第19回
サイバー犯罪に関する
白浜シンポジウム
19th SHIRAHAMA CYBER CRIME SYMPOSIUM
& 第10回 情報危機管理コンテスト
10th CRISIS MANAGEMENT CONTEST

2015. 5/21(木)～23(土)

この1年のサイバーセキュリティ関連の立法と裁判例

弁護士　国立情報学研究所客員教授　JPCERT/CC理事

岡村久道　（情報学博士）

過去1年間におけるICT関連立法

- ICTに関する法整備は次の3種類に大別
- アクセル役とブレーキ役が混在

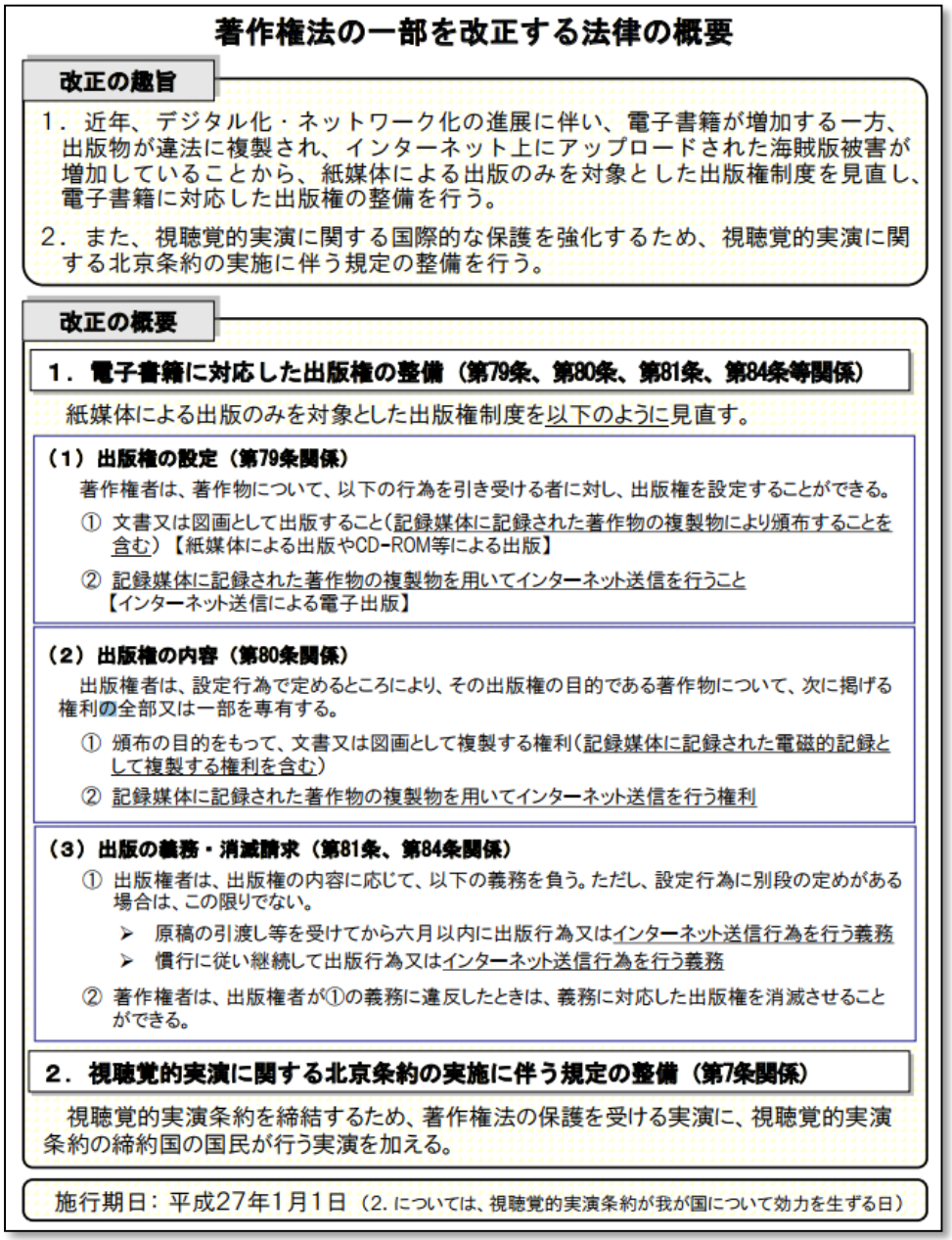
1. ICTの利活用を推進するためのもの（アクセル役）
   - **電波法（改正）**←新たな無線システムに関し、ICTインフラとしての普及促進等のため、電波利用料についての利用料低減等を図る
   - **著作権法（改正）**← 電子出版への対応
   - **放送法（改正）**← NHKのインターネット活用業務の拡大等

2. 違法・有害情報対策（ブレーキ役）
   - **児童ポルノ法（改正）**← 児童ポルノ所持罪の新設等
   - **私事性的画像記録の提供等による被害の防止に関する法律（新法）**← リベンジポルノ対策

3. **サイバーセキュリティ対策（ブレーキ役）**
   - **電気通信事業法（改正）**
   - **サイバーセキュリティ基本法（新法）**

参考－電波法平成26年改正

- 平成26年4月23日公布。
- 主として、電波の有効利用を促進する観点から、電波利用料について料額の見直しを図る。
- 具体的には、
  1. 携帯電話関係について新たに電波利用料の軽減係数が導入され、それによって関係事業者の負担軽減が図られた。
  2. スマートメーターやM2M等の新たな無線システムに関し、ICTインフラとしての普及促進のため、電波利用料に上限額を設定。
  3. 音声によって災害発生を住民に伝達する同報系デジタル防災行政無線、ホワイトスペースを用いたエリア放送の電波利用料について利用料低減。
- 他にも、ラジオ放送の難視聴解消を目的として、小電力のFM中継局整備に対する支援が電波利用料の使途に追加され、技術基準適合証明等の表示方法に係る規定が整備される等の措置。



著作権法の一部を改正する法律の概要

改正の趣旨

1．近年、デジタル化・ネットワーク化の進展に伴い、電子書籍が増加する一方、出版物が違法に複製され、インターネット上にアップロードされた海賊版被害が増加していることから、紙媒体による出版のみを対象とした出版権制度を見直し、電子書籍に対応した出版権の整備を行う。

2．また、視聴覚的実演に関する国際的な保護を強化するため、視聴覚的実演に関する北京条約の実施に伴う規定の整備を行う。

改正の概要

1．電子書籍に対応した出版権の整備（第79条、第80条、第81条、第84条等関係）

紙媒体による出版のみを対象とした出版権制度を以下のように見直す。

（1）出版権の設定（第79条関係）

著作権者は、著作物について、以下の行為を引き受ける者に対し、出版権を設定することができる。

① 文書又は図画として出版すること（記録媒体に記録された著作物の複製物により頒布することを含む）【紙媒体による出版やCD-ROM等による出版】

② 記録媒体に記録された著作物の複製物を用いてインターネット送信を行うこと【インターネット送信による電子出版】

（2）出版権の内容（第80条関係）

出版権者は、設定行為で定めるところにより、その出版権の目的である著作物について、次に掲げる権利の全部又は一部を専有する。

① 頒布の目的をもって、文書又は図画として複製する権利（記録媒体に記録された電磁的記録として複製する権利を含む）

② 記録媒体に記録された著作物の複製物を用いてインターネット送信を行う権利

（3）出版の義務・消滅請求（第81条、第84条関係）

① 出版権者は、出版権の内容に応じて、以下の義務を負う。ただし、設定行為に別段の定めがある場合は、この限りでない。

- 原稿の引渡し等を受けてから六月以内に出版行為又はインターネット送信行為を行う義務
- 慣行に従い継続して出版行為又はインターネット送信行為を行う義務

② 著作権者は、出版権者が①の義務に違反したときは、義務に対応した出版権を消滅させることができる。

2．視聴覚的実演に関する北京条約の実施に伴う規定の整備（第7条関係）

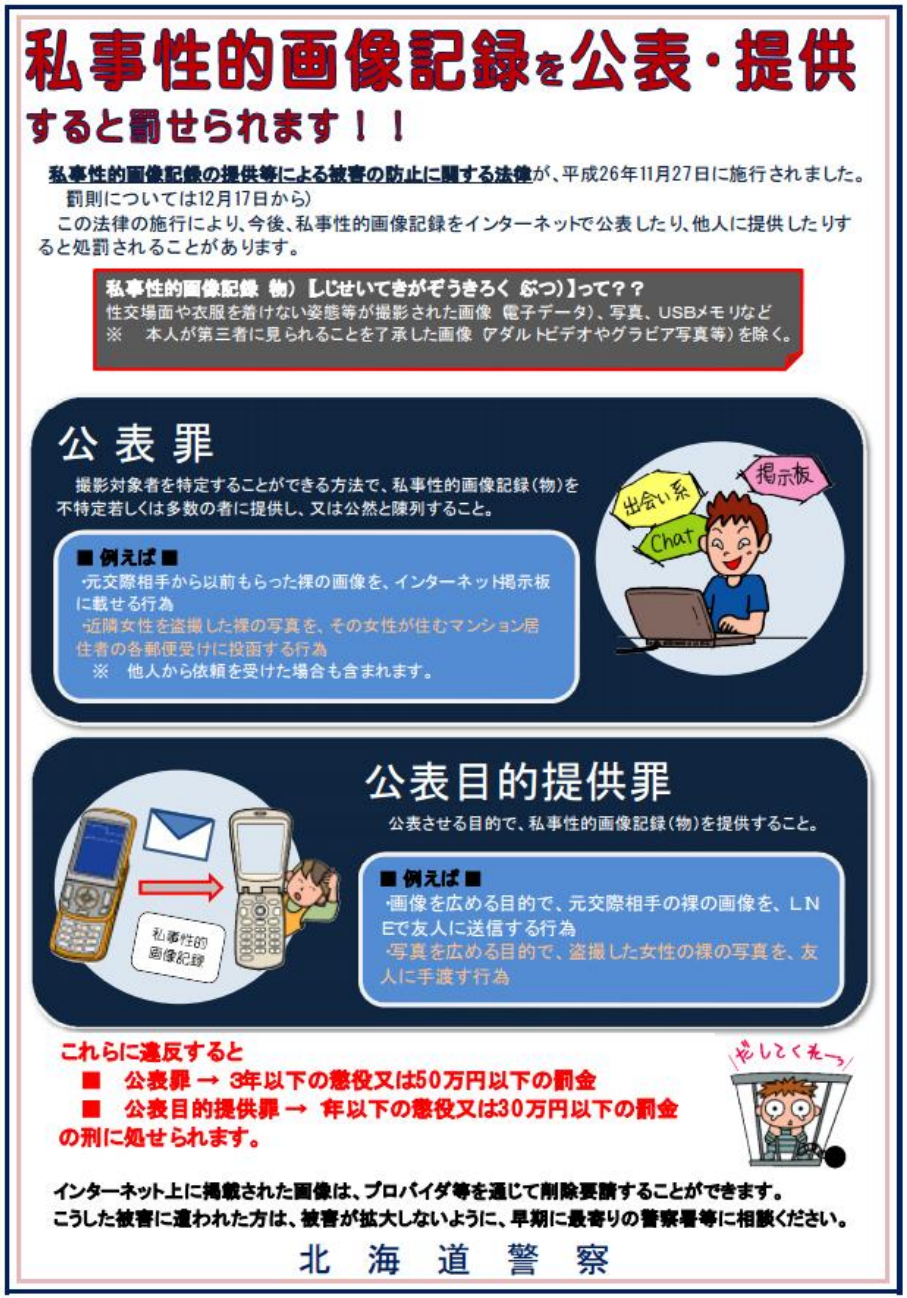
視聴覚的実演条約を締結するため、著作権法の保護を受ける実演に、視聴覚的実演条約の締約国の国民が行う実演を加える。

施行期日：平成27年1月1日（2.については、視聴覚的実演条約が我が国について効力を生ずる日）

出典･文化庁サイト

参考－著作権法平成26年改正の概要

電子書籍に対応した出版権の整備（第79条、第80条、第81条、第84条等関係）が中心。



出典･北海道警サイト

参考ー「私事性的画像記録の提供等による被害の防止に関する法律」（リベンジポルノ防止法）の概要

「近時、交際中に撮影した元交際相手の性的画像（私事性的画像記録）等をその撮影対象者の同意なく、インターネットを利用するなどして公表する行為により、被害者が長期にわたり多大な精神的苦痛を感じる事案が多数生じているという実情に鑑み、個人の名誉及び私生活の平穏（プライバシー）の侵害による被害の発生又はその拡大を防止するため、私事性的画像記録の提供等を処罰するとともに、私事性的画像記録に係る情報の流通によって名誉又は私生活の平穏の侵害があった場合における……プロバイダ責任制限法……の特例及び当該提供等による被害者に対する支援体制の整備等について定める」（警察庁サイト）

電気通信事業法平成26年改正とサイバーセキュリティ１

電気通信事業法の改正の背景等について

1

○ 今日の電気通信ネットワークは、携帯電話を中心とする多様なサービスの提供により**設備の構成が複雑化**※1し、また、スマートフォンの普及等により、**通信量が急増**※2。

※1 携帯では、音声網とデータ網が並存。更に、データ網では、通信速度(高速:3G、超高速:3.9G)や端末を機能させる基本ソフト(アンドロイドOS、iOS)ごとに設備が並存。

※2 移動通信の通信量は、**1年間で約1.7倍、3年間で約7.7倍増加。**

○ このため、電気通信サービスの**重大事故**(2時間以上かつ3万人以上の事故)は、**平成20年度以降、毎年15件以上**発生し、**10年前**(平成15年度。7件)**に比べて、倍以上の件数で推移**するとともに、**規模が拡大**※3。

※3 H24年度は、重大事故が**17件発生。**
H23年度は、約半数の事故が**100万人以上**に影響。H24年度は、半数超の事故が**半日以上**継続、**移動通信・ネット関連**の事故が**増加**(ともに41%)。

○ 現行の電気通信設備の**技術基準等は**、電気通信事業法の制定時(昭和59年)に、**固定電話の事故対策を中心**に規定。今日の電気通信ネットワークでは、**携帯電話やインターネットを利用したサービスなど多様なサービスが提供**され、法制定時とは**状況が大きく変化。**

○ このような状況を踏まえ、総務省では、平成25年4月から、**事故防止の在り方を検討**する**有識者検討会**※4を開催。本検討会は、同年**10月に報告書**を取りまとめ。**今回の改正**は、**当該報告書に基づき行うもの。**

※4 「多様化・複雑化する電気通信事故の防止の在り方に関する検討会」:
座長:酒井善則(放送大学特任教授東京渋谷学習センター所長)。座長を含め構成員6名。計7回開催。

○ 具体的には、**事業者の自主的な取組による事故防止を基本**としつつ、**その取組を適切に確保する制度的枠組みを整備**する観点から、事故防止に係る措置の①**内容の充実**や②**対象の見直し**を行うもの。

出典･総務省サイト

電気通信事業法平成26年改正とサイバーセキュリティ 2

電気通信事業法の改正内容について

2

1.「管理規程」の実効性確保

・ 事業者ごとに事故防止の取組を作成・届出させる「**管理規程**」(自主基準)**の記載事項として、全社的・横断的な「設備管理の方針・体制・方法」等を規定。**これにより、設備管理が専門化・細分化し、設備管理の縦割り化が進む中で多発する「設備全体の不整合(関連設備間の設定値の誤設定等)に起因する事故」を防止。

・ 「管理規程」の**変更命令や遵守命令を追加。**これにより、事業者が「管理規程」を適切に見直さない場合等の**是正措置を確保。**

2. 経営レベルの「電気通信設備統括管理者」の導入

・ 設備管理の専門化・細分化や外部委託等が進む中で、社内の部門間や社外を含めた全体調整、事故防止の方針・体制・方法等への経営陣の主体的関与の強化を図るため、**経営レベルの責任者として、「電気通信設備統括管理者」の選任を義務付け。**

3.「電気通信主任技術者」による監督の実効性確保(現場の監督機能の強化)

・ 現場の設備管理の監督責任者である「**電気通信主任技術者**」について、その**具体的な職務内容を総務省令で定め、権限を明確化。**(現行法上、その職務は、設備の「工事、維持・運用」の監督とのみ規定され、具体的に担うべき職務が不明確)

・ 電気通信事業者に対し、選任した**電気通信主任技術者が、**ネットワーク関連技術の変化の中、**監督に必要な専門知識を維持・向上できるよう、登録講習機関が行う**設備の「工事、維持・運用」の監督に関する**講習を受講させることを義務付け。**

4. 回線非設置事業者※への対応

・ **回線非設置事業者のうち、国民生活に重要な役割を果たすサービス**(有料かつ大規模なサービス)**を提供する者には、回線設置事業者と同様の事故防止の規律**(技術基準、管理規程、電気通信設備統括管理者、電気通信主任技術者)**を課す**ことにより、利用者保護を実現。

※ 自らは通信回線を保有せず、通信回線を有している事業者(回線設置事業者。NTT東西等)から通信回線を借りてサービス提供する事業者。ネット関連事業者等。

出典･総務省サイト

セキュリティ領域への追い風になるか？
ー新たにサイバーセキュリティ基本法が制定・施行

- 平成26年11月6日に第187回国会で可決・成立。全面施行済み。
- 背景
  - IT・ICTはもはや不可欠の社会基盤であるが、脅威は増大・深刻化
  - 平成12年成立のIT基本法では、高度情報通信ネットワーク社会の形成というアクセルに重点が置かれる半面、ブレーキの側面としては「安全性の確保等」（同法22条）が謳われる程度にとどまり、サイバーセキュリティ施策の司令塔となるべき政府機関をはじめ、推進体制に関する明確な法的根拠すら乏しかった。
  - IT基本法の制定から14年の歳月を経て、IT・ICTを取り巻く諸情勢が大きく変化したことに鑑み、新たな時代に即した施策が求められてきた。
  - 東京オリンピック・パラリンピックに向けた大きな課題。
- 目的（1条）
  - 「諸情勢の変化に伴い、情報の自由な流通を確保しつつ、サイバーセキュリティの確保を図ることが喫緊の課題となっている状況」に鑑み、IT基本法と相まって、我が国のサイバーセキュリティの施策を総合的・効果的に推進し、もって、①経済社会の活力の向上・持続的発展、②国民の安全・安心に暮らせる社会の実現、③国際社会の平和及び安全の確保並びに④我が国の安全保障への寄与を目的。

サイバーセキュリティとは何か？－定義（2条）

次の措置が講じられ、その状態が適切に維持管理されていることとして定義。

1. 電磁的方式により記録され、又は発信・伝送・受信される**情報**の安全管理に必要な措置
2. **情報システム**及び**情報通信ネットワーク**の安全性・信頼性の確保に必要な措置←（電磁的記録媒体を通じた電子計算機に対する不正な活動による被害の防止のために必要な措置を含む－同条括弧書き）
   ←スタックスネット事件

- 客体（対象）→ 情報それ自体、情報システム、情報通信ネットワークを網羅
- 守るべきもの → 安全（性）・信頼（性）の管理・確保
- 行うべきこと → それに必要な措置全般

- そのため、サイバーテロはもとより、不正送金被害や内部不正等も含んだ、極めて広い概念

サイバーセキュリティ基本法の概要

第Ⅰ章．総則

■目的（第1条）

■定義（第2条）

⇒「サイバーセキュリティ」について定義

■基本理念（第3条）

⇒ サイバーセキュリティに関する施策の推進にあたっての基本理念について次を規定

① 情報の自由な流通の確保を基本として、官民の連携により積極的に対応

② 国民1人1人の認識を深め、自発的な対応の促進等、強靭な体制の構築

③ 高度情報通信ネットワークの整備及びITの活用による活力ある経済社会の構築

④ 国際的な秩序の形成等のために先導的な役割を担い、国際的協調の下に実施

⑤ IT基本法の基本理念に配慮して実施

⑥ 国民の権利を不当に侵害しないよう留意

■関係者の責務等（第4条～第9条）

⇒ 国、地方公共団体、重要社会基盤事業者（重要インフラ事業者）、サイバー関連事業者、教育研究機関等の責務等について規定

■法制上の措置等（第10条）

■行政組織の整備等（第11条）

第Ⅱ章．サイバーセキュリティ戦略

■サイバーセキュリティ戦略（第12条）

⇒ 次の事項を規定

① サイバーセキュリティに関する施策の基本的な方針

② 国の行政機関等におけるサイバーセキュリティの確保

③ 重要インフラ事業者等におけるサイバーセキュリティの確保の促進

④ その他、必要な事項

⇒ その他、総理は、本戦略の案につき閣議決定を求めなければならないこと等を規定

第Ⅲ章．基本的施策

■国の行政機関等におけるサイバーセキュリティの確保（第13条）

■重要インフラ事業者等におけるサイバーセキュリティの確保の促進（第14条）

■民間事業者及び教育研究機関等の自発的な取組の促進（第15条）

■多様な主体の連携等（第16条）

■犯罪の取締り及び被害の拡大の防止（第17条）

■我が国の安全に重大な影響を及ぼすおそれのある事象への対応（第18条）

■産業の振興及び国際競争力の強化（第19条）

■研究開発の推進等（第20条）

■人材の確保等（第21条）

第Ⅲ章．基本的施策（つづき）

■教育及び学習の振興、普及啓発等（第22条）

■国際協力の推進等（第23条）

第Ⅳ章．サイバーセキュリティ戦略本部

■設置等（第24条～第35条）

⇒ 内閣に、サイバーセキュリティ戦略本部を置くこと等について規定

附則

■施行期日（第1条）

⇒ 公布の日から施行（ただし、第Ⅱ章及び第Ⅳ章は公布日から起算して1年を超えない範囲で政令で定める日）する旨を規定

■本部に関する事務の処理を適切に内閣官房に行わせるために必要な法制の整備等（第2条）

⇒ 情報セキュリティセンター（NISC）の法制化、任期付任用、国の行政機関の情報システムに対する不正な活動の監視・分析、国内外の関係機関との連絡調整に必要な法制上・財政上の措置等の検討等を規定

■検討（第３条）

⇒ 緊急事態に相当するサイバーセキュリティ事象等から重要インフラ等を防御する能力の一層の強化を図るための施策の検討を規定

■IT基本法の一部改正（第４条）

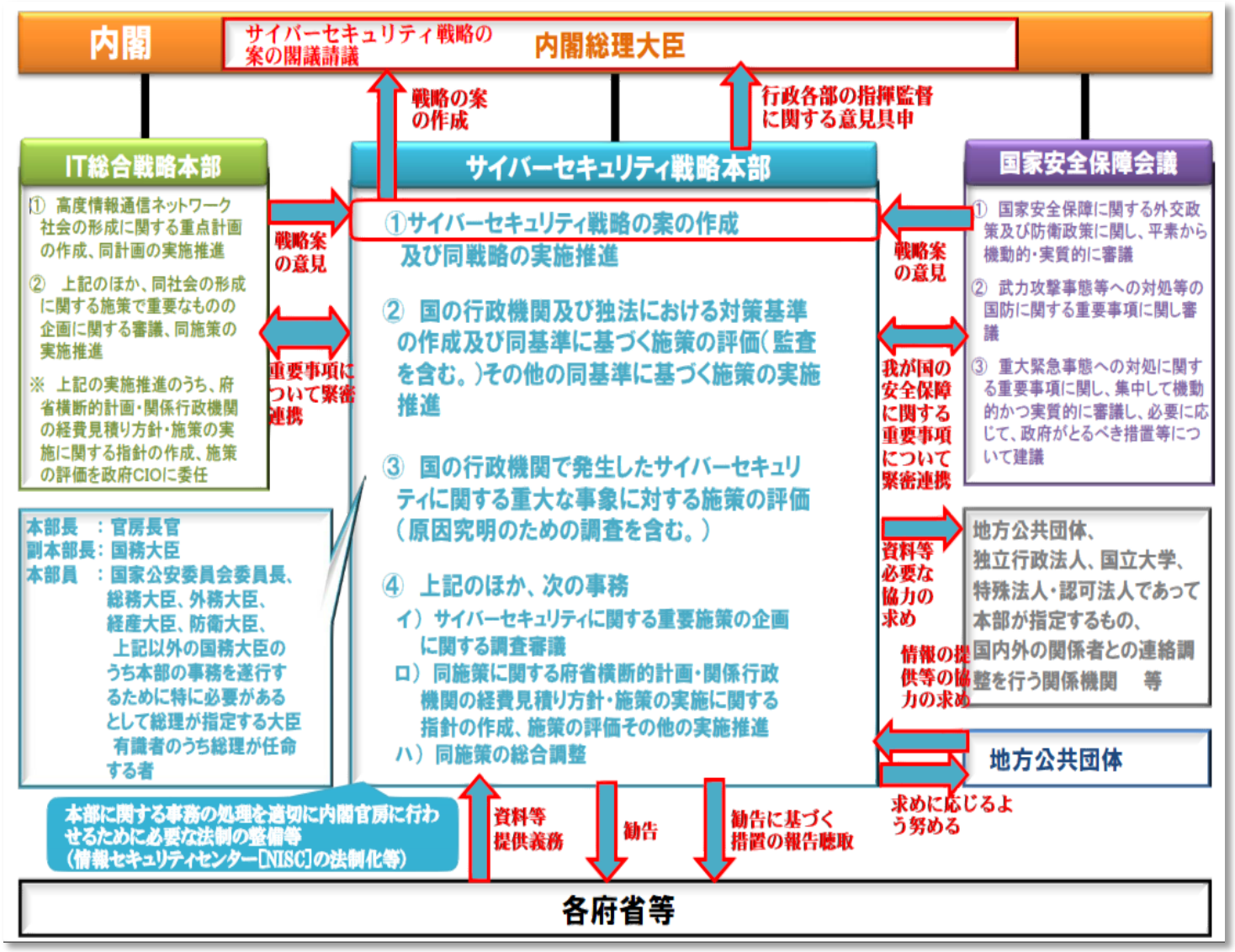
⇒ IT戦略本部の事務からサイバーセキュリティに関する重要施策の実施推進を除く旨規定

出典･NISCの公表資料

サイバーセキュリティ基本法の特色等

- 国の主導的役割
  - IT基本法7条は民間主導を原則としていたが、本法は官民一体の連携（16条）を謳いつつ、国の主導的役割を示す。
- 政府の司令塔の明確化
  - サイバーセキュリティ戦略本部の設置　→　後述
- 重要インフラ等のセキュリティを重視
  - 重要社会基盤事業者（6条）、サイバー関連事業者その他の事業者（7条）、教育研究機関（8条）の責務を定める点に特色。
- 基本法としての性格
  - **今後の本法に基づく施策の実施に必要な法制上の措置等（10条）、行政組織の整備等（11条）は、新たに設置された司令塔（サイバーセキュリティ戦略本部）に委ねられる。**

サイバーセキュリティ戦略本部の機能・権限（イメージ）



出典・NISCの公表資料

今後におけるサイバーセキュリティ領域の法整備

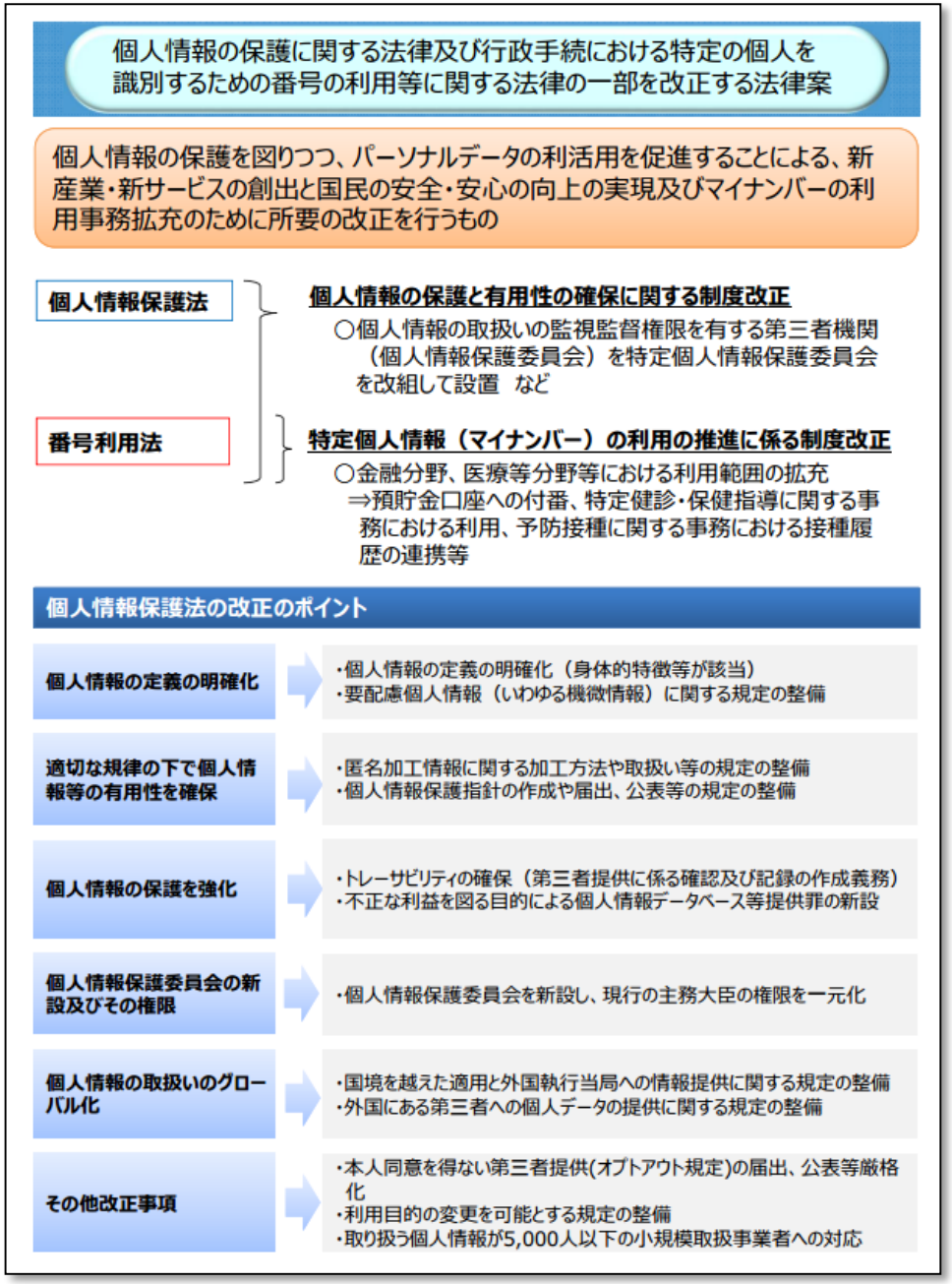
- 個人情報保護法改正案の国会提出
  - これまで個人情報保護法が定める個人データの安全管理措置規定が、サイバーセキュリティに関する実質的な一般法の役割を営んできた。
  - 今回の改正案は、全面施行後約10年を経て、初の大改正。
  - 検討段階で利活用推進派と保護強化派が対立。
  - マイナンバー法の改正とペアリングされた法案。

- 営業秘密の保護強化を図った不正競争防止法改正案の国会提出
  - 保護されるべき情報は個人情報だけではない。
  - 技術ノウハウや顧客名簿の不正漏えい対策も重要。

- 以下、順に説明

個人情報保護法改正案の概要

- 内閣官房「パーソナルデータに関する検討会」で平成25年 9月から改正に向けた検討作業を開始。
- 検討段階で利活用推進派と保護強化派が対立。
- 平成26年6月に検討会での議論を踏まえてIT総合戦略本部が制度改正大綱を公表してパブコメ。
- 平成27年3月10日、最終的な法案を閣議決定。
- 同日、衆議院議案受理。
- マイナンバー法の改正案とカップリングした「個人情報の保護に関する法律及び行政手続における特定の個人を識別するための番号の利用等に関する法律の一部を改正する法律案」という体裁。
- 今後、本格的な国会審議が開始される予定。



出典：内閣官房サイト

個人情報の定義の明確化－個人識別性 1

現行法2条

1　この法律において「個人情報」とは、生存する個人に関する情報であって、当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）をいう。

赤色文字の部分が実質的な変更点

改正案2条（改正案は改正後の個人情報保護法の条項を指しており、以下も同様）

1　この法律において「個人情報」とは、生存する個人に関する情報であって、次のいずれかに該当するものとする。

（一）　当該情報に含まれる氏名、生年月日その他の記述等により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）

（二）　個人識別符号が含まれるもの

2　この法律において「個人識別符号」とは、次のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものとする。

（一）　特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した符号であって、当該特定の個人を識別することができるもの

（二）　個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

個□情報の定義の明確化－個人識別性 2

- 「定義の明確化」という意味
  - 個人情報の定義に赤字部分（個人識別符号）が追加されたことになる。
  - 個人識別符号は、特定の個人を識別することができるものに限定。
  - したがって、現行の保護法の個人情報の定義と実質的に同一。拡張されたわけではない。ただ、明確化されたということ。
  - ただし、後述の「匿名加工情報」とするための方法が、（一）号と（二）号で異なる。

- 残された課題
  - 利活用推進派からすれば満足すべき内容であるのに対し、保護強化派からすれば不満が残る内容。しかし、個人情報概念の拡大は、情報公開法制とのトレードオフになるおそれ。
  - 「符号のうち、政令で定めるもの」として、具体的な内容は政令へ先送り。

個人情報の定義の明確化－要配慮個人情報 1

改正案2条

3　この法律において**「要配慮個人情報」とは、**本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他**本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報**をいう。

改正案17条2項

2　個人情報取扱事業者は、次に掲げる場合を除くほか、**あらかじめ本人の同意を得ないで、要配慮個人情報を取得してはならない。**

一 法令に基づく場合

二 人の生命、身体又は財産の保護のために必要がある場合であって、本人の同意を得ることが困難であるとき。

三 公衆衛生の向上又は児童の健全な育成の推進のために特に必要がある場合であって、本人の同意を得ることが困難であるとき。

四 国の機関若しくは地方公共団体又はその委託を受けた者が法令の定める事務を遂行することに対して協力する必要がある場合であって、本人の同意を得ることにより当該事務の遂行に支障を及ぼすおそれがあるとき。

五 当該要配慮個人情報が、本人、国の機関、地方公共団体、第七十六条第一項各号に掲げる者その他個人情報保護委員会規則で定める者により公開されている場合

六 その他前各号に掲げる場合に準ずるものとして政令で定める場合

個人情報の定義の明確化ー要配慮個人情報 2

- 要配慮個人情報 規定の新設
  - 要配慮個人情報とは、いわゆる機微情報に相当する意味。
  - 現行法には規定がなかったが、EU指令に準じて新設。
  - 取得のために原則として本人同意が必要。

- 残された課題
  - 「政令で定めるもの」として、具体的な内容は政令委任へ。
  - 除外事由についても一部を政令委任。

個□情報の有用性の確保－匿名加工情報 1

- 関係する定義
  - 「匿名加工情報」を「個人を識別できないよう加工したものであり、個人情報を復元できないもの」と定義（改正案2条9項）。
  - 「匿名加工情報データベース等」を、匿名加工情報を含む情報の集合物であって、特定の匿名加工情報を電子計算機を用いて検索することができるように体系的に構成したものその他特定の匿名加工情報を容易に検索することができるように体系的に構成したものとして政令で定めるものと定義（改正案2条10項）。
- 個人情報取扱事業者の義務
  - 匿名加工情報（匿名加工情報データベース等を構成するものに限る。以下同じ。）の作成は、個人情報保護委員会規則で定める基準に従い加工（改正案36条1項）。
  - 個人情報保護委員会規則で定める基準に従い安全管理措置を講じる（改正案36条2項）。
  - 匿名加工情報は本人同意なしに第三者提供が可能だが、匿名加工情報を作成・提供する際は、一定の項目を公表等（改正案36条3項・4項）。
  - 自ら作成した当該匿名加工情報を取り扱うに当たっては、当該匿名加工情報の作成に用いられた個人情報に係る本人を識別するために、当該匿名加工情報を他の情報と照合してはならない（改正案36条5項）。

個□情報の有用性の確保－匿名加工情報 2

- 匿名加工情報取扱事業者の義務
  - 「匿名加工情報取扱事業者」を「匿名加工情報データベース等を事業の用に供している者」と定義（改正案2条10項）。
  - 匿名加工情報は本人同意なしに第三者提供が可能だが、匿名加工情報を作成・提供する際は、一定の項目を公表等（改正案37条）。
  - 本人を識別するために他の情報と照合を禁止（改正案38条）。
    ←再識別化防止のための規定。
  - 安全管理措置を講じる（改正案39条）。
- 残された課題
  - どのように加工すれば足りるのかについては、個人情報保護委員会規則で定める基準が確定するまで待つ必要。

個□情報の保護の強化ートレーサビリティの確保

- トレーサビリティの確保1－第三者提供に係る記録の作成等
  - 個人情報取扱事業者は、個人データを第三者に提供したときは、個人情報保護委員会規則で定めるところにより、当該個人データを提供した年月日、当該第三者の氏名等の記録を作成し、一定の期間保存（改正案25条）。
- トレーサビリティの確保2－第三者提供を受ける際の確認等
  - 個人情報取扱事業者は、第三者から個人データの提供を受けるに際しては、個人情報保護委員会規則で定めるところにより、当該第三者による当該個人データの取得の経緯等を確認するとともに、当該個人データの提供を受けた年月日等の記録を作成し、一定の期間保存（改正案26条）。
- 個□情報データベース等提供罪
  - 個人情報取扱事業者（その者が法人である場合にあっては、その役員、代表者又は管理人）若しくは従業者又はこれらであった者が、その業務に関して取り扱った個人情報データベース等を自己若しくは第三者の不正な利益を図る目的で提供し、又は盗用したときは、1年以下の懲役又は50万円以下の罰金に処する（改正案83条）。
- これらは名簿屋対策という意味も有する。

個人情報保護委員会の新設及びその権限

- 概要
  - 個人情報保護委員会を新設し、タテ割りとなってきた現行の主務大臣の権限を一元化。
  - 立ち入り検査の権限も付与。
  - 認定個人情報保護団体の認定・監督。
  - 政令によって、事業所管大臣への委任が可能。

- 課題
  - 積極的に評価すべき。
  - 個人情報保護委員会の組織強化が課題。
  - 各種業法との関係を整理する必要。

個□情報の取扱いのグローバル化

- 国境を越えた適用と外国執行当局への情報提供に関する規定の整備。
- 外国にある第三者への個□データの提供に関する規定の整備。
- 国内の個人情報を取得した外国企業にも適用。

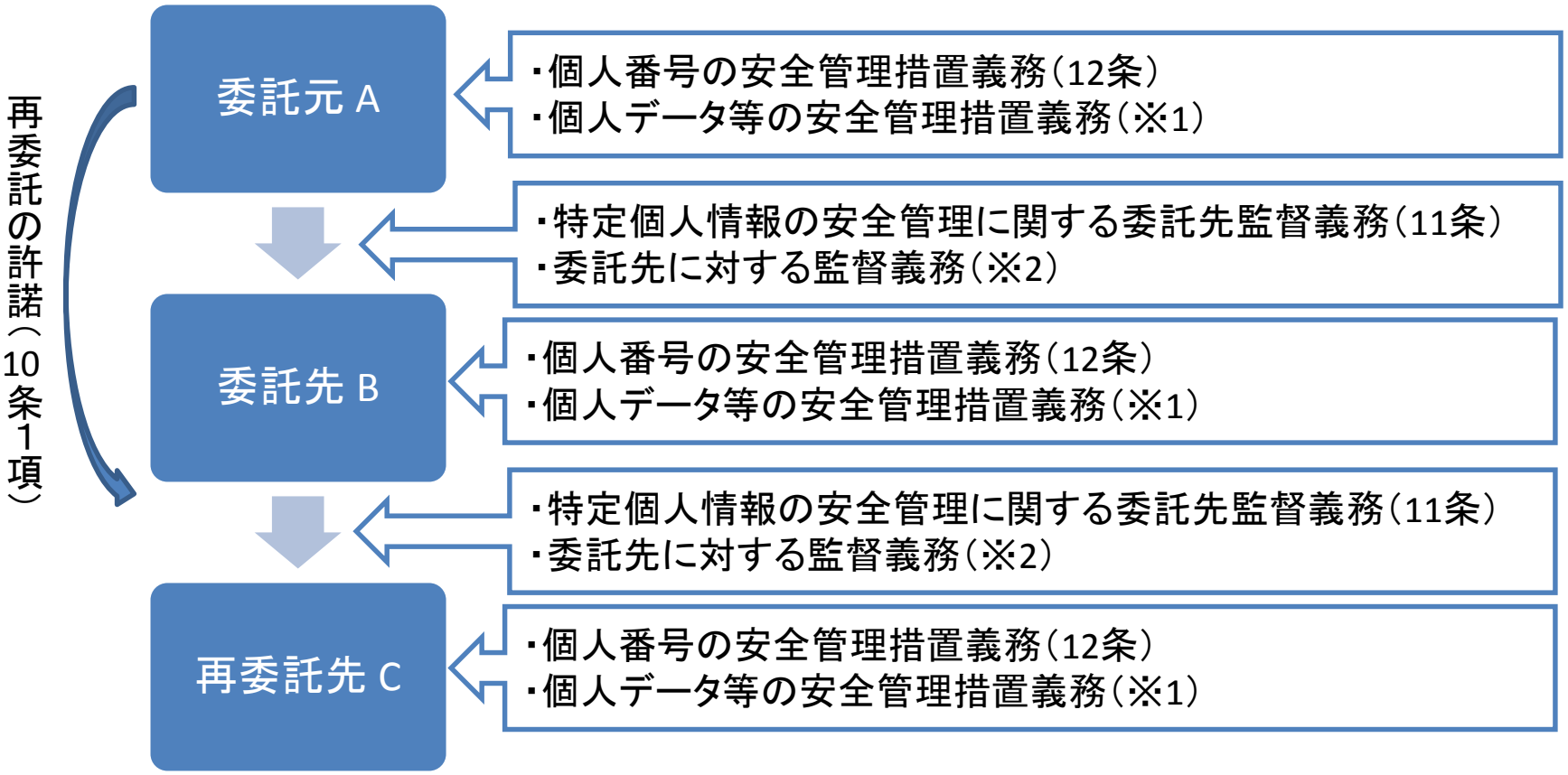
その他改正事項

- 本人同意を得ない第三者提供(オプトアウト規定)の届出、公表等厳格化。
- 取扱う個人情報が5,000人以下の小規模取扱事業者への適用除外を廃止。
- 利用目的の変更を可能とする規定の整備は、消費者団体等からの反対論が強く、今回は見送り。

番号法（マイナンバー法）では、本年（2015年）10月から個人番号通知開始－同法におけるセキュリティ規定の適用関係

	行政機関の長	独立行政法人等	個人情報取扱事業者等
個人番号	**番号法12条** **個人番号利用事務実施者及び個人番号関係事務実施者は、個人番号の漏えい、滅失又は毀損の防止その他の個人番号の適切な管理のために必要な措置を講じなければならない。**		
特定個人情報	行政機関個人情報保護法6条－同法上の保有個人情報	独立行政法人等個人情報保護法7条－同法上の保有個人情報	・個人情報保護法20条（個人情報取扱事業者）－同法上の個人データ ・本法28条（個人情報取扱事業者でない個人番号取扱事業者）－本法上の特定個人情報

再委託の制限、委託先の監督（10条・11条）等

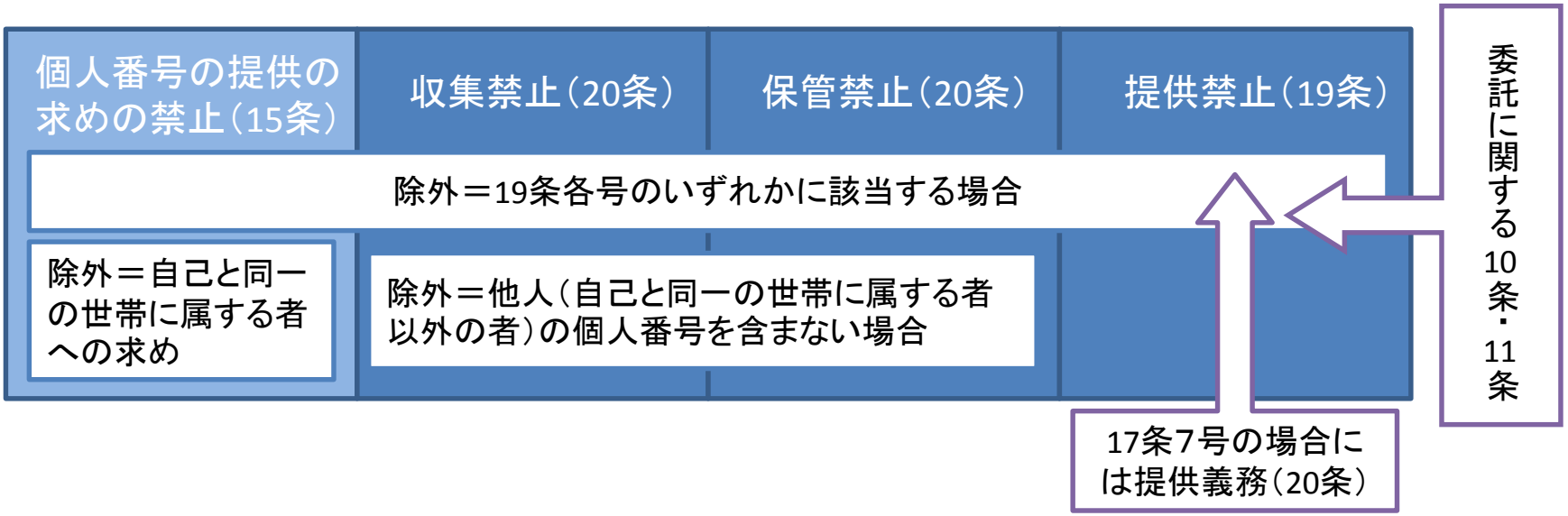


※1 個人情報保護法20条等
※2 個人情報保護法22条等

（出典・岡村久道「共通番号法入門」）

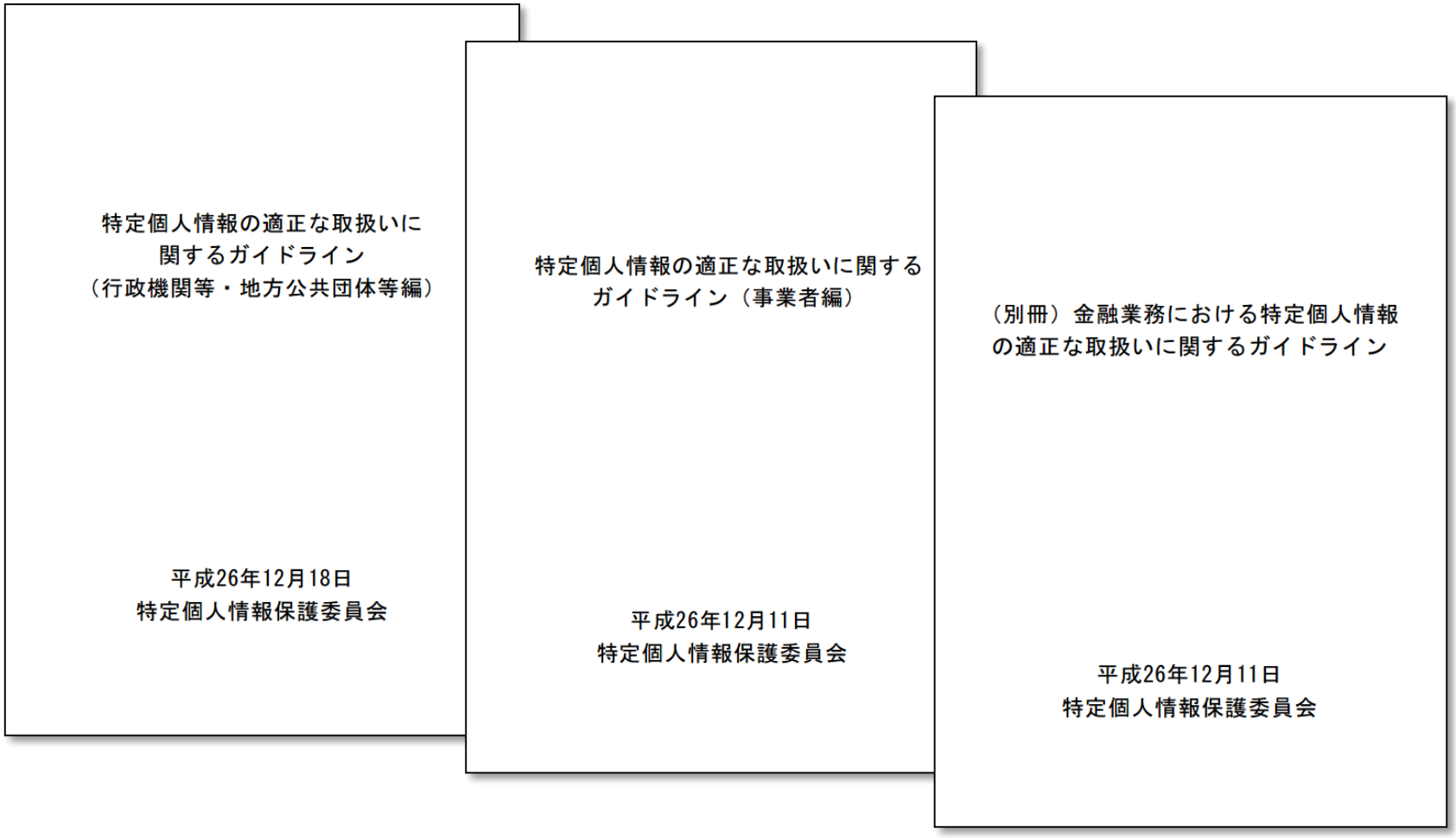
特定個人情報の提供の制限等（19条）

- 19条は、特定個人情報の提供を原則禁止しつつ、例外的に提供が許容される場合として、1号から14号までの事由を規定。
- 本法では、特定個人情報に限定して、個人情報保護3法が定める提供制限条項の適用を、いったん全面的に除外した上で（29条・30条）、新たなルールを定める。
- 各号で提供の主体（提供元）、提供先、提供事由を区分して個別的に限定列挙、それ以外は利用不可。ポジティブリスト方式。
- それ以外の場合、特定個人情報の収集・保管も禁止（20条）。



（出典・岡村久道「共通番号法入門」）

特定個人情報保護委員会が平成26年12月にガイドラインを公表



※　安全管理措置の詳細は、上記ガイドライン別添の「特定個人情報に関する安全管理措置（事業者編）」に記載あり。

要点

○　番号法における安全管理措置の考え方

番号法は、個人番号を利用できる事務の範囲、特定個人情報ファイルを作成できる範囲、特定個人情報を収集・保管・提供できる範囲等を制限している。したがって、事業者は、個人番号及び特定個人情報（以下「特定個人情報等」という。）の漏えい、滅失又は毀損（以下「情報漏えい等」という。）の防止等のための安全管理措置の検討に当たり、次に掲げる事項を明確にすることが重要である。

A　個人番号を取り扱う事務の範囲
B　特定個人情報等の範囲
C　特定個人情報等を取り扱う事務に従事する従業者（注）（以下「事務取扱担当者」という。）

（注）「従業者」とは、事業者の組織内にあって直接間接に事業者の指揮監督を受けて事業者の業務に従事している者をいう。具体的には、従業員のほか、取締役、監査役、理事、監事、派遣社員等を含む。

○　安全管理措置の検討手順

事業者は、特定個人情報等の適正な取扱いに関する安全管理措置について、次のような手順で検討を行う必要がある。→1

A　個人番号を取り扱う事務の範囲の明確化
B　特定個人情報等の範囲の明確化
C　事務取扱担当者の明確化
D　特定個人情報等の安全管理措置に関する基本方針（以下「基本方針」という。）の策定
E　取扱規程等の策定

○　講ずべき安全管理措置の内容

事業者は、安全管理措置の検討に当たり、番号法及び個人情報保護法等関係法令並びに本ガイドライン及び主務大臣のガイドライン等を遵守しなければならない。

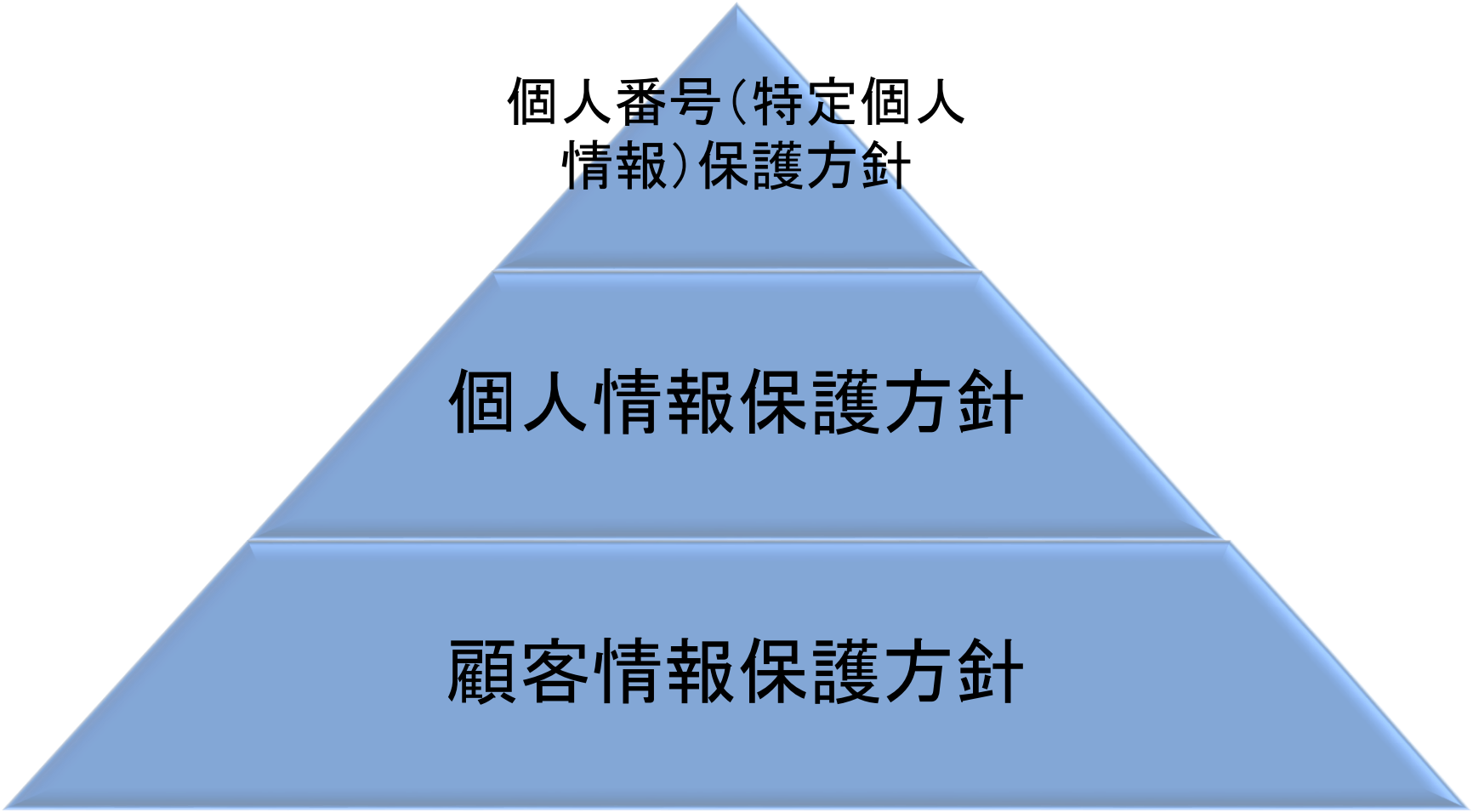
本ガイドラインは、次に掲げる項目に沿って記述している。→2

A　基本方針の策定
B　取扱規程等の策定
C　組織的安全管理措置
D　人的安全管理措置
E　物理的安全管理措置
F　技術的安全管理措置

参考－番号法にいう安全管理措置義務（12条）

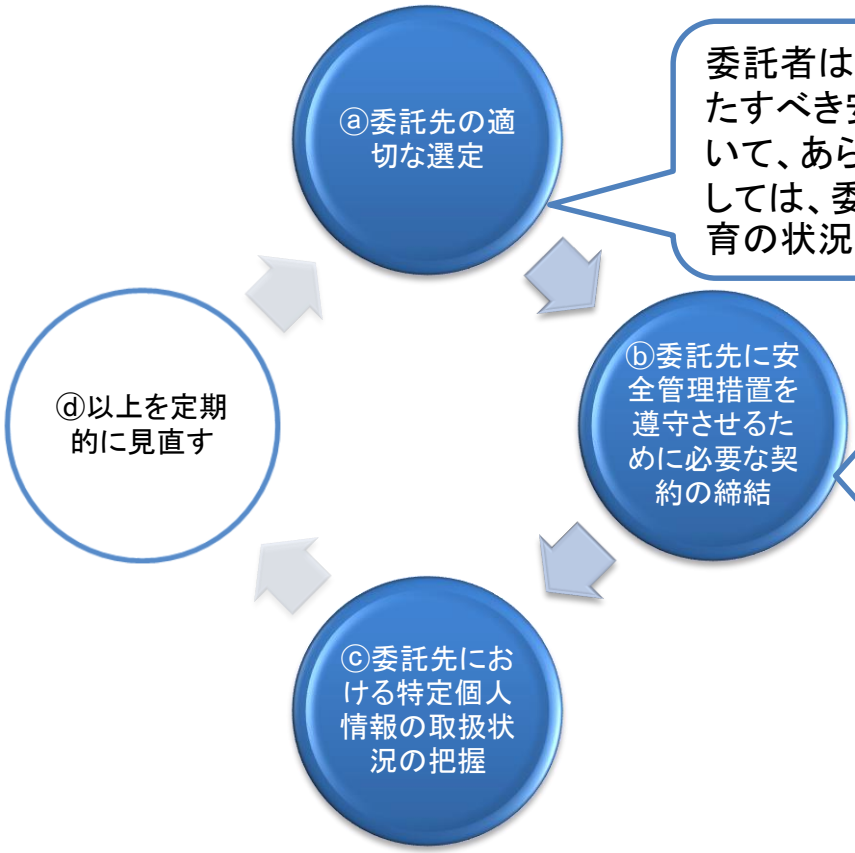
- 特定個人情報保護委員会は、特定個人情報保護委員会ガイドライン事業者編に別添された「特定個人情報に関する安全管理措置（事業者編）」によって、事業者における安全管理措置の内容に関し、次のとおり明確化を図っている（事業者編GL47頁以下）。
- 基本的には、従来におけるISMSをベースにした内容となっている。

金融機関の場合



参考－番号法にいう委託先に対する監督（11条）

本条は、委託者が、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受託者において講じられるよう監督するという趣旨の規定であり、特定個人情報保護委員会ガイドライン事業者編20頁は、次のとおり説く。



委託者は、委託先において、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か否かについて、あらかじめ確認しなければならず、具体的な確認事項としては、委託先の設備、技術水準、従業者に対する監督・教育の状況、その他委託先の経営環境等が挙げられる

契約内容として、秘密保持義務、事業所内からの特定個人情報の持出しの禁止、特定個人情報の目的外利用の禁止、再委託における条件、漏えい事案等が発生した場合の委託先の責任、委託契約終了後の特定個人情報の返却又は廃棄、従業者に対する監督・教育、契約内容の遵守状況について報告を求める規定等を盛り込まなければならず、また、これらの契約内容のほか、特定個人情報を取り扱う従業者の明確化、委託者が委託先に対して実地の調査を行うことができる規定等を盛り込むことが望ましい

特定個人情報保護評価（番号法26条～28条）

- 制度の概要
  - 特定個人情報保護委員会は、特定個人情報を適切に管理するために講ずべき措置を定めた指針を作成・公表し（26条）、これを踏まえて、行政機関の長等は、特定個人情報の漏えいその他の事態の発生の危険性および影響に関する評価（特定個人情報保護評価）を実施して評価書を作成・公示し、国民の意見を求めて見直した上、特定個人情報保護委員会の承認を得る（27条）。なお、同法の規定による場合を除き、特定個人情報ファイルの作成は禁止（28条）。
  - 諸外国で「プライバシー影響評価」（PIA：Privacy Impact Assessment）と呼ばれるものに相当。これは、プライバシーに対してITシステムの導入等が及ぼす影響を事前評価して、その保護措置を講じる仕組み。
- 関連規則等
  - 特定個人情報保護委員会は、特定個人情報保護評価について、同法27条1項に基づき、「特定個人情報保護評価に関する規則」を制定。
  - また、同法26条に基づき、特定個人情報保護評価指針を公表。
  - さらに、「特定個人情報保護評価指針の解説（平成26年11月11日更新）」も公表。

個人情報だけではない
ー企業その他の団体の情報漏えいと法的責任

- 本人からプライバシー侵害で損害賠償請求
- 監督官庁から個人情報保護法違反で行政処分
- 個人番号が含まれていれば、さらに責任は重い

他にも全体について
- 信用失墜によるマーケットからの放逐
- 業法違反による行政処分など

	個人情報	それ以外の情報
自社取得・保有情報	顧客名簿 従業員名簿	自社の開発技術情報
他社から業務上預かった情報	他社から加工を承った顧客名簿	発注元から新製品開発のため下請企業が預かった情報

いわば自爆！

- 契約違反として契約解除（取引打ち切り）・損害賠償請求

営業秘密の流出防止のための法整備（不正競争防止法改正案）

- 法整備に向けた検討作業と改正案の国会提出
  - 経済産業省の産業構造審議会・知的財産分科会「営業秘密の保護・活用に関する小委員会」において平成26年9月から検討を開始。
  - 平成27年3月13日に閣議決定。同日、衆議院議案受理。
- 背景－営業秘密について
  - 重要性が増大し、国際競争力や雇用の基盤となっている
  - 情報通信技術の高度化、スマートフォンなどの携帯情報端末の普及等によって、窃取行為が容易化、多様化及び複雑化
  - 実際に営業秘密の窃取事例が内外で増加
- サイバーセキュリティ基本法の関連規定
  - （民間事業者及び教育研究機関等の自発的な取組の促進）
  - 15条1項　国は、中小企業者その他の民間事業者及び大学その他の教育研究機関が有する知的財産に関する情報が我が国の国際競争力の強化にとって重要であることに鑑み、これらの者が自発的に行うサイバーセキュリティに対する取組が促進されるよう、サイバーセキュリティの重要性に関する関心と理解の増進、サイバーセキュリティに関する相談に応じ、必要な情報の提供及び助言を行うことその他の必要な施策を講ずるものとする。

営業秘密の流出防止のための法整備の概要

「不正競争防止法の一部を改正する法律案【不競法】」の概要

1. 背　景

秘密として管理される企業情報（技術情報、顧客名簿などの「営業秘密」）を巡って、スマートフォンの普及、サイバー攻撃技術の高度化といった　IT環境の変化等を背景に、情報漏えいが深刻化。一方で、オープン＆クローズ戦略の広がり等を背景に、競争力や雇用の基盤として、企業情報の重要性が増大。このため、企業情報の漏えい防止のため、法制面における抑止力の向上等を図る必要がある。

2. 法案の概要

企業情報を不正に窃取、転売、使用する行為に対して、刑事、民事の両面で抑止力向上を図る。
（1）刑事：処罰範囲の整備、罰則水準の引上げ、非親告罪化等の措置を講じる。
（2）民事：訴訟において被害企業が公平な賠償を受けることを可能とすべく、除斥期間の延長、原告立証負担の軽減等を講じる。

3. 措置事項の概要

A. 抑止力の向上

（1）法定刑の引上げ等

抑止力向上のため、罰金刑を引き上げる。（現行：個人1千万円以下、法人3億円以下）また、犯罪収益を没収できることとする。

【第21条第1項、第3項、第10項】

（2）非親告罪化

営業秘密侵害罪を非親告罪とする（公訴提起にあたって被害者からの告訴が不要となる）。

【新第21条第5項】

（3）立証負担の軽減

立証が困難である「加害者（被告）の企業情報の不正使用」について、一定の要件の下、被害者の立証負担を軽減する。（被告が当該情報の不使用を立証）

【新第5条の2】

（4）企業情報使用物品の譲渡・輸出入等行為

企業情報を侵害して生産された物品を譲渡・輸出入等する行為を、損害賠償や差止請求の対象とするとともに、刑事罰の対象とする。

【民事：新第2条第1項第10号】
【刑事：新第21条第1項第9号】

B. 処罰範囲の整備

（1）企業情報窃取等の未遂行為

「サイバー攻撃」などによる企業情報窃取や転売等の未遂行為を刑事罰の対象とする。

【新第21条第4項】

（2）転々流通した企業情報の転得者

転々流通する企業情報について、不正に取得されたことを知って取得した者による使用、転売等を刑事罰の対象とする。（現行：実行行為者からの直接の取得者のみ）

【新第21条第1項第8号】

（3）クラウドなど海外保管情報の窃取

日本企業が国内で管理し、海外で保管する情報の「取得・領得」行為も刑事罰の対象とする。（例：海外サーバーからの情報窃取など）

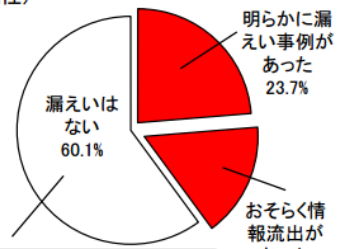
【新第21条第6項】

＜最近の営業秘密漏えい事例＞

- 新日鐵の高機能鋼板の技術情報がポスコ（韓）に漏えい(2012提訴)
- 東芝のフラッシュメモリの技術情報がSKハイニックス（韓）に漏えい(2014提訴)
- ベネッセの顧客情報がSE・名簿事業者等に漏えい(2014)

情報の漏洩の実態

少なくとも約4割の大企業（全企業で約14%）で情報漏えいの疑い（これも氷山の一角に過ぎない可能性）



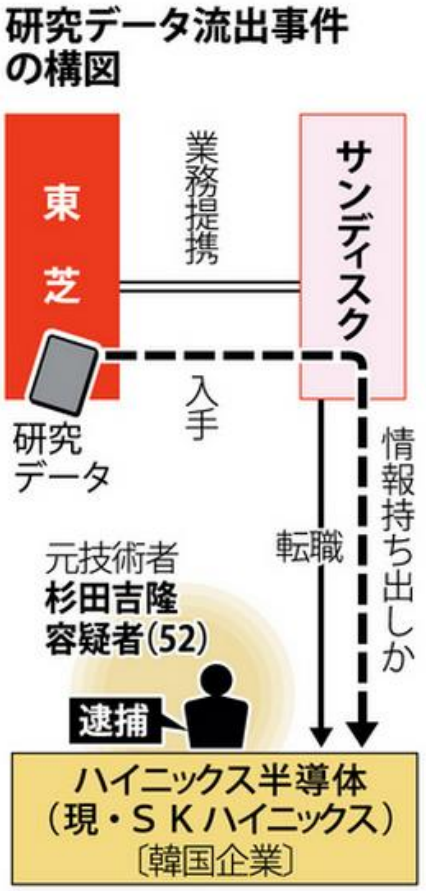
※「漏えいはない」とした企業の約3割は、そもそも、漏えい防止措置を何ら取っていないと回答

（出典）経済産業省『平成24年度　人材を通じた技術流出に関する調査研究』アンケート調査（回答約3000社）

出典：経済産業省サイト

営業秘密関係の参考判例
東京地判平成27年3月9日（東芝データ流出事件）

- 概要
  - 東芝のNAND型フラッシュメモリーに関する研究データを、共同研究企業の半導体メーカー元社員（被告人）がコピーして、韓国企業に流出させた事件。
- 判決要旨
  - 不正競争防止法違反（営業秘密開示）の罪で懲役5年、罰金300万円の実刑判決。
  - 我が国の産業で重要な半導体分野の営業秘密を他国の競業他社に流出させ、社会に大きな衝撃を与えた、東芝の損害額は莫大、転職先での地位を維持するために、自らの意思で情報を開示しており、刑事責任は重いと判示。



出典･毎日新聞ウェブ版

サイバーセキュリティ関係の参考判例
東京地判平成26年6月6日（ベライゾンジャパン事件）

- 事案の概要
  - 国際電話発信サービス契約が、リトアニアの個人番号への国際電話によって不正利用されたことを理由に、それによって増えた通話料の支払拒絶が認められるかどうかが問題となった事案。
- 判決要旨
  - 利用者側が敗訴。
  - 被告は、原告が、被告に対し、不正利用等の疑いのある通話等を速やかに通知すべき義務に違反した旨主張するが、契約上において、当該通知義務を負うべき根拠は見当たらず、他に原告が通知義務を負う旨が合意されたことを認めるに足りる証拠もない。また、国際電話回線の不正利用は、電気通信サービスを提供する電気通信事業者の通信設備の異常に起因するものではなく、電気通信サービスの提供を受ける当事者が利用する機器やソフトウェアのセキュリティ対策の不備に起因するものであり、そうすると、不正利用の防止及び不正利用が発生した場合の被害の拡大防止は、基本的には、電気通信サービスの供給を受ける当事者の被告の責任に属する事柄である。
  - 原告を含む多くの電気通信事業者が、独自のアルゴリズム（検出手法）により、不正利用等の疑いがある通話等について探知し、これを顧客に通知する対応をとっているが、不正利用等が顧客の設備に起因するものであること等に照らせば、上記対応が通信サービスを提供する電気通信事業者の法的義務に基づくものとはいえない。

サイバーセキュリティ関係の参考判例
東京地判平成26年1月15日判時2215号30頁（公安テロ情報流出事件）

- 事案の概要
  - イスラム教徒である原告らが、警視庁、警察庁及び国家公安委員会は、①モスクの監視など、原告らの信教の自由等の憲法上の人権を侵害し、また、行政機関個人情報保護法や東京都個人情報保護条例に違反する態様で個人情報を収集、保管及び利用し、②その後、情報管理上の注意義務違反等により個人情報をインターネット上に流出させた上、適切な損害拡大防止措置を執らなかったものであるとして、東京都等に対し国家賠償請求した事案。
- 判決要旨
  - 「本件データは、警察職員によって外部記録媒体を用いて持ち出されたものと考えるのが相当である。」「警視総監としては、本件データが外部へ持ち出され、その情報が外部のパソコンに接続されれば、〇〇ソフト等を通じてインターネット上に流出して、不特定多数の者に伝播し、それによって原告らに多大な被害を与えるおそれがあることが十分に予見可能であった」から、「警視総監としては、原告らの個人情報が絶対に漏えいすることのないよう、徹底した漏えい対策を行うべき情報管理上の注意義務を負っていた」。「外事第三課内で使用されているコンピュータの中には、外部記録媒体の使用履歴の証跡管理その他の管理が不十分と思われるものが一部存在することが判明した……ことからすれば、外事第三課内におけるセキュリティ規程等を実際に遵守するよう徹底する管理体制は不十分なものであ」り、このことが、外部記録媒体を用いたデータの持出しにつながったとみるのが相当である。したがって、警視総監には、情報管理上の注意義務を怠った過失があり、国家賠償法上違法であ」り、「被告東京都は責任を負う。」

サイバーセキュリティ関係の参考判例
東京地判平成26年 3月17日労経速 2207号9頁
（学校LANセキュリティ事件）

- 事案の概要
  - 東京都教育委員会が、江戸川区公立学校事務職員であった原告に対し、懲戒減給処分をしたところ、原告が処分の取消しを求めた事案。処分理由は、原告が学校LAN用パソコンのセキュリティを破ることを目的に、同パソコンからハードディスクを取り外し、変換プラグを使用して、目的外使用が禁止されていることを知っていたにもかかわらず、他の事務用パソコンに同ハードディスク内のデータの一部を転送したこと、同区内小中学校の全事務職員に対して、学校LAN用パソコンからデータを取り出せることについて教唆する不適切な内容の電子メールを送信したというもの。
- 判決要旨
  - 請求棄却（当該職員側が敗訴）。
  - 「学校LANには、保護すべき個人情報の蓄積及び使用を含んでいることから、学校LAN用パソコンには、〇〇という専用のUSBメモリを使用しないと、データを取り出すことができないよう、高度なセキュリティ対策が施されている上、〇〇を利用するにはセキュリティ管理者である各校の校長の許可が必要であることが認められ、本件データ転送行為は、そのような高度なセキュリティ対策が施されている学校LAN内のデータを、セキュリティ管理者の許可を要する正規の手続を踏むことなく、学校LANの外部に取り出したものであるから、それ自体、非常に悪質な行為である」。
  - 「原告は、……江戸川区内小中学校の全事務職員157名に対し、〇〇の使用という正規の手続を潜脱して学校LAN内のデータを外部に取り出す必要があるときは、原告に連絡することによりそれを実現することができる旨を喧伝する本件メール送信行為に及んだというのであるから、学校LANのセキュリティ担当者をして学校LANの安全性に脅威を感じさせ、その安全性を再確認するための方策をとることを余儀なくさせるのに十分な行為を行ったものということができる。また、原告が本件データ転送行為により転送したデータは暗号化されたものであったとはいえ、これが解読される危険性を否定することはできないのであって、本件データ転送行為及び本件メール送信行為によりもたらされた結果も軽視することはできない。」

サイバー報セキュリティ関係の参考判例
東京地判平成26年1月23日平23(ワ)32060（SQLインジェクション事件）①

- 事案の概要
  - 原告との商品受注システム設計、保守等の委託契約に基づき被告が製作したアプリケーション（EC-CUBEを被告がカスタマイズしたもの）が脆弱であったため、原告ウェブサイトで商品の注文をした顧客のクレッジトカード情報が流失した事案で、被告の上記委託契約の債務不履行に基く損害賠償責任が認められた事例。
- 判決理由
  - SQLについてログは残されていなかったが、流失原因はSQLインジェクション攻撃によるものと推認（他に原告主張のクロスサイトスクリプティングは流出原因とは認められず）。
  - 被告は、本件システム発注当時（平成21年2月4日）の技術水準に沿ったセキュリティ対策を施したプログラムを提供することが黙示的に合意されていたと認められ、本件システムでは顧客の個人情報を本件データベースに保存する設定となっていたことからすれば、被告は、当該個人情報の漏洩を防ぐために必要なセキュリティ対策を施したプログラムを提供すべき債務を負っていた。（続く）

東京地判平成26年1月23日平23(ワ)32060（SQLインジェクション事件）②

- 判決理由（続き）
  - それ以前からSQLインジェクション攻撃でデータベース内の大量の個人データが流出する事案が相次いで発生しており、K省やIPAが、SQL文の組み立てにバインド機構を使用し，又はSQL文を構成する全ての変数に対しエスケープ処理を行うこと等によるSQLインジェクション対策の必要性について注意喚起していた。
  - これらの事実に照らすと、被告は、本件システム発注契約締結時点で、本件データベースから顧客の個人情報が漏洩することを防止するために、SQLインジェクション対策として、バインド機構の使用又はエスケープ処理を施したプログラムを提供すべき債務を負っていたが、いずれも行われていなかった部分があり、被告は上記債務を履行しなかったから責任がある。
  - 原告のシステム担当者が、顧客のクレジットカード情報のデータがデータベースにあり、セキュリティ上はクレジットカード情報を保持しない方が良いことを認識し、被告から本件システム改修の提案を受けていながら、何ら対策を講じずにこれを放置したことは、本件流出によるクレジットカード情報の漏洩の一因となったことは明らかであるから、上記原告の過失を考慮しも3割の過失相殺をするのが相当である

東京地判平成26年1月23日平23(ワ)32060（SQLインジェクション事件）③

- 本判決が残した教訓
  - システムベンダ側
    - 契約に明文がなくても、契約締結当時の技術水準に沿ったセキュリティ対策を施したシステムを提供することが黙示的に合意されていることになる。
    - これに対抗しようとすれば、SLAを明記したり、システム改修提案をしておくことも方法だが、それとともに、「技術水準に沿ったセキュリティ対策」について、日頃から注視しておく必要。もちろん制度面についても。
  - 発注者側
    - システム改修提案などがあれば放置すべきではない。さもないと過失相殺を受けるおそれ。
    - そのため、あるいは、それとともに、「技術水準に沿ったセキュリティ対策」について、日頃から注視しておく必要。もちろん制度面についても。
- まとめ－Security by Design
  - プライバシー・バイ・デザイン（Privacy by Design）という言葉があるが、これからは、セキュリティ・バイ・デザイン（Security by Design）を考えていくべき。
  - 「情報セキュリティに配慮した措置を講ずることを意識した『Security by Design』の社会システムの構築について検討を行う。」（総務省情報セキュリティ アドバイザリーボード「総務省における情報セキュリティ政策の推進に関する提言」20頁）

結びに代えてーサイバーセキュリティの今後

- ご清聴、ありがとうございました。