



寄稿

制御システムの セキュリティに関する 業界動向と標準化

02

ペイメントトークン 利用による 決済セキュリティ 強化の潮流

08

CONTENTS

- 01 ご挨拶
温故知新 ～JNSA15周年に寄せて～
- 13 JNSAワーキンググループ紹介
- 13 ● 海外市場開拓WG
- 16 ● マイナンバー対応情報セキュリティ検討WG
- 18 会員企業ご紹介
- 22 JNSA会員企業情報
- 23 イベント開催の報告
- 23 ● 第5回日韓情報セキュリティシンポジウム開催報告
- 25 ● JNSA 2014年度活動報告会
- 27 ● ライトニングトーク夏祭り2015 参加レポート
- 28 インターネット安全教室
- 29 SECURITY CONTEST (SECCON) 2015
- 31 事務局お知らせ
- 40 会員紹介
- 42 JNSA年間活動

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

温故知新 ～ JNSA 15 周年に寄せて～

JNSA 理事

株式会社NTTデータ セキュリティビジネス推進室
セキュリティ・エバンジェリスト

西尾 秀一



JNSAは今年設立15周年を迎えますが、この間にITおよびセキュリティに係る技術、ビジネス環境、ならびに、人や組織は大きく変化してきました。

JNSAが設立された2000年前後を振り返ってみましょう。2000年と言えば、何と云っても2000年問題が話題となっていました。コンピュータシステムの不具合が社会に与える影響の大きさに、初めて世の中の関心が集まった出来事だったのではないのでしょうか。家庭への光回線であるNTTのBフレッツの試験提供が始まったのもこの年で(本サービス開始は2001年)、本格的なブロードバンドの普及が始まりました。モバイル系では、KDD・DDI・IDOの合併によりKDDIが発足し、Yahoo!モバイルがサービスを開始しています。また、今や当たり前のカメラ付き携帯電話が当時のJ-PHONE(現ソフトバンク)から初めて発売されました。

ネットワークサービス系では、Amazon.comが日本で初めてサービスを開始したのが2000年でした。当初は、国内最大のオンライン書店として話題となりましたが、今や書籍のみならずあらゆる製品を扱うオンラインショッピングサイトとなっています。前年の1999年にはYahoo!オークションが開始され、2ちゃんねるも立ち上がりました。ただ、このころはまだブログが主流で、いわゆるSNSはまだ始まっていませんでした。

セキュリティ関連では、情報セキュリティマネジメントの国際規格であるISO/IEC17799(現在のISO/IEC27000シリーズ)が初めて国際規格化されたのが2000年で、まさにISMS元年とも言える年です。ラックのセキュリティ監視センター(現JSOC)が設立されたのもこの年で、同年開催された九州・沖縄サミットの不正アクセス監視を担当して注目されました。セキュリティ専業会社であるNRIセキュアテクノロジーズやNTTデータ・セキュリティ(1999年設立、現NTTデータ先端技術)もこのころ設立されています。

振り返れば、この15年の大きな変化に対し、セキュリティ業界もユーザ企業も必死で食らいついてきたという感があります。2000年というITにとって大きなターニングポイントとなった年に生まれたJNSAが、これまで果たしてきた役割は決して小さくなかったと思います。IoTの普及やビッグデータの活用、そして2020年開催の東京オリンピック・パラリンピックの開催へ向け、次の5年、10年、15年先のIT社会がどうなっているか、ワクワクしながら思いを馳せると共に、JNSAが今後果たすべき役割について、会員企業の皆様と大いに議論していきたいと思っています。

制御システムのセキュリティに関する 業界動向と標準化

KPMG コンサルティング株式会社
武部 達明

2014年のソチオリンピックでは、空調設備の制御システムがインターネットからアクセス可能となることがセキュリティ研究者によって発見され、すぐに担当者に通知されて事なきを得た。制御機器本体あるいは制御システム自体に十分なセキュリティが備わっていることはまれであり、オープン化の波に乗り、高機能、低価格、利便性の追求から、商用の汎用IT技術を製品・システム内に取り込んだ制御機器・制御システムには、外部からの侵入を許容しかねないリスクが潜んでいる。安全性を確保しながら制御システムの利便性を高めるには配慮と工夫が必要である。これを機に今一度、重要インフラを支える制御システムのセキュリティが点検され、2020年の東京オリンピックが無事に開催されるよう祈念する次第である。

1. はじめに

黎明期には、独自OS、独自プロトコル、閉じたネットワークで構成された制御システムは、オープン化の波に乗り、高機能、高付加価値、高生産性を目指してLinux OS、IPネットワーク、Windows OSなどの汎用IT技術、民生品（COTS: Commercial Off The Shelf）を取り込んで進化してきた。しかし、セキュリティ上の問題があることが判明し、情報機器・情報システムへの対策は進められたが、制御システムへの対策は出遅れた。

図1に示すように、セキュリティ攻撃ツール・手法は年々高度化し、操作も簡単になったため、攻撃に要するスキルの閾（しきい）値が下がり、その結果、誰もが攻撃者になれる危険性ははらむこととなった。これらのツールは民生品を対象として発展してきており、民生品を多用している制御システムに

も適用可能であることを示唆している。

図2は、ICS-CERTに報告された制御システムのインシデントの原因を分類している。このうちSpear Phishingには、Adobe Readerの脆弱性を利用するExploitコードを高度なセキュリティツールでPDFファイルに組み込み、E-mailでオペレータに送付するなどの攻撃も含まれると推測される。

制御システムが担う役割の重要性と、事故が発生したときのインパクトの大きさから、制御システムのセキュリティについての議論が始まり、近年耳目を集めるようになった。各業界では、セキュリティに関する取組みが始まり、セキュリティの課題、統制、ベストプラクティスなどの成果が、業界の標準、さらには国際標準へ影響を与えることになる。

このような背景を踏まえ、本稿では、米国、ヨーロッパ、日本におけるセキュリティの標準化活動について述べ、また国際標準の動向についても説明する。

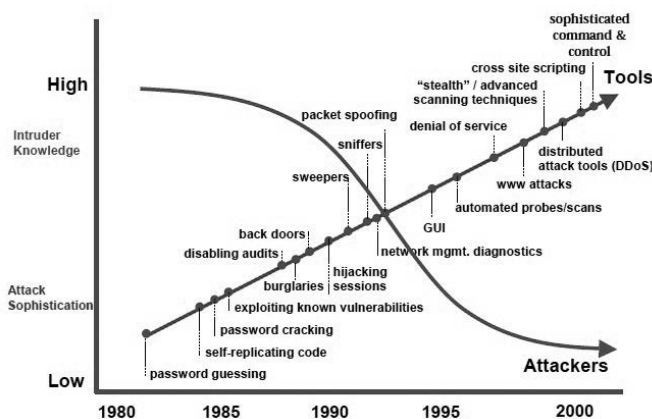


図1 攻撃ツールの高度化 vs 攻撃者技術力

出典：CMU/SEI-2002-SR-009、Page10

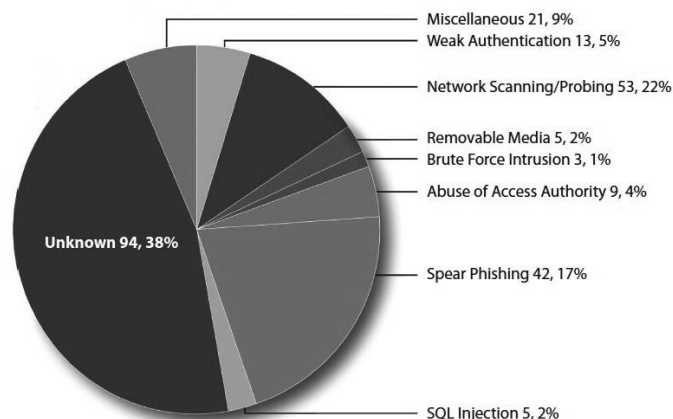


図2 インシデントの分類

出典：ICS-CERT Monitor September 2014 – February 2015 より

2. 米国の動向

図3に、米国を中心として展開された各セキュリティプロジェクトのスコープを、分野ごとに制御システムのライフサイクル上に記したものを示す。

業界分野として、電力、石油・ガス、化学薬品、上下水道、運輸・鉄道、通信が挙げられている。

ライフサイクルでは、要件、研究、開発、テスト、評価、デモ、導入、運用のフェーズが定義されている。

図を見ると、全分野にまたがっての要件定義を考慮した活動がPCSRF、研究フェーズのセキュリティを検討したのがAGA、電力分野で研究から開発初期までをカバーしたのがTCIP、電力と石油・ガスの一部の分野で開発・テスト・評価フェーズに渡って検討したのがNSTB、電力分野で導入フェーズを考慮したのがFERC、NERC、石油・ガス分野で研究から導入まで考慮したのがI3P SCADA、ガス・石油分野でテストから導入まで考慮したのがLOGIC、電力、石油・ガス、化学薬品分野で研究、開発、運用フェーズで考慮したのがISA99ということがわかる。

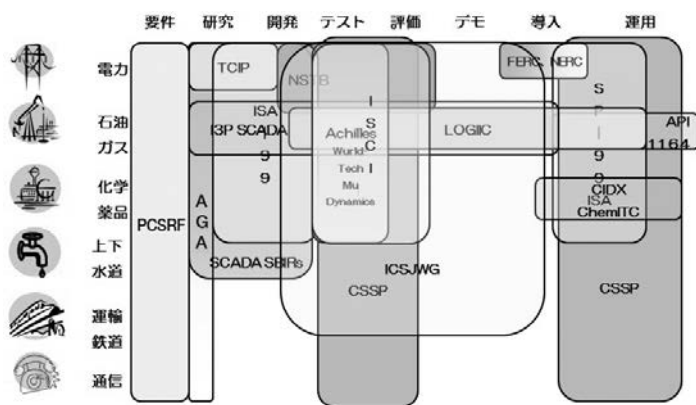


図3 米国制御システムセキュリティ・カバレッジ

2.1 全体像

DHS¹はPCSF（Process Control Systems Forum）を立ち上げ、政府、大学、産業などから330を超す組織を集め、活動を展開した。PCSFは、制御システムのセキュリティ標準、ツール、教育・トレーニング、セキュリティ要件、セキュリティテストなど、多くのテーマで成果物を出した。この活動は、ICSJWG（Industrial Control Systems Joint Working Group）に引き継がれ、年2回のミーティングとして開催されている。ミーティングでは、制御システムセキュリティに関する課題、成果、対抗策、業界の動向などにおける研究から実運用までのテーマが発表されており、政府、大学、事業者、ベンダ、システムインテグレータ、セキュリティコンサルタントなど幅広い層の参加者を集めている。

DHSはCSSP（Control Systems Security Program）で制御システムのセキュリティ評価を行い、結果を「Common Cyber Security Vulnerabilities Observed in DHS Industrial Control Systems」という報告書としてまとめ、脆弱性の原因が、プログラムソースコード品質、Webサービス、ネットワークプロトコル、パッチ不適用、不十分な識別・認証、暗号不使用、セグメント化しないネットワーク設計などに起因するとしている。

DHSはINL²で、上級セキュリティトレーニングを開催し、4日間のトレーニング後、丸1日かけて、攻撃チーム（Red Team）、守備チーム（Blue Team）に分かれ、用意されたミニプラント設備を使った演習を行う。この演習の参加者は、セキュリティ守備の難しさ、攻撃によるダメージの深刻さを理解し、制御システムのセキュリティを推進する立場となる。これにより、制御システムユーザ、ベンダ、システムインテグレータの意識改革がなされる仕組みとなっている。

¹ Department of Homeland Security, <http://www.dhs.gov>

² Idaho National Laboratory, <http://www.inl.gov>

2.2 業界動向

石油・ガス業界では大学の研究機関主導のプロジェクトである I3P³ で、制御システムセキュリティのリスク分析など、6つの分野で成果をあげた。

LOGIIC⁴ は、石油・天然ガス会社と DHS S&T (Science and Technology) とで行っているプロジェクトであり、争点となっているセキュリティのテーマについて、研究・対策を発表している。

API⁵ は、パイプラインシステムのセキュリティに関するガイダンスドキュメントを API 1164 として出版した。

AGA⁶ は、SCADA の通信を暗号メカニズムによって保護するため、AGA 12 を企画した。Part 2 は Retrofit Link Encryption for Asynchronous Serial Communication である。

CIDX (Chemical Industry Data eXchange) では、Cybersecurity Vulnerability Assessment Methodologies でサイバーセキュリティ上の脆弱性を評価する手法をまとめ、IEC 62443-2-1 の制御システム特有のマネジメントとして結実し、活動は ChemITC⁷ に引き継がれている。

電力業界では、多数存在する規模の異なる電力供給業者のセキュリティに対する信頼性を確保するため、NERC CIP 002-5、CIP 003-5、CIP 004-5、CIP 005-5、CIP 006-5、CIP 007-5、CIP 008-5、CIP 009-5、CIP 0010-1、CIP 0011-1 が制定された。現在 Version 5 であり、法的強制力を伴う監査に使用される。

NIST は、スマートグリッドに対して、ガイドライン NIST IR 7628 を公開した。これには、電力市場 7 ドメインでの相互運用性、各ドメイン間サービス、

ユースケースの列挙とセキュリティ要件の分析などが書かれている。

SGIP⁸ の CSWG (Cyber Security Working Group) は、ユースケースを分析し、リスクチェックを行った後、上位レベルのセキュリティ要件を定義し、セキュリティアーキテクチャ、既存のスマートグリッド標準を使い適合性評価をできるようにしている。

また、CSWG は、セキュリティバグに対応するため、AMI (Advanced Metering Infrastructure) Smart Meter のファームウェアアップデートのテストフレームワークも用意している。

DOE は制御システムのセキュリティについてプロジェクトを通じた評価を行うことで、セキュリティに関する実情と課題を明らかにし、課題を克服する目標に向かってマイルストーンを設定したロードマップを提案した (図 4)。

これによると、セキュリティ文化の醸成、リスクの評価と監視、リスク低減の新保護対策の開発と実装、インシデント管理、継続的セキュリティ改善の分野で、短期、中期、長期、ゴールのフェーズ毎の目標が定められている。

最終的には、セキュリティ文化として、関係者にサイバーセキュリティのベストプラクティスが日常的に普及し、エンドユーザサイトで制御システムのセキュリティアーキテクチャおよび物理層でのセキュリティが評価・監視され、リスク低減の施策として、インシデント発生時も問題解析を即時実行し、問題点の特定後、定常状態に戻せるようになっており、継続的セキュリティ改善として、産官学が連携を取り、サイバーセキュリティの進歩を維持することができることを目指している。

³ Institute for Information Infrastructure Protection, <http://www.thei3p.org>

⁴ Linking to the Oil and Gas Industry to Improve Cybersecurity, <http://logiic.automationfederation.org>

⁵ American Petroleum Institute, <http://www.api.org>

⁶ American Gas Association, <http://www.aga.org>

⁷ Chemical Information Technology Center, <http://chemitc.americanchemistry.com>

⁸ Smart Grid Interoperability Panel, <http://www.sgip.org>

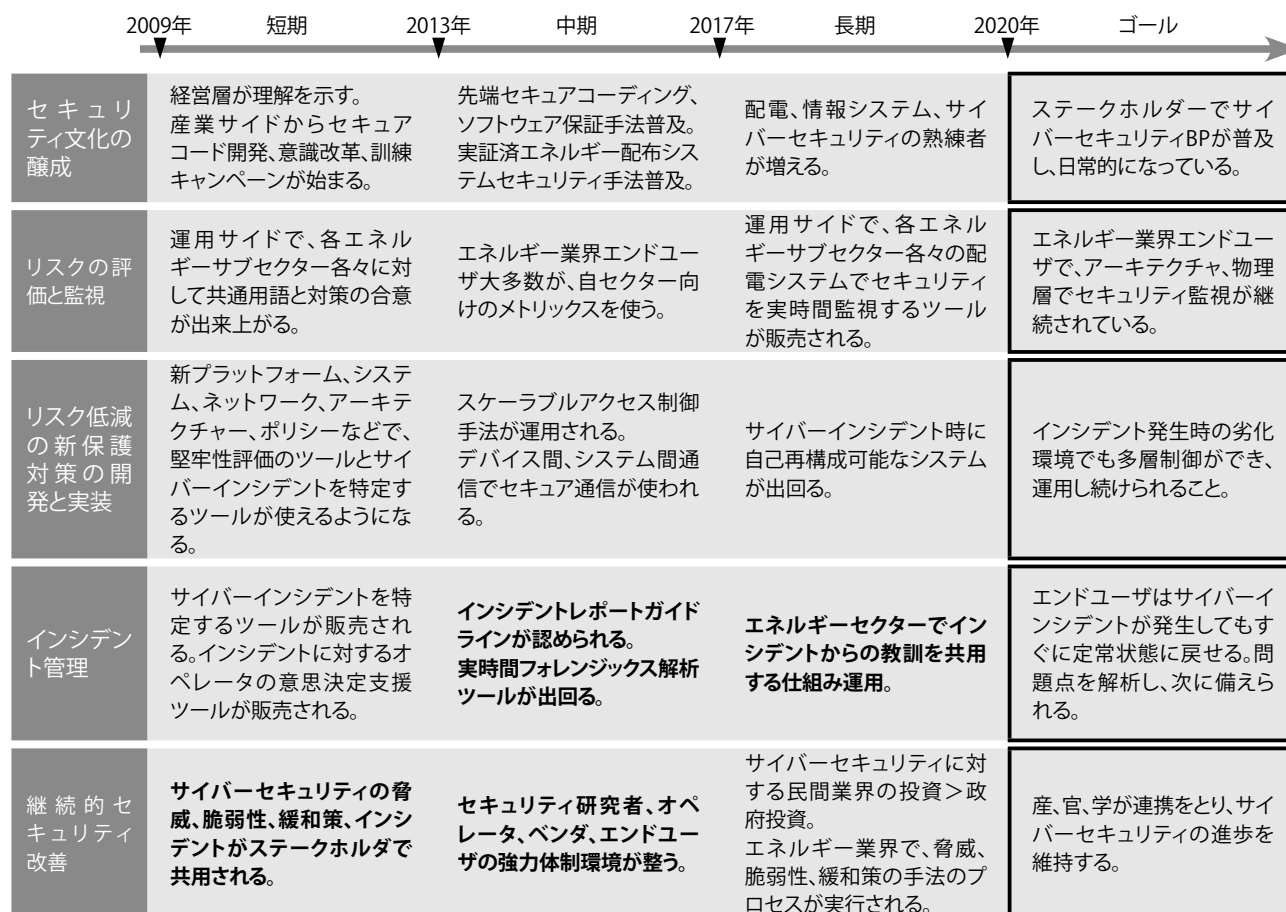


図 4 DOE security roadmap Version 2

出典：Roadmap to Achieve Energy Delivery Systems Cybersecurity, Exhibit 4.1.1 Strategies for Achieving Energy Delivery Systems Cybersecurity より

3. ヨーロッパの動向

英国では NISCC⁹ が SCADA の 7 つのパートからなる Good Practice Guide を作成・公開したが、後に CPNI¹⁰ に引き継がれた。

オランダでは、TNO¹¹ が SCADA Security Good Practices for the Drinking Water Sector を出した。

これは、水道業界に対するガイドラインではあるが、他の業界にも有用な内容となっている。

WIB¹² は、ハーグに本拠地を置く制御システムエンドユーザの集まりで IEC 62443-2-4 の原型となる WIB 2.0 を作成した。これは、供給者のセキュリティの成熟度をランク分けしたセキュリティ要件を記述する。IEC 62443-2-4 では、供給者側からの意見を取り入れ、

9 National Infrastructure Security Coordination Centre

10 Centre for the Protection of National Infrastructure, <http://www.cpni.gov.uk>

11 Netherlands Organization for Applied Scientific Research, <http://www.tno.nl>

12 Working-party on Instrument Behavior, <http://www.wib.nl>

他の IEC 62443 シリーズとの重複を解消し、間もなく標準として公開される。

4. 日本の動向

日本では、制御システムのセキュリティについての活動は、2007 年～2008 年頃から活発化した。内閣官房はサイバーセキュリティ戦略で重要インフラ防護をテーマアップし、経済産業省は制御システムセキュリティ検討タスクフォースをスタートさせ、IPA¹³ は、国内外の制御システムセキュリティについてヒアリングを行い、報告書を公開している。JPCERT/CC¹⁴ は、制御システム関連ドキュメントのいくつかを翻訳し公開している。

制御システムのセキュリティについての保証をするためには評価が有効であるが、ISCI の評価基準を用いた評価を行える CSSC¹⁵ が国家プロジェクトとして設立された。CSSC は、ISCI の評価ドキュメントを和訳した上で参加企業などから専門家を募集レビューをした後、評価の再現性を上げるためのフィードバックを行い、ISCI に貢献している。

5. 制御システムの脆弱性

制御システムの脆弱性は、存在してはならないものであるが、残念ながら簡単にはなくなる。これは、多くの関係者が指摘している。制御システムが設計、開発、実装された時代にはセキュリティの概念がなく、またセキュリティを備えた製品・システム・アプリケーションを設計・開発・実装するプロセスのオーバーヘッドが高いため供給者内で十分理解されず優先順位を落とされ、プロセスの確立に時間がかかったためである。セキュリティの概念がなかった時代に完成された製品が、10 年～20 年の

寿命をまだ全うしていないので、制御システムの脆弱性は容易になくならない。生産性を上げるため、古いコードをレトロフィットして使い回していることも制御システムの脆弱性の原因としてあげられる。

もともと制御機器は、リソースが潤沢でない組み込み機器として発展してきたため、アセンブラで開発され、後にポータビリティとシステム記述能力に富んだ C 言語が使われるようになり、多くのソフトウェアが開発された。

C 言語を使った初期の開発者達は、Brian W. Kernighan と Dennis M. Ritchie による「The C Programming Language」をバイブルとして、コードを書いたが、C 言語は、文字列操作、メモリ操作に関するライブラリを数多く提供しており、想定外の入力データからメモリを守れない。この弱点（脆弱性）を悪用する技術が発見され、任意のバイナリを実行する攻撃法が生み出された。脆弱性は IT 製品のいたるところで発見され、公開され続けている。また、この脆弱性に対応する攻撃方法も公開されつづけている。

脆弱性は、供給者視点ではバグであるが、攻撃者視点では攻撃コードを開発するネタとなり、マルウェアとして組み込まれて被害者のマシンで実行されるよう配備される。あるいは E-mail の添付ファイルに組み込まれ、あるいは E-mail で示される URL のリンク先からブラウザ経由でダウンロードされ実行される。関係者はこれらのリスクから制御機器・制御システムを守ることが求められている。

6. 国際標準

IEC 62443 シリーズのほとんどは、ISA 99 によって作成され、IEC TC 65/WG 10 での審議を経て国

13 Information-technology Promotion Agency, Japan(独立行政法人情報処理推進機構) <http://www.ipa.go.jp>

14 Japan Computer Emergency Response Team Coordination Center (JPCERT コーディネーションセンター)、<http://www.jp-cert.or.jp>

15 Control System Security Center (技術研究組合 制御システムセキュリティセンター)、<http://www.css-center.or.jp>

際標準となる。

制御システムへのリスクは、日々変化していくため、リスクの捕え方、アプローチ方法によって、合意内容は変化する。IEC 62443 ではリスクに対するコントロールとして4レベルのグレード別にセキュリティ要件を決定した。

Part 1 は、当該標準の考え方の根底を成す概念、モデル、用語、Part 2 は、組織に対するセキュリティ要件、Part 3 は、制御システムのシステム全体としてのセキュリティについての要件、Part 4 は、制御システムを構成する制御機器、アプライアンス、アプリケーションについての要件を扱う。

IEC 62443 では、リスク評価をしながらサブシステム分割を行い、必要とするレベルを定め、必要なセキュリティ機能要件を FR1 ～ FR7 より選択し、設計、実装する。FR1 ～ FR7 の詳細は、システムセキュリティ要件として、IEC 62443-3-3 に記述される。

制御システムを構成する制御機器などに関する標準は、IEC 62443-4-1、IEC 62443-4-2 であり、それぞれ保証要件、機能要件を記述する。

ISCI は、IEC 62443 シリーズおよび ISO/IEC 15408 (Common Criteria)、IEC 61508 Part 3、RTCA/DO-178B、The Security Development Lifecycle、OWASP CLASP などのセーフティおよびセキュリティのベストプラクティスを参照して評価基準を作成し、これらの成果を IEC 62443 シリーズに反映してきた。また、ISA 99 には、ISO/IEC JTC 1 SC 27 のエキスパートも参加しているため、今後ますます発展するものと思われる。

7. おわりに

IEC 62443 シリーズは、ISA 99、IEC TC 65/WG 10、WIB、ISCI、ISO/IEC JTC 1 SC 27 の活動により、制御システムのセキュリティに相応しい標準として日々発展を続けている。また、ISMS 認証、成熟度認証、制御機器評価・認証、制御システム評価・認証に使われ、得られた問題点を吸収しながら、時代の要望に即したものとして発展している。これらが活用され、制御システムのセキュリティ向上に役立つことを期待する。

【参考文献】

- (1) Keith A. Stouffer, Joseph A. Falco, et al., "The NIST Process Control Security Requirements Forum (PCSRF) and the Future of Industrial Control System Security, " TAPPI Paper Summit - Spring Technical and International Environmental Conference, 2004, pp. 1337-1344
- (2) IEC/TS 62443-1-1 Industrial communication networks - Network and system security - Part 1-1: Terminology, concepts and models
- (3) IEC 62443-2-1 Industrial communication networks - Network and system security - Part 2-1: Establishing an industrial automation and control system security program
- (4) IEC/TR 62443-3-1 Industrial communication networks - Network and system security - Part 3-1: Security technologies for industrial automation and control systems
- (5) IEC 62443-3-3 Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels

* 本文中の会社名（商号）は各社の商標または登録商標です。

ペイメントトークン利用による 決済セキュリティ強化の潮流

タレスジャパン株式会社 e-セキュリティ事業部
シニアテクニカルスペシャリスト 山神 真吾

1. はじめに

決済取引において、機密データを保護するための最も効果的な方法は何か。それはクレジットカードに関連する機密データを一切持たないことである。守るべきデータがなくなれば、攻撃を受ける可能性は低くなる。セキュリティ対策としては最も効果が高い。ただし、機密データを安全な形で伝送しなければ、決済取引は成立しない。決済取引を完了するためには、別の代替手段が必要となる。

スマートフォンやタブレット端末の普及により、決済取引を取り巻くセキュリティ環境にも大きな変化が見られた。専用線を前提としていた時代のセキュリティでは、もはやモバイル端末からの決済取引は保護できない。事業者向けのモバイル決済ソリューションとして mPOS が登場し、消費者・カード会員向けのソリューションとしてペイメントトークンの利用が始まった。この2つのソリューションはクレジットカードに関連する機密データを事業者側で保持しないこと、既存の決済ネットワークに影響を与えず決済取引が完結することで共通している。

2013 年ごろから、国内でも事業者・加盟店によるスマートフォンおよびタブレット端末を活用したクレジットカード決済サービスの取り扱いが始まった。このような決済サービスは m POS (mobile Point of Sales) と呼ばれている。では、決して安全とは言いきれないモバイルネットワーク環境でいかに機密データを保護しつつ、決済を完了するのか。m POS では、P2PE (ポイント TO ポイント暗号) により、カード受付から加盟店センターまで一貫して機密データを暗号化する。また DUKPT (Derive Unique Key Per Transaction) と呼ばれる鍵管理プロトコルで、トランザクションごとにユニークな暗号鍵を生成利用する。万が一暗号鍵が傍受されても、次の決済では異なる鍵で暗号化しているため、決済情報を復号化することはできない。決済情報はクレジットカードを受け付けたカードリーダーで暗号化さ

れるため、事業者・加盟店は決済情報を持たない。

2014 年 3 月、国際ブランド 6 社が参加し、EMV Payment Tokenization Specification/Technical Framework が発表された。ペイメントトークンをどのように安全に実装するのか、トークンの形式、トークン化システムの要件について基準を定めている。ここで定義されているペイメントトークンは特にモバイル端末を利用した決済での利用を想定している。Tokenization 自体はそれほど新しい技術ではないものの、決済向けのトークン化技術・ペイメントトークンの利用は始まったばかりで、今後利用が拡大する見込みだ。昨年 10 月から米国で本格利用が始まったペイメントトークンによる決済は、今年 7 月には大陸を超えイギリスでも開始されている。

この文章では、ペイメントトークンとは何か、ペイメントトークンのセキュリティ面での長所、決済取引におけるセキュリティの将来について、論考する。

2. ペイメントトークンとは

トークン化は暗号化と異なり、カード番号を元の番号と関連性のない番号・代理の値に置き換える技術である。したがって、トークンから元の番号を演算で割り出すことはできない。EMV.co の仕様書ではトークンは ISO の標準で定められた 13 桁から 19 桁の数値と定義されているが、既存の決済インフラでの取引に対応するため、影響を考慮し実カード番号と同じ桁数でトークンが生成される場合が多い。ただし、必須というわけではない。実カード番号：PAN での決済処理と同様、Luhn チェックと呼ばれる演算・検証に対応し、BIN (銀行識別番号) や Expiry Date といった要素も含まれる。ただし、既に発行済みのカード番号と重複してしまうと処理ができないため、実カード番号とは異なるトークン専用の BIN が割り当てられる。

3. ペイメントトークンのセキュリティ面での長所

ペイメントトークンを利用することで、実カード番号：PANはモバイルデバイス内に保存されない。PANはトークンサービスプロバイダ（TSP）側に安全な状態で保管されている。トークンサービスプロバイダ（TSP）はペイメントトークン＝デバイスアカウントナンバー（DAN）を生成し、DANとPANをマッピングする。DANとPANを紐づけて格納するデータベースをToken Vaultと呼ぶ。Token Vaultでは非常に機密性の高いデータを取り扱うため暗号化されており、金融業界で実績のある方法でセキュリティ管理をするように、EMV.coのドキュメントでも言及されている。また、Token VaultにはToken Requestor IDやDomain情報も含まれ、DANを利用できる場所を制限・管理することができる。

万が一、DANを不正に傍受されたとしても、次

の決済取引には利用できない。DAN単体では決済処理されない。動的な暗号文が決済処理の承認に必要なだからである。また、小売店のメリットとして、決済に利用するPOS端末が攻撃を受けたとしても、POSからクレジットカード番号が漏洩することはない。小売店では実カード情報を取り扱わないからだ。小売店、加盟店センターではペイメントトークンが通過するだけなので、負担が軽くなる。

ペイメントトークンを利用したNFC決済フロー例について、図1にまとめている。消費者がスマートフォンをタップし、NFC決済取引を開始する。小売店のPOS端末、加盟店センターを経由し、決済ネットワークへDANと動的暗号文が送信される。決済ネットワークはDANに紐づいたPANを取得するため、トークンサービスプロバイダ（TSP）へ照会を実施する。TSPはToken Vault内のDAN/PANマッピング情報を確認し、PANを決済ネットワークに返却する。この一連の照会作業をDe-tokenizationと呼ぶ。決済ネットワークは返却されたPANと動

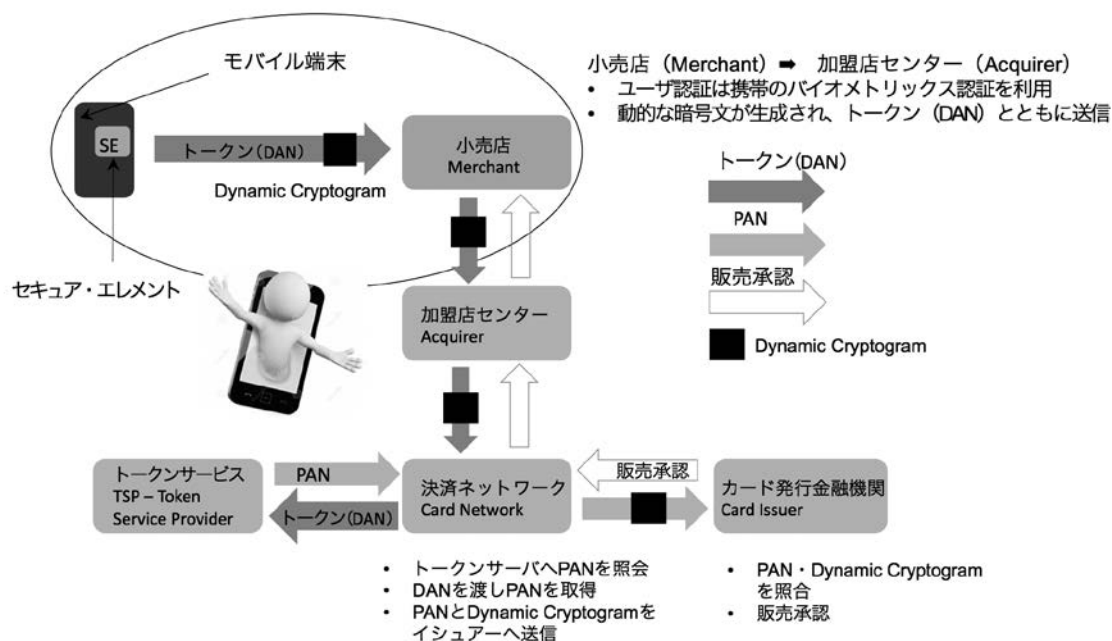


図1：ペイメントトークンによるNFC決済フロー例

的な暗号文をカード発行金融機関に送信し、販売承認を取得する。販売承認は加盟店センターを経由し小売店へ送信され、決済処理が完了する。

4. HCE とペイメントトークン

決済トークンはモバイルデバイスの安全が確保された領域に保管されるのが一般的である。eSE（組み込み型の IC チップ）や UICC（SIM カード）などセキュアエレメント（SE）を利用する方法、TEE（汎用 OS とは区切られた信頼されたアプリケーション実行環境）など実装方法は様々だ。そうした方法の中で特に注目を集めている技術がある。HCE：ホストカードエミュレーションである。既に国際カードブランドの各社が HCE への対応を表明している。さて、HCE とは何で、いったいなぜ注目を浴びているのか。

HCE とはクラウドベースのモバイル決済ソリューションである。モバイル端末側のセキュアエレメントを利用するのではなく、クラウド上でカードをエミュレーションする技術である。CE（カードエミュ

レーション）モードを利用すると、モバイルアプリが直接 NFC コントローラにアクセスできるようになる。HCE ではモバイル端末からの決済処理にペイメントトークンが利用される。ペイメントトークンや認証情報はセキュリティが強化されたクラウド上に保管される。これまでモバイル端末側に配置されていたセキュアエレメント（SE）がクラウドに移動したようなイメージである。

また、盗難・紛失によるカード利用を停止するような場合も、クラウド上に DAN や認証情報があることから即時に停止させることが可能で、運用面のメリットも非常に高い。万が一、不正取引が発生した場合も決済ごとに生成される動的な暗号文と認証プロセスにより、リアルタイムでの検知が可能で、取引の無効化とモバイルデバイスのブロックが可能である。

ビジネス面でも、HCE を導入するメリットがある。現状、セキュアエレメント（SE）と NFC を利用した決済には、MNO、MNO-TSM、SP と様々なプレーヤーが存在し、関係者間の調整、書類作成、交渉などに多くの時間を費やしてきた。HCE ではカード発

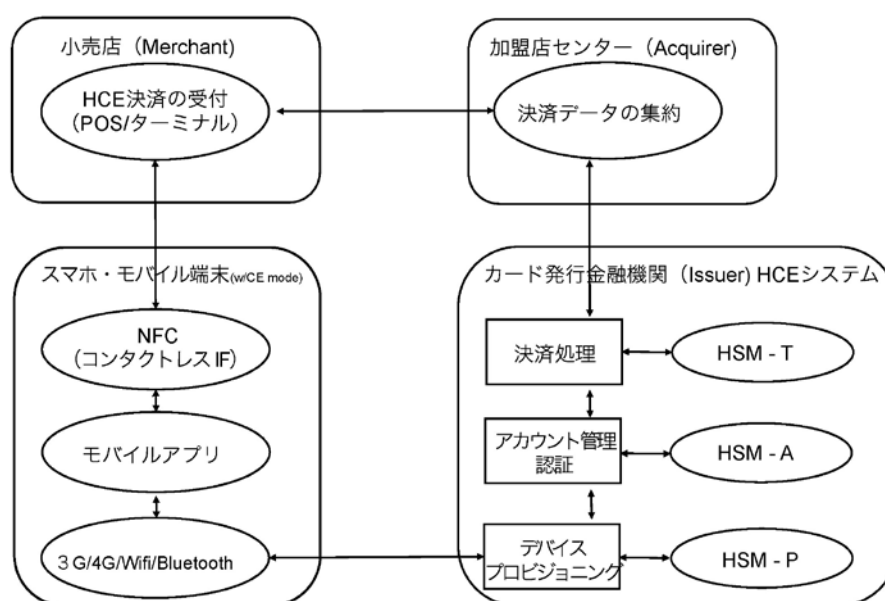


図2：HCE を構成する要素

行金融機関（Issuer）主導で、プロジェクトを進めることができることから、複雑化していたプロセスをシンプルにすることが可能で、導入までの時間と費用を削減することが可能である。

一方、HCE の利用にあたり、「クラウド環境ではセキュリティが十分でない」と警鐘をならす人々が一部に存在する。もちろん鍵管理がアプリケーションレイヤで実施されていると仮定するとその考え方は正しい。ソフトウェアの脆弱性を突いた攻撃により、鍵や決済データが漏洩してしまう可能性がある。しかし、金融機関や決済サービス事業者はそうしたセキュリティ面のリスクを理解して、バックエンドにある HCE システムに HSM（ハードウェア・セキュリティ・モジュール）を配置しセキュリティレベルを高めている。決済処理、アカウント管理・認証、モバイルデバイスとのセキュアセッションの確立、デバイス認証情報の割り当て（プロビジョニング）と HSM は活躍している。また、現状、弊社把握している範囲では、ソフトウェアベースの鍵管理を採用しているカード発行金融機関は存在しない。

5. HCE やペイメントトークンの将来

もちろん、市場の将来について、完璧に予測することは困難だ。ただ、今後 HCE やペイメントトークンが近い将来復旧していく好材料が存在しているのは事実で、新しい潮流に乗り遅れないように、準備を進めていくべきである。2014 年閣議決定された「日本再興戦略」改訂で、日本政府は 2020 年までにキャッシュレス対応を完了することを、日本クレジット協会がクレジットカードは 2016 年 12 月末までにクレジットカードの 80% を EMV 化すること、2020 年に EMV 化 100% を目標に掲げている。もちろん EMV 化＝コンタクトレス化ではない。

簡単な説明にとどめるが、EMV には接触型と非接触型の決済取引が存在する。実装方法は異なるもののカード偽造や盗難・紛失カードの不正利用を防止するという目的で共通している。接触型の EMV

ではチップを利用した強力な暗号処理と動的な暗号文を活用したカード認証手順で、偽造カードの不正利用を効果的に防止してきた。

非接触型決済には現状①プラスチックカードに搭載された非接触型 IC チップを利用する方式②モバイル端末の NFC を利用する方式の 2 つがあり、②の場合、必ずしも安全とは言い切れない無線通信環境を利用するため、必然的にペイメントトークンを利用するケースが多い。①のプラスチックカードに実カード番号ではなく、ペイメントトークンを格納するようになるのかどうかはまだはっきりしていないものの、盗難・紛失時の損失を最小限にすることができるため、近い将来 EMV チップにペイメントトークンを格納する利用事例が出てくるかもしれない。

EMV 接触型決済の普及が一番の優先事項であるが、2020 年という目標まで残された時間はそれほど長くはない。米国と同様に、コンタクトレス化と EMV 化が同じタイミングで加速していく可能性は十分に有り得る。

近年の訪日旅行者（インバウンド）が増加しており、訪日旅行者が使い慣れない現地通貨のことを気にせず、小売店でスムーズな決済を実行することは重要である。ビジネスチャンスを逃さないのは商売の鉄則だ。販売機会の拡大と商取引の活性化はオリンピック開催に向けて、共通のゴールである。その準備にあたり、決済取引が安全で効率的になっていくのは間違いない。安全で効率的な決済実現に向け、HCE やペイメントトークンの利用が拡大する可能性が高い。HCE とペイメントトークンは対面決済の安全性を高めるだけでなく、オンライン・非対面決済でもセキュリティ強化に有効で、これから伸びていく技術であると考えられる。

一方、21 世紀の初めごろから 10 年以上 IC カードベースの電子マネーを利用し、「かざす」決済に慣れ親しんできた日本居住者にとって、スマートフォンを「タップしてかざす」決済への期待・要求は今のところそれほど強いものではないかもしれない。

ペイメントトークン利用による決済セキュリティ強化の潮流

また、NFC の Type-A / Type-B のカードリーダーの設置、既存カードリーダーのファームウェアの改修を進め、「タップしてかざす」決済が可能な場所を増やしていくことが一つの大きな課題となっている。日常生活の中で利用できることが普及の第一条件である。コンビニエンスストアやスーパーで利用できる状況になれば、消費者の利用は一気に加速する。

また、日本特有の決済環境、国内完結型取引（＝オンアス取引）も考慮しなければならない。トークンによる決済情報のルーティングが確実に実行されるようになるまでに、決済事業者間の微調整・協力も必要になる。

ビジネス面では日本居住者向けには、スムーズなクレジット決済プラスワンのサービス＝特典、リワードの提供等、消費者を引き付ける魅力、付加価値を高める必要がある。ただし、CLO（＝カード・リンクド・オファー）が即収益増加につながるわけではない点に注意すべきだ。プロモーション・キャンペーンの原資が乏しい小規模店舗が CLO による特典付与・キャッシュバックを実施するのは難しい。小規模小売店の経営改善に直結するのかどうかについては賛否両論がある。

専用ハードウェアによる偏りのない乱数生成が必要である。

HSM はハードウェア・セキュリティ・モジュールの略称で、鍵管理と暗号・乱数処理を実行する。HSM は決済インフラの様々な場面で利用されていることはあまり知られていない。

- EMV チップ用のデータ生成
- EMV チップを搭載したクレジットカード発行
- 既存の決済インフラのトランザクション保護（PAN/PIN/MAC を含む決済取引データの保護）
- モバイルデバイスとのセキュアセッションの確立
- ペイメントトークン（DAN）の生成・乱数処理
- ペイメントトークン（DAN）のプロビジョニング

弊社は業界をリードする HSM メーカーで、HCE や決済トークンの実装作業を支援する目的でコマンドや API を準備している。HCE を実装するサービスプロバイダとの導入事例も豊富で、標準化された仕様部分だけでなく、国際ブランド各社が定める独自実装・変更要求にも柔軟に対応し続けている。

6. モバイル決済における HSM の必要性

HCE やペイメントトークンを利用して安全な取引を実行するためには HSM が不可欠である。法律や規則で強制されるものではないものの、HCE やペイメントトークンを実装するにあたり HSM の利用はデファクトスタンダードとなっている。仮にペイメントトークン管理システムが攻撃を受けた場合、単に決済ができないだけでなく、企業は信用を失い、事業継続が困難な状態になりうる。国際ブランドは HSM の利用を推奨している。安全性が必ずしも確保されているとは言えない無線環境を利用することからも、HSM で鍵をアプリケーションから分離して管理するのは必然だ。また、ペイメントトークンは演算により元の値が解読されることがないように、

海外市場開拓 WG

株式会社インフォセック
WG リーダー 樋口 健

■ はじめに

海外市場開拓WGは、日本独自のサイバーセキュリティ製品やサービスにスポットライトを当て、「Made in Japan」のサイバー防御ソリューションを広くグローバル市場に提案・販売していこうという「大志」を掲げた、海外進出を志すセキュリティ企業有志によるWGです。

日本のサイバーセキュリティ市場は順調に拡大していますが、多くの技術や製品・サービスを海外に頼っているのが現状です。製品事業が育っていないことで防御対策技術の開発技術者が育ちにくい、「頭数に縛られるビジネス」から脱却しないと市場規模が成長せず優秀な人材も育たない、といった懸念もあります。

そのようなことから、海外に効果的に進出するための様々な道具立てやベストプラクティス、人脈などをシェアし、All Japan体制で海外に切り込む活動を展開し、販路開拓と保守サポートのための現地企業とのコラボレーション、運転資本の調達、各国法制度対応や契約書文案の整備、進出先での要員採用などのノウハウを共有しよう！という趣旨のもと、本WGは発足しました。

■ 概要

まず、参加メンバーによる討議に基づき、WGの狙いと活動目標を以下の通り設定しました。

1) 海外市場開拓WGの狙いは以下の4項目とする。

- 日本国内のセキュリティ製品・サービス事業者を束ね、All Japan体制で海外市場進出への足掛かりを作る（共同で市場開拓を推進することで、コストとリスクを分散する）
- 成功事例を作って成果とノウハウを共有し、国内製品のパッケージ化、ブランド化を図る（サイバーの世界にも「Made in Japan」クオリティを）
- 当該活動に対する日本政府による後押しを得る

- 「使命感・魂・想い」を共有する同志を集める

2) WGのターゲット市場は「アジアパシフィック＋北米」とする。

- ASEAN諸国は日本同様の地政学的リスクを有し、経済成長と共にサイバー関連リスクが増加中。ノウハウ・資金の両面において日本に対する期待感は強く、欧米企業に市場を席卷される前に存在感を示しておきたい
- 一方、ASEAN地域でビジネス展開するうえでは、欧米での導入実績は重要。北米で通用しない製品はグローバルでも通用しない

3) 主な活動内容、想定アウトプットは以下の通りとする。

- 先行して海外市場に進出しているサイバー関連企業の事例を調査（日本国内企業に加えて海外ベンチャーの事例も）
- 海外進出に関する共通課題の抽出と、課題解決指針の策定（販路開拓、製品保守体制の整備、現地人材の採用、事業拠点の整備、活動資金の獲得、現地の規制・届出を含む法務契約面の対応…等を纏めて「海外サイバー市場開拓マニュアル」を執筆）
- 共同プロモーション活動を展開（海外展示会への出展、メディアへの露出）
- 経済産業省・外務省など関連官庁とのタイアップを企画・調整

■ WGの構成

5月のキックオフ後、WGを“日本のサイバー防御製品を輸出する専門商社”に見立てた上で、機能別の3つの分科会を設置、それぞれ並行して具体的な検討作業を進める体制を整え、月1回ペースで定例会を開催しました。（注：(L)はリーダー、(SL)はサブリーダー）

JNSA ワーキンググループ紹介

- ・ 製品サブWG：(L) FFRI 金居氏、(SL) NEC 一宮氏
WG参加企業の製品・サービスをマッピングし、これらを組み合わせた「Made in Japan」のサイバー防御ソリューションをパッケージ化。これらを網羅した英文紹介資料などを纏めるグループ
- ・ 市場・法規制サブWG：(L) 日本企画 利氏、(SL) インフォセック 進藤氏
ターゲット国の市場動向と法規制動向を調査し、当該国に進出するうえでの課題と解決策を纏めるグループ
- ・ 渉外サブWG：(L) NEC 中間氏、(SL) アークン 呂氏
当WGとして参加するイベントの取り纏めや対外広報対応、関連省庁との渉外活動を展開するグループ

の試みである海外出展への道を急ピッチで進めることとなりました。

参加メンバーの旅費は全て手弁当での参加でしたが総勢8社14名が当日交代でブースに立ち、各社のパネルやカタログ展示と製品サブWGが急ぎ作成したWGメンバー企業の商材総合カタログ、各社が持参したノベルティ等の配布を行いました。JNSAで在庫として残っていたものにリーダー自らアイロンプリントでロゴを付けた即席スタッフジャンパーを全員が着用しカタログを配布する様子は、当日の展示会場でもかなり目立っていたと言えるでしょう。

当日は数少ないJapan ブースであるということ、また毎日数回開催したブースプレゼンの効果もあり盛況な賑わいをみせ、当初用意したJNSA商材総合カタログ200部は2日目の半ばで在庫が付き、急ぎ現地で印刷補充するという勢いをみせました。当日の様子は、スキャンネットセキュリティ様とZDNet Japan様が記事にして下さっていますのでぜひご覧下さい。今回の初の試みの成功を機に、今後は北米市場調査団やRSAカンファレンスUSAでの出展なども進めていきたいと考えています。

■ RSA Conference APJ 出展

このように本WGは4月に発足、5月にキックオフをしたばかりではありましたが、JNSAが7月22日（水）-24日（金）にシンガポールで開催される「RSA Conference Asia Pacific & Japan2015」に協力していたこと、そして、WGメンバーの熱意によりJNSA初



当日の JNSA ブースの様子



WG メンバー企業の商材総合カタログ

■ WG 参加メンバー

WG メンバーは随時募集中です。ぜひ2016年のRSA Conference APJでは一緒に出展しませんか？

株式会社インフォセック	樋口健 (WGリーダー)	株式会社シグマクシス	笠松隆幸
株式会社アークン	蛭間久季	ソフトバンクテクノロジー株式会社	鈴木直博
株式会社アークン	名倉崇之	ソフトバンクテクノロジー株式会社	久保祐人
株式会社アークン	呂 天元	株式会社ディアイティ	杉本康則
(ISC) 2ジャパン	衣川俊章	デジタルアーツ株式会社	本澤直高
アルプスシステムインテグレーション株式会社	菅野泰彦	日本企画株式会社	利 哲平
株式会社インフォセック	松下めぐみ	日本電気株式会社	吉野真一
株式会社インフォセック	進藤剛洋	日本電気株式会社	中間貴規
EMCジャパン株式会社RSA事業本部	水村明博	日本電気株式会社	一宮隆祐
NRIセキュアテクノロジーズ株式会社	橋本 淳	株式会社ネクストジェン	二村廉太
NRIセキュアテクノロジーズ株式会社	与儀大輔	ユニアデックス株式会社	大平伸一郎
株式会社FFRI	金居良治	株式会社ユービーセキュア	田中大介
株式会社FFRI	川原一郎	株式会社ラック	佐々木紅
株式会社GENUSION	中島盛義	株式会社ラック	青木和仁
株式会社GENUSION	益永哲生		



マイナンバー対応情報セキュリティ検討 WG

トレンドマイクロ株式会社
WG リーダー 萩原 健太

■ はじめに

本WGでは、マイナンバー制度の開始が目前に迫る中、企業がどのような準備を行えばよいのか、また現在行っている準備が適当なのか等、より現場の拠所となる成果物を目指し、検討・作成を行っているWGです。

■ 概 要

内閣官房や特定個人情報保護委員会をはじめとした政府機関から様々な指針やガイドラインなどが示されていますが、まだ企業におけるマイナンバー対応は進み切っておりません。また、いざマイナンバー対応を行うために体制構築を始めようとするといくつかの壁にぶつかります。

まず一つ目は「どこからマイナンバーに関する情報を収集するのか」という壁です。現行のマイナンバーは税・社会保障・災害の三分野に限られていますが、関連する情報は政府機関から複数文書等が公開されています。また情報量も増えてきているため、今度は読み切れない(本来の言葉の意味や意向も含めて)個人や組織も多いと考えられます。

二つ目は集めた情報を活かして、「どのように社内

体制を構築するのか」という壁です。マイナンバーの収集～廃棄までの各プロセスを理解し、また様々なリスクを想定し、社内体制を整備する必要があります。既存の文書等では伝わりきらない、より具体的構築作業をイメージできる情報の整理が必要です。

そして三つ目は「安全管理措置をどこまで実施するのか」という壁です。いかなる企業においても、基本方針・取扱規定を策定し、組織的・人的・物理的・技術的な安全管理措置の検討が必要です。費用をかけられるのであればいくらかでも高いレベルでのセキュリティ対策を施すことが出来ますが、費用には限りがあります。最低限の安全管理措置がどのくらいなのかを知ることが出来れば企業における安全管理措置の対応も推進されると考えます。そこで、セキュリティのベースラインを議論し、組織の体制構築や見直しに役立つチェックシートの検討をします。

このような壁を解決するために、当該WGではそれぞれの課題解決が図れるように「情報集約」「構築検討」「情報セキュリティ」の3つのチームを設けて検討を行っております。尚、検討結果の第一弾を2015年9月を目標とし、リリースに向けた検討を迅速に進めております。またマイナンバー制度や検討結果をより広く認知頂けるように、セミナーなどの開催も予定しております。



【WG 構成】

WGチーム名称	成果物(予定)	チームリーダー	サブリーダー
全体	全体	萩原 健太 (トレンドマイクロ)	松森 健一 (デジタルアーツ)
情報集約	情報収集ポータル	根津 研介 (NTT データ先端技術)	富田 高樹 (みずほ情報総研)
構築検討	構築検討キット	松森 健一 (デジタルアーツ)	持田 啓司 (大塚商会)
情報セキュリティ	リスク分析シート	工藤 雄大 (大日本印刷)	古川 勝也 (SecureWorks Japan)

【WG 参加企業一覧】 (50 音順にて記載)

上記、各チームに計28社の皆様にご参加、ご尽力を頂いております。

企 業 名	
株式会社アイピーキューブ	総合警備保障株式会社
株式会社アズジェント	ソフトバンク・テクノロジー株式会社
アドソル日進株式会社	大日本印刷株式会社
インタセクト・コミュニケーションズ株式会社	デジタルアーツ株式会社 (※ 発起人)
エヌ・ティ・ティ・アドバンステクノロジー株式会社	SecureWorks Japan 株式会社
エヌ・ティ・ティ・データ先端技術株式会社	トレンドマイクロ株式会社
株式会社大塚商会	日本ユニシス株式会社
キヤノンITソリューションズ株式会社	日本電気株式会社
株式会社ケーケーシー情報システム	ネットワンシステムズ株式会社
株式会社コンシスト	株式会社日立ソリューションズ
株式会社サイバード	富士通株式会社
新日鉄住金ソリューションズ株式会社	株式会社富士通ソーシャルサイエンスラボラトリ
JPCERT コーディネーションセンター	みずほ情報総研株式会社
セコムトラストシステムズ株式会社	株式会社ラック

【直近のスケジュール】

2015年5月：発足検討会(デジタルアーツ様による発起)
2015年6月：WG発足・検討の開始
2015年9月：リリース・セミナーの開催

※以降は鋭意改善を実施予定。

会員企業ご紹介 40

アイマトリックス株式会社

<http://www.imatrix.co.jp/>

imatrix

アイマトリックス株式会社は2000年に創立、主に電子メールシステムのセキュリティに関連するサービス、技術・市場開発を行っています。「マトリックスキャン」に代表されるメールセキュリティソリューションを初め、Webセキュリティをプラスしたクラウド型セキュリティサービス「マトリックスクラウド」や、システム単独にてメールシステムの構築を実現する統合型メールシステム「マトリックスメール」の開発・販売も行っています。いずれもアイマトリックス独自開発の技術による自社製品であり、国内大手通信事業者から、企業、大学、ISPと多岐にわたる多くの団体・組織に提供しています。

マトリックスキャン APEXⅢ

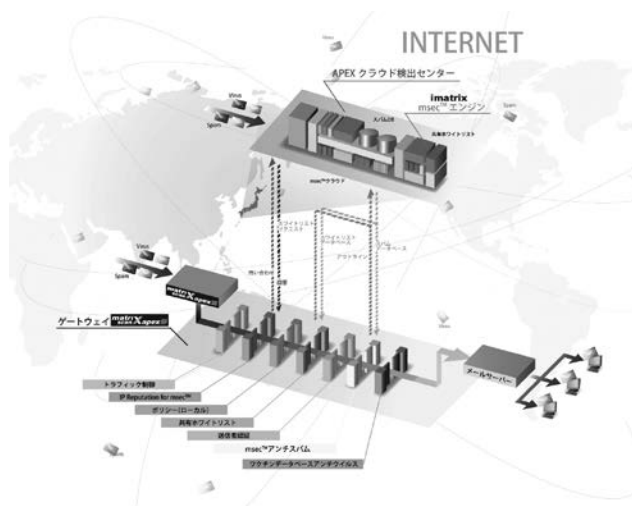
ビジネスにおけるコミュニケーションインフラとして重要な電子メール。昨今、海外発のスパム以上に日本語のスパムが増加傾向にあります。マトリックスキャンAPEXⅢは、独自開発「msec™」テクノロジーにより、日本語に特化したデータベースを収集し、国産ならではの信頼性を実現しています。

msecアンチウイルスを標準搭載し、メールを感染経路とするウイルスの侵入を確実に防御します。

「msec™」テクノロジー

自社開発の国産技術であり、未知の脅威に対応する先端技術をもちいて包括的にマルウェアを検知し、標的型攻撃にも柔軟に対応します。また、セキュリティプラットフォームの拡充を速やかに行える設計となっているため、新しいアンチマルウェアテクノロジーやアルゴリズムを容易に製品に採用することが可能です。

matriX scan X apex



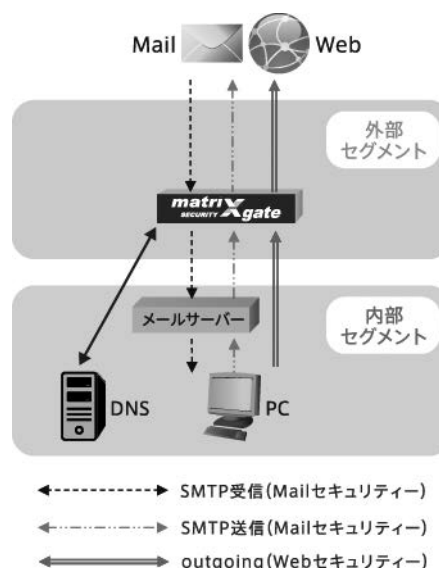
マトリックス ゲート

matriX SECURITY gate

2015年10月リリース予定!

マトリックスキャンにWebセキュリティ機能を搭載したアプライアンス製品を、新たにリリースいたします。

Webセキュリティ機能としては、不正サイトへの閲覧規制だけでなく、DBDサイトへのアクセス遮断によりマルウェア感染を防止し、C&Cサーバー通信経路を遮断することでPC情報の搾取を防御。入口と出口の両面から最新のサイバー攻撃に対応します。



お問い合わせ先：アイマトリックス株式会社 カスタマーリレーションズ セールス TEL: 044-272-6771
〒216-0004 神奈川県川崎市宮前区鷺沼3-2-6 鷺沼センタービル4F

【これまでも、これからも、エンタープライズのお客様と共に。】

アライドテレシスはエンタープライズ市場(SouthSIDE)を守り続けて、もうすぐ30年を迎えます。
これからもSouthSIDEのお客様と価値観を共有しながら、IT基盤のスペシャリスト集団であり続けます。

【お客様のご要望に沿った各種セキュリティソリューションをご提案します。】

ネットワーク専門メーカーとしての長い経験や豊富な情報、積極的な研究開発を通じて、ハード・ソフトを知り尽くしているアライドテレシスはソリューション分野、さらにお客様のさまざまなビジネス課題を解決するコンサルティングサービスのご提供へと、事業領域を拡大しています。お客さまのニーズを十分に理解し、最適な製品、ソリューション、サービスをつくり、ご提供します。

Secure Enterprise SDN Solution "SES"

お客様の課題に対しネットワーク運用・管理の効率化とセキュリティの強化を図るべく、アプリケーション連動ソリューションの集大成として企業向け各種アプリケーションと連動させた、次世代型ネットワークSDNによるソリューションを提供します。

▼ S E S の 機 能

App連動プロビジョニング

セキュリティ統制

ふるまい検知

ネットワークの管理工数の増大とセキュリティレベル維持の2つを解決します。
アライドテレシスが提案するSecure Enterprise SDN Solution



※Secure Enterprise SDNとは、オフィス環境のさまざまなネットワーク機器に対し、SDNの最大の特徴であるソフトウェア(アプリケーション)との連携/連動によるネットワークの動的な変更によりネットワーク運用管理の効率化とセキュリティの強化を実現するソリューションの総称です。

脅威を可視化する統合監視ソリューション "Envigilant"

アライドテレシスの信頼性の高いIPネットワーク上に革新的なテクノロジーを組み合わせることにより統合型セキュリティ監視プラットフォーム "Envigilant" を実現します。

この "Envigilant" では、IPカメラによる監視だけでなく、ガンマ線検出センサー、バイオセンサーなどの各種センサーを統合することにより、脅威を事前に「見える」状態にすることが可能です。また、ダッシュボード機能により、包括的な管理が可能であり、高い操作性を提供します。

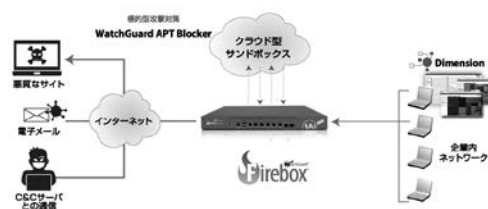


ウォッチガード・テクノロジー・ジャパン株式会社は、統合型セキュリティアプライアンスの老舗ベンダーとして、独自のセキュリティ統合技術によるネットワークセキュリティプラットフォームを提供しています。WatchGuard Firebox シリーズ / XTM シリーズを中心に、ベストオブブリードのセキュリティ機能、ポリシーベースの操作性に優れた管理ツール、ネットワークセキュリティ可視化ツール、標的型攻撃対策などを提供しています。



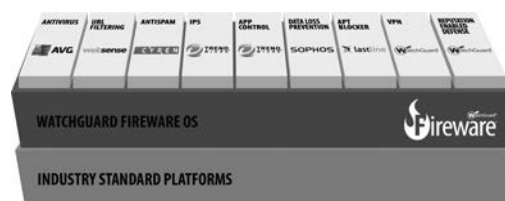
最適なセキュリティ対策とエンタープライズクラスのパフォーマンスの両立

企業のネットワークに必要なすべてのセキュリティ機能が統合された最高性能のセキュリティプラットフォームにより、高度なセキュリティ機能と驚異的なネットワークパフォーマンスを実現し、妥協のない安全なセキュリティ対策と高い費用対効果でビジネスに貢献します。



ベストオブブリードのセキュリティ機能

洗練されたベストオブブリードセキュリティ機能群が、ウォッチガードの独自 OS Firewall で1台のアプライアンスに統合されます。各機能はモジュール形式で実装されているため、必要に応じて各機能のライセンスをアクティブ化することで、すぐに利用を開始できます。統合セキュリティの大きなメリットとして、高度なセキュリティ機能を低コストで実現することが可能です。



標的型攻撃対策 WatchGuard APT Blocker

ウイルス対策や不正侵入検知などシグネチャ型のセキュリティ対策で対応が困難な未知のマルウェアを、クラウド上のサンドボックス（米 Lastline 社または MSS ベンダー）と連携することで標的型攻撃を検知、ブロックします。先進のフルシステムエミュレーションによるサンドボックス技術を活用した検知プロセスにより、大規模ネットワーク向けの製品と同等の高度な技術を1台のアプライアンスで実装し、悪質なマルウェアによる攻撃を阻止します。

セキュリティインテリジェンス WatchGuard Dimension

定評あるネットワーク可視化ツールである WatchGuard Dimension はアプライアンスの標準ツールとして活用することが出来ます。ビジュアル化されたセキュリティの状況の監視により、管理者は容易にセキュリティの状況を把握し、直感的に操作が可能な管理コンソールで容易にセキュリティ対策のアクションを行う事が可能で、管理者の負荷を大幅に軽減します。



お問い合わせ先：ウォッチガード・テクノロジー・ジャパン株式会社

〒106-0041 東京都港区麻布台 1-11-9 CR 神谷町ビル 5 階

TEL 03-5797-7205 URL: https://www.watchguard.co.jp

KPMGは監査、税務、アドバイザリーサービスを提供するプロフェッショナルファームのグローバルネットワークです。世界155カ国のメンバーファームに約162,000名の専門家を擁し、深い専門知識と知見を世界中のクライアントに提供しています。

KPMG コンサルティングは、KPMG ジャパンのメンバーファームとして、グローバル規模での事業モデルの変革や経営管理全般の改善をはじめとしたアドバイザリーを提供します。具体的には、事業戦略策定、業務効率の改善、収益管理能力の向上、ガバナンス強化やリスク管理、IT戦略策定やIT導入支援、サイバーセキュリティ対策支援、組織人事マネジメント変革などを提供しています。

最適化されたサイバーセキュリティアドバイザリーサービスをワンストップで提供

IT環境の劇的な変化に伴い、サイバー攻撃は重層的な攻撃手法がとられることが増え、従来型の対策では防御が困難であることが指摘されています。実際、多くの企業では攻撃を受けてから後追いの対応をとらざるを得ないのが現状で、今後は従来の情報セキュリティ管理態勢をサイバーセキュリティ仕様へと高度化していかなくてはなりません。KPMGのサイバーセキュリティアドバイザリーサービスは、グローバルネットワークを活かして得られた、世界規模での研究成果や導入事例を踏まえたうえで、顧客最適化されたサービスを提供することが可能です。人・組織／プロセス／テクノロジーというサイバーセキュリティ上考慮すべき異なるスキルが必要なサービスを、各専門家が連携しながらワンストップで提供する体制を整えています。

Prepare サイバーアクセスメントサービス

サイバー攻撃の防御態勢に関する現状の問題点を明らかにし、サイバー攻撃防御態勢の改善ロードマップ立案をトータルに支援します。

【サービスの一例】

サイバー攻撃防御態勢クイック診断
サイバー侵入テスト
モバイルセキュリティ診断
無線LANセキュリティ診断
SNS利用のセキュリティ診断
顧客情報・営業秘密のセキュリティ診断
海外拠点のセキュリティ診断

サイバー攻撃防御態勢の核となる体制、システム、ルール、PDCAの要素について、強化、改善するための活動をトータルに支援します。

【サービスの一例】

サイバーセキュリティ組織の立上げ支援
サイバーセキュリティポリシー立案支援
モバイル・無線LANセキュリティ強化支援
SNSセキュリティ強化支援
サイバー攻撃防御態勢の高度化支援
セキュリティ担当役員の補佐

Protect サイバーマネジメントサービス

Integrate サイバーインテグレーションサービス

時々刻々と進化していくサイバー攻撃に対して、防御態勢を有効に機能させ続けるために、既存の企業活動との統合、定着をトータルに支援します。

【サービスの一例】

サイバー攻撃情報インテリジェンス支援
GRC活動との統合支援
事業継続計画（BCP）との統合支援
サイバー攻撃に関する教育啓発支援
グローバルな防御態勢への変革支援
制御システムの防御態勢への変革支援
サイバー攻撃防御態勢変革支援



サイバー攻撃が発生した際の広報・メディア対応、事実究明、再発防止策の立案、展開について、適切かつ迅速なアドバイスでトータルに支援します。

【サービスの一例】

緊急対策本部の立上げ運営支援
緊急時のメディア対応支援
サイバー攻撃に関する情報開示支援
サイバー攻撃の痕跡調査フォレンジック
サイバー攻撃の損失額の算定支援
再発防止策の展開支援

Detect & Respond サイバーレスポンスサービス

JNSA 会員企業のサービス・製品・イベント情報

■製品紹介■

○標的型攻撃検知サービス「PatoLogphinR」 (パトログフィン)

標的型攻撃を高い精度で検知するサービスです。ウイルス対策ソフトやIPS/IDSなどの既存対策では検知できない標的型攻撃の発生を検知して、適切な対策の実施をサポートします。ネットワーク構成の変更や新たな機器の購入が不要なので、コストを抑えて短期間で導入可能です。プロキシログの分析により、オフィス環境に対する標的型攻撃を検知し、感染端末と緊急対応策をご報告するサービスです。

【製品情報詳細】

<http://www.nttdata.com/jp/ja/lineup/patologphin/index.html>

◆お問い合わせ先◆

株式会社NTTデータ
セキュリティビジネス推進室
TEL: 050-5546-2556

○特権アカウント管理ソリューション CyberArk (サイバーアーク)

標的型攻撃はActive Directoryを狙います。ドメイン管理者アカウントを窃取できれば、管理下のすべてのユーザとコンピュータを支配できるからです。CyberArkは以下の対策を実施し、Active Directoryを標的型攻撃から守ります。

- ・パスワード管理の強化
- ・信頼できる端末やユーザのみにアクセスを制限
- ・管理者アカウントの定期的な監査と使用状況の確認

【製品情報詳細】

<http://www.dit.co.jp/products/cyber-ark/>

◆お問い合わせ先◆

株式会社ディアイティ
ネットワークセキュリティ事業部
TEL: 03-5634-7652
E-mail: product-info@dit.co.jp

■イベント情報■

○カスペルスキー 「脆弱性対策セミナー」 カスペルスキーが考えるこれからのぜい弱性対策

APT攻撃や標的型攻撃など、既存のセキュリティ対策では防御が難しい攻撃による被害が相次いでいます。本セミナーでは、頻発するサイバー攻撃について企業防衛の観点より対策のポイントや被害例についてご紹介するほか、エンドポイントにおけるマルウェア対策や、脆弱性の効果的な検知及び対策ソリューションについてデモを交えてご紹介いたします。

【イベント情報詳細】

<http://data.kaspersky.co.jp/seminar01>

◆お問い合わせ先◆

株式会社カスペルスキー セミナー事務局
TEL: 03-5259-5437
E-mail: jp-event-admin@kaspersky.com

第5回日韓情報セキュリティシンポジウム開催報告

2015年7月13日(月)に韓国ソウルにて「第5回日韓情報セキュリティシンポジウム」を韓国知識情報保安産業協会(略称KISIA)と共催で開催いたしました。このシンポジウムは2011年より日本と韓国とで交互に開催しており、本年が5回目の開催となります。前回は2014年11月に東京で開催し、2018年韓国冬季オリンピック、そして2020年東京オリンピック・パラリンピックを視野に入れたセキュリティ連携活動を行うことでKISIAと合意をいたしました。それを受けての今回のシンポジウム開催となります。日本からは招聘講師を含む11名が参加し、全体で150名の参加者となりました。

まず始めに、両国の国家戦略について日本からは内閣サイバーセキュリティセンター(NISC)藤田清太郎参事官と韓国からは未来創造科学部情報保護企画課のイカンヨン事務官にお話をいただきました。

藤田参事官からは、日本のサイバーセキュリティ基本法とサイバーセキュリティ戦略案についてお話いただきました。サイバーセキュリティ基本法は我が国の方針を定めたものであり、「サイバーセキュリティ」というカタカナ名称が法律用語に使われたことは大変珍しいことだそうです。新たな「サイバーセキュリティ戦略」では、情報セキュリティは経済発展の一分野と位置付け、国家安全保障も含めるようになったことが特徴だそうです。戦略を支える柱と

しての研究開発と人材育成についても触れられて本セッションは終了しました。

続いてイカンヨン事務官からは、韓国の国家背景、国家戦略の外観と情報共有の状況などについて説明があり、次にCIIP、ISMSや中小企業向けのSECURITY STAR施策などの説明があり、最後に韓国のサイバーセキュリティのチャンスと弱点が共存する国であるという特性から、日本と今後お互いに連携協調して発展していきたいとお言葉がありました。これからは日韓の協調の機会が多いので、緊密な協力関係を築いていきたいとの言葉で締めくくられました。

続いて、KISIA シムジョンヒョン会長、JNSA 田中英彦会長、韓国未来創造科学部情報保護政策官 チョンハンギョン局長のご挨拶がありました。

シムジョンヒョン会長からは、7月は情報保護の月であり本シンポジウムは国際協力のモデルとして位置付けられつつある、今後も日本と韓国のネットワーク作り結び付けたいのご挨拶がありました。次に日本の田中英彦会長からは、オリンピックに向けた経験の共有や両国の経済発展を目的に、両国の相互理解を深めることを期待したいのご挨拶がありました。そして韓国チョンハンギョン局長からは、両国のネットワーク共有が続くことを祈念するとの言葉がありました。



イベント開催の報告

ランチタイムをはさみ午後のセッションは両国のオリンピック委員会の方のご講演です。日本からは東京オリンピック・パラリンピック競技大会組織委員会のテクノロジーサービス局局長である館剛司氏からお話いただきました。

館氏からは、2020年の大会時に想定されるリスクや何を準備する必要があるのか、何をどう守るのかについて、そして最後に大会のレガシー（遺産）についての考察をお話されました。

続いて韓国からは平昌冬期オリンピック大会組織委員会オサンジン局長がお話されました。まず、ピョンチャン冬期オリンピックの外観について説明があり、次に、ゲームネットワーク、アプリケーション、データセンター、ATOSの提案するCHP/CHSデータセンターの構成などについて、いかにセキュリティ対策を行うかについて説明がありました。個人情報保護の事前評価サイトの開発最大では50万の個人情報を扱うことになるため、様々な有識者たちがオリンピックCERTを構築してノウハウの構築やパターンの共有などを行っているそうです。少ない予算で効率的に最適なセキュリティ対策を構築することをめざしているとのことでした。

続いてのセッションはIoTをテーマに、日本からはJNSA 調査研究部会長でインターネットイニシアティブ社の加藤雅彦氏にご講演いただきました。

加藤氏からは日本のIoTの状況についての説明とJNSAのIoTセキュリティWGの取り組みについてお話いただきました。韓国からは、イグルーセキュリティ社のナムヒョンウ研究所長にご講演いただきました。身近となっているIoTであるが攻撃が多いことも報告されており、その対策の必要性についてお話されました。

続いては両国のパネルディスカッションです。座長は日本側はJNSA 副会長でKDDI社の中尾康二氏、韓国はスンチョンヒヤング大学のヨム教授、パネリストは日本側はJNSA 副会長で日本マイクロソフト社の高橋正和氏、JNSA 事務局長でディアイティ社

の下村正洋氏、韓国側はKISAのソングョンホ団長とホンギョン KISIA 副会長、ユンドユシク KISIA 副会長です。

日本側からは今年度の新たな取り組みであるJNSA CERCの紹介などを行い、韓国側からは共同の市場調査や東南アジアへ向けた市場開拓の提案など、活発なディスカッションが行われました。



その後、日韓企業による企業紹介が行われ、最後に中尾氏とヨム氏により以下の合意事項が確認され、日韓シンポジウム2015は閉会となりました。

日韓シンポジウム2015合意事項

- ・ 2016年5月に日本で第6回日韓情報セキュリティシンポジウムを開催する、また、オリンピック/パラリンピックの成功のための情報交換を促進し、年内にワークショップを行う
- ・ 両国のサイバーセキュリティ協力の強化のため、多角的な視点での両国協力関係を構築する、そのための多角的な協力を実施する
- ・ 市場調査を含めた情報交換を推進する、特にIoTセキュリティの市場調査などの具体的なアクションアイテムは2015年内を目処に確定していく
- ・ ビジネスの機会提供を模索し東南アジアへのグローバル進出を目的とした相互協力を模索する

JNSA 2014年度活動報告会

2015年6月9日(火)秋葉原UDXギャラリーネクストにて「JNSA 2014年度活動報告会」が開催されました。JNSAの部会・ワーキンググループより前年度の活動報告と今年度の活動計画を発表するとともに、JNSAの活動内容を会員以外にも広く周知することを目的として、毎年6月に開催しています。当日は176名の参加者をお迎えし、盛況のうちに終了いたしました。

JNSA 2014年度活動報告会プログラム

2015年6月9日(火)9:30~15:30 於:秋葉原UDXギャラリーネクスト

トラック1 (NEXT1 / 定員: 180名)	
◆午前の部	
【A1】電子署名 WG	9:30-10:00 (30分)
「2014年度電子署名WG成果報告」	WGリーダー: 宮崎一哉氏 (三菱電機株式会社)
【A2】PKI相互運用技術WG (パネルディスカッション)	10:00-11:30 (90分)
「改正個人情報保護法による情報セキュリティへの影響」ビッグデータ・IoT時代における個人情報の保護と利活用	
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: 宮内 宏氏 (五番町法律事務所 弁護士)	
福田 尚弘氏 (パナソニック株式会社)	
... 11:30 ~ 12:30 昼休み ...	
◆午後の部	
【A3】アイデンティティ管理 WG	12:30-13:00 (30分)
「2014年度アイデンティティ管理WG成果報告」	富士栄 尚寛氏 (伊藤忠テクノソリューションズ株式会社)
【A4】未来予測検討プロジェクト	13:00-13:20 (20分)
「未来予測検討プロジェクト活動報告 ~2020年のサイバー脅威とは~」	
プロジェクトリーダー: 唐沢 勇輔氏 (ソースネクスト株式会社)	
休憩 (10分)	
【A5】脅威を持続的に研究する WG	13:30-13:45 (15分)
「問題の本質を見抜こう! 脅威を持続的に研究するWGの紹介」	
WGリーダー: 大森 雅司氏 (株式会社日立システムズ)	
WGサブリーダー: 岡谷 貢氏 (富士通株式会社)	
本川 祐治氏 (株式会社日立システムズ)	
【A6】組織で働く人間が引き起こす不正・事故対応 WG	13:45-14:00 (15分)
「内部不正のキモに働きかけるために」	WGリーダー: 甘利 康文氏 (セコム株式会社IS研究所)
【A7】IoTセキュリティ WG	14:00-14:15 (15分)
「拡大するIoTとそのセキュリティについて」	WGリーダー: 松岡 正人氏 (株式会社カスペルスキー)
【A8】スマートフォン活用セキュリティポリシーガイドライン策定 WG	14:15-14:30 (15分)
「スマートデバイスのガイドラインって難しい? ~より広く活用頂くために~」	
WGリーダー: 柝沢 直樹氏 (トレンドマイクロ株式会社)	
休憩 (10分)	
【A9】セキュリティ市場調査 WG	14:40-15:10 (30分)
「2014年度セキュリティ市場調査報告書より ~市場調査WG活動成果発表~」	川越 弘大氏 (株式会社イーセクター)
【A10】シンギュラリティ調査 WG	15:10-15:25 (15分)
「シンギュラリティの最新動向」 ~コンピュータが人間の知性を凌駕する~	
WGリーダー: 広口 正之氏 (リコージャパン株式会社)	

イベント開催の報告

トラック2 (NEXT3 / 定員: 80名)	
【B1】日本セキュリティオペレーション事業者協議会 (ISOG-J) 報告	9:30-9:45 (15分)
「脆弱性診断士に!!! おれはなるっ!!!!」	WG1 リーダー: 上野 宣 氏 (株式会社トライコーダ)
◆午後の部	
【B2】セキュリティ理解度チェック WG 報告 JNSA ソリューションガイド活用 WG 報告	12:30-13:10 (40分)
「関係法令 (マイナンバー法等) の問題追加やプレミアム版の更改について」	セキュリティ理解度チェック WG リーダー: 萩原 健太 氏 (トレンドマイクロ株式会社)
「2014 年度 JNSA ソリューションガイド活用 WG 活動報告」	JNSA ソリューションガイド WG リーダー: 秋山 貴彦 氏 (株式会社アズジェント)
休憩 (10分)	
【B3】教育部会	13:20-13:50 (30分)
「新 IT スキル標準 (iCD) との SecBoK 連携活動および講師紹介ポータル開設のご紹介」	部会長: 平山 敏弘 氏 (日本アイ・ビー・エム株式会社)
休憩 (10分)	
【B4】社会活動部会 (BoF)	14:00-15:30 (90分)
「IT 環境の変化に対応していくインシデント対応の模索」	
コーディネータ: 高橋 正和 氏 (日本マイクロソフト株式会社)	
パネリスト: 有村 浩一 氏 (JPCERT コーディネーションセンター)	
徳田 敏文 氏 (日本アイ・ビー・エム株式会社)	
西尾 秀一 氏 (株式会社 NTT データ)	
村上 晃 氏 (日本 CSIRT 協議会 運営委員)	

活動報告会の発表資料は JNSA のウェブサイトで公開しています。ぜひご覧ください。

<http://www.jnsa.org/seminar/2015/0609/index.html>

ライトニングトーク夏祭り2015 参加レポート

ソースネクスト株式会社
唐沢 勇輔

2014年12月のライトニングトーク大忘年会に引きつづき、2015年7月30日(木)に社会活動部会主催で「ライトニングトーク夏祭り2015」を開催いたしました。若手も含めて色々な方に、もっとJNSAの活動に顔を出していただければとの思いから、「JNSA会員であること」のみを参加資格として、テーマも絞らずに開催しました。



今回は飛び入り参加も含めて10名の方に登壇いただき、以下のようなテーマでお話いただきました。

- ・第五の次元
- ・セキュリティでお仕事するということ Ver. 十三ヶ月目
- ・愛・セキュリティ
- ・社会人10年目の苦悩 ～見えた一筋の光～
- ・古くて新しいMalvertising問題
- ・社内ルールは無力? メール誤送信の実態調査からわかった「従業員のセキュリティ意識」
- ・セキュリティエンジニアの休日の過ごし方

ライトニングトーク登壇投票			
順位	氏名	所属	得票数
1	山口 幸治	社会人10年目の苦悩 ～見えた一筋の光～	10票
2	大塚 昌平	第五の次元	4票
3	大塚 昌平	セキュリティでお仕事するということ Ver. 十三ヶ月目	4票
4	唐沢 勇輔	古くて新しいMalvertising問題	5票
5	森田 裕也	社内ルールは無力? メール誤送信の実態調査からわかった 「従業員のセキュリティ意識」	6票
6	中塚 隆	愛猫にラグジュアリーなサービスを提供したいが セキュリティに不安がある女子はどう身を守るか	1票

- ・愛猫にラグジュアリーなサービスを提供したいがセキュリティに不安がある女子はどう身を守るか
- ・温故知新構造化プログラミングの取り組みを振り返る

ゆる～い話からちょっとまじめな話題まで多岐にわたるテーマで個人的にも大変楽しませていただきました。1人7分ずつのライトニングトークが終わると、聴講者が1人3票を気に入った人に投票します。今回の1位は文句なしで「愛猫にラグジュアリーなサービスを提供したいがセキュリティに不安がある女子はどう身を守るか」でエントリーされたアドソル日進の中原様でした。1位の方には賞金1万円を贈呈させていただきました。

そして第二部は、1位～5位の方にパネラーになっていただき、お酒や食事をいただきながらのフリートークです。個人的にはライトニングトーク大会は第一部も大変面白いですが、この第二部が本番です。道後、白浜、越後湯沢などのセキュリティカンファレンスも夜が本番などと言われますが、パネラーを無視して(!)会場内で繰り広げられる議論は楽しいだけでなく、とてもレベルが高いもので、私自身非常に勉強になってます。

解析と使用許諾の関係、アニメの攻殻機動隊に出てくる攻性防壁のように攻撃者に対する攻撃は許されるか? など、オープンな場所ではなかなかできない議論が繰り広げられていました。

会員の皆様も、ぜひ次回は登壇者として、あるいは聴講者としてご参加いただければ幸いです。



2015 年度 「インターネット安全教室」のご案内

～パソコンや携帯電話で思わぬトラブルや犯罪にまきこまれないために～

誰でも手軽にインターネットに接続できるようになった今日、ウイルス感染、詐欺行為、プライバシー侵害など情報犯罪の被害にあう危険性がますます高くなってきています。いかに技術が進歩しても、ひとりひとりの意識の向上、モラルの徹底がなければ、これらの被害を防ぐことはできません。JNSAでは、経済産業省の委託事業として一般市民の情報セキュリティ知識向上のセミナー「インターネット安全教室」を、過去10年にわたって実施してきました。2014年度より経済産業省補助金事業、独立行政法人情報処理推進機構 (IPA) 委託事業として、引き続き「インターネット安全教室」を全国で開催して参ります。

【開催概要】

- 【主 催】 独立行政法人情報処理推進機構 (IPA)、NPO 日本ネットワークセキュリティ協会
【共 催】 全国各地のNPO・団体・自治体・学校など
【協 力】 全国読売防犯協力会
【後 援】 サイバーセキュリティ戦略本部、警察庁、新聞各社、各地自治体、都道府県警察等

インターネット安全教室とは？

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

会場では参加者全員に、ドラマやドキュメンタリーを通じて最新の情報セキュリティに対する脅威が学べる「映像で知る情報セキュリティ」の最新版DVDのほか、情報セキュリティ対策のポイントをわかりやすく解説する教材「インターネット安全教室」、子ども向けの「小中学生のためのインターネット安全教室」、家庭向けリーフレット「みんなで守って安全・安心8か条」「親子で守って安全・安心10か条」を配布し、情報セキュリティの向上にお役立ていただいております。



こんな方はぜひご連絡下さい

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

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

最新の開催状況については、「インターネット安全教室」ホームページをご確認ください。

<https://www.ipa.go.jp/security/keihatsu/net-anzen.html>



SECURITY CONTEST (SECCON) 2015

サイバー攻撃やマルウェア感染など、情報セキュリティを脅かす事件・事象が近年相次いで発生しており、日々悪質化するこれらの攻撃を防御するためには、優秀な情報セキュリティ技術者の育成とスキルの高度化が不可欠となっています。

このような背景を受け、2012年に日本ネットワークセキュリティ協会(JNSA)内にセキュリティコンテスト実行委員会が設立されました。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、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標として、セキュリティ技術を競うコンテストを継続して開催しています。

初年度のコンテストは、社会人を対象としたものでしたが、その後年々、対象・規模を広げ、昨年度の「SECCON 2014」は、国内だけでなく世界58ヵ国から4,000人を超える参加者を数え、世界的に見ても最大規模といえる大会に成長しました。

本年6月9日には「SECCON 2015」事業開始式を実施し、今年度のSECCON開催スケジュール発表や今年度の新たな取り組みである「サイバー甲子園」開催の説明を行いました。協賛企業、後援省庁からもメッセージをいただき、当日の様子はテレビをはじめ各種メディアで取り上げられました。「SECCON 2015」は、開催地域、競技の種類・内容ともにさらに向上させ、CTF入門者向けワークショップ「CTF for ビギナーズ 2015」、女性限定のワークショップも開催し、より多くの方が参加できる「ハッカー大会」の実施を目指します。

【開催概要】

【主催】

SECCON実行委員会(日本ネットワークセキュリティ協会)

【後援】

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

【参加対象者】

情報セキュリティ技術に興味のある学生、社会人(年齢不問)

【協賛企業の募集】

JNSAでは、このような取り組みを継続的に実施するために、関係省庁・組織から協力をいただくほか、民間企業から広く協賛を募り、SECCON 2015を運営します。

我が国における情報セキュリティ人材のすそ野の拡大、レベルアップを図り、グローバルにおいても第一線で活躍することのできる人材を輩出するという本活動の趣旨に賛同し、ご支援いただける協賛企業を募集しております。

スポンサーメニューをご用意しておりますので、詳細はJNSA事務局 <sec@jnsa.org> までお問い合わせください。

【開催スケジュール】

■ SECCON 2015

日程	開催大会	会場	内容
2015年8月26日(水)	SECCON 2015 横浜大会	パシフィコ横浜	CEDEC CHALLENGE
2015年10月24日(土)	SECCON 2015 広島大会	広島市立大学	熱血シェルコード
2015年11月7日(土)	SECCON 2015 福島大会	会津大学	サイバー甲子園 【18歳以下】／【学生限定】
2015年11月8日(日)	SECCON 2015 大阪大会	グランフロント大阪	CSIRT 演習
2015年11月28日(土)	SECCON 2015 九州大会	九州工業大学	Attack & Defense 【学生限定】
2015年12月5日(土) 2015年12月6日(日)	SECCON 2015 オンライン予選	インターネット	CTF 予選(日本語+英語)
2016年1月30日(土)	SECCON 2015 決勝大会 (intercollege)	東京電機大学	CTF 決勝戦(日本語)
2016年1月31日(日)	SECCON 2015 決勝大会 (international)	東京電機大学	CTF 決勝戦(英語)

■ CTF for ビギナーズ 2015

日程	開催大会	会場	内容
2015年6月7日(日)	CTF for ビギナーズ2015 博多	富士通株式会社	Attack & Defense 【学生限定】
2015年6月14日(日)	CTF for ビギナーズ2015 札幌	札幌市産業振興センター	Binary, Web, CTF
2015年7月4日(土)	CTF for ビギナーズ2015 東京	東京電機大学	Binary, Network, Web, CTF
2015年7月5日(日)	CTF for ビギナーズ2015 長野	株式会社電算	Binary, Network, Web, CTF
2015年9月12日(土)	CTF for ビギナーズ2015 熊本	東海大学	Network, Web, CTF
2015年10月3日(土)	CTF for ビギナーズ2015 滋賀	立命館大学	Binary, Network, CTF
2015年10月17日(土)	CTF for ビギナーズ2015 奈良	奈良先端科学技術大	Attack & Defense 【学生限定】
2015年11月7日(土)	CTF for ビギナーズ2015 大阪	大阪南港ATC	CTF in Kansai Open Forum

■ CTF for GIRLS 2015

日程	開催大会	会場	内容
2015年4月28日(火)	第3回 CTF for GIRLS	御茶ノ水ソラシティ	バイナリ分野 (ソフトウェア解析) 【女性限定】
2015年内に開催予定			

最新の開催状況については、「SECURITY CONTEST 2015」ホームページをご確認ください。

<http://2015.seccon.jp/>

主催セミナーのお知らせ

● JNSA設立15周年記念

「JNSAセキュリティセミナー」

主 催: NPO日本ネットワークセキュリティ協会

会 場:

鹿児島県 9/4(金) サンプラザ天文館6階Aホール

岡山県 9/28(月) 山陽新聞社本社9階大会議室

北海道 11/17(火) 札幌市民ホール

大阪府 11/26(木) 第二吉本ビルディング 貸会議室

沖縄県 12/17(木) 調整中

● 組織で働く人間による不正・事故は止められるのか?

内部不正対策14の論点」発売記念セミナー

主 催: NPO日本ネットワークセキュリティ協会

組織で働く人間が引き起こす不正・事故対応WG

日 程: 2015年9月9日(水)

会 場: コクヨホール(品川)

● マイナンバー対応情報セキュリティセミナー(仮)

主 催: NPO日本ネットワークセキュリティ協会

マイナンバー対応情報セキュリティ検討WG

日 程: 2015年10月5日(月)

会 場: 秋葉原UDX ギャラリーNEXT

● JNSA設立15周年記念シンポジウム

主 催: NPO日本ネットワークセキュリティ協会

日 程: 2015年10月15日(木)

会 場: ペルサール飯田橋駅前 ホールA

後援・協賛イベントのお知らせ

1. 第11回IPAひろげよう情報モラル

・セキュリティコンクール2015

主 催: 独立行政法人情報処理推進機構

日 程: 2015年4月1日(水)～11月30日(月)

作品募集期間:2015年4月1日(水)～9月7日(月)

2. 平成27年度 情報モラル啓発セミナー

主 催: 中小企業庁、各経済産業局、

公益財団法人ハイパーネットワーク社会研究所

会 場: 大分県 9/4(金) コンパルホール

千葉県 10/6(火) TKPガーデンシティ千葉

福島県 11/12(木) ザ・セレクトン福島

石川県 12/11(金) 北國新聞 20階ホール

兵庫県 1/14(木) 神戸コンベンションセンター

徳島県 2/2(火) 阿波観光ホテル

3. 価値創造で新たなステージへ

～未来をデザインするiコンピテンシディクショナリ～

主 催: 独立行政法人情報処理推進機構

日 程: 2015年9月15日(火)

会 場: 銀座ブロッサム 中央会館

4. ID & IT Management Conference 2015

主 催: ノーサレンダー株式会社

日 程: 2015年9月18日(金)

会 場: ANAインナーコンチネンタルホテル東京

5. Code Bali 2015

主 催: Code Bali運営事務局

日 程: 2015年9月21日(月)～23日(水)

会 場: Padma Hotel Legian, Bali

6. 情報セキュリティワークショップ in 越後湯沢2015

主 催: 特定非営利活動法人新潟情報セキュリティ協会、
情報セキュリティワークショップ in 越後湯沢
実行委員会

日 程: 2015年10月9日(金)～10日(土)

会 場: 湯沢町公民館、湯沢ニューオータニ

7. Email Security Conference 2015

ID Management Conference 2015

主 催: 株式会社ナノオプト・メディア

会 場: 東京 10/9(金) UDXカンファレンス

大阪 10/16(金) グランフロント大阪

8. CODE BLUE

主 催: CODE BLUE 実行委員会
日 程: 2015年10月28日(水)～29日(木)
会 場: ベルサール新宿グランド

9. Gartner Symposium/ ITxpo 2015

主 催: ガートナー・ジャパン株式会社
日 程: 2015年10月28日(水)～30日(金)
会 場: ホテル日航東京
(10月よりヒルトン東京お台場に名称変更)

10. ITGI Japan カンファレンス2015

主 催: 日本ITガバナンス協会
日 程: 2015年11月12日(木)
会 場: 大崎ブライツコアホール

11. Internet Week 2015

主 催: 一般社団法人日本ネットワークインフォメーションセンター
日 程: 2015年11月17日(火)～20日(金)
会 場: 富士ソフトアキバプラザ

12. かごしまITフェスタ2015

主 催: かごしまITフェスタ実行委員会
日 程: 2015年12月5日(土)～6日(日)
会 場: 鹿児島アリーナ

JNSA部会・WG2015年度活動

1. 社会活動部会

部会長: 丸山司郎 氏/株式会社ラック
副部会長: 西尾秀一 氏/株式会社NTTデータ

日本社会のサイバーセキュリティへの適応を推進するためメディア等を通じた情報発信や社会貢献活動、政府機関や海外組織との連携など、JNSAの社会的活動を推進する。

具体的には、JNSAとしての情報発信の後押し、パブコメ対応や行政との意見交換会、ワークショップ、勉強会や記者懇談会などの普及啓発活動、委託事業などの社会貢献活動、講師派遣などの外部組織支援、国際・他団体連携などを進める。

また、東京オリンピック・パラリンピックに向けたセキュリティ推進活動として、JNSA会員企業メンバーを中心とする業界横断の「JNSA-CERC(仮称)」の立ち上げも検討する。

【未来予測検討プロジェクト】

(リーダー: 唐沢勇輔 氏/ソースネクスト株式会社)

東京オリンピックを見据えた3～5年先の脅威予測を行ない、書籍などの成果物を通じて社会への啓発を図る。具体的な内容としては、下記を検討する。

- － 5年後のサイバー攻撃とは
- － 企業における情報セキュリティ対策
- － 家庭における情報セキュリティ対策
- － 脅威の技術動向など

＜予定成果物＞

- ・ 書籍「5年後の未来予測(仮)」の出版

【セキュリティ啓発WG】

(リーダー: 山田英史 氏/株式会社ディアイティ)

「インターネット安全教室」の内容検討や運営サポート、広報活動の検討などを行う。

【海外市場開拓WG】

(リーダー: 樋口健 氏/株式会社インフォセック)

日本国内のセキュリティ事業者による海外市場開拓を加速すべく、All Japan体制でノウハウの共有とコスト・リスクの分散を図る。

主な活動内容としては、3年程度を目安に下記を行っていく。

- ・ 先行して海外市場に進出している企業の事例調査
- ・ 共通課題の抽出と解決指針策定
- ・ 販路開拓、製品保守体制の整備、現地人材の採用、事業拠点の整備、活動資金の獲得、現地の規制/届出、法務契約面の対応など
- ・ 共同プロモーション活動の展開
- ・ 海外展示会への出展、メディアへの露出

・経済産業省など主管庁とのタイアップ

<予定成果物>

- ・海外進出企業の事例調査
- ・海外進出マニュアル

2.調査研究部会

部会長:加藤雅彦 氏/株式会社インターネットイニシアティブ

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NTTデータ)

個人情報漏えい編、発生確率編の調査を継続し、報告書を作成し公開する。2014年個人情報漏えい編の調査報告書を作成し公開する。2015年個人情報漏えいインシデントの調査を行う。

<予定成果物>

- ・2014年調査報告書
- ・2015年上半期調査報告書

【セキュリティ市場調査WG】

(リーダー:木城武康 氏/株式会社日立システムズ)

2004年度以来継続で行っている情報セキュリティ市場調査を、同じ仕組みで実施する。

<予定成果物>

- ・2015年度情報セキュリティ市場調査報告書

【IPv6セキュリティ検証WG】

(リーダー:許先明 氏/株式会社ブロードバンドタワー)

- ・IPv6固有のSecurity問題は存在するかの再検討
- ・IPv6環境におけるSecurity対策手段の再検討
 - －各種SecurityツールのIPv6対応状況の調査
 - －各種SecurityツールのIPv6環境への投入

<予定成果物>

- ・調査報告の実施

【スマートフォン活用セキュリティポリシーガイドライン策定WG】

(リーダー:栃沢直樹 氏/トレンドマイクロ株式会社)

従来のエンタープライズ向けのスマートフォン利用のみなら

ず、コンシューマ(個人)利用も視野に入れたスマートフォン利用にあたっての、リスクを踏まえた有効な活用方法の周知、また、スマートフォンと従来の端末(PCなど)との境界もなくなり始めていることから、位置付けについても改めて議論を行う。

<予定成果物>

- ・議論テーマに対する外部向けアウトプットの公開(予定)

【SaaSセキュリティWG】

(リーダー:長谷川長一 氏/株式会社ラック)

WG名称を「SNSセキュリティWG」から改称し、従来のテーマ(SNS)だけでなくパブリッククラウド(SaaS)のセキュリティを扱う。勉強目的の活動を実施し、原則として調査研究報告書等は作成しないが、集まった知見はNSF2016等で発表・公開する。

【組織で働く人間が引き起こす不正・事故対応WG】

(リーダー:甘利康文 氏/セコム株式会社)

以下の3方向から「組織で働く人間が引き起こす不正・事故」に対する考察を深め、ソリューションの提言、提案を行うことを目的とする。

- (1) 人の意識や組織文化、
- (2) 組織の行動が影響を受ける社会文化や規範、
- (3) 不正を防ぐシステム

<予定成果物>

- ・「組織で働く人間が引き起こす不正・事故」における「本質的に解決すべき課題」、「ベストプラクティス」事例の紹介など。
- ・セミナー等への積極的出講による啓発活動の展開。

【シンギュラリティ調査WG】

(リーダー:広口正之 氏/リコージャパン株式会社)

コンピュータの知性が人類を凌駕するというシンギュラリティ(技術的特異点)については、まだまだ日本における認知度が低いため、シンギュラリティに関する啓発活動を継続して実施する。

<予定成果物>

- ・シンギュラリティ調査報告書
- ・シンギュラリティ関連文献の出版

【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)

2020年東京オリンピック、パラリンピック開催時、インターネット接続されるIoT機器を安心・安全にするための啓発活動を行う。

今年度は、2014年度の調査結果のとりまとめから、2015年度以降実施すべきことを計画する予定。案として汎用デバイスをベースにした脆弱性の実験等。

＜予定成果物＞

- ・調査結果報告書

【脅威を持続的に研究するWG】

(リーダー:大森雅司 氏/株式会社日立システムズ)

- (1) 変化する顧客ニーズの分析整理とビジネスアプローチの検討
- (2) サイバー空間問題・安保外交政策・国内外市場動向の追跡調査
- (3) 高度標的型攻撃設計対策ガイドに関する技術策の検討
- (4) 重要インフラ・制御系・社会インフラ等分野に係る問題整理

＜予定成果物＞

上記活動を通じて得られた知見や問題点等をホワイトペーパーに纏めて、公開予定。

【マイナンバー対応情報セキュリティ検討WG】

(リーダー:萩原健太 氏/トレンドマイクロ株式会社)

本WGでは、サブWGに分かれて下記の活動を行い、企業のマイナンバー対応に間に合うよう9月末までに成果物を公開する。

- ・マイナンバー制度開始に向けたプロセスを整理し、企業がマイナンバー制度開始に向けた準備を行えるようにする
- ・マイナンバー制度に関する情報収集を行い、マイナンバー情報ポータル(仮)を作成する
- ・どのような対策をどこまでやればいいのか、組織的・人的・物理的・技術的セキュリティ対策を整理する。

＜予定成果物＞

- ・マイナンバー制度対応マニュアル(仮)

3.標準化部会

部会長:中尾康二 氏/KDDI株式会社

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

【アイデンティティ管理WG】

(リーダー:宮川晃一 氏/日本ビジネスシステムズ株式会社)

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

＜予定成果物＞

- ・「ロール管理 第3版」

- ・「書籍改定 改訂2版」

【国際化活動バックアップWG】

(リーダー:中尾康二 氏/KDDI株式会社)

国際標準化活動の情報共有を継続的に実施する。また、韓国KISIAとの共同フォーラムの開催を行い、韓国セキュリティベンダーグループとの連携を強化する。

【電子署名WG】

(リーダー:宮崎一哉 氏

/三菱電機株式会社 情報技術総合研究所)

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

＜予定成果物＞

- ・PDF署名(PAdES)プロファイル標準仕様ドラフト
- ・署名検証プロセスに関する標準仕様ドラフト
- ・経済産業省委託事業向け報告書

【PKI相互運用技術WG】

(リーダー:松本泰 氏/セコム株式会社)

IoT/M2M等の次世代インフラセキュリティの核となるべきPKIおよび暗号技術を念頭に、関係者の意見交流の場を提供し、PKI day等のイベントで情報発信を行っていく。

【セキュアプログラミングWG】

(リーダー:塩田英二 氏/TIS株式会社)

標準化活動に関して意見交換、情報共有を行う。

4.教育部会

部会長:平山敏弘 氏/日本アイ・ビー・エム株式会社

良質かつ社会のニーズに適合したセキュリティ人材の育成のため、必要とされる知識・技能等の検討を行い、実際の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や講師のデータベースを作成し、講師紹介サイトの公開、登録講師による講義・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。

【情報セキュリティ教育実証WG】

(リーダー:平山敏弘 氏/日本アイ・ビー・エム株式会社)

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

＜予定成果物＞

- ・情報セキュリティ講義コンテンツ

【情報セキュリティ講師人材DBWG】

(リーダー:長谷川長一 氏/株式会社ラック)

情報セキュリティ教育研究WGから名称変更。

JNSA教育部会メンバーの教える場とスキル向上の場を提供できるような企画や広報活動等を実施する。

まず第一弾の活動は、情報セキュリティ教育のコンテンツや講師のDBを作成する。

<予定成果物>

- ・ JNSA教育部会 講師紹介サイト

【セキユ女WG】

(リーダー:北澤麻理子 氏/ドコモ・システムズ株式会社)

IT・セキュリティキャリア女性活性化WGから名称変更。女性セキュリティエキスパートの交流場所を提供する(会社の枠を超えた連携を可能にする)、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勉強会や講演会を主催し、女性のIT・セキュリティスキル向上に貢献することを目的に活動を行う。

5.会員交流部会

部会長:小屋晋吾 氏/トレンドマイクロ株式会社

情報セキュリティ業界の健全な発展のために会員向けサービスを充実させ、業界の発展に貢献する。

具体的には、勉強会や製品紹介サイトの運営、各種ガイドラインと製品との関連付け、情報交換・情報発信などを行う。

【セキュリティ理解度チェックWG】

(リーダー:萩原健太 氏/トレンドマイクロ株式会社)

日本の情報セキュリティのリテラシー向上を目指し、「理解度セルフチェックサイト」、「情報セキュリティ理解度チェック」、「情報セキュリティ理解度チェック・プレミアム」の利用者増加のための活動を行う。

<予定成果物>

- ・ マイナンバーや個人情報保護法などを反映した問題作成

【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)

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

<予定成果物>

- ・ JNSA内の他部会/WGが作成した成果物とソリューションガイドとの連携
- ・ 関係諸団体が作成した各種ガイドラインとソリューションガイドの連携
- ・ 関係諸団体が有しているWeb内でのバナー掲載促進

【経営課題検討WG】

(リーダー:菅野泰彦 氏/

アルプスシステムインテグレーション株式会社)

中小企業における経営課題を調査・検討し、JNSA会員の事業を応援する。

<予定成果物>

- ・ 活動を通して分かった中小セキュリティ企業の経営課題のまとめ

6.西日本支部

支部長:嶋倉文裕 氏/富士通関西中部ネットテック株式会社

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

【企画・運営WG】

(リーダー:大財健治 氏/

株式会社ケーケーシー情報システム)

JNSA 会員および西日本地域のセキュリティレベルの向上を目指し、一般向けの公開セミナーに加えて、昨年に引き続き近畿経済産業局との連携を強化し、組込系の繋がるモノづくり・セキュリティセミナーを経営者向けに開催する。また地域のセキュリティレベル向上のため、関西で活動する団体の合同セミナーを年2〜3回実施すると共に、本部との合同セミナーも継続して積極的に開催していく。

【中小企業向け情報セキュリティポリシーサンプル作成WG】

(リーダー:嶋倉文裕 氏/

富士通関西中部ネットテック株式会社)

情報セキュリティポリシーサンプル0.92版を中小企業に対応するための整理。まずはスタンダード(雛形)を2015年秋をめどに作成する。レファレンスについては、雛形作成後を予定。

<予定成果物>

- ・ 中小企業向け情報セキュリティポリシーサンプル(雛形)

7.U40部会

部会長:長澤駿 氏/富士通エフ・アイ・ピー株式会社

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活動を行う。

【JNSAラボネットWG】

(リーダー:赤松孝彬 氏/株式会社ディアイティ)

- ・ JNSA内、ラボネットを利用した検証での環境の提供。
- ・ ラボネットを利用した技術検証の実施。

【勉強会企画検討WG】

(リーダー:唐沢勇輔 氏/ソースネクスト株式会社)

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。勉強会は講師からの講義だけでなく、グループディスカッションやライトニングトーク、ハンズオンを取り入れ、意見交換を活発化する。部会員以外のJNSA会員からも勉強会参加者を募り、部会員同士・JNSA会員・講師との人脈形成を行う。

8.情報セキュリティ教育事業者連絡会(ISEPA)

代表:与儀大輔 氏/NRIセキュアテクノロジーズ株式会社

今年度は、ISEPAとしての活動は休止。教育部会との連携を検討する。

9.日本セキュリティオペレーション事業者協議会(ISO-G-J)

代表:武智洋 氏/日本電気株式会社

セキュリティ診断士に関する検討として、診断士(Webアプリケーション)に必要な知識などの整理を継続する。また、情報セキュリティ小六法の改訂を行う他、一般向けセミナー、内部セミナーおよび勉強会等を適宜実施する。

＜予定成果物＞

- ・ セキュリティ診断士に向けての検討書等
- ・ IT関連法規のケーススタディ事例解説(セキュリティ小六法の強化・充実化)等
- ・ セミナー実施報告書(内部向け)

【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)

診断士資格の設立に向けて以下を行う。

- － 診断士(Webアプリケーション)資格の要項や必要な知識などの整理
- － 資格試験としての体制についての検討
- － 診断士(プラットフォーム)スキルマップの整備

＜予定成果物＞

セキュリティ診断士に向けての検討書等

【セキュリティオペレーション技術WG】

(リーダー:川口洋 氏/株式会社ラック)

セキュリティ技術の情報交換及びセミナーを各社持ち回りで実施予定。(1ヶ月～2ヶ月に1度)

【セキュリティオペレーション関連法調査WG】

(リーダー:川崎基夫 氏/JPCERT/CC)

月1回を目処としたWG定例会合を設ける。パブリックコメント窓口や講演会については適宜必要に応じて実施する。

＜予定成果物＞ 情報セキュリティ小六法(改訂版)

【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:井上博文 氏/日本アイ・ビー・エム株式会社)

月次定例WGの他、一般向けセミナーを2回(10月・2月)開催予定。また、8月に集中検討(合宿)を実施予定。

【標的型攻撃対策検討WG】

(リーダー:齋藤衛 氏/株式会社インターネットイニシアティブ)

オンラインおよびオフラインでの事案情報共有、勉強会等の実施(発生事案の状況によるが、年3～4回のWG開催を想定)。

10.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

今年度もJNSAインターンシップを実施する。9月には企業見学会を実施予定。

11.SECCON実行委員会

今年度も企業スポンサーを募り、「SECCON 2015」として全国的にセキュリティコンテストを実施予定。今年度は新たなカテゴリとして学校対抗の決勝大会も実施する。CTF初心者向けや女性限定のワークショップの開催にも注力する。

JNSA 役員一覧 2015 年 8 月現在

会 長 田中 英彦 情報セキュリティ大学院大学 学長
副会長 高橋 正和 日本マイクロソフト株式会社
副会長 中尾 康二 KDDI株式会社

理 事 (50音順)

荒川 賢一 エヌ・ティ・ティ・アドバンステクノロジー株式会社
遠藤 直樹 東芝ソリューション株式会社
大城 卓 新日鉄住金ソリューションズ株式会社
小椋 則樹 ユニアデックス株式会社
河内 清人 三菱電機株式会社情報技術総合研究所
後藤 和彦 株式会社大塚商会
小屋 晋吾 トレンドマイクロ株式会社
下村 正洋 株式会社ディアイティ
田井 祥雅 マカフィー株式会社
西尾 秀一 株式会社NTTデータ
西本 逸郎 株式会社ラック
藤伊 芳樹 大日本印刷株式会社
藤川 春久 セコムトラストシステムズ株式会社
水村 明博 EMCジャパン株式会社
三膳 孝通 株式会社インターネットイニシアティブ

幹 事 (50音順)

我妻 三佳 日本アイ・ビー・エム株式会社
安達 智雄 日本電気株式会社
岡庭 素之 キヤノンITソリューションズ株式会社
加藤 雅彦 株式会社インターネットイニシアティブ
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
工藤 雄大 大日本印刷株式会社
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
小屋 晋吾 トレンドマイクロ株式会社
佐藤 憲一 株式会社OSK
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
高木 経夫 ユニアデックス株式会社
高橋 正和 日本マイクロソフト株式会社
辻 秀典 ネットワンシステムズ株式会社
中尾 康二 KDDI株式会社
西本 逸郎 株式会社ラック
能勢 健一郎 東芝ソリューション株式会社

樋口 健 株式会社インフォセック
蛭間 久季 株式会社アーケン
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Kaspersky Labs Japan
本川 祐治 株式会社日立システムズ
森 直彦 エヌ・ティ・ティ・アドバンステクノロジー株式会社
油井 秀人 富士通エフ・アイ・ビー株式会社
与儀 大輔 NRIセキュアテクノロジーズ株式会社

監 事

土井 充 公認会計士 土井充事務所

顧 問

井上 陽一
今井 秀樹 東京大学 名誉教授
佐々木 良一 東京電機大学 教授
武藤 佳恭 慶應義塾大学 教授
前川 徹 サイバー大学 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
安田 浩 東京電機大学 教授
山口 英 奈良先端科学技術大学院大学 教授
大和 敏彦 日本ラドウェア株式会社
吉田 眞 東京大学 名誉教授

事務局長

下村 正洋 株式会社ディアイティ

【あ】

(株)アーク情報システム
 (株)アークン
 アイネット・システムズ(株)
 (株)アイビーキューブ **New**
 アイマトリックス(株)
 アカマイ・テクノロジーズ合同会社
 (株)アズジェント
 アドソル日進(株)
 (株)アビリティ
 (株)網屋 **New**
 アライドテレシス(株)
 アルテア・セキュリティ・コンサルティング
 (株)アルテミス
 アルプスシステムインテグレーション(株)
 EMCジャパン(株)
 (株)イーセクター
 イーロックジャパン(株)
 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
 インタセクト・コミュニケーションズ(株)
 (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
 ウェブルート(株)
 ウォッチガード・テクノロジー・ジャパン(株) **New**
 (株)AIR
 SCSK(株)
 (株)エス・シー・ラボ
 SGシステム(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ー(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)
 エヌ・ティ・ティ・ソフトウェア(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)FFRI
 (株)OSK
 (株)大塚商会

【か】

(株)Kaspersky Labs Japan
 キヤノンITソリューションズ(株)
 グローバルセキュリティエキスパート(株)
 クロストラスト(株)
 (株)ケーケーシー情報システム
 KDDI(株)
 KPMGコンサルティング(株) **New**
 (株)神戸デジタル・ラボ **New**
 (株)コムネットシステム
 (株)コンシスト

【さ】

(株)サイバーエージェント
 サイバーソリューション(株)
 (株)サイバード **New**
 サイボウズ(株) **New**
 (株)サーバーワークス **New**
 (株)JMCリスクソリューションズ
 ジェイズ・コミュニケーション(株)
 JPCERTコーディネーションセンター
 (株)GENUSION
 (株)シグマクシス
 シスコス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)信興テクノミスト
 新日鉄住金ソリューションズ(株)
 新日本有限責任監査法人
 セイコーソリューションズ(株)
 (株)セキュアソフト
 セキュリティ・エデュケーション・アライアンス・ジャパン
 SecureWorks Japan(株)
 セコム(株)
 セコムトラストシステムズ(株)
 総合警備保障(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
 損保ジャパン日本興亜リスクマネジメント(株)

【た】

大興電子通信(株)
 大日本印刷(株)

タレスジャパン(株)
TIS(株)
(株)ディアイティ
デジタルアーツ(株)
デロイトトーマツ リスクサービス(株)
(株)電通国際情報サービス
テンプスタッフ・テクノロジー(株) **New**
東芝ソリューション(株)
ドコモ・システムズ(株)
トレンドマイクロ(株)

【な】

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)
日本セーフネット(株)
日本電気(株)
日本電子計算(株)
日本電信電話(株)
日本ビジネスシステムズ(株)
日本ヒューレット・パッカード(株)
日本マイクロソフト(株)
日本ユニシス(株)
日本ラドウェア(株)
(株)ネクストジェン
ネットワンシステムズ(株)

【は】

パナソニック(株)
(株)日立システムズ
(株)日立ソリューションズ
飛天ジャパン(株)
(株)PFU
華為技術日本(株)
富士ゼロックス(株)
富士ゼロックス情報システム(株)
富士通(株)
富士通エフ・アイ・ピー(株)
富士通関西中部ネットテック(株)
(株)富士通ソーシャルサイエンスラボラトリ
(株)ブロードバンドタワー

【ま】

マカフィー(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・ソフトウェア(株)
(株)三菱総合研究所

三菱総研DCS(株)
三菱電機インフォメーションシステムズ(株)
三菱電機(株)情報技術総合研究所
三菱電機インフォメーションネットワーク(株)
(株)三宅
(株)メトロ

【や】

(株)ユービーセキュア
ユニアデックス(株)

【ら】

(株)ラック
(有)ラング・エッジ
リコージャパン(株)
(株)リンクトブレイン
(有)ロボック

【わ】

(株)ワイ・イー・シー
(株)ワイズ

【特別会員】

(ISC)2 Japan
一般社団法人 コンピュータソフトウェア協会
ジャパン データ ストレージ フォーラム
公益財団法人 ソフトピアジャパン
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
東京情報大学
東京大学大学院 工学系研究科
一般社団法人 IIOT
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
一般社団法人 日本スマートフォンセキュリティ協会 **New**
特定非営利活動法人 日本セキュリティ監査協会
一般財団法人 日本データ通信協会 タイムビジネス協議会

株式会社日立システムズ 大森 雅司



JNSA 会員の皆さま、こんにちは。

株式会社日立システムズの大森雅司(おおもり まさし)です。NTTソフトウェアの大森章充(おおもりたかみつ)さんより、「ぜひ、同じ岡山県出身で、大森繋がりで!」とご紹介いただきましたので、本コーナーの執筆を担当させていただきます。

私がセキュリティに関わるようになったのは、10数年前にセキュリティ部署に異動になったのがきっかけでした。入社当時は、ソフトウェア開発やシステム構築を行っていたのですが、次は「セキュリティでもやってみるか!」といった単純な気持ちでセキュリティの世界に飛び込みました。それから、色々と縁が開け、関西に一時転勤したり、火事場プロジェクトに投入されたり、政府機関に出向したりと、良くも悪くも貴重な経験をすることができました。今振り返ると、当時辛かったことでも今の自分の血となり肉となっているのだなと、しみじみと感じます。

現在社内では、新規セキュリティサービスの開発やグローバル関係の仕事をしています。お恥ずかしながら、英語が堪能な訳ではないので、毎回汗をかきながら会議に臨んでいます。つたない英語ながら、セキュリティに限らず、訪問した国の文化や日本への印象などについて話すのが楽しいです。

JNSA には、昨年10月から参加させていただいており、若輩ながら10月に発足した「脅威を持続的に研究するWG」のリーダーを務めさせていただいております。本WGは、サイバーセキュリティの脅威動向を従来のITだけの視点ではなく、法律、危機管理、安全保障等の複数視点で分析することで、問題の本質を見抜くことを目的としています。近年のサイバーセキュリティは、ITに閉じた世界ではなく、国際政治や危機管理、安全保障などの複数のドメインに跨った問題になっています。本質を見抜く為には、「様々なバックグラウンドを持った人を交えて意見交換をする」「現場に出向いて問題内容を肌で感じる」ことが重要と考え、WGで意見交換会や見学ツアーを企画しています。例えば、「IoT」や「制御セキュリティ」の問題も、実際の運用現場を見ることで、伝聞とは違った問題や発見があります。参加したいと思う方がいらっしゃいましたら、お声掛けください。

堅い話が続いてしまいましたが、最後に私の趣味をお話したいと思います。ずばり、私の趣味は“旅”です。これまで海外は20数か国と多く無い(?)ですが、国内は47都道府県を制覇しました。全都道府県制覇では飽き足らず、現在は離島巡りを続けています。多良間島、奥尻島、沖永良部島など、マイナーな島にも足を運んでいます。旅は、心をリフレッシュしてくれ、毎回新たな発見があります。仕事も私生活も、自分の目や耳で「見た」「聞いた」「感じた」経験は、かけがえのない人生の財産です。

こんな私ですが、頻繁に色々な場所に出没していますので、気楽にお声掛けいただければ幸いです。

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。）

富士通エフ・アイ・ピー株式会社 長澤 駿



JNSA 会員のみなさま、はじめまして。富士通エフ・アイ・ピー株式会社、長澤と申します。

この度、ソースネクスト唐沢様よりご紹介を受け、自己紹介させていただきます。

弊社はデータセンター機能を基盤とした ICT サービスを提供しております。その中で、データセンターにてお預かりするシステムのセキュリティ対策や、自社内のセキュリティ対策に日々取り組んでいます。

情報セキュリティに関わるようになったのは、入社後配属された部署（特に希望はしていない）がきっかけでした。大学では情報工学を専攻していましたが、セキュリティについての知識はほとんどありませんでした。

5 年ほどはシステムの脆弱性検査などを担当し、現在は社内ネットワーク監視・調査、社員のセキュリティ教育等のセキュリティ啓発などを担当しています。教育では、できるだけ専門用語を使わないことや、日常に例えた表現にするなど、まずはセキュリティ対策に興味を持ってもらうことを考え、活動しています。

JNSA との関わりは、新人時代上司に「JNSA で若手が集まる会ができればいいんだけど、行ってみない？」という誘いを受けたことがきっかけです。以来「U40 部会」に参加させていただいています。当初は初めて聞く言葉や技術にとまどっていましたが、いつの間にか「U40 部会」でも古株となり、現在は U40 部会長を担当しています。

「U40 部会」では若手の育成・人脈作りを目的に、「気軽に参加できる」をテーマに活動しています。私自身、まだまだ知らないことばかりで、毎回多くのことを学ばせていただいています。特に懇親会は、会社だけでは得られない貴重な情報交換の場となっています。話が白熱し、帰りが終電間際（笑）となることも。ここまでセキュリティに興味を持つことができたのも、JNSA での活動があったからこそと感じています。ご興味のある方や、自社の若手を参加させたい！と思っている方がいらっしゃいましたら、是非気軽にご参加（ご紹介）ください。

微力ではございますが、JNSA をはじめとしたセキュリティ業界の発展に貢献できるよう努力して参りますので、ご指導のほどよろしくお願いいたします。

JNSA 年間活動 (2015 年度)

4 月	4 月 7 日	第 1 回幹事会	2015 年 4 月から 2016 年 2 月 「インターネット安全教室」開催
	4 月 10 日	PKI Day 2015「サイバーセキュリティの要となる PKI を見直す」	
	4 月 28 日	第 3 回 CTF for GIRLS	
5 月	5 月 9 日	「産学情報セキュリティ人材交流会～インターンシップに向けて」	
	5 月 12 日	2015 年理事会	
6 月	6 月 7 日	CTF for ビギナーズ 2015 博多	
	6 月 9 日	JNSA 2014 年度活動報告会 / 2015 年度総会 (秋葉原 UDX)	
	6 月 14 日	CTF for ビギナーズ 2015 札幌	
	6 月 22 日	JNSA 臨時スキルアップ TF 実世界の暗号・認証技術に関する勉強会	
7 月	7 月 4 日	CTF for ビギナーズ 2015 東京	
	7 月 5 日	CTF for ビギナーズ 2015 長野	
	7 月 7 日	第 2 回幹事会	
	7 月 13 日	第 5 回日韓情報セキュリティシンポジウム (韓国ソウル)	
8 月	8 月 26 日	SECCON 2015 横浜大会	
	8 月 27 日	第 3 回幹事会	
9 月	9 月 4 日	JNSA セキュリティセミナー in 鹿児島 (サンプラザ天文館)	
	9 月 9 日	組織で働く人間による不正・事故は止められるのか? ～「内部不正対策 14 の論点」発売記念セミナー～ (コクヨホール)	
	9 月 12 日	CTF for ビギナーズ 2015 熊本	
	9 月 28 日	JNSA セキュリティフォーラム in 岡山 (山陽新聞社本社)	
10 月	10 月 3 日	CTF for ビギナーズ 2015 滋賀	
	10 月 5 日	マイナンバー対応情報セキュリティセミナー (仮)	
	10 月 15 日	JNSA 設立 15 周年記念シンポジウム (ベルサール飯田橋駅前ホール A)	
	10 月 17 日	CTF for ビギナーズ 2015 奈良	
	10 月 24 日	SECCON 2015 広島大会	
11 月	11 月 7 日	SECCON 2015 福島大会	2015 年 4 月から 2016 年 2 月 「インターネット安全教室」開催
		CTF for ビギナーズ 2015 大阪	
	11 月 8 日	SECCON 2015 大阪大会	
	11 月 17 日	JNSA セキュリティセミナー in 札幌 (札幌市民ホール)	
	11 月 26 日	JNSA セキュリティセミナー in 大阪 (第二吉本ビルディング 貸会議室)	
	11 月 28 日	SECCON 2015 九州大会	
12 月	12 月 5 日～6 日	SECCON 2015 オンライン予選 (日本語・英語)	
	12 月 17 日	JNSA セキュリティセミナー in 沖縄 (調整中)	
	12 月 18 日	第 4 回 CTF for GIRLS	
1 月	1 月 30 日	SECCON 2015 決勝大会 (intercollege)	
	1 月 31 日	SECCON 2015 決勝大会 (international)	
2 月			
3 月			

★ JNSA 年間スケジュールは、<http://www.jnsa.org/aboutus/schedule.html> に掲載しています。

★ JNSA 部会、WG の会合議事録は会員情報のページ <http://www.jnsa.org/member/index.html> に掲載しています。(JNSA 会員限定です)

JNSA について

■会員の特典

1. 各種部会、ワーキンググループへの参加
2. 会員勉強会への参加
3. CISSP・SANS 等教育の会員向け割引
4. 「JNSA ソリューションガイド」
(製品・サービス紹介サイト) への情報登録
5. 理解度チェック・プレミアムの販売 (代理店)
6. JNSA 会報の配布 (年 2 回予定)
7. メーリングリスト及び Web での情報提供
8. 活動成果の配布・報告書元データの提供 (会員限定)
9. イベント出展の際のパンフレット配布
10. 人的ネットワーク拡大の機会提供
11. 調査研究プロジェクトへの参画

お問い合わせ

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 3F

TEL: 03-3519-6440

TEL: 03-3519-6441

E-Mail: sec@jnsa.org

URL: <http://www.jnsa.org/>

西日本支部

〒532-0011 大阪府大阪市淀川区西中島 5-14-10

サムティ新大阪フロントビル (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.40

2015 年 9 月 18 日発行

©2015 Japan Network Security Association

発行所

特定非営利活動法人 日本ネットワークセキュリティ協会 (JNSA)

E-Mail: sec@jnsa.org URL: <http://www.jnsa.org/>

印刷

プリンテックス株式会社

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。

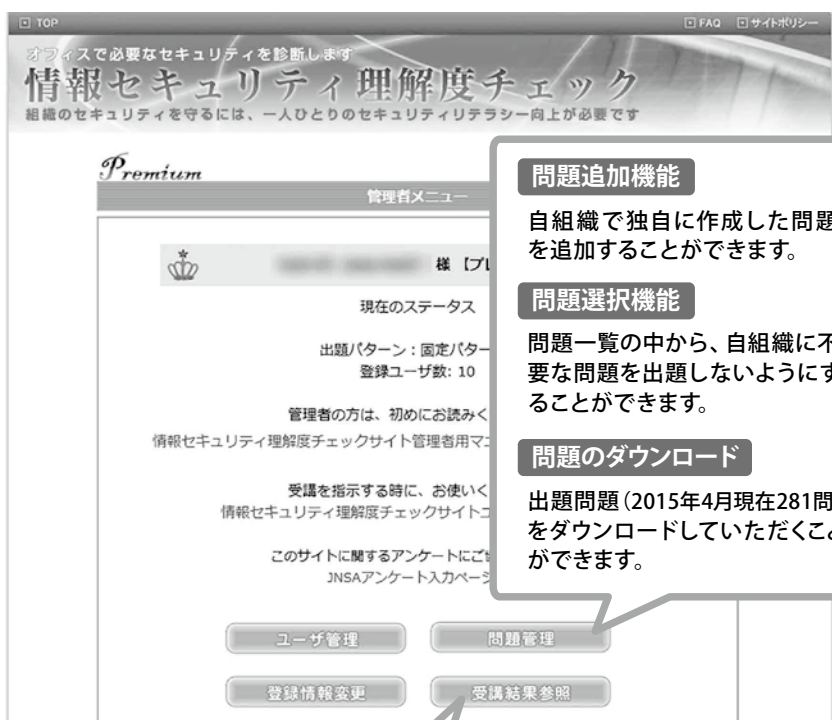
<料金の一例>

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题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。



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 3F
TEL 03-3519-6440 FAX 03-3519-6441
E-mail: sec@jnsa.org URL: <http://www.jnsa.org/>

西日本支部

〒532-0011 大阪府大阪市淀川区西中島5-14-10 サムティ新大阪フロントビル (株) デイアイティ内
TEL 06-6886-5540