特定非営利活動法人
日本システム監査人協会報

2015 年 2 月号
No 167

No. 167（2015 年 2 月号）＜1 月 25 日発行＞

久々に投稿論文を掲載いたしました。BCP の大きな課題を解決するアイデアです。是非、ご一読を！

2015 年 2 月 20 日 13 時 30 分から、通常総会が開催されます。詳しくは、「協会からのお知らせ『第 14 期通常 総会のご案内』」をご覧ください。

マイナンバー事業者ガイドラインが公表されました。「注目記事」をご覧ください。

蝋梅

巻頭言

『６ヶ月で構築する個人情報保護マネジメントシステム実施ハンドブック』刊行

会員番号 1760 斎藤由紀子（事務局長 副会長 個人情報保護監査研究会主査）

当協会では、1998 年に「情報システム監査実践マニュアル」を刊行して以来、2005 年「情報システム監査実践マニュアル 第 2 版」、2006 年『個人情報保護マネジメントシステム実践マニュアル』（「PMS 実践マニュアル」と呼ぶ）、2008 年 2 月「J-SOX 対応 IT 統制監査実践マニュアル」を刊行しており、今回『6ヶ月で構築する個人情報保護マネジメントシステム実施ハンドブック』（「PMS 実施ハンドブック」と呼ぶ）は、約 7 年ぶりの刊行である。

（出版案内：http://www.saaj.or.jp/shuppan/ ）

「PMS 実施ハンドブック」は、2010 年 4 月に「PMS 実践マニュアル」の簡易版をめざして検討をはじめた。対象として中堅企業を想定し、日常業務に追われる事業者は、プライバシーマークを取得しなければならないとしても、本をじっくり読んでいる暇はないだろうという前提で、推奨版の「3301 個人情報取扱規程」と「3430 安全管理規程」を核とした 70 様式を策定した。構造は 2 年ほどで完成し、その後セミナーやコンサルタントで事業者に紹介していったが、事業者は、本書添付の様式を見て、「このように作ればよいのか」と理解してくれる。すると「解る」ことが快感となり、どんどん「自分ひとりで解っていかれる」ことに驚く。出版を担当してくださった同文館の担当者の方も、校正を重ねるうちに、個人情報保護管理者になれるほどの知識を持たれたのに驚嘆した。我々が目指したのはそういうことだったので、この本を読まれる方の頭の中に、どんどん PMS のイメージが出来上がってきて、楽しみつつ PMS を構築されることを期待している。

これまでご協力いただいた事業者の方々と、同文館のご担当者に深く感謝申し上げたい。

＜目次＞

各行から Ctrl キー+クリックで
該当記事にジャンプできます。
（各記事末尾には目次へ戻るリンク有）

＜目次＞

2015.1

投稿論文 【IT-BCP の実効性を高める訓練･演習とその監査】

会員番号 0283 松井秀雄 （近畿支部 BCP 研究プロジェクト）

IT-BCPを策定しただけの状態は、あたかもコーディングができただけで単体テストや統合テストを一度も行っていないソフトウェアの状態に似て、考慮漏れや記述ミスなどが存在する可能性が強い事から、有事の際に機能しない可能性が強い。当論文では、IT-BCPが有事の際に機能する「実効性」を高めるための方策とその監査について考察を行うものである。

1．IT-BCPの実効性を高めるためにISOや各種ガイドラインで推奨されている事項

1.1 BCPに関係するISO での要求事項

BCP に関する ISO としては、ISO22301 があり、策定した事業継続計画(以下 BCP と略記)の実効性を検証する要求事項として「8.5 演習およびテスト」がある。

また、IT-BCP に関する ISO として ISO27031［注 1］があり、その中で実効性を高める取り組みとして、「7.5 意識・能力の向上、および訓練プログラム」があげられている。

いずれのISOにおいても、BCPの実効性を検証する手段として訓練・演習・テストが期待されている。

［注 1］ ISO/IEC 27031 : Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity

1.2 各種ガイドラインでの推奨事項

多くの省庁から BCP に関するガイドラインが公開されているが、代表的な例として経済産業省のガイドラインと総務省のガイドラインで IT-BCP の実効性を高めるために何が推奨されているかを次に確認する。

経済産業省から平成 24 年に公開された「IT サービス継続ガイドライン・改訂版」では、「5.4 テストと監査」の目的として、「IT サービス継続計画の有効性を確認するとともに、IT サービス継続マネジメントが正しく維持されているかを確認するため」と記載されている。ここから、IT-BCP の「有効性」を確認する手段として「テスト」、「IT サービス継続マネジメントの維持」を確認する手段として「監査」が有効と考えられている。

総務省から平成20年に公表された「地方公共団体におけるICT部門の事業継続計画(BCP)策定に関するガイドライン」に次の記述がある。

「ステップ 7:ICT 部門内の簡易訓練」の【必要性】:

策定した初動計画をはじめとした計画が非常時に有効に機能するためには、定期的に訓練を実施して、職員等関係者が計画どおりに行動できるようにすることが必要不可欠である。また、計画の実効性の確認や改善のためにも必要である。

「ステップ 16:本格的な訓練の実施」の【必要性】:

「策定した業務継続のための行動計画や事前対策が非常時に有効に機能するためには、定期的に訓練を実施して、職員等関係者が理解を深め、計画どおりに行動できるようにすることが必要不可欠である。

ステップ 7 で実施した訓練に加えて、より高度な訓練を実施する。

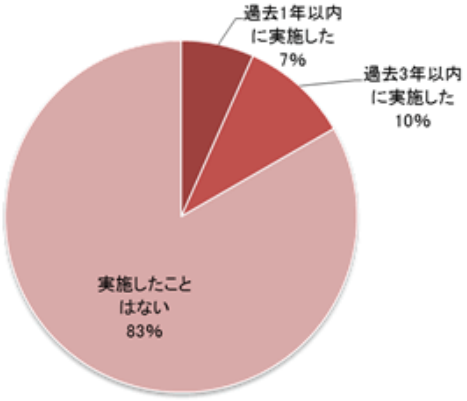
以上に見てきたとおり、ISO やガイドラインの中でも訓練・演習・テストの重要性が記述されており、BCP の実効

性を確認し改善を進めるために「訓練・演習・テスト」が有効な手段と考えられている。

2．IT-BCP の訓練・演習に関する世間の取り組み状況

2.1 民間企業の状況

IT-BCP の訓練：本番機の停止を伴う IT-BCP の訓練を実施していますか？（回答企業数：30 社）



IT-BCP の訓練：ユーザー部門などを巻き込んで IT-BCP の訓練を実施していますか？（回答企業数：30 社）

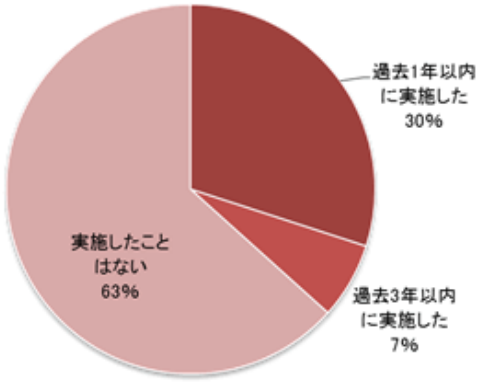


図 1 民間企業の IT-BCP 訓練の実施状況

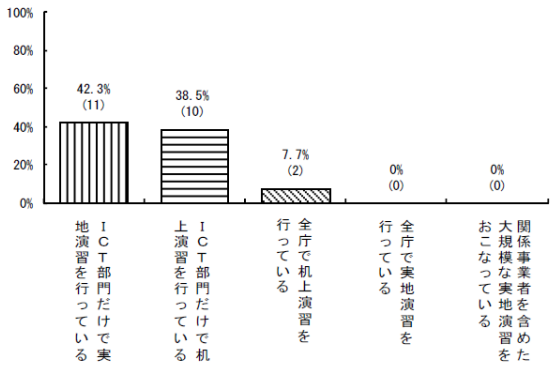
出典：「IT-BCP サーベイ 2013」プライスウォーターハウスクーパース株式会社 2013 年

IT-BCP を策定した後、本番機を利用した訓練を実施していない企業が 8 割を超えており、ユーザー部門を巻き込んだ訓練を実施していない企業は 6 割を超えるなど、実効性を確保するための訓練が殆ど実施されていない実態がうかがえる。

このような状態で有事を迎えた場合、極めて悲惨な状態になるかは明らかであろうと思われる。

2.2 自治体の状況

都道府県（策定している 26 団体中）



市区町村（策定している 188 団体中）

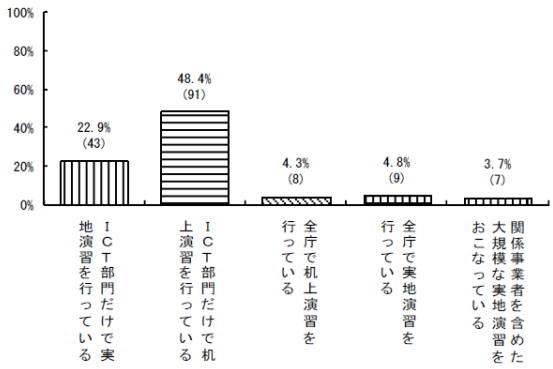


図 2 自治体の情報システムに関する業務継続訓練の実施状況

出典：「地方自治情報管理概要 電子自治体の推進状況」 総務省 （平成25年4月1日現在）26 年 3 月公表

図2に示すごとく、IT-BCP を策定できている自治体の中で、策定した IT-BCP の訓練・演習を行っている自治体は半分に満たない状況である。

2.3 訓練・演習が行えない理由の調査

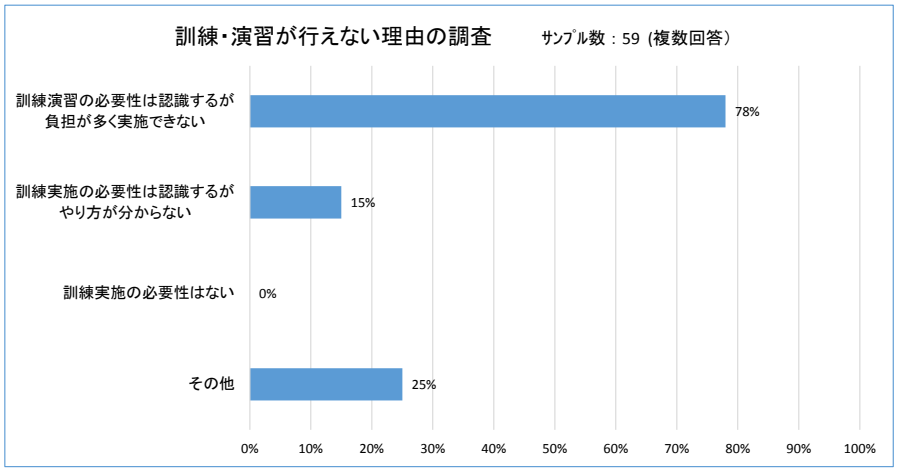


図 3 自治体で IT-BCP 訓練が行えない理由の調査

出典「災害発生時の業務継続及び ICT の利活用等に関する調査にかかる補足調査」総務省 平成 24 年

訓練・演習が行えない理由を調査した上図から、「負担が大きい事」、「やり方が分からない」という理由が大勢を占めている。また、「その他」と回答された自治体からのコメントの中に、「本番業務システムに対する影響」を懸念して次のような理由が上げられている。

・実機訓練の場合、本番運用への影響・調整や、訓練によるトラブルの発生のリスクがある。

・訓練中の操作により予想外のトラブルが発生し、通常業務に影響が出る懸念がある。

・情報機器はほぼすべての業務に関係しており、訓練の実施により停止する業務が発生し、市民サービスに影響するため困難である。

これらの状況を踏まえると、「負担が少ない訓練・演習の方法」や「本番業務に影響を与えない訓練・演習の方法」を周知できれば、訓練・演習を実施する組織が増えるものと期待できる。

3. 訓練・演習・テストを行うことで得られた気付きと改善

テストの種類は、IT サービス継続ガイドライン・改訂版（経済産業省）の「5.4 テストと監査 表 5.4-1 テストの種類と概要」で次のように記述されている。

表1 テストの種類と概要

テストの種類	実施内容	メリット	デメリット
机上チェック	・計画の内容をレビュし、不具合を修正する。 ・計画に定めた各種内容の有効性を検証する。	早期に実施可能であり、事業への影響が少ない。必要要員も最少である。	対応能力の向上や対応手順の良否の検証は難しい。
ウォークスルー	・計画に定めた各種内容の有効性を検証する。	早期に実施可能であり、事業への影響が少ない。必要要員も最少である。机上チェックよりも、より末端の対応手順を検証できる。	計画自身の整合性の検証が中心であり、計画発動時の具体的な課題提示は難しい。

テストの種類	実施内容	メリット	デメリット
シミュレーション	・計画発動時に予想される状況を前提として、計画の実行に必要かつ十分な情報が記載されていることを確認する。	状況を与えることで、より深い計画の検証を行う。あらかじめ与えられた状況内であるが、これに沿って例えば対応チームごとに対応手順内容を検証できる。	必要要員は多くなる。
ロールプレイング	・テスト実施の途中で状況を追加付与し、参加者の状況判断や意思決定の可否、連絡体制などを検証する。	計画を実行する判断者の訓練になり、判断資料の手当てなどが確認できる。	想定状況を多数設定するため、事前準備の負荷は大きい。参加者の十分な知識も必要となる。必要要員は多い。
実機訓練	・実際の設備などを用いたテストを実運用及び実作業で行えることを検証する。	代替施設や設備に関して実際の手順を適用し、実効性の有無を確認できる。代替システム切り替えなど実際の手順を経験できる。	業務に影響する可能性があり、周到な準備が必要である。現場レベルで多数の要員確保も必要となる。

出典:IT サービス継続ガイドライン・改訂版 経済産業省

この内容は、ISO 22301:2012 の「用語の定義 3.18 演習」や ISO/IEC 27031 の「7.5 Awareness, competency and training program」に相当するものである。

上記4つが机上で行う訓練・演習に該当し、5番目が実機を使うものである。

中でも、「ロールプレイング」の項目に、「テスト実施の途中で状況を追加付与し、参加者の状況判断や意識決定の可否、連絡体制などを検証する」とあり、「予期せぬ事態」への対応能力の向上が考慮されている。

3.1 実機テストで得られる気付きと改善

筆者は次のような実機使用障害回復テストを経験した事がある。

① 2センター間の代替テスト （主センターと代替センター間で基幹業務を代替できるかを確認）

② 1センター内で各種システム構成要素の障害を想定して代替機器による回復テスト

これらの訓練を通じて得た気付きと改善は次のとおりである。

・手順書の誤りや抜け漏れを発見でき、修正を行う事ができた。

・主センターで行った業務処理プログラムや関連手順の更新が代替センター側に反映されていない事が判明し、現時点の実運用に即応した内容に変更できた。

・操作員が経験を蓄積できた。

・2度目以降は操作への不安感が少なくなり、人的ミスが減少した。

・初期のテストほど予定外の事象が起きやすいため、色々な経験ができた。

・システムソフトの不具合を発見でき、修正を行う事ができた結果、システム自体の問題が減少した。

3.2 机上テストで得られる気付きと改善

筆者が机上で行う訓練・演習の良い手法を探していたところ、DIG という手法が一部の業界で使われている事を知り、それを IT 版にアレンジする事を思いついた。以下にその適用方法と得られた知見について述べる。

3.2.1 DIGとは

DIG とは、Disaster Imagination Game の頭文字をとって名付けられたもので、1997年に当時三重県消防防災課に勤めていた平野昌氏、他、数氏の協力で開発されたものであり、一般市民が独力でも企画・運営できる簡易型の防災図上訓練ノウハウである。参考資料として次のものがある。

「市区町村による風水害図上型防災訓練の実施支援マニュアル」

http://www.fdma.go.jp/neuter/topics/houdou/h23/2305/230525_1houdou/02_houdoushiryou.pdf

3.2.2 DIGのITへの適用

オリジナルの DIG では、「自然条件の確認」～「都市構造の確認」～「人的・物的防災資源の確認」～「災害に対する強さ弱さの理解」という段階を経た検討を行い、自組織の災害に対する強み・弱みを把握する。 これを IT 環境に置き換えて、「外部インフラの把握」～「内部インフラの把握」～「人的資源・IT 資源の把握」～「災害に対する備えあるもの・ないものの理解」という段階を経て検討を進めるというアイディアを筆者が考案した。その内容を整理したのが次図である。

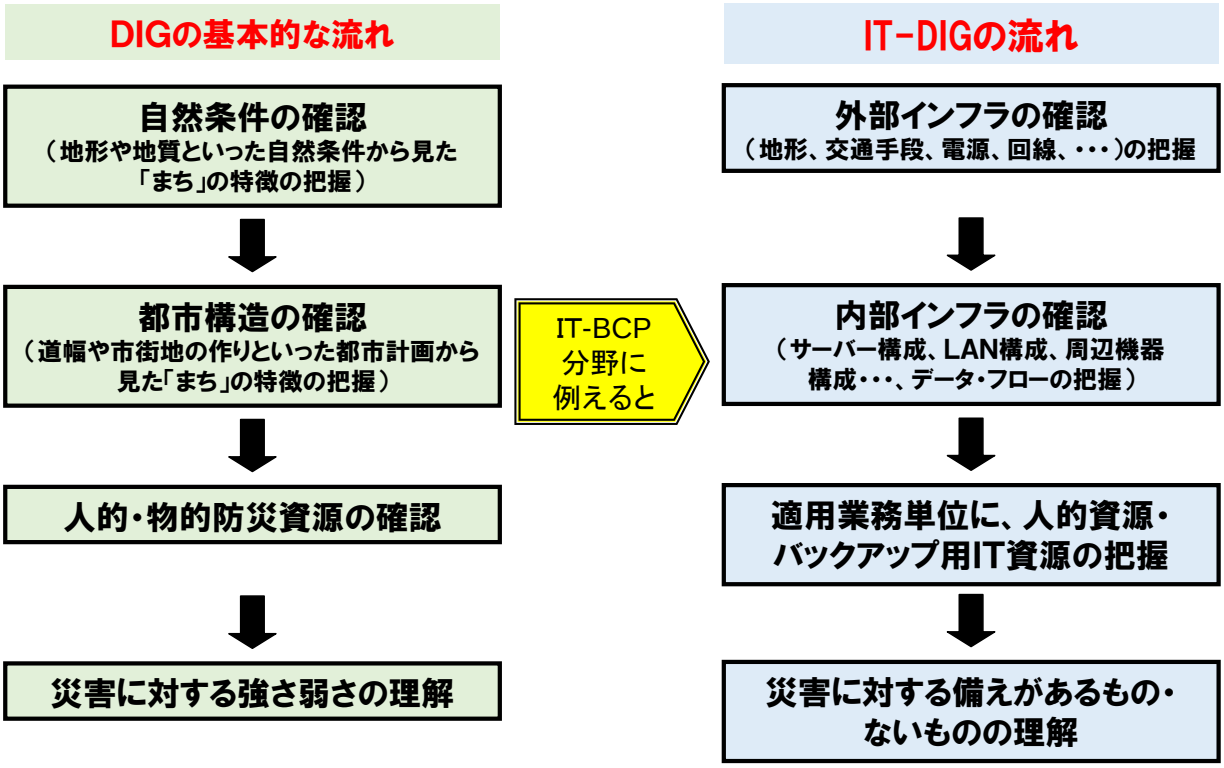
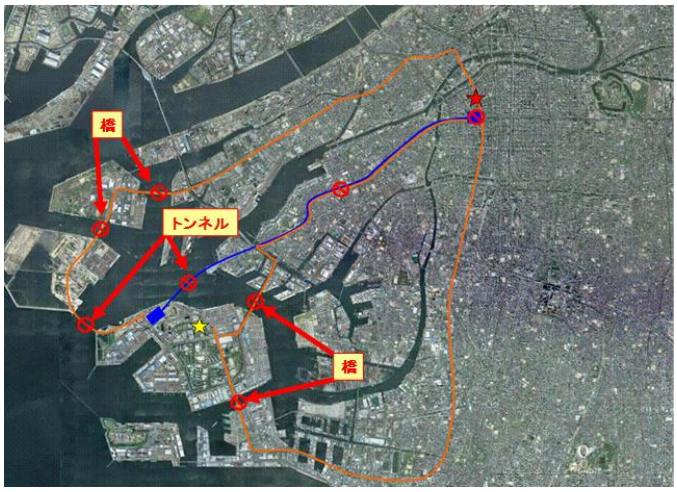


図4　オリジナル DIG をヒントに考案した IT 版 DIG の流れ

筆者のこの着想をもとに、全国IBMユーザー研究会の下部組織である関西IT研究会（平成23年度T3チーム）のメンバー7人と共に適用事例の検討を行った成果を以下に示す。なお、図5と図6の著作権、所有権は全国IBMユーザー研究会連合会（全国研）に帰属する。

3.2.3　外部インフラの確認

システム部門の主要メンバーは通常本社ビルに勤務しており、本社ビルは大阪市内中心部にある。一方、電算センターは大阪南港にあり、運用担当メンバーだけが勤務している。 有事の際にシステム担当部署の主要メンバーが電算センターに駆けつけて現場で指揮をとれるかどうか地図を使って検証してみた。

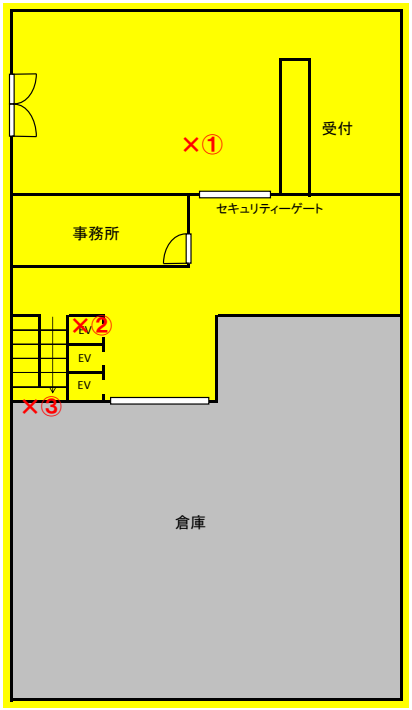


＝リスクのある場所

図5　電算センターへのアクセス・ルートの検証

その結果、電算センターへ行くルート上に「橋」や「トンネル」が多数あり、災害によってこれらの「橋」や「トンネル」が通行止めになると現場に駆けつけることが極めて困難になる事が判明した。

3.2.4　内部インフラの確認



①入館（セキュリティゲート）
被害の想定＞緊急時の入館方法が知らされていない
対応策　　＞ビル管理側に確認

②エレベータ
被害の想定＞緊急時にはエレベータが使用不能になる
対応策　　＞階段を利用

③階段
被害の想定＞階段の広さが解らないと、機材搬入に利用できるかが解らない
対応策　　＞階段、踊り場の広さを確認

④消火装置
被害の想定＞ハロンガス消火装置があるため、動作時には入室が出来ない
対応策　　＞入室可能になる時間を確認

図6　電算センター建物への出入りとフロアー間移動ルートの確認

次のような事項が主な確認事項となる。

・電算センターや本社ビルの標高　（海抜何メーター）
・自家発電装置の有無や設置場所の標高　（海抜何メーター）
・自家発電装置の許容時間
・外部からのネットワークの接続場所
・有事の際の建物への入退館や移動の可否　（この点に関する検討資料を図6に示す）

緊急時の入館方法が知らされていない事や機材の搬入ができるか否か分からないなど、この検討をするまで気が付かなかった不安要素が次々判明した。

3.2.5 人的資源の確認

電算センター内で復旧に従事する要員や、本社内にいて情報システム部門として復旧に従事する要員が最低限、何人必要なのかを確認した。 このような検討はかつて実施した事が無かったが、IT-DIGの一連の検討の中でその必要性に気付いて実施できた。

3.2.6 バックアップ用IT資源の確認

機器構成図と予備機資料を元に適用業務単位に、電算センター及び本社事務所内のバックアップ用IT資源の確認を行う。

① 予備用機器など復旧に必要な機器の準備状況

② 機材の移送・搬入出は可能か

その結果、次の事が確認できた。

①予備機器が用意されていないもの:

一部のネットワーク機器、LANケーブル、電源ケーブル、電話線、テーブルタップ等

②電算センター内、事務所内は複数の搬入出経路があり、近隣階層にあるため搬入出は可能だが、拠点間の移送は交通上の問題でリスクが多く、現実的ではない。

⇒ 拠点内に準備がない予備機器が必要になった場合は、復旧が予定通りに進まない可能性(リスク)がある。

3.2.7 災害に対する備えがあるもの、ないものの理解

・複数の対応策が考えられる場合、「判断基準」をできる限り明確化しておく必要がある。同時に「判断する人」(指揮命令系統)も明確化しておく必要がある。

→例えば、「データセンターに連絡がつかず状況が不明な場合や、○時間経過した時点で交通手段が復旧しない場合、A案は諦め、B案に移行する」など

・意外に「外部環境」に不安要素が多い事が分かった。

→自社で復旧対応できない不安要素に関しては、代替案を事前に用意しておくべき。

・手順書等の保管先に関しても災害時の被害を想定した上で決定したほうが良い。

→緊急時の連絡網(取引先一覧やベンダーの連絡先など)も手順に含められているべき。

3.2.8 IT-DIGを行って得られた気付きのまとめ

IT-DIG を使って検討した結果得られた気付きは次のとおりである。

・外部インフラを含めて可視化することにより、従来からの手法でコンピュータ資源や手順書だけに注目していた時よりも広い視野で検討が行える様になった。その結果、意外に「外部環境」に不安要素が多い事が判明した。

・IT-DIG 手法により可視化された材料がある事で、詳細な業務内容や機器構成を知らないメンバーでも全員参加の議論ができるようになった。

・複数の対応策が考えられる場合、判断基準をできる限り明確化しておく必要がある。
更に、「判断する人」(指揮命令系統)も明確化しておく必要がある。

・視野広く検討するには好適な手法との印象を得た。

・実機を使わない事に起因した限界がある。
例:代替機への切り替えに要する時間の測定できない。
手順書に書かれた入力コマンドのスペル・ミスを発見できない。

情報システムを取り巻く外部環境の構成要素は、図7にあるとおり多岐にわたる。

これらの構成要素が与える影響について実機を使って確認するのは困難である一方、IT-DIG の精緻化により検討できるのではないかと考えている。

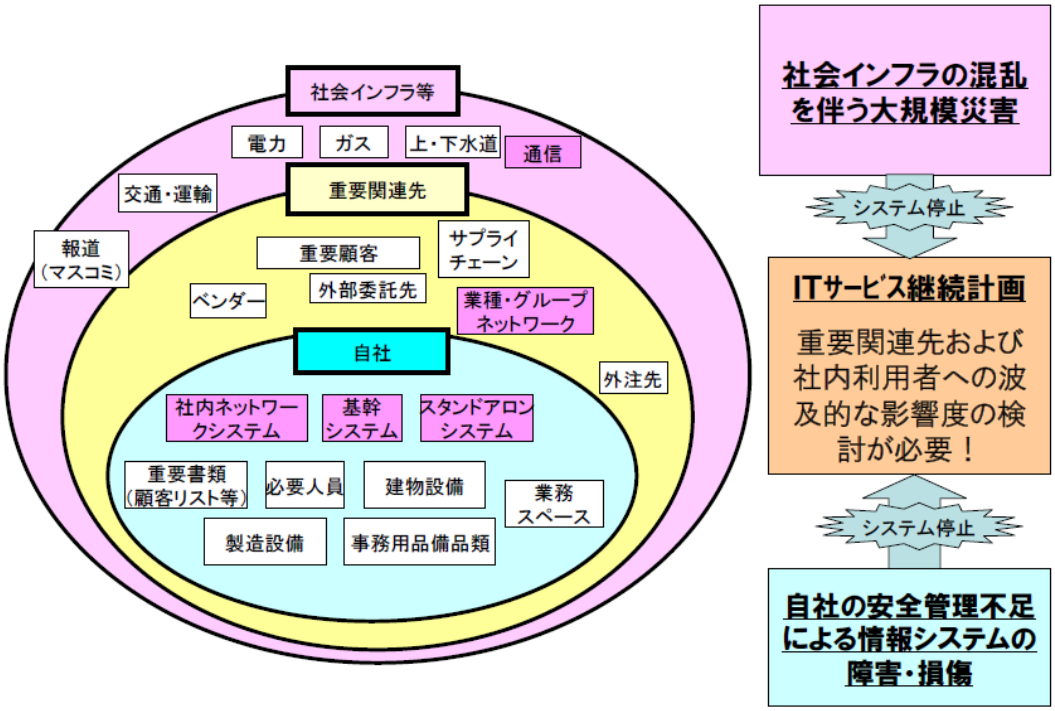


図7　情報システムを取り巻く社会環境と IT サービス継続計画

出典:IT サービス継続ガイドライン・改訂版　経済産業省

3.3　実機や机上の訓練・演習で得た改善効果のまとめ

イ. IT-BCP 文書の改善効果

・手順書の間違いを訂正できた。

ロ. IT-BCP を実施する人の成長効果

・実施作業の担当内容を経験することで、自分が果たすべき役割を会得できた。

・操作経験を重ねる事で操作への不安感がなくなり、ミスが減少した。

ハ. 情報システム自体の改善効果

・ソフトウェアの修正漏れが判明し対応できた。

・システム設定パラメーターのミスが判明し修正できた。

4．訓練・演習を行う事で生じるリスク

これまで、訓練・演習の効果について述べてきたが、良い事ばかりでなくリスクがある事も紹介しておく。

4.1　実機を使う場合のリスク

イ. 本番機を使う場合

・テスト後の本番稼働時に後遺症を残す可能性がある。

某金融機関で休日に本番機を使ったテストを実施した際、テストで行った為替送金取引データが翌日の勘定系処理に混入するという事件が発生した事がある。

ロ. テスト機を使う場合

・システム資源名称などが本番機との相違点があるため、手順の確認に限界があり、テスト機で確認したコマンド入力内容がそのまま本番機で使えるとは限らない。

・テスト機は一般的にシステム規模が本番機よりも小さいため、代替系への切り替え時間の測定ができない。

4.2 机上訓練だけの場合のリスク

実機を使わないと発見できないミス(コマンドのスペル・ミスなど)が存在し、確認できる事項に限界がある。

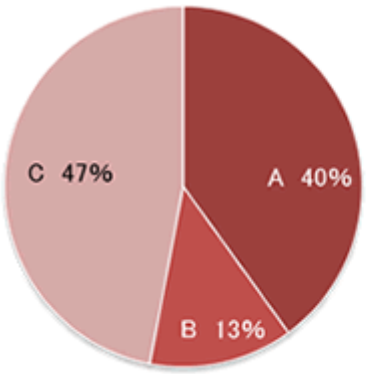
4.3 リスクのまとめ

「本番機を使う訓練」・「テスト機を使う訓練」・「机上訓練」いずれにもそれなりのリスクや限界があり、どれか一つのタイプの訓練だけで他の訓練をしなくて済むという訳にはならないので、リスクが小さく取組負担の少ない机上訓練から実機を使う訓練へ順次取り組むのが良いと考えられる。

5. IT-BCPの実効性に関するシステム監査を行う場合の視点

IT-BCP が策定されていても有事の際に本当に役に立つのかという不安を払拭するためにシステム監査人は公平中立な第三者としてその実効性について監査を行い、組織体の長に状況を正しく報告する必要がある。

内部監査部門は、IT-BCP の策定状況や訓練の実施状況などを監査していますか？
(回答企業数:30 社)



#	回答結果	%
A	内部監査部門は、IT-BCPの策定状況や訓練の実施状況を定期的に確認している。	40
B	内部監査部門は、過去にIT-BCPの監査を行ったことはあるが、不定期である、または、それほど重視していない。	13
C	内部監査部門は、過去にIT-BCPの監査を行ったことはない。	47

図8 IT-BCP に関する監査の実施状況
出典:「IT-BCP サーベイ 2013」プライスウォーターハウスクーパース株式会社 2013 年

内部監査部門においては、「過去に IT-BCP の監査を行ったことはない」と回答した企業は、47%と約半数を占めている。システム監査人が IT-BCP の策定状況や訓練実施状況を確認することは、IT-BCP の実効性改善に有効であるため、今後の改善が望まれる。

5.1 「システム管理基準」の中でBCPの実効性監査に関係する主な事項

システム管理基準の中で事業継続計画に関する記述が Ⅰ. 情報戦略 5. 事業継続計画 にあり、その「趣旨」を踏まえて、実効性監査にどのように関係するのかを確認しておく。ここに記載した「趣旨」は、次の資料から得た。

「趣旨」の出典 :「システム管理基準の管理項目と統制目標の対応(例)【Excel 形式】」 経済産業省
http://www.meti.go.jp/policy/netsecurity/downloadfiles/appendix_2.xls

イ. 組織体の長の承認

(以下、括弧付き数字は、システム管理基準の管理項目、「Ⅰ. 情報戦略 5. 事業継続計画」の項番)

(2) 事業継続計画は、利害関係者を含んだ組織的体制で立案し、組織体の長が承認すること。

【システム管理基準の趣旨】:事業継続に関わる事象が発生した場合に全ての利害関係者が円滑に対応できるようにするため、利害関係者を含んだ組織体制で実行性の高い事業継続計画を立案し、組織体の長が承認する必要がある。

ロ. 従業員の教育訓練

(3)事業継続計画は、従業員の教育訓練の方針を明確にすること。

【システム管理基準の趣旨】:事業継続に関わる脅威が発生しても、迅速かつ確実に事業継続計画に定められた手続を実行できるようにするため、事業継続計画には従業員の教育訓練の方針を明確にする必要がある。

ハ. 関係各部に周知徹底

(4)事業継続計画は、関係各部に周知徹底すること。

【システム管理基準の趣旨】:事業継続計画の実行性を高めるため、事業継続計画を関係者に周知徹底する必要がある。

ニ. 見直しと更新

(5)事業継続計画は、必要に応じて見直すこと。

【システム管理基準の趣旨】:事業継続計画の有効性を維持するため、必要に応じて見直し及び更新を行う必要がある。

5.2 システム監査人が監査の際に確認すべき事項

上記 5.1 で「システム管理基準」における BCP の実効性監査に関係する主な事項を述べたが、システム監査人が BCP の実効性を監査する際にはそれらの事項を確認すべきと考え、以下にそのポイントを述べる。

イ. 組織体の長の承認

組織体の長が承認を与えた記録の確認

組織体の長が次のリスクを正しく認識した事を確認する。

・「訓練をするリスク・しないリスク」

・本番機を使うリスク・使わないリスク

・テスト機を使うリスク・使わないリスク

・机上訓練の限界

ロ. 従業員の教育訓練

・訓練参加者リストの確認

・訓練で得た気づきや課題点を整理した文書の確認

ハ. 関係各部に周知徹底

・関係部署の一覧リスト

・関係部署に周知した記録の確認

ニ. 見直しと更新

・IT-BCP 資料類が見直し・更新されている事の確認

・関係部署へ最新版が配布されている事の確認

6. まとめ

前記[図 1]で示したが、策定した IT-BCP について、「ユーザー部門を巻き込んだ訓練を実施したことはない」という企業が 60%以上あり、本番機を利用した訓練についても未実施の企業が 80%を超えるなど、実効性を確保

するための訓練・演習が十分に実施出来ていない現状がある。IT-BCP は、策定しただけでは有事の際に機能しない可能性が高く、訓練・演習を通じて見直しを適宜実施し、IT-BCP 自体の実効性を上げて行く必要がある。

しかし、前記[図 3]で示したとおり、訓練の必要性は認識されながら、「負担の大きさ」や「本番業務への懸念」のため訓練が実施されていないという現状がある。 その課題に対して、次の手順を提言したい。

① 比較的作業負担が軽く実機への影響が無い訓練として IT 版 DIG に取り組む。

② 次に本番業務への影響が無い実機訓練として「テスト機」を使った訓練に取り組み、机上訓練の限界をカバーする。

③ 最終的な確認として「本番機」を使った訓練に取り組み、テスト機による訓練の限界をカバーする。

このようにして訓練でカバーできる範囲を広げながら、可能な限り IT-BCP の実効性が高められて行く事を願っている。

以上

＜目次＞

2015.1

めだか　【マネジメントシステム内部監査におけるシステム監査人の役割】

マネジメントシステム内部監査におけるシステム監査人の役割を考えてみたい。

先ず、マネジメントシステムとは何か。management systemでネット検索すると、情報処理系の、入力系、処理系、出力系で構成されるシステム、データベース管理システム(DBMS)、ネットワーク管理システムなどがある。また、国際標準系の品質マネジメントシステム(QMS)、環境マネジメントシステム(EMS)、情報セキュリティマネジメントシステム(ISMS)や、個人情報保護マネジメントシステム(PMS)のように、一定の目標に向かって、Plan-Do-Check-Actを回して継続的改善を図るマネジメントシステムがある。

「マネジメントシステム内部監査におけるシステム監査人の役割」は、国際標準系のマネジメントシステムを回す際にCheckの要素の内部監査において、対象を情報処理システムとするシステム監査人の役割をテーマにしている。経済産業省システム管理基準に、Ⅵ. 共通業務 3. 品質管理が以下のように規定されている。

> 3.1 計画(2)
> (1)品質目標に基づいて品質管理の計画を定め、ユーザ、企画、開発、運用及び保守の責任者が承認すること。
> (2)品質管理計画は、方法、体制等を明確にすること。
> 3.2 実施(2)
> (1)業務の工程終了時に、計画に対する実績を分析及び評価し、責任者が承認すること。
> (2)評価結果は、品質管理の基準、方法、体制等の改善に反映すること。

情報システムの品質を管理する基準として、品質目標に基づいて品質管理の計画を定め、実施し、工程終了時に、実績を分析及び評価して、品質管理の基準、方法、体制等の改善に反映するよう規定している。過日、システム監査人は情報処理システム監査技術者としてホス・トコンピュータあるいはメイン・フレームの時代の情報処理システムを対象としていた。今や、情報処理システムは、ネットワークを通じて広く社会の基盤の一部になっていて、利用者はそれが情報処理システムであるとして特別に意識しないで利用している。つかみどころがないため、システム監査人の役割を規定することが難しくなってきている。情報処理システムという言葉も、情報技術(Information Technology)と言われるようになっている。

しかし、考えてみると、システム監査人は、情報処理システム監査を核にして、情報セキュリティ監査、内部統制監査、個人情報保護内部監査を渦巻きのように折り込んできた。マネジメントシステム内部監査におけるシステム監査人の役割というようにシステム監査人の役割を見直すと、新たにシステム監査人に期待される役割が見えてくる。

(空心菜)

(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。)

＜目次＞

2015.1

投稿【システム監査人の魅力】

会員番号 0557 仲 厚吉 （会長）

会報の年間テーマが、システム監査人の魅力 となりました。当協会ではシステム監査人の魅力を向上させるべく取り組んでおります。2015 年度の本部計画を次のようにご報告いたします。

2015 年度の協会運営の方向性として、システム監査の普及、促進活動の一層の推進のため、協会の信頼性を高めることを目的とした協会活動を行う。会員各位から寄附を頂いた実績をもとに東京都へ申請した「認定 NPO 法人」の認定を目指す。認定によって協会の信頼性、システム監査人の社会的評価の向上を図る。また、システム監査の活性化の一環として、IT-Audit 等の ISO 化、JIS 化、システム監査に関連する他団体との交流、会員とのコミュニケーション向上のためホームページの整備、会員ポータルサイトの導入を進める。IT ガバナンス（Corporate governance of information technology）、IT 人材の育成をテーマにシステム監査の活性化、システム監査人の活用を図る。

（1）2015 年度の協会事業について

協会事業の方向性は次の3点とする。

1）システム監査人の社会的評価の向上

「認定 NPO 法人」認定によって、公認システム監査人資格のブランド化を図る。

2）システム監査の活性化

システム監査活性化委員会の活動を中心にシステム監査を社会に必須のものとして活性化させる。

3）協会組織の充実

協会組織を整備し、会員の信頼に応えるよう体制を充実させる。また、世代交代に取り組む。

（2）システム監査の活性化の一環として、次の活動を行う。

1）IT－Audit 等、システム監査基準の ISO 化、JIS 化を推進する。

2）システム監査に関連する他団体との交流を進める。IT ガバナンス、IT 人材の育成をテーマにシステム監査の活性化、システム監査人の活用を図る。

3）会員とのコミュニケーション向上のため、ホームページの整備、会員ポータルサイトの導入を進める。

（3）2015 年度の予算編成について

2015 年度は、協会収支が「谷の年」で厳しい収支状況であることを考慮し、また事業活動についての考えに基づき予算を編成する。

1）編成方針

予算編成方針は、収益性とともに活動性をより重要とする。

2）事業活動

事業活動は、収支バランスを原則とする。収支は、公認システム監査人等認定事業収支が隔年上下変動することを考え、2年タームで取り組む。事業活動によっては、重要性や緊急性を考え例外を認める。

3）事務局

斎藤由紀子事務局長以下、事務局業務の効率化を図り、会員サービスの向上に取り組むとともに、会計（安部主査、藤澤理事、梅里理事）と協力して、協会の健全運営に努める。また、会員とのコミュニケーション向上のため、ホームページを整備し、会員ポータルサイトの導入に向け予算措置を講じる。

以上

＜目次＞

2015.1

第１９８回　月例研究会　（２０１４年１２月１６日開催）報告

会員番号 0056 藤野明夫（情報セキュリティ監査研究会）

【講演テーマ】 「企業におけるセキュリティ戦略」

【講師】日本アイ・ビー・エム株式会社　IBM Computer Security Incident Response Team (CSIRT)
IT Forensic Analyst　守屋　英一　氏

【日時】 2014 年 12 月 16 日（火曜日）18:30～20:30

【場所】 機械振興会館　地下 2 階ホール

【講演骨子】

本年3月、NTT 出版より「サイバーセキュリティ」という本を出版させて頂きました。 本書では、サイバー攻撃を社会的背景、技術的対策、法律および企業経営などの様々な視点から問題の解決に向けて解説しています。

本講演では、本書の内容を踏まえて、サイバー攻撃及び内部犯行による企業への影響に対して、企業が取り組むべきセキュリティ戦略について解説させていただきます。

・サイバー攻撃及び内部犯行の現状
・人的資源マネジメントが困難な時代
・多様なセキュリティ技術の存在
・企業におけるセキュリティ戦略

【講演概要】

１． 略歴

2001 年に、インターネット・セキュリティ・システムズに入社し、セキュリティオペレーティングセンターで、クライアント企業のネットワークセキュリティの監視業務に携わってきた。2007 年にインターネット・セキュリティ・システムズが日本アイ・ビー・エムに買収されたことにより、日本 IBM 社員となったが業務は継続した。2011 年に経営品質・情報セキュリティ推進室に異動し、現在、IBM Computer Security Incident Response Team（CSIRT）というチームに加わり、社内の不正アクセス事件への対応および ISMS 内部監査を担当している。また、明治大学ビジネス情報倫理研究所客員研究員、日本シーサート協議会運営委員及びインシデント事例分析 WG リーダー等の社外活動にも従事している。

２． 企業におけるセキュリティ戦略の必要性について

現在、IBM では、全世界を対象とした 24 時間の監視体制が敷かれている。これは、時差を利用し、各地域の監視員が、それぞれの地域が昼のとき、自分の地域と他の地域の監視をするというものである。

グローバル企業は常にサイバーテロの標的になっているという認識のもと、適切なセキュリティ戦略をとる必要がある。「戦略」という言葉を使ったが、企業における戦略とはなんであろうか。中央大学大学院　戦略経営研究科　遠山亮子教授は、企業における戦略を以下のように定義している。「『ありうべき姿』を達成するために自分の持っている経営資源と自分が適応すべき経営環境とを関連付けた地図とシナリオである。ただ、『正しい選択』がいつまでも正しいとは限らない。」

企業にとってセキュリティはコストとして認識されている。したがって、景気が悪いと圧縮対象になってしまい、景気が良くなるとそれを強化しようということになる。しかしながら、一度サイバー攻撃を受けると経済的損失や社会的信用の失墜等の経営上の甚大な被害を被ることになり、景気の変動によってセキュリティを強めたり弱めたりすることは許されない。一方、昨今、サーバ攻撃等の手口はますます巧妙化し、その対策に要するコストは増加する一方であり、すべてに対応することは困難である。そこで、企業にとって重要な資産はどれかを選定し、メリハリをつけたセキュリ

ティ対策への投資が必要になる。すなわち、前述の「経営資源と自分が適応するべき経営環境とを関連付けた地図とシナリオ」策定、すなわち、戦略的思考が必要になる。

以下、昨今のサイバーテロを筆頭とする種々のサイバー攻撃あるいは内部不正の動向と、これらの脅威に対してどのようなセキュリティ戦略を策定すべきかを解説する。

３． サイバー犯罪の動向

最近のサイバー犯罪の動向について、説明する。

３．１ サイバー犯罪の増加

近年、サイバー犯罪が増加している。最近、日本で発生した重要な二例をご紹介する。

通信教育の某社は、今年 7 月に子会社が内部犯行による数千万件の顧客個人情報漏洩事件を起こしたために、その経営に重大な影響が出てきている。この会社では、2015 年 3 月期連結決算の税引き後利益が補償等のため、90億円～10億円の上場以来初の赤字となる見通しを発表した。

また、外部からの攻撃により、顧客情報が盗まれる事件が相次いで発生した。これは、その会社自身のコンピュータが直接ウイルスに感染したのではなく、顧客である利用者のコンピュータにウイルスが感染し、ID/パスワードが盗まれ、それにより不正アクセスが行われた。

企業本体ではなく、子会社の内部犯行や顧客側のセキュリティ対策の不備により、顧客情報が盗まれ、当該企業が大きな損害を被っている。

３．２ サイバー犯罪増加の原因について

近年、社会環境の変化、技術の進歩等により、犯罪が発生する要因が増加している。ここで、どのようなときに犯罪が発生するかということを説明した「日常活動理論」と呼ばれるものをご紹介する（表 1 参照）。

表 1 日常活動理論

	動機・目的	背景・原因
動機づけられた犯罪者	＜金＞ 金銭的動機、経済的動機 ＜怨恨＞ 上司への不満（評価、待遇、給与）、人間関係の不満、不当解雇	＜正社員＞ 終身雇用・年功序列の廃止、転職、起業 ＜非正規社員＞ 低賃金、雇用が不安定 キャリア形成の貧困化
潜在的な犯行対象物	＜情報＞ 機密情報（知的財産、営業機密）顧客情報、開発情報、従業員情報 ＜システム＞ システムの破壊、システムの悪用	＜電子データ＞ 情報が電子データ化されたことで、一度に大量の情報を持ち出すことが可能になった ＜システム＞ 分業化、専門家され、全体の把握が困難になっている
監視性の低い場所	＜社外＞ 外部委託先、アウトソーシング先 ＜ルール＞ ルールが存在しない ＜監視＞ 情報の管理が不十分 ルール違反しても処罰されなかった	＜社外＞ 経営の効率化が図られ、社外への業務移転が進んだ ＜ルール＞ ルールの陳腐化が早まっている ＜監視＞ 性善説を基本としているため、職務分掌が進んでいない

日常活動理論とは、「動機づけられた犯行者」、「適当な標的」、「有能な監視者の欠如」という三要素が重なり合うとき、犯罪が発生するという理論である。最近は、表1に示す通り、これらの三要素が重なり合う状況が増える傾向にある。

終身雇用が終わり、正規雇用でも転職することが多くなってきた。自身が作ったパワーポイントのデータを持ち出し、

自分の仕事を効率化するために、転職先でそのパワーポイントデータを使うデータの使いまわしが現実に起きている。

さらに、昔と違ってデータが持ち出しやすくなった。USB メモリにより、何万人もの顧客情報を簡単に持ち出すことができ、また、USB を使用しなくともクラウドサービスにデータをアップすることでも盗み出すことができる。USB を使わない、クラウドを使わないというルールがあるだけで、運用上のチェックが行われず、折角のルールが有名無実になっている企業もある。

無線LANに接続されたパソコンを通じてデータを社外に送信することを、ルール上、禁止していても、スマートフォンのテザリング機能によって持ち出されてしまうことがある。また、土日に自宅で仕事をするためにクラウドサイトにウェブメールでデータを送り、自宅でサイトからデータを取得し、作業実施後、サイトにデータを送り、月曜にその結果をウェブメールでサイトから戻して仕事を続けるということがある。これなどはウェブメールの ID/パスワードが分かってしまうと情報を抜き取られてしまう。

技術の進歩にルールが追いついていない面があり、陳腐化しないうちに早目にルールを決める必要がある。また、ルール化した後も、そのルールが遵守されているかチェックしていくことが必要である。

３．３　スマートデバイスと SNS による新たな脅威

スマートフォン、タブレット端末等のスマートデバイスの普及により、その業務利用と私的利用の境界の曖昧さによる新たな脅威が発生している（表 2 参照）。

トレンドマイクロ社の 2014 年 8 月 26 日のプレスリリースによれば、「あなたは個人所有のスマートデバイスを、業務のために利用したことがありますか？」という質問に対して、「利用する」と回答した割合が、2012 年に 48.0%であったのが、2014 年は 63.1%に増加している。

表 2　スマートフォンの利用目的

		利用内容	
		業務利用	私的利用
利用場所	社内	• ホワイトボードの撮影と同期 • 会議の録音と同期 • 名刺情報の登録	• SNSへの投稿 • アプリの利用 • ウェブメールの確認 • オンラインストレージの利用
	社外	・リモートアクセス 社内メールの閲覧・修正 業務データの作成・修正	

ホワイトボードの撮影、会議の議事録の録音をクラウドにアップすると、情報が取られるリスクがある。また、どこにいても顧客の情報を確認できる名刺情報登録サイトというサービスがあるが、一部のサービスでは名刺情報を登録すると、登録した相手に対して「誰々があなたを登録しました。あなたも登録しませんか」とメールが飛ぶことになっていて、登録したことが相手に分かってしまい、顧客の不信感を買う要因になりうる。

一番問題なのは、個人所有のデバイスについて、その内容を企業側が見たくても、従業員に拒絶されればそれ以上の強制はできないということである。たとえ従業者から一札取っていたとしても、拒絶されたらそれ以上の追求は現実的に不可能である。この対策としては、スマートデバイスを業務で使用する可能性がある場合、会社から貸与するしかなく、現実にそういう企業が増えている。

また、SNS（ソーシャルネットワークサービス）の浸透も新たな脅威になりつつある。従業員のプライベートな場での

発言であっても企業名をうっかり出してしまったり、また、その発言内容から企業名が特定できるような発言をした場合、その企業の内部情報の漏えいやその企業の見解と取られるおそれがある。これを規制するのはなかなか困難で、従業員に自覚を促すよう注意するしかない。

このように、技術の進歩によりリスクは拡大しつつある。

３．４　不正送金の増大

最近、ネットバンキングにおける不正送金が増加している。とくに、法人口座からの不正送金の増加が著しい。警察庁の発表では、2013 年上期に 213 百万円であったものが 2014 年上期には 1,852 百万円と一年で9倍も増加している(表 3 参照)。中小企業が被害に遭うと資金繰りができず廃業に追い込まれる可能性があり、深刻な問題である。

表 3　平成 26 年上半期のインターネットバンキングに係る不正送金事犯の発生状況について

期間	件数	被害額
Ｈ２６上	1,254	約 18 億 5,200 万円（約 148 万円/件）
Ｈ２５下	1,098	約 11 億 9,300 万円（約 109 万円/件）
Ｈ２５上	217	約 2 億 1,300 万円（約 98 万円/件）

出典:警察庁「平成 26 年上半期のインターネットバンキングに係る不正送金事犯の発生状況について」、2014.9.4
http://www.npa.go.jp/cyber/pdf/H260904_banking.pdf

不正送金は組織的に行われている。不正送金の手口を以下に示す（図１参照）。

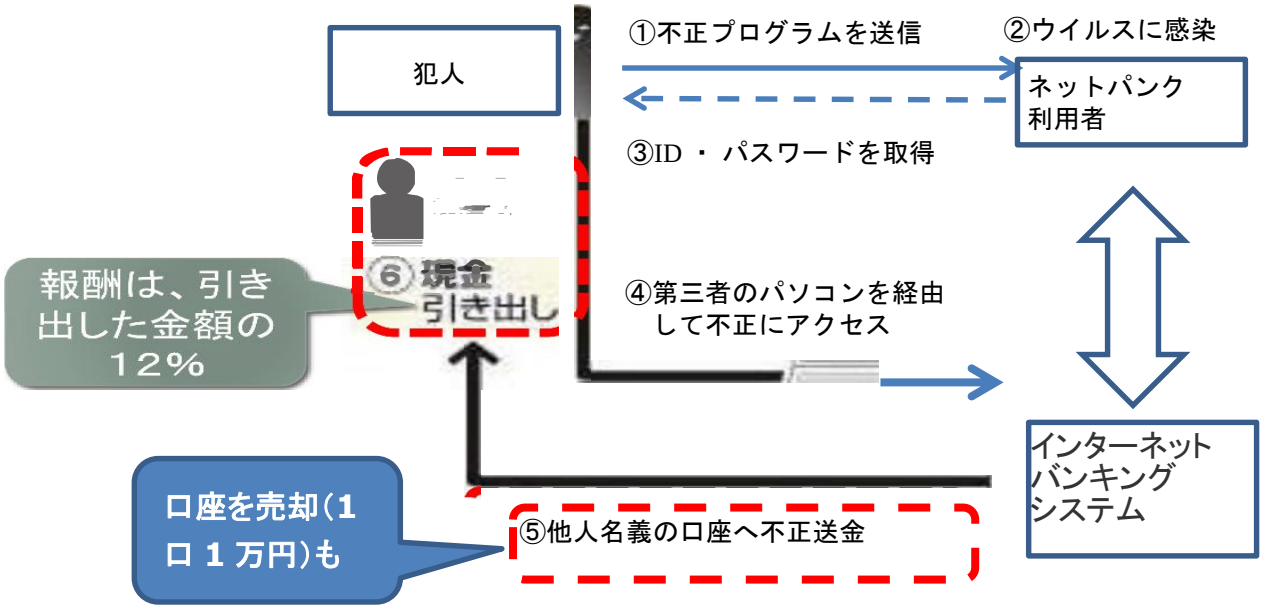


図1　不正送金の手口

①犯人からネットバンク利用者に不正プログラムを送信、②ネットバンク利用者がウイルスに感染、③犯人がＩＤ /パスワードを取得、④犯人が第三者のパソコンを経由して不正にアクセス、⑤ネットバンク利用者のインターネットバンキングシステムから他人名義の口座へ不正送金、⑥犯人による現金引き出し。

報道によると、口座が１口１万円で売られており、引き出した金額の１２%が出し子の報酬になっているそうである。

金融機関でも、ワンタイムパスワードの使用等対策を打ってはいるが、まだまだ、被害は拡大している。

海外の事例では、不正送金の発見を遅らせるために送金データを改ざんするという手の込んだ手口の犯罪が発生している。その手口は以下のとおりである(図 2 参照)。①ウイルスに感染した顧客が、②正規の手順でオンライン・バンキングへアクセスし、③「A社に 1 万円送金」の指示をするとウイルスに感染した Windows の API が、指示内容を「B社に 10 万円の送金」に改ざんする。「B社に 10 万円の送金完了」のメッセージを受け取ると、ウイルスに感染した Windows の API が、再び、そのメッセージを元の指示内容と同じ、「A社に 1 万円の送金完了」のメッセージに改ざんする。

これにより、顧客は、正しくA社に 1 万円が送金されたと思いこんでしまい、不正送金に気付くのが遅れる。

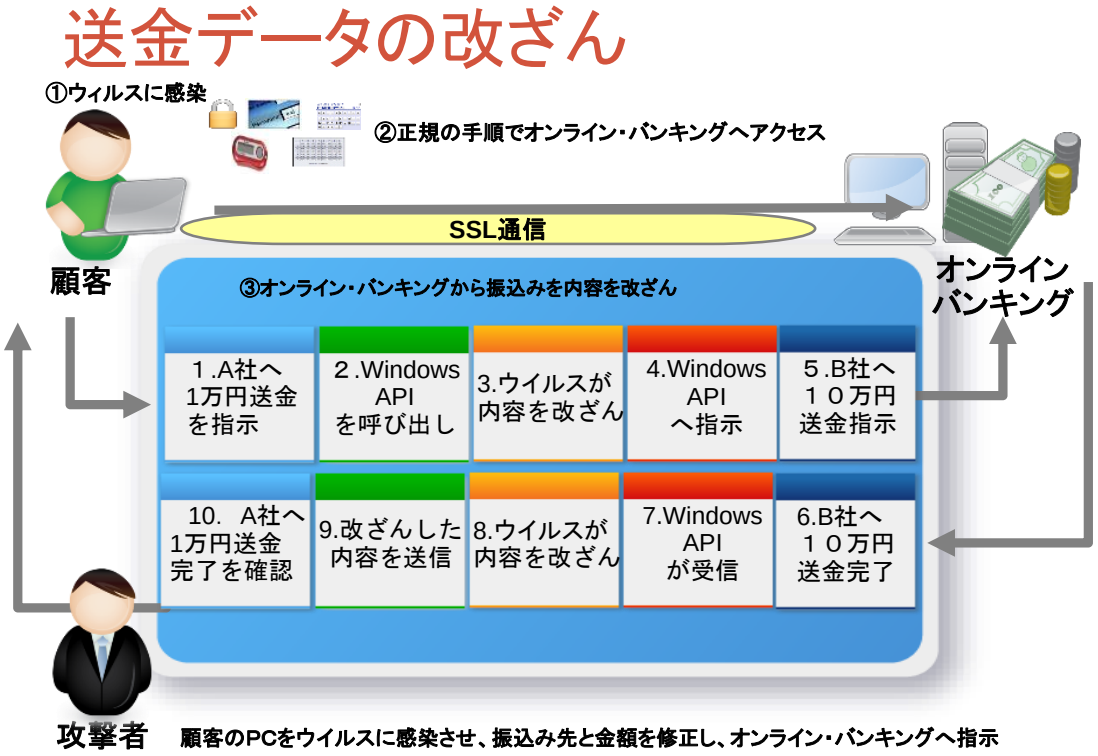


図 2　送金データの改ざん

３．５　サイバー攻撃の目的の変化と高度化及びそれ生む背景

サイバー攻撃の目的が変化し、それにともない手口が高度化している。

2001 年ごろから始まったサイバー攻撃は、当初は愉快犯であった。その内容は DDOS 攻撃、ハクティビズム(政治的社会的な主張を行うためのハッキング)という比較的分かりやすいものであった。2003 年ごろから、金銭目的のサイバー攻撃が行われるようになってきた。しかし、そこで用いられる手法は、無差別なウイルス配布やスパムメール等、適切なツールを導入すれば検出、予防可能なものであった。ところが 2007 年ごろから始まった情報搾取は、標的型攻撃、APT 等、攻撃中の検知はもとより、攻撃を受けた後でも、攻撃を受けたことすら認識できないほど、極めて高度な手法を用いるものも多くなってきた。これらの高度な攻撃の中には、その攻撃がなかったことを証明することができないものもある。このような状況のなかで情報セキュリティ担当者は、毎日、不安な日々を送っている。さらに最近は、サイバーテロ、サイバー戦争といわれるほど、高度かつ広範で破壊的な攻撃も表れている。

これらの高度かつ影響の大きなサイバー攻撃が発生する要因には、技術の発展とグローバル化に加え、あらゆる面で責任の分界点が曖昧になってきたことがあると感じている。かつては、情報システムは機器もソウトウェアも運用

要員も自前が当たり前であったが、近年、クラウドサービスやビジネスプロセスアウトソーシング（以下、「BPO」）が普及してきた。2013 年にはクラウドサービスの利用率は 33%に達し、BPO の売上は、4 兆円にもなっている。自前の世界では全てがその企業の責任であったが、クラウドサービスや BPO では、どこまでがこれらのサービス受託者の責任で、どこまでが委託者の責任であるかが曖昧である。また、スマートフォンの国内普及率は 37%、SNS の利用者は 6 千万人に上っているが、これらの世界ではプライベートと仕事の間の境界が曖昧になっている（情報通信白書平成26年版、総務省、[http://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h26/pdf/26honpen.pdf]等による）。

サイバー攻撃を行う者は、高度な技術を以って、この責任分界の曖昧な部分を巧みに突いてくる。しかし、最終的には、その企業が全責任を取らざるを得ないのである。

４． サイバーセキュリティ対策について

以下に、サイバーセキュリティ対策に関する基本的な考え方や具体的な取り組みを紹介する。

４．１ サイバーセキュリティ対策に関する新たな動きと課題

2014 年 11 月 6 日にサイバーセキュリティ戦略の基盤となる「サイバーセキュリティ基本法」が、衆議院本会議で可決成立した。そこには、サイバーセキュリティは国の責務と明記されている。前述のような深刻な状況のなかで政府も本格的に動き出した。

次に、民間企業が連携してサイバーセキュリティ対策に取り組む日本シーサート協議会という任意団体の活動をご紹介したい。この団体は、各企業の CSIRT(Computer Security Incident Response Team)、すなわち、サイバーセキュリティインシデントに対応するチームが集まってサイバーセキュリティ対策を協議する団体であり、情報搾取が始まったころの 2007 年に会員 6 社で創設され、2014 年 11 月現在、加盟企業数は、65 チームに達している。講師も運営委員を務めるが、ここでは、各参加企業が通常は表に出ないインシデント事例を持ち寄り、社内および社外への連絡方法、社内体制(法務、営業など)、効果的な再発防止策に関する分析等行い、「効率的な対応」や「効果的な対策」を導き出そうとしている。自社の恥を晒すことになるので、当初は事例を提供せずに聞くだけの参加者が多かった。そこで今はインシデント提供を輪番制にしている。

たとえば、オペレーションについて、コールセンターへの投資、広報対応、人の用意等、経営者に可視化するのはどうしたらいいか、といったことや、退職者の PC は使い回しされ、再インストールされてデータが消滅し、退職者が不正行為をした場合、証拠がなくなるというおそれがあるが、それでは、退職者の PC をいつまでデータを保存しておけばよいかといった実際的な問題等をディスカッションしている。ここでは対話による暗黙知の形式知化が企業を跨ってなされている。サイバーセキュリティ対策のような、職人芸ともいうべき高度な専門性を必要とし、また、攻撃側の技術が絶え間無く高度化していく分野では、このプロセスはたいへん有効である。

自社の恥を晒す面もあるが、それを補って余りある収穫があり、サイバーセキュリティに責任を持つ方の参加をお勧めする。加盟するには、事前に 2 回会合に出席していただく必要があり、その後、加盟企業による推薦状と加盟申請を提出していただき、問題がなければ加盟していただく。現在、20 社程度の企業が入会待ちである。

先日、プレユーザー含めて 80 社が集まってディスカッションしたなかで、経営層をどう説得していくかが課題であるという議論になった。サイバーセキュリティは施策の有効性が明示的に捉えにくく、投資対効果が経営層にアピールしにくい。ますます高度化するサイバー攻撃に対して、金をかければきりがなく、どの当りで手を打つかを経営層に納得させるのは本当に難しいと思う。

企業がグローバル化していくなかで、M&Aなどで、今までなかった人材、企業が入ってくる。当然、海外の人材も入ってくるが、そのとき、コンプライアンスに対する行動様式が全く違うことがある。たとえば、日本人は、A をやってはいけないというと、Aを含めてその周辺のことはやってはいけないと解釈するが、例えば、ある海外の人材は、A 以外

は全部やって良いと解釈することがある。社内ルールをブラックリスト型からホワイトリスト型に転換を求められるケースもある。

４．２　コーポレートガバナンスの一部としてのセキュリティ対策

リスクマネジメントは、広義のコーポレートガバナンスの最上層を構成する（図3参照）

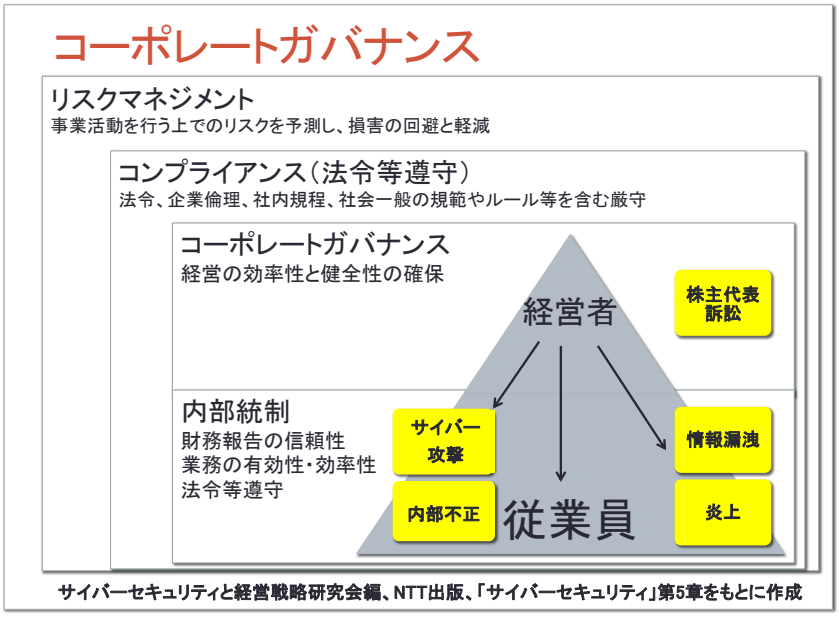


図 3　コーポレートガバナンス

コーポレートマネジメントは、図 3 のような階層構造で捉えることができる。サイバーセキュリティ対策は、再上層のリスクマネジメントの一部を構成し、コーポレートマネジメント上、最も重要な要素の一つである。

図 4 は、講師が独自に作成した、サイバーセキュリティに関するリスクマップの一例である。リスクの大きさは、一般にその事象が発生した際の事業への影響度の大きさ（図の縦軸）とその事象の発生頻度（図の横軸）の関係で捉えることができる。事象が顕在化することにより、新たな事象の発生の可能性や事業への影響度の評価が変化する。サイバー攻撃は機密情報や個人情報の漏洩につながる可能性があり、内部不正も同様である。従業員による SNS への投稿も炎上に繋がる可能性がある。

事業への影響度	Very Low	Low	Med-Low	Med-High	High
High		● サイバー攻撃	● 機密・個人情報の漏洩		
Mid-High			● 内部不正	● 炎上	
Medium-Low				● 従業員による SNS への投稿	
Low					
Very Low					

事業計画で定めた期間内で想定される発生頻度

図 4　サイバーセキュリティに関するリスクマップ

日本における従来のリスクに対する予算プロセスは、事業戦略立案と並行して、情報担当部門が、サイバーセキュリティに関するリスク分析を行って予算要求をしてきた。つまり、事業部門が策定する事業戦略に基づく予算要求と、サイバーセキュリティに関する予算要求が独立に行われている。この事業部門が策定する事業戦略に基づく予算要求と、情報システム担当部門がサイバーセキュリティリスク分析に基づいて行う予算要求との調整は、部門間の予算調整という観点で財務担当者が行うので、一般的に事業部門の予算要求が優先され、事業戦略に織り込まれていないセキュリティ対策費は、削られるか次年度にまわされてしまうことが多い。

本来は、事業遂行のためのリスク対策であるから、その調整は全社的観点で行われなければならない。情報システム担当部門の作業は、リスクの取りまとめのレベルにとどめ、財務責任者が、情報システム担当部門が提示したリスク要因を事業部門が提出する事業戦略に当てはめ、リスク分析を行って、全社的な予算を立案する。こうしないと、ますます高度化し増大するサイバー攻撃に対して対策が常に後手にまわってしまうおそれがある。サイバーセキュリティリスク対策をコーポレートガバナンスの一環として行うということは、こういうことである。このやり方を取り入れるべきであると考える。

４．３　セキュリティ対策の選定と運用

サイバーセキュリティに関係する具体的な技術要素とプロセスの全体像を図５に示す。

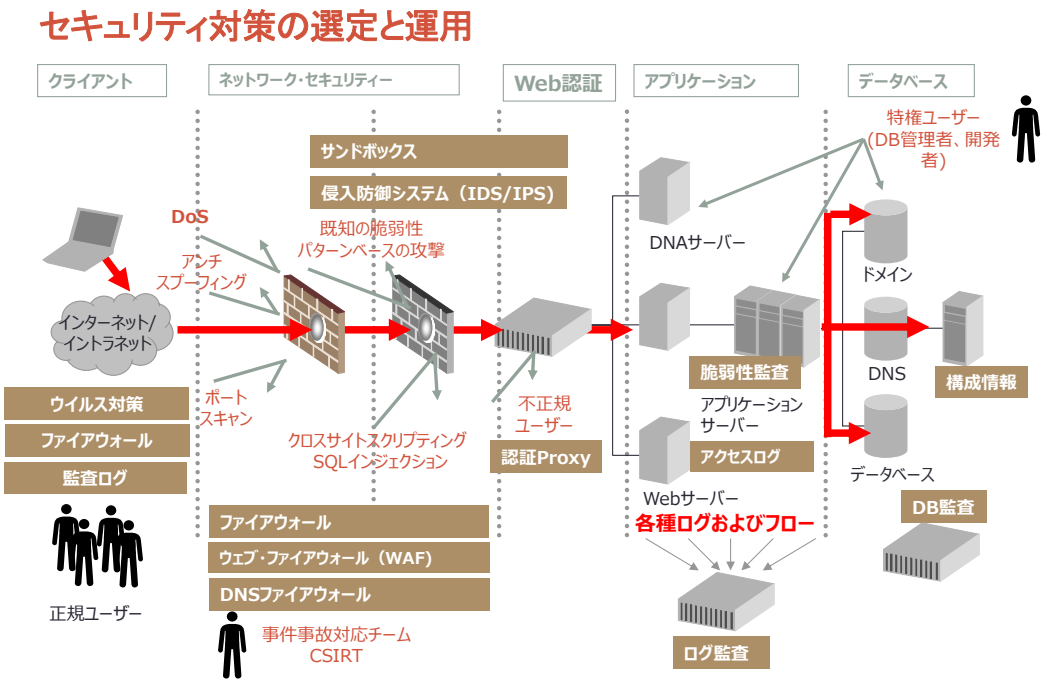


図５　サイバーセキュリティに関係する具体的な技術要素とプロセスの全体像

ツール等について二、三説明する。「サンドボックス」は、外部から受け取ったプログラムを保護された領域、「箱」の中に閉じ込めてから動作させ、外部から侵入した悪質なウイルスであっても「箱」の外にあるデータなどに影響を与えることはできないようにするものである。子どもをサンドボックス（砂場）の外で遊ばせないという言葉からきたと言われる。

IDS（Intrusion Detection System、侵入検知システム）は、ネットワークを流れるパケットを監視して、不正アクセスと思われるパケットを発見したときにアラームを表示するとともに、当該通信記録を収集し保存する仕組みである。

IPS（Intrusion Prevention System、侵入防止システム）は、サーバやネットワークへの不正侵入を阻止するツールである。侵入を検知する上記、IDS の機能を拡張し、侵入を検知したら接続の遮断などの防御をリアルタイムに行う。

サーバ等の各種ログを集めて定期的にログ監査を行い過去に問題が発生していないか調べることも必要である。

運用にあたっては、アクセス制限、不要なサービスの停止、ネットワーク分離、トラップの敷設や定期的なログの監視といった措置が必要である。トラップの敷設は IPA も勧めている有効な対策のひとつである。サイバー攻撃を仕掛けるものは、抜け穴を探すために可能性のあるパスにランダムにアクセスするから、通常使わないアカウントあるいはサーバにアクセスしてくる可能性がある。これらをわざと設置しておけばサイバー攻撃の早期発見に繋がる可能性が高い。

ただし、これらのツールや運用プロセスを全部設定、策定し、実施しようとすると、投資額は、数百万～数千万円かかる。前述ように、コーポレートガバナンスの観点で、優先度をつけてサイバーセキュリティに係るツールや運用プロセスを選定することが求められる。

４．４　セキュリティ対策に関する二、三の補足

フォレンジック（不正アクセスや機密情報漏洩などコンピュータに関する犯罪が生じた際に、原因究明や捜査に必要な機器やデータ、電子的記録を収集・分析し、その証拠を明らかにすること）は、企業内部で実施しても１台１週間はかかる。外注すると、契約等の段取りとフォレンジックの実施で、外注先がすぐに対応した場合でも数週間、数十万円から数百万円の費用がかかる。

トレンドマイクロ社、「セキュリティインテリジェンスホワイトペーパー『2013 年国内における持続的標的型攻撃の分析』」によれば、サイバー攻撃の8割は、脆弱性を利用したものではないということである。

また、日本全体のセキュリティセンターを運営する独立行政法人情報処理推進機構（IPA）では「『高度標的型攻撃』対策に向けたシステム設計ガイド」（https://www.ipa.go.jp/files/000042039.pdf）を発行している。ここに掲げられている対策の主な項目は、①ネットワーク通信経路設計によるコネクトバック通信の遮断、②ファイル共有の制限、③管理制限アカウントのキャッシュ禁止、④認証機能を活用したコネクトバック通信の遮断とログ監視、⑤プロキシのアクセス制御によるコネクトバック通信の遮断と監視、⑥運用管理専用の端末設置とネットワーク分離と監視、⑦トラップアカウントによる監視、⑧ログオンの監視である。

前述のトレンドマイクロ社の「サイバー攻撃の８割は脆弱性を利用したものではない」という指摘と、この IPA の枚挙する対策項目を見ると、サイバー攻撃の高度化により、既存のセキュリティ対策があまり役に立たなくなりつつあり、サイバーセキュリティ対策は、アクセス制御やログ監視といった対策が求められている（だからといって、既存のセキュリティ対策が無意味といっているわけではない）。要は攻撃があるという前提で対策を立てる必要があるということである。

４．５　サイバーセキュリティ対策のための組織構築について

いずれにせよ、問題が起こってからでは遅く、グレーの段階で止めたい。そのためには、ツールを整えたり運用ルールを策定するだけでは不十分で、組織としての運営体制を確立しなければならない。

とくに、サイバーセキュリティに関するインシデントを継続的に監視し、検出し、対策を講じる CSIRT(Computer Security Incident Response Team)が重要であり、この人材を育成する必要がある。

しかしながら、CSIRT を含むサイバーセキュリティ人材は不足している。ある調査では、人材不足解消について６割の企業が何らかの姿勢で取り組む意向を示してしているものの、具体的には何も行っていないという回答が半数近くを占めている。これにはキャリアパスの問題もある。たとえば、CSIRT の一員として働いても、その後にどこに行くか明確でなく、不安感を抱いている者も多い。セキュリティ人材はある意味で特殊技能者であり、明確な人事処遇の方針を示すことが必要である。

もうひとつ、サイバーセキュリティ対策において組織上考慮しなければいけない重要なポイントがある。それは、サイバーセキュリティに関わる人材の職務を分掌することである。一人の人がすべてのことができないように職務を分掌し、管理者の承認を経る手順を策定し、実施することが内部犯行を防ぐ上で重要である。

前述のごとく人材の流動化とグローバル化に伴い、もはや、日本の企業は、とくにサイバーセキュリティに関わる部分については従来の性善説を捨てなければいけないということである。特殊技能者ゆえに役割と権限が一人又は少数の人間に集中しがちであるが、そのようなやり方をしていて問題を起こせば、その企業はコーポレートガバナンスが出来ていないという批判に晒されることになる。

５． まとめ

以上、述べたように、サイバーセキュリティの問題は企業の存続と事業の継続に関わる極めて重要な課題である。ただし、これを単なるコスト、必要経費として捉えるのではなく、むしろ、コーポレートガバナンスの一環として、社会的価値の創造及び利益最大化の手段、すなわち、事業戦略上重要な経営資源として前向きに戦略的に取り組むべきである。さすれば、サイバーセキュリティへの対応により、他社との差別化が実現されるであろう。

最後に、P.F.ドラッカーの言葉を紹介したい。

「ライオンが檻から逃げたら責任は飼い主にある。過失により檻が開いたか、地震でカギが外れたかは関係ない。ライオンが凶暴であることは避けられない。」

要するに、サイバーセキュリティに関し、企業は故意・過失を問わず広範な責任を負っているということである（以上、サイバーセキュリティと経営戦略研究会編、NTT 出版、「サイバーセキュリティ」第 5 章による）。

本講演が、サイバーセキュリティ及びその周辺の問題に取り組む方々の参考になれば幸いである。

講演、以上

【質疑】

質問：日本シーサート協議会への参加条件をもう少し詳しくしりたい。

回答：日本シーサート協議会の参加に関する詳しいご案内については、事務局(nca-sec@nca.gr.jp)にまずは連絡して頂きたい。参加費は無料である。

質問：サイバーセキュリティ対策は、ツールによる措置よりも防御的措置の方に移りつつあるということであるが、その原因は何か。

回答： なかなか難しいが、既存のセキュリティ対策が無力化されつつあることが原因の一つである。高度な技術を持つ攻撃者は自ら開発したウイルスを作成するのでウイルス対策ソフトでは検知が困難である。また、ファイアウォールも擦り抜ける技術を持っている。要するに前述のトレンドマイクロ社の指摘どおり、攻撃に脆弱性を使わないなど、あらゆる手段を使って対策の回避が行われている。

金銭目的のものは既存の対策でかなり対応できるが、ある特定の企業を標的とした技術的に高度なもの、サイバーテロとか情報搾取では、ツールによる対応は困難で、アクセス制御やログ監視といった対策を取る必要がある。リアルタイムにログを収集してフォレンジックを行うことがあるが、何日もかかる。影響、範囲を限定し、分析を自動化する仕組みを作っている。これを用いて重点的な監視を行う。

質問:システム監査的な考えで防御を高度化するアイデアはあるか。

回答: ログの監視のノウハウにシステム監査的な考え方を適用できる可能性がある。企業によって通信の仕組みに、あるパターンがある。そのパターンに応じてネットワークをうまく分離し、検出すべきイベント、すなわち、アラートを出すべきイベントを定める。ログを収集したあとにそれを分析し、実際にそのアラートが上がったイベントがサイバー攻撃であったか否かを判断し、それによってネットワークの構成を最適化し、アラートを出すべきイベントを再設定していく。この過程をスパイラル的にやっていくという必要があるのではないか。

質問:医療機関におけるセキュリティ対策に関して留意事項はあるか。

回答:医療機関は詳しくない。しかし、電子カルテ等、センシティブな情報はネットにつながず、クローズド環境で取り扱う必要があるのではないか。これらをオンラインで共有することでリスクが顕在化してくると考える。

【報告者所感等】

サイバー攻撃の現状とそれに対する対応策を、興味深い具体的な事例を適宜おりまぜて紹介された。

報告者なりに講演の概要を以下のようにまとめてみたので参考にされたい。

サイバー攻撃は、その手口が年々高度化し、その目的も以前の愉快犯的なものから、金銭目的、情報搾取、さらに、サイバーテロへと変質している。とくに情報搾取などでは、攻撃を受けた痕跡を残さないものもある。

また、攻撃の手口の高度化により、既存の防御のツールは無力化されつつあり、従来型のアクセス制限、ログの監査といった予防的措置を地道に行うという対策に戻りつつある。当然、攻撃による被害も、経済的損失のみならず、企業としての存続が危ぶまれるような社会的信用の失墜等、甚大なものになりつつある。

さらに、企業においては、人材面でも流動化やグローバル化が進展しており、内部犯行のリスクが高まっている。

これに対しては、もはや、従来のコスト、あるいは、必要経費といった消極的局所的な意識での対応は不可で、コーポレートガバナンスの再上層を構成するものとして、経営者の責任で対応しなければならない。むしろ、サイバーセキュリティについて、社会的価値の創造及び利益最大化に繋がる差別化戦略として積極的に取り組むべきである。

以上

＜目次＞

2015.1

～「経済産業省ガイドライン」の読みこなしポイント～
「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」特別号
2014 年 12 月 12 日改正のポイント

個人情報保護監査研究会

※個人情報保護監査研究会注:「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」が、2014年(平成26年)12月12日付けで告示・施行されました。

【主な改正点】(METIパンフレットより:)

1. 第三者からの適正な取得の徹底
2. 社内の安全管理措置の強化
3. 委託先の監督の強化
4. 共同利用制度の明確な説明
5. 消費者等本人に対する分かりやすい説明の取組

今回は、特別号として、改正された内容についてご紹介します。

※文中アンダーライン部分が追加・改正された部分です。全文については、改正METIガイドライン本文を参照してください。

【改正点１】：第三者からの適正な取得の徹底

・第三者から個人情報を取得する場合には、適法に入手されていること等確認する事が望ましい。

・適法に入手されていることが確認できない場合は、取引を自粛することを含め、慎重に対応することが望ましい。

2-2-2. 個人情報の取得関係（法第17条～第18条関連）

（１）適正取得（法第17条）

> 法第17条
> 個人情報取扱事業者は、偽りその他不正の手段により個人情報を取得してはならない。

不正の利益を得る目的で、又はその保有者に損害を与える目的で、秘密として管理されている事業上有用な個人情報で公然と知られていないものを、不正に取得したり、不正に使用・開示した場合には不正競争防止法が科され得る。

また、第三者からの提供により、個人情報を取得する場合には、提供元の法の遵守状況(例えば、オプトアウト、利用目的、開示手続、問合わせ・苦情の受付窓口を公表していることなど)を確認し、個人情報を適切に管理している者を提供元として選定するとともに、実際に個人情報を取得する際には、例えば、取得の経緯を示す契約書等の書面を点検する等により、当該個人情報の取得方法等を確認した上で、当該個人情報が適法に取得されたことが確認できない場合は、偽りその他不正の手段により取得されたものである可能性もあることから、その取得を自粛することを含め、慎重に対応することが望ましい。

※個人情報保護監査研究会注：第三者提供を受ける側も、不正に取得（データセンターやインターネットを経由して個人情報を盗むなど）で取得していないことを確認するよう求めています。

【改正点２】：社内の安全管理措置の強化

・外部からのサイバー攻撃対策の追加。

・内部不正対策の組織的、物理的、技術的安全管理措置の項目の追加。

2-2-3-2. 安全管理措置（法第20条関連）

法第20条

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

特に中小企業者においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。

※個人情報保護監査研究会注：外部からのサイバー攻撃対策や、内部不正対策の組織的、物理的、技術的安全管理措置の項目が追加されました。しかし中小企業者では、資源に余裕が無い場合も多いため、事業の規模や取り扱う個人データの性質及び量等実態をよく認識して、対策を講じるように追記されました。

組織的安全管理措置

①「個人データの安全管理措置を講じるための組織体制の整備」（追加部分のみ、以下同じ）

- 個人データの安全管理の実施及び運用に関する責任及び権限を有する者として、個人情報保護管理者を設置し、原則として、役員を任命すること
- 個人データの取扱いを総括する部署の設置、及び個人情報保護管理者が責任者となり、社内の個人データの取扱いを監督する「管理委員会」の設置
- 個人情報保護対策及び最新の技術動向を踏まえた情報セキュリティ対策に十分な知見を有する者（必要に応じ、外部の知見を有する者を活用し確認することを含む）などによる、監査実施体制の整備

【規程等に記載することが望まれる事項の例】

（1）取得・入力

- スマートフォン、パソコン等の記録機能を有する機器の接続を制限し、媒体及び機器の更新に対応する。）

人的安全管理措置

人的安全管理措置とは、従業者（「個人情報取扱事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいい、雇用関係にある従業員（正社員、契約社員、嘱託社員、パート社員、アルバイト社員等）のみならず、取締役、執行役、理事、監査役、監事、派遣社員等も含まれる。）に対する、業務上秘密と指定された個人データの非開示契約の締結や教育・訓練等を行うことをいう。

物理的安全管理措置

- 入退館（室）の記録
- 業務上許可を得ていない記録機能を持つ媒体及び機器の持ち込み及び持ち出しの禁止と検査の実施
- カメラによる撮影や作業への立ち会い等による記録又はモニタリングの実施

技術的安全管理措置

技術的安全管理措置については、①から⑧までの各項目を遵守するとともに、複数の手法を組み合わせ、個人データ及びそれを取り扱う情報システム全体の安全性を確保することが重要である。

①「個人データへのアクセスにおける識別と認証」

- ワンタイムパスワードによる認証、物理的に所持が必要な認証デバイス(ICカード等)による認証、

＊識別と認証においては、複数の手法を組み合わせて実現することが望ましい。

＊生体認証を利用する場合には、当該識別と認証の方法を実施するために必要な情報(例えば、指紋、静脈)が、特定の個人を識別することができることから、個人情報に該当する場合があることに留意する。

②「個人データへのアクセス制御」

＊個人データを格納するためのデータベースを構成要素に含む情報システムを構築する場合には、当該情報システム自体へのアクセス制御に加えて、情報システムの構成要素であるデータベースへのアクセス制御を別に実施し、それぞれにアクセス権限を設定することが望ましい。

＊アクセス権限の設定を情報システム全体と別に実施する場合にあっては、無権限アクセスからの保護に係る機器等の設定として、特に不要アカウントの無効化や初期設定されている標準アカウントのパスワード変更を実施することが望ましい。

③「個人データへのアクセス権限の管理」

＊個人データにアクセスできる者を許可する権限については、情報システム内において当該権限を含む管理者権限を分割する等して、不正利用を防止することが望ましい。

④「個人データへのアクセスの記録」

＊個人データへのアクセスや操作の成功と失敗の記録については、情報システムを構成する各システムへのアクセスや操作の成功と失敗等の記録を組み合わせ、各個人データへのアクセスや操作の失敗を全体として記録することが考えられる。

＊採取した記録を漏えい、滅失及びき損から保護するためには、当該記録を適切に管理された外部記録媒体ないしログ収集用のサーバ等に速やかに移動することが望ましい。

＊システム管理者等の特権ユーザーのアクセス権限を用いても、採取した記録を改ざん・不正消去できないよう、対策することが望ましい。

⑤「個人データを取り扱う情報システムについて不正ソフトウェア対策」

- ウイルス対策ソフトウェアの安定性の確認(例えば、パターンファイルや修正ソフトウェアの更新の確認)
- 端末及びサーバ等のオペレーティングシステム(OS)、ミドルウェア(DBMS等)、アプリケーション等に対するセキュリティ対策用修正ソフトウェア(いわゆる、セキュリティパッチ)の適用
- 組織で許可していないソフトウェアの導入防止のための対策

⑥「個人データの移送 (運搬、郵送、宅配便等)・送信時の対策」

- 個人データの移送時における紛失・盗難に備えるための対策(例えば、媒体に保管されている個人データの暗号化等の秘匿化)
- 盗聴される可能性のあるネットワークにおける、個人データの暗号化等の秘匿化(例えば、SSL、S／MIME等)
- ＊暗号を利用する場合には、復号に必要な鍵についても十分注意して管理する必要がある。

⑦「個人データを取り扱う情報システムの動作確認時の対策」

- 情報システムの動作確認時のテストデータとして個人データを利用することの禁止(正確な動作確認を要する等、個人データの利用が不可欠な場合であっても、動作確認に影響のない範囲で、個人データの一部を他のデータに置き換える等の措置を講じることが考えられる。)

⑧「個人データを取り扱う情報システムの監視」

＊特権ユーザーによる個人データへのアクセス状況については、特に注意して監視することが望ましい。

- 個人データを取り扱う情報システムへの外部からのアクセス状況の監視（例えば、IDS・IPS等）

  ＊監視システムを利用する場合には、事業者等が業務で行う送受信の実態に合わせ、当該装置について適切に設定し、定期的にその動作を確認することが必要になる。

2-2-3-3. 従業者の監督（法第21条関連）

> 法第21条
>
> 個人情報取扱事業者は、その従業者に個人データを取り扱わせるに当たっては、当該個人データの安全管理が図られるよう、当該従業者に対する必要かつ適切な監督を行わなければならない。

特に中小企業者においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。

【従業者のモニタリングを実施する上での留意点】

本ガイドライン及び雇用管理分野における個人情報保護に関するガイドライン第10に規定する雇用管理に関する個人情報の取扱いに関する重要事項とは、モニタリングに関する事項等をいう。

※個人情報保護監査研究会注：上記ガイドラインでは、雇用管理上の重要事項（この場合はモニタリング）を実施するときは、”あらかじめ労働組合等に通知し、必要に応じて協議を行うことが望ましい。”との規定に従うことを促しています。

【改正点３】：委託先の監督の強化

・内部不正対策の委託先の安全管理措置の確認、定期的な監査等の追加。

・再委託先以降も同様の措置を行うことが望ましい。

2-2-3-4. 委託先の監督（法第22条関連）

> 法第22条
>
> 個人情報取扱事業者は、個人データの取扱いの全部又は一部を委託する場合は、その取扱いを委託された個人データの安全管理が図られるよう、委託を受けた者に対する必要かつ適切な監督を行わなければならない。

特に、中小企業者においては、事業の規模及び実態、取り扱う個人データの性質及び量等に応じた措置を講じることが望ましい。

優越的地位にある者が委託元の場合、委託元は、委託先との責任分担を無視して、本人からの損害賠償請求に係る責務を一方的に委託先に課す、委託先からの報告や監査において過度な負担を強いるなど、委託先に不当な負担を課すことがあってはならない。

①委託先の選定

委託先の選定に当たっては、委託先の安全管理措置が、少なくとも法第20条で求められるものと同等であることを確認するため、以下の項目が、委託する業務内容に沿って、確実に実施されることについて、委託先の社内体制、規程等の確認、必要に応じて、実地検査等を行った上で、個人情報保護管理者（CPO）等が、適切に評価することが望ましい。

（ア）組織的安全管理措置

- 安全管理措置を講じるための組織体制の整備

- 安全管理措置を定める規程等の整備と規程等に従った運用
- 個人データの取扱状況を一覧できる手段の整備
- 安全管理措置の評価、見直し及び改善
- 事故又は違反への対処

（イ）人的安全管理措置

- 雇用契約時における従業者との非開示契約の締結、及び委託契約等（派遣契約を含む。）における委託元と委託先間での非開示契約の締結
- 従業者に対する内部規程等の周知・教育・訓練の実施

（ウ）物理的安全管理措置

- 入退館（室）管理の実施
- 盗難等の防止
- 機器・装置等の物理的な保護

（エ）技術的安全管理措置

- 個人データへのアクセスにおける識別と認証
- 個人データへのアクセス制御
- 個人データへのアクセス権限の管理
- 個人データのアクセスの記録
- 個人データを取り扱う情報システムについての不正ソフトウェア対策
- 個人データの移送・送信時の対策
- 個人データを取り扱う情報システムの動作確認時の対策
- 個人データを取り扱う情報システムの監視

③委託先における個人データ取扱状況の把握

定期的に、監査を行う等により、委託契約で盛り込んだ内容の実施の程度を調査した上で、個人情報保護管理者（CPO）等が、委託の内容等の見直しを検討することを含め、適切に評価することが望ましい。

委託先が再委託を行おうとする場合は、委託を行う場合と同様、委託元は、委託先が再委託する相手方、再委託する業務内容及び再委託先の個人データの取扱方法等について、委託先から事前報告又は承認を求める、及び委託先を通じて又は必要に応じて自らが、定期的に監査を実施する等により、委託先が再委託先に対して本条の委託先の監督を適切に果たすこと、及び再委託先が法第20条に基づく安全管理措置を講ずることを十分に確認することが望ましい。再委託先が再々委託を行う場合以降も、再委託を行う場合と同様とする。

【個人データの取扱いを委託する場合に契約に盛り込むことが望まれる事項】

- 委託先において、個人データを取り扱う者（委託先で作業する委託先の従業者以外の者を含む）の氏名又は役職等（なお、委託の実態に応じて、例えば、契約書とは別に、個人データを取り扱う者のリスト等により、個人データを取り扱う者を把握するなど、適切な対応を行うことが望ましい。）
- 再委託を行うに当たっての委託元への文書による事前報告又は承認
- 契約内容が遵守されなかった場合の措置（例えば、安全管理に関する事項が遵守されずに個人データが漏えいした場合の損害賠償に関する事項も含まれる。）

【改正点４】：共同利用制度の趣旨の明確化

・事業者が共同利用を円滑に実施するために共同利用者における責任等を追加

・共同利用者の範囲の明確化

2-2-4. 第三者への提供（法第２３条関連）

（３）第三者に該当しないもの（法第２３条第４項関連）

（iii）共同利用（法第２３条第４項第３号関連）

> 法第２３条第４項第３号
>
> 次に掲げる場合において、当該個人データの提供を受ける者は、前３項の規定の適用については、第三者に該当しないものとする。
>
> ３ 個人データを特定の者との間で共同して利用する場合であって、その旨並びに共同して利用される個人データの項目、共同して利用する者の範囲、利用する者の利用目的及び当該個人データの管理について責任を有する者の氏名又は名称について、あらかじめ、本人に通知し、又は本人が容易に知り得る状態に置いているとき。

以下の①から④までの情報をあらかじめ本人に通知し、又は本人が容易に知り得る状態に置いておくとともに、共同して利用することを明らかにしているときには、当該個人データの提供を受ける事業者は、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性があると考えられることから、第三者に該当しない。

①共同して利用される個人データの項目

個人データの項目について、本人に通知し、又は本人が容易に知り得る状態に置いていなければならない。

事例1）氏名、住所、電話番号

事例2）氏名、商品購入履歴

②共同して利用する者の範囲

「共同利用の趣旨」は、本人から見て、当該個人データを提供する事業者と一体のものとして取り扱われることに合理性がある範囲で当該個人データを共同して利用することである。

したがって、共同利用者の範囲については、本人がどの事業者まで将来利用されるか判断できる程度に明確にする必要がある。

なお、当該範囲が明確である限りにおいては、事業者の名称等を個別にすべて列挙する必要がない場合もある。

事例）本人がどの事業者まで利用されるか判断できる程度に明確な形で示された「提携基準」及び「最新の共同利用者のリスト」等を、共同利用者の全員が、本人が容易に知り得る状態に置いているとき

③利用する者の利用目的

共同して利用する個人データについて、その取得時の利用目的をすべて、本人に通知し、又は本人が容易に知り得る状態に置いていなければならない。

利用目的が個人データの項目によって異なる場合には区別して記載することが望ましい。

④当該個人データの管理について責任を有する者の氏名又は名称

開示等の求め及び苦情を受け付け、その処理に尽力するとともに、個人データの内容等について、開示、訂正、利用停止等の権限を有し、安全管理等個人データの管理について責任を有する者の氏名又は名称について、本人に通知し、又は本人が容易に知り得る状態に置いていなければならない。

ここでいう「責任を有する者」とは、共同して利用するすべての事業者の中で、第一次的に苦情の受付・処理、開示・訂正等を行う権限を有する事業者をいい、共同利用者のうち一事業者の内部の担当責任者をいうものではない。

【改正点５】：消費者等本人に対する分かりやすい説明のための参考事項

・個人情報取扱事業者は、本人に対して、個人情報保護を推進する上での考え方や方針等について、分かりやすい表現で説明するために参考とすべき基準を追記。

５．個人情報取扱事業者がその義務等を適切かつ有効に履行するために参考となる事項・規格

(1)個人情報保護のためのマネジメント体制の確立

(2)個人情報保護を推進する上での考え方や方針の策定等

(3)消費者等本人に対する分かりやすい説明の実施

事業者は、消費者等本人との信頼関係を構築する観点から、消費者等本人に対して、個人情報取扱事業者の個人情報保護を推進する上での考え方や方針等について、以下に掲げる基準を参考にして、冗長で分かりにくい表現を避け、消費者等本人に誤解を与えることなく分かりやすい表現で表示することが望ましい。

分かりやすい説明の実施に際して参考とすべき基準

１．記載事項

（１）必要十分な記載事項

１ 個人情報の取扱いに関する情報として、以下の７項目が記載されていること

1)提供するサービスの概要

2)取得する個人情報と取得の方法

3)個人情報の利用目的

4)個人情報や個人情報を加工したデータの第三者への提供の有無及び提供先

5)消費者等本人による個人情報の提供の停止の可否、訂正及びその方法

6)問合せ先

7)保存期間、廃棄

２．記載方法

（１）取得する個人情報とその取得方法に係る記載方法

２ 取得する個人情報の項目とその取得方法について、可能な限り細分化し、具体的に記載していること

３ 取得する個人情報の項目やその取得方法のうち、消費者等本人にとって分かりにくいものを明確に記載していること

（２）個人情報の利用目的に係る記載方法

４ 取得する個人情報の利用目的を特定し、具体的に記載していること

５ 個人情報の利用目的が、取得する個人情報の項目と対応して記載されていること

６ 取得する個人情報の利用目的のうち、消費者等本人にとって分かりにくいものを明確に記載していること

（３）第三者への提供の有無及び個人情報や個人情報を加工したデータの提供先に係る記載方法

７ 個人情報取扱事業者が取得する個人情報や個人情報を加工したデータを第三者に提供する場合、その提供先（事後的に提供先を変更する場合は提供先の選定条件を含む）及び提供目的が記載されていること

８ 個人情報取扱事業者が取得した個人情報を加工したデータを第三者に提供する場合、その加工方法が記載されていること

（４）消費者等本人による個人情報の提供の停止の可否及びその方法に係る記載方法

9 消費者等本人が個人情報取扱事業者による個人情報の取得の中止又は利用の停止が可能であるかが記載され、可能である場合には取得の中止方法又は利用の停止方法を明示して記載していること

上記の「参考とすべき基準」は、個人情報を含む「パーソナルデータ」を利活用してサービスを行う事業者が、消費者から「パーソナルデータ」を取得し利用する際に、消費者に対して行う情報提供や個人情報保護を推進する上での考え方や方針等を分かりやすく説明した文書等の内容の適切性を第三者が事前に評価する際のツールとして経済産業省が策定した「評価基準」を基に作成したものである。

同評価基準の評価方法等については、経済産業省ホームページの「個人情報保護」のページ中に掲載されている。

（経済産業省ホームページの「個人情報保護」のページ）

http://www.meti.go.jp/policy/it_policy/privacy/index.html

★★「個人情報の保護に関する法律についての経済産業分野を対象とするガイドライン」等に関するQ＆A★★

（2014 年 12 月 12 日更新）

事業者の各取扱部門が独自に取得した個人情報を取扱部門ごとに設置されているデータベースにそれぞれ別々に保管している場合において、ある取扱部門のデータベースと他の取扱部門のデータベースへのアクセスが、規程上・運用上厳格に禁止されているときには、「容易に照合することができ」（法第2条第1項）ないといえますか。(2014.12.12)	他の取扱部門のデータベースへのアクセスが規程上・運用上厳格に禁止されている場合であっても、双方の取扱部門を統括すべき立場の者等が双方のデータベースにアクセス可能なときには、当該事業者にとって「容易に照合することができ」る 状態にあると考えられます。ただし、経営者、データベースのシステム担当者などを含め社内の誰もが規程上・運用上、双方のデータベースへのアクセスを厳格に禁止されている状態であれば、「容易に照合することができ」る とはいえないものと考えられます。(2014.12.12)
共同利用開始後、途中から新たな事業者が共同利用に参入することはできますか。	共同利用開始後に新たな事業者が共同利用に参入しようとする場合には、原則として、共同して利用する者の範囲（法第23条第4項第3号）を変更することができず（同条第5項）、改めて共同利用手続を採る必要があります。ただし、本人がどの事業者まで利用されるか判断できる程度に共同利用者の範囲が明確にされている場合には、個別列挙が必要でない場合もあると考えられますので、その場合には、引き続き共同利用を行うことができるものと考えます。(2014.12.12)

次回は、「2-2-4.第三者への提供（法第23条関連）」の読みこなしポイントを掲載します。

バックナンバー目次 http://1.33.170.249/saajpmsMETIGL/000METIGL.html

（↑バックナンバー目次のURLが変更となりました。）

個人情報保護監査研究会 http://www.saaj.or.jp/shibu/kojin.html

■

＜目次＞

2015.1

北信越支部 【2014 年度 石川県例会 報告】

会員 No. 1281　北信越支部 宮本 茂明

以下のとおり2014年度 北信越支部石川県例会を開催しました.

・日時：2014 年 12 月 6 日（土） 13:00-17:00　　参加者：10 名

・会場：IT ビジネスプラザ武蔵（石川県　金沢市）

・議題：１． 2014 年度 西日本支部合同研究会参加報告

２．「金融機関におけるコンティンジェンシープラン策定整備とそのシステム監査」研究報告

* 西日本支部合同研究会報告作成にご協力いただいた皆様からのコメントと参加者による意見交換を実施

◇研究報告

「金融機関におけるコンティンジェンシープラン策定整備とそのシステム監査」

報告者（会員 No.1281　宮本 茂明）

本報告は、2014 年度西日本支部合同研究会に向け北信越支部報告としてまとめたものである。長野県例会で報告に関する意見交換を行った後、長谷部様から提供いただいた報告をベースとし、小嶋様、藤原様ほか北信越支部の方々からのコメント、意見交換結果を加え、日本銀行の調査レポート、金融情報システムセンター(FISC)のガイドラインから作成したものである。報告作成にご協力いただいた皆様に深く感謝する。

はじめに

（1）2011 年 3 月 11 日に発生した東日本大震災は、地震の規模やそれによる津波など、すべてが従来の業務継続計画の想定をはるかに超える規模で発生した。長期間・広範囲にわたる社会インフラの寸断や、原子力発電所の損壊による特定地域への立入り制限など、社会全体に大きな影響を与える二次的な災害まで発生した未曾有の大規模災害であった。

（2）東日本大震災において、金融機関は全体としては、震災後も安定的に業務を継続し、正常な決済機能等を維持したが、一方で認識していなかった課題が浮かび上がった。従来のコンティンジェンシープランで想定していなかった事象が発生し、準備していた対策が十分に機能しなかった事例が、少なからずみられた。

（3）東日本大震災で認識した課題に基づき、各金融機関はコンティンジェンシープランを見直し、業務継続態勢の整備に取組んできた。北信越支部では、金融機関の関連企業に勤務する会員を中心に取組事例を整理し、それに対して電力、情報通信など社会インフラを担う他業態勤務者、およびシステム監査人、ＩＴコーディネータなどの立場から、課題を複眼的に洗い上げる機会をもった。その研究成果を報告する。

Ⅰ．東日本大震災被災時の金融機関の業務継続

１．東日本大震災における金融機関の対応

「東日本大震災におけるわが国決済システム・金融機関の対応」(2011 年 6 月 24 日　日本銀行決済機構局)の資料から、「被災地金融機関・決済システムの対応」「被災地を含む全国的な決済システム・金融機関の対応」について以下に概要をまとめる。

（1）被災地金融機関・決済システムの対応

①預金者への対応

被災地金融機関は、震災直後から被災店舗の復旧と業務の再開に懸命に取り組まれた。復旧困難な店舗については、近隣に臨時窓口や仮設店を設置し、近隣店舗で業務を代替するなどの対応がとられた。

被災した預金者に対し、預金証書、通帳を紛失した場合に預金者であることを確認のうえ払戻しを行い、届出の印鑑がない場合に本人確認のうえ、拇印での払戻しを行うなどの柔軟な対応がとられた。

②金融機関間の連携・協力

近隣の金融機関が協力して現金を被災地金融機関に配送するなど金融機関間の連携・協力により業務が継続された。避難地域に被災者の取引金融機関が存在しないケースで取引金融機関以外での預金の払戻し対応も行われた。

（2）被災地を含む全国的な決済システム・金融機関の対応

①決済システムの動向

決済システム、金融機関は、全体として安定的な稼働を続けた。これは、決済システムと金融機関が日頃から業務継続体制の整備に地道に取り組んできたことも寄与していると考えられる。被災地の金融機関で本部が損壊、流失する例があったが、預金や貸出等の基本データは、共同システムによって処理・管理されておりデータが消失するといった事態は回避された。

②一部行のシステム障害発生と全銀システムの決済時間延長

一部大手行で義援金が一部口座に大量に集中し、その後の対処ミスとあいまって大規模なシステム障害が発生した。このシステム障害を受け、全銀システム、日銀ネットの決済時間延長の措置がとられた。

③被災地における停電、東京電力管下における計画停電等への対応

東北地方では、震災直後ほぼ全域にわたって停電が発生した。東北地方に所在する金融機関は自家発電機の稼働により、震災当日 11 日(金)の業務を継続した。多くの金融機関が、預金者の便宜を図るため、12 日(土)、13 日(日)も自家発電機の稼働により一部の店舗を開き、預金者対応を行った。13 日(日)夜から順次停電が解消し、14 日(月)以降多くの金融機関が商用電力のもとで業務可能となった。

東京電力管下で計画停電が実施された。計画停電の対象となった金融機関の本部やシステムセンター、主要支店等では、停電時間帯に自家発電機を稼働させ、業務を通常どおりに継続した。自家発電機を備えていない支店や ATM は、計画停電時間中に営業を停止する金融機関がみられた。

２．東日本大震災における金融機関の対応　（北信越支部 意見交換/コメントより）

（1）人命に係るリスクへの対応

東日本大震災では、人命第一が再確認された。お客様はもちろん、従業員も含めて、すばやく避難することが重要であり、現場のリーダーにより業務を停止する判断ができることの重要性が認識された。

（2）被災者支援

地域金融機関では、各営業エリアにおいて、地震や台風・大雪等に被災し直接的・間接的に経営に影響が出ている中小企業や個人事業主の復旧と資金繰りを幅広く支援するため、「災害復興特別融資」の取扱いを行っている。更に震災復興ボランティア活動も企業として組織的にバックアップしている。

地域金融機関は、これらの被災時対応なくして地域のお客さまからの支持は得られないと認識しており、当然のことと捉えられている。

Ⅱ．東日本大震災後の業務継続態勢整備への取り組み状況の変化

１．東日本大震災で認識した業務継続態勢の課題と現状 （北信越支部 意見交換/コメントより）

（１）業務継続態勢整備アプローチの課題

従来、業務継続態勢整備のアプローチは、被害のきっかけとなり得る脅威に基づくシナリオを策定し、そのシナリオに沿って被災状況を想定し、業務継続計画を策定するという「結果事象」型アプローチによるものだった。東日本大震災において、このアプローチで策定された業務継続計画では、想定外の事象が発生して対応しきれないことが散見された。

（２）実効性向上への検討課題

業務継続態勢の実効性に関する検討課題が明らかになった。

① バックアップセンターの実効性(立地条件、建物・設備要件、要員・資源移動、ﾊﾞｯｸｱｯﾌﾟ復元方式など)

② 通信手段の実効性（目的別通信手段、災害に強い通信回線の冗長化方法など）

③ 停電対策の実効性（自家発電装置の能力把握、燃料確保など）

④ その他（特例払戻しや顧客への営業案内など）

（３）業務継続計画の周知

業務継続計画は、実際に周知徹底されているかが重要である。年に１回は、訓練を実施し、全職員に周知徹底を図っていく必要がある。

（４）被災想定

業務継続計画では、大規模災害等を想定していることが多いが、どこまで想定するのか判断が難しい。東日本大震災の教訓として、想定されるべきリスクを網羅することは困難であり、想定外のことが起こることを念頭に、想定外のことが起こった場合に、いかに被害を減らせるかが重要と考える。

（５）重要業務と復旧目標時間

東日本大震災を受け、重要業務と復旧目標時間の見直しが行われている。

（６）マニュアル整備

非常時優先業務に対応して、基幹系システムである勘定系システムや、各決済系システム、各種サブシステムの復旧に向けた対応フローと手順、各リスクシナリオと障害発生箇所毎の代替手順・復旧手順整備が行われている。

２．東日本大震災被災後の業務継続体制の整備状況変化

「業務継続体制の整備状況に関するアンケート（2012 年 9 月）調査結果」(2013 年 1 月 18 日 日本銀行金融機構局）の資料から、東日本大震災の前後での金融機関における業務継続体制の整備状況変化について以下に概要をまとめる。

（１）業務継続体制の整備

- ✧ 全社的な業務継続体制「整備済みで、定期的に見直し」: 8 割
  - ・ 東日本大震災における自社および他社の経験等を踏まえた業務継続体制の見直し「実施済み」/「実施中」： 97%
- ✧ 業務継続の実効性「実効性で一部不十分な部分が残っている」: 6 割
  - ・ 具体的に不十分な部分：「全社ベースでの訓練による検証」、「要員の確保」、「バックアップオフィスの整備」、「自家発電設備の整備」、「重要な関係先の業務継続計画との整合性」
  - ・ 東日本大震災前との比較では、「要員の確保」、「マニュアルの整備」の増加幅が大きい。

（2）被災シナリオ／被災想定

✧ 被災シナリオの想定原因事象：

・地震、感染症: 9 割, ・システム大規模障害：8 割, ・風水害，火災, 津波：7 割,

・公共インフラサービス提供停止：6 割, ・計画停電：5 割, ・原子力関連施設事故：4 割

✧ 東日本大震災以降「従来想定していなかった原因事象を新たに追加」: 6 割

・追加した被災シナリオの主な原因事象：「原子力関連施設の事故」、「計画停電」、「津波」

✧ 被災シナリオの結果事象として想定しているもの：

・「メインのコンピュータがほぼ全面的使用不能」: 9 割,

・「メインの執務場所がほぼ全面的使用不能」: 8 割, ・「出勤者の大幅減少」: 7 割

（3）重要業務

✧ 最優先で復旧する主な「重要業務」:

「流動性預貯金 MRF/MMF の払戻し（現金支払)」「日銀当座預金決済」

「個別の振込・送金・振替」「内国為替決済（全銀システム)」

✧ 最優先で復旧する「重要業務」の復旧目標時間：「4 時間以内」7 割

・東日本大震災前との比較では、「当日中」が減少，「4 時間以内」が増加

（4）経営資源の確保

✧ 業務継続で必要となる確保済の資源：

・「システムの稼働に必要な資源」「要員の生活に必要な資源」確保済み： 8 割

✧ 東日本大震災以降、業務継続で必要となる資源等（見直し済もの)：

・「通信手段の拡充」: 7 割,「要員の生活に必要な資源の備蓄量や調達・配分方法の見直し」: 6 割,

「自家発電設備の設置拠点の拡大」: 4 割

（5）津波対策

✧ 津波による被災拠点想定：

・各拠点の立地条件を踏まえ津波による被災拠点を想定：5 割

・今後、地方公共団体の動向等を踏まえ新たに想定する可能性がある：3 割

✧ 主な津波対策：

・「初動対応の発動基準を設定」、「各拠点の判断で避難できる権限委譲」、「基本方針の策定」、

「避難経路や誘導手順の策定」、「初動対応訓練」

（6）マニュアルの整備

✧ 業務継続計画発動時に利用する「重要業務」遂行のための各種マニュアルの整備状況：

・「各部署で作成しており、社内全体での整合性を検証している」:6 割

・「各部署で作成しているが、社内全体での整合性は未検証」:2 割

✧ マニュアルの更新・保管「マニュアルが常に利用可能な最新のものとなっている」: 8 割

✧ マニュアルの周知「マニュアルが担当者全員に周知・徹底されている」:9 割

（7）訓練

✧ 年 1 回以上定期的に訓練を行う業務：「資金決済面の訓練」: 8 割,「現金供給」: 6 割

✧ 訓練の規模：「全社ベース」で訓練：7 割

✧ この 2 年間で実施したことのある主な訓練：各業態とも多様な訓練を実施

「安否確認システムによる連絡訓練」「バックアップセンター切替訓練」「手作業訓練」の実施多い

３．バックアップ・コンピュータセンター整備状況

３．１　バックアップ・コンピュータセンター整備への取組み　（北信越支部 意見交換/コメントより）

（１）自営サーバのバックアップセンター整備（取組み例）

基幹系システムについてのバックアップセンターは整備したが、それとは別に設置しているコマンドセンターのバックアップセンターは、「人」の移動が課題となっている。

全てのシステムについてバックアップセンターを整備すると莫大な投資が見込まれる。このため、サブシステムについては、基幹システムをＤＢサーバとして利用する一部のサブシステムや対外系システム・決済系システムを除きバックアップセンターを整備しておらず、バックアップデータの隔地保管のみ実施している。システム重要度（「最重要」「重要」「一般」の３レベル区分）が「重要」以上のサブシステムについては、障害回復訓練を定期的に実施し、その結果に基づき対応手順を整備している。

（２）地銀共同センターの利用（取組み例）

勘定系については、地銀共同センターを利用しており、災対センターが遠隔地に構築されている。

サブシステムについては、主にデータセンターのクラウドサービスを利用しているが、バックアップセンターについては費用面で折り合いがつかず整備していない。

①災対センターの運用体制

地銀共同センターの災対センターは、他システムの運用拠点となっており、オペレータ等の運用担当者が配置されており、通常のセンターから切り替えることにより、災対センターだけで地銀共同システムの運用が可能となっている。

②災対センターへの切り替え体制

大規模災害発生時には、いくつかのパターンに分けたシナリオを想定し、緊急対策本部の立ち上げから災対センターへの切り替えまでの体制が構築・整備されている。緊急対策本部と各運用拠点や加盟銀行を連携するための連絡手段としては、各行運用端末・優先電話・地銀共同イントラネット・衛星携帯電話・テレビ会議・その他携帯・固定電話といった通信手段を使用することとなっている。

③共同センターの障害訓練

共同センターでは、期初に年度計画を策定して、共同センターと加盟銀行合同の障害訓練（全銀システム障害訓練、大規模震災発生時の情報連携訓練)、共同センター単独障害訓練（机上訓練、実地訓練、実機訓練、通信訓練）を実施している。

３．２　バックアップ・コンピュータセンター整備状況

「バックアップ・コンピュータセンターに関するアンケート（2012 年 9 月）調査結果」（2013 年 4 月 5 日　日本銀行金融機構局）の資料から、バックアップ・コンピュータセンターの整備状況ついて以下に概要をまとめる。

（１）重要業務と B/U システムの設置状況

* B/U システム：メインセンターとは別の場所に設置されていて、被災時等に利用するバックアップシステム

✧　「主な重要業務」の継続手段（被災当日）：

・全てまたは一部の業務を B/U システムで継続：約 4～5 割

・全ての業務を手作業で継続：約 4～5 割

✧ 「主な重要業務」の継続手段（翌営業日以降の対応）

・全てまたは一部の業務を B/U システムで継続：約 6～9 割

・全ての業務を手作業で継続：「日銀当座預金決済」約 3 割，「内国為替決済」「振込・送金」約 2 割

・手作業でも継続できない：「給与振込」約 1 割

（2）B/U 預金・為替システムのスタンバイ状況

・「ホットスタンバイ」または「ウォームスタンバイ」：約 3 割

・「コールドスタンバイ」：約 5 割

・「基本ソフトウェア等未導入（ハードウェアのみ確保）」：約 2 割

（3）B/U センターの要員配置

✧ 切替要員の配置

・「B/U センターへの駆けつけが不要」：約 6 割

・「メイン センター／他拠点から駆けつけが必要」：約 4 割

✧ 運用要員の配置

・「B/U センターへの駆けつけが不要」： 約 4 割

・「メイン センター／他拠点から駆けつけが必要」：約 6 割

（4）B/U 預金・為替システムへの切替所要時間

✧ B/U 預金・為替システムへの切替所要時間：平均 約 19 時間

* B/U 預金・為替システムへの切替所要時間 = 要員駆けつけの所要時間＋システムの切替作業時間
＋後追い入力の所要時間（後追い入力後業務再開ケース）

・要員駆けつけの所要時間：平均 3 時間

・システムの切替作業時間：平均 11 時間

・後追い入力タイミング：「後追い入力後に業務再開」：3 割，「業務再開後に後追い入力」：約 6 割

・後追い入力の所要時間 ：平均 12 時間

（5）切替所要時間と重要業務（流動性預金の払戻＜現金支払＞）の継続手段の関係

・切替所要時間が「3 時間以下」の金融機関では、「全ての業務を B/U システムで継続」：約 9 割

・切替所要時間が長くなるにつれて、「手作業で継続」の割合が高くなる傾向

（6）B/U データの取得

✧ B/U データ（元帳）の取得間隔

・「メインと B/U 同時更新または 5 分以内」：約 4 割 ， 「24 時間超」：約 1 割

✧ B/U データ（元帳）の保管場所

・「預金・為替システム B/U センター」：約 6 割，「メイン・B/U センター以外の保管施設」：約 3 割

（7）B/U 預金・為替システム稼働後の他システムとの同期

・「同期が失われるシステムへの対応は未定」：約 5 割

（8）メインシステムへの切戻し

・「手順整備済み」：約 3 割 ， ・「システム的には可能だが手順は未整備」：約 6 割

（9）預金・為替システムに関する課題認識と取組み

✧ 震災後の課題認識

・「切替に伴い発生する欠落データへの対応」:約 4 割，

・「（B/U センターでの）大量振込・振替処理データの受付機能」：約 3 割，・「切戻し手順」：約 3 割

✧　現在優先的に取り組んでいる事項

・「切替に伴い発生する欠落データへの対応」：約 3 割，・「他システムの B/U システム充実」：約 2 割

・「切替に伴い外部センターとの間で発生する欠落データへの対応」：約 2 割

Ⅲ．実効性向上を目指したコンティンジェンシープラン策定整備（レジリエンス向上への取り組み）

１．業務継続計画とコンティンジェンシープラン

FISC「金融機関等におけるコンティンジェンシープラン策定のための手引書（第 3 版追補 2)」の資料から、コンティンジェンシープランについて以下に概要をまとめる。

（１）コンティンジェンシープラン（緊急時対応計画）の定義

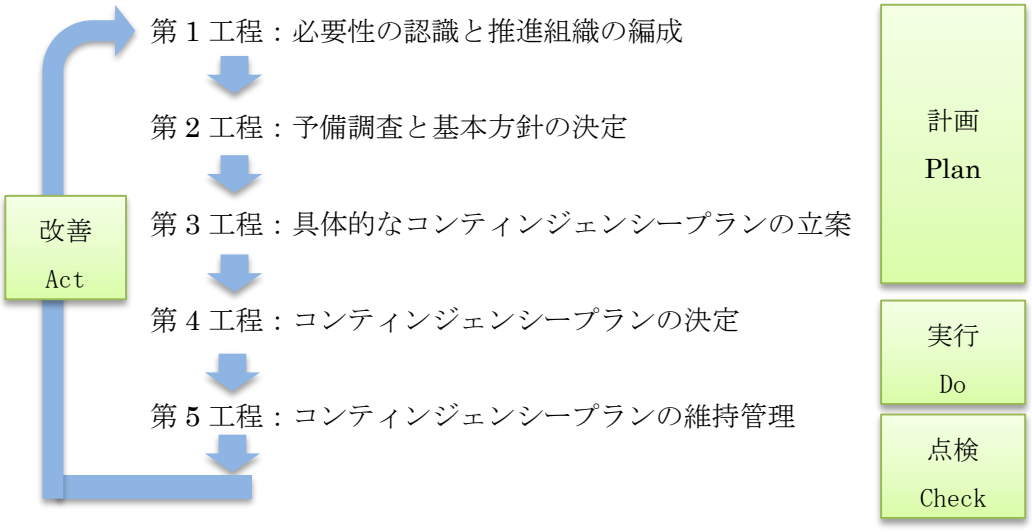
コンティンジェンシープランとは、金融機関等のコンピュータセンター、営業店、本部機構等が、不慮の災害や事故・犯罪、障害等により重大な損害を被り業務の遂行が果たせなくなった場合に、各種業務の中断の範囲と期間を極小化し、迅速かつ効率的に必要な業務の復旧を行うためにあらかじめ策定された緊急時対応計画のことである。

（２）業務継続計画とコンティンジェンシープラン

コンティンジェンシープランが対象とするリスクは、業務継続計画のリスクの内、システムリスク、事務リスク等のオペレーショナルリスクと人命に係るリスクである。

（３）コンティンジェンシープラン策定の流れ（PDCA）

コンティンジェンシープラン策定は、下記の工程に従って進める。第１～第４工程の「計画」フェーズでは、経営層の承認と全社的なコンセンサスが重要となる。「実行」フェーズにおいては、社内体制整備に加え、消防・警察・自治体・社会インフラ等の外部組織への協力依頼を行うことにより、支援体制の充実を図る。「点検」フェーズにおける定期的な教育・訓練・監査とプランの見直しがコンティンジェンシープラン策定整備の要となる。



２．東日本大震災を踏まえたコンティンジェンシープラン整備の取組み（北信越支部　意見交換/コメントより）

（１）危機管理計画・業務継続計画の見直し（取組み例）

東日本大震災を契機として、銀行グループ全体での基本方針を明確にし、従来の危機管理計画・業務継続計画を大幅に見直しを実施した。地方銀行として、常に人道的配慮を最優先とし、金融システムの継続に努めることにより、地域社会・経済の安定と回復に貢献することを基本理念としている。

非常時優先業務を①預金払戻し業務（小口現金支払い）、②決済業務（内国為替、手形交換等）、③融資業務（融資や返済に関する適時的確な対応）に選定。それぞれに目標復旧時間を設定しており、預金払い戻し業務は危機発生から４時間、決済業務・融資業務は２４時間としている。これらの業務のために人・物・金を確保する計画を策定している。

これらの体制の整備内容について職員に対して教育し、各種シナリオに基づく訓練を定期的に行うと共に、計画の見直しを継続的に実施することも、危機管理計画・業務継続計画の重要な構成要素としている。訓練においては、重要な外部委託先と連携した訓練の実施も想定している。

（２）FISC 手引書によるコンティンジェンシープラン整備の取り組み（取組み例）

FISC の「金融機関等におけるコンティンジェンシープラン（緊急時対応計画）策定のための手引書」に則り、コンティンジェンシープランを策定、整備している。

コンティンジェンシープランについては、経営層（取締役会）の承認と全社的な周知は必須であり、PDCA を回すことが重要であり、「コンティンジェンシープランの維持管理体制の整備」「コンティンジェンシープランの維持管理」工程は特に重要と考えている。

（３）コンティンジェンシープラン実効性向上に向けた取り組み（取組み例）

コンティンジェンシープラン実効性を向上さすため以下の取り組みを実施している。

①バックアップセンターの実効性向上

- バックアップすべき業務の再検討
- 目標復旧時間や自社経営環境を考慮したバックアップ保有方針の再検討
- 欠落した取引データの復元手順の整備
- バックアップデータ隔地保管の見直し（媒体による移送、伝送によるバッチ処理、伝送によるリアルタイム処理）
- スプリット・オペレーション（デュアル・オペレーション等）の導入
- 要員の確保（各要員の交通手段の把握、非常事態発生時に徒歩３０分以内に出勤可能な要員の把握）

②通信手段の整備

- コミュニケーションのための通信手段
- 業務データ伝送のための通信手段

③電力調達手段の整備

- 自家発電装置の増強
- 自然エネルギー発電の利用や蓄電（太陽光発電）
- 非常用電源車の導入

④その他の取組事例

- 本部・営業店・センターの免震化工事
- 業務継続に必要な物資の確保（水、食料、燃料）
- 特例払戻し、重要物の格納、顧客案内の掲示等を含む緊急時対応訓練
- 資金および国債の決済を担う日銀ネット（日本銀行金融ネットワークシステム）、および内国為替を担う全銀システム（全国銀行データ通信システム）の運営主体（日本銀行、社団法人全銀ネット）との連携

３．共同センター，データセンター/クラウドシステム利用上の課題（北信越支部 意見交換/コメントより）

（１）共同センター，データセンター/クラウドシステム利用上の留意点

勘定系については共同センターを利用し、各種サブシステムについてはデータセンターのクラウドシステムを利用しているケースにおいて、コンティンジェンシープランに関し以下の点に留意する必要がある。

- 両センターは全く別の拠点に存在し、当然ながら災害発生時の被害と回復の程度には差が出ることが予想される。
- 両サイトと銀行の拠点を結ぶネットワークについても、様々なケースを想定しておく必要がある。複数のサブシステムと勘定系が連動して機能しているため、これらの連携が取れない場合の対応手順や、連携がとれないことを想定した障害運用訓練を行うことが重要である。
- これらのことを充分考慮した目標復旧時間や業務継続手順となっているかも、コンティンジェンシープランに対するシステム監査のポイントとして再度見直す必要がある。

Ⅳ．コンティンジェンシープランに対するシステム監査

１．コンティンジェンシープランに対する監査

FISC「金融機関等のシステム監査指針」の資料から、コンティンジェンシープランの監査について以下にチェックポイントの概要をまとめる。

（１）情報システムのコンティンジェンシープランの策定と維持管理

①コンティンジェンシープランの策定

- コンティンジェンシープランの策定及び重要な変更は、関係部署の同意を得たうえで、取締役会の承認を得ているか。
- コンティンジェンシープランは、重大なシステム障害等が発生した場合、最悪のシナリオや最大リスク等を迅速に、経営陣及び緊急時のリスク対応部門へ報告する体制を盛り込んでいるか。

②コンティンジェンシープラン策定のための体制

- コンティンジェンシープラン策定においては、情報システム部門だけでなく、事務企画部門、営業企画部門、ユーザー部門等が参画しているか。

③リスク分析と評価

コンティンジェンシープランの策定においては、次のような洗出しと評価が行われているか。

✧ 想定されるリスク(原因)の洗出し

・コンティンジェンシープラン策定においては、情報システム部門だけでなく、事務企画部門、営業企画部門、ユーザー部門等が参画しているか。

✧ リスク(原因)の発現により、自社業務（外部委託業務を含む）にどのような影響を与えるのかといったリスク(結果)の洗出し

・時期・時間帯による差異や被害が段階的に進展したり、長期にわたって継続する状況等が考慮されているか。また、広範囲に重大な影響等を及ぼすようなシステム等の障害については、時限性や社外への影響等にも留意されているか。

✧ リスク(結果)に伴う自社の業務と経営資源の洗出し、優先順位づけ

・重要な業務（外部へ委託した業務を含む)、システム、アプリケーション、データ、ﾊｰﾄﾞｳｪｱ

・業務継続に必要な拠点(本部組織、コンピュータセンター、営業店等) 等

④復旧手順の作成

・ 重要な業務について、拠点ごとに複数の被害の発生パターンに応じた復旧手順が作成されているか。

⑤教育・訓練

・ 教育・訓練計画を作成し、必要に応じて取締役会等の承認を得ているか。
・ 教育・訓練計画に基づき、全役職員（外部委託先を含む）に対し定期的に教育・訓練を実施しているか。
・ 訓練は、1）実地訓練と机上訓練の適切な組み合わせ、2）外部委託先との共同の実地訓練の実施、3）バックアップシステムの正常稼働の確認（平常システムへの切戻し後の平常システムの正常稼働も確認）等、効果的な内容になっているか。
・ 必要に応じて、同業他社、監督官庁、中央銀行、業界団体、協同組織中央金融機関、ライフライン業者、外部委託先、地方自治体等の関連する複数の外部組織と合同で行う訓練の計画が策定されているか。

⑥コンティンジェンシープランの維持管理

・ コンティンジェンシープランの維持管理手続に基づき、定期的な見直しが実施されているか。
・ 他金融機関の障害事例や中央防災会議等の検討結果が報告された場合、及び最新の環境変化や状況変化に即しシステムリスクなどの内容に変更が生じた場合、必要に応じて見直しが実施されているか。

（2）緊急事態に対する準備

①緊急時対応組織の準備

・ コンティンジェンシープランには、緊急事態における対策本部及び各拠点組織の構成と役割が明記されているか。
・ コンティンジェンシープランの発動と解除の判断責任者と判断基準が定められているか。
・ コンティンジェンシープラン発動後の指揮命令系統は、対策本部内部、各拠点組織内部、対策本部と拠点間を含めて明確にされているか。また、重要な外部委託先等との連携体制についても考慮されているか。
・ 対策本部と拠点組織の連絡が取れない場合のルール(拠点組織長への権限委譲等)が定められているか。
・ 緊急事態発生時に連絡を必要とする外部組織とそれぞれの連絡方法のリストが作成されているか。
  例： 警察、消防、監督当局、日本銀行、地方公共団体、業態協会、ライフライン事業者、医療関係先、全銀センター、CD/ATM 中継センター、各種ベンダー、サプライチェーン、警備会社、近隣金融機関、対外接続先、各種設備保守会社　等
・ 外部委託している場合、緊急時対応に係る契約条項に必要事項が漏れなく記載されているか。
  例：1）優先的にサポートを受けること、2）外部者との役割分担　等
・ 社内外の情報収集・発信の窓口は一元化されているか。

②人員及び資産の安全確保

・ 勤務時間外の緊急時の、役職員の安否や所在の確認方法が定められているか。
・ 生活用品等の必要な物品が、拠点ごとの事情に応じて準備され、維持管理されているか。
・ 交通遮断、電話不通等により各役職員から所定の連絡先への連絡がとれない場合を想定した、次のような行動基準が定められているか。

例：1）本人、家族の安全優先、2）居住地域での救助・復旧活動への協力、3）警察、その他官公庁等の勧告・命令等の遵守、4）利用すべき交通手段　等

③通信手段の確保及び情報収集

・ 役職員間、組織間の連絡のために、次のようなルートの異なる複数の手段が確保されているか。

例： 専用回線による構内電話網、携帯電話、PHS、無線機、公衆電話、電子メール、衛星電話、災害時伝言サービス　等

④緊急用資源と搬送手段の確保

・ コンピュータセンター、重要な拠点の本番用施設及び災害対策用施設においては、自家発電装置が備えられているか。また、非常時に利用する施設、設備、端末等を確認しているか。なお、自家発電装置は、これらの施設、設備、端末等を利用するのに十分な供給容量や対応可能時間を有しているか。

・ データ及び重要ドキュメントのバックアップが取得され、隔地保管されているか。

⑤緊急時の業務運営の方法

・ 優先すべき業務が明確になっているか。また、優先すべき業務のうち、緊急時に継続すべき必要最小限の業務についても明確になっているか。

・ 手作業で代替する業務について次のような事項を決定しているか。

例：1）手作業での代替が可能な業務の手順、2）手作業で使用する帳票、3）手作業マニュアル等

・ 災害対策システムについて次のような事項を決定しているか。

例：1）バックアップすべき業務、2）バックアップに必要な資源、3）バックアップ保有方針　等

⑥災対システムーバックアップサイト等の対応

・ 災害対策システムは、コンティンジェンシープランと整合性がとれているか。また、バックアップサイトの保有について検討されているか。

・ 通常運用システムとの差異(当初から判明している差異及び通常運用システムの変更の災害対策システムへの反映未了による差異)は管理され、災害対策システム稼働時に対応できるようになっているか。

⑦広報活動の準備

・ 緊急時広報活動手続きは、迅速かつ正確に情報（障害内容・原因・復旧見込み等）が伝達されるように考慮されているか。

・ マスコミ対応の一切を行う組織が対策本部に設置され、また、責任者が任命されているか。

⑧損害状況評価の方法

・ 拠点組織と対策本部の損害状況の伝達方法が明らかになっているか。

・ 被災拠点からの災害状況連絡事項には、被害の程度の他に対処方法、業務継続の可否、復旧見通し等を見極められるような項目も含まれているか。

（3）各拠点(対策本部・コンピュータセンター・営業店等)における各フェーズの対応手順

①初期対応の手順

・ 初期対応手続きが定められ、維持管理されているか。

・ 初期対応手続きは、人命尊重が第一であることが明記されているか。

②暫定対応の手順

・ 暫定対応へ移行するための責任者が定められ、次の内容についての手続きが定められているか。

1) 対策本部における暫定対応移行決定の確認
2) 拠点内組織への暫定対応移行の周知及び暫定対応の内容の指示
3) 暫定対応の進捗、稼働状況、発生した問題点等についての情報収集と、対策本部への報告、必要な応援要員や支援物資の要請

・ 暫定対応システムの稼働準備の手続きが定められているか。
・ 暫定対応システムの稼働開始の手続きが定められているか。
・ 営業店等における暫定対応のための業務処理手続きが定められているか。

③本格復旧の手順

・ 本格復旧対応の準備手続きが定められているか。
・ 暫定対応システムから通常運用システムへの移行手続きが定められているか。

２．コンティンジェンシープランに対する監査のポイント（北信越支部 意見交換/コメントより）

（１）監査としての危機管理計画・業務継続計画への関わり

監査として危機管理計画や業務継続計画に関わる際には以下の点に留意する必要がある。

・ 計画そのものを精査し、内容に問題や齟齬がないかを検証，外部の要因に基づく見直しが行われているか確認する。
・ 訓練に立ち会うことにより、計画の実行に障害となる問題がないかを検証する。金融機関側だけでなく委託先での状況についても監査として実地に立ち会って検証することが必要。

Ⅴ．今後への課題

１．今後の課題（日本銀行アンケートより）

「業務継続体制の整備状況に関するアンケート（2012 年 9 月）調査結果」(2013 年 1 月 18 日 日本銀行金融機構局）の資料から、業務継続体制の整備状況の課題について以下に概要をまとめる。

（１）体制整備を進めるにあたってのボトルネック

・ 体制整備を進めるにあたってのボトルネックとしては、「他社・他業態の業務継続計画との相互依存関係を踏まえた実効性検証の困難性」や「整備推進を統括する部署のマンパワー（およびスキル）不足」、「予算制約」が多い。
・ 東日本大震災前との比較でみると、体制整備を進めるにあたって、「整備推進を統括する部署のマンパワー不足」が増加している。

（２）今後、実施ないし充実が望ましいと考える訓練

・ 今後、実施ないし充実が望ましいと考える訓練としては、「社内横断的な全行訓練」、「リアルタイム型シナリオ・ブラインド訓練」、「ストリートワイド訓練」が多い。

２．今後への課題（北信越支部 意見交換/コメントより）

（１）外部委託先を含めた業務継続態勢の整備

✧ バックアップサイトにおける外部委託先との連携強化に向けた実効性のある訓練の継続実施
✧ 業務継続計画策定におけるパブリッククラウドの有効利用に向けた取り組み
・パブリッククラウドの利用については、特に地方銀行や信用金庫等での利用率が低い状況にある。クラウド利用が進まない理由としては、顧客情報保護など情報セキュリティの不安、サー

ビスの信頼性、法律・規制に対する懸念などが挙げられる。

・しかしパブリッククラウドの利用事例は徐々に増えつつあり、情報系システム（営業支援、電子メール、社内情報共有、e ラーニング）など多くの領域で利用されてきている。

・業務継続計画において安否確認や情報共有のインフラなどでパブリッククラウドを活用する金融機関が増えていく可能性がある。パブリッククラウド利用を健全に促進させ、一層広げていくためには、金融機関とクラウド事業者との間でクラウドのメリットやリスク、適切なリスク管理のあり方について共通認識を持つことが必要である。

（２）金融機関と地域の防災関連当局や社会インフラ事業者との連携

✧ 金融機関と防災関連当局や社会インフラ事業者が、地域を取り巻くリスクを共有するためのコミュニケーションの「場」の創設

・地域金融機関にとって、地域のレジリエンス向上に向けた「官民協働」の取り組みは重要な経営課題となっている。

［取り組み例］県と銀行の災害時の応援協定、県と銀行の移住・交流推進に向けた連携協定

✧ 金融機関と防災関連当局や社会インフラ事業者が連携するストリートワイド訓練の実施を通じた、地域の金融・決済機能維持にかかる対応策全体の実効性確認

（３）社会的なニーズに応える業務継続態勢の整備

✧ 社会的なニーズが高まっている銀行振込の時間延長に対応する業務継続態勢の強化

✧ 将来的には、即時決済の「２４時間３６５日」対応に見合う業務継続態勢の高度化

おわりに

西日本支部合同研究会での北信越支部報告作成にあたって、メールを活用し、北信越支部会員から情報/コメントを提供してもらい、意見交換を行いまとめ上げた。支部会員有志の皆さんの協力の成果であると考える。

今回の活動を通じて、「正常な金融・決済機能の維持」には各金融機関の企業努力とともに、金融システム全体、また地域社会全体としての取組が必要であり、レジリエンス向上のため更なる取組強化が必要であることを認識した。支部会員が日々の業務において本研究の成果を活かし、各々の立場で地域のレジリエンス向上に貢献くだされば幸いである。

今後とも支部例会・研究会と合わせて、インターネットを活用した組織コミュニケーションの向上を図り、支部会員間で幅広く意見交換を行う活動を展開していきたい。

【参考文献】

- 「東日本大震災におけるわが国決済システム・金融機関の対応」2011 年 6 月 24 日 日本銀行決済機構局 http://www.boj.or.jp/research/brp/ron_2011/ron110624a.htm/
- 「業務継続体制の整備状況に関するｱﾝｹｰﾄ（2012 年 9 月）調査結果」2013 年 1 月 18 日 日本銀行金融機構局 http://www.boj.or.jp/research/brp/ron_2013/ron130118a.htm/
- 「ﾊﾞｯｸｱｯﾌﾟ・ｺﾝﾋﾟｭｰﾀｾﾝﾀｰに関するｱﾝｹｰﾄ（2012 年 9 月）調査結果」2013 年 4 月 5 日 日本銀行金融機構局 http://www.boj.or.jp/research/brp/ron_2013/ron130405a.htm/
- 「金融機関等におけるｺﾝﾃｨﾝｼﾞｪﾝｼｰﾌﾟﾗﾝ策定のための手引書（第 3 版追補 2）」2013 年 3 月 金融情報ｼｽﾃﾑｾﾝﾀｰ
- 「金融機関等のシステム監査指針（改訂第 3 版）」2014 年 3 月 金融情報ｼｽﾃﾑｾﾝﾀｰ

以上

＜目次＞

2015.1

近畿支部　【第１４９回定例研究会（ISACA 大阪支部合同）報告】

（ISACA 大阪支部 今本憲児）

１．テーマ　　地域情報化と防災
～CATV ネットワークを利用した緊急告知と地方公共団体の ICT-BCP の現況～

２．講師　　㈱嶺南ケーブルネットワーク　顧問（情報通信担当）　川端 純一 氏

３．開催日時　　２０１４年１２月１３日（土）　１５：００～１７：００

４．開催場所　　大阪大学中之島センター　３階　講義室３０１

５．講演概要

巨大地震や異常気象などの災害に強いまちづくりのポイントとなるのは、①自助、②近助、③共助、④公助、の4つである。特に災害発生直後においては、自分の身は自分で守り（①自助）、向こう三軒両隣が相互に助け合い（②近助）、自主防災組織を組織して地域ぐるみで助け合う（③共助）、といった近隣の人たちの連携（地域防災）が、最も重要になってくるが、それをサポートするのが④公助になる。

地方公共団体による、災害による市民の被害を最小にするための、迅速で正確な、市民のライフスタイルに合わせた多様な情報伝達も④公助の1つである。今回はその事例として、（1）敦賀市地域防災情報システムについて、ご紹介いただいた。また、地方公共団体における（2）業務継続計画（BCP）の策定について、ご講演いただいた。

（1）敦賀市地域防災情報システムの紹介

- 福井県は民放テレビが 2 社しかないため、ケーブルテレビ（CATV）への需要が高く、平成 26 年 6 月末現在で、㈱嶺南ケーブルネットワークの CATV 加入世帯数は 26,482 世帯（市内全世帯の約 94%）になる。敦賀市は、原子力発電所の立地地域であるため、原子力災害時や一般災害時に市民にいち早く、的確な情報を伝達するために、㈱嶺南ケーブルネットワークでは、防災放送チャンネル（防災情報提供用の専用チャンネル）を設けている。
- 平成 26 年 8 月 31 日現在、敦賀市には CATV 以外にも、以下の防災情報の伝達手段がある。
インターネット（敦賀市ホームページ）、携帯電話への Tonbo メール送信、コミュニティーFM、地域防災無線（EPZ 圏内：Emergency Planning Zone：原子力発電所周囲の 10 キロ圏内の防災対策を重点的に構築

すべき地域)、防災情報伝達システム(屋外スピーカー)

- 防災センターで一回情報を入力すれば、上述の防災情報伝達手段に、同じ内容の情報が迅速に、一括で発信されるシステムが作られている。
- 防災情報伝達システム(屋外スピーカー)は、災害の状況や敦賀市からの避難情報、全国瞬時警報システム(J-ALERT)で受信した緊急地震速報などを、CATV ネットワーク及び地域WiMAX経由で放送するシステムである。㈱嶺南ケーブルネットワークが運営している有線ネットワーク網(CATV ネットワーク網)と地域WiMAXとで、通信インフラを冗長化することで、万が一の通信不良時でも確実に放送することができるようにしている。屋外スピーカーに関しては、有事の際に、スピーカーから音が鳴らないという事態が起こらないために、1日4回定時ミュージックを鳴らして、点検を行っている。

(2) 業務継続計画(BCP)の策定について

「地方公共団体における ICT 部門の業務継続計画(BCP)策定に関するガイドライン(平成 20 年 8 月 総務省)の内容をベースに、BCP 策定についてご講演いただいた。

- BCP は、災害に対してレジリエンシー(しなやかに)対応していくために策定するものである。災害発生時の緊迫した最中に、決められたルール(分厚いマニュアル)通りに対応することは難しい。そのため、A4 用紙1枚ほどの簡単にまとめられた BCP は、社員が容易に理解することができ、素晴らしいと考えている。
- 机上訓練の本当の目的は、社員の「意識改革」にある。机上訓練を通して、社員に対して、リスクを考えた行動を意識付けるとともに、自分は今何をしなければならないのか、自覚させる。
- 同ガイドラインは、「自らは無事で住民や企業の救援に全力で当たれる前提」で書かれているが、この前提は、自らが深刻な被害を受けることを想定しておらず、そのような状況下での業務の継続が考慮されていないため、無理がある。
- 一般的に各団体の地域防災計画は、「自らは無事で住民や企業の救援に全力で当たれる前提」で書かれているが、この前提は、自らが深刻な被害を受けることを想定しておらず、そのような状況下での業務の継続が考慮されていないため、ここに BCP 策定の必要性が生じる。
- ICT 部門の BCP 策定で、策定対象・策定範囲の絞りこみの際は、システム成熟度を意識して、策定期間、工数、策定人員、策定費用等、無理をしないように留意する。無理をしてしまうと、実際に災害が発生した場面で機能しなくなる。
- BCP は策定する事が大事である。しかし、地方公共団体においては、BCP 策定はあまり進んでいないのが現状である。

6. 所感

東日本大震災の際は、欲しい情報が中々手に入らず、ノイズの入った情報が錯綜し、歯痒い思いをしたことがあった。そのため、敦賀市の防災情報システムのように、信頼できる情報が適切なタイミングで発信されることは、災害発生時に大変重宝するし、他の地方公共団体でもこのような取り組みが進んで欲しい、と感じた。今回の敦賀市の取り組みを伺って初めて、私の住んでいる市でも同じような取り組みを行っていることを知った。私の危機管理意

識の低さは否めないが、地方公共団体においても、もっと積極的に、このような取り組みをしていることを、住民にアピールして欲しい、と感じた。

BCP の策定に関して、川端氏が仰った「A4 用紙 1 枚ほどの簡単にまとめられた BCP は、社員が容易に理解することができ、素晴らしい」の点は、私も共感できた。全ての事を想定して対策を立てることは難しいし、あまり細かに策定すると、実際に災害が発生した際にマニュアルをいちいち確認して、その場で理解しながら動かなければならず、迅速な対応が求められる状況下では、あまり機能しなくなる、と感じたからだ。但し、A4 用紙 1 枚にまとめても、内容が薄っぺらいと、どう動けばよいかわからず、結局は無用の長物になってしまう。そのため、なかなか難しいとは思うが、社員がしっかりと理解し行動できる、多すぎず少なすぎず、バランスのとれた分量で、BCP を策定する必要があると思った。

今回の講演を拝聴し、災害に対してレジリエンシー（しなやかに）対応していくため、必要な情報を必要な時に入手できる情報源の確保と、その情報を利用して災害に対して柔軟に対応できるような BCP の策定が重要であることを、改めて確認できた。

以上

＜目次＞

2015.1

注目情報（2014.12～2015.1）※各サイトのデータやコンテンツは個別に利用条件を確認してください。

■ 特定個人情報保護委員会、「特定個人情報の適正な取扱いに関するガイドライン」告示(2014/12/11)

特定個人情報保護委員会(委員長、堀部政男一橋大学名誉教授)は、12 月 11 日、「特定個人情報の適正な取扱いに関するガイドライン」を告示した(報道発表は、2014/12/18)。これは、「事業者編」、事業者編の金融業向け「別冊」及び「行政機関等・地方公共団体等編」の三編からなり、マイナンバー制度発足に伴う特定個人情報[注]の取扱いについて、事業者と行政機関等が実施すべきことやその留意点が示されている。

[注]:「特定個人情報」とは、個人番号をその内容に含む個人情報をいう（番号法第 2 条第 8 項)。

とくに、事業者編(金融機関向け別冊を含む)は、2016 年 1 月 1 日から、すべての事業者に義務付けられる源泉徴収票等への個人番号の記載等に関して、法に定められた個人番号の適正な取扱い方法(情報システム上の実装も含む)の指針となるもので、極めて重要なものである(番号法には直罰規定がある)。URL を下記に示す。

「特定個人情報の適正な取扱いに関するガイドライン(事業者編)」
http://www.ppc.go.jp/files/pdf/261211guideline2.pdf

「(別冊)金融業務における特定個人情報の適正な取扱いに関するガイドライン」
http://www.ppc.go.jp/files/pdf/141211kinyu-guideline.pdf

「特定個人情報の適正な取扱いに関するガイドライン(行政機関等・地方公共団体等編)」(2014/12/18 告示)
http://www.ppc.go.jp/files/pdf/261218guideline.pdf

なお、マイナンバー制度とシステムの概要については、会報 1 月号(第 166 号)掲載の月例研究会「マイナンバーと民間サービスとの連携を目指して」(2014/11/19 開催)の報告を参照されたい(会報 1 月号 P11～23)。

■ IPA、「2014 年度情報セキュリティ事象被害状況調査」報告書を公開(2015/1/15)

情報処理推進機構(IPA)は、1 月 15 日、「2014 年度情報セキュリティ事象被害状況調査」報告書を発表した。調査対象期間は 2013 年 4 月～2014 年 3 月、調査対象 13,000 企業、回答数 1,913 件、有効回答率 14.7%である。

サイバー攻撃の被害にあったという回答は 4.2%、発見のみの回答は 15.1%であり、合計(遭遇率)は 19.3%。前回の 13.8%から 5.5 ポイント増加した。ウェブサイトに関する被害が多数を占め、内容は、「ウェブサイトのサービスの機能が低下させられた」が最も多く 22.5%、「ウェブサイトのサービスが停止させられた」被害も 13.8%となっている。ウェブサイトが被害に遭う原因は、管理アカウントの窃取、ウェブサーバの脆弱性への攻撃などである。

標的型攻撃を受けたのはサイバー攻撃に遭遇した前述の 19.3%(368 社)のうち、30.4%(112 社)であった。そのうち被害にあった割合は 18.8%(21 社)。なお、その手口は、「同僚や取引先、サービス事業者からのメールを装い、添付したウイルスファイルを開かせる」が最も多く 54.5%(61 社)、次に「電子メールに表示された URL 経由で攻撃用のウェブサイトに誘導される」が 40.2%(45 社)である。標的型攻撃メールは、ウイルスが添付されているだけでなく、開封を促すため文面等が巧妙になっていることから注意が必要である。報告書等の URL は、以下のとおり。

1) 調査報告書:　https://www.ipa.go.jp/files/000043418.pdf
2) プレスリリース全文:　https://www.ipa.go.jp/files/000043388.pdf
3) プレスリリース(別紙):　https://www.ipa.go.jp/files/000043389.pdf

なお、サイバー攻撃の動向や手口等、サイバーセキュリティに関しては、月例研究会「企業におけるセキュリティ戦略」(2014/12/20 開催)の報告が本会報に掲載されているので参照されたい。

＜目次＞

2015.1

【協会主催イベント・セミナーのご案内】

■近畿支部第 45 回システム監査勉強会（大阪）

申し込み受付中	日時：2015年2月 21 日（土）13:00～17:00 場所：大阪大学中之島センター　2 階　講義室 201		
	SAAJ 本部の月例研究会の DVD を視聴し、討議する。		
	テーマ 1	第 196 回月例研究会(2014 年 10 月 30 日開催) 「オープンデータを中心にIT政策の動向全般」	
		講師	経済産業省　CIO補佐官　平本　健二　氏
		講演骨子	2020 年に向け世界最先端 IT 国家創造宣言が現在進められているが、その中核となるオープンデータ、オープンガバメントの動向、及び、IT 政策の取り組み状況や課題について解説を行う。番号制度、パーソナルデータ、セキュリティの話ではなく、攻めの IT 戦略が話の中心となる。
	テーマ 2	第 197 回月例研究会(2014 年 11 月 19 日開催) 「マイナンバーと民間サービスとの連携を目指して」	
		講師	経済産業省　CIO補佐官　満塩　尚史　氏
		講演骨子	平成 28 年度からマイナンバー制度と呼ばれる社会保障・税番号法（「行政手続きにおける特定の個人を識別するための番号の利用等に関する法律」）が利用開始される。このマイナンバー制度では、個人に付与される個人番号は、法律で定められた業務以外での利用や他人に提供することはできない。一方、民間サービスにおいても、マイナンバー制度を利用したいという意見もある。前記の通り、個人番号そのものは、利用することはできないが、個人番号を使わないで、ID 連携トラストフレームワークを活用し、民間サービスとマイナンバー制度を連携させ、利活用できる可能性がある。 また、社会保障・税番号制度では、個人に個人番号を付与するだけでなく、法人や行政機関に法人番号を付与し、インターネット経由で法人番号、法人名、本社所在地が、提供される。ここでは、マイナンバー制度の概要と、マイナンバーを民間サービスで利活用する仕組みとしての ID 連携トラストフレームワークをご紹介します。更には、法人番号の民間利活用に関する期待についてもご紹介します。
お申し込み			http://www.saaj.or.jp/shibu/kinki/benkyoukai45.html

■システム監査普及サービス（全国）

申し込み常時受付中	情報システムの健康診断をお受けになりませんか。　実費のみのご負担でお手伝いいたします。	
	概要	経験豊富な公認システム監査人が、皆様の情報システムの健康状態を診断・評価し、課題解決に向けてのアドバイスをいたします。これまでに多くの監査実績があり、システム監査普及サービスを受けられた会社等は、その監査結果を有効に活用されています。 システム監査の普及・啓発・促進を図る目的で実施しているものです。監査にかかる報酬は無償で、監査の実施に要した実費（通信交通費、調査費用、報告書作成費用等）のみお願いしております。ご相談内容や監査でおうかがいした情報等は守秘します。 詳細はHPでご案内しています。（ http://www.saaj.or.jp/topics/hukyuservice.html ）
お問合わせ		システム監査事例研究会主査　大西（Email：　jireiken@saaj.jp　）

＜目次＞

■中堅企業向け「6ヶ月で構築するPMS」セミナー（東京）

申し込み常時受付中	概要	個人情報保護監査研究会著作の規程、様式を用いて、6 ヶ月でPMSを構築するためのセミナーを開催します。 詳細をHPでご案内しています。(http://www.saaj.or.jp/shibu/kojin.html)
	基本コース	月 1 回(第 3 水曜日)14 時～17 時(3 時間)×6 ヶ月 ※他に、月 2 回の応用コースなどがあります。
	料金	9 万円/1 名～(1 社 3 名以上割引あり)
	会場	日本システム監査人協会 本部会議室(茅場町)
	テキスト	SAAJ『個人情報保護マネジメントシステム実施ハンドブック』

■公認システム監査人特別認定講習（東京・大阪）

開催中	公認システム監査人(CSA:Certified Systems Auditor)およびシステム監査人補(ASA:Associate Systems Auditor)の資格制度にもとづく、認定条件を得るための講習です。	
	概要	システム監査技術者試験と関連性のある各種資格の所有者については、特別認定制度に基づく本講習により、CSA・ASA 認定申請に必要な資格要件を満たすことができます。特別認定制度の詳細はHPで公開しています(http://www.saaj.or.jp/csa/shosai.pdf)。
お申し込み		講習開催スケジュールと申し込み先をHPでご案内しています。 (http://www.saaj.or.jp/csa/tokubetsu_nintei.html)

【外部主催イベント・セミナーのご案内】

■ＩＳＡＣＡ東京支部 2015 年 1 月度月例会（東京）

日時:2015 年 1 月 28 日(水) 18:30～20:10 場所:日本教育会館 一ツ橋ホール	
テーマ	クラウドインフラ環境におけるセキュリティと統制
講師	アマゾン データ サービス ジャパン株式会社 プロフェッショナルサービス本部 セキュリティコンサルタント 高田 智己 氏 セキュリティ・アシュアランス本部 本部長 日本・アジア太平洋地域担当 梅谷 晃宏 氏 ソニー銀行株式会社 システム企画部 マネージャー(基盤統括担当) 大久保 光伸 氏
概要	昨今、コストの最適化やビジネス要件に対する迅速性・俊敏性といったことを求める様々な企業でクラウドが活用されています。本講演ではクラウドのインフラストラクチャーに求められるセキュリティや統制について解説をし、実例を交えてどのようにクラウドの評価と導入を行ったか紹介を致します。
詳細	http://www.isaca.gr.jp/education/

＜目次＞

2015.1

協会からのお知らせ 【 第 14 期通常 総会のご案内 】

日本システム監査人協会　事務局

日本システム監査人協会(SAAJ)会員各位

■第13期通常総会のご案内

日本システム監査人協会の第14期通常総会を、下記の通り開催致します。
万障お繰り合わせの上ご出席をお願い申し上げます。

記

1. 日時: 2015年2月20日(金)　13:30～ (受付開始:12:45)
2. 場所: 東京都港区芝公園3丁目5番8号 機械振興会館 地下3階 研修1室
　アクセス:http://www.jspmi.or.jp/kaigishitsu/access.html
3. 第14期通常総会議事　13時30分 ～ 15時
　13:30開 会
　(1) 2014年度 事業報告の件
　(2) 2015年度 事業計画の件
　(3) 2015年度 予算の件
　(4)その他
　15:00閉 会
　(休 憩)
4. 特別講演　15時30分 ～ 17時
　15:30 開演
　演題:「激変するIT社会のなかで IT人材が担うべき新たな役割
　～ イノベーションとITガバナンスの主体としてのIT人材 ～ 」
　講師:独立行政法人情報処理推進機構(IPA)
　IT人材育成本部長 理事 田中 久也 氏
　17:00 閉演

5. 懇親会　17時30分 ～ 19時30分
　17:30 開 場 (機械振興会館地下3階会議室)
　参加費:3,000円 (当日会場にてお支払いください)
　20:00 閉 場

※総会、懇親会の参加申込は2015年1月末に、協会ホームページにて受け付けます。

以上

＜目次＞

2015.1

協会からのお知らせ

【ＣＳＡ／ＡＳＡ資格をお持ちの方へ ：資格更新申請手続きについて】

2015 年度公認システム監査人及びシステム監査人補の更新手続きのお知らせです。

・資格認定期限が 2014 年 12 月 31 日で満了となる方について、認定の更新手続を行います。

・資格更新申請の受付期間は 2015 年 1 月 1 日(木)から 1 月 31 日(土)までの 1 か月間です。

・今回の更新対象者は、資格認定番号が下表の方です(2014 年度よりすべて 2 年度ごとの更新です)。

	取得年度	CSA 認定番号	ASA 認定番号	**2015 年 1 月更新**	ご参考 2016 年更新
1	2002 年度	K00001～K00253	H00001～H00193		○
2	2003 年度	K00254～K00320	H00194～H00263		○
3	**2004 年度**	**K00321～K00357**	**H00264～H00316**	**○**	
4	2005 年度	K00358～K00401	H00317～H00384		○
5	2006 年度	K00402～K00447	H00385～H00433		○
6	**2007 年度**	**K00448～K00478**	**H00434～H00473**	**○**	
7	2008 年度	K00479～K00518	H00474～H00514		○
8	**2009 年度**	**K00519～K00540**	**H00515～H00538**	**○**	
9	**2010 年度**	**K00541～K00553**	**H00539～H00557**	**○**	
10	2011 年度	K00554～K00568	H00558～H00572		○
11	**2012 年度**	**K00569～K00580**	**H00573～H00586**	**○**	
12	2013 年度	K00581～K00596	H00587～H00595		○

・資格更新申請には、更新申請書や継続教育実績申告書などの提出が必要です。準備をお願いします。

・更新手続の詳細は、HP の「CSA の資格をお持ちの方へ」(http://www.saaj.or.jp/csa/forCSA.html)をご覧ください。

＜目次＞

2015.1

新たに会員になられた方々へ

新しく会員になられたみなさま、当協会はみなさまを熱烈歓迎しております。
先月に引き続き、協会の活用方法や各種活動に参加される方法などの一端をご案内します。

・協会活動全般がご覧いただけます。 http://www.saaj.or.jp/index.html
・会員規程にも目を通しておいてください。 http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・皆様の情報の変更方法です。 http://www.saaj.or.jp/members/henkou.html

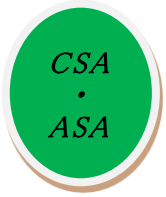
・会員割引や各種ご案内、優遇などがあります。 http://www.saaj.or.jp/nyukai/index.html
　セミナーやイベント等の開催の都度ご案内しているものもあります。

・各支部・各部会・各研究会等の活動です。 http://www.saaj.or.jp/shibu/index.html
　皆様の積極的なご参加をお待ちしております。門戸は広く、見学も大歓迎です。

・皆様からのご意見などの投稿を募集しております。
　ペンネームによる「めだか」や実名投稿があります。多くの方から投稿いただいておりますが、さらに活発な利用をお願いします。この会報の「会報編集部からのお知らせ」をご覧ください。

・協会出版物が会員割引価格で購入できます。 http://www.saaj.or.jp/shuppan/index.html
　システム監査の現場などで広く用いられています。

・セミナー等のお知らせです。 http://www.saaj.or.jp/kenkyu/index.html
　例えば月例研究会は毎月100名以上参加の活況です。過去履歴もご覧になれます。



・公認システム監査人へのSTEP-UPを支援します。
　「公認システム監査人」 と「システム監査人補」で構成されています。
　監査実務の習得支援や継続教育メニューも豊富です。
　CSAサイトで詳細確認ができます。 http://www.saaj.or.jp/csa/index.html

・PDF会報と電子版会報があります。 (http://www.saaj.or.jp/members/kaihou_dl.html)
　電子版では記事への意見、感想、コメントを投稿できます。
　会報利用方法もご案内しています。http://www.saaj.or.jp/members/kaihouinfo.pdf

・右ページをご覧ください。 http://www.saaj.or.jp/toiawase/index.html
　各サイトに連絡先がある場合はそちらでも問い合わせができます。

＜目次＞

2015.1

【　ＳＡＡＪ協会行事一覧　】

赤字：前回から変更された予定

2015 年	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
1 月	7 日 16:00 総会資料(〆) 8 日 理事会:通常総会資料原案審議 9 日 総会開催案内掲示・メール配信 19 日 会計:2013 年度決算案 24 日 会計:2013 年度会計監査 26 日 総会申込受付開始(資料公表) 31 日 償却資産税・消費税	認定委員会:CSA・ASA 更新申請受付 〔申請期間 1/1～1/31〕 20 日 第 199 回月例研究会 20 日 春期公認システム監査人募集案内 〔申請期間 2/1～3/31〕	10 日 会計:支部会計報告期限 16 日 近畿支部:支部総会
2 月	5 日 理事会:通常総会議案承認 20 日 第 14 期通常総会・特別講演 25 日 法務局:資産の変更登記、 活動報告書提出 **28 日 年会費納入期限**	CSA・ASA 春期募集(2/1～3/31) 28 日-3 月 1 日 事例研:第 25 回システム 監査実務セミナー(前半)	
3 月	2 日 東京都への事業報告書提出 2 日 年会費未納者宛督促メール発信 4 日 認定 NPO 法人東京都による調査 12 日 理事会	4 日 第 200 回月例研究会 14-15 日 事例研:第 25 回システム 監査実務セミナー(後半)	
4 月	9 日 理事会 末日 法人住民税減免申請	認定委員会:新規 CSA/ASA 書類審査	19 日 2015 年春期情報技術者試験
5 月	14 日 理事会 29 日 会費未納者チェック(6 月 1 日督促)	認定委員会:新規 CSA/ASA 面接	
6 月	11 日 理事会 末日 支部会計報告依頼(〆切 7/14) 末日 助成金配賦額決定(支部別会員数)	10 日 新規 CSA/ASA 承認	
	以下は、2014 年に実施した行事一覧です。		
7 月	1 日 会費未納者督促状発送 8 日 支部助成金支給 10 日 理事会	1 日 秋期公認システム監査人募集案内 〔申請期間 8/1～9/30〕 3 日 第 192 回月例研究会 22 日 第 193 回月例研究会	14 日 支部会計報告〆切
8 月	(理事会休会) 会費督促電話作業(役員) 23 日 中間期会計監査	秋期公認システム監査人募集開始～9/30 20 日第 194 回月例研究会 30-31 日 事例研:第 24 回システム監査実務セミナー(前半)	30～31 日東北支部:合宿研修会 30～31 日近畿支部:システム監査体験セミナー(実践編)
9 月	11 日 理事会	13-14 日 事例研:第 24 回システム監査実務セミナー(後半) 8 日 第 24 回CSAフォーラム 18 日 第 195 回月例研究会	6～7 日中部、北信越支部/JISTA 中部合同合宿
10 月	9 日 理事会	30 日 第 196 回月例研究会	25 日 近畿支部:IT-BCP 体験セミナー
11 月	13 日 理事会 14 日 予算申請提出依頼(11/30〆切) 支部会計報告依頼(1/10〆切) 18 日 2015 年度年会費請求書発送準備 20 日 会費未納者除名予告通知発送 30 日 予算申請提出期限	中旬 認定委員会:CSA 面接 19 日 第 197 回月例研究会 20 日 CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 28 日 認定委員会:CSA 面接結果通知	29 日 西日本支部合同研究会 (開催場所:大阪市)
12 月	1 日 2015 年度年会費請求書発送 2015 年度予算案策定 11 日 理事会:2015 年度予算案、 会費未納者除名承認 12 日第 14 期総会資料提出依頼(1/9〆切) 19 日 会計:2014 年度経費提出期限	6 日 法制化検討 PT 事前打合せ 6 日 事例研:第 16 回課題解決セミナー 10 日 認定委員会:CSA/ASA 更新手続案内メール発信 16 日 第 198 回月例研究会 20 日 CSA 認定証発送 21 日 第 25 回 CSA フォーラム	13 日 東北支部:支部総会

※注　定例行事予定の一部は省略。

＜目次＞

2015.1

会報編集部からのお知らせ

1. 会報テーマについて
2. 会報記事への直接投稿(コメント)の方法
3. 投稿記事募集

□■ 1. 会報テーマについて

2014 年度の年間テーマは、「○○○のためのシステム監査」とし、四半期ごとに「○○○のための」について具体的なテーマを設定して、システム監査に関する皆様からのご意見ご提案を募集してまいりました。様々なご意見ご提案をいただき、ありがとうございました。

2015 年度の年間テーマは、「システム監査人の魅力」です。これまでは「システム監査」に焦点を当ててきましたが、今年度は「システム監査人」に焦点を当てて考えてみたいと思います。2 月号から 4 月号までは、「マネジメントシステム内部監査におけるシステム監査人の役割」をテーマといたします。皆様の幅広いご意見をお待ちしています。

会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマももちろん大歓迎です。皆様のご意見を是非お寄せ下さい。

□■ 2. 会報の記事に直接コメントを投稿できます。

会報の記事は、

1)PDF ファイルの全体を、URL(http://www.skansanin.com/saaj/)へアクセスして、画面で見る

2)PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る

3)会報 URL(http://www.skansanin.com/saaj/)の個別記事を、画面で見る

など、環境により、様々な利用方法をされていらっしゃるようです。

もっと突っ込んだ、便利な利用法はご存知でしょうか。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」)

□■ 3. 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(毎月メール配信)を利用してください)
2. 会員投稿 (Word の投稿用テンプレート(毎月メール配信)を利用してください)
3. 会報投稿論文 (「会報掲載論文募集要項」及び「会報掲載論文審査要綱」があります)

会報記事は、次号会報募集の案内の時から、締め切り日の間にご投稿ください。 システム監査にとどまらず、情

報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します。ただし、投稿された記事については、表現の訂正や削除を求め、又は採用しないことがあります。また、編集担当の判断で字体やレイアウトなどの変更をさせていただくことがあります。

次の投稿用アドレスに、次号会報募集案内メールに添付されるフォーマット(Word)を用いて、下記アドレスまで、メール添付でお送りください。

投稿用アドレス:saajeditor ☆ saaj.jp (☆は投稿時には@に変換してください)

バックナンバーは、会報サイトからダウンロードできます(電子版ではカテゴリー別にも検索できますので、ご投稿記事づくりのご参考にもなります)。

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。

会員限定記事

【本部・理事会議事録】(当協会ホームページ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/

■会報は会員への連絡事項を含みますので、会員期間中の会員へ自動配布されます。
会員でない方は、購読申請・解除フォームに申請することで送付停止できます。

【送付停止】 http://www.skansanin.com/saaj/

■□■SAAJ会報担当━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━
編集委員: 藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、藤野明夫
編集支援: 仲厚吉 (会長)
投稿用アドレス: saajeditor ☆ saaj.jp (☆は投稿時には@に変換してください)
━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━━

＜目次＞