JNSA PRESS
JAPAN NETWORK SECURITY ASSOCIATION
AUTUMN 2012 VOL. 34

寄稿

暗号技術による個人情報保護の制度と技術の動向

03

CONTENTS

01 ご挨拶
「育てる側・育つ側」
12 JNSAワーキンググループ紹介
● 情報セキュリティ対策マップ検討WG
15 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
● JNSA 2011年度活動報告会
21 インターネット安全教室
24 中小企業向け指導者育成セミナー
26 事務局お知らせ
34 JNSA年間活動
35 会員紹介

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

育てる側・育つ側

株式会社 Kaspersky Labs Japan　情報セキュリティラボ
Under40 部会 部会長
前田　典彦

多くの業界、各企業や組織にとって、人材育成はおそらく永遠のテーマであり、課題です。情報セキュリティの分野においても同様であることは、みなさまご案内の通りかと存じます。

JNSA Under40部会(以下U40部会)は、40歳以下の若年層の方々を構成メンバーとして活動している部会です。ほかの部会は、活動のテーマと内容が具体的で、それが部会やワーキンググループの名称からも見てとれるかと思うのですが、U40部会だけは少々性格を異にするような気がしています。そもそも、部会の名称だけを見ても、若手の部会である以外に内容は見えてきません。

U40部会は、JNSA設立当初から存在したわけではなく、部会としての活動が始まったのは2007年からとなっています。実は、当社がJNSAに加盟したのは同じ2007年の12月ですので、私自身はU40部会発足当初から関わっているわけではないのですが、発足初年度の部会活動趣旨として、若年層の積極的な運営参加による団体の若返り、会員間の交流の強化、若年層の活動活性化のための情報流通強化、セキュリティ業界・社会への貢献・関与などを目的とする、とあります。これは、現在の部会においても引き続き目的としているところであり、発足当初からぶれることはなく継続していると自認しています。

例えば、U40部会が主催する勉強会を通じて、知識知見の拡張や深耕を行い、いろいろな方々にお会いしてお話をすることで幅広く人脈の形成ができる活動は、将来きっとどこかで必ず役に立つときが来るであろうと思いますし、なにより、やっている当人たちが楽しんでいるところが特長だと感じています。

私が数年間U40部会の活動に参加してきて、一つ思うことがあります。至極当然のことではありますが、「待っていては何も起きないし、楽しくない」ということです。受け身でいることは楽なこともある反面、それに慣れてしまうと、いざ自身で考え行動する必要に迫られたときに、おそらくパフォーマンスを上げることはできないでしょう。

今年のDEFCON(世界最大のハッカーイベント)におけるKeith B. Alexander氏の基調講演に、興味深い発言があります。「サイバー空間を防衛するために米国が必要とする人材がこの中にいる」という趣旨です。氏は米国国家安全保障局(NSA)および中央保安部(CSS)の長ですので、その発言は非常に深く重いものであることは容易に推測できますが、先述の受け身であることと対極に居るような人々に対し「君たちの力が必要だ」というアプローチを行うことは、

人材育成の観点では非常に効果的であると感じました。残念ながら私自身は日本に居たので、会場の雰囲気を肌で感じることができたわけではないのですが・・・

人材を育成する必要がある側と、その対象者層との間の調和と意図の適合が、人材育成の鍵であるように思います。単なる教育とは全く性格を異にすることは明白です。U40部会の構成メンバーの多くは、年齢層としても立場としても育つ側にあるわけですが、こういったことを念頭に今後も活動していければと考える次第です。

最後に、U40部会はいつでも新規部会員を募集しています。JNSA会員企業のかたで40歳以下であればどなたでも参加できますので、是非お気軽にお声掛けいただければ幸いです。

暗号技術による個人情報保護の制度と技術の動向

セコム株式会社 IS 研究所
松本　泰、伊藤　忠彦

1. はじめに

個人情報を適切に保護するための暗号技術については、個人情報保護法が施行された当時から現在に到るまで、様々な議論があったようです。個人情報に限らず、暗号技術により情報を保護するためには、「暗号アルゴリズム」、「暗号モジュールの実装」、「暗号化に利用する鍵の管理」、それらすべてが適切である必要があります。

7月3日に開催された「JNSA ／第2回 鍵管理勉強会」ではこうした暗号技術・鍵管理技術のあるべき姿と、これらの技術が制度にどう組み込まれていくべきか等を念頭に、「暗号技術による個人情報保護の制度と技術の動向」を勉強会のテーマとして取り上げ、議論を行いました。

本稿では、鍵管理勉強会の議論も踏まえ、日本と米国の状況を説明し、今後の日本における課題を考察します。

2. 我が国における議論と現状

我が国の個人情報保護法は、2003 年に成立し、2005 年から全面施行されましたが、同法の施行は、情報セキュリティ業界に対しても非常に大きなインパクトがありました。こうした中、同法第 2 条第 1 項と第 20 条について、個人情報の解釈と暗号技術の扱いに対して、過去からいくつかの議論があったようです。以下に同法第 2 条 1 項と第 20 条を示します。

法第 2 条第 1 項
この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により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こととなるものを含む。）をいう。

法第 20 条
個人情報取扱事業者は、その取り扱う個人データの漏えい、滅失又はき損の防止その他の個人データの安全管理のために必要かつ適切な措置を講じなければならない。

同法に対しては、主務官庁が作成するガイドラインが 40 以上存在し、その中でそれぞれが第 2 条第 1 項と第 20 条の解釈を示しています。例えば、「個人情報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」（経済産業省 2009 年改訂）では、同法第 2 条第 1 項の「個人情報」について「暗号化等により秘匿化されているかどうかを問わない」としています。同時に、同ガイドラインは同法第 20 条の対策として「高度な暗号化等による秘匿化を講じる事は望ましい」としています。また、漏えい時には「影響を受けた本人及び主務大臣に報告することが望ましい」としていますが、「高度な暗号化等の秘匿化が施されている場合」は本人への連絡は省略して構わないとしています。

一方「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」（厚生労働省）では、個人情報の定義として「暗号化されているか否かを問いません」としていますが、別紙の Q & A では、「『個人に関する情報』であっても、暗号化により特定の個人を識別できなければ『個人情報』に該当しません」としています[1]。他にも多くの主務官庁毎のガイドラインがありますが、「安全管理措置」における暗号化等の扱いについては、様々な解釈がなされており、かつ、曖昧な扱いになっているように見受けられます。例えば、経済産業省のガイドラインでの「高度な暗号

[1] 厚生労働省の Q&A では、医療情報を 2 次利用する場合の、連結可能匿名性のために識別子の暗号化を意識したものだと思われます。

化」や厚生労働省のQ＆Aにある「特定の個人を識別できない暗号化」が何を指すかは明確に規定されていません。

2010 年 5 月に総務省の「利用者視点を踏まえた ICT サービスに係わる諸問題に関する研究会」の第二次提言では、安全管理措置を講じる際の考え方や技術的保護措置について、暗号技術のみでなく、認証、鍵管理等についても触れています。しかし技術紹介に留まっており、それらの技術を活用させる制度については触れていません。こうした状況に対して内閣官房情報セキュリティセンター（NISC）が主催する「情報セキュリティ政策会議」が 2010 年 5 月に公表した「国民を守る情報セキュリティ戦略」には、以下の記述があります。

> **個人情報保護の推進**
> 各事業分野ごとの個人情報保護に関するガイドラインの見直し、企業から個人情報等の情報の漏えいを防止する観点から、情報の適切な暗号化等を促進するため、漏えいした個人情報に適切な技術的安全管理措置が施されていた場合の手続の簡略化等、各事業分野の特性を踏まえつつ、事業者に暗号化等を行うインセンティブを付与するための見直しを行う。

「国民を守る情報セキュリティ戦略」の指摘は、内閣府の個人情報保護専門調査会でも検討されたように見受けられますが、この調査会が 2011 年 7 月に発行した報告書には、以下のような記述があります。

> 公的な認証制度がないため、法令で求めるレベルに十分な安全管理措置の判断基準はどのように確保するのかが課題である。

現在の我が国において、暗号技術による個人情報の保護は有用だという認識はあり、様々な活動はあるのですが、それを支えるスキームが不十分といった状況にあるのではないでしょうか。

3. 米国 HITECH 法の事例

前節で、日本における「暗号技術による個人情報保護」の状況について説明しましたが、では海外ではどういう状況なのか気になるところです。ここでは、米国の医療分野の事例、具体的には、米国 HIPAA/HITECH 法の事例を説明します。

米国においては、1996 年に医療情報のプライバシー保護等を包括する法律である HIPAA[2] が成立しました。しかしながら、適用対象事業体が医療機関のみ、取り締まり権限を保有するのが健康福祉省[3] のみ、情報漏えいに対する罰則が軽いなど、その適用対象や権限が十分でないという指摘がありました。それらを受け、2009 年に米国再生・再投資法[4] の一部として成立した HITECH 法[5] では、HIPAA 適用対象事業体に対し機密性に関する追加要項が課せられました。HITECH 法では HIPAA の罰則規定も大幅に拡大されました。例えば、個人識別可能な医療情報を漏えいした場合は、最大で 10 年の懲役及び 150 万ドルの罰金（1 件については最大 5 万ドル）が課せられる可能性があります。また、健康福祉省以外に州の司法長官にも取り締まり権限が与えられました。

HITECH 法の漏えい通知ルール

HITECH 法おいて、特に個人情報・プライバシー保護との関連性が高い要項として、保護医療情報[6] が漏えいした場合に対象者全員への通報を義務付け

[2] Health Insurance Portability and Accountability Act
[3] HHS：Department of Health and Human Services
[4] ARRA：American Recovery and Reinvestment Act
[5] Health Information Technology for Economic and Clinical Health Act)
[6] PHI：Protected Health Information

るとともに、うち 500 人分以上の保護医療情報が漏えいした場合に、健康福祉省、連邦取引委員会[7]及びメディアに対して通報を行うよう義務付けている点があります。

HITECH 法における個人情報漏えいとは

HITECH 法において、情報が安全でなく（unsecure）、健康福祉省及び連邦取引委員会に通報義務が発生する事態を明示するため、健康福祉省は保護医療情報についてのガイドラインを更新し、無権限者による使用、判読、及び復号をできなくするための、暗号化と破棄についての技術と方法論を記載しています。
同法では、それらの技術と方法論で守られた情報が漏えいしても、NIST[8] の技術ガイドラインに記載される方法（表 1）による暗号化又は破棄が為されているならば、安全（secure）な医療情報であるとしています。

HITECH 法のスキーム

HITECH 法において適用対象事業体（Covered entity）に対する主務官庁は健康福祉省なのですが、技術的なガイドライン、HITECH 法で要求される情報システムの試作、技術や啓発活動促進のための R & D プログラム、テストデータ等を NIST が提供しています。また、個人情報を適切に保護するための暗号技術、その暗号モジュールの安全性を試験する CMVP[10] も NIST が行っています。このように、医療サイドの要望ベースの法案を、NIST が技術的にサポートするスキームになっています。（図 1）

CMVP は、米国政府機関が暗号技術ソリューションを調達する際の基準ですが、客観的な評価がもとめられる暗号技術ソリューションでは、評価の難しさもあり、CMVP のような評価・認証制度が重要な意味を持つ様になりました。CMVP の基準達成は、暗号技術ソリューションベンダーにとって高いハードルだったのですが、そのハードル越えを米国政府が支援することにより、ベンダーを育成した側面もあります。HITECH 法の法制度においても、高額な罰金などの刑事罰を規定する一方で、通知義務を守れば一定の範囲内で罰が軽減される可能性があり、CMVP により認証された暗号技術ソリューションの選択は利用者（適用対象事業体）のインセンティブとして働いているようです。

4. 自己暗号化ストレージ（記憶媒体）

前節では、米国 HITECH 法の事例を説明しま

表 1：HITECH 法が引用するガイドライン一覧[9]

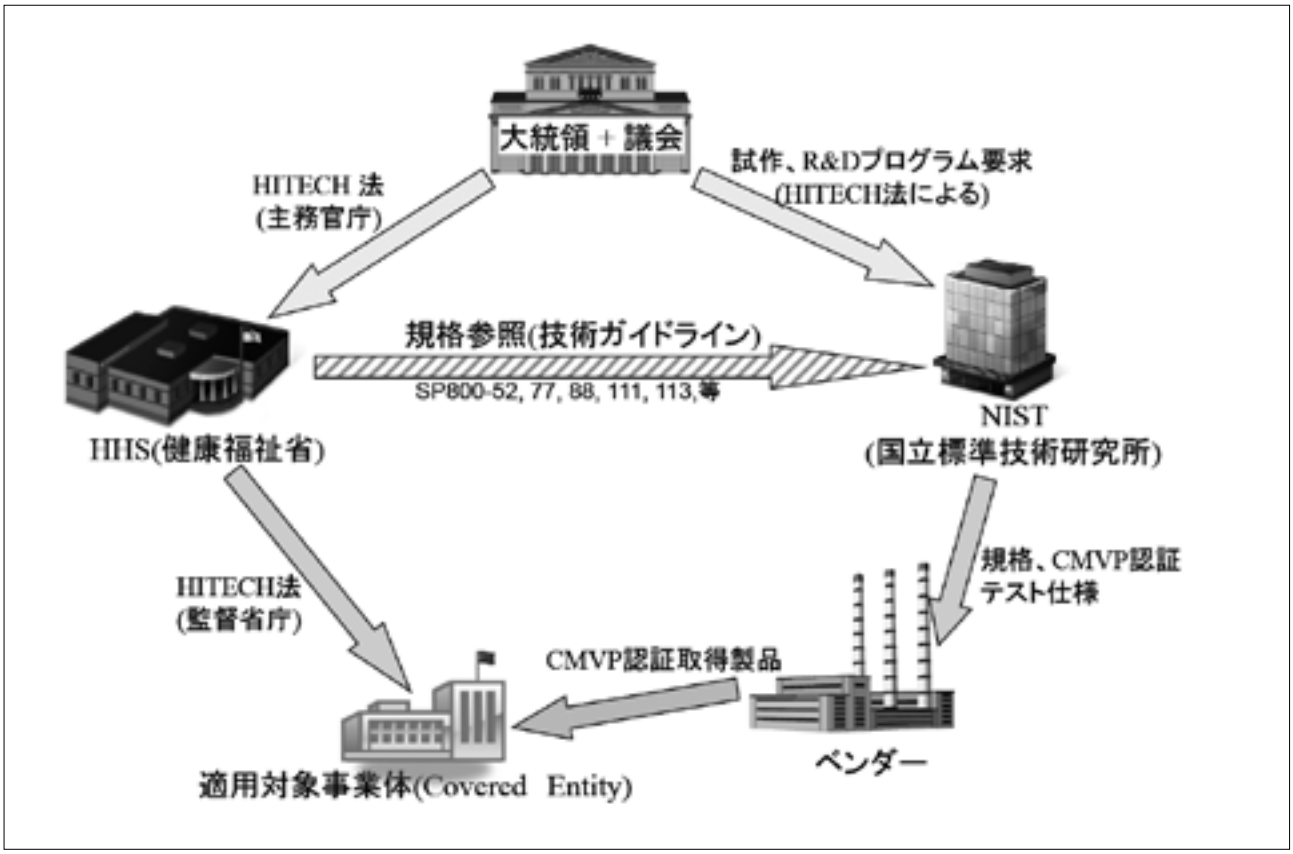
セキュリティのドメイン	ガイドラインの例	内容
移動中のデータ（Data in Motion）	NIST SP800-52 （2005）	安全な TLS の利用法
	NIST SP800-77 （2005）	安全な IPsec VPNs の利用法
	NIST SP800-113（2008）	安全な SSL VPNs の利用法
保管データ（Data at Rest）	NIST SP800-111（2007）	エンドユーザ向けのストレージ暗号化
使用中のデータ（Data in Use）	なし	処理中の秘密情報の扱いなど
データの処分（Data Disposed）	NIST SP800-88 （2004）	電子メディアの破壊など

[7] FTC：Federal Trade Commission
[8] 国立標準技術研究所 (National Institute of Standards and Technology)
[9] HITECH Breach Notification Interim Final Rule -（Ⅱ）Guidance Specification より抜粋。
[10] Cryptographic Module Validation Program：FIPS 140-2 に基づいて米国・カナダで運用されている暗号モジュール評価制度であり、米国及びカナダ政府による、セキュリティ機器の調達基準として用いられています。

したが、このHITECH法における「データ保管」（Data at Rest）の技術的なガイドラインは、SP800-111（Guide to Storage Encryption Technologies for End User Device）になります。米国においては、このガイドラインに沿ったデータ保管のエンドユーザ向けのソリューションとして、比較的「鍵管理」が容易な、「自己暗号化ストレージ」なる製品カテゴリの暗号技術ソリューションが数多く出現しています。これは、ディスクの盗難や置き忘れ等への対策であり、日本においても、その扱いが課題となっています。例えば、PCを持ち出す際にどの程度の保護措置を行うのか、デバイス紛失時の対処方法、完全に持ち出し禁止にすると利便性の問題が生じる、などが課題として指摘されていました。

自己暗号化ストレージ製品としては、HDD、SSD、USBデバイスがあります。ここでは最初にSP800-111における自己暗号化ストレージの概念を紹介します。また、自己暗号化USBデバイス実装におけるCommon Criteria（ISO/IEC 15408）のプロテクションプロファイルとして、2011年にNSA[11]が発行した、Protection Profile for USB Flash Drive[12]（以下PP for USB）を紹介します。

図1：HITECH法のスキーム



[11] アメリカ国家安全保障局：National Security Agency

[12] このPP for USBは、CCRA（CCに基づいたセキュリティ評価結果の相互認証に関する協定）加盟国のグローバルな政府調達要件として発行されています。

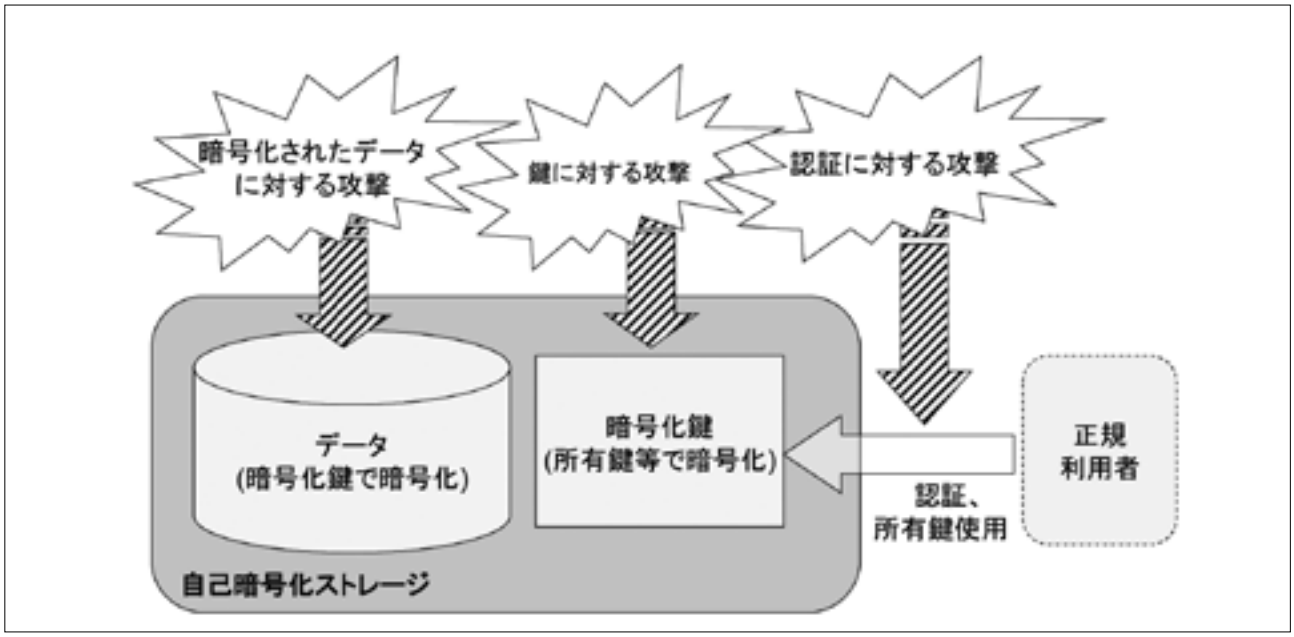
SP800-111 における自己暗号化型ストレージの概念は図 2 で示されています。保管データはデータ暗号化用の鍵（以下 DEK）で暗号化されストレージに保管され、データ暗号化鍵は正規の利用者が所持する鍵暗号化用の鍵（KEK）により暗号化され保管されます。利用者は KEK を複数の認証要素に分散することも可能です。正規の利用者は認証要素を使い認証 [13] された後に、KEK を使う事で DEK を取り出し、DEK を使い復号することでデータを取り出します。SP800-111 では暗号化されたデータ及び暗号鍵に対する安全性については言及されていましたが、鍵管理や認証構造については十分言及されていなく、CMVP と各ベンダーの実装に任されているようです。SP800-111 を受け、2008 年以降、多くのベンダーが、自己暗号化機能付き USB フラッシュデバイスを製品化しており、また CMVP の認証を取得しています [14]。

これまでの CMVP 認証取得製品では、利用者（役割）認証構造をはじめ詳細な仕様については各社が独自に実装していましたが、2011 年 NSA により作成された PP for USB では、SP800-111 の概念を実装する方式が述べられています。（図 3）具体的には、鍵及び秘密情報の管理や、それらの強度を同程度にすることにより暗号モジュール全体の安全性を確保する方法が述べられています。

PP for USB では、2 種類の鍵（DEK 及び KEK）と最大 3 種類の認証要素が秘密情報として用いられます。それらの関係は以下のようになります。

データは AES（Advanced Encryption Standard）[15] により暗号鍵 DEK を用いて暗号化され、暗号化された状態でデバイスに保存されます。DEK は AES 又は排他的論理和によりは暗号鍵 KEK を用いて暗号化され、暗号化された状態でデバイスに保存されま

図 2：自己暗号化ストレージが対応する攻撃



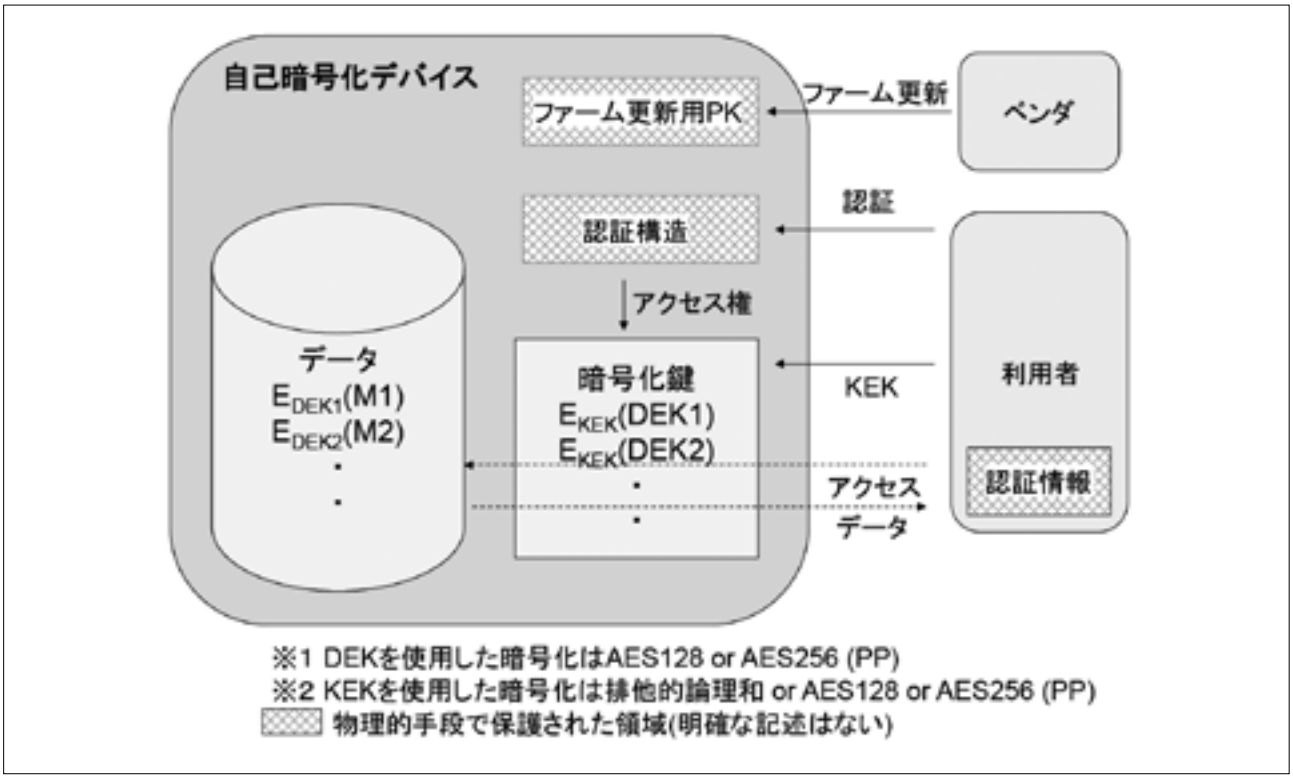
[13] ここでの認証は Authentication の意味ですが、CMVP 等に関する記述における認証は Certification の意味なので注意願います。
[14] IPA の「暗号モジュール試験及び認証制度のご紹介」では、USB フラッシュドライブとして、セキュリティレベル 2 のものが 8 件、セキュリティレベル 3 のものが 13 件、CMVP 認証されていると紹介されています。
[15] 米国政府標準暗号。

す。KEK は①辞書にある単語 9 個以上からなるパスフレーズ（を一方向関数で処理したもの）、② 2^256 以上の情報量を持つトークン、③その他の認証要素、の排他的論理和により使用の度に計算されます。ここで①又は②は必ず含まれなければいけませんが、3 種類全て用いる必要はありません。ここで注目したいのは、DEK を 256 ビットとしても、①～③全てと KEK が同程度の鍵空間を持つ事です。

PP for USB では、データを暗号化する鍵である DEK が取りうる領域を「エントロピ」という概念で表現し、KEK や認証要素も DEK と同程度のエントロピ（≒鍵強度）を持つ事を要求しています。また、デバイスや利用者の OS 内に秘密情報を残さないような細かな規定をし、アクセス制御についても言及しています。暗号技術ソリューションの安全性は、設計、実装、運用、管理のうち一番低いものに落ちることは以前から頻繁に指摘されていましたが、実際には徹底されているとは言いがたい状況でした。PP for USB では、暗号モジュールの各段階における強度を「鍵のエントロピ」という形で統一することを要求しており、鍵管理という点でも参考になります。

表 2 は米国における自己暗号化ストレージの規格、認証基準等です。これらの規格群により個人情報を安全に保護するための技術要求を明確にし、また、要求を満たした暗号技術ソリューションへの認証制度等が整備され、そうした製品の利用にインセンティブを付与する法制度があり（HITECH 法等）、また、実際に利用できる暗号技術ソリューションが多く出現しています。これは、適切な暗号技術に対してベンダーと利用者へのインセンティブを与える制度的なスキームが機能している結果ではないでしょうか。

図 3：PP for USB における自己暗号化デバイスの概念図



5. 日本における今後の課題

米国においては、先に示した「自己暗号化ストレージ」は暗号技術を利用した適切な個人情報保護のための暗号技術ソリューションとして確立しつつあるようです。

我が国において、2005 年に全面施行された個人保護法は、社会に大きなインパクトを与え、また、情報セキュリティ業界においても個人情報保護バブルとも揶揄されるほどに大きな影響がありました。しかし、施行から 8 年も経過したにも係わらず、個人情報を適切に保護するための暗号技術ソリューションの状況は、米国の状況とは大きく異なるように見受けられます。

個人情報保護法第 20 条の「個人データの安全管理のための必要かつ適切な措置」は、様々な観点があり単純な日米比較が出来る訳ではありません。しかし、データ保管のための暗号技術ソリューション確立という観点からは、我が国は、米国より大きく遅れているように見受けられます。日米の比較から、今後、我が国で検討されるべきことは、以下の 3 点になるのではないでしょうか。

(1) 個人情報保護法に関連する技術ガイドラインの統合
(2) 暗号技術における鍵管理技術の重要性の周知と施策
(3) 情報化社会における技術と制度の整合

個人情報保護法に関連する技術ガイドラインの統合

我が国において、個人情報保護法のガイドラインは、各業界の主務官庁毎に作成されています。確かに、業界毎に守るべき組織や情報が異なるため、個別のガイドラインの必要性はあります。

米国の個人情報保護法は、セクトラルモデルであり、やはり、そのガイドラインは個別の業界毎に作成されているようです。しかし、個人情報を適切に保護するための技術ガイドラインとしては、NIST が作成しているもの（SP800 シリーズ）が参照されている場合が多いようです。

NIST の SP800 シリーズに近いものとしては、我が国の内閣官房情報セキュリティセンターの「政府機関の情報セキュリティ対策のための統一基準群」等がありますが、これは、政府機関向けのものであり、民間の規範となるものを目指している訳ではないように見受けられます。こうしたこともあり、個人情報保護法に関しては、各業界向けには統一された技術ガイドラインが整備されていません。各技術ガイドライン要求は業界毎に作成され、統合されていませんし、既存の各ガイドラインにしても技術要件が明確に規定できていません。これが「個人データを安全管理するた

表 2：自己暗号化ストレージを取り巻く規格、標準、認証制度

類　別	規格、標準、認証制度
ガイドライン	NIST SP800-111
仕様	TCG Opal[16] 自己暗号化ディスク仕様など
プロテクションプロファイル	NSA フルディスク暗号化のプロテクションプロファイル、2011/12/1、バージョン 1.0
	NSA USB フラッシュデバイス用のプロテクションプロファイル、2011/12/1、バージョン 1.0
FIPS140-2　認証製品（CMVP）	TCG Opal 仕様の自己暗号化ディスク（Seagate のハードディスク、Samsung の SSD などの製品）
	多くの暗号化 USB デバイス

[16] 標準技術を策定する業界団体である TCG（Trusted Computing Group）によるストレージ暗号化に向けての規格のこと。

めの必要かつ適切な措置」に対応した適切な暗号技術ソリューションが確立しない原因のひとつになっているのではないでしょうか。

暗号技術における鍵管理技術の重要性の周知と施策

暗号技術ソリューションが適切に機能するには、「暗号アルゴリズム」、「暗号モジュールの実装」、「暗号化に利用する鍵の管理」全てが適切に機能しないといけません。

暗号アルゴリズムが安全でも、例えば暗号鍵を管理するパスワードに脆弱なものを使用したり、実装に脆弱性が存在すれば、データが漏えいする可能性は高まり全体として十分な強度が保てません。つまり、暗号アルゴリズムの強度だけでなく、暗号化に利用する鍵管理の運用や実装も含めて適切なレベルになるよう考える必要があります。我が国においては、この部分の認識が希薄であり、特に鍵管理に関する技術や運用のプラクティスもおざなりになっていたのではないでしょうか。

エンドユーザ向けの自己暗号化ストレージ等の暗号技術ソリューション利用において、「暗号アルゴリズム」に関しては電子政府推奨暗号アルゴリズムを参照すればよいのですが、「暗号モジュールの実装」、「暗号化に利用する鍵の管理」に関しても我が国の制度は十分機能してないように見受けられます。今後は、利用者レベルの鍵管理を提供する仕組みや、その実装の安全性を保証する認証制度を整備するべきではないでしょうか。

米国の場合、暗号技術を利用したものに関しては、CMVP が認証制度として定着しており、利用者は多くのことを理解せずとも CMVP 認証製品リストから暗号技術ソリューションを選択すればよいことになります。個人情報保護専門調査会の報告書では、暗号技術ソリューションが定着しない理由として公的な認証制度がないことを挙げていますが、実際には、我が国においても、米国の CMVP に対応する JCMVP（Japan Cryptographic Module Validation Program）[17] があります。しかし、この JCMVP の認知度は非常に低く、また、認証製品も米国の CMVP に比べ極端に少ないのが現状です。これにはいくつかの要因がありますが、そのうちのひとつは、鍵管理技術の重要性が認識されていないことではないでしょうか。JCMVP の様な認証制度を機能させ、暗号技術ソリューションを活用する上でも、鍵管理技術の重要性を周知させることが必要でしょう。

情報化社会における技術と制度の整合

情報技術、情報通信技術が社会の基盤として不可欠となるにつれて、情報セキュリティと制度との関係が重要になっています。そのような状況で、2000 年以降、情報セキュリティにも関係の深い、様々な制度が施行されてきました。しかしながら、技術と制度が噛み合わないために、こうした制度が有効に機能していない面が多々あるのではないでしょうか。また、制度の見直し等の議論においても、技術と制度の関係者の間で意思疎通が成立していないように感じることがよくあります。本稿では、個人情報保護法に着目し、「情報化社会における技術と制度の整合」の必要性を考察することを試みているところがあります。

社会から、適切な個人情報保護の仕組みが求められており、実際に適切な暗号技術を利用すれば効果的な対策が可能なはずにも拘わらず、ベストプラクティスと言えるような暗号技術ソリューションが確立できていません。これは、個々の技術の問題というよりは、もう少し広い問題で、技術と制度を整合させるためのスキームに課題があるように感じられます。。このあたりの考察は、本稿において、まだまだ稚拙なところはあるかと思いますが、今後の情報化社会に対応した情報セキュリティの制度と技術のあるべき姿を議論する上で参考になれば幸いです。

[17] JIS X 19790 に基づいて IPA により運用される暗号モジュールの評価制度。2012 年より CMVP との共同認証も行っている。

参考文献

◇国内の法令・ガイドライン

個人情報保護法 , (2003)

個人情報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（2009 年改正）
http://www.meti.go.jp/policy/it_policy/privacy/kaisei-guideline.pdf

医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン（2010 年改正）
http://www.ajha.or.jp/about_us/nintei/pdf/101014_1.pdf

「医療・介護関係事業者における個人情報の適切な取扱いのためのガイドライン」に関するＱ＆Ａ（事例集）、(2010 年改正)
http://www.mhlw.go.jp/topics/bukyoku/seisaku/kojin/dl/170805iryou-kaigoqa.pdf

◇国外の法令・ガイドライン

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191)

American Recovery and Reinvestment Act of 2009 (Pub.L. 111-5)（HITECH はこの一部）

HITECH Breach Notification Interim Final Rule, (2009)
http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/breachnotificationifr.html

NIST, Guide to Storage Encryption Technologies for End User Device（SP800-111）, (2007)
http://csrc.nist.gov/publications/nistpubs/800-111/SP800-111.pdf

◇その他の参考資料

暗号モジュール試験及び認証制度のご紹介
http://www.ipa.go.jp/security/jcmvp/documents/open/jcmvp_session_20120312.pdf

「国民を守る情報セキュリティ戦略」における「情報セキュリティ政策会議」
http://www.nisc.go.jp/conference/seisaku/

個人情報保護専門調査会報告書
http://www.cao.go.jp/consumer/iinkai/2011/067/doc/067_110826_shiryou3.pdf

JNSA 第 2 回鍵管理勉強会（2012）
http://www.jnsa.org/seminar/seckey/120703/

NSA, Protection Profile for Full Disk Encryption,（日本語訳：フルディスク暗号化のプロテクションプロファイル）(2011)
原文：http://www.niap-ccevs.org/pp/PP_FDE_v1.0/
日本語：http://www.ipa.go.jp/security/publications/niap/spp-jp/pp_fde_v1.0-J0.1.pdf

NSA , Protection Profile for USB Flash Drives,（日本語訳：USB フラッシュデバイス用のプロテクションプロファイル）(2011)
原文：http://www.niap-ccevs.org/pp/PP_USB_FD_v1.0/
日本語：http://www.ipa.go.jp/security/publications/niap/spp-jp/pp_usb_fd_v1.0-J0.1.pdf

FIPS140-2, http://csrc.nist.gov/publications/PubsFIPS.html

謝　辞

本稿の執筆および、第二回鍵管理勉強会の企画では、みずほ情報総研の小川博久様に有益なご助言を頂きました。
ここに感謝致します。

JNSA ワーキンググループ紹介

情報セキュリティ対策マップ検討 WG

WG リーダー　富士通株式会社　奥原　雅之
WG サブリーダー　富士通株式会社　長谷川　喜也

■ 発足の背景

情報セキュリティ対策マップ検討 WG は、技術部会に所属する WG です。組織にとって最適な情報セキュリティ対策を系統的に検討する場面においては、対策するべき情報セキュリティの全体像を正確に把握できるドキュメントがあると大変便利です。そこで、「組織が持つ情報セキュリティの対策を正確に描ける地図」がもしあるとしたら、それは一体どういうものかということを検討し、作成するための手法、記述モデル、および汎用的な標準情報セキュリティ対策マップ案を開発することを目的に 2009 年 1 月より活動を開始、今年で 4 年目を迎えました。

■「情報セキュリティ対策マップ」は何故必要か

以下の様な悩みを的確に解決する方法を皆様はお持ちでしょうか?

『A さんの会社では、ファイアウォールを導入してから大分経ったので入れ替えを検討している。

新しいファイアウォールの選定をする担当になった A さんは、情報セキュリティ製品ベンダを呼んで話を聞いたところ、そのベンダは「当社では、価格の高いファイアウォールと、価格の安いファイアウォールの二種類を扱っている。価格の高いファイアウォールには、価格の安いファイアウォールに搭載されていない UTM（統合脅威管理）の機能があり、特にアンチウイルス機能が自慢だ。ここにあるガイドラインにも、『複数ベンダが提供する不正プログラム対策ソフトの利用を検討するように』と書いてある。」とあるガイドラインを提示しながら説明した。

この話を上司にしたところ、「当社では全てのパソコンにアンチウイルスソフトウェアを導入してウイルス対策を行っているから、いまさらファイアウォールの所にアンチウイルス機能はいらないと思うが、それが必要だというガイドラインがあるのであれば、その有効性を良く検討しなさい。」との回答が返ってきた。

A さんは困った。「確かにファイアウォールと個々のパソコンの二箇所でウイルス対策をした方が、セキュリティは高い気がする。しかし、パソコンのウイルス対策だけでは足りない、とも言い切れない。ベンダが提示したこのガイドラインは、当社のリスクに対応する対策として適切なのだろうか。」』

この悩みを解決するためには、A さんの会社のリスクと取り得る対策の関係を正確に記述する方法が必要です。それがあって初めて「当社のこのリスクは、この対策で対応する」と決定することができるのです。そのための拠り所となるのが、世の中の全ての対策の関係を表した地図「情報セキュリティ対策マップ」なのです。この WG ではこの「情報セキュリティ対策マップ」の開発を目指しています。

■ 検討の様子

2008 年 12 月に準備会を開催し、2009 年 1 月より正式に WG として活動を開始しました。これまで、ほぼ二週間ごとに活動をおこない、4 年目となった 2012 年 8 月現在、通算 79 回の WG を開催しています。2011 年には長期にわたり活動した事を評価され、JNSA 表彰を受賞しました。

これまでの活動では、世の中のガイドラインに載っている、情報セキュリティ対策といわれる物をたくさん収集してきて、それを分類するところから検討を始め、集まった対策をグループ分けしてグループ間の構造を表した「対策構造図」（図 1）や、2 つの対策間の関係を繋げていってツリー構造で表した「川図法(仮称)」(図 2) などを開発してきました。

現在は、情報セキュリティ対策そのものの構造に着目して、オブジェクト指向を取り入れた、「対策オブジェクトモデル V3」（図 3）を創案し、その有効性を JIS Q 27002（ISO/IEC 27002）を使って検証中です。

図 1. 対策構造図

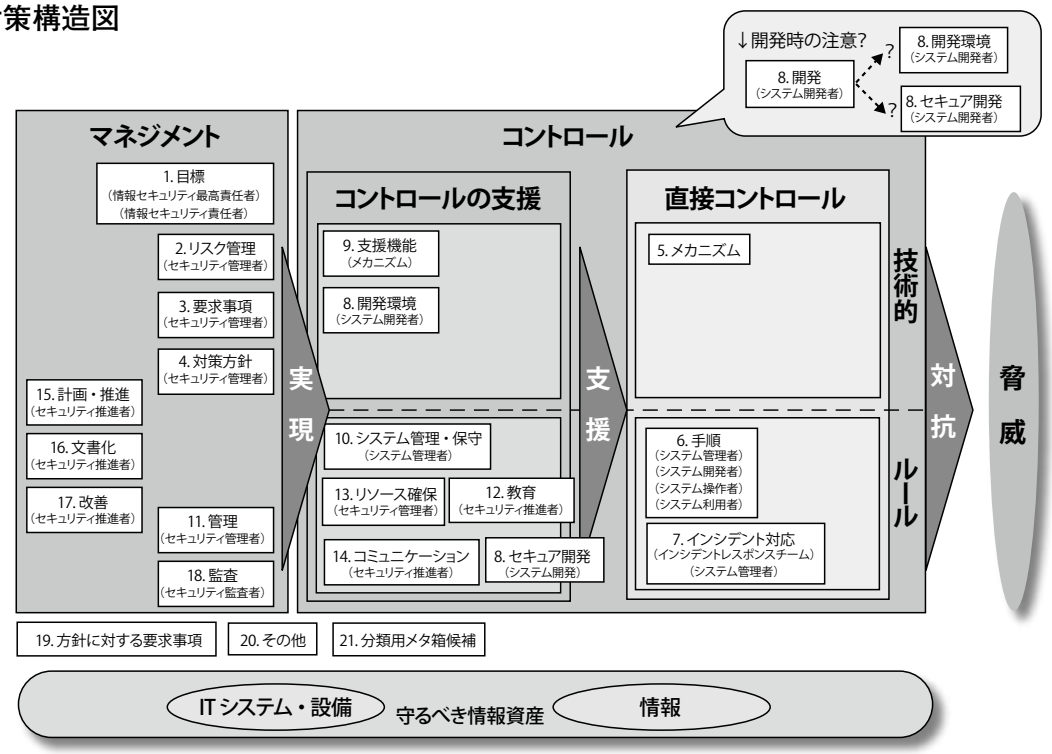
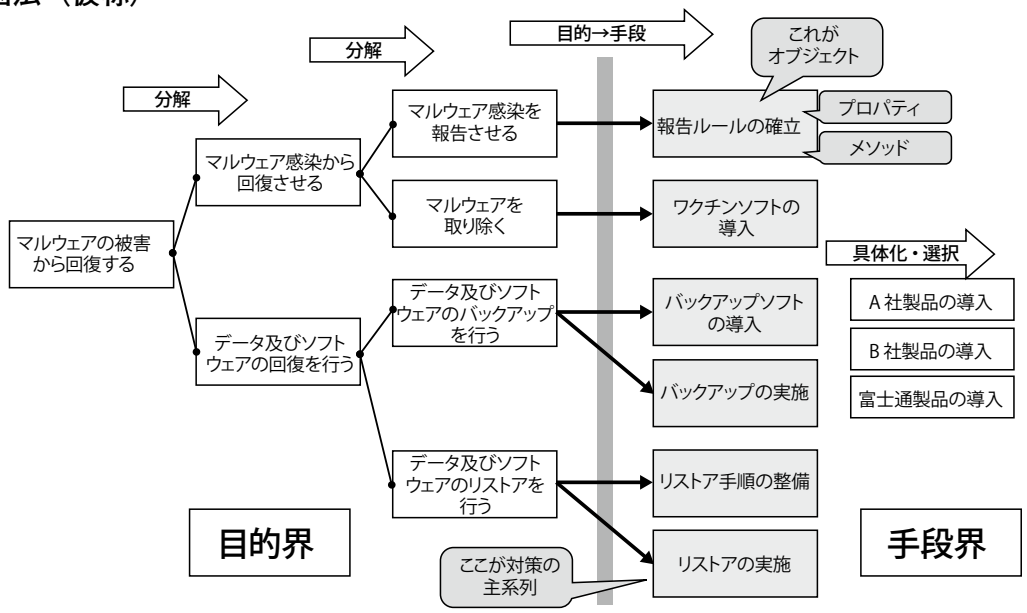


図 2. 川図法（仮称）



JNSA ワーキンググループ紹介

図 3. 対策オブジェクトモデル V3

オブジェクト		「管理策」。		
プロパティ		方針 目的 機能 要求事項 場所 条件 時間 実施者 対象者・対象物		
メソッド	計画	検討する 計画する	コストを算定する 文書化する	方針を確立する 有効性の測定方法を決める
	準備	責任者を明確化する 機能を明確化する 導入条件を明確化する リソースを確保する 手順を確率する	利用者を明確化する 要求事項を明確化する 導入する時を明確化する 導入する 手順を文書化する	実施者を明確化する 導入場所を明確化する 手順を明確化する 利用者を教育（訓練）する
	実施	【実施する】 レビューする	実施時に注意を払う 実施を記録する	保守（維持）する
	レビュー	実施状況を監査する	有効性を測定する	見直す
	改善	改善する	廃止する	

WG 発足当初は、3 年で結果を出す予定でしたが、はからずも 4 年目に突入してしまい、今年こそは皆様にお披露目できる成果物を完成させたいと思い活動をしています。

グループのメンバーは「来る物は拒まず、去る者は追わず」の方針で募集しているため、登録者数は 30 名を超えていますが、コアとなって活動をしているのは、7 名程度です。ご興味のある方は、いつでも歓迎をしておりますので、是非ご参加ください。

会員企業ご紹介34

株式会社イーセクター

http://www.esector.co.jp/

株式会社イーセクターはセキュリティプロダクト専門のディストリビューターです。
世界中から優れた製品を集め、特定のメーカーやプラットフォームに依存することなくお客様のニーズやご予算に最適なソリューションを販売するのみならず、運用提案、サイジング等のプレサポートからシステム構築、保守まで提供します。

シーイーシーグループ
CEC
Computer Engineering & Consulting

30余年のパッケージソフトウェア販売・保守実績。
豊富なセキュリティ商品で、お客様のセキュアなシステム構築を支援します。

イーセクターの特長

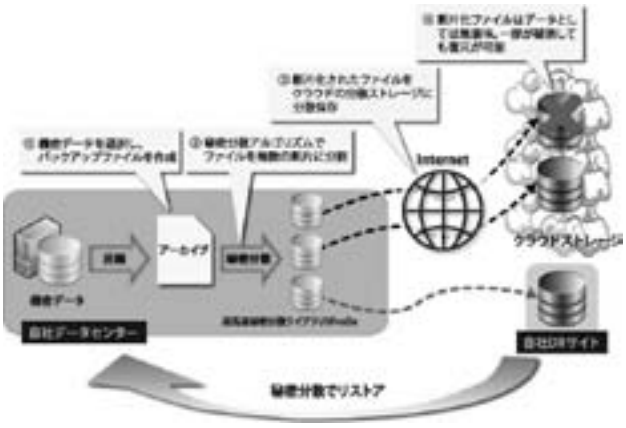
◆メーカーや特定の製品にしがらみがないためユーザ本位の提案ができる
◆システム設計、サイジング、導入支援等のサポートが充実している
◆情報漏洩、情報消失に注力したソリューションの提供
◆システムインテグレーター、データセンター事業者向けにも製品を拡充
◆プライベート／パブリッククラウドやスマートフォンなどの最新のニーズにもいち早く対応
◆ひとつのカテゴリに複数のソリューションを用意し、お客様がニーズや予算に応じて多彩な選択が可能

最新販売製品 eSECTORSecureOnlineBackup

機密データを秘密分散で断片化し、分散保存します。
BCP（事業継続計画）対策や障害対策、ディザスタリカバリに最適なソリューションです。

■ 秘密の情報を意味のない複数の断片へ「分散」
■ 断片を一定個数(しきい値)以上集めて「復元」

「暗号」とはレベルの異なる安全性、しきい値未満の断片からは、スーパーコンピュータを10億年使っていたとしても、秘密の情報は一切漏れない。



イーセクターイベント情報

仮称のため、変更になる場合があります。

11月開催予定。
当社が推奨する製品をご紹介
参加費:無料
詳細は、WEBで告知致します。
http://www.esector.co.jp/

お問い合わせ先
株式会社イーセクター　プロダクトソリューション部
〒150-0022 東京都渋谷区恵比寿南1-5-5　JR恵比寿ビル8F
TEL:03-5789-2443　FAX:03-5789-2575
Email: ESECinfo@cec-ltd.co.jp

株式会社カスペルスキー

http://www.kaspersky.co.jp/

カスペルスキーとは

カスペルスキーはPCおよびネットワークを保護する世界最高レベルの情報セキュリティソリューションを提供する、国際的なソフトウェア開発企業です。
カスペルスキーは1997年創設以来、本社の所在地であるロシアをはじめ英国、フランス、ドイツ、オランダ、日本、中国、韓国、米国など29カ国の事業所で、2300人を超えるプロフェッショナルな社員が情報セキュリティ製品の開発・販売・サポートにあたっています。

■世界をリードする開発力

ユージン・カスペルスキー率いるウイルス研究所はウイルス対策分野で豊富な経験を有するスペシャリストを擁し、この分野では初めてヒューリスティックウイルス分析、言語テキスト分析の開発に成功しました。このようなイノベーションがカスペルスキー製品の基本であり、マーケットをリードする原動力です。
有力ITメディア、テスト機関から数々の賞を受けた業界最高レベルの製品は、すでに100カ国以上の国で販売され、ユーザーは全世界で3億人を超えます。

■導入実績

欧米諸国ではすでにトップシェアを誇るカスペルスキー。つねに先手必勝のウイルス対策は、世界中の多くの国でその性能が評価され、企業や国家のネットワーク保護に一役買っています。すでに日本国内においてもその堅実で強固な技術が評価され、業界のリーディングカンパニーをはじめ、官公庁、公共・教育機関まで幅広く導入されています。

代表的な製品

カスペルスキー 2012 マルチプラットフォームセキュリティ

カスペルスキー2012マルチプラットフォームセキュリティは、Windows、Mac、そしてAndroidの3つのOSに対応し、1本で3台までの機器に自由な組み合わせでインストールできる新しいタイプのセキュリティ製品です。
SNS、ネット検索、またはオンラインバンキングなどのさまざまなアクティビティが、PCで、Macで、そしてスマートフォンで、いつでも自由にできる時代です。だからこそ、あらゆる危険に対する準備が大切です。
セキュリティ製品を選ぶとき、高性能であることはもちろんのこと、所有する機器すべてを守りたいと考えるあなたのニーズに応える製品です。

Kaspersky Open Space Security（企業向け製品）

Kaspersky Open Space Securityは、企業ITインフラを世界最高レベルのアンチマルウェアプロテクションで保護する総合セキュリティソリューションです。構成するアプリケーションは完全に統合されており、すべてのプラットフォーム上でシームレスに作動します。出先や自宅などのリモート環境も含め、ネットワーク上のすべてのワークステーション、ノートブック、ファイルサーバー、スマートフォンを完全に保護し、企業のエンドポイント全体の安全を常に守ります。

Kaspersky Open Space Securityの特徴

- 強化された保護技術で、企業のエンドポイント全体のセキュリティを一元管理
- あらゆるインターネット脅威に対抗する革新的なプロテクション
- 未知のマルウェア攻撃からもシステムを迅速に保護
- シグネチャベースのプロアクティブによる保護とクラウドベースの保護技術がひとつになった、これまでにない強力なプロテクション

Best of Show Award　特別賞

Kaspersky Small Office Securityは、2010年6月9日から11日まで幕張メッセで開催されたINTEROP TOKYO 2010 “Best of Show Award”にて、プロダクトアワード部門－情報セキュリティ製品カテゴリーで特別賞を受賞しました。
また、カスペルスキーアンチウイルスは数々のアワードに輝いています。ここでは、授与されたアワードの内、権威ある賞の数々をご紹介します。

JNSA 会員企業情報

JNSA 会員企業のサービス・製品・イベント情報です。

■イベント情報■

○「スマートフォン&モバイルEXPO」に出展
～株式会社カスペルスキー

株式会社カスペルスキーは2012年10月24日（水）から幕張メッセにて開催されます「スマートフォン&モバイルEXPO」に出展いたします。Kaspersky Endpoint Security for Smartphone を中心に法人向け製品を出展いたします。
本製品をお使いいただくことで、企業が所有するスマートフォンの紛失・盗難などの被害にあった際には、リモートで端末内のデータを消去することができるほか、GPS追跡機能を使って端末の位置も特定できます。

【製品情報詳細】
http://www.kaspersky.co.jp/beready

◆お問い合わせ先◆
株式会社カスペルスキー
E-Mail: sales@kaspersky.co.jp

○日経BP社主催 「Security 2012」に出展
～タレスジャパン株式会社

タレスジャパンはSecurity 2012に参加します。
みなさまのご来場をお待ちしております。

●展示
会期：2012年10月10日（水）～12日（金）　10:00～17:30
会場：東京ビッグサイト（東4-6ホール、会議棟）
展示ブース：4-20

●講演
「貴社のデータ保護対策は万全ですか？～最新調査から読み解く暗号化導入のトレンド～」
日時：2012年10月12日（金）14:00～14:40

【イベント情報詳細】
http://expo.nikkeibp.co.jp/security/2012/index.html

◆お問い合わせ先◆
タレスジャパン株式会社　e-セキュリティ事業部
TEL: 03-6234-8180
E-Mail: jpnsales@thales-esecurity.com

■サービス情報■

○ CompTIA Cloud Essentials認定資格提供開始

CompTIA Cloud Essentials認定資格は、クラウド導入に際し、ビジネスと技術的の両方から見たメリット/デメリットを判断し運用できるスキルを証明するワールドワイドのベンダーニュートラルな認定試験です。クラウド導入の懸念事項としてあげられる「セキュリティ」の対策や対応についても出題されます。

【サービス情報詳細】

http://www.comptia.jp/cont_certif_cloudessentials_cl0-001.html

◆お問い合わせ先◆
CompTIA日本支局
TEL：03-5226-5345
E-Mail: info_jp@comptia.org

JNSA 2011年度活動報告会

JNSA の 2011 年度の活動内容を報告する 2011 年度活動報告会が、下記の要領で行われました。当日は 173 名の方にご参加いただき、盛況な開催となりました。

■ 日　時：	2012 年 6 月 8 日（金）9：55 ～ 15：40
■ 場　所：	ベルサール神田　（千代田区神田美土代町 7 住友不動産神田ビル）
■ 主　催：	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）
■ 定　員：	トラック 1 （Room2 ／定員：90 名）
	トラック 2 （Room3+4 ／定員：160 名）

発表資料は次の URL に掲載されていますので、ぜひあわせてご覧ください。

http://www.jnsa.org/seminar/2012/0608/

トラック 1

■ アイデンティティ管理 WG

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）より、「2011年度セキュリティにおけるアイデンティティ管理WG成果報告」というテーマで、発表されました。2011年度に討議された、「グローバル環境におけるアイデンティティ管理」および「企業におけるロールマネジメント」の内容が報告されました。

■ U40 部会

U40部会長前田典彦 氏（株式会社Kaspersky Labs Japan）より、U40部会の活動内容について発表されました。U40部会は、メンバーの対象を40歳未満とし、JNSAにおける若年層の活動の活性化や部会員の人脈形成・知見拡大を目的とした部会です。 部会には「ラボネットWG」と「勉強会企画検討WG」の二つのWGがあります。 ラボネットWGで昨年度から継続実施している家電検証、および実施した勉強会の内容を中心に報告を行いました。

■ 情報セキュリティ教育研究 WG

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）より、「実践的情報セキュリティ教育」－次世代教育 “Learning Explosion” の視点から－ というテーマで昨年度までの活動実績、および今後の計画・展開について発表されました。

■ 情報セキュリティチェックシート

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）より、情報セキュリティチェックシートWGの現状と課題について発表がありました。西日本支部では、中小企業向けに個人情報保護対策WG、情報セキュリティチェックシートWG、出社してから退社するまでのリスク対策WGと活動を行ってきました。情報セキュリティチェッシートWGは、出社してから退社するまでのリスク対策WGの成果をもとに、現状の情報セキュリティチェックシートの不足内容や構成、整理の仕方を検討し、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改版を行っています。今回の活動報告会で

は、ワークの進捗状況と現状の問題点が報告されました。

トラック２

■ セキュリティ市場調査 WG

セキュリティ市場調査WGメンバー菅野泰彦 氏（アルプスシステムインテグレーション株式会社）より2010～2011年度セキュリティ市場調査結果と2012年度の展望について発表されました。従来は経済産業省の委託事業という枠組みから、年度末にその年度までの推定実績と翌年度の見通しを報告書として提供していましたが、2010年度からはJNSA独自調査として調査を実施し、WGメンバーで1年間調査結果の検討と議論を重ねており、その結果の報告と2012年度の展望についての発表がありました。

■ セキュリティ被害調査 WG

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）より、2011年のインシデント発生確率の調査結果が報告されました。2010年の同調査の項目の一部を引継いた、企業における携帯電話／パソコン／USBメモリの紛失と盗難、電子メールの誤送信について、また、新たに加えられたSNSに関する調査についても報告がされました。これらに加えて、利用者の普段の行動の分析の元、インシデント発生と行動特性の関係についても解説されました。

■ 日本セキュリティオペレーション事業者協議会（ISOG-J）

ISOG-Jメンバー田島正弘 氏（NTTデータ先端技術株式会社）より、「サイバー攻撃の変遷に伴う、ISOG-Jへの期待の変化と今後」というテーマで情報共有に関連した官民連携の活動について、また、今後の ISOG-Jの向かうべき方向について報告がありました。

■ 情報セキュリティ対策マップ検討 WG BoF

標的型攻撃時代に必要な情報セキュリティ対策マップとは」というテーマでBoFが行われました。

コーディネータ：

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WGリーダー）

パネリスト：

加藤雅彦 氏（株式会社インターネットイニシアティブ）
二木真明 氏
やすだなお 氏（株式会社ディアイティ）

情報セキュリティ対策マップ検討 WG BoF

昨今、標的型攻撃には多層型防御が必要といわれており、情報セキュリティ対策の網羅的な可視化手法はますますその重要性が増すと考えられます。今求められている「情報セキュリティ対策マップ」はどのようなものか、について、ディスカッションが進められました。

■ SNS セキュリティ WG BoF

「SNSの安全な歩き方～被害状況・対策方法・ベストプラクティス～」というテーマでBoFが行われました。

パネリスト：

高橋正和 氏（日本マイクロソフト株式会社）
長谷川長一 氏（株式会社ラック）
守屋英一 氏（日本アイ・ビー・エム株式会社）
柳澤智 氏（富士通株式会社）

昨年10月の設立時から行っているSNSセキュリティの調査結果に基づいた現在のSNSにおける「実被害の状況」、利用者が「実施可能 な対策」、そして、WGメンバーのSNS利用におけるセキュリティ対策と考え方についての調査結果から、「SNS利用のベストプラクティス」が紹介されました。会場からも様々なご意見やご質問が上がり、活発な討論の場となりました。

JNSAでは、今後も各ワーキンググループの活動を中心に、様々なアプローチによる情報を発信し、情報化社会に貢献すべく努めて参ります。どうぞご期待下さい。

SNS セキュリティ WG BoF

2012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。

今年度はインターネット安全教室のホームページをリニューアルし、新たに「Web版・インターネット安全教室」を公開いたします。従来のビデオ教材に加え、講師による解説動画や、パソコン・ソフトウェアのセキュリティ設定の方法、実際の安全教室会場でよくある質問とその回答集なども紹介し、家庭や学校にいながらインターネットの安全な使い方をウェブサイト上で学習できます。

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）

［開催一覧］（次頁）一覧をご覧下さい。（2012年9月20日現在）

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、石川県、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・坂内）
E-Mail:caravan-sec@jnsa.org

2012年度「インターネット安全教室」開催一覧

（2012.9.20現在）

No.	日程	開催地	共催団体	会場
1	4月20日(金)	群馬	NPO法人おおたIT市民ネットワーク	ぐんま国際アカデミー
2	4月27日(金)	長野	NPO法人グループHIYOKO	安曇野市市民活動センター「くるりん広場」
3	5月16日(水)	岐阜	NPO法人泉京・垂井	垂井町立府中小学校
4	5月23日(水)	東京	NPO情報セキュリティフォーラム	板橋区消費生活センター
5	5月26日(土)	岐阜	岐阜市消費生活センター	岐阜市消費生活センター ハートフルスクエアーG 2階 大研修室
6	5月29日(火)	長野	上田市マルチメディア情報センター	上田染谷丘高校 そめやホール
7	5月31日(木)	京都・京田辺市（新規）	京田辺市産業振興課	京田辺市社会福祉センター 第1研修室
8	6月14日(木)	大阪	NPO法人きんきうぇぶ	河内長野市立千代田小学校
9	6月21日(木)	東京	三鷹市立井口小学校	三鷹市立井口小学校
10	6月22日(金)	群馬	NPO法人おおたIT市民ネットワーク	太田市立中央小学校
11	7月10日(火)	東京	大正大学	大正大学
12	7月11日(水)	岐阜	かにぱそこんくらぶ	みのかも文化の森 美濃加茂市民ミュージアム
13	7月15日(日)	北海道	北海道情報セキュリティ勉強会（せきゅぽろ）	北見市芸術文化ホール 5階 多目的室
14	7月18日(水)	東京	大正大学	大正大学
15	7月20日(金)	群馬	NPO法人おおたIT市民ネットワーク	太田市立城東中学校
16	7月22日(日)	秋田	NPO法人ノースウインド	ITチャオ！
17	7月24日(火)	長野	NPO法人グループHIYOKO	松本市安原地区公民館
18	7月26日(木)	秋田	NPO法人ノースウインド	ITチャオ！
19	7月28日(土)	滋賀	NPO滋賀県情報基盤協議会	滋賀県立八幡工業高等学校

20	7月30日(月)	神奈川	NPO情報セキュリティフォーラム	相鉄岩崎学園ビル 6階604室
21	8月6日(月)	三重	PCシエル	四日市市　桜地区市民センター
22	8月7日(火)	福島	特定非営利活動法人日本コンピュータ振興協会	白河市役所
23	8月7日(火)	長野	NPO法人グループHIYOKO	たつのパークセンターふれあい
24	8月16日(木) 午前	沖縄	NPO法人フロム沖縄推進機構	宮古島市 マリンターミナルビル 2F 研修室
25	8月16日(木) 午後	沖縄	NPO法人フロム沖縄推進機構	宮古島市 マリンターミナルビル 2F 研修室
26	9月4日(火)	大阪	NPO法人きんきうぇぶ	河内長野市立南花台西小学校
27	9月6日(木)	大阪	NPO法人きんきうぇぶ	河内長野市立南花台東小学校
28	9月6日(木)	大阪	NPO法人きんきうぇぶ	河内長野市立楠小学校
29	9月8日(土)	東京	中野区立新山小学校	中野区立新山小学校
30	9月14日(金)	神奈川	NPO情報セキュリティフォーラム	横浜市上白根コミュニティハウス
31	10月4日(木)	山口・岩国市（新規）	NPO法人岩国パソコンの会	岩国市中央図書館 視聴覚室
32	10月13日(土)	神奈川	NPO情報セキュリティフォーラム	小田原市生涯学習センター けやき
33	10月13日(土)	宮崎	宮崎公立大学	宮崎公立大学 交流センター 多目的ホール
34	10月20日(土) 午前	沖縄	NPO法人フロム沖縄推進機構	那覇市 沖縄産業支援センター（予定）
35	10月20日(土) 午後	沖縄	NPO法人フロム沖縄推進機構	那覇市 沖縄産業支援センター（予定）
36	10月21日(日) 午前	沖縄	NPO法人フロム沖縄推進機構	うるま市 沖縄IT津梁パーク（予定）
37	10月21日(日) 午後	沖縄	NPO法人フロム沖縄推進機構	うるま市 沖縄IT津梁パーク（予定）
38	10月27日(土) 午前	沖縄	NPO法人フロム沖縄推進機構	名護市産業支援センター（予定）
39	10月27日(土) 午後	沖縄	NPO法人フロム沖縄推進機構	名護市産業支援センター（予定）
40	10月28日(日)	神奈川	NPO情報セキュリティフォーラム	磯子区役所 いそご区民活動支援センター
41	11月17日(土)	神奈川	NPO情報セキュリティフォーラム	川崎市中原区民館 視聴覚室
42	11月19日(月)	神奈川	NPO情報セキュリティフォーラム	ヴェルク横須賀 6階 ホール
43	11月26日(月)	神奈川	NPO情報セキュリティフォーラム	磯子区根岸地区センター
44	11月30日(金)	三重	PCシエル	尾鷲市立尾鷲中学校 体育館
45	12月3日(月)	大阪	NPO法人きんきうぇぶ	河内長野市立川上小学校
46	12月4日(火)	神奈川	NPO情報セキュリティフォーラム	磯子区屏風ヶ浦地域ケアプラザ
47	12月18日(火)	神奈川	NPO情報セキュリティフォーラム	ウェルネスさがみはら 7階 視聴覚室
48	1月22日(火)	大阪	NPO法人きんきうぇぶ	河内長野市立石仏小学校
49	2月13日(水)	神奈川	NPO情報セキュリティフォーラム	葉山町福祉文化会館 大会議室

経済産業省 中小企業情報セキュリティ対策促進事業

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24年度

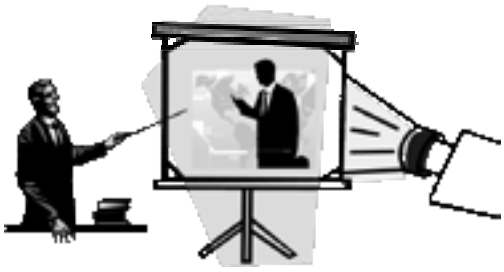
主催：経済産業省
特定非営利活動法人 日本ネットワークセキュリティ協会

ポイント その1
企業が知っておくべき最新の情報を解説

ポイント その2
PDCA を意識した実効性のある対策を演習で体感

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/

ｽｹｼﾞｭｰﾙ	午前（9:30～12:15）			～昼食（12:15～13:15）～	午後（13:15～17:00）	
項目	情報セキュリティ重要ポイント解説（60 分）	日常業務上の運用チェック基本解説（20 分）	情報セキュリティ対策の課題洗い出し（85 分）		課題の実施状況チェックと見直しの討議（90 分）	企業ごとのルール見直し演習（60 分）
内容	テキストにより、最新情報や最近の注意点など、時流に沿ったポイント解説を行う。	日常業務の中で事故発生の危険性チェックや、計画や対策の段階にさかのぼって見直しをするための PDCA を解説する。	いくつかの企業の業務風景のビデオを視聴し、PDCA を意識したリスク発見演習を行う。		ビデオに出てくる課題の原因について、チェックや見直しの観点で討議する。	企業ごとのルールを、グループ討議により見直しを行う。
備考	講義	講義	グループワーク		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、途中に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、NPO法人ITコーディネータ協会、全国中小企業団体中央会、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
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的立場にある方々（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 ※・前年度・前々年度のセミナー参加者の方にも受講をお勧めします。 ・ITコーディネータの方は本セミナーを受講されると知識ポイント（6.5 時間分）が付与されます。
参加者の特典	• 指導用ツール（講習用テキスト、指導者用マニュアル、指導用ビデオ教材、IPA 資料）を無償でお渡しします。 • 配布する指導用ツールで講習会を開催される場合、実施報告をいただくことで謝金をお支払します（2013 年 2 月末開催分まで）。 • セミナー参加者専用サイトにより、その他指導用の補足資料等を随時提供します。
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

※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 10 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①（札　幌）	札幌商工会議所	2012年10月12日（金）	北海道経済センター
	北海道②（函　館）	北海道中小企業団体中央会道南支部/函館商工会議所/北海道渡島管内商工会連合会/北海道檜山管内商工会連合会/ITCはこだて/はこだてIKA	2012年10月30日（火）	函館商工会議所
東　北	岩　手	調整中	2012年12月6日（木）	岩手県商工会連合会
	宮　城	仙台商工会議所	2012年9月18日（火）	仙台商工会議所
関　東	茨　城	水戸商工会議所/茨城県商工会連合会/茨城県商工会議所連合会/NPO法人ITコーディネータ茨城/茨城県中小企業団体中央会/公益財団法人茨城県中小企業振興公社	2012年9月26日（水）	水戸プリンスホテル
	埼　玉	NPO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/社団法人埼玉県商工会議所連合会/財団法人埼玉県産業振興公社	2012年10月18日（木）	大宮ソニックシティ
	千　葉	柏商工会議所/NPO法人ちば経営応援隊	2012年8月28日（火）	柏商工会議所
	東　京①	東京商工会議所	2012年10月29日（月）	ベルサール八重洲
	東　京②	東京商工会議所	2013年1月 22日（火）	東京商工会議所
	長　野	一般財団法人塩尻市振興公社/塩尻商工会議所	2012年11月22日（木）	塩尻インキュベーションプラザ
中　部	愛　知	名古屋商工会議所/一般社団法人中部産業連盟	2012年10月16日（火）	中産連ビル
	岐　阜	大垣商工会議所/財団法人ソフトピアジャパン	2012年11月20日（火）	ソフトピアジャパンセンタービル
	三　重	三重県商工会連合会/三重県中小企業団体中央会/NPO法人ITコーディネータ三重	2013年1月16日（水）	三重県総合文化センター
	富　山	富山商工会議所/富山県中小企業団体中央会/社団法人富山県情報産業協会/NPO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	2012年10月25日（木）	富山県総合情報センター
	石　川	金沢商工会議所/石川県商工会連合会/NPO法人石川県情報化支援協会	2012年11月9日（金）	金沢商工会議所
近　畿	京　都	京都商工会議所	2012年12月13日（木）	京都商工会議所
	大　阪	大阪商工会議所	2012年9月11日（火）	大阪商工会議所
	奈　良	奈良商工会議所/奈良県中小企業診断士会/奈良県商工会連合会	2012年11月6日（火）	奈良商工会議所
中　国	広　島	広島商工会議所/NPO法人ITコーディネータ広島	2012年9月7日（金）	広島国際会議場
四　国	愛　媛	松山商工会議所	2012年11月2日（金）	松山市男女共同参画推進センター
九　州	福　岡	福岡商工会議所	2012年9月 4日（火）	福岡商工会議所
	宮　崎	宮崎商工会議所/宮崎県ソフトウェアセンター	2012年11月28日（水）	宮崎商工会議所
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/財団法人沖縄県産業振興公社	2012年10月 2日（火）	沖縄産業支援センター

事務局お知らせ

JNSA ANNOUNCE

主催セミナーのお知らせ

● NSF2012 in Kansai

主　催：日本ネットワークセキュリティ協会西日本支部
日　時：2012年10月24日(水)
会　場：新梅田研修センター
URL：　http://www.jnsa.org/seminar/nsf/2012kansai/

後援・協賛イベントのお知らせ

1. Gartner Symposium/ITxpo 2012

主　催：ガートナー ジャパン株式会社
日　時：2012年10月3日(水)～5日(金)
会　場：ホテル グランパシフィック LE DAIBA
URL：　http://gartner-em.jp/symposium2012/

2. 電子署名・認証業務普及セミナー

主　催：一般財団法人日本情報経済社会推進協会
日時・会場：
2012年10月 5日(金)：東京(AP西新宿4階)
2012年10月26日(金)：名古屋(AP名古屋 名駅8階)
2012年11月 9日(金)：横浜(AP横浜駅西口4階)
2012年11月22日(木)：大阪(AP大阪4階)
2012年12月 7日(金)：東京(AP東京八重洲通り11階)
URL：　http://www.jipdec.or.jp/dupc/event/shomei/

3. 平成24年度　情報モラル啓発セミナー

主　催：中小企業庁、各地方経済産業局、
財団法人 ハイパーネットワーク社会研究所
日時・会場：
2012年10月：大阪
2012年11月：宮城
2012年12月：長野
2013年 2月：愛知
URL：　http://www.hyper.or.jp/moral

4. 情報セキュリティワークショップin 越後湯沢2012

主　催：情報セキュリティワークショップ in 越後湯沢
実行委員会
日　時：2012年10月12日(金)～10月13日(土)
会　場：新潟県南魚沼郡湯沢町(湯沢町公民館等)
URL：　http://www.anisec.jp/yuzawa/

5. PacSec 2012 セキュリティ カンファレンス

主　催：dragostech.com inc
日　時：2012年11月14日(水)～11月15日(木)
会　場：青山ダイアモンドホール
URL：　http://pacsec.jp/

6. Internet Week 2012

主　催：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　時：2012年11月19日(月)～22日(木)
会　場：富士ソフトアキバプラザ(東京都千代田区)
URL：　https://internetweek.jp/

7. かごしまITフェスタ2012

主　催：鹿児島ITフェスタ実行委員会
日　時：2012年11月30日(金)～12月2日(日)
会　場：鹿児島アリーナ
URL：　http://www.it-festa.jp/

JNSA 部会・WG2012 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）

外部に向けた情報発信や対外的な社会貢献活動、国際連携や他組織との連携などを推進する。

具体的には、政府関連のパブコメ対応や勉強会などの対外活動、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：平田敬 氏／株式会社ブリッジ・メタウェア）

2012年度も引き続き、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、シンポジウムの企画開催、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）

2012年度も引き続き、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」の内容検討及びセミナー講師を行う。

【在宅勤務における情報セキュリティ対策検討WG】

（リーダー：冨田高樹 氏／みずほ情報総研株式会社）

昨年度に作成した「在宅勤務における情報セキュリティ対策ガイドブック」を改訂する。改訂に際しては、昨今の社会的ニーズを踏まえ、「節電要請の可能性のある環境下での事業継続とセキュリティ対策」の視点から、活用可能なソリューションやノウハウについても追記する。

成果物「オフィスの節電と在宅勤務における事業継続・情報セキュリテイ対策ガイドブック」を7月13日に公開

【日本の政党政策評価WG】

（リーダー：米澤一樹 氏／株式会社シマンテック）

日本の各党の情報セキュリティに対する政策を、民間という立場から評価し公表することで、我が国政府に対する、JNSAの存在価値を高める。

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く。

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の安全な利用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（本調査）を実施し、報告書を作成し公開する。2011年発生確率調査の結果から本調査のテーマを選択・深堀り、および 2011年調査以外の他エリアの発生確率調査を実施する。2011年個人情報漏えい調査報告書を作成し公開する。2012年の調査に向けて、調査項目の検討、準備および調査を実施する。

＜予定成果物＞

- 「2011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）」
- 「2011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）」
- 「2011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 サマリ版 英訳）」
- 「社内教育に役立つ 個人情報漏えいインシデント調査結果（データ集2011 CD-ROM）」
- 「2011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（上半期速報）＞」

【セキュリティ市場調査WG】

（リーダー：加藤雅彦 氏／株式会社インターネットイニシアティブ）

昨年度に引き続き、従来と同様の枠組みで市場調査を行い、結果を公表する。

＜予定成果物＞

- 2012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）

IPv6対応時のセキュリティ確保のため、現状のIPv6環境に対する攻撃等を分析できる環境を構築し、基礎データを収集する。

【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のリリースを予定。WGの開催と正式版リリース後に情報交換会の開催を行う。

＜予定成果物＞

- 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）

【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）

SNSのセキュリティ、プライバシーの扱い方を、報告書としてまとめる。

＜予定成果物＞

- SNS上での情報交換、WGの開催と、報告書のとりまとめ及び報告書SNSサイトの更新等。

【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）

組織で働く人間が引き起こす事故、すなわち意図を持った「内部不正」と、意図のない「ヒューマンエラー」を対象として、これらの「内部不正・事故」の防止／抑止方法論を具体的にまとめることを目的とする。

＜予定成果物＞

- 内部不正・事故抑制に関する具体的ソリューションの提案書（ソリューションガイド）
- 内部不正・事故対応の具体事例（ベストプラクティス）集

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。

【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）

今年度よりWG名を「セキュリティにおけるアイデンティティ管理 WG」から変更。

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＞

- ロール管理ガイドライン
- クラウド環境におけるアイデンティティ管理書籍改訂版

【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）

セキュアシステム構築技術の普及・啓蒙と関連する標準化活動への関与を通しての貢献を行う。
セキュアプログラミングの原則に関するSC27WG4ほか国際標準関連活動へのコメント、OWASP等他団体との連携等。

＜予定成果物＞

未定（今年度は成果物として公開物は無く次年度の準備）

- セキュアプログラミングの原則に関するSC27WG4ほか国際標準関連活動へのコメント
- OWASP等他団体との連携　など

【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
- マップ作成ガイド（仮称）
- キーマンズネット記事

【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）

JNSAとISFとの連携、およびKISIAとの連携など、JNSAと国際連携にかかわる検討を行い、必要な共同成果物の策定に努め、JNSAの他WG活動の活性化につなげる。

2度のISO/SC27会合（5月、10月）、ISF総会などへの参加を通じて、ISFとの国際連携につき、一定の方向性を出す。連携の方向性が見出せない場合は、ISFとの関係の見直しを考える。（年度末を目処）

また、韓国KISIAとの連携についても、具体的な活動に向けた整理を実施し、連携活動を軌道に乗せる。

＜予定成果物＞

- 「クラウドセキュリティにかかわる技術ガイドライン」のドラフト

2012年5月開催のISO/SC27会合で大枠のフレームを策定し、具体的なドラフトは、10月ISO/SC27において提案する予定。

【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、活動の成果をPKI day 2012等のイベントで発表する。

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研究WG】
（リーダー：長谷川長一 氏／株式会社ラック）

今年度よりWG名を「セキュリティ講師スキル研究WG」から変更。情報セキュリティ教育に必要なインストラクションスキルの他、必要なスキル、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、ストリーミング等）の研究を行う。

＜予定成果物＞

- 情報セキュリティ教育の手引き2012年度版（仮称）

【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）

今年度よりWG名を「情報セキュリティ基本教育実証WG」から変更。

平成24年度も、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回の講義を継続実施中。また東京デザインテクノロジー専門学校においては、昨年の情報セキュリティ講義の受講対象者を広げ通期（12ヶ月）で計30回の講義を実施中。講義内容は座学講義に加えて実機利用やケーススタディなどの実践力強化講義となっている。後期は、教育部会として人材育成に関わる新たな試みとして、「情報セキュリティ教育研究WG」で研究した成果を協力してくれる学校での実証を特別講義や公開講座として実施予定。

＜予定成果物＞

- 講義資料「情報セキュリティ」の作成及びJNSA HP上での公開。
- WG実証成果についてはJNSA活動成果として学会での論文発表を予定。

【IT・セキュリティキャリア女性活躍推進WG】
（リーダー：北澤麻理子 氏／ドコモ・システムズ株式会社）

IT業界で働く女性たちの環境やキャリアプラン等の実態および意識を調査し、課題を抽出して改善方策を考察する。同時に、Face to Faceにこだわらない参加形態を模索。働き方の多様性を提言するための検証の場とする。

＜予定成果物＞

- 情報セキュリティ業界で働く女性の実態調査報告書（仮称）

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、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：大溝裕則 氏／株式会社JMC）

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。今年度は、ITリテラシー問題セットの追加を行う予定。

【JNSAソリューションガイド検討WG】
（リーダー：村上智 氏／株式会社シマンテック）

2011年度内のソリューションカイドのリリースを受け、2012年度は「JNSAソリューションカイド検討WG」から名称を変更。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及び会員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、西日本におけるネットワーク社会のセキュリティレベルの維持・向上に資すると共に、リスクの変化に応じた機動的な対応の実践を支援するため、先進性を追及、質の高いサービスを提供する事を目的として、中小企業に軸足を置いた活動を行う。

また新企画として、近畿経済産業局と情報セキュリティの現在について定例会議を開催する。

【情報セキュリティチェックシートWG】
（リーダー:鳴倉文裕 氏／富士通関西中部ネットテック株式会社）

リスクを洗い出し、評価、対策することを支援する「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」と情報セキュリティチェックシートとの対応付けを行い、現状の情報セキュリティチェックシートの不足内容や構成、整理の仕方を検討し、中小企業が実際にチェック・アクションに活用出来る情報セキュリティシートチェックシートへと改訂を行う。

また、クラウド、スマートフォンと言った新しいサービスやデバイスのセキュリティについても、情報セキュリティチェックシートへの取り込み方を検討する。

＜予定成果物＞

- 情報セキュリティチェックシート　改訂版

【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）

2011年度版「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」で対応しなかったスマートデバイス、クラウド向けに、中小企業におけるセキュリティ対策を検討する。

＜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）

西日本企業のセキュリティ啓発を目的として、セミナーおよび勉強会を実施していく。

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にとどまらず、グループディスカッションやハンズオンも取り入れ活発な意見交換を行う。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／株式会社ラック）

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・検査のためのガイドライン」（検討中）
- 「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：調整中）

新たにサービス利用者向けのガイドラインを作成に向けて、フィージビリティスタディを行うことで活動を進める。

【セキュリティオペレーション技術WG】
（リーダー：川口洋 氏／株式会社ラック）

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）

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。

【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：多田昭仁 氏／株式会社日立情報システムズ）

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を予定。

JNSA 役員一覧　2012 年 8 月現在

会　長	田中　英彦	情報セキュリティ大学院大学 研究科長 教授
副会長	髙橋　正和	日本マイクロソフト株式会社
副会長	中尾　康二	ＫＤＤＩ株式会社
副会長	大和　敏彦	ＺＴＥジャパン株式会社

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株式会社
兜森　清忠	マカフィー株式会社
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
村上　智	株式会社シマンテック
山田　秀樹	EMCジャパン株式会社
吉原　勉	株式会社インターネットイニシアティブ

幹　事（50音順）

安達　智雄	日本電気株式会社
大島　耕二	株式会社ネットマークス
大溝　裕則	株式会社ＪＭＣ
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
北折　昌司	東芝ソリューション株式会社
北澤　麻理子	ドコモ・システムズ株式会社
郷間　佳市郎	株式会社日立システムズ
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
髙橋　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
森　直彦	エヌ・ティ・ティ・アドバンステクノロジ株式会社
半田　富己男	大日本印刷株式会社
樋口　健	株式会社インフォセック
平田　敬	株式会社ブリッジ・メタウェア
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
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	株式会社ラック
米澤　一樹	株式会社シマンテック
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	慶応義塾大学　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

会員企業一覧　(2012年9月1日現在　145社　50音順)

【あ】

(株)アーク情報システム
(株)アークン
(株)アイ・ティ・フロンティア
(株)アイテクノ
アイネット・システムズ(株)
アイマトリックス(株)
アルテア・セキュリティ・コンサルティング New
(株)アルテミス
アルプスシステムインテグレーション(株)
イーデザイン損害保険(株)
EMCジャパン(株)
株式会社イーセクター New
伊藤忠テクノソリューションズ(株)
イルポンテ(株)
学校法人 岩崎学園
(株)インターネットイニシアティブ
(株)インテック
(株)インテリジェントウェイブ
インフォサイエンス株式会社 New
(株)インフォセック
ウェブルート株式会社 New
(株)AIR
エクスジェン・ネットワークス株式会社 New
SCSK(株)
(株)エス・シー・ラボ
NRIセキュアテクノロジーズ(株)
NECネクサソリューションズ(株)
NHN　Japan(株)
NKSJリスクマネジメント(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コムテクノロジー(株)
(株)NTTデータ
(株)NTTデータCCS
NTTデータ先端技術(株)
F5ネットワークスジャパン(株)
オー・エイ・エス(株)
(株)OSK
(株)大塚商会

【か】

(株)Kaspersky Labs Japan
キヤノンITソリューションズ(株)
九電ビジネスソリューションズ(株)
京セラコミュニケーションシステム(株)
クオリティソフト(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)
(株)コンシスト
CompTIA　日本支局

【さ】

(株)サイバーエージェント New
サイバーソリューション(株)
(株)シー・エス・イー
CA Technologies
(株)JMC
ジェイズ・コミュニケーション(株)
JPCERTコーディネーションセンター
(株)シグマクシス
シスコシステムズ合同会社
システム・エンジニアリング・ハウス(株)
(株)シマンテック
(株)情報経済研究所
新日鉄ソリューションズ(株)
新日本有限責任監査法人
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)
ZTEジャパン(株)
ソニー(株)
ソフォス(株)
ソフトバンク・テクノロジー(株)
(株)ソリトンシステムズ

【た】

大興電子通信(株)
大日本印刷(株)
(株)大和総研ビジネス・イノベーション
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)
(株)電通国際情報サービス
東京エレクトロン デバイス(株)
東芝ソリューション(株)
ドコモ・システムズ(株)
株式会社豊通エレクトロニクス New
トレンドマイクロ(株)

【な】

西日本電信電話(株)
日信電子サービス(株)
日本アイ・ビー・エム(株)
日本アイ・ビー・エム　システムエンジニアリング(株)
日本オラクル(株)
日本サード・パーティ(株)
日本セーフネット(株)
日本電気(株)
日本電信電話(株)
日本ビジネスシステムズ(株)
日本ベリサイン(株)
日本マイクロソフト(株)
(株)ネクストジェン
(株)ネットマークス
ネットワンシステムズ(株)

【は】

パスロジ(株)
パナソニック(株)
(株)日立システムズ
(株)日立ソリューションズ
(株)PFU
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)富士通マーケティング
フューチャーアーキテクト(株)
(株)ブリッジ・メタウェア
(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)
(株)三菱総合研究所
三菱総研DCS(株)
三菱電機(株)情報技術総合研究所
三菱電機情報ネットワーク(株)
(株)メトロ

【や】

(株)ユービーセキュア

【ら】

(株)楽堂
(株)ラック
リコージャパン(株)
(有)ロボック

【わ】

(株)ワイ・イー・シー
(株)ワイズ

【特別会員】

(ISC) 2　Japan
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
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
社団法人　日本インターネットプロバイダー協会
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　日本電子認証協議会

JNSA 年間活動（2012 年度）

4 月	4 月 21 日、26 日	「Hardening Zero・Softening Zero」後援
	4 月 27 日	第 1 回幹事会
5 月	5 月 11 日	2012 年度理事会
	5 月 19 日～ 20 日	SECCON つくば大会（関東地区）
	5 月 23 日～ 25 日	「自治体総合フェア 2012」協賛
	5 月 24 日～ 26 日	「第 16 回サイバー犯罪に関する白浜シンポジウム」後援
	5 月 25 日～ 26 日	「学びのイノベーション＆セキュリティフェア 2012」
	5 月 30 日～ 6 月 1 日	「ワイヤレスジャパン 2012」「スマートフォン / ケータイショップ EXPO」 「M2M クラウド EXPO」後援
	5 月 31 日	ISOG-J 主催セミナー「セキュリティ関連法律を学ぼう！！～ 改正不正アクセス禁止法と 改正刑法（通称：ウイルス作成罪）について ～」
6 月	6 月 8 日	2011 年度 WG 活動報告会（ベルサール神田）
	6 月 8 日	2012 年度総会（ベルサール神田）
	6 月 12 日～ 15 日	「Interop Tokyo 2012」後援
	6 月 27 日	第 2 回幹事会
	6 月 29 日	第 10 回 関西情報セキュリティ団体合同セミナー
7 月	7 月 2 日～ 3 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 2012」後援
	7 月 3 日	第 2 回 鍵管理勉強会
	7 月 17 日～ 18 日	「SecureAsia@Tokyo2012 カンファレンス」後援
	7 月 25 日	節電環境における情報セキュリティ対策セミナー（大阪）
	7 月 27 日	JNSA WG 合同セミナー「セキュリティ事故の傾向とソーシャルメディアの安全な使い方 ～最新の情報セキュリティ事情～」
8 月	8 月 8 日 他	「平成 24 年度情報モラル啓発セミナー」後援
		8/8 熊本、8/30 広島　他
	8 月 24 日	第 3 回幹事会
9 月	9 月 12 日	「平成 24 年度情報モラル啓発セミナー（香川）」後援
	9 月 19 日、21 日	「ID & IT Management Conference 2012」協賛
		9/19 大阪、9/21 東京　他
10 月	10 月 3 日～ 5 日	「Gartner Symposium/ITxpo 2012」後援
	10 月 5 日　他	「電子署名・認証業務普及セミナー」後援
		10/5 東京、10/26 名古屋　他
	10 月 12 日～ 13 日	「情報セキュリティワークショップ in 越後湯沢 2012」協力
	10 月 24 日	「NSF2012 in Kansai」JNSA 西日本支部主催セキュリティセミナー（新梅田研修センター）
11 月	11 月 9 日　他	「電子署名・認証業務普及セミナー」後援
		10/9 横浜、11/22 大阪　他
	11 月 14 日～ 15 日	「PacSec 2012 セキュリティ カンファレンス」後援
	11 月 15 日	「2012 日韓情報セキュリティシンポジウム」（韓国ソウル）
	11 月 19 日～ 22 日	「Internet Week 2012」後援
	11 月 30 日～ 12 月 2 日	「かごしま IT フェスタ 2012」後援
12 月	12 月 7 日	「電子署名・認証業務普及セミナー（東京）」後援
1 月		
2 月		
3 月		

2012 年 4 月～
2013 年 3 月
「インターネット
安全教室」開催

2012 年 8 月～
2013 年 2 月
「平成 24 年度
中小企業向け
指導者育成
セミナー」開催

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。）

三井物産セキュアディレクション株式会社　佐山　享史

JNSA会員の皆様、はじめまして。この度日本電気株式会社(NEC)の佐藤さんよりご紹介頂き、本コーナーを担当させて頂くことになりました三井物産セキュアディレクション株式会社(MBSD)の佐山と申します。

私は現在、テクニカルコンサルタントという肩書で、企業のITセキュリティ全般の改善を図るコンサルティング業務を行っております。「ITセキュリティ全般」と書いております通り、技術的な内容だけでなく、規程やルールの作成、教育や啓蒙など情報管理に関連する内容まで実施しています。セキュリティに関してお困りのことがありましたら、お気軽にご相談頂ければ幸いです。

私がセキュリティに携わるようになったのは10年ほど前、まだセキュリティ機器といえばファイアウォールという時代にIDS(不正検知システム)を使った不正アクセス監視サービスを立ち上げたプロジェクト(当時は三井物産の中のプロジェクトでした)に誘いを受けてからでした。24時間365日、来る日も来る日もセキュリティアラートを分析する仕事は思った以上に過酷で、救急車を呼び即入院となる、20代で痛風になる等、物理ウイルスに弱い体になっていきました(笑)。
コンサルティング事業部への異動を契機に、お客様先に常駐してセキュリティ対策を推進する業務を行った後、現在は監視経験を基に主に運用、技術の両面から企業のセキュリティリスクを削減するセキュリティ専門のコンサルタントをしております。

JNSAの中では、主にISOG-J WG2に参加させて頂いております。WG2では技術的な話題を中心にお話をしているのですが、同業他社の技術者の方々と直接会話できることは貴重で非常に良い刺激となっています。今後も積極的に参加して、JNSA会員企業の皆様はもちろん、セキュリティ業界全体に貢献できればと考えておりますので、引き続きよろしくお願い致します。

では、最後に仕事以外の話を簡単にさせて頂きます。私は小学校から野球を始め、その後もテニス、サッカー、ラグビーとずっと体育会系でした。社会人になってからもジムで継続的にトレーニングを行う日々を送っていたのですが、2年ほど前に「今までやってこなかったことにチャレンジしよう」と一念発起し、ピアノを始めました。現在も毎週ピアノ教室に通い、第二の人生を送っております。何かの機会に私の演奏を見かけることがありましたら、どうぞ温かい目で大きな拍手をお願い致します。

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

三菱電機情報ネットワーク株式会社　田中　朗

JNSA会員の皆様、はじめまして。三菱電機情報ネットワーク株式会社（MIND）の田中と申します。今回、日本電信電話株式会社（NTT）の南端さんから紹介を受け、本コーナーの執筆を担当することになりました。

現在私はMINDで２４時間３６５日のセキュリティ監視運用サービスを提供する仕事をしています。製品やシステムと違い、目に見えない運用サービスのしかもセキュリティという普通の人には少し難しめのものを、お客様に理解いただくのに日々苦労しています。セキュリティはいまや必要ということは認識されるようになりましたが、本当はお客様の事業に如何に役に立つかを説明し、納得して頂くが鍵であると信じています。

自己紹介になりますが私は昔から麻雀、トランプに始まりゲーム、パズルの類は何でも好きです。皆さんも少なからず楽しんでいるTVゲームは黎明期からの付き合いになっています。そんな中もう25年ほど楽しんでいる、数独で有名になったペンシルパズルのお話を少しさせていただきます。ペンシルパズルは自分でも手軽に作って楽しむ事ができるパズルです。パズル仲間から解く要領で同じように作る事ができることを教わって以来、自分でもいくつか作成して雑誌に投稿しています。自分で作成してわかったのは、パズルは作り手が意図を持って作られていることです。パズルを解くことは作者とのある種の戦いでもあります。解き方の迷路の中一つ一つ論理を積み重ね正解にたどり着くわけですが、途中作者の罠にはまり勘違いすると解けずにハタンすることもままあります。

セキュリティの仕事をしていると、時にこのパズルを解くのと同じ状況になっていると思えることがあります。ログを追いかけ一つ一つの事実を積み重ねて、何が起きているかを突き止め、時には攻撃者の意図を推測して、いかにしてシステムを守るかといったことを導きだすロジックはパズルを解くのとそっくりではないでしょうか。

こんな私はJNSAではセキュリティサービス事業者の協議会であるISOG-Jにて、最近のサイバー攻撃に対する対策検討に、自身の経験や現在の業務を通じて少しでも役立てればと参加しております。昨今の攻撃は複雑化、先鋭化しているためこれまでのように一組織だけで立ち向かうには限界があり、JNSAやISOG-Jさらには各種団体を通じた知識の共有を進め、連携を強めていくことが必要と感じています。JNSAの活動を通じて、皆さんが安心して利用できるインターネット、IT環境になることを目指して微力ながら一歩ずつ進んでいきたいと思っています。

事務局お知らせ
JNSA ANNOUNCE

JNSA について

■会員の特典

1. 各種部会、ワーキンググループ・勉強会への参加
2. セキュリティセミナーへの会員料金での参加および主催カンファレンスへの招待
3. 発行書籍・冊子の配布
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
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.34

2012 年 9 月発行

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

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