JUAS グローバルフォーラム

2017年度　分科会活動成果報告

- セキュリティ
- リージョナルITマネジメント

2018年4月

JUAS

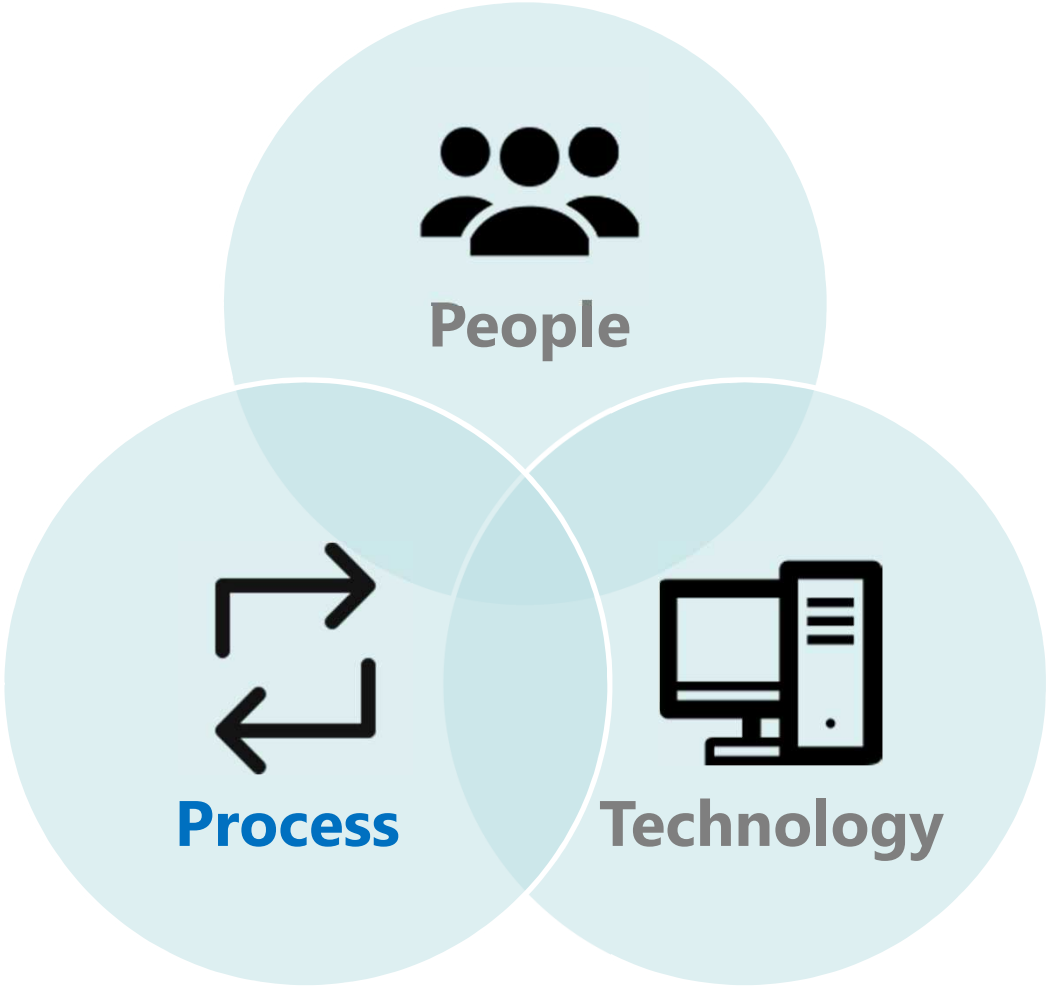
JUAS グローバルフォーラム
2017年第2回セキュリティ分科会

2017年7月10日

黒島　善知
寺内　敏晃
長部　克広
宮内　大輝
長沼　祐介
権田　昇平
斉藤　克浩
春崎　孝祐
奈良坂　純

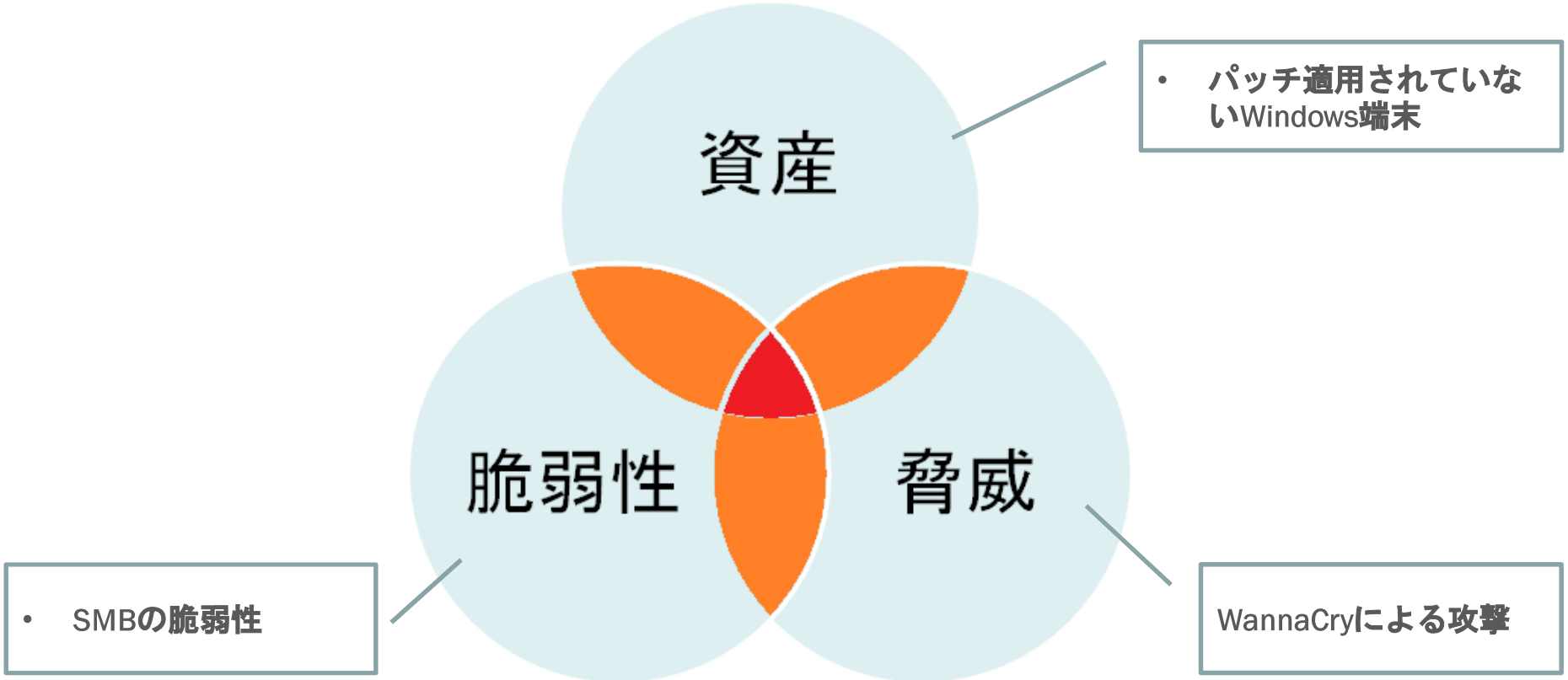
情報セキュリティにおける3要素

本活動報告では情報セキュリティ3要素における
プロセスについて議論する。



サイバーセキュリティの発生要因

サイバーリスクは要因の組み合わせによってリスクが高まる。
例：WannaCry



情報セキュリティとは

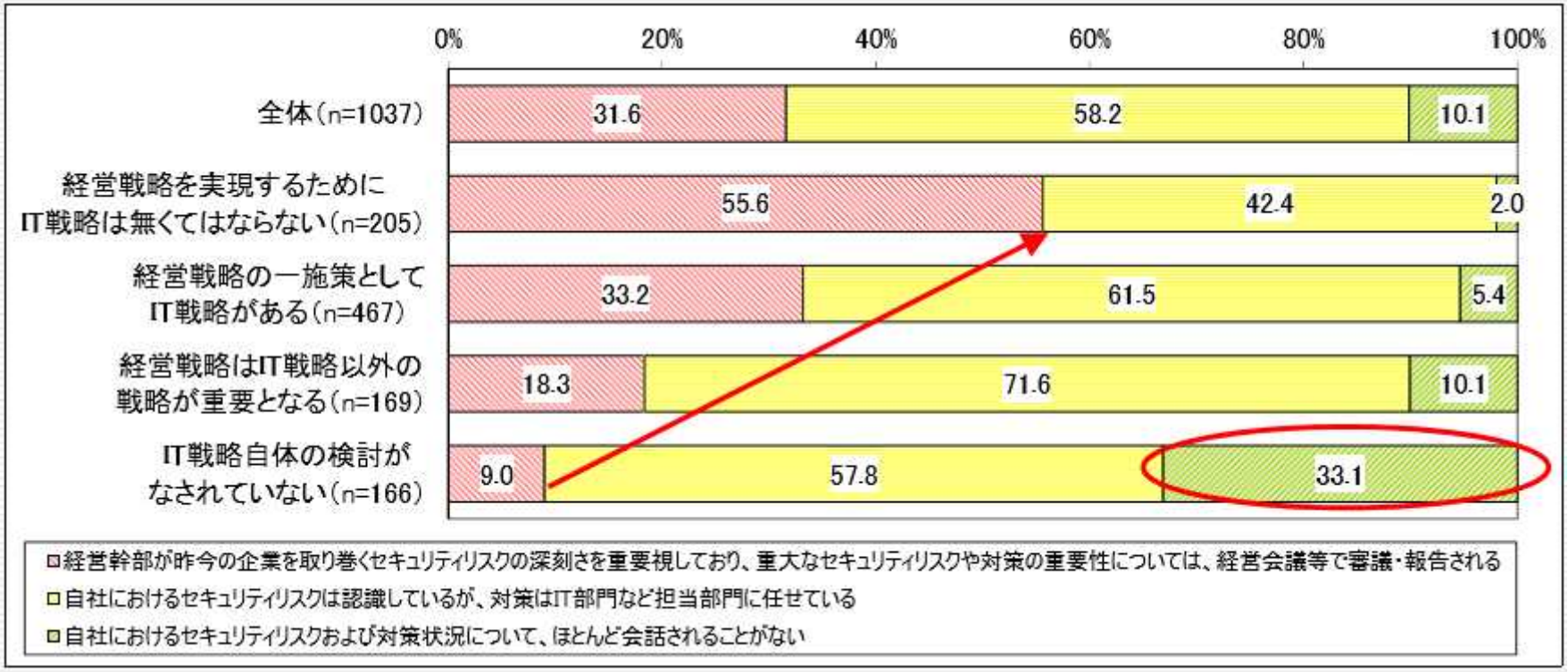
この会社における情報セキュリティプログラムの
問題点は何でしょうか？

我が社の機密情報を
絶対に漏洩しないと指切り
げんまんで約束して下さい。

これが今後は新しい情報
セキュリティプログラムの
基礎となります。

経営戦略とIT戦略の関係別 経営幹部の情報セキュリティへの関与度合い

経営戦略とIT戦略の関係が強い企業ほど、経営幹部が情報セキュリティに関与し、情報セキュリティの確保が重要な経営課題であると捉えられて いる。



出所：*JUAS 企業IT動向調査報告書2017*

情報セキュリティプロセス浸透度チェック

https://freeonlinesurveys.com/s/kSnF4RQc　※匿名による回答となります。

Plan	1. セキュリティポリシー、スコープ、ターゲットが定められている。
	2.セキュリティ計画が作成されている。
Do	3. セキュリティに関するポリシー、プロセスが文書化されている。
	4.セキュリティ計画が実行されている。
Check	5.セキュリティ計画の実行結果がモニタリングされている。
	6. 実行結果はセキュリティ責任者に報告されている。
Act	7. セキュリティ責任者はレビュー結果に対して改善に向けたフィードバックをしている。
	8. セキュリティ責任者のフィードバックを反映した新たな情報セキュリティ改善計画が立案・実行されている。

JUAS

海外での情報セキュリティに関する悩み

海外において情報セキュリティに関する課題は
グローバルITガバナンスと密接に関係している。

- 日本はポリシーなど整備が進んでいる一方**海外は対象外**。
- 本社から方針や評価項目は下りてくるが**展開は現地主導**。
- 日本基準の方針だと**海外に展開するのが難しい**。
- 現地担当者に状況を報告させてもITだけ終わってしまい**他部門が巻き込まれていない**。
- IT担当者が居ない会社の方が（内容を理解していない為か）自己診断結果が高い傾向にあり**現実と異なる**。
- セキュリティ対象が複数の会社や事業部門に跨る場合、各現地担当窓口や日本側との**調整が大変**。
- 海外では**責任と権限が無ければ人が動かない**。
- 日本では（海外のセキュリティが）**話題にならない**。
- そもそも**セキュリティに明るい人財が社内に居ない**。

2017年6月23日準備会より

JUAS

情報セキュリティプロセス（ISMS）

情報セキュリティ管理プロセスは**ISMS**と呼ばれている。

ISMS (Information Security Management System)

An information security management system (ISMS) is a set of policies concerned with security management or IT related risks.

The governing principle behind an ISMS is that an organization should design, implement and maintain a coherent set of policies, process and system to manage risks to its information assets, thus ensuring acceptable levels of information security risks.

From Wikipedia

ISMSはテクニカルプロセスではなく
マネジメントプロセスである。

JUAS

何故包括的なフレームワークが必要なのか

情報セキュリティの分野では**攻撃者が断然有利**。

攻撃する側はセキュリティ上の弱点を
一つだけ突破すれば良い。

防御する側は**数多くのセキュリティ課題**を把握し、**いつ来るか分からない攻撃**に準備しなければならない。

それ故**防御する側には体系的なセキュリティフレームワークが必要**。

ISO 27001

代表的なISMSグローバルフレームワークとして**ISO 27001**が多くの組織に導入されている。

ISO/IEC 27001:2013

ISO/IEC 27001:2013 is a specification for an information security management system (ISMS) which was published on 25th September 2013.

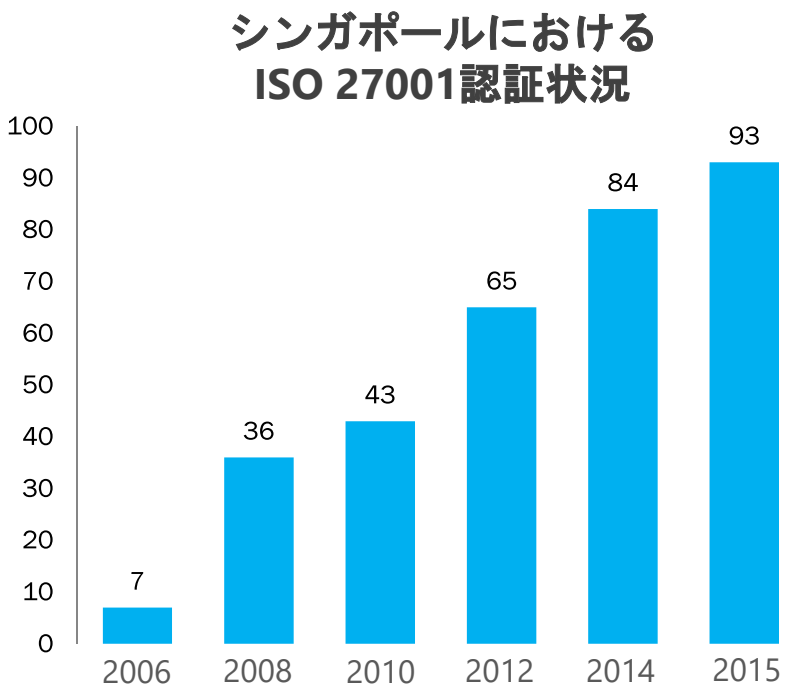
From Wikipedia

JUAS

各国におけるISO 27001認証状況

ISO 27001は世界150ヶ国に導入されており2015年時点で27,536の企業が認証を受けている。認証を受けた企業の30%は日本。シンガポールにおける認証企業数は**93**のみ。

Top 10 countries for ISO/IEC 27001 certificates - 2015		
1	Japan	8240
2	United Kingdom	2790
3	India	2490
4	China	2469
5	United States of America	1247
6	Romania	1078
7	Italy	1013
8	Germany	994
9	Taipei, Chinese	939
10	Spain	676



出所：*ISO Survey (http://www.iso.org/iso/home/standards/certification/iso-survey.htm)*

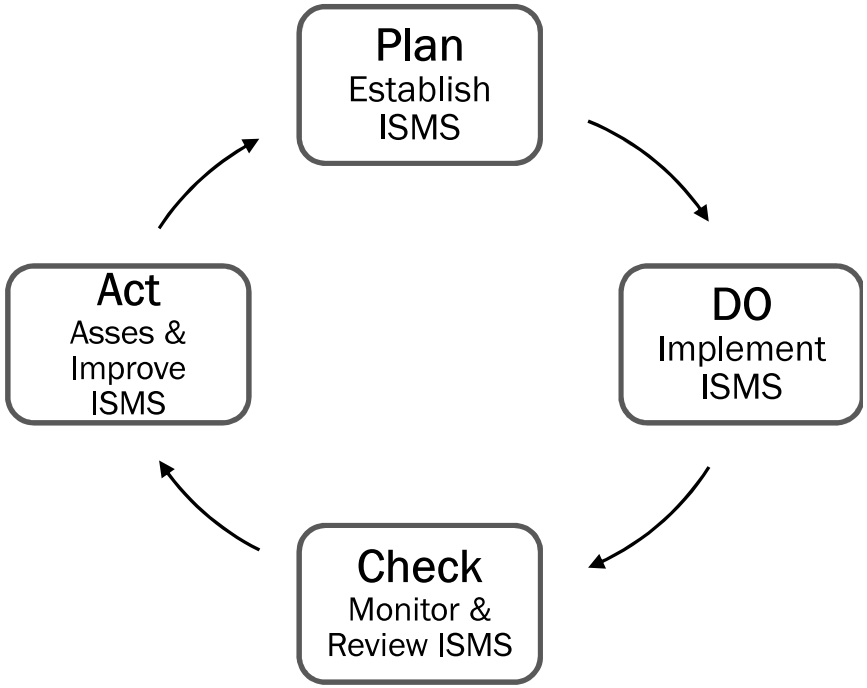
JUAS

ISO 27001の内容

ISO 27001は基本要件とAnnex Aから構成されている。
ISO標準プロセスに基づいて情報セキュリティ監査を行う。

Standard Requirements

0. Introduction
1. Scope
2. Normative References
3. Terms and Definitions
4. Context of the Organization
5. Leadership
6. Planning
7. Support
8. Operation
9. Performance Evaluation
10. Improvement
11. Annex A-Reference Control Objectives and Controls



Annex Aの内容

Annex Aはさらに**18からなる大項目**で構成されており
Control Objectiveは合計で**114項目**ある。

A.5　Information Security Policies
A.6　Organization of Information Security
A.7　Human Resource Security
A.8　Asset Management
A.9　Access Control
A.10　Cryptography
A.11　Physical and Environmental Security
A.12　Operations Security
A.13　Communications Security
A.14　System Acquisition, Development, and Maintenance
A.15　Supplier Relationships
A.16　Information Security Incident Management
A.17　Information Security Aspects of BCM
A.18　Compliance

※各項目に関してさらに詳細なControl Objectiveが記されている。

JUAS

ISO 27001に関する論点

ISO 27001は有効なフレームワークであるが、あくまでも
情報セキュリティ管理手段の一つに過ぎない。導入が目的と
ならぬよう企業は有効性や効果を導入前後で評価する必要がある。

導入前	• 認証を取得することが目的になりがち。 • ガイドラインの記述内容はハイレベルであるためセキュリティに関する経験が無い場合、具体的な実装まで落とし込むのは難しい。現場を知っているスタッフの参画が必須。 • 情報セキュリティはITの仕事だと勘違いされる傾向がある。全社的な取組であることをマネジメントが示す必要がある。
導入後	• 認証を維持することが目的になると活動が形骸化してしまう。 • 文書化が肥大化してしまいメンテナンスが大変。 • あくまでも情報セキュリティ管理が主目的であるため守備範囲が限定的である。ガバナンスを強化する為にはビジネスの観点から何を重視すべきかという点を意識して他のフレームワークと組み合わせた方がより効果的。

JUAS

情報セキュリティプロセスに関するまとめ

まとめ

- サイバーリスクは**要因の組み合わせによって発生する**。
- 情報セキュリティに関してはユーザーを「**信頼**」しても「**信用**」してはならない。
- ISMSとは情報セキュリティに関する**マネジメントポリシー及びプロセスを指す**。
- サイバーアタックは攻撃する側が有利であるため**防御する側は体系的なセキュリティ対策**が求められる。
- ISO 27001はISMSに関する**体系的なグローバルセキュリティフレームワーク**である。
- 組織における情報セキュリティは**トップマネジメントからスタッフまで一人一人の心がけ**で成り立っている。
- ISO 27001は有効なフレームワークであるが、あくまでも**情報セキュリティ管理手段の一つに過ぎない**。導入が目的とならぬよう企業は有効性や効果を導入前後で評価する必要がある。

JUAS

次回活動

	分科会トピック	メンバー	準備会
7月10日（月）	情報セキュリティ プロセス	黒島　善知 寺内　敏晃 長部　克広 宮内　大輝	日程：6月23日 場所：伊藤忠
10月10日（火）	情報セキュリティ人	黒島　善知 奈良坂　純 権田　昇平	日程：未定 場所：コニカミノルタ
1月15日（月）	情報セキュリティ テクノロジー	黒島　善知 斉藤　克浩 春崎　孝祐	日程：未定 場所：未定

JUAS グローバルフォーラム
2017年第3回セキュリティ分科会

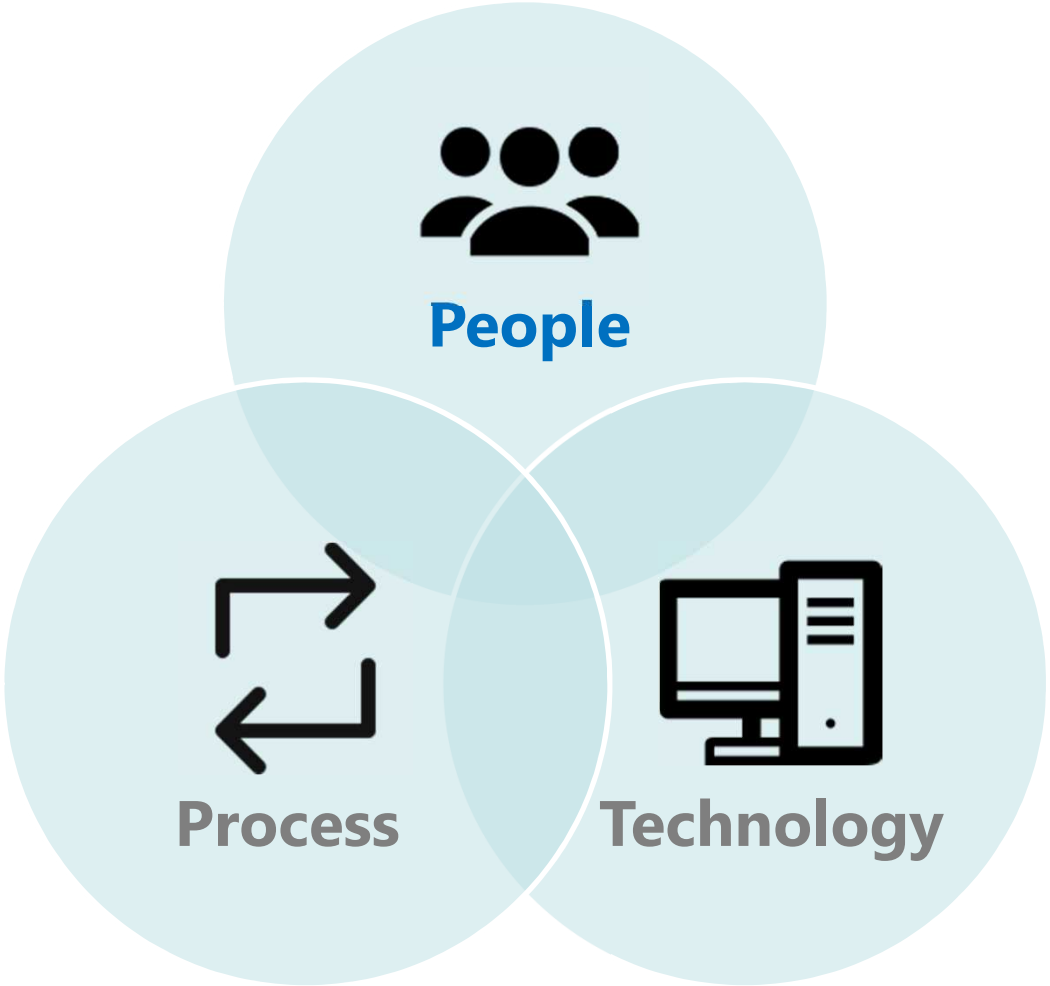
2017年10月10日

黒島　善知
寺内　敏晃
長部　克広
宮内　大輝
権田　昇平
斉藤　克浩
春崎　孝祐
奈良坂　純

JUAS

情報セキュリティにおける3要素

本活動報告では情報セキュリティ3要素における
人・教育・啓蒙活動について議論する。



東南アジア現地日本企業における情報セキュリティの状況

現地進出日本企業における情報セキュリティ上の問題は、現地事業所のトップが情報セ キュリティ対策の重要性を理解しておらず、また、現地の情報セキュリティや各種のリス クに関する実情を把握していないことと、日本の本社が情報セキュリティ対策の重要性を 認識していないことに起因して発生しているケースが多い。

1) 現地事業所のトップが情報セキュリティの重要性を理解しておらず、情報システムの管 理や情報セキュリティ対策の実施を現地スタッフ任せにすることが多い。そのため、情 報システムの管理や情報セキュリティ対策が適切にあるいは全く実施されない
2) 機密情報管理とウイルス対策の実施状況を、現地事業所のトップが把握していないこと が多い
3) 機密情報管理とウイルス対策の実態を現地事業所のトップが把握していても、それらの 問題を経営上の問題と認識していないため、日本の本社からの指示がない限り適切な対 応がとられることがない
4) 日本の本社においても、情報セキュリティ対策の重要性を認識していない場合が多く、 現地事業所に対して情報セキュリティ対策の実施を指示することは少ない

株式会社三菱総合研究所：2009年「各国における情報セキュリティに対する取り組みに関する調査」

JUAS

情報セキュリティ教育・啓蒙活動に対する学習障害

現地スタッフに対してに情報セキュリティに取り組んでいるものの、いくつかの学習障害によって効果的に情報セキュリティ教育・啓蒙活動が進んでいない。

■いくつかの学習障害のパターン

1) 情報セキュリティは私の仕事ではない
2) 悪いのはハッカーやIT
3) ゆでガエルの寓話
4) 「まだ自社で事故は起きていないので大丈夫だ」という妄想
5) 文化的な問題

参考：ピーター・M・センゲ「学習する組織」

情報セキュリティは私の仕事ではない

原因

- 個人が取り扱っている会社の情報セキュリティに対して責任感を持っていない。
- 自分たちが情報セキュリティ活動を行わなくても、自分の仕事は問題なく機能していると思っている。
- 情報セキュリティはITの仕事だと思っている。

対策

- 情報セキュリティに関する組織的なビジョン・目的を全スタッフに徹底させる。
- 日頃から各個人に対して情報セキュリティに関する啓蒙活動を行う（ニュースレター、ポスター）。
- 各部門、個人が行っている情報セキュリティ活動をKPIとして評価する（部門毎の整理・整頓、トレーニング参加など）

JUAS

悪いのはハッカーやIT

原因

- 情報セキュリティについて責任感を持っていない。
- 外的要因（サイバーアタック、セキュリティ施策）が問題と認識している為、防止策について積極的に参加しない・または事故発生時に責任転嫁する。

対策

- 情報セキュリティに関する組織的なビジョン・目的を全スタッフに徹底させる。
- 日頃から各個人に対して情報セキュリティに関する啓蒙活動を行う（ニュースレター、ポスター）。
- 情報セキュリティプロセスには各個人の協力が必須であることを周知する。

JUAS

ゆでガエルの寓話

原因

- 普段から情報セキュリティ事故が頻発しているため、記録もしていないし。現状が当たり前だと考えている。
- 徐々に起きている脅威に対してタイムリーに対応出来ていない、対応しなければいけないと考えていない。

対策

- 情報セキュリティ事故を文書化して事故の発生状況を可視化する。
- 情報セキュリティに対してKPIを設定し、あるべき姿を周知徹底する。
- 活動状況について必ずモニタリング・フィードバックを行う。

まだ事故は起きていない

原因

- 外部の事故は自社とは関係ないと考えている。
- 他社の事例から学ばない組織文化。

対策

- 他社の情報セキュリティ事故をケーススタディとして定期的に勉強する習慣をつける。
- 情報セキュリティ事故は誰にでも起きる可能性があるという認識を組織全体に根付かせる。

JUAS

文化的な問題

原因

- 問題が起きても責任を問われるため、ユーザーやIT担当者がタイムリーに報告しない。

対策

- 「Bad news first」を徹底できる信頼関係、文化を根付かせる。
- 問題が起きた原因を追究だけでなく、起きた問題に関する対応を評価するようにインシデント管理プロセスを見直す。

JUAS

次回活動

	分科会トピック	メンバー	準備会
7月10日（月）	情報セキュリティ プロセス	黒島　善知 寺内　敏晃 長部　克広 宮内　大輝	日程：6月23日 場所：伊藤忠
10月10日（火）	情報セキュリティ人	黒島　善知 奈良坂　純 権田　昇平	日程：- 場所：コニカミノルタ
1月15日（月）	情報セキュリティ テクノロジー	黒島　善知 斉藤　克浩 春崎　孝祐 洞内　聡志	日程：未定 場所：未定

JUAS グローバルフォーラム
2017年第4回セキュリティ分科会

2018年1月15日

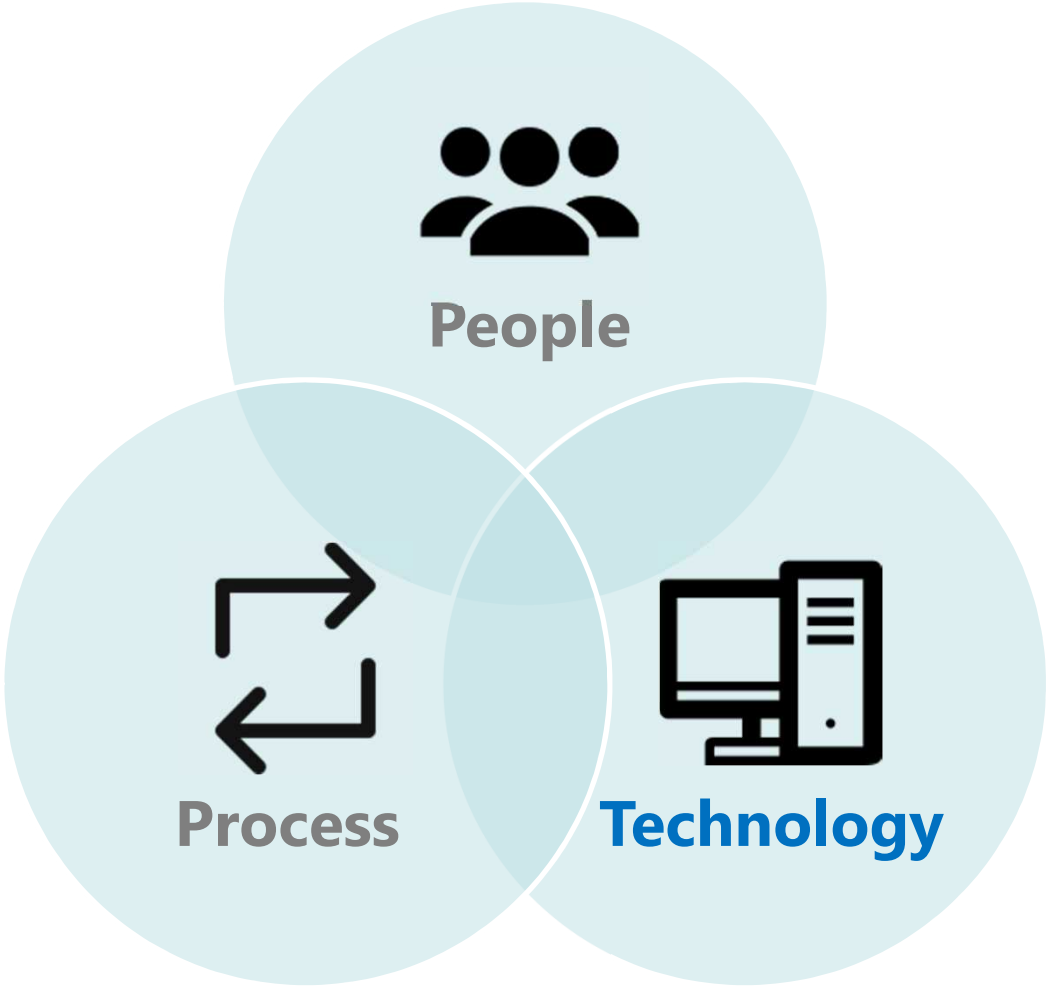
黒島　善知
寺内　敏晃
長部　克広
宮内　大輝
権田　昇平
斉藤　克浩
春崎　孝祐
奈良坂　純
小藪　美里
※敬称略

セキュリティ分科会

第2回	プロセス、ポリシー、ISMSフレームワーク（ISO 27001）
第3回	人、教育、啓蒙活動
第4回	情報セキュリティテクノロジー、ソリューションマップ

情報セキュリティにおける3要素

本活動報告では情報セキュリティ3要素における
テクノロジーについて議論する。



質問

貴社の状況について下記の質問について回答してください。

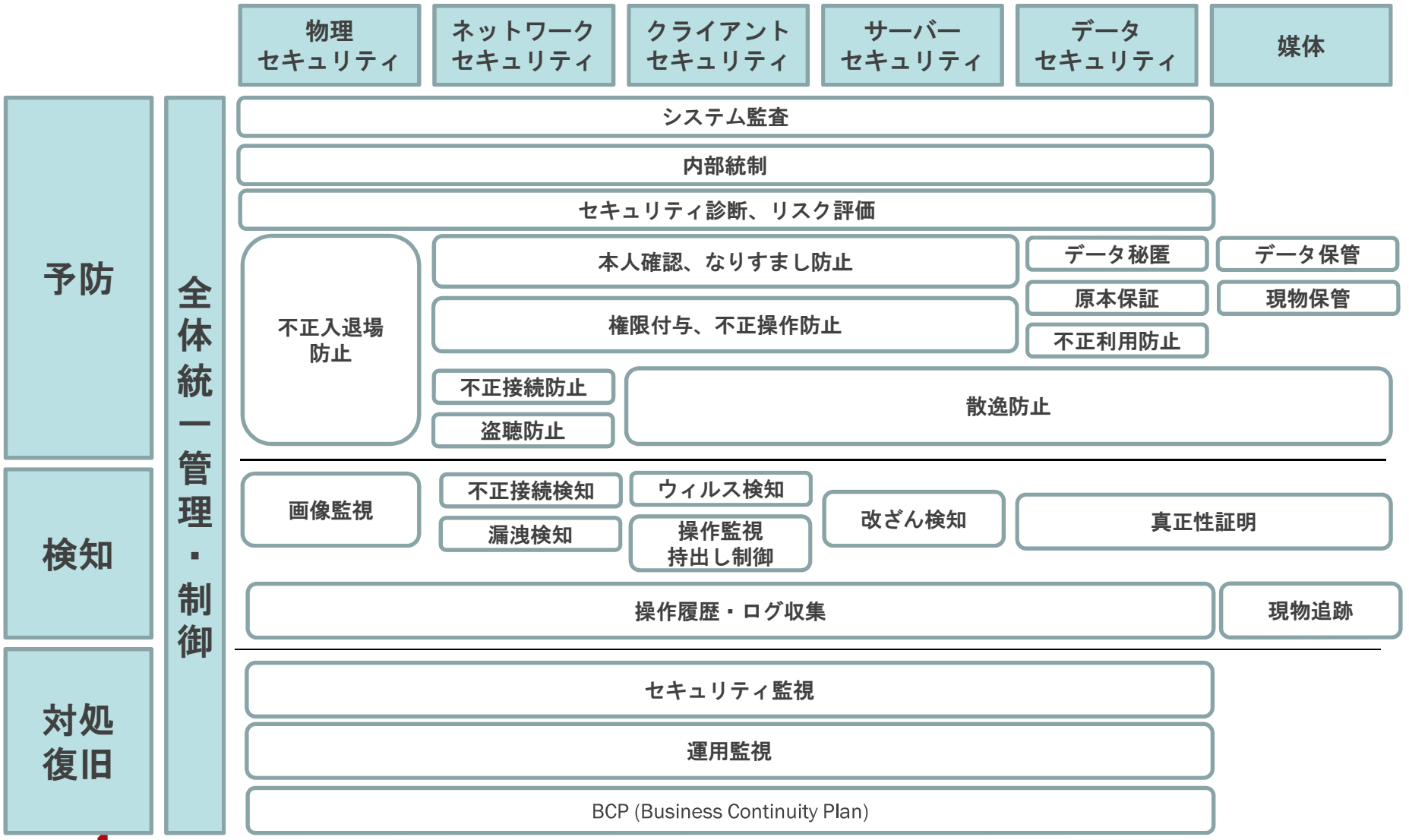
〇：実行・管理共に行われている
△：実行しているが管理が不十分
×：実行されていない

- システム監査を行っていますか？（〇、△、×）
- 内部統制を行っていますか？（〇、△、×）
- セキュリティ診断、リスク評価を行っていますか？（〇、△、×）
- 不正入退場システム/セキュリティドア等を管理していますか？（〇、△、×）
- ログイン認証基盤、なりすまし防止は実行されていますか？（〇、△、×）
- 権限管理、不正操作防止は行われていますか？（〇、△、×）
- 不正接続防止（アクセス）は行われていますか？（〇、△、×）
- （ネットワークデータの）盗聴防止は行われていますか？（〇、△、×）
- データ秘匿（暗号化）は行われていますか？（〇、△、×）
- データ原本保証は行われていますか？（〇、△、×）
- データ不正利用防止は行われていますか？（〇、△、×）
- 情報の散逸防止は行われていますか？（〇、△、×）
- データ保護（バックアップ）は行われていますか？（〇、△、×）
- 機密情報の現物保管は行われていますか？（〇、△、×）
- 画像監視（セキュリティカメラなど）は行われていますか？（〇、△、×）

質問

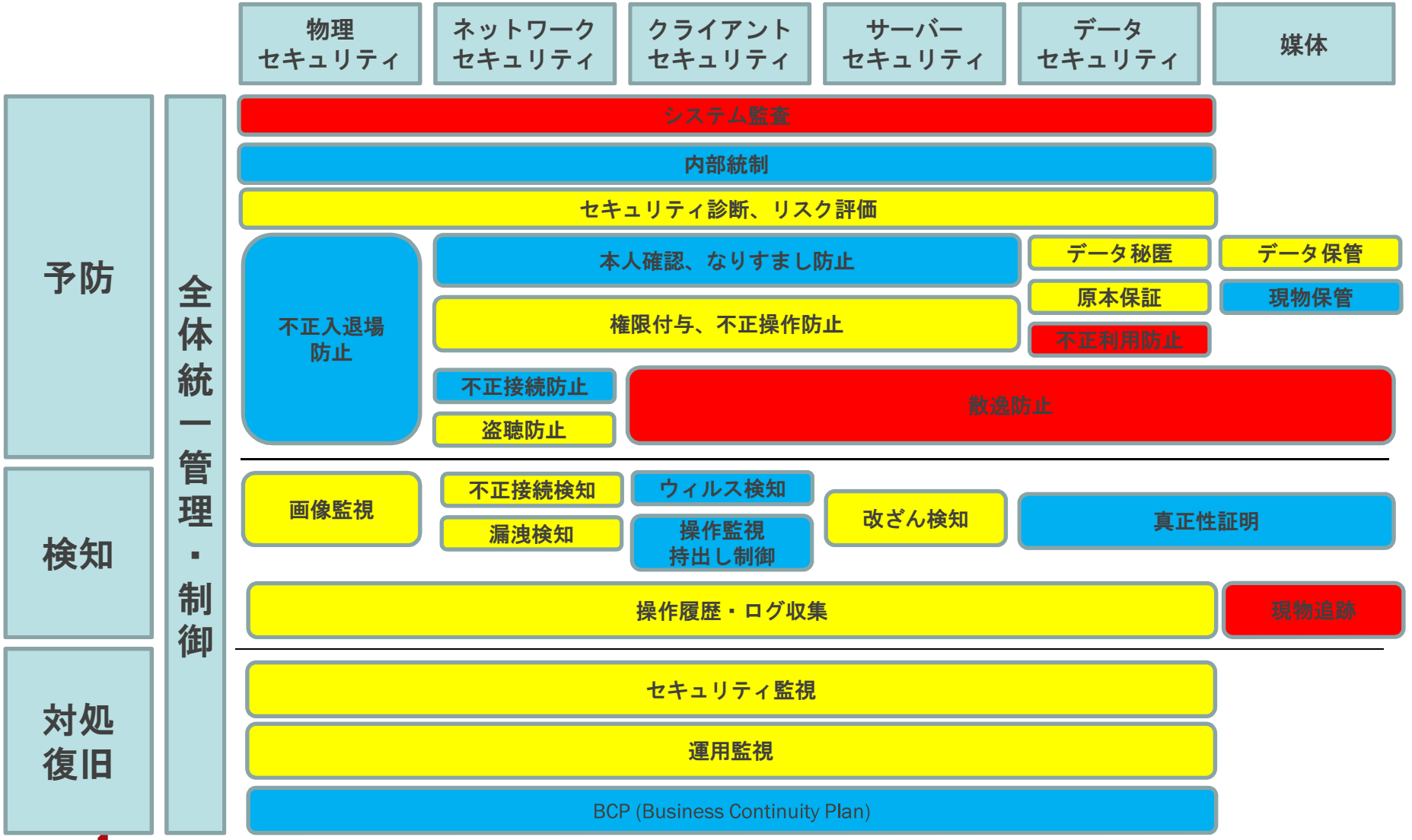
- 不正接続検知は行われていますか？（〇、△、×）
- ネットワーク漏洩検知は行われていますか？（〇、△、×）
- ウィルス検知は行われていますか（〇、△、×）
- データの持ち出し制御は行われていますか？（〇、△、×）
- 情報の改ざん検知は行われていますか？（〇、△、×）
- 真正性証明（証明書）は利用していますか？（〇、△、×）
- 操作履歴、ログ管理は行っていますか？（〇、△、×）
- 情報媒体の現物追跡は可能ですか？（〇、△、×）
- セキュリティ監視は行っていますか？（〇、△、×）
- 運用監視は行っていますか？（〇、△、×）
- BCPは計画、テスト、文書化されていますか？（〇、△、×）

情報セキュリティリスク対策マップ



参考）三菱電機インフォメーションシステムズ：情報セキュリティ対策マップ

情報セキュリティリスク対策マップ（例）



参考）三菱電機インフォメーションシステムズ：情報セキュリティ対策マップ

第4回対策マップに関する意見交換

対策が十分

- 内部統制は本社レビューがあり出来ている
- 不正入退場管理
- ウィルス検知
- ネットワーク関連は本社関連で出来ている
- 本社経由のメール、ネットワークは出来ている
- サーバはローカルにないので本社側にあるため監査対象のシステムがない。

対策が不十分

- 現物管理
- 物理的なセキュリティ
- データ管理。データ保管、データ毎のリスク管理を部門毎に取組んでいる
- ローカルPC、クライアント層の管理が不十分
- セキュリティ監査

まとめ

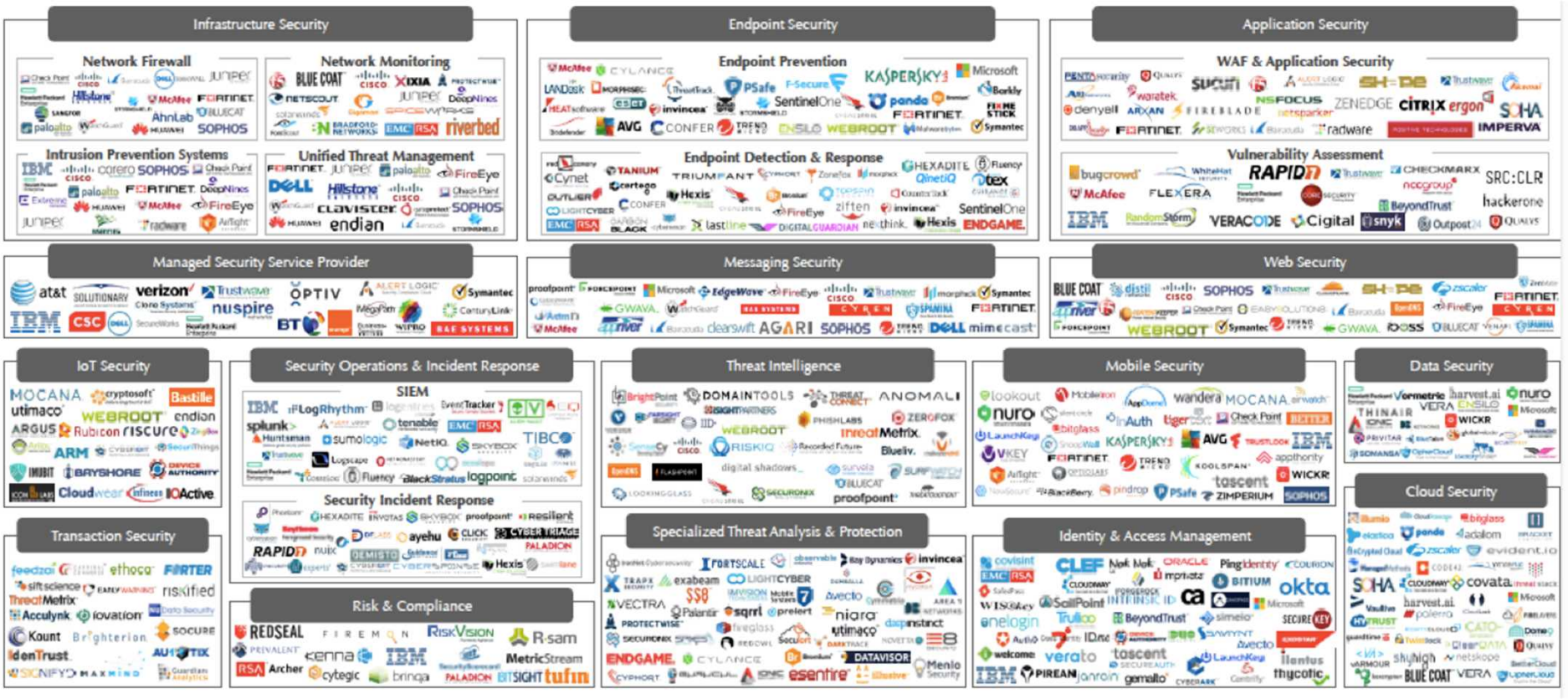
- 本社経由で共通化出来ているところは対策が出来ているが
- 一方ローカル主導、クライアント層は対策が遅れている
- ITリソースが足りない
- 対策に対する意識が薄い
- Regional ITとして情報セキュリティをどのように展開するか課題として考えている

今後の対応計画

- クライアント層、パッチ管理の強化。LANdeskなどPC管理
- 仮想PC（Citrix）の導入
- FW、エンドポイントの地域共通化
- グローバルセキュリティ方針の制定
- 物理的な情報セキュリティの強化（データ保管、入退室管理、セキュリティカメラ）

JUAS

情報セキュリティリスク製品マップ



JUASグローバルフォーラム
2017年度活動成果報告

リージョナルITマネジメント

目次

1. 研究対象
2. 地域統括拠点での問題意識
3. 地域統括・支援の現状と課題
4. 解決の方向性と提言
5. その他（各社取組例やメンバー間の話題）
6. 分科会メンバー

I. 分科会での研究対象

グローバル本社、地域統括拠点、現地法人のITに関する

- レポートライン
- 役割責任分担・権限

2016年度活動（標準化・共通化）を踏まえ、メンバーの関心が高い上記のエリアを抽出。現状や課題の議論を深めていった。

2. 地域統括拠点での問題意識

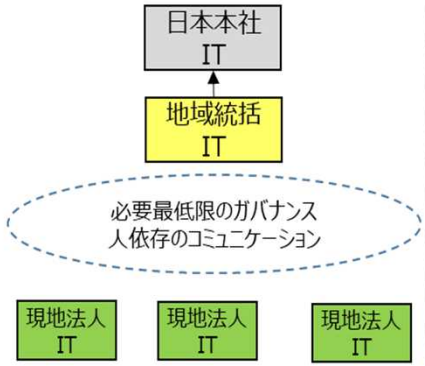
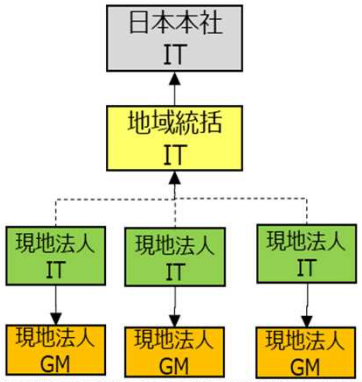
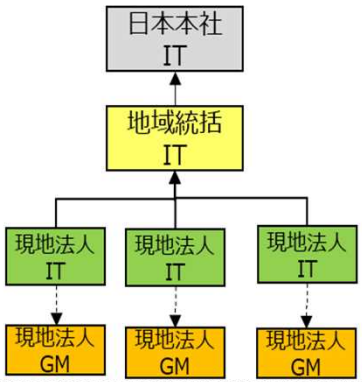
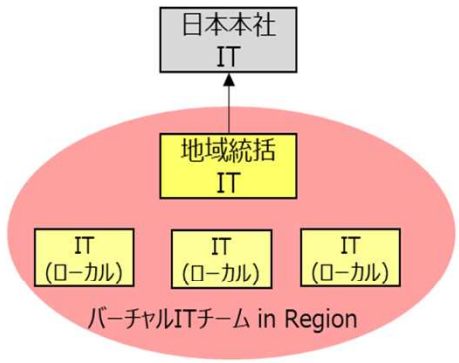
グローバル一体での経営が求められる中での課題

当地域に必要なITガバナンスが有効にきかせられているか

- グローバル本社や地域統括拠点の方針・施策が拠点に徹底できていない
- 地域や拠点の重要プロジェクト、セキュリティ対策への有効な手が十分に打てていない
- グローバルやリージョナルとしての共通化・標準化が十分に進められていない
- グローバルやリージョナルでのシナジーが十分にとれていない

3. 現状の把握 – GHQ/RHQ/拠点の組織

GHQ: グローバル／日本本社
RHQ: 地域統括

	No レポートライン	Dotted レポート	Solid レポート	One Regional Team
IT組織形態				
概要	地域統括会社にIT部門はあるがオフィシャルに現地法人のITにはレポートラインがない。	ローカルITから地域統括ITへDotted レポートがあるが、プライマリレポートはローカルのGMかDirectorであり、ビジネス面でのレポート優先	ローカルITから地域統括ITレポートがメイン。ITファンクションレポート優先。ローカルのGMやDirectorへ一応dottedレポートがある。	ITは全員リージョンないしはグローバル所属。ただし勤務地は地域統括であったり現地法人であったりバラバラ。場所に関係なくバーチャルにチームを構成欧米・外資系に見られる。
利点	○地域統括の現地法人ITへの関わりが最小限であり、ガバナンスに割くリソースは少ない。 ○地域統括は戦略業務のみに専念。ただし実行が難しい。	○現地法人のITマネージャーとの間にドットレポートあるため、現地法人のIT戦略、予算に関与しやすい。また、最新状況も把握しやすい。 ○各種承認もファンククショナル側が行う場合があり、ガバナンスしやすい。 ○現地法人GMとの良好な関係性が重要。 ○（担当者評価もRHQで行う場合）活動を管理しやすい。	○完全にITファンクション軸でマネジメント、ガバナンスが可能 ○リソースを柔軟に使うことができる。 ○IT予算、各種承認をファンクション側で行うことができる。（予算は現地が持っている。ただし一定金額以上のIT投資は、本社承認が必要となっている。） ○組織内の人材ローテーションが容易	○ITリソースを最適配置できる。無駄がない。（同じ業務をしている人が別の場所にいない） ○組織内のIT人材ローテーションが可能（キャリアパス。 ローカル to リージョン or グローバル）
課題	×地域統括からの強制力がない ×現地法人IT予算立案なども関われない ×現地のITマネージャー個人とのリレーションによるガバナンス（＝弱い） ×JSOXなどの日本からの要件に対してのみ最低限の対応を実施にとどまるリスク。	×あくまで実評価は現地法人GMなので、コントロールが十分でない場合がある。 ×IT予算の承認が現地法人のため、その都度説明が必要。施策推進についても同様で、都度理解を得る必要あり。 ×現地法人ITはその現法の仕事しかできない。	×現地法人ビジネス側との関係性を良好に保つ必要がある。 ×リージョンIT側の体制がないと多岐にわたるマネジメント/ガバナンス業務に対応できない。	×業務システムやインフラがグローバルもしくはリージョナルレベルで標準化しないと成立しない。 ×コミュニケーションロスが少ないグローバル人材で構成されている必要がある。人件費へのインパクトの可能性あり。 ×中央集権型ではない日本企業では難しいか。

メンバー間では、概ね左から3つの類型のどれかにあてはまることが分かった

3. 現状の把握 – GHQ/RHQ/拠点の役割分担

メンバー間で個別に違いはあるものの、共通の分類軸で現状把握や課題抽出を行った

	GHQ	RHQ	現地法人	共通点	課題
IT戦略・中長期計画	グローバル戦略策定	リージョナル戦略策定・実行	リージョナルに従う。戦略色は薄い(一部大規模現法は戦略あり)	-グローバル戦略はあるが日本メイン。地域特性は考慮されていない。海外については大方針のみ -グローバルの大方針を参照しつつ、独自のリージョンIT戦略を立案している。 -リージョン戦略へのグローバル関与は少ない。	-一部大規模現法のITが強い。 -リージョンITが実行も行う場合は負荷が高い。 -IT子会社の海外拠点との関係
IT年次計画・予算計画	重要案件の把握	現法計画のレビュー・策定代行	策定・決定	下に同じ	下に同じ
IT予算を握っている	関与なし 報告・提出のみ	○ (リージョン予算)	○	-基本現地法人の予算として計上される。 -現地法人ITが作成するパターンと、リージョンが作成代行するパターンがある(ITが弱い場合など) -日本へは一応報告・提出するがレビューなどはないことが多い。	-現地法人での予算化なので、重要案件が予算化されたい場合がある。(事業側の承認が必要)
プロジェクト承認	一定金額以上(大)	一定金額以上(中)	○	-稟議規定に従う。	-タイミングがまちまち(コンセプトフェーズだったり、ベンター決定後だったり) -IT基点の投資は把握できているが事業基点のものはもれる場合がある。
プロジェクト実行	グローバル案件のみ(インフラ系)	リージョナル案件のみ	○	-リージョナル案件実行部隊がいるパターン -プロジェクト支援がメインのパターン	リージョナルのリソース不足。
プロジェクト支援機能	真に重要・緊急の場合のみ	○	-(実行主体)	-ローカルの案件で火が吹いた場合と、火を吹きそうな案件、戦略案件はリージョンからサポートする。	-日本からの支援はあると助かるが、及び腰。。。(人材育成の観点からも) -コストチャージが課題。(支援分の負担を現法にどうもってもらうか。) -リソースが十分でない(量と質の面で)支援できる人が少ない。

3. 現状の把握 – GHQ/RHQ/拠点の役割分担（続）

	GHQ	RHQ	現地法人	共通点	課題
調達・購買	一部メニューの用意	GHQメニューの展開	○	-メニューはあるが強制力がない。→ボリュームが取れない→現地で買ってしまう。 -調達部門との関係性	-メニューはあるが強制力がない。→ボリュームが取れない→現地で買ってしまう。 -リージョンでがんばっても実現できない。 -ソフトウェアはできても、ハードがきつい。（現地の保守サポート力）
技術的選択	関与はごく一部	関与するが強制力なし	○	上記「購買・調達」、下記「ベンダー選定・管理」と同様	
ベンダー選定・管理	関与はごく一部	助言、一部は選定に関与	○	-グローバル標準ベンダーがない。（インフラは比較的可能だが、業務アプリは。。。）	コストだけできまるパターンにどう対応するか。

メンバー間での情報交換や議論を通じて、

お互いの課題・悩みを共有し、整理することができた。

3. メンバー間 共通の課題

拠点

- IT計画・開発・運用に必要な十分な体制が整っていない

一方で、

地域統括

- 地域施策を企画・実行する、また拠点を支援できるだけの十分な体制が整っていない
- 組織の形にかかわらず、予算は拠点の事業計画に紐付いており、強制力が発揮しにくい

4. 解決の方向性 – 自分たちはどうありたいか

地域統括がより強いガバナンスを発揮できるようにしたい

- より強い地域統括の組織・体制・権限
  - セキュリティ対策なども確実に実行できるよう、予算含めた権限を強化したい
- グローバル方針と地域の現状をバランスさせた、地域としての施策立案と実行
- 拠点とのコミュニケーション強化。拠点の動きや情報が確実に入るようにして、ガバナンス・支援を行いたい

JUAS

4. 今後の取り組みに向けた提言

①　本社/地域統括/拠点のIT部門間レポートラインの見直し

- 現状の課題や、会社ごとのガバナンスの考え方に沿って、ありたい姿を検討

②　地域統括と拠点間のIT部門の役割責任分担の明確化

③　地域統括と拠点間、またIT部門内での人員配分の再検討

- 拠点で自己完結すべき役割と、それに見合った体制
- 地域統括で担う役割（ガバナンス、支援他）と、それに見合った体制

4. 今後の取り組みに向けた提言

④　予算確保に関する方針の再検討

- 拠点で調整・確保すべきIT関連予算（例：　ビジネス戦略に対応する投資）
- 地域統括が確保（またはその指示）すべきIT関連予算（例：インフラ・セキュリティ）

地域統括や拠点の経営（CEO, CFO）・経営管理とのコミュニケーションを
しっかりとることが大前提
本社とのコミュニケーションはそれ以前の問題として不可欠

5. 地域ベースでの各社の取り組み・工夫（一例）

Regional IT会議

地域内IT部門間の情報共有基盤構築

- 定期的な地域内IT部門長・メンバーの会議
- 対面・非対面でのコミュニケーションの強化
- ガバナンス・シナジー

定期的な拠点からの報告と、RHQから拠点へのフィードバック

- 各拠点からの定例報告
- 地域統括から拠点に、各拠点での取り組み・事例・課題を紹介
- 次の地域内でのコミュニケーションにつなげる

拠点のIT運営委員会への関与

JUAS

5. メンバー間でのその他の話題（順不同）

本社との関係

- 本社の指示・施策の内容の粒度が低いケースにおいて、その実施にあたっての地域統括の裁量は十分か
- 本社の指示や依頼の頻度やボリュームに見合った地域統括の体制になっているか
  - アジア地域では国・拠点の数が多いうえ、状況や成熟度がバラバラ。指示・依頼・施策の展開と消化のロードは低くない

ローカルのモチベーションの維持向上

- リージョナル組織メンバーとしての役割付与や成長を促せるか
- 人材のモビリティ（拠点間の異動など）

5. メンバー間でのその他の話題（順不同）

駐在員の役割

- ローカライズが求められているのか、駐在員としての継続した役割が期待されているのか

当地ならではのチャンス

- 本社・日本よりは経営トップとの距離が近いのは、地域で施策を描き、実行できる「機会」

6. リージョナルITマネジメント分科会メンバー

内田弘之*	Tokio Marine Asia Pte. Ltd.
土屋孝文**	NS Solutions Asia Pacific Pte.Ltd.
伊東英文	DIC Asia Pacific PTE LTD
石原裕明	FUJIFILM Asia Pacific Pte. Ltd.
長谷部隆 洞内聡志	Fuji Xerox Asia Pacific Pte Ltd
丹羽麻裕	Idemitsu International (Asia) Pte. Ltd.
白砂修一	Nippon Steel & Sumitomo Metal Southeast Asia Pte. Ltd.
奈良康博	NYK Business Systems South Asia Pte. Ltd.
城後匠 椎野浩幸	Suntory Business Systems Asia Pte. Ltd.
横田隆	YAMAHA MOTOR ASIA PTE LTD

※リーダー(*)、サブリーダー(**) 以外のメンバーは会社アルファベット順、JUASメンバーとして前任→後任の順

JUAS

ありがとうございました