企業のマイナンバー対応と情報セキュリティー対策

2015/11/18

ヤフー株式会社 CISO Board
楠 正憲

自己紹介 – 楠 正憲（くすのきまさのり）

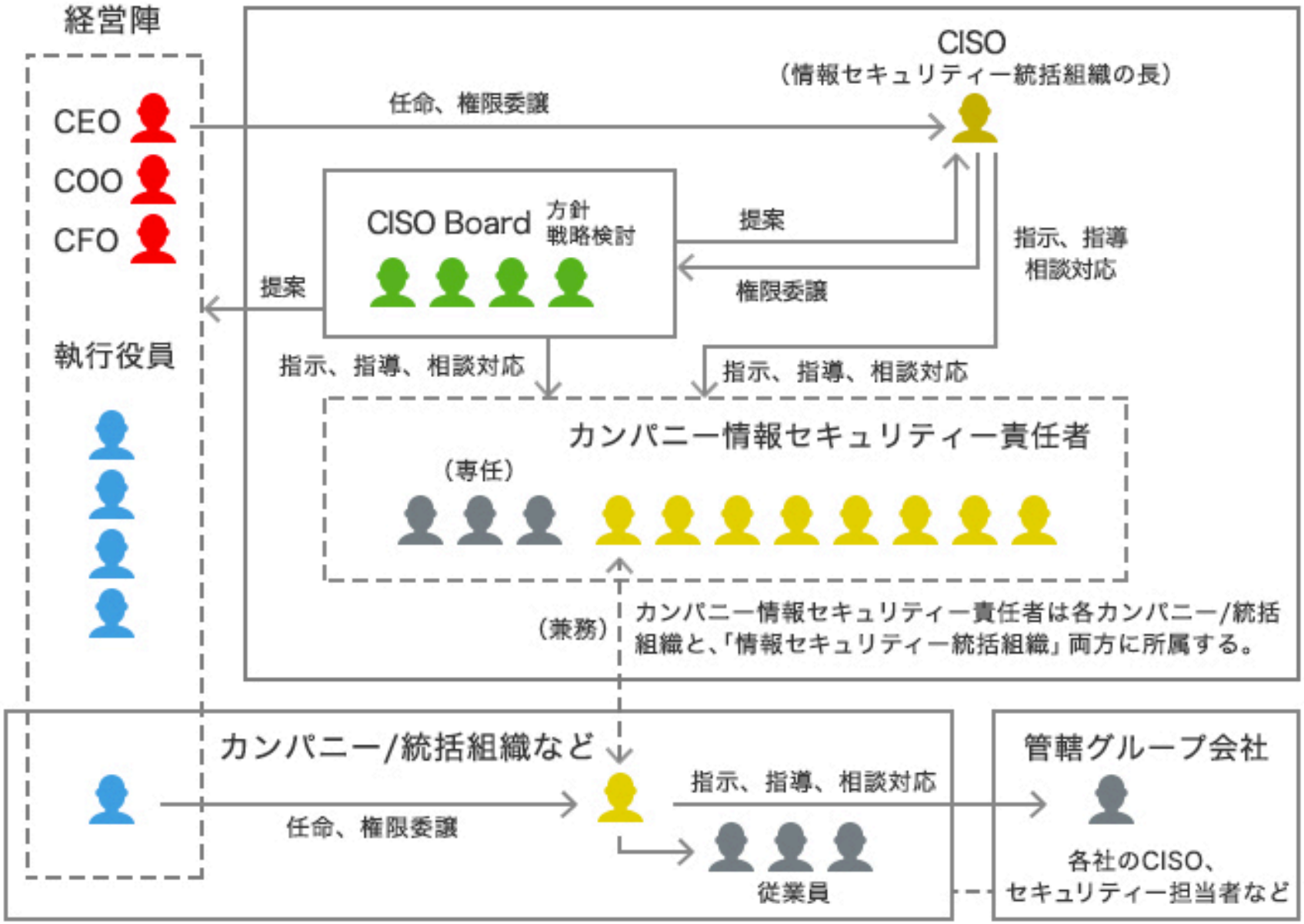
1998年2月 インターネット総合研究所 入社
- JPIX運用管理, CBook24.com IPv6の推進など

2002年10月 マイクロソフト 入社
- Windows Server製品部 Product Manager
- 経済産業省 情報セキュリティー総合戦略
- 技術戦略部長としてBlaster事案の対応などに従事
- 警察庁 総合セキュリティー対策会議 委員
- NISC 技術戦略専門委員会 グランドチャレンジWG 委員
- サイバー犯罪に関する白浜シンポジウム＆情報危機管理コンテスト 審査委員

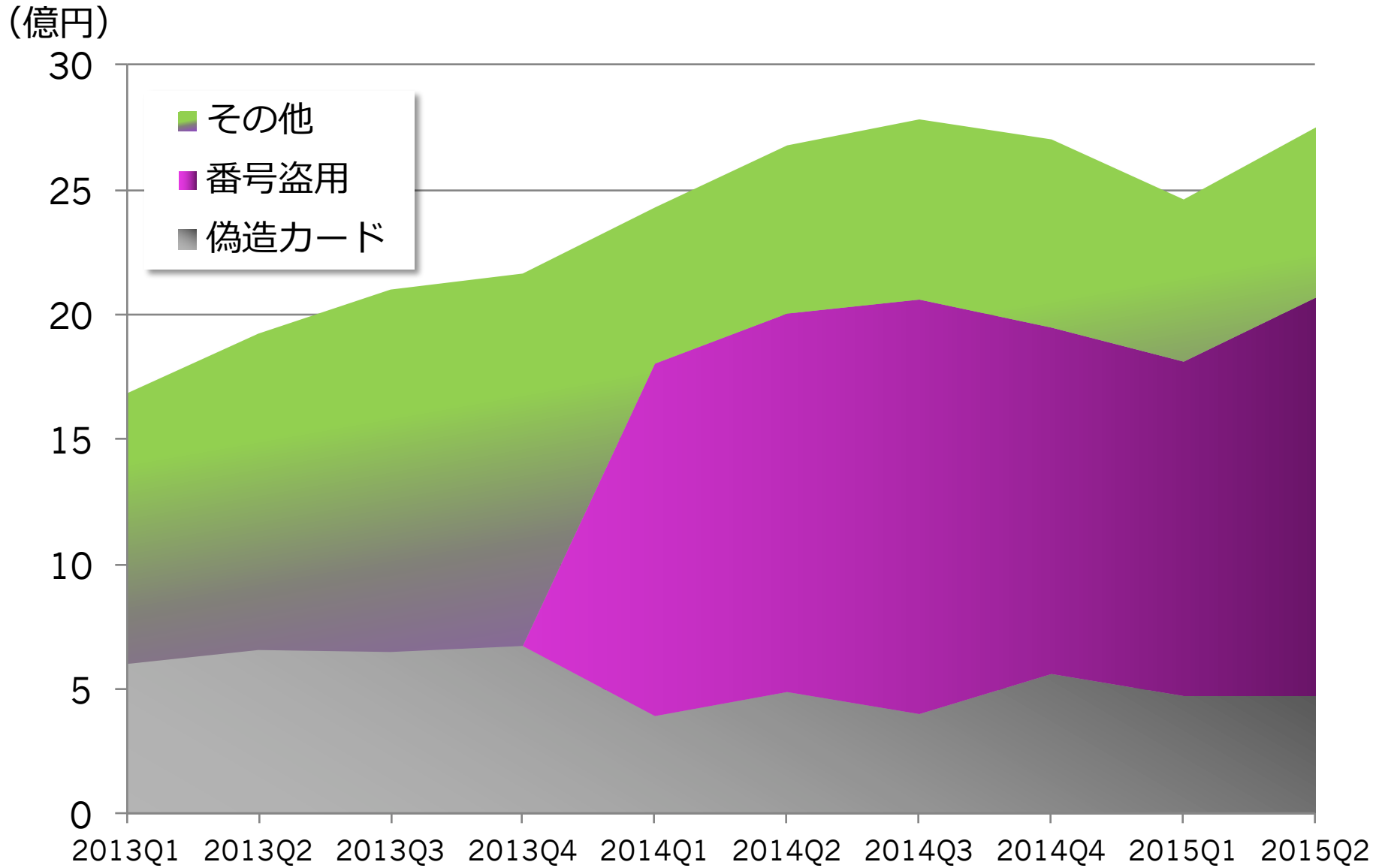
2011年12月 内閣官房 任用 (非常勤)
- 社会保障改革担当室 番号制度推進管理補佐官
- 情報通信技術 (IT) 総合戦略室 政府CIO補佐官（総括担当） 2013年4月～
- 厚生労働省 CIO補佐官 (併任) 2015年6月～9月

2012年7月 ヤフー株式会社 入社
- 技術調査室 室長、ID本部長、決済金融カンパニー 情報セキュリティー責任者
- CISO Board メンバー、福岡市 政策アドバイザー (ICT)
- Open ID Foundation Japan 代表理事

ヤフージャパンの情報セキュリティー体制

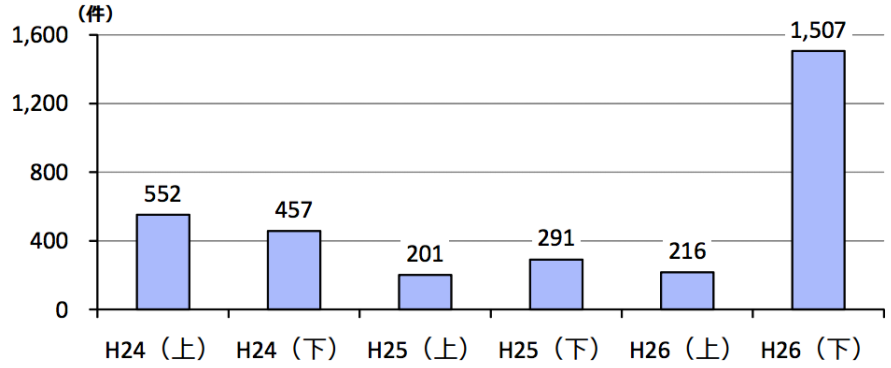


番号盗用の被害が偽造カードを上回った

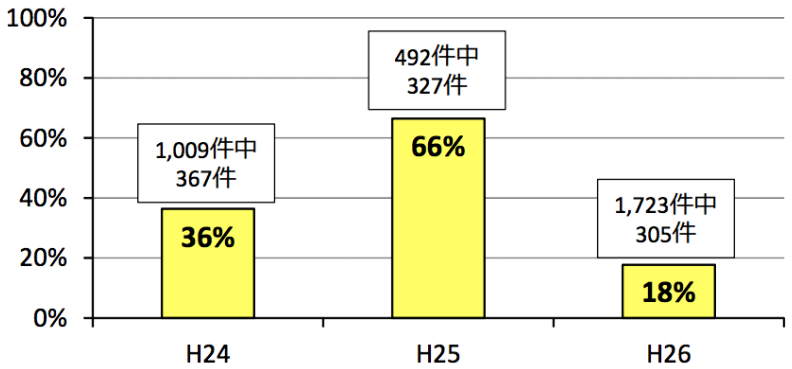


クレジットカード不正使用被害の集計結果について - 日本クレジット協会 (2015.9)

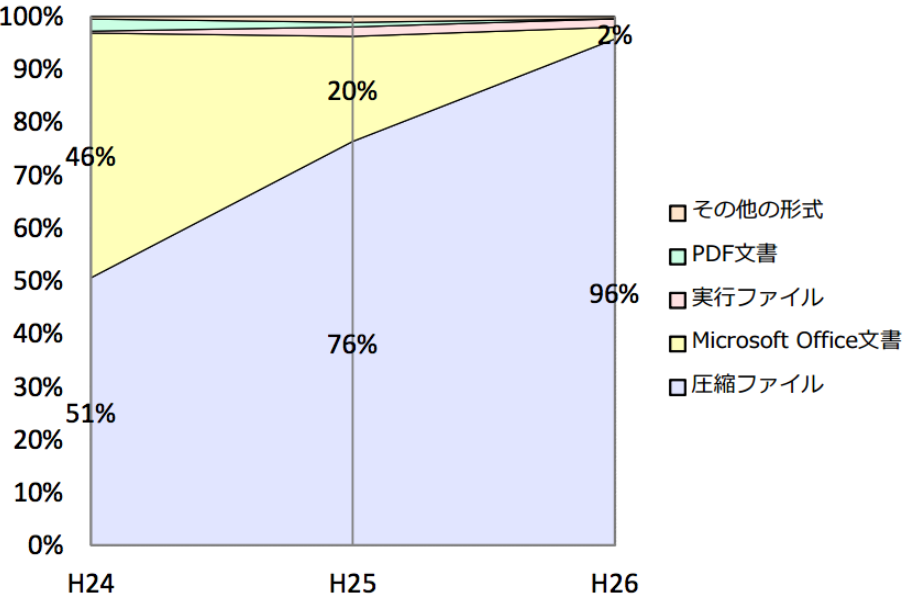
標的型メールによる攻撃の推移



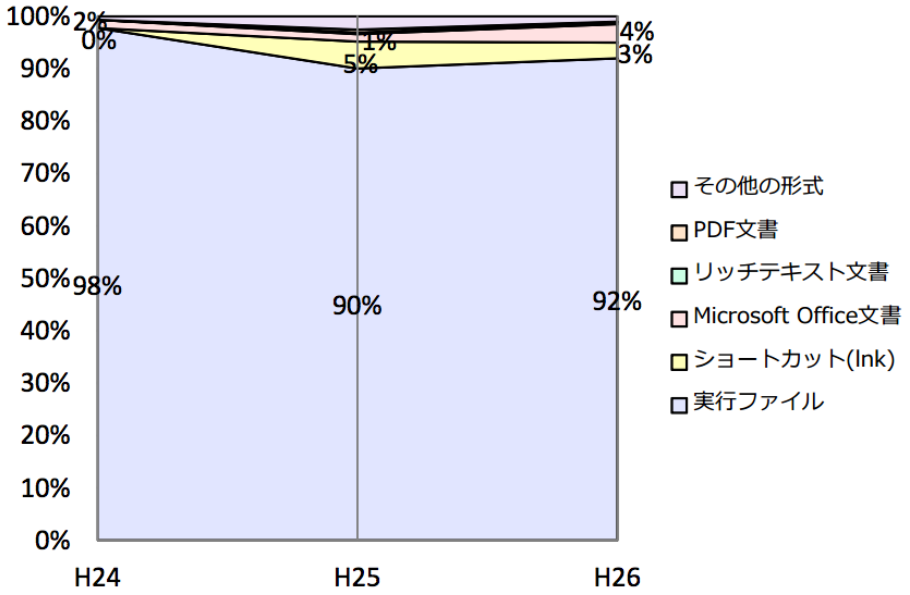
【図２－２　警察が把握した標的型メール攻撃の件数】



【図２－３　フリーメールアドレスを送信元とする標的型メール攻撃の割合】



【図２－４　標的型メールに添付されたファイル形式の傾向】



【図２－５　圧縮ファイルに格納されたファイル形式の傾向】

https://www.npa.go.jp/kanbou/cybersecurity/H26_jousei.pdf

2013年から多発した不正侵入・ID漏洩

サービス	公表日	対象件数	対応
Twitter	**2/4**	**25万件**	**該当アカウントのPWをリセット**
Evernote	**3/4**	**5000万件**	**全アカウントのPWをリセット**
JINS	**3/15**	**2059件**	**補償・カード再発行手数料を負担**
Goo	4/4	10万件	該当アカウントをロック
Tポイント	4/8	299件	該当IDを利用停止しポイントを回復
JR東日本	4/17	97件	ログイン停止措置後、利用者に連絡
資生堂	5/22	682件	ログイン停止措置後、利用者に連絡
ヤフー	**5/23**	**148.6万件**	**流出可能性のあるPW、QAの削除**
三越・伊勢丹	**5/27**	**8289件**	**サイト上で利用者にPW変更を要請**
阪神・阪急	**5/29**	**2382件**	**メール連絡しコールセンターを設置**
トヨタ	**6/20**	**漏洩なし**	**ウイルス感染の確認を呼び掛け**
任天堂	7/5	2.4万件	個別に連絡し仮PWを再発行
コナミ	7/10	35252件	ログイン停止措置後、利用者に連絡
楽天	7/10	非公表	不正利用された利用者にポイント返還
OCN	**7/24**	**400万件**	**メール以外のサービスを一時停止**
アメーバ	8/13	243266件	個別連絡しPW変更を依頼
2ちゃんねる	**8/26**	**4.9万件**	**申込受付・ログインの停止**
Adobe	**10/3**	**3800万件**	**該当する利用者に連絡しPWをリセット**

2013年にヤフーで発生した標的型攻撃

- **2013年4月**
  ポータルサイトを管理するシステムへの不正アクセス検知
  ユーザー情報の一部を抽出する不正プロセスを検知し遮断
  データの漏洩はなし

- **2013年5月**
  別手法でのシステムへの再度の不正アクセスを検知
  最大2,200万件のIDと、そのうち149万件の不可逆暗号化されたパスワード、パスワード再設定に必要な情報の一部が流出した可能性

- **2013年10月**
  ゼロデイ攻撃を検知
  社内用の管理サーバ上でのパスワードダンプを検知し遮断
  サービスおよびユーザーへの影響なし
  分析の結果マルウェア感染と水のみ場攻撃を確認

2013年5月23日

ヤフー株式会社

「当社サーバへの不正なアクセスについて」(5/17発表)の追加発表

[illegible]「当社サーバへの不正なアクセスについて」の件で、引き続き調査を続けていたところ、新たに前回の最大2200万ID(Yahoo! JAPAN総ID数 約2億)のうち、148.6万件について、ユーザ情報が抽出されたパスワードリマインダを悪用した第三者による再設定[illegible]

[illegible]

これらの情報だけではYahoo! JAPAN IDを使ってログインすることはできませんが、ユーザーの皆様にご心配をおかけすることとなってしまったことを深くお詫び申し上げます。

本日19時より、秘密の質問を利用してパスワードを再設定するための機能を一時的に停止しました。また、対象のIDの利用者に対して、5月24日の早朝を目途に強制的にパスワードと秘密の質問をリセットいたしますので、ユーザーの皆様にはログイン時に表示される再設定画面の案内にしたがって、ご自身で再設定の手続きをお願いいたします。

対象のIDかどうかの確認はこちら

[illegible]

また、今回、対象IDではない方についても、今後安心してサービスをご利用頂くため、下記リンク先[illegible]る対策を講じることをご一考いただければ幸いです。

もっと安全ガイド

[illegible]

弊社では、今回の事態を深刻に受け止め、全社を挙げて引き続き再発防止策を速やかに実行してまいります。

マイナンバーの利用シーン

※現時点で想定されているものであり、今後の検討過程において変更があり得るものである。

誕生

通知カード(イメージ)
個人番号　○○……○○
生年月日　○年□月△日
性別　男
氏名　番号太郎
住所　△県○市□町1-1-1

【通知カード】
- 市町村長は、住民票に住民票コードを記載したときは、速やかに、個人番号を指定し、その者に対し、当該個人番号を通知カードにより通知しなければならない。

個人番号を通知　1234 …

市役所

個人番号カード交付申請

個人番号カードの交付

【個人番号カード】
- 希望する者に対し、市町村長が交付。
- 氏名、住所、性別、生年月日、個人番号のほか、顔写真を表示。
- カード1 枚で本人確認と個人番号の確認が可能。

（表面）
（裏面）

年金事務所

住民票、課税証明書の添付を省略可能。

厚生年金の裁定請求の際に番号を提示

国民健康保険加入手続きの際に番号を提示

退職前に加入していた健康保険の被保険者資格喪失証明書の添付を省略可能。

退職

従業員やその扶養家族の番号を源泉徴収票に記載し、市役所や税務署に提出

源泉徴収票
1234 …… …

会社

児童手当の認定請求の際に番号を提示

年金手帳や健康保険証の添付を省略可能。

子育て

扶養家族の番号を会社に提示

学校

奨学金の申請の際に番号を提示

アルバイト先や会社に番号を提示

国民年金の第3号被保険者の認定、健康保険の被扶養者認定の手続きの際に、課税証明書の添付を省略可能。

高等学校等就学支援金申請手続きの際に番号を提示

住民票や保護者等の課税証明書の添付を省略可能。

高校生　大学生等　就職　結婚

関連法規における民間に対する罰則

	行為	マイナンバー法の法定刑	同種法律における類似既定の罰則		
			行政機関個人情報保護法・独立行政法人等個人情報保護法	個人情報保護法	住民基本台帳法
番号の取扱者が対象	個人番号利用事務、個人番号関係事務などに従事する者や従事していた者が、**正当な理由なく、業務で取り扱う個人の秘密が記録された特定個人情報ファイルを提供**	**4年以下の懲役 200万以下の罰金（併科あり）**	**2年以下の懲役 100万以下の罰金**	–	–
	個人番号利用事務、個人番号関係事務などに従事する者や従事していた者が、**業務に関して知り得たマイナンバーを自己や第三者の不正な利益を図る目的で提供し、または盗用**	**3年以下の懲役 150万以下の罰金（併科あり）**	**1年以下の懲役 50万以下の罰金**	–	**2年以下の懲役 100万以下の罰金**
誰でも対象	人を欺き、人に暴行を加え、人を脅迫し、又は、財物の窃取、施設への侵入等により個人番号を取得	3年以下の懲役 or150万以下の罰金	–	–	–
	委員会から命令を受けた者が、委員会の命令に違反	2年以下の懲役or50万以下の罰金	–	6月以下の懲役 30万以下の罰金	1年以下の懲役 50万以下の罰金
	委員会による検査等に際し、虚偽の報告、虚偽の資料提出をする、検査拒否等	1年以下の懲役or50万以下の罰金	–	30万以下の罰金	30万以下の罰金
	偽りその他不正の手段により個人番号カードを取得	6月以下の懲役or50万以下の罰金	–		30万以下の罰金

過失による個人番号の漏洩に対して刑事罰が科される訳ではない

個人番号を取得する際の留意事項

利用目的はきちんと明示！

・マイナンバーを取得する際は、利用目的を特定して明示（※）する必要があります。
（例）「源泉徴収票作成事務」「健康保険・厚生年金保険届出事務」

・源泉徴収や年金・医療保険・雇用保険など、複数の目的で利用する場合は、まとめて目的を示しても構いません。

※　個人番号を取得するときは、個人情報保護法第18条に基づき、利用目的を本人に通知又は公表する。また、本人から直接書面に記載された個人番号を取得する場合は、あらかじめ、本人に対し、その利用目的を明示する。

本人確認は成りすまし防止のためにも厳格に！

・マイナンバーを取得する際は、他人の成りすまし等を防止するため、厳格な本人確認を行います。

・本人確認では、①正しい番号であることの確認（番号確認）と②手続を行っている者が番号の正しい持ち主であることの確認（身元確認）を行います。

番号確認だけでなく身元確認も必要

個人番号の確認

個人番号カード

通知カード or **番号付き住民票** 等

※　上記が困難な場合は、過去に本人確認の上で作成したファイルの確認

等

身元（実存）の確認

運転免許証 or **パスポート** 等

※　上記が困難な場合は、健康保険の被保険者証と年金手帳などの２つ以上の書類の提示

等

※　雇用関係にあるなど、人違いでないことが明らかと個人番号利用事務実施者が認めるときは、身元（実存）確認書類は要しない

個人番号だけを詐取したところで他人になりすませる訳ではない

求められる安全管理措置

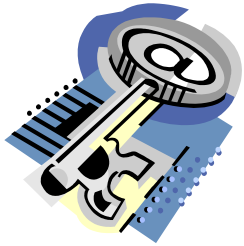
【安全管理措置】
○事業者は、マイナンバー及び特定個人情報の漏えい、滅失又は毀損の防止その他の適切な管理のために、必要かつ適切な安全管理措置を講じなければなりません。また、従業者に対する必要かつ適切な監督を行わなければなりません。
○中小規模事業者に対する特例を設けることにより、実務への影響に配慮しています。

基本方針の策定
取扱規程等の策定

＜組織体制例＞
責任者〇〇課長

事務取扱
担当□□係

事務取扱
担当者▲▲



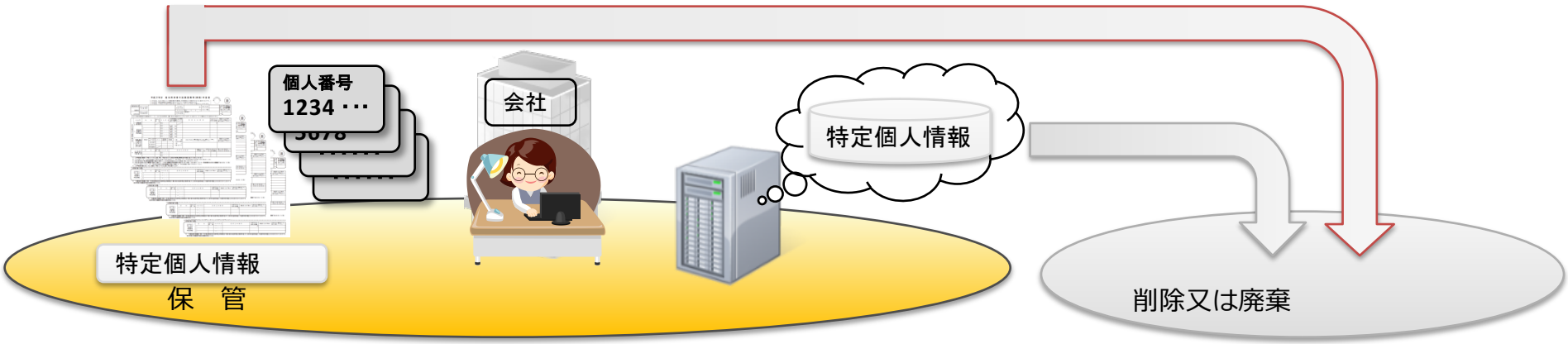
組織的安全管理措置

人的安全管理措置

物理的安全管理措置

技術的安全管理措置

マイナンバーの保管・廃棄に関する規定



【特定個人情報の保管制限】
○法律で限定的に明記された場合を除き、特定個人情報を保管してはなりません。

【特定個人情報の収集・保管制限（廃棄）】
○法律で限定的に明記された場合を除き、特定個人情報を収集又は保管することはできないため、社会保障及び税に関する手続書類の作成事務を処理する必要がなくなった場合で、所管法令において定められている保存期間を経過した場合には、マイナンバーをできるだけ速やかに廃棄又は削除しなければなりません。

名簿屋が本人の許諾なく個人番号を保有しているだけで違法

ヤフーにおけるマイナンバー対応

経営陣の理解とタスクの洗い出し、責任者の設置

- Yahoo! JAPANではCISOが全体を把握し、関連部署が対応

各部門での対応

- 情報セキュリティー部門
  - 情報区分をはじめとした規定類の見直し
  - 関連会社の実情把握・対応体制の確認
- 人事部門・財務部門
  - 関連する業務の洗い出し、業務フロー等の検討
- 情報システム部門
  - 影響するパッケージの対応状況などの情報収集
  - 改修計画の策定・改修の実施

対応にあたっての主要な論点

- 特定個人情報の取扱ルール
  - 保管場所・情報システムでの取扱ルール
  - 個人番号つき書類を扱う居室等の物理的安全管理措置
- 従業員からの個人番号の取得時期
  - 2015年10月からか、2016年1月か、それ以降か
- 個人番号の受け渡し方法 （従業員・個人事業主）
  - 電子メール等で個人番号を受け取るとライフサイクル管理が困難
- 個別システム・帳票などの対応
  - パッケージの番号対応・バージョンアップ計画はどうなっているか
  - これまでExcelで回してきた業務をどうするか
- 関連会社についての情報の把握
  - 人事・経理などバックオフィス業務を統合してるか
  - ISMS グループ認証を取得しているか
- 金融系子会社における顧客からの個人番号取得
  - 新規顧客の登録時における個人番号取得
  - 既存顧客からの個人番号取得の時期

実際やってみての所感など

全てをベンダー任せにできる訳ではない

- アウトソーシングを活用する場合であっても何を外部ベンダーに任せることができて、何を社内で実施する必要があるのか、よくよく確認が必要となる
- 人事系のパッケージはおおむね個人番号に対応するが、カスタマイズ部分の影響や個人事業主との取引や謝金の支払いなどでの対応は要注意

まずは責任者の設置と業務の洗い出しから

- 番号関係事務は人事・経理・情報システムにまたがる

だいたいISMSを回していれば対応できるが…

- 「廃棄」を確実に実施するためには、個人番号の保存は局所化することが望ましい
- 税関係情報の保存期間は7年、廃棄処理のバッチを作り込んだとしても実際に回し始めるのはかなり先となる

マイナンバーは攻撃者から狙われるのか

- 詐取したところで悪用して利益を得ることが難しい
  - 気に入らない相手が隠している所得を勝手に税申告するとか？
- 不当な目的での提供や盗用自体に刑事罰を科しており、名簿屋が扱うには法的リスクが個人情報と比べて大きい
  - 個人情報の転売と比べて刑事事件としての立件が容易
- 自己情報を照会するには個人番号カードとPINが必要
  - 配偶者にヘソクリや過去の経歴がバレたりすることはない

- クレジットカード番号やID・パスワードと比べると、盗用した場合の経済的利益は小さく、転売の法的リスクが大きな制度となっている
- 番号が民間も含めて広く利用され、盗用することの利益が大きい米国・韓国と比べてリスクは限定的

IoT時代へ向けた新たな脅威（時間があれば）