CISM Certified Information Security Manager
An ISACA Certification

ISACA
Trust in, and value from, information systems
Tokyo Chapter

パネルディスカッション

2013年10月26日
ＩＳＡＣＡ東京支部 ＣＩＳＭ委員会

パネラー

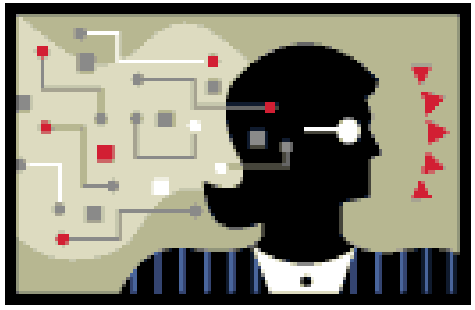
- 株式会社ラック　長谷川 長一
- 日本クラウドセキュリティアライアンス　山崎 英人
- 警察庁　間仁田 裕美
- 情報システム監査株式会社　関　和正
  CISM委員会 委員長

コーディネータ

- 株式会社アイ・ティ・フロンティア　長久 浩三

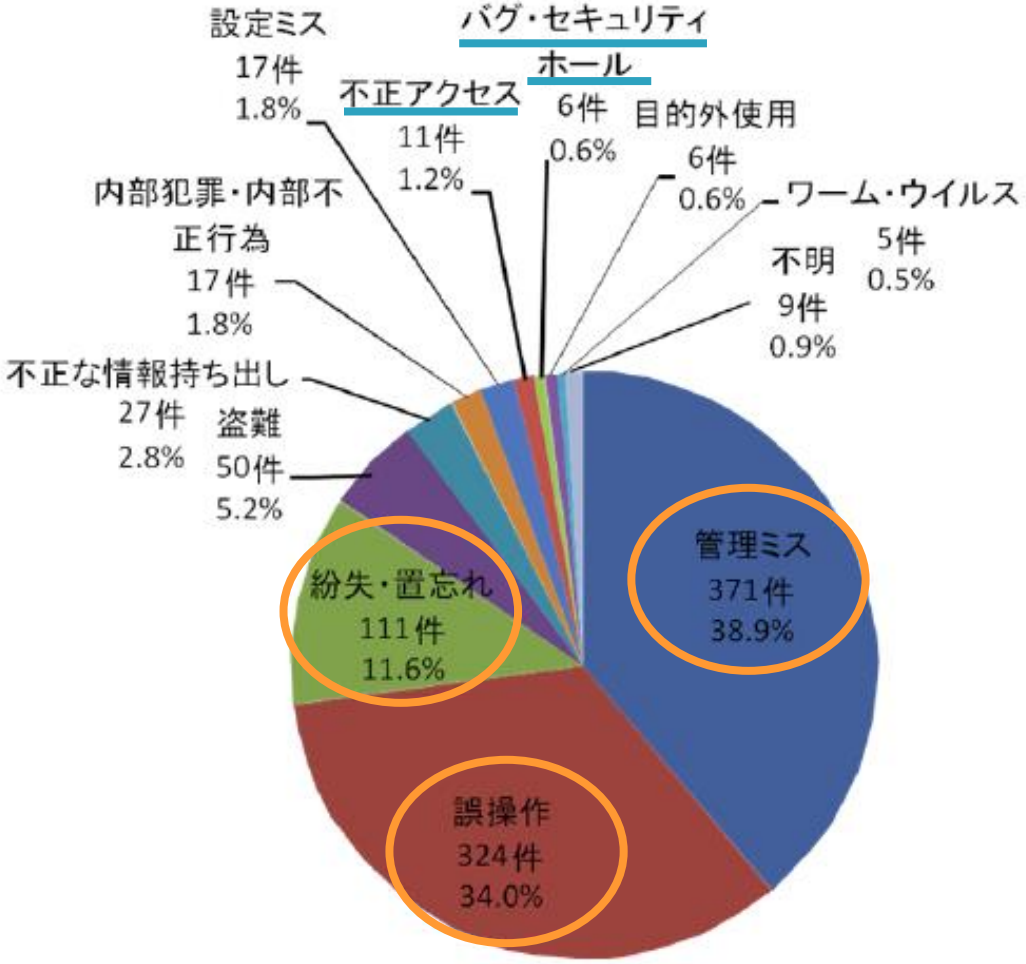
ディスカッションのテーマ

「組織におけるIT利用者の
セキュリティ意識を高めるためには」



１．ＩＴ利用者のセキュリティ意識の課題

（１）情報漏えいの原因
セキュリティの意識低下に関わるインシデントが多くみられる。



JNSA 2012 情報セキュリティインシデントに関する調査報告書より

１．ＩＴ利用者のセキュリティ意識の課題

（２）セキュリティ意識が起因する発生原因と内容

No	原因	発生率	内容
1	管理ミス	38.9	**引越し後に個人情報の行方がわからなくなった。**個人情報の受け渡し確認が不十分で、受け取ったはずの個人情報が紛失した。情報の公開、管理ルールが明確化されておらず、誤って開示してしまった。
2	誤操作	34	**宛先間違い**によって、電子メール・FAX・郵便の**誤送信**が発生した。
3	紛失・置き忘れ	11.6	**電車、飲食店など外部の場所で**、情報媒体等を**紛失または置き忘れてしまった。**
4	不正な情報持出し	5.2	社員・派遣社員、外部委託先業者、出入り業者、元社員などが、顧客先、自宅などで**私用するために情報を持ち出して、持出し先から漏えいした。**
5	内部犯罪・内部不正行為	1.8	社員・派遣社員など内部の人間が、機密情報を悪用するために不正に取得して持ち出した。**持ち出した情報を使って犯罪を行ったり、売買してりした漏えいした。**
6	設定ミス	1.8	Web等の**設定ミスで外部から閲覧できる状態になっていた。**
8	バグ・セキュリティホール	0.6	**OS、アプリケーション等のバク・セキュリティホールなど**によりWeb等から**機密情報が閲覧可能、または漏えいした。**

１．ＩＴ利用者のセキュリティ意識の課題

（３）今年上半期の個人情報漏洩事件・事故の一例

2013/10/10　大手電力会社は、原発事故で避難している住民の賠償関連書類などを業務委託先の職員が屋外のゴミ箱に捨てていた。

2013/9/30　某監査機構は、監査の取引先の氏名や取引残高などが保存されていたUSBメモリを、持出し禁止にも関わらず持ち出して紛失した。

2013/9/27　空港子会社の従業員が店舗を利用した俳優のクレジットカード伝票を携帯電話で撮影し写真をTwitter上に投稿していた。

2013/9/25　M県は県内企業の購買・開発担当者等461名に対しメール送信したところ、送信先の企業名・部署名・担当者名・メールアドレスが記載されたファイルを誤って添付して送信した。

2013/05/27　H県K市において、同市男性職員が女性職員に依頼して市住民情報システムより個人情報を取得し、調査会社の知人に漏らして現金を受け取っていた。

2013/5/21　小学校教師が同僚と深夜まで飲食して泥酔して、担当している学級の答案用紙や点数表を鞄ごと紛失した。

１．ＩＴ利用者のセキュリティ意識の課題

（４）皆さんの周りでセキュリティ意識が欠如して
いると思われることはありますか？

例

a. 会社やお客様の貸与品を紛失※する

※紛失物＝入館証、携帯電話、USBメモリ、PC、書類

（a）飲酒して帰宅途中にPCの入ったカバンを紛失した。
（b）電車の網棚に入館証とUSBメモリの入ったカバンを置き忘れた。
（c）飲食店などのテーブルに携帯電話を置き忘れた。
（d）組織変更などで移動を繰り返すうちに重要書類を無くした。
（e）重要書類を誤って廃棄するものと一緒に捨ててしまった。

b. メールの誤送信

（a）宛先に別に会社の社員が含まれていることに気づかず送った。
（b）添付ファイルを誤って別の会社のファイルを付けて送った。
（c）添付ファイルにパスワードや暗号化を掛けずに送った。

１．ＩＴ利用者のセキュリティ意識の課題

（４）皆さんの周りでセキュリティ意識が欠如して
いると思われることはありますか？

例

c. データベースのアクセス権限を見直していない

（a）組織変更などで現在の業務に関係ない者が見れてしまう
状態のまま放置している。

（b）利用者に合ったアクセス権限を与えていない。（全員管理者権限）

d. PCやUSBメモリなどの持出し管理ができていない

（a）持出しの手続きはあるが形式的なものになっている。

（b）個人情報や機密情報が含まれているか把握できていない。

（c）持ち出す前にバックアップを取っていない。

e. 情報資産の棚卸が出来ていない

（a）情報資産の棚卸や台帳を更新ができていない。

（b）情報資産の重要度に応じた識別ができていない。

１．ＩＴ利用者のセキュリティ意識の課題

（４）皆さんの周りでセキュリティ意識が欠如していると思われることはありますか？

例

f. ウイルス対策が確実にできていない

（a）OSのアップデートやウイルス対策ソフトが最新の状態か確認していない。または、確認する仕組みや運用かない。

（b）サーバを停止する運用できていないため、OSのアップデートやウイルス対策ソフトの更新が遅れている。

g. 公共の場での会話

ロビー、エレベータ、交通機関、飲食店などの第三者がいる場所で平気で仕事の話をしている。

h. SNSの利用

Twitterやfacebookなどにお客様や会社の情報を書き込んでいる。

i. 報告遅延

インシデントが起きているのに報告が遅い。

2．セキュリティ意識欠如の原因

何故、セキュリティ意識が欠如するのでしょうか？

ルールも有る、セキュリティ教育もしている、監査もやっているのに何故

例

a. 自分はインシデントを起こさないと思っている。

b. インシデントが起きても影響がないと思っている。

c. 誰も見ていないので違反しても判らない思っている。

d. 業務が最優先で、セキュリティは二の次だと思っている。

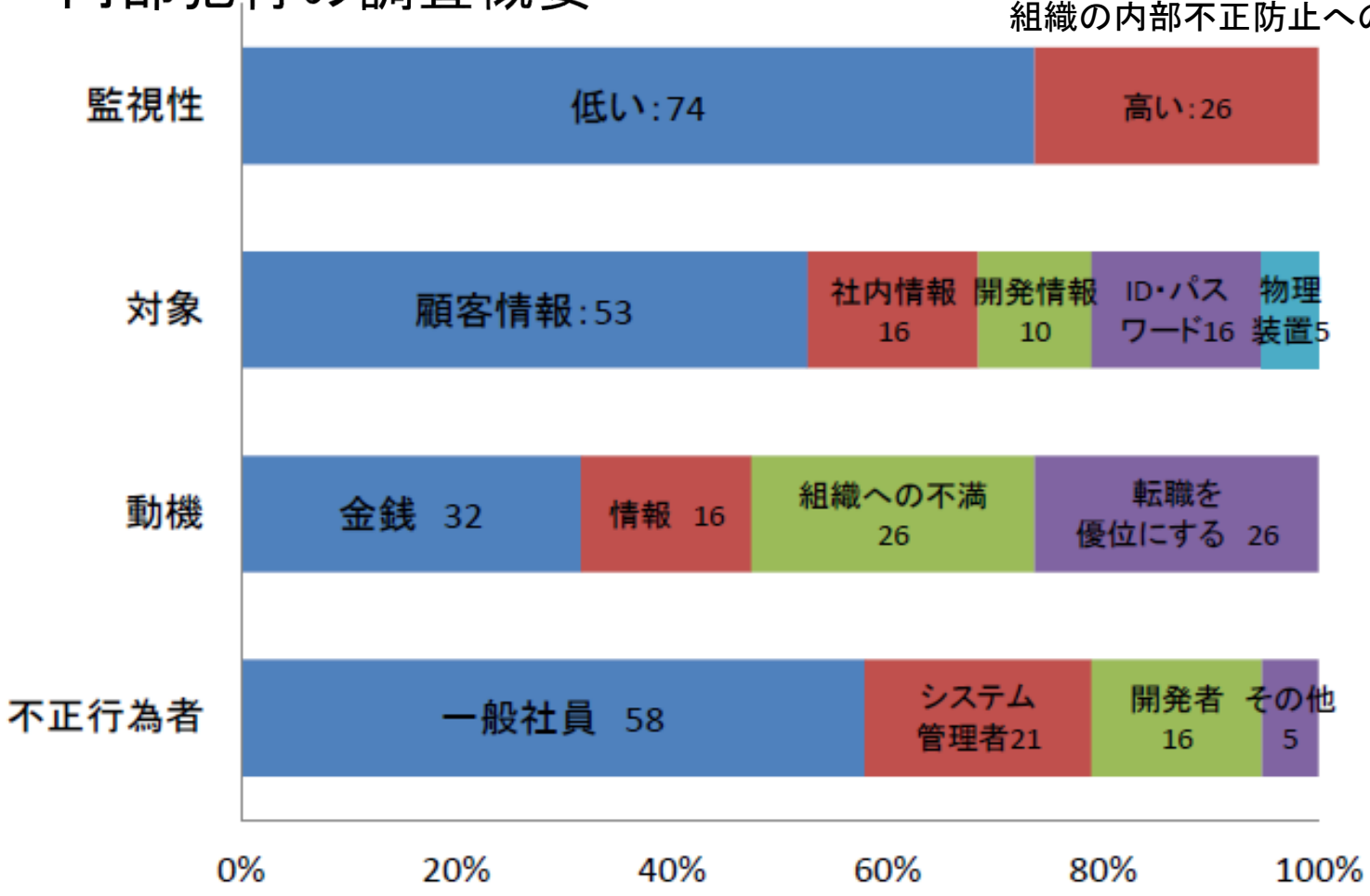
e. 人事評価や給与、組織に不満を持っていて、会社のルールに従いたくない。逆に利用して儲けたい。

2．セキュリティ意識欠如の原因

何故セキュリティ意識が欠如するのでしょうか？

内部犯行の調査概要

2013/3/15「IPA テクニカルウォッチ
組織の内部不正防止への取り組み」より



３．ＩＴ利用者のセキュリティ意識を高めるには

皆さんの会社や組織で取り組んでいることがあれば聞かせてください。

３．ＩＴ利用者のセキュリティ意識を高めるには

ヒント１

小松原明哲著書「ヒューマンエラー」より

■「知らないことはしない」「知らないことは聞く」の躾
「だろう作業」厳禁　このアプリ、たぶんダウンロードしても大丈夫だろう。

職場では原則を徹底する**「躾（しつけ）」が大切**

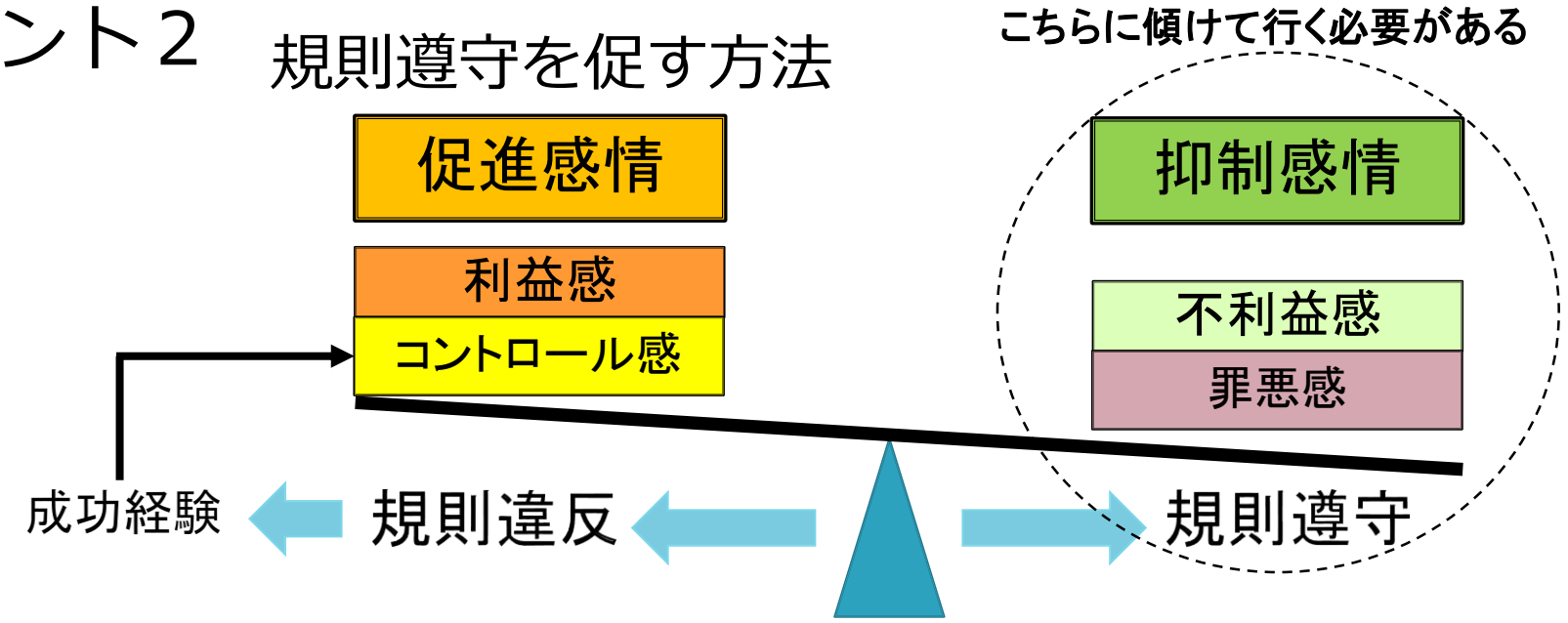
■ＷＨＹを教える知識教育
ＨＯＷ（どのように）だけでなく Ｗｈｙ（なぜそうなのか）ということも理解させる。

・面倒な手順、規則であれば、**その理由を理解させる。**

・人間は本質的にケチ、楽に簡単にしようとする本能がある。

３．ＩＴ利用者のセキュリティ意識を高めるには

ヒント２　規則遵守を促す方法



社会心理学　KSABモデルを使って、段階を踏みながら規則遵守行動を定着させる

K（Knowledge）**規則を知っている**：規則をその理由とともに、知ってもらう。
S（skill）**スキルを持つ**：規則を実行するための技術、技量を身に着けてもらう。
A（attitude）**前向きの態度をもつ**：規則を守ろうという態度、気持ちをもってもらう。
B（behavior）**行動できる**：KSAの結果として、規則を遵守する行動が出来るようになる。

小松原明哲著書「ヒューマンエラー」より

３．ＩＴ利用者のセキュリティ意識を高めるには

ヒント３　規則遵守を促す方法

小松原明哲著書「ヒューマンエラー」より

方　法	内　容
精緻化見込み理論	違反を起こすとどうなるか、結末と、自分が日ごろ行っている行動を対比させ、行動を振り返り、反省させる。
認知的不協和理論	規則の意義、自分の理想を考えさせた後、グループ討議を行い平素の行動とのギャップを指摘して、反発心をあおる。 その反発心はギャップを埋める行動を促す。
集団雰囲気	規則の順守度の高い職場に入れて、自然に染みつかせる。
決意表明	朝会、ミーティング、年頭に今年の決意を書いて全員が張り出すなど、全員の前で自分の決意を表明させる。
段階的依頼法	小さな規則遵守の目標を掲げさせ、それが実行できたら徹底的に褒める。そして次にもう少し大きな目標を立てて出来たら褒める。この繰り返しで徐々に遵守行動がとれるようになる。

４．まとめ

（１）ルール遵守
- 目的を理解させ、段階的に遵守行動がとれるようにする。
- 違反者は罰則し、反省と学びの機会を与える。

（２）セキュリティ教育
- ケーススタディなど討議の機会を設け、自ら考え気付きを与える。
- 起きた場合を想定した訓練を行い、対策の必要性を理解させる。

（３）ＩＴの利便性と危険性認識
- リスク低減の自動化、人的ミスをカバーする仕組みを取り入れる。
- 使い方によって危険が伴うことを理解させる。

（４）インシデント情報の共有
- 事例を共有して、危険性と発生原因・再発防止策を理解させる。

（５）人事制度と連携
- セキュリティの取り組みを目標に加え、成果を評価する。

ご清聴ありがとうございました。

パネルディスカッション

「組織におけるIT利用者のセキュリティ意識を高めるためには」