組織と個人の総合的対応力向上を目指したサイバーセキュリティ人材育成戦略

奈　良　　将，石　野　貴　子

1. は　じ　め　に

1995 年 11 月 15 日に施行された科学技術基本法[*1] の第 5 期（2016 年度から 2020 年度の範囲）で提唱された Society 5.0 は，IoT（Internet of Things）で全ての人とモノがつながることによりサイバー空間（仮想空間）とフィジカル空間（現実空間）が高度に融合する社会を目指している．また，2014 年 11 月 6 日に成立したサイバーセキュリティ基本法[*2] が 2018 年 12 月 12 日に改正され，官民の多様な主体が相互に連携し，サイバーセキュリティに関する施策の推進に係る協議を行うためのサイバーセキュリティ協議会[*3] が発足した．さらに，サイバー攻撃の被害を受けた組織から他の組織へ迅速な情報共有を行うことでサイバー攻撃の被害の拡大を防ぐため，サイバーセキュリティ戦略本部[*4] の役割に，サイバーセキュリティに関する事案が発生した際の国内外関係者との連絡調整が追加された．

このような社会的状況の中，企業にもサイバー空間に特化したセキュリティ対策が求められている．基本的な対策を計画的に実施するだけでなく，攻撃を受けた際の迅速な対応が不可欠であり，それに対応できるサイバーセキュリティ人材の育成が重要になっている．

本稿では，2 章でサイバーセキュリティ人材が不足する背景と，組織で求められる人材について明確にし，3 章で日本ユニシス株式会社とグループ会社（以降，日本ユニシスグループ）における「サイバーセキュリティ戦略[1]」で定義したサイバーセキュリティ人材と，その育成計画について述べる．

2. サイバーセキュリティに対応する人材

本章では，サイバーセキュリティ人材が不足する背景とその役割を述べる．

2.1 情報セキュリティとサイバーセキュリティの違い

情報セキュリティとは，組織が情報資産を様々な脅威から守り，その状態を維持することを指す．組織は守るべき情報資産を明確にし，その脅威およびリスクを機密性や完全性や可用性の観点で評価，対策を実施し，その対策の有効性を定期的に見直し更新していく．この維持していく活動（マネジメントシステム）では，Plan（計画），Do（実行），Check（検証），Act（対策・改善）の PDCA サイクルを回して適切に管理することが重要である．

一方，サイバーセキュリティは，ネットワークで繋がっている目に見えないサイバー空間におけるセキュリティである．コンピューターだけではなくスマートフォンや IoT に分類される監視カメラ，スマート家電，自動車等と対象が多岐にわたることから，組織が

守るべき情報資産やサイバー空間における脅威を抽出することが難しい．

2.2　サイバーセキュリティ人材が不足する背景

組織のネットワークがグループ企業やサプライチェーンと接続することにより，自組織ネットワークとそれ以外との接続境界が増えている．さらにクラウド利用の広がりやモバイル端末からの自組織ネットワークへのアクセス等により，組織のセキュリティ考慮範囲も広がっている．そのため，リスクや重要度に応じた多層防御や，攻撃にいち早く気付き対応するための監視機能や体制の整備等，接続境界から侵入された後の対応が求められている．侵入された後の被害を最小限に抑えるというダメージコントロールは，脅威に気付く，攻撃者の攻撃パターンを把握する，外部と連携し情報を入手する，といったことが重要であり，それらを実行できるサイバーセキュリティ人材を確保しなければならない．サイバーセキュリティ人材が不足すると，サイバー攻撃の被害を拡大させ，ネットワークで繋がっている協業先や情報を預かっているエンドユーザ等への二次被害を発生させることになる．

また，攻撃にも変化があり，過去にはいたずらや自身の技術力の誇示が目的とされていたが，その後金銭目的や特定の思想の主張が増え，現在では組織的，国家的な攻撃も公表されている．それに伴い攻撃のレベルが格段に上がってきたことも，防御する側の組織がサイバーセキュリティ人材の不足を感じる要因と考えられる．

2.3　サイバーセキュリティ人材の役割

サイバーセキュリティは，組織内の専門家だけが意識をすればよいわけではなく，組織の活動に係わる全ての役職員が，各々の役割に応じた意識を持つことが重要である．

一般社団法人日本サイバーセキュリティ・イノベーション委員会（JCIC）[*5] はセキュリティ人材を，IT ベンダー/セキュリティ関連企業に所属しセキュリティを主たる業務とする「サイバーセキュリティ専門人材」と，本来の業務を担いながら IT を利活用する中でセキュリティスキルも必要となる「プラス（＋）・セキュリティ人材」に大別している[3]．これを踏まえ，組織内で求められる人材の役割について述べる．

2.3.1　サイバーセキュリティ専門人材

サイバー攻撃が問題になっている現在では，プラス・セキュリティ人材と共に企業におけるサイバーセキュリティ専門人材の重要性が高まっている．サイバーセキュリティ専門人材のスキルは多岐にわたっており，独立行政法人情報処理推進機構（IPA）では従来の IT スキル標準である ITSS（IT Skill Standard）に加え，IT 企業や一般企業の情報システム部門の従事者のスキル強化を図る取り組みとして ITSS ＋（プラス）[4] を定義し，セキュリティ領域の人材の役割を表 1 のように細分化している．

表 1　ITSS ＋セキュリティ領域の専門分野[4]

専門分野	説　明
情報リスクストラテジ	自組織または受託先における業務遂行の妨げとなる情報リスクを認識し，その影響を抑制するための，組織体制の整備や各種ルール整備等を含む情報セキュリティ戦略やポリシーの策定等を推進する．自組織または受託先内の情報セキュリティ対策関連業務全体を俯瞰し，アウトソース等を含むリソース配分の判断・決定を行う．
情報セキュリティデザイン	「セキュリティバイデザイン」の観点から情報システムのセキュリティを担保するためのアーキテクチャやポリシーの設計を行うとともに，これを実現するために必要な組織，ルール，プロセス等の整備・構築を支援する．
セキュア開発管理	情報システムや製品に関するリスク対応の観点に基づき，機能安全を含む情報セキュリティの側面から，企画・開発・製造・保守等にわたる情報セキュリティライフサイクルを統括し，対策の実施に関する責任をもつ．
脆弱性診断	ネットワーク，OS，ミドルウェア，アプリケーションがセキュアプログラミングされているかどうかの検査を行い，診断結果の評価を行う．
情報セキュリティアドミニストレーション	組織としての情報セキュリティ戦略やポリシーを具体的な計画や手順に落とし込むとともに，対策の立案や実施（指示・統括），その見直し等を通じて，自組織または受託先における情報セキュリティ対策の具体化や実施を統括する．また，利用者に対する情報セキュリティ啓発や教育の計画を立案・推進する．
情報セキュリティアナリシス	情報セキュリティ対策の現状に関するアセスメントを実施し，あるべき姿とのギャップ分析をもとにリスクを評価した上で，自組織または受託先の事業計画に合わせて導入すべきソリューションを検討する．導入されたソリューションの有効性を確認し，改善計画に反映する．
CSIRT[*6] キュレーション	情報セキュリティインシデントへの対策検討を目的として，セキュリティイベント，脅威や脆弱性情報，攻撃者のプロファイル，国際情勢，メディア動向等に関する情報を収集し，自組織または受託先に適用すべきかの選定を行う．
CSIRT リエゾン	自組織外の関係機関，自組織内の法務，渉外，IT 部門，広報，各事業部等との連絡窓口となり，情報セキュリティインシデントに係る情報連携及び情報発信を行う．必要に応じて IT 部門と CSIRT の間での調整の役割を担う．
CSIRT コマンド	自組織で起きている情報セキュリティインシデントの全体統制を行うとともに，事象に対する対応における優先順位を決定する．重大なインシデントに関しては CISO や経営層との情報連携を行う．また，CISO や経営者が意思決定する際の支援を行う．
インシデントハンドリング	自組織または受託先におけるセキュリティインシデント発生直後の初動対応（被害拡大防止策の実施）や被害からの復旧に関する処理を行う．セキュリティベンダーに処理を委託している場合には指示を出して連携する．情報セキュリティインシデントへの対応状況を管理し，CSIRT コマンドのタスクを担当する者へ報告する．
デジタルフォレンジクス	悪意をもつ者による情報システムやネットワークを対象とした活動の証拠保全を行うとともに，消されたデータを復元したり，痕跡を追跡したりするためのシステム的な鑑識，精密検査，解析，報告を行う．

情報セキュリティインベスティゲーション	情報セキュリティインシデントを対象として，外部からの犯罪，内部犯罪を捜査する．犯罪行為に関する動機の確認や証拠の確保，次に起こる事象の推測等を詰めながら論理的に捜査対象の絞り込みを行う．
情報セキュリティ監査	情報セキュリティに係るリスクのマネジメントが効果的に実施されるよう，リスクアセスメントに基づく適切な管理策の整備，運用状況について，基準に従って検証又は評価し，もって保証を与えあるいは助言を行う．

セキュリティ領域の専門分野が細分化されている理由は，セキュリティインシデント対応要員としての役割が増加しているからである．その中でも，「CSIRT キュレーション」「CSIRT リエゾン」「CSIRT コマンド」「脆弱性診断」「デジタルフォレンジクス」は技術的に高い専門性が求められるため，人材の確保が難しく，サイバーセキュリティ専門人材の不足の一因となっている．一方，「情報リスクストラテジ」「情報セキュリティデザイン」「情報セキュリティアナリシス」「情報セキュリティインベスティゲーション」「情報セキュリティ監査」は管理側の側面が強く，既存の情報セキュリティ人材の延長線として捉えることができる．

これらのサイバーセキュリティ専門人材を増員するには，スキルの見える化を実施の上，自組織で不足している専門分野の人材を把握し，不足点について強化するべきであるが，一般企業では，サイバーセキュリティ専門人材の専門分野全てを自社内に配置することは難しいため，セキュリティベンダーや IT ベンダーのサービスを有効活用することも考慮すると良い．その際に留意すべき点として，「CSIRT キュレーション」「CSIRT リエゾン」「CSIRT コマンド」「インシデントハンドリング」の 4 分野は，一部の専門分野のみを自社内に配置するという判断は避けるべきである．何故ならば，4 分野の人材は CSIRT チームとしてセキュリティインシデント対応を実施するため，迅速な連携が不可欠であり，自社内の環境について熟知していなければならないからである．

日本シーサート協議会[*7]には，353 チーム（2019 年 6 月 19 日時点）が登録[5]されており，大企業は自社で人材を確保または育成している一方，まだ多くの企業が自社でチームを組むことができていない現状が推測される．

2.3.2 プラス・セキュリティ人材

プラス・セキュリティ人材の役割は，担当業務を理解しているからこそ気付く，ビジネス上のセキュリティリスクの見極めやリスク対応策の妥当性の判断，サイバーセキュリティ専門人材と連携したセキュリティの確保である．プラス・セキュリティ人材を活用する場面の例として，「経営層が事業投資等の経営判断をする際に，セキュリティ視点で助言をする」，「事業部門で新たなビジネスを企画する際に，セキュリティを考慮する」が挙げられる．一般企業では，サイバーセキュリティ専門人材が担う役割の一部をセキュリティベンダーや IT ベンダーに任せるという選択肢があるが，プラス・セキュリティ人材が担う役割については，ビジネスや経営に大きく関わるため，自組織内の役職員が担うべきである．

プラス・セキュリティ人材の育成には，組織の定期的な人事異動（ローテーション）が活用できる．セキュリティ専門組織で一定のセキュリティスキルを身に付けた後現場に戻ることで，プラス・セキュリティ人材となる．これを繰り返すことで，組織内にプラス・セキュリティ人材が増えていく．一般企業の場合は，情報システム部門でセキュリティ担当となり，セキュリティベンダーやITベンダーとの業務上のやりとりを通じてセキュリティスキルを身に付けることができる．組織内でのローテーションが難しい場合は，普段からセキュリティ意識が高い社員をプラス・セキュリティ人材候補とし，セキュリティ技術の研修受講やセキュリティ外部団体への参画を通じてセキュリティスキルを身に付けるよう，業務やコストを配慮する．

また，プラス・セキュリティ人材の育成に際しては，ローテーションや担当業務外の活動が含まれることから，そのキャリアパスを明確にしておくことも重要となる．

3.　日本ユニシスグループにおける人材育成

日本ユニシスグループの人材育成計画は，中期経営計画に沿って策定した各種戦略に基づき策定しており，セキュリティについても同様に計画を策定し，継続的に人材を育成している．本章では，日本ユニシスグループにおけるセキュリティ人材育成事例について述べる．

3.1　2000年代の人材育成計画

2003年10月に経済産業省が公表した「情報セキュリティ総合戦略[*8]」を受けて，2004年2月に「日本ユニシスグループ情報セキュリティ総合戦略」を策定した．この戦略では，「人・組織的対策」として，「グループ体制と人材育成の強化」を掲げ，PDCAサイクルの運用に不可欠な人材を中心に育成を実施した．

この期間に育成対象とした人材は，2.3.1項で述べたITSS＋の専門分野のうち「情報セキュリティデザイン」「セキュア開発管理」「情報セキュリティアドミニストレーション」「情報セキュリティ監査」を担う人材と，2.3.2項で述べたプラス・セキュリティ人材である．セキュリティ対策の適切かつ効果的な実装に向けた脅威や脆弱性の抽出およびリスク分析は，組織内の対策だけではなく顧客のシステム開発にも有用なスキルであるため，顧客を担当する部門のシステムエンジニアを対象とした．

さらに，社内で定義したシステムエンジニアの人材モデルにセキュリティ人材を加えたり，3.4節で述べるようにシステムエンジニアの保有スキルを調査する項目にセキュリティに関する項目を加えるなど，育成計画だけでなく，育成の成果を測る施策についても検討し実施した．

3.2　2010年代の人材育成計画

中期経営計画に沿ってグループ全体の技術強化を目的とし策定した「技術統括戦略[*9]」において「セキュリティ技術者育成計画」を策定し現在も継続中である．育成計画策定時にはITベンダーに必要とされる人材を定義し，グループ内で強化すべき人材を明確にし

た後，具体的な育成内容を検討した．

この期間に育成対象とした人材は，2.3.1 項で述べた ITSS ＋の専門分野のうち「情報リスクストラテジ」「脆弱性診断」「情報セキュリティアナリシス」「デジタルフォレンジクス」「CSIRT キュレーション」「CSIRT リエゾン」「CSIRT コマンド」を担う人材と，2.3.2 項で述べたプラス・セキュリティ人材である．

この期間に育成した人材に求める役割を，顧客を担当する部門のシステムエンジニアについては「部門案件に適したセキュリティ対策を可能にするセキュリティ技術者」および「セキュリティインシデント発生時の初動対応が可能な技術者」，セキュリティ専門組織のシステムエンジニアについては「高度なセキュリティ技術を習得し部門案件へのセキュリティ技術支援を行うセキュリティ技術者」として，役割に応じたカリキュラムを作成した．

その後，現場業務を監督する組織長に対するサイバー空間の脅威やセキュリティ運用に関する研修を追加した．これにより，既存の新人研修，若手研修，部門システムエンジニア研修と併せて，役割や成長に応じたカリキュラムでのサイバーセキュリティ研修体系が実現できた（図 1）．

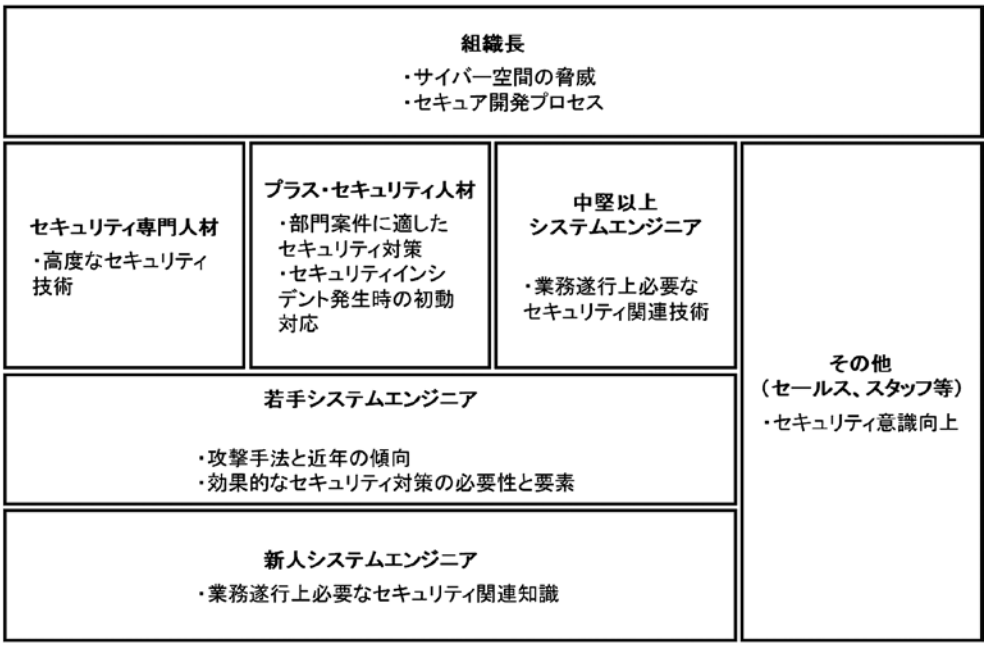

図 1　サイバーセキュリティ研修体系

3.3　今後の人材育成計画

今後は日本ユニシスグループの「サイバーセキュリティ戦略」に基づき，人材育成計画を適宜改訂していく．日本ユニシスグループの「サイバーセキュリティ戦略」とは，本特集号の基調論文[1]にて述べているように，顧客・パートナーと共に社会を豊かにする価値を提供し，社会課題を解決する企業にふさわしいサイバーセキュリティ・マネジメントを

実現することをミッションとした戦略である.

「サイバーセキュリティ戦略」では重点項目として人材育成を挙げており，グループ役職員のスキル・能力・意識を向上させることで「多様な企業をつなぐビジネスエコシステム創出企業に成長するためにプロアクティブでセキュアな環境を提供する」という戦略のビジョンを支える.

組織全体のスキルの向上を図るには，一様のカリキュラムを実施すればよいというものではなく，組織に求められる人材の種別を特定し，中期的な育成戦略と継続的な投資に基づき，適切なトレーニングや実務経験を積み重ねていかなければならない．日本ユニシスグループでは，表2のように役職員を分類し，高いスキルを持つサイバーセキュリティ専門人材の育成だけに限らず，組織全体のプラス・セキュリティ人材の能力を高めるための人材育成計画を策定している.

表2　サイバーセキュリティ人材の対象

人材種別	分　　類
サイバーセキュリティ専門人材	専門組織システムエンジニア
プラス・セキュリティ人材	経営層
	組織長
	システムエンジニア
	サービスエンジニア
	ビジネスプロデューサー*10
	セールス
	スタッフ

サイバーセキュリティ専門人材は専門組織システムエンジニアとして分類する一方，プラス・セキュリティ人材は役職員の役割毎にきめ細かな育成を実施するため7分類とした．分類毎の人材育成方針を述べる.

1）専門組織システムエンジニア

専門組織システムエンジニアとはセキュリティ分野に関して高度な専門性を有するシステムエンジニアを指す．2.3.1項で述べたITSS＋の専門分野を，日本ユニシスグループとして表3のように再定義し，各々の役割としている.

表3　専門組織システムエンジニアの役割

ITSS＋での専門分野	日本ユニシスグループでの専門分野
情報リスクストラテジ	セキュリティコンサルタント： サイバーセキュリティの統制全般をリードするコンサルタント
情報セキュリティアナリシス	

情報セキュリティデザイン （セキュリティ全体）	セキュリティアーキテクト： サイバーセキュリティ対策全体を実装するアーキテクト
情報セキュリティデザイン （セキュリティソリューション）	セキュリティソリューションエンジニア： セキュリティソリューション（製品，運用）を担当するスペシャリスト
脆弱性診断	脆弱性診断士： 脆弱性診断サービスのスペシャリスト
CSIRT キュレーション	CSIRT エンジニア： セキュリティインシデントへの対応を担当するスペシャリスト
CSIRT リエゾン	
CSIRT コマンド	
インシデントハンドリング	
デジタルフォレンジクス	フォレンジックエンジニア： デジタルフォレンジクスを担当するスペシャリスト
情報セキュリティインベスティゲーション	
情報セキュリティ監査	セキュリティ監査人： セキュリティ監査を担当するスペシャリスト

サイバーセキュリティにおける専門組織システムエンジニアの主な役割は，セキュリティ分野の企画や現場部門の開発支援，セキュリティインシデントが発生した際に迅速に適切な対応ができることである．各専門分野の専門性を高めることを目指し，育成する．

専門組織システムエンジニアに対する育成方針は以下の通りである．

・最新のセキュリティ情報の取得や役割毎の専門性を高めるための，セキュリティ専門研修や外部団体，海外のセキュリティカンファレンス等のイベントへの積極的な派遣．
・CISSP（Certified Information Systems Security Professional）認定資格[*11]や，情報処理安全確保支援士[*12]の取得の積極的な推進．
・セキュリティインシデントが実際に起きた場合を想定したサイバーセキュリティ演習や訓練の定期的な実施．
・顧客へのセキュリティサービスの提供や社内セキュリティの運用維持等の業務によるサイバーセキュリティ対策経験の蓄積．

2）経営層

サイバーセキュリティにおける経営層の主な役割は，リスク/セキュリティ対応責任者として上位マネジメントが危機管理に対する認識を深めるとともに，リスク事案が発生した場合の組織的対応・措置の理解及び，平時におけるサイバーセキュリティへの投資判断を実施することである．これらが実施できる状態を目指す．

経営層に対する方針は以下の通りである．

・経営会議等の経営層が集合する場において，最新のセキュリティ動向を把握及び経営層同士の情報共有の実施．

・経営層を対象にしたサイバーセキュリティ経営セミナーへの積極的な参加.
・重大なセキュリティインシデントの発生を想定したリスク対応研修の実施.

3) 組織長

サイバーセキュリティにおける組織長の主な役割は，プロジェクトにおけるセキュリティリスクの低減，部下のサイバーセキュリティ意識向上，自身が担当しているプロジェクトでセキュリティインシデントが発生した場合のリーダーシップの発揮である．日本ユニシスグループでは階層的に組織長を配置している．組織的なセキュリティスキル向上を推進し実行するため，現場業務を監督する組織長は，サイバー空間における脅威と顧客に提供するサービスやソリューションへの適切なセキュリティ対策の実装の必要性を理解できている状態を目指し，育成する．

組織長に対する育成方針は以下の通りである．

・セキュリティリスク及び，リスクを低減するための手段の理解の促進.
・日本ユニシスグループのセキュリティポリシーやプロセスに対する深い理解の促進.
・セキュリティインシデントへの対応方法に関する深い理解の促進.

4) システムエンジニア

サイバーセキュリティにおけるシステムエンジニアの主な役割は，セキュアなシステムを構築することである．サイバーセキュリティ研修体系に基づき，成長段階に応じた育成を実施する．

新人システムエンジニアには，新入社員研修の中でセキュリティの基礎知識を教育し，今後業務を遂行する上でスキルを身に着けるための基礎ができている状態を目指し，育成する．

若手システムエンジニアには，日本ユニシスグループのシステムエンジニアとして最低限身に着けておくべきセキュリティ知識・スキルの習得を目指し，育成する．具体的には，セキュリティの e-Learning や，指名制による定期的な集合研修を実施する．

中堅以上のシステムエンジニアには，より高度なサイバーセキュリティスキルの習得を目指し，育成する．中堅以上のシステムエンジニアは日本ユニシスグループの社員の中で多くの割合を占めており，顧客対応・システム構築を実施する膨大なプロジェクトの中核的役割を担っている．そのため，中堅以上のシステムエンジニアのサイバーセキュリティスキル向上は特に重要である．

システムエンジニアに対する育成方針は以下の通りである．

・段階的なサイバーセキュリティ研修の実施.
・システム構築におけるセキュリティリスクを効果的に低減できる，より深いセキュリティ技術の習得.
・セキュリティインシデントの初動対応のスキルの向上.
・システム開発におけるセキュリティプロセスのより深い理解の促進.
・システムエンジニアとサイバーセキュリティ専門人材間の情報共有や交流の場の設定.

検討している段階的な研修・施策の一部を表 4 に纏めた.

表 4　段階的なサイバーセキュリティ研修・施策例

発達段階	研修・施策内容	
新人	情報セキュリティ概論	組織で情報資産を扱う者にとって必要な情報セキュリティ対策について，その重要性と主な構成要素を習得．組織の特徴に合わせてセキュリティ対策が必要な部分の発見方法と，近年の傾向に合わせたセキュリティ対策の実装方法の概要を習得.
	ネットワークセキュリティ基礎	IT 基盤の設計や実装を実施する上で，考慮すべきネットワーク上のセキュリティの要素とそのポイントについて習得．また，攻撃者が繰り出す攻撃手法も確認し，攻撃手法に合わせた具体的な対策を習得.
若手	Web アプリケーションセキュリティ基礎	Web アプリケーションの脆弱性を狙った攻撃に対抗するため，開発者として最低限理解しておくべき，Web アプリケーションの脆弱性，代表的な攻撃手法とその対策，言語に依存しない原理・原則を習得.
	サイバーセキュリティ対策オーバービュー	近年の傾向を踏まえて，どのようなセキュリティ知識・対策が必要になるかについて，入口対策を中心に習得．攻撃手法について身をもって体験することにより，現場での効果的なサイバーセキュリティ対策に必要な要素を習得.
中堅	セキュリティインシデント対応入門	セキュリティインシデント発生時の対応方法とその準備について習得．セキュリティインシデント対応に関わる全体像を習得した上で，初動対応部分に当たる内部/出口対策とログを利用した検知を中心に習得．習得を通じて企業やクラウドで運用されているシステムにセキュリティインシデント対応の準備を組み込めるようにする.
	Web アプリケーション開発者向けセキュリティ	アプリケーションに潜む脆弱性を診断する技術を習得．アプリケーションの脆弱性を見つける勘所と，その手法の習得を通じて，セキュアなシステムを構築する技術を習得.
共通	社内セキュリティコンテスト	サイバーセキュリティに関する攻撃・防御の両方の立場から，暗号，ネットワーク技術，セキュアプログラミング等，様々な問題が出題されるコンテスト．参加者同士で競い合うことでサイバーセキュリティスキルを向上させる.

5）サービスエンジニア

サイバーセキュリティにおけるサービスエンジニアの主な役割とは，システムの監視や運用・保守業務におけるセキュリティインシデントを防止することである．サイバーセキュリティの状況の変化に合わせ，現状の運用・保守方法の見直しの提言ができ，新たな

セキュリティインシデントを発見できる状態を目指し，育成する．

サービスエンジニアに対する育成方針は以下の通りである．

・社内の運用・保守プロセスに則ったセキュリティの見直しの促進．

・セキュリティインシデント対応スキルの向上．

・過去のインシデント情報の共有の促進．

6）ビジネスプロデューサー

サイバーセキュリティにおけるビジネスプロデューサーの主な役割とは，新規事業創出の初期段階で，サイバーセキュリティを踏まえたサービス企画を実施することである．新規事業をスモールスタートさせる際に，セキュリティに対する投資が充分に確保されるよう注意を払う．新規事業にはIoTやビックデータ分析等に代表される新技術が採用されることも多く，採用に伴うセキュリティリスクを理解しておかなければならない．セキュリティリスクへの対応の重要性を理解し，感度が高い状態を目指し，育成する．

ビジネスプロデューサーに対する育成方針は以下の通りである．

・新規事業を企画する上での，サイバーセキュリティに対する重要性の認識の向上．

・新技術に関するセキュリティリスクの理解の促進．

7）セールス

サイバーセキュリティにおけるセールスの主な役割とは，顧客に提供するシステムのセキュリティを意識し，ビジネスに組み込むことである．セールスは顧客に最も近い存在として，顧客のサイバーセキュリティに対する意識を高め，セキュアなシステムを顧客に提案できる状態を目指し，育成する．

セールスに対する育成方針は以下の通りである．

・顧客へのセキュリティに関するヒアリングスキルの向上．

・システム提案に組み込めるセキュリティ商品の知識の拡大．

・顧客にセキュリティ投資への理解を促す提案スキルの向上．

・重要な顧客情報の保護．

8）スタッフ

サイバーセキュリティにおけるスタッフの主な役割とは，自身の業務遂行上のセキュリティリスクを理解し，セキュリティインシデントを起こさないことである．スタッフには日本ユニシスグループ全社の重要な情報を扱っている組織が多く，所持している情報が誤って外部に流出することを防がなければならない．そのため，多様化するサイバーセキュリティの動向を把握し，情報を守ることができる状態を目指し，育成する．

スタッフに対する育成方針は以下の通りである．

・サイバーセキュリティに関する最新の基礎知識についての定期的な啓発．

・各組織の重要情報を一層適切に扱う風土の醸成．

3.4　セキュリティスキルの見える化

人材育成でスキルの見える化が困難であるという課題はどの分野にも共通しており，セキュリティ分野も同様である．セキュリティ分野は専門性の高さから，スキルが属人化しやすい傾向にある．また，スキルの多様性から強化が必要なポイントを特定しづらいという課題がある．スキルの見える化の課題を解決するため，日本ユニシスグループでは，役職員が自身のスキルレベルを登録することでスキルの見える化ができるスキル調査システムを導入している．この仕組みを活用し，セキュリティに関しては登録するスキルを詳細化することで，より効果的な人材育成施策の実施を計画している．

スキル調査システムに登録したスキルは，セキュリティ製品の領域を例として挙げると図2のようにグラフ化され，登録者のスキルが視覚的に分かりやすくなっている．また，スキル項目は毎年見直され，最新化している．

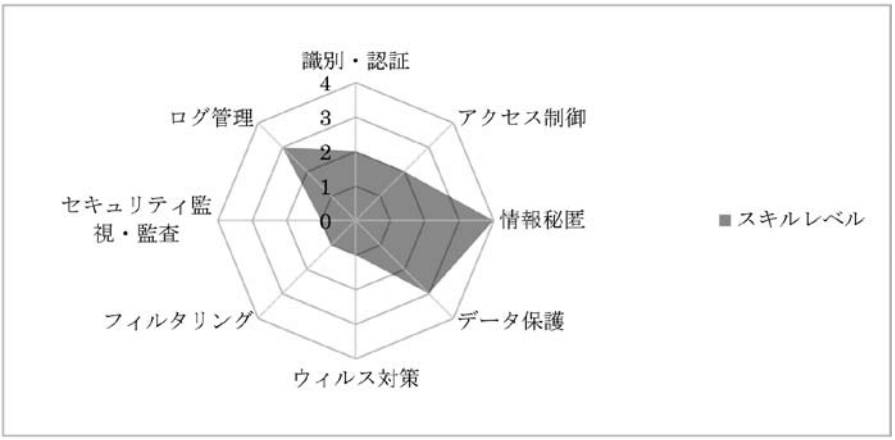

図2　個人のスキル調査結果グラフイメージ図

2019年度は，「サイバーセキュリティ戦略」に基づき，組織として習得すべきスキルとスキルレベルを精緻化・最新化し，実際の調査結果を比較することで今後のスキル強化施策の方向性を定めていくと共に，キャリアパスの見直しを検討していく．

また従来は，研修の実施後に行うアンケートの研修有益度や研修理解度の数値を基に施策の効果を測定していたが，実際のスキルに反映されているか見えづらいという課題があった．スキル強化施策を実施する前後でスキル調査システムの結果を比較することで，施策効果の見える化についても改善していく予定である．

今後の予定として，組織内に必ず一定のセキュリティスキルを持った人材を戦略的に配置し，配置した人材からサイバーセキュリティに関する情報を発信する，周囲にスキルの継承を実施する等，組織的にプラス・セキュリティ人材のサイバーセキュリティ能力の向上を実施できる施策を検討している．また，セキュリティ専門組織所属ではないがサイバーセキュリティスキルの高い人材を発掘し，セキュリティ専門組織の人材とローテーションを実施することで個人のサイバーセキュリティ能力の向上も図っていく．

3.5　サイバーセキュリティ専門人材の発掘

サイバーセキュリティ専門人材として活動するための重要な要素として，技術力とともにセキュリティに対する高い関心や安全確保への使命感を持っていることが挙げられる．日本ユニシスグループの多くのシステムエンジニアはセキュリティを主たる業務とする専門組織には所属せず，顧客のシステムを構築する中で自然にセキュリティに携わっている．セキュリティに高い関心を持っている人材は潜在的に存在しているが，発掘が困難である．

そのような人材を発掘するため，日本ユニシスグループは，社内育成プログラムの一環として社内セキュリティコンテスト「日本ユニシスグループ社内 CTF」を開催している．CTF（Capture The Flag）とは，コンピューターのハッキング技術を競うゲームである．サイバーセキュリティに関する攻撃・防御の両方の立場から，暗号，ネットワーク技術，プログラミング等，様々な問題が出題され，参加者同士で競い合う．一カ所に集合しての実施ではなく，オンライン上で一定期間を設けて実施することで，全国に散らばる日本ユニシスグループ役職員全員が参加しやすいようにしている．CTF の企画段階における問題の作成についても，セキュリティ専門部署と有志が協力して実施している．

上位入賞者は全社的イベントであるテクニカル・シンポジウム[*13]にて表彰し，グループ全体でサイバーセキュリティに取り組んでいることを意識してもらい，コミュニティ形成の場としている．

4. お　わ　り　に

組織に求められるサイバーセキュリティ人材について，情報セキュリティ人材との違いを述べた上で役割を整理し，日本ユニシスグループの人材育成への取り組みを例として紹介してきたが，サイバーセキュリティ人材の育成は一朝一夕には終わらない．セキュリティの分野は技術革新のペースが非常に速いため，「ここまで育成したら完了」という最終的なゴールはなく，組織は常に新しい技術を追いかけ，継続した育成が何よりも重要である．

IT 企業だけではなく一般企業においても，自組織におけるサイバーセキュリティスキルを見える化できる仕組みと，見える化の結果から判明した不足部分に対して，自組織内で育成するのか，外部調達をするのか優先順位をつけつつ判断することが重要である．本稿がサイバーセキュリティ人材の育成を検討する際の参考になれば幸いである．

最後に，本稿執筆にあたりご協力・ご指導頂いた全ての皆様に深く感謝し，御礼申し上げます．

＊1　日本の科学技術政策の基本的な枠組みを与えるものであり，日本が「科学技術創造立国」を目指して科学技術の振興を強力に推進していく上でのバックボーンとして位置づけられる法律

＊2　サイバーセキュリティに関する施策を総合的かつ効率的に推進するため，基本理念を定め，国の責務等を明らかにし，サイバーセキュリティ戦略の策定その他当該施策の基本となる事項等を定めた法律であり，2015年1月9日に施行された．サイバーセキュリティ協議会の設立が定められた改正法は2019年4月1日に施行された
＊3　サイバーセキュリティ基本法で定める，官民の多様な主体が相互に連携して情報共有を図り，必要な対策等について協議を行うための協議会
＊4　サイバーセキュリティ基本法第二十五条で定められた，サイバーセキュリティに関する施策を総合的かつ効果的に推進するため，内閣に置かれる組織
＊5　安心安全なデジタル社会を確立するための非営利・独立の民間シンクタンク
＊6　Computer Security Incident Response Teamの略称．コンピューターやネットワーク上で何らかのセキュリティ問題が発生していないか監視すると共に，万が一問題が発生した場合にその原因解析や影響範囲の調査等を実施する組織
＊7　単独のCSIRTだけで活動するのではなく，互いに協調する場を持ち，これまでにない高いレベルでの緊密な連携体制の実現を目指しながら，共通の問題を解決する場を設けることを目的として，設立された協議会
＊8「世界最高水準の『高信頼性社会』実現による経済・文化国家日本の競争力強化と総合的な安全保障向上」を基本目標に，三つの戦略と42の施策項目を提言している
＊9　日本ユニシスグループ全体の技術強化とビジネス拡大への貢献を目的とし，2009年から実行している戦略
＊10　新事業・新サービス創出に向けた価値発見（妄想・発想）から，事業化・商品化に向けたビジネスモデル構想・実行まで，全体を取り仕切る人材．
＊11　$(ISC)^2$（International Information Systems Security Certification Consortium）が認定を行っている国際的に認められた情報セキュリティ・プロフェッショナル認証資格
＊12　独立行政法人情報処理推進機構が認定を行っている情報系国家資格
＊13　日本ユニシスグループ社員一人一人の技術力の向上と，組織としての技術の蓄積と共有を目的とした催し

参考文献

［1］　澤田　雅広，「日本ユニシスグループのサイバーセキュリティ戦略」，ユニシス技報，日本ユニシス，Vol.39 No.2 通巻141号，2019年9月
［2］「JIS Q 27000：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－用語」，日本規格協会，2019年3月20日
［3］「セキュリティ人材不足の真実と今なすべき対策とは」，JCICシンクタンクレポート，一般社団法人日本サイバーセキュリティ・イノベーション委員会（JCIC），2019年2月
https://www.j-cic.com/pdf/report/Human-Development-Plus-Security.pdf
［4］　ITSS＋（プラス）・ITスキル標準（ITSS）・情報システムユーザースキル標準（UISS）関連情報，セキュリティ領域，独立行政法人情報処理推進機構，
https://www.ipa.go.jp/files/000058688.xlsx
［5］　一般会員（チーム）情報，日本コンピュータセキュリティインシデント対応チーム協議会，https://www.nca.gr.jp/member/index.html
［6］　平成29年度企業において育成すべき人材の知識・スキル及びカリキュラムに関する調査，内閣サイバーセキュリティセンター，
https://www.nisc.go.jp/inquiry/pdf/curriculum_honbun.pdf
［7］　清野　好紀，吉田　恵美，「日本ユニシスグループにおける情報セキュリティ専門人材の育成」，ユニシス技報，日本ユニシス，Vol.28 No.3 通巻98号，2008年11月

※　上記参考文献に含まれるURLのリンク先は，2019年7月2日時点での存在を確認．

執筆者紹介　奈　良　　将（Sho Nara）

2012年日本ユニシス(株)入社．公共部門にて官公庁のシステム構築・運用保守，自治体における小中学校の経営効率化業務を担当．2017年より，社内のセキュリティ・クラウド・データサイエンスなどに関する技術者育成に取り組む．現在，組織開発部に所属．情報処理安全確保支援士．

石　野　貴　子（Takako Ishino）

金融システム開発，インターネット接続環境における技術的セキュリティ対策適用業務，ISMSおよび個人情報保護等の情報セキュリティマネジメントシステム構築支援業務を経て，技術・マネジメント両観点からの情報セキュリティコンサルティング業務の経験を基に人材育成を担当．現在，プロセスアウトソーシング本部企画推進部に所属．CISSP．情報処理安全確保支援士．