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 09

- 内部者の不正行為

1. ハインリッヒの法則
   1 件の重大な事故・災害の背景には、29 件の軽微な事故・災害が起こっており、300 件のヒヤリ・ハットが起きていると言われる。

2. ヒヤリ・ハット
   重大な事故や災害に至らないが、重大事故につながりかねない事故寸前の危険な事例のこと。

3. Cyber Security Watch Survey
   米国 CERT（Computer Emergency Response Team）の 2011Cyber Security Watch Survey では、2010 年に発生した全てのサイバー犯罪のうち、標的型攻撃などの組織の外部からの攻撃に起因するものが 73%を占め、残りが組織の内部者による不正行為によって引き起こされたものと報告されている。

   (1) Cyber Security Watch Survey の報告によると、外部からの攻撃によるものと、内部者の不正行為によるものについてどちらの被害額が大きいかの質問に対して、外部からの攻撃が 38%であり、内部者による不正行為が 33%であった。

   (2) 内部者は価値のある重要な情報の場所を知っており、社内の情報システムの知識やアクセス権をもつことから、内部者による不正行為が発生すると被害が大きくなると考えられる。

   (3) 日本ネットワークセキュリティ協会（JNSA、Japan Network Security Association）が 2010 年に実施した「2010 年のインシデントに関する調査」によると、内部者の不正行為による個人情報の漏えいに関するインシデントは 2005 年から 2010 年の間、毎年の全ての漏えい人数のうち、4%から 30%を占めている。

4. 情報収集の困難性
ヒヤリ・ハットに関する事例について情報収集が困難な理由は、「風評被害が発生する恐れ」や「利害関係者との調整がつかない」などの理由から公開されることが稀であることから、内部者による不正行為の発生しやすい環境や、効果的な対策などの検討が難しい現状がある。

5. 内部不正と内部犯行
IPA の「組織内部者の不正行為によるインシデント調査ー調査報告書」では、「うっかりミス」、「企業内のルール違反」などを含めた全体の内部者の不正行為を「内部不正」とし、その中で、犯罪として立件に至ったものを特に「内部犯行」と呼んでいる。

6. 内部犯行者
CERT の「Insider Threat Study（ITS）」では、以下の三つの条件を満たす者と定義している。

(1) 現在もしくは過去の社員、その他の被雇用者もしくはビジネスパートナー
(2) 組織の IT システム(ネットワーク、システム、データ)への正規に認められたアクセス権を持っている、もしくは持っていた者
(3) 意図的にそのアクセス権を用い、組織の情報の機密性、完全性、可用性に対して負の影響をもたらした者

7. 内部犯行の分類概要および特徴
ITS では、内部犯行の分類および特徴を以下のように分類している。

(1) システム悪用(Employee Fraud)
組織の財やサービスをごまかし(Deception）やペテン(Trickery）で手に入れる。

- ✓ しばしば内部者の金銭的問題が関係する。
- ✓ 1/3 のケースで、外部の手引き者が存在した。情報改ざんについては、同僚がおぜん立てすることが多い。
- ✓ 内部脅威者のストレスを引き起こすものが観察される。（例えば借金、家族問題など）

(2) 情報の持ち出し(Theft of Information)
機密や知財に関連する情報などを組織から盗み出す。

- ✓ 内部脅威者は、情報窃取のリスクに関連する個人的な傾向(Personal Predispositions)をもつ。たとえば、期待に反した待遇(報酬、昇進、オンライン活動への自由、倫理感、プロジェクト期限など他)についての不満を持っている。組織を辞めた後に侵入可能なように、アクセス経路を作っていることが多い。
- ✓ 前兆があるが、ほとんどの場合、組織は技術的な前兆を見落としている。
- ✓ 管理者は、前兆を見逃がさないようにモニタリングをすべきで、そのようにポリシを策定すべきである。
- ✓ 信頼(Trust)は、リスクを軽減する。

(3) 破壊行為(IT Sabotage)
特定個人、組織(含む組織のデータ、システム、日常業務)に損失を与えるという意志に基づいた悪意ある行動

- ✓ 知的財産(IP)を金銭目的で売ろうとするものは少なく、むしろ、転職や起業などの際の自己のビジネスの優位のため、また、外国政府などへ持ち出す。
- ✓ IP を盗む者は、科学者、エンジニア、プログラマやセールスパーソンが多い。
- ✓ 盗む対象は、通常の業務で扱っている情報が多いので、これを防ぐのは困難である。
- ✓ 転職、処遇などの組織への不満、肩書などはすべて情報を盗む意思決定に影響する。
- ✓ 情報は、さまざまな手法を使い、退職から 1 ヶ月以内に盗まれている。
- ✓ 退職の 1 ヶ月前と 1 ヶ月後の、2 ヶ月のモニターが必要である。この間の外部とのやり取りをすべてログしておくべきである。

8. 知的財産(IP、Intellectual Property)
特許、著作権、商標、意匠、科学的公式、ソースコードの一部であり、顧客に関する機密情報のような財産的な情報(Proprietary Information)を含めた独自・創造的な発想。

9. IP の盗難
内部者がITを利用し、IPを組織から盗むことを指す。但し、ID(Identification)の盗難は除かれる。

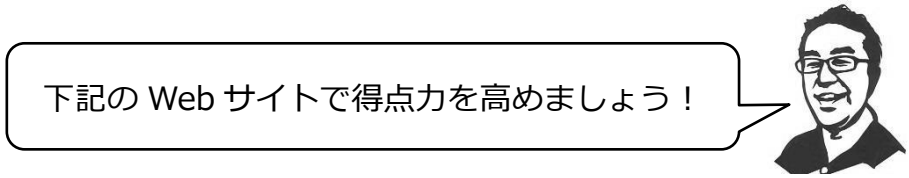
10. TBP(Trusted Business Partner)
信頼あるビジネスパートナー。契約に基づいて、ある組織(企業、団体)に向けてサービスを提供する外部企業・団体(組織的 TBP)または部外者(個人的 TBP)を指す。サービスを提供するためには、組織は、TBP に対して特許データ、重要資料、内部インフラの構成などの情報へのアクセス権限を提供しなければならない。

11. TBP の例、
組織的 TB には、組織から、顧客向けのサポート業務を委託された企業があり、一方、個人的 TBP の例としては、その組織と個人契約を締結するコンサルタントや契約社員および臨時の社員(パートタイム)などが含まれる。

12. 内部犯行調査で明らかになったポイント

(1) 多くの内部犯行者は悪意ある行動に身を冒す個人的な傾向を有している
(2) 多くの内部犯行者の不満は期待が裏切られたことに端を発する
(3) 処罰や(従業員にとって)好ましくない出来事が破壊行為の発生確率を上げる
(4) 多くの場合、犯行の兆候を示す振る舞いが確認されているが、看過される
(5) 侵入するため、そして痕跡を隠すために組織の経営層に気づかれぬように裏口を設ける。大半の行為は退職後にその裏口を用いて行われる
(6) 組織は技術的な前兆を見落としている
(7) 物理的、技術的アクセス制御の欠如が破壊行為を容易にする

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/