JNSA PRESS
JAPAN NETWORK SECURITY ASSOCIATION
SPRING 2012 VOL. 33

寄稿

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

サイバー攻撃の脅威とセキュリティ対策

CONTENTS

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

情報セキュリティに係る経済産業省の取組

経済産業省商務情報政策局
情報セキュリティ政策室長
江口　純一

日本の産業界の競争力の強化を考える時、現在、将来を問わずITなくしては語れない時代になったことは既にご承知のことと思います。しかし、インターネットの普及により世の中の様々な分野で「便利」になる一方、「危険」も常に伴います。

昨今のサイバー攻撃を見ると、従来の能力誇示目的で不特定多数に攻撃するものから、特定の組織を標的にし、主として知的財産等の機密情報の窃取を目的とした「標的型サイバー攻撃」へと変化しています。

特に、国や政府機関、企業に対する攻撃が増え、その手法も複雑化、大規模化していることが大きな特徴です。

こうした現状を考えると、ITの世界での「安全・安心」な国民生活及び企業活動を確保するためには、情報セキュリティが必要不可欠になっていると言えます。

経済産業省では、一昨年12月より今後取り組むべき対策を議論してまいりました「サイバーセキュリティと経済 研究会」（委員長:村井純慶応義塾大学教授）の中間とりまとめを昨年8月に公表しました。本報告書を踏まえて現在進めている取組をご紹介させていただきます。

1つ目は、「標的型サイバー攻撃への対応」です。前述のように、従来のサイバー攻撃は、不特定多数のユーザに不正プログラムを大量配布する方法が多かったものの、近年は、特定の組織・個人を確実に感染させることが目的の標的型サイバー攻撃が多く、わが国では2007年から2011年の4年間で6倍に増えています。そこで、個々のユーザが標的型サイバー攻撃を受けた際に、同様の攻撃による被害の拡大の防止及び未然防止のため、昨年10月に、重工、重電等、重要インフラ等で利用される機器の製造業者を中心に情報共有の場を構築する目的から、「J―CSIP」（ジェイシップ＝サイバー情報共有イニシアティブ）を立ち上げました。

今後は、情報共有ルール等の整備を行い、順次参加企業の拡大を図るとともに、IPA（情報処理推進機構）をハブとした官民連携の情報共有を実施していきます。

2つ目は、「制御システムの安全性確保」です。ここ数年、発電プラントなどの重要インフラ等を支える制御システムは、外部ネットワークとの接続や制御システムに使用されるOSの共通化が進行しており、サイバー攻撃の脅威が現実化しています。

電力やガス、水道といった国民生活及び企業活動を支える重要インフラ施設がサイバー攻撃を受けた場合、社会的影響は図り知れません。

そこで、昨年10月には、こうした重要インフラ等の制御システムのセキュリティ強化を

図るため、「制御システムセキュリティ検討タスクフォース」を立ち上げました。今後は、タスクフォースでの議論を踏まえ、セキュリティ検証施設の構築、評価・認証スキームの構築等を日米協力のもと進めることで、重要インフラ等におけるセキュリティ強化を図ってまいります。

また、一般ユーザや企業の方々自身の情報セキュリティに対する意識向上も欠かせません。当省では「インターネット安全教室」や「中小企業向け指導者育成セミナー」を通じた普及・啓発活動を実施してまいりました。一般ユーザを対象とした「インターネット安全教室」は、2011年度で9年目を迎え、2010年度までに5万人以上の方々に受講いただきました。また、「中小企業向け指導者育成セミナー」では、大企業と比べ情報セキュリティ対策が遅れがちである中小企業の指導的立場にある方（ITコーディネータ、中小企業診断士等）に対し、全国27箇所（2011年度）でセミナーを行いました。

こうして情報セキュリティに対する意識が一般ユーザや中小企業の方々に徐々に浸透しつつあるのも、JNSA及び全国の共催団体の皆様の多大な御協力の賜物であると考えております。この場をお借りして感謝申し上げます。

また、JNSAにはICT教育推進協議会との連携により、実践教育を通じた人材育成を御検討いただいておりますが、当省としても今後の議論を注視するとともに成果に期待したいと思います。

我が国全体としての情報セキュリティレベルの向上を図ることが当省の重要なミッションだと考えておりますので、引き続き、政府の取組に御協力賜れれば幸いです。

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

セコム株式会社 IS 研究所
甘利　康文、新井　真司、内田　順一

要　旨

組織運営にインパクトを与える内部要因事故は、社会における情報化の進展によって、かつてより大規模にかつ頻繁に発生するようになっている。また、個人情報保護や組織の内部統制の意識の高まりから、より問題視されるようになり、メディア等で取り上げられる機会が増えている。内部情報流出に代表される、組織で発生する事故は、情報システムや組織への物理的侵入などの外部からの脅威によるものよりも、組織で働く従業員の不正やヒューマンエラーなど組織内部にその原因が存在するものの方がはるかに多いと言われている。

一方、内部不正やヒューマンエラーなどの組織における内部要因事故は、発生してもその損失が多額になったり人命に関わったりしない場合には、発生した組織の内部で処理されることが多く、その実態や原因が明確な形で公開されることは極めて少ない。そのため、内部要因事故を防ぐ手法が、本質的観点から系統的に検討されることはまれで、その対策も、情報漏洩防止のための IT ソリューションを導入したり、カメラや出入管理システムを設置したりなどの対症療法に偏りがちであった。

我々は、この現状に対し、犯罪学で培われた種々の犯罪予防論をベースに、内部要因事故の本質的な発生要因を考察するとともに、その抑制・防止方法を考案した。

本稿は、この考察結果を、先に公表したセキュリティの基本的考え方 [1, 2] を基礎として整理[1] し、解説及び提言を試みたものである。提言に際しては、犯罪学の基本的考え方に、セキュリティを守るサービスを多くの組織に対して提供してきた実務家としての知見も加味し、具体的で実用性の高いものとすることを意識した。本稿で提案する方法論を適用することによって、多くの組織において、そこで働く従業員が引き起こす内部要因事故に対する具体的対策の方向性が明らかになるものと考える。

キーワード

犯罪予防論、内部不正、ヒューマンエラー、セキュリティ、組織論、内部統制

1. はじめに

組織における損失は、外部からの脅威によるものよりも、従業員の内部不正・ヒューマンエラーなどの内からの要因で発生しているものの方が多いという報告がなされている [5, 6]。

この内部要因事故による損失は、組織の内部で処理されることが多いため、その実態は公になりにくい。しかし、その発生頻度は高く、財務的にも組織運営を圧迫する要因の一つとなっているものと考えられる。そのため、内部要因事故の損失を効果的に削減することが出来れば、組織運営上大きな効果が期待出来る。

これまでも、組織における内部要因事故に関しては、様々なセキュリティ対策が考えられてはきたが、セキュリティ対策が正常に機能している場

[1] 2009 年 12 月 18 日 日本セキュリティ・マネジメント学会（JSSM）「個人情報の保護研究会」「先端技術・情報犯罪とセキュリティ研究会」合同研究会、及び 2010 年 6 月 26 日 JSSM 第 24 回全国大会にて、本稿で説明する方法論検討の途中経過概要を報告 [3] した他、2011 年 8 月 5 ～ 9 日 国際犯罪学会第 16 回世界大会では、本稿で説明する方法論そのものの概要を発表 [4] した。

合には損失が発生しない、その必要性を認識していてもその対策レベルの目安がない、対策に真摯に取り組んでもステークホルダーから評価を得られにくい等の理由により、多くの場合、カメラや出入管理システムを設置したり、情報漏洩防止のためのソリューションを導入したりなどの対症療法的対策に留まっている。

本稿[2]では、組織の内部要因から発生する損失へのセキュリティ対策として、「組織のあり方」という観点に着目して、これまで長年に渡って様々な組織のセキュリティを見てきた実務家の立場から考察を加え、従業員が引き起こす事故を抑止するフレームワークについて論ずる。加えて、この考え方に基づいて検討した具体的対策手法について提案する。

2. セキュリティの定義と対象

本来の「セキュリティ」は、情報セキュリティや犯罪対策を超える広い概念を包含する。本稿では、我々が、先に提案したセキュリティの定義 [1, 2] をベースにして論を進める。

本来のセキュリティとは、「オペレーション（日々の営み）が、運営主体によってあらかじめ定められたプランに則って運営され、理由の如何によらず、それが阻害されないこと」であり、セキュリティ対策によって、そもそもの守るべき対象は「組織のオペレーション」である。犯罪被害や情報漏洩など、組織のオペレーションを阻害する要因をインシデント（事故）と呼ぶ。

一般に、セキュリティを考える際には、人・物・金、そして情報をインシデントから守る必要があると言われる [7]。これらは、組織を構成する要素であり、組織を運営するために必要なもの（リソースプロパティ、以下「プロパティ」と表記）でもある。プロパティが守られないと、その組織のオペレーションは、あらかじめ定めたプラン通り回らなくなる。それゆえ、「組織のオペレーションが回り続ける状態」を実現するためには、これらのプロパティを守る必要が生じる。これは、本質的観点からセキュリティを捉える上で重要な考え方である。セキュリティをこのように捉えると、防犯対策から、情報セキュリティ、そして本稿の対象である内部不正やヒューマンエラーによるミスなどの組織の内部要因事故への対策までを、「セキュリティ対策」として一元的に考えることができるようになる。

3.「組織のオペレーション」を守る

組織のセキュリティを考える場合、人・物・金、そして情報などのプロパティを守ることに目が向いてしまいがちになる。しかし、前述のとおり、本来のセキュリティ対策において守るべき対象は、いかなる場合においても「その組織のオペレーション」である。

人は、組織のオペレーションを担っている際に、正常な判断が働かず不正をしてしまうことがある。一般には、これを「魔がさす」と表現する。また、ヒューマンエラーにより悪意無くミスをしてしまうことも少なくない [8]。この「魔がさす」「ミスをする」のは、組織で働く人が根源となる脅威である。この脅威に対応するためには「そこで働く人に『魔がささない』『ミスが出ない』組織環境」が必要となる。

また、内部不正対策を考える場合には、事故発生時に組織のオペレーションへの影響を小さくし、事業をいかに早く通常通り復旧させるかの視点（BCP、BCM）が重要である。さらに、組織のオペレーションを守るという観点からは、「その対策がオペレーションを逆に阻害しないか」を常に意識する必要がある。

[2] 本稿の内容は、あくまでも筆者らの研究者の立場からの私見であり、必ずしも筆者らが所属する組織の見解と一致するものではない。

事業所におけるヒューマンエラーの抑制は安全工学の重要な一分野であり、多くの研究者や実務家によって、具体的対応方法が検討、確立されてきた。しかしながら安全工学で扱う対象は、工場や交通機関などの事業所で、大きな物理的エネルギーを伴う作業が多いという傾向があった。大きなエネルギーを伴う作業では、ひとたび事故が発生すると、その被害が広範囲に及んだり、人命に関わったりすることが多く、社会や組織のオペレーションに大きな影響を及ぼす。ヒューマンエラーの重要な研究対象として、大きなエネルギーを伴う作業が位置づけられた主な理由はここにあるものと考えられる。

一方、社会における情報化の進展により、組織のオペレーションに影響を及ぼす業務は、大きなエネルギーを伴うものに限らなくなってきている。一般的オフィスで起こる、ヒューマンエラーによる単純ミスが瞬時に広範囲に波及し、社会や組織のオペレーションに大きな影響を与えるケース[3]も少なくない。「組織のオペレーションを守る」という観点に立つと、人が引き起こす単純なミスも抑えるべき重要な対象となる。

また、事務のミスは「内部不正の言い訳」となることもある [9]。この観点からも、ミスが発生しない、もしくはミスが発生しても早期にそれが是正できる職場をつくることが重要となる。従業員がミスをしてしまう環境は、従業員にとって内部不正が出来る環境でもあることに留意する必要がある。

4.「働く人」を守る

どのような組織であれ、そのオペレーションを担っているのは人である。人抜きではどのような組織も動かない。人は組織を構成する最重要プロパティである。

一方で、人は、その立場に関わらず、魔がさして不正をしたり、ヒューマンエラーによるミスを犯したりすることがある。特に、組織の経営に携わる人間が行う不正やミスは、一組織のオペレーションに留まらず、社会全体に大きな影響を及ぼすことも少なくない。

「魔がさす」ことは、組織で働く人間に対する脅威であり、組織や社会における地位によらず誰にでも起こりうる。イスラム教では、その人間観の根底に「人の本性は弱いものである」という性弱説[4]の考え方が流れている [10]。この考え方は、古くイスラム教の成立と時を同じくして、提唱されたものであるが、孟子や荀子が唱えた性善説・性悪説と並立する概念として注目に値する。

組織のオペレーションを守るためには、職位や職責に関係なく、人間の持つ「弱い」という本性を考慮し [11]、そこで働く人を保護し、人に内在するノウハウやスキルを守る対策が必要となる。

5. 防犯手法の２つの方向性

犯罪は「犯罪企図者」が「犯罪の機会」に遭遇することで成り立つ。この成立要件を満たさなければ、原理的に犯罪は起こりえない。この成立要件を崩す手法として「犯罪機会論」「犯罪原因論」という２つの考え方に基づく防犯方法論がある[5]。「犯罪者に犯罪の機会を与えないことによって、犯罪を未然に防止しよう」という取り組みが犯罪機会論による防犯、「犯罪者が犯罪者たるに至った社会原因を究明し、それを除去することによって犯罪を防止しよう」という取り組みが犯罪原因論による防犯である。

[3] 2005 年に発生した「61 万円 1 株」を「1 円 61 万株」と取り違えた株式誤発注事件などが有名である。

[4] イスラム世界では、弱い存在の人間が誘惑に負けないように支援する目的で、多くのしきたりや習慣がある。女性のベール着用、飲酒禁止などはその一例である。

[5] 犯罪学では、防犯の方法論は原因論から機会論に移り、やがて双方を融合する形に変遷して来ている。

前者の犯罪機会論に立脚した防犯理論の一つに、「状況的犯罪予防論（Situational Crime Prevention）」がある [12]。「犯罪が発生する場所の環境」を犯罪発生の主要因と捉えて、その環境要因を除去することで、即効性のある防犯対策を行おうというものである。この手法を、実世界のみならず情報セキュリティ分野に適用しようとする検討もなされている [13]。

後者の犯罪原因論に立脚した防犯理論は、犯罪者の特性や更生を考え予防していく考え方である。一般に社会全体を対象とした場合、ある人物を犯罪企図者にしてしまう要因を特定することは難しく、さらにその除去には様々な制約があることが多い。一方、組織を対象とし、不正などの内部要因事故の抑止を考える場合、犯罪企図者を生み出す組織要因を特定することは十分に可能である。そして、その組織要因を除去し、組織の文化を変えていくことで、犯罪原因に着目した犯罪予防への道が拓ける。

本稿では犯罪機会論、犯罪原因論の考え方を融合させ、「状況的犯罪予防論」、「組織論」の二つの観点から、組織に対する防犯理論の適用を考える。加えて、「組織のオペレーションを守る」サービスを提供する実務家の視点も加味し、そのノウハウを反映することで、実際の組織において適用可能な具体的対策フレームワークの提言を試みる。

6. 内部不正抑制に応用可能な各種犯罪理論

ここでは、本稿で提言する組織における内部要因事故抑制手法の基盤とした各種犯罪理論について概観する。

6.1.「不正のトライアングル」理論

内部不正に関して着目すべき理論の一つに、20世紀半ばに Cressey が提案した「不正のトライアングル理論（Fraud Triangle Theory）」[14] がある。この考え方を内部不正抑制のアプローチとして適用すると、職場としての組織から、

- 犯行に至る動機／プレッシャー
- 犯行を行いやすい機会
- 犯行を自己正当化する事由

の3つの要因を取り除く対策となる。

6.2 日常活動理論

Cohen と Felson によって提唱された「日常活動理論（Routine Activity Theory）」[15] は、

- 犯罪企図者
- 犯罪のターゲット
- 監視者の不在

という条件が重なったときに犯罪が成立するという理論である。彼らは、犯行機会を減少させるためにライフスタイルを変えることを提唱しており、この理論は、犯罪機会論の一種とも考えることができる。

一般に、日常活動理論において防犯を実現するためには、常駐警備員や民間ボランティア等を配置したり、監視カメラを設置したりすることによって、最後の「監視者」の要件に関与する。

本理論は、日本においても子どもの防犯施策への適用が検討されている [16] が、内部要因事故への適用も十分可能である。

6.3 合理的選択理論と性弱説

人の振る舞いを考察するうえで、基盤となる前提の一つに、「人間は自己利益の最大化を目指して合理的な判断と行動を行う」という「合理的選択理論」と呼ばれる考え方がある。犯罪学の多くもこの考え方に立脚し、通常の場合、人は合理的判断を行って、自らを不利な状況に追いやる犯罪に至ることは無いとしている。しかしながら、人は「置かれた（社会的、物理的）環境や状況」によって、弱くなることがあり、「目先の利」などの誘惑に負けて魔がさし、犯罪者となることがある。この人間の本性を表す言葉が「性弱説」である [17]。

6.4 割れ窓理論

犯罪予防の基本的考え方に Kelling が提唱した「割れ窓理論（Broken Windows Theory）」[18] がある。小さな乱れを放置しておくと、大きな犯罪を呼び起こしてしまうという考え方である。

小さな不正を見逃さない風土を作ることによって、環境全体が徐々に浄化されていくというこの考え方は、ニューヨーク市を始め、多くの地域で効果をあげている犯罪予防論として有名である。

6.5 組織内犯罪への防犯手法の適用

内部不正等の内部要因事故発生の抑制を考えた場合、環境に働きかけて、それを引き起こすことが、誰が考えても（合理的に）割に合わないという状況を作り出すという方向性の対策が考えられる。これが「犯罪機会論による内部不正抑制」の考え方である。

これに対して、所属する組織文化の醸成によって、本来善良であるにも関わらず性弱という本性を持つ人間に働きかけて、「誘惑に負けて犯罪者にならないようにしよう」、「犯罪企図を持たせないようにしよう」とする方向性の対策、すなわち「組織文化の醸成による内部不正抑制」が考えられる。いわば犯罪原因論の組織への適用である。組織などの閉じた社会では、社会一般を対象とする場合と異なり、人に着目した犯罪原因論も分析や具体的対策を行いやすく、十分に検討の対象となる。

7. 状況的犯罪予防論による内部不正抑制

本稿では、まず 2003 年に Cornish と Clarke によって提案された状況的犯罪予防論 [19] のフレームワークに沿って、組織内部で発生する内部不正への適用を試みた手法を提案する。

内部不正を考える場合、犯罪機会に遭遇した人間に「魔がさす」ことで、初めてその人間が犯罪企図を持つことになる。社会一般における状況的犯罪予防論では、犯罪企図者の存在を前提としているが、組織内部における状況的犯罪予防論においては、「状況が、弱い人間を犯罪企図者にしてしまう」側面も重視している。

我々は、この状況的犯罪予防論をベースとし、「予防策の増強（物理的に不正がしにくい状況）」、「発覚リスクの増強（不正が見つかる状況）」、「利得の抑制（不正が割に合わない状況）」「誘因の排除（その気にさせない状況）」、「弁解余地の排除（言い訳を許さない状況）」の構築を目指す５つの観点から、内部不正を抑制するための方策を整理した。そして、各々について、セキュリティサービス業務の実務的知見、及び、犯罪学で培われた方法論（「不正のトライアングル理論」「日常活動理論」「合理的選択理論と性弱説」等）をベースとして考察し、それぞれの項目についての５つの具体的抑制手法を考案した。表１はそのフレームワークを示したものである[6]。

以下、各項目について説明する。

7.1 予防策の強化

物理的に内部不正を働きにくい状況を作ることである。

7.1.1 対象物の強化

バリア強化等の手段により、内部犯行からターゲット自体を守る方策が「対象物の強化」である。ここで言うターゲットとは、現金、在庫、備品、OA 機器、情報等の、組織運営に必要なもの、すなわちプロパティのことである。組織のオペレーションを守るという観点から、契約情報、個人情報等、失ったり漏洩したりすることで組織の信頼を損なう情報プロパティの重要性が高まっている。

[6] 本表各主項目は、社会一般を対象とした先行研究 [19] をベースとしているが、組織における内部不正対策に合うように、原表 [19,20] の主意を尊重しつつ邦訳している。

「収納、施錠の徹底」「保管庫・金庫の導入」「情報アクセス制限の設定」「情報アクセスの際の認証の設定」などで実現する。「対象物の強化」は、「守りの基本」であり、ほかの方策に先んじて実現すべきものである。

7.1.2 入口でのコントロール

内部犯行ターゲットへのアクセス性をコントロールすることである。物や情報などの対象へのアクセス可否を左右する「資格と必要性」の要件は、対象ごとに決めておく必要がある。ある人物が、たとえアクセスの「資格」を有している場合でも、状況からその「必要性」がない場合には、入口での規制が必要である。例えば、その組織の一員であり入室資格を有している場合でも、通常は、深夜や休日の入室は必要がないことが多く、何らかの確認が必要となることなどがあげられる。この要件を、十分に吟味して定めることが、「入口でのコントロール」による内部要因事故防止の成否を決めることになる。

情報アクセスの場合にも、アクセス行為の「資格と必要性」を考慮したコントロールをすることが重要である。

アクセスログを記録することは、後日、調査の可能性を残しておくということで、内部不正予防の意味がある。

7.1.3 出口での検査

組織からの物品や情報の不正持出しを、出口でチェックする仕組みを構築することである。
万引き防止ワイヤレスタグ等による物品持出しの検査を行ったり、組織内部ネットワークと外部のネットワークの間をつなぐゲートウェイで、組織から外に出て行く情報に注意したりすることがこ

表１　状況的犯罪予防論をベースとした内部不正抑制手法

予防策の増強 （物理的にできない）	発覚リスクの増強 （やると見つかる）	利得の抑制 （割に合わない）	誘因の排除 （その気にさせない）	弁解余地の排除 （言い訳を許さない）
対象物の強化	**防犯意識の向上**	**対象の隠蔽**	**ﾌﾗｽﾄﾚｰｼｮﾝ・ｽﾄﾚｽ削減**	**ルールの設定**
収納、施錠徹底	ID証装着励行・声掛け徹底	現金・貴重品・情報の扱者限定	良好な職場内ｺﾐｭﾆｹｰｼｮﾝ確保	社会正義優先原理の宣言
保管庫・金庫の導入	貸出し管理実施(ログ記録)	存在情報の限定提供	面接・コーチングの実施	誓約書の回収
情報アクセス制限の設定	インシデントの迅速報告徹底	組織の融通性との勘案	従業員の経済状況把握と支援	社内規定の繰返し指導・確認
情報アクセスの認証実施	防犯意識向上の啓発活動実施	情報提供・秘匿ポリシー策定	生活習慣の把握と対応	規定の定期的見直し・修正
入口でのコントロール	**自然監視性確保**	**対象の除去**	**争いの回避**	**指示サインの明示**
入室管理の実施	死角排除による視認性確保	ｷｬｯｼｭﾚｽｼｽﾃﾑ導入	配属先配慮などの人事施策	諸室での制限事項等の明示
「資格と必要性」の確認	遮蔽物の整理・ﾚｲｱｳﾄ工夫	不要在庫・備品の適正処分・管理	「組織存在意義専心文化」醸成	資料への社外秘等サイン明示
入室ログ取得と管理	PCﾃﾞｨｽﾌﾟﾚｲ視認性確保	不要情報の確実な消去・廃棄	組織内派閥の解消	組織規定集の配布
カギとIDカード等の認証強化	時間的死角排除(単独勤禁止等)	処分・廃棄の確認(監査)	「適材適所」人事の徹底	社内ﾈｯﾄでの規定公開
出口での検査	**匿名性の排除**	**所有者の明確化**	**感情のコントロール**	**良心への働きかけ**
退出管理の実施(ログ記録)	ID証装着の徹底	物へのID付与	従業員の不平不満への対応	良心に働きかける標語の制定
電子タグ等による持出し管理	出入・行動ログ取得/管理	情報へのID付与と変更禁止処理	定期的面接の実施	掲示や配布による標語の周知
GWでの出情報(流出等)管理	ﾌﾟﾘﾝﾄｱｳﾄ/情報ｱｸｾｽﾛｸﾞ管理	在庫・備品の付番管理徹底	ハラスメントの発見と対応	全員唱和による標語の浸透促進
所持品検査(監査)の実施	全ての人間に実施(例外排除)	漏洩情報の特定技術導入	透明性・納得感のある人事/処遇	組織から従業員への「信頼」表明
接近性の抑制	**管理者の活用**	**転売市場への介入**	**内在する不正誘導圧力の低減**	**ルール遵守への支援**
重要エリアへの出入限定	明示的「監視」の実施	ﾈｯﾄｵｰｸｼｮﾝ情報チェック	悪しき組織因習の撤廃	運用実態にあったﾙｰﾙ制定
重要情報のアクセス制限	管理者の意識付け	ネット裏情報チェック	「外の目」導入(組織改編/異動等)	違反不能な仕組み導入
現金・貴重品取扱機会の低減	従業員の意識涵養	ﾎﾟﾘｼｰ宣言と迅速届出/法的対応	組織トップの明確な意思表示	ﾙｰﾙの啓発
持ち出し容易性の制御	組織文化醸成、指導・是正実施	情報公表と情報収集窓口の設置	従業員啓発による組織文化刷新	違反ﾍﾟﾅﾙﾃｨ制定・運用徹底
ツールのコントロール	**組織による系統的モニタリング**	**対象の低価値化**	**模倣犯罪の抑制**	**依存症への対応**
合鍵不能システム導入	総合的内部統制担当部署設置	盗品の流通性低減手段導入	小さな不正を糺す姿勢維持	私生活の観察
携帯電話・ｽﾏﾎ・PC・記憶媒体制限	独立した内部情報収集窓口設置	情報暗号化/時限管理/DRM	信賞必罰の徹底	生活習慣改善の支援
ｺﾋﾟｰ・FAX・ﾌﾟﾘﾝﾀ管理実施	システムによるチェック・監査実現	線引き小切手利用	事件発生時の顛末公表	外部専門家相談ルート提供
ﾒｰﾙ管理・ｱｯﾌﾟﾛｰﾄﾞ管理	定期・不定期監査の並行実施	盗品の製品番号公開と届出	新規類似犯対応ﾎﾟﾘｼｰ公表	解決不能時対応手段の留保

れにあたる。

出口において不定期に従業員の所持品についての検査を行うことも、牽制効果が期待できる。前項と同様、記録を取るだけでも意味がある。

7.1.4 接近性の抑制

対象に近づけないようにすることで、魔がさして生じた従業員の犯行企図を、芽のうちに摘み取る対策である。

犯行ターゲットへのアクセス性や、持ち出し容易性を制御することで実現する。職場内で犯行対象物を扱う機会を減らすこともこの対策である。重要エリアへの出入制限、重要情報へのアクセス制限、現金や貴重品取扱機会の低減などが具体的施策として考えられる。

犯行企図の萌芽を摘み取るためには、「犯行が出来ない」ようにすることが重要である。

7.1.5 ツールのコントロール

不正に必要なツール等を使えないようにする対策である。

合鍵を作れない錠前や、シンクライアントPCの採用などがこれにあたる。私有バッグの職場への持ち込みを制限したり、制服からポケット等を取り去り、その収納を最小限にしたりするのもこの対策である。

情報の不正持ち出しへの対策としては、携帯電話やPC、カメラの持ち込みや、USBメモリ等外部記憶媒体の使用を制限する等の施策がこれにあたる。コピー機、FAX、プリンタなどのOA機器の管理を行うことも有効である。メールの送信管理を実施したり、外部サーバー等へのファイルのアップロードを制限したりするなどのネットワーク的対策も忘れずに行う。PC画面キャプチャーや、印刷・書き込みを不能とする対策も有効である。

昨今、スマートフォンの利用が急増している。PCの利用に関しては厳格なセキュリティポリシーを設定し、運用を徹底していても、スマートフォンの利用には対応が遅れている組織が多い。スマートフォンは、盗聴器であり、盗撮器であり、さらに、USBメモリであり、通信機でもある。スマートフォンの扱いについてもセキュリティポリシーを定め、組織の事業形態によっては、持ち込み禁止、接続禁止等の対応が必要である。

なお、本対策は、意図的な不正への対応策ではあるが、ITを使って情報の外部持ち出しや不用サイト等へのアクセスをできなくする対策は、意図しない従業員のミスを防止するためにも有効である。

7.2 発覚リスクの増強

「不正が見つかる」状況を作ることによって犯意を抑制しようとするものである。

7.2.1 防犯意識の向上

警備員などのセキュリティ担当者が当然することを、一般の従業員が、当たり前の行為として自然に出来るようにしておくことである。

ID証を装着していない人がいたら声をかける、物を貸し出したり、持ち出したりする時は記録をつける、インシデントが発生した場合の報告を速やかにできるようにしておくなどがこれにあたる。QC活動のように、従業員に対する防犯意識向上のための啓発活動を、自主サークル活動のような形で実施することも意味がある。

7.2.2 自然監視性確保

組織内で行われている行為を、常に見えるようにしておくことである。視界を妨げる物を整理する、レイアウトを工夫する等によって死角をできるだけ排除することが基本である。

情報系においては、PCディスプレイの表示を誰もが見えるようにする、メールのやり取りを見えるようにしておくなどの方策が考えられる。

夜間や休日などの単独勤務を禁ずることも、時間的な死角を排するという意味で、この自然監視性確保の範疇に入る。

7.2.3 匿名性の排除

組織内で行われた行為について、その主体を確認することができるようにしておくことで、不正の発生を防止する効果が期待出来る。

具体的にはIDカード等による出入管理システム導入と社員行動の把握、ID常時装着の徹底などによって実現する。プリントアウトや情報アクセスのログなど、総合的なログ管理を行うことも有効である。異常が発生した場合の、状況のトレーサビリティを高め、事後の監査を行いやすい環境を作ることで、内部不正に対する牽制を行う。

「魔がさす」ことは、その人間の組織や社会における地位によらず起こりうることに注意して行う。組織で働く「すべての人間」の行動について、匿名性を排除、行動の主体を明確にし、責任分界点がきちんと認識されていることが重要である。

7.2.4 管理者の活用

組織を統括する管理者が、内部不正やミスを正式なミッションとして明示的にモニタリングすることである。

管理者が常に見守っていることが、組織や従業員にとって、どのようにプラスに働くかを理解させる必要がある。従業員の意識改革を行って、組織の中に、管理者が部下の行動を確認するのが当たり前という空気を作ることができるかどうかが鍵となる。

未熟で性弱な従業員のミスを、問題発生前にチェックし是正することは、管理者の第一義的な責任である。

7.2.5 組織による系統的モニタリング

組織の公正さ、組織内の正義を維持することをミッションとする部署を設置すると共に、組織内にそれを実現するためのインフラを導入することで実施する。

セキュリティを含むリスクマネジメントに対して、部門毎に対応している組織もあるが、系統的モニタリングのためには、各部門間の障壁を排除した、一元的な管理体制が望ましい[7]。

多様な切り口からの定期/不定期監査を並行して一元的に行うと共に、備品/在庫管理も徹底する。従業員に貸与した鍵やIDカードなどのアクセスコントロールツール、PCや携帯電話などの情報機器、法人クレジットカードやタクシー券などの金券類の紛失に対しては、意図的な内部不正、意図のないミスによらずタイムリーな対応が必要である。

不正の予防と発見を支援するためには、常駐警備員等の第三者的立場の専任スタッフを配置する対策も推奨される。また、「人による運用」だけではなく、システムによる機械的、物理的なモニタリングを併用するのが良い。具体的には、機械警備や出入管理システム、持ち出し防止タグ、CCTVカメラ、在庫管理システムなどのシステム導入や、情報漏洩対策として情報セキュリティソリューションを採用することによって不正やミスの抑止を実現する。特に、夜間の残業、早朝・休日出勤等の単独勤務時の管理は盲点となりやすい。社内規定を定める他、これを管理するシステムが必要となる。

また、組織内部の自浄作用の活用のために、公益通報者保護法の趣旨に鑑み、通常業務の指揮命令系統から独立させた形で、報告受付のための情報収集窓口を設置する。内部からの正当な指摘に対しては誠実に対応し、報告者の不利益が起こらないように留意する。

内部から提供された不正事案の情報が、組織運営にどのような形で活かされたかを情報提供者にフィードバックしたり、組織内にアナウンスしたりすることも重要である。組織の対応が不十分だと、情報提供した報告者は組織の自浄能力に限界

[7] COSO-ERMでは、部門閉鎖的な（Silo型の）セキュリティ対策から脱皮し、総合的な対策とするよう推奨している。

を感じ、問題事案がマスメディアやネットなどに公開されることにつながる可能性もある。

7.3 利得の抑制

内部不正を行ったとしても、「費用対効果」的観点から「割に合わない」状況を作ることで、それを予防しようとする対策である。内部不正に費やす手間や心理的負担を増やす手法と、得られる「収穫物」の価値を下げる手法の二つの手段が考えられる。

7.3.1 対象の隠蔽

組織にある内部不正の対象（物や情報）の存在や保管場所を秘匿する手法である。対象に関する情報管理を徹底することで実現する。具体的には、従業員に対して、職務に不必要な情報は提供しないということである。対象の存在秘匿は、そもそもの犯意を生まないという優れた対策となる。

ただし、提供情報を制限すると、従業員の自由度を奪い、組織としての融通が利かなくなって「組織のオペレーション」に支障を来す場合もあるため、注意が必要である。

組織としての従業員への情報提供ポリシーを策定した後に、アクセス権の設定、情報の暗号化や、物品管理などで実現していく。

7.3.2 対象の除去

物や情報などの内部不正の対象を、物理的に取り去り、置かないという手法である。

例えば、交通費等の清算金の口座振込みや、各種チケット類、プリペイドカード、法人クレジットカードの活用などによって「現金が存在しない職場」を作ることは、有効に働く内部不正防止の施策になり得る。また、棚ズレ品・デッドストックなどの不要在庫や、不要備品の処理や破棄を適正に行うことも重要であり、帳簿上の除却処理が終了した後においても、破棄した物が市場に流れたりしないように、確実に適正な方法で廃棄されたかを確認する。

パソコンや情報媒体の廃棄にあたっては、記録された情報を確実に消去し、情報の確実な消去が保証されない場合には、情報記憶媒体を物理的に破壊した後に廃棄する。パソコン、情報媒体の廃棄に際しては、無知によるミスを発生させないようにする従業員啓発も重要である。

7.3.3 所有者の明確化

物や情報などの内部不正の対象に対してなんらかの方法でIDを付与することで、不正に持ち出されたとしても、所有者が判るようにしておくことである。在庫などの内部不正の対象になり得るものについて、その唯一性を証明できる製造番号等の記録を残しておくことも有効である。

対象の所有者を明確にし、トレーサビリティを確保しておくことは、市場における価値を下げ、流通性を低下させることにもつながる。

物理的な対象である在庫や備品の付番管理を徹底すると共に、情報[8]に関しても、その重要さに応じて電子透かしなどのID付与技術を導入する。

7.3.4 転売市場への介入

転売市場に介入することで、組織内部から不正に持ち出された物品の換金を防ぎ、不正を行っても利益がもたらされないようにすることである。

在庫や備品など、現金以外の物品が組織内部から不正に持ち出された場合、その物品は、何らかの方法で転売され、換金されることが多い。

そのため、組織内部から物品が不正に持ち出される事実があった場合、ネットに流れるオークション情報や裏情報をチェックし、もしそこで不正に持ち出されたことが明らかな物品を発見した場合、警察等への速やかなる届け出や法的措置を取る。

[8] テキスト情報へのID付与は、テキストに作成者などの情報を入れ、書込み禁止とするような簡単な方法でも実現可能である。

これらの対応を取る旨のポリシーは、組織内外に対してあらかじめ宣言しておく。また、第三者がそれ発見することを想定して情報公開を行うと共に情報収集窓口を用意しておく。

転売市場への速やかなる対応は、犯罪者に利益がもたらされることを防ぎ、犯人特定の機会を高めて、再発防止につながる。転売市場に対して速やかなる対応が出来るようにするためには、前項の「所有者の明確化」は重要な要件となる。

7.3.5 対象の低価値化

組織内部から不正に持ち出された物品に対して、「盗品である」ことが判る何らかの目印を付与することで換金を防ぎ、犯罪者に利益がもたらされないようにする対策である。

例えば、現金や物品を不正に持ちだそうとした時に、紙幣や物品に、染料によって盗品であることを示すマークを残すシステムを採用して、盗品を特定できるようにする。このマークは証拠になるだけでなく、盗品の市場価値を大幅に下落させる。そのため、犯罪者にとっては、せっかくリスクを冒し、手間をかけて物品を窃取しても、その行為は全く「割に合わない」ものとなる。

「犯罪益の低価値化」は、このような手法の他、情報の暗号化や時限管理、情報の利用や複製を制御・制限する技術（DRM）などのITソリューションの採用、現金化できる者を限定する「線引き小切手」の利用、物品のシリアル番号管理などの手段などで実現できる。

対象を低価値化し、不正によって利益が得られにくくする対策は、「魔がさす」ことによる出来心的不正に留まらず、意志を持って行われる犯罪に対しても有効に働く。

7.4 誘因の低減

組織の環境を整備し、職場内に居る潜在的な犯罪企図者に心理的に働きかけることで、内部不正を起こす気にさせない（犯罪企図の顕在化を防ぐ）対策である。状況的犯罪予防論的対策に、原因論的考え方を一部取り入れて、状況をコントロールすることで、弱い人間に犯罪企図が発生することを抑える試みである。

7.4.1 フラストレーション・ストレスの削減

自分の能力が発揮できて、周囲との良好なコミュニケーションがとれる自分の「社会的な居場所」としての「快適な職場環境」がある場合、人は、その快適な環境を失うことにつながる内部不正（犯罪）をしようとは思わない。

逆に、過大なフラストレーションやストレスを感じ、コミュニケーションも十分に取れない職場では、従業員の職場に対するネガティブな感情が膨らんで、そのはけ口として内部不正を働く犯罪企図が発生しやすくなる。

本手法は、面接やアンケート、人事異動、コーチングやカウンセリングなどの人事的方策によって、従業員が感じるプレッシャーやフラストレーション、そしてストレスを早期に把握し、犯罪企図の発現につながる可能性のあるネガティブな感情をコントロールしようとするものである。

高利の借金を抱え、その返済に追われる状況に追い込まれた人間は、強いストレスを抱えて、それから逃れるために、横領などの内部不正に至ることがある。面接やカウンセリングなどによって、個人のストレス等を把握し、問題を認識した場合、その解決を手助けすることは、犯罪誘因を取り除き、内部不正を防ぐ上で特に有効である。

個人的な借金の要因となる交友関係や、なんらかの依存症的悪癖がある場合、それに対応することも重要である。

7.4.2 争いの回避

相互不信や冷戦構造を内包する組織では、そのはけ口として内部不正が発生する可能性が高くなる。そこで、組織内における相互不信や冷戦の要因を除去し、組織内にわだかまりや、マイナス要

因としての対抗心が蓄積することが無いようにする対策が重要となる。

具体的には、どうしてもそりが合わない人同士を近づけないようにする人事的方策や、個人の好き嫌いを超越して組織の存在意義をより深く追求することに専心する組織文化の醸成などによって実現する。

組織の合併などで組織内に派閥的グループが出来てしまった場合には、意識してそれを解消するようにする。具体的には「組織の意志」としての、派閥力学を超越した判断基準を明示する、派閥や出身組織によらない「適材適所」人事を行うなどの施策によって実現する。

7.4.3 感情のコントロール

組織には、従業員の一人ひとりがもつ感情のぶつかり合い結果として鬱憤が溜まることがある。悪い形で鬱憤が蓄積した組織では、そのはけ口として内部不正が発生する可能性が高くなる。

それゆえ、組織を構成する人間が、己の感情をコントロールし易くし、組織内に悪い形の鬱憤が溜まりにくいようにする対策が重要となる。

具体的施策として、組織を構成する一人ひとりの希望や、不平・不満を、適切な方法で吸い上げ、それに対応する機会を、組織の制度として設けることがあげられる。

昇格降格などの人事異動や、業績評価などを行うタイミングは、人の感情が揺れ、結果として組織内に鬱憤が溜まりやすい時期となるため、制度として面接を行う機会を設け、不平や不満の緩和を行うのが望ましい。

評価項目と基準を明確にした、透明性のある業績評価の実施と、納得感のある処遇の実現が、組織に鬱憤を溜めないために重要となる。

また、組織内で「セクハラ」や「パワハラ」などのハラスメントが横行していたりすると、組織内に鬱憤を蓄積させる原因となる。そのため、どのような行為がハラスメントにあたるかを周知し、研修による啓発を行って、組織内でハラスメント行為を起こさせない体制を作る。また、それにも関わらずハラスメントが発生した場合には、すばやく適切に対応することも重要である。

また、ネット上にある組織の「裏情報サイト」などにも注意することで、自らの組織内で「サービス残業の強要」や「見えないハラスメント行為」が行われていないかについて、チェック出来る可能性もある。

7.4.4 組織に内在する不正誘導圧力の低減

組織によっては、過去からの悪しき因習によって、半ば公然と内部不正が行われていることがあるかもしれない。また、法規やガイドライン等の変更によって、過去は認められていた行為が、突然、不正となる場合もある。組織の文化として、それをするのがあたりまえという形で、内部不正が行われ続けられている場合、それを是正するには相当のエネルギーを要する。

組織の因習として行われている内部不正を是正するためには、その組織のトップが、悪しき因習、悪しき組織文化からの脱却を組織の構成員一人ひとりに対して明確に宣言することが欠かせない。これは例えば、「○○は、組織ルールの違反行為（社会に対する犯罪行為）である。一切行わないことを厳命する。」といった形で、具体的に表現することが有効である。

また、善良な「外部の目」の導入と、かつその「外部の目」が、「組織文化を変える権限を持っていること」の２要件も重要である。

具体的には、徹底した業務監査の実施、内部からの報告に対する情報収集窓口の設置とその運用の徹底などによって実現する。組織改革や責任者の人事異動などによって、組織のスクラップ＆ビルドを行うことも、新鮮な「外部の目」を入れることにつながるため有効である。

悪しき組織文化の刷新は、「正しさに関する当たり前の感覚の醸成」、「清潔な仲間意識の醸成」、「法

令遵守以上の規範性の醸成」を行う研修を実施するなどして、組織で働く従業員一人ひとりに対して「公正を第一とする行動規範」を根付かせて、組織文化を培っていくことで実現する。

7.4.5 模倣犯罪の抑制

割れ窓理論から、「組織内における小さな不正を放っておくことは、不正への無関心の象徴となり、大きな不正につながる」と言える。内部不正の発生を防ぐためには、組織の内部に無秩序の雰囲気を作ってはいけない。

「小さな不正」に対しても、注意、叱責、指導の対象とし、黙認しないことで、従業員に対して、小さな不正を許さない組織の姿勢を示すことができ、それがひいては大きな不正の予防につながる。小さな不正に対応した場合には、個人名を伏せる形で、その顛末を公表し、類似の手口が新たに発生した場合の対応ポリシーを、組織内に宣言するのも良い。

また、小さな不正を早期に是正することに合わせて、注意、叱責、指導等のマイナス評価が、長期にわたり残らないシステムも重要である。

7.5 弁解余地の排除

内部不正に及ぶ弁解の余地を無くし、たとえ従業員が犯罪企図を持ったとしても、実際の犯行として顕在化することを抑える対策である。

組織における、多くの内部不正は「言い訳」によって自己正当化して行われる。一部業界で問題となることの多い「談合」は、「組織のため」を言い訳として、正当化されていることが多い。

内部不正に及ぶ前の自己正当化のための弁解の余地を取り除くことで、たとえ従業員が犯罪企図を持ったとしても、実際の犯行にブレーキをかけることが可能となる。

7.5.1 ルールの設定

「社会にとって正しいこと」を優先した、組織ルールを作り、組織トップの名で組織全体に浸透させる。不正を許さない組織文化を醸成するための基本である。

「組織のため」という言い訳を排除するためには、「組織にとって正しいこと」よりも「社会にとって正しいこと」がより優先される旨を明示[9]したルールが必要である。

ルールに関しては、従業員がその組織に入るタイミングの研修で、ルール設定の背景を含めて、その内容について指導する。加えて、ルール遵守の誓約書を取るなどの施策も推進する。

社会状況の変化等によって、ルールが陳腐化した場合には、見直しを行い、「ルールが実態に合わない」などの言い訳を許さないようにすることも重要である。

7.5.2 指示サインの明示

その場や、その状況で行ってはいけないことを示す「指示サイン」等を、場所や対象に明示する対策である。これにより、「禁止事項だとは知らなかった」という類の言い訳を排除することにつながる。

コピー機の前に「私物コピー厳禁」、金庫のある部屋に「経理関係者以外立ち入り禁止」等のサインを掲示したり、資料に「社外秘」サインを表示したりすることがこれにあたる。

また、ルール集の配布や、組織内イントラネットにそれを周知させるコンテンツを作成して、ルールを、そこにいる誰もが簡単に見ることができるようにしておくことも重要である。

7.5.3 良心への働きかけ

犯罪企図を持ってしまった人間が依然として

[9] 「明示の実例」としては以下がある。
http://www.secom.co.jp/recruit/01company/idea.html

もっている良心に働きかけることで、内部不正の実行を、最後の段階で思い止まらせることである。「社会にとって正しいことをする」ポリシーや「組織の理念」等を基にして、心に響く標語を作成し、配布や掲示などで従業員全員に周知する。また、朝礼や研修などことある毎に、全員でそれを唱和するなどの施策によって、良心に働きかける。

人は全幅の信頼を寄せられていると、「良心の呵責」があって、簡単に悪いことは出来ない存在でもある。この観点から、組織で働く従業員が、信頼されている自分を認識していることは重要である。組織で働く従業員に対して、組織側の「信頼」が雇用の根底にあるべきことは当然であり、従業員がそれを意識できるようにする。

7.5.4 ルール遵守への支援

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。

これを防ぐためには、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。

具体的には、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。

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。そのため、ルールの形骸化に対しては、組織として特に注意が必要である。

また、従業員が無意識のうちに、ついうっかりルール違反をすることがないように、組織として支援することも重要である。具体的には、無知による違反を起こさせないことを目的とした研修を実施したり、違反が出来ない仕組みを導入したりすることである。スパムメール排除のためのフィルタリングや、ウイルス対策ソフト、複数のメール宛先を自動的にBCCとする等、ITを利用したセキュリティ対策の導入は、ヒューマンエラーを自動的に未然に防ぐ効果が期待できる。社会的に問題となったファイル交換ソフトを検知、排除するソフトの導入も、不用意な情報漏洩の対策となり得る。

ルール策定にあたっては、ルールを守りやすい環境を合わせて提供し、それと同時にルール違反に対するペナルティも用意する。これらの運用が徹底されなくなると、ルールを守る意識が希薄となり、その遵守が徹底されなくなる。

7.5.5 依存症への対応[10]

従業員が、基本的には善良であり、合理的な判断と行動をする存在である限りにおいては、ここまでの対策で、内部不正の抑制に相当の効果が期待できる。一方、この前提が、薬物やアルコール、ギャンブル、カルトなどへの依存や、組織外における不適切な交友関係などによって崩れた場合、常識的な対応では、内部不正の発生を防ぐことが難しくなる。

そのため、組織としては、従業員がなんらかの依存症的状況に陥っていないかどうかに注意を払う必要がある。

[10] 社会一般を対象としたCornishらの整理[19, 20]では、「薬物・酒類のコントロール」となっているが、本稿では組織の内部不正抑制の観点から表記のように変更している。

日々の様子の観察、面接などによって、従業員の私生活の状況を把握し、過度の依存症や、問題のある人間関係などがある場合、その解決を手助けする。私生活の状況把握のための面接やカウンセリングは、前述した従業員の「フラストレーション・ストレスの削減」(7.4.1 項) を兼ねても良い。依存症への対応は、組織内部だけの対応で解決出来ないことも多いため、医師や弁護士、カウンセラーなどの外部専門家に協力を仰ぐことも選択肢に入れる。

また、どうしても解決が出来ない場合に備え、「円満退職」への道を、あらかじめ就業規則に定めておく。

8. 組織文化による内部不正抑制

内部要因事故への対策は、組織という閉じた集団が対象であり、社会一般という漠とした集団を対象にしているわけではない。そのため、犯罪者を作る組織内の要因を特定し、それを変える手段を考える手法（原因論的アプローチ）も有効に機能する。

我々は、この観点から組織に内在する不正やミスの原因に焦点を当て、犯罪原因論的立場から「組織文化」の醸成による内部不正 / ミス抑制の方法論を考察した。

具体的には、ある人物が組織に就職してから、退職するまでを想定して、時間軸順に、

- 募集と就職時、
- 就職後数ヶ月、
- 在職中、
- 重要ポスト異動時、
- 退職時、

の５つのフェーズに分けて、内部不正企図やミスを生み出さないための組織要件を整理した。

加えて、各々のフェーズについて、筆者らの経

表２　職業ライフサイクル、組織論的観点からの内部不正 / ミス抑制手法

募集と就職時 （適格人材雇用と教化開始）	就職後数ヶ月～ （組織文化の定着）	在職中 （ミス/重圧、誘惑対応・ES向上）	重要ポスト異動時 （職責再認識・職権乱用抑制）	退職時 （リスクを残さない）
募集時の組織理念の提示	**入社後研修/OJT実施**	**技術による未然防止と早期対処**	**上位職者への責任自覚推進**	**迅速処理の実施**
組織理念、組織存在意義提示	ｶﾙﾁｬｰｼｮｯｸ緩和・対応	技術的ﾌｫｰﾙﾄﾄﾚﾗﾝｽ施策導入	組織ﾌｨﾛｿﾌｨの再確認	意志再確認と迅速処理
判断、意志決定、行動の基準提示	集合研修実施	各種監視/証跡確保/IT的対策	組織の判断基準再確認	迅速な職務解任/権限・行動制限
理念、基準共感者採用の宣言	同僚/先輩と親睦・情報交換促進	行動ﾛｸﾞ自動取得	研修実施と誓約書回収	退職スケジュールの早期確定
非共感者の自発的応募断念促進	悩みﾋｱﾘﾝｸﾞ機会設定	Up-to-dateな最適技術導入	自覚啓発へのﾄｯﾌﾟのｺﾐｯﾄﾒﾝﾄ	退職理由調査と結果の有効活用
採用時選考	**プロ意識の醸成**	**不正巻込まれリスクへの対応**	**コンプライアンスの再徹底**	**情報セキュリティ対策**
人格、性癖、生活態度の確認	仕事をすることの誇り醸成	不適切交友、依存症対応	幹部としてのﾙｰﾙ/責任再確認	情報ｱｸｾｽ権の迅速制限
注意力、適応性、経済状況の確認	ｴﾌｪｸﾀﾝｽへの意識付け	収入実質ダウンへの注意	関連法規研修の実施	情報ｱｸｾｽ監査強化/誓約書回収
総合的観点の採用基準策定	社会貢献の実績紹介	ｿｰｼｬﾙｴﾝｼﾞﾆｱﾘﾝｸﾞ、癒着に注意	ｺﾝﾌﾟﾗｲｱﾝｽ関連ｽﾀｯﾌの配置	ﾒｰﾙ・PC・OA機器使用制限
不採用者への誠実、迅速な対応	先輩の仕事見学/体験談聴聞	過度重責感からの解放	個人の贈答受納/無理強要の禁止	退職者関与知財への注意
採用決定時と就職時の手続き	**将来目標の意識付け**	**健全私生活の支援(金銭面)**	**監査機能の充実**	**貸与物の回収**
内定式、入社式などの儀式挙行	本当のプロへの憧憬意識醸成	緊急資金融資制度の設置	ｼｽﾃﾑによる自動的監査支援	貸与品(ID証、制服等)の回収
宣誓書、誓約書回収	複数キャリアパスモデルの提供	総合的な自助努力支援	職位によらず毅然対応	鍵類回収への特別注意
理念訓示、意識再確認	収入推移の目安モデル提示	従業員間の金銭貸借制限	幹部への監査ポリシー周知	貸与品紛失時の厳格対応
貸与品の責任管理の意識付け	自己研鑽機会の提供と周知	各種手当等での私生活支援	監査機能の独立性確保	健康保険任意継続時に注意
採用時研修	**適切な評価と指導**	**健全私生活の支援(非金銭面)**	**複数確認と不正ﾘｽｸ管理制度**	**コンプライアンス対応**
組織理念、意義の集合研修	「業務評価」への意識付け	各種専門家/専門機関紹介	重要物取扱時の複数対応・確認	各種社会保険等の説明/処理
ﾙｰﾙ遵守意識啓発	「役割期待」と「評価項目」明示	家族の健康管理支援	無条件の「資格と必要性」判断	未払金/有休/退職金処理
違和感・ｱﾚﾙｷﾞｰ感情への対応	「透明性」と「納得性」確保	勤務時間弾力運用	ﾘｽｸﾏﾈｼﾞﾒﾝﾄﾌﾟﾛｸﾞﾗﾑの導入	退職後義務説明/誓約書回収
従業員家族へのﾒｯｾｰｼﾞ発信		私生活安定化/充実化支援	人事異動・長期休暇取得義務化	住居/貸付金/提供便益の合意
ルールの指導	**相談窓口の用意**	**モラール管理**	**マスメディアへの対応**	**退職後の関係維持**
ルールとその策定背景の指導	ｶﾙﾁｬｰｼｮｯｸ/失望/不安へ対応	個人ﾐｯｼｮﾝ明確化支援	「ｽﾃｰｸﾎﾙﾀﾞｰ窓口」意識再確認	(公式/非公式)送別会等の実施
集合研修/OJT/ﾈｯﾄ学習の併用	相談担当先輩(メンター)選任	ES重視/職場活性化/研鑽機会	事故時の事実確認と誠実対応	感謝状、記念品等の贈呈
ﾍﾟﾅﾙﾃｨへの意識付け	ｺﾐｭﾆｹｰｼｮﾝｷﾞｬｯﾌﾟ解消	家族の理解支援/適正賃金支払	事実/正式方針のみ発表	連絡先メンテと定期連絡
理解度確認試験の実施		能力把握/多様ｷｬﾘｱﾊﾟｽ体系準備	各社平等対応と情報同時公開	「退職後は『外部の人間』」に注意

験則をベースに、犯罪予防論や組織論、労働管理論などの学術的知見も加えて考察し、それぞれのフェーズについて５つの具体的抑制手法をフレームワークとして考案した。表２にその結果を示す。本章の内容は、従業員の内部不正やミスを特に重要視するセキュリティ産業における筆者らの経験をベースに考察したもの[11]であるため、一般的な組織にとっては極端すぎると感じる向きもあるかもしれない。各組織において具体的対応手段を検討する際に、この内容を参考に適宜取捨選択してもらえればと考えている。

8.1 募集と就職時

適格人材を採用し、加えて採用時の教育・研修という人材育成を徹底することで内部要因事故が発生する潜在リスクを出来るだけ抑えようというアプローチである。

内部要因事故を引き起こしやすい人を従業員として採用しない根本的対策と言える。その組織の、社会における存在意義、行動原理、共通理念等を示し、それに賛同し、かつ常識的な注意力を持った人材のみを雇用するのが基本である。

8.1.1 募集時における組織理念の提示

人材の募集に際し、組織の設立理念、沿革、存在意義、行動原理等、組織の文化、フィロソフィや、組織のあらゆる行動や意志決定の際の判断基準（いわば「組織のＤＮＡ」）を明確な形で提示し、それに共感共鳴できる人材を求める旨を宣言することである。

これによって、その組織の理念に賛同する応募者を集めると同時に、その組織の基本的考え方に馴染まない者の応募をなくすことができる。

8.1.2 採用時選考

一般社会の場合と違い、組織の場合は、採用時の選考手法を工夫することによって、リスクの高い人物を雇用しないようにすることが可能である。

一般に人材採用時には、実績や資格、能力などの組織の業務を遂行できる資質を持つかという点に注意が向きがちであるが、内部不正やミスなどによって引き起こされる事故の抑制という観点からは、その人物の人格や、性癖、組織への適応性、注意力、経済状況、生活態度という点に注意する必要がある。

採用選考の際には、雇用に関する明確な採用基準を作っておく必要がある。たとえ能力や実績が優れていても、精神の安定性、協調性等その他の部分も考慮し、組織のオペレーション全体を考えて総合的に判断するのが望ましい。

また、不採用となった応募者に対しては、誠実かつ迅速にその旨を伝えることも重要である。

8.1.3 採用決定と採用時の手続き

採用選考で各種の採用基準に合致し、採用を決定した人物には、その旨を早急に伝えると共に、「採用内定書」などの正式文書を交付する。

採用者の心に組織の一員になるという自覚を植えつけるために、内定書の交付は、「内定式」などの儀式として行うことが望ましい。内定式の際には、組織の理念等を再度認識させ、組織のルール遵守や、反社会的行為、違法行為などを行わない旨を、「宣誓」させ、誓約書を兼ねた就職承諾書を回収するのも良い。

内定後に、精神的に不安定な状態に陥る人間もいるため、内定確定後のフォローも考慮する。雇用開始日に制限が無い場合には、内定と雇用開始の間に日をおかない。

雇用に際して発生する様々な個人的事案に対しての、物理的、経済的支援も、その人間の組織へのロイヤリティを向上させるうえで効果がある。

就職時にも、入社式など何らかの儀式を設定し、

[11] あくまでも筆者らが考察した私見であり、必ずしも筆者らの所属する組織のものではない。

そこで、組織幹部による組織の理念等の訓示を行うことに加え、ルール遵守意識を再び徹底する。各種社会保険のための必要書類の回収や、従業員証（ID 証）や制服などの貸与、健康保険証の交付などは、できるだけ速やかに行う。

貸与物には管理番号を付与して、その管理を徹底する。鍵、カード等は、紛失時、早急な対応が必要であるため、その管理は特に徹底する。また、貸与期間が、長期間に渡るものもあるため、貸与物管理簿自体の管理についても十分に注意を払う。

貸与に際しては、貸与である旨の再確認と、紛失の場合の対応などのルールを説明する。

8.1.4 採用時研修

多くの組織では、新たに従業員を雇用したタイミングに合わせて採用時研修が行われる。

採用直後から「現場」に配属して、OJT で職務を教え始める組織もあるが、内部不正抑制という観点からは、組織の行動原理や理念、ルールを再徹底し、ルール遵守意識を強く根付かせる研修を、職務と切り離した形で、Off-JT（集合研修）で行うのが望ましい。

新入従業員に組織の考え方を周知し、啓発することが目的の研修であるため、指導される内容に違和感を覚える者も出てくる場合があるが、丁寧に指導することで、組織の将来を託す優秀な従業員を育成する。

従業員の家族は、犯罪原因論的観点からは重要な存在である。そのため、組織として新入従業員の家族に対してもメッセージを発信し、「組織のＤＮＡ」やルールに対しての理解者になってもらうことにも意味がある。

8.1.5 ルールの指導

職場のルールや関連法規遵守などコンプライアンスの徹底のためには、その組織にどのようなルールや、守らなければいけない関連法規があるかの知識が欠かせない。実際に、ルールを知らなかったことによって問題が発生した事例は多い。

このような事態を避けるために、集合研修や、職場における OJT、e ラーニングなどを組み合わせながら、ルールや関連法規の教育、指導を徹底する必要がある。

ルールの教育、指導の際には、「なぜそのルールが策定されたのか（WHY）」を理解させる。加えて、ルールを守ることで自らにもたらされるメリットなどについて、事例研究などを行って、考えさせる。WHY について人々の納得が得られなくなったルールについては、陳腐化している可能性もあり、適宜見直しを行うべきである。

教育、指導の際には、ルール違反をした場合の組織が社会から受ける非難や影響、有形無形の処分や制裁など、ペナルティの情報も伝えて考えさせる。

ルールの教育、指導に関しては、違反の際に、知らなかった、聞いていないという言い訳を排除するために、研修の内容を本人にも確認させて記録を残す。例えば、ルールや関連法規の理解度を、採用当初の「試用期間」を終了する要件としての試験科目にすることも、ルール遵守徹底の施策として有効である。

8.2 就職後数ヶ月～

採用後数ヶ月間の時期は、新規採用者にとって、新たな変化にさらされる時期となる。

この時期に、組織の中に自らの居場所を見つけ、自己実現のための場として位置付けることが出来た人間は、活きいきと働き始め、やがては組織の中核となる人材として飛躍していく。このような人間は内部不正等の問題を起こすことも少ない。

本節では、新しく入った人間が、その組織で活きいきと働ける人材となるきっかけをつくるために、組織として採用後数ヶ月間で出来ることについて論を進める。

8.2.1 採用数ヶ月後の新人研修／ OJT 実施

多くの新入従業員は、採用直後の研修を終えて、実際の仕事の現場に配属されると、組織の外から見た姿と内から見た姿の違いに戸惑いを感じる。カルチャーショックや、失望感を感じるのは、多くの新入従業員が直面する問題であり、これによって自暴自棄[12]に陥ったり、「うつ」になったりする場合もある。

このような不安定な状況を緩和し、組織の存在意義や仕事の意味を再確認するために、現場での OJT と合わせて、採用後数ヶ月の時点で、集合研修を設定するのが望ましい。新人が抱える様々な悩みを、同僚や先輩を交えて解消するのが目的である。

8.2.2 プロ意識の醸成

プロフェッショナルな組織人として、仕事をすることへの誇りを醸成することである。

「自らの仕事が人々や社会のためになっている感覚」、すなわち「自己の活動が周りに（良い）変化をもたらすことができたという感覚（効力感：Feeling of Efficiency）」は、「エフェクタンス（Effectance）」[21] とも呼ばれ、自らを「プロフェッショナル」として自覚するために必要不可欠な感覚である。

自らの将来に、どのようなプロとしての仕事があり、その仕事が周りにどういう変化をもたらしうるか」を意識させることが重要である。組織の仕事で得た「礼状」や受賞事案を紹介し、それを得るまでの「苦労話」を聞かせるのも良いし、活きいきと働く優れた先輩の仕事ぶりを見せ、自らも頑張ることでその域に達することが出来ると感じさせるのも良い。

真のプロフェッショナルは、仕事そのものを通して自己実現欲求が満たされているため、不正に関わることは少なくなる。

8.2.3 将来目標の意識付け

組織に入って間もない人間に対し、将来のロールモデルとしての様々な先輩の成功例を見せ、そこに至るまでの複数のキャリアパスを示して、モチベーションを与えようとする施策である。

組織の中での、自らのキャリアイメージを明確に持たせ、それに向かって頑張ることに意識を集中させることで、内部不正の機会があったとしても、それに関わることを抑制できる。また、キャリアアップによって実現される「収入推移の目安モデル」なども示すと、未来に希望を持たせ、内部不正を抑止する効果が期待出来る。

組織に個人の能力開発を支援するための制度がある場合は、その説明も行う。

8.2.4 適切な評価と指導

組織に入ったばかりの新入従業員に対し、「組織における業務評価」の存在とその意義を理解させると共に、「評価項目」と、組織としての各従業員への「役割期待」を明示することである。これによって、評価の「透明性」と「納得性」を確保する。

新入従業員自身に、自らがどう動けば良いかの行動の指針、すなわち役割期待を考えさせることに加え、「組織の風通し」を良くする効果が期待出来る。

8.2.5 相談窓口の用意

実際に仕事の現場に配属されて、カルチャーショックや失望感、生活の変化からくる不安やストレスを感じている新入従業員に対して、相談に乗る窓口を設ける施策である。

新入従業員にとって、配属された部署における上司は親子ほど年が離れていることも少なくなく、相談窓口としては敷居が高いことも多いため、配属された新人ごとに、メンターとして身近に相談に乗る役割を持たせた、年齢の近い先輩をつける。

[12] 一般に、自暴自棄に陥った人間は、犯罪企図を抱きやすい傾向を持つため注意が必要である。

8.3 在職中

組織で働く従業員は、日々の業務を遂行する上で、様々な状況を経験する。喜びや達成感を感じ「働く者としての至福」を覚える状況も多い一方、精神的重圧やストレス、ジレンマなどの心理的追い込まれ感を感じる局面も少なからず存在する。また善意や、他意無く行った行為が、大問題に発展してしまうケースも起こり得る。

フルタイムで働く人であっても、一般にはその手持ち時間の3割程度[13]で仕事をしているに過ぎない。手持ち時間のうち7割を占めるのが個人としての生活時間である。この個人としての生活で問題を抱えた場合、通常通りの仕事が出来なくなる場合も多い。それゆえ、組織で働く従業員に100%の能力を発揮してもらい、組織のオペレーションをきちんと担う要員となってもらうために、組織として従業員の「個人の生活」を守る必要が生じる場合もある。

本節では、組織で働く人間が、普段の業務を行う上において、また個人として生活するにおいて直面する様々な状況に適切に対応し、内部不正やミスなどの問題の発生を抑制するために組織として出来ることについて述べる。

8.3.1 技術による未然防止と早期対処

組織内で発生するかもしれない不正行為やヒューマンエラーによるミスなどを、安全工学やインダストリアルエンジニアリング（IE）、ITなどの技術的知見と方策を使って未然に防いだり、早期対処したりする対応である。

組織を回す当事者は、人間である以上、「ついうっかりで」、「ついなあなあで」、「よく知らずに」という原因で、ルールから外れた行為をしてしまうことがある。事故が発生した際に、原因を作った人間にペナルティを課したとしても、根本的解決にならず、逆に関係している人間を臆病にさせ、それが組織運営の妨げになることもある。

そのため、無知やその性弱性から従業員がルールから外れた行為やミスをしてしまったとしても、安全側に倒れる「フォールトトレランス」の措置を施し、事故を未然に防止したり、事故が発生した場合でも、大事に至らない対策をとったりすることは、従業員に安心感をもたらし、のびのびとした仕事が出来る組織をつくることにつながる。

また、それにも関わらず禁止行為などを行った場合、すぐに分かるようにモニタリングの手段も導入し、早期解決が出来るようにしておく。モニタリング手段を用意しておくことは、後々の原因究明や捜査などの「フォレンジック」の手立てを残しておくことにもつながる。

対策の具体例として、データなどの監査システムの導入、たとえば、内部統制やリスク管理に役立つさまざまなソフトウェアを用いて、主要業績指標（KPI: Key Performance Indicators）等のモニタリングを常時行うことも効果的である。また、外部記憶媒体の管理と規制、情報や不正ソフトのフィルタリングの適用、データの自動暗号化、システム操作の自動ログ化などの情報セキュリティ面の対策技術の導入も考えられる。

情報セキュリティの対策以外では、車両の各種安全装置による事故防止や、テレマティクス、ドライブレコーダーによる車両運転記録、GPS位置検索端末による持ち出し情報機器の紛失対策、GPS携帯電話を使った営業員の位置把握と外出時勤怠管理などが考えられる。

導入可能な技術は、時代や組織の業態によって変わるため、世の中に存在する各種安全技術を注意深くリサーチし、検討した後に導入することが

[13] 2007年の平均労働時間1850時間（厚生労働省「毎月勤労統計調査」）を、1日あたり8時間分の睡眠時間を除いた年間時間数5840時間で除して計算した値。

[14] 2005年4月の福知山線脱線事故では、運転士への罰則的制度が、その遠因になったというマスコミ報道もある。

望ましい。

また、本項で実現する具体的方策は、従業員を萎縮させ組織のオペレーションを逆に阻害すること[14]もあるため、導入に関しては慎重を期す必要がある。

8.3.2 不正巻き込まれリスクへの対応

「組織で働く従業員がおかれている環境や状況」から犯罪誘因を取り去ることで、内部不正を抑制しようという取り組みである。

組織として、不適切な団体との関係がある場合には、弁護士や警察などとも相談してその関係をきっぱりと絶つことは言うまでもないが、従業員が個人的に、業務遂行の妨げとなる、不適切な交友や、反社会的なカルト団体などとの関係がある場合についても相談に乗り、必要に応じて弁護士などの専門家の助けも借りながら、その関係の清算を支援する[15]。

従業員に対し、各種依存症の危険についての意識付けを普段から行い、健全な社会生活を破壊するものであることについての注意喚起も忘れずに行う。

高利借金への依存は生活破綻の要因となるため、その利用を制限する。既に借金等で困窮している従業員に対しては、その生活改善意志を確認し、健全生活に戻るための自助努力の支援を行う。

組織として、従業員の実質的収入が減る施策を行うことは、生活困窮へのきっかけとなる可能性もあることから注意が必要である。過度の時間外労働や、時間外労働への賃金不払いは、従業員の不満の源になり、ミスや不正などの事故へつながることもある。労務管理のコンプライアンスを徹底することは当然である。

派遣社員やアルバイトなどの非正規労働者がいる場合、共に働く仲間であることに留意し、その対応には十分配慮する必要がある。また、外国人労働者を従業員として雇用する場合には、彼らの常識や習慣、価値観が、日本人のそれとは大きく異なることに留意する。

人の不用意な行動や、ミスにつけ込む手法である「ソーシャルエンジニアリング（Social Engineering）」[22]のリスクから、従業員を守ることも重要である。仲間うちの会話や、組織から出る廃棄物、業者等に成りすまされた電話で不用意にした会話、職場内の掲示物などから情報が漏れるリスクを念頭におき、従業員の啓発を行う。

これまで、多くの内部不正が、従業員と取引業者などのステークホルダーとの私的な交流が遠因となって行われてきた。従業員と組織のステークホルダーとの行き過ぎた関係による不正が起きないように、明確なルールを設定し、公表したうえで、その運用を徹底する。

また、日々の業務を遂行する上で、全ての責任が、あたかも一人の担当者にかかるような感覚を持たせないようにすることにも配慮が必要である。そのような感覚は、心理的重圧となって、小さな異常が発生した場合の虚偽報告につながり、それが大きな事故に発展する場合がある。

従業員が安心して働くことが出来るようにするため、業務上の行為から発生した民事訴訟案件などには、組織として対応する。

貸与物や金券類は、定期的に監査し、紛失等の場合は速やかに報告させ、対応する[16]。この場合、従業員を罰するスタンスでは報告が滞り、それが問題に発展することが多いため、性弱な従業員を守るというスタンスで事に当たることが重要である。

組織で働き、日々の生活を営んでいる従業員の「不正巻き込まれリスク」を減らすために一番大切なことは、従業員自身のリスクに関する感性を高

[15] 暴力団排除条例が各都道府県で施行されている。

[16] 外部に流出した場合、不正使用の可能性がある、鍵やIDカードなどのアクセスコントロールツール、ブランクの信憑書類、情報機器、法人クレジットカードやタクシー券などに注意する。

めることである。このような組織文化を構築することで、従業員が直面する、日々変化する多様なリスクに対応していくことが出来るようになる。

8.3.3 健全私生活の支援（金銭面）

従業員の収入以上の生活は、組織内で発生する種々の問題の源になることが多い。ここでは、内部不正などの人為的事件のリスクを抑制するために、組織として、金銭面について従業員を守っていく方策について論を進める。

不可抗力などによって突発的にまとまったお金が必要になった場合に対応するために、組織として従業員に資金を貸し出す「緊急資金融資制度」を設けることが推奨される。従業員を、緊急な金銭的な逼迫状況から救済することが目的であるため、スムーズな融資を行い、金利や返済期間にも配慮する。

私生活において発生した金銭的逼迫状況からの救済という目的に鑑み、この制度を利用する条件として、金銭の必要理由については必ず申告させる。計画性の欠如に金銭的逼迫の原因がある場合は、それが再発しないように指導、啓発を行う。金銭の手当て以外で、従業員の私生活をサポートする手段がある場合は、それを使うことも選択肢に入れ、組織として総合的に相談に乗れる制度とするのが望ましい。

従業員間で、まとまった金額の金銭貸借を行うことは、組織内トラブルの要因となることも多いためこれを禁止する。

また、従業員のライフステージや家族構成の変化に合わせて、資金の積み立て制度を提供したり、各種手当てを支給したりする制度の導入も考えられる。

従業員の生活が収入に見合わないものになったり、金遣いが急に派手になったりした場合、何らかの対応が必要になるケースがあることから、組織としては、プライバシーに配慮しつつも注意をもって従業員を見守る姿勢も必要となる。

8.3.4 健全私生活の支援（非金銭面）

従業員が、私生活で抱える可能性のある問題は金銭面に留まらない。組織として、従業員の私生活をサポートすることは、従業員の家族を、組織の味方とすることにもつながる。

従業員がプライベートで遭遇する法的問題や、健康問題に対応するために、弁護士や税理士などの専門家や、優れた医師や病院などを紹介する制度を設ける。

また、家族が健康面の問題を抱えると、その従業員は組織における仕事で、100％の能力を発揮出来なくなることが多い。そのため、組織としては、法定義務のある従業員自身の健康管理に準ずるレベルで、その家族の健康管理についても考えた方が良い。

2006 年に「労働時間等設定改善法」が施行され、社会全体で労働者のワークライフバランスを重視する動きがでている。組織には「従業員の健全なる私生活」を支援することが求められている。特に、保育が必要な乳幼児や、要介護者が従業員の家族にいる場合などに、配慮する必要がある。

ワークライフバランス施策として、個人に出退勤時間のある程度の自由を認めるフレックスタイム制や、時間管理を完全に個人に任せる裁量勤務制を採用した場合、仕事の時間管理がおろそかになり、むやみに働いて健康を害するなどのマイナス面が出るケースもあるため注意する。

組織のオペレーションを阻害する要因である「従業員の私生活の乱れ」リスクを除去するという観点から、組織として「従業員の結婚」や「家族との同居」等、生活全般を手助けする制度も意味を持つようになってきている。

8.3.5 モラール管理

従業員を真に幸せにする組織では、人々が活きいきと働き、その環境を失うことにつながる内部不正を働く人間は出て来にくい。そのため、組織に所属する従業員の働く満足度（ES: Employee

Satisfaction）を高め、働くこと自体が従業員の幸せにつながる組織を作ることは、内部不正が発生しにくい環境を作ることに直結する。

「組織のミッション」達成に対し、特に優れた貢献のあった従業員を昇進・表彰対象とし、その事実と共に、それに至った詳細な理由を周知するのも良い。「組織のミッション」を、各人が納得できる形で「個人のミッション」に分解して渡すこと[17]は、「ESの向上」「組織の活性化」の第一歩である。

「表彰と制裁」は、組織が従業員のモラールと意識をコントロールする上で表裏一体のものである。そのため、表彰は、先に述べた制裁措置発動の場合と同様に、公正に公平に行う必要がある。本人や周囲に納得感の得られない表彰・制裁は、組織のモラールアップに逆効果を及ぼすこともある。

組織への礼状や好意的な「お客様の声」などは、従業員に必ず紹介し、それが「個人の行動」に端を発したものであった場合、社内報や各種ミーティング等でその個人を表彰・賞賛[18]する。

逆に、組織内においてルール違反が発生した場合には、あらかじめ定め、周知された制裁規定に則って、制裁措置を発動する。従業員に、ルール遵守の意識を深く根付かせるために、小さいルール違反や事故であっても、その運用は厳正に行う必要がある。ただし、その厳正な処罰が、その後の従業員の育成に影響しない組織の文化も重要である。具体的には、制裁が評価に及ぶ期間を短期に限定する手法が考えられる。

大きな組織では、従業員の視野が、自分の所属する事業所からなかなか拡がらない場合がある。「組織が社会に対するミッションを遂行する姿」、「組織の現在進行形の姿」を従業員に実感させるために、組織内の色々な仕事を見る機会を作ることにも意味がある。

ES向上のためには、組織の理念、社会に対する存在意義や沿革、事業内容、従業員それぞれが行っている業務が、家族から理解されることも重要である。仕事場を従業員の家族に公開する「家族参観日」を設ける、クリスマスや家族の誕生日、結婚記念日などに家族への感謝状とともにプレゼントを贈る、職場のイベントや、表彰式などに家族を招待するなど、様々な具体的施策が考えられる。

人は成長したいという本能を持つ動物である。従業員に対して、自らのキャリアパスを再考する機会を設けて、組織内外で転身する機会を与える、各種研修・教育を受ける機会を作る、資格や学位などの取得支援をする等の具体的施策で、自らの能力を向上させる機会を与えることにも意味がある。

職務における発明考案などには、最低限のコンプライアンスに則った対応だけでなく、組織への貢献に応じた報奨制度を用意し、従業員に広く周知する。

人がエフェクタンスを感じるためには、自分の価値観に合致する仕事を、自分の強みを十分に発揮して行い、かつそれが世の中から受け入れられているという感覚が欠かせない。そのために、組織として、従業員一人ひとりの持つ能力を把握、適切な管理を行って、それを活かし、かつ従業員自身の希望が反映できる複線の人事体系を実現することが望ましい。

報酬、収入面からエフェクタンスを感じてもらうために、従業員の能力・適性と、業績を正しく評価し、それに報いる。納得できる賃金を提供することは、従業員を雇用する組織に課せられた重要な役割であり、ESのためにもこれは欠かせない。

定年まで雇用するという原則は、日本社会においても過去のものとなる傾向にある。その人間をより必要とする別の組織があったり、その人間が

[17] これは、論語の言うところの「天命を知る」を体現することにも通じる
[18] 皆の拍手で賞賛の意を表す、いわゆる「パチパチ表彰」なども効果的である。
[19] 大学病院・医学部の「医局・講座制」は、ある意味、これを具現化させた制度となっている。また、防衛省では、自衛隊除隊後の活躍の場を開拓するのが、自衛官の士気高揚のための重要な施策となっている。

より能力を発揮できるチャンスがあったりする場合に備え、飛躍の機会を提供できる体制[19]を用意しておくことは、従業員のモチベーションアップに貢献し、組織全体のモラール向上につながる。働き方が多様化している昨今、定年まで雇用することだけが、組織としての真の雇用責任ではないということに注意が必要である。

従業員のモラールを維持し、モチベーションを高く保つためには、エフェクタンスの感覚に加え、周囲からの支援（関係性）、そして、自分の仕事のある程度の部分については、自分の裁量で進めているという感覚（自律性）が必要である [23, 24]。

また、組織内部に「極端な不満分子」を抱えることは、組織の構成要員全体に悪影響を与え、モラールダウンにつながることもある。そのため、「円満退職」という選択肢を用意しておくことも重要である。

8.4 重要ポスト異動時

従業員の中には、所属する組織の中で業績を積み、職位が上がって重要な地位に就くものも出てくる。また、始めから重要なポストで雇用を開始する場合もある。

組織内部で重要ポストに就いた者（以下、「幹部」）の、最大の役割は「判断」である。そしてその判断は、個人ではなく、組織としての意志を示すものになる。組織内で責任ある立場にある幹部の判断により行われた内部不正や事故、これらの見逃しや不作為、事実隠蔽などは、個人としてではなく、組織の意志によって為されたものと見なされる。組織ぐるみの不正や事故は、世の中に与える影響が大きく[20]、組織のオペレーションに大きなインパクトを与えて、その存続自体が危うくなることも少なくない。

また、幹部も人間である以上、性弱な本質を持ち内部不正に関わる行為をしてしまうことがある。幹部が関わる不正などの行為には、組織内の「ブレーキ」が利かないことも少なくない。

本稿で示す各種内部不正や、認識不足によって発生するミスへの対策は、組織のオペレーション、とその存続を考えた場合、組織幹部に対してこそ、より必要になると言える。

8.4.1 上位職への責任自覚の推進

幹部の判断は、組織全体や、管轄する部署の意志を示すものとなる。組織内外のステークホルダーが持ち込む多くの案件に対して、幹部が行った判断の誤りや「ぶれ」、不作為は、組織としての行動と見なされる。幹部に登用された人間の責任は重大である。

幹部に登用された人間に対しては、出来るだけ早いタイミングで、組織のとるあらゆる行動の基本となるフィロソフィ、すなわち、組織の社会に対する存在意義、沿革、行動原理、組織の文化などの、組織の行動や意志決定の際の判断の基本となる考え方を再徹底する必要がある。

新任幹部に対し、これらを再徹底する啓発は、組織トップに課せられた重要業務である。組織トップの確固たる意思（コミットメント）を得て為されなければならない。

8.4.2 コンプライアンスの再徹底

幹部の判断は、組織の意志を表し、その行動を決定するものであるため、関係法規や組織内外のルールに関するコンプライアンスは、幹部に登用される前と比べて、桁違いに重要なものとなる。「よく知らず」にという理由からコンプライアンスに抵触する判断をしてしまうことは許されない。

そのため、幹部登用時の関連法規や組織内外のルールに関する実務研修は必須である。幹部が、関連法規やルール全体を把握するのに無理がある場合、関連法規やルールに詳しいスタッフをつけ

[20] 多くの人の生活に直接的な影響を与えた事件の代表例として、2005 年に発覚した「耐震強度偽装事件」があげられる。

るなどの施策も考えられる。

職務上知り得た情報を元に株式売買などを行ういわゆるインサイダー取引には、幹部の家族を含めて特に注意する。また、組織の内外からの贈答品等を個人で受け取ったり、外部業者などに職責を背景とした法外な圧力をかけたりする行為は、職位や職責を利用した内部不正の第一歩となり得ることから、これを禁止する[21]。

8.4.3 監査機能の充実

前章の「系統的モニタリング」の項において、組織の通常の指揮命令系統から独立した、「組織の監査」をミッションとする部署の設置とそのためのインフラ導入の必要性について述べたが、この部署の行う「監査」は、組織トップを始めとした幹部の行いについても厳正に適用される必要がある。組織トップや上級幹部といえども、「弱い存在」としての人である以上、監査の網から外してはならない。幹部就任時に監査ポリシーへの承諾を取り、書面への署名の形で残しておく。

監査という行為を人が行う限りにおいては、組織トップや、上級幹部の内部不正を、全くの利害関係のない第三者として、100% 追及し切るのは難しいことが多い。監査という「難しい職務」を、職務遂行者の感情を出来るだけ入れずに行うためには、「人による運用」だけではなく、IT による監視技術を導入し、システムによる自動的な監査支援も行えるようにする。

制度的観点、運用的観点、そして技術的観点の３つから、内部監査機能、外部監査機能、そして監査役（監査委員会）の機能を充実させ、内部不正の発生を早期に知り、是正出来るようにする。それと同時に、不正に際しては、毅然とした対応を取る体制を準備する。

監査機能の独立性は重要である。会社法[22]で「監査役会設置会社においては、監査役は、三人以上で、そのうち半数以上は、社外監査役でなければならない。」とされているように、実効性のある監査組織が必要である。

8.4.4 複数確認体制と不正リスク管理制度

金庫の施解錠や、組織の口座からの大口の出金・送金、重要ファイルにアクセスするなど、組織のオペレーションに大きな影響を与える内部不正が発生しやすい業務の遂行には、それを行う人間の職位によらず、複数の人間で対応・確認する等、特別な管理を行う。

どのような職位の人間に対しても、先に述べた「資格と必要性」の基準を公正に適用する。これが、内部不正につながる行為の判断を行う上での大元となる。

米国などで、職務内容、行動規範、職務権限などを明文化し、行動を常時モニタリングすることで、問題点を早期に発見、是正していくリスクマネジメントプラグラム [25] が導入され始めている。この種の手法に関しては、自らの組織できちんと機能するかを検討し、うまく機能する場合には組織全体での導入を推進するのが良い。

また、責任ある立場で、組織としての判断を行う立場にある幹部を、長期にわたって同じ職務に就かせないような人事異動を行ったり、定期的に長期休暇の取得を義務づけ、その間の職務を代行者に行わせたりする仕組みを構築することなども、不正の抑制や、その芽を長期潜伏させずに発見することにつながる。

組織における内部不正は部署、職位によらず発生するが、金銭の出入りを管理する部署、物品の購入を集中して担当する部署、商品の仕入れや販

[21] 宅配便で送達される等で、断ることが難しい贈答品に対しては、組織内でオークションを行って現金化し、収益を慈善団体等に寄付している組織もある。

[22] 会社法 335 条３項

売を担当する部署などでは、特に注意して管理する必要がある。

8.4.5 マスメディアへの対応

重要ポストについた人間が、意識しなければならないもの一つにマスメディアがある。「組織の顔」としてのマスメディアへの対応は、幹部の重要な役割の一つである。

マスメディアの向こうには、組織にとってその存続を左右するステークホルダーとしての顧客や株主、納税者などが存在する。マスメディアへの対応を誤ると、組織の行動が曲解され、評判を落とすことで組織のオペレーションに多大なる影響を及ぼすことがある。

組織が関わる何らかの事故が発生した際のマスメディアへの対応には特に注意を要する。事故とその内容発表の間には限られた時間しかない場合が多いため、許された時間で可能な限りの事実確認を行い、「確認された事実」と「未確認の事柄」を明確に分けた形で対応する。組織としての事後対応の正式な方針が未定の場合には、「決定次第正式にアナウンスする」旨を、時限を指定して伝えることが基本である。必要な場合には、誠実に陳謝し、誰の目からも謝意を表していることが判るようにする。

未確認事項と未決定事項に関してのコメントは避け、「事実」と「組織としての正式な方針」のみを、誠実に発表する。

対応の際には関係者の動線にも注意を払い、非公式なコメントが外部に出ないように配慮する。また、メディア各社に平等対応し、すべてのマスメディアに対し、同じ情報が同時に届くようにする[23]。明らかになった事実、及び組織としての正式な方針は、紙面でも配布すると同時に、プレスリリースとして、ネット上にも公開し、憶測情報を流布させない対応を行う。

8.5 退職時

組織で行われる多くの内部不正は、退職が決まった（もしくは決意した）従業員の手によってなされている。米国では、退職者の半数以上が、機密情報を持ち出しているとの報告 [26] もある。

定年退職、健康上の理由、私生活上の都合による退職を除く、従業員の意志による退職は、従業員がその組織で働くことに、相対的に魅力を感じなくなった時に発生する。従って、この段階に至った従業員が行う内部不正は、組織の求心力で防ぐことは難しい。また、退職を決めた従業員は、組織に対してネガティブな感情を持っていることも少なくなく、かつ組織の内部事情にも詳しい。そのため、内部不正防止という観点に立つと、退職を決心した従業員の扱いには、組織として細心の注意を払う必要がある。

8.5.1 迅速処理の実施

自己意志による退職は、大抵の場合、それを正式に申し出た段階で、すでにその意思が堅固である場合が多い。正式に退職の申し出があった場合、それを引き伸ばすことは、従業員に不信感を抱かせると共に、不正を行う時間と機会を与えることになる。

退職を申し出た従業員に対しては、面談等で直接その意志を再確認した後に、速やかに退職処理を行い、「円満退職」とするのが原則である。退職を申し出た従業員からは、組織内で担っていた役割を外し、業務の引継などに必要なものを除いて、その権限を制限する。

退職意思再確認のための面接では、その意志を確認すると共に、引継など、退職までに行う組織内でのアクションとそのスケジュールを確定する。

[23] 1 社にスクープを許すと、そこから取材合戦に発展することがある。これが組織のオペレーションに影響を及ぼす可能性は無視できない。

加えて、退職理由などのヒアリングと、組織内の役割を外すこと、権限を制限することなどの説示と確認を行う。

退職に至るまでのスケジュール確定は、当人に退職後の行動に関する展望を与え、その目を未来に向かせることにつながる。

また、ヒアリングで引き出した情報は、より本音に近い「想い」や、顕在化していない組織の問題情報が含まれることもあるため、内部不正を抑えるヒントとなり得る。

8.5.2 情報セキュリティ対策

従業員が退職するタイミングは、その従業員が、組織の情報の不正持ち出しを行うタイミングでもある。米国で行われた企業の IT 管理者を対象とした意識調査 [27] では、9 割の人間が「明日解雇されるなら、職場の機密情報を持ち出す」と回答した。組織としては、情報を持ち出す内部不正が、従業員が退職する際に最も起きやすいことを念頭におき、情報セキュリティ対策に細心の注意を払う必要がある。

この観点から、退職を申し出た従業員の、情報への不要なアクセス権は、速やかに制限する。また、記録された情報アクセスのログを基に、過去に遡って、どのような操作を行ったかの監査も行う。電子情報のみならず、紙に記載された情報にも注意し、重要書類は原則としてすべて回収する。

退職日まで、メールを使えるようにする場合でも、メールによる組織外への添付情報送信や、外部サーバーなどへのファイルアップロードなどが出来ないようにする。

さらに、PC での、外部媒体への書き込みを規制する、プリンタやコピー機、FAX などの OA 機器の使用を制限するなどの物理的対策も考えられる。加えて、退職予定者を組織内で独りにせず、常にその行動を周囲から見通せるようにする。

これらの物理的、IT 的対策以外にも、「退職意思の確認面接」の際に、職場内の情報の扱いを含めて再確認し、心理的に牽制することも必要である。

営業部門などで自らが開拓した営業人脈の情報や、研究開発部門などで自らが開発した技術やノウハウなどの情報は、その従業員自身が、自分に属する個人の資産と認識していることも少なくなく、それが、情報の持ち出しにつながることもあるため注意を要する。

8.5.3 貸与物の回収

鍵や各種アクセスコントロールシステムのカード、法人クレジットカード、従業員証（ID 証）、健康保険証、従業員バッジ、制服、業務用携帯電話、業務用 PC、顧客名簿など、在職中に組織から退職者に対して貸与したものは回収するのが原則である。

組織内で担っていた役割が外れた場合に必要のないものは、退職日を待たずに早期に回収する。鍵やカードは、それを持ったままの退職を許してしまうと、後々、犯罪のツールとして使われてしまうものであるため、特に注意して扱い、少なくとも退職日までには貸与した全ての鍵を回収しなければならない。制服や従業員バッジなども組織外に流出した場合、不正に使われることがあるため、注意して回収する。

紛失などの理由により、退職日までに、これらの貸与物を回収出来ない場合は、あらかじめ定めた紛失手続きを行う。

健康保険証は、身分証明書として広く社会で通用するため、組織退職後に保険加入を任意継続する場合は、不正や犯罪のツールにならないよう特に注意を促す。

8.5.4 コンプライアンス対応

退職に際し、退職者と組織の間で、お互いが納得のいく形での合意を形成して、退職者に組織に対しての不満や不信感を抱かせないようにすることが基本である。加えて、退職者に、退職後も自

らに課せられる義務を意識させ、組織に対して不利な行動をとらないという合理的な行動を促す。

退職に際しては、関連法規を遵守し、各種社会保険、退職金の処理と説明を速やかに行って、退職者、及び組織に残る他の従業員が、組織に対して不安や不信感を抱かないように配慮する。

未払い賃金や手当金などがある場合には、速やかにこれを支払う。未消化の法定有給休暇の扱いについても検討し、あらかじめ規定を定めておく。

在職中の発明、考案や著作などの知財に関する扱いについても、関連法規などを遵守する形で原則的な扱いを定めて、退職者と組織との間で合意を形成し、覚え書きを取り交わしておく。

組織がこれまでに提供した賃金以外の便益や、貸付金、社宅や寮などの住居についての退職後の扱いについても、規定をあらかじめ定めておくと共に、退職に際して、その運用に関して改めて合意を形成しておく。住居については、話し合いによって、人道的観点も考慮に入れて適切な対応を行う。

加えて、守秘義務や競業避止義務などの、退職後も課せられる義務や、関連法規の説明も行って、退職者、組織の双方が納得できる誠実な対応を行う。

8.5.5 退職後の関係維持

退職者が、将来的に、顧客や取引先としてその組織にとってのステークホルダーになり得ることを考慮に入れて誠実に対応する。退職時に公式、非公式に送別会、壮行会を行ったり、感謝状や記念品を贈ったりすることにも意味がある。「退職者の会」を組織し、退職後も連絡先のメンテナンスを行うのが望ましい。会報を送ったり、定期的に懇親会を開いたりすることは、連絡先のメンテナンスや、退職後の組織との関係維持に有効である。

一方で、退職者は、退職後には組織外の人間となることに注意を要する。組織に対して良い感情を持たずに辞めた人間がいることも考慮に入れ、過去に世話になった人間であっても安易に組織内部に入れることには注意が必要である。

9. おわりに

これまで、ほとんど公開されていないものの、組織の多くでおそらくはかなり常態的に発生しているであろう内部不正や、ヒューマンエラーによる悪意や他意のないミスは、組織のオペレーションを内側から蝕む「組織の生活習慣病」とでも呼ぶべきものである。「組織の生活習慣病」を予防したり、治療したりするには、投薬や手術などに相当する「内科的治療」や「外科的処置」に留まらず、「組織の生活習慣」を改める必要がある。これは「人間の生活習慣病」の場合と同じである。

「組織を回しているのが人である」以上、「組織の生活習慣」を変化させるには、組織で働く人々の意識を変え、行動を、ひいては従業員一人ひとりの考え方と習慣を改めさせる必要がある。

本稿においては、先に提案したセキュリティの定義をベースとして、「状況的犯罪予防論」「組織の文化論」の双方の観点から、内部不正やミスを抑制するための組織のあり方、そしてそこに至る具体的方法論を示した。

本稿で示した手法が、内部不正やミスなどの組織における内部要因事故抑制の一助となり、ひいては産業界がさらに発展するためのきっかけとなれば幸いである。

参考文献

[1] Yasufumi AMARI: The Fundamental Definition of Security, Proc. BUEE2008 (The 9th International Symposium on Building and Urban Environmental Engineering), pp.203-207, Hong Kong (2008)
[2] 甘利康文 : セキュリティの上位概念的考え方について、信学技報、Vol.105, No.687, pp.5-8 (2006)
[3] 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不正 / ミスの抑制手法、日本セキュリティ・マネジメント学会 第 24 回全国大会発表要旨 , pp41-42 (2010)
[4] Yasufumi Amari: How to Control Employee Fraud and Human Error Using the Basic Concept of Security, The Book of Abstracts, 16th World Congress of the International Society for Criminology, p.189, Kobe (2010)
[5] [独] 情報処理推進機構：情報漏えいインシデント対応方策に関する調査報告書 http://www.ipa.go.jp/security/awareness/johorouei/report.pdf (2007)
[6] Kathy Grannis: Troubled Economy Increases Shoplifting Rates', National Retail Federation (USA) Website, http://www.nrf.com/modules.php?name=News&op=viewlive&sp_id=746 (2009)
[7] 日本セキュリティ・マネジメント学会（編）：セキュリティハンドブックⅠ～Ⅲ、日科技連 (1998) など
[8] S．ケイシー：事故はこうして始まった！ ヒューマン・エラーの恐怖 (赤松幹之 訳)、科学同人 (1995) など
[9] 中田 亨：「事務ミス」をナメるな！、光文社 (2011)
[10] 片倉もとこ：イスラームの日常世界 , 岩波書店 (1991)
[11] 内田勝也：情報セキュリティの現場で起きている「教育不足」本当の「専門家」に求められているのは、本質を理解する力、日経 BP 社 Safety Japan、http://www.nikkeibp.co.jp/sj/2/interview/37/ (2005)
[12] Martha J. Smith and Derek Cornish, eds.: Theory for Practice in Situational Crime Prevention (Crime Prevention Studies, vol. 16), Criminal Justice Press, http://www.popcenter.org/library/crimeprevention/volume_16/ (2003)
[13] 内田勝也：情報セキュリティへの状況的犯罪防止論の適用 http://www.uchidak.com/InfoSecPsycho/20100922_uchidak01.pdf (2010)
[14] Donald R. Cressey: Other people's money a study in the social psychology of embezzlement, Free Press (1951)
[15] Lawrence E. Cohen and Marcus Felson: Social Change and Crime Rate Trends: A Routine Activity Approach, American Sociological Review, Vol.44, pp.588-605 (1979), (and "A Theory of Crime Problems", http://www.popcenter.org/learning/pam/help/theory.cfm)
[16] 原田 豊 : 子どもの被害の測定と防犯活動の実証的基盤の確立、社会技術研究開発事業 平成 21 年度研究開発実施報告書 (2010), http://www.ristex.jst.go.jp/examin/criminal/pdf/H21_harada_houkokusho.pdf
[17] 内田勝也：情報セキュリティ心理学について、http://www.uchidak.com/InfoSecPsycho/20100922_uchidak00.pdf (2010)
[18] George L. Kelling, Catherine M. Coles: "Fixing Broken Windows", Simon & Schuster (1997)
[19] Derek B. Cornish and Ronald V. Clarke: 'Opportunities, Precipitators and Criminal Decisions: A Reply to Wortley's Critique of Situational Crime Prevention' (2003), http://www.popcenter.org/Responses/crime_prevention/PDFs/Cornish&Clarke.pdf
[20] Situational Crime Prevention, http://www.popcenter.org/25techniques/
[21] Robert W. White: Motivation Reconsidered: The Concept of Competence, Psychological Review, Vol.66, No.5, pp.297-333 (1959)
[22] Kevin D. Mitnick et al.: The art of deception: controlling the human element of security, Wiley (2002)
[23] Richard M. Ryan and Edward L. Deci: Self-Determination Theory and the Facilitation of Intrinsic Motivation, Social Development, and Well-Being., American Psychologist, Vol. 55, No. 1, pp.68-78 (2000)
[24] Edward L. Deci and Richard Flaste: Why We Do What We Do: The Dynamics of Personal Autonomy, G..P. Putnam's Sons, New York (1995) [桜井茂男訳 : 人を伸ばす力　～内発と自律のすすめ～ , 新曜社 (1999)]
[25] 不正リスク管理実務ガイド検討委員会、八田 進二 編：企業不正防止対策ガイド、日本公認会計士協会出版局 (2009)
[26] Symantec and the Ponemon Institute Press Release: More Than Half of Ex-Employees Admit to Stealing Company Data According to New Study, http://www.symantec.com/about/news/release/article.jsp?prid=20090223_01 (2009)
[27] Cyber-Arc Software: IT Savvy Employees Likely to Steal Company Data Before They Leave (2008), http://www.cyber-ark.com/news-events/pr_20080827.asp

(注 参照 URL は、2012 年 1 月中旬 現在)

サイバー攻撃の脅威とセキュリティ対策

株式会社アイ・ティ・フロンティア
長久　浩三

はじめに

昨年は、政府機関や防衛産業などの企業がサイバー攻撃の被害を受け、日本中に警鐘を鳴らした年になったと言える。かつての、パソコンにウイルスを感染させて驚かせるようなイタズラや技術自慢などの愉快犯とは違い、社会的主張や利益を得るために、ターゲットを定めて、必要とする情報を盗む、あるいはシステムの制御を奪い被害を与えるなど、目的も大きく変わってきている。急速に進化する情報技術に合わせてセキュリティの脅威も進化しているのだ。この脅威から大切な情報やシステムを守るためには、サイバー攻撃の危険性を認識し、対策も進化させて行かなくてはならない。こうした状況で、私は自社の情報セキュリティを担当する立場から、既存の対策を改めて見直す必要があった。そのため、専門家の方々の意見やさまざまな情報機関から、脅威と攻撃の手口に関する情報を収集し、具体的な対策について研究を行った。その成果として、サイバー攻撃の脅威とセキュリティ対策について以下の通りまとめてみた。

1. サイバー攻撃の脅威と危険性

サイバー攻撃は、大きく2種類に分類できる。

一つはターゲットを特定せず、迷惑メールやセキュリティホールを悪用するウイルスなどを無差別に送りつけて、組織や個人に混乱をもたらす古典的なもの。

もう一つは、組織や個人にターゲットを絞り、あらゆる手段を用いて目的の情報を盗む、サービス機能を失わせる（DDoS攻撃）、システムの制御を奪ったりするものである。

後者が標的型攻撃と呼ばれ、2010年以降は「APT（Advanced Persistent Threat）攻撃」という言葉も使われている。APT攻撃の例として、2009年12月にGoogleをはじめとする複数の企業に被害を及ぼした「オーロラ攻撃」がある。ゼロデイアタックの手法によってIE（InternetExplorer）の脆弱性を利用し、知的財産やGmailアカウントを盗むなどの大きな被害を発生させた。

APT攻撃は情報を盗むだけではなく、スタックスネット（Stuxnet）と呼ばれる制御系システムを攻撃した例もある。手口はコンピュータに接続するUSBメモリによって感染を広げ、目的のシステムの制御を奪うというものだ。攻撃にはWindowsのショートカットファイルに存在する脆弱性を悪用しており、ショートカットファイルのアイコンを表示するだけで、任意のプログラムが実行される。

2010年9月に、イランの核燃料施設のウラン濃縮用遠心分離機が標的にされ、この攻撃で約8400台の遠心分離機の全てが稼働不能に陥ったとのニュースもある。また、このような攻撃に使われたソフトウェアは、ブラックマーケットで流通していると言われ、一般企業や個人を対象にした攻撃に広がる恐れもあり警戒が必要である。

制御系システムを狙った攻撃は、日本国内でも起きている。自動車や化学工場の製造ラインを管理する制御システムがウイルスに感染し、操業停止に追い込まれるなどの深刻な被害が、昨年3月までに少なくとも10件発生していることが経済産業省の調査で分かった。今やソフトウェアは、自動車、航空機、列車などの交通機関、水道、電気、ガスなどのライフラインを動かす殆どのシステムに使われており、制御系のシステムを狙った攻撃は、我々の生活や生命を脅かすほど危険性が高いことを認識する必要がある。

2. 標的型攻撃の手口

被害に遭わない為にも手口を認識しておく必要がある。近年の標的型攻撃は主に次のような手法が使われる。

（1）攻撃手法

①初期潜入段階

メールやUSBメモリ、Webサイトの閲覧を通じ

てウイルスに感染させる。
②攻撃基盤構築段階
浸入したPC内でバックドアを作成し、外部のC&Cサーバ（バックドアをコントロールする指令サーバ）と通信を行い、新たなウイルスをダウンロードする。
③システム調査段階
ターゲットの情報やシステムに関わる情報を調査・取得する。
④攻撃最終目的の遂行段階
調査した情報を基に攻撃専用のウイルスをダウンロードして攻撃を遂行し、ターゲットの情報を盗む、またはシステムの制御を奪う。

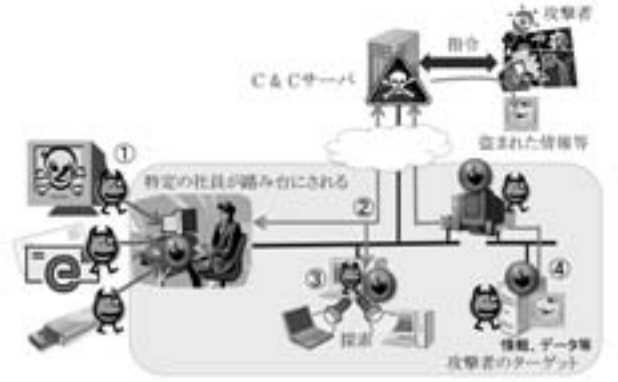


図 1 標的型攻撃の手法

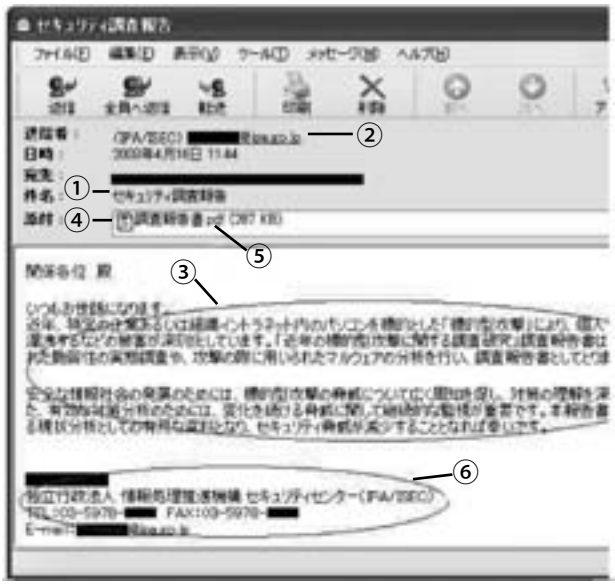
(3) 人の心理の弱点を突くメールなどの手口

これは一般的にソーシャルエンジニアリングとよばれ、人の心の隙間やミスにつけ
込むもので、例えば、ゴミ箱の紙屑などから攻撃の糸口を見つけ、ありとあらゆる
手段を使い情報を盗むなどの方法である。

メールは知人の名前を名乗り、内容もごく日常的なもので送られてくる。見分けるのは難しいが、これまで公開されているケースを見ると、内容はやや唐突感があり、添付ファイルやURLを開くよう誘導する文章が書かれている。不自然な気がしたら、安易に添付ファイルやURLをリクックせずに、電話で送信者に確認するなど、慎重な対応が必要である。

【ウェブ等で公表されている情報を加工して使用した事例】

IPA（独立行政法人情報処理推進機構）の「標的型攻撃メールの分析に関するレポート」から、「メール受信者をだますテクニック」の一部を紹介する。
① メールの受信者が興味を持つと思われる件名
② 送信者のメールアドレスが信頼できそうな組織のアドレス
③ 件名に関わる本文
④ 本文の内容に合った添付ファイル名
⑤ 添付ファイルがワード文書やPDF ファイルなど
⑥ ②に対応した組織名や個人名などを含む署名



引用：IPA「標的型攻撃メールの分析に関するレポート」

図2　IPA をかたって政府関係組織に送られたメール

【標的型攻撃メールの記載内容の傾向】

メールの内容は、受信者が興味を持ちそうな仕事関係のテーマが多い。例えば「研修会」「会議資料」「情報セキュリティの注意喚起」など、標的に合わせて使い分けられている。

分類	割合	テーマ事例（抽象化済）
イベント	38%	国際会議、シンポジウム、研修会、選挙、法令改正、VIP会合日程、役員人事異動、来訪者情報、社内ウイルス調査
報告書	32%	外交機密文書、国際情勢、海外資源、政府部局報告書、情報セキュリティ調査、ウイルス・不正アクセス届出状況、会議資料
ニュース・注意喚起	30%	東日本大震災、金融情勢、国際情勢、外交情報、政府予算、製品事故、情報セキュリティ注意喚起、新型インフルエンザ

表1　テーマによる分類

引用：IPA「標的型攻撃メールの分析に関するレポート」

(4) 攻撃の手口は進化する

攻撃者は潜入手口を進化させている。新たな手口ではメールにファイルは添付されておらず、Webサイトを案内するURLが添付されており、正規のWebサイトだと思って見ているうちにマルウェアに感染させるような、高度な隠蔽技術が使われる。裏では正規のWebサイトが複数改ざんされ、複数のサーバが乗っ取られて踏み台に使われる。Webアプリの開発担当者やサーバの構築担当者、運用担当者は、脆弱性対策を徹底するだけでなく対策を進化させて行く必要がある。

3. 中国からの攻撃に国際社会では警戒を強めている

中国では複数のグループで形成された「紅客連盟」というハッカー集団が存在する。また、中国政府は人民解放軍所属のハッカー部隊を保有しており、アメリカと中国近隣諸国ではサイバーテロの警戒を強めている。

図3の円グラフは、メールヘッダに記録されたIPアドレスを国別に集計したものである。約1/3が中国で管理するIPアドレスからのものだ。なお、不明の35%は、メールヘッダを入手できなかったものである。

アメリカ国防総省は、昨年5月「外国政府からのサイバー攻撃を『戦争行為』とみなし、サイバー攻撃を受けた際は武力行使も辞さない」と発表した。サイバー空間を陸、海、空、宇宙空間に次ぐ第5の新たな戦場と宣言し「サイバーコマンド」という部隊を創設し本格的な運用を開始している。台湾と中国では経済交流は進んでいるが、水面下では激しい攻防が行われており、台湾はサイバー部隊「老虎部隊」を設立し、中国をはじめとする海外からの攻撃に備えている。サイバー攻撃は、今や世界各国で深刻な問題として取り上げられており、多くの国で対策が進められている。

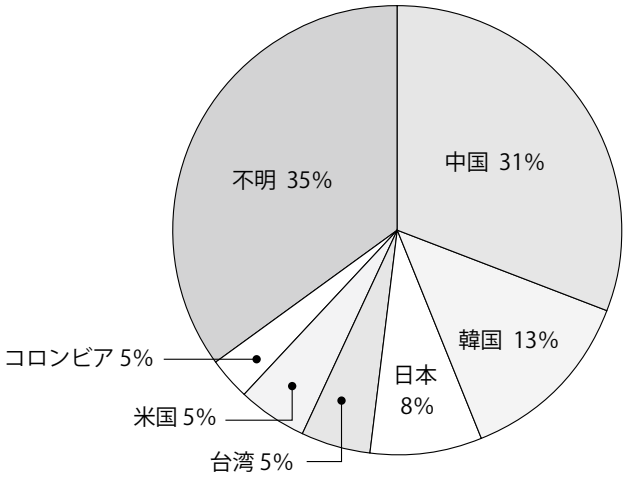


図3　標的型攻撃メール発信 IP アドレスの国別内訳

引用：IPA「標的型攻撃メールの分析に関するレポート」

4. 日本のサイバー攻撃への取り組み

政府は三菱重工業などへのサイバー攻撃をきっかけに、昨年10月に情報セキュリティ政策会議を開催し、政府と経済界を中心に官民が連携してサイバー攻撃の被害防止に取り組むことを決めた。今年1月には、各府省庁にCSIRT（情報セキュリティに即座に対応する組織）の保有を求めるとともに、国の最高情報セキュリティ責任者（CISO）を設置する方針を決めている。

また、今年1月1日の読売新聞で「防衛省が対サイバー兵器を開発」という記事が一面を飾った。防衛省がサイバー攻撃を受けた際に、攻撃経路を逆探知して攻撃元を突き止め、攻撃者のプログラムを無効化するというものだ。

しかし、日本では有事法制でサイバー攻撃が想定されておらず、サイバー兵器を対外的に使用できないばかりか、使用すると逆に刑法のウイルス作成罪などに抵触する可能性もある。また、こういった兵器や活動は、防衛省の自前のシステムを守るためのものであり、国民の生命と財産を守ることは想定されていない。従って、日本ではサイバー攻撃に対しては、自ら守るしかないのが実情だ。政府の一刻も早い法的整備と対策が望まれる。

5. サイバー攻撃への対策

対策は技術的なものだけでなく、組織的、人的といった多重防御で考えることが効果的である。これまでのセキュリティ対策の経験や専門家の意見、IPAなどの情報を基に、取り組むべき対策を以下の7点に纏めた。

(1) 従来の入口対策を見直す

既存の対策を見直し、入口で何を防ぎ、出口で何を防ぐかを考えて、ネットワークを設計することが重要である。そのため、メールゲートウェイやフィルタリング機能を見直す。Webアプリケーションの運用があれば、WAFを適用するなどを検討する。また、以下のようなフィルタリングやスパムメール、マルウェア対策機能を搭載したソリューションを利用するのも有効である。

a. 送られてきたメールの中身を分析し、送信元サーバのIPアドレスや送信者のドメインが悪意のあるものでないか評価する。
b. メールに添付されたファイル名の偽造をチェックしたり、ファイルの中身を解析して実行ファイルが含まれていないか調べる。
c. メールに記載されたURLが安全なサイトかを調べ、スパムメールかを判断し、一定の安全性をクリアーしたものだけを中に入れる。

(2) 出口対策を加える

ウイルスがLAN内に入り込んだ際の動きに注目し、その活動を最小限に抑え、万一浸入されても、情報を外に持ち出させないことがポイントである。

a. 内部プロキシ経由の外向け通信のみ許可し、プロキシを使わない端末からの直接通信を遮断する。
b. システムプロキシにJAVAスクリプトやMETAタグを利用したリダイレクト機能を実装し、リダイレクトに対する応答でウイルス通信を遮断する。
c. ネットワークをVLANなどで細分化し、ウイルスの感染範囲を狭める。
d. LAN内の通信を監視し、普段使われていないサービスの通信が発生したときはその原因を追究する。

(3) 監視の強化と発見時の対応手順を整備する

攻撃者がネットワークに侵入するためには、ターゲットに対して何度もアタックを繰り返す。そのため、普段からファイヤーウォールのログなどを監視し、不審な動きを捉えるようにする。また、不正アクセスやウイルス感染が発覚した際に、何をどうするのか手順を整備し、定期的に訓練を行っておく。

(4) 脆弱性対策を徹底する

攻撃の手口はさまざまだが、脆弱性対策の遅れや放置によって被害を受けた例をよく聞く。従って、いかに脆弱対策を徹底できるかが対策のカギを握る。

a. OSの適正なバッチ適用やウイルス対策ソフトを最新版にする。
b. AdobeやJava、Microsoftなどのアプリケーションソフトの脆弱性対策を徹底する。

c. 徹底するには、利用者から状況報告させ責任者がチェックするといった人間系の人的な対策も有効である。
d. パスワードの脆弱性対策として、パスワードは3種類の文字で8桁以上で類推しにくいものにし、定期的に変更するなどの運用を行う。
e. Webアプリケーションは、設計、開発、テストの各フェーズで脆弱性のチェックを行う。また、ツールなどで脆弱性診断を行うことも有効である。
f. Webサーバに対しては、セキュリティベンダーの脆弱性診断などを活用すると効果的である。
g. オープンソースを使用する場合は、サポートを受けられないケースが多いため、積極的に脆弱性情報を収集し必要な対策を取る。また、ソースは初期設定のままで使用しないことも重要である。
h. プログラムを台帳で管理し、脆弱なプログラムが見つかったら、ただちに影響範囲を特定し対応できるようにする。

(5) サーバを集約する

サーバの設置場所やシステム環境が異なるとセキュリティ対策のバラツキが起き、攻撃を受けた際の影響範囲の特定や対策を取ることが難しくなる場合がある。そのため、出来る限りサーバを集約したほうが監視や対策が容易になる。ただし、集約したことによるリスクもあるのでアセスメントを行うことが重要である。

(6) 重要情報を峻別する

自社にとって価値の高い情報資産は何か、守るべき情報は何処に有るのかを明確にする。重要な情報資産は、単純にWindowsのフォルダーに保管するのではなく、認証機能のある、文書管理ツールなどを使って管理するとよい。また、インターネットからの接続が無い場所に置くことも効果的である。さらに、利用者を限定するなどアクセス権限の管理も必要である。

(7) セキュリティ教育・意識啓発

攻撃者は、人の心の隙間や心理的な弱さを突いてくる。怪しいメールが届いたら添付ファイルやURLを簡単にクリックしない、業務に関係ないWebサイトを閲覧しないよう行動を正すなど、普段から意識を高めておくことが重要である。そのためにサイバー攻撃による危険性の理解、基本動作が出来るよう定期的な教育や確認テスト、掲示板などによる注意喚起、視覚に訴えるポスター掲示、自律的なセキュリティ活動に対する経営の評価など、意識が向上する活動を取り入れることが効果的である。

おわりに

今後も、サイバー空間を舞台にした不正行為は、さらに激しくなると予想される。特にモバイル端末への攻撃は、Androidの脆弱性を狙う攻撃が増える可能性が高い。モバイル端末のドライブバイ攻撃やモバイルボットネットが出現する可能性もある。さらに、水道、電気、ガスなど、日常生活に欠かせない産業システムへの脅威にも警戒が必要だ。また、世界的な経済不安から、標的は情報だけでなく金銭を目当てにする攻撃も増えてくると思われる。人の心理的な部分を突くよう、攻撃の手口はますます巧みになるだろう。脆弱性対策を怠ったり安易な行動は、自分だけでなく多くの人に被害を及ぼすことになる。サイバー攻撃を対岸の火事だと考えず、誰もが目の前にある脅威として認識することが重要である。そのためにも、日々の基本動作を確実にして、危機回避できるよう感度を高めて、対策に取り組むべきである。

JNSA ワーキンググループ紹介

SNS-WG

日本マイクロソフト株式会社
WG リーダー　高橋　正和

SNS-WG は、2011 年 10 月に発足、現在 20 名ほどのメンバーで運営している。すでに WG を 3 回開催した他、Facebook のクローズドグループを使った活発な意見交換を行っている。また、SNS は、社会的な関心も高く、既に WG メンバーによる SNS のセキュリティに関する講演も行っている。

■ 発足の背景

SNS は、利点も多いがリスクもある。私は、mixi を業務とは関係のない分野の交流に利用しているが、つい最近までは、Facebook のような実名主義の SNS は、時刻を伴った位置情報、知人関係、家族や趣味といった個人的なことの記録と公開による、リスクが高いと考えて使用を控えていた。

しかし、SNS の普及が進むに従って、セキュリティやプライバシーについて質問を受けるようになったのだが、本質的な理解をしていないため、自信を持って答えることができない。加えて WASAF（Web Application Security Forum）、INTEROP、INTERWEB 等、様々な活動にかかわる中で、SNS を含めた現在の技術や利用法を理解していないと感じるようになった。

やはり、新しい技術・利用方法は、昔の知識の延長線上では対応できないと考え、改めて取り組んでみることにした。せっかくなので、一人でやるよりも、WG で知恵を合わせた方が、よりしっかりしたアウトプットも出せると考え、SNS-WG を立ち上げることにした。

■ SNS とは

SNS = Social Network Service は、思ったよりも幅の広い概念で、さまざまなサービスが SNS に分類されている。有名なところでは、mixi、Twitter、Facebook、Google+、Linkedin 等がある。また、ゲームをベースとした SNS として、Gree やモバゲーなど、そして YouTube、USTREAM、ニコニコ動画等の動画サイトも、SNS に含める場合が少なくない。面白いことに、Facebook 上のゲーム Zynga が Facebook よりも収益を上げるなど、SNS 上に独自の経済圏ができている。

SNS 普及には、技術的な発展と、社会的な変化が背景となっている。現代は価値観やライフスタイルの多様化が進み、社会として共通の価値観を持つことが難しい。この多様な個性が、それぞれの価値観を共有する場を見つける手段として、SNS が進んでいる面がある。

SNS は、利用者の広がりに伴って、広告を中心としたビジネスプラットフォームとしても注目されている。そして、アルビン・トフラーが第三の波で書いている「プロシュマー」に相当するような、積極的にビジネスにかかわる利用者も目立つようになった。

SNS は、広告の分野で、ポータルサイト、検索エンジンに続く、三番目の広告の手法と位置付けられている。

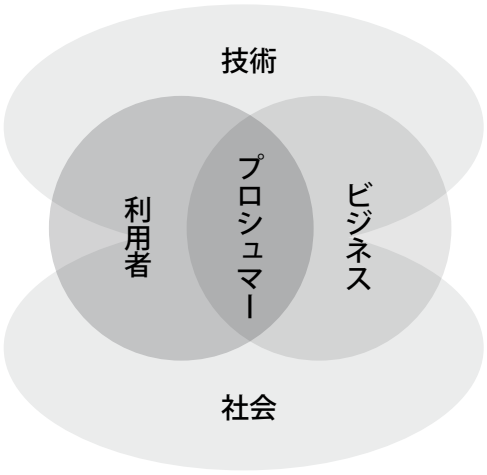
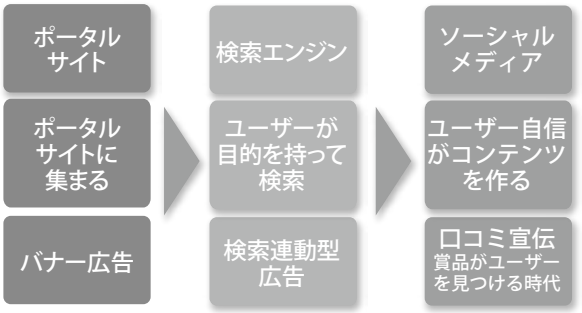


図 1　SNS を取り巻く環境

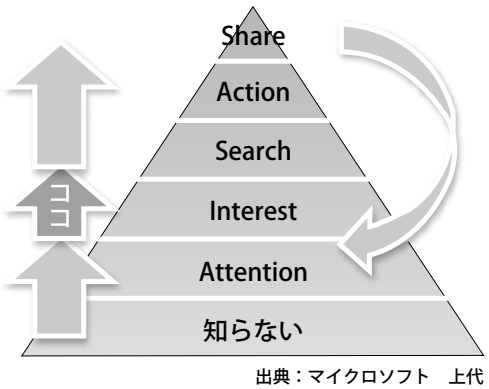
JNSA ワーキンググループ紹介



出典：ソーシャルネットワーク革命がみるみるわかる本

図２　インターネットの広告手法

しかし、すべてのオンライン広告が、SNS に移行するわけではないと考えられている。第 3 回 WG における日本マイクロソフトの上代氏の講演によれば、SNS は、主に AISAS モデル上の Interest、Share と各フェーズへのフィードバックに効果があるとしている。マーケティング 3.0 と呼ばれる SNS の消費者間の情報交換に注目した、新しいマーケティング理論も注目されていることから、SNS が果たす役割は、さらに広がっていく可能性が高い。



出典：マイクロソフト　上代

図３　SNS 広告の位置づけ

■ SNS の課題：セキュリティとプライバシー

NSF 2012 の SNS-WG のセッションでも議論したように、課題の整理はまだ途上であり、構造的に捉えるには至っていない。ワーキングメンバーの日本 IBM 守屋氏は SNS における課題を図 4 のように整理している。

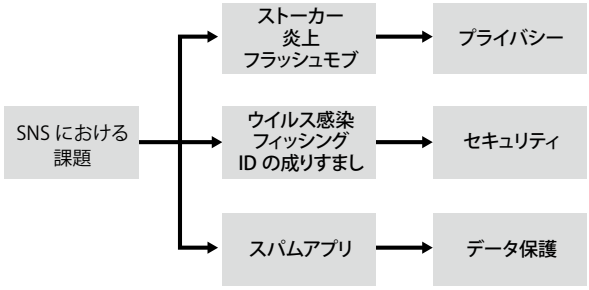


図４　SNS における課題

SNS では、セキュリティよりもプライバシーに関する懸念が高く、さらに、ストーカー被害などの現実社会での危険につながることも懸念されている。

図 5 は、Facebook がデフォルトで公開する情報の推移で、より多くの情報を公開する方向に推移している事がわかる。この変化は、これまで非公開であったデータが、突然、公開されてしいまうという問題も内在している。

■ SNS-WG の活動

SNS のセキュリティは、まだ課題のフレームワークも不明瞭な状態にあると考えている。SNS-WG ではメンバー間で Facebook 上でのディスカッションを中心に、有識者による講演などを通じて、SNS のセキュリティに対する理解を深めて行こうとしており、これをガイドラインなどの形で公開していく予定である

興味を持っていただいた方は、ぜひ、WG メンバーとして参加して頂きたい。

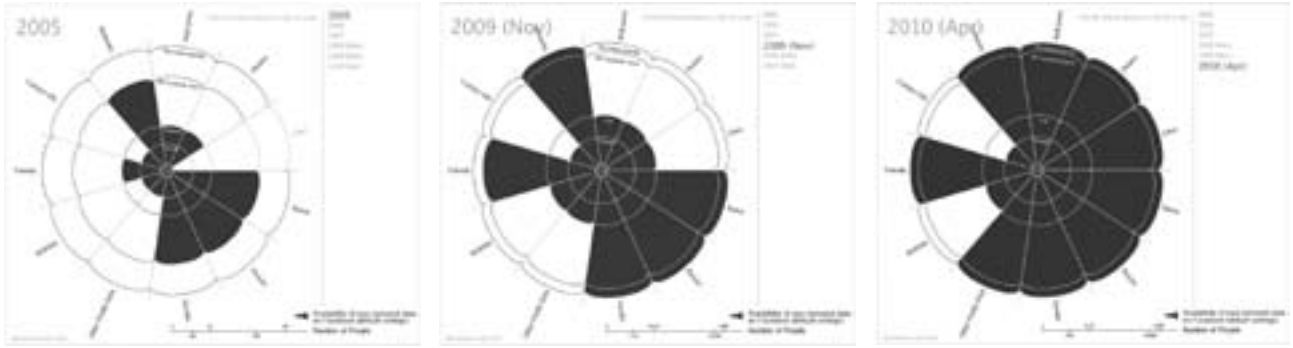


図 5　Facebook のデフォルトでの公開情報の推移

出典：The Evolution of Privacy on Facebook　http://www.mattmckeon.com/facebook-privacy

2 月 29 日 SNS と法律勉強会の風景

会員企業ご紹介㉝

SCSK 株式会社

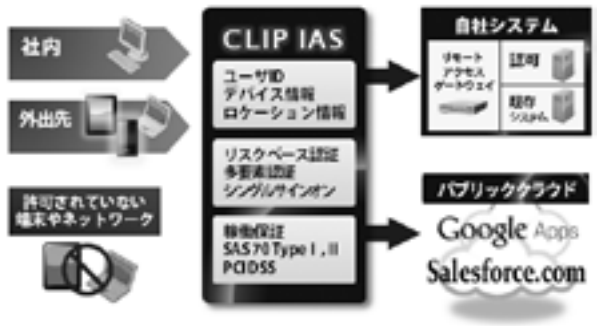
http://www.scsk.jp/

SCSK株式会社は、2011年10月に住商情報システム株式会社と株式会社ＣＳＫが合併し誕生しました。
両社の各産業分野における技術力・ノウハウ・知財などを相互に活用するとともに、システム開発、ITインフラ構築、ITマネジメント、BPO（ビジネス・プロセス・アウトソーシング）、ITハード・ソフト販売を有機的に統合することで、フルラインナップのサービスをご提供いたします。
また、住友商事をはじめとするお客様の世界各国におけるITシステム・ネットワークのサポート実績を活かし、グローバルITサービスカンパニーとして、さらなる飛躍を目指してまいります。

クラウド型統合認証サービス CLIP IAS

CLIP IASの多要素認証

解読プロセスを困難にした独自の暗号化技術で保護された暗号鍵やワンタイムパスワード、秘密の質問で、ID/パスワードのみの認証を強化します。



リスクベース認証

アクセスした利用者の【ID/パスワード】【デバイス情報】【ロケーション情報】から、不正アクセスのリスク度が高いと判断された場合、追加の認証やアクセス拒否をし、不正アクセスを防ぎます。ID/パスワードがたとえ合っていた場合でも、不審なアクセスを防止します。

スマートフォン、クラウドをもっと安全に

◆スマートフォン/タブレット端末対応
◆主要クラウドサービスに標準対応
（Google Apps、Salesforce.com）

既存システムのリモートアクセスに

◆オンプレミス型システムの認証強化
◆SSL/VPNの認証連携

管理負担とコストを低減

◆メンテナンス不要
◆サーバ、ハードウェアトークン不要

信頼性の高いクラウドサーバよりサービス提供

◆稼働保証あり
◆SAS 70Type Ⅰ Ⅱ
◆PCI DSS

CLIP IAS　検索

メール誤送信防止サービス PlayBackMail Online

今すぐ始められる
クラウド型 メール誤送信防止対策

◆主要メールサーバ対応
（Google Apps, Office365, Exchange Server, Sendmail 等）
◆クライアントへのアプリケーション導入不要
◆月額150円/ユーザ

■販売代理店募集中■

PlayBackMail　検索

PC不正操作リアルタイム防止・ログ監査ソリューション 情報漏えい対策 モニタリング・サービス

内部脅威から情報を守る
月額利用型 情報漏えい対策

◆端末監視による「不正な操作の検知と防止」
◆ログ分析による「不審な操作の把握と原因追究」
◆英語・中国語対応

情報漏えい　モニタリング　検索

お問い合わせ先
SCSK 株式会社
IT エンジニアリング事業部　新規事業開発室
〒135-8110 東京都江東区豊洲 3-2-20 豊洲フロント
03-5859-3294　gapps-info@ml.scsk.jp

NRI セキュアテクノロジーズ株式会社

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

情報セキュリティ課題のワン・ストップ解決企業。それが私たちNRIセキュアです。

情報セキュリティの維持・向上によるリスク削減は、重要な経営課題となっていますが、単なる技術の導入だけでは解決しません。NRIセキュアは、テクノロジーとマネジメントの両輪で、情報セキュリティの課題をワン・ストップで解決します。

■セキュリティ・コンサルティング

セキュリティ・ポリシーや各種ルール・ガイドラインの策定、システムや情報セキュリティ・マネジメントの監査・評価、対策の実行支援、PCI DSS準拠支援など、情報セキュリティ管理に必要な施策をトータルにサポートするコンサルティングサービスを提供します。

■セキュリティ診断

高度化・多様化するWebサイトへのサイバー攻撃や、重大なセキュリティ事故が頻発するなか、NRIセキュアでは高度なスキルやノウハウを持つコンサルタントが、実際と同様の疑似攻撃を行うことにより、ツールでは検知しにくい脆弱性を発見します。また、過去の診断結果との比較評価や問題点への推奨対策を含む詳細な報告書、報告会、無料の再診断により、お客さまのセキュリティ維持・向上を強力に支援します。

[メニュー] Webアプリケーション診断、プラットフォーム診断、データベース診断、スマートフォンアプリケーション診断、無線LAN診断、ソースコード診断、PCI DSS ASVによる脆弱性スキャン

■マネージドセキュリティサービス「FNCサービス」

FNCサービスは、ITセキュリティのプロフェッショナルがお客様の立場に立って、セキュアなネットワークの設計、構築、運用までを行うフルアウトソーシングサービスです。ベンダーフリーの立場で、お客様にとっての全体最適を重視したベストプラクティスをご提供します。ハード、ソフト、運用管理、セキュリティ監視等において、所有からサービス利用型にすることで、コストや人的負荷を大幅に軽減可能です。

また、WAFやDBファイアウォール、次世代ファイアウォール、DLP、MDM、リモートアクセス環境などに関わる製品やサービスもピンポイントでご提供可能です。

■セキュリティ人材育成・研修

NRIセキュアオリジナルの研修や、米国SANS Instituteとの提携によるグローバルスタンダードなカリキュラムをご用意しています。セキュリティ関連業務に携わる技術者のスキルアップや、セキュリティ戦略を策定・推進できる管理者の養成を通じて、組織におけるセキュリティ文化の醸成・確立を目指していきます。

■セキュアファイル交換サービス「クリプト便」

インターネットを介した電子ファイルのやり取りを、安全に実現するファイル交換サービスです。SSL通信のほか、送信ファイルはNRIセキュアのFNC（ファイアウォールネットワークセンター）で24時間・365日体制で監視・保護されているだけでなく、AESで暗号化されており、厳重に守られています。情報セキュリティ格付け「AAAis」を取得しており、その安全性は高く評価されています。

ASP/SaaSのため、自社管理のサーバやPCにソフトをインストールする必要はなく、全社導入も簡単です。また、APIを自社システムに組み込んで、より業務を高速化・最適化している事例も増えています。

クリプト便

AAAis I.S.Rating 10000080106C1101

■セキュリティ管理ソリューション「SecureCube」シリーズ

組織内のセキュリティを維持・向上するための幅広いソリューションで、お客様の環境でのセキュリティ対策を強力に支援します。

- SecureCube / Central　セキュリティ GRC ソリューション
- SecureCube / Access Check　エージェントレス型特権 ID 管理ソリューション
- SecureCube / Labeling　情報資産の識別・整理ソリューション
- SecureCube / Mail Adviser　メール誤送信防止ソリューション
- SecureCube / Secret Share　秘密分散技術を活用したオンラインストレージサービス

☞世界各地のクラウドにデータを分散保管する「世界分散ストレージサービス」も提供

SecureCube

お問い合わせ先

NRI セキュアテクノロジーズ株式会社

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

TEL：03-6274-1011

E-Mail：info@nri-secure.co.jp

ZTE ジャパン株式会社

http://www.zte.co.jp

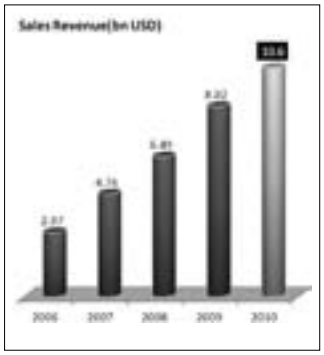
ZTE中兴

ZTEは通信機器とネットワーク・ソリューションの世界的なリーディング・プロバイダーです。世界に7万人以上の社員を擁し、140ヵ国、500社以上の通信事業者に、革新的な製品とお客様のニーズにあったカスタムメイドのサービスを提供しています。通信機器業界で近年最も飛躍的な発展を遂げている会社の1社です。

ZTEとは?

ZTE は 1985 年香港に隣接する中国深圳市に、現会長である侯為貴（Hou Weigui ／ホウ・ウェイグイ）によって設立されました。ZTE は通信機器業として飛躍的な発展を遂げ、端末製品等製品群を拡大するとともに、1995 年から海外事業展開を始めました。1997 年深圳証券取引所に、2004 年香港証券取引所に上場しました。中国初の香港証券取引所上場企業であり、中国唯一の上場通信メーカーとして、情報公開に積極的に取り組んでいます。2010 年には売上高が 100 億 U.S.ドルを超え、また 2011 年上半期には中国国外の売上が全体の売上の 56%に達しました。

ZTE は、常に最先端の研究開発をしています。売上高の約 10% を研究開発に投じており、現在 ZTE 社員の内、約4割がR&Dスタッフです。世界 15 ヶ所に研究開発センターを設置しています。また各種技術の国際的な標準化にも積極的に取り組んでおり、通信規格標準化組織で主導的役割を果たしています。



売上高

ZTEジャパンの概要

ZTE ジャパンは ZTE Corporation の 100%出資会社として 2008 年 4 月に設立されました。日本の通信事業者向けに、最先端の有線・無線の通信ネットワーク・ソリューション、3G 端末・スマートフォン・データカード等の携帯端末製品を提供しています。携帯電話・データカード等の端末事業では、2009 年より日本通信様、Willcom 様等への 3G データカード製品の提供、2010 年秋よりソフトバンク様に携帯端末の提供を行っています。またネットワークソリューション事業では、2011 年に Wireless City Planning 様に AXGP 基地局の納入を始めました。

日本で提供している製品群

ネットワークソリューション事業

ネットワークソリューション事業では、LTE FDD/TDD、WiMAX 等のモバイルブロードバンドソリューションをモバイルオペレータ様向けに提供しています。更に、ルータ、スイッチなどの IP 製品を軸にクラウドコンピューティングへの貢献を重点戦略テーマの一つとして取り組んでいます。

ZTE は、世界最先端の製品開発力、幅広い製品･ソリューション群、カスタマイズ、プライス競争力などの優位性をもとに、日本のお客様に”いつでもどこでも高速に使える”環境を実現するネットワーク製品・ソリューションを提供していきます。

共通プラットホーム

お問い合わせ先

ZTEジャパン株式会社

〒105-0001東京都港区虎ノ門5-13-1虎ノ門40MTビル6階

TEL:03-5408-5700　FAX:03-5408-0752

タレスジャパン株式会社
http://www.thales-esecurity.com/japan

THALES

タレス e-Securityは、世界中の企業、金融サービス、防衛機関、および政府機関向けにグローバルな暗号化セキュリティソリューションを提供するリーディングカンパニーです。
40年にわたる実績を持つタレスのソリューションは、お客様の最も機密性の高いデータを保護し、エネルギーおよび航空宇宙業界のトップ5企業中4社および世界中の政府ネットワークで採用され、世界中で行われる決済処理の80%以上を保護しています。

タレスの暗号化セキュリティソリューション

タレスのセキュリティソリューションは、HSM（ハードウェアセキュリティモジュール）の技術をベースにした包括的な製品ラインナップによって、Data in Use（使用中のデータ）、Data at Rest（保存されたデータ）、Data in Motion（移動中のデータ）の全てのデータに対して、暗号技術を用いた強力な保護を実現します。

決済セキュリティ

payShield 9000は、決済システムの保護専用に設計されたHSMです。金融業界のセキュリティ監査要件に完全に準拠しており、すべての主要カードスキームにおけるカード発行およびトランザクションの保護に採用されています。
現在は世界中のカードトランザクションの80%以上を保護しています。

アプリケーションセキュリティ

nShieldは、多目的用途向けHSMです。高速な暗号処理、強力なアクセス制御、物理的アクセスからの保護（耐タンパ性）といった機能を備え、FIPS140-2 Level3認定を受けた、クラス最高のセキュリティを実現します。各種標準APIをサポートし、PKIやDB暗号化など暗号アプリケーションとのシームレスな連携が可能です。

ストレージセキュリティ

keyAuthorityは、ストレージ環境における暗号鍵管理を行うアプライアンス製品です。IEEE P1619.3鍵管理標準に準拠し、暗号化機能が組み込まれたテープライブラリ、スイッチ、ディスクアレイなどが使用する暗号鍵を統合的に管理します。FIPS140-2 Level3クラスの堅牢なハードウェアで暗号鍵を保護し、暗号鍵の可用性を保証します。

ネットワークセキュリティ

Datacryptorは、イーサネットフレームの暗号化を行うネットワークアプライアンス製品です。IPsecのような追加ヘッダーによるオーバーヘッドがなく、ショートパケットに対してもワイヤレートでの暗号化通信を提供します。100Mbps、1Gbps、10Gbpsの各モデルを使用して、広域WAN環境でのフルメッシュの暗号化を効果的に実現します。

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
〒107-0052 東京都港区赤坂２丁目17-7 赤坂溜池タワー8階
TEL:03-6234-8180　FAX:03-6234-8181
Email：jpnsales@thales-esecurity.com

JNSA 会員企業のサービス・製品・イベント情報です。

■製品情報■

○ スマートデバイス向け認証強化システム「SHieldMobile」

私物のタブレット端末やスマートフォンなどの企業内利用（BYOD）が増加する中、スマートデバイスからイントラネットへアクセスする際のセキュリティ対策がより重要度を増しています。
「SHieldMobile」はAndroidとiOSに対応したスマートデバイス用の認証強化システムで、SSL-VPN装置連携や二要素認証などにより、スマートデバイスの安心・安全なイントラネットアクセスでスピーディなビジネス対応を実現します。

【製品情報詳細】
http://www.ssl.fujitsu.com/products/network/netproducts/shieldmobile/

◆お問い合わせ先◆
富士通ソーシアルサイエンスラボラトリ
（富士通SSL）
お問い合わせ総合窓口
ssl-info@cs.jp.fujitsu.com

○クラウドセキュリティに関する総合的解説書

（株）情報経済研究所では、クラウドセキュリティの解説書を出版しました。（執筆：勝見）
クラウドセキュリティのポイントを全て網羅‼
クラウドのインシデント事例とセキュリティ課題、誰が何を言っているか、どのようなサービスがどう活かされているか、どんな可能性があるか、など、包括的に紹介し検討しています。
東日本大震災で活躍したクラウドの情報も含め、BCPの視点からも見逃せません。
版元は㈱インプレスR&Dです。下記にお問合せ・ご発注ください。

【製品情報詳細】
http://www.impressrd.jp/news/111018/CloudSecurity2011

◆書籍に関するお問い合わせ先◆
インプレス インターネットメディア総研
ご相談窓口
お問い合わせ総合窓口
TEL：0120-350-995　03-5275-1087

■サービス情報■

○サイバー攻撃の脅威にセコムがトータルサポート『セコム・サイバー攻撃対策サービス』

未知のウイルスを使った「新しいタイプの攻撃」は、インターネットの”入口対策”だけでは防げません。
「セコム・サイバー攻撃対策サービス」は、情報の「出口」対策を徹底し、２４時間３６５日の監視体制と迅速な対応で、標的型攻撃に対して機密情報などの漏洩を防止します。深刻な事態に陥った場合、要請に基づき現地対応により被害の拡大を防止するとともに、根本的な問題解決に向けた対応を行ないます。

【サービス情報詳細】
http://www.secomtrust.net/service/cyber-attack/

◆お問い合わせ先◆
セコムトラストシステムズ株式会社
E-mail：sts-info5@secom.co.jp
TEL：03-5775-8641

PKI Day 2011 <番号制度時代のPKI> 開催報告

セコム株式会社 IS 研究所
水戸　和

去る 9 月 26 日（月）、赤坂の山王健保会館にて PKI 相互運用技術 WG 主催 PKI Day 2011 が開催されました。今年で 7 回目を迎える PKI Day ですが、今回は副題を“番号制度時代の PKI”として、現在法制化の議論が行われている「社会保障・税に関わる番号制度」を本格的なデジタル社会への移行のための社会基盤の整備と捉え、そのようなデジタル社会における PKI の方向性を議論しようという趣旨で開催されました。これまでの PKI Day を振り返ってみると、第 1 回目の副題が“PKI 最新動向”となっていたものが、今回は“番号制度時代の PKI”となっているように、PKI Day で扱う題材が技術としての PKI から、社会的な問題に対するソリューションとしての PKI へと変化を迎えているようにも見受けられます。このことを裏付けるかのように、午後のパネルディスカッションでは経済産業省 CIO 補佐官の満塩尚史氏や弁護士の宮内宏氏といった、幅広い肩書きの方が参加され、熱い議論を繰り広げられました。

■講　演

最初の発表は“セキュリティ＆プライバシーの課題とマイクロソフト U-Prove”と題してマイクロソフトの渡辺清氏から、オンラインサービスの普及に伴い生じているセキュリティ・プライバシ・スケーラビリティの 3 要件を満たす新しい認証技術として Microsoft 社の推進する U-Prove 技術の紹介が行われました。この U-Prove を認証に用いることにより、ユーザーは問い合わせに対し必要とする情報のみ開示することが可能であり、Privacy by Design を実現した技術となっているとのことでした。

二人目は“楕円曲線暗号における PKI”と題し、筑波大学助教の金岡晃氏より RSA と並ぶ公開鍵暗号アルゴリズムとして知られる楕円曲線暗号（以下、ECC）の普及の背景、暗号強度を決定する複数のパラメータの紹介から OpenSSL に実装された ECC のパフォーマンスの評価まで、ECC 全般に亘る発表が行われました。

質疑では、ECC 関連の多くの特許を抑えている Certicom 社について言及され、金岡氏からは”実装にあたって特許問題で苦労している人も多いはずで、そろそろ（ECC 関連の特許マップなどを）まとめる動きがあってもいいはず”との発言がありました。また、金岡氏から会場への逆質問への回答として電子パスポートでの ECC 使用実態の解説がなされるといった一幕もありました。

小休憩を挟み、三人目の発表は PKI Day 初参加の NTT 情報流通プラットフォーム研究所の武藤健一郎氏から“SSL における暗号危殆化サンプル調査の報告”と題し、実際に稼動している SSL サーバーの証明書の署名アルゴリズム、サーバーの対応する SSL コネクション、そしてクライアント（OS・Web ブラウザ）における暗号・ハッシュアルゴリズムの対応状況といったものの調査報告が行われました。

サーバー証明書の調査では、危殆化が懸念されている RSA1024 と MD5 の組み合わせを用いるサーバーは昨年度の調査でほぼ無くなるなど、順調に移行が進んでいるようにも見受けられましたが、一方でサーバーが受け入れ対応している暗号・ハッシュアルゴリズムでは古いデバイスへの接続対応のため未だに RC4-MD5 の接続に対応しているサーバーが大部分を占めているという事実も示されました。また、クライアント側で使用する OS、ブラウザの違いによっても、SSL 接続において用いられる暗号・ハッシュアルゴリズムに違いが出るため、サーバー側、クライアント側双方で危殆化の対策が必要であるとの見解を示されました。質疑では、

サーバー側でRC4-MD5を利用した接続を許可しない設定にすることの可能性について言及され、業務系や組み込み系といったデバイスへの対応が問題となるとの見解が示されました。また、会場からのコメントとして、“ベンダーとしてはクライアントにベネフィットを示すことが出来ないと移行を促しにくい、各ベンダーのコツコツとした努力が不可欠である”との見解が示されていました。

昼休み前最後の発表は、産業技術総合研究所（AIST）の山口利恵氏から“日本におけるRSA1024・SHA-1の移行に関する施策”と題し、先の武藤氏の発表にもあったRSA1024・SHA-1の危殆化に合わせて行われる公的個人認証サービス（JPKI）、政府認証基盤（GPKI）、地方公共団体組織認証基盤（LGPKI）といった国や自治体の運用しているPKIでの暗号移行について説明が行われました。2014年度に移行開始を予定しているこれらのシステムですが、国や自治体のような複数の運営者の問題や、e-Taxのようなアプリケーションやハードウェア（ICカードや利用端末）の移行問題といった複合的な問題を抱えているという事実が紹介されていました。

午後の部の講演では日本情報経済社会推進協会（JIPDEC）の木村道弘氏から“最近の欧州PKI事情”と題し、欧州におけるPKI標準化体制の歴史的推移から欧州各国の電子署名法の要件になっているAdES（Advanced Electronic Signature）を例にとり実際に標準化された技術の紹介、そして直近の欧州PKI標準化組織の動向の紹介がなされました。

欧州におけるPKI標準化体制については、欧州標準化委員会（CEN）が要求仕様を作成、欧州電気通信標準化機構（ETSI）が対応する技術仕様を策定という形を目指していたが、十分に機能していなかったため、EC指令によって規格そのものも含めた再編成が取り組まれているとのことでした。質疑では欧州でのタイムリーな話題としてDigiNotarにおける適合性評価の問題について扱われ、ETSIによる基準はあくまで最低限の認定（クオリファイ）であり、実際は運用によってレベルに大きな差が生まれてしまっているという問題点が指摘されていました。

■ パネルディスカッション

パネルディスカッションでは「社会保障と税に関わる番号制度」における法人番号の扱いを主な題材に、JNSA PKI相互運用技術WGのリーダーで、内閣官房で番号制度検討を行う情報連携基盤技術WG、社会保障分野SWGの委員も勤めるセコムの松本泰氏をモデレーターとして、同様に情報保護評価SWG委員を勤める宮内宏法律事務所の宮内宏氏、情報連携基盤技術WGの委員である東京工科大学教授の手塚悟氏、経済産業省CIO補佐官の満塩尚史氏、そして日本ベリサインの佐藤直之氏の5名という番号制度を語るにはこれ以上ないメンバーによるディスカッションが繰り広げられました。

まず、松本氏からこれまで技術的な問題にフォーカスしていたPKIにおける議論は今後、証明書が「何を証明するのか」といった制度的な側面についても行っていく必要があるという提言が行われ、そのケーススタディとしての番号制度に関する検討状況の解説と、付番・本人確認・情報連携という番号制度の実現する3つの機能についての説明がありました。その中でPKIの証明書は、従来からの人が紙の書類を読むことを前提とした本人確認ではない、曖昧性のないデジタル技術を前提とした番号制度の様な制度、すなわち「デジタル時代の社会基盤としてのアイデンティティ管理」に基づいて発行されるべきものであると指摘し、これが実現することにより番号制度がデジタル社会の社会サービスプラットフォームとして機能するとの見解が示されました。一方で、現在の番号制度に関する検討では法人番号に関する検討が不十分であり、法人の意思がどのように確認されるかが不明

瞭であるとの指摘がなされました。

これを受け、手塚氏からは現在の番号制度の中で行われている法人番号について、「個人」のライフサイクルと「法人」のライフサイクルの違いに言及し、個人に対して行われるのと同様のフレームワークを適応するのは困難であると指摘し、同時にこれら境界にある個人事業主の存在に関しても検討が必要との見解が示されました。

続いて満塩氏からは、ユーザーとしての観点から番号制度の目的・効果に注目して番号制度について論じる必要性が指摘されました。その一例に氏の私見として、番号制度による法人認証が導入されることにより、申請者の存在確認・申請事実の確認・申請内容の確認のうち前者2点の仕事を自動化できるというワークフロー削減の可能性を示しました。一方で、申請内容の確認のような人手によって実現するほうが効率的な仕事も依然として存在するため、番号制度により実現される機能と人手による仕事のバランスをとることが大事との見解が示されました。

宮内氏は、法務上の観点から、現状の法人の電子認証制度やその証明書の内容の紹介に続いて、法人の意思表示がどのように行われているかという点に関して「代理方式」と「機関方式」の2つの方式を紹介し、代理方式の必要性が求められる認証（Authentication）と異なり、電子署名においては機関方式と同様の運用が望ましいと示す一方で、従来の法人印と同様に法人の中の個人に電子署名に用いる私有鍵やパスワードを預けることがあってよいのか？という問題点を指摘していました。

最後に、佐藤氏からはPKIと電子署名法について、現状の電子署名法において企業の電子認証行為は管轄外となっており、署名実施者個人から見ても電子署名法における認証認定業務では企業との所属関係などは取り扱われないため、企業としての機関による意思表示や、企業人としての個人による代理での意思表示が出来ておらず、商業登記に基づく電子認証制度用いた企業の代表者による個人の認証しか行えていない事実が指摘され、番号制度の制定にあわせ電子署名法の改正も含めた検討が必要との見解が示されていました。

そして、自由討論ではこれらの発表を題材にして法人格による電子署名の法令化可能性と、その署名管理を民間事業者が行う可能性を題材に、議論が行われました。満塩氏からは法人番号を含んだ証明書の可能性について、証明書にとって「修正」という概念が存在しないことを指摘し、代表者名のような比較的高い頻度で変更される情報を入れるのは不適当であるとの指摘がされていました。

最後の質疑では会場から「こういった制度があると何が出来るか、と言った議論だけではなく、Trustと言う視点に立って、何を”信じて”こういった制度が機能するのか、といった点について考えることも必要」と言う指摘がなされました。松本氏からも、Trustが崩壊してしまったオランダのDigiNotarの事例から様々学ぶことも多いのではないかと言う返答がなされるなどの意見交換がなされていました。

今年のPKI Dayは、プライバシー問題等に対応するU-Prove、組み込み機器に対する楕円暗号、そして、パネルディスカッションでのTrustという観点など、技術としてのPKIから、社会的な問題に対するソリューションとしてのPKIと言う方向性が強く出ていたように思われました。タイトルにある「番号制度」の導入はそういったソリューションとしてのPKI時代の嚆矢として大いに期待したいと思うと同時に、PKIの可能性を示すマイルストーンとして十分な検討がなされてほしいと感じました。

参考URL：http://www.jnsa.org/seminar/pki-day/2011/index.html
http://www.jnsa.org/result/pki/index.html

西日本支部主催　セキュリティセミナー「NSF 2011 in Kansai」

株式会社インターネットイニシアティブ
関西支社技術部　齋藤　聖悟

JNSA西日本支部では地域のセキュリティレベルの向上を目的としてNSF 2011 in Kansaiを下記の要領で開催しました。

日　時: 2011年10月5日(水)9時50分～17時20分
会　場: 大阪国際会議場グランキューブ大阪
主　催: NPO 日本ネットワークセキュリティ協会 西日本支部
定　員: 150名
概　要: 中小企業における情報セキュリティの現場にあったクラウド、スマートフォンの運用のポイントについて
料　金: 無料

2011年に入ってクラウドやスマートフォンの企業への導入が本格化する中、中小企業の情報セキュリティ対策の現状に、これらの最新トレンドをどのように組み込んで行けばよいかを探ることを目的に開催しました。

開催挨拶

西日本支部の井上支部長がJNSAおよび西日本支部の発足以降の歩みと現状、これからのJNSAについて紹介を行ないました。

基調講演

奈良先端科学技術大学院大学 山口英教授からは「クラウドやスマホとの付き合い方」と言う題名で、これまでのコンピュータシステムと何が違い、何がメリットなのかを解説戴きました。

仮想化・集中の技術をベースとするクラウドについては運用のプロフエッショナルの知見を活用した利用を推奨するという立場で、保有から利用、独占から共有へのメリットによりTCO削減以上のメリットはあるが、パブリッククラウドについてはベンダーロックインや適正なトラブル対応がされるかなどサービス事業者の選定には注意が必要との指摘がありました。

スマートフォンについてはBOYD対策の視点から、どのような業務で使用するのか？ビジネスプロセスを明らかすることが大切であり、クラウドに比べるとStepByStepでのアプローチが大切と言う解説でした。

日本ではこれから本格的な導入活用が始まるが、諸外国では相当に活用が進んでおり、見習うべきところが沢山あると言うメッセージには多くの参加者が考えさせられたのではと思います。

中小企業セキュリティ

西日本支部からは富士通関西中部ネットテック株式会社 嶋倉文裕氏が「中小企業セキュリティ」と題し、現状の中小企業セキュリティ対策としてJNSA 西日本支部が作成した「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」の活用方法について解説頂きました。また中小企業でクラウドやスマートフォンなど新たな技術や新デバイスへの対応のための考慮すべき点について問題提起をして頂き、その後のクラウドセッションとスマートフォンセッションへの導入付けになったと思います。

クラウドセキュリティ

クラウドセキュリティのセッションでは二人の方に講演頂きました。

株式会社インターネットイニシアティブ 加藤雅彦氏は3月11日東北地方太平洋沖地震直後に実際に行ったクラウドでの震災支援について実際のtwitterでのやり取りを交えながら発表されました。またその体験から中小企業がクラウドを利用する場合には緊急時と平常時のセキュリティを分けて考えたほうがいいのでは、という提起がなされました。

株式会社ディアイティ 河野省二氏からは経済産業省が発行したクラウドセキュリティの活用について紹介頂きました。

クラウドコンピューティングに対する漠然とした不安を整理解説しそれらを「見える化」するためにクラウドサービス利用のための情報セキュリティマネジメントガイドラインの活用方法を解説頂きました。

後半では「最近気になるクラウドに関する思い込みセキュリティってありますか？」「セキュリティの強度と可用性のバランス」をテーマに加藤氏と河野氏の思いを語って頂きました。

スマートフォンセキュリティ

スマートフォンセキュリティのセッションでは株式会社カスペルスキー 前田典彦氏からスマートフォンのマルウェア検知状況について解説頂きました。

特に2011年に入って急激にその利用が増加しているスマートフォンのセキュリティ対策の必要性を強調されていました。

引き続きラックホールディングス株式会社 山城重成氏からスマートフォンのプラットフォームによるマルウェアの違いやウィルスの基本構造を解説頂き、遠隔操作でカメラを使用した盗撮や盗聴でAndroid端末がマルウェアに感染する様子のデモを交えながら、最後にキャリアによる対策・個人による対策についてまとめて頂きました。

パネルディスカッション

パネラーとして嶋倉氏、河野氏、前田氏、「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」の取りまとめを担当したアイネット・システムズ株式会社 元持哲郎氏に加わって頂き、最新の事例を元に複数の視点から中小企業におけるクラウドやスマートフォン導入時・運用時の問題点や対策のポイントについてディスカッションを行って頂きました。

その結果、クラウド・スマートフォンについては導入が本格化、特にクラウドについては活用事例やセキュリティガイドラインなどが整備されつつあり、中小企業での導入も積極的に行い得る状況にあるとの共通認識に至りました。しかし、スマートフォンについては利用者視点を踏まえたセキュリティ対策がまだまだ途上にあり、慎重な対応が必要との意見が大勢を占め、基調講演の山口教授の「スマートフォンの活用にはビジネスプロセスの構築と業務の改善が必須」と言う指摘に呼応した形で、スマートフォン単体のセキュリティだけではなく、業務プロセス全体を考えてのセキュリティ対策が必要との警鐘でまとまりました。

NSF 2011 in Kansaiを終えて

3年ぶりとなる大阪でのセミナー開催で、色々と不安要素がありましたが、関心の高い内容だったためか多数の申し込みを頂き、事前受付は満席となり、当日は129名の参加者を集め、盛況なセミナーとなりました。アンケート結果も“大変有益であったが44%”、“有益であったが55%”と好評で成功したと思います。

アンケート一部抜粋

- 基調講演、クラウド、スマホの内容が良く理解できた。
- 最新の動向や、本質的な課題は何なのか、といった点で、非常に勉強になりました
- スマートフォンセキュリティについては、マルウェアのトレンドが具体的に紹介されており、有意義でした。デモもよかったです。
- クラウドセキュリティ等のパネルディスカッションで有益な情報も聞けてよかった。

ただ、予想よりも多くの方に申し込みいただいたため、参加できなかった方がいらっしゃったのも事実で、またアンケートの中では関西でのセキュリティに関連したイベントが少ないという指摘もありました。

- 関西でのセミナーが少ないので増やしてほしい
- 西日本支部での勉強会やセミナーの回数を増やしてほしい

今回のセミナーでは企業ブースコーナーを併設すると共に出社してから退社するまでソリューションマップを配布するなど積極的な取組みを行いましたが、これからも関西圏のセキュリティレベル向上のためJNSA 西日本支部としてセミナー・勉強会を継続していきますのでご期待ください。

「2011 日韓情報セキュリティシンポジウム」の報告

【日　程】　2011年11月10日(木)13：00～18：45

【場　所】　五反田ゆうぽうと

【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)
特定非営利活動法人日本セキュリティ監査協会(JASA)
韓国知識情報保安産業協会(KISIA)

【後　援】　総務省、経済産業省、情報セキュリティ政策会議、独立行政法人情報処理推進機構(IPA)、
JPCERTコーディネーションセンター、Telecom-ISAC Japan

【参加人数】　合計148名
＜内訳＞韓国側：36名、日本側：112名(一般参加者：91名　関係者16名　事務局5名)

「2011日韓情報セキュリティシンポジウム」は、2011年11月10日(木)、五反田ゆうぽうとにて開催いたしました。当シンポジウムは、日韓の情報セキュリティの向上を目指す企業と人の交流を図り、グローバルな体制が必要とされる情報セキュリティに関して両国に共通の課題を議論し、共通の理解を得る目的で、日本ネットワークセキュリティ協会(JNSA)、日本セキュリティ監査協会(JASA)、韓国の知識情報セキュリティ協会(KISIA)が協力して開催したものです。

今回は、本年1月に韓国ソウルで開催した「第1回日韓情報セキュリティシンポジウム」を受けて第2回目として日本で開催いたしました。

プログラムは、JASA土居会長、JNSA田中会長、KISIA李会長の挨拶に始まり、「大規模インシデントの予防と対応」というテーマでJNSA副会長中尾康二氏とアンラボ張氏の講演、「スマートフォンと情報セキュリティ」というテーマで株式会社ラック西本逸郎氏とFasoo.com李氏の講演、「クラウドコンピューティングと情報セキュリティ」というテーマで伊藤忠テクノソリューションズ株式会社佐藤元彦氏とSECUI.COM南氏の講演、そして、IPAとKISA(韓国インターネット振興院)による取り組み紹介のあと、最後に「情報セキュリティ産業のアジア展開と日韓連携」というテーマでモデレータに日本側は中尾氏、韓国側は韓国情報保護学会長Dr. Youmを迎え、パネルディスカッションを行いました。当日は総勢148名(内韓国側36名)の参加者を集め、パネルディスカッションでは日韓の連携の具体化についても討議されました。また、別室で韓国企業による展示会も開催され、こちらも多くの方々にご参加いただきました。次回は2012年11月に韓国ソウルで第3回シンポジウムを開催予定です。

2011 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年度より開催してまいりました。

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。

今年度は一般向けビデオ・冊子教材を刷新し、よりリアリティある映像と初心者にもわかりやすい解説冊子が完成いたしました。新規教材の完成に伴い従来のプログラムも見直し、来場者参加型でよりいっそう楽しく学べるインターネット安全教室を開催しております。

また、3月3日には、インターネット安全教室 in 東京 ～ネットとうまくつきあうために～ と題し、第4回全国情報セキュリティ啓発シンポジウムを開催いたしました。

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。

なお、現時点での開催状況は以下のとおりです。

【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、学校等

［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）

［共催団体］（次頁）一覧をご覧下さい。（2012年2月2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」共催団体募集について◆

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、茨城県、鳥取県、高知県、山口県、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

2011年度「インターネット安全教室」共催団体一覧

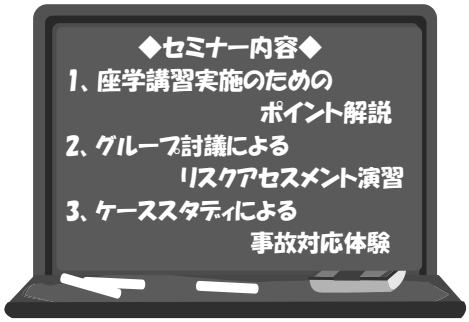
（2012.2.2現在）

地域	県名等	団体名
北海道・東北	北海道	NPO くるくるネット
		旭川情報産業事業協同組合
		北海道情報セキュリティ勉強会（せきゅぽろ）
	青森県	財団法人八戸地域高度技術振興センター
		青森県情報サービス産業協会
		NPO 法人 IT 支援ネットあおもり
		株式会社ソフトアカデミーあおもり
	岩手県	NPO デジタルネットワークいわて
	秋田県	NPO ノースウインド
		NPO 法人 IT サポートあきた
		秋田大学
	宮城県	仙台インターネット推進研究会
	福島県	特定非営利活動法人日本コンピュータ振興協会
関東	栃木県	NPO 栃木県シニアセンター
	群馬県	NPO おおた IT 市民ネットワーク
		太田市役所
	埼玉県	NPO 市民と電子自治体ネットワーク
	千葉県	NPO 法人松戸 ITV ネットワーク
		NPO 浦安防犯ネット
		NPO 南房総 IT 推進協議会
	東京都	NPO 法人イーパーツ
	神奈川県	NPO 情報セキュリティフォーラム
		藤沢市総務部 IT 推進課
甲信越・北陸	新潟県	NPO 新潟情報セキュリティ協会
	富山県	株式会社富山県総合情報センター
	石川県	（社）石川県情報システム工業会
	福井県	NPO ナレッジふくい
	山梨県	NPO 法人ＩＴコーディネータ山梨（ITC 山梨）
		山梨大学
	長野県	上田市マルチメディア情報センター
		NPO 法人グループ HIYOKO
東海・近畿	岐阜県	NPO かにぱそこんくらぶ
		財団法人ソフトピアジャパン

地域	県名等	団体名
東海・近畿	岐阜県	NPO 法人アツマールぎふ
		NPO 法人泉京・垂井
		多治見市情報センター
	三重県	くわな PC ネット
		PC シエル
	静岡県	NPO 法人静岡情報産業協会
	愛知県	NPO 東海インターネット協議会
	滋賀県	NPO 滋賀県情報基盤協議会
	京都府	IT コンソーシアム京都
	大阪府	GIS 総合研究所
		大阪工業大学
		NPO 法人きんきうぇぶ
	兵庫県	兵庫県立大学大学院応用情報科学研究科
	奈良県	NPO なら情報セキュリティ総合研究所
		奈良県社会教育センター
	和歌山県	NPO 情報セキュリティ研究所
中国・四国	島根県	NPO プロジェクトゆうあい
	岡山県	岡山県インターネットセキュリティ対策連絡協議会
	広島県	福山市役所情報政策課
		近畿大学工学部
	香川県	ｅーとぴあ・かがわ（かがわ県民情報サービス㈱）
		NPO 法人 ITC かがわ
	愛媛県	愛媛県 IT 推進協会
	徳島県	財団法人　ｅーとくしま推進財団
九州・沖縄	福岡県	西日本短期大学
	佐賀県	NPO 法人シニアネット佐賀
	長崎県	長崎県立大学
	熊本県	NPO NEXT 熊本
	大分県	財団法人ハイパーネットワーク社会研究所
	宮崎県	宮崎公立大学
	鹿児島県	NPO 法人鹿児島インファーメーション
	沖縄県	石垣市役所　企画開発部　情報推進課
		NPO 法人フロム沖縄推進機構

中小企業の経営者等に対して、情報セキュリティに対する適切なアドバイスを行なう地域の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。事業開始４年目となる今年度は、過去のセミナーの集大成として、「中小企業にこそ求められる情報セキュリティ対策」など指導者の実践に役立つ内容で展開します。

情報セキュリティ対策の指導力向上と、中小企業の情報セキュリティレベルの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/

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）
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、開催地の商工会議所・商工会連合会・中小企業団体中央会
開催地・日程	全国 25 箇所で 2011 年 8 月～2012 年 2 月に開催 （開催地別日程は別表のとおり）
開催時間	9:30～17:00 （9:00 受付開始）
参加人数	各会場 50～100 名
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、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。
セミナー内容	参加者の方々が、地域で講習会を実施したり、指導の実践に役立てるための内容で行います。 ① 座学講習実施のためのポイント解説 座学講習を行うための講習会スケジュール（2時間程度数種類）と説明ポイントの解説を行います。また、講習の中で、タイムリーで話題性のある情報を提供できるように、最新の情報セキュリティ動向をお伝えします。 例：スマートフォン、ソーシャルメディア、クラウドサービス、BCP 等 ② リスクアセスメント演習 ある企業の業務風景を映像化したビデオを見て、グループ討議でリスクアセスメントの演習を行います。直接的なリスクだけでなく関連して発生しうるものなど、そこに潜むリスクを探し出すことで、気づきを養うとともに中小企業に対して適切に対策提案を行うためのスキルを養います。 ③ ケーススタディによる事故対応体験 情報セキュリティ事故（インシデント）の事例を基にして、対応方法をグループ討議しながらロールプレイ形式で演習を行い、事故対応の疑似体験をします。セミナーにより体験したことを中小企業指導に役立ててもらうとともに、地域の講習会で事故対応時の注意点などとして伝えられるようにしていただきます。
参加者に期待すること	本セミナーに参加された方々へは指導用ツールの提供や中小企業向け講習会の開催を支援しますので、ぜひ情報セキュリティ普及啓発活動に本セミナーを役立てていただければ幸いです。 • 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）をお渡しします • 配布する指導用ツールを用いて中小企業の情報セキュリティ講習会を開催された場合、実施報告レポートを提出いただくことで謝金をお支払します（2012 年 2 月末開催分まで）。 • セミナー参加者専用サイトにより、その他の指導用の補足資料等を随時提供していきます。
参加費	無料（事前登録制）

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 27 回
※今年度のセミナーは全て終了しました。

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	札幌商工会議所	2011 年 8 月 30 日（火）	北海道経済センター
	北海道②	帯広商工会議所 / 北海道中小企業団体中央会 十勝支部事務所 / 北海道十勝管内商工会連合会	2011 年 12 月 15 日（木）	帯広商工会議所
東　北	宮　城	仙台商工会議所	2011 年 9 月 22 日（木）	仙台商工会議所
関　東	栃　木	宇都宮商工会議所	2011 年 10 月 26 日（水）	宇都宮商工会議所
	東京①	東京商工会議所	2011 年 11 月 1 日（火）	東京商工会議所ビル
	東京②	東京商工会議所	2012 年 1 月 30 日（月）	東京商工会議所ビル
	神奈川	神奈川県商工会連合会 / 神奈川県商工会議所連合会	2011 年 9 月 6 日（火）	相鉄岩崎学園ビル
	千　葉	柏商工会議所 /NPO 法人ちば経営応援隊	2011 年 10 月 12 日（水）	柏商工会議所
	新　潟	新潟商工会議所 / 財団法人にいがた産業創造機構 / 特定非営利活動法人新潟情報セキュリティ協会	2011 年 11 月 25 日（金）	NICO プラザ
中　部	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	2011 年 12 月 13 日（火）	富山県総合情報センター
	愛　知	名古屋商工会議所 / 社団法人中部産業連盟	2011 年 9 月 9 日（金）	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 1 月 18 日（水）	ソフトピアジャパンセンタービル
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。	2011 年 12 月 9 日（金）	京都商工会議所
	大　阪	大阪商工会議所	2011 年 11 月 15 日（火）	大阪商工会議所
	兵　庫	神戸商工会議所 /NPO 法人 ITC 近畿会	2011 年 9 月 15 日（木）	神戸市産業振興センター
	和歌山	田辺商工会議所 /NPO 情報セキュリティ研究所	2011 年 12 月 1 日（木）	情報交流センター ビッグ・ユー
	福　井	ふくい産業支援センター / 福井県商工会議所連合会 / 福井県商工会連合会 / 福井県中小企業団体中央会 / 福井県情報化支援協会	2012 年 2 月 2 日（木）	福井県産業情報センタービル
中　国	広　島	広島商工会議所 /NPO 法人 ITC 広島	2011 年 10 月 20 日（木）	広島商工会議所
	岡　山	岡山商工会議所	2011 年 11 月 22 日（火）	岡山商工会議所
	鳥　取	米子商工会議所	2011 年 11 月 8 日（火）	米子商工会議所
	山　口	下関商工会議所 / IT コーディネータやまぐち協同組合	2012 年 1 月 27 日（金）	下関商工会館
四　国	徳　島	徳島県商工会連合会	2012 年 1 月 13 日（金）	あわぎんホール
九　州	福　岡	福岡商工会議所	2011 年 9 月 27 日（火）	福岡商工会議所
	大　分	大分商工会議所 /NPO 法人大分 IT 経営推進センター 財団法人ハイパーネットワーク社会研究所	2011 年 11 月 29 日（火）	大分商工会議所
	鹿児島	鹿児島商工会議所	2011 年 10 月 14 日（金）	鹿児島商工会議所
	宮　崎	宮崎商工会議所 / 宮崎県ソフトウェアセンター	2012 年 1 月 20 日（金）	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	2011 年 10 月 7 日（金）	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

● **インターネット安全教室 in 東京**

主　催：経済産業省,日本ネットワークセキュリティ協会
日　時：2012年3月3日(土)
会　場：大手町サンケイプラザ
URL：　http://www.net-anzen.go.jp/symposium/

後援・協賛イベントのお知らせ

1. 自治体総合フェア

主　催：一般社団法人　日本経営協会
日　時：2012年5月23日(水)～25日(金)
会　場：東京ビッグサイト(東京国際展示場)
西展示棟・西3ホール
URL：　http://www.noma.or.jp/lgf/index.html

2. 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

主　催：株式会社リックテレコム
日　時：2012年5月30日(水)～6月1日(金)
会　場：東京ビッグサイト
西3・4ホール　会議棟
URL：　http://www.wjexpo.com

JNSA 部会・WG2011 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)

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)

2010年度に引き続き、経済産業省委託事業「平成23年度コンピュータセキュリティ早期警戒体制の整備事業『インターネット安全教室』」の企画・運営、共催団体へのサポート等を行っていく。

【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)

2010年度に引き続き、経済産業省委託事業「平成23年度コンピュータセキュリティ早期警戒態勢の整備事業『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」の内容検討を行っていく。

【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)

今夏は、節電に向けて在宅勤務が増加することが見込まれているが、十分な対策なしに在宅勤務等が実施されることで、情報漏洩のリスクが高まる恐れがあることから、限られた時間の中でどのような点に留意し、どのような対策を講じればよいかについて、会員の持つノウハウをオンラインで集成して文書としてとりまとめ、JNSAのWebサイトで無償公開し、一般企業等での対策の参考にしていただく。

オフィスの節電対策のための「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7月に公開した。

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）

2010年の発生確率調査（トライアル）の結果からテーマを選択・深堀りし、また2010年の調査項目以外の他エリアも追加検討し、2011年発生確率調査（本調査）を実施する。リスク評価検討WGと連携し、発生確率調査の必要条件の決定や、統計的検証を行う。2010年個人情報漏えい調査の報告書の公開、および2011年の同調査も継続して実施する。予定成果物は、

- 「2010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」（7月公開）
- 「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 個人情報漏えい編」

【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）

国内の情報セキュリティ市場の現況を調査・分析し、報告書を作成する。今年度は、2010年度版完成予定。また、2011年度版の調査を行い、年内に報告書をまとめることを目指す。

予定成果物は、

- 「2010年度版国内情報セキュリティ市場調査報告書」
- 「2011年度版国内情報セキュリティ市場調査報告書」

【IPv6セキュリティ検証WG】
（リーダー：林憲明 氏／トレンドマイクロ株式会社）

組織内ネットワークに対し、意図せずにIPv6接続した利用者が及ぼしうる被害とその対策について検討を行う。

共同検証実施後、3回程度のミーティング開催により報告書を仕上げる。管理者の知らぬ間に一部IPv6化された場合にどのような管理手法が考えられるのか、制限していた項目が制限されなくなることはあるのか、IPv4環境下において、安全対策上実施していた項目が使えなくなることはあるのか等の項目について報告を行う計画。

予定成果物は、「2011年 IPv6セキュリティ検証報告書」

【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）

企業においてスマートフォンの利便性を損なわず安全に業務利用するためのガイドラインの策定と関連の研究、勉強会、情報交換の実施。「スマートフォン活用セキュリティガイドラインβ版」の続編となる完全版と、関連する情報資料の策定とリリース予定。

予定成果物は、「スマートフォン活用セキュリティガイドライン2011年度版」

【SNSセキュリティWG】（新規）
（リーダー：高橋正和 氏／日本マイクロソフト株式会社）

利用者を急速に増やしているSNSは、セキュリティやプライバシーについての新たな問題を提起している。一方で、これらの問題点が個人や企業の利用者が参考とすべき情報が少ないことから、SNSをITインフラの一形態として、安全な利用を促すことを目的として以下の活動を行う。

- SNSのセキュリティとプライバシーに対する調査（現状把握）
- 上記調査に基づく、安全な利用方法の取りまとめ（対策の提案）
- SNSを使ったセキュリティ啓発手法の研究（利用方法の研究）

予定成果物は、

- セキュリティの観点から見たSNSの現状と課題
- SNSの安全な利用方法についての資料
- SNSを使った啓発活動の試行（SNSのコンテンツとして作成）
- SNSを通じた、これらの成果物の公表

3. 標準化部会

（部会長：中尾康二 氏／KDDI株式会社）

【セキュリティにおけ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）

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。

今年度は、ロールマネジメントについての議論と成果物の作成、番号制度やプライバシについての勉強会と議論、ID管理のあるべき論の議論（グローバル環境、ハイブリット環境など）等を実施する予定。

予定成果物は、「アイデンティティ管理におけるロールマネジメント（仮）」

【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）

セキュアなシステム開発を開発現場寄りの立場から考え、課題を討議する。なお、この2、3年は、国際規格を討議テーマとして地道な検討・評価を行う方針としている。

ISO/IEC 27034は、その第一部がISO/IEC JTC1/SC27で最終委員会ドラフトとなったが、依然として内容が抽象的であるため有効と思えず、日本として別の切り口からの貢献ができないかSC27/WG日本委員会とともに探っている。今後は、特に分散システムやプロダクトラインでのセキュリティ保証に役立つ規格内容への誘導といったアプローチに焦点をあてたい。

予定成果物は、討議成果の国際規格への反映、解説

的文書の作成等。

【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」の作成に関し、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等のアウトプットを作成する。

WGでは、対策マップ記述モデル、作成手法、標準対策マップ案の作成等を検討する予定。

また、8月にキーマンズネットにてWG活動の内容を記事として公開した。（4回連載）

【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。

ISFとのワークショップ（2011年6月）の開催、ISF総会（2011年10月）への参加、KISIAとの連携支援、およびISFとの共同成果物の作成を進める。なお、ISO/SC27への成果物については、2011年10月会合への入力を目指す。

予定成果物は、「クラウドセキュリティにかかわる技術ガイドライン」ドラフト

なお、作成したドラフトは、2011年10月開催のISO/SC27会合で提案した。

【PKI相互運用技術WG】
（リーダー：松本泰 氏／セコム株式会社）

WG活動での情報共有、PKI day 2011などのイベントでの提案、提言を行う。また、ネット社会における信頼（TRUST）の仕組みを提案、提言していく。

予定成果物は、「番号制度とPKIの関係等」等のペーパを出すことを検討。

【リスク評価検討WG】
（リーダー：二木真明 氏／SCSK株式会社）

過去のインシデント事例や社会的な傾向などをもとに、ある組織のリスク量を実際に推定するための基本的なモデルを考える。当面、モデルの複雑化はなるべく おさえ、リスクの概観を定量化できるような「どんぶり」モデルを目標とする。（その後の検証を経てモデルをより精緻なものにしていく）

予定成果物は、「情報セキュリティリスクの統計的推定手法に関する検討報告書（仮称）」

4. 教育部会

（部会長：安田直 氏／株式会社ディアイティ）

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、教育に関する実証実験を行うことで、その成果を会 員で共有し、更に論文発表や成果物を一般公開することにより会員のみならず社会に対しても還元することでJNSAの存在意義を高めていく。

【セキュリティ講師スキル研究WG】
（リーダー：長谷川長一 氏／株式会社ラック）

「セキュリティ講師スキル研究調査報告書（仮）」を作成し、その実証実験を行う。これにあたっては、基本教育実証WGやU40部会、女子BoFなどとも連携し、相互の活動を活性化し、成果を充実させたものとしたい。また、これらの結果は「セキュリティ講師スキル基準2011年度版（仮）」として、JNSA 会員や外部へ広く公開することを予定している。

予定成果物は、

- 「セキュリティ講師スキル研究調査報告書 2010年度版（仮）」
- 「セキュリティ講師スキルガイド 2011年度版（仮）」

【情報セキュリティ教科書執筆者WG】
（リーダー：塩見友規 氏／
三井物産セキュアディレクション株式会社）

作成した「情報セキュリティプロフェッショナル教科書」の普及、活用方法の検討、改版に向けての検討を行う。

【情報セキュリティ基本教育実証WG】
（リーダー：平山敏弘 氏／日本アイ・ビー・エム株式会社）

平成23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。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。

合計15回分の講義資料の作成、およびWG活動成果の論文採録を予定。

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

日本では、特にIT系分野で社会的に活躍している女性が少ないと指摘されているが、実態を把握し、環境も含め改善の道がないか検討する。

将来的には、業界に向けて、実務で活躍する女性たちの声を提言として発信する。

予定成果物は、通年の活動結果をまとめ、報告書はJNSAの成果発表会などで公開し、意見交換を実施する。必要に応じてセミナーやシンポジウム等を開催する。

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、勉強会や会員交流会の企画、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。

具体的には、新しい問題（目標40問）を作成し、プレミアム版のユーザ事例を収集して、サイト、セミナーなどで公開する予定。

予定成果物は、新しい問題の作成・公開、ユーザ事例の公開

【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）

JNSA会員企業のPRの場として、会員企業が有している各種ソリューションを紹介するWebサイト （JNSAソリューションガイド：仮称）の構築を目的に活動を継続する。

予定成果物は、

「JNSAソリューションガイド（仮称）」WEBサイト

- Webサイト
- 運用手順書他、関連ドキュメント一式

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。

【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）

「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」との紐付けによる情報セキュリティチェックシートの見直しや、新しいデバイスの出現に伴うリスクに対応する情報セキュリティ対策について整理を行う。

【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年度公表「出社してから退社するまで中小企業の情報セキュリティ対策実践手引き」の対象読者からのフィードバックを行う。

具体的には、対象読者からのフィードバック及び「情報セキュリティチェックシート」見直しに伴う手引きを修正する。また、新しいデバイス出現に伴うリスクに対応するための「追補版」作成を検討する。

予定成果物は、必要であれば以下2点の成果物を作成

- 「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た、セミナーおよびメンバー企業・連携他団体との交流による勉強会を実施していく。

2－3ヶ月に一度の勉強会を企画。また秋に西日本支部としてのセミナー、他団体との合同セミナー開催を予定している。

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内にて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を実施する。具体的には、IPv6環境におけるセキュリティ検証、家電機器DLNA実地検証を行う予定。

予定成果物は、

- IPv6検証報告
- DLNA検証報告

【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。

部会にて勉強会で取り上げたいテーマを持ち寄り、その

中からテーマを絞って講師打診、会場や日程の調整を行う。

1～1.5ヶ月に一回のペースで開催する。U40メンバー優先にはなるが、継続してJNSA会員への聴講枠開放も行う予定。

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）

ISEPA情報セキュリティ資格マップをサイトにて公開。8月に情報セキュリティ大学院大学とセミナーを開催。

【広報WG】

（リーダー：勝見勉 氏/NPO日本セキュリティ監査協会）

イベントの企画・開催のみならず、ホームページなど、様々な媒体を通して、ISEPAの活動成果等のお知らせを発信する。

【スキルWG】

（リーダー：衣川俊章 氏／(ISC)2　Japan）

情報セキュリティ人財の育成を行うにあたって利用・参照できる指標を「人財アーキテクチャ」として策定し、その利活用についても「使える」情報を継続的に提供する。

【相互認証WG】

（リーダー：小林佑光 氏／SEA／J）

数多くある情報セキュリティ資格がそれぞれ発信している情報をまとめたり、資格や教育プログラム間で相互の認証が行われるような働きかけを行っていく。

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。

【セキュリティオペレーションガイドラインWG】

（リーダー：許先明 氏／株式会社ラック）

セキュリティ診断・検査のためのガイドラインを検討する予定。

予定成果物は、「セキュリティ診断・検査のためのガイドライン」

【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（IPv6、スマートフォン等）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）

「MSS事業者のための情報セキュリティ小六法」外部公開予定。また、これに関連するガイドラインを検討予定。

予定成果物は、「MSS事業者のための情報セキュリティ小六法」

【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。

JNSA 役員一覧　2011 年 12 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）

後沢　忍	三菱電機株式会社　情報技術総合研究所
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
勝見　勉	株式会社情報経済研究所
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
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
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
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
近藤　伸也	キヤノンＩＴソリューションズ株式会社
佐藤　憲一	株式会社ＯＳＫ
佐藤　徹次	ネットワンシステムズ株式会社
佐藤　友治	株式会社ブロードバンドセキュリティ
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
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
藤田　平	株式会社シマンテック
二木　真明	ＳＣＳＫ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	株式会社ラック
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1月5日現在　146社　50音順)

【あ】

(㈱)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)
(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)ISAO
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
(株)インフォセック
(株)ウィテック
(株)AIR
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
関電システムソリューションズ(株)
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(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】

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
住商情報システム(株)
(株)セキュアブレイン
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)
ソフトバンクBB(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)
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　ｼｽﾃﾑｽﾞｴﾝｼﾞﾆｱﾘﾝｸﾞ(株)
日本オラクル(株)
日本サード・パーティ(株)
日本サムスン(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)
パナソニック電工(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)ブロードバンドセキュリティ
(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
(株)MONET

【や】

(株)ユービーセキュア

【ら】

(株)楽堂
(株)ラック
リコー・ヒューマン・クリエイツ(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（2011 年度）

4 月	4 月 19 日	「セキュリティ & リスクマネジンメントサミット 2011」後援
	4 月 25 日	第 1 回幹事会
	4/27 ～ 28 日	「IT インフラストラクチャ&データセンターサミット 2011」後援
5 月	5 月 10 日	2011 年度理事会
	5 月 25 ～ 27 日	「ワイヤレスジャパン 2011/ モバイルパワー 2011」後援
	5 月 27 日	「第 9 回迷惑メール対策カンファレンス」後援
	5 月 26 ～ 28 日	「第 15 回サイバー犯罪に関する白浜シンポジウム」後援
6 月	6 月 1 日	第 2 回幹事会
	6 月 7 ～ 10 日	「Interop Tokyo 2011」後援
	6 月 8 日	2010 年度 WG 活動報告会（アルカディア市ヶ谷）
	6 月 8 日	2011 年度総会（アルカディア市ヶ谷）
	6 月 18 日	「ISACA 大阪支部設立 25 周年記念講演会」後援
7 月	7 月 7 日	「MCPC　スマートフォンセキュリティセミナー」後援
	7 月 13 ～ 15 日	「自治体総合フェア 2011」協賛
	7 月 22 日	「仮想化インフラ・ワークショップ 06」協賛
	7 月 26 日　他	「平成 23 年度情報モラル啓発セミナー」後援　　7/26 鹿児島、7/29 鳥取　他
8 月	8 月 4 日	「組織力向上を目指したキャリアパスとスキルの可視化セミナー」　後援
	8 月 17 日	第 3 回幹事会
	8 月 31 日～ 9 月 1 日	「Cloud Computing World 2011」「Next Generation Data Center 2011」後援
9 月	9 月 14 日、16 日	「ID & IT　Management Conference 2011」後援
	9 月 26 日	「PKI Day 2011」（山王健保会館）
10 月	10 月 3 ～ 5 日	「Gartner Symposium & Itxpo 2011」後援
	10 月 5 日	JNSA 西日本支部主催セキュリティセミナー（グランキューブ大阪）
	10 月 6 日	第4回幹事会
	10 月 7 ～ 8 日	「学びのイノベーション & セキュリティフェア」後援
	10 月 7 ～ 8 日	「情報セキュリティワークショップ in 越後湯沢 2011」協力
	10 月 31 日～ 11 月 1 日	「ロジスティクスソリューションフェア 2011」協賛
11 月	11 月 1 日　他	「平成 23 年度情報モラル啓発セミナー」後援　11/1 青森　11/17 岐阜
	11 月 4 ～ 5 日	「ハイパーネットワーク別府湾会議」後援
	11 月 9 日	「ITGI Japan カンファレンス　2011」後援
	11 月 9 ～ 10 日	「PacSec 2011」後援
	11 月 10 日	「2011　日韓情報セキュリティシンポジウム」
	11 月 12 日	「子どもワークショップたじみ」後援
	11 月 30 日～ 12 月 2 日	「Internet Week 2011」後援
12 月	12 月 2 ～ 4 日	「かごしま IT フェスタ」後援
	12 月 5 日	第5回幹事会
	12 月 12 ～ 13 日	「デジタル・フォレンジック・コミュニティ 2011 in Tokyo」後援
1 月	1 月 25 日	「Network Security Forum 2012 (NSF2012)」（ベルサール神田）
	1 月 25 日	「JNSA 賀詞交歓会」（ベルサール神田）
2 月	2 月 14 日	「サイバー情報共有のためのワークショップ」（ベルサール八重洲）
3 月	3 月 3 日	「インターネット安全教室　in 東京」（大手町サンケイプラザ）

2011 年 4 月～
2012 年 3 月
「インターネット
安全教室」開催

2011 年 8 月～
2012 年 2 月
「平成 23 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。）

日本電気株式会社　佐藤　靖士

JNSA会員の皆様はじめまして。この度NTTコムテクノロジー株式会社の門田さんよりご紹介をいただきました､日本電気株式会社(NEC)の佐藤と申します。

私は現在、弊社NECと関連会社にて運用しているセキュリティオペレーション関連の業務に従事し、それらのサポートや運用管理等を行っております。NECというとハード・ソフトの製造・販売、システム構築などSIerというイメージが強いかも知れませんが、実はActSecureというSOCの運用も行っており、監視サービスやセキュリティ診断サービス等も提供していますので、興味のあるかたはご相談頂けると幸いです。

このように今でこそセキュリティ関連の業務に携わっている私ですが、入社から数年間はUNIX系OSの開発や、通信･業務用ミドルウェアの設計･開発を手がけており、セキュリティについては、ファイルやNWのアクセス制御を設定する、あるいはアプリ間の通信を暗号化するなど、主に利用者視点から関わるだけでした。

転機となったのは2003年頃、FW等セキュリティ製品の開発に携わった事です。それ以前の｢提供されるセキュリティ機能｣を利用する立場から、｢提供するセキュリティ機能｣を設計・実装する側になったことで、｢敵を知り己を知らば｣という諺よろしく脅威となる攻撃側を強く意識するようになり、以後攻撃手法や攻撃者の行動調査等に従事する契機となりました。

以降数年はそのような技術的側面からの調査・研究に携わっていましたが、一方で現実に発生するセキュリティインシデントに対しては、常時の監視や問題への対処、更には事後対策など、運用面が重要であると感じるようになり、今の活動に至っております。

現在JNSAでは主にISOG-J WG2に参加させて頂いております。WG2は特に技術的な話題が多く、現場で活躍されている技術者の方々の声を直接聴き、また意見交換が出来る数少ない場所であると思います。このような場に参加させて頂けていることに感謝しつつ、多少なりとも私自身、その中でお役に立てるよう活動していきたいと思います。

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

日本電信電話株式会社　南端　邦彦

JNSA 会員の皆様、はじめまして。日本電信電話株式会社（NTT）の南端と申します。今回、NTT データ先端技術株式会社の小林さんから紹介を受け、本コーナーを担当することになりました。

私は現在、大手町で研究企画部門のプロデュース担当に所属しており、プロデューサーとしてセキュリティビジネスに関する企画などの仕事をしています。

プロデューサーというと、TV 番組でも作るの？というイメージがありますが、私のミッションは、NTT の研究所が持つ特許技術や技術ノウハウを活用し、NTT グループ各社と連携しながらビジネスを創造することです。私が言うのも何ですが、研究所の技術は非常に高度なので、まずは十分に理解することから始め、そしていかにお客様に役立つか、NTT グループ全体の事業に貢献できるのかという観点で、色々思いをはせながらビジネスのアイデアを日々考えています。

JNSA の中では、ISOG-J を中心とした活動をしています。私自身、かれこれ 10 年以上、SE としてセキュリティシステムの提案・構築をしたり、ファイアウォール、IDS/IPS といったセキュリティ機器の保守運用をしたり、セキュリティサービスの企画をしたりと、様々なセキュリティに関する業務に携わってきました。そして、これまでの経験も踏まえ、セキュリティオペレーションの重要性がさらに増すと考え、ISOG-J に参加することを決めました。

ISOG-J において、一つの成果として WG1 より 2010 年 8 月に公開した「マネージドセキュリティサービス選定ガイドライン」の執筆に参加できたことは、非常に有益な経験でした。ISOG-J には、高い技術力、豊富な知識、そして熱い思いを持つ方々が沢山いらっしゃるので、日々刺激を受けながら活動に参加しています。

仕事の話はこれくらいにしたいと思いますが、中・高・大学とバスケットボール部に所属していました。社会人になってからは縁遠くなり、体重も徐々に増えてきまして、毎年毎年、人間ドックで言われることが多くなってくる始末。「先生、バスケがしたいです。」と言いたい今日この頃です。しかし、中々時間が取れないこともあって、“楽に”やせる方法は無いか思案中です。ちなみに過去に 2ヶ月で 8kg のダイエットをしましたが、バスケだけに見事にリバウンドしました。良いダイエット方法があれば是非教えて下さい。

とりとめなく書いてしまいましたが、JNSA の活動に積極的に参加できたことで、人脈や視野が以前と比べられないくらい広がったと思います。今後も少しでもその活動に貢献し、JNSA 会員企業の皆様の繁栄の一助となればと思いますので、引き続きどうぞよろしくお願い致します。

JNSA について

■会員の特典

1. 各種部会、ワーキンググループ・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.33

2012 年 3 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