JNSA PRESS
JAPAN NETWORK SECURITY ASSOCIATION
SPRING 2018 VOL.45

寄稿

要求中心的なOSINT手法と平昌オリンピックを狙った攻撃の解析例

02

IoTセキュリティとセキュリティ製品の動向

08

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

井の中の「ゆでガエル」にならないために
～ 目指せ圧力団体 ～

JNSA 理事
株式会社ベネッセインフォシェル
代表取締役社長　丸山　司郎

JNSAが活動を開始してから18年がたちました。

その間、生々流転、ネットワークセキュリティ、情報セキュリティ、サイバーセキュリティとその呼ばれ方も変遷し、ビジネス範囲は拡大発展を続けており、1月時点での会員数が213社と引き続き隆盛を誇っております。

なぜ、JNSAがこれだけの長い期間存続し続け、かつ成長出来ているのかを考えてみると

・情報セキュリティ業界が引き続き成長している
・下村事務局長のもつ「高い志」がぶれずに続いている
・時代や環境の変化に適応し組織形態を変化させてきている
・実社会に対する影響力があり、業界としての意思を実現できる立場にある

などが挙げられます。

改めて、JNSAらしさとは何か?を考えてみると、「ゆるい規律の中で、社会正義を前提とする情報セキュリティ活動を、利益や所属組織とは関係なく、企画して実行してみる場」と捉えております。その結果、設立の趣旨「ネットワーク･セキュリティの必要性を社会にアピールし、かつ、諸問題を解決していく」における、「必要性を社会にアピールする」については、ある程度その目的を達成できたと言えるのではないでしょうか。

そして、これからのJNSAを考えると、「人々の善意をそのまま成果に変えられる非営利組織」として、その目的を見直す時期に来たのかも知れません。

情報セキュリティにおける社会変革の強力な推進者として、政府と協力して政策転換を促し、市場の力を活用して情報セキュリティを担保することで、情報社会を健全に発展させること、つまりは、JNSA設立の当初に、山口英教授のおっしゃっていた「圧力団体」を目指す事を明確に意識するタイミングにが来たのではないでしょうか。

日本のセキュリティ業界が自己満足の対策で世界に取り残されないため、業界全体で変革させなければならない課題に以下のものがあると考えております。

・セキュリティ技術者が尻込みせず、最先端の攻撃手法を調査し対策を検討できる環境
・グローバルな競争環境の中で、我が国独自ルールによる産業発展の阻害要因の排除
・将来にわたって、国民、社会を守れる技術、人材、仕組みの構築
・情報セキュリティにおける、世界共通ルールの合意形成

これからのJNSAの活動によって、政府でもなく、企業でもない、非営利特定法人という立場でしかできない情報セキュリティに関する社会問題を、皆さんと一緒に解決していければ幸いです。

要求中心的なOSINT手法と平昌オリンピックを狙った攻撃の解析例

セコム株式会社 IS 研究所
稲垣　俊

1. はじめに

サイバー空間における攻撃者の優位性は、しばしば議論の対象となる。攻撃側は自由に攻撃対象を選べるだけでなく、防御側の出方を見つつ攻撃を進化させることができる。その一方で防御側はどのような攻撃を受けうるのかを想定し、限られたリソースで対策を決定しなくてはならない。この意思決定を支援するために公開情報を用いるという試みこそがOSINT（Open Source INTelligence）である。

本稿ではサイバーセキュリティにおける要求中心的なOSINT手法を紹介したのち、その一例として平昌オリンピックを狙った攻撃解析の結果の一部を示す。なお、今回は情報整理手法を示すことが主目的である。本来であれば含むべき、情報源および提供された情報の信憑性に関する議論にはあえて踏み込んでいないことに注意されたい。

2. サイバーセキュリティとインテリジェンス

「インテリジェンス」それ自体の普遍的な定義は確認されていない。ここでは、本稿で議論するインテリジェンスを定義するために、次のふたつのインテリジェンスに関する定義を参考にした。それらはインテリジェンスに関する小林の定義「政策決定者が国家安全保障上の問題に関して判断を行うために政策決定者に提供される、情報から分析・加工された知識のプロダクト、あるいはそうしたプロダクトを生産するプロセス」（小林良樹「インテリジェンスの基礎理論」）[1]、および脅威インテリジェンスに関するガートナーのMcMillanの定義「資産に対する既存あるいは今後現れうる脅威や危害に関する経験に基づく知見である」（Rob McMillan「Definition: Threat Intelligence」）[2]である。

> 本稿では「資産に向けられた脅威に対抗する意思決定者の要求に基づき、収集、処理、解析された情報であり、意思決定を支援する生産物および生産プロセス」を脅威インテリジェンスと呼ぶ。また、「オープンソースすなわち公開情報から法的かつ倫理的に入手できる情報を用いたインテリジェンス生産プロセス」を本稿ではOSINTとして扱う。

本定義では意思決定者がインテリジェンスの要求者であり、消費者であることを示している。サイバー攻撃に対する脅威インテリジェンスについても、意思決定者が誰であるか何を要求しているのかを明確にした要求中心的な脅威インテリジェンス生産を行わなければならない。

MWR InfoSecurityらが作成したフレームワークでは、インテリジェンス消費者という観点から脅威インテリジェンスを4種類に分類した[3]。それらは戦略（Strategic）脅威インテリジェンス、作戦（Operational）脅威インテリジェンス、戦術（Tactical）脅威インテリジェンス、技術（Technical）脅威インテリジェンスである。表1はそれぞれのインテリジェンスの概要を示している。インテリジェンスの消費者が異なるということは、彼らから要求されるインテリジェンスも異なる。したがって、インテリジェンス生産者は消費者に合わせてインテリジェンスを提供しなければならない。

この4種類の脅威インテリジェンスは先に本稿で定義した要求中心的な脅威インテリジェンスと相性が良いため、次節以降ではこれらに沿った形でインテリジ

表1　脅威インテリジェンスの分類

種類	消費者 / 要求者	概要
戦略脅威インテリジェンス	役員などの主要な意思決定者	組織の重要な意思決定に影響を与えうる情報
作戦脅威インテリジェンス	セキュリティ担当のマネージャなど	組織に対する攻撃情報（攻撃者像など）
戦術脅威インテリジェンス	セキュリティ担当者	攻撃者の手口
技術脅威インテリジェンス	アプライアンスなど	IP アドレスなどのデータ

ェンス例を紹介する。

3. インテリジェンスの準備

インテリジェンスは何らかの意思決定を支援する情報である。したがって、それを生産するためには要求が必要となる。本稿ではオリンピック関係組織の経営者が次のような状況に遭遇したことを仮定することにした。

> オリンピック開催にあたり、スポンサー/パートナー企業として大会を支えることとなった。近日中にサイバー攻撃対策の指針を立てるので、その判断材料が欲しい。

そして、この状況における各要求者の要求を仮定し、インテリジェンスを生産する。

なお、今回用いた情報収集手法はOSINTのみである。短期間で情報収集を行うことを仮定したため、情報収集期間は2018年2月21、22、23日および26日の4日間のみとした。また、今回は情報整理手法の一例を示すことが主目的であるため、情報源や提供された情報の信憑性に関する議論をあえて行っていないことに注意して欲しい。次節以降では戦略脅威インテリジェンスと戦術脅威インテリジェンスの一部を示す。また、戦術脅威インテリジェンスの一例として図1に開会式を狙った攻撃のタイムラインを示す。

4. 戦略脅威インテリジェンスの例

まずは経営者のような上層部の意思決定者を想定としたインテリジェンスについて記述する。

> **要求**
> 2020年のオリンピック開催にあたり、スポンサー/パートナー企業として大会を支えることとなった。それに先立ち、サイバー攻撃対策の指針を立てるために、その判断材料が欲しい。その参考として2018年の平昌オリンピックを対象にしたサイバー攻撃の情報をまとめ、その特徴について報告せよ。

4.1. 状況の要約

遅くとも2017年12月頃からオリンピック関係組織に対する攻撃が複数行われている[4, 5, 6]。そのうちの

図 1　平昌オリンピックの開会式を狙った攻撃のタイムライン

2018-02-09T19:15	メインプレスセンターの IPTV が遮断 [16, 17]
2018-02-09T19:15	接続障害が発生、その後 1 日以上続く [8, 18, 19]
2018-02-09T19:**	メインプレスセンターの IPTV が復旧 [17]
2018-02-09T19:**	組織委員会はネットワークからサーバを遮断 [16]
2018-02-09T19:**	上記対応に伴い公式 Web サイトの一部がアクセス不能 [16, 17]
2018-02-10T08:**	公式 Web サイトが復旧 [16, 8]
2018-02-10	オリンピックの報道官が障害はサイバー攻撃が原因であると発表 [7]
2018-02-12	Cisco の Talos が攻撃に用いられたと思しきマルウェアの解析結果を公表 [15]
2018-02-12	各種メディアがサイバー攻撃について報道
2018-02-12	Microsoft が攻撃に EternalRomance （ ER ）が用いられた可能性を示唆 [20, 21]
2018-02-12	Intezer がマルウェア解析に基づくアトリビューションの結果を公表 [13]
2018-02-13	ENDGAME がマルウェア解析結果を公表 [23]
2018-02-15	Talos の研究者がマルウェアから ER の PoC に類似する断片を発見 [22]
2018-02-15	三井物産セキュアディレクションがマルウェア解析結果を公表 [24]
2018-02-20	トレンドマイクロがマルウェア解析結果を公表 [25]
2018-02-24	ワシントンポストがアメリカ諜報機関の話として、ロシアの攻撃関与を示唆 [12]

ひとつはオリンピック開会式が行われた時間に会場の通信や公式サイト、チケットの発券機能などのサービスを利用不能に追い込んだ[7]。なお、競技の進行自体には影響がなく、12時間後に障害はほぼ復旧した[8]。

4.2. 国家規模の関与が疑われる攻撃

一部のメディアは今回の攻撃に国家規模の攻撃者が関与している可能性を報じている。しかしながら、ここで重要であるのはどの国が攻撃をしたのかということではなく、高度な攻撃が大規模に行われたということである。そのような攻撃に対して、一組織であらかじめ防御策を展開することは困難である。攻撃を防ぐよりもむしろ普通ではない状態に迅速に気付き、対処可能なシステムや人員を確保すべきだろう。それを踏まえた上で、様々なメディアが報じる攻撃者について収集した情報を記載する。

攻撃に北朝鮮またはロシアが関与している可能性を一部メディアが論じている。今回オリンピックが開催された韓国は北朝鮮の核開発を巡り、緊張状態が続いている。しかしながら、北朝鮮要人の訪韓や、統一チームの大会参加などで融和ムードとなっていること[9]を挙げ、北朝鮮が攻撃に関与している可能性が低いと見積もる見解もある[10]。

ロシアは組織的なドーピングを指摘され、今回のオリンピックに国家として参加することが認められなかった。そのロシアが国際反ドーピング協会に対して悪意を向ける可能性があるとして、攻撃者の候補に挙げている機関も存在する[10,11]。特に、ワシントンポストはアメリカ諜報機関が非公式に公表した内容として、ロシアが攻撃の背後にいると報道している[12]。また、技術的な分析からは中国が関与していると思しき攻撃に似た痕跡が確認されたとの報告もあった[13]。

4.3. 攻撃の起点となりうる関連企業

今回発生したインシデントのひとつは攻撃の起点がどこであるか未だ判明していないが、一部のメディアは攻撃を解析した結果からオリンピック運営関係企業が攻撃の起点になっている可能性があるとの見解を示している[14]。攻撃の痕跡に基づく推測のみから当該企業が攻撃の起点であると判断することは早計である。しかしながら、関連企業からイベントに対する攻撃が始まる可能性を承知し、それを踏まえて対策を検討することは防御者にとって有益であると考えたため、それを踏まえたインテリジェンスを以下に記載した。

当該企業に対する攻撃はオリンピック開催のひと月以上前から行われている可能性があり、その場合入念に準備が行われていたことが予想できる。国家規模の攻撃であれば、このようなことが起きた事例は珍しくない。なお、当該企業は現在大手セキュリティベンダと調査にあたっている最中であるため、詳細なコメントを避けている。

オリンピックのような大規模なイベントになれば関係者は爆発的に増加する。攻撃者が目的を達成させるためには、そのうちのセキュリティが最も弱い部分を狙うだけでよい。重要なことは自組織がそのような弱い部分になる可能性を考慮し、攻撃に素早く気づきそれを迅速に封じ込める耐性を作ることである。その封じ込めを適切に行うためには事前の準備が必要となるが、今回のオリンピックでは封じ込めに伴い、公式サイトが停止するという自体が発生した。そのようなことが起きないよう、あらかじめリスクを適切に評価した上で、問題を最小限に食い止める必要があるだろう。

4.4. 破壊が目的の攻撃

今回の攻撃のうちひとつは情報窃取よりも破壊を目的としている可能性が高い[15]。大規模なイベントや重要インフラなど稼働していること自体が大きな意味を持つシステムに対して、このような攻撃が行われることもある。そのことを認識せず、情報窃取の脅威を重視した対策のみを施した場合、本質的なリスクを低減させることは難しいだろう。

今回の場合、重要なことはインシデントから素早く立ち直り、業務を継続させることである。事前に分析やシステム構成の検討を行うのみならず、十分に訓練することも必要となる。机上訓練などを通して、どのような時に何をしなければならないのか、どこに何を伝えなければならないのかを把握しておくことで、円滑な問題解決を行うことができるようになるだろう。

5. 作戦脅威インテリジェンスの例

公開情報を対象に情報収集を行ったところ、主にふたつの攻撃に対する報告が寄せられていることがわかった。ひとつはフィッシングメールを用いた攻撃であり、もうひとつは開会式を狙った攻撃である。

複数のセキュリティベンダがそれぞれの攻撃について報告を行っている。したがって、それらは大規模に発生した攻撃または実害を引き起こした攻撃であることがわかる。以下では、各攻撃の攻撃者像についてまとめた内容を記述する。

> **要求**
> インテリジェンス要求者が守るべき組織（防御対象組織）を狙う攻撃者の目的、素性について判明する限りを報告せよ。これを基に、2020年のオリンピックにおいて防御対象組織が狙われる可能性があるか判断するために必要な情報を提供せよ。

5.1. フィッシングメールを用いた攻撃

2017年末から続く平昌オリンピックを狙ったフィッシング攻撃について、CrowdStrikeやMcAfeeが報告を行っている[4, 5, 6]。フィッシングメールを受信した者の多くはイベント関係者であり、その内容を分析すると韓国に狙いを定めたものであったことがわかった。フィッシングメールが韓国語で記載されていただけでなく、それを被害者に開かせるための「おとり」として鳥インフルエンザの話題が用いられていた。これは2017年末からオリンピック開催周辺地域で流行が懸念されていたものである。さらに、マルウェアが動作するためには韓国で広く用いられているワープロソフトが必要であった。また、攻撃が行われた時刻は韓国の国家テロ対策センターが訓練中であったことから、攻撃者は内部事情をよく把握している可能性があるようである。

今回の攻撃が何者によって、なぜ行われたかを特定することは困難であるが、攻撃対象に関する入念な調査が行われたうえで攻撃が行われていたことがわかる。必要に応じて攻撃者像を推定することは、防衛リソース振り分けの一助となるかもしれない。

5.2. 開会式を狙った攻撃

開会式を狙った攻撃はあるマルウェアによって引き起こされたものである可能性が高いとCiscoのTalos Intelligenceは報告している[15]。そして、そのマルウェア（Olympic Destroyer）は自己を複製しながら破壊を行う。マルウェアそれ自体には破壊機能が主に実装されていることから、今回の攻撃の目的は破壊であるとTalosは結論付けた。

Intezerは攻撃に用いられたマルウェアを解析した[13]。そして、その一部について、国家の関与が疑われている攻撃者が用いるコードとの類似性を報告している。なお、当該攻撃者は欧州、米国、日本の重要セクターを狙い、知財情報の窃取等を行っていたという報告が上がっている。

ソースコードの流出、バイナリの再利用、偽旗作戦など様々な可能性を考えられるものの、高度な攻撃の背景には国家規模の存在が絡んでいる可能性を否定できない。すなわち、単なる一般的なセキュリティ対策ではこのような攻撃を防ぎきれない可能性があることを心に留めなければならない。

6. おわりに

今回は紙面の都合上、戦術脅威インテリジェンスと技術脅威インテリジェンスを割愛するが、先に示した2種類のインテリジェンス同様にそれらも要求に応じて生産することが可能である。

特にイベントが発生したばかりの際には、様々なセキュリティベンダが各種インテリジェンスを発表し、それぞれの情報が更新され続ける。それらを効率よく表現するためには図1で示したようにイベントと記事の発行を時系列で表示するとよい。

なお、弊社では2017年に世界的に問題となったランサムウェアWannaCryに対しても公開情報とタイムラインを用いてインシデントの概要を把握する試みを実施した[26]。興味を持たれた読者はそちらも参照していただきたい。

参考文献

[1] 小林良樹（2014）「インテリジェンスの基礎理論」、立花書房
[2] Rob McMillan（2013）「Definition: Threat Intelligence」、<https://www.gartner.com/doc/2487216/definition-threat-intelligence>（参照2018-02-26）
[3] MWR InfoSecurity（2015）、「Threat Intelligence: Collecting, Analysing, Evaluatin」、<https://www.ncsc.gov.uk/content/files/protected_files/guidance_files/MWR_Threat_Intelligence_whitepaper-2015.pdf>
[4] Falcon Intelligence Team（2018）「Malicious Spear-Phishing Campaign Targets Upcoming Winter Olympics in South Korea」、CrowdStrike, Inc.、<https://www.crowdstrike.com/blog/malicious-spear-phishing-campaign-targets-upcoming-winter-olympics-in-south-korea/>（参照2018-02-26）
[5] Ryan Sherstobitoff et al.（2018）、「Malicious Document Targets Pyeongchang Olympics」、McAfee, LLC、<https://securingtomorrow.mcafee.com/mcafee-labs/malicious-document-targets-pyeongchang-olympics/>（参照2018-02-26）
[6] Ryan Sherstobitoff et al.（2018）、「Gold Dragon Widens Olympics Malware Attacks, Gains Permanent Presence on Victims' Systems」、McAfee, LLC、<https://securingtomorrow.mcafee.com/mcafee-labs/gold-dragon-widens-olympics-malware-attacks-gains-permanent-presence-on-victims-systems/>（参照2018-02-26）
[7] Sean Ingle(2018)「Winter Olympics was hit by cyber-attack, officials confirm」、The Guardian、<https://www.theguardian.com/sport/2018/feb/11/winter-olympics-was-hit-by-cyber-attack-officials-confirm>（参照2018-02-26）
[8] BBC（2018）「Winter Olympics hit by cyber-attack」<http://www.bbc.com/news/technology-43030673>（参照2018-02-26）
[9] Zeeshan Aleem（2018）「Hackers attacked the opening ceremony of the Winter Olympics. The question is who they were.」、VoxMedia、<https://www.vox.com/world/2018/2/12/17003444/winter-olympics-cyber-attacks-russia-north-korea>（参照2018-02-26）
[10] Doug Olenick（2018）「Russian actors mentioned as possibly launching cyberattack on 2018 Winter Olympic Games」、SC Media、<https://www.scmagazine.com/russian-actors-mentioned-as-possibly-launching-cyberattack-on-2018-winter-olympic-games/article/743835/>（参照2018-02-26）
[11] Feike Hacquebord、「Update on Pawn Storm: New Targets and Politically Motivated Campaigns」、Trend Micro Incorporated、<https://blog.trendmicro.com/trendlabs-security-intelligence/update-pawn-storm-new-targets-politically-motivated-campaigns/>（参照2018-02-26）
[12] Ellen Nakashima（2018）「Russian spies hacked the Olympics and tried to make it look like North Korea did it, U.S. officials say」、The Wasington Post、<https://www.washingtonpost.com/world/national-security/russian-spies-hacked-the-olympics-and-tried-to-make-it-look-like-north-korea-did-it-us-officials-say/2018/02/24/44b5468e-18f2-11e8-92c9-376b4fe57ff7_story.html>（参照2018-02-26）
[13] Jay Rosenberg（2018）「2018 Winter Cyber Olympics: Code Similarities with Cyber Attacks in Pyeongchang」、Intezer、<http://www.intezer.com/2018-winter-cyber-olympics-code-similarities-cyber-attacks-pyeongchang/>（参照2018-02-26）
[14] Chris Bing（2018）「Atos, IT provider for Winter Olympics, hacked months before Opening Ceremony cyberattack」、CyberScoop、<https://www.cyberscoop.com/atos-olympics-hack-olympic-destroyer-

malware-peyongchang/>（参照2018-02-26）
[15] Warren Mercer et al.（2018）、「Olympic Destroyer Takes Aim At Winter Olympics」、Cisco Systems, Inc.、<http://blog.talosintelligence.com/2018/02/olympic-destroyer.html>（参照2018-02-26）
[16] 김형열（2018）、「개회식 때 평창조직위 홈피 사이버 공격…10일 오전 복구『邦訳：開会式の時、平昌組織委員会ホームページサイバー攻撃…10日午前、復旧』」、SBS、<https://news.sbs.co.kr/news/endPage.do?news_id=N1004617403>（参照2018-02-26）
[17] 聯合ニュース（2018）、「[올림픽] IOC·평창조직위、사이버 공격 확인…안전 위해 세부내용 비공개『邦訳：[五輪]IOC・平昌組織委員会、サイバー攻撃確認…安全のために細部内容非公開』」、<http://www.yonhapnews.co.kr/bulletin/2018/02/11/\\0200000000AKR20180211032900007.HTML>（参照2018-02-26）
[18] NICOLE PERLROTH（2018）、「Cyberattack Caused Olympic Opening Ceremony Disruption」、The NewYork Times、<https://www.nytimes.com/2018/02/12/technology/winter-olympic-games-hack.html>（参照2018-02-26）
[19] Waqas Amir（2018）、「Cyber Attack Disrupts Winter Olympics Website During Opening Ceremony」、HACKREAD、<https://www.hackread.com/cyber-attack-disrupts-winter-olympics-website-opening-ceremony/>（参照2018-02-26）
[20] Windows Defender Security Intelligence(2018)、<https://twitter.com/WDSecurity/status/963308636276584448>（参照2018-02-26）
[21] Windows Defender Security Intelligence（2018）、<https://twitter.com/WDSecurity/status/963887214835859457>（参照2018-02-26）
[22] Paul Rascagnères（2018）、<https://twitter.com/r00tbsd/status/964055076590403584>（参照2018-02-26）
[23] Amanda Rousseau et al.（2018）、「Stopping Olympic Destroyer: New Process Injection Insights」、Endgame、<https://www.endgame.com/blog/technical-blog/stopping-olympic-destroyer-new-process-injection-insights>（参照2018-02-26）
[24] 吉川 孝志、菅原 圭（2018）、「Olympic Destroyerの内部構造を紐解く」、三井物産セキュアディレクション株式会社、<https://www.mbsd.jp/blog/20180215.html>（参照2018-02-26）
[25] 岡本 勝之（2018）、「平昌五輪開会式に影響を及ぼしたとされる不正プログラムを解析」、トレンドマイクロ株式会社、<http://blog.trendmicro.co.jp/archives/17023>（参照2018-02-26）
[26] 葛野 弘樹ら（2017）、「WannaCryを事例としたセキュリティレポートの分析」、情報処理学会、コンピュータセキュリティシンポジウム 2017

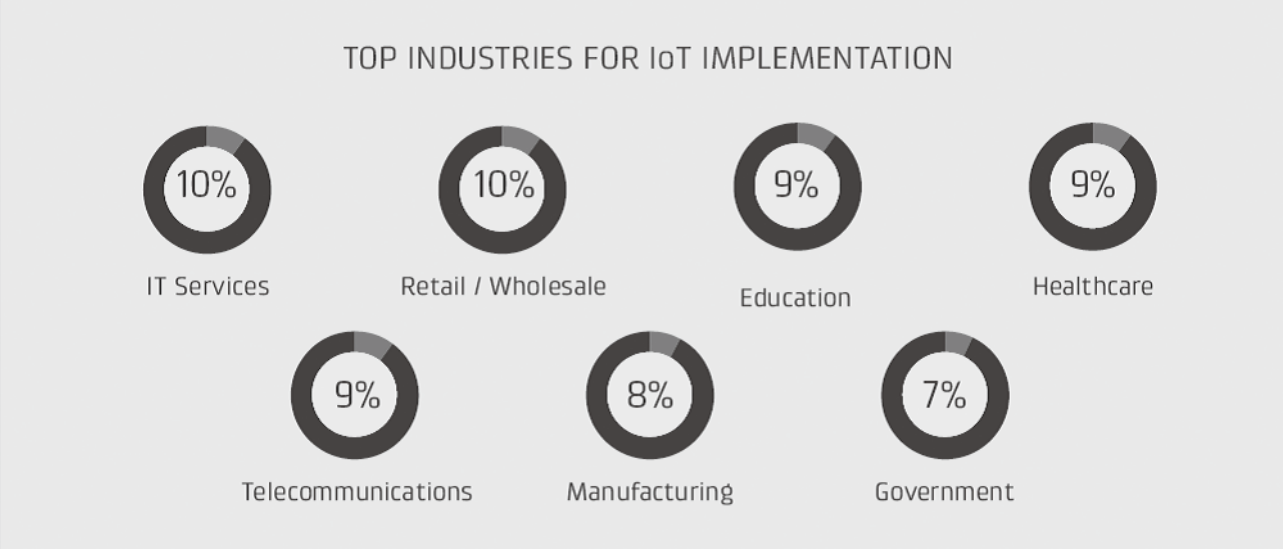
IoTセキュリティとセキュリティ製品の動向

Value Creation Frontier 代表
衣川　俊章

今回は、「最新米国サイバーセキュリティ事情」ということで、IoTセキュリティとセキュリティ製品の動向を書かせていただきたいと思います。ここで書かせていただいている情報は、筆者が米国でのカンファレンス・セミナーでの参加と、調査資料などをベースにまとめさせていただいております。

IoTセキュリティ

ある調査によると、IoT技術を何らかの形で利用している組織は32%、1年以内には導入しようと計画している組織まで含めると69%となっています。特に大企業で、かつ分散され広範囲でデバイスが存在し（例えば、電気メーターや自動車など）、かつそれがビジネスに不可欠な要素になっている組織での導入が進んでいるようです。



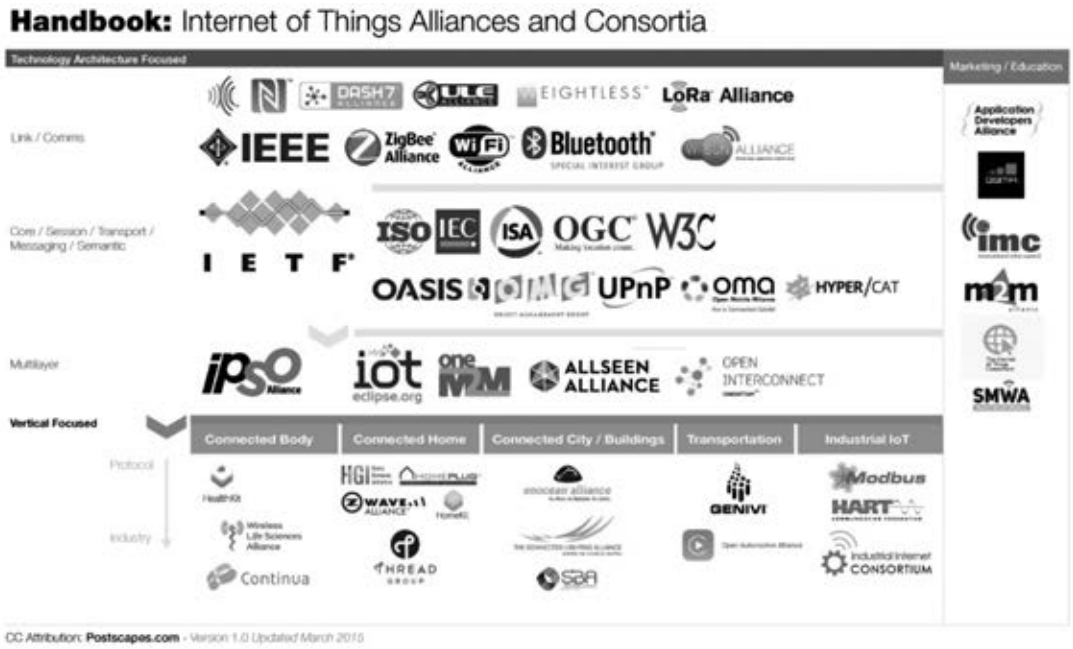
導入に際しての最大の懸念事項はセキュリティで、IoT特有のネットワークインフラの構築が必要であると言われています。

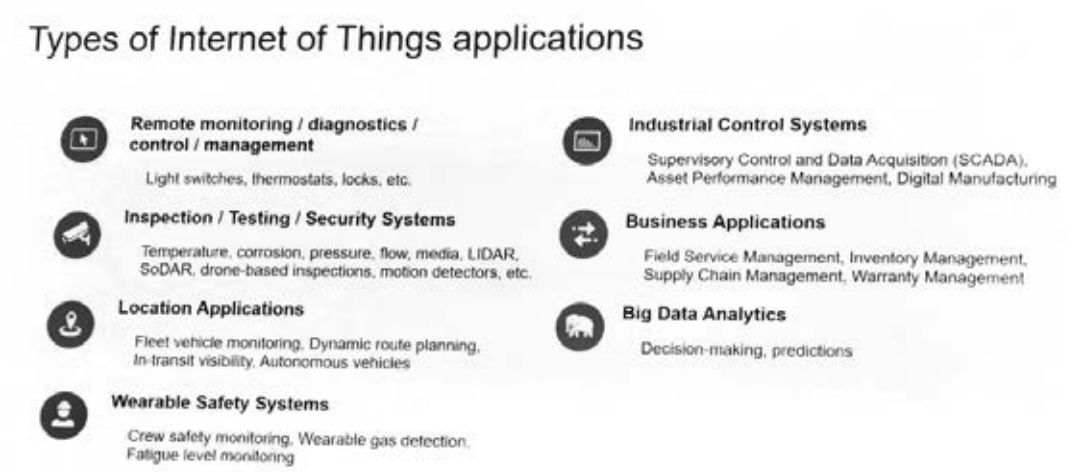
一方で、IoTにおける脅威としては、66%のIoTネットワークではセキュリティ違反が発生しており、DDoS通信のうち10%がIoTシステムを狙ったものであるとも言われています。残念ながら、IoTデバイスは70%が非暗号化ネットワークを利用し、50%では認証が弱く、結果66%では攻撃を許してしまっているという数字も出ています。

前述を踏まえ、セキュリティ対策に関しては、ネットワーク・エンドポイントモニタリングに関して注力しているベンダーが多くなって来ています。また、ネットワークアクセスにおいても、今までのインターネットではコネクションをまず優先し、その上での認証という考え方になっていますが、IoTネットワークでは、認証をまず実施し、その上でコネクションを許可するという発想に基づく構築が必要であると言われています。また、IoTネットワーク構築に際しては、論理・物理的に分離されたネットワークを考えるべきであるとも言われています。

ただ、IoTのそもそもの課題として、業界全体が混沌としている状況です。エッジデバイスは種類、数とも増加し続けており、それに呼応する為の複雑で細分化されたアプリケーション、多様なプロトコルや形態の存在、それらのコネクティビティの安全性を含めた確保も検討を進めていかなければいけない状況であります。それに関しての標

準やガイドラインがまだ充分に整備されていない（様々な団体などが設立されていて、整備への取り組みは始まっていますが）のも現状です。





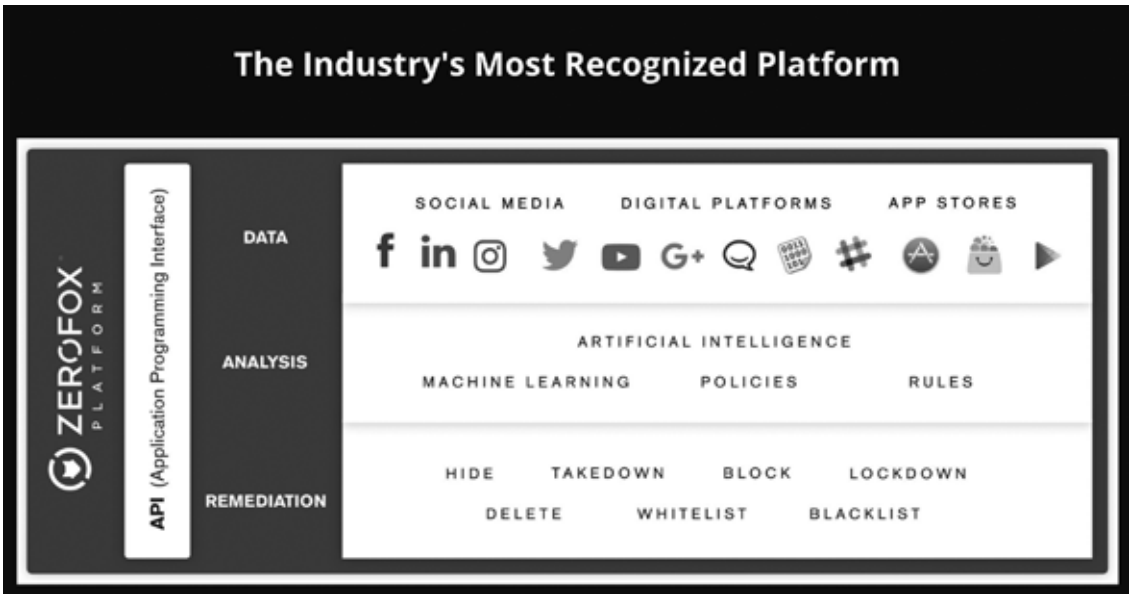
セキュリティという観点では、センサー・エンドポイントレベルでのビルトインをどこまでやれるかが課題とも言われています。昨今では、Raspberry Piなどの普及によって、低スペックエッジデバイスにおけるセキュリティビルトインが今までより加速していくのではとの予測があります。あとはリアルタイムでのネットワーク・デバイス運用管理も必要要素であると考えられています。

セキュリティ製品動向

一時期、セキュリティ製品がエンドポイント保護にシフトしていき始めた時期がありました。今でもエンドポイントセキュリティエリアへのベンダー進出、特にAI活用を売りとしているベンダーは継続しており、むしろ飽和状態かつ、製品毎の差別化が分かりづらくなってきているように感じられます。そこで、次世代IDSを中心としたネットワークレベルセキュリティの復活が見受けられるようになって来ています。更に、エンドポイントとネットワーク製品との連携をするケースが増えてきています。これによって差異化を図ったり、包括的なセキュリティ提供を図ることを各社が目指していることと考えられます。

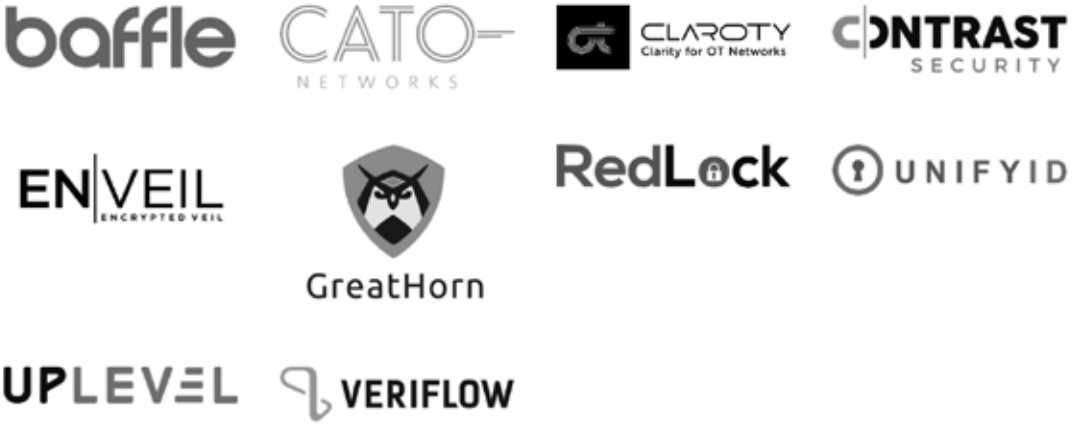
エンドポイントに限らずセキュリティ製品へのAI活用は引き続き継続しており、アンチフィッシングツール、ネットワーク検疫・分析製品、脆弱性検査ツール、面白い所では、ソシアルメディアモニタリングツールでの利用などが出てきています。

＊例：ソシアルメディアモニタリングツールーZeroFox



ただ、革新的なアイデアや技術活用での新製品が出てきていないのも現状です。この4月開催のRSAでのInnovation Sandbox表彰企業がどのようが技術なのかには、興味があります。

＊2017年Innovation Sandbox選出スタートアップ企業



直接製品動向とは直接関係ありませんが、スタートアップ企業関連の直近話題としては、2015年度のRSA Innovation Sandboxの最優秀企業であるインシデントレスポンスオーケストレーションのパイオニアであるPhantom CyberがSplunkに買収されました。もう一つの話題として、スタートアップ企業が米国政府案件に入り込むケースは中々見られませんでしたが、先日Cybereasonが米国政府セキュリティ評価標準・認証であるFedRAMP申請を始めたというニュースが入りました。この認証取得には10ヶ月、かつ1億円近い費用が掛かるのが、スタートアップ取得は進んでいなかった大きな理由でした。これに他のスタートアップが容易に追随するとは思えませんが、1社でもこの取組みを始めたことは、政府におけるセキュリティ対策にスタートアップの先進技術が活用される活路を開いたという意味で大きいと見られています。

参考文献：

1. Cradlepoint “State of IoT 2018” (https://cradlepoint.com/white-paper/state-iot-2018)
2. Postscapes IoT Alliance and Consortium (https://www.postscapes.com/internet-of-things-alliances-roundup/)
3. ZeroFoxホームページ (https://www.zerofox.com/platform/)
4. RSA Conference 2017 Innovation Sandbox (https://www.rsaconference.com/events/us17/agenda/innovation-sandbox-contest

JNSA ワーキンググループ紹介

JNSA 標準化部会・電子署名ワーキンググループ

電子署名 WG リーダー
三菱電機株式会社　宮崎　一哉

■ はじめに

2013年4月に標準化部会のもとに電子署名WGを立ち上げてから5年が経過しました。その当時の意気込みを思い出しながらこの5年で達成したこと、達成できなかったことを振り返るとともに、電子署名WGコアメンバの溢れる思いから派生的（噴出的?）に設立することとなった日本トラストテクノロジー協議会（JT2A）について紹介します。

■ これまでの活動について

電子署名WGは標準化部会に属する組織であり、その主要な目的は電子署名に関わる標準化です。標準原案作成タスクフォースが標準化を推進するタスクフォースです。この5年間で関わってきた標準のいくつかを表1に掲げます。標準化のためには国内外で開催される標準化会議に出席することはもちろん、電子署名の規格にはETSI/TC ESI(欧州電気通信標準化機構/電子署名基盤技術委員会) が大きな影響力を持っているため、電子署名WGではETSIの会員となり、欧州で開催される電子署名関連の会議に参加して必要な調整を行ってきました。

表1　標準化活動

組　織	規　格	概　要
ISO/TC 154	ISO 14533-3:2017 Processes, data elements and documents in commerce, industry and administration -- Long term signature profiles -- Part 3: Long term signature profiles for PDF Advanced Electronic Signatures (PAdES)	PAdES（PDF 長期署名）プロファイル規格を策定。発行済み。
ISO/TC 171	ISO 32000-2:2017 Document management -- Portable document format -- Part 2: PDF 2.0	PAdES 規格部分の策定に協力。 発行済み。
	ISO/CD 19005-4 Document management -- Electronic document file format for long-term preservation -- Part 4: Use of ISO 32000-2 (PDF/A-NEXT)	PDF/A-NEXT の長期署名規格部分の提案に協力。委員会原案段階。
ISO/IEC JTC 1/SC 34	ISO/IEC 26300:2015 Open Document Format for Office Applications (OpenDocument) v1.0	OpenDocument の長期署名規格部分の策定に協力。発行済み。
	ISO/IEC 29500 : Part 2: Open Packaging Conventions	Office Open XML の長期署名規格部分の提案に協力。改定準備中。
ISO/TC 215	ISO 17090-4:2014 Health informatics -- Public key infrastructure -- Part 4: Digital Signatures for healthcare documents	医療情報向けの電子署名プロファイル規格策定に協力。現在改定に協力中。

JAHIS（一般社団法人保健医療福祉情報システム工業会）	JAHIS ヘルスケア PKI を利用した医療文書に対する電子署名規格 Ver.1.1	医療情報向けの電子署名プロファイル規格策定に協力。現在改定に協力中。
	ヘルスケア PKI を利用した医療文書に対する電子署名規格 PAdES 編 Ver.1.0	医療情報向けの PAdES プロファイル規格策定に協力。
	JAHIS 電子処方せん実装ガイド Ver.1.0	電子処方せん向けの XAdES（XML 長期署名）プロファイル規格策定に協力。
JNSA	SHA-1 衝突の実現による電子署名への影響と対策	SHA-1 衝突の発見による電子署名への影響と対策につき、JNSA より公表。
TBF（タイムビジネス協議会）	電子署名検証ガイドライン	タイムビジネス協議会との共同作業により、電子署名の検証に関するガイドラインを作成。
TBC（タイムビジネス認定センター）	「SHA-1 衝突の実現」による時刻認証業務認定事業者が発行するタイムスタンプへの影響について	SHA-1 衝突の発見によるタイムスタンプへの影響に関する公表コメント作成に協力。
Cryptrec	「暗号技術ガイドライン」	暗号技術ガイドラインの SHA-1 の電子署名に関する部分の作成に協力。

また、JAHISやCryptrecなどの他団体からの要請に応じ、標準化に協力してきました。電子署名は決して新しい技術ではありませんが、近年の国際的かつ本格的な利用拡大により更に進化（深化）しており、標準化作業もまだしばらく続くことが予想されます。

電子署名WGは、電子署名関連の普及啓発も大きな目的の一つとしており、スキルアップタスクフォースがこれを担当しています。これまで、表2に掲げるような活動を行ってきました。電子署名やそのベースとなるPKIは実装・運用ともに複雑であり、暗号はもちろん、ソフトウェアだけでなくハードウェアの知識を要する場合もあるため、特に若手に対する啓発活動が極めて重要だと認識しています。先進技術に関する勉強会だけでなく、基礎的な技術についても勉強できるような機会を設けようと考えています。

表2　普及啓発活動

形　式	概　要
勉強会	JNSA 内外、国内外の専門家を招き、周辺技術も含む話題の技術の最新動向などの詳細を講義
PKI Day	PKI 相互運用技術 WG との共催で、PKI を様々な観点から捉え、有識者による講演会を実施
定例講演会	毎年春秋の 2 回、電子署名に関連したテーマを設けた基調講演と LT（ライトニングトーク）を実施
ハンズオン	PKI や電子署名のプログラムに実際に触れての基礎から最先端までの実習型の勉強会
ホームページ、フェイスブック	電子署名 WG 関連イベントの通知・紹介や、過去の講演資料等を公開
リンク集	電子署名に関わる主要な情報へのリンク集の提供（図 1）
合宿	定例会議ではできないような深い議論や周辺テーマについての議論をじっくりと実施

JNSA ワーキンググループ紹介

図1 電子署名関連リンク集（http://esig.jnsa.org/portal-search/）　※近日公開予定

■ JT2Aについて

デジタル社会が進展し、あらゆるモノやサービスが連携していく時代となりました。このような社会変革の中で、自身の組織やサービスに対するセキュリティの向上はもちろん、連携を前提とした接続先やデータに対するトラスト（信頼）の重要性が増大しています。電子署名は実在証明やデータ改ざん検知などのトラストを確立するための技術として電子署名WGでテーマアップしていますが、本人や機器等の認証技術や近年話題となっているブロックチェーン、EUのeIDAS規則で定義されたトラステッドリストなど、デジタル社会上でトラストを実現できそうな技術は電子署名に留まりません。電子署名を超えたより幅広い仕組みについて、セキュリティベンダーのみでなくユーザーを含めて利用面からも検討ができないか、との思いが複数のメンバの間に募った結果、新たな組織として日本トラストテクノロジー協議会（JT2A）を設立することとしました（図2）。

JT2Aは、この6月に開催されるJNSA2018年度総会での承認を受け、JNSA傘下にて正式に発足します（http://www.jnsa.org/aboutus/04.html の組織図をご覧ください）。代表として慶應義塾大学の手塚教授に、副代表としてセコム株式会社/PKI相互運用技術WGリーダーの松本様氏に就任頂きます。運営委員長には当協議会発足の第一の功労者であるみずほ情報総研株式会社/電子署名WGサブリーダーの小川氏が就任します。

図2　JT2Aホームページ（http://www.jt2a.org/）

■今後の活動について

電子署名WGでは、今後も標準化と普及啓発を軸に活動を続けていきます。表1に「電子署名検証ガイドライン」を掲げましたが、これは極めて重要で、標準規格にまで完成度を高める必要を感じています。電子署名フォーマットの標準に沿ったデータの生成はできても、それを正しく検証したり、検証結果を誤解の無いように表示したり、といった基準が曖昧では、それこそトラストを形成することはできません。現に検証プログラムによって検証の結果が異なるケースも見られます。ETSI/TC ESIでも2012年頃から規格化を進めているものの、まだフィックスできていないほど困難な作業ですが、2018年度は是非取り組もうと思います。このほか、既存の標準規格の見直しや情報提供のためのホームページや電子署名に参考となるツールの充実化にも取り組みます。

JT2Aでは、リモート署名ガイドラインの作成と「オンライン手続におけるリスク評価及び電子署名・認証ガイドライン」の改定を2018年度の目標とし、それぞれタスクフォースを設定して取り組むこととしています。前者はマイナンバーカードの有効活用や安全な電子契約サービスを提供することにつながりますし、後者は必要とするトラストを実現するために、どのようなレベルの電子署名や認証を実現する必要があるかの指針となります。

電子署名WG及びJT2AはJNSA会員であればどなたでも参加できます。JT2Aではユーザー企業向けの会員枠も設定予定です。ご興味を感じられた方は是非ご参加ください。

JNSA ワーキンググループ紹介

日本セキュリティオペレーション事業者協議会（ISOG-J）

日本電気株式会社
武智　洋

■ ISOG-Jについて

日本セキュリティオペレーション事業者協議会（Information Security Operation providers Group Japan 略称：ISOG-J）は、セキュリティオペレーション技術向上、オペレータ人材育成、および関係する組織・団体間の連携を推進することによって、セキュリティオペレーションサービスの普及とサービスレベルの向上を促し、安全で安心して利用できるIT環境実現に寄与することを目的として2008年に設立されました。

2018年2月時点でセキュリティオペレーションに関連する企業42社が参画し、複数のワーキンググループを構成しながら、特色のある活動を行っています。

■ 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　株式会社トライコーダ）

主に脆弱性診断のガイドライン作りや普及啓発のためのWGで、OWASP Japanとの共同WGである「脆弱性診断士スキルマッププロジェクト」としても活動しています。

脆弱性診断士のスキルマップや学びの指針となるシラバス、適切な診断実施のための「Webアプリケーション脆弱性診断ガイドライン」などを作成して公開しています。また、作成したガイドラインの普及のためにハンズオントレーニングも開催しています。

主な成果物：

■ Webアプリケーション脆弱性診断ガイドライン
http://isog-j.org/output/2017/WebAppPentestGuidelines.html

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

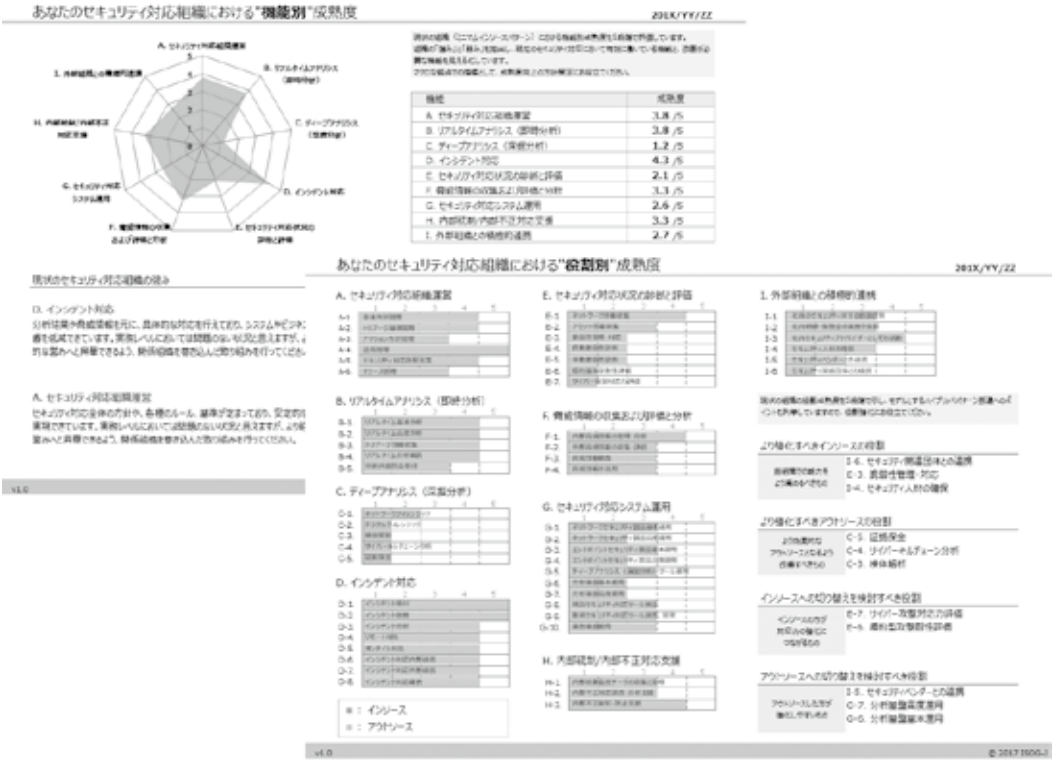
セキュリティオペレーション技術WG(WG2)は2008年6月のISOG-J発足当時からあるワーキンググループです。セキュリティオペレーションに関する技術全般を広く対象とし、参加組織が持ち回りで開催しています。セキュリティトレンドの紹介、現在進めている研究、SOC施設の見学、人材育成の方法などテーマは多岐にわたります。ISOG-J会員企業であればどなたでも参加できるようになっており、新規加盟企業最初の受け入れ窓口としても機能しています。そしてもちろん毎回のWGの後には懇親会がセットされており、日本のセキュリティオペレーションの未来を肴に熱い議論がいつも繰り広げられています。

■ 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　NTTセキュリティ・ジャパン株式会社）

本ワーキンググループはその名のとおり、セキュリティオペレーションの認知向上、普及啓発を目的に、他のWGと連携しながら、ISOG-Jから生み出された様々な成果を発信する役目を担っています。他のセキュリティ関連団体との連携や、イベントの企画などを通じて、日本におけるセキュリティオペレーションレベルの向上に寄与できるよう活動しています。

最近では「セキュリティ対応組織成熟度調査タスクフォース」を立ち上げ、国内におけるSOC/CSIRTの実態を明

らかにする活動も展開予定ですので、JNSA会員の皆様におかれましても、ご協力のほどどうぞよろしくお願いいたします。



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

セキュリティオペレーション連携WG(通称WG6)は2016年から活動をしています。

旬な課題について議論を行い、その成果で出せるものは公開してセキュリティ業界への貢献になればと活動をしています。これまでに「セキュリティ対応組織(SOC/CSIRT)の教科書」や「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」」をリリースしたり、InternetWeekや各所の勉強会などで発表を行ったりしています。

参加メンバーの熱量に支えられ、議論の内容はすべて公開できるものばかりではありません。これからも議論を続けようと、今日も夜の街へ繰り出すのでした。

JNSA ワーキンググループ紹介

主な成果物：

■ セキュリティ対応組織の教科書 v2.0
http://isog-j.org/output/2017/Textbook_soc-csirt_v2.html

■ 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」
http://isog-j.org/output/2017/5W1H-Cyber_Threat_Information_Sharing_v1.html

■ グローバル動静共有プロジェクト（リーダー：佳山　こうせつ　富士通株式会社）

セキュリティオペレーションに求められるニーズやモチベーションは日々ダイナミックに変遷しています。技術だけではカバーしきれない“動静”、特にグローバルでの変化にスコープを当て議論してきました。

1年という短期的なプロジェクトでしたが、各社のSOCが技術と動静をただしく紐付け時代の先手を打つため、グローバルな動静情報を持ち寄り断片的な情報から関連性を見出し共有する取り組みとしました。

このようなボランティアベースの活動による情報の共有が、前向きなセキュリティの活性化につながってくれれば嬉しいです。

主な成果物：

■ セキュリティ動静マップ 2017 年まとめ
http://isog-j.org/output/2018/2017_global_movement_mapping.html

■　今後の活動について

ISOG-Jでは今後も各ワーキンググループにおける活動を通じて、より多くのみなさまにお役立ていただけるような成果物の作成、講演会などのイベントを実施していく予定です。志を同じくして積極的に発信していける仲間を増やすべく、メンバー募集も行っておりますので、世の中に伝えたいことがある！という熱い思いを持ったセキュリティオペレーション関連事業者の方はぜひ参加をご検討いただければ幸いです。

■ 参加企業（2018年3月26日現在）

株式会社インターネットイニシアティブ	株式会社トライコーダ
SCSK株式会社	日商エレクトロニクス株式会社
NRIセキュアテクノロジーズ株式会社	日本アイ・ビー・エム株式会社
NECソリューションイノベータ株式会社	株式会社日本総合研究所
NECネクサソリューションズ株式会社	日本電気株式会社
エヌ・ティ・ティ・コミュニケーションズ株式会社	日本電信電話株式会社
NTTセキュリティ・ジャパン株式会社	日本ユニシス株式会社
株式会社エヌ・ティ・ティ・データ	ネットワンシステムズ株式会社
エヌ・ティ・ティ・データ先端技術株式会社	パーソルテクノロジースタッフ株式会社
NTTテクノクロス株式会社	株式会社PFU
株式会社Kaspersky Labs Japan	PwCサイバーサービス合同会社
グローバルセキュリティエキスパート株式会社（GSX）	株式会社日立システムズ
興安計装株式会社	富士通株式会社
株式会社神戸デジタル・ラボ	株式会社富士通ソーシアルサイエンスラボラトリ
サイボウズ株式会社	丸紅OKIネットソリューションズ株式会社
株式会社セキュアソフト	三井物産セキュアディレクション株式会社
SecureWorks Japan株式会社	三菱電機インフォメーションネットワーク株式会社
セコムトラストシステムズ株式会社	株式会社ユービーセキュア
ソフトバンク株式会社	ユニアデックス株式会社
ソフトバンク・テクノロジー株式会社	株式会社ラック
株式会社ディアイティ	株式会社リクルートテクノロジーズ

会員企業ご紹介㊺

SecureWorks Japan 株式会社

https://www.secureworks.jp/

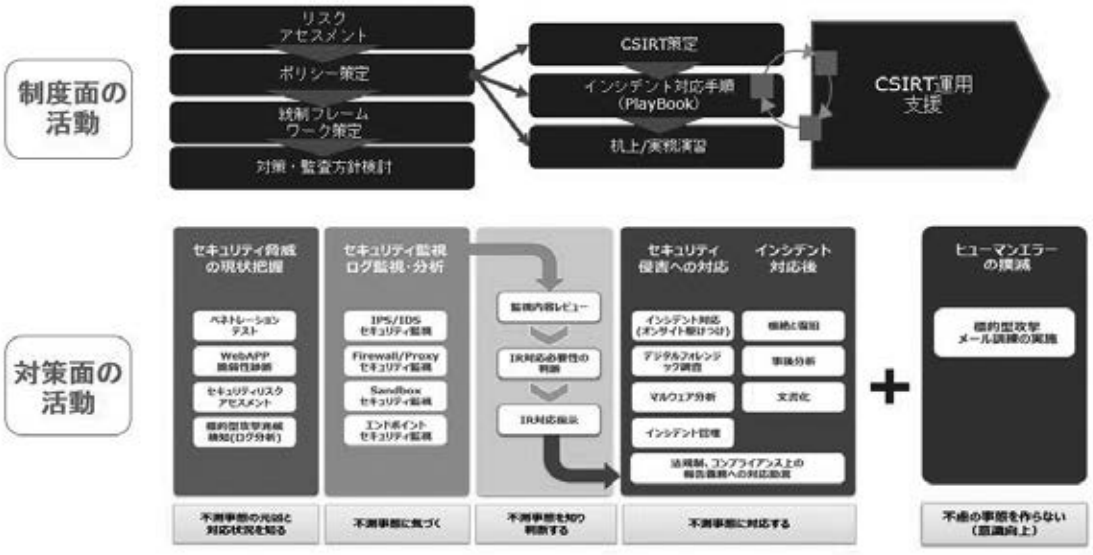
Dell Technologies グループの一員であるSecureworks は、機械学習を駆使して高度なデータ分析を行う、独自の解析エンジン「カウンター・スレット・プラットフォーム（CTP）」と、サイバー特殊部隊である「カウンター・スレット・ユニット（CTU）」のリサーチ結果を統合して導き出した実用的なインテリジェンスを用いて、サイバー上の脅威をリアルタイムに可視化、その対抗策をすべてのサービスに反映させて、現在世界55ヶ国、4,400社のお客様をご支援する総合セキュリティ対策サービスプロバイダーです。

グローバルにサービス展開するSecureworks

インターネットを介したサイバー攻撃に国境はなく、日々巧妙化・悪質化するサイバー攻撃に対して「早期警戒」を実現するためには最新かつ実践的なインテリジェンスが必要です。Secureworksは18年以上に亘り、2,500 億以上のセキュリティ・イベントを日々処理し、日本を含む世界5カ所のセキュリティ・オペレーション・センター(SOC)を通して24時間365日、常時休むことなくお客様のITインフラを監視し続けています。

セキュリティ・サービスに特化した当社が、これまでのセキュリティ投資の有効活用をご支援します

Secureworksは、リスク・アセスメント、CSIRT運用支援などの制度面だけでなく、セキュリティ・コンサルティング、脆弱性診断、24時間365日のセキュリティ監視、インシデント対応などの対策面まで網羅したエンドツーエンドのセキュリティ・サービスを提供し、お客様が「予測、防御、検出、そして対応」をテクノロジ、プロセス、そして人・組織において強化し、高度化するサイバー攻撃へのリスクを最小限に抑えることを実現します。



お問い合せ	SecureWorks Japan株式会社 E-mail : SCWX_PreSales@Secureworks.com 代表電話 : 03-6893-2317

ジェネシス・ジャパン株式会社

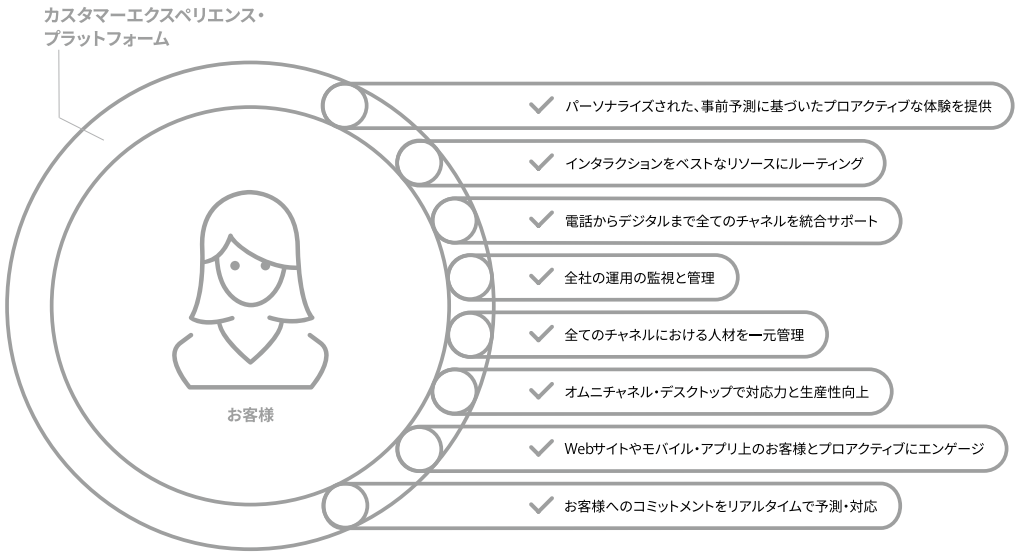
http://www.genesys.com/jp/

GENESYS™

お客様とのつながる瞬間（Moments Connected）を演出するジェネシス・ソリューション

ジェネシスは、1990年に設立された米国デイリーシティに本拠を置くコンタクトセンターおよびカスタマーエクスペリエンス・ソリューションのリーディング・カンパニーです。 世界100カ国10,000社以上で導入されているCustomer Experience Platformは、毎年250億件以上のお客様と企業とのインタラクションの価値を最大化し、ビジネスの成果と永続的な関係構築を支えています。

ジェネシスのソリューションがお客様にもたらす価値



ジェネシスが提供する３つのカスタマーエクエスペリエンス・プラットフォーム

Genesys Customer Experience Platformは、企業戦略に沿って顧客接点を管理し、パーソナライズされたカスタマーエクスペリエンスを提供するための統合プラットフォームです。デジタルからリアルまで全てのコンタクト・チャネルの統合、カスタマージャーニーの可視化、サービスに関わるワークフォース管理やプロセスの最適化を実現します。ジェネシスでは、企業規模やオンプレミス/クラウドなどの導入形態など、お客様のニーズに合わせて導入いただけるよう、３種類のCustomer Experience Platformを提供しています。

PureCloud

クラウド・ベースのカスタマーエクスペリエンス・プラトフォーム。クラウドの特性を活かし、柔軟かつ迅速に機能を強化。ユーザー自らでビジネスの変化に合わせて運用をコントロールし、常に最適な顧客体験を提供します。

PureConnect

コンタクトセンターからデジタルまですべてのコンタクト・チャネルを管理するとともに、IVR、通話録音、レポーティング、WFMなどカスタマーサービスに必要な機能をオール・インで提供するカスタマーエクスペリエンス・プラトフォーム。

PureEngage

リアルからデジタルまで真のオムニチャネル・エンゲージメントを実現するCXプラットフォーム。グローバルな導入、堅牢性とスケーラビリティ、企業ニーズに沿ったカスタマイズなど、企業戦略に沿った顧客体験を演出します。

問い合わせ先	ジェネシス・ジャパン株式会社 マーケティング本部 〒169-0074 東京都新宿区北新宿2-21-1 新宿フロントタワー14階 Eメール:marketingjapan@genesys.com　電話：03-5989-1430

富士ソフト株式会社

https://www.fsi.co.jp/

FUJISOFT

富士ソフト株式会社は、1970年創立の独立系ITソリューションベンダーです。自動車、FA・OA、家電（AV機器）等に関連する組込み系ソフトウェアの開発や、金融、製造、流通、文教分野等における業務系システムの構築を行っています。昨今では、当社が有するノウハウ、プロダクト、有力ベンダーとの協業により、AI、IoT、セキュリティ、クラウド、ロボットテクノロジー、モバイルや自動車分野での新技術を活かした付加価値の高いシステムインテグレーションサービスの提供に取組んでいます。高齢者福祉施設など多彩なシーンで利用いただいているコミュニケーションロボット「PALRO」をはじめとするロボット技術、モバイルを活用したペーパーレス会議やテレワークなどシームレスに仕事ができる環境づくりを提案しています。

富士ソフトのセキュリティサービスの特長

1．特定メーカーのサービス／ソリューションに固執せず、お客様に最適なご提案が可能
→独立系ベンダーの強み

2．システムにとらわれないリスク低減策の実施が可能
→業務系／組込み系開発で国内最大規模の技術者集団（連結:13,500人）

3．専門家によるセキュリティトータルサービスを実現
→70名以上の情報処理安全確保支援士とネットワーク／データベーススペシャリストが多数在籍

手間のかかるリスク分析と対策を富士ソフトが多角的に支援

富士ソフトが対策に必要な個所を見える化し、対策スケジュール作成のため、予算化に対するアプローチの手間を大幅に削減。

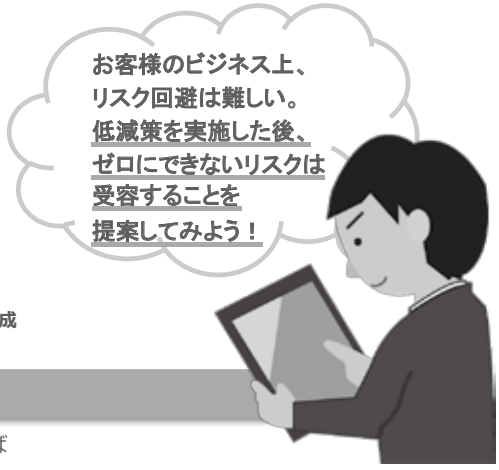
有償調査/検査/対策計画支援

1.セキュリティ調査/診断

Webサイト目視診断/Webアプリケーション脆弱性診断/OSS脆弱性診断/
モバイルアプリ脆弱性診断/サーバ脆弱性診断/プラットフォーム脆弱性診断/
クラウドサービス脆弱性診断

2.セキュリティコンサルティング

リスク対策プランニング支援/ポリシー作成支援/インシデント対応マニュアル作成支援/SOC-CSIRT構築支援/セキュリティ監査実施/個人情報保護法対策支援



無償簡易診断サービス

問診形式「**セキュリティ対策状況簡易診断**」簡単な質問に答えて頂ければ
当社の専門家が対策状況を採点、今後の対策をアドバイスします。

富士ソフトが提供するセキュリティソリューション一覧

●調査／診断
- セキュリティリスク診断
- Webサイト脆弱性
- ネットワーク脆弱性
- サーバ脆弱性
- PC／モバイルリスク診断

●運用／監視
- 運用／保守
- インシデント監視（SOC）

●対策／構築支援
<NW・IT>
- セキュリティ設計
- ソリューション／サービス選定支援
- ソリューション／サービス導入支援
- ソリューション／サービスチューニング支援

<組込>
- セキュリティ設計
- セキュア製造
- セキュア検査保証

●インシデント対応
- 初動対応
- インシデント対応
- 事態収拾支援
- 再発防止支援
- セキュリティ構築／運用／保守／監視とセットのインシデント総合補償

●教育／訓練支援
- 社員向け「情報セキュリティ教育」（e-learning）
- 経営者向け「情報セキュリティセミナー」
- Webサイト運営管理者向け教育支援
- Webサイトセキュアコーディング教育支援
- 標的型攻撃メール訓練
- インシデント対応訓練支援（CSIRT）

お問い合せ

富士ソフト株式会社
〒231-8008　神奈川県横浜市中区桜木町1-1　TEL：050-3000-2100
営業本部クラウド＆ソリューション事業部ソリューション営業部 セキュリティ営業グループ
Email：sec-info@fsi.co.jp

JNSA 会員企業のサービス・製品・イベント情報

■サービス紹介■

○R-ISAP　情報セキュリティ研修

いつも研修サービスにご愛顧頂き有難うございます。
リコージャパン　研修事務局です。
私たちはPMS、ISMS/クラウドセキュリティの審査員研修や情報セキュリティ監査人研修等を定期的に開催しています。企業内の運営事務局担当者等にも有益な資格になります。
※JIS Q 15001 改定差分研修を開始しました。詳細は下記URLより確認して、お申込ください。

【サービス情報詳細】
http://www.ricoh.co.jp/sales/solutions/training/index.html

◆お問い合わせ先◆
リコージャパン株式会社
リコー情報セキュリティ研究センター
TEL: 0120-165-340
E-mail: inquiry_training@ricoh-japan.co.jp

■製品紹介■

○AIの学習機能が未知のマルウェアを防御「Cylance PROTECT」

メトロが扱うCylancePROTECTは、日々誕生する亜種を含む新たなマルウェアの脅威をAIの学習機能を用いて予測検知します。2017年5月頃より世界中で被害が報じられているWannaCry等と呼ばれるマルウェアに対しても、CylancePROTECTはマルウェアが生まれる前から検知が可能であった事が確認されています。サポート期限切れOSやスタンドアロンの端末でも変わらずご利用いただけます。

【製品情報詳細】
http://www.metro.co.jp/products/security/cylance/

◆お問い合わせ先◆
株式会社メトロ
TEL: 03-5484-1022
E-mail: sol-sales@metro.co.jp

○インターネット分離ソリューション - SCVX

【インターネット分離ソリューションが実現する安全性】
SCVX（自社開発）では、コンテナ技術を活用したネットワーク分離によって安全性を確保。
万一、Webブラウジングにて悪意あるソフトウェアがダウンロードされてしまった場合でもその影響を 最小限に留め、ローカル端末側の環境を確実に守ります。
同製品は地方自治体向けに幅以広い導入実績を誇り、2017年4月までに約80団体もの自治体様に採用頂きました。今年度においては教育委員会・金融市場をターゲットとして展開を進めております。

【製品情報詳細】http://jscom.jp/scvx/
動画サイト：http://jscom.jp/scvx/

◆お問い合わせ先◆
ジェイズ・コミュニケーション株式会社
営業本部東日本営業部第2グループ
氏名：吉岡洋希（よしおか　ひろき）
連絡先：yoshioka@jscom.co.jp
TEL: 03-6222-5858

○犯罪捜査の視点でサイバーセキュリティの経営課題を見える化C3(シーキューブ)

従来のパターンファイルやシグネチャではなく、サイバー犯罪捜査のノウハウを利用して解析を行う『C-Audit』は、エージェントレスで環境を選ばず、組織内のセキュリティ対策の有効性や妥当性を可視化します。
加えて、従業員の意識能力を図る『CVT』、NISTのサイバーセキュリティフレームワークを使った『CREATe』を組み合わせ、リスクマネジメントに必要な「人・プロセス・IT」の3つの軸で組織全体のセキュリティ対策の現状を可視化します。

【サービス情報詳細】https://www.ni3.co.jp/c3

◆お問い合わせ先◆
株式会社NIインテリジェントイニシアティブ
営業部 TEL: 0120-165-340
E-mail: info@ni3.co.jp

イベント開催の報告

Network Security Forum 2018

2018年1月24日（水）、東京・ベルサール神保町にてJNSA主催シンポジウム「Network Security Forum 2018」が開催されました。サイバーセキュリティ戦略本部、総務省、経済産業省、独立行政法人 情報処理推進機構のご後援のもと、当日はのべ267名の参加者をお迎えし、盛況のうちに開催されました。

本セミナーでは、情報セキュリティ分野における時事に即したトピックについての講演、JNSAの部会、WG活動におけるテーマを中心にセッションを展開しました。

基調講演として総務省谷脇康彦審議官をお招きし、ご講演いただきました。また特別対談として、WHITE MOTION代表である蔵本雄一氏とJ-Auto-ISACメンバーによる、昨今話題となっている自動車のIoTに関する対談を実施いたしました。午後からは二つのトラックに分かれ、JNSAの各活動成果に関連した講演、「ベンダー各社が予測する、2018年の脅威」と題して、脅威予測を発表されている複数のベンダーによる2018年想定される脅威の動向やその対応についてのパネルディスカッションも行いました。

各講演の資料（一部を除く）はJNSAのWebサイトで公開していますのでぜひご覧下さい。
http://www.jnsa.org/seminar/nsf/2018/pro.html

NSF2018　基調講演の様子

Network Security Forum 2018 〈プログラム〉

トラック１（Ｒｏｏｍ１＋２）

【Ｓ１ 基調講演】10：00 ～ 10：50〈50 分〉

データ主導社会とサイバーセキュリティ

総務省　政策統括官　谷脇 康彦 氏

＝＝＝　10：50 ～ 11：00　休憩　＝＝＝

【Ｓ２ 特別対談】11：00 ～ 12：00〈60 分〉

自動車産業が歩む「セキュリティ」と「セーフティ」の道

合同会社 WHITE MOTION　最高経営責任者（CEO）　蔵本 雄一 氏

J-Auto-ISAC　井上 弘敏 氏（本田技研工業株式会社）

山﨑 雅史 氏（マツダ株式会社）

中島 一樹 氏（トヨタ自動車株式会社）

＝＝＝　12：00 ～ 13：00　昼休み　＝＝＝

トラック１（Ｒｏｏｍ４＋５）

【Ａ１】13：00 ～ 14：00〈60 分〉

内部不正 WG 招致講演「人間の意思決定の神話と現実」

長瀬 勝彦 氏（首都大学東京 教授）

＝＝＝　14：00 ～ 14：10　休憩　＝＝＝

【Ａ２】14：10 ～ 14：50〈40 分〉

効果的なゲーム教育のための Tips

長谷川 長一 氏（株式会社ラック/ゲーム教育 WG リーダー）

＝＝＝　14：50 ～ 15：00　休憩　＝＝＝

【Ａ３】15：00 ～ 16：00〈60 分〉

サイバーセキュリティ・IoT・トラストについて
～日本トラストテクノロジー協議会発足～

1. **サイバーセキュリティに求められるトラストと JT2A の活動**
   手塚 悟 氏（慶應義塾大学大学院政策・メディア研究科特任教授/JT2A 代表）
2. **IoT に求められるトラストと JT2A の活動**
   松本 泰 氏（セコム株式会社 IS 研究所/PKI 相互運用技術 WG リーダー/JT2A 副代表）
3. **日本トラストテクノロジー協議会の概要**
   小川 博久 氏（電子署名 WG サブリーダー/リモート署名 TF リーダー/JT2A 運営委員長）

＝＝＝　16：00 ～ 16：10　休憩　＝＝＝

トラック２（Ｒｏｏｍ１＋２）

【Ｂ１】13：00 ～ 13：40〈40 分〉

セキュリティ対応組織力を上げるコツ
～成熟度の可視化と、情報共有の心得～

阿部 慎司 氏

（NTT セキュリティ・ジャパン株式会社/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）

【Ｂ２】13：40 ～ 14：10〈30 分〉

IoT セキュリティ早引きガイド解説

松岡 正人 氏

（株式会社カスペルスキー/IoT セキュリティ WG リーダー）

＝＝＝　14：10 ～ 14：20　休憩　＝＝＝

【Ｂ３ミニシンポジウム】14：20 ～ 15：50〈90 分〉

「社会活動部会で勝手に予測する、どうなる 2018 年のセキュリティ」

司会：丸山 司郎 氏（株式会社ベネッセインフォシェル/社会活動部会長）

コメンテーター：

鵜飼 裕司 氏（株式会社 FFRI 代表取締役社長）

下村 正洋 氏（株式会社ディアイティ 取締役会長）

西本 逸郎 氏（株式会社ラック 代表取締役社長）

丸山 満彦 氏（デロイト トーマツ リスクサービス株式会社 代表取締役社長）

15:50 トラック１＝＝＝ 終了 ＝＝＝

トラック１（Ｒｏｏｍ４＋５）

【Ｂ４パネルディスカッション】16：10 ～ 18：00〈110 分〉

「セキュリティプロフェッショナル誕生秘話」～高度セキュリティ人材の育成方法はあるのか～

モデレーター：与儀 大輔 氏（NRI セキュアテクノロジーズ株式会社）

パネリスト：新井 悠 氏（トレンドマイクロ株式会社）

岩井 博樹 氏（デロイト トーマツ サイバーセキュリティ先端研究所）

辻 伸弘 氏（ソフトバンク・テクノロジー株式会社）

寺島 崇幸 氏（株式会社ディアイティ/SECCON 副実行委員長）

JNSA 賀詞交歓会・JNSA 賞表彰式のご報告

賀詞交歓会

恒例のJNSA賀詞交歓会は、2018年1月24日（水）、東京・ベルサール神保町にて開催されました。約150名の方にご参加いただき、大変盛況な会となりました。

冒頭、JNSA副会長の中尾 康二氏より開会の挨拶を申し上げ、来賓としてお招きした内閣官房内閣サイバーセキュリティセンター副センター長の内閣審議官　三角 育生氏、総務省政策統括官（情報セキュリティ担当）谷脇 康彦氏、経済産業省大臣官房 サイバーセキュリティ・情報化審議官　伊東　寛氏よりご挨拶をいただき、独立行政法人情報処理推進機構 理事長 富田達夫氏による乾杯のご発声のもと、開宴しました。

JNSA 賞　表彰式

歓談の後、今回で12回目を迎えた毎年恒例のJNSA賞の表彰式が執り行われました。各賞の受賞者をご紹介後、中尾副会長から表彰状と記念の盾、副賞が授与されました。

受賞者と受賞理由は以下の通りです。受賞者の皆様、おめでとうございました。

個人の部（2件）

◇ トラストセキュリティ関連技術普及の組織立ち上げに尽力し、JNSAの活性化に大きく貢献

○ 小川 博久 氏（電子署名WG/リモート署名TFリーダー／みずほ情報総研株式会社）

2016年度のJNSA電子署名WGの活動において、WGメンバに加え、電子認証局会議、タイムビジネス協議会、JIPDEC等の団体メンバをとりまとめてリモート署名調査研究に係る報告書を作成したことに引き続き、2017年度には電子署名WG/リモート署名TFのリーダーとして、各団体、省庁を巻き込んで検討を進めることでリモート署名ガイドラインを策定した。また、将来のトラストセキュリティ関連技術を検討･標準化･普及するための組織「日本トラストテクノロジー協議会（JT2A）」の立上げに尽力し、セキュリティITベンダのみでなくユーザ企業の会員取り込みのための仕掛けを創出することなどによって、JNSAの知名度向上や活動の活性化に対して極めて大きな貢献があった。

◇ 海外進出支援を進めるとともに海外での活動活性化に尽力し、JNSAの知名度向上に大きく貢献

○ 一宮 隆祐 氏（海外市場開拓WGリーダー／日本電気株式会社）

JNSA海外市場開拓WGリーダーとして、WG運営に尽力した。今年度7月にシンガポールで開催された展示会「INTERPOL World 2017」では、ジェトロの支援を受けて実施したJapan Pavilionにて JNSAブースのサポートやレセプションパーティの運営などに尽力し、多数の記事に取り上げられるなど大きな成果を上げた。同年11月のアブダビ視察団では団長を務め、各訪問先との現地打合せの陣頭指揮をとり、今後のUAEへの進出に関して有益な情報を得ることに貢献した。

また、サブWGでは、これから海外進出を検討する中小企業等にとって非常に有益な情報となる海外進出マニュアルの作成を進めており、JNSAの活動の活性化と知名度の向上に大きく貢献した。

ワーキンググループ（WG）の部（1件）

◇ 情報セキュリティ教育を波及させ、JNSAの社会貢献と知名度向上に大きく貢献

○ 教育部会 ゲーム教育WG（WGリーダー：株式会社ラック　長谷川 長一 氏）

アナログゲームというこれまでJNSAにて注目されていなかった媒体、「セキュ狼」カードゲームと「マルコン」ボードゲームを成果物として完成させ、これまでアプローチできていなかったITの知識をほとんどもっていない層、特に若年層に対しJNSAに対する興味関心を吸引するきっかけをつくりだした。

また、これら成果物を活用した活動による実証実験を繰り返し実施することで、ファシリテーター育成が行われ、ゲーム教育WGによる主催ではない、草の根活動として同WGの成果物を使用したゲーム教育イベントが全国各地で開催されている。

これら一連の活動は、WGが掲げている「ゲーム」の力を活用し、情報セキュリティ教育を波及させるとの目的達成にむけ大きく貢献するとともに、JNSAの知名度向上や活動の活性化に多大の貢献を果たしている。

JNSA 賞受賞者の皆さん

イベント開催の報告

「クロスボーダー時代におけるアイデンティティ管理セミナー」を開催

JNSA 標準化部会　アイデンティティ管理WGリーダー
日本電気株式会社　宮川　晃一

JNSA アイデンティティ管理WGが主催する、「クロスボーダー時代のアイデンティティ管理セミナー」がINFORIUM豊洲イノベーションセンターにて行われました。

当日は80名ほどの聴衆の中、デジタルアイデンティティの幅広いテーマについて、各種セッションが繰り広げられました。

■ 日　　時：2018年1月26日（金）14：00～18：30
■ 場　　所：NTTデータショールーム INFORIUM
■ 主　　催：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）
　　標準化部会　アイデンティティ管理WG
■ 協　　力：株式会社NTTデータ
■ 講演資料：http://www.jnsa.org/seminar/2018/0126/

【概　要】

「アイデンティティ管理WG」ではこれまでのWG活動の成果を広く知っていただくため、不定期に独自のセミナーを開催しています。

今年度は「クロスボーダー時代におけるアイデンティティ管理」をテーマに開催いたしました。
近年、働き方や企業/個人、国、業界など様々なものが変化して、その境界（ボーダー）があいまいになる中で、ワークライフバランス、セキュリティ、コンプライアンスを確保する上でアイデンティティがなすべき役割が大きくなってきています。

このような時代に求められるアイデンティティ管理について、各セッションを通して幅広い内容を発表いたしました。

以下、セッション毎に実施した概要を簡単にご報告いたします。

【A-1】（開会のご挨拶）「クロスボーダー時代のID管理とは」
宮川 晃一 氏（日本電気株式会社／アイデンティティ管理WGリーダー）

最初に開会のご挨拶から始まり、WGの今までの活動をご紹介いたしました。次にクロスボーダー時代の意味を解説し、通常「クロスボーダー」と言う言葉は「国際間」と言う意味で使われることが多いがネットワークや個人／企業、人／モノと言った関係性も含めたものと説明しました。その中でどのようにアイデンティティを管理すべきかと言うことが本日のセミナーの主旨となっていることを解説いたしました。

【A-2】（講演）「コンシューマIDのエンタープライズ領域での活用」
富士榮 尚寛 氏（伊藤忠テクノソリューションズ株式会社 西日本システム技術第2部 部長代行）

通常、FacebookやTwitter 等のコンシューマのIDをエンタープライズに適用して、利用することは考えにくいことですが、ユーザの利便性を考慮すると今後はBYOIDと言った発想になるのは必然的かもしれません。本セッションの中ではエンタープライズIDの求められる保障レベルについて整理し、コンシューマのIDの適用シナリオをLINEを例に解説いただきました。

【B-2】「GDPRをきっかけに考えるグローバルなアイデンティティ管理」

北野 晴人 氏（デロイトトーマツリスクサービス パートナー）

本年5月25日からGDPR(EUデータ保護指令・一般データ保護規則)が施行されることからグローバル関連企業は各種対応に追われている状況があります。

その中において、グローバル化に必要な個人データ（人）に対するガバナンスの考え方を解説いただき、アイデンティティ管理は統合をめざすITの中でセキュリティの要となり、かつ合理化、コスト削減、コンプライアンスなどに有用な基盤となるとご説明をいただきました。

【A-3】「クロスボーダー時代におけるデジタルアイデンティティの活用、及びそのセルフコントロールとトラストの両立実現に向けて 」

桑田 雅彦 氏（日本電気株式会社 IoT基盤開発本部 ソフトウェアアドバンストテクノロジスト（サイバーセキュリティ））

個人のデジタルアイデンティティ情報（個人データ）は様々な形に加工され利用用途も様々になってきています。クロスボーダーな時代において、それがどこに向かっているのかを最初に解説いただき、個人のデジタルアイデンティティ情報の結合・融合・分離に係るメリット・デメリットをご説明いただきました。

その上で、その解題に対する一つの解決策を提示いただき、活用の仕組みについての提言をいただきました。

【B-3】「クロスボーダー時代の認証技術と海外･国内の動向」

八束 啓文 氏（EMCジャパン株式会社RSAシステムズ・エンジニアリング部 部長）

木村 優一 氏（ジェムアルト株式会社 IDP事業部 ディレクター OEM & グローバルパートナー）

佐藤 公理 氏（エントラストジャパン株式会社シニアテクニカルセールスコンサルタント CISSP/CISA/CISM）

最初にクロスボーダー時代におけるユーザ認証の重要性について解説をいただき、OTPやPKI、生体認証のトレンドについて解説いただきました。また、講演各社における多要素の事例についてご説明いただきました。コロンビア政府（金融機関）やNASAジェット推進研究所の事例などとても興味深い事例でした。

イベント開催の報告

【A-4】「ソーシャル名寄せの恐怖 ～あなたの情報、知らないうちにこんなことに～ 」
星野 亮 氏（株式会社NTTデータ セキュリティ技術部 課長）

最初に「名寄せ」の意味について解説いただき、よい意味合いと悪い意味合いがあることを整理していただきました。次に「SPOKEO」と言う個人情報の検索サービスの紹介がありました。SNSの公開情報や電話帳などから名前やメールアドレス、電話番号や住所などが検索できるものです。

発表者自身が実際に有償サービスに申し込んで生々しいリアルな体験を発表していただき、個人のデジタルアイデンティティ情報がいかに拡散しているかを感じ取ることができました。また、拡散させないためにはどうしたらよいかと言うことを解説いただきました。

【B-4】「ブロックチェーンが実現する（かもしれない）未来のIDとID管理基盤の姿」
貞弘 崇行 氏（株式会社アイピーキューブ ITコンサルタント）

今後未来のアイデンティティ管理基盤として、ブロックチェーン技術を利用した「Self-Sovereign Identity（SSID）」について解説をいただきました。

ブロックチェーンと言うと、通常はビットコインをはじめとする仮想通貨を連想しがちですが、非金融分野での活用方法の1つとして大変興味深い事例かと思います。

SSIDが今後どのような広がりをみせるのか今後もWGではウォッチしていきたいと思います。

【A-5】（特別講演）「改正個人情報保護法･GDPRとID情報」
湯淺 墾道 氏（情報セキュリティ大学院大学学長補佐/教授）

特別講演として、湯浅先生より個人情報保護法の改正ポイントとGDPRについて解説いただきました。その後、アイデンティティ情報が漏えいした場合の対応や報告義務および罰則など、諸外国を例にご説明いただき今後日本がどのような方向に向かうのかをご説明いただきました。大変参考になりました。

【A-6】（パネルディスカッション）

「エキスパートがばっちり予測！クロスボーダー時代に求められるアイデンティティ管理とは」

※モデレーター：山田 達司氏（株式会社エヌ・ティ・ティ・データ¦シニアスペシャリスト（セキュリティプリンシパル））
※パネリスト：　工藤 達雄氏　（NRIセキュアテクノロジーズ株式会社｜上級ソリューション・アーキテクト）
下道 高志氏（日本オラクル株式会社｜ソリューションディレクター　工学博士, CISA, CISM）
中島　浩光氏（株式会社マインド・トゥー・アクション｜代表取締役）
富士榮 尚寛氏（伊藤忠テクノソリューションズ株式会社｜部長代行）

最後のセッションとして、アイデンティティ業界では知らない人はいないと言われるメンバーでパネルディスカッションを行いました。最初にモデレーターの山田さんから本パネルの主旨についてご説明いただきました。

次に工藤さんからは今後のID管理に係る取り組みとして「同意管理」「関係性管理」「自己主権型アイデンティティ管理（SSID）」について解説がありました。下道さんからは認証とアイデンティティの関係性について説明があり、特に「SAML認証」と言われることの気持ち悪さのご説明が印象的でした。中島さんからは「ももいろクローバーZ」の応援衣装での登場に度肝を抜かれましたが、認可の説明する題材として「ももいろクローバーZ」のファンクラブサイトを例にわかりやすく解説をいただきました。山田さんからはパネリストからのお話をもとに、今回の「クロスボーダー時代のID管理」について必要な技術や法規制などエンタープライズの視点からパネラーにするどい質問していただき、白熱した討論となりました。

【本セミナーと通して】

今回はテーマが広かったこともあり、内容が多岐に渡りましたが今後のアイデンティティ管理の課題や向かう方向性については少し道筋が見えてきた気がしました。

本セミナーで収集したアンケート結果も満足度が高いものがありましたので今後も不定期ではありますがWG主体の公開セミナーは企画していきたいと思います。

なお、本セミナーの開催にあたりご協力をいただきました皆様に厚く御礼を申し上げます。

セミナー終了後の懇親会は「ファミリーマート」づくしと言うことで「おでん台」をまるごとお借りして盛大に開催されました。予算も安く済みますのでお勧めです。

2017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年度より独立行政法人情報処理推進機構（IPA）が運営主体となり、JNSAが事務局を運営しています。

【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、啓発チラシや家庭向けリーフレット「みんなで守って安全・安心8か条」「親子で守って安全・安心10か条」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

安全教室_2017年度開催実績

（2018年3月10日）

	日　程	開催地	共催団体	会　場
1	2017年4月13日	福岡県	NPOスキルアップサービス	田ノ浦市民センター
2	2017年5月9日	兵庫県	JNSA	兵庫県立リハビリテーション中央病院研修ホール
3	2017年5月13日	岐阜県	インターネット安全教室レディースチーム	垂井町立垂井小学校
4	2017年5月15日	兵庫県	JNSA	兵庫県立リハビリテーション中央病院研修ホール
5	2017年5月19日	北海道	北海道情報セキュリティ勉強会	北海道知内高等学校 体育館
6	2017年5月23日	栃木県	NPO栃木県シニアセンター	栃木県シルバー大学南校
7	2017年5月24日	東京都	JNSA	東京都立両国高等学校
8	2017年5月26日	神奈川県	NPO情報セキュリティフォーラム	愛川町中津公民館　1階　会議室
9	2017年5月27日	岐阜県	JNSA	ハートフルスクエアG　大研修室(岐阜市消費生活センター)
10	2017年6月12日	三重県	NPO東海インターネット協議会	玉城中学校　体育館
11	2017年6月24日	福島県	特定非営利活動法人日本コンピュータ振興協会	福島市立福島第二小学校
12	2017年7月1日	熊本県	NPO　NEXT熊本	嘉島町立嘉島中学校
13	2017年7月2日	鹿児島県	NPO鹿児島インファーメーション	鹿児島市立西陵中学校 体育館
14	2017年7月3日	佐賀県	長崎県立大学	佐賀県立神埼高等学校
15	2017年7月5日	福島県	特定非営利活動法人日本コンピュータ振興協会	桑折町立伊達崎小学校
16	2017年7月6日	鹿児島県	NPO鹿児島インファーメーション	学校法人神村学園　アリーナ
17	2017年7月7日	徳島県	公益財団法人　e−とくしま推進財団	徳島市立津田小学校
18	2017年7月9日	栃木県	NPO法人栃木県シニアセンター	小山市生涯学習センター
19	2017年7月10日	徳島県	公益財団法人　e−とくしま推進財団	神山町立神山中学校
20	2017年7月11日	徳島県	公益財団法人　e−とくしま推進財団	鳴門市明神小学校
21	2017年7月13日	徳島県	公益財団法人　e−とくしま推進財団	那賀町相生中学校
22	2017年7月14日	東京都	JNSA	中野区立南台小学校
23	2017年7月18日	東京都	JNSA	中野区立南台小学校
24	2017年7月14日	徳島県	公益財団法人　e−とくしま推進財団	阿南市羽ノ浦小学校
25	2017年7月18日	福岡県	NPOスキルアップサービス	北九州市立年長者研修大学校 穴生学舎 2階　第2研修室
26	2017年7月18日	徳島県	公益財団法人　e−とくしま推進財団	徳島市立方上小学校
27	2017年7月19日	徳島県	公益財団法人　e−とくしま推進財団	阿波市市場小学校
28	2017年7月23日	北海道	北海道情報セキュリティ勉強会	富良野文化会館2階
29	2017年7月31日	埼玉県	埼玉県県民生活部青少年課【新規】	浦和コミュニティセンター　第15集会室
30	2017年8月18日	滋賀県	NPO滋賀県情報基盤協議会	多賀町中央公民館
31	2017年8月23日	大阪府	NPO法人きんきうぇぶ	富田林市立人権文化センター
32	2017年8月25日	滋賀県	NPO滋賀県情報基盤協議会	草津市立志津小学校
33	2017年9月2日	岩手県	盛岡情報ビジネス専門学校【新規】	盛岡情報ビジネス専門学校　306教室
34	2017年9月8日	福島県	JNSA	いわき明星大学

	日　程	開催地	共催団体	会　場
35	2017年9月8日	栃木県	JNSA	金田南中学校体育館
36	2017年9月14日	佐賀県	NPO法人シニアネット佐賀	佐賀市兵庫公民館
37	2017年9月23日	三重県	PCシエル	長島総合自動車学校
38	2017年9月29日	佐賀県	NPO法人シニアネット佐賀	江北町ネイブル
39	2017年10月2日	群馬県	JNSA	みどり市商工会館
40	2017年10月4日	福岡県	NPOスキルアップサービス	北九州市立年長者研修大学校 穴生学舎 2階　第2研修室"
41	2017年10月5日	鳥取県	特定非営利活動法人こども未来ネットワーク【新規】	とりぎん文化会館 第2会議室
42	2017年10月6日	佐賀県	NPO法人シニアネット佐賀	佐賀市アバンセ
43	2017年10月24日	佐賀県	NPO法人シニアネット佐賀	唐津市都市コミュニティセンター
44	2017年11月6日	広島県	福山市	内浦公民館
45	2017年11月7日	神奈川県	NPO情報セキュリティフォーラム	ヴェルクよこすか　6階　第1会議室
46	2017年11月8日	広島県	福山市	常石公民館
47	2017年11月8日	神奈川県	NPO情報セキュリティフォーラム	おだわら市民交流センターUMECO 会議室5・6
48	2017年11月11日	宮城県	特定非営利活動法人地域情報モラルネットワーク	東北工業大学一番町ロビー2F
49	2017年11月13日	秋田県	JNSA/秋田県立大学	秋田県立大学　本荘キャンパス
50	2017年11月14日	秋田県	JNSA/秋田県立大学	秋田県立大学　秋田キャンパス
51	2017年11月16日	徳島県	公益財団法人e-とくしま推進財団	吉野川市学島小学校
52	2017年11月18日	奈良県	なら情報セキュリティ総合研究所	帝塚山大学　東生駒キャンパス　1号館
53	2017年11月19日	奈良県	なら情報セキュリティ総合研究所	帝塚山大学　東生駒キャンパス　1号館
54	2017年11月22日	滋賀県	NPO滋賀県情報基盤協議会	多賀町立多賀小学校 体育館
55	2017年11月23日	北海道	Enywhere	恵庭市市民会館
56	2017年11月25日	山形県	酒田市教育委員会【新規】	東北公益文科大学　酒田キャンパス　公益ホール
57	2017年11月29日	広島県	福山市	幕山公民館
58	2017年12月3日	北海道	旭川情報産業事業協同組合	旭川市科学館
59	2017年12月6日	島根県	益田市学校警察連絡協議会【新規】	益田警察署
60	2017年12月8日	佐賀県	NPO法人シニアネット佐賀	佐賀市嘉瀬公民館
61	2017年12月9日	福岡県	NPOスキルアップサービス	北九州市立大学北方キャンパス本館 D-503教室
62	2017年12月9日	鹿児島県	NPO鹿児島インファーメーション	いちき串木野市市民文化センター
63	2017年12月12日	福岡県	NPOスキルアップサービス	北九州市立年長者研修大学校 穴生学舎 2階　第2研修室
64	2017年12月13日	広島県	福山市	引野公民館
65	2017年12月14日	栃木県	NPO栃木県シニアセンター	栃木県シルバー大学校南校
66	2017年12月15日	徳島県	公益財団法人e-とくしま推進財団	上浦小学校
67	2017年12月17日	北海道	北海道情報セキュリティ勉強会	森町公民館
68	2017年12月19日	広島県	福山市	網引公民館

	日　程	開催地	共催団体	会　場
69	2017年12月19日	神奈川県	JNSA	第三管区海上保安本部
70	2017年12月20日	北海道	くるくるネット	室蘭市立天沢小学校
71	2017年12月21日	佐賀県	NPO法人シニアネット佐賀	伊万里市ケーブルテレビジョン2F
72	2018年1月11日	三重県	くわなPCネット	桑名市総合福祉会館
73	2018年1月17日	佐賀県	NPO法人シニアネット佐賀	佐賀市本庄公民館
74	2018年1月22日	佐賀県	NPO法人シニアネット佐賀	武雄市文化会館
75	2017年1月24日	北海道	Enywhere	恵庭市柏小学校
76	2018年1月28日	愛知県	NPO東海インターネット協議会	ナディアパーク
77	2018年1月31日	佐賀県	NPO法人シニアネット佐賀	伊万里市ケーブルテレビジョン2F
78	2018年2月1日	栃木県	NPO栃木県シニアセンター	栃木県シルバー大学校南校
79	2018年2月6日	広島県	福山市	西公民館
80	2018年2月9日	佐賀県	NPO法人シニアネット佐賀	佐賀市高木背公民館
81	2018年2月9日	大阪府	大阪市保健所南西部生活衛生監視事務所	
82	2018年2月10日	山口県	いわくに市民活動支援センター	NPO法人岩国パソコンの会
83	2018年2月16日	広島県	福山市	川口公民館
84	2018年2月16日	宮城県	特定非営利活動法人地域情報モラルネットワーク	東北生活文化大学
85	2018年2月16日	神奈川県	NPO情報セキュリティフォーラム	葉山町福祉文化会館　大ホール
86	2018年2月16日	和歌山県	NPO情報セキュリティ研究所	印南町立清流小学校
87	2018年2月17日	福岡県	公益財団法人 ハイパーネットワーク社会研究所	上毛町中央公民館
88	2018年2月20日	大阪府	NPO法人きんきうぇぶ	富田林市立人権文化センター
89	2018年3月3日	長崎県	長崎県立大学	長崎県立大学シーボルト校
90	2018年2月28日	佐賀県	NPO法人シニアネット佐賀	唐津ケーブルテレビジョン　会議室
91	2018年2月28日	鹿児島県	与論情報化グループ e−○k	与論町立与論中学校

SECURITY CONTEST (SECCON) 2017

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。

2017年12月に行われたSECCONオンライン予選では、102ヵ国から累計4,347人が参加し決勝大会への出場枠をかけた戦いが繰り広げられました。2017年度の決勝大会は国内決勝と国際決勝に分かれて開催され、国内決勝大会の優勝はチームTokyoWesternsで彼らには文部科学大臣賞が授与、国際決勝の優勝は昨年に引き続き韓国のチームCykorで彼らには経済産業大臣賞が授与されました。

また、決勝大会と同時にカンファレンス、ワークショップ、展示などを同会場で行い、のべ600名を超える参加者がありました。

【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
- 外務省（2017年8月1日以降の開催大会に後援）
- 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
- OWASP Japan
- 日本シーサート協議会

[SECCON Beginners とは]

SECCON Beginners 2017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）の初心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: info2017@seccon.jp）
2017年度スポンサー企業はSECCONホームページ（http://2017.seccon.jp/）をご覧下さい。

■SECCON2017 開催スケジュール

日　　程	開催大会	会　　場	競技内容
2017年12月9日~10日	SECCON 2017オンライン予選	インターネット	CTF予選(日本語+英語)
2018年2月17日	SECCON 2017 決勝大会	東京電機大学	国内決勝大会
2018年2月18日~19日		東京電機大学	国際決勝大会

※SECCON決勝大会には、オンライン予選で入賞したチーム以外に、国内・海外のCTF大会等の招待枠があります。

■SECCON Beginners 2017 開催スケジュール

回	日　　程	開催大会	会　　場	演習内容
1	2017年5月27日	SECCON Beginners 2017 長野	株式会社電算	Binary, Forensic (Network), Web,CTF予定
2	2017年6月24日	SECCON Beginners 2017 盛岡	盛岡情報ビジネス専門学校	
3	2017年7月1日	SECCON Beginners 2017 名古屋	株式会社中電シーティーアイ	
4	2017年8月26日	SECCON Beginners 2017 広島	広島県情報プラザ	
5	2017年9月23日	SECCON Beginners 2017 仙台	東北大学片平キャンパス	
6	2017年10月7日	SECCON Beginners 2017 東京	東京都立産業技術高等専門学校	
7	2017年11月18日	SECCON Beginners 2017 鹿児島	鹿児島キャリアデザイン専門学校	
8	2017年12月2日	SECCON Beginners 2017 長崎	長崎県立大学	

■CTF for GIRLS 開催スケジュール

回	日　　程	開催大会	会　　場	演習内容
1	2017年6月16日	第7回ワークショップ	株式会社インターネットイニシアティブ	ネットワーク
2	2017年8月19日	学生対象ワークショップ	株式会社富士通ラーニングメディア	暗号・Web
3	2017年12月15日	第8回ワークショップ	株式会社富士通ラーニングメディア	フォレンジック

※SECCON BeginnersとCTF for GIRLSにはSECCON決勝大会への出場枠はありません。

【2018年度のSECCON展開】

初心者向けCTF大会（オンライン、オフライン）の実施をはじめ、より多くの人にCTFに興味をもってもらう活動を継続していきます。

SECCON Begnnersについては、初心者向けに限らず、中級者以上向けのワークショップとして各地での実施を検討しています。

SECCON
スポンサー募集中！
https:2017.seccon.jp/

SECCON2017メールマガジン登録
CTFに興味を持っている人・SECCON参加者や参加検討中の方々を対象にメールマガジンを発行しています。2017年度のメールマガジン登録を希望する方はこちらからご登録をお願いします。
https://frm.f2ff.jp/form/seccon_ml/
（SECCON2017運営事務局ナノオプト・メディアのサイトです）

後援・協賛イベントのお知らせ

1. 自治体総合フェア2018
主　催： 一般社団法人日本経営協会
日　程： 2018年5月16日（水）～18日（金）
会　場： 東京ビッグサイト

2. 第22回サイバー犯罪に関する白浜シンポジウム
主　催： 和歌山県、和歌山県警、白浜町、
情報システムコントロール協会大阪支部（ISACA）、
和歌山大学、近畿大学生物理工学部、
NPO情報セキュリティ研究所
日　程： 2018年5月24日（木）～26日（土）
会　場： 和歌山県立情報交流センターBig・U

3. ガートナー セキュリティ&リスク・マネジメント サミット 2018
主　催： ガートナージャパン株式会社
日　程： 2018年7月24日（火）～26日（木）
会　場： 八芳園

4. CEBIT 2018
主　催： Deutsche Messe AG
日　程： 2018年6月11日（月）～ 15日（金）
会　場： ドイツ・ハノーバー国際見本市会場

5. CEBIT ASEAN Thailand 2018
主　催： IMPACT
日　程： 2018年10月18日（木）～20日（土）
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）

6. Gartner Symposium/ITxpo 2018
主　催： ガートナージャパン株式会社
日　程： 2018年11月12日（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

◆ ガートナー セキュリティ& リスク・マネジメント サミット 2018 ◆

Gartner Summits

今日のデジタル・ビジネスのスピードとスケールに追いつくためには、今直ぐに準備を開始する必要があります。世界中のCISOとセキュリティ／リスク管理のエグゼクティブ・リーダーが一堂に会する本サミットにおいて、どのようにリーダーシップ能力を研鑽し、いかに世界的に高まっているセキュリティ・リスク問題に対してセキュアなデジタル・ビジネスを実現していけばよいのかについて提言を行います。

【参加メリット】
- 国内外のアナリストが最新の分析、事例、実践すべきプラクティスを提言
- 個別の課題について相談できるアナリストとの個別ミーティング
- アナリストや参加者同士のネットワーク構築の機会

【会　　期】2018年7月24日（火）～26日（木）
【会　　場】八芳園
【参加料金】
2018年6月12日（火）まで
→早期割引価格 120,000円（1名様・税別）
2018年6月13日（水）以降
→通常価格 136,000円（1名様・税別）
※グループ特別割引：
同時に4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
⇒ http://www.gartner.co.jp/event/srm/

JNSA部会・WG2017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

日本社会のサイバーセキュリティへの適応を推進す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、パブコメ対応や行政との意見交換会、ワークショップ、勉強会や記者懇談会などの普及啓発活動、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・他団体連携などを進める。

【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。

【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ソリューションの拡販を実現する。

- APAC地域における統治代理店の開拓、商談発掘から受注までの実績を作る
- 作成途中の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「海外市場進出マニュアル」を纏める。

＜予定成果物＞

- 海外進出マニュアル

【CISO支援WG】

（リーダー（仮）:高橋正和 氏／
株式会社Preferred Networks）

CISOになったばかりの方がどのような活動をしていけばよいのかの指針をもち、実際に行動していくことができるように、サポートできる情報を提供する。

＜予定成果物＞

- CISOハンドブック

【JNSA CERC】

（リーダー：高橋正和 氏／
株式会社Preferred Networks）

会員間でのインシデント情報共有のための仕組みを充実させるとともに、流通するコンテンツの拡充を図る。

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、まずは被害報告（報道や報告書）の標準化を検討する。

＜予定成果物＞

- 2015/2016年個人情報漏えいインシデント調査報告書
- 被害報告（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:木城武康 氏／株式会社日立システムズ）

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。

＜予定成果物＞

- 2017年度情報セキュリティ市場調査報告書

【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）

以下の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。2017年度は、昨年度に引き続き、特に(1)に重点をおいた活動を行う。

(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

＜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記事の公開
- 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）

国内外の各組織団体が提供をはじめたIoTセキュリティのガイドをまとめたレポートの作成と、2016年度に公開したガイドの使い方講座の提供によるIoTセキュリティの整理と啓発活動「IoTセキュリティガイド、ワークショップ・セミナー」を開催する。

＜予定成果物＞

- セキュリティガイドの更新

【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）

複数のバックグラウンドと知見を持った人を集めた意見交換会を通じて、サイバー分野における真の脅威と業界の構図を見極め、問題に沿った解決策をガイドする。

【マイナンバー対応情報セキュリティ検討WG】

（リーダー:萩原健太 氏／トレンドマイクロ株式会社）

マイナンバー関連の意見提出の取りまとめや定期的に勉強会を開催する。

※2017年9月活動終了

3. 標準化部会

部会長：中尾康二 氏／ＫＤＤＩ株式会社
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、議論を進めることとしたい。

【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。

【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）

アイデンティティ管理の必要性の啓発および導入指針の提示などによる普及促進、関連他団体との連携により市場活性化を目的とした活動を行う。

＜成果物目的テーマ＞

- ID管理システム導入のためのチェックリスト（6月にチェックリスト公開予定）
- IDの融合と分離（6月にレポート公開予定）
- 若手技術者向け教育コンテンツの作成と勉強会（セミナー）の開催（新規）

＜勉強目的テーマ＞

- IoTにおける認証・アクセス制御連携
- EU規則の動向勉強会
- プライバシー関連の動向勉強会

＜予定成果物＞

- ＩＤ管理システム導入のためのチェックリスト
- ＩＤの融合と分離（研究レポート）
- 若手技術者向け「ＩＤ管理技術の基礎」

【国際化活動バックアップWG】

（リーダー:中尾康二 氏／KDDI株式会社）

国際標準化活動の情報共有を継続的に実施する。

韓国KISIAとの共同フォーラム（7月に韓国にて）の開催を行い、韓国セキュリティベンダーグループとの連携を強化する。さらに、ＩｏＴセキュリティに関する国際標準化（経済産業省主体）を視野に入れたＪＮＳＡとしての貢献についても考えていく。

＜予定成果物＞

- 日韓シンポジウム開催報告書

【電子署名WG】

（リーダー:宮崎一哉 氏／
三菱電機株式会社　情報技術総合研究所）

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＞
- PDF署名（PAdES）プロファイルのISO国際標準化
- リモート署名ガイドライン

【PKI相互運用技術WG】
（リーダー:松本泰 氏／セコム株式会社）

PKI相互運用技術に関する勉強会を開催。年間4回程度のWG開催のほか、「PKI day 2017」を開催する。また、暗号技術等に関連した勉強会を開催する。

＜予定成果物＞
- PKI Day 2017 イベントでの発表

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、情報セキュリティ教育のシラバスや講義資料およびSecBoK更新版の作成とともに教育界・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。

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＞
- 大学シラバス対応版
- SecBoK2018

【ゲーム教育WG 】
（リーダー:長谷川長一 氏／株式会社ラック）

ゲームを活用した体験学習・振り返り教育の調査研究及び普及・促進。

＜予定成果物＞
- ファシリテーションスキルガイドブック 第1版
- ボードゲーム「Containment」

【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、実践での大学などでの講義を通じて、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＞
- 岡山理科大学での「情報セキュリティ」講義の実施
- 情報セキュリティ講義コンテンツの更新、新規作成

【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、テーマは次年度の初回WGにメンバーで検討する。

＜予定成果物＞
- 2016年度の脆弱性情報勉強会のアウトプット

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の健全な発展のために会員向けサービスを充実させ、業界の発展に貢献する。

具体的には、勉強会や製品紹介サイトの運営、各種ガイドラインと製品との関連付け、情報交換・情報発信などを行う。また、新規会員向けのJNSA活動説明会を春と秋に実施する。

【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

- 関係諸団体が有しているWeb内でのバナー掲載促進

【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)

中小企業や大企業の中の比較的小さなセキュリティ部門における情報セキュリティ対策推進のための様々なアイディアを具現化して、情報セキュリティ産業の育成に資する。

<予定成果物>

- セキュリティ導入課題俯瞰図（更新）
- 以下は、2016年度の成果物記載の3つの課題解決策
- 中小・コンシューマ向けセキュリティ保険提案書
- JNSA既存資産を有効活用した課題解決コンテンツ
- 中小企業向け情報資産推計ロジック

「JNSA既存資産を有効活用した課題解決コンテンツ」は普及啓発・ビジネス推進に役立つJNSAの膨大な資産を再利用しつつ、課題解決に役立つクイックガイドを想定。

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

JNSAのWG成果物の普及促進、WEB改善活動を行う他、新たに会員企業増加施策として2017年上半期に全国セミナーを実施、経済産業省とタイアップし加盟企業増加を目指す。

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。

【経営者向け情報セキュリティ対策実践手引きWG】
(リーダー:河野愛 氏／
株式会社インターネットイニシアティブ)

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、必要性の見える化施策を検討する。

<予定成果物>

- 経営者向け情報セキュリティ対策実践手引き(仮称)

【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目指す。

【技術研究WG】
（リーダー：久保智夫 氏／株式会社サーバーワークス）

内部勉強会やJASA等との共同勉強会等も含めたものとして、研究(勉強) テーマを1回完結式ではなく継続して研鑽する。

8. U40部会

部会長：赤松孝彬 氏／株式会社ディアイティ

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:稲葉悠 氏／
セコムトラストシステムズ株式会社)

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:杉野広典 氏／
NECネクサソリューションズ株式会社)

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・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＞

- 教育コースのSecBoKマッピング

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

「各脆弱性診断ガイドラインの作成」を行う。また、各社持ち回りでテーマ設定の上、1～2か月に一回WG活動を行うとともに、セミナーを2回（5月・2月）開催する。

ユーザー企業を起点とした情報（Indicator）共有の仕組みについての議論やセキュリティ対応組織の教科書の改訂、MITRE本に関する活動を実施する。

「グローバル動静情報共有プロジェクト」の活動も予定。

＜予定成果物＞

- Webアプリケーション脆弱性診断ガイドライン（4月）
- セキュリティ対応組織の教科書の改訂版（10月）
- Internet Week 2017での公開向け資料（11月）

【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（5月・2月）開催予定。また、8月に集中検討（合宿）を実施した。

【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。集中検討（合宿：夏・冬）

ユーザー企業を起点とした情報（Indicator）共有の仕組みについて（1年間の議論を予定）、セキュリティ対応組織の教科書の改訂、MITRE本の翻訳あるいは解説本の執筆、ISOG-J内アンケートの実施、分析など。

【PJ（グローバル動静情報共有プロジェクト）】

最新のグローバルでのセキュリティに関する情報を持ち寄り、グローバルな観点での”動静”の本質的な把握を行う。1ヶ月に1回のプロジェクト活動を行う予定。

11. 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53名の学生の参加があった。11月には、「これからのIT人材のキャリアを考える」と題して学生と若手社員を対象としたを開催し、48名の参加があり、次回開催を期待する声が寄せられた。

12. SECCON実行委員会

実行委員長：竹迫良範 氏
副実行委員長：寺島崇幸 氏／株式会社ディアイティ

今年度も企業スポンサーを募り、「SECCON 2017」として全国的にセキュリティコンテストを実施。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する。

JNSA 役員一覧 2018 年 2 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	KDDI株式会社

理　事（50音順）

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
小椋　則樹	ユニアデックス株式会社
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	三菱電機株式会社情報技術総合研究所
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
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）

安達　智雄	日本電気株式会社
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
嶺村　慶一	株式会社アークン
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
清水　　智	トレンドマイクロ株式会社
下村　正洋	株式会社ディアイティ
鈴木　英樹	株式会社OSK
高木　経夫	ユニアデックス株式会社
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
中尾　康二	KDDI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
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
本川　祐治	株式会社日立システムズ
森　　直彦	エヌ・ティ・ティ・アドバンステクノロジ株式会社
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
渡辺　一範	株式会社インフォセック

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 教授
武藤　佳恭	慶應義塾大学 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3月現在　213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) New
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) New
(株)アピリッツ
(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)
(株)イーセクター
イーロックジャパン(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 New
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)
NHN テコラス(株)
エヌ・ティ・ティ・アドバンステクノロジ(株)
NTT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)
エヌ・ティ・ティレゾナント(株)
(株)FFRI
エムオーテックス(株) New
(株)エルテス
(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 New
KDDI(株)
KPMGコンサルティング(株)
興安計装(株) New
(株)構造計画研究所 New
(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) New
(株)コンシスト

【さ】
サイエンスパーク(株)
(株)サイバーエージェント
サイバー・ソリューション(株)
サイボウズ(株)
(株)サーバーワークス
G・O・G(株)
ジーブレイン(株)
JBCC(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)
JPCERTコーディネーションセンター
ジェネシス・ジャパン(株) New
(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 New
情報セキュリティ(株) New
(株)信興テクノミスト
新日鉄住金ソリューションズ(株)
セイコーソリューションズ(株)
(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)
TIS(株)

(株)ディアイティ
デジタルアーツ(株)
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
東京エレクトロン デバイス(株)
東京海上日動リスクコンサルティング(株) New
東芝デジタルソリューションズ(株)
ドコモ・システムズ(株)
有限責任監査法人トーマツ
凸版印刷(株)
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 New
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)
日本プルーフポイント(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) New
(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)
BAEシステムズ・アプライド・インテリジェンス・ジャパン(株) New
(株)日立システムズ
(株)日立ソリューションズ
飛天ジャパン(株)
(株)PFU
(株)B5NOTE New
PwCサイバーサービス合同会社
華為技術日本(株)
(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) New
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 New ボラトリ
(株)Preferred Networks
FRONTIER(株) New
(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)
三菱電機インフォメーションシステムズ(株)
三菱電機(株)情報技術総合研究所
三菱電機インフォメーションネットワーク(株)
(株)mediba
(株)メトロ

【や】

(株)ユービーセキュア
ユニアデックス(株)

【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)
(有)ロボック

【わ】

(株)ワイズ

【特別会員】

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

JNSA 年間活動（2017 年度）

4月	4月19日	PKI Day 2017「IoT・ブロックチェーン時代の PKI」
	4月26日	第1回　幹事会
	4月29日	産学情報セキュリティ人材交流会〜インターンシップに向けて
5月	5月10日	2017 年度　理事会
	5月27日	SECCON Beginners 2017 長野
6月	6月8日	JNSA 全国横断セキュリティセミナー 2017　福岡
	6月12日	JNSA 2016 年度活動報告会 / 2017 年度総会（秋葉原 UDX）
	6月16日	CTF for GIRLS　第7回ワークショップ
	6月24日	SECCON Beginners 2017 盛岡
	6月26日	JNSA 全国横断セキュリティセミナー 2017　名古屋
	6月27日	JNSA 全国横断セキュリティセミナー 2017　大阪
7月	7月1日	SECCON Beginners 2017 名古屋
	7月13日	JNSA 全国横断セキュリティセミナー 2017　仙台
	7月20日	JNSA 全国横断セキュリティセミナー 2017　東京
	7月21日	第2回幹事会
8月	8月19日	CTF for GIRLS　学生対象ワークショップ
	8月26日	SECCON Beginners 2017 広島
9月	9月21日	第3回　幹事会
	9月23日	SECCON Beginners 2017 仙台
10月	10月7日	SECCON Beginners 2017 東京
11月	11月18日	SECCON Beginners 2017 鹿児島
	11月22日	第4回　幹事会
	11月25日	産学情報セキュリティ人材育成セミナー IT 人材のキャリアを考える」
12月	12月2日	SECCON Beginners 2017 長崎
	12月5日	CTF for GIRLS　第8回ワークショップ
	12月9日	SECCON 2017 オンライン予選
	12月10日	SECCON 2017 オンライン予選
	12月15日	CTF for GIRLS　第8回ワークショップ
	12月15日	SecurityDay 2017
1月	1月19日	第5回　幹事会
	1月24日	Network Security Forum 2018
	1月24日	賀詞交換会
	1月26日	アイデンティティ管理 WG セミナー「クロスボーダー時代のアイデンティティ管理セミナー」
2月	2月17日	SECCON 2017 決勝大会（国内決勝大会）
	2月18日	SECCON 2017 決勝大会（国際決勝大会）
	2月19日	SECCON 2017 決勝大会（国際決勝大会）
	2月26日	IoT セキュリティ WG セミナー「IoT セキュリティセミナー 」
	2月27日	ISEPA セミナー「情報セキュリティ人材育成セミナー」
3月	3月8日	JNSA ゲーム教育 WG「セキュリティゲーム体験イベント」
	3月9日	JNSA 拡大幹事会
	3月16日	NSF2018 in Kansai
	3月23日	第6回　幹事会

2017 年 4 月から 2018 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、http://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 http://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。）

株式会社ラック　佐々木　紅

JNSA会員の皆さま、株式会社ラックの佐々木と申します。
多くの方は、初めて私の名前を聞かれると存じますが、私の自己紹介をさせていただきます。

JNSAにおいては、海外市場開拓WGが発足された当初より参加しております。といいましても、現在シンガポールで活動中のため、WGの活動に貢献できておらず、いわゆる幽霊部員と化しており、唯一、海外でのカンファレンス・視察調整において活動しております。（写真は、今年のシンガポールInterpol Worldの時のもの）

まずは、簡単に私のラックにおける経歴を紹介いたします。

- ●2000年ラック入社
- ●IDS製品（当時、IPSは無かった…）サポート
- ●自社の脆弱性情報収集・検証製品リーダ
- ●コンサルティング（この間中国、米国での案件従事）
- ●2015年よりシンガポールで活動

現在は、シンガポールでASEAN諸国を中心に渉外・営業・コンサル・PMと様々な活動をしています。（ラックが海外で業務をしていることをご存知ない方も多いのでは）

会員の皆さまも一度はシンガポールに出張されたことがあるかと存じます。そして色々な経験をされたことと思います。と言う私もいま貴重な経験をしている最中です。
私が得ている経験は、次のようなものです。

- ●多様性
  シンガポールでは中国語、英語、マレー語、タミール語が公用語
- ●スピード
  議論の結論、意思決定など、あらゆる決断が早い
- ●ワークライフバランス
  シンガポールの方は皆さん大変勤勉ですが、定時に退社し家族・友人・自分の時間を大切されています
- ●日本の文化に対する興味、日本のモノへの安心感
  シンガポールの方々は、日本の製品に対して大変高い信頼感、そして安心感をお持ちです

日々刺激にあふれたシンガポールで、私たちラックが培ってきた経験をもとに、失敗は最高の財産であると信じ色々なことにチャレンジしています。と、格好良く書きましたが実際は山あり谷ありで、ほぼ決まっていた案件が大逆転負けという苦い経験もたくさん得ることができました。

プライベートでは、3年前よりスキューバダイビング、昨年よりヨガを始めています。何も考えずにただただ自然に溶けこみ、自分を見つめる時間を持つことが、私のワークライフバランスになっています。
仕事における「動」。そして私生活における「静」を両立し、グローバルで人の役に立てる人間になりたいと考えています。

会員の皆さま、もしシンガポールに居らっしゃることがございましたら、気軽に連絡くださいませ。
最後に、海外市場開拓WGの皆さまいつもありがとうございます。これからも頑張りましょう！

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。）

トレンドマイクロ株式会社　萩原　健太

JNSA会員の皆さま、幹事・会員交流部会部会長の萩原健太（はぎはら けんた）です。まだ書いていなかったのが見つかってしまい？本稿を執筆させて頂きます。

簡単に学歴です。私は明治学院大学法学部政治学科を卒業し、法政大学大学院公共政策研究科修士課程を修了しています。文系です。

現在はトレンドマイクロに籍を置きながら、JNSA、日本シーサート協議会（NCA）、コンピュータソフトウェア協会（CSAJ）などで活動しています。

元々、ITにはあまり興味がなく、当然セキュリティにも興味がありませんでした。しかし、大学時代に選挙に関する勉強をしているうちに、電子投票の仕組みに興味を持ち、コンピュータやインターネットを使った遠隔投票が行える社会を構築できないかと考えるようになりました。投票所に行かずに投票を行うと、「直接選挙」の原則（本人が候補者を直接選ぶ）や「秘密選挙」の原則（誰に投票したか知られない）の課題に直面し、それらを解決するためには、セキュリティの観点を欠かすことができませんでした。結局、その答えは（途中で私の興味と関心が変わったこともあり）見つかっていませんが、これがきっかけでセキュリティをもう少し学びたいと思い、トレンドマイクロに入社し、セキュリティ業界に身を置くこととなりました。

トレンドマイクロでは、営業・マーケティングなどを担当し、2012年にはTM-SIRTを作り、2013年には2011年頃から兼務していた統合政策担当の専属（小屋晋吾さんの部下（現在は株式会社豆蔵ホールディングス所属））となり、CSIRT活動や業界団体での活動、社内のプロジェクト支援や講演などを行うようになりました。さらに今年度からは産学連携を一層強化していく役割も追加されます。

さて話は変わりますが、私は幼少期から野球をやっていました。残念ながら中学時代に身体を壊し、早々に引退してしまいましたが、今はたまに野球の審判をやっています。審判としての心構えや所作などは、サイバーセキュリティにも通じるものがあります。ここでは書ききれないので、飲んだ時に是非お話しましょう。サイバーセキュリティも好きですが、野球の話はもっと好きなので…(笑)

最後に、私は特出したスキルや知識を持っているわけではありませんし、大して面白い話も出来ていないかもしれません。（たまには面白い話もしているはずですが…）

私がサイバーセキュリティの世界で貢献出来ることは多くないかもしれませんが、少しでも皆さまのお力になれますよう、今後もサイバーセキュリティ業界のため、広くは日本のサイバー空間の安全のために微力ながら努めてまいります。

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）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. 年 2 回の 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：http://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.45

2018 年 3 月 30 日発行
©2018 Japan Network Security Association
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: http://www.jnsa.org/

印　刷
プリンテックス株式会社

SECCONとは

SECCONは、セキュリティ・キャンプ講師経験者をはじめとする有志により設立され、日本のセキュリティ技術の底上げと人材の発掘・育成を目的として、2012年からその活動を始めました。

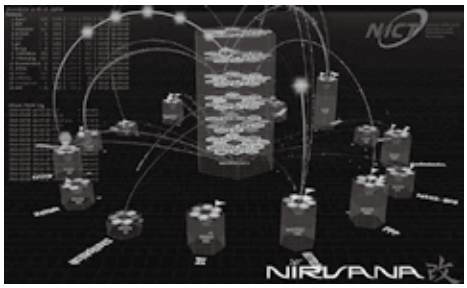
2017年のSECCONの活動

- SECCON 2017オンライン予選
- SECCON 2017 x CEDEC CHALLENGE
- SECCON Beginners（全国8か所）
- SECCON Beginners NEXT（中級レベル以上）※初開催
- SECCON Beginners CTF（初心者向けCTF）※初開催
- CTF for GIRLS （全2回）
- CTF for SchoolGIRLS（学生向け）※初開催
- 攻殻機動隊 REALIZE PROJECT x CTF for GIRLS in CODE BLUE

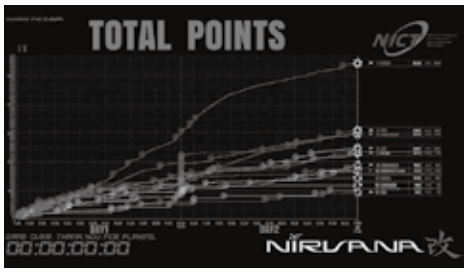
▼ ワークショップの様子

▲ ビギナーズCTFの様子

▼ カンファレンスの様子



▲▼ 決勝大会で使われた
NIRVANA改 SECCONカスタム Mk-IV
（画像提供：情報通信研究機構）



SECCON2017決勝大会

2017年は102ヵ国、4,347名が参加したオンライン予選から上位の日本チームは国内大会、全体の上位12チームは国際大会に出場しました。
またCTF大会のほかにカンファレンスやワークショップなども実施しました。
国際大会では日本のチームが3位入賞する活躍を見せました。

▲ 国際決勝大会会場

2018年度のSECCONの展開

2017年3月には初心者向けのCTF大会（オンライン、オフライン）の実施を予定しており、より多くの人にCTFに興味を持ってもらう活動を継続していきます。
SECCON Beginnersも初心者向けに限らず、中級者以上向けのワークショップも東京以外での実施を検討しています。

スポンサー募集中！
https:2017.seccon.jp/

SECCON2017メールマガジン登録
CTFに興味を持っている人・SECCON参加者や参加検討中の方々を対象にメールマガジンを発行しています。2017年度のメールマガジン登録を希望する方はこちらからご登録をお願いします。
https://frm.f2ff.jp/form/seccon_ml/
（SECCON2017運営事務局ナノオプト・メディアのサイトです）

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、外務省（2017/8/1以降）、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）、OWASP Japan、日本シーサート協議会

サイバーセキュリティ小説コンテスト

大賞：賞金100万円＋角川スニーカー文庫より書籍化！2018年3月30日より受け付け開始！

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

協賛 サイボウズ Microsoft HITACHI Inspire the Next 株式会社 日立システムズ JPRS JAPAN REGISTRY SERVICES Symantec TREND MICRO Securing Your Journey to the Cloud 株式会社ベネッセインフォシエル

協力 NISC 内閣サイバーセキュリティセンター National center of Incident readiness and Strategy for Cybersecurity 後援：サイバーセキュリティ戦略本部

運営 KADOKAWA カクヨム

©2018 NPO日本ネットワークセキュリティ協会
イラストレーション：久正人

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: http://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