SPRING 2023
VOL. 52

JNSA PRESS

JAPAN NETWORK SECURITY ASSOCIATION

寄稿記事

03 中小企業におけるサイバーセキュリティのリアルな実例と現実的対策

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

日本独自のセキュリティ対策の推進へ

情報通信研究機構　主管研究員
JNSA 副会長　中尾　康二

近年の情報ネットワークの広域化、高速化、利便性の向上、及び情報システムの高度化、大容量化、高機能化などを背景に、通信の信頼性はもとより、情報システム及び企業における情報セキュリティ技術およびサイバーセキュリティ技術の重要性が増しています。

このような環境において、最近よく耳にするセキュリティ関連のキーワードとして、「ゼロトラスト」や「SBOM」などがありますが、ここでは、SBOMについて少し掘り下げてみたいと思います。

SBOMは、Software Bill of Materials（ソフトウェア部品表）の略称で、各製品のソフトウェア部品（コンポーネント等）をその製品の購入者/利用者に対して直接または公開情報として提供することを要求するものです。SBOMを利用することで、システム構築者はソフトウェアコンポーネントが最新であることを確認でき、新しい脆弱性にも迅速に対応することが可能となります。また、ソフトウェアの購入者にとっては、ソフトウェアの脆弱性分析、製品のリスク分析などに役立てることができ、SBOMはサプライチェーンの環境においてソフトウェア資産のセキュアな管理方法として早いタイミングで米国において注目されていました。2021年5月には「ソフトウェアのサプライチェーンセキュリティの強化」として、米国の大統領令（EO14028）に政府調達におけるSBOM活用が明記されたことをきっかけに、米国統制当局を中心とした取引組織へのSBOM整備の義務化などが急速に進みつつあります。米国における流れを受け、日本の総務省（通信分野におけるSBOM導入調査）、経済産業省（自動車業界、医療機器業界、ソフトウェア業界におけるSBOM活用モデルの検討等）などにおいてもSBOMがソフトウェア管理の施策として取り上げられるようになりました。

では、米国でどのようにSBOMが注目されるようになったのでしょうか。いろいろな解釈があるかもしれませんが、オープンソースソフトウェア（OSS）の活用の検討がその発端になっていると理解します。すなわち、OSSの活用にあたっては、各OSSソフトウェアの著作者が定めたライセンスを遵守し、OSSの適切な管理を実施することが必要となります。そのため、The Linux Foundation の公式プロジェクトの一つである「OpenChainプロジェクト」では、各組織が組織内に確立すべきOSSコンプライアンスプログラムの要件を「OpenChain仕様」として規定し、その普及を推進しており、OpenChain仕様をISO/IEC 5230として2020年に国際規格化を完了させました。

ISO/IEC 5230はOpenChain仕様がほぼそのまま国際規格となったもので、その要求事項の一つとして「BoM（Bill of Materials）」を規定しており、OSSコンポーネントの部品表の作成・管理のためのプロセスが存在することを要求しています。部品表としては、供給ソフトウェアを構成するOSSコンポーネント、識別されるライセンス、ユースケース、改変の有無などが部品要素として定義されています。

以上のことから、米国政府におけるSBOMの議論は、OSSコンポーネントの部品表の作成・管理プロセスと深い関係があり、サプライチェーンセキュリティのためのソフトウェア管理としてSBOMの整備に目を向け、政府調達におけるSBOM活用やSBOM整備の義務化を推進していく流れとなったと読み解けます。米国の活動の素晴らしいところは：

1. 早いタイミングでOSS業界団体により、OpenChain仕様化が手掛けられたこと
2. 当該仕様を国際標準化させ、世界的規模での仕様活用に目を向けたこと
3. 米国政府内部のサプライチェーンセキュリティの検討WGで、OpenChain仕様に目を付け、サプライチェーンセキュリティのソフトウェア管理の手法として提言し、それを大統領令としてトップダウンの指示をしたこと
4. 上記の活動を受け、政府調達ソフトウェアに対するSBOMの活用を促進したこと

などが挙げられると思います。

日本として、米国による素晴らしい活動を見習い、それらを積極的に取り入れることには大賛成ですが、今後は日本独自のセキュリティ要件を加味した日本主導型のセキュリティ対策の推進が大きく期待されるところです。特に、セキュリティベンダーが集結する我々JNSAにとっては以下のような活動が期待されるのではないでしょうか。

- 日本のビジネス環境で取得する生のセキュリティ要件を中立的、かつ網羅的に収集・整理できること
- 抽出した要件を満足するような対策仕様（OpenChain仕様のような）の検討を専門メンバで策定できること
- 作成する対策を政府に提言できること
- 検討した対策を各セキュリティベンダーにおいて実証評価を行い、対策仕様の改善、精度向上を推進できること

これまでのJNSAの活動においても、上記のような活動は個別の活動として実施されてきたと認識していますが、JNSAが主導して日本におけるセキュリティ対策の大きな流れを作っていける時期に来ていると痛感しております。そのためには、JNSAにおける若手メンバによる具体性をもった忌憚のないアイディアが必要です。2023年のJNSAにおいては、若手のアイディアや斬新な構想を真摯に捉え、それらのアイディアに基づいたJNSAにおける活動の構想を練り、日本独自のセキュリティ対策の推進に貢献するための第1歩を踏み出せるよう切に期待します。

中小企業におけるサイバーセキュリティのリアルな実例と現実的対策

大阪商工会議所　経営情報センター　課長
野田　幹稀

サイバーセキュリティに関する啓発情報やマスコミ報道は、中小企業に対するメッセージ性がやや稀薄なケースが散見される。とりわけ公表される被害事例は大企業や政府関係機関、外国企業のものが中心であり、中小企業の被害事例が紹介されることは滅多にない。これでは中小企業は当事者意識を持ちにくい。本稿では、中小企業におけるサイバーセキュリティのリアルな実例と現実的な対策方法につき紹介する。

サイバー攻撃の「攻撃する側」は、個人ハッカーによる愉快犯から、犯罪組織（国家を含む）による経済犯に変化してきている。経済犯である以上、攻撃者は「黒字」を前提としているので、一種のビジネスであり、一定のビジネスモデルに基づき利益が最大化するよう、分業して効率的に実施しているものと考えられる。

「攻撃される側」も変化している。IoT の急増により、攻撃対象の絶対数自体が増えてきている。IoT は物理的に小さいため、ウイルス対策ソフト等を入れられないケースが多く、視界に入らない場所に置かれている場合も少なくないため、多くの場合、資産管理されていない。よって、サイバー攻撃の恰好のターゲットになる。横浜国立大学の調査によると、セキュリティを講じていない IoT をインターネットに接続したところ最短 38 秒でコンピュータウイルスに感染したとのことである。もはや、サイバー空間は「リスクがある」などという次元ではなく「無法地帯」といえよう。

では実際のところ、中小企業にサイバー攻撃がどの程度来ているのか、ということだが、2018 年に大阪府内の、業種・規模などがまちまちの 30 社の中小企業にご協力を頂き、大阪商工会議所、神戸大学、東京海上日動火災保険㈱と共同研究調査をしたところ、実に 30 社全て（100％）で攻撃が確認された。2019 年度に独立行政法人情報処理推進機構（以下、IPA）から請け負い実施した「サイバーセキュリティお助け隊実証事業（以下、お助け隊実証）」では、1 社あたり平均で月 56 件の「外→内」の攻撃、月 4 件の「内→外」の不正通信が観測された。

次に、サイバー攻撃の対象に地域的差異や業種的差異があるのだろうか。2019 年度、2020 年度のお助け隊実証で大阪商工会議所が日本電気㈱などと共同調査したところ、大都市圏である大阪・京都・兵庫と、大都市圏以外の滋賀・奈良・和歌山との比較では有意差が見られなかった。また、業種による有意差も見いだせなかった。「うちみたいな業種は、狙われることはない」といった認識の中小企業経営者は少なくないが、根拠なき過信といえよう。

ここで IPA の「情報セキュリティ 10 大脅威」の上位案件を、中小企業に関連づけながら見てみよう。

2023 年の「組織」における脅威の 1 位は「ランサムウエア」である。ランサムウエアの身代金の額は比較的少額であるケースもあり、被害者の 32％が身代金を支払ったという調査結果もある。数年前にＮＨＫがランサムウエアの犯罪者集団「REvil」に取材したシーンがニュースで放映された。記者が「身代金を払ったらデータを元に戻すか？」と質問すると「必ず戻す。我々は信用を失ったら終わりだ」と回答していた。パソコンの画面の向こう側にも“必死のパッチになっている血の通った人達”がいるのである。最近は「RaaS（Ransomware as a Service）」なる言葉も登場し「悪のエコシステム」が“円滑に”回っているとさえ言われている。

数年前、ある中小企業の経営者が大阪商工会議所に相談に来られた。直接的な相談内容は「ビットコインって何ですの？」といったものだった。

相談員は仮想通貨の概要と入手方法について淡々と説明したが、帰り際に「そもそも、なぜビットコインが必要になったのですか？」と質したところ、「いや～実はなぁ、パソコンやってたら、いきなりパソコンが動かなくなったんや。ビットコインで払ったら直りますって出てきてん。どうやったらビットコインが手に入るんか知りたいんですねん。パソコン動かんと仕事にならへんねん」と。民話のような話だが、これは実話である。

次に脅威２位の「サプライチェーン攻撃」について。サプライチェーンの頂点に君臨する大企業に対し、「貴社の取引先中小企業が受けたサイバー攻撃被害が貴社（大企業）にも及んだ経験があるか」を聞いたアンケート調査（2019 年 5 月、大阪商工会議所が大企業 118 社に実施）によると、25％の大企業が、取引先中小企業が受けたサイバー攻撃被害に起因して大企業側もサイバー攻撃被害を受けていることが分かった。

そして、今後同じようなことが起きた場合、「その原因を作った中小企業に対してどういう対応を取るか？」との質問に対し、実に 47％は「損害賠償請求をする」と回答し、29％は「取引停止も辞さない」と回答している。要するに、中小企業がサイバー攻撃を受けるということは、「被害者なのに加害者になってしまい、最終的には事業継続が困難になることもありうる」ということである。これは中小企業にとっては耳の痛い話である。

2020 年 1 月に下請法の下請け振興基準が改正され、「下請事業者の努力」として「必要なセキュリティ対策を行うこと」、「それに対する親事業者の協力」として「セキュリティ対策の助言・支援を行うこと」が明記されたものの、依然として、大企業側がその優越的地位を濫用して特定のセキュリティサービスの利用を下請け先等に強要することは法律上許されていない。また大企業側が下請け中小企業側にセキュリティ対策の実施を“依頼”した場合、当該コストが（自社への）納入価格に転嫁され、結果として仕入原価が上がるケースもある。この場合、下請け中小企業側のセキュリティ対策投資は、結果として元請け大企業が実質的に肩代わりするのと同じになってしまう。だから大企業側の調達部門は、下請け中小企業に対しサイバーセキュリティ対策の推進を求めたがらない傾向にある。これは同じ大企業の情報システム部門やコーポレートガバナンス部門の思惑と相反しがちである。

次に脅威３位の「標的型攻撃」についてだが、中小企業の経営者と話をしていると、大抵は「うちみたいな中小企業は狙われへん。標的になんかされへんって」と仰る。しかし、先述の通り、最近のサイバー攻撃の多くは経済犯罪ゆえ、攻撃者側も効率性を重視する。したがって、よほど世界レベルの高度な技術を有する会社は別として、通常、攻撃者は、中小企業のことを１件１件個別に事前調査して、特定の会社を狙い撃ちしたり、狙いから外したり、といった“１tol マーケティング”はやっていないと思われる。そんなことをやっていてはペイできないからである。よって、標的型攻撃メールといっても、その実態はバラマキ型の絨毯爆撃メールであり、「うちなんて、標的になるほど、有名な会社ではない」と、油断すべきではない。どんな中小企業でも、広く浅く「標的」になり得るという意識が必要である。

また「うちには値打ちある情報なんてない」と言う経営者が多いが、情報の価値を決めるのは「情報を持っている側」ではなく「情報を盗む側（又は買う側）である」と認識すべきであろう。

私は事あるごとに IPA の担当者などに「標的型攻撃」という言葉を何か別の言葉に変えるように進言しているが、なかなか取り合ってもらえない。「標的型攻撃」というのは、攻撃対象が大企業であることを想定したネーミングであるように感じる。このフレーズは、中小企業のサイバーセキュリティ意識をかえって阻害しているようにすら感じる。「特定の属性を狙った攻撃」などに変更できないものだろうか。

ここからは、中小企業へのサイバー攻撃の事例

（上記の共同研究調査、実証事業等）を幾つか紹介する。

従業員約 10 人の金属製品製造業 A 社では、ラトビアという旧ソ連の国から、管理者パスワードでログインされ、パソコンが長期間にわたり遠隔操作されていた。同社の社長は調査前には「うちなんて、狙われる技術もないし、値打ちのある個人情報も持っていない」と言っていた。ラトビアに取引先、現地工場、出張経験もなく、同国に関係する IT サービスも受けていない。この会社について、とりわけショックだったのは、社長の息子である専務が IT 企業出身者であった点である。そんな企業ですらやられている。

従業員約 80 人の土木工事業 B 社では、社内端末が、深夜を含め、外部の悪性サイトと通信していた。こうした事象は多くの中小企業で日常的に発生しているものと推定されるが、気付いてすらいないのが現状であろう。蛇足ながら、同社の社長は工学博士である。そんな社長がいる会社ですら課題の存在に気付いていないのである。

従業員約 40 人の建築材料卸売業 C 社では、外部の大量のゾンビ化したパソコンから大量の通信が送られ、通信が飽和状態になり営業妨害を被る DDos 攻撃に遭っていた。

従業員約 80 人の化学品卸売業 D 社は、ウイルス感染に伴い、社員のメールアドレスで迷惑メールが多数の取引先に送信されてしまい、取引先のメールサーバが同社からのメールを遮断してしまった。

従業員約 900 人の事務用文具製造販売業の E 社では、自社運営の通販サイトに不正アクセスを受け、顧客のクレジットカード情報が漏洩。同通販サイトは 4 ヵ月間閉鎖を余儀なくされ、4 千万円の逸失利益が発生した。

このように増加・巧妙化するサイバー攻撃の現状に対し、中小企業では、実際、どの程度の対策をしているか、について、先述の 2019 年度、2020 年度のお助け隊実証参加企業での調査結果を紹介する。

先ず「人」の現状だが、専任担当者がいると回答した企業は 1 割未満であり、6 割の中小企業で、専任担当者はもとより兼任担当者すら不在というのが実態である。一般的に問題視される「ひとり情シス」どころか「ゼロ情シス」である。

少し話が横道に逸れるが、「ひとり情シス」は常に孤独であり、重責であり、陽が当たらないポジションである。人事考課という点でも「何も問題が起こらなくて当たり前。せいぜい平均点がもらえる程度。何か問題が起こったら大減点」といった、“美味しくない”立場である。情シスの離職率は高く、ある IT ベンダーの調査によると、従業員 100 人～ 1000 人未満の中堅企業の離職率は 21％と非常に高い。IT 人材の不足が懸念されている今後のわが国にあって、また今後一層サイバー攻撃が激烈化する可能性があるなかにあって、こうした情シス担当者の「地位や処遇の低さ」「離職の多さ」は由々しき問題だといえよう。情シスは、本来、戦略部門として遇されるべきである。

情シスのメンタルを更に悪化させるであろう調査結果が IPA の「中小企業の従業員へのアンケート調査（2021 年 12 月）」で明らかになった。「会社の情報管理ルールに違反した従業員が、その事実を、会社や上司に報告したか」という質問項目で、43％が「1 度も報告を行わなかった」と回答している。経営者や情シスが把握していない「かくれサイバートラブル」が一定数発生しているかもしれない可能性を示している。

次に、サイバー攻撃対策にかけている「お金」についてだが、お助け隊実証参加企業（従業員数中央値：約 10 人）では、地域に関係なく、8 割の中小企業で年 10 万円未満というのが実情である。つまり、月 1 万円未満しか拠出できておらず、経済安全保障という観点からみると、実に心許ないと言わざるを得ない。

では、お金も、人も、時間も不足がちな中小企業は、どのように対策をしていけばいいのだろうか？

先ず、中小企業の経営者に持って頂きたい視点として、サイバー対策を「金食い虫の費用」でな

く「将来の金稼ぎのための投資」と捉えて頂くことである。サイバー攻撃を完全に防ぐことはできないが、リスクをかなり低減することは可能であろう。100 万円の売上を新たに創ることは非常に難しいが、100 万円の新たな (そして無駄な) 支出を防ぐことは比較的簡単であろう。100 万円の非生産的な支出を防ぐために、何らかのセキュリティ対策をすることは、多少の出費とはなるが、中長期的にはそれを相殺して余りある売上と信用の向上をもたらすことだろう。

ここで、サイバー攻撃被害に遭った中小企業の被害額つまり「無駄な支出」の実例を紹介する。

社員 30 人のサービス業である F 社は、受信メールに添付されていたワード文書のマクロを有効にしたところ、PC 1 台がウイルスに感染し、外部に対し偽装メールが送信された。その結果、原因や被害範囲調査費用に 364 万円、再発防止のコンサルティング費用 44 万円、再発防止のセキュリティシステム導入費用 214 万円、計 622 万円の被害があった。このうち、原因調査の 364 万円と再発防止コンサルの 44 万円は、もし、このインシデントが発生していなかったら、支払うことのなかったコストなので、この 400 万円は「無駄な支出」というべきだろう。一方で、セキュリティシステム導入費の 214 万円は「無駄な支出を未然に防ぐための投資」と位置づけられるので、もし、この企業が予め 214 万円の投資をして予防線を張っていたなら、400 万円の「無駄な支出」も発生しなかった、という計算になる。つまり「200 万の投資で 400 万の被害を防止する」ということだ。

こういった計算方法は「後付けの結果論」かもしれないが、サイバーセキュリティに関する「費用と投資」の関係性を考えるうえでの参考事例にはなろう。

中小企業の悩みは「何から始めたらいいか分からない」「どこまでやったらいいか分からない」といったものである。そんな中小企業は IPA の「中小企業の情報セキュリティ対策ガイドライン」の一読から始めるべきだろう。あわせて、同じ IPA の「5 分でできる！情報セキュリティ自社診断」で足元のチェックし、スコアに応じた「やるべきこと」を確認する。次に読んだり調べたりというフェイズから一歩進み、実践フェイズとして「情報セキュリティ 5 か条」に取り組むこと。

「何かに頼りたい」「少しだけしかお金は出せない」という中小企業は、経済産業省・IPA が実証事業を経てその事業スキームを構築し、現在は国の登録制度となっている「サイバーセキュリティお助け隊サービス」を利用するのも一考であろう。人もお金も時間も不足がちな中小企業に特化した、格安で、導入・運用ともに簡単なサイバーセキュリティのワンパッケージサービスである。国に登録されたサービスゆえ、ユーザ企業は「わが社は、中小企業として、最低限のセキュリティ対策をやっています」と公言することもできよう。また、「お助け隊サービス」を利用していたにもかかわらずサイバー攻撃被害に遭ってしまったとしても「中小企業に求められるべき現実的な対策（国に登録されたサービス）をやっていたのですから（取引停止等は）許して下さいよ」というエクスキューズを述べていただくこともできよう。

JNSA ワーキンググループ紹介

標準化部会・電子署名ワーキンググループ

三菱電機株式会社
電子署名 WG リーダー　宮崎　一哉

1.はじめに

現在の電子署名WGは2013年4月に発足してはや9年が経過します。(「現在の」といったのは、2003年頃に電子署名検討WGというワーキンググループがあったからです。https://www.jnsa.org/active/press/vol8/3-1WG.pdf)

2014年3月発行のJNSA Press 第37号（https://www.jnsa.org/jnsapress/vol37/5_WG.pdf）及び2018年3月発行のJNSA Press第45号（https://www.jnsa.org/jnsapress/vol45/3_WG-1.pdf）で現電子署名WGを紹介し、今回が3度目の紹介となります。

2000年前後に日本を含めて各国で電子署名法が制定されてから随分と経ちますし、利用する暗号技術も十分に枯れていますが、未だに活動を続けなければならないことには以下のような要因がありそうです。

・主にコロナ禍に起因する仕事環境の変化に伴う電子契約の登場（新しい電子署名の登場）
・EUでのトラストサービスの法制化（eIDAS規則）とそれに伴う標準規格の充実
・我が国が世界に向けて提唱したDFFTでのトラストサービスの重要性への認識の高まり
・DXを始めとしたもろもろの電子化推進でのトラスト技術の必要性

電子署名WGは発足以来、100回以上の定例会議を重ね、テーマによってはアドホック会議も実施しつつ、また合宿で集中討議を行いながら、数々の成果を生み出してきました。本稿では、前回の報告以降、どのような変化があり、どのような検討をし、どのような成果が得られたかを差分を中心に紹介します。

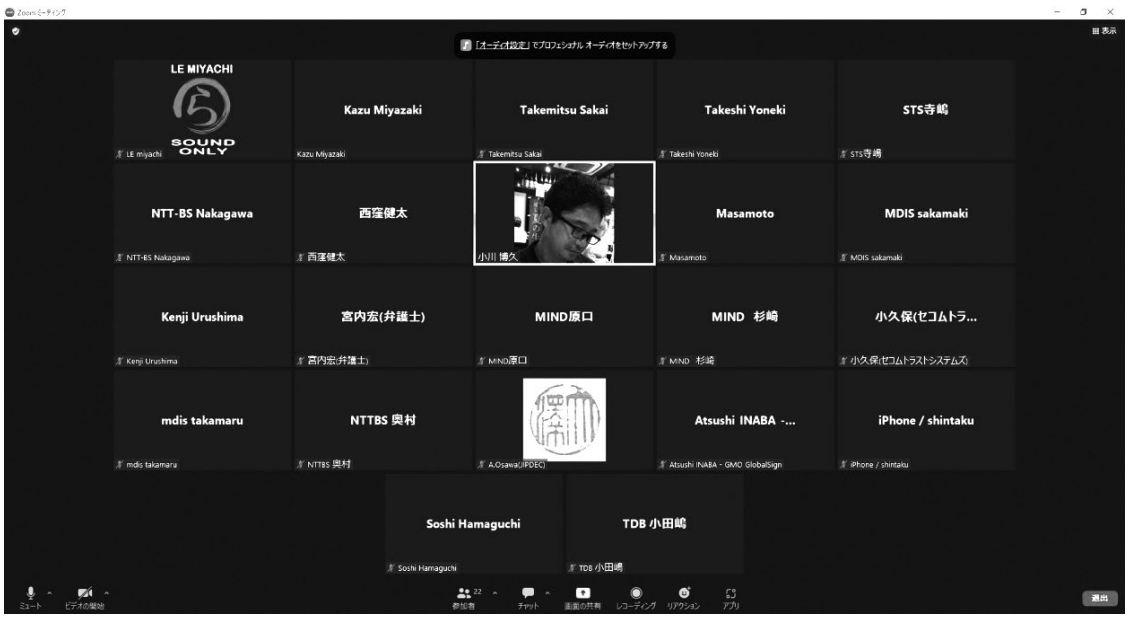


図1　最近の定例会議の様子（リモートばかり、、、）

2.電子署名Q&A

2020年9月16日に公開したこのQ&Aの背景には、電子契約の台頭に伴い、新たな電子署名として、いわゆる立会人型署名（事業者署名型署名）が出現したことがあります。

JNSA ワーキンググループ紹介

電子署名法主務三省（当時：総務省、経済産業省、法務省）から2020年7月と9月の二回にわたり電子契約サービスに関するＱ＆Ａが公開され、その中で立会人型署名（三省Q&Aでは「利用者の指示に基づきサービス提供事業者自身の署名鍵により暗号化等を行う」電子署名と表わされています）に関する見解が示されましたが、電子署名に馴染みのない方にはややハードルが高い内容となっています。このような状況を踏まえ、少しでも多くの方に電子署名に対するご理解を深めていただけますよう、電子署名WGでは「電子署名Q&A」を作成し、公開することといたしました（https://www.jnsa.org/result/e-signature/e-signature-qa/）。

3.デジタル署名検証ガイドライン

2021年3月31日に作成（4月15日公開）の本ガイドラインは、タイムビジネス協議会（TBF）との共同で2013 年に作成した「電子署名検証ガイドライン」の改定版で、JNSA メールマガジン215号（2021年7月9日配信）でも紹介しています（https://www.jnsa.org/aboutus/jnsaml/ml_bk215.html）。

DXに伴うデジタル化とネットワーク化の進展に伴い、デジタルデータの保証と取り扱う人やサービスの信頼性が、これまで以上に必要とされるようになっています。中でもデータの作成責任とその真正性は、アナログ時代においては「署名」や「押印」によって担保されてきましたが、デジタル時代においては、それに相当する技術として「電子署名」があります。

署名は文書等にそれが付与され、受領者が署名を確認することで文書等の真偽や価値の判断材料となります。しかし、可視データであるアナログの「署名」や「押印」と違い、「電子署名」は機械処理としての「署名検証」が必要であり、検証ツール（ソフトウェア）に依存せざるを得ません。さらに、電子署名は様々な要素から構成されており、その判定には細心の注意を必要とします。その判定基準が検証ツールによって異なると、同じデータに対する判定が異なる結果となり、デジタル化の阻害要因となりかねません。それを防ぐため、電子署名のうち公開鍵暗号技術に基づくデジタル署名について検証のためのガイドラインである「デジタル署名検証ガイドライン」を作成しました（https://www.jnsa.org/result/e-signature/data/e-signature-guideline_v1.0_20210331.pdf）。

4.電子署名保証レベル（要約版）

2001年4月電子署名法が施行された時は「電子署名」とは「公開鍵暗号を利用したデジタル署名と公開鍵インフラ（PKI）」を前提としていました。一方で電子認証によるクラウド利用のサービスが一般化したこともあり、電子署名サービスも多様化し色々な電子署名の技術や方式が使われるようになりました。これは本稿の2章でも述べた立会人型署名の出現が典型例です。

従って現在では単純に「電子署名＝デジタル署名＋PKI」とは言えません。しかし技術や方式が異なる電子署名方式の比較は簡単ではありません。「技術に関する電子署名の保証レベル」を専門家が公平に策定し標準化を行い電子署名利用者が目的に合った選択ができるようになることが重要です。

電子署名ワーキンググループでは新たに保証レベルタスクフォースを発足し電子署名の保証レベルの策定を行いました（https://www.jnsa.org/result/e-signature/2022/index.html）。

最終的にはガイドブックの公開を目指していますが、本資料はその要約版として公開したものです。電子署名サービスの仕様検討時や、電子署名の利用者も自身が利用する電子署名の保証レベルを知る為の参考ガイドとして本資料をご利用ください。

5.標準化活動

電子署名関連の標準化は、データの流通、インタオペラビリティ確保に重要であるとともに、それを主導することで日本の状況にも即した内容となることが期待されます。

電子署名WGではISO/TC 154（行政・商業・工業用書式及び記載項目）において長期署名プロファイルの標準規格化を推進しています。

JNSAは2019年にJIPDEC（日本情報経済社会推進協会）からISO/TC 154の国内審議団体を引継ぎました。長期署名プロファイル国際標準規格であるISO 14533シリーズは電子署名WGメンバーが主導して標準化を行って来ました。現在、ISO 14533シリーズは現在Part1からPart4までの4種類が発行されています。

2021年10月4日には、XAdES長期署名プロファイル国際規格の改定を達成しました。これは、日本（JNSA）が提案しプロジェクトリーダーとして標準化していた、XML署名をベースとしたXAdES長期署名プロファイルの2nd editionへの改定です。今回の改定では最新仕様にすると共に、欧州eIDAS規則仕様との互換性もまとめました。コロナ禍にニーズが高まっている電子（デジタル）署名国際標準規格の最新版となります。

また、ECOM（次世代電子商取引推進協議会）で策定した次の長期署名プロファイルのJIS原案作成もJIPDECから引き継ぐこととなっています。

- JISX5092:2008 CMS利用電子署名（CAdES）の長期署名プロファイル
- JISX5093:2008 XML署名利用電子署名（XAdES）の長期署名プロファイル

6.おわりに

電子署名WGのアクティブメンバーは20名から30名ほどです。月1回の定例会議のほか、頻繁な懇親会や合宿が特長です（コロナ禍の影響でここ数年は実施できませんでしたが、、、）。

今後は、電子署名のJISの改定とPAdES版の作成、電子署名保証レベルに関する報告書の作成、デジタル署名の検証結果を表現する検証レポートの標準案の検討を、進めていく予定です。DXを取り入れて業務展開しつつ信頼性を高めたい方、あるいは、社会のトラストに貢献したい方、ぜひ一緒に活動していきましょう。

なお、電子署名WG及びJT2Aの最近の成果（図2）は次のURLが示すページで紹介していますので、ご活用いただければ幸いです。
https://www.jnsa.org/result/e-signature/

図2　電子署名WG/JT2A　報告書・成果物のページ

会員企業ご紹介52

株式会社エーアイセキュリティラボ

https://www.aeyesec.jp/

Aeye Security Lab

DX時代に対応！高品質・低コストな脆弱性診断内製化ツール

AeyeScan（エーアイスキャン）は簡易操作でハイレベルな脆弱性診断が実施できる診断の内製化ツールです。

診断を何度行っても追加費用はなし。クラウド環境により新しい脆弱性にもすぐに対応。迅速にツールへ反映。

診断には、人の手で行わざるを得ない作業（フォーム値の入力や画面数調査など）が必ずありました。
AeyeScanはAIやRPAを活用し、それらを自動化。
今まで何時間もかかっていた単純作業を一瞬で終わらせることに成功しました。

これにより網羅的かつ常に最新の診断を短時間で何度も行うことを可能にしました。

沢山の大手企業様に導入いただいております！

自動化された機能は他にも沢山あります！

このような方におすすめ

AeyeScan

- セキュリティエンジニア不足でお困りの方
- 既存の診断方法では診断コストがかかっている方
- 一律で行う診断より頻繁な診断を必要としている方
- レベルを担保しつつ自動化できる部分は自動化したい方
- 担当の人材だけでなく関係者全員が把握できるレポートが必要な方
- 診断にかかる無駄な時間を削減したい方
- サポートは受けたいがトレーニングを受ける時間がない方

お問い合せ	株式会社エーアイセキュリティラボ 〒101-0054 東京都千代田区神田錦町二丁目2番地1　KANDA SQUARE 11F WeWork 内 AeyeScanサイト　https://www.aeyescan.jp/

株式会社フーバーブレイン

https://www.fuva-brain.co.jp/

フーバーブレインは、「ITツール事業」及び「ITサービス事業」を営んでおります。当社が提供する**セキュリティツール及び働き方改革ツールの「ITツール事業」**と、**当社ITツールの提供に伴う保守・役務に加え、子会社GHインテグレーション株式会社の受託開発・SESを含めた「ITサービス事業」**の２事業によって、**お客様の生産性及びクオリティオブライフの向上を支援**します。

ITツール事業

【セキュリティツール】

■ **Eye“247” AntiMalware**

世界５億台の利用者で世界規模の確かなセキュリティ実績を誇り、セキュリティベンダー評価機関の最高評価を受賞する**Bitdefenderによるマルウェア対策エンジン**と国内随一を誇る**フーバーブレイン独自マルウェア・グレーツール対策エンジン**の**２つを連携したセキュリティーツール**です。

■ **Cato SASE Cloud**

CATO NETWORKS社が提供する**次世代型のネットワークサービスで、SASEを実現するネットワーク**です。当社は「Cato SASE Cloud」のディストリビューターとして、企業様の導入に関する相談の受付、販売パートナーの募集を行っております。

【働き方改革ツール】

■ **Eye“247” Work Smart Cloud**

「誰が・どこで・いつ・どのくらいの時間・どんなPC操作をしたか」を記録・可視化し、**勤務状況・業務効率・セキュリティなど、あらゆる角度から分析できるクラウド『業務可視化』サービス**です。従業員の勤務時間と作業時間の乖離や業務生産性を把握したり、情報漏えいリスクのある操作を監視・制限することができます。

ITサービス事業

【保守・役務提供】

セキュリティツール及び働き方改革ツール提供に伴う導入・運用支援役務及び保守サポートを提供しております。

【受託開発・SES】

パートナー企業からの開発委託案件の対応及びパートナーSIerと協業して、主に**大手通信事業者へITエンジニア人材を提供**しております。

お問い合せ	株式会社フーバーブレイン 〒102-0094 東京都千代田区紀尾井町4-1　ニューオータニガーデンコート22F TEL：03-5210-3061　WEB：https://www.fuva-brain.co.jp/ EMAIL：info@fuva-brain.co.jp

株式会社ラック
https://www.lac.co.jp/

たしかなテクノロジーで　「信じられる社会」を築く。

ラックは練度の高い多様なテクノロジーを駆使して安心・安全な社会基盤を築き、人々が互いを支え合い、笑顔でいられる社会の実現を目指して活動しています。

私たちは、「国を衛る」という熱い想いを、一貫して持ち続けてきました。1995年に今日のような情報社会の到来を予見し、情報セキュリティ事業を他に先駆けて立ち上げて以来、情報技術革命の進展に合わせて巧妙化、多様化するサイバー攻撃の最前線に立ってノウハウを蓄積してきました。

■ 事業内容

他社に先駆けて始めたセキュリティ対策サービスと独立系のITベンダーとして幅広い領域のSIサービスを提供。
サイバー攻撃や情報漏洩事故発生時に救急対応でご支援する「サイバー119サービス」、AIを活用した「診断サービスDiaforce」、24時間365日体制で契約組織をサイバー攻撃から見守る「JSOCセキュリティ監視・運用サービス」、サイバーセキュリティに関する教育・訓練を提供する「ラックセキュリティアカデミー」、金融機関を支援する金融犯罪対策センターをはじめとするエキスパートによる「セキュリティコンサルティング」など、総合的なサイバーセキュリティサービスを提供しています。そして、金融機関をはじめとする大手企業を軸とした、基幹システムやITシステム開発を担うセキュリティサービスの複合的な提供で、「信じられる社会」を築いていきます。

■ JNSA会員企業と、サイバー攻撃対策で連携します

JNSA会員企業と当社のセキュリティサービス連携や、情報漏洩などのサイバー事故発生時の支援などにおいての協業など、様々なパートナーシップについても遠慮なくご相談ください。

お問い合せ	**株式会社ラック** **〒102-0093 東京都千代田区平河町2-16-1 平河町森タワー** **Email：eigyo-toiawase@lac.co.jp　https://www.lac.co.jp/**

JNSA 会員企業のサービス・製品・イベント情報

■製品紹介■

○ NECの本人確認サービス「Digital KYC」

NECの本人確認サービス「Digital KYC」は、この度、顔認証による本人確認回数が累計1,500万回を突破しました。
NECでは顔認証による本人確認の他、銀行認証による本人確認、公的個人認証（マイナンバーカード）による本人確認を提供しており、様々な方式での本人確認に対応しています。
【製品情報詳細】
https://jpn.nec.com/fintech/kyc/index.html
◆お問い合わせ先◆
NEC Digital KYC 担当
Mail: ai_ide@fdit.jp.nec.com

■製品紹介■

○ AeyeScan（エーアイスキャン）｜内製化を実現する脆弱性診断ツール

AIの活用によって、専門的になりがちな脆弱性診断を誰でも、いつでも、分かりやすく。Webセキュリティの知識や開発経験がなくても、自社環境がなくても使えるクラウド型Web脆弱性診断ツールです。
自動化によりWebサイトの診断時間を大幅に縮小するだけでなくOWASP ASVS等にも準拠した高品質な診断をご提供します。
【製品情報詳細】
https://www.aeyescan.jp/
◆お問い合わせ先◆
株式会社エーアイセキュリティラボ
Mail: info@aeyesec.jp

■製品紹介■

○ Vulnerability Explorer（Vex）

優れた検査シナリオ再現力と検出率を有する純国産のWebアプリケーション脆弱性検査ツールです。
きめ細かい設定や使いやすいUI、多種多様なレポートにもこだわり、また、手動診断チームや各セキュリティベンダーからの意見や要望を取りこみ、常に進化を続けています。
ユーザ様自身が自走して運営出来るよう、導入時から運用が定着するまで、国産ベンダーならではの安心のサポートもご提供しております。
【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
Mail: sales@ubsecure.jp

■サービス紹介■

○ Eye “247” Work Smart Cloud

インストールしたPCの端末情報やPC操作などのログを自動取得し「内部不正対策」ができるクラウドサービスです。個人情報を持ったPC端末の特定やファイル操作の記録、USBメモリなどの記憶媒体や印刷機などの外部機器の使用記録や制御ができます。また、カスタム設定をすることで上長やシステム管理者に様々なアラートを送信することもできるので、テレワークでも活用しやすいサービスです。
【製品情報詳細】
https://www.eye247wsc.jp/
◆お問い合わせ先◆
株式会社フーバーブレイン
https://www.fuva-brain.co.jp/
TEL: 03-5210-3061
EMAIL: info@fuva-brain.co.jp

■サービス紹介■

グローバルで活動をするIT業界団体の「CompTIA」では、ベンダーニュートラルとして広く認知されているCompTIA認定資格を提供しています。
様々なIT分野での業務基準となるCompTIA認定資格は、セキュリティやDX人材の育成にも広く活用され、270万人以上に取得されています。
グローバルで認知されているセキュリティフレームワークとも高い親和性があり、わかりやすいキャリアパスも特徴の一つです。
【製品情報詳細】
https://www.comptia.jp/about/comptia-cybersecurity-pathway.html
◆お問い合わせ先◆
CompTIA日本支局
Mail: info_jp@comptia.org

イベント開催の報告

日本 ISMS ユーザグループ／日本ネットワークセキュリティ協会 主催 情報セキュリティマネジメント・セミナー 2022
27000 シリーズの最新動向とベストプラクティスの提案

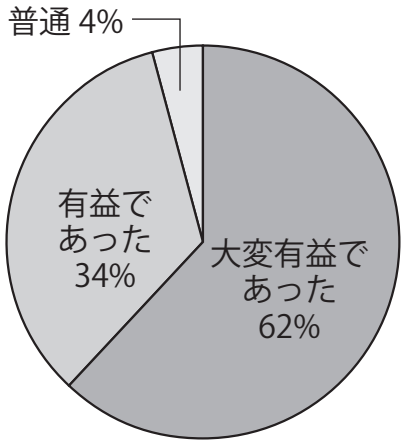
標準化部会　日本ISMSユーザグループでは毎年12月にISMS（情報セキュリティマネジメントシステム）の標準化動向と「ISMSの実施・運用に関わるベストプラクティス」に関する研究成果をセミナーとして情報発信しています。今年度は12月16日（金）に開催しました。

今年度のトピックとして標準化動向に大きな変化がありました。組織にとって有用な情報セキュリティ対策のベストプラクティスを提供するISO/IEC 27002の改定（2022年2月発行）および情報セキュリティマネジメントシステム（ISMS）の要求事項を定めるISO/IEC 27001の改定（2022年10月発行）です。これらの規格改定についてISO/IEC JTC1/SC27 WG1のメンバーによる解説および今後ISMS認証組織としてどのように対応していくべきか方向性を模索するパネルディスカッションを実施することでISMSの認証組織が今後どのように取り組んでいけば良いか不安を抱いていることについて一つの方向性が示せたのではないかと思います。

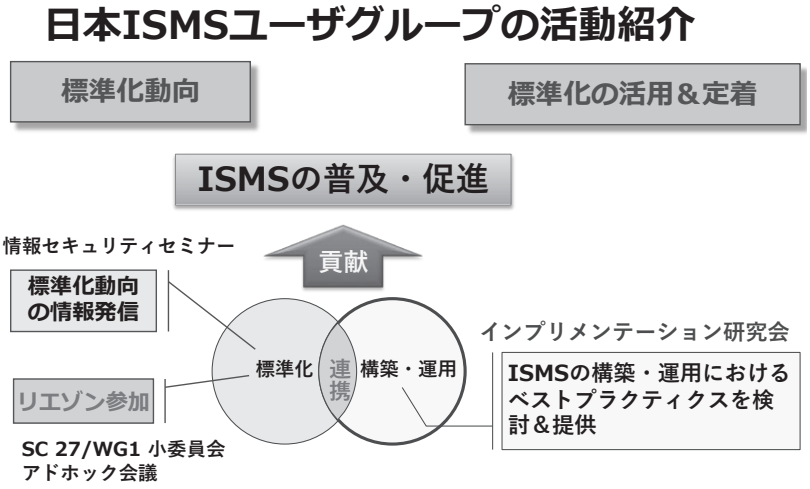
また、ISMSの実施・運用に関わるベストプラクティスについて利用者の視点から整理・検討・共有を進めているインプリメンテーション研究会では2つのテーマを発表しました。テーマ1は最新の環境の変化（クラウド利用の拡大やテレワークの定着など）を事例としてISMSの適用範囲や認証範囲について規格要求事項の観点から再確認をすると共にリスクの変化に対応するための考え方や方針について解説しました。また、テーマ2では各組織共通的な悩みである効率的なリスクアセスメント手法についてリスクアセスメント手順や改善事例などを共有しました。

セミナーの参加申込みは500名定員のところ676名で参加人数537名という大勢の方にご参加頂きました。参加頂きました9割上の方に有益であったという好評価を頂くと共に来年のセミナー参加や今後の活動に期待するメッセージを頂きました。

また、アンケート形式をGoogleアンケートに変更することで回答率のアップおよび多くの来年のセミナーに向けてのご意見、ご要望を頂くことが出来ました。今後の活動のインプット情報として有用に活用したいと思います。



【参加者の感想】



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. 自治体総合フェア2023（第27回）
主　催：一般社団法人日本経営協会
日　程：2023年5月17日～19日
会　場：東京ビッグサイト　西３ホール

2. 第27回サイバー犯罪に関する白浜シンポジウム
主　催：サイバー犯罪に関する白浜シンポジウム
実行委員会
日　程：2023年5月25日～27日
会　場：メイン会場：
和歌山県立情報交流センター「Big・U」
サブ会場：ホテルシーモア

3. ワイヤレスジャパン2023
ワイヤレス・テクノロジー・パーク（WTP)2023
主　催：株式会社リックテレコム
日　程：2023年5月24日～26日
【オンデマンド配信】2023年6月5日～19日
会　場：東京ビッグサイト　西3・4ホール

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ＦＦＲＩセキュリティ
副部会長：唐沢勇輔 氏／Japan Digital Design 株式会社

社会問題となったサイバーセキュリティリスクに対して、JNSAが共助組織として貢献していくため、社会活動部会は時事問題に対するタイムリーな情報発信や勉強会の開催、政府機関や関係団体とのパイプ役となったセキュリティ政策の促進などの従来からの活動を継続していく。

また、新たな取り組みとして、産学の連携強化のための協議会の推進を行う。

【海外市場開拓WG】
（リーダー：松本照吾 氏／
アマゾン ウェブ サービス ジャパン株式会社）

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。

また、海外の業界団体とのコミュニケーションを踏まえたマッチングなどを支援するとともに展示会によらず海外展開を促進できるようなチャネル情報の共有を行う。

＜予定成果物＞
- イベント出展等

【CISO支援WG】
（リーダー：髙橋正和 氏／
株式会社Preferred Networks）

経営陣の一員としての活躍が期待されているCISO業務についての、フレームワークを提案し、公表資料作成、出版、セミナーなどで発表する。

＜予定成果物＞
- 書籍出版を予定

【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。

【中小企業支援施策WG】
（リーダー：岩本真人 氏／トレンドマイクロ株式会社）

関係支援機関/支援者との協働による中小企業の情報セキュリティ対策導入を促進する官民による支援施策の検討とその実践、中小企業の情報セキュリティ市場の拡大を捉えたJNSA会員のソリューション展開への寄与を目的として会合を開催する。

＜予定成果物＞

- 支中小企業の情報セキュリティ対策導入を促進する官民による支援施策の検討に基づく成果物（支援施策コンテンツ、報告書など）

【みんなの「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）

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「サイバーセキュリティ」をテーマとしたコミックを8本制作し、JNSAのTwitterで広く発信する。

大島悠先生に原作を依頼、花園みずき先生に作画を依頼し、コミック発信は（株）角川アスキー総合研究所、(株)KADOKAWAに協力いただく。

＜予定成果物＞

- twitterによるSNSコミックを配信

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。

【セキュリティ市場調査WG】
（リーダー：礒部良輔 氏／興安計装株式会社
サブリーダー：玉川博之 氏／Modis株式会社）

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＞

- 2021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、これらの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。

2022年度も引き続き、特に(1)に重点をおいた活動を行う。

また、コロナ禍で日常になったテレワーク環境下における取組も積極的に聞き出したい。

＜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。

【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
サブリーダー：西浦真一氏／
キヤノンITソリューションズ株式会社）

サイバーインシデント被害者に発生しうる、金銭的負担項目とその被害額を調査・算定し、成果物としてまとめる。

＜予定成果物＞

- 報告書：「インシデント損害額調査レポート2022」

【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セキュリティに関連する調査研究を継続する。

【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）

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し、国内ベント等を介して、広く情報発信する。

【AIセキュリティWG】

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

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し、国内ベント等を介して、広く情報発信する。

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。さらに、近年のデジタル化促進にともなる技術要素についても積極的に取り上げ、標準化部会での技術共有や課題抽出を実施していく。

【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＞

- 特権ID解説書の改定
- デジタルアイデンティティのセルフラーニング用のコンテンツを順次作成予定（Youtube動画など新しいコンテンツの形を検討する。）

【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＞

- 長期署名プロファイル標準の改定案
- 署名検証プロセス及び署名検証レポートに関する
- 標準仕様案
- 電子署名保証レベルに関する報告書

【日本ISMSユーザグループ】

（リーダー：魚脇雅晴 氏／
エヌ・ティ・ティ・コミュニケ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の改定内容の取り込みをユーザ視点で検討＆整理
- ISMSの実装＆運用についての事例研究（選定した2テーマ）
- 情報セキュリティマネジメントセミナーでの研究成果発表、講演資料公開

【PKI相互運用技術WG】

（リーダー：松本泰 氏／セコム株式会社）

デジタル社会におけるPKIの重要性をアピールしていく。

＜予定成果物＞

- セミナーイベント「PKI day」の開催
- 鍵管理勉強会などでの発表

4. 教育部会

部会長：平山敏弘 氏／学校法人電子学園

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SecBoK2021年英語版の作成・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。2022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。

SecBoK2022更新版の展開、およびSecBoK2023改定委員会活動を実施し、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。

また、JNSAが、「辻井重男セキュリティ論文賞」の構成団体の1組織として、教育部会が代表して、運営委員会委員および査読委員として参画している。運営委員及び査読委員については、毎年複数名にご協力を頂いている。この活動は、若手セキュリティ研究者支援及び育成の一環として実施している。

＜予定成果物＞

- SecBoK改定委員会｜SecBoK2023
- 辻井論文賞関連｜表彰論文の選定、および講評など

【ゲーム教育WG 】

（リーダー：長谷川長一 氏／株式会社ラック）

ゲームやその要素（ゲーミフィケーション）を活用した教育のコンテンツやカリキュラムの開発と実施、さらに実施結果の評価や振り返りを行う。実施に際しては、WG内でのゲーム教育のファシリテーターの育成と維持、そのための機会（イベント、演習授業等)創出、学校(大学や高専等）への講師派遣、プロモーション活動を行う。

＜予定成果物＞

- 「MalwareContainment」オンライン版、ファシリテーション資料類

【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＞

- 情報セキュリティ講義の講義資料
- 中小企業向け情報セキュリティ講義の講義資料
- クラウドサービス セキュリティ 講義の演習

【セキュ女WG】

（リーダー：北澤麻理子 氏／
エヌ・ティ・ティ・コムウェア株式会社）

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。

以下のような過去の活動に基づき、勉強会、会合を継続する。

・女性のキャリア形成や仕事の進め方など、相談ができる場を提供
・守秘義務を守りつつ、業務で得た疑問の話し合い、他社の事例を紹介しあう場の提供
・セキュリティの仕事は幅広のため、他の人が従事している業務を知る機会を提供
・仕事、育児、介護、自身の自由時間をどのようにマネジメントするかTipsを得るためのタイムマネジメントの情報交換を実施
・プレゼン経験を積むため全員がプレゼンターとなり、参加者全員からフィードバックをもらう会を実施
・ワーキンググループメンバーが講師の勉強会を開催
・外部有識者の講演会を主催

5．会員交流部会

部会長：扇健一 氏／株式会社日立ソリューションズ

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サービスについては、ユーザ、会員ともに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・問題やカテゴリの改修

【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。

社会活動部会や中小企業支援施策WGと協力して、サービスの改修を検討する。

＜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＞

- 全セキュリティお仕事紹介ビデオ
- 全国セミナーの開催

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。

2019年に本部会で策定した「サイバーセキュリティ業務における倫理行動宣言」の運用を軸に、各WGで活動を行う。

【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。また、昨年度調査WGで行っていた海外事例調査なども必要に応じて実施。

＜予定成果物＞

- 法令改正の提案書

【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するとともに、国内における事例研究を行う。

どういった業務に、リスクがあるかを具体的に参照できる資料の完成を目指す。

＜予定成果物＞

- 法令リスク研究一覧

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。

また、西日本支部が主催となる「NSF 2022 in Kansai」を5月13日に開催。大阪商工会議所の協力の元、会場とオンライン併用で開催。

【今すぐ実践できる工場セキュリティ対策のポイント検討WG】

（リーダー：岡本登 氏／富士通株式会社）

現場実態を考慮したセキュリティ対策の考え方や新たなサイバー対応BCP策定に必要な観点などを整理し、中堅・中小製造現場のセキュリティ向上を支援することを目的とする。

＜予定成果物＞

- リスクアセスメントハンドブック
- セキュリティ対策ハンドブック
- サイバー対応BCP策定ハンドブック

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：奥澤美穂 氏／株式会社Speee）

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。

【Inside IT WG】

（リーダー：羽鶴颯 氏／
株式会社セキュアスカイ・テクノロジー）

ITの基礎技術を初歩の初歩から学べるワークショップを国内各地で開催し、IT業界全体の知識・技術力の底上げを目的とした活動を行う。 ワークショップの対象は、大学生～新卒2年目までの若手を中心として、理系文系関係なくITについて学び直したいと考えている個人で、年齢所属に関係なく幅広い層を想定している。

開催は、土曜日、日曜日、祝日などの休日の午後を利用し、講師は、ワーキンググループ参加メンバーが行う予定。

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事業を実施することによって、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環境実現に向けて寄与することを目的とする。

＜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
  各種技術トピックとセキュリティオペレーションに対する影響の調査
- TS1（セキュリティサービス認定検討タスクフォース）
  各種問い合わせ対応（当初の目的を果たしたため本TFは終了の意向）

【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）

要求にマッチしたセキュリティ診断サービスを的確に効率よく選択できるように、ユーザ向けセキュリティ診断サービスの解説書を作成する。セキュリティ診断サービスを向上するために、サービスを提供している技

術者のレベルを計ることが可能な指標について検討する。

【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／
GMOサイバーセキュリティbyイエラエ株式会社）

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）

セキュリティオペレーション事業者間の共通の課題の認識および、課題の対応や対処について検討を行い、必要に応じて成果物を外部への公開を行う。

＜予定成果物＞

- 各所での発表資料、JNSA全国セミナー発表資料

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改訂（リモート署名TF）
- 欧州(eKYC/eIDAS関連)のリモートにおける本人確認事例の調査概要
- セミナー等での講演資料

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

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インターンシップの推進支援を実施する。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」については、昨年度はコロナ禍の合間となった11月末開催としたが、本年は開催方法と実施時期を改めて検討する。

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

例年通り、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、年間を通して活動を行う。

イベントは、昨年同様にSECCON CTF、電脳会議、ワークショップ、CTF Biginners、CTF for Girlsを実施するとともに、今年度は、地方での開催（2〜4か所）も再開する。なお、新型コロナウィルス感染状況によるが、オフラインとオンラインを併用したハイブリッド開催を計画している。活動予算については、今年度協賛企業の協賛金を充当する予定。協賛金収入の目標は前年度21年度並みを目標とする。

14. サイバーセキュリティ産学連携推進協議会

会長：田中英彦 氏／
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
ステアリングコミッティチェア：大塚玲 氏／
情報セキュリティ大学院大学
事務局長：橋本正樹 氏／情報セキュリティ大学院大学

2021年8月より設立準備会を発足し、検討してきたサイバーセキュリティ分野における産学連携活動について、本年3月に理事会にて承認されたため、「サイバーセキュリティ連携推進協議会」として、2022年度より活動を開始する。

本年度の主な活動は、産学連携を推進するために我が国のサイバーセキュリティ分野に関する研究の実態、産業界のニーズ・課題、連携に係る課題などを調査し、産学連携を推進するための方策について検討する。

なお、これらを推進するために、JNSA会員企業の積極的な参加を募り、また、「学」においても参加組織や研究者等の参加を促す。

JNSA 役員一覧　2023 年 1 月 1 日現在

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）
天野　　隆　（東芝デジタルソリューションズ株式会社）
新井　一人　（トレンドマイクロ株式会社）
伊藤　　新　（エヌ・ティ・ティ・アドバンステクノロジ株式会社）
井上　統之　（KDDI株式会社）
梅野　　寛　（大日本印刷株式会社）
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　　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）
齋木　　啓　（日鉄ソリューションズ株式会社）
櫻井　秀光　（Musarubra Japan 株式会社）
西本　逸郎　（株式会社ラック）
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FFRIセキュリティ）
三膳　孝通　（株式会社インターネットイニシアティブ）
八束　啓文　（RSA Security Japan合同会社）
山口　政博　（ユニアデックス株式会社）
与儀　大輔　（グローバルセキュリティエキスパート株式会社）

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）
伊藤　　昇　（グローバルセキュリティエキスパート株式会社）
岡庭　素之　（キヤノンITソリューションズ株式会社）
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　（エヌ・ティ・ティ・コムウェア株式会社）
倉持　浩明　（株式会社ラック）
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）
佐藤　　健　（NRIセキュアテクノロジーズ株式会社）
佐藤　俊介　（大日本印刷株式会社）
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）
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）
能勢　健一朗　（東芝デジタルソリューションズ株式会社）
野間　祐介　（株式会社インターネットイニシアティブ）
日向　　亨　（トレンドマイクロ株式会社）
平山　敏弘　（学校法人電子学園）
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）
三池　聖史　（ユニアデックス株式会社）
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）
矢野　由紀子　（日本電気株式会社）

監　事

野村　文雄　（野村公認会計士事務所|イースト国際税理士法人）

顧　問

今井　秀樹　（東京大学 名誉教授）
金子　啓子
佐々木良一　（東京電機大学名誉教授|サイバーセキュリティ研究所客員教授）
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 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
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　2月1日現在　267社　50音順

【あ】

RSA Security Japan（同）
（株）RSコネクト
あいおいニッセイ同和損害保険（株）
（株）アイネス総合研究所 New
アイネット・システムズ（株）
（株）アイピーキューブ
アイマトリックス（株）
アイレット（株）
アクセンチュア（株）
アクモス（株）
（株）アシスト
（株）AGEST
（株）アズジェント
（株）アスタリスク・リサーチ
アドソル日進（株）
アドビ（株）
アビームコンサルティング（株）
（株）アピリッツ
アマゾン ウェブ サービス ジャパン（株）
（株）網屋
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）
（株）アレクソン New
アンテナハウス（株）
EY新日本有限責任監査法人
EYストラテジー・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
インターネット セキュア サービス（株） New
（株）インテック
インフォサイエンス（株）
（株）インフォセック
Woven Planet Holdings, Inc.
Utimaco IS GmbH
（株）エーアイセキュリティラボ
AOSデータ（株）
エスアイエス・テクノサービス（株） New
SCSK（株）
SGシステム（株）
SBテクノロジー（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）
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セキュリティ・ジャパン（株）
（株）エヌ・ティ・ティ・データ
エヌ・ティ・ティ・データ先端技術（株）
NTTテクノクロス（株）
NTTビジネスソリューションズ（株）
（株）FFRIセキュリティ
エムオーテックス（株）
㈱エムティーアイ
（株）OSK
（株）大塚商会
岡三情報システム（株）
沖電気工業（株）
ONWARD SECURITY JAPAN（株）

【か】

（株）カスペルスキー
学校法人 片柳学園
兼松エレクトロニクス（株）
キヤノンITソリューションズ（株）
キヤノンマーケティングジャパン（株）
（株）クエスト
（株）クレスコ・デジタルテクノロジーズ
グローバルセキュリティエキスパート（株）
xID（株）
（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）構造計画研究所 New
（株）神戸デジタル・ラボ
（株）コスモス・コーポレイション
コニカミノルタ（株）
CompTIA日本支局 New

【さ】

サービス&セキュリティ（株）
ServiceNow Japan（同）
サイエンスパーク（株）
CyberArk Software（株） New

(株)サイバーエージェント
(株)サイバージムジャパン
(株)サイバーセキュリティクラウド
サイバー・ソリューション(株)
(株)サイバーディフェンス研究所
サイバーリーズン(同) New
サイボウズ(株)
(株)さくらケーシーエス
Sansan(株)
GMOグローバルサイン(株)
GMOグローバルサイン・ホールディングス(株)
GMOサイバーセキュリティ byイエラエ(株)
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)
シナック
(株)SHIFT
Japan Digital Design (株)
情報セキュリティ(株)
(株)信興テクノミスト
ステラサイバー
ストーンビートセキュリティ(株)
(株)Speee
(株)スリーシェイク New
セイコーソリューションズ(株)
セイルポイントテクノロジーズジャパン(同)
(株)セキュアサイクル
(株)セキュアスカイ・テクノロジー
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)
Zホールディングス(株) New
綜合警備保障(株)
ソースネクスト(株)
ソニー(株)
(株)ソフトクリエイト New
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)ダイレクトクラウド
(株)大和総研
高砂熱学工業(株)
(株)宝情報
タレスDISジャパン(株)
(株)中電シーティーアイ
中部テレコミュニケーション(株)
(株)ChillStack
都築電気(株)
TIS(株)
(株)ディアイティ
DBJデジタルソリューションズ(株)
テクマトリックス(株)
デジサート・ジャパン(同)
デジタルアーツ(株)
鉄道情報システム(株)
Tenable Network Security Japan(株)
デロイト トーマツサイバー(同)
学校法人電子学園
(株)電通国際情報サービス
東京海上ディーアール(株)
(株)東芝
東芝ITサービス(株)
東芝デジタルソリューションズ(株)
凸版印刷(株)
(株)TRUSTDOCK
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
日鉄ソリューションズ(株)
日本アイ・ビー・エム(株)
日本オラクル(株)
日本企画(株)
日本シノプシス(同)
一般財団法人日本情報経済社会推進協会
日本情報通信(株) New
(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)
日本マイクロソフト(株)
ニュートラル(株)
ニューリジェンセキュリティ(株) New
ネットワンシステムズ(株)

【は】
パーソルクロステクノロジー（株）
パーソルプロセス&テクノロジー（株）
（株）バイオリンク
（株）パソナ
パナソニック（株）
パロアルトネットワークス（株）
ぴあ（株）
（株）PFU
PwCコンサルティング（同）
東日本電信電話（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
（株）日立ソリューションズ・クリエイト
飛天ジャパン（株）
BIPROGY（株）
（株）ファインデックス
（株）フーバーブレイン
フォーティネットジャパン（同）
富士ソフト（株）
富士通（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）
富士フイルムシステムズ（株）
富士フイルムビジネスイノベーション（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
（株）ベリサーブ New
ポールトゥウィン（株） New
北陸通信ネットワーク（株）

【ま】
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）
みずほリサーチ&テクノロジーズ（株）
三井物産セキュアディレクション（株）
（株）三菱総合研究所
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）
三菱電機ソフトウエア（株）
Musarubra Japan（株）
（株）mediba
Modis（株）

【や】
（株）ユーザベース New
（株）ユービーセキュア
ユニアデックス（株）
（株）横浜銀行 New
（株）YONA

【ら】
楽天グループ（株）
（株）ラック
Rapid7 Japan（株）
（有）ラング・エッジ
（株）ranryu New
（株）リクルート
リコージャパン（株）
（株）両備システムズ
（株）LainZ
（株）レオンテクノロジー
（有）ロボック

【わ】
（株）ワイズ

【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
ジャパン データ ストレージ フォーラム
一般社団法人重要生活機器連携セキュリティ協議会
国立研究開発法人情報通信研究機構
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
一般社団法人 ソフトウェア協会
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
一般財団法人 日本サイバーセキュリティ人材キャリア支援協会
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。）

株式会社ソフトクリエイト　阿部　信児

JNSA会員の皆様、はじめまして。ソフトクリエイトの阿部と申します。
この度は事務局よりご挨拶の機会を頂きましたので、自己紹介をさせて頂きます。

私は2022年3月に（株）ソフトクリエイトへ入社しており、前職でもJNSAにお世話になっていたことから、現職でも微力ながら活動に参加いたしたく2022年８月より加盟させていただきました。

みなさんはソフトクリエイトという会社はご存じでしょうか?
ソフトクリエイトは、中堅、中小企業様向けに多数のインテグレーション実績を有した独立系システムインテグレーターと言う顔と、L2Blocker、Fire Logic、Survey Eyesのようなセキュリティ関連製品のメーカーとしての顔、2つの顔を持つIT企業になります。
弊社では従来からセキュリティやDXについて対応していましたが、昨今の顧客ニーズの高まりにより2022年度から注力事業としてそれぞれセキュリティサービス事業部とデジタルサービス事業部を設立し活動しております。その中で私はセキュリティサービス事業部に所属しSOCのサービス企画検討や、アセスメント/コンサルサービス、診断サービス等セキュリティ全般に携わり、中堅、中小企業のセキュリティレベル向上の為に活動しています。

私の経歴についてですが20年以上IT業界に在籍しており、最初はデータベースやプログラミングから始まりその後ネットワークエンジニアとして活動する中で金融系への対応が増えてきました。
金融系と言えば言わずと知れたPCIDSSへの対応がある為、自然とセキュリティ業界にシフトしていきました。と言うとスマートですが途中５年ほど中国でビジネスをしていたり、ベンチャーキャピタルに関わっていたりと、常に新しく面白そうな事へアンテナを張りチャレンジをし続けたい体質のようで、なんにでも首を突っ込みながら現職に落ち着いております。
面白そうな事を見つけて首を突っ込む癖は昔から全く変わっておらず、思い起こせば小学生時代にはベーマガ買って巻末のプログラムを見ながら真似して組み上げ改造して遊んでいました。ベーマガ懐かしいと思った皆さん。語らいましょう（笑）
現在でも日々の業務でIT/セキュリティ関連にアンテナを張ることは当然ながら、一見関係ない分野にもアンテナを張りどこかでコラボレーションする事が無いか考えながら未来を想像し過ごしております。

執筆にあたり事務局からは、趣味や情報セキュリティに関してリクエストを受けておりますが、この場で趣味の話を始めると本誌を占領してしまう為、詳細は直接お会いさせて頂いた際にでもお話させて頂きますが、スクーバダイビングやスキーを中心にアウトドア的な活動は何でも楽しませて頂いております。

今後もJNSAに貢献できるよう活動し、またセキュリティ業界の方々とも企業/組織を超え連携し、より良い時代を作っていけたらと考えております。ご指導・ご鞭撻のほど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。）

CompTIA日本支局　板見谷　剛史

JNSAの皆様、初めまして。CompTIAの板見谷（イタミヤ）と申します。今回事務局さんのお誘いで自己紹介の機会を頂きました。この機会が皆さんとお近づきのきっかけになりましたら、とてもありがたいです。

私に今の立場があるのは、「偶然」と「出会い」のおかげであり、「想い」によるものです。

私は元々インテリア系志望で、ある専門商社に入社しました。ですが、PCの構造すら知らない私が「たまたま」配属されたのは、オフィスや学習環境とITの融合を提案する社内ベンチャー的事業部の技術営業でした。

商社ですので、お客様のニーズや課題に沿うものは何でも取り扱えます。そして予算を達成できるのであれば、私が気に入ったものも、取り扱いができます。その中で、人材育成の提案で付加価値を高めようとする一匹狼的先輩と「出会い」ました。その先輩が初代CompTIA日本支局の事務局長になる岸田正寿さん（故人）です。岸田さんがCompTIA認定資格の先見性を感じ取り、企業や学校に提案をされているのを見て、私は岸田さんから学び、提案をするようになりました。

その後、事業部の解体により、既に別の道を歩んでいた2001年春、CompTIA日本支局設立準備総会のお知らせを知ります。そこには事務局長として岸田さんの名前が書いてありました。何気なく岸田さんに連絡を取りましたら「暇なら受付を手伝ってくれない?」と誘われ、その総会後「何なら明日から来ない?」という言葉から、実は今に至ります。

うわべの評価に左右されず、良いものは良い、と言えることが、何よりも私の動力源です。CompTIAに21年も居られるのは、CompTIA認定資格の健全な試験開発プロセスと業務基準としての役割があってこそです。多くの皆さんに知ってほしい、ただそれだけでここまでやってきました。2001年当時はプチ資格ブームで、ベンダーニュートラルを謳う資格も多数ありましたが、今ではほとんど残っていません。地道に「想い」を伝えてきたことが、実を結んでいると自負しています。

私はセキュリティの専門家ではありません。人材育成の専門家です。人材育成は省略できませんが、効率的・効果的にはできます。そして人を巻き込み楽をして行うこともできます。JNSAに加盟される皆さんにもこれらを実感いただけるよう、これから尽力致しますので、今後ともよろしくお願い申し上げます。

最後に、私の一番の趣味は、プロレス観戦です。大日本プロレスや鈴木秀樹、ジャンボ鶴田のことなら、負けません。どなたか一緒に語り合える方がいらっしゃれば、SNSでメッセージをお待ちしています。

JNSA 会員特典

■会員の特典

1. 各種部会、ワーキンググループへの参加
2. 会員向け勉強会への参加
3. 活動報告書や成果物の会員限定情報の入手
4. 会員専用 Web やメーリングリストでの情報入手
5. 人脈拡大と相互交流
6. 教育受講やイベント参加時の会員割引
   （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
〒 105-0004 東京都港区新橋 5-7-12-4F
E-Mail：sec@jnsa.org
URL： https://www.jnsa.org/

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.52

2023 年 3 月 31 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

〒105-0004 東京都港区新橋5-7-12-4F
E-mail: sec@jnsa.org　URL: https://www.jnsa.org/