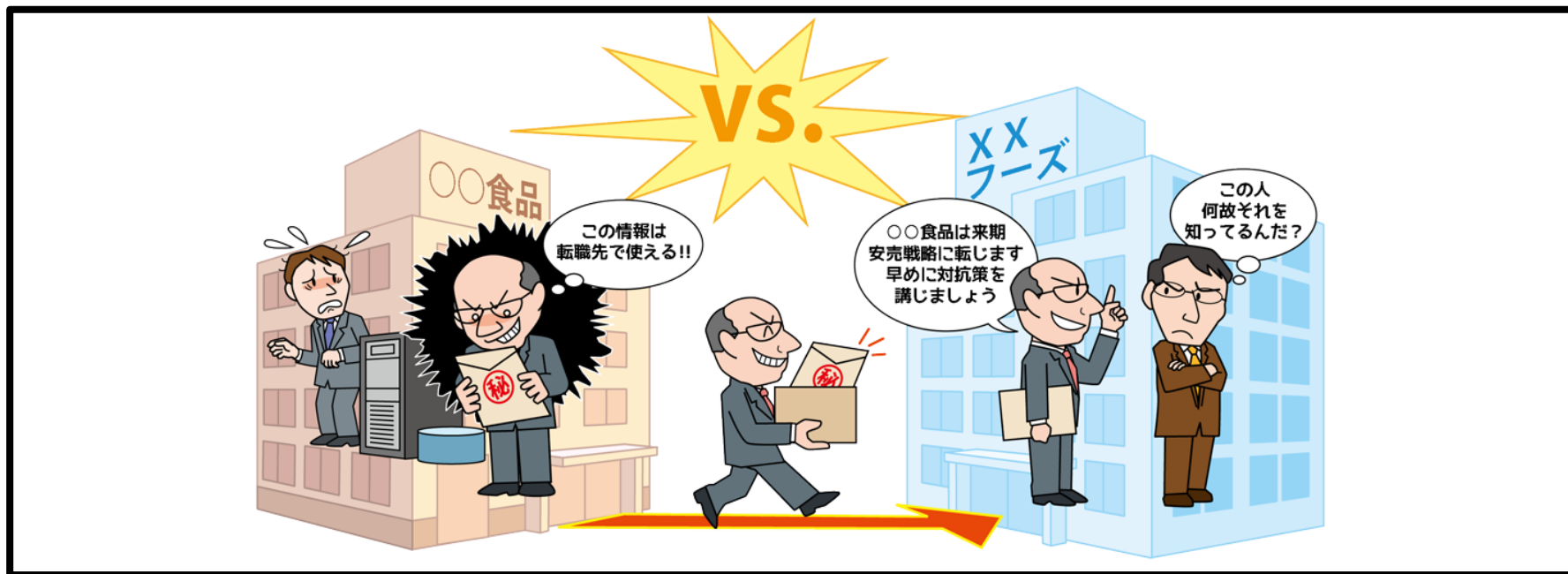


【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～



- 組織の従業員や元従業員等による機密情報の漏えい
- 組織関係者による不正行為による、組織の社会的信用の失墜、損害賠償による経済的損失
- 不正に取得した情報を他組織に持ち込んだ場合、その組織も損害賠償等の対象になるおそれがある

【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

● 攻撃手口

- ・内部の従業員は重要情報にアクセスしやすい
- ・悪意をもって情報を外部に提供してしまう

■ アクセス権限の悪用

- ・付与されたパスワードを悪用し、組織の重要情報を取得
- ・必要以上のアクセス権限を付与していると被害が大きくなる

■ 在職中に割り当てられたアカウントの悪用

- ・在職中に使用していたアカウントを使って不正に情報を取得

■ 内部情報の不正な持ち出し

- ・USBメモリー、HDD、メール、クラウドストレージ、
スマホカメラ、紙媒体等での持ち出し



【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

● 2022年の事例／傾向①

■ 市立高校で成績流出、内部犯行の可能性^(※1)

- ・2022年7月、市立高校に通う生徒3人の成績等の**個人情報**がInstagramに投稿され、約90人に閲覧されていた
- ・何者かが**教員のIDとパスワードを用いて**生徒の成績等を管理している学習支援ソフトにアクセスし、情報を入手したとみられている
- ・生徒用のタブレット端末で学習支援ソフトにアクセスしていたケースがあり、**その端末では誰でも個人情報を閲覧できる状態**になっていた

【出典】

※1 市立函館高校で模試成績など流出・SNS掲載 部内者の仕業か（NHK NEWS WEB）

<https://www3.nhk.or.jp/sapporo-news/20220722/7000048853.html>

【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

● 2022年の事例／傾向②

■ 寿司チェーン社長、転職先に営業秘密持出し^(※1)

- ・2022年9月、カッパ・クリエイトの社長が**不正競争防止法違反**の疑いで警視庁に**逮捕**された
- ・同社長は2020年11月に**ライバル企業**から**転職**しており、元部下を利用して商品原価等の**営業秘密**を持ち出していた
- ・転職先の商品企画部長は**データを不正利用した**として、転職元の元部下はデータの**パスワードを漏えいした**として**共に逮捕**された

【出典】

※1 かっぱ寿司運営会社社長ら逮捕 不正競争防止法違反容疑 警視庁（NHK NEWS WEB）

<https://www3.nhk.or.jp/news/html/20220930/k10013843141000.html>

【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

● 対策

■ 経営者、管理者

・被害の予防①

-基本方針の策定

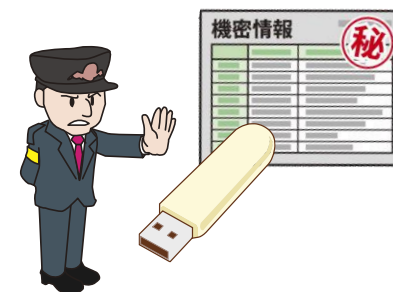
情報取扱**ポリシー**の作成、内部不正者に対する**懲戒処分等**を規定した**就業規則等**を整備する

-資産の把握、対応体制の整備

重要資産を**把握**し、その**重要度**を**ランク付け**した上で重要情報の**管理者**を定める

-重要情報の管理、保護

- 重要情報の利用者IDおよびアクセス権の**登録・変更・削除に関する手順**を定めて運用する
- 従業員の異動や離職に伴い不要となった利用者ID等は**直ちに削除**する
- それらの適切な管理、**定期的な監査**を実施する
- 利用者IDの共用禁止等の処置、DLP等のツールの導入を検討する



【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

● 対策

■ 経営者、管理者

・被害の予防②

－物理的管理の実施

- －重要情報の**格納場所**や執務室への**入退室管理**
- －記録媒体の**利用制限**、**持ち出し/持ち込みの管理**
- －記録媒体の廃棄時には適切な**データ消去の運用**を実施
- －消去できない場合は媒体の物理的な破壊も検討
- －リース品は**初期化**してから返却 等



【4位】内部不正による情報漏えい

～不正に情報を取得しない、取得させない、使用しない！～

● 対策

■ 経営者、管理者

・情報リテラシーや情報モラルの向上

－人的管理およびコンプライアンス教育の徹底

・攻撃の予兆／被害の早期検知

－システム操作履歴の監視

重要情報へのアクセス履歴や利用者の操作履歴等の**ログ、証跡を記録し、監視**する
さらに、監視していることを**従業員に周知**する

・被害を受けた後の対応

－組織の方針に従い各所へ**報告、相談**する

※上司、CSIRT、関係組織、公的機関等

－影響調査および原因の追究、対策の強化

－内部不正者に対する適切な**処罰の実施**

