資料４－３

特定個人情報等の利用状況の
ログ分析・確認について

平成31年○月

個人情報保護委員会事務局

はじめに

特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）では、特定個人情報について「取扱規程等に基づく運用を行うとともに、その状況を確認するため、特定個人情報等の利用状況等を記録し、その記録を一定の期間保存し、定期に及び必要に応じ随時に分析等するための体制を整備する」ことを求めています。

地方公共団体等における多くの事務は、情報システムを用いて行われており、その操作記録等のログは保管されている場合がほとんどですが、それらのログを分析・確認する実施手順の目安はありませんでした。

平成30年度に実施した、特定個人情報の取扱いの状況に係る定期的な報告においても、「ログをどのように分析・確認すればよいか分からない」との意見が多く寄せられたことを踏まえ、ログの分析・確認の手法について一例を作成し、公表することとしました。

なお、本事例は地方公共団体等がログの分析・確認するに当たり、あくまでも参考として示したものであるため、各機関の事務の特性や情報システムの構成等を踏まえて、対応することを妨げるものではありません。

ログを分析・確認するための手順

ログを分析・確認するための手順はおおむね以下のとおりです。

①目的の明確化	ログを分析・確認する目的を明確にします。
②実施体制の整備	ログを分析・確認するための体制を整備します。
③対象の選定	ログを分析・確認する対象を選定します。
④ログの出力	情報システムからログを出力します。
⑤ログの分析・確認	①の目的に合う観点で分析・確認を行います。
⑥結果報告	確認結果を総括責任者等へ報告します。

次のページ以降、各項目について詳しく説明していきます。

①ログを分析・確認する目的の明確化

最初にログを分析・確認する目的を明らかにします。特定個人情報の適正な取扱いに関するガイドライン（行政機関等・地方公共団体等編）では、目的を「取扱規程等に基づく運用の状況を確認するため」と規定しており、その手法として情報システムの場合、ログイン実績やアクセスログと、関連する書面の記録を照合することを例示しています。

なお、ここでいう「取扱規程等に基づく運用の状況」とは、例えば次のようなものが考えられます。

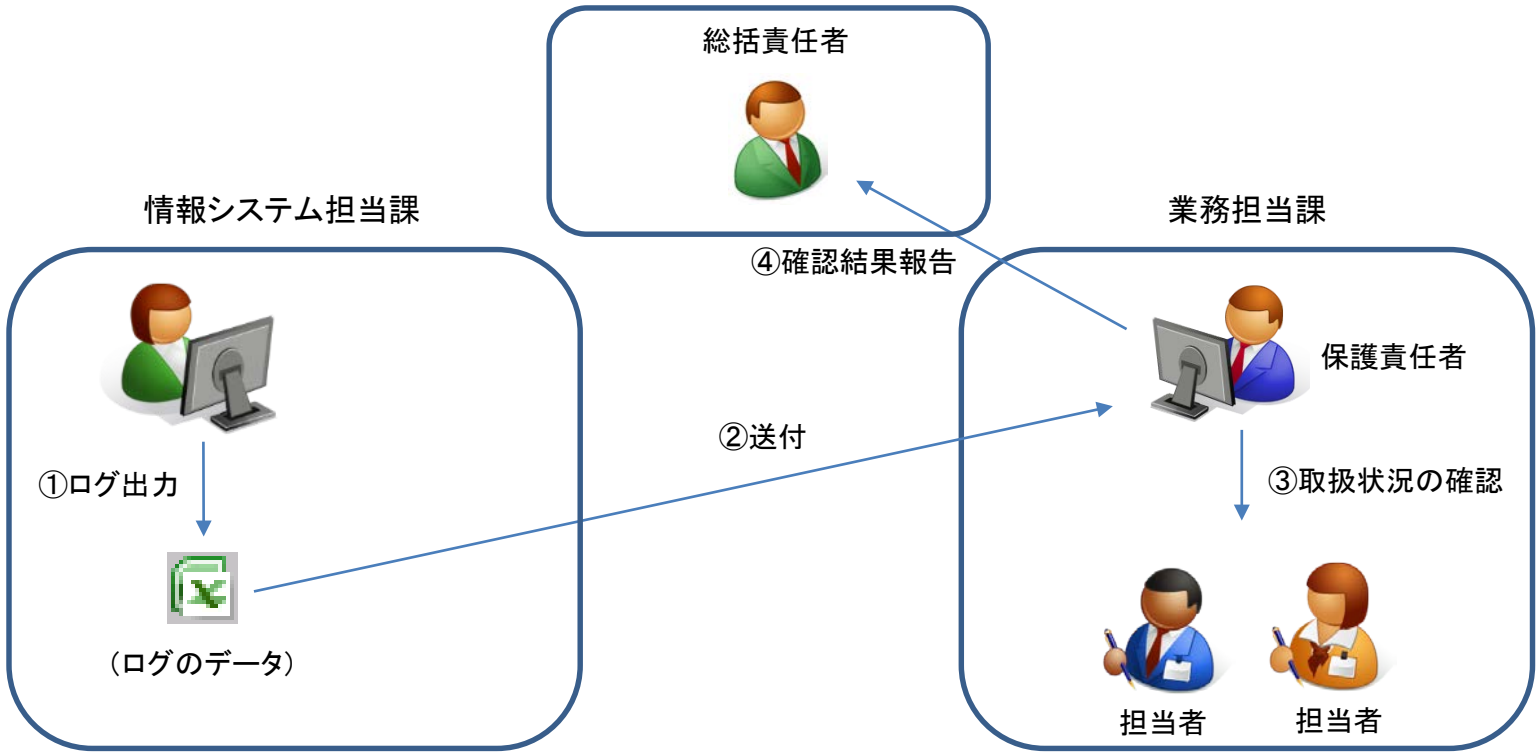
- 特定個人情報等を不必要に閲覧・持ち出しをしていないか
- 特定個人情報等の取扱いにおいて誤った操作・処理をしていないか
- 特定個人情報等を標的とした不正アクセスを受けていないか

②ログを分析・確認するための体制整備

目的を明らかにしたら、どのような体制でログを分析・確認するかの整備を行います。

一般的に、情報システムのログは、機関内のシステム担当課のみ出力できるようにしていることが多いですが、システム担当課の職員は、ログの分析・確認の対象となる業務に精通していないため、①ログの出力はシステム担当課で行い、②そのデータを業務担当課の保護責任者へ送付し、③保護責任者は自身の担当課内の取扱状況を確認する、というように分担することが考えられます。

また、業務担当課の保護責任者は確認後、④確認結果を総括責任者等に報告し、必要に応じて改善をしていくことが望ましいです。



③ログを分析・確認する対象の選定

情報システムのログは、取扱事務によっては膨大な量が出力されるため、全てのログを網羅的に分析・確認することは、現実的には困難です。そのため、特定個人情報等を取り扱う事務の中で、どのログをどれくらいの期間（※）で重点的に分析・確認すれば目的を達成できるかを検討し、選定します。

【検討の結果、分析・確認の対象を選定した例】

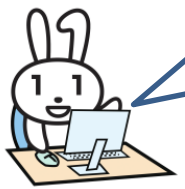
・税務課は他の課に比べ大量の特定個人情報等を扱うため、操作誤りがないかを確認する。

・国民健康保険課は特定個人情報等を外部記録媒体に書き出す業務があり、紛失等での情報漏えいの危険があるため、USBメモリの使用ログを確認する。

・過去に個人番号が映った画面をプリントスクリーン機能で印刷して持ち出した不正事例があったため、操作内容にプリントスクリーンが使われていないかを確認する。

・情報提供ネットワークシステムの副本が正しく登録されているか確認するため、情報提供のエラーログを確認する。

※　期間については、毎月や隔月といった短い間隔で行うことが望ましいです。
これは、間隔が長すぎるとログが大量となり、情報システムがログを出力する際の負荷で停止してしまったり、確認対象とする事務の内容を忘れてしまうためです。
また、対象は定期的に変更し、幅広く分析・確認していることを周知すれば、特定個人情報の不適切な取扱いを抑止できることも期待できます。



④情報システムからのログ出力

情報システムからログを出力する方法は、導入している情報システムによって異なりますが、
多くの情報システムでは、ログ出力機能が実装されており、操作方法も難しくありません。
もし、操作方法が不明な場合は、その情報システムを導入した事業者等に確認してください。

【出力したログの例】

日時	職員名	端末番号	操作内容	処理結果	個人番号参照
2019/02/02 19:48:52	Aさん	172.16.12.xxx	ログイン	成功	なし
2019/02/03 22:11:03	Zさん	172.16.100.xxx	参照	対象者宛名番号：A8193	あり
2019/02/04 08:20:18	Eさん	172.16.13.xxx	ログイン	成功	なし
2019/02/04 08:25:33	Aさん	172.16.11.xxx	ログイン	成功	なし
2019/02/04 08:30:19	Bさん	172.16.24.xxx	書き出し	失敗	あり
2019/02/04 09:00:30	Fさん	172.16.31.xxx	ログイン	成功	なし
2019/02/04 09:01:41	Cさん	172.16.11.xxx	プリントスクリーン	成功	あり
2019/02/04 09:15:45	Fさん	172.16.31.xxx	参照	対象者宛名番号：A2321	あり
2019/02/04 10:04:25	Dさん	172.16.18.xxx	参照	対象者宛名番号：A1030	あり
2019/02/04 13:01:41	Dさん	172.16.18.xxx	参照	対象者宛名番号：A1030	あり
2019/02/05 16:52:03	Dさん	172.16.18.xxx	参照	対象者宛名番号：A1030	あり
2019/02/07 12:34:38	Dさん	172.16.18.xxx	参照	対象者宛名番号：A1030	あり
・・・	・・・	・・・	・・・	・・・	・・・

※　情報システムによっては、出力する項目（日時や操作内容等）を選択することもできます。
最初に決めた目的に合う項目を選択し出力することで、不必要な項目を省略することができます。

⑤ログを分析・確認する際の観点

ログを出力したら、表計算ソフトやデータベースソフトに取り込むことで、分析・確認が行いやすくなります。必ずしも高度な分析ソフト等を導入する必要はなく、表計算ソフトのフィルタ機能や検索機能を利用しても分析・確認することは可能です。分析・確認する際の観点を以下に例示します。

【分析・確認する観点の例】（不必要な閲覧や持ち出しがされていないかを確認する目的での観点の場合）

	日時	職員名	端末番号	操作内容	処理結果	個人番号参照
	2019/02/02 19:48:52	Aさん	172.16.12.xxx	ログイン	成功	なし
①	2019/02/03 22:11:03	Zさん	172.16.100.xxx	参照	対象者宛名番号：A8193	あり
	2019/02/04 08:20:18	Eさん	172.16.13.xxx	ログイン	成功	なし
	2019/02/04 08:25:33	Aさん	172.16.11.xxx	ログイン	成功	なし
	2019/02/04 08:30:19	Bさん	172.16.24.xxx ③	書き出し	失敗	あり
	2019/02/04 09:00:30	Fさん	172.16.31.xxx	ログイン	成功	なし
	2019/02/04 09:01:41	Cさん	172.16.11.xxx ④	プリントスクリーン	成功	あり
	2019/02/04 09:15:45	Fさん	172.16.31.xxx	参照	対象者宛名番号：A2321	あり
	2019/02/04 10:04:25	Dさん	172.16.18.xxx	参照	対象者宛名番号：A1030	あり
	2019/02/04 13:01:41	Dさん	172.16.18.xxx	参照	対象者宛名番号：A1030	あり
⑤	2019/02/05 16:52:03	Dさん	172.16.18.xxx	参照	対象者宛名番号：A1030	あり
	2019/02/07 12:34:38	Dさん	172.16.18.xxx	参照	対象者宛名番号：A1030	あり
	・・・	・・・	・・・	・・・	・・・	・・・

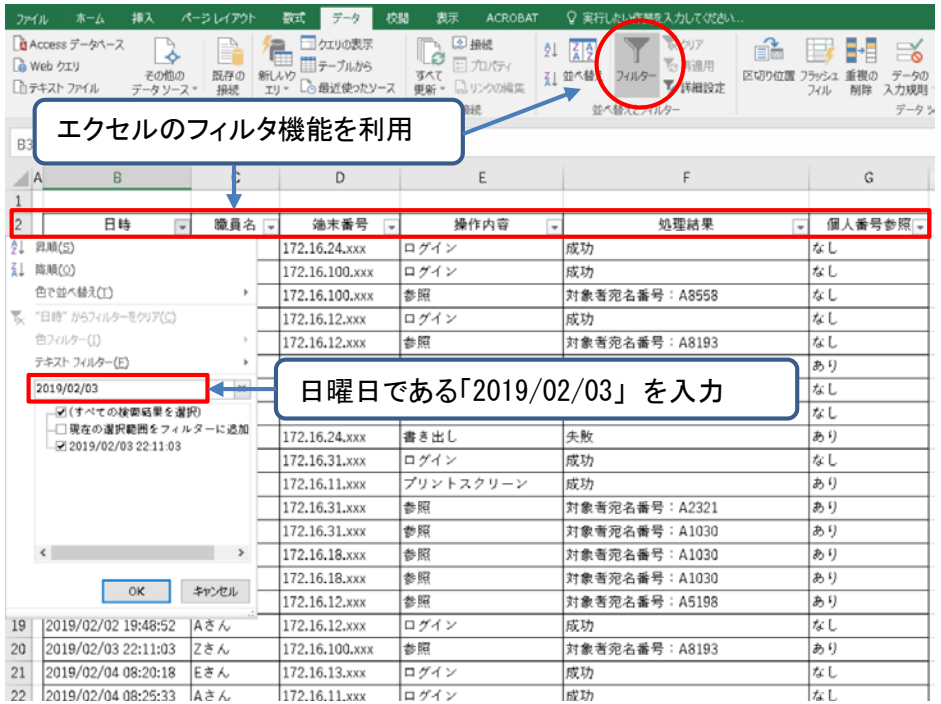
②

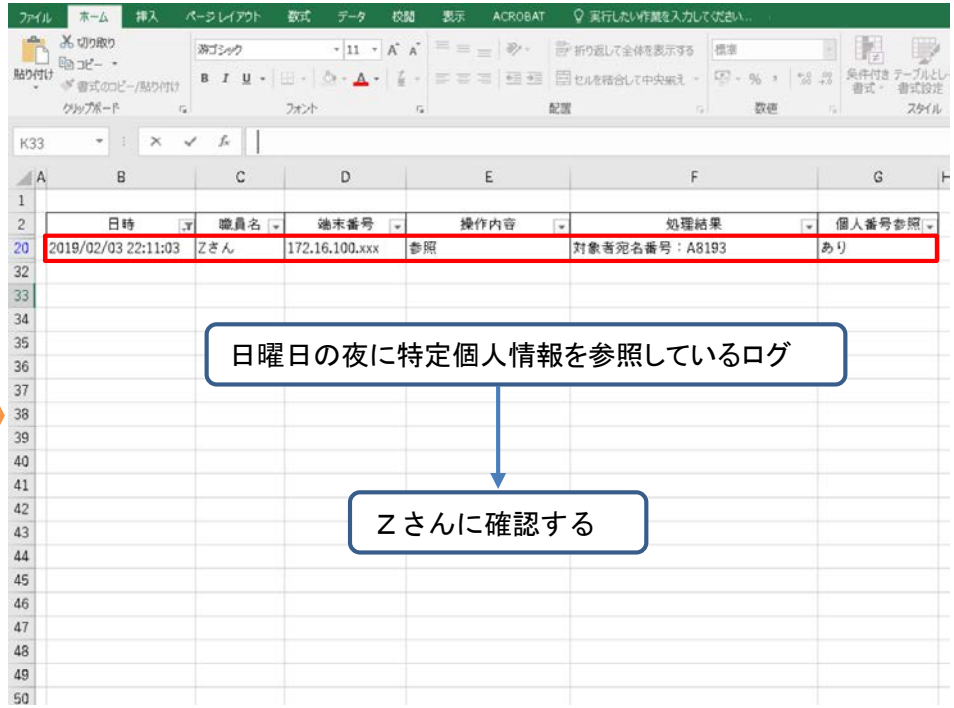
①不自然な曜日時間帯に特定個人情報を参照をしている。
②通常とは異なる端末を使用している。
③権限が付与されていない操作で特定個人情報を取得しようとしている。
④通常行う必要がない操作で特定個人情報を取得している。
⑤同一の特定個人情報を何度も参照している。

【参考】フィルタ機能の利用

例えば、休日の閉庁日に特定個人情報を閲覧した事績がないか確認する場合は、出力したログをエクセルファイルで開き、フィルタ機能を利用して確認対象の日にちを入力します。

エクセルのフィルタ機能の操作方法は、以下のとおりです。





ログだけを見るのではなく、関連する書類（例えば出勤簿や届出書等）と照合し、その操作が適切だったのかを確認することも有効な手法です。

⑥ログの分析・確認の結果報告

ログの分析・確認を行い、確認結果を取りまとめたら、問題の有無にかかわらず、総括責任者等に報告をすることが望ましいです。

これは、ログの分析・確認を組織全体として取り組んでいることを明確にするとともに、不適切な取扱いがあった場合、速やかに対処を行うことができるようにするためです。

また、ログの分析・確認が組織的に行われていることを研修の機会等を通じて周知することで、不正行為の抑止・牽制となることも期待できます。

【結果報告書の例】

平成○年○月○日

特定個人情報総括責任者　殿

特定個人情報保護責任者

住民税システムに関する特定個人情報の操作ログ確認結果

下記のとおり、住民税システムにおける特定個人情報の操作ログを確認しましたので報告します。

記

期間	平成○年○月○日～平成○年○月○日
不正・目的外利用	なし
誤操作・処理誤り	１件　（詳細は別紙のとおり）
備考	―

以上