2015.06.05JSSA大会

ISMS情報セキュリティ対策における営業秘密保護の考察

Considerations for "the protection of the trade secret"
in the Information Security Management System (ISMS)

2015年06月05日

情報セキュリティ合同研究会

発表者　高橋孝治・植野俊雄

ISMS情報セキュリティ対策における営業秘密保護の考察

目　　次

1．研究の背景とねらい

1-1. ISMS情報セキュリティと機密情報流出事件

ISMS情報セキュリティ対策では、
ISO27001に定めるリスクマネジメントの手法で、
ISO27002で示す管理策ガイド等を参考に管理策を採用して、
情報セキュリティの保護の仕組みを整備・運用する。

しかし、このように整備されたISMS情報セキュリティの保護対策の裏を掻い潜って秘密情報を持ち出し、競合企業や名簿業者等に持ち込むという事件が繰り返し発生している。

昨年、以下のような大事件が新聞等で報道された。

・半導体研究データが従業者によって持ち出され、転職した他国の企業に持ち込まれた事件　（2014年3月容疑者逮捕）
・顧客データを記憶装置に移して持ち出し売却し、それが他社DMに利用された事件　（2014年7月容疑者逮捕）

1．研究の背景とねらい

1-2. IPA情報セキュリティ10大脅威で「内部不正」が上位に

IPAが2015年2月に公表した**「情報セキュリティ10大脅威 2015」**では、**「内部不正」が第2位**に選ばれた。

出典：IPA「情報セキュリティ10大脅威 2015」(2015年2月6日公表)　2015年1月実施

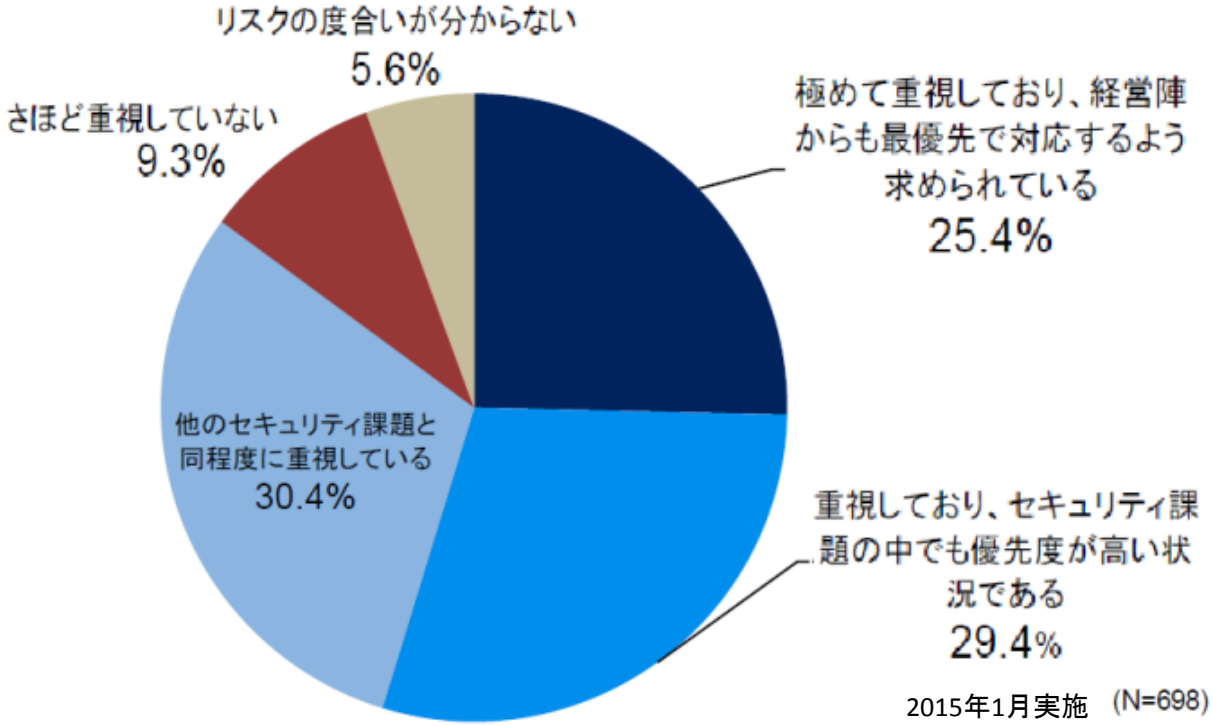
【2014年】【2015年】

第5位　⇒　第1位　インターネットバンキングやクレジットカード情報の不正利用
第11位 ⇒ 第2位　内部不正による情報漏えい
第1位　⇒　第3位　標的型攻撃による諜報活動
第2位　⇒　第4位　ウェブサービスへの不正ログイン
第4位　⇒　第5位　ウェブサービスからの顧客情報の窃取
：

1．研究の背景とねらい

1-3. 高まる内部犯行による機密情報流出への危機感

JIPDEC／ITRの「企業IT利活用動向調査2015」の速報結果の発表資料の中で示されている
「内部犯行による重要情報の漏洩・逸失」のリスクに対する重視度合い



出典：JIPDEC／ITRの「企業IT利活用動向調査2015」速報結果の2015年3月24日の発表

1．研究の背景とねらい

1-4. ISMS情報セキュリティで どう営業秘密を守るか

これら悪意ある意図的な情報流出事件では、
不正競争防止法の営業秘密に対する不正取得行為
などで検挙されている。 (新聞報道などによる)

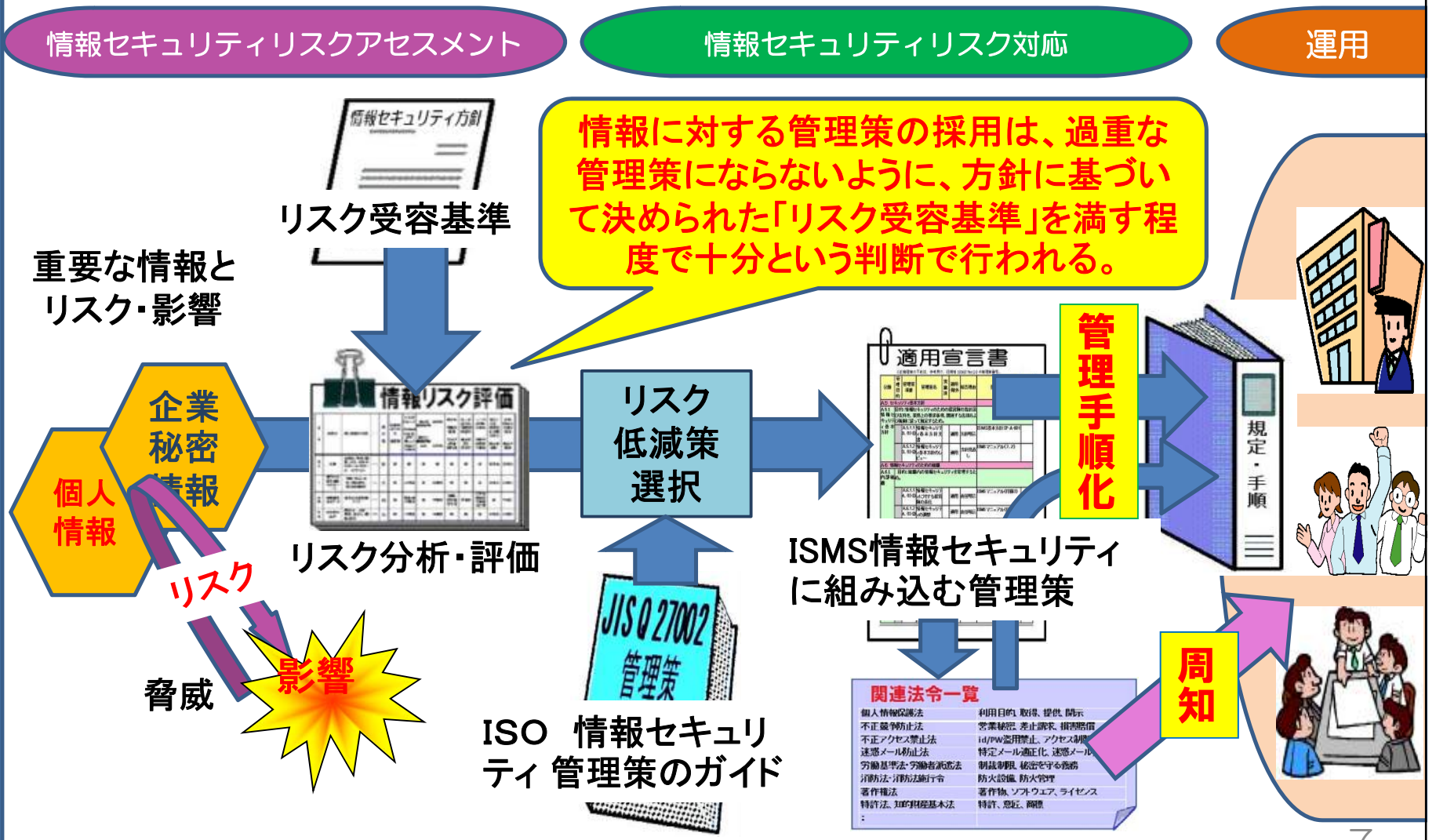
ISMS情報セキュリティ対策では、これらの犯罪行為からも秘密情報を守らなければならない。

しかし、ISO27001の情報セキュリティのリスクマネジメントの手法でISO27002の管理策ガイド等を参考に管理策を採用する際に、
「営業秘密」とか「不正競争防止法」とかいう言葉はほとんど現れてこないので、営業秘密保護が不完全になりやすいのではないかと考えられる。

そこで、 ISMS情報セキュリティ対策で、
「営業秘密の保護」の有効な対策を講じるにはどうすればよいか、
を研究し、考察した。

2. ISMS情報セキュリティ対策と関連法令との関係

2-1. ISO27001 ISMSによる情報セキュリティリスクマネジメント



2. ISMS情報セキュリティ対策と関連法令との関係

2-2. 情報セキュリティ関連法令とガイドラインの状況

関連法令（主なもの）	ガイドライン（主なもの）	備　考
個人情報保護法 （H21.6.5改正）	経済産業分野を対象とするガイドライン （H26.12.12改正） 雇用管理分野における個人情報保護に関するガイドライン(H24.5.14改正） JIS Q 15001：2006個人情報保護マネジメントシステム−要求事項（H18.5.20）	マイナンバー法（行政手続における特定の個人を識別するための番号の利用等に関する法律）（H26.7.17公表） 特定個人情報の適正な取扱いに関するガイドライン(事業者編)(H26.12.11）
不正競争防止法 （H24.3.31改正）	営業秘密管理指針（H27.1.28改訂） 包括的対策は「営業秘密保護マニュアル」（仮称）として今後改訂発行予定。 組織における内部不正防止ガイドライン （第3版2015.3.3　IPA）	従来の指針では不正競争防止法の罰則の適用が厳密過ぎたのが、改正で適用しやすくした、等の変更。 （従業員への罰則適用が強化されたということであるので、従業員に注意喚起する必要がある）
不正アクセス禁止法 （H25.5.31改正）	コンピュータ不正アクセス対策基準 （H12.12.28改定）	
特定電子メール送信適正化法（H23.6.24改正）	特定電子メールの送信等に関するガイドライン（H23.8.31改正）	

2. ISMS情報セキュリティ対策と関連法令との関係

2-3. ISO27002情報セキュリティ管理策ガイドによる法令対応

A.18 順守　　A.18.1 法的及び契約上の要求事項の順守

A.18.1.1 適用法令及び契約上の要求事項の特定　⇒　関連法令、規制、契約要求事項の一覧化

【関連法令一覧】

個人情報保護法	利用目的、取得、提供、開示
不正競争防止法	営業秘密、差止請求、損害賠償
不正アクセス禁止法	id/PW盗用禁止、アクセス制御管理
迷惑メール防止法	特定メール適正化、迷惑メール禁止
労働基準法・労働者派遣法	制裁制限、秘密を守る義務
消防法・消防法施行令	防火設備、防火管理
著作権法	著作物、ソフトウエア、ライセンス
特許法、知的財産基本法	特許、意匠、商標
:	

関連法令と要求事項を特定

周知

A.18.1.2 知的財産権　⇒　ソフトウエアのライセンス管理

A.18.1.3 記録の保護　⇒　記録の法的保管期限の管理

A.18.1.4 プライバシー及び個人を特定できる情報（PII）の保護管理策　⇒個人情報保護法対応

管理手順化

2. ISMS情報セキュリティ対策と関連法令との関係

2-4. 管理策ガイドに沿って管理手順化される法令要求（例）

A.18.1.1 適用法令及び契約上の要求事項の特定　⇒　関連法令、規制、契約要求事項の一覧化

A.18.1.2 知的財産権　⇒　ソフトウエアのライセンス管理

A.18.1.3 記録の保護　⇒　記録の法的保管期限の管理

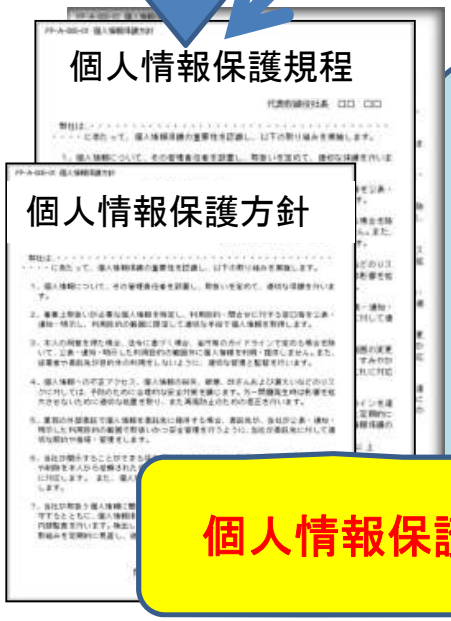
A.18.1.4 プライバシー及び個人を特定できる情報（PII）の保護管理策　⇒個人情報保護法対応

管理手順化

【関連法令一覧】

個人情報保護法	利用目的、取得、提供、開示
不正競争防止法	営業秘密、差止請求、損害賠償
不正アクセス禁止法	盗用禁止、アクセス制御管理
迷惑メール防止法	ール適正化、迷惑メール禁止
	を守る義務
	管理
著作権法	著作物、ソフトウエア、ライセンス
特許法、知的財産基本法	特許、意匠、商標
:	

個人情報保護法と要求事項を特定



ホームページ

当社が取り扱う個人情報とその利用目的

(1)お客様個人情報

(2)株主様個人情報

(3)お取引先様個人情報

(4)採用応募者・従業員

(5)当社への問合せ・訪問者

個人情報保護法への対応

2. ISMS情報セキュリティ対策と関連法令との関係

2-5. 管理策ガイドで管理手順化されない法令要求（例）

A.18.1.1 適用法令及び契約上の要求事項の特定　⇒　関連法令、規制、契約要求事項の一覧化

【関連法令一覧】

個人情報保護法	利用目的、取得、提供、開示
不正競争防止法	営業秘密、差止請求、損害賠償
不正アクセス禁止法	id/PW盗用禁止、アクセス制御管理

周知

法令関連の管理策のガイドの「A.18.1.1 適用法令及び契約上の要求事項の特定」によって作成した【関連法令一覧】では、不正競争防止法と、その要求事項である営業秘密、差止請求、損害賠償などが特定され、

周知 の対象になるが、

それ以上具体化されることはあまりない。のが実情である。

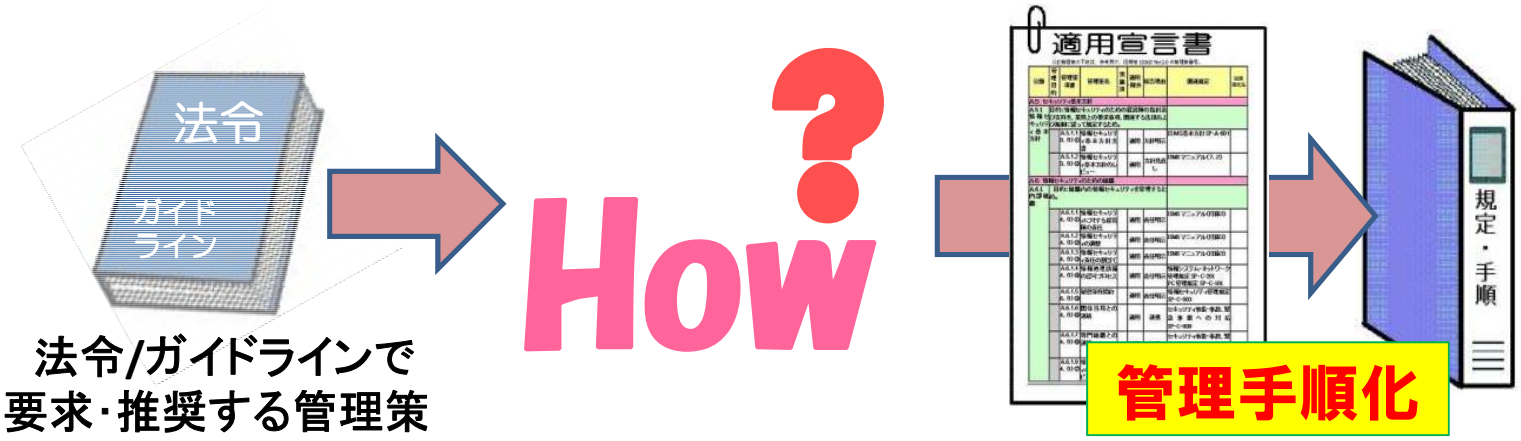
問題

関連法令要求事項に対する管理策追加と手順化が行われていない

3. 関連法令要求事項の適切な把握方法の検討

3-1. 関連法令要求事項の把握と対処方法の検討

関連法令の要求事項を把握し、それを管理策や手順に結び付ける方法が必要



3. 関連法令要求事項の適切な把握方法の検討

3-2. 関連法令要求事項を特性分類に沿って把握するワークシート

関連法令の要求事項を以下のような“特性分類”で整理することができる。

要求分類	組織・経営者・管理責任者	従業者
体 制 整 備	方針、体制、内部監査、 マネジメントレビュー、改善	ー ー
情報保護管理	リスクマネジメント、 規程・手順の整備、見直し改善 方針・規定・手順の周知徹底	目的・自身の役割を理解、 開催教育研修に出席、 ルールの認識・遵守 異常等の報告
手 続 事 項	規程・手順への反映、 周知徹底、施行確認	手続の理解・遵守、 例外の報告
罰 則 の 適 用	罰則の制定、周知、契約・誓約取得、 違反者への罰則適用	合意の誓約・契約 処罰受入・損害賠償

4. 関連法令の情報セキュリティ要求事項の抽出

3−2.の
「 関連法令要求事項を特性分類に沿って把握するワークシート」
で、**以下の関連法令の要求事項を特性分類で整理してみた。**

法令要求事項の特性分類 把握WS

要求分類	組織・経営者・管理責任者	従業者
体 制 整 備	方針、体制 内部監査、マネジメントレビュー、改善	－－
情報保護管理	リスクマネジメント、規程・手順の整備、見直し改善 方針・規定・手順の周知徹底	目的・自身の役割を理解、開催教育研修に出席、ルールの認識・遵守 異常等の報告
手 続 事 項	規程・手順への反映、周知徹底、施行確認	手続の理解・遵守、例外の報告
罰則の適用	罰則の制定、周知、契約・誓約取得、違反者への罰則適用	合意の誓約・契約 処罰受入・損害賠償

標準パターン

4-1. 個人情報保護法/JIS Q 15001
4-2.不正競争防止法(営業秘密)/営業秘密管理指針
4-3. 不正アクセス禁止法

4. 関連法令の情報セキュリティ要求事項の抽出

4-1. 個人情報保護法/JIS Q 15001 の情報セキュリティ要求事項

要求分類	組織・経営者・管理責任者	従業者
体 制 整 備	個人情報保護方針、体制、内部監査、 マネジメントレビュー、改善	ー ー
情報保護管理	個人情報のライフサイクルに亘る取扱いの リスクマネジメント、 規程・手順の整備、見直し改善 方針・規定・手順の周知徹底	目的・自身の役割を理解、 開催教育研修に出席、 ルールの認識・遵守 異常等の報告
手 続 事 項	利用目的、取得、提供、利用目的の変更、 開示等の請求対応、漏洩事故時の監督機 関届出等の手続の規程・手順への反映、 周知徹底、施行確認	手続の理解・遵守、 例外の報告
罰 則 の 適 用	罰則があることの周知、 社内の罰則の制定、周知、契約・誓約取得、 違反者への罰則適用	罰則についての認識、 合意の誓約・契約 処罰受入・損害賠償

4. 関連法令の情報セキュリティ要求事項の抽出

4-2.不正競争防止法(営業秘密)／営業秘密管理指針の情報セキュリティ要求事項

要求分類	組織・経営者・管理責任者	従業者
体 制 整 備	営業秘密管理意思、 体制、内部監査、 マネジメントレビュー、改善	ーー
情報保護管理	営業秘密の特定、 秘密管理性・有用性・非公知性及び 不正取得行為に関するリスクマネジメント、 規程・手順の整備、見直し改善 営業秘密管理意思・規定・手順の周知徹底	目的・自身の役割を理解、 開催教育研修に出席、 ルールの認識・遵守 異常等の報告
手 続 事 項	不正取得行為に対する訴え、 差止・損害賠償請求の手続の策定	ーー
罰則の適用	刑罰があることの周知、 社内の罰則の制定、周知、契約・誓約取得、 違反者への罰則適用	刑罰についての認識、 社内罰則の合意の誓約・ 契約、処罰受入・損害賠償

4. 関連法令の情報セキュリティ要求事項の抽出

4-3. 不正アクセス禁止法 の情報セキュリティ要求事項

要求分類	組織・経営者・管理責任者	従業者
体 制 整 備	アクセス管理方針、体制、内部監査、マネジメントレビュー、改善	ー ー
情報保護管理	許可されていない情報アクセスに関するリスクマネジメント、規程・手順の整備、見直し改善 方針・規定・手順の周知徹底	目的・自身の役割を理解、開催教育研修に出席、ルールの認識・遵守 異常等の報告
手 続 事 項	アクセス許可申請手続きの規程・手順への反映、周知徹底、施行確認、不正アクセス行為に対する訴え手続策定	手続の理解・遵守、例外の報告
罰則の適用	刑罰（適用しやすく改正）があることの周知、社内の罰則の制定、周知、契約・誓約取得、違反者への罰則適用	刑罰についての認識、社内罰則の合意の誓約・契約、処罰受入・損害賠償

5.関連法令要求事項を考慮したISMS情報セキュリティ対策

ワークシートに沿って4-1～4-3で
各法令の要求事項を特性分類に沿って把握できた。

特性分類に沿って把握した法令の要求事項は、
（分類済みなので）そのまま手順に展開できる。

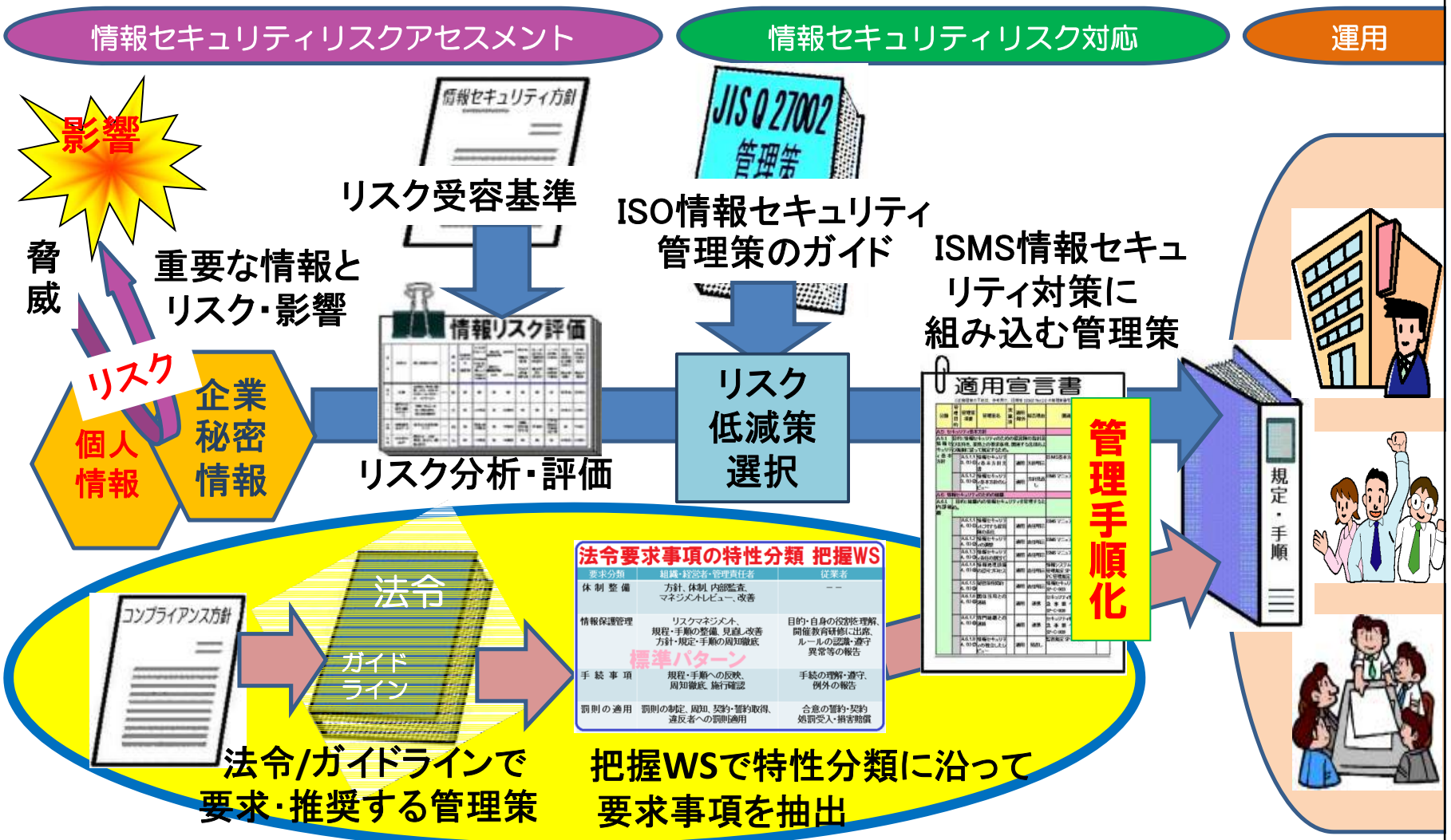
4-1～4-3　で例示した法令の情報セキュリティ要求事項を
ISMSの“情報セキュリティ”のリスクマネジメントに統合すると、
次スライドのようになる。

5.関連法令要求事項を考慮したISMS情報セキュリティ対策

分類	組織・経営者・管理責任者	従業者
体制整備	ISMS方針、個人情報保護方針、営業秘密管理意思、アクセス管理方針、体制、内部監査、マネジメントレビュー、改善	ーー
情報保護管理	重要な情報のCIA、個人情報のライフサイクルに亘る取扱い、営業秘密の特定、秘密管理性・有用性・非公知性及び不正取得行為、許可されていない情報アクセスに関するリスクマネジメント、規程・手順の整備、見直し改善方針・営業秘密管理意思・規定・手順の周知徹底	目的・自身の役割理解、開催教育研修に出席、ルールの認識・遵守異常等の報告
手続事項	アクセス許可申請手続き、個人情報の利用目的・取得・提供・利用目的の変更・開示等請求対応、漏洩事故時の監督機関届出等の手続、の規程・手順への反映、周知徹底、施行確認 ウィルス等被害の届出、不正アクセス行為・不正取得行為に対する訴え、差止・損害賠償請求の手続の策定	手続の理解・遵守、例外の報告
罰則適用	刑罰などの罰則があることの周知、社内の罰則の制定、周知、契約・誓約取得、違反者への罰則適用	罰則があることの認識、社内罰則合意の誓約・契約、罰受入・損害賠償

5.関連法令要求事項を考慮したISMS情報セキュリティ対策

法令対応を加味した ISO27001 ISMSリスクマネジメント



5.関連法令要求事項を考慮したISMS情報セキュリティ対策

「営業秘密保護」の考慮に伴うISMS情報セキュリティ対策の変更点

(1) 「営業秘密」の3要件を満たすための配慮が重要である。
（第2条第6項①秘密管理性、②有用性、③非公知性）

(2) 従業員による、秘密情報の売却、産業スパイ行為 などの不正を想定して、対策を講じる必要がある。

(3) 従業員の不正が不正アクセス防止法や不正競争防止法に対する違反であると証明できる根拠と証拠を保持し、不正持ち出しされた情報の差し止めや返還の訴訟に勝てるように、仕組みを整備しておく必要がある。

(4) 法令対策を講じる際には、リスク受容基準の判断による緩和は禁物である。 内部の者による不正発生の可能性を見積るよりも、内部の者の不正があった場合の影響の大きさを見積って、それを判断して対策を講じるべきである。

6. 課題と今後の進め方

(1)「4-3. 情報セキュリティ関連法令による要求事項の一般的な特性」のような特性ベースで研究と考察を行ったので、具体的なガイドラインや JIS Q 27002などでガイドされている管理策のレベルまで紐付した上での検討は未実施で、更に 詳細レベルの検討と検証が必要。

(2) マイナンバー制度、個人情報保護法やそれらのガイドライン改正のフォローが必要。

(3) ガイドライン「営業秘密管理指針」の改訂に伴って今後発行される詳細なガイドマニュアルのフォローが必要。

この「営業秘密保護マニュアル」で高度の包括的対策が示されると思われる。
なお、不正競争防止法の「罰則を適用しやすくした」の改正に関し、従業者に「罰則適用が強化された」ことを注意喚起する必要がある。

ISMS情報セキュリティ対策における営業秘密保護の考察

ご清聴ありがとうございました

