JNSA PRESS
JAPAN NETWORK SECURITY ASSOCIATION
SPRING 2016 VOL.41

寄稿

職場の5Sで考える情報セキュリティ
02

IoTセキュリティを支える「暗号技術によるトラスト」の重要性
10

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

進化する制御システムの先にある未来とは

JNSA 理事
セコムトラストシステムズ株式会社
藤川　春久

1997年5月、テルアビブにある某社でVPN製品の技術研修を受けていました。ようやく標準化が進んだIPsecベースの製品で、高額な専用線からインターネットを利用した仮想専用線の時代になるとかで、いち早くビジネスで活用すべく研修に参加していました。私のサイバーセキュリティとの関わりはここから始まったように思います。その後、19年近くサイバーセキュリティに携わってきた中で常に感じていた事は、見えない脅威から守るばかりで能動的に脅威と対峙できないというジレンマ。IoTが進行する現在ではあらゆる製品に搭載されているシステムの中身が分からないことから生じる不安も感じざるを得ません。

昨年、ドイツ車で排気ガスの不正が発覚しました。不正は「違法なソフトウェア」によるもので、リコールはソフトウェアの修正が中心になるということでした。車に搭載されている制御システム（ソフトウェア）は何ができるのか気になりました。最近の自動車は輸出先の国の法律や安全基準に適合するよう、車に搭載するコンピューター（以下、車載システム）が非常に細かく制御できるようになっており、エンジンの制御だけでなく走行機能や電子機器など車全体を制御できるようです。もしも、この車載システムに誰でもアクセスでき、重要な制御機能の設定が変更されてしまったら、事故にも繋がりかねません。自動車を所有する個人が車載システムの設定情報を変更する方法（「Coding」と呼ばれている）について情報発信しているサイトがあることを知りました。私も車を所有しておりますが、点検等はディーラーにお任せしています。ディーラーによれば車の整備にはメーカー公認資格が必要で、専用システムが無ければ車載システムにアクセスできないとのこと。しかし実際には、車載システムにアクセスするためのプログラムや、車とPCをOBDIIコネクタとLANケーブルで接続する方法、ランチャーを起動すると車に接続を開始して車台番号が表示される等の情報がサイトに掲載されています。プログラムにはPINコード生成機能があり、認証手続き無しに車載システムにアクセスできるようです。OBDIIコネクタとWi-Fi機器が合体した製品もあるようで、これを利用すると車外からも設定変更が可能となるようです。メーカーがセキュリティ対策を強化する筈なので、この状態がこのまま続くとは思えませんが現時点ではアクセス制御の強化が必要な製品もあるようです。

自動車だけでなく身の回りの多くの製品がネットワーク接続できるようになりその先にはインターネットへの接点もある筈です。生活全体がインターネットと切り離せない社会の到来。安心した生活を送るにはサイバーセキュリティの更なる進化も必要な時代となってきたようです。

職場の５Ｓで考える情報セキュリティ

JNSA 組織で働く人間が引き起こす不正・事故対応WG
大日本印刷株式会社　野津　秀穂

1. はじめに

５Ｓは、製造業の職場で定着している改善活動手法の一つである。５Ｓに情報セキュリティをテーマに加えることにより、身になじんだ改善活動として情報セキュリティに取り組むことが可能になる。

本稿は、西本逸郎ラック最高技術責任者の御好意を得て、2009 年の講演「セキュリティ強化に役立つ職場の「５Ｓ」活動」をベースに他の情報セキュリティ活動との関連を交えて紹介する。

2. 情報セキュリティ事故に関する原因分析

「５Ｓで考える情報セキュリティ」の紹介に先立ち、本稿が対象範囲とする情報セキュリティ活動の課題を明確にしておきたい。

筆者が所属する印刷産業を例として、2009 年から 6 年間で日本印刷産業連合会に報告された 77 件の個人情報の取扱いにおける事故を現象別に分類した割合を図 1. に示す。

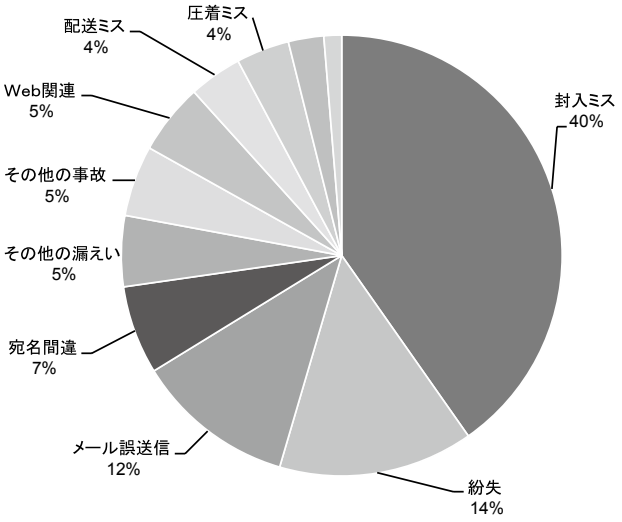


図 1.　印刷産業における個人情報に関する事故 [1]

総件数は、少ないものの原因のほとんどが、「封入ミス」などの「作業ミス」に起因する。

同様の傾向は、JNSA セキュリティ被害調査ワーキンググループの報告書（図2.）にも見受けられる。

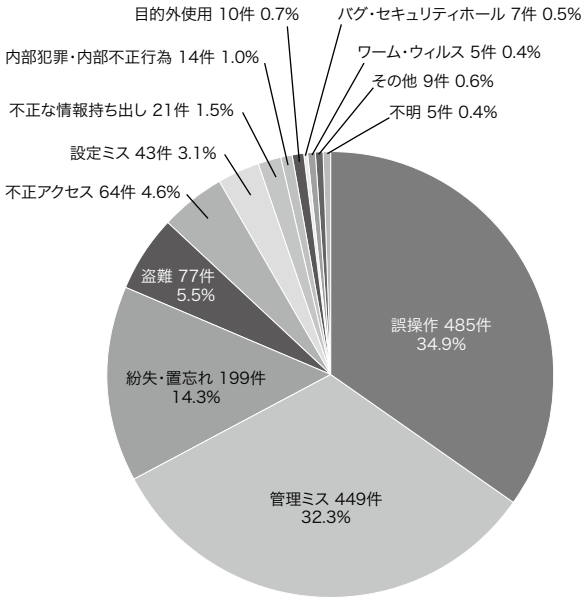


図 2.　JNSA2013 年集計　漏えい原因比率
（引用）JNSA 2013 年情報セキュリティインシデントに関する調査報告書

２つの事例における「作業ミス」「誤操作」は、ヒューマンエラーである。「管理ミス」はルール未整備またはルール不徹底により、作業者が判断を誤った事例である。印刷産業に限らず、ほぼ全ての業種において、原因比率で「ミス」が大半を占める。

本稿では、「ミス」抑止を課題とし、職場の日常業務の中で有効な情報セキュリティ活動を考える。

●本稿の内容は、筆者の個人的見解であり、必ずしも筆者が所属する組織の見解ではない。

1.　JFPI REPORT No.152 平成 26 年度 個人情報に関する事故報告ｐ 21　一般社団法人 日本印刷連合会 2015 年 7 月

3.「ミス」抑止に関する考え方

「ミス」に起因する情報セキュリティ事故は、工程内で発見され最終納品前に除去できたとしても軽視すべきではない事象であり、原因分析と対策(再発防止活動)がなされている。

3.1　ハインリッヒの法則[2]

ハインリッヒの法則は、「一つの重大事故の背景には、29の軽微な事故があり、その背景には、300の異常（ヒヤリ・ハット）が存在し、さらに幾千もの不安定状態が存在する。」という考え方である。

軽微な事故や「ヒヤリ・ハット」が「ミス」を原因とした事象である。事故の背景には必ず多くの前触れがあるので、類似した要因を持つ大きな事故に至らないよう「ミス」についても、ルールの見直し、作業改善など組織的な対策により重大事故防止に役立てることが求められる。

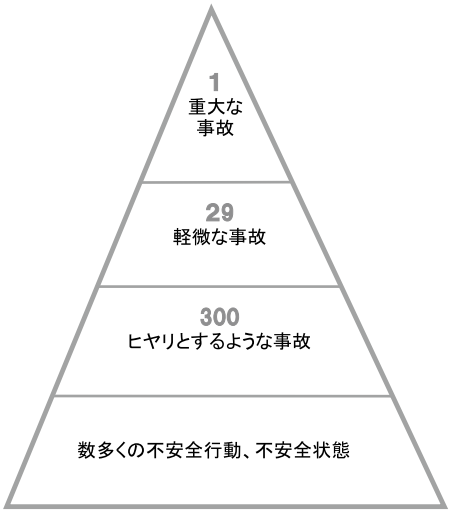


図3．ハインリッヒの法則

3.2　割れ窓理論[3]

建物の窓が壊れていることを放置すると、誰も注意を払っていないという象徴となり、「やがて他の窓もまもなく全て壊される」。「割れ窓」を「危険状態」と認識する。これが「割れ窓理論」の考え方である。

情報セキュリティでも、「ミス」への再発防止策を放置すると、大きな問題も気にならなくなり、その結果、事件に発展することもある。職場でも機密情報が机上放置されている状況（ルールの未整備やルール不徹底）では、何か問題が起きる可能性が常態化する。小さな不正を見逃さない組織風土を作ることにより、環境全体が除々に浄化されていくという考え方は、情報セキュリティ以外の分野でも、効果をあげている。

3.3　不安全行動[4]

大丈夫だろうなどの理由で意図的にルールを無視したり、悪意はないが不適切に行動したりして、結果として情報セキュリティ事故につながる行為を犯罪学では「不安全行動」という。「ミス」は、このような「不安全行動」から生じることが多い。

適切なルールを制定し、教育を行っても「不安全行動」が減少するとは限らない。効果的な工夫が求められる課題である。

4.「ミス」抑止のための取り組み

以上の「ミス」抑止の考え方に基づき、情報セキュリティ事故の原因で、「ミス」の発生は、無視できない課題と認識できた。「ミス」撲滅活動は連綿として各企業で取り組まれ一定の効果を上げている。

4.1　ヒヤリ・ハット活動

ハインリッヒの法則に基づき、作業者が体験したヒヤリ・ハット事例を集めて、事故防止のための対策につなげるよう活用する取組みを「ヒヤリ・ハット活動」

2. ハインリッヒ研究会編訳「ハインリッヒの事故防止」1956年
3. George L. Kelling, Catherrine M. Coles:“Fixing Broken Windows”, Simon & Schuster 1977年
4. 環境犯罪学からのアプローチ「内部不正対策14の論点」JNSA編　東京大学大学院 医学系研究科 高木大資　2015年

と言う。事故防止のための対策は、ミスを犯した個人の技量に起因すると考えず、ルール整備・見直しや技術的改善などマネジメントの課題として取り組むことが必要である。

ヒヤリ・ハット事例を集める際、体験した作業者が自己の技量不足を原因として感じると報告に至らないことがある。作業者は技量の研鑽も一つの目標であるため、技量不足を「ミス」として捉えないからである。また、前述の「不安全行動」のように当事者意識が欠如していると見逃すこともある。

この場合でも、技量不足をミスの原因としてはならない。技量が不足しても事故に至らないよう防御機能を持つ工程設計を考えるなどマネジメントの課題とする。

作業者が体験を「どのように感じるか」をうまく引き出すことにより、当事者意識を持った改善活動が実現する。指導者と作業者がコミュニケーションを重ねて事例を収集することが重要になる。

［コラム］
マネジメントの分野で「火の用心管理」というと全く別の行動を指し、悪いマネジメントの見本とされる。どのような場面で使うか、この用語を使う場合の留意点である。
マネジメント分野での「火の用心管理」とは、
江戸時代は火事が多かったが、城主が天守閣から「今日は、風が強く出火が心配だ」と感じて、家老に「火の用心せよ」と命令した。
家老は、町役人に「火の用心せよ」と伝えた。
町役人は番太（岡っ引き）に「火の用心せよ」と伝え、番太は、拍子木をたたいて「火のよーじん」と声をあげて町内を巡わった。伝言は伝わったが実際の効果につながっているか？
本来は、「火の元点検」、「残り火の消し忘れ点検」など、トップの方針である「防火」を実現するため、各階層の管理者にて、具体的施策を明確にしないといけない。

４.２　火の用心活動

作業者が見逃す「ヒヤリ・ハット」や「不安全行動」を見つける活動として「火の用心活動」がある。発見する点検者を決めて職場をパトロールし、「（常態化した）割れ窓」を見つけたら「イエローカード」「レッドカード」を貼り改善テーマに取り上げる。

「火消し」より「火の用心」、「危険状態を見逃さない」という視点で、大きな事故が起きる前、つまり「ヒヤリ・ハット」程度の小事故や「ヒヤリ・ハット」が顕在化する前の「不安全行動」の時点で対策する活動である。点検者が客観的に事例を収集するため、作業者が見逃している（作業者は日常作業のため不自然さを感じない）事象の発見に役立つ。まずは、顕在化している「割れ窓」を発見することに努めるが、事後的な対処に終始しないよう、危険状態になりそうな可能性を発見することも心掛けたい。ここでも点検者は作業者と充分なコミュニケーションを取り、当事者意識の高揚を図りながら進める。作業者の積極的参加は必須である。

４.３　小集団活動

職場内で小グループを編成し行う改善活動として「小集団活動」がある。特に品質管理を目的とした場合「ＱＣサークル」と呼ぶ。

「小集団活動」は、作業者の自発的な活動テーマとして扱うことを原則として発足し、当初は、休憩時間や就業時間後に実施し業務時間に含めなかった。現在では、業務時間中の改善活動としている。日本を除き世界的には、改善は、スタッフ部門など専門チームの職務であり、作業者の職務として改善活動を位置づけることは、諸外国から軋轢を生じことがある。日本の活動でも、課題発見の精度（重要な課題が漏れなく発見できたか）や改善のレベルは、必ずしも問わない。作業者一人ひとりが、自分の作業を見つめ、改善提案を通して経営に参画している意識を持つことにより、仕事へのモチベーションを高揚させるところに、大きな効果を求めている。

小集団活動は、業務として会社が認め、良い成果については改善として採用し、達成感を職場で共有化することにより活動が活性化する。達成感がモチベーシ

ョンの高揚に結び付き「不安全行動」の発生が抑制できる。

4.4　PDCAサイクル

目標を設定してその実行計画（Plan）を立案し実行（Do）し、実行結果と計画（目標値）との乖離（誤差）を測定して評価（Check）する。計画（目標値）と実行結果に乖離（誤差）があった場合には、是正措置・対策（Act）を講じる。

実行結果をチェックして次の改善活動に結びつける仕組みをフィードバック・システムと呼び、「マネジメント（管理）」の基本的な考え方である。

1950 年代、品質管理の父といわれる W・エドワード・デミング博士が、生産プロセス（業務プロセス）の中で継続的に行うために改善プロセスが連続的なフィードバックループとなるように提案した。このためデミングサイクル（Deming cycle）とも呼ぶ。

ＰＤＣＡサイクルの考え方は、製造プロセス品質の向上や業務改善などに広く用いられており、情報セキュリティマネジメントシステム（ISO27001）や個人情報保護マネジメントシステム（JISQ15001）の基礎となるマネジメントの仕組みである。

ＰＤＣＡサイクルは、第二次世界大戦中にドイツのフォン・ブラウン博士が、ロンドン攻撃のために開発したＶ２ロケット兵器の技術として発明した自動姿勢制御機構（フィードバック制御＝ＰＤＣＡ）がＰＤＣＡの起源となる。大戦後、フォン・ブラウン博士はアメリカに移住し、アポロ計画の中心的科学者として活躍した。軍事機密だったＰＤＣＡサイクルは、その後、品質管理や経営学に広く応用された。

この方式の画期的な点は、飛行中に推進方向を自動修正しながら目標を達成する方式にある。

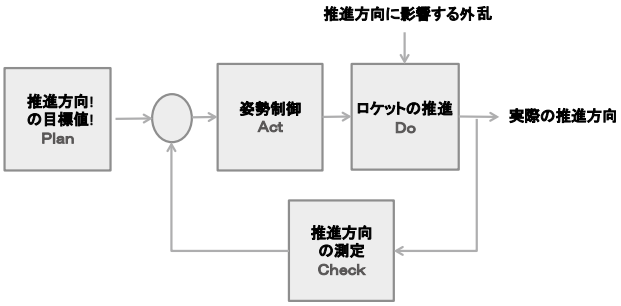


図4．Ｖ2ロケットの自動姿勢制御機構

同時期に、アメリカでもＪ．Ｗ．フォレスター博士の研究チームが、フィードバック制御を用いて爆撃機を砲撃するための自動照準装置の開発を進めた。

この研究は、戦後にＰＤＣＡを企業活動などに広く応用された。[5]　ＰＤＣＡを企業活動に応用する効果としては、プロセス（作業工程）を測定（観測）しながら、作業中に是正指示を行い目標達成する（例えば、後工程に不良品を送らない）ことにある。

1916 年、H. ファイヨールは、著書「産業並びに一般の管理　都筑栄訳」の中で「管理とは、予測し、組織し、命令し、調整し、統制すること」と定義した。この「統制」が、後に「ＰＤＣＡ」と融合しマネジメントシステムとして確立した。

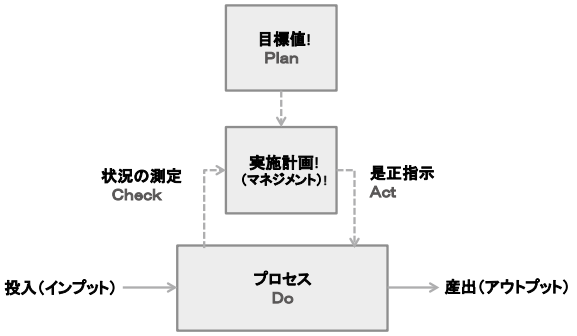


図5．ＰＤＣＡサイクルの経営学への応用 [6]

5．インダストリアル・ダイナミックス」J.W. フォレスター著　石田 晴久、小林 秀雄訳　紀伊国屋書店　1971 年
6．企業活動のモデル「経営戦略論」 H.I. アンソフ著、広田寿亮訳　産業能率短期大学出版部　1985 年

４.５　５S活動

「５S活動」とは「整理」「整頓」「清掃」「清潔」「躾（しつけ）」のことで、いずれも「S」で始まる言葉の総称。製造業では職場改善の原点でもある。

「５S活動」は日本でつくられた「皆が当たり前のことを、当たり前に行う」ための管理手法であり、今日では世界中で実施されている。[7] 表１には、海外で取り組まれている５Sの各国語訳の事例を示す。

「皆が当たり前のことを、当たり前に行う」ことの重要性について改めて整理すると、例えば、担当者が替わっても、同品質の製品やサービスが求められるのは当然のことであり、顧客は、つくった人（またはサービスする人）に関心があるわけではなく、購入する製品やサービスに満足することを求めている。そのため会社では「決められたことを、決められたように確実に守り、実行できる人」を育てることが重要になることが認識できる。

４.６　それでも事故は起きる

「ヒヤリ・ハット活動」、「火の用心活動」、「小集団活動」、「ＰＤＣＡサイクル」、「５S活動」が一定の効果をあげているものの、前掲 JNSA セキュリティ被害調査ワーキンググループの報告書のとおり、それでも事故は起きる。

情報セキュリティに関する社内ルール、業務手順書、改善見直し手順などは多岐に及び、もとより教育により知識としては知っているが、実際に自分の業務に、どのルールが適用するかと判断する際に齟齬が生じることがある。[8] 知識と行動を結びつけるためにも、追加策を工夫したいところである。

他の活動と独立した特別な活動と考えることなく、日常の改善活動に情報セキュリティの視点を加えることにより、知識と行動の遊離を抑制し、当事者意識を持ち、身に溶け込んだ活動としたい。

本稿では、製造業の職場で「作業者がなじんだ日常の改善活動」として「５S活動」を取り上げ、情報セキュリティの視点を加えることを紹介する。

5. セキュリティ強化に役立つ職場の「５S」

「５S活動」の利点は、「整理」、「整頓」から始まり、改善対象を身の回りから探す、わかり易さにある。

「５S活動」は規制を求めるものではなく、「働きやすい」環境をつくることを目指す。働きやすい環境は、ミスを防止し、情報セキュリティ強化に役立つ。

情報セキュリティ強化は、製品・サービスの競争力を

表１.　５Sの各国語標記例

日本語	英語	イタリア語	フランス語	オランダ語	インドネシア	マレー語	繁字体	簡字体
５S	５S	５S	５S	５S	５R	５B	５S	５S
整理	sorting	SCEGLIERE e SEPARARE	S'organiser	Scheiden	Ringkas (Buang)	Buang	整理	整理
整頓	setting in order	SISTEMARE e organizzare	Situer	Schikken	Rapi (Beres)	Beres	整頓	整頓
清掃	shining	SORVEGLIARE	Scintiller	Schoonmaken	Resik (Bersih)	Bersih	清掃	清扫
清潔	standarizing	STANDARDIZZARE e migliorare	Standaliser	Standaardiseren	Rawat (Bebas)	Bebas	清潔	清洁
躾（しつけ）	systaining discipline	SOSTENERE nel tempo	Suivre	In Stand houden of Systematiseren	Rajin (Biasa)	Biasa	維持紀律	素養

7.「改善のための５Sと英語表現」松崎 久純、山名 敏文　三修社　2005 年
そのまま使えるモノづくり現場の英語コミュニケーション　松崎 久純「工場管理」日刊工業新聞 2010 年 2 月から 5S を連載
8. 内部不正の原因と対策に関する考察「内部不正対策 14 の論点」JNSA 編　大日本印刷　野津 秀穂　2015 年
ここでは、当事者意識の醸成「教育によって得た知識と自分の行動が必ずしも結びついていない」課題を提起している。

高め、安全性も高める。「情報セキュリティ」は製品・サービスの品質そのものであることを認識し、モチベーションの高揚にも役立てたい。

「５Ｓ活動」は、作業者個人の単独活動ではなく、「小集団活動」の中で、すべての人が参加することを原則としている。作業者が自分の作業を見つめると共に、自分の作業について後工程への貢献度を知り、自分の作業と自職場全体の目標の共有化を意識する「きっかけ」としたい。職場における人間関係（主観的な協働意識）は、作業効率に大きな影響をもたらすことが知られている。[9] 作業能率改善は、「作業ミス」の抑制にも効果が期待できる。

このように「５Ｓ活動」は、情報セキュリティも包含した改善活動の１つとなるが、独立した活動として捉えると、職場で実践している他の改善活動の考えと分離し、作業者の混乱を誘引する。他の改善活動の考え方も取り入れ体系化し、一体化することで、初めて身についた実感のある活動となる。

情報セキュリティ強化に役立つ職場の５Ｓ活動を紹介する中で、他の改善活動の関連にも触れたい。

5.1 「整理」Sorting

整理は , 必要なものと不必要なものを分けることです。
Sorting, the Necessary from Unnecessary.

もし必要なものと不必要なものが一緒にされていると、間違ったモノや情報を選ぶリスクがある。

整理することで、見知らぬ情報の存在や機密にすべき情報が無造作にさらされているなどの誤りを、ミスが起きる前に発見できるメリットがある。

整理は、職場のスペースを効果的に使用することも助ける。整理することで、仕事は随分とラクになる。

職場にあるモノや情報は、すべて必要なものばかりだろうか？注意深く見ると「もしかしたら必要かもしれない」「廃棄してしまって後に必要だったら…」など、保管期限が明確でないこと、廃棄や消去のタイミングについて判断がつかないので、ついつい不要になった書類やデータを保管していることがある。不要になった書類やデータを保管していると、漏えいなどのリスクを抱え続ける（リスクの常態化）ことになる。

不要なものは「整理」して捨てる。
（例）
- 書類やメールは内容を確認し、社外秘・秘・極秘など情報の重要度に応じて分類し、必要な情報は保管期限を定める。
- 分類した情報の責任者が誰かを決める。
- 不要なものを判断して捨てる。多くのものを残すことで、必要なものを探す効率が悪くなる。
- 得意先から預かった情報は、業務終了後に返却または消去・廃棄する。保管する場合は、保管期限を決めて得意先の了解を得る。
- 重要な書類は、鍵のかかる袖机やキャビネットに保管し、勝手に持ち出されないようにする。
- データは、サーバに保管しアクセス管理を徹底する。

「整理」は、「あるべき姿」を決めることであり、「ＰＤＣＡサイクル」の実行計画（Plan）に位置する。「整理」という言葉で目的（解決すべき課題）を定義しているので、作業者自らが身の回りの課題を探し易い。考え方が定着した次の段階では、「ヒヤリ・ハット活動」で収集した事例を解決すべき課題として取り上げて「整理」する。

5.2 「整頓」Setting in Order

「整頓」は、誰もが必要なものを見つけられるように、すべてのものを便利に配置することです。
Setting in Order, Means the Convenient Placing of all Items, so Everyone can Easily Find What They Need.

9. ハーバート大学メイヨー博士が、1924 ～ 1932 年にアメリカのウエスタン・エレクトリック社ホーソン工場で行った実験では、作業集団の人間関係が作業能率に介在していることがわかり、経営管理の人間関係論として発展した。

情報セキュリティの観点では、必要なものを取り出せるだけではなく、情報が紛れたり紛失したり行方不明にならないような具体的施策が必要である。

必要なものを探して歩き回るのは、時間のムダとなる。整理と整頓は、職場のムダを減らす。

仕事を大変にするためではなく、仕事をシンプルかつラクにするための５Ｓ活動として意識したい。何かを規制するゼロサムではなく、目的を達するための施策を工夫するポジティブサムで考える。

必要なものをいつでも取り出せるよう「整頓」する。
（例）
- 使ったものは元の位置に戻す。
- 新しく入ったものはルールに従い配置する。
- 重要な情報の管理は、貸出し記録等に記録をつけて、所在を明確にする。
- 権限のある人だけが取り出せるアクセス管理設定も必要。

整理された状態から、誰もが、必要な時に、必要なものや情報を即座に取り出せるよう「一目でわかる」工夫をする。例えば、書類はバインダー等に綴じて背表紙をつけ、複数の文書が綴じられている場合はインデックスをつける。データは、フォルダに分類して保管する。重要度の分類表示と保管期限、管理者の表示も忘れてはならない。

「整理」で決めた「あるべき姿」を具体的に実施するのが「整頓」であり、「ＰＤＣＡサイクル」の「実行(Do)」に位置する。

５.３ 「清掃」Shining

「清掃」は、きれいにすることです。
きれいにするために点検清掃します。
Shining is Cleaning.
Let's Check and Keep Everything Tidy.

整理整頓をしていても、汚れや垢は溜まる。清掃の中に点検を組み込んで清掃点検とすることで問題の原因を見つけ、対策を講じ改善することが望まれる。

きれいに掃除をすることで、品質や歩留まりの向上につながり、「ミス」の抑制になる。いつでも職場をきれいに維持する。この意味は、仕事が終わったときだけでなく、仕事をしている間も、きれいにするということである。例えば、使った書類は、その都度、所定の位置に戻す。受領したデータは、その都度、情報の重要度を分類し必要な情報は保管期限を定めサーバに保管してアクセス権限を設定する。

常に見直しを実施し、不要になった情報を破棄・消去して「清掃」する。
（例）
- 不要なメモや不要な一時ファイル等は削除する。
- 情報の内容に応じて、シュレッダー処理する。
- 重要な情報は、バックアップも検討する。
- 異動となった人のアクセス権限の見直しを行う。
- 不要サイトへの通信を遮断する。

「清掃」は、「整理」（あるべき姿）としての計画と実行した「整頓」の差異を点検することであり、「ＰＤＣＡサイクル」の評価（Check）に位置する。日常作業を自ら点検する「自己点検」の他、「火の用心管理」の点検者によるパトロールも「清掃」に相当する。

「清掃」して初めて、残る課題（不備事項）を発見することもできる。

５.４ 「清潔」Standardizing

「清潔」は、整理、整頓、清掃の基準を維持することです。基準を維持するために、標準化を進めます。
Standardizing, Means Maintaining Standards for Sorting, Setting in Order and Shining.

整理、整頓、清掃を一度は実施できるが、継続することは難しい。清潔は、整理、整頓、清掃をいつも実施し続けることである。実施し続けるために標準化を進める。自分の仕事がし易くなるように自ら工夫する。この結果「きれい」な状態を維持する。未整備な状態を「いつもの状態」と無感覚に陥ってはならない。

常に「清潔」にして異常信号を見逃さない。
（例）
- コンピュータ・ウイルス対策やパソコンのセキュリティ対策を実施し感染予防をする。
- 会社で購入したアプケケーションは、使用許諾を守り適切なソフトウェアを使用する。不正なソフトウェアは使わない。
- 会社の資産が盗難に遭わないよう盗難防止を行う。

「清潔」は、「清掃」で発見した課題を改善する工夫であり「ＰＤＣＡサイクル」の「是正計画（Act）」に位置する。是正計画は、対処療法的な対策ではなく、継続できるよう対策手順として標準化する。

5.5 「躾（しつけ）」Sustaining Discipline

「躾」は、「全員が決められたことを、決められたように、必ず実行できるようになる」ことです。
このために、決めたことをルール化して維持します。
Sustaining Discipline, Means Everybody doing what is expected, as expected. Let's Take What has Been Decided and Create a set of Rules.

「躾」とは、仏教用語の習気（じつけ）を原義とする。習気（じつけ）とは、善悪の判断が、香りが衣に染み付いて残存するような「自然に身についている」様子を言いう。小笠原礼法により「躾」という文字に統一して使われるようになった。躾を身につけるためには、もちろん練習・訓練が必要だが、社会問題となるような暴力や虐待、調教を「躾」と呼ぶことは間違った解釈である。

決められたルールや手順を正しく守る習慣を「躾」る。
職場での教育も大切ですが、社員として、遵守しなければいけない項目がある。
（例）
- 改善した対策は、ルール化して全員に教育する。
- 教育内容を理解し、役割レベルに応じて実践する。
- 実践の結果を振返り、できていない部分を強化する。
- ウイルス等に感染したら、感染が拡大しないようネットワークケーブルが抜けるよう訓練する。

５Ｓ活動を小集団活動に取り入れることにより全員が当事者意識を持って自らの作業を見つめ、自分の仕事を大切に考えてもらいたい。

6. 終わりに

製造業の職場で定着している改善活動手法の一つである５Ｓに情報セキュリティをテーマに加えることにより、身になじんだ改善活動として情報セキュリティに取り組むことを紹介した。

本稿は、2009 年の西本逸郎ラック最高技術責任者の講演「セキュリティ強化に役立つ職場の「５Ｓ」活動」の考え方をベースとしている。改めて謝辞を申し上げます。

IoTセキュリティを支える「暗号技術によるトラスト」の重要性

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

1. はじめに

昨今、IoTの取り組みに対する世の中の関心の高まりに合わせて、情報セキュリティ業界においてもIoTのセキュリティに関する関心が高まっています。そもそもバズワードとも言えるIoTは、その定義自体が曖昧であり、その曖昧なIoTのセキュリティとなると更に曖昧となります。しかしながら、情報セキュリティ業界の一般的な意見としては、IoTが真っ当になるためには、セキュリティの対応が大変！そんなに甘くない！といった意見が、多数を占めるのではないではないでしょうか。

こうした中、将来に数百億個にものぼると言われるIoTデバイスやそれらから構成されるシステムの運用において、その脆弱性対応に翻弄されないためには、脆弱性を最小限にするためのIoTデバイスやそれらから構成されるシステムの設計時における「セキュリティ・バイ・デザイン」の取り組みが重要になると考えられます。そのセキュリティ・バイ・デザインにおいて、IoTのセキュリティのベースとなる機能の多くは、暗号技術により実現されると考えられますが、その一方、実装上において脆弱性を生みやすい部分自体も、暗号技術の実装部分だと考えられます。

暗号技術をどのように利用するかは、ビジネス面からみても重要な課題になります。大量のセンサーやアクチュエータ等のIoTデバイスと多様なクラウドサービスが連携するシステムによって提供されることが想定されているIoTによるサービスでは、ステークホルダー間の多様な信頼関係を構築できる必要があります。IoTデバイスから構成されるシステムにおいては、この多様な信頼関係構築のために暗号技術による「認証」「署名」等を使い、秘匿性の確保やサービスの分離のために「暗号化」を使ってこれらの課題を解決することは不可欠です。また、IoTデバイスのプログラムの更新時においても、そのプログラムの検証が暗号技術より行われると考えられます。

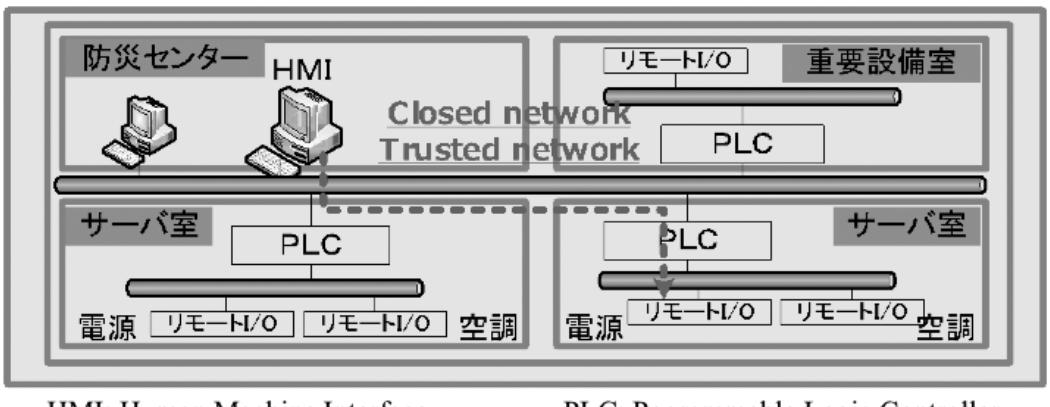
本稿では、こうしたIoTセキュリティのベースとなる機能等を「暗号技術によるトラスト」として捉え、その取り組みの重要性を解説します。

2. 重要インフラにおける物理セキュリティ環境によるトラスト

本題のIoTにおける暗号技術、および暗号技術によるトラストの話に入る前に、暗号技術があまり利用されていない重要インフラの制御システムにおける物理セキュリティ環境によるトラストについて説明します。

ここでは、重要インフラにおけるセキュリティのベースとなるトラストを説明するために 図1に示すデータセンターにおける電源や空調の制御をおこなうビルオートメーションシステムを想定して説明します。

今日において、多くの重要インフラの制御システムおよびそのネットワークは、堅牢な重要施設おける物理的



HMI: Human Machine Interface　　PLC: Pogrammable Logic Controller

図1　ビルファシリティネットワークのイメージ

なゾーニング等よる「強い物理セキュリティ環境」と人の運用により基本的なトラストが構成されていると考えられます。図1の例では、空調の制御に使われる防災センターとサーバ室間のビルオートメーションシステムのネットワークに、HMI（Human Machine Interface）としてPCのコンソールが接続されています。多くの場合、このHMIへのログインにはパスワードが必要になり、また、このPCから他の機器への通信ではBACnet等の標準化されたプロトコルが利用されていますが、そこには暗号技術による認証等は限定的にしか実装されていないのが実情のようです。そのため、このビルオートメーションシステムのネットワークを守るためには、物理的にネットワークを隔離する「物理セキュリティ環境」を構築する必要があります。そして、この物理セキュリティ環境によって隔離されたネットワークは「トラステッドネットワーク」と呼ばれています。

こうした状況の中、近年、重要インフラの制御システム、制御ネットワークへのサイバー攻撃が現実のものになりつつあり、それには以下のような背景があると考えられます。

(1) 重要インフラにおける制御システムの標準化、汎用化、コモディティ化
(2) 重要インフラの制御システムにおける様々な情報連携の要求
(3) 制御システムへの攻撃手法等の拡散

従来からの重要インフラにおける制御システムのクローズドネットワーク／トラステッドネットワークにおいては、隔離されたネットワークがそのセキュリティの前提になっていたため、そのボーダ（物理的なボーダ＆論理的なボーダ）を突破されると非常に脆弱という問題が浮上しています。

こうした問題に対応する動きの一つに、「日本データセンター協会」と「東京大学グリーンICTプロジェクト」が共同で設立し、筆者も副査として活動している「ファシリティ・インフラＷＧ[2]」の活動があります。この「ファシリティ・インフラWG」では、ビルオートメーションシステムの一層の活用を目指し、データセンターをこうした技術の先進的利用者と位置付け活動しています。

ファシリティ・インフラWGでは、活動を始めるにあたってビルディングオートメーション技術の導入ステージについて、図２にある3つのフェーズに分けて議論を行うことにしました。その最初のステップとして、これらのうちフェーズ１に対応したビルディングオートメーションシステムの設計・運用の為のガイド「建物設備システムリファレンスガイド [3]」(以下、リファレンスガイド)を2015年12月、内部向けに発行しています。

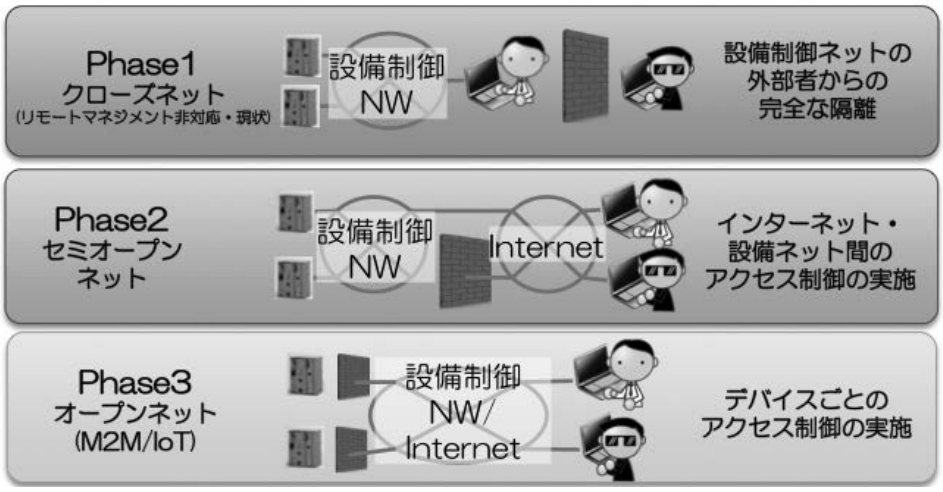


図2　ビルファシリティネットワークの３つのフェーズ

リファレンスガイドでは、ビルオートメーションシステムのネットワークを適切に外部から隔離することによって、システムのトラストを確保することを目指しています。そのため、リファレンスガイドで紹介しているセキュリティ管理策の内容は、適切な物理的ボーダー設計・構築方法や、その物理セキュリティを担保する運用方法となっています。このようなボーダーによる区画は、その構築・運用が比較的容易ではあるものの、前述したようにボーダーを突破されると非常に脆弱であるという課題があり、また、運用時における自由度にも課題があります。

そこで、フェーズ3において目指されているのが、より発展的なビルディングオートメーションシステムのあり方として「物理セキュリティ環境によるトラスト」だけに頼らない「暗号技術によるトラスト」の実現を目指したビルディングオートメーションシステムということになります。そして、図2において示したように、フェーズ3のビルディングオートメーションシステムはまさしくIoT時代におけるビルディングオートメーションシステムと言えるものになります。

3. IoT における暗号技術によるトラスト

センサーやアクチュエータ等のIoTデバイスとネットワークが、物理セキュリティ環境に依存しない場所おいて動作可能となると、それは、様々なイノベーションをもたらすと考えられます。そして、その際「物理セキュリティ環境によるトラスト」に代わって必要になるものが、「暗号技術によるトラスト」であると言えます。

ビジネス／サービスの観点から見たIoTシステムでは、様々なステークホルダーも含めた信頼関係（トラストモデル）を構築する必要があります。この信頼関係の構築は、主に暗号技術で利用される暗号鍵の関係性等により実現します。こうしたことも含めて、暗号技術は、IoTのセキュリティだけではなく、IoTにおけるビジネス自体の実現またはIoTによるイノベーションにとって必須な技術であると考えられます。

図3は、IoTではなく、現状のインターネットサービスのイメージで、ビジネスレイヤーにおいて顧客とサービス間のトラストをつくるために実際はどのような仕組みが取り入れられているかを説明した図です。インター

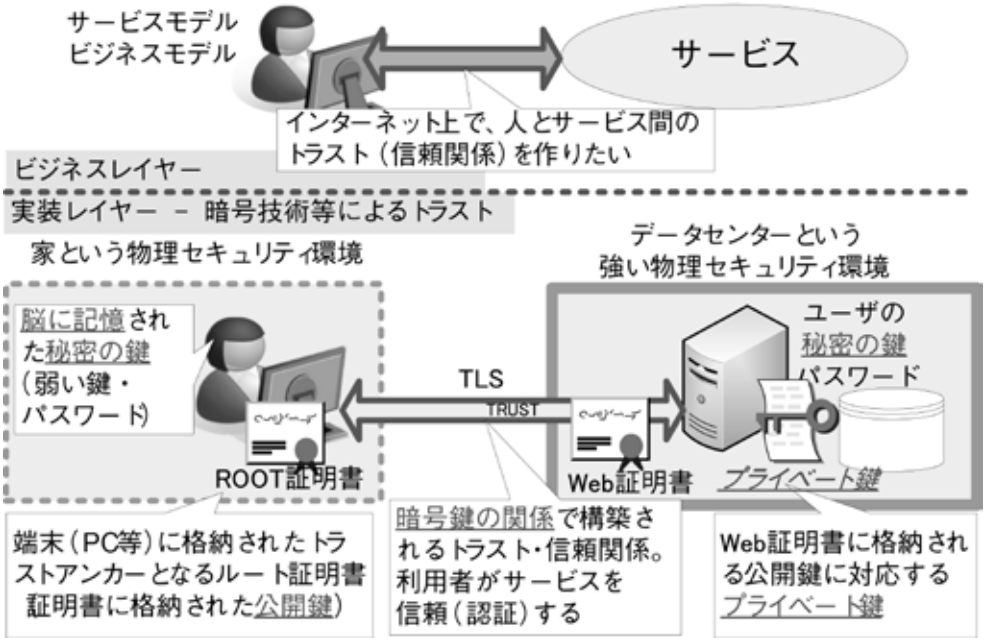


図3　インターネットにおけるサービスと暗号技術

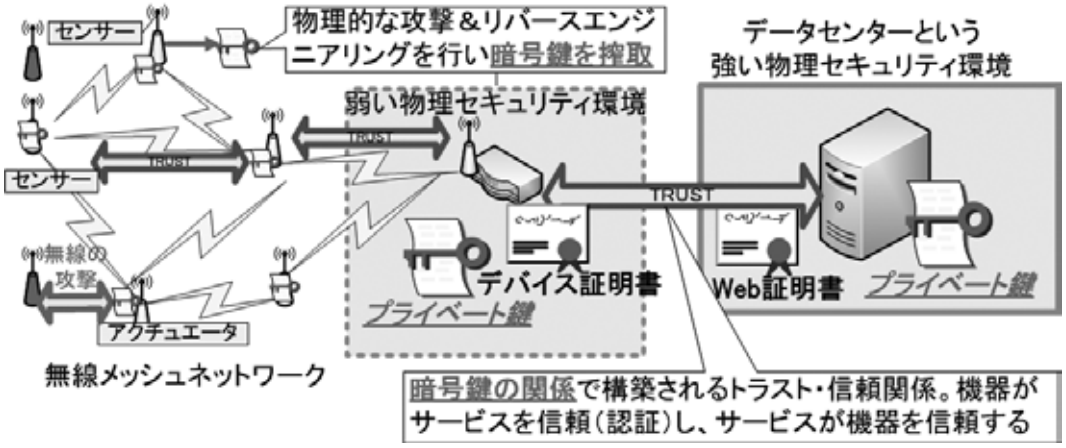


図4　IoT サービスと暗号技術

ネット越しのサービスにおいて、ビジネスレイヤーにおける信頼関係は、暗号鍵の配置等により決定される暗号技術によるトラストにマッピングされます。

このように、インターネット上のサービスにおいて、暗号技術はごく普通に利用されていますが、トラストは暗号技術だけで達成されている訳ではありません。例えばパスワードというものは人の脳に記憶された秘密の鍵を使います。また、PCは、オフィスといった物理セキュリティ環境に設置されます。センター側の暗号鍵にしても、それは（情報システムの）情報セキュリティだけで守っているわけではなく、物理セキュリティ環境でも守っている訳です。

これに対して図4は、IoTサービスをイメージした例になります。大量のIoTデバイスを接続するラストワンマイル、ラストワンメートルにおいて、その設置の自由度等の理由により無線通信を利用する場合、物理セキュリティを施すことが難しい為、必然的に暗号技術によるトラストが重要になります。また、IoTデバイスが、「弱い物理セキュリティ環境」において多く利用されることを想定した場合、物理セキュリティ環境も含めた「暗号鍵」の保護に代わって、IoTデバイス自身のハードウェアによる「暗号鍵」の保護の重要性が浮上します。さらに、数百億のIoTデバイスを想定した場合、その鍵管理等を人の記憶に頼ることはできませんから、そのためにもIoTデバイスに対した発行されるクレデンシャル管理や暗号鍵管理のための技術も非常に重要な役割を果たします。

IoTデバイスはセンサー、アクチュエータを含んだよりインテリジェントなデバイスが使われると想定されますが、これまで説明してきたように、物理セキュリティ環境の依存性が少ない環境の利用がより進むことも想定されます。現時点でそのような「弱い物理セキュリティ環境」で利用されている代表的なデバイスとしては、交通カードなどのICカードがあげられます。IoTデバイスにおいても、ICカードと同様に物理的攻撃に強い耐タンパーなセキュアエレメントと、そこに格納された暗号鍵やクレデンシャルなどから構成されるIoTデバイス自体のハードウェアセキュリティが非常に大きな意味を持ちます。

4. 車におけるトラストのパラダイムシフト

「物理セキュリティ環境によるトラスト」から、「暗号技術によるトラスト」へパラダイムシフトが起こりつつあるものの一つに自動車があります。

現在の自動車は、排気ガス規制をクリアするためのエンジン制御に始まり、車両姿勢安定化システム、自動ブレーキシステム等、自動車の多くの制御がECU(Electronic Control Unit)により実現されています。そして現在では、自動運転等を巡って熾烈な開発

競争が起きています。また、利用者ニーズに対応するビジネス戦略のようなところでも、いろいろなITサービスと自動車をつなぎたい、利用者のさまざまなITデバイスを自動車につなぎたいといった要求が高まっています。

従来からのECUおよびECUを繋ぐ車載LANは、重要インフラの制御ネットワークと似た性格がありました。すなわち、車載LANは、車内という閉じた物理セキュリティ環境で守られたクローズドネットワークであるという前提で設計され、ECUに関する多くのセキュリティも、設計の秘密で多くが守られてきたところがあります。

こうした状況に対して「つながることにより価値を高める」という要求を満たすために、車の外部的にも、車の内部的にも、デジタルデータの連携やECUの連携による制御の要求が高まっています。こうしたことから、車載LAN、ECUなどの状況が大きく変化しつつあり、それに対応するために、暗号技術によるトラストが求められるようになって来たと言えます。

「暗号技術によるトラスト」の観点から見たECU・車載LANの理想的な実装は、設計の秘密が最小限であり、暗号鍵が格納された耐タンパーなセキュアエレメントが個々のECUに格納されたものになります。そして、自動車がユーザーの手に渡った後でもECU自身が持つセキュアエレメントに格納された信頼の起点（Root of Trust）を元に、様々な外部からアクセス時のアクセス管理・権限管理や、ECU自体のプログラム管理（例えばコード署名の検証）がおこなわれることになります。ECU外部との信頼関係に基づいたアクセス管理では、車載LANを介して他のECU等との信頼関係や、ECUを介した通常時における外部との信頼関係に加えて、車検時や故障時にディーラーでおこなわれるような車およびECUの保守時のアクセス管理も重要になります。

この車およびECUの保守時のアクセス管理の問題は、多くの重要インフラの制御システム等も同様の課題を抱えています。自動車も重要インフラも、利用者および周囲の人間の生命の安全に重大な影響を及ぼす可能性があるため、様々な場所での保守やリモート保守の仕組みが不可欠となります。しかし、このリモート保守回線や保守ポートがサイバーセキュリティ的にはバックドアになっている場合が少なくなく、これが新たなサイバー攻撃の脅威となっています。

こうした課題に対応するECUのセキュリティ要件は、様々なところで議論されています。例えば、欧州の新しいR&DフレームワークHorizon 2020のプロジェクトであるSHARCS (Secure Hardware-Software Architectures for Robust Computing Systems) プロジェクト[4]において取りまとめられた要求があります。表1は、このプロジェクトが2015年12月に公開した報告

表1 自動車の ECU における権限管理

番　号	ロール	権限レベル	権　限
ユーザロール１	ECU 製造者	高い	ECU 自体へのアクセスとアップデート
ユーザロール２	自動車メーカー		各装置へのアクセスとアップデート
ユーザロール３	修理工場		自動車メーカーから配布されたツールをもとに各装置へのアクセスとアップデート
ユーザロール４	検査機関 / 警察		OBD ポートから各装置の状態の読み込み
ユーザロール５	オーナー / 運転手	低い	アクセス権なし

Horizon 2020 Program, SHARCS(Secure Hardware-Software Architectures for Robust Computing Systems), Deliverable D2.1, “SHARCS Applications and framework requirements for secure-by-design systems” から抜粋・訳

書[5]で示されたECUのECU外部からのアクセス権限リストになります。この表からも分かる通り、1台の自動車に非常に多くののECUが搭載される中、その中の1台のECUでさえも数多くのクレデンシャル管理・アクセス権限管理が必要になります。

以上で説明した「物理セキュリティ環境によるトラスト」から「暗号技術によるトラスト」へのパラダイムシフトは、今後、自動車に限らず様々な業界に波及し、それが今後の社会を支えるIoTシステムとなって行くと考えられます。

5. おわりに

本稿では、IoTデバイス、IoTシステムにおける暗号技術によるトラストの重要性を中心に説明してきました。暗号技術によるトラストは、IoTのセキュリティのベースとなるものであると同時に、IoTビジネス、サービスのベースとなるものです。

しかし、そもそもリソースが限られるIoTデバイス等に暗号技術を実装していくのは容易ではありません。IoTデバイスの省電力等の要求や、制御の時間等の要求から軽量な暗号アルゴリズムや軽量な暗号プロトコル、低遅延な暗号アルゴリズム等が必要になる場面も考えられます。IoTサービスの運用面から見た場合の課題は、なんと言っても大量のIoTデバイスに対応する大量の暗号鍵管理（暗号鍵の配置展開）をどのように行うのか等があります。このようにIoTにおける暗号技術は、非常に多くの技術的なチャレンジが必要な分野になります。

紙面の関係等もあり、今回は、暗号技術によるトラストを実現するための技術課題等は十分に説明できませんでしたが、まずは、暗号技術によるトラスト自体の重要性についての理解の助けに多少でもなれば幸いです。

参考資料

[1] 第2回 CRYPTREC の在り方に関する検討グループ　資料
http://www.meti.go.jp/policy/netsecurity/cryptrec_hp02.pdf

[2] データセンター設備のサイバーセキュリティ対策に向けた活動開始～「ファシリティ・インフラWG」をキックオフ
http://www.jdcc.or.jp/news/article.php?nid=eccbc87e4b5ce2fe28308fd9f2a7baf3&sid=108

[3] 建物設備システムリファレンスガイド 第1版、日本データセンター協会＆東大グリーン ICT プロジェクト
（非公開）

[4] SHARCS Secure Hardware-Software Architectures for Robust Computing Systems
http://www.sharcs-project.eu

[5] Deliverable D2.1: SHARCS Applications and framework requirements for secure-by-design systems
http://www.sharcs-project.eu/m/filer_public/39/f7/39f7a59a-c305-412d-9ce0-480df1d2ac50/sharcs-d21.pdf

JNSA ワーキンググループ紹介

社会活動部会

株式会社ラック　部会長　丸山　司郎
株式会社NTTデータ　副部会長　西尾　秀一

「社会活動」という定義は様々ありNPOの活動そのものが社会活動とも言えるわけですが、JNSA社会活動部会はその前身が「政策部会」であったことからもわかるとおり元々は、我が国のサイバーセキュリティ戦略など、政府機関や行政機関が推進するサイバーセキュリティ政策に対して、民間のセキュリティ専門家およびIT専門家の立場から積極的に提言活動を行っていこうという目的から設立された部会です。現在は、その活動の範囲を拡げ、メディア・イベント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の社会的活動全体を推進するための様々な活動に取り組んでいます。

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ています。

■ 2015年度の活動実績

今年はJNSA設立15周年ということもあり、特に積極的な活動に取り組んできました。

(4月)
・新部会長・副部会長決定
・会員内セキュリティ情報共有の仕組みであるJNSA CERCの検討開始

(5月)
・フェロー制度の検討開始
・15周年記念地方セミナーの検討開始

(6月)
・総会においてJNSA CERC発足を宣言
・15周年記念論文募集開始
・日本年金機構の事案を受け、記者懇談会「サイバー攻撃を受けた際の対応について」を開催 [25日]

(7月)
・米国輸出管理規制パブコメ（ワッセナーアレンジメント）への意見提出
・ライトニングトーク（LT）大会夏祭りを開催[31日]

(9月)
・15周年記念地方セミナーとして鹿児島セミナー開催 [4日]
・経済産業省との意見交換会開催 [25日]
・岡山セミナー開催 [28日]

(10月)
・総務省との意見交換会開催 [8日]
・15周年記念イベント(NSSF-15、記念論文表彰、フェロー認定およびパーティ)開催 [15日]

(11月)
・未来予測検討PJの成果として「サイバーセキュリティ2020 脅威の近未来予測」を刊行 [6日]
・サイバーセキュリティ月間官民連携プロジェクト検討開始
・札幌セミナー開催 [17日]
・大阪セミナー開催 [26日]

(12月)
・沖縄セミナー開催 [17日]
・ワッセナーアレンジメントに関する経済産業省等との意見交換会開催 [24日]

(1月)
・LT新年会を開催 [7日]
・サイバーセキュリティ月間攻殻機動隊コラボ特設サイト公開[29日]

(2月)
・金沢セミナー開催 [22日]

(3月)
・サイバーセキュリティ月間攻殻機動隊コラボイベントを秋葉原で開催 [5日]

■ 部会メンバー募集中

2015年度の活動をご覧いただいてわかるとおり、本部会の活動は当初目的であったパブコメ対応や政府機関等への提言に留まらず、日本社会が直面しているセキュリティ上の課題に対して、内外の関係者と共に様々なアプローチで解決の方向性を見出そうという議論を交わす場となっています。単独の企業ではなかなか取

り組み事が難しい課題に対しても、15年の間にJNSAが築いてきた社会的な信頼性や認知度を背景に、政府機関や国内外の関連団体、記者などとの直接対話が可能な活動が本部会の魅力だと思います。是非、会員企業の皆様におかれましても、本部会への参加メンバーの派遣をご検討いただければ幸いです。

「君、良い腕をしているな。今から社会活動部会の仲間になれ！」

1月　LT 新年会の様子

1月　LT 新年会討論会の様子

■ 社会活動部会メンバーリスト

氏名	社名
部会長　丸山　司郎	(株)ラック
副部会長　西尾　秀一	(株)NTTデータ
中山　貴禎	(株)アズジェント
佐藤　一裕	アドソル日進(株)
野田　俊夫	アドソル日進(株)
二木　真明	アルテア・セキュリティ・コンサルティング
菅野　泰彦	アルプス システム インテグレーション(株)
進藤　剛洋	(株)インフォセック
樋口　健	(株)インフォセック
堀江　徹	ウォッチガード・テクノロジー・ジャパン(株)
根津　研介	NTTデータ先端技術(株)
岡庭　素之	キヤノンITソリューションズ(株)
秋山　卓司	クロストラスト(株)
内山　公雄	KPMGコンサルティング(株)
菅野　誠仁	セコムトラストシステムズ(株)
唐沢　勇輔	ソースネクスト(株)
下村　正洋	(株)ディアイティ
桑原　和也	デジタルアーツ(株)
古川　勝也	Secure Works Japan (株)
小屋　晋吾	トレンドマイクロ(株)
中島　大輔	日本アイ・ビー・エム(株)
徳田　敏文	日本アイ・ビー・エム(株)
高橋　正和	日本マイクロソフト(株)
大和　敏彦	日本ラドウェア(株)
津金　典子	日本ラドウェア(株)
辻　秀典	ネットワンシステムズ(株)
丹野　隆志	富士通(株)
小川　博久	みずほ情報総研(株)
冨田　高樹	みずほ情報総研(株)
飛田　孝幸	三井物産セキュアディレクション(株)
西本　逸郎	(株)ラック

JNSA ワーキンググループ紹介

IoT セキュリティ WG

株式会社カスペルスキー
WG リーダー　松岡　正人

IoT セキュリティWG は、コンシューマユーザー向けの製品やサービスの開発をおこなう開発者および企業の方に、最低限知っておいていただきたい事柄をまとめたセキュリティガイドの作成を進めています。2014 年の立ち上げからすでに2年余り経ち、わずかな間に世の中は大きく変化してIoTという言葉がいままで想像もしなかった分野や製品に対して使われるようになりました。

便利さや今後のビジネスの拡大に対する期待と呼応するように、そのセキュリティやプライバシーに対する不安の声も拡大していますので、セキュリティ弱者となりがちな一般の方々により安全にIoTを通じてネットワークやInternetの利便性と効果を得ていただくために、まず、提供する側が対処すべき事柄や、対応、準拠すべき標準などについての知識を得るための基礎的な資料となるべく、WGメンバー一同で作成を進めつつ、新しい規格や仕様、標準化の流れ、あるいは新たに実現した技術や、登場した製品などについて、実際に利用するか開発された方々との議論を通して知見を広め、私たち自身が納得できるものを発行できればと考えています。

それでも、この2年余りの世界の変化には驚くばかりです。世界中でIoT でビジネスを推進するためのコンソーシアムや標準化団体が林立して、主導権の奪い合いが激化しています。開発用の端末も数百円で入手出来る時代となり、誰でも簡単にネットワークに繋がる機器を作って動かすことができるようになり、3Dプリンターと組み合わせることで製品開発は企業から個人の手に移り始めています。年少の女の子向けのバービー人形に会話する機能が搭載され、ユーザーからプライバシーやセキュリティの問題を指摘され、エンターテイメントシステム経由で乗用車がハッキングされる様子がYoutubeで注目を集めただけでなく、お茶の間のニュースで流れ、いままでは便利だと思っていたすべてのモノがつながる世界の到来はかならずしもバラ色の未来ではないということをメディアも伝え始めています。しかし、対策はほとんど語られていません。

IoTという考え方は、ネットワークがすべての電子デバイスに浸透し、いままで電子デバイスが利用されなかった領域でも使われることによって、より生活しやすく、効率が良い生活環境が得られるようになることを想定して語られることが多いのですが、裏を返せば、それらの仕組みを悪意ある人たちが別の目的で利用することのないようにセキュリティを効果的に実装する必要があるのです。

しかし、家電などコンシューマ向けの製品は価格や耐久性、デザインや性能を語られることはあっても、セキュリティという指標で製品の品質や素晴らしさを語られることはありませんでした。今後、IoTという考え方が浸透することで、その表現や言葉は変化していったとしても、これからのIT 技術は生活や社会の仕組みとつながることを前提として、より簡潔で堅牢なアーキテクチャや仕様に基づいた仕組みを実現するために最適化、再構築されていくのではないかと思います。そして、セキュリティはかならず幾重にも張り巡らされたIoT ネットワーク、より安全な生活インフラのために欠かせないものなのです。

そのために、まずは開発者に、そして次は利用者にIoT デバイスのセキュリティについて正しく理解してもらうことで、みんなが家庭の中にある様々な機器のセキュリティに関心を持ち、適切な対処ができる社会を実現することができるのではないかと期待しています。IoT で繋がることのメリットを最大限に得ることのできる、より良い社会の実現に向け、なにがしかのお手伝いができることを願っています。

■「IoT セキュリティ WG」メンバー一覧

名前	会社名
リーダー　松岡　正人	(株) カスペルスキー
武田　洋介	(株) アイピーキューブ
中原　歌織	アドソル日進 (株)
高木　昌彦	(株) アピリッツ
作本　直樹	アライドテレシス (株)
和田　弘之	アライドテレシス (株)
二木　真明	アルテア・セキュリティ・コンサルティング
手塚　信之	SCSK (株)
境　　稔	SCSK (株)
玉木　誠	SCSK (株)
亀田　勇歩	SCSK (株)
小川　朝也	NTTソフトウェア (株)
戸田　勝之	NTTデータ先端技術 (株)
近藤　伸明	(株) 神戸デジタル・ラボ
松本　悦宜	(株) 神戸デジタル・ラボ
久保　智夫	(株) サーバーワークス
高橋　大成	(株) サーバーワークス
有村　浩一	JPCERTコーディネーションセンター
満永　拓邦	JPCERTコーディネーションセンター
阿部　真吾	JPCERTコーディネーションセンター
洞田　慎一	JPCERTコーディネーションセンター
細田　将	セコム (株)
鈴木　和之	綜合警備保障 (株)
藤川　真樹	綜合警備保障 (株)
相原　弘明	(株) ソリトンシステムズ

名前	会社名
半田　富己男	大日本印刷 (株)
中村　亮大	大日本印刷 (株)
林　　憲明	トレンドマイクロ (株)
酒井　美香	日本IBMシステムズ・エンジニアリング (株)
杉浦　昌	日本電気 (株)
島　　成佳	日本電気 (株)
関　　徳男	日本電気 (株)
長坂　啓司	日本プロセス (株)
瀬田　晃彦	日本ユニシス (株)
福田　尚弘	パナソニック (株)
堀部　千壽	パナソニック (株)
武田　一城	(株) 日立ソリューションズ
尾崎　誠	ユニアデックス (株)
三池　聖史	ユニアデックス (株)
荒川　一之	ユニアデックス (株)
東海林　昌幸	(株) ラック
山下　勇太	(株) ラック
川上　昌俊	(株) ラック
篠原　崇宏	(株) ラック
鈴木　翔	(株) ラック
又江原　泰彦	(株) ラック
鵜山　通夫	サブスクライバ
古城　隆	サブスクライバ
兜森　清忠	オブザーバ
桐山　隼人	オブザーバ

JNSA ワーキンググループ紹介

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

富士通関西中部ネットテック株式会社
WG リーダー　嶋倉　文裕

■ 13 年ぶりの改版

JNSAでは情報セキュリティポリシーサンプル0.92a版を2002年に公開しました。公開から12年以上の間に、スマートデバイス、クラウド、SNSといった新しい技術やサービスの登場、国際標準のISO/IEC27001：2013、ISO/IEC27002：2013の更新など、大きな変化がありました。そこでJNSA西日本支部では、これまでの活動から、リスク認識と対策導入後のその効果や運用状況のチェックの重要性を痛感していたこともあり、情報セキュリティポリシーサンプルの改版に取り組むこととしました。今回の改正では特にリスク認識と、対策の効果や運用状況のチェックをサンプルに盛り込むことに注力しています。

改版した情報セキュリティポリシーサンプルは4月に1.0版として一般公開の予定です。

■ 概要

情報セキュリティポリシーサンプル1.0版の読み手の対象者と文書一覧を示します。

対象者	情報セキュリティポリシーサンプル　1.0版
全員	①情報セキュリティ基本方針 情報セキュリティ方針
	③外部委託先管理規程
	⑧セキュリティインシデント報告･対応規程
管理者	②人的管理規程
	④文書管理規程
	⑤監査規程
	⑥物理的管理規程
	⑦リスク管理規程
	⑨システム変更管理規程
	⑩システム開発規程
	⑪システム管理規程
	⑫ネットワーク管理規程
利用者	⑬システム利用規程
	⑭スマートデバイス利用規程
	⑮SNS利用規程

今回の改版のポイントは以下のとおりです。

(1) 0.92a版の踏襲

1.0版の作成にあたり、0.92a版の文書を踏襲することを基本としています。ただし、以下の3点を考慮しています。

① ISO/IEC27001：2013付属書Aとの対応付けが可能なものはその明示
② 記載する対策はISO/IEC27002：2013の実施の手引きレベルを参考
③ 管理者、利用者を分離した全体の構成の見直し

(2) 情報セキュリティ対策の日々の運用を重視

日々の情報セキュリティ対策の運用が適切に実施されていることを確認するプロセスを確立するための項目を規程に盛り込みました。

(3) 主語、対象、役割を明記

1.0版では、できるだけ主語、対象、役割を明記することとしました。誰が（責任者、管理者、利用者）、何を行うのか、どういう責任（行為、記録、確認･承認）を果たすのか、を明確にすることとしました。

(4) リスクの認識

リスクの認識は、経営方針、情報セキュリティ基本方針をふまえ、組織を取り巻く内外の状況を把握し、自組織に適したセキュリティ要件・セキュリティ管理策を決定する上で重要です。

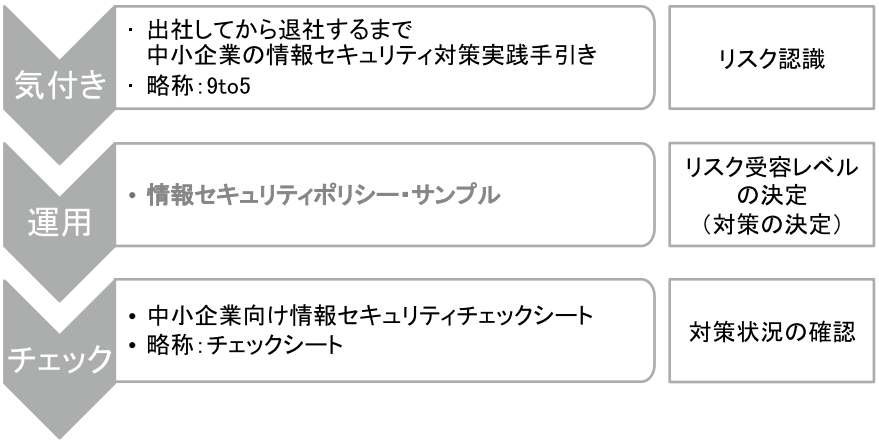
このため、改版した情報セキュリティポリシーサンプルの4月での一般公開時に合わせて公開する「情報セキュリティポリシーサンプル改版（1.0版）概要」には、リスク認識についての説明を記載予定です。

■ これまでの JNSA 西日本支部成果物との関係

JNSA西日本支部では、これまで「中小企業向け情報セキュリティチェックシート」、「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」を作成してきました。

今回、改版した情報セキュリティポリシーサンプルとこれまでの成果物には次ページの相関関係（図1）があります。

図 1 成果物の相関図



組織は、これらのJNSA西日本支部の成果物を活用することで情報セキュリティを自律的に推進することができ、「JNSAソリューションガイド」を合わせて活用することにより、具体的な情報セキュリティ対策の実現の検討が可能になります。

西日本支部では、「中小企業向け情報セキュリティチェックシート」、「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」、「中小企業向け情報セキュリティポリシーサンプル」の3部作の作成に伴い、休止していた「中小企業向け情報セキュリティチェックシート」、「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」の両WGと、「中小企業向け情報セキュリティポリシーサンプル」WGを終了します。

4月以降のWG活動については、新たな取り組みを検討中です。「参加したい」「ちょっと興味がある」という方がいらっしゃいましたら、お気軽にお声掛けください。

■ WG メンバー

井上　陽一	JNSA顧問
大財　健治	（株）ケーケーシー情報システム
河野　愛	（株）インターネットイニシアティブ
久保　智夫	（株）サーバーワークス
久保　寧	富士通関西中部ネットテック（株）
嶋倉　文裕	富士通関西中部ネットテック（株）
西川　和予	（株）GENUSION
元持　哲郎	アイネット・システムズ（株）
吉崎　大輔	日本電気（株） （現、NECソリューションイノベータ（株）在籍）

改訂にご協力頂いた皆様
青木　茂
今村　武司
宇佐川　道信
塩田　廣美

会員企業ご紹介㊶

株式会社神戸デジタル・ラボ

http://www.kdl.co.jp/

株式会社神戸デジタル・ラボ（KDL）は、Webビジネスを中心として、情報システム開発・運用・保守サービスのほか、攻める先端技術開発や、守る情報セキュリティソリューションを提供する独立系ベンダーです。業種や業態によって企業のIT戦略もさまざまですが、人や企業とのコラボで生まれるITを「創」、「攻」、「守」で、お客様をサポートしています。

急増するサイバー攻撃に立ち向かう。企業の信頼を守る砦!

コンピュータやネットワークの不正侵入による破壊、改ざん。企業の信頼を一瞬のうちに失墜させる、このようなサイバー攻撃が急増しています。

Proactive Defense は、セキュリティの最前線を知るプロフェッショナルによる充実のサービス。ホワイトハッカーが率先する万全のチーム体制、納得のプロセス、そして最高の品質とリーズナブルな価格で、見えないサイバー攻撃に対するガードを固めます。

Proactive Defense 情報セキュリティサービス

http://www.proactivedefense.jp/

お問合せ	株式会社神戸デジタル・ラボ　セキュリティソリューション事業部 TEL:0120-996-535　e-mail:info@proactivedefense.jp

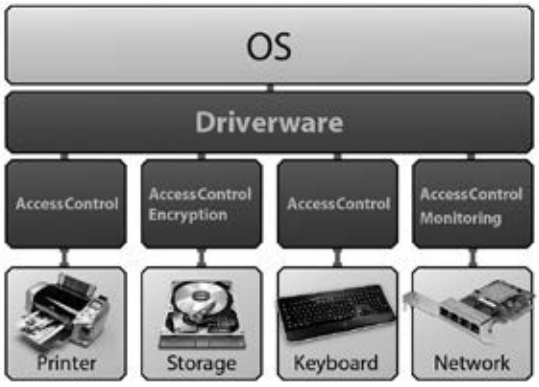
サイエンスパーク株式会社

http://www.sciencepark.co.jp/

1994年創業、PCおよび専用システムの周辺機器向けデバイスドライバの開発で培ったハードウェア制御技術、ドライバ技術をベースにした情報セキュリティ製品の開発・販売を行っています。独自技術「Driverware セキュリティSDK」は多数のセキュリティ製品開発会社に採用されています。

【Driverware セキュリティSDK概要】

DriverwareセキュリティSDKは情報セキュリティシステムを開発する際にご利用頂ける開発キットです。
本SDKを利用すると、独自の情報セキュリティシステムを簡単に開発できます。



【Driverware セキュリティSDK 特徴】

・アプリケーションに依存しない
・どんな経路でアクセスしても制御可能
・アプリケーションより優先して動作
・メンテナンスが簡単

【Driverware セキュリティSDK機能】

・ネットワーク制御 ‥ IPアドレス、ポート単位でのTCP/UDP通信制御、ログ収集
・アクセス制御 ‥ ファイル単位で読込みと書込みの許可、禁止を設定
・ログ収集 ‥ ファイル単位でのログ収集
・認証機能 ‥ ファイル単位での持ち出しを検知し第3者による許可、禁止を指示
・ライティング制御 ‥ CD/DVD/BDへの書込み許可、禁止
・印刷制御 ‥ 印刷の許可・禁止・ログ収集
・外部デバイス制御 ‥ iPhone、Android端末、その他携帯端末の制御
・暗号 ‥ ファイル単位でのリアルタイム暗号・復号
・その他 ‥ キーボード等のHID (Human Interface Device) 制御

【対応OS】

・Windows Vista / Windows 7 / Windows 8 / Windows 8.1 / Windows 10

お問合せ	サイエンスパーク株式会社　セキュリティ製品営業課　TEL 046-255-2544 〒252-0024 神奈川県座間市入谷3-1649-2

パロアルトネットワークス株式会社

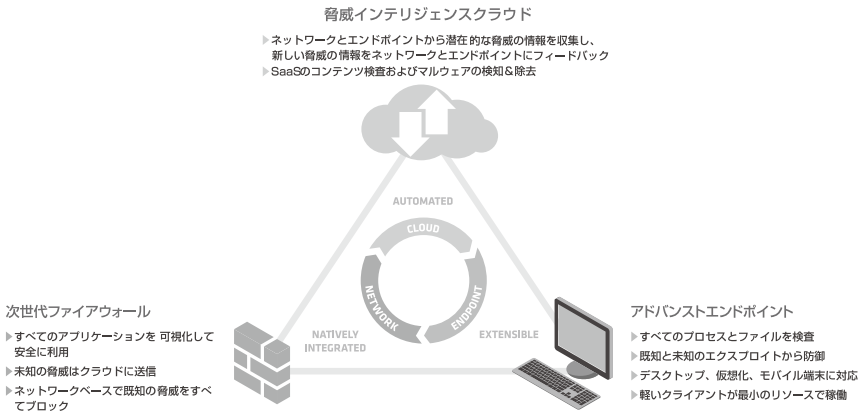
https://www.paloaltonetworks.jp/

次世代セキュリティ企業、パロアルトネットワークス

パロアルトネットワークスは、全世界で26,000社を超える顧客を持つ、サイバーセキュリティの新時代をリードする次世代セキュリティ企業です。サイバー攻撃による被害が増加する昨今、企業や組織の損失を防ぐには、各セグメントにおけるセキュリティを多層的に自動連携させる、パロアルトネットワークスの『次世代セキュリティプラットフォーム』が有効です。

次世代セキュリティプラットフォームでお客様のビジネスを防御

パロアルトネットワークスの提供する『次世代セキュリティプラットフォーム』は、次世代ファイアウォール、脅威インテリジェンスクラウド「WildFire」、アドバンストエンドポイント「Traps」で構成されます。ネットワーク、クラウド、エンドポイントにおける最新のセキュリティ機能を相互連携させ、標的型攻撃を含む高度で巧妙なサイバー攻撃からお客様のビジネスを守ります。



拡張し続ける次世代セキュリティプラットフォーム

パロアルトネットワークスは、2015年に脅威情報の相関データを実用化するサイバー脅威インテリジェンスサービス「AutoFocus」を日本市場で提供開始し、2016年前半より、企業や組織内での利用も増えているSaaSアプリケーションの安全利用を実現するセキュリティサービス「Aperture」を提供予定です。パロアルトネットワークスは、最新のサイバー攻撃に対応すべく、次世代セキュリティプラットフォームのさらなる強化を進めています。

AutoFocus	Aperture
	
世界中から集められたサイバー脅威情報の相関データを提供するクラウドサービス。サイバー情報に優先度付けを行い、実用的なセキュリティ情報を提供。	利用を許可されたSaaSアプリケーションの可視化と制御を可能とするサービス。SaaSアプリケーションの可視化、分析、ポリシー制御を実現。

お問い合わせ先：パロアルトネットワークス株式会社

https://www.paloaltonetworks.jp/　Tel：03-3511-4050　Email：infojapan@paloaltonetworks.com

株式会社 PFU

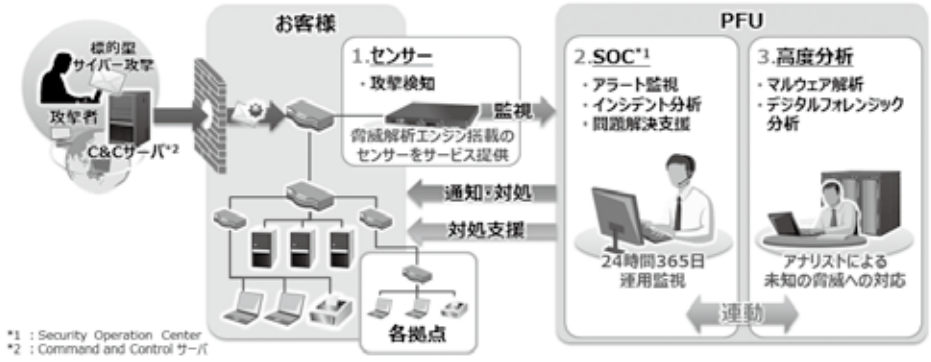
http://www.pfu.fujitsu.com

a Fujitsu company

株式会社PFUは、最先端技術の研究開発や製品提供、マルチベンダ製品の運用・保守までを一貫して行う国内唯一のセキュリティ・ソリューションベンダーです。標的型サイバー攻撃の内部対策を実現する製品や、標的型サイバー攻撃の状況を24時間365日監視を行うサービスなどを提供しています。

標的型サイバー攻撃対策支援サービス

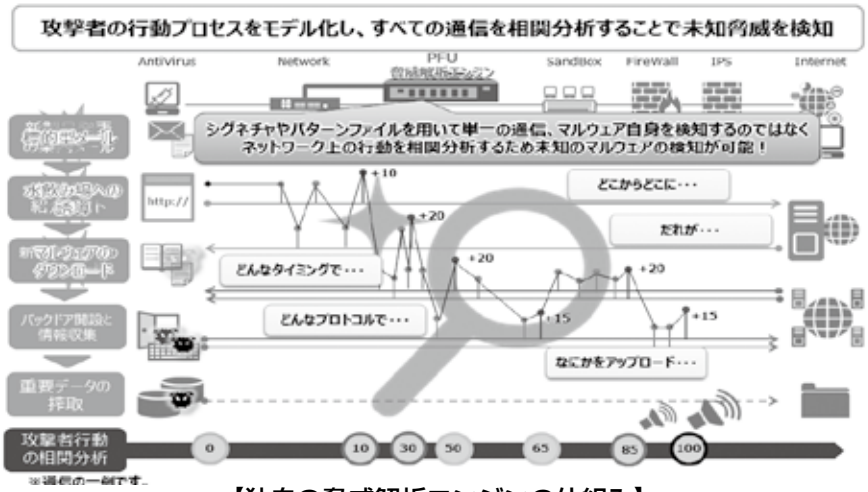
当社エンジニアがお客様に代わり、標的型サイバー攻撃の状況を24時間365日監視を行うセキュリティ運用サービスです。本サービスにより、セキュリティ運用の負担を大幅に軽減できるとともに、専門スキル不足の解消と脅威の発見から対処までの時間を大幅に短縮することが可能です。



【サービス提供イメージ】

独自技術による高い攻撃検知能力

当社独自の標的型サイバー攻撃検知技術「Malicious Intrusion Process Scan」を搭載したセンサーを導入することで、従来のセキュリティ対策をすり抜ける標的型サイバー攻撃もリアルタイムに検知し、情報漏えいのリスクを低減します。



【独自の脅威解析エンジンの仕組み】

iNetSec

お問い合わせ先：株式会社 PFU

〒220-8567　神奈川県横浜市西区みなとみらい 4-4-5 横浜アイマークプレイス

TEL：045-305-6046　　URL：http://www.pfu.fujitsu.com/inetsec/

JNSA 会員企業のサービス・製品・イベント情報

■製品紹介■

○ビジネス電話帳　ProgOffice Enterprise」

「ビジネス電話帳　ProgOffice Enterprise」は、スマートフォンの端末に情報を残さず、セキュリティ高く利用できるWeb電話帳です。電話帳情報（アドレス帳情報）や、発着信履歴、メール、SMSなどの情報を端末に残さず利用が可能です。情報を残さないだけではなく、端末認証など多要素認証も行っています。
さらに、電話帳に名刺情報や営業情報、スケジュールなどを表示し、状況確認しながら連絡できるなど業務の効率化もはかれます。

【製品情報詳細】
https://www.ntts.co.jp/products/progoffice_enterprise/

◆お問い合わせ先◆
ＮＴＴソフトウェア株式会社
ビジネスソリューション事業部
TEL: 03-5782-7347

JNSA15周年記念イベントのご報告

JNSA 事務局

JNSAは2000年4月13日に設立総会を行い発足しましたので、2015年度はちょうど15周年の節目の年となりました。10周年の時には特に大々的にイベントは行いませんでしたので、15周年はぜひ何か記念イベントをやろうということになり、社会活動部会が中心となり企画検討を行うこととなりました。

JNSA設立15周年記念イベント「Network Security Special Forum（NSSF15）」
http://www.jnsa.org/seminar/2015/nssf15/

15周年企画のメインイベントとして、日本セキュリティ・マネジメント学会(以下JSSM）と共催での論文募集とその発表の場としてJNSAの活動の振り返りも含めたJNSA設立15周年記念イベント「Network Security Special Forum（NSSF15）」（日程：2015年10月15日、会場：ベルサール飯田橋）の開催がありました。「NSSF15」では、未来を見据えるプログラムとして基調講演にマッスル株式会社玉井社長をお招きし「未来への挑戦：「人のためのロボット」の実用化」という演題でご講演いただいた他、JNSA副会長である日本マイクロソフト株式会社高橋氏による講演「セキュリティ過去と未来」で、過去～現在～未来のセキュリティ業界の振り返り、JNSAの活動の歩みと共に説明していただきました。

JNSA設立15周年記念論文 優秀論文審査発表
http://www.jnsa.org/seminar/2015/nssf15/paperaward.html

また、論文募集の一次審査を通過した4名による論文発表と最終選考もこの場で行いました。「学術論文」の部はNTTデータ金子朋子氏と東京大学川中隆章氏に、「自由形式論文」はセコム甘利康文氏とNTTデータ大谷尚通氏に発表していただきました。審査委員の方々による当日の最終審査の結果、最優秀賞は大谷氏、優秀賞が残る3名と決定し、受賞者には賞金とスポンサー賞が授与されました。

JNSAフェローの称号を贈呈
http://www.jnsa.org/seminar/2015/nssf15/fellowship.html

さらに、2015年に新たに新設したフェロー制度の第一回認定者として、JNSA設立時から長年にわたってJNSAの活動を支えてこられた顧問である井上陽一氏と大和敏彦氏の2名が決定し、記念品であるフェローバッチと認定証が贈呈されました。

そして、夜にはJNSA会員と過去から現在まで御世話になっている方々をお招きして記念パーティを飯田橋カナルカフェで開催しました。この日のために準備を行ってきた設立十五周年記念イベント実行委員メンバーの企画による、豪華景品があたるセキュリティビンゴ大会やクイズ大会、設立以来の写真の投影、そして最後には有志の協賛によるお堀での打ち上げ花火など、楽しい一夜を過ごしました。

15 周年記念パーティの風景

JNSA15周年記念企画はシンポジウムとパーティだけではありません。2015年度はJNSAの活動をアピールする地方セミナーを鹿児島、岡山、大阪、沖縄、札幌、金沢の6箇所で開催しました。セミナーのプログラムはJNSAの活動成果を主なコンテンツとしてJNSAで最も認知度が高いインシデント被害調査結果の解説やソリューションガイドサイト・理解度チェックサイトの紹介やマイナンバー対応ポータルサイトの紹介などで構成し、今まで馴染みの薄かった地方でもJNSAの活動や成果物を知ってもらうために地方へ赴き講演を行いました。JNSAでは過去にも地方でセミナーを行ってきましたが、そのほとんどは国等の委託事業によるものであり、JNSA自身の活動のPRとしてのセミナーは行っていませんでした。今回地方セミナーを行うことにより、各地域のNPOや団体、自治体等との連携がより強まり、またJNSAの活動を知ってもらうよい機会となりました。各地では終了後に地域の方々との懇親会を設けていただき心より感謝しております。毎年地方セミナーを行うのは大変ですが、せっかくできた連携の輪を今後も継続していければと思います。

JNSAのほとんどの活動は会員メンバーの自発的なアイデアや協力により運営されています。今回の企画のほとんどは社会活動部会で行いましたが、JNSAの活動に協力して下さる方々は随時募集しています。ぜひ色々なことをJNSAという場で試してみていただけたらと思っております。多くの方の活動への御参加をお待ちしています。

沖縄セミナーパネルディスカッションと終了後の交流会風景

JNSA賀詞交歓会・JNSA賞表彰式のご報告

賀詞交歓会

恒例のJNSA賀詞交歓会は、2016年1月25日（月）、東京のコートヤード・マリオット銀座 東武ホテルにて開催されました。今回は約140名の方にご参加いただき、大変盛況な会となりました。

冒頭、JNSA会長 田中英彦氏より挨拶を申し上げ、来賓としてお招きした、内閣官房内閣サイバーセキュリティセンター 内閣審議官 谷脇康彦氏、総務省大臣官房審議官 池永敏康氏、経済産業省大臣官房審議官 前田泰宏氏の各氏よりご挨拶を頂き、独立行政法人情報処理推進機構 理事長 富田達夫氏の乾杯のご発声のもと、開宴しました。

内閣官房内閣サイバーセキュリティセンター
内閣審議官　谷脇康彦 氏

総務省大臣官房審議官
池永 敏康 氏

経済産業省大臣官房審議官
前田 泰宏 氏

独立行政法人情報処理推進機構
理事長　富田 達夫 氏

JNSA 賞授賞式

しばらく歓談が続いた後、今回で10回目を迎えた毎年恒例のJNSA賞の表彰式が執り行われました。各賞の受賞者をご紹介後、田中会長から表彰状と記念の盾、副賞が授与されました。

受賞者と受賞理由は以下の通りです。受賞者の皆様、おめでとうございました。

個人の部（1件）

◇ 未来予測プロジェクトリーダーとして活動、脅威予測の書籍発行に多大な貢献

○唐沢　勇輔 氏（ソースネクスト株式会社）

東京オリンピック・パラリンピックが開催される2020年に向けた脅威予測を行ない、社会への啓発を図ることを目的とした未来予測のプロジェクトのリーダーとして書籍「サイバーセキュリティ2020 脅威の近未来予測」の発刊に尽力した。

◇ JNSAの情報セキュリティ管理体制に多大な貢献

○後藤　忍 氏（セコムトラストシステムズ株式会社）

JNSA情報セキュリティ指針及び情報資産取扱規程の策定に向けて事務局を支援し、JNSAの情報セキュリティ管理体制の構築に多大なる貢献を行った。

◇ 電子署名実証環境の整備や勉強会の開催、会員獲得でJNSAに多大なる貢献

○宮地　直人 氏（株式会社ラング・エッジ）

電子署名に関わる実証環境の整備や多数の勉強会を企画開催するとともに、会員やサブスクライバを獲得するなど、JNSAの知名度向上と活動の活性化に多大の貢献を果たした。

イベント開催の報告

ワーキンググループ(WG)の部（1件）

◇ WGの活動が協会の活性化ならびに情報セキュリティの向上に大きく貢献

○マイナンバー対応情報セキュリティ検討WG
（WGリーダー:トレンドマイクロ(株) 萩原　健太 氏/サブリーダー:デジタルアーツ(株) 松森　健一 氏）
今年度の国内の大きな関心事である「マイナンバー対応」について活発に議論を行い、「マイナンバー情報セキュリティ対策ポータル」サイトを公開した。公開後行ったセミナーでは多くの参加者を集め、その時勢に合った活動はメディアでも取り上げられ、JNSAの知名度向上、さらには社会全体における情報セキュリティ向上に寄与した。

特別賞（4件）

◇ インターネット安全教室を中心とする情報セキュリティ普及啓発活動を活発に実施することにより、広く一般社会のセキュリティ知識の向上に貢献

○特定非営利活動法人グループHIYOKO

○特定非営利活動法人スキルアップサービス
継続的に安全教室を各地域にて開催し、インターネット安全教室の普及に貢献している。

◇情報セキュリティ業界に大きく貢献

○CTF for GIRLSの運営メンバー
情報セキュリティ技術に興味がある女性を対象に、女性限定CTFワークショップを企画開催してきた。2015年には国内初となる女性限定のCTF大会を開催し、「CTF for GIRLS」を対外的にも注目を浴びる大きなイベントにすることで、JNSAの知名度向上と情報セキュリティ業界の活性化に大きく貢献した。

JNSA 賞受賞者の皆さん

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年度からは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、今年度も引き続き「インターネット安全教室」を全国で開催しました。

【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、その他各開催地大学・新聞各社・県・県警　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、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

2015年度「インターネット安全教室」開催一覧

（2016.2.15現在）

	日　程	開催地	共催団体	会　場
1	5月20日(水)	群馬	おおたIT市民ネットワーク	太田市役所セミナールーム
2	5月30日(土)	岐阜	JNSA	岐阜市消費生活センター
3	6月1日(月)	北海道	NPO法人くるくるネット	室蘭市中小企業センター
4	6月1日(月)	東京	JNSA	共立女子大学
5	6月4日(木)	東京	JNSA	昭和女子大学
6	6月6日(土)	東京	JNSA	港区立白金小学校2年生
7	6月6日(土)	東京	JNSA	港区立白金小学校5年生
8	6月12日(金)	大阪	NPO法人きんきうぇぶ	羽曳野市西浦東小学校（教職員向け）
9	6月13日(土)	東京	JNSA	中野区立新山小学校
10	6月26日(金)	群馬	おおたIT市民ネットワーク	太田市役所セミナールーム
11	7月9日(木)	岐阜	インターネット安全教室レディースチーム	垂井町立府中小学校
12	7月10日(金)	山口	NPO法人岩国パソコンの会	岩国市玖珂公民館
13	7月11日(土)	長野	上田市マルチメディア情報センター	中吉田自治会
14	7月12日(日)	秋田	NPO法人ノースウインド	ITチャオ!
15	7月16日(木)	滋賀	NPO滋賀県情報基盤協議会	甲賀市立柏木小学校
16	7月26日(日)	秋田	NPO法人ノースウインド	ITチャオ!
17	9月4日(金)	沖縄	NPO法人フロム沖縄推進機構	糸満市立西崎小学校　体育館
18	9月8日(火)	沖縄	NPO法人フロム沖縄推進機構	うるま市立中原小学校　視聴覚室
19	9月15日(火)	大阪	NPO法人きんきうぇぶ	富田林市立人権文化センター
20	9月20日(日)	秋田	NPO法人ノースウインド	ITチャオ!
21	9月25日(金)	北海道	NPO法人くるくるネット	室蘭市中小企業センター
22	9月26日(土)	島根	とっとりままくらぶ	米子コンベンションセンタービッグシップ
23	9月27日(日)	三重	PCシエル	長島総合自動車学校
24	10月6日(火)	神奈川	特定非営利活動法人 NPO情報セキュリティフォーラム	川東タウンセンターマロニエ 2階 集会室202
25	10月11日(日)	三重	PCシエル	鈴鹿工業高等専門学校
26	10月15日(木)	秋田	NPO法人ノースウインド	ITチャオ!
27	10月17日(土)	群馬	おおたIT市民ネットワーク	世良田行政センター　研修室
28	10月24日(土)	兵庫	兵庫県立大学大学院応用情報科学研究科	兵庫県立大学大学院
29	10月28日(水)	滋賀	NPO滋賀県情報基盤協議会	甲が市立小原小学校　6年
30	10月30日(金)	兵庫	沼島･かおりハートネットワーク	沼島総合センター　2階　大集会室
31	10月31日(土)	福岡	NPO法人スキルアップサービス	北九州市立大学 北方キャンパス 本館D-601 教室
32	11月5日(木)	神奈川	特定非営利活動法人 NPO情報セキュリティフォーラム	ヴェルクよこすか　6階　ホール
33	11月5日(木)	徳島	公益財団法人e−とくしま推進財団	鳴門市撫養小学校　2階　視聴覚教室①
34	11月5日(木)	徳島	公益財団法人e−とくしま推進財団	鳴門市撫養小学校　2階　視聴覚教室②
35	11月6日(金)	福岡	NPO法人スキルアップサービス	北九私立年長者研修大学校周望学舎 第4 研修室
36	11月8日(日)	秋田	NPO法人ノースウインド	ITチャオ!
37	11月8日(日)	徳島	公益財団法人e−とくしま推進財団	とくぎんトモニプラザ　4階　会議室2
38	11月9日(月)	和歌山	NPO情報セキュリティ研究所	近畿大学付属和歌山高等学校･中学校
39	11月10日(火)	兵庫	JNSA	川西市役所　消費生活センター
40	11月11日(水)	滋賀	NPO滋賀県情報基盤協議会	栗東市立治田西小学校

	日　程	開催地	共催団体	会　場
41	11月18日(水)	群馬	おおたIT市民ネットワーク	太田市役所セミナールーム
42	11月21日(土)	愛知	NPO東海インターネット協議会	オフィスオオモリ　2階会議室
43	11月24日(火)	徳島	公益財団法人e−とくしま推進財団	鳴門市立桑島小学校
44	12月3日(木)	栃木	NPO法人栃木県シニアセンター	栃木県シルバー大学校
45	12月4日(金)	長野	PCシエル(安曇野)	安曇野市穂高公民館
46	12月4日(金)	広島	福山市	福山市広瀬公民館
47	12月6日(日)	鹿児島	NPO法人鹿児島インファーメーション	鹿児島アリーナ
48	12月8日(火)	神奈川	特定非営利活動法人 NPO情報セキュリティフォーラム	川崎市多摩市民館　第1会議室
49	12月10日(木)	広島	福山市	福山市湯田公民館
50	12月19日(土)	宮城	NPO法人地域情報モラルネットワーク	一般財団法人みやぎ婦人会館　第1研修室
51	12月21日(月)	沖縄	非特定営利活動法人フロム沖縄推進機構	八重山商工高等学校
52	12月22日(火)	広島	福山市	福山市緑丘公民館
53	1月14日(木)	三重	くわなPCネット	桑名市総合福祉会館
54	1月17日(日)	福島	特定非営利活動法人日本コンピュータ振興協会	二本松市立東和小学校
55	1月17日(日)	島根	NPOプロジェクトゆうあい	松江市民活動センター　201研修室
56	1月19日(火)	沖縄	非特定営利活動法人フロム沖縄推進機構	沖縄県三重城合同庁舎
57	1月21日(木)	滋賀	NPO滋賀県情報基盤協議会	甲賀市立小原小学校　5年
58	1月22日(金)	島根	Rubyプログラミング少年団	松江市八雲社会福祉センター 「アルバホール」会議室
59	1月24日(日)	秋田	NPO法人ノースウインド	ITチャオ!
60	1月26日(火)	千葉	JNSA	船橋市立峰台小学校(児童)
61	1月26日(火)	千葉	JNSA	船橋市立峰台小学校(保護者)
62	1月26日(火)	千葉	JNSA	船橋市立峰台小学校(児童と保護者)
63	1月28日(木)	栃木	NPO栃木県シニアセンター	栃木県シルバー大学校
64	1月30日(土)	北海道	旭川情報産業事協同組合	旭川市科学館 学習･研修室
65	2月1日(月)	福岡	NPO法人スキルアップサービス	北九州市立年長者研修大学穴生学舎 3 F 大会議室
66	2月9日(火)	福岡	NPO法人スキルアップサービス	松ヶ枝南市民センター　第4会議室
67	2月10日(水)	鹿児島	NPO法人与論情報化グループ e−○k	与論町中央公民館
68	2月12日(金)	東京	NPO法人アクティブSITA	せりがや会館
69	2月13日(土)	大阪	NPO法人きんきうぇぶ	富田林市立明治池中学校
70	2月18日(木)	群馬	NPO法人おおたIT市民ネットワーク	太田市立生品小学校　体育館
71	2月20日(土)	香川	e−とぴあ･かがわ (かがわ県民情報サービス㈱)	e-とぴあ･かがわ　BBスクエア
72	2月20日(土)	北海道	北海道情報セキュリティ勉強会(せきゅぽろ)	仁々志別多目的センター
73	2月20日(土)	福岡	NPO法人スキルアップサービス	筒井諮問センター　多目的ホール
74	2月21日(日)	秋田	NPO法人ノースウインド	ITチャオ!
75	2月21日(日)	島根	NPO法人プロジェクトゆうあい	松江市民活動センター
76	2月24日(水)	神奈川	特定非営利活動法人 NPO情報セキュリティフォーラム	葉山町福祉文化会館　大会議室
77	2月28日(日)	奈良	特定非営利活動法人 なら情報セキュリティ総合研究所	生駒市北小平尾自治会館

SECURITY CONTEST (SECCON) 2015 決勝大会

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「SECCON」を継続して実施しています。

今年度はオンラインを含む6回の地方予選大会と5つの連携大会を経て、本年1月30日（土）・31日（日）にSECCON 2015を締めくくる決勝大会が開催されました。初日は学生限定の「intercollege決勝大会（学生大会）」、2日目は世界の強豪チームが出場する「international決勝大会（国際大会）」の2回に分けて実施し、「international決勝大会（国際大会）」には、日本から8チームの他、海外から米国・韓国・台湾・ロシア・ルーマニア・ベトナム・タイの計10チームが参戦する世界レベルのハッキング対決が繰り広げられました。

「SECCON 2015 決勝大会」開催概要

日　時： 2016年1月30日（土）　11:30〜17:00「intercollege決勝大会（学生大会）」
2016年1月31日（日）　10:00〜16:30「international決勝大会（国際大会）」
会　場： 東京電機大学 東京千住キャンパス 1号館 1階 100周年ホール
主　催： SECCON実行委員会（NPO日本ネットワークセキュリティ協会）
言　語： 英語・日本語

1月30日（土）の「intercollege決勝大会（学生大会）」には地方予選と連携大会を勝ち抜いた学生18チームが出場し、チームdodododoが優勝しました。31日（日）の「international決勝大会（国際大会）」では、65ヶ国、累計3,343人の中から各予選大会を勝ち進んだ18チームが一堂に集まり、その実力を競い合いました。優勝した韓国のチームCykorkinesisには、優勝特典として「DEF CON CTF 2016 finals」出場権が与えられました。

また、intercollege決勝大会（学生大会）で優勝したチームdodododoの4人のメンバーと、international決勝大会（国際大会）で健闘したTomoriNaoさん（チーム「TomoriNao」）に文部科学大臣賞が授与された他、international決勝大会（国際大会）に出場した日本チームのメンバー全員に経済産業大臣激励文が授与されました。

決勝大会の詳細結果は「SECURITY CONTEST 2015」ホームページで公開しています。
http://2015.seccon.jp/result.html

遠藤利明 東京オリンピック・パラリンピック大臣ご視察の様子

international 決勝大会の様子

事務局お知らせ
JNSA ANNOUNCE

主催セミナーのお知らせ

● PKI DAY 2016
主　催: NPO日本ネットワークセキュリティ協会
　　PKI 相互運用技術WG
日　程: 2016年4月22日（金）
会　場: フクラシア品川クリスタルスクエア

● 2015年度活動報告会
主　催: NPO日本ネットワークセキュリティ協会
日　程: 2016年6月予定

後援・協賛イベントのお知らせ

1. 第12回IPAひろげよう 情報モラル・セキュリティコンクール2016
主　催: 独立行政法人情報処理推進機構
日　程: 2016年4月1日（金）～11月30日（水）
作品募集期間: 2016年4月1日（金）～9月7日（水）

2. SECURE TOKYO 2016
主　催: （ISC）^{2} Japan
日　程: 2016年4月27日（水）
会　場: 東京電機大学

3. 自治体総合フェア 2016
主　催: 一般社団法人日本経営協会
日　程: 2016年5月18日（木）～5月20日（金）
会　場: 東京ビッグサイト

4. 第20回サイバー犯罪に関する白浜シンポジウム
主　催: サイバー犯罪に関する白浜シンポジウム
　　実行委員会
日　程: 2016年5月19日（木）～5月21日（土）
会　場: 和歌山県立情報交流センターBig・U

5. ワイヤレスジャパン 2016
主　催: 株式会社リックテレコム
　　日本イージェイケイ株式会社
日　程: 2016年5月25日（水）～5月27日（金）
会　場: 東京ビッグサイト

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。

2015年は東京オリンピック・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-CERC」を立ち上げた他、ライトニングトーク大会、JNSA十五周年記念イベント、サイバーセキュリティ官民連携プロジェクトの企画検討などを行った。

【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年先の脅威を予測検討し、書籍「サイバーセキュリティ2020 脅威の近未来予測」を2015年11月に発行した。

<成果物>

- 2015年11月 書籍「サイバーセキュリティ2020 脅威の近未来予測」発刊

【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)

IPA(情報処理推進機構)からの委託事業「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)

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。

<成果物>

- 2014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)

活動休止中。

【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、集まった知見はセミナー等で発表・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

＜成果物＞

・ 2015年5月　書籍「組織で働く人間が引き起こす不正・事故をどう防ぐか『内部不正対策14の論点』」発刊

【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。

＜成果物＞

・ IoT調査レポート

【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）

情報集約チーム・構築検討チーム・情報セキュリティ対策チームの3つのサブチームに分かれて検討を行い成果物「マイナンバー対応のための情報ポータル」を制作し9月に公開。

＜成果物＞

「マイナンバー対応のための情報ポータル（企業向け）」

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い。

【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。

2015年は7月13日に日韓情報保護シンポジウムを韓国ソウルで開催した。

【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。2014年度より継続して経済産業省委託事業PDF長期署名プロファイルに関する国際標準化事業を実施している。

＜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。

＜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。2015年4月「講師紹介サイト」を公開。

【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）

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。

＜成果物＞

- 2016年1月に新規問題を追加。また、プレミアム利用者向けにマイナンバーに関する問題を追加。

【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。

＜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にとどまらず、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

活動休止中。

9.日本セキュリティオペレーション事業者協議会（ISOG-J）

代表:武智洋 氏/日本電気株式会社

セキュリティ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なう。

- 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

産学協同で今後の情報セキュリティ業界を支える人材を育成するための実践的なインターンシップの実現に向けた検討を行なう。情報セキュリティ業界を目指す学生と企業との交流会の企画検討や企業見学会の受け入れも行う。

11.SECCON実行委員会

情報セキュリティ人材の発掘･育成を目的に、所属や年齢に関係なく誰でも参加できるコンテストとして平成25年度より「SECCON」という名称で継続実施している。

全国各地で攻撃･防御両者の視点を含むセキュリティの総合力を試すコンテスト CTF（Capture the Flag)、サイバー甲子園などの他、初心者向けのワークショップCTF for ビギナーズの開催や女性限定のCTF for GIRLSなどを行っている。

JNSA 役員一覧　2016 年 3 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　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）

荒川　賢一　エヌ・ティ・ティ・アドバンステクノロジ株式会社
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
内田　憲宏　キヤノンITソリューションズ株式会社
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
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
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
西本　逸郎　株式会社ラック
能勢　健一朗　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　株式会社アークン
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

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

会員企業一覧　2016年3月現在　170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)　New
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)
(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(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)
エヌ・ティ・ティ レゾナント(株)　New
(株)FFRI
(株)OSK
(株)大塚商会

【か】

(株)カスペルスキー
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)
(株)神戸デジタル・ラボ
(株)コムネットシステム
(株)コンシスト

【さ】

(株)サーバーワークス
サイエンスパーク(株)　New
(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
サイボウズ(株)
(株)JMCリスクソリューションズ
ジェイズ・コミュニケーション(株)
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
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
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）
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）
日本プルーフポイント（株） New
日本プロセス（株） New
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）
パロアルトネットワークス（株） New
（株）日立システムズ
（株）日立ソリューションズ
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）富士通ソーシア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・ソフトウエア（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】
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 New
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 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
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

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。）

NECソリューションイノベータ株式会社　早川　敦史

JNSA会員の皆様、はじめまして。NECソリューションイノベータ株式会社の早川敦史（はやかわ　あつし）と申します。この度は株式会社日立システムズの大森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。

私は入社から数年はPKIや指紋認証に関連した業務を行っていましたが、その後十年程、統合ID管理やWebシングルサインオンなど、どちらかというと業務やインフラ寄りのセキュリティ基盤の構築を生業としていました。数年前より弊社内のサイバーセキュリティビジネスを推進するグループにて、ビジネスの立ち上げやセキュリティ人材育成を中心とした業務を行っています。ちなみに私とJNSAの関わりは、PKI製品を扱っていた関係で参加していたChallengePKI 2001の活動まで遡ります。その頃は社会人二年目で右も左もわからない若輩者でしたが、参加されている皆様にご指導いただきながら、非常に濃い経験をさせていただいたことを記憶しております。

さて弊社では昨年、社内にセキュリティイノベーションセンター（SIC）という活動拠点を立ち上げました。この場所はセキュリティに関する検証・解析や教育・演習を行う環境と会議スペースを併設しており、文字通りイノベーションを起こすために様々な工夫を取り入れた空間となっております。社外の方とコラボレーションを行う場所でもありますので、ご興味ある方はぜひお声がけください。

最近は「CSIRT」というキーワードをきっかけとしてお客様のお話を聞く機会が増えておりますが、異口同音に「（どこから手をつけていったらいいか／どこまでやったらよいか）わからない」と言われることが多いです。セキュリティに関わる人はよく聞く言葉ですが、以前と異なるのは確実に考慮する範囲が広がっていることです。それは組織体制や人材育成、経営層の関わり方など様々な要因が複雑に絡み合ってきています。自身の経験だけではそれぞれのお客様に対して最適な解というのは出しづらいのですが、JNSAでの活動はこのような課題に気づきを与えてくれるものであると感じています。現在ISOG-JのWGや「あさまでSOCプロジェクト」などに参加していますが、私からも皆様に対しても何らか有用なものが提供できるように活動の中でフィードバックしていきたいと思います。

ここからは個人的な話となりますが、私の趣味は自転車の整備と輪行といって自転車を電車に乗せて様々な土地を巡ることです。ただ今は子供が小さいことから、なかなか外に漕ぎだす機会が作れていないのが現状です。右肩上がりの体重増加を止めるためにも、今年は近場でもよいので自転車に乗る機会を増やして、まずは体重の現状維持を目指します！

最後に今年で不惑の四十歳となりますが、変化の激しいセキュリティ業界ではまだまだ惑い続けると思います（笑）そのような中でも前進の一歩を確実に踏み出していきつつ、少しでもJNSAに、ひいてはセキュリティ業界の発展のために貢献していきたいと思います。

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。）

株式会社カスペルスキー　越野　由華

JNSA会員の皆様、はじめまして、株式会社カスペルスキー 越野 由華と申します。

この度、富士通エフ・アイ・ピー 長澤様より「U40部会」仲間として紹介をして頂きました。セキュリティ業界はまだ日が浅く、このような協会誌に執筆する事になり大変恐縮ではございますが自己紹介申し上げます。

ご縁があってカスペルスキーで働き始めたのは2015年4月の事です。IT業界にはいたものの、実はまったくセキュリティについては無知でした。そんな私でしたが、入社してから色々と学ばせて頂く機会を頂き、セキュリティの重要性に今更ながら感化されました。そして、セキュリティ初心者からスタートしたことを活かして現在主に担当しているのがCSR（Corporate Social Responsibility）活動です。

現在弊社では会社の指針である『Save the World from IT threats : IT上の脅威から世界を守る』の下、様々なCSR活動を行っております。その一環として昨年10月に開始致しましたのが働く女性に向けたネットセキュリティ啓発プロジェクトです。

なぜ女性?と思われる方もいらっしゃるかもしれません。それは、今や多くの女性が男性と肩を並べて働く時代ですが、IT系の話となるとまだまだ苦手意識を持たれる女性も少なくないからです。でも、現実は苦手とは言っていられません。老若男女の別なくPCやスマートデバイスでサービスを使ったり仕事を行っているのが実状です。しかし、サイバー犯罪からの自己防衛を日常的な事として捉えている女性は一握りです。そのような中、自身の経験も踏まえながら、初めてネットセキュリティ対策に向き合うときに感じる不安や疑問を身近な例を上げて説明したり、専門用語を極力避けて、さらに補足を加えたりしながらコンテンツの作成を行っております。また、お仕事帰りに気軽にネットセキュリティについて学んでいただける場として『KASPRSKY After 7 Seminar』と題し、平日の夜7時から毎月1回女性限定セミナーを開催しております。

これまでも本活動の実施に際して、多くの方のご協力や助言を頂きながら進めて参りました。今後も皆様からの暖かいご支援を賜れましたら幸甚です。

最後に個人的な自己紹介を加えさせて頂きます。我が家には愛犬が一匹おりまして、近所に新しくできたペット施設を良く利用しています。そこでは飼い主の健康の上にペットの健康も維持できるという事で、様々な飼い主向け健康増進プログラムが用意されています。その中から先日初めてドッグヨガに挑戦してみました。ドッグヨガは人間のポーズに犬が自然と協力してくれるように接するのですが、普段とは違う愛犬とのコミュニケーションや、参加者同士の交流もできてとても新鮮でした。愛犬がいらっしゃる方は是非一度試してみて下さい。

こんな私ですが今後ともどうぞよろしくお願い申し上げます。

JNSA 年間活動（2015 年度）

4月	4月7日	第 1 回幹事会
	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 セキュリティフォーラム 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	緊急セミナー「待ったなし！マイナンバーの取扱と安全管理 〜監督省庁の実務担当者に聞く〜」（秋葉原 UDX）
	10月 15 日	JNSA 設立 15 周年記念イベント「Network Security Special Forum（NSSF15)」 （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 20 日	第 4 回幹事会
	10月 24 日	SECCON 2015 広島大会
11月	11月7日	SECCON 2015 福島大会
		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9日	第 5 回幹事会
	12月 15 日〜 17 日	IoT セキュリティウィーク in 沖縄 2015 シンポジウム （沖縄県立博物館・美術館 講堂）
	12月 18 日	第 4 回 CTF for GIRLS
1月	1月 26 日	JNSA アイデンティティ管理 WG10 周年記念 「企業及びクラウドにおけるアイデンティティ管理セミナー」 （NTT データショールーム INFOROUM）
	1月 30 日	SECCON 2015 決勝大会（intercollege）
	1月 31 日	SECCON 2015 決勝大会（international）
2月	2月 22 日	サイバーセキュリティセミナー 2016 （北陸総合通信局連携セミナー）
3月	3月1日	NSF 2016 in Kansai (第二吉本ビルディング　貸会議室）
	3月 24 日	第 6 回幹事会

2015 年 5 月から 2016 年 2 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）

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.41

2016 年 3 月 15 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/

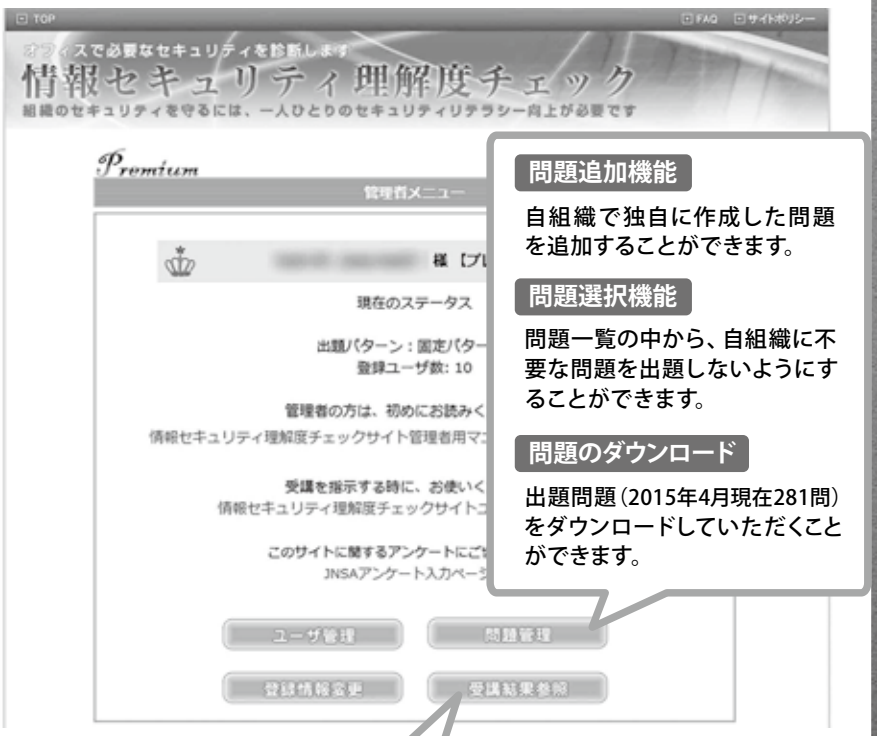
印　刷
プリンテックス株式会社

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。



問題追加機能

自組織で独自に作成した問題を追加することができます。

問題選択機能

問題一覧の中から、自組織に不要な問題を出題しないようにすることができます。

問題のダウンロード

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

管理者機能の強化

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

＜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

JNSA

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

〒105-0003 東京都港区西新橋1-22-12 JCビル 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）ディアイティ内
TEL 06-6886-5540