ISGA
Information Security Governance Association

情報セキュリティガバナンス協議会
2014 年度　ワーキンググループ２
最終報告書

内部犯行問題に関する検討

2015年7月

目次

1. 背景・目的

■ 背景・目的

企業の情報・ITを巡る深刻な脅威としては、サイバー攻撃や災害、さらに内部犯行が挙げられる。特に内部犯行については、実効的な対策が乏しく、発生した際の被害規模が大きい点で深刻である。たとえば、2014年7月9日に発覚した、通信教育大手のベネッセコーポレーションの顧客情報が流出した問題では、子会社の再委託先が雇った派遣社員がデータを持ち出した疑いがかけられている。

そこで、本WGでは、内部者（グループ企業、委託先を含む）の犯行をどのように防ぐべきか、技術的対策の要否や教育・モラル形成のあり方等について検討を行う。

2.検討 メンバー

■ 検討メンバー　（社名：五十音順　氏名：敬称略）

グローバルセキュリティエキスパート株式会社	多山　信彦
株式会社京王ITソリューションズ	加藤　良夫
株式会社ジェイティービー	戸田　磨
新日本有限責任監査法人	青波　久恵
積水化学工業株式会社	平尾　安明
株式会社高島屋	上原　佳都雄
	舛田　基城
デロイトトーマツリスクサービス株式会社	丸山　満彦
日本コムシス株式会社	森村　市郎
	井原　正人
	杉本　博之（～2014/10/31）
日本電気株式会社	甲田　輝彦
富士通株式会社	平野　秀幸
富士ゼロックス株式会社	杉森　祐司
（事務局）	
株式会社三菱総合研究所	川口　修司
株式会社三菱総合研究所	綿谷　謙吾
株式会社三菱総合研究所	江連　三香（～2014/12/9）

3.検討経緯

■ 会合

第1回	8/ 29(金)	自己紹介、内容・進め方の検討、スケジュール
第2回	9/19(金)	課題意識の共有
第3回	10/16(木)	アウトプット、今後の進め方に関する検討
第4回	11/20(木)	ご講演（IPA小松文子様） 「組織における内部不正の動向と防止策」
第5回	12/ 4(木)	議論、中間報告準備
本会合	12/15(月)	中間報告
第6回	1/22(木)	チェックリスト項目の作成
第7回	2/19(木)	チェックリスト項目の見直し、確認
第8回	3/10(火)	最終報告準備
本会合	3/18(水)	最終報告
第9回	4/9(木)	最終報告書とりまとめ

4. 検討内容①

■ 内部不正対策を議論するにあたり、企業・組織として守るべき情報の明確化、現状を把握する対象範囲について議論をおこなった

企業・組織として守るべき情報

- 内部不正という観点では、顧客/取引先の個人情報は、管理レベル「高」
- 従業員の個人情報であっても、給与、能力評価、自己申告等の情報は管理レベル「高」
- 製造業の技術情報や営業活動にかかわる情報も含まれるのではないか

↓

今年度は個人情報・営業秘密を対象に整理し、企業・組織として守るべき情報を絞り込むための考え方を整理

現状把握対象

- 自社：役職員、ビジネスパートナー、パート、アルバイト
- グループ会社（国内）：業務内容、取り扱う情報、事業の規模等様々
- グループ会社（海外）：カルチャー、言語、地理的なギャップ等々管理上のハードルが高い
- 外部委託先/再委託先/再々委託先・・・現状把握をどのように実施するか。方法としては自己評価を依頼する、委託元自らがヒアリングを実施することなどが考えられる

↓

現状把握すべき対象は多岐にわたるため、様々な観点から対策を検討する必要がある

4. 検討内容②

■現状を把握する方法として、IPA「組織における内部不正防止ガイドライン」に着目し、ガイドライン及び内部不正チェックシートを参考に議論をおこなった。同ガイドラインは、内部不正防止の方法を5原則25分類（下表参照）の観点から整理しており、網羅的に対策を検討する上で有用と考えられる。

犯行を難しくする	捕まるリスクを高める	犯行の見返りを減らす	犯行の挑発を減らす	犯罪を容認する言い訳を許さない
1.犯行対象を防御的に強化する ・スクリーンロックの設定 ・アクセス制御の設定 ・退職者の ID 削除/確認者設置 ・パスワードポリシーの設定 ・PC の物理チェーンロック、固定具 ・盗用防止スクリーン	6.監視者を増やす ・複数人での作業環境の設定 ・防犯ベルの設置 ・特権階級の分散化/管理者の増員 ・個人情報売買の監視 ・アクセスログの監視	11.標的を隠す ・電子ファイルのアクセス権限の設定 ・PC/USB メモリの保管場所設定	16.欲求不満やストレスを減らす ・職場での円滑なコミュニケーションの推進 ・上司や同僚に頻繁に相談できる環境整備 ・適切な人事・作業管理（業務量の軽減）	21.規則を決める ・情報セキュリティポリシーの策定 ・個人情報管理策の作成 ・就業規則 ・障害対策等の手順の明確化 ・管理/運用策の策定 ・雇用契約
2.施設への出入を制限する ・ID カード（身分証明）の確認 ・電子カードアクセス ・手荷物検査	7.自然監視を補佐する ・守りやすい空間の設計（外部から見えるガラス面積の拡大） ・オフィスのフリースペース化 ・投書箱による密告者をサポートする	12.対象を排除する ・電子ファイルのアクセス権限の設定 ・PC の持込許可制度 ・業務上で必要な閲覧項目を絞る ・紙の廃棄/溶解処理	17.対立を避ける ・情報セキュリティの管理部門を設置し、上司との対立を避ける ・適切な人事・作業管理（業務量の軽減）	22.指示を掲示する ・情報セキュリティポリシーの掲示 ・個人情報管理策の掲示 ・就業規則の掲示 ・目的外利用の禁止の掲示 ・不正事例の掲示（匿名）
3.出口で検査をする ・ID カード（身分証明）の確認 ・手荷物検査 ・メールやネットの監視	8.匿名性を減らす ・ID カード、社員バッチの携帯 ・ID による管理 ・持ち出し台帳による管理	13.所有物を特定する ・PC/USB メモリに登録番号シールをつける ・電子ファイル/紙ファイルに管理番号をつける ・複写台帳管理	18.感情の高ぶりを抑える ・パワハラの禁止 ・人種的中傷の禁止 ・適切な人事・作業管理（業務量の軽減）	23.良心に警告する ・持ち出し厳禁であることを掲示 ・管理レベルを表示／印字 ・不正競争防止法などの研修・教育 ・ルール厳守への自己サイン
4.犯罪者をそらす ・通路／出入り口の閉鎖 ・物理レベルに応じた入退制限 ・金属探知器	9.現場管理者の利用 ・CCTV（監視カメラ）の設置 ・機密情報へのアクセスは複数人による作業制限	14.市場を阻止する ・不正競争防止法 ・不正監査/不正検査 ・個人情報売買の禁止/監視	19.仲間からの圧力を緩和する ・適切な人事・作業管理（業務量の軽減）	24.遵守を補佐する ・利用 PC/USB メモリの登録管理/貸出規則を簡単にする ・施錠保管キャビネットの設置 ・シュレッダーの設置 ・相談窓口の整備
5.道具や対抗手段を制御する ・非登録の PC/CD/USB メモリの持込/持出/書出し禁止 ・携帯電話の持ち込み禁止 ・メールやネットの利用制限・禁止（フィルタリング等）	10.フォーマルな監視体制を強化する ・侵入警報装置 ・警備員	15.利益を否定する ・重要情報の暗号化 ・重要情報にノイズや電子透かし各種ウォーターマークを注入	20.模倣犯を阻止する ・インシデントの手口の公開を慎重にする ・インシデントの証跡を残さない	25.薬物・アルコールを規制する ・職場での飲酒禁止/検査 ・アルコールなしの行事

（出所）IPA「組織内部者の不正行為によるインシデント調査」
※5原則25分類と内部不正ガイドラインの各項目の対応については、IPA「組織における内部不正防止ガイドライン」付録Ⅵを参照

4. 検討内容③

■ ガイドライン・チェックシートを基に議論した結果、内部不正チェックシートの「対策の指針」・「どのようなリスクがあるか」・「対策のポイント」等を読み込むことにより、リスクベースで実効性のある自己評価は可能であるが、下記の課題点・改善点があげられた

課題点・改善点

- 評価実施者が情報セキュリティの知識を十分持ち合わせていない場合は、正確な評価が難しい
- 実務レベルでは、IPA内部不正防止ガイドラインの「対策の指針」・「どのようなリスクがあるか」・「対策のポイント」等を読み込む時間的余裕がないため、正確な評価の実施が難しい
- 自己評価を行う場合は、その判断基準をわかりやすく定義する必要がある
- 上記自己評価結果の妥当性を第三者が判断できる枠組みが必要
- 外部委託先の評価は、委託先による自己評価の他、定期的に現場確認が効果的（整理整頓状況等）
- 関連会社/外部委託先等の教育/研修をどのようにするか
- 関連会社/外部委託先等の技術的対策に関わる費用負担をどうするか
- IPAガイドラインは情報セキュリティマネジメントシステム（ISMS）と異なり、職場環境の項目がある。内部不正防止のために、職場環境にフォーカスをあてた施策を検討する必要がある
- 内部不正対策の他サイバー攻撃対策による情報漏洩対策として、一歩踏み込んだ教育・研修を実施したほうがよい。社員の情報リテラシー教育や性善説から性悪説への意識改革が必要となる
- チェックリストを活用して現状把握し、遵守・実施できていない事項は、リスクベースで対応方針を検討し対策を実施するなど、PDCAの管理サイクルを定期的にまわす必要がある

IPA内部不正チェックリストをベースに、現場での具体的施策を明示し利用しやすいチェックリストを作成

5. 内部犯行対策チェックリスト

■ アウトプット：内部犯行対策チェックリスト（現場の具体的な対策に立脚したもの）
- IPA「組織における内部不正防止ガイドライン」のチェックリストを活用し、現場で利用しやすいものを作成
- 各項目の記載方針は下表のとおりである
- IPA「組織における内部不正防止ガイドライン」項目

1. 基本方針
2. 秘密指定、アクセス権指定
3. 物理的対策
4. 技術・運用管理
5. 証拠確保
6. 人的管理
7. コンプライアンス
8. 職場環境
9. 事後対策
10. 組織の管理

項目	IPAガイドラインの項目を転記
内容	IPAガイドラインより転記
具体的実施項目	IPAガイドラインより転記
事例/リスク	ワーキングループ参加企業の具体的な取り組みを記載
リスクの解説	対策が不十分な場合のリスクを具体的に記載
議論のポイント	ワーキンググループでの議論の内容を記載

5. 1 組織の管理体制

まとめ

組織の管理体制ではCCO（Chief　Compliance　Officer）やCLO（Chief Leagal　Officer）を設置する企業が増えている。しかし、形式的にCCOやCLOの設置をしても実効的な管理が出来る訳ではない。

CCOやCLOが機能するためには、以下のようなポイントが考えられる。

1. CCOやCLOの役割や権限、責任の明確化と社内周知。
2. CCOやCLOの方針を具体的な計画に落とし込み、実行可能な組織と紐付する。例えば、法務室長を役員登用してCCOとし、法務室を実行部隊として活用。
3. 役割を担う役員が関係分野に対する知見やノウハウを持っていること。
4. 関係する部署をメンバーとした委員会を作り、CCOやCLOの方針が関係部署に横展開できるようにする。
5. グループ会社がある場合は、グループ各社にもCCOやCLOを任命させ、本社と連動した活動を推進させる。
6. 会社評価や個人評価のコンプライアンス項目のウエイトを高くする。
7. CCOやCLOの名称を使用しない。CCOやCLOは他の意味でも略語として使用されており、従業員が同じ意味で認識しない可能性もある。誰もがわかる“読んで字の如く”がよい。

5. 1 組織の管理体制

項目	4-1. 基本方針（2）-①総括責任者の任命と管理体制の承認
内容	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。）
具体的実施項目	1.総括責任者には、事業を考慮した実効的で効率的な内部不正対策を実現するために情報セキュリティと経営を理解できる者を任命します。
事例/リスク	• 企業グループ全体の内部統制や監査に責任を持つCCO,CLOの任命。
リスクの解説	• 統括責任者が不明確な場合は、必要な予算や要員を割り当てることが困難となる。 • 業務横断的な管理ができず、組織として効果的な対策ができない。
議論のポイント	• CCO（コンプライアンス）、CLO（リーガル）を設置する企業が増えてきており、内部不正対策として必要な要素になってきている。 ＊例えば、監査は監査部、人的管理・職場環境管理は人事部、情報システムの管理はシステム部、情報管理は総務部等、縦割りの組織を横断的に取りまとめる責任者の任命。 • 各社がガバナンスに苦慮しているので、全体を管理する役員を設置することが重要である。 • CCO、CLOを設置するだけではなく、いかに機能させるかが重要である。 • 法務担当者等が役員になることで、コンプライアンスを重視する等社内に向けたメッセージにつながる可能性がある。 • 社内浸透を考えた場合名称も考慮したほうがよい。CLOよりも最高法務責任者の方が理解は進む可能性がある。

5. 2　異動・退職時の管理

まとめ

一般的に、異動や退職といった人事的な措置は、その対象となる者が望む結果と必ずしも一致しないことが考えられる。そのような背景から、データの持ち出し、データの改ざん・削除といった内部不正が行われるきっかけとなりうる可能性がある。したがって、内部不正が行われる可能性を低くし、かつ、事後に内部不正の事実確認や影響調査を実施できるよう、検討を行う必要がある。

検討のポイント

- 退職時手続の検討
  - ー秘密保持契約への誓約（退職後の機密保持や競合他社での就業禁止などの検討が必要）
  - ー外部記憶媒体の接続や外部ストレージへの接続といったデータの持ち出しなどのチェック（フォレンジック技術の活用も検討）
- 異動や退職時のアクセス権の即時変更・削除
  - ー個々人に紐づく情報資産の把握
  - ー人事情報との連携
  - ー部門やプロジェクト単位で管理しているものは特別な配慮が必要
- アクセス権の不正使用の実態把握
  - ー退職、離任後も有効なIDとその利用実態の検査（アクセスログの検査など）
- 事後調査のための情報保全
  - ーアクセスログの保全
  - ー利用端末のハードディスク全体の保全（フォレンジック技術の活用）

5. 2　異動・退職時の管理

項目	4-2-2.アクセス権指定（5） - ②情報システムにおける利用者のアクセス管理
内容	情報システムを管理・運営する担当者は、異動又は退職により不要となった利用者ID及びアクセス権を、ただちに削除していますか？
具体的実施項目	・利用者ID及びアクセス権の登録・変更・削除の手続きに漏れがないように、人事異動に関連する人事手続き等と連携した運用を行う。 ・利用者ID及びアクセス権が適切に付与されているかを確認するために、人事異動の時期に、一斉にアクセス権の要件を見直す。
事例/リスク	• 利用者IDとアクセス権設定に最新の利用者情報（人事情報など）と連携させる。 • 運用状況を監査する。 • 利用ログを監視し、利用頻度に応じてアクセス権を削除する。
リスクの解説	• 異動又は退職によって不要となった利用者IDが削除されていないと、役職員及び元役職員によって不正に利用されて、重要情報にアクセスされる恐れがある。 • 不正を犯した役職員及び元役職員の責任を追及できない、企業や団体の管理責任が問われる。

5. 2　異動・退職時の管理

項目	4-2-2.アクセス権指定（5） - ②情報システムにおける利用者のアクセス管理
議論のポイント	• 退職者のアクセスログを30日前からとることはベストプラクティスとなりうる。 • 退職時にセキュリティのレビューを受けてパスしないと退職金が払われないケースもある（フォレンジックを受ける必要あり）。 • 突然退職など退職にも様々なケースがあるので、対策を複数考える必要がある。 • アメリカの場合は、退職するとすぐにアクセス権がなくなるが、日本の場合即時性はない。 • 産休や出向時、休眠状態のアカウントをどのように扱うか、またリアルタイムにアカウントを削除できていない場合どのような対策をとるべきかを検討する必要がある。 • 異動後1か月間はアカウントを残し、その期間で引継等を行うようにしている。（リスクとして、この期間中に出向先のアドレスが決まり次第、今までの情報を転送をしているケースがある） • PJごとにファイルサーバへのアクセス権限、フォルダの権限を設定して運用。イントラとインターネット経由でアクセスできるフォルダについてディレクトリを設定し、修正や変更の記録を取るようにしている。 • ファイルサーバ上でしか編集できない仕組みや、ファイルをダウンロードできないような仕組みにしていく必要があるのではないか。 • 休職者のアカウントについて、BYODを認めていなければ休職者がアクセスする可能性は低いが、休職者のアカウントを使った成りすましのリスクがある。 • ADとIDが連携していないケースでは、人事情報とサーバのアカウントがひも付られておらず、誰がアクセスしているかを判断できない。このようなケースの企業に対してどのような対策をとるべきかを検討する必要がある。 • 人事情報とファイルサーバのアカウントをひも付けて運用している場合、異動した際に管理者が再度設定しなおす必要がある。 • 社内情報のアカウントを管理できていても、部門単位のサーバなどローカルで運用されているアカウントなどは管理できていない可能性がある。

5. 2　異動・退職時の管理

項目	4-6.人的管理（21）雇用終了及び契約終了による情報資産等の返却
内容	役職員の雇用終了時及び請負等の契約先との契約終了時に、取り扱いを委託した情報資産のすべてを返却または完全消去し、情報システムの利用者IDや権限を削除していますか？
具体的実施項目	• 誓約書や契約書には、雇用終了時や契約終了時に情報資産の返却及び契約先所有のPC等からの完全消去に関する記載が必要です。 • 取り扱いを委託した情報資産及び入館証の権限がすべて返却されたことを確認する必要があります。 • 情報システムから元役職員の利用者IDや権限が削除されたことを確認する必要があります。 • 契約先所有のPC等に保存されたすべての重要情報を完全消去した旨の確証を契約先からとる。 • 雇用終了間際に情報の持ち出し等をの不正が発生しやすいことから、雇用終了前から一定期間から、PC等をシステム管理部門等の管理下に置く。
事例/リスク	• 情報資産、情報システムの利用者IDや権限について、貸与、返却時にチェックシートを用いて本人と確認を行います。 • 上記チェックシートを、証跡として一定期間、保存管理します。
リスクの解説	• 取り扱いを委託した情報資産を返却又は完全消去させないと、重要情報が元役職員や元契約先から漏えいしてしまう恐れがあります。 • 入館証や貸出機器の返却及び情報システムから権限の削除が行われていないと、建物に不正侵入されたり、ネットワークから情報システムに不正侵入されたりし、情報資産を持ち出される恐れがあります。

5. 2　異動・退職時の管理

項目	4-6.人的管理（21）雇用終了及び契約終了による情報資産等の返却
議論のポイント	• 雇用終了時の秘密保持契約に競合他社にいかないという規定を入れる。 • 競業他社に転職した場合、不正競争防止法の観点から、敗訴してもよいから訴える方がよいのではないか（会社としての意思表示につながる）。 • アクセス権限付与時には個人別管理シートに記入し、異動時や退職時に確認する運用としているケースがある。 • 基幹システムのサーバ管理がしっかりできていても、部門システムのサーバについては管理が曖昧になっていることがある。 • ファイルサーバも人事異動の際に変更漏れが発生しやすい。 • 退職者のアクセスログを30日前から取得・確認することはベストプラクティスとなりうる。 • 社員は退職しない限りIDの期限はないが、アルバイトなどはIDの有効期間を設定し、延長申請がないと自動的に使用不可となる仕組みにしている。 • 退職の意思表明時点では情報の持ち出しなどを済ませている可能性があるので、不穏な動きを事前に検知する方策を検討する必要がある。

5. 3　システム管理者の権限管理

まとめ

システム管理者の権限管理に関しては、一般的な人的・組織的な管理施策、特権ID管理などのツールを利用した技術面での管理施策がある。どのような権限管理施策を適用するかは、(1)権限管理を実施する対象(サーバ, DB) ,(2)適用対象範囲(全社/特定部門、特定業務サーバ/部門サーバなど), (3)管理対象の情報重要度, (4)実現コストなどにより、検討を進めることになる。

検討ポイントは以下が考えられる。

1. ダブルオペレーション(作業の相互監視)
2. ダブルオペレーションを適用できない場合、作業実施申請(実施)書と操作ログの突合による作業確認
3. 権限管理の特定人物への権限集中化の回避(複数の権限管理者でのローテーション)
4. 情報資産の洗い出しと整理をおこない、情報資産の重要度の重み付け（格付け）をし、重要度が大きい情報を対象に、権限管理を適用する
5. サーバOSの特権IDの権限を分離し、職務に必要な最小限の特権だけに制限（ツール利用）

5. 3　システム管理者の権限管理

項目	4-2-2.アクセス権指定（6）システム管理者の権限管理
内容	複数のシステム管理者がいる場合は、情報システムの管理者IDごとに適切な権限範囲の割り当てを行い、相互に監視できるように設定していますか？ また、システム管理者が一人の場合は、ログ等により監視していますか？
具体的実施項目	• システム管理者を決める際には、高い規範意識等の適性を満たす者を任命する。 • 複数の管理者を任命し、相互に監視する。 • 一人のシステム管理者に権限が集中しないように権限を分散する。 • 相互に監視するために、作業内容や作業日時等が記載された作業報告を作成して残し、作業報告を別のシステム管理者が確認する。 • システム管理者は、特権を必要とする操作以外では特権を用いて操作を行わないようにする。
事例/リスク	• システムTOP画面に最近利用したユーザの名前を表示し、誰が利用しているか他の管理者が確認できる。 • 重要なシステムデータをダウンロードしたログは、5年間保存する。 • 必要最低限のアクセス権を付与する。 • 一人のシステム管理者に権限が集中しないように権限を分散する。 • システム管理者は、高い規範意識等の適性を満たす者を審査し承認する。 • 作業内容や作業日時等が記載された作業報告により監視、チェックを行う。 • 作業内容は全て監視され、特定の操作や条件下でのアラート、利用停止されるシステムとする • 特権処理の局所化を行う。

5. 3　システム管理者の権限管理

項目	4-2-2.アクセス権指定（6）システム管理者の権限管理
リスクの解説	• 権限範囲を適切に割り当てていないと、例えば、利用者IDの不正登録及び削除が発生し、不正登録による重要情報の不正使用や、不正な削除による業務妨害等の恐れがある。 • 一人の管理者に権限が集中している場合は、情報システムの破壊及び重要情報の削除等の妨害によって事業継続が不可能となる恐れがある。
議論のポイント	• 現実には システム管理者が一人しかいないケースもある。その場合は、事後的にシステム管理者の操作履歴等をシステム管理者の上席等が確認している。もしくは、複数人の立会によるオペレーションで代替している。 • 一人に全権限を与えるのではなく、二人そろわないと作業が完結しない仕組みの構築（パスワードを前半と後半に分けて2人が揃わないとパスワードが揃わないようにするなど） • 銀行はダブルオペレーションが基本となっている（ミスの防止、相互監視の観点） • 生体認証や二要素認証は金融等では導入されているが、一般企業で導入されている事例はまだ少ないのではないか。 • 証明書ベースでの認証も考えられる。 • 特権者の作業をダブルオペレーションにする必要があるのではないか（ログを取得して事後で検討するだけではダメ）。 • 特権者＝全部の権限を持っている人と定義すると、特権者の全権限を複数の人に分けるのは一つの方策となるのではないか。 • 一般的には個別システムでみるとシステム管理者が全権限を持っているが、全てのシステムの権限を持っている管理者のケースはまれである。しかし規模の小さな企業であれば全システムの権限を持つ管理者がいるケースがありうる。 • 特権者の上の特権を持たせるsuper adminを作るツールがある。super adminのログを取得することができるので、下位の管理者の牽制につながる。

5. 4　ログの取得・確認

まとめ

内部不正の事実確認、影響調査のため、ログを網羅的に取得し、改ざんされないよう安全に定められた期間保管する。また内部不正の早期発見のため、管理部署を決定しログを定期的に確認する。

ログの取得・確認は、ハードルの高い管理策であり、以下のポイント・課題が考えられる。

１．ログの取得

- 重要情報へのアクセス履歴や、操作履歴（端末PC・スマートデバイスの操作、メール送受信、Web利用等）等情報システムに関わるログを網羅的に取得する。例えば、サーバログが取得できない場合は、利用記録簿の作成、2名以上でのオペレーション実施等代替統制の検討が必要。
- ログの取得を行っている事実を従業員に通知したり、取得したログを従業員に還元することは、内部不正を抑止する効果があると考えられる。実施に際しては利用者のプライバシーを考慮し労働組合等の合意を得ることが望ましい。
- 守るべき情報の種類に応じてログの保存期間を決定する。

２．ログの確認

（１）一般ユーザのログの確認

すべてのログの確認は現実的ではなく、また業務利用と不正利用とを機械的に区別することが困難である。不正監視のためのポリシーを策定して異常を検知する方法が考えられる。例えば、個人情報の漏えい対策としては下記が考えられる。

- 利用時間帯が不自然（早朝、深夜、休日等の利用は、管理者が利用者に確認する）
- 利用回数が不自然に多い（担当業務内容、業務量とログの整合性を管理者が利用者に確認する）
- データのダウンロード機能等大量データの漏えいに直結するリスクのあるアプリケーション機能の利用は管理者が確認する。

（２）システム管理者のログの確認

- システム管理者が特権ID等システム系の高権限IDを利用する場合は、作業実施前の事前申請をルール化し、システム管理者の統括管理者が事後的に事前申請内容とログとを突き合わせて確認する必要がある。
- ログの取得が困難な場合は、システム管理者とシステム管理者以外の者が2名以上で作業し、ログの代替としてオペレーション内容の記録（画面のハードコピー等）等を文書で残す。

5. 4　ログの取得・管理

項目	4-5.証拠確保（17）情報システムにおけるログ・証跡の記録と保存
内容	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・証跡を定めた期間に従って安全に保護していますか？（推奨）
具体的実施項目	• 内部不正の早期発見及び事後対策のため、ログ・証跡を記録して安全に保存する。 • 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)等を取得する。 • 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する。 • ログは定期的に確認します。多量なファイルへのアクセスや業務範囲外のファイルへのアクセス等の通常の業務と異なる事象が発見された者に対して、事象確認又は監視強化等の対策を行う。 • 利用者のプライパシー等を考慮して、ログ・証跡を収集することを労働組合等と合意をとる。 • ログ・証跡の保存を行っている事実を従業員に通知することは、内部不正の発生を抑止する。
事例/リスク	• PC及びファイルサーバ上のログは記録し、最低半年以上は保存する。 • 定期的に監視する。 • ログの保存項目、保存期間、監視内容等の要件を明確にする。 • 重要情報へのアクセス履歴及び利用者の操作ログは三年以上記録し、リアルタイムに監視する。 • セキュリティ機能に関する事象を記録する。 • ログの削除や改ざんができないようにする。 • システムの変更に伴うログは、ログのモニタリング担当者以外がアクセスできないログ保管専用サーバに保存する。 • ログなどの保存方法、保存期間は、法的要件を踏まえる必要があるため、コンプライアンス部もしくは法務部と協働して決定する。

5. 4　ログの取得・管理

項目	4-5.証拠確保（17）情報システムにおけるログ・証跡の記録と保存
リスクの解説	• 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る恐れがある。 • 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、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る。 • ログ・証跡が安全に保存されていないと、処罰等の根拠として認められない場合がある。
議論のポイント	• 一般ユーザをすべて確認することは難しいので、異常値を発見する方法を考える必要がある。 • 一般ユーザの場合業務利用と不正利用とは機械的に区別できないので、監視ポリシーを策定する方法が考えられる。たとえば、個人情報の漏えい対策としては以下の確認ポイントが考えられる。 - 利用時間帯が不自然（早朝、夜間、休日） - 利用者の担当業務を勘案すると利用回数が多く不自然 - データのダウンロード機能等大量データの漏えいに直結するリスクのあるアプリケーション機能の利用等 • インターネットアクセスログについて、ユーザがインターネットへアクセスした、直近一週間にアクセスしたサイトURLと回数をユーザにメールで通知している(タイミングは毎週でなく不定期でだいたい１回／年ぐらい)。 • メールアーカイブの保存については、社外へ送信したメールの内容を５年間保存している。 • 携帯電話で大量のパケット利用者に対して、月中に警告メールの配信(手動)。 • スマートフォンの位置情報や、サイト訪問履歴、アプリ一覧などを自社開発のMDMで管理。 • ログを実際には取っていないが、「ログを取得しています」という情報をWarningとして出しているケースがある。 • 違法サイトを定義ファイルで指定しており、アクセスした場合警告が出るようにしている。 • メールは会社のものであることを、どのように社員に説明するかが課題。同意がない場合、内部統制を理由に閲覧すると問題になる可能性がある。

5. 4　ログの取得・管理

項目	4-5.証拠確保（18）システム管理者のログ・証跡の確認
内容	システム管理者のアクセス履歴や操作履歴等のログ・証跡を記録して保存するだけでなく、そのログ・証跡の内容を定期的にシステム管理者以外が確認していますか？
具体的実施項目	• 情報システムのログは、通常取得されるエラーのログに加えて、日常のシステムに対する管理、運用作業の記録についても取得する。 • 情報システムの設定変更や運用に関する作業をログに記録し、定期的にその作業のログの内容をシステム管理者の上司や総括管理者が確認する。 • 情報システムにおいて、ログ・証跡を収集できない場合には、情報システムの管理者の作業内容をドキュメントに記録し、定期的にその作業内容をシステム管理者の上司や総括管理者が確認する。
事例/リスク	• システムの変更に伴うログは、ログのモニタリング担当者以外がアクセスできないログ保管専用サーバに保存する。 • ログのモニタリングを実施していることをニュースレターやモニタリング結果の報告を以って定期的に従業員に周知する。 • システム管理者のログは別マシンに保存し、システム管理者がアクセスできないようにする。 • 運用監視手順を作成し周知する。 • 不正/異常発生時の自動通知をする。 • システム管理者を監視する者がリアルタイムにログを監視する。
リスクの解説	• システム管理者の行為がモニタリングされてないことにより、①システム管理者自身の不正な行為を誘発、検知できない②システムが意図した設計通り維持されない③不適切なアクセス権限が付与される④重要な情報が漏えいする、といったリスクが高まることが考えられる。 • システム管理者は大きな権限を持つため、システム管理者以外の者が、システム管理者向作業報告を確認して監視をしていないと、作業の正当性及び真正性を確認することや、システム管理者の内部不正を検知することが困難になる。

5. 4　ログの取得・管理

項目	4-5.証拠確保（18）システム管理者のログ・証跡の確認
議論のポイント	• ログ取得していることをアナウンスすることで、不正をしようとしている者の牽制にはつながる。 • 証券会社等であれば、毎日ログを確認しており特権IDを持っている人の不正は防げる。 • 利用時間帯（夜間、休日）、回数、大量ダウンロード、IDの種類、情報の重要度、機能別等のログを取得する必要があるのではないか。 • 内部不正の対策としてログの事後確認が重要。 • 金融機関ではシステム領域で暗号化されていない情報の存在を知っている者が狙うことがある（作業のために一度復号化する必要があるのでそこを狙う）。 • ワークファイル等のログをとることは少ないので、ダブルオペレーションとすることで防いでいる。 • システム系のIDについては事前申請が必要となるので突き合わせて確認ができる。 • 業務系IDは事前届け出が不要なので、不審な動きを検知するような仕組みを作る必要がある。 • ログを取得できない場合は、ダブルオペレーションにしたうえで、ハードコピーをとるようにする。 • ログ・証跡の記録と保存はシステム的に実装可能であるが、ログ・証跡の実効的な確認は難しい。 • システム管理者サイトのログについて、個人情報ではないが、PCの拠点管理者がPC情報の一括ダウンロードできる機能があり、そのダウンロードした操作履歴を５年間保存。 • ログの取得が困難なケースもあるため複数人の立会による作業とすることで防いでいる。ログの代替としてオペレーション内容の記録（画面のハードコピー等）で代替することもある。 • システム系のIDについては作業実施の事前申請を運用として実施することができるので、事前申請内容とログを突き合わせて確認ができる。

6. おわりに

■ 今後の課題

「情報の種類」及び「チェック対象」により、実状に応じて活用できるチェックリストの検討

- 「情報の種類」の特性（情報漏洩時の影響範囲、リスクの高低）に応じた、チェックリストの「実施項目」を充実させる（個人情報、取引先情報、営業秘密情報、人事情報、製品開発情報　等）
- 「チェック対象」に応じたチェックリストの「実施事項」を充実させる（自社、グループ会社、外部委託先、大企業、中堅・中小企業、個人事業主　等）
- 「実施項目」を第三者が実施有無の確認が可能なものとする

内部不正対策として、情報システム部門だけではなく他部署との連携を進める方策の検討

- ワークライフバランスや業務プロセスの可視化等は一般の会社では推進されているが、なぜセキュリティと関係するかを議論する必要がある
- 職場環境や人的管理の実施項目はIT部門だけでは対応できず、人事や総務との連携が重要となる
- IPAガイドブックでも情報システム部門が主担当となる部分の議論はなされているが、他部署をどのように巻き込んでいくかの視点はまだない

6. おわりに

■ WG２の年度活動を終えて

- 会合を通じて各社から得た情報は、気付きの機会ともなり、貴重なアドバイスとなっている。
- 本報告書は「最終報告書」ではありますが、WG２の活動記録であり、活動を通じて共有できた各社の具他的な取り組み、知見、悩み、残課題等が混在しております。したがって記載内容に整合性のとれていない箇所等ございますが、本報告書の読者の皆様に少しでも役立てば幸いです。
- 独立行政法人情報処理推進機構（IPA）の小松文子様から、 「組織における内部不正の動向と防止策」とについてご講演いただきました、ありがとうございました。
- WG２の皆様、事務局の皆様ありがとうございました。