JNSA PRESS
JAPAN NETWORK SECURITY ASSOCIATION
SUMMER 2019 VOL. 47

寄稿

アイデンティティ関連要素技術の変遷とプライバシー

AI・IoTによるイノベーションを支える暗号技術によるトラスト

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

より多くの学生にセキュリティ業界に進んでもらうには

電気通信大学　情報理工学研究科　教授
セキュリティ情報学プログラム　兼任
情報処理学会フェロー　吉浦　裕

セキュリティの専門教育を行うセキュリティ情報学プログラムに所属している。プログラムの学部定員は40名で、約3割が学部卒で就職し、7割が大学院卒で就職する。プログラムからセキュリティ業界への就職について最近3年間のデータを調べた。電機メーカーに入社した学生の何割がセキュリティ部門に配属されたかといった入社後の配属先を調べ切れなかったため、正確な数値ではないが、就職者全体の約20%がセキュリティ業界に進んでいた。このような現状を踏まえ、より多くの学生にセキュリティ業界に進んでもらう方法について考えてみた。

セキュリティ業界は、これまで高い技術を持つ学生（高度技術人材と呼ぶことにする）を集めてきたように思うが、今後は、ボリュームゾーンの人材すなわち全科目で万遍なく中以上の成績を修める人材（バランス型人材）をもっと集めるのはどうだろうか。バランス型人材は、ネットワークやセキュリティで即戦力のレベルにはないかもしれない。しかし、基礎学力が高く、勤勉で組織順応性が高いので、技術とビジネスの両方にまたがる組織の中核になれる。

バランス型人材が仕事を選択する際には、やりがいと面白さだけでなく、労働時間、収入、キャリアパスを総合的に判断するだろう。セキュリティ人材のキャリアパスについては、JNSAが非常に優れたレポートを発表しており、高い見識を持って取り組んでおられる。しかし、キャリアパスの問題は難しい。バランス型人材については日本的な企業内昇進をベースにして真正面から取り組むしかないと思う。一方、既に一部取り組まれていると思うが、高度技術人材については、日本的でないキャリアパスもありうる。より自由な勤務形態や仕事内容、自己啓発の自由度拡大、業界有名人へのプロモート、産学間の異動、企業間公募やプロ野球界のようなフリーエージェント制があってもいい。なお、これらは、企業の業務の継続性を保証する仕組みと併用する必要がある。これらの対策はコストとリスクを伴うが、高度技術人材を終身で全て企業内に抱え、バランス型人材と高度技術人材の両方にポストを用意することに比べれば、人材にとっても企業にとっても幸せかもしれない。

一方、セキュリティ特にサイバーセキュリティの専門教員が日本全体に少ないという問題がある。その結果、サイバーセキュリティ分野の学生がなかなか育たない。企業のサイバーセキュリティ技術者にもっと大学教員になっていただければ、大学の教育の問題と企業のキャリアパスの問題を同時に緩和できる。大学教員になるには博士号が必要であるため、産学が協力して、企業の技術者が大学の社会人向け博士課程に入学しやすくする必要がある。博士課程では、100ページにおよぶ学位論文と1時間におよぶ発表スライドを一貫した論理に沿って書き上げる。この訓練は、将来の大学への転出に役立つだけでなく、実務能力の向上にも有益であり、企業にとってもメリットがあると思う。

アイデンティティ関連要素技術の変遷とプライバシー

板倉　景子

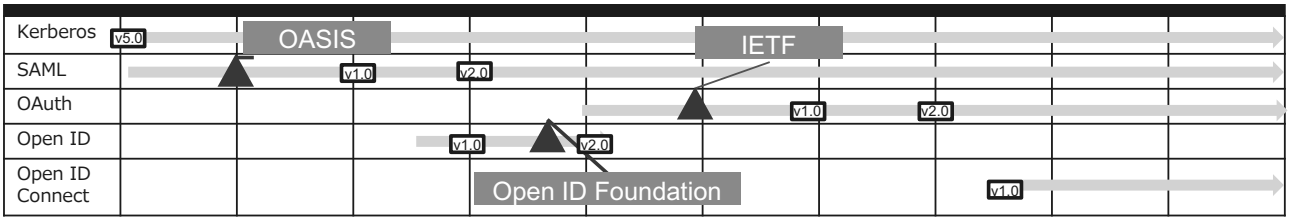
1. はじめに

あらゆるデバイスがインターネットに接続しインターネット上を流通するデータ量も増大しているなか、アイデンティティ管理の重要性も日増しに増大している。

アイデンティティ関連要素技術は多岐に及ぶが今回は前半部分で認証、認可の技術仕様を振り返りながら、後半部分ではもう少し抽象概念である「アイデンティティ」とそれにまつわるプライバシーについて記載する。

1.1 認証 / 認可プロトコル、標準仕様

まず簡単に認証 / 認可のプロトコル、標準仕様について代表的なものを整理する。

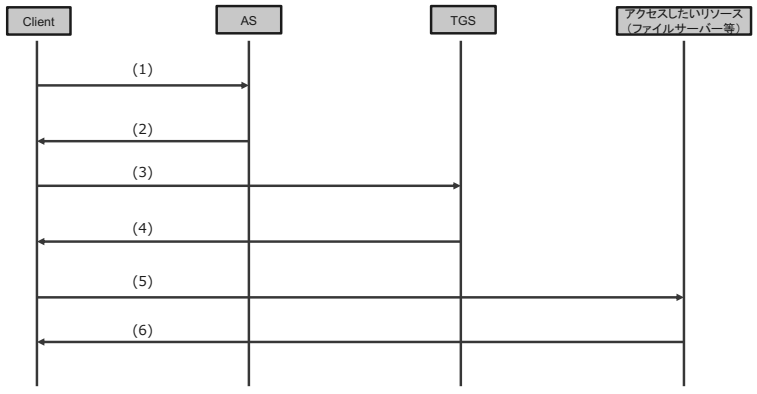


プロトコル/標準仕様年表

1.2 Kerberos

MITにより開発された認証プロトコルであり、1989年から利用されている。Windows Server Active Directory環境におけるユーザー認証として利用されることでも有名である。

ユーザーIDやパスワードといった認証情報はKDC(Key Distribution Center) と呼ばれる認証サーバで一元管理され、KDCが発行するチケットを用いて認証を行う。

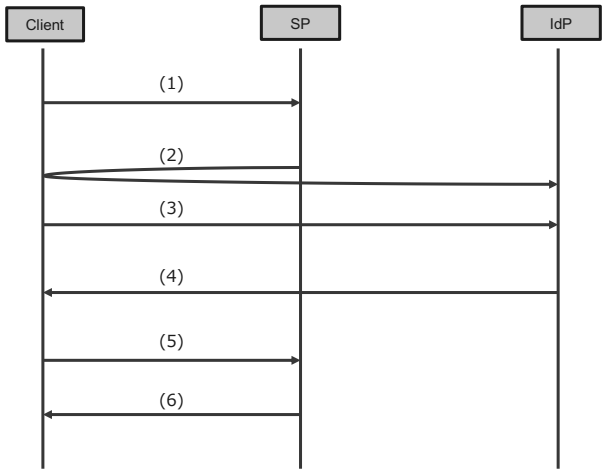


Kerberosシーケンス

1. クライアントは資格情報を入力しASにTGTを要求（Windowsドメイン環境の場合、ログイン時に自動的に実行）
2. 資格情報が正しければASはクライアントへTGTを発行
3. リソースへアクセスするためTGSにSTを要求
4. TGTを確認しTGSはクライアントへSTを発行
5. リソースへSTを提示
6. STを確認しアクセス許可

1.3 SAML

SAMLはSecurity Assertion Markup Languageの略で、OASIS3によって策定された、認証情報や属性情報をHTTPやSOAPなどで連携するためのXMLベースの標準仕様である。



SAMLシーケンス

1. クライアントはSPへアクセスする。
2. Idpへリダイレクトし認証要求を送付
3. クライアントは資格情報をIdPへ送付
4. IdPの認証サービスで認証しAssertionを生成し署名
5. クライアントはAssertionをSPへPOST
6. SPにてAssertion署名を検証し検証結果がOKであればサービスへのアクセス許可

1.4 OAuth

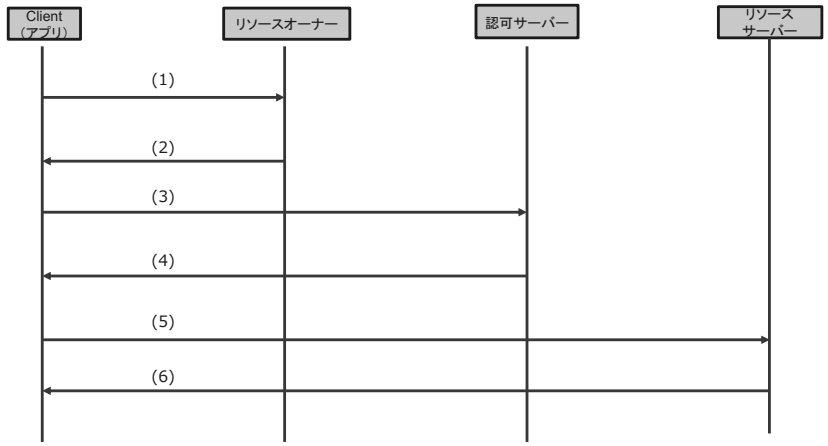
これまでの認証/認可のアーキテクチャは、複数のサービスが連携する場合はクレデンシャル情報をそのまま渡していたり、各社各様のAPIアクセス認可の仕組みを提供していたりした。(Flickr Auth, 2005 Google AuthSub, Yahoo! BBAuth, …)

しかし、マイクロサービスのような複数サービスが協調して動作するようなアーキテクチャではサービスごとに認証/認可を行う必要があるため、認証情報やアクセス制御ポリシーの管理が煩雑になる。

OAuthとは対象のリソースへのアクセスを許可させるためのフレームワークであり、認証結果や認可情報をAPIサーバ間で共有することで認証情報やアクセス制御ポリシーを一元化し管理が容易になるという利点がある。

OAuth2.0について解説されている「OAuth2 in Action」では、このトークンをValet Keyと喩えている。OAuth1.0は2007年12月にOAuth Core 1.0として公開され、2009年6月にセキュリティの改善がされOAuth Core 1.0 Revision Aとしてリリースされた。そして、2010年4月にはThe OAuth 1.0 Protocol (RFC 5849) として定義され、2012年にOAuth2.0のV2-31が出ている。

OAuthはSAML,Kerberos,WS-* と違って、クライアントアプリケーションがトークンの中身を分析しないことも特徴の一つといえる。ただし、「誰が」というのを表しているわけではないので、別の人がそのトークンを利用してしまえばアクセスができてしまう。

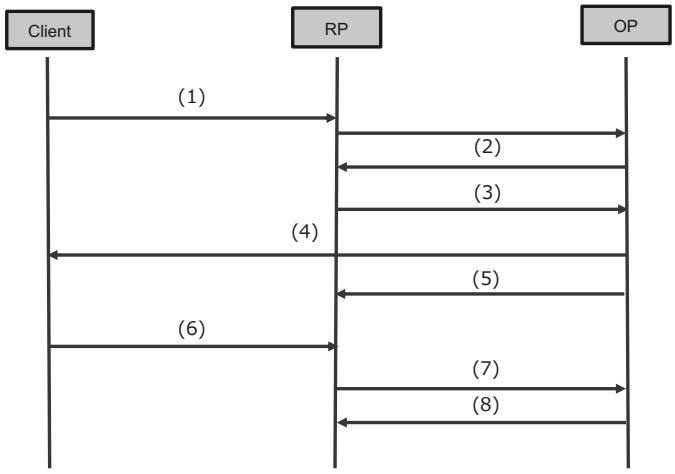


OAuthシーケンス

1. クライアントはResource Owner（ユーザー）へアクセスを許可するかどうか問い合わせ
2. Resource Ownerがアクセスを許可
3. クライアントは認可サーバーへ認可権限をリクエスト
4. 認可サーバーはクライアントへアクセストークンを発行
5. クライアントはアクセストークンをリソースサーバーへ提示
6. リソースサーバーはアクセストークンがデータの利用権限を持っていることを確認し、アクセス許可

1.5 Open ID Connect

Open ID ConnectはOAuth2.0の拡張仕様の一つであり、OAuth2.0を利用して認証やID連携をする際に必要な機能を標準化したものといえる。これを利用することによりWebアプリケーションやネイティブアプリケーション間でアイデンティティ情報を流通させる仕組みをより簡単に安全に実現できるようになった。



Open ID Connectシーケンス

1. RP登録用エンドポイントにPOSTリクエスト
2. 動的RP登録
3. RPはOPに認可リクエスト
4. OPはユーザーへアクセス権限付与の同意をリクエスト
5. ユーザーが同意したらOPは認可応答をRPへ返答
6. ユーザーはアクセストークン、IDトークンをRPへ提示
7. RPはアクセストークンを用いてUserInfoエンドポイントへにリクエスト
8. UserInfoエンドポイントはユーザーに紐づくアイデンティティ情報を返却

1.6 FIDO

なお、パスワードに変わる新たな認証標準としてのFIDOについても触れておきたい。FIDOとはFIDOアライアンスによって策定されている認証標準であり、パスワードの代わりにユーザーの公開鍵と署名を送付することで認証を行う仕組みである。なお、秘密鍵はユーザーのスマートフォンなどに保管されるためサーバー側に送付する必要が

ない。技術仕様が公開されているため、様々なメーカーが自社製品やサービスで利用を進めている。

1.7 社会的背景

かつて情報の活用が企業内に閉じていた時代から、それが企業間、インターネットを通じた第三者へと変化していくにつれその背景にある要素技術も変遷をたどっている。アイデンティティ関連要素技術の変遷は企業の境界を超えた情報の利活用の変遷とも言えるのではないか。

1.7.1 [昨今の動向]情報利活用によるサービス改善・新サービス提供への期待の高まり

総務省「平成28年 通信利用動向調査」によれば、インターネットを利用している個人の割合は83.5%であり、上昇傾向にある。

また、スマートフォンを保有する個人の割合も年々上昇しており、56.8%の個人が保有し、個人がいつでもどこでもインターネットにアクセスし様々なサービスを利用できる環境が整ってきている。

加えて、あらゆるデバイスがインターネットに接続するようになり、インターネット上を流通するデータ量は増大の一途を辿っている。

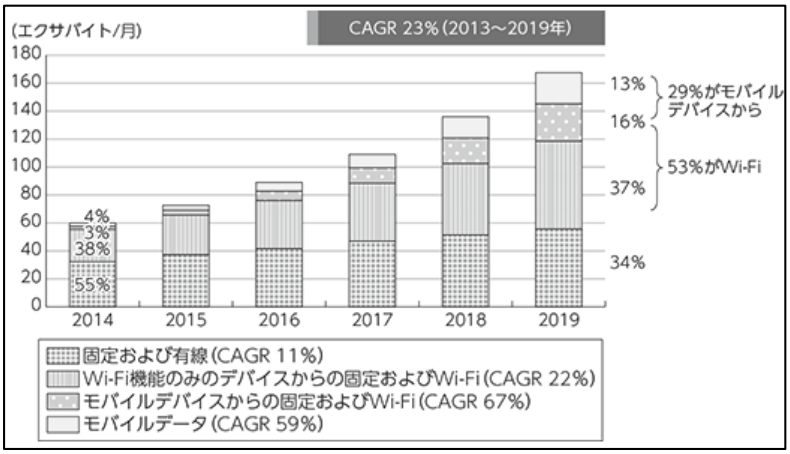


図1　データトラフィックの推移及び予測
出典：総務省「平成28年度　情報通信白書」

このような環境下において、インターネット上に流通する情報を利活用することによる既存のサービスの改善や、新たなサービスの提供へ期待が高まっている。

また、金融機関などの機密情報がwebや端末からのアクセスが年々増える傾向であり。イギリスの金融機関の統計を見ると、2007年から2018年の間で日常的にオンラインバンキングサービスを使用している個人の割合が40%程上昇しているという。このように色んなモノやサービスがインターネット環境で連携していく中でアイデンティティ管理の重要性が増加している。

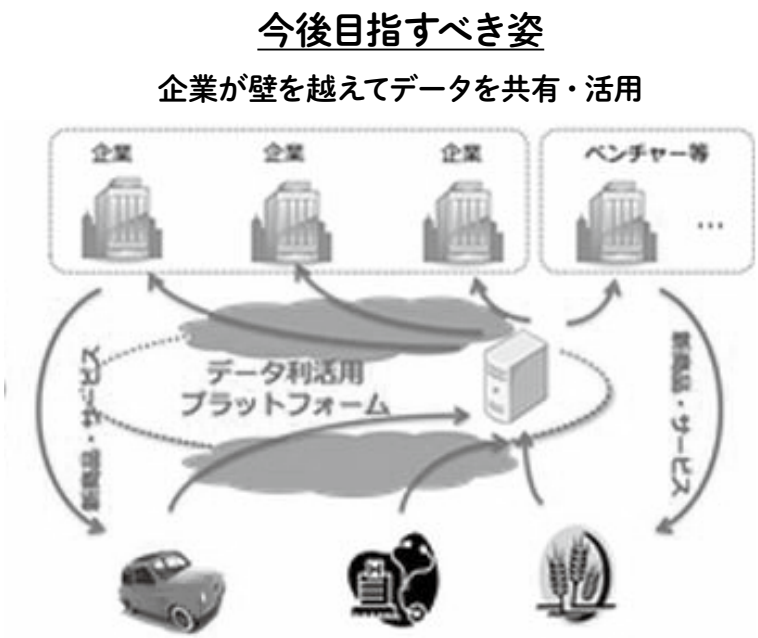


図 2　データを利活用した新たな付加価値の創出
出典：経済産業省「データ駆動型イノベーション」

1.8 本人確認手段の多様化

OAuthやOpen ID Connectといった認証 / 認可の技術はWebサービスにおける本人確認技術としても利用されている。昨今、Webサービスの利用においてはソーシャルログイン機能の普及が進んでおり、メルカリ、Airbnb、Uberといったサービスも Facebookアカウントでの個人情報登録及びログインが可能となっている。

事業者	会員数	提供サービス
Facebook	20 億	認証、ソーシャルグラフ
Twitter	1 億 7500 万	認証、ソーシャルグラフ
Google	1 億 7000 万	認証、アドレス、決済、Google Apps
Yahoo! Japan	2500 万	認証、アドレス、決済、ポイント

出典：Facebook社 Mark Zuckerbergによる投稿及びSocial Media Lab記事より筆者作成
https://www.facebook.com/zuck/posts/10103831654565331
https://gaiax-socialmedialab.jp/post-30833/

1.8.1 eKYC

「eKYC」とは、オンラインで完結する本人確認方法のことである。「電子的にあなたの顧客を知る」という意味の英語「electronic Know Your Customer」の略から来ている。

これまで銀行や保険会社、資金移動業者や仮想通貨交換業者などの業務の一部ではオンラインでの本人確認ができなかった。そのため、これらの業者とユーザーが一定の取引を行う際には、オフラインで本人確認が行われてきた。

これが、2018年11月の犯罪収益移転防止法施行規則の改正によって、オンラインで完結する本人確認方法、つまり「eKYC」の利用が一定の範囲（以下の2つの方法）で可能となった。

1. 「顔写真付きの身分証明書と自分の顔」の写った写真の送付、もしくは「自分の顔とICカード形式の身分証データ」の送付
2. 1と同様に「身分証明書」の画像もしくは「身分証データ」をオンラインで送付した上で、ユーザー名義の銀行口座開設やクレジットカード発行時の本人確認記録を他の事業者を通して確認することで本人確認

直近でも、メルペイは4月23日、LINE Payは4月24日、顔認証を利用したオンライン本人確認（e-KYC）を相次いで導入した。[2]

1.8.2 Self Sovereign Identity（SSI）

このような本人確認手段の変化の中で新たに出てきている概念がSelf Soverign Identity（自己主権型アイデンティティ）という概念である。これはユーザーが個人の情報を保持、コントロールし、サービスプロバイダにどこまで提供するかどうかを個人自身で決定するという考え方である。具体的にはEthereum開発者であるFabian VogelstellerがGitHubでSSIを実現するEthereum規格案を公開したりしている。

1.9 情報銀行

データの主権を個人に持たせるという点では、政府にて進めている施策として「情報銀行」やPDS（Personal Data Store）の取り組みも紹介しておきたい。

PDSとは個人が本人のデータを蓄積・管理し、他者と限定的に共有して活用することを可能にする仕組みであり、「情報銀行」とは集中PDSとして個人の情報を預託し、匿名化等の処理を施した上で事業者に提供するデータブローカである。

データ流通・利活用に関する国民の不安や不信感を払しょくするためにも、これらの取り組みを通じてデータ流通への個人の関与を強化していくことを進めている。

1.10 アイデンティティ関連要素にまつわるインシデントとプライバシー課題

インターネット上で様々なサービスが提供される中、そのサービスのいくつかではセキュリティ事故も発生している。2018年ではデータ侵害による被害の81%は二要素認証を使用しない脆弱なID・パスワードに対して行われており、[3]パスワードよりも強固な生体認証、行動分析、ハード・ソフトセキュリティトークンなどの重要性は増加している。

---

[2] https://jp.merpay.com/news/2019/04/ekyc_postpay/

[3] Verizon Data Breach Investigation Report
https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

企業でセキュリティ事故が発生し個人情報を悪用されることによりプライバシーが侵害されることの他に、企業がデータを利活用した結果、プライバシー侵害が生じる場合もある。
インターネット上に流通する情報量が増大し、かつその情報を処理する技術も進んだ結果として、これまでは特定の個人を識別できなかった情報が複数の情報と組み合わせることにより、特定の個人を識別することができるようになった。
企業はそれらの情報を利活用して、新たなサービスを提供したり、既存のサービスを改善しているが、消費者にとってはそれをプライバシーの侵害と感じ、問題となるケースがある。
法規制において、このプライバシー問題は現在時点でも曖昧性が残っており、事業者のセキュリティ対策が不十分であり、法規に違反しプライバシー侵害となる事例だけでなく、事業者が意図的に法制度の規範が曖昧な領域へ挑戦していることにより発生している事例もある。

本寄稿では深くふれることができなかったが、サービス提供者側の企業または個人がどのようなプライバシー意識を持っているか、どのようにサービス購入者との信頼関係を構築していくべきか議論の余地がある。
そもそも、プライバシーというのは画一的に語ることが非常に難しい概念であり、関係性の中で成立する相対的な概念といえる。現実をいかにリスクベースで評価できるかがプライバシー対策の重要なポイントであるだろう。

2. 終わりに

データを囲い込むのではなく活用するという流れの中で個人が自分自身のデータの主導権を握るべきという考え方が進んでいる。
自分を必要最低限にどうやってIdentifyしてもらうのかということを今後も考えていかなければいけないだろう。

参考文献

[1] サイバーセキュリティ.com「個人情報漏洩事件一覧」
https://cybersecurity-jp.com/leakage-of-personal-information（2017年7月18日参照）

[1] Justin Richer Antonio Sanso (2017) OAuth2 in Action

[2] https://w3c-ccg.github.io/did-spec/

AI・IoTによるイノベーションを支える暗号技術によるトラスト

セコム株式会社 IS 研究所
JNSA PKI 相互運用技術 WG リーダー
松本　泰

1. はじめに

Society5.0が目指す超スマート時代において、AI・IoTによるイノベーションが期待されている。IoTは、繋がることによる価値の創造が求められており、また、AIは、IoTの吐き出すビッグデータを処理するといったことにより様々な産業におけるイノベーションが期待されている。

AI・IoTによるイノベーションが期待されている分野に自動車、医療デバイス等があるが、これらの分野においては、従来からの法的な規制がある。これらの規制が必要な分野において、ソフトウェアや機械学習済みデータの更新が行われるAIエッジを想定した場合、利用時の規制が強化される方向に向かうと考えられる。

利用時の規制を考えた場合、製品プロバイダー・サービスプロバイダーは、利用時における個々のデバイスのトレーサビリティ／トラッキングを確実に実行する必要に迫られる。また、サイバーセキュリティ上だけではなく、セーフティやプライバシーについてもそのインシデントに対するアカウンタビリティが強く求められることになるが、これらの対応に暗号技術によるトラストが非常に重要な役割を果たす。

このようにAI・IoTによるイノベーションに対応するAIエッジは、暗号技術によるトラストの実現が重要になる。こうしたことに対応するために、暗号技術とハードウェアーセキュリティをベースにしたデバイス自体のアーキテクチャ変革が必要であり、こうした技術をベースにしたIoTデバイスが、超スマート時代の産業競争力に結びつくと考えられる。

2. AI・IoTによるイノベーションと規制

AI・IoTによるイノベーションでは、リアル空間に大量に配置されたIoTデバイスが、大量のデータをサイバー空間に吸い上げ学習し、その学習結果をAIエッジに反映するといったモデルが考えられている。このようなAIエッジの考え方が社会に大きなインパクトを与えると考えられている分野／製品に、自動運転などを目指す自動車や、AI医療診断等に利用する医療デバイスがある。

このような自動車や医療デバイスなどは、従来からの「モノ」としての規制が存在する。例えば自動車であれば、車種に対して型式認証と呼ばれる法規・技術要件・安全性を満たした製品に与えられる認証を取得し、この型式認証を取得した車種の個々の車が、法的に要求される出荷検査を経た後に初めて公道を走ることができる。また、医療デバイスであれば、医薬品と同様に、臨床実験において、その効果と安全性が証明された後、承認というフェーズを経て初めて製品の出荷が可能となる。

しかし、AI・IoT等技術の発展と、これらのよるイノベーションの期待等を背景に、この規制のあり方に変化が見られる。例えば、米国における医療の規制管轄官庁であるFDA（米国食品医薬品局）では、2017年からデジタルヘルスソフトウェア事前認証プログラム（Digital Health Software Precertification (Pre-Cert) Program）を開始しているが、ここでは、新たな製品出荷後の規制、すなわち利用時の規制のあり方が示されている。

同様のことは、自動運転への期待が高まる自動車においても起きている。2019年5月、「道路交通法の一部を改正する法律案」が可決し成立した。これは、国連配下の自動車基準調和世界フォーラム(WP29)において自動運転車の国際基準作りに向けた作業の反映でもあるが、この法律の大きな主旨のひとつは「自動運行装置等に組み込まれたプログラムの改変による改造等に係る許可制度」になる。

このような規制が必要な分野におけるAIエッジでは、従来からの「モノ」としての規制だけではなく、利用時の規制、サービスとしての規制が求められることになる。この際、製品プロバイダー・サービスプロバイダーは、AIエッジの利用時おけるに、確実なトレーサビリティ／トラッキング、そして、インシデントなどに対応するアカウタビリティが強く求められることになる。

図1に、これらの関係を示す。

3. 利用時の規制に対応した暗号技術によるトラスト

AIエッジとなる医療デバイスや自動車等において、利用時のソフトウェアや機械学習済みデータの更新が出来ることは、社会を変革させる可能性があるが、これらには、利用時の規制が求められる。

利用時における規制的要求は、概ねセーフティ、プライバシー、セキュリティの確保になると考えられるが、これらの規制に対応するためには、個々のデバイス（医療デバイス、個々の自動車、および、自動車内の個々のECU等）が、確実に個体識別でき、その状態が（リモートから）把握でき、更にセキュアなソフトウェアと学習済みデータ等の更新が可能であることが求められる。また、強い規制という観点からは、これらの客観的な説明、および、証明できることが非常に重要になる。

こうした利用時の規制に対応するAIエッジの実装への要求は、トレーサビリティ・トラッキグ、アカウンタビリティ等に対応する何らかの説明および証明の仕組みになるが、この証明の仕組みは、「トラスト」と言い換えることができる。

このような説明／証明、すなわちトラストには、情報セキュリティで言われるところのCIA の中のI(インテグリティ）を継続的に、また効率的に可能とする実装が重要になる。そして、このインテグリティを効率的に実現するためには、暗号技術、とくデジタル署名技術が、重要な役割を果たす。

規制における重要な視点は、一般的には、セーフティに対する規制の対応が重要であり、セキュリティの対応だけを意味する訳ではないことに注意する必要がある。このように暗号技術によるトラストの実装は、セーフティに対する規制への対応でもある。

AI・IoT によるイノベーションにとって、利用時のソフトウェアと学習済みデータの更新が重要だと考えると、そもそものビジネスモデルが売り切りの製品販売から、利用時重視のサービス中心のビジネスモデルに変化していく。サービスの視点、特にサブスクリプションモデルなどのビジネスモデルを想定した場合、大量のAIエッジの効率的な管理の観点が欠かせないが、ここにも暗号技術によるトラストが大きな役割を果たす。確実なトレーサビリティ・トラッキグの仕組みなしには、サービス時の何らかの課金の仕組みは難しい。すなわち、ビジネス的観点からも暗号技術によるトラストが必要になる。

4. 暗号技術によるトラストの実装および標準化動向

このような利用時の規制に対応するAIエッジにお

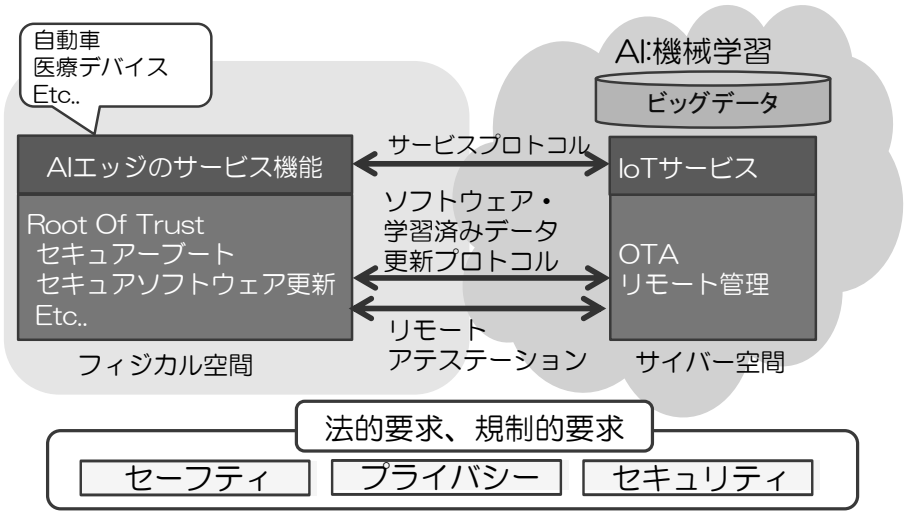


図1. AIエッジ、機械学習、規制の関係

ける「証明の仕組み」すなわち「暗号技術によるトラスト」は、AIエッジの信頼の起点(Root OF Trust)、デバイスIDの一意性、耐タンパ性の確保等がベースとなって構築されることは想像難くない。こうした暗号技術によるトラストを実現するアーキテクチャは、ここ10数年でスマートフォーンという形で非常に進化してきた。そして現在、これらスマートフォーンで培われてきた技術が、様々なIoTデバイス・AIエッジに適用されつつある。

ここでの技術的に重要なキーワードとして、TEE（Trusted Execution Environment）とアテステーションがある。TEEは、概ね、一般のアプリケーションと分離された実行環境（Execution Environment）になるが、この実行環境においてトラストが要求されるアプリケーションが実行される。TEEの実装には、様々なアーキテクチャが提案され、また実装されているが、TEEを利用するAPIはGlobal Platform において標準化されており、これらがIoTデバイスに実装されつつある。また、TEEが組み込まれることを想定したIoTデバイス向け半導体、SoC（System-on-a-chip）が、数多く開発されている。

一方、IoTデバイス・AIエッジをリモートから管理するアテステーションの標準化が進んでいる。IETFでは、2019年3月に開催されたIETF104プラハから、リモート・アテステーション・プロシージャ（Remote Attestation Procedures - RATS）がワーキンググループとして活動を始めているが、このRATSは、リモート環境のIoTデバイスの正当性の確認・証明等、すなわちリモート・アテステーションに使われていくことが想定されている。

このアテステーションという概念は、従来からPCに内蔵されたTPM等を利用して実装されてきたが、それほどブレークしたとは言い難いところがあった。PCの場合、PCの管理を利用する人に頼っていた側面があったためと考えられる。

これに対して、現在、膨大な数のIoTデバイスを人手に頼らずにリモート管理するといった要求からリモート・アテステーションが俄然注目を浴びている。こうした仕組みの標準化が出来れば、多様なIoTデバイスを、大量にかつ効率的にリモート管理が可能になり、すなわち低コストでIoTデバイスを保守することが可能になる。そして、こうしたことがイノベーションにつながる。

トラストなアテステーションを生成しようとした場合には、ハードウェアセキュリティ、Root of TrustやTEEなどに依存することになるが、このトラストなアテステーションは、「利用時の規制」や、サブスクリプションモデルのビジネスにおけるIoTデバイス・AIエッジにとって非常に重要な役割を果たすことになる。

5. おわりに

既存の法規制等が、AI・IoTによるイノベーションを阻害していると考えられる一方、本質的に規制が必要な分野においては、規制のパラダイムシフトが起こりつつある。こうした分野においては、新たな法規制などに対応できるIoTデバイス・AIエッジの暗号技術によるトラストが重要となり、これらが低コストで実現できることが、今後の超スマート社会における競争力の源泉ともなる。

参考文献

PKI day 2019 午前の部　IoTのトラスト
https://www.jnsa.org/seminar/pki-day/2019/

FDA Digital Health Software Precertification (Pre-Cert) Program
https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program

IETF: Remote ATtestation ProcedureS (rats)
https://datatracker.ietf.org/wg/rats/

JNSA ワーキンググループ紹介

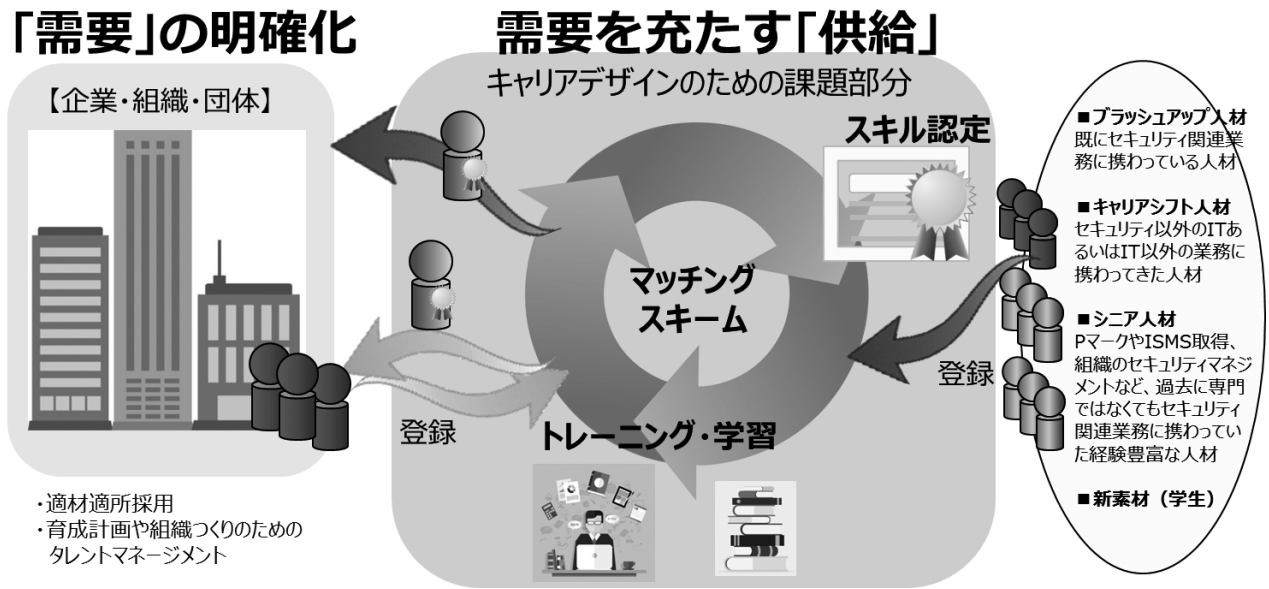
ISEPA（情報セキュリティ教育事業者連絡会）
JTAG

キャリアデザイン WG リーダー（株式会社 VSN） 玉川　博之
認定 WG リーダー（株式会社ラック） 大槻　晃助

■ JTAGについて

国内の情報セキュリティ事業者やユーザー企業・人材サービス事業者、教育提供事業者が広く協力して、セキュリティ人材ニーズの明確化、情報セキュリティ人材の基盤拡充策について検討を行っています。セキュリティ分野がより魅力的な分野となり、長期活躍するキャリア基盤を構築する目的のもと、２つのWGを中心に相互に連携しながら活動しています。

情報セキュリティの業務や役割は専門技術に限らず管理部門、営業部門、さらにすべての組織運営に関わるマネジメント領域まで多岐に渡ります。それらを整理しながら職としての待遇や将来性を高めるための施策や道しるべを導き出す「キャリアデザインWG」と、そこでアウトプットされたデザインを土台にして精度の高い実力値認定の仕組みを創る「認定WG」の２つとなります。



■ キャリアデザインWG

キャリアデザインワーキンググループでは、セキュリティに関わる人を調査し、キャリアアップやキャリアチェンジのモデルデザインを検討しています。2018年はセキュリティ業務の中でも特に、『自社内のセキュリティ維持向上に携わっている方』へインタビューをし、レポートを発表しました。

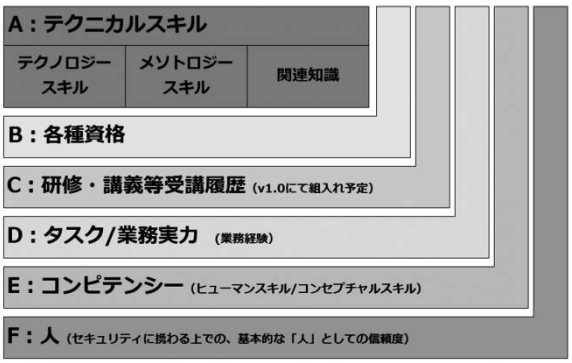
現在、メールを含むインターネットを利用しない業務は少なく、一人ひとりがセキュリティを意識する時代において、社内のセキュリティ担当者に求められることが増えています。

セキュリティ担当の方は何をきっかけにセキュリティ業務に携わるようになったのか、必要な知識をどのように学んだのかを調査しています。キャリアの在り方が多様化する時代となった今、学んだセキュリティ知識、業務経験を活かせるキャリア開発の在り方を検討していきます。このキャリア開発の在り方は認定ワーキンググループとも連携をしながら、キャリアと評価が連動する仕組みづくりを目指しています。

キャリアデザインワーキンググループの今後の活動として、中小企業や地方自治体などへもアプローチを試み、より幅広いキャリアの形を模索していきます。また、キャリアを築く『人』にもフォーカスを当てていく予定です。多くの業界で人材不足と言われる世の中、特に必要なセキュリティだからこそ、人が求めるキャリア形成の形が実現できるよう調査・検討を進めていきます。

■ 認定WG

認定WGではセキュリティ人材のスキル認定制度作りを念頭におきながら、まずは人材定義や業務定義、また、その尺度を統一させて真の実力値を判定する基準作りを進めています。先般、β版として「セキュリティ業務を担う人材のスキル可視化ガイドライン」を公開しました。



β版では図のA,B,Dを指標化するロジックを開発しました。かなりの打ち合わせ回数、時間を掛け綿密に練り上げています。

また、現在では正規版のリリースに向けてC,E,Fの組込みや全体判定するための仕組みを検討しています。並行してトライアルを実施しながら、それぞれの指標の精度を上げる検討も継続しています。

尚、目指す職務や役割に対しての効果的且つ効率的な教育や研修などのリファレンス化も並行して進めていきます。

■ 活動参加について

現在、主軸となって活動しているメンバーは業種や職種、ポジションや年齢など多岐に渡っています。結果として、それぞれのメンバーが多種多様な経験をもっていることで広い視点からの議論が展開されています。これはセキュリティベンダーや大企業に偏らないJTAG本来の姿へ向けて大きな力となっています。

尚、JTAGではシニア人材の再活躍仕組み作り、というテーマも盛り込まれています。少子高齢化や長寿化による個人の長い職業人生設計としてセキュリティ分野はチャンスが大きく、また、組織内外においての他分野からの人材流通の起爆剤にもなることから、メンバーの議論も自然と熱がはいります。

ご参加をお待ちしておりますので各WGの案内はJTAG事務局へご連絡ください。jtag-sec@jnsa.org

JNSA ワーキンググループ紹介

標準化部会　日本 ISMS ユーザグループ

日本 ISMS ユーザグループ　リーダー
NTT コムソリューションズ株式会社　魚脇　雅晴

■ 日本ISMSユーザグループについて

「日本ISMSユーザグループ(J-ISMSUG)」は、2004年より任意団体として活動しておりましたが、JNSAの広いセキュリティ活動と連結することで、その活動範囲/参加メンバの拡大、活動成果の有効活用を促進したく、この度JNSA標準化部会のWGとして新たに合流いたしました。

これまでJ-ISMSUGでは、ISMS認証取得企業とISMS専門家が、経験的な知識に基づく意見交換・議論を進めることでISMSの構築・運用に関わるベストプラクティスを提供し、日本におけるISMS普及・促進に貢献する目的で活動してきました。

活動概要

J-ISMSUGではISMSを構築・運用する上でISO/IEC 27001等の規格をどう読み解いて、企業活動にISMSを積極的に実践活用する方法を検討、研究し、国内外へ発信します。具体的にはISMS認証取得企業（ユーザ）とISMSの専門家が連携し、意見交換・議論を進めることでISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供し、日本における健全かつ効果的なISMS普及・促進に貢献する活動を行っています。J-ISMSUGには以下の主な活動があります。

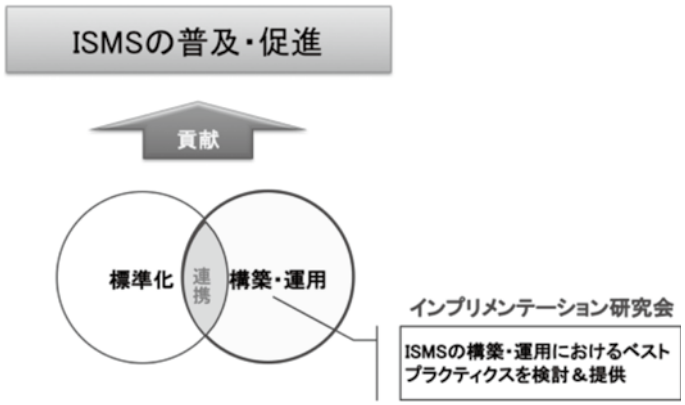


図.1　日本ISMSユーザグループの活動趣旨

- インプリメンテーション研究会におけるISMSの構築や運用における課題検討（毎月）
- 情報セキュリティマネジメントセミナーの開催と研究結果の発表（12月）

研究会の様子

1）インプリメンテーション研究会の活動紹介

J-ISMSUGでは、２００６年に2つのWG(以下の表）の活動を実施していましたが、ISMSの有効性測定を行うための「メジャメントWG」が一段落したため、それ以降はインプリメンテーションWG(インプリメンテーション研究会と呼ぶ）が毎月ISMSの構築や運用における課題検討を進めています。本研究会において扱うテーマとしては国際規格改定に伴う改定内容のブレークダウンや実際の運用現場で発生する課題を明確化し、対応方針や対応方法についての研究や、直近では企業を取り巻く環境の変化（サイバー攻撃、クラウド利用など）などに伴うリスクに対し、組織としてどう取り組むか研究しています。（表.1 過去のテーマ一覧参照）

表.1　過去のテーマ一覧

年度	インプリメンテーションWG	メジャメントWG
2006	■本WGの活動紹介＆ISMS導入に関する課題の事例紹介	■有効性測定の基本的な考え方＆取り組み事例紹介
2007	■情報セキュリティ研修・啓発 ■効率的リスクアセスメント	■有効性測定の基本的な考え方＆新たな取り組み事例紹介 （進捗状況含む）
2008	■ISMS構築事例に見る有効性測定構築の傾向 ■業務委託先のセキュリティ評価	■有効性測定の基本的な考え方＆共通フレームワーク案 （進捗状況含む）
2009	■標準的なリスク分類と具体的な管理策の対応のモデル化 ■管理策の有効性評価を効果的に行うモニタリング手法のモデル化	■ISO/IEC27001における「有効性測定」
2010	■標準的なリスク分類と具体的な管理策の対応のモデル化 ■管理策の有効性評価を効果的に行うモニタリング手法のモデル化	■ISO/IEC27001における「有効性測定」
2011	■可視化手法を用いたリスク対策モデル ■ISMS全体の有効性評価手法	■管理策の有効性測定
2012	■可視化手法を用いたリスク対策モデルとその実践的応用 ■ISMS実践手法　BCPのモデル化の検討	■管理策の有効性測定
2013	■ISMS推進事務局の悩みと解決策 ■有効性評価に基づくISMS実践活用	メジャメントWGは有効性評価に関する成果を持って活動を休止。インプリメンテーション研究会に一本化して活動。
2014	■ISMS推進事務局の悩みと解決策 ■ISMS規格改訂にともなう実装方法の検討	
2015	■ISMSを成功させる理想的なCISOの条件 ■減らないインシデントの特効薬	
2016	■サイバー攻撃を事例としたリスクマネジメントの実践 ■運用フェーズにおける有効性の評価	
2017	■現場と連携したリスクアセスメント手法の実践活用 ■内部監査を有効に運用するための手法の考察	
2018	■ISMS規格要求事項から紐解く最新のビジネス環境リスク （サイバー攻撃、クラウド利用への対応方法についての考察） ■働き方改革における情報セキュリティ	
2019	■最新の環境変化に伴うISMSの実装検討（活動中） ■各社の事例から学ぶISMSの実装について（活動中）	

JNSA ワーキンググループ紹介

2）情報セキュリティセミナーの開催

毎年１２月にJ-ISMSUGの活動内容の一般公開と非メンバとの意見交換を目的として、「情報セキュリティセミナー」を開催しています。本セミナーでは、J-ISMSUGの活動だけではなく、最新の国際標準化の動向、及び喫緊のサイバー攻撃の脅威などの情報共有も積極的に進めています。昨年は標準化動向として、ISO/IEC 27000ファミリー規格の最新動向やサイバーの概念、IoT、研究会の成果発表として最新のビジネス環境リスクや働き方改革等をテーマとして実施し、参加募集開始後、１週間もしないうちに満席状態となり、実際の参加人数も171名という盛況な結果となりました。

今後の活動について

今年も新しいテーマ（最新の環境変化に伴うISMSの実装検討＆各社の事例から学ぶISMSの実装）を設定し、インプリメンテーション研究会の活動を継続的に実施しています。今年は新規のメンバーも続々と参加して頂いており、これまで以上に活発な議論が期待できます。皆さんのご参加をお待ちしております。（飛び入り参加も大歓迎なのでJNSA事務局へご連絡頂ければ幸いです。）

会員企業ご紹介47

キヤノンマーケティングジャパン株式会社

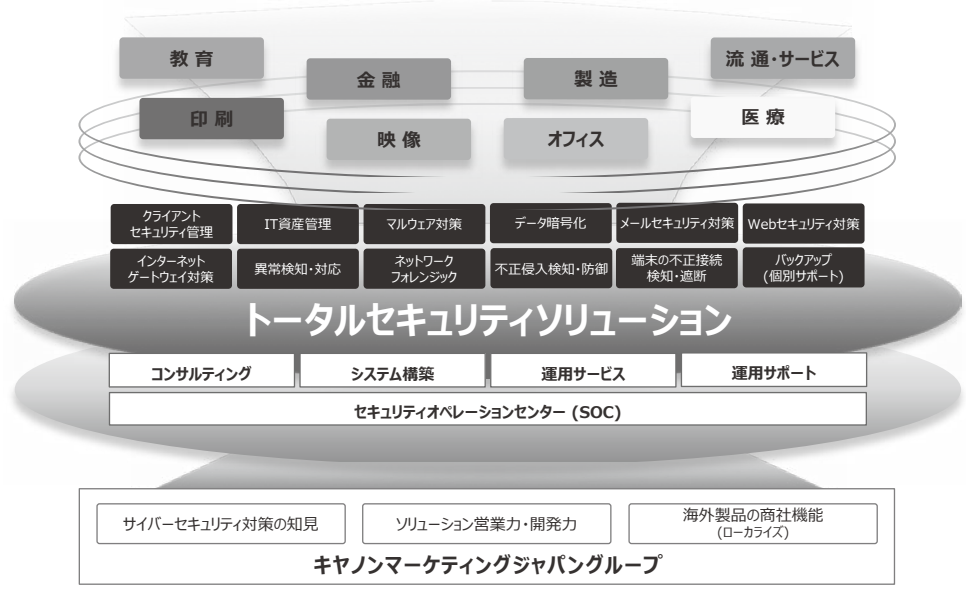
https://canon.jp/8060

Canon
キヤノンマーケティングジャパングループ

お客さまを深く理解し ともに発展することで 社会課題の解決に貢献していきます

キヤノンマーケティングジャパン※ は、キヤノン製品ならびに関連ソリューションの国内マーケティングを主な事業としています。ITソリューションとしてセキュリティソリューション事業を展開しており、国内および海外ベンダーの販売代理店として実績のある製品を用意するとともに、ITセキュリティ製品・サービスの自社開発などもしています。長年培ってきた情報セキュリティ対策に関する経験とノウハウをもとに、お客さまの様々な課題解決を目指した「トータルセキュリティソリューション」を提案しています。

※ 2019年1月より、ITセキュリティ事業の統括機能をキヤノンマーケティングジャパンが担い、グループ全体でソリューションラインアップの強化および事業領域の拡大を進めています。



主要ITセキュリティ製品・サービス

マルウェア対策ソリューション

ESETセキュリティ ソフトウェア シリーズ

総合情報漏えい対策ソリューション

GUARDIANWALLシリーズ

中小オフィス向けIT支援サービス

中小オフィス向けIT支援サービスHOME

マルウェア情報局

最新のマルウェアレポートや セキュリティトレンドなどの情報を発信

Web ｜ https://eset-info.canon-its.jp/malware_info/
Twitter ｜ @MalwareInfo_JP

セキュリティオンラインセミナー

いつでもどこでも自席に居ながら学べる セキュリティセミナーを開催

Web ｜ https://cweb.canon.jp/product/it-sec/seminar/webinars/

パーソルプロセス&テクノロジー株式会社

https://www.persol-pt.co.jp/

パーソルプロセス&テクノロジー株式会社は、パーソルグループの、「ITOセグメント」中核会社として、人・プロセスデザイン・テクノロジーの力で、ビジネスプロセスを変革し、人と組織の生産性を高めていくことを使命としています。
お客様の事業課題に応じたコンサルティングやシステム開発、アウトソーシングのほか、RPAやAIなどのあらゆるテクノロジーを駆使したサービスを通じて、グループで掲げる「はたらいて、笑おう。」のビジョンを実現してまいります。

主力事業

コンサルティング
業務アウトソーシングやシステム開発・運用だけでは解決できない、お客様が直面している課題や、将来起こる問題に対し、お客様と共に考え実行し、共に成果を創出いたします。

システムソリューション
お客様の事業課題に対し、企画段階から参画し、AI、RPAなどあらゆるテクノロジーから最適なソリューションを提案、お客様の事業価値の最大化を支援いたします。

アウトソーシング
優秀な人材と、多くのお客様の支援で培ったプロセス運用力で、日々の業務改善だけでなく、根本的な業務プロセス改革までを行い、お客様に伴走するパートナーとして事業成長に貢献いたします。

セキュリティサービスについて

パーソルプロセス&テクノロジーは、セキュリティ業務全般の常駐型セキュリティアウトソーシングを提供しており、官公庁や大手通信事業者をはじめ金融業、大手製造業、小売業、セキュリティベンダーなど幅広い業種のお客様をご支援しております。総合人材サービスならではの高い採用力・育成力に加え、独自のアウトソーシングのノウハウを実装した約100名からなるセキュリティエンジニア専門チームがお客様のセキュリティ課題を解決いたします。

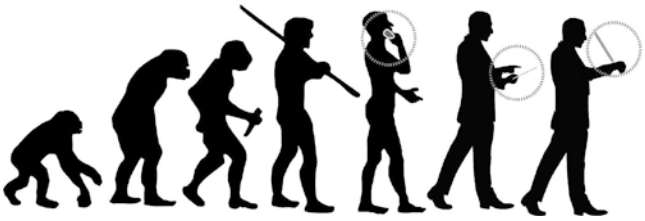
セキュリティアプライアンス設計・構築	セキュリティアプライアンス機器の選定/構築/検証/更新 主要プロダクト：次世代ファイアウォール/ロードバランサー/WAF/エンドポイントセキュリティサーバ/サンドボックス/UTM/WEBフィルタ/EDR等
SIEM設計・構築	SplunkをSIEMの設計/構築/導入 官公庁や金融業をはじめ様々な業種にSIEMの要件定義/設計/構築/専用アプリケーション開発/導入
セキュリティ運用・監視	イベント分析、インシデント検知、インシデントレスポンスをはじめとしたSOC（セキュリティオペレーションセンター）の定常運用及び運用手順書作成SOCアナリストとしてログ監視や問い合わせ対応等
脆弱性診断	脆弱性診断/対応トラッキング WebサイトCMSなどのWeb脆弱性診断を中心にOS/ミドルウェア/ネットワークなどの脆弱性診断
コンサルティング	情報セキュリティコンサルティング及びそのアシスタント GDPR施行前後に法対応及び初期運用・高度化支援、並びにセキュリティコンサルティング廻りのヒアリング・調査の実施、ドキュメント作成支援等

お問い合せ	パーソルプロセス&テクノロジー株式会社 TEL: 03-6385-6790　MAIL: marketing-ppt@persol.co.jp

株式会社ネクストジェン

https://www.nextgen.co.jp

CREATING NEW FORM OF COMMUNICATIONS



株式会社ネクストジェンは、通信キャリア向けのビジネスをメインとして2001年に創業しました。
以降、キャリア向けビジネスで蓄積した音声システムに関する技術力やノウハウを、エンタープライズ向けや、SIP/VoIPに特化したセキュリティ事業に応用し、多彩な製品・ソリューションを展開しています。

Security Solutions

SIP/VoIP セキュリティ診断サービス

通信事業者やSIP関連機器の開発ベンダー向けに、システムの脆弱性やセキュリティリスクに関する診断を実施し、検出したセキュリティリスクに適切な対策をご提案します。
これまでに国内外で50社、200件を超えるシステムに診断を実施、世界的に見ても有数の実績を兼ね備えたサービスです。

News BlueTC社およびTÜV TRUST社と共同で欧州大手通信キャリアのセキュリティ監査を実施
https://www.nextgen.co.jp/new/2019/04/2019040901.html

VoIP IDS & フォレンジック『NX-C6000 /NX-C6500』

問題解析の作業効率向上、サイレント故障やセキュリティ的な脅威の検出など、IP電話システムの保守上の課題を解決するために必要な機能を集約した、SIP対応ネットワークフォレンジック＆IDS製品です。

VoIP 診断ツール『NX-VNS』『NX-V3S』『NX-V3R』

NX-VNS :
多様なメソッド、コールパターン、プレゼンス/IM機能を実装し、複雑なシナリオもGUIで簡単に作成・実行が可能なSIP多機能シミュレータです。

NX-V3S :
SIPサーバーや端末の堅牢性を検証するためのファジングツールです。ネクストジェンが診断サービスで検出してきた問題を含む300万以上の異常SIPメッセージパターンを搭載、試験対象に潜在している脆弱性を検出します。

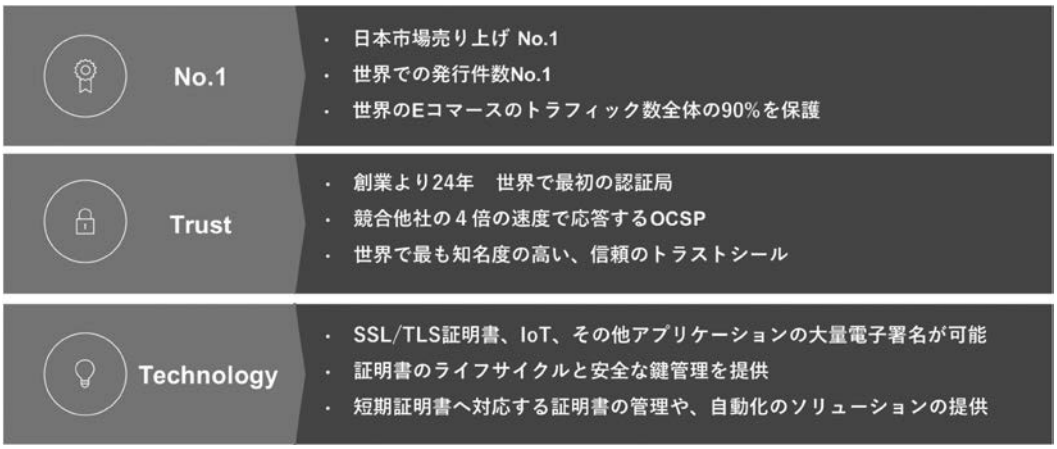
NX-V3R :
異常なRTPやRTCPパケットを送出して、サーバーや端末のRTP/RTCPスタックの堅牢性を検証するためのツールです。

Contact

株式会社ネクストジェン　技術企画部
TEL：03-5793-3230　問い合わせフォーム：https://www.nextgen.co.jp/contact/

デジサート・ジャパン合同会社
https://www.digicert.co.jp/

デジサート・ジャパン合同会社は、デジサート、シマンテック、ジオトラストブランドを配下に持つ、認証局世界最大手DigiCert Inc.の完全子会社である。SSL/TLSサーバ証明書、PKI、IoTセキュリティソリューションを国内で販売する。1996年に日本ベリサインとして認証局の運用を開始し、事業売却に伴い2012年にシマンテック、2017年にデジサートの子会社となった。



同社の主力製品の一つであるSSL/TLSサーバ証明書は法人向け証明書のトップシェアを占め、大手銀行をはじめ、業界を問わず様々な企業に導入されている。
SSL/TLSサーバ証明書はインターネット通信の暗号化及びウェブサイトの真正性を証明する手段として利用され、近年ブラウザがHTTP（非暗号化）通信を警告対象とみなすようになったことに伴い利用が大きく広がっている。証明書にはDV、OV、EVの3タイプがあり、同社が主に取り扱うのは企業の実在性を認証したうえで発行されるOV、EV証明書である。DV証明書は、ジオトラストブランドから販売されている。
同社の証明書導入顧客に配布されるノートン™セキュアドシールは認知度が高く、ウェブサイトに掲載することで信頼性をアピールするとともに、ロゴをクリックすることで認証情報の検証を可能とする。また、ウェブサイトが悪質なソフトウェアに感染の恐れがあることを警告するマルウェアスキャン、ハッカーによる攻撃で利用されるウェブサイトの弱点を特定する脆弱性アセスメント機能は同社のSSL/TLS サーバ証明書が持つ特徴である。

もう一つの主力製品であるDigiCert PKI Platformは、個人やその利用機器向けの電子証明書の発行、更新、失効管理するプラットフォームであり、アクセス管理、通信の暗号化、デジタル署名を実現させるソリューションとなる。大量の証明書に対応しているため、スケーラビリティが高く、様々な用途に対応し、企業規模に関係なく豊富な周辺サービスが利用できるように設計されている。

また、デジサートはPKI専業ベンダーとして高い知見と経験を持ち、ネットワークやIoT分野を中心に、様々な業種においてグローバルの規格化、標準化の活動に参画している。CA/ブラウザフォーラム、IETF/AllSeen Alliance/WiFi Alliance/IICのメンバーもしくはボードメンバー、ISOCのセキュリティーアドバイザーを務めており、Directed Exchange/NFCタグ/WFA Passpoint 2.0/CABF BR/.onion証明書等の標準の共同執筆の実績がある。

お問い合せ	デジサート・ジャパン合同会社 電話番号：0120-707-637（平日9：30～17：30）｜ Email：websales_jp@digicert.com

JNSA 会員企業のサービス・製品・イベント情報

■イベント紹介■

○最大3時間、無料で参加できるセキュリティ最前線
セミナー一覧（8月まで）
アシストのセキュリティ対策セミナーは、各種テーマで年間100名以上が参加。
標的型（サイバー）攻撃対策、ID管理やログ管理の最新情報と解決策が気軽に学べます。ハンズオンセミナーは製品の動作をお手元のPCで実体験いただけます。
【イベント情報詳細】
https://www.ashisuto.co.jp/pr/security/seminar.html
◆お問い合わせ先◆
株式会社アシスト　システム基盤技術統括部
E-mail: ssj_semi@ashisuto.co.jp

■製品紹介■

○あらゆる環境の特権IDを簡単かつ強固に管理
『特権アクセス管理ソリューション』】
組織内外の枠を超えて増加するサーバ。これらをメンテナンスする特権IDは大きなリスクを内包しています。アシストでは様々な環境の特権IDを簡単かつ強固に管理し、監査にも有効な証跡を取得するソリューションを提供しています。不正アクセスや情報漏洩の脅威を最小化しながら運用負荷を軽減することで、安全で円滑な業務の遂行に貢献します。
【製品情報詳細】
https://www.ashisuto.co.jp/product/theme/security/tokken-access.html
◆お問い合わせ先◆
株式会社アシスト　システム基盤技術統括部
E-mail: sk_info@ashisuto.co.jp

○「暗号鍵管理 SafeNet HSM」
SafeNet HSMは、オンプレミス、仮想、クラウド環境のアプリケーションによって使用される暗号鍵を厳重に保護します。
鍵のライフサイクル（鍵生成、保管、破棄）を通して、サーバ上に一切秘密鍵が出ることはありません。ブロックチェーン、GDPR、IoT、PCI DSS、デジタル署名、DNSSEC、証明書署名、データ暗号化などのソリューションでコンプライアンス要件に対処できます。
【製品情報詳細】
http://www.intellilink.co.jp/security/products/solution/Safenet_nw_HSM.html
◆お問い合わせ先◆
NTTデータ先端技術株式会社
セキュリティ事業部　セキュリティオペレーション担当
TEL: 03-5859-5426
E-mail: il-HSM-sales@intellilink.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いただけますので、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
◆お問い合わせ先◆
株式会社ユービーセキュア
E-mail: vex-sales@ubsecure.jp

○Morphisec（モルフィセック）
エンドポイントセキュリティ
MorphisecはMoving Target Defenseという、全く新しい技術を使用した次世代のAPT対策ソリューションです。
攻撃者が悪用するために必要なリソースを見つけることができないように、ユーザーメモリ空間の構造をプロセス生成時毎に変化させます。
これにより、シグネチャ・学習エンジンベースと違い、ゼロデイ攻撃だけではなく全く手法が違う攻撃も含めた高度な脅威を防ぎます。
アップデート不要、CPU負荷もプロセス生成時のみです。
◆お問い合わせ先◆
株式会社インテリジェント ウェイブ
Phone: 03-6222-7300
E-mai: iwi_security@iwi.co.jp

「RSA Conference USA 2019」JAPANパビリオン出展

海外市場開拓WGリーダー　一宮　隆祐（NEC）

JNSA海外市場開拓WGに参加する会員企業8社は2019年3月4日（月）から8日（金）にかけて米国 サンフランシスコで開催された「RSA Conference USA 2019」にJAPANパビリオンを出展いたしました。「JAPAN」冠のブースにて、各社が一丸となり自社製品・サービスをアピールした結果、パビリオンには日本を含む52か国 2,200名を超える来場があり、具体的な商談にも数多く繋がりました。

RSA Conference USA 2019 概要

名称：RSA Conference USA 2019　https://www.rsaconference.com/events/us19
会場：米国 サンフランシスコ, “Moscone Center”
日程：2019年3月4日（月）-　2019年3月8日（金）[展示会は7日まで]

JAPAN パビリオン出展企業

1. アドソル日進株式会社
2. アルプスシステムインテグレーション株式会社（現地名称NetSTAR）
3. 株式会社インフォセック
4. エムオーテックス株式会社（現地法人Interfocus）
5. 国立研究開発法人情報通信研究機構（NICT）
6. 株式会社ディアイティ
7. 株式会社日立システムズ
8. 日本電気株式会社株式会社（NEC）

概要

RSA Conference USA 2019には約43,000名、700社もの企業・組織が出展。国際パビリオンとしては、日本を含む8カ国（日本、イスラエル、ドイツ、カナダ オンタリオ州、スペイン、英国、韓国、中国北京Z-Park）が出展し、自国の企業を支援・アピールをしていました。

JAPANパビリオンはRSA Conference USA へ初出展ということもあり、場所の確保に苦労をしました。出展場所の確保は、スポンサーや前回出展企業が優先されるため、2018年4月に予約がオープンになった時点でほぼ埋まり、初出展企業は後回しにされます。初出展企業の場所の確定は何度も延期された末、2018年8月に出展スペースを確保できました。

今回、JAPANパビリオンは濃紺『サムライブルー』をベースに造作し、パンフレットや寿司消しゴムをノベルティとして活用しながら集客に努めました。特にノベルティの“寿司消しゴム”に目を止め、それをきっかけにブースでのデモ、リードを獲得する流れが多くありました。その他にも、1時間に一度ミニプレゼンを行い、小さいブースながらもJAPANパビリオンは賑わいをみせ、具体的な商談にも数多く繋がりました。

イベント開催の報告

また、3月6日（木）の夜には、近くの日本食レストランの一角を貸し切り（100人規模を想定）、日本食を食べながらネットワーキング、商談を行うことを目的としたレセプション「Sushi Night」を開催しました。RSA Conferenceの来場者に対してチラシを配布し、集客を行いました。雨が降っており、展示会場からも離れていたため集客に苦戦することを予想していましたが、開場前から店外に列ができ、想定を遥かに超える200人以上が来場する結果となりました。多少の混乱はあったものの、運営メンバーの奮闘とお店の協力により、事故もなく無事に終えることができました。本来のレセプションの目的はあまり達成できず、運営面での課題・反省はありますが、日本食人気を肌で感じことができ、日本人の誇りを感じる瞬間でした。

JAPANパビリオンは国際パビリオンとしては最小のスペースながらも、計4日間で52か国 2,200名を超えるリードを獲得できました。実際に展示員としてブースに立つと、予想以上に日本や日本のサイバーセキュリティ製品・サービスに興味を持っていることを感じました。出展企業によっては、北米進出や販路拡大となりえる商談もあり、本出展の有効性が検証できたことは日本のサイバーセキュリティ産業としても大きな成果と言えます。この成功を足掛かりに、今回の反省を活かし、次回のJAPANパビリオン出展に繋げていきたいと考えています。

最後にJAPANパビリオン出展・運営においては、本当に多くの方々にご支援・ご協力を頂きました。この場を借りて感謝申し上げます。

JNSA海外市場開拓WGでは、海外展示会への出展や海外市場調査、海外進出マニュアルの作成、メンバー企業間での情報共有などの活動を行なっています。また、RSA Conference USA 2020（日程・場所は下記をご参照ください）への出展を予定しております。海外ビジネスを既に実施している企業、海外進出を計画中の企業、また海外事業に関心のある個人など、ぜひお気軽にWGへご参加ください。

RSA Conference USA 2020 概要
会場：米国 サンフランシスコ, “Moscone Center”
日程：2020年2月24日（月）－ 2020年2月28日（金）

PKI day 2019 「IoTのトラスト」「トラストサービスの在り方」

セコム株式会社 IS 研究所
JNSA PKI 相互運用技術 WG リーダー　松本　泰

◆はじめに

今年度のJNSA PKI相互運用技術WGと電子署名WGが主催するセミナー PKI Day 2019 [1]は、2019年4月17日に140名余りの参加者のもと開催されました。毎年、恒例となっているPKI day ですが、ここ数年は、Society5.0等にみられる社会の変化に対応したPKIとトラストをテーマに開催しています。

今回PKI day では、午前の部において「IoTのトラスト」、午後の部においては「トラストサービスの在り方」というトラストを中心にそえたテーマで、それぞれ講演とパネルディスカションを行い、密度の濃い議論が展開されTRUST day とも言える1日になりました。

◆午前の部 「IoTのトラスト」

午前の部の「IoTのトラスト」では、低コストで高機能なIoTデバイスに組み込まれた暗号技術をベースとした「IoTのトラスト」について、標準化の観点、プラットフォームの観点、半導体(SoC: System-on-a-Chip)の観点等から、その意義等も含めた議論がなされました。

午前の部の「IoTのトラスト」の講演者とパネルディスカションの登壇者は、以下の通りです。

【講演】	IoTにおけるトラスト実現に向けた技術的な仕組み 講師:株式会社レピダム　代表取締役　菅野 哲 氏
【講演】	セキュアなIoTを構築する技術 − Azure Sphere、Azure IoT Hubの場合 講師:日本マイクロソフト株式会社　エバンジェリスト　太田　寛 氏
【講演】	IoTセキュリティ強化のための技術戦略解説 講師:SHコンサルティング株式会社　代表取締役社長　河崎 俊平 氏
【パネルディスカション】「IoTのトラスト」	
モデレータ: 松本　泰 氏　セコム株式会社 IS研究所 パネリスト: 菅野　哲 氏　株式会社レピダム　代表取締役 太田　寛 氏　日本マイクロソフト株式会社　エバンジェリスト 河崎　俊平 氏　SHコンサルティング株式会社　代表取締役社長	

午前の部「IoTのトラスト」では、異なる観点からのパネルディスカションでの議論を念頭に、立場の異なる3名の方に講演して頂きました。

最初の講演者の菅野氏からは、IETFにおけるIoTのトラストに関わる標準化の動向などを中心に講演して頂きました。IETFにおいて、メモリやCPU等に関して制約のあるデバイスを前提としたプロトコル等の標準化が盛んに議論されていますが、この制約のあるデバイスにおいてトラストを実現するための仕組みの検討について紹介がなされました。紹介された中でアテステーションに関する標準化の話がありましたが、これはIoTデバイス等が自身の正当性を証明する仕組みの中心となる概念でもあり、今後、非常に注目される動向になるかと思います。

二人目の講演者の太田氏からは、マイクロソフトのIoTプラットフォームであるAzure Sphere、Azure IoT Hubについて講演して頂きました。このAzure Sphere 等のIoTプラットフォームは、サービスとして

完成度が高く、その意味するところは比較的分かり易かったかと思います。PKI day 的には、Azure Sphere のコアコンポーネントのひとつである Azure Sphere MCU、更には、このMCUに組み込まれた暗号モジュールであるPluton security Subsystem等の紹介から、IoTにおいて暗号技術を実装することの目的や意義の理解が深まったのではないでしょうか。

最後の講演者の河崎氏からは、IoTの実体とも言えるSoCにおいて、ハードウェアーセキュリティを実現するアーキテクチャや、こうしたSoCの開発動向、更にSoCの製造、IoTデバイスの製造、サービスに至る鍵管理などサプライチェーンについて話して頂きました。昔、半導体は「産業の米」といわれていた時代がありましたが、膨大な数のIoTは、膨大な数の半導体とその生産に支えられ、これらに暗号技術が組み込まれていくことを実感させられるお話だったかと思います。

パネルディスカションでは、松本がモデレータを務め、この立場の異なる3名の方の話から「IoTのトラスト」の話を噛み合わせるべく、議論を進めました。バズワード化しているIoTに対して、抽象的な概念でもあるトラストという難しいテーマではありますが、この「IoTのトラスト」に関連する様々な活動の紹介等から、その意味するところが理解できたかと思います。また、この「IoTのトラスト」が、今後のIoTに関連するビジネスを進める上でも、また、IoTに関連した産業競争力を高める上でも重要だという認識が深まったのではないでしょうか。

◆午後の部 「トラストサービスの在り方」

午後の部の「トラストサービスの在り方」では、トラストサービスの関わる世界の動向、トラストサービスに 関する技術と法制度の在り方や、日本で議論すべきトラストサービスとは何か等について議論されました。

午後の部の「トラストサービスの在り方」の講演者とパネルディスカションの登壇者は、以下の通りです。

【講演】	米国航空産業で利用されるPKI **講師**:株式会社コスモス·コーポレイション　濱口 総志 氏
【講演】	英国オープン·バンキングにおけるトラストの確立 **講師**:株式会社野村総合研究所 IT基盤技術戦略室 上席研究員　崎村 夏彦 氏
【講演】	Society5.0を支えるトラストサービスとトラスト基盤 **講師**:慶應義塾大学　大学院政策メディア研究科 特任教授　手塚　悟 氏
【パネルディスカッション】「トラストサービスの在り方」	
モデレータ:	佐藤　雅史 氏　JNSA 電子署名WGサブリーダー /JT2A 運営委員
パネリスト:	宮内　宏 氏　宮内·水町IT法律事務所　弁護士
	宮地　直人 氏　有限会社ラング·エッジ
	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
	濱口　総志 氏　株式会社コスモス·コーポレイション
	崎村　夏彦 氏　株式会社野村総合研究所　IT基盤技術戦略室 上席研究員

午前の部「トラストサービスの在り方」では、そもそも、トラストとは何か、トラストサービスとは何か、なぜ、トラストが重要になっているのかといった、より本質的な議論を念頭に3名の方にご講演して頂きました。

現在、こうした議論と類似した活動が、総務省の「プラットフォームサービスに関する研究会 [2]」と、その配下の「トラストサービス検討ワーキンググループ」で行われていますが、今回の講演者、パネリストの崎村氏、手塚氏、宮内氏は、この研究会の構成員でもあります。

最初の講演者の濱口氏からは、米国の航空業界におけるPKIの利用事例をお話し頂きましたが、この話題は、午前中の「IoTのトラスト」にも繋がる話でもあり非常に興味深いものでした。それは、(大型の)航空機のソフトウェアのサプライチェーン管理は、PKIによる署名の連鎖(Chain of Trust)により検証され、また、個々の航空機の運行管理における航空機を取り囲む様々なステークホルダーの信頼関係の構築、維持にもPKIが利用されているというものでした。

二人目の講演者の崎村氏は、総務省の研究会の構成員でもあり、プラットフォームビジネスおよびトラストに関して造詣の深い方になります。講演の前半は、ずばりトラストについての見解を話されましたが、ここでは「トラストの本質は、確認しないこと」という、これは当事者に代わって、トラストサービスプロバイダー等が確認していることを意味しますが、これに関しては、この後のパネルディションでも大いに議論されました。崎村氏の講演の後半は、英国オープン・バンキングにおけるトラストの実装事例と、その実装にまつわる数々の課題に関するもので、これも大変興味深い話をして頂きました。

最後の講演者である手塚氏は、総務省の研究会の構成員でもあり、またワーキンググループの主査でもありますが、この研究会とワーキンググループにおける議論や、こうした研究会が立ち上がった背景などについて、非常に広範囲な話をして頂きました。

パネルディスカションでは、３名の講演者のほか、欧州におけるトラストサービスの標準化に詳しい宮地氏と、「プラットフォームサービスに関する研究会」の構成員である弁護士の宮内氏も加わり、トラスト、および、トラストサービスに関する法制度のあり方や技術の標準化など多角的な議論が展開されました。ここでの議論の内容は、非常に広範囲で、また深く、とても短い紙面で説明できるものではありません。総論としては、今後の社会(Soceity5.0、超スマート社会)においてトラストは、益々重要になるが、そのトラストの実現には多くの課題があり、その課題解決向けて様々な努力が必要になるといったことになろうかと思います。

◆おわりに

今回のPKI dayでは、ここ数年のPKI day と同じく、Society5.0等にみられる社会の変化に対応したPKIをテーマに開催しました。

超スマート社会において、また、経済等がグローバル化する中、個人や組織、更にモノ(IoT)は、時間や空間を超えた非常に複雑な信頼関係が求められており、その求めに応じるのがIoTのトラストであり、また、トラストサービスの役割となると考えられます。

参考文献

[1] PKI day 2019
https://www.jnsa.org/seminar/pki-day/2019/

[2] 総務省プラットフォームサービスに関する研究会
http://www.soumu.go.jp/main_sosiki/kenkyu/platform_service/index.html

事務局お知らせ
JNSA ANNOUNCE

後援・協賛イベントのお知らせ

1. Interop Tokyo 2019
主　催：Interop Tokyo 実行委員会
日　程：2019年6月12日～14日
会　場：幕張メッセ・国際会議場

2. Iotセキュリティウィーク 2019 by CCDS
主　催：一般社団法人重要生活機器連携セキュリティ協議会
日　程：2019年6月17日
会　場：東京大学 一条ホール

3. サルオフ#1- 署名ブタ野郎は認証先輩の夢を見ない
主　催：OsSAL オープンソース署名&認証ラボ
日　程：2019年6月19日
会　場：浅草橋ヒューリックホール カンファレンス

4. 日本セキュリティ・マネジメント学会　全国大会
主　催：一般社団法人日本セキュリティ・マネジメント学会
日　程：2019年7月6日
会　場：株式会社日立製作所中央研究所

5. INTERPOL World 2019
日　程：2019年7月2日～4日
会　場：Sands Expo and Convention Centre, Singapore

6. セキュリティ&リスク・マネジメントサミット 2019
主　催：ガートナー ジャパン株式会社
日　程：2019年8月5日～7日
会　場：ANAインターコンチネンタルホテル東京

7. JAIPA Cloud Conference 2019
主　催：日本インターネットプロバイダー協会
日　程：2019年9月5日
会　場：品川グランドホール

8. サイバーセキュリティ TOKYO
主　催：都立産業技術高等専門学校
日　程：2019年9月28日、29日
会　場：都立産業技術高等専門学校

9. GartnerSymposium／ITxpo 2019
主　催：ガートナー ジャパン株式会社
日　程：2019年11月12日～14日
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 2019 ◆

Gartner

デジタル化が加速する現在、セキュリティは誰かの特別な問題ではなく、誰にとっても当たり前の問題となっています。セキュリティはユビキタスなものであり、あらゆるビジネス活動の根底には必ずセキュリティのファンダメンタルが存在します。本サミットでは、新たな時代に向けて、セキュリティ／リスク管理のリーダーはどのようにリーダーシップを発揮し、何をすべきなのかについて、実践的な提言を行います。

【主なトピック】
- サイバーセキュリティ、脅威管理、デジタルへの信頼
- より安全なクラウド・コンピューティングの実現
- スマート・マシーン、AI、モノのインターネットにおけるリスクと可能性
- デジタル・ビジネスにおけるモバイル・セキュリティ　他

【会　　期】
2019年8月5日（月）・6日（火）・7（水）

【会　　場】
ANAインターコンチネンタルホテル東京

【参加料金】
2019年6月24日（月）まで
→ 早期割引価格　128,000円（1名様・税別）
2019年6月25日（火）以降
→ 通常価格　145,000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
⇒ https://gartner-em.jp/srm/

JNSA部会・WG2019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／Japan Digital Design 株式会社

日本でもサイバーセキュリティがビジネスとして成立する時代となり、様々な社会問題が提起される事となってきた。そのような中、JNSAがサイバーセキュリティ界における、社会問題の解決者として、今まで以上に社会に貢献していくために、従来から行ってきた活動の見直しを行うとともに、政策提言活動を行っていく。

具体的には、適正なセキュリティ事業遂行の促進、業界団体としての政策提言のとりまとめ、政府と協力した政策の促進、メディアや市場の力を活用した普及啓発活動、外部組織支援、国際・他団体連携などを行う。

【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、RSA Conference USA 2020およびその他の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、セキュリティ専門家人狼（英語版）を通じて、JNSA発のコンテンツの海外展開の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。

さらにセキュリティ事業に特化した輸出関連の勉強会（成果物）も検討を進める。

＜予定成果物＞

- セキュリティ専門家人狼（英語版）プロモーション動画
- 海外市場進出ガイド改版
- 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ハンドブックをより実践的な内容にしたPhase-2を作成し公開する。

＜予定成果物＞

- CISOハンドブック Phase-2

【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。

【サイバーセキュリティ小説コンテスト実行委員会】

（実行委員長：本川祐治 氏／株式会社日立システムズ）

サイバーセキュリティを取り巻く環境が年々厳しさを増す中、広くサイバーセキュリティ意識の向上が不可欠であると考え、コンテンツがもつ拡散力に注目し、セキュリティ知識の普及とネットリテラシーの向上、ネットを守るハッカーへの興味とイメージアップ、セキュリティ人材育成を促進することを目的として、Web小説サイト「カクヨム」上で、サイバーセキュリティ小説コンテストを2018年度に初開催し、今年度も引き続き開催する。

＜活動予定＞

スポンサーの募集

- 応募者向けの情報提供、Q&A対応
- 応募者向けの施設見学会
- 応募者向け説明会の開催
- コンテスト結果発表と表彰式の開催

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）

2018年の個人情報漏えいインシデント調査のデータを分析し、報告書を公表する。2019年の個人情報漏えいインシデントの収集を行う。

個人情報漏えいインシデント調査の新しい体制を検討し、構築へ向けた準備を行う。被害報告(報道や報告書)様式の検討結果をまとめ、公表する。

＜予定成果物＞

- 2018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）様式の検討結果報告書

【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＞

- 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に関連するセキュリティの啓発を目的としたセミナーを開催するとともに、IoTセキュリティを導入するための、すぐに使えるガイドの作成と公開に向けた活動を行う。

＜予定成果物＞

- （仮題）IoTセキュリティを導入するためのすぐに使えるガイド

【脅威を持続的に研究するWG】

（リーダー：甲斐根功 氏／株式会社日立システムズ）

昨年度に引き続き、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とともに、情勢に応じた旬なネタを集めた情報交換会を実施する。また、公益社団法人日本医業経営コンサルタント協会と連携し、医療分野机上演習を実施する。本年度は、2018年度作成の医療分野シナリオを基に病院職員を対象に、近畿地区協議会の各支部主催（支援：研究会）において横展開を図る。

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。

【デジタルアイデンティティWG】

（リーダー：宮川晃一 氏／日本電気株式会社）

エンタープライズにみならず、広くデジタルアイデンティティに関する様々な課題を検討し、デジタル社会の基礎ととなるIDの重要性の啓蒙やプライバシー関連の問題提起等を行う。

＜予定成果物＞

- 認証要素、認可要素、その関係の整理（研究レポート）
- クレデンシャル情報の歴史の整理（研究レポート）

【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、及び国際標準化（IoTエラーログに関する）の支援を継続的に実施する。また、韓国KISIAとの意見交換会を継続し、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としての貢献を本格化していく予定である。

＜予定成果物＞
- 日韓連携作業によるIoTセキュリティガイドライン（案）
- ITU-T勧告草案 “Standard format of IoT error logs for security incident operations (X.elf-IoT)”

【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

【IoT機器セキュリティログ検討WG】
（リーダー：渥美清隆 氏／株式会社ラック）

「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＞
- 未定

【日本ISMSユーザグループ】
（リーダー：魚脇 雅晴 氏／
NTTコムソリューションズ株式会社）

ISMS認証取得企業（ユーザ）とISMSの専門家が連携し、意見交換・議論を進めることでISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供し、日本における健全かつ効果的なISMS普及・促進に貢献する活動を行う。

＜予定成果物＞

必要に応じて、成果物として以下に関連するものをまとめ、公開する。
- 「最新の環境変化に伴うISMSの実装検討」
- 「各社の事例から学ぶISMSの実装について」

【PKI相互運用技術WG】
（リーダー：松本泰 氏／セコム株式会社）

PKIの相互運用を中心に、情報交換を行い、その方向性をPKI day などのイベントで公開していく。

＜予定成果物＞
- PKI day 2019の開催資料

4. 教育部会

部会長：平山敏弘 氏／株式会社アイ・ラーニング

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SecBoK2020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。2019年度も引き続き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す。

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。

SecBoK2020更新版の作成、および大学での使用事例などを盛り込んだ利用ガイド版作成などの活動を実施する。

＜予定成果物＞
- 大学シラバス対応版
- SecBoK2020の検討および作成

【ゲーム教育WG 】
（リーダー:長谷川長一 氏／株式会社ラック）

情報セキュリティ学習をテーマとしたゲームの企画・開発、普及啓発、及びそれらに関わる実証実験活動を行う。

＜予定成果物＞
- 「Malware Containment」デジタル版
- 「Malware Containment」ファシリテーターガイド及び附属書

【情報セキュリティ教育実証WG】
（リーダー：平山敏弘 氏／株式会社アイ・ラーニング）

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＞
- 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）

会社の枠を超えた連携を目的として、女性セキュリティエキスパートの交流場所を提供するとともに、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ための活動を行う。

勉強会を開催し、テーマはWG参加者の意見を検討して決定する。

5. 会員交流部会

部会長：萩原健太 氏／
グローバルセキュリティエキスパート株式会社

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。またセキュリティ理解度チェックについても利用者の増加に伴い、安定的に運用可能な環境の整備強化を検討する。

なお、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は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／
グローバルセキュリティエキスパート株式会社）

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（有料サービス）のユーザ数増加に向けた対外活動を実施する。

プレミアム版の利用者の増加に伴い、安定的に運用可能な環境の整備強化を検討する。

＜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
- 必要に応じてシステム改修（検討中）

【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。

今年度は検索ロジックの見直し作業を行う予定。

＜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）

WGメンバーの情報交換を目的として、会合を開催する。

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

WG成果物普及促進やマーケティング知識習得により、JNSAの認知度向上、会員獲得を目的とした活動を軸に運営を行う。主な活動としては、会員企業増加施策の企画、会員企業向け勉強会のほか、全国セミナーの実施など。

＜予定成果物＞

- 全国セミナーの実施
- ブランドガイド作成
- その他ノベルティ等の検討

7. 事業コンプライアンス部会

部会長：西本 逸郎 氏／J株式会社ラック
事務局：唐沢 勇輔 氏／Japan Digital Design 株式会社

サイバーセキュリティサービスの提供者が、ネットワーク社会、サービスを享受するお客様、そしてサービス従事者として自らを守るために、適正なセキュリティサービス事業遂行の在り方について検討する。

2018年度の「サイバーセキュリティ事業における適正な事業遂行の在り方に関する検討委員会」にて取りまとめた「サイバーセキュリティ事業者行動規範（案）」と「サイバーセキュリティ事業者の基本指針（案）」について継続して議論を実施し、今後の運用方策含めて検討を行い、成果物として公開する。

8. 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。

【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。

＜予定成果物＞

- 中小企業において目指すセキュリティデザイン（仮称）

9. 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。

10. 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

情報セキュリティ教育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目的として活動する。

また、キュリティ人材の不足に対して、人材育成やキャリアパスの検討を行うための活動「JTAG（ジェイタッグ）」を継続する。

＜予定成果物＞

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

11. 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

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活動する。

例年通り、ワーキンググループを単位とした活動を行う。

WGの他、次のタスクフォース、プロジェクトを立ち上げ、活動を行う。

- TF（セキュリティサービス認定検討タスクフォース）
  経済産業省サービス高度化検討会の事務局からの問い合わせ対応を行う。
- 新技術とオペレーションPj
  新技術がもたらすセキュリティ運用の影響についての議論・検討を行う。

＜新技術とオペレーションPj：年間活動予定＞

新しい技術に関して、メンバーが雑談レベルから情報交換ができる場を立ち上げます。

個別の技術トピックについて集中的に勉強会を実施して、参加者の理解とセキュリティオペレーション観点からの議論を深めます。

メンバー数の増加、会員企業所在地の分散などに対応するため、通常の会合とオンラインサービスを使った会合を組み合わせたグループ運営を試行します。

＜予定成果物＞

- ペネトレーションテストに関連したガイドライン

- 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」 v3.0
- InternetWeek2019での公開向け資料
- 新技術とオペレーションPJ：参加者間での講義ノートなどの共有
- ISOG-Jメンバーへの勉強会サマリ共有

【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／株式会社川口設計）

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つつ、他の団体やユーザー企業などとの連携強化を検討し、さらなる価値向上を目指す。

【セキュリティオペレーション連携WG】

（リーダー：武井滋紀 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。検討や議論の結果の各種成果物を公開し、業界団体や一般ユーザー向けへの知見の提供を行う。

12. 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ことを目的として活動する。

リモート署名TFと真正保証TFでそれぞれ活動を行う。

リモート署名TFでは、引き続きモート署名ガイドラインの作成を進める。真正保証TFでは、本人確認に関するテクニカルガイドブックを作成する。

＜予定成果物＞

- リモート署名ガイドライン
- 本人確認に関するテクニカルガイドブック（各府省情報化統括責任者（CIO）連絡会議発行）
- B2B向け本人確認に関するテクニカルガイドブック

13. 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77名の学生の参加があった。

14. 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

今年度も協賛企業の協力を得て、SECCONを開催予定。

また、情報セキュリティ技術を向上できる初心者向け勉強会「SECCON Beginners」を全国各地で開催するほか、女性限定ワークショップ「CTF for GIRLS」開催し、情報セキュリティ人材の発掘・育成と国内の情報セキュリティレベルの底上げを図る。

JNSA 役員一覧　2019 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　日鉄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
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
本城　啓史　株式会社エヌ・ティ・ティ・データ
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　キヤノンマーケティングジャパン株式会社
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
日向　　亨　トレンドマイクロ株式会社
平山　敏弘　株式会社アイ・ラーニング
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　日本エレクトロセンサリデバイス株式会社
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
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／日本エレクトロセンサリデバイス株式会社
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　2019年6月現在　233社　50音順

【あ】

(株)アーク情報システム
(株)IHIエスキューブ　New
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)
(株)アイ・ラーニング　New
アイレット(株)
アクセンチュア(株)
アクモス(株)
(株)アシスト　New
(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)
(株)網屋
アライドテレシス(株)
アラクサラネットワークス(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)
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)
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
(株)NTTファシリティーズ エンジニアリング　New
(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
キヤノンマーケティングジャパン(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)ケイテック　New
(株)ケーエムケーワールド　New
(株)km2y
KDDI(株)
KPMGコンサルティング(株)
コインチェック(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】

ServiceNow Japan(株)　New
サイエンスパーク(株)
(株)サイバーエージェント

（株）サイバーセキュリティクラウド New
（株）サイバーディフェンス研究所
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
JBCC（株）
一般社団法人 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
Japan Digital Design（株） New
情報セキュリティ（株）
（株）信興テクノミスト
ストーンビートセキュリティ株式会社 New
（株）Speee
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
（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リスクマネジメント（株）

【た】

大興電子通信（株）
大日本印刷（株）
（株）大和総研ビジネス・イノベーション New
（株）宝情報
タレスジャパン（株）
（株） 中電シーティーアイ
TIS（株）
（株）ディアイティ
デジサート・ジャパン合同会社 New
デジタルアーツ（株）
（株）デジタルハーツ
鉄道情報システム（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）
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）
トレノケート（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）
日鉄ソリューションズ（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
（株）日本ソフトウェア特許開発
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）
（株）日立システムズ
（株） 日立製作所

(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)
(株)PFU
PwCコンサルティング合同会社
華為技術日本(株)
ファイア・アイ(株)
(株)ファインデックス
(株)VSN
(株)フーバーブレイン
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
(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
(株)メルカリ New

【や】

株)ユービーセキュア
ユニアデックス(株)
(株)YONA

【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
(有)ロボック

【わ】

(株)ワイズ

【特別会員】

一般社団法人 IIOT
(ISC)2　Japan
一般財団法人 沖縄ITイノベーション戦略センター
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
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
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トラストサービス推進フォーラム

他二社

JNSA 年間活動（2019 年度）

4月	4月12日	第1回　幹事会
	4月17日	PKI Day 2019
	4月27日	産学情報セキュリティ人材育成検討会　交流会
5月	5月10日	2019 年度　理事会
6月	6月12日	JNSA 2018 年度活動報告会 / 2019 年度総会（ベルサール神保町）
	6月21日	第11回　CTF for GIRLS
7月		
8月	8月24日	SECCON　Beginners（苫小牧工業高等専門学校）
	9月1日	CTF for School GIRLS
9月	9月7日	SECCON　Beginners（石川工業高等専門学校）
10月	10月5日	SECCON　Beginners（東京都立産業技術高等専門学校）
	10月19日・20日	SECCON CTF 予選（インターネット）
	10月26日	SECCON　Beginners（九州大学伊都キャンパス内）
11月		
12月	12月21日・22日	SECCON 2019（CTF・カンファレンス）
1月	未定	NSF 2019
	未定	賀詞交換会
3月	未定	NSF 2019 in　Kansai

★ 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。）

アドソル日進株式会社　野田　俊夫

JNSA会員の皆様、はじめまして。アドソル日進の野田（のだ）と申します。
このたび事務局からの主命（?）により本稿を書かせていただきます。

簡単に経歴を紹介させていただきます。
1999年　アドソル日進入社
　　基幹ネットワーク管理と最新技術のキャッチアップを担う部署に所属
2005年　各部署を転々と異動
　　ネットワーク系の技術者としてシステム開発に携わる
2014年　セキュリティ関連部署に異動
2015年　JNSAとの出会い
2019年　情報システム部に異動
　　次世代社内ITの導入推進を担当。

入社当時は好奇心が旺盛で新技術に飛びつく傾向があるため、まだ枯れてない技術を用いて痛い目を見ることが人よりも多かったと思います。それも最終的には知見を広め技術習得に結び付くことになり、それぞれの挑戦は無駄な努力ではなかったと考えています。当初からセキュリティへの興味はありましたが、どちらかというと「いかにかい潜るか」を考えることが多く、その点においては労を惜しまない性格でした。もともとネットワーク系のスキルがあり加えてセキュリティに関連する資格をたまたま取得したため、弊社がセキュリティに関して力を入れ始めた5年ほど前にセキュリティの関連部署へ異動し、そしてこの異動がJNSAとの貴重な出会いのきっかけになりました。

新しい部署ではセキュリティ対策プラットフォームのプロダクト開発に携わり、販売支援のコンサルを中心に活動しました。そのため「セキュリティ」というものが社会にどのような影響を与えるのかを学ぶ目的でJNSAの社会活動部会への参画を決めました。

社会活動部会へ参加したときは、ちょうど年金機構の件で盛り上がっていた時期でした。部会の方々は関係省庁の方々との意見交換会では「他社の手本となるような情報公開」について前向きな議論を交わし、省庁の方々も真摯に耳を傾けていました。正直影響力の大きさを目の前で実感し、驚いたことを覚えています。

この業界で5年ほど活動して時折自分自身が「ひょっとしてこの業界にむいている?」と感じる時があります。セキュリティの対策を考えるうえで重要な要素の一つに「攻撃側の視点で考える」ことがあります。ショートカットや、抜け道を積極的に探す本来の性格?にマッチしているからと自己分析していますが…実際のところはどうでしょうか。

プライベートでは週末にバイクを乗っています。社会人になり免許を取得してから2台ほどのっていますが、まだ大型のバイクには今まで縁がなく乗ったことがありません。先日たまたま先輩ライダーの方から「大型乗りたいなら体力的にも早いほうがいい」と助言され、もうそんな心配される歳になったのだと感じつつ、せっかく免許を持っているのだから今年はぜひ大型にバイクにのるべく計画を立てています。おすすめのバイクがあればぜひ教えてください。

最後になりますが、今後も社会活動部会の皆様とともにセキュリティ業界の発展に尽くせるよう精進していきたいと思います。まだまだ勉強が足りない身ですが、今後ともよろしくお願いいたします。

三井物産セキュアディレクション株式会社　洲崎　俊

JNSA会員の皆様、三井物産セキュアディレクションの洲崎と申します。この度、株式会社ユービーセキュアの田中様よりご紹介をいただき、こちらでご挨拶させていただきます。

私は、脆弱性診断やペネトレーションテストなどを中心としたセキュリティサービスの提供に従事しているセキュリティエンジアです。JNSAでの活動としては、ISOG-J（日本セキュリティオペレーション事業者協議会）のWGに参加させていただき、自分の専門としている脆弱性診断サービスに関して診断実施者のためのスキルマップやガイドラインの作成、初心者向けのハンズオントレーニングの提供などに携わらせていただきました。

私は現在社会人13年目となりますが、「セキュリティは今後必要になりそうだし仕事として良さそう」という恥ずかしながら非常に安易な考えでセキュリティベンダに入社したことを皮切りに、初めてセキュリティと出会いました。学生時代はメディア系の学科出身であったこともあり、サーバやアプリケーションの開発・運用経験なども無く、新人当時はセキュリティに関する知識などは完全にゼロの状態でした。正直何からやればいいのかもわからない状態からのスタートでしたが、その後いつの間にか気がつけばセキュリティの魅力にとりつかれ、今日に至ります。

さて、話は変わりますが、私は個人的にここ数年、プライベートにて勉強会のようなITイベントを企画・開催したり、運営に携わるような活動をしております。良く勉強会やカンファレンスに参加する意義や理由などについて度々話題となりますが、個人的にはこういったイベントは、参加すれば誰でもめきめきスキルが伸びるなどというわけではなく、何かの「きっかけ」を得るための場ではないかと思っています。「きっかけ」の内容は人によって様々であり、新しい知識や人との出会いであったり、人前で発表をする機会かもしれません。大事なのは参加することよりも、参加して何を持ち帰るかということではないでしょうか。

私自身は、これまで参加したイベントで様々な「きっかけ」をいただき、刺激をうけたことで、今日の自分があるのではないかと思っております。そして何より、多くの方との素晴らしい出会いがありました。恐らくこういった活動を通じなければ知り合えなかったであろう他業界の方と交流ができたのも非常に良かったことの一つです。また、一緒に飲みに行く相手にも不自由しなくなりました（笑）

といったような経緯から、私は自分が運営するイベントが、参加する皆様のなんらかの「きっかけ」となれば良いなと思い、仕事以外のライフワークとして活動しております。この記事を読んでくださっている皆様も何か新しい「きっかけ」を得るために、是非ITイベントに足を運んでみてはいかがでしょうか？

最後になりましたが、少しでも世の中がセキュアになるように今後も活動していく所存であり、どこかでお会いする機会もあるかと思いますので、皆様よろしくお願いいたします。

SECURITY CONTEST (SECCON) 2019

SECCON（セクコン）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。

【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］（2018年度実績）

- 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
- 独立行政法人 情報処理推進機構
- 一般財団法人 日本情報経済社会推進協会
- 一般社団法人 日本経済団体連合会
- 日本シーサート協議会

[協　賛]（2018年度実績）

プラチナスポンサー：SecHack365

ゴールドスポンサー：日本電気株式会社、富士通株式会社

シルバースポンサー：株式会社インターネットイニシアティブ、NRIセキュアテクノロジーズ株式会社、KDDI株式会社、セコムトラストシステムズ株式会社、ソフトバンク株式会社、株式会社ディアイティ、日本アイ・ビー・エム株式会社、日本電信電話株式会社、パナソニック株式会社、株式会社日立システムズ、株式会社Flatt、LINE株式会社

ブロンズスポンサー：株式会社アクセル、株式会社アズジェント、E.N.Nach、株式会社インフォセック、株式会社エヌ・ティ・ティ・データ、CODE BLUE、株式会社サイバーディフェンス研究所、サイボウズ株式会社、Digital Travesia、大日本印刷株式会社、株式会社ディー・エヌ・エー、トレンドマイクロ株式会社、株式会社日本レジストリサービス、任天堂株式会社、パーソルテクノロジースタッフ株式会社、株式会社ブロードバンドセキュリティ、合同会社ヘマタイト、ヤフー株式会社、株式会社ラック

インフラスポンサー：さくらインターネット株式会社

機材協力：ヤマハ株式会社

ツールスポンサー：株式会社ヌーラボ

[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: info2019@seccon.jp）

[開催スケジュール]

■SECCON2019

日　程	会　場	内容
2019年10月19日(土)、20日(日)	インターネット	SECCON CTF予選
2019年12月21日(土)、22日(日)	AKIBA SQUARE 秋葉原コンベンションホール	SECCON CTF(国際)
		SECCON CTF(国内)
		カンファレンス・ワークショップ等

※ SECCON CTF（国際・国内）には、CTF予選で上位入賞したチーム以外に、連携大会招待枠があります。

■SECCON 2019 Workshop

日　程	会　場	内容
2019年8月31日(土)	広島市立大学サテライトキャンパス(広島)	ワークショップ

■SECCON Beginners 2019（CTF未経験者向け勉強会）

日　程	会　場	内容
2019年8月24日(土)	苫小牧高等専門学校(北海道)	ワークショップ+CTF演習
2019年9月7日(土)	石川高等専門学校(金沢)	
2019年10月5日(土)	東京都立産業技術高等専門学校(東京)	
2019年10月26日(土)	九州大学伊都キャンパス(福岡)	

■CTF for GIRLS(女性限定勉強会)

日　程	会　場	内容
2019年6月21日(金)	富士通ラーニングメディア(東京)	第11回ワークショップ
2019年9月1日(日)	未定	CTF for School GIRLS × NEXT ※学生優先
2020年1月~2月	未定	第12回ワークショップ

※SECCON BeginnersとCTF for GIRLSにはSECCONCTFへの出場枠はありません。

[SECCON Beginnersとは]

日本国内の CTF のプレイヤーを増やし、人材育成とセキュリティ技術の底上げを目的としたCTF 未経験者向け勉強会です。海外のCTF でも上位に入る若手のCTFプレイヤーにより運営されており、CTF 未経験の方でも CTF に参加できるよう、わかりやすくセキュリティ技術を教えるワークショップです。

[CTF for Girlsとは]

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情報セキュリティ技術について学ぶワークショップや、その他女性向けCTFイベントの開催を行っており、毎回定員に達する

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

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.47

2019 年 6 月 12 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