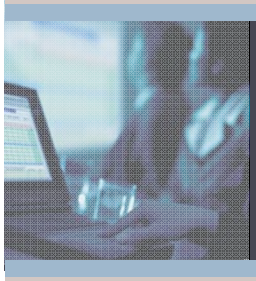
IAIS 一般社団法人 行政情報システム研究所
The Institute of Administrative Information Systems



www.iais.or.jp/seminar/

平成27年度

CIO補佐官講座

第5回

講座　ネットワークとセキュリティ

講師　満塩　尚史

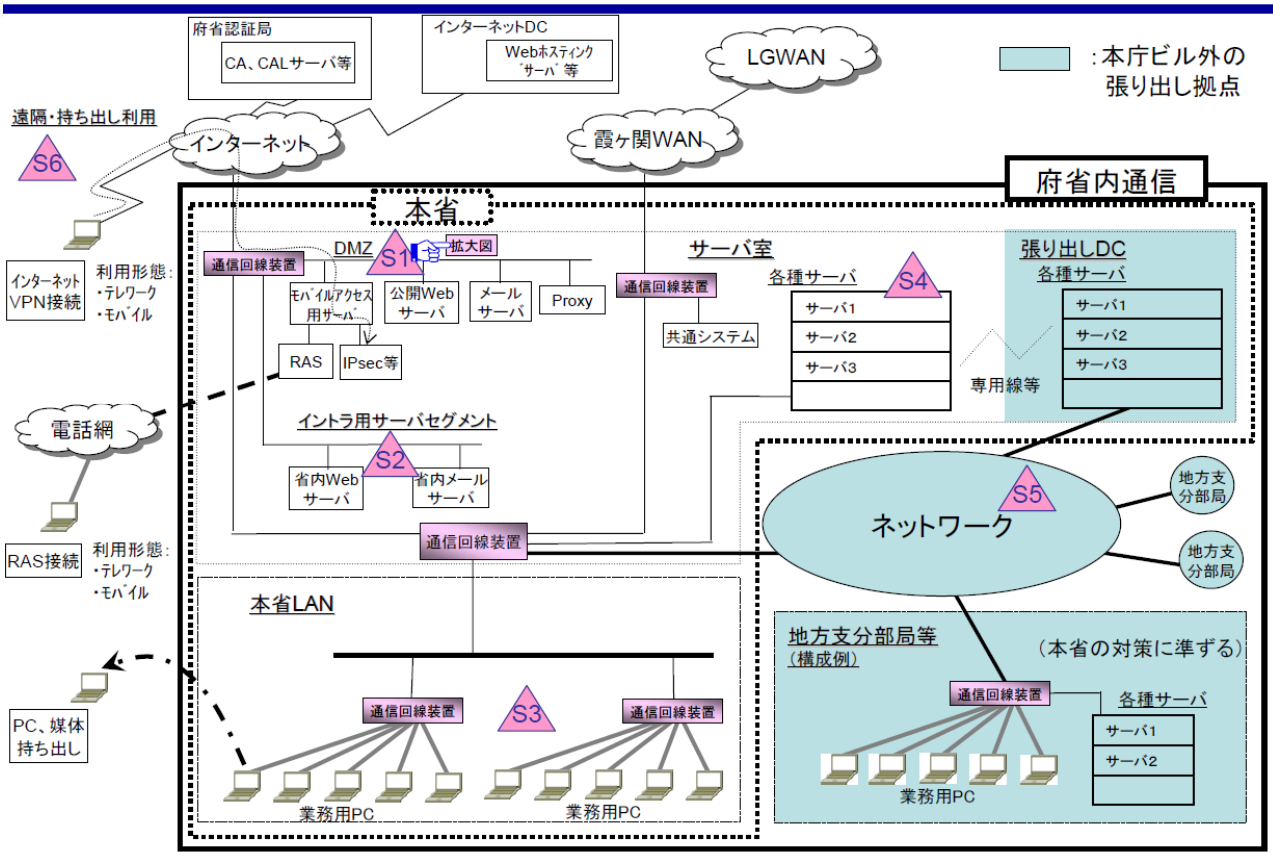
IAIS

目次

- 政府機関のネットワークモデル
- 政府共通ネットワーク再編方針
- サイバーセキュリティ基本法
- 政府機関の情報セキュリティ対策のための統一基準群
- 高度サイバー攻撃対処のためのリスク評価等のガイドラインについて
- 情報セキュリティを企画・設計段階から確保するための方策 SBD(Security by Design)
- マイナンバー制度

政府機関のネットワークモデル

ネットワークモデル　全体図



平成19年 4月19日第36回CIO補佐官等連絡会議での第4ワーキングの報告書より

政府共通ネットワーク再編方針

1. ネットワーク再編の背景

世界最先端IT国家創造宣言（平成25年6月14日閣議決定、平成26年6月24日改定）（抜粋）

3. 公共サービスがワンストップで誰でもどこでもいつでも受けられる社会の実現
（2）国・地方を通じた行政情報システムの改革

政府のIT投資に関するポートフォリオ管理を導入するとともに、政府情報システム改革に関するロードマップに基づき、政府CIOの指導の下、重複する情報システムやネットワークの統廃合、必要性の乏しい情報システムの見直しを進めるとともに、政府共通プラットフォームへの移行を加速する。あわせて、政府共通プラットフォームについて、開発環境やリモート・デスクトップ機能など、政府のプライベートクラウドとしての環境及び機能を整備し、その充実を図る。

※ 同宣言工程表（抜粋）
2013年度～2014年度にかけて、政府内のネットワークの統廃合に向けた調査研究を実施し、2014年度内にその結果を踏まえたネットワークの再編方針を策定する。

政府内のネットワークについて、重複投資を回避しつつ、政府共通プラットフォームと連携して、①～③に資する共通基盤として再編する方策を検討

①府省共通の機能・サービス提供の拡充
②ワークスタイル変革、業務改革の推進
③セキュリティ強化、業務継続の確保

1

2. 政府内ネットワークの概況

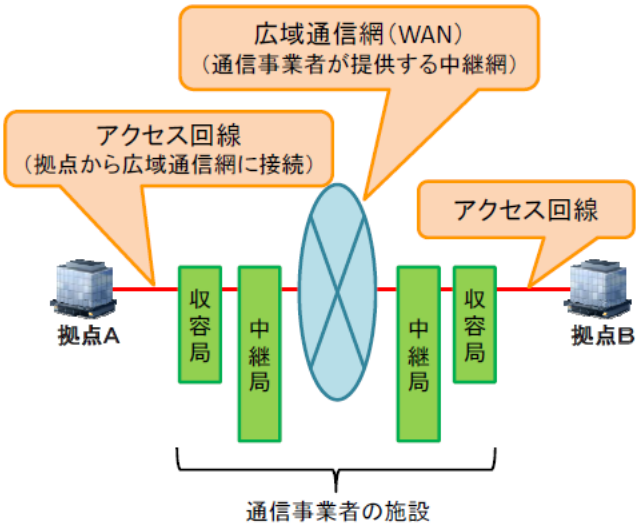
膨大な数の庁舎等（６千超）に対し、非常に多くの回線（約１万６千）が接続。

表：政府内ネットワークの概況

集計項目	集計結果
情報システム数 （回線契約等有り）	301システム
接続拠点数（庁舎等）	6,021拠点
広域通信網（WAN）の数	269回線
アクセス回線等の数	15,731回線
（うち2拠点間の専用線等）	（776回線）
（うちアクセス回線）	（13,883回線）
（うちインターネット回線）	（1,072回線）
契約帯域（アクセス回線等）	559,255Mbps
回線費用（年間） （広域通信網（WAN）、アクセス回線等）	約120億円

※ 平成26年４月１日時点の実態調査結果を集計。
※ 契約帯域及び費用は、有効回答が得られた回線分。

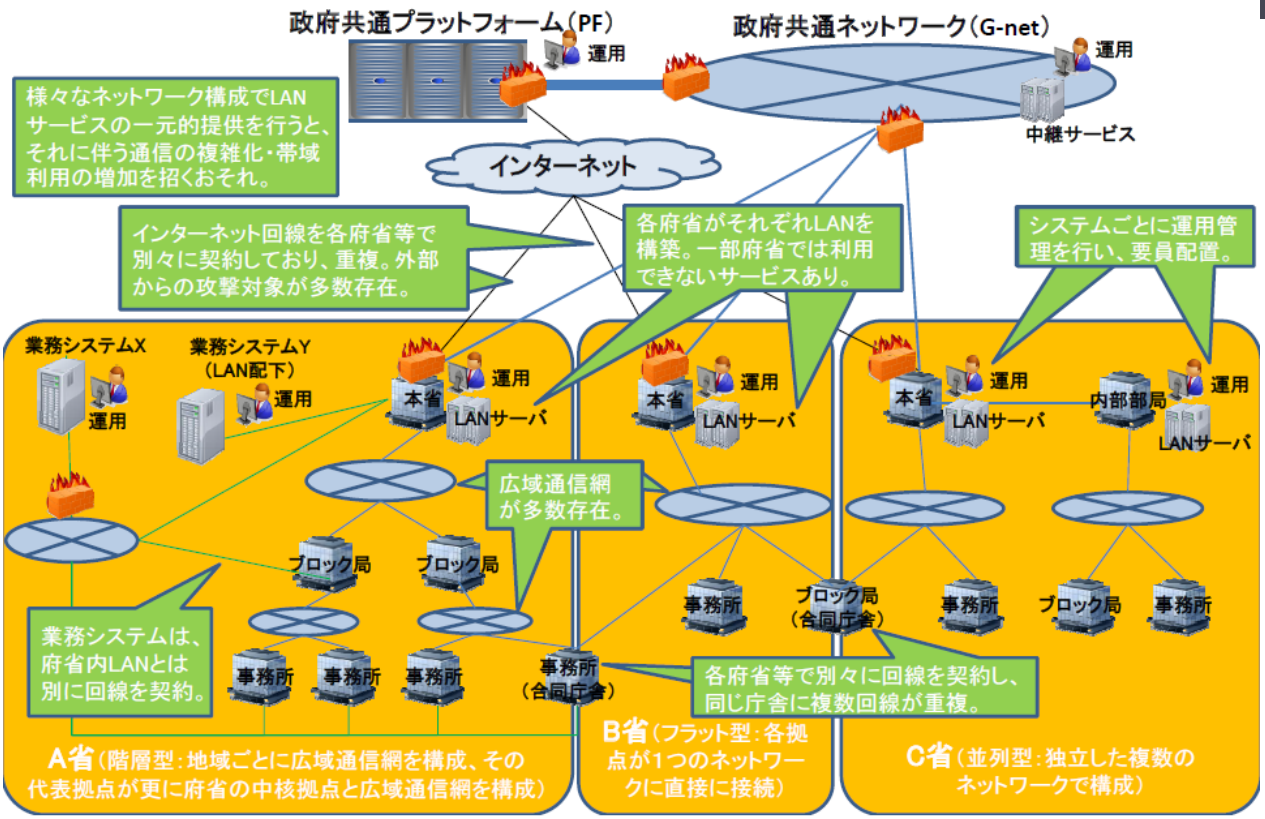
【凡例：広域通信網（WAN）、アクセス回線】



! 視点①：統合によりシンプルで強固なネットワークを効率的に整備できないか

2

3. 現状の政府内ネットワークの構成（イメージ）



4. 政府内ネットワークの現状①

各府省・各システムでそれぞれ回線を整備するため、特に合同庁舎で多数の回線等が重複。

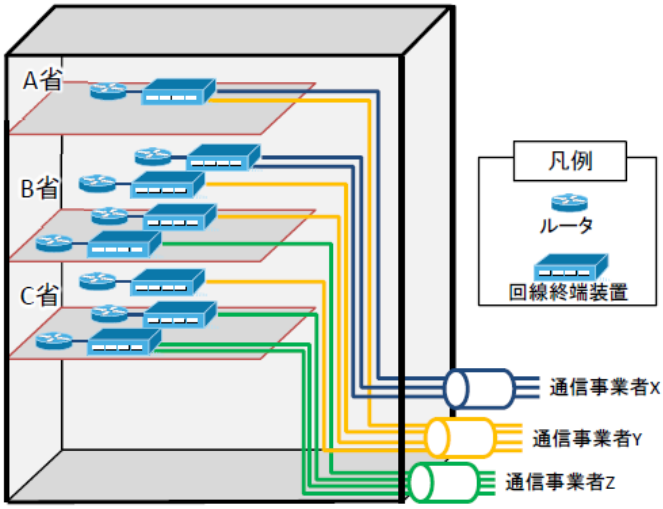
【拠点ごとの回線数】
→ 半数以上の拠点に複数回線あり

表：拠点数（敷設する回線数ごと）

回線数	拠点数	割合
1本	2,686拠点	47.5%
2本	1,182拠点	20.9%
3本	1,254拠点	22.2%
4～9本	456拠点	8.1%
10本以上	79拠点	1.4%

※ 平成26年4月1日時点の実態調査結果を集計。

【模式図】ある合同庁舎でのアクセス回線の状況
→ 回線やルータ等の機器が同一庁舎に多数存在



視点②：集約により各拠点の回線等の整備・管理の合理化が図れないか

4

5. 政府内ネットワークの現状②

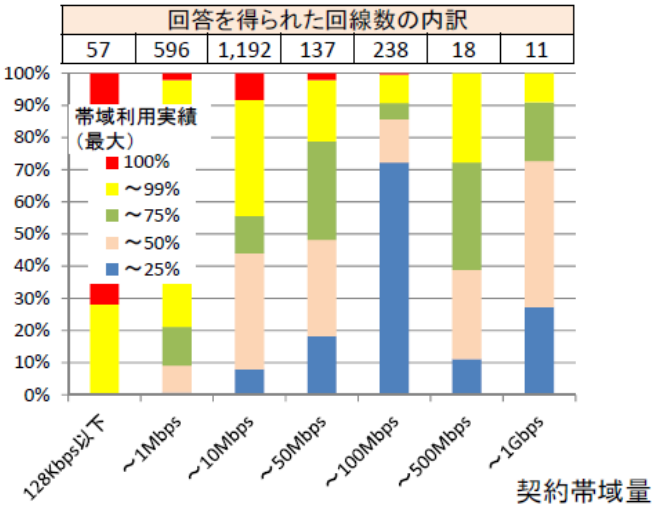
契約帯域量の大きい回線を中心に、通信のピーク時でも帯域利用が低調な回線が存在。

表：帯域利用実績（最大値・平均値の相関）

帯域利用実績		最大（最大値／契約帯域量）					
		～25%	～50%	～75%	～99%	100%	総計
平均（平均値／契約帯域量）	～25%	300	563	272	945	104	2,184
	～50%				5	47	52
	～75%			1	3	2	6
	～99%				3	1	4
	100%					3	3
	総計	300	563	273	956	157	2,249

約４割（※）の回線で、ピーク時でも契約帯域の半分以上を利用せず

図：契約帯域別の帯域利用実績（最大値）



※ 平成26年4月1日時点の実態調査で、帯域の利用実績を得られた回線のうち、帯域保証有りの2,249回線を対象に整理。

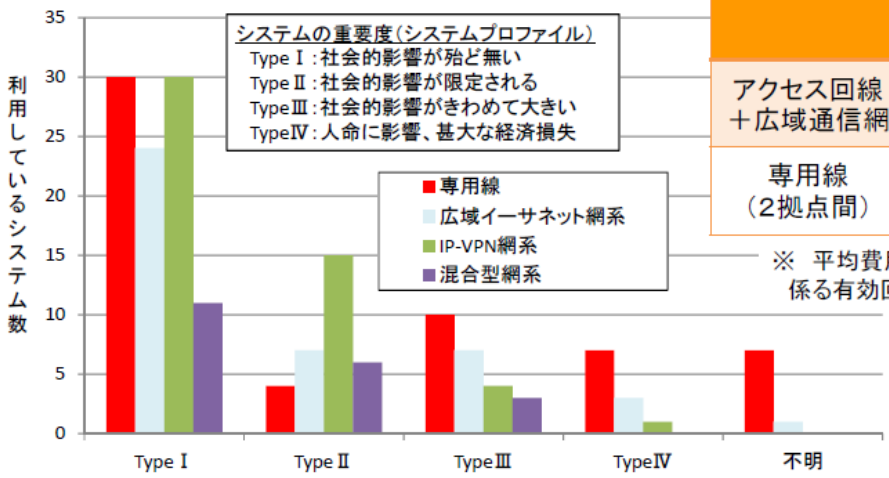
視点③：回線の集約・共有により、帯域利用の平準化と総帯域量の抑制を図る必要がないか

5

6. 政府内ネットワークの現状③

重要度が高くない情報システムにおいても、費用面で割高な専用線の利用が存在。

図：システム重要度と回線種別



表：アクセス回線と専用線の平均費用の比較

	回線数（※）	1回線当たりの平均費用（年間）
アクセス回線＋広域通信網	12,152回線（アクセス回線）	555千円/Mbps（広域通信網分を含む）
専用線（2拠点間）	445回線	1,222千円/Mbps

※ 平均費用の算出に係る有効回答分。

平均費用は2倍以上

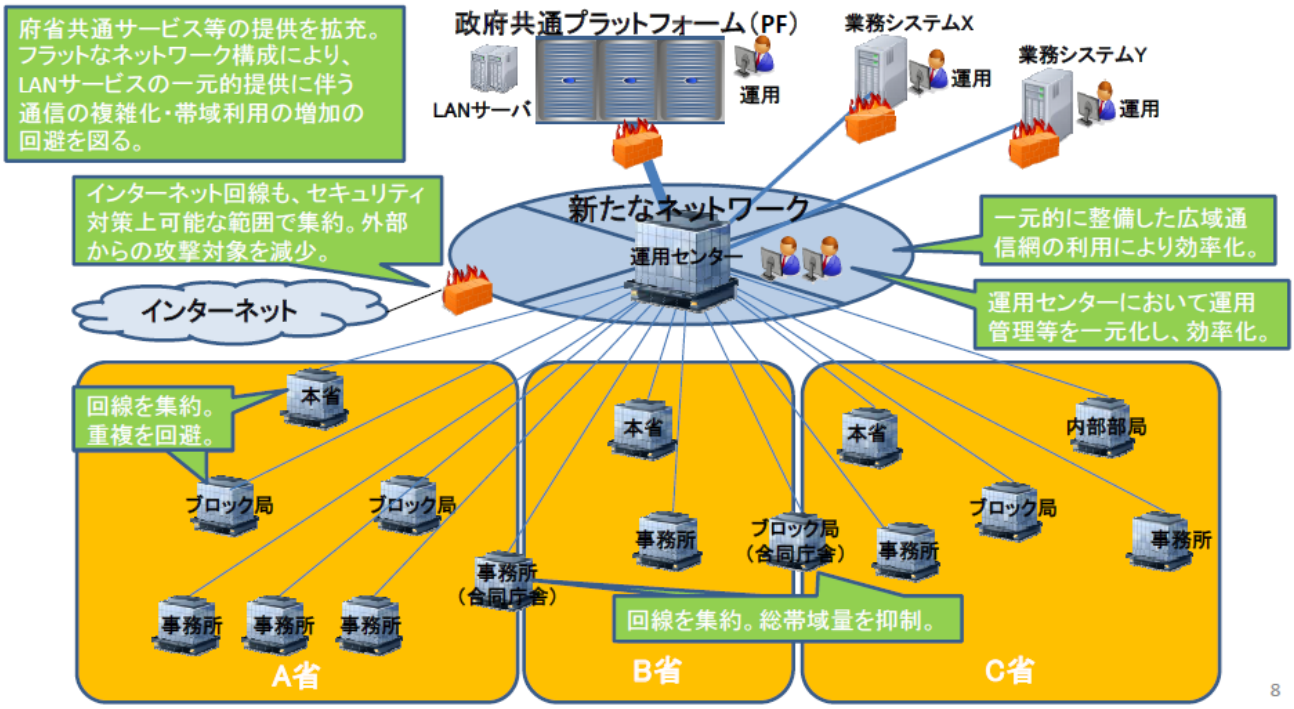
！ 視点④：専用線から広域通信網の利用に切り替えられないか

【参考】 金融（を含む）分野の全国規模のネットワークにおいても、広域通信網が利用されている。
例：全国銀行データ通信システム（全銀システム）、郵政総合情報通信ネットワーク（PNET）

6

【参考】政府内ネットワークの将来像（イメージ）

広域通信網を一元的に整備。拠点ごとに集約されたアクセス回線がフラットに接続し、便利（府省共通サービス等の提供拡充）や安全（迅速なセキュリティ対応）を一層向上。



8

サイバーセキュリティ基本法

サイバーセキュリティ基本法案の概要　資料1－2（参考）

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、強靱な体制の構築

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

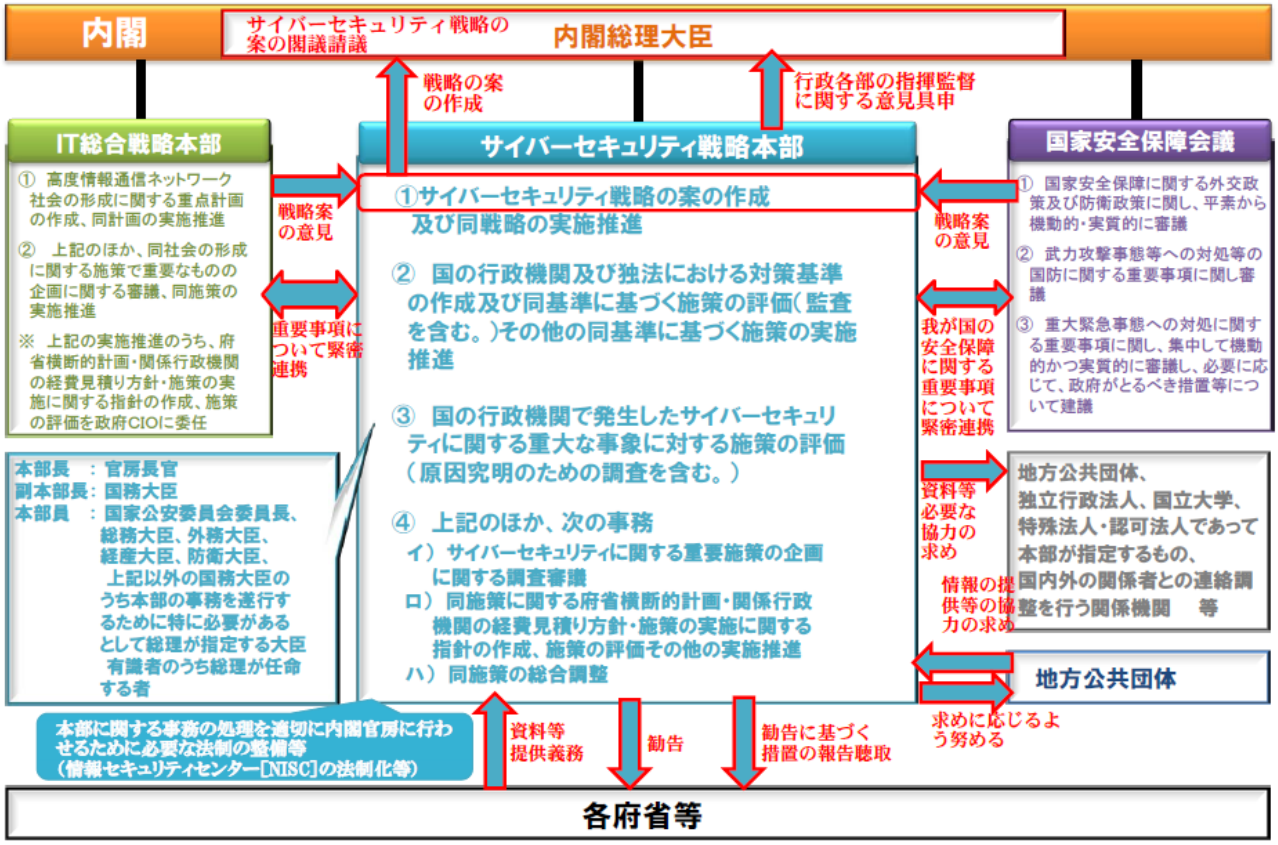
■検討（第３条）

⇒ 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

サイバーセキュリティ戦略本部の機能・権限（イメージ）

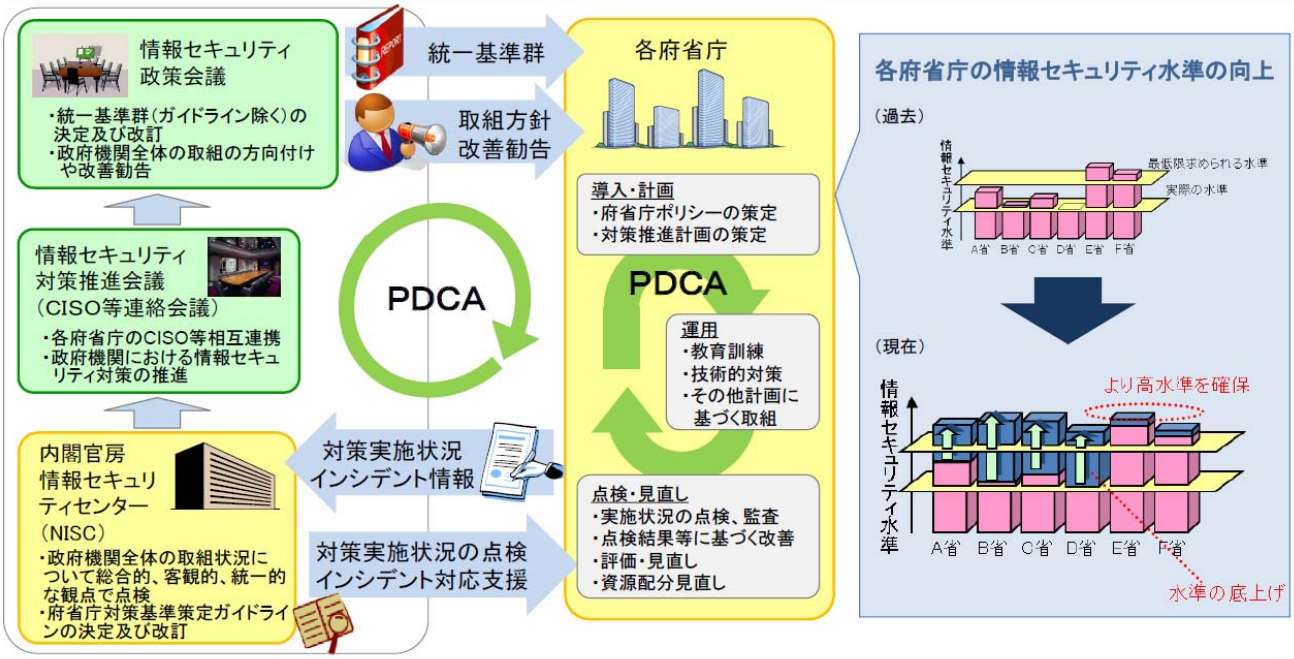


IAIS

政府機関の情報セキュリティ対策のための統一基準群

政府機関の情報セキュリティ対策のための統一基準群とは

- 「政府機関の情報セキュリティ対策のための統一基準群」（以下、「統一基準群」という。）は、政府全体の情報セキュリティ水準を向上させるための統一的な枠組み。
- 各府省庁は、統一基準に準拠した情報セキュリティポリシー及び、対策推進計画を策定し、対策を実施する。



統一基準群（平成26年度版）の改定概要

現行の統一基準群の課題

◆毎年の改定により基準が複雑化・肥大化・形骸化

◆脅威の高度化・多様化や技術進展などの環境変化

改定の方向性（※）

◆統一基準群の実効性の向上

（1）各府省庁が直面する情報セキュリティリスクを踏まえてCISO自らの判断で目標や実施計画を策定し、これに基づく対策の実施・評価・点検や、計画の見直しを行うよう求めることで、府省庁独自のPDCAサイクルによる自律的対策強化を図る。

（2）定義や用語の明瞭化・簡潔化、冗長表現の排除、名宛人毎の遵守事項の集約化、形骸化した規定の見直し等により、分かりやすく、守られやすい基準作りを目指す。

◆新たな脅威・技術への対応

（3）標的型攻撃から守るべき重点業務・情報を特定し、攻撃の早期検知や、侵入後の活動を困難化するため、内部対策をリスクに応じて計画的に講ずる。

（4）情報システムの構築等の外部委託の際、委託先における不正機能の混入などを防止するための管理体制を求める。

（5）私物スマートフォン等の業務使用について、責任者の設置及び安全管理措置の規定により、厳格な管理を求める。

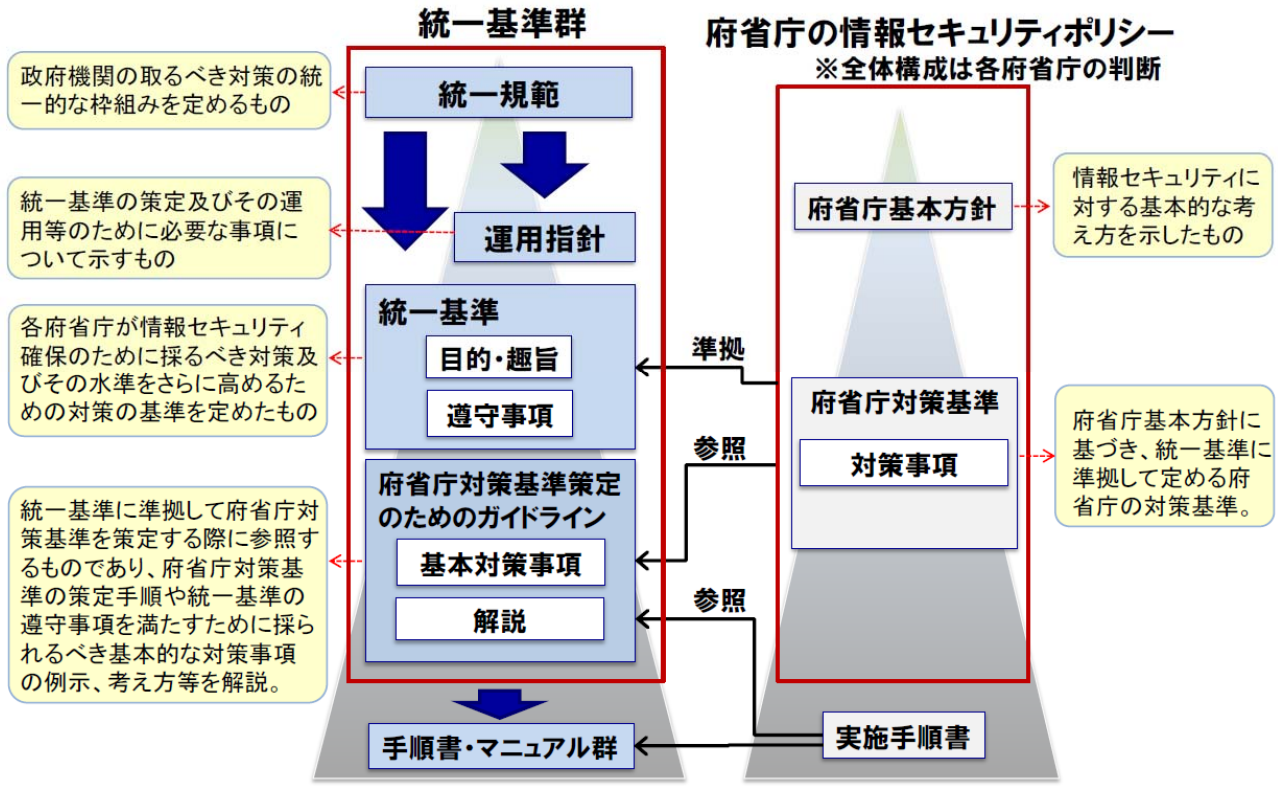
（6）SNS、グループメールサービス等の利用に際して責任者の設置、なりすまし防止対策の実施、機密情報の取り扱いの禁止等を求める。

（7）USBメモリ等について、ウイルス混入や紛失等の脅威に対抗するための利用手順を定めるよう求める。

（8）複合機等について、国際規格への適合や適切な設定等、必要な対策を講ずるよう求める。

（※「サイバーセキュリティ戦略」（平成25年6月情報セキュリティ政策会議決定）において決定された事項を踏まえ検討。）

統一基準群と府省庁ポリシーの関係



3.1.1 情報の取扱い②

■ 格付の区分

【機密性についての格付区分】

格付の区分	分類の基準
機密性3情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性を要する情報
機密性2情報	行政事務で取り扱う情報のうち、秘密文書に相当する機密性は要しないが、漏えいにより、国民の権利が侵害され又は行政事務の遂行に支障を及ぼすおそれがある情報
機密性1情報	公表済みの情報、公表しても差し支えない情報等、機密性2情報又は機密性3情報以外の情報

【完全性についての格付区分】

格付の区分	分類の基準
完全性2情報	行政事務で取り扱う情報（書面を除く。）のうち、改ざん、誤びゅう又は破損により、国民の権利が侵害され又は行政事務の適切な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
完全性1情報	完全性2情報以外の情報（書面を除く。）

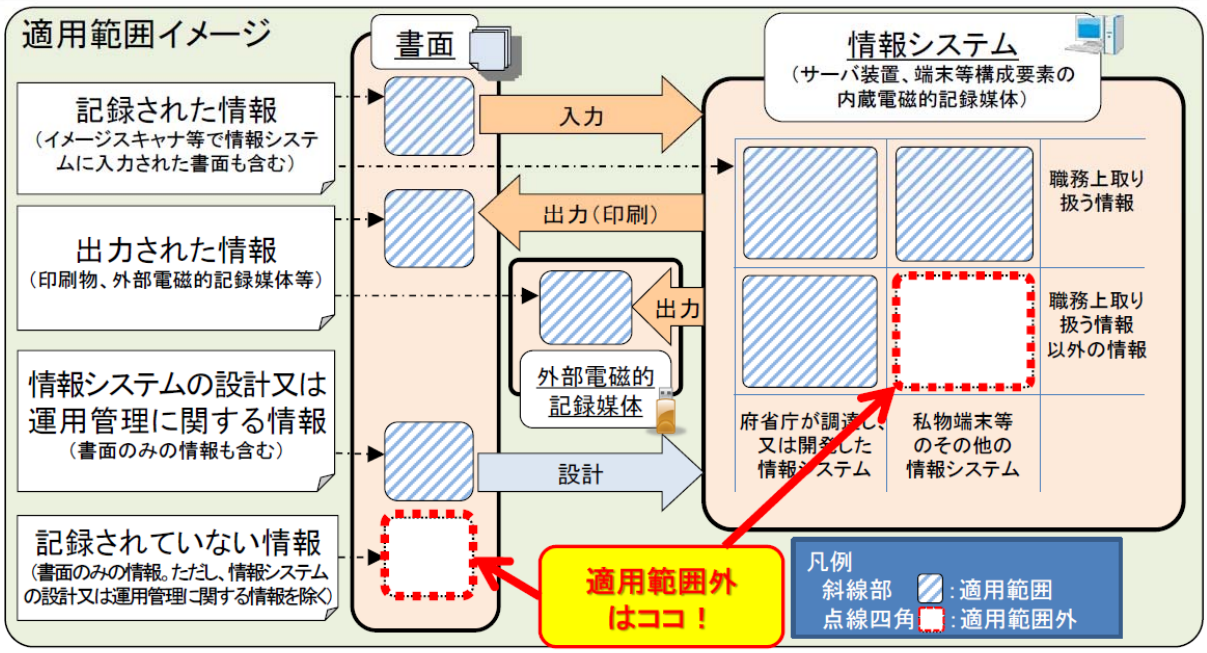
【可用性についての格付区分】

格付の区分	分類の基準
可用性2情報	行政事務で取り扱う情報（書面を除く。）のうち、その滅失、紛失又は当該情報が利用不可能であることにより、国民の権利が侵害され又は行政事務の安定的な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報
可用性1情報	可用性2情報以外の情報（書面を除く。）

1.1 本統一基準の目的及び適用範囲②

■統一基準の適用を受ける「情報」の範囲

1.1(2)(b) 本統一基準において適用範囲とする情報は、以下の情報とする。
（ア） 行政事務従事者が職務上使用することを目的 として府省庁が調達し、又は開発した情報システム若しくは 外部電磁的記録媒体に記録された情報（当該情報システムから出力された書面に記載された情報及び書面から情報システムに入力された情報を含む。）
（イ） その他の情報システム又は外部電磁的記録媒体に記録された情報（*中略*）
（ウ） （ア）及び（イ）のほか、府省庁が調達し、又は開発した情報システムの設計又は運用管理に関する情報



10

2.1.1 組織・体制の整備

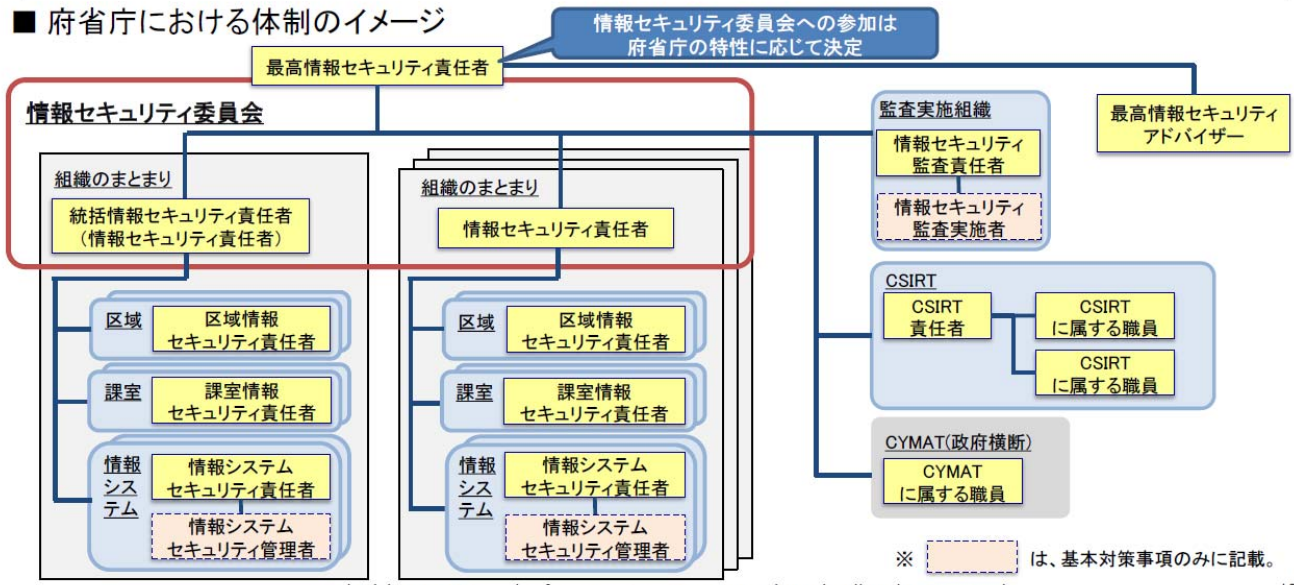
CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

■ 本項の概要

- 情報セキュリティ対策は、それに係る全ての行政事務従事者が、職制および職務に応じて与えられている権限と責務を理解した上で、負うべき責務を全うすることで実現される。これらの権限と責務を明確にし、必要となる組織・体制を整備することが必要。

＜主な遵守事項＞
2.1.1(1)(a) 府省庁は、府省庁における情報セキュリティに関する事務を統括する最高情報セキュリティ責任者を一人を置くこと。
2.1.1(2)(a) 最高情報セキュリティ責任者は、（*中略*）情報セキュリティ委員会を置くこと。

■ 府省庁における体制のイメージ



13

2.2.2 例外措置

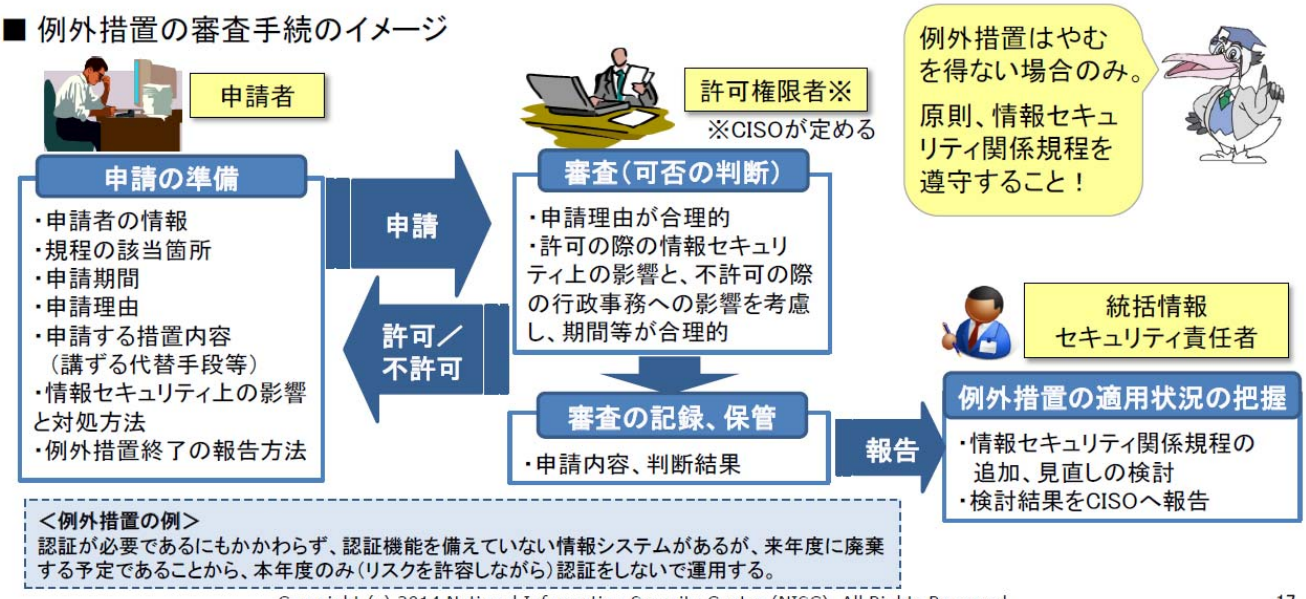
CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

■ 本項の概要

- 規定された対策の内容と異なる代替の方法や規定された対策を実施しないことを認めざるを得ない場合に対処するための手続が必要。

＜主な遵守事項＞
2.2.2(1)(a) 最高情報セキュリティ責任者は、例外措置の適用の申請を審査する者及び、審査手続を定めること。
2.2.2(2)(a) 行政事務従事者は、定められた審査手続に従い、許可権限者に規定の例外措置の適用を申請すること。

■ 例外措置の審査手続のイメージ



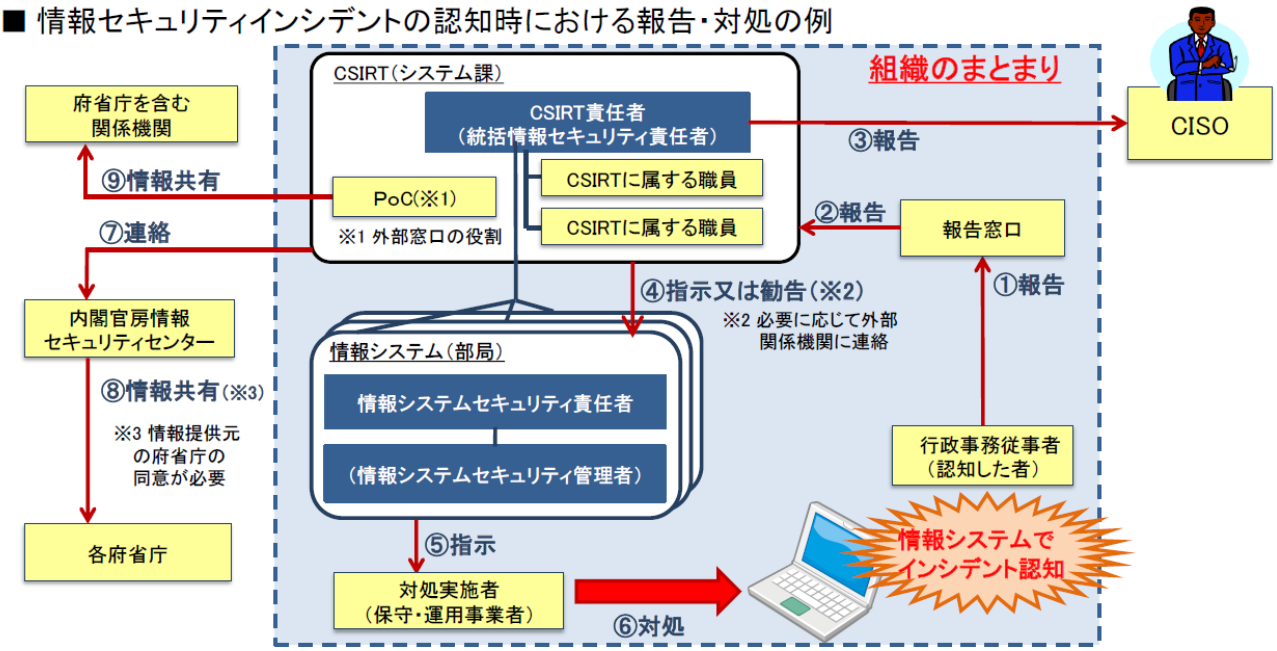
＜例外措置の例＞
認証が必要であるにもかかわらず、認証機能を備えていない情報システムがあるが、来年度に廃棄する予定であることから、本年度のみ（リスクを許容しながら）認証をしないで運用する。

2.2.4 情報セキュリティインシデントへの対処 ［参考］

■ CSIRTとは

Computer Security Incident Response Teamの略。
府省庁の情報システムに対する情報セキュリティインシデントが発生した際に、当該府省庁が発生した事案を正確に把握し、被害拡大防止、復旧、再発防止等を迅速かつ的確に行うことを可能にするための機能を有する体制

■ 情報セキュリティインシデントの認知時における報告・対処の例



2.3.1 自己点検

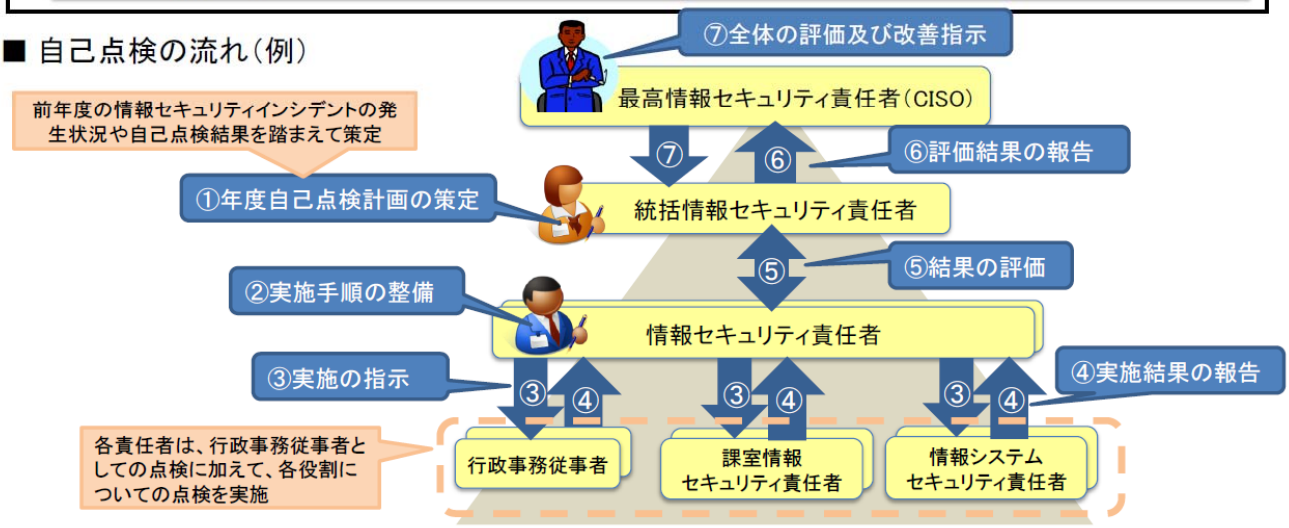
■ 本項の概要

CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

- 自己点検は、行政事務従事者が自らの役割に応じて対策事項を実施しているかどうかを確認するだけでなく、組織全体の情報セキュリティ水準を確認する目的もあることから、適切に実施することが重要。

＜主な遵守事項＞
2.3.1(1)(a) 統括情報セキュリティ責任者は、*(中略)*年度自己点検計画を策定すること。
2.3.1(1)(b) 情報セキュリティ責任者は、行政事務従事者ごとの自己点検及び自己点検の実施手順を整備すること。
2.3.1(2)(b) 行政事務従事者は、*(中略)*自己点検及び自己点検の手順を用いて自己点検を実施すること。
2.3.1(3)(b) 最高情報セキュリティ責任者は、自己点検結果を全体として評価し、*(中略)*統括情報セキュリティ責任者及び情報セキュリティ責任者に改善を指示すること。

■ 自己点検の流れ（例）



3.2.1 情報を取り扱う区域の管理①

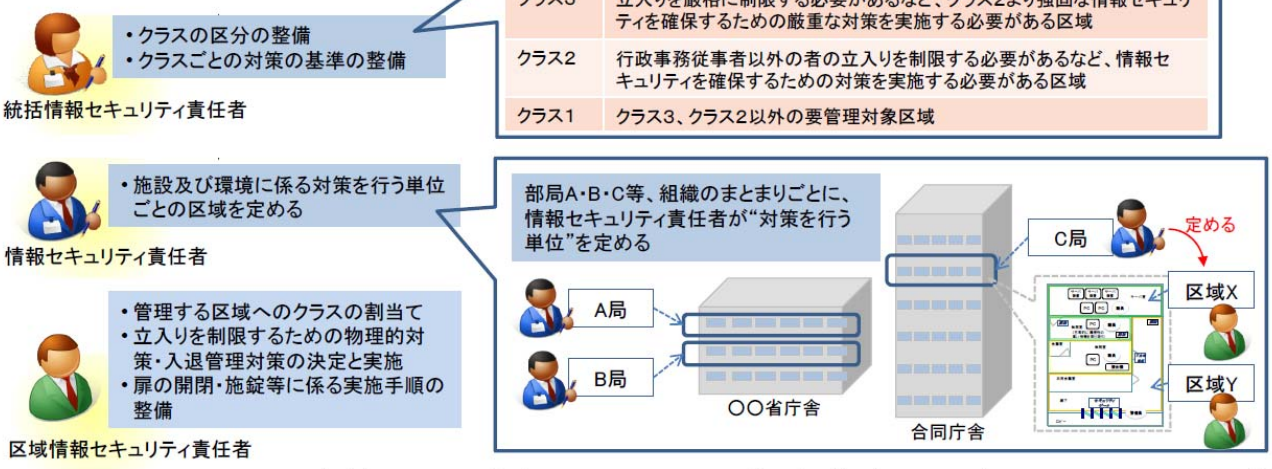
■ 本項の概要

CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

- 執務室、会議室、サーバ室等の情報を取り扱う区域に対して、物理的な対策や入退管理の対策を講ずることで区域の安全性を確保することが必要。

＜主な遵守事項＞
3.2.1(1)(b) 統括情報セキュリティ責任者は、要管理対策区域の特性に応じて、以下の観点を含む対策の基準を定めること。
（ア）*(中略)*施錠可能な扉、間仕切り等の施設の整備、設備の設置等の物理的な対策。
（イ）許可されていない者の立入りを制限するため*(中略)*の入退管理対策。
3.2.1(2)(a) 情報セキュリティ責任者は、*(中略)*対策の基準を踏まえ、施設及び環境に係る対策を行う単位ごとの区域を定めること。
3.2.1(3)(a) 区域情報セキュリティ責任者は、管理する区域に対して定めた対策を実施すること。

■ 責任者ごとの役割



4.1.1 外部委託 ［参考］サプライチェーン・リスクへの対応

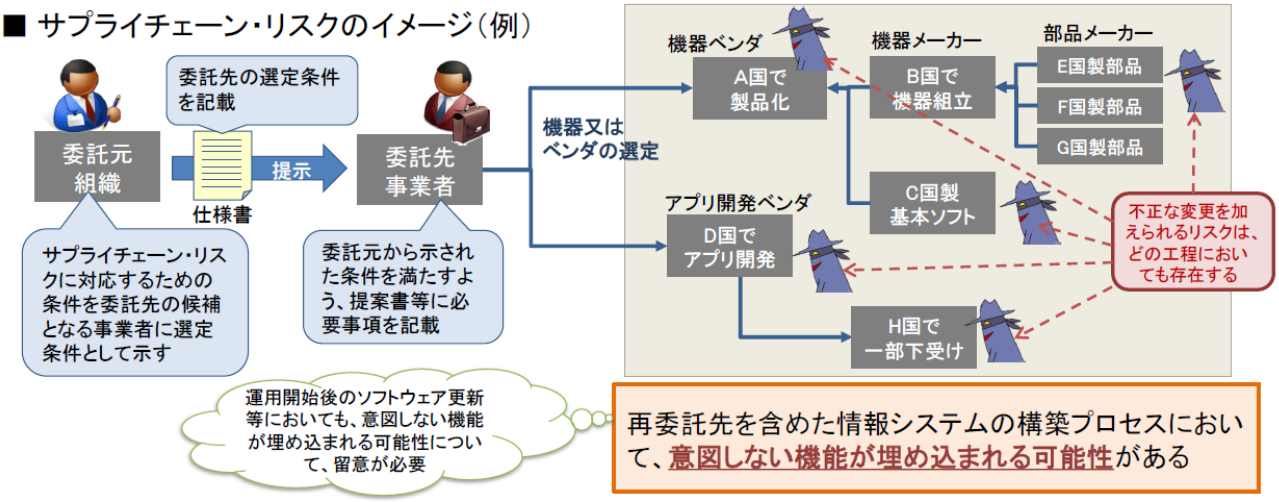
■ サプライチェーン・リスクへの対応

発注元において、
「要求しない機能が存在しない検証」
は著しく困難
（全数検査は事実上不可能）

委託先における委託事業の実施状況及び、サプライチェーン・リスクへの対応のための厳格な管理体制等を求める管理策を強化することで代替。

- 委託先企業又はその従業員、再委託先等による意図せざる変更が加えられないための管理体制の明確化
- 委託事業の実施場所、委託事業従事者の所属・専門性・実績及び国籍に関する情報の提供
- 情報セキュリティ監査の受入れ

■ サプライチェーン・リスクのイメージ（例）



再委託先を含めた情報システムの構築プロセスにおいて、**意図しない機能が埋め込まれる可能性**がある

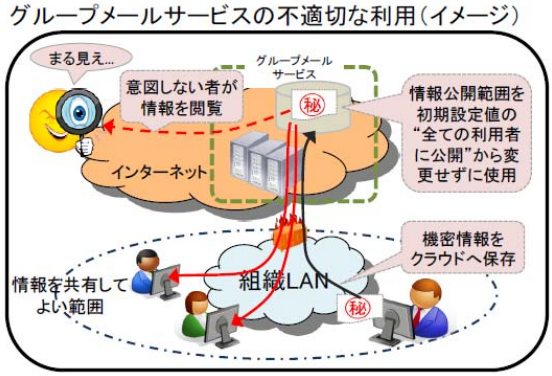
4.1.2 約款による外部サービスの利用② ［参考］機密情報流出の事例

脅威の概要

- 約款に同意して利用する一般消費者向けのサービス（グループメールサービス等）には、情報セキュリティに関する十分な条件設定が行えないものも多く、当該サービスの利用が機密情報の流出につながるおそれがある。

＜最近の事例＞
- 2013年7月　インターネット上でメールを共有できる民間企業の無料サービスで個人情報や中央官庁の内部情報等が誰でも閲覧できる状態になっていた

グループメールサービスの不適切な利用（イメージ）

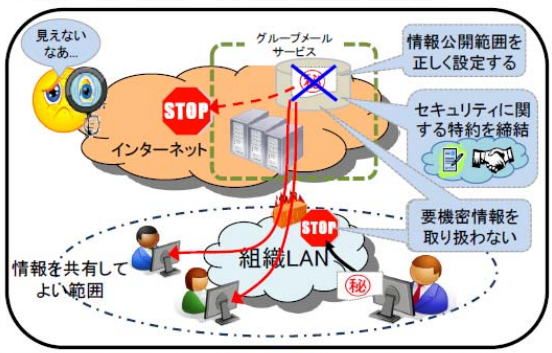


主な対策

- 約款による外部サービスの利用に係る責任者を設置し、アクセス権設定等の安全管理措置を含む利用手順を整備する。
- セキュリティ水準を十分確保するための特約等を締結する（この場合は4.1.1項を遵守）、又は機密性の高い情報を取り扱わない。

＜統一基準群（平成26年度版）における対策事項＞
- 4.1.2項　約款による外部サービスの利用　等

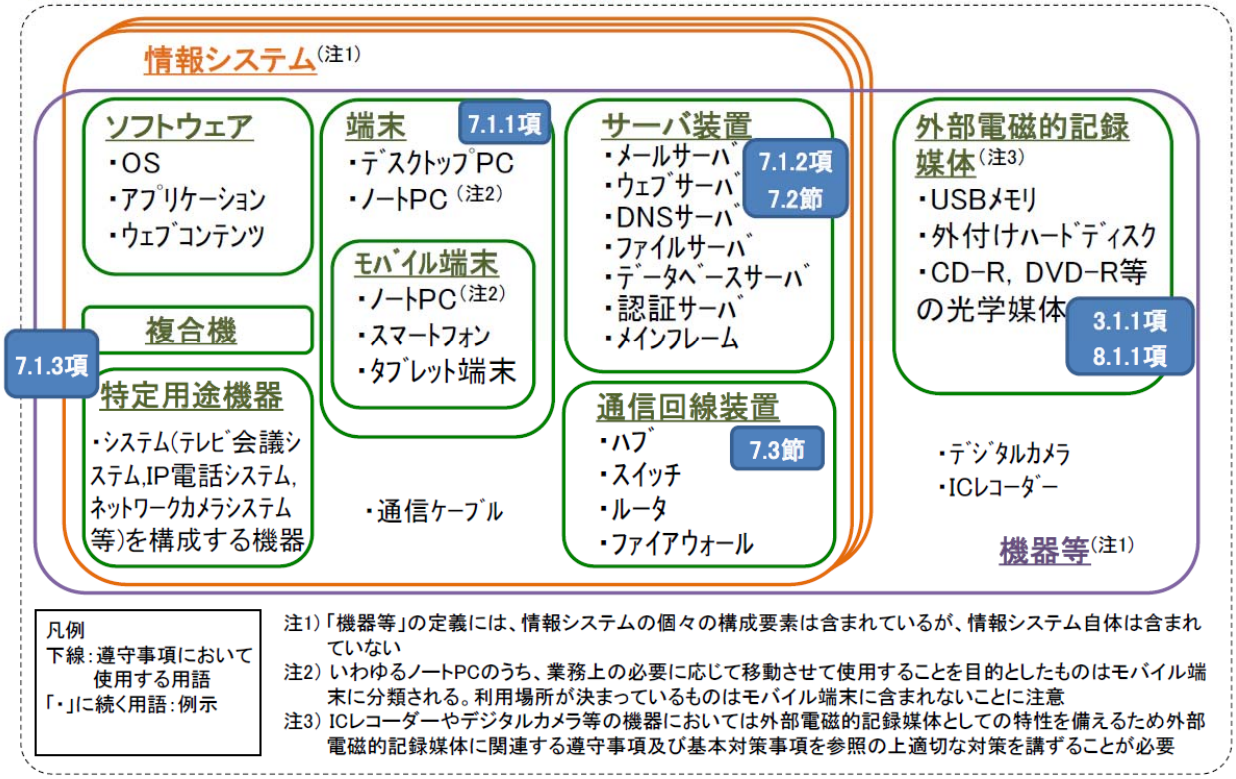
グループメールサービスの適切な利用（例）



（※）約款による外部サービス：民間事業者等が約款に基づきインターネット上で提供する情報処理サービスであって、当該サービスを提供するサーバー装置において利用者が情報の作成、保存、送信等をおこなうものをいう。ただし、利用者が必要とする情報セキュリティに関する十分な条件設定の余地があるものを除く。

7　情報システムの構成要素

■「情報システム」、「機器等」及びその関係



凡例
下線：遵守事項において使用する用語
「・」に続く用語：例示

注1)「機器等」の定義には、情報システムの個々の構成要素は含まれているが、情報システム自体は含まれていない
注2) いわゆるノートPCのうち、業務上の必要に応じて移動させて使用することを目的としたものはモバイル端末に分類される。利用場所が決まっているものはモバイル端末に含まれないことに注意
注3) ICレコーダーやデジタルカメラ等の機器においては外部電磁的記録媒体としての特性を備えるため外部電磁的記録媒体に関連する遵守事項及び基本対策事項を参照の上適切な対策を講ずることが必要

59

IAIS

高度サイバー攻撃対処のための リスク評価等のガイドライン

資料１－１

NISC National Information Security Center

高度サイバー攻撃対処のための リスク評価等のガイドラインについて

平成26年６月
内閣官房情報セキュリティセンター

高度化・巧妙化を続ける標的型攻撃

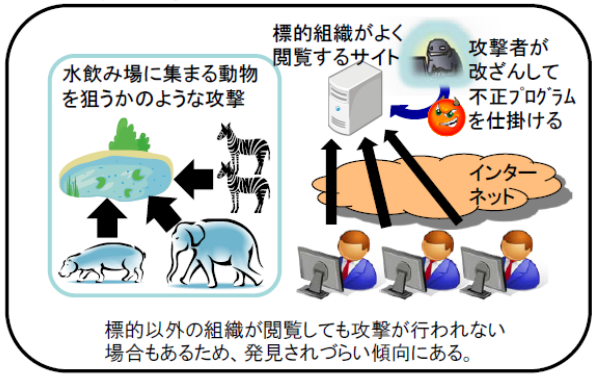
NISC

- 従来の標的型攻撃は見た目で判別可能なものも少なくなかったが、手口の高度化・巧妙化が進んでおり、水飲み場型等の新たな手口による攻撃も発生しているなど、職員側での対策では防ぎきれない状況にある。

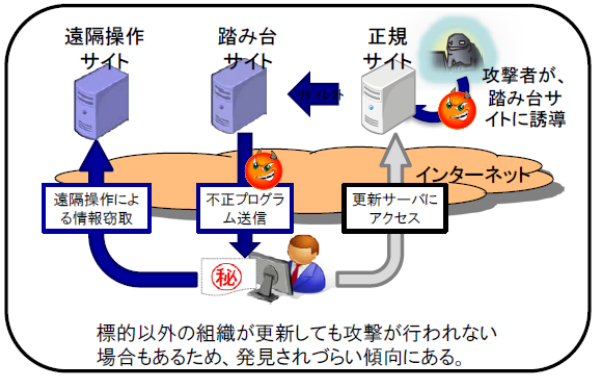
近年見られる標的型攻撃の新たな手口

- 水飲み場型攻撃：標的組織がよく閲覧するウェブサイトを改ざんし、閲覧した端末を不正プログラムに感染させる。
- ソフトウェアの更新プログラムを悪用した攻撃：広く利用されているソフトウェアの正規サイトを改ざんし、ソフトウェアの更新を行った端末を不正プログラムに感染させる。
- やり取り型（メール）攻撃：業務に関連するメールを複数回やりとりし、相手を信用させた上で不正プログラムを添付したメールを送付して感染させる。

水飲み場型攻撃（イメージ）



ソフトウェアの更新プログラムを悪用した攻撃（イメージ）



本取組の全体像

各府省庁

ＣＩＳＯ

① 残存リスク等の把握
② 対策導入計画（案）の評価・承認

リスク評価ダッシュボード

報告等

方針指示

取組の実施方針を組織として決定（予算等の配分を含む。）

関係部署

① 標的とされる蓋然性の高い業務領域の選定
② リスク評価の実施
- 保護対象の特定
- 残存リスク等の把握

③ 対策導入計画（案）の作成
④ リスク評価ダッシュボードの作成

報告

情報セキュリティ対策推進会議 等

報告等

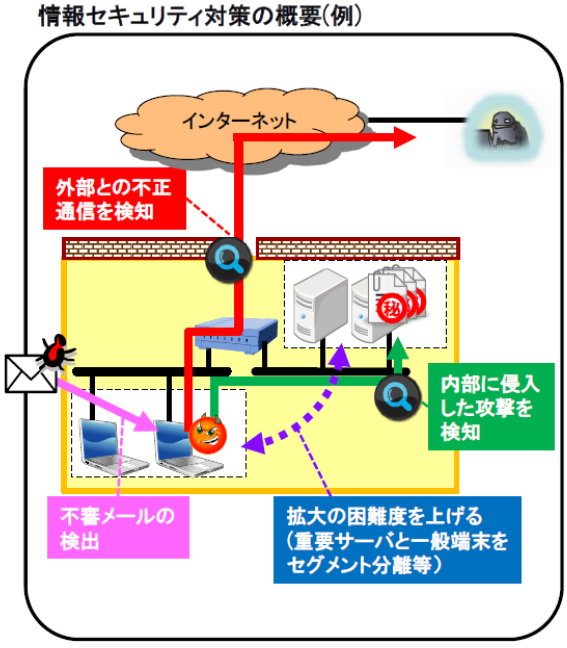
NISC 等

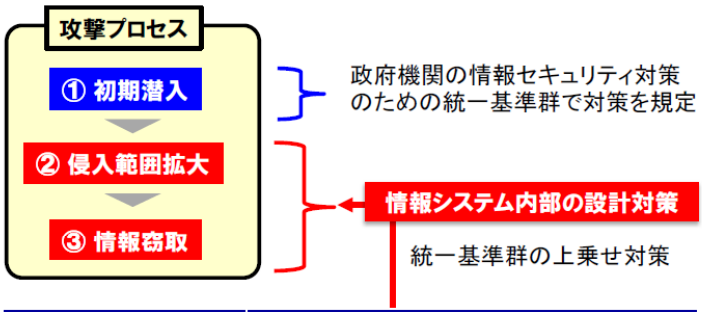
○ 実施状況等の取りまとめ
○ 本取組の見直しに係る検討
○ 対策等に係る評価検討体制の構築を含む本取組の運用管理

高度サイバー攻撃対処のための対策導入

- 情報システムが不正プログラムに感染したとしても、攻撃者が情報の窃取等を達成する前に攻撃を検知・遮断するための対策を導入する。

情報セキュリティ対策の概要(例)





対策目的	対策方針
攻撃を遮断し、侵入範囲の拡大を防止する	• ハッキング技術を用いた内部探索がしづらいシステム設計 • 機器を乗っ取りづらいシステム設計
攻撃の兆候を監視し、早期に発見・検知する	• 攻撃（主に攻撃失敗）の痕跡が残るシステム設計 • 攻撃の兆候を発見・検知するためのトラップ（罠）の設置 • 上記の継続的な監視

CISOによる方針決定

NISC

- リスク評価ダッシュボードによる報告を踏まえ、CISOが対策導入計画の実行方針を承認・決定する。

リスク評価ダッシュボード　CISOによる方針決定等における判断材料として、高度サイバー攻撃対処に係る情報セキュリティ対策の進捗状況等を可視化したもの。

自府省庁において保護対象とする業務領域が妥当かどうか	**①保護対象とする業務領域** ・保護対象とする業務領域の概要 ・脅威事象発生時の影響　等
現状における残存リスクが受容可能な状況かどうか	**②情報システムに係るリスク評価結果** ・対策実施状況に係る現状点検結果 ・現状における残存リスク　等
リスク評価結果等に照らし、計画内容が妥当かどうか	**③次年度以降の対策導入計画** ・次年度の対策導入計画の概要 ・次年度以降の対策実施状況の推移 ・計画時における対策実施状況（予定）　等

スライド 5

IAIS

「高度標的型攻撃」対策に向けたシステム設計ガイドライン

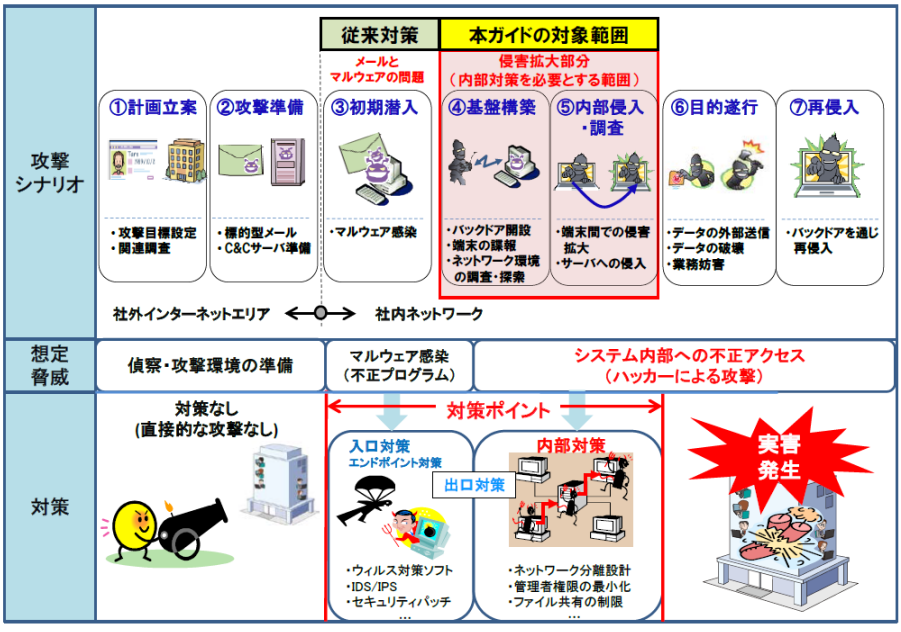


図 2.2.2 攻撃シナリオと対策の関係

「高度標的型攻撃」対策に向けたシステム設計ガイドライン

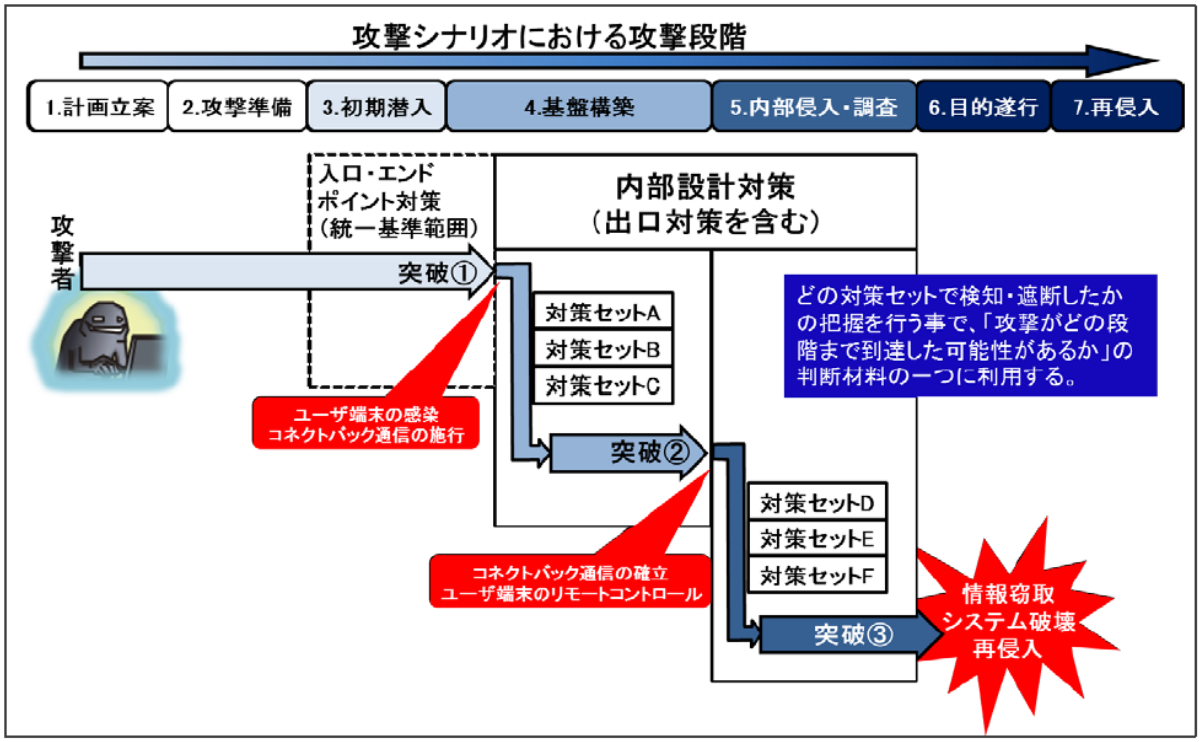


図 2.3-2 各攻撃段階におけるリスク評価チャート

「高度標的型攻撃」対策に向けたシステム設計ガイドライン

セット No	前版との対応*	対策セット名称	統制目標
対策セット A	断①	ネットワーク通信経路設計によるコネクトバック通信の遮断	ユーザ端末から直接インターネット上の C&C サーバへ接続するコネクトバック通信を遮断および検知する。
対策セット B	断③＋視①	認証機能を活用したコネクトバック通信の遮断とログ監視	ユーザ端末から認証機能を持たないプロキシを突破して C&C サーバへ接続するコネクトバック通信を遮断および検知する。
対策セット C	断②＋視②	プロキシのアクセス制御によるコネクトバック通信の遮断と監視	CONNECT メソッドを利用してセッションを維持するコネクトバック通信を遮断および検知する。
対策セット D	断④＋断⑤	運用管理専用の端末設置とネットワーク分離と監視	ユーザ端末に保存されている重要情報（運用管理業務で使われている管理者情報や機微情報など）の窃取を防止し検知する。
対策セット E	断⑦＋視⑤＋新規視③	ファイル共有の制限とトラップアカウントによる監視	攻撃者によりリモートコントロールされたユーザ端末から、周囲のユーザ端末へファイル共有機能を悪用した内部侵害拡大を防止する。また、ファイル共有が業務上必要な場合は監視を強化し、不正なファイル共有機能の利用を検知する。
対策セット F	断⑥＋新規視④	管理者権限アカウントのキャッシュ禁止とログオンの監視	攻撃者に管理者権限のアカウント情報を窃取させない。および、万が一窃取されたときも管理者権限のアカウントの不正使用を検知する。

*対応 ： 前版にて記載したシステム設計対策セットとの対応　【凡例】 断: 遮断策　　視: 監視策

# 情報セキュリティを企画・設計段階から確保するための方策
SBD(Security by Design)

情報セキュリティを企画・設計段階から確保するための方策 (SBD(Security by Design))

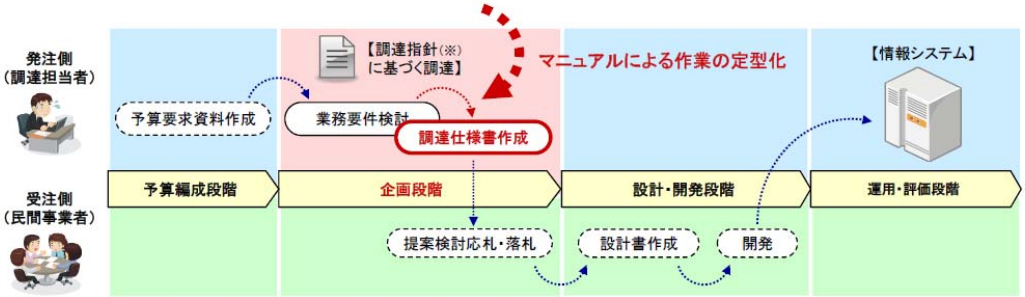
NISC

問題認識： 行政情報システムの企画・設計段階から情報セキュリティ対策を考慮すべき

SBD検討会構成員
（座長）東工大 山岡准教授
（委員）大手ベンダー、システム関連事業者関連団体、府省庁CIO補佐官 等
（オブザーバ）関連府省庁 等

『情報セキュリティを企画・設計段階から確保するための方策に係る検討会（SBD検討会）』を設置
- 検討課題
  - ✓ 調達仕様書の「**情報セキュリティ要件の不明瞭さ**」から、調達者と供給者の合意形成に支障を来す。
  - ✓ 結果として、「**不公平な調達**」、「**過度なセキュリティ対策**」、運用開始後の「**セキュリティ事故**」を招くおそれ。
- 解決方針
  - ✓ 調達担当者が調達仕様書作成時に「**情報セキュリティに係る仕様**」を適切に組み込める方法を確立する。

検討成果
『情報システムに係る政府調達におけるセキュリティ要件策定マニュアル』
- 調達担当者がシステム特性に応じて「**調達仕様書にセキュリティ要件を記載する方法**」を解説
- 「**対策要件集**」及び「**対策要件選定作業の定型化**」等のツールによる調達担当者の支援



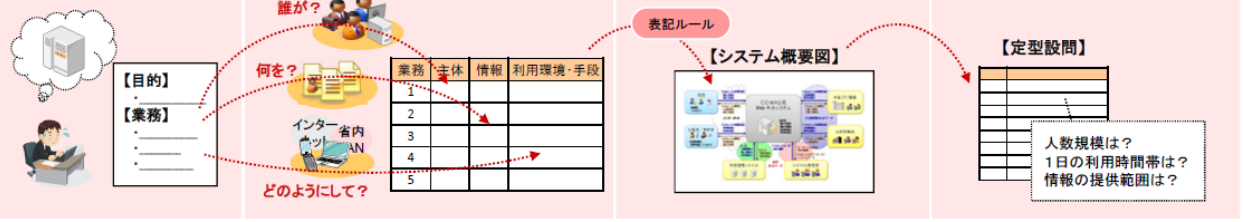
※ 調達指針：情報システムに係る政府調達の基本指針（H19.3.1 CIO 連絡会議決定）

『情報システムに係る政府調達におけるセキュリティ要件策定マニュアル』による作業の定型化

【マニュアル利用場面】 調達指針に基づく調達において、調達仕様書に盛り込むべきセキュリティ要件を検討する際に以下の作業を行う。

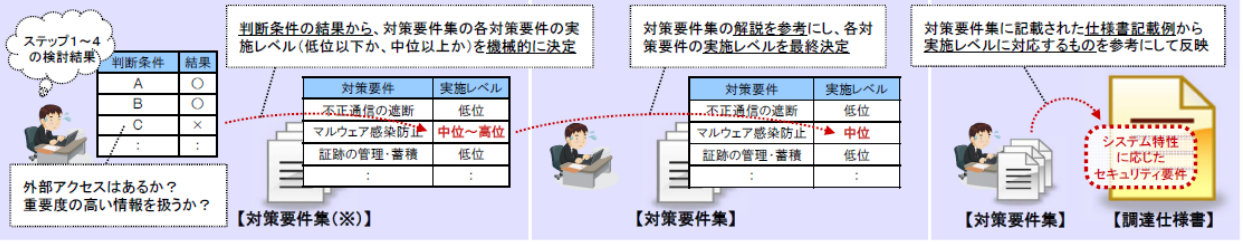
■ 業務要件の検討 （対象業務をシステム概要図にまとめ、定型設問に回答する）【※ 他の方法による代替可】

ステップ1	ステップ2	ステップ3	ステップ4
目的及び業務を洗い出す	業務の特徴を3つの観点から整理する	システム概要図を表記ルールに基づいて作成し、要件を俯瞰する	定型設問により業務要件を詳細化する



■ セキュリティ要件の策定 （業務要件を判断条件にあてはめ対策要件を決定する）

ステップ5	ステップ6	ステップ7
判断条件を判定し、対策要件ごとの実施レベルを検討する	実施レベルを確定し、対策要件を決定する	調達仕様書に反映する



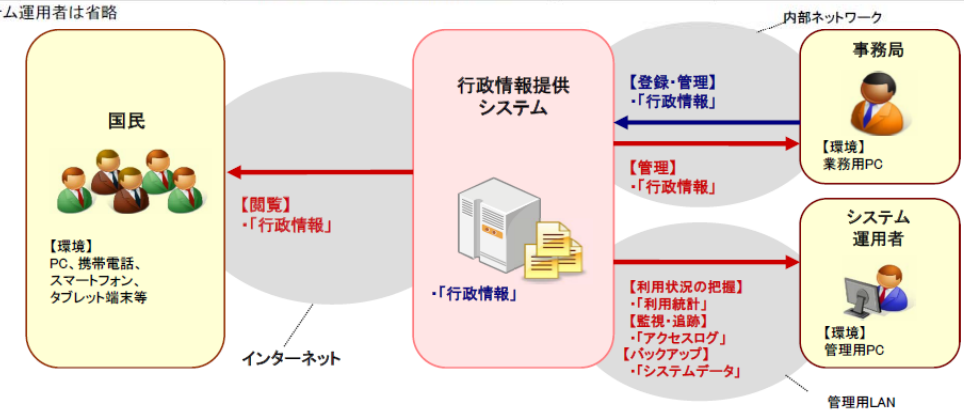
（※）侵害対策、不正監視等の24種類の対策要件、3段階の実施レベル（対策の強度）に応じた仕様書記載例に関する解説

活用例①行政情報提供システム：ステップ1～4

- 行政情報（機密性1）をウェブページに公開する、一般的な行政情報提供のためのWEBページシステムを想定する。

主体	業務	業務（細分化後）の概要	情報	利用環境・手段
国民	行政情報の閲覧	行政情報を表示し、内容を確認する。	「行政情報」	インターネット、PC、携帯電話、スマートフォン、タブレット端末
事務局	行政情報の登録	サーバにコンテンツ（行政情報）を登録する。	「行政情報」	内部ネットワーク、業務用PC
		サーバに登録済みのコンテンツ（行政情報）を更新及び削除する。	「行政情報」	

※システム運用者は省略



 スライド 7

活用例①行政情報提供システム：ステップ5　判断条件による検討

- 整理した業務要件や判断条件の解説等を参考に、6つの設問に「○」「×」の二択で回答する

名称	観点分類	判断条件	判断結果	判断結果の解説
A. 外部アクセスの有無	利用環境・手段	インターネット等の通信回線を介して（情報の管理ポリシが異なる）外部から情報システムにアクセスしてサービスの利用、業務の遂行、情報システムの管理等を行うか。	○	インターネットを介して情報システムにアクセスされる
B. 情報の重要度	情報	漏えいした場合や正常にアクセスできない場合に、深刻な損害を被る可能性がある重要性の高い情報を取り扱うか。	×	扱う情報は公開情報（機密性1）であり、重要性の高い情報は取り扱わない
C. 情報保存時の安全性	情報	入退室管理等の物理対策だけでなく、情報システムが保存する情報についてより一層の安全を期すために追加的対策をさらに行うべきと考えるか。	×	情報の重要性は低く、サーバ上での保存のみ（モバイルPCによる情報処理等なし）のため、不要
D. 利用者の限定要否	主体	情報システムにアクセスする主体は、利用資格のある者、職員、グループのメンバー等の特定の者に限定されるか。	×	システムへアクセスする利用者（国民）※は特定の者に限定されない
E. アカウントの多様性	主体	利用者によって利用可能なサービスや業務が異なる等、利用者の特徴にバリエーションがあるか。	×	想定されない
F. 複数部局による利用	主体	情報の取り扱い方や利用目的等が異なる複数の部局等の間で共用されるか。	×	想定されない

※管理者は除く
（管理者権限の保護対策は必ず要件に含まれる）

ステップ6へ

活用例①行政情報提供システム：ステップ6　対策要件の決定

- ステップ5の結果から自動的に得られた推奨結果と、付録Aの対策要件解説を参考に、実施レベル（省略／低／中／高）を決定する

対策区分	対策方針	対策要件	判断条件対応関係	実施レベル 省略	低位	中位	高位
侵害対策（AT: Attack）	通信回線対策（AT-1）	通信経路の分離（AT-1-1）	A or F			○	
		不正通信の遮断（AT-1-2）	A			○	
		通信のなりすまし防止（AT-1-3）				○	
		サービス不能化の防止（AT-1-4）				○	
	不正プログラム対策（AT-2）	マルウェアの感染防止（AT-2-1）	-		○		
		マルウェア対策の管理（AT-2-2）	A or B	○			
	セキュリティホール対策（AT-3）	構築時の脆弱性対策（AT-3-1）	-		○		
		運用時の脆弱性対策（AT-3-2）	A			○	
不正監視・追跡（AU: Audit）	証跡管理（AU-1）	証跡の蓄積・管理（AU-1-1）	B or C		○		
		証跡の保護（AU-1-2）			○		
		時刻の正確性確保（AU-1-3）	-		○		
	不正監視（AU-2）	侵入検知（AU-2-1）	A			○	
		サービス不能化の検知（AU-2-2）		○			
アクセス・利用制限（AC: Access）	主体認証（AC-1）	主体認証（AC-1-1）	D	○			
	アカウント管理（AC-2）	ライフサイクル管理（AC-2-1）	D	○			
		アクセス権管理（AC-2-2）	E	○			
		管理者権限の保護（AC-2-3）	-		○		
データ保護（PR:Protect）	機密性・完全性の確保（PR-1）	通信経路上の盗聴防止（PR-1-1）	B or C	○			
		保存情報の機密性確保（PR-1-2）		○			
		保存情報の完全性確保（PR-1-3）		○			
物理対策（PH:Physical）	情報搾取・侵入対策（PH-1）	情報の物理的保護（PH-1-1）	-		○		
		侵入の物理的対策（PH-1-2）			○		
障害対策（事業継続対応）（DA: Damage）	構成管理（DA-1）	システムの構成管理（DA-1-1）	B		○		
	可用性確保（DA-2）	システムの可用性確保（DA-2-1）	-		○		

：ステップ5の判断条件の結果に基づき、提示される推奨レベル

情報システムに係る政府調達における情報セキュリティ要件策定マニュアル 対策要件一覧

※ 二重下線(青字)の箇所については、仕様書に記載する際には具体化が必要な箇所である。

対策区分		対策方針		対策要件の名称		判断条件対応関係	仕様記載例(案)【低位】	仕様記載例(案)【中位】	仕様記載例(案)【高位】
AT	侵害対策	AT-1	通信回線対策	AT-1-1	通信経路の分離	A or F		不正の防止及び発生時の影響範囲を限定するため、所属する府省庁とは情報の管理ポリシーが異なる外部と通信を行う電子計算機及び内部のみと通信を行う電子計算機を通信回線上で分離すること。	不正の防止及び発生時の影響範囲を限定するため、所属する府省庁とは情報の管理ポリシーが異なる外部との通信の有無、業務目的、所属部局等の情報の管理体制に応じて電子計算機を通信回線上で分離すること。
				AT-1-2	不正通信の遮断	A		通信回線を介した不正を防止するため、不正アクセス及び許可されていない通信プロトコルを通信回線上にて遮断する機能を備えること。	(← 同様)
				AT-1-3	通信のなりすまし防止	A		情報システムのなりすましを防止するために、サーバの認証機能を備えること。	情報システムのなりすましを防止するために、サーバの認証機能を備えるとともに、許可されていない端末、サーバ装置、通信回線装置の接続を防止する機能を備えること。
				AT-1-4	サービス不能化の防止	A		サービスの継続性を確保するため、構成機器が備えるサービス停止の脅威の軽減に有効な機能を活用して情報システムを構築すること。	サービスの継続性を確保するため、情報システムの負荷がしきい値を超えた場合に、通信遮断や処理量の抑制等によってサービス停止の脅威を軽減する機能を備えること。
		AT-2	不正プログラム対策	AT-2-1	マルウェアの感染防止	-	マルウェア(ウィルス、ワーム、ボット等)による脅威に備えるため、マルウェアの感染を防止する機能を備えるとともに、新たに発見されるマルウェアに対応するために機能の更新が可能であること。	(← 同様)	(← 同様)
				AT-2-2	マルウェア対策の管理	A or B			システム全体としてマルウェアの感染防止機能を確実に動作させるため、当該機能の動作状況及び更新状況を一元管理する機能を備えること。
		AT-3	セキュリティホール対策	AT-3-1	構築時の脆弱性対策	-	情報システムを構成するソフトウェア及びハードウェアの脆弱性に悪用した不正を防止するため、開発時及び構築時に脆弱性の有無を確認の上、運用上対処が必要な脆弱性は修正の上で納入すること。	(← 同様)	(← 同様)
				AT-3-2	運用時の脆弱性対策	A	運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を行う方法(手順等)を備えること。	運用開始後、新たに発見される脆弱性を悪用した不正を防止するため、情報システムを構成するソフトウェア及びハードウェアの更新を効率的に実施する機能を備えるとともに、情報システム全体の更新漏れを防止する機能を備えること。	(← 同様)
AU	不正監視・追跡	AU-1	証跡管理	AU-1-1	証跡の蓄積・管理	B or C	情報システムに対する不正の検知、発生原因の特定に用いるために、情報システムの利用記録、例外	情報システムに対する不正の検知、発生原因の特定に用いるために、情報システムの利用記録、例外	(← 同様)

AU	不正監視・追跡	AU-1	証跡管理	AU-1-1	証跡の蓄積・管理	B or C	情報システムに対する不正の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関する証跡を蓄積し、【　　】の期間保管すること。	情報システムに対する不正の検知、発生原因の特定に用いるために、情報システムの利用記録、例外的事象の発生に関する証跡を蓄積し、【　　】の期間保管するとともに、不正の検知、原因特定に有効な管理機能(証跡の検索機能、証跡の蓄積不能時の対処機能等)を備えること。	(← 同様)
				AU-1-2	証跡の保護	B or C	証跡の不当な消去や改ざんを防止するため、証跡に関するアクセス制御機能を備えること。	証跡の不当な消去や改ざんを防止するため、証跡に対するアクセス制御機能を備えるとともに、ログのアーカイブデータの保護(消失及び破壊や改ざんの脅威の軽減)のための措置を含む設計とすること。	証跡の不当な消去や改ざんを防止するため、証跡に対するアクセス制御機能及び消去や改ざんの事案を検出する機能を備えるとともに、ログのアーカイブデータの保護(消失及び破壊や改ざんの脅威の軽減)のための措置を含む設計とすること。
				AU-1-3	時刻の正確性確保	-	不正行為の追跡や情報セキュリティ侵害時において証跡の解析等を容易にするため、システム内の機器を正確な時刻に同期する機能を備えること。	(← 同様)	(← 同様)
		AU-2	不正監視	AU-2-1	侵入検知	A		不正行為を迅速に対処するため、通信回線を介して所属する府省庁外と送受信される通信内容を監視し、不正アクセスや不正侵入を検知及び通知する機能を備えること。	不正行為に迅速に対処するため、府省庁内外で送受信される通信内容の監視及びサーバ装置のセキュリティ状態の監視等によって、不正アクセスや不正侵入を検知及び通知する機能を備えること。
				AU-2-2	サービス不能化の検知	A			サービスの継続性を確保するため、大量のアクセスや機器の異常による、サーバ装置、通信回線装置又は通信回線の過負荷状態を検知する機能を備えること。
AC	アクセス・利用制限	AC-1	主体認証	AC-1-1	主体認証	D		情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち【　　】の認証を行う機能として、【　】の条件を満たす方式を採用すること。	情報システムによるサービスを許可された者のみに提供するため、情報システムにアクセスする主体のうち【　　】の認証を行う機能及び主体認証情報の推測や盗難等のリスクの軽減を行う機能として、【　　】の条件を満たす方式を採用すること。
		AC-2	アカウント管理	AC-2-1	ライフサイクル管理	D		主体のアクセス権を適格に管理するため、主体が用いるアカウント(識別コード、主体認証情報、権限等)を管理(登録、更新、停止、削除等)するための機能を備えること。	(← 同様)
				AC-2-2	アクセス権管理	E			情報システムの利用範囲を利用者の職務に応じて制限するため、情報システムのアクセス権を職務に応じて制御する機能を備えるとともに、アクセス権の割り当てを適切に設計すること。
				AC-2-3	管理者権限の保護	-	アカウント管理者による不正を防止するため、アカウントの管理権限を制御する機能を備えること。	(← 同様)	(← 同様)
PR	データ保護	PR-1	機密性・完全性の確保	PR-1-1	通信経路上の盗聴防止	B or C		通信回線に対する盗聴行為や利用者の不注意による情報の漏えいを防止するため、通信回線を暗号化する機能を備えること。	(← 同様)
				PR-1-2	保存情報の機密性確保	B or C		情報システムに蓄積された情報の搾取や漏えいを防止するため、保護すべき情報を利用者が直接アクセス可能な機器に保存しないこと。	情報システムに蓄積された情報の搾取や漏えいを防止するため、保護すべき情報を利用者が直接アクセス可能な機器に保存しないことに加えて、保存された情報を暗号化する機能を備えること。
				PR-1-3	保存情報の完全性確保	B or C			情報の改ざんや意図しない消去等のリスクを軽減するため、情報の改ざんを検知する機能又は改ざんされていないことを証明する機能を備えること。
PH	物理対策	PH-1	情報搾取・	PH-1-1	情報の物理的保	-	情報の漏えいを防止するため、【　　】等に	(← 同様)	(← 同様)

マイナンバー制度

マイナンバー

社会保障・税番号制度

愛称：マイナちゃん

概要資料

平成27年５月版

内閣官房 社会保障改革担当室

内閣府 大臣官房 番号制度担当室

マイナンバー制度の導入趣旨

番号制度は、複数の機関に存在する個人の情報を同一人の情報であるということの確認を行うための基盤であり、社会保障・税制度の効率性・透明性を高め、国民にとって利便性の高い公平・公正な社会を実現するための社会基盤（インフラ）である。

社会保障・税・災害対策の各分野で番号制度を導入

効果

- より正確な所得把握が可能となり、社会保障や税の給付と負担の公平化が図られる
- 真に手を差し伸べるべき者を見つけることが可能となる
- 大災害時における真に手を差し伸べるべき者に対する積極的な支援に活用できる
- 社会保障や税に係る各種行政事務の効率化が図られる
- ＩＴを活用することにより添付書類が不要となる等、国民の利便性が向上する
- 行政機関から国民にプッシュ型の行政サービスを行うことが可能となる

実現すべき社会

- より公平・公正な社会
- 社会保障がきめ細やかかつ的確に行われる社会
- 行政に過誤や無駄のない社会
- 国民にとって利便性の高い社会
- 国民の権利を守り、国民が自己情報をコントロールできる社会

1

マイナンバー制度の概要

番号制度は、複数の機関に存在する特定の個人の情報を同一人の情報であるということの確認を行うための基盤であり、社会保障・税制度の効率性・透明性を高め、国民にとって利便性の高い公平・公正な社会を実現するための基盤（インフラ）である。

個人番号

- 市町村長は、住民票コードを変換して得られる個人番号（12桁）を指定し、通知カードにより本人に通知

個人番号カード

- 市町村長は、申請により、顔写真付きの個人番号カードを交付
- 個人番号カードは、本人確認や番号確認のために利用

法人番号

- 国税庁長官は、法人等に、法人番号（13桁）を指定し、通知
- 法人番号は原則公開され、民間での自由な利用が可能

個人情報保護

- 法定される場合を除き、特定個人情報の収集・保管を禁止
- 国民は情報提供等記録開示システムで、情報連携記録を確認
- 個人番号の取扱いを監視・監督する特定個人情報保護委員会を設置
- 特定個人情報ファイル保有前の特定個人情報保護評価を義務付け

情報連携

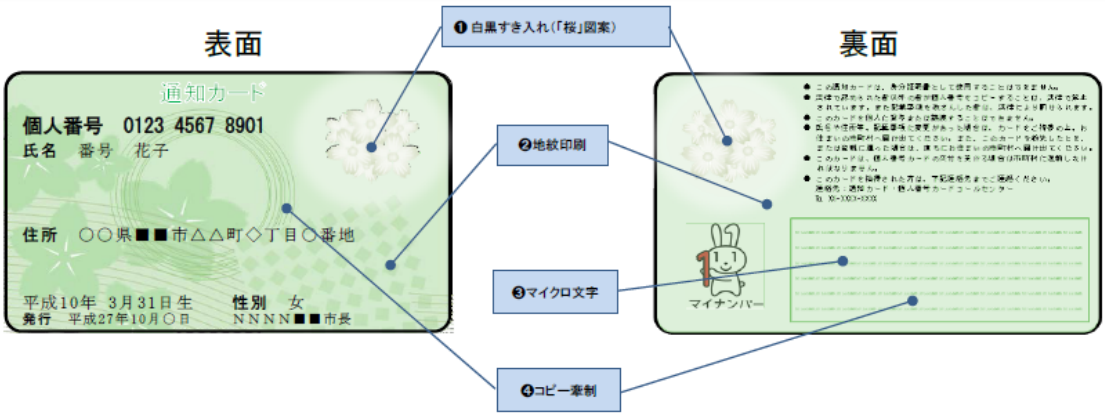
- 複数の機関間において、それぞれの機関ごとに個人番号やそれ以外の番号を付して管理している同一人の情報を紐付けし、相互に活用する仕組み

個人番号の利用分野		
社会保障分野	年金分野	年金の資格取得・確認、給付を受ける際に利用
	労働分野	雇用保険等の資格取得・確認、給付を受ける際に利用 ハローワーク等の事務等に利用
	福祉・医療・その他分野	医療保険等の保険料徴収等の医療保険者における手続に利用 福祉分野の給付を受ける際に利用 生活保護の実施等に利用 低所得者対策の事務等に利用
税分野		国民が税務当局に提出する確定申告書、届出書、調書等に記載 当局の内部事務等に利用
災害対策分野		被災者生活再建支援金の支給に関する事務に利用 被災者台帳の作成に関する事務に利用

- 上記の他、福祉、保健若しくは医療その他の社会保障、地方税又は防災に関する事務その他これらに類する事務であって条例で定める事務に利用（第9条第2項）。

2

通知カード（案）



セキュリティ対策	内容と必要性
❶ 白黒すき入れ	図柄の陰影を表現可能な透かし技術で、紙幣と同様の偽造対策効果あり。（複写不可、偽造困難）
❷ 地紋印刷	微細な線やグラデーション等で複雑な模様を背景に施すことにより、偽変造が困難となる。
❸ マイクロ文字	特定の箇所に通常のコピー機やプリンターでは印刷できない微細な文字を配置することにより、偽造が困難となる。
❹ コピー牽制	コピー時に「複写」の文字が浮かび上がることで、複写による偽造が困難となる。

3

個人番号カード

市町村長は、当該市町村が備える住民基本台帳に記録されている者に対し、その者の申請により、その者に係る個人番号カードを交付するものとする。（第17条第1項）

個人番号カードの券面には、「氏名」、「住所」、「生年月日」、「性別」、「個人番号」等が記載され、「本人の写真」が表示され、かつ、これらの事項等がICチップに記録される。（第2条第7項）

① 個人番号カードは、本人確認の措置において利用する。（第16条）

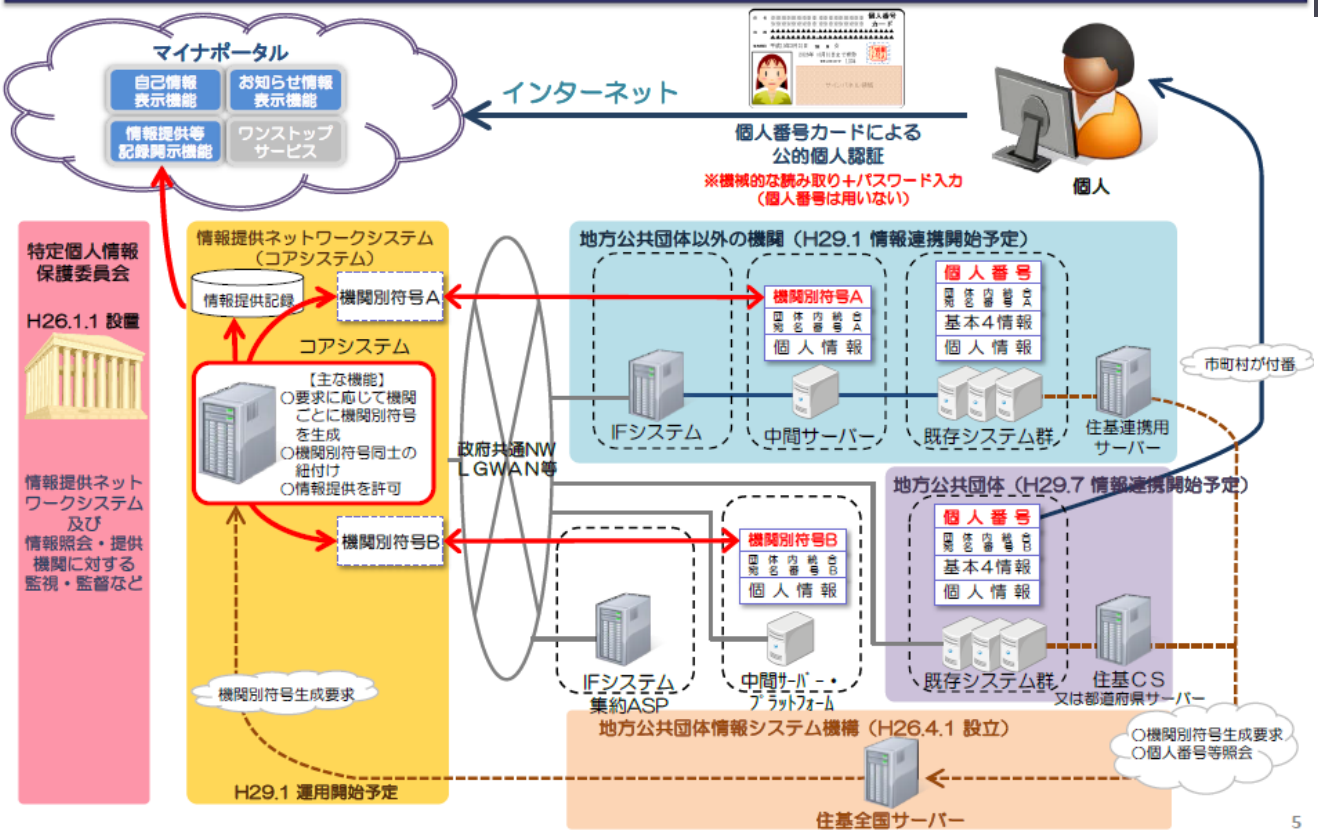
② 市町村の機関は、個人番号カードを、地域住民の利便性の向上に資するものとして条例で定める事務に利用することができる。（第18条第1号）

③ マイナポータルへのログイン手段として、「電子利用者証明」の仕組みによる公的個人認証に利用する。

④ 個人番号カードの所管は、総務省とする。

4

マイナンバー制度における情報連携の概要



マイナンバー制度における安心・安全の確保

マイナンバー制度に対する国民の懸念

- 個人番号を用いた個人情報の追跡・名寄せ・突合が行われ、集積・集約された**個人情報が外部に漏えい**するのではないかといった懸念。
- 個人番号の不正利用等（例：他人の個人番号を用いた**成りすまし**）等により財産その他の被害を負うのではないかといった懸念。
- 国家により個人の様々な個人情報が個人番号をキーに名寄せ・突合されて**一元管理**されるのではないかといった懸念

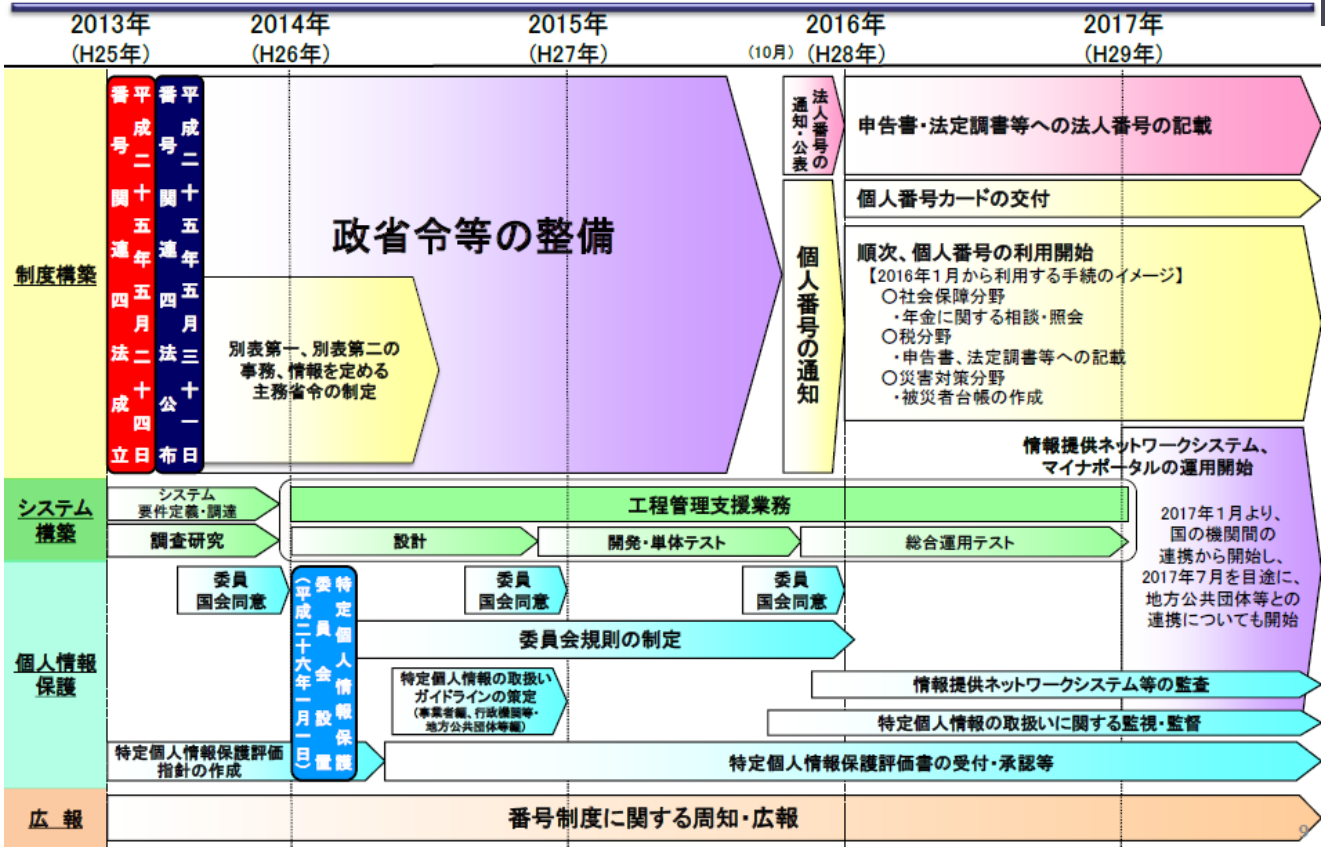
制度面における保護措置

① 本人確認措置（個人番号の確認・身元（実存）の確認）（番号法第16条）
② 番号法の規定によるものを除き、特定個人情報（マイナンバーをその内容に含む個人情報）の収集・保管、特定個人情報ファイルの作成を禁止（番号法第20条、第28条）
③ 特定個人情報保護委員会による監視・監督（番号法第50条～第52条）
④ 罰則の強化（番号法第67条～第77条）
⑤ マイナポータルによる情報提供等記録の確認（番号法附則第6条第5項）

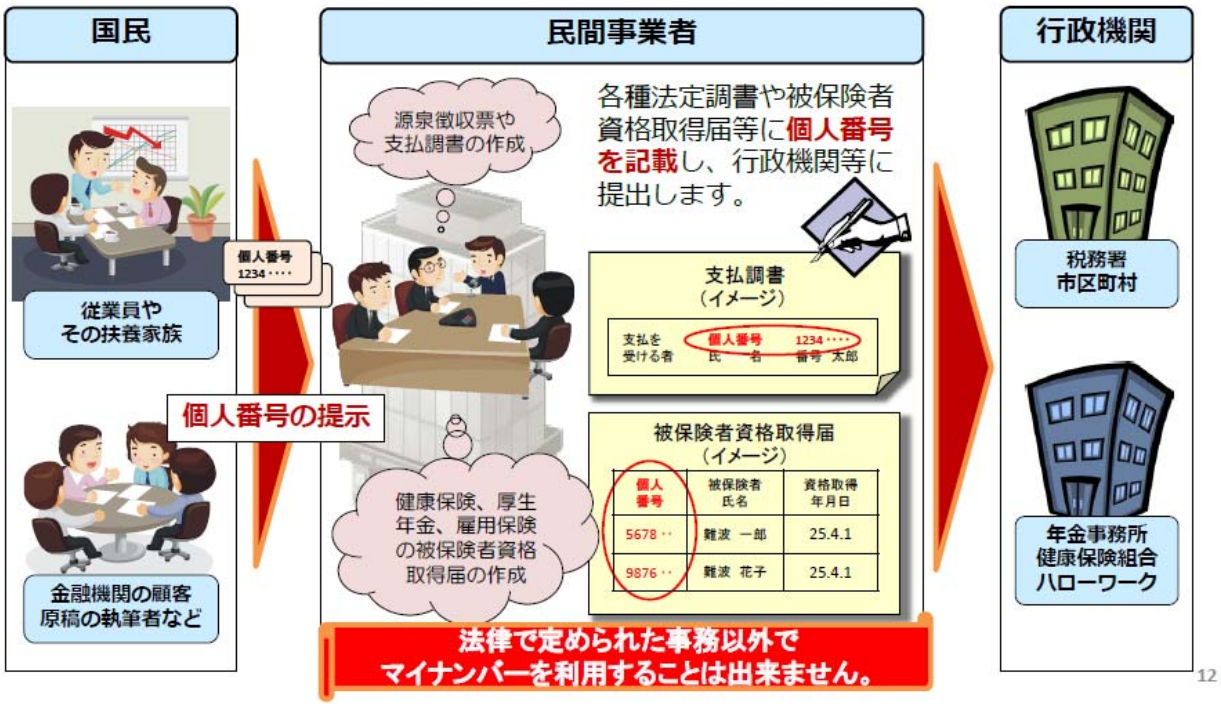
システム面における保護措置

① 個人情報を一元的に管理せずに、分散管理を実施
② 個人番号を直接用いず、符号を用いた情報連携を実施
③ アクセス制御により、アクセスできる人の制限・管理を実施
④ 通信の暗号化を実施

マイナンバー制度導入のロードマップ（案）



民間事業者も、税や社会保障の手続で、マイナンバーを取り扱います。



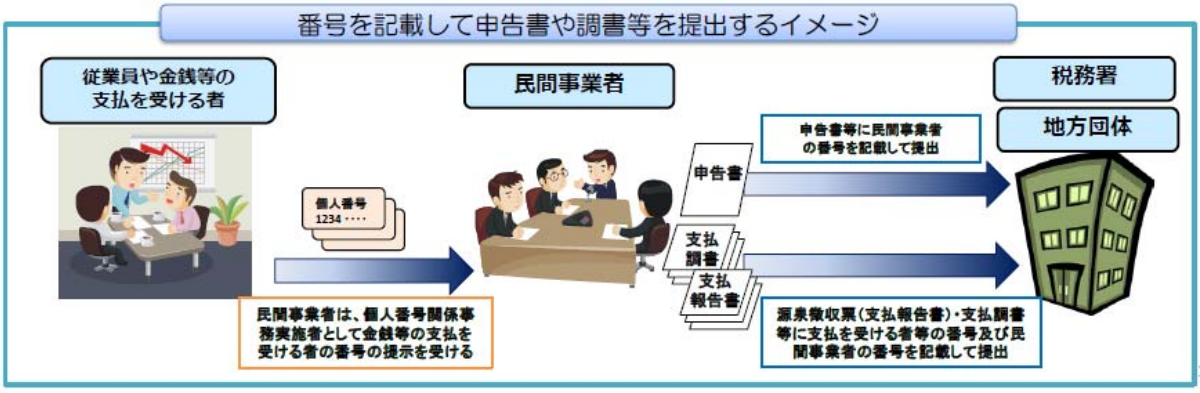
税務関係の申告書等に、マイナンバーを記載して提出します。

国税通則法　（書類提出者の氏名、住所及び番号の記載等）
第百二十四条　国税に関する法律に基づき税務署長その他の行政機関の長又はその職員に申告書、申請書、届出書、調書その他の書類を提出する者は、当該書類にその氏名（法人については、名称。以下この項において同じ。）、住所又は居所及び番号（番号を有しない者にあつては、その氏名及び住所又は居所）を記載しなければならない。（略）
※地方税関係の申告書等の様式については、地方税に関する法令に規定。

税務関係の申告書、申請書、届出書、調書その他の書類に番号を記載

○ 税務関係の申告書、申請書、届出書、調書その他の書類に番号の記載欄を追加
○ 法定調書等については、主に支払者及び支払を受ける者の個人番号又は法人番号を記載
○ これ以外にも、例えば、
・給与所得の源泉徴収票（給与支払報告書）には、控除対象配偶者及び控除対象扶養親族等の個人番号を記載
・生命保険金等の支払調書には、その支払の基礎となる契約を締結した者の個人番号又は法人番号を記載

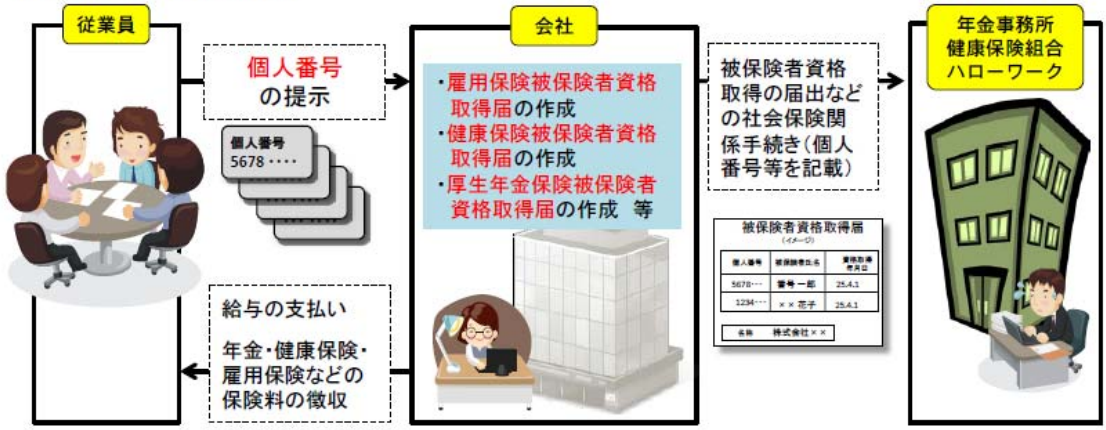
番号を記載して申告書や調書等を提出するイメージ



13

社会保障関係の申請書等に、マイナンバーを記載して提出します。

従業員の給与・福利厚生



主な提出書類の例	提出者	提出先	根拠条文
雇用保険被保険者資格取得届	適用事業所の事業主	ハローワーク	雇用保険法施行規則第6条
雇用保険被保険者資格喪失届	適用事業所の事業主	ハローワーク	雇用保険法施行規則第7条
健康保険・厚生年金保険被保険者資格取得届	適用事業所の事業主	健康保険組合・日本年金機構	健康保険法施行規則第24条 厚生年金保険法施行規則第15条
健康保険・厚生年金保険被保険者資格喪失届	適用事業所の事業主	健康保険組合・日本年金機構	健康保険法施行規則第29条 厚生年金保険法施行規則第22条

15

マイナンバー取得の際の本人確認では、番号確認と身元確認を行います。

個人番号の確認	身元（実存）の確認
 個人番号カード	 個人番号カード
通知カード or 住民票（番号付き） 等	運転免許証 or パスポート 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	※ 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

18

マイナンバーには、利用、提供、収集の制限があります。

【マイナンバーの利用制限】
○マイナンバーの利用範囲は、法律に規定された社会保障、税及び災害対策に関する事務に限定されています。本人の同意があったとしても、利用目的を超えて利用することはできません。※例：マイナンバーを社員番号に利用することはできません。

【マイナンバーの提供の要求】
○社会保障及び税に関する手続書類の作成事務を行う必要がある場合に限って、本人などに対してマイナンバーの提供を求めることができます。

【マイナンバーの提供の求めの制限】
○法律で限定的に明記された場合を除き、マイナンバーの提供を求めてはなりません。

【特定個人情報の提供制限】
○法律で限定的に明記された場合を除き、特定個人情報を提供してはなりません。

【特定個人情報の収集制限】
○法律で限定的に明記された場合を除き、特定個人情報を収集してはなりません。

21

マイナンバーの保管（廃棄）にも制限があります。

【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。

24

法人にも法人番号（13桁）が指定され、個人番号と異なり、どなたでも自由に利用可能です。

指定
・国税庁長官は、①設立登記法人、②国の機関、③地方公共団体、④その他の法人や団体に13桁の法人番号を指定します。
・これら以外の法人等でも一定の要件を満たす場合、届け出ることにより法人番号の指定を受けることができます。
会社や国の機関等については、特段の手続を要することなく、法人番号が指定されます。

ポイント！
１法人に１番号のみ

通知
・平成27年10月から法人の皆さまに法人番号などを記載した通知書の送付を開始する予定です。

ポイント！
登記上の所在地に通知書をお届け

公表
・法人番号を指定した法人等の①名称、②所在地、③法人番号をインターネットを通じて公表します。
WWW

ポイント！
法人番号はどなたでも自由に利用可能

25

法人番号は、名称・所在地と共にインターネット上で公表され、データダウンロードも可能です。

国税庁法人番号公表サイトの特徴

① 法人情報を番号・名称・所在地で検索
② 法人情報のダウンロード機能
③ Web-API機能（システム間連携インタフェース）

＋

④ マルチデバイス対応
パソコンからの利用に加えて、タブレット、スマートフォンからも利用可能

検索機能
- あいまい検索
- 絞り込み検索
- 五十音順、都道府県別の並び替え

データダウンロード機能
- 月末時点のすべての最新情報
- 日次の更新情報
- データ形式はCSV、XML

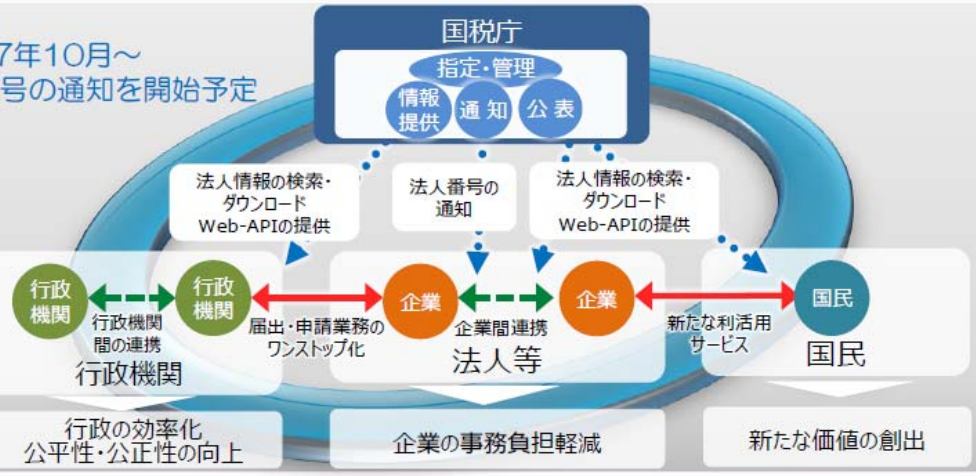
Web-API機能
企業等のシステムから法人情報を直接取得するためのインタフェースの提供

（※）公表機能の詳細については、国税庁HPのトップページの 社会保障・税番号制度 をクリック。
http://www.nta.go.jp/mynumberinfo/index.htm

26

法人番号で、わかる。つながる。ひろがる。

平成27年10月～
法人番号の通知を開始予定



わかる。
法人番号により企業等法人の名称・所在地がわかる。
- 法人番号をキーに法人の名称・所在地が容易に確認可能
- 鮮度の高い名称・所在地情報が入手可能となり、取引先情報の登録・更新作業が効率化

つながる。
法人番号を軸に企業等法人がつながる。
- 複数部署又はグループ各社において異なるコードで管理されている取引先情報に、法人番号を追加することにより、取引情報の集約や名寄せ作業が効率化
- 行政機関間において、法人番号付で個別の法人に関する情報の授受が可能となれば、法人の特定や名寄せ、紐付け作業が効率化

ひろがる。
法人番号を活用した新たなサービスがひろがる。
- 行政機関間での法人番号を活用した情報連携が図られ、行政手続における届出・申請等のワンストップ化が実現すれば、法人（企業）側の負担が軽減
- 民間において、法人番号を活用して企業情報を共有する基盤が整備されれば、企業間取引における添付書類の削減等の事務効率化が期待されるほか、国民に対しても有用な企業情報の提供が可能

27

マイナポータルについて

マイナンバー制度の導入に併せて新たに構築する個人ごとのポータルサイトを、マイナちゃんにちなみ「マイナポータル」とすることに決定しました。

マイポータルの機能や、これまでマイガバメントで提供するとしていた官民横断的なワンストップサービスなどを一体的に提供する個人ごとのポータルサイトとして、より親しみを感じられるよう「マイナちゃん」の名前にちなみ「マイナポータル」としました。

マイナポータル

平成29年１月以降
順次サービス開始予定

- ①自己情報表示
  自治体などが保有する自らの特定個人情報の閲覧
- ②情報提供等記録表示
  国や自治体などの間の特定個人情報のやり取りの記録の閲覧
- ③お知らせ情報表示
  自治体などからの予防接種や年金、介護などの各種のお知らせの受け取り
- ④ワンストップサービス
  引っ越しなどライフイベントに関する手続きの官民横断的なワンストップ化
- ⑤電子私書箱
  行政機関や民間事業者などから支払証明書などの各種電子データを受領し活用する仕組み
- ⑥電子決済サービス
  納税や社会保障などの決済をキャッシュレスで電子的に行うサービス

ねんきんネット　e－Tax

連携先は今後eLTAX等に順次拡大する予定

他のサイトとのＩＤ連携、データ連携

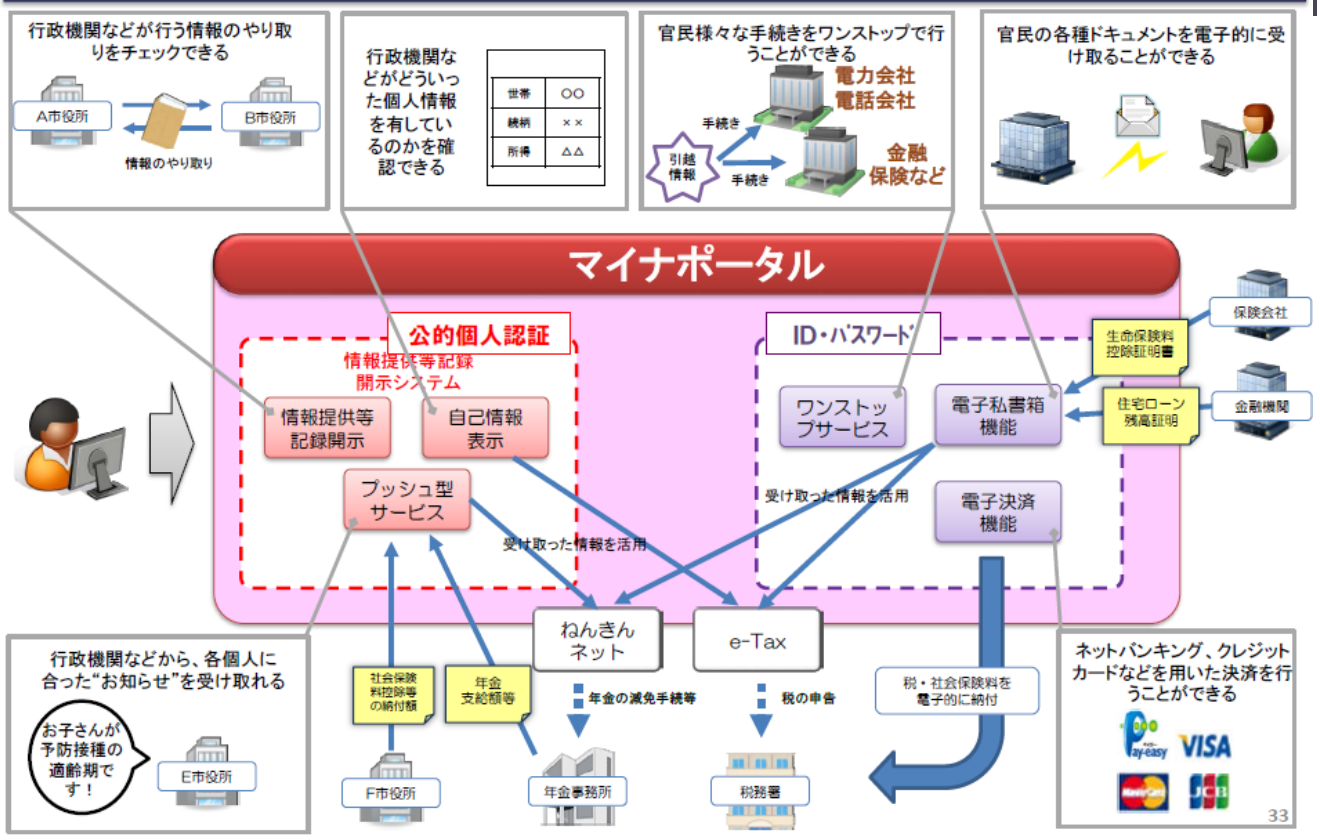
マイガバメント(仮称) ※世界最先端IT国家創造宣言
マイポータルを活用し利便性の高いオンラインサービスをPCや携帯端末など多様なチャンネルで利用可能に

マイポータル(仮称) ※マイナンバー法附則に基づく
マイナンバーに係る情報表示や行政サービスを提供

- ①自己情報表示
  行政機関などが持っている自分の特定個人情報について確認する機能
- ②情報提供等記録表示
  自分の特定個人情報をいつ、誰が、なぜ情報提供したのかを確認する機能
- ③プッシュ型サービス
  一人ひとりに合った行政機関などからのお知らせを表示する機能
- ④ワンストップサービス
  行政機関などへの手続を一度で済ませる機能

32

マイナポータル



33

公開情報への法人番号の併記について

公開情報への法人番号の併記について（案）概要

資料３－１

背 景

● **世界最先端IT国家創造宣言**（平成26年6月24日閣議決定）

「法人番号については行政機関が法人に係る情報を公開する際の併記や、既存の法人に係る各種の番号との連携により、法人に係る情報についての検索・利用を容易にし、その利用価値を高める」

● **マイナンバー等分科会「中間とりまとめ」**（平成26年5月20日）

「行政がインターネット等で公開する法人情報について、法人番号による検索・収集・利用を容易にし、公開情報の利用価値を高める観点から、先ず率先して平成28年1月以降国や地方公共団体が公開する法人情報には法人番号を付すこととする。そのために、関連する手続きにおいて法人番号を求め、行政機関内においても法人情報の適正な管理を図るものとする。」

【具体的な取組内容】

対 象 者	行政機関・独立行政法人等・地方公共団体は公開する法人情報に法人番号の併記を行う。
対 象	行政機関・独立行政法人等・地方公共団体がWebページ等で公開する法人情報 （具体例：調達、免許・許認可、処分・勧告、補助金交付、リコール届出、求人等）
併記時期	マイナンバー制度の利用開始となる平成28年1月1日以降に公開する法人情報について法人番号の併記を行う。

法人番号併記へのニーズが高いと思われるケース

- 「世界最先端 IT 国家創造宣言工程表」に記載のある「調達、免許・許認可、処分・勧告、補助金交付、リコール届出、求人等の情報」の項目
- 情報の分野に限らず大量のデータの管理や検索を目的としデータベース化されているもの
- 決算等、調査、研究等、事故などの安全安心に係る情報、審判等、合併などの企業結合に係る重宝、所管法人の一覧