキュリティガイドライン ver 1.0」（IoT 推進コンソーシアム/総務省/経済産業省、2016年7月）の内容を日本から提案し、この文書のセキュリティ管理策に反映されている。

ISO/IEC TS 27100 策定の経過

時期	検討テーマ	進捗・結論
2017/ 4～9	サイバーセキュリティ全般	二つの文書を作ることを決定 ISO/IEC TS 27100 ISO/IEC TS 27101（その後　27110に番号を変更）
2017/10 ～2018/3	ISO/IEC TS 27100	プロジェクト開始前の検討期間
2018/ 4～10		新規作業項目提案（NWIP）作成とその投票
2019/2		作業原案（Working Draft）から検討開始
2021/1 ?		出版

ISO/IEC TS 27100 の特徴　1/3

ISO/IEC TS 27100,
Information security, cybersecurity and privacy protection – Cybersecurity – Overview and concepts

1. ISO/IEC JTC 1/SC 27 で策定するサイバーセキュリティ関連文書群の基礎となる文書
   - 「サイバーセキュリティ ― 概要及び概念」

2. サイバーセキュリティについての説明書
   - 要求事項や指針・手引を規定するものではない。

ISO/IEC TS 27100 の特徴　2/3

3. サイバーセキュリティという語について、組織の目的や活動分野に応じた理解があること想定している。
   - 以下のICT活用場面ごとに、サイバーセキュリティの脅威とエンティティの役割を概説（8章）
     - 組織一般
     - 産業分野の自動化システム、制御システム
     - 製品・サービスの供給者関係
     - 通信サービス/ISP
     - 公的機関
     - 重要インフラ
     - 個人

ISO/IEC TS 27100 の特徴　3/3

4. ISMS関連規格を担当する SC 27/WG 1 の視点で、サイバーセキュリティとの関係に触れている。

- 組織マネジメントの視点から概念整理
  - 技術の解説は他の文書に譲る。
- SC 27 の文書に必須の話題として、情報セキュリティとサイバーセキュリティの関係、ISMSとサイバーセキュリティの関係を説明

サイバーセキュリティとは　－用語定義－

- ISO/IEC TS 27100 におけるサイバーセキュリティの定義：

  人々、社会、組織及び国をサイバーリスクから守ること

  「守ること」・・・ safeguarding

- 情報セキュリティの定義（ISO/IEC 27000 より）：

  情報の機密性、完全性及び可用性を維持すること

  「維持すること」・・・ preservation

視点、関心の違いが際立っている。

サイバーセキュリティの定義について（1/2）

1. 情報セキュリティとの関係

- 関心の対象は
  サイバー空間に置かれたエンティティの状態で
  あり、情報の状態ではない。

- サイバーセキュリティが損なわれる事態に対して
  情報の機密性、完全性、可用性の毀損が
  - 多くの場合に原因の一部として関係するが、
  - 原因として常に意識されるわけではない。

サイバーセキュリティの定義について（2/2）

2. サイバーリスクとは

- この語は ISO/IEC TS 27100 では無定義だが、サイバー空間におけるリスクを示唆
  - 「リスク」の定義は ISO/IEC 27000 のものを採用：
    目的に対する不確かさの影響
    - 目的を持つ主体は、
      サイバー空間に置かれたエンティティである人、
      社会、組織及び国
    - 目的はさまざま：
      安全、経済活動・生産活動・社会活動の維持、財産や経済的利益の保全、プライバシー保護、・・・
      - 目的の多様性が、サイバーセキュリティの理解がさまざまであることに関係

サイバー空間の要素

- 一般に、サイバー空間の意味について理解はさまざま:
  - 物理的なものか/通信の場として認識するネットワークか
  - 人や組織を含むか否か
  - 人や組織の活動を含むか否か
  - 情報を含むか否か　・・・
- ISO/IEC TS 27100 におけるサイバー空間の要素

分類	サイバー空間の構成要素
物理的要素	ネットワーク、システム
人的要素	人、組織
活動	プロセス、サービス
情報	以上の構成要素を媒体として存在し、流通する情報

目　次

1. サイバーセキュリティの概念
　　― ISO/IEC TS 27100 を参考にして　―

2. サイバーセキュリティの現場と
　　サイバーリスクの類型

3. ISMSの基本的な関心

4. サイバーセキュリティにおけるISMSの役割

サイバーセキュリティの現場

サイバーセキュリティの多様な場面から、典型的な現場と関心を取り上げると・・・

― ICT活用場面（スライド8、ISO/IEC TS 27100）を参考に ―

（1） 組織におけるICT活用

事業継続、社員・職員の安全、情報の保護、・・・

（2） 重要インフラを担う事業における安全・継続

電力、ガス、医療、流通など重要インフラの稼働確保、社会機能の安定供給、・・・

（3） 製品・サービスの供給者関係

供給者の責任、サプライチェーン・リスク、・・・

（4） 個人

プライバシー保護、財産の保全、・・・

それぞれのサイバーリスクの型を以降に整理

サイバーセキュリティの外部性

- どの場面においても、サイバー空間に置かれた組織や個人が相互に影響しあう側面がある。
  1. 脅威/リスク源に、他者の存在が関係する。
  2. 組織や個人の活動が他者に影響を与える。

- 生態系の用語にならって、この状況を「エコシステム」として記述する例もある。
  - IoTにおけるセキュリティ/プライバシーの文書である ISO/IEC 27400 (CD) に用例がある。
  - サイバーセキュリティにおける用法では、系の恒常性維持についての意識は希薄か。

リスクの例 （1）組織におけるICT活用

組織にとって

- 組織の機器に脆弱性があり、攻撃の踏台に悪用される。
- 受信した偽装メールを契機にウイルスに感染する。

外部者にとって

- 組織の機器が踏台になり、外部者がサイバー攻撃を受ける。
- 組織から漏洩したメールで偽装メールが作られて、外部者に送られる。

リスクの例 （2）重要インフラ

組織にとって

- ネットワークを通して制御システムがサイバー攻撃を受ける。
- 制御システムの構成機器に故障が起こる。
  - 自動化・制御のための情報*が損なわれる。

  ＊センサーから得た情報、アクチュエータに指示する情報
  - 自動化・制御のための情報の伝達が阻害される。
  - 自動化・制御システムの正常な運転が損なわれる。
- 重要インフラ機能の稼働が損なわれる。

外部者にとって

- 重要インフラに依存する国民の安全が損なわれる。

リスクの例　(3)製品・サービスの供給者関係

供給者にとって

- 供給する製品・サービスに脆弱性、品質不良や不具合が存在する。

調達者にとって

- 調達した製品・サービスの脆弱性、品質不良や不具合のために
  - 情報のCIAが損なわれる。
  - 情報システムの稼働が損なわれる。
  - 金銭的損害を被る。

外部者にとって

- 製品・サービスを利用する国や社会の利益が損なわれる。

リスクの例 （4）個人

個人にとって

- 端末がウイルスに感染する。
  - 情報漏洩
  - 金銭的損害　暗号化されたデータの復元には・・
- 調達した製品・サービスに脆弱性や不具合がある。
  例：　ネットワークカメラの脆弱性
  - 個人情報が漏洩する。プライバシーが侵害される。
- 加害者となるおそれ：　IoT機器が脆弱な設定のために攻撃の踏台に悪用される。　例：　簡易なパスワード

外部者にとって

- ネットワークカメラなどの個人のIoT機器が踏台に悪用され、外部者がDDoS攻撃を受け、ネットワーク上のサービスが影響を受ける。

目　次

1. サイバーセキュリティの概念
　　― ISO/IEC TS 27100 を参考にして　―

2. サイバーセキュリティの現場と
　　サイバーリスクの類型

3. ISMSの基本的な関心

4. サイバーセキュリティにおけるISMSの役割

組織で決定する ISMS の基本的事項

- ISMSの基本的な要求事項の中に、サイバーセキュリティとの関わりを認識する手がかりがある。
  1. **情報セキュリティ目的**（ISO/IEC 27001:2013, 6.2）・**情報セキュリティ方針**（同 5.2）
  2. **利害関係者**（同4.2）
     - サイバー空間における利害関係者とは
     - 組織が認識する利害関係者の要求事項は
     - 利害関係者の関心は・・・ 例えば、事業継続／取引関係(調達者・供給者)／情報セキュリティリスクにおけるつながり
     - 利害関係者であると自らが認識していない他者もサイバー空間に広く存在
  3. **ISMS の適用範囲**（同 4.3）
     - サイバー空間にある他者とISMS適用範囲の関係は

ISMS の基本形（1/2）

- 関心の対象： 組織自身の情報
  - 情報セキュリティリスクアセスメントの目的に関連して、
    「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」（ISO/IEC 27001:2013, 6.1.2 c）1））
  - ISMSの適用範囲は、通常は組織の全部又は一部であり、外部には及ばない。
    - 典型的には、事業部門や場所・事業所で特定
    - 参考：旧規格（2005年版）では、ISMS の適範囲を記述する用途として、事業・組織・所在地・資産・技術を列挙

ISMS の基本形（2/2）

- 関心の対象： 預かった情報
  - 取引先から預かった情報、個人顧客の情報

- 関心の対象： 預けた情報
  - 例： 外部のクラウドサービス環境に組織の情報を置く。
  - 関連： 外部委託したプロセスの管理
    （ISO/IEC 27001:2013, 8.1）

基本形を越えるISMSの機能

ISMSには、基本形を越えて、外部者を認識し、関係するリスクの管理に資する機能がある。

ISMSには、サイバーリスクの外部性に対応する機能がある。

→　次のスライドから

ISMSに関係する外部者 （1/3）

1. 組織がISMSにおいて間接的に管理することを意図している外部者 ＝ 委託先

   例　　情報を取り扱う業務の委託先

   利用しているITサービスの供給者：
   クラウドサービスプロバイダ等

- ISMS要求事項においては、「外部委託したプロセス」の管理として言及（ISO/IEC 27001:2013, 8.1）
- 委託先を利害関係者とする例も、しない例もあるか。

「利害関係者」の意味　（参考：ISO/IEC 27000 における定義）

a. 組織の決定又は活動に対して影響を与える可能性のある個人又は組織
b. 組織の決定又は活動の影響を受ける可能性のある個人又は組織
c. 組織の決定又は活動の影響を受けると認識している個人又は組織

ISMSに関係する外部者 （2/3）

2. 組織における情報セキュリティの状況を、関心を持って見る外部者

例　　個人情報を預けている個人
取引先
組織が提供しているITサービスの利用者
所管行政機関

- ISMS要求事項において、「利害関係者のニーズ及び期待の理解」として言及 (ISO/IEC 27001:2013, 4.2)

「利害関係者」の意味　（参考：ISO/IEC 27000 における定義）

a. 組織の決定又は活動に対して影響を与える可能性のある個人又は組織
b. 組織の決定又は活動の影響を受ける可能性のある個人又は組織
c. 組織の決定又は活動の影響を受けると認識している個人又は組織

ISMSに関係する外部者 （3/3）

3. 情報セキュリティインシデントによって組織が影響を与える結果になるおそれのある外部者

例　　インターネット上の個人、組織
　　国民、社会

- ISMS要求事項において、「利害関係者のニーズ及び期待の理解」として言及 (ISO/IEC 27001:2013, 4.2)
- サイバーセキュリティにおける典型的な利害関係者
- ISMSにおいても、利害関係者として認識され得る

「利害関係者」の意味　（参考：ISO/IEC 27000 における定義）

a. 組織の決定又は活動に対して影響を与える可能性のある個人又は組織
b. 組織の決定又は活動の影響を受ける可能性のある個人又は組織
c. 組織の決定又は活動の影響を受けると認識している個人又は組織

サイバーセキュリティへの対応の基礎

- ISMSには、サイバーセキュリティへの対応の基礎になる機能がある。
  - 情報セキュリティ目的/方針の確立
  - 利害関係者とその要求事項の特定
  - ISMS適用範囲の決定

- これらのプロセスを実施することによって、
  1. サイバーセキュリティの状況を認識し、
  2. サイバーセキュリティへの対応の基礎を確立し、
  3. サイバーリスク特定の前提を認識する。

目　次

1. サイバーセキュリティの概念
　　― ISO/IEC TS 27100 を参考にして　―

2. サイバーセキュリティの現場と
　　サイバーリスクの類型

3. ISMSの基本的な関心

4. サイバーセキュリティにおけるISMSの役割

組織が置かれている
サイバーセキュリティの現場を特定する

例えば、

1. サプライチェーンにおけるISMSの役割
    - サービスの調達
    - サービスの供給
    - 製品・部品の調達
    - 製品・部品の供給　・・・　品質問題

2. 重要インフラの維持におけるISMSの役割

3. サイバー空間に存在する個人・組織に対する責任におけるISMSの役割：　エコシステムの認識

該当するISMSの類型を知る

	ISMSの類型	関連規格例	ISMSの適用範囲	影響を及ぼす範囲
1	組織の情報を守るISMS	ISO/IEC 27001 ISO/IEC 27002 ISO/IEC 27017	組織全体又は特定範囲	ISMSの適用範囲
2	製品・サービス調達者としての組織	ISO/IEC 27017		供給者
3	サイバー空間に置かれた組織の責任 • 他者に対する影響の認識	ISO/IEC 27100 ISO/IEC 27400		不特定の他者
4	製品供給者の施策 • 脆弱性対策、品質確保、情報提供	ISO/IEC 29147	—	—
5	サービス供給者の施策 • 預かった情報のCIA維持 • 脆弱性対策、品質確保、情報提供	ISO/IEC 27017	当該サービス事業部門	サービスの顧客
6	重要インフラを担う視点のISMS	ISO/IEC 27011 ISO/IEC 27019	重要インフラ機能	国民・社会・国

ISMSの位置づけを再確認し、ISMSの基本事項に反映する

1. サイバーセキュリティのさまざまな現場の中で、組織の位置を知る:　サプライチェーン、重要インフラ事業、等。
2. サイバーセキュリティに関係する、組織の外部状況を知る。
3. ISMSの基本事項にこれらを反映する。
    - 情報セキュリティ目的と情報セキュリティ方針
    - 利害関係者を含む外部者とその要求
    - ISMSの適用範囲、ISMSが影響を及ぼす範囲

サイバーセキュリティへの対応を、
「ISMSを確立し、実施し、維持し、継続的に改善する」
(ISO/IEC 27001:2013, 4.4) という組織活動の中に組み込む。

目　次

1. サイバーセキュリティの概念
　　― ISO/IEC TS 27100 を参考にして　―

2. サイバーセキュリティの現場と
　　サイバーリスクの類型

3. ISMSの基本的な関心

4. サイバーセキュリティにおけるISMSの役割