「ISACAのサイバー資格CSXとCISM資格について」

講演者　*ISACA 東京支部 副会長 坂川克己*

目次

1. CSX (Cyber Security neXus), Cyber Security Framework, CISM , キャリアパスとの関係

2. Cyber Security Frameworkについて（NIST版を例示）

3. 実務的に焦点が当たっている事
(2014 Nov, Las Vegas conference から）

1. CSX (Cyber Security neXus), Cyber Security Framework, CISM , キャリアパスとの関係

CSX とは。

・CSX(*) とは、ISACAが提唱するCyber securityに関わるプロフェショナルの育成と資格認定の体系となります。

・同時に標準キャリアパスとの整合性を持たせています。
標準キャリアパスは、SFIA (*)が提唱するスキル標準レベルと整合しています。

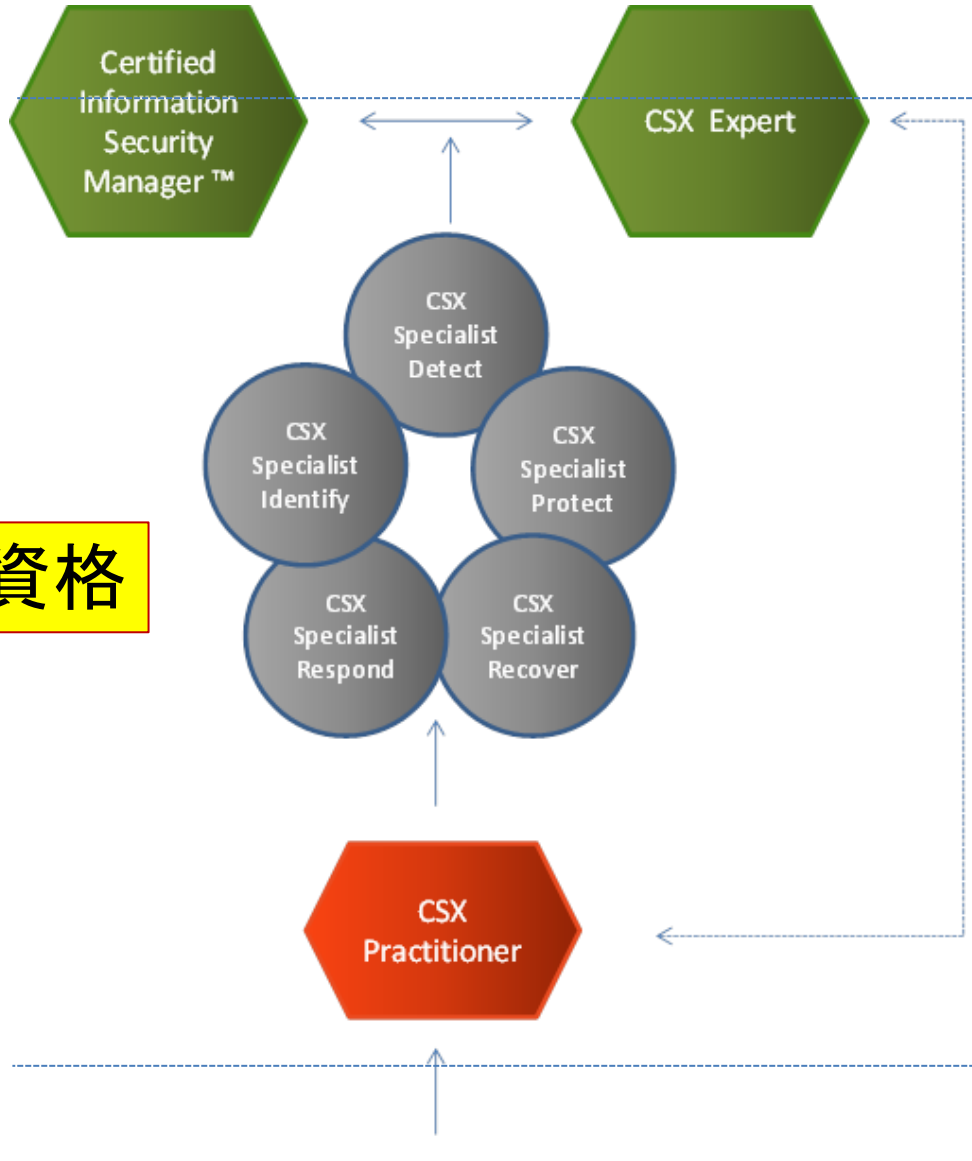
・高等学校教育のカリキュラム標準となるシラバスを提案しています。

(*) CSX (Cyber Security neXus)

SFIA (Skills Framework for the Information Age)

CSX　キャリア　・パス

Skills Framework for the Information Age 第6版



資格

Level -7：業界において屈指の実力

Level -6：
知識や経験を背景に多くの実績

Level -5：

～

Level -4：

～

フレームワーク

Level -3：
前提知識や入門的な資格を保有

Level -2

Level -1

Skills Framework for the Information Age 第6版

SFIA（Skills Framework for the Information Age: 情報化時代のためのスキルのフレームワーク）では、情報通信技術関連の責任において専門家が必要とするスキルについて説明している。

http://www.sfia-online.org/ja/reference-guide/SFIA6-reference

各スキルは、スキルが使用される最大7つの各レベルの定義の概要と説明で構成されている。これらの説明は、スキルとレベルの組合せによって、各スキルを使用するコンピテンシーレベルがどのように決定されるかの詳細に関する参考情報を提供する。

http://www.sfia-online.org/en

CSX 資格の4区分

	CSX Fundamentals Certificate	Certification		
		CSX Practitioner	CSX Specialist	CSX Expert
Exam Availability	Available by accessing the Cybersecurity Fundamentals Certificate Exam from the ISACA website	From August 2015	To Be Determined	To Be Determined
Requirements	Knowledge based certificate for those want to obtain knowledge.	-Passage of CSX Practitioner examination -Compliance with ISACA's Code of Professional Ethics -Compliance with ISACA's CSX CPE Policy is required to maintain certification	-Hold a CSX Practitioner or a CSX Expert certification in good standing -Passage of a CSX Specialty examination(s) -Compliance with ISACA's Code of Professional Ethics -Compliance with ISACA's CSX CPE Policy is required to maintain certification	-Passage of CSX Expert examination -Compliance with ISACA's Code of Professional Ethics -Compliance with ISACA's CSX CPE Policy is required to maintain certification

	CSX Fundamentals Certificate	Certification		
		CSX Practitioner	CSX Specialist	CSX Expert
Exam Availability	Available by accessing the Cybersecurity Fundamentals Certificate Exam from the ISACA website	From August 2015	To Be Determined	To Be Determined
Requirements	Knowledge based certificate for those want to obtain knowledge.	-Passage of CSX Practitioner examination -Compliance with ISACA's Code of Professional Ethics -Compliance with ISACA's CSX CPE Policy is required to maintain certification	-Hold a CSX Practitioner or a CSX Expert certification in good standing -Passage of a CSX Specialty examination(s) -Compliance with ISACA's Code of Professional Ethics -Compliance with ISACA's CSX CPE Policy is required to maintain certification	-Passage of CSX Expert examination -Compliance with ISACA's Code of Professional Ethics -Compliance with ISACA's CSX CPE Policy is required to maintain certification
Domain Percentage	Domain1-Cybersecurity Concepts (10%) Domain2-Cybersecurity Architecture Principles (20%) Domain3-Network, System, Application, & Data (40%) Domain4-Incudent Response (20%) Domain5-Security of Evolving Technology (10%)	Domain 1-Identify (13-15%) Domain 2-Protect (33-37%) Domain 3-Detect (21-25%) Domain 4-Respond (16-18%) Domain 5-Recover (10-12%)	To be determined	To be determined
Type/Length of Exam	Given 2 hours (120 minutes) to complete the computerbased exam and 75 multiple-choice questions, the passing score is 65%.	The exam is a computerbased exam delivered at a Prometric testing center(*). Four hours seat time is scheduled.	The exam is a computerbased exam delivered at a Prometric testing center. Four hours seat time is scheduled.	The exam is a computerbased exam delivered at a Prometric testing center. Four hours seat time is scheduled.
Language	English	English	English	English

まず、知識ベースの ”Cybersecurity Fundamentals Certificate” が
エントリーレベルの資格となります。この資格は、

- the National Institute of Standards and Technology (NIST),
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

- National Initiative for Cybersecurity Education (NICE),
http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf

という世界レベルの知識体系との互換性を維持しながら開発されています。また、

- The Skills Framework for the Information Age (SFIA) という英国に本部を持つスキルフレームワークにも準拠しています。

・UK’s cyber security skills (参考)
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/289806/bis-14-647-cyber-security-skills-business-perspectives-and-governments-next-steps.pdf

キャリアパス図からも読み取れる様に、上位の資格を目指すためには、まずエントリーレベルの”Cybersecurity Fundamentals Certificate” に合格する必要があります。

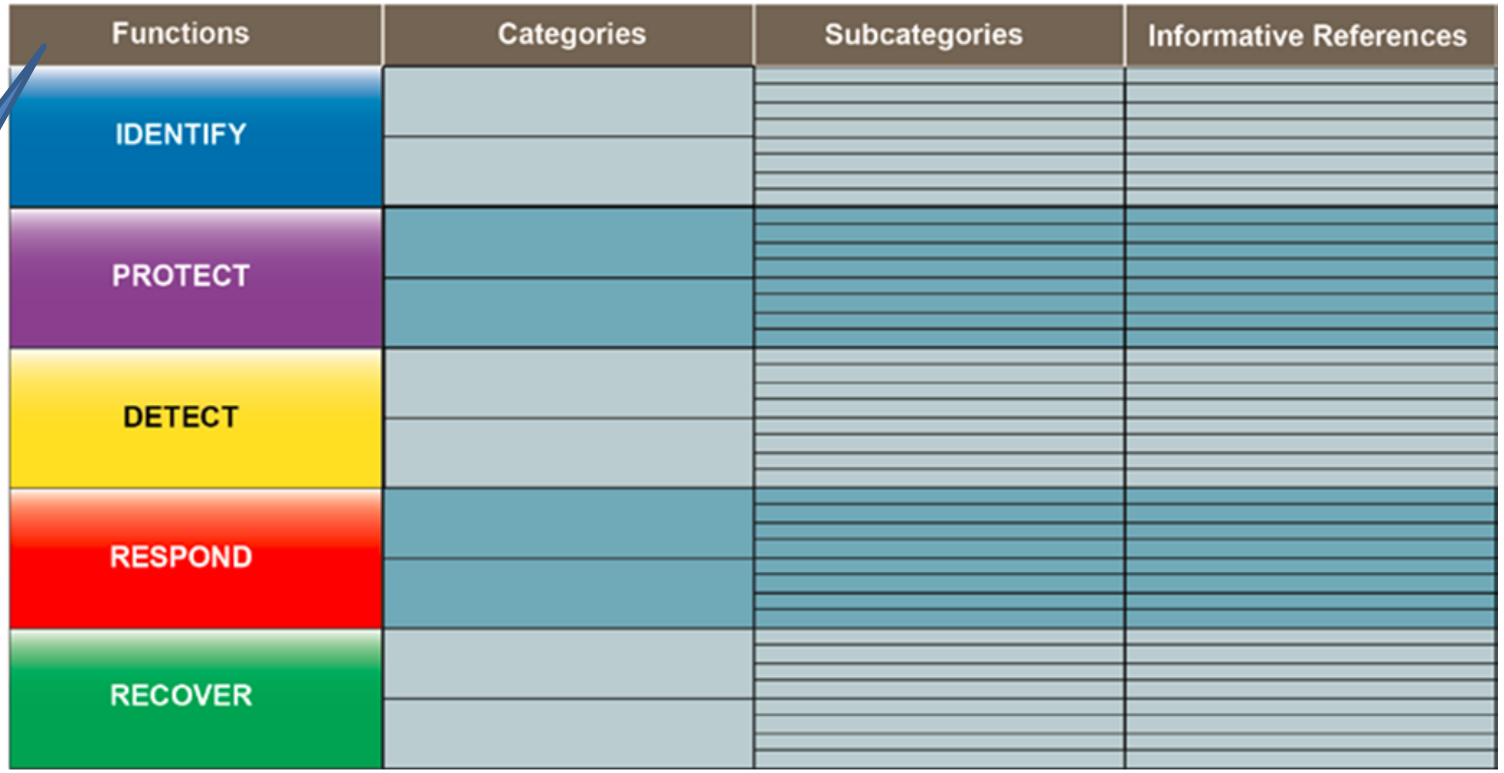
前表に概要を一覧します。(*) **Prometric testing center** での受験地は、2015年8月時点で東京と大阪でも受験可能となっています。

現在、試験やトレーニングは英語のみでの提供になりますが、セキュリティ運用やCSIRT要員にとって大変実行力のある資格ですので、是非ご検討下さい。
日本語のマニュアル、トレーニング、試験の提供時期は未定ですが、現在本部で検討中です。下記に主なCSXの関連情報のリンクを載せます。(P.15参照)

2. Cyber Security Frameworkについて（NIST版を例示）

Cyber Security Framework　って何？。

Figure 1: Framework Core Structure



この5つのエリア、観たことありますよね。

Table 1: Function and Category Unique Identifiers

＜参考:NISTの説明＞

はじめに

2001年9月11日のテロ以降、米国政府のセキュリティに関する取組は大きく変わったと言われています。米国NIST（国立標準技術研究所: National Institute of Standards and Technology）では、情報セキュリティに関する様々な規格、標準、ガイドラインを策定していますが、その背景も9.11前と9.11後では大きな変化が見られます。NISTの活動に大きな変化をもたらした法律は、FISMA（フィスマ）という法律です。この法律では、連邦政府機関が情報セキュリティを強化することを義務付け、NISTに対しては、そのための規格やガイドラインの開発を義務付けています。

(注)FISMA：Federal Information Security Management Act of 2002（連邦情報セキュリティマネジメント法)

米国では、このように、情報セキュリティ対策の実施を法律で義務付けています。この法律の対象となるのは、連邦政府機関や、連邦政府機関より業務委託を受けている民間の外部委託先です。

NISTでは、FISMAの規定を受けて、「FISMA導入プロジェクト（The FISMA Implementation Project）」を立ち上げ、FISMAリスクマネジメントフレームワークという、情報セキュリティを継続的に改善・向上させる枠組みや多くの規格、ガイドラインを開発しました。

これらNISTの文書群は、その内容を見ると、政府機関だけではなく、企業の経営者、セキュリティ担当者などが、自組織の情報セキュリティ対策を向上させるために役立つ資料と言えます。

FISMAの規定

2002年12月に制定された「電子政府法」のタイトルIII「連邦情報セキュリティマネジメント法（FISMA）」は、各連邦政府機関に対して、情報および情報システムのセキュリティを強化するためのプログラムを開発、文書化、実践することを義務付けています。また、同法は、NIST（米国国立標準技術研究所）に対しては、連邦政府がFISMAに準拠するための支援をすることを義務付けています。

（注）FISMAの規定は、各連邦政府機関より業務委託を受けている外部委託先にも適用されます。

https://www.ipa.go.jp/security/publications/nist/fisma.html

＜参考： NIST を参照できるサイト、US ＆日本 ＞

Framework for Improving Critical Infrastructure Cybersecurity

Version 1.0 National Institute of Standards and Technology February 12, 2014
http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

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
1.0 版
米国国立標準技術研究所 (National Institute of Standards and Technology)
2014 年2 月12 日

https://www.ipa.go.jp/files/000038957.pdf

NIST　Cyber Security Framework　抜粋

Function	Category	Subcategory	Informative References	
PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP):** **（情報プロテクションのプロセスと手順）** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.			
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) （権限が切り離されているかどうか、個々人の権限棚卸など人間系実務などもサイバーセキュリティには含まれる）		
	Maintenance (PR.MA): **（維持管理）** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	（省略）		
	Protective Technology (PR.PT): **（プロテクト技術）** Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	（省略）		
DETECT (DE)	（省略）			
RESPOND (RS)	（省略）			
RECOVER (RC)	（省略）			

Function	Category	Subcategory	Informative References	
IDENTIFY (ID)	Asset Management (ID.AM): (アセット・マネジメント) The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy. (データ、人物、デバイス、システム、ファシリティ)	**ID.AM-1:** Physical devices and systems within the organization are inventoried (組織内の物理的デバイス、システム)	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8	
		ID.AM-2: Software platforms and applications within the organization are inventoried (組織内のソフトウエア・プラットフォーム、アプリケーション)	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8	
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established (全ての作業要素に対するサイバーセキュリティ役割と責任)	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11	CP-2 CONTINGENCY PLAN Control: The organization: a. Develops a contingency plan for the information system that: PS-7 THIRD-PARTY PERSONNEL SECURITY Control: The organization: PM-11 MISSION/BUSINESS PROCESS DEFINITION Control: The organization: a. Defines mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation; and (ミッション・プロセス、ビジネス・プロセスの定義) b. Determines information protection needs arising from the defined mission/business processes and revises the processes as necessary, until achievable protection needs are obtained. (プロテクトさせる要求や必要性を決定する)

Function	Category	Subcategory	Informative References	
IDENTIFY (ID)	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. （サイバーセキュリティ・リスクのマネジメント、ポリシー、手順、プロセスを使ったマネジメント）	**ID.GV-1:** Organizational information security policy is established		
		ID.GV-4: Governance and risk management processes address cybersecurity risks	· COBIT 5 DSS04.02 · ISA 62443-2-1:2009 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · NIST SP 800-53 Rev. 4 **PM-9, PM-11**	**PM-9 RISK MANAGEMENT STRATEGY（リスク管理戦略）** Control: The organization: a. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations, and the Nation associated with the operation and use of information systems; （国家的枠組みとの連携） b. Implements the risk management strategy consistently across the organization; and （組織横断的なリスク管理戦略） c. Reviews and updates the risk management strategy [Assignment: organization-defined frequency] or as required, to address organizational changes. （リスク管理戦略の更新、維持管理）

<参考：　１，２　の参考なリンク先　＞

１ CSX　全体概要　及びFundamental 試験、
http://www.isaca.org/cyber/Pages/Cybersecurity-Fundamentals-Certificate.aspx

２）Get Certified　(資格試験)　概要案内；
https://cybersecurity.isaca.org/csx-certifications

３）CSX-Fundamental資格概要；
https://cybersecurity.isaca.org/csx-certifications/csx-fundamentals-certificate

４）CSX-Fundamental 資格試験のExam Guide
（本部サイトからダウンロード可能）
http://www.isaca.org/cyber/Documents/CSX-Exam-Guide_bro_Eng_1014.pdf

５）CSX-Fundamental資格試験のオンラインCBT受験申込サイトへのリンク
http://www.isaca.org/cyber/Pages/Cybersecurity-Fundamentals-Certificate.aspx

3. 実務的に焦点が当たっている事
(2014 Nov, Las Vegas conference から）

当日、スクリーンのみとなります。

ありがとうございました。