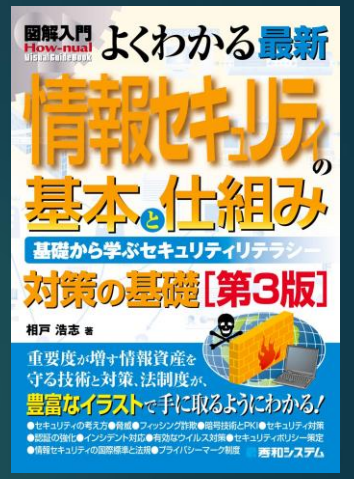
内部不正対策はなぜ難しいか?

2024年11月27日

金融情報システム監査等協議会
米川　敦

Profile



- 楽天5社を兼務（楽天、カード、銀行、証券、ペイ　2023～）
- 前職　住友信託銀行～三井住友信託銀行 CSIRT （2003～2022）
- 金融情報システム監査等協議会 会長（2010年から運営）
- 内閣官房 内閣サイバーセキュリティセンター NISC
  サイバーセキュリティ監査官、ペネトレ統括班長(2016～2018)
- FISC安全対策基準の策定 (2005 - 2019)
- セキュリティの国際資格を運営する ISC2 より Information Security Leadership Awards 2019 を2部門受賞
  Senior Security Professional, Community Service Star
- CISSP、CISA、公認システム監査人、情報セキュリティ監査人
- 台湾HITCONでの海外講演も10年！ (2012, 2013, 2015, 2021)
- 銀行員が個人で情報発信すると広報、監査が煩いので相戸浩志という名前を使っています
- 「情報セキュリティの基本と仕組み」著者、３万５千部！大学の教科書に採用10年！

本スライド内容について

- 新聞等で公表されている内容に基づいて説明しています
- 機密情報は一切ありません
- 会社の業務とも関係ありません
- 直近10年の金融機関の事例は扱いません

IPA「情報セキュリティ10大脅威 2024 脅威ランキング」

2023年に発生した社会的に影響が大きかったと考えられる情報セキュリティにおける事案から、IPAが脅威候補を選出し、情報セキュリティ分野の研究者、企業の実務担当者など約200名のメンバーからなる「10大脅威選考会」が脅威候補に対して審議・投票を行い、決定したものです

https://www.ipa.go.jp/security/10threats/10threats2024.html

https://www.ipa.go.jp/security/10threats/10threats2023.html

2024年

順位	「組織」向け脅威
1	ランサムウェアによる被害
2	サプライチェーンの弱点を悪用した攻撃
3	内部不正による情報漏えい等の被害
4	標的型攻撃による機密情報の窃取
5	修正プログラムの公開前を狙う攻撃（ゼロデイ攻撃）
6	不注意による情報漏えい等の被害
7	脆弱性対策情報の公開に伴う悪用増加
8	ビジネスメール詐欺による金銭被害
9	テレワーク等のニューノーマルな働き方を狙った攻撃
10	犯罪のビジネス化（アンダーグラウンドサービス）

2023年

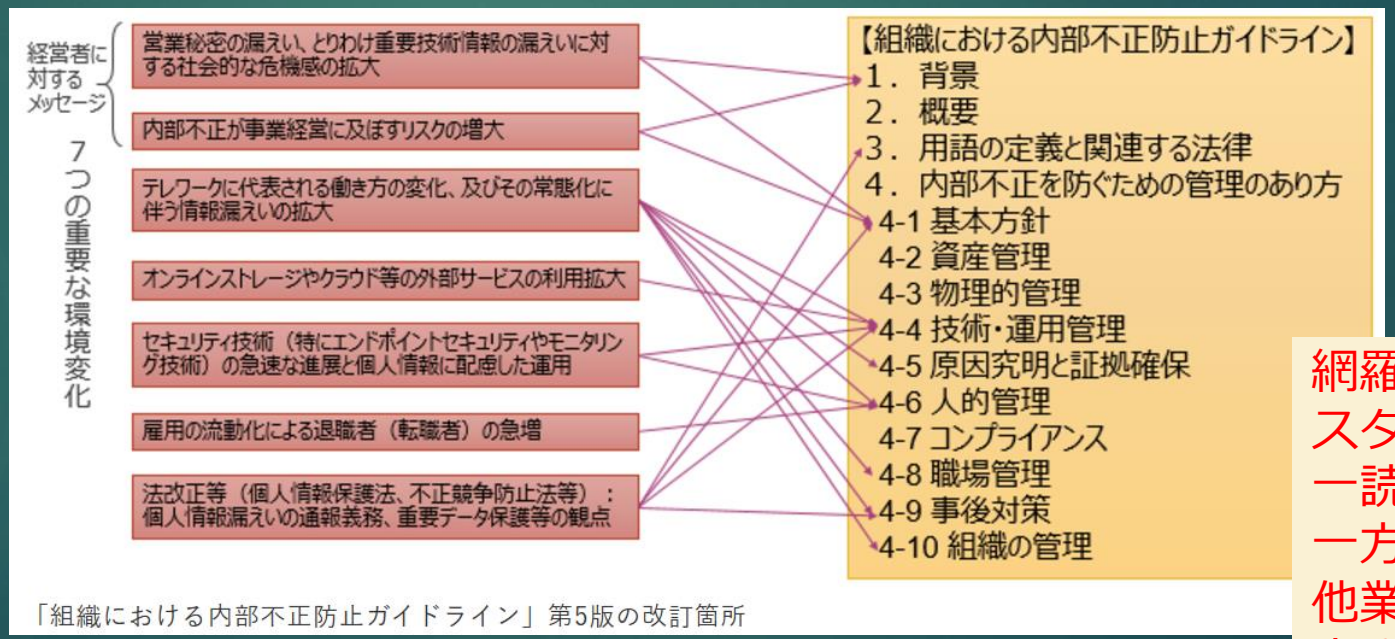
順位	組織
1位	ランサムウェアによる被害
2位	サプライチェーンの弱点を悪用した攻撃
3位	標的型攻撃による機密情報の窃取
4位	内部不正による情報漏えい
5位	テレワーク等の ニューノーマルな働き方を狙った攻撃
6位	修正プログラムの公開前を狙う攻撃 （ゼロデイ攻撃）
7位	ビジネスメール詐欺による金銭被害
8位	脆弱性対策情報の公開に伴う悪用増加
9位	不注意による情報漏えい等の被害
10位	犯罪のビジネス化 （アンダーグラウンドサービス）

社会的影響は大きい
標的型攻撃と同程度

IPA「組織における内部不正防止ガイドライン」

組織内部者の不正による顧客情報や製品情報などの漏えいは事業の根幹を揺るがすインシデントであり、内部不正が発生するリスクの把握や効果的な対策の検討は、組織にとって喫緊の課題です。IPAでは、このような背景から、企業やその他の組織において必要な内部不正対策を効果的に実施可能とすることを目的として2013年に「組織における内部不正防止ガイドライン」を作成し、2022年4月に改訂版第5版を公開しました

https://www.ipa.go.jp/security/guide/insider.html



網羅的に書かれている
スタンダードとして
一読したい
一方で、金融機関は
他業種とはリスクが
大きく異なる

今年話題の内部不正

- 2024年3月20日の報道によると、大谷翔平選手の銀行口座から少なくとも450万ドルが不正送金された
- この話をアイスブレイクにしたくて、年内に講演しています
- 違法賭博（スポーツ賭博）
- かけがえのないパートナーとして、大きな権限を手に入れていた
- 大金（あぶく銭）を手にした人の多くは、ギャンブルにのめり込む
  （羽振りが良くなった人を、反社は決して見逃さない、囁く）
- 事件が過ぎ去れば、通訳は替えが効く存在だった
- 一平ちゃんは必要じゃなかった、過大評価だった

＜対策＞長く担当させると不正を招く、人事ローテーション！
高い権限を付与する時は、監視、牽制もセットで！

内部不正で報道された事例

- 内部不正の報道の多くは、金融機関や大企業
- 社会の信用を預かる金融機関、大企業は信用失墜するし、社会的制裁の意味合いがある
  （報償責任主義、稼いでいる＝商品やサービスに責任がある）
- 着服、横領が多い、だいたい1億～20億円
  利率の良い金融商品があると嘘をつき、直接、お金を預かる
- 還流取引、キックバック
- 機密情報の持ち出しは、大きく2種類
  - 個人情報（名簿）の持ち出し、売却（西の電話屋さん）
  - 経営に関わる重要機密の持ち出し、不正競争防止法違反（お寿司屋さん）
- 不正会計の話は企業統治、J-SOXで伺ってください

金融機関の着服、横領の手口

- 「一般に公開していない、特別に利率の良い金融商品があります」
- 「一口 500万円、預けていただければ、月利3%の利子が付きます」
- 1回で預かれる額が大きい、出張費を経理でちょろまかすのとは、スケールが違う
- 昔からの手口
- 金額が大きい場合、顔が広く契約を集めるのは営業として優秀で、社内で表彰とか、特別な役職をもらっていることが多い

主な対策（着服、横領）

- 2005年、兵庫県の某銀行員が顧客の預金を9億円以上着服していたことが切っ掛け、FRIDAYなどで話題になり、行政処分が出ました
- 事件後、銀行業界は夏期休暇を5日間取得、土日を連続して、9連休を取得しないといけなくなった
- お客さんが「私の預金、どうなっています？」と営業店に聞きに来た時に、着服していた職員が不在だと、発覚する
- 当初は休暇扱いで出社し仕事をしていた管理職が多かったが、金融庁に大変厳しく指導されて、銀行業界では厳格に守られている
- 同じ営業職員が長く担当しないよう、担当者や支店は定期的に人事異動でローテーションするようになった

主な対策（着服、横領）

- 2005年、兵庫県の某銀行員が顧客の預金を9億円以上着服していたことが切っ掛け、FRIDAYなどで話題になり、行政処分が出ました
- 事件後、銀行業界は夏期休暇を5日間取得、土日を連続して、9連休を取得しないといけなくなった
- お客さんが「私の預金、どうなっています？」と営業店に聞きに来た時に、着服していた職員が不在だと、発覚する
- 当初は休暇扱いで出社し仕事をしていた管理職が多かったが、金融庁に大変厳しく指導されて、銀行業界では厳格に守られている
- 同じ営業職員が長く担当しないよう、担当者や支店は定期的に人事異動でローテーションするようになった

主な対策（機密情報の持ち出し）

- 個人情報の持ち出しについては、USBメモリ使用を禁止したり、外部送信メールはBcc強制とか、上席承認が必要だったり
- HDD暗号化、DLP（Data Loss Prevention）の導入や、CASBによるクラウドでの出入りの監視
- 機密情報へのアクセスは、認証強化により対策できる
- しかし、正当な権限を有する役職員からのアクセスは、退職前に急にアクセスが増えるとか、夜間に大量に印刷しているとか、監視しても極端なケースしか検出できない

動機、人の欲望

キリスト教には、「７つの大罪」という区分がある傲慢

傲慢　**俺こそが社長に相応しい**（お寿司屋さん）
大谷翔平は俺を必要としている

強欲　高級マンション、高級車、高級腕時計、宝石

嫉妬　同期と比べて**出世が遅れた**、俺の給料は安い

憤怒　過度のノルマ、処遇への不満

色欲　**異性への情熱**
（2001年 青森県＊＊公社 14億5,900万円　ア＊ータ）
（2009年 大手証券　キャバクラ通い、全顧客148万人分、損害は70億円以上）

暴食　高級寿司や高級ワイン

怠惰　働かずに儲けたい、**ギャンブル**

「ロマンス」と「ギャップ」は不正のトリガー

ロマンス

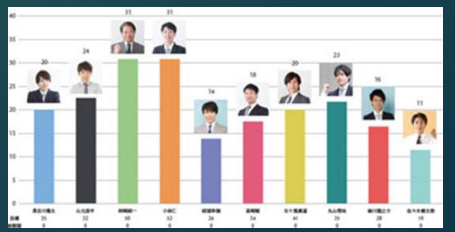
- Bigになりたい、フェラーリを所有したい
- 一昔前だと、愛人を囲う（歴史上の偉人）


ギャップ

- 俺はもっと凄い奴だ、社会は、会社は、俺を評価していない
- 理想と現実のギャップを何としても埋めようとする
- 脳が一度快感を覚えてしまったら、それは薬物中毒に近い、自分の意志では簡単に止められない、ギャンブル依存症
- フェラーリを買ったら、より猛烈にもう1台フェラーリが欲しくなる、不正を途中で自分から止めること、降りることは出来ない

内部不正の動機（憤怒、不満、嫉妬）

- 過度のノルマや、営業成績を競争させるようなことをしてはいけない
- 10人に順位を付ければ、必ず成績トップがいれば、10番目のビリも発生する
- 数字は公正 → 数字だけの評価が真実を見えにくくする
- 不本意な異動、人事評定、必ず発生する一部の不満を抑え込むためにも、微かな希望を持たせるローテーションが必要
- 会社の統合、合併時は要注意（大手証券のケースが該当）



内部不正を生み出す環境（機会）

- 不正を行うことが出来る職場環境
- 一人で作業が完結する、記録が残らない、誰もチェックしない
- 一人の担当者に長く任せっきり
- 本社から距離的に離れている
- 誰も見に来ない、チェックしない、点検しない
- 上司が長期にわたり不在
- 管理部門や監査部門が機能していない

内部不正の心理的ハードル（正当化）

- 窃盗や詐欺と比べて、犯罪の心理的ハードルが低い
- 横領に気づかなければ、誰も不幸にはならないと考えている
- 発覚しないように、毎日出勤し、（着服した）顧客へのケアも怠らないので、職場で信頼を得ていたりする（自分は悪い奴じゃない）
- 機密情報の持ち出しは、持ち出しそのものが発覚しなければ、数字上は殆ど分からない、バレなければ罪の意識は殆ど無い
- 誰だって、少しくらいの嘘を付いて生きているんだ（という言い訳）

内部不正の先に、組織あり

- 個人情報（名簿）が高く売れるということは、名簿を使ったビジネスが活況ということ
- 個人情報の買取価格は、数年前より高騰している
- 不正に持ち出された名簿だと分かっていて、買い取る業者、その業者から名簿を買う企業がたくさんいる
- 不正に入手した名簿を利用したマーケティングに正当性など無い
- 一平ちゃんや、某製紙会社で起きたバカラ賭博など、賭けの負け金をきっちり回収する組織がある

対応がちょっと難しいケース①

- 機密性の為に暗号化すると、後から査閲が困難になる
- メール添付ファイルに、当事者同士でパスワードをかけるケース、特に取引先のポリシーに従う時、このパスワードは担当者しか分からない
- 役員のメールは、誰が査閲するのが適切か？
- 機密性（暗号化やアクセス権限の厳格化）が、内部不正の発見を遅らせる

対応がちょっと難しいケース②

- Type-C USBがノートPCの電源ケーブルとして使われて、USBポートを封じるのが難しくなった
- メールに加え、LINEやショートメッセージなど、取引先、顧客との連絡方法が多岐に渡り、監視や制限（添付ファイルやスクリーンショット）が難しい
- 内線電話が無くなり、スマホを使っていると、私物持ち込みが分かりにくい
- テレワークや、座席のフリーアドレス化、外部委託や派遣から、事務フロアでどこの誰が働いているのか、顔も名前も分からなくなった
  → 誰か分からないなら、内部不正（持ち出し）しても気が付かないだろう

防ぎ方

動機
人事の適正な評価、これは業績評価、能力評価を数字だけでやってしまうと、数字だけを合わせようとして逆効果、部下の管理は上司の仕事

機会
ログが残せる、IT化で抜き打ち監査もやり易い、大量データの持ち出しはログで発見できる

正当化
公務員や銀行員はコンプライアンス研修が必須カルチャー、不正を行った際どう処分されるか、最初に理解させている

- 内部不正をやりにくくする環境 = ITは、ゼロトラスト
  内部不正を発生させにくい人の信頼 = 人は、トラスト

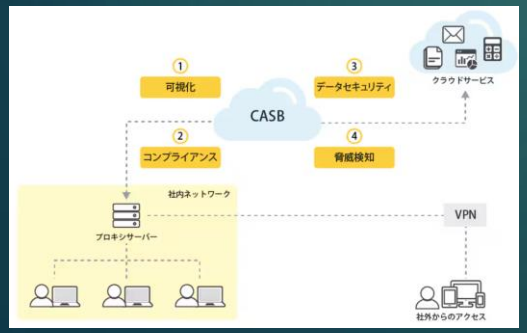
対策いろいろ

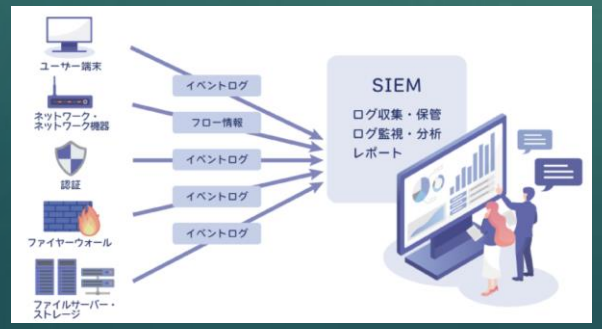
①アクセス権管理

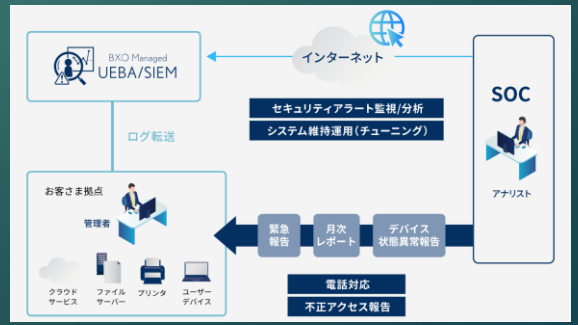
ActiveDirectoryで、セキュリティポリシーを設定しやすくなった
人材の流動化、外部委託先や派遣、出向から、所属が複雑化

②持ち出し困難化

ペーパーレス化、プリンタでの印刷も画像ログで証拠を残せる
クラウドの出入りは旧来はSSLで監視しづらかったが、CASBでPC側に
エージェントをインストールすることで監視、管理できる
委託先も派遣も出向も、所属元への業務報告や勤怠をクラウド経由で行うので、
やっぱりクラウドの監視、管理は難しい
PCはEDRとかエージェントだらけ、思ったようには監視、管理できない







対策いろいろ

③ログの記録

SIEMでPCの操作ログやファイルサーバへのアクセスを統合監視、さらにUEBAなら振舞検知も可能

ログだけで内部不正への対応は困難、やはり未然防止が重要 → ④

④ルール化と周知徹底

USBメモリ使用禁止、事務フロアへの私物持ち込み禁止には、クリアバッグ

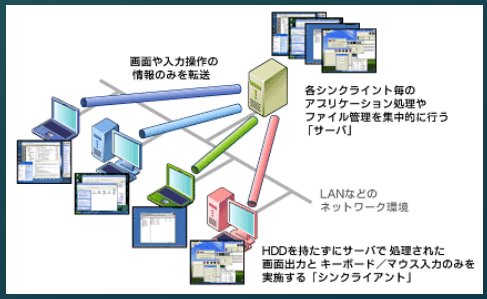
データセンターは徹底しやすいが、多種の業務を行うフロアに一律ルールは困難

禁止ルールが多いと、ファイル授受が必要な業務が非常に面倒になる（監査も）

⑤職場環境の整備

デスクトップ仮想化（VDI、Daas）により、PCのローカルへのデータ保存を禁止できる、データ、ファイルの出入りもログ記録、監視できる

システム環境の構築も、人の信頼の向上も、時間がかかる



まとめ

- 「今、内部不正の脅威が高まっています」
- というのは営業トークです、昔から脅威は高い
- ヒトが集団生活を始めた時から脅威は高い、ニホンザルの群れにも内部不正（餌のちょろまかし）はある
- ソリューションで解決できる話じゃなくて、解決しにくい困難な問題だと、最初に理解する
- そうしないと、「内部不正は簡単に防げるんだ」とワクワクした役員の理想と、なかなか徹底できない困難とのギャップに苦しむことになる