＜NewsRelease＞
報道関係各位

NO MORE 情報漏えい
情報漏えいの「自分ごと化」プロジェクト。

MOTEX
Secure Productivity

2017年3月30日
エムオーテックス株式会社

全国47都道府県のビジネスパーソン1,410名&情報システム部門担当100名に聞いた

「セキュリティ教育の実態調査」

ヒヤリハット経験をしている“セキュリティ危機予備群”のビジネスパーソンは約3割。関東地方はセキュリティ意識が高い!?
ビジネスパーソンの5人に1人がセキュリティ知識を身につけたいと思うものの、
方法が分からない“セキュリティ教育難民”に！
8割以上の情シスが社内のセキュリティ教育に改善の必要ありと回答！
情シスが抱える課題のTOP3は、「時間」、「お金」、「社員の興味・関心」。

エムオーテックス株式会社（本社：大阪市淀川区、代表取締役社長：河之口達也、以下MOTEX）は、社会的問題である「情報漏えい」の解決、防止に貢献していく**“NO MORE 情報漏えいプロジェクト”**を2014年10月に発足しました。同プロジェクトでは、セキュリティの原理原則をまとめたセキュリティブック『7つの習慣・20の事例』の提供を2017年2月23日（木）に開始しました。本セキュリティブックの公開に伴い、セキュリティ教育を調査テーマとした**「セキュリティ教育の実態調査」**を発表します。

今回の調査では、**“セキュリティ教育”**をテーマに設定。セキュリティに関して教育を受ける全国のビジネスパーソン1,410名（各都道府県30名）に自身のセキュリティに関する知識について調査しました。さらに、社内でセキュリティ教育を施す立場に立つことの多い「情報システム部門（以下、情シス）」に勤めている方100名に調査を行い、ビジネスパーソンとは異なる立場の意見を集めました。調査結果については、**“NO MORE 情報漏えいプロジェクト”**の監修者である**徳丸浩氏**（HASHコンサルティング株式会社代表）より解説をいただいています。以下が調査結果となります。本調査結果をぜひご活用いただけますと幸いです。

＝ 調査結果ダイジェスト ＝

TOPICS①セキュリティ管理の実態について

✓ビジネスパーソンの7割以上がセキュリティ知識に自信が無いと回答。
✓ヒヤリハット経験をしている「セキュリティ危機予備群」のビジネスパーソンは約3割に。

TOPICS②セキュリティ教育への意識とその教育環境について

✓ビジネスパーソンの7割以上がセキュリティ知識の習得に前向き。一方、5人に1人がその知識習得のための具体的な方法が分からない、“セキュリティ教育難民”であることが明らかに！

TOPICS③情シスが抱える社内のセキュリティ教育への課題について

✓自社のセキュリティ知識レベルに、約半数の情シスが不満を抱えている結果に。今後、セキュリティ事故を引き起こしてしまう恐れがある役職は、第1位「新入社員」、ついで「外勤（営業系）」、「経営層（社長・役員）」に。
✓8割以上の情シスが社内のセキュリティ教育に改善の必要ありと回答！情シスが抱える課題は、「時間」、「お金」、「社員の興味・関心」！
✓インシデント対応に1カ月あたり32時間、1日あたり1.6時間を費やしている状況。また、セキュリティ教育のための「予算はない」と3割以上の情シスが回答。セキュリティ教育改善のためには、経営者へもっとアピールすべき!?
✓「自分ごと化できる事例の紹介」、「親しみやすいコンテンツの利用」。社員がセキュリティ知識を身につけるにあたり、情シスはこの2点を重要視！

【調査概要】

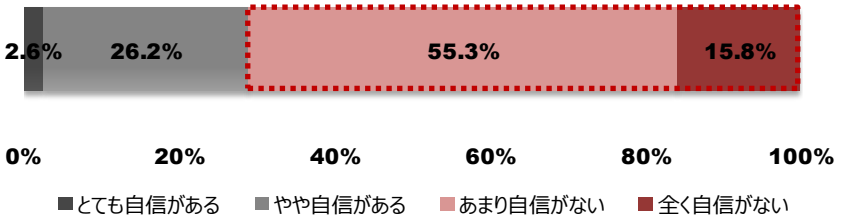
■調査方法　：インターネット調査
■調査機関　：楽天リサーチ株式会社
■調査期間　：2017年2月8日（水）～ 10日（金）
■調査対象①　：23～59歳の男女ビジネスパーソン / 合計1,410名　※各都道府県30名に割付
■調査対象②　：情報システム部門に勤めている社員 / 合計100名

TOPICS①セキュリティ管理の実態について

ビジネスパーソンの7割以上がセキュリティ知識に自信が無いと回答。
ヒヤリハット経験をしている「セキュリティ危機予備群」のビジネスパーソンは約3割に。

Q1.あなたはセキュリティの知識に自信がありますか？
（SA／n=ビジネスパーソン1,410名）

7割以上（71.1%）が自信が無い！



全国47都道府県のビジネスパーソン（各都道府県30名／合計1,410名）に対し、自身のセキュリティの知識についての自信の有無を調査。7割以上（71.1%）が「自信が無い」と回答し、セキュリティの知識に不安を持つビジネスパーソンが大多数に上ることが明らかになりました。

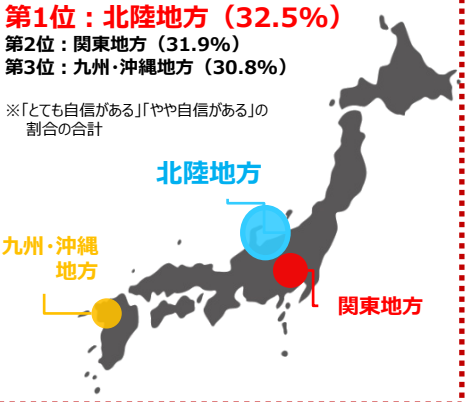
各地方ごとに比較してみると、「自信がある」「やや自信がある」と答えた割合が高かった地域は、北陸地方（32.5%）、ついで関東地方（31.9%）、九州・沖縄地方（30.8%）となりました。

＜参考：地方比較 ～その①～＞

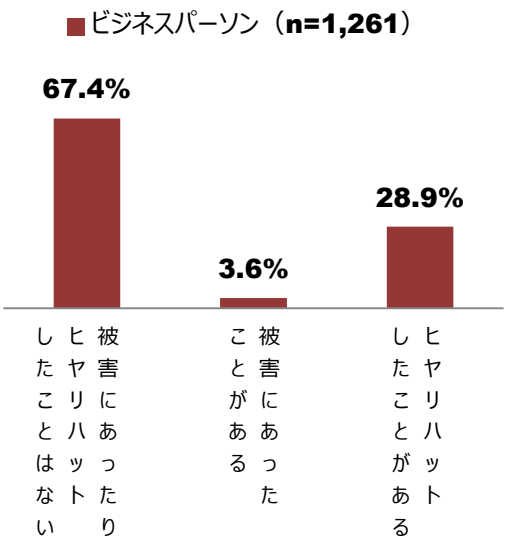
「自信がある」と答えたエリアは？（Q1）

第1位：北陸地方（32.5%）
第2位：関東地方（31.9%）
第3位：九州・沖縄地方（30.8%）

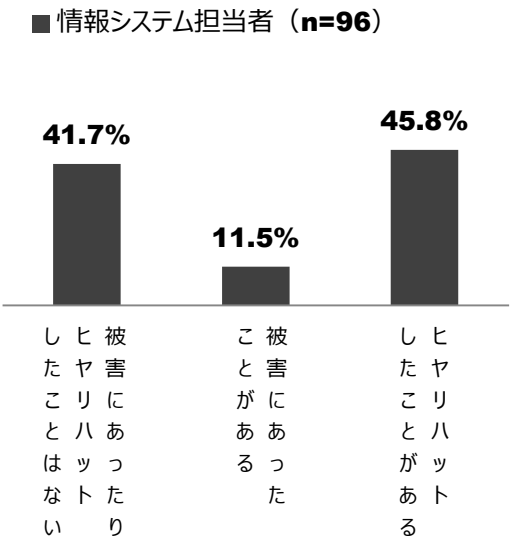
※「とても自信がある」「やや自信がある」の割合の合計



Q2.あなたは、過去1年以内にセキュリティの被害にあったり、もしくはヒヤリハット（※1）したことはありますか？
（SA／n=「わからない」と回答したビジネスパーソンを除く1,261名）



Q3.あなたの職場で、過去1年以内に企業としてセキュリティの被害にあったり、もしくは社員がヒヤリハットしたことはありますか？
（MA／n=「わからない」と回答した情報システム部門担当者を除く96名）



そこで、日々の業務で起こり得るセキュリティの被害やヒヤリハットについて過去1年以内の有無を問うと、ビジネスパーソンでは約3割（28.9%）が、ヒヤリハットを経験していることが判明。また、企業のセキュリティを管理する立場にある情シスに至っては、4割以上（45.8%）が所属している企業の社員のヒヤリハット経験を把握していると回答しました。危ういところで被害を逃れている**「セキュリティ危機予備群」**が実は多く存在していることがわかります。

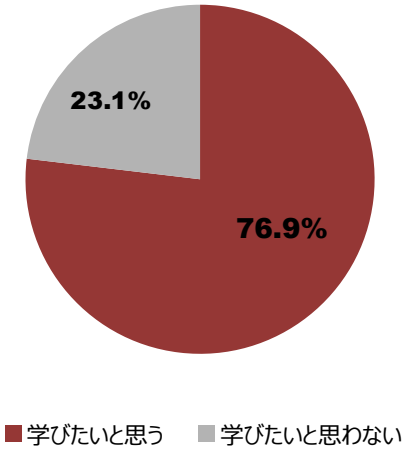
また、企業として実際に被害や事故を起こしてしまったことのある情シスに対し、その要因を伺うと（MA／n=56）、「メールの誤送信（1位）」が最も多く、ついで、「ウイルス感染（２位）」、「スマホやPCの盗難（３位）」「外部攻撃を受けた（4位）」「ランサムウェアに感染した（5位）」「情報漏えいをした（6位）」「その他（7位）」という結果となりました。

（※1） 被害にあいそうになったが回避し、被害にあわなかったこと。それによって「もしかしたら危険だったかもしれない」と思うこと。

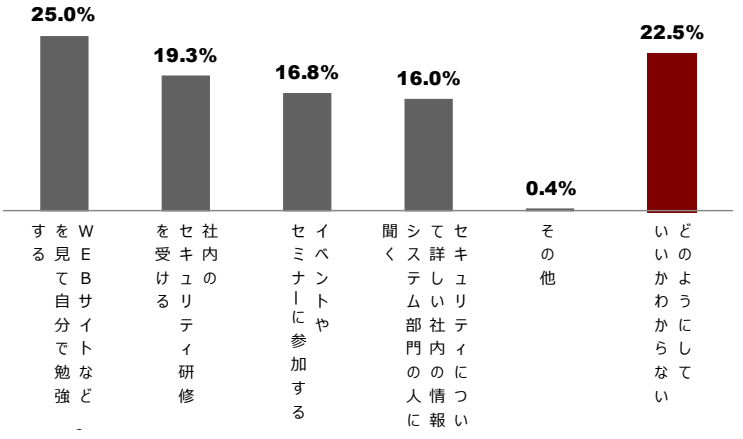
TOPICS②セキュリティ教育への意識とその教育環境について

ビジネスパーソンの7割以上がセキュリティ知識の習得に前向き。一方、5人に1人がその知識習得のための具体的な方法が分からない、“セキュリティ教育難民”であることが明らかに！

Q4.自身のセキュリティ知識を向上させるために、セキュリティを学びたいと思いますか？
（SA／n=ビジネスパーソン1,410名）

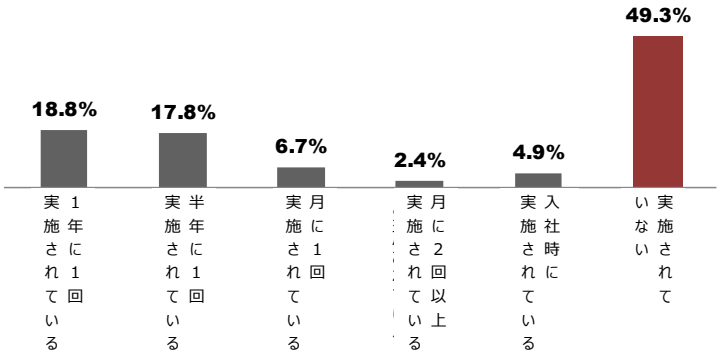


Q5.セキュリティに関して学ぶために、まず何をすればよいと思いますか。
（SA／n=ビジネスパーソン1,410名）



次に、セキュリティ教育への意識とその教育環境をテーマにビジネスパーソンへ調査。セキュリティ知識を向上させるために、学びたいかと問うと、7割以上（76.9%）が「学びたい」と回答。さらに、その知識の向上のために、まず何をすればよいと思うかを聞いたところ、「WEBサイトなどを見て自分で勉強をする（25.0%）」が最も多く、ついで、「社内のセキュリティ研修を受ける（19.3%）」という結果に。一方で、「どのようにしていいかわからない（22.5%）」と、ビジネスパーソンの5人に1人が回答、知識を向上させたいと思うものの、その方法が分からない“セキュリティ教育難民”であることが明らかとなりました。

Q6.あなたの職場では、セキュリティに関する教育や研修は実施されていますか？
（SA／n=「わからない」と回答したビジネスパーソンを除く1,188名）



また、現在勤めている職場における、セキュリティに関する教育や研修の実施の有無を調査。実施していると回答した中では、「1年に1回実施されている（18.8%）」が頻度としては最も多い結果になりました。一方で、約半数（49.3%）のビジネスパーソンが「自社では、教育や研修が実施されていない」と回答。セキュリティの知識をビジネスパーソンが身に付けるにあたって、現状、教育環境は決して十分ではないことが伺えます。

＜参考：地方比較 ～その②～ ＞

「学びたい」と答えたエリアは？（Q4）

第1位：北海道・東北地方（80.0%）
第2位：関東地方（79.5%）
第3位：北陸地方（79.2%）、九州・沖縄地方（79.2%）

1年に1回以上教育が実施されているエリアは？
※「入社時のみ実施」は除く（Q6）

第1位：関東地方（56.6%）
第2位：中国地方（50.0%）
第3位：近畿地方（48.4%）

※「1年に1回実施されている」「半年に1回実施されている」「月に1回実施されている」「月に2回以上実施されている」の合計の割合で算出

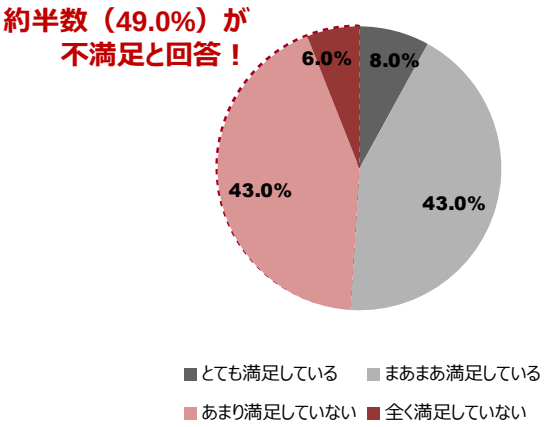
関東地方は「セキュリティ知識の自信」も比較的高かった地域。学習意欲、教育の実施度と合わせて関東地方が高い値を出しました。

学習意欲が高い値となった北海道・東北地方。3位の北陸地方はQ1の「自信」も1位にランクイン。関心が高いことが伺えます。

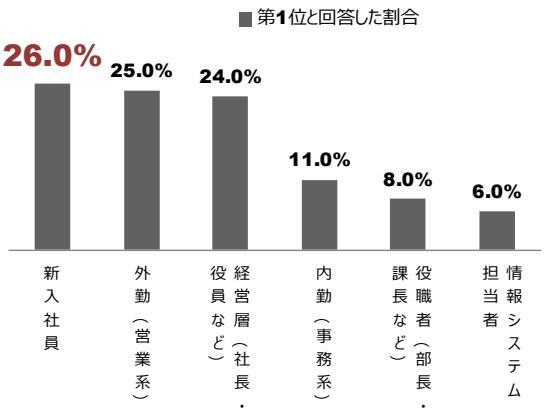
TOPICS③情シスが抱える社内のセキュリティ教育への課題について

自社のセキュリティ知識レベルに、約半数の情シスが不満を抱えている結果に。
今後、セキュリティ事故を引き起こしてしまう恐れがある役職は、
第1位「新入社員」、ついで「外勤（営業系）」、「経営層（社長・役員）」に。

Q7.あなたは自社のセキュリティ知識レベルについて満足していますか？
（SA／n=情報システム担当者100名）



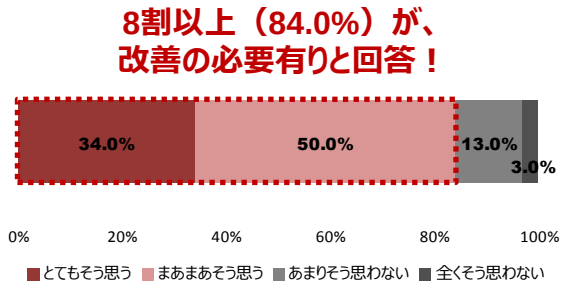
Q8.今後セキュリティ事故が起こる可能性が最も高いと考えられる役職を教えてください。
（SA／n=情報システム担当者100名）



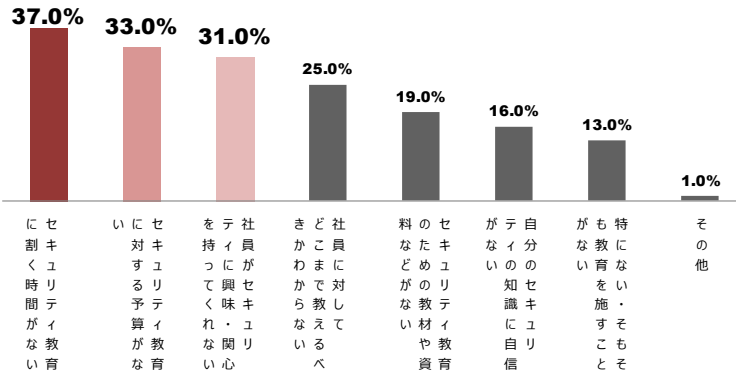
次に、情シスに対し、自社のセキュリティ知識レベルについての満足度を問うと、約半数（49.0%）が不満に思っていると回答。自社のセキュリティ知識レベルに対し、不安視していることが分りました。そこで、今後、セキュリティ事故を引き起こしてしまう恐れがあると思われる役職を伺うと、第1位は、「新入社員／26.0%」、ついで「外勤（営業系）／25.0%」、「経営層（社長・役員など）／24.0%」という結果となりました。この調査結果を受けて、徳丸氏は**「新入社員は社会人経験が浅いことからまだ意識や知識があまりないこと、外勤はスマホや書類等を外出先で紛失する恐れがあること、経営層は秘密情報に触れる機会が多い上に他人から注意される機会が少なく自己流の対応を行っている場合が多いからではないか」**とコメントしました。

8割以上の情シスが社内のセキュリティ教育に改善の必要ありと回答！
情シスが抱える課題は、「時間」、「お金」、「社員の興味・関心」！

Q9.社内でのセキュリティ教育に改善の必要があると感じますか？
（SA／n=情報システム担当者100名）



Q10.セキュリティに関して教育を施す際に、困っていることは何ですか。
（MA／n=情報システム担当者100名）



情シスに対して、社内のセキュリティ教育について改善が必要か否かを調査すると、8割以上（84.0%）が改善が必要であると回答しました。また、セキュリティに関する教育を施すにあたり困っていることを問うと、「セキュリティ教育に割く時間がない（37.0%）」が第1位に、ついで、「セキュリティ教育に対する予算がない（33.0%）」、「社員がセキュリティに興味・関心を持ってくれない（31.0%）」という結果となり、情シスは、「時間」、「お金」、「社員の興味・関心」の改善に課題を感じていることが分かりました。

インシデント対応に1カ月あたり32時間、1日あたり1.6時間を費やしている状況。
また、セキュリティ教育のための「予算はない」と3割以上の情シスが回答。
セキュリティ教育改善のためには、経営者へもっとアピールすべき!?

Q11.就業時間のうち、インシデント対応にとられる時間は何割ですか。
1ヵ月の仕事を100%として考えてください。
（FA／n=情報システム担当者100名）

インシデント対応にとられる時間の平均の割合／1カ月
20%

→

インシデント対応にとられる平均時間／1カ月
32時間

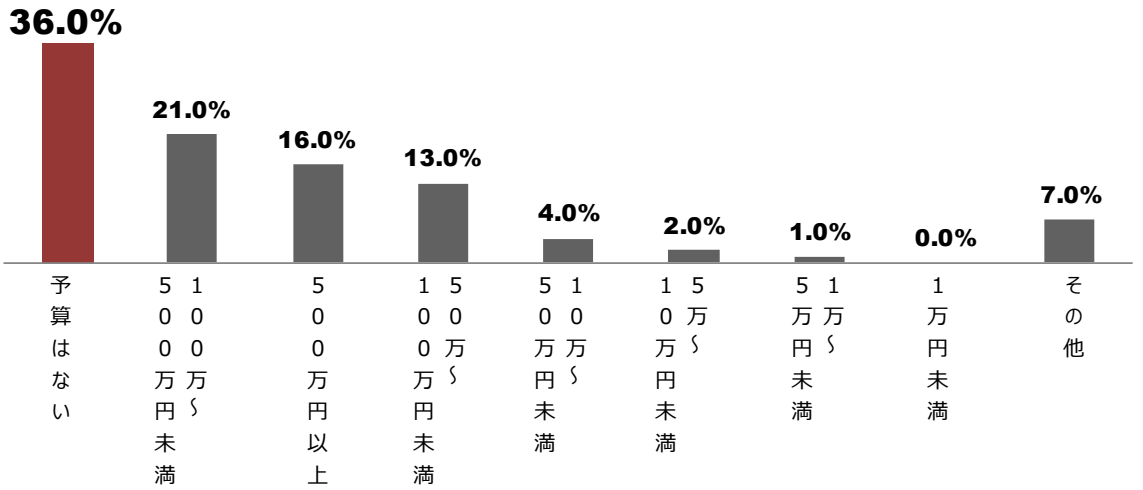
※1日8時間労働×20日勤務の場合
160時間×20%

→

インシデント対応にとられる平均時間／1日
1.6時間

※インシデント対応にとられる時間／1カ月
32時間÷20日勤務

Q12.セキュリティ教育のための年間の予算を教えてください。
（SA／n=情報システム担当者100名）

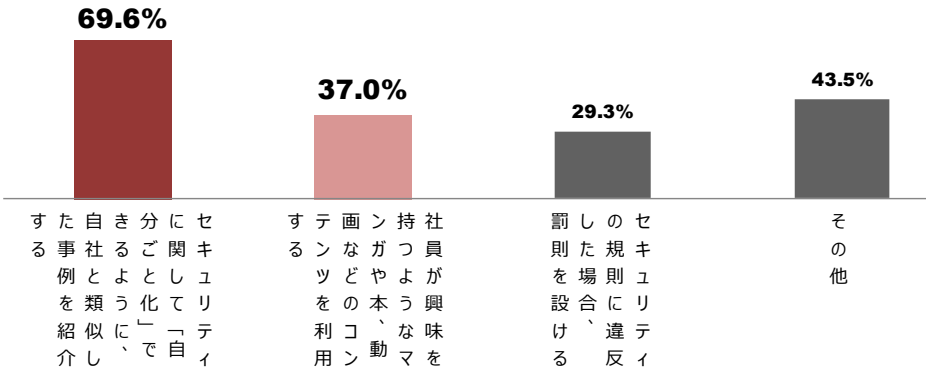


セキュリティ教育の改善にあたり、情シスが最も課題に感じている「セキュリティ教育に割く時間」。この調査結果を受け、情シスが1カ月あたりに業務領域であるセキュリティに関する事件や事故といったインシデントにどれ程の時間を要しているかを調査すると、1カ月あたり平均20%を割いていることが分かりました。時間に換算すると1カ月あたり32時間、1日あたり1.6時間を費やしている試算となります（※1日8時間労働×20日勤務として計算）。
これに対し、徳丸氏は**「インシデント対応に要する時間を減らすためには、まず教育などによりインシデントの要因を減らし、インシデントそのものを減らすこと。また、ありがちなインシデントについては予め手順を明確にして、対応の訓練をしておくことにより、スピーディかつ正確にインシデント対応を行うことが重要です」**とコメント。

また、「時間」についで、課題として挙がったのが「セキュリティ教育に対する予算がない」ということ。その現状を調査してみると、「予算はない（36.0%）」という回答が最も多く、セキュリティ教育に対する企業の予算の確保は満足とは言えない状況が伺えます。これに対し、徳丸氏は**「予算がない、あるいは限られている中でセキュリティ教育を実施する上では、IPA（独立行政法人 情報処理推進機構）やMOTEXが発行している低コストの優れたツールを活用すること。また、経営者に対して予算を確保するための働きかけを継続していくことが重要です」**とコメントしました。

「自分ごと化できる事例の紹介」、「親しみやすいコンテンツの利用」。
社員がセキュリティ知識を身につけるにあたり、情シスはこの2点を重要視！

Q13.セキュリティに関する知識を社員に身につけさせるために、どのような点に注力すればよいと思いますか。
（MA／n=「わからない」と回答した情報システム部門担当者を除く92名）



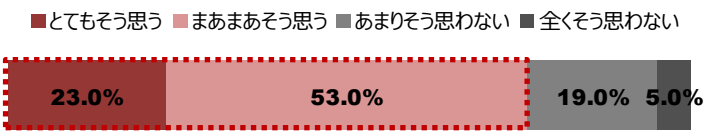
情シスがセキュリティ教育の改善のための課題の一つに挙げた「社員の興味・関心」。この調査結果を受けて、社員にセキュリティ知識を身につけさせるために注力すべきことを問うと、約7割（69.6%）の情シスが「セキュリティに関して自分ごと化できるように、自社と類似した事例を紹介する」を重要視していることが分かりました。ついで、「社員が興味をもつようなマンガや本、動画などのコンテンツを利用する」に、約4割（37.0%）の情シスが回答し第2位に。これに対し、徳丸氏は、**「自分ごと化には、確かに自社と類似した状況での事例が有効であるし、教育にあたっては、わかりやすさと正確さを両立したテキストが重要になります」**とコメントしました。

ご参考）セキュリティ教育ツール、7割以上の情シスに需要有り！
セキュリティの原理原則をまとめたセキュリティブック
「セキュリティ 7つの習慣・20の事例」

昨今のITの進化に伴いセキュリティも変化が激しく、より複雑になっています。これらの課題を解決すべく、MOTEXは情報漏えいの「自分ごと化」を促す**“NO MORE 情報漏えいプロジェクト”**の一環として、**セキュリティの原理原則をまとめたセキュリティブック『セキュリティ 7つの習慣・20の事例』**を制作し、電子データ（PDF）を無償で提供。日常生活に結びつく**「セキュリティ 7つの習慣」**と、身の回りの情報漏えいリスクを**「20の事例」**にまとめています。シンプルな内容にかわいらしいキャラクターを添え、「パスワードを強くすること」「ソフトウェアを最新の状態に保つ」といった、読者が自身の生活に重ね合わせて考えることができる構成になっています。

また、情シスに対して、「セキュリティ教育を行うための教育ツール（本や資料、テストなど）があれば使ってみたいか」と伺ったところ、7割以上（76.0%）の情シスが使ってみたいと回答。セキュリティ教育を担う情シスから、教育ツールに対する需要が分かりました。MOTEXでは、情シスをはじめ企業のセキュリティ教育を担う方へ、本書の導入、活用を訴求して参ります。

Q.セキュリティ教育を行うための教育ツール
（本や資料、テストなど）があれば使ってみたいと思いますか。
（SA/n=情報システム部門担当者100名）



7割以上（76.0%）の情シスに需要有り！

【提供内容（セキュリティブック・講師用資料・テスト）概要】

コンテンツはすべてWebからダウンロード・購入申し込みが可能です。
http://www.motex.co.jp/vision/enlightenment_activity/education_book/

①セキュリティブック『セキュリティ 7つの習慣・20の事例』
PDF：無償
書籍版：1,200円（税・送料別）
※リリース記念キャンペーン実施中（4/28まで）
キャンペーン特別価格800円（税・送料別）
※LanScopeユーザー様は600円（税・送料別）でご提供します
発行　：エムオーテックス株式会社
ページ：100ページ

①


③


②講師用資料
PDF：無償
※書籍版を10冊以上購入の方には、編集可能なPPTデータをご提供します

②


③テスト
PDF：無償
※書籍版を10冊以上購入の方には、編集可能なExcelデータをご提供します

NO MORE 情報漏えいプロジェクト 特設サイト

2014年の“NO MORE 情報漏えいプロジェクト”発足に合わせて特設サイトをオープン。本サイトでは、「情報漏えい」に対する知識を深め自分ごと化してもらうためにケーススタディやコラムを公開。そのほか、一般公開アンケートによる意識調査レポートの発表や「情報漏えい」のリスクを分かりやすく覚えることのできる、妖怪キャラクターを用いた診断コンテンツ“情報漏えい 百鬼夜行”を展開しています。

サイト名　　：NO MORE 情報漏えいサイト
サイトURL　：http://www.motex.co.jp/nomore/
Facebook　：www.facebook.com/motex.nomore

エムオーテックスについて

MOTEXは、ネットワークシステム管理・ネットワーク情報漏えい対策商品LanScopeシリーズの企画・設計・開発から販売を一貫して行っているメーカーです。**“LanScope Cat”**は、多くの企業が抱えるIT資産管理や情報セキュリティ対策の課題を解決し、企業成長をサポートするセキュリティツールです。1996年の発売以来、時代のニーズに応じて進化しつづけ、その結果多くの企業の信頼を集め、LanScopeシリーズは国内導入実績10,000社※1を突破。また、IT資産 / PC構成管理ソフトウェア部門で12年連続シェアNo.1※2となるほか、顧客満足度No.1※3など統合運用管理ソフトとして数々の賞を受賞しています。MOTEXは、今後もお客様の企業利益を創出するセキュリティ対策をご提案します。

※1：当社調べ
※2：富士キメラ総研「2016 ネットワークセキュリティビジネス調査総覧 上巻」の「IT資産 / PC構成管理ツール」分野（2015年度）
※3：中小企業向けセキュリティアワード2015「今後も利用し続けたいIT資産管理製品　第1位」「誰かにすすめたいIT資産管理製品 第1位」

【会社概要】

社名　　：エムオーテックス株式会社
代表取締役社長　：河之口 達也
設立　　：1990年
資本金　　：2,000万円
本社所在地　：大阪市淀川区西中島5-12-12 エムオーテックス新大阪ビル
URL　　：http://www.motex.co.jp/