



認定 NPO 法人

日本システム監査人協会報

2020年11月号

No.236

No.236 (2020年11月号) &lt;10月25日発行&gt;

デジタル化による攻め

セキュリティ対策による守り

#巻頭言 #北海道支部報告

#第250回月例研究会



画像提供: 西場師守

## 巻頭言

## 『 デジタルガバナンスコードの意義 』

会員番号 608 三谷 慶一郎 (副会長)

2020年8月に経済産業省と東京証券取引所は共同で「デジタルトランスフォーメーション (DX) 銘柄」として35社を選定しました。またその中から小松製作所とトラスコ中山の2社を「DX グランプリ 2020」としてデジタル時代を先導する代表的企業として発表しています。DXは既にあらゆる企業にとって重要な経営テーマになっているといえるでしょう。

企業のDX推進を後押しする政策として、経済産業省は「デジタルガバナンスコード」の策定とそれに基づく認定制度の実施を予定しています。デジタルガバナンスコードは、2019年から検討が進められていたもので、企業がDXに取り組んでいくために実践すべき事柄を、ちょうどコーポレートガバナンスコードのようにまとめて整理したものです (ご縁があって私も検討作業に加わっています)。企業は、自社がこのデジタルガバナンスコードを遵守していることを、ステークホルダー (投資家、従業員、取引先等) に対して開示することによって、DX推進企業としてアピールすることができます。

DXを目指す企業と、その準備を怠っている企業とでは、中期的にその競争力に大きな差が生まれるでしょう。しかしDXを進めようとしているかどうかは、直接財務諸表等に現れるものではないため、外部から見て把握することが困難です。これを可視化できるようにすることがデジタルガバナンスコードの目的だと言えます。

デジタルガバナンスコードは、「1. 経営ビジョン・ビジネスモデル」「2. 戦略 (①組織づくり・人材に関する方策、②ITシステム・デジタル技術活用環境の整備に関する方策)」「3. 成果と重要な成果指標」「4. ガバナンスシステム」の大きく4つの項目から構成されています。先に述べた通り、今年度からこれらの観点に基づき「DXを推進する準備が十分にできている」と見なせる企業を認定する制度が開始されることとなります。

デジタルガバナンスコードは、企業がDXつまり、デジタル技術を活用して、ビジネスモデルやそれに付随する組織、プロセス等を変革させて競争優位をつくるスタートラインに立っていることを第三者的に評価するものです。これは戦略性・有効性を目的としたシステム監査とかなり近い概念だと考えられるのではないのでしょうか。デジタルガバナンスコードの周辺にも監査人の活躍の余地はあると考えます。

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。

## <目次>

○ 巻頭言 .....	1
『 デジタルガバナンスコードの意義 』	
1. めだか .....	3
【 システム監査人のターニングポイント – ファクトフルネスを考える 】	
2. 投稿 .....	4
【 コラム 】 AI 時代に負けないために、システム監査人はどうあるべきか？ (11)	
3. 本部報告 .....	8
【 「個人情報保護法 2020」の改正内容 ～PMSハンドブック読者！必読！～ 第5回 】	
【 第250回月例研究会：講演録 既存対策を凌駕し続けるサイバー脅威と整備すべき態勢 】	
4. 支部報告 .....	14
【 北海道支部 2020年度9月の月例研究会 】	
5. 注目情報 .....	18
【 「情報セキュリティ白書 2020」無料 PDF 版が公開 IPA 】	
6. セミナー開催案内 .....	19
【 協会主催イベント・セミナーのご案内 】	
【 情報システム監査実践マニュアル(第3版)～特別頒布のご案内～ 】	
7. 協会からのお知らせ .....	21
【 新たに会員になられた方へ 】	
【 協会行事一覧 】	
8. 会報編集部からのお知らせ .....	23

## めだか 【 システム監査人のターニングポイント – ファクトフルネスを考える 】

新型コロナウイルス感染症は基本的な感染予防対策で感染を最小限に抑える—こまめな手洗い、三密を避ける、鼻と口をマスクするなどである。新型コロナウイルス感染症との戦いは長期戦となってきた。感染の可能性は誰にでもあり感染者への差別は許されないと思う。



さて、「FACTFULNESS」という本を紹介しよう。最初、質問 1 から質問 13 までであるが、そのうち質問 1、質問 2、質問 3 と質問 9 を挙げてみる。

質問 1 現在、低所得国に暮らす女子の何割が初等教育を修了するでしょう？

A 20% B 40% C 60%

質問 2 世界で最も多くの人住んでいるのはどこでしょう？

A 低所得国 B 中所得国 C 高所得国

質問 3 世界の人口のうち、極度の貧困にある人の割合は、過去 20 年でどう変わったでしょう？

A 約 2 倍になった B あまり変わっていない C 半分になった

質問 9 世界中の 1 歳児の中でなんらかの病気に対して予防接種を受けている子供はどのくらいいるでしょう？ A 20% B 50% C 80%

次に、分断本能、世界は分断されているという思い込みについて説明がある。すなわち、レベル 1 は 1 日 1 ドルおよそ 10 億人、レベル 2 は 1 日 4 ドルおよそ 30 億人、レベル 3 は 1 日 16 ドルおよそ 20 億人、レベル 4 は 1 日 32 ドルおよそ 10 億人という所得になっている。人は、何事も 2 つのグループに分けて、いわゆる「二項対立」を求めるが、事実はその単純ではない。現在、世界の大部分は真ん中のレベル、つまりレベル 2 とレベル 3 にて暮らしている。

続いて、ネガティブ本能、世界はどんどん悪くなっているのか。直線本能、世界の人口はひたすら増え続けるのか。恐怖本能、危険でないことを恐ろしいと考えてしまうのか。過大視本能、目の前の数字がいちばん重要なのか。パターン化本能、ひとつの例がすべてに当てはまるのか。宿命本能、すべてはあらかじめ決まっているのか。単純化本能、世界はひとつの切り口で理解できるのか。犯人捜し本能、誰かを責めれば物事は解決するのか。焦り本能、いますぐ手を打たないと大変なことになるのか、とある。

システム監査人は、FACTFULNESS、すなわち、10 の思い込みを乗り越え、データを基に世界を正しく見る習慣を、みずから持ちたいものだ。ちなみに、1 C 2 B 3 C 9 C である。(空心菜)

資料：「FACTFULNESS 10 の思い込みを乗り越え、データを基に世界を正しく見る習慣」ハンス・ロスリング、オーラ・ロスリング、アンナ・ロスリング・ロンランド 著 上杉周作、関美和 訳 日経 BP 社

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

<目次>

## 【コラム】AI時代に負けないために、システム監査人はどうあるべきか？（11）

会員番号 1644 田淵隆明（近畿支部 システム監査法制化推進プロジェクト）

### 1. はじめに

戦後最大の国難とも言われる新型コロナについては、ワクチンの確保が進み（政府が無償供給を検討との報道あり）、国産の治療薬である「アビガン」（ファビピラビル）の承認申請が行われた（文献3）。**我々は、何としてでも、この危機を乗り切らねばならない。後述するように、2006年の会計基準の改悪である「研究開発費の一律費用処理」は新薬開発の支障になっている。**1月号より、「AI時代に負けないために、システム監査人はどうあるべきか」の連載を始めたが、その契機となったのは、下記の3点の疑問であった。

- ・何故、平成の時代に、日本人がここまで劣化してしまったのか？
- ・何故、このようなデタラメがまかり通る時代になってしまったのか？
- ・何故、他のG7先進国と異なり、日本だけが景気回復出来ないのか？

⇒それには次の8個の原因・元凶があると筆者は考えている。

#### ★平成が“暗黒の時代”となった「8個の元凶」★

- ①「新自由主義」的政策による、中間層の破壊と階級の固定化。(⇒2・6月号)
- ②「ゆとり教育」による、学力低下・学級崩壊及びモラルの低下、**及び、大学のカリキュラムの不備**(6・7・8・9・10月号)
- ③「SI認定・登録」の廃止(2003年、2010年)によるIT業界の劣化及びIT有資格者の地位の低下(⇒1月号)
- ④「製造物責任法」の立法不備による、不備ソフトウェアの放置(⇒3月号)
- ⑤「研究開発費の一律費用処理」による、頭脳軽視と近視眼的経営(⇒4・5・6月号)
- ⑥ ⑤と合わせ技での「金融検査マニュアル」による開発力低下(⇒5月号)
- ⑦誤った時価会計の導入による混乱、及び、会計基準の不備(⇒7・9月号)
- ⑧数学を知らない経済学者・アナリストの闊歩(⇒10月号)

今回は②と⑤と⑥を取り上げます。また、前回に引き続き、「2021年問題」を取り上げます。

### 2. 「英会話」を巡る不毛な論争

1970年代からしきりにマスコミで取り上げられるようになった「日本人は何故英語が話せないのか？」・・・という問いかけは、「文法不要論」や「学校英語不要論」に行きつくことが少なくなかった。結局のところ、「文法か会話か？」という不毛な二元論が繰り返され、根本的な英語力の向上は実現しなかった。特に、「会話中心＝実用的」というテーゼの暴走は、「フォーマルな表現」の蔑視や、俗語(Slang)や Politically Incorrectなフレーズの氾濫を誘発する結果となってしまった。筆者も英語会議に出席することは少なくない方であるが、**ビジネス・レベル以上の英語力を確保するには、文法力・語彙力は必要不可欠**である。勿論、ToEICでネイティブ・レベルとされるAランク(860以上)を得るには、相当高度な文法知識が求められることは言うまでもない。

筆者は「英語が話せない理由」は、文法教育にあるのではなく、以下のことを教えなかったことに真の原因があると考えている。

- ①(特に米語における)語頭 h・語尾 d/t の黙音化、フレーズ内での音素の消失・変化
- ②アクセントを取らない冠詞・接続詞・前置詞・関係代名詞・人称代名詞における音素の消失・変化
- ③帯気音(p→f=ph, b→v, c/k→ch, t/d→th, r→rh/wr など)の理論
- ④鼻音(t/d→n, p/b→m)の同化現象、母音に挟まれた子音の消滅、母音連続による異化現象

★仏語の Liason, Enchainement, Elision の考え方などは特に有用であるので、指導要領に盛り込むべきである。特に米国の東部諸州では第一外国語は仏語であり、所謂「東部訛り」の要因の1つと考えられる。

米国では1980年代以降、急速にこれらの現象が進行した。[文献5]と[文献6]を比較して頂きたい。また、上記の①～④については、[文献1]と[文献2]に詳述してあるので、是非、御覧頂きたい。

★don' t の t を発音しないのも、in a が「イナ」、in the が「インナ」と聞こえるのも、and の Liason 禁止も仏語教育の影響と考えられる。ただし、仏語と異なり、-s, -ts, -st は発音する。

古い話で恐縮であるが、筆者の中学時代「ゴダイゴ」というロックバンドが人気を集めていた。そのヒット曲の1つの「Holy and Bright」のサビの部分の歌詞は次の通りである。[文献4]

Holy, holy and bright, a star is shining so holy and bright.  
Holy, holy and bright, never let it go out of your sight.

敢えてカタカナで表現すれば、次のような発音に近い。

ホウリ、ホウリ・エン・ブライ・(タ)(※)、スターリ・シャイニン、ソ、ホウリ・エン・ブライ  
ホウリ、ホウリ・エン・ブライ、ネヴァー・レリゴー、アウド・ヴォー・サイ

※冠詞 a はアフタクト扱いであり、bright の t と lision して「ブライ・タ」となる。初期版では a が無く、「ブライ」となる。

### 3. 「研究開発費の一律費用処理」及び「金融検査マニュアル」

先日、米国の Trump 大統領が新型コロナに感染し、3 日後に公務に復帰した。その際に注目されたのが新薬やワクチンの開発と承認のスピードの問題である。我が国ではそのスピードは大変遅く、[参考文献 3]のような報道があったものの、10/12 時点で承認に至っていない。製薬分野に限らず、精密機械など、昭和の日本の繁栄を支えた我が国の産業競争力は、暗黒の平成 30 年間を通じて下落を続け、回復の糸口は見いだせていない。やはり、**2006 年の「財務諸表等規則」の改悪により、繰延資産の「試験研究費」が廃止され、研究開発費(R&D 費用)が全て一律費用処理されるようになったことが響いている**と考えられる。しかも、(約 5%を除いて)税務上損金に算入できない。これは研究開発費が「罰金・課徴金」や「接待交際費」と同等の扱いを受けていることに他ならない。この制度改悪の結果、研究開発をすればするほど赤字となり、更に、2010 年度までは金融検査マニュアルによる「貸し剥がし」に怯えるという、**製造業が新製品を開発するには極めて過酷な状況**が 2006 年以降継続している。これは先進国 G7 で唯一の狂態であり、一刻も早い改正が必要である。なお、**IFRS(国際会計基準)も米国基準も中国基準も、研究開発費は資産計上可能**である。

★具体的な改正条文案としては、上場企業については「財務諸表規則」の第二十八条第一項に第 12 号を追加し、現行の第 12 号の「その他」を繰り下げるだけで対応可能である。

(無形固定資産の区分表示)

第二十八条 無形固定資産に属する資産は、次に掲げる項目の区分に従い、当該資産を示す名称を付した科目をもつて掲記しなければならない。

- 一 のれん
- 二 特許権
- 三 借地権 (地上権を含む。)
- 四 商標権
- 五 実用新案権
- 六 意匠権
- 七 鉱業権
- 八 漁業権 (入漁権を含む。)
- 九 ソフトウェア
- 十 リース資産 (財務諸表提出会社がファイナンス・リース取引におけるリース物件の借主である資産であつて、当該リース物件が第二号から前号まで、次号及び第十二号に掲げるものである場合に限る。)
- 十一 公共施設等運営権
- 十二 研究開発費(研究及び開発のために発生した費用の内、製造原価に含まれないものであって、一般管理費に計上しないもの)**
- 十三 その他

※1.「連結財務諸表規則」については、本規則が準用されるため改正は不要。

※2.中小企業については、「会社計算規則」の第七十四条第三項において同様の改正を行えばよい。

### 4. 【補足 1】”金曜日は肉食禁止”のドイツ・バイエルン州とオーストリア

8 月号・9 月号において、文化的背景の話題を取り上げた。ドイツと言えば先進国であり、日本では、「政教分離が徹底している」というイメージが強い。しかし、実情は真逆である。

特に、南部の Bayern (バイエルン) 州(州都は München)では、**金曜日は肉食禁止**の慣習があり、ハンバーガー・ショップのメニューも金曜日は魚メニューのみとなる。世界に輝く自動車メーカー BMW (Bayerische Motoren Werke AG)、Audi、サッカーのブンデス・リーガ(Fußball Bundesliga)の強豪であるバイエルン・ミュンヘン(Fußball-Club Bayern München e.V.)のある Bayern 州で、このような慣習が存在することを意外に思う日本人は少なくないと思われる。

※これは法的義務ではない。また鶏肉は除かれる。しかし、復活祭直前の「聖金曜日」(受難の金曜日)には、レストランでの音楽の演奏の禁止であり、ディスコやクラブは閉店しなければならないという法律がある。この「聖金曜日」についての規制は、西隣のBaden-Württemberg(バーデン・ビュルテンブルク)州など多くの週にも存在する。Baden-Württemberg州には、ERPシステムのSAP SEのほかMercedes-Benz, Porscheなどの本社がある。また、有名なディペア発祥の地でもある。

同様のことは、隣国のオーストリア(Österreich)においても見られる。なお、**ギリシャにおいては、水曜日も肉食を避ける慣習が存在する。**また、火曜日は縁起の悪い日とされ、お祝いごとは避けるべきである。そして、彼らにとって忌まわしき5月29日にお祝い事をする事は"御法度"である。

また、Bayern州に限らず、ドイツ全国で、「教会税」(Kirchensteuer)が存在する。つまり、教会が徴税権を有しているものであり、これは中世の「10分の1税」に起源を有する。同様の例は、同じドイツ語圏のオーストリア・スイスのほか、アイスランド・スウェーデン・デンマーク・フィンランドなどの欧州諸国も見られる。

国際化が進む中、外国人とのコラボレーションが増え続けている。システム監査の精度向上のためには現場の協力が不可欠であり、こうした外国の事情を積極的に学ぶ必要があることは言うまでもない。

### 5. 【補足2】 AI と翻訳の関係(続編) 【システム監査専門家の出番】

これまで、AIは多義語翻訳について大きな課題があることを述べて来た。前置詞などを用いずに、単に「A B」という配列がある場合、次のような解釈が有り得る。

- ① AがBする。(Aが名詞/代名詞の主格で、Bが動詞)
- ② AをBする。(Aが名詞/代名詞の対格(直接目的格)で、Bが動詞)
- ③ AにBする。(Aが名詞/代名詞の与格(間接目的格)で、Bが動詞)
- ④ AでBする。(Aが名詞/代名詞の手段を表す格(ラテン語なら奪格、ロシア語ならば造格)で、Bが動詞)
- ⑤ AからBする。(Aが名詞/代名詞の出発点を表す格(ラテン語なら奪格)で、Bが動詞)
- ⑥ AはBである。(Aが名詞/代名詞の主格で、Bは形容詞で、コプラ動詞(be動詞)が省略されている)
- ⑦ AのB (AはBを所有している。Aは名詞/代名詞の属格(所有格))

★コプラ動詞を省略する言語は稀であり、属格で語尾変化をしない言語の多くはof, de, 「的」などの前置詞等を用いる。しかし①~⑤は混乱する場合がある。もし③④⑤のAの語形が同形ならば何が起ころうか?

1950年以前の中国語の「何」、「之」、「於」、「為」、「与(興)」などは、多義的な解釈の原因となった。

★前回、ローマ帝国はラテン語とギリシャ語のバイリンガル国家であり、西半分のラテン語話者と東半分のギリシャ語話者の意思疎通において重大な問題が発生していたことを述べた。今回は、そのことが惹起した世界史上の大事件を取り上げることとする。まさに、誤訳恐るべし。

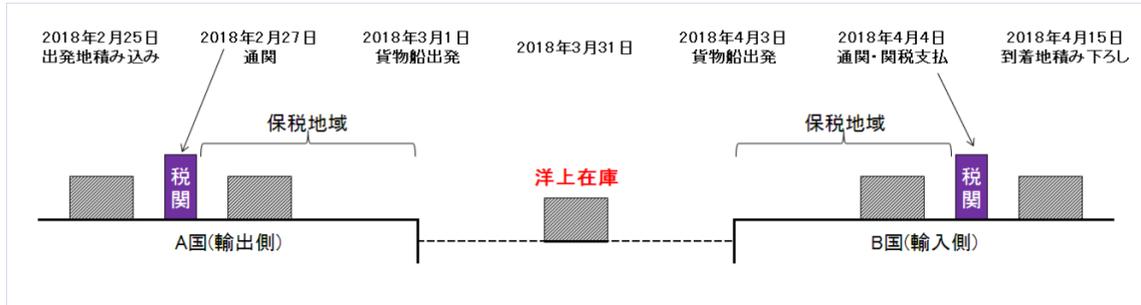
### 6. 【補足3】 「2021年問題」と海外への有償支給の関係 【システム監査専門家の出番】

前回、「2021年問題」への対応の要点を再度取り上げることとする(詳細は文献[1]の第7章・第10章、文献[2]の第3章を参照)。まず、2020年にIncotermsが改訂されたので確認する(Incoterms2010に存在したDATが廃止され、DPUが追加されていることに注意が必要)。

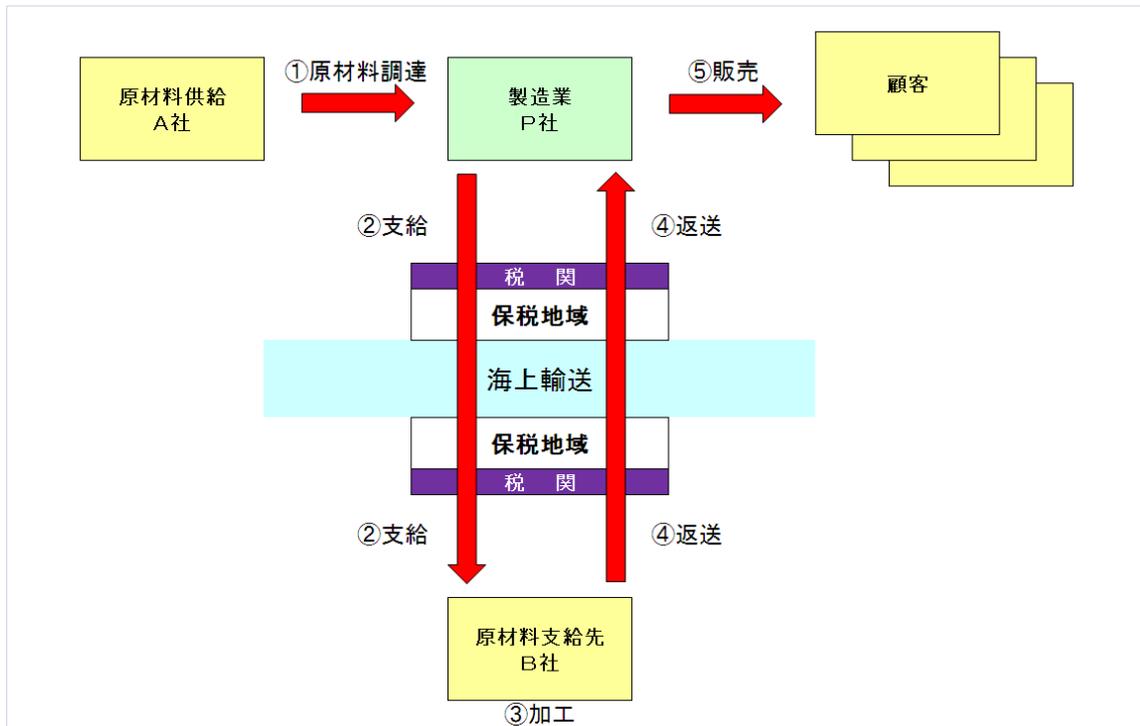
項番	記号	引渡	☆: 売り側負担		★: 買い側負担		▼ 所有権の移転ポイント																
			英語	日本語	海上・内陸 水陸のみ	JETROの克服 水陸のみ(コンテナ)	1	2	3	4	5	6	7	8	9	10	11	12	13	14			
1	EXW	発地	Ex Works	出荷工場渡し条件	---	---	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★	★
2	FCA	発地	Free Carrier	運送人渡し条件	---	○	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
3	FAS	発地	Free Alongside Ship	船側渡し条件 (本船の横まで)	○	○	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
4	FOB	発地	Free On Board	本船甲板渡し条件	○	○	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
5	CFR	発地	Cost and Freight	運賃(船積み条件 保険料なし)	○	○	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
6	CIF	発地	Cost, Insurance and Freight	運賃(船積み条件 保険料込み条件 保険料なし)	○	○	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
7	CPT	発地	Carriage Paid To	運賃(船積み条件 保険料なし)	---	○	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
8	CIP	発地	Carriage and Insurance Paid To	運賃・ 保険料込み条件	---	○	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
9	DAP	着地	Delivered At Place	仕向地持渡し	---	---	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
10	DPU	着地	Delivered At Place Unloaded	仕向地荷降渡し	---	---	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆
11	DDP	着地	Delivered Duty Paid	仕向地持渡し・ 関税込み条件	---	---	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆	☆

※Incoterms2020においては、DAT(Delivered At Terminal)が廃止され、代わりに、DPU(Delivered At Place Unloaded)が新設された。

我が国の輸出産業の場合、工業製品の輸出等においては、航空便よりも船舶便のほうが多数を占めている。その場合、輸出国側での会計処理と輸入国側での会計処理のタイムラグが問題となる。一般に製品が船舶に積載された状態で決算日を迎えた場合、「洋上在庫」と呼ばれることが多いが、これはロジスティクス・システム(SAPならばSDとMMに相当する)における重要テーマでもある。【システム監査専門家の出番】



前回、企業会計基準第 29 号・同適用指針第 30 号が強制適用となる「2021 年問題」(2021 年 4 月 1 日以降に開始する事業年度から強制適用) について特集として取り上げたが、海外の会社に工程の一部を外注する場合、原材料・半製品・製品の流れは次のようになる。



この②と④の過程で、税関を通ることとなる。税関では「売買取引」に限らず、貸与や譲渡取引においても(実質価格を計算した上で)関税が課せられることとなる。その結果、②の段階の原価が B 社に露見することになる。

- ※1. 我が国の「関税定率法」によると、関税は CIF 価格(本体価格+運賃+保険料)に対して掛けられる。
- ※2. 我が国の「消費税法」によると、「CIF 価格+関税」に対して掛けられる(通関手数料には掛からない)。

※以上述べたことは筆者の私見であり、いかなる団体をも代表するものではありません。また、法令の適用・会計基準の適用等につきましては、必ず、御自身でご担当の会計士その他の専門家の方々への御確認・照会をお願いします。

<参考文献>

[1] 「軽減税率」田淵隆明が語る、IFRS&連結会計〔I〕〔II〕: "In Varietate Concordia", EU の知恵に学べ IFRS では何故そう考えるのか? (2020/07/15)

[2] 「軽減税率」田淵隆明が語る、「国際取引における連結上の照合・相殺消去」再考(2020/03/30)

[3] 「アビガン」近く承認申請へ 国産"第 1 号"に期待(2020 年 9 月 21 日)  
<https://www.youtube.com/watch?v=Vrtc7NPwhak>

[4] "Holy and Bright" <https://www.youtube.com/watch?v=b52q65Xnk-Y>

[5] "We're All Alone."(Rita Coolidge,1977) <https://www.youtube.com/watch?v=wzcDVchi6bE>

[6] "We're All Alone."(Boz Scaggs,2011) <https://www.youtube.com/watch?v=CO2itzCPCYg>

[7] 日本発ドイツ便り、金曜日には魚を  
[http://www.lgn.co.jp/lagunatravel/top\\_page\\_tou/kaigaigennchitayori/erikosann/erikosannnododoitsudayori193.pdf](http://www.lgn.co.jp/lagunatravel/top_page_tou/kaigaigennchitayori/erikosann/erikosannnododoitsudayori193.pdf)

[8] <https://www.agiasofia.com/>

<目次>

**「個人情報保護法 2020」の改正内容 ～PMSハンドブック読者！必読！～ 第5回**

会員番号 2581 齊藤 茂雄（個人情報保護監査研究会）

今月号では「個人情報保護に関する法律」（以下、保護法 2020 と呼ぶ）「第四章 第二節(仮名加工情報)」について解説します。「個人情報の保護に関する法律等の一部を改正する法律」の原文は、[個人情報保護委員会の公表ページ](#) をご参照ください。

2020年6月15日公表ロードマップ：<https://www.ppc.go.jp/aboutus/minutes/2020/20200615/>  
[https://www.ppc.go.jp/files/pdf/200615\\_shiryoku1.pdf](https://www.ppc.go.jp/files/pdf/200615_shiryoku1.pdf)

赤字：「保護法 2020」新設または改正条項

※ SAAJPMS研究会コメント

「仮名加工情報」の定義は本シリーズ1回目（会報 232号）で述べました。「仮名加工情報」とは“他の情報と照合しない限り識別することができない”がキーワードで、特定の個人を識別できない情報として加工して事業者内部で利用することを基本にしており、安全管理は必要ですが、データの利活用には便利な設定になっています。

**第二節 仮名加工情報取扱事業者等の義務****第35条の2（仮名加工情報の作成等）**

- 1 個人情報取扱事業者は、仮名加工情報（仮名加工情報データベース等を構成するものに限る。以下同じ。）を作成するときは、他の情報と照合しない限り特定の個人を識別することができないようにするために必要なものとして個人情報保護委員会規則で定める基準(※1)に従い、個人情報を加工しなければならない。
- 2 個人情報取扱事業者は、仮名加工情報を作成したとき、又は仮名加工情報及び当該仮名加工情報に係る削除情報等（略）を取得したときは、削除情報等の漏えいを防止するために必要なものとして個人情報保護委員会規則で定める基準(※1)に従い、削除情報等の安全管理のための措置を講じなければならない。

※ 「仮名加工情報」の定義は、第2条（定義）9に規定されており、「匿名加工情報」の定義とほぼ同じですが、「匿名加工情報」の定義の、“当該個人情報を復元できないようにしたもの”が抜け落ちた内容になっています。「匿名加工情報」は“個人情報ではない”とされていますが、「仮名加工情報」は、「照合・復元してはならない」とし、「個人情報としての安全管理」を求められます。

※ GDPR（前文 26）では、「仮名化データ」と呼び、個人情報とみなすとともに、追加的な情報が分離して保管されることを前提として技術上、組織上の措置を講じなければならないとしています。（GDPR 第4条5項）

※1 「個人情報保護委員会規則で定める基準」は、2021年4月前半に公布される予定です。（2020年6月15日公表ロードマップ）

**第35条の2（仮名加工情報の作成等） つづき**

- 3 仮名加工情報取扱事業者（個人情報取扱事業者である者に限る。以下この条において同じ。）は、第十六条の規定にかかわらず、法令に基づく場合を除くほか、第十五条第一項の規定により特定された利用目的の達成に必要な範囲を超えて、仮名加工情報（個人情報であるものに限る。 ※2）以下この条において同じ。）を取り扱ってはならない。
- 4 仮名加工情報についての第十八条の規定の適用については、同条第一項及び第三項中「、本人に通知し、又は公表し」とあるのは「公表し」と、同条第四項第一号から第三号までの規定中「本人に通知し、又は公表する」とあるのは「公表する」とする。
- 5 仮名加工情報取扱事業者は、仮名加工情報である個人データ及び削除情報等を利用する必要がなくなったときは、当該個人データ及び削除情報等を遅滞なく消去するよう努めなければならない。この場合においては、第十九条の規定は、適用しない。

※2 仮名加工情報（個人情報であるものに限る。）とありますが、「個人情報でない仮名加工情報」について法律条文では言及されていません。政令にも委任していないので、ガイドライン等で示される可能性があります。

※ 「仮名加工情報」は、法第 16 条の規定（利用目的による制限）が適用され、特定された利用目的の達成に必要な範囲を超えて取り扱うことはできません。ただし、今後「個人情報でない仮名加工情報」の利用目的の変更について、別途ガイドライン等に示される可能性があります。

※ 第 4 項において、法第 18 条（取得に際しての利用目的の通知等）の準用により、本人への通知が不要となり公表だけでよいとされています。

法第 18 条第一項準用：「あらかじめその利用目的を公表している場合を除き、速やかに、その利用目的を公表しなければならない。」

法第 18 条第三項準用：「利用目的を変更した場合は、変更された利用目的について、公表しなければならない。」

※ 第 5 項では、「仮名加工情報」および「削除した情報等）」を利用する必要がなくなった時は遅滞なく消去することを前提として、法第 19 条（データ内容の正確性の確保等）を適用しないとしています。これは利活用を主目的とするための措置と類推できます。

**第35条の2（仮名加工情報の作成等） つづき**

- 6 仮名加工情報取扱事業者は、第二十三条第一項及び第二項並びに第二十四条第一項の規定にかかわらず、法令に基づく場合を除くほか、仮名加工情報である個人データを第三者に提供してはならない。この場合において、第二十三条第五項中「前各項」とあるのは「第三十五条の二第六項」と、同項第三号中「、本人に通知し、又は本人が容易に知り得る状態に置いて」とあるのは「公表して」と、同条第六項中「、本人に通知し、又は本人が容易に知り得る状態に置かなければ」とあるのは「公表しなれば」と、第二十五条第一項ただし書中「第二十三条第一項各号又は第五項各号のいずれか（前条第一項の規定による個人データの提供にあっては、第二十三条第一項各号のいずれか）」とあり、及び第二十六条第一項ただし書中「第二十三条第一項各号又は第五項各号のいずれか」とあるのは「法令に基づく場合又は第二十三条第五項各号のいずれか」とする。

※ 「仮名加工情報である個人データ」は、法第 23 条 1（本人に同意を得ないで第三者提供してはならない）、法第 23 条 2（オプトアウトおよび要配慮個人情報のオプトアウト禁止）、法第 24 条 1（本人に同意を得ないで外国にある第三者への提供してはならない）にかかわらず（つまり、本人

同意や、オプトアウトの定義は適用しないが)、法令に基づく場合を除くほかは、原則として第三者提供を禁じています。

- ※ 第 23 条 5 (第三者に該当しないもの) として、「委託」「事業承継」「共同利用」を規定しており、この第 35 条の 2 においても適用されて、第三者提供が可能です。
- ※ 第 23 条 3 (第三者提供時に本人に通知または公表する項目) は、本人への通知を不要とし、公表だけでよいとしています。
- ※ 第 25 条 1 項ただし書き (第三者提供に関わる記録作成の除外) では、法令で基づく場合などや、「委託」「事業承継」「共同利用」を規定し、記録作成を不要としています。
- ※ つまり、法令で基づく場合などや、「委託」「事業承継」「共同利用」以外は、「仮名加工情報」について第三者提供する場合は、「公表」と、「第三者提供の記録作成」が必要となります。

### 第35条の2 (仮名加工情報の作成等) つづき

- 7 仮名加工情報取扱事業者は、仮名加工情報を取り扱うに当たっては、当該仮名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該仮名加工情報を他の情報と照合してはならない。
- 8 仮名加工情報取扱事業者は、仮名加工情報を取り扱うに当たっては、電話をかけ、郵便若しくは民間事業者による信書の送達に関する法律(平成十四年法律第九十九号)第二条第六項に規定する一般信書便事業者若しくは同条第九項に規定する特定信書便事業者による同条第二項に規定する信書便により送付し、電報を送達し、ファクシミリ装置若しくは電磁的方法(電子情報処理組織を使用する方法その他の情報通信の技術を利用する方法であつて個人情報保護委員会規則で定めるものをいう。)を用いて送信し、又は住居を訪問するために、当該仮名加工情報に含まれる連絡先その他の情報を利用してはならない。
- 9 仮名加工情報、仮名加工情報である個人データ及び仮名加工情報である保有個人データについては、第十五条第二項、第二十二條の二及び第二十七條から第三十四條までの規定は、適用しない。

※ 第 8 項で、「含まれる連絡先その他の情報を利用してはならない」との表現から、「仮名加工情報」がどのようなものか見えてきます。利用してはならないとは、逆に「仮名加工情報」には電話番号、住所などが残っていて構わないとも解釈できます。この点が「匿名加工情報」と異なり、個人情報としての取扱いが必要となるポイントです。

※ 第 9 項で、「仮名加工情報」に適用しないとする条項は以下の通りです。

- ・ 第 15 条第 2 項：利用目的を変更する場合は合理的に認められる範囲を超えてはならない
- ・ 第 22 条 2：漏洩等重大な事態が生じた場合は個人情報保護委員会に報告
- ・ 第 27 条：保有個人データに関する事項の公表
- ・ 第 28 条：開示
- ・ 第 29 条：訂正等
- ・ 第 30 条：利用停止等
- ・ 第 31 条：開示等に応じない場合の理由の説明
- ・ 第 32 条：開示等の請求手続等に応じる手続
- ・ 第 33 条：利用目的および開示等に応じる場合の手数料およびその徴収方法

・第34条：開示等の請求等に関わる訴えを提起する場合の事前の請求

**第35条の3（仮名加工情報の第三者提供の制限等）**

- 1 仮名加工情報取扱事業者は、法令に基づく場合を除くほか、仮名加工情報（個人情報であるものを除く。次項及び第三項において同じ。）を第三者に提供してはならない。
- 2 第二十三条第五項及び第六項の規定は、仮名加工情報の提供を受ける者について準用する。この場合において、同条第五項中「前各項」とあるのは「第三十五条の三第一項」と、同項第一号中「個人情報取扱事業者」とあるのは「仮名加工情報取扱事業者」と、同項第三号中「、本人に通知し、又は本人が容易に知り得る状態に置いて」とあるのは「公表して」と、同条第六項中「個人情報取扱事業者」とあるのは「仮名加工情報取扱事業者」と、「、本人に通知し、又は本人が容易に知り得る状態に置かなければ」とあるのは「公表しなければ」と読み替えるものとする。

※ 第35条の2では、仮名加工情報の作成時について規定していますが、ここでは改めて第三者提供の禁止を規定しています。また、「個人情報でない仮名加工情報」があるかのように記述していますが、現時点でそれがどのようなものかを説明する条文はありません。

※ 第2項では第35条2第6項と同様、第三者提供に当たらないケースとして、第23条5を読み替えた上で、従来通り、「委託」「事業承継」「共同利用」を規定しています。

**第35条の3（仮名加工情報の第三者提供の制限等） つづき**

- 3 第二十条から第二十二条まで、第三十五条並びに前条第七項及び第八項の規定は、仮名加工情報取扱事業者による仮名加工情報の取扱いについて準用する。この場合において、第二十条中「漏えい、滅失又は毀損」とあるのは「漏えい」と、前条第七項中「ために、」とあるのは「ために、削除情報等を取得し、又は」と読み替えるものとする。

※ 第20条の適用では、安全管理措置の目的を漏えいの防止のみとし、滅失・毀損の防止は対象としていません。「仮名加工情報」は分析などの利活用を目的としており、そのため情報の最新性、正確性の維持を求めないこととされたと思われます。

※ 「仮名加工情報」についても、個人情報と同様に、第21条（従業員の監督）、第22条（委託先の監督）、第35条（苦情の処理）、第35条2第7項（削除情報等・仮名加工情報の他の情報との照合禁止、第35条2第8項（仮名加工情報に含まれる情報の流用禁止）が適用されます。

次回は、「第四章 第4節 監督（第40条—第46条）（旧第3節）」から解説します。

SAAJ「PMSハンドブック」ご紹介サイト：<https://www.saj.or.jp/shibu/Kojin/kojin.html>

認定 NPO 法人日本システム監査人協会 個人情報保護監査研究会 ■

<目次>

2020.10

**第 250 回月例研究会：講演録****テーマ：【既存対策を凌駕し続けるサイバー脅威と整備すべき態勢（前もっての身構え）】**

会員番号 6023 山口 達也（月例研究会）

**【講師】株式会社サイバーディフェンス研究所 専務理事/上級分析官****名和 利男 氏****【日時・場所】2020年9月3日（木）18：30 - 20:30、機械振興会館 地下2階ホール（神谷町）****【テーマ】「既存対策を凌駕し続けるサイバー脅威と整備すべき態勢（前もっての身構え）」****【要旨】**

サイバー空間を積極的に利用することで恩恵を受けているのは我々だけではなく、「悪意のある者ら」も同様であることを念頭に置く必要がある。

我々がDX（デジタルトランスフォーメーション）を通じて、価値提供の方法を抜本的に変化させ、同時にサイバー攻撃が成功しにくい環境を作っても、攻撃を成功させる事が死活問題である「悪意のある者ら」は、即座にその原因を取り除くことができるように進化するのである。つまり、私たちのセキュリティ対策を常に凌駕し続けていくことを意味している。

このような認識と覚悟をもって、これから整備すべき態勢（前もっての身構え）について考える

**【講演録】**

講演に先立ち、小野会長より、月例研究会第250回の節目に当たって、冒頭挨拶を頂いた。

**I. 昨今の事例から考察される「得べき教訓」「ゼロデイ脆弱性」「セキュリティインシデントの傾向」**

本年にはいつてから発生した我が国の大手電機メーカーへのサイバー攻撃や、ここ数年で発生している周辺諸国の軍・防衛産業への不正アクセス事案を例にみても、攻撃者側の攻撃戦略（Attack Strategy）が着実に進展している。また国家レベルでの対策の枠組みを備える諸外国と比較し、我が国では既存の（法的）枠組み＝単独企業での対応による防衛努力が継続されている。これらの点は今後我が国のサイバーセキュリティ対策を推進する上での「得べき教訓」として認識すべきである。

また著名な Web ブラウザー、ネットワーク管理機能、携帯メールアプリ、ウィルス対策ソフトにおけるゼロデイ脆弱性が存在し、予防対策だけでは十分な対応が難しい現状となっている。

更には昨今のセキュリティインシデントの傾向として、脆弱性を利用した不正アクセスは依然多いものの、それ以上にヒューマンエラーによるものが多い傾向がある。特に本年5月以降、リモートワークの急激な拡大に伴ってか、メールのサーバーやアカウントの不正利用が目立つようになってきている。

**II. サイバーレジリエンス態勢**

これらの状況を踏まえれば、サイバー空間に依存している事業においては、レジリエンス態勢の維持・向上が重要である。レジリエンスを高めることで、早期の正常な事業環境を復元し、通常業務の再開が可能となる。このレジリエンス態勢を高めていく上で、重要となるのは、状況認識である。特にサイバーテロのような緊急性の有無を判断するためには当事者による「主観的な評価」が必要となる点に留意すべきである。

リスク管理は本来、潜在的な脅威を評価し、それらの脅威を回避する最良の方法を見つけるための手続き的管理である。しかしながら、サイバー攻撃が、複雑化、大規模化し、攻撃対象領域が拡大・深化、攻撃戦略が多様化・重層化・個別化・高度化・弾力化する現状においては、潜在的脅威の見出し・識別・特例・評価は困難になってきている。これは同時に「回避する最良の方法」の適用可能範囲が急速に縮小することも意味しており、そのようなリスク環境を踏まえても、レジリエンス態勢の高度化は重要となっている。

### Ⅲ. 第 2 部「個別事案紹介」

※第 2 部は限定公開となっているため、講演録は割愛致します。

#### 【所感】

極めて具体的な事例を元に、現在のサイバー攻撃の実態、それに対する防衛側の実態を紹介頂き、サイバー攻撃が他人事ではなく、すぐそこにある重大な脅威であると痛感させられた。またその対応についても従来のリスクマネジメントの考え方では既に対応しきれない状況があり、そのためにレジリエンス態勢（not 体制）高度化の重要性、そのために何を考え、実践していくべきかという点について明確なイメージを持つことができた。

以 上.



<目次>

2020.10

**支部報告 【 北海道支部 2020 年度 9 月の月例研究会 】**

会員番号 1448 宮崎雅年 (北海道支部)

北海道支部では、以下のとおり 2020 年度 9 月の月例研究会を開催しました。

- ・日時：2020 年 9 月 25 日 (金) 18:30～20:30 参加者：4 名
- ・会場：札幌市男女共同参画センター OS 研修室 (札幌市)
- ・演題：『「情報セキュリティ白書 2020」を読んで』
- ・講師：北海道支部長 宮崎 雅年 氏

**<講演概要>**

IPA (情報処理推進機構) では、「情報セキュリティ白書」を 2008 年から毎年発行しており、今年で 13 冊目を数える。この白書は、前年度の情報セキュリティの概況に始まり、情報セキュリティに関する国内外のインシデントの発生状況および被害実態と対策、脆弱性の現状と対策、国内外の政策などのほか、毎年タイムリーな話題を新たに取り上げている。

この白書には、情報セキュリティに関する国内外の官民の各種データおよび資料が掲載されていることから、内容に網羅性および参照性が高く、自身の研鑽だけでなく、教育・研修の資料作りにも参考となるもので、講師は 2012 年から毎年購入している。(全文 PDF 版は、IPA の Web サイトから無償ダウンロード可能)

最新の「情報セキュリティ白書 2020」では、新たな話題として、下記をとりあげている。

- ・クラウドの情報セキュリティ (インシデント、被害の実態、課題とその対応など)
- ・次代を担う青少年を取り巻くネット環境 (SNS を介した犯罪、不確かな情報、e スポーツとオンラインゲームなど)

なお、本発表の内容は講師の個人的意見であり、講師が所属する企業・団体の意見を代弁するものではない。

**<講演内容>****1. 2019 年度の情報セキュリティの概況**

2019 年度に起きた情報セキュリティインシデント・事件として、EC サイトアカウントに多数の不正アクセスがあったこと、スマートフォン決済サービスが不正アクセス被害を受けてサービス廃止に至ったこと、就職情報サイト運営会社が「内定辞退率」データを販売したこと、情報機器リユース会社において廃棄予定 HDD の流出が発覚したこと、Emotet のばらまき型メールによる攻撃が急増したこと、などが挙げられる。

また、情報セキュリティ政策・イベントとして、米中の緊張が高まったこと、2020 オリンピック・パラリンピック東京大会に向けた新技術の導入および対策・演習の実施、個人情報保護法改正案の閣議決定などが挙げられる。

## 2. 情報セキュリティインシデント・脆弱性の現状と対策

2019年度に世界で観測されたインシデントの状況では、フィッシングとビジネスメール詐欺、情報漏えい、ランサムウェアによる攻撃が挙げられ、国内では、Web サイト改ざん、フィッシングが挙げられる。

国内において注目される新たな脅威として、Emotet 感染、ランサムウェアによる攻撃が挙げられる。

被害が継続している理由は、背景として様々な要因による ID とパスワードの漏えいおよび ID とパスワードのリストの流通がある。一方、ユーザ側の問題としてパスワードの使い回しがあり、サービス提供者側に求められるものとして、多要素認証の追加などのセキュリティ対策の強化がある。

## 3. 情報セキュリティインシデントの手口と対策

国内組織の海外現地法人を狙った標的型攻撃や未公開の脆弱性を悪用した標的型攻撃など、今後も日本の組織が標的とされる状況は続くものと予想され、組織ごとの対策だけでなく、海外を含む企業グループ全体でセキュリティ対策を講じていく必要がある。

標的型攻撃はメールにおける騙しの手口と添付ファイルの手口がある。添付ファイルの手口は Microsoft Office の脆弱性やマクロ機能を悪用する手口のほか、オンラインストレージサービスを悪用する手口がある。

標的型攻撃への対策は、利用者向けの対策として不審メールに対する注意力の向上、オンラインストレージサービスを悪用した手口の周知、マクロ機能の危険性の周知、ウイルス感染を想定した訓練と教育のほか、システムによる技術的な対策として不審メールを確保できる仕組みの確立、適切な修正プログラムの適用、ホワイトリスト化やブラックリスト化によるファイルの実行防止がある。

ビジネスメール詐欺では、CEO を詐称する攻撃のほか、新規取引先の見積書の価格修正を装う攻撃が新たな手口として現れた。これは、従来は振込先の口座の変更を要求する手口が多数だったが、偽の口座を記載した見積書を「価格の修正」と称して送り付けたものである。

ビジネスメール詐欺への対策は、周知徹底と情報共有のほか、電子署名によるなりすまし防止、送金処理のチェック体制強化、類似ドメインへの対策等がある。

DDoS 攻撃を行うボットネットが拡大しており、サービスおよびソフトウェアの脆弱性を悪用されたり、ウイルス感染させられたコンピュータのほか、ルータおよび IoT 機器を攻撃対象とした手法も取り入れられている。

DDoS 攻撃の被害に遭った場合の対策は、アクセスログや通信ログ等の確認、想定外の IP アドレスからのアクセスを遮断、監視の継続があり、攻撃に加担しないための対策は、OS やファームウェアを最新の状態に維持、パスワードを初期値から変更、組織内から外向けの通信の監視がある。

Windows の脆弱性を対象とした攻撃は、Windows7 以前の OS に存在する BlueKeep の脆弱性を悪用した攻撃が依然として確認されており、最新の OS への移行が望まれるところである。

CMS 本体や CMS のプラグインの脆弱性を悪用した攻撃が確認されている。これも、ソフトウェアを最新の状態に維持することが対策として挙げられる。

IoT 機器の脆弱性を狙う新たなウイルス Neko、Asher、Gafgyt (別名、Ayedz) が確認された。IoT 機器を対象とした攻撃への対策は、製品開発者が行うべき対策として修正プログラムの公開、アップデートを実施できるように設計すること、製品利用者が行うべき対策としてアップデート方法の確認、脆弱性情報の

収集、修正プログラムの速やかな適用が挙げられる。

Emotet に感染させる手口は、マクロ付き Word ファイルを添付したりメール本文に不正な URL リンクを記載したばらまき型メールの手口が使われる。ばらまき型メールに使われるメールは、本物のメールと信じ込ませるために過去にやり取りしたメールを窃取することで正規のメールを利用したり、新型コロナウイルスや賞与支給を題材としたようなメール受信者の興味・関心を惹く題材を悪用していることが確認されている。

Emotet のばらまき型メールがマクロ付き Word ファイルの送り方を変えていることから、Emotet に感染しないための対策は、不審なメールは無視して削除することであるが、今後も手口が変化する可能性があるため、JPCERT/CC や IPA が紹介している対策を検討するとともに、一般的なウイルス対策と同様の多層的な防御の実施がある。

Emotet に感染した後の対応は、一般的なウイルス感染と同様で、感染端末をネットワークから隔離し、組織内の全端末のセキュリティソフトによるフルスキャン等を行うとともに、被害を受ける可能性のある関係者への注意喚起のほか、組織として迅速に適切な対応を行えるよう準備・訓練をしておくことも重要である。

インターネットバンキングの情報を窃取し、不正送金を行うウイルスとして Ursnif への感染を狙ったばらまき型メールが確認されている。これは、正規のメールへの返信を装うメールで、パスワード付きの zip ファイルが添付され、パスワードはメール本文に記載されており、この添付ファイルを解凍するとマクロ付きの Word ファイルが出力されて、そのファイルを開いてマクロを有効化すると感染するというものである。

そのほか、Get2 Goenloader を使用して別のウイルスへの感染を狙うばらまき型メールが確認されている。

これは、マクロ付きの Excel ファイルが添付されたメールで、Excel のマクロを有効化すると偽のプログレスバーが表示され、背後で別のウイルスがダウンロードされるものである。

ばらまき型メールへの対策は、一般利用者における対策としてセキュリティソフトの導入、不用意にメールや添付ファイル内の指示に従わない、OS やソフトウェアのバージョンを常に最新に保つ、Word ファイルや Excel ファイルを開いたときにマクロを有効化しない、組織・企業における対策として不審なメールを受信した際の報告窓口を設ける、ウイルス感染を想定した利用者の訓練と教育を行う、不審なメールを確保できる仕組みの確立、適切な修正プログラムの適用、特定のファイル形式について実行許可・禁止の設定、公開されているばらまき型メールに関する注意喚起情報を組織内で共有がある。

スマートフォンの利用拡大に伴って正規サイトを模した偽サイトへ誘導する手口として、SMS をきっかけとするものがある。SMS のメッセージの例は、宅配便の不在通知を装うもの、送信元を偽装して携帯通信会社等を装うもの、金融機関を装うもの等である。SMS をきっかけとする手口に共通の対策は、SMS 内のリンクを基本的に利用しないことである。

偽のセキュリティ警告など、Web ブラウザの表示をきっかけとする手口が確認されており、本物の警告か、偽物の警告か、両方を想定した対応をするため、信頼できる情報源で確認することが必要である。

アプリのインストール、特にスマートフォンへの不正アプリのインストールが報告されており、アプリは公式マーケットから入手することを心がけるとともに、開発元の信頼性を慎重に確認することが必要である。

騙しの手口に共通する対策は、手口を知り、日ごろの備えをする一方、目にした情報の真偽は確かな情報源で確かめ、判断に迷ったら信頼できる相手に相談することである。

#### 4. 情報セキュリティを支える基盤の動向

国内の情報セキュリティ政策は、政府全体として「サイバーセキュリティ戦略」の見直し、重要インフラの情報セキュリティ対策強化があり、経済産業省として産業サイバーセキュリティ研究会、政府情報システムのためのセキュリティ評価制度（ISMAP）、J-CSIP（サイバー情報共有イニシアティブ）がある。

国外の情報セキュリティ政策の状況は、国際社会と連携した取り組みがあり、日米のサイバー連携のほか、EU 諸国および ASEAN 諸国とのサイバー連携がある。

セキュリティ人材の不足という認識から情報セキュリティ人材の育成として、経済産業省および関係省庁等の取り組みがあり、産業サイバーセキュリティセンターによる中核人材育成プログラムのほか、情報セキュリティ人材育成のための国家試験および国家資格として情報セキュリティマネジメント試験、情報処理安全確保支援士制度がある。

制御システムの情報セキュリティのほか、IoT の情報セキュリティの重要性が高まっている。特に IoT の情報セキュリティ対策強化の取り組みとして、IoT 関連セキュリティガイド等の改訂・新規発行、IoT 機器に対する規制の強化がある。

#### 5. 次代の担う青少年を取り巻くネット環境

18 歳が成年となったことから、インターネットと選挙の関わりが注目を浴びることとなる一方、SNS を介した犯罪のほか、フェイクニュースなどの不確かな情報の拡散が問題となっている。

e スポーツとオンラインゲームという新たな分野が開拓されたほか、同世代の生徒・大学生による情報セキュリティの啓蒙活動が広がっている。

#### 6. クラウドの情報セキュリティ

クラウドサービスでは、システムバグ、システムの設定・更新不備、システム故障、設定ミスの悪用、それぞれに起因するインシデントが確認されている。

クラウドサービスの中で、新型コロナウイルス感染拡大防止のために急速に利用が拡大しているリモート会議システムにおいて、脆弱性が確認されている。

#### 7. 最後に

ウイルス対策ソフトおよびソフトウェアを最新の状態に維持するだけでは不十分だが、個人や小規模事業者にとそれ以上の技術的な対策を求めるのは過大な要求でしょう。しかし、最新のセキュリティ動向の情報を共有することで、先行する類似の事例を回避することは可能でしょう。デジタル庁新設後に注目したい。

<目次>

2020.10

## 注目情報 (2020.9~2020.10)

## ■ 「情報セキュリティ白書2020」 無料PDF版が公開

【独立行政法人情報処理推進機構 (IPA)】

2020/9/3

北海道支部の報告 (2020 年度 9 月の月例研究会) にありました「情報セキュリティ白書 2020」ですが、以下 URL (IPA の Web サイト) へアクセスしてアンケートに答えることで、無料 PDF 版を読むことができます。

<https://www.ipa.go.jp/security/publications/hakusyo/2020.html>

- ① パスワード付 zip ファイルをダウンロードする
- ② アンケートに回答するとパスワードが通知される



序章	2019 年度の情報セキュリティの概況
第 1 章	情報セキュリティインシデント・脆弱性の現状と対策
1.1	2019 年度に観測されたインシデント状況
1.2	情報セキュリティインシデント別の手口と対策
1.3	情報システムの脆弱性の動向
第 2 章	情報セキュリティを支える基盤の動向
2.1	国内の情報セキュリティ政策の状況
2.2	国外の情報セキュリティ政策の状況
2.3	情報セキュリティ人材の現状と育成
2.4	組織・個人における情報セキュリティの取り組み
2.5	国際標準化活動
2.6	安全な政府調達に向けて
2.7	その他の情報セキュリティ動向
第 3 章	個別テーマ
3.1	制御システムの情報セキュリティ
3.2	IoT の情報セキュリティ
3.3	次代を担う青少年を取り巻くネット環境
3.4	クラウドの情報セキュリティ
特別寄稿	セキュリティマネジメントの日米企業比較

&lt;目次&gt;

2020.10

## 【 協会主催イベント・セミナーのご案内 】

## ■ SAAJ 月例研究会 (東京)

第 2 5 2 回	日時	2020年11月19日(木) 18:30~20:30
	場所	機械振興会館地下2階ホール 及び オンライン (Zoom ウェビナー)
	テーマ	テレワーク時代におけるシステム監査について
	講師	東洋大学 総合情報学部 教授 島田裕次 氏
	講演骨子	新型コロナウイルスの影響によって、企業・官公庁・大学など様々な組織でテレワークやオンライン授業などが急速に普及している。この結果、監査対象業務も大きく変革し、今までなかなか進まなかったDXが急速に進んでいる。このような状況下において、システム監査の役割がより一層重要になっている。本講演では、テレワーク時代のシステム監査について検討していきたい。
	参加費	SAAJ 会員 1,000 円 非会員 3,000 円
	お申込み	<a href="http://www.saa.or.jp/kenkyu/kenkyu/252.html">http://www.saa.or.jp/kenkyu/kenkyu/252.html</a>

## ■ SAAJ 月例研究会 (東京)

第 2 5 3 回	日時	2020年12月4日(金) 18:30~20:30
	場所	オンライン (Zoom ウェビナー)
	テーマ	「企業価値向上に向けたシステム活用について (J-SOX)」(仮題)
	講師	アンリツ株式会社社外取締役 青木和義 氏
	参加費	SAAJ 会員 1,000 円 非会員 3,000 円
	お申込み	第 252 回終了後にご案内します。

&lt;目次&gt;

2020.10

## 特別頒布のご案内

平成30(2018)年版システム監査基準/システム管理基準改訂に対応

## 情報システム監査実践マニュアル(第3版)

認定NPO法人 日本システム監査人協会【監修】

システム監査の導入からフォローアップに至る業務を、事例を交えて実践的に解説

B5版384ページ 定価5,200 + 税

## ○本書の特徴



## 1.テーマごとに監査(管理)のポイントを詳説

システム監査基準、管理基準の各項目をさらに掘り下げ、効率的・実践的な監査のポイントを11のテーマ別に解説。近年の社会情勢を踏まえ、ITガバナンス、AI、アジャイル開発など、最近導入が進んできた新しい監査テーマにも対応しています。

## 2.監査書類・監査チェックポイント集のダウンロードデータ付き

巻末には、監査書類の様式・作成例や監査チェックポイント集を掲載し、ダウンロードして実務で使える、書籍と対応したWeb資料も用意されています。

## 3.多様な執筆陣

執筆者は、日本システム監査人協会の各研究会等で活動している会員に加え、平成30(2018)年版の基準の改訂作業に共同で参画したシステム監査学会、ISACA 東京支部の多数の会員が参画しており、日本におけるシステム監査関連3団体のノウハウが詰まっています。

## 【目次】

第1部 組織経営における情報システムの役割とシステム監査

第2部 システム監査の実践方法

第3部 システム管理基準の実践的な活用のポイント(11の活用例)

第4部 システム監査の事例(4つの事例)

第5部 資料編(書式・監査評価のポイントをExcelファイルで提供)

※ダウンロード 監査評価 ポイント の内容	①	システム監査基準/管理基準ファイル(各管理項目について確認すべきサブコントロールと確認方法を記載。(1フェーズ(例:企画)/シート)
	②	上記1を全フェーズ/1シートにしたファイル(チェックポイントの抽出に便利)
	③	第3部11の活用例毎のポイントの11ファイル

お申込み方法：森北出版宛

eigyo@morikita.co.jp FAX:03-3264-8709

■ 代金引換便にて発送いたします。 ※手数料¥330(税込)を別途申し受けますので、ご了承ください。

書名	価格(税込)	会員価格(税込)	ご注文冊数	出版社処理欄
情報システム監査実践マニュアル(第3版)	¥5,720 →	¥5,148		8511①
個人情報保護マネジメントシステム実践マニュアル	¥4,620 →	¥4,158		8512②
IT統制監査実践マニュアル	¥4,840 →	¥4,356		8513③
貴社名・部門名：	氏名：			
	TEL：			
お届け先住所：〒				

※ご記入いただいた個人情報は、書籍の発送目的のためにのみ使用させていただきます。

&lt;目次&gt;

## 【 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。  
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。

- ・ホームページでは協会活動全般をご案内 <https://www.saa-j.or.jp/index.html>
- ・会員規程 [https://www.saa-j.or.jp/gaiyo/kaiin\\_kitei.pdf](https://www.saa-j.or.jp/gaiyo/kaiin_kitei.pdf)
- ・会員情報の変更方法 <https://www.saa-j.or.jp/members/henkou.html>

- ・セミナーやイベント等の会員割引や優遇 <https://www.saa-j.or.jp/nyukai/index.html>  
公認システム監査人制度における、会員割引制度など。

- ・各支部・各部会・各研究会等の活動。 <https://www.saa-j.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。  
ペンネームによる「めだか」や実名投稿には多くの方から投稿いただいております。  
この会報の「会報編集部からのお知らせ」をご覧ください。

- ・「発注者のプロジェクトマネジメントと監査」「6か月で構築する個人情報保護マネジメントシステム」「情報システム監査実践マニュアル」などの協会出版物が会員割引価格で購入できます。  
<https://www.saa-j.or.jp/shuppan/index.html>

- ・月例研究会など、セミナー等のお知らせ <https://www.saa-j.or.jp/kenkyu/index.html>  
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。 <https://www.saa-j.or.jp/csa/index.html>

- ・過去の会報を公開 <https://www.saa-j.jp/03Kaiho/0305kaihoIndex.html>  
会報に対するご意見は、下記のお問合せページをご利用ください。

- ・お問い合わせページをご利用ください。 <https://www.saa-j.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。

【 SAAJ協会行事一覧 】		赤字：前回から変更された予定	2020.10
	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
10月	8：理事会	10（土）13:30 第251回月例研究会 情報システム監査実践マニュアル （第3版）出版記念講演	18：秋期情報処理技術者試験  31：関東地区主催 会員向け SAAJ 活動説明会
11月	12：理事会 13：予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/8〆切） 16：2020年度年会費請求書発送準備 26：会費未納者除名予告通知発送 30：本部・支部予算提出期限	19：第252回月例研究会 中旬：秋期 CSA 面接 下旬：CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 下旬：CSA 面接結果通知	28：「2020年度西日本支部合同 研究会 in Nagoya」
12月	1：2020年度年会費請求書発送 1：個人番号関係事務教育 10：理事会：2021年度予算案 会費未納者除名承認 第20期総会審議事項確認 11：総会資料提出依頼（1/11〆切） 14：総会開催予告掲示 20：2020年度経費提出期限	4：第253回月例研究会  16：CSA/ASA 更新手続案内メール 〔申請期間 1/1～1/31〕  25：秋期 CSA 認定証発送	12：協会創立記念日
1月	11：総会資料提出期限 16:00 14：理事会：総会資料原案審議 30：償却資産税・消費税申告 30：2020年度会計監査	1-31：CSA・ASA 更新申請受付 21：春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕	11：支部会計報告期限
2月	1：総会申込受付開始（資料公表） 4：理事会：通常総会議案承認 28：2021年度年会費納入期限	2/1-3/31：CSA・ASA 春期募集  下旬：CSA・ASA 更新認定証発送	19：第20期通常総会
3月	5：年会費未納者宛督促メール発信 11：理事会 27：法務局：資産登記、 活動報告書提出 東京都：NPO 事業報告書提出	1-31：春期 CSA・ASA 書類審査	
<b>前年度に実施した行事一覧</b>			
4月	9：理事会（休会）	初旬：春期 CSA・ASA 書類審査 10：月例研究会（延期） 中旬：春期 ASA 認定証発行	19：春期情報技術者試験（中止）
5月	14：理事会	中旬・下旬土曜：春期 CSA 面接（延期）	
6月	1：年会費未納者宛督促メール発信 11：理事会 20：年会費未納者督促状発送 21～：会費督促電話作業（役員） 28：支部会計報告依頼（〆切 7/13） 30：助成金配賦額決定（支部別会員数）	6：月例研究会（延期）  上旬～下旬土曜：春期 CSA 面接 （実施/延期については個別に連絡）	認定 NPO 法人東京都認定日 （2015/6/3）
7月	6：支部助成金支給 9：理事会	11：月例研究会（延期） 上旬：春期 CSA 面接結果通知 中旬・下旬：春期 CSA 認定証発送 中旬：秋期 CSA・ASA 募集案内	13：支部会計報告〆切
8月	（理事会休会） 22：14:00 中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30 29-30：第36回システム監査実務セミナー 前半	
9月	10：理事会	～秋期 CSA・ASA 募集中～9/30迄 3：第250回月例研究会 12-13：第36回システム監査実務セミナー 後半	

&lt;目次&gt;

**【 会報編集部からのお知らせ 】**

1. 会報テーマについて
2. 会報バックナンバーについて
3. 会員の皆様からの投稿を募集しております

**□ ■ 1. 会報テーマについて**

2020年の会報年間テーマは

**「システム監査人のターニングポイント」**です。

システム監査の過去、未来においてターニングポイントとなった①外部環境の変化、②技術的な変化、③今後予想されることを焦点に議論し、お互いの知見や意見を交換することを目的として設定しました。

参考までに例示を紹介させていただきます。

- ①の例示：マイナンバー制度
- ②の例示：クラウドコンピューティング、ブロックチェーン
- ③の例示：AI、自動運転、IoT、ビッグデータ等に関する技術的な進展と法制度

あくまでも例示ですのでこれらにとらわれる必要はありません。

会報テーマ以外の皆様任意のテーマ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. 会報のバックナンバーについて**

協会設立からの会報第1号からのバックナンバーをダウンロードできます。

<https://www.saaj.jp/03Kaiho/0305kaihoIndex.html>

### □ ■ 3. 会員の皆様からの投稿を募集しております。

募集記事は次の通りです。

□ ■ 募集記事	
1. めだか	匿名（ペンネーム）による投稿 原則 1 ページ 下記より投稿フォームをダウンロードください。 <a href="https://www.saaj.jp/03Kaiho/670502KaihoTokoForm2.docx">https://www.saaj.jp/03Kaiho/670502KaihoTokoForm2.docx</a>
2. 記名投稿	原則 4 ページ以内 下記より投稿フォームをダウンロードください。 <a href="https://www.saaj.jp/03Kaiho/670502KaihoTokoForm2.docx">https://www.saaj.jp/03Kaiho/670502KaihoTokoForm2.docx</a>
3. 会報掲載論文 (投稿は会員限定)	現在「論文」の募集は行っておりません。

#### ■ 投稿について 「会報投稿要項」

- ・ 投稿締切：15 日（発行日：25 日）
- ・ 投稿用フォーマット ※毎月メール配信を利用してください。
- ・ 投稿先：[saajeditor@saaj.jp](mailto:saajeditor@saaj.jp) 宛メール添付ファイル
- ・ 投稿メールには、以下を記載してください。
  - ✓ 会員番号
  - ✓ 氏名
  - ✓ メールアドレス
  - ✓ 連絡が取れる電話番号
- ・ めだか、記名投稿には、会員のほか、非会員 CSA/ASA、および SAAJ 関連団体の会員の方も投稿できます。
  - ✓ 会員以外の方は、会員番号に代えて、CSA/ASA 番号、もしくは団体名を表記ください。

#### ■ 注意事項

- ・ 原稿の主題は、[定款](#)に記載された協会活動の目的に沿った内容にして下さい。
- ・ 特定非営利活動促進法第 2 条第 2 項の規定に反する内容（宗教の教義を広める、政治上の主義を推進・支持、又は反対する、公職にある者又は政党を推薦・支持、又は反対するなど）は、ご遠慮下さい。
- ・ 原稿の掲載、不掲載については会報部会が総合的に判断します。
- ・ なお会報部会より、表現の訂正を求め、見直しを依頼することがあります。また内容の趣旨を変えずに、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。

お問い合わせ先：[saajeditor@saaj.jp](mailto:saajeditor@saaj.jp)

<目次>

**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。会員パスワードが必要です）

[https://www.saaj.or.jp/members\\_site/KaiinStart](https://www.saaj.or.jp/members_site/KaiinStart)

ログイン ID（8桁）は、年会費請求書に記載しています。

=====

■発行：認定 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、会員宛の連絡事項を記載し登録メールアドレス宛に配信します。登録メールアドレス等を変更された場合は、会員サイトより訂正してください。

[https://www.saaj.or.jp/members\\_site/KaiinStart](https://www.saaj.or.jp/members_site/KaiinStart)

掲載記事の転載は自由ですが、内容は改変せず、出典を明記していただくようお願いします。

■□■ S A A J 会報担当

編集委員：竹原豊和、安部晃生、越野雅晴、坂本誠、豊田諭、福田敏博、柳田正、山口達也

編集支援：会長、各副会長、各支部長

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）

Copyright(C)1997-2020、認定 NPO 法人 日本システム監査人協会

<目次>