第三者証明書
「トッパングループのマイナンバー管理業務」の活用について

2017年7月7日

凸版印刷株式会社
法務・知的財産本部　コンプライアンス部　灘

◆ マイナンバー法の厳しい罰則規定（民間企業、個人に係わるもの）

	行為	懲役	罰金
①	**正当な理由がなく**、マイナンバー**ファイル**を「提供」	4年以下	**200万円以下**
②	**不正**な利益を得る目的で、**マイナンバー**を「提供」、「盗用」	3年以下	**150万円以下**
③	**不正**アクセス等による**マイナンバー**の「取得」	3年以下	**150万円以下**
④	**委員会**の命令違反	2年以下	**50万円以下**
⑤	**委員会**への虚偽報告、立入検査拒否等	1年以下	**50万円以下**
⑥	**不正**な手段による「**マイナンバーカード**」等の「取得」	6月以下	**50万円以下**

- 罰則は、“不正“な行為をした者や会社に対して適用される
- しかし、不適切な取扱いがあれば、「個人情報保護委員会」の立入検査がありうる。

◆ 民間企業で**構じなければならない**安全管理措置
そして、安全管理措置の**未実施は、法令違反となりうる**

1.組織的安全管理措置（義務）	a 組織体制の整備 b 取扱規程等に基づく運用 c 取扱状況を確認する手段の整備 d 情報漏えい等事案に対応する体制の整備 e 取扱状況の把握及び安全管理措置の見直し
2.人的安全管理措置（義務）	a 事務取扱担当者の監督 b 事務取扱担当者の教育
3.物理的安全管理措置（義務）	a 特定個人情報等を取り扱う区域の管理 b 機器及び電子媒体等の盗難等の防止 c 電子媒体等を持ち出す場合の漏えい等の防止 d 個人番号の削除、機器及び電子媒体等の廃棄
4.技術的安全管理措置（義務）	a アクセス制御 b アクセス者の識別と認証 c 外部からの不正アクセス等の防止 d 情報漏えい等の防止

システムやインフラ（ネットワーク、サーバなど）に関係が深い部分

物理的安全管理措置

事業者は、特定個人情報等の適正な取扱いのために、次に掲げる物理的安全管理措置を講じなければならない。

	項 目	内 容	具体例
a.	特定個人情報等を取り扱う区域の管理	特定個人情報等の情報漏えい等を防止するために、「管理区域」及び「取扱区域」を明確にし、物理的な安全管理措置を講ずる	管理規程へ「管理区域」および「取扱区域」を定義する、など
b.	機器及び電子媒体等の盗難等の防止	管理区域及び取扱区域における特定個人情報等を取り扱う機器、電子媒体及び書類等の盗難または紛失等を防止するために、物理的な安全管理措置を講ずる	入退室管理方法としては、ＩＣカード、ナンバーキー等による入退室管理システムの設置。電子媒体の持ち込み制限。端末へのワイヤーロック設置、など
c.	電子媒体等を持ち出す場合の漏えい等の防止	特定個人情報等が記録された電子媒体または書類等を持ち出す場合、容易に個人番号が判明しない措置の実施、追跡可能な移送手段の利用等、安全な方策を講ずる	セキュリティ便や簡易書留の利用。電子媒体の場合は暗号化や指紋認証付USBの利用、など
d.	個人番号の削除、機器及び電子媒体等の廃棄	復元できない手段で削除または廃棄する 削除または廃棄した記録を保存する。委託する場合には、委託先が確実に削除または廃棄したことを証明書等により確認。	専用のデータ削除ソフトウェアの利用又は物理的な破壊。容易に復元できない手段を採用する、など

技術的安全管理措置

事業者は、特定個人情報等の適正な取扱いのために、次に掲げる技術的安全管理措置を講じなければならない。

	項 目	内 容	具体例
a.	アクセス制御	情報システムを使用して個人番号関係事務または個人番号利用事務を行う場合、事務取扱担当者及び当該事務で取り扱う特定個人情報ファイルの範囲を限定するために、適切なアクセス制御を行う	個人毎にログインIDを付与する。利用端末を制限する、など
b.	アクセス者の識別と認証	特定個人情報等を取り扱う情報システムは、事務取扱担当者が正当なアクセス権を有する者であることを、識別した結果に基づき認証する	管理システムによる認証、など
c.	外部からの不正アクセス等の防止	情報システムを外部からの不正アクセスまたは不正ソフトウェアから保護する仕組みを導入し、適切に運用する	セキュリティソフトの導入。定期的なセキュリティ監査の実施、など
d.	情報漏えい等の防止	特定個人情報等をインターネット等により外部に送信する場合、通信経路における情報漏えい等を防止するための措置を講ずる	ファイアーウォールの設置。ネットワーク接続の制限、など

漏えいしたときの企業イメージのへのダメージが大きいことから、役員からの方針として
「従業員の分であっても、トッパングループから1点たりとも漏えいすることがないように」

そのためには

講じなければならない安全管理措置を各社で確実に実施しなければならない

しかし

各社で、それぞれ物理的・技術的な対応を図ると
新たな費用や人的工数が発生し、またリスクも残る可能性がある

そこで

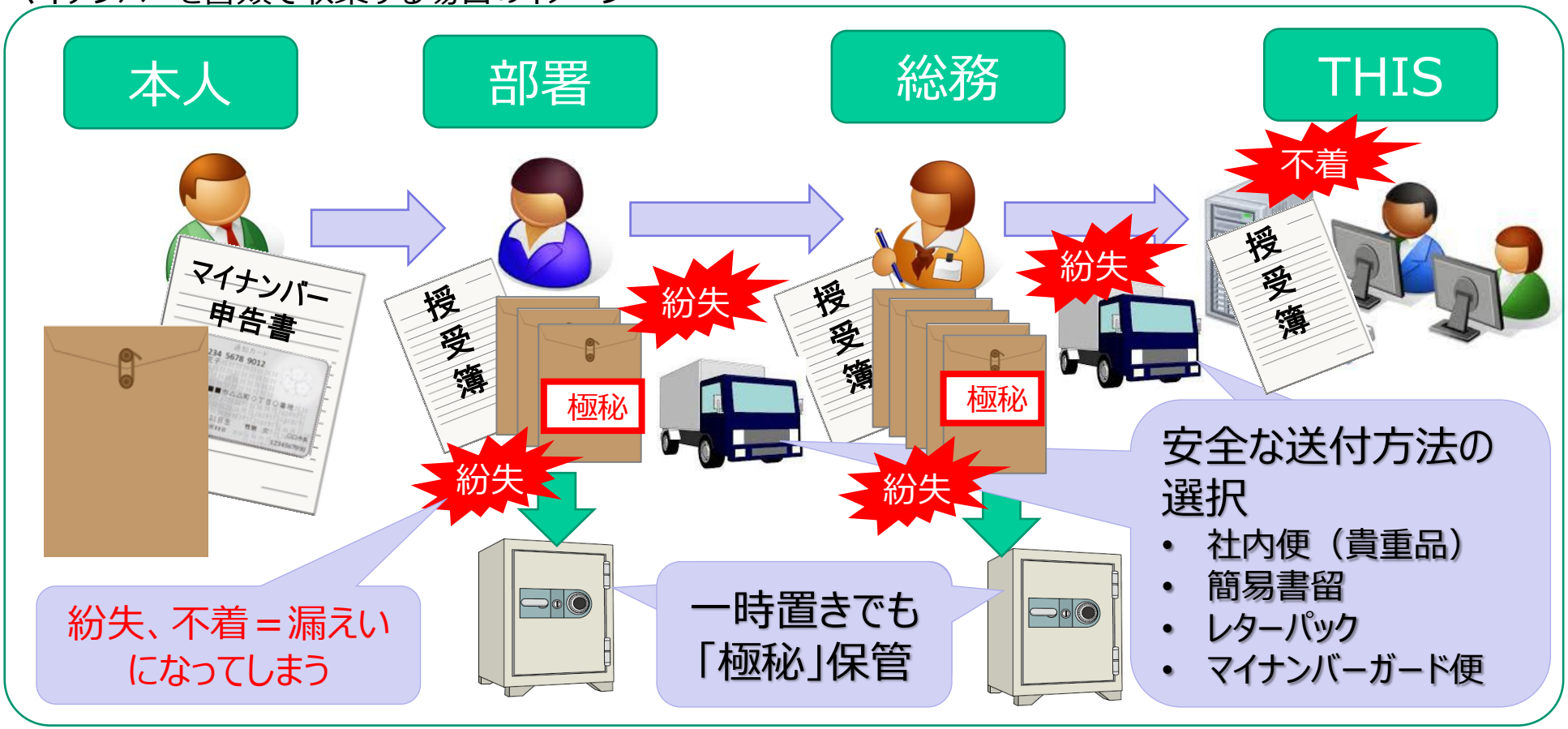
【解決策①】　THISで一元的に運用管理

- ✓ THISは、トッパングループの給与計算受託会社であり、個人情報取扱いの実績がある
- ✓ 一元的に管理することで、各社でのマイナンバーの保管管理のリスクを極小化できる
- ✓ 独立したマイナンバー管理システム導入や安全管理措置を講じることで、適切な保管管理が行なえる
- ✓ 各社で物理的・技術的な安全管理措置を行なうより、１箇所で集中的に費用をかけるため、グループとしてのトータルコストを低減できる

THISで一元管理するとしても

「書類」を前提にすると、関係者が多数存在し、その全ての工程で
徹底した漏えいリスク対策は難題であり、廃棄記録や授受記録の管理の負荷もかかる

マイナンバーを書類で収集する場合のイメージ



マイナンバーに触れなければいけない人だけに限定しなければならない

つまり

全国各地に多数存在する総務、経理などの関係事務実施者とTHISとが
直接やり取りができる方法が必要

しかし

現状の社内ネットワークをそのまま使うと、部外者のアクセスによる漏えいの可能性

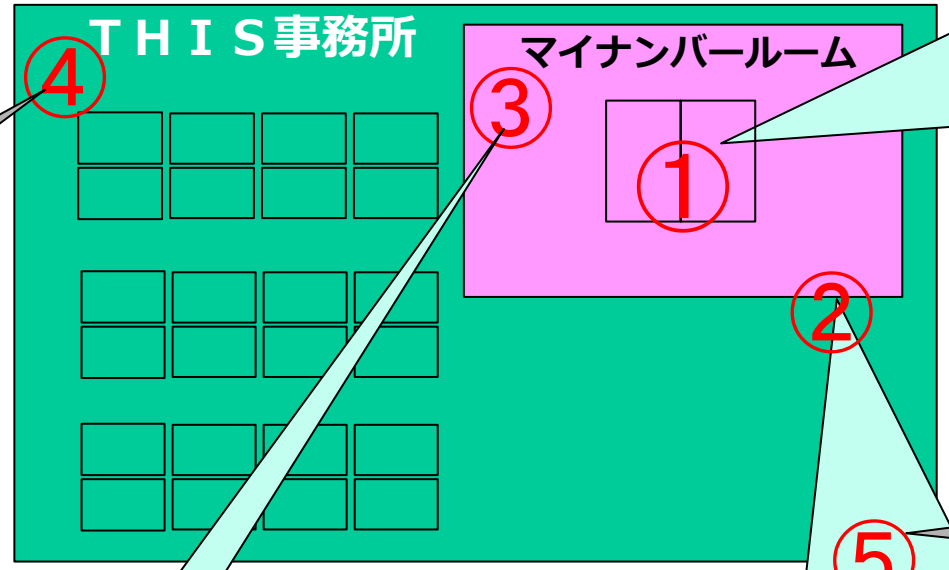
そこで

【解決策②】 マイナンバー用のセキュアな環境を構築

- ✓ THISからの漏えいリスクを徹底的に排除した環境
- ✓ やり取りは、電子データのみで、書類での授受はゼロにする
- ✓ 関係事務実施者は、マイナンバー取り扱い業務しかできない環境
- ✓ 関係事務実施者の作業コントロールは、THISが担う

THISからの漏えいリスクを徹底的に排除した環境の構築

✓ THIS事務所内に新たにマイナンバー取扱い専用室を設けた



④THIS事務所
監視カメラ

③管理区域
監視カメラ

②管理区域の入退管理

外側　ICカード認証＆パスワード入力　内側

アンチパスパック

⑤THIS事務所
入室管理

THISからの漏えいリスクを徹底的に排除した環境の構築

✓ マイナンバールーム内の情報機器からの漏えい対策

マイナンバールーム

マイナンバールームへ入室できる者は専任者と管理者のみ（現時点4人）

LanScopeによるデバイス制御、アクセスログ監視

専用FWの設置

インターネット接続禁止

メール送信禁止（受信のみ）

HDDの暗号化

カメラ付携帯の持ち込み禁止

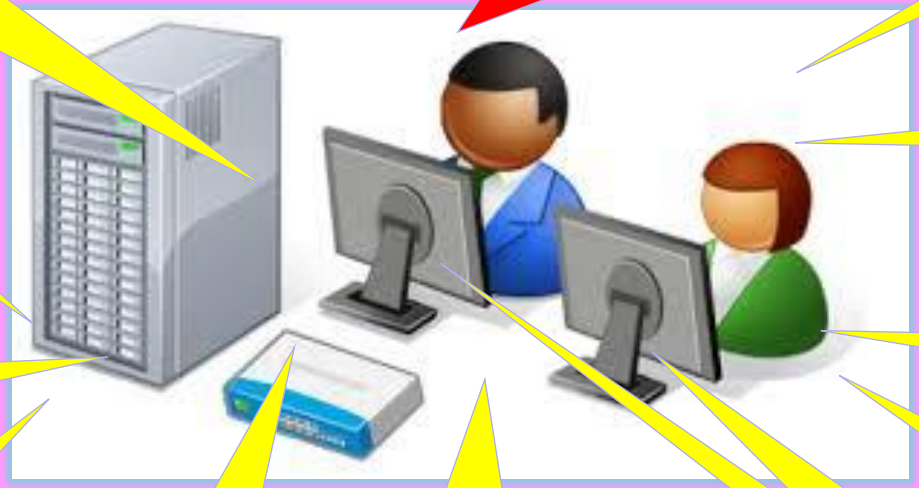
ワイヤーロックによる固定

専用PCのみで操作が可能

MN処理専用ADアカウント

アクセスログの記録

USB機器書き出し対策



関係者とのマイナンバーのやり取りは電子データのみ

✓ マイナンバー用のセキュアな環境を構築した

本人

FastNumber

本人がマイナンバーを登録

「FastNumber」

- ✓ THISから通知されたID、パスワードでログイン
- ✓ 登録する機能しかない
- ✓ ダウンロードするとデータは自動消去される

FastNumberやマイナンバー管理システムに直接アクセスできるのは、「マイナンバー専任者」で、「マイナンバー専用室」からのみ

マイナンバー専用室

THIS

マイナンバー専任者

ダウンロード/消去

ログイン情報の登録

税務署

eTAXで税申告

マイナンバー提供

「関係事務実施者用ファイルサーバ」

マイナンバー提供依頼

マイナンバー抽出

マイナンバー情報の登録

「マイナンバー管理システム」

総務・経理
(関係事務実施者)

THISとマイナンバーのやり取りが出来るのは、登録された「関係事務実施者」のアクセス権が設定されたフォルダのみ

委託元は、委託先の監督をしなければならない

番号法に基づき委託者自らが果たすべき安全管理措置と同等の措置が講じられるよう必要かつ適切な監督を行わなければならない。

しかし

THISにマイナンバー取扱を委託しているグループ会社は55社
監査する側と受ける側の問題をどう解決するか？

そこで

【解決策③】 第三者証明の活用

- ✓ 本社が代表幹事会社としてTHISの監査を実施することはできるが、委託元にはプライバシーマークを取得している会社もあり、それぞれの委託先監査の手順を集約して行なうことは、本社側の負荷もかかる
- ✓ 委託元が監査と同等の措置をとったとの説明責任を果たすには、第三者証明が説得力ある
- ✓ また、個人事業主など、社外の人からのマイナンバーを収集する際に、安心感を持ってもらうためにも役立つ

◆ 感想

《内容について》

- 委託元から別途監査を要請されることなく、第三者証明で代行することはできた。
- 一方、個人事業主への案内に、第三者証明を取得している旨をアピールしたが、認知がまだ十分なレベルに至っていないせいか、それをもって安心感を持ってもらえたということには至らなかった。

《費用面について》

- 毎年、同額の費用が発生するとなると、THISのような社内向けサービス子会社では、費用面で、継続利用が難しい。
- 日本印刷産業連合会のプライバシーマーク審査料だと２年で約30万円ですむ。（THISは小規模事業者にあたるため）
- 日本印刷産業連合会からは、プライバシーマークを取るように働きかけられていることもあり、重複しての支出は厳しい。

◆ 要望

- 第三者証明の利用シーンは多く想定されるので、第三者証明サービスの認知度を上げるためにも、利用しやすさへの配慮をお願いしたい。