2016.06.03JSSA大会

情報セキュリティ対策における営業秘密保護の考察

Study of including “the protection of the trade secret ”
in the information security management system.

2016年06月03日

情報セキュリティ合同研究会

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

0. はじめに：情報セキュリティ研究プロジェクトの活動

情報セキュリティ専門監査人部会と合同で研究プロジェクトを開催（主査：川辺良和氏）

研究テーマと概要：　中小組織を対象に、主としてマネジメントの側面に着目して
情報セキュリティの諸問題を取り上げ、セキュリティの確立と強化のために
有効な考え方や具体的実施策を提案し利用してもらうことを目標にしている。

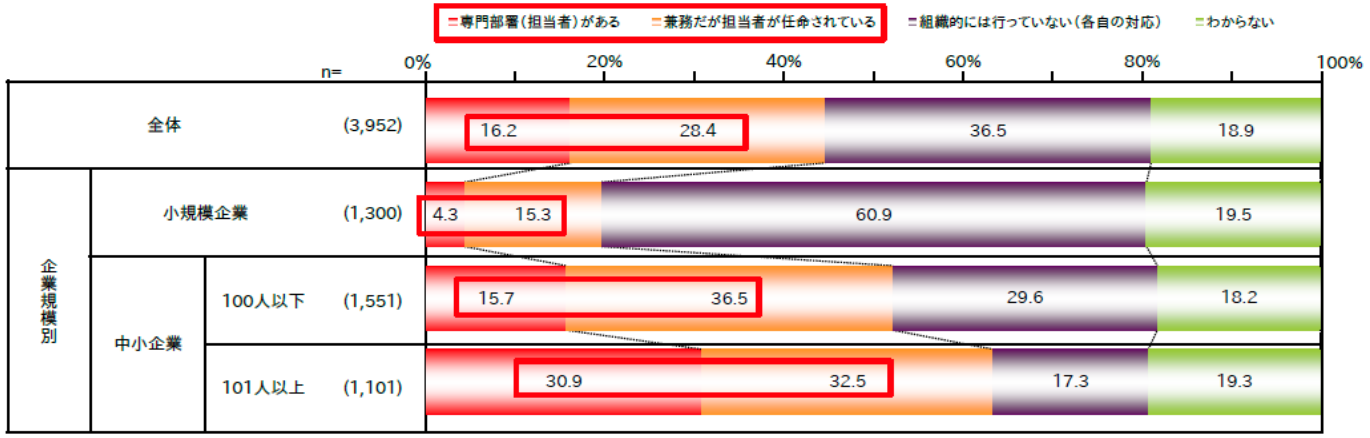
研究対象となる組織：以下のIPA調査報告で示されるような状況にある中小組織

情報セキュリティ対策に関する組織的な体制の実態

情報セキュリティ対策担当者がいる小規模企業は19.6%

- “情報セキュリティ対策に係る専門部署または担当者”がいる割合は、
小規模企業で19.6%、100人以下の中小企業で52.2%、101人以上の中小企業で63.4%　である。

Q22　貴社の情報セキュリティ対策はどのような体制で行われていますか。（ひとつだけ）



出典：IPA「2015年度 中小企業における情報セキュリティ対策に関する実態調査」報告書について（2016年3月8日）

1．研究の背景とねらい

1-1 情報セキュリティ対策と秘密情報流出事件

情報セキュリティ対策では、一般に、
①ISO27001 ISMS規格に沿ってマネジメントシステムを構築し、
②「ISO27001の付属書Aの管理策」及び「ISO27002 で推奨されている実施策」から選択・採用して、情報セキュリティ対策の仕組みを整備し、運用する。

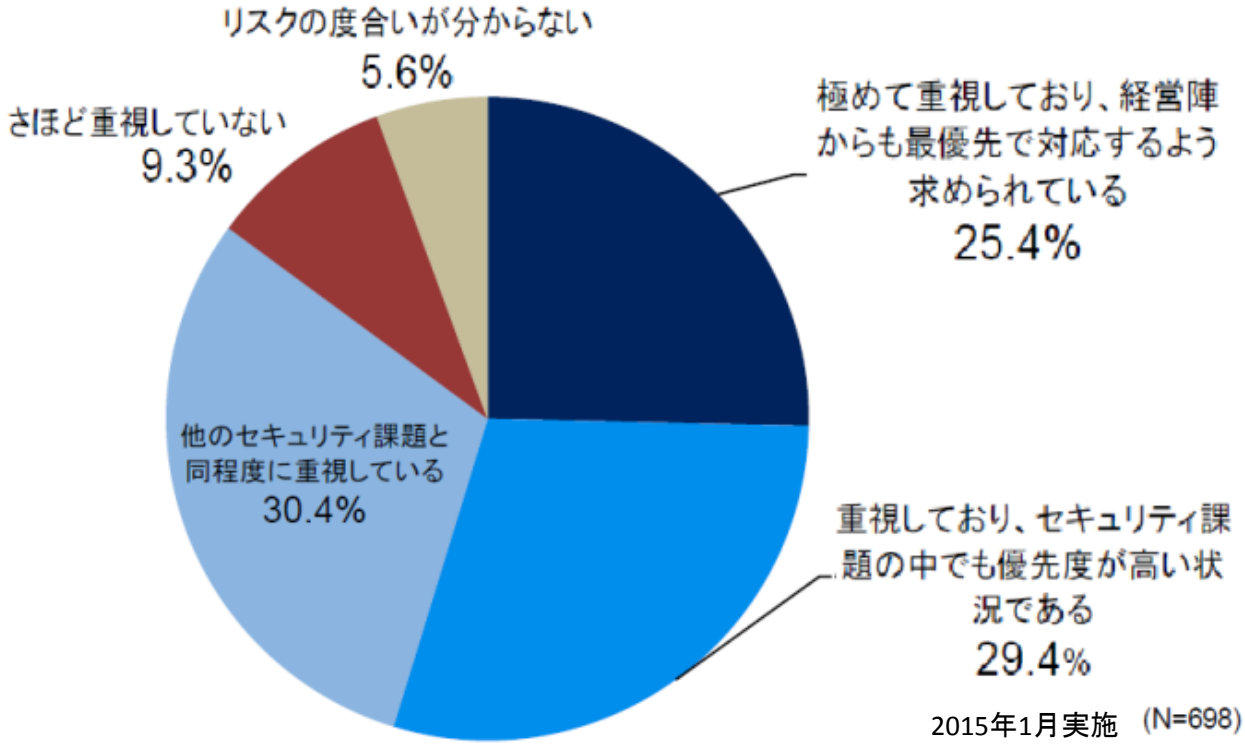
しかし、このように整備された情報セキュリティ対策の仕組みの裏を掻い潜って、
◆秘密情報を不正持ち出して競合企業や名簿業者等に持ち込むという事件、
◆標的型メールなどでウィルスを感染させ個人データを盗むという外部攻撃、
が繰り返し発生している。

典型的な例として、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）
・顧客データが委託先従事者によって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）
・標的型メール攻撃を受けて、従業員のパソコンから年金個人情報が漏洩したという事件（2015年6月）

1．研究の背景とねらい

1-2 高まる内部犯行による秘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の度合い



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

1-3 秘密情報流出の脅威

IPAの最近の「情報セキュリティ10大脅威」にみる秘密情報流出の脅威

	１０大脅威２０１３	１０大脅威２０１４	１０大脅威２０１５	１０大脅威２０１６
1位	クライアントソフトの脆弱性を突いた攻撃	標的型メールを用いた組織へのスパイ・諜報活動	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	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
2位	標的型諜報攻撃の脅威	不正ログイン・不正利用	内部不正による情報漏えい	標的型攻撃による情報流出
3位	スマートデバイスを狙った悪意あるアプリの横行	ウェブサイトの改ざん	標的型攻撃による諜報活動	ランサムウェアを使った詐欺・恐喝
4位	ウイルスを使った遠隔操作	ウェブサービスからの利用者情報の漏えい	ウェブサービスへの不正ログイン	ウェブサービスからの個人情報の窃取
5位	金銭窃取を目的としたウイルスの横行	オンラインバンキングからの不正送金	ウェブサービスからの顧客情報の窃取	ウェブサービスへの不正ログイン
6位	予期せぬ業務停止	悪意あるスマートフォンアプリ	ハッカー集団によるサイバーテロ	ウェブサイトの改ざん
7位	ウェブサイトを狙った攻撃	SNSへの不適切な情報公開	ウェブサイトの改ざん	審査をすり抜け公式マーケットに紛れ込んだスマフォアプリ
8位	パスワード流出の脅威	紛失や設定不備による情報漏えい	インターネット基盤技術を悪用した攻撃	内部不正による情報漏えいとそれに伴う業務停止
9位	内部犯行	ウイルスを使った詐欺・恐喝	脆弱性公表に伴う攻撃	巧妙・悪質化するワンクリック請求
10位	フィッシング詐欺	サービス妨害	悪意のあるスマートフォンアプリ	脆弱性対策情報の公開に伴い公知となる脆弱性の悪用増加

出典：IPAの「情報セキュリティ10大脅威2016」（2016年3月31日）

1．研究の背景とねらい

1-4 情報セキュリティ対策で どう営業秘密を守るか

これら悪意ある意図的な情報漏洩事件では、
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)

ISO27001 ISMS規格に沿ったマネジメントシステム、及び、
「ISO27001の付属書Aの管理策」と「ISO27002の実施策ガイド」を参考に
選択・採用した対策で、これらの犯罪行為から秘密情報を守る必要がある。

しかし「 ISO27001の付属書Aの管理策」と「 ISO27002の実施策ガイド」を
参考に情報セキュリティ対策を選択・採用しようとしても、
「営業秘密」とか「不正競争防止法」とかいう言葉は現れてこないので、
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、ISO27001/ISO27002に沿った情報セキュリティ対策で、
有効な「営業秘密の保護」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. 情報セキュリティ対策と関連法令との関係（問題提起）

2-1　ISO27001/ISO27002情報セキュリティ管理策による法令対応

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
⇒①関連法令・規制・契約上の要求事項と、②③これらの要求事項を満たすための組織の取組みを特定

【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
：	

①関連法令と要求事項を特定・周知

③対策手順化

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・保管方法の管理
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・番号法対応

②対策手順化

2. 情報セキュリティ対策と関連法令との関係

2-2　ISO27001/ISO27002管理策で対策が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

⇒ **①関連法令・規制・契約上の要求事項の特定**

③これらの要求事項を満たすための組織の取組みを特定

【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

①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

2. 情報セキュリティ対策と関連法令との関係

2-2　ISO27001/ISO27002管理策で対策が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

⇒ ①関連法令・規制・契約上の要求事項の特定

③これらの要求事項を満たすための組織の取組みを特定 → 未実施

【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

① 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。

③対策 手順化

問題

法令要求事項に対する「対策の追加と手順化」が行われていない

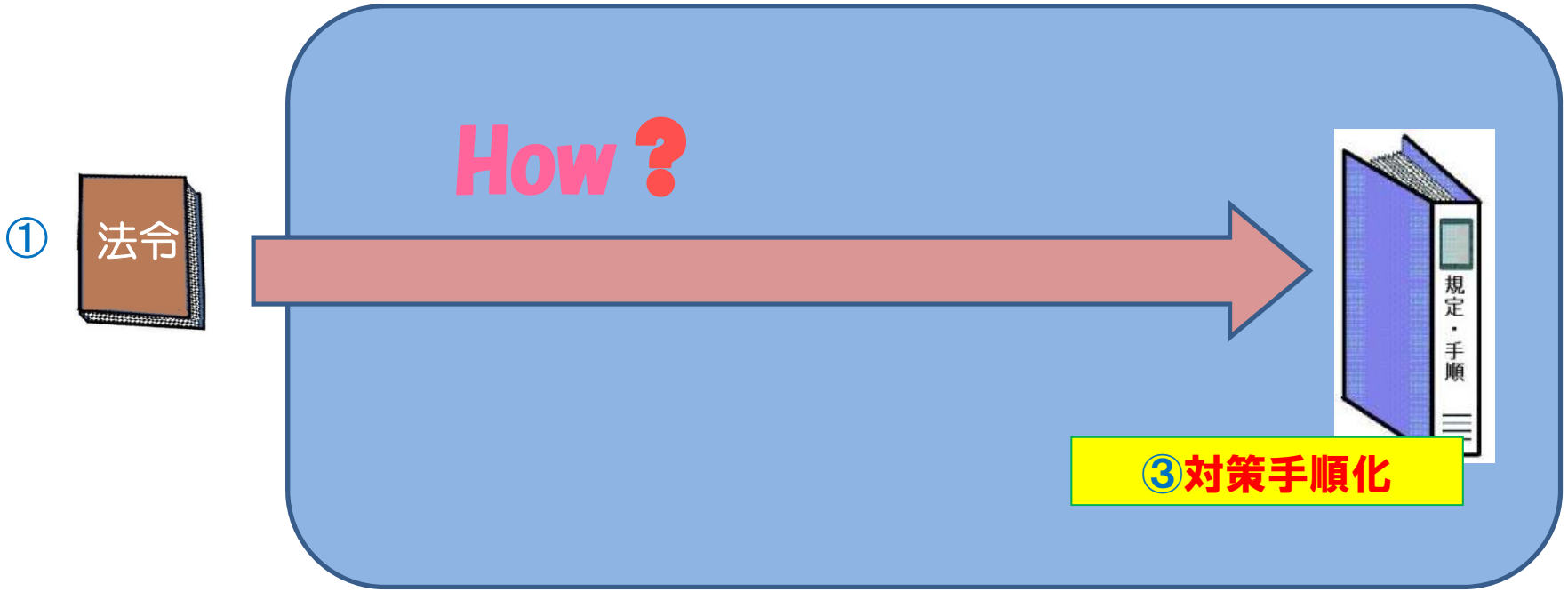
3. 関連法令要求事項を遵守するための対策の採用(課題)

3-1 関連法令要求から遵守するための対策を想定するのは困難

①関連法令と要求事項を特定する。

法令要求事項から「必要な対策を直接想定して手順化する」ことは困難

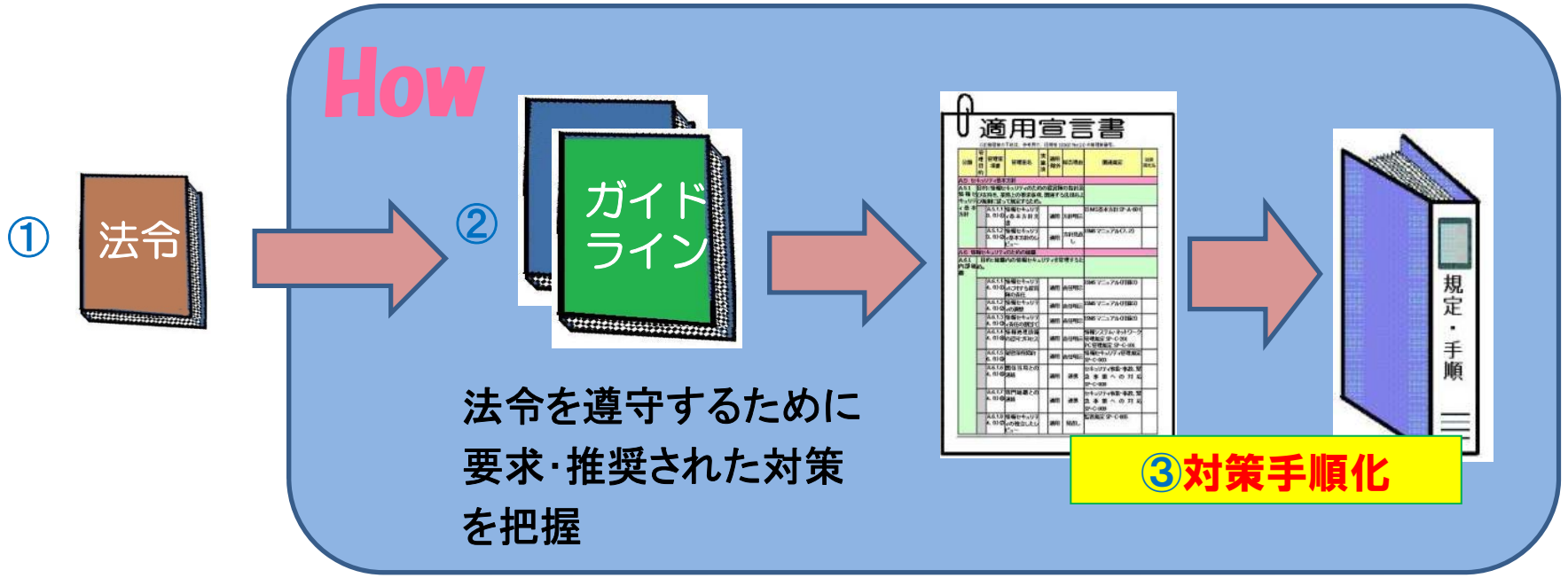
③対策を手順化する。



3. 関連法令要求事項を遵守するための管理策の採用

3-2. 関連法令に関するガイドラインを利用して管理策を把握

①関連法令の要求事項を特定する。
②法令を遵守するために要求・推奨された対策を把握する。・・・これが重要
③必要な対策を選択し、手順化する。



多くの組織で、この手順を踏まないため、
法令を遵守するための適切な対策が手順化されない。

3. 関連法令要求事項を遵守するための管理策の採用

3-3. 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（解決案1）

「 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、
法令の要求事項を
マネジメントシステムの視点による
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 標準パターン	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

・不正競争防止法(営業秘密) 及び 営業秘密管理指針
を基に要求事項を特定してみた。⇒　次スライド

他に以下についても試行してみた。
・個人情報保護法/JIS Q 15001個人情報保護マネジメントシステム
・不正アクセス禁止法

3. 関連法令要求事項を遵守するための管理策の採用

3-4.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を、3.3で提案したワークシートで整理した結果

前回報告はここまで

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. 営業秘密保護のためのガイドライン（調査結果）

最近発行されたので、追加検討した。

(注)「営業秘密」だけではなく、より幅広い「秘密情報」としてガイドされている。

4．1 営業秘密に関する法令とガイドラインの関係

不正競争防止法
（営業秘密関係）

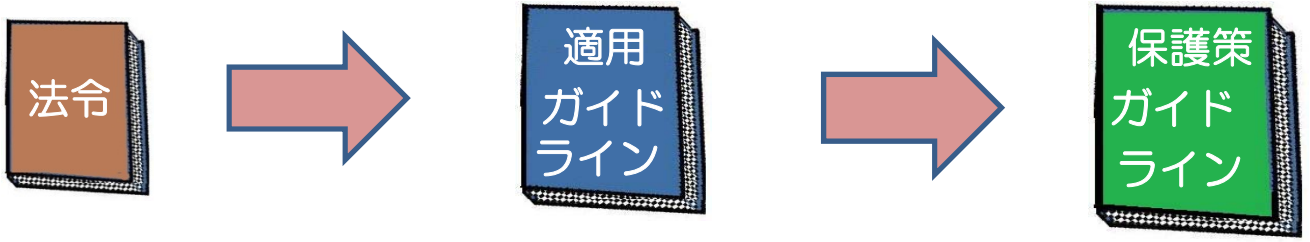
2条 定義
15項 6号　この法律において「営業秘密」とは、秘密として管理されている生産方法、販売方法その他の事業活動に有用な技術上又は営業上の情報であって、公然と知られていないものをいう。
4条 損害賠償請求権
5条 損害額・不正使用の推定
7条 侵害行為立証時の書類提出命令
10条 民事訴訟時の保護
21条 懲役・罰金・不当収益没収

営業秘密管理指針
営業秘密として法的保護を受けるために必要となる最低限の水準の対策を示す。

2．秘密管理性について
(1)秘密管理性要件の趣旨
(2)必要な秘密管理措置の程度
(3)秘密管理措置の具体例（媒体別）
(4)社内外で営業秘密を共有する場合の秘密管理性の考え方
3．有用性の考え方
4．非公知性の考え方

秘密情報(注)の保護ハンドブック
秘密情報を決定する際の考え方や、その漏えい防止のために講ずるべき対策例、万一情報が漏えいした場合の対応方法等を示す。

第2章 保有情報の把握・評価、秘密情報決定
第3章 3-1 秘密情報の分類
3-2 分類に応じた情報漏洩対策選択
3-3 秘密情報の取扱方法等ルール化
3-4 具体的な情報漏えい対策例
第4章 秘密情報管理の社内体制のあり方
第5章 他社の秘密情報に係る紛争への備え
第6章 漏えい事案への対応

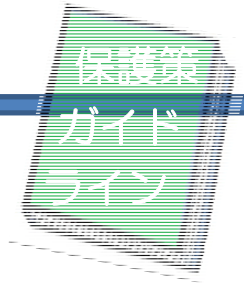


「不正競争防止法」
（昭和9年法律第14号、
平成27年7月10日
法律第54号全面改正）

「営業秘密管理指針」
（平成15年1月30日制定、
平成25年8月16日改訂、
平成27年1月28日全面改訂）

「秘密情報の保護ハンドブック
～企業価値向上に向けて～」
（経済産業省平成28年2月8日発行）

4. 営業秘密保護のためのガイドライン

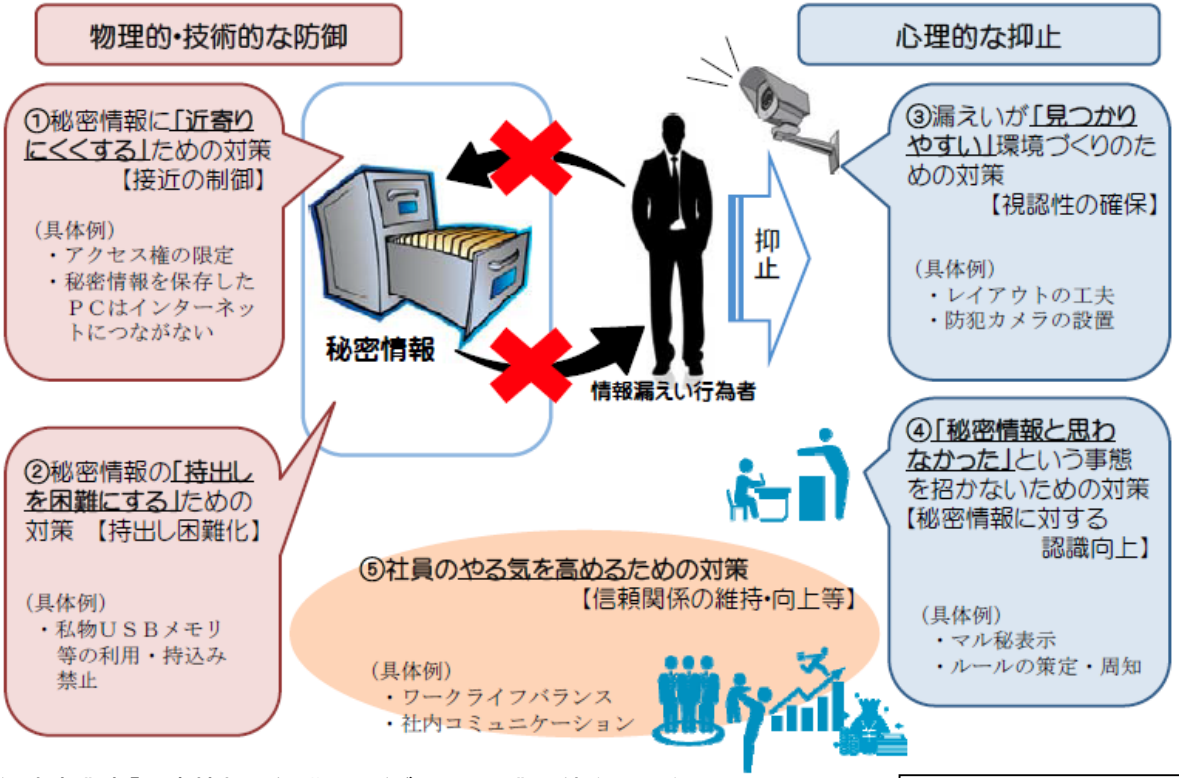


4．2「秘密情報の保護ハンドブック」とは

★場所・状況・環境に潜む「機会」が犯罪を誘発する という犯罪学の考え方なども参考

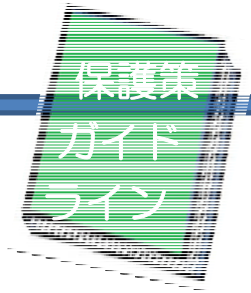
★秘密情報の漏えい要因　となる事情 を考慮

⇒5つの「対策の目的」を設定



出典：経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～」のP18の 図表3（1）5つの対策の目的 を引用

4. 営業秘密保護のためのガイドライン



4．3「秘密情報の保護ハンドブック」 5つの対策の目的　とは

物理的な防御

（1）接近の制御
目的：アクセス権限がない者を秘密情報に近づけないようにする。

（2）持出し困難化
目的：秘密情報を無断で複製したり持ち出すことを物理的、技術的に阻止する。

心理的な抑止

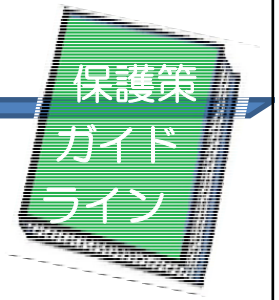
（3）視認性の確保
目的：秘密情報への接触が記録されたり、他人に目撃されたり、事後的に分かるような環境によって、漏えい行為が見つかると認識させる。

（4）秘密情報に対する認識向上（不正行為者の言い逃れの排除）
目的：情報漏えいを行う者に「秘密情報・社外持出禁止だと知らなかった」というような言い逃れができないようにする。

（5）信頼関係の維持・向上等
目的：秘密情報の管理に関する意識を向上させる。
(企業の生産性向上や効率的な経営の実現などの観点からも重要)

出典：経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～」

4. 営業秘密保護のためのガイドライン



4．4「秘密情報の保護ハンドブック」5つの対策例

（1）**接近の制御**：アクセス権限がない者を秘密情報に近づけないようにする。
- 対策例：①当該情報について知るべき者にだけアクセス権を与える正式なルールを策定
- ②秘密情報に対するアクセス権者の範囲を適切に設定
- ③施錠管理・入退室制限等の区域制限、等

（2）**持出し困難化**：秘密情報を無断で複製したり持ち出すことを物理的、技術的に阻止する。
- 対策例：①秘密情報が記載された会議資料等の回収
- ②PCの固定
- ③記録媒体の複製制限
- ④従業員の私物メモリの持込み・利用を制限

（3）**視認性の確保**：漏えい行為が見つかると認識させる
- 対策例：①職場のレイアウトの工夫
- ②資料・ファイルの通し番号管理
- ③録画機能付き防犯カメラの設置
- ④入退室の記録
- ⑤PCのログ確認、等

（4）**秘密情報に対する認識向上**：「知らなかった」というような言い逃れができないようにする。
- 対策例：①秘密情報の取扱い方法等に関するルールの周知し
- ②秘密情報が記録された媒体へ秘密表示、等

（5）**信頼関係の維持・向上等**：秘密情報の管理に関する意識を向上させる。
- 対策例：①情報漏えいと結果について事例を周知
- ②働きやすい職場環境の整備や適正な評価等による、企業帰属意識の醸成、モチベーションの向上
- ③職場のモラルや従業員等との信頼関係を維持・向上

出典：経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～」

4. 営業秘密保護のためのガイドライン

4．5 「秘密情報の保護ハンドブック」対策 のISMS管理策 との比較

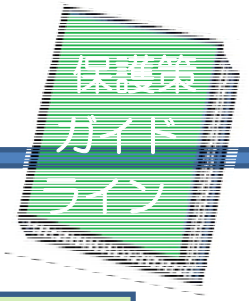
参考資料1の「情報漏えい対策一覧」で示されている対策をISMSと比較した

ガイドライン参考資料1の情報漏えい対策一覧	解説ページ	関連ISMS管理策
1．従業員等に向けた対策		
①「接近の制御」		
a. ルールに基づく適切なアクセス権の付与・管理	26	A.9.1.1 A.9.1.2 A.8.1.3 A.9.4.1 A.9.2.2 A.7.3.1 A.9.2.6 A.9.2.5
b. 情報システムにおけるアクセス権者のID登録	27	A.9.2.1 A.9.2.4 A.9.3.1 A.9.4.2 A.9.4.3
c. 分離保管による秘密情報へのアクセス制限	29	A.8.2.1 A.8.2.2 A.8.2.3 A.8.3.1 A.11.1.1 A.11.1.2 A.11.1.3 A.11.2.9 A.9.1.1 A.13.1.3
d. ペーパーレス化	33	該当なし
e. 秘密情報の復元が困難な廃棄・消去方法の選択	33	A.8.3.2 A.11.2.7
②「持出し困難化」		
【書類、記録媒体、物自体等の持出しを困難にする措置】		
a. 秘密情報が記された会議資料等の適切な回収	35	A.8.2.3
b. 秘密情報の社外持出しを物理的に阻止する措置	35	A.11.2.5
c. 電子データの暗号化による閲覧制限等	35	A.8.2.3 A.10.1.1 A.10.1.2
d. 遠隔操作によるデータ消去機能を有するPC・電子データの利用	36	A.6.2.1
【電子データの外部送信による持出しを困難にする措置】		
e. 社外へのメール送信・Webアクセスの制限	36	A.9.1.2 A.13.2.3
f. 電子データの暗号化による閲覧制限等（再掲）	36	A.8.2.3 A.10.1.1 A.10.1.2
g. 遠隔操作によるデータ消去機能を有するPC・電子データの利用（再掲）	36	A.6.2.1
【秘密情報の複製を困難にする措置】		
h. コピー防止用紙やコピーガード付の記録媒体・電子データ等により秘密情報を保管	37	該当なし
i. コピー機の使用制限	37	A.11.2.8
j. 私物のUSBメモリや情報機器、カメラ等の記録媒体・撮影機器の業務利用・持込の制限	37	該当なし
【アクセス権変更に伴いアクセス権を有しなくなった者に対する措置】		
k. 秘密情報の消去・返還	39	A.8.1.4 A.6.1.5 A.13.2.4

参考：経済産業省「秘密情報の保護ハンドブック～企業価値向上に向けて～」

ISMS管理策には無いような対策が「秘密情報の保護ハンドブック」にはあり、
秘密情報の保護のために「秘密情報の保護ハンドブック」の活用が必須といえる。

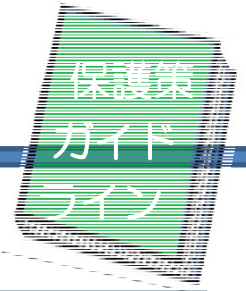
5. ガイドラインの活用方法（研究）



5．1 「秘密情報の保護ハンドブック」の活用方法の検討結果

活　用　方　法	特徴 マネジメントシステム	特徴 管理策/実施策
①「秘密情報の保護ハンドブック」単体で 秘密情報保護の仕組みを構築する。	独　自	当該ハンドブック
② ISO31000リスクマネジメントで 秘密情報の保護を目的に、 「秘密情報の保護ハンドブック」を参考に リスクと管理目標、リスク対応選択肢を決定	ISO31000 リスクマネジメント	当該ハンドブック
③ ISO27001のISMSで、 主たる管理策ガイドラインとして 「秘密情報の保護ハンドブック」を参照	ISO27001　ISMS	当該ハンドブック
④ ISO27001のISMSで、管理策ガイドラインとして「ISO27001管理策/ISO27002実施策」に加えて、「秘密情報の保護ハンドブック」を参照	ISO27001　ISMS	ISO27001管理策 ISO27002実施策 ＋ 当該ハンドブック

5. ガイドラインの活用方法



5．2「秘密情報の保護ハンドブック」の活用方法毎の適用組織の検討結果

適用組織

活用方法	マネジメントシステム	管理策/実施策
①「秘密情報の保護ハンドブック」単体で秘密情報保護の仕組みを構築する。	独　自	当該ハンドブック
	企業リスクマネジメント（ERM）も、ISO27001 ISMSも、構築予定のない組織向き	
② ISO31000リスクマネジメントで秘密情報の保護を目的に、「秘密情報の保護ハンドブック」を参考にリスクと管理目標、リスク対応選択肢を決定	ISO31000 リスクマネジメント	当該ハンドブック
	企業リスクマネジメント（ERM）構築済み 又は 予定のある組織向き	
③ ISO27001のISMSで、主たる管理策ガイドラインとして「秘密情報の保護ハンドブック」を参照	ISO27001　ISMS	当該ハンドブック
	将来ISO27001 ISMS構築予定のある組織向き	
④ ISO27001のISMSで、管理策ガイドラインとして「ISO27001管理策/ISO27002実施策」に加えて、「秘密情報の保護ハンドブック」を参照	ISO27001　ISMS	ISO27001管理策 ISO27002実施策 ＋ 当該ハンドブック
	ISO27001 ISMS構築済みの組織向き	

6. 課題と今後の進め方

＜当研究の深化＞

(1) さらなる詳細検討を進め、研究の深堀と検証

特にISO27001 ISMSを前提としないで、例えば「秘密情報の保護ハンドブック」を、
・企業のリスクマネジメント（ERM）の一環として取り組む場合、又は、
・対策だけ採用する場合、
の詳細検討など。

(2) この研究を研究論文として纏める

＜新テーマ研究＞

(3) 経産省-IPAの「サイバーセキュリティ経営ガイドライン」の 中小組織への活用の研究

（2015.12.28発行）

従来から、サイバー攻撃への対策は色々検討されているが、「サイバー攻撃」は防ぎきれないと認めて、サイバー攻撃を受けた場合に備えて、早期発見、初動対応、顧客・取引先への通知等を含めた緊急時の体制整備の項目を洗い出す。経営者がこれらを認識して取組み、適切な公表・通知を行うことは、訴訟リスクの面からも重要。

(4) ISO27017クラウドセキュリティ管理策 の 中小組織への活用の研究

ビジネス変化への迅速な対応やＩＴコスト低減のために、今やクラウドコンピューティングの利用は必須の状況。フットワークの良い中小組織こそ、利用しやすいとも言える。しかし、予期せぬ停止やデータの喪失などのリスク想定とそれに備えた対応をすることが重要であり、これを分かりやすくガイドすることが必要。

など・・・

＜共通＞

(5) これら研究を進めるための研究プロジェクトメンバー募集

ご清聴ありがとうございました。

研究会は、さらに情報セキュリティとシステム監査の有効性と効率性を「深堀り」します。研究会への参画をお待ちしております。

情報セキュリティ合同研究会

＜2015年度　研　究　会　参　加　メ　ン　バ　ー＞
川辺 良和　【㈲インターギデオン】：主査
齋藤 敏雄　【日本大学】
山本　孟　【MHOアシストラボ】
高橋 孝治　【高橋孝治公認会計士事務所】
芳仲　宏　【東京地方裁判所】
長野 加代子【㈱ピーアンドアイ】
黒川 信弘　【黒川技術士・行政書士事務所】
高野 美久　【NECソリューションイノベータ㈱】
植野 俊雄　【ISU】：発表者