JNSA PRESS
JAPAN NETWORK SECURITY ASSOCIATION
AUTUMN 2017 VOL.44

寄稿

トラストセキュリティの概要と最近の話題

02

内部犯行から企業の秘密情報を守るには。ますます重要となってきた出口対策

07

CONTENTS

特定非営利活動法人
日本ネットワークセキュリティ協会
NPO Japan Network Security Association

IT + IoT/OT セキュリティ

JNSA 理事
マカフィー株式会社
セールスエンジニアリング本部
本部長　櫻井　秀光

「使用しているOSやアプリケーションのセキュリティパッチは最新のものを適用出来ていますか？」という問いに対して、多くの方は、「それはセキュリティ対策のキホンの“キ”、当然出来ている」とお答えになるかも知れない。ただ、実状に関して不安にならざるを得ない事例が発生した。WannaCryとPetyaの大流行である。

PetyaはWannaCryと比較すると初期感染経路や感染手法が複雑なので、今回はWannaCryのケースをベースに話を進めていきたい。WannaCryは日本時間の5月12日（金）の夜に、ヨーロッパで感染が確認されてから瞬く間に世界中に感染を拡大した。現時点で感染している端末は全世界で50万台以上であると言われている。WannaCryの感染がここまで拡大したのは、これまでのランサムウェアとは異なり、自己増殖型のワーム型であったことに起因するが、感染拡大に利用されたのは、Microsoft製品に関する“既知”の脆弱性であった。Microsoft社は本脆弱性を修正するためのセキュリティパッチ（MS07-010）を日本時間の3月15日に公開しているので、セキュリティパッチを迅速に且つ適切に適用出来ていればWannaCryの感染は防げたことになる。

今回、セキュリティパッチを迅速に且つ適切に適用出来ていた故に被害を受けなかったケースも多くあるだろうが、気になるのは、WannaCryの感染がPCだけではなく、駅のデジタルサイネージや銀行ATM、さらには小売店舗の端末や工場の制御端末など、IoT（Internet of Things）やOT（Operation Technology、制御システム）機器に飛び火していた点である。「使用しているOSやアプリケーションのセキュリティパッチは最新のものを適用出来ていますか？」という文頭の問いに対して、IT機器であるパソコン等に関しては自信をもってYesと回答できるかもしれないが、自社にIoT/OT機器が存在する場合に、それらに関しても同じ回答となるであろうか。

今年の4月1日に「産業サイバーセキュリティセンター」が発足した。本センターにおいては、“ITとOT両方”のセキュリティ対策を推進していける人材を育成していく、という点が事業内容として明記されている。IT機器と比較するとIoT/OT機器に対するセキュリティ対策の実施度/成熟度は明らかに低い。ただ、IT機器と同じ対策をIoT/OT機器に対して実施すれば良いというほど簡単なものではなく、IoT/OT機器の特性を理解して、適切な対策を検討していく必要がある。2020年には、インターネットにつながる「モノ」（=IoT/OT機器）の数が500億個を超えると言われている。「IT + IoT/OT セキュリティ」対策の検討と実施の推進は待った無しの状況にある。

トラストセキュリティの概要と最近の話題

JNSA 電子署名 WG サブリーダー
有限会社ラング・エッジ
宮地　直人

1. はじめに

昨今では電子文書やデータのトラスト（信頼性）が問題になるケースが増え、「その文書が作成したのは誰なのか？またいつ存在していたのか？」と言う問いが新聞を賑わせている。これに対する1つの答えが、電子署名等の技術の利用である。

本稿では電子文書やデータの信頼性を守る電子署名のような技術を「トラストセキュリティ」と呼び、その概要と最近の関連トピックスを紹介する。なお「トラストセキュリティ」は造語であり一般的に使われ定義されている用語ではない。

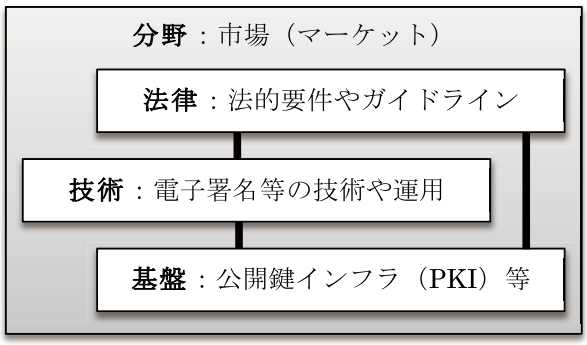
1.1. トラストセキュリティとは

電子文書等のコンテンツのセキュリティと言えば、暗号化やアクセス制御のようにコンテンツ自体を直接守る技術が一般的である。一方でコンテンツを第三者が閲覧する場合、そのコンテンツを誰がいつ作成し改ざんも無いと言うことを示す必要がある。この場合コンテンツ自体とは別に信頼性を守るセキュリティ、つまりトラストセキュリティが必要となる。

トラストセキュリティにおいて重要な点は「第三者」の存在と視点である。トラストセキュリティではトラストの証拠（エビデンス）を、第三者が検証できることが要求される。

2. トラストセキュリティの概要

トラストセキュリティは大きく分けて、「法律」「技術」「基盤」の3つの要素から構成される。これらの要素はターゲットとなる市場毎に要件が異なる。単純に技術だけの問題では無く、基盤と法律が絡むことが理解を難しくしている面があることは否めない。本稿ではトラストセキュリティの概要を要素毎に紹介する。



トラストセキュリティの構造図

2.1. 法律：法的要件やガイドライン

電子化以前において文書は紙として保存され、自筆署名や押印をすることで信頼性を担保していた。電子化された電子文書においては「電子署名」をすることで「紙の署名や押印と同等」と認める為の要件を定めた「電子署名法」やガイドラインを定めている国が多い。

◎ 日本

日本では「電子署名法」をはじめとして、「e文書法」「タイムビジネスに関わる指針」等の法律やガイドラインがある。ここではこれらの詳細は説明しないが、市場毎に関連する法律を確認することは必須と言える。日本では多くの法律においてPKIベースのデジタル署名（RSA署名等）が求められる。

◎ 欧州

欧州においては各国に電子署名法が存在しており、EUとして「電子署名指令」が定められていた。しかしより強い効力の「eIDAS規制」が施行された。適格な電子署名の法的有効性について手書き署名と同等と規定している。

eIDASはEUの「規制」である為に各国の電子署名法よりも強い拘束力を持つ。eIDAS規制では後述する「技術」や「基盤」についても明確に定義されており、現時点では最も整備されたトラストセキュリティと言える。欧州ではeIDAS規制に適合することで、電子署名

を利用した各国相互の電子取引が可能となっている。

Chapter III - Trust Services
Section 3 - Qualified trusted services
TSP:認証局やトラスト・リスト
Section 4 - Electronic Signatures
電子署名（XAdES/PAdES等）
Section 5 - Electronic seals
電子シール:組織や法人による電子署名
Section 6 - Electronic time stamps
電子タイムスタンプ

欧州eIDAS規制の電子署名関連部を抜粋

◎ **米国**

米国は欧州や日本とは少し事情が異なる。米国の電子署名法は「ESIGN Act」と呼ばれるもので、PKIベースのデジタル署名を要求しない。電子証拠（エビデンス）ベースの電子署名を認めている。既に多くのクラウド署名と言われるサービスがESIGN Actに準拠して使われている。

ESIGN Actでは細かい要件は求めておらず、必要に応じて証拠を提出する必要がある。具体的にはサービスの認証時や署名時の情報やログを保存し監査する運用が求められる。

なお米国においてもPKIベースのデジタル署名が求められる分野もあり、全てが非PKI電子署名と言う訳ではない。

Basic Requirements:
1. Intent to sign must be clear.
   署名する意図が明白でなければならない
2. The signature must be associated with the record.
   署名は記録と関係していなければならない
3. There must be clear consent to do business electronically.
   はっきりした電子取引の同意が必要
4. There must be access to records.
   記録へアクセスが可能でなければならない
5. No tampering of documents.
   文書の改ざんがされていないこと

米国ESIGN Actの基本要求

◎ **アジア**

アジアでは欧州eIDASのように国を跨り相互に有効な規制や法律を決める動きは無い。一方で中国や韓国においても電子署名やタイムスタンプは普及して来ており、アジア圏内における電子取引を活性化する為に今後相互運用についても検討されることを期待したい。

2.2. 技術：電子署名等の標準化技術

トラストセキュリティが第三者の検証を前提にしている以上、相互運用性の確保は必須となる。

日本と欧州は同じデジタル署名の技術を前提としていることから、10年以上前のECOM（次世代電子商取引推進協議会）の時代から共同して技術の標準化や相互運用性試験等を行ってきている。欧州ではETSI（欧州電気通信標準化機構）が電子署名技術の標準化を行ってきている。JNSAはETSIのアソシエート・メンバーであり、情報交換や仕様検討をおこなっている。

◎ **長期署名と検証**

「長期署名」は長期保管にも対応した電子署名の形式であるが、本来は「Advanced Electronic Signature」であり「先進署名」と呼ぶべき技術だ。例えばXML署名とXML長期署名のXAdESを比較すると以下の差異がある。

1. 署名証明書保護（XML署名ではオプション）
2. 署名タイムスタンプ：署名時刻を保証
3. 長期保管対応：検証可能期間の延長

1.と2.は長期保管しない場合でも有用な項目であり、XML署名よりもXAdESを通常利用すべきである。欧

州のeIDAS規制においても「適格署名」として長期署名形式が採用されている。XAdES以外にも、CMS形式のCAdESや、PDF形式のPAdES等がある。

長期署名は日本においても長期署名プロファイルとしてJIS化やISO化を推進してきた。しかしeIDAS規制では、欧州独自の長期署名仕様が標準化された。欧州の仕様は幾つかの点でJISプロファイルとは相容れない属性があり、今後別の道を進むのか歩み寄るのか検討が必要な状況にある。

また検証の標準化も課題である。署名自体は標準化されているが、検証手順に関しては決して明確になっていない。検証を標準化することで異なるベンダー間の相互運用が可能になる。

◎ 秘密鍵保管と利用

欧州のeIDAS規制では適格証明書と秘密鍵はSSCD（セキュア署名生成デバイス）に格納することが求められる。日本ではそこまでの要求はまだ無いが、SSCDに格納することが望ましい。

利用者の手元で利用するSSCDは、ICカードが最も一般的である。ICカードから秘密鍵を抜き出したり複製したりすることはできない。日本においてもマイナンバーカード（JPKI）やHPKIカード等で利用されている。

サーバーやクラウド側で使われるSSCDがHSM（ハードウェアセキュリティモジュール）である。最近ではクラウドHSMとして大量の利用者の秘密鍵を保管できるものが増えている。

◎ 電子認証

電子署名においてもサーバー連携して利用されるクラウド署名やリモート署名が使われはじめている。この時に重要となる技術が電子認証である。電子署名時には特に高い認証レベルが要求されることが多い。

欧州のeIDAS規制ではeIDとしてオンラインにおける公的個人認証のレベルも定義されている。日本では電子署名時の認証についてJNSAリモート署名TFにて検討と策定を進めている。

◎ 短期証明書（ワンタイム証明書）

電子署名時に短期間（1回）だけ有効な電子証明書と秘密鍵を発行し、署名後すぐ秘密鍵を破棄する電子署名の運用方法がある。署名時に必ず有効である為に「失効」の考え方を不要とできる利点がある。日本ではまだ事例は少なく標準化もされていないが、今後利用が進む可能性がある。

◎ 電子シール

電子シールは欧州のeIDAS規制で定義された利用方法であり、技術的には電子署名とほぼ同じであるが署名者が自然人では無く、法人や部署や組織である点が異なる。例えば電子領収書に用いられるが、コード署名も法人名の証明書で署名されるので電子シールの一種と言える。

日本においては法的な裏付けが無くまだ一般的では無いが、今後電子社会において必要性が高まることが予想される。

◎ 暗号スイート

現在電子署名で一般に使われている暗号アルゴリズムは、RSA-2048bitとSHA-2である。当面はこれで良いとしても次世代の暗号スイートとして、例えば量子コンピュータへの耐性を持つ、耐量子暗号の調査と検討は進めるべきである。

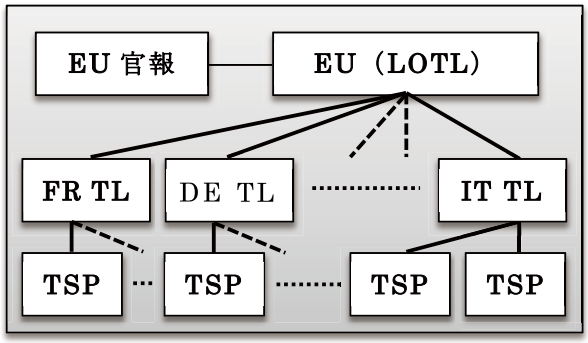
◎ 運用とエビデンス保管

特に米国ESIGN Actでは重視されるが、デジタル署名を行う場合であっても、運用ポリシーの策定とログ等の証拠の管理と保管は必須と言える。特にクラウド署名やリモート署名においてはサーバーが関与する為に運用や管理は特に重要となる。

2.3. 基盤：公開鍵インフラ（PKI）等

最後の要素は基盤である。日本と欧州ではPKIがベースになっている。PKIではルート証明書を頂点としたPKIドメインに分けられる。日本では公的なPKIドメインとしてGPKI・LGPKI・JPKI・商業登記・認定認証局があるが、これらはブリッジ認証局を介して並列的な構造で相互接続されている。

欧州のeIDAS規制ではトラストリスト（Trusted List）と言うツリー型の構造により登録各国のPKIドメインを相互接続している。まず国単位で認定された適格TSP（Trust Service Provider：認証局等）をまとめたトラストリストを作成、次にEUのEC証明書をトップとしたLOTL（リストオブトラストリスト）でトラストのツリー構造が作られる。既にAdobe Reader/Acrobatが対応している。

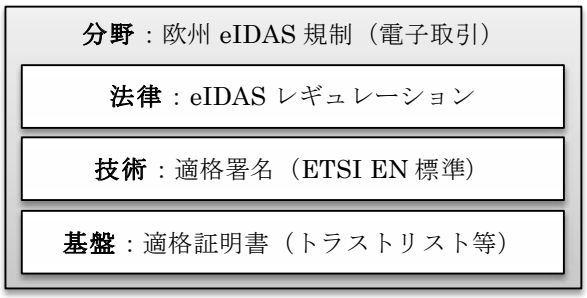


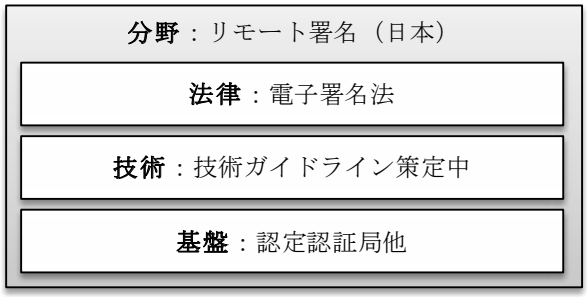
欧州eIDAS規制のトラストリスト

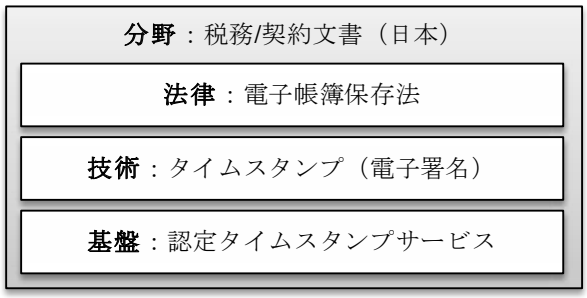
日本の基盤は国内に閉じており、海外との連携も検討が必要である。他に新たな基盤としてブロックチェーン利用の可能性もあるだろう。更にIoT時代にも対応したトラスト基盤も必要である。

3. トラストセキュリティ適用分野の分析

「法律」「技術」「基盤」をトラストセキュリティの適用分野（市場）毎に分析をした。







他にも色々な分野や市場があるが「法律」「技術」「基盤」がどうかと言う視点で見て頂きたい。

4. 最近の話題

4.1. マイナンバーカード（JPKI）

JPKIは住基カードからマイナンバーカードに変更となり、新たに認証用の利用者証明書が含まれた。これに

よりオンライン時の本人確認への道が開けた意義は大きい。例えば今秋正式開始予定のマイナポータルにおいてもマイナンバーカードを利用した認証や署名が可能となる。

マイナンバーカードの課題としては、個人情報となる4情報（氏名・性別・生年月日・住所）が含まれる署名用証明書の管理や、検証時の失効確認に申請と課金がかかる点がある。

オープンソースのICカードドライバであるOpenSCにて、マイナンバーカードへの対応が進んでいることも、新たな利用やサービスへの道を開く可能性があり期待される。

4.2. リモート署名とクラウド署名

欧州ではeIDAS規制対応のクラウド署名として、アドビシステムズ社が中心となりCSC（クラウド署名コンソーシアム）が設立された。CSCではAPIやプロトコルの技術仕様を標準化してクラウド署名の普及を目指している。

日本では2015～2016年度に、経済産業省の電子署名法研究会とJNSA電子署名WGメンバーが中心となり関係各団体が連携したリモート署名TFにてサーバーによる署名の技術仕様や運用ポリシーを検討してきた。2017年度は、これまでの検討結果をまとめた技術ガイドラインの公開を目標とし、新たにユーザー企業も加え、仮称JTSC（Japan Trusted Signature-service Consortium）の立ち上げを目指している。

4.3. 海外ベンダーや欧州ETSI/CENの動き

欧州のETSI/CENは日本や米国にeIDAS規制をベースにした相互運用を推進する為に動き出している。今年の3月8日には米国で「US Government and EU Workshop on Digital Signatures!」を、7月4日には日本で「日欧インターネットトラストシンポジウム」を開催している。また欧州のHSMベンダーや前述のCSCも春以降に相次いで担当者が来日してセミナーを開催している。

JNSAにおいてもリモート署名TFやJTSC（仮称）を中心に今後相互運用を含め対応していく予定である。

4.4. PDF/PAdESのISO標準

8年近くの歳月がかかったが、PDF 2.0であるISO 32000-2がやっと発行された。またJNSA電子署名WGの標準原案作成TFが参加してきたPAdESプロファイルISO 14533-3も発行段階をむかえている。ISOにおけるPDFの電子署名については基本的な仕様が出揃ったと言える。

4.5. 医療情報分野

電子処方箋の運用ガイドラインが2016年3月に厚生労働省より公開され、これをベースにJAHIS（一般社団法人保健医療福祉情報システム工業会）から2017年5月に「JAHIS電子処方せん実装ガイド Ver.1.0」が公開された。

医療情報では既にHPKIと言う基盤があり電子化が推進されている分野である。

5. おわりに（JNSA 電子署名 WG）

トラストセキュリティは今まさに色々な市場で必要とされ活況を呈してきている。eIDAS規制をベースに海外からも黒船が来ており日本としての対応も検討が必須となっている。

筆者としては若い技術者の皆さんにもトラストセキュリティの知識を持って頂きたいと考えている。本稿で示した通りクラウドへの展開も始まっており、地味かもしれないが新しい市場においてやりがいのある分野である。もしトラストセキュリティに興味があれば是非一度JNSAの電子署名WGに参加頂くか、勉強会も開いているのでそちらでも情報を得ることができる。JNSA電子署名WG実験サーバー（http://eswg.jnsa.org/）で勉強会の予定や各種情報を得ることができるので是非チェックや参加を検討して欲しい。

最後に、本稿の内容は、筆者の個人的見解であり、JNSA電子署名WGの見解ではない。内容に問題があれば筆者が全ての責を負うものである。

内部犯行から企業の秘密情報を守るには。ますます重要となってきた出口対策

ネットワンシステムズ株式会社
栗田 晴彦

1．初めに

本年 6 月に経済産業省から、「営業秘密の保護・活用について」という資料が公表されている。企業の情報資産を守るために「不正競争防止法」という法律があるが、その趣旨に沿って、保護すべき「営業秘密」の定義や、背景、体制、保護ガイドブックなどの説明がなされている。

最近は、サイバーセキュリティというと、標的型攻撃やランサムウェアといった言葉が話題になることが多いが、こと情報漏洩ということとなると、内部犯行の脅威は依然として非常に大きい。今までにも、ライバル会社への研究開発情報等の知的財産漏洩や個人情報漏洩・転売などの事件が、幾度となく発生してきてしまっており、度々ニュースにも取り上げられてきた。今後も、この脅威は増えることはあっても減ることはない。内部犯行対策に対してこれらの事件から学ぶべきことは今でも非常に多い。

内部不正に対する事例・調査やこのガイドブックに記載の対策内容を軸に、技術的な視点から企業における内部不正対策の考え方とポイント、特に出口対策の重要性について記述したい。

2．不正競争防止法が適用対象。「通常アクセス」による不正

本稿では、法律の詳しい説明・解釈をすることが趣旨ではないが、多くの内部犯行による情報漏洩事件で被告は「不正競争禁止法」で告発されている。この法律は、営業情報や設計情報などの企業の重要な知的財産を保護し、公正な競争と国際約束の的確な実施を確保するために 1993 年に作成されたものだ。

通常の、サイバー空間での不正アクセスや情報漏洩では、「不正アクセス禁止法」で訴えられるが、何故、それが適用されないのか？　その理由は、情報へのアクセス方法が「不正なアクセス」ではなく、業務上正当に与えられた「アクセス権限を濫用」して、情報漏洩を起こすということにある。

例えば、ハッキングなどで別な管理者の ID/PW を盗んで、それを悪用して顧客 DB にアクセスしたのであったら、不正アクセス禁止法で訴えられていたであろう。あるいは、不正なプログラムを作成してそれを動かし、情報を入手していたら同じく不正アクセス禁止法の対象となっていただろう。

内部犯行の典型的なパターンでは、システムの管理権限など正当に付与された権限を用いて情報を入手している。更に、日常の仕事の中で、それらを USB デバイスに書出す、メールに添付して送付するなど、持出をおこなっている。つまり、通常の業務遂行の一環で、「不正アクセス」せずとも情報の入手と持出しが可能であり、通常業務との見分けがつきにくいのが「内部犯行」の典型的であると言わざるを得ない。

様々な報告書を見てみると、以下の 3 つが共通する技術的な課題として挙げられている。

－過剰なアクセス権限の付与
－ログ取得やログ監視の漏れ
－ USB などの書出しの制御不足

以下では、これらの問題に対する対策を深堀したい。

3．秘密情報保護ハンドブック / 内部不正対策ガイドラインに見られるセキュリティ対策

内部不正に対抗し、企業の重要な情報を万全に守るためには、どうしたらよいのか?そのガイドとして以下の 2 つが挙げられる。

1.「秘密情報保護ハンドブック」（以下、保護ハンドブックと略称）：

2015 年 1 月の不正競争防止法の改正を受け、秘密情報を具体的にどのように守るかを示すために、2016 年 2 月に策定。

（経済産業省　秘密情報の保護ハンドブック）

http://www.meti.go.jp/policy/economy/chizai/chiteki/pdf/handbook/full.pdf

2.「組織における内部不正対策ガイドライン」：

IPA（独立行政法人　情報処理推進機構）が、度重なる内部犯行を受け、2013 年に作成。最新版は第 4 版（2017 年 1 月）。前述の保護ハンドブックでも、技術的な対策面では本ガイドラインを参照している。

（IPA　組織における内部不正対策ガイドライン）

https://www.ipa.go.jp/files/000057060.pdf

本稿では、この2つを参考としながら、技術的対策を考察したい。内部不正への技術的な対応は、大きく分けると下記の 3 つの対策カテゴリーに分類するとわかりやすい。

1．ＩＤ管理：必要な人が必要な情報・リソースにのみアクセスできることを保証する。認証と権限管理を含む
2．ログ管理：不正やその予兆を事前に検知し、インシデント発生時にはその影響範囲や内容をすぐに特定できる
3．出口対策：USB デバイス、印刷物や電子メール、Web アクセスなどでの情報の持出を防止する

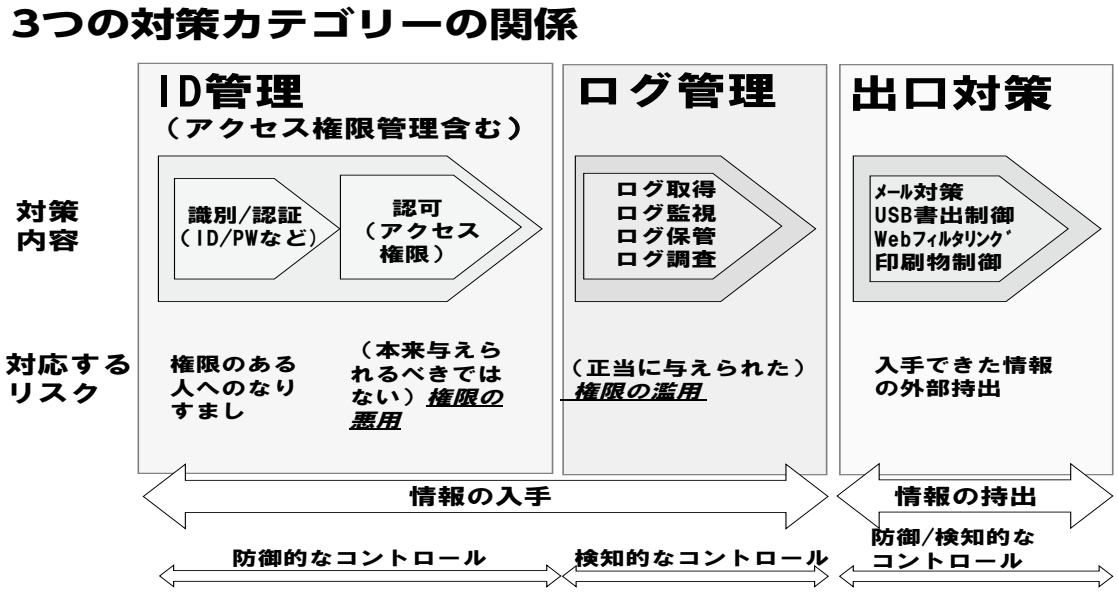


図 1：3 つの対策カテゴリーの関係

これらが、多層防御の考えでみられる「各層」を構成し、企業の秘密情報の外部への「不正な」漏洩リスクを低減する働きをしている。なお、これらの３対策カテゴリーは、図２で示す、保護ガイドブックでの５つの対策目的の最初の３つの技術的対策にほぼ対応している。

接近の制御⇒　　ＩＤ管理
持出し困難化⇒　出口対策
視認性の確保⇒　ログ管理

この３つを主軸で考えることで、大まかには対策はカバーできると考えてよいであろう。

図２：　秘密情報保護ハンドブック　の５つの「対策の目的」と３対策カテゴリーの関係

注：保護ハンドブックでの「対策の具体例」には、物理的対策も含まれているので、３対策カテゴリーとは必ずしも一致しない。また、接近の制御の例には、ネットワーク分離が含まれるが本稿では省いている。6. まとめの項を参照のこと。

4．ＩＤ管理やログ管理の限界

内部不正対策、あるいは内部統制を考えた場合、あるいはセキュリティ管理の基本を考えた場合、対策のベースは、ＩＤ管理とログ管理と言っても異論はないであろう。金融業界でのデータ保護のデファクトスタンダードである、PCI DSS や、個人情報保護法のガイドラインでも、ID 管理とログ管理は大項目で取り扱われているし、最近 IoT(あるいは、IIoT）で話題となっている制御系システムに対する基準の IEC62443-1-1 でも、7 つの基本要求のうちの 3 つが、この分野である。

ただし、内部不正対策として現実の業務への適用を検討してみると、以下の限界が見えてくる。

＜ID管理の限界＞

認証強化：そもそも、正当な本人がアクセスするので、どれだけ認証を強化しても意味がない。

権限管理強化：必要最小限の権限に出来たとしても、そもそも情報へのアクセスを許すわけであるから、権限の濫用は防ぎようがない。それを、防止するには、複数名に権限を細分化するなどがあるが、業務プロセスの変更を伴い、業務効率が落ちる。

権限管理強化の限界の良い例は、運用管理者の特権がある。特権は与えない方がよいが、どうしても必要な業務がある。特権を与えた場合の濫用を防ぐために、権限を分けての 2 名体制での作業などがよく取られるが、夜間や緊急時などどうしても 1 名での作業を認めざるを得ないのが現状である。

ID 管理の限界、つまり権限の濫用を防ぐことに限界があるので、通常はその部分をログ管理（特にログ監視）でカバーするという考えとなるが、残念ながらそれにも大きな障壁が存在する。

＜ログ管理の限界＞

ログ監視：不正と思われるアクセスパターンを考え、そのクライテリアでアラートを出すのが通例であるが、誤報がほとんどで有効な監視となりにくい。

内部不正対策で、よくログ監視の閾値に挙げられるのが、「大量のダウンロードや印刷」、「休日や夜間などのアクセス」、「退職予定者の秘密情報へのアクセス」などである。ただし、それを行ったから必ずしも不正行為という訳ではなく、正当な目的でアクセスする場合がほとんどである。そもそも、最小権限の考え方に沿えば、アクセス出来るということは、その行為（「例えば休日や夜間のアクセス」）が認められていることなので、それが不正かどうかの判断は困難を極める。休日や夜間のアクセスが問題なら、そもそも権限をなくしアクセスを禁止する方が最小権限の考えに沿っているのだ。

また、誤報か不正かどうかの最後の判断は、セキュリティ部門では困難でありその利用者部門でせざるを得ず、大量の誤報が出てしまうので、そのチェックが形式的にならざるを得ない。

この点で、標的型攻撃やマルウェアなどの外的脅威を、IDS 等のセキュリティ監視システムで監視するモデル（ＳＯＣ等）とは、同じログ監視とはいっても本質が異なることを留意すべきである。外的脅威は、攻撃のパターン化がしやすく、明らかに通常アクセスとは異なる振る舞いがある。そのため、（最近は高度な攻撃も多いが）まだ監視がしやすく、実際に多くの標的型攻撃では監視システムにひっかかっている。

＜内部不正では、検知より抑止を＞

図 1 では、ログ管理を技術的対策である「検知策」としているが、面白いことに、図 2 の保護ハンドブックでは、ＩＤ管理（接近の制御）や出口対策（持出困難化）を「物理的･技術的な防御」とまとめているのに対し、ログ管理は、

「心理的な抑止」の一項目としている。内部犯行対策に関しては、ログ管理へはこのぐらいの思い切りが重要と考える。権限の濫用に伴う内部不正に対するログ監視は、非常に困難であるうえ、それで発見されたケースは非常に少ない。よって、無理に発見することだけを目指すのではなく、「ログを取得し監視されているのだ」という抑止効果を狙うのである。こう考えれば、「いくら頑張って監視しても結局内部不正は見つからない。監視は意味がない、やめてしまえ」という圧力に対抗できる。

コンサルティングで関わったあるお客様では、「不正の発見」ということをあきらめ、抑止効果を中心に考えているところがあった。例えば、大量のファイルアクセス上位 30 名を社内に Web 公表する、不定期に部門を選び出し、その部門員のアクセスを徹底的にチェックするなど、監視していることを「情宣」することで不正のやる気をそぐ方法だ。

5．出口対策の重要性

ID 管理やログ管理でも十分コントロールできない情報漏洩リスクを、最後に「水際で」制御するのが、出口対策であり、近年、重要性がさらに強調されている。

IPA の「内部不正による情報セキュリティインシデント実態調査　－調査報告書－（2016 年 3 月）」の中に、出口対策の考察に重要な 2 つのデータがあるので紹介したい。

表 1　効果的だと思う対策の比較

内部不正経験者		対　策	経営者・システム管理者	
順位	割合		順位	割合
1位	50.0%	ネットワークの利用制限がある（メールの送受信先の制限、Web メールのアクセス制御、Web サイトの閲覧制限）	2位	30.0%
2位	46.5%	技術情報や顧客情報などの重要情報にアクセスした人が監視される（アクセスログの監視等を含む）	4位	27.0%
3位	43.0%	技術情報や顧客情報などの重要情報は特定の職員のみがアクセスできる	1位	43.9%
4位	25.0%	職務上の成果物を公開した場合の罰則規定を強化する	12位	12.8%
5位	23.5%	管理者を増員する等、社内の監視体制を強化する	11位	13.1%

調査報告書　P42 表 13 を転記

お分かりのように、内部不正経験者の答えた有効な対策上位 1 位～ 3 位が、それぞれ出口対策、ログ管理、ID 管理に該当している。内部不正を経験した本人の意見なので説得力があるが、やはり ID 管理やログ管理の対策の限界と、それに比べた出口対策の重要性を示す証拠と考えてよいだろう。

また、この調査報告書の P19 に、持出手段のランキングがあり、上位から USB メモリー(53.0%)、電子メール(28.9%)、

紙媒体（18.8%）となっており、それにHDD、Webアップロードなどが続いている。
今後のクラウドなどの外部ストレージやコラボレーションインフラの普及を考えると、外部記憶媒体、電子メール、Webアップロードの3種類が主な出口対策の対象と考えるが妥当であろう。

PCI DSS、個人情報保護法のガイドラインなどの今までの基準では、出口対策はほとんどカバーされることはないが、保護ハンドブックや、内部不正防止ガイドラインには、かなり具体的な記載が見られる。

＜「秘密情報の保護ハンドブック」に記載のある出口対策　（従業員等に向けた対策部分）＞

－社外へのメール送信・Webアクセスの制限
－電子データの暗号化による閲覧制限等
－遠隔操作によるデータの消去機能を有するPC・電子データの利用
－私物のUSBメモリーや情報機器、カメラ等の記憶媒体・撮影機器の業務利用・持込の制限

＜「内部不正対策ガイドライン」に記載のある出口対策＞

－私物の記憶媒体の持込制限、外部記憶媒体の利用制限ソフトウェアの導入
－ Webアクセスでのコンテンツフィルタリング
－電子メールでのメール送信再確認や上司の承認機能、添付ファイルの強制暗号
－リモートで情報機器内の重要情報を消去できるツールやサービス

これからは、内部不正に対する対策として、出口対策は必須の検討対象となったということであろう。

＜今後、主流となる、IRM、CASB＞

保護ハンドブックでは、出口対策「電子データの暗号化による閲覧制限等」の中で、「アクセス権を有するIDでログオンしたPCでのみ閲覧できる」 として、対策を具体例で記載している。これを実現できるソリューション、IRM (Information Right Management) が、最近注目を浴びており、幾つかのソリューションが出ている。
これを導入すれば、ログオンした人への閲覧制限のみならず、コピーや複製、転送の制限、更には漏洩後のデータの消去（暗号化鍵の権限制限）など遠隔操作でのデータ消去へも対応できる。
データ自身を暗号化するので、外部記憶媒体、メール、Webなどの流出経路に関係なく制御がかかるので、今後は、出口対策の決め手として、導入する企業が増えてくるであろう。10年前にあるお客様のコンサルティングでこのIRMの選定に関わったが、当時に較べてツールの完成度も高まっており、導入の敷居は確実に下がっている。
この場合は、残存するリスクとして、暗号化をし忘れる、あるいは暗号化するが権限設定を間違えるという事象を考える必要があり、フォルダーに入れると自動的に適切な権限で暗号化する、DLP（Data Loss Prevention）などと組み合わせて未暗号のものを探すなど、そのリスクを低減するためのソリューションも検討すべきであろう。
また、Webアクセスの多様化と高度化の動きを受け、出口対策の中にCASB（Cloud Access Security Broker）などが、含まれてくる時代も遠からず来ると考えており、すでにCASB、DLP、IRMなどの統合も生まれてきている。

6．まとめ

以上、内部犯行の事例・調査やガイドブック等をベースに、内部犯行に対する出口対策の重要性を述べてきた。この出口対策はお分かりのように、当然標的型攻撃を代表とする外部脅威への対策としても極めて有効である。乗っ取りなどを受けた端末からの情報持出を防ぐ最後の防波堤として機能するのである。

なお、本稿では、最近話題のネットワーク分離については触れなかったが、Web分離や、基幹ネットワークとOA ネットワークの分離などとしてよく検討されるこの対策も、「入口対策」と同時に「出口対策」としても有効である。これに関しては、紙面の都合で、割愛せざるを得なかったことをご了承いただきたい。

最近、セキュリティ対策として多層防御が当たり前に言われ始めたが、各々の層での防御の内容と目的が明確にされているとは言い難い。やみくもに防御を重ねても、実は大きなリスクへの検討が抜けている場合があり、効率的で効果的な対策とはならない。それぞれの対策で何が出来るかと同程度に、何が出来ないかを理解することも重要である。

本稿が皆様のセキュリティアーキテクチャ検討の一助となれば幸いである。

JNSA ワーキンググループ紹介

JNSA 標準化部会・アイデンティティ管理ワーキンググループ

アイデンティティ管理WG リーダー
日本電気株式会社　宮川　晃一

■ はじめに

本WGでは、アイデンティティ管理における様々な課題をWG討議の中で検討し、必要性の啓蒙および導入指針の提示による普及促進、市場活性化を目的に活動しています。

アイデンティティ管理はセキュリティの基本要素である、４Ａ（認証、認可、管理、監査）に深く関係しており、セキュリティポリシーを実装する上での共通基盤として非常に重要な分野です。また、最近は企業内のアイデンティティ管理だけではなく、クラウド環境やＩｏT、ビックデータ、ＡＩ等の活用においてもプライバシーデータの保護や流通時の課題を含めて、まだまだ検討すべきことがが多い状況です。

■ WGの沿革

本WGは、2005年に実施したBoFからスタートを開始し、今年で12年目を迎えることができました。WGを開始した当初は議論もまとまらず、方向性が定まりませんでした。しかしながら、当時IT関連の書籍を見回しても、ID管理に関する実務的な書籍が少なく圧倒的に情報が不足している状況でしたので、WGとして各社のノウハウ的な部分を取りまとめ解説書を作成することで意見が一致しました。これが後に書籍として出版することにつながり、大きな成果の1つとなっています。また、他にも「特権ID管理」や「ロール管理」、他団体とのコラボレーションによる成果物など継続的に外部発信ができていることを考えますと、本WGが果たしている役割は非常に大きいものがあるのではないかと自負しています。また、参加しているWGメンバー数も毎年増加傾向にあり、今年度は50人を突破いたしました。

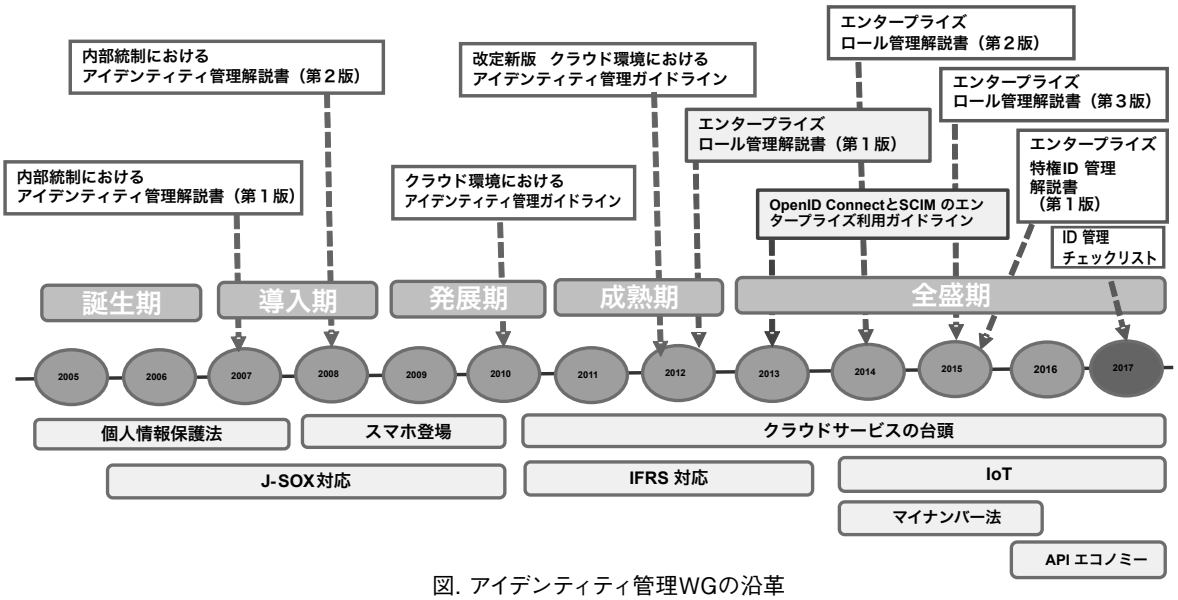


図. アイデンティティ管理WGの沿革

■ 最新の活動状況

2017年7月12日に「ID管理システム導入における現状把握チェックリスト（第1版）」を公開いたしました。
（http://www.jnsa.org/result/2017/std_idm/）

本書は企業内における「ID管理システム」導入時に課題となる「システム化の範囲」ついて、指標となるチェックリストを提示することで、各企業や団体がどの程度ID管理ができているのか、またどの部分が不足しているのかを定量的に知ることが可能となります。提案するSIer・ベンダにおいては、提案時におけるシステム化の範囲についての根拠とすることが可能となり、顧客との齟齬が発生しにくいメリットがあります。

導入を検討している企業や団体においては、システム化の範囲や予算についての精緻化をする助けになります。また監査人においては監査の補助資料としても使っていただけるのではないかと思っています。また、チェック項目数も対象システム数によって増加しますが最低35項目～となっていますので、気軽にお使いいただくことができるのではないかと思います。

チェックリストを使っていただく際は、まずチェックリストの目的や背景および利用方法をご一読いただき、ご理解の上ご使用していただければ幸いです。

図. ID管理システム導入における評価の実施（Excelシート）

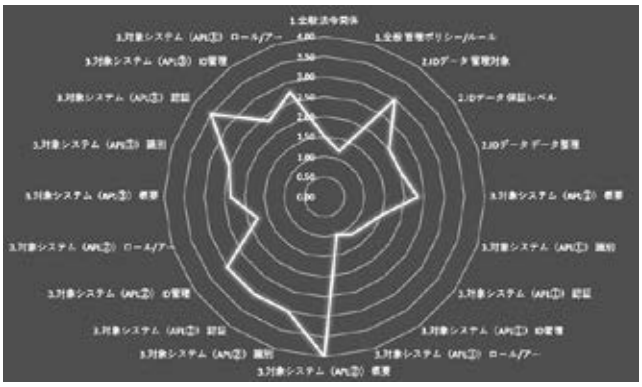


図. ID管理システム導入における現状把握度合（レーダーチャート）

■今後の活動について

現在、IoTやチャットボットにおける認証・認可やプライバシーの問題についての議論を行っています。ある程度議論がまとまるようでしたら成果物として取り組む予定にしています。また、今年度はWG独自のセミナーも企画中ですのでご期待いただければと思います。

最後に、WGメンバーの皆様および事務局の皆様、いつもWG運営にご協力いただきましてありがとうございます。紙面上をお借りしてお礼を申し上げます。引き続きどうぞよろしくお願いします。

JNSA ワーキンググループ紹介

WG討議の状況

■書籍のご案内

改訂新版クラウド環境におけるアイデンティティ管理ガイドライン
(インプレス R&D Security Series (NextPublishing))
http://amzn.asia/3AVI1Hx

メンバーリスト

■ リーダー

宮川　晃一 (日本電気株式会社)

■ メンバー (会社名順)

貞弘　崇行 (株式会社アイピーキューブ)
八束　啓文 (EMCジャパン株式会社)
齊藤　亘 (EMCジャパン株式会社)
篠原　信之 (イオンアイビス株式会社)
富士榮　尚寛 (伊藤忠テクノソリューションズ株式会社)
新嘉喜　康治 (伊藤忠テクノソリューションズ株式会社)
稲吉　英宗 (伊藤忠テクノソリューションズ株式会社)
木村　慎吾 (株式会社インテック)
深澤　聡 (SCSK株式会社)
金子　敬祐 (SCSK株式会社)
川嶋　亮平 (SCSK株式会社)
矢萩　雅広 (SCSK株式会社)
工藤　達雄 (NRIセキュアテクノロジーズ株式会社)
石井　晋也 (NRIセキュアテクノロジーズ株式会社)
内田　健一 (NECソリューションイノベータ株式会社)
長谷川　昌彦 (NECソリューションイノベータ株式会社)
山田　達司 (株式会社エヌ・ティ・ティ・データ)
星野　亮 (株式会社エヌ・ティ・ティ・データ)
杉村　耕司 (エヌ・ティ・ティ・データ先端技術株式会社)
久米田　博 (NTTテクノクロス株式会社)
荒井　正和 (エヌ・ティ・ティレゾナント株式会社)
齊藤　光司 (KPMGコンサルティング株式会社)
深谷　貴宣 (KPMGコンサルティング株式会社)
笠松　隆幸 (株式会社シグマクシス)
伊藤　栄二 (株式会社ディアイティ)
大森　潤 (有限責任監査法人トーマツ)
櫻田　仁詩 (有限責任監査法人トーマツ)
中垣　光生 (有限責任監査法人トーマツ)
栃沢　直樹 (トレンドマイクロ株式会社)
板倉　景子 (日本アイ・ビー・エム株式会社)
竹内　和弘 (日本アイ・ビー・エム株式会社)
酒井　美香 (日本アイ・ビー・エム システムズ・エンジニアリング株式会社)
市川　貴浩 (日本アイ・ビー・エム システムズ・エンジニアリング株式会社)
飯塚　昭 (日本オラクル株式会社)
木村　優一 (日本セーフネット株式会社)
吉嶋　正和 (株式会社日本総合研究所)

桑田　雅彦 (日本電気株式会社)
駒沢　健 (日本電信電話株式会社)
見上　昌成 (日本ビジネスシステムズ株式会社)
安納　順一 (日本マイクロソフト株式会社)
小野寺　匠 (日本マイクロソフト株式会社)
村田　裕昭 (日本マイクロソフト株式会社)
扇　健一 (株式会社日立ソリューションズ)
新井　雅 (富士通株式会社)
今堀　秀史 (富士通関西中部ネットテック株式会社)
福原　幸一 (富士通関西中部ネットテック株式会社)
恵美　玲央奈 (株式会社富士通ソーシアルサイエンスラボラトリ)
大村　夏都哉 (株式会社富士通ソーシアルサイエンスラボラトリ)
佐藤　公理 (マカフィー株式会社)
大久保　雄介 (ユニアデックス株式会社)
大竹　章裕 (株式会社ラック)
中井　恵子 (株式会社ラック)
中島　浩光 (サブスクライバ：株式会社マインド・トゥー・アクション)

■ 顧問

後藤　厚宏 先生 (情報セキュリティ大学院大学 学長・教授)

会員企業ご紹介44

NRI セキュアテクノロジーズ株式会社

http://www.nri-secure.co.jp

NRI SECURE TECHNOLOGIES

情報セキュリティのプロフェッショナル集団、NRIセキュアテクノロジーズ

NRIセキュアテクノロジーズは、野村総合研究所グループの情報セキュリティ専門企業です。国内外の関連資格を取得し、世界レベルでの研さんに励んできた専門家が、お客様の事業を支える高品質で的確なサービスを提供します。

NRI セキュアの3つの強み

1. 「経営」の視点から情報セキュリティ対策をサポート
   単品のコンサルティングやソリューションの提供にとどまらず、最高情報セキュリティ責任者（CISO）を補佐するパートナーとして、「経営目線」で情報セキュリティ施策の全体最適を支援。マネジメント面からもお客様の事業を支えます。
2. 国内外で政策提言などに携わり、情報セキュリティ業界をけん引
   国内外の情報セキュリティ関連の施策を検討する委員会への参画を通じて、制作や標準化のナビゲーションを実現。業界全体での情報セキュリティの最適化とコスト低減を推進しています。
3. 海外拠点を活かしてお客様のグローバル展開に対応
   NRI セキュアや NRI グループの海外拠点および海外の提携セキュリティベンダーを活用し、情報セキュリティサービスの 24 時間化を進めるとともに、お客様のグローバル展開の支援を行います。

お客様のサイバーセキュリティを攻守両面の技術で支援するスペシャリスト集団が、情報システムの安全性の評価や解析、堅牢なネットワークの設計・構築から24時間365日の高度な監視およびインシデント対応を行います。

運用管理サービス
- セキュアインターネット接続サービス
- セキュアWebネット管理サービス
- 標的型攻撃対策サービス
- エンドポイントセキュリティ
- セキュリティログ監視サービス ほか

テクニカル系コンサルテーション
- セキュリティ診断（Webサイト、基盤、データベース、スマートフォン、ソースコード、デバイス、車両システム、ブロックチェーン）
- セキュア設計評価
- Webサイト探索棚卸GR360
- サイバーアタックシミュレーション ほか

セキュリティ人材育成サービス
- SANSトレーニング
- (ISC)²関連レビュートレーニング
- TEAM Professor
- セキュアEggs研修 ほか

情報セキュリティのスペシャリストが、世の中のセキュリティ環境や法制度・各種ガイドラインの整備状況を踏まえ、お客様のセキュリティ課題の解決に最適なソフトウエア製品やクラウドサービスをご提供します。

IDセキュリティソリューション
- SecureCube / Access Check
- Uni-ID ほか

ファイルセキュリティソリューション
- クリプト便
- POSTUB ほか

オフィスITセキュリティソリューション
- PC Check Cloud ほか

企業・組織などが直面している人や組織、情報システムなどのセキュリティにかかわる課題に対し、専門的な調査、報告、提言を行います。セキュリティ標準や規格への準拠・監査のためのコンサルティングのほか、多種多様なセキュリティ教育も実施しています。

システムマネジメント系コンサルテーション
- 情報セキュリティ監査、セキュリティリスク評価
- CISO支援
- 認証取得支援（PCI DSS、ISMS、ISO27001など）
- セキュリティ対策状況可視化サービス
- IoTセキュリティコンサルティングサービス ほか

3つの事業を柱に、総合的に情報セキュリティ課題を解決

情報セキュリティのスペシャリスト集団が、お客様のセキュリティに関するさまざまな課題の解決を総合的に支援します。3つの主要事業のシナジーにより、テクノロジーとマネジメントの両面から、お客様の信頼できるパートナーとして、情報セキュリティに関するあらゆる脅威に立ち向かいます。

資格取得者数 2017年8月1日現在

高度情報処理技術者: のべ458名
（うち情報セキュリティスペシャリスト 173名）
CISA（公認情報システム監査人）: 77名
CISM（公認情報セキュリティマネージャー）: 40名
CISSP（情報システム・セキュリティ・プロフェッショナル認定資格）: 37名
GIAC（Global Information Assurance Certification）: のべ156名

お問い合わせ

NRI セキュアテクノロジーズ株式会社
http://www.nri-secure.co.jp/
〒100-0004
東京都千代田区大手町1-7-2東京サンケイビル
【電話】03-6706-0622 【E-mail】info@nri-secure.co.jp

情報セキュリティ株式会社
https://isec.ne.jp/

情報セキュリティ株式会社（iSEC）は、情報セキュリティに特化して事業を展開している数少ない企業の一つです。同分野での豊富な専門知識と業務経験、充実したネットワーク、高い研究開発力を有しています。またそれらをもとに、顧客の予算や利用形態、他システムとの整合性などさまざまな要素を勘案し、「最適な提案」を導き出します。

さらに、技術革新のための研究を怠らず、日々移り変わるIT業界のトレンドや新手のサイバー攻撃に対応しています。2017年7月に「サイバーセキュリティ研究調査室」を新設したほか、サイバーセキュリティにおいて高い技術力を誇るイスラエル企業との業務提携を進めています。

【当社が提供するソリューション一覧】

1. セキュリティの提供

■システム要件定義・設計
セキュリティに関する知見を豊富に備えた技術者が、上流フェーズでのセキュリティ要件作成および設計をサポートします。

■セキュリティ導入開発
ビジネスを促進する快適なネットワーク設計やデータ設計、および次世代型ファイアウォール、IDS/IPS、WAF、マルウエア対策製品、フィルタリング製品などを組み合わせたシステム開発を行います。

2. 保守・運用

顧客のネットワーク環境や要件に応じた最適な運用をサポートします。24時間365日の監視により、トラブルの未然防止やインシデント発生時の迅速な対応が可能となります。自社開発のツールを用い、高品質で効率的なセキュリティ運用を心がけています。

3. 監視・防御

未知の脅威を検知するためのSIEM（Security Information and Event Management）やログ解析の研究に力を入れています。機器のログにとどまらず、ログイン・ログオフからわかる人間の動き、イベント等の環境要因を考慮した相関分析により、将来影響を与える可能性があるパターンを特定する研究を行っています。

4. 脅威分析

■マルウエア解析サービス
顧客が解析を希望するファイルを安全な受け渡し方法で受領し、解析。基本動作を確認してレポートを作成します。

■自動型脆弱性診断サービス
独自にツールを組み合わせ、プラットフォーム・ミドルウエア・アプリケーションのレベルを網羅する診断を行っています。

■手動型脆弱性診断サービス
顧客のウェブサイトの構造や設置場所、ポリシーに合わせた診断方法を判断し、適用します。また、報告書の提出や報告会の実施、是正に対するサポートから是正後の再診断まで、要望にあわせて対応しています。

5. 情報セキュリティマネジメントに対する助言と教育

■情報セキュリティ監査
「内部監査（助言型）」と「外部監査（保証型）コンピュータフォレンジック」の両面から、情報セキュリティマネジメントシステムの確立をサポートします。

■教育
講義形式、模擬訓練、e-learningなど、多彩なメニューからお客様のニーズに合った教育をお選びいただけます。

6. フォレンジック

「ネットワークフォレンジック」と「コンピュータフォレンジック」による調査結果をもとに、組織内部の不正行為や外部からの不正アクセスの法的証拠をつかむ手法を提案します。また、「証拠保全」「解析」「証拠提出」までの一連の手続きを過不足なく行うための仕組み作りをサポートします。

お問い合わせ

情報セキュリティ株式会社　https://isec.ne.jp/
〒650-0012 神戸市中央区北長狭通4丁目9-26 西北神ビル3階
電話：078-381-8980　メール：general_info@isec.ne.jp

PwC サイバーサービス合同会社

http://www.pwc.com/jp/cyberservices

PwCサイバーサービス合同会社は、PwC Japanグループ(監査・アシュアランス、コンサルティング、ディールアドバイザリー、税務、法務など)においてサイバーセキュリティ・サービスを提供しています。サイバーセキュリティの専門家、研究者を多数擁しており、PwCグローバルネットワークと連携することで、国内外のサイバーセキュリティ動向に精通したサービスを提供しています。

MESSAGE

サイバーインシデント発生を前提とし、迅速に復旧するレジリエントセキュリティを提唱

従来、サイバー攻撃対策は、事故を発生させない対策に投資されてきました。しかし、守るだけで、100% 事故を防ぐことは不可能です。
そこで、防御策を実装すれば万全という固定概念を捨て、その防御策が破られる可能性を前提に準備と対策をすることが必要です。つまり、防御策に加え、抑止・検知・回復を、そしていざという時には迅速に復旧させるかにも注力して準備することが重要です。
“レジリエントセキュリティ”を提唱するPwC サイバーサービスは、組織がレジリエントセキュリティを実現するためのサポートをしています。

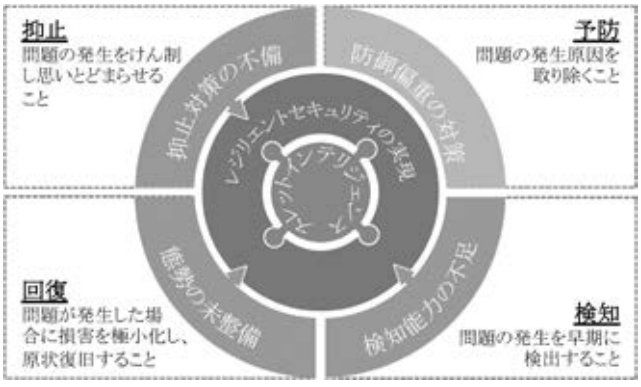
VALUE

グローバルに展開するプロフェッショナルの英知を結集したインテリジェンスの活用

PwC サイバーサービスでは、グローバルに展開するサイバーセキュリティのプロフェッショナルと連携し、セキュリティ対策の意思決定者が必要とするスレットインテリジェンスを収集、評価して、活用しています。
スレットインテリジェンスとは「脅威に対する意思決定を支援する、適切に分析・評価された情報」です。

SERVICES

スレットインテリジェンスをベースとしたサービス展開によりレジリエントセキュリティを実現



PwC サイバーサービスが提供するサイバーセキュリティサービスは、意思決定に必要な分析･評価した情報であるスレットインテリジェンスをベースとして組み込んでいます。
さらに、PwC グローバルネットワークと連携することで、国内外を問わず、収集・分析を行い蓄積された情報を活用しています。
そして、予測可能な攻撃の回避、被害の低減、素早い復旧を可能にするレジリエントセキュリティを実現しています。

お問合せ	PwC サイバーサービス合同会社 E-mail : JP_Cons_pcs.info@pwc.com　電話 : 03-3546-8430

株式会社プロット
https://www.plott.co.jp/

Create Next Communication
プロット

プロットは、1968年に創業し今年50周年を迎える、企業向けセキュリティ製品/サービスを開発･提供するセキュリティベンダーです。標的型攻撃による情報流出が大きな問題となっている昨今、各企業においては情報セキュリティ対策はもちろん、従業員教育の重要性が高まってきています。プロットでは、こうした脅威に対応する標的型攻撃対策用の製品/サービスを提供し、悪意ある攻撃から企業の機密情報を強固に守るお手伝いをしています。

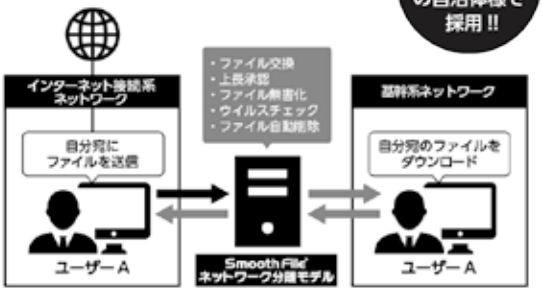
プロットの標的型攻撃対策ソリューション

分離ネットワーク間での ファイル交換

Smooth File® ネットワーク分離モデル

異なったネットワーク間でのファイルのやり取りを安全に行います。
ファイル交換時にファイル内のマクロスクリプトや埋め込みオブジェクトなどの危険因子を除去するファイル無害化を実施し、高いセキュリティを実現します。

全国150以上の自治体様で採用!!



ご確認ください **http://www.smoothfile.jp/separation/**

高い原本維持を実現した 高速ファイル無害化エンジン

Fast Sanitizer

外部からの悪意を高速で除去し、ゼロデイ攻撃などによる侵入を防御する国産のファイル無害化エンジン。
Microsoft Officeファイル、PDFファイル、画像ファイルから悪意を仕込まれやすいマクロスクリプトや埋め込みオブジェクトなどの危険因子を除去します。
APIでの提供により、既存のソリューションと組み合わせることも可能です。

5つの特徴

1. 高い原本維持性能
2. 高速な無害化処理
3. SMB（ファイル共有）機能内包
4. Active Directory連携
5. 純国産、実績多数のコアロジック採用

ご確認ください **http://www.fastsanitizer.jp/**

受信メールの無害化

TempBox® メール無害化モデル

メールの無害化を行うツール。標的型攻撃メールによる被害を様々な機能で未然に防ぎます。フィルタリング機能、メールの無害化、メールの二重配送機能といった機能で悪意あるメールを無害化します。
メール原本保持の為のメールアーカイブソリューションもご提供しています。

ご確認ください
http://www.tempbox.jp/outline/public_security.html

標的型攻撃メールの模擬訓練

CYAS

セキュリティ意識の向上を目的にした訓練クラウドサービス。標的型攻撃メールを模したメールを繰り返し配信することで警戒心を養います。テンプレートは100以上。訓練結果は自動的にレポート化され、管理画面からのダウンロードも可能です。

「ASPICクラウド・IoTアワード2016」において、ASP・SaaS部門「支援業務系グランプリ」を受賞

ASPIC クラウド・IoT アワード 2016

ご確認ください **http://www.cyas.jp/**

お問い合わせ： 株式会社プロット　フリーダイヤル 0120-40-2610
【大 阪 本 社】　〒530-0001　大阪市北区梅田3-3-20 明治安田生命大阪梅田ビル23F　TEL 06-6341-8360
【東 京 本 社】　〒108-0073　東京都港区三田3-11-36 三田日東ダイビル2F　TEL 03-5730-1400
【名古屋営業所】　〒460-0008　名古屋市中区栄1-3-3 AMMNATビル7F　TEL 052-228-6655

ISO9001：2008 認証取得　ISO27001：2013 認証取得

株式会社メトロ

http://www.metro.co.jp

技術と感動をつなぐ Metro

1971年の設立以来、ソフトウェア開発、ビジネスインテリジェンス（BI）、セキュリティの分野で、ノウハウの蓄積と最先端技術の導入による信頼性のきわめて高い利用技術、応用技術、サービスを提供しています。コンピュータの基本ソフトウェア開発・業務アプリケーションに関する請負、要員派遣、コンサルティング事業、情報処理システムのSIサービス、セキュリティソリューション提供、ETLツールを使用したデータ統合を中心としたビジネスインテリジェンス（BI）など、多様なサービスでお客様のニーズに応えています。

メトロのセキュリティソリューション

さまざまなセキュリティリスクに対応する最適な環境をご提案します

ネットワーク	サーバ	エンドポイント
UTM		
IPS/IDS（NW型）	ウイルス対策（ソフトウェア型）	
脆弱性診断		
DBセキュリティ	メール誤送信防止	
		HDD暗号化
		外部デバイス制御

メトロは技術力 No.1 の誇りを持っています

確かな技術力を背景に、熟練されたエンジニアから構成されたインテグレーション・サポート分野においては高い評価をいただいています。お客様が直面する問題を克服し、迅速かつ丁寧に対応、課題をすぐに理解し、素晴らしい価値を提供します。

セキュリティ 25 年以上の歴史から生まれる自信とメトロのブランド力

メトロがセキュリティビジネスを開始したのは、1991 年。まだセキュリティという言葉が世の中で重要視される以前に、ワンタイムパスワード製品の日本最初の総代理店となったことが始まりでした。1998 年にはそれまで 3 年間検証していた暗号化製品の日本語版の総代理店となるなど、セキュリティビジネスの先端を常に目指しながら 25 年以上の歴史を培ってきました。しかし、そこにはただ歴史があるだけではありません。お客様を第一に考える姿勢と、そのために必要となる製品知識や技術力がその背景として存在しています。

お問合せ	株式会社メトロ 〒108-0023　東京都港区芝浦4-6-8　住友不動産田町ファーストビル 9F TEL : 03-5484-1020　MAIL:marketing@metro.co.jp　WEB:http://www.metro.co.jp/

JNSA 会員企業のサービス・製品・イベント情報

■製品紹介■

○内部に潜む脅威を顕在化【Vectra® Networks】

日本でも導入が進んでいるVectra® Networksは社内のネットワークに接続するだけで自動且つリアルタイムに内部に潜む脅威を検出します。特徴は、サイバー攻撃の脅威レベルと精度をスコアリングし、インシデントハンドリングすべきホストを自動で優先順位付けし、教えてくれます。また継続モニタリングにより潜在リスクを丸裸にします。

【製品情報詳細】
https://contacts.nissho-ele.co.jp/vectra_catalog.html

◆お問い合わせ先◆
日商エレクトロニクス株式会社
ネットワーク&セキュリティ事業本部
TEL: 03-6272-5281
E-Mail: cyber_security@nissho-ele.co.jp

○統合セキュリティアプライアンス WatchGuard Fireboxシリーズ

WatchGuard Fireboxシリーズは、1Uラックマウントモデルから卓上モデル、仮想アプライアンスやAWS対応などラインアップが充実。
総合セキュリティパッケージTotal Security Suiteをご用意しており、標的型攻撃対策やエンドポイントでのランサムウェア検知・防御機能を含む、包括的なセキュリティ対策を1台のアプライアンスで実現し、最適なコストで多層防御を実現することができます。

【製品情報詳細】
https://www.watchguard.co.jp/

◆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）営業部
TEL: 03-5797-7205
E-Mail: jpnsales@watchguard.com

○Sophos Intercept X

Intercept X は、シグネチャーレス型のエンドポイントセキュリティ製品です。既存の他社製アンチウイルス対策製品と共存でき、セカンドオピニオンとして動作します。またウイルスの個体を検知するのではなく、エクスプロイト手法を検知するため、シグネチャーは不要です。ランサムウェア対策として、暗号化の開始と同時にファイルをバックアップするため、悪意ある暗号化と判断された場合自動的にファイルを復旧します。クラウド管理型の製品で、サーバーは不要です。

【製品情報詳細】
https://www.sophos.com/ja-jp/products/intercept-x.aspx

◆お問い合わせ先◆
ソフォス株式会社
営業部
TEL: 03-3568-7550
E-Mail: sales@sophos.co.jp

○SYMPROBUS Targeted Mail Training

SYMPROBUS Targeted Mail Trainingは、巧妙化する標的型攻撃メールに対する意識付けのトレーニングを実施する担当者様を強力にサポートする標的型攻撃メール対応の教育訓練ソリューションです。

◆主な機能
①疑似マルウェアや偽装URLをつかった訓練メールの送信
②開封状況やアンケート結果の自動収集
③アンケートページ、教育用コンテンツへの誘導

代理店様も随時募集しております。貴社やお客様先へのOEM等ご要望がございましたら、お気軽にお問い合わせください。

【製品情報詳細】
https://www.acmos.co.jp/service/detail60.html

◆お問い合わせ先◆
アクモス株式会社　セキュリティ営業部
TEL: 03-5217-3155
E-Mail: security_sales@acmos.jp

JNSA 会員企業情報

○TrustShelter/VA
「脆弱性管理に苦労してませんか?」

「公開された脆弱性の影響調査に時間がかかる。。」
「今日中に影響サーバの報告なんて無理。。」
「社内のとりまとめが大変。。」
そんな脆弱性管理の運用でお困りのすべての方に。
本サービスは公開された脆弱性情報とお客様サーバの構成情報を自動収集し、影響有無を瞬時に可視化。
クラウドサービスのため導入の手間も一切不要。
ぜひ一度、無償トライアルをお試しください。
もうExcelの運用には戻れなくなります!

【製品情報詳細】
https://www.ntt-tx.co.jp/products/trustshelter/va/

◆お問い合わせ先◆
ＮＴＴテクノクロス株式会社
クラウド&セキュリティ事業部
TEL: 045-212-7577
E-Mail: websecsol@cs.ntt-tx.co.jp

○WebALARM
「Web改竄被害増大!貴社は大丈夫ですか?」

サイバー攻撃にて、マルウェアを潜伏され、知らぬ間に有害サイトへの踏み台にされていたり、利用者へウィルスをまき散らしていたり、そんな脅威を5つの機能で完璧に防御します。専門要員は不要でサーバーへ導入いただくだけです。未知のマルウェアは、ウィルス対策ソフトや今までのセキュリティ対策では完全に防ぐことはできません。被害者（＝利用者にとっては加害者）になる前に是非導入を!

【製品情報詳細】
http://www.elock.co.jp/webalarm/solutions1.html

◆お問い合わせ先◆
イーロックジャパン株式会社
E-Mail: webalarm-support@elock.co.jp

■サービス紹介■

○マネージド・セキュリティ・サービス（MSS）

ネットワンのマネージド・セキュリティ・サービスは、お客様環境に設置された監視対象機器から出力されたログをセキュリティ分析基盤で24時間365日リアルタイムで分析し、セキュリティアナリストの知見を活かして重大なインシデントからお客様の情報資産を守ります。さらにネットワンのハードウェアサポートと連携することで、イベント検知から保守対応まで一貫したサービスをご利用いただけます。

【サービス情報詳細】
http://www.netone.co.jp/biz/service/securityservice-mss.html

◆お問い合わせ先◆
ネットワンシステムズ株式会社
市場開発本部セキュリティ戦略支援部
E-Mail: sec-senryaku@netone.co.jp

■イベント紹介■

○ウォッチガード ソリューションセミナー
～ランサムウェア対策・標的型攻撃対策～

6月に発生したPetya2.0などの悪質なランサムウェアに対し効果的なセキュリティ対策を行う上で必要なものは何か?是非セミナーへ参加してランサムウェア対策のヒントを入手しましょう。

日　時： 2017年9月8日（金） 15時開始
場　所： ウォッチガード セミナールーム
住　所： 東京都港区麻布台1-11-9 BPRプレイス神谷町 5階
費　用： 無料（先着20名） お申込み：以下URLより

【イベント情報詳細】
https://secure.watchguard.com/SM-09.08.2017-JAPAN-SEMINAR_Details.html

◆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
マーケティング部
TEL: 03-5797-7205　E-Mail: jpnsales@watchguard.com

「JNSA 全国横断セキュリティセミナー 2017」を開催

マーケティング部会では、JNSA会員勧誘と地域でのセキュリティ啓発を目的として、「JNSA 全国横断セキュリティセミナー 2017」を、全国５都市で開催しました。

福岡、名古屋、大阪、仙台、東京の５ヶ所で開催したこのセミナーは、午前の部は「SIer・セキュリティ事業者向け」、午後の部は「一般企業向け」と内容を変えて実施しました。

今年度初めて企画したこの全国横断セミナーですが、午前・午後合わせて全国で約500名と多くの方が参加され、各会場では熱心に聴講いただき多くの質問がなされるなど、好評のうちに終了いたしました。

そして午前の部ではJNSA入会のメリットを理解してもらい早速２社に入会をいただきました。さらに、午後の部ではあらためて昨今のセキュリティ事情を認識していただき、更なる対策の向上に意識が高まった様子でした。

今回のセミナーは、次の三点を企画意図として開催いたしました。

1. 政府のセキュリティ対策の支援施策の紹介
2. 全国各地域でJNSAの有益な活動のお知らせ
3. JNSAからのメッセージ発信(セキュリティ事業者への入会勧誘、一般企業へのセキュリティ啓発)

午前の部では、国内の施策や政府による補助金制度などのお客様への有益な情報や、ユーザー企業への提案に役立つ情報、さらにはJNSAに加盟することで得られるメリットについて具体的に紹介しました。

そして午後の部では、企業経営に役立つであろう国内の情報セキュリティに関する補助金制度などの政府施策と、「中小企業の情報セキュリティ対策ガイドライン」の活用方法や事例を基にした具体的な対策を紹介しました。

政府支援施策の内容紹介については、今回のセミナーで始めて知った方が多く、講演後の質疑応答で「どこでこのような情報を得られるのか」「詳細について教えてほしい」などの質問が相次ぎ、参加者の高い関心が伺えました。

SIerやセキュリティ事業者としては、セキュリティビジネスにおける課題を各参加者それぞれが持たれており、特に顧客企業の経営者に対して費用対効果を含めた提案に苦慮している企業が多く、経営層への理解を得ることの難しさが改めて浮き彫りになりました。さらにはビジネスをする上での人材育成、要員研修で苦慮しているといった人材面での不足感も顕著でした。

また、一般企業の方の状況は、セキュリティ対策の進捗に各社間の差異があり、その違いがアンケートのコメントに表れていました。特にこれから本格的に対策を行う企業にとっては、「事例が具体的、かつリスク洗い出し、ポリシー作成など手順がわかり大変参考になった」というコメントも多くあり、有益な内容であったといえます。

最後に、今回は東京含め５都市で開催し、各地域での開催要望は多かったものの、参加者数についてはもう一息といった感はぬぐえません。告知・集客での工夫が必要と感じますが、定期的にこのようなセミナーを行うことで、地域所在のセキュリティ事業者のJNSAへの入会も増え、それをきっかけにユーザー企業のセキュリティ対策向上及びセキュリティ事業者のビジネスの成長に貢献していくと考えています。

イベント開催の報告

【セミナー概要】

◆**名　称**: JNSA 全国横断セキュリティセミナー 2017

◆**主　催**: NPO日本ネットワークセキュリティ協会(JNSA)

◆**後　援**: 経済産業省、一般社団法人中部産業連盟(名古屋会場)

◆**協　賛**: (午後の部)
EMCジャパン株式会社(RSA)、アイマトリックス株式会社、アドソル日進株式会社、
アルプス システム インテグレーション株式会社、イーロックジャパン株式会社、
ウォッチガード･テクノロジー･ジャパン株式会社、株式会社カスペルスキー、ソフォス株式会社、
株式会社宝情報、株式会社ディアイティ、デジタルアーツ株式会社、トレンドマイクロ株式会社、
株式会社プロット　　*五十音順

◆**料　金**: 無　料

◆**対象者**: 【午前の部】セキュリティビジネスをされている、またはこれから参入される企業の方
【午後の部】セキュリティ対策を導入されている、または検討されている企業の方

◆**会場別参加者数**

会場	開催日	参加者数(単位:名)	
		午前	午後
福岡	2017年6月8日(木)	22	49
名古屋	2017年6月26日(月)	28	38
大阪	2017年6月27日(火)	48	61
仙台	2017年7月13日(木)	25	36
東京	2017年7月20日(木)	82	98
参加者数合計		205	282

[会場風景]

INTERPOL World 2017 JAPAN パビリオン出展 & JAPAN ネットワーキングイベント レポート

JNSA海外市場開拓WGに参加する会員企業10社は2017年7月5日（水）から7日（金）にかけてシンガポールで行なわれた「INTERPOL World 2017」に出展いたしました。

展示会では各社がそれぞれ趣向を凝らしたブースを構え、JAPANパビリオンには目標の500名を超える約1,000名（重複含む）もの来場があり、その関心の高さがうかがえました。

また、初の試みとして「JAPANネットワーキングイベント」と題した商談会を開催し、約140名のお客様が日本の文化や食事を楽しみながら出展企業と交流し、ビジネスのきっかけ作りをしました。

名　称　INTERPOL World 2017

会　場　Suntec Singapore Convention & Exhibition Centre

日　程　**◯展　示：**
- ●2017年7月5日（水）9：30 – 18：00
- ●2017年7月6日（木）9：30 – 18：00
- ●2017年7月7日（金）9：30 – 17：00

◯ネットワーキングイベント：
- ●2017年7月5日（水）17：00 – 19：30

概　要

INTERPOL World 2017には8,362名が参加。展示会には34カ国226社が出展し、日本を含む8カ国（日本、フランス、イスラエル、イタリア、韓国、シンガポール、スイス、米国）はそれぞれ各国のパビリオンを出展し、自国の企業を支援・アピールしていました。

今回のJAPANパビリオンのテーマを『縁』とし、漢字で『縁』とプリントした特製のうちわや企業紹介リーフレットの配布、そしてJNSA丸山理事がINTERPOL World TVの取材を受け、日本のセキュリティ業界の状況やJNSAの役割の紹介、JAPANパビリオンのアピールを行い、集客に努めました（取材の模様はYouTubeに公開されています）。また、各社の展示ブースでは、製品・サービスの紹介動画の活用や、兜の展示、また折鶴を配布する等、趣向をこらしていたのが印象的でした。その結果、JAPANパビリオンには3日間合計で約1,000名（重複含む）もの来場があり、今後に繋がる『縁』をつくれたと考えております。

また今回、初の試みとしてJAPANネットワーキングイベントを7月5日（水）に開催いたしました。本イベントでは、セキュリティと日本文化の融合を目指し、各社が1卓ずつテーブルを持ち、そこで料理や日本酒、日本のお菓子をふるまいながら商談するスタイルを採用いたしました。開会の挨拶ではINTERPOL 奥隆行 様にスピーチいただき、シンガポール日本人会 和太鼓同好会による太鼓のパフォーマンスや書家 田中紫花 様による書道パフォーマンス、最後のLucky Draw（くじ引き）までイベントは大盛況でした。当初、集客に苦戦すると考えておりましたが、最終的には140名以上の方が来場され、来場者は日本文化を体感、出展企業はビジネスのきっかけを掴むことができたと考えており

イベント開催の報告

ます。また、日本らしさをアピールするために男女共に浴衣を着て対応したメンバーが多く、和服文化に関心を持たれる来場者も多くいらっしゃいました。

今回、経済産業省及びジェトロの支援があり、JAPANパビリオンとして10社もの日本企業が海外展示会に出展することができました。出展成果についても目標の500件（名刺枚数など）を大きく上回る結果となりました。今回の『縁』から成功事例がうまれ、そのノウハウを会員企業が共有し、また新たな機会がうまれる、今後そのような好循環を創りだせればと考えております。加えて、現地での認知度・信頼を得るためにも、会員企業が継続して海外出展・アピール可能な仕組みを構築していくことが必要だと感じました。

展示会・ネットワーキング出展企業
株式会社網屋
株式会社インフォセック
NRIセキュアテクノロジーズ株式会社
株式会社FFRI
株式会社ディアイティ
日本企画株式会社
日本電気株式会社
株式会社日立システムズ
株式会社ユービーセキュア
株式会社ラック

ネットワーキング出展企業
トレンドマイクロ株式会社

協　力
書家・筆跡診断士 田中 紫花 様
シンガポール日本人会 和太鼓同好会

その他、JAPAN ネットワーキングイベントでは、カンファレンスの聴講でシンガポールにいらしていた沢山の方々にもご協力頂きました。本当にありがとうございました。

JNSA海外市場開拓WGでは、海外展示会への出展や海外市場調査、海外進出マニュアルの作成、メンバー企業間での情報共有などの活動を行なっています。現在海外進出を検討している企業様、また海外事業に関心のある方、既に海外ビジネスを展開しているが情報収集したい企業様など、ぜひお気軽にWGへご参加下さい。

2017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、2003年度から実施してきました。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（JNSA）

［共　　催］ 全国各地のNPO・団体・自治体・学校など

［協　　力］ 全国読売防犯協力会

［後　　援］ サイバーセキュリティ戦略本部、警察庁、その他各開催地大学・新聞各社・県・県警等（以上予定）等

インターネット安全教室とは？

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

会場では参加者全員に、ドラマやドキュメンタリーを通じて最新の情報セキュリティに対する脅威が学べる「映像知る情報セキュリティ」の最新版ＤＶＤのほか、スマートフォン利用に関するミニパンフレット、啓発チラシや家庭向けリーフレット「みんなで守って安全・安心8か条」「親子で守って安全・安心10か条」を配布し、情報セキュリティの向上にお役立ていただいております。

こんな方はぜひご連絡下さい

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

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

最新の開催状況については、「インターネット安全教室」ホームページをご確認ください。
https://www.ipa.go.jp/security/keihatsu/net-anzen.html

安全教室_2017年度開催スケジュール

（2017.8現在）

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

	日　程	開催地	共催団体	会　場
31	2017年9月2日	岩手	盛岡情報ビジネス専門学校【新規】	盛岡情報ビジネス専門学校　306教室
32	2017年9月8日	福島	JNSA	いわき明星大学
33	2017年9月8日	栃木	JNSA	金田南中学校体育館
34	2017年9月23日	三重	PCシェル	長島総合自動車学校
35	2017年10月2日	群馬	JNSA	みどり市商工会館
36	2017年10月4日	福岡	NPOスキルアップサービス	北九州市立年長者研修大学校 穴生学舎2階第2研修室
37	2017年10月5日	鳥取	特定非営利活動法人こども未来ネットワーク【新規】	とりぎん文化会館　第2会議室
38	2017年11月7日	神奈川	NPO情報セキュリティフォーラム	ヴェルクよこすか　6階　第1会議室
39	2017年11月8日	神奈川	NPO情報セキュリティフォーラム	おだわら市民交流センターUMECO 会議室5・6
40	2017年11月11日	宮城	特定非営利活動法人地域情報モラルネットワーク	東北工業大学一番町ロビー2F
41	2017年11月25日	山形	酒田市教育委員会【新規】	東北公益文科大学酒田キャンパス公益ホール
42	2017年12月12日	福岡	NPOスキルアップサービス	北九州市立年長者研修大学校 穴生学舎2階第2研修室
43	2018年2月16日	宮城	特定非営利活動法人地域情報モラルネットワーク	東北生活文化大学
44	2018年2月16日	神奈川	NPO情報セキュリティフォーラム	葉山町福祉文化会館　大ホール

SECURITY CONTEST (SECCON) 2017

SECCONとは、情報セキュリティをテーマに多様な競技を開催する情報セキュリティコンテストイベントです。実践的情報セキュリティ人材の発掘・ 育成、技術の実践の場の提供を目的として、2012年に始まりました。世界の情報セキュリティ分野で通用する実践的情報セキュリティ人材の発掘・育成を最終目標として、まずはICTに関わるすべての人材への情報セキュリティの考え方や知見を広めることでセキュリティ予備人材の裾野を広げ、さらにその中から世界に通用するセキュリティ人材を輩出し、よって日本の情報セキュリティレベルを世界トップレベルに引き上げることを目的として活動を行っています。

2017年1月に行われたSECCON 2016 決勝大会（国際大会）では、日本最大の「ハッカー大会」として、99ヶ国から累計4,349人が参加、決勝大会には日本から10チームとオンライン予選大会と連携大会を勝ち抜いた8ヶ国14チームが参加し、東京で世界レベルのハッキング対決が繰り広げられました。カンファレンスや企画展示などを同時開催し、3日間で1,000名を超える方の来場がありました。

【開催概要】

［主　催］SECCON実行委員会（特定非営利活動法人日本ネットワークセキュリティ協会）
［運　営］株式会社ナノ・オプトメディア
［後　援］

- 高度情報通信ネットワーク社会推進戦略本部
- サイバーセキュリティ戦略本部
- 警察庁
- 総務省
- 公安調査庁
- 外務省（2017年8月1日以降の開催大会に後援）
- 文部科学省
- 国立研究開発法人 情報通信研究機構（NICT）
- 独立行政法人 情報処理推進機構（IPA）
- 一般財団法人 日本情報経済社会推進協会（JIPDEC）
- 一般社団法人 日本経済団体連合会（経団連）
- OWASP Japan
- 日本シーサート協議会

[SECCON Beginners とは]

SECCON Beginners 2017は、コンピュータセキュリティ技術を競う競技であるCTF (Capture The Flag) の初心者を対象とした勉強会です。本勉強会では、CTFに必要な知識を学ぶ専門講義と実際に問題に挑戦してCTFを体験してもらう演習を行います。

[CTF for GIRLSとは]

CTF for GIRLSは、情報セキュリティ技術に興味がある女性を対象に、気軽に技術的な質問や何気ない悩みを話しあうことが出来るコミュニティを作る事を目的に立ち上げられました。コミュニティ形成の一環として女性同士で情報セキュリティ技術を教え合うCTFワークショップや、その他女性向けCTFイベントの開催を行っています。

[協賛企業の募集]

SECCONの運営は民間企業等からの協賛金により行っています。SECCONでは年間を通じてスポンサーを募集しておりますので、お気軽にお問合せ下さい。（SECCON運営事務局: info2017@seccon.jp）
2017年度スポンサー企業はSECCONホームページ（http://2017.seccon.jp/）をご覧下さい。

■SECCON2017 開催スケジュール

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

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

■SECCON Beginners 2017 開催スケジュール

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

■CTF for GIRLS 開催スケジュール

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

最新の開催状況については、「SECCON 2017」ホームページ(http://2017.seccon.jp/)をご確認ください。

事務局お知らせ
JNSA ANNOUNCE

後援・協賛イベントのお知らせ

1. iコンピテンシ ディクショナリ活用セミナー
主　催：特定非営利活動法人スキル標準ユーザー協会
日　程：2017年9月1日（金）から10月13日（金）
（全4日間）
会　場：仙台、大宮、岡山、京都

2. Security Days Fall 2017
Email Security Conference 2017
ID Management Conference 2017
主　催：株式会社ナノオプト・メディア
日　程：2017年9月26日(火)：大阪
2017年9月27日（水）から29日(金)：東京
会　場：【大阪】ナレッジキャピタル・カンファレンスルーム
【東京】JPタワーホール＆カンファレンス

3. 第16回 迷惑メール対策カンファレンス（大阪）
第17回 迷惑メール対策カンファレンス（東京）
主　催：一般財団法人インターネット協会
（IAjapan）
日　程：2017年9月26日（火）大阪
2017年9月29日（金）東京
会　場：（大阪）ナレッジキャピタル･カンファレンスルーム
（東京）JPタワーホール＆カンファレンス

4. 情報セキュリティワークショップ
in 越後湯沢2017
主　催：ＮＰＯ新潟情報セキュリティ協会
日　程：2017年10月6日（金）から10月7日（土）
会　場：湯沢町公民館、湯沢東映ホテル

5. Gartner Symposium/ITxpo 2017
主　催：ガートナージャパン株式会
日　程：2017年10月31日（月）から11月2日（水）
会　場：グランドプリンスホテル新高輪 国際館パミール

6. CODE BLUE
主　催：CODE BLUE実行委員会
日　程：2017年11月7日（火）から11月10日（金）
会　場：東京･新宿 ベルサール新宿グランド

7. ITGI Japan Conference 2017
主　催：日本IT ガバナンス協会
日　程：2017年11月13日（月）
会　場：東京コンファレンスセンター品川

8. Internet Week 2017
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：2017年11月28日（火）から12月1日（金）
会　場：ヒューリックホール&ヒューリックカンファレン

9. IPA中小企業情報セキュリティ講習能力養成セミナー
主　催：独立行政法人情報処理推進機構
期　間：2017年7月から2017年12月
会　場：全国30ヵ所

10. 第13回IPAひろげよう情報モラル・セキュリティコンクール 2017
主　催：独立行政法人情報処理推進機構
作品募集期間：
2017年6月1日(木) ～2018年3月31日(土)
会　場：独立行政法人情報処理推進機構

JNSA部会・WG2016年度活動

1. 社会活動部会

部会長：丸山司郎 氏／株式会社ベネッセインフォシェル
副部会長：唐沢勇輔 氏／ソースネクスト株式会社

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

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

【セキュリティ啓発WG】

（リーダー:山田英史 氏／株式会社ディアイティ）

独立行政法人情報処理推進機構（IPA）委託事業である「インターネット安全教室」 の内容検討や運営サポート、広報活動の検討などを行う。

【海外市場開拓WG】

（リーダー:一宮隆祐 氏／日本電気株式会社）

昨年度の活動を継続し、Made-in-Japanソリューションの拡販を実現する。

- APAC地域における統治代理店の開拓、商談発掘から受注までの実績を作る
- ・作成途中の海外市場に進出する上での手順や課題と解決策を纏めた「海外市場進出マニュアル」を纏める。

＜予定成果物＞

- 海外進出マニュアル

【CISO支援WG】

（リーダー:河野省二 氏／株式会社ディアイティ）

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

＜予定成果物＞

- CISOハンドブック

【JNSA CERC】

（リーダー：高橋正和 氏／日本マイクロソフト株式会社）

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

2. 調査研究部会

部会長：前田典彦 氏／株式会社カスペルスキー

情報セキュリティにおける各種の調査および研究活動を行う。セキュリティ被害、情報セキュリティ市場などの統計分析事業、および、重要度や緊急度の高いテーマに関する脅威分析、対策研究を推進する。適切な時期、形式を用いて適宜情報公開を行い、調査研究における成果を広く社会に還元する。新規性や緊急性の高いテーマの検討が必要となる場合においては、勉強会、BoFなどを随時行うなどして、柔軟かつ迅速な対応を行う。

【セキュリティ被害調査WG】

（リーダー:大谷尚通 氏／
株式会社エヌ・ティ・ティ・データ）

個人情報漏えいインシデント調査の長崎県立大学への移管を継続して実施し、調査体制を確立する。
長崎県立大学と共同で個人情報漏えいインシデント調査を実施し、報告書を公表する。

インシデント被害の定量化に向けて、まずは被害報告（報道や報告書）の標準化を検討する。

＜予定成果物＞

- 2015/2016年個人情報漏えいインシデント調査報告書
- 被害報告（報道や報告書）の標準化テンプレート

【セキュリティ市場調査WG】

（リーダー:木城武康 氏／株式会社日立システムズ）

国内で情報セキュリティに関するツール、サービス等の提供を事業として行っている事業者を対象として、推定市場規模データを算出し報告書として公開する。

＜予定成果物＞

- 2017年度情報セキュリティ市場調査報告書

【組織で働く人間が引き起こす不正･事故対応WG】

（リーダー:甘利康文 氏／セコム株式会社）

以下の3方向から「組織で働く人間が引き起こす不正・事故」に対する考察を深め、ベストプラクティスの紹介、提案、啓発を行うことを目的とする。2017年度は、昨年度に引き続き、特に（1）に重点をおいた活動を行う。

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

＜予定成果物＞

- 「組織文化醸成によるES向上」に向けた各組織の取組事例ヒアリング調査と、調査内容をベースとした記事の公開
- セミナー等への積極的出講による啓発活動の展開

【IoTセキュリティWG】

（リーダー:松岡正人 氏／株式会社カスペルスキー）

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

＜予定成果物＞

- セキュリティガイドの更新

【脅威を持続的に研究するWG】

（リーダー:大森雅司 氏／株式会社日立システムズ）

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

【マイナンバー対応情報セキュリティ検討WG】

（リーダー:萩原健太 氏／トレンドマイクロ株式会社）

マイナンバー関連の意見提出の取りまとめや定期的に勉強会を開催する。

3. 標準化部会

部会長：中尾康二 氏／ＫＤＤＩ株式会社
副部会長：松本泰 氏／セコム株式会社

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

【アイデンティティ管理WG】

（リーダー:宮川晃一 氏／日本電気株式会社）

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

＜成果物目的テーマ＞

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

＜勉強目的テーマ＞

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

＜予定成果物＞

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

【国際化活動バックアップWG】

（リーダー:中尾康二 氏／KDDI株式会社）

国際標準化活動の情報共有を継続的に実施する。

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

＜予定成果物＞

- 日韓シンポジウム開催報告書

【電子署名WG】

（リーダー:宮崎一哉 氏／
三菱電機株式会社　情報技術総合研究所）

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

＜予定成果物＞

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

【PKI相互運用技術WG】

（リーダー:松本泰 氏／セコム株式会社）

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

＜予定成果物＞
- PKI Day 2017 イベントでの発表

4. 教育部会

部会長：平山敏弘 氏／アクセンチュア株式会社

社会のニーズや時代の変化に適合したセキュリティ人材育成のため、必要とされる知識・技能等の検討を行い、実際に大学や専門学校等で評価実験を行う。また、情報セキュリティ教育のコンテンツとして、情報セキュリティ教育のシラバスや講義資料およびSecBoK更新版の作成とともに教育界・産業界への展開・使用を促進することで、情報セキュリティ人材の育成に貢献する。

さらに、継続して講師データベースへの登録講師や講師予備軍の若手による講義・勉強会の開催等、教える場の提供を支援することにより、JNSA教育部会メンバーのスキル向上を目指す。

加えてセキュリティコンテストとは異なる新たな実践教育ツールの開発や検証に対しても検討を行う。

＜予定成果物＞
- 大学シラバス対応版
- SecBoK2018

【ゲーム教育WG 】

（リーダー:長谷川長一 氏／株式会社ラック）

ゲームを活用した体験学習・振り返り教育の調査研究及び普及・促進。

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

【情報セキュリティ教育実証WG】

（リーダー:平山敏弘 氏／アクセンチュア株式会社）

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

＜予定成果物＞
- 岡山理科大学での「情報セキュリティ」講義の実施
- 情報セキュリティ講義コンテンツの更新、新規作成

【セキュ女WG】

（リーダー：北澤麻理子 氏／
ドコモ・システムズ株式会社）

女性セキュリティエキスパートの交流場所を提供し（会社の枠を超えた連携を可能にする）、セキュリティに関する専門スキルを持ちたい女性を応援する。

勉強会を中心に活動し、テーマは次年度の初回WGにメンバーで検討する。

＜予定成果物＞
- 2016年度の脆弱性情報勉強会のアウトプット

5. 会員交流部会

部会長：萩原健太 氏／トレンドマイクロ株式会社

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

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

【セキュリティ理解度チェックWG】

（リーダー:萩原健太 氏／トレンドマイクロ株式会社）

理解度チェックの継続的な問題の見直しを行うと共に、プレミアム版のユーザー数増加に向けた対外活動を実施する。

＜予定成果物＞
- 理解度チェックの問題アップデート

【JNSAソリューションガイド活用WG】

（リーダー:秋山貴彦 氏／株式会社アズジェント）

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

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

【経営課題検討WG】
(リーダー:菅野泰彦 氏／
アルプスシステムインテグレーション株式会社)

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

<予定成果物>

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

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

6. マーケティング部会

部会長：小屋晋吾 氏／株式会社豆蔵ホールディングス

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

7. 西日本支部

支部長：嶋倉文裕 氏／
富士通関西中部ネットテック株式会社

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

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

経営者に情報セキュリティ対策の必要性を訴求し、対策に投資をしてもらうため、必要性の見える化施策を検討する。

<予定成果物>

- 経営者向け情報セキュリティ対策実践手引き(仮称)

【企画・運営WG】
(リーダー:小柴宏記 氏／ジーブレイン株式会社)

JNSA会員および西日本地域のセキュリティレベルの向上を目指す。

【技術研究WG】
（リーダー：久保智夫 氏／株式会社サーバーワークス）

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

8. U40部会

部会長：赤松孝彬 氏／株式会社ディアイティ

若年層を対象メンバーとして、JNSAの若返り、若年層の活動活発化、幅広い人脈形成を目的として勉強会を中心とした活動を行う。

【for Rookies WG】
(リーダー:稲葉悠 氏／
セコムトラストシステムズ株式会社)

セキュリティ関連業務経験3年未満を対象とし、若手をはじめとした人的ネットワークの形成および知識向上を目的とする。

「いまさら聞けない相談事」を主に参加者が講師を担当などアクティブラーニング方式で行う。

【勉強会企画検討WG】
(リーダー:杉野広典 氏／
NECネクサソリューションズ株式会社)

U40部会員の知識・スキル向上を目指し、勉強会を企画・開催する。内容によってはJNSA会員からも広く勉強会参加者を募り、部会員同士・JNSA会員・講師との人脈形成を行う。

9. 情報セキュリティ教育事業者連絡会（ISEPA）

代表：持田啓司 氏／株式会社ラック

事業者間の連携や情報交換による業界活性化、政府機関への政策提言や政策実現ための適切な事業者紹介などを実施。年間活動予定として、セミナー開催、情報共有会議を行う。

＜予定成果物＞

- 教育コースのSecBoKマッピング

10. 日本セキュリティオペレーション事業者協議会（ISOG-J）

代表：武智洋 氏／日本電気株式会社
副代表：本田秀行 氏／日本電気株式会社

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

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

「グローバル動静情報共有プロジェクト」の活動も予定。

＜予定成果物＞

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

【セキュリティオペレーションガイドラインWG】

（リーダー:上野宣 氏／株式会社トライコーダ）

各脆弱性診断ガイドラインを作成する。

【セキュリティオペレーション技術WG】

（リーダー:川口洋 氏／株式会社ラック）

最新の技術動向を調査し、最適なセキュリティオペレーション技術を探究し、技術者の交流を図る。

【セキュリティオペレーション認知向上・普及啓発WG】

（リーダー:井上博文 氏／日本アイ・ビー・エム株式会社）

セキュリティオペレーションの必要性に関する認知度向上を図り、月次定例WGの他、一般向けセミナーを2回（5月・2月）開催予定。また、8月に集中検討（合宿）を実施予定。

【セキュリティオペレーション連携WG】

（リーダー：武井滋紀 氏／NTTテクノクロス株式会社）

セキュリティの運用について各社共通の課題の議論、検討を行う。集中検討（合宿：夏・冬）

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

【PJ（グローバル動静情報共有プロジェクト）】

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

11. 産学情報セキュリティ人材育成検討会

座長：江崎浩 氏／東京大学大学院教授

昨年度に引き続き、情報セキュリティ業界での就労体験の機会提供を目的にJNSAインターンシップを実施する。4月29日（土・祝日）には学生と企業間の意見交換・交流のための交流会を東京大学と大阪のサテライト会場で実施し、両会場で53名の学生が参加した。今年度は秋に学生、若手社員らを対象としたインターンシップ報告会イベントを開催する予定。

12. SECCON実行委員会

実行委員長：竹迫良範 氏
副実行委員長：寺島崇幸 氏／株式会社ディアイティ

今年度も企業スポンサーを募り、「SECCON 2017」として全国的にセキュリティコンテストを実施。昨年に引き続き、CTF初心者向けや女性限定のワークショップの開催にも注力する。

JNSA 役員一覧　2017 年 8 月現在

会　長	田中　英彦	情報セキュリティ大学院大学 名誉教授
副会長	髙橋　正和	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）

遠藤　直樹	東芝デジタルソリューションズ株式会社
大城　卓	新日鉄住金ソリューションズ株式会社
小椋　則樹	ユニアデックス株式会社
笠原　久嗣	エヌ・ティ・ティ・アドバンステクノロジ株式会社
河内　清人	三菱電機株式会社情報技術総合研究所
後藤　和彦	株式会社大塚商会
小屋　晋吾	株式会社豆蔵ホールディングス
櫻井　秀光	マカフィー株式会社
佐藤　憲一	株式会社OSK
下村　正洋	株式会社ディアイティ
土屋　茂樹	株式会社エヌ・ティ・ティ・データ
西本　逸郎	株式会社ラック
藤伊　芳樹	大日本印刷株式会社
藤川　春久	セコムトラストシステムズ株式会社
丸山　司郎	株式会社ベネッセインフォシェル
水村　明博	EMCジャパン株式会社
三膳　孝通	株式会社インターネットイニシアティブ

幹　事（50音順）

安達　智雄	日本電気株式会社
伊藤　良孝	株式会社インターネットイニシアティブ
大木　由利	大日本印刷株式会社
北澤　麻理子	ドコモ・システムズ株式会社
木村　滋	シスコシステムズ合同会社
後藤　忍	セコムトラストシステムズ株式会社
駒瀬　彰彦	株式会社アズジェント
崎山　秀文	キヤノンITソリューションズ株式会社
嶋倉　文裕	富士通関西中部ネットテック株式会社
清水　智	トレンドマイクロ株式会社
下村　正洋	株式会社ディアイティ
鈴木　英樹	株式会社OSK
高木　経夫	ユニアデックス株式会社
髙橋　正和	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
中間　俊英	株式会社ラック
能勢　健一朗	東芝デジタルソリューションズ株式会社
平田　敬	株式会社アークン
平山　敏弘	アクセンチュア株式会社
二木　真明	アルテア・セキュリティ・コンサルティング
前田　典彦	株式会社カスペルスキー
本川　祐治	株式会社日立システムズ
森　直彦	エヌ・ティ・ティ・アドバンステクノロジ株式会社
油井　秀人	富士通エフ・アイ・ピー株式会社
与儀　大輔	NRIセキュアテクノロジーズ株式会社
渡辺　一範	株式会社インフォセック

監　事

土井　充	公認会計士 土井充事務所

顧　問

井上　陽一	
今井　秀樹	東京大学 名誉教授
佐々木　良一	東京電機大学 教授
武藤　佳恭	慶應義塾大学 教授
前川　徹	国際大学グローバル・コミュニケーション・センター 所長
森山　裕紀子	早稲田リーガルコモンズ法律事務所 弁護士
安田　浩	東京電機大学 学長
大和　敏彦	株式会社アイティアイ
吉田　眞	東京大学 名誉教授

JNSAフェロー

井上　陽一	JNSA顧問
大和　敏彦	JNSA顧問/株式会社アイティアイ

事務局長

下村　正洋	株式会社ディアイティ

会員企業一覧　2017年8月現在　197社　50音順

【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)アイピーキューブ
アイマトリックス(株)
アイレット(株)
アクセンチュア(株)
アクモス(株)
(株)アズジェント
アドソル日進(株)
(株)アピリッツ
(株)網屋
アライドテレシス(株)
アルテア・セキュリティ・コンサルティング
(株)アルテミス
アルプスシステムインテグレーション(株)
EMCジャパン(株)
(株)イーセクター
イーロックジャパン(株)
イオンアイビス(株)
伊藤忠テクノソリューションズ(株)
学校法人 岩崎学園
(株)インターネットイニシアティブ
(株)インテック
(株)インテリジェントウェイブ
インフォサイエンス(株)
(株)インフォセック
ウォッチガード・テクノロジー・ジャパン(株)
(株)AIR
SCSK(株)
(株)エス・シー・ラボ
SGシステム(株)
EDGE(株)
NRIセキュアテクノロジーズ(株)
NECソリューションイノベータ(株)
NECネクサソリューションズ(株)
NHN テコラス(株)
エヌ・ティ・ティ・アドバンステクノロジ(株)
エヌ・ティ・ティ・コミュニケーションズ(株)
エヌ・ティ・ティ・コムウェア(株)
NTTコムソリューションズ(株)
NTTセキュリティ・ジャパン(株)
NTTテクノクロス(株)
(株)エヌ・ティ・ティ・データ
(株)エヌ・ティ・ティ・データCCS
エヌ・ティ・ティ・データ先端技術(株)
エヌ・ティ・ティレゾナント(株)
(株)FFRI
(株)エルテス
(株)OSK
(株)大塚商会
岡三情報システム(株)

【か】

(株)カスペルスキー
キヤノンITソリューションズ(株)
(株)クエスト
(株)クリエイティブジャパン New
グローバルセキュリティエキスパート(株)
KDDI(株)
KPMGコンサルティング(株)
(株)神戸デジタル・ラボ
(株)コスモス・コーポレイション
(株)コンシスト

【さ】

サイエンスパーク(株)
(株)サイバーエージェント
サイバー・ソリューション(株)
サイボウズ(株)
(株)サーバーワークス
G・O・G(株)
ジーブレイン(株)
JBCC(株) 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)シグマクシス
シスコシステムズ合同会社
システム・エンジニアリング・ハウス(株)
情報セキュリティ(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
SecureWorks Japan(株)
セキュリティ・エデュケーション・アライアンス・ジャパン
セコム(株)
セコムトラストシステムズ(株)
綜合警備保障(株)
ソースネクスト(株)
ソニー(株)
ソフォス(株)
ソフトバンク(株)
ソフトバンク・テクノロジー(株)
(株)ソリトンシステムズ
SOMPOリスケアマネジメント(株)

【た】

大興電子通信(株)
大日本印刷(株)

(株)宝情報
タレスジャパン(株)
TIS(株)
(株)ディアイティ
デジタルアーツ(株)
デロイト トーマツ リスクサービス(株)
(株)電通国際情報サービス
東京エレクトロン デバイス(株) New
東芝デジタルソリューションズ(株)
ドコモ・システムズ(株)
有限責任監査法人トーマツ
凸版印刷(株) New
トレンドマイクロ(株)

【な】

(株)ナノオプト・メディア
日商エレクトロニクス(株)
日本アイ・ビー・エム(株)
日本アイ・ビー・エム　システムズ・エンジニアリング(株)
日本オラクル(株)
日本企画(株)
日本セーフネット(株)
(株)日本総合研究所 New
日本電気(株)
日本電信電話(株)
日本ビジネスシステムズ(株)
日本プルーフポイント(株)
日本プロセス(株)
日本マイクロソフト(株)
日本ユニシス(株)
(株)ネクストジェン
ネットワンシステムズ(株)

【は】

パーソルテクノロジースタッフ(株)
(株)パソナテック New
パナソニック(株)
パロアルトネットワークス(株)
BAEシステムズ・アプライド・インテリジェンス・ジャパン(株) New
(株)日立システムズ
(株)日立ソリューションズ
飛天ジャパン(株)
(株)PFU
PwCサイバーサービス合同会社 New
華為技術日本(株)
(株)ファインデックス
(株)VSN
フォーティネットジャパン(株)
富士ゼロックス(株)
富士ゼロックス情報システム(株)
富士通(株)
富士通エフ・アイ・ピー(株)
(株)富士通エフサス New
富士通関西中部ネットテック(株)
富士通クライアントコンピューティング(株)
(株)富士通ソーシアルサイエンスラボラトリ
(株)ブロードバンドセキュリティ
(株)ブロードバンドタワー
(株)プロット
(株)ベネッセインフォシェル
北陸通信ネットワーク(株)

【ま】

マカフィー(株)
(株)豆蔵ホールディングス New
丸紅OKIネットソリューションズ(株) New
丸紅情報システムズ(株) New
みずほ情報総研(株)
三井物産セキュアディレクション(株)
三菱スペース・ソフトウエア(株)
(株)三菱総合研究所
三菱総研DCS(株)
三菱電機(株)情報技術総合研究所
三菱電機インフォメーションシステムズ(株)
三菱電機インフォメーションネットワーク(株)
(株)mediba
(株)メトロ

【や】

(株)ユービーセキュア
ユニアデックス(株)

【ら】

(株)ラック
(有)ラング・エッジ
(株)リクルートテクノロジーズ
リコージャパン(株)
(有)ロボック

【わ】

(株)ワイズ

【特別会員】

一般社団法人 IIOT
(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
一般社団法人重要生活機器連携セキュリティ協議会
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
長崎県立大学情報システム学部情報セキュリティ学科
一般社団法人 日本インターネットプロバイダー協会
一般社団法人 日本クラウドセキュリティアライアンス
一般社団法人 日本コンピュータシステム販売店協会
特定非営利活動法人 日本システム監査人協会
特定非営利活動法人 日本情報技術取引所
一般社団法人 日本スマートフォンセキュリティ協会
特定非営利活動法人 日本セキュリティ監査協会
一般財団法人 日本データ通信協会 タイムビジネス協議会

JNSA 年間活動（2017 年度）

4月	4月19日	PKI Day 2017「IoT・ブロックチェーン時代の PKI」
	4月26日	第1回　幹事会
	4月29日	産学情報セキュリティ人材交流会〜インターンシップに向けて
5月	5月10日	2017年度　理事会
	5月27日	SECCON Beginners 2017 長野
6月	6月8日	JNSA 全国横断セキュリティセミナー 2017 福岡
	6月12日	JNSA 2016 年度活動報告会 / 2017 年度総会（秋葉原 UDX）
	6月16日	CTF for GIRLS　第7回ワークショップ
	6月24日	SECCON Beginners 2017 盛岡
	6月26日	JNSA 全国横断セキュリティセミナー 2017 名古屋
	6月27日	JNSA 全国横断セキュリティセミナー 2017 大阪
7月	7月1日	SECCON Beginners 2017 名古屋
	7月13日	JNSA 全国横断セキュリティセミナー 2017 仙台
	7月20日	JNSA 全国横断セキュリティセミナー 2017 東京
	7月21日	第2回幹事会
8月	8月19日	CTF for GIRLS　学生対象ワークショップ
	8月26日	SECCON Beginners 2017 広島
9月	9月21日	第3回　幹事会
	9月23日	SECCON Beginners 2017 仙台
10月	10月7日	SECCON Beginners 2017 東京
11月	11月18日	SECCON Beginners 2017 鹿児島
	11月22日	第4回　幹事会
12月	12月2日	SECCON Beginners 2017 長崎
	12月5日	CTF for GIRLS　第8回ワークショップ
	12月9日	SECCON 2017 オンライン予選
	12月10日	SECCON 2017 オンライン予選
1月	（未定）	NSF 2018（予定）
	（未定）	賀詞交換会（予定）
2月	2月17日	SECCON 2017 決勝大会（国内決勝大会）
	2月18日	SECCON 2017 決勝大会（国際決勝大会）
	2月19日	SECCON 2017 決勝大会（国際決勝大会）
3月		

2017年4月から2018年3月
「インターネット安全教室」開催

★JNSA 年間スケジュールは、http://www.jnsa.org/aboutus/schedule.html に掲載しています。
★JNSA 部会、WG の会合議事録は会員情報のページ http://www.jnsa.org/member/index.html に掲載しています。（JNSA 会員限定です）

会員紹介（当コーナーでは、JNSA で活躍されている会員の方に、リレー方式で自己紹介をしていただきます。）

NTTデータ先端技術株式会社　河島　君知

JNSA会員の皆さま、はじめまして。NTTデータ先端技術の河島君知（かわしま　きみとも）と申します。このたびユニアデックス株式会社の田内さんからのご紹介により本稿を執筆させていただきます。

私はセキュリティ業界に14年間携わっています。これまで携わってきた業務は多く、セキュリティインシデント管理システム開発(SIEM+トラブルチケットシステムのようなシステム)、IDS・FW・WAF・DBF監視サービスや脆弱性情報配信・インシデントレスポンス業務の立上げなど、企画・開発・運用する機会をいただきました。

最初に任せていただいた業務はIDS監視サービスの運用です。当時はインシデント対応に忙殺される日々が1年以上続き、「しっかり寝る時間を作る！」ということが第一の業務目標になっていきました。第一の目標を達成すべく必死に試行錯誤し冒頭のインシデント管理システム開発を中心に多くの自動化・効率化を進めました。活動が実り、ゆっくり寝られる日々を迎えられた時の達成感を今でも覚えています。当時必死に開発したシステムの思想は現在も機能しているのですが、これは自分事として真剣に取り組んだ結果だったと感じています。こういった経験から、私は自分事として業務に取り組むきっかけを作ることを大切にしています。

セキュリティに携わって長いのですが、私の基礎技術や知識は、セキュリティとは関係ない分野にあります。私の基礎は、広帯域網活用の研究開発や、ライフラインを機能させる新システム構築業務で身に付けた思考や基礎技術です。セキュリティの活用には業務知識やさまざまな技術の基本を理解していることが前提にあり、その上でセキュリティ知識を利用することが重要だと、これまでの業務を通じて実感してきました。

現在は、セキュリティ業界で経験してきたことを少しでも活かしたいと考え、お客さまのセキュリティ対応組織（SOC/CSIRT）の立上げや運用を支援しています。また、セキュリティ運用事業者団体であるISOG-Jでは、各WGで知識の共有・議論をさせていただきながら、業界の発展に貢献できることがないか？業界を担っていく若手に伝えられる経験がないか？との思いで、セミナーでの講演・ドキュメントの執筆にも参画させてもらっています。・・などと想いを持って活動に参画させてもらってはいますが酒豪が多い業界、活動後は必ず愉しいお酒を呑みながら、逆に私の方が勉強させてもらっている毎日です。

JNSA活動の中で少しでも良い刺激を提供できるよう参加を続けさせていただきたいと考えておりますので、皆さまどうぞよろしくお願いします。

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。）

トレンドマイクロ株式会社　栃沢 直樹

JNSA会員のみなさま、はじめまして。

アイデンティティ管理WGで活動させて頂いておりますトレンドマイクロ株式会社 栃沢 直樹（とちざわ なおき）と申します。

このたび、伊藤忠テクノソリューションズの富士榮 尚寛さんからご紹介いただき、本稿の執筆を担当させて頂きます。

こちらの会員紹介のコーナーでご紹介されている皆様の多くは会社生活をエンジニアとしてスタートされている方かと思いますが、私の社会人生活はセールスからのスタートでした（それも全く業界の違う・・・）。ITに全く縁のない仕事をしておりましたが、社会人3年目に国際ネットワークを構築するSI企業に転職をし、企業ネットワーク、ゲートウェイシステムの提案に携わるようになりました。その業務の中で、一緒に活動をしていたエンジニアの方の影響を受け、自分もエンジニアとしてのキャリアを積んでいきたいと感じるようになり、MSPサービスの提案・運用、プロジェクトマネジメントなどを経て、セキュリティソリューションを提案、デリバリを行うエンジニアとして活動するようになりました。

現在はよりセキュリティに特化した形でユーザ企業様の提案をしていきたいと考え、現職にてセキュリティベンダーの立場から販売パートナー様へのソリューション提案、技術支援を行うとともに、プラットフォームベンダー様とのテクノロジーアライアンスを担当しております。

JNSAのアイデンティティ管理WGには、当時同じ会社にいらっしゃったラックの大竹 章裕さんにご紹介を頂き、参加させて頂くようになりました。アイデンティティ管理を専任で担当した経験はなく、現在の業務の中でも直接的に対応することはなかなかありませんが、企業セキュリティにおいてもクラウドの利活用が広がる中でID管理の重要性はより大きくなってきておりますし、IoT分野でもアイデンティティ管理のあり方の議論も活発になってきていると感じております。

ワーキンググループに参加させて頂く中で、アイデンティティ管理分野でのプロフェッショナルの皆様とは少し異なる視点（セールススタートという経歴も含めて）で情報発信していければと考えております。

プライベートでは夏は野球観戦しながらのビール（埼玉西武ライオンズファンです！）、冬はスキーと比較的アクティブ？に活動しております。

このアクティブさをJNSAの活動でも生かせればと思っております。今後ともよろしくお願い申し上げます。

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. 会員勉強会への参加
3. (ISC)2・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

お問い合せ

特定非営利活動法人
日本ネットワークセキュリティ協会　事務局
〒 105-0003 東京都港区西新橋 1-22-12 JC ビル 4F
TEL：03-3519-6440
TEL：03-3519-6441
E-Mail：sec@jnsa.org
URL：http://www.jnsa.org/

西日本支部
〒 532-0011 大阪府大阪市淀川区西中島 5-14-10
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.44

2017 年 9 月 13 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: http://www.jnsa.org/

印　刷
プリンテックス株式会社

セキュリティにまつわる課題解決を支援します

JNSAソリューションガイド

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

活用のポイント・メリット

- IPA中小企業ガイドラインなどに対応する製品・サービスを検索できる！
- 十大脅威等最新の脅威から検索できる!
- マイナンバー対策に必要な製品サービスを検索できる！

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

JNSA

情報セキュリティ理解度チェック プレミアム

http://slb.jnsa.org/eslb/

情報セキュリティリテラシー

企業リスク管理の第一歩

情報漏えいがもたらす直接間接の損害は、企業の価値を損ね、業績を直撃します。情報システムの障害は事業の運営管理を阻害し、規模によってはその存続を左右します。情報事故は企業管理上、大きなリスク要素となってきています。情報事故の要因のほとんどは、一般従業員の過失やミスであり、その背景には、情報セキュリティへの知識・経験不足があります。従業員の情報セキュリティリテラシーの確保は、企業経営上のリスク管理課題の第一と言えます。

JNSA 理解度チェックサイト

情報セキュリティリテラシー教育の第一歩

JNSA では、2007 年 1 月に個人利用向け「情報セキュリティ理解度セルフチェック」サイトを開設し、一般従業員が業務上身につけるべき情報セキュリティ知識を自習により確認できるサービスを提供してきました。2008年12 月からは、企業の管理者が自社の社員を登録して履修させ、その結果を管理できるサービス「情報セキュリティ理解度チェック」サイトも開設。社員が個別的関心で受講するだけでなく、組織として自社の到達レベルを確認したり、同業種内でのランキングにより、自社のセキュリティレベルが他社に比較してどの程度かがわかるサービスも提供しています。

知っておきたい情報セキュリティとは・・・

一般のオフィスワーカーが仕事をする上で、最低限身につけておいてほしい、セキュリティに関する“常識”的知識の程度を確認するものです。PC、メール、ウイルス、紙や記憶媒体の取扱い等、オフィスの内外で日常的に接する情報やさまざまなシーンにおいて、守るべきこと、やってはいけないことを確認し、身につけるものです。
問題を解く形式で、解説を確認することで情報セキュリティリテラシーが身につきます。Web ベーストレーニング（WBT）と言われる、自動・自習のシステムにより、場所と時を選ばず、また管理者がいちいちお膳立てする手間を省いて、効率よく情報セキュリティ教育を実施できます。

出題のカテゴリ

- 電子メールの知識と利用法
- インターネットの利用法と注意点
- ウイルスの知識と対処方法
- パスワードの知識と管理
- PCの利用上の注意点
- オフィスにおける情報セキュリティ
- ルールや規則の遵守
- 社外における情報セキュリティ

自習の方法

- 問題は各カテゴリから万遍なく25 問抽出し出題されます
- ユーザは 1 問ごとに 4 択から正解と思うものを選択します
- 25 問を 1 時間以内に解き採点結果を確認します
- 各問の意味や間違った理由を解説を見て学びます
- 繰り返し受講することで多くの問題に挑戦できレベルアップが図れます

管理者による管理

- 受講対象者をユーザとして登録、追加、削除します（個人情報の登録は不要）
- 問題セットを選択し学ばせたい問題を選択します
- 自社独自の問題を作成登録できます
- ユーザの受講結果を確認・未受講ユーザのチェックができます
- 自組織の平均得点をレーダーチャートでカテゴリ別に確認。業種や全体の平均との比較もできます
- 受講結果はCSVダウンロード可。ユーザを個別管理・フォローできます

プレミアム版の特典やサービスの詳細情報は裏面をご覧ください。

JNSA NPO 日本ネットワークセキュリティ協会
http://www.jnsa.org
〒105-0003 東京都港区西新橋 1-22-12 JC ビル 4F　TEL：03-3519-6440　E-Mail：slb@jnsa.org

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

〒105-0003 東京都港区西新橋1-22-12 JCビル 4F
TEL 03-3519-6440　FAX 03-3519-6441
E-mail: sec@jnsa.org　URL: http://www.jnsa.org/

西日本支部
〒532-0011 大阪府大阪市淀川区西中島5-14-10 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