米国におけるサイバーセキュリティの人材育成と内部脅威に関する取り組みの現状

八山　幸司
JETRO/IPA New York

1　はじめに

インターネットの発達とともにサイバー攻撃は多様化し高度化してきたが、重要インフラがターゲットになるなどサイバー攻撃はより人々の生活を脅かすものとなってきている。特に近年では IoT などの発達により、あらゆるデバイスがサイバー攻撃の対象となりつつある。さらに企業は外部のサイバー攻撃だけでなく内部脅威にも対応が必要となり、また多くの機密情報を持つ政府も対応に追われている。米国では昨年 12 月 18 日にサイバーセキュリティ法案が成立するなど、サーバーセキュリティ対策の動きが加速化しているが、これら対策を確実に実施し、高度化するサイバー空間の脅威に対抗するために、サイバーセキュリティ対策を担う人材育成が益々重要になってきており、長期的・短期的な戦略が必要されてきている。今号では、米国におけるサイバーセキュリティの人材育成と内部脅威への取り組みについて紹介する。

最初に近年のサイバーセキュリティの動向について紹介する。サイバーセキュリティの市場は拡大の一途を見せ、今後も急成長が続くと見られている。その背景にはサイバー攻撃による被害が大きくなっているため、より高度なセキュリティが必要とされている点があり、以前はウィルスなどの被害が多かったものが、近年では機密情報を狙った高度なサイバー攻撃が増えている。サイバーセキュリティ人材の需要は更に高まっており、民間と政府の両方で優秀な人材の確保が急務となっている。また、市場で求められる人材はセキュリティ技術だけでなく、組織内で様々な役割をこなし各部署と連携できるような優秀なソフトスキルを持っていることも条件となっており、このことが益々人材不足を生み出している。

次に、サイバーセキュリティの人材育成の取り組みについて紹介する。サイバーセキュリティ対策では企業のビジネスを理解することが不可欠であるため、民間企業では様々な業務を学ぶことでセキュリティに活かすクロス・トレーニングが注目されている。また、シミュレーションによりセキュリティを学ぶシステムでは IoT に対応したものが登場しており、ベンチャー企業からはオンライン講座で優秀な人材を発掘するサービスも登場している。政府の取り組みでは、オバマ大統領からサイバーセキュリティの人材育成を目的とした TechHire イニシアチブが出されている。また、政府機関では様々な省庁が連携して人材育成に取り組む NICE イニシアチブが出され、政府の支援を受けて官民連携のサイバーセキュリティ研究も進められている。

最後に、内部脅威への取り組みについて紹介する。内部脅威は外部からのサイバー攻撃と並んで被害額が大きく復旧にかかる時間も長い。しかしながら、企業の IT システムが複雑化・巨大化しているため、セキュリティ担当者は対応が難しいだけでなく、日常の業務によって追い付いていないのが実状である。このため、内部脅威の対策に様々なテクノロジーが登場しており、情報漏えい防止システム、ID アクセス管理システム、クラウドのセキュリティ、ログ解析、システム上の不審な活動を分析する SIEM（Security information and event management）などが多く使われている。内部脅威者への研究も進んでおり、企業に不満を抱える従業員がアクセス権を悪用することで業務妨害、機密情報の盗難、企業に対する詐欺行為に及んでいる。

政府や企業において多くの機密情報を持つ米国では、海外からのサイバー攻撃だけでなく内部からの脅威にもさらされている。IT の進化は目まぐるしく早く、攻撃手法も防御する方法もこれまでにないほど高度化している。しかしながらサイバーセキュリティの人材育成を同じ早さで行う方法はなく、将来を見据えた長期的な対応が求められている。組織における人材の育成を得意とする日本と違い人材の流動が激しい米国だが、

サイバーセキュリティの分野においては人材を企業にとどまらせ育成していくことに転換し始めている。新たな段階に進みつつある米国のサイバーセキュリティの人材育成を紹介する。

図表 1 はサイバーセキュリティ法案に関連したオバマ大統領・議会の様子である。

図表 1:サイバーセキュリティ情報共有法案(CISA)について言及するオバマ大統領(上)
CISA が通過したときの上院の様子(中)
2016 年予算法案に付帯されたサイバーセキュリティ法案に署名するオバマ大統領(下)

出典:Mashable、CommonDreams、US News[1]

[1] http://mashable.com/2015/12/17/congress-cisa-cybersecurity-omnibus/#iYxlWm5p7mqy
http://www.commondreams.org/news/2015/10/27/codifying-government-surveillance-senate-passes-cisa
http://www.usnews.com/news/articles/2015-12-18/obama-signs-cybersecurity-law-in-spending-package

2　サイバーセキュリティの市場

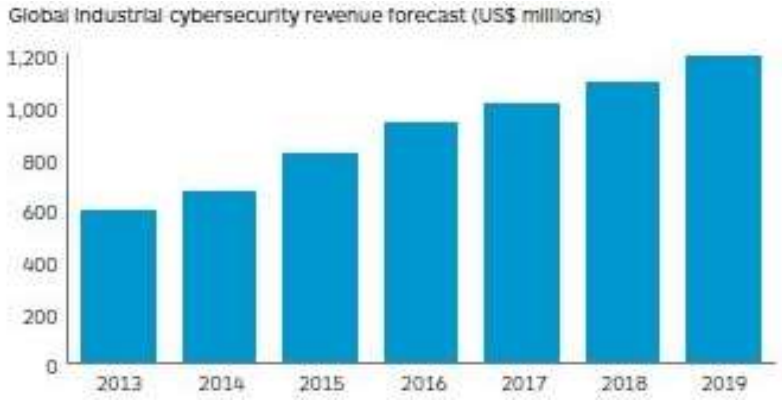
（1）　サイバーセキュリティの市場と動向

a.　サイバーセキュリティ市場

IT システムの重要性が増していることからサイバーセキュリティ市場はさらなる拡大が期待されている。米調査会社 MarketsandMarkets 社によれば、サイバーセキュリティの世界市場は 2015 年の 1063.2 億ドルから 2020 年には 1702.1 億ドルに達すると予測され、特に膨大な機密データを扱う政府機関、軍、自治体、金融、保険、ヘルスケアなど様々な分野でサイバーセキュリティへの投資が増えている。また対策別ではデータ暗号化、認証システム、脆弱性診断、DDoS 攻撃対策（分散型サービス妨害攻撃）などへの投資が増えており、ベンチャー企業への投資もクラウドやモバイルにおける革新的な技術を持つ企業に集まっている[2]。さらに、製造業におけるサイバーセキュリティ市場にも注目が集まっており、米調査会社 IHS 社によると産業システムにおけるサイバーセキュリティへの投資は 2013 年に 5 億 8,900 万ドルと製造業全体の 1%にも満たないことがわかっている。製造業のサイバーセキュリティ市場は 2019 年には 12 億ドルと 2013 年の 2 倍に達すると見ており、様々な面でサイバーセキュリティ市場の拡大が期待されている[3]。

図表 2 は、製造業におけるサイバーセキュリティ市場を示したグラフとなっている。

図表 2：製造業におけるサイバーセキュリティ市場



出典：IHS[4]

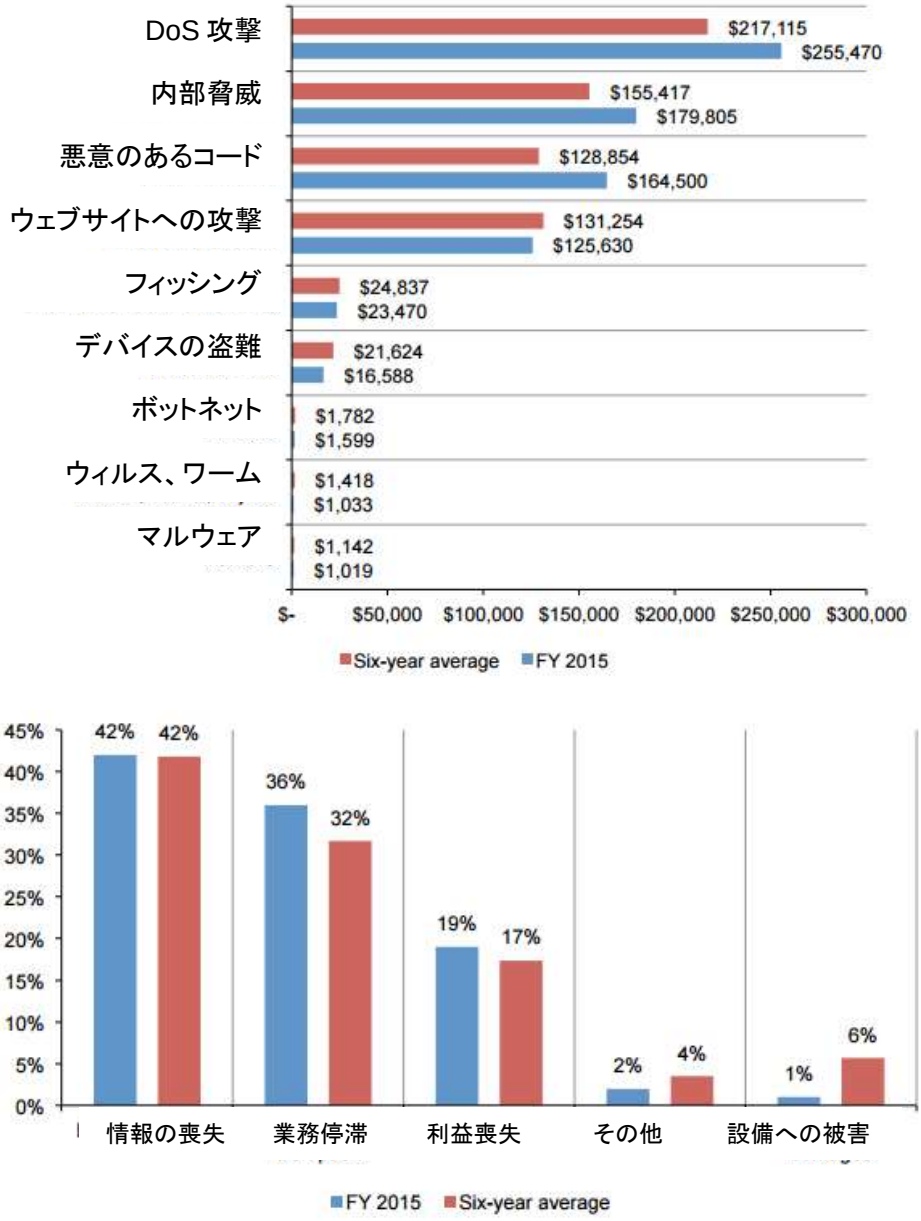
b.　サイバーセキュリティの動向

サイバー攻撃が高度化するに伴い企業への被害も大きくなっている。米サイバーセキュリティ専門シンクタンク Ponemon Institute 社の調査によると、米国のほぼ全ての企業がウィルスやマルウェアによるサイバー攻撃を受けており、53%が悪意のあるコード（malicious code）、43%が内部脅威、36%が DoS 攻撃（サービス妨害攻撃）を受けている。しかしながらサイバー攻撃による被害額で見た場合、ウィルスやマルウェアによる被害額は 1 社あたり年間 1,000 ドルほどで減少傾向にある一方、悪意のあるコード、内部脅威、DoS 攻撃による被害額は約 15 万～25 万ドルと非常に大きく増加傾向にある。また、被害の多くがデータの喪失や事業の停滞など直接的なものであり、高度なサイバー攻撃により企業に大きな被害をもたらす傾向が続いている[5]。

[2] http://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html
[3] http://blog.ihs.com/q23-the-brave-new-world-of-cybersecurity
[4] http://blog.ihs.com/q23-the-brave-new-world-of-cybersecurity
[5] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5208enw.pdf

図表 3 の上のグラフはサイバー攻撃による 1 件あたりの被害額を示したもので、下のグラフは被害の内容を示している（赤は 2010~2015 年の平均、青は 2015 年）。

図表 3：サイバー攻撃による 1 件あたりの被害額（上）と被害の内容（下）



出典：Ponemon Institute[6]

連邦政府機関におけるサイバー攻撃の被害も深刻化している。国土安全保障省（Department of Homeland Security：DHS）傘下の米コンピューター緊急対応チーム（United States Computer Emergency Readiness Team：US-CERT）に寄せられたサイバー犯罪の被害件数は、2006 年に 5,503 件だったものが 2014 年には 6 万 7,168 件と、8 年ほどで被害件数は約 11 倍に増加している[7]。

[6] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5208enw.pdf
[7] http://www.gao.gov/assets/670/669810.pdf p.6

図表 4 は、US-CERT を管轄する DHS の内部となっている。

図表 4：US-CERT を管轄する DHS の内部

出典：Council on Foreign Relations[8]

（2） サイバーセキュリティの労働市場

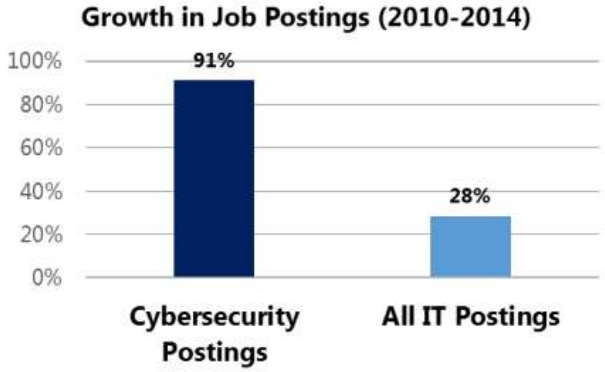
a. 需要が高まるサイバーセキュリティの人材

サイバーセキュリティの労働市場では、様々な形で人材の需要が高まっている。米人事コンサルティング BurningGlass 社によると、サイバーセキュリティの求人は IT 全体の 11%を占め、2010 年から 2014 年にかけて 91%の増加となっており、他の IT 関連の求人の 3 倍以上の伸びとなっている。最も人材の需要が高いのは専門サービス、金融保険、製造・防衛関連であり、過去 5 年で見ると金融分野、ヘルスケア、小売業での需要が伸びており、特に金融分野は需要が高く伸びも大きい。金融分野でサイバーセキュリティの人材の需要が埋まらない背景には、法律[9]によりサイバーセキュリティと金融の両方の知識とスキルを持つ人材を必要している点がある。この 2 つのスキルを同時に得る機会は非常に少ないため、企業が求める人材の需要と市場の供給に隔たりがあることが大きな理由の一つとなっている。この他サイバーセキュリティの求人全体の傾向として、業界団体が発行している技能認定証や豊富なキャリアを要件としているなど、労働市場の供給側がすぐには解消できない点が課題となっている[10]。

図表 5 はサイバーセキュリティ関連と IT 全体の求人数の増加率となっており、**図表 6** はサイバーセキュリティの分野別の求人数となっている。

[8] http://blogs.cfr.org/cyber/2015/07/20/the-challenges-facing-computer-security-incident-response-teams/
[9] 2002 年に制定されたサーベンス・オクスリー法（Sarbanes-Oxley Act：SOX 法）。企業の不正会計から投資家を保護することを目的に、企業に対して金融情報開示の強化などを定めた法律。
http://www.investopedia.com/terms/s/sarbanesoxleyact.asp
[10] http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

図表 5:サイバーセキュリティ関連と IT 全体の求人数の増加率



出典:BurningGlass[11]

図表 6:分野別のサイバーセキュリティ関連の求人数

	Industry Sector	求人数の割合	求人数	2010～2014 年にかけての増加率
専門サービス	Professional Services	37%	49,765	57%
金融、保険	Finance and Insurance	13%	17,873	131%
製造、軍事関連	Manufacturing & Defense*	12%	15,968	57%
公共機関	Public Administration	7%	9,725	N/A**
IT	Information	6%	8,522	65%
ヘルスケア	Health Care and Social Assistance	6%	7,915	118%
小売、流通	Retail Trade	3%	3,505	120%
その他	Other	15%	19,983	N/A**

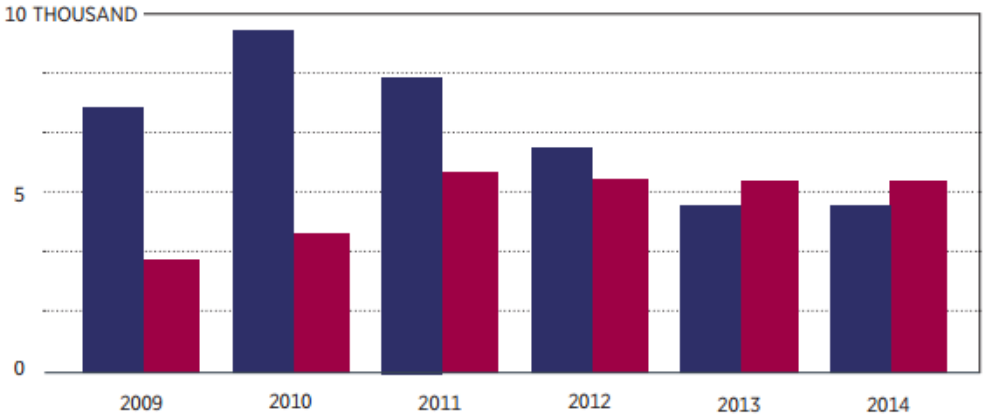
出典:BurningGlass[12]

連邦政府においてもサイバーセキュリティの人材不足が深刻となっている。連邦政府における情報セキュリティ技術者の数は政府全体で 9 万 2,863 人となっており、政府職員 22 人に 1 人が情報セキュリティ技術者となっている。2010 年までは退職者数よりも雇用者数の方が大幅に多かったものの、毎年雇用数者が減り続け、2014 年は雇用者数が 4,709 人に対して退職者数が 5,335 人と減少傾向となっている[13]。この背景には、現在のサイバーセキュリティの人材の需要が非常に高く、特に優秀な技術者は供給が少ない点があり、政府機関でも雇用のプロセスにかかる時間が最大 6 ヶ月と長すぎる点や、民間企業の給与が政府機関よりも 3 万ドル以上も高いなど様々な課題がある[14]。2015 年 4 月には、DHS がサイバーセキュリティの人材を確保するためにシリコンバレーに事務所を開くなど、サイバーセキュリティの人材確保のために様々な取り組みを進めている[15]。

図表 7 は連邦政府におけるサイバーセキュリティの人材の雇用者数と退職者数を示したグラフで、青が雇用者数、赤が退職者数となっている。

[11] http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
[12] http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
[13] http://www.federalnewsradio.com/wp-content/uploads/pdfs/pps_cyber.pdf
[14] https://news.clearancejobs.com/2015/04/28/government-agencies-still-struggle-cybersecurity-talent/
[15] http://www.reuters.com/article/cybersecurity-rsa-dhs-idUSL1N0XI1NY20150421

図表 7:連邦政府におけるサイバーセキュリティの人材の雇用者数と退職者数



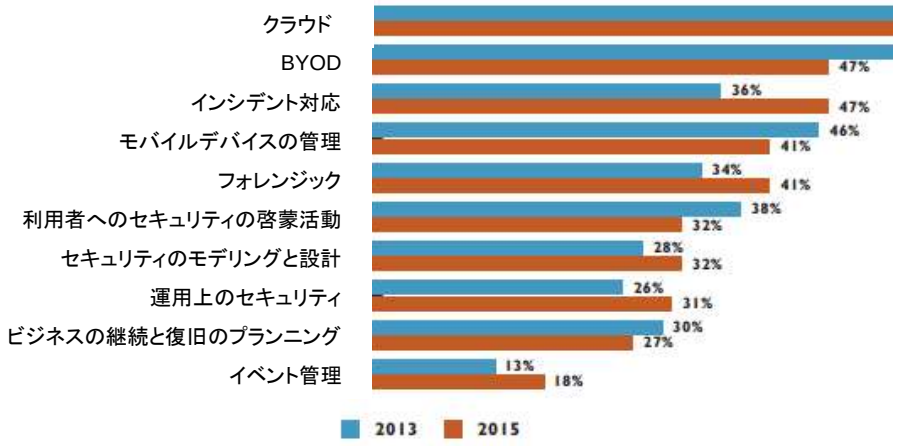
出典:Booz Allen Hamilton[16]

b. 市場で求められる人材

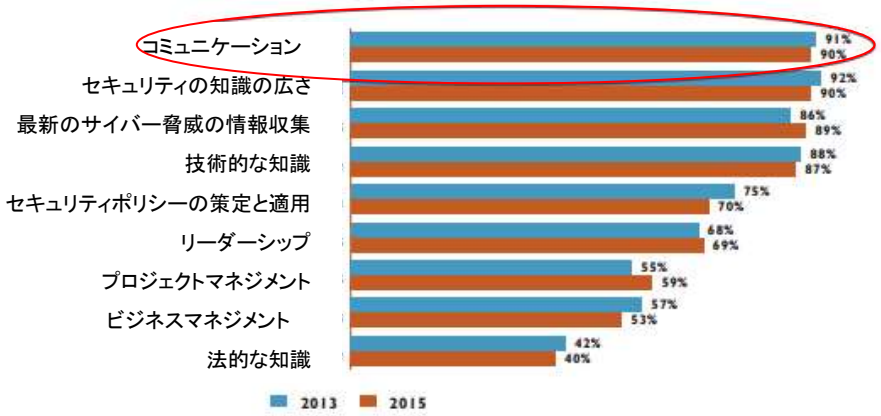
米コンサルティング企業 Frost & Sullivan 社が企業に対して行った聞き取り調査では、北米におけるサイバーセキュリティ関連の職業の収入は年収 12 万ドル以上が 38%を占め、年収 10 万ドル以上で 61%となっており、需要に対して供給が追いついていないことを示している。技術的な面では今後 3 年でクラウド、BYOD[17]、インシデント対応、リスクマネジメントに対する需要が高まると多くの企業が回答しているが、企業は情報セキュリティ技術者に対してコミュニケーション能力など個人のソフトスキルも重要視している[18]。企業のセキュリティ担当者は情報漏えいが起きた場合などに法務部や重役と連携して動く必要があるため、技術的な面だけでなく様々な役割をこなすためのソフトスキルが必要とされるためである[19]。

図表 8 の上のグラフはセキュリティの需要が予想される分野となっており、下のグラフは企業が技術者に求めるスキルとなっている。

図表 8:セキュリティの需要が予想される分野(上)と技術者に求めるスキル(下)



[16] http://www.federalnewsradio.com/wp-content/uploads/pdfs/pps_cyber.pdf
[17] Bring Your Own Device。個人のモバイルデバイスを業務で使用することを指す。
[18] https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf p.20
[19] http://www.computerworlduk.com/blogs/infosecurity-voice/security-awareness-is-not-enough-stop-people-taking-risks-3605901/



出典:Frost & Sullivan[20]

（3） 企業が求める資格認証

企業は、求めるサイバーセキュリティの人材に資格認証（Certification）を求めることが多く、資格認証の重要性が増してきている。米国における IT 関連の求人の 23%で資格認証を要件とする一方、サイバーセキュリティの求人では 35%と資格認証を重要視する傾向がある。サイバーセキュリティの資格認証は非営利団体や企業などから出されており、**図表 9** は主なサイバーセキュリティ関連の資格認証となっている。

図表 9:主な資格認証

レベル	資格名	概要
基礎レベル	Security+	ネットワークからクラウドまで情報セキュリティの基礎的な内容を幅広く扱う。IT 関連の資格認定を行う業界団体 CompTIA が提供している。
	GIAC Security Essentials (GSEC)	情報セキュリティの業務で必要とされる主に技術的な面での基礎スキルを扱う。情報セキュリティのトレーニングを提供する SANS Institute 社による資格認証。
	Certified Information Privacy Professional (CIPP)	情報プライバシーに関する資格認証であり、法規制、プライバシーの概念、データの取り扱いなどを対象とする。情報プライバシーの非営利組織 IAPP が提供する。
	Systems Security Certified Practitioner (SSCP)	1 年以上の実務経験を必要とし、モニタリングやインシデント対応など、情報セキュリティの業務に必要な知識とスキルを扱う。サイバーセキュリティの資格認定とトレーニングを提供する非営利組織(ISC)²が提供。
上級（3～5 年の実務経験）	Certified Information Systems Security Professional (CISSP)	需要の高い資格認証であり、5 年以上の実務経験を必要とする。リスク管理、セキュリティ評価、監査、ID アクセス管理など 8 つの分野を扱う。(ISC)²が提供。
	Certified Information Systems Auditor (CISA)	情報システム監査、セキュリティ、システム管理に関する資格認証であり、5 年以上の実務経験が必要。情報システム監査・情報セキュリティの専門家団体 ISACA が提供。
	Certified Information Security Manager (CISM)	マネジメントレベルの情報セキュリティに関する資格認証であり、セキュリティガバナンス、コンプライアンス、インシデント管理などを対象とする。ISACA が提供。

[20] https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

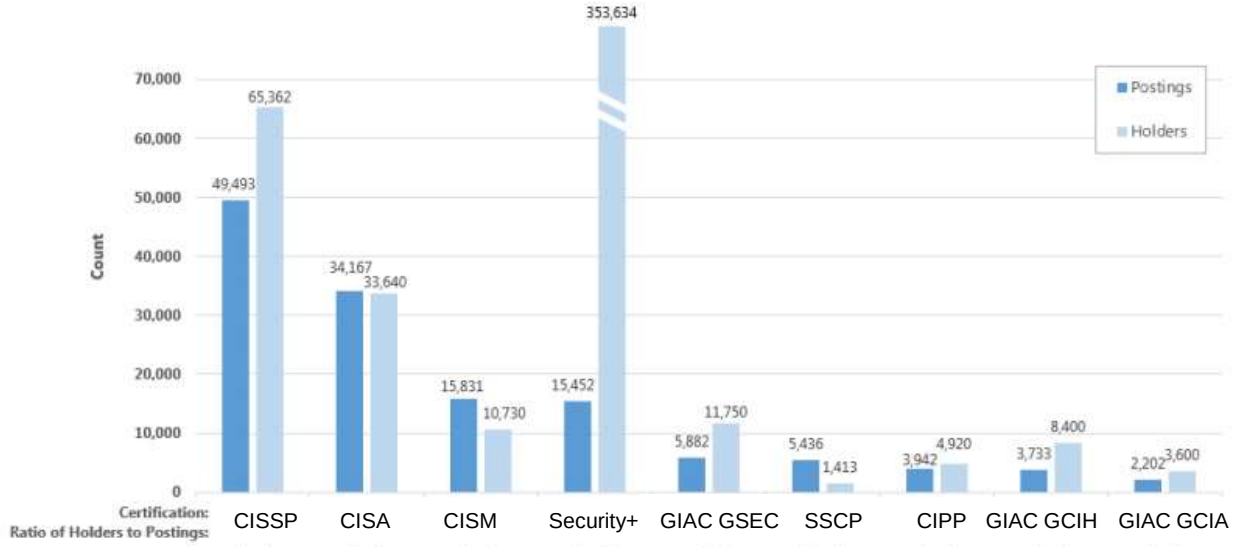
	GIAC Certified Incident Handler (GCIH)	インシデント対応に特化した資格認証であり、サイバー攻撃の検知、攻撃手法の熟知、脆弱性の分析などを扱う。SANS Institute 社が提供。
	GIAC Certified Intrusion Analyst (GCIA)	侵入検知に特化した資格認証であり、侵入検知システムの知識や通信トラフィックの分析などを扱う。SANS Institute 社が提供。

出典：各種情報を基に作成[21]

これらの資格認証の中でも特に需要が高いのが CISSP であり、2014 年全体のサイバーセキュリティの求人全体の 21%にあたる 4 万 9,493 件が CISSP を要件にしている。CISSP の保有者は 2015 年 7 月現在 6 万 5,362 人だが、多くはすでにサイバーセキュリティの職に就いていると見られるため、実際には CISSP を要件とする求人数に対し同認証の保有者が大きく足りていないと考えられる。Security+は保有者数が 35 万 3,634 人に対し要件とする求人数は 1 万 5,452 件と極端に少ないが、これは未経験者が基礎知識をつけるために Security+を取る場合が多く、企業も評価基準に入れないことが多いためである[22]。また、同じ役職であっても資格認証を持っている場合には給与が約 20%高いなど、企業が資格認証を重視する傾向がうかがえる[23]。

図表 10 は、サイバーセキュリティ関連の求人数と資格認証の保有者数を示したもので、青が求人数、水色が資格認証の保有者数となっている。なお、求人数については 2014 年全体のものであるが、資格認証の保有者数の時期は認定団体によって異なる。

図表 10：サイバーセキュリティ関連の 2014 年の求人数と資格認証の保有者数



出典：BurningGlass[24]

[21] https://certification.comptia.org/certifications/security
https://www.giac.org/certification/security-essentials-gsec
https://iapp.org/certify/cipp
https://www.isc2.org/sscp/default.aspx
https://www.isc2.org/cissp/default.aspx
http://www.isaca.org/certification/cism-certified-information-security-manager/pages/default.aspx
https://www.giac.org/certification/certified-intrusion-analyst-gcia
https://www.giac.org/certification/certified-incident-handler-gcih
[22] http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf
http://www.csoonline.com/article/3021031/it-careers/which-certifications-matter-most-for-those-new-to-security.html
[23] https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf p.18
[24] http://burning-glass.com/wp-content/uploads/Cybersecurity_Jobs_Report_2015.pdf

これらの資格認証は政府の調達にも役立てられている。国防総省（Department of Defense：DoD）は、政府職員や民間業者が機密性の高いデータを使った業務に就く場合には、対応した資格認証を求めている。これらの資格認証は DoD が求める基準 DoD Directive 8570.1 に基づいて作られており、DoD と民間の組織が連携することで資格認証が DoD の求める人材の育成に活用されている[25]。

3　サイバーセキュリティの人材育成の取り組み

（1）　民間の取り組み

a.　クロス・トレーニングの活用

民間企業はサイバーセキュリティの人材の確保と育成に様々な取り組みを進めている。米軍需企業 Lockheed Martin 社ではサイバーセキュリティの人材育成のために、数年前から 1,600 人のセキュリティ関連の従業員に複数の業務を経験させるクロス・トレーニングを実施している。クロス・トレーニングは異なる業務を経験させてセキュリティ技術の幅を広げることを目的したものである。例えば、セキュリティアナリストのチームから 1 人を防衛、諜報、国際取引、顧客関係などの異なる部署へ異動させることで、新しい環境下でサイバーセキュリティのコンピュータ・フォレンジクスや情報保証につながる知識を学ばせ、セキュリティ技術の幅を広げることができる[26]。

また、同社では独自の情報センターで業務とトレーニングを組み合わせた取り組みを進めている。同社は世界中にセキュリティの分析を行うセキュリティ情報センター（Security Intelligence Centre）を設置している。ここでは新入社員にトレーニングや、防衛関連などの業務に就かせることでセキュリティの技術を磨いている。諜報活動などより高度なセキュリティの業務に就くために、必要に応じて国家の機密情報にアクセスするための資格であるセキュリティ・クリアランス（Security clearance）を取得させている。これらの取り組みは、業務の中にトレーニングを統合させることで持続的なスキルアップを目指した同社の人材育成方法を示したものとなっている[27]。

図表 11 は Lockheed Martin 社のセキュリティ情報センターとなっている。

図表 11：Lockheed Martin 社のセキュリティ情報センター

出典：Lockheed Martin[28]

[25] https://www.isc2.org/dod-8570/default.aspx
https://www.isc2.org/dodmandate/default.aspx
[26] http://www.afcea.org/content/?q=Article-cross-training-empowers-cyber-experts
[27] http://www.afcea.org/content/?q=Article-cross-training-empowers-cyber-experts
[28] http://www.lockheedmartin.com/us/news/features/2013/fighting-cyber-threats-with-a-fleet-of-security-intelligence-cen.html

クロス・トレーニングはすでに複数の企業で活用されており、カナダの IT 企業 Herjavec Group 社はクロス・トレーニングを活用して人材を育て、サイバーセキュリティの分野で急成長した成功例となっている。2003 年に設立した同社はセキュリティの製品とサービスを提供していたが、成長とともに IT サービス企業を買収し事業を拡大していった。事業拡大の中で同社がストレージサービスを始める際には、セキュリティを固めるために買収した企業の技術者をサイバーセキュリティ部門へ異動させ、クロス・トレーニングにより情報セキュリティ技術者を育成する方法を取った。これにより同社はセキュリティの人材を充実させ、カナダでも有数のセキュリティサービス事業者（MSSP）となり、現在は米国やヨーロッパへと展開している[29]。

b. シミュレーションツール

サイバーセキュリティのトレーニングのためのシミュレーターを提供する企業が出てきている。米ベンチャー企業 root9b 社はセキュリティのための様々なツールを提供しており、その中の 1 つである DAEDALUS はサイバーセキュリティのトレーニング用ツールとなっている。同ツールはユーザーの環境下で様々なシナリオのサイバー攻撃を再現できるツールであり、サイバー攻撃をシミュレーションすることでネットワークの設計の不備やシステムの脆弱性を確認することが出来る。また、コンピュータ・フォレンジクス（コンピュータ法科学）[30]などにも使用できるため、様々なシステムの運用における情報セキュリティ技術者のトレーニングや戦略の立案なども可能となっている[31]。同社は DHS や米航空機製造 Boeing 社と契約を結んでおり、DAEDALUS を含むセキュリティツールを提供している[32]。

スペインの IT 企業 Indra 社では、IoT のセキュリティシミュレーションが可能なシステムを提供している。2015 年 11 月に発表された同社の iPhalanx は様々なサイバー攻撃を再現できるツールであり、サイバー攻撃や侵入の検知、コンピュータ・フォレンジクス、セキュリティの評価などを行うことができる。iPhalanx は実際のセキュリティ指令センターなどの情報を集めた最新の攻撃手法が組み込まれており、国立標準技術研究所（National Institute of Standards and Technology：NIST）が提供する最新の脆弱性に関するデータベースの情報を取得することが可能となっている。iPhalanx の大きな特徴は IoT のシミュレーションにも使用できる点であり、モバイルデバイスや IoT デバイスをエミュレーター[33]としてシステム上で稼働させシナリオに組み込むことが可能である。iPhalanx はすでに複数の大学で使用されており、セキュリティのトレーニングに効果的であると注目を集めている[34]。**図表 12** は、Indra 社のセキュリティ指令センターとなっている。

図表 12：Indra 社のセキュリティ指令センター

出典：ZDNet[35]

[29] http://www.csoonline.com/article/2938567/data-protection/robert-herjavec-cybersecurity-company.html
[30] 電子記録媒体などからデータの復元や解析を行なう技術。
[31] http://www.prnewswire.com/news-releases/root9b-announces-daedalus--the-next-generation-cyber-range-300095972.html
[32] http://boeing.mediaroom.com/Boeing-and-root9B-Partner-to-Offer-In-depth-Cybersecurity-Training
http://www.cbsnews.com/news/former-nsa-intel-officials-take-new-approach-to-cyber-defense-at-root9b/
[33] コンピューター上で実際の機械の動作を模倣するソフトウェア。
[34] http://www.zdnet.com/article/from-iot-threats-to-forensics-how-this-simulator-is-helping-sharpen-cybersecurity-skills/
[35] http://www.zdnet.com/article/from-iot-threats-to-forensics-how-this-simulator-is-helping-sharpen-cybersecurity-

c. サイバーセキュリティ関連のベンチャー企業

ベンチャー企業の中には独自の方法でサイバーセキュリティの人材を探し、企業へ優秀な人材を紹介するサービスを提供している社もある。ベンチャー企業 HackerRank 社では、同社のウェブサイト上で求職中のエンジニアに対しコーディング（プログラミング）技術をテストし、企業が求めるスキルにマッチした人材を紹介している。すでに世界中から 100 万人以上のエンジニアがテストを受けており、同社を利用して人材を探す企業の中には米投資会社 Goldman Sachs 社、米 IT 企業 Amazon 社、米大手小売 Wal-Mart 社などがいる。優秀な人材を素早く探す必要のあるサイバーセキュリティの分野などで活用が期待されている[36]。

Cybrary 社はサイバーセキュリティのオンライン講座を無料で提供しており、企業が優秀な人材にコンタクトできるようになっている。通常 3,000 ドルから 5,000 ドルかかるサイバーセキュリティのオンライン講座を無料で提供することで話題を集め、開設からわずか 8 ヶ月で約 16 万人のユーザーが同社のサービスを利用している。同社のビジネスモデルは企業からサイバーセキュリティのコンテンツを集め、スポンサーとなった企業にはユーザーへのコンタクトの機会を与えている。女性エンジニアを支援する非営利組織 Women in Technology と提携するなど、様々な面から人気を集めている[37]。

図表 13 は、Cybrary 社のオンライン講座となっている。

図表 13：Cybrary のオンライン講座

出典：CIO[38]

skills/

[36] http://www.cnbc.com/2015/05/12/the-cybersecurity-talent-war-you-dont-hear-about.html
http://www.cnbc.com/2015/05/12/resumes-a-thing-of-the-past-hackerrank-hopes-so.html

[37] http://thedailyrecord.com/2015/01/13/cybrary-it-launches-free-it-training-platform/
http://www.cio.com/article/2975324/demo/traction-watch-cybrary-helps-fill-gap-of-1-million-unfilled-cyber-security-jobs.html

[38] http://www.cio.com/article/2975324/demo/traction-watch-cybrary-helps-fill-gap-of-1-million-unfilled-cyber-security-jobs.html

（2） 政府による取り組み

a. 連邦政府

連邦政府は政府機関や軍事関連のセキュリティを向上させるために、サイバーセキュリティの人材育成を積極的に進めている。2015 年 3 月、オバマ大統領は IT 分野のエンジニアを増やすことを目的に教育と雇用環境を整備する TechHire イニシアチブを発表した。このイニシアチブでは、①企業と提携し必要な人材のマッチング、②若い世代のトレーニングに 1 億ドルの投資、③需要の高い分野への民間企業のトレーニングサービスの導入、の 3 つを柱としている。具体的には IT に関連した雇用とトレーニングの機会を提供するコミュニティを都市に形成するというもので、地域の企業との雇用プログラムの立ち上げや学生向けに数ヶ月の集中短期トレーニングを提供する。同イニシアチブの立ち上げ時には 300 社の企業と 20 都市が参加を表明した[39]。2015 年 11 月には同イニシアチブの成果が公表され、14 都市でコミュニティが立ち上げられたという[40]。

図表 14 は TechHire イニシアチブを発表するオバマ大統領となっている。

図表 14：TechHire イニシアチブを発表するオバマ大統領

出典：National League of Cities[41]

2015 年 11 月には大統領府から連邦政府機関の新しいセキュリティガイドラインとして Cybersecurity Strategy and Implementation Plan が発表された。これは同年 6 月に発生した人事管理局（Office of Personnel Management：OPM）の大規模な情報流出を受けて出されたもので、機密情報を保護しサイバー攻撃に対して素早い検知、対応、復旧を 13 省庁に求める内容となっている。さらにサイバーセキュリティの人材を確保するために新しいガイドラインの策定と、不足している分野についてまとめることが求められた[42]。OPM はこの要請を受けて 2015 年 11 月、人材が不足しているサイバーセキュリティの分野の報告を各省庁に要請しており、回答を受けて人材確保に動くこととなる[43]。

[39] https://www.whitehouse.gov/the-press-office/2015/03/09/fact-sheet-president-obama-launches-new-techhire-initiative
[40] https://www.whitehouse.gov/the-press-office/2015/11/17/fact-sheet-white-house-and-department-labor-launch-100-million-techhire
[41] http://citiesspeak.org/2015/03/09/what-obamas-new-techhire-initiative-can-do-for-cities/
[42] https://www.whitehouse.gov/sites/default/files/omb/memoranda/2016/m-16-04.pdf
[43] https://www.chcoc.gov/content/special-cybersecurity-workforce-project

b. 政府機関

不足するサイバーセキュリティの人材を補うために、様々な形で即戦力となる人材の育成も進められている。2010 年に立ち上げられた National Cybersecurity Workforce Framework（NICE）は、サイバーセキュリティの人材育成を国家課題として連邦政府機関が協力して教育プログラムを提供するイニシアチブとなっている。NICE は、NIST を中心として合計 20 省庁が参加している。同イニシアチブでは以下の取り組みが進められている[44]。

- サイバーセキュリティの啓蒙活動：DHS の主導で進められる。サイバーセキュリティやインターネットの利用について理解を深め、教育やキャリアパスにつながる啓蒙活動を行う。

- サイバーセキュリティの教育：国立科学財団（National Science Foundation：NSF）と教育省（Department of Education：DoED）の主導で進められる。サイバーセキュリティに関連した授業やプログラムを、義務教育、高等教育、職業訓練プログラムまで幅広く提供する。

- サイバーセキュリティの人材確保：DHS、OPM、DoD、労働省（Department of Labor：DoL）が中心となって進める。この中でも特に DHS 内に設置されている National Initiative for Cybersecurity Careers and Studies（NICCS）が中心となって雇用対策を進める。NICCS では、キャリアを構築したい人のためにオンラインや教室でのトレーニングプログラムを提供し、政府機関向けにもオンラインコースを用意している[45]。

また DHS では産業分野に特化したサイバーセキュリティのトレーニングの機会を提供している。産業制御システムを中心とした情報セキュリティを扱う DHS 傘下の ICS-CERT（Industrial Control Systems Cyber Emergency Response Team）では、実践的な産業制御システムのサイバーセキュリティトレーニングを提供している。このトレーニングは 5 日間にわたって行なわれ、重要インフラのオペレーター、マネジメント、ソフトウェア開発者など産業制御システムに携わる人を対象とした内容となっている。トレーニングの 1 日目と 2 日目は基礎的な内容やセキュリティツールの使い方を学び、3 日目からは 40 人の参加者が 2 チームに分かれサイバー攻撃からの防御方法を練習する。4 日目はさらに実践的な内容であり、2 チームが攻撃側と防御側となり様々なツールを使って攻撃と防御の両方を実践することとなる。最終日にはまとめとしてディスカッションが行なわれる。この 5 日間にわたるトレーニングの費用は無料であり、内容の質の高さから注目が集まっている[46]。

c. 関連団体

大学と連携してサイバーセキュリティの研究を進める企業も出ている。連邦政府の支援により運営される非営利組織 MITRE は IT を含む様々なテクノロジーを研究する機関であり、2014 年 10 月からはメリーランド大学と連携してサイバーセキュリティの研究を進めている。この取り組みは、NIST が進める官民連携のサイバーセキュリティ研究開発 National Cybersecurity Center of Excellence（NCCoE）の一環として MITRE が選定されたもので、研究拠点はパートナーシップを結んだメリーランド大学内に設置される。またこの研究開発は、連邦政府が支援する連邦研究開発センター（Federally funded research and development center：FFRDC）の 1 つであり、FFRDC の 43 の研究開発の中でも初のサイバーセキュリティの研究開発として注目を集めている[47]。メリーランド大学以外にもデラウェア大学（University of Delaware）をはじめとする 9 大学と共同研究していくことが発表されており、官学連携によるサイバーセキュリティ研究が始まっている[48]。

[44] https://www.fbcinc.com/e/nice/about.aspx
[45] https://niccs.us-cert.gov/education/education-home
[46] https://secure.inl.gov/icsadv0416/
[47] http://www.mitre.org/news/press-releases/mitre-partners-with-university-system-of-maryland-to-operate-new-cybersecurity
[48] http://www.udel.edu/udaily/2015/oct/cybersecurity-affiliates-102814.html

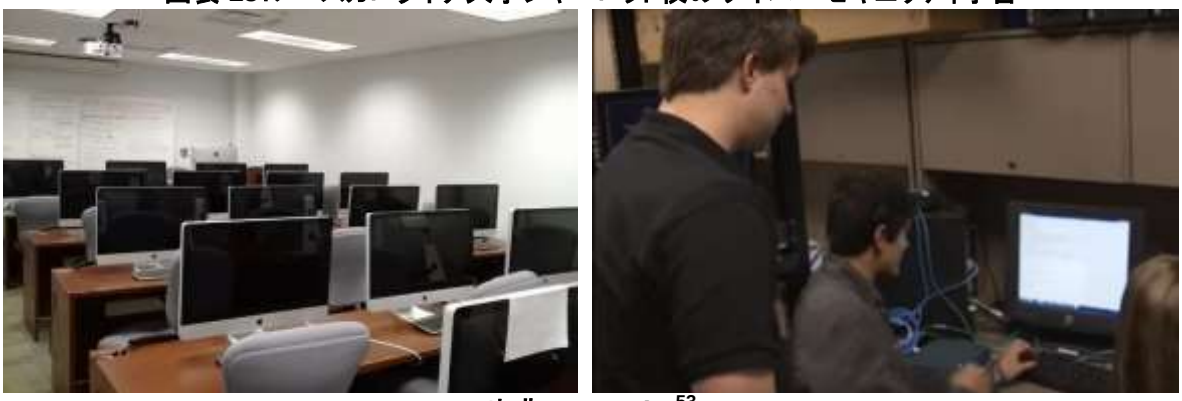
（3） 教育機関の取り組み

連邦政府は大学機関と協力してサイバーセキュリティの学習機会を高める取り組みを進めている。防衛関連企業 Ryathon 社の調査によると、若い世代の 43%がサイバーセキュリティの学習機会が得られず、61%がサイバーセキュリティの仕事そのものについて知らないということがわかっており[49]、大学からサイバーセキュリティのキャリアパスを用意する取り組みが始まっている。DHS と国家安全保障局（National Security Agency：NSA）は共同でサイバーセキュリティの研究開発と教育を大学機関へ促進する National Centers of Academic Excellence（CAE）を設置している。CAE では情報保障（Information assurance）、サイバーディフェンス、サイバーオペレーションの 3 つの分野で大学機関に研究と教育プログラムのサポートを提供しており、この中のサイバーオペレーションは上記の NICE イニシアチブの一環となっている[50]。

CAE を通してサポート受けている大学の 1 つであるノースカロライナ大学シャーロット校（University of North Carolina at Charlotte）では、CAE のサポートによりサイバーセキュリティのカリキュラムと研究施設を充実させている。カリキュラムでは学士から博士号までサイバーセキュリティの学位を用意しており、授業用ラボとしてコンピュータ・フォレンジクスのための施設が整った Computer Forensics Lab や様々なメーカーのネットワーク機器やサーバーが設置された IT Infrastructure Lab が用意されている。また、サイバーセキュリティ研究センターCyberDNA ではセキュリティ技術について様々な研究が行われている[51]。この他、CAE では 2014 年 7 月にニューヨーク大学（New York University）など 5 校が参加し、生徒と教師が NSA で研修を受けるインターンシップの機会が与えられるなど、様々な支援が行なわれている[52]。

図表 15 は、ノースカロライナ大学シャーロット校のサイバーセキュリティ学習の様子となっている。

図表 15：ノースカロライナ大学シャーロット校のサイバーセキュリティ学習



出典：YouTube[53]

49 https://www.staysafeonline.org/download/datasets/16847/Securing%20Our%20Future%20Closing%20the%20Cybersecurity%20Talent%20Gap.pdf

50 https://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml
https://www.nsa.gov/academia/nat_cae_cyber_ops/index.shtml

51 http://sis.uncc.edu/academics/cyber-security-academic-program

52 https://www.nsa.gov/public_info/press_room/2014/cyber_ops_ctrs_of_excellence.shtml

53 https://www.youtube.com/watch?v=E3eIUibwuhI&feature=youtu.be

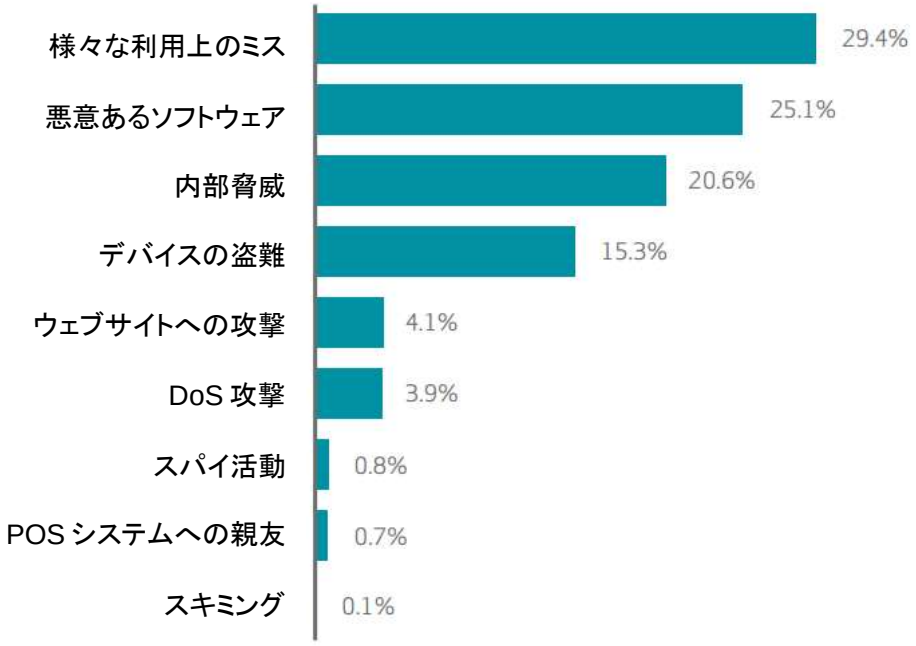
4　内部脅威への取り組み

（1）　内部脅威の動向

内部脅威による被害は大きいものの、様々な理由により対策が進んでいない。米大手通信会社 Verizon 社がサイバーセキュリティと情報漏えいについてまとめたレポート「Verizon 2015 Data Breach Investigations Report」によると、2014 年に発生したセキュリティインシデント[54]は世界全体で 7 万 9,790 件にのぼり、その中で内部関係者の犯行によるセキュリティインシデントは 3 番目に多く全体の 20.6%を占めていた[55]。米サイバーセキュリティ専門シンクタンク Ponemon Institute の調査では、内部脅威による被害額も 1 件あたり約 18 万ドルとサイバー攻撃と並んでおり（**図表 3** 参照）、被害の回復までにかかる日数はサイバー攻撃よりも長い、平均 68.9 日となっている[56]。

図表 16 は 2014 年に発生したセキュリティインシデントを示したグラフであり、**図表 17** はサイバー攻撃ごとの問題解決にかかる日数（赤は 2010~2015 年の平均、青は 2015 年）を示したグラフとなっている。

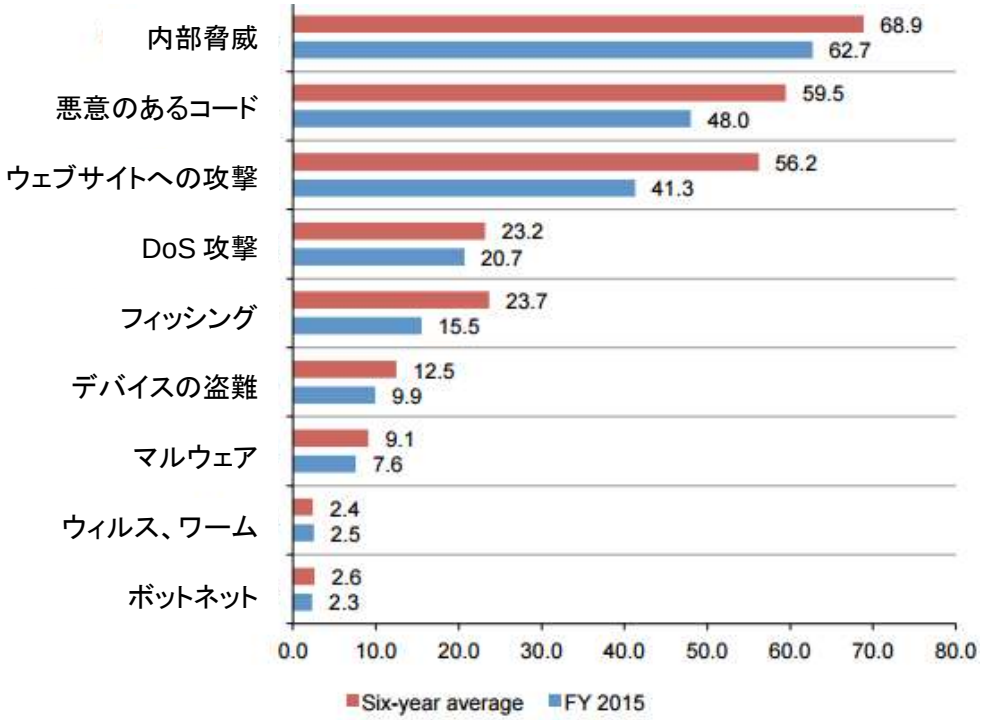
図表 16：2014 年に発生したセキュリティインシデント



出典：Verizon[57]

[54] ここではシステムや情報資産の侵害などの被害につながるサイバーセキュリティ関連の事故を指す。
[55] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf p.3
[56] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5208enw.pdf
[57] http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigation-report-2015_en_xg.pdf

図表 17:サイバー攻撃ごとの問題解決にかかる日数



出典:Ponemon Institute[58]

しかしながら内部脅威者への対応に際しては様々な業務上の問題が出ており、その中には多すぎるアクセス権の変更要請(62%)、例外扱いなど一貫性のないアクセス権の承認(45%)、セキュリティソフトの値段(30%)、アクセスの認証や監視の困難さ(29%)などにより内部脅威者への対応が困難になっているという[59]。米連邦政府においても内部脅威はセキュリティ上の重要な課題となっており、米ソフトウェア開発企業 SolarWinds 社が連邦政府内の IT 担当者に聞き取り調査した内容によると、64%の担当者が外部からのサイバー攻撃よりも内部脅威による被害の方が大きいと回答している。しかしながら、内部脅威への対策に取り組んだのは半数以下の 46%にとどまっており、内部脅威に対する対策が後回しになっている背景には以下のような問題が浮かび上がっている[60]。

- 多すぎるネットワーク通信量(40%)
- 職員に対するセキュリティトレーニングの不足(35%)
- クラウドの利用増加(35%)
- システム変更の頻度が多くセキュリティ対策に追われる(34%)
- モバイルデバイスの利用増加(30%)
- 対策ソフトが高価(27%)
- BYOD の利用増加(27%)

(2) 内部脅威を防ぐテクノロジー

内部脅威に備えたソフトウェアやシステムは、様々な種類のものが代表的なセキュリティ企業から登場している。US-CERT によると、内部脅威の 71%が企業内のネットワーク経由での犯行であり、続いて端末の盗

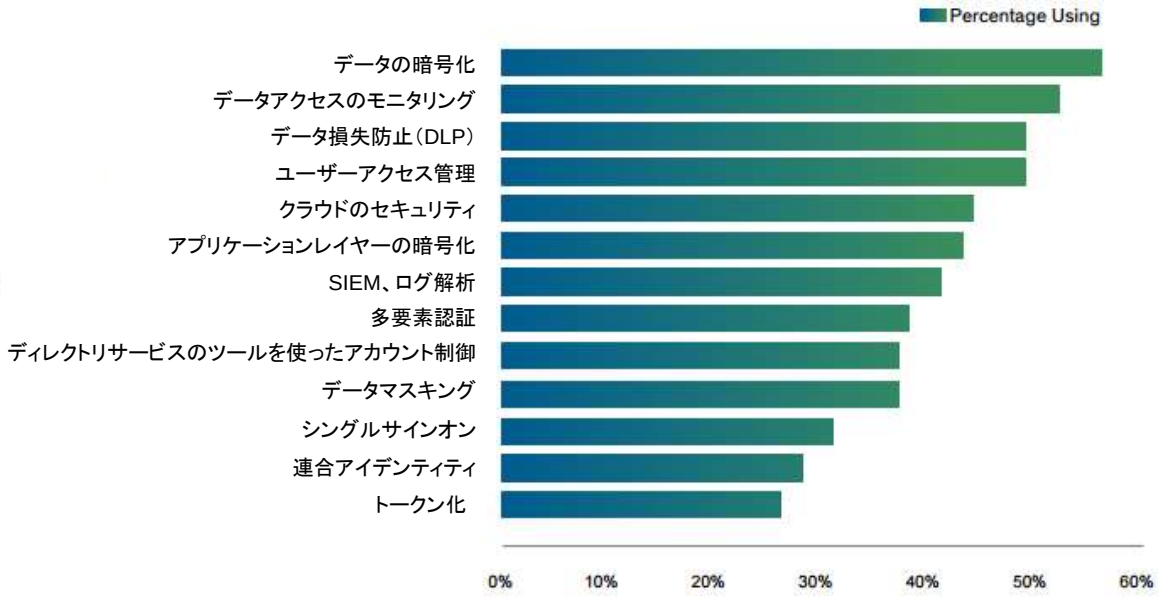
[58] https://ssl.www8.hp.com/ww/en/secure/pdf/4aa5-5208enw.pdf
[59] http://www.raytheoncyber.com/rtnwcm/groups/cyber/documents/content/rtn_257010.pdf p.6～p.8
[60] http://www.solarwinds.com/company/newsroom/press_releases/threats_to_federal_cybersecurity.aspx

難など物理的接触による犯行（28%）、外部からのリモート接続（21%）となっている[61]。このためネットワークやデータに関連した対策に力を入れる企業が増えており、セキュリティ企業 Vormetric 社の調査では企業の 7 割以上がネットワークの監視、データ利用の追跡、データ管理時の対策が内部脅威に有効であると回答し、特にデータ関連の内部脅威対策に対しては半数近くの企業が投資を増やしていくと回答している[62]。

内部脅威の対策として多く使用されているテクノロジーにはデータの暗号化、データへのアクセス管理、機密情報を外部へ送らないようにする情報漏えい防止（Data Loss Prevention：DLP）システム、ID のアクセス管理システムなどがあり、これらは半数以上の企業で利用されている。この他、クラウドのセキュリティ、ログ解析やシステム上の不審な活動を分析する SIEM（Security information and event management）などのテクノロジーが内部脅威対策に利用されている[63]。

図表 18 は、内部脅威の対策に使用されるテクノロジーとなっている。

図表 18：内部脅威の対策に使用されるテクノロジー



出典：Vormetric[64]

（3） 内部脅威の特徴

内部脅威に対する研究も進んでおり、組織内の活動から内部脅威へつながるプロセスがわかっている。カーネギーメロン大学（Carnegie Mellon University）内に設置されているコンピューター緊急対応チーム（Computer Emergency Readiness Team：CERT）では 2002 年から内部脅威に関する研究を進めており、内部脅威を様々な角度から分析したレポートを公表している。本レポートの中で同チームは、IT を使った内部脅威を①業務妨害、②知的財産の盗難、③企業に対する詐欺行為の 3 つに分類し、それぞれに組織内

[61] https://www.us-cert.gov/sites/default/files/publications/Combating%20the%20Insider%20Threat_0.pdf
[62] http://blog.vormetric.com/2015/01/30/top-3-surprising-results-from-the-2015-vormetric-insider-threat-report/
[63] http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf
[64] http://enterprise-encryption.vormetric.com/rs/vormetric/images/CW_GlobalReport_2015_Insider_threat_Vormetric_Single_Pages_010915.pdf

の活動から内部脅威へつながるプロセスを示した MERIT モデル（Management and Education of the Risk of Insider Threat Model）を構築している[65]。以下は 3 つの内部脅威の発生プロセスとなっている。

①業務妨害

内部脅威による業務妨害はほぼすべての重要インフラに関わる企業・組織で発生しており、IT システムにアクセス権のある管理者やエンジニアが企業を解雇または退職した後に犯行が及ぶケースが多く見られた。内部脅威者は組織に何らかの不満を持っており、組織内でのトラブルが重なることでストレスを募らせ、犯行への引き金となっている。犯行前にはシステムへの細工など不審な行動が見られるため、内部脅威者の挙動やシステムを監視することで兆候をつかむことができるとしている。一方で、内部脅威の兆候を見つけても従業員への過大な信頼によって兆候を無視してしまうトラストトラップと呼ばれるケースにおちいることもある[66]。

行動	内容
期待した待遇を得られないことへの不満	個人の性格から様々な欲求が内部脅威者の期待へと変化するが、期待が実現すると次の欲求が生まれて新しい期待へと変化する。期待が実現している間は新しい期待と実現の繰り返しとなるが、期待した内容が得られない場合は不満へと変化することとなる。
兆候とストレスの増大	内部脅威者が持つ不満は従業員の行動の中で兆候として、他の従業員とのトラブル、急な欠勤、遅刻、早退、仕事の能率低下といった形で現れる。その兆候に対してアクセス権の剥奪や降格など不適切な制裁をすると、新たな不満を生み出し、内部脅威者の不満を増大させる。
犯行の準備	内部脅威者が企業への妨害工作を実行する際には、事前に何らかの技術的な準備から進めることが多い。中には攻撃時の被害を拡大させるためにデータのバックアップを故意に行わないといったものがあり、企業はこれらを内部脅威の兆候として利用することが出来る。 例：ハッキング用ツールのダウンロード、侵入用のバックドアアカウントの設定の失敗、職場での不適切なインターネット接続、解雇・契約終了後のシステムへの接続、侵入用のバックドアアカウント、パスワード解析ソフトのインストール、リモート接続ツールのインストール、コンピューター端末の脆弱性の探索
トラストトラップ（企業）	従業員への過大な信頼はリスクの大きさを見誤るトラストトラップ（Trust Trap）につながる恐れがある。企業の管理職は従業員のやる気や生産効率を高めるために良好な信頼関係を築くことを重視することがあるが、信頼関係を築くことに労力を費やすあまり必要最低限の従業員の監視を怠ってしまうケースがある。トラストトラップでは、従業員に高い信頼を置くあまり、従業員の監視がおろそかになる可能性を示している。

②機密情報の盗難

内部脅威による機密情報の盗難にはソフトウェアのコード、ビジネスプラン、顧客情報、製品情報の盗難などが挙げられる。内部脅威者には科学者、エンジニア、プログラマ、営業職が多く、業務として機密情報へ容易にアクセスできるため、勤務時間内に犯行に及んでいる。個人的な金銭的利益のために機密情報を盗

[65] http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30310 p.1～p.16
[66] http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30310

むケースはまれであり、多くは転職先での利用、新しいビジネスの立ち上げ、海外の企業・組織へ引き渡すために犯行に及ぶことが多い。このため、MERIT モデルでは機密情報を盗む内部脅威を以下の 2 つのパターンに分けている[67]。

行動	内容
単独犯	このケースでは、内部脅威者の多くが機密情報にアクセスできる立場についており、給与や知的財産の所有権といった企業への不満から他社への転身を考えるようになる。これらの内部脅威者の約 3 分の 1 が転職を有利にするために盗んだ機密情報を利用するなど、企業内での立場、企業への不満、転職への欲求が大きいほど機密情報の盗難につながりやすくなる。内部脅威者が退職願を出した日の前後 1 ヶ月間にわたって機密情報を盗むケースが多いため、その期間における電子メール送信先や添付ファイル、ファイルの印刷やダウンロード、ファイルがコピーされた外部メディアを追跡する必要がある。
複数人の犯行	単独犯とは異なり他の組織に利益を与えることを動機としていることから、半数以上が他社に知財の情報を渡し、3 分の 1 は海外に流出している。情報を盗む機会を狙っているため、重要なプロジェクトへの参加を希望するなど情報へのアクセスの機会を増やそうとする。また、業務メールの使用やノートパソコンにデータをダウンロードして外部へ持ち出すなど、通常業務に見える形でデータを持ち出すため、企業から持ち出されたデータを追跡できるようにすることが重要となる。

③企業に対する詐欺行為

個人的な利得のためにデータの盗難や改ざんを行なう内部脅威は、損害が平均 4 万ドルと企業に大きいダメージを残す。多くの場合は個人的または近親者への経済的な利益を動機として、長期にわたって繰り返し行なわれる。このケースで企業の機密情報を盗む内部脅威者の 40%が外部の人間と共謀しており、25%が外部から依頼されて実行に移している。業務を有利に進める目的などでシステムのデータを改ざんする場合には、発覚を防ぐために同僚など他の内部の人間と協力して行うこともある。これらの犯行を防ぐためには、内部脅威者の経済的な問題や組織内での行動、機密データの検証、必要以上のアクセス権を与えないようにすることが重要となる[68]。

そして CERT の本レポートでは、内部脅威者への対応策として、以下の項目を掲げている[69]。

① 内部脅威者の動機と事前準備段階への対策

a. **【従業員の不満や懸念していることを聞き入れるためのプロセスを導入する】**:従業員の不満を聞きいれることで、従業員が不満を晴らすために企業への被害を考えることを軽減する。

b. **【従業員の行動などについて情報を共有するプロセスを導入する】**:匿名による報告を受け付けるなど、従業員が報告しやすいプロセスを導入する。マネジメント、セキュリティ、人事、法律家などで情報を共有する。

c. **【問題のある行動についての情報を文書化し、対策へとつなげる】**:文書化することで情報を整理し、内部脅威者の行動を辿ることができるようにする。

[67] http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30310
[68] http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=30310
[69] http://resources.sei.cmu.edu/asset_files/TechnicalReport/2008_005_001_14981.pdf

② 内部脅威者による攻撃への防御

a. **【従業員が持つシステムへのアクセス権を速やかに削除するポリシーを構築する】**：仮想ネットワークやファイアウォールを含めた従業員のアクセス権を速やかに削除することで、内部脅威者の攻撃の機会を減らす。

b. **【システム管理者にとって必要な操作手順を決めておく】**：内部脅威者に必要以上のシステムの操作を許可すると脆弱性を悪用した攻撃を許してしまうため、システム管理に必要な操作を決めておく。

c. **【セキュリティポリシー、管理、技術的な対抗策を講じておくことで、技術的に簡単な攻撃を防ぐようにする】**：内部脅威者による犯行のうち 61%は技術的に高度な攻撃手法ではなく脆弱性を突くといった単純な攻撃であるため、セキュリティポリシーなどを徹底することで攻撃の機会を減らす。

d. **【包括的なパスワードの管理に関するポリシーを作成し、従業員に周知させる】**：内部脅威者による犯行の 3 分の 1 が他のアカウントを使ったものであり、他の従業員のアカウントのパスワードを盗むといったケースも多数見られた。このため、パスワードの管理に関するポリシーを徹底させる。

e. **【包括的なアカウント管理のポリシーを作成し、徹底する】**：不正侵入用のバックドアアカウントの検知、アカウントの管理と利用記録の追跡、共用アカウントを利用するメンバーの関係の確認、全アカウントの監視、アカウントの無効化に関するポリシーを作成、徹底する。

f. **【悪意のあるプログラムのコードを検知するために必要な、ハードウェア、ソフトウェア、システム設定を導入する】**：内部脅威者の中には事前に悪意のあるコードを組み込み、そのコードを自動で削除するプログラムを仕込んでいたため、悪意のあるプログラムやコードを検知できるシステムを導入することが求められる。

g. **【リモート接続に対して複数のセキュリティを導入する】**：リモート接続からは機密情報にアクセスできないようにするなど、様々なセキュリティ対策を講じる。

③ 内部脅威者による攻撃の検知

a. **【内部脅威者を検知するために必要なシステムのログを監視するシステムを構築し、ログの保護にバックアップなどを備える】**：いくつかのケースでは、顧客がアカウントを使用できなかったことから、ログの追跡により内部脅威者による犯行が発覚している。このため、ログを監視することシステムを導入することが有効と見られている。また、内部脅威者はログが犯人の特定に有効であることを熟知しているため、常にログをバックアップすることが必要である。

b. **【内部脅威者を調査する場合には法的措置も視野に入れる】**：犯人の特定には内部脅威者の自宅のコンピューターなどを確認することが有効となる場合もあるため、家宅捜索など法的措置を活用する。

④ 被害を受けた場合の復旧策

a. **【重要システムの生存性を高めることができるポリシーや手順を導入する】**：いくつかのケースでは、機密データを破壊もしくは暗号化する、システムを利用不可能にする、ネットワークに障害を引き起こすといった手段が取られている。このため、内部脅威者の犯行による障害が発生した場合には、重要なシステムを迅速に復旧するために必要な生存性と強靭性を確保できるポリシーを導入しておく。

b. **【データのバックアップや復旧は確実にし、定期的なテストを実行する】**：内部脅威者の犯行の中にはバックアップデータの削除だけでなく、データが格納されているメディアを盗むといったケースも見られた。このため、データのバックアップにおいても冗長性のあるシステムを導入する。

5 終わりに

サイバーセキュリティに対するニーズは益々高まり、サイバーセキュリティ関連の様々な制度や対応策が創設されている。その一方で、実施を担う人材の不足が大きな問題になってきている。セキュリティ人材の不足は政府にとどまらず、シリコンバレーですら深刻になってきており、今回紹介したように、産学官それぞれが様々な事業等を通じて、将来のサイバーセキュリティ対策を担う人材の育成に努めている。
また、サイバーへの脅威として大きくなってきているのが、内部犯罪などの内部脅威である。今回紹介したように、本問題では人間の心理を分析することで、より効果的な対策を行えないか検討が進んでいる。
このように、サイバーセキュリティにおいては、技術開発や制度整備を進めるだけでなく、人材育成や人間心理の分析など「人間」の部分が重要であり、そして人材育成などには長い時間を要するため、中長期的な戦略を持って進めることが重要である。これは我が国でも同様である。今回紹介した米国での取り組みも参考になるのではないだろうか。