情報セキュリティマネジメント試験合格講座 午後試験対策 10

● 内部犯行の低減と検出

1. TBP(Trusted Business Partner)
〔　　〕あるビジネスパートナー。契約に基づいてサービスを提供する外部企業・団体(〔　　的　〕TBP)または部外者(〔　　的　〕TBP)。

2. 内部犯行の低減と検出に関するアドバイス

(1) TBP のポリシと処理手順を理解すること
(2) アクセスが許可された IP をモニタリングすること
(3) アクセス権を管理すること
(4) TBP の人事ポリシと処理手順を理解すること
(5) 職場で起こる〔 ネ　　ブ 〕な問題点を予測し、管理すること
(6) 関係者のアクセス権を削除した際、システム上でも確実に実施すること
(7) 責務の分離を強化すること
(8) 情報を保護する責任が TBP にもあることを、明確に契約に記述すること

✓ TBP のポリシと処理手順
組織的 TBP 内での物理的セキュリティ、従業員教育、従業員の経歴調査、セキュリティ対応手順、あるいはその他の(不測の事態に備えての)防護策など。

✓ TBP の人事ポリシと処理手順
TBP は従業員の経歴を徹底的に調査し、大丈夫と判断してから重要なデータの扱いを任せることを、TBP と業務契約を結んでいる組織は主張すべきである。

3. 情報流出 I (道具的犯行)
情報持ち出しなどの違反行為が、ある目的(例えば情報売却による金銭獲得)に沿った合理的な手段となっている事例。

4. 情報流出 II (表出的犯行)
情報持ち出しなどの違反行為が、〔　　的　〕な満足を得る(例えば鬱憤晴らし、情報を把握することで心理的な優位性を保つ)手段となっている事例。

5. 国内調査による内部犯行の特徴

種類		内容および特徴			
		システム悪用	情報流出Ⅰ (道具的犯行)	情報流出Ⅱ (表出的犯行)	破壊行為
個人的・人格的な特徴 (IT 能力／技術)		業務で使用している端末が使用できる程度の IT 技術の者が多くを占めていた。(高い IT 能力を有さない)	システム管理などの相対的に高い IT 技術を有する者が多い。	情報流出Ⅰと同じ傾向。	情報流出Ⅰと同じ傾向。
環境要因	業務の専門性	分業化され、専門化された業務に就いている者が多く、業務の監視性については、全体的に低い状況。			
	職場への不満	〔　①　〕	不満を感じていない者が相対的に多い。	システム悪用と同じ傾向。	情報流出Ⅰと同じ傾向。
犯行状況	動機	〔　②　〕	システム悪用と同じ傾向。	〔　③　〕	情報流出Ⅱと同じ傾向。
	その他	個々の事例や分類によって大きく異なり、日常業務で使用していたシステムに、組織の内部または外部からアクセスして犯行を行った事例や、情報収集のため〔 キ 〕を利用していた事例、他の従業員のメールを自宅で自動受信設定していた事例もあった。			

6. ルーティンアクティビティ理論（Routine Activity Theory）
犯罪者、犯行対象物、場所の三つの要因が重なった場合に犯行が発生するとしている。犯罪を未然に防ぐためにはこれらを同時に起こさないよう、「監視者」「行動規制者」「管理」が必要であるとしている。

要因	対策
（動機づけられた）犯罪者	行動規範者
（潜在的な）犯行対象物	監視者
（監視性の低い）場所	管理者

ルーティンアクティビティ理論では、違反者の意図や目標対象に対して、外部からのコントロールや抑止が困難な場合もある。一方で、〔　　者　〕の設置などによって外部からのコントロールを可能な「環境」を適切に定めることを主眼として、犯罪機会の低減、予防する研究に、状況的犯罪予防の理論がある。

7. 状況的犯罪予防
「ある特定の犯罪問題を削減するための、極めて実践的かつ効果的な手段」と定義され、犯罪に関連する多くのプロセスや要因について予防するための方策を検討するために用いられる。

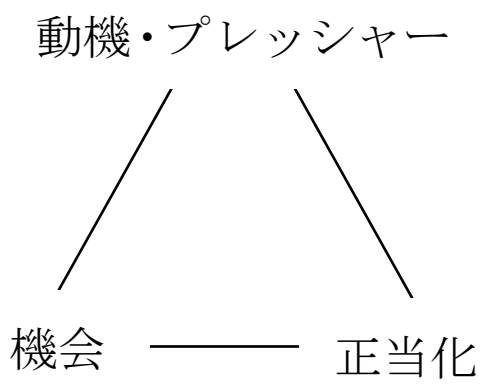
✓ 状況的犯罪予防における犯罪予防策の 5 分類
(1) 犯行を難しくする
技術的な対策を強化することで犯罪行為を難しくする
(2) 捕まるリスクを高める
管理や監視を強化することで捕まるリスクを高める
(3) 犯行の見返りを減らす
犯行を難しくするための技術的対策によって、犯行者から適切な目標物を遠ざけることや隠すことが困難な場合に適用
(4) 犯行の挑発を減らす
外部からの挑発による犯罪行為を抑止
(5) 犯罪を容認する言い訳を許さない
犯行者による自らの行為の正当化理由を排除する

8. 不正のトライアングル

ドナルド・R・クレッシーは、横領の発生要因は脆弱な内部統制や不充分な監視システムが根本的な原因ではなく、当事者が雇用主の信頼に意図的に背くことにより不正行為が発生すると分析している。

具体的には、動機・プレッシャー（例えば〔　　〕）を抱え、機会（この問題が自分の経済的に信頼されている立場を利用すれば、秘密裏に解決できること。例えば〔　　〕）を意識し、正当化（その解決策を実行しても、信頼された人物としての自分のイメージを損なわないで済むような理由付け。例えば〔　　〕）を考えつく時に発生すると考え、この「動機・プレッシャー」、「機会」、「正当化」を不正のトライアングルと定義している。

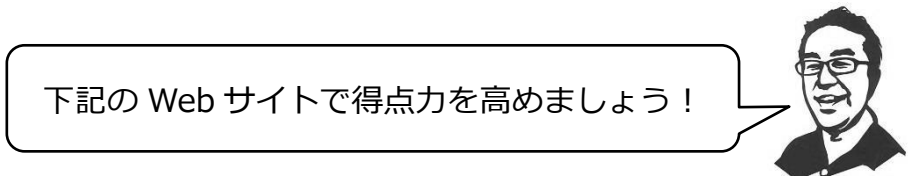
Donald R. Cressey "Fraud Triangle"



9. 不正のトライアングルに基づく対策

不正のトライアングルに基づいて内部不正対策を行う場合には、不正のトライアングルの 3 つの要因に関して低減する対策を検討することになる。例えば、〔　　〕などの対策を実施することで内部不正を行う「機会」を低減させて、内部不正の件数の低減を図ることができる。

出典：IPA「組織内部者の不正行為によるインシデント調査－調査報告書－」



- ✓ 翔泳社「情報セキュリティマネジメント要点整理＆予想問題集」
- ✓ 情報セキュリティマネジメント試験合格講座　http://rakupass.com/security/