内部不正防止への取り組み
～「組織における内部不正防止ガイドライン」の紹介～

2014年1月29日

独立行政法人**情報処理推進機構**
技術本部 セキュリティセンター

はじめに

- 「組織おける内部不正防止ガイドライン」
  - 公開　2013年3月（英語版2013年9月)
  - http://www.ipa.go.jp/security/fy24/reports/insider/index.html

- 本日の内容
  - ガイドラインの概要　（背景、目的、構成）
  - ガイドラインの使い方

問い合わせ先: isec-economics@ipa.go.jp

背景
～ 内部不正の実態 ～

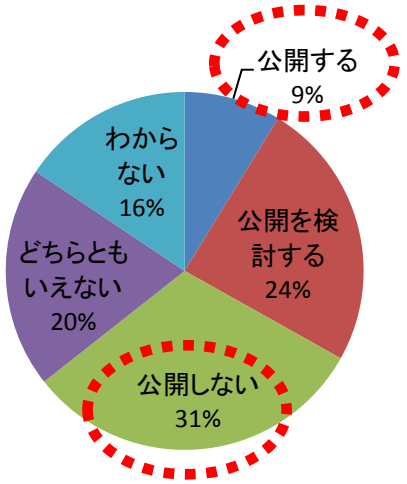
- 組織の**事業の根幹を脅かす**事件が報道されている。
  しかし、事件は一般的に組織内で処理されるため、**氷山の一角**

- 情報セキュリティの隠れた問題（**情報を公開したくない**）
  - 風評被害が発生する恐れや関係者との調整がつかない等から情報が公開されない
  - 組織間での情報共有が難しく、全体概要をつかむことが難しい

Q 有益な対策を検討する事例として**情報を公開する可能性**はありますか？

届出を行う公的または**中立的な機関**が「個人や企業名等が特定できない状態での公開」をすることで**関係者から合意が得られた**場合

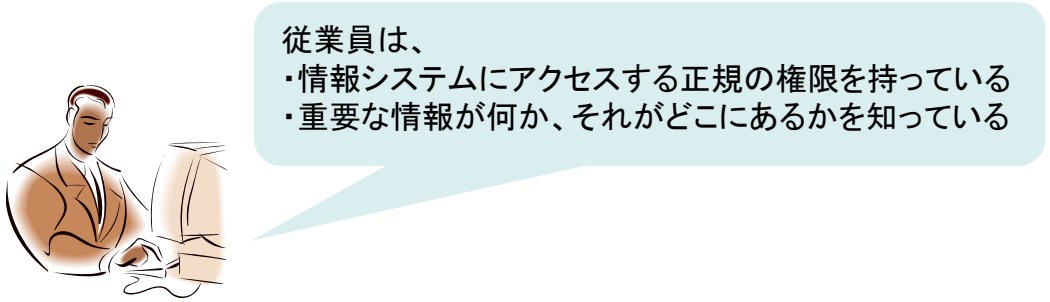
（経営者、管理者を対象としたアンケート調査より）



背景
～ 内部不正の実態 ～

- 事件の特徴
  - ビジネス上有用なノウハウや技術等の営業秘密の漏洩ルートのほとんどが従業員からの漏洩
    （経済産業省「営業秘密の管理実態に関するアンケート調査」調査結果（確定版）より）
  - 「外部からの攻撃」と比較すると、平均して1件あたりの個人情報の漏洩数が多い
    （JNSA「情報セキュリティインシデントに関する調査報告書～個人情報漏えい編～」より）

- それぞれの組織で、経験等をもとに個別に対応している
  - 情報共有が困難なため、組織を越えた対策検討が難しい



ガイドラインの目的

- 内部不正によるインシデント発生を防止するための環境整備に役立てて頂くためのガイドライン
- これまで 内部不正対策を「考えてこなかった」「何をすればよいかわからなかった」という企業も考慮した内容
  （特に中小企業に重きをおいている）
- 内部不正防止だけでなく、発生してしまった際の早期発見・拡大防止にも対応した環境整備を推進

ガイドラインの構成

1章　背景
内部不正の実態、ガイドラインの目的

2章　概要
ガイドラインの構成と活用方法、 体制構築

3章　用語の定義と関連する法律
内部不正等の用語定義と関連する法律概要

4章　内部不正のための管理の在り方
10の観点から対策項目（30項目）を提示

後で例示

4-1. 基本方針 (2項目)
4-2. 資産管理 (5項目)
4-3. 物理的管理 (4項目)
4-4. 技術的管理 (5項目)
4-5. 証拠確保 (2項目)
4-6. 人的管理 (3項目)
4-7. コンプライアンス (2項目)
4-8. 職場環境 (3項目)
4-9. 事後対策 (2項目)
4-10. 組織の管理 (2項目)

付録Ⅰ　内部不正事例集
実際に発生した17の内部不正事例

付録Ⅱ　チェックシート
現状を把握するためのチェックシート

付録Ⅲ　Q&A集
対策内容を補足するためのQ&A

付録Ⅳ　他のガイドライン等との関係
他のセキュリティとの対応、差分

付録Ⅴ　基本方針の記述例
基本方針の雛形

(特徴)
アンケート調査から分析

各項目に対応する具体的なソリューション
→ 内部不正対策ソリューションガイド

用語の定義
～ 内部者と内部不正の定義 ～

- **内部者**
  - 役員、従業員及び契約社員等の社員に準ずるもの（以下、総称して「役職員」という。）又は、元役職員であった者のうち、以下の2つのどちらかでも満たした者とする
    - 組織の情報システムや情報に対して直接又はネットワークを介したアクセス権限を有する者
    - 物理的にアクセスしうる職務についている者（清掃員や警備員等を除く）
- **内部不正**
  - 不正の芽を摘むという意味から、違法行為だけでなく、情報セキュリティに関する内部規程違反等の不正行為も含める
  - 内部不正の行為としては、顧客名簿や技術ノウハウ等の重要情報や情報システム等の情報資産の窃取、持ち出し、漏洩、消去・破壊等を対象とする
  - 元役職員が退職後に在職中に得ていた情報を漏洩する行為などについても、内部不正として取り扱う

ガイドラインの使い方

ステップ1

チェックシートで、30項目の対策状況を確認

ステップ2

各項目の対策を3段階の流れで検討

①「対策の指針」：チェックシートの項目

②「どのようなリスクがあるか」：対策の必要性を理解

③「対策のポイント」：具体的な対策に落とし込むヒント

ステップ1　内部不正チェックシート
～ チェックシートで現状を把握 ～

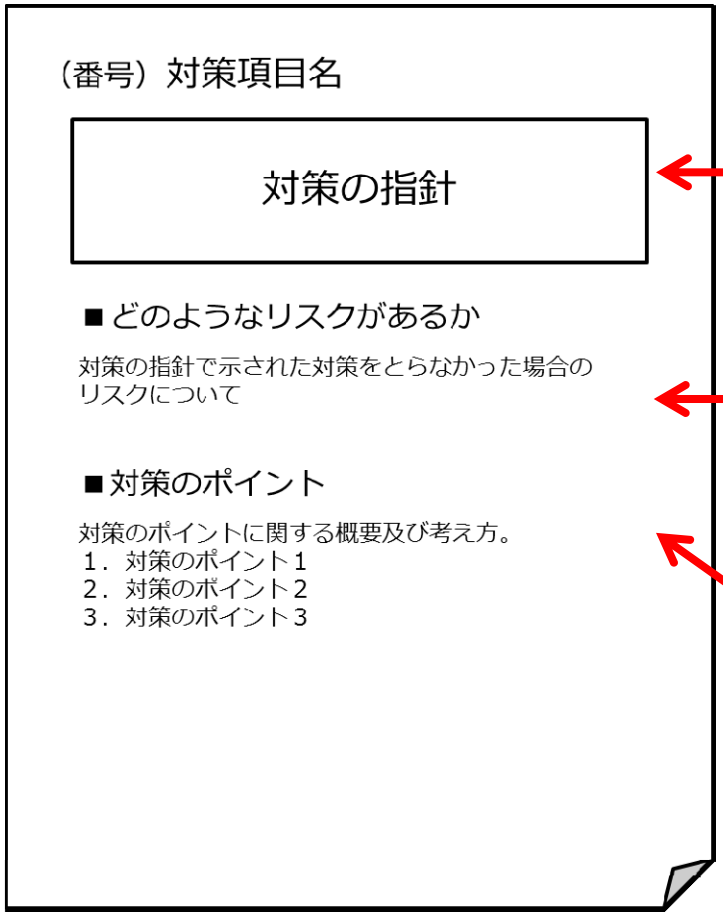
※ □：主担当/実施部門、[ ]：サポート/実施補助・確認部門

No	内容	チェック欄				
4-1．基本方針						
(1)	内部不正の対策が経営者の責任であることを組織内外に示す「基本方針」を策定し、役職員に周知徹底していますか？	□：経営者（最高責任者）				
(2)-①	経営者は、内部不正対策の総括責任者の任命及び管理体制と実施策の承認を行っていますか？ （ただし、経営者が組織全体に目が届く組織であれば、自ら内部不正対策の実施にあたり、管理体制を必ずしも構築する必要はありません。）	□：経営者（最高責任者）				
⋮						
4-7．コンプライアンス						
(22)	就業規則等の内部規程を整備し、正式な懲戒手続を備えていますか？	□		[ ]	[ ]	[ ]
(23)	内部者に対して重要情報を保護する義務があることを理解させるために「秘密保持誓約書」等を要請していますか？	□		[ ]	[ ]	[ ]

30の対策項目に対応

各項目に関係する部門を示している

ステップ2　対策検討
～ 3段階で検討～



①「対策の指針」を読んで、対策の概要を捉える。

②「どのようなリスクがあるか」を読んで、対策しない場合のリスクを知る。
インシデントが発生した場合の事業に与える影響を考える。
事業に与える影響が小さく、リスクを許容できると判断すれば、必ずしも対策する必要はない。

③②の事業に与える影響から、「対策のポイント」を読んでコストやリソース等を考慮し具体的な実施策を立案する。
「付録Ⅲ：Q&A集」や「付録Ⅳ：他のガイドラインとの関係」JNSAソリューションガイドを参考。

※ 社会背景や企業規模等によって、②の許容可能なリスクが変化する ことから、
③で立案した具体的な実施策を定期的に見直すことが望ましい。

対策例1　4-1 基本方針
(1)経営者の責任の明確化

内部不正対策は経営者の責任であり、経営者は基本となる方針を組織内外に示す「基本方針」を策定し、役職員に周知徹底しなければならない。　←①対策の指針

■どのようなリスクがあるか？　←②どのようなリスクがあるか

経営者のリーダーシップにより「基本方針」を策定しないと、社内外における経営責任の所在があいまいになり、実効性のある管理体制の整備が困難となります。また、「基本方針」は経営者の内部不正防止に向けた意志を伝えるものでもあり、策定しないと経営者の意志が役職員に伝わらず、具体的な対策を立てることや役職員に内部不正対策を周知徹底することが困難になります。

■対策のポイント　←③対策のポイント

経営者は、内部不正対策の大枠となる基本方針を策定し、内部不正対策の方向づけを行わなければなりません。経営者は対策を実効性のあるものとするために実施状況をモニタリング 、評価することによって基本方針を定期的に見直していきます。

1. 経営者が内部不正対策の方向づけ、モニタリング、評価に関与して組織内外において責任を持ちます。
2. 本ガイドライン等を参考にし、基本方針を策定(Q&A1:P65)します。
3. 組織が保護すべき重要な情報（重要情報）を定めます。
4. 策定した基本方針に照らし合わせ、役職員に内部不正対策を教育等によって周知徹底します。

より具体的な内容を知りたい場合に参照

対策例1　4-1 基本方針
(補足) 付録Ⅲ：Q&A集

- より具体的な対策内容をQ&Aで補足

対策のヒントとなるQ&A（1）

Q-1基本方針をどのように策定すればよいかわかりません。(4-1(1))
A-1本ガイドラインの示す基本方針は、既存の情報セキュリティ基本方針を利用すること想定しています。必要ならば、内部不正対策に関する事項を追記すればよいと考えています。しかし、情報セキュリティ基本方針を策定していない組織も考えられるため、そのような組織を対象に最低限の内容を示します。 基本方針では、社内での重要情報の保護・管理の徹底、及び社外への説明責任の観点から以下の3項目を最低限定めてください。 ①経営者は経営課題の一つとして、リスク管理を行う必要があることを認識し、その一環として内部不正を防止し、重要情報を保護・管理することの重要性を示します。 ②保護・管理すべき重要情報を示し、その重要情報に関して事業上の重要性を示します。重要情報とは、企業及び団体の事業に大きな影響を与える情報です。例としては、戦略的な情報及び公開されていない知的財産を含む製造・開発情報や営業情報等です。また、秘密管理を行うことが義務付けされた関係者から ・ ・ ・

対策例2　4-5 証拠保全
（17）情報システムにおけるログ・証跡の記録と保存

内部不正の早期発見及び（27）の事後対策の影響範囲の観点から、重要情報へのアクセス履歴及び利用者の操作履歴等のログ・証跡を記録し、定めた期間に安全に保存することが望ましい。

■どのようなリスクがあるか？

ログ・証跡を記録していないと、ログ・証跡から不正行為の前兆となる行為を知ることができないため、発見の遅れや、発見時に被害が大きくなっているといった恐れがあります。

また、ログ・証跡が保存されていないと、内部不正が発生した場合に（27）に述べる事後対応において、内部不正の原因特定及び内部不正者の追跡、影響範囲等の調査が困難になります。また、ログ・証跡が安全に保存されていないと、（22）に述べる処罰等の根拠として認められない場合があります。

関連項目を参照して、対策検討で不足が生じないように考慮

■対策のポイント

内部不正の早期発見及び事後対策の観点から、以下のようにログ・証跡を記録して安全に保存します。

1. ログは、重要情報へのアクセス履歴や、利用者の操作履歴（Webのアクセスログやメールの送受信履歴等）等を取得します。
2. 証跡は、設定したポリシーに応じて、上記のログ以外の日時、利用者、操作端末、操作内容、送受信の内容等の情報を取得します。

・
・
・

対策例2　4-5 証拠保全
（関連項目）4-7 コンプライアンス

(22)法的手続きの整備

内部不正を犯した内部者に対する解雇等の懲戒処分を考慮し、就業規則等の内部規程を整備して、正式な懲戒手続に備えなければならない。

■どのようなリスクがあるか？

内部不正を犯した内部者に対する懲戒処分を就業規則等の内部規程に盛り込まれてない場合や正式な懲戒手続きが整備されていない場合には、内部者から不当処分の訴えにより懲戒処分が無効となる恐れがあります。

■対策のポイント

懲戒処分を行なう場合には、内部規程において懲戒処分及び秘密保持義務に関する項目を定めておくことが必要です。

1. 内部規程には、懲戒処分の対象となる内部不正（例：営業秘密の侵害、個人情報の目的外利用等）に関する記載が必要です。
2. 内部規程には、秘密保持義務の対象となる重要情報を客観的に特定できる記載が必要です。
3. 解雇等の懲戒処分は、根拠となる内部規程に基づき、かつ労働法制を遵守して処分を行なう必要があります。
4. 適切な懲戒処分を決定するために、査問委員会等によって事実関係を明らかにする必要があります。

(17)証拠保全対策が必要

対策例2　4-5 証拠保全
（関連項目）4-9 事後対策

(27)事後対策に求められる体制の整備

内部不正の影響範囲を特定するために、事象の具体的状況を把握するとともに、被害の最小化策や影響の拡大防止策を実施しなければならない。また、必要に応じて組織内外の関係者との連携体制を確保しなければならない。

■どのようなリスクがあるか？

内部不正の影響範囲を特定できないと、迅速な事後対策が施せないだけではなく、法的処置等の対応を検討できなくなる可能性もあります。さらに、内部不正の調査や対処について第三者サービス（デジタル・フォレンジック 解析やインシデン対応 支援等）を利用する際に必要となる情報や伝達方法を取り決めておかない場合には、適切なサービスを受けられない恐れがあります。

■対策のポイント

事後対策に求められる体制を構築するためには、以下のような内容を整備する必要があります。

1. 内部不正による被害の最小化、及び影響の拡大を防止にするために、求められる対応手順や報告手順等を事前に取り決めておく必要があります。内部不正の具体的な状況を把握し、影響範囲を調査するためには、「いつ、誰が、何をしたのか」に関する検証可能な証拠 を保全する必要があります。

(17)証拠保全対策が必要

対策例3　4-8 職場環境
（25）適正な労働環境及びコミュニケーションの推進

本ガイドラインの特徴：権限を持つ者が不正行為を行わない環境作りについて

業務量及び労働時間の適正化等の健全な労働環境を整備するとともに、業務支援を推進する体制や相談しやすい環境を整える等の職場内において良好なコミュニケーションがとれる環境を組織全体で推進することが望ましい。

■どのようなリスクがあるか？

業務量及び労働時間が健全な労働環境が整備されていないと、特定の従業員の業務量が過大になり、それを解消するために負荷軽減や作業時間短縮を目的とする内部不正を行う可能性があります。また、業務遂行が困難になると従業員の不満が高まることで内部不正への誘因になります。また、相談しやすい環境等の良好なコミュニケーションが十分でない場合には、業務への悩みやストレスを抱えた状態での作業が続くことにより、内部不正が発生する恐れもあります。

■対策のポイント

職場環境や労働環境の整備においては、総務部門や総務担当者が主体となり、業務量や労働時間等を適正化する必要があります。また、相談しやすい環境を整備し、職場の信頼関係に配慮するとともに、業務の支援や上司や同僚との良好なコミュニケーションがとれる環境を推進する必要があります。

1．特定の従業員が休暇取得できない状態や長時間残業が継続している状態のように、極端に業務負荷が高い場合には、業務量や労働時間を適正な範囲にする必要があります。

・
・
・

ご清聴ありがとうございました

IPA

＜PR＞

http://www.jitec.ipa.go.jp/ip/