個人情報保護対策と政府機関情報セキュリティ対策統一基準

独立行政法人等情報公開・
個人情報保護担当者連絡会議
2013年1月21日

日本ヒューレット・パッカード株式会社　個人情報保護対策室長
元　内閣官房情報セキュリティセンター　参事官補佐・指導専門官
佐藤　慶浩　http://yosihiro.com/profile/

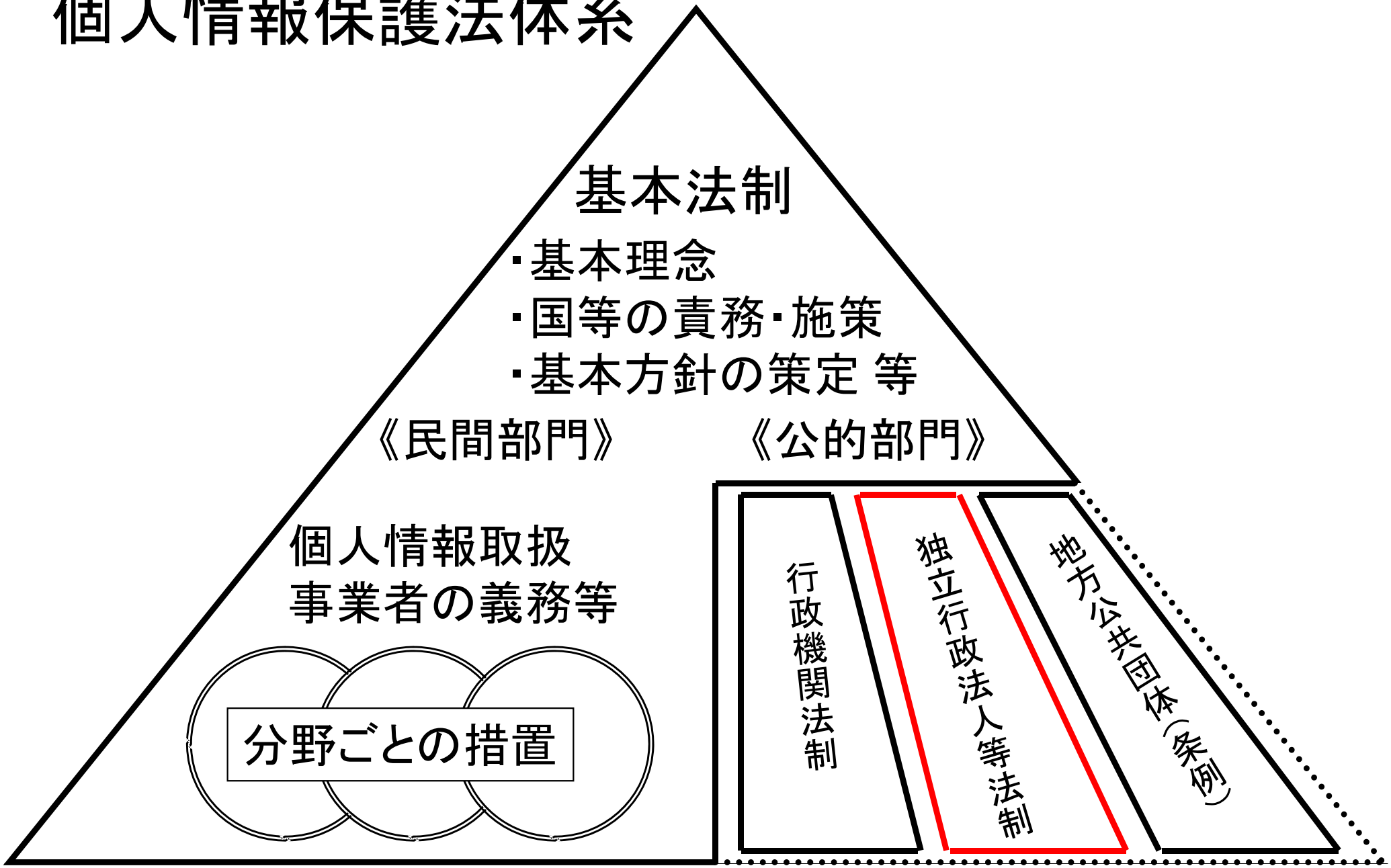
© Copyright 2012 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice.

目次

個人情報保護法
個人情報保護対策と情報セキュリティ対策
政府機関情報セキュリティ対策統一基準
情報セキュリティ対策の実践

個人情報保護法

個人情報保護法体系


基本法制
・基本理念
・国等の責務・施策
・基本方針の策定 等
《民間部門》
《公的部門》
個人情報取扱
事業者の義務等
分野ごとの措置
行政機関法制
独立行政法人等法制
地方公共団体（条例）

個人情報保護法　独立行政法人等

独立行政法人等の保有する個人情報の保護に関する法律
独立行政法人等の保有する個人情報の保護に関する法律施行令
独立行政法人等の保有する個人情報の保護に関する法律に係る行政手続等における情報通信の技術の利用に関する法律施行規則

独立行政法人等保有する個人情報の適切な管理のための措置に関する指針について（行政管理局長通知）
独立行政法人等の保有する個人情報の保護に関する法律の施行に当たって（行政管理局長通知）
個人情報の適切な管理等の徹底について（行政情報システム企画課長通知 ）

http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/horei_kihon.html

個人情報保護法の位置づけ

自動車の運転と道路交通法の関係に似ています。

道路交通法を守るために運転するわけではありません。
安全な運転をするための（最低限の）ルールが道路交通法で定められています。
自分のためにすること（速度制限など）と、他の人のためにすること（方向指示器の点灯など）で、他の人も安全になり、結果的に自分もまた安全になることで、安全に自動車を利用することができるようになります。

個人情報保護法の位置づけ

事業者による個人情報の利用について安心してもらうための法律です。

安心してもらうための（最低限の）ルールが個人情報保護法で定められています。

安心してもらうことによって、事業者は個人情報を利用することができるようになります。

個人情報保護法の位置づけ

法律の対応として難しく考えるよりは・・・
お客様に対するビジネスマナーとして考えるのがとりかかりやすい。（と思います。）

そう考えながら内容を理解すると、かなり当たり前のことが要求されているだけです。
マナーを守らない人が多いと法令等により規制されてしまいます。

個人情報保護法の説明が、道路交通法の学科教習だとすると、これからご紹介するのは、安全運転教習です。

個人情報保護対策と情報セキュリティ対策

あるシンポジウムのアンケート結果から

■プライバシーや個人情報保護の対策には、情報流出対策や不正アクセス対策などの情報セキュリティ以外の対策として、どのようなことがあるか具体的に2つ以上ご存知ですか？

1．はい　　2．いいえ　　3．よくわからない

24名

「はい」の場合、
ご存知のものを2つだけ具体的にお書きください：

回答数　57名

正解＝13名 (23%)

個人情報保護対策 「法律による主な義務」

個人情報保護法
- 利用目的の通知
- 利用目的の範囲内での利用
- ご要望（開示、訂正、利用停止等）に応じる
- 第三者提供する場合の同意取得
- 情報の安全管理

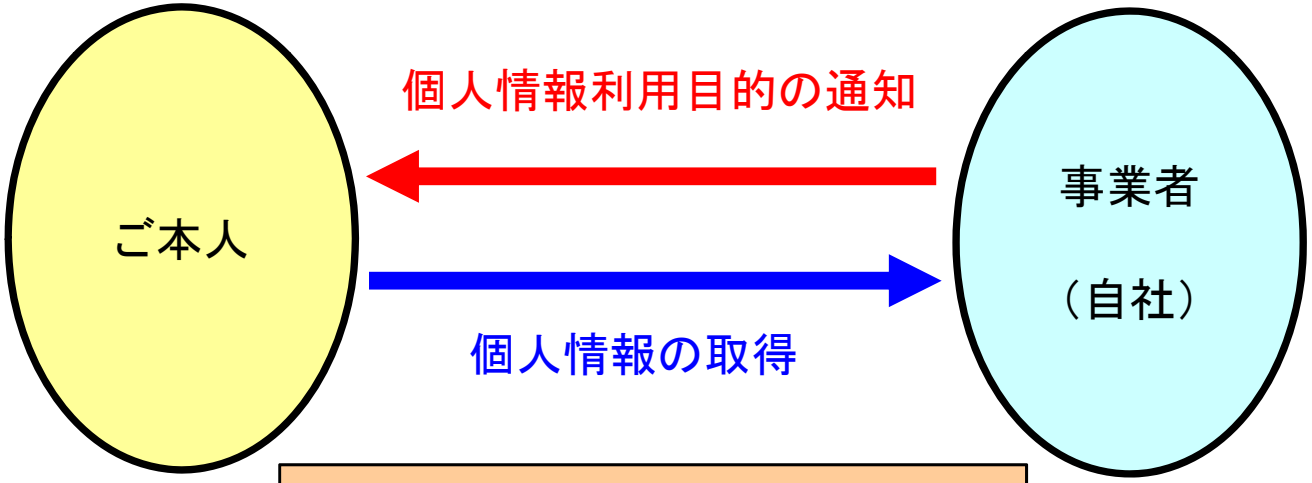
特電法（特定電子メールの送信の適正化等に関する法律）
（通称、迷惑メール防止法）
- 電子メール送信の同意取得
- 電子メール送信時の特定項目の記載

個人情報保護対策
「利用目的の通知」

個人情報保護法による義務

個人情報を取得する際には、必ず、「利用目的」を取得時にご本人に知らせなければなりません。

「利用目的」の表記方法は会社の標準を作るのも一例。その場合には、個々の社員が「利用目的」を勝手に作文しないようにします。



利用目的を通知せずに、個人情報を取得すると、取得する行為そのものが違法となります。

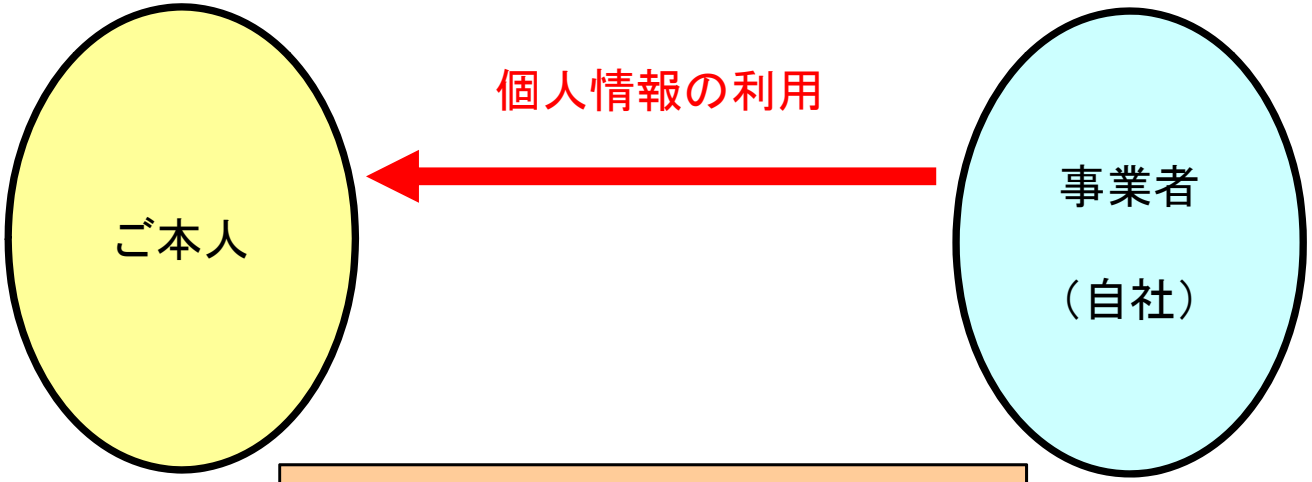
個人情報とは：お客様、取引先、下請けなど個人を特定できる情報を含むものすべて
取得とは：氏名の記入や、Web画面入力、名刺をいただくことなど

同意を得る必要はありませんが、安心できない利用目的だと、個人情報を教えてもらえません。

個人情報保護対策
「利用目的の範囲内での利用」

個人情報保護法による義務

個人情報を利用する際には、ご本人に知らせた「利用目的」を達成する範囲内だけで利用しなければなりません。

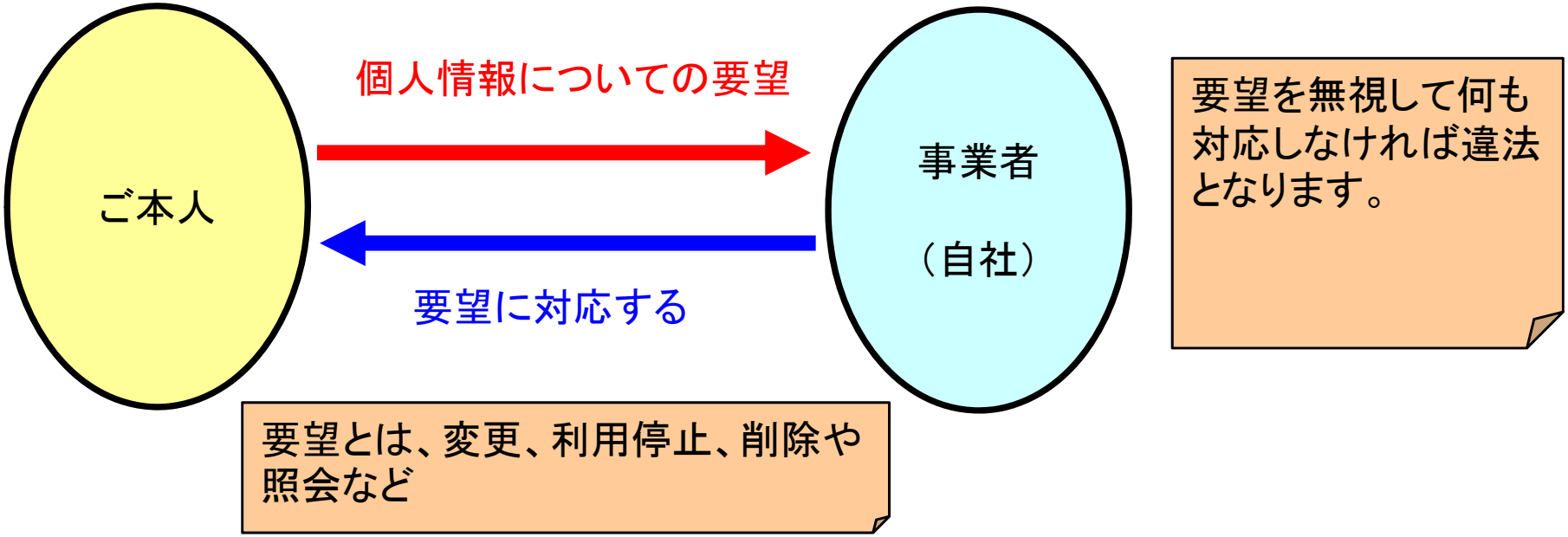


個人情報の利用とは：たとえば、住所の情報を使ってダイレクトメールを送付することや、電話番号情報を使ってセールスの電話をかけることなどがあります。

個人情報保護対策
「ご要望に応じる」

個人情報保護法による義務

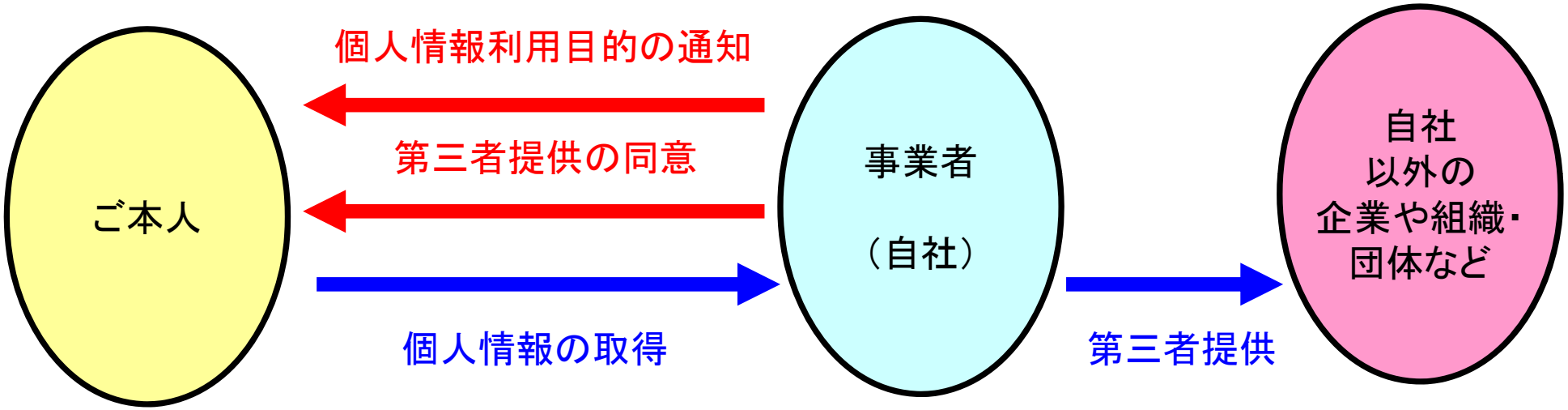
個人情報についてご本人からご要望があれば、それに対応しなければなりません。



個人情報保護対策
「第三者提供の同意」

個人情報保護法による義務

個人情報を自社以外に提供する（参照させる）際には、ご本人から、予め「第三者提供の同意」を得なければなりません。

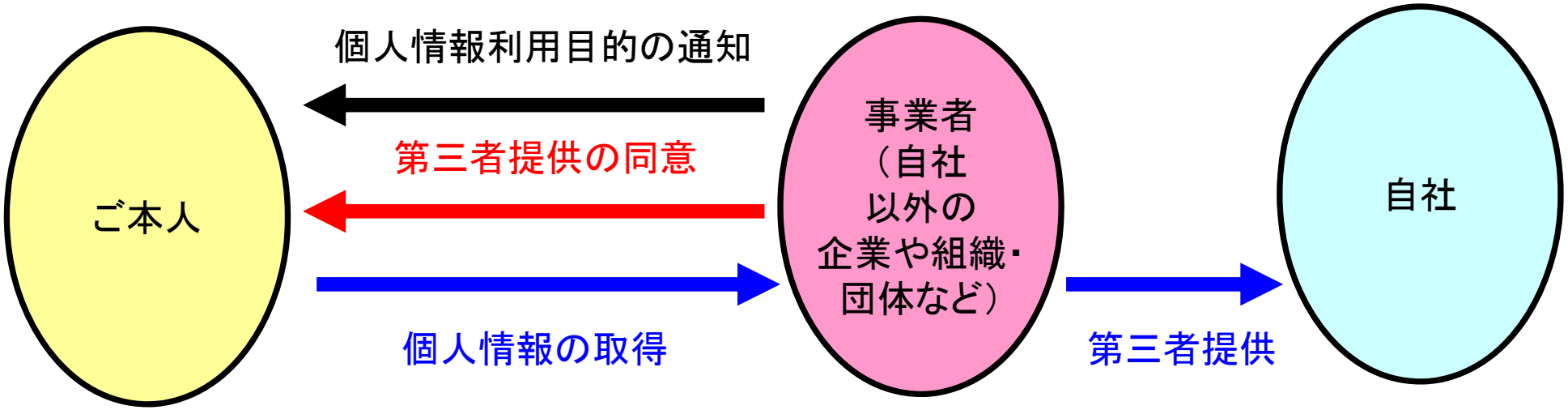


ご本人から第三者提供の同意を予め得ずに、個人情報を自社以外に提供すると違法になります。
イベントやセミナーの共催であっても、例外ではありません。
業務を社外に委託している場合には、その旨を通知したり同意を得たりする必要はありません。

個人情報保護対策
「第三者提供の同意」

個人情報保護法による義務

個人情報をご本人以外から取得（入手）する場合には、自社に対する第三者提供の同意を予め得てもらったものに限ります。

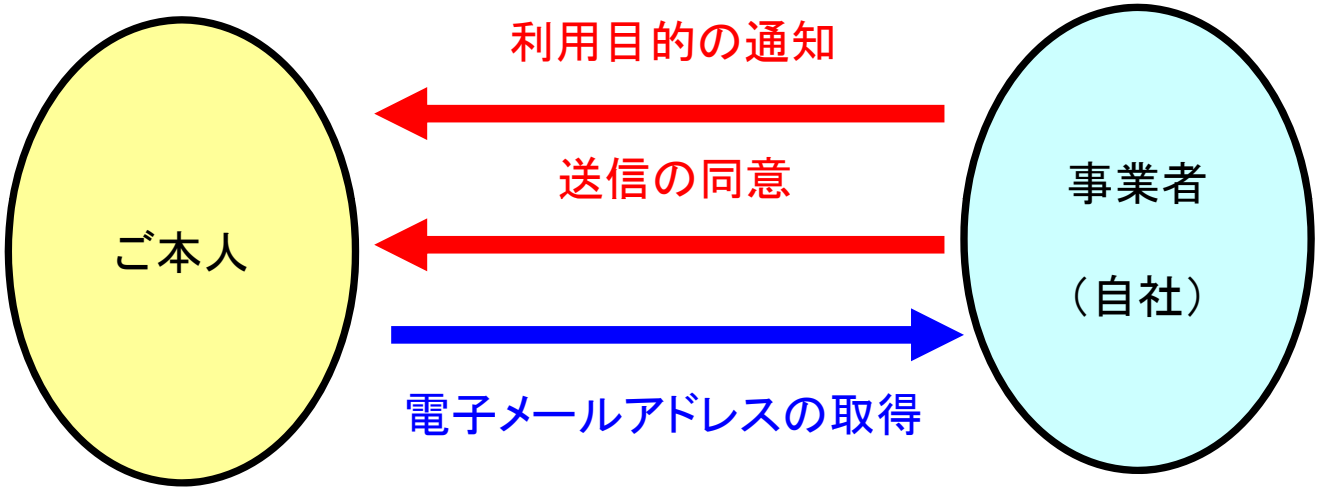


ご本人以外から取得する場合には、最初に取得する人が、事業者以外への第三者提供の同意を得る必要があります。
第三者提供の同意を得ていないものを取得すると、提供を受けた者は不正入手という違法になります。
イベントやセミナーの共催であっても、例外ではありません。
<u>名簿業者も同様です。</u>

個人情報保護対策
「電子メール送信の同意」

特電法（迷惑メール防止法）による義務

電子メールを送信する場合には、予め同意を得なければなりません。

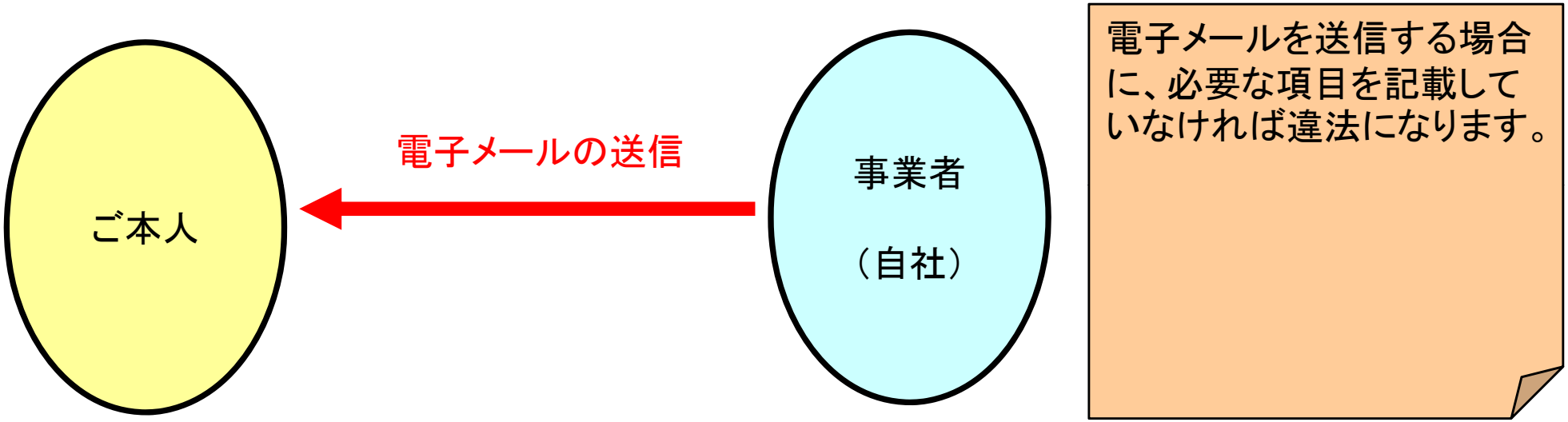


ご本人から電子メール送信の同意を予め得ずに、電子メールを送信すると違法になります。
実際には、「特定電子メール（≒広告宣伝メール）」に該当する内容の電子メール送信だけが対象です。

個人情報保護対策
「電子メール送信時の記載項目」

特電法（迷惑メール防止法）による義務

電子メールを送信する場合には、必要な項目を記載して送信しなければなりません。



必要事項：
a) 送信責任者の氏名・名称
b) オプトアウト手順（連絡先メールアドレスやウェブページのURLなど）
c) オプトアウトができることの説明
d) 送信責任者の住所
e) 問い合わせ先（電話番号、メールアドレスなど何らか）

http://yoshihiro.cocolog-nifty.com/postit/2008/11/post-1186.html

同意を得る／利用を断られる
オプトイン／オプトアウト

オプトアウト（利用停止）

個人情報の利用を断られたことにより、利用しない又は利用を停止する

オプトイン（同意原則）同意を得るための2つの方式

明示方式：何かの動作によって同意をしてもらう方式

→動作を確認できなければ、不同意として扱う

例：同意するなら　□　を塗りつぶしてください。

暗黙方式：何の動作もなく同意をしてもらう方式

→何も動作していなくても、同意とみなす

例：同意しないなら　□　を塗りつぶしてください。

例：選択してください。■同意する　　□同意しない

個人情報と同意状態の管理

例：

連絡手段で区別

- 電子メール（同意必要）
- ＦＡＸ
- 電話
- 郵便

状態値

- Ｙes（同意）
- Ｎo（不同意）
- Ｕnkown（未確認）
- Ｉsolate（利用禁止）

ID	電子メール	FAX	電話	郵便	氏名	連絡先
1	Y	Y	Y	Y	佐藤	・・・
2	Y	U	N	U	鈴木	・・・
3	Y	N	N	N	田中	・・・
4	I	I	I	I	伊東	・・・

検討事項：

●部署ごとの管理の場合、部署間連携方法

●お問い合わせ時の本人確認手段

同意（＝オプトイン：Opt-in）取得率の向上

お客様に同意をしていただきやすい文章で取得する必要がある。

「HPからの製品案内をお送りしてもよろしいでしょうか？」

「HPからのプリンター製品に関する案内をお送りしてもよろしいでしょうか？」

「HPからのプリンター製品に関する案内を1ヶ月間に最大1回お送りしてもよろしいでしょうか？」

目的や頻度を限定すれば、同意取得率は向上する場合がある。

目的が広ければ、色々な目的に使えるが、同意取得率が低下する場合がある。

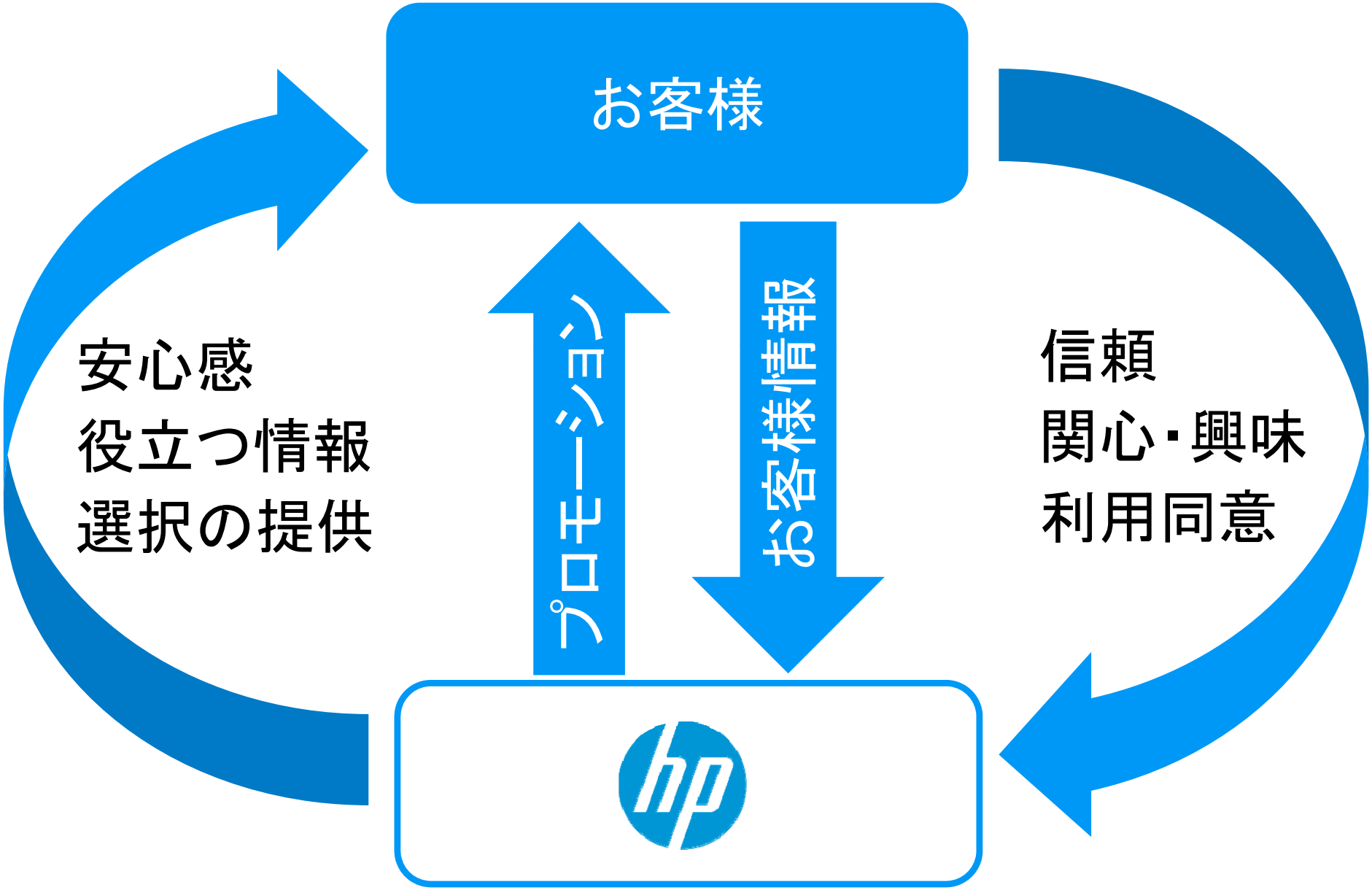
個人情報保護でのポイント
～顧客に提供する情報の品質改善～

合法であっても問い合わせは来る
→問い合わせにて、合法を納得させられなければ、苦情になる
→問い合わせを軽減するために、対策や説明、同意の有無をわかりやすくする

数撃てば当たる的な販売促進活動は自滅する
→利用停止要求を軽減するために、提供する情報の品質を改善し、継続して情報提供して欲しいと思われる情報の発信をする

参考：
拙稿「法律から始めない個人情報保護対策」
科学技術振興機構発行
情報管理　2006年8月号 (VOL.49 NO.5)
http://www.jstage.jst.go.jp/article/johokanri/49/5/49_225/_article/-char/ja/

個人情報保護でのポイント

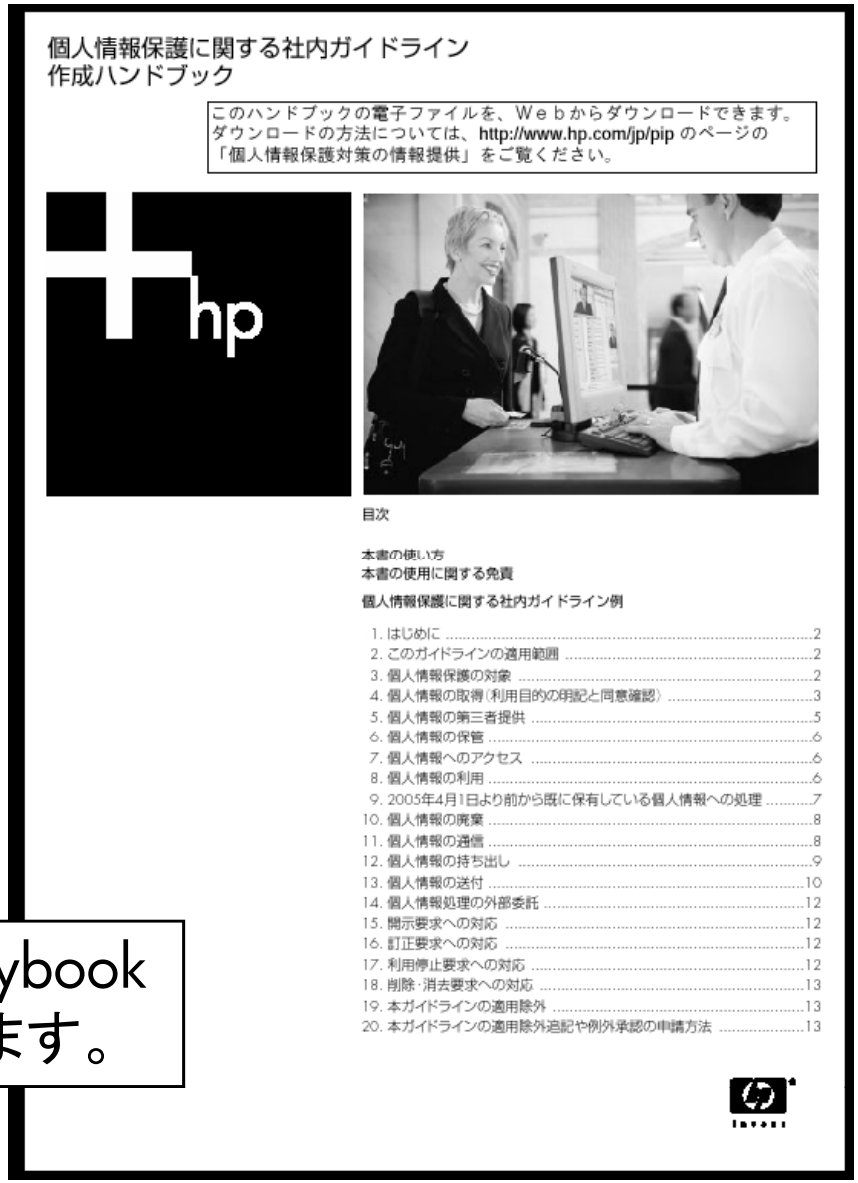


個人情報保護でのポイント

お客様情報をいただくとき
　利用目的の記載
　利用同意の取得
　共催等の他社と連携するときには特に注意

お客様情報を使うとき
　利用停止の対象者ではないことの事前確認
　　※部署単位だけでなく全社での確認も必要
　利用停止したいと思われない連絡方法と内容
　　基本は、マナーの再確認、安心感に留意
　利用停止する準備
　　※部署単位だけでなく全社での停止にも備える

参考：日本ヒューレット・パッカード
個人情報保護に関する社内ガイドライン



個人情報保護に関する社内ガイドライン
作成ハンドブック

このハンドブックの電子ファイルを、Ｗｅｂからダウンロードできます。
ダウンロードの方法については、http://www.hp.com/jp/pip のページの
「個人情報保護対策の情報提供」をご覧ください。

目次

本書の使い方
本書の使用に関する免責
個人情報保護に関する社内ガイドライン例

1. はじめに 2
2. このガイドラインの適用範囲 2
3. 個人情報保護の対象 2
4. 個人情報の取得（利用目的の明記と同意確認） 3
5. 個人情報の第三者提供 5
6. 個人情報の保管 6
7. 個人情報へのアクセス 6
8. 個人情報の利用 6
9. 2005年4月1日より前から既に保有している個人情報への処理 7
10. 個人情報の廃棄 8
11. 個人情報の通信 8
12. 個人情報の持ち出し 9
13. 個人情報の送付 10
14. 個人情報処理の外部委託 12
15. 開示要求への対応 12
16. 訂正要求への対応 12
17. 利用停止要求への対応 12
18. 削除・消去要求への対応 13
19. 本ガイドラインの適用除外 13
20. 本ガイドラインの適用除外追記や例外承認の申請方法 13

http://yosihiro.com/go/hp/privacybook
からPDFファイルをダウンロードできます。

個人情報保護対策 「法律による主な義務」

個人情報保護法
- 利用目的の通知
- 利用目的の範囲内での利用
- ご要望（開示、訂正、利用停止等）に応じる
- 第三者提供する場合の同意取得
- 情報の安全管理

特電法（特定電子メールの送信の適正化等に関する法律）
（通称、迷惑メール防止法）
- 電子メール送信の同意取得
- 電子メール送信時の特定項目の記載

個人情報保護法第20条
安全管理措置 と ガイドライン

経済産業省ガイドライン

・個人情報取扱事業者は、その取り扱う個人データの漏洩、滅失又は毀損の防止その他の個人データの安全管理のため、組織的安全管理措置、人的安全管理措置、物理的安全管理措置、及び技術的な安全管理措置を講じなければならない。

組織的 安全管理措置	人的 安全管理措置	物理的 安全管理措置	技術的 安全管理措置

経済産業省
個人情報保護法ガイドライン 第20条

（安全管理措置）

●組織的安全管理措置

　情報のライフサイクル（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄）

●人的安全管理措置

　教育

●物理的安全管理措置

●技術的安全管理措置

　5A（ Authentication, Access Control, Administration, Auditing, Assurance)

経済産業省ガイドライン：
個人情報のライフサイクルに沿った安全管理措置

①個人情報の取得・入力
利用目的・情報移転の了解を事前に得る
必要最低限の取得→使用予定のないものは取得しない
②個人情報の移送・送信
宛先間違え、遺失、盗聴などの予防や防止、被害の軽減対策など
③個人情報の利用・加工
利用者の制限（無許可者からのアクセス防御）
最小情報、最小数量の利用制限（許可者の最小権限）
取扱い手順の明確化（許可者の注意義務）
情報格付けの継承、ｼｽﾃﾑ要件の継承
④個人情報の保管・バックアップ
情報漏洩・書き換えの防御
情報格付け、ｼｽﾃﾑ格付け：所在の管理、視認性の確保
⑤個人情報の消去・廃棄
廃棄手順の明確化（電子化前後の廃棄手順を含む）

経済産業省
個人情報保護法ガイドライン 第20条

（安全管理措置）

●組織的安全管理措置

　情報のライフサイクル（取得・入力、移送・送信、利用・加工、保管・バックアップ、消去・廃棄）

●人的安全管理措置

　教育

●物理的安全管理措置

●技術的安全管理措置

　5A（ Authentication, Access Control, Administration, Auditing, Assurance)

経済産業省
個人情報保護法ガイドライン 第20条

56ページにわたり、具体的な指針が書かれているが、特に20条　安全管理措置については、11ページを割いて詳述している。

20条のガイドライン（抜粋）

1. 組織的措置
2. 人的措置
3. 物理的措置
4. 技術的措置：
    1. 個人データへのアクセスにおける識別と認証
    2. 個人データへのアクセス制御
    3. 個人データへのアクセス権限の管理
    4. 個人データのアクセスの記録
    5. 個人データを取り扱う情報システムに対する不正ソフトウェア対策
    6. 個人データの移送・通信時の対策
    7. 個人データを取り扱う情報システムの動作確認時の対策
    8. 個人データを取り扱う情報システムの監視

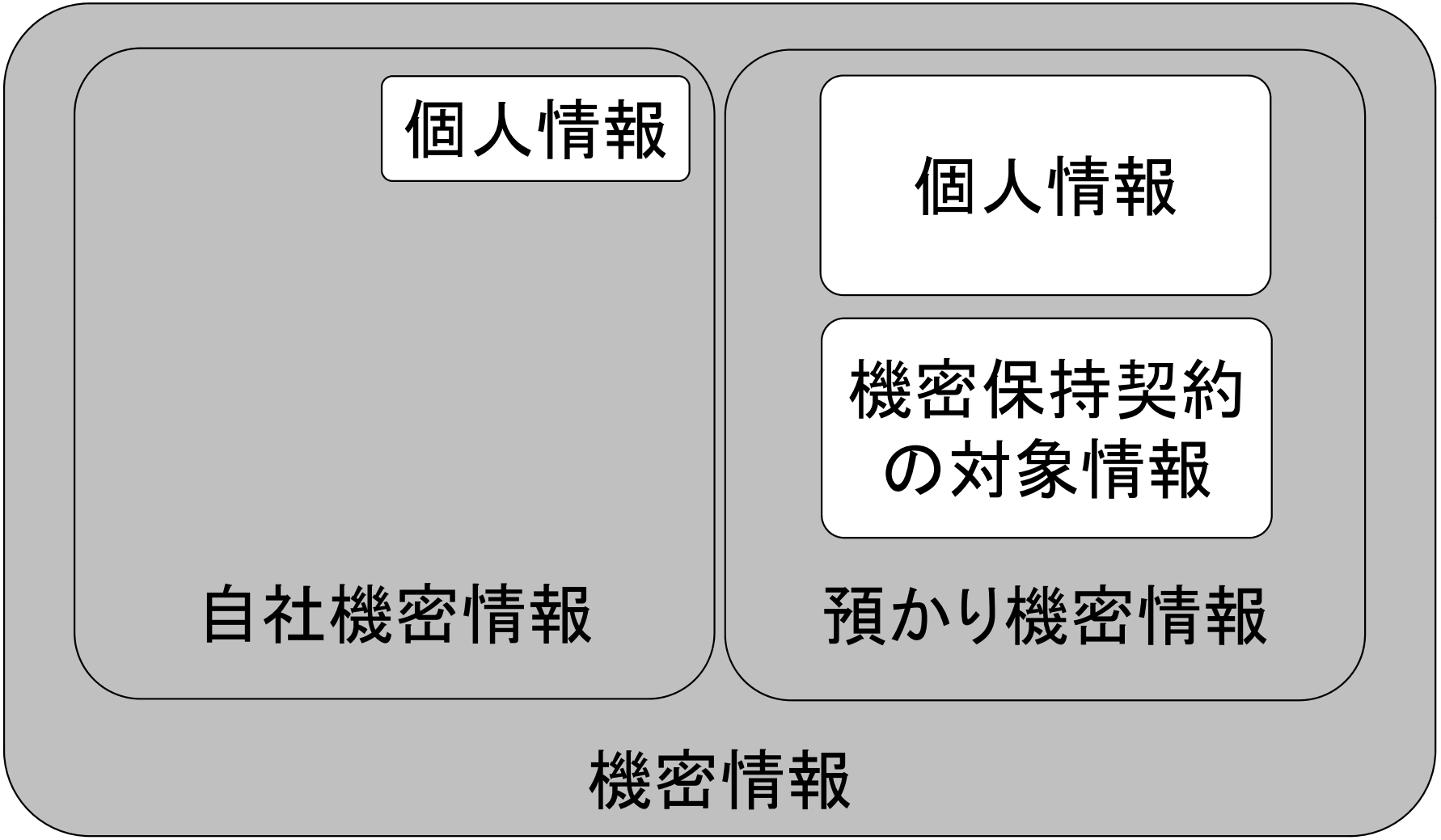
経済産業省
個人情報保護法ガイドライン 第20条

http://yosihiro.com/infosec/index.html#security_architecture

- つぎはぎシステムを防ぐ
  セキュリティアーキテクチャ
- 5A (Authentication, Access Control, Administration, Auditing, Assurance)

個人情報の安全管理措置

個人情報と機密情報の関係



情報管理の不徹底の顕在化

新たな脅威が登場したわけではない

- 機密情報管理が徹底していなかった。
- 個人情報の流出や紛失等でそのことが顕在化した。

- 管理が不十分であったとは言い切れないが、不徹底が潜在的にあった。

- 情報に対する価値観や環境の変化。
- 現代の企業は、変化に対応することで安定する必要がある。（変化しないことが安定ではない）

参考：営業秘密　～営業秘密を守り活用する～

経済産業省 http://www.meti.go.jp/

不正競争防止法

営業秘密管理指針

–参考資料1：営業秘密管理チェックシート

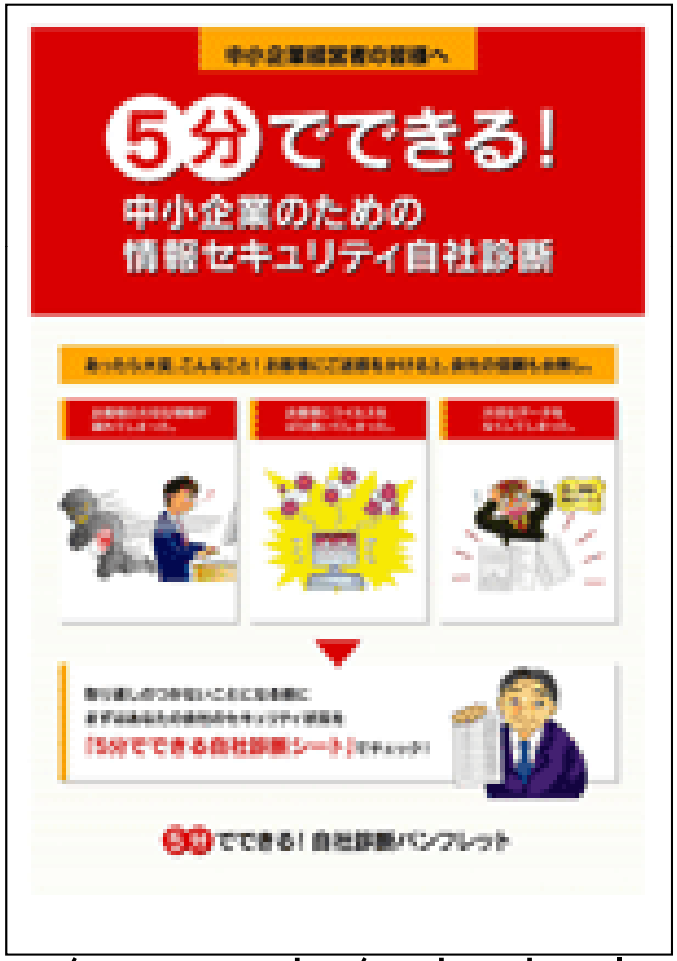
トップページ > 政策別に探す > 経済産業 > 知的財産の適切な保護 >
知的財産政策／不正競争防止 > 営業秘密
http://www.meti.go.jp/policy/economy/chizai/chiteki/trade-secret.html

参考：中小企業向け情報セキュリティ対策

IPA（情報処理推進機構）http://www.ipa.go.jp/

－5分でできる！ 自社診断パンフレット

－5分でできる！ 自社診断シート



http://www.ipa.go.jp/security/manager/know/sme-guide/index.html

個人情報保護法　独立行政法人等

独立行政法人等保有する個人情報の適切な管理のための措置に関する指針について（行政管理局長通知）
http://www.soumu.go.jp/main_sosiki/gyoukan/kanri/040914_2.html

政府機関情報セキュリティ対策統一基準

内閣官房情報セキュリティセンター
政府機関情報セキュリティ対策統一基準

http://www.nisc.go.jp/active/general/kijun01.html

抜粋

「政府機関の情報セキュリティ対策のための統一基準」について

2006年8月2日

内閣官房情報セキュリティセンター
NISC (National Information Security Center)
http://www.nisc.go.jp/

目次

1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

統一基準とは

統一基準ができる前・・・
「政府機関における情報セキュリティ対策はどのようになっていますか？」というお問い合わせをいただいた際には、
「各政府機関により対策内容が異なります。」という対応をしていました。

統一基準によって・・・
「各政府機関では統一基準に沿って情報セキュリティ対策基準を定めています。取り扱う情報等により、それ以上の対策基準を定めている機関もあります。」
と回答できるようになりました。

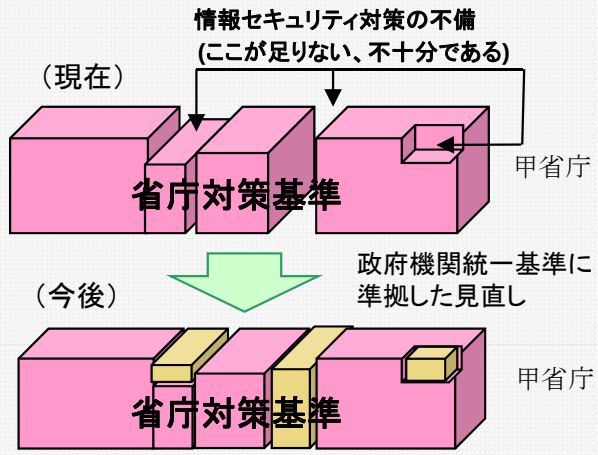
政府機関統一基準の策定の目的

● 世界最先端のIT(情報技術)国家にふさわしい情報セキュリティ水準を目指して、統一基準を運用

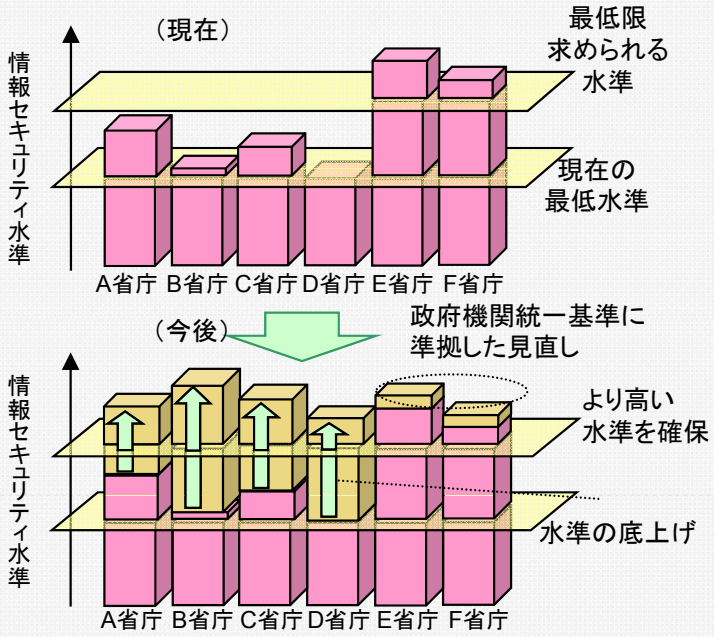
各府省庁の現状	政府機関統一基準による運用	
各省庁基準はバラバラ	統一化整合化	バラバラ解消 ① 各府省庁でバラバラな情報セキュリティ対策を統一 → 政府機関の情報セキュリティ対策水準を向上させるフレームワーク(政府基本方針、運用指針)を情報セキュリティ政策会議で決定(9月)
各省庁基準は穴空き	具体的な対策提示	穴が埋まる ② 各府省庁に具体的な対策を適用しやすい形で提示 → 具体的な実施手順を作成する際に参照すべきマニュアル等を今後多数作成(重要なものは年内目途)
本質的原因 専門的人材不足	人材不足補完効果 一石三鳥	迅速・的確 ③ 技術、環境の変化に伴う情報セキュリティ対策の要求水準の高度化にも迅速・的確に対応

各府省庁の対策の統一化・整合化と水準の向上

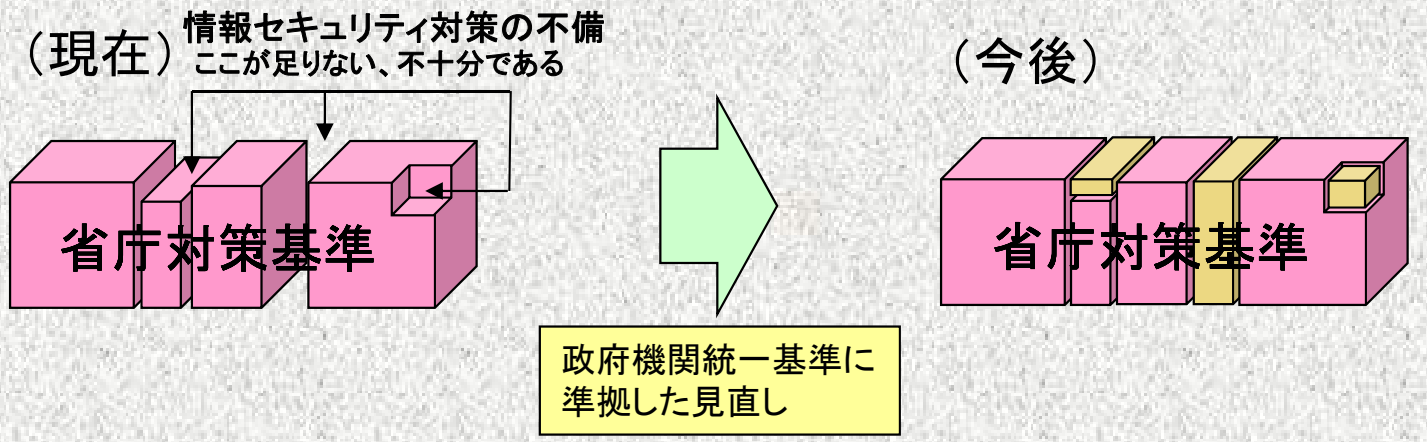
① 政府機関統一基準による省庁対策基準の補完



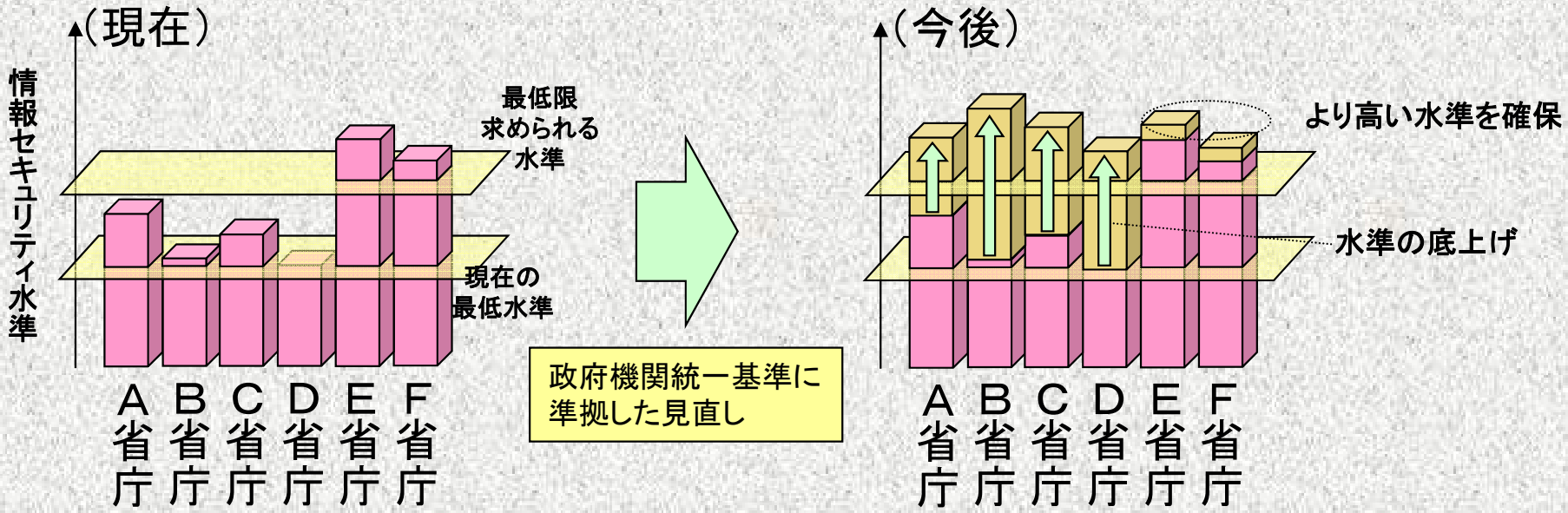
② 各府省庁の情報セキュリティ水準の向上



① 政府機関統一基準による省庁対策基準の補完



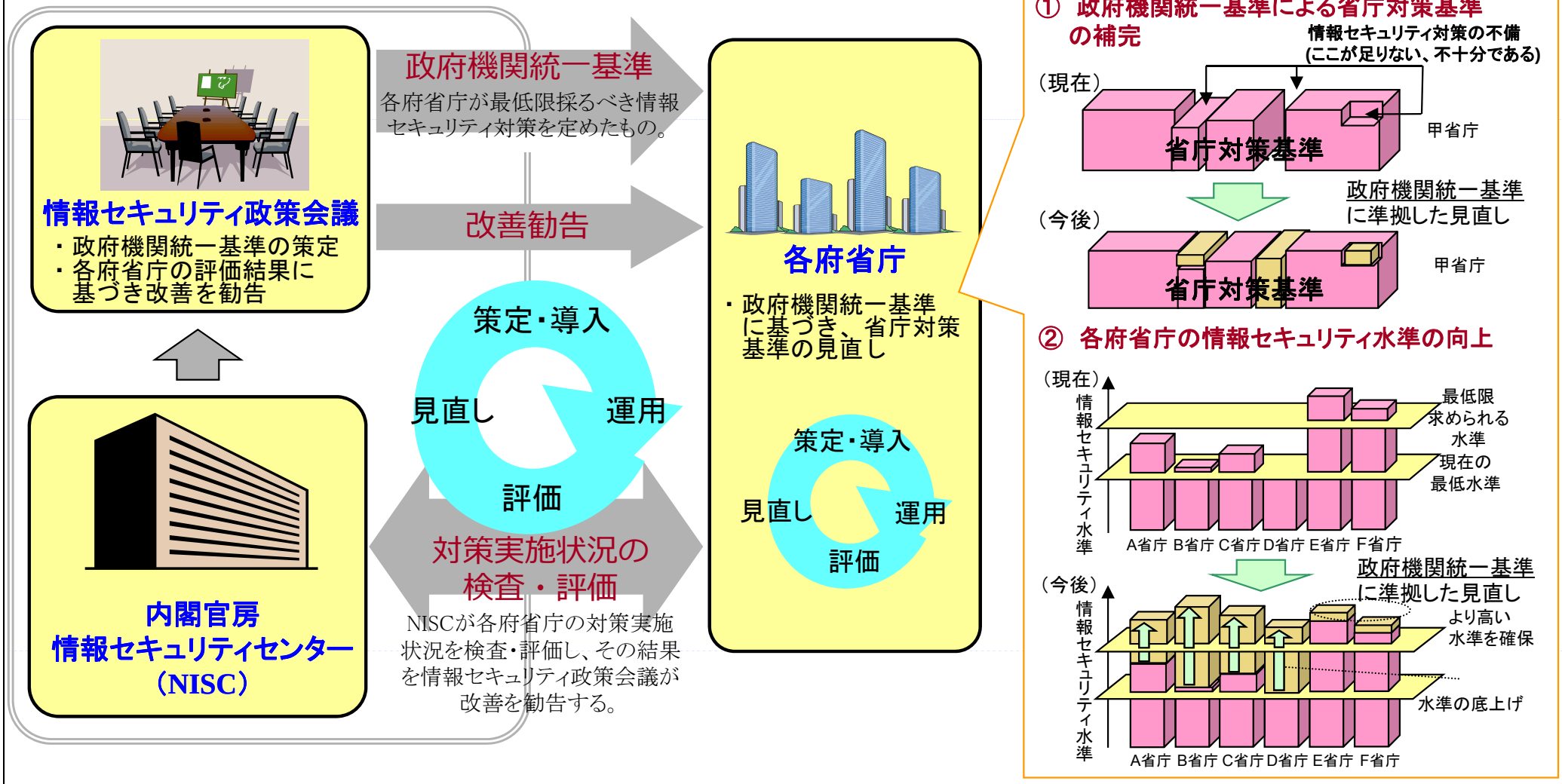
② 各府省庁の情報セキュリティ水準の向上



個別設計図としての「政府機関統一基準」

○**政府機関全体としての情報セキュリティ水準の向上を図る**ための「個別設計図」として、**「政府機関の情報セキュリティ対策のための統一基準」**を策定。

○各政府機関は本基準を踏まえて対策を実施し、**内閣官房情報セキュリティセンター（NISC）が対策実施状況を検査・評価**。その結果に基づき、**情報セキュリティ政策会議が改善を勧告**。

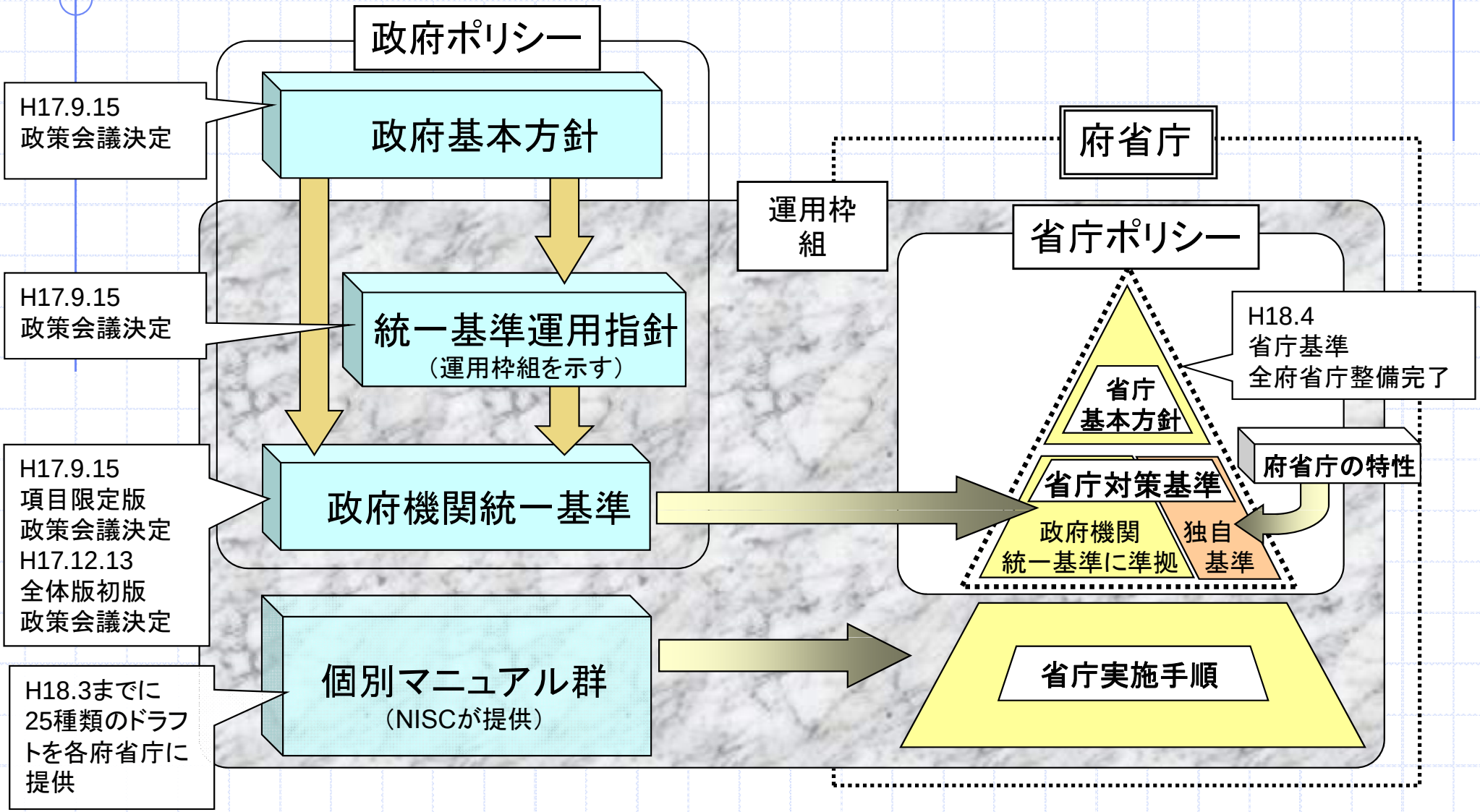


目次

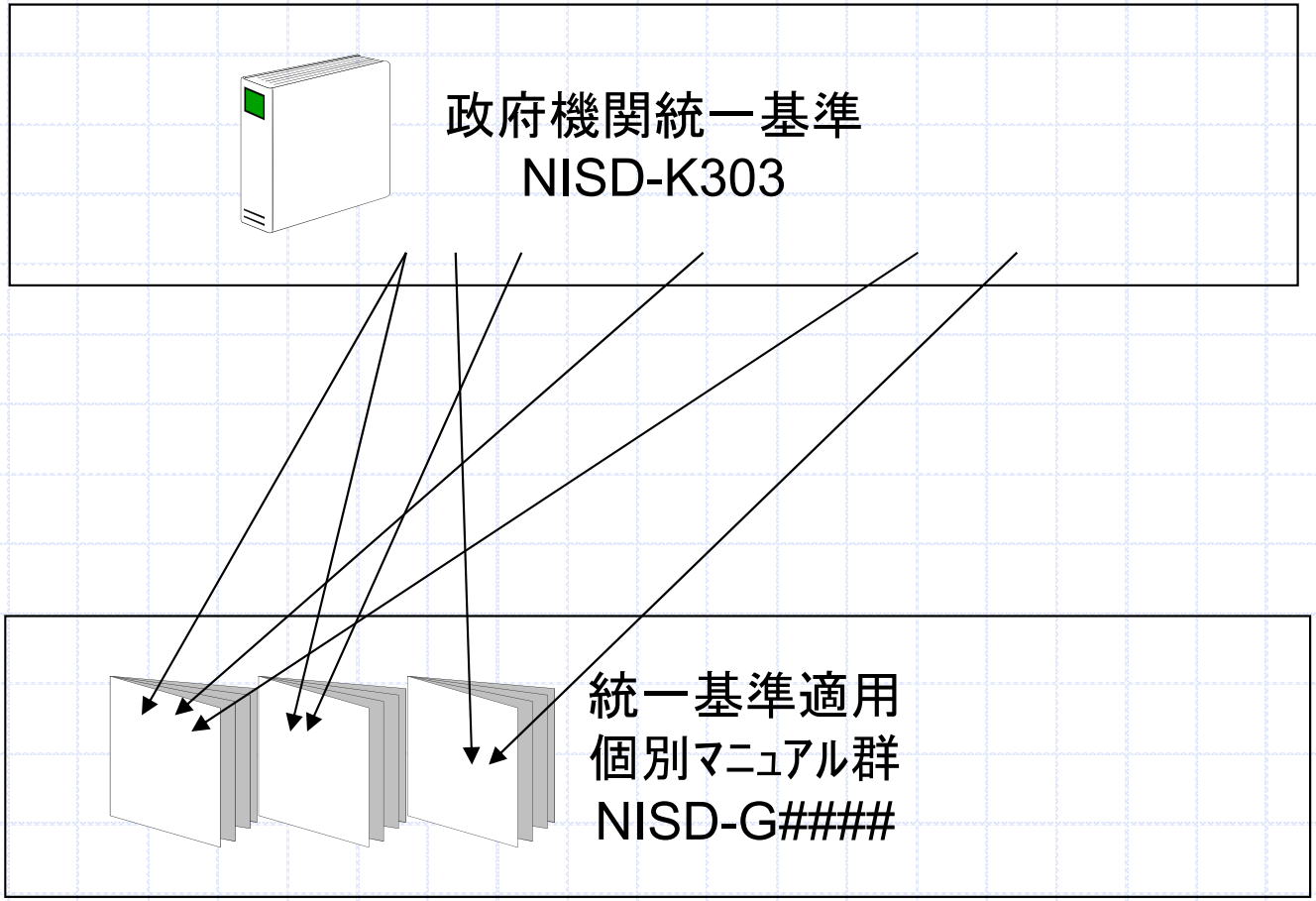
1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

統一基準

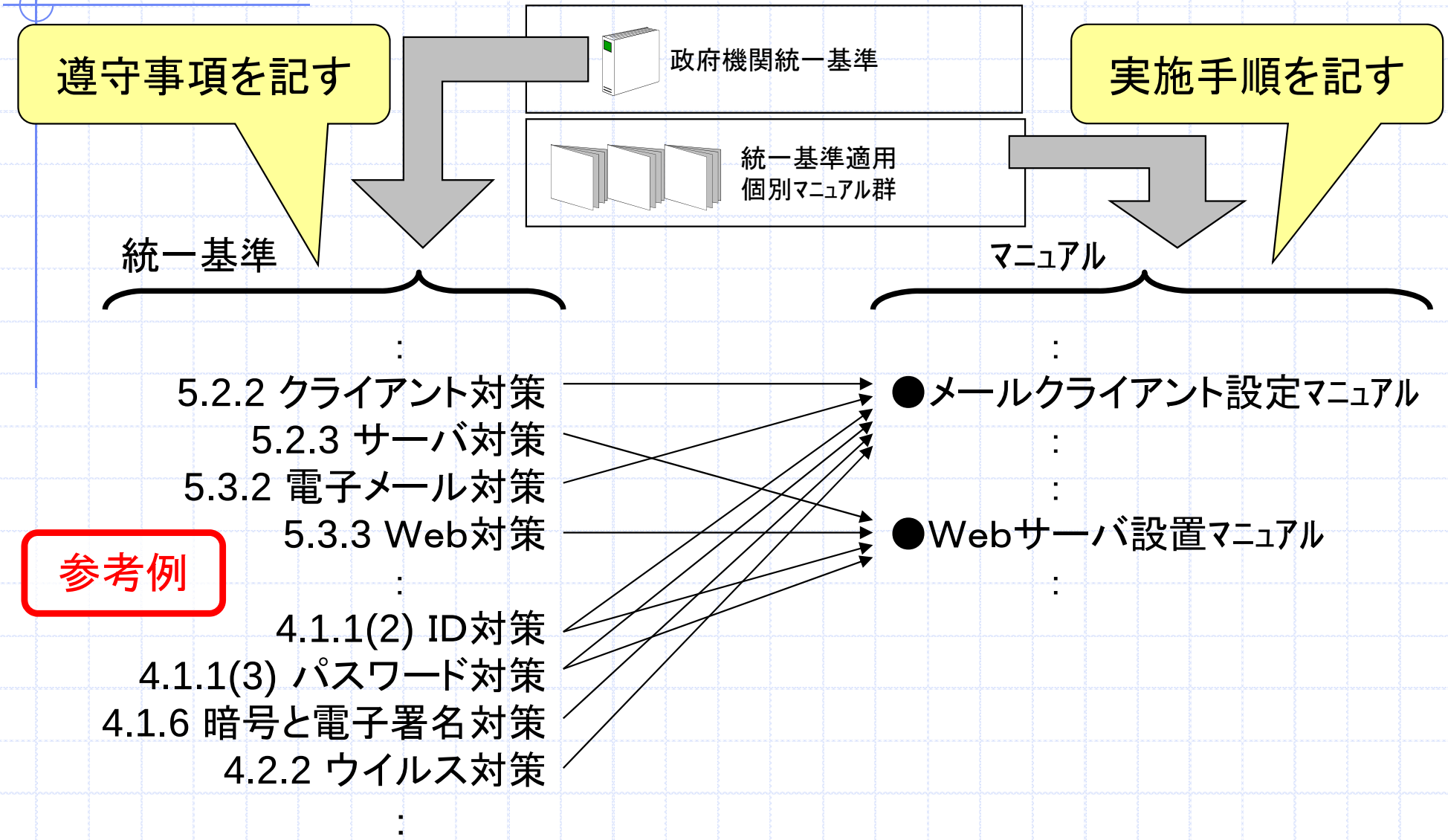
第1部　総則
1.1.1 本統一基準の位置づけ



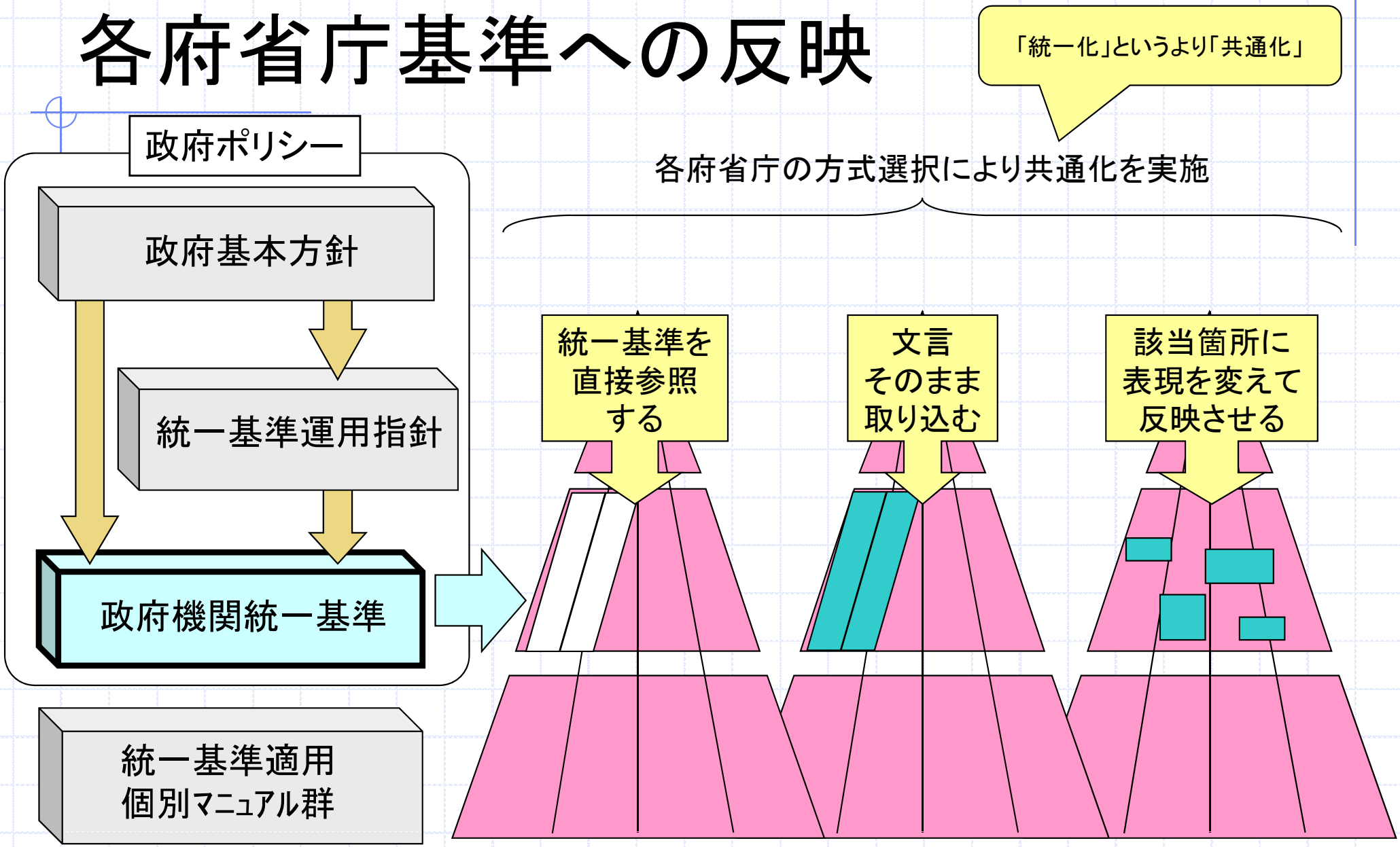
政府機関統一基準と個別マニュアルの関係



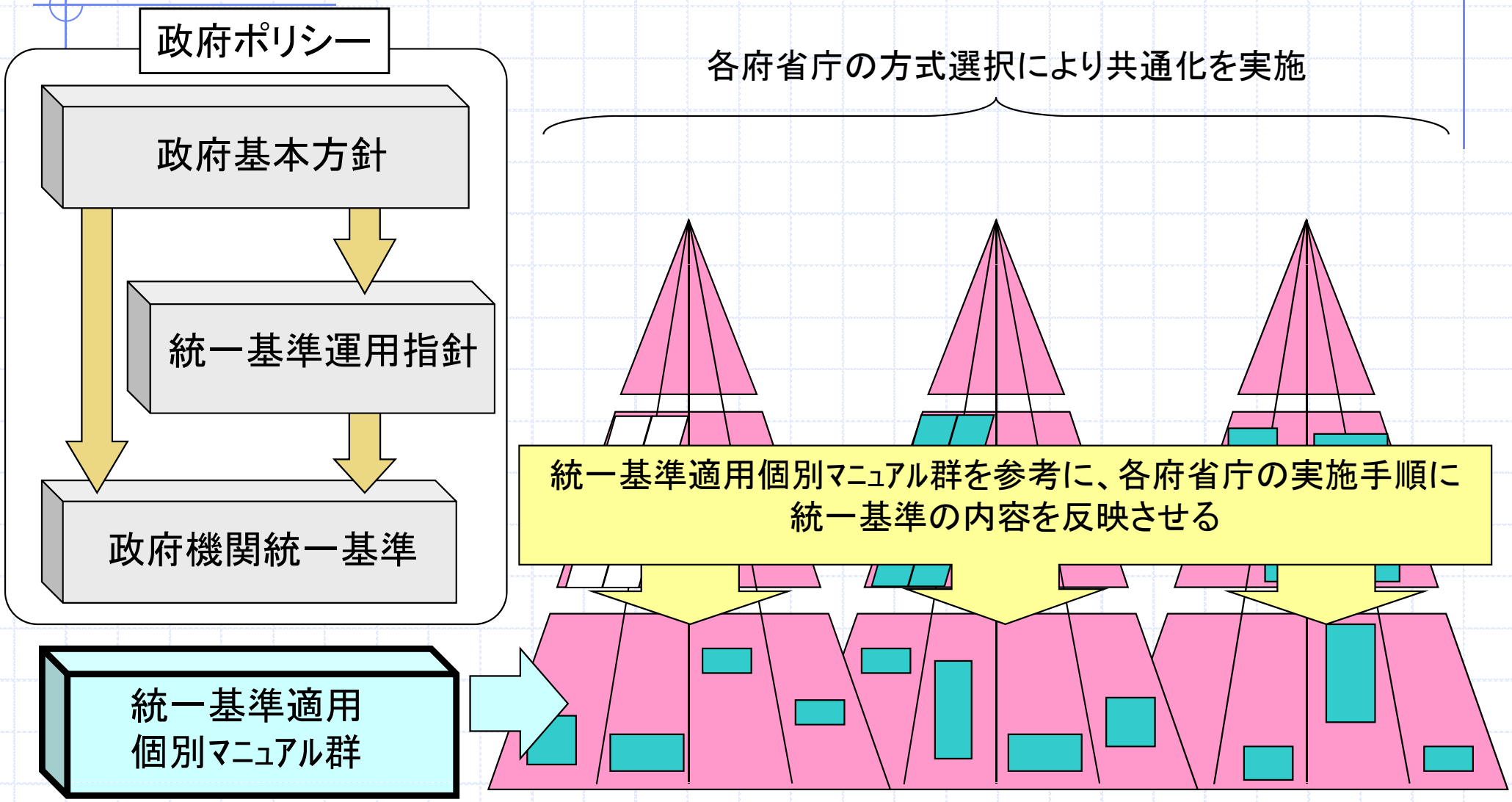
政府機関統一基準と個別マニュアルの関係



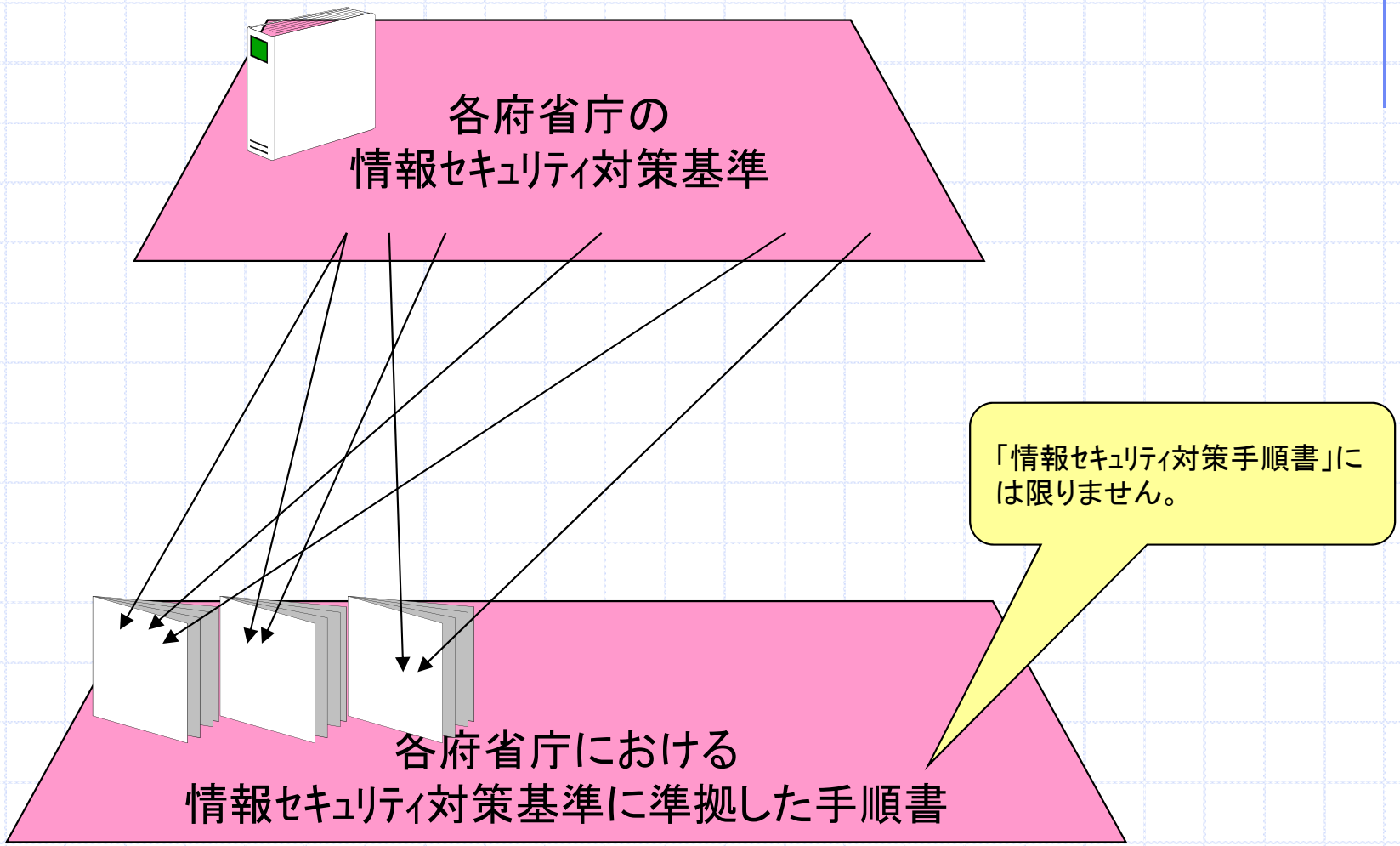
政府機関統一基準
各府省庁基準への反映



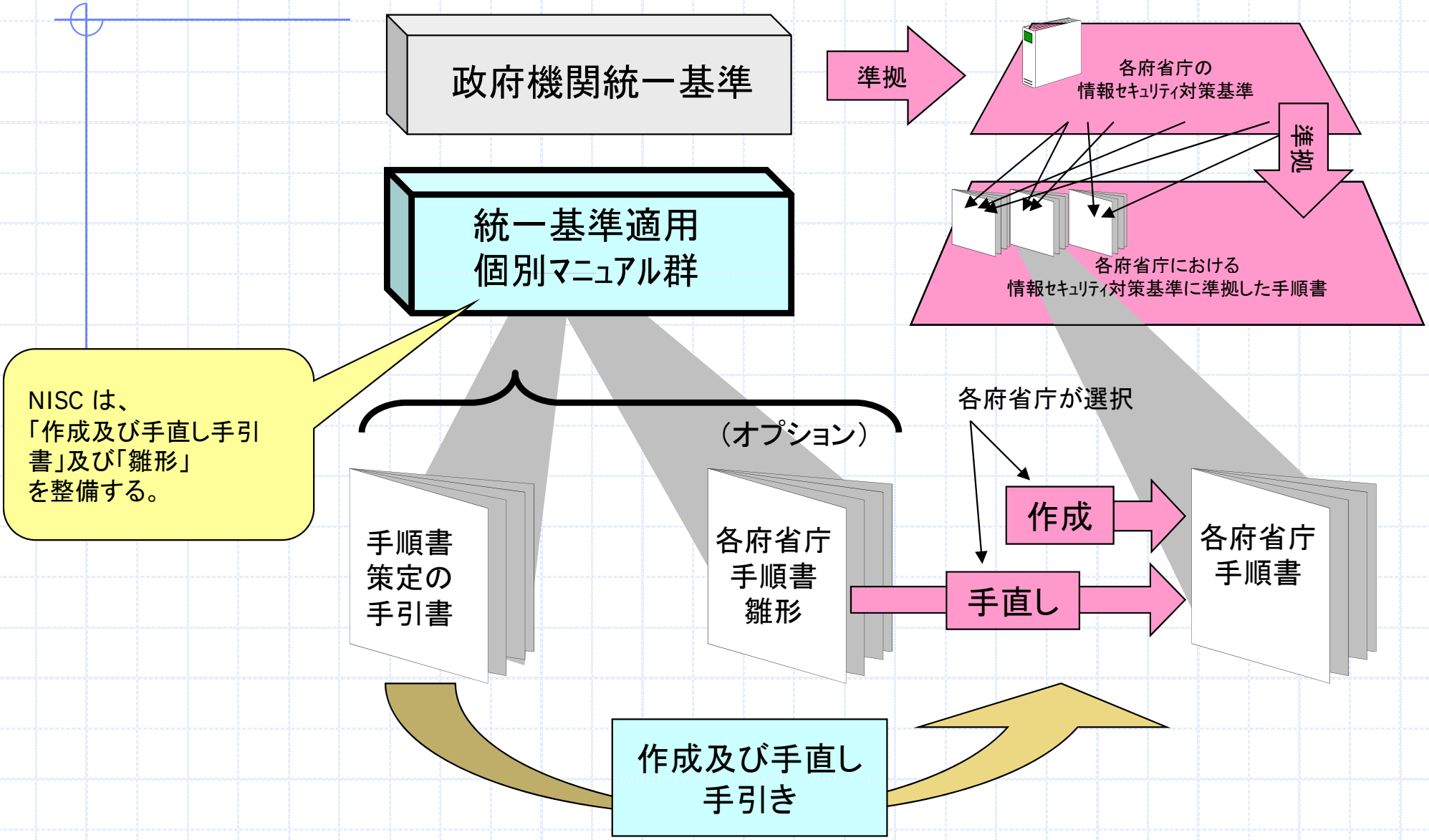
政府機関統一基準
各府省庁実施手順への反映



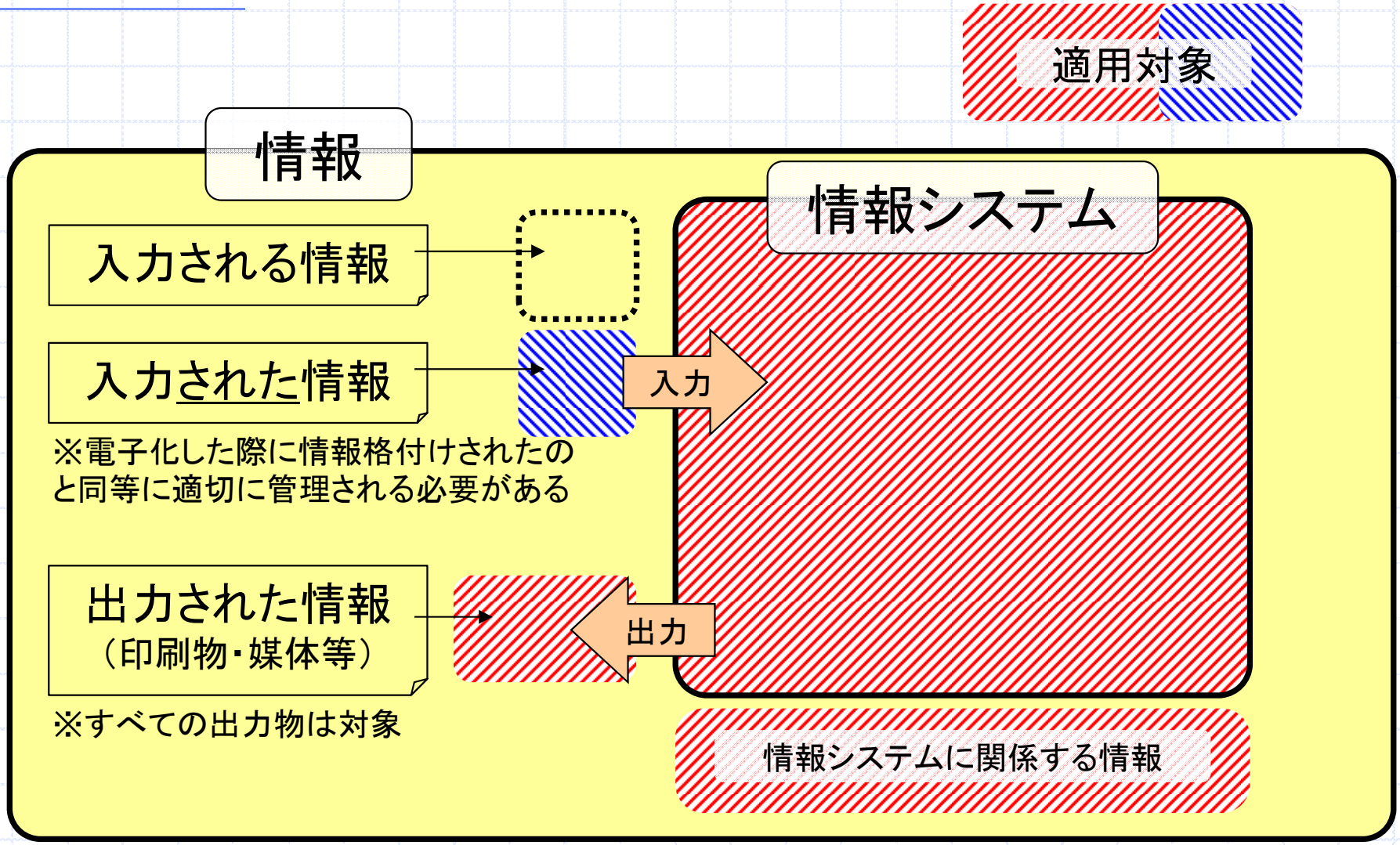
各府省庁における情報セキュリティ対策基準とそれに準拠した手順書



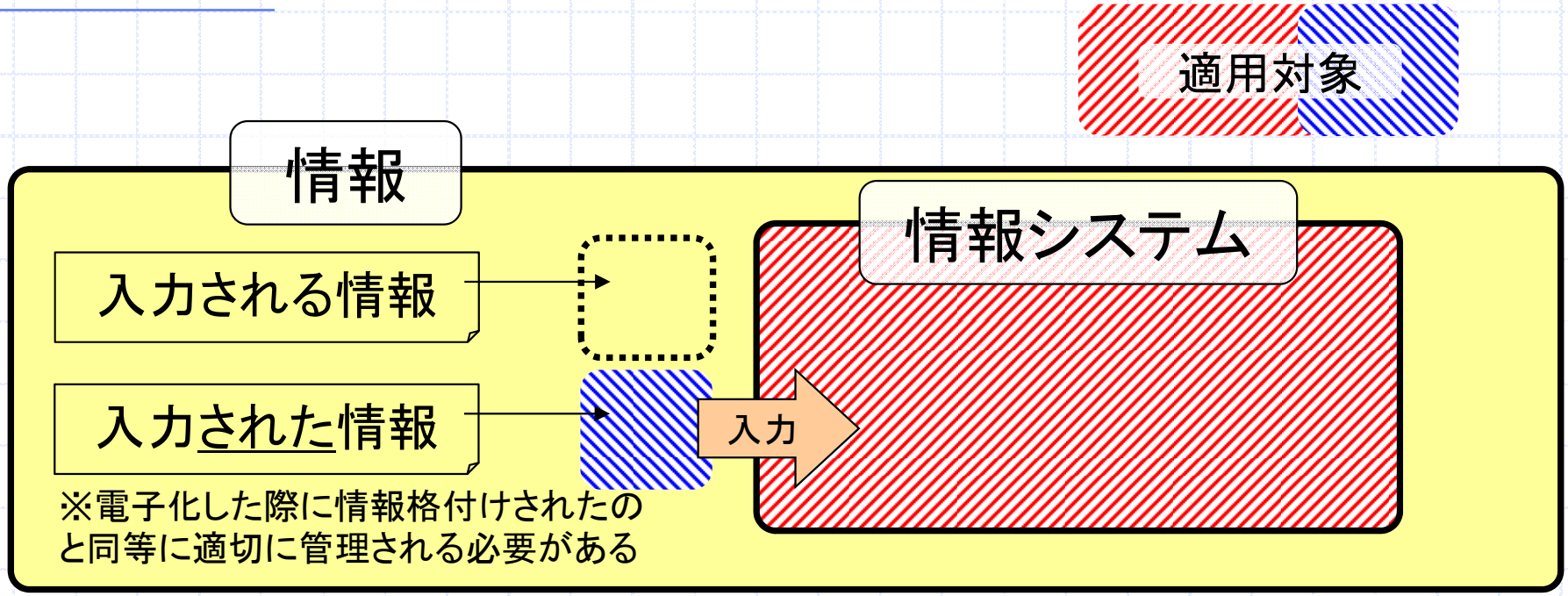
統一基準適用個別マニュアル群



政府機関統一基準の適用対象範囲



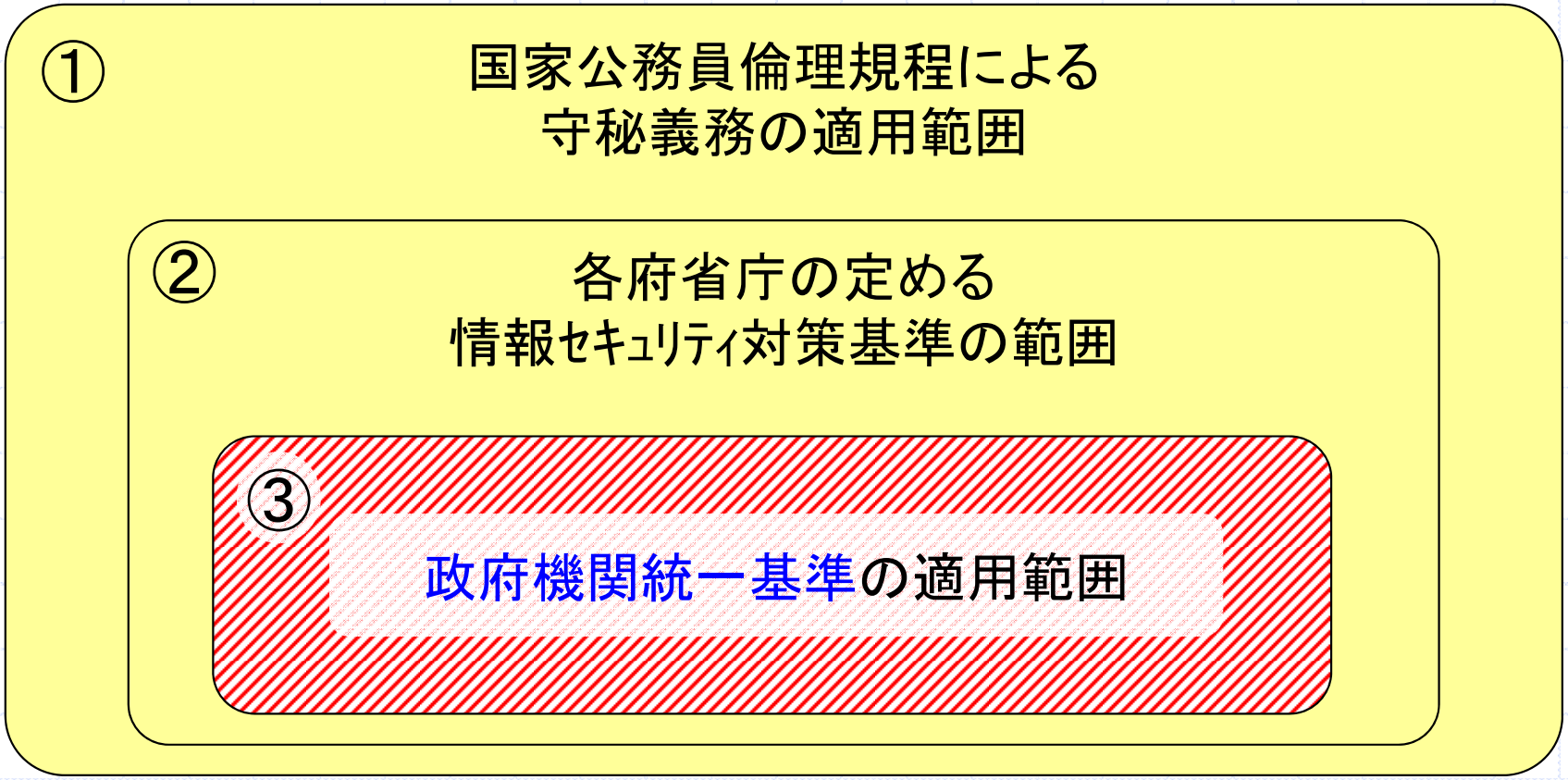
政府機関統一基準の適用対象範囲



情報システムに入力されるまでの情報は、すべて対象外。
情報システムに入力され、それが情報格付けされた時点を以って、その情報は、情報ｾｷｭﾘﾃｨ対策基準の定めと同等の安全管理措置が講じられる必要がある。
紙などの非電子の情報については、本統一基準とは別途の規程等により、適切に管理される必要があるが、それについては、本基準の定めるところではない。
情報システムに入力するまで安全管理措置が講じられていなかった情報が、入力の際の格付けによって管理が必要になる場合、それは本基準が追加の管理要件を求めているのではなく、本来必要であったことが、本基準により明確になっただけだと考えられる。

政府機関統一基準の適用対象範囲

本統一基準だけで、すべての情報セキュリティ対策を網羅するのではない。



統一基準

第1部　総則
1.1.2 本統一基準の使い方

（3）全体構成 『部、節及び項の3つの階層によって構成される。』

第 X 部

X.Y 節

X.Y.Z 項

趣旨（必要性）

～～趣旨説明文～～

遵守事項

(1)

(a)　～～遵守事項本文～～

解説：　～～(a) の解説文～～

(b)　～～遵守事項本文～～

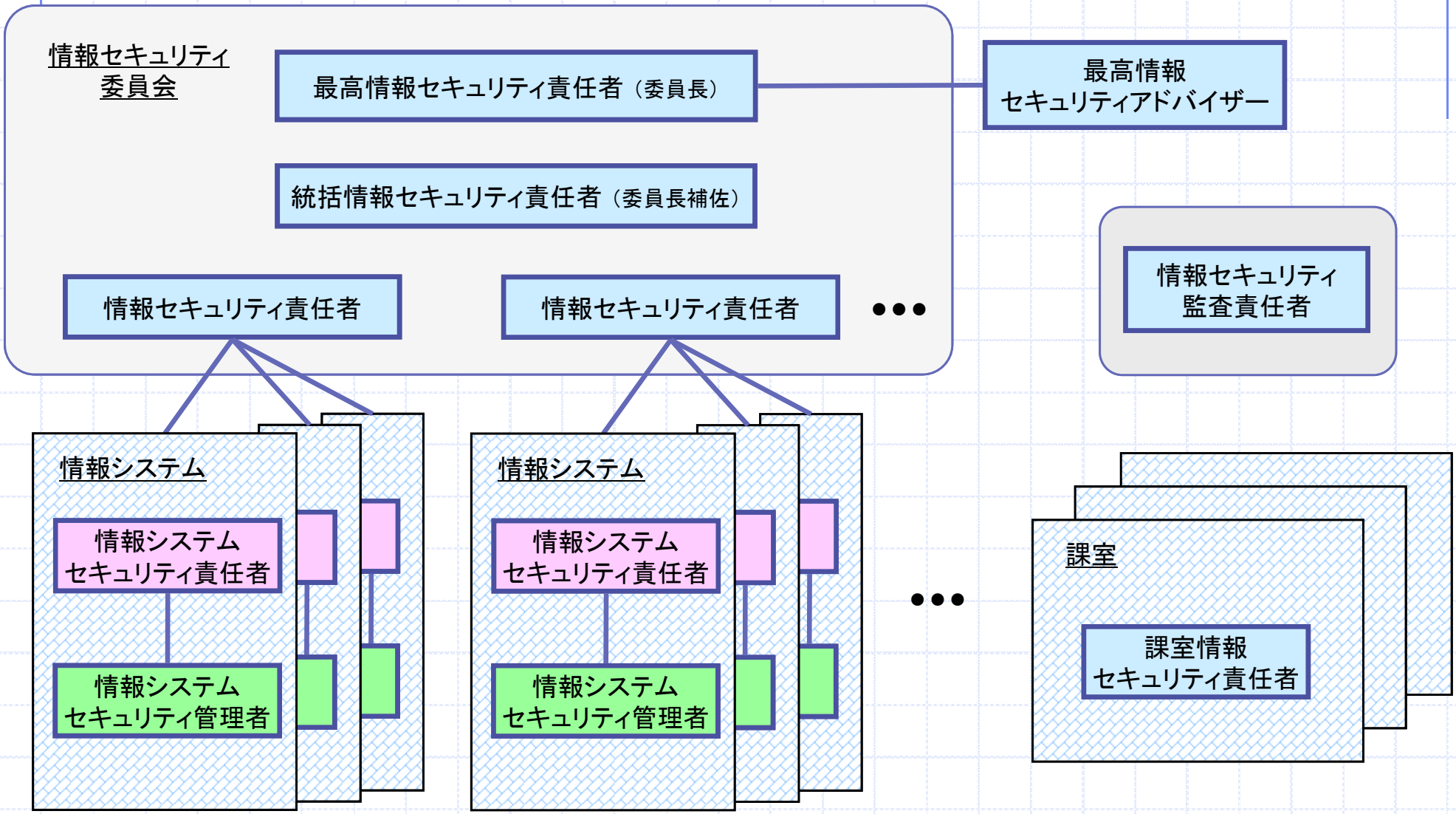
解説：　～～(b) の解説文～～

(2)

解説文は
「統一基準解説書」
にだけ記載

統一基準

統一基準解説資料　別添資料
A.1.1 組織・体制イメージ図



統一基準

第2部　組織と体制の構築
2.1 導入

2.1.3 違反と例外措置

（2）例外措置

『 (f)　最高情報セキュリティ責任者は、例外措置の適用審査記録の台帳を整備し、例外措置の適用審査記録の参照について、情報セキュリティ監査を実施する者からの求めに応ずること。』

★府省庁における、すべての例外措置について、随時回答できる状態にしておく必要があります。

統一基準

第2部　組織と体制の構築
2.2 運用

2.2.1 情報セキュリティ対策の教育

★啓発＜教育＜訓練

★毎年度最低1回 ＆ 着任時3ヶ月以内の受講
　人は現在の自分の立場で理解するため、同じ内容であっても受講済み教育の再受講が効果的である。

★受講状況の管理

★未受講者への受講勧告

★受講状況の組織としての把握

★受講義務の明示（本人の責任）

★受講支援（上司の義務）

◎基本的な遵守事項を実践することも大切

統一基準

第2部　組織と体制の構築
2.2 運用

2.2.2 事故及び障害の対応

★事前準備＝体制、報告手順、対応手順、緊急連絡網の整備
（強化事項：府省庁外からの通報も想定）

★事前準備に基づく、計画内対応と計画外対応

★One stop & Non-stop
＝ 窓口設置 & 無期限待機防止

★原因調査、再発防止策立案と実施支援

◎準備した内容を周知することは大切

統一基準

第2部　組織と体制の構築

2.3 評価

2.3.1 情報セキュリティ対策の自己点検

2.3.2 情報セキュリティの監査

後で詳しく説明します。

統一基準

第2部　組織と体制の構築

2.4 見直し

2.4.1 情報セキュリティ対策の見直し

『 (a) 情報セキュリティ関係規程を整備した者は、各規定の見直しを行う必要性の有無を適時検討し、必要があると認めた場合にはその見直しを行うこと。』

『 (b) 行政事務従事者は、自らが実施した情報セキュリティ対策に関連する事項に課題及び問題点が認められる場合には、当該事項の見直しを行うこと。』

統一基準

第3部　情報についての対策
3.1.1 情報の格付け

『

(a) 情報セキュリティ委員会は、行政事務で取り扱う情報について、機密性、完全性及び可用性の観点による当該情報の格付け及び取扱制限の基準並びに格付け及び取扱制限を明示する手順を整備すること。

』

「重要度」のような単一観点ではなく、三つの観点を区別して対策を講じる。

① 機密性、完全性、可用性の3つの観点

② 「格付け」の基準

③ 「取扱制限」の基準

次のスライドで紹介

④ 「格付け」及び「取扱制限」を明示する手順

3.2.1 で紹介

すべての行政事務従事者は、各府省庁の定めた、これらの「基準」と「手順」により「格付け」と「明示」をしなければならない。

「格付け」と「取扱制限」（Classification と Marking）

格付け	分類基準	取扱制限

政府共通の指定
必須の指定
段階的な指定
格付けによって、本統一基準に含まれる遵守事項が選択されて対策内容が定まる。

各府省庁個別の指定
任意の指定
無段階の指定
取扱制限の指定によって、各府省庁が定める「取扱制限」基準により対策内容が決まる。

「格付け及び取扱制限」を指定するための判断を
誰が ← 指定判断者 （※統一基準において指定実施者は情報の作成・入手者）
どのように ← 判断基準、方法
実施するのかについてを、
各府省庁が「格付け及び取扱制限の基準」に含めて定める。

統一基準

統一基準解説資料　別添資料
A.1.2 情報の格付け一覧（1／3）

機密性による情報の格付け

格付け	分類基準	取扱制限
機密性3情報	秘密文書に相当する機密性を要する情報	例）　複製禁止 再配付禁止 暗号化必須
機密性2情報	秘密文書に相当する機密性は要しないが、直ちに一般に公表することを前提としていない情報	
機密性1情報	機密性2情報又は機密性3情報以外の情報	

統一基準

統一基準解説資料　別添資料
A.1.2 情報の格付け一覧（2／3）

完全性による情報の格付け

格付け	分類基準	取扱制限
完全性2情報	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確な遂行に支障（軽微なものを除く。）を及ぼすおそれがある情報	例） ○年○月○日まで保存
完全性1情報	完全性2情報以外の情報	

統一基準

統一基準解説資料　別添資料
A.1.2 情報の格付け一覧　（3／3）

可用性による情報の格付け

格付け	分類基準	取扱制限
可用性2情報	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	例） 1時間以内復旧
可用性1情報	可用性2情報以外の情報	

統一基準

第3部　情報についての対策
3.2.1 情報の作成と入手

(1)業務以外の情報の作成又は入手の禁止

(2)情報の作成又は入手時における
格付けの決定と取扱制限の検討

必ず格付けを実施

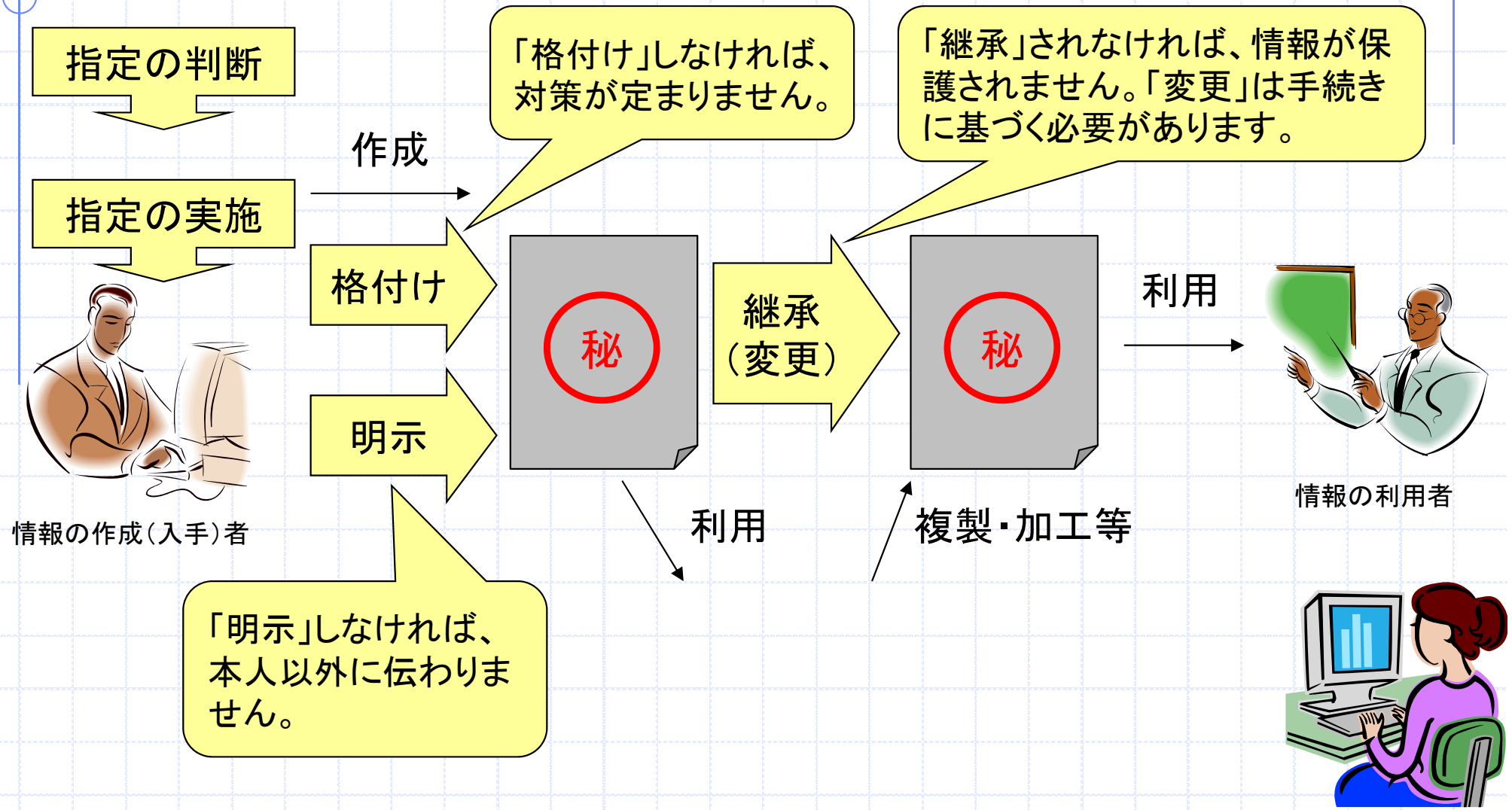
必要性を必ず検討し、必要に応じて取扱制限を指定

(3)格付けと取扱制限の明示

(4)格付けと取扱制限の継承

(5)格付けと取扱制限の変更

情報の格付け（及び取扱制限）



統一基準

第3部　情報についての対策
3.2.1 情報の作成と入手

3.2.1 (3)格付けと取扱制限の明示

1.1.3 用語定義より

『「明示」とは、情報を取り扱うすべての者が当該情報の格付けについて共通の認識となるように措置することをいう。なお、情報ごとの格付けの記載を原則とするが、特定の情報システムについて、当該情報システムに記録される情報の格付けを規定等により明記し、当該情報システムを利用するすべての者に当該規定を周知することなどについても明示に含むものとする。』

4.1 情報セキュリティについての機能

遵守事項の構成

情報セキュリティについての機能

(a) ○○○を行う必要性の有無を検討すること。

(b) ○○○を行う必要性があると認めた情報システムには、○○○を行う機能を設けること。

(c) ○○○を行う必要性があると認めた情報システムには、▼▼▼をすること。

(d) ・・・・・

(a) で必要性があると判断された情報システムに対して、(b) 以後の遵守事項を適用する。

目次

1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

３．１
統一基準作成時の配慮事項

●構造・体系化した全体構成
遵守内容の重複を許容
●遵守事項の主体者（主語）を明記
●遵守事項の実施内容（述語）を単純化
●主体者は、セキュリティ対策での役割（帽子）としている
組織上の役職（椅子）は、全員を表す「行政事務従事者」のみ
「課室情報セキュリティ責任者」に「課長」（椅子）を想定しているが、それ以外はすべて役割（帽子）としている
●実施内容は具体的なものを原則
具体性の度合いは、共通化現実性と方策限定の必要性に応ずる
●逐条解説文による補足説明

３．２
政府機関としての事項

●作業の委任
→現実の実施者よりも高い役職者が主体者の場合あり
●規程文書決済者が唯一
→第１部、２～３部、４～６部で分割してもよい
●リスク・エスカレーションの不在
→手続きの整備を求めているが、現場管理職によるエスカレーションでもよい
●監査室不在
→監査規程との整合に言及していない
●未定稿は行政文書ではない
→未定稿について言及していない
●事務部門以外は別途強化遵守事項あり
→行政事務と著しく異なる業務については別途の基準を検討

目次

1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

4. 政府機関以外での活用方法について

DO

●情報セキュリティ対策体制の検討
●情報の対象の検討
●格付け・取扱制限表、明示の定義の検討
●定義用語の検討
●一括置換（→の右側は参考例）
「行政事務」→「業務」
「行政事務従事者」→「社員」
「機密性１情報」→「非機密情報」
「機密性２情報」→「社外秘情報」
「機密性３情報」→「極秘情報」
●節・項の取捨選択
●強化遵守事項の取捨選択

4. 政府機関以外での活用方法について

DO NOT

●部・節・項構成を変更しない
→第7部を新設して追加する
→別規程を設け、統一基準対応規程については、事務部門など適合する部門だけを対象とする
→統一基準との対応関係を管理するのもよい
→★追加事項、懸念事項についてはパブコメで意見提出
●主語をセキュリティ体制上の役割（帽子）以外にしない
→帽子の任命部分で吸収させる
●述語を統合しない
→解説部分の追記をなるべく検討する

目次

1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

5. その他

●標識と運転席（サインポスト＆コックピット）
・府省庁基準による有言実行を構築（実行状況の把握）
・基準文書の記述により対策実施が担保
・実効性に問題があれば、基準文書を改訂して改善

アクセルペダル＋走行速度メーター
→メーターが建前ならば、横並び対策になる
走行速度メーターと標識による指示
→区別して構築
タクシーなら安心とは必ずしもならない

5. その他

●フラクタルなPDCA
・年度計画
・情報のライフサイクル
・情報システムのライフサイクル
●日常的な全員参加型のリスク判断
・情報：情報の格付け
・情報システム：必要性の判断
●日常的な全員参加型の自己点検
・情報（第2～3部）：教育理解度の再確認としての自己点検
→人ごとに集計
・情報システム（第4～5部）：ｵﾝﾀｲﾑ・ﾁｪｯｸﾘｽﾄとしての自己点検
→システムごとに集計

5. その他

●専任監査者ではなくてもできる監査領域の拡大

・遵守事項実施状況の判断は主体者自身による情報提供を前提

・専任監査者は、妥当性・実効性の確認を優先

・自己点検作業が多大な印象があるかもしれないが、その分、監査は容易

目次

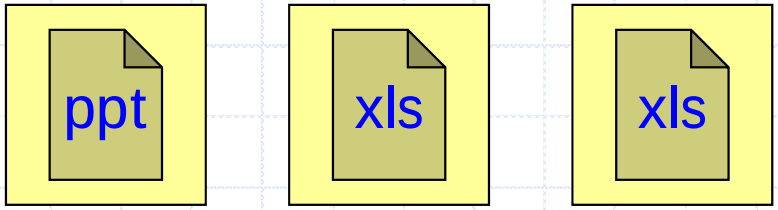
1. 経緯の紹介
2. 政府機関統一基準の説明
3. 文体の特徴と想定事項について
4. 政府機関以外での活用方法について
5. その他
6. 統一基準による自己点検と監査の概略
7. 質疑応答

6. 自己点検と監査の概略

●自己点検

各遵守事項についての主体者自身による自己点検

・遵守性の自己申告



●監査

全遵守事項及びその他についての主体者以外による確認

・統一基準と府省庁基準、関連規程の準拠性の確認

・自己点検結果の妥当性の確認

・重点検査による実効性の確認

※統一基準単独では、監査以外については遵守性を重視

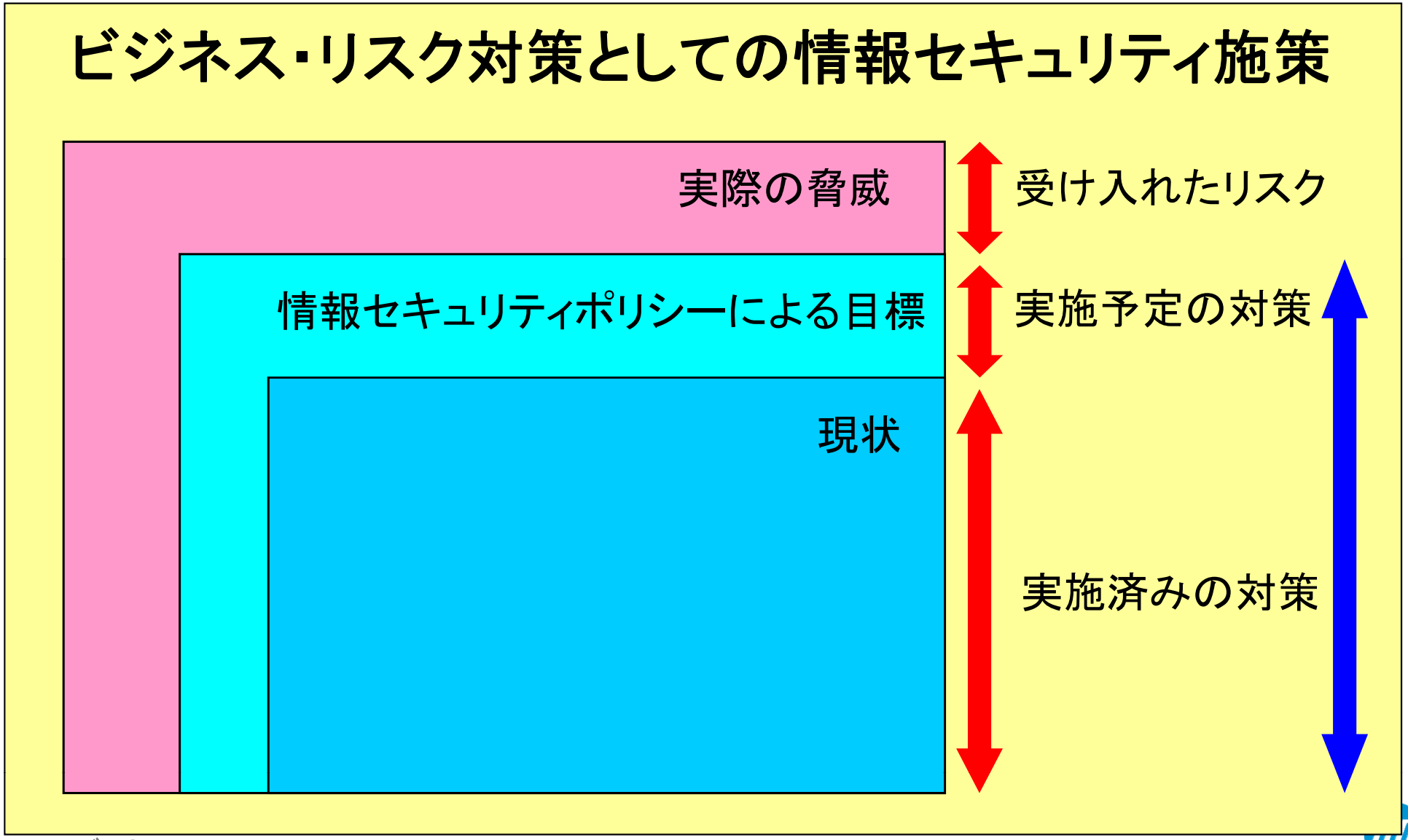
政府機関情報セキュリティ対策統一基準の特徴

日本企業の実践を基礎とした国産基準

２重のＰＤＣＡを回す
リスク分析を集約せず日々現場で実施する
自己点検を重視すること
主語を明確にして人の役割を重視すること
例外を想定すること

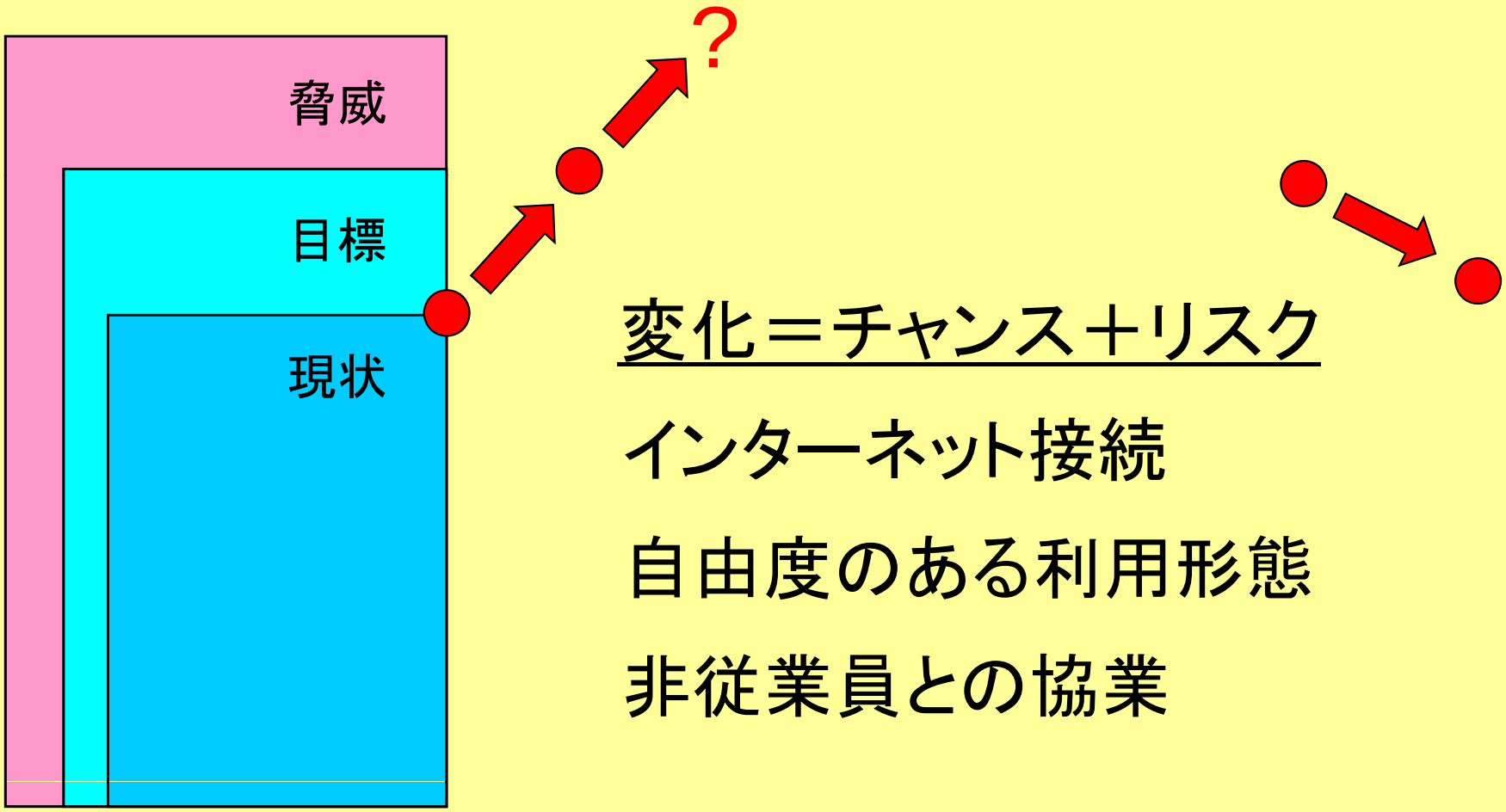
情報セキュリティ対策の実践

最低基準ではなく適正基準
「何をするか及び何をしないか」



最低基準ではなく適正基準
「何をするか及び何をしないか」

ビジネス・リスク対策としての情報セキュリティ施策



変化＝チャンス＋リスク

インターネット接続

自由度のある利用形態

非従業員との協業

利活用と保護のバランスを取るには？

守れるルールだけが、守られる。

実施できるルールだけを設けて、「ルールはすべて守るものである」という意識を定着させることが、結果的にルール遵守を定着させることができる。
できることの他に、できれば望ましいようなルールを混在させて、「必ずしも守らなくてもよいルールもある」という意識を持たれることは好ましくない。
遵守するための具体的な実施方法が明確になっていないルールを設けることは避ける。
情報利活用の要求に即したバランスを保つルールを設けることが重要。

利活用と保護のバランスを取るには？

性善説を前提にして性悪説も想定する

性善説を前提とする。その上で、性悪説についても想定すると考えることが重要。

性善説であれば、「ルールは守られる」というところから検討し始めることができる。

性悪説への対策は、ルールを守っている性善説の人達によって実施するしかないことを忘れてはいけない。

参考：BYODについて

モバイルIT環境としてのセグメント設計
Trusted Domainの設計
SoA としての BYOD の位置づけの明確化

http://yosihiro.com/ speech/#2012-10-17

参考：ソーシャルメディア利用について

業務利用と業務外利用（私用）を明確に分けて検討する
・業務利用はガイドライン
・業務外利用はガイダンス

http://yosihiro.com/ speech/#2012-11-29

目次

個人情報保護法
個人情報保護対策と情報セキュリティ対策
政府機関情報セキュリティ対策統一基準
情報セキュリティ対策の実践

発表資料のダウンロード

http://yosihiro.com/speech/#2013-01-21

お問い合わせ

twitter

http://twitter.com/4416sato