特定非営利活動法人
日本システム監査人協会報

2012年2月発行
No 132

No.132（2012年2月　発行）

会報電子版の記事　目次

めだか　【共通番号制「マイナンバー」利用成るか】　投稿

政府は2011年6月、社会保険と税の一体改革に併せ、「社会保障・税番号大綱」で個人に「番号」、法人に「法人番号」を交付する「マイナンバー」制度をまとめた。

2011年8月2・3日付け日本経済新聞の「経済教室」欄で“動き始めた共通番号制（上・下）”として、当該記事が掲載されていた。そこには効用（ポイント）として、以下の項目が挙げられている。

（寒椿：森林公園にて、埼玉）

・共通番号制導入で煩雑な手続き解消など利点
・統一的な番号なら情報の誤り放置あり得ず
・震災時にも被災者の税負担減免などに効果
・銀行口座の開設や住民登録でも活用すべし
・個人情報保護への懸念にシステム面でも配慮
・民間利用は地域経済の活性化にも寄与する

このように、戸籍・年金・パスポート・運転免許証等の公的情報・書類・手続き、医療機関・金融機関・電気・ガス等のサービスや各種保険契約等の民間での利用等々、共通番号制（マイナンバー）は多くの面で活用され、的確でかつ迅速な業務遂行が可能となり業務効率を大幅に上げるであろう。
上記の関連業務および当該情報システムの改善等の経済効果も大きなものになることが予想される。多くの関連情報システムにおける有効活用は、システム開発を含め筆者も大変興味がある。

しかし、本当に「マイナンバー」制度の成立はなるだろうか。

新聞記事にもあるが、約10年前の「住民基本台帳ネットワーク（住民票コード）」は有効に活用されているとは思えない。民間利用が禁止されたのが原因だともある。筆者も「住民基本台帳」を使用したことは一度もない。また、国民の個人番号制への警戒感を払拭するには、政府への信頼が今よりもっと高まらなければならない、ともある。多くの国民にとっては、現在の政府では信頼するに当たらないであろう。民間利用が可能となると、個人情報保護の観点からも多くの議論・反論があるであろう。

新聞記事（下）には結論として、“番号制度とはまさに国のあり方を議論することと同義であり、諸外国でもそれぞれの歴史や文化に根差した制度となっている。今後も、様々な立場から国民的な議論が起きることを期待したい”と結ばれている。

「社会保障・税番号大綱」の公表から約半年が経った今、社会保障・税の一体改革が座礁に乗り上げている感があるだけでなく、共通番号制度についても議論が行われているとは思えず、新聞にも関連記事の掲載は見ない。国民的な議論にほど遠いと感じるのは筆者だけだろうか。

（格物致知）

（このコラム文書は、投稿者の個人的な意見表明であり、SAAJの見解ではありません。）

本　部　連　絡

1. 会長人事 （2012.1 速報）

長年、SAAJ の顔としてご活躍、ご指導いただいた鈴木信夫会長の後任として、新会長に沼野伸生氏が推薦され、1月理事会で承認されました。沼野氏（副会長）は、月例研の主査として活躍されていますので、会員の中で知らない人はいないでしょう。

システム監査普及や IT 関連のシステム開発、設備投資などの有効性評価への活動とあわせ、当協会の財政基盤の確保という課題をふくめ、まずは会長業務の引き継ぎ中です。同時に、事務局長も馬場氏から仲氏へバトンタッチするということで、一気に世代交代を迎えています。

2月の総会にむけ、現状の課題、新年度への取り組みについて、議論が交わされています。

会報への登場は、総会後を予定。今年は、理事の改選期にあたるため、新しい体制がスタートしてから、新任理事の紹介を兼ねて、特集を組ませていただく予定です。

2. CSA 更新 （2012.1 末速報）

この1月末で、更新が必要な CSA/ASA の認定者は、個別の案内メールが送信されています。

更新時期を迎え、更新手続を失念すると失効しておりますので、CSA/ASA を名乗ることは出来なくなります。手続に必要な書類を送付していない方はいらっしゃいませんか。

1 月31日の消印までが通常の更新受付期間でした。失効すると再登録が必要になります。新しい認定証や更新の連絡は、順次、申請書類が審査された後、2月中には送付される予定です。

具体的な申請方法など、SAAJ 公式サイトの CSA 更新手続の案内サイトで再確認ください。

http://www.saaj.or.jp/csa/csakoshin.html

3. 総会の案内 （2012.2）

SAAJ 総会は、2 月 24 日（金）午後より、東京港区芝公園の機械振興会館地下会議室で開催されます。

2011 年の活動報告、2012 年活動計画の説明、審議のほか、理事の改選が予定されています。

4. 会員の住所変更、所属変更

異動や退職、転職で、SAAJ 事務局からの連絡物、および、電子メールによる会報の送付先に変更を必要とする方は、準備しておいてください。

1） 会員番号、会員向けに通知された ID、パスワードが必要です。

2） 連絡先など、個人情報の変更は、会員自身で変更処理できます。

3） 会報は、登録された、電子メールアドレスに送付されます。

定期異動の時期を迎えますので、会員情報の編集方法について、後述しています。（2011.10 の再掲）

研究会、セミナー開催報告、支部報告

■【平成 23 年度 北信越支部石川県例会報告】

以下のとおり平成23年度 北信越支部石川県例会を開催し研究報告を行いました。

日時:2011 年 12 月 10 日(土) 13:00-17:00
会場:IT ビジネスプラザ武蔵(金沢市)
例会議題::

- ✧ 2011 年を振り返って・2012 年の計画について
- ✧ 報告 1:「西日本支部合同研究会(岡山開催)」参加報告
- ✧ 報告 2:「モバイルシステムについて」清水 尚志 氏
- ✧ 報告 3:「情報セキュリティ『新しいタイプの攻撃』の概要と対策」宮本 茂明

■報告の概要

◇研究報告　（北信越支部 情報セキュリティ監査研究会）

「情報セキュリティ『新しいタイプの攻撃』の概要と対策」

報告者（会員 No.1281 宮本 茂明）

防衛関連企業や政府機関へのサイバー攻撃など標的型サイバー攻撃による被害が拡大しており、外部からのサイバー攻撃に対する情報セキュリティ対策について、これまでの不特定多数を対象とした攻撃への対策に加え、特定の標的に対する攻撃への対策が必要となってきている。

システム監査/情報セキュリティ監査を実施する上でもこれらの動向把握が必要であり、今回情報セキュリティ攻撃の動向と『新しいタイプの攻撃』の概要と対策の現状について、IPA 関連の資料を中心に整理を行った。後述の参考文献の資料を引用させていただいたが、このように充実した資料を公開いただいている IPA に感謝する。

1. 情報セキュリティ攻撃の動向

ドライブ・バイ・ダウンロード攻撃等従来の攻撃手法を組み合わせ、特定の標的を攻撃する「新しいタイプの攻撃」が出てきている。最近のサイバー攻撃の動向について以下に紹介する。

(1)ドライブ・バイ・ダウンロード攻撃

Web サイトを閲覧した際に、パソコン利用者の意図に関わらずパソコンにダウンロードさせる攻撃である。「ガンブラー型攻撃」が有名であり、攻撃は収束していない。

[最近の動向]
2004 年：
Web ﾌﾞﾗｳｻﾞの脆弱性を狙った悪意あるサイトを用意して閲覧者を待ち伏せ攻撃

2006 ～ 2007 年：

Web サイト攻撃ツールを使用することで、正規サイトを改ざんし、閲覧者を誘導／攻撃

2008 年：

SQL インジェクション攻撃を利用した、正規サイトを改ざんにより、閲覧者を誘導／攻撃

2009 年：

Web サイト管理者の FTP アカウント情報窃取を行う「ガンブラー型攻撃」の猛威

正規ｻｲﾄの改ざんにより、閲覧者を誘導/攻撃　FTP ｱｶｳﾝﾄ情報窃取の連鎖により、被害拡大

2010 年：

正規 Web ｻｲﾄの Web サーバ設定ファイルの書き換え。ｽｸﾘﾌﾟﾄ実行禁止でも、閲覧者誘導

正規サイトが利用する、外部広告配信サービスやアクセス解析サービスが配信する部品を改ざん。

Web ページを改ざんしないで、閲覧者を誘導/攻撃

⑵DDoS 攻撃　（分散型サービス妨害攻撃：Distributed Denial of Service Attack）

大量の「Web ページの表示要求」等によるサービス妨害攻撃である。

- ボット型ウィルスに感染された大量の個人パソコンからリクエストが発信され、攻撃アクセスに対し、個別に遮断する等の対処が難しい
- DDoS 攻撃の目的：金銭目的、組織に対する抗議、嫌がらせ、社会的・政治的意図等

[最近の動向]

ネットユーザ同士がネット上で集結し集団の意図として攻撃が行われている

（思想の対立による DDoS 応酬）

2010 年 3 月　：掲示サイト「2 ちゃんねる」への攻撃

2010 年 11 月　：内部告発サイト「WikiLeaks」への攻撃応酬

⑶ソーシャルエンジニアリング

人間の心理的な隙や行動のミスにつけ込んで個人が持つ秘密情報を入手する攻撃である。

[最近の動向]

SNS が特に攻撃者から狙われている

2010 年 3～4 月：

Facebook　「製品のベータテスト参加で iPad 無料進呈」

⇒Apple 社の公式ｻｲﾄに見せかけた偽サイト・・・生年月日、携帯電話番号を窃取

Twitter　「iPad を無料でもらえる」

⇒ツイート内の URL をクリックすると偽サイトに誘導

『短縮 URL』サービスの悪用　・・・ドメイン名を確認せずにアクセス

2010 年 6～8 月：

日本 携帯電話向け SNS 「モバゲータウン」、「GREE」の偽サイト（フィッシング目的）

⇒　ポイント 3 倍当選等 なりすましメールで誘導

(4)標的型攻撃メール

情報窃取を目的として特定の組織や個人に送られるウィルスメールによる攻撃である。

項目	標的型攻撃メール	マスメールウィルス
メール感染機能	なし	あり
テーマ・内容	限定的 （関心事、説得が適切）	一般的
攻撃目的	特定の組織の情報窃取 システムの妨害	社会騒乱
言語	日本語	主に英語
添付ファイル	文書形式	実行形式
差出人アドレス	詐称	不定
ｳｨﾙｽ対策ｿﾌﾄの検知率	低い　(検体収集困難)	高い
感染後のPCの症状	特に変わらず	重い / PCダウン

標的型攻撃メールの手口も以下のように変化してきている。

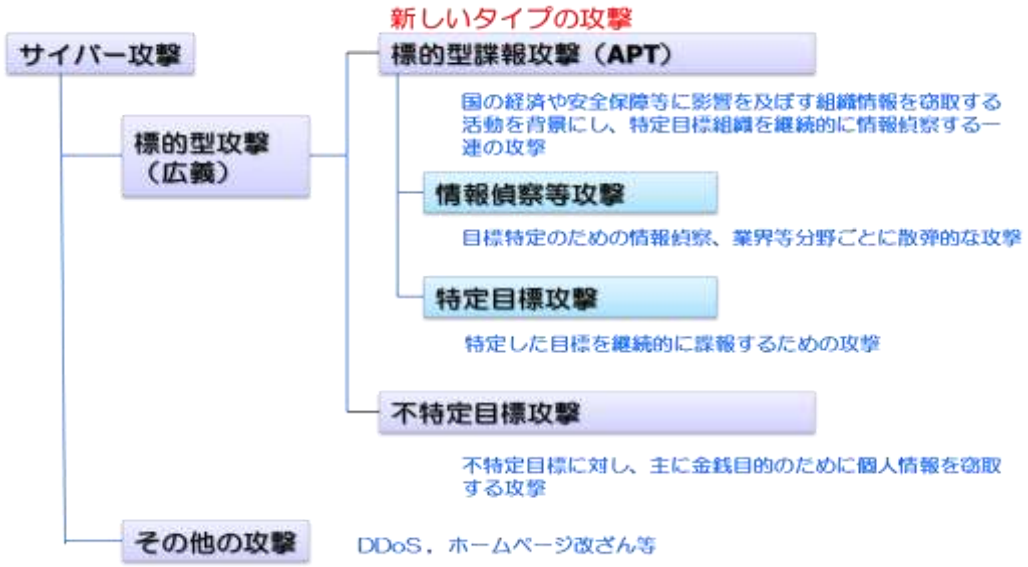
- ✓ 添付ファイルが付いていないケース
- ✓ HTML ﾒｰﾙ本文に悪意あるサイトへのリンク（ﾘﾝｸ先の URL と画面上の表示を変える）
- ✓ 組織内に大量の標的型攻撃メール配信

　組織内の本物業務メールを加工し多数の従業員に標的型攻撃メールを配信

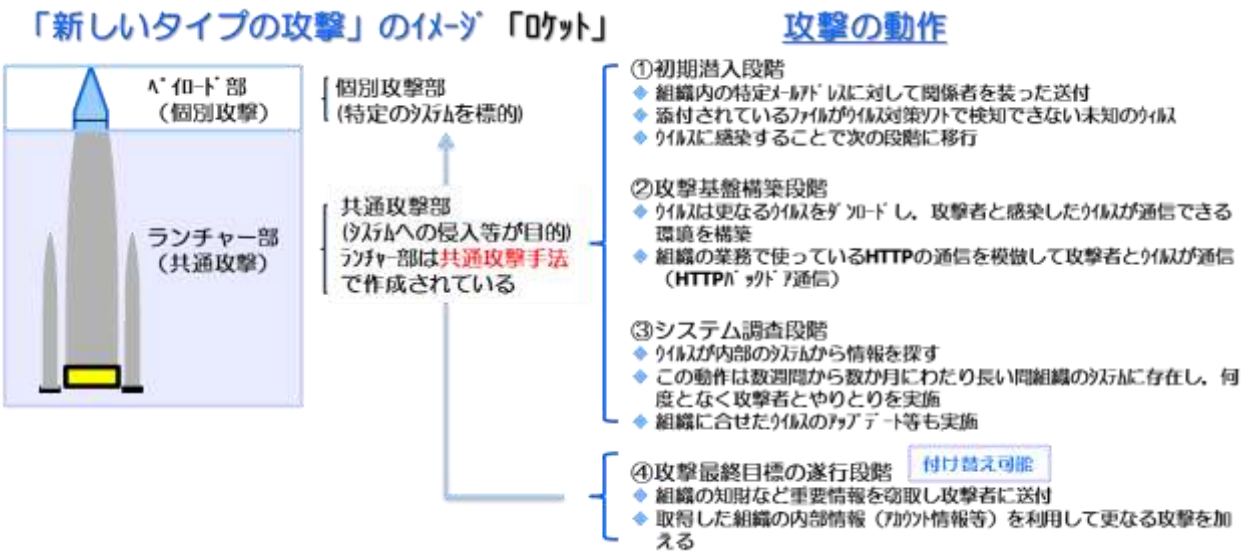
　* 組織内の正規の担当者から正規のﾒｰﾙに類似したﾒｰﾙが届くと開いてしまう可能性が高い

(5)新しいタイプの攻撃　　APT(Advanced Persistent Threats)　[標的型諜報攻撃]

脆弱性を悪用し、複数の既存攻撃を組み合わせ、ソーシャルエンジニアリングにより特定の企業や個人を狙う、対応が難しく執拗な攻撃である。



システム潜入等の「共通攻撃手法」攻撃＋情報窃取の目的に応じた「個別攻撃手法」攻撃

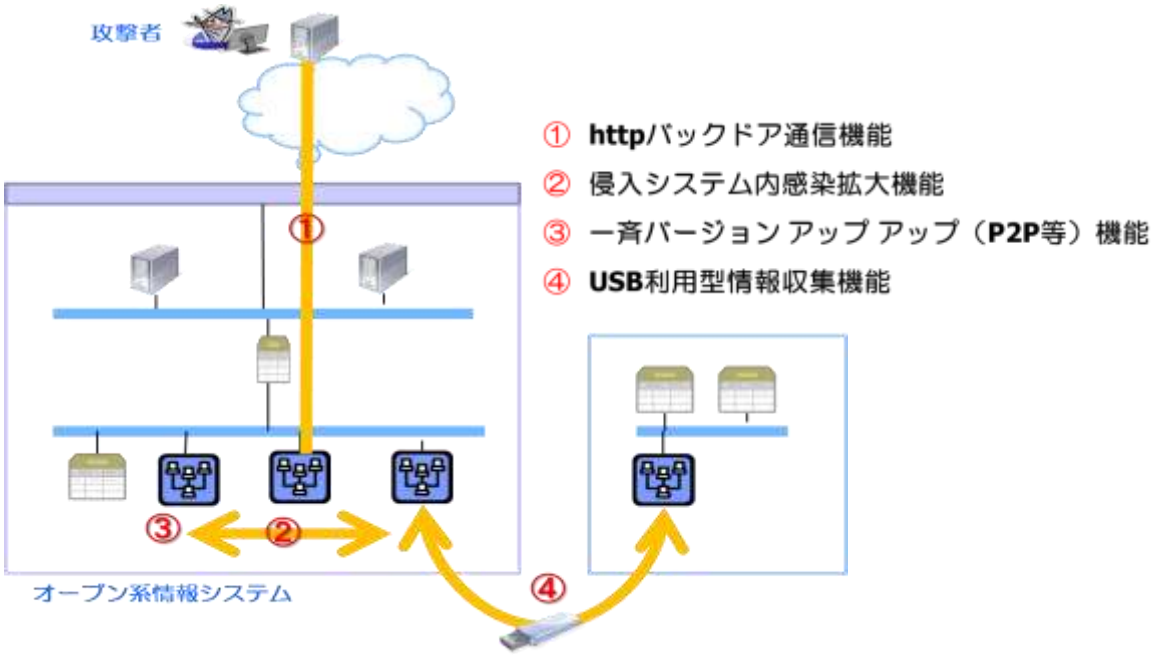


➢　「新しいタイプの攻撃」の脅威：

「個別攻撃手法」の対象が、情報システム、制御システム等幅広いシステムが対象となり、個別の防御対策が困難。意図と動機「誰がなんの為に行っているか」は未判明。

➢　「新しいタイプの攻撃」における共通動作機能

「発見しにくく静かな攻撃」を実現する４つの共通動作機能から構成されている。



共通動作機能	組織内のシステムでの動作	役割
①**http**バックドア通信機能	組織内で利用するhttp等，組織にとって必要とする通信プロトコルやポートを利用してバックドア通信を行う． 主に次の4つのパターン通信がある． • ﾌﾟﾛｷｼを介して行うHTTPﾌﾟﾛﾄｺﾙに類する通信 • ﾌﾟﾛｷｼを介して行う独自ﾌﾟﾛﾄｺﾙ通信 • ﾌﾟﾛｷｼを介さないHTTPﾌﾟﾛﾄｺﾙに類する通信 • ﾌﾟﾛｷｼを介さない独自ﾌﾟﾛﾄｺﾙ通信	ウイルスと攻撃者のサーバとの通信を確立する
②侵入システム内感染拡大機能	組織内ネットワーク感染により，脆弱性を利用したシステム内へウイルスを拡散する．	システム内の情報をより効率的に窃取するためにより多くの端末へ感染させる
③一斉バージョンアップアップ（**P2P**等）機能	拡散したウイルスに，攻撃者のサーバからダウンロードされた拡張機能モジュールを一斉更新する．	システム内に拡散されたウイルスに対して効果的な攻撃を行わせる機能を持たせるようにする
④**USB**利用型情報収集機能	USBを介してクローズ系システムに拡散し，クローズ系システム内情報を収集する． USBがオープン系システムに戻った時に収集情報を使て送信する． USBを介して攻撃サーバからの命令や更新機能をクローズ系システムに伝達する．	クローズ系情報を収集などの攻撃を行うため，USBにウイルスを混入させて攻撃を行う

2.「新しいタイプの攻撃」への対策

IPA から「新しいタイプの攻撃」への対策を考えていく上での参考ガイドとして、「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」が公開されている。内容は、IPA「脅威と対策研究会」において、攻撃仕様の分析、実証実験を交えた対策の検討を行った結果をまとめたもので、解決策の一例が示されている。2011 年 8 月に初版が発行された後、11 月に第 2 版へ改版され、出口対策も 6 種から 8 種に増えている。また、解決策の中には実証実験中のものもあり、継続し情報をフォローしていく必要がある。

(1)対策の考え方

組織の守るべき資産の明確化、リスクの評価に基づいて、一つの対策だけでなく多層の防御を実施する必要がある。

① 脅威は極力上流で食い止める
　　技術的対策だけでなく、標的型メールの取扱い規則も重要
② 侵入を阻止できなかった時の攻撃活動の抑止、
　　被害の極小化を図るための対策を考えておく ⇒　**『出口対策』**
③ 最後の砦となる守るべき情報の保護の強化
④ システム全体の監視と証跡の分析
⑤ 組織全体のセキュリティ・マネジメントやコンティンジェンシープランの整備

(2)「新しいタイプの攻撃」への出口対策

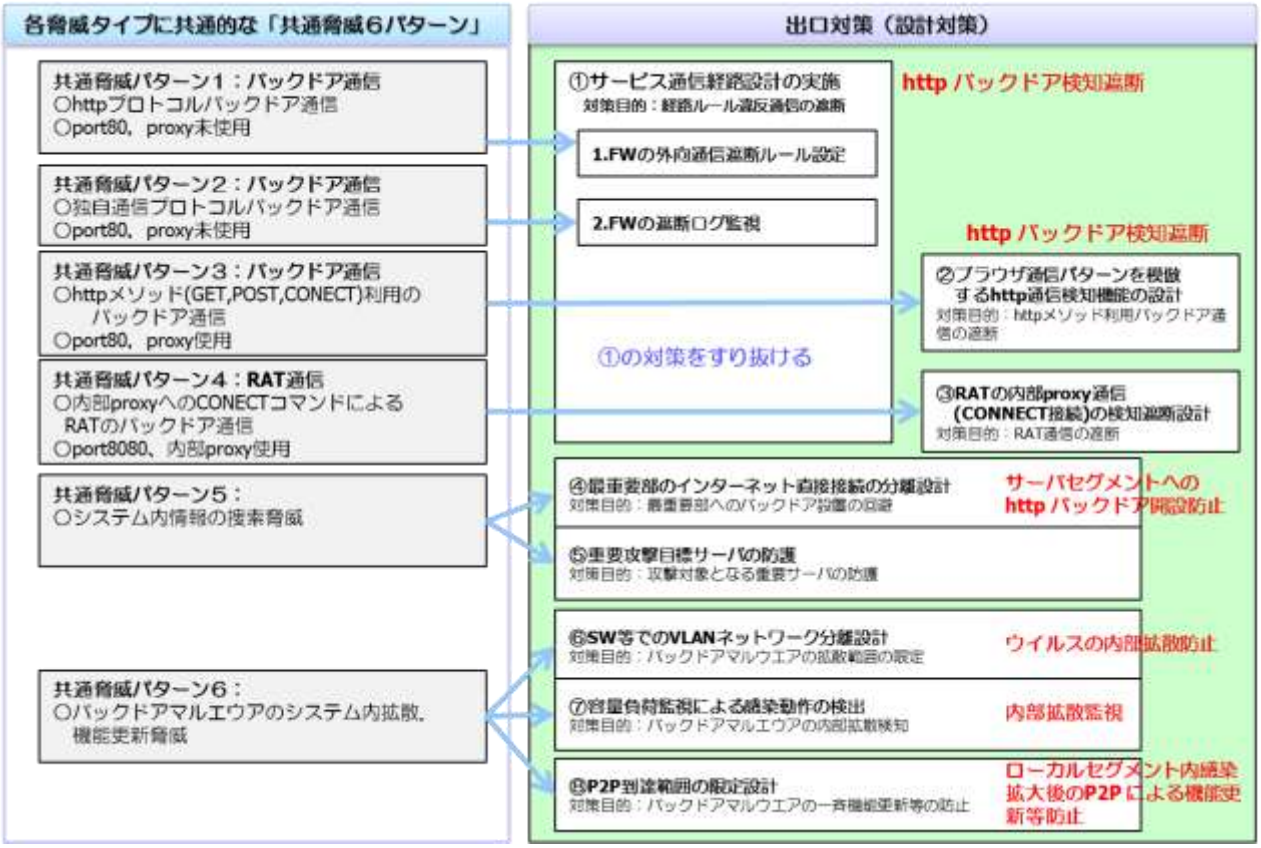
「入口対策」ではできないことがあり、攻撃者が意図している通信を止め、組織への影響を回避する「出口対策」が必要となる。

- 従来の設計対策思想の限界と出口対策の位置づけ
  - ✓ 入口対策（従来の設計対策思想）の限界

    脅威の侵入段階で阻止する対策（境界防衛）の限界
    - ゼロデイの脆弱性
    - 利用ｻｰﾋﾞｽに紛れた通信
    - 遮断ログに記録されない
  - ✓ 出口対策（新たな設計対策思想）

    脅威の侵入段階で阻止する対策（境界防衛）
    - 覗き見と情報持ち出し段階での防止策
    - 出口方向のバックドア通信を止めれば、最終影響（情報窃取、情報破壊）は回避される

➢　共通脅威６パターンと８つの「出口対策」



➢　出口対策の設計・実装のための対策要件定義

今回のガイドライン改訂で、設計構築時に各工程で検討・設計作業が必要な事項を作業単位に洗い出した WBS も示されていて、プロジェクト計画時にセキュリティ設計に必要な作業の洗い出しに活用できるようになっている。

3. 外部からの攻撃対策に対するシステム監査

各種基準（システム管理基準、システム監査基準、情報セキュリティ管理基準、情報セキュリティ監査基準、ISMS 等）にそったシステム監査に加え、最新の外部からの攻撃対策に関するシステム監査/情報セキュリティ監査が必要となると考える。日々新しくなる外部からの攻撃に関する技術情報をキャッチアップし、今後外部からの攻撃対策に対するシステム監査手法について検討していきたいと考えている。

［参考文献］

- 「IPA 情報セキュリティ白書 2011」 2011 年 6 月　独立行政法人 情報処理推進機構

- 「『新しいタイプの攻撃』の対策に向けた設計・運用ガイド」2011 年 8 月/ 11 月
  独立行政法人 情報処理推進機構
  http://www.ipa.go.jp/security/vuln/newattack.html

- IPA テクニカルウォッチ:『標的型攻撃メールの分析』に関するレポート 2011 年 10 月
  独立行政法人 情報処理推進機構
  http://www.ipa.go.jp/about/technicalwatch/20111003.html

- 「サイバーセキュリティと経済 研究会」中間とりまとめ　2011 年 8 月
  経済産業省
  http://www.meti.go.jp/press/2011/08/20110805006/20110805006.html

- IPA 「新しいタイプの攻撃、標的型攻撃の実態と対策について紹介」2011 年 11 月
  独立行政法人 情報処理推進機構
  http://www.ipa.go.jp/security/J-CSIP/index.html

以上

注目情報（2012/1/1～1/31）

日本ネットワークセキュリティ協会では、毎年、JNSA 2011 セキュリティ十大ニュースをまとめて公表している。
http://www.jnsa.org/result/news10/ によると、2011 年は、非常事態に立ちすくむという副題がついている。

【第 1 位】9 月 19 日「重要情報を狙った標的型攻撃の嵐が吹き荒れる」
～ 新たな攻撃手法に対抗するには ～

【第 2 位】3 月 11 日「東日本大震災で未曾有の被害」
～我々はこの大震災から何を学び、何をなし得るか～

【第 3 位】7 月 15 日「サイバー攻撃が軍事力に」
～各国が対応を進める中、「戦争を放棄」した日本は対応できず？ ～

【第 4 位】6 月 30 日「大震災で BCP 見直しが求められる」　～ 未曾有の大災害に BCP は機能したのか ～

【第 5 位】6 月 22 日「スマートフォンの脅威増大」　～ スマホ、セキュリティ対策の行方は？ ～

【第 6 位】4 月 26 日「ついに 1 億人の個人情報漏えい」　～ 企業はこの教訓を生かさねばならない ～

【第 7 位】4 月 1 日「クラウドの情報セキュリティガイドライン公表」　～ クラウドサービスの進展に禍福あり ～

【第 8 位】5 月 1 日「アノニマス、グローバル企業等を攻撃」　～ 独善「ハクティビスト」の暴走 ～

【第 9 位】2 月 26 日「京大入試 IT カンニング事件」　～ 国内初の携帯電話とネット投稿を利用した不正入試 ～

【第 10 位】6 月 17 日「ウイルス作成罪成立」　～ 不正プログラム作成をフセイでくれるのか・・・ ～

2012 年の今年は、年初から企業の業績低迷、巨額の赤字報告が続いています。
サイバーテロへの関心の高まり、刑法改正によるセキュリティ犯罪対策の本格化、など、2012 年もにぎやかそうです。

全国のイベント・セミナー情報

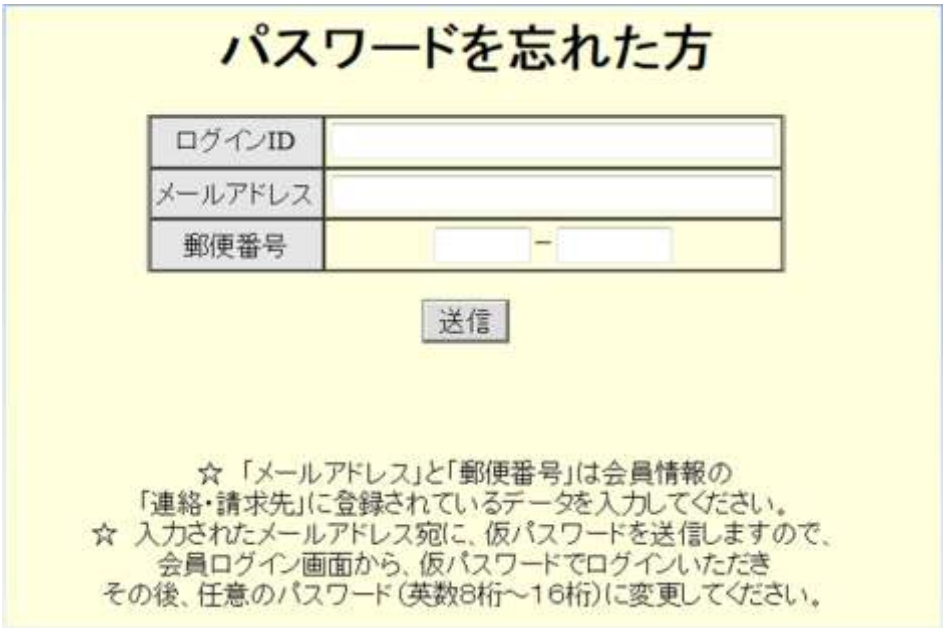
SAAJ 総会は、2 月 24 日（金）午後より、東京港区芝公園の機械振興会館地下会議室で開催されます。
2011 年の活動報告、2012 年活動計画の説明、審議のほか、理事の改選が予定されています。
特別講演では、システム監査の ISO 化について、審議の最新状況が報告される予定です。
開催の詳細は、 http://www.saaj.or.jp/ をご確認ください。

事務局からのお知らせ【会員情報の変更】　2012.2.6

§ 会員は、ご自分の登録情報を確認、変更するためには、
協会ホームページから会員サイトにログインします。

URL：https://www.saaj.or.jp/members_site/KaiinStart

§ パスワードを忘れた方は、以下のページに進んでください。



§ 会員サイトでは、理事会議事録の閲覧などができます。

§ 会員情報変更画面で、会費納入日やCSA/ASA更新日の確認などができます。

（入会年月日は工事中で、表示されない場合があります。）

この画面で、住所変更、所属変更、メールアドレスの変更などができます。

以上

（SAAJ事務局）

会報編集部からのお知らせ

1.会報投稿記事 2010 / 2011 アワード開催　受賞者報告
2.会報への投稿記事募集
3.コメントを投稿される方へ

■□■ 会報投稿記事 2010/2011 アワード開催のお知らせ　（報告）

12月号で案内しましたように、次の通り、会員の投票形式により、受賞記事を選びました。受賞されたかたは、2月の総会で記念品を贈呈します。アワードの実施に伴い、従来の図書カード配布方式は、なくなります。

対象投稿記事

2011 年会報アワード　:2011/1-12 までの会報に掲載された記事を選定の対象とします

会員の投票による選出３点

減災：事業継続監査の観点から　（めだか、受賞者名は当日公表）
東日本大震災を体験して　（高橋典子さん）
保証業務に係る調査研究と保証型システム監査の一考察　（榎本吉伸さん）

2010 年会員の投票による選出２点

失敗を通して学んだシステム監査の勘所　/　システム監査の専門家　（めだか　同点）
第 152 回月例研究会（IT 分野の会計検査）　（細野浩一郎さん）

選定方法　:

2011 年12月31日 23:59 を締め切りとする、投票をおこなった。その結果（得票順）、上位から選出。
投票には、SAAJ の会員が1票を投票できます。期間内に投票された投票を単純集計して判定した。

投票期間:

12/1 より 12/31　の 23:59 まで

□■ ２．会報への投稿を募集

会員の皆様からの、投稿を募集しております。分類は次の通りです。

１．めだか　（Word の投稿用テンプレートを利用してください。会報サイトからダウンロードできます）
２．会員投稿　（Word の投稿用テンプレートを利用してください）
３．会報投稿論文（論文投稿規程があります）

これらは、いつでも募集しております。 気楽に投稿ください。
特に新しく会員となられた方（個人、法人）は、システム監査への想いやこれまで活動されてきた内容で、
システム監査にとどまらず、IT 化社会の健全な発展を応援できるような内容であれば歓迎いたします。

次の投稿用アドレスに、テキスト文章を直接送信、または Word ファイルで添付していただくだけです。
投稿用アドレス:saaj-kaihoh ☆ yahoogroups.jp （☆は投稿時には@に変換してください）

会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します。

□■ 3. コメントを投稿される方へ

気にいった記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。
コメント記入、投稿は、気になった記事の下部コメント欄に直接入力し、投稿ボランをクリックするだけです。
動画でも紹介しますので、参考にしてください。
（ http://www.skansanin.com/saaj/ の記事、「コメントを投稿される方へ」 ）

会員限定記事

【本部・理事会議事録】（会員サイトから閲覧ください。パスワードが必要です）

＝＝

■発行：　NPO 法人　日本システム監査人協会　会報編集部
〒103-0025　東京都中央区日本橋茅場町２－８－８共同ビル６F
■ご質問は、下記のお問い合わせフォームよりお願いします。
【お問い合わせ】　http://www.saaj.or.jp/toiawase/
■送付停止は、購読申請・解除フォームに申し込んでください。
【送付停止】　http://www.skansanin.com/saaj/

■□■ＳＡＡＪ会報担当━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
編集： 竹下和孝、仲　厚吉、安部晃生、成 楽秀、桜井由美子、清水恵子、山田 隆、片岡 学、
木村陽一、藤野明夫　　投稿用アドレス：saaj-kaihoh☆yahoogroups.jp（☆は安全対策）
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━