JNSA PRESS
JAPAN NETWORK SECURITY ASSOCIATION
AUTUMN 2020 VOL. 49

寄稿

可視化からはじめる製造現場のサイバーリスク対策
02

組み込みアプリケーションの実装におけるセキュリティ上の課題
06

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

テレワーク時代のインシデント対策 ～境界型セキュリティから ゼロトラストセキュリティへ～

株式会社ディアイティ
JNSA 理事　青嶋　信仁

テレワークによる業務環境が一気に進みだしたその変化の結果として通信経路が多様化する中、従来、セキュリティ対策の考えで主流であった境界型セキュリティの限界を迎え、通信経路の守りが十分ではないことを前提としたゼロトラストセキュリティへの移行が注目されています。

従来、業務で取り扱われる情報は、境界に置かれたゲートウエイ製品などによるセキュリティ対策を主体に行われており、エンドポイント側ではウイルス対策ソフトレベルで補完的に守られているという状況でした。境界が分散して多様化する環境においては、エンドポイントでの自立した単独でのセキュリティ対策が必要になり、従来の教科書や試験にもできたような境界型を基本としたセキュリティ対策の考え方の変更が求められる時期が来たといえます。

このような変化において、表立って議論されることは少ないものの非常に影響が大きいのが、テレワーク環境における分散したエンドポイントに対するインシデント対応です。インシデント対応をフェーズ毎でみていくと、「検知」段階においては、従来の境界におかれた検知機能が必ずしも有効に働かず、個々のエンドポイントの機能に依存する問題があります。また、「受付/トリアージ」の段階においては、一般社員と同じようにテレワーク環境に置かれたシステム管理者やCSIRTに対して必要な通知や報告が届くのか、コミュニケーションの連携に支障がないかが問題になります。さらに「インシデントレスポンス」段階では、コンピュータフォレンジックを行わないと解決できない場面において、テレワーク環境にある解析対象機器から必要なデータや各種情報をすぐに入手できないことも想定しておかなければなりません。併せて、解析対象機器の回収と代替機提供といった物流の問題も考えておかなければなりません。これらの問題は従来のインシデントレスポンスに比べて対処の遅れと被害の拡大を招きます。このような問題に対する解決策としてEDR（Endpoint Detection and Response）などのインシデント対応を考慮したエンドポイント製品が注目を集めています。EDRは、その機能から初期対応への効果が高く、従来製品が苦手であった大量のエンドポイント機器への監視やインシデント対応が可能となるなど、状況によっては従来より素早い対応が期待できるレベルになっており、日本でも導入が進み実績を積んでいるところです。

日本のセキュリティ対策は、欧米から常に4，5年は遅れていると言われていますが、世界で一斉にテレワーク環境が利用されるようになっている状況にある今、この機会に弾みをつけて一気に進化してほしいと期待しています。

可視化からはじめる製造現場のサイバーリスク対策

富士通株式会社
岡本　登

1．はじめに

いま、製造業は大きな変革を迫られている。ITを活用した新たなイノベーションを目指す一方で、新型コロナウイルスなどの感染症と経済打撃に立ち向かわなければならない。これまでにも国内経済は、オイルショック、バブル崩壊、リーマンショック、東日本大震災と幾度となく危機的な状況を乗り越えてきた。製造現場では、基本に立ち返り、やるべきことを徹底して行うための管理を中心に仕事の見直しが推し進められた。あらたな脅威が現れれば、愚直とも言えるほど改善を積み重ねて乗り越えていくことが日本の強みではないだろうか。

しかし、残念ながらサイバーリスクに対する取り組みはまだまだ低調だと感じる。ここ数年、多くの工場の実態を見てきたが、工場内のネットワークインフラ基盤は過去からあまり変化することなく、改善の余地がかなりあると言える。

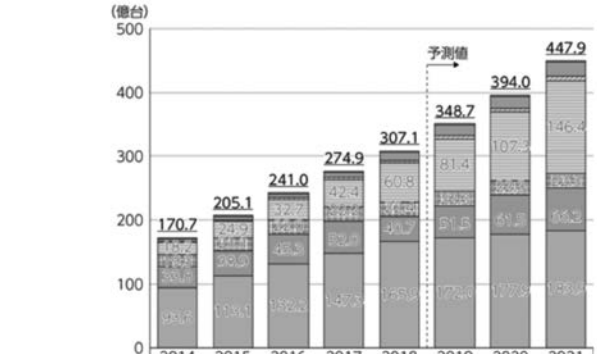
本稿がサイバーリスクは感染症と同じく、今、対策をしておかなければならないリスクであると認識をしていただくきっかけになれば幸いである。

2．10年以上遅れている実態

情報系環境（OA環境）におけるセキュリティ意識と対策はかなりのレベルまで成熟してきていると思われる。それでも、完璧な防御はあり得ないため、侵入後対策としてのレジリエンス強化が注目されている。一方、製造現場では、2005年に外部から持ち込まれたパソコンをネットワークに接続したことが原因で工場設備がウイルスに感染し、自動車製造工場（海外）が停止するという事故が発生しているが、2017年のWannaCry流行時には、これと同様の原因で工場が停止する被害が出ている。この実態から考えると、セキュリティ対策はここ10数年は進化していないと言える。

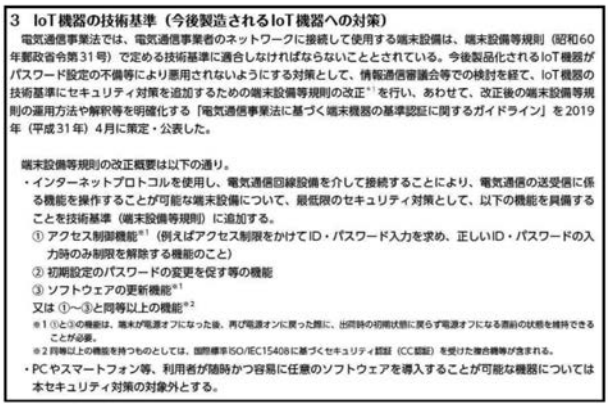
ウイルスやワームなどのサイバー脅威は技術的にも高度化され、より強力に変化している。しかし、これが理由で製造現場が被害を受けているわけではない。WannaCryの場合、感染後の動作は高度ではあるが、情報系環境であれば最初の感染は十分に防げるレベルだと思われる。また、仮に誰かの端末が感染したとしても他の端末が基本的な対策を施していれば拡散する可能性は低い。しかし、製造現場に感染したパソコンを持ち込まれたら、WindowsOSで動作している工場内の装置は無対策のため全滅する可能性が高い。実験によると、WannaCryは5、6秒で50台程度の端末に最初のアクションを起こすことが分かっている。

製造現場での活用が期待されているIoT機器に関しては、その脆弱性が話題になることも多く、最近の情報通信白書でもIoT機器のセキュリティ対策が取り上げられている。



	2014	2015	2016	2017	2018	2019	2020	2021
	170.7	205.1	241.0	274.9	307.1	348.7	394.0	447.9
軍事・宇宙・航空	0.03	0.04	0.04	0.05	0.03	0.04	0.05	0
自動車	3.8	4.7	6.0	7.5	13.5	16.6	19.1	22.0
医療	2.0	2.3	2.8	3.4	3.9	4.8	5.9	7.1
産業用途	18.2	24.9	32.7	42.4	60.8	81.4	107.3	146.4
コンピュータ	19.3	21.1	22.0	22.2	22.4	22.3	22.3	22.3
コンシューマ	33.8	38.9	45.3	52.0	40.7	51.5	61.5	66.2
通信	93.6	113.1	132.2	147.3	165.9	172.0	177.9	183.9

図1．世界のIoTデバイス数の推移及び予測
（総務省　令和元年版　情報通信白書より）



3　IoT機器の技術基準（今後製造されるIoT機器への対策）

電気通信事業法では、電気通信事業者のネットワークに接続して使用する端末設備は、端末設備等規則（昭和60年郵政省令第31号）で定める技術基準に適合しなければならないこととされている。今後製品化されるIoT機器がパスワード設定の不備等により悪用されないようにする対策として、情報通信審議会等での検討を経て、IoT機器の技術基準にセキュリティ対策を追加するための端末設備等規則の改正*1を行い、あわせて、改正後の端末設備等規則の運用方法や解釈等を明確化する「電気通信事業法に基づく端末機器の基準認証に関するガイドライン」を2019年（平成31年）4月に策定・公表した。

端末設備等規則の改正概要は以下の通り。

・インターネットプロトコルを使用し、電気通信回線設備を介して接続することにより、電気通信の送受信に係る機能を操作することが可能な端末設備について、最低限のセキュリティ対策として、以下の機能を具備することを技術基準（端末設備等規則）に追加する。

① アクセス制御機能*1（例えばアクセス制限をかけてID・パスワード入力を求め、正しいID・パスワードの入力時のみ制限を解除する機能のこと）

② 初期設定のパスワードの変更を促す等の機能

③ ソフトウェアの更新機能*1

又は①～③と同等以上の機能*2

※1 ①と③の機能は、端末が電源オフになった後、再び電源オンに戻った際に、出荷時の初期状態に戻らず電源オフになる直前の状態を維持できることが必要。

※2 同等以上の機能を持つものとしては、国際標準ISO/IEC15408に基づくセキュリティ認証（CC認証）を受けた複合機等が含まれる。

・PCやスマートフォン等、利用者が随時かつ容易に任意のソフトウェアを導入することが可能な機器については本セキュリティ対策の対象外とする。

図2．IoTセキュリティ対策の推進
（総務省　令和元年版　情報通信白書より）

一方、工場内の既存装置は使用年数も長く、現在もなお、数多くのWindowsXPが動いている実態にも目を向けるべきではないだろうか。

3．脅威に負けないために必要なこと

サイバーセキュリティ対策のリファレンスとして国内でも活用する企業が増えてきたNIST サイバーセキュリティフレームワーク(CSF)では、リスク管理を識別、防御、検知、対応、復旧の5つの機能で定義している。CSFに関する解説は別の機会に譲るとして、ここでは、この5つの管理機能に沿って、製造現場の課題とサイバーセキュリティ対策を考察してみる。

①識別

工場内のネットワークに接続されている端末や装置は確実に把握できているだろうか?これまで多くの工場を見てきた経験から、資産管理が非常に弱いと感じている。リスト化された機器一覧は最新化されず、実態調査を行ってみると管理者も知らない端末が見つかることもある。また、工場内ネットワークの管理もかなり怪しい。セグメント化されずに数珠つなぎで延長されたLANが工場内に張り巡らされている状態では、端末や装置がどこに繋がっているのかを人手で的確に把握し、維持管理することはきわめて難しい。

従って、考慮すべき対策としては、やはり資産管理の徹底ということになるのだが、これを属人化あるいは形骸化させないためには人手を介さずにすべてを自動で行えることが重要である。このような機能を持つ製品も数多くあるが、工場内ではネットワークアドレス部が想定外なIPアドレスを持つ端末が存在するケースもあり、漏れなくすべてを拾い集めて可視化できることがポイントになる。

②防御

工場内への脅威の侵入口はそれほど多くはない。情報系環境のように、個人の端末からのメールの送受信やWEBサイトを閲覧するようなことはないため、外部ネットワークとの接続がない場合に想定される侵入口は、工場LANへの直接接続か工場内機器へのUSBメモリー挿入に絞られる。しかし、これらを規制することは工場運営上かなり難しい。また、保守用ネットワークや情報系ネットワークなどの外部ネットワーク接続がある場合でも、意図しない工場の稼働停止を避けるなどの理由から、その境界にFWなどが導入されていないか、設置されていても工場を脅威から守るための防御設定が適切ではないことが多い。

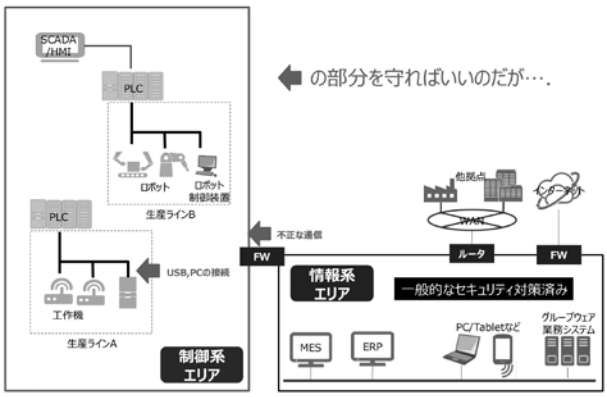


図3．工場セキュリティの防御ポイント

パッチ適用やアンチウイルス対策などのエンドポイントセキュリティ対策が導入できない事情も併せて考えると、残念ながら既存ネットワークに大きく手を加えることなく適用できる有効な防御策は少ない。それでも何

らかの製品導入を検討する際は、考え得るリスクシナリオをしっかりと検証することが重要である。

③検知

工場内に侵入したサイバー脅威を検知する仕組みはほとんど導入されていない。工場内通信は情報系環境のようなクライアントとサーバーもしくはクラウドとの通信のように垂直的で経路が集約されるようなものよりは、装置間などの水平的な通信の方が多いため、ネットワーク上の検知機能を効率的に配置することが難しい。また、工場内装置が何らかのマルウェアに感染したとしても、工場の操業に直接的な影響を与えない場合もあり、表面的な事象として認識できないこともある。実際に、情報持ち出しの機能を持つワームに感染した工場を調査する機会があったが、時々トラフィックが増大する程度で操業にはほとんど影響が見られなかった。(増大量によってはチョコ停が発生する可能性はある)

検知対策として最も単純な方法は、工場内LAN通信をすべてキャプチャし、リアルタイムに分析することである。一般的にはリピータハブにキャプチャー装置を繋ぐ方法とスイッチのミラーリング機能を使う方法があるが、工場に導入されているネットワーク装置の多くはミラーリング機能を持たない単機能なスイッチであり、両者とも対応できない。また仮にミラーリング機能を持つスイッチが導入されていたとしても、すべてのキャプチャデータを採取するには、データ量やキャプチャ装置の配置に課題が残る。そこでもう少しハードルを下げた別の方法を以下に示す。

工場内通信は比較的パターン化されているので、このパターンの崩れを可視化することができれば、ワームの拡散活動の検知などに有効であることが実験的に分かっている。スイッチにはポートを流れたデータをカウントする機能を有するものもあり、これを短い時間間隔で採取し、前日、前週、前月などのデータと比較すれば、特異点を見つけることができる。さらに通信フローデータを分析できれば、より精度の高い異常検知が可能になる。ただし、この場合でも、ネットワークの構成は変わらないが、インテリジェントスイッチへのリプレースは必要となる。

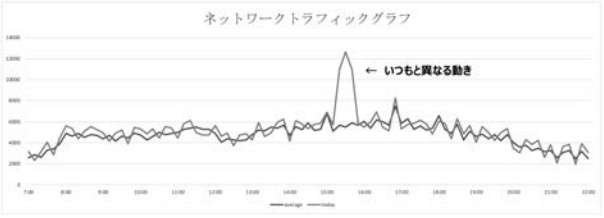


図4．トラフィック変化の可視化

④対応

リスク低減のために拡大を防ぎ、影響を緩和し、インシデントを解決に導くためには、早期対応が重要である。もちろん対応のためには検知できることが前提となるが、ここではその前提をクリアしたとして話を進める。

情報系環境では、端末のマルウェア感染が検知されると、直ぐにネットワークから切り離すことが推奨されている。しかし、工場系環境では、感染装置の特定そのものが難しいことに加え、仮に特定できたとしてもネットワークから切り離す判断は容易ではない。なぜなら、この1台を停止させるとライン全体が止まってしまう可能性もあるからだ。稼働に影響がなければ動かし続けたいと考える工場関係者も多い。

そこで検知情報を元に的確に対応するためには、あらかじめサイバーリスクに合わせたBCPを検討し、手順を可視化しておく必要がある。中でもWannaCryのようなワームは、無防備な工場内装置に対して短時間のうちに感染を広げるため、被害を最小限に抑えるためには素早い行動が求められる。この場合、BCPに従って人が判断し対応するスピードでは間に合わない可能性もあるため、人に代わってネットワークシステムとして自動的に遮断するような仕組みの検討も必要である。

⑤復旧

早期復旧のためには、被害範囲が特定でき、BCPなどで復旧プロセスが明確になっている必要があるが、そもそも現在のBCPは自然災害や火災などを想定したものであり、サイバーリスクを考慮したものではない。ワーム感染によって工場が全停止に至った場合、復旧後に1台でも対応漏れが残っていると、数時間後には再度同じことが起こるということを考慮しなけれ

ばならない。従って、作業効率的な手順だけでは復旧はできない。

工場内の装置はパソコンのようにマルウェアチェックを行うことが難しく、簡単に感染の有無を識別することはできない。一方で全装置を初期化あるいは入れ替えるという方法では大きなコストが発生する。感染範囲を絞り込むには、資産管理情報の装置OS種別を活用する方法や通信パターンの崩れから被害エリアを推測する方法などが考えられる。しかし確実ではないため、ブロック毎に高機能なスイッチを仮置きしながらキャプチャデータで状況を可視化し、徐々に復旧範囲を広げるなど慎重に進めて行く必要がある。なお、先の検知、対応が適切に機能していれば、被害範囲が最小限に抑えられることは言うまでもない。

4．製造業の未来のために

一つの製品の生産には多くの企業が関係している。今後、サプライチェーンのすべてでスマート化が進めば、製造現場の効率化やデータ活用は飛躍的に高まることになるが、一方で相互の依存度も高くなる。従って、製造現場のリスクマネジメントはひとつの工場だけの問題ではない。サプライチェーンのどこかで問題が発生すれば、その影響は全体に大きく波及する。例えば、先般の大雨による一部地域の浸水被害は多くのIT機器製造に影響を及ぼした。

日本の製造業はもちろん大企業だけではない。多くの中小企業や町工場に支えられていることを考えると、彼らを巻き込んだ形でリスクマネジメントを進めて行かなければならない。

ここまで製造現場の現状とサイバーリスク対策について述べてきたが、自然災害と違いサイバー脅威は弱者を襲う。新型コロナの影響などにより経済環境が厳しくなるなか、対策に大きな投資は難しいが、今できることから始めないと日本の製造業の未来は危ういのではないだろうか。

セキュリティ視点において、情報系環境との10年のギャップは簡単には埋まらない。しかし製造現場の情報化はどんどん進んでいく。高度化された工場が砂上の楼閣とならないようにすぐにでも行動を起こすべきである。

＊執筆者プロフィール

富士通株式会社
岡本　登（おかもと のぼる）
ネットワークサービス事業本部
シニアマネージャー
okamoto.noboru@fujitsu.com

組み込みアプリケーションの実装における セキュリティ上の課題

日本シノプシス合同会社
松岡　正人

組み込み機器開発は、Linux や Windows などの汎用の OS を利用することでパソコン化し、開発の容易さを手に入れた一方でシステムが肥大化し品質を担保するのが困難になり、出荷後にハードウェアの統合や、ネットワーク処理で問題が明らかになることが後を絶ちません。本記事では、実際の実装上の問題によって発生した脆弱性の調査をもとに、典型的な課題について振り返ってみたいと思います。

序文

現在、ネットワーク接続型の組み込み機器の多くは Linux OS を採用しているか、必要なネットワーク接続のための機能を有する組み込み OS を採用しており、Windows、VxWorks、QNX など古くから使われている汎用の組み込み OS もあれば、Apple 社の iOS のように特定の端末のために開発された OS もある。さらに、データベース、ウェブ、オンライン・ゲーム、決済などを利用するためのフレームワークやライブラリ、ウェブサービスの API などを組み合わせて利用することで様々なアプリケーションを提供している。そして個々のコンポーネントが内包する脆弱性は、開発提供元の各ベンダーが対処するのが常だが、それらを統合するためのプログラムコードは利用するコンポーネントのガイドラインに則って書き、単体テストやシステムテスト、異常系テスト、場合によってはファジングやペネトレーションテストを行うことで、開発者が担保する必要がある。

ところが、なんらかの事情で適切なテストが行われることなく市場に出荷されるコードも少なくない。この記事で取り上げる事例も、個々のコンポーネント、OS やデバイスドライバー、ライブラリーやフレームワークなどの脆弱性ではなく、不適切なコードによる予期しなかった脆弱性についてである。

弊社のセキュリティ・リサーチャのロンドンチームが今年の 4 月に公開した、CVE-2020-7958 biometric data extraction in Android devices、というレポートがある。調査したメンバーと会話した結果を織り交ぜながら、ソフトウェア開発の厄介な点についてハイライトできればと思う。

調査対象のデバイス：

対象デバイスは 2019 年に登場した OnePlus 7 Pro、このモデル以外の調査は行っていない。少人数で短期間に実施するためだ。中国製のこの端末は純粋な Android 端末ではなく、Android をベースに OnePlus が独自に手を加えている OxgenOS を採用している。2015 年に最初のリリースが行われてから UI だけでなく様々な改良を行っているが、基本的なオリジナルの Android と構造は同じである。ちなみに、このモデルを選択したのは、最初からハイエンドの機種（機能が一番多い）の脆弱性を調べるほうがいい（何か発見できる可能性が高い）だろうと考えたからだ。

ARM Trust Zone と Qualcomm QSEE によるシステムの保護：

ARM 社はセキュアな OS の実行環境のために Trust Zone という仕組みを提供している。これは半導体レベルでセキュアなソフトウェアの実行を実現するためのもので、ブートローダーがセキュアかどうかを判定し、セキュアな OS の起動を行い、指紋や顔認証などの生体認証などの仕組みを OS やアプリケーションか

ら論理的に分離することができる。OnePlus 7 Pro も Trust Zone を採用している。

Trust Zone ではハードウェアがリセットされると、下図の手順で順次必要なモジュールを読みだして起動していく。最初はブート ROM が Trusted Boot Firmware を起動し、TEE（Trusted Execution Environment）というセキュアなメモリ空間と REE（Rich Execution Environment）という非セキュアなメモリ空間とに分けて管理することで、安全に動作させたいコードを「Secure World」内で保護することができる。

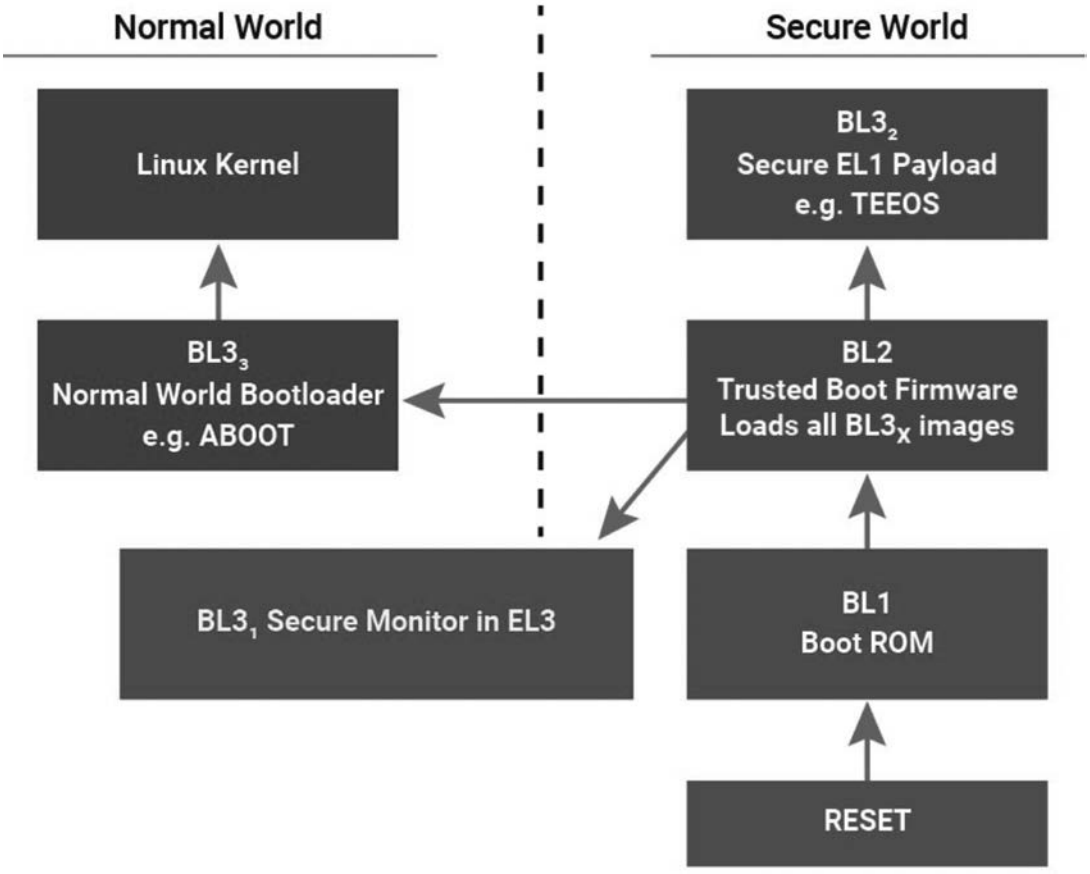


Fig.1″ Trust Zone におけるブート・シーケンス″

また、Trust Zone では TEE の実装はいくつかの選択肢があるが、OnePlus 7 Pro では Qualcomm 社の QSEE（Qualcomm Secure Execution Environment）が実装されており、Trust Zone で構成されたシステムは以下のような構成になっている。

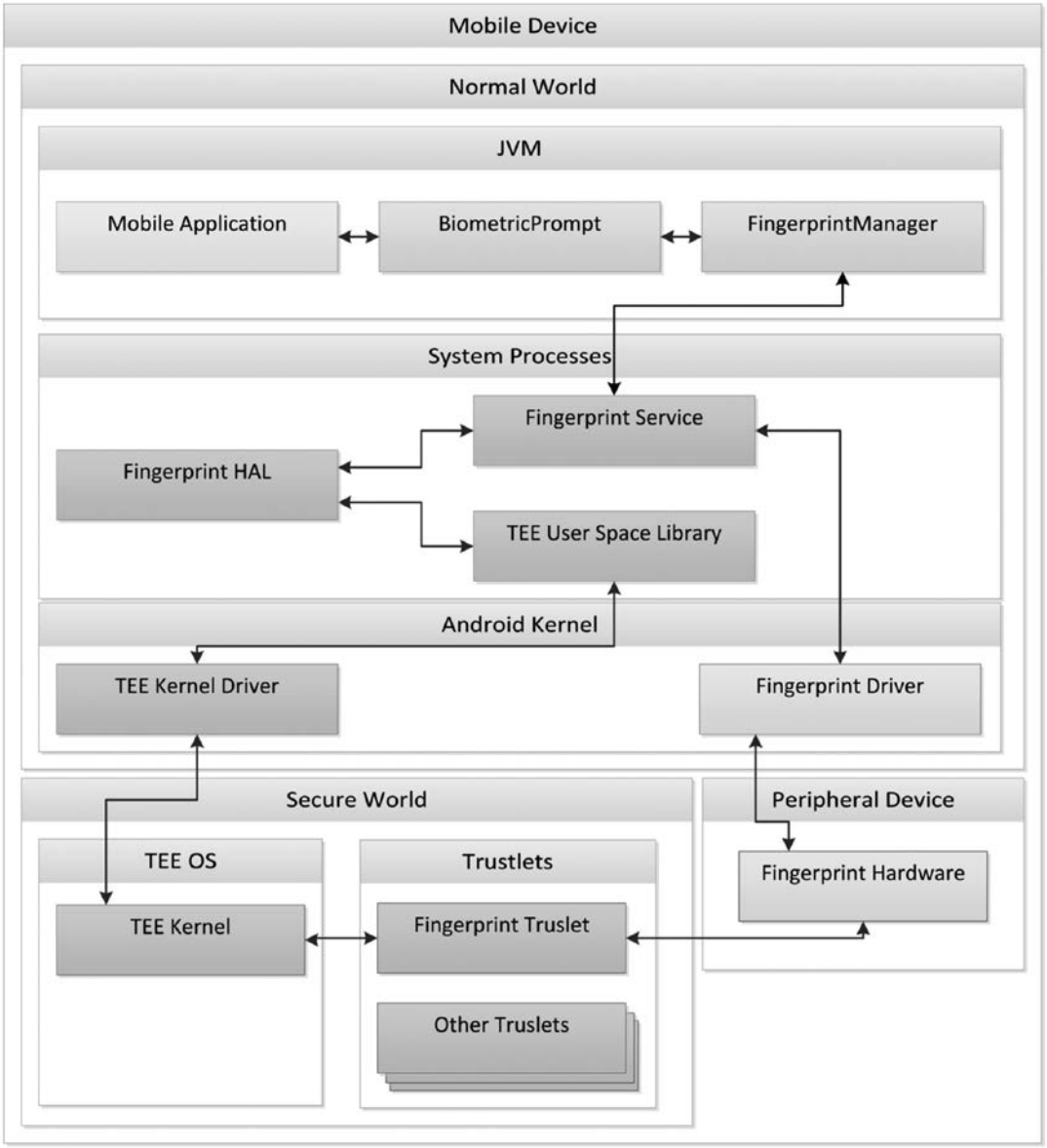


Fig.2:" Trust Zone によるシステム構成図"

TEE は "Secure World" と書かれた部分で、Android（OxygenOS）とは論理的に分離されているのがわかる。

さて、本稿で述べる脆弱性は、Secure World 内で指紋センサー（Fingerprint Hardware）で取得した指紋の画像データを認証するために TEE 内の Fingerprint Trustlet で処理する際のものであるが、指紋の画像データは REE（Fig.2 の Android Kernel も含む Normal World のブロック）内に渡されることがないようにしなければならない。これは Android の開発者向けのガイド（https://source.android.com/security/authentication/fingerprint-hal）にも" 指紋認証 HIDL" の項目で次のように注意書きがある。

- ベンダー固有の HAL 実装では、TEE で必要な通信プロトコルを使用する必要があり、未処理の画像と処理済みの指紋の特徴は、信頼できないメモリに渡さないこと
- このような生体認証データはすべて、TEE などのセキュア ハードウェアに保存する必要がある
- 従って、ルート権限取得によって生体認証データが侵害されないようにする必要がある

もちろん、OnePlus 7 Pro の指紋センサーと認証の仕組みは上記に則って実装されていた。

解析を始め、最初に取っつきやすい REE 側の指紋センサーのコンポーネントを調べてみた。libgf_ud_hal.so という共有オブジェクトが REE の指紋認証用のサブシステムに含まれており、ルート化された端末の /vendor/lib64/ に見つけることができた。そこで、OnePlus のダウンロードサイトから img ファイルを入手して調べてみると /vendor/lib64/ とファイル群をみつけることができた。libgf_ud_hal.so には goodix::SZCustomizedProductTest::factoryCaptureImage() というメソッドが含まれていた。ここから先は根気のいるリバースエンジニアリングを伴う作業の繰り返しとなり、ようやく擬似コード（Pseudocode）を生成するところまでたどり着いた。なお、これらの作業は root 化し、USB デバッグモードでホスト PC のデバッグ環境と接続してあったことを付け加えておく。

```
__int64 __fastcall goodix::SZCustomizedProductTest::factoryCaptureImage(goodix::SZCustomizedProduct
{
  goodix::command::FactoryCaptureImage *Command; // x0 MAPDST
  unsigned int rv; // w21
  const char *errfmt; // x0

  if ( raw_data_out )
  {
    Command = malloc(0x1502Cu);
    if ( Command )
    {
      memset(Command, 0, sizeof(goodix::command::FactoryCaptureImage));
      Command->ae_expo_start_time = ae_expo_start_time;
      Command->field_1C = uchar;
      Command->field_1E = ushort2;
      Command->Parent.target = 1003;
      Command->Parent.cmd_id = 17;
      rv = goodix::HalBase::invokeCommand(&this->HalBase, &Command->Parent, 0x1502C);
      if ( !rv )
      {
        memcpy(raw_data_out, &Command->captureImageResponseBuffer, sizeof(GF_SZ_TEST_RAWDATA));
        free(Command);
        return rv;
      }
      free(Command);
    }
    else
    {
      __android_log_print(6, "[GF_HAL][SZCustomizedProductTest]", "[%s] out of memory, cmd", "facto
      rv = 1001;
    }
  }
  else
  {
    __android_log_print(6, "[GF_HAL][SZCustomizedProductTest]", "[%s] param is erro", "factoryCaptu
    rv = 1004;
  }
  errfmt = gf_strerror(rv);
  __android_log_print(
    6,
    "[GF_HAL][SZCustomizedProductTest]",
    "[%s] exit. err=%s, errno=%d",
    "factoryCaptureImage",
    errfmt,
    rv);
  return rv;
}
```

Fig.3:” 擬似コード goodix::factoryCaptureImage()”

得られた擬似コードから、Target ID（擬似コード内の target）が 1003、Command ID（同じく cmd_id）が 17 とわかったことで、これを使って TEE 内の Fingerprint Trustlet の機能を呼び出すことができるのではないかと想像してみる。このようなコマンドの構造を解き明かしていくと、goodix::HalBase::invokeCommand() を呼び出し、QSEE のライブラリ libQSEEComAPI.so と通信し、指紋画像のデータを格納するメモリーを確保するだろうことが想像できる。

また、SZCustomizedProductTest のインスタンスを生成するには HalContext インスタンスに有効なリファレンスを渡さなければならないが、運のいいことに goodix::HalBase::invokeCommand() が何度も繰り返し呼び出されていたことから指紋センサーのデータを処理に関わっていることは明白で、goodix::HalBase のインスタンスには HalContext への有効なポインターが含まれていることがわかった。これらの作業が厄介なのは、root 化したデバイスでの root のアクセス可能な領域を思い出してもらえればわかると思うが、指紋センサーの画像データを処理して認証する仕組みは TEE（Fig.1 の Secure World）内の Trustlet として実装されているため REE（Fig.1 の Normal World）から直接アクセスすることができず、TEE 内の実装がどのようになっているのかは、リバースエンジニアによって得た少ない証拠を積み重ねていくことしかできないからである。

しかし、擬似コードを得ることができた為、あとは Trustlet の機能と、初期の解析で獲得した target=1003、cmd_id=17 のパラメータを利用した Trustlet をエクスプロイトするコードの作成ということになる。

詳細は本文最後に記載した URL にあるブログ記事本文を参照願うとして、エクスプロイトコードは完成し、機能した。REE 内の指定したメモリー領域に指紋センサーのデータをコピーすることができたのである。指紋センサーと指紋認証が動作することをテストするためのコードが Trustlet 内に残っていたためである。

対策と振り返り：

テスト用のコードを削除する、つまり cmd_id=17 を受け取ってテストするコマンドハンドラーを取り去ることで解決したが、#ifdef によって開発時の指紋センサーの試験時にはこのコマンドハンドラーを活かし、出荷用のコードはコマンドハンドラーを省けば良いだけである。これがたんなる不注意によるものなのか、開発者にとっては留意すべきはこの一点だろう。現時点で有効な高度なセキュリティ技術だが、やはりシステム全体、各コンポーネントや基盤技術をサポートした安全なソフトウェアの開発の脆弱性はコードの中に潜んでいたのである。

なお、本調査に際して、速やかに対応していただいた OnePlus 社の関係者には謝意を申し上げる。

参照先 URL

英　語：https://www.synopsys.com/blogs/software-security/cve-2020-7958-trustlet-tee-attack/

日本語：https://www.synopsys.com/blogs/software-security/ja-jp/cve-2020-7958-trustlet-tee-attack/

JNSA ワーキンググループ紹介

西日本支部

アイネット・システムズ株式会社
西日本支部長　元持　哲郎

■ 西日本支部の活動ポリシー

西日本支部は２００１年発足以降、一貫して、関西に多い中小企業を対象に、IT利活用を促進すると共に、積極的にITを安全に利用して頂く上で必要となる情報セキュリティに関わる様々な成果物の作成と、IT利活用を行う組織が情報セキュリティ対策の実践にあたり、ヒントとなる情報を提供するセミナーの企画・開催を、活動の二本柱としています。

これまで、日常業務に潜む情報セキュリティリスクの気付きの手引き、組織が情報セキュリティ活動を実施するにあたり必要となる情報セキュリティポリシーのサンプル、また実際の情報セキュリティレベルを評価するためのチェックシート等、様々な成果物を中小企業向けに作成してきました。

成果物の作成、またセミナーを企画するにあたり、日本の多くの組織がリスクについて過剰に意識し、ITの利用を控えてしまう傾向がありますが、IT利用効果を最大限に引き出し、禁止事項を最小限に留め、リスクを低減することを基本に、検討・企画しています。

■「Security by Design」WG

現在は、ITの組織への導入において、経営者から投資の承認が下りたという前提で、導入前に、非機能要件であるセキュリティ要件を検討するWG活動を行っています。セキュリティ要件だけではなく、ITの導入が経営課題を解決したことをどのように測定・評価するのか？セキュリティ対策の有効性をどのように評価するのか？また、セキュリティ運用をどのように行なうのか？等、総合的に考慮することで、情報システム部門と経営者及び他部門との継続的なコミュニケーションを円滑にするための潤滑油の役割を果たす成果物の作成を目指しています。目標が大きすぎたためか、やや発散気味の活動になっていますが、今年度中の成果物完成を目指しています。

■「工場のセキュリティ」WG

製造の現場に於いても装置のネットワーク化、IoTの導入が積極的に行われていますが、ネットワークへの接続リスク、IoTの導入リスクまで十分に考えられていないようです。しかし、一方で、制御装置、IoT機器へのサイバー攻撃やマルウェア感染のインシデントは年々増加しています。そこで、中小の製造業が多い西日本支部に相応しい「工場のセキュリティ」を検討するWGを、今年度は新たに立ち上げようとしています。

■セミナー企画

残念ながら、新型コロナウイルスの影響で活動を見合わせていますが、毎年「NSF in Kansai」と言うセミナーを、西日本ならではの視点で企画、開催しています。また、関西にある情報セキュリティの団体と協同で「関西情報セキュリティ団体合同セミナー」を年４回開催しています。新型コロナウイルスの状況が落ち着き次第、活動再開予定です。

JNSA ワーキンググループ紹介

■最後に

WG活動では、毎回「ここだけの話ですが」を合言葉に、話が大きく本題から脱線してしまうこともしばしばです。脱線話（自由放談）と言っても、井上顧問、金子顧問をはじめビジネス経験豊富な各メンバーのセキュリティに関連した貴重な話が聞け、他ではできない経験ができます。今年度は、新たに「工場のセキュリティ」WGを立ち上げます。是非、西日本支部の活動にご参加して頂き、一緒に成果物を作成しましょう！

WGメンバー

元持　哲郎（西日本支部長　アイネット・システムズ株式会社）
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）
金子　啓子（JNSA顧問、大阪経済大学　経営学部）
大室　光正（株式会社インターネットイニシアティブ）
河野　　愛（株式会社インターネットイニシアティブ）
小柴　宏記（ジーブレイン株式会社）
嶋倉　文裕（サブスクライバ）
古川　佳和（大阪商工会議所）
吉崎　大輔（日本電気株式会社）
米澤　　美奈（株式会社ソリトンシステムズ）

WG協力者

青木　　茂
今井　　実
大財　健治
塩田　廣美
西川　和予

組織で働く人間が引き起こす不正・事故対応 WG

セコム株式会社 ＩＳ研究所
WGリーダー　甘利　康文

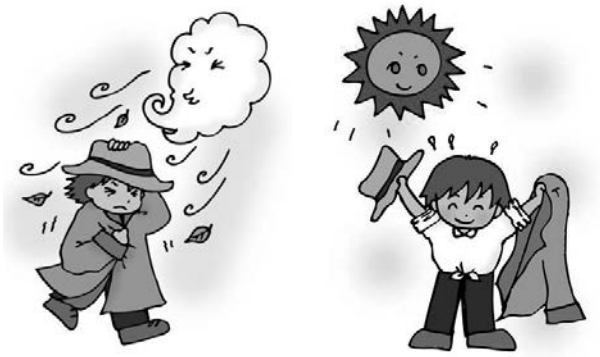
本WGは、いわゆる「情報セキュリティ」をスコープとするJNSAにおいては、異色の活動を行っている少し変わったＷＧです。前回のＷＧ紹介[1]からご無沙汰してしまいましたが、今回は最近の活動を中心に、ＷＧの紹介をさせて頂きます。

組織で働く人間に起因する事故（不正）には、情報システム的な対策だけでは防ぎきれないものも多く見られます。犯罪学では「犯罪企図（犯罪への意志）を持った人間」が「犯罪の機会」に遭遇することで犯罪が起こると考えています。そのため、犯罪抑止には「犯罪企図者を作らない」、「犯罪機会を作らない」の２つの方向性があるとされています[2]。情報システム的に「あれはダメ、これもダメ」とする対策は、後者の犯罪機会を作らない対策です。これは、イソップ寓話の「北風的」な対策であって、不正が表立つことの抑制はできるものの、犯罪企図という不正の根を解消するは至りません。そのため、この対策では、働く人間による情報漏えいという不正は抑制できたとしても、横領や背任などの不正には効果は期待できません[1]。

過去の調査で、働く人間が不正を働く原因に、職場の人事面、組織面の問題や不満があることが指摘されています。働く人間の満足度（ES: Employee Satisfaction）を向上させ、働く喜びが感じられる職場環境を作りだす「太陽的」な対策は、職場の人事面の問題や不満を解消する方向性の対策であり、働く人間に、そもそもの「悪意」を起こさせない、不正の根本に働きかける本質的な対策になり得ます。

また、その太陽的な性格から、生産性の改善や退職の抑制、人材採用面などのプラスが期待できる文字通りのポジティブな施策にもなります。ES向上は、これらプラスの効果が主役の施策であり、不正抑制は、あくまでも副次的な脇役という位置付けです。

現在、多くの組織でES向上のための様々な工夫が行われています。しかし、その目指すところは、生産性を上げたり、退職を抑制したりなどであり、多くは、目的を達成して完結してしまいます。また、ES向上の工夫は、開示しても売上などに直接関係することが薄いため、積極的にアピールする組織は必ずしも多くはありません。また、不正抑制の観点からES向上を目指している例も多くありません。



情報セキュリティに関わるJNSA会員企業を主として、世の中の組織が、自らの職場を「人が活きいきとやりがいを持って働ける環境」にするために、どのように考え、どのような工夫をしているか。本WGの最近の活動では、これらを掘り起こし、その知見を共有しようとしています。「働く人間が、活きいきとやりがいを持って働ける環境」作りのために様々な工夫を行っている組織の、その工夫を共有することで、お互いに「良いとこ取り」が出来るようにすることを狙っています。具体的には、さまざまな組織の人事、組織系部署を訪問、責任者にES向上の取組、工夫をヒアリングし、その内容を記事にまとめて、以下のJNSAのサイトで公開させて頂いております。

インタビュー連載「日本の人事と内部不正」
https://www.jnsa.org/result/soshiki/index.html

また、同様の趣旨の下、JNSAの年次イベント「Network Security Forum」における招致講演を企画、実施し、これまでに、意思決定や組織論、リーダーシップ論に関するお話しも頂いております。

○ **NSF2018「人間の意思決定の神話と現実」**
東京都立大学（首都大学東京）長瀬勝彦 教授

JNSA ワーキンググループ紹介

○ **NSF2019「働く人々のための本質組織論〜組織の不条理や不正が起こらない良い組織作りのためのエッセンシャル・リスク・マネジメントの視座〜」**
早稲田大学大学院 西條剛央 客員准教授

○ **NSF2020「内部不正をしようとする気を起こさせないための組織論『フォロワーシップ型リーダーシップ論』〜時代を問わず、生き残る組織をつくる〜」**
金沢工業大学虎ノ門大学院　伊藤俊幸 教授（元海上自衛隊海将）

WG活動の詳細は、上記の公開ページをご覧頂くとして、本稿では、これまでの活動で判った、各組織のES向上の取組に共通する最大公約数的内容を要約し、キーワード的に示します。

○ **働く人々の間のコミュニケーション促進**
- 組織の「風通し」確保
- 制度、空気感醸成、情報システムによる様々な情報の共有

○ **働く人々の健康への配慮**

○ **様々な働き方の容認**
- ワークライフバランス、ダイバーシティ等
- 制度、情報システムによるアシスト

○ **評価と処遇**
- 人は「パンのみに生きるにあらず」だが、「パン」は重要（不足は不正の直接要因）
- コミュニケーションによる評価の納得性と適正感の確保
- 「成長の機会」提供

ES向上の本気の「太陽施策」は、心に働きかけて、働く人々の意識を変え、プラス効果を生み出します。これは、退職者の減少、求職者の増加という具体的な形で現れます。情報漏えいの多くが（悪意のある）退職者によるという現実に鑑みて、これには、情報セキュリティにおける効果も期待出来ます。

情報セキュリティに限らず、あらゆるケースに適用出来るセキュリティの定義とは「対象組織のオペレーション（OP）があらかじめのプラン通りに円滑に運営されていること」[3]です。そのOPを回しているのは「そこで働いている人」に他なりません。

組織の本質は「人的Network」であり、これを有効に活用することは、組織による価値創造[3]というOPを促進することになります。ITの力も借りて、そのNetworkに内在する、人に関わるリスクをはじめとした「捉えがたい様々なリスク」[4]を低減することはNetwork Securityの新しいフィールドになり得ます。リスクの少ない良い職場環境（人的Network環境）は「平穏なOPの維持」、すなわちその組織のセキュリティに不可欠だからです。各ノード（人材）が高性能でも、ノード間のNetworkが機能しなければ、組織はその本来の価値を発揮出来ません。人々のコミュニケーションをより円滑に行えるようにすることで、組織の本質である「人的Network」を涵養、そして多様な働き方を実現する。このような太陽的な方向にJNSAの新しい活動のフィールドが広がっているのではないかと思います。

【参考文献】

[1] 甘利康文：組織で働く人間が引き起こす不正・事故対応WG, JNSA Press Vol.35, pp.6-7 (2013) https://www.jnsa.org/jnsapress/vol35/4_WG.pdf

[2] 甘利康文、新井真司、内田順一：セキュリティ実現の原点から見た内部要因事故抑制手法, JNSA Press Vol.33, pp.3-29 (2012)　https://www.jnsa.org/jnsapress/vol33/3_kikou.pdf

[3] 甘利康文：セキュリティの本質：医療/医学, そして技術は何のためにあるのか, 日本情報経営学会誌 Vol.38, No.3, pp.40-52 (2018)　https://r2ec.jp/news/1312/

[4] 甘利康文：「リスクの本質」を考える体系構築のために, リスク工学研究 Vol.16, pp.9-14 (2020) https://www.risk.tsukuba.ac.jp/pdf/bulletin16.pdf#page=13

会員企業ご紹介㊾

グローバルセキュリティエキスパート株式会社

https://www.gsx.co.jp/

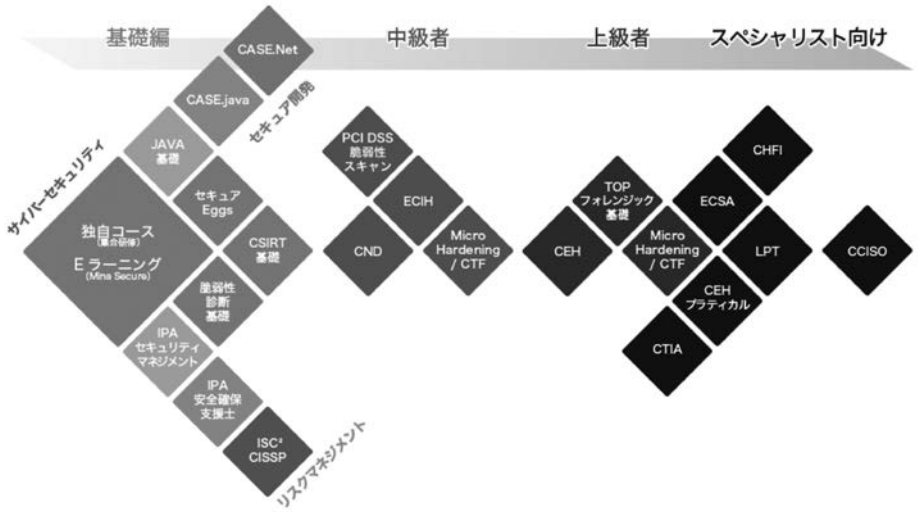
GSX
GLOBAL SECURITY EXPERTS

「企業として、個人として、確かな成長を」
～サイバーセキュリティ教育で支える～

今、私たちの働き方が大きく変わろうとしています。これまで自宅から会社へ通勤して仕事をするのが当たり前だった日常が、ここ数か月で大きく変化し、今では自宅で仕事をする人も増えてきました。この在宅勤務とオンサイト勤務（現場勤務）はより二極化が進んでいくことでしょう。

さて在宅勤務で変わることは様々です。その1つとして、より能力や結果によって判断されるいわゆる「能力/成果主義」的思考が強まることです。また、企業がテレワークに移行するにあたって、挙げられているのがセキュリティ課題です。今回、強引にテレワークを実施した組織も根本的なセキュリティ課題が解決されているわけではなく、また、事業自体のデジタル化の必要性も叫ばれています。今後、サイバー空間の活用が増えれば増えるほど、サイバーセキュリティの知識を有する人材や部門が重宝されていくことは間違いないでしょう。

グローバルセキュリティエキスパート社では、サイバーセキュリティの教育を基礎から上級者までオンライン・オフライン双方で提供しています。能力の指標としてわかりやすい資格として、またセキュリティの全般的防御を学べるEC-Councilの「Certified Network Defender（CND）」や、サイバー攻撃を知る「Certified Ethical Hacker（CEH）」などを提供しています。この2つは単なる座学ではなく、演習を通して、己を知り、敵を知ることができます。さらにセキュア開発を学ぶことができる「CASEシリーズ」やお客様毎にカスタマイズした教育、「Micro Hardening」のようなより実践的な演習も提供しています。



サイバーセキュリティ教育を通じて個人が成長するとともに、その成長によって企業はよりセキュリティの強化が自組織で実施することができます。新しい時代に備えた「確かな能力」と「確かなセキュリティ」。新しい時代の新しい経営においても必要不可欠なものではないでしょうか。

お問い合せ	グローバルセキュリティエキスパート株式会社 〒105-0022 東京都港区海岸1-15-1 スズエベイディアム4F Web: https://www.gsx.co.jp/

アビラ合同会社
https://oem.avira.com/ja

Avira

Aviraは1986年にドイツで設立され、セキュリティ市場において30年以上にわたり最先端の技術を提供し続けています。

Aviraはドイツ・ヨーロッパを中心に80年代からアンチウイルスソフトウェアを販売しています。第3者機関の評価においても長年にわたり常にグローバルトップクラスのベンダーとして名を連ねており、これまでの数々の受賞歴がその品質を証明しています。

当社は、長年培ったその高い技術力と品質に基づいたセキュリティのコア技術によって、より広く多くの人々・企業守ることをミッションとしています。そのため、コンシューマー製品を中心にグローバル展開するとともにOEMを通じた技術提供も積極的に行っています。既に多数のグローバル企業にご利用頂いており、全世界に5億人以上のユーザがいます。当社のOEMソリューションは様々なセキュリティ製品やクラウドサービス、IoT機器等への組み込みが可能です。また、Revenue shareやPay per useモデルなどの柔軟なライセンス方式がご利用頂けます。是非貴社の製品ポートフォリオの強化、セキュリティ対策の強化にご検討ください。

アンチウイルスエンジン

組み込み型アンチウイルスエンジン
SAVAPI

携帯向けアンチウイルスエンジン
MAVAPI

Proxy環境向けアンチウイルスエンジン
ICAP with SAVAPI

組み込み
クラウド
情報
サーバー

高度な脅威分析エンジン

ゼロデイ対策クラウド分析エンジン
Avira Protection Cloud

ゼロデイ対策オンプレミス分析エンジン
Virtual NightVision Appliance

クラウド解析サンドボックス
Cloud Sandbox API

脅威情報

URLレピュテーション
Avira URL Cloud

脅威情報
Threat Intelligence Feed

プライバシー

通信暗号化、接続IP秘匿
Avira PhantomVPN

IoT

ルーター組込み型IoTデバイス管理
Avira SafeThings

ホワイトラベル※

エンドポイントセキュリティ製品
AVIRA PRIME

通信暗号化、接続IP秘匿製品
Avira PhantomVPN

アビラ合同会社
〒100-0005　東京都千代田区丸の内3-4-1　新国際ビル8階
Email: contact.oem.jp@avira.com
Web: https://oem.avira.com/ja

JNSA 会員企業のサービス・製品・イベント情報

■サービス紹介■

○商工会議所サイバーセキュリティお助け隊サービス
国産ＵＴＭ（レンタル）による「お守り」、２４Ｈ３６５Ｄ「見守り」、アラート通知による「お知らせ」、電話・メールでの「相談」インシデント時の（お助け実働隊地域ＩＴ事業者にによる）「駆け付け」、駆け付けに適用される「簡易な保険」、セキュリティ関係情報の「お届け」などがパッケージ化され、月額税込６，６００円（全国のいずれかの商工会議所・商工会の会員企業の価格。非会員でも同８，２５０円の明朗会計）
（サービス提供主体：大阪商工会議所）
【サービス情報詳細】
https://www.osaka.cci.or.jp/cybersecurity/utm/
◆お問い合わせ先◆
大阪商工会議所
経営情報センター（野田・中川・古川・石田）
TEL: 050-7105-6004
Email: cybersecurity@osaka.cci.or.jp

■サービス紹介■

○CylancePROTECT Managed Service for LanScope
新型コロナウイルス感染症対策で急激に増加するテレワークにおいて、勤務状況の把握／セキュリティの確保などを目的とし、LanScopeシリーズを無償提供いたします。
マルウェア検知結果のサマリーレポートを作成し、ご提供します。
【サービス情報詳細】
https://www.lanscope.jp/telework/promotion/
◆お問い合わせ先◆
エムオーテックス株式会社
E-mail: bd-sales@motex.co.jp

■サービス紹介■

○テレワーク導入 セキュリティアセスメントツール（無償サービス）
現在のセキュリティ対策状況について、総務省「テレワークセキュリティガイドライン」をもとに5つの観点で網羅的にチェックするアセスメントツールを無償で提供します。20問の質問に回答するだけで、テレワークを想定したセキュリティ対策が十分か、現状のセキュリティリスクを見える化し、対策の検討が必要な項目、推奨対策案を知ることができます。また、セキュリティコンサルタントによる対策立案の支援も提供しています。
【サービス情報詳細】
https://jpn.nec.com/cybersecurity/service/telework_riskassessment.html
◆お問い合わせ先◆
日本電気株式会社
E-mail: info@cybersecurity.jp.nec.com

■サービス紹介■

○i-Cybertech SOCサービス
弊社では、OT環境に対応したSOC運用サービスを提供しています。運用には、製造業・電気・ガス・水道・化学・石油・工場などの産業制御システム（ICS）の資産管理、リアルタイムモニタリング、異常検知、脆弱性診断に対応した、Nozomi Networks社製の「Guardian」を用いています。他にも適宜、自社開発製品やOT環境に適した海外製品を取り入れています。
また、顧客自身がSOC運用を行う場合を想定した、製品運用トレーニングも実施しています。
【サービス情報詳細】
https://www.isec.ne.jp/services/i-cybertech_soc/
◆お問い合わせ先◆
情報セキュリティ株式会社
TEL: 078-381-8980
E-mail: support-soc@isec.ne.jp

■サービス紹介■

一般的な外部からの脆弱性診断では探しにくい、潜在的なセキュリティ上・品質上の問題点を開発段階で発見できるソースコード診断。上流での問題解決によりコストや労力の削減を可能にします。弊社ではお客様のご要望にお応えし、さらに対応言語を増やしました。セキュリティプロフェッショナルによる手動診断に加え、安価に実施できるツール診断もご用意し、セキュアなアプリケーションの実現をサポートいたします。

【サービス情報詳細】

https://www.sqat.jp/sqat-core/

https://www.sqat.jp/cracker-probing-eyes-core/

◆お問い合わせ先◆

株式会社ブロードバンドセキュリティ

E-mail: sqat-inq@bbsec.co.jp

■製品紹介■

○Security Scorecard

自社や取引先のセキュリティ対策状況を瞬時に把握！

ドメイン名を基に、インターネット上の公開情報から自社のみならず国内外のグループ企業や取引先のセキュリティ対策状況を攻撃者視点で瞬時に把握できるセキュリティ・レーティング・サービスです。全10項目を5段階で評価し、問題点を具体的に指摘します。

サプライチェーン含むセキュリティ管理を効率的に計画、実施する事が可能となります。

【製品情報詳細】

https://www.tokiorisk.co.jp/service/cyber/ssc/

◆お問い合わせ先◆

東京海上日動リスクコンサルティング株式会社

TEL: 03-5288-6591

E-mail: pirates@tokiorisk.co.jp

■製品紹介■

OneLoginはIDとディレクトリサービスの統合管理及びシングルサインオンと認証強化をクラウドサービスとして提供いたします。5000を超えるクラウドサービスにシングルサインオンが可能です。

【製品情報詳細】

https://www.onelogin.com/jp

◆お問い合わせ先◆

OneLogin,Inc.,

TEL: 080-4869-4728

E-mail: yuichi.kimura@onelogin.com

事務局お知らせ

JNSA ANNOUNCE

後援・協賛・協力イベントのお知らせ

1. Japan Security Summit 2020
主　催：Japan Security Summit 2020 実行委員会
日　程：2020年9月1日 – 2020年10月16日（オンライン）
2020年10月27日 – 2020年10月28日
会　場：オンライン／日本科学未来館

2. 2020年度IPA中小企業情報セキュリティ講習能力養成セミナー
主　催：独立行政法人情報処理推進機構
日　程：2020年9月～2021年1月
会　場：全国12か所および動画配信
（オンデマンド形式）
日時、会場については、新型コロナウイルスの状況を考慮のうえ決定いたします

3. Black Hat Asia 2020
主　催：Black Hat Asia 2020
日　程：2020年9月30日～2020年10月2日
会　場：オンライン

4. 令和2年度「情報モラル啓発セミナー（北海道・山形・富山・山梨・兵庫・山口・愛媛）」及び「情報モラルシンポジウム（大分）」
主　催：中小企業庁、東北経済産業局、関東経済産業局、近畿経済産業局、中部経済産業局、四国経済産業局、中国経済産業局、内閣府沖縄総合事務局、九州経済産業局、公益財団法人ハイパーネットワーク社会研究所
日　程：2020年9月30日– 2021年2月下旬
会　場：北海道・山形・富山・山梨・兵庫・山口・愛媛・大分

5. SECURITY DAYS 2020
主　催：株式会社ナノオプト・メディア
日　程：2020年10月7日 – 2020年10月9日
会　場：JPタワーホール&カンファレンス（KITTE 4F）

6. サイバーセキュリティTOKYO for Junior
主　催：東京都立産業技術高等専門学校
日　程：2020年10月31日 – 2020年11月1日
会　場：東京都立産業技術高等専門学校品川キャンパス

7. Gartner IT Symposium/Xpo(r) バーチャル
主　催：ガートナー ジャパン株式会社
日　程：2020年11月17日 – 2020年11月19日
会　場：オンライン

8. ワイヤレスジャパン2020
主　催：株式会社リックテレコム・
日本イージェイケイ株式会社
日　程：2020年12月1日 – 2020年12月3日
会　場：東京ビッグサイト　青海展示棟　Aホール

9. セキュリティ&リスク・マネジメント サミット バーチャル
主　催：ガートナー ジャパン株式会社
日　程：2020年12月2日 – 2020年12月4日
会　場：オンライン

10. 関西物流展
主　催：関西物流展実行委員会
日　程：2021年6月16日 – 2021年6月18日
会　場：インテックス大阪

JNSA部会・WG活動内容

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：森克宏 氏／
JPCERTコーディネーションセンター）

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 2021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、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＞

- 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を支援するための、CISOハンドブックを展開する。

本年は、第2弾として技術評論社からの出版と、JNSA Webからの資料公開を予定している。

＜予定成果物＞

- CISOハンドブック第2弾（出版）
- 関連ドキュメントの公開

【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。

【中小企業対策支援施策検討会】

（リーダー：岩本真人 氏／トレンドマイクロ株式会社）

次のような観点について意見交換を行い、その結果を国や自治体などの公的機関や支援団体等への提言の形に纏める。

- 情報セキュリティベンダーはこのマーケットをどう捉えるのか
- 中小企業と情報セキュリティベンダーの双方にとっての利益となる対策導入のモデル
- 中小企業と情報セキュリティベンダー双方がWin-Winの状態を得るために必要な公的な支援施策

＜予定成果物＞

- 中小企業対策支援施策への提言、もしくは意見書などを想定し、具体的な成果物については、会合にて決定する。

【みんなで作ろう「サイバーセキュリティコミック」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活動を行う。

＜予定成果物＞

- SNSコミック8回配信

2. 調査研究部会

部会長：前田典彦 氏／株式会社ＦＦＲＩセキュリティ

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）

これまでの個人情報漏えいインシデントの調査と報告書作成をみなおし、今後の調査実施可否を決定する。

＜予定成果物＞

- 2019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、報告書

【セキュリティ市場調査WG】
（リーダー：礒部良輔 氏／興安計装株式会社）

国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継続して実施予定。

＜予定成果物＞

- 2019年度情報セキュリティ市場（国内）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）

(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・事故を防ぐシステム、以上の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。

2020年度も引き続き、特に(1)に重点をおいた活動を行う。（働き方改革/新興感染症対策等にも関係するテレワークへの取組も意識する）

＜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記事公開
- JNSA Pressへの寄稿、セミナー等への出講

【インシデント被害調査WG】
（リーダー：神山太朗 氏／あいおいニッセイ同和損害保険株式会社）

インシデント被害額の算定に関する新しい調査テーマで調査研究活動をおこなう。新しい調査テーマを試行し、正式に調査活動を開始する。

＜予定成果物＞

- 新調査テーマ関連の報告書

【IoTセキュリティWG】
（リーダー：松岡正人 氏／日本シノプシス合同会社）

IoTに限らず、新しい技術に関連するセキュリティ上の課題を整理・共有し、外部の組織などと連携しながら適切なリスクや脅威についての理解を広める支援をする。

＜予定成果物＞

- 「AIのサイバーセキュリティリスクと脅威について」取り纏める予定

【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。情勢に応じた旬なネタを集めた情報交換会を実施する。

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、国際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）

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なるIDの重要性の啓蒙

やプライバシー関連の問題提起や標準化に向けた意見交換を行う。

＜予定成果物＞

- 「IoT環境におけるアイデンティティ管理（仮称）」
- 「認証要素、認可要素とその関係（仮称）」

【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：阿部健二 氏／株式会社ラック）

「ＩＴU-T 勧告化が完全に完了する2020年9月までは、WGにて勧告化を支援すること。本勧告をＪＮＳＡの中で活用、実装できる環境構築（Ｔｅｓｔｂｅｄなどを含む）について検討すること。CCDSとの連携を進め、上記の検討をベースにＪＮＳＡのWGとして継続するか否かを決定すること。

＜予定成果物＞

- ＩＴＵ－Ｔ　勧告X.Ｅｌｆ-ｉｏｔ

【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。

- ISO/IEC27002の改定内容について適用管理策の観点での検討&整理
- ISMSの実装&運用についての事例研究（テーマ選定中）

【PKI相互運用技術WG】

（リーダー：松本泰 氏／セコム株式会社）

PKIの技術、標準化、法制度等の情報交換及び、議論を行う。関連して、eKYC、暗号鍵管理勉強会等を企画する予定。

＜予定成果物＞

- PKI day 2019の開催資料、JNSA PressへのPKI day 2020開催報告への寄稿を検討する。

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。2020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＞

- SecBoK2020

【ゲーム教育WG 】

（リーダー：長谷川長一 氏／株式会社ラック）

ボードゲームやカードゲームを利用したサイバーセキュリティ教育の普及と企画、ゲーム教育のノウハウのナレッジ化、ゲーム教育のファシリテーターの育成。

＜予定成果物＞

- 「Malware Containment」デジタル版（仮称）
- 「ゲーム教育ファシリテーターガイド（仮）」

【情報セキュリティ教育実証WG】
（リーダー：垣内由梨香 氏／
日本マイクロソフト株式会社）

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。

また作成した成果物（講義コンテンツ）のJNSA会員企業への共有と他の学校関連や団体への展開を計画している。

＜予定成果物＞

- セキュリティ基本教育コンテンツ

【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可能にし、女性セキュリティエキスパートの交流場所を提供する。また、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。

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ー向けのサービスをマーケティング部会と連携しながら拡充させる。

特にソリューションガイドを、ユーザーにも、会員にもより利用しやすい環境とするための改修を行う。また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：西浦真一 氏／
キヤノンマーケティングジャパン株式会社）

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＞

- 理解度チェック新規問題作成・問題改修

【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）

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

6. マーケティング部会

部会長：小屋晋吾 氏／ニュートラル株式会社
副部会長：持田啓司 氏／株式会社ラック

JNSAの認知度向上やWG成果物の普及促進を目的とした活動を行うとともに、会員企業を獲得するための施策を立案、実行する。

＜予定成果物＞

- 全国セミナーの実施
- その他ノベルティ等の検討

7. 事業コンプライアンス部会

部会長：西本逸郎 氏／株式会社ラック

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う。

＜成果物＞

- サイバーセキュリティ業務における倫理行動宣言

【企画WG】

（リーダー：唐沢勇輔 氏／
Japan Digital Design 株式会社）

本部会の企画検討や外部機関とのPoCを担う。また、賛同企業の募集など、部会全体の取り組みに関する企画運営を行う。

＜予定成果物＞

- 法令改正の提案書

【調査WG】

（リーダー：小村誠一 氏／
エヌ・ティ・ティ・アドバンステクノロジ株式会社）

海外の事例や関連法制度に関する調査を実施する。今年度は英米におけるサイバー犯罪法体系の調査や、海外における事例を調査予定。

＜予定成果物＞

- 調査結果を資料として公開

【法令リスク研究WG】

（リーダー：田原祐介 氏／株式会社ラック）

サイバーセキュリティ業務の法令リスク一覧を作成したり、国内における事例研究を行う。どのような業務に、どういったリスクがあるか参照できる資料作成を目的とする。

＜予定成果物＞

- 法令リスク研究を一覧として公開

8. 西日本支部

支部長：元持哲郎 氏／アイネット・システムズ株式会社

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システム導入、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のあるべき姿を検討する。

＜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形式で行う。

【勉強会企画検討WG】

（リーダー：永塚遼 氏／SCSK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

事業者間の連携や情報交換による業界活性化のための活動を行う。また、政府機関への政策提言や政策実現のための適切な事業者紹介を行う。

＜予定成果物＞

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

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。

＜新技術とオペレーションPj：年間活動予定＞

・新技術とオペレーションPj
　新たな技術トピックのうち、オペレーションに影響が出そうなものはどれか検討
　特に取り上げるものを決定してブレーンストーミングと議論
・TSI(セキュリティサービス認定検討タスクフォース)
　「情報セキュリティサービス基準適合審査」検討会事務局と連携

＜予定成果物＞

- マネージドセキュリティサービス選定ガイド Ver2.0

【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）

ユーザ向けセキュリティ診断サービスの解説書や、事業者向けのセキュリティ診断サービスのガイドラインを作成することを目指す。

【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ついての認知度向上を目的とし、普及啓発活動を行う。

【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。

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（株式会社三菱総合研究所）

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。

＜予定成果物＞

- リモート署名ガイドラインの公開を予定

13. 産学情報セキュリティ人材育成検討会

座長：江﨑浩 氏/東京大学 大学院

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、引き続きJNSAインターンシップを実施する。

学生と企業間の意見交換・交流のための「JNSAインターンシップ交流会」を例年春季に開催しているが、秋以降に開催を検討する。

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

継続的に協賛企業の協力を得て、SECCON CTFならびに初心者向け勉強会「SECCON Beginners」、女性限定ワークショップ「CTF for GIRLS」を開催予定。

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り活動を行う。

JNSA 役員一覧　2020 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 東京大学 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）

青嶋　信仁	（株式会社ディアイティ）
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）
後藤　　忍	（セコムトラストシステムズ株式会社）
小屋　晋吾	（ニュートラル株式会社）
櫻井　秀光	（マカフィー株式会社）
佐藤　憲一	（株式会社OSK）
西本　逸郎	（株式会社ラック）
藤伊　芳樹	（大日本印刷株式会社）
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）
山口　政博	（ユニアデックス株式会社）

幹　事（50音順）

秋葉　淳哉	（エヌ・ティ・ティ・アドバンステクノロジ株式会社）
有松　龍彦	（株式会社インフォセック）
岩竹　智之	（ユニアデックス株式会社）
大木　由利	（大日本印刷株式会社）
斧江　章一	（キヤノンマーケティングジャパン株式会社）
垣内　由梨香	（日本マイクロソフト株式会社）
香取　弘徳	（株式会社フーバーブレイン）
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）
下村　正洋	（NPO日本ネットワークセキュリティ協会）
鈴木　英樹	（株式会社OSK）
関場　哲也	（株式会社カスペルスキー）
高野　敏男	（日本電気株式会社）
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）
中間　俊英	（株式会社ラック）
野間　祐介	（株式会社インターネットイニシアティブ）
能勢　健一朗	（東芝デジタルソリューションズ株式会社）
萩原　健太	（グローバルセキュリティエキスパート株式会社）
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FFRIセキュリティ）
本川　祐治	（株式会社日立システムズ）
元持　哲郎	（アイネット・システムズ株式会社）
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）
金子　啓子	（大阪経済大学 経営学部）
佐々木良一	（東京電機大学総合研究所特命教授¦サイバーセキュリティ研究所所長）
武藤　佳恭	（慶應義塾大学 教授）
手塚　　悟	（慶應義塾大学 環境情報学部 教授）
前川　　徹	（東京通信大学情報マネジメント学部 学部長 教授）
森山　裕紀子	（早稲田リーガルコモンズ法律事務所 弁護士）
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

会員企業一覧　2020年9月現在　245社　50音順

【あ】

(株)RSコネクト
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
アイレット(株)
アクセンチュア(株)
アクモス(株)
(株)アシスト
(株)アズジェント
アドソル日進(株)
アドビシステムズ(株)
Avast Software Japan(同)　New
アビラ(同)
(株)アピリッツ
アマゾン ウェブ サービス ジャパン(株)
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)
EY新日本有限責任監査法人
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
インプレイス(株)　New
ウォッチガード・テクノロジー・ジャパン(株)
AOSデータ(株)　New
SCSK(株)
SGシステム(株)
SBテクノロジー(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)
NECプラットフォームズ(株)　New
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
(株)FFRIセキュリティ
エムオーテックス(株)
(株)エムティーアイ　New
エントラストジャパン(株)　New
(株)OSK
(株)大塚商会
岡三情報システム(株)
沖電気工業株式会社　New

【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)ケーエムケーワールド
(株)km2y
KDDI(株)
KDDIデジタルセキュリティ(株)
(株)KPMG FAS
KPMGコンサルティング(株)
コインチェック(株)
興安計装(株)
(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（同）
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
（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）
Sign.net Japan G.K. New
（株）さくらケーシーエス
GMOグローバルサイン（株）
G・O・G（株）
（株）シーディーネットワークス・ジャパン New
ジーブレイン（株）
ジェイズ・コミュニケーション（株）
（株）JSOL
JBサービス（株）
JBCC（株）
一般社団法人 JPCERT コーディネーションセンター
シスコシステムズ（同）
システム・エンジニアリング・ハウス（株）
Japan Digital Design （株）
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）
（株）Speee
セイコーソリューションズ（株）
（株）セキュアサイクル
（株）セキュアスカイ・テクノロジー
（株）セキュアソフト
セキュアワークス（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）
ソフトバンク（株）
（株）ソリトンシステムズ
（株）ソルネットシステム
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
（株）宝情報
タレスDIS CPLジャパン（株）
Checkmarx Ltd
（株） 中電シーティーアイ
都築電気（株） New
TIS（株）
（株）ディアイティ
デジサート・ジャパン（同）
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）
（株）東芝 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）
Toyota Research Institute-Advanced Development, Inc.
トランスコスモス（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（同）
（株）日本総合研究所
日本電気（株）
日本電信電話（株）
日本ビジネスシステムズ（株）
日本プロセス（株）
日本マイクロソフト（株）
日本ユニシス（株）
ニュートラル（株） New
（株）ネクストジェン
ネットワンシステムズ（株）

【は】

パーソルテクノロジースタッフ（株）

パーソルプロセス&テクノロジー（株）
（株）パソナテック
パナソニック（株）
パロアルトネットワークス（株） New
（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
（株） 日立ソリューションズ・クリエイト New
飛天ジャパン（株）
BBソフトサービス（株）
（株）PFU
PwCコンサルティング（同）
華為技術日本（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
富士フイルムシステムズ（株）
（株）Preferred Networks
（株）ブロードバンドセキュリティ
（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）
丸紅情報システムズ（株）
丸紅ネットワークソリューションズ（株）
みずほ情報総研（株）
三井物産セキュアディレクション（株）
三菱スペース・ソフトウエア（株）
（株）三菱総合研究所
三菱総研DCS（株）
三菱電機（株）
三菱電機インフォメーションシステムズ（株）
三菱電機インフォメーションネットワーク（株）
（株）mediba

【や】

（株）ユービーセキュア
ユニアデックス（株）
（株）YONA

【ら】

（株）ラック
Rapid7 Japan（株） New
（有）ラング・エッジ
（株）リクルート
リコージャパン（株）
（株）レピダム
（有）ロボック

【わ】

（株）ワイズ
OneLogin, Inc. New

【特別会員】

一般社団法人 IIOT
（ISC）2　Japan
大阪商工会議所
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
トラストサービス推進フォーラム
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

他2社

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。）

サイエンスパーク株式会社　畑　正憲

JNSA会員の皆さま。サイエンスパーク株式会社の畑と申します。
この度はアドソル日進株式会社の野田様よりご紹介をいただき、自己紹介をさせていただきます。どうぞよろしくお願いいたします。

先に弊社の紹介を少し。サイエンスパークという会社をご存じですか？各地にある研究開発拠点の「○○サイエンスパーク」をご想像された方も少なくはないかもしれませんが、直接的な関係はありません。

弊社はカメラやカードリーダーといったPCなどに接続するデバイスを制御する「デバイスドライバー」関連の開発を軸にした事業展開をしており、そのデバイスドライバーの技術を利用したセキュリティ製品の提供を行っています。

JNSAには2015年から会員企業として参加させていただいておりますが、実はNSF2003のセキュリティ論文募集において、慶應義塾大学 武藤教授との共著で「安心して暮らせる社会構築のためのセキュリティ戦略とドライバーウエアの提案」を提出し佳作をいただいております。

私についてですが、弊社のセキュリティ製品である「Driverware Software」の開発に携わっております。

Driverware SoftwareはWindowsおよびMACのエンドポイントセキュリティ基盤であるDriverware SDKと、このSDKを組み込むパッケージソフトウェアです。

Driverware SDKを使用することでエンドポイントセキュリティの製品開発が可能であり、自社製品のパッケージソフトウェアへの組み込みのほか、他社製品へも組み込みいただいております。

開発拠点は丹沢山地を望む神奈川の中部に位置し、普段は引きこもり生活を続けているがために、都会に出て見聞を広めてこい」とのお達しを受け、JNSAの社会活動部会に参加させていただきました。

部会やJNSA主催イベントに参加させていただくと、私のセキュリティの知識は偏りがありまだまだ勉強することが多いと痛感するに至りまして、これは良い機会をいただけたと思う次第であります。

プライベートでは、趣味と呼べるほどではありませんがDIYで自宅をいろいろといじっています。休暇期間は外出を自粛して、レンジフードを省エネで掃除が簡単なものに交換したり、愛猫が開き戸を開けたままにしないように別の入り口として扉にペットドアをつけたりしていました。

普段はコンピューター上で動作するソフトウェアを開発しておりますが、手に残るハードウェアはまた違った達成感があると思います。

昔は手動で頑張れば良いと思っていましたが、電動工具は偉大です。1つ買うと同じバッテリーで動作する他の工具も欲しくなってしまいます。

そして気が付くと電動工具が増えたりしますが、活躍よりも収集がメインとならないようにしなくてはいけませんね。

それでは会員の皆さま、事務局の皆さま、今後ともよろしくお願いいたします。

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。）

SCSK株式会社　永塚　遼

JNSA会員の皆さま、はじめまして。SCSKの永塚と申します。
事務局の方からご依頼いただきましたので、私の自己紹介をさせていただきます。

SCSKには転職で入社しました。会社としては住友商事グループのシステムインテグレーターとして、ソフトウェアやシステム開発・販売がメインですが、その中のセキュリティを専門に扱う部署に属しており、SOCサービスの企画検討や脆弱性診断業務に携わっております。

JNSAにはU40部会の勉強会を中心に参加させていただいております。また、2020年度よりU40部会の勉強会企画検討WGのリーダーを務めてさせていただくこととなりました。これまではJNSA事務局の1階に一堂に介して開催することが多かったのですが、新型コロナの影響によってオンラインでの開催への切り替えることとなり、その内容や開催方法の詳細を詰めていることになります。前例のない取り組みではありますが、その検討過程を面白くも感じております。

大学時代は情報工学を専攻しておりましたが、画像処理を研究テーマとしており、セキュリティについてはあまり勉強してきませんでした。新卒入社した後はアプリケーション開発やインフラ構築を行っておりましたが、情報セキュリティスペシャリスト（現情報処理安全確保支援士）の試験に合格したことをきっかけにセキュリティ運用に携わるようになりました。セキュリティの仕事にはアプリケーション、ネットワーク、コンピュータアーキテクチャ、法律などの幅広い知識が求められ、また技術の移り変わりが激しいため、要求されるハードルは高いと感じておりますが、その分、やりがいの大きい業務を任される機会も多いと感じております。

話は変わりますが、昔からテレビゲームを趣味としてよくやっています。前提知識や環境を理解した上で、CPUや人相手に、より勝率の高い戦略・戦術を練ることが面白いと感じております。また、もう一つの趣味として資格試験があり、仕事内外問わず様々な資格を受験、取得しております。こちらも根本的なところは同じと感じており、効率よく知識を蓄え、試験対策を行い、資格取得というゴールを目指す過程を楽しんでおります。

最後になりましたが、今後もJNSAの活動に少しでも多く貢献できるように努めてまいりたいと考えております。また、勉強会の開催にあたって皆さまのご協力をいただくこともあるかと思います。その際はご協力のほどどうかよろしくお願いいたします。

SECURITY CONTEST (SECCON) 2020

https://www.seccon.jp/2020/

SECCON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］（2019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］（2019年度実績）

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、SecHack365、日本電信電話株式会社、ネットエージェント株式会社、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、ネットワンシステムズ株式会社、防衛省

ブロンズスポンサー：　株式会社アズジェント、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、ジェイズ・コミュニケーション株式会社、株式会社ディアイティ、Digital Travesia、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VSN、北陸通信ネットワーク株式会社、ヤフー株式会社、株式会社ラック、株式会社ブロードバンドセキュリティ

インフラスポンサー：　さくらインターネット株式会社

機材スポンサー：　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: info2020@seccon.jp）

[開催スケジュール]

■SECCON 2020

日　程	会　場	内容
2020年10月10日（土）、11日（日）	インターネット（オンライン開催）	CTF(日本語＋英語)

■CTF for GIRLS

日　程	会　場	内容
2020年12月	インターネット（オンライン開催）	第15回ワークショップ
2021年2月	未定	4-Girls CTF 2020

■SECCON Beginners 2020（CTF未経験者向け勉強会）

日　程	会　場	内容
2020年5月23日（土）、24日（日）	インターネット（オンライン開催）	CTF(日本語)

■SECCON 2020 Workshop

日　程	会　場	内容
2020年12月19日(土)	インターネット（オンライン開催）	ワークショップ・セミナー

[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、毎回定員に達する人気イベントです。

SECCONメールマガジンのご登録はこちらから！

https://s.bmb.jp/bm/p/f/tf.php?id=jnsa_12212_6440&task=regist

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（CISSP,SANS, セキュア Eggs, EC-Council 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.49

2020 年 9 月 25 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

知っておきたい情報セキュリティ
理解度チェックサイト プレミアム
http://slb.jnsa.org/eslb/

活用のポイント・メリット

- 社員教育をしたいがコストは最小限にしたい
- 問題を自分で作る時間がない
- 社員のレベルを把握したい

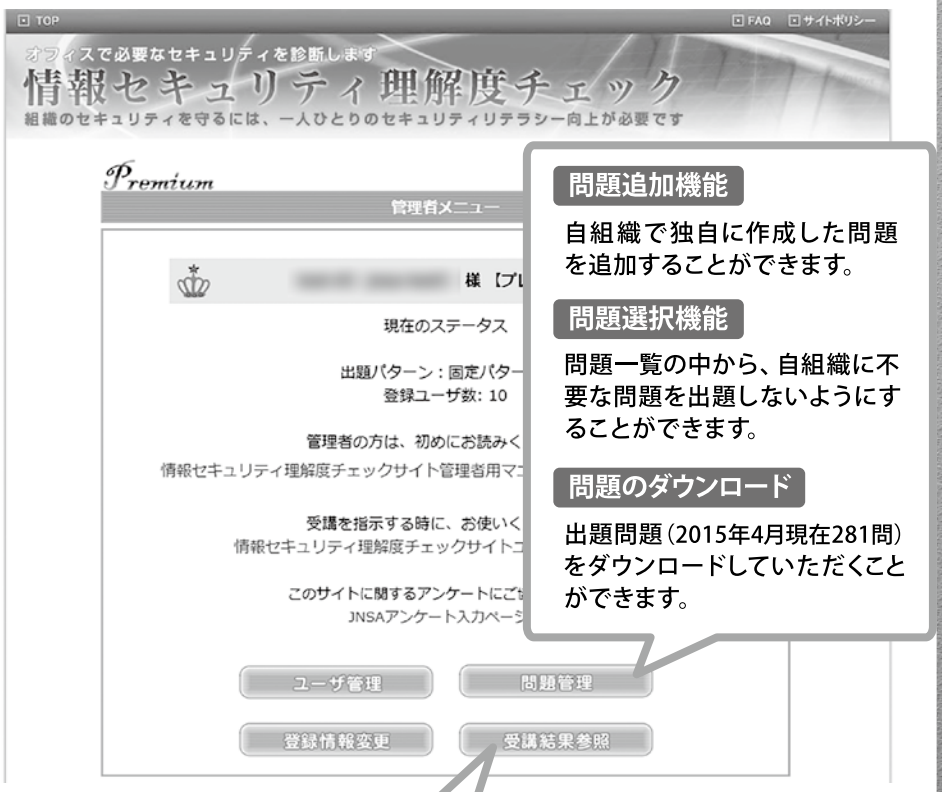
「情報セキュリティ理解度チェック・プレミアム」は、無償版「理解度チェックサイト」を、組織ごとにカスタマイズできる機能がついた有償サービスです。管理者機能をより強化し、独自の問題の追加も可能です。ぜひ社内教育や情報セキュリティ関連の補助ツールとしてご活用下さい。

＜料金の一例＞
登録人数51名～100名の場合
年間利用料[定価]：50,000円(税別)

登録人数により、7コースご用意しております。詳しくは事務局までお問合せください。

なお、無償版の「情報セキュリティ理解度チェック」サイトもございますので、是非お試しください。

【お問合せ先】slb@jnsa.org



問題追加機能
自組織で独自に作成した問題を追加することができます。

問題選択機能
問題一覧の中から、自組織に不要な問題を出題しないようにすることができます。

問題のダウンロード
出題問題（2015年4月現在281問）をダウンロードしていただくことができます。

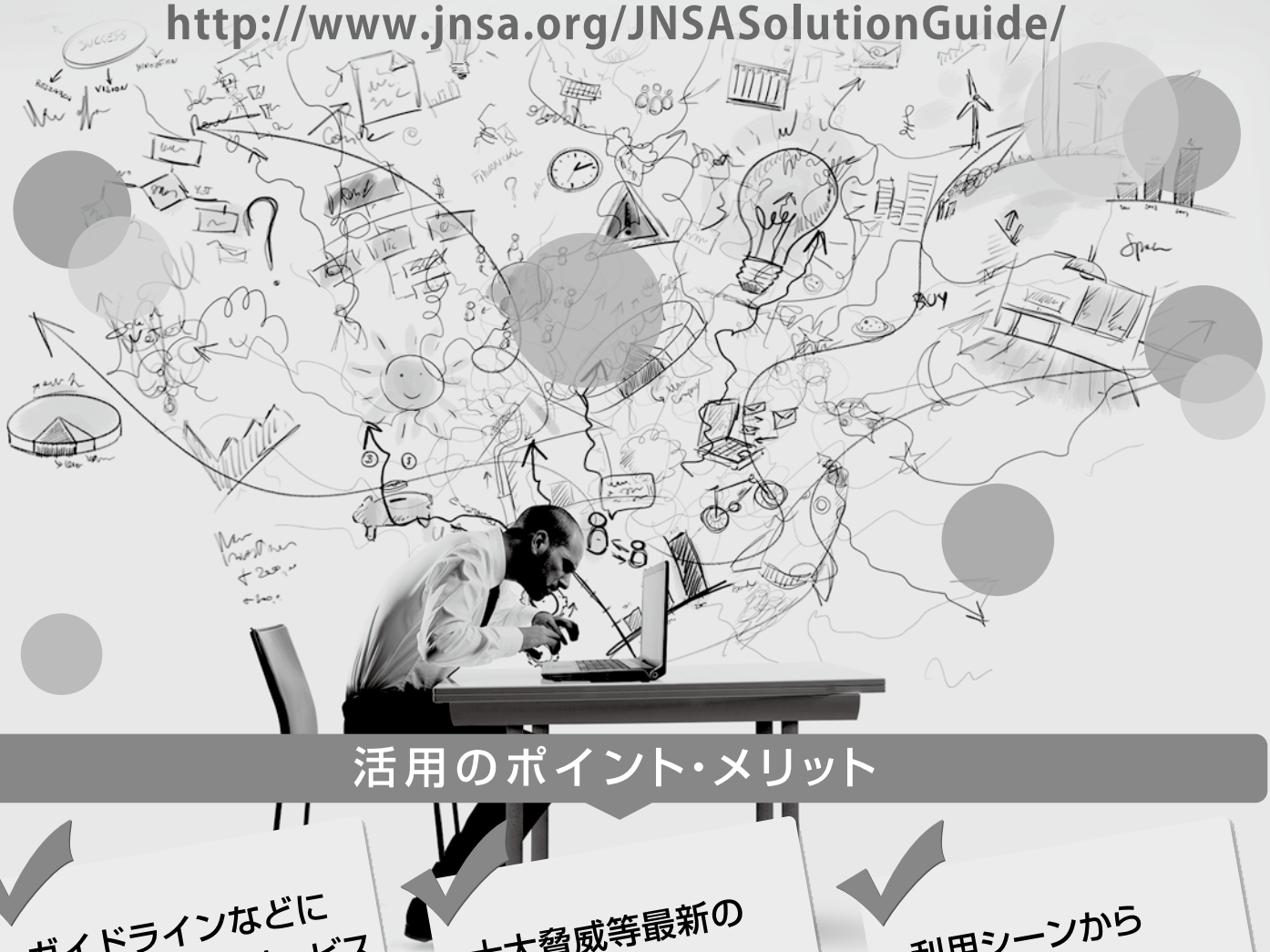
管理者機能の強化
受講者（ユーザ）の受講結果を見ることができます。ダウンロードできるcsvファイルの内容がより詳しくなり、誰がどのように間違えたかがわかります。

JNSA

セキュリティにまつわる課題解決を支援します

JNSAソリューションガイド

http://www.jnsa.org/JNSASolutionGuide/



活用のポイント・メリット

ガイドラインなどに
対応する製品・サービス
を検索できる!

十大脅威等最新の
脅威から検索できる!

利用シーンから
対策を検索できる!

JNSAソリューションガイドサイトは、JNSAの会員企業が取り扱うネットワークセキュリティに関する製品やサービス、イベント情報などをご紹介しているサイトです。さまざまな角度から検索できるような仕組みになっていますので、セキュリティ製品やサービスの導入をご検討される際にはぜひご活用下さい。

JNSA

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 06-6886-5540