NPO 日本ネットワークセキュリティ協会
Japan Network Security Association

JNSA 2018年度活動報告会

「日本ISMSユーザグループ 成果報告」

日本ISMSユーザグループ
リーダー
魚脇 雅晴

活動報告の内容

1. 日本ISMSユーザグループとは？
2. JNSAに合流した経緯
3. 過去の活動状況のご紹介
4. 2018年の取り組み
5. 2019年の活動

日本ISMSユーザグループとは？

「日本ISMSユーザグループ(J-ISMSUG)」は、2004年より任意団体として活動していましたが、2018年からJNSA標準化部会に合流しました。

J-ISMSUGでは、ISMS認証取得企業とISMS専門家が、経験的な知識に基づく意見交換・議論を進めることでISMSの構築・運用に関わるベストプラクティスを提供し、**日本におけるISMS普及・促進に貢献する目的で活動**しています。

JNSAに合流した経緯

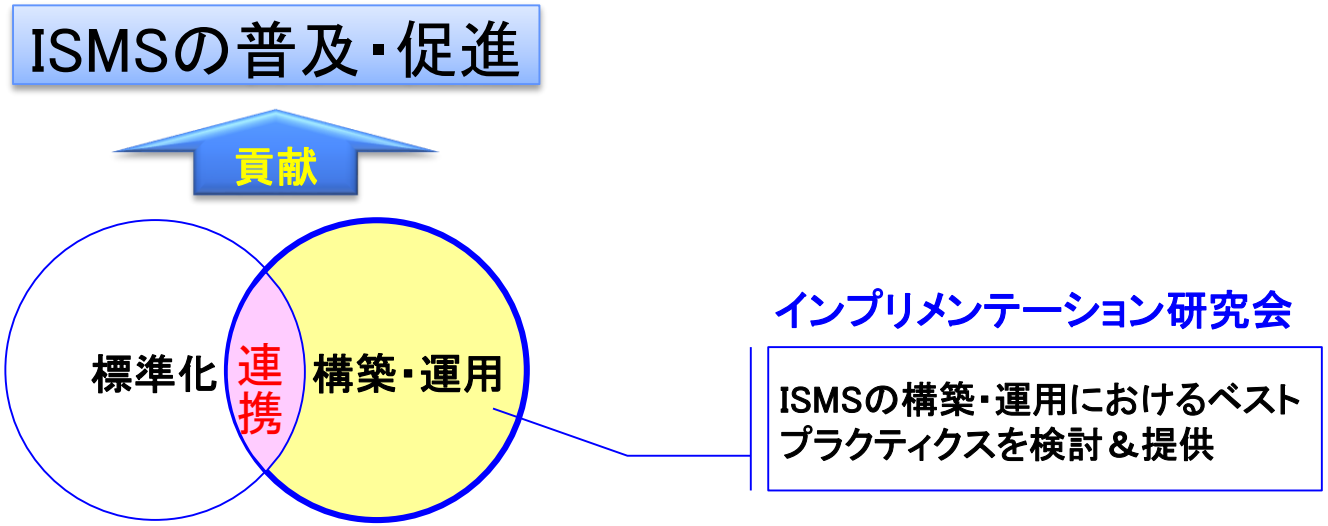
「日本ISMSユーザグループ(J-ISMSUG)」は、2004年より任意団体として活動しておりましたが、JNSAの広いセキュリティ活動と連結することで、その活動範囲/参加メンバの拡大、活動成果の有効活用を促進したく、この度JNSA標準化部会のWGとして新たに合流いたしました。

日本ISMSユーザグループ活動概要

JNSA

■活動目的と活動概要

J-ISMSUGではISMSを構築・運用する上で規格をどう読み解いて、企業活動にISMSを積極的に実践活用する方法を検討、研究し、国内外へ発信します。具体的にはISMS認証取得企業（ユーザ）とISMSの専門家が連携し、意見交換・議論を進めることで**ISMSの構築・運用に関わるユーザ視点でのベストプラクティスを提供し、日本における健全かつ効果的なISMS普及・促進に貢献する活動**を行っています。



活動概要

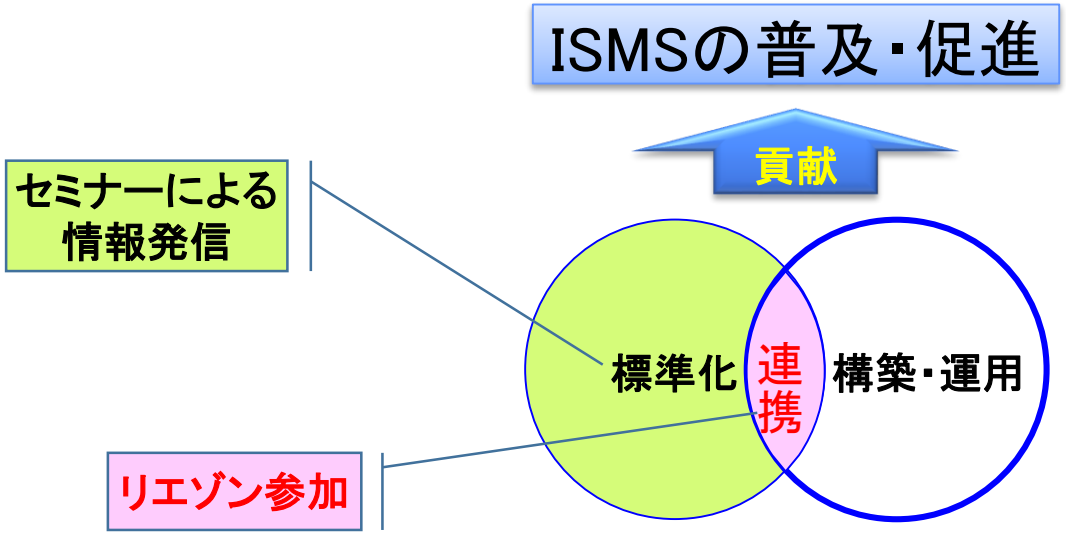
■標準化動向

①「情報処理学会 情報規格調査会　第1種専門委員会　SC 27/WG 1 小委員会」

上記の**アドフォック会議にリエゾンとして参加し、ユーザー目線で「理論的な正しさ」だけでなく、「現場で理解し、使いこなせること」と、「認証取得と維持・継続」という観点**で混乱が生じないように規格の作成や改正に関する方向性について意見を提言

②情報セキュリティセミナーでの標準化動向の発信

SC 27/WG 1 のメンバーによる規格の標準化動向＆解説

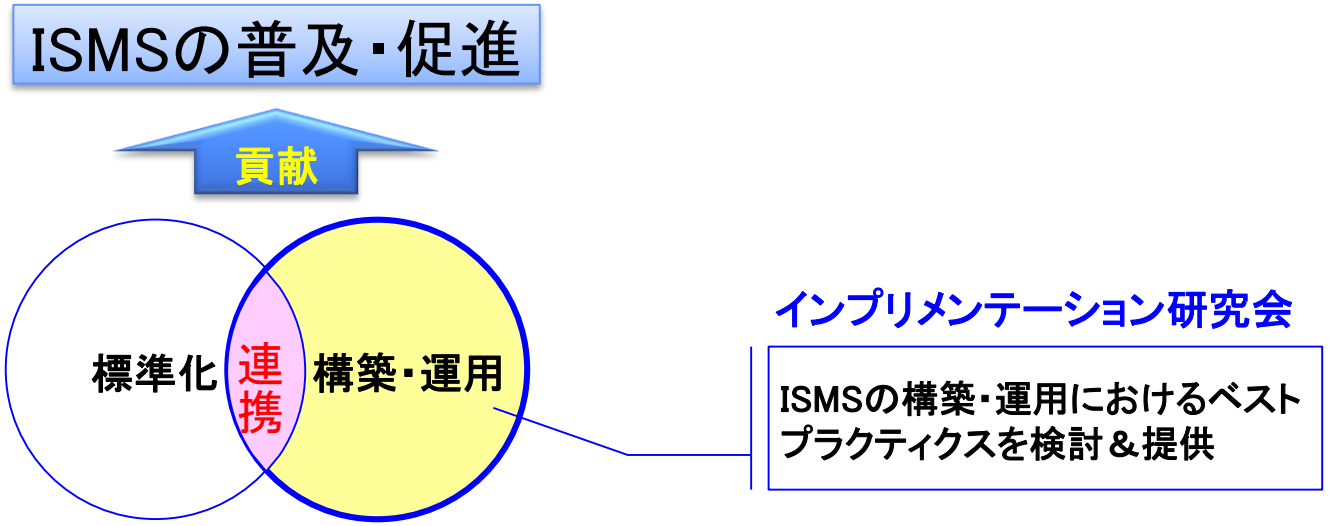


活動概要

■インプリメンテーション研究会

ISMSの導入・運用における諸問題の解決に関する研究

〇毎月最終木曜日に定例開催（18:00～21:00）
〇毎年2テーマを設定し、前半テーマ1、後半テーマ2を集中討議
〇研究会のテーマだけでなく、各社の疑問や悩みも解決
　（コンサル目線ではなく、実践経験に基づく回答・・・）
〇会員でなくともオブザーバー制度でお試し参加可能



過去の活動状況のご紹介
（2006～2012）

年度	インプリメンテーションWG	メジャメントWG
2006	■本WGの活動紹介＆ISMS導入に関する課題の事例紹介	■有効性測定の基本的な考え方＆取り組み事例紹介
2007	■情報セキュリティ研修・啓発 ■効率的リスクアセスメント	■有効性測定の基本的な考え方＆新たな取り組み事例紹介（進捗状況含む）
2008	■ISMS構築事例に見る有効性測定構築の傾向 ■業務委託先のセキュリティ評価	■有効性測定の基本的な考え方＆共通フレームワーク案（進捗状況含む）
2009	■標準的なリスク分類と具体的な管理策の対応のモデル化 ■管理策の有効性評価を効果的に行うモニタリング手法のモデル化	■ISO/IEC27001における「有効性測定」
2010	■標準的なリスク分類と具体的な管理策の対応のモデル化 ■管理策の有効性評価を効果的に行うモニタリング手法のモデル化	■ISO/IEC27001における「有効性測定」
2011	■可視化手法を用いたリスク対策モデル ■ISMS全体の有効性評価手法	■管理策の有効性測定
2012	■可視化手法を用いたリスク対策モデルとその実践的応用 ■ISMS実践手法　BCPのモデル化の検討	■管理策の有効性測定

過去の活動状況のご紹介
（2013～2018）

年度	インプリメンテーションWG	メジャメントWG
2013	■ISMS推進事務局の悩みと解決策 ■有効性評価に基づくISMS実践活用	メジャメントWGは有効性評価に関する成果を持って活動を休止。インプリメンテーション研究会に一本化して活動。
2014	■ISMS推進事務局の悩みと解決策 ■ISMS規格改訂にともなう実装方法の検討	
2015	■ISMSを成功させる理想的なCISOの条件 ■減らないインシデントの特効薬	
2016	■サイバー攻撃を事例としたリスクマネジメントの実践 ■運用フェーズにおける有効性の評価	
2017	■現場と連携したリスクアセスメント手法の実践活用 ■内部監査を有効に運用するための手法の考察	
2018	■ISMS規格要求事項から紐解く最新のビジネス環境リスク（サイバー攻撃、クラウド利用への対応方法についての考察） ■働き方改革における情報セキュリティ	

研究会での活動の成果の紹介

研究会では規格要求事項を実ビジネスに展開する上で単純に展開するだけでなく、**効率的＆有効な手法**を検討しています。

- 管理策の有効性測定
- **可視化手法（マインドマップ）を用いたリスク対策モデル**
- ISMSを成功させる理想的なCISOの条件
- 減らないインシデントの特効薬
- サイバー攻撃を事例としたリスクマネジメントの実践
- 現場と連携したリスクアセスメント手法の実践
- などなど

事例紹介
可視化手法（マインドマップ）を用いたリスク対策モデル

事例紹介

可視化手法を用いたリスク対策モデル
～　マインドマップを利用したリスクアセスメント手法　～

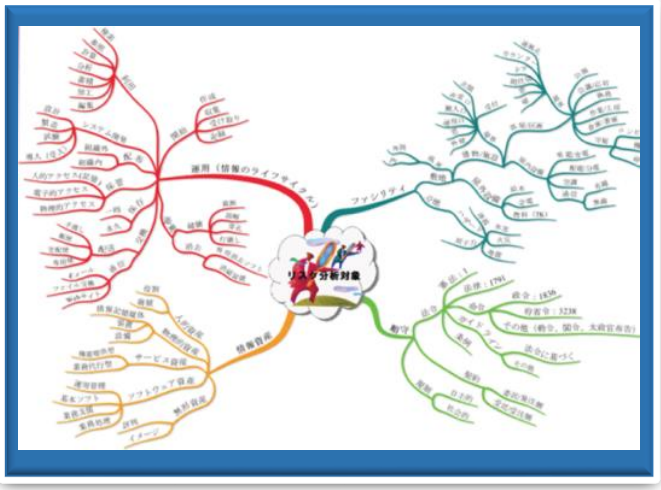
JNSA

情報資産の脅威とｾｷｭﾘﾃｨ事象（ｲﾝｼﾃﾞﾝﾄ含む）の関連を可視化 → 脅威が顕在化する要因となる脆弱性と対策（案）の検討

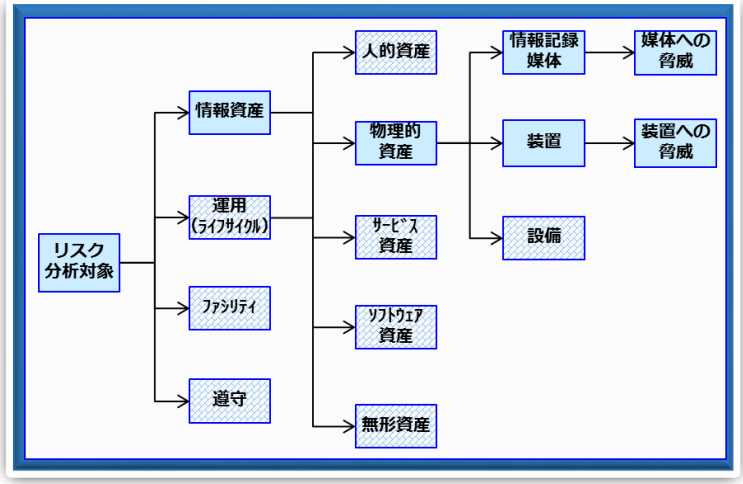
課題：複数のﾏｲﾝﾄﾞﾏｯﾌﾟに同様の脅威やｾｷｭﾘﾃｨ事象が出現して、使いにくい（脆弱性と対策（案）も重複）

情報資産を集約し、共通部分と個別の部分が判るようにする → ISMSの現場で使いやすいツールとして再整理

ﾏｲﾝﾄﾞﾏｯﾌﾟを利用したﾘｽｸｱｾｽﾒﾝﾄ手法



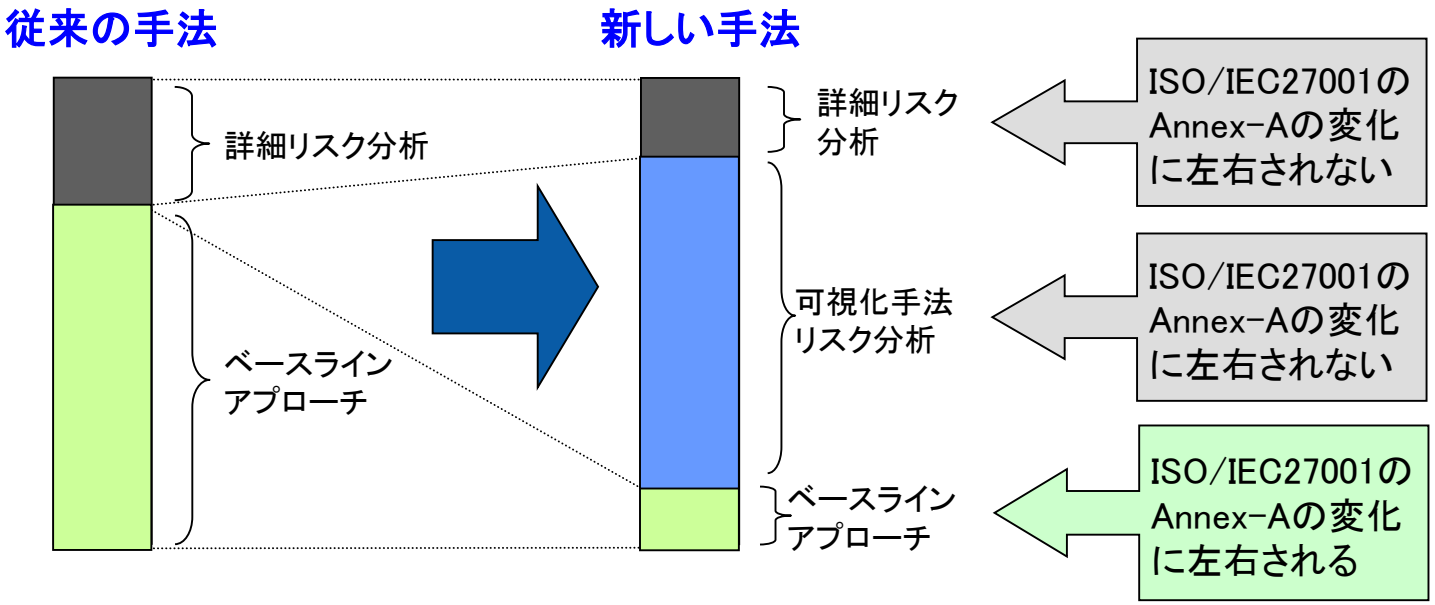
リスク分析対象　情報資産



可視化手法を用いたリスク対策モデル
～ マインドマップを利用したリスクアセスメント手法 ～

JNSA

リスクアセスメント可視化の手法の狙い

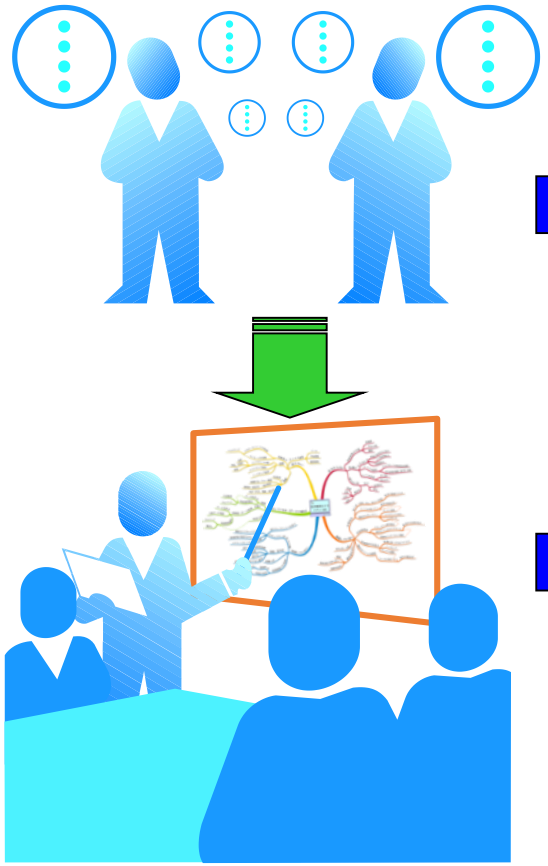


・可視化手法の採用によって、**27001/27002の改定（直近では2013改定）の影響を受けにくくし、ISMS構築組織の負担軽減を実現**する。

可視化手法を用いたリスク対策モデル
～ マインドマップを利用したリスクアセスメント手法 ～

JNSA

可視化手法は、なぜ「マインドマップ」なのか



詳細リスク分析で一般に行われる「ブレーンストーミング」は、各自の検討結果を知ることはできるが思考過程は共有することは困難である。

マインドマップは、分析者の思考過程が**「キーワードの連鎖」**の形で可視化されるため、参加者全員でその**思考過程を共有し、レビュー**することができる。

事例紹介

可視化手法を用いたリスク対策モデル
～　マインドマップを利用したリスクアセスメント手法　～

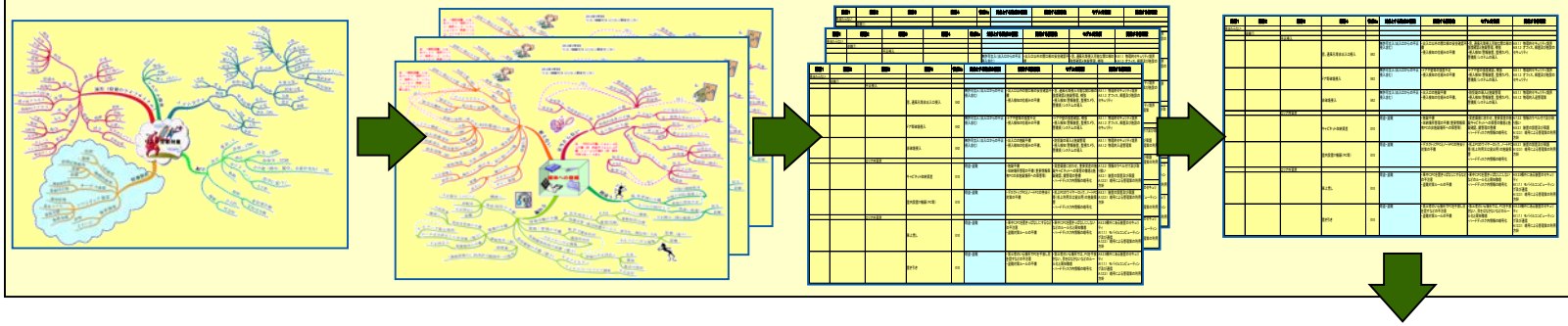
●この流れを維持することが、リスク対策の有効性の維持につながっている。

リスク分析対象のモデル化

個別対象のモデル化

脅威・脆弱性に対する対策リスト作成

対策リストの名寄せと整理



採用したリスク対策リスト（実装管理策）

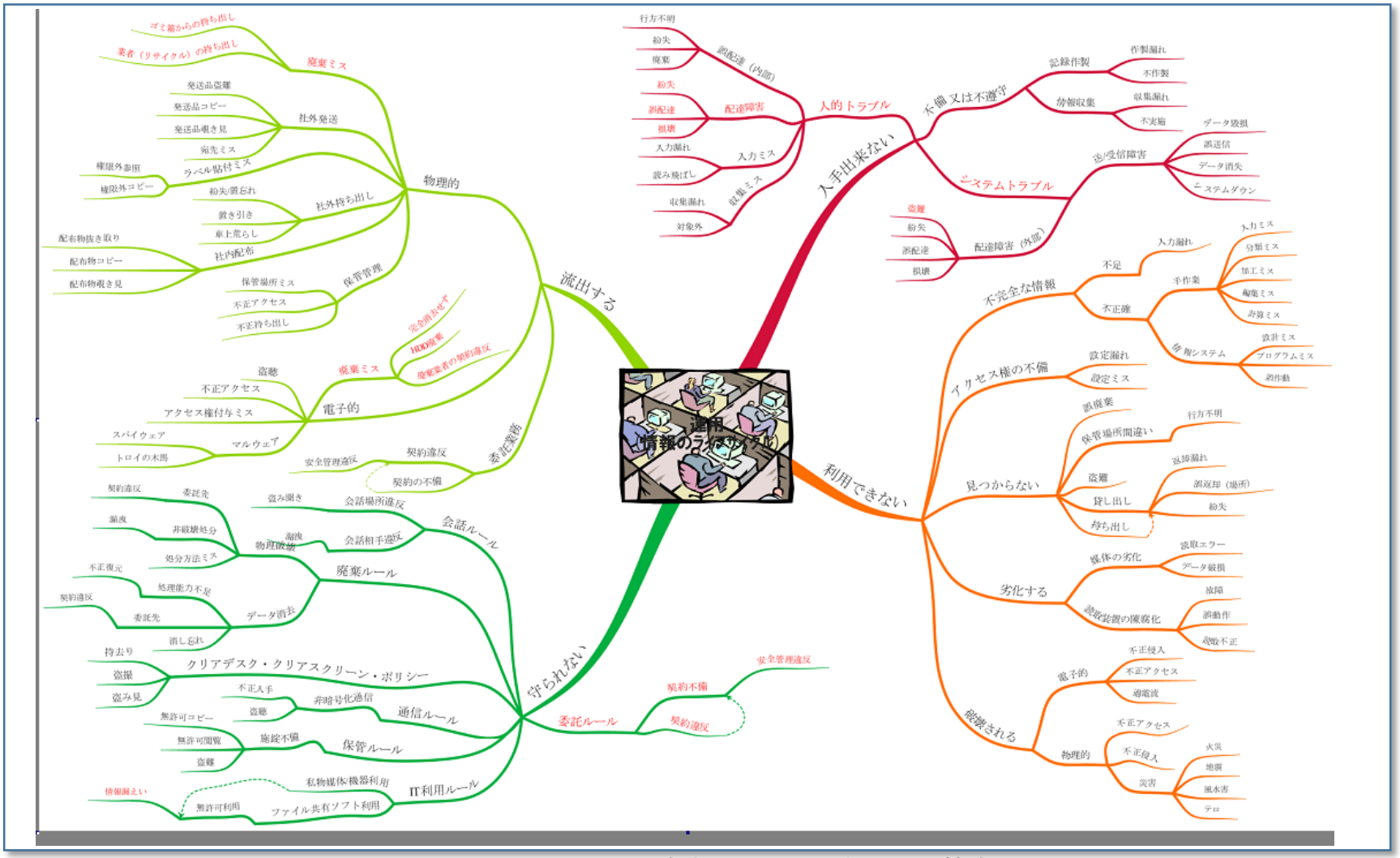
◯リスク分析可視化の効果

・リスク分析対象から最終的なリスク対策の採用まで、一貫した流れの元で管理ができる
・それぞれの**モデル、又はリストに関連する変化が起きた場合、どの部分に影響が及ぶかの特定が容易**（リスク対策の陳腐化の防止）
・**リスクアセスメントを体系化することにより、リスクアセスメント要員が交替した場合でも、その考え方、手順が維持することが可能。**

事例紹介

可視化手法を用いたリスク対策モデル
～　マインドマップを利用したリスクアセスメント手法　～

JNSA



事例紹介

リスク対策モデル「脅威と対策一覧」

JNSA

①マインドマップ応用の脅威関連図から作成

②脅威の分類を体系化し、対策の実装を支援する

③マインドマップの4階層の内容を基に関連する脆弱性とモデル対策を記入する

階層1	階層2	階層3	階層4	脅威No	対象とする脅威の種類	関連する脆弱性	モデル対策例	関連する管理策
見当たらない								
	盗難①							
		不正侵入						
			窓、通風孔等非出入口侵入	042	無許可立入(出入口からの不正侵入含む)	出入口以外の開口部の安全確認不備 侵入検知の仕組みの不備	・窓、通風孔等侵入可能な開口部の強度確認と施錠管理、補強 ・侵入検知(警報装置、監視カメラ、警備員)システムの導入	A.9.1.1 物理的セキュリティ境界 A.9.1.3 オフィス、部屋及び施設のセキュリティ
			ドア等破壊侵入	042	無許可立入(出入口からの不正侵入含む)	ドアや壁等の強度不足 侵入検知の仕組みの不備	・ドアや壁の強度確認、補強 ・侵入検知(警報装置、監視カメラ、警備員)システムの導入	A.9.1.1 物理的セキュリティ境界 A.9.1.3 オフィス、部屋及び施設のセキュリティ
			非破壊侵入	042	無許可立入(出入口からの不正侵入含む)	出入口の施錠不備 侵入検知の仕組みの不備、	・防犯錠の導入と施錠管理 ・侵入検知(警報装置、監視カメラ、警備員)システムの導入	A.9.1.1 物理的セキュリティ境界 A.9.1.2 物理的入退管理策
		エリア内資産						
			キャビネット収納資産	010	窃盗・盗難	施錠不備 収納場所管理の不備(重要情報保有PCの非施錠場所への保管等)	・資産価値に合わせ、重要資産の施錠キャビネットへの保管の徹底と施錠確認、鍵管理の整備 ・ハードディスク内情報の暗号化	A.7.2.2 情報のラベル付け及び取り扱い A.9.2.1 装置の設置及び保護 A.12.3.1 暗号による管理策の利用方針
			室内設置IT機器(PC等)	010	窃盗・盗難	デスクトップPCとノートPCの持去り対策の不備	・机上PCのワイヤーロック、ノートPC等(机上利用又は貸出用)の施錠保管 ・ハードディスク内情報の暗号化	A.9.2.1 装置の設置及び保護 A.12.3.1 暗号による管理策の利用方針
		エリア外資産						
			車上荒し	010	窃盗・盗難	車中にPCを置きっぱなしにするなどの不注意 盗難対策ルールの不備	・車中にPCを置きっぱなしにしないなどのルール化と周知徹底 ・ハードディスク内情報の暗号化	A.9.2.5構外にある装置のセキュリティ A11.7.1 モバイルコンピューティング及び通信 A.12.3.1 暗号による管理策の利用方針
			置き引き	010	窃盗・盗難	第三者のいる場所でPCを手放し目話すなどの不注意 盗難対策ルールの不備	・第三者のいる場所では、PCを手放さない、目をはなさないなどのルール化と周知徹底 ・ハードディスク内情報の暗号化	A.9.2.5構外にある装置のセキュリティ A11.7.1 モバイルコンピューティング及び通信 A.12.3.1 暗号による管理策の利用方針

2018年の取り組み

■インプリメンテーション研究会 （毎月最終木曜日開催）

・ISMS規格要求事項から紐解く最新のビジネス環境リスク
（サイバー攻撃、クラウド利用への対応方法についての考察）
・働き方改革における情報セキュリティ

■Workshop（Prof. Edward Humphreys とのディスカッション） （4/13）

■情報セキュリティマネジメントセミナー （12/7）

【標準化動向】
・「ISO/IEC 27000ファミリー規格の最新動向」
・「サイバーセキュリティの概念－国際標準化の動向を背景に－」
・「IoTセキュリティガイドラインの国際標準化動向」

【研究会成果報告】
・「ISMS規格要求事項から紐解く最新のビジネス環境リスク（サイバー攻撃、
クラウド利用への対応方法についての考察）」
・「働き方改革における情報セキュリティ」

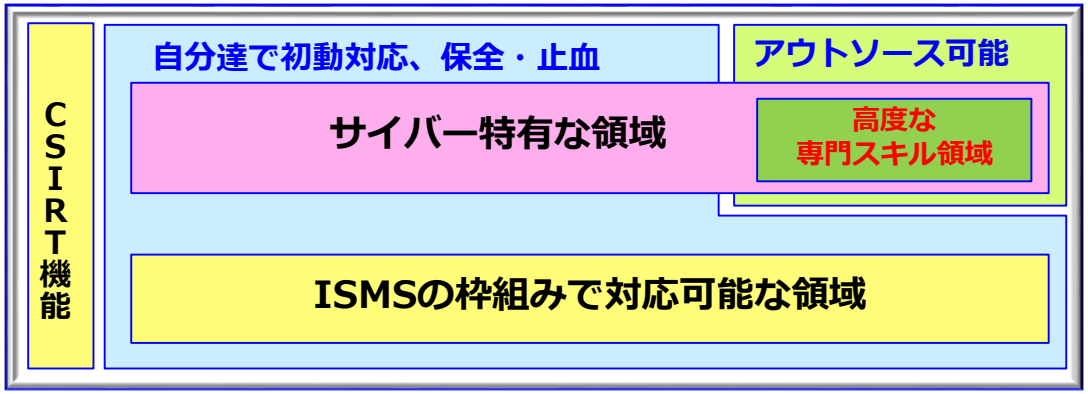
2018年の取り組み
■インプリメンテーション研究会 （テーマ概要）

NO	テーマ名	テーマ概要
1	ISMS規格要求事項から紐解く 最新のビジネス環境リスク （サイバー攻撃、クラウド利用への対応方法についての考察）	企業を取り巻くビジネス環境はめまぐるしく変化しており**最新のビジネス環境リスク（クラウド利用、サイバー攻撃）**に的確に対応が出来ている組織は少なく、従来のISMSの規格の枠組みの活動だけでは対応が難しい状況となっている。 本発表ではサイバー攻撃やクラウド利用という新たなリスクに対して、組織的な対応をするための方法論を提案する。具体的には**各組織ですでに構築済みのISMSの枠組みに加えて新たにリスク対応が必要となる＋α（補足事項）を可視化することで必要となる機能を明示**する。
2	働き方改革における情報セキュリティ	昨今では、公共・民間を問わず働き方改革が急速に浸透しております。**働き方改革に関連し、導入される仕組みやツール類は新たなリスクを発生させる可能性**があります。そのため、**事例などを元にセキュリティ上のポイントをまとめ**、セキュリティの向上を図る。

2018年の取り組み
■インプリメンテーション研究会　テーマ１（抜粋）

・ISMS規格要求事項から紐解く最新のビジネス環境リスク

事例：サイバー攻撃への対応方法についての考察



可視化

ISMSの実装で対応可能な領域
とサイバー特有の領域

CSIRT機能	機能項目	対応管理策（1）	対応管理策（2）
インシデント事後対応の機能	・インシデントハンドリング ・コーディネーション ・コンピュータ・フォレンジックス　等	ISMSの枠組みで対応可能	サイバー特有の対応が必要 高度な専門スキルが必要
インシデント事前対応の機能（事前準備）	・セキュリティ関連情報提供 ・インシデント/セキュリティイベント検知 ・技術動向調査　等		
セキュリティ品質向上の機能（平時のとき）	・リスク評価分析 ・事業継続性、災害復旧計画作成・改変 ・セキュリティコンサルティング　等		

2018年の取り組み
■インプリメンテーション研究会　テーマ２（抜粋）

・働き方改革における情報セキュリティ

ビジネスツールでの対策3：サービスの堅牢化

有事の際の証拠紛失や、社員等の退職によるデータの紛失が発生するリスク。

利用するサービスは堅牢ですか？

- 有事に備えて、必要な監査ログや情報の保全を図っていますか？
- 社員の退職とともに、情報資産にアクセス不可能とならない対策がとられていますか？

管理策実践の例

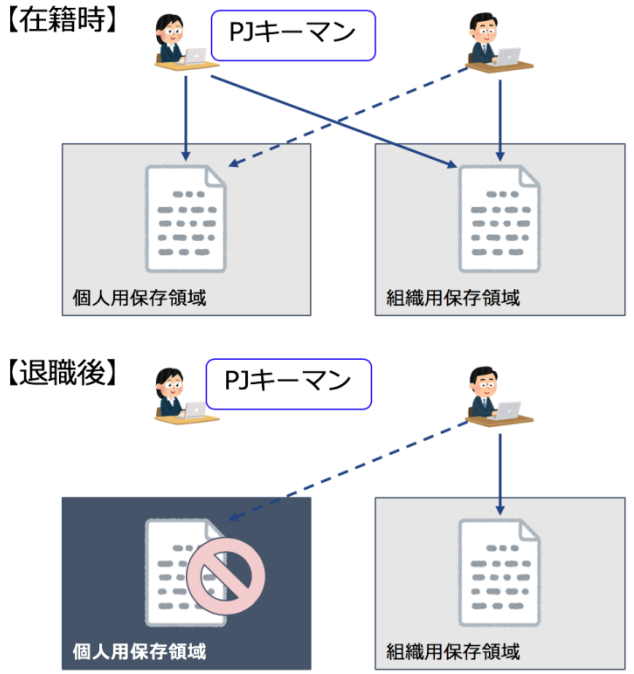
- 監査に必要なログを取得出来るよう、オプションサービスを申し込む。（A.14.4.2）
- サービスの特性（個人・組織）を理解し、組織として必要な情報を混在利用しない。（A.8.2.3）

➢関連リスク

✓証拠の紛失

✓情報の紛失

補足：クラウド上のデータ保存に関する注意



個人用保存領域に置かれたファイルであっても、**アクセス権**を付与すれば**問題なく利用**できる。
そのため、保存場所を意識せずに利用している場合がある。
問題に気がつかない。

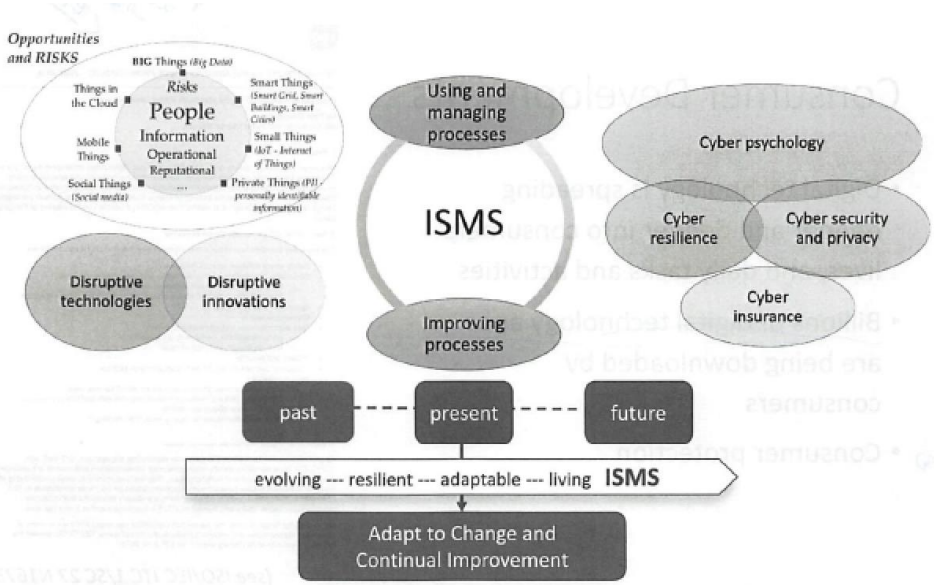
個人用の領域のため、退職の**アカウント削除**により、個人用保存領域の**ファイルがアクセスできなくなる。**
重要な資料を個人領域で作成した場合には、**情報紛失のリスク**となる。

2018年の取り組み

■Workshop

■Workshop（Prof. Edward Humphreys とのディスカッション）（4/13）

・日本ISMSユーザグループの活動の紹介
・ISMS and Future Landscapes（Prof. Edward Humphreys ）
・ディスカッション



2018年の取り組み
■情報セキュリティマネジメントセミナー

■情報セキュリティマネジメントセミナー開催 （12/7） ・・・171名参加

【標準化動向】
- 「ISO/IEC 27000ファミリー規格の最新動向」
- 「サイバーセキュリティの概念　ー国際標準化の動向を背景にー　」
- 「IoTセキュリティガイドラインの国際標準化動向」

【研究会成果報告】
- 「ISMS規格要求事項から紐解く最新のビジネス環境リスク（サイバー攻撃、クラウド利用への対応方法についての考察）」
- 「働き方改革における情報セキュリティ」

参考：セミナー資料掲載
https://www.jnsa.org/seminar/2018/1207/

2019年の取り組み
■インプリメンテーション研究会へのお誘い

2019年は下記の2テーマに取り組んでいます。
（デザイン思考によるターゲット分析も試行中）
ご興味のある方は一緒に検討に参加頂ければ幸いです。
冷やかしも大歓迎ですので、気軽に事務局へご連絡ください。

テーマ1：　最新の環境変化に伴うISMSの実装検討

テーマ2：　各社の事例から学ぶISMSの実装について

2019年の取り組み
■インプリメンテーション研究会（討議模様）