Soliton®

サイバーセキュリティリスク対策セミナー

経営者視点で
サイバーセキュリティ経営ガイドライン
を読み解く

株式会社ソリトンシステムズ　執行役員

株式会社Ji2　取締役　最高執行責任者

長谷部 泰幸

はじめに

■40分で全部読める:　本体は20ページ

概要 2ページ

本文 18ページ

付録 14ページ

誰に向けたガイドライン？

- 経営者を一義的な読者として想定※

- どんな会社の経営者？

  - ITに関するシステムやサービスを供給※

    →情報通信業／IT企業

  - 経営戦略上 IT の利活用が不可欠※

    →ユーザー企業

※「サイバーセキュリティ経営ガイドライン」記載の文章をそのまま転載

初の『経営』ガイドライン

■かなりご苦労されたと推察

- ■経営者へのアドバイス
- ■ガバナンスや危機対応
- ■経営の意思決定
- ■エンドユーザー経営者

：

情報セキュリティとの違い

■本ガイドラインでの定義

(4) サイバーセキュリティ、サイバーセキュリティリスク

サイバーセキュリティとは、**サイバー攻撃**により、情報漏えいや、期待されていたITシステムの機能が果たされない等の不具合が生じないようにすること。

サイバーセキュリティリスクとは、そうした不具合が生じ、それによって**企業の経営**に何らかの影響が及ぶこと。

(6) 情報セキュリティ

情報の機密性、完全性、可用性を維持すること。

※本ガイドライン　P28 付録D　『用語の定義』より　　但し、イラストはISMS教材を参照して追記

ちなみに法律では・・・

■サイバーセキュリティ基本法での定義

第2条　この法律において「サイバーセキュリティ」とは、電子的方式、磁気的方式その他人の知覚によっては認識することができない方式により記録され、又は発信され、伝送され、若しくは受信される情報の漏えい、滅失又は毀損の防止その他の当該情報の安全管理のために必要な措置並びに情報システム及び情報通信ネットワークの安全性及び信頼性の確保のために必要な措置が講じられ、その状態が適切に維持管理されていることをいう

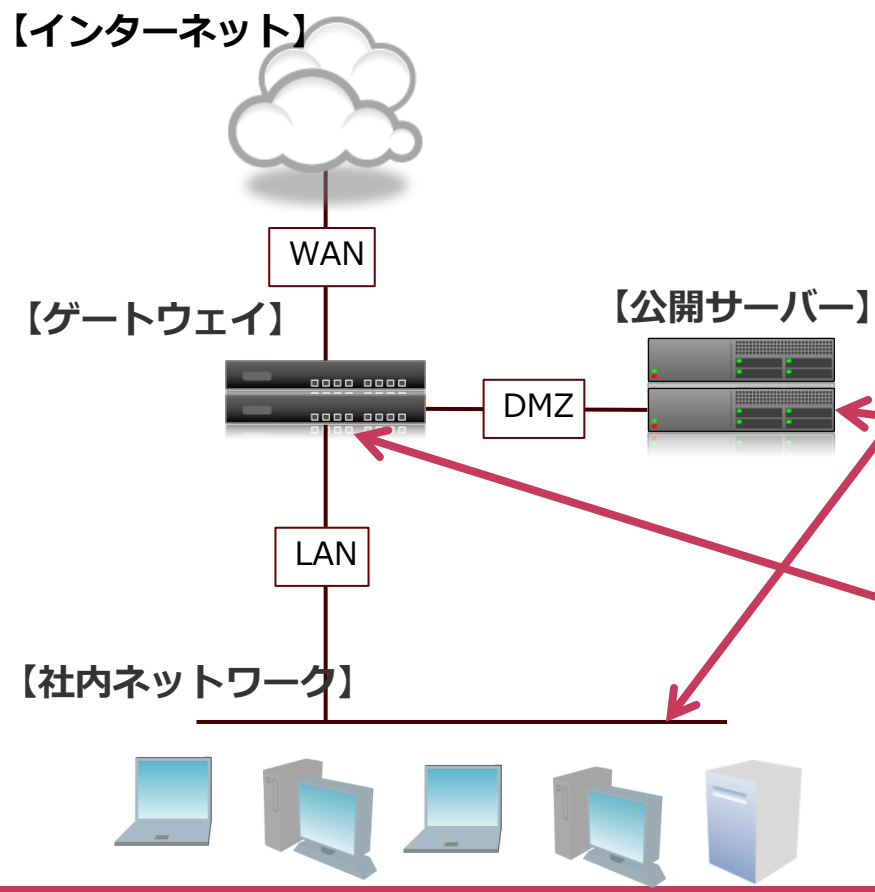
※あまりにも読みにくいため、原文のカッコ書きを全部省略

【解釈すると】

ネットワークシステムの安全性と信頼性を守ること

想定はサイバー攻撃

■企業ネットワーク



■認識済みの３大攻撃

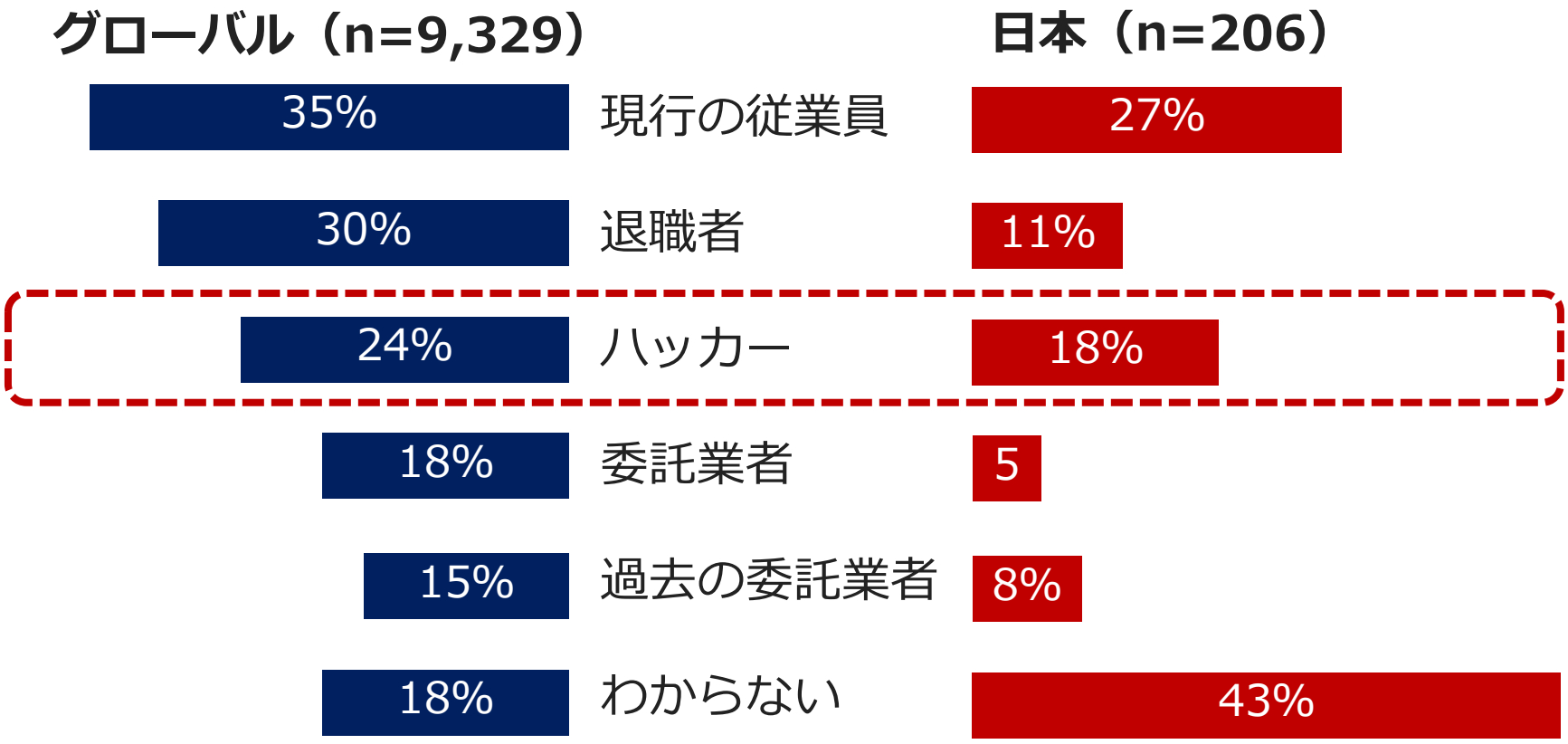
想定攻撃種類		
1. メール型攻撃	攻撃防止	不審メー URLやカ
	攻撃検知	ウィルス対 パターンカ
	対応態勢	Web参照 低減
2. サーバ型攻撃	攻撃防止	海外Web
	攻撃検知	検知を迅 監視レベ
	対応態勢	データ破
	被害回復	内部侵入 その内容
3. 大量通信型攻撃	攻撃防止	攻撃発生
	攻撃検知	大規模大
	対応態勢	経営層、
	被害回復	被害特定

【参考】決済業務等の高度化に関するスタディ・グループ
～銀行業界の取り組みと高度化に向けて
「５　決済の安全性・安定性」から一部抜粋
三菱東京UFJ銀行　IT事業部　2014年10月20日

7

企業におけるサイバー攻撃

■セキュリティ事案に関する日本の現状



【参考】　プライスウォーターハウス クーパース　「グローバル情報セキュリティ調査 2015」

10分でポイントを理解する

冒頭で・・・

サイバーセキュリティは
経営問題

３原則＋10項目

■３原則を認識し10項目を責任者に指示せよ

（序）背景／活用方法

3 原則

重要 10 項目

なぜ経営者？　その１

■リーダーシップを発揮していない･･･

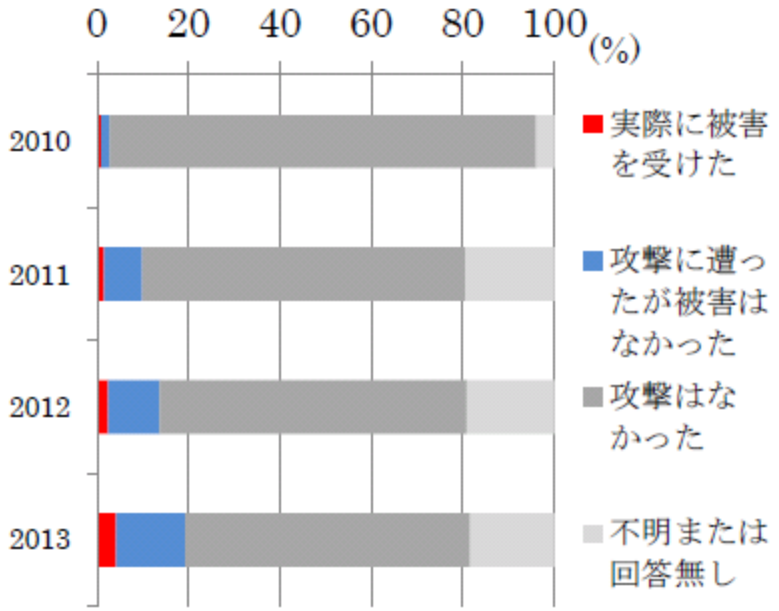


図１　サイバー攻撃（ウイルス以外）被害を受けた企業の割合）[1]

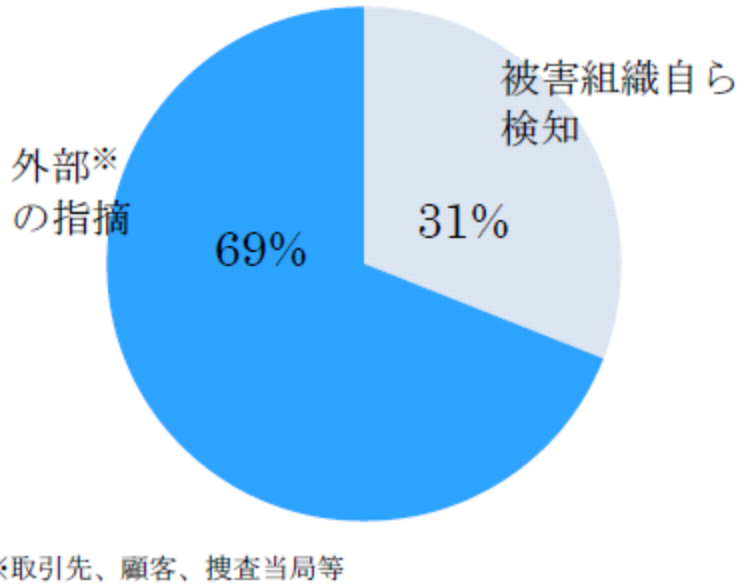


図２　セキュリティ侵害の発覚経緯 [2]

※「サイバーセキュリティ経営ガイドライン」記載の図をそのまま転載

なぜ経営者？　その２

■海外の経営者は意識が高い・・・

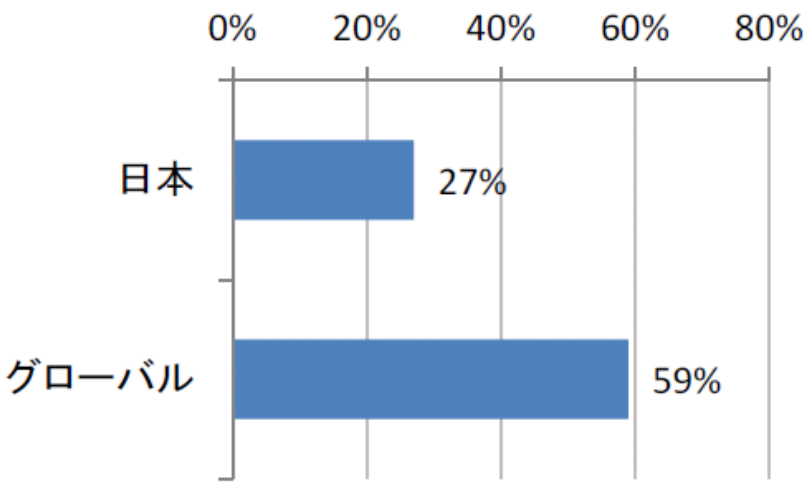


図３　積極的にセキュリティ対策を推進する経営幹部がいる企業 [3]

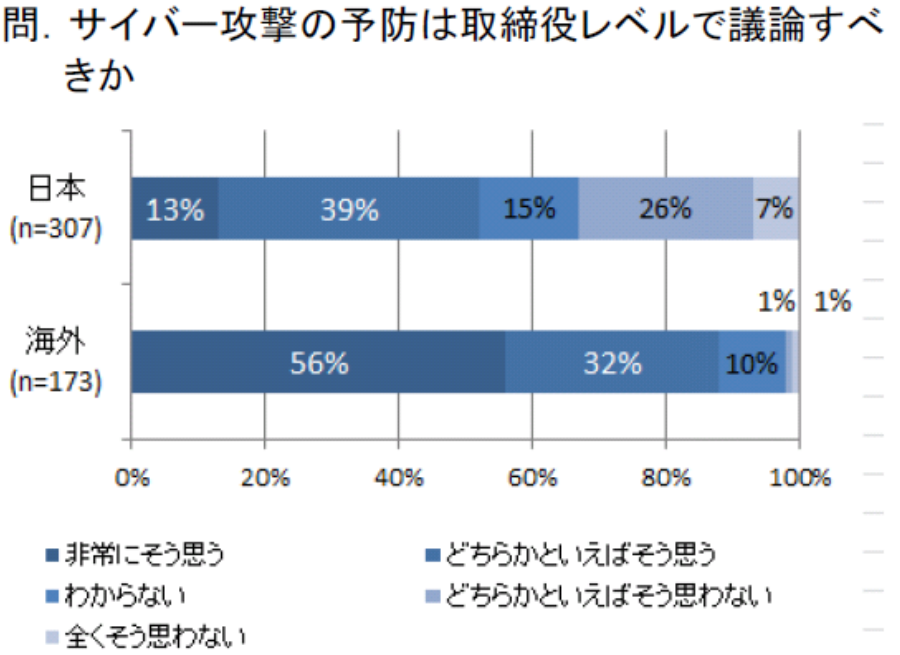


図４　サイバー攻撃への対処を議論するレベル [4]

※「サイバーセキュリティ経営ガイドライン」記載の図をそのまま転載

活用方法

■なお…別のガイドラインも参照

グローバル（n=9,329）

【当ガイドライン】

35% 現行の従業員

30% 退職者

24% ハッカー

18% 委託業者

15% 過去の委託業者

18% わからない

【別ガイドライン】

【参考】　プライスウォーターハウス クーパース　「グローバル情報セキュリティ調査 2015」

3原則

①

【原文】セキュリティ投資に対するリターンの算出はほぼ不可能であり、セキュリティ投資をしようという話は積極的に上がりにくい。このため、サイバー攻撃のリスクをどの程度受容するのか、セキュリティ投資をどこまでやるのか、経営者がリーダーシップをとって対策を推進しなければ、企業に影響を与えるリスクが見過ごされてしまう。

②

【原文】子会社で発生した問題はもちろんのこと、自社から生産の委託先などの外部に提供した情報がサイバー攻撃により流出してしまうことも大きなリスク要因となる。このため、自社のみならず、系列企業やサプライチェーンのビジネスパートナー等を含めたセキュリティ対策が必要である。

③

【原文】ステークホルダー（顧客や株主等）の信頼感を高めるとともに、サイバー攻撃を受けた場合の不信感を抑えるため、平時からのセキュリティ対策に関する情報開示など、関係者との適切なコミュニケーションが必要である。

3原則の要点を解釈

① 経営リーダーの判断が最重要

② 系列・集団として考える

③ 新たな企業コミュニケーション活動

10項目

【原文そのもの】

3．1．リーダーシップの表明と体制の構築
（1）サイバーセキュリティリスクの認識、組織全体での対応の策定
（2）サイバーセキュリティリスク管理体制の構築

3．2 サイバーセキュリティリスク管理の枠組み決定
（3）サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定
（4）サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示
（5）系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握

3．3．リスクを踏まえた攻撃を防ぐための事前対策
（6）サイバーセキュリティ対策のための資源（予算、人材等）確保
（7）IT システム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保
（8）情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備

3．4．サイバー攻撃を受けた場合に備えた準備
（9）緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施
（10）被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

10項目の要点を解釈

分類	10項目
■基本方針	（1）リスク認識とグランドデザイン
	（2）リスク管理体制
■管理の枠組み	（3）目標と計画策定
	（4）PDCAの構築
	（5）系列とパートナー
■防ぐ対策	（6）経営資源の確保
	（7）外部委託対策
	（8）社外コミュニケーション
■有事の対処	（9）対応体制
	（10）開示と広報

付録C　ISO/IEC27000

分類	10項目	ISO/IEC27000
■基本方針	（1）リスク認識とグランドデザイン	5.1／5.2
	（2）リスク管理体制	5.3／6.1
■管理の枠組み	（3）目標と計画策定	5.1／6.1／6.2
	（4）PDCAの構築	7.4／8.1／8.2／8.3／9.1／9.2／10.1／10.2／17.1／18.1／18.2
	（5）系列とパートナー	8.1
■防ぐ対策	（6）経営資源の確保	7.1／7.2
	（7）外部委託対策	8.1／15.1／15.2
	（8）社外コミュニケーション	6.1
■有事の対処	（9）対応体制	16.1
	（10）開示と広報	6.1

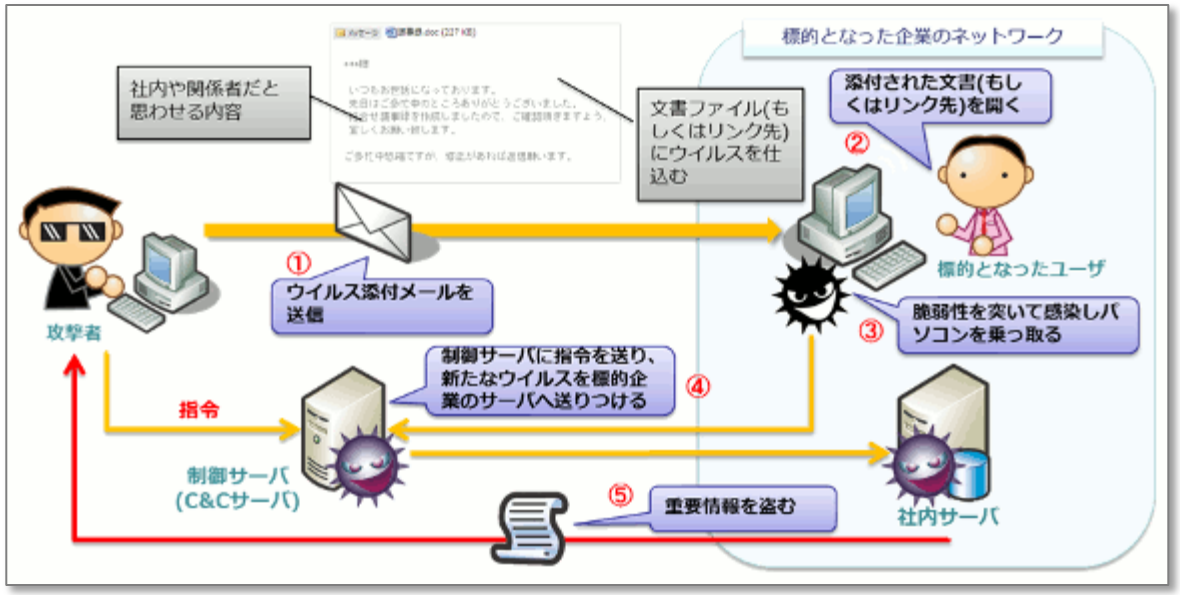
経営者が気にすること

タイミング･･･なぜ『今』か

■経営者の仕事は『変化への対応』

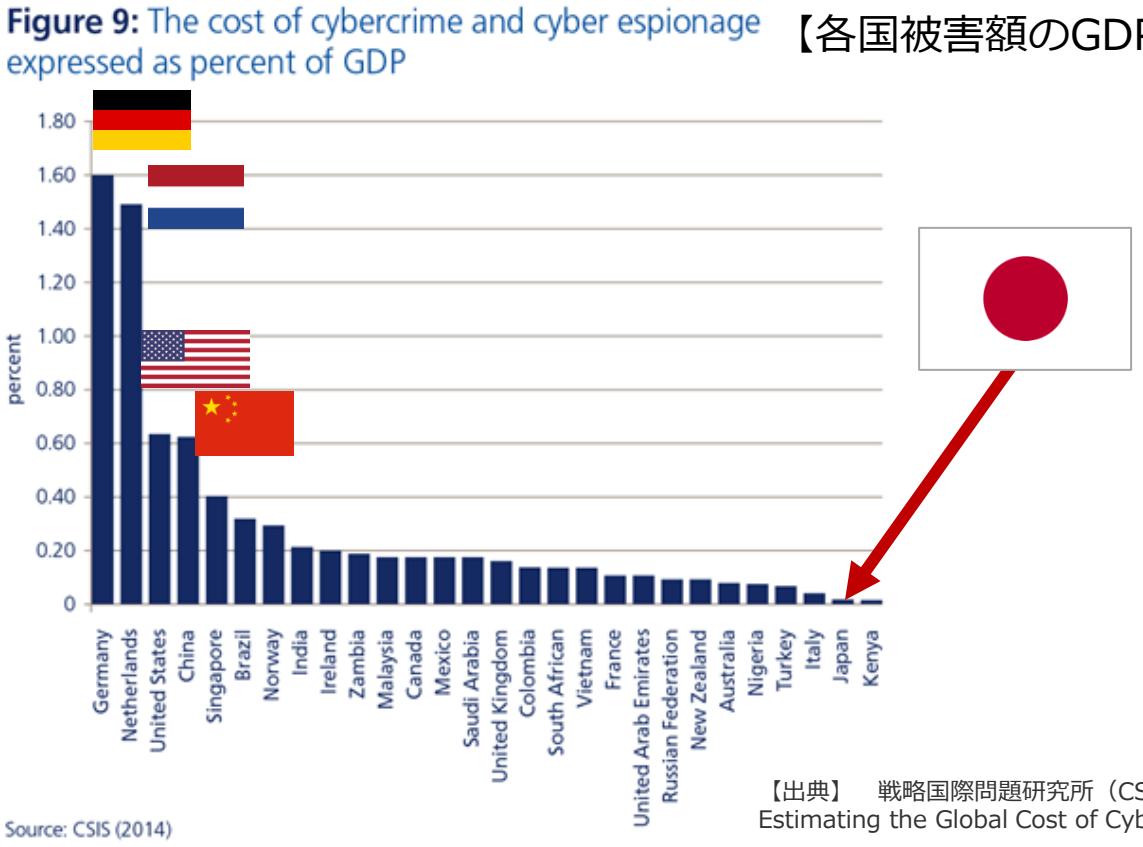
■10年以上前に聞いたサイバー攻撃？

オージス総研Webマガジン（2004年3月号）
「標的型メール攻撃の仕組み」のイラスト



経営環境・・・海外比較

■欧米と事情が違うのでは…



【各国被害額のGDP比】

【出典】　戦略国際問題研究所（CSIS）「Net Losses: Estimating the Global Cost of Cybercrime」2014年6月

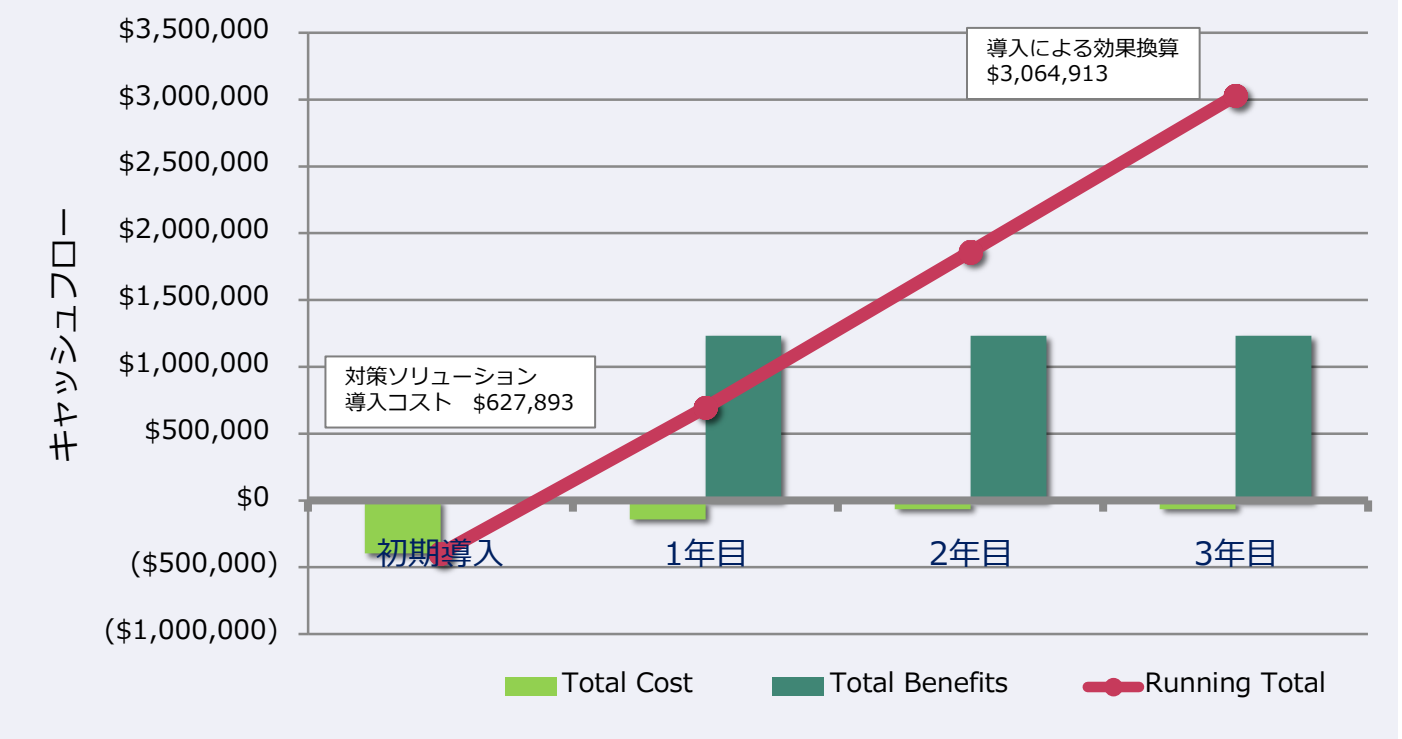
優先順位・・・経営インパクト

不正会計	情報漏えい ← サイバー？
談合・カルテル	従業員や非正規の犯罪行為
特別背任	不当表示
業務上過失致死傷（爆発・火災）	セクハラ・パワハラ
国内での贈収賄	過労死
海外での贈収賄	インサイダー取引
自然災害（地震・異常気象）	環境規制違反
パンデミック	金融規制違反
反社会勢力との関係	製品事故・食品事故
反市場勢力による買収	薬事不正

ROI･･･意思決定の要

■PCエージェント常備型のソリューション

- 日本の自動車会社の米国現地法人では4年4カ月で388%のROI



【出典】米Forrester Research社　The Total Economic Impact Of EnCase Cybersecurity For Incident Response

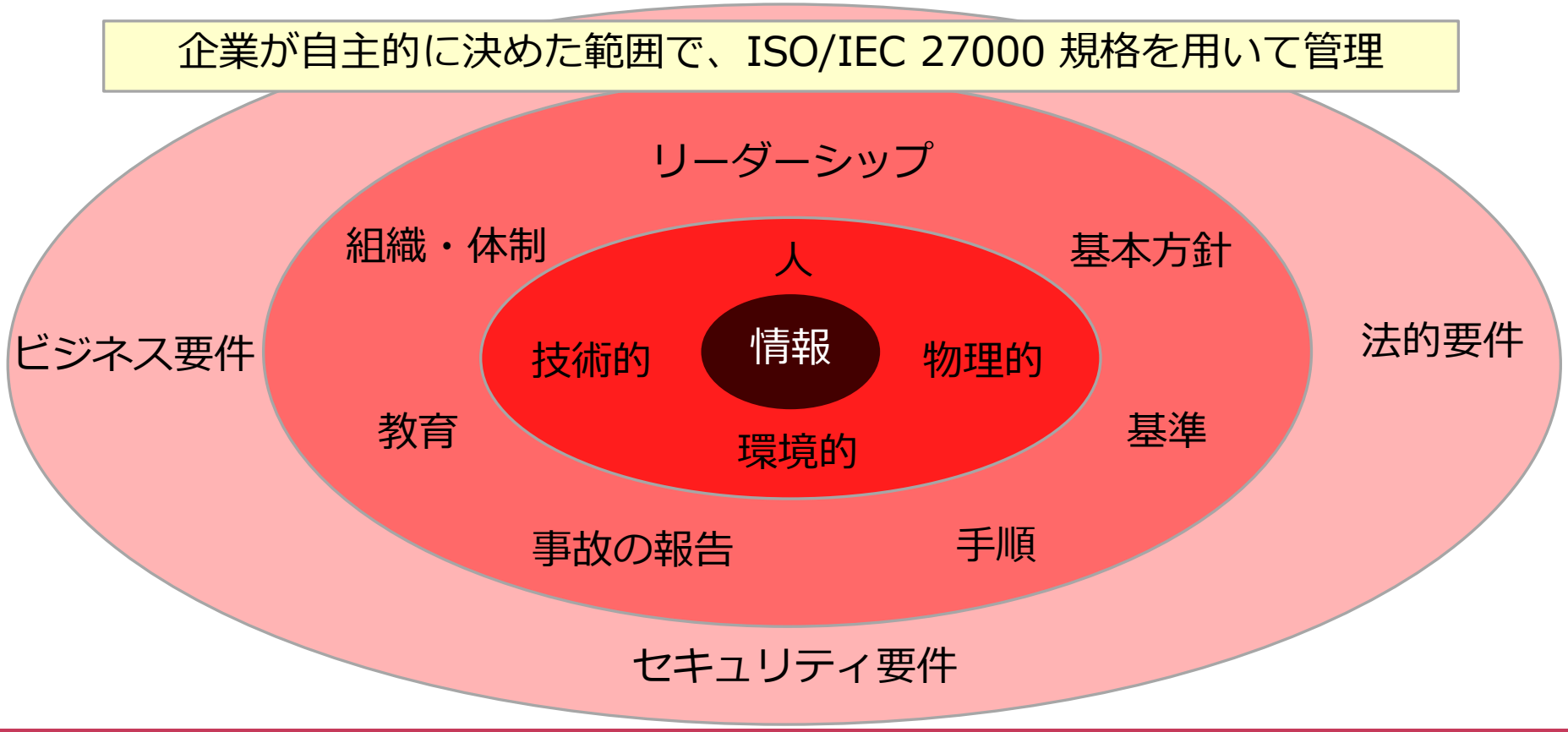
罰則･･･未対応の場合

■取締役の『善管注意義務違反』になる？

法令	内容例	対象条項
■個人情報保護法	安全管理措置義務	20条
	従業者の監督義務	21条
	委託先の監督義務	22条
	主務大臣による報告徴収、勧告、命令の処分	32～34条
	違反・報告未提出・虚偽報告に対する罰則	56～58条
■銀行法	金融機関の場合は、各々の業法が定める 顧客情報の適正取り扱い義務違反として 業務改善命令の対象となりうる	12条2-2 52条44-3
■保険業法		100条2
■金融商品取引法		40条２

既存の管理策・・・だめなのか

■管理策の対象にサイバー攻撃を追加？



体制･･･CISOとCSIRT

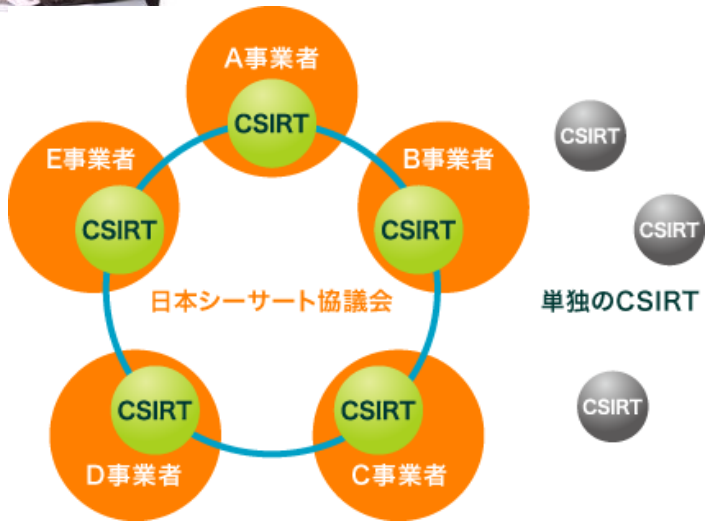
■20ページで「CISO」が18回登場

一般社団法人 日本CISO協会 Japan CISO Association

「経営に役立つ セキュリティの実現に向けて」

ー今こそ問われる CISO の役割

CSIRT 日本シーサート協議会



経営者への提言

ガイドラインの利用は

経営者がリードしないと
解決しない世の中に
なりつつあるようです

として、分かりやすく『補足』しましょう。

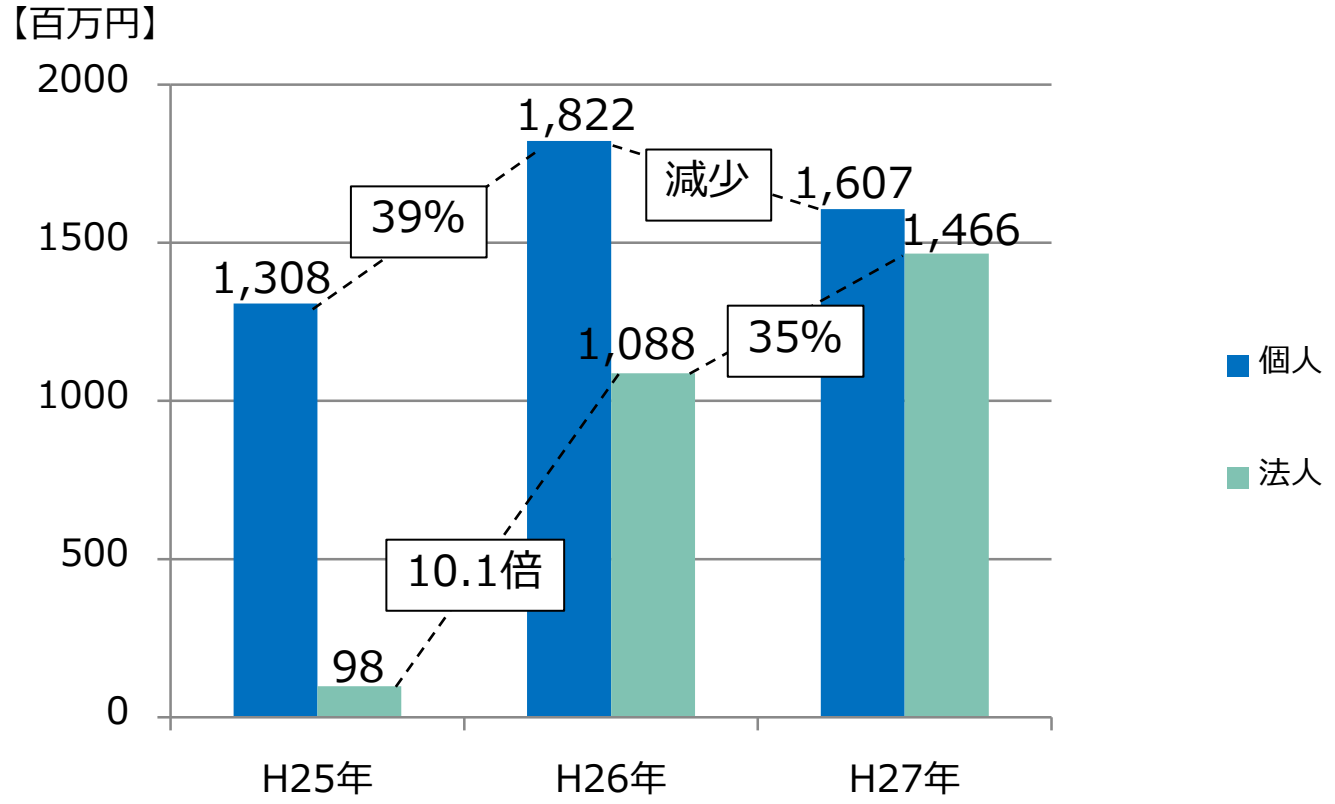
環境変化を伝える：15年

■15年前との比較例

【現在】		【15年前】	
	時価総額　世界１位 57兆円		パソコンメーカー iphone: 2007年
Alphabet	世界２位 53兆円	Google	設立2年 赤字会社
楽天	売上：7,135億円 社員：13,000人		売上：30億円 社員：260人
		無	Facebook：2004年 YouTube：2005年 LINE：2010年

環境変化を伝える：2-3年

■法人被害の例：不正送金10倍→4割増



【参考】　警察庁「平成27年中のインターネットバンキングに係る不正送金事犯の発生状況について」　平成28年3月3日

ガバナンス側の立場の場合

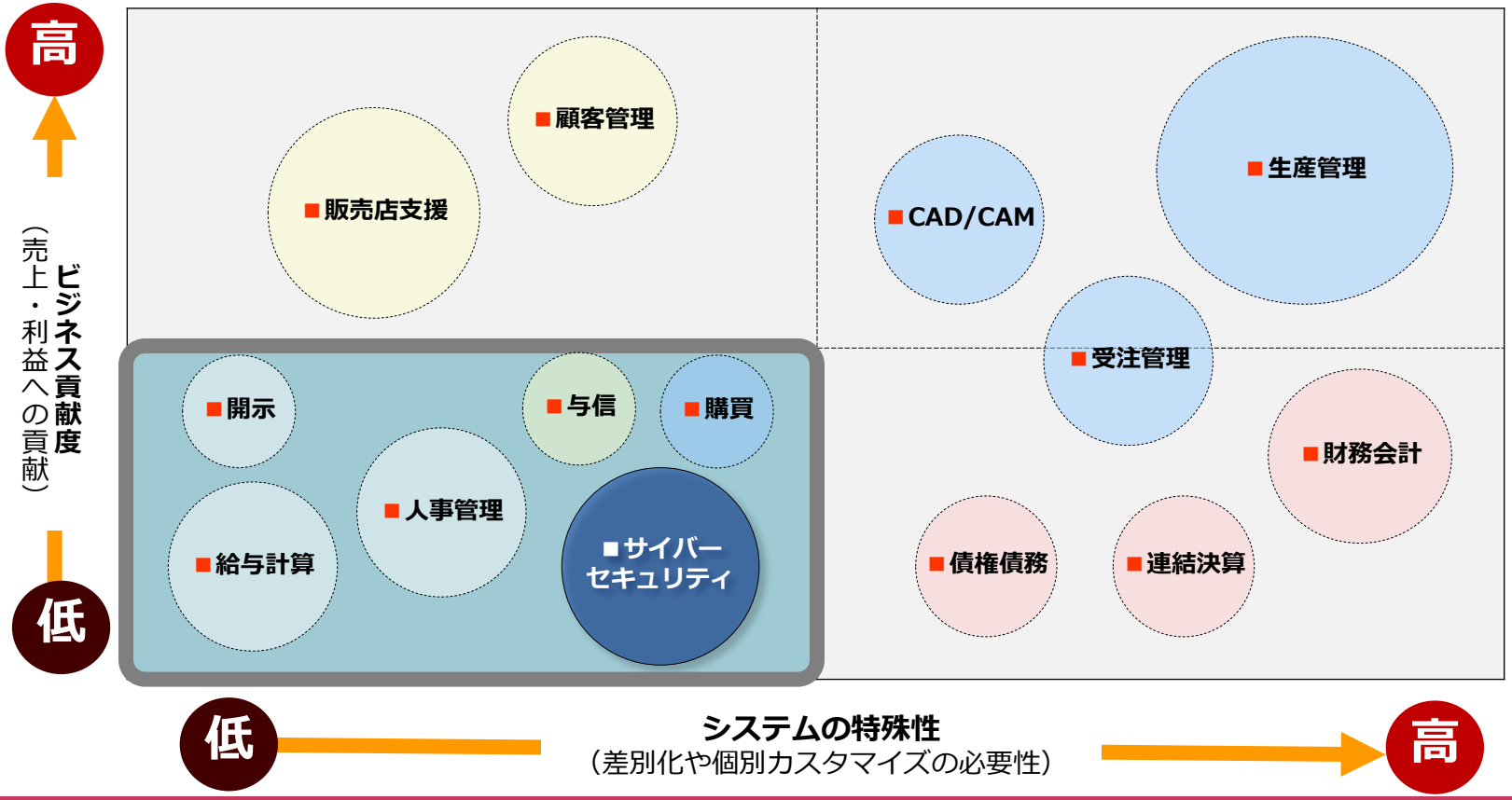
■経営者が見慣れたリスク対応策に付加

仕組みづくりの目的	仕組みと実践プログラム例	
【防止】 未然に防ぐ	●リーダーによるガバナンス	経営陣の役割・経営陣の監視など
	●行動基準の策定と実行	ミッション・バリュー・行動規範など
	●教育研修	啓発プラグラム・テーマ別研修など
	●情報とコミュニケーション	方針・マニュアル・憲章・レターなど
	●評価システム	成果評価・懲罰・採用基準など
【発見】 問題を見つける	●監査とモニタリング	外部/内部監査・自己チェックなど
	●報告体制・相談体制	内部通報制度・ヘルプラインなど
【対処】 適切に対応する	●個別の違反対応	社内手続・外部専門家による対処
	●継続的な改善活動	防止プログラム修正・自己申請制度

サイバー攻撃対応を
各実践プログラムのオプションに

IT企画側の立場の場合

■IT投資を全体のROIバランスで説明する



社内セキュリティの立場の場合

■ISO27000の枠組みの適用範囲拡大

■NISTの枠組導入検討を経営者に提言

- アメリカ国立標準技術研究所
- 元々は重要インフラ向け
- 2014年に枠組みを公開
- 業界別の利用実例がある
- IPAが和訳し公開している

機能の一意の識別子	機能	カテゴリーの一意の識別子	カテゴリー
ID	特定	ID.AM	資産管理
		ID.BE	ビジネス環境
		ID.GV	ガバナンス
		ID.RA	リスクアセスメント
		ID.RM	リスク管理戦略
PR	防御	PR.AC	アクセス制御
		PR.AT	意識向上およびトレーニング
		PR.DS	データセキュリティ
		PR.IP	情報を保護するためのプロセスおよび手順
		PR.MA	保守
		PR.PT	保護技術
DE	検知	DE.AE	異常とイベント
		DE.CM	セキュリティの継続的なモニタリング
		DE.DP	検知プロセス
RS	対応	RS.RP	対応計画の作成
		RS.CO	伝達
		RS.AN	分析
		RS.MI	低減
		RS.IM	改善
RC	復旧	RC.RP	復旧計画の作成
		RC.IM	改善
		RC.CO	伝達

ご支援プログラム

■オリジナル管理者セミナーを提供中

管理者セミナー
企業危機管理

講師
XXXXXXX
ソリトンシステムズ／Ji2

- ●危機管理の基本
- ●実務ポイント
  - ・体制構築・再構築
  - ・予防対策・事前対策
  - ・初動対応
  - ・従業員教育
- ●まとめ

企業の危機管理を最も効率的・効果的に社内構築するための考え方を90分で学ぶ管理者向けセミナーです。

管理者セミナー
サイバー犯罪

講師
XXXXXXX
ソリトンシステムズ／Ji2

- ●サイバー犯罪15年間の動向
- ●2011年以降のサイバー犯罪
- ●直近1年のサイバー犯罪
- ●調査実務の現場から

不正調査専門サービス企業から見たサイバー犯罪のグローバルな動向や、最新事情の全体を90分で俯瞰します。