育てろ！情報セキュリティ人財

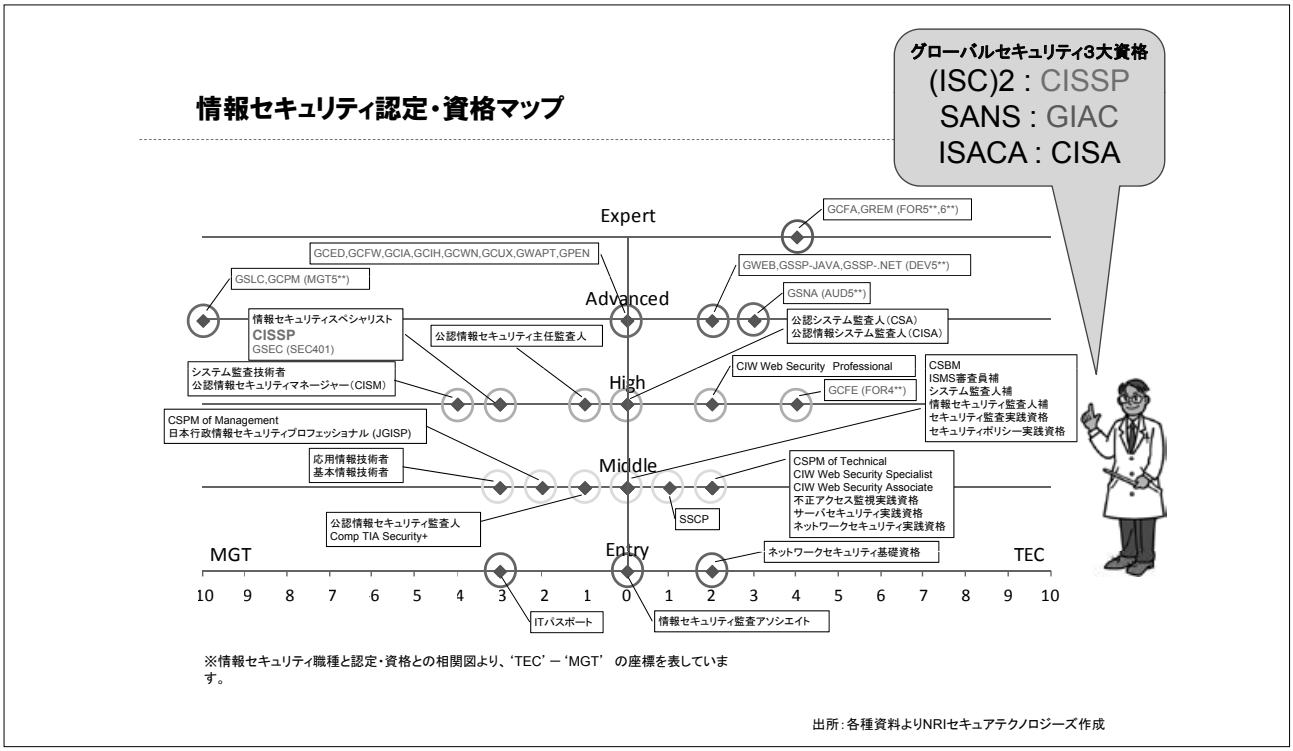
JNSA 幹事
NRI セキュアテクノロジーズ株式会社
上級セキュリティコンサルタント
与儀　大輔

不足が叫ばれる情報セキュリティ人材育成とセキュリティ資格制度

・資格認定制度の現状と期待される効果

情報セキュリティに関する資格は、国内資格とグローバル資格に大別されます。国内資格でも国家資格に該当するのが情報処理技術者試験として「ITパスポート」「情報セキュリティアドミニストレーター」や「ISMS審査員」「ITコーディネーター」などです。国内の民間資格はセキュリティ・エデュケーション・アライアンス・ジャパン（SEA/J）が提供する「CSBM」「CSPM」や特定非営利活動法人 日本セキュリティ監査協会（JASA）の「CAIS」等が該当します。

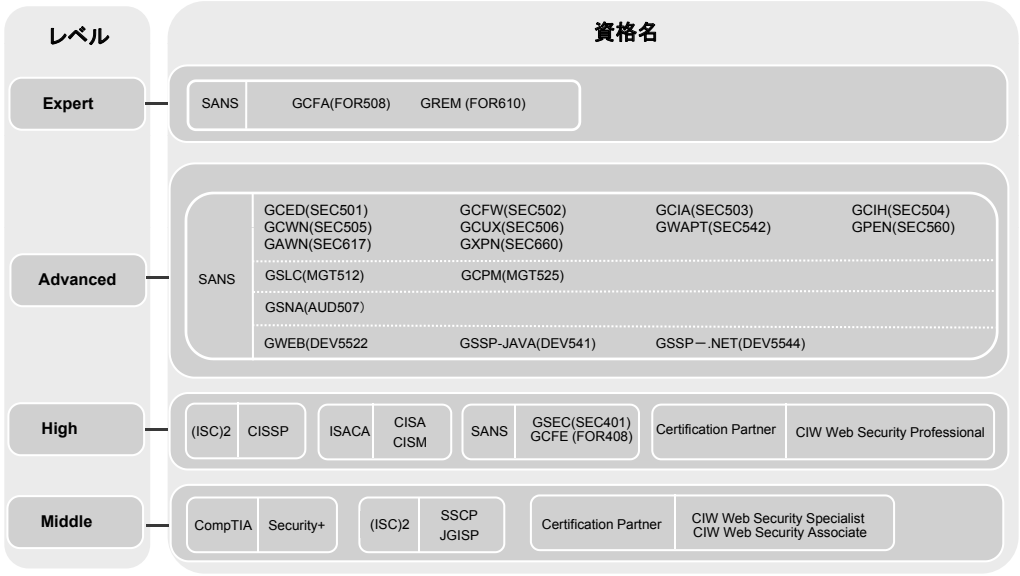
グローバル資格はベンダーニュートラルの資格とベンダー資格とに分類出来ます。ベンダーニュートラルの資格とは製品やサービスに特化しない資格であり代表的なグローバル資格では（ISC）2“アイエスシースクエア”※1が認定する「CISSP」※2「SSCP」※3やCompTIAが認定する「Security+」、SANS※4の「GIAC」、ISACAの「CISA」「CISM」などが該当します。特にCISSP、CISA、GIACはグローバル三大資格として認知度が高く、米国国防総省では情報保障に関わる職員や同省の取引先に取得が義務付けられています。さらに外資系企業などではセキュリティ技術者等の情報セキュリティ人材の採用要件となる例が増加しています。また、ベンダー資格はマイクロソフトやシスコシステムズ、オラクル等が各社独自の認定基準で運営を行っています。



※情報セキュリティ職種と認定・資格との相関図より、‘TEC’－‘MGT’ の座標を表しています。

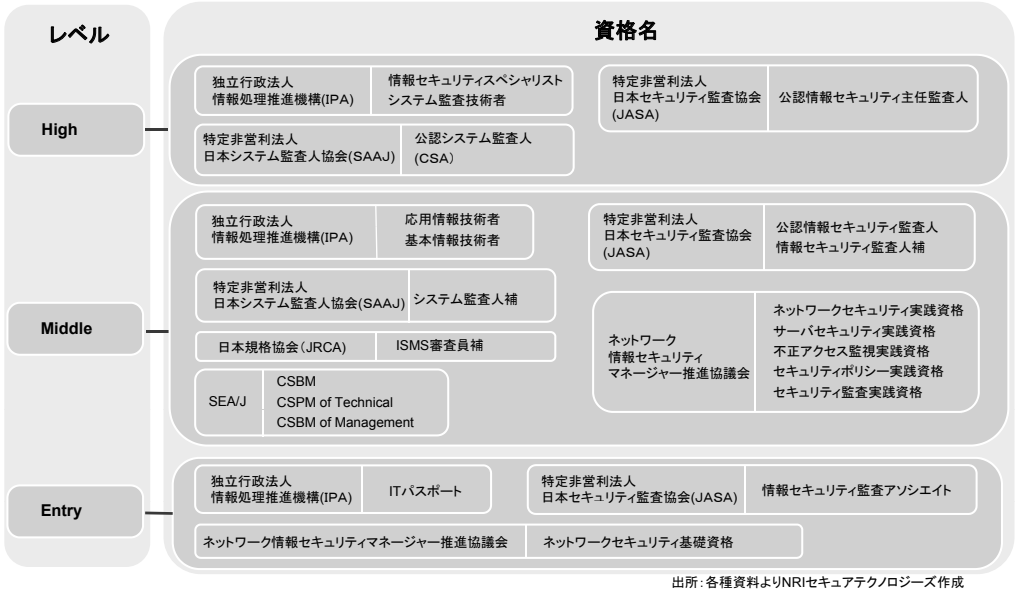
出所：各種資料よりNRIセキュアテクノロジーズ作成

グローバル資格のレベルマップ



出所：各種資料よりNRIセキュアテクノロジーズ作成

国内資格のレベルマップ



出所：各種資料よりNRIセキュアテクノロジーズ作成

一方、学校教育に目を向けますと情報セキュリティ大学院大学などでは情報セキュリティ修士課程を開講しています。

ITに関わる人口が年々増加する環境において産学官で情報セキュリティに関わる各種取組や資格制度が立ち上がり、セキュリティを学ぶ機会が増加していると言えるのではないでしょうか。その背景としては、企業や組織が相次ぐサイバー攻撃への対策に備えるために情報セキュリティ対策のレベル向上を必須として取組を強化しており、情報セキュリティに関わる人材に高度な専門知識やマネージメント能力を求めていると考えられます。(ISC)2が世界中の情報セキュリティ業務従事者約12,000人にヒアリング調査した「グローバル情報セキュリティワークフォース調査2013」[※5]によると、情報セキュリティ人材のニーズは高く毎年10%以上増加すると予想されています。

情報セキュリティ人材ニーズ

情報セキュリティ人材は、ここ数年の経済状況にも関わらず、増加し続けている。また、今後も継続に増加すると予測されている

単位：千人

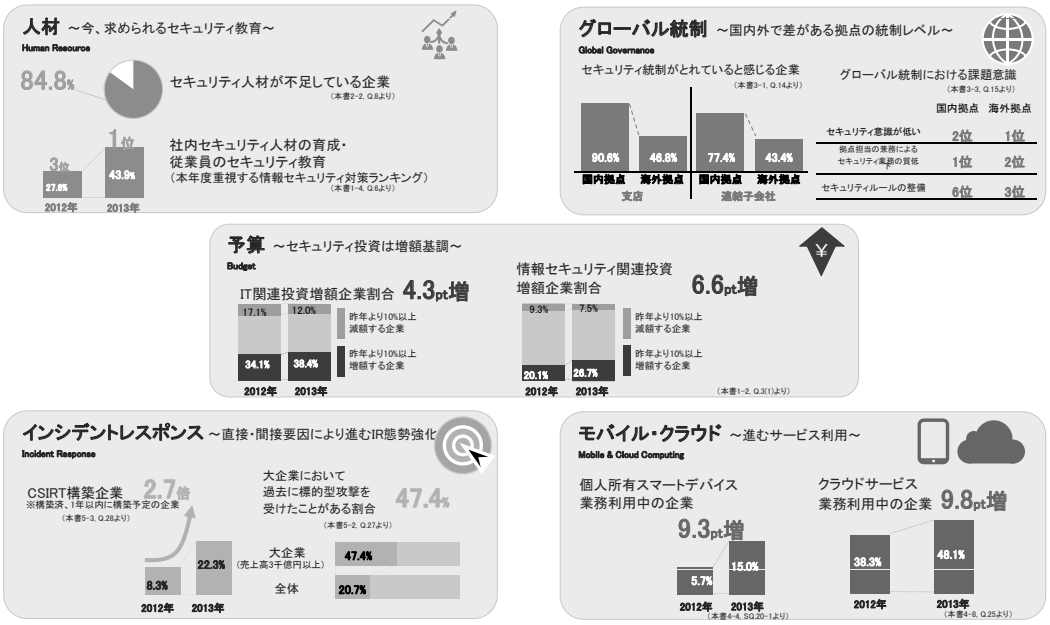
Thousands	2010	2011	2012	2013	2014	2015	2016	2017	2012-2017 CAGR
Americas	921	1,045	1,181	1,331	1,495	1,673	1,867	2,081	**12.0%**
EMEA	617	704	797	892	995	1,108	1,230	1,363	**11.3%**
APAC	748	817	894	981	1,079	1,191	1,320	1,463	**10.4%**
Total	**2,286**	**2,566**	**2,872**	**3,204**	**3,568**	**3,972**	**4,416**	**4,908**	**11.3%**

Americas:北米、中米、南米
EMEA:ヨーロッパ、中東及びアフリカ
APAC：アジア太平洋

出典：2013年(ISC)2グローバル情報セキュリティワークフォーススタディ

また、NRIセキュアテクノロジーズが発行する「企業における情報セキュリティ実態調査 2013」によると、情報セキュリティ人材が不足していると感じる企業は85%であり、本年度重視する情報セキュリティ対策として、「社内人材の育成や従業員教育」が昨年の3位（28%）から1位（44%）に急上昇しています。

数字で見る情報セキュリティ実態2013 ～ 情報セキュリティ強化における5大指針 ～



出所：NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査 2013」

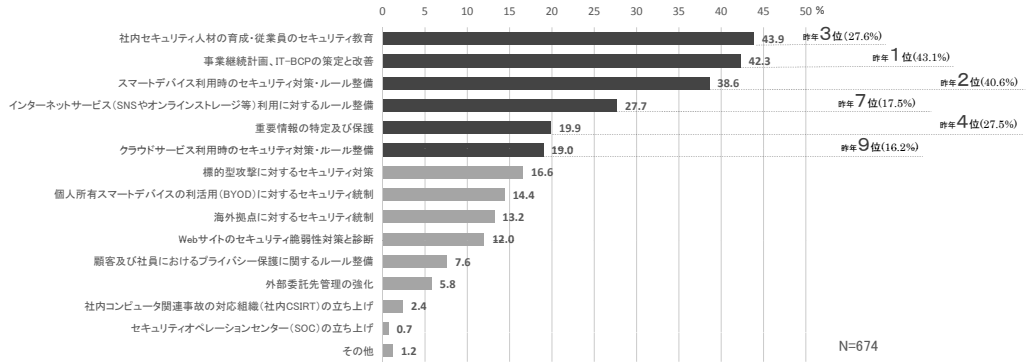
1-4. 本年度(2013年度)重視する情報セキュリティ対策

人材育成や、クラウド・SNSのルール整備を重視する企業が増加傾向

- 昨年度と比較して、「社内セキュリティ人材の育成・従業員のセキュリティ教育」が大幅に増加しており、3位から1位に上昇している。この結果より、社内意識の向上を図る企業が増えていることが分かる。
- Top3には入らなかったものの、昨年度から大幅に順位を上げた「インターネットサービス」や、「クラウドサービス」におけるルール整備が上位に入ったことから、これらのサービスを活用するとともに、セキュリティ対策を重視している企業が多いことがうかがえる。

Q6. 貴社において、2013年度に重視する情報セキュリティ対策は何ですか。（最大3つまで選択可）

本年度重視する情報セキュリティ対策（複数回答）



出所：NRIセキュアテクノロジーズ「企業における情報セキュリティ実態調査 2013」

つまり情報セキュリティ人材が足りないから育成確保が必要であるという認識が高まると共に情報セキュリティを確保する上で、より広範囲な知識と経験が求められ、業務従事年数のみではなく資格によって個人の能力を客観的に証明することが求められる時代になって来ているのではないでしょうか。広範囲な知識と実践能力を兼ね備え、更に資格を持ったセキュリティプロフェッショナルが日々脅威の増す情報セキュリティ事案を対処することにより組織のリスクが軽減されると言えます。

自組織にセキュリティプロフェッショナルを有する事が困難であっても、せめて外部の専門家と会話が出来るレベルの人材は育てておかなければなりません。何故ならインシデントが発生した場合、全てを自組織のみで解決することは困難であり、外部の専門家やセキュリティベンダーに協力を仰ぐ事が必要になるからです。

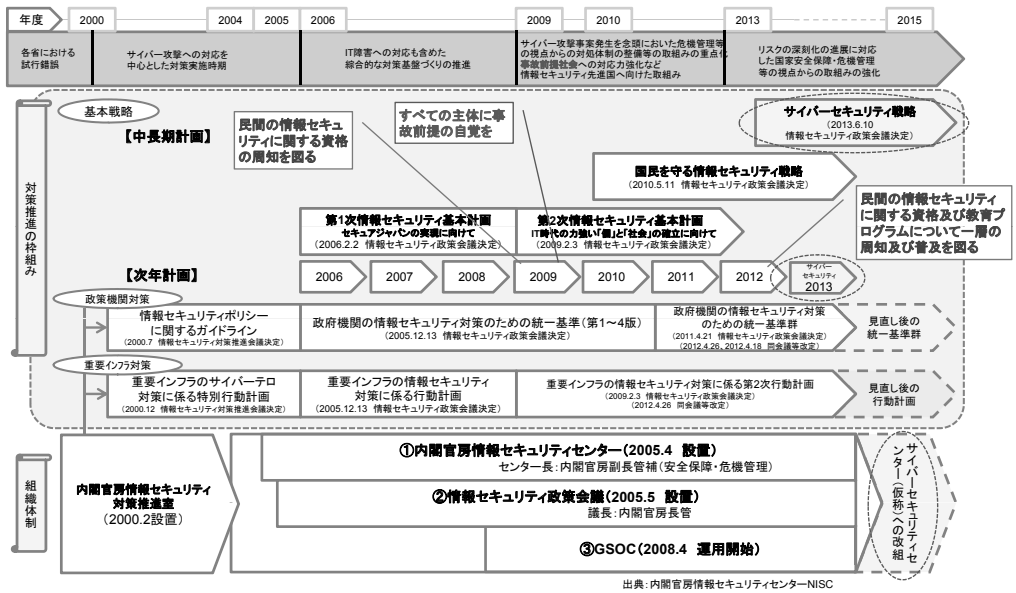
・課題と目標

我々の生活においてもITは重要なインフラとしての役目を担っています。

情報セキュリティ分野においてはポリシー作成やシステムの導入、運用管理、BYODなど導入検討の業務のみならず、内部統制やCSR、コンプライアンスなど組織としての対応を迫られている多くの課題があります。しかしながら山積した諸問題を解決するには知識と経験が必要であるにも関わらず、その経験値を持った人材は非常に少なく更に経験値を図る基準も不明確であるという現状があります。

情報セキュリティ人材の不足は国も認識しており、政府の情報セキュリティ政策会議等において「サイバーセキュリティ戦略」、3カ年計画である「第1次2次情報セキュリティ基本計画」、単年度計画である「サイバーセキュリティ2013」、「情報セキュリティ人材育成プログラム」など人材育成の重要性と基本方針が示されています。

我が国の情報セキュリティ政策の推移



出典:内閣官房情報セキュリティセンターNISC

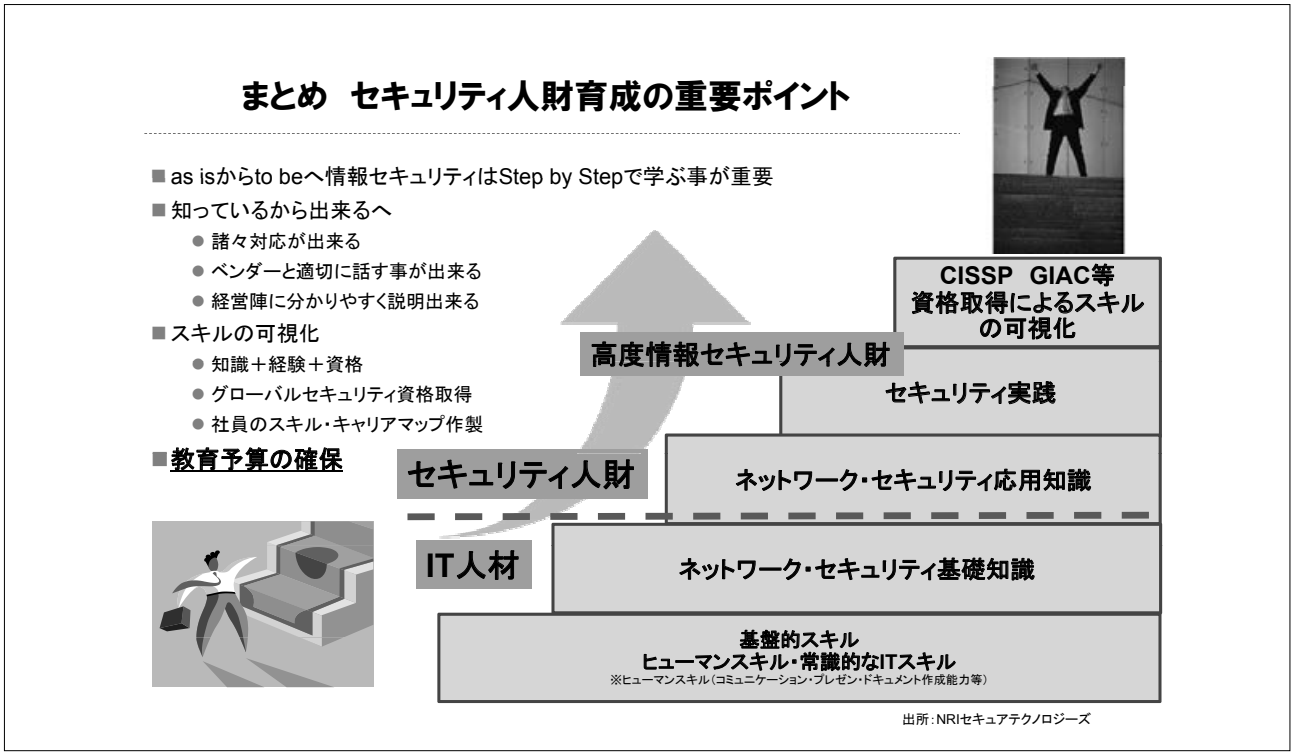
しかしながら我が国の現状について情報処理推進機構（IPA）の報告「情報セキュリティ人材の育成に関する基礎調査」（2012年4月27日）によると、我が国で従業員100人以上の企業の情報セキュリティ技術者は現在約23万人いますが、そのうち約14万人は何らかの教育やトレーニングを行う必要があり、また技術者の総数も約2.2万人不足していると推計されていることから、更なる教育コースの充実やスキルの可視化が課題となっています。

大企業や政府機関のシステムが関東に集中していることから、情報セキュリティ人材も関東に集中しています。中小企業においてはセキュリティ担当者を配置する予算も人も無いのが実態です。つまり情報セキュリティ対策に格差が生じ始めているのです。格差解消の為には中小企業のセキュリティ担当者への教育機会を拡大させると共に、費用を法人税から減免するなどの処置も必要だと考えます。更に大企業に多く在籍している情報セキュリティ有資格者が地方や中小企業に対して勉強会などの支援を行うコミュニティの醸成やヘルプデスクのようなプラットフォーム等の検討も必要ではないでしょうか。

頻発するサイバー攻撃を見れば、海外進出を果たしたグローバル企業のみならず、インターネットは世界に繋がっているのですから脅威はすぐ近くに潜んでいることが分かります。今その脅威と戦うプロフェッショナルが求められているのです。

・人材から人財へ

「人は城、人は石垣、人は堀」という言葉がありますが、私は、セキュリティ人材とはセキュリティを構成する材料ではなく、掛け替えのない財産である「人財」と考えています。セキュリティをより強固にする上で国際的に通用する知識と能力を兼ね備えた人財育成は欠かせません。その為には企業の経営層は情報セキュリティに関わる人財育成に適切な予算を確保し継続することが求められます。



情報セキュリティ人財は今日教育をしたから明日から実務が出来るわけではありません。基礎的な知識の習得から始め、徐々に実践的な演習なども行う等のStep by Stepで学ぶ事が重要です。育成において留意する事は、まず現状を把握（as is）して、何が足りないのかを理解した上で人材育成の有るべき姿であるゴール（to be）を明確に定める事が重要です。そしてそのゴールに向かって中長期、短期の人財育成ロードマップを作成し実行することも不可欠です。

・情報セキュリティ人財を育成・確保する為の提言

①「攻撃者」と「サイバー脅威」は変化を続けており、常に最新動向把握等の情報収集を行う。ツールやシステム強化のみではセキュリティが守れない事を認識する

② セキュリティを強化する為に人財育成が欠かせない事を理解する。更に自組織の「人材」をどのように「高度情報セキュリティ人財」に育成するのかインセンティブを含めてTo-beを検討する

③ 社員のスキルを可視化しキャリアマップを作成する。セキュリティ教育や資格取得を実施する際には、グローバルで通用するかを選定条件にする

是非とも経営者の皆様には情報セキュリティへの理解を深めて頂き、必要な教育予算の確保をお願い致します。

参　考

※1　(ISC)2(International Information System Security Certification Consortium：国際情報システムセキュリティ認証コンソーシアム）は、米国のNPO(非営利団体）です。 CISSP(Certified Information Systems Security Professional)SSCP(Systems Security Certified Practitioner）は(ISC)2 が認定している資格です。

※2　CISSP (Certified Information Systems Security Professional)：
全世界の情報セキュリティの専門家に対し、高水準の専門性を認定する資格です。情報セキュリティを包括的・体系的に理解することが要求される内容などが高く評価され、現在、世界135カ国に約90,000名、日本では約1,300名の認定取得者がいます。

※3　SSCP(Systems Security Certified Practitioner)：
ネットワーク・システムの開発や運用などに従事し、情報セキュリティを「技術」だけではなく「組織」の観点からも理解し、情報セキュリティ専門家や経営陣とコミュニケーションを図ることができる人材を認証する資格です。

※4　SANS(SysAdmin, Audit, Network, Securityの略）は、世界最大かつ最も信頼される情報セキュリティ教育のブランドです。SANS Institute(本部：米国メリーランド州）が研修プログラム及びGIAC各種認定資格試験を運営していますが、SANSの研修メソッドは、設立以来20年以上にわたり、その有効性が評価されています。情報セキュリティの最も重要な技術分野の詳細スキルに対応しており、米国政府をはじめ民間企業でも多数が採用しています。

※5　(ISC)2 2013年(ISC)2グローバル情報セキュリティワークフォーススタディ
https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/2013-ISC2-Global-Information-Security-Workforce-Study.pdf