資料2-1

# 「情報セキュリティポリシーガイドライン」改定のための論点について

2014年10月6日

総務省
MIC Ministry of Internal Affairs and Communications

# 改定のための論点について

「地方公共団体における情報セキュリティポリシーガイドライン」（以下、「ガイドライン」という）の前回改定時（平成２２年１１月）からの情報セキュリティに関わる脅威の高度化、多様化や技術進展などの社会的環境の変化を踏まえ、今回の改定にあたり、改定の是非も含め、重点的に議論すべき項目について整理したものです。

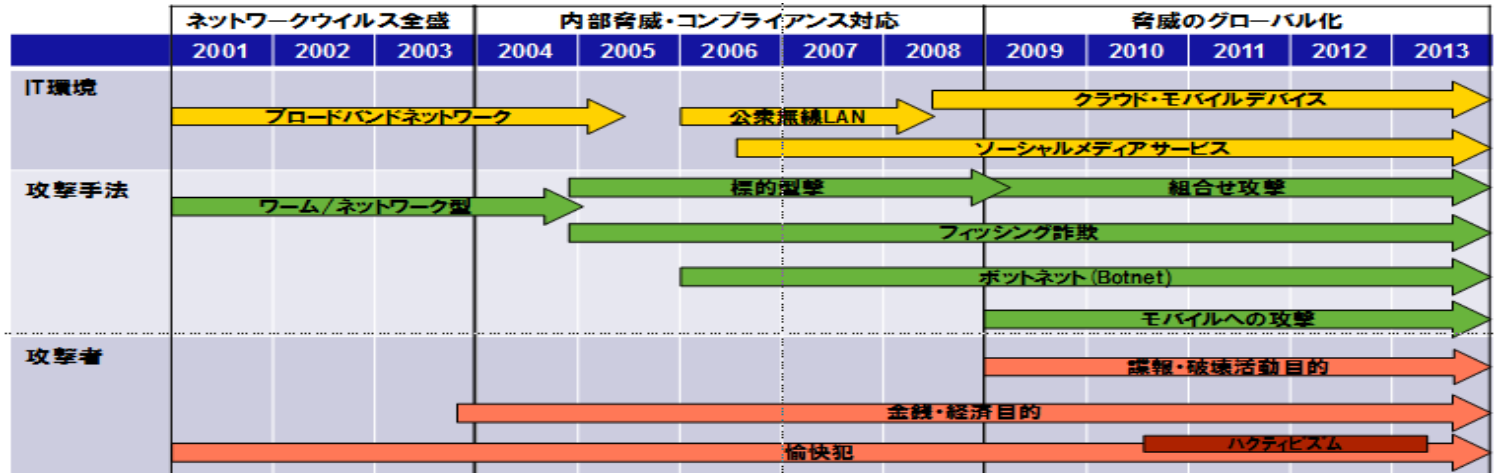
# ガイドライン改定の背景

## 平成25年度、平成26年度の調査

- 「政府機関の情報セキュリティ対策のための統一基準群」の改定内容（ＮＩＳＣ：２０１４年）の整理
- 「ＩＳＯ／ＩＥＣ２７００１：２０１３」（国際規格：２０１３年）,「ＪＩＳ　Ｑ　２７００１：２０１４」（ＪＩＳ規格：２０１４年）の改定内容の整理
- 政府発行の関連文献からの整理
  - －クラウドサービス提供における情報セキュリティ対策ガイドライン（総務省：２０１４年）
  - －重要インフラにおける情報セキュリティ確保に係る『安全基準等』の策定にあたっての指針（ＮＩＳＣ：２０１３年）
  - －スマートフォン・クラウドセキュリティ研究会　最終報告（総務省：２０１２年）
  - －一般利用者が安心して無線LANを利用するために（総務省：２０１２年）
  - －企業等が安心して無線LANを導入・運用するために（総務省：２０１３年）　等
- 地方公共団体における情報セキュリティポリシー運用状況の調査からの整理
  - －２０１３年度に実施された「電子行政サービスの改善に向けた情報セキュリティに関する調査研究」での地方公共団体の調査結果

※改定に当たっては、関連する法制度についても留意しながら検討

## 昨今のIT環境の変化




出典：IPA「情報セキュリティ白書2014」より引用

# 調査結果とIT環境の変化を踏まえたガイドライン改定の観点

## IT環境の変化

- **IT保有形態の変化**
  - 団体・企業におけるクラウド（持たざるIT）利用の加速
  - 不特定多数でリソースを共有するパブリッククラウドの増加
  - 外部サービス利用による事件・事故等のリスク所在変化
- **デバイスの変化**
  - 携帯性・操作性に優れたスマートデバイスの普及
  - アプリ追加やネットワーク接続も従来端末より簡単に
- **ワークスタイルの変化**
  - いつでもどこでも仕事ができる環境による生産性向上と人材活用の動き（在宅勤務、テレワーク）
- **通信環境の変化**
  - 無線LAN、公衆無線LANの普及
  - 仮想ネットワーク、可用性強化要求の高まり
- **情報発信・共有の場の変化**
  - IT空間を使って、誰もが意見・情報を発信・共有
  - これらの情報の活用に様々な可能性が期待
- **ITの重要性の更なる高まり**
  - 社会活動・企業活動において、ITはなくてはならないものに
  - 自治体においては、住民情報を扱う重要な情報基盤
- **サイバー攻撃の悪質化**
  - 特定のターゲット・情報資産を狙った犯罪の増加
  - 検知・対応が遅れた場合の被害は甚大に

## ガイドライン改定の観点

| | |
|---|---|
| クラウド等の外部サービス対応 | 改定の議論が必要と認識（利用可否、採用基準など） |
| スマートデバイス対応（貸与のスマートデバイス） | 現実的な対策技術をふまえ、改定を進める |
| 最新ネットワーク対応 | 改定の議論が必要と認識（利用可否、具体注意事項など） |
| BYOD（Bring your own device）対応（支給以外の端末の業務利用） | 改定の議論が必要と認識（利用可否、具体シーンなど） |
| SNS対応 | 改定の議論が必要と認識（概念の広がりへの対応など） |
| 可用性強化 | 現実的な対策技術をふまえ、改定を進める |
| CSIRT機能 | 改定の議論が必要と認識（必要性、位置づけ、役割など） |
| 標的型攻撃対策 | 現実的な対策技術をふまえ、改定を進める |

総務省 MIC Ministry of Internal Affairs and Communications

# 改定観点ごとの改定内容（案）

本研究会では、観点を含む議論テーマについて、改定の背景や国を含む様々なセキュリティ要請事項などをふまえて議論を行う。

| ガイドライン改定の観点 | | 論点を含む議論テーマ |
|---|---|---|
| クラウド等の外部サービス対応 | → | ①外部委託（クラウドサービス等）<br>②外部委託（サプライチェーン・リスク）<br>③外部委託（委託先管理） |
| 最新ネットワーク対応 | → | ④ネットワークの利用（公衆通信網の利用） |
| BYOD（Bring your own device）対応<br>（支給以外の端末の業務利用） | → | ⑤支給以外のスマートデバイス等の業務利用 |
| SNS対応 | → | ⑥SMS（ソーシャルメディアサービス：SNS、ストリーミング等）の業務利用 |
| CSIRT機能 | → | ⑦情報セキュリティインシデント対策体制の強化 |

# ① 外部委託（クラウドサービス等）

論点整理表：
項番40、63、68

**改定の背景（環境変化）**

- IT保有形態の変化
  - 団体・企業におけるクラウド（持たざるIT）利用の加速
  - 不特定多数でリソースを共有するパブリッククラウドの増加
  - 外部サービス利用による事件・事故等のリスク所在変化
- 通信環境の変化
  - 無線LAN、公衆無線LANの普及
  - 仮想ネットワーク、可用性強化要求の高まり

**現状ガイドライン**

- 外部委託の考え方は、人や物や作業のアウトソーシングが中心であり、クラウドサービスのような外部サービス利用の概念が弱かった。

**ガイドライン改定観点**

- クラウドサービスで機密情報を利用する時の改定観点は、以下となる。
  - 住民情報などの機密性の高い情報は国内法の適用される範囲に置くこと
  - 自治体によるデータセンターの自治体データ保管場所の監督、立ち入り等が実施できること
  - 外部サービスを利用する際の通信はセキュアな回線を使用すること（VPN、専用線等）
  - セキュリティ要件を満たすデータセンターを利用すること（【解説】に要件例を記載）
- 要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合（約款による外部サービス等の利用）、利用するサービスのサービスレベルや想定されるリスクを十分踏まえた上で利用を判断し、適切に対策を講ずることが必要である。

**NISC等の考え方**

- クラウド等の外部サービスを利用し行政事務を遂行する場合、「外部委託」に規定する事項を特約として締結する
- 要機密情報を取り扱わない場合であって、委託先における高いレベルの情報管理を要求する必要が無い場合には、民間事業者が約款に基づきインターネット上で無料で提供する情報処理サービス等を利用することも考えられる。
  ※政府統一基準：4.1.2 約款による外部サービスの利用　より

# ＜参考＞約款による外部サービス利用リスク事例

## 脅威の概要

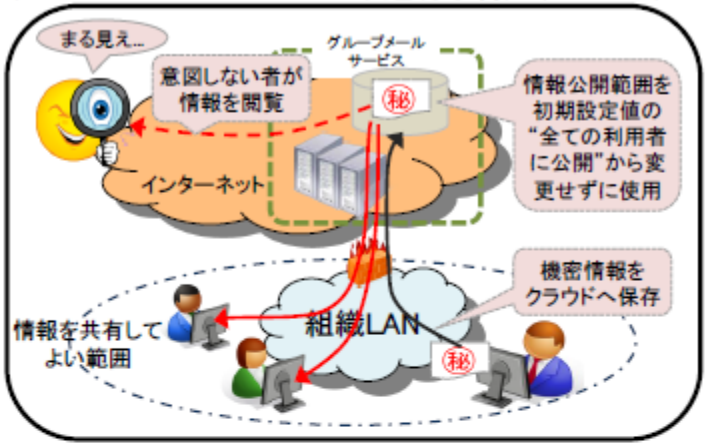
- 約款に同意して利用する一般消費者向けのサービス（グループメールサービス等）には、情報セキュリティに関する十分な条件設定が行えないものも多く、当該サービスの利用が機密情報の流出につながるおそれがある。

＜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

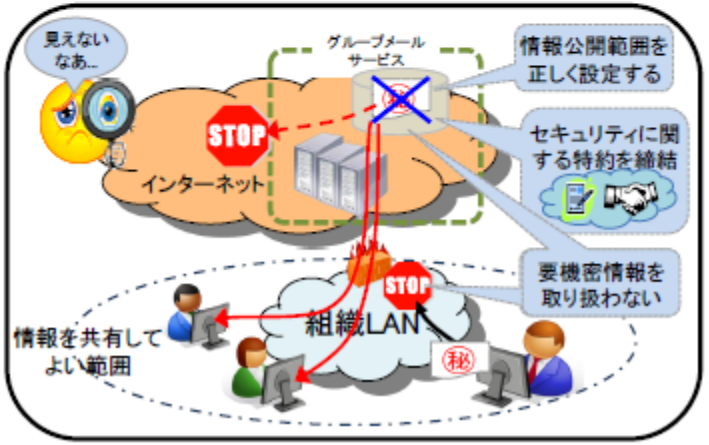
## 主な対策

**・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（「3.7.4 外部委託」を遵守）、又は機密性の高い情報を取り扱わない。**

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）




出典：NISC「政府機関の情報セキュリティ対策のための統一基準群（平成26年度版）について」を参照し作成

# ② 外部委託（サプライチェーン・リスク）

論点整理表：
項番61、62

**改定の背景（環境変化）**

- IT保有形態の変化
  - 団体・企業におけるクラウド（持たざるIT）利用の加速
  - 不特定多数でリソースを共有するパブリッククラウドの増加
  - 外部サービス利用による事件・事故等のリスク所在変化
- 通信環境の変化
  - 無線LAN、公衆無線LANの普及
  - 仮想ネットワーク、可用性強化要求の高まり

**現状ガイドライン**

- 自治体側でセキュリティ要件を考慮し、委託先を選定していた。また、監査についても必要に応じて実施するという考え方であった。
- 委託先による不正行為のリスクについての検討が弱かった。（調達の際に、知らないうちに不要なソフトウェアが導入される等）
- 再委託に関する考慮が弱かった。（原則禁止）

**ガイドライン改定観点**

- 外部委託の際は、要求しない機能が埋め込まれることを防ぐため、委託先において自治体の要件に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とすることが必要である。
- 改定観点は、以下となる。
  - 自治体は委託先の選定条件を定義すること（【解説】に例を記載）
  - 自治体は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強化すること
  - 自治体は委託先の情報セキュリティ対策の履行状況を確認すること

**NISC等の考え方**

- 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。
- 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。

※政府統一基準：4.1.1 外部委託　より

# ② 外部委託（サプライチェーン・リスク事例）

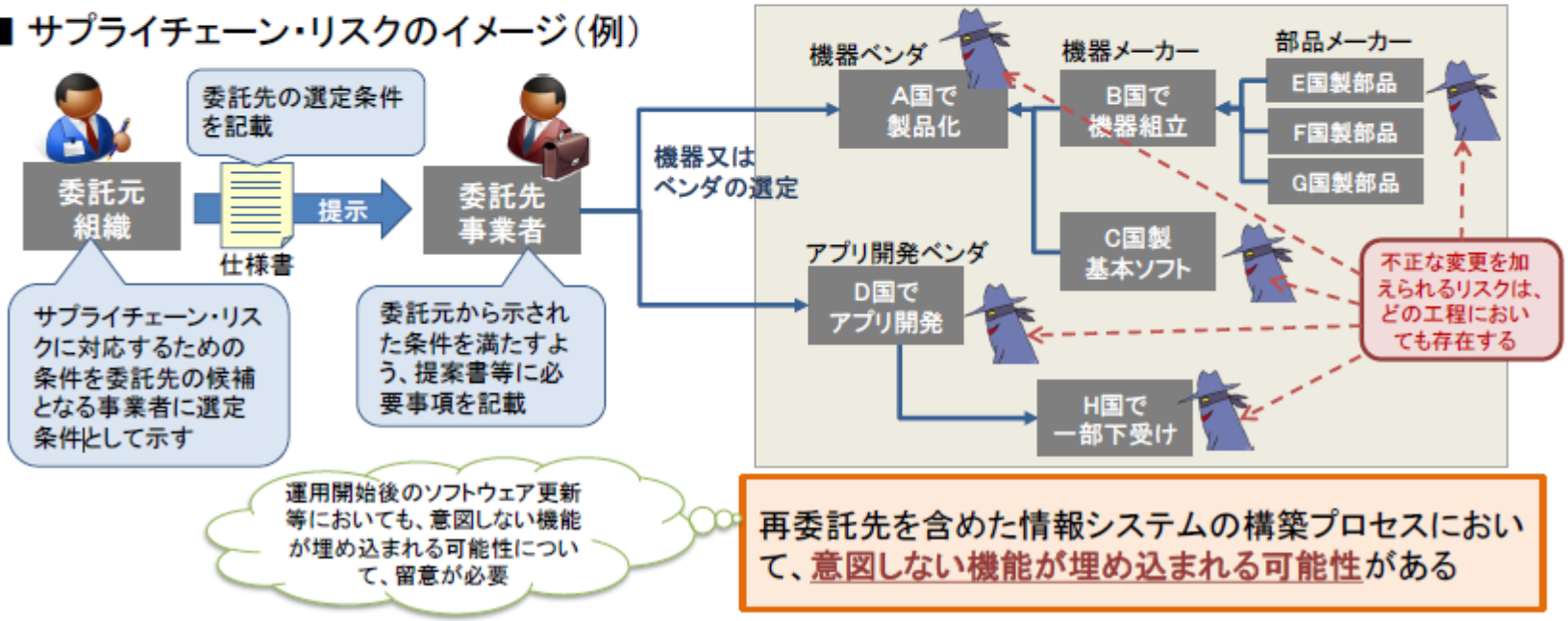
■ サプライチェーン・リスクへの対応

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、<u>意図しない機能が埋め込まれる可能性</u>がある

**出典：NISC「政府機関の情報セキュリティ対策のための統一基準群（平成26年度版）について」より引用**

# ③ 外部委託(委託先管理)

論点整理表：
項番65

**改定の背景（環境変化）**

- IT保有形態の変化
  - 団体・企業におけるクラウド（持たざるIT）利用の加速
  - 不特定多数でリソースを共有するパブリッククラウドの増加
  - 外部サービス利用による事件・事故等のリスク所在変化
- 通信環境の変化
  - 無線LAN、公衆無線LANの普及
  - 仮想ネットワーク、可用性強化要求の高まり

**現状ガイドライン**

- 自治体側でセキュリティ要件を考慮し、委託先を選定していた。また、監査についても必要に応じて実施するという考え方であった。
- 委託先による不正行為のリスクについての検討が弱かった。（作業場所への私物スマートデバイス等の持込み、定期的なログの確認等）
- 再委託に関する考慮が弱かった。（原則禁止）

**ガイドライン改定観点**

- 外部委託の際、委託先における情報セキュリティ対策を直接管理することが困難な場合は、委託先において自治体の要件に適合した情報セキュリティ対策が確実に実施されるよう、委託先への要求事項を調達仕様書等に定め、委託の際の契約条件とすることが必要である。
- 改定観点は、以下となる。
  - 自治体は委託先の選定条件を定義すること（【解説】に例を記載）
  - 自治体は委託先の情報セキュリティ対策の履行状況を確認すること
  - 自治体は委託先がその業務の一部を再委託する場合は、再委託先でも情報セキュリティが確保されるよう委託先に担保させること

    ※上記を踏まえて現状の記述内容を見直す
  - （参考資料）「個人情報保護に関する法律についての経済産業分野を対象とするガイドラインの改定」内容も踏まえた見直しを実施する。

**NISC等の考え方**

- 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、外部委託を実施する際には、選定基準及び選定手続に従って委託先を選定すること。また、以下の内容を含む情報セキュリティ対策を実施することを委託先の選定条件とし、仕様内容にも含めること。
- 情報システムセキュリティ責任者又は課室情報セキュリティ責任者は、契約に基づき、委託先における情報セキュリティ対策の履行状況を確認すること。

※政府統一基準：4.1.1 外部委託　より

# ④　ネットワークの利用（公衆通信網の利用）

**論点整理表：**
**項番18、21、25、26**

**改定の背景（環境変化）**

- ワークスタイルの変化
  - いつでもどこでも仕事ができる環境による生産性向上と人材活用の動き（在宅勤務、テレワーク）
- 通信環境の変化
  - 無線LAN、公衆無線LANの普及
  - 仮想ネットワーク、可用性強化要求の高まり

**現状ガイドライン**

- 通信環境の変化により、無線LANや公衆通信網の普及が進み、庁舎外から業務を行うという観点での対策概念が弱かった。
- 庁内の端末からのアクセスが中心であり、ワークスタイルの変化やニーズに対する考慮が弱かった

**ガイドライン改定観点**

- 自治体庁舎外から庁内の情報システムにアクセスする環境を構築する場合、使用する通信回線は、安全な通信回線サービスを利用することが望ましいが、利用可能なサービスが限られている場合等、安全なサービスを利用できない場合を考慮する必要がある。
- 在宅勤務（テレワーク）等の業務も含め、リモートアクセスでの業務時におけるリスクを十分検討し、必要な対策を実施しておく必要がある。
- 改定観点としては、以下となる。
  - 原則、安全な通信回線サービスを利用すること
  - リモートアクセス環境を構築する場合は、通信内容の暗号化等の対策を行うこと。
  - 自治体は、例外的に公衆通信網を利用する場合は、取り扱われる情報の制限等の精査を行うこと
  - 公衆通信網を利用する場合は、VPN接続、認証処理及び通信内容の暗号化等の対策を実施すること
  - 庁舎内で住民、観光客に公衆通信回線を提供する場合は、庁内の情報システムとネットワークを切り分け、不正アクセスを防止する対策を行うこと
  - 参考として「テレワークセキュリティガイドライン」(総務省発行最新版)を参照するよう記述を追記する

**NISC等の考え方**

- 情報システムセキュリティ責任者は、府省庁内通信回線にインターネット回線、公衆通信回線等の府省庁外通信回線を接続する場合には、府省庁内通信回線及び当該府省庁内通信回線に接続されている情報システムの情報セキュリティを確保するための措置を講ずること
- 情報システムセキュリティ責任者は、公衆電話網を経由したリモートアクセス環境を構築する場合は、利用者の主体認証及び通信内容の暗号化等、情報セキュリティ確保のために必要な措置を講ずること

※政府統一基準：7.3.1通信回線　より

# ⑤ 支給以外のスマートデバイス等の業務利用

論点整理表：
項番14、44

**改定の背景（環境変化）**

- デバイスの変化
  - 携帯性・操作性に優れたスマートデバイスの普及
  - アプリ追加やネットワーク接続も従来端末より簡単に
- ワークスタイルの変化
  - いつでもどこでも仕事ができる環境による生産性向上と人材活用の動き（在宅勤務、テレワーク）

**現状ガイドライン**

- 支給以外のパソコンについての考慮はされていたが、常に持ち歩き、インターネットに接続できるスマートデバイスについての概念が弱かった。
- デバイスはパソコンが中心であり、デバイスの進化によりスマートデバイスの機能が強化されることに関する考慮が弱かった。

**ガイドライン改定観点**

- 行政事務は、自治体から支給された端末を用いて行うべきだが、出張や外出等の際に自治体支給以外の端末を使用を検討する団体が今後出てくることも考えられる。その際は、行政事務を行う職員等が定められた手順及び安全管理措置の実施を順守するよう、責任者の厳格な管理が必要となる。
- 改定観点としては、以下となる。
  - 自治体は、組織の実情を把握し、支給以外の端末の持ち込みによるリスクを認識
  - 支給以外の端末の利用頻度が高ければ、自治体から端末を支給すること、又は、厳格な管理の下、安全に支給以外の端末を利用させることを考える。（管理例について【解説】に記載する）

※支給された端末についてのセキュリティは、資料2-3項番13,17,19参照

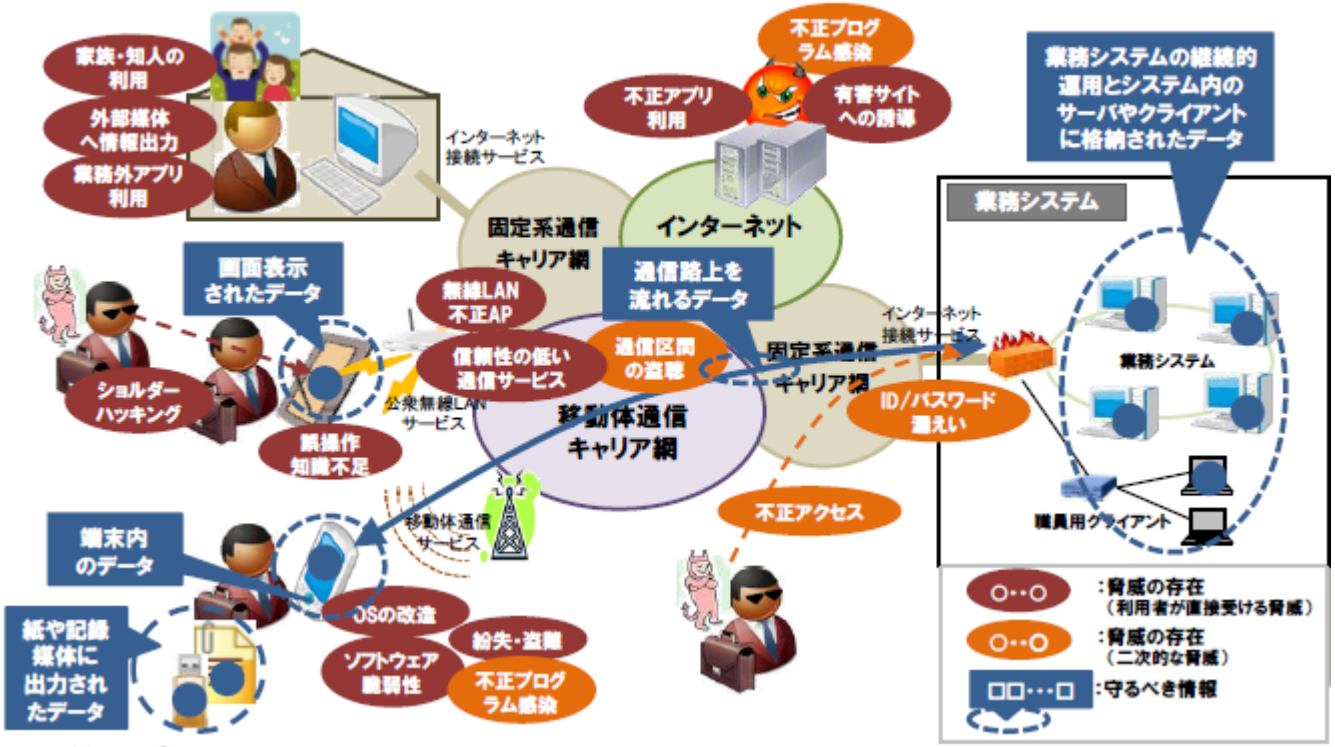
**NISC等の考え方**

- 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。
- 要機密情報を取り扱う府省庁支給以外の端末について、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とともに、行政事務従事者に適切に安全管理措置を講じさせること。

※政府統一基準：8.2.1府省庁支給以外の端末の利用　より

# ⑤　支給以外のスマートデバイス等の業務利用のリスク事例

■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




■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

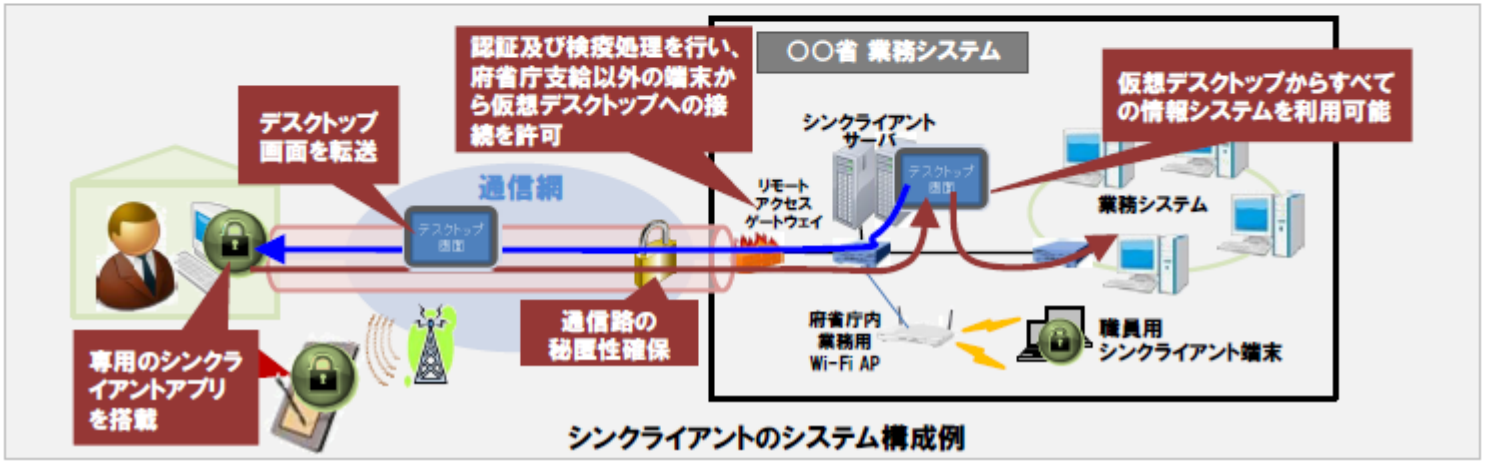
**利用者による対策のみに委ねるのは危険！**

出典：NISC「政府機関の情報セキュリティ対策のための統一基準群（平成26年度版）について」を参照し作成

# ⑤　支給以外のスマートデバイス等の業務利用例

## ■私物端末に情報を保存しないことを前提とした利用形態例


セキュアブラウザ活用型ソリューションのシステム構成例




シンクライアントのシステム構成例

出典：NISC「政府機関の情報セキュリティ対策のための統一基準群（平成26年度版）について」より引用

# ⑥ SMS(ソーシャルメディアサービス：SNS、ストリーミング等)の業務利用

論点整理表：
項番15、45

| 改定の背景（環境変化） | ・情報発信・共有の場の変化<br>・IT空間を使って、誰もが意見・情報を発信・共有<br>・これらの情報の活用に様々な可能性が期待 |
|---|---|

## 現状ガイドライン

- スマートデバイスやタブレット端末が普及しておらず、様々なモノがインターネットにつながっていたわけではなかったことから、SNSやストリーミング等、ソーシャルメディアサービスを利用した情報発信を行うという概念が弱かった。

## ガイドライン改定観点

- 住民への情報提供など、ソーシャルメディアサービスを使う場合は約款による外部サービスを利用することが考えられる。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となる。
- 改定観点としては、以下となる。
  - ・自治体は発信する情報の内容の精査を行うこと（住民情報などの機密性の高い情報の発信の禁止）
  - ・自治体は、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の防止対策を実施すること
  - ・自治体は、予告なしでのサービスの中断・停止対策を検討すること

| NISC等の考え方 | ● 府省庁の自己管理ウェブサイトに当該情報を掲載した上で、ソーシャルメディアサービスを併用するなど、国民が一次情報源を確認できる形にする<br>※政府統一基準：4.1.3ソーシャルメディアサービスによる情報発信　より<br>● 要機密情報（機密性2以上に相当する情報）の発信の禁止<br>※政府機関におけるソーシャルメディアの利用に係る情報セキュリティ対策等について（注意喚起）<br>：NISC注意喚起（平成25年5月1日）より |
|---|---|

# ⑥ SMS(ソーシャルメディアサービス：SNS、ストリーミング等)の業務利用

**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

## 具体的対策例

**運用手順等の整備**

- アカウント名やアカウントの自由記入欄等を利用した運用組織の明示
- アカウントの自由記入欄等へのアカウント運用ポリシーの掲載
- 府省庁ウェブサイトへのアカウント名の掲載
- URL短縮サービスの原則利用禁止
- 認証アカウント（公式アカウント）の利用（提供されている場合）
- パスワード等の主体認証情報の適切な管理

**責任者の設置**

- 利用するソーシャルメディアサービスごとに責任者を設置

**要安定情報の自己管理ウェブサイトへの掲載**

- 要安定情報を国民に提供する場合は、当該情報を府省庁の自己管理ウェブサイトへ掲載

出典：NISC「政府機関の情報セキュリティ対策のための統一基準群（平成26年度版）について」より引用

# ⑦ 情報セキュリティインシデント対策体制の強化

論点整理表：
項番8、10、22、
42、49、58

**改定の背景（環境変化）**

- ITの重要性の更なる高まり
  - 社会活動・企業活動において、ITはなくてはならないものに
  - 自治体においては、住民情報を扱う重要な情報基盤
- サイバー攻撃の悪質化
  - 特定のターゲット・情報資産を狙った犯罪の増加
  - 検知・対応が遅れた場合の被害は甚大に

**現状ガイドライン**

- 緊急時の報告ルートや責任者の存在、情報セキュリティ委員会でのセキュリティポリシーの策定等、それぞれの活動の必要性は説明しているが、情報セキュリティインシデントにおける情報収集、調査、対処、窓口機能等、包括的に対応する体制を整備するという概念が弱かった。

**ガイドライン改定観点**

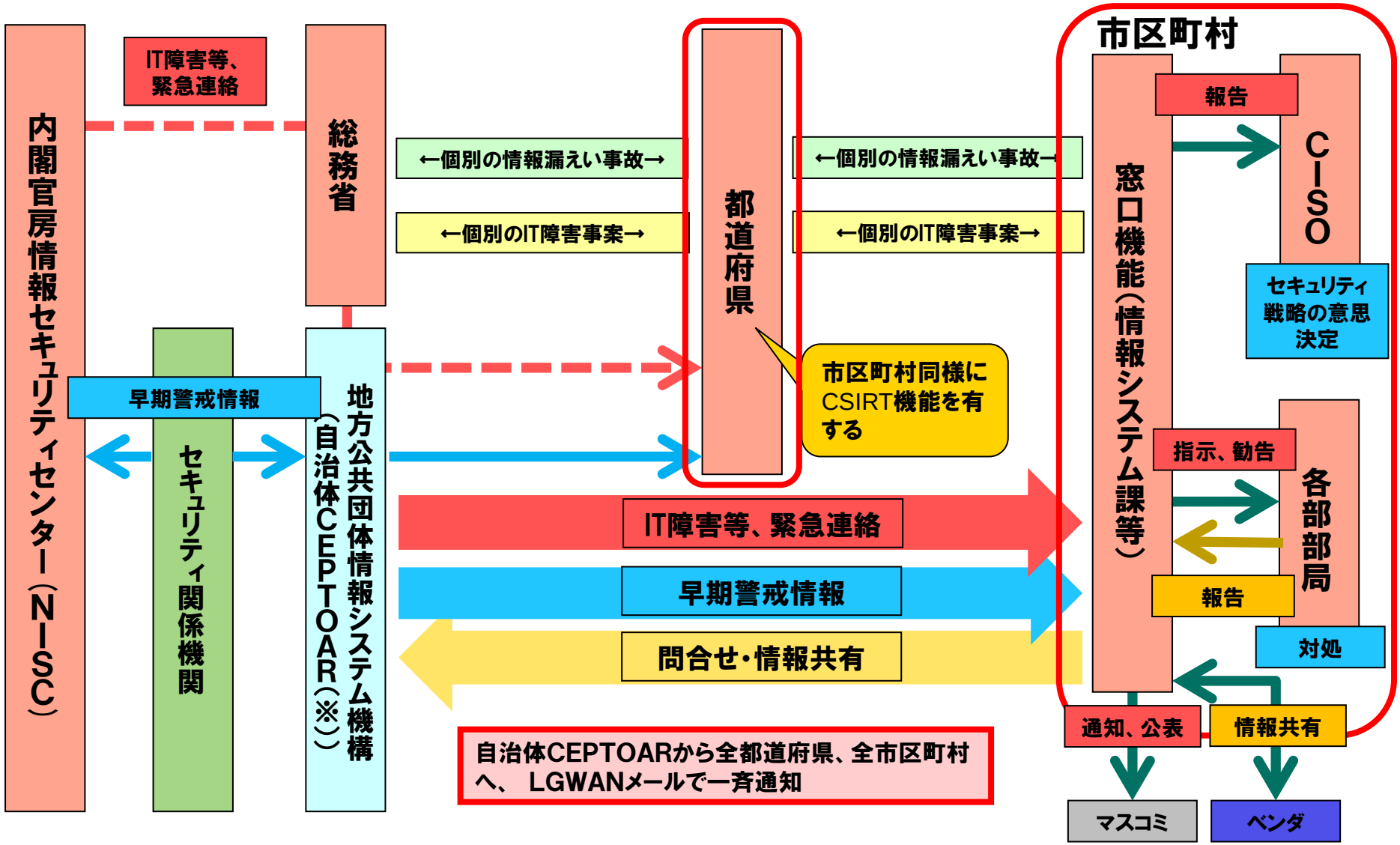
- 情報セキュリティインシデントを認知した場合は、最高情報セキュリティ責任者に早急にその状況を報告するとともに、被害の拡大を防ぎ、回復のための対策を講ずる必要がある。
- 改定観点としては、以下となる。
  - 自治体における、セキュリティ事件・事故への一元的な窓口組織の位置づけ、役割の検討(インシデント発生部署以外への情報提供、ベンダとの連絡調整、マスコミ対応等)
  - CISO機能の位置づけ、役割の検討、窓口組織との関係性
  - 構成するメンバの役割、意識づけ、人材確保のための施策
  - 注)として、CSIRT機能と窓口組織の関係について記載(自治体CEPTOAR、J-LIS、NISC等との連携)

**NISC等の考え方**

- CSIRTは、認知した情報セキュリティインシデントに関係する情報セキュリティ責任者に対し、被害の拡大防止等を図るための応急措置の実施及び情報セキュリティインシデントからの復旧に係る指示又は勧告を行うこと。
- 情報システムセキュリティ責任者は、所管する情報システムについて情報セキュリティインシデントを認知した場合には、府省庁で定められた対処手順又はCSIRTの指示若しくは勧告に従って、適切に対処すること。

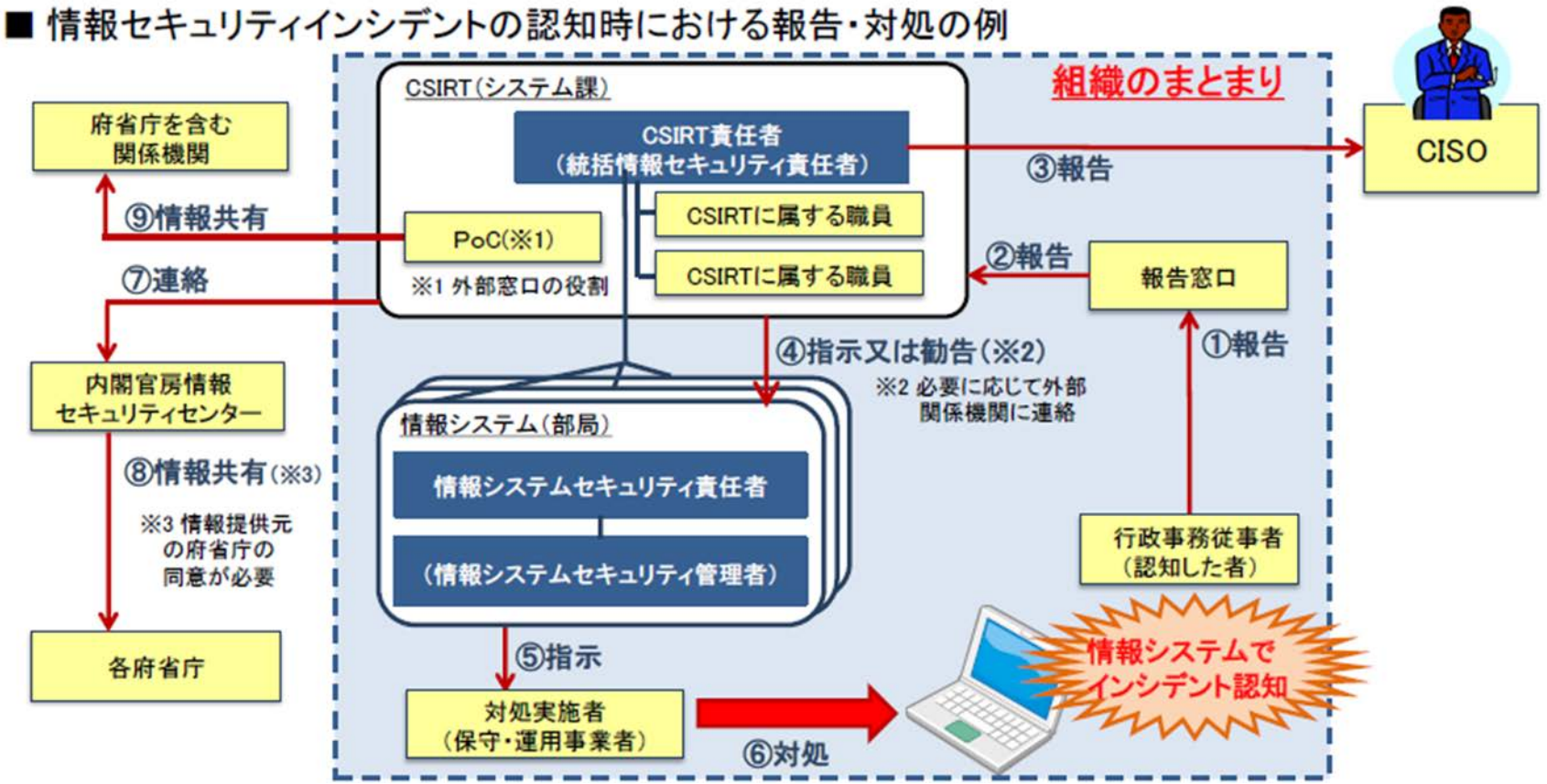
※政府統一基準：2.2.4情報セキュリティインシデントへの対処　より

# ⑦ 情報セキュリティインシデント対策体制の強化事例




※CEPTOAR（セプター）：Capability for Engineering of Protection, Technical Operation, Analysis and Responseの略。重要インフラ分野（10分野）で整備する「情報共有・分析機能」のこと。自治体CEPTOARについては、地方公共団体情報システム機構が事務局を担当している。

# ⑦　情報セキュリティインシデント対策体制の強化事例




出典：NISC「政府機関の情報セキュリティ対策のための統一基準群（平成26年度版）について」より引用