政府の情報セキュリティ対策

2016年12月12日

経済産業省CIO補佐官

経済産業省最高情報セキュリティアドバイザー

満塩　尚史

経歴①

- 経歴
  - 1996年　筑波大学大学院博士課程物理学研究課修了　理学博士、国内暗号ソフトウェアベンダー入社
  - 1998年　KPMGコンサルティング株式会社　入社
  - 2003年　環境省CIO補佐官
  - 2008年　株式会社イマーディオ設立　代表取締役
  - 2010年　経済産業省CIO補佐官・最高情報セキュリティアドバイザー（現職）
  - 2013年　内閣官房　IT総合戦略室　政府CIO補佐官（現職）
  - 2015年　厚生労働省CIO補佐官（6月－9月）
- 最近の業務
  - 法人ポータル、ID連携トラストフレームワーク、行政手続におけるAIの利活用
- 資格等
  - 理学博士（筑波大学大学院博士課程物理学研究課修了）
  - 公認情報システム監査人（CISA）

経歴②

- 業務経験
  - ITガバナンス関係

    政府機関の刷新可能性調査、運用経費の見直しプロジェクト、最適化計画レビュー、予算要求レビュー、ITIL

  - 情報システム監査

    情報セキュリティ関係情報セキュリティポリシー策定、ISMS認証取得、Pマーク取得支援、情報セキュリティ監査、政府機関情報セキュリティポリシー策定、情報セキュリティマネジメントシステムの導入支援

  - 電子署名関係

    認証局監査、Webtrust関連業務、認定認証業務取得支援

- 書籍等
  - 『未来を拓くマイナンバー―制度を使いこなす事業アイディア』中央経済社,
  - 『COBIT実践ガイドブック　日本ITガバナンス協会／監修』日経BP社
  - 『知っておきたい電子署名・認証のしくみ』 日科技連出版社
  - 『ネットビジネスのセキュリティー　　セキュリティポリシーの上手な作り方』 日科技連出版社

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）

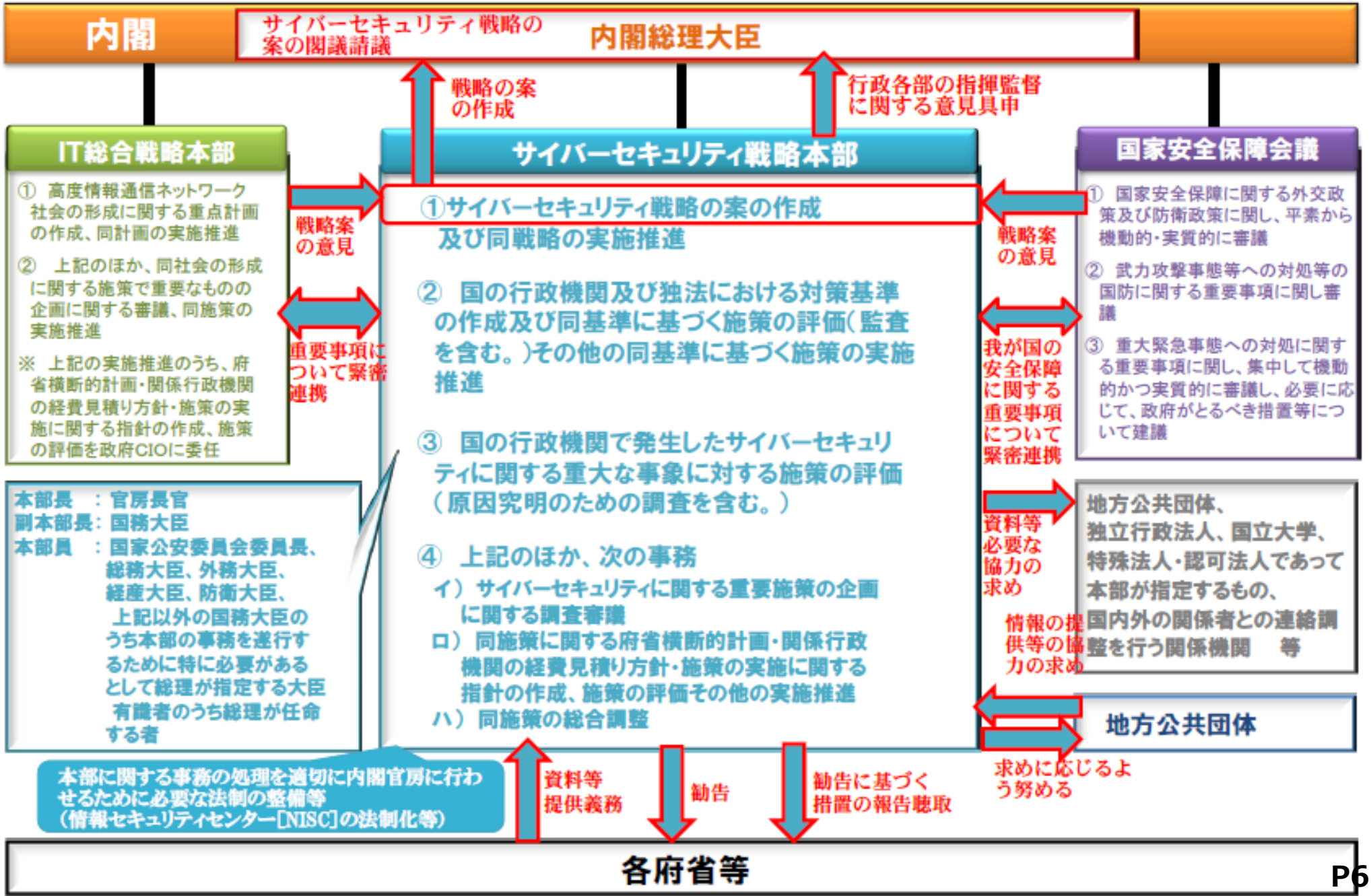
⇒ IT戦略本部の事務からサイバーセキュリティに関する重要施策の実施推進を除く旨規定

「サイバーセキュリティ」の定義

● 第2条

この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式（以下この条において「電磁的方式」という。）により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置（情報通信ネットワーク又は電磁的方式で作られた記録に係る記録媒体（以下「電磁的記録媒体」という。）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。）が講じられ、その状態が適切に維持管理されていることをいう。

サイバーセキュリティ戦略本部の機能・権限（イメージ）



サイバーセキュリティ戦略

資料２－１

新たなサイバーセキュリティ戦略
～政府機関等のサイバーセキュリティ対策の抜本的強化～

平成27年8月

内閣官房内閣サイバーセキュリティセンター

政府機関等のサイバーセキュリティ対策の抜本的強化（1/3）

日本年金機構の情報流出事案等を踏まえ、政府機関等のサイバーセキュリティ対策について、所要の法改正を含め、抜本的な強化を図る。

（注）「日本再興戦略」改訂2015（平成27年6月30日閣議決定）に盛り込まれた施策を含む追加的施策を新たなサイバーセキュリティ戦略に盛り込み、積極的かつ総合的に推進する。

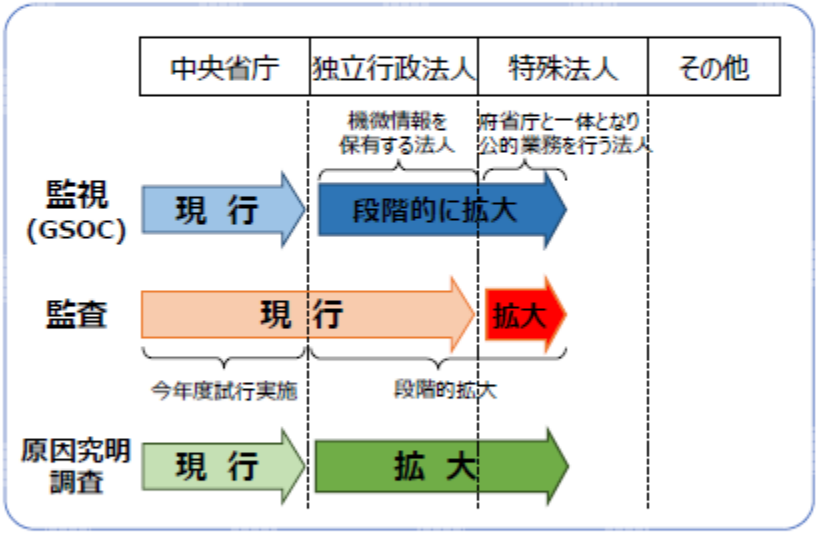
1．NISCの機能強化

■ GSOCの大幅な機能強化

- 政府機関情報セキュリティ横断監視・即応調整チーム（GSOC）システムの検知・解析機能及び運用体制の強化

■ 業務対象の拡大等

- 監視・監査・原因究明調査業務の対象について、政府機関（中央省庁）に加え、独立行政法人、政府機関と一体となって公的業務を行う特殊法人等に段階的に拡大（所要の法改正について速やかに検討）



■ 連携推進体制の強化

- 独立行政法人情報処理推進機構（IPA）及び国立研究開発法人情報通信研究機構（NICT）をはじめ、大規模なサイバー攻撃への対処等に対する知見を有する者との積極的な連携（所要の法改正について速やかに検討）

■ NISCの要員強化

- 高度セキュリティ人材の民間登用等による対処能力の一層の強化

政府機関等のサイバーセキュリティ対策の抜本的強化（2/3）

2．政府全体の取組強化

■ 政府機関における体制強化

- 政府機関等におけるインシデント対応チーム（CSIRT）体制の強化
- 初動対処に向けた組織的対応体制（幹部を含む。）の構築や政府全体の実践的訓練の実施等による危機管理体制の強化

■ 攻撃リスク低減のための対策強化（対策強化のための方針を早急に策定）

- インターネット接続口の更なる集約化
- 標的型攻撃に対する多重防御の取組の加速化
- 大量の個人情報等の重要情報を取り扱う情報システムのインターネットからの分離
- 政府機関における全面的なクラウドサービスへの移行を見据えた対策の強化

■ 人材・予算の確保

- 行政機関におけるセキュリティ人材の育成促進
- 所要の予算について行政効率化等により節減した費用等をサイバーセキュリティ対策へ振り向け（「サイバーセキュリティ関係施策に関する平成28年度予算重点化方針」に基づき、IoTセキュリティの確保、政府機関の対策強化、人材育成等に重点）

政府機関等のサイバーセキュリティ対策の抜本的強化（3/3）

3． その他の重要課題への取組強化

■ 重要インフラに関する取組強化（本年中を目途に具体策を決定）

- 社会環境の変化や既存の知見の集積等を踏まえ、重要インフラの対象範囲を見直し（継続実施）
- 情報共有環境の構築と体制の整備、及び演習・訓練の実施による継続的改善

■ セキュリティ人材の育成のための演習環境の整備（本年度中に人材育成総合強化方針(仮称)を策定）

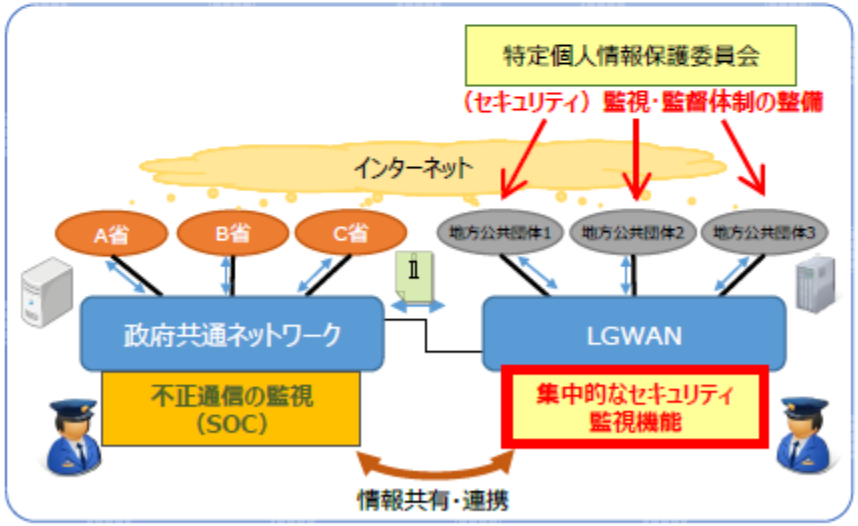
- クラウド環境の実践的な演習環境の整備等（国立研究開発法人情報通信研究機構（NICT）との積極的な連携）

■ 即応予備チームの体制整備

- 政府機関、独立行政法人、民間企業等から緊急時の対処チームへの参加等を可能とする体制の整備（法改正について速やかに検討）

■ マイナンバー制度の円滑な導入に向けた対策の強化

- 特定個人情報保護委員会において、関係機関と連携して監視・監督体制を整備（本年度中を目途）
- 総合行政ネットワーク（LGWAN）について集中監視機能を設ける等、GSOCとの連携による国・地方を俯瞰した監視・検知体制を整備
- 官民連携を実現する認証連携のための枠組みの取組方針を策定（本年中を目途）



■ 事案対処に関する取組強化

- サイバー攻撃を組織的に行う集団等の動向分析と捜査機関等との情報共有
- 対処機関における能力の質的・量的向上

新たな「サイバーセキュリティ戦略」について（全体構成）

資料2－2

1 サイバー空間に係る認識

- サイバー空間は、「**無限の価値を産むフロンティア**」である人工空間であり、人々の経済社会の活動基盤
- あらゆるモノがネットワークに連接され、実空間とサイバー空間との融合が高度に深化した「**連接融合情報社会（連融情報社会）**」が到来
  同時に、サイバー攻撃の被害規模や社会的影響が年々拡大、脅威の更なる深刻化が予想

2 目的

- 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって「経済社会の活力の向上及び持続的発展」、「国民が安全で安心して暮らせる社会の実現」、「国際社会の平和・安定及び我が国の安全保障」に寄与する。

3 基本原則

① 情報の自由な流通の確保　② 法の支配　③ 開放性　④ 自律性　⑤ 多様な主体の連携

4 目的達成のための施策

①後手から**先手**へ　／　②受動から**主導**へ　／　③サイバー空間から**融合**空間へ

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

■ **安全なIoTシステムの創出**
安全なIoT活用による新産業創出

■ **セキュリティマインドを持った企業経営の推進**
経営層の意識改革、組織内体制の整備

■ **セキュリティに係るビジネス環境の整備**
ファンドによるセキュリティ産業の振興

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■ **国民・社会を守るための取組**
事業者の取組促進、普及啓発、サイバー犯罪対策

■ **重要インフラを守るための取組**
防護対象の継続的見直し、情報共有の活性化

■ **政府機関を守るための取組**
攻撃を前提とした防御力強化、監査を通じた徹底

国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

■ **我が国の安全の確保**
警察・自衛隊等のサイバー対処能力強化

■ **国際社会の平和・安定**
国際的な「法の支配」確立、信頼醸成推進

■ **世界各国との協力・連携**
米国・ASEANを始めとする諸国との協力・連携

横断的施策

■ **研究開発の推進**
攻撃検知・防御能力向上(分析手法・法制度を含む)のための研究開発

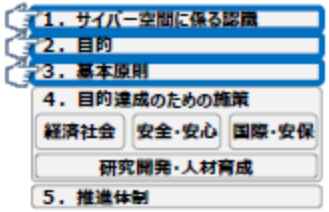
■ **人材の育成・確保**
ハイブリッド型人材の育成、実践的演習、突出人材の発掘・確保、キャリアパス構築

5 推進体制

- 官民及び関係省庁間の連携強化、オリンピック・パラリンピック東京大会等に向けた対応

新たな「サイバーセキュリティ戦略」について（総論）

1.サイバー空間に係る認識　　2.目的　　3.基本原則



➢ 本戦略は、2020年オリンピック・パラリンピック東京大会の開催、そしてその先の2020年代初頭までの将来を見据えつつ、今後3年程度の基本的な施策の方向性を示すもの。

1　サイバー空間に係る認識

➢ サイバー空間は「国境を意識することなく自由にアイディアを議論でき、そこで生まれた知的創造物やイノベーションにより、無限の価値を産むフロンティア」である人工の空間で、経済社会の活動基盤である。

➢ 実空間のモノやヒトが、サイバー空間により物理的制約を超えて連接することで、実空間とサイバー空間の融合が高度に深化した「連接融合情報社会（連融情報社会）」が到来しつつある。

➢ 一方、国民生活・経済社会活動への重大な被害や我が国の安全保障に対するサイバー脅威も高まっている。今後、こうした脅威が更に深刻化することが予想される。

2　目的

➢ 「自由、公正かつ安全なサイバー空間」を創出・発展させ、もって**「経済社会の活力の向上及び持続的発展」**、**「国民が安全で安心して暮らせる社会の実現」**、**「国際社会の平和・安定及び我が国の安全保障」**に寄与する。

3　基本原則

本戦略の目的達成のための施策の立案及び実施に当たり、以下に示す基本原則に従う。

① 情報の自由な流通の確保：サイバー空間発展の基盤として、情報の自由な流通が保証された空間を維持

② 法の支配：実空間と同様にサイバー空間に対しても「ルールや規範」の適用を徹底

③ 開放性：常に参加を求める者に開かれ、新たな価値を生み出す空間として保持

④ 自律性：各者の主体的な行動により、悪意ある行動を抑止する自律的メカニズムを推進

⑤ 多様な主体の連携：様々な主体の適切な連携関係構築とダイナミックな対処策実現

我が国は、上記の５つの基本原則に従うとともに、国民の安全・権利の保障のため、政治・経済・技術・法律・外交その他の採り得る全ての有効な手段を選択肢として保持する。

新たな「サイバーセキュリティ戦略」について（各論②）

4.目的達成のための施策

国民が安全で安心して暮らせる社会の実現　～2020年・その後に向けた基盤形成～

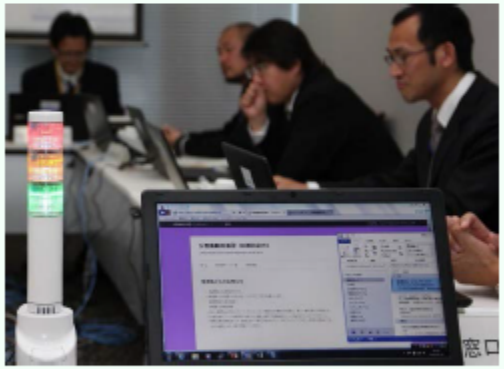
■国民・社会を守るための取組

- ソフトウェア等の脆弱性関連情報の収集やインターネット上の各種のサイバー攻撃等観測システムの連携・強化の推進
- 攻撃を受けた端末の利用者に対する注意喚起等の推進
- 整備が進む公衆無線LAN等のセキュリティ確保のための対策検討
- 地域における普及啓発活動の促進、中小企業や地方公共団体への啓発・支援
- サイバー犯罪への対処能力・捜査能力の向上に向けた取組の強化
  （通信履歴の保存の在り方についての関係事業者における適切な取組の推進を含む）

▲双方向型の普及啓発セミナー（サイバーセキュリティカフェ）

■重要インフラを守るための取組

- 重要インフラ分野の範囲及び各分野内での「重要インフラ事業者」の範囲の継続的な見直し
- より効果的かつ迅速な官民の情報共有、政府機関内での必要な連携、訓練・演習の実施の推進
- マイナンバー制度の円滑な運用確保のため地方公共団体に必要な政策を実施し、国・地方の全体を俯瞰した監視・検知体制や、専門的・技術的知見を有する監視・監督体制を整備
- スマートメーター等の制御系について、国際標準に即した第三者認証制度の活用等を推進



▲サイバー攻撃等に対する対応能力向上のための演習
（重要インフラ分野横断的演習）

■政府機関を守るための取組

- ペネトレーションテスト等を通じたセキュリティ対策を徹底、サプライチェーン・リスクへの対応、政府機関情報セキュリティ横断監視・即応調整チーム(GSOC)による検知・解析機能強化、 標的型攻撃に対する多重防御の取組加速等による防御力の強化
- マネジメント監査等を通じた組織の体制・制度の検証・改善、リスク評価に基づく組織的な対策・管理等による組織的対応能力の強化
- 新たなIT製品・サービスの特性を踏まえた政府統一的なセキュリティ対策の策定・推進
- 独立行政法人や、府省庁と一体となり公的業務を行う特殊法人等への監視・監査・原因究明調査の実施等による総合的な対策強化

新たな「サイバーセキュリティ戦略」について（各論④・推進体制）

4.目的達成のための施策　　5.推進体制

横断的施策

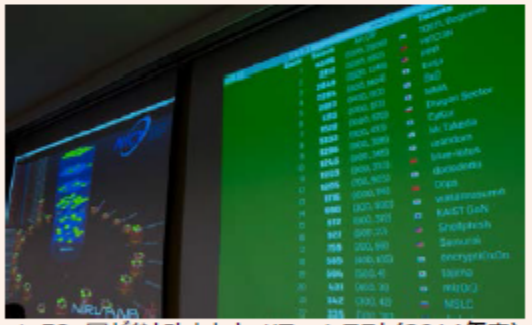
■研究開発の推進

- 関係者間の情報・データの共有等によるサイバー攻撃の検知・防御能力の一層の向上
- 融合領域の研究促進、及び安全保障のためのコア技術（暗号技術等）の保持
- 各国が強みを有する技術を有機的に組み合わせた国際連携による研究開発の推進

▲ 合宿形式で知識・技能を学ぶセキュリティキャンプ

■人材の育成・確保

- 他分野の知識も併せ持つハイブリッド型人材の育成促進
- 高等教育等における産学官連携の推進・実践的演習の充実
- 初等中等教育段階からの教育の充実
  （論理的思考力やモノの基礎的動作原理の理解促進、教員の指導力向上に向けた研修等の改善・充実）
- サイバー演習環境のクラウド環境における整備、産学官共同による教材開発の支援
- 国際的競技イベント等を通じたグローバル水準の高度人材の発掘・確保
- 実践的能力を評価する資格制度の創設、標準的なスキルの基準の整備等の推進



▲ 58ヶ国が参加したセキュリティコンテスト(2014年度)

5　推進体制

- NISC対処能力の一層の強化や産学官及び関係省庁間の連携強化によるサイバー攻撃の検知・分析・判断・対処の機能強化
- 国家の関与が疑われる高度な攻撃に対し、戦略本部とNSC（安全保障）・重大テロ対策本部（危機管理）と緊密に連携
- オリンピック・パラリンピック東京大会等に向け、リスクの明確化、組織・施設・協力関係の構築・維持、十分な訓練を実施

- 戦略本部は、各年度の年次計画及び年次報告を作成するとともに、経費見積り方針を策定する。

サイバーセキュリティ2015

「サイバーセキュリティ2015(案)」の概要について

資料１－１

新たなサイバーセキュリティ戦略に基づく最初の年次計画として、2015年度に実施する具体的な取組を戦略の体系に沿って示したもの（以下は主な施策例）。

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

■安全なIoTシステムの創出

- IoTに係る大規模な事業に対し、セキュリティ・バイ・デザインに必要な働きかけを実施【内閣官房】
- M2M機器・IoTのセキュリティに係る横断的なガイドラインの策定【総務省及び経済産業省】
- エネルギー分野のガイドラインとして、スマートメーターのセキュリティ評価技術・手順を実証【経済産業省】

■セキュリティマインドを持った企業経営の推進

- サイバー攻撃によるリスクを投資家に開示することの可能性を検討【内閣官房及び金融庁】
- 経営ガイドラインの策定【経済産業省】
- 「橋渡し人材層」としての能力向上を図るセミナー等を実施【内閣官房及び経済産業省】
- ISACを活用した情報共有体制の拡充【総務省】

■セキュリティに係るビジネス環境の整備

- 政府系ファンド等の活用検討【経済産業省】
- 著作権法におけるリバースエンジニアリングに関する適法性を明確化【文部科学省】
- 制御システムセキュリティ認証の拡大【経済産業省】

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■国民・社会を守るための取組

- マルウェアに感染したユーザーを検知し、マルウェアの除去等を促す取組を実施【総務省】
- 安全な無線LAN環境の整備に向けて、必要となる対策の検討、周知啓発を実施【総務省】
- 通信履歴等の保存の在り方について、ガイドラインの解説の改正を踏まえ対応【警察庁及び総務省】

■重要インフラを守るための取組

- 東京オリンピック・パラリンピック競技大会に重大な影響を与えるサービス・事業者・分野の候補を選定【内閣官房】
- マイナンバーの監視・監督体制や、LGWANにおける集中的なセキュリティ監視機能の整備【特定個人情報保護委員会、内閣官房及び総務省 他】

■政府機関を守るための取組

- 各府省庁の情報システムに対してペネトレーションテストを実施【内閣官房】
- 国の行政機関における統一基準群等に基づく施策の取組状況に関する監査制度を設計するとともに、試行的な監査を実施【内閣官房】

国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

■我が国の安全の確保

- 情報収集・分析機能の強化に加え、サイバー攻撃対策に係る訓練を実施【警察庁】
- カウンターインテリジェンスに係る取組の推進【内閣官房】
- サイバー攻撃時においても持続的な部隊運用を確保するための取組を継続【防衛省】
- 部外インフラ等、関係主体との連携深化【防衛省】

■国際社会の平和・安定

- 二国間協議や多国間協議に参画し、国際法の適用や国際的なルール・規範作り等に積極的に関与し、我が国の意向を反映【内閣官房及び外務省】
- 国際テロ組織の活動等に関する情報の収集・分析の強化【内閣官房、警察庁及び法務省】
- 各国における能力構築を支援【内閣官房 他】

■世界各国との協力連携

- ASEAN諸国との連携を強化【内閣官房 他】
- インターネットエコノミーに関する日米政策協力対話にて一致した、米国との情報共有を強化【総務省】
- 包括的な日米サイバー防衛の連携【防衛省】

横断的施策

■研究開発の推進

- 世界最先端のサイバー攻撃観測・分析技術、暗号基盤技術等に関する研究開発を実施【総務省】
- 法律や国際関係、安全保障、経営学等の社会科学的視点も含め様々な領域の研究との連携、融合領域の研究を促進【内閣官房】
- 戦略的イノベーション創造プログラム（SIP）の枠組み等により研究開発を推進【内閣府】

■人材の育成・確保

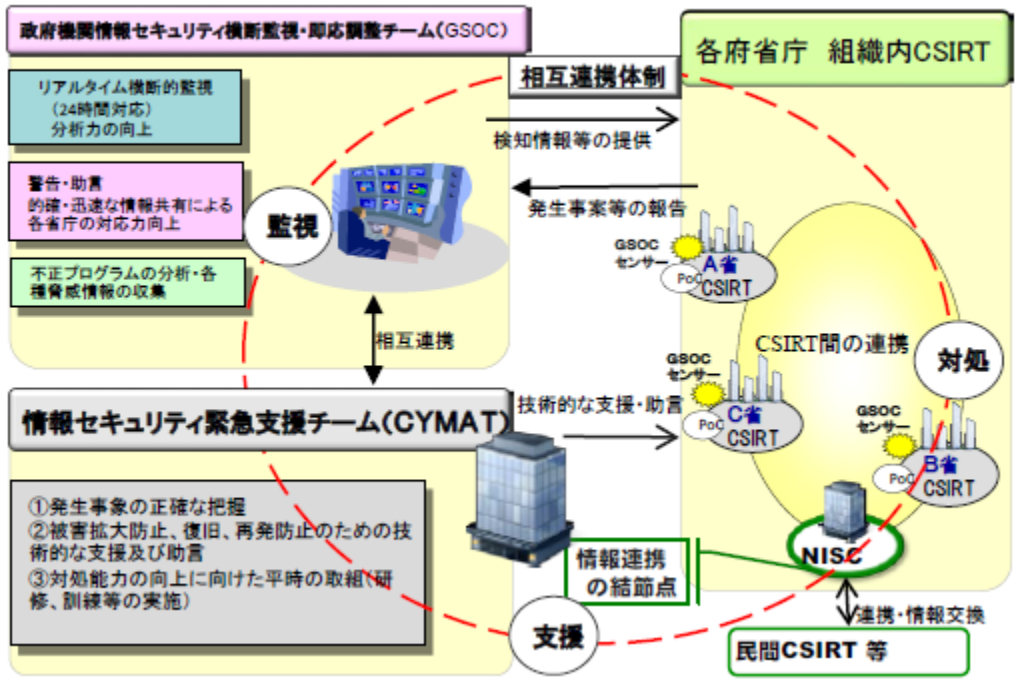
- 高度なITの知識と経営などその他の領域における専門知識を併せもつ人材の育成【文部科学省及び経済産業省】
- 初等中等教育に携わる教員等を対象とした研修、情報交換【文部科学省】
- 情報処理技術者試験において実践的な能力を適時適切に評価するための更新制度の導入の検討【経済産業省】
- サイバー防御演習を通じた実践的セキュリティ人材の育成【総務省】

推進体制

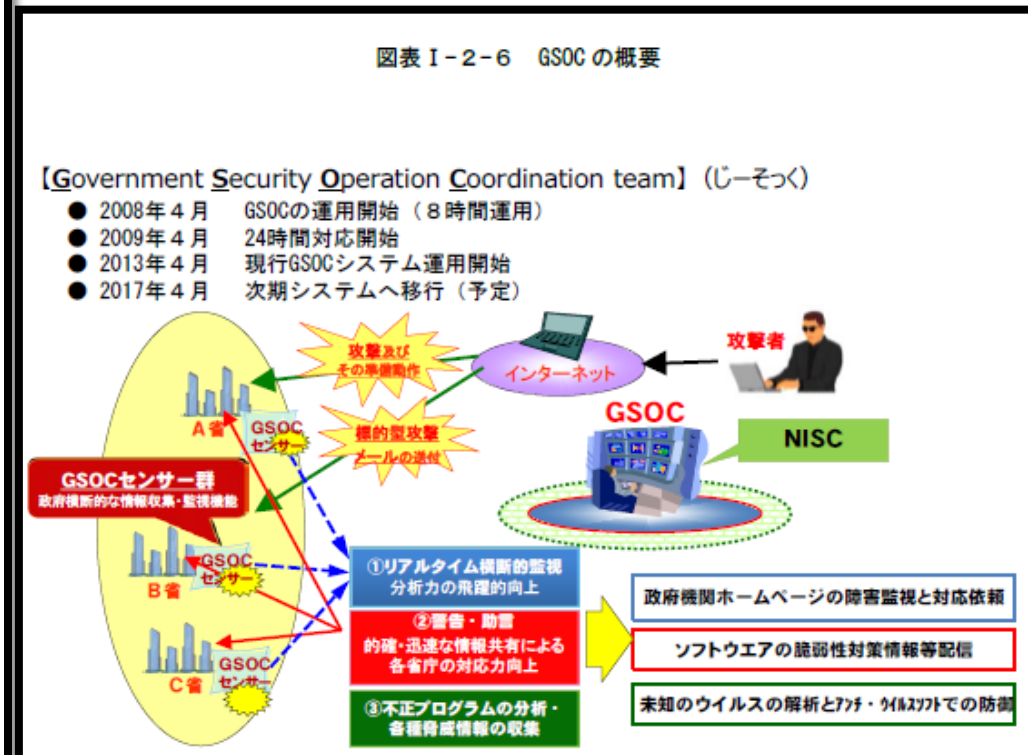
- 伊勢志摩サミットにおけるサイバーセキュリティの確保や東京オリンピック・パラリンピック競技大会に向けた対策の検討【内閣官房】

サイバーセキュリティ政策に係る年次報告（2015年度）

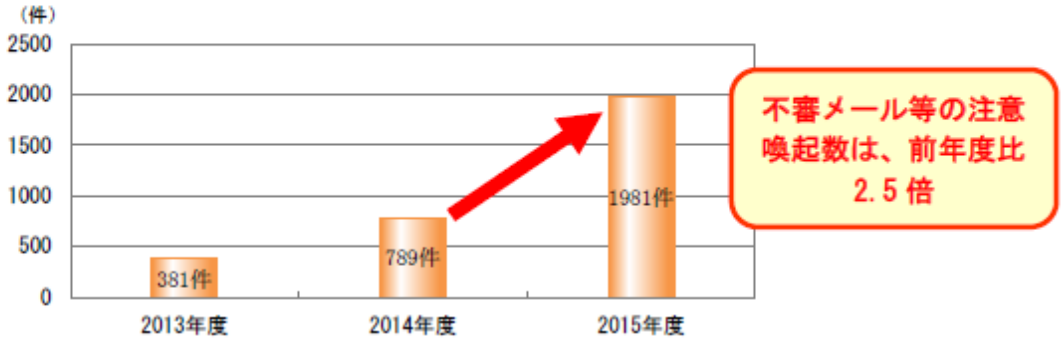
図表Ⅰ-2-1　政府機関における情報集約・支援体制の枠組み



図表Ⅰ-2-6　GSOC の概要



図表Ⅰ-2-4　不審メール等に関する注意喚起の件数の推移



経済産業省

2015年度の総合評価・2016年度の全体方針

最高情報セキュリティ責任者
大臣官房長　嶋田　隆

2015年度においても、政府機関等を狙った標的型攻撃やDDoS攻撃などのサイバー攻撃は活発化し続け、こうした攻撃から重要な情報や業務サービス等を保護するための総合的な情報セキュリティ対策の更なる強化が迫られた。

こうした中、2015年度に当省で実施した主な取り組みは以下のとおりである。

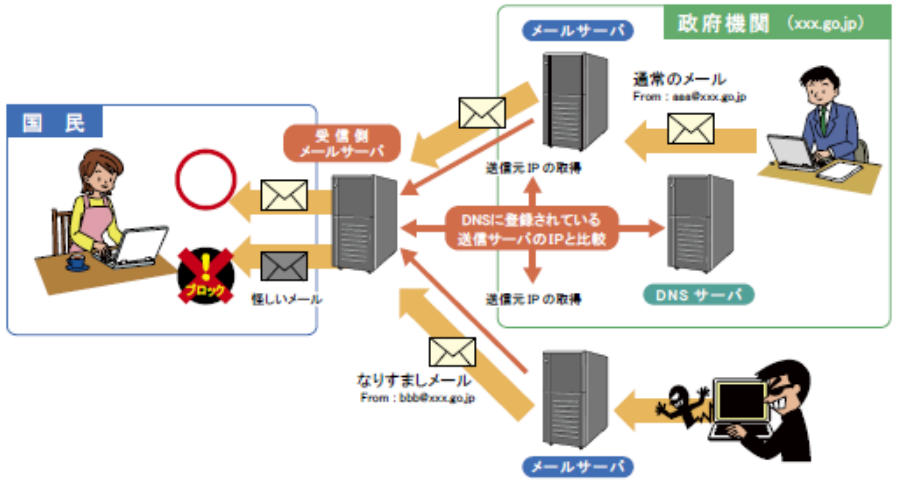
(1) 2014年度に改正した当省情報セキュリティポリシーに基づく、各課室毎に策定している情報の管理と取扱いのルールの再整備と点検
(2) 独自に規定されていた特許庁の情報セキュリティポリシーを廃止・統合し、省全体において一元的に情報セキュリティ対策を推進
(3) 高度化する標的型メール攻撃への対処方法等に関する訓練や動画コンテンツ等を含む分かり易い教材を用いた職員教育の徹底
(4) 職員、組織、情報システムを対象とした監査・点検による情報セキュリティ対策実施状況の評価と改善
(5) 活発化・多様化するサイバー攻撃等への対処として、重要な情報システムにおけるセキュリティ強化策の技術的検討及び実施

今後、2020年の東京オリンピック・パラリンピックに向け、政府機関を含め我が国全体での情報セキュリティ対策を今まで以上に強化していくことが求められている。

このため、当省では、2016年度において、以下の方針の下、取組を実施する。

(1) 標的型攻撃に対するソフト・ハード両面での対策の更なる強化
(2) 基幹となる情報システムにおけるネットワークセキュリティの更なる強化
(3) 省全体としてのインシデント・レスポンス体制・機能の更なる強化
(4) サイバーセキュリティ人材育成総合強化方針に基づく環境整備と人材の育成
(5) 政府機関の情報セキュリティ対策のための統一基準群の改定を踏まえた新たな情報セキュリティポリシー等の整備

図表１　SPFを活用したなりすまし対策の概要



別添３－10　NISC 発出注意喚起文書及びサイバーセキュリティ対策推進会議決定等

1　「サービス不能攻撃への対処について（注意喚起）」（2015 年 11 月 25 日発出）

事　務　連　絡
平成27年11月25日

各府省庁情報セキュリティ担当課室長 殿

内閣官房 内閣サイバーセキュリティセンター
内閣参事官（政府機関総合対策担当）

サービス不能攻撃への対処について（注意喚起）

昨今、公的機関や重要インフラ関係事業者等を標的としたサービス不能攻撃（DoS 攻撃及び DDoS 攻撃）の発生が多数報道されています。

「政府機関の情報セキュリティ対策のための統一基準」6.2.3 においては、システムの可用

サイバーセキュリティ2016

サイバーセキュリティ2016(案)の概要について

資料２－１

サイバーセキュリティ戦略に基づく２期目の年次計画として、2016年度に実施する具体的な取組を戦略の体系に沿って示したもの（以下は主な施策例）。

経済社会の活力の向上及び持続的発展

～ 費用から投資へ ～

■安全なIoTシステムの創出

- IoT（Internet of Things）に係る大規模な事業に対し、企画・設計段階からセキュリティを確保するために必要な働きかけを引き続き実施【内閣官房】
- IoT推進コンソーシアムを通じてIoTセキュリティガイドラインを策定し、対策を推進【総務省及び経済産業省】
- スマートメーターのセキュリティガイドラインを電気事業法の保安規定に位置付ける【経済産業省】

■セキュリティマインドを持った企業経営の推進

- サイバーセキュリティ経営ガイドラインの普及【経済産業省】
- 情報開示の推進とインセンティブの検討【内閣官房】
- 金融業界横断的な演習を実施【金融庁】
- ICT分野の情報共有体制の拡充【総務省】

■セキュリティに係るビジネス環境の整備

- 企業育成等、セキュリティの成長産業化【経済産業省】
- 著作権法におけるソフトウェア製品等の解析（リバースエンジニアリング）に関する適法性を明確化【文部科学省】
- IoTシステムのセキュリティ認証制度にかかる評価・検討【経済産業省】

国民が安全で安心して暮らせる社会の実現

～ 2020年・その後に向けた基盤形成 ～

■国民・社会を守るための取組

- IoTに関する攻撃を含む攻撃観測網の強化【総務省】
- 民間の取組主体と協力し、サイバーセキュリティに関する普及啓発を実施【内閣官房】
- 地方公共団体における緊急時対応の支援【総務省】
- 一般財団法人日本サイバー犯罪対策センターとの連携【警察庁】

■重要インフラを守るための取組

- 「重要インフラの情報セキュリティ対策に係る第３次行動計画の見直しに向けたロードマップ」に従った検討【内閣官房及び重要インフラ所管省庁等】
- 重要インフラ対策の中核を担う人材育成や技術開発を行う体制を強化【経済産業省】

■政府機関を守るための取組

- 統一基準群の改定及び各府省庁の情報セキュリティポリシーの整備促進【内閣官房】
- 試行的な監査の結果を踏まえた各府省庁に対する監査及び厚生労働省（日本年金機構を含む）に対する施策の評価の実施【内閣官房】

国際社会の平和・安定及び我が国の安全保障

～ サイバー空間における積極的平和主義 ～

■我が国の安全の確保

- 対処機関における情報収集・分析機能及び対処能力向上【警察庁、法務省、防衛省、関係各省】
- 社会インフラへのサイバー攻撃に関する任務保証の観点からの知見向上・関係主体との連携深化【防衛省】

■国際社会の平和・安定

- 国際的な情報発信の強化【内閣官房、外務省、関係各省】
- 国際法・規範の議論と法執行の国際連携の両面から、サイバー空間への法の支配の確立に積極的に関与【内閣官房、外務省、関係各省】
- ASEAN等における能力構築を政府一体的に支援【内閣官房、外務省、関係各省】

■世界各国との協力連携

- 伊勢志摩サミットにおいて立ち上げが決定された「サイバーに関するG7作業部会」を通じ、G7各国との政策協調及び実務的な協力を強化【内閣官房、外務省】
- 二国間協議や多国間協議を通じたASEANや米国等、世界各地域のパートナーとの連携の更なる強化【内閣官房、外務省、関係各省】

横断的施策

■研究開発の推進

- 政府、重要インフラ、企業・団体、個人等に対するサイバー攻撃の対策技術やサイバーセキュリティ関連情報の大規模集約技術の研究開発を行う【総務省】
- IoT・ビッグデータ・AI（人工知能）等の進化により実世界とサイバー空間が相互連関する社会を支える研究開発等の実施【経済産業省】
- 戦略的イノベーション創造プログラム（SIP）の枠組みにより、制御・通信機器の真正性／完全性確認技術を含む研究開発を行う【内閣府】

■人材の育成・確保

- 「新・情報セキュリティ人材育成プログラム」及び「サイバーセキュリティ人材育成総合強化方針」に基づく施策を促進【内閣官房】
- 「情報処理安全確保支援士」の創設に係る必要な制度整備を行うとともに、制度の普及を図る【経済産業省】
- サイバー攻撃への対処能力の向上に向けた実践的サイバー防御演習（CYDER）等を通じサイバーセキュリティ人材育成を行う【総務省】

推進体制

- 東京オリンピック・パラリンピック競技大会を見据えたリスク評価、対処体制の構築、総合的分析機能の強化、関係機関との協力体制の整備等【内閣官房】

政府機関統一基準

政府機関等の情報セキュリティ対策のための統一基準

NISC National center of Incident readiness and Strategy for Cybersecurity

「政府機関等の情報セキュリティ対策のための統一基準群」の改定(案)について

平成28年6月

内閣官房

内閣サイバーセキュリティセンター

統一基準群（平成26年度版）策定後の主な経緯

26年8月　民間企業の大量個人情報流出事案を踏まえた対策強化の指示

☛ 機微度の高い情報を始めとする情報管理の徹底を推進

27年1月　サイバーセキュリティ基本法の完全施行

☛ 独法の対策強化、戦略本部による監査の実施、NISCの機能強化等を推進

27年5月　日本年金機構における不正アクセスによる情報流出事案の発生

☛ 事案対処体制の強化、標的型攻撃を前提とした対策強化等を政府機関全体で推進

27年9月　新たなサイバーセキュリティ戦略の決定

☛ 新たに直面した脅威・課題への対応、IT製品・サービスの普及に伴う対策強化を推進

28年3月　サイバーセキュリティ人材育成総合強化方針の決定

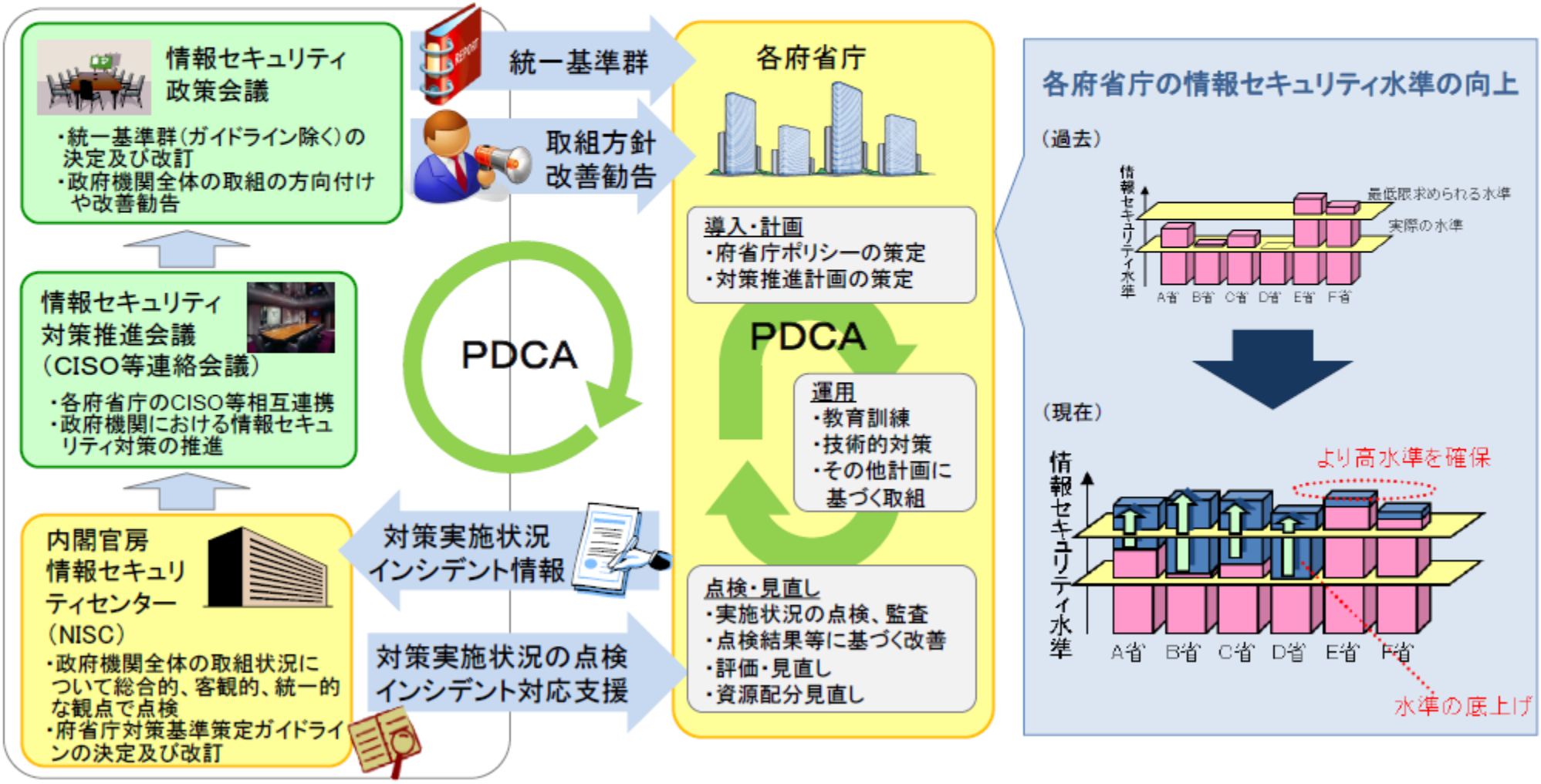
☛ 政府機関における専門人材の確保・育成や一般職員の素養向上への取組方針

28年4月　サイバーセキュリティ基本法の改正法案の成立

☛ 指定法人への適用範囲の拡大等（公布の日から6月以内に施行）

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

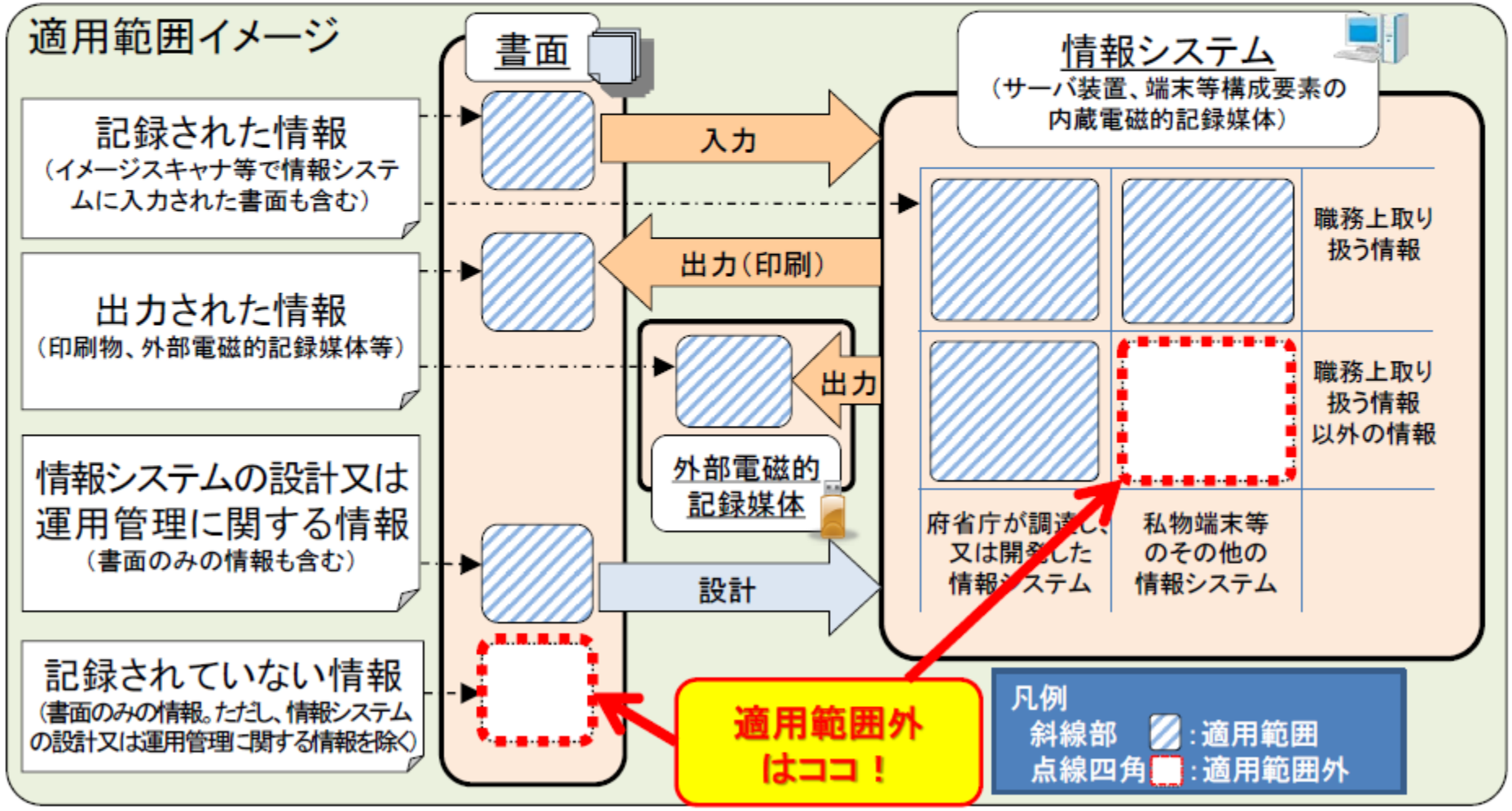
- 「政府機関の情報セキュリティ対策のための統一基準群」（以下、「統一基準群」という。）は、政府全体の情報セキュリティ水準を向上させるための統一的な枠組み。
- 各府省庁は、統一基準に準拠した情報セキュリティポリシー及び、対策推進計画を策定し、対策を実施する。



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



2.1.1 組織・体制の整備

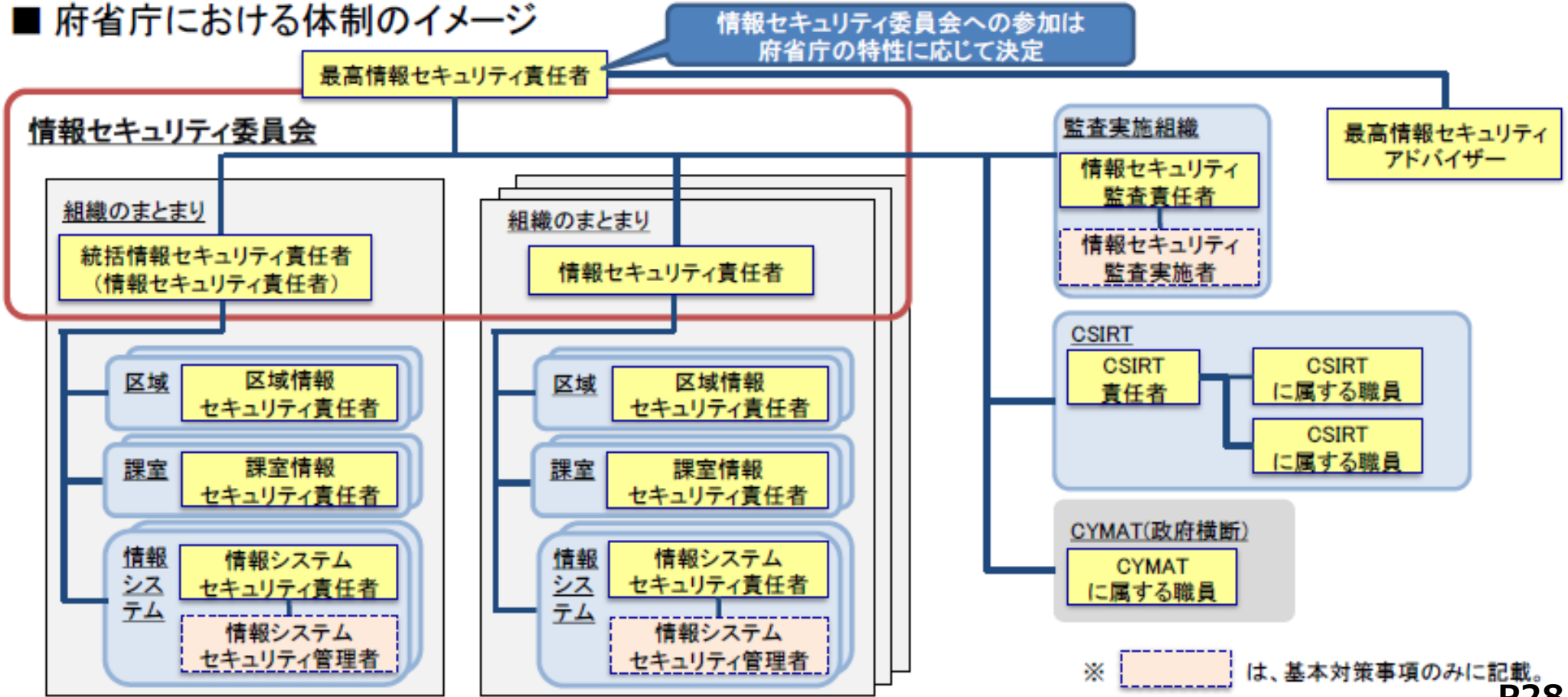
CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

■ 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



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

申請者

申請の準備

・申請者の情報
・規程の該当箇所
・申請期間
・申請理由
・申請する措置内容
（講ずる代替手段等）
・情報セキュリティ上の影響と対処方法
・例外措置終了の報告方法

申請

許可／不許可

許可権限者※
※CISOが定める

審査（可否の判断）

・申請理由が合理的
・許可の際の情報セキュリティ上の影響と、不許可の際の行政事務への影響を考慮し、期間等が合理的

審査の記録、保管

・申請内容、判断結果

報告

統括情報セキュリティ責任者

例外措置の適用状況の把握

・情報セキュリティ関係規程の追加、見直しの検討
・検討結果をCISOへ報告

例外措置はやむを得ない場合のみ。
原則、情報セキュリティ関係規程を遵守すること！

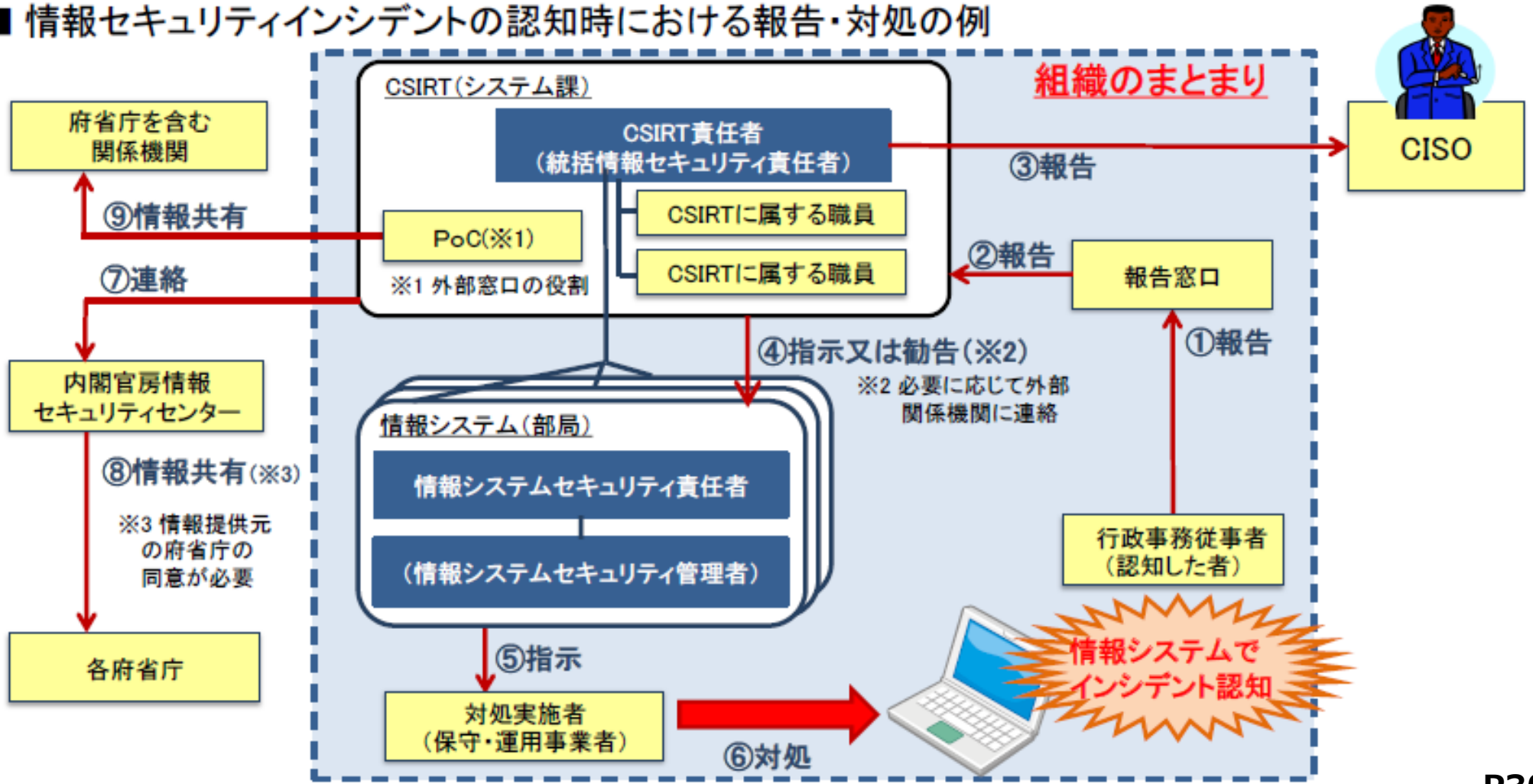
＜例外措置の例＞
認証が必要であるにもかかわらず、認証機能を備えていない情報システムがあるが、来年度に廃棄する予定であることから、本年度のみ（リスクを許容しながら）認証をしないで運用する。

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



2.3.2 情報セキュリティ監査

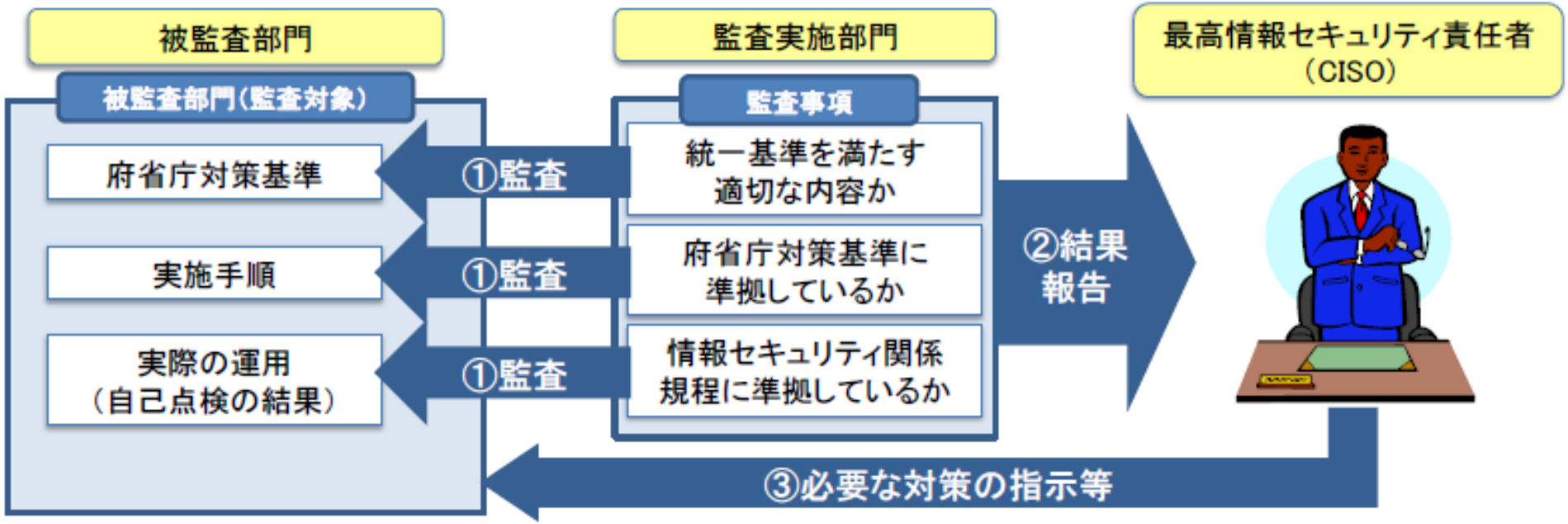
CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

■ 本項の概要

- 情報セキュリティ対策の実効性を担保するためには、情報セキュリティ対策を実施する者による自己点検だけでなく、独立性を有する者による情報セキュリティ対策の監査を実施することが必要。
- 監査の結果で明らかになった課題を踏まえ、最高情報セキュリティ責任者は、情報セキュリティ責任者に指示、必要な対策を講じさせることが重要。

＜主な遵守事項＞
2.3.2(1)(a) 情報セキュリティ監査責任者は、対策推進計画に基づき監査実施計画を定めること。
2.3.2(2)(a) 情報セキュリティ監査責任者は、監査実施計画に基づき、以下の事項*(下図に記載)*を含む監査の実施を監査実施者に指示し、結果を監査報告書として最高情報セキュリティ責任者に報告すること
2.3.2(3)(a) 最高情報セキュリティ責任者は、監査報告書の内容を踏まえ、指摘事項に対する対処計画の策定等を情報セキュリティ責任者に指示すること。

■ 情報セキュリティ監査のイメージ



機密性についての格付の定義

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、行政文書の管理に関するガイドライン（平成 23 年４月１日内閣総理大臣決定。以下「文書管理ガイドライン」という。）に定める秘密文書に相当する機密性を要する情報を含む情報
機密性２情報	行政事務で取り扱う情報のうち、行政機関の保有する情報の公開に関する法律（平成 11 年法律第 42 号。以下「情報公開法」という。）第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含む情報であって、「機密性３情報」以外の情報
機密性１情報	情報公開法第５条各号における不開示情報に該当すると判断される蓋然性の高い情報を含まない情報

完全性についての格付の定義

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 おそれがある情報
完全性１情報	完全性２情報以外の情

可用性についての格付の定義

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。）

3.1.1 情報の取扱い③

■ 取扱制限の表示の例

【機密性についての取扱制限の表示例】

取扱制限の種類	表示例
複製について	複製禁止、複製要許可
配布について	配布禁止、配布要許可
暗号化について	暗号化必須、保存時暗号化必須
印刷について	印刷禁止、印刷要許可
転送について	転送禁止、転送要許可
転記について	転記禁止、転記要許可
再利用について	再利用禁止、再利用要許可
送信について	送信禁止、送信要許可
参照者の制限について	○○限り
期限について	○月○日まで○○禁止

情報の格付のみでは安全管理措置が不十分になるおそれがある場合に、取扱制限の明示は有効な対策になります。

【完全性についての取扱制限の表示例】

取扱制限の種類	表示例
保存期間について	○○まで保存
保存場所について	○○において保存
書換えについて	書換禁止、書換要許可
削除について	削除禁止、削除要許可
保存期間満了後の措置について	保存期間満了後要廃棄

【可用性についての取扱制限の表示例】

取扱制限の種類	指定方法
復旧までに許容できる時間について	○○以内復旧
保存場所について	○○において保存

3.2.1 情報を取り扱う区域の管理①

CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

■ 本項の概要

- 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

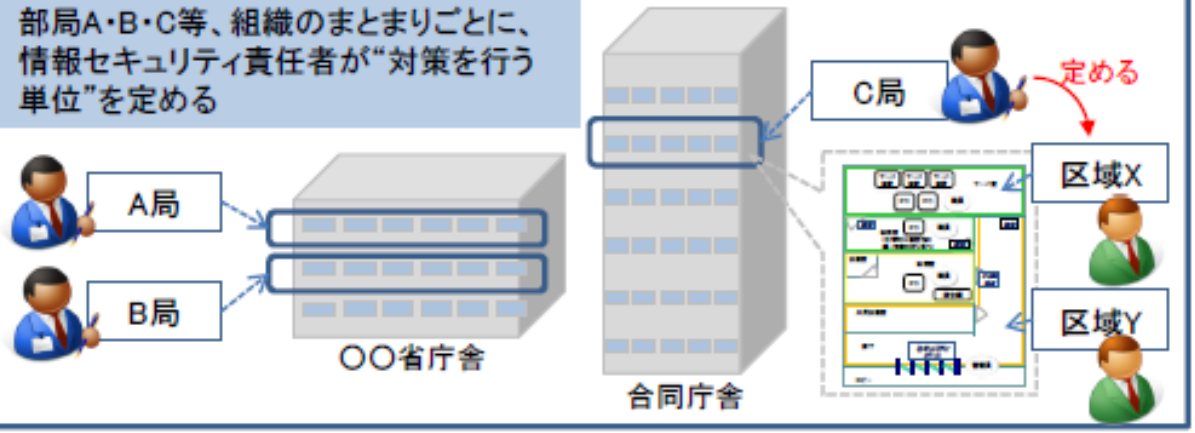
統括情報セキュリティ責任者
・クラスの区分の整備
・クラスごとの対策の基準の整備

クラス	クラスの区分の定義（例）
クラス3	立入りを厳格に制限する必要があるなど、クラス2より強固な情報セキュリティを確保するための厳重な対策を実施する必要がある区域
クラス2	行政事務従事者以外の者の立入りを制限する必要があるなど、情報セキュリティを確保するための対策を実施する必要がある区域
クラス1	クラス3、クラス2以外の要管理対象区域

情報セキュリティ責任者
・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

部局A・B・C等、組織のまとまりごとに、情報セキュリティ責任者が“対策を行う単位”を定める

区域情報セキュリティ責任者
・管理する区域へのクラスの割当て
・立入りを制限するための物理的対策・入退管理対策の決定と実施
・扉の開閉・施錠等に係る実施手順の整備



3.2.1 情報を取り扱う区域の管理②

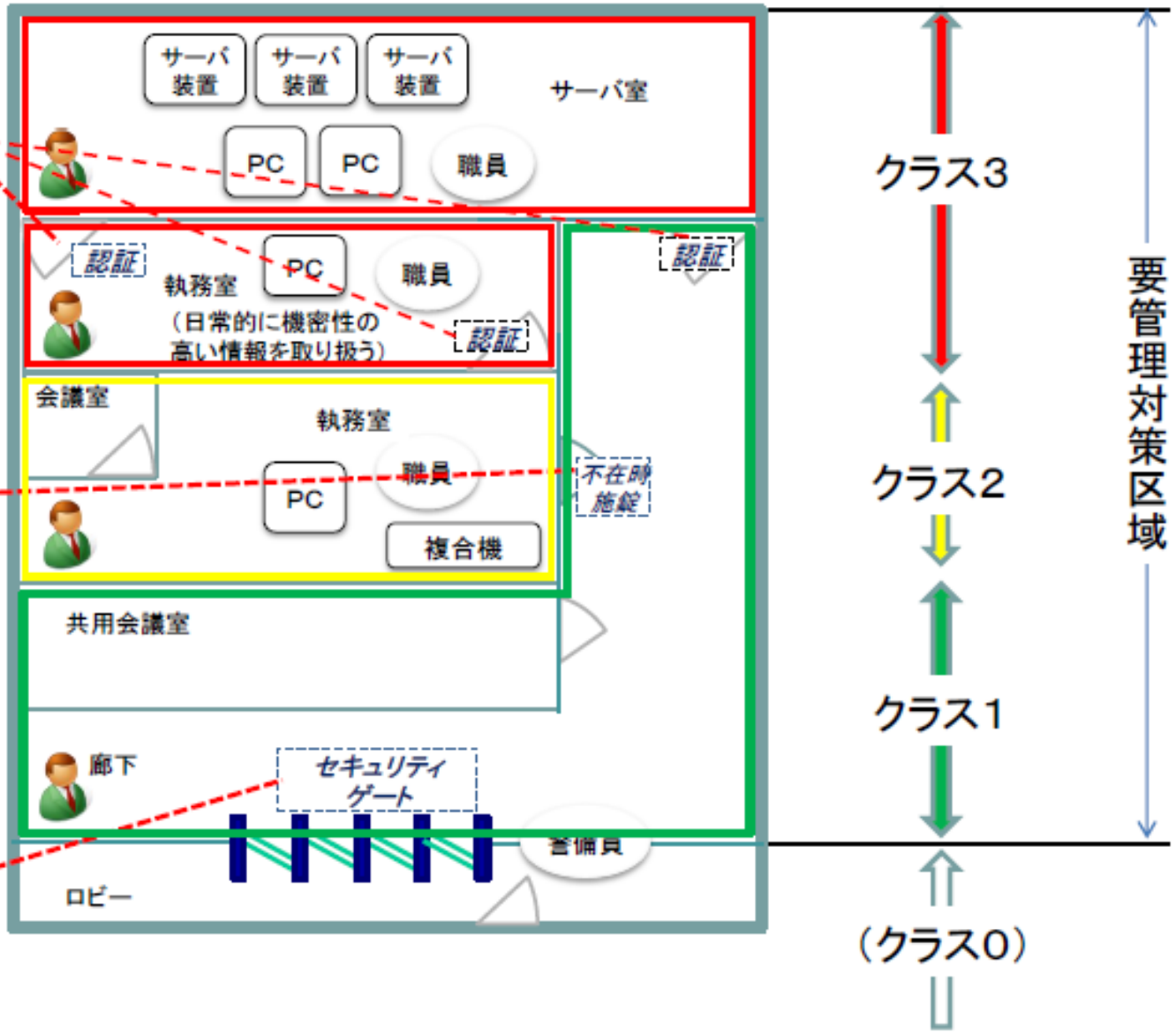
CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

■要管理対策区域へのクラスの割当ての例

・常に施錠、電子錠
・一部の限られた者のみ入室可
・訪問者に帯同、業者が作業を行う場合は立会又は監視

・全員不在時施錠
・行政事務従事者と許可された者のみ入室可
・訪問者の確認

・身分証明書、入館カード等の着用、明示（クラス2、3でも同様）
・訪問者の身元の確認



4.1.1 外部委託 ［参考］サプライチェーン・リスクへの対応

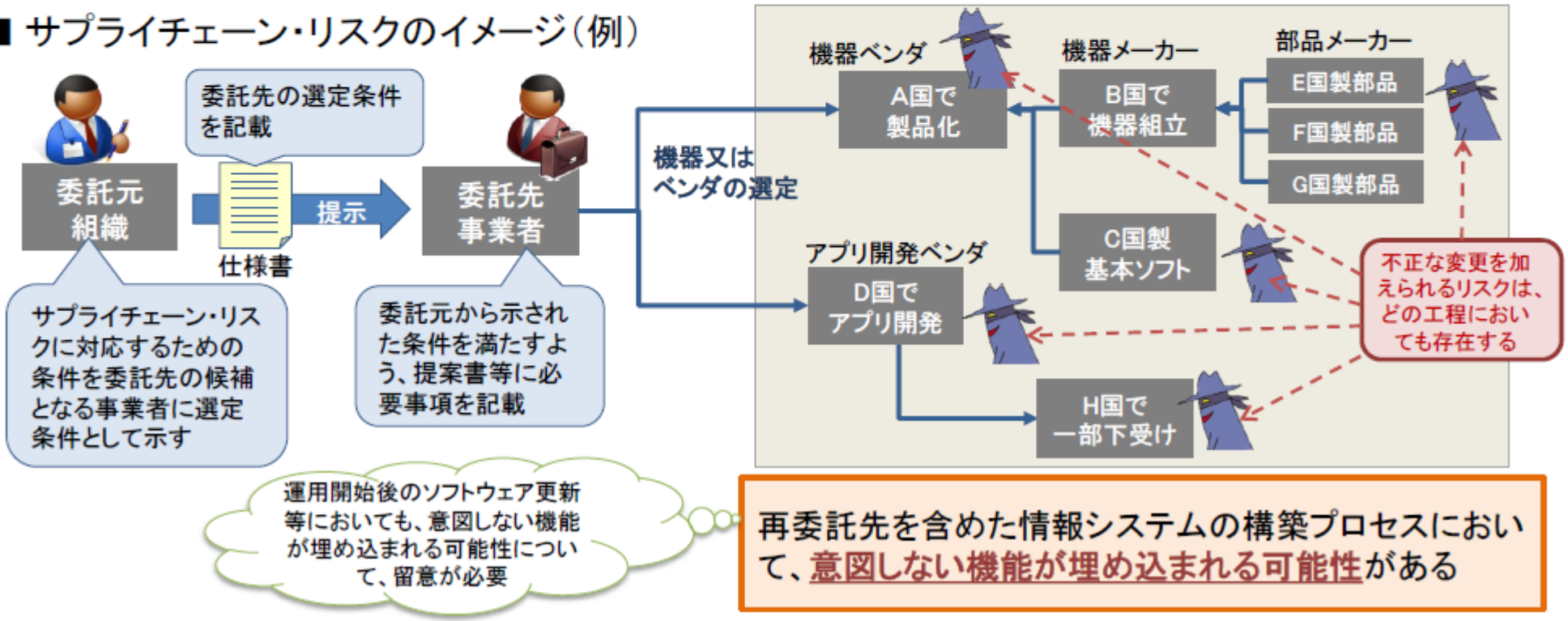
■ サプライチェーン・リスクへの対応

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）



P36

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。

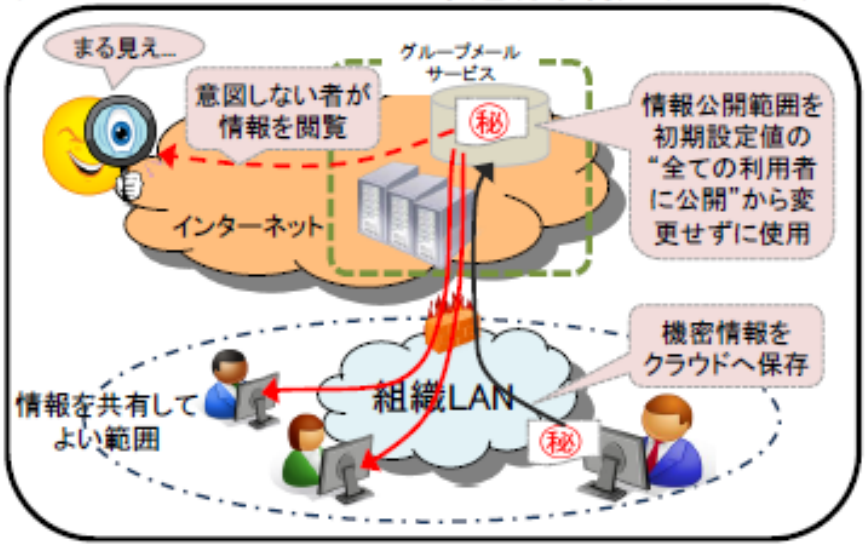
＜最近の事例＞
- 2013年7月　インターネット上でメールを共有できる民間企業の無料サービスで個人情報や中央官庁の内部情報等が誰でも閲覧できる状態になっていた

主な対策

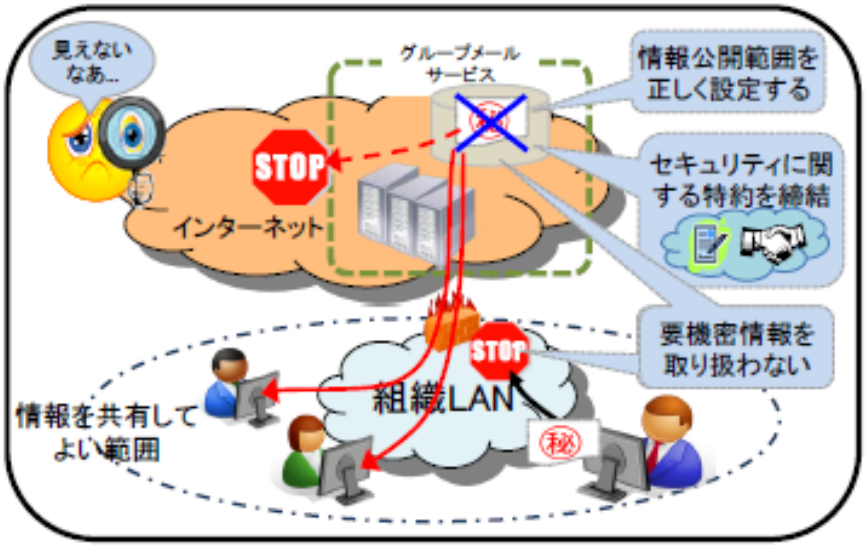
- 約款による外部サービスの利用に係る責任者を設置し、アクセス権設定等の安全管理措置を含む利用手順を整備する。
- セキュリティ水準を十分確保するための特約等を締結する（この場合は4.1.1項を遵守）、又は機密性の高い情報を取り扱わない。

＜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不適切な利用（イメージ）



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。

4.1.3 ソーシャルメディアサービスによる情報発信①

■ 本項の概要

CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

- ソーシャルメディアサービスを使うには約款による外部サービスを利用せざるを得ず、政府ドメイン名も使用できないため、当該サービスを利用した情報発信を行う場合は、なりすましの防止や可用性の確保等の対策が必要。

＜主な遵守事項＞
4.1.3(1)(a) 統括情報セキュリティ責任者は、*(中略)*情報セキュリティ対策に関する運用手順等を定めること。
4.1.3(1)(b) 情報セキュリティ責任者は、*(中略)*利用するソーシャルメディアサービスごとの責任者を定めること。
4.1.3(1)(c) 行政事務従事者は、要安定情報の国民への提供にソーシャルメディアサービスを用いる場合は、府省庁の自己管理ウェブサイトに当該情報を掲載して参照可能とすること。

代表的なソーシャルメディアサービス

ソーシャルネットワーキングサービス(SNS)	動画共有サイト	ブログ
例）Twitter、Facebook、mixi	例）YouTube、ニコニコ動画	例）アメーバブログ、Yahoo!ブログ

一般的な特徴

- 誰でも参加可能
- 参加者同士のコミュニケーション
- 情報が瞬時に拡散

脅威の概要

- アカウントのなりすまし・乗っ取りによる虚偽情報の発信
- 予告なしでのサービス中断・停止

※ 職員がソーシャルメディアサービスを私的に利用する場合は、総務省が公開している「国家公務員のソーシャルメディアの私的利用に当たっての留意点」（平成25年6月）を参照のこと。
http://www.soumu.go.jp/menu_news/s-news/01jinji02_02000084.html

6.2.3 サービス不能攻撃対策

CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

■ 本項の概要

- 政府機関の情報システムのうち、インターネットからアクセスを受けるものについては、サービス不能攻撃を想定し、システムの可用性を維持するための対策を実施することが必要。

＜主な遵守事項＞

6.2.3(1)(a) 情報システムセキュリティ責任者は、*(中略)*サービス提供に必要なサーバ装置、端末及び通信回線装置が装備している機能又は民間事業者等が提供する手段を用いてサービス不能攻撃への対策を行うこと。

6.2.3(1)(b) 情報システムセキュリティ責任者は、*(中略)*サービス不能攻撃を受けた場合の影響を最小とする手段を備えた情報システムを構築すること。

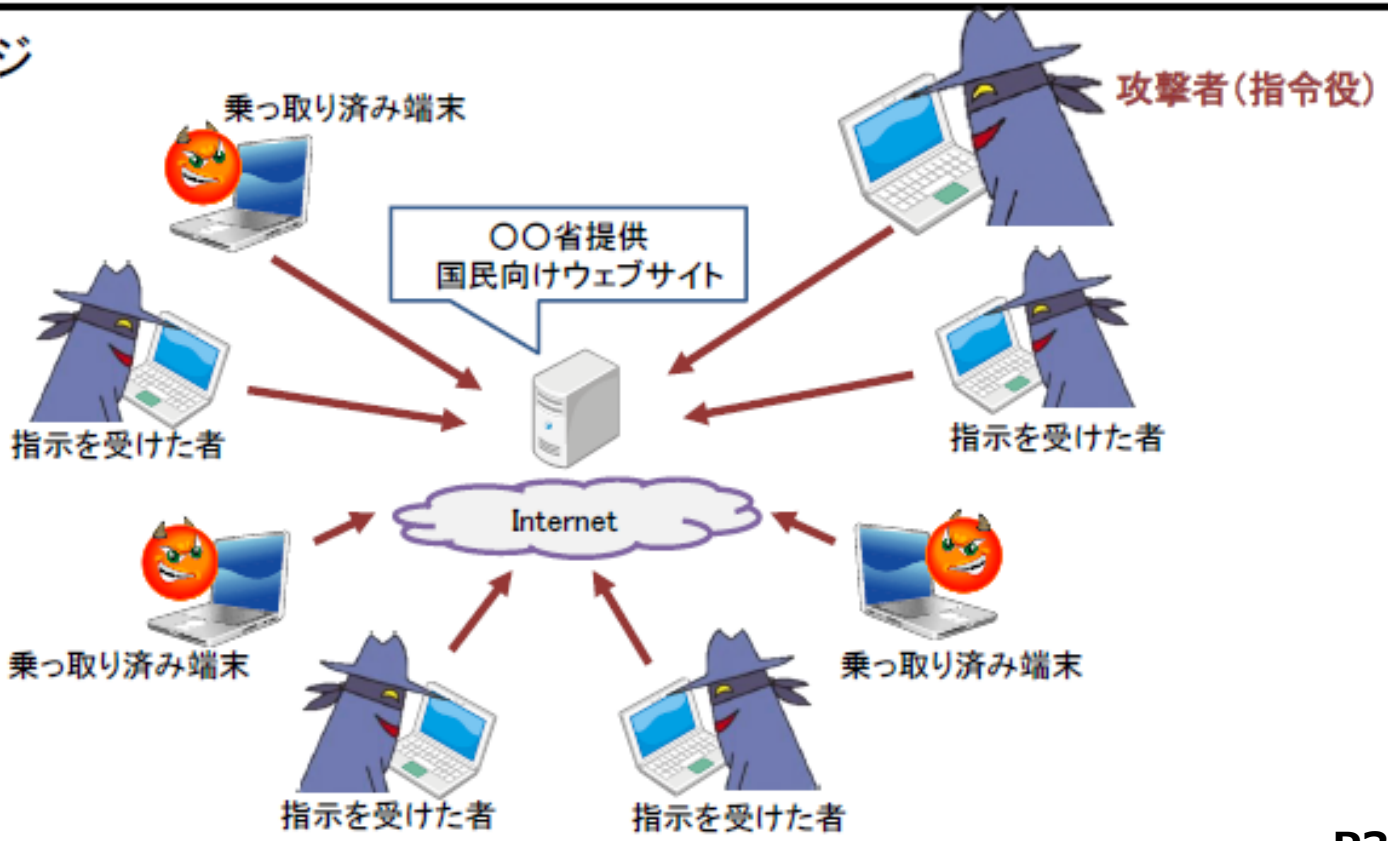
6.2.3(1)(c) 情報システムセキュリティ責任者は、*(中略)*サービス不能攻撃を受けるサーバ装置、端末、通信回線装置又は通信回線から監視対象を特定し、監視すること。

■ サービス不能攻撃のイメージ

DDoS攻撃:
標的のサイトに対して、複数箇所から一斉に大量のアクセス要求を送り、サイトが応答しきれず、サーバーダウンを引き起こし、サービスを提供できない状態に陥れる攻撃。

攻撃を受けるサイト側は、攻撃元のIPアドレスが分かる程度の情報しか得られず、攻撃側の実態を解明するのは困難なため、適切な対策が講じにくい。

攻撃開始を指示する指令役が存在し、その他の攻撃起点としては、指示を受けた者による手動操作のほか、予め不正プログラムに感染させて乗っ取った端末を遠隔操作するものがあるとする説がある。



6.2.4 標的型攻撃対策①

CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

■ 本項の概要

- 標的型攻撃の一連の攻撃活動は、未知な手段も用いて実行されるため、完全に検知及び防御することが困難。入口対策と内部対策からなる対策体系によって攻撃に備えることが必要。

＜主な遵守事項＞
6.2.4(1)(a) 情報システムセキュリティ責任者は、*(中略)*標的型攻撃による組織内部への侵入を低減する対策（入口対策）を講ずること。
6.2.4(1)(b) 情報システムセキュリティ責任者は、*(中略)*内部に侵入した攻撃を早期検知して対処する、侵入範囲の拡大の困難度を上げる、及び外部との不正通信を検知して対処する対策（内部対策）を講ずること。

※ 標的型攻撃：特定の組織に狙いを絞り、その組織の業務習慣等内部情報について事前に入念な調査を行った上で、様々な攻撃手法を組み合わせ、その組織に最適化した方法を用いて、執拗に行われる攻撃

■ 標的型攻撃及びその対策のイメージ

6.2.4 標的型攻撃対策

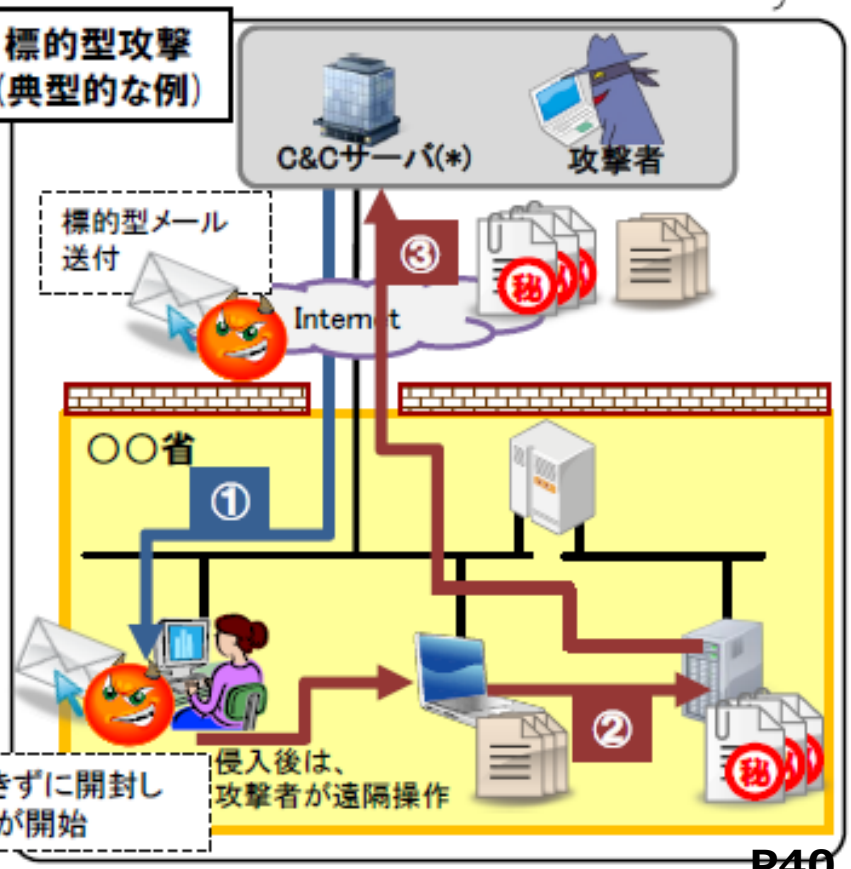
入口対策
・組織内部への侵入を低減

内部対策
・内部に侵入した攻撃を早期検知し対処
・侵入範囲の拡大の困難度を上げる
・外部との不正通信を検知して対処

重点的に守るべき業務を取り扱う情報システムは、「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」に基づく重点対処

標的型攻撃の攻撃プロセス
① 初期潜入
② 侵入範囲拡大
③ 情報窃取

標的型攻撃（典型的な例）



標的型メールを回避できずに開封し攻撃者による遠隔操作が開始

(*) C&Cサーバ(Command & Controlサーバ):
攻撃者が遠隔操作するために用いる。初期潜入された端末は定期的にC&Cサーバにアクセスし、指示内容を確認して実行する。

8.2.1 府省庁支給以外の端末の利用①

CISO | 統括 | 情セキ | 課室 | 情シス | 区域 | 行事

■ 本項の概要

- 行政事務は、府省庁から支給された端末を用いて行うべきであるが、出張や外出等の際にやむを得ず府省庁支給以外の端末を使用する必要が生じる場合がある。その際は、行政事務従事者が定められた手順及び安全管理措置の実施を遵守するよう、責任者の厳格な管理が必要。

＜主な遵守事項＞

8.2.1(1)(a) 統括情報セキュリティ責任者は、府省庁支給以外の端末により行政事務に係る情報処理を行う場合の許可等の手続に関する手順を定めること。

8.2.1(1)(b) 統括情報セキュリティ責任者は、要機密情報について府省庁支給以外の端末により情報処理を行う場合の安全管理措置に関する規定を整備すること。

8.2.1(1)(c) 情報セキュリティ責任者は、*(中略)*安全管理措置の実施状況を管理する責任者を定めること。

8.2.1(1)(d) 前号で定める責任者は、*(中略)*端末の盗難、紛失、不正プログラム感染等により情報窃取されることを防止するための措置を講ずる*(中略)*こと。

■ 府省庁共通で考慮していただきたい事項

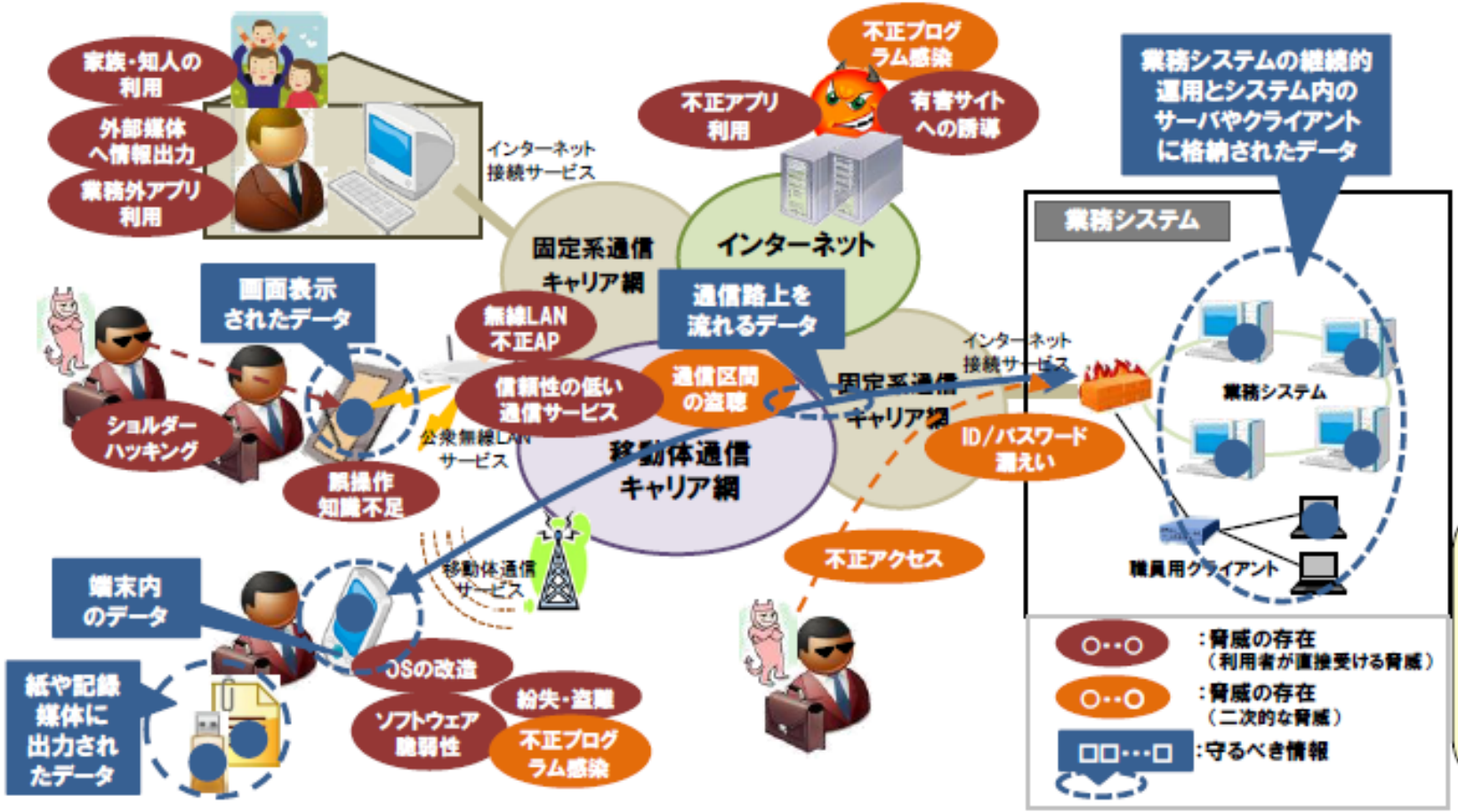
私物端末の利用を認める／認めないにかかわらず、以下事項について、組織として考慮しておくことが重要。

黙認、放置しない

- 組織の実状を把握し、私物端末の持ち込みによるリスクを認識。
- 禁止しても例外的な私物端末利用は発生すると考える。
- 例外的な私物端末の利用頻度が高ければ、府省庁から端末を支給すること、又は、厳格な管理の下、安全に私物端末を利用させることを考える。

8.2.1 府省庁支給以外の端末の利用②

■私物端末の利用におけるセキュリティ脅威と守るべき情報の例



各府省情報化統括責任者（CIO）補佐官等連絡会議ワーキンググループ報告「私物端末の業務利用におけるセキュリティ要件の考え方」（http://www.kantei.go.jp/jp/singi/it2/cio/hosakan/wg_report/index.html）を参考に作成

■対策の考え方

- 利用する端末や利用範囲を限定することによるリスク低減
- 私物端末に業務データを残さない仕組み等の技術的な対策を講じることによるリスク低減
- 利用者との責任分界の明確化

利用者による対策のみに委ねるのは危険です！

統一基準群の位置づけの見直し及び独立行政法人等への適用範囲の拡大

統一基準群を、基本法に基づく政府機関及び独立行政法人等におけるサイバーセキュリティに関する対策の基準と位置づける。
独立行政法人等において、所管府省庁の助言等の下、情報セキュリティ対策が適切に講じられるよう、対策基準等の策定、体制の構築、対策実施状況の評価等に関する規定を追加する。

サイバーセキュリティ基本法（平成26年法律第104号）（抜粋※）　※平成28年4月成立の改正法施行後の条文
第二十五条　サイバーセキュリティ戦略本部は、次に掲げる事務をつかさどる。
（略）
二　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。

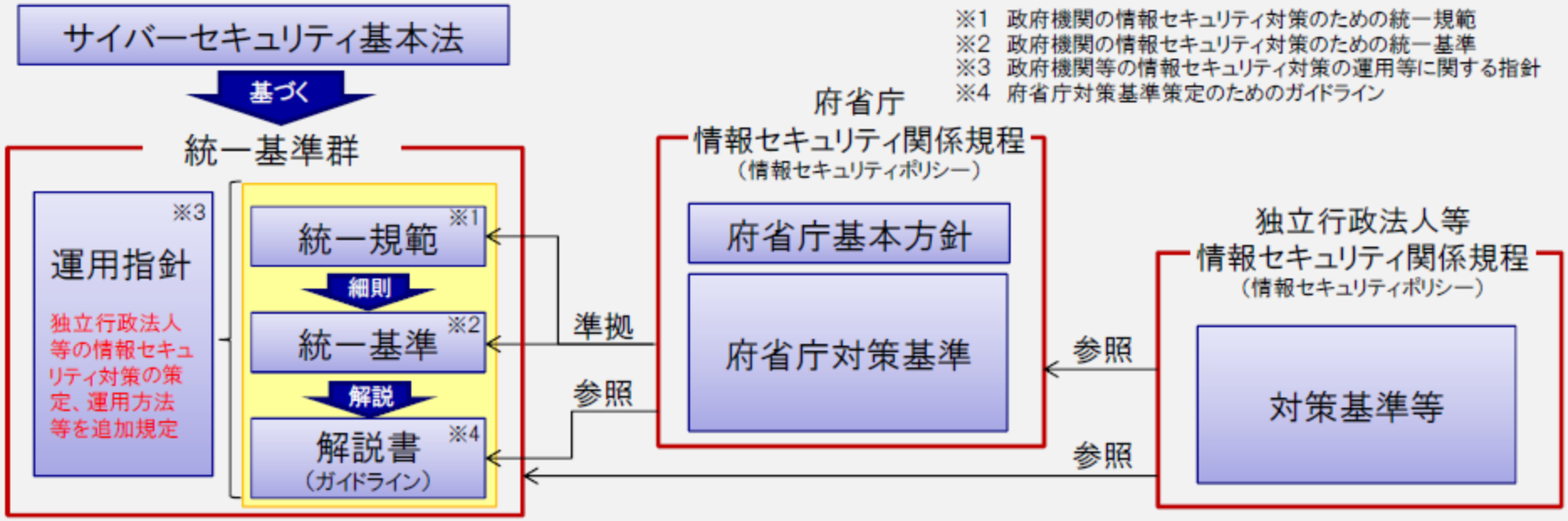
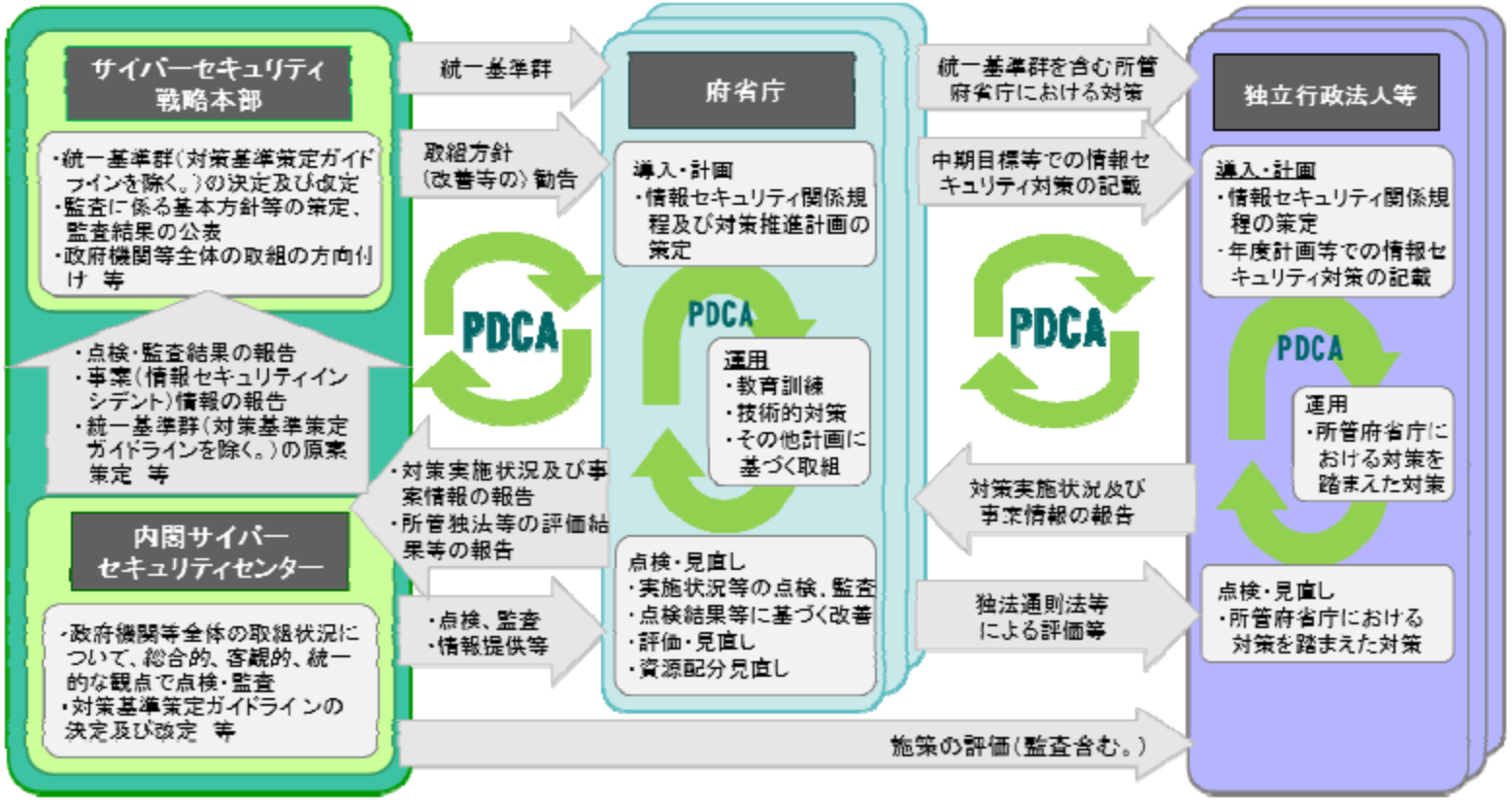


図　サイバーセキュリティ基本法と統一基準群及び情報セキュリティ関係規程の関係

監査に係る規定整備及び政府機関等の情報セキュリティ対策の強化

基本法第25条第1項第2号に基づく監査の実施に係る規定を整備し、以下のとおり独立行政法人等を含む政府機関等のセキュリティ強化に向けたPDCA※サイクルを明確化する。

サイバーセキュリティ基本法（平成26年法律第104号）（抜粋：平成28年4月成立の改正法施行後の条文）
第二十五条　サイバーセキュリティ戦略本部は、次に掲げる事務をつかさどる。
（略）
二　国の行政機関、独立行政法人及び指定法人におけるサイバーセキュリティに関する対策の基準の作成及び当該基準に基づく施策の評価（監査を含む。）その他の当該基準に基づく施策の実施の推進に関すること。



※ PDCA：（Plan〔計画〕、Do〔実行〕、Check〔評価〕、Act〔改善〕）

日本年金機構事案等の外部動向を踏まえた規定の見直し・強化

日本年金機構における不正アクセスによる情報流出事案を始めとする事案（情報セキュリティインシデント）の発生状況やサイバー攻撃の動向、IT利活用環境の変化等を踏まえ、以下の規定の追加及び強化を図る。

事案発生に備えた対処体制（CSIRT※）、対処・連絡手順等の整備に係る規定の強化

- 事案対処に必要な知識・能力を有する対処体制（CSIRT）の構築、外部専門家による支援
- 発生した事案の対処に係る意思決定手法や判断基準、対処方法等の事前準備

※ CSIRT（Computer Security Incident Response Teamの略称）

標的型攻撃等による不正プログラム感染の発生を前提とする情報システムの防御策の強化

- 情報システムの重要な情報を扱う部分のインターネットからの分離
- セキュリティ監視の集中・強化等を目的とした、インターネット接続口の集約
- 実行プログラム形式ファイルが添付された電子メール受信時のシステム措置
- サイバー攻撃を受けた際の影響範囲の特定、原因究明等を適切に実施するための通信記録の管理

情報及び情報システムへの不正アクセスの防止等を目的とする対策の見直し・強化

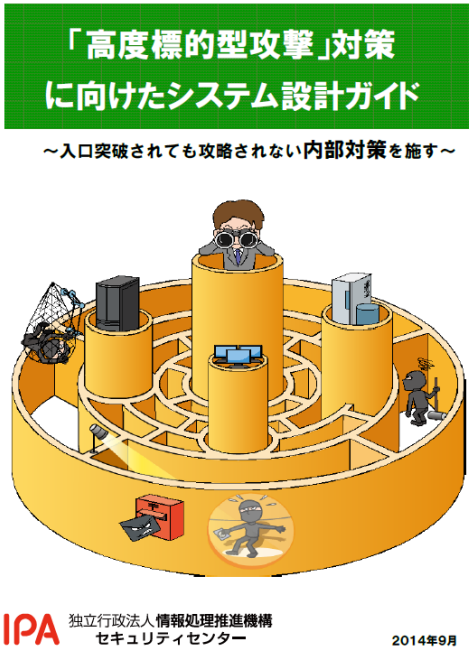
- 個人情報や機微な情報を始めとした機密性・完全性の高い情報を大規模かつ体系的に管理するデータベースに対する対策

新たなIT製品・サービスの普及等に伴う対策事項の明確化

- 情報の取扱いを外部事業者に委ねる際のリスク評価に基づくクラウドサービス※利用可否の判断
- 必要に応じて委託事業の実施場所（クラウド構成機器の所在地等）、準拠法・裁判管轄の指定
- クラウドサービス及び提供事業者の信頼性の確認

※ 外部事業者が有する物理的又は仮想的なコンピュータ資源を利用者の需要に応じて柔軟に提供するサービス

APT対策
IPA 「高度標的型攻撃」対策に向けたシステム設計ガイド




攻撃シナリオ
従来対策
本ガイドの対象範囲
メールとマルウェアの問題
侵害拡大部分
（内部対策を必要とする範囲）
①計画立案
②攻撃準備
③初期潜入
④基盤構築
⑤内部侵入・調査
⑥目的遂行
⑦再侵入
・攻撃目標設定
・関連調査
・標的型メール
・C&Cサーバ準備
・マルウェア感染
・バックドア開設
・端末の諜報
・ネットワーク環境の調査・探索
・端末間での侵害拡大
・サーバへの侵入
・データの外部送信
・データの破壊
・業務妨害
・バックドアを通じ再侵入
社外インターネットエリア
社内ネットワーク
想定脅威
偵察・攻撃環境の準備
マルウェア感染（不正プログラム）
システム内部への不正アクセス（ハッカーによる攻撃）
対策
対策なし
(直接的な攻撃なし)
対策ポイント
入口対策
エンドポイント対策
出口対策
内部対策
・ウィルス対策ソフト
・IDS/IPS
・セキュリティパッチ
…
・ネットワーク分離設計
・管理者権限の最小化
・ファイル共有の制限
…
実害発生

攻撃シナリオにおける攻撃段階

1.計画立案 | 2.攻撃準備 | 3.初期潜入 | 4.基盤構築 | 5.内部侵入・調査 | 6.目的遂行 | 7.再侵入

入口・エンドポイント対策（統一基準範囲）

内部設計対策（出口対策を含む）

攻撃者

突破①

ユーザ端末の感染
コネクトバック通信の施行

対策セットA
対策セットB
対策セットC

突破②

コネクトバック通信の確立
ユーザ端末のリモートコントロール

対策セットD
対策セットE
対策セットF

突破③

情報窃取
システム破壊
再侵入

どの対策セットで検知・遮断したかの把握を行う事で、「攻撃がどの段階まで到達した可能性があるか」の判断材料の一つに利用する。

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

Security by Design（SBD）

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

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)）

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

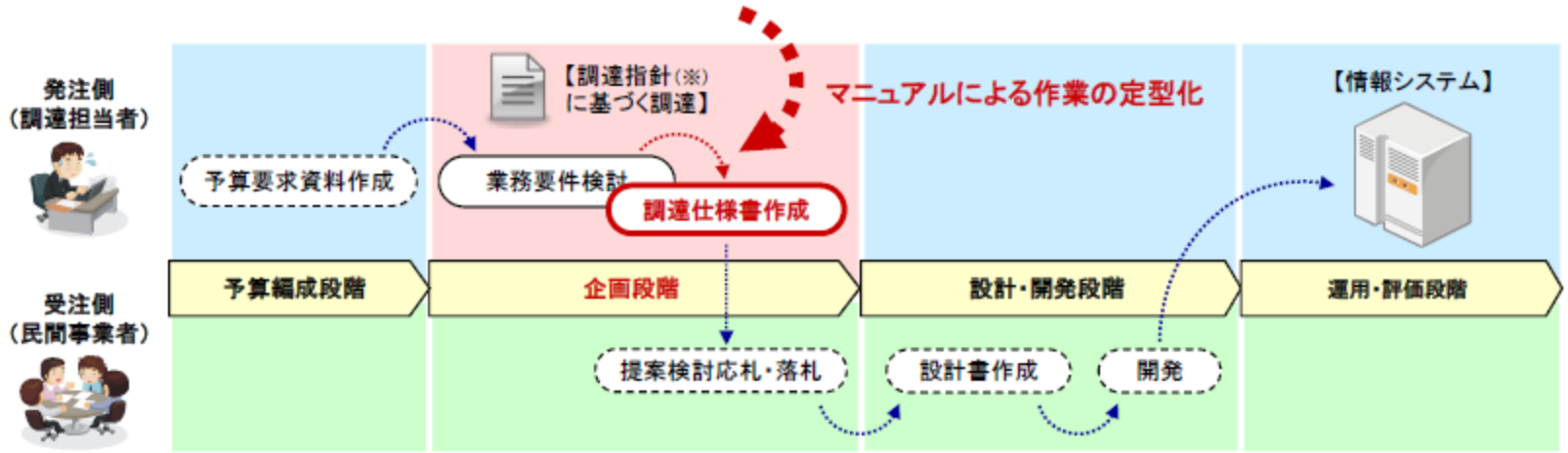
『情報セキュリティを企画・設計段階から確保するための方策に係る検討会（SBD検討会）』を設置

■ 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

目的及び業務を洗い出す

ステップ2

業務の特徴を3つの観点から整理する

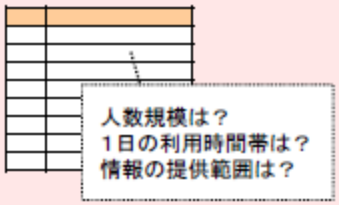
業務	主体	情報	利用環境・手段
1			
2			
3			
4			
5			

ステップ3

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

ステップ4

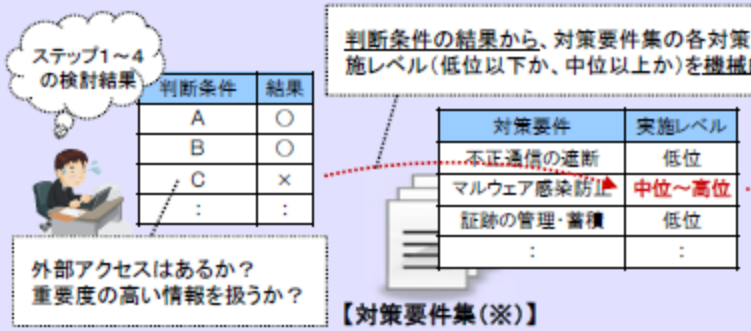
定型設問により業務要件を詳細化する



■ 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）

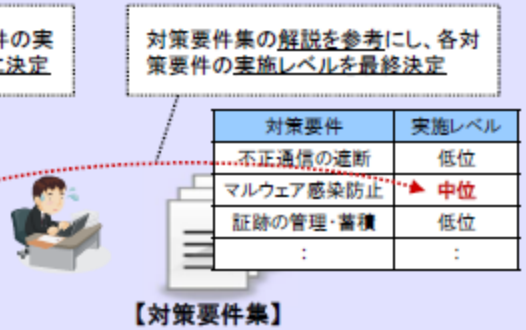
ステップ5

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



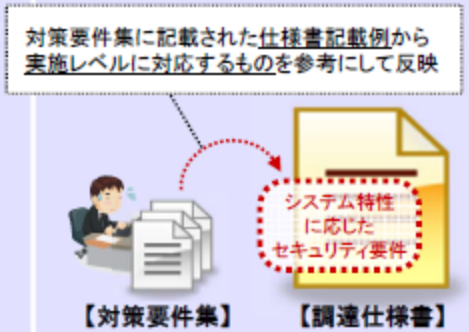
ステップ6

実施レベルを確定し、対策要件を決定する



ステップ7

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

表 11 対策要件集の構成

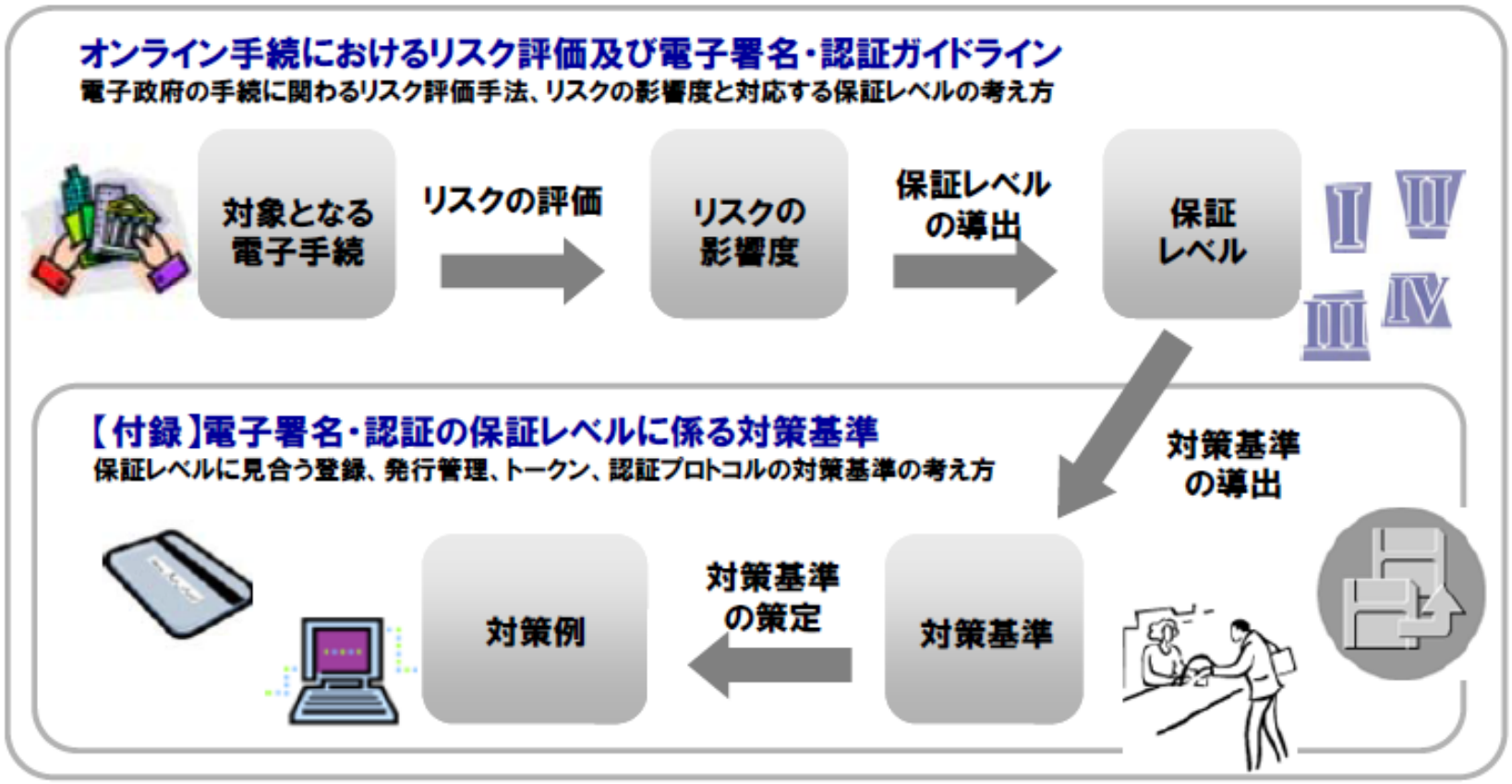
対策区分	対策方針	対策要件	判断条件対応関係（※）	実施レベル有無		
				低位	中位	高位
侵害対策（AT: Attack）	通信回線対策（AT-1）	通信経路の分離（AT-1-1）	A or F		有	有
		不正通信の遮断（AT-1-2）	A		有	
		通信のなりすまし防止（AT-1-3）			有	有
		サービス不能化の防止（AT-1-4）			有	有
	不正プログラム対策（AT-2）	不正プログラムの感染防止（AT-2-1）	-	有		
		不正プログラム対策の管理（AT-2-2）	A or B			有
	セキュリティホール対策（AT-3）	構築時の脆弱性対策（AT-3-1）	-	有		
		運用時の脆弱性対策（AT-3-2）	A	有	有	
不正監視・追跡（AU: Audit）	ログ管理（AU-1）	ログの蓄積・管理（AU-1-1）	B or C	有	有	
		ログの保護（AU-1-2）		有	有	有
		時刻の正確性確保（AU-1-3）	-	有		
	不正監視（AU-2）	侵入検知（AU-2-1）	A		有	有
		サービス不能化の検知（AU-2-2）				有
アクセス・利用制限（AC: Access）	主体認証（AC-1）	主体認証（AC-1-1）	D		有	有
	アカウント管理（AC-2）	ライフサイクル管理（AC-2-1）	D		有	
		アクセス権管理（AC-2-2）	E			有
		管理者権限の保護（AC-2-3）	-	有		
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		有	
		保存情報の機密性確保（PR-1-2）			有	有
		保存情報の完全性確保（PR-1-3）				有

オンライン手続におけるリスク評価及び電子署名・認証ガイドライン

1. ガイドラインの概要

NISC

- 我が国の電子政府における認証方式の設計にあたり活用可能な「ものさし」を確立することを目的として策定。
- ガイドラインは、対象となる電子手続に関するリスク評価手法とこの手法により導出される「リスクの影響度」、影響度に応じた認証方式の「保証レベル」の導出、各保証レベルに求められる対策基準を規定。



2. ガイドラインの概要(リスクの影響度と保証レベル)

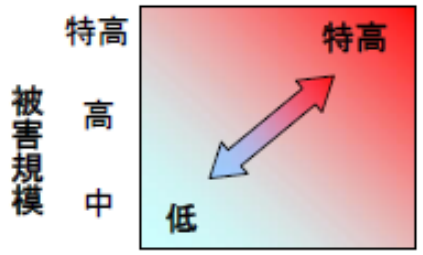
● リスクの影響度の定義

「リスク影響度」を「特高」「高」「中」「低」の4段階に定義。

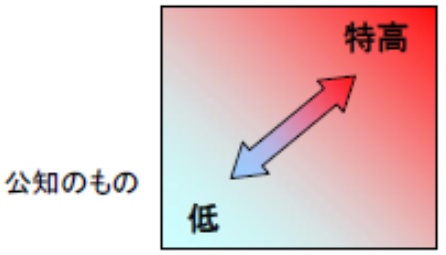
● リスクの評価

いくつかのリスクが想定されるが、オンライン申請等の電子政府サービスにおいては、「機微情報の漏えい」と「金銭的被害」の2つのリスクが主に発生する可能性があり、この2つのリスクについて影響度の導出方法を定義。

【金銭的損害に係るリスクの影響度】



【機微情報の漏えいに係るリスクの影響度】



生命の危険又は差別や名誉毀損等の社会的不利益につながるもののうち、回復が困難なもの

● 総合的リスク評価の導出

「総合的なリスクの影響度」の導出においては、金銭的損害に係るリスク、機微情報の漏えいに係るリスクの他、二次的被害、申請者等の特性、回復可能性など、全ての要素を考慮の上、手続固有の特性を踏まえ導出する。

● リスクの影響度による保証レベルの導出

「総合的なリスクの影響度」から「保証レベル」を導出する。この保証レベルに応じた「対策基準」を参照することにより、当該手続きのリスクの影響度に見合った合理的な認証方式の選択が可能となる。

総合的なリスクの影響度	保証レベル
特高	レベル4
高	レベル3
中	レベル2
低	レベル1

3. ガイドラインの概要(対策基準)

■ 各保証レベルに求められる具体的な対応基準を、4つの評価軸ごとに規定。
■ 対策基準の適用の考え方(※1※2)など、基準実現のための配慮事項についても規定。

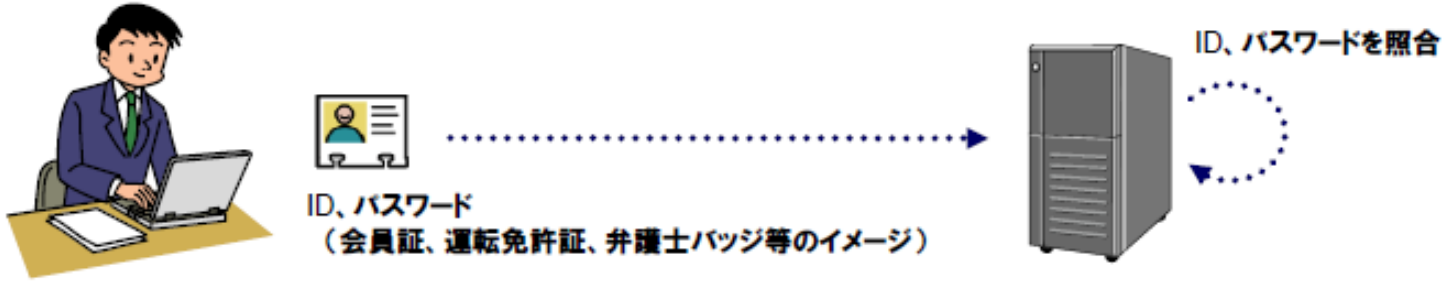
＜主な対策基準＞

保証レベル	登録	発行・管理	トークン	認証プロセス	署名等プロセス
レベル4	(窓口) ・写真付き身分証明1種の提示 ・申請情報の台帳照合 ・重複登録ではないことの確認	・手渡し、本人限定受取郵便、によるトークン発行	・レベル3の基準に加え、耐タンパ性が確保されたハードウェアトークンを利用すること	・レベル3と同等の基準	・電子政府推奨暗号リストに記載の署名方式 ・電子署名用の証明書の用途は電子署名限定
レベル3	(窓口) ・写真付き身分証明1種(or他2種)の提示 ・申請情報の台帳(又は公的証明書)照合 (郵送 or オンライン) ・申請書に対する電子署名 ・申請情報の台帳(又は公的証明書)照合	・レベル4の方法に加え、書留郵便、書留郵便+ダウンロード、電子署名+ダウンロード、によるトークン発行	・レベル2の基準に加え、複数の認証要素を利用すること	・レベル2と同等の基準に加え、フィッシングの脅威に対する耐性	・電子政府推奨暗号リストに記載の署名方式
レベル2	(窓口) ・写真付き身分証明1種(or他2種)の提示 (郵送 or オンライン) ・申請情報に他機関の登録情報(クレジットカード番号等)を含めて申告	・レベル3の方法に加え、分割配付(一方を郵送)、メール通知後のダウンロード、によるトークン発行	・認証情報の推測確率が16384分の1未満であること	・レベル1と同等の基準に加え、盗聴、セッション・ハイジャック、中間者攻撃の脅威に対する耐性	
レベル1	(窓口 or 郵送 or オンライン) ・身元確認は不要 ・メールアドレスの到達確認	・レベル2の発行方法に加え、電子メールによる送付、ダウンロード、によるトークン発行	・認証情報の推測確率が1024分の1未満であること	・オンライン上の推測、リプレイ攻撃の脅威に対する耐性	

※1 上位基準の採用: 認証方式の強度とコスト及び利便性は一般的にトレードオフの関係にあり、コストや利便性等の多様な観点による総合的な判断が必要となる。
※2 代替基準の採用: ガイドラインの対策基準は絶対的なものではなく、同等の代替基準であれば他の対応策による代替が許容される。

4. 認証と電子署名の働き

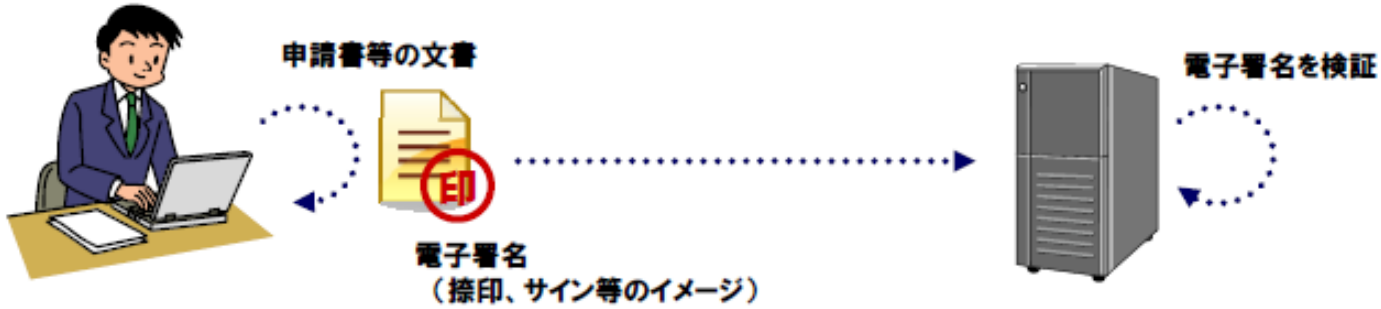
認証（アクセス元の利用者の本人確認を行うこと）



自身の**身元**を相手に伝える

相手が誰かを確認する

電子署名（文書の作成者の確認を可能とする情報、またはそのような情報を文書に付与する行為のこと）



自身が**作成者**であることを示す

文書の**作成者が誰か**を確認する

平成29年度
サイバーセキュリティ関連予算

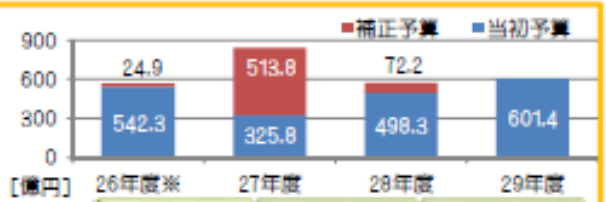
政府のサイバーセキュリティに関する予算

平成29年度予算概算要求額

601.4億円

（平成28年度当初予算額　498.3億円）

サイバーセキュリティに関する予算として切り分けられない場合には計上していない。



主な施策例及び予算額

		平成29年度概算要求	平成28年度第2次補正	平成28年度当初予算
【内閣官房】	内閣サイバーセキュリティセンター予算	28.7億円	4.2億円	17.3億円
【警察庁】	サイバーテロ対策用資機材の増強等	4.1億円	—	4.0億円
【警察庁】	サイバーセキュリティ対策に係る人材育成基盤の整備	8.7億円	—	—
【総務省】	ナショナルサイバートレーニングセンター（仮称）の構築	35.1億円	—	7.2億円
【総務省】	ICT環境の変化に応じた情報セキュリティ対応方策の推進事業	4.0億円	—	4.0億円
【総務省】	IoT時代におけるサイバーセキュリティ総合対策実証事業	—	5.0億円	—
【総務省】	自治体の情報セキュリティ対策の強化	5.0億円	—	—
【外務省】	情報セキュリティ対策の強化	6.3億円	—	4.1億円
【外務省】	サイバー空間に関する外交及び国際連携	0.2億円	—	0.1億円
【経済産業省】	産業系サイバーセキュリティ推進事業	8.0億円	25.0億円	—
【経済産業省】	（独）情報処理推進機構（IPA）交付金	45.5億円	4.0億円	42.5億円
【経済産業省】	サイバーセキュリティ経済基盤構築事業	23.5億円	—	21.6億円
【防衛省】	作戦システムセキュリティ監視装置の整備	7.0億円	—	—
【防衛省】	サイバー攻撃等への対処能力を強化するサイバーレジリエンス技術の研究	7.0億円	—	—
【個人情報保護委】	特定個人情報（マイナンバーをその内容に含む個人情報）に係るセキュリティの確保を図るための委員会における監視・監督体制の拡充	14.3億円	—	2.6億円
【厚生労働省】	本省及び日本年金機構等の関係機関における情報セキュリティ対策の強化	47.1億円	1.8億円	39.6億円
【文部科学省】	大学や高専におけるセキュリティ人材の育成	4.5億円	—	3.8億円
【金融庁】	金融業界横断的なサイバーセキュリティ演習の実施	0.6億円	—	0.3億円
【国土交通省】	重要インフラ事業者等に対する情報セキュリティ強化策	2.2億円	—	0.3億円

平成28年度第2次補正予算

72.2億円

サイバーセキュリティに関する予算として切り分けられない場合には計上していない。

※　平成26年度の数値は、社会保障と税に関する番号制度の導入に伴うシステム開発（内閣官房）等も含む。

経済産業省の施策例

○産業系サイバーセキュリティ推進事業（IPA交付金）

平成28年度補正予算　：25.0億円
平成29年度当初予算　：8.0億円

- IPA（（独）情報処理推進機構）に「産業系サイバーセキュリティ推進センター（仮称）」を創設。世界的な専門人材を招聘し、攻撃対応演習等を実施。

演習のイメージ

①セキュリティ、ネットワーク、制御システムの基礎
ネットワークやシステム構築の演習

②多様な攻撃パターンへの対応訓練

③講師が作成したシナリオに基づく演習

④演習シナリオを研修員自らが作成、実践

○情報セキュリティ対策促進・IT製品の評価・認証等（IPA交付金）

平成28年度補正予算：4.0億円
平成29年度当初予算：45.5億円（42.5億円）

- サイバー攻撃などのセキュリティ関連情報の収集・評価・分析や、対策方法の提案・実施・普及に取り組む。
- また、政府調達等のためのIT製品のセキュリティ評価・認証や、高度セキュリティ人材育成のための研修を実施。

標的型サイバー攻撃情報の共有

①セキュリティ関連情報の収集

IPA

②評価・分析

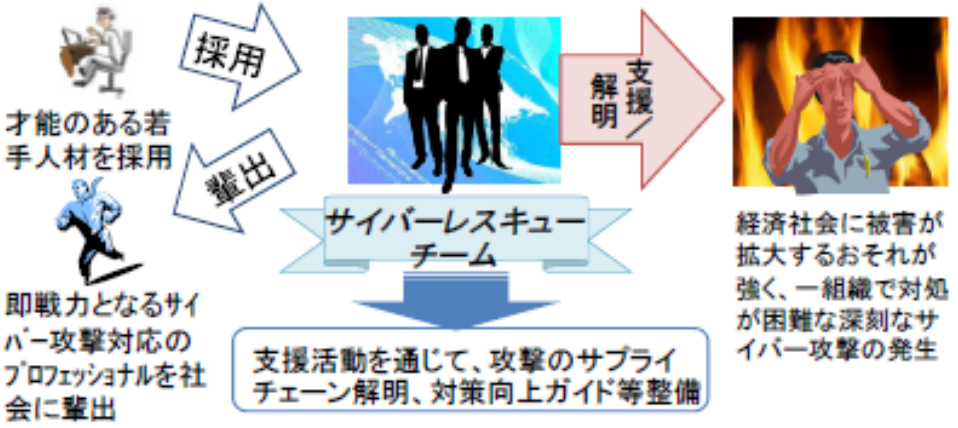
・重要インフラ機器製造
・電力
・ガス
・石油
・化学
・資源開発
・公的機関　など

③対策方法の提案・実施・普及

○サイバーセキュリティ経済基盤構築事業

平成29年度当初予算：23.5億円（21.6億円）

・経済社会に被害が拡大するおそれが強く、一組織で対処困難なサイバー攻撃について、IPAのサイバーレスキュー隊により、被害状況を把握し、被害拡大防止の初動対応を支援。



・攻撃対応連絡調整窓口（窓口CSIRT）の連携により、サイバー攻撃の温床となっている国際的攻撃基盤を共同駆除。

（参考）官民データ活用推進基本法

定義（官民データ、AI、IoT、クラウド）

- この法律において「官民データ」とは、電磁的記録に記録された情報（国の安全を損ない、公の秩序の維持を妨げ、又は公衆の安全の保護に支障を来すことになるおそれがあるものを除く。）であって、国若しくは地方公共団体又は独立行政法人（独立行政法人通則法第二条第一項に規定する独立行政法人をいう。第四の七の１において同じ。）若しくはその他の事業者により、その事務又は事業の遂行に当たり、管理され、利用され、又は提供されるものをいうこと。
- この法律において「人工知能関連技術」とは、人工的な方法による学習、推論、判断等の知的な機能の実現及び人工的な方法により実現した当該機能の活用に関する技術をいうこと。
- この法律において「インターネット・オブ・シングス活用関連技術」とは、インターネットに多様かつ多数の物が接続されて、それらの物から送信され、又はそれらの物に送信される大量の情報の活用に関する技術であって、当該情報の活用による付加価値の創出によって、事業者の経営の能率及び生産性の向上、新たな事業の創出並びに就業の機会の増大をもたらし、もって国民生活の向上及び国民経済の健全な発展に寄与するものをいうこと。
- この法律において「クラウド・コンピューティング・サービス関連技術」とは、インターネットその他の高度情報通信ネットワークを通じて電子計算機（入出力装置を含む。以下同じ。）を他人の情報処理の用に供するサービスに関する技術をいうこと。

推進計画及び会議

● 推進計画

- 政府は、官民データ活用推進基本計画を定めなければならないこと。
- 都道府県は、官民データ活用推進基本計画に即して、都道府県官民データ活用推進計画を定めなければならないこと。
- 市町村は、官民データ活用推進基本計画に即し、かつ、都道府県官民データ活用推進計画を勘案して、市町村官民データ活用推進計画を定めるよう努めるものとすること。

● 会議

- 官民データ活用の推進に関する施策を総合的かつ効果的に推進するため、高度情報通信ネットワーク社会推進戦略本部に、官民データ活用推進戦略会議（以下「会議」という。）を置くこと。
- 高度情報通信ネットワーク社会形成基本法について、高度情報通信ネットワーク社会推進戦略本部の所掌事務に次に掲げる事務を追加すること等所要の規定を整備すること。
  - １　官民データ活用推進基本計画の案の作成及び実施の推進に関すること。
  - ２　１のほか、官民データ活用の推進に関する施策で重要なものの企画に関する調査審議、施策の評価その他の官民データ活用の推進に関する施策で重要なものの実施の推進及び総合調整に関すること。