サイバー社会に求められるセキュリティ技術者育成の実践

Practice of Training Security Engineers Desired in Cyber Society

● 佳山こうせつ　● 山下眞一郎　● 奥原雅之

あらまし

高度な技術を持ったセキュリティ技術者の育成は，従来より国内外を問わず重要な課題であり，育成のための様々な人材モデルが提案されてきた。一方，企業グループ内に多種多様なセキュリティ関連の業務がある富士通のようなICTベンダーでは，これらを遂行するために必要なスキルを持つ技術者の計画的育成において，既存のセキュリティ技術者人材モデルをそのまま使うことは困難であった。そこで富士通は，独自の「セキュリティマイスター」というセキュリティ技術者人材モデルを定義し，このモデルに基づく人材認定制度の運用を2014年1月から開始した。また，セキュリティ部門にとどまらず，システム開発，ICT運用，コーポレートなどの各部門を含めたセキュリティ技術者人材モデルを策定し，部門ごとに必要な人材の定義から，人材の発掘および育成プログラムを提供した。

本稿では，これらの人材モデルに基づいた各組織における実践の内容と，その効果について紹介する。

Abstract

The training of security engineers with advanced technical skills has been a key issue both in Japan and overseas and various human resource models have been proposed for it. Meanwhile, for vendors of information and communications technology (ICT) with a wide variety of security-related operations in their corporate group, such as Fujitsu, it was difficult to use the conventional security engineer human resource models as they were in the systematic training of engineers with skills required to perform these operations. Accordingly, Fujitsu defined its original model of security engineer human resources, called Security Meister, and started implementing a human resource certification system based on this model in January 2014. In addition to the Security Division, we have formulated security engineer human resource models including those for Systems Development, ICT Operation, Corporate and other divisions to define human resources required for the respective divisions, discover human resources and provide training programs. This paper presents the details of the activities in the respective organizations based on these human resource models and the results.

ま え が き

高度な技術を持ったセキュリティ技術者の育成は，従来より国内外を問わず重要な課題である。

日本では，経済産業省が独立行政法人情報処理推進機構（IPA）とともに策定したITスキル標準[(1)]において「自社の経営戦略やIT戦略の一環として情報セキュリティ戦略（対策）を立案・推進する役割を担う人材を育成等の方法により確保すべきである」とし，これに併せて情報処理技術者試験を制度化している。

米国では，White House Cyberspace Policy Review June 2009[(2)]を受け，米国国立標準技術研究所（NIST：National Institute of Standards and Technology）が，サイバーセキュリティ教育のためのプログラムであるNICE（National Initiative For Cybersecurity Education）を提供し，National Cybersecurity Workforce Framework[(3)]に基づいて体系化された人材育成を実現している。

グローバルスタンダードとしては，米国規格協会（ANSI）よりISO/IEC17024の認証を受けたInternational Information Systems Security Certification Consortium[(4)]がCISSP（Certified Information Systems Security Professional）認定資格を提供している。更に，大手ヘルスケアサービス企業やそのほかの主要企業において，CISSP認定資格の取得が情報セキュリティ関連業務従事者の必須事項とされており，世界各国で9万7000名以上（2015年3月現在）がCISSP認定資格を取得している。

このように，それぞれの組織や認定資格が現代のサイバー社会に必要なセキュリティ技術者人材モデルを提示し，安心・安全な社会の実現に向け大きな役割を果たしている。一方で，富士通のようなICTベンダーにおいては，企業グループ内に多種多様なセキュリティ関連の業務がある。これらの業務を遂行するために必要なスキルを持つ技術者の計画的育成を考えると，既存のセキュリティ技術者人材モデルをそのまま使うことは，以下の理由により困難である。

（1）ITスキル標準やCISSPでは，人材像の粒度が「セキュリティエンジニア」のレベルで設定されており，実業務を担当するために必要な各種の業務スキルを育成する上では細密度が不足している。

（2）NICEは人材類型が細分化されており，上記の問題は解決できるが，定義されている人材類型が米国のビジネスモデルを前提としているため，日本の業務にそのまま当てはめることは難しい。

（3）経営層の意思決定に必要な情報をエスカレーションするためには，各現場と経営層を橋渡しするための人材が必要であり，現場ごとにそれぞれ異なるセキュリティ人材像に応える必要がある。

このため，富士通ではこれらの既存の人材モデルを参考にしながら，日本国内とグローバル双方に適用できる独自の人材モデルを定義し，それに基づくセキュリティ技術者の認定である「セキュリティマイスター認定制度」の運用を2014年から開始した。本稿では，このセキュリティ技術者人材モデルの考え方と，認定制度の運用について述べる。

セキュリティ技術者人材モデル

企業において，セキュリティ業務は情報部門やセキュリティ部門だけでなく，様々な部門に散在している。企業として現代のサイバーセキュリティに対する脅威に立ち向かうためには，こうした脅威から守るための人材のポートフォリオを考慮して，全ての業務を検討する必要がある。例えば，セキュリティ部門の人材を高度に育成するだけではなく，企業内の組織ごとに必要なセキュリティ技術者像を明確化し，育成していくことが求められる。また，システム開発，ICT運用，コーポレートの各部門などに対しても必要とされるセキュリティ技術者の人材モデルを定義する。更に，システム運用や法律，経営だけでなく，セキュリティも理解し実践できる人材を計画的に育成する。これによって，企業におけるセキュリティ対応力のベースライン向上を実現し，経営リスクの低減に大きく貢献できる。

その実現に向け，富士通では独自のセキュリティ技術者人材モデルである「セキュリティマイスター」を定義した。このモデルでは，企業内の様々なセキュリティ業務に対応するため，セキュリティ人材を三つの領域，15の類型に細分化して定義している。

図-1に示すように「領域」は，そのセキュリティ

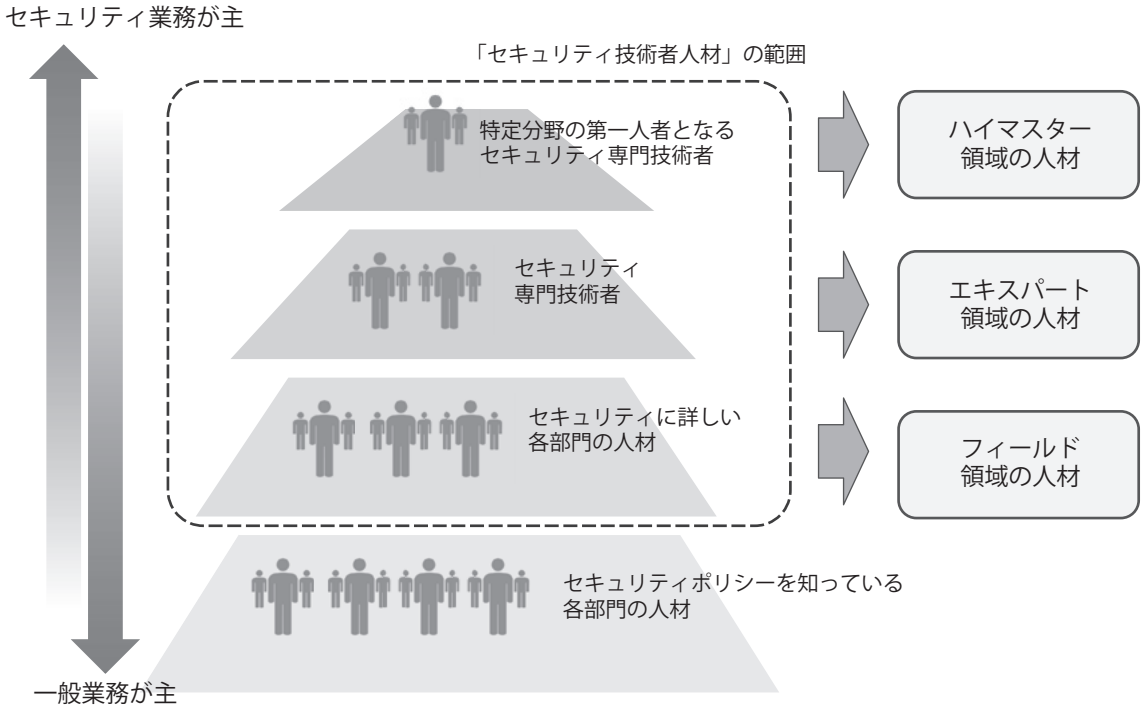

図-1　三つの人材領域

技術者がどの程度セキュリティ技術に特化した業務を遂行しているかを表現する区分である。セキュリティ業務への特化レベルが高いものから順に，ハイマスター領域，エキスパート領域，フィールド領域の3領域を定義した。

(1) ハイマスター領域

特定分野における業界最高レベルのセキュリティ技術を有し，日々変化する高度な脅威に対抗するための人材

(2) エキスパート領域

高度なセキュリティ特化技術を有し，高度なサイバー攻撃に対抗する最適なソリューションを提供するための人材

(3) フィールド領域

システム開発・サービス運用現場で高度なセキュリティ技術の適用を推進し，お客様業務の安心・安全を実現するための人材

「類型」は，各領域内で業務に合わせて細分化された人材の詳細モデルであり，前述のNICEなどの人材モデルを参考にしながら富士通独自のノウハウも加味し，**表-1**のように定義した。

各類型には，その人材類型の技術者が持つべきスキル，想定される業務，推奨される資格などがそれぞれ詳細に定義されている。グローバル化を意識し，前述のCISSP資格の取得を前提とすることなども考慮した。セキュリティインシデントハンドラーの類型定義を**図-2**に示す。このように詳細に定義することで，求められる人材像を細分化でき，必要な教育の選択や開発につなげることができる。

また，各類型の技術者に求められるスキルは，大別すると**図-3**に示すようにセキュリティコア，情報技術系，非情報技術系の三つに分類できる。

表-1　人材類型の定義

領域	類型
ハイマスター	・コードウィザード ・コンピュータウィザード ・グローバルホワイトハッカー ・シニアセキュリティコーディネーター
エキスパート	・セキュリティプロダクトエキスパート ・セキュリティネットワークコーディネーター ・サイバーリスクアセッサー ・ペネトレーションテスター ・サイバーリサーチャー ・セキュリティアナリスト ・フォレンジックエンジニア
フィールド	・システムセキュリティエンジニア ・上級システムセキュリティエンジニア ・セキュリティインシデントハンドラー ・上級セキュリティインシデントハンドラー

<table>
<tr><td rowspan="2">  </td><td>人材概要</td><td rowspan="2">スキルマップ</td><td>基礎理論</td><td></td><td>データベース</td><td></td></tr>
<tr><td rowspan="6">システム運用部門に籍を置き，システムのセキュリティ運用設計および運用現場のセキュリティを担当する</td><td>アルゴリズムとプログラミング</td><td></td><td>ネットワーク</td><td>■</td></tr>
<tr><td>コンピュータ構成要素</td><td>■</td><td>セキュリティ</td><td>■■</td></tr>
<tr><td>システム構成要素</td><td>■</td><td>サービスマネジメント</td><td>■■</td></tr>
<tr><td>ソフトウェア</td><td>■</td><td>システム監査</td><td></td></tr>
<tr><td>ハードウェア</td><td></td><td>システム戦略</td><td></td></tr>
<tr><td>マルチメディア</td><td></td><td>法務</td><td></td></tr>
<tr><td>主な業務</td><td colspan="6">システムの要件定義段階において顧客とセキュリティ運用要件を折衝する
システムの運用設計段階においてシステム全体のセキュリティ運用（※）およびデシジョンテーブルを定義する
※必要となるログの定義，トリガーの設計，パッチ運用設計など
システムのテスト段階において設計したセキュリティ運用が実際に運用できるか確認する
OSやミドルウェア，プロダクトの出力するログを見てセキュリティインシデントかどうかデシジョンテーブルに従って一時切り分けと応急処置を行う</td></tr>
<tr><td>ビジネス貢献/必要性</td><td colspan="6">運用サービスの品質（セキュリティ）向上</td></tr>
<tr><td>標準スキル</td><td colspan="6">セキュリティに関する応酬話法ができる
想定脅威に対する運用対策を考えられる
セキュリティを考慮したシステム運用の設計ができる
・コンピュータの構成要素，システムの構成要素について理解している
・インターネット技術（IPv4，NAT，DNS，Proxyなど）について理解している
・情報資産に対する物理的脅威，技術的脅威，人的脅威を理解している
・Webサービスに対する代表的な攻撃手法と攻撃された場合の脅威と対策について理解している
・代表的なOSやミドルウェア，プロダクトが出力するログを理解している
セキュリティインシデント発生時に現場のとりまとめができる</td></tr>
<tr><td>推奨スキル</td><td colspan="6">情報セキュリティスペシャリストまたはネットワークスペシャリストを取得している</td></tr>
</table>

図-2　人材類型定義の例(セキュリティインシデントハンドラー)

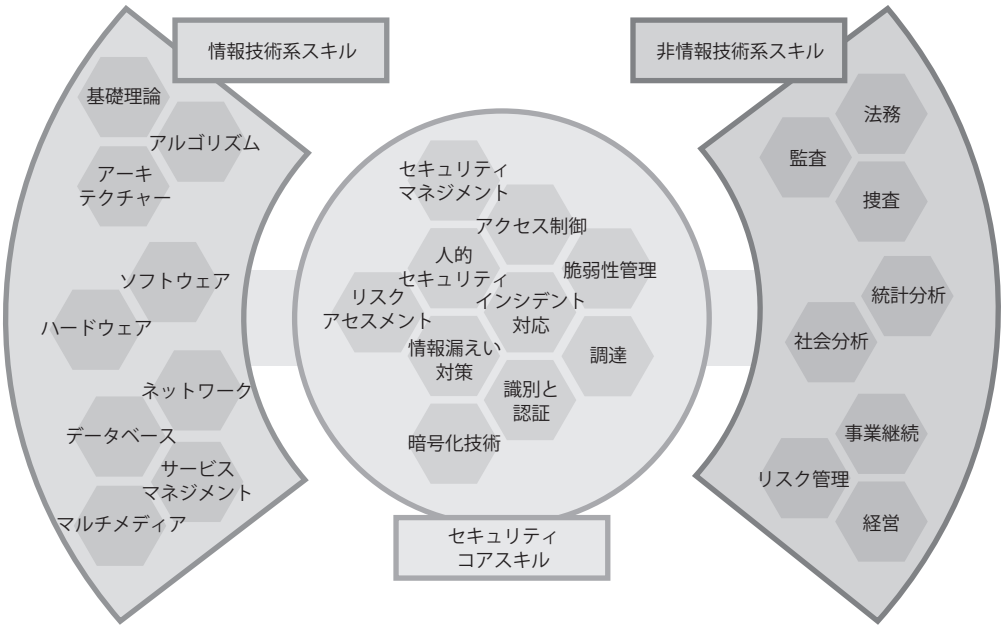

図-3　富士通のセキュリティ技術者人材モデル

組織がセキュリティ技術者に求めるのは，実はセキュリティコアスキルや情報技術系スキルといったいわゆる理系のスキルだけでなく，非情報技術系スキルといった文系のスキルも挙げられる。

例えば，セキュリティインシデントの分析業務では，経営者の意思決定に必要な情報を分析する

ために，ネットワークなどの情報技術系スキル，社会分析やリスク管理などの非情報技術系スキル，そしてセキュリティコアスキルをバランス良く兼ね備えるハイブリッドな人材が必要になる。

セキュリティマイスター認定制度

本章では，本セキュリティ技術者人材モデルに基づき，企業内にどの程度セキュリティ技術を持つ技術者が在籍しているかを可視化し，これに基づいてセキュリティ技術者を計画的に育成するために推進している「セキュリティマイスター認定制度」について述べる。本制度の認定プロセスを**表-2**に示す。

本制度の特徴は，認定プロセスの中で一般的な認定試験を採用していないことである。認定試験制度の維持には莫大なコストがかかり，一企業で実施するのは現実的ではない。このため，必要となる知識の確認については，情報処理技術者試験やCISSPなど外部資格の取得を前提とすることで，認定試験に代えることとした。

また，ハイマスターについては，その性格上定型的な認定方式の確立が難しいため，現段階では既存ハイマスターによる面接に合格することを必須要件としている。つまり，現在認定されている既存ハイマスターを納得させるだけの実績とスキルを持っていないと認定されないという制度設計である。

富士通では，それぞれの領域における目標人数を以下のように定め，計画的・継続的に育成し，各現場へ配備することとした。

・ハイマスター領域：20名
・エキスパート領域：100名
・フィールド領域：580名

富士通には約2万7000名のエンジニアが在籍するが，そのうち40 ～ 50名に一人がセキュリティマイスターとして配備されるように算出されており，人材の受け皿と育成のバランスを考慮した数値となっている。

2015年8月現在，約400名のセキュリティマイスターが認定され，各現場でサイバー攻撃を想定した対策や組織のセキュリティ対策レベルの向上に貢献している。

表-2　認定プロセス

領域	認定プロセス
ハイマスター	・書類審査 ・既認定ハイマスターによる面接
エキスパート	・必須外部資格の取得 ・必須教育の受講（4 ～ 7日） ・書類審査
フィールド	・必須教育の受講（2日） ・教育修了テストの合格

資質ある技術者の発掘と育成

セキュリティマイスター認定制度によりセキュリティ技術者の人材モデルを明確に定義し，そのスキルの保有者を可視化することで，資質ある技術者の発掘につなげることができる。ネットワークやデータベースの深い理解と経験を有する優秀な人材は開発部門に，社会分析やリスク管理の深い理解と経験を有する優秀な人材はスタッフ部門に在籍していることが多い。これまでセキュリティ技術者はセキュリティ部門の人間を育成することが多かったが，セキュリティに活用可能な資質を有する技術者を組織横断で発掘することが，効果的な育成につながる。

富士通では，人材の発掘とセキュリティ技術者数の拡大につなげるために，本認定制度の関連イベントとして，グループ全体の従業員を対象とした社内セキュリティコンテストを開催した。社内セキュリティコンテストはCTF（Capture the Flag）という競技形式を採り，ネットワークの通信から不正な通信を見つけ出す技能を競わせる問題などを出題する。また，技能を発揮する様子を**図-4**のようにリアルタイムで表示するダッシュボード機能を取り入れた。これにより得意な技術を可視化し，潜在する有能な技術者を発掘できる。本コンテストを2014年度より年2回の頻度で実施しており，結果としてセキュリティ部門以外の開発部門やコーポレート部門から数多くの入賞者を生み出し，グループ全体が潜在的に保有しているセキュリティ資質のある技術者を発掘することに成功した。

素養のある人材を発掘した後に必要となる次のプロセスは，実践力を重視したプログラムによるセキュリティ技術者の育成である。各現場の業務経験に比べセキュリティ業務の経験が乏しい人材に向けて，経験値を高め，サイバー攻撃の全貌を理解させる育成プログラムが効果的である。

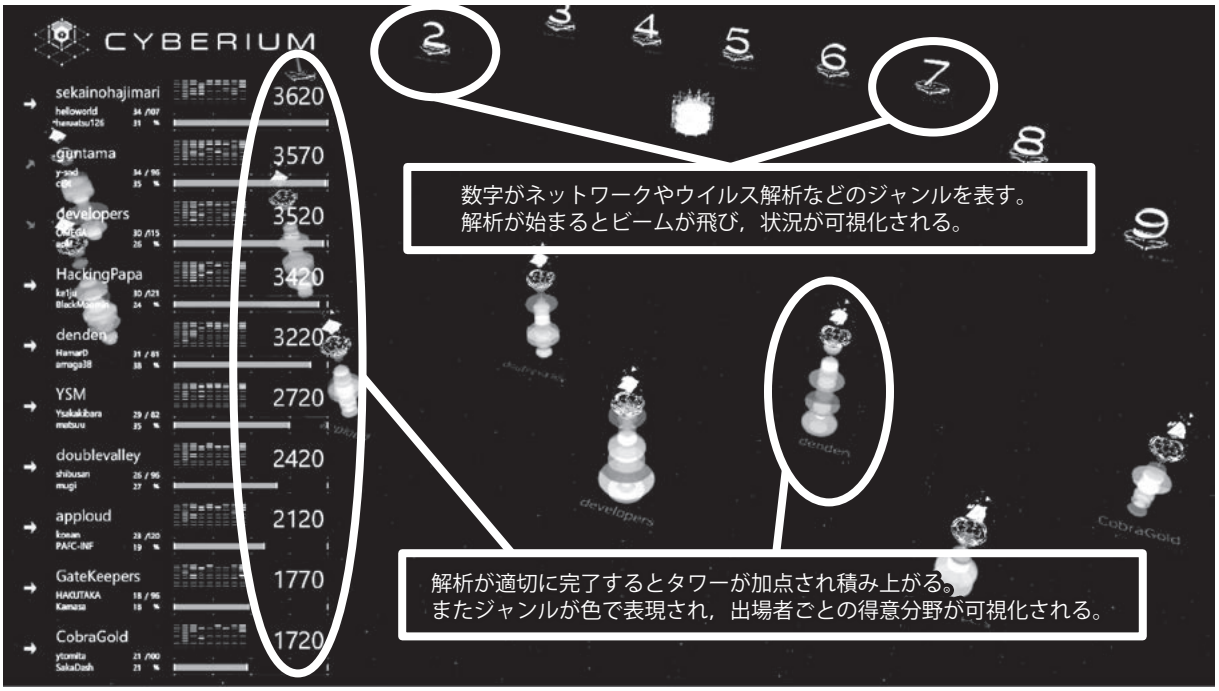

図-4　コンテストを可視化するダッシュボード

そこで，富士通のこれまでの知見を活かし，サイバーレンジ（仮想演習場）による演習を全面的に採用したプログラムを開発した。現場で頻繁に遭遇する状況を再現する環境と，高度な攻撃をシミュレーションするシナリオとを併せた独自のセキュリティ技術者育成プログラムである。以下に示す七つの特徴を持つ実践的な演習により，セキュリティインシデント（侵入事件）が発生している状況下で事業を可能な限り継続させつつ，一つのセキュリティインシデントの初動から分析，エスカレーション，クロージング（完了）までのプロセスを網羅的に体験できる。なお，本育成プログラムは，富士通ラーニングメディアを通じてお客様にも提供可能となっている。

(1) 富士通のコアテクノロジーを活用した仮想環境で，一般的に実装されるネットワークとサーバ構成を完全に再現
(2) 業務データが流れるリアルな環境における攻撃と防御の疑似体験と各種検証の実施
(3) 現実の攻撃者が使用する攻撃の手口とプロセスの全体像をハンズオン形式で実際に体験
(4) 3Dグラフィックによる独自開発のダッシュボードで攻撃と防御の状況を可視化することにより，受講者の理解をサポート
(5) 受講者自身が解析した結果に基づく攻撃手口のタイムラインレポート作成を実習
(6) タイムラインレポートに基づく，意思決定者へのエスカレーションを実習
(7) 暫定策だけでなく，恒久策の策定提案を演習としてシミュレーション

一度認定されたセキュリティ技術者は，更にその専門技量を向上させるとともに，後進の育成も期待される。また，認定者同士が情報交流することで，お互いの課題を解決するなどの相乗効果も期待できる。このため，富士通ではセキュリティマイスター認定者のコミュニティ形成に向け，以下のような取組みを行っている。

・マイスター認定者のためのSNSサイトの開設
・マイスター認定者のメーリングリストの提供
・高度な技術を持つマイスターによる自主勉強会の実施
・マイスター同士が直接出会う場となる定例会の実施

上記の取組みにより，セキュリティはセキュリティ部門の仕事という固定観念を払拭し，組織横断で取り組む意識の醸成が進みつつある。一般的

にセキュリティ部門と非セキュリティ部門との間には，いくつかの意見の隔たりがある。マイスター認定制度による人材交流は，技術者同士の相互理解を進め，こうした現状を打開する強力な推進力となり得る。このような部門間の橋渡しを行う人材は，今後のサイバー社会においてより重要性が増していくものと考えられる。

むすび

本稿では，今日のサイバー社会に必要なセキュリティ技術者の育成について，富士通の取組みであるセキュリティマイスター認定制度を交えて述べた。また，様々な人材育成の考え方を活かし，企業の成熟につなげるため，セキュリティ部門だけでなく企業全体で必要なセキュリティ技術者人材モデルを提示し，組織を横断したセキュリティ技術者の育成の施策とその効果について論じた。

サイバー社会において，セキュリティ対策スキルはあらゆる企業に必要不可欠である。富士通では，セキュリティマイスターが高度なセキュリティ業務を遂行するとともに，組織間の橋渡し人材として機能し，それぞれの現場にセキュリティ意識を醸成することによって，ヒューマンセントリックインテリジェントソサエティを支える，安心・安全をお客様に提供できると考えている。

参考文献

(1) 独立行政法人情報処理推進機構：IT人材における情報セキュリティの育成ニーズ・課題調査最終報告書（詳細版）．平成26年3月．
https://www.ipa.go.jp/files/000039527.pdf

(2) White House：Cyberspace Policy Review．June 2009.
https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf

(3) NIST：National Cybersecurity Workforce Framework.
http://csrc.nist.gov/nice/

(4) (ISC)^2:IT Certification and Security Exparts.
https://www.isc2.org/

著者紹介

佳山こうせつ（かやま　こうせつ）
クラウド事業本部サイバーディフェンスセンター 所属
現在，外郭団体との協働，およびグループ会社と連携した人材育成業務に従事。

奥原雅之（おくはら　まさゆき）
クラウド事業本部サイバーディフェンスセンター 所属
現在，情報セキュリティに関わる富士通グループの戦略策定とセキュリティ施策推進業務に従事。

山下眞一郎（やました　しんいちろう）
クラウド事業本部サイバーディフェンスセンター 所属
現在，社内セキュリティインシデント緊急対応，および情報分析業務に従事。