情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

研究・イノベーション学会
国際問題分科会

DXとサイバーセキュリティ –
日本的モデルの脆弱性・強靭性

2021年　9月15日（水）18:00-20:00

情報セキュリティ大学院大学　教授
藤本 正代

はじめに

自己紹介とセキュリティ分野研究の全体像

自己紹介

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 1993年5月MIT科学技術政策大学院修了。
- 2000年6月東京工業大学社会理工学研究科経営工学専攻博士課程修了。経営工学博士。
- GLOCOM客員研究員。インターリスク総研及び富士ゼロックス株式会社にて、情報セキュリティに係る調査研究・コンサルティング、医療情報システム関連の業務等に従事。
- 内閣サイバーセキュリティセンター普及啓発・人材育成専門調査会委員、総務省情報通信審議会専門委員等を歴任。

最近の活動

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 政府委員等

- 内閣サイバーセキュリティセンター普及啓発・人材育成専門調査会委員
- 総務省　サイバーセキュリティタスクフォース構成員
- 電気通信事業におけるサイバー攻撃への適正な対処の在り方に関する研究会 構成員
- 総務省　国立研究開発法人審議会・宇宙航空研究開発機構部会　専門委員
- 全国社会保険労務士会連合会個人情報保護委員会委員
- 地方公共団体情報システム機構　認証業務情報保護委員会委員
- ASPIC　IoT・クラウドアワード審査員、等

■ 調査研究事業

- 内閣サイバーセキュリティセンター（NISC)の実証実験事業「平成30年度戦略マネジメント層の育成手法に関する調査」

■ 講演等

- 業界団体(技術産業関連など)、
- 企業（中小企業、情報通信関連）、等多数

IISECの4コース制カリキュラム

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

総合学習

- 情報セキュリティ特別講義
- 情報セキュリティ輪講
- Presentations for Professionals
- 情報セキュリティ運用リテラシーⅠ・Ⅱ

数理科学

- 暗号・認証と社会制度
- 暗号プロトコル
- アルゴリズム基礎
- 数論基礎
- 暗号理論
- AIと機械学習

サイバーセキュリティとガバナンス

- ハッキングとマルウェア解析
- 法学基礎
- 知的財産制度
- 不正アクセス技法
- セキュアシステム構成論
- サイバーインテリジェンス
- セキュア法制と情報倫理
- セキュリティの法律実務
- 個人識別とプライバシー保護

セキュリティリスクマネジメント

- 情報セキュリティマネジメントシステム
- セキュリティシステム監査
- セキュリティ管理と経営
- 組織行動と情報セキュリティ
- マスメディアとリスク管理
- リスクマネジメント
- リスクの経済学
- 統計的リスク管理
- 統計的方法論
- セキュリティ監査
- 国際標準とガイドライン
- 情報セキュリティ心理学

システムデザイン

- インターネットテクノロジ
- ネットワークシステム設計・運用管理
- 情報デバイス技術
- 情報システム構成論
- オペレーティングシステム
- セキュアプログラミングとセキュアOS
- プログラミング
- ソフトウェア構成論
- 実践的IoTセキュリティ

ハンズオン

- セキュアシステム実習
- セキュリティ実践Ⅰ ＆セキュリティ実践Ⅱ
  NWとWebアプリのセキュリティ検査と対策演習、デジタルフォレンジック演習、Capture The Flag (CTF)入門と実践演習、インシデント対応とCSIRT基礎演習

情報セキュリティ大学院大学とIoTセキュリティ人材育成

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 情報セキュリティ大学院
  - 学生の7-8割が、IT企業、官庁等の社会人
  - 技術、マネジメント、法律・制度のミックス
  - 即戦力 vs. 基礎力　＋人脈形成
  - enPiT-proにおいて東大、慶応義塾、中央大、東北大、九州大、長崎県立大、和歌山大などと連携したセキュリティ教育

- IoTセキュリティ人材育成
  - 2017年から3年間、IPAのIoTセキュリティ人材育成の教材開発プロジェクトを受託
  - 2016年にIoTセキュリティの授業を試行、2018年から正規科目
  - AIと機械学習を追加

セキュアシステム実習

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

※今回のプレゼンテーマ“増大するサイバー脅威に対して、(組織的に)どう対応すればよいのか。また被害を最小限に食い止めるにはどのようなノウハウがあるのか”に関係する体験型学習例

セキュアシステム実習のねらい

- 「ネットワーク経由の情報セキュリティ攻撃とその防御および検知」をテーマとし、攻撃者がどのようなツールや手法を用いてネットワーク不正侵入行為を行うか、またどのような防御方法や検知方法が有効かについて、実習を通して理解する。
- その上で、セキュアなシステムの構築方法についても考察する。

https://www2.iisec.ac.jp/education/curriculum/syllabus_20.html

企業等における情報セキュリティマネジメントの取組

ISMS

- 情報セキュリティマネジメントシステム
- 国際標準：JIS Q 27001:2014（ISO/IEC 27001:2013）
- 情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項

情報資産を保護するISMS

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

情報セキュリティマネジメントの標準

JIS Q 27001:2014（ISO/IEC 27001:2013）
情報技術―セキュリティ技術―情報セキュリティマネジメントシステム―要求事項

- リスクマネジメントプロセスを適用することによって
- 情報の機密性，完全性及び可用性を維持し，
- リスクを適切に管理しているという信頼を利害関係者に与える

情報セキュリティの3要素

会社情報管理の延長線上としても考えやすい概念
紙であれ、デジタルデータであれ、情報資産としての価値を評価し、それに見合った保護対策を実施する。

情報の機密性，完全性及び可用性を維持する

情報セキュリティの3要素

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 機密性（confidentiality）

認可されていない個人，エンティティ又はプロセスに対して，情報を使用させず，また，開示しない特性。

〔例〕化学工業（企業）の男性元社員がスマートフォンの液晶技術に関する情報を不正に中国企業に漏洩。不正に入手した情報をUSBメモリーにコピーし、私用のパソコンから中国企業にメールで送る。

■ 完全性（integrity）

正確さ及び完全さの特性。

〔例〕食品会社が集団食中毒事件の際に製造工程におけるタンクの洗浄記録等を改ざん／発電所事故の検査記録や修理記録が改ざん／工場の排水データを改ざんし報告／マンションの耐震強度偽装、など。

■ 可用性（availability）

認可されたエンティティが要求したときに，アクセス及び使用が可能である特性。

〔例〕2006年のライブドアショック（東京地検等の強制捜査で売買注文が急増してシステム障害が発生する危険があるとして東証1部、2部、マザーズの全銘柄の取引を強制的に停止

注記：真正性、責任追跡性、否認防止、信頼性などの特性を維持することを含めることもある。
※エンティティは、“実体”、“主体”などともいう。情報セキュリティの文脈においては、情報を使用する組織及び人、情報を扱う設備、ソフトウェア及び物理的媒体などを意味する。

リスクマネジメントプロセス（ISO/IEC27005:2018 第3版）

※第4版に向けての作業が進んでいるので、今後内容が変わる可能性があります。

- リスクマネジメントのコンテキスト（状況把握）を確立する（対象範囲、コンプライアンス義務、使用するアプローチ/方法、および組織のリスク許容度や意欲などに関連する方針と基準）。
- インシデントが発生する可能性またはインシデントシナリオ、それが発生した場合に予測されるビジネス上の結果を判断するために、情報資産、脅威、既存の対策や脆弱性を考慮して、関連する情報リスクを定量的または定性的に評価（つまり、識別、分析、および評価）し、「リスクのレベル」を決定する。
- その「リスクのレベル」を使用して優先順位付けをし、リスクを適切に処理する（すなわち、モディファイ*[情報セキュリティコントロールの使用]、保有[受け入れる]、回避および/または[第三者と]共有する）。
- プロセス全体を通じて利害関係者に情報を提供し続ける。
- リスク、リスク処理、義務、基準を継続的に監視およびレビューし、重要な変更を特定して適切に対応する。

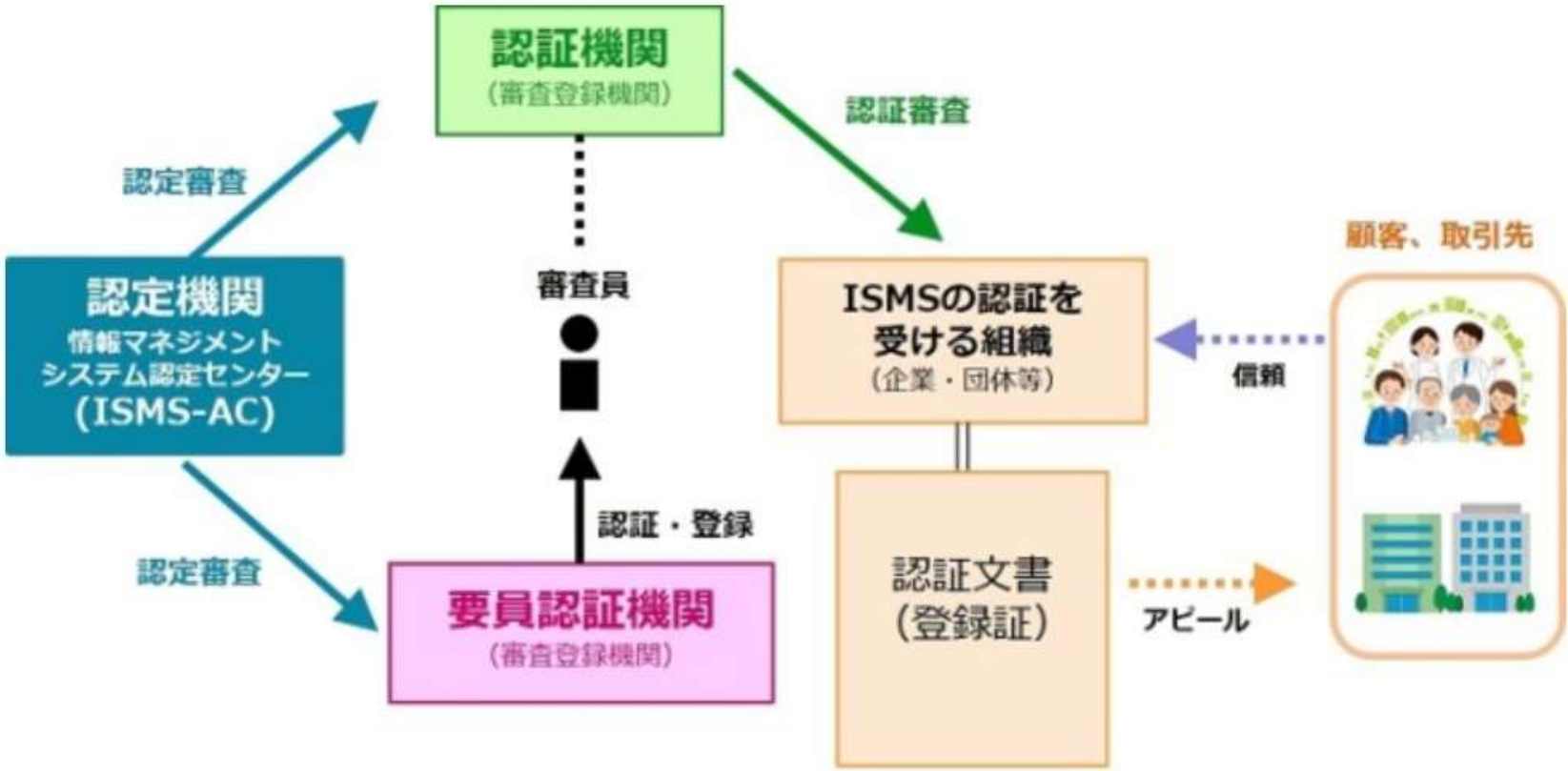
情報資産台帳を作成することからスタート

さまざまなリスク対策から選択したり、組み合わせる

*モディファイ…部分的に修正（変更）

参考：https://www.iso27001security.com/html/27005.html

認証制度



情報セキュリティマネジメントシステム(ISMS)適合性評価制度の概要
https://isms.jp/isms/about.html

世界の認証取得数

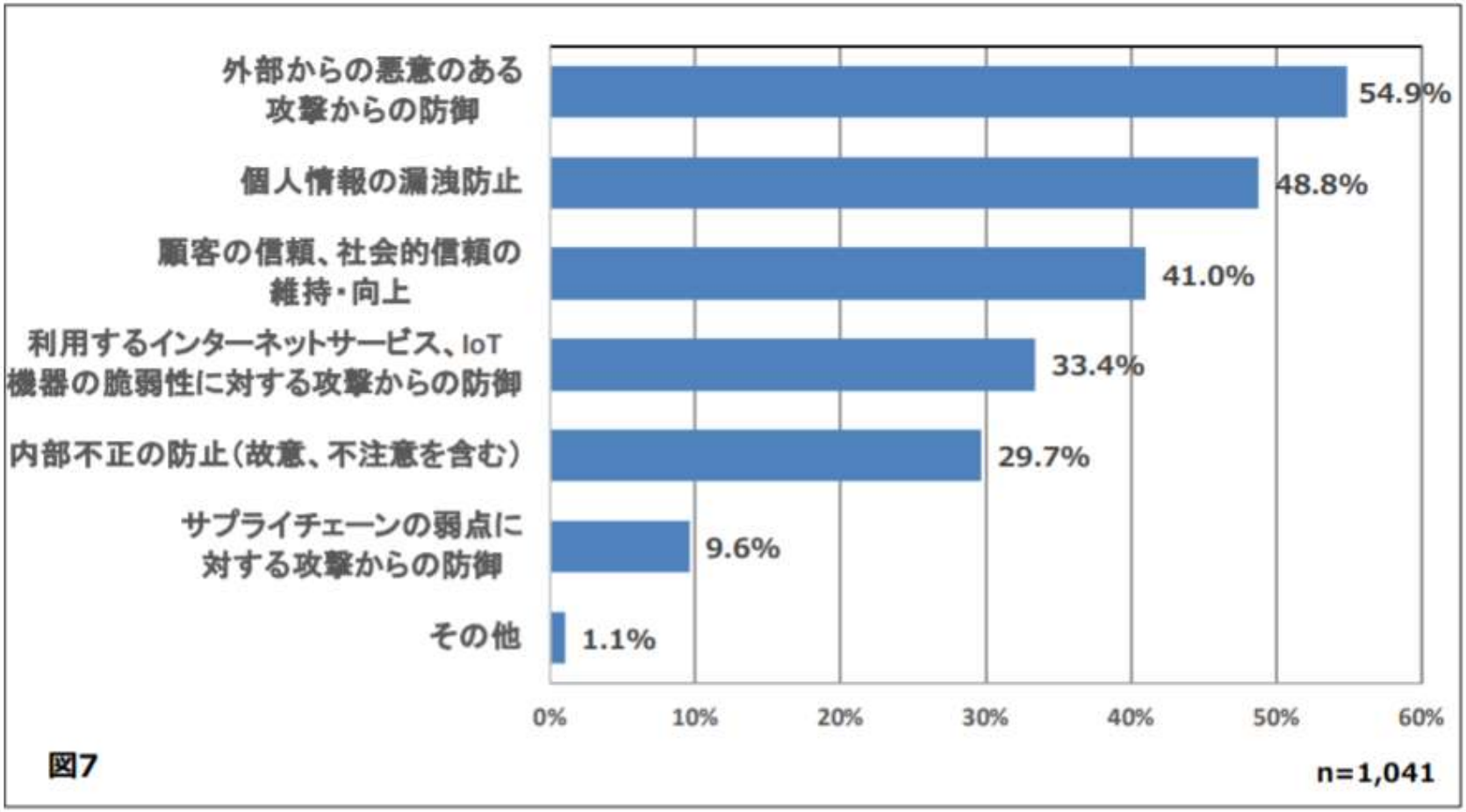
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

No.	Country	certificates
1	China	12403
2	Japan	5645
3	United Kingdom of Great Britain and Northern Ireland	3327
4	India	2226
5	Italy	1827
6	Netherlands	1326
7	Germany	1281
8	United States of America	1058
9	Spain	997
10	Taiwan, Province of China	895

1. ISO Survey 2020 results - Number of certificates and sites per country and the number of sector overall 2021年9月6日
https://isotc.iso.org/livelink/livelink?func=ll&objId=18808772&objAction=browse&viewType=1

普及の背景～ ISMS認証

情報セキュリティに期待する効果

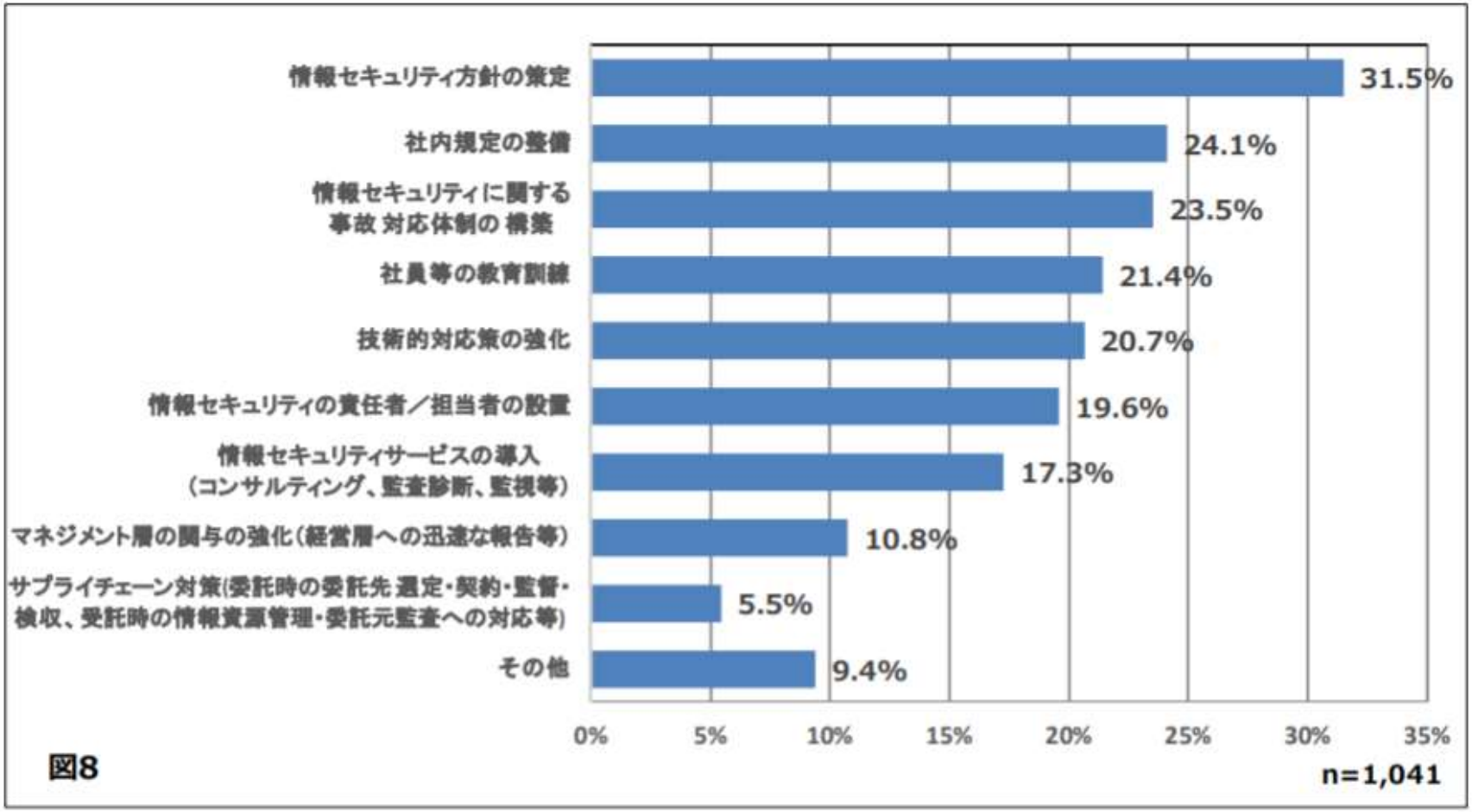


情報セキュリティと認証制度に関する調査報告書2020 年 6 月
一般社団法人情報マネジメントシステム認定センター（ISMS-AC）
https://isms.jp/enquete/2019/report2019.pdf

普及の背景～ ISMS認証

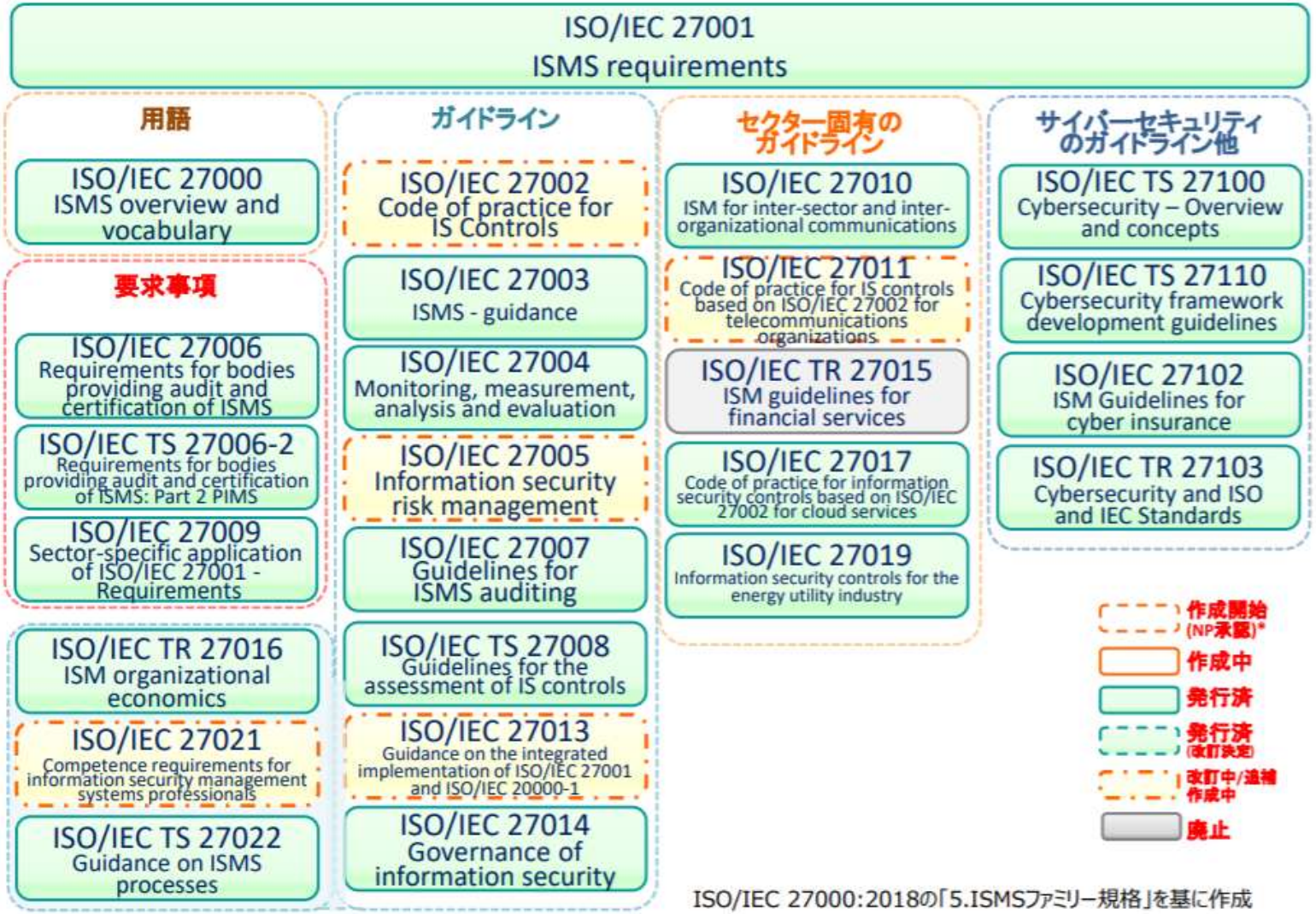
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

現在実施している情報セキュリティへの取組み



情報セキュリティと認証制度に関する調査報告書2020 年 6 月
一般社団法人情報マネジメントシステム認定センター（ISMS-AC）
https://isms.jp/enquete/2019/report2019.pdf

ISO/IEC 27000ファミリーの概要



ISO/IEC 27000:2018の「5.ISMSファミリー規格」を基に作成

ISO/IEC 27000ファミリーについて(2021.06.07)
https://www.jipdec.or.jp/smpo/u71kba000000jjgv-att/27000family_20200610.pdf

DX with Cybersecurity

DXについて

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

経済産業省『デジタルトランスフォーメーションを推進するためのガイドライン（DX 推進ガイドライン）Ver. 1.0』におけるDXの定義

「企業がビジネス環境の激しい変化に対応し、データとデジタル技術を活用して、顧客や社会のニーズを基に、製品やサービス、ビジネスモデルを変革するとともに、業務そのものや、組織、プロセス、企業文化・風土を変革し、競争上の優位性を確立すること。」

https://www.meti.go.jp/press/2018/12/20181212004/20181212004-1.pdf

DX（私見）：
企業の競争力の源泉（コアコンピテンス）が大きく変わる、、
ライバル企業が変わる、、
・・・

IT活用と少し違うニュアンス、、、？

DX with Cybersecurityでは、ITやセキュリティの知識に加え、事業の理解や変化への対応等、より戦略に即した発想が重要になる。

DXwithCybersecurity

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■新しいデジタル技術の活用とリスクマネジメント
～DX with Cybersecurity～

- 企業が新たなデジタル技術を活用する効果を最大限に享受するためには、デジタル技術を使って何を実現したいのかを明らかにするとともに、事業に致命的な影響を与えるリスクの洗い出しを行うことが重要。
- そのリスクの1つとしてデジタル技術の活用に対応するサイバーセキュリティへの対応は最も重要な柱

「サイバーセキュリティ2020概要」
https://www.nisc.go.jp/active/kihon/pdf/cs-senryaku-cs2020-gaiyou.pdf

たとえば、IoTの場合

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

自動運転

- CAN（車載機器ネットワークの標準的な通信プロトコルでController Area Networkの略）への侵入で、ブレーキ、ステアリングの操作、パネルに誤表示
  - Hackers Remotely Kill a Jeep on the Highway – With Me in It
    - https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway

- 2018年3月19日（現地時間）、米国アリゾナ州で実験走行中のUber（ウーバー）の自動運転車が、歩行者に衝突
- 自動運転車が初めて歩行者を死亡させる事故。

街の人は、自動運転の実験が行われていることを知っていたのか？

警察庁「遠隔型自動運転システムの公道実証実験に係る道路使用許可の申請に対する取扱いの基準」の策定について（通達）
実施主体は、地域住民を始めとする関係者に対し、実験の内容等について走行前 に広報又は説明を行うこと。

DX with Cybersecurityに必要な人材

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

サイバーセキュリティ人材育成

役割

経営層	戦略マネジメント層	実務者層・技術者層
● 事業継続と価値創出のために重要なサイバーセキュリティ対策を、リスクマネジメントの一環として実施	● 経営層の方針を踏まえた対策立案、実務者・技術者の指揮 ● リスクマネジメントを支える中心的役割	● 経営層の方針を踏まえた、セキュリティ対策の企画・構築・実施 ● 経営層・戦略マネジメント層を支え、チームの一員として対処できる人材

「サイバーセキュリティ2020概要」

組織体制（例）

CIO/CISO

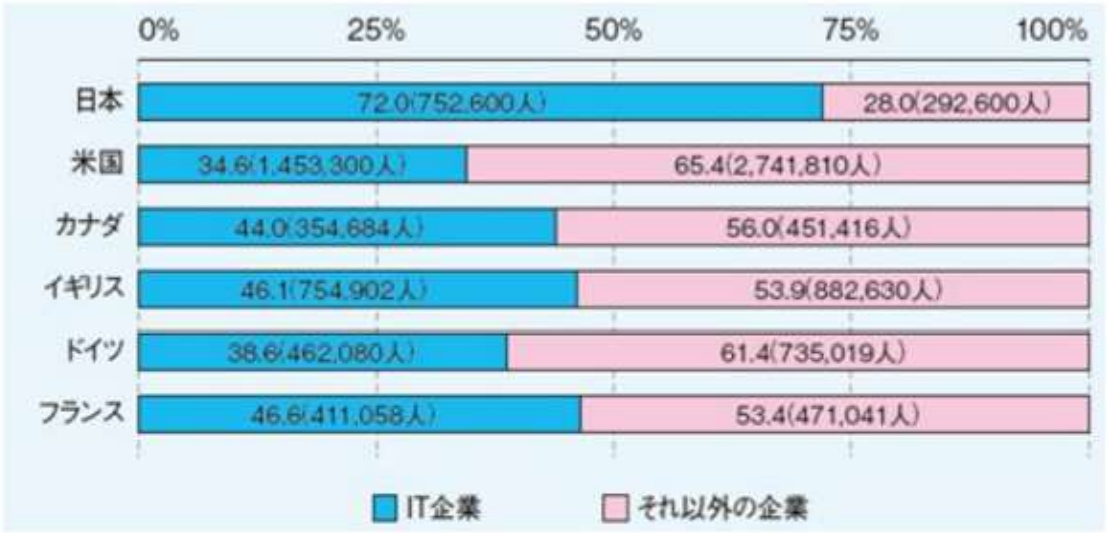
DX with Cybersecurityの責任部署は？？

IT人材のIT企業への偏り

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

○IT企業に所属する情報処理・通信に携わる人材の割合を比較すると、日本は72.0%と突出して高い。
（一方、日本以外の国は概ね5割以下であり、中でも米国は34.6%）

<日米、欧州等のIT企業・IT企業以外の企業における情報処理・通信に携わる人材の割合>



（出典）独立行政法人情報処理推進機構「IT人材白書2017」 https://www.ipa.go.jp/files/000059087.pdf

日本的モデルの脆弱性・強靭性、、、

※上記の出典等:

○日本:2015年国勢調査結果（IT企業として扱った業種は、「ソフトウェア業」、「情報処理・提供サービス業」、「インターネット附随サービス業」。情報処理・通信に携わる人材として扱った職種は、「システムコンサルタント・設計者」、「ソフトウェア作成者」、「その他の情報処理・通信技術者」）

○米国:職業雇用統計（IT企業として扱った業種は、「511200 Software Publishers」、「518200 Data Processing, Hosting, and Related Services」、「541500 Computer Systems Design and Related Services」。情報処理・通信に携わる人材として扱った職種は、「11-3020 Computer and Information Systems Managers」、「15-1100 Computer Occupations」）

○カナダ:カナダ情報局（Statistics Canada http://www.statcan.gc.ca）のデータを基にICTCが作成（出典元「Digital Economy Annual Review 2015」）、情報処理・通信に携わる人材の職種、IT企業として扱った業種は米国の基準に準拠。

○イギリス、ドイツ、フランス:EU統計局（Eurostat）が保有する労働力調査（EU LFS）の結果を調査会社であるempiricaが入手し分析したものを利用

22

NISC、DX with Cybersecurity実践に向けた人材の確保、育成、活躍促進に係る主な政策課題と方向性
https://www.nisc.go.jp/conference/cs/jinzai/dai15/pdf/jinzai_houkousei

セキュリティインシデント事例

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■ 決済サービスへの不正アクセス

- 2019年7月1日　サービス開始
- 7月2日　お客様からの問い合わせ、海外 IP からのアクセスを遮断、クレジット／デビットカードからのチャージ利用を停止
- 7月30日　パスワードリセットの実施
- 8月1日　サービス廃止を決定
- 9月30日　サービス廃止

※2020年2月25日：申出者への払戻し業務を終了

https://www.7andi.com/library/dbps_data/_template_/_res/news/2019/20190801_01.pdf
https://www.7pay.co.jp/info/info_20200225_01.html

■ 個人情報の取り扱い不備

- 2018年3月1日　サービス開始
- 2019年7月31日　一時休止を決定
- 8月5日　7,983名を対象としたプライバシーポリシー同意取得の不備とサービスの廃止についてプレスリリース

※8月26日　個人情報保護委員会から勧告と指導

https://www.recruitcareer.co.jp/r-dmpf/01/

DX事業に関連したセキュリティインシデント

たとえば、

- ITを活用した新規サービスにおける不正利用
- 個人情報を含むデータ利活用の失敗、等

インパクト

サービス廃止等

サイバーセキュリティの確保が
DX事業の推進を左右する

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

人材育成の取組

教育カリキュラムのトライアル

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2018年（平成30年度）

カリキュラムのモデル化

2．2

○内外のセキュリティ専門人材と協働するために必要となる知識は、部門・人材層等によって異なるため、「プラス・セキュリティ」知識は一意に体系化される性質のものではないが、知識を提供するプログラムが広く普及していくためには一定のモデル化が必要である。

○このため、まずは、今後デジタル化が進んでいく中で特に需要が高まると考えられる、「DXを推進する部門の責任者あるいは主要な役割を担う管理職」（※）を対象層としてモデルカリキュラム開発を試行。

（※）DX経営推進者・DX事業推進者等、部課長級であって、必ずしもITやセキュリティに関する専門知識や業務経験を有していない方を念頭。

○特に、NISCにおいては、過去に整理された「戦略マネジメント層」向けのモデルカリキュラムと対応し、コンピュータ・情報通信ネットワーク・インターネット・サイバーセキュリティに関する知識のうち、DX推進の中で専門家との協働に当たって、最低限必要で役に立つと考えられる基礎知識の整理作業を行った。※1/21 普及啓発・人材育成専門調査会 参考資料2-1参照

<戦略マネジメント層育成モデルカリキュラム(2018年)>

最低限必要で役に立つと考えられる基礎知識を体系化

作業①：DX事業推進に際し活用が想定される場面から逆算し、どのような状態を目指すかを整理した。

↓

作業②：実務目線からIT 初心者に必要な知識が整理された「IT パスポートシラバス」を参照し、ｉ：詳細な目標とｉｉ：予め理解することが望ましいと考えられる基礎概念を整理した。

【詳細は1/21 普及啓発・人材育成専門調査会参考資料2-2等を参照】

↓

情報セキュリティ大学院大学において実施されたプログラム（試行カリキュラム）において、上記の作業結果を参考にしていただいた。

【詳細は1/21 普及啓発・人材育成専門調査会資料1-7を参照】

※（出典）サイバーセキュリティ戦略本部 普及啓発・人材育成専門調査会「サイバーセキュリティ人材の育成に関する施策間連携ワーキンググループ 報告書」（2018年5月）15

DX with Cybersecurity実践に向けた人材の確保、育成、活躍促進に係る主な政策課題と方向性
https://www.nisc.go.jp/conference/cs/jinzai/dai15/pdf/jinzai_houkousei

参考：DXwithCybersecurity
教育カリキュラム内容1日目

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2020年11月18日（水）（Web会議）	
10:00～10:30	開会の辞・カリキュラム内容説明 情報セキュリティ大学院大学　教授　藤本 正代
10:30～11:30	【自己紹介】（各6分×10名）
11:30～12:30	【講義】「DX with Cybersecurityの全体像」 国立情報学研究所／東海大学情報通信学部 客員教授　三角 育生 氏
12:30～13:30	昼食
13:30～14:30	【講義】「DXを構成するIT関連基礎知識」 イグレック株式会社 理事　八剱 洋一郎 氏
14:40～15:40	【講義】「IoTから入る情報セキュリティの基礎」 情報セキュリティ大学院大学 教授　松井 俊浩
15:50～16:50	【企業プレゼン】「DX事業事例とITおよびサイバーセキュリティ技術」（仮） 全日本空輸株式会社 取締役 常務執行役員　三浦 明彦 氏
17:00～18:30	【Webワークショップ】（自由に意見交換） 参加者でディスカッションテーマを決めて意見交換

参考：DXwithCybersecurity
教育カリキュラム内容2日目

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2020年11月19日（木）（Web会議）	
9:00～10:20	【講義】「DXのためのリスクマネジメントと事故対応」 情報セキュリティ大学院大学　教授　藤本 正代
10:30～12:00	【講義】「DX及びサイバーセキュリティの関係法令」 西村あさひ法律事務所 弁護士　北條 孝佳 氏
12:00～13:00	昼食
13:00～13:50	【企業プレゼン】「三井倉庫グループの情報システム概要について」 三井倉庫ホールディングス株式会社 執行役員 情報システム担当 糸居 祐二 氏
14:00～14:50	【企業プレゼン】「三菱マテリアルのデジタル・ビジネストランスフォーメーションの取り組み」三菱マテリアル株式会社 経営戦略本部長補佐、CDO（Chief Digital Officer）　亀山 満 氏
15:00～15:50	【企業プレゼン】「アシックスのデジタル及びITの取り組み」 株式会社アシックス IT統括部　常務執行役員（CDO兼CIO）　富永 満之 氏
16:00～18:00	3日目の予定及びチーム編成説明＋Webワークショップ(自由に意見交換)

参考：DXwithCybersecurity
教育カリキュラム内容3日目

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

2020年11月20日（金）（Web会議）	
9:30～10:00	チーム演習の説明
10:00～12:00	**【チーム演習】** 自社の新規事業開発とサイバーセキュリティの取組における課題と解決策案をまとめる。（経営トップへの報告イメージ）
12:00～13:00	昼食
13:00～15:00	**【各チームによる発表】**A、B、Cチーム発表（各40分×3チーム）
15:10～16:10	**【発表サマリー・講評】**＋受講者アンケート　自由に意見交換
16:10～16:30	閉会の辞　情報セキュリティ大学院大学　藤本 正代
16:30～17:00	休憩
17:00～19:00	**【Workshop・意見交換会】** **「サイバー脅威主体の「攻撃戦略」の変化」** 株式会社サイバーディフェンス研究所　専務理事/上級分析官 名和 利男 氏を招いて

教育カリキュラムからの示唆

■ 日数や参加者等

- 日数・時間については、丁度よいという意見と、長いという意見が半々であった。
- 毎週1～2時間程度で数回実施する分散型がよいという意見もあったが、集中的に学習できる今回の形式に賛同する意見の方が多かった。
- 受講者や講師のヒアリングで次のような話もあった。
  - ◆ DXを推進する立場の人が基礎知識を学ぶことは、当然のことと思っている。セミナーの中でITの基礎をカバーするのは必須であり、それなりに時間を割いてもらいたい。
  - ◆ 受講者について、DX推進責任者から指名を受けて参加した方もいるという印象を受けた。
  - ◆ ITに詳しい受講者からの質問に専門性の高い内容があり、はじめは場違いなところに来たと思ったが、段々そうした方との交流にも慣れてきた。

■ 内容等

- 構成については、それぞれ役に立ったという意見が主流
  - ◆ DXwithCybersecurity全体像についての理解
  - ◆ 他社の取組事例が参考になったという意見が多数
  - ◆ 社内の関係者などとのコミュニケーションに、本カリキュラムで得た知識が活用でき相互理解につながった、という意見もあった

内容は多いほうが良いが、日数は短く
↓
教育方法を工夫する必要がある

参考：https://www.nisc.go.jp/conference/cs/jinzai/dai14/pdf/14shiryou0107.pdf

教育カリキュラムからの示唆

情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 内容等
  - さらに深く知りたい内容として次のような意見があった
    - 社内ネットワークの構築
    - ユーザー認証
    - 個人情報保護
    - サイバー攻撃の現状
    - セキュリティ訴訟
    - 多要素認証の重要性の説明や具体的な手法、等

参考：https://www.nisc.go.jp/conference/cs/jinzai/dai14/pdf/14shiryou0107.pdf

DX with Cybersecurity セミナー

情報セキュリティ大学院大学
MATION SECURITY

ISSスクエア特別セミナー

DX with Cybersecurity
DX推進企業の事例紹介

主催：研究と実務融合による高度情報セキュリティ人材育成プログラム（ISSスクエア）
共催：特定非営利活動法人NPO情報セキュリティフォーラム

2021年10月22日(金)
Web開催

時　刻	内　容　　司会：藤本 正代
13:00～13:10	開会挨拶 モデレーター：八剱 洋一郎 氏
13:10～13:55	**『新・サイバーセキュリティ戦略の方向性：DX with Cybersecurityの推進』** 内閣官房 内閣サイバーセキュリティセンター（NISC）基本戦略第1グループ 内閣参事官　佐伯 宜昭氏
13:55～14:40	**『三菱マテリアルが挑むIT戦略／DX戦略』** 三菱マテリアル株式会社 執行役員CIO／システム戦略部長　板野 則弘氏
14:40～14:50	休　憩
14:50～15:35	**『Dは道具、Xが目的。中堅企業のリアルDXとは？』** 株式会社　アールシーコア 取締役　宮本 眞一氏
15:35～16:20	**『ANAのDX with Cybersecurityの取り組みについて』** ANAホールディングス株式会社 常勤監査役　三浦 明彦氏
16:20～16:30	休　憩
16:30～18:10	**パネルディスカッション「日本におけるDXとサイバーセキュリティの実際」** 司会：八剱洋一郎氏 パネリスト： 佐伯 宜昭氏 板野 則弘氏 宮本 眞一氏 三浦 明彦氏
18:10～18:20	閉会挨拶 情報セキュリティ大学院大学教授　藤本正代

今年10月開催

申込用サイト
https://iss.iisec.ac.jp/event/details/ISS2-seminar2021.html

ありがとうございました

fujimoto@iisec.ac.jp