ＰＣネットワークの管理･活用を考える会
第２回　情報モラル･セキュリティ分科会

事例から学ぶ情報セキュリティルールの作成･守らせ方の作法

2009年1月28日(大阪)
2009年1月30日(東京)

ＢＭコンサルタンツ(株)
逸木　通隆

● ルールを守れない理由

(1) ルール無し

(2) ルールが貧弱

(3) ルールを理解しているが忘れていた

(4) ルールを理解しているが手続きが多い、複雑

(5) ルールを理解しているが守っている状態を維持するのが困難

(6) ルールを理解している状態を維持するのが困難

(7) ルールを理解できない

(8) ルールを守る気が無い

ルールを守る者がルールを守る意識を持つために

ルールが備えなければならない必要条件

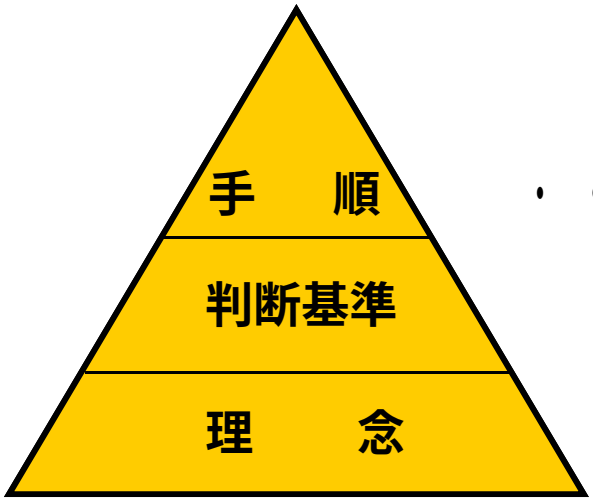
① 理解し易い ② 忘れにくい ③ 簡単、平易 ④ 守り易い ⑤ 覚え易い

2. 情報セキュリティルールを守らせる対策

ルールを守れない理由	ルールを守らせる対策 Do: IT化(ツール導入等)	ルール平易化	ルール簡素化	ルール管理強化	ルール充実	ルール策定	教育(周知・徹底)	罰則(又は制裁)	Check: 自己点検、内部監査	指摘点是正	Act: 是正結果確認
1 ルール無し						○	○		○	○	○
2 ルールが貧弱					○		○				
3 ルールを理解しているが忘れていた				○			○				
4 ルールを理解しているが手続きが多い、複雑			○				○				
5 ルールを理解しているが守っている状態を維持するのが困難	○		△				○				
6 ルールを理解している状態を維持するのが困難	○		△				○				
7 ルールを理解できない		○	○				○				
8 ルールを守る気が無い							△	○			

○:実施　△:検討要

● 情報セキュリティポリシーの階層構造と考え方



・・・ マニュアル、手順書、様式

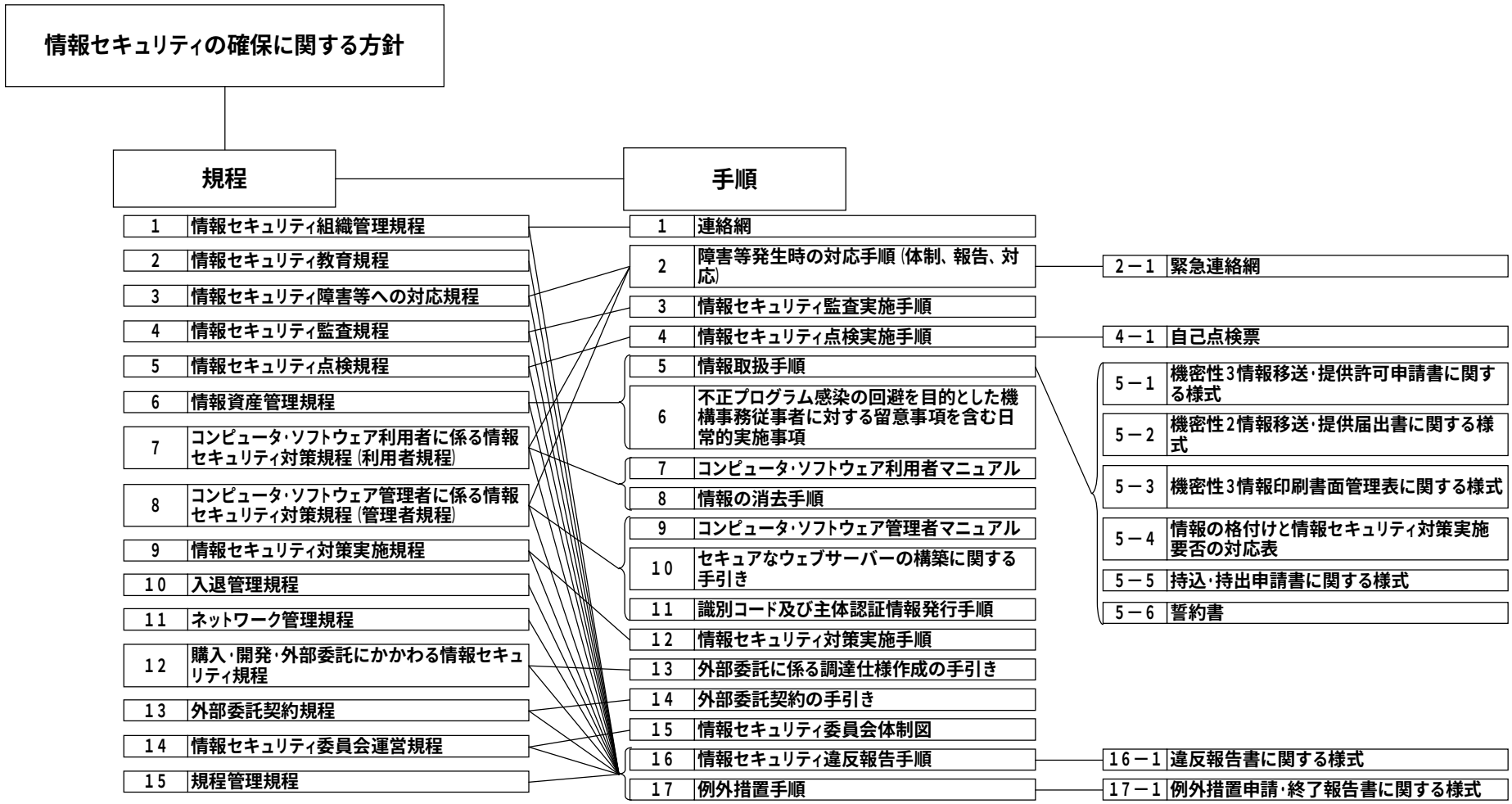
・・・ 規程

・・・ 方針

理念が大本にあり、理念を踏まえて判断基準を策定、判断基準に即して具体的な判断レベル決めや作業手順作成をする。3者の整合を維持することが必要である。

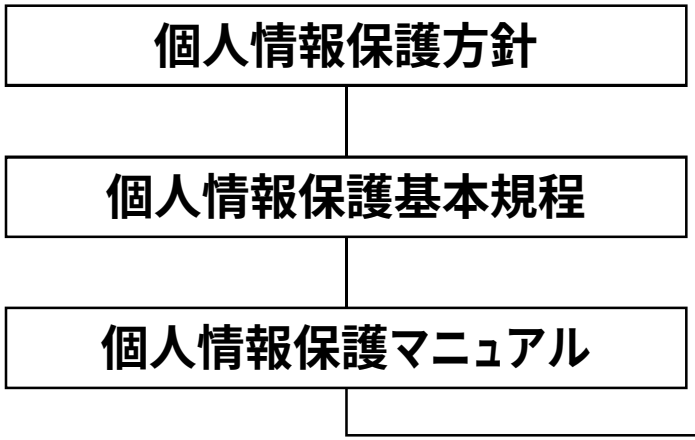
3. 情報セキュリティルール作成の作法

● 政府統一基準に沿った情報セキュリティポリシー構成例



3. 情報セキュリティルール作成の作法

● Pマーク要求事項(JIS Q 15001:2006)に沿った情報セキュリティポリシー構成例



連番	基本規程	マニュアル	成果物名
1	第０５条	第０４条	001-個人情報管理台帳
2	第０５条	第０４条	002-預託提供共同利用個人情報管理台帳
3	第１５条	-	003-個人情報保護基本方針
4	第１５条	-	004-個人情報保護基本規程
5	第１５条	-	005-個人情報保護マニュアル
6	第０８条	第０７条	006-個人情報体制図
7	第０５条	第０４条	007-入出庫管理表等７種
8	第０７条	第０６条	008-業務フロー作成手順書
9	第０７条	第０６条	009-リスク分析手順書
10	第０７条	第０６条	010-リスク分析報告書
10	第０７条	第０６条	010-リスク分析報告書(サンプル)(第２版)

70	第４４条	第３８条	070-予防処置計画書兼結果報告書
71	第４３条	第３７条	071-内部監査業務フロー
72	ー	ー	072-提出書類一覧(サンプル)
73	第４５条	第３９条	073-代表者の見直しに係る事項報告書
74	第４５条	第３９条	074-マネジメントレビュー結果兼改善指示書
75	第４４条	第３８条	075-改善計画書
76	第４４条	第３８条	076-改善結果報告書

条項と成果物(様式)の対応表の公開

連番	基本規程	マニュアル	成果物名
15	第３７条	第２６条	015-個人情報保護教育計画書
16	第３７条	第２６条	016-個人情報保護研修資料
17	第３７条	第２６条	017-達成度（理解度）テスト
18	第３７条	第２６条	018-個人情報保護教育受講者名簿
19	第３７条	第２６条	019-理解度テスト回収状況
20	第３７条	第２６条	020-個人情報保護教育実績報告書

3. 情報セキュリティルール作成の作法

● 情報セキュリティ方針例

グループは「ITを通じた様々なサービス提供によりリーディング企業グループにふさわしい企業市民となり、お客様、社員とその家族、株主などすべてのステークホルダーから評価いただける企業価値の向上を目指す」を経営理念として活動しています。

経営理念

経営理念実現には、情報セキュリティに関し高い企業モラルを堅持し、お客様のシステムやデータ等の情報資産ならびにグループの経営資源としての情報資産をあらゆる脅威から保護することが重要な課題となります。

ここに情報資産の適切な保護を徹底するために情報セキュリティに関する方針を定め、これを推進します。

情報セキュリティ理念

● 情報セキュリティ管理体制

グループは、グループ全体の情報セキュリティに関するあらゆるリスクに対応するためのマネジメントシステムとしてグループコンプライアンス会議を運営します。

またグループ内各社においても本方針に則り、情報セキュリティマネジメントシステムを運営します。

● 法的及び契約上の要求事項への準拠

グループは、個人情報保護法を始めとする情報セキュリティに関する法令、その他の規範、ガイドライン、および契約上のセキュリティ要求事項を遵守します。

● 情報セキュリティ管理規定の制定

⋮

● 継続的改善

本方針が遵守されていることを確認するために、グループコンプライアンス会議において、定期的に情報セキュリティマネジメントシステムの実施状況を評価し、継続的な改善に努めます。

実施方針

制定日：　　年　月　日

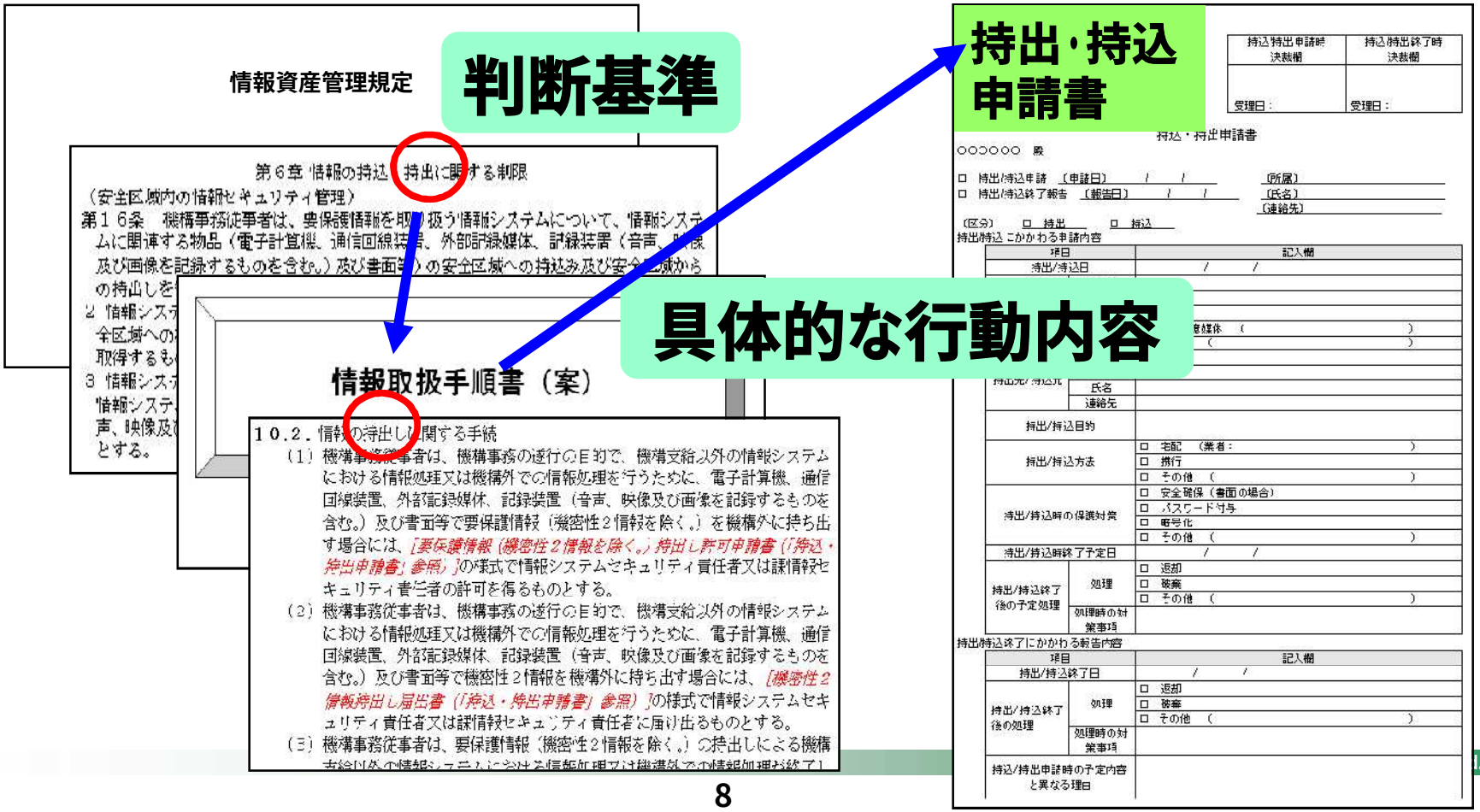
株式会社

代表取締役社長

3. 情報セキュリティルール作成の作法

● ポリシー間の関係例

会社から要保護情報を持出す場合、「情報資産管理規程」を読み“持出制限”されている物品にあたるかどうか判断し、該当する場合「情報取扱手順書」を読み、手順と使用する申請書を入手して責任者に申請する。

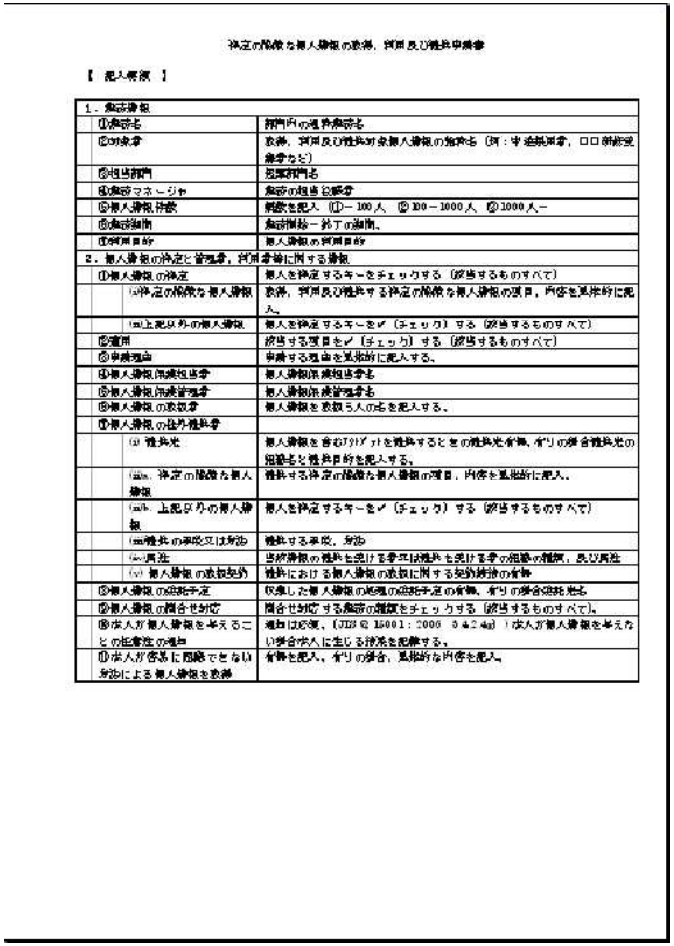


3. 情報セキュリティルール作成の作法

● 様式例 ： 様式には記入要領をつける

様式

記入要領



3. 情報セキュリティルール作成の作法

● 記入要領作成例 ： 記入要領は具体的に記述する

様式

個人情報保護管理者　殿

特定の機微な個人情報の取得、利用及び提供申請書

個人情報保護マニュアル第９条第１項の規定にのっとり下記の通り申請します。

申請日：　○○年○月○日

申請者：○○部　○○　○○

記

１．業務情報			
①業務名			
②対象者			
③担当部門		④業務マネージャ	
⑤個人情報件数	件		
⑥業務期間	年　月　日～　年　月　日		
⑦利用目的			

２．個人情報の特定と管理者、利用者等に関する情報

①個人情報の特定	(i)特定の機微な個人情報	
	(ii)上記以外の個人情報	□氏名　□住所　□生年月日 □メールアドレス　□職業 □勤務先□会社(組織)名 □上記以外の項目

記入要領

【 記入要領 】

１．業務情報		
	①業務名	部門内の通称業務名
	②対象者	取得、利用及び提供対象個人情報の総称名（例：中途採用者、○○研修受講者など）
	③担当部門	起票部門名
	④業務マネージャ	業務の担当役職者
	⑤個人情報件数	概数を記入（①～100人　②100～1000人　③1000人～
	⑥業務期間	業務開始～終了の期間。
	⑦利用目的	個人情報の利用目的
２．個人情報の特定と管理者、利用者等に関する情報		
	①個人情報の特定	個人を特定するキーをチェックする（該当するものすべて）
	(i)特定の機微な個人情報	取得、利用及び提供する特定の機微な個人情報の項目、内容を具体的に記入。
	(ii)上記以外の個人情報	個人を特定するキーを✔（チェック）する（該当するものすべて）

● 記述の作法

- 原則として**中学校までに習う漢字のみ**を使う。
- 読み方が難しかったり、一般的でなかったりするものには、**ふりがな**を付ける。
- 従業員や職員が読んで理解しにくい(と思う)用語や表現には**注釈**を付ける。
- **だれが、だれに、いつ、何を、どうしなければならないかを明確**に記述する。

● 機関決裁の作法

- 決裁機関の例
  - ー 情報セキュリティ方針は**社長**
  - ー 情報セキュリティ規程は**CIO**
  - ー 情報セキュリティマニュアル、手順書、書式は**下位組織**

情報セキュリティルールの体系は、理念、判断基準、手順の３段階で簡素に。
記述は、初めて読む人にもわかりやすく、具体的に。

● ノートパソコン、USBメモリ等の持ち出しの作法

・ノートパソコン、USBメモリ等の持ち出し規則の例

・機密情報の取引先等との授受、社外持出し時の盗難、紛失による情報漏えい対策として以下の情報は暗号化すること。

- 手渡し又は配送により授受する記憶媒体に格納した情報
- 電子配信する情報
- 社外持出しする記憶媒体に格納した情報

業務連絡書を発行して周知・徹底

暗号化規定、マニュアル制定

全従業員、委託先関係者e-ラーニング受講

→

現場からのクレームを反映して改訂

→

(ルール緩和)

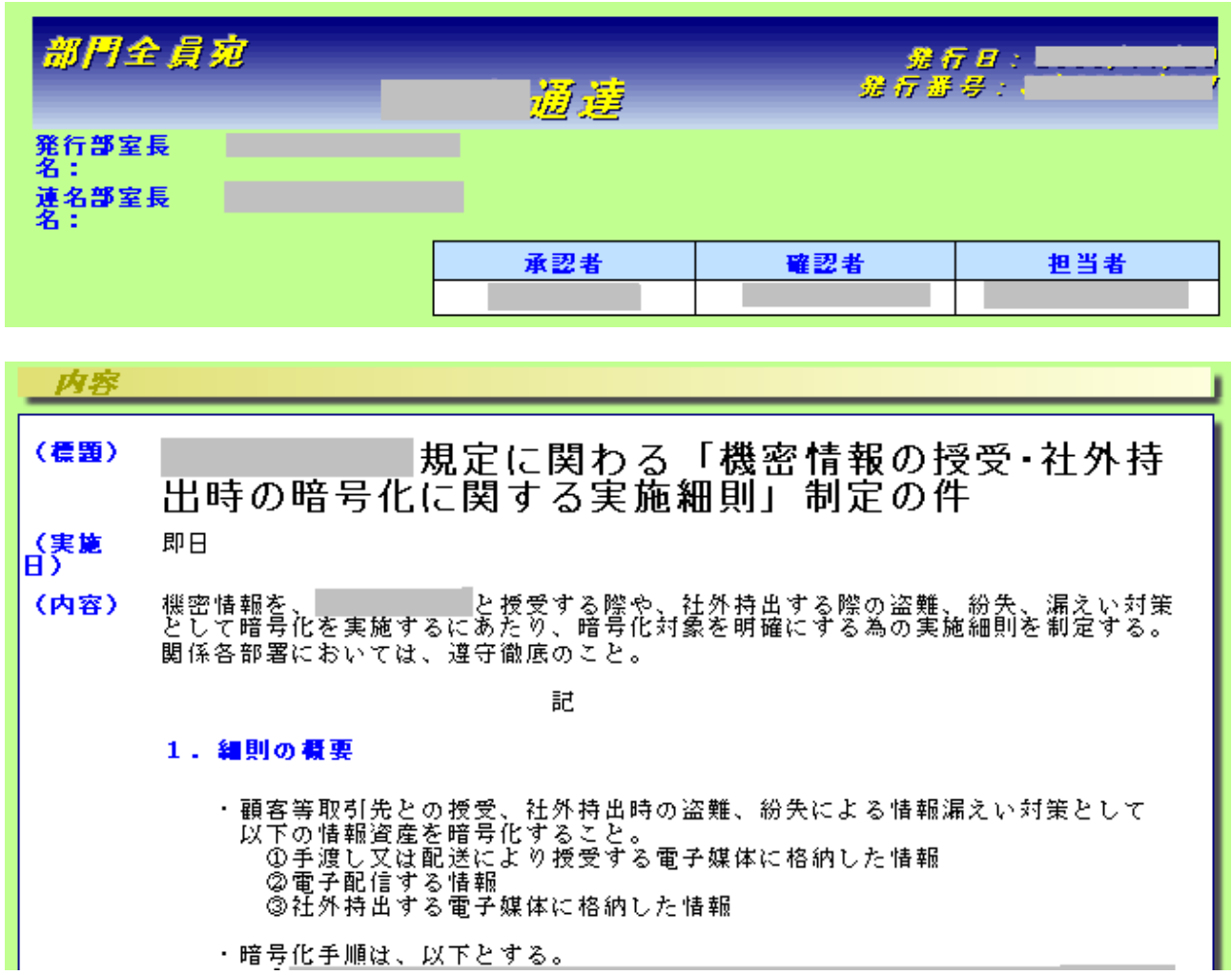
都度許可 → 期間許可

(ルール強化)

持出す機密情報の事前特定ルール厳格化

持出し専用パソコン、USB

● 業務連絡書(サンプル)例



部門全員宛

通達

発行日：

発行番号：

発行部室長名：

連名部室長名：

承認者	確認者	担当者

内容

（標題） 規定に関わる「機密情報の授受・社外持出時の暗号化に関する実施細則」制定の件

（実施日） 即日

（内容） 機密情報を、と授受する際や、社外持出する際の盗難、紛失、漏えい対策として暗号化を実施するにあたり、暗号化対象を明確にする為の実施細則を制定する。
関係各部署においては、遵守徹底のこと。

記

１．細則の概要

・顧客等取引先との授受、社外持出時の盗難、紛失による情報漏えい対策として以下の情報資産を暗号化すること。
①手渡し又は配送により授受する電子媒体に格納した情報
②電子配信する情報
③社外持出する電子媒体に格納した情報

・暗号化手順は、以下とする。

● 電子メール利用の作法

・電子メール利用規則の例

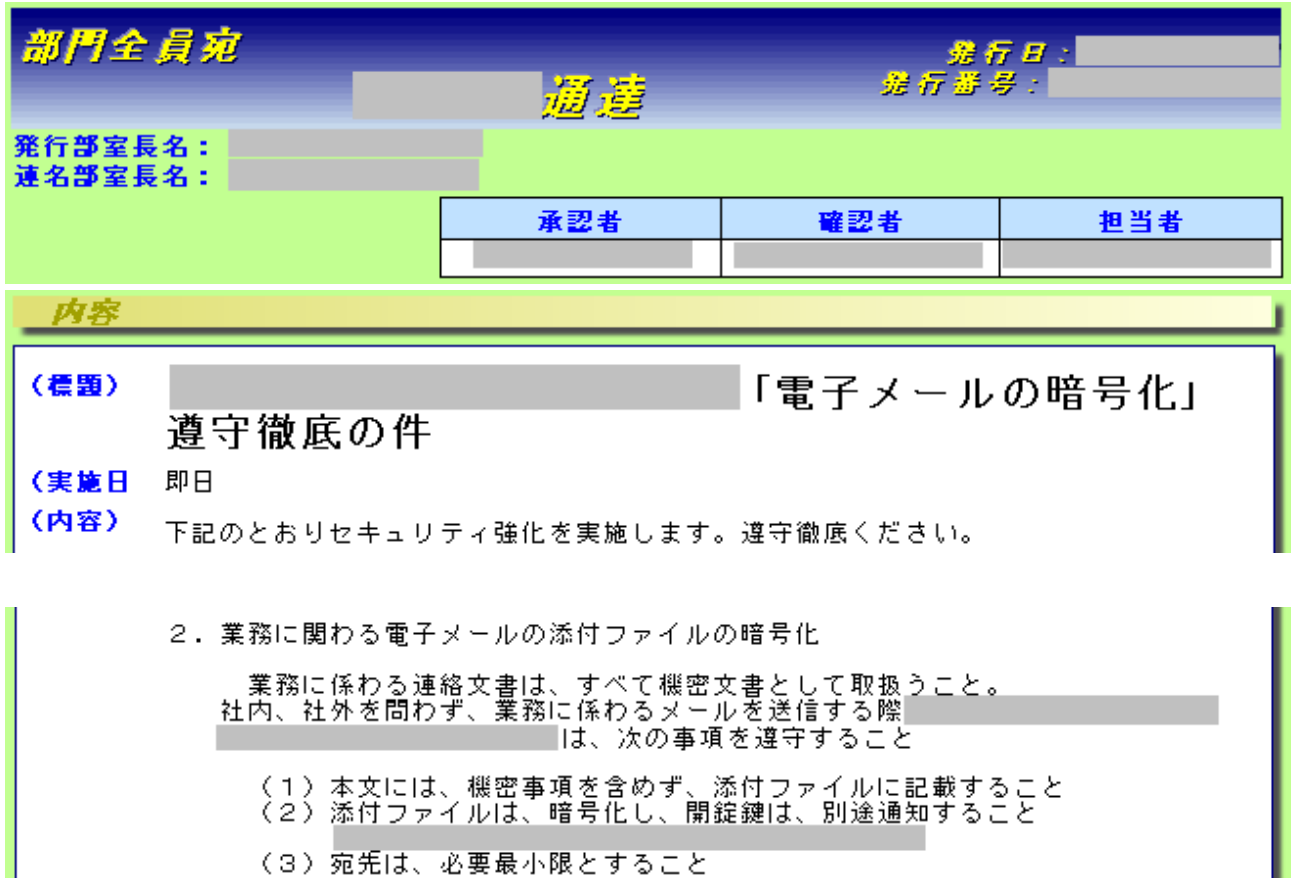
- 業務に係わる連絡文書は、すべて機密文書として取扱うこと。
- 社内宛、社外宛を問わず、業務に係わるメールを送信する際は、次の事項を遵守すること
  - 本文には、機密事項を含めず、添付ファイルに記載すること
  - 添付ファイルは暗号化し、開錠鍵は別途通知すること
  - 宛先は必要最小限とすること

業務連絡書を発行して周知・徹底

メールアーカイブ実施

全従業員、委託先関係者e-ラーニング受講

● 業務連絡書(サンプル)例



部門全員宛

[redacted] 通達

発行日：[redacted]
発行番号：[redacted]

発行部室長名：[redacted]
連名部室長名：[redacted]

承認者	確認者	担当者
[redacted]	[redacted]	[redacted]

内容

（標題）[redacted]「電子メールの暗号化」遵守徹底の件

（実施日）即日

（内容）下記のとおりセキュリティ強化を実施します。遵守徹底ください。

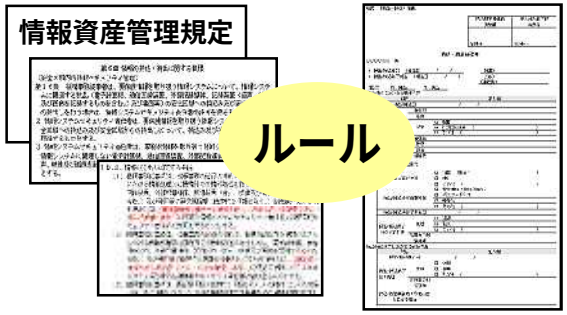
２．業務に関わる電子メールの添付ファイルの暗号化

業務に係わる連絡文書は、すべて機密文書として取扱うこと。
社内、社外を問わず、業務に係わるメールを送信する際[redacted]は、次の事項を遵守すること

（１）本文には、機密事項を含めず、添付ファイルに記載すること
（２）添付ファイルは、暗号化し、開錠鍵は、別途通知すること[redacted]
（３）宛先は、必要最小限とすること

4. 情報セキュリティポリシーの守らせ方の作法

● 守らせ方の例 ： ルールはできた。周知教育した。あとは守らせる側の本気を着信。

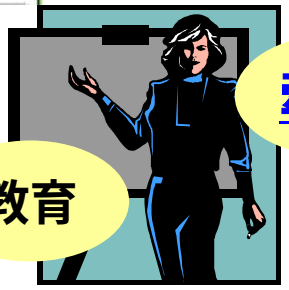


ルール

周知

啓発

教育



牽制

納得と得心

点検

OK！

NO！

懲戒を受ける可能性のあることをしっかりと認識させる

5. まとめ

(1) 情報セキュリティルール策定者は、ルールを適用する者の要望と会社の方針との間でバランスの取れたルールを策定する

(2) 情報セキュリティルール運用者は、ルールを適用する対象者に、周知、教育をする

(3) 最高情報セキュリティ責任者は、①運用状況の点検・監査、②クレームなどの指摘を受付け、③指摘事項の是正を指示する

(4) 各担当者は、(1)～(3)を継続して実施する。また、最高情報セキュリティ責任者は、継続して実施する意思表示をする

(5) 会社は、ルールに違反した者に対して罰則を科すことを明確にする（牽制）。また、会社は、現にルール違反した者に対して罰則を科す

ＢＭコンサルタンツ株式会社
逸木通隆

〒105-8624　東京都港区海岸１－１４－５　ＴＩＳ竹芝ビル
TEL (03)5402-2421　　e-mail：ituki@tis.co.jp

情報セキュリティポリシー策定、改訂、情報セキュリティ監査、ＩＳＭＳ、その他情報セキュリティのお問合せは

ISMS審査員、情報セキュリティアドミニストレータ、情報処理システム監査技術者

専門分野

情報セキュリティポリシー策定　インターネットデータセンタービル建設監理

情報セキュリティ監査　個人情報保護　情報セキュリティマネジメントシステム構築

安全対策／危機管理　事業継続(BCP/BCM)

実　績

個人情報保護法対応支援　プライバシーマーク認定取得支援　ＩＳＭＳ認証取得支援

情報セキュリティ監査　個人情報保護監査　関連分野の講演、研修