第3回　情報セキュリティマネージャー
CISMカンファレンス in Tokyo

講演3：
「昨今のセキュリティ事情と
情報セキュリティマネージャに求められる
スキル」

日本ヒューレット・パッカード株式会社
エンタープライズサービス事業統括
木村　晴雄
2015/01/24

Agenda

1. 情報セキュリティを取り巻く、状況の変化
2. 長期的なセキュリティ戦略の必要性
3. セキュリティマネージャに求められるスキル（資質）とCISM
4. 監査人とセキュリティマネージャの共通点

1、情報セキュリティを取り巻く、状況の変化

世界におけるセキュリティのトレンドと影響

現在では、ほとんどの企業にとって、セキュリティの脅威は対岸の火事ではなく、
そして、被災したときの被害は企業経営に重大なダメージを与える可能性があります。

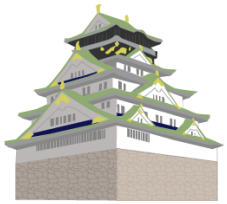
Cyber Threat	56%の組織が何らかのサイバー攻撃被害の経験
サプライチェーンの影響	データ侵害事故の44%がサードパーティのミス
金銭的な損失	データ侵害事故における平均$8.6Mの損失金額
風評被害	事故発生により企業の時価総額は平均30%低下
保護にかかる費用	IT予算の8%をセキュリティ対策で使用

昨今のセキュリティ事情を考えて・・・。

これまでに発生したセキュリティ事故を振り返り、また現状を考えてみると、
現状および近い将来においては、Cyber Space環境(ICT/Internet)はどう考えても。

攻撃側

防御側



さらに、以下に示すような事項によって、より攻撃側が優位である。

■攻撃側の自由度

ー攻撃は外部からのみ行われない。(内部犯行、社外で感染したPCの持込など)
ー攻撃側は彼らの好きな時間・タイミングに行われる。
ーまた攻撃者は増大している。

■防御側の制約

ー防御側の対応は制限される。(基本的に「耐える」行動しか選択肢がない。)
ー過去のシステムなどは、そもそも攻撃を受けることを前提としていない。
ーそもそも、「ゼロデイ」、「標的型/APT」は既存のITにとって想定外。
(パッチは事前に提供されるもの・・・。という理解で作られたシステム)

今後の情報セキュリティに対して求められる事項

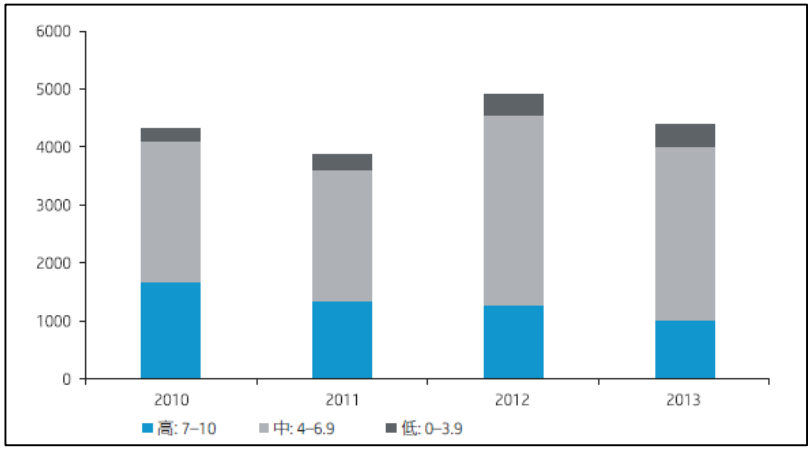
脆弱性はなくならず、攻撃者は高度に進化し、保護対象は広がります。

IT利用は広範囲にわたり、インターネットを活用しないという選択肢は現実的でなくなる	いつでも、どこでも攻撃を受けることが前提
ソフトウェアの脆弱性はゼロにはならない	当面は無くならないと想定すべき
「ゼロデイ」を踏まえた脆弱性管理とその対応の考慮	「防ぐことができない」期間が存在することの考慮
攻撃者は執拗になり、かつ様々な情報・技術を活用して目的を達成しようとする	攻撃手法が高度化しており、従来型の方法では対応不能
管理しなければならない機器・情報は増加し、かつ事故時の企業への影響が増大	HPの調査によると、日本での被害平均は約7億円/件

脆弱性の件数と脆弱性情報の価値

脆弱性については、現時点ではなくなることはなく、個人情報や企業機密と同様に、
脆弱性に関する情報も価値があるものとして取引されます。

NVDにより計測された脆弱性の開示件数（深刻度別:2010-2013年）



出典：HP「サイバーリスクレポート2013」

2010年からの動向を見ても、安定している傾向と判断されます。

※重要なこととして、これは開示された件数であり、全ての件数ではないことです。

ブラックマーケットでの情報の価値

種別	金額(1件)
基本的な個人情報(名前、誕生日)一式	$3
銀行口座の詳細情報	$5
クレジットカード情報	$10 - $45
Paypal / eBayのアカウント情報	$27

Information is Beautiful.net / World's Biggest Data Breachesより抜粋

未公開脆弱性（ゼロディ脆弱性）
エクスプロイトの価格表

ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000

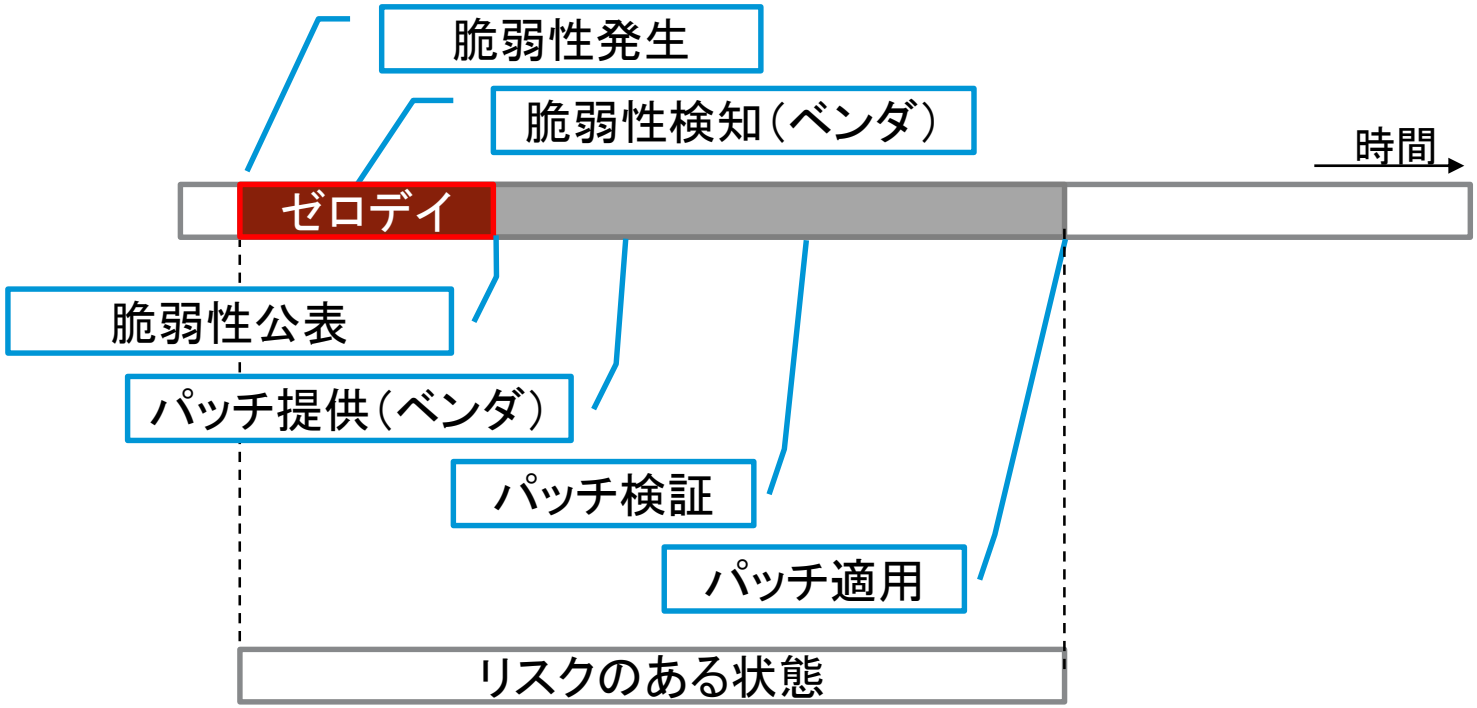
"Rough price list for zero-day exploits", according to Forbes

「ゼロデイ」の考慮

ある脆弱性が発生し、認知され、パッチが提供され、それが対象のシステムに適用されるまでには、時間が必要となります。

現在においては、多くの企業・組織で自社のリスク戦略に組み込まなければならない課題となっています。

脆弱性の発生から、対応できるまでの時間について

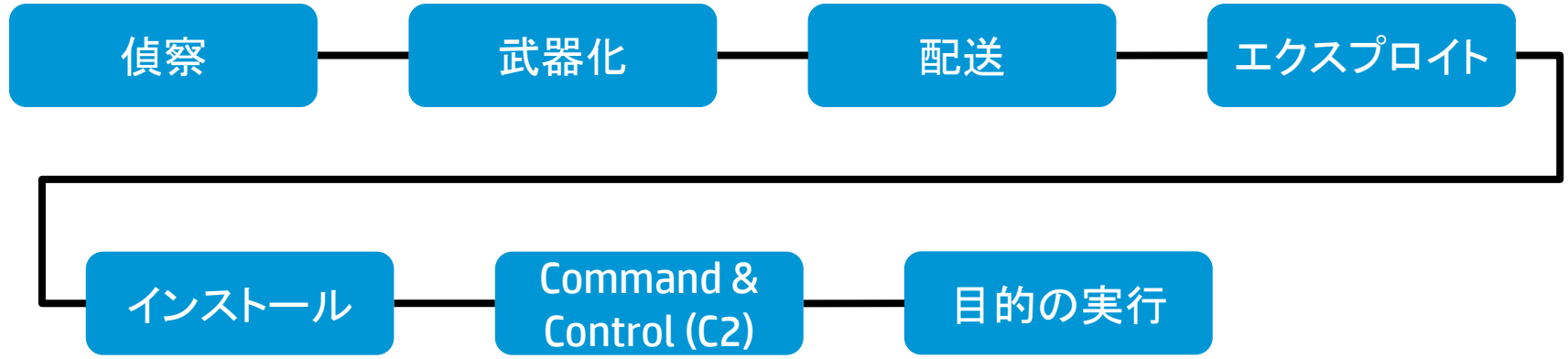


外部からの攻撃シーケンス考察（サイバー・キルチェーン）

攻撃側は単純・力任せ（Brute Force）な侵攻だけでなく、確立した攻撃手法を準備して、目的の達成を図ろうとします。

企業・組織としても、彼らの行動を理解することによって、リスクシナリオの検討を深化させていくことが可能となります。

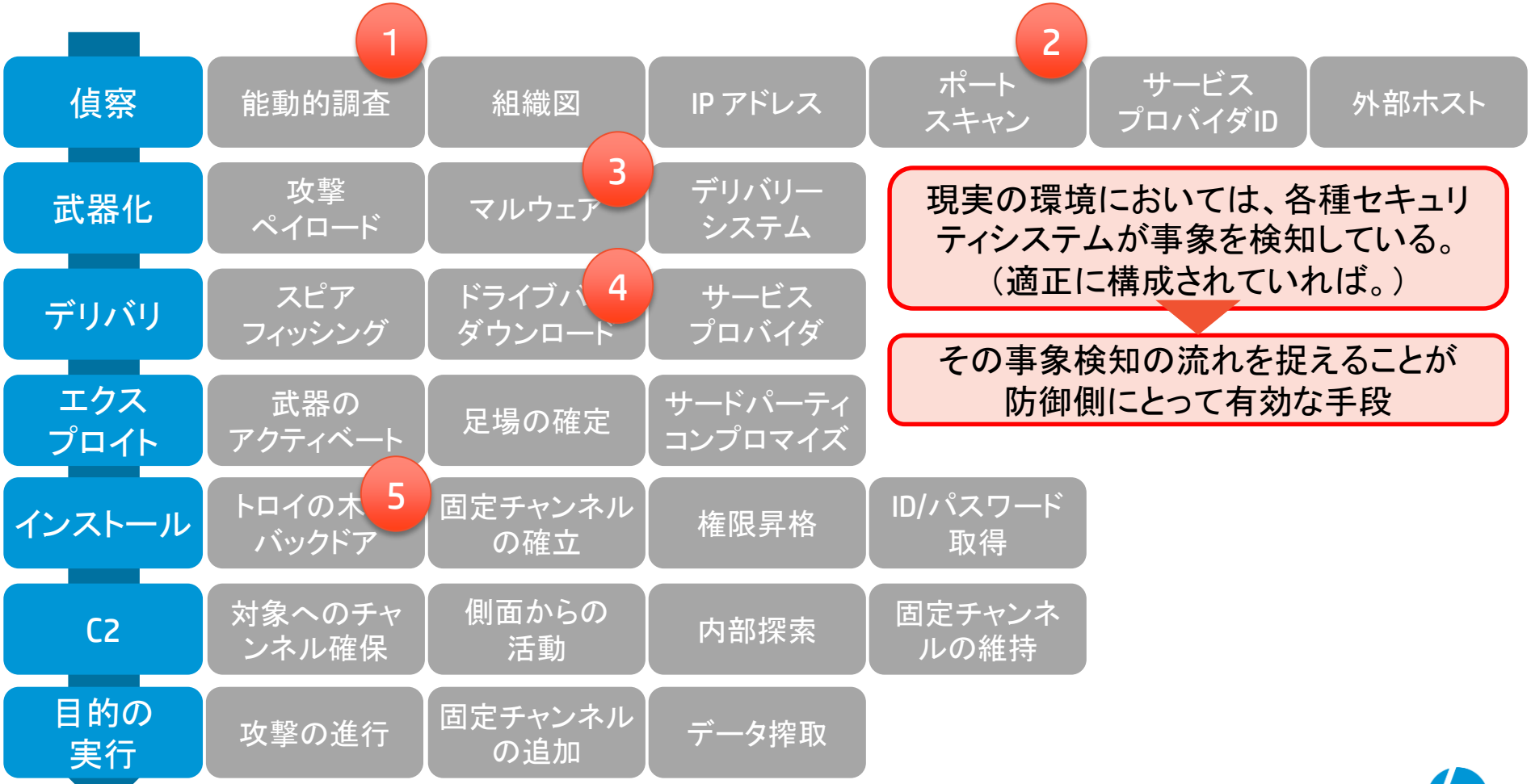
サイバー・キルチェーン



- 軍事作戦の切る・チェーンを、サイバー攻撃者の活動に当てはめていったもの。
- 右側に移行するにつれ、攻撃が深化していく。
- 2009年ロッキードマーティン社のMike Clopper氏によって提唱された考え方。
- 標的型攻撃などの「意図を持った」攻撃を軍事作戦になぞらえ、インシデントレスポンスの考え方を提唱。

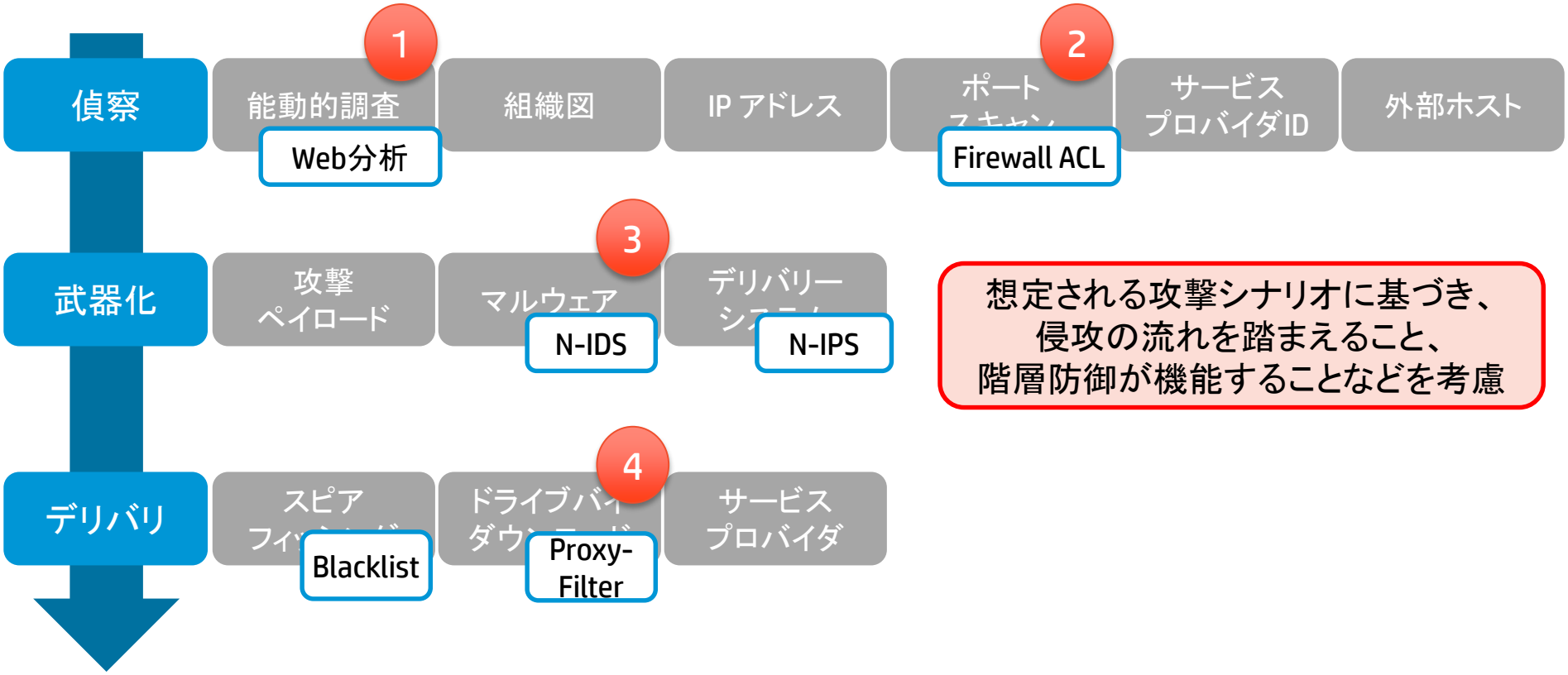
侵攻の例

各攻撃シーケンス内・間での振舞いを検知し、事前に防御を行うことと、リスクシナリオの検討時においても、どのように攻撃をされる可能性があるのかを理解することが重要です。



その対応方法（例）

攻撃を受ける際のパターンを予測、対応を準備し、適切な防御を検討します。
ただし、すべての階層で防御を行うことは、現実的には不可能なので、
企業のリスク対応方針、有効性・コスト対効果などを考慮して、保護を実装します。



防御方法に関わる対応技術の例

現時点においては、様々な製品や技術を組み合わせて利用することが求められます。

	検知	拒否	中断	緩和	欺く
偵察	Web分析	ファイアウォールACL			
武器化	ネットワークIDS	ネットワークIPS			
デリバリ	警戒ユーザー	プロキシフィルター	ゲートウェイAV	キューイング	
エクスプロイト	ホストIDS	パッチ	DEP		
インストール	ホストIDS	chroot	アンチウィルス		
C2	ネットワークIDS	ファイアウォールACL	ネットワークIPS	ターピット	DNSリダイレクト
目的の実行	監査ログ			QoS	ハニーポット

時代の変化に対応の検討

新しい「時代」には新しい考え方（戦略）が必要になります。

ITの進化に伴い、従来の固定的な「ポリシー」、「規則」では、変化する将来に対応することができなくなります。長期的な視野の元、セキュリティ戦略の見直し・策定が必要となります。

		企業での利用 (1960-1980)	個人+企業での利用 (1980-2000)	すべてが繋がる (2000-2020)
主要なテクノロジ		ホスト、ミニコン	ホスト、サーバ、PC	サーバ、PC、BYOD、 クラウド、IoT…
セキュリティアーキテクチャ（一部）	物理	いわゆるマシン室	データセンタ(DC)、執務室	DC、執務室、クラウド
	アクセス制御	利用規定	アクセスリスト	職責分掌、知る必要
	境界防御	ー	NW機器での制御	NW,サーバでの制御
	端末管理	ー	アンチウィルス	アンチウィルス、IPS等
	インシデント	ー	ログ収集	ログ管理/振舞い分析
	プロセス	IT部門でのみ策定	IT部門でのみ策定	ビジネス要件に基づき策定
セキュリティガバナンス	戦略	ー	IT部門内での戦略	セキュリティ戦略 セキュリティフレームワーク
	規則	アクセスルール	ポリシー、セキュリティ教育	ポリシー、セキュリティ教育
	対象	IT部門、利用者	全社員、パートナー	全社員、パートナー、 顧客を含むIT利用者
	モデル	特になし	IT部門による管理	経営層によるガバナンス

2、長期的なセキュリティ戦略

リアクティブな対応からプロアクティブな対応へ

情報セキュリティにおける取り組みは、「外圧」に起因するものが多く、「後追い的対応」となっていることが多数見受けられます。

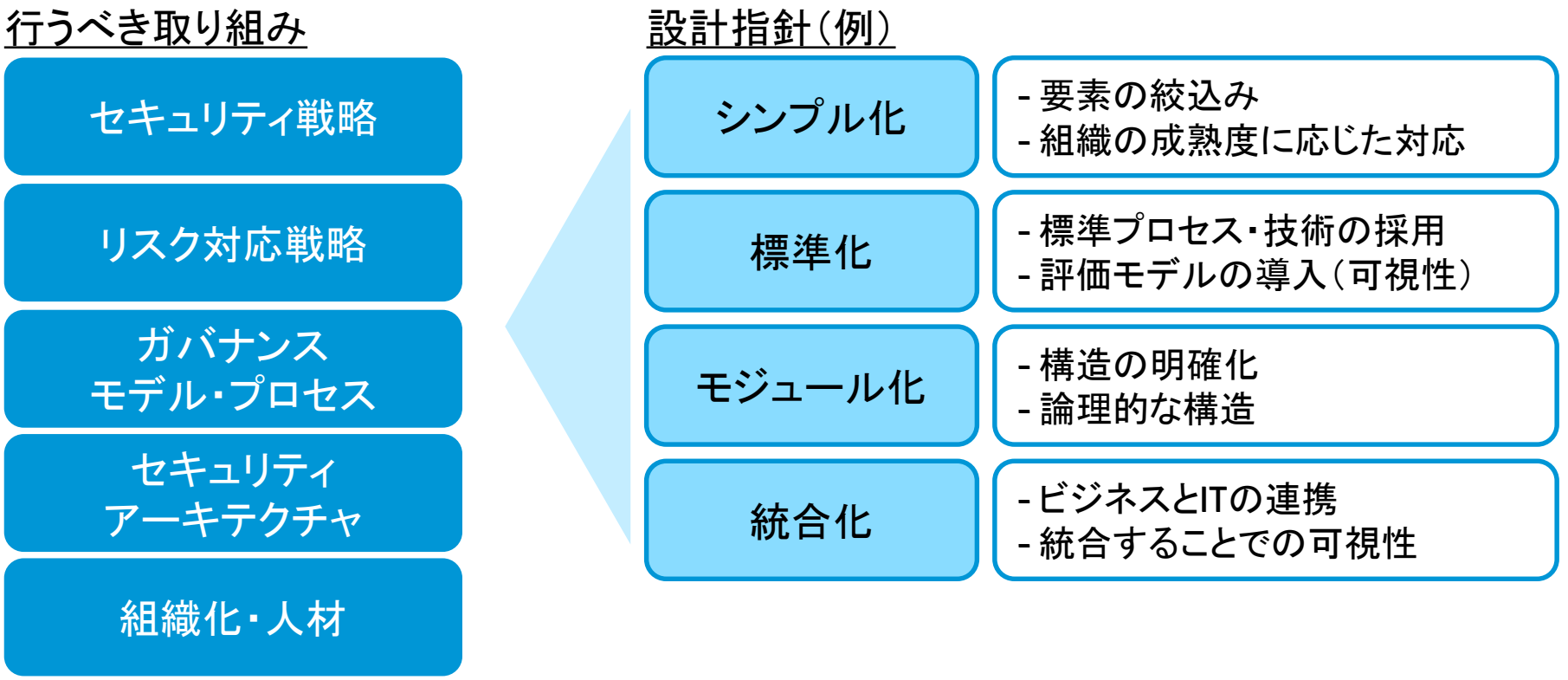
事故の発生が、企業継続に大きなダメージを与えることを踏まえれば、被害発生後／社会的な圧力が発生してからではなく、事前に経営課題として取り組みを行い、プロアクティブに対応できる体制を確立・維持することが求められます。

そのためには、以下のような取り組みを行っていく必要があります。

行うべき取り組み	概要
セキュリティ戦略	現状の把握と目標の策定 経営課題としての位置づけと役割定義
リスク対応戦略	目標の策定（リスク選好、許容） リスク評価・対応
ガバナンス モデル・プロセス	ガバナンスモデルの定義 評価モデルの定義
セキュリティ アーキテクチャ	戦略を実現するための保護システムのモデル化、フレームワークなどを有効に活用したアーキテクチャ立案
組織化・人材	全社組織としての組織整備と人材確保、育成 （と予算化）

プロアクティブな対応の実現について

設計、立案するに際して以下のような設計指針を活用することは有益です。
また、各取り組み項目については、既に様々な標準モデルやフレームワークが提供されているため、それらを有効に活用することが望ましいです。



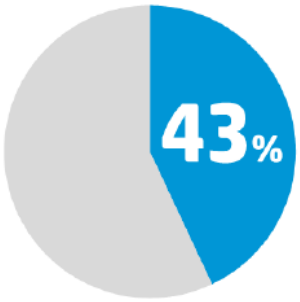
3、セキュリティマネージャのスキル（資質）とCISM

セキュリティ戦略とセキュリティマネージャー

セキュリティ戦略を立案・策定するには、IT課題としての対応にとどまらず、経営課題としての取り組む必要があります。

今後セキュリティマネージャーに求められる要件は、単なるITに関わるセキュリティのエキスパートではなく、企業活動におけるリスク対応をリードする能力が求められます。

そのためにはセキュリティマネージャーが、企業のビジネス要件に合致するセキュリティ戦略を立案していくことが必要となります。



情報のリスクは組織の俊敏さを損なうとエグゼクティブの**43%**は信じている。しかし、情報に金銭的な価値を見出しているのは、その内の**半数**だけである。

シニア・エグゼクティブの23%しか、データ漏洩への対応に満足を感じていない。

ビジネスリーダーとしてのCISOの進化

Business Risk Leader	20% ↑
Information Security Leader	45%
Security Manager	35% ↓

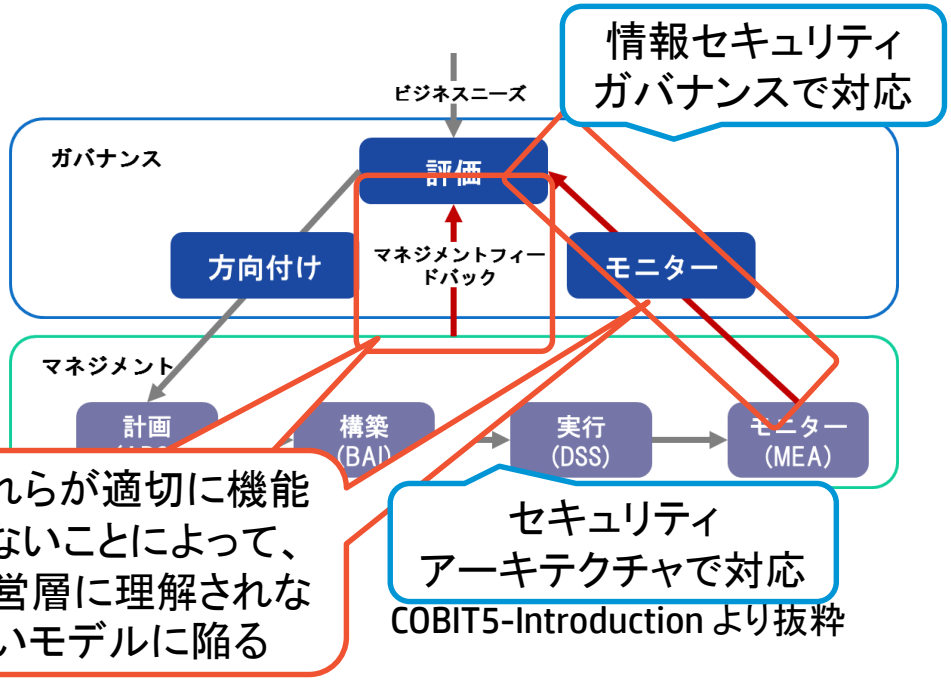
セキュリティマネージャーに求められるスキル（資質）

経営層で「情報セキュリティ」について、好ましいイメージを持っている人は多くありません。
しかし、そのほとんどが必要性については高く感じている現状があります。
なぜ理解されないのかについては、以下の事項が挙げられます。
以下のような事項を明確にし、立案・実現させることができる能力が求められます。

- 経営へのインパクトが理解しづらい（投資対効果、被害の影響と発生率）
- ITに対しての理解度が低い（どうやって評価したら良いか分からない）
- 責務・役割が明確に定義されていない。

経営層がセキュリティガバナンスにおいて、
上記のような事象に陥るケースにおいては、
右記のような「ガバナンスされる」という事態が
発生しているものと判断されます。

今後求められてくるスキル（資質）としては、特に「経営層が理解できるようにすること」



COBIT5-Introduction より抜粋

（参考）セキュリティ事故における経営層の理解

一例として、漏洩事故発生時の対応についての調査においても、必要性は認識しているが、
自分がどのように関わるのか、責任の認知などについても、経営層の認知は低いものとなっています。

漏洩事故発生時の対応プロセスにおける経営層の関与

経営層の関与が必要であると認識	79%
対応プロセスを知っている	47%
責任を背負っていると感じている	45%
漏洩事故発生時の状態をより明確にする方法 ：専門家を関与させ、経営層に教育と情報提供を行う ：過度に適切ではない報告書と報告会の実施	 67% 54%
効果的な対策が実装できていない原因として ：コミュニケーション不足 ：リーダーシップ不足 ：経営層の監督不足 ：対応策の有効性が測定できない	 70% 68% 58% 54%

Ponemon Institute「Executive Breach Response」より抜粋

セキュリティマネージャーとCISM

セキュリティマネージャーが立案すべき、セキュリティ戦略については、CISMが要求するドメインによってほとんどカバーされます。

行うべき取り組み	CISMでのドメイン
セキュリティ戦略	情報セキュリティガバナンス（ドメイン1）
リスク対応戦略	情報リスクの管理とコンプライアンス（ドメイン2）
ガバナンスモデル・プロセス	情報セキュリティプログラムの開発と管理（ドメイン3）
セキュリティアーキテクチャ	情報セキュリティインシデント（ドメイン4）
組織化・人材	

（参考）CISMレビューマニュアルでの記載項目

CISMレビューマニュアル(2012年版)で記載している記載項目

情報セキュリティガバナンス	情報セキュリティガバナンスの概要 効果的な情報セキュリティガバナンス 情報セキュリティの概念と技術 情報セキュリティガバナンスの範囲と憲章 情報セキュリティガバナンスの評価尺度 情報セキュリティ戦略の概要 情報セキュリティ戦略の開発	情報セキュリティ戦略の目的 セキュリティの現状の決定 情報セキュリティ戦略の策定 戦略の資源 戦略の制約 戦略実施のための行動計画
情報リスクの管理とコンプライアンス	リスク管理の概要 リスク管理戦略 効果的な情報セキュリティリスク管理 情報セキュリティリスク管理の概念 リスク管理の実施 リスク評価と分析の手法 リスク評価	情報資源の評価 目標復旧時間 ライフサイクルプロセスへの統合 セキュリティ統制のベースライン リスクの監視と伝達 教育と啓蒙 文書化
情報セキュリティプログラムの開発と管理	情報セキュリティプログラム管理の概要 情報セキュリティプログラムの目標 情報セキュリティプログラムの概念 情報セキュリティプログラムの範囲と憲章 情報セキュリティ管理のフレームワーク 情報セキュリティフレームワークの構成要素 情報セキュリティプログラムロードマップの定義	情報セキュリティ基盤とアーキテクチャ アーキテクチャの実装 セキュリティプログラム管理および管理活動 セキュリティプログラムサービスおよび業務活動 統制と対策 セキュリティプログラム評価尺度とモニタリング
情報セキュリティインシデント	インシデント管理の概要 情報セキュリティマネージャー インシデント管理資源 インシデント管理の目的 インシデント管理の評価尺度と指標 インシデント管理手続の定義	インシデント管理能力の現状 インシデント対応計画の開発 業務継続および災害復旧手順 インシデント対応および業務継続/災害復旧計画のテスト 対応および復旧計画の実施 インシデント後の活動と調査

4、監査人とセキュリティマネージャの共通点

情報セキュリティマネジメントとシステム監査の目的

情報システムにまつわるリスクに対するコントロールを適切に整備・運用(・監査)する目的としては、以下の事項があり「セキュリティマネジメント(監査基準※部分)」、「システム監査(監査基準)」は下記の同一の目的を実現するために実施されます。

・情報システムが、組織体の経営方針及び戦略目標の実現に貢献するため
・情報システムが、組織体の目的を実現するように安全、有効かつ効率的に機能するため
・情報システムが、内部又は外部に報告する情報の信頼性を保つように機能するため
・情報システムが、関連法令、契約又は内部規程等に準拠するようにするため

管理基準	セキュリティマネージャー	監査人	監査基準
組織体が主体的に経営戦略に沿って効果的な情報システム戦略を立案し、その戦略に基づき情報システムの企画・開発・運用・保守というライフサイクルの中で、効果的な情報システム投資のための、またリスクを低減するためのコントロールを適切に整備・運用するための実践規範		組織体の情報システムにまつわるリスクに対するコントロールがリスクアセスメントに基づいて適切に整備・運用されているかを、独立かつ専門的な立場のシステム監査人が検証又は評価することによって、保証を与えあるいは助言を行い、もってITガバナンスの実現に寄与することにある	

出典:経済産業省「システム監査基準」、「システム管理基準」

マネジメント基準・監査手続に見る必要な知識の関連性

セキュリティマネジメントで求められる「情報セキュリティ管理基準」と「監査手続」においては、基本的には視点が異なっているが、内容としては共通点が多数あります。

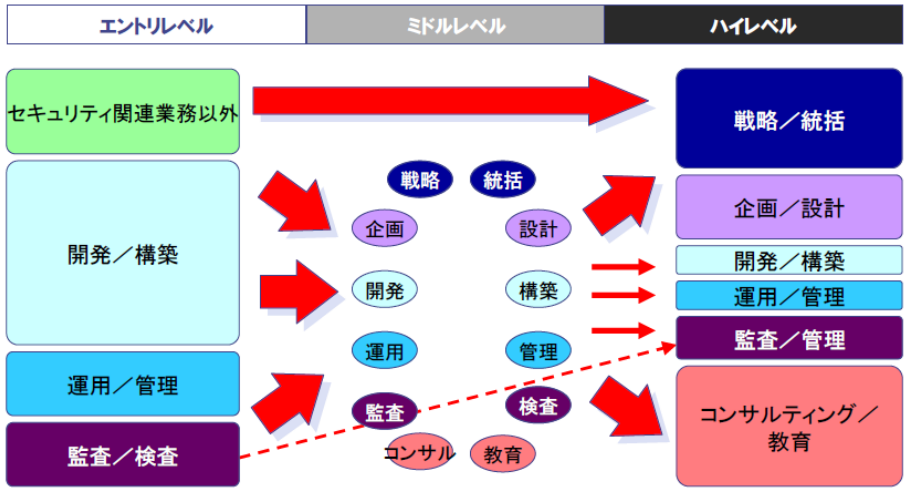
また監査人にとっても、セキュリティマネージャが立案する情報セキュリティの管理基準や、必要となるマネジメント基準、情報セキュリティ戦略や計画立案を理解することで、監査手続の品質向上にも繋がります。

情報セキュリティ管理基準				監査手続（マネジメント編）	
大項目	マネジメント基準		主たる監査対象	監査手続	留意点
情報セキュリティマネジメントの確立 中項目 適用範囲の定義	情報セキュリティマネジメントの適用範囲および境界を定義する	組織は以下の点を考慮して適用範囲及び境界を定義する ・自らの事業 ・体制 ・所在地 ・資産 ・技術の特徴	情報セキュリティに関する基本計画 監査技法 閲覧(レビュー)	情報セキュリティ基本計画に以下が定義されていることを確認する ・自らの事業 ・体制（責任や役割の定義など） ・所在地 ・資産 ・技術の特徴	前回の監査からの変更点について、担当者に確認する

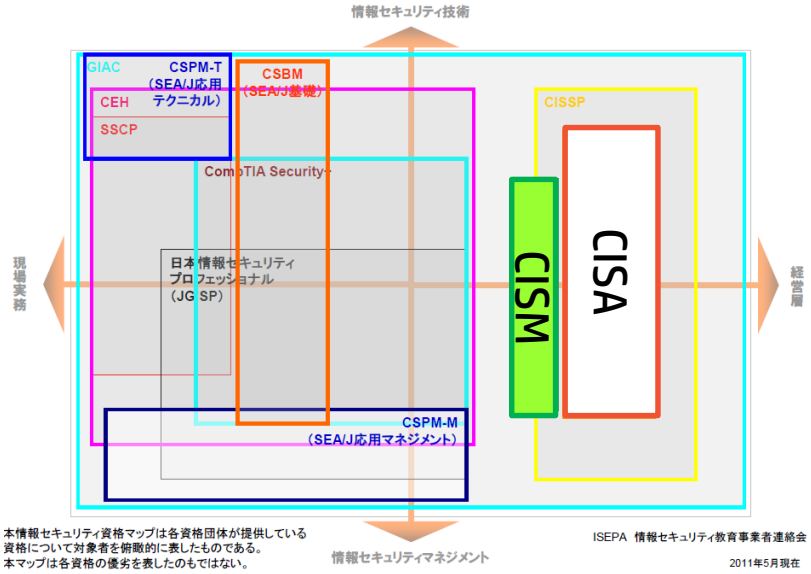
出典：経済産業省「情報セキュリティ監査手続ガイドライン」

キャリア開発としてのセキュリティマネジメント知識

キャリア開発を検討される上で、未知の世界を開拓することも選択肢としてありますが、
自身の経験を優位に生かすことで、スムーズに知識の幅を広げられます。



出典：IPA「情報セキュリティ人材の育成に関する基礎調査　調査報告書」



出典：JNSA「ISEPA_情報セキュリティ資格マップ」

最後に

「我々にも起こり得るのか？」ではなく、「いつ起こるか？」

「我々は対応できるか？」ではなく、「どうすれば生き延びられるか？」

What we have to look at now is the fact that the question should change. It should be not, "Can it happen to us," but "When is it going to happen to us?" And not, "Can we respond to it," but "How can we survive it?"

by Brett Wahlin, VP Global CISO, Hewlett-Packard

September 12, 2013 for ZDnet

出展：http://www.zdnet.com/thought-leader-interview-hps-global-ciso-brett-wahlin-on-the-future-of-security-and-risk-7000020626/

参考文書(リンク)および免責条項について

参考文書

- Cyber Security Report 2014
  ※2015年02月頃リリース予定
- Cyber Security Report 2013
  http://info.hpenterprisesecurity.com/register_hpenterprisesecurity_cyber_risk_report_2013?src=hpweb
- Enterprise 20/20
  http://www8.hp.com/h30458/us/us/discover-performance/it-execs/2014/apr/enterprise-2020.html
- サイバーセキュリティ犯罪により発生する費用　調査報告(Ponemon Institute)
  http://www8.hp.com/jp/ja/software-solutions/ponemon-cyber-security-report/index.html
- HP Security White Papaers
  http://www8.hp.com/jp/ja/software-solutions/enterprise-security.html
- Executive Breach Response
  http://h10131.www1.hp.com/campaign/executive-breach-response/
- 日本HP エンタープライズセキュリティ
  http://www8.hp.com/jp/ja/software-solutions/enterprise-security.html

免責について

本資料の記載事項については、個人の見解であり、日本HPの公式な見解ではありません。

本資料については、一般的な参考目的の利用に限られるものとし、特定の目的を前提とした利用、
専門的な判断材料としての利用等は行わないでください。