



寄稿

「記録媒体紛失」による 情報漏洩事故を減らす 現実的方法について

02

DUKPTの概要と その応用

08

CONTENTS

- 01 ご挨拶
セキュリティコンテスト
「SECCON 2013」開催の意味と
日本のハッカーの実力
- 12 JNSAワーキンググループ紹介
● セキュリティ理解度チェックWG
- 14 会員企業ご紹介
- 17 JNSA会員企業情報
- 18 イベント開催の報告
● 2013年第3回日韓シンポジウム報告
- 21 インターネット安全教室
- 22 中小企業向け指導者育成セミナー
- 24 事務局お知らせ
- 33 会員紹介
- 35 JNSA年間活動

セキュリティコンテスト 「SECCON 2013」開催の 意味と日本のハッカーの実力

サイボウズ・ラボ株式会社
SECCON 実行委員長
竹迫 良範



世界で一番有名な日本人ハッカーは誰でしょうか。実はケビン・ミトニックの逮捕に協力した米国国籍の物理学者「下村努」さんです。このときの逮捕劇を書いた本は映画ザ・ハッカー（原題：Takedown）の原作にもなりました。下村努さんを越える知名度のハッカーが日本で誕生することはあるのでしょうか。世界から見た日本のセキュリティのイメージは残念ながらあまり良いものではありません。相次ぐ情報漏えい事故や初歩的なウイルス感染の事件が報道されていて、日本にはきちんとした技術力を持った強いセキュリティ技術者が存在しないのではないかとされています。この日本のイメージを覆すことはできないかと、昨年からSECCON実行委員会を組織して活動を開始しています。

世界ではCTF（Capture The Flag）という情報セキュリティ技術をチームで競うコンテストが各地で開催されていて、世界的にはほぼ毎週どこかでCTFの大会が開かれているまでになっています。さすがにハッキング能力の高さを示すために、他国のインフラを攻撃することは倫理的に出来ませんが、CTFというゲームのルールに則ったコンテストで日本のチームが上位に来ることによって、その実力を正々堂々とアピールすることができます。日本にもきちんとした技術力を持った強いハッカーが存在していることを世界にアピールできる恰好のチャンスです。

野球やサッカーなどのスポーツの分野では、世界に通用する人材を日本から輩出していますが、それは甲子園予選やアマチュアスポーツ大会など多くの地方大会が盛んに行われていて、全国の学校に野球グラウンドやサッカーコートなどがあるからです。工学系の分野だと高専ロボコン、各種プロコン、技能五輪などの成功事例が数多くあります。これらの現状に対して、日本のセキュリティ分野のコンテストはまだその段階になく、これから土壌を整備していくフェーズです。SECCONは、日本でCTFの枠にとらわれない様々なセキュリティコンテストを実施し、世界に通じる優秀なセキュリティ技術者を輩出するための環境を各地に作って、地元文化に根付かせることを目標としています。

将来の日本のセキュリティ技術者がハッキング技術を勉強する場としてSECCONが存在し、一つのきっかけになってくれることを願っています。アンダーグラウンドの世界に引き込まれないためにも、家庭や学校や職場の理解を常に得つつ、表舞台でセキュリティ技術を学び、それが社会に役立ち、正当に評価される環境を日本でも作ることが大事です。その点において現状のSECCONでは、数多くの後援団体様や協賛企業様のご支援を受けられている意義は大きく感謝しております。

引き続きJNSA会員皆様のご理解とご高配をいただければ幸いです。

「記録媒体紛失」による情報漏洩事故を減らす現実的方法について

JNSA 組織で働く人間が引き起こす不正・事故対応 WG
セコム IS 研究所 甘利 康文

1. はじめに

筆者らは、JNSA Press Vol.33で「セキュリティ実現の原点から見た内部要因事故抑制手法」と題して、内部不正および従業員のヒューマンエラー抑制に関する問題提起と提言を行う小論^[1](以下、内部要因事故抑制手法論)を発表した。これに対しては、情報セキュリティ分野に留まらない複数の関係者より問合せを頂戴した他、JNSAにおいても、この小論を契機として「組織で働く人間が引き起こす不正・事故対応WG^[2]」が発足した。本稿は、このWGにおける筆者の発言を元とし、「私有デバイスによる情報持ち出しがなぜ起きるのか」についての仮説を述べると共に、世の中に対して、その対策に関する現実的方法を提言することを目的としたものである。

2. 私有デバイスによる情報持ち出しという「内部不正」

ネット検索すると、機密情報の入ったデバイスの紛失事故が、多くの組織で起きていることが見て取れる。そして、紛失したデバイスのうちの少なくない数が私物、すなわち私有デバイスである。私有デバイスは、パスワード設定や情報暗号化など、紛失や盗難の場合に備えた対策が行き届いていないことも多い。そのため、組織で働く従業員が、私有デバイスを業務に用い、仮に、それが紛失や盗難事故にあった場合、情報流出のリスクは相当高いものとなる。

実際、「情報持ち出しを禁止する」という職場のルールがあるにもかかわらず、そこで働く人間がその

「ルールを無視」し、アングラで、もしくは公然と、私有デバイスを使ってそれを行っているという事例は少なからず存在する。これは、少なくない組織で、ルールに抵触する「不正行為」が行われているということである。そして、この行為が元となって、ある割合で、私有デバイスの紛失や盗難といった実際の事故が発生している。

一方、ネットを見る範囲では、組織の情報が記録された私有デバイスの紛失事故が発生した場合、それを発生させた組織における再発予防対策は、「情報の取扱い要領を定める」、「取扱注意を徹底する」、「研修会を開催する」、「職場内ルールを厳格化する」など、一言で言うと「運用を再徹底する」に留まるものが多い。

3. なぜ私有デバイスが用いられるのか？

筆者らは、先の内部要因事故抑制手法論^[1]の7.5.4項、「ルール遵守への支援」において、以下のように指摘した。

組織で働く人間は、その組織のオペレーションの一部を担い、なんらかの価値を作り出すことをそもそもの目的として働いているのであり、ルールを守るために働いているのではない。そのため、ルール遵守に相当の手間が掛かり、組織のオペレーションをスムーズに行うことを必要以上に阻害する場合、やがてそのルールはオペレーション優先の形で形骸化し、守られなくなっていく。

「情報持ち出しを禁止する」という職場のルールが

● 本稿の内容は、筆者の個人的見解であり、必ずしも筆者が奉職する組織の見解と一致するものではない。

● 本稿では、ノートPCや、USBメモリ、デジタルカメラなどの「情報を記録し、それを持ち出すことのできるIT機器全般」を「デバイス」、そのうち「個人が所有するもの」を「私有デバイス」、業務上の必要性からの情報持ち出しのために組織が用意し、万が一の紛失や盗難などに備えて暗号化などの情報漏洩対策を施したデバイスを「公用デバイス」と呼ぶ。

あるにもかかわらず、少なくない組織の中で、私有デバイスを使い、それに抵触する「不正」が行われている主な理由はここにあるものと考えられる。

「情報持ち出しを禁止する」というルールを制定した組織においては、そのルールゆえ、暗号化など万が一の紛失や盗難による情報漏洩対策を施した「情報持ち出しを前提とした公用デバイス」を用意できないのが普通である。情報を持ち出さないと業務が回らない組織で、「情報持ち出し禁止ルール」が策定された場合、そこで働く人間は「背に腹は代えられない」ことから私有デバイスを用いてルールに抵触する行為を行わざるを得なくなる。実際、「情報持ち出し禁止」ルールがあるにもかかわらず、私有デバイスによる情報持ち出しという「不正」が行われている組織の多くでは、「それをしないと仕事にならない」状況が発生していることを仄聞している。「組織のルールを遵守すると、仕事にならない」という状況では、そのルールは守られるはずもない。ルールが組織のオペレーションの実態に合わないのである。

そして、公然とルール違反が行われている組織の中では、多かれ少なかれ、以下の状況が発生しているはずである。

ルールが形骸化し、守られない状況が常態化すると、ルール違反をすることに口実を与えてしまう。また、ルールが一旦形骸化すると、それを超える行動のガイドラインが存在しないことから、事実上ルールが無い状態にもなる。^[1]

4. 「個人情報保護法のガイドライン」によって立ち現れるリスク

個人情報保護法がきっかけとなって、社会の情報漏洩に対する意識は高まり、「機密情報が入った可搬デバイスの紛失や盗難」が、「情報漏洩事故」として報道されることが多くなった。

経済産業省が2009年10月に発表した「個人情報

の保護に関する法律についての経済産業分野を対象とするガイドライン」では、法による保護の対象とする個人情報について、以下のように定義している。

「個人情報」とは、生存する「個人に関する情報」であって、特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができるものを含む。）をいう。「個人に関する情報」は、氏名、性別、生年月日等個人を識別する情報に限られず、個人の身体、財産、職種、肩書等の属性に関して、事実、判断、評価を表すすべての情報であり、評価情報、公刊物等によって公にされている情報や、映像、音声による情報も含まれ、暗号化等によって秘匿化されているかどうかを問わない（ただし、「2-2-3-2.安全管理措置（法第20条関連）」の対策の一つとして、高度な暗号化等による秘匿化を講じることは望ましい。）

このガイドラインを拠り所として、社会一般では、「生存する『個人に関する情報』」であって、特定の個人を識別することができる情報」は、暗号化されている、いないにかかわらず「個人情報」であると認識されている。そのため、個人情報が入ったデバイスを紛失したり、それが盗難にあったりした場合には、たとえその中の情報がどんなに強固に暗号化されていたとしても、「個人情報漏洩事故」とされる。

このような「事故」は、マスコミなどでも取り上げられ、世間から組織の不祥事として扱われる。事故発生後に、それを起こした組織が「暗号化などの情報漏洩対策を施している」と広報したとしても、社会は「その情報漏洩対策がどの程度安全か」を知るすべはない。社会からは、「暗号化等によって秘匿化されているかどうかを問わず」（個人）情報漏洩と見なされるため、事故を起こした組織に対する信用は毀損される。個人情報が入ったデバイスの紛失、盗難に関しては、情報暗号化の有無にかかわらず、組織として

は、大きな風評リスクを抱えていることになる。

5. 「現在起こっていること」に関する仮説

本項では、「生存する『個人に関する情報』であって、特定の個人を識別することができる情報」を、それが暗号化されている、いないにかかわらず、一律に「個人情報」とみなし、「漏らしてはいけない」とすることから生じる問題について考える。このことが、万が一のデバイス紛失に備えた暗号化処理など、情報漏洩に対するためのセキュリティ対策に関する組織のモチベーションを削ぐ要因になっている可能性は否定出来ない。

情報がデバイスに格納された形で持ち出されて、それを紛失した場合、たとえデバイスや情報にどのようなセキュリティ対策が為されていたとしても「情報漏洩事故」と見なされる。この現状においては、組織の情報セキュリティ担当者としては、情報漏洩事故を起こさないようにするためには「『情報持ち出し禁止』のルールを策定すること」以外に打つ手は無い。

<コラム>

情報が暗号化されているがいまいが、それがデバイスに格納された形で持ち出され、紛失した場合、その組織は「情報漏洩事故」を起こした組織として非りをうける。持ち出されたデバイスは、常に「紛失のリスク」にさらされる。この状況では、組織の情報セキュリティ担当者は、情報持ち出しに関して「(実質)禁止」というルールを作らざるを得ない。「情報持ち出し禁止」のルールさえあれば、たとえ私有デバイスで情報が持ち出されて紛失事故に至ったとしても、情報セキュリティ担当者としては「その責の多くは持ち出した人間にある」と、ある程度責任回避することが出来る。その後の対応も「運用面を再徹底する」ということで釈明することが可能となる。このように、組織にとって

は、現状で唯一採れる手段である「『情報持ち出し禁止』のルールを作ること」は、コストもかからない、一番簡単な自らを守るための手段となる。

これは相当に斜めからの見方ではある。しかし、少なくとも組織において、「当たらずといえども遠からず」なのではないだろうか。

先に指摘した通り、「形骸化したルール」の存在は、事実上「ルールが無い状態」を作り出す。「情報持ち出し禁止ルール」のある組織では、論理上、情報持ち出しを前提とした、暗号化などの対策をされた公用デバイスを準備できない。一方、そこで働く人間は、「情報を持ち出さないと仕事にならない」から、そのルールに抵触することにさほど抵抗感を感じずに、十分な情報漏洩対策がなされていない私有デバイスを用いて情報を持ち出す。このような状況では、組織の情報セキュリティ担当者が、「私有デバイスを用いて(不正に)情報を持ち出す場合には、最低限パスワードの付与や暗号化をお願いします」という呼びかけを行うといった、笑い話のようなことは出来る訳もない。組織のルールとして「情報持ち出し禁止」にもかかわらず、「情報を持ち出さないと仕事にならない」という理由で、私有デバイスによる情報持ち出しが行われている。このような状況下では、情報セキュリティに関わるIT産業界としても、技術的に出来ることに限りがあることがお解り頂けるだろう。

現在の暗号技術のレベルに鑑みると、一般に推奨されている暗号がテクニカルに破られるリスクと、外部に持ち出されたデバイスを紛失するリスクを比べた場合、はるかに大きいのは後者である。仕事上の必要性から、暗号化などのセキュリティ対策が行われないう形で、情報が私有デバイスに入れて持ち出され、万が一それを紛失した場合、そのデバイス内部の情報は「ただ漏れ」である。それに加え、持ち出された情報は、公式に管理されているわけではないため、組織として、その影響を正確に把握することも困難となる。

この場合、情報を持ち出した当事者は、ルールに抵触する「内部不正」を行った者として組織内部で何らかの処分を受け、事故を起こした組織も世間から相応の誹りを受ける。組織は、「情報の取扱い要領を定める」、「取扱注意を徹底する」、「研修会を開催する」、「職場内ルールを厳格化する」などの再発防止の対策を打ち出すだろう。しかし「情報を持ち出さない」と仕事にならない状況がある以上、私有デバイスを使って情報は持ち出され続ける。「情報持ち出し禁止」に関するルール違反は、構造的に、起こるべくして起きているという見方ができるのである。

6. 提言

ここまでで、「情報持ち出し禁止」に関するルール違反（内部不正）では、いわゆる「三すくみの状態」が発生していることがお解り頂けるだろう。その大元は、組織における「守れないルール」にある。そして、多くの組織において「守れないルール」を策定せざるを得ない根本は、社会のルールが「守れないルール」であることによる。

本稿では、社会のルールを「守れるルール」とするために、先にあげた「ガイドライン」を以下のように変更することを提言したい。

「個人情報」とは、生存する「個人に関する情報」であって、特定の個人を識別することができるものをいう。・・・(中略)・・・暗号化等によって秘匿化されているかどうかを問わない（ただし、「2-2-3-2.安全管理措置（法第20条関連）」の対策の一つとして、暗号化等による高度な秘匿化とその運用が共に適正になされている場合は、たとえ情報媒体の紛失、盗難、情報の誤送信等の事象が起こったとしても、それを情報漏洩事故とはみなさない。）

個人情報保護法の運用ガイドラインにある「但し書き」を上記のように変更することで、情報セキュリティに携わるIT産業界は、「情報を持ち出さないと仕事にならない」という必然的な必要性がある「情報持ち出し」に関して、「暗号化等による高度な情報秘匿化とその運用によって、その利用を特定の者に限る」ための技術的なソリューションを提供することが可能となる。

機密情報を扱うユーザー組織には、社会から認められている「安全な公的情報持ち出し手段」として、持ち出し情報を高度に暗号化したり、それを安全に管理運用したりするソリューションを適用したデバイス（公用デバイス）を用意し、それを現場で働く人間に対して提供する新たなインセンティブが生まれる。「業務上の必要性によって情報を持ち出す場合には、『ソリューションA』により暗号化を施し、『ソリューションB』により適正に管理された公用デバイスを用いること」のような形で、その組織で働く人間が「実質的に守れるルール」を策定することも可能となる。

この状態で、デバイスの紛失等の事象が起こったとしても、社会的に「情報漏洩事故」とは見なさない前提であるため、組織としては風評リスクを回避できる。加えて、各種のセキュリティ対策が施された公用デバイス内の情報は、現実的には、特定の人間以外の不正利用が不可能であることから、大きな実害も生じない。

「情報媒体の紛失、盗難、情報の誤送信等の事象が起こったとしても、それを情報漏洩事故と見なさないようにする」ためには、ユーザー組織において各種技術ソリューションの運用がきちんと行われているかどうかについての、第三者による認証も必要となるだろう。暗号の認証としては、現在、総務省および経済産業省が共同設立したCRYPTRECによるものがあるが、これは暗号化強度を技術的に評価するのが主目的である。デバイスに入れる情報に、どんなに強

い暗号化アルゴリズムを適用したとしても、パスワードなどの鍵の管理に不備があるなど、運用が徹底されていない場合、総体としての持ち出し情報のセキュリティレベル低下は免れない^[3]。

そのため「暗号化等による高度な秘匿化とその運用が共に適正になされている」かどうかの認証は、「JIS Q 15001(個人情報保護マネジメントシステム)」のように、運用管理面の評価を重視する形にしなければならないだろう。これまでも「CRYPTRECで推奨された暗号化がなされていたならば、情報が流出した場合においても、情報漏洩とみなさないようにしては」という提言はあった^[4]。しかし、いかに「推奨暗号化アルゴリズムによる強固な暗号化」がなされていたとしても、その暗号を解読するための鍵管理などの運用が杜撰であったとしたら、総合的観点からの情報の機密性は損なわれてしまう。本稿の提言は、技術のみならず、この運用までもを総合的に評価、認証し、問題が無ければ、たとえ、デバイスの紛失、盗難、情報の誤送信等が起きたとしても、それを「情報漏洩事故とは見なさない」とするものである。

<コラム>

十分強い強度で暗号化された情報であっても、それが流出した場合の世間の反応は、「極めて微小ではあるが、数学的にはゼロではない可能性」に対して、社会がミスリードに陥り、過剰反応しているためではないかと考えられる。現在利用が推奨されている暗号化アルゴリズムの多くは「十分に強く」、総合的観点からは、何らかの方法で「復号キー」を入手しない限り、一般の人間、環境では、実質上解読不能と言っても良い。多くの場合、心配すべきは「暗号化アルゴリズムの弱さ」ではなく、「何らかの方法で『復号キー』を知られてしまうこと」である。そのため、通常の場合においては、復号キーを知られてしまわないように管理運用に十分な注意を払わなければならない。

個人情報保護法の運用ガイドラインにある「但し書き」に、社会の現実にあった変更を加えることで、業務上の必要性から情報を持ち出さざるを得ない多様な業界のユーザー組織に、「情報に高度な秘匿化を施し、その利用を特定の者に限る」ための「技術的手段、管理運用的手段」を導入する強いモチベーションが発生する。当然、それを提供するIT産業界側にも具体的ソリューションを開発、提供する新しいインセンティブが生まれる。加えて、組織の管理運用状況を認証する公的体制に対する新しいニーズも生まれるだろう。ユーザー組織で働く個人の仕事が回る。組織のオペレーションが回り、風評リスクも抑えられる。情報セキュリティ分野や社会に新しい需要が生まれることでIT産業がさらなる発展をし、「本当の意味での情報漏洩」も抑えられる。良いことづくめである。

7. 本提言の別の視点 ～ 暗号化情報の扱いに関する矛盾 ～

現在、パブリックネットワークでは、VPN技術を用いることにより、ネットバンキングやクレジット決済、確定申告や医療情報など、相当な機微情報が、暗号化され、通信されている。このケースでは、情報がパブリックネットワークを流れるにもかかわらず、特定の人間以外にはそれが解読できないものとして扱われている。その情報がどのようなサーバーを経由して通信されているかなどについては、ほとんど気にされることもない。しかし、先の「ガイドライン」を杓子定規的に解釈するならば、たとえその暗号化強度がどのようなものであったとしても、個人を特定できる暗号化情報は「公にさらしてはいけない個人情報」であり、それがインターネットのようなパブリックネットワークを流れることは「個人情報流出」に当たるという解釈も可能となるのである。しかしながら、今現在も、暗号化された情報は、どんなに機微なものであったとしても、パブリックネットワークを介して公然とやり取りがなされており、社会はそのことから多大なる恩恵を受けている。

現在、たとえ同等の強さで暗号化された情報であったとしても、それが入ったデバイスが紛失や盗難に遭うと事故として扱われる一方で、それがパブリックネットワークを流れることについては、問題視されていないという状況が起きている。これは明らかに矛盾である。本稿の提言は、この矛盾を解消しようとするものである。

＜コラム＞

過去、事故発生に関して、「可能性が全くない時以外は、研究者は『ゼロではない』という表現をよく使う」という研究者の発言がマスコミに流れたことがあるが、「数学的にゼロではないもの」に対する専門家の見解を解釈する場合には十分な注意が必要であろう。世の中では、これが主な要因となって、暗号化された情報の解読可能性についての「過剰反応」が起きているものと考えられる。「非常に微小で実質上無視できるものの、数学的にはゼロではないもの」を、「ゼロではない」と表現するのは、論理的な厳密性を論ずる際の「学術畑方言」、「研究者方言」である。「ゼロではない」という類の専門家の発言が、世間を混乱させている例はこれに限らない。人々は落ちる可能性が「ゼロではない」のに飛行機に乗る。現実的な議論では、このことを忘れてはならないだろう。

8. おわりに

先の、内部要因事故抑制手法論では、「組織として、従業員がルール遵守をする行為に必要以上の手間がかからないように支援する必要がある」旨について触れたが、これは「情報漏洩事故と見なす基準」についても同様である。

社会正義に反しない範囲で、組織のオペレーションの実態にあったルールを策定し、運用していくことである。そのためには、組織のオペレーションを熟知している人間が、ルール策定をする必要がある^[1]。

この提言は、組織のルールという観点のものであるが、これは「世の中のルール」についても同様である。「普通では守れないルール」、これはルールに問題がある。社会のオペレーションの実態にあったルールを策定しなければ、守れるはずがない。

実社会で回っているオペレーションと、ルールとの乖離、矛盾。ここにメスを入れることにより、「ルール違反」という、組織内部で行われている「内部不正」は大いに減るはずである。

【参考文献】

- [1] 甘利康文, 新井真司, 内田順一: セキュリティ実現の原点から見た内部要因事故抑制手法, JNSA Press Vol. 33, pp.3-29 (2012)
- [2] 甘利康文: 組織で働く人間が引き起こす不正・事故対応WG, JNSA Press Vol. 35, pp.6-7 (2013)
- [3] 松本泰, 伊藤忠彦: 暗号技術による個人情報保護の制度と技術の動向, JNSA Press Vol. 34, pp.3-11 (2012)
- [4] 辻井重男: 情報社会のセキュリティと倫理の課題, Fundamentals Review Vol.1, No.3, pp.10-26 (2008)

DUKPT の概要とその応用

タレスジャパン株式会社
住田 敦

■ はじめに

Webアプリケーションやデータベースのセキュリティについては多くの書籍・雑誌で取り上げられ、幅広く知られていますが、電子決済系のセキュリティについてはあまり知られていないのが現状と思います。よって、今回は電子決済系、特に昨今話題となっているスマートフォン等を使ったカード決済システムで注目されているセキュリティ・プロトコルであるDUKPTがどのようなシステムで使われ、どういった利点があるのかをご紹介します。また、この技術がその他の分野にも応用可能である点も併せてご紹介いたします。

■ DUKPT とは

旧来の電子決済では、決済を行う端末（小売り店舗等で金額を入力し、クレジットカードの情報を読み取るもの）から決済を処理するサーバまでの間は専用回線となっていました。現在は決済をiOSやAndroid端末などに決済用のハードウェアを組み合わせ、インターネットを経由して行うというケースが増えてきました。このようなケースで盗聴などの可能性を考えると、専用

線を使う場合に比べ、より強固な通信の暗号化が必要となり、図1のような範囲の通信においてこのプロトコルの利点が注目されています。

まずDUKPTとはDerived Unique Key Per Transactionの略でANSI X9.24 part1にて規定されたプロトコルです。トランザクション毎にデータの暗号鍵を変えることで暗号通信のセキュリティ強度を上げることを目的としています。つまり、あるトランザクション・データが盗聴され、万が一鍵が推測されて復号化されたとしても他のトランザクションのデータまでデータ漏洩の影響が無いということが大きな特徴となっています。

しかしながら、複数の端末を使う場合に、トランザクション毎の鍵が同じになったり、どの鍵を使うかを通信経路上で交換してしまったりしたのではセキュリティ強度としてはあまり高いものになりません。よってDUKPTでは図2のような処理フローを採用しています。その大まかな流れは以下のとおりです。

1. サーバ側で暗号鍵用のシードを作成します。次に端末ベンダーは各端末固有情報を作成し、端末に渡すと同時にサーバ側にも渡します。サーバはこの情報

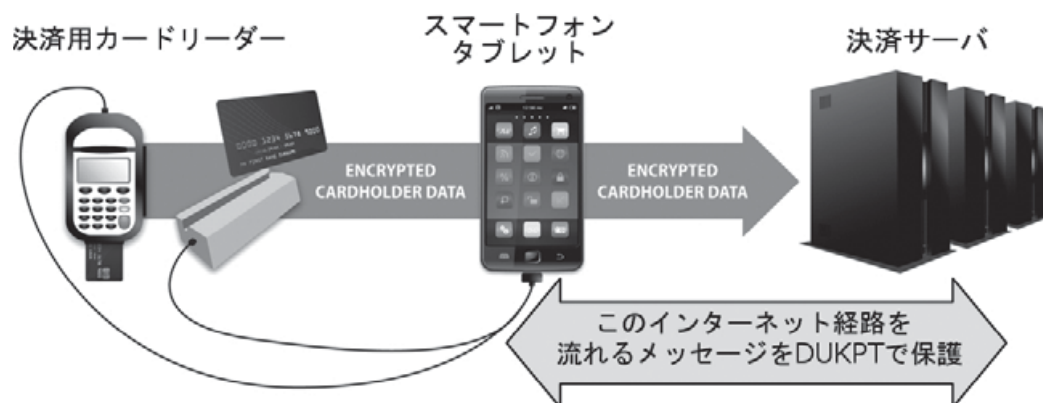


図1: DUKPTの適用範囲

を元に各端末固有の暗号鍵用のシードを作成し、それを端末に渡します。

2. 端末は初期化時といったタイミングでシード情報から鍵を作成し、その時点でシードを破棄します。端末側では作成された鍵から別の鍵を派生させていくという形でトランザクション毎の鍵を作成していきます。つまり、サーバとの通信毎にデータを暗号化して送りますが、この時、はじめから何番目に作った鍵かというトランザクション番号という情報と、どの端末であるかという端末情報を暗号化されたデータに付加し、サーバに送信します。
3. データを受け取ったサーバは、端末情報とトランザクション番号を元に、サーバ上のシード情報から暗号化鍵を生成し、データを復号化して取り出します。

■ DUKPT の利点

端末毎にシードが異なるため、同じ暗号鍵が使われるという可能性は低く、また鍵情報は通信経路上では交換されず、サーバ上でトランザクション毎に送られてきたデータを元に再計算されて使われるため、漏洩の心配もありません。

このような利点に加え、通信にセッションという考え方は無いため、例えばトランザクション番号 n 番の通信の後に、番号 $n+5$ 番に対応するデータがサーバに送信されたとしても、サーバは $n+5$ と端末情報の2つの情報を元に暗号化鍵を計算するだけです。

つまり、 $n+1$ から $n+4$ 番の情報やそれに対応する鍵

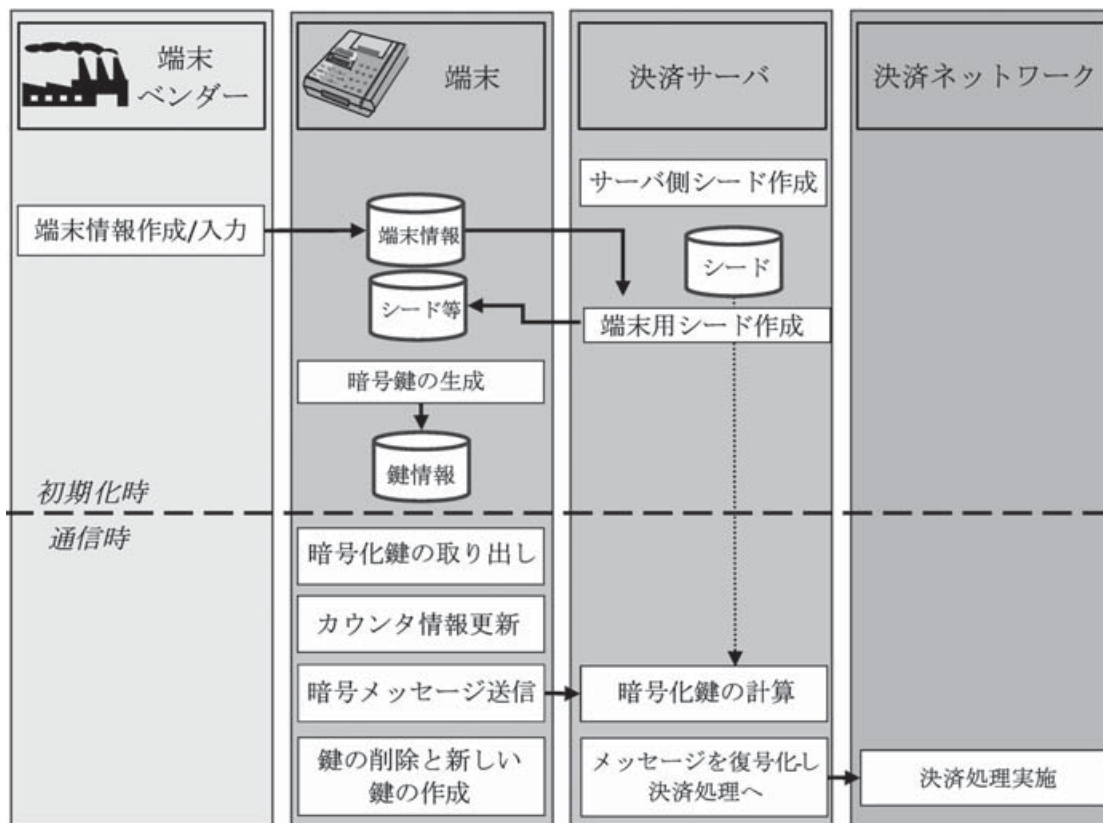


図2: DUKPT 処理フロー概要

の情報は $n+5$ 番の鍵を生成するために不要であるということも特徴の一つとなっています。

先に、インターネットを使うことにより、強固な暗号化が必要になると述べました。

鍵を1回1回変えることが出来る以外にも、この DUKPT という方法を使ったほうが良い理由があります。

従来の決済系の通信は、専用回線のみが使われていたため、PIN（決済で使用される暗証番号）のみを暗号化していました。この場合であれば、PINを確認するロジックと端末間で何かしらの鍵の共有の仕組みがあれば問題はありませんでした。しかしながら、インターネットを経由する場合にはそれ以外の情報、例えば決済ではPAN（クレジットカードのカード会員番号）といったものも暗号化すべきであると、決済系のグローバルセキュリティ基準である PCI DSS（国際ペイメントブランドのVISA, MasterCard, American Express, JCB, Discoverの5社が策定）でも求められています。この場合、カードの中の個々の情報を使うロジックごとに鍵を管理していくという方法よりも、メッセージの電文すべてを暗号化してやり取りをしたほうが効率的になります。そのような通信の中で、アプリケーション両端を結んだ暗号化通信を決済系では P2PE（Point 2 Point Encryption）と呼びますが、以前はベンダーごとにその実装が異なるため、マルチベンダーの環境に適応するには考慮点がありました。しかしながら、スタンダードである DUKPT をベースにしたソリューションを用いればベンダーをまたがった暗号化ソリューションが容易に実装可能となるといった利点が出ます。

■ DUKPT の考慮点

ここまで DUKPT の利点を挙げましたが、重要な考慮点が2つあるので、それをご紹介します。

1つめとして、端末側でシードを元に暗号化鍵を生

成すると前にご紹介しましたが、シードから生成できる鍵の個数に上限があり、その上限に達した場合には新しいシードを端末側に配布する必要があります。この配布の仕組みは、DUKPT の規定の範囲外となります。しかしながら、このシード情報が盗まれた場合には端末のなりすましといった問題が発生するため、電子メールの添付ファイルとして送信して手作業にて端末にUSBキーや何かでコピーをするというやり方は推奨されません。しかしながら、シードを更新する必要がある端末が出るたびに、専用のエンジニアがジュラルミンケースにシード情報の入った記憶媒体を入れて持ってきて更新作業を厳重に実施していくというのも、端末の数や人件費を考えると現実的ではありません。

このような考慮点を解決するため、DUKPT を実装した製品を提供しているベンダーは、Remote Key Loading という仕組みで端末に対してシード情報を遠隔地から配布する仕組みを実装しています。Remote Key Loading に規定はありませんが、多くのベンダーは基本的にはPKIをベースにした暗号通信により安全にシード情報を配布する仕組みを提供しています。

2番目として、DUKPT 自体に端末とサーバの相互認証といった仕組みは無いため、例えば端末に入れている鍵のシード情報が盗まれればその端末の偽造は可能となりますし、サーバ側のシード情報が盗まれれば偽造されたサーバが決済情報を集めてしまう可能性があります。こういった場合に備え、DUKPT では端末側のシード情報は初めの鍵作成の時点ですぐに破棄するという実装となっています。しかしながら、サーバ側はクライアントから送られた情報での鍵の再計算のために持ち続ける必要があるため、HSM(Hardware Security Module) といった外部のセキュアハードウェアにシード情報を安全に保持しておくことが現実には推奨されています。

■ DUKPT の応用的な適用例

ここまで、DUKPTの仕組みとその利点、決済系でどのように使われるかをご紹介しましたが、他の分野にもこの仕組みは適用可能です。

例えばファイルをファイルサーバにアップロードする仕組みへの応用が考えられます。

製造業の分野において、重要な設計図情報などのファイルをアップロードする場合、情報漏洩に備えて通信経路を暗号化することは必須であり、そのようなセキュリティはすでに実装済みのシステムは多いと思います。しかしながら近年の標的型攻撃の手法から考えると、ファイルサーバでファイル受け取った時点で復号化してしまうと、そのサーバがハッキングされた場合にはサーバ内で情報を奪取されてしまうという危険性が生じます。ここで、図3のようにファイルをストレージにストアするまで暗号化ファイルごとに異なる鍵で暗号化して送信すれば、暗号化されているために奪取されたとしても情報を読むことが出来ませんし、もし仮に1ファイルのみの情報が解読され、漏洩さえたとしてもそれ以外のファイル情報は別の鍵で守っているため、漏洩から守ることが可能となります。

こういった利点に加え、ストレージ側において、ファイルごとに暗号化した鍵をすべて、どこかに保持して

おくという必要は一切無いということも利点の一つです。1つ1つのファイルに対して、何番目の鍵を使ったかという情報だけを付加しておけば、復号化のタイミングで鍵を計算すれば良いだけですので、大量の鍵をどうやって守るかを考える必要はなく、シード情報だけに重点を置いて保守をすれば良いという形となります。ただし、端末側での鍵の再生成の仕組みはDUKPTの規格としては提供されていませんので、端末側に再度送る場合には、そこでサーバからクライアントへの新規のDUKPTのトランザクションを発生させて新しい鍵で再暗号化して端末に送るといった仕組みを別途考える必要があります。

■ おわりに

電子決済という重要度の高い情報を取り扱う分野にて使われているセキュリティ技術の1つとして、DUKPTをご紹介しました。

セキュリティ技術は、適用分野が増えるにつれて、特定分野固有のものが增多していますが、そのようなものの1つとして今回知っていただくのと同時に、他の分野に適用すると新たな利点が生まれるものがあるといった観点で、今後のソリューション作成の一助としていただければ幸いです。



図3: DUKPT 応用例

セキュリティ理解度チェック WG

WG リーダー トレンドマイクロ株式会社 小屋 晋吾

セキュリティ理解度チェック WG は、経済産業省委託事業としてスタートした「理解度チェックサイト」の開発・運営をするために 2006 年に発足しました。

現在は JNSA のサイトとして運営し、外部へ無償・有償のサービスとして提供しています。

■ 理解度チェックサイト

企業・団体等の組織における IT 利用者を対象として、基礎的な情報セキュリティ知識の理解度をセルフチェックできるサイトを構築し、情報セキュリティの普及啓発を行うために開発されました。

サイトは、無償で利用できる機能と、「プレミアム版」と呼ばれる有償で利用できる機能を持っており、販売代理店を通じて一般に販売されています。

販売代理店からはこのサイトを「ツール」として利用し、その後のセキュリティコンサルや、製品導入、本格的な教育を行うためのアセスメントに有効に利用しているという声が聞かれます。



このサイトで出題される問題は

- ・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
- ・ルールや規則の順守
- ・社外における情報セキュリティ

の 8 つのカテゴリーに分けられており、一回の受講で 25 問の問題が出題されます。

二回目以降は、出題パターンも変わるため、繰り返しの受講で知識の底上げを行う事も可能になっています。

無償版であっても管理者はユーザーの受講結果を把握でき、同業種企業との比較などが行えます。



有償提供の「プレミアム版」では、さらに独自問題の追加や、管理者による出題問題の選択、受講者の回答内容などの確認ができるため、その後のセキュリティ教育をより具体的に実施できるようになります。

無償版、「プレミアム版」合わせた総受講回数は既に 10 万回を超え、多くの方に利用されるサイトとなりました。

■ WG の活動

WG では主に以下の活動を行います。

- ・問題作成・メンテナンス
- ・販売代理店開拓
- ・理解度チェックサイト PR 活動

■ 問題作成・メンテナンス活動

日々目まぐるしく変わる情報セキュリティの世界では、理解度をチェックするためにも問題の鮮度が重要になります。WG メンバーは定期的に新しい問題を作成したり、以前の問題を修正したりする必要があります。

理解度チェックサイトの問題は比較的反読性（リテラシー）の低い方でも問題内容が理解できるよう、またいろいろなセキュリティポリシーの企業でも違和感がないよう配慮して作る必要があります。

メンバー曰く、「回答選択肢の4つめが思いつかない・・・」という感じです。

■ 販売代理店開拓活動

現在6社の会員が代理店として「プレミアム版」の販売を行われています。

本年はもう少し販売店を増やし、販売量を増やしていきたいと考えています。

なお、9月までに販売店になっていただくと社内使用特典や、代理店登録費用が初年度無料になるキャンペーンを実施中です。

■ 理解度チェックサイト PR 活動

せっかくのメンバーの血と汗と涙の結晶の「理解度チェックサイト」。「プレミアム版」のみならず、無償版もさらに多くの方に使っていただき、日本の企業のセキュリティリテラシー向上に寄与したいと考えています。

エンドユーザー向けセミナーや JNSA のアクティビ

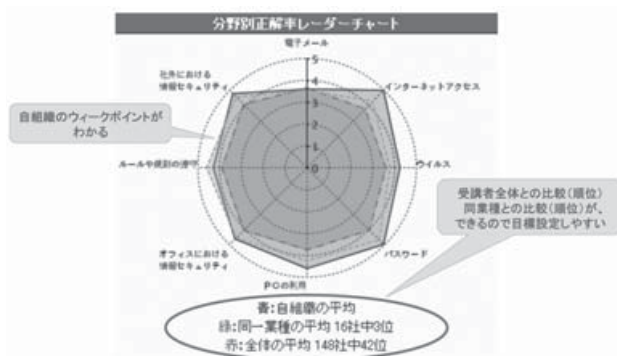
ティへの相乗りなど、低コストマーケティングで効果を上げていきたいと思っています。

■ 最後に

セキュリティ脅威の変遷から、ツールやサービスの単体導入では効果的なセキュリティシステムを維持する事が困難になってきました。体制、規程、対策技術、教育を合わせて提案していかなければならないと言われて暫く時間が経ちますが、多くの企業から、この「教育」の実施方法や成果の評価が困難との声が聞かれます。

我々の WG ではその課題をエンドユーザー、販売店両方の立場から解決できるようにこれからも努力していきます。

皆様も是非本 WG に参加いただき、一緒に回答選択肢で頭をひねってみませんか？



会員企業ご紹介 36

イーロックジャパン株式会社

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

Enjoy the Life

「すべては安心があって__」



イーロックジャパン株式会社

TEL:03-3265-1169 E-Mail:info@elock.co.jp

マカフィー株式会社

<http://www.mcafee.com/jp>



マカフィーは、インテル・コーポレーション (NASDAQ:INTC) の完全子会社であり、セキュリティ・テクノロジー専門のリーディングカンパニーです。世界中で使用されているシステム、ネットワーク、モバイルデバイスの安全を実現する革新的なソリューションとサービスを提供し、ユーザーのインターネットへの安全な接続、webの閲覧およびオンライン取引の安全を確実に支えています。

【Security Connected で実現するセキュリティ対策の最適化】

情報も脅威もボーダーレス化してきたといえる現在、世界中で日々発生している最新の脅威情報をリアルタイムにキャッチし、自社のシステム上のセキュリティリスクを可視化して迅速な対応を施さなくてはなりません。

マカフィーでは、これからの企業のセキュリティ対策としてナレッジ・プロセス・プロダクトを通じ、プロアクティブな統合管理を実現するフレームワーク「Security Connected」を提案しています。

ナレッジ

McAfee Global Threat Intelligence (GTI: グローバル脅威情報) の活用によるナレッジ形成

脅威と脆弱性および対策情報をプロアクティブに関連付け、わかりやすく即座に活用できるインテリジェンスを提供。

マカフィーでは世界30カ国に500名以上の研究者を擁する McAfee Labs を通じてグローバルでの最新脅威を把握・分析し GTI として提供しています。

プロセス

セキュリティ管理プロセスの最適化 — McAfee ePolicy Orchestrator(ePO)

マカフィーの統合コンソール ePO は、GTIと連携し、マカフィーの多様なセキュリティ製品との管理統合により、セキュリティにおける PDCA サイクルの実現を支援します。

プロダクト

プロダクトの統合一元管理 — McAfee ソリューションポートフォリオ

マカフィーでは、エンドポイント・セキュリティ、ネットワーク・セキュリティ、データプロテクション、リスク・アンド・コンプライアンスの分野において幅広いセキュリティ対策製品を提供しています。

エンドポイント セキュリティ

ブラック方式、ホワイトリスト方式からインテルの共同開発によるステルスマルウェア対策まで、様々な保護を提供しています。

ネットワーク/サーバー セキュリティ

仮想パッチソリューション、ネットワーク活動の監視といった最新の脅威対策で多層防御を実現、標的型攻撃を阻止します。

データ プロテクション

多様化するエンドポイント、肥大化する企業の情報資産に対して包括的な情報漏えい対策を提供します。

リスク・アンド・コンプライアンス管理

最新の脅威に対して IT インフラのセキュリティ状態の可視化、脆弱なエンドポイントへの対策としてアドバイザリー機能を提供します。

ソリューション、プロダクトラインナップの詳細はWebをご参照ください。

<http://www.mcafee.com/japan/enterprise/securityconnected/>

お問い合わせ先：マカフィー株式会社 〒150-0043 東京都渋谷区道玄坂1-12-1 渋谷マークシティウエスト20F
TEL: 03-5428-1100 FAX: 03-5428-1480

有限会社 ラング・エッジ

<http://www.langedge.jp/>



有限会社ラング・エッジは、親会社であるアンテナハウス株式会社が得意とするドキュメント技術を中心とした分野のセキュリティ製品の開発と受託開発をおこなっています。得意分野はPKIのノウハウを生かした電子署名・暗号化(DRM)・認証技術です。

特に電子署名に関してはPAdES(PDF長期署名)とXAdES(XML長期署名)を中心に、ETSI(欧州)プラグテストへの参加や標準化作業にも積極的に参加しています。納品実績として官公庁・地方自治体・一部上場企業をはじめとした多数があり、豊富なノウハウを有しています。開発製品は全て独自開発しており、カスタマイズの要求や受託開発にも応えられます。

電子署名やドキュメントの開発に関するお悩みがあれば是非ご相談ご連絡下さい。

PDF長期署名ライブラリ LE:PAdES:Lib



Linux版とWindows版があります。

コマンド・C++・JavaのAPIが使えます。

サーバ組み込み以外にもアプリケーションでの利用も可能です。クライアント側でプラグインによるサーバ連携の署名も可能です。

長期保管を省いたライト版もあります。

PDF長期署名は最近急速にニーズが高まっています。この機会にぜひご検討ください。

XML長期署名ライブラリ LE:XAdES:Lib



Windows版です。Linux版ご相談下さい。

C++またはC#から利用可能です。

署名対象はXML以外にテキスト・バイナリも可能で、複数同時に署名が可能です。

発売以来5年が過ぎ、官公庁・地方自治体や、上場企業等に多数の採用実績があります。

応用製品「図面XML署名ツール」もダウンロード販売中です。不動産登記対応です。

PKI-DRMシステム LE:PKI-DRM:System



PKI技術(電子証明書等)を利用してPDF等のドキュメントの閲覧を制御するDRMシステムを実現します。iPhoneやAndroidへの対応も検討中です。学術系電子書籍配信の実証実験の採用実績があります。

認証/認可システム受託開発



学術系SAML/Shibboleth開発実績あります。他にもOpenID Connect関連の実績もあります。認証に関する受託開発ご相談下さい。

また認証技術を利用したクラウド開発にも対応します。

PDF基本ライブラリ LE:PDF:Lib



Linux版とWindows版があります。

PDFの解析と編集を行う独自開発ライブラリです。PDFの知識が必要になる為に受託開発時の組み込みライブラリとして提供します。

依存性が少なく軽量のPDFライブラリです。

各製品のデモンストレーションやご相談・お打合せにも対応しています。
お気軽にお問い合わせください。

お問い合わせ先

有限会社ラング・エッジ(担当:宮地)

〒101-0032 東京都千代田区岩本2-14-12 宮崎ビル2F
03-3862-2268 contact@langedge.jp

JNSA 会員企業のサービス・製品・イベント情報です。

■サービス紹介■

○標的型攻撃診断・復旧サービス

標的型攻撃診断・復旧サービスとは、「現状把握」「対処」「再発防止」の3つで構成されています。一般的なネットワーク入口・出口での対策も勿論大切ですが、万全に防ぐことができない為、定期的に感染兆候がないかのチェックや、攻撃を受けた際にどこまで防御できて残存リスクは何か、運用でのカバーはどこまでできているかを把握し、いざ感染した際は復旧を円滑にできるようにするといった、攻撃対策を強化するサービスです。

【サービス情報詳細】

<https://www.softbanktech.jp/security/network-security/apt-check/>

◆お問い合わせ先◆

ソフトバンク・テクノロジー株式会社

TEL: 03-5206-3357

E-Mail: sbt-ipsol@tech.softbank.co.jp

■イベント紹介■

○サイバー攻撃対策セミナー 2013

実例にみるサイバー攻撃の手口とその対策

サイバー攻撃はターゲットの組織に合わせた攻撃を行うため、攻撃を発見することも困難です。その実態について事例解説と、サイバー攻撃の被害を最小限にとどめるための対策を紹介します。

■ 第2回: 9月6日 (金)

情報漏えいやウイルス感染につながる不正サイトへの誘導を防ぐ

■ 第3回: 10月4日 (金)

サイバー攻撃発見に不可欠なログ収集

【イベント情報詳細】

<http://www.dit.co.jp/seminar/13apt/index.html>

◆お問い合わせ先◆

株式会社ディアアイティ

○高度情報セキュリティ人材育成イベント開催

グローバルに認知されているセキュリティセミナーを10月に3コース開催いたします。

- ① SANS: SEC504 Hacker Techniques, Exploits and Incident Handling
- ② SANS: SEC575 Mobile Device Security and Ethical Hacking
- ③ (ISC)2: CSSLP 8ドメインレビューセミナー

JNSA会員企業様は特別割引価格にてお申込みいただけますので、JNSA事務局 (sec@jnsa.org) までお問合せください。

【イベント情報詳細】

<http://www.nri-secure.co.jp/service/learning/index.html>

◆お問い合わせ先◆

NRIセキュアテクノロジーズ株式会社

セキュリティキャリア デイバロップメントセンター事務局

TEL: 03-6274-1234

E-Mail: scdc@nri-secure.co.jp

2013年第3回日韓シンポジウム報告

今年で3回目になる日韓シンポジウムが、5月21日にソウルのCOEXコンベンションセンターで開催されました。共催のKISIA（知識情報セキュリティ産業協会）とJNSA（日本ネットワークセキュリティ協会）、JASA（日本セキュリティ監査協会）は、日本と韓国との情報セキュリティに関する情報共有と、情報セキュリティ企業との連携を目指しています。

参加者数は141名で、日本からは20名の参加がありました。末尾に当日のプログラムを掲載します。



日韓シンポジウム報告

第1部

冒頭に、KISIA会長のチョギュゴン氏、JASA会長の土居範久氏、JNSA会長の田中英彦氏から、それぞれご挨拶がありました。

両国の情報セキュリティ戦略紹介

第1部は、両国の活動の情報交換という位置付けで、現状の概要が説明されました。最初に、「両国の情報セキュリティ戦略紹介」というテーマで、韓国のKISA侵害予防団のシンファス団長から、「韓国のサーバーセキュリティ動向及び今後の課題」について話がありました。2013年3月20日の韓国でのサイバーテロの経緯などについても紹介され、正常・関心・注意・警戒・警告というレベルで対応を取っていることが話されました。

日本の情報セキュリティ戦略

次に、JNSAの中尾康二副会長から、「日本の情報セキュリティ戦略」というテーマでNISC等の活動が紹介され、攻撃の状況を見せるデモや、「サイバー情報共有イニシアティブ（J-CSIP）」の紹介の他、クラウドサービスのセキュリティについても触れられました。

コーヒーブレイクを挟んで質疑応答が行われ、モバイルと個人情報保護法について、またプライバシーを確保しながら安全に使うといった内容について活発に議論されました。

両国の情報セキュリティ市場の現況

二つ目のテーマは「両国の情報セキュリティ市場の現況」というテーマで、忠北大学のキムテソン教授から、「韓国情報セキュリティ市場及び技術の現状」が紹介されました。韓国では情報セキュリティ関係のプロフェッショナルやサービス関係の人材が少ないことが

課題になっているとのことでした。

日本からはニフティ株式会社の久保田朋秀氏より「日本の情報セキュリティ市場の現況」ということで、主にクラウドを中心にした情報セキュリティや監査について、統計情報を交えて日本の現状について説明がありました。

日韓シンポジウム報告

第2部

昼食を挟んで第2部の最初は、「機関活動の紹介及び協力案の検討」というテーマで、参加3団体の活動内容と現状が各々紹介され、パネルディスカッション形式で今後の活動に関する議論が行われました。

パネルディスカッション 1

最初に日韓双方の座長による概要と進行についての方向性が示されました。

- ・日本側：中尾副会長
- ・韓国側：ヨムフンヨル教授

次に各団体を代表して、背景や目的・活動内容など現状について発表がありました。

- ・JNSA：下村理事
- ・JASA：永宮事務局長
- ・KISIA：イジャンフン常勤副会長

韓国では、情報セキュリティ関連では製品に関するものが80%程度で、サービスに関するものが日本より少ないのが現状だそうです。

パネルディスカッション 2

次のパネル討論では、Fasoo.comのLee, SangMin氏、SECUIのチャヨンギン常務、アルテア・セキュリティ・コンサルティングの二木真明氏、株式会社インター

ネットイニシアティブの加藤雅彦氏が加わり、それぞれ意見表明を行いました。その後、中尾副会長とイジャンフン常勤副会長が日韓双方のまとめを行い、最後に次のような作業部会（WG）の作成が提案され、満場一致で了承されました。

- ・クラウドコンピューティングWG
- ・情報セキュリティ人材育成WG
- ・ビジネスのための情報セキュリティ交流WG

当面はメールベースで議論を進め、必要に応じてオフラインでも協議をすることで合意しました。

午後のコーヒブレイクの後、日韓双方の参加企業が紹介されました。韓国から4社、日本から3社が参加しました。参加企業名は下記です。

- ・MirageWorks Inc.
- ・BLUEMOONSOFT Co., Ltd.
- ・WOWSOFT Inc.
- ・IGLOO Security, Inc.
- ・株式会社ディアイティ
- ・株式会社ラック
- ・NRIセキュアテクノロジーズ株式会社

今回は、韓国でもクラウドがサービスとしてそれほど定着しているわけではないと感じましたが、何かのきっかけでブレイクする可能性は高いと思われます。

今後の日韓双方の情報セキュリティ対応の充実を期待したいと思います。

第3回 日韓情報セキュリティシンポジウムプログラム

[日時：2013.5.21(火) / 場所：COEX Hall E5(3F)]

時間	詳細内容	発表者
09:30 ～ 09:50	参加者登録	
09:50 ～ 10:10	はじめに 会長挨拶 1 会長挨拶 2	チョギュゴン 会長 (KISIA) 土居 範久 会長 (JASA) 田中 英彦 会長 (JNSA)
	第 1 部 ①両国の情報セキュリティ戦略紹介	
10:10 ～ 10:40	韓国のサイバーセキュリティ動向 及び今後の課題	シンファス 団長 (KISA 侵害予防団)
10:40 ～ 11:10	日本の情報セキュリティ戦略	中尾 康二 副会長 (JNSA/ KDDI 株式会社)
11:10 ～ 11:20	Coffee Break	
	②両国の情報セキュリティ市場の現況	
11:20 ～ 11:40	韓国情報セキュリティ市場及び技術現況	キムテソン 教授 (忠北大学)
11:40 ～ 12:00	日本の情報セキュリティ市場の現況	久保田 朋秀 (JASA/ ニフティ株式会社)
12:00 ～ 13:30	昼 食	
	第 2 部 ③機関活動の紹介及び協力案の討論	
13:30 ～ 14:50	— 座長 — 中尾 康二副会長 (日本) / ヨムフンヨル教授 (韓国) — 発表 — 下村 正洋 (JNSA) 永宮 直史 (JASA) イジャンフン常勤副会長 (KISIA)	— パネリスト — イジャンフン常勤副会長 (KISIA) Lee, SangMin 常務 (Fasoo.com) チャヨンギョン常務 (SECUI) 永宮 直史 (JASA) 二木真明 (アルテア・セキュリティ・コンサルティング) 加藤雅彦 (株式会社インターネットイニシアティブ)
14:50 ～ 15:00	Coffee Break	
15:00 ～ 17:30	参加企業の紹介 (韓国 4 社 / 日本 3 社)	MirageWorks Inc. BLUEMOONSOFT Co., Ltd. WOWSOFT Inc. IGLOO Security, Inc. 株式会社ディアイティ 株式会社ラック NRI セキュアテクノロジーズ株式会社
17:30 ～ 18:00	景品抽選及び閉会	

2013 年度 「インターネット安全教室」のお知らせ

～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。

こうした状況をふまえ、経済産業省とNPO日本ネットワークセキュリティ協会(JNSA)では、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2003年度より開催しております。

会場では参加者全員に、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」「まんがインターネット安全教室」、家庭向けリーフレット「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。

経済産業省、NPO日本ネットワークセキュリティ協会(JNSA)は、引き続き全国各地の共催団体の方々のご協力を得て「インターネット安全教室」を開催し、さらなる情報セキュリティ普及啓発活動を展開してまいります。

【開催概要】

- 【主 催】 経済産業省、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
- 【後 援】 情報セキュリティ政策会議、警察庁、その他各開催地新聞社・県・県警等(以上予定)

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。

<http://www.net-anzen.go.jp/>



◆「インターネット安全教室」共催団体募集◆

以下の地域での開催にご協力いただける団体を募集しております。
山形県、宮城県、茨城県、鳥取県、高知県、長崎県、その他離島など

- ・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

とお考えの団体等におかれましては、是非とも「インターネット安全教室」の共同開催をご検討下さい。また、そのような団体をご存知の方は是非事務局までご紹介下さい。

詳しくは下記のお問い合わせ先までご連絡下さい。

【お問い合わせ先】 NPO日本ネットワークセキュリティ協会(JNSA) 事務局(担当: 林・黒川)
E-Mail: caravan-sec@jnsa.org

情報セキュリティ対策

中小企業向け指導者育成セミナー

～グループ討議を中心とした実践型研修！～

平成25年度

主催：経済産業省
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



ポイント その1

講習会でのテキストの効果的な使い方

ポイント その2

リスクの洗い出し演習：
業務フローと情報システム管理
の両面から

ポイント その3

指導に役立つ資料やツールを
無償提供

中小企業の経営者等に対して、情報セキュリティ対策のアドバイスが適切に行える指導者を育成するため、全国で指導者育成セミナーを開催いたします。情報セキュリティ知識と指導力向上により、中小企業の情報セキュリティ対策強化にお役立ていただくために、ぜひご参加ください。



セミナー開催概要

<http://www.jnsa.org/ikusei/seminar/>

スケジュール	午前（9：30～12：00）※予定			午後（13：00～17：00）※予定	
項目	テキストを使用した講習会の実施方法 (15分)	2時間講習プログラムの組み立て方 (20分)	重要キーワードの紹介 (80分)	リスク洗い出し演習 (170分)	チェックリスト作成演習 (60分)
内容	講習会でのテキストの効果的な使い方についての解説。	講習会の2時間講習プログラムの進め方についてグループ討議。	重要キーワードと対応するページの紹介	業務フローと情報システム管理の両面で確認する事の重要性を解説し、リスクの洗い出しを行い、発表する。	課題を基にチェックリストを作成し発表。
備考	講義	講義	講義	講義・グループワーク	グループワーク

※進行状況により途中の時間帯は変動することがあります。また、途中で事務局からの説明や休憩をはさみます。

主催	経済産業省、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）
後援	独立行政法人情報処理推進機構、日本商工会議所、全国商工会連合会、特定非営利活動法人ITコーディネータ協会、全国中小企業団体中央会、一般社団法人中小企業診断協会、株式会社商工組合中央金庫（予定）、開催地の商工会議所・商工会連合会・中小企業団体中央会・その他団体等
参加対象者	中小企業の経営者等に対して情報セキュリティを指導する立場にある次のような方々。 ITコーディネータ、中小企業診断士、日商マスター、EC実践講師、その他中小企業に対して指導の立場にある方々（各団体指導員、IT関連企業の方等）、団体職員（商工会議所関係者及び商工会関係者、中小企業団体中央会関係者）等 ※毎年内容は変わっていますので、過去のセミナー受講者の方もぜひご参加ください。
参加者の特典 （過去の受講者も含む）	- 地域で指導者として活動される場合、セミナーでお配りした資料等はご自身の活動の中で自由にお使いいただけます。また、セミナーテキストも無償でご提供します。 - 指導者として登録された方が地域で条件に合致した講習会を開催される場合には、実施報告レポートの作成に対する謝金をお支払いします。（事前申請制・過去の指導者育成セミナー受講者も含む） - セミナー受講者でご希望の方については、「お近くの指導者」として、本事業のホームページ（http://www.jnsa.org/ikusei/）にお名前や保有資格を掲載して相談先として紹介いたします。 - セミナー受講者（過去の受講者も含む）は、より実践的な指導方法を学ぶことができる「講師スキル養成セミナー」（札幌・仙台・大阪・広島）の4回開催予定）の受講資格を得ることができます。 - IPA（情報処理推進機構）による指導上の相談窓口をご利用いただけます。 - ITコーディネータの方は本セミナーを受講されると実践力ポイント（6.5時間分）が付与されます。
参加費	無料（事前登録制）
その他	- 開催地域ごとの開催予定日、会場などは、裏面の会場別日程をご覧ください。 - 本事業のホームページでは、情報セキュリティの基礎知識やビデオ解説入りeラーニング、確認テストなどを掲載しています。情報セキュリティの基礎知識の習得や再確認にお使い下さい。（http://www.jnsa.org/ikusei/）

本事業のホームページでは、情報セキュリティの基礎知識やビデオ解説入りeラーニング、確認テストなどを掲載しています。情報セキュリティの基礎知識の再確認にお使いください。

中小企業情報セキュリティ対策促進事業ホームページ <http://www.jnsa.org/ikusei/>

セミナー実施会場別日程

- ・全国 20 ヶ所予定、定員は 30 ～ 50 名程度（各会場により異なります）
- ・時間 9：30 ～ 17：00 （一部地域では開始時間が異なります）

※最新の情報は本事業のホームページをご覧ください。 9月2日現在

ブロック	都道府県	地域後援団体	開催日	実施会場
北海道	北海道 (札幌)	札幌商工会議所	2013年9月27日（金）	北海道経済センター
	北海道 (旭川)	旭川商工会議所 / 旭川情報産業事業協同組合	2013年11月15日（金）	道北経済センター
東 北	秋田	秋田商工会議所	2013年11月8日（金）	秋田市にぎわい交流館 AU
	他	開催地調整中		
関 東	栃木	宇都宮商工会議所	2013年10月11日（金）	宇都宮商工会議所
	埼玉	特定非営利活動法人埼玉ITコーディネータ / さいたま商工会議所 / 埼玉県商工会連合会 / 埼玉県中小企業団体中央会 / 一般社団法人埼玉県商工会議所連合会 / 公益財団法人埼玉県産業振興公社	2013年10月31日（木）	大宮ソニックシティ
	千葉	柏商工会議所 / 特定非営利活動法人ちば経営応援隊	2013年10月8日（火）	柏商工会議所
	東京	東京商工会議所	2013年11月11日（月）	TKP大手町 カンファレンスセンター
	横浜	神奈川県商工会議所連合会 / 神奈川県商工会連合会 / 特定非営利活動法人 NPO 情報セキュリティフォーラム	2013年9月24日（火）	神奈川中小企業センタービル
	静岡	静岡商工会議所 / 特定非営利活動法人IT静岡 / 一般社団法人静岡県中小企業診断士協会	2013年11月20日（水）	静岡県産業経済会館
中 部	愛知	名古屋商工会議所 / 一般社団法人中部産業連盟	2013年10月23日（水）	ウインクあいち
	富山	富山商工会議所 / 富山県中小企業団体中央会 / 一般社団法人富山県情報産業協会 / 特定非営利活動法人ITコーディネータ富山 / 株式会社富山県総合情報センター	2013年11月29日（金）	富山県総合情報センター
近 畿	京都	京都商工会議所 ※京都会場は 10:00～17:00 の開催となります。	2013年12月13日（金）	京都商工会議所
	大阪	大阪商工会議所	2013年11月5日（火）	大阪商工会議所
	兵庫	神戸商工会議所 / 特定非営利活動法人ITC近畿会	2013年10月15日（火）	神戸市産業振興センター
中 国	広島	広島商工会議所 / 特定非営利活動法人ITコーディネータ広島	2013年10月4日（金）	RCC文化センター
	島根	松江商工会議所	2013年11月25日（月）	松江商工会議所
四 国	高松	高松商工会議所 / 特定非営利活動法人ITCかがわ / 一般社団法人香川県中小企業診断士協会	2013年12月5日（木）	高松商工会議所
九 州	福岡	福岡商工会議所	2013年10月18日（金）	福岡商工会議所
	長崎	長崎商工会議所（予定） / 長崎県商工会議所連合会（予定） / 公益財団法人長崎県産業振興財団（予定）	2013年11月22日（金）	長崎商工会館
沖 縄	沖縄	沖縄県商工会連合会 / 沖縄県商工会議所連合会 / 那覇商工会議所 / 公益財団法人沖縄県産業振興公社	2013年10月29日（火）	沖縄産業支援センター

主催セミナーのお知らせ

● 平成25年度中小企業向け指導者育成セミナー

主催：経済産業省

NPO日本ネットワークセキュリティ協会

後援：独立行政法人情報処理推進機構

日本商工会議所、全国商工会連合会

特定非営利活動法人ITコーディネータ協会

全国中小企業団体中央会

一般社団法人 中小企業診断協会

株式会社商工組合中央金庫

開催地の商工会議所・商工会連合会・中小企業

団体中央会・その他団体等

日程：2013年9月～2014年2月末（予定）

経済産業省とNPO日本ネットワークセキュリティ協会では、2008年度より開催している、中小企業の指導者となる方々への情報セキュリティの知識習得と中小企業向け指導法習得を目的としたセミナーを、今年度も全国各地で開催致します。

開催の詳細につきましては、ホームページをご覧ください。

URL：http://www.jnsa.org/ikusei/

● インターネット安全教室

主催：経済産業省

NPO日本ネットワークセキュリティ協会

後援：情報セキュリティ政策会議、警察庁、その他

参加費：無料

経済産業省とNPO日本ネットワークセキュリティ協会では、2003年度より開催している、一般の方向けの情報セキュリティ啓発セミナー「インターネット安全教室」を今年も全国各地で開催中です。

開催の詳細につきましては、ホームページをご覧ください。

URL：http://www.net-anzen.go.jp/

● SECCON 2013

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）

後援：情報セキュリティ政策会議、総務省、

文部科学省、経済産業省、警察庁、

独立行政法人情報処理推進機構（IPA）、

独立行政法人情報通信研究機構（NICT）、

一般社団法人日本経済団体連合会（経団連）、

一般財団法人日本情報経済社会推進協会

（JIPDEC）

日程・会場：

<地方予選会>

8月22日～23日：パシフィコ横浜

（SECCON×CEDEC CHALLENGE）

10月5日～6日：信州大学 工学部

10月5日～6日：九州工業大学 情報工学部

10月20日：香川大学 総合情報センター

11月9日～10日：会津藩校 日新館

11月30日～12月1日：札幌市産業振興センター

11月30日～12月1日：インテックビル

「タワー111」スカイホール

12月14日～15日：ウインクあいち

12月14日～15日：マイドームおおさか

<オンライン予選会>

1月25日～26日：情報セキュリティ大学院大学

<全国大会>

3月1日～2日：東京電機大学

（東京千住キャンパス）

日本全体のセキュリティ技術の底上げと人材の発掘・育成をはかる目的で、学生から社会人まで参加できる日本最大のハッカー大会「SECCON 2013」を開催いたします。

開催の詳細につきましては、ホームページをご覧ください。

URL：http://2013.seccon.jp/

後援・協賛イベントのお知らせ

1. S/MIME普及シンポジウム 2013 September

主 催：一般財団法人日本情報経済社会推進協会
(JIDPEC)
日 程：2013年9月9日(月)
会 場：機械振興会館会議室研修1
U R L： <http://www.jipdec.or.jp/project/anshinkan/event/20130909.html>

2. 中小企業庁委託事業

「平成25年度 情報モラル啓発セミナー」

主 催：中小企業庁、各経済産業局、
(公財)ハイパーネットワーク社会研究所
日程・会場：
2013年 9月：福岡・愛媛
2013年10月：北海道
2013年11月：島根・和歌山
2013年12月：神奈川
2014年 2月：三重
U R L： <http://www.hyper.or.jp/moral>

3. ID & IT Management Conference 2013

主 催：ノーサレンダー株式会社
日程・会場：
2013年9月18日(水)：ANAクラウンホテル
(大阪)
2013年9月20日(金)：ANAインターコンチネンタル
ホテル東京
U R L： <http://nosurrender.jp/idity2013/>

4. Gartner Symposium/ITxpo 2013

主 催：ガートナー ジャパン株式会社
日 程：2013年10月15日(火)～17日(木)
会 場：ANA インターコンチネンタルホテル東京
U R L： <http://gartner-em.jp/symposium2013/>

5. ITGI Japan カンファレンス 2013

主 催：日本ITガバナンス協会
日 程：2013年11月13日(水)
会 場：(社)全国社会福祉協議会 灘尾ホール
U R L： <http://itgi.jp/conf201311/>

6. Internet Week 2013

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(JPNIC)
日 程：2013年11月26日(火)～29日(金)
会 場：富士ソフトアキバプラザ
U R L： <https://internetweek.jp/>

7. かごしまITフェスタ2013

主 催：かごしまITフェスタ実行委員会
日 程：2013年11月29日(金)～12月1日(日)
会 場：鹿児島アリーナ
U R L： <http://www.it-festa.jp/>

JNSA 部会・WG2013 年度活動

1. 社会活動部会

(部会長: 西本逸郎 氏 / 株式会社ラック)
(副部会長: 丸山司郎 氏 / 株式会社ラック)

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に、外部に向けてメディア等を通じた情報発信や対外的な社会貢献活動、国際連携や政府機関等他組織との連携などを推進する。

具体的には、JNSA としての情報発信の後押し、政府関連の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対外活動、委託事業や外部への普及啓発などの社会貢献活動、指導者育成や講師派遣などの対外的支援活動、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: 松本照吾 氏 / 株式会社インフォセック)

経済産業省委託事業「インターネット安全教室」の内容検討、共催団体へのサポートを行う。

【指導者育成セミナー講師WG】

(リーダー: 持田啓司 氏 / 株式会社大塚商会)

経済産業省委託事業「中小企業情報セキュリティ対策促進事業」の枠組みの中、「中小企業向け指導者育成セミナー」のプログラム検討及びセミナー講師を行う。

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)

主に調査活動と技術的研究や勉強会などを行っている。調査事業としては被害調査および市場調査を2大事業として推進し、技術的研究としてIPv6などの新コンピューティング技術の調査研究、およびスマートフォン、SNSの安全な利用、内部犯行等に関する調査研究を行う。また、新たな技術の調査研究に必要な勉強会、BoFなどは随時行う。

【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)

発生確率調査を継続し、報告書を作成し公開する。2011年発生確率調査の結果から調査項目の修正、深掘りし、2012年の発生確率調査を実施する。2012年個人情報漏えい調査報告書を作成し公開する。

< 予定成果物 >

「2012年情報セキュリティインシデントに関する調査報告書 個人情報漏えい編」

「2012年情報セキュリティインシデントに関する調査報告書 発生確率編」

【セキュリティ市場調査WG】

(リーダー: 勝見勉 氏 / 株式会社情報経済研究所)

2004年度以来継続実施している市場調査を、同じ枠組みで実施する。

< 予定成果物 >

「2013年度市場調査報告書」

【IPv6セキュリティ検証WG】

(リーダー: 許先明 氏 / 株式会社ラック)

現場におけるIPv6環境でのSecurityの知見を蓄積し、公開する。

- ・実際のIPv6環境における攻撃の観測
- ・IPv4環境及びIPv4/v6 DualStack環境との比較
- ・Server構築からの全体的なSecurity知見の収集及び公開

【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: 加藤智巳 氏 / 株式会社ラック)

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正式版リリース後の情報交換と改定検討を行う。

【SNSセキュリティWG】

(リーダー: 高橋正和 氏 / 日本マイクロソフト株式会社)

2012年度でまとめた報告書のアップデートに加えて、新たなメディアについても、報告書をまとめていく予定。あまりITに詳しくない人にとってもSNSを安全に使っていただけるような、小冊子の作成も予定している。

【組織で働く人間が引き起こす不正・事故対応WG】

(リーダー: 甘利康文 氏 / セコム株式会社)

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

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

<予定成果物>

- ・「組織で働く人間が引き起こす不正・事故」における、本質的に解決すべき課題の提示（PDF形式の文書など）
- ・「組織における内部不正ガイドライン」の「ソリューションガイド」

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。具体的には、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、国際標準との親和性の高い案件については、国際標準への提案も視野に入れて、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、市場活性化を目的とする。

<予定成果物>

「アイデンティティ管理におけるロールマネジメント（第2版）」

【情報セキュリティ対策マップ検討WG】

（リーダー：奥原雅之 氏/富士通株式会社）

「情報セキュリティ対策マップ」の作成に関する以下のアウトプットを作成する。

- ・組織全体の情報セキュリティ対策の状況を確認することができる「情報セキュリティ対策マップ」のコンセプト
- ・これを作成するための手法や記述モデル
- ・実例としての汎用的な標準情報セキュリティ対策マップ案

<予定成果物>

- ・標準対策マップ案
- ・活動報告書

【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）

KISIA との共同フォーラムの開催（5月、ソウル）。

ISF との連携については、ISO/IEC 27036-4 の規格化の共同作業がメインになったこともあり、これまでのワークショップや総会参加は当面見合わせることにした。年2回のISO/IEC JTC1/SC27 会合で、今後のさら

なる進め方についても議論を進める予定である。

【電子署名WG】

（リーダー：宮崎一哉 氏

/三菱電機株式会社 情報技術総合研究所）

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

<予定成果物>

- ・PDF署名（PAdES）の適用に関する標準仕様ドラフト
- ・署名検証手順に関するガイドライン

【PKI相互運用技術WG】

（リーダー：松本泰 氏/セコム株式会社）

PKIに関する課題をWGなどで議論し、そうした活動の成果をPKI day 等のイベントで発表する。

【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）

半期に3回程度検討会を実施し、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：安田直 氏/株式会社ディアイティ）

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と共に、部会メンバーが実際に教育を行う機会を持ち、その成果を会員共同プロジェクトや産学協同プロジェクトとして実施することにより会員ならび社会に還元する。

【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）

今年度は、岡山理科大学において、履修2単位対象となる半期（6ヶ月）で計15回の講義を実施予定。TECH-Cにおいては不定期に通年で十数回程度の情報セキュリティ講義を実施予定。その他、教育部会として人材育成イベントの実施を計画中。

【情報セキュリティ教育研究WG】

（リーダー：長谷川長一 氏/株式会社ラック）

情報セキュリティの実践的な教育の手法や技術の調査研究。

昨年できなかった、情報セキュリティ教育の様々な方式（座学、演習、ワークショップ、ケーススタディ、

PBL、競技等)、手法や技術(クラウド、ソーシャルメディア、ストーリーミング等)の調査・研究を、勉強会方式で行う。

【IT・セキュリティキャリア女性活性化WG】

(リーダー:北澤麻理子氏/ドコモ・システムズ株式会社)

勉強会や講演会を隔月目途に主催し、女性のIT・セキュリティスキル向上に貢献する。

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:小屋晋吾氏/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。

【JNSAソリューションガイド活用WG】

(リーダー:小屋晋吾氏/トレンドマイクロ株式会社)

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

6. 西日本支部

(支部長:井上陽一氏/JNSA顧問)

関西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、IT利活用の実現・推進のため、産官共同して、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。

【情報セキュリティチェックシート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)

中小企業向け情報セキュリティチェックシートの改版を行い、中小企業が実際に実践可能な情報セキュリ

ティチェックシートへの作成を行う。

＜予定成果物＞

「情報セキュリティチェックシート(改版版)」

【出社してから退社するまでのリスク対策WG】

(リーダー:元持哲郎氏/アイネット・システムズ株式会社)

「情報セキュリティチェックシート」見直しに伴う、「情報セキュリティチェックシート」と「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」との整合性を確保するための修正作業を行うと共に、修正版及び追補版の検討を行う。

＜予定成果物＞

「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修正版」

「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追補版」

【企画・運営WG】

(リーダー:齋藤聖悟氏/

株式会社インターネットイニシアティブ)

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的とし、勉強会および関西情報セキュリティ団体合同セミナー等を実施する。

7. U40部会

(部会長:前田典彦氏/株式会社Kaspersky Labs Japan)

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:一宮隆祐氏/日本電気株式会社)

・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:前田典彦氏/株式会社Kaspersky Labs Japan)

U40部会員の知識・スキル向上を目指し、勉強会を企画・開催する。勉強会は講師からの講義だけでなく、グループディスカッションやライトニングトーク、ハンズオンを取り入れ、意見交換を活発化する。部会員以外のJNSA会員からも勉強会参加者を募り、部会員同士・JNSA会員・講師との人脈形成を行う。

8. 情報セキュリティ教育事業者連絡会 (ISEPA)

(代表:与儀大輔 氏/NRIセキュアテクノロジーズ株式会社)

今年度は、四半期ごとのセキュリティ人材数のWeb公開の継続及び事業者の連携事例の発表の継続を予定している。また、ISEPA イベント開催の検討も行う。

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/株式会社ラック)

セキュリティオペレーションの普及・啓発及び事業者間の技術レベル及びサービスレベル向上にむけた各種活動を行う。

<予定成果物>

「セキュリティ診断者のための基準」策定(検討中)及び「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)

セキュリティ診断に関わる技術者の持つべき技術等の基準を検討し、自主基準を策定予定。

【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実施。また、事業者間の情報連携の実践を検討予定。

【セキュリティオペレーション関連法調査WG】

(リーダー:出口幹雄 氏/富士通株式会社)

法改正、警察庁からの情報提供、官民情報共有などのSOC事業者の契約に関する意見交換。

【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:佐藤功隆 氏/日本IBM株式会社)

内部及び外部セミナーの企画、その他イベント運営、ISOG-J全般運営を実施予定。

【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)

標的型サイバー攻撃に関する情報共有と官公庁との情報連携。

10. 産学情報セキュリティ人材育成検討会

JNSA インターンシップを4月より開始、4/27(土)には東大にて発足後第1回交流会を行った。5月に学生と企業のマッチング、6月に合同説明会、7月以降にインターンシップを実施し、秋には報告会を予定。

11. SECCON実行委員会

日本全体のセキュリティ技術の底上げと人材の発掘・育成をはかる目的で、学生から社会人まで参加できる日本最大のハッカー大会「SECCON2013」の企画立案・問題作成を行います。

(SECCON2013の年間スケジュールはP24を参照下さい)

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

理 事 (50音順)

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
小橋 喜嗣 エヌ・ティ・ティ・アドバンステクノロジー株式会社
勝見 勉 株式会社情報経済研究所
桑田 潤 大日本印刷株式会社
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
桜井 鐘治 三菱電機株式会社 情報技術総合研究所
下村 正洋 株式会社ディアイティ
橘 伸俊 株式会社ネットマークス
西尾 秀一 株式会社NTTデータ
西本 逸郎 株式会社ラック
藤川 春久 セコムトラストシステムズ株式会社
宮園 充 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
本橋 裕次 マカフィー株式会社

幹 事 (50音順)

安達 智雄 日本電気株式会社
岡庭 素之 キヤノンITソリューションズ株式会社
勝見 勉 株式会社情報経済研究所
加藤 雅彦 株式会社インターネットイニシアティブ
兜森 清忠 株式会社シマンテック
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
郷間 佳市郎 株式会社日立システムズ
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
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 株式会社ネットマークス
高橋 正和 日本マイクロソフト株式会社

田中 年男 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 株式会社アーケン
二木 真明 アルテア・セキュリティ・コンサルティング
森 直彦 エヌ・ティ・ティ・アドバンステクノロジー株式会社
安田 直 株式会社ディアイティ
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 仙吉 日本アイ・ビー・エム株式会社

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 中央大学 教授
北沢 義博 法律事務所フロンティア・ロー 弁護士
武藤 佳恭 慶應義塾大学 教授
前川 徹 サイバー大学 教授
村岡 洋一 早稲田大学 教授
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
吉田 眞 東京大学 名誉教授

事務局長

下村 正洋 株式会社ディアイティ

【あ】

株式会社アーク情報システム
株式会社アークン
株式会社アイ・ティ・フロンティア
株式会社アイテクノ
アイネット・システムズ株式会社
アイマトリックス株式会社
アルテア・セキュリティ・コンサルティング
株式会社アルテミス
アルプスシステムインテグレーション株式会社
EMCジャパン株式会社
株式会社イーセクター
イーロックジャパン株式会社 **New**
伊藤忠テクノソリューションズ株式会社
イルボンテ株式会社
学校法人岩崎学園
株式会社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式会社 **New**
株式会社インテック
株式会社インテリジェントウェイブ
インフォサイエンス株式会社
株式会社インフォセック
ウェブルート株式会社
株式会社AIR
エクスジェン・ネットワークス株式会社
SCSK株式会社
株式会社エス・シー・ラボ
SGシステム株式会社
NRIセキュアテクノロジーズ株式会社
NECネクサソリューションズ株式会社
エヌ・ティ・ティ・アドバンステクノロジー株式会社
エヌ・ティ・ティ・コミュニケーションズ株式会社
エヌ・ティ・ティ・コムウェア株式会社
NTTコムテクノロジー株式会社
エヌ・ティ・ティ・ソフトウェア株式会社 **New**
株式会社エヌ・ティ・ティ・データ
株式会社NTTデータCCS
NTTデータ先端技術株式会社
F5ネットワークスジャパン株式会社
株式会社OSK
株式会社大塚商会

【か】

株式会社Kaspersky Labs Japan
キヤノンITソリューションズ株式会社
グローバルセキュリティエキスパート株式会社
クロストラスト株式会社
株式会社ケーケーシー情報システム
KDDI株式会社
株式会社コンシスト

【さ】

株式会社サイバーエージェント
サイバーソリューション株式会社
株式会社シー・エス・イー
株式会社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式会社
JPCERTコーディネーションセンター
株式会社シグマクシス
シスコシステムズ合同会社
システム・エンジニアリング・ハウス株式会社
株式会社シマンテック
株式会社情報経済研究所
株式会社ジュラリス **New**
株式会社信興テクノミスト **New**
新日鉄住金ソリューションズ株式会社
新日本有限責任監査法人
株式会社セキュアソフト **New**
セキュリティ・エデュケーション・アライアンス・ジャパン
セコム株式会社
セコムトラストシステムズ株式会社
ソースネクスト株式会社 **New**
ソニー株式会社
ソフォス株式会社
ソフトバンク・テクノロジー株式会社
株式会社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式会社

【た】

大興電子通信株式会社
大日本印刷株式会社
株式会社大和総研ビジネス・イノベーション
タレスジャパン株式会社

TIS株式会社
株式会社ディアイティ
デジタルアーツ株式会社
株式会社電通国際情報サービス
東京エレクトロン デバイス株式会社
東芝ソリューション株式会社
ドコモ・システムズ株式会社
株式会社豊通エレクトロニクス
トレンドマイクロ株式会社

【な】

日信ITフィールドサービス株式会社
日本アイ・ビー・エム株式会社
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
日本オラクル株式会社
日本サード・パーティ株式会社
日本セーフネット株式会社
日本電気株式会社
日本電信電話株式会社
日本ビジネスシステムズ株式会社
日本マイクロソフト株式会社
株式会社ネクストジェン
株式会社ネットマークス
ネットワンシステムズ株式会社

【は】

パスロジ株式会社
パナソニック株式会社
株式会社日立システムズ
株式会社日立ソリューションズ
飛天ジャパン株式会社
株式会社PFU
華為技術日本株式会社 **New**
富士ゼロックス株式会社
富士ゼロックス情報システム株式会社
富士通株式会社
富士通エフ・アイ・ピー株式会社
富士通関西中部ネットテック株式会社
株式会社富士通ソーシャルサイエンスラボラトリ
株式会社富士通マーケティング
フューチャーアーキテクト株式会社

【ま】

マカフィー株式会社

みずほ情報総研株式会社
三井物産セキュアディレクション株式会社
株式会社三菱総合研究所
三菱電機インフォメーションシステムズ株式会社 **New**
三菱総研DCS株式会社
三菱電機株式会社情報技術総合研究所
三菱電機情報ネットワーク株式会社
株式会社メトロ

【や】

株式会社ユービーセキュア

【ら】

LINE株式会社
株式会社ラック
有限会社ラング・エッジ **New**
リコージャパン株式会社
有限会社ロボック

【わ】

株式会社ワイ・イー・シー
株式会社ワイズ

【特別会員】

(ISC)² Japan
一般社団法人 コンピュータソフトウェア協会
ジャパン データ ストレージ フォーラム
公益財団法人 ソフトピアジャパン
データベース・セキュリティ・コンソーシアム
特定非営利活動法人デジタル・フォレンジック研究会
電子商取引安全技術研究組合
東京大学大学院 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セキュリティ監査協会
一般社団法人 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。）

アルプス システム インテグレーション株式会社 菅野 泰彦



皆様こんにちは。アルプス システム インテグレーション株式会社 セキュリティ事業部 渉外グループの菅野泰彦（かんのやすひこ）と申します。JNSA では、2009年からセキュリティ市場調査WG、2010年からセキュリティ啓発WG、2011年からJNSA ソリューションガイド検討WG、2012年から社会部会の活動に参加させていただいております。また弊社の本多則克が、昨年まで在宅勤務における情報セキュリティ対策検討WGに参加させていただいておりました。各WGで活動を共にする皆様や事務局の方々と真剣で楽しい交流を重ねることは、仕事はもちろん、これからの人生においても大切なつながりだと思っています。

東日本大震災の折、アルプス電気グループの東北各拠点工場へ向けて、水・非常食・衣類・その他の生活必需品を毎日の様にピストン輸送していたあの時、JNSA の理事の方が、本当に気の利いた即効性の有る救援物資を、2011年3月23日と25日の2回にわたって100点以上、間引き運転で込み合う電車に乗って池上線の雪谷大塚にある弊社まで届けてくださいました。それらは即日、東北の工場周辺の被災地の皆様に送り届けられました。こうして大勢の皆様のおかげをもちまして、東北のもののづくり産業は驚くほど早期に復旧を遂げました。復旧・復興にあたっては、セキュリティ分野を含む専門家や関係者が、日頃培った理論だけではなく実践力・行動力を今尚継続して発揮いただいております。

弊社アルプス システム インテグレーション株式会社は1990年創立、1995年からWebフィルタリング製品を開発・販売してきた日本のフィルタリング業者の草分けで、情報漏洩防止対策製品の自社開発・販売を推進する企業です。これらの製品は、企業や公共施設が平穏で正常に稼働している場面での安全安心を提供するものであり、セキュリティ市場の商品の中では主にインターナル（内部的）なセキュリティ事故を予防する種類のものです。従いまして、経済活動が順調に行われていて、セキュリティ業界の発展に貢献するJNSAの会員の皆様に認知されてはじめて満足に行く仕事ができると考えております。

現在私は、弊社の業務としてフィルタリングの利用啓発の講演を担当しておりますが、一般の方々に情報セキュリティの重要性を伝えていくJNSAの普及啓発活動に通じるテーマであることから、この分野での専門性を追求し精進して行く事を目標にしております。

これまでの皆様の温かいご支援ご協力に感謝しつつ、これからも微力ながら皆様と共にJNSAの活動をしていく所存です。どうかひとつ今後ともよろしくお願い申し上げます！

SCSK株式会社 手塚 信之



JNSA会員の皆様、はじめまして。SCSK株式会社の手塚信之と申します。株式会社ディアイティの青嶋様よりご紹介を受け、今回本コーナーを担当させていただくことになりました。

最初に私の業務のご紹介を。私自身は、この十数年、各種セキュリティ製品・サービス担当として仕事をしてきましたが、最近は少し立場を変えて、主にITシステムの運用管理よりの業務に携わっています。

具体的にはSplunkというデータ解析プラットフォーム製品を担当し、システムの障害解析からリソース管理やWebアクセス解析、毛色の異なるところでは各種センサーデータの有効活用といったことをお客様と一緒に考えていく業務となります。

皆様おなじみのログ管理の観点でのセキュリティのご相談もありますが、これまで直接関わったことのない業務領域のお話も多く、社内の各領域の専門家たちの力を借り、いろいろな刺激を受けつつ業務を進めています。

業務は少し変わったものの、セキュリティという分野への興味は尽きず、昨年JNSAでの活動としては「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」、「SNSセキュリティWG」に参加させていただいております（懇親会になると特に調子が出てきます!）。今年も引き続き活動に参加し、少しでも皆様のお役に立てればと思っています。

また、JNSA活動における今年の個人的な目標として、制限ぎりぎり最後に参加させていただいたU40部会の活動にひとりでも多くの若手を巻き込みたいと考えています。若いうちは業務調整がなかなか難しいこともありますが、同じ分野に携わる方々と交わる機会はとても得がたいものだと思います。ご興味のある方はとりあえず一度参加してみることをお勧めします。

少し堅めの自己紹介となりましたが、最後に余談を。

仕事を離れたプライベートでは、お酒と音楽、SFや歴史小説にはまりつつ、のんびりぼんやり過ごしています。こちら方面でも同好の士がいらっしゃいましたら、ぜひ一献ご一緒に。

それでは皆様、今後ともよろしくお願いいたします。

JNSA 年間活動 (2013 年度)

4 月	4 月 1 日～11 月 30 日	第 9 回 IPA 情報セキュリティ標語・ポスター・4 コマ漫画コンクール 2013	
	4 月 10 日	第 1 回幹事会	
	4 月 27 日	「産学情報セキュリティ人材育成交流会～インターンシップに向けて～」	
5 月	5 月 13 日	2013 年度理事会	
	5 月 15 日～17 日	「自治体総合フェア 2013」協賛	
	5 月 23 日～25 日	「第 17 回サイバー犯罪に関する白浜シンポジウム」後援	
	5 月 24 日	第 13 回 関西情報セキュリティ団体合同セミナー	
	5 月 27 日	第 2 回幹事会	
	5 月 29 日～31 日	「ワイヤレスジャパン 2013」後援	
6 月	6 月 7 日	JNSA 2012 年度活動報告会 (秋葉原 UDX)	
	6 月 7 日	2013 年度総会 (秋葉原 UDX)	
	6 月 11 日～14 日	「Interop Tokyo 2013」後援	
7 月	7 月 1 日～2 日	「ガートナー セキュリティ & リスク・マネジメント サミット 2013」後援	
	7 月 19 日	第 3 回幹事会	
	7 月 29 日	JNSA WG 合同セミナー「セキュリティ事故の傾向と企業で安全にソーシャルメディアを使うために～社員教育のススメ～」	
8 月	8 月 22 日～23 日	SECCON 関東大会 (横浜)	
	8 月 27 日	時事ワークショップ	
9 月	9 月 9 日	「S/MIME 普及シンポジウム 2013 September」後援	
	9 月 13 日 他	「平成 25 年度 情報モラル啓発セミナー」(9/13 福岡、9/27 愛媛) 後援	
	9 月 18 日 他	「ID & IT Management Conference 2013」(9/18 大阪、9/20 東京) 協力	
10 月	10 月 5 日～6 日	SECCON 甲信越大会 (長野)	
	10 月 5 日～6 日	SECCON 九州大会 (福岡)	
	10 月 15 日～17 日	「Gartner Symposium/ITxpo 2013」後援	
	10 月 20 日	SECCON 四国大会 (香川)	
	10 月 22 日	「平成 25 年度情報モラル啓発セミナー」(北海道) 後援	
11 月	11 月 7 日	「平成 25 年度情報モラル啓発セミナー」(島根) 後援	2013 年 7 月～ 2014 年 3 月 「インターネット安全教室」 開催
	11 月 9 日～10 日	SECCON 東北大会 (福島)	
	11 月 13 日	「ITGI Japan カンファレンス 2013」後援	
	11 月 26 日～29 日	「Internet Week 2013」後援	
	11 月 29 日～12 月 1 日	「かごしま IT フェスタ 2013」後援	
	11 月 30 日～12 月 1 日	SECCON 北海道大会 (札幌)	
	11 月 30 日～12 月 1 日	SECCON 北陸大会 (富山)	
12 月	12 月 14 日～15 日	SECCON 東海大会 (名古屋)	2013 年 9 月～ 2014 年 2 月 「平成 25 年度中小企業向け 指導者育成セミナー」 開催
	12 月 14 日～15 日	SECCON 関西大会 (大阪)	
1 月	1 月 25 日～26 日	SECCON オンライン予選会	
2 月			
3 月	3 月 1 日～2 日	SECCON 全国大会 (東京)	

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. 「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
4. JNSA 会報の配布 (年 2 回予定)
5. メーリングリスト及び Web での情報提供
6. 活動成果の配布・報告書元データの提供 (会員限定)
7. イベント出展の際のパンフレット配付
8. 人的ネットワーク拡大の機会提供
9. 調査研究プロジェクトへの参画

お問い合わせ

特定非営利活動法人

日本ネットワークセキュリティ協会 事務局

〒105-0003 東京都港区西新橋 1-22-12 JC ビル 3F

TEL: 03-3519-6440

TEL: 03-3519-6441

E-Mail: sec@jnsa.org

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

西日本支部

〒532-0011 大阪府大阪市淀川区西中島 5-14-10

サムティ新大阪フロントビル (株)ディアイティ内

TEL: 06-6886-5540

入会方法

Web の入会申込フォームにて Web からお申し込み、または、書面の入会申込書を FAX・郵送にてお送り下さい。折り返し事務局より入会に関する御連絡をいたします。

JNSA Press vol.36

2013 年 9 月 1 日発行

©2013 Japan Network Security Association

発行所

特定非営利活動法人 日本ネットワークセキュリティ協会 (JNSA)

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

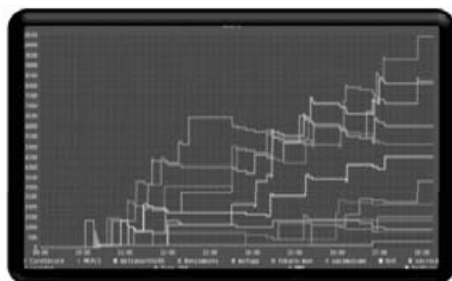
印刷

プリンテックス株式会社

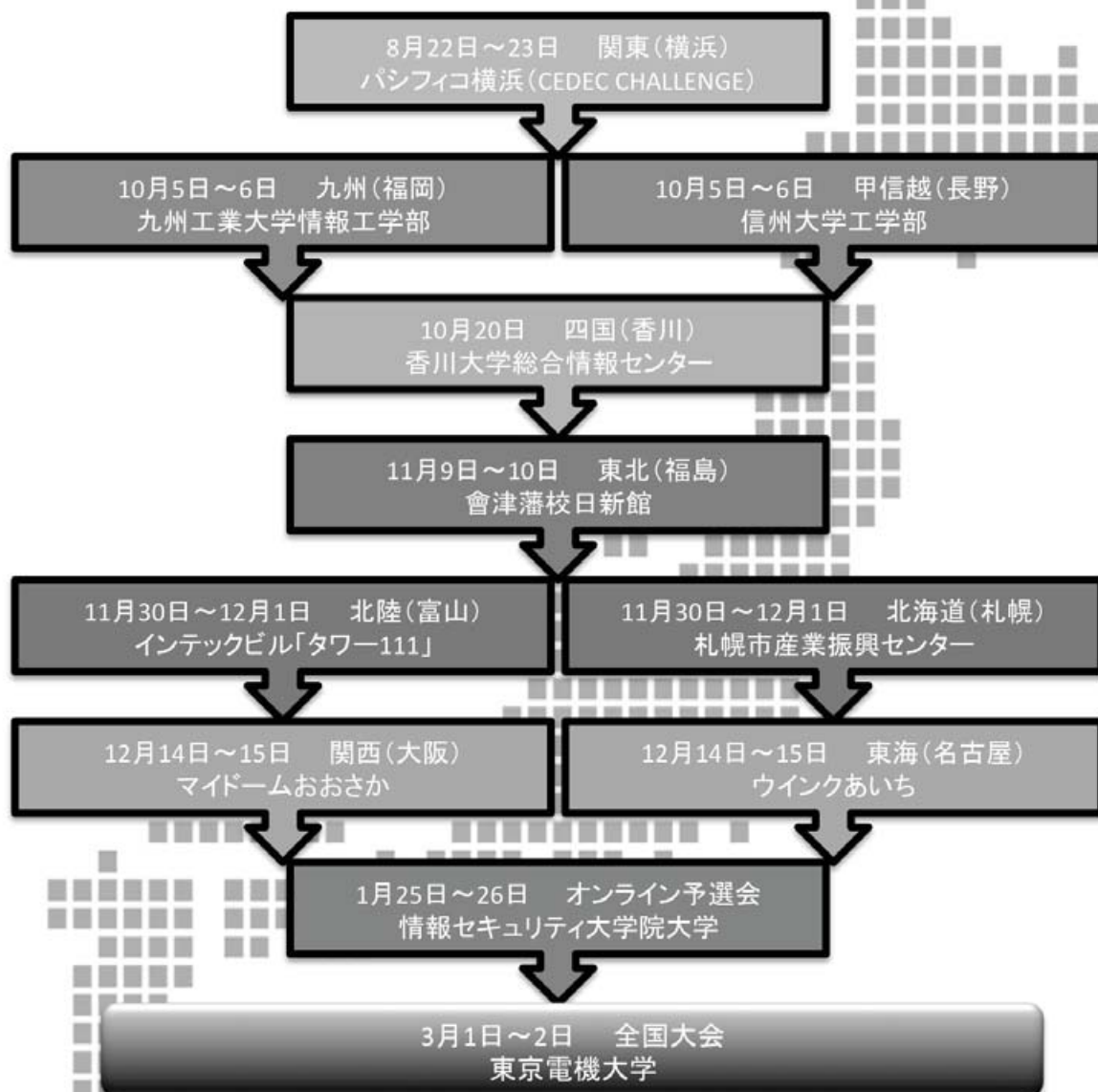
SECCON

日本最大のセキュリティコンテスト「SECCON 2013」始動！

SECCON 2013は、昨年度にJNSAが学生を対象に実施した大会に、同じく昨年度経済産業省が社会人向けに実施した「CTFチャレンジジャパン」を融合し、所属や年齢を問わず、学生から社会人まで参加できる日本最大の「ハッカー大会」を目指します。



○大会スケジュール



○詳細はこちら

※全国大会には各会場の優勝者が出場できます。

<http://2013.seccon.jp/>

NPO 日本ネットワークセキュリティ協会(JNSA)内 SECCON実行委員会 事務局
E-Mail: info@seccon.jp TEL:03-3519-6440 FAX:03-3519-6441



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

〒105-0003 東京都港区西新橋1-22-12 JCビル 3F
TEL 03-3519-6440 FAX 03-3519-6441
E-mail: sec@jnsa.org URL: <http://www.jnsa.org/>

西日本支部

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