JNSA PRESS

JAPAN NETWORK SECURITY ASSOCIATION

AUTUMN 2018 VOL. 46

寄稿

人はなぜメールのマルウェアを実行するのか?
02

脆弱性診断、ここに導かれて
08

経営者に情報セキュリティ対策の必要性を訴求する手法について
12

CONTENTS

特定非営利活動法人
日本ネットワークセキュリティ協会
NPO Japan Network Security Association

ネットワーク事業者における セキュリティ対策

JNSA 理事
KDDI 株式会社
技術開発戦略部　三宅　優

今年の5月23日に、「電気通信事業法及び国立研究開発法人情報通信研究機構法の一部を改正する法律」が公布されました。電気通信事業法の改正には、深刻化するサイバー攻撃への通信事業者の対処の促進も含まれています。皆さんもご存じのように、セキュリティの観点から問題があるIoT機器がネットワークに大量に接続されたことにより、サイバー攻撃の標的がIoT機器に移行し、マルウェアに感染したIoT機器が増加しています。そこで、サイバー攻撃の送信元となるマルウェア感染機器などの情報を共有するための制度を整備し、通信事業者による利用者への注意喚起・攻撃通信のブロック等を促進するための法律改正が行われました。

インターネットワークを使っている方には、ネットワーク事業者側でもっとサイバーセキュリティ対策を行ってほしいと思っていらっしゃる方も多いと思います。私は、国連傘下の電気通信に関わる標準化活動に参加しておりますが、その場においても多くの国から国際連携によるサイバーセキュリティ対策を求める声が上がりますが、各国の法律・規制や政策の違いから統一的なものを作るのは容易ではありません。例えば、日本では憲法で通信の秘密が保証されており、原則として通信の内容を見ながら判断することはできません。この制約の下で日本は、消費者保護の観点から、政府と通信事業者を含む民間企業が連携してサイバーセキュリティ対策を行ってきており、ネットワーク側でのセキュリティ対策の重要性を認識しているとともに、他国よりも先んじた取り組みを行っていると思います。

IoT時代になり、これまでのセキュリティ対策では不十分になるとともに、多くの人々(機器製造者、機器設置者、利用者、等) がセキュリティについて考えなければ、安全性が確保できなくなりつつあります。しかし、多くのものはセキュリティ機能が無くても動きますし、セキュリティの知識が無くても利用できてしまいますので、この状況 (期待するセキュリティ対策が行われない) を踏まえた対応が必要です。前述の通り、ネットワークにおいては法律改正により以前より踏み込んだ対策が取られようとしており、今後対策が進むと考えられますが、ネットワーク側での対策には通信の秘密等の制限がありますし、すべての通信を詳細に解析して対策することも困難です。IoT時代に向けて多くのセキュリティ対策が検討されていますが、ネットワーク側の対策はその1つであり、さらに多くの種類の対策が必要な状況です。ネットワーク利用者がセキュリティの知識が無くても安全に利用できる環境を構築していくことが必要とされている中で、多種多様な企業、団体が参加するJNSAの場において、セキュリティに対する課題を共有し、新たなセキュリティ対策や取り組みが相互に作用して効果を発揮するような活動ができればと思います。

人はなぜメールのマルウェアを実行するのか？

株式会社ラック
鈴木　悠

1. はじめに

「メールに添付されている不審なファイルやURLはむやみに開かない。」メールからのマルウェア感染等を想定し、その対策として多くの組織でルールの規定、教育・訓練、注意喚起が行われている。しかし、それにも関わらず必ず不審な添付ファイルを開封する人がいる。

メールを用いた攻撃は、システム的対策と人的対策の双方が必要となる。しかし、人的対策に対し、人を起点とした心理的側面から検討する研究は少ない。本稿では、標的型攻撃を想定したメール訓練における現状から、その背景となる人の心理的側面について考察すると共に有効策を述べる。

2. メール訓練における現状

メールを用いた標的型攻撃に対し、教育･訓練という人へのアプローチを試みる施策にメール訓練がある。メール訓練の有効性については、短期的（2週間）および長期的（約1年）な教育効果が確認されている[1]。つまり、メール訓練を定期的に実施することにより、不審な添付ファイルやURLを開く人を減らすことが出来る。

しかし、得られる効果は一定数に留まり、完全に0人にすることは難しい。例えば、メール訓練を毎年実施しているA社では、訓練メールの添付ファイルやURLを開いた人の割合（以下、開封率とする）が15%から下がらない（図1参照）[2]。

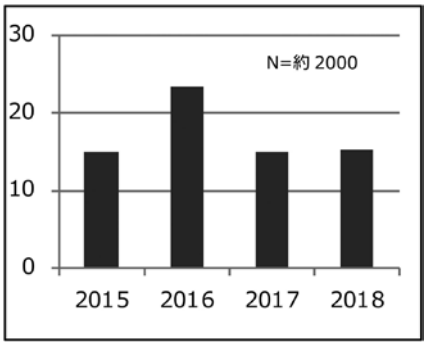


図1.　年度別開封率（%）

A社においては、前年度の開封者に対し、もう一度同じ文面の訓練メールを配信するという試みが行われている。その結果、2017年度では37.2%、2018年度では33.3%が同一文面の訓練メールにて再び添付ファイルを開封していた。このように、メール訓練において学習効果が得られない層が必ず一定数存在する。

3. 態度ー行動の関係

人間が何らかの決定に基づいて行動する背景には、物事に対する考え方や姿勢としての「態度（attitude）」がある。この態度は、先天的なものではなく、様々な経験や学習を通して後天的に形成されている[3]。

この形成された人の態度を外的な力により変化させることを「態度変容」という。人の態度が変容するステップをモデル化したものに「連合命題評価モデル（APEモデル）」がある（図2参照）[4]。

外部の影響からこれまでの経験による推測が活性

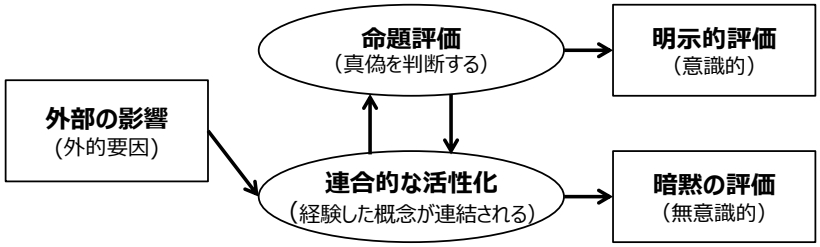


図2.　連合命題評価モデル

化し、その演繹的推論から真偽判断を行い行動するというものである。受信したメールに対し、メールの差出元や本文内容等の情報から推測し、正規か否かを判断し、開封または削除といった行動を行う。

この態度変容を促進するものに「学習[5]」と「説得[6]」がある。メールを利用した攻撃では、攻撃者がメール本文等の「説得」により、受信者の態度を変容させ、添付ファイルや本文内のURLを開かせようとする。これをメール訓練により「学習」することで開封させないという構図である。

学習に関しては既にメール訓練の有効性が示されているため、本稿では説得に焦点をあてる。

4. 攻撃者による説得

説得とは、コミュニケーションにより受け手の理性や感情に働きかけ、相手の自発性を尊重しながら、送り手の意図する方向に受け手の意見、態度、行動を変化させることである。相手の説得に応じれば態度及び行動が変化し、逆に応じなければ元の態度を守る。

説得は、動機付けと認知的能力で決まるとする「精緻化見込みモデル[7]」がある（表1参照）。

表1.　精緻化見込みモデル

		動機付け	
		高	低
認知的能力	高	中心的ルート	
	低		周辺的ルート

「動機付け」とは内容が妥当かどうかを吟味しようとすることであり、吟味する能力が「認知的能力」である。認知的能力は学習により高めることができるが、思考を妨害する要因がある場合には十分に発揮されない。

動機付け及び認知的能力が高い場合、受け手が説得されて開封する確率が高まる（中心的ルート）。逆に、動機付け及び認知的能力が低い場合、受け手は判断に迷い、判断材料を求める（周辺的ルート）。メールを用いた説得では、中心的ルートは本文の説得力、周辺的ルートにおいては差出元への信頼が影響するという結果がある[8]。

5. メール受信者の判断と行動

心理学では性格とリスク行動に関する研究が行われており、性格→認知的要因→リスク行動という因果構造が示唆されている[9]。セキュリティという観点においても、これまでにセキュリティ事故と性格特性を明らかにしようとする研究が行われてきた。

標的型メールの検証実験において、開封群は非開封群よりも自己効力感（課題解決能力の自己評価）が高く、被害を小さく予想するという結果がある[10]。

一方、ヒューマンエラーを起こしやすい性格には情緒不安定性・非調和性・非勤勉性があるとし、スキル向上の意識が低いため事故を起こしやすいと考察されている[11]。

このような性格傾向があることを踏まえたうえで、攻撃者の説得によるメール受信者の態度変容とその有効策を考察する。

6. 態度変容と有効策の考察

6.1. 環境的・身体的要因

図2の連合命題評価モデルでは、外部の影響に対して連合的な活性化が発生しないと無意識的な行動（暗黙の評価）に繋がる。

ヒューマンエラーの発生する環境的な要因として業務集中があり[12][13]、多忙により思考力が低下すると、受信したメールを吟味することなく反射的に開封する可能性がある。このような場合、メール訓練による学習効果は発揮されないため、労務管理も重要である。

6.2. 認知的能力

訓練メールの開封率は、メール習熟度、1日当たりのメール数、処理メール通算、メール訓練経験の有無で差がある[1]。このため、本稿では認知的能力を

メールの利用頻度が高く、メール訓練経験がある人とする。

（1）認知的能力：高

認知的能力が高い人の開封率は、論拠の質、つまりメールの巧妙さに依存する。例えば、同一文面の訓練メールであっても、差出人がフリーメールアドレスの場合は開封率が27.3%だが、自組織のドメインの場合は40.6%と開封率が高くなる [2]。標的型攻撃メールは手口が年々巧妙化しており、「不審メール」ではなくなってきている。このため、認知的能力が高い人であっても開封することも想定し、疑わしいメールを受信した際や開封時の報告は周知徹底しておきたい。また、メール訓練を実施した際には、報告受理後のインシデント対応についても訓練しておくことが有効だろう。

なお、メール訓練において、興味本位で開封する人がいる。これは、ヒューマンエラーとは異なり、意図する違反行動である。心理学では、「リスクテイキング（不安全）行動」に該当し、自己中心性と楽観視により引き起こされるとしている [14]。万が一マルウェア感染被害が発生した場合の組織及び業務への影響とその責任について言及し、違反行動に対するモニタリングを強化することが有効だろう。

（2）認知的能力：低

認知的能力が低い開封者には、これまでの先行研究から、自己に基づき判断する「自己効力感」[10]と他者に基づき判断する「信頼」[8]のいずれかが作用していると考える。

自己効力感が高い人は、自分には「知識」と「これまで感染しなかった経験」があるから大丈夫と思い込む「正常化バイアス」が強く働き、マルウェアに感染する確率とその被害を低く見積もる。

有効策として、訓練により警戒心を高めることが示されており [10]、マルウェア感染を擬似体験することも効果的とされる [15]。

6.3. 動機付け

メール訓練では、複数の文面パターンが用いられる。訓練メールのテンプレート別の開封率では、組織内通達に似た文面において開封率が高い（表2参照）[2]。また、メール訓練後のアンケートにおいても、開封理由を業務への関連性に言及する人が多い（表3参照）[2]。

表3.　訓練メール開封理由の割合（%）

開封理由	回答率
判断できなかった	28.4
業務に関連すると思った	**55.8**
不審だが念のため確認した	7.4
興味本位で開封した	5.3
誤送信と思い確認した	1.1
うっかり開封した	17.9

業務関連度と開封率における統計的な有意差は訓練対象組織によって異なり、業務関連度が高い場合だけでなく無関係である場合も開封率が高く因果関係は不明である [1]。本稿では、動機付けを業務関連度

表2.　訓練メールテンプレート別開封率上位5（%）

件名	平均	添付型	URL型
人事発令	36.7	19.3	42.5
至急：PDFに関する注意喚起	20.4	32.6	14.4
当社代表取締役社長の番組出演に関するお知らせ	18.0	5.4	22.2
【医療費通知】	17.0	17.0	16.9
事業継続計画の定期見直し	16.2	-	16.2

と仮定したうえで、業務への関連有無に関わらず開封率が高くなる理由について考察する。

（1）動機付けに影響を及ぼす要素

他者の行動へ影響を及ぼす潜在能力に「社会的勢力[16]」（表4参照）がある。この社会的勢力の影響が及ぶ背景には、情報源への信頼が関係している[17]。

人は、メールが正規か否かを判断する際、差出元やメール本文に含まれるいくつかの要素による影響を受けている。

表4.　社会的勢力

名称	内容
報酬勢力	報酬、承認、賞賛、見返り
強制勢力	不利益、懲罰、叱責
正当勢力	権威、権力による義務化
準拠勢力	魅力、同一視、追従
専門勢力	集団内の専門的知識
情報勢力	集団外の専門的知識

（2）動機付け：高

メールの受信者が、業務に関連する内容と認識した際、開封という行動に及ぼす影響力として表5のようなものが考えられる。

表5.　業務関連度が高い場合の影響力の例

影響力	内容
強制勢力	・内容を確認しないことの処罰
正当勢力	・上司や親組織からの依頼 ・管理部門からの通達
専門勢力	・システム部門からの注意喚起
情報勢力	・既知の外部組織からの回覧

このような影響力を強く受ける人または組織内環境である程、内容を確認しない事によるデメリットがマルウェア感染リスクを上回り開封する。

業務関連度が高いメールに対しては、判断がつかない場合の開封前の確認手段（電話での本人確認、第三者への確認、イレギュラー対応発生時のマニュアル等）を決め、周囲に相談しやすい環境作りをしておくことが有効だろう。

（3）動機付け：低

メールの内容が業務に関連していなくても開封する場合は、受信者が感じたメリット/デメリット（表6参照）や興味がマルウェア感染リスクを小さく見積もった場合、または思考せず反射的に開封している場合が考えられる。

表6.　業務関連度が低い場合の影響力の例

影響力	内容
報酬勢力	・金銭的報酬（還付金、返金） ・承認的報酬（取材対応依頼）
強制勢力	・支払い請求、訴訟通告 ・情報漏えいへの対処依頼

業務関連度が高い場合は客観的なデメリットによる判断であるのに対し、業務関連度が低い場合は主観的な判断が強く影響する。つまり、好奇心が強い、不安傾向が高い、物事を深く考えないといったような性格との関連があるのではないかと推測している。

心理学の古典的な性格テスト実験に、新聞の占い欄をコピーして配布し自分に当てはまるか5段階で評価をさせるというものがある。その実験結果では、平均4.26とほとんどの被験者が自分の性格に当てはまると回答している[18]。つまり、明らかに不審な点がなければ、人は業務関連度の有無に関わらず、自分宛にメールが来た時点で、どんな内容であっても「自分と結び付ける」可能性がある。このため、業務関連度ではなく、訓練メールテンプレートと開封者の性格特性との関連を検証する必要がある。

ただし、たとえメールを開封しやすい性格特性があったとしても、個人の性格や能力が有効に機能する職

種や業務もある。安易に開封者を叱咤・排除せず、セキュリティ意識を高める人的対策と制限や監視等のシステム的対策を個別に強化することにより、組織も人も守れるようになることが組織にとって有益である。

6.4. 各要因と有効策の実施による効果

メールの不審な添付ファイルやURLを開封する人について、心理的な側面から考察した要因と有効策を図3に示す。

まず、メールを受信した際には、組織が導入しているシステム的対策によってメールが選別される。入口対策としてサンドボックスやフィルタリング等により受信者への不審なメールの到達を防ぐ、出口対策としてネットワーク機器による制限や監視等によりマルウェア感染後の被害を封じ込めることで脅威を低減させる。これらのシステム的対策を標的型メールがすり抜けた場合、または予算の関係上システム的対策が導入できない場合、人的対策に頼るしかない。

攻撃者にとっては、いくつか送信したメールのうち、誰かが開封すればそれで目的は達成する。このため、組織のセキュリティ意識を全体的に高めても、1人の脆弱な人がいれば組織のセキュリティホールとなり得る。1人の脆弱な人が攻撃者が遠隔操作するマルウェアに感染すれば、組織ドメインを管理するActiveDirectory等を経由して組織内の被害は拡大する可能性がある。

本稿の考察では、環境的・身体的、認知的能力、動機付けの3つの要因から開封率が高まる理由とその有効策について述べた。特に注意すべき点は、動機付け（業務関連度）に関係なく反射、興味、恐怖等で開封する人が一定数存在し、セキュリティ教育・訓練を実施してもその効果が得られにくいと考えられることである。図3に示すとおり、各要因に対する有効策は異なる。メール訓練結果から開封者の開封理由についても言及し、効果的な有効策を実施することで、セキュリティの費用対効果を高めることができるだろう。

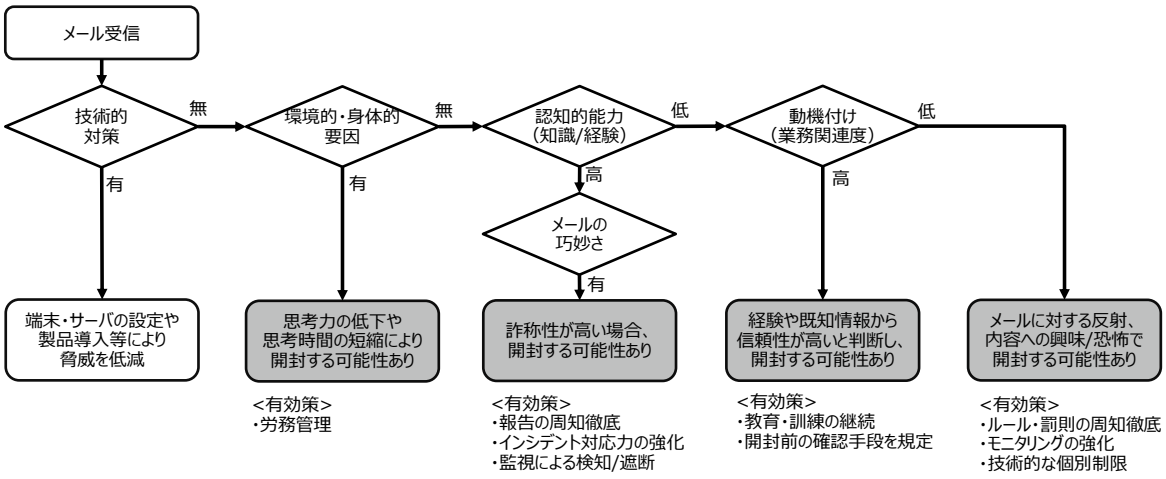


図3.　メールの不審な添付ファイルやURLを開封する過程とその有効策

参考文献

[1] 一般社団法人JPCERT コーディネーションセンター (2011年). 2009年度ITセキュリティ予防接種調査報告書. https://www.jpcert.or.jp/research/2011/inoculation20110309.pdf

[2] 株式会社ラック (2015～2018). ITセキュリティ予防接種サービス結果 (未公刊)

[3] Allport, G. W. (1935). Attitudes. Hand-book of social psychology, 798-844. Clark University Press.

[4] Gawronski, B., & Bodenhausen, G. V. (2011). The associative-propositional evaluation model: Theory, evidence, and open questions. Advances in Experimental Social Psychology, 44, 59-127.

[5] Lott, B. E., & Lott, A. J. (1968). A learning theory approach to interpersonal attitudes. Social Psychology, 67-88. Academic Press.

[6] Hovland, C. J. I., & Kelley, H. (1953). Communication and persuasion. Yale University Press.

[7] Petty, R. E., & Cacioppo, J.T. (1986). The elaboration likelihood model of persuation, Advances in Experimental Social Psychology, 19, 123-162.

[8] 小松文子・高木大資・吉開範章・松本勉 (2011). 情報セキュリティ対策を要請する説得メッセージによる態度変容の調査と実験, 情報処理学会論文誌, 52, 2526-2536.

[9] 上市秀雄・楠見孝 (1989). パーソナリティ・認知・状況要因がリスクテイキング行動に及ぼす効果. 心理学研究, 69, 81-88.

[10] 寺田剛陽・鳥居悟・安野智子・瀧澤弘和・新真知 (2013). リスク認知に基づく標的型メール対策の検討, 情報処理学会研究報告, SPT-5.

[11] 加藤岳久 (2013). 情報事故における性格とセキュリティ意識との相関に関する研究. http://jairo.nii.ac.jp/0063/00006803/en

[12] 島成佳・安 玲未・高木 大資 (2015). ITシステム運用現場のヒューマンエラーに影響を及ぼす要因分析と考察, 情報処理学会論文誌, 56, 2210-2218.

[13] 中村美香・近藤浩子・岩永喜久子・今井裕子・杉田歩美・須川美枝子・永井弥生 (2016). 看護職がインシデント・アクシデントを繰り返す要因に関する研究, 北関東メディカルジャーナル, 66, 279-288.

[14] James, R. (1990). Human Error, Cambridge University Press.

[15] 浜津翔・栗野俊一・吉開範章 (2015). 集団的防護動機理論に基づく情報セキュリティ対策実行意思モデルの提案とその活用, 情報処理学会論文誌, 56, 2200-2209.

[16] Raven, B. H. (1965). Social influence and power. Current studies in social psychology, 371–382.

[17] Nesler, M. S.& Aguinis, H. & Quigley, B. M.& Tedeschi, J. T. (1993). The Effect of Credibility on Perceived Power. Journal of Applied Social Psychology, 23, 1407–1425.

[18] Forer, B.R. (1949). The fallacy of personal validation: A classroom demonstration of gullibility. Journal of Abnormal and Social Psychology, 44, 118-123.

脆弱性診断、ここに導かれて

株式会社セキュアスカイ・テクノロジー
越智　郁

はじめに

「導かれているね」「一見関係なさそうだけど、繋がっているんだね」。

今回の寄稿の内容をお話しすると、このような反応を頂くことが何度かありました。言ってしまえば単に「新卒で脆弱性診断を職業にしようと思った理由」ですが、これを「おもしろい」と言ってくださる方もいるということで今回筆をとりました。

いまのわたし

現在、私は社会人2年目です。この春に希望が叶って東京へ転勤し、4か月が経過しました。

もともと、私以外の同期が全員福岡勤務を希望しており、「同期を大切にしてほしい」や「新人教育に十分なリソースを割きたい」という会社の要望で、1年目は福岡で勤務していました。

転勤後もメイン業務は変わらず、診断チーム内で脆弱性診断を行っています。まだまだOJT期間中ではありますが、最近は任せてもらえる範囲が増えてきたことや、先輩方と一緒に脆弱性やシステムの挙動について議論できるようになってきたことが嬉しいです。

さて、業務の内外問わず、私の周りには精力的に様々なことに挑戦されている方が多いと感じています。同じように自分なりに挑戦をしていると、それに対してポジティブな声かけをしていただけることも増えました。

このように私が物事に挑戦できるようになったのは、2つの大きなきっかけと、たくさんの縁に導かれたからだ考えています。

1つめの大きなきっかけ「情報網はライフライン」

工業高等専門学校、通称「高専」をご存知でしょうか。工業について、中学卒業後の早期から専門教育をうけることができる5年制の学校です。

私の周りでは工業について興味があったり、ロボコンやプロコンに惹かれたり、モノ作りが好きだったり、何よりも就職に強いという特色を魅力に思い、入学する人が多かったように感じます。

私が高専の存在を知ったのは、中学2年生の進路面談のときでした。将来の夢や希望する学校が無かった私に、担任から好きなものについてと尋ねられ、「パソコン」と答えたことがきっかけで、高専をおすすめされました。（パソコンといっても、友人とメールをしたり、Webサイトを見たりといった程度です。）

私が希望する県立高校の普通科に、福岡県の学区制という制度上、入学が難しかったことや、私立高校への進学は親に禁止されていたこともあり、おすすめされた高専を目指そうと考え猛勉強しました。

努力の甲斐あって高専に入学できましたが、何か目標があったわけではありません。なんとなく選択した学科のカリキュラムは機械制御の色がとても強く、入学後すぐに工場で機械加工の実習を受けたときに「卒業無理かもしれない」と思ったことは未だに鮮明に覚えています。

また、数学が苦手で、数学コンプレックスを抱えての高専生活となりました。（習熟度別教材の学習塾で、中学3年生のときに小学校4年生のプリントから学び始めた程です。）

2年生になると専門科目が増え、理系の色がより強まっていく中で、寝る間も惜しんで勉強し、ようやく成績が維持できる現実に徐々に疲れてきます。

ロボコンや課外活動、専門科目に打ち込んでキラキラしていた同級生をいつも「素敵だな、羨ましいな」と思っていました。それでも私が勉強を続けたのは、「成績という目に見える数字が良ければ、こんな私でも、クラスメイトに仲間として認めてもらえるのではないか?」と考えたからです。せめて勉強くらいできなければ、私には価値がない、目標があって頑張っている人たちのそばにいてはいけないと思っていました。

そんなモヤモヤした気持ちを抱えたまま進級し、3年生の夏。

私は教室で過呼吸を起こして倒れました。

これをきっかけに、私は教室に行けなくなりました。たびたび過呼吸を起こすようになり、条件反射のように教室が怖いと思うようになりました。

登校したものの調子が悪くそのまま帰宅することや、保健室で無気力に花を眺めて1日が終わることもたくさんありました。成績も急降下してしまいましたが、先生方や看護師さん、親友の支えもあり、工夫しながら授業に出席することでなんとか進級にこぎつけました。

そんななか迎えた春休み、とある午後のこと。

遅めの昼食をとりながら何とはなしにテレビをつけると、TV局はどのチャンネルも、茶色の世界と、切迫したリポーターのアナウンスが流れていました。

4年生となっても、相変わらずの生活でした。進路を考える時期を迎え、周りは就活に向けてインターンシップの参加を検討しているようでした。

「このままでは周りに置いていかれてしまう。」…焦った私は、周りがみんな行くからという理由でインターンシップへ応募しますが、履歴書には動機もかけないまま提出してしまうほどの受け身な姿勢でした。

夏休み。慣れないスーツを着て、福岡県内にある情報通信系の企業へ出社しました。会社概要を教わったり設備見学をさせて頂いたり、学びの多い充実した5日間は、あっという間に最終日を迎えました。

「例年であれば、インターンシップのまとめを行っていただいておりましたが、今年度はこれだけはどうしても話させてください。全員、現場に行ってきた担当者からです。」—— この前置きから、私たちインターンシップ生に向けた最後の講義が始まりました。

スライドの写真は、春休みの3月11日以降にTVで見た映像と似た、茶色の世界でした。

九州から東北へ、復旧活動を手伝うために工事用の専用車を交代で運転して、被災地へ応援にかけつけたこと。重要な機材を配置した拠点の復旧に取り組んだこと。一刻も早い復旧を目指して工事に取り組んだこと。——担当の方の言葉が続きます。

「みなさん、どうしてここまでするかわかりますか。情報網はライフラインだからです。みなさんがライフラインと想像するのは、水道、ガス、電気でしょう。情報も同じです。連絡できていれば助かった命があるかもしれない。適切な救助活動や支援には、迅速な情報伝達があってこそ。情報網はそこを支える部分です。」

それから復旧が進むにつれて、僅かながらも避難所に笑顔が戻ったお話を聞きました。

このお話を聞いて、私は情報の持つ力と、当たり前の日々の尊さを感じました。それと同時に、自分には価値がないとぼんやり過ごしていた毎日をとても恥ずかしく思いました。そしてふと、入試の面接で「具体的にはわからないが、社会や人の役に立てるエンジニアになりたい」と話したことを思い出します。

「情報の分野で、エンジニアを目指そう。」

はじめて私の中で目標ができた瞬間でした。

2つめの大きなきっかけ「セキュリティ・キャンプ」

高専を卒業した20歳の春。私は地方国立大学の工学部へ3年次編入します。

大学へ3年次編入をして一番驚いたことは、高専で学んだ専門科目が大学の単位としてほとんど認定されないことでした。

同じ大学の機械工学科に編入した高専のクラスメイトはたくさん単位認定をもらい、スカスカの時間割だったのに対し、知能情報工学科に編入した私は「留年確定」と言われるほど単位認定が少なく、ほぼ全ての時間に講義が入る状態となり、授業に追われる1年となりました。

1年間、簡単であるとか授業が被らないとか、単位取得に特化した講義を選択し、良い成績で単位を取るという講義の受け方をし続けた結果、冬頃には、この大学に来た目的に疑問を持つようになっていました。

学年末試験も迫ってきた頃、IPAの未踏プロジェクトの講演会がありました。必修の連絡があり、しぶしぶ参加します。講演ではスーパーエンジニアたちの活

躍や成果が紹介されていましたが、単位の方が大事だった私は、こっそり講義のレポートをしていました。

思いのほかレポートが早く終わり、申し訳程度に配布されたパンフレットを開くと、そこに挟まれた一枚の「セキュリティ・キャンプ全国大会2014」の案内。サイバーセキュリティについての簡単な紹介や、合宿形式で学びを深めるといった記載がありました。

頭の中で自分がそれまでに考えていた「情報」が揺らぐ瞬間でした。情報は単に伝わればOKではなく「正しく」「安全に」伝わる必要があるのでは、と。気づけば前の席に座っていた友達に声をかけていました。

「これ、一緒に勉強して応募しない?」

期末試験が終了し、友人らと定期的にセキュリティ勉強会を始めました。最初は過去の応募用紙に沿って勉強する予定でしたが、設問のレベルに自分たちが全く追いついていなかったので、とりあえずで「XAMPPでWebサーバを立てる」書籍に沿って学習しました。また、私はネットワーク・セキュリティクラス（当時）に興味を持っていたので、ネットワーク「っぽい」本を図書館で借り、書籍ベースで勉強を始めました。

朝から晩まで、勉強漬けの春休みを過ごし、大学4年生の5月頃。今年度のセキュリティ・キャンプの応募用紙が発表されたという内容を見て、サイトにアクセスします。私の応募したい「ネットワーク・セキュリティクラス」の応募用紙は指定のファイルから抽出せよ、という条件がついていました。ところが指定のファイルには拡張子がなく、テキストエディタで開くと文字化けしています。勉強の甲斐なく、今の自分は応募すらさせてもらえないととてもショックを受けました。

その日の晩、実名制SNSを見ていると、出身高専の先生が「今年の応募用紙は面白いね」と取り上げているのに気づきました。思わず、応募用紙について悩んでいることをコメント欄に書くと「バイナリエディタ」と返事がありました。バイナリエディタというものを知らなかった私は、まずバイナリエディタを取得し、応募用紙のファイルを開いてみました。しかし、私の理解としては先の文字化けとなんらかわりません。ダンプはただの英数字、テキスト表示も文字化けしていたので文字化けのまま、という認識です。

翌日、研究室にてバイナリエディタで表示したものを印刷し、何かヒントはないか、なにか法則性がないかと見ていました。紙を数時間睨み続ける私を不審に思った指導教員に元ネタを提供したところ、あっさり「これが何かわかったよ」とのこと。というわけで、この文字化けは、私がダウンロードに失敗したのではなく、きちんと人間が理解可能な形になることがわかったので、改めてにらめっこを続けることになります。

それから3日間、思いつく限りのことを試しましたが、わかったことといえばテキスト表示のエリアに「http」「TCP」の文字があるくらいでした。いい加減煮詰まってきたのもあり、一旦応募用紙は忘れて、勉強の続きをすることにしました。そのときは「パケットキャプチャ」について書籍の掲載順に勉強していたのですが、「ファイルの取り出し方」の機能について記載があることに気づきました。

もしや、と思って応募用紙をパケット解析ソフトで開くと、そこに現れたのはhttpでファイルをやり取りする通信で、該当の通信から応募用紙を無事に入手できました。

応募締め切りまでの残り時間は、応募用紙の設問を仕上げて行きました。技術的な設問は、わからなくてもかならず手を動かして調べ試しました。自由記述の設問は、きっかけ1で書いたような、なぜ情報に興味を持ったのかと、そこからなぜセキュリティに興味をもったのかについて書き込みました。

応募用紙の提出前夜、準備からいれると約半年。やりきった達成感で思わず泣けてきてしまい、選考に通らなくても悔いはないと思いながら、事務局に送付しました。

私の熱意が応募用紙から審査の方に届いたのかはわかりませんが、ありがたいことに私は全国大会への切符を手に入れました。セキュリティ・キャンプの具体的な内容は、様々な媒体で取り上げられていますのであえて詳細には書きませんが、私にとって色々な価値観が揺さぶられる5日間でした。

セキュリティ・キャンプは終了後、感想文を提出して本当の終わりになります。今回寄稿にあたり、感想文を初めて開いたのですが、いまの私に繋がる決意表明

を見つけることができました。

「ここからが私のスタート。これからどうなのか、未来はわからない。他人に惑わされてしまうことも容易に想像できるし、落ち込む私の姿も浮かぶ。でも逃げたくはないし、逃げる必要もなさそうだ。つらいときはここでの思い出と、たくさんの出会いが私を支えてくれるから。自分の歩幅で、歩み続けていこうと思う。」

そしてそれから

ここまでの内容ですと、インフラエンジニアになっていそうですが…なぜ脆弱性診断を職業として選んだかというと、セキュリティでご飯を食べることがリアルに想像できるようになったからです。

大学院に進学し、今度こそしっかり就職活動を見据えて行動しようと考えたとき、インターンシップでよい影響を受けた身として、再度インターンシップに参加しようと自然に考えました。また、より深く社会を知るために、次は現場配属型のインターンシップを希望し、各種条件に合ったものに申し込みました。履歴書や面接にて、ここまでの話をしていたため、セキュリティに興味をもっていると判断されたのでしょう。セキュリティの部署に配属されました。

ここで初めて私にとってセキュリティ、ひいては脆弱性診断という仕事が、SF作品に出てくるような特殊なものではなく、現実の仕事なんだという実感を得ました。これをきっかけに、情報が「正しく」「安全に」伝わるように貢献したい。セキュリティエンジニアを目指そうと考えるようになりました。

導かれて

終わりに、最近私がふっと思っていることを書かせてください。みなさんは、今の仕事ややっていることに、この体験が通じているのかもしれないというものはありますか。

私が初めてパソコンに触れた記憶は、保育園に入園したくらいの頃で、メモ帳でひらがなを打っていました。父に渡されたローマ字変換表には「を」の対応として「O」と書かれており、私の名前「おちかをる」の「を」が打てず、何度試しても「おちかおる」になってしまうというものです。父に聞いても自分で考えなさいの一点張りでした。後日、ふと「わ」は「WA」だから「を」は「WO」とひらめいて入力し、「おちかをる」の入力に成功しました。誰に褒められたわけではありませんが、画面に「を」が打てた時、とても嬉しかったことを覚えています。

同意を得るのは難しいかもしれませんが、個人的にはこの体験はなんとなく脆弱性診断と似ていると思っています。メモ帳では単に画面の表示ですが、Webアプリケーションの診断であれば、診断対象の特性や入力値に対する出力の内容や傾向を見ながら、擬似攻撃を試行錯誤するので、様子を見ながらあれこれ試すという部分が似ているな、と。

また、初めてWebに触れた記憶は私にとって好ましい思い出で、父が電話線を利用してインターネットの設定をしてくれて、家族で母が好きなキャラクターの公式Webサイトへアクセスしたというものです。

当時と変わり、Webサイトやアプリケーションは特別なものからごく日常のものとなりましたが、そのシステムは誰がどんなふうに利用するのか、お客様の資料を元に考えながら日々業務に取り組んでいます。

私は今、様々な縁に導かれるかのように脆弱性診断の業務に取り組んでいます。この先の未来がどうなっていくか、全く想像ができませんが、周りの方への感謝を忘れず、自分の歩幅で、歩み続けていければと思います。

経営者に情報セキュリティ対策の必要性を訴求する手法について

西日本支部　経営者向け情報セキュリティ対策実践手引き WG
西日本支部長　嶋倉　文裕

1. はじめに

企業における、情報セキュリティに関連する事故や事件による影響範囲は甚大であり、ひとたび発生させると、いままでの人材や技術など、社会に投資・貢献してきた努力が、一瞬にして「無に帰す」ことになる。情報セキュリティ事故は情報漏洩といった機密性の侵害に注目されがちであるが、マルウェアの侵入による工場ラインの停止や、不安定な動作による製品品質の劣化、低下、製品の出荷の遅れ・停止を招くこともあり、これらの経営への影響は計り知れない。

また、今後さらにIoT化により業務とITが密接に関係していくことを考慮すると、情報セキュリティ対策は、全ての組織にとって喫緊の課題である。

そのため、常日頃から、自組織がどのような環境でオペレーションを行っているのか、情報セキュリティ対策がどの程度実施されているのか、どのようなリスクにさらされており、どの程度の対策をしておくべきなのかを把握し、対応を決断することが経営者や経営層には問われているが、経営層にとって情報セキュリティリスクは、理解しにくいものである、というのが実態である。

それでは、情報セキュリティに起因する影響をできる限り最小限にし、情報セキュリティ対策が事業継続への投資として必要不可欠であることを経営者に理解していただくにはどうすれば良いか?

西日本支部の「経営者向け情報セキュリティ対策実践手引きWG」（以下、Risk WG）では、その解として経営者に情報セキュリティ対策の必要性を訴求し、対策に投資をしてもらうために、必要性の見える化として、ISO31000（リスクマネジメント）のリスクマネジメントを参考にして、自組織そのものを評価するための手段の検討を行った。

本稿では、Risk WGの成果物である「経営者のための情報セキュリティ対策　―ISO31000から組織状況の確定の事例―」に記載する、ISO31000の「組織の状況の確定」というステップを中心に、情報セキュリティの目的を明確にし、自組織の情報セキュリティに係るリスクの把握、リスクの評価、リスク対応を決断し、必要な対策の見える化について紹介する。

2. リスクアセスメントとマネジメントの考え方

「組織の状況の確定」は、ISO31000のリスクアセスメントの一ステップで、図1の位置づけとなる。

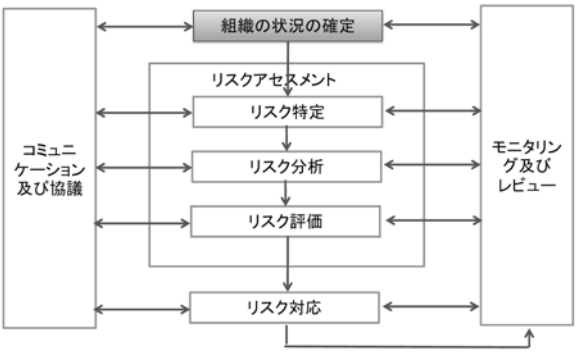


図1　ISO31000のリスクマネジメントプロセス

なお、ISO31000のリスクマネジメントプロセスの各ステップにおいて「コミュニケーション及び協議」が関連づけられているが、Risk WGでは、「コミュニケーション及び協議」を誰と行うのか、経営視点でのリスクとして捉えて行うために必要なことは何かを考え、それを図2に整理した。

組織には様々なリスクが存在し、情報セキュリティリスクはそのうちの一つではあるが、情報セキュリティリスクによる経営や業務への影響を情報システム部門のみで把握するには困難であり、経営者、業務部門でしかわからないことがある。

そのため、情報セキュリティリスクには、経営者、業務部門と情報システム部門が一体に対応することが必要であり、その要となる経営者、業務部門と情報システム部門間の「コミュニケーション及び協議」を効率的に進めるには、組織全体で共通の言葉と意味でリスクの認識を持つことが求められる。

例えば、図2では情報セキュリティリスクが、システ

ムリスクや品質リスクに影響することを示しており、情報セキュリティリスクによるシステムリスク、品質リスクを把握し、それぞれにおける対策の明確化を「コミュニケーション及び協議」を通じ行うことを示す。

逆に言えば、情報セキュリティリスクがシステムリスクや品質リスクに何ら、影響を与えない組織であれば、対策は不要であり、リスクを正しく把握することは無駄な投資を防ぐことになる。

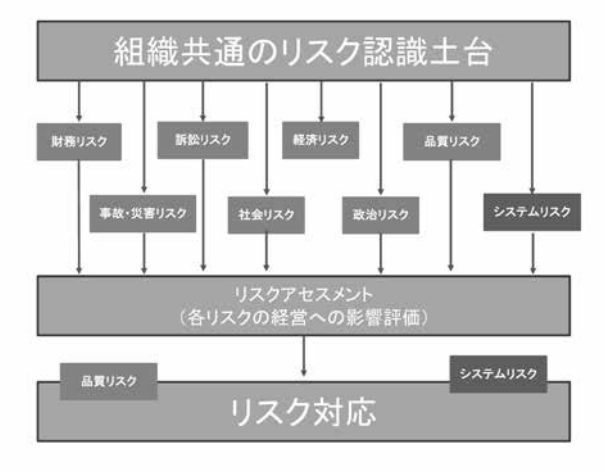


図2　リスクの共通土台

3. 組織の状況の確定方法

3.1　外部状況と内部状況

組織の目的を明確化するISO31000の「組織の状況の確定」では、リスク管理において考慮するのが望ましい外部及び内部の要因を定めている。

以下にISO31000に記載されている外部状況、内部状況の例を示す。

3.2　組織の状況の確定方法

Risk WGでは、経営の視点から自組織の状況の確定を行うことで、図3に示す以下の事項が明確にできると考えた。

(1) セキュリティ対策の目的、望まれる対策とレベル
自組織の社会における位置づけ、社会や顧客からの期待など、外部からの要請が自組織のセキュリティの動機付け、対策の範囲やレベルの要件となる。

(2) 対策の範囲
把握した外部状況、内部状況から対策すべき範囲が明確となる。

表1　外部状況と内部状況例

外部状況例	国際、国内、地方又は近隣地域を問わず、社会及び文化、政治、法律、規制、金融、技術、経済、自然並びに競争の環境
	組織の目的に影響を与える主要な原動力及び傾向
	外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観
内部状況例	統治、組織体制、役割及びアカウンタビリティ
	方針、目的及びこれらを達成するために策定された戦略
	資源及び知識として把握される能力（例えば、資本、時間、人員、プロセス、システム、技術）
	内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観
	組織の文化
	情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む。）
	組織が採択した規格、指針及びモデル
	契約関係の形態及び範囲

(3) リスクの低減
目的を達成するために、軽減すべきリスク、最低限受容可能なリスクを識別する。
(4) 予算
リスク軽減に向けて、運用も含めた必要な費用と、自組織で投資可能な費用から、予算計画を立案する。

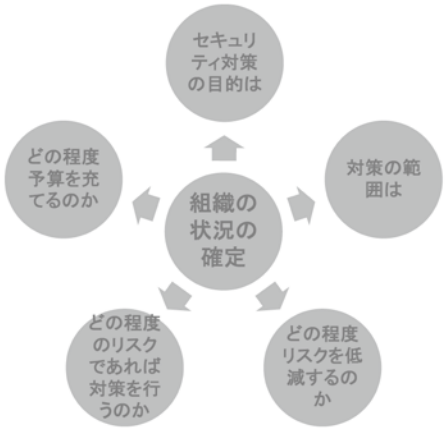


図3　組織の状況の確定を行う視点とは

3.3　経営環境の分析

Risk WGでは、経営に訴求する方法として、図4の一般に使われる以下のマクロ環境(PEST)とミクロ環境（Five Forces：5つの競争要因）を利用できないか、検討を行った。マクロ環境は、企業が統制不可能なこと、ミクロ環境は企業が準統制可能なこととして捉えている。

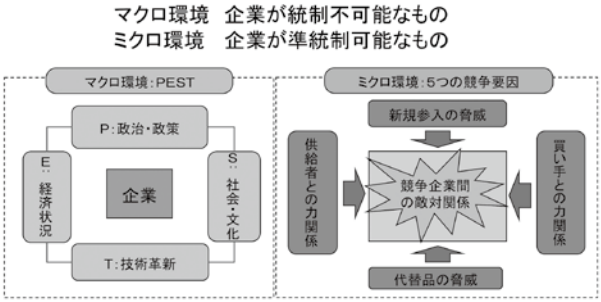


図4　マクロ環境とミクロ環境

3.4　外部状況、内部状況とマクロ環境、ミクロ環境の関係の再整理

Risk WGでは、ISO31000の外部状況、内部状況とマクロ環境（PEST）、ミクロ環境（Five Forces）の関係について検討を行い表2に再整理した。

マクロ環境、ミクロ環境とも外部要因であり、これらはISO31000の外部状況との関係で整理できる。

また、3.2項に示すとおり、自組織の社会における位置づけ、社会や顧客からの期待など、外部からの要請といった外部状況が、自組織のセキュリティの動機付けの大きな要因となり、セキュリティ対策の範囲、レベルの要件となる。

一方、内部状況は自組織の様々な要因と紐づけられ、セキュリティの視点では、表3に示す現状の対策状況となる。

以上を踏まえ、セキュリティにおける外部状況、内部状況の関係をまとめると、以下のように整理できる。

- 外部状況が自組織のセキュリティ対策の動機付けとなり、目指すセキュリティの姿が定まる
- 内部状況は、自組織の現状であり、内部要因により現状のセキュリティレベルとなっている
- 目指すセキュリティの姿と現状のセキュリティレベルの差異が改善すべき対策となる

図5にその関係を示す。

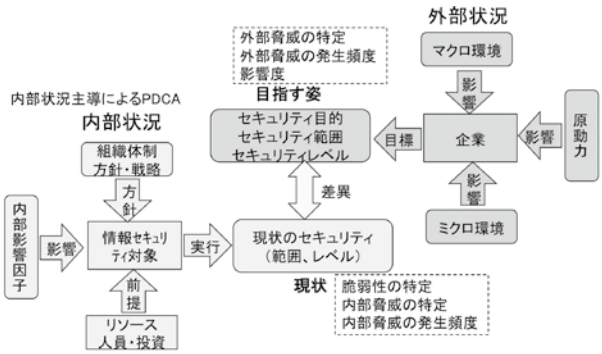


図5　セキュリティにおける外部状況と内部状況の関連

目指す姿との差異が確認されれば、図6のように、内部状況および外部状況を踏まえたPDCAを行い、組織体制や方針・戦略へのフィードバック、内部影響

表2　外部状況とマクロ環境、ミクロ環境

		分類	セキュリティとの関係	再分類	
外部状況	国際、国内、地方又は近隣地域を問わず、社会及び文化、政治、法律、規制金融、技術、経済、自然並びに競争の環境	政治	P:政策により、セキュリティ攻撃等セキュリティ脅威が増大	マクロ環境	要求要件
		経済	E:セキュリティ投資に影響		
		金融	セキュリティ投資に影響		
		社会及び文化	S:脅威、セキュリティ対策に影響（要リスク評価）		
		技術	T:脅威、セキュリティ対策に影響（要リスク評価）		
		法律/規制	脅威、セキュリティ対策に影響（要リスク評価）		
		自然	脅威、セキュリティ対策に影響（要リスク評価、事業継続）		
		競争環境	ミクロ環境:脅威、セキュリティ対策に影響（要リスク評価）	ミクロ環境	
	組織の目的に影響を与える主要な原動力及び傾向	N/A	組織の目的に影響を与えるセキュリティレベル（最低のセキュリティレベルより大） セキュリティ対策の目的、セキュリティ対策の範囲、セキュリティレベル	セキュリティ対策の目的 セキュリティ対策の範囲 セキュリティレベル	
	外部ステークホルダとの関係並びに外部ステークホルダの認知及び価値観	株主	業種により外部から要求されるセキュリティレベル（最低のセキュリティレベル） セキュリティレベル、範囲		
		顧客			
		取引先他			

表3　内部状況の再整理

		分類	セキュリティとの関係	再分類	
内部状況	統治、組織体制、役割及びアカウンタビリティ	統治	脆弱性:組織的対策	組織体制・方針・戦略	現状
		体制			
		役割			
	方針、目的及びこれらを達成するために策定された戦略	経営方針	脆弱性:組織的対策		
		情報セキュリティポリシー群			
	資源及び知識として把握される能力（例えば、資本、時間、人員、プロセス、システム、技術）	資本	セキュリティ投資	リソース（人、金、プロセス）	
		人員/時間	リスク評価分析、セキュリティ対策・管理を行う人材		
		プロセス/システム	リスク評価分析、セキュリティ対策・管理方法		
		技術	リスク評価分析、セキュリティ対策・管理を行う技術力		
	内部ステークホルダとの関係並びに内部ステークホルダの認知及び価値観	経営者	脆弱性:組織的対策 ※内部組織の関係、認知及び価値観に基づき組織を構成する	内部影響因子	
		セキュリティ管理部門			
		情報システム部門			
		従業者			
	組織の文化	組織の行動原理 ※ITリテラシー	脆弱性:人的対策、技術的対策 ※組織の文化を考慮して人的対策、技術的対策を検討する		
		組織の思考様式 ※ITリテラシー			
	情報システム、情報の流れ及び意思決定プロセス（公式及び非公式の両方を含む）	情報資産	脆弱性:組織的対策、人的対策、技術的対策、物理的対策	セキュリティ対策の対象=現状のセキュリティレベル	
		情報処理			
		情報資産を取り扱う物理的範囲			
		リスク評価・分析			
	組織が採択した規格、指針及びモデル	規格/指針	脆弱性:組織的対策	現状のセキュリティレベル	
		モデル			
	契約関係の形態、内容及び範囲	従業員との契約	脆弱性:人的対策		
		取引先との契約			

因子への説得、またリソース・人員・投資への再整備などを行うこととなる。

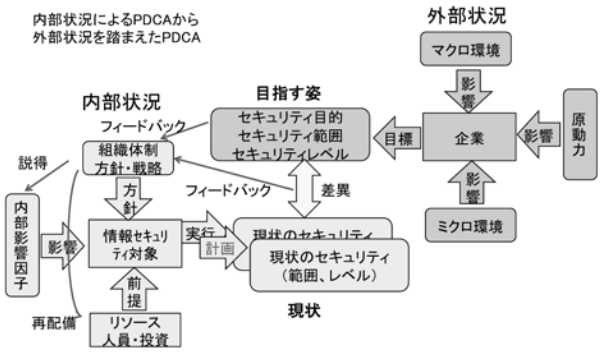


図6　目指す姿との差異が確認された場合

3.5　目指す姿への推進

現状から目指す姿に推進するとき、必ずしも順調にいくとは限らず、正しいと考えていたものが、時代の変化・技術の進歩等により必ずしも正しいとは言い切れなくなることや、失敗、挫折、訂正、変更や後戻りなど、目指す姿へ直線的に最短、最小コストでいけないことのほうが多いかもしれない。

また日常における情報セキュリティは「今そこにある危機」に対して、スピード感をもった対応が要求されるケースもある。

前述の「目指す姿」への推進は、PDCAサイクルのような長い周期（例えば、1年）での取り組みとなるが、日々の脅威や脆弱性の変化の対応や、不幸にも情報セキュリティの侵害を検知した時には、自社への影響、状況を把握し、その対応の意思決定、およびその対応の実行という措置を短期間で行う必要がある。この短期間でのプロセスはOODA（Observe（監視）、Orient（情勢判断）、Decide（意思決定）、Act（行動））と呼ばれ、目指す姿にフィードバックを行うことも考慮する必要がある。

4.　モデル企業での必要な対策を導くプロセス

これまでの検討結果を踏まえ、Risk WGでは様々な企業のケースが考えられるため、いくつかの仮想モデル企業を作成しモデルケースでの経営者への情報セキュリティ対策の必要性を訴求する方法を試案した。

それらのモデル企業毎に、経営者の視点による外部状況、内部状況を整理し、その差異とセキュリティ対策を放置することで招く恐れのある被害を金額で明示する、図7に示す見える化、および目指す姿の差異を改善するための施策を、図8に示す投資費用、回収計画という形で、経営者に向けた見える化の手法の検討を行った。

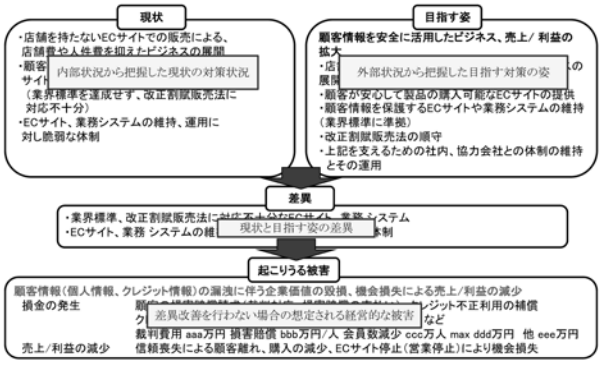


図7　現状と目指す姿の例

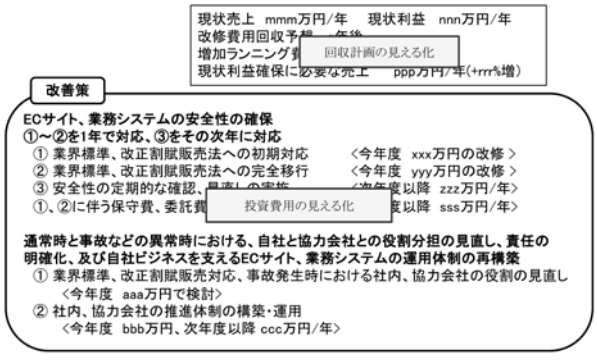


図8　投資計画と回収計画例

5. 最後に

Risk WGの成果物である「経営者のための情報セキュリティ対策　―ISO31000から組織状況の確定の事例―」の第2部には、WGで想定した仮想モデル企業について外部状況、内部状況を整理し、必要な対策を導くプロセスの見える化例を作成しており、経営者にセキュリティ対策の必要性を訴求したい読者の方の参考となれば幸いである。

また、組織がなぜ情報セキュリティ対策を行うのか、その動機付けや情報セキュリティ対策への投資を経営者に決断して頂くためのアプローチを本Risk WGで実施したが、これまでの西日本支部での活動は、情報セキュリティ対策を行うことが前提となっている組織にアプローチする活動であり、西日本支部は図9に示す関連性をもった成果物を作成してきた。

これらについてもご利用頂ければ幸いである。

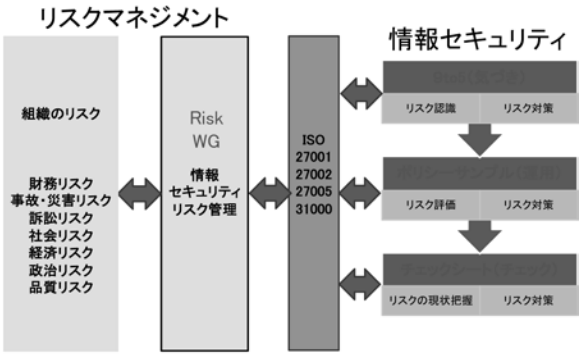


図9　西日本支部の成果物の関係

参考

西日本支部の成果物と参照先

＜気付き＞

「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」　略称：9to5

https://www.jnsa.org/result/2013/chusho_sec/

＜運用＞

「中小企業向け情報セキュリティポリシー・サンプル」　略称：ポリシーサンプル

https://www.jnsa.org/result/2016/policy/

＜チェック＞

「中小企業向け情報セキュリティチェックシート」　略称：チェックシート

https://www.jnsa.org/seminar/nsf/2014kansai/

＜リスクマネジメント＞

「経営者のための情報セキュリティ対策 ―ISO31000から組織状況の確定の事例―」

https://www.jnsa.org/result/2018/west_tebiki/

JNSA ワーキンググループ紹介

U40 部会

U40 部会　部会長
NEC ネクサソリューションズ株式会社　杉野　広典

■ U40部会について

U40部会は、40歳以下を対象メンバーとしてJNSAの若返り、若年層の活動活発化やスキルアップ、幅広い人的ネットワークを形成することを目的として2007年に設立されました。昨年は設立10周年を迎え、10周年イベントが盛大に行われております。会場提供にご協力頂きました株式会社サイバーエージェント様にはこの場を借りてお礼申し上げます。

U40の主な活動としては、テーマを決めて実施する勉強会を中心に活動しており、取り扱う内容の選定は部会メンバーの様々な意見が反映されています。

また今年度は、JNSA教育部会と連携して、JNSAがリモート講義を担当している岡山理科大学の講義を3回担当させていただきました。このように、40歳以下の若年層の方が勉強会だけでなく、公的な人材育成という貴重な機会を得ることができる部会となっています。

■ for Rookies WG

リーダー：岡島 麗奈
（株式会社サイバーエージェント）

本WGは、セキュリティ関連業務経験3年未満を対象とし、若手間をはじめとした人的ネットワークの形成およびスキルアップを目的として活動しています。勉強会内容としては、「いまさら聞けない相談事」を主に部会メンバーが講師を担当するアクティブラーニング方式で実施しています。

参加メンバーには20歳代の方も多く、全体的に年代が近いこともあるのか質問や議論等が活発に起こるWGとなっています。勉強会後には懇親会を実施しており、情報交換や各々の仕事の話などを話題に交流を深めています。

■ 勉強会企画検討WG

リーダー：深谷 隆（日本プロセス株式会社）

本WGは、部会メンバーではなく外部の方に講師を依頼してお話いただく勉強会を実施しています。勉強会のテーマとしては、直近では「CTF」や「ダークウェブ」を取り上げて実施しており、非常に幅広い内容となっています。また、勉強会の内容によっては部会外のJNSA会員からも参加者を募っています。本WGでも勉強会後には懇親会を実施しており、場合によっては終電間際までセキュリティに関して熱く語り合っています。

■ 今後の活動について

U40部会では、今後もそれぞれのWGを通して、様々なテーマで多くの方々にお役立ていただけるような勉強会を実施していきます。今までは、会場のキャパシティの影響で最大でも40名程度でしたが、今後は貸会議室を借りることでより多くの方に参加いただけるように検討しています。そして、勉強会だけでなく教育

部会と連携して実施している講義も継続していき、より多くの若手の方々に講師の経験を積んでいただきたいと思っています。

また、運営についても積極的に意見を取り入れてより良くしていきたいと思っていますので、忌憚のないご意見を頂ければと思います。

最後に、部会メンバーの皆様および事務局の皆様には、会議室の確保や講師の方へのご依頼などの運営にご協力いただきましてありがとうございます。紙面をお借りして厚くお礼申し上げます。

■過去の勉強会履歴（過去5年間）

開催日	タイトル	講師（敬称略）
2013/3/6	OpenFlow/SDN	宮永 直樹
2014/7/18	GPGPUによる高速パスワード解析	赤松 孝彬
2015/1/8	Hardening、サイバー演習の裏側	中西 克彦
2015/3/16	Microsoftのセキュリティあれこれ	垣内 由梨香
2015/5/29	ソーシャルサービスのあれこれ	伊藤 秀行
2015/6/12	IBM様 SOC見学会	徳田 敏文
2015/8/21	piyokango氏に聞くセキュリティ情報収集	piyokango
2015/11/18	マルウェア解析入門	石丸 傑
2015/12/4	フォレンジック解析入門	伊藤 耕介
2016/3/25	サイバー脅威インテリジェンスの動向	角丸 貴洋
2016/6/21	セキュリティと機械学習	愛甲 健二
2016/9/6	脅威のモデル化	小野寺 匠
2016/12/14	エンジニアがいまさら聞けない一般常識シリーズ ～海上保安庁って防衛省だっけ～	佳山 こうせつ
2017/4/5	国家レベルから民衆レベルに渡る　サイバー攻撃の理解と対策	名和 利男
2017/8/28	フォレンジック体験ワークショップ	赤松 孝彬
2017/9/15	CTFから海外へ	寺島 崇幸
2017/12/13	IIJ様 SOC見学会	中嶋 功
2018/1/31	Malware Containment 体験会	JNSAゲーム教育WG
2018/4/20	セキュリティホールを見つけよう！脆弱性診断ハンズオン	小笠原 清志
2018/6/22	Webアプリケーション脆弱性診断の概要と意外と知らない XSSのetc.	長沼 果萌
2018/9/5	AIを用いたダークウェブからのインテリジェンス抽出について	林 翔太

JNSA ワーキンググループ紹介

CISO 支援ワーキンググループ

CISO 支援 WG リーダー
株式会社 Preferred Networks　高橋　正和

CISO支援ワーキンググループは、今年５月に「CISOハンドブック」を公開しました。本稿では、CISOハンドブックの作成の経緯を中心に、CISO支援WGの活動をご紹介いたします。

CISO ハンドブック（CISO支援ワーキンググループ）
https://www.jnsa.org/result/2018/act_ciso/

■ CISO支援WGの設立

CISO支援WGの設立は、前WGリーダーの河野さんと私の「PDCAの”Check”はファクトベースで実施すべきだ」との議論がきっかけとなりました。そして、「CISOが経営会議に報告する内容としてチェック項目と評価手法をまとめること」を目標に、一般社団法人日本CISO協会、日本ISMSユーザグループ、特定非営利活動法人日本セキュリティ監査法人（JASA）の支援をいただき、2016年にJNSA CISO支援WGを設立することになりました。

設立当初は、構想がある程度固まっていたことから、比較的早く完成すると考えていました。WGメンバー募集の活動予定を見ると、5か月程度で完成すると考えていたようです。

しかし、実際にはなかなか作業が進まず、「もうすぐ公表できる」との報告を続けたことから、「蕎麦屋の出前」プロジェクトと、ありがたくない呼ばれ方もしていました。

[2016年当初の計画]

4月初旬	キックオフ　理想的なCISO像についての意見交換
4月中旬以降	タスクフォースによる成果策定
5月以降	月に1回程度の成果報告会
9月以降	成果物のプロモーションを兼ねた勉強会、セミナーの開催

第一回CISO支援WG

第一回のCISO支援WGは2016年4月に開催されました。ここでの議論は、「CISOハンドブック」の内容とはずいぶんと違った内容で、CISOの組織論に終始し、当初考えていた経営会議への報告内容に関する議論には至りませんでした。この時の議論は、インタビュー記事[1]で取り上げて頂いた武田さんのコメントに集約されていると思います。

[1] 全ての悩めるCISOにささげる――「CISOハンドブック」はいかにして生まれたか
http://www.itmedia.co.jp/enterprise/articles/1807/06/news026.html

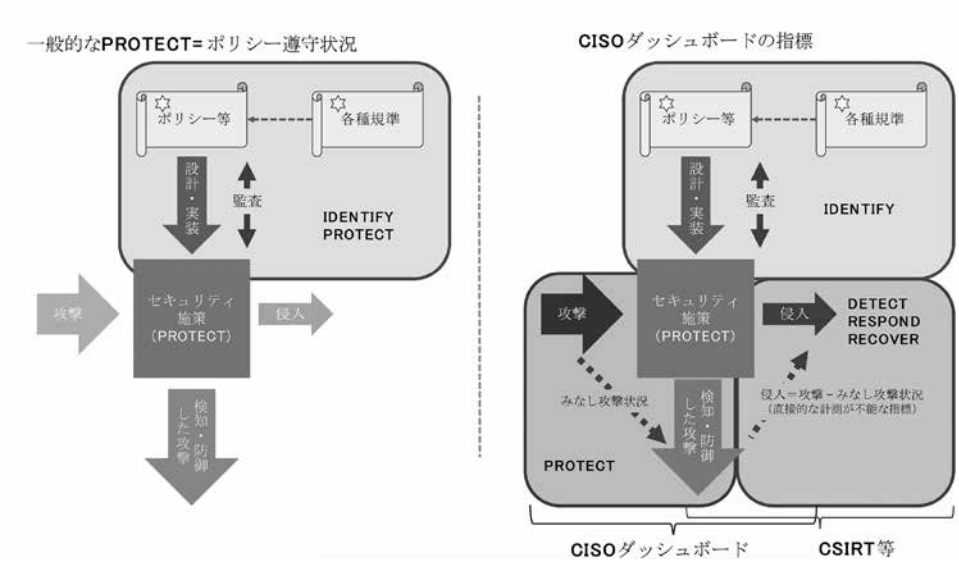
「そもそもCIO（Chief Information Officer：最高情報責任者）自体が破綻しているところが多く、ピンとこなかった。セキュリティでオフィサー？　そんなの機能しないでしょ！　と。そもそも組織によって、その位置付けも大きく変わるのではないか、という話からスタートしていた」

CISOダッシュボード

CISOハンドブックの作成は、ミーティングとMLを通じて作業を進めましたが、なかなか議論がまとまりません。成果物のイメージがないと議論が進まないと考え、想定される計測項目と考え方を、「CISOダッシュボード」としてまとめ、2017年1月に、WGのメーリングリストにポストしました。

「CISOダッシュボード」では、以下の4項目による組織のセキュリティ状況評価を提唱しています。

- Attack condition: どの程度の攻撃に直面しているのか（＝検出しているのか）
- Protection condition: 対策の状況は計画通りか（Assuranceの領域）
- Suspicious activity: 侵入を許したか、その可能性はあるか
- Indirect activity: PCの紛失、建屋への侵入、人事上のトラブルなど懸念事項



セキュリティ施策の考察（出典：CISOハンドブック）

ダッシュボードの成果であったかは定かでありませんが、WGは、河野さんを中心に断続的に作業を続け、2017年9月には「清書前の暫定版」をまとめ、WGメンバーによる校正を始めることになりました。

WGの再始動とCISOハンドブックの公開

しかし、再びWG活動が停滞します。2017年10月に私が転職し、12月には河野さんが転職したことから、WGとしての作業が進まない状況に陥りました。このため、2018年1月に私が暫定リーダーとなり、WG活動を続けることになりました。

ドキュメントの公開に向けたミーティング（編集会議）をWGに呼び掛けたところ、執筆メンバーとなった荒木さん、池上さん、北澤さん、田中さん、西尾さん、福岡さんに参加をいただき、何度かのミーティングを経て、公表できる内容にまとめることができました。

ミーティングは、それぞれの持ち味を感じる活発な議論と共に、多面的な角度から検討することができました。私自身も学ぶことが多く、刺激を受ける楽しい時間でした。このディスカッションの一部は、「CISOハンドブック」のコラムへと発展していきました。

そして、「CISOハンドブック」は、第一回のミーティングから2年を経て2018年5月に公開することができました。嬉しいことに、複数のメディアで取り上げて頂いただけではなく、JPCERT/CCやIPAのWebでもご紹介頂きました。また、2018年6月のJNSA活動報告会でも執筆メンバーと共に、ハンドブックの紹介をすることもできました。

今後の活動について

今後は、「インシデントシミュレーション」と「クラウドを前提としたセキュリティ対策」の二つの活動を予定しています。

CISOハンドブックの一部として公開をしている「インシデントシミュレーション」はワークショップとしての展開を目指しています。また、想像以上にクラウドファーストが進んでいるIT環境のセキュリティ基盤となるモデルとして「クラウドを前提としたセキュリティ対策」まとめて行きたいと考えています。

企業におけるCISOの重要性は高まっており、多くの企業がCISOを求めていると感じています。セキュリティベンダーにとっても製品やサービスの提案を進める上で、CISO業務の理解は欠かせないと考えています。

CISOハンドブックは、CISO業務の大枠をドキュメントとして形にしたものだと考えています。CISOハンドブックが、皆様がセキュリティ対策を進める上での一助になれば幸いです。

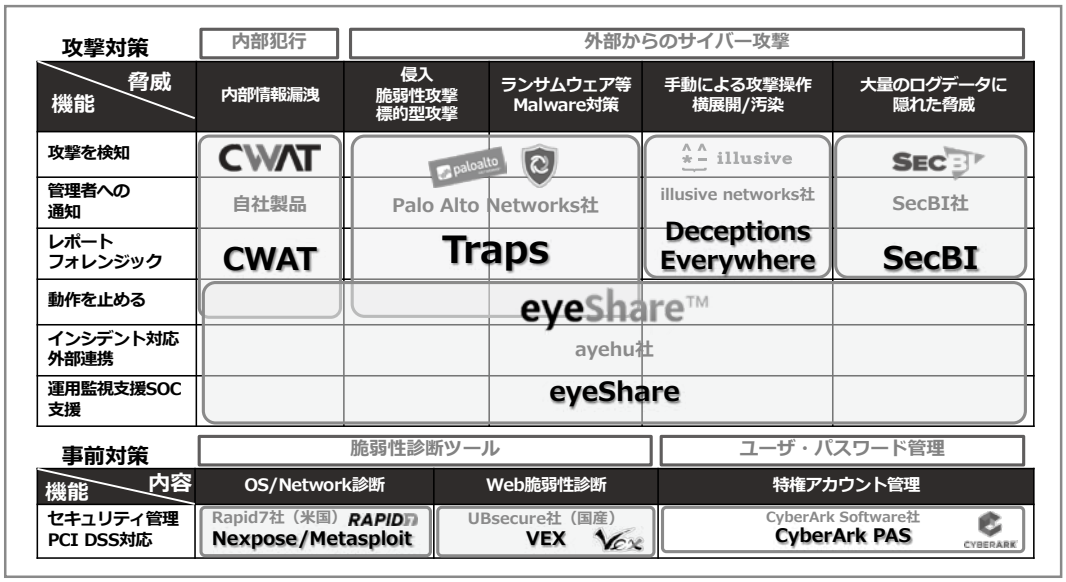
会員企業ご紹介46

株式会社インテリジェント ウェイブ

http://www.iwi.co.jp/

株式会社インテリジェント ウェイブは、クレジットカード取引や銀行・証券などの金融業の領域で、大量のデータをリアルタイム、低遅延かつ正確に伝送処理するネットワークの基礎技術を国内において30年以上提供することで圧倒的シェアを占めています。これら金融業界における長年の経験により、情報セキュリティに関する深い知見を保有しており、また、イスラエル他の諸外国との長年の交流と併せて、外部からのサイバー攻撃、不正取引や内部情報漏洩を防御する為の、情報セキュリティ技術とソリューションを提供しています。

■ 当社が提供するサイバーセキュリティ ソリューション



エンドポイント対策製品

CWAT® インテリジェントウェイブ社「シーワット」

内部情報漏洩対策／IT資産管理
PC操作ログの取得とポリシー制御

Traps Advanced Endpoint Protection パロアルトネットワークス社「トラップス」

エクスプロイト／マルウェア対策
エンドポイント上での不正実行防止

illusive イリュージブネットワークス社「デセプション エブリウェア」

攻撃されていることを誤検知なく検出
デセプション（欺瞞情報）で攻撃者を騙す

業務効率化支援製品

SECBI セックビーアイ社「セックビーアイ」

自律解析エンジンによるログ解析
見つけにくい隠れた脅威・攻撃を検出

eyeShare™ アイエフ社「アイシェア」

CSIRT業務支援
ロボットによる運用の自動化

RAPID7 ラピッドセブン社「ネクスポーズ」「メタスプロイト」

脆弱性診断／ペネトレーションテスト
N/W上の機器を一斉スキャン

お問い合わせ先	株式会社インテリジェント ウェイブ　セキュリティソリューション本部 E-mail : iwi_security@iwi.co.jp　　電話 : 03-6222-7300

株式会社サイバーディフェンス研究所

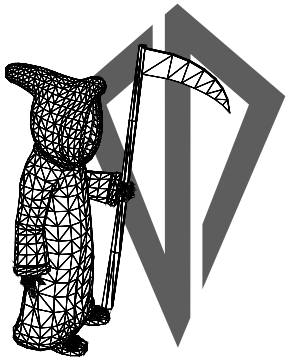
https://www.cyberdefense.jp/

CyberDefense

“人間がもたらす脅威には、人間しか対処できない。”

サイバーディフェンス研究所は、ハッカーを中心とするセキュリティ技術者集団です。
「人間がもたらす脅威には、人間しか対処できない。」という信念のもと、様々な分野で突出した専門性をもつ異能のエンジニアたちが一丸となり、一般的なセキュリティサービスとは一線を画する高い品質、ユニークな発想、アグレッシブなアプローチのサービスで、社会に貢献しています。

| SERVICES |



CyberDefense

INCIDENT RESPONSE | インシデント対応サービス

精緻なフォレンジック調査と脅威インテリジェンスを活用した高品質なインシデント対応サービス。

PENETRATION TESTING | 侵入テスト・脆弱性診断

高度な知識と豊富な経験、優れた攻撃センスを併せ持つハッカーによる、極めて実戦的な侵入テスト。

OTHER SERVICES | 教育・開発・コンサルティング

CSIRTの機能強化支援、ハンズオントレーニング、サイバー演習実施、脅威インテリジェンス基盤の開発、各種調査研究など、様々な手法でお客様の課題解決を支援。

| CONTACT INFORMATION |

サイバーディフェンス研究所　営業部
TEL : 03-3242-8700 | FAX : 03-3242-8703 | email : sales@cyberdefense.jp

株式会社セキュアスカイ・テクノロジー

https://www.securesky-tech.com/

Secure Sky Technology Inc.

会社説明

「インターネットを安全にしたい」

その想いを原点に、2006年3月に、大手セキュリティ企業のWebアプリケーションセキュリティ部門のエンジニアが中心となり設立。自社開発の診断ツールを活用し、品質は高いままスピードと低価格でご提供できる診断サービスを実現。その後、セキュア設計・開発ガイドライン策定支援と教育サービス、クラウド型WAF「Scutum（スキュータム）」と、事業を拡大してまいりました。株式会社セキュアスカイ・テクノロジーは、Webアプリケーションセキュリティという切り口で、お客様のビジネスをサポートいたします。

Webアプリケーションの脆弱性に関する３つのアプローチ

Webアプリケーションの要件定義から運用に至る各フェーズに対する、一貫したセキュリティサービスをご提供いたします。

■脆弱性を「作らない」/ 支援サービス

約20社に対し、セキュアプログラミング教育を実施し、約10社に対しセキュア開発ガイドライン策定の支援を行っております。

■脆弱性を「見つける」/ 診断サービス

年間500サイト以上の診断を実施しております。

■脆弱性を「無害化する」/ 防御サービス

国内SaaS型WAF市場8年（2010年～2017年）連続シェアNo.1

※ミック経済研究所刊、株式会社アイ・ティ・アール刊、富士キメラ総研刊 調査

支援活動

九州を拠点とする以下のセキュリティコミュニティ活動団体を対象に、情報セキュリティ人材育成支援の一環として支援活動を行っています。

【セキュリティとんこつ「ばりかた勉強会」】 http://d.hatena.ne.jp/barikata-sec/

【北九州情報セキュリティ勉強会「セキュ鉄」】 https://sites.google.com/site/seckitakyu/

【九州学生エンジニア連合】 https://student-kyushu.org/

お問い合わせ先	株式会社セキュアスカイ・テクノロジー Tel : 03-3525-8045 ｜ Mail : info@securesky-tech.com

トレノケート株式会社

http://www.trainocate.co.jp/SCT180930kb

TRAINOCATE

新入社員から高度IT人材・経営層まで全階層をカバーする1,000以上のコースをご提供

<IT研修 対応分野>

対応スキルレベル		IT運用管理	クラウド	ストレージ/サーバー	セキュリティ	ネットワーク	仮想化	OS	データベース/データ分析	Web/プログラミング	要件定義/SWE/BA
段階	ITSSレベル										
ハイレベル	4以上	○	○	○	○	○	○				○
ミドルレベル	3相当	○	○	○	○	○	○	○	○	○	○
エントリーレベル	2~3相当	○	○	○	○	○	○	○	○	○	○
IT基礎	0~1相当		○	○	○	○	○	○	○	○	

新入社員からトップエグゼクティブまでのビジネススキル研修、グローバル人材育成も行っています

<コース例>

情報セキュリティ対策 ログ分析編 ～攻撃の足跡を見逃さない技術～	2日	¥160,000	集合研修
目次 1. ログ分析とは　2. ログ管理　3. ログ分析手法　4. オペレーションシステムのログ　5. アプリケーションのログ　6. ネットワークのログ　7. セキュリティ機能のログ　8. ログ分析の実際　9. ログ分析のためのツール	日程 2018年：11/26, 12/25 2019年：1/28, 3/6		

お問合せ先	トレノケート株式会社　http://www.trainocate.co.jp/SCT180930kb 〒163-6019 東京都新宿区西新宿6-8-1　住友不動産新宿オークタワー20階 〒530-0005 大阪府大阪市北区中之島3-2-18　住友中之島ビル11階 〒460-0004　愛知県名古屋市中区新栄町2-13　栄第一生命ビル6階 0120-009686 (無料) トレノケート　検索

JNSA 会員企業のサービス・製品・イベント情報

■サービス紹介■

○潜伏脅威診断サービス
日商エレクトロニクスが国内唯一の代理店として販売するVectra Networks社製 Xシリーズを活用し、お客様に代わって企業インフラ内に潜伏した脅威を調査/診断します。LAN内トラフィックを一定期間モニタリングし、隠れたサイバー攻撃などを可視化するスポットサービスです。専門のセキュリティアナリストが監視結果を分析の上、対策の提案を含めた診断レポートを提供します。
【サービス情報詳細】
https://www.nissho-ele.co.jp/press/2018/1808_securityservice.html
◆お問い合わせ先◆
日商エレクトロニクス株式会社
セキュリティ本部セキュリティサービス部
TEL: 03-6272-3980
E-mail: cyber_security@nissho-ele.co.jp

○IBM CSIRT研修
セキュリティ事故対応に数多くのご支援をしているIBMの専門家が経験をもとに事故対応・CSIRT構築の肝をご教示いたします。
•2018年11月5日（月）～8日（木）　4日間
　東京・茅場町　40万円（1人・税別）
　（フォレンジックスキル不要）
•経済産業省第四次産業革命スキル習得講座
　「Reスキル講座」
•厚生労働大臣指定教育訓練講座
＊研修内容＊
•CSIRTの概要とインシデント対応、外部からの攻撃によるインシデント対応、など
【サービス情報詳細】
https://ibm.co/Zsmo96
◆お問い合わせ先◆
日本アイ・ビー・エム株式会社
E-mail: eba2443@jp.ibm.com

■イベント紹介■

○Security Days Fall 2018 Tokyo内講演
　「サイバー攻撃の最新動向」
キヤノンITソリューションズのマルウェアラボでは、国内外で検出されたマルウェアを日々解析しています。そんなマルウェア解析者の視点から具体的なサイバー攻撃例をもとにサイバー攻撃の最新動向とその対策を紹介します。
日時：2018年10月4日(木) 9:35～10:15
場所：JPタワー ホール＆カンファレンスセンター
住所：東京都千代田区丸の内二丁目7番2号 KITTE 4,5階
費用：無料（事前登録制）
【イベント情報詳細】
https://eset-info.canon-its.jp/info/event/
◆お問い合わせ先◆
キヤノンITソリューションズ株式会社
TEL: 03-6701-3475
E-mail: seminar-info@canon-its.co.jp

■製品紹介■

○国内シェアNo.1 ログ管理ツール【ALog】
ALogシリーズは、様々な情報システムのログを1カ所に集約、解析し、企業のあらゆる課題解決に貢献するソフトウェアです。
独自の変換ロジックで、システムが出力する難解なログを、 ユーザー操作通りのログに翻訳変換。目的に応じた多種多様なレポートを作成出来ます。
情報漏洩や内部不正対策はもちろん、ランサムウェアの検知や働き方改革にまで、ALogシリーズで収集したログはあらゆるシーンにご活用頂けます。
【製品情報詳細】
https://www.amiya.co.jp/lp/lpalog/
◆お問い合わせ先◆
株式会社網屋｜営業本部　東日本営業部
TEL: 03-6822-9996 （ダイヤルイン）
E-mail: bv-sales@amiya.co.jp

○Webアプリケーション脆弱性検査ツール『Vex』
Vexは定期的な自社サイトの検査、開発工程でのテストなど、様々なシーンでいつでも・何度でも利用できます。導入企業からは低コスト・高機能・診断サービスでの品質向上・操作性・サポート力など総合的に高い評価を頂いています。検査コストを削減し検査品質を向上したい企業様に、Vexが脆弱性対策を全力でサポートします。2週間無料でトライアルを頂けますので、国産ツールであるVexをこの機会に是非お試しください。
【製品情報詳細】
https://www.ubsecure.jp/vex/overview
◆お問い合わせ先◆
株式会社ユービーセキュア
https://vex.ubsecure.jp/inquiry/inquiry

JNSA 2017 年度活動報告会

2018年6月12日（火）ベルサール神保町にて「JNSA 2017年度活動報告会」が開催されました。JNSAの部会・ワーキンググループより前年度の活動報告と今年度の活動計画を発表するとともに、JNSAの活動内容を会員以外にも広く周知することを目的として、毎年6月に開催しています。当日は183名の参加者をお迎えし、盛況のうちに終了いたしました。

【当日のプログラム：午前】

【A1】9：45-10：50〈65分〉調査研究部会

「協働の会の活動目的と報告」〈15分〉

脅威を持続的に研究するWG リーダー：大森 雅司 氏（㈱日立システムズ）

<発表概要>本WGでは、サイバー問題における正しい課題の理解と普及啓発を目的に、NISC、JPCERT/CC、IPA、JASAと連携した協働の会を発足しました。協働の会では、各分野の実情を踏まえた現場調査に基づき、問題の背景や関係性を含めた論点整理を経て、情報交換会を通じて発信を行っています。本セッションでは、2017年度の活動において見えてきた「重要インフラ」「産業システム」をキーワードとしたサイバー問題の背景や課題を中心に協働の会の活動状況について紹介します。

「2017年情報セキュリティインシデントに関する調査報告」〈30分〉

セキュリティ被害調査WGリーダー：大谷 尚通 氏（㈱エヌ・ティ・ティ・データ）

<発表概要>2017年の個人情報漏えいインシデントに関する調査結果を報告します。2017年1月から12月までに公開されたインシデント情報を長崎県立大学とWGが共同で調査・分析しました。近年は大規模なインシデントが減少しているが、インシデントが発生した時に組織へ求められる説明責任は、大きくなっています。WGでは、個人情報漏えいなどのインシデントが発生した時の公表や報告書の執筆に関するガイドを作成しましたので、その内容も紹介します。

「2017年度 国内情報セキュリティ市場調査報告」〈20分〉

セキュリティ市場調査WG：森田 翔 氏（株式会社km2y）

<発表概要>2017年度年間を通して分析作成した国内情報セキュリティ市場調査がまとまったので報告します。本報告は、2016年実績推定値2017年2018年推定値を元に各市場の状況の変化を考察したもので、成果発表会を通して共有したいと考えます。

休憩（10：50 - 11：00）

【A2】11：00-11：50〈50分〉調査研究部会、ISOG-J

「新しい価値を創造する人事論的、組織論的なセキュリティ対策とは？」〈20分〉

組織で働く人間が引き起こす不正・事故対応WG リーダー：甘利 康文 氏（セコム㈱）

<発表概要>現在、本WGでは、活きいきとやりがいを持って働ける「従業員満足度(ES: Employee Satisfaction)の高い職場環境」を創出するための様々な工夫を調査し、紹介する活動を行っています。働く人間に「悪い意思決定」をさせない環境を提供するための工夫を掘り起こし、共有することが、これまでの内部不正対策にない、新しい方向性からのセキュリティ対策、すなわちマイナスを防ぐのではなく、新しい価値を創り出すプラスのセキュリティ対策になるはずとの想いからです。今回は、この1年で実施した調査の概要を中心にWG活動の概要を報告させて頂きます。

「ISOG-Jの2017年度成果物あれこれ」〈30分〉

ISOG-J セキュリティオペレーション認知向上・普及啓発WGリーダー：阿部 慎司 氏（NTT セキュリティ・ジャパン㈱）

ISOG-J セキュリティオペレーション連携WGリーダー：武井 滋紀 氏（NTTテクノクロス㈱）

<発表概要>日本セキュリティオペレーション事業者協議会（ISOG-J）はセキュリティ事業者が集まり複数のワーキンググループを構成し活動しています。本講演では、各ワーキンググループにおけるガイドラインの発行や講演会、他団体との連携などの2017年度の活動成果と、2018年度に予定している取り組みついてご報告いたします。

【当日のプログラム：午後】

【A3】13：00-13：50〈50分〉標準化部会

「2017年度 電子署名WG成果報告/JT2A紹介」〈30分〉

電子署名WG サブリーダー：小川 博久 氏（みずほ情報総研㈱）

＜発表概要＞発足6年目を迎える電子署名WGは、PDF長期署名プロファイルのISO規格を策定（経済産業省事業）、電子処方箋への電子署名適用検討（保健医療福祉情報システム工業会）を行いました。また、今年はPKI相互運用技術WGと電子署名WGを基に「日本トラストテクノロジー協議会（JT2A)」を正式に発足し、リモート署名を含め、超スマート社会（Society5.0）を想定したトラスト技術の検討を行います。本発表では、2017年度の活動と2017年度の計画といくつかのトピックを紹介します。

「2017年度 アイデンティティ管理WG成果報告」〈20分〉

アイデンティティ管理WG リーダー：宮川 晃一 氏（日本電気㈱）

＜発表概要＞アイデンティティ管理WGは発足13年目を迎えます。その間IT環境は大きく様変わりしましたが、ID管理、認証・認可のテーマにつきましては、どのようなIT環境においても普遍的なテーマとして取り上げられ、重要なテーマの1つとなっています。昨年度は「チャットボットにおける認証・認可の課題」や「認証・認可の前提となる要素」について検討を行いましたのでその概要と、今年度の活動内容についても合わせてご紹介いたします。

休憩（13：50 - 14：00）

【A4】14：00-14：30〈30分〉西日本支部

「経営者向け情報セキュリティ対策実践手引き　報告」

西日本支部長：嶋倉 文裕 氏（富士通関西中部ネットテック㈱）

＜発表概要＞JNSA西日本支部では、主に中小企業の現場の方々を対象に、情報セキュリティ上のリスクに取り組むためのツールの開発に取り組んできました。経営者向け情報セキュリティ対策実践手引きWGでは、経営の視点から情報セキュリティ対策の必要性を検討し、対策に投資するための判断をするための、見える化施策を検討してきました。今回はその検討成果についてご報告します。

【A5】14：30-15：30〈60分〉社会活動部会

「CISOハンドブック：業務執行として考える情報セキュリティ」

CISO支援WG リーダー：高橋 正和 氏（㈱Preferred Networks）

＜発表概要＞情報セキュリティは、危険性・損失といったマイナス面ばかりで、ビジネスへの貢献というプラスの視点で議論される事はほとんどありません。しかし、経営陣として、CISOがセキュリティに取り組むためには、危険性や損失だけではなく、ビジネスへの貢献といった経営的な取り組みが求められます。本セッションでは、「CISOハンドブック」を題材に、業務執行としてのセキュリティという視点から、経営陣の一員としてのCISOを議論します。

【会場の様子】

活動報告会の発表資料はJNSAのウェブサイトで公開しています。ぜひご覧ください。
https://www.jnsa.org/seminar/2018/0612/

「JNSA 全国横断サイバーセキュリティセミナー 2018」

マーケティング部会では、地域でのセキュリティ啓発とJNSAの知名度向上を目的として、「JNSA 全国横断サイバーセキュリティセミナー2018」を、大阪、金沢、札幌、東京、沖縄の全国5都市で開催いたしました。

会員企業の皆様にスポンサーとして協賛いただき開催するこの全国横断セミナーは今年度で2回目となりますが、昨年同様大変好評で、参加受付開始後10日ほどで大阪、東京会場が満席となりました。

【セミナー概要】

◆名　称：　JNSA 全国横断サイバーセキュリティセミナー2018

◆主　催：　NPO日本ネットワークセキュリティ協会（JNSA）

◆後　援：　経済産業省、NPO ITコーディネータ協会
（金沢会場のみ）石川県商工会議所連合会、一般社団法人石川県情報システム工業会
（札幌会場のみ）札幌商工会議所
（沖縄会場のみ）一般社団法人九州経済連合会、公益財団法人沖縄県産業振興公社、
一般財団法人沖縄ITイノベーション戦略センター
沖縄県商工会議所連合会、那覇商工会議所

◆協　賛：　（社名昇順）
EMCジャパン株式会社(RSA)、アイマトリックス株式会社、
アルプス システム インテグレーション株式会社、
ウォッチガード・テクノロジー・ジャパン株式会社、
株式会社サイバーディフェンス研究所、
大日本印刷株式会社、株式会社ディアイティ、
デジタルアーツ株式会社、トレノケート株式会社、
ネットワンシステムズ株式会社、
株式会社 日立システムズ、株式会社日立ソリューションズ、
株式会社ユービーセキュア

◆料　金：　無　料

◆対象者：　企業内セキュリティ担当者、SIerのセキュリティ製品販売者

◆開催会場

会場名	開催日	会場名
大阪	2018年8月29日（水）	第二吉本ビルディング貸し会議室
金沢	2018年9月5日（水）	金沢商工会議所
札幌	2018年9月18日（火）	札幌商工会議所
東京	2018年9月26日（水）	浅草橋ヒューリックカンファレンス
沖縄	2018年10月4日（木）	沖縄産業支援センター

今回のセミナーでは、まず始めにJNSAの講師が最新のセキュリティ脅威と対策ポイントについて解説をおこない、続いてISOG-J（日本セキュリティオペレーション事業者協議会）メンバーが、ISOG-Jの成果物である「セキュリティ対応組織成熟度セルフチェックシート」と「セキュリティ対応組織の教科書」を紹介しながら自組織のセキュリティ成熟度を測る方法をご紹介しました。

続いて、今回のセミナーの目玉でもある経済産業省サイバーセキュリティ課の方によるご講演です。「産業サイバーセキュリティ強化へ向けた経済産業省の取組の紹介」と醍して、サイバー攻撃の現状や経済産業省のサイバーセキュリティ政策動向、経済産業省が取り組みを進めているサイバーセキュリティ経営ガイドライン、コネイン税制、情報セキュリティサービス基準の策定等の政策についてご説明いただきました。

最後に、JNSA講師が、JNSAで公開している様々なお役立ちツールの使い方をご紹介し、セミナー終了後は「セキュリティなんでも質問コーナー」として、情報セキュリティに関する様々な質問に当日の講師が個別に対応いたしました。

大阪会場でのISOG-J講演の様子

金沢会場での経済産業省様講演

会場では、セミナースポンサー提供のドリンクやお菓子、カタログ類をみなさまにお配りし、また、ITコーディネータ協会後援イベントのため、ITコーディネータ資格保持者の方にはITC実践力ポイントが、CISSPとCAI資格保持者にはCPEポイントが付与されました。アンケート結果（大阪会場のみ）では、ぜひ来年度も開催して欲しいという意見が複数見受けられました。地方では経済産業省本省の方の講演を聞く機会は少ないと思いますので、ぜひ来年度も要望があれば企画したいと考えております。

2018年度「インターネット安全教室」のご案内

～パソコンやスマートフォンで思わぬトラブルや犯罪にまきこまれないために～

誰でも手軽にインターネットに接続できるようになった今日、ウイルス感染、詐欺行為、プライバシー侵害など情報犯罪の被害にあう危険性がますます高くなってきています。いかに技術が進歩しても、ひとりひとりの意識の向上、モラルの徹底がなければ、これらの被害を防ぐことはできません。JNSAでは、経済産業省の委託事業として一般市民の情報セキュリティ知識向上のセミナー「インターネット安全教室」を、2003年度から実施してきました。2014年度より経済産業省補助金事業、独立行政法人情報処理推進機構（IPA）委託事業として、引き続き「インターネット安全教室」を全国で開催して参ります。

【開催概要】

［主　　催］ 独立行政法人情報処理推進機構（IPA）、 NPO日本ネットワークセキュリティ協会（JNSA）

［共　　催］ 全国各地のNPO・団体・自治体・学校など

［協　　力］ 全国読売防犯協力会

［後　　援］ サイバーセキュリティ戦略本部、警察庁、その他各開催地大学・新聞各社・県・県警等（以上予定）等

インターネット安全教室とは？

家庭や学校からインターネットにアクセスする人々を対象に、どうすればインターネットを安全快適に使うことができるか、被害にあったときにはどうすればいいかなど、情報セキュリティに関する基礎知識を学習できるセミナー「インターネット安全教室」を開催しております。

会場では参加者全員に、ドラマやドキュメンタリーを通じて最新の情報セキュリティに対する脅威が学べる「映像知る情報セキュリティ」の最新版ＤＶＤのほか、スマートフォン利用に関するミニパンフレット、を配布し、情報セキュリティの向上にお役立ていただいております。

こんな方はぜひご連絡下さい

・一般市民向けの情報セキュリティセミナーを実施したいがコンテンツがない
・教材を製作するにもコストも手間もかかるのでなかなかできない
・セミナー運営のノウハウがない
・しかし、情報セキュリティは大切。普及活動を行わないといけないと思っている

とお考えの団体さまがいらっしゃいましたら、ぜひ「インターネット安全教室」の共同開催をご検討下さい。

最新の開催状況については、「インターネット安全教室」ホームページをご確認ください。
https://www.ipa.go.jp/security/keihatsu/net-anzen.html

SECURITY CONTEST (SECCON) 2018

SECCONとは、情報セキュリティをテーマに多様な競技を開催する情報セキュリティコンテストイベントです。実践的情報セキュリティ人材の発掘・ 育成、技術の実践の場の提供を目的として、2012年に始まりました。世界の情報セキュリティ分野で通用する実践的情報セキュリティ人材の発掘・育成を最終目標として、まずはICTに関わるすべての人材への情報セキュリティの考え方や知見を広めることでセキュリティ予備人材の裾野を広げ、さらにその中から世界に通用するセキュリティ人材を輩出し、よって日本の情報セキュリティレベルを世界トップレベルに引き上げることを目的として活動を行っています。

2018年2月に行われたSECCON 2017決勝大会（国際大会）では、日本最大の「ハッカー大会」として、99ヶ国から累計4,349人が参加し、東京で世界レベルのハッキング対決が繰り広げられました。カンファレンスや企画展示などを同時開催しました。

【開催概要】

［主　催］SECCON実行委員会（特定非営利活動法人日本ネットワークセキュリティ協会）
［運　営］株式会社ナノ・オプトメディア
［後　援］

- 高度情報通信ネットワーク社会推進戦略本部
- サイバーセキュリティ戦略本部
- 警察庁
- 総務省
- 公安調査庁
- 文部科学省
- 経済産業省
- 国土交通省
- 国立研究開発法人 情報通信研究機構（NICT）
- 独立行政法人 情報処理推進機構（IPA）
- 一般財団法人 日本情報経済社会推進協会（JIPDEC）
- 一般社団法人 日本経済団体連合会（経団連）
- 日本シーサート協議会

[SECCON Beginners とは]

SECCON Beginners 2018は、コンピュータセキュリティ技術を競う競技であるCTF（Capture The Flag）の未経験者を対象とした勉強会です。本勉強会では、CTFに必要な知識を学ぶ専門講義と実際に問題に挑戦してCTFを体験してもらう演習を行います。

[CTF for GIRLSとは]

CTF for GIRLSは、情報セキュリティ技術に興味がある女性を対象に、気軽に技術的な質問や何気ない悩みを話しあうことが出来るコミュニティを作る事を目的に立ち上げられました。コミュニティ形成の一環として女性同士で情報セキュリティ技術を教え合うCTFワークショップや、その他女性向けCTFイベントの開催を行っています。

[協賛企業の募集]

SECCONの運営は民間企業等からの協賛金により行っています。SECCONでは年間を通じてスポンサーを募集しておりますので、お気軽にお問合せ下さい。（SECCON運営事務局: info2018@seccon.jp）

2018年度スポンサー企業はSECCONホームページ（https://2018.seccon.jp/）をご覧下さい。

■SECCON2018 開催スケジュール

日　　程	開催大会	会　　場	競技内容
2018年10月27日-28日	SECCON CTF予選	インターネット	CTF予選(日本語+英語)
2018年12月22日-23日	SECCON CTF(国際)	AKIBA SQUARE 秋葉原コンベンションホール	国際決勝大会(2日間)
2018年12月23日	SECCON CTF (国内)		国内決勝大会(1日間)

■SECCON Beginners 2018 開催スケジュール

日　　程	開催大会	会　　場	演習内容
2018年9月1日	SECCON Beginners 2018広島	広島市立大学サテライトキャンパス	ワークショップ+CTF演習
2018年10月6日	SECCON Beginners 2018東京	東京都立産業技術高等専門学校	ワークショップ+CTF演習
2018年10月6日	SECCON Beginners 2018東京		Beginners NEXT
2018年11月24日	SECCON Beginners 2018名古屋	㈱中電シーティーアイ	ワークショップ+CTF演習
2019年1月予定	SECCON Beginners 2018関西	未定	ワークショップ+CTF演習

■CTF for GIRLS 開催スケジュール

日　　程	開催大会	会　　場	演習内容
2018年6月22日	第9回　ワークショップ	㈱富士通ラーニングメディア	Web分野
2018年8月19日	第2回　CTF for School GIRLS	㈱日立システムズ	ネットワーク
2019年2月8日	第10回　ワークショップ	未定	Crypto分野

最新の開催状況については、「SECCON 2018」ホームページ（https://2018.seccon.jp/）をご確認ください。

SECCONでは、メールマガジンを発行しています。
・各種大会、ワークショップ等の開催アナウンスと開催報告
・SECCON実行委員メンバーやCTF for Girlsメンバーによるコラム
・スポンサー企業からのお知らせ

メールマガジンのご登録はこちらから!
https://frm.f2ff.jp/form/seccon_ml/

事務局お知らせ

JNSA ANNOUNCE

後援・協賛イベントのお知らせ

1. CodeBali2018
主　催： ID-SIRTII
日　程： 2018年10月9日～12日
会　場： パドマリゾートレギャン（インドネシア）

2. CEBIT ASEAN Thailand 2018
主　催： IMPACT
日　程： 2018年10月18日～20日
会　場： インパクト･エキシビジョン&コンベンションセンター（バンコク/タイ）

3. iコンピテンシ ディクショナリ活用セミナー
主　催： 特定非営利活動法人スキル標準ユーザー協会
日　程： 2018年10月18日、11月1日、15日、29日
会　場： 大阪、大宮、札幌、岡山（詳細はHPでご確認下さい）

4. ITGI Japan カンファレンス 2018
主　催： 日本ＩＴガバナンス協会
日　程： 2018年11月13日
会　場： 東京コンファレンスセンター品川

5. Internet Week 2018
主　催： 一般社団法人日本ネットワークインフォメーションセンター
日　程： 2018年11月27日～30日
会　場： ヒューリックホール&ヒューリックカンファレンス

6. Cybertech Tokyo 2018
主　催： Cybertech Tokyo実行委員会
日　程： 2018年11月29日～30日
会　場： 虎ノ門ヒルズフォーラム

7. 2018年度IPA中小企業情報セキュリティ講習 能力養成セミナー
主　催： 独立行政法人情報処理推進機構
日　程： 2018年7月～12月
会　場： 全国15～20ヵ所（詳細はHPでご確認下さい）

8. 情報モラル啓発セミナー | 情報モラルシンポジウム
主　催： 中小企業庁、北海道経済産業局、東北経済産業局　四国経済産業局、関東経済産業局、中部経済産業局、内閣府沖縄総合事務局、九州経済産業局、公益財団法人ハイパーネットワーク社会研究所
日　程： 2018年9月～2019年2月
会　場： 全国10ヵ所（詳細はHPでご確認下さい）

9. SECON 2019
主　催： SECON 2019 Organizing committee
日　程： 2019年3月6日～3月8月
会　場： KINTEX （大韓民国　ソウル）

■Gartner Symposium/ITxpo 2018■

Gartner®
SYMPOSIUM ITXPO®

最適なテクノロジ戦略を策定および実行するには、市場トレンドを明確に理解することが極めて重要です。ひとつとして同じ戦略はありませんが、デジタルな未来の構想と実現はどの組織にも共通したニーズです。先見性に富むスピーカー、ビジネスの第一線で活躍している多くのCIOおよび企業のリーダー、業界の専門家、テクノロジ・プロバイダーが一堂に会するGartner Symposium/ITxpoでは、デジタル・トランスフォーメーションの促進に必要なインスピレーション、専門知識、そして確固たる自信を得ることができます。
本イベントで最新トレンドを捉え、未来のIT／ビジネス戦略を形成する方法を見つけてください。

【会　　期】
2018年11月12日（月）～11月14日（水）
【会　　場】
グランドプリンスホテル新高輪　国際館パミール
【参加料金】
2018年10月10日（水）まで
→早期割引価格　174,000円（1名様・税別）
2018年10月11日（木）以降
→通常価格　198,000円（1名様・税別）
※グループ特別割引：
同時に5名様ご登録で1名様分無料

イベントの詳細・参加お申込みはこちら
⇒ https://gartner-em.jp/symposium/

JNSA部会・WG2018年度活動

1. 社会活動部会

部会長：丸山司郎 氏／株式会社ベネッセインフォシェル
副部会長：唐沢勇輔 氏／ソースネクスト株式会社

JNSAが情報セキュリティにおける社会変革の強力な推進者となるため、メディア等を通じた情報発信や社会貢献活動、政府機関や海外組織との連携など、JNSAの社会的活動を推進する。

具体的には、JNSAとしての情報発信の後押し、政府と協力した政策転換の促進、メディアや市場の力を活用した普及啓発活動、委託事業などの社会貢献活動、講師派遣などの外部組織支援、国際・他団体連携などを行う。

また、情報セキュリティ業界の自主規制の指針検討を行う。

【セキュリティ啓発WG】

（リーダー：山田英史 氏／株式会社ディアイティ）

独立行政法人情報処理推進機構（IPA）委託事業である「インターネット安全教室」の内容検討や運営サポート、広報活動の検討などを行う。

＜予定成果物＞

・インターネット安全教室の活動報告書

【海外市場開拓WG】

（リーダー：一宮隆祐 氏／日本電気株式会社）

昨年度の活動を継続し、Made-in-Japanのセキュリティソリューションの海外展開・拡販を業界団体として促進する。

具体的には、展示会出展による参加企業の販売代理店の開拓、商談発掘の支援、海外セキュリティコミュニティとの連携を実施する。また、JNSA ゲーム教育WG開発のゲーム（セキュリティ専門家人狼など）の英語翻訳を行い、JNSA発のコンテンツの海外展開可能性についても検証する。

海外市場に進出する上での手順や課題と解決策を纏めた「海外市場進出ガイド」のアップデートを実施する。

セキュリティ事業に特化した輸出関連の勉強会（成果物）開催も検討する。

＜予定成果物＞

- 英語版 セキュリティ専門家人狼の説明書・ガイドブック（ゲーム教育WGとの共同成果物）
- 海外市場進出ガイド
- セキュリティ事業特化の輸出関連ガイド

【CISO支援WG】

（リーダー：髙橋正和 氏／株式会社Preferred Networks）

CISOを支援するための情報を取りまとめ公開する。

＜予定成果物＞

- CISOハンドブック
- セミナー・ワークショップ

【JNSA CERC】

（リーダー：髙橋正和 氏／株式会社Preferred Networks）

緊急時の情報交換のプラットフォームとして活動する。

2. 調査研究部会

部会長：前田典彦 氏／株式会社カスペルスキー

情報セキュリティにおける各種の調査および研究活動を行う。セキュリティ被害、情報セキュリティ市場などの統計分析事業、および、重要度や緊急度の高いテーマに関する脅威分析、対策研究を推進する。適切な時期、形式を用いて適宜情報公開を行い、調査研究における成果を広く社会に還元する。新規性や緊急性の高いテーマの検討が必要となる場合においては、勉強会、BoFなどを随時行うなどして、柔軟かつ迅速な対応を行う。

【セキュリティ被害調査WG】

（リーダー：大谷尚通 氏／株式会社エヌ・ティ・ティ・データ）

個人情報漏えいインシデント調査の長崎県立大学への移管を継続して実施し、調査体制を確立する。長崎県立大学と共同で個人情報漏えいインシデント調査を実施し、報告書を公表する。

インシデント被害の定量化に向けて、引き続き個人情報などのセキュリティインシデントの公表、および報告書の執筆に関するガイドを完成させて発表する。

＜予定成果物＞

- 2017年個人情報漏えいインシデント調査報告書
- インシデント報告(報道や報告書)の標準化テンプレート

【セキュリティ市場調査WG】
（リーダー：蜂巣悌史 氏／株式会社km2y）

国内で情報セキュリティに関するツール、サービス等の提供を事業として行っている事業者を対象として、推定市場規模データを算出し報告書として公開する。

また、近年のセキュリティ市場拡大の伴う、市場調査の調査内容、セキュリティ区分の見直しを行う。

＜予定成果物＞

- 市場調査方法及びセキュリティ区分の見直し案
- 2018年度情報セキュリティ市場調査データ

【組織で働く人間が引き起こす不正･事故対応WG】
（リーダー：甘利康文 氏／セコム株式会社）

(1)人の意識や組織文化、(2)組織の行動が影響を受ける社会文化や規範、(3)不正を防ぐシステム、の3方向から「組織で働く人間が引き起こす不正・事故」に対する考察を深め、ベストプラクティスの紹介、提案、啓発を行うことを目的とする。

2018年度も引き続き、特に(1)に重点をおいた活動を行う。

＜予定成果物＞

- 「組織文化醸成によるES向上」に向けた各組織の取組事例ヒアリング調査と、調査内容をベースとしたWeb記事の公開。
- JNSA Pressへの寄稿、セミナー等への積極的出講による啓発活動の展開。

【IoTセキュリティWG】
（リーダー：松岡正人 氏／株式会社カスペルスキー）

IoTセキュリティWGが過去に蓄積し、レポートに展開してきた知見を広め、活用の促進を図るために活動する。

＜予定成果物＞

- 勉強会、オープンセミナー開催

【脅威を持続的に研究するWG】
（リーダー：大森雅司 氏／株式会社日立システムズ）

サイバーセキュリティを取巻く環境の変化に応じ顧客ニーズや課題を捉え直し、国内外における新たなビジネスアプローチやマーケットの構図の変化を調査する。

＜予定成果物＞

- ホワイトペーパー（必要に応じて）

3. 標準化部会

部会長：中尾康二 氏／
国立研究開発法人情報通信研究機構
副部会長：松本泰 氏／セコム株式会社

業種・業界・分野等の標準化・ガイドライン化などを推進する。特に、JNSA目線のセキュリティベースラインの提供、情報セキュリティ対策ガイドラインの策定などを進める。また、国際標準/国際連携との親和性の高い案件については、国際標準への提案やコメントや日韓連携案件も視野に入れて、議論を進める。

【IoT機器セキュリティログ検討WG】
（リーダー:萩原健太 氏／トレンドマイクロ株式会社）

「IoT機器のセキュリティログの国際標準化」と「IoT機器のインシデント対応を行いやすくするための環境整備」を目的とし、機器提供組織のインシデント対応の負担軽減やセキュリティサービスを提供する組織のビジネス拡大を図る。

＜予定成果物＞

- 「セキュリティオペレーションを想定したIoT機器のログについて（仮）」（WG検討内容のサマリ）

【アイデンティティ管理WG】
（リーダー：宮川晃一 氏／日本電気株式会社）

IT環境の急激な変化における様々なアイデンティティ管理に関する課題をWG討議の中で検討し、必要性の啓蒙および導入指針の提示による普及促進、市場活性化を目的とする。

＜予定成果物＞

- 「IoT環境におけるアイデンティティ管理とは（仮称）」

【国際化活動バックアップWG】
（リーダー：中尾康二 氏／
国立研究開発法人情報通信研究機構）

国際標準化活動の情報共有を継続的に実施する。また、韓国KISIAとの共同フォーラムの開催など海外のセキュリティベンダーグループとの連携強化を図った活動を行う。

＜予定成果物＞

- 調整中

【電子署名WG】

（リーダー：宮崎一哉 氏／ 三菱電機株式会社）

電子署名（含タイムスタンプ）関連技術の相互運用性確保のための調査、検討、標準仕様提案、相互運用性テスト、及び電子署名普及啓発を行う。

＜予定成果物＞

- 署名検証プロセスに関する標準仕様ドラフト
- 長期署名プロファイルの改定案
- 電子署名関連情報のリンク集

【PKI相互運用技術WG】

（リーダー：松本泰 氏／セコム株式会社）

PKI の技術、標準化、法制度等の情報交換及び、議論を行うことを目的とする。年間4回程度のWG開催のほか、IETF参加報告会を開催する。「PKI Day 2018」の開催を行い、「PKI Day 2019」開催に向けたディスカッションを行う。

＜予定成果物＞

- なし （PKI day 2019の開催資料）

4. 教育部会

部会長：平山敏弘 氏／アクセンチュア株式会社

社会のニーズや時代の変化に適合したセキュリティ人材育成のため、必要とされる知識・技能等の検討を行い、実際に大学や専門学校等で評価実験を行う。また、情報セキュリティ教育のコンテンツとして、講義シラバスや講義資料およびSecBoK2018年版の作成・公開を通じて、教育界・産業界への展開・使用を促進することで、情報セキュリティ人材の育成に貢献する。2018年度は特に情報系大学における講義カリキュラム指標であるJ17との連携とASEANを中心とした海外教育機関との連携によるセキュリティ人材育成への貢献を目指している。

さらに、継続して講師データベースへの登録講師や講師予備軍の若手による講義・勉強会の開催等、教える場の提供を支援することにより、JNSA教育部会メンバーのスキル向上を目指す。加えてセキュリティコンテストとは異なる新たな実践教育ツールの開発や検証に対しても検討を行う。

＜予定成果物＞

- SecBoK2018

【ゲーム教育WG 】

（リーダー:長谷川長一 氏／株式会社ラック）

情報セキュリティに関するゲームを用いた教育や普及啓発の普及と促進、ファシリテーターの養成、JNSAゲームのブランド化等。

＜予定成果物＞

- 「セキュリティゲームファシリテーターガイドブック（仮称）」

【情報セキュリティ教育実証WG】

（リーダー：平山敏弘 氏／アクセンチュア株式会社）

情報セキュリティを教えることが出来る高度なスキルをもった人材を育成するために、大学などで講義を自ら実践することで、実践力とハイレベルスキルの習得を目的とする。

＜予定成果物＞

- 全15回分の授業コンテンツ
- 新たな講師経験者（教えることができる人材）の誕生

【セキュ女WG】

（リーダー：北澤麻理子 氏／
ドコモ・システムズ株式会社）

女性セキュリティエキスパートの交流場所を提供し（会社の枠を超えた連携を可能にする）、セキュリティに関する専門スキルを持ちたい女性を応援する。

勉強会を中心に活動し、テーマは年度の初回WGにメンバーで検討する。

5. 会員交流部会

部会長：萩原健太 氏／トレンドマイクロ株式会社

情報セキュリティ業界における健全な発展と貢献のため、会員向けのサービスとユーザー向けのサービスをマーケティング部会と連携しながら拡充させる。

特にソリューションガイドを、ユーザーにも、会員にもより利用しやすい環境とするための改修を行う。また会員向けの説明会や、政府統一基準群の改定予定を受けた各種ガイドライン等の勉強会、また紐づけについて継続的して実施する。

【セキュリティ理解度チェックWG】

（リーダー：萩原健太 氏／トレンドマイクロ株式会社）

理解度チェックの継続的な問題の見直しを行うと共に、プレミアム版のユーザー数増加に向けた対外活動を実施する。

＜予定成果物＞
- 理解度チェックサイトへの要望などへの対応
- 理解度チェックの問題アップデート

【JNSAソリューションガイド活用WG】
（リーダー：秋山貴彦 氏／株式会社アズジェント）

ソリューションカイドの更なる活用を踏まえ、年間の活動を通じて会員企業自身のPRとその企業が有しているソリューションのPRを図る。

＜予定成果物＞
- JNSA内の他部会/WGが作成した成果物とソリューションガイドとの連携
- 関係諸団体が作成した各種ガイドラインとソリューションガイドの連携
- ソリューションガイドサイトのリニューアル

【経営課題検討WG】
（リーダー：菅野泰彦 氏／
アルプスシステムインテグレーション株式会社）

前年度の活動を受け、企業の経営指標にサイバーセキュリティ投資の可視化（IT投資の内数として）を実態に即し、具体的で実務的な観点から検討。

年度内に答申案を仕上げる。

JNSAの過去の成果物を見返し利用し、温故知新、導入促進、普及啓発に繋がる、購入決裁者への訴求力のある資料の編集を行う。

＜予定成果物＞
- サイバーセキュリティ投資を可視化した経営指標答申案
- 非IT中小企業の購入決裁者向け製品・サービスの紹介資料

いずれも電子ファイルベースでの成果物とする。

6. マーケティング部会

部会長：小屋晋吾 氏／株式会社豆蔵ホールディングス

昨年度に引き続き、JNSAのWG成果物の普及促進を目的とした活動や、会員企業増加施策を企画、運営する。

主な活動は、会員企業増加施策の企画、Web改善の企画、会員企業向け勉強会のほか、一般向けセミナーの実施など。

＜予定成果物＞
- 全国セミナーの実施
- その他ノベルティ等の検討

7. 西日本支部

支部長：嶋倉文裕 氏／
富士通関西中部ネットテック株式会社

西日本に拠点を置くメンバー企業が中心となり、提携団体との協働の下、西日本のネットワーク社会におけるセキュリティレベルの維持・向上に資すると共に、産官共同して、IT利活用の実現・推進のため、西日本に集積する中小企業がリスクの変化に応じた機動的な対応を行うことができる機会づくりを支援する。

【企画・運営WG】
（リーダー：小柴宏記 氏／ジーブレイン株式会社）

JNSA会員および西日本地域のセキュリティレベルの向上を図る企画を立案、実施する。および会員企業向けの勉強会を実施する。

【中小企業のためのSecurity by Design WG】
（リーダー：大室光正 氏／
株式会社インターネットイニシアティブ）

これまでの西日本支部の活動の成果物を元に、経営者の情報セキュリティ投資の承認を得た後、中小企業の情報システム部門が考えるべき導入、運用、廃止までのライフサイクルを考慮した情報セキュリティシステムの姿を検討する。

8. U40部会

部会長：杉野広典 氏／
NECネクサソリューションズ株式会社

若年層を対象メンバーとして、JNSAの若返り、若年層の活動活発化、幅広い人脈形成を目的として勉強会を中心とした活動を行う。

【for Rookies WG】
（リーダー：岡島麗奈 氏／
株式会社サイバーエージェント）

セキュリティ関連業務経験3年未満を対象とし、若手をはじめとした人的ネットワークの形成および知識向上を目的とする。「いまさら聞けない相談事」を主に参加者が講師を担当などアクティブラーニング方式で行う。

【勉強会企画検討WG】
（リーダー：深谷隆 氏／日本プロセス株式会社）

U40部会員の知識・スキル向上を目指し、勉強会を企画・開催する。内容によってはJNSA会員からも広く勉強会参加者を募り、部会員同士・JNSA会員・外部講師との人脈形成を行う。

9. 情報セキュリティ教育事業者連絡会（ISEPA）

代表：持田啓司 氏／株式会社ラック

事業者間の連携や情報交換による業界活性化、政府機関への政策提言や政策実現ための適切な事業者紹介などを実施。年間活動予定として、セミナー開催、情報共有会議を行う。

＜予定成果物＞

- セキュリティ関連スタッフ調査報告書
- 教育コースのSecBoK対応マップ
- スキル認定ガイドライン

10. 日本セキュリティオペレーション事業者協議会（ISOG-J）

代表：武智洋 氏／日本電気株式会社

各WGで活動を実施する。MSSガイドv2.0への更改に向けた議論、セキュリティ対応組織（SOC、CSIRT）強化に向けたサイバーセキュリティ情報共有の「5W1H」の更改に向けた議論、次世代エンドポイントセキュリティ製品についての議論を実施する。

InternetWeek2018での講演やプログラム委員参加のほか、ISOG-J内でのアンケート実施予定。

＜予定成果物＞

- 各脆弱性診断ガイドライン
- MSSガイドv2.0
- セキュリティ対応組織(SOC,CSIRT)強化に向けたサイバーセキュリティ情報共有の「5W1H」 v2.0
- InternetWeek2018での公開向け資料

【セキュリティオペレーションガイドラインWG】
（リーダー:上野宣 氏／株式会社トライコーダ）

各脆弱性診断ガイドラインを作成する。

【セキュリティオペレーション技術WG】
（リーダー:川口洋 氏／株式会社ラック）

最新の技術動向を調査し、最適なセキュリティオペレーション技術を探究し、技術者の交流を図る。

【セキュリティオペレーション認知向上・普及啓発WG】
（リーダー:阿部慎司 氏／NTTセキュリティ・ジャパン株式会社）

セキュリティオペレーションの必要性に関する認知度向上を図り、月次定例WGの他、一般向けセミナーを2回開催予定。

【セキュリティオペレーション連携WG】
（リーダー：武井滋紀 氏／NTTテクノクロス株式会社）

セキュリティの運用について各社共通の課題の議論、検討を行う。月次定例会の他、集中検討会（夏・冬）開催予定。

11. 日本トラストテクノロジー協議会（JT2A）

運営委員長：小川博久 氏（みずほ情報総研株式会社）

電子署名や電子認証などを含むトラストテクノロジーに関連する事業者及び利用者が主体となり、産学官及び国内外の関連団体と連携して信頼性を担保するための技術等の検討を行い、より信頼できる電子社会の促進に寄与する。

＜予定成果物＞

- リモート署名ガイドライン

12. 産学情報セキュリティ人材育成検討会

座長：江崎浩 氏/東京大学 大学院教授

情報セキュリティ業界での就労体験の機会提供を目的にJNSAインターンシップを実施する。4月に学生と企業間の意見交換・交流のための交流会を東京大学と大阪のサテライト会場で実施し、両会場で67名の学生の参加があった。

夏期実施に向けたJNSAインターンシップ参加企業は15社となっている。

13. SECCON実行委員会

実行委員長：花田智洋 氏／国立研究開発法人情報通信研究機構
副実行委員長：寺島崇幸 氏／株式会社ディアイティ

企業スポンサーを募り、「SECCON 2018」として全国的にセキュリティコンテストを実施する。昨年に引き続き、CTF初心者向けや女性限定のワークショップの開催にも注力していく。

JNSA 役員一覧　2018 年 6 月現在

会　長　田中　英彦　情報セキュリティ大学院大学 名誉教授
副会長　髙橋　正和　株式会社Preferred Networks
副会長　中尾　康二　国立研究開発法人情報通信研究機構

理　事（50音順）

新井　一人　トレンドマイクロ株式会社
遠藤　直樹　東芝デジタルソリューションズ株式会社
大城　　卓　新日鉄住金ソリューションズ株式会社
笠原　久嗣　エヌ・ティ・ティ・アドバンステクノロジ株式会社
河内　清人　三菱電機株式会社
河野　省二　日本マイクロソフト株式会社
後藤　和彦　株式会社大塚商会
小屋　晋吾　株式会社豆蔵ホールディングス
櫻井　秀光　マカフィー株式会社
佐藤　憲一　株式会社OSK
下村　正洋　株式会社ディアイティ
高木　経夫　ユニアデックス株式会社
土屋　茂樹　株式会社エヌ・ティ・ティ・データ
西本　逸郎　株式会社ラック
藤伊　芳樹　大日本印刷株式会社
藤川　春久　セコムトラストシステムズ株式会社
丸山　司郎　株式会社ベネッセインフォシェル
水村　明博　EMCジャパン株式会社
三宅　　優　KDDI株式会社
三膳　孝通　株式会社インターネットイニシアティブ

幹　事（50音順）

浅田　　享　エヌ・ティ・ティ・アドバンステクノロジ株式会社
安達　智雄　日本電気株式会社
有松　龍彦　株式会社インフォセック
伊藤　良孝　株式会社インターネットイニシアティブ
大木　由利　大日本印刷株式会社
垣内由梨香　日本マイクロソフト株式会社
北澤麻理子　ドコモ・システムズ株式会社
木村　　滋　シスコシステムズ合同会社
後藤　　忍　セコムトラストシステムズ株式会社
駒瀬　彰彦　株式会社アズジェント
崎山　秀文　キヤノンITソリューションズ株式会社
嶋倉　文裕　富士通関西中部ネットテック株式会社
下村　正洋　株式会社ディアイティ
鈴木　英樹　株式会社OSK
髙橋　正和　株式会社Preferred Networks
辻　　秀典　ネットワンシステムズ株式会社
中間　俊英　株式会社ラック
能勢健一朗　東芝デジタルソリューションズ株式会社
萩原　健太　トレンドマイクロ株式会社
平山　敏弘　アクセンチュア株式会社
二木　真明　アルテア・セキュリティ・コンサルティング
前田　典彦　株式会社カスペルスキー
嶺村　慶一　株式会社アークン
本川　祐治　株式会社日立システムズ
森　　駿　ユニアデックス株式会社
油井　秀人　富士通エフ・アイ・ピー株式会社
与儀　大輔　NRIセキュアテクノロジーズ株式会社

監　事

土井　充　公認会計士 土井充事務所

顧　問

井上　陽一
今井　秀樹　東京大学 名誉教授
佐々木良一　東京電機大学総合研究所 特命教授¦サイバーセキュリティ研究所 所長
武藤　佳恭　慶應義塾大学 教授
手塚　　悟　慶應義塾大学大学院 特任教授
前川　　徹　国際大学グローバル・コミュニケーション・センター 所長
森山裕紀子　早稲田リーガルコモンズ法律事務所 弁護士
安田　　浩　東京電機大学 学長
大和　敏彦　株式会社アイティアイ
吉田　　眞　東京大学 名誉教授

JNSAフェロー

井上　陽一　JNSA顧問
大和　敏彦　JNSA顧問/株式会社アイティアイ

事務局長

下村　正洋　株式会社ディアイティ

会員企業一覧　2018年9月現在　222社　50音順

【あ】

(株)アーク情報システム
(株)アークン
あいおいニッセイ同和損害保険(株)
アイネット・システムズ(株)
(株)アイピーキューブ
アイマトリックス(株)
アイレット(株)
アクセンチュア(株)
アクモス(株)
(株)アズジェント
アドソル日進(株)
アドビシステムズ(株)
アビラ合同会社
(株)アピリッツ
アマノセキュアジャパン(株)　New
(株)網屋
アライドテレシス(株)
アルテア・セキュリティ・コンサルティング
(株)アルテミス
アルプスシステムインテグレーション(株)
EMCジャパン(株)
EYアドバイザリー・アンド・コンサルティング(株)
イオンアイビス(株)
伊藤忠テクノソリューションズ(株)
学校法人 岩崎学園
(株)インターネットイニシアティブ
(株)インテック
(株)インテリジェントウェイブ
インフォサイエンス(株)
(株)インフォセック
ウォッチガード・テクノロジー・ジャパン(株)
(株)AIR
SCSK(株)
(株)エス・シー・ラボ
SGシステム(株)
EDGE(株)
NRIセキュアテクノロジーズ(株)
(株)NIインテリジェントイニシアティブ
NECソリューションイノベータ(株)
NECネクサソリューションズ(株)
エヌ・ティ・ティ・アドバンステクノロジ(株)
エヌ・ティ・ティ・コミュニケーションズ(株)
エヌ・ティ・ティ・コムウェア(株)
NTTコムソリューションズ(株)
NTTセキュリティ・ジャパン(株)
NTTテクノクロス(株)
(株)エヌ・ティ・ティ・データ
(株)エヌ・ティ・ティ・データCCS
エヌ・ティ・ティ・データ先端技術(株)
(株)エヌ・ティ・ティ ネオメイト　New
エヌ・ティ・ティレゾナント(株)
(株)FFRI
エムオーテックス(株)
(株)OSK
(株)大塚商会
岡三情報システム(株)

【か】

(株)カスペルスキー
キヤノンITソリューションズ(株)
(株)クエスト
(株)クリエイティブジャパン
グローバルセキュリティエキスパート(株)
(株)km2y
KDDI(株)
KPMGコンサルティング(株)
興安計装(株)
(株)構造計画研究所
(株)神戸デジタル・ラボ
(株)コスモス・コーポレイション
コニカミノルタ(株)
(株)コンシスト

【さ】

サイエンスパーク(株)
再春館システム(株)　New
(株)サイバーエージェント
(株)サイバーディフェンス研究所　New
サイバー・ソリューション(株)
サイボウズ(株)
G・O・G(株)
ジーブレイン(株)
(株)JMCリスクソリューションズ
ジェイズ・コミュニケーション(株)
(株)JSOL　New

JBCC(株)
JPCERTコーディネーションセンター
ジェネシス・ジャパン(株)
(株)シグマクシス
シスコシステムズ合同会社
システム・エンジニアリング・ハウス(株)
(株)シマンテック
情報セキュリティ(株)
(株)信興テクノミスト
新日鉄住金ソリューションズ(株)
(株)Speee New
セイコーソリューションズ(株)
(株)セキュアスカイ・テクノロジー New
(株)セキュアソフト
SecureWorks Japan(株)
セキュリティ・エデュケーション・アライアンス・ジャパン
セコム(株)
セコムトラストシステムズ(株)
綜合警備保障(株)
ソースネクスト(株)
ソニー(株)
ソフォス(株)
ソフトバンク(株)
ソフトバンク・テクノロジー(株)
(株)ソリトンシステムズ
SOMPOリスケアマネジメント(株)

【た】

大興電子通信(株)
大日本印刷(株)
(株)宝情報
タレスジャパン(株)
(株) 中電シーティーアイ New
TIS(株)
(株)ディアイティ
デジタルアーツ(株)
鉄道情報システム(株) New
デロイト トーマツ リスクサービス(株)
(株)電通国際情報サービス
東京海上日動リスクコンサルティング(株)
東芝デジタルソリューションズ(株)
有限責任監査法人トーマツ
ドコモ・システムズ(株)
凸版印刷(株)
トレノケート(株) New
トレンドマイクロ(株)

【な】

(株)ナノオプト・メディア
日商エレクトロニクス(株)
日本アイ・ビー・エム(株)
日本アイ・ビー・エム　システムズ・エンジニアリング(株)
日本オラクル(株)
日本企画(株)
日本シノプシス合同会社
日本セーフネット(株)
(株)日本総合研究所
日本電気(株)
日本電信電話(株)
日本ビジネスシステムズ(株)
日本プロセス(株)
日本マイクロソフト(株)
日本ユニシス(株)
(株)ネクストジェン
ネットワンシステムズ(株)

【は】

パーソルテクノロジースタッフ(株)
パーソルプロセス&テクノロジー(株)
(株)パソナテック
パナソニック(株)
パロアルトネットワークス(株)
東日本電信電話(株) New
(株)日立システムズ
(株) 日立製作所 New
(株)日立ソリューションズ
飛天ジャパン(株)
(株)B5NOTE
BBソフトサービス(株) New
(株)PFU
PwCサイバーサービス合同会社
華為技術日本(株)
ファイア・アイ(株) New
(株)ファインデックス
(株)VSN
フォーティネットジャパン(株)
富士ゼロックス(株)
富士ゼロックス情報システム(株)
富士ソフト(株)
富士通(株)
富士通エフ・アイ・ピー(株)
(株)富士通エフサス

富士通関西中部ネットテック（株）
富士通クライアントコンピューティング（株）
（株）富士通ソーシアルサイエンスラボラトリ
（株）Preferred Networks
FRONTIER（株）
（株）ブロードバンドセキュリティ
（株）ブロードバンドタワー
（株）プロット
（株）ベネッセインフォシェル
北陸通信ネットワーク（株）

【ま】

マカフィー（株）
（株）豆蔵ホールディングス
丸紅OKIネットソリューションズ（株）
丸紅情報システムズ（株）
みずほ情報総研（株）
三井物産セキュアディレクション（株）
三菱スペース・ソフトウエア（株）
（株）三菱総合研究所
三菱総研DCS（株）
三菱電機（株）
三菱電機インフォメーションシステムズ（株）
三菱電機インフォメーションネットワーク（株）
（株）mediba

【や】

（株）ユービーセキュア
ユニアデックス（株）
（株）YONA New

【ら】

（株）ラック
（有）ラング・エッジ
（株）リクルートテクノロジーズ
リコージャパン（株）
（株）レピダム New
（有）ロボック

【わ】

（株）ワイズ

【特別会員】

一般社団法人 IIOT
（ISC）2　Japan
一般社団法人 コンピュータソフトウェア協会
ジャパン データ ストレージ フォーラム
国立研究開発法人情報通信研究機構 New
一般社団法人重要生活機器連携セキュリティ協議会
一般社団法人セキュアIoTプラットフォーム協議会 New
データベース・セキュリティ・コンソーシアム
特定非営利活動法人デジタル・フォレンジック研究会
電子商取引安全技術研究組合
東京大学大学院 工学系研究科
長崎県立大学情報システム学部情報セキュリティ学科
一般社団法人 日本インターネットプロバイダー協会
一般社団法人 日本クラウドセキュリティアライアンス
一般社団法人 日本コンピュータシステム販売店協会
特定非営利活動法人日本システム監査人協会
特定非営利活動法人　日本情報技術取引所
一般社団法人日本スマートフォンセキュリティ協会
特定非営利活動法人日本セキュリティ監査協会
一般財団法人 日本データ通信協会 タイムビジネス協議会

他二社

JNSA 年間活動（2018 年度）

4月	4月17日	PKI Day 2018「超スマート社会（Society 5.0）におけるトラストの在り方」
	4月28日	産学情報セキュリティ人材交流会〜これからの IT 人材のキャリアを考える
5月	5月13日	サイバーセキュリティ小説コンテスト説明会
	5月18日	第1回　幹事会
	5月21日	2018 年度　理事会
	5月23日	電子署名 WG 春祭り「電子署名の世界（SIGN WORLD）」
6月	6月12日	JNSA 2017 年度活動報告会 / 2018 年度総会（ベルサール神保町）
	6月22日	第9回　CTF for GIRLS
7月	7月13日	第2回　幹事会
8月	8月19日	第2回　CTF for School GIRLS
	8月29日	JNSA 全国横断サイバーセキュリティセミナー（大阪）
9月	9月1日	SECCON Beginners 2018（広島）
	9月5日	JNSA 全国横断サイバーセキュリティセミナー（金沢）
	9月18日	JNSA 全国横断サイバーセキュリティセミナー（札幌）
	9月26日	JNSA 全国横断サイバーセキュリティセミナー（東京）
	9月21日	第3回　幹事会
10月	10月4日	JNSA 全国横断サイバーセキュリティセミナー（沖縄）
	10月6日	SECCON Beginners 2018 ／ Biginners NEXT（東京）
	10月27日	SECCON CTF　予選
	10月28日	SECCON CTF　予選
11月	11月24日	SECCON Beginners 2018（名古屋）
12月	12月21日	Security Day 2018（熱海）
	12月22日	SECCON CTF（国際）
	12月23日	SECCON CTF（国際）
	12月23日	SECCON CTF（国内）
1月	（未定）	NSF 2018（予定）
	（未定）	賀詞交換会（予定）
2月	2月8日	第10回　CTF for GIRLS
3月	（未定）	NSF 2019 in Kansai（予定）
	3月4日−8日	RSA Conference 2019 出展（サンフランシスコ）

2018年5月から2019年3月
「インターネット安全教室」開催

★ JNSA 年間スケジュールは、https://www.jnsa.org/aboutus/schedule.html に掲載しています。
★ JNSA 部会、WG の会合議事録は会員情報のページ https://www.jnsa.org/member/index.html に掲載しています。（JNSA 会員限定です）

会員紹介（当コーナーでは、JNSA で活躍されている会員の方に、リレー方式で自己紹介をしていただきます。）

株式会社ユービーセキュア　田中　大介

JNSA会員の皆さま、株式会社ユービーセキュアの田中と申します。この度、株式会社ラックの佐々木さまよりバトンパスがあり、自己紹介の機会を賜りました。どうぞよろしくお願いいたします。

私とJNSAの出会いは、さかのぼること9年前、当時同じ部署にいた教育担当の勧めで参加したISEPA（情報セキュリティ教育事業者連絡会）のスキルワーキンググループに参加したことがきっかけです。直近では、海外市場開拓WGに発足当初より参加し、2017年度よりサブリーダーとして及ばずながら活動推進に努めております。

ユービーセキュアには、ＮＲＩセキュアテクノロジーズ株式会社から2013年1月より出向しております。弊社開発ソフトウェアである『Vex（Webアプリケーション脆弱性検査ツール）』と脆弱性診断サービスの営業として日々顧客開拓や数字とにらめっこしておりますが、海外市場開拓WG活動への参加と時を同じくして、Vexの海外進出や海外セキュリティ企業との協業など、「グローバル」がキーワードになる仕事が増えてまいりました。学生の時から「その国や地域のバックグラウンドがセキュリティの考え方に与える影響」について興味があった者としては、毎日ネタに事欠きません。最近では、この興味を読み物にまとめたいと考えるようになっております。

話は変わってプライベートですが、夏の離島シュノーケリング、冬のバックカントリースキーと日常生活から離れた時間を過ごしております。が、いかんせん一番の趣味である「Bar巡り」が私の成長を促していることから、最近ダイエットを目的としたボクササイズを始めました。しかし、運動後のご褒美がさらなる成長を促している感が否めません。ちなみにお酒はジンとウイスキーを好んで飲みます。洋酒がお好きな会員さまがいらっしゃいましたら、是非お声掛けください。

今回の自己紹介を書くにあたり、改めてこれまでを振り返ってみると、セキュリティに携わり20年近くも経っておりました。まさに光陰矢の如しです。今後も日々の業務やJNSAの活動を通じてお客様の安心安全、セキュリティ業界の一助となれるよう精進してまいります。

最後になりましたが、海外市場開拓WGの皆さま、いつもお忙しいところ活動にご参加いただき、ありがとうございます。これからも「日本発世界」を合言葉に頑張っていきましょう！

デジタルアーツ株式会社　武田　いづみ

JNSA会員の皆さま、はじめまして。デジタルアーツ株式会社の武田　いづみ（たけだ　いづみ）と申します。この度、トレンドマイクロ株式会社　萩原さんよりご紹介をいただき、私の自己紹介をさせていただきます。どうぞ、よろしくお願い致します。

私は大学を卒業後、某SIer企業に就職し、5年ほどSEとして勤めておりました。SEといっても、文系出身の私にとっては、IT業界自体が未知の世界で、恥ずかしながらPCの繋ぎ方にも四苦八苦していました。当初はUNIXベースのシステムの構築支援やミドルウェアの検証などのプロジェクトに配属され、新人なのでほぼお手伝いでしたが、ITの基礎を学ぶにはもってこいの環境でした。

そのうち、自社の製品を取り扱うメーカーの立場で仕事がしたいと考えるようになり、ミドルウェアのメーカーに転職しました。ここでは、メインフレームのマイグレーションやデータベースの拡販に従事しておりました。スタートアップの企業でしたので、広報やプロモーションの立ち上げから担当することになり、以来10数年、IT業界で広報やプロモーション、営業推進などの業務に携わっております。

そんな私がセキュリティの世界に飛び込んだのは、IT資産管理のメーカーへ2016年に転職したことがきっかけでした。IT資産管理の世界も、PCなどの端末情報を管理するだけではなく、OSのパッチやソフトウェアバージョンの管理、USBデバイス制御、フィルタリング、ふるまい検知など、脆弱性対策や情報漏洩対策の機能を搭載しており、広報やプロモーション活動で情報発信するため、セキュリティ業界の動向やセキュリティ製品などについて学びはじめました。当時はJNSAの調査レポートや資料などをよく参考にさせていただきました。

デジタルアーツでは、主に広報を担当しておりますが、この7月からJNSAの活動に参加させていただいています。一方で、セキュリティ業界に身を置き始めて日が浅く、まだまだ勉強が足りないなと痛感しています。一日も早く、皆さんの会話についていけるよう、また有益な活動や情報提供ができるよう、知識や経験を身につけるべく、精進していきたいと思います。

プライベートでは、福岡県出身なのでソフトバンクホークスの野球観戦が趣味で、ホークスの試合が関東であると、暇を見つけては球場に足を運んでいます。ホークスファンの方がいらっしゃれば、是非お話ししましょう。

JNSAの皆さま、今後ともよろしくお願い申し上げます。

JNSA 会員特典

■会員の特典

1. 各種部会、ワーキンググループへの参加
2. 会員向け勉強会への参加
3. 活動報告書や成果物の会員限定情報の入手
4. 会員専用 Web やメーリングリストでの情報入手
5. 人脈拡大と相互交流
6. 教育受講やイベント参加時の会員割引（SANS、（ISC）^{2}）等
7. 製品・サービス紹介サイト（JNSA ソリューションガイド等）への情報登録
8. 理解度チェック・プレミアムの販売（代理店）
9. 調査研究プロジェクトへの参画
10. JNSA 会報誌の配布

お問い合せ

特定非営利活動法人
日本ネットワークセキュリティ協会　事務局
〒 105-0003 東京都港区西新橋 1-22-12 JC ビル 4F
TEL：03-3519-6440
TEL：03-3519-6441
E-Mail：sec@jnsa.org
URL：https://www.jnsa.org/

西日本支部
〒 532-0011 大阪府大阪市淀川区西中島 5-14-10
新大阪トヨタビル（株）ディアイティ内
TEL：　06-6886-5540

入会方法
　Web の入会申込フォームにて Web からお申し込み、または、書面の入会申込書を FAX・郵送にてお送り下さい。折り返し事務局より入会に関する御連絡をいたします。

JNSA Press vol.46

2018 年 9 月 30 日発行

発行所
特定非営利活動法人 日本ネットワークセキュリティ協会（JNSA）
E-Mail: sec@jnsa.org　　URL: https://www.jnsa.org/

印　刷
プリンテックス株式会社

NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

〒105-0003 東京都港区西新橋1-22-12 JCビル 4F
TEL 03-3519-6440　FAX 03-3519-6441
E-mail: sec@jnsa.org　URL: https://www.jnsa.org/

西日本支部
〒532-0011 大阪府大阪市淀川区西中島5-14-10 新大阪トヨタビル （株）ディアイティ内
TEL 06-6686-5540