経営者・マネージャーが知るべき情報セキュリティ

エレクトロニック・サービス・イニシアチブ
大垣　靖男

自己紹介

- 氏名：大垣 靖男（おおがき やすお）
- 職業：
  - エレクトロニック・サービスイニチアチブ代表取締役社長
  - 岡山大学大学院非常勤講師/PHP技術者認定機構顧問など
  - Webサイト構築関連のコンサルティングなど
    - テクニカル・セキュア開発（開発体制・コード検査・ツール販売・セキュリティパッチサービス）など
- ネット
  - http://blog.ohgaki.net/
  - yohgaki – Facebook/Twitterなど
  - yohgaki@ohgaki.net

IoT(Internet of Things)は悪夢

- IoT - あらゆるモノにコンピュータが組み込まれ便利になる世界！
- セキュリティ – まともに管理されていないデバイスの大量出現！

- IoTはセキュリティにとって悪夢のような存在になる

- 管理されていないIoTデバイスだけでなく、攻撃用IoTデバイスの簡単かつ大量に作れる時代がやってきた

便利なIoTデバイス

無線でキー入力を送信

無線で動画・画像を送信

SDカードサイズのPC

CPU付きキーボードデバイス

便利なWiFiデバイス

これらのIoTデバイスは安全に管理される？
5年後？10年後は？












既に危険なIoTの代表例

既に危険なモノの代表例

内容

- 第一部：情報セキュリティの現状は？
- 第二部：体系的なITセキュリティとは？
- 第三部： ITシステム管理に必要な要素とは？
- 第四部： ITシステム開発に必要な要素とは？

第一部
情報セキュリティの現状

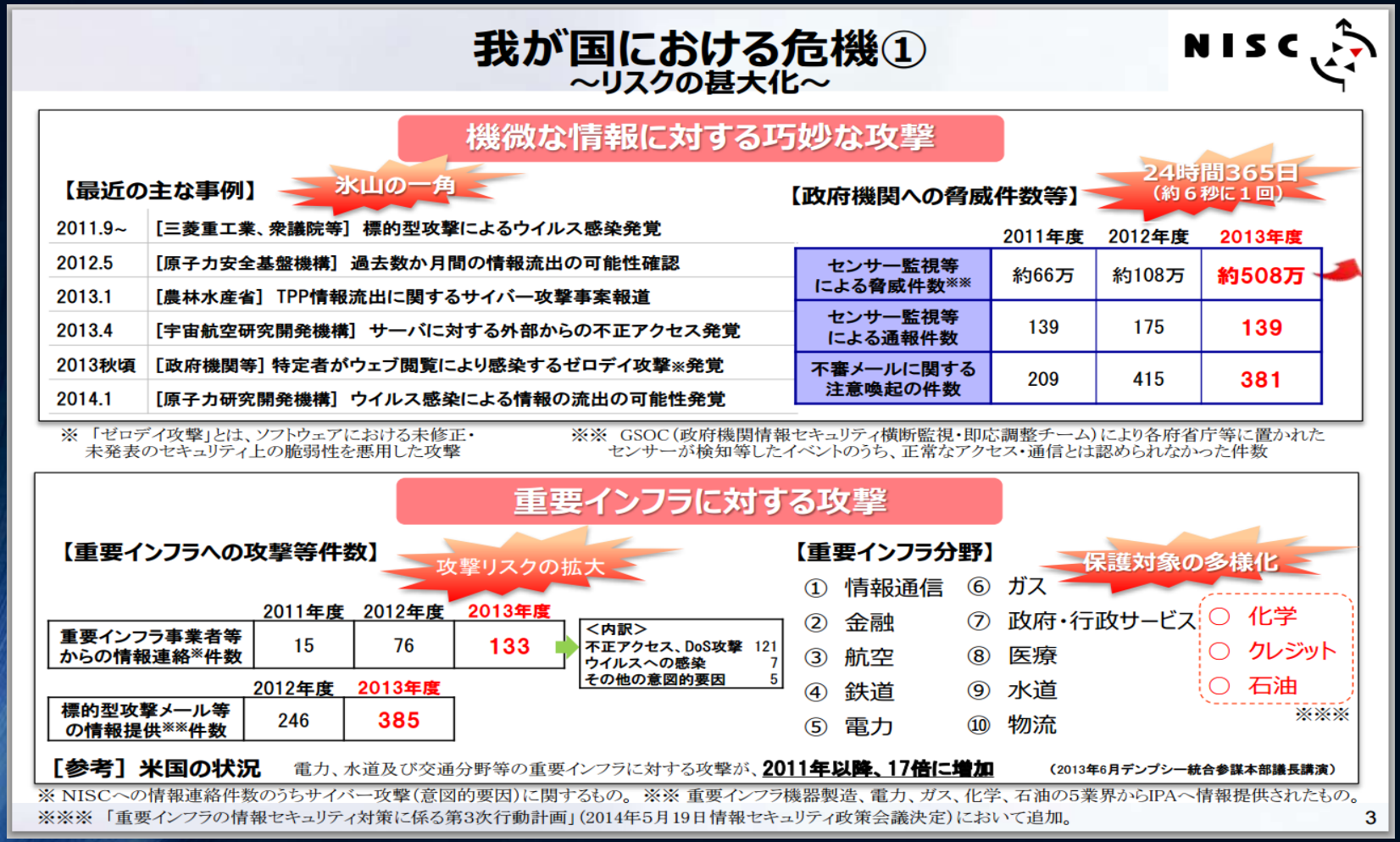
情報セキュリティは薄氷の上

これだけは知って欲しい

情報セキュリティは薄氷の上

全てのIT機器、ユーザーは狙われている

情報セキュリティの現状
我が国のサイバーセキュリティ戦略



我が国における危機①
～リスクの甚大化～

NISC

機微な情報に対する巧妙な攻撃

【最近の主な事例】　氷山の一角

2011.9～	[三菱重工業、衆議院等] 標的型攻撃によるウイルス感染発覚
2012.5	[原子力安全基盤機構] 過去数か月間の情報流出の可能性確認
2013.1	[農林水産省] TPP情報流出に関するサイバー攻撃事案報道
2013.4	[宇宙航空研究開発機構] サーバに対する外部からの不正アクセス発覚
2013秋頃	[政府機関等] 特定者がウェブ閲覧により感染するゼロデイ攻撃※発覚
2014.1	[原子力研究開発機構] ウイルス感染による情報の流出の可能性発覚

※「ゼロデイ攻撃」とは、ソフトウェアにおける未修正・未発表のセキュリティ上の脆弱性を悪用した攻撃

【政府機関への脅威件数等】　24時間365日（約６秒に１回）

	2011年度	2012年度	2013年度
センサー監視等による脅威件数※※	約66万	約108万	約508万
センサー監視等による通報件数	139	175	139
不審メールに関する注意喚起の件数	209	415	381

※※ GSOC（政府機関情報セキュリティ横断監視・即応調整チーム）により各府省庁等に置かれたセンサーが検知等したイベントのうち、正常なアクセス・通信とは認められなかった件数

重要インフラに対する攻撃

【重要インフラへの攻撃等件数】　攻撃リスクの拡大

	2011年度	2012年度	2013年度
重要インフラ事業者等からの情報連絡※件数	15	76	133

＜内訳＞
不正アクセス、DoS攻撃　121
ウイルスへの感染　7
その他の意図的要因　5

	2012年度	2013年度
標的型攻撃メール等の情報提供※※件数	246	385

【重要インフラ分野】　保護対象の多様化

① 情報通信　② 金融　③ 航空　④ 鉄道　⑤ 電力
⑥ ガス　⑦ 政府・行政サービス　⑧ 医療　⑨ 水道　⑩ 物流
○ 化学　○ クレジット　○ 石油　※※※

［参考］米国の状況　電力、水道及び交通分野等の重要インフラに対する攻撃が、**2011年以降、17倍に増加**　（2013年6月デンプシー統合参謀本部議長講演）

※ NISCへの情報連絡件数のうちサイバー攻撃（意図的要因）に関するもの。 ※※ 重要インフラ機器製造、電力、ガス、化学、石油の5業界からIPAへ情報提供されたもの。
※※※ 「重要インフラの情報セキュリティ対策に係る第3次行動計画」（2014年5月19日情報セキュリティ政策会議決定）において追加。

3

出典： http://ogc.or.jp/wp/wp-content/uploads/2014/09/140822Y_Taniwaki.pdf

情報セキュリティの現状
我が国のサイバーセキュリティ戦略

我が国における危機②
～リスクの拡散・グローバル化～

NISC

攻撃の対象範囲の拡散

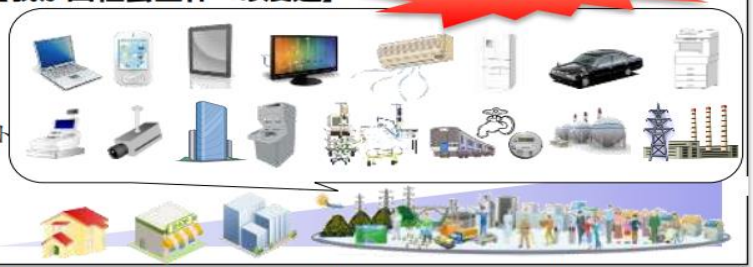
【スマートフォンの普及等】　国民1人1人へ

スマートフォン
世帯保有率が**5倍**に急増※
（2010年末：約10%→**2012年末：約50%**）
携帯端末を標的とする不正サイトが**20倍**に急増
（2011年度末：約3千 → **2013年度末：約5万7千**）

スマートカー
1台に搭載される車載コンピュータは**100個以上**、ソフトウェアの量は**約1000万行**※※

スマートメーター（次世代電力量計）
電力会社による開発・導入の開始
［主な予定］
・東京：2023年度までに**2700万台**の導入完了
・関西：2023年度までに**1300万台**の導入完了

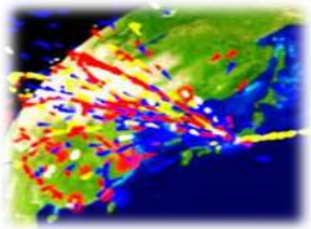
【我が国社会全体への浸透】　いつでもどこでも何でも



※　総務省「平成25年版情報通信白書」
※※　（独）情報処理推進機構（IPA）「自動車の情報セキュリティへの取組みガイド」（2013年8月）

世界中からの多様な主体による攻撃

【海外からの我が国への攻撃状況※】　グローバル化



国名（国コード）	ホスト数	割合
中国（CN）	37,149	47%
韓国（KR）	6,005	8%
日本（JP）	5,820	7%
台湾（TW）	3,351	4%
アメリカ（US）	3,240	4%
ロシア連邦（RU）	2,237	3%
ブラジル（BR）	2,123	3%
香港（HK）	1,608	2%
タイ（TH）	1,504	2%

【最近の主な事例】　国家関与の可能性

2011.3	［韓国］政府機関等の40のウェブサーバへのDDoS攻撃発生 ***→ 日本の家庭用PCが踏み台となり攻撃指令サーバ化***
2013.3	［韓国］重要インフラに対する大規模サイバー攻撃発生 ***→ 使用された不正プログラムが我が国でも同時期に確認***
（参考）	
2013.5	［米国］国家機密や企業機密を窃取する標的型攻撃について、**外国政府・軍の関与の可能性を政府が指摘**※※

※　（独）情報通信研究機構（NICT）のインシデント分析システム「nicter（ニクター）」より（右図は「国別ホスト数Top10」2014年1月22日現在）
※※　ホワイトハウス「営業秘密侵害を低減するための米国政府戦略」（2013年2月）及び国防総省「年次報告書」（2013年5月）

4

出典：　http://ogc.or.jp/wp/wp-content/uploads/2014/09/140822Y_Taniwaki.pdf

国が情報セキュリティ対策に乗り出す理由

- インターネットのインフラ化
- 国家レベル、組織的な情報システムへの攻撃
- 金銭目的に留まらない攻撃目的（スパイ行為、軍事戦略）
- 重要インフラを含むシステムがリスクにさらされる
- 高度化する情報システムへの攻撃
- あらゆる分野で進まない情報セキュリティ対策

- サイバーセキュリティ基本法案（2014年11月）

重要インフラ以外のシステムは大丈夫？！

- 攻撃者は重要インフラ以外のシステムもターゲットにする

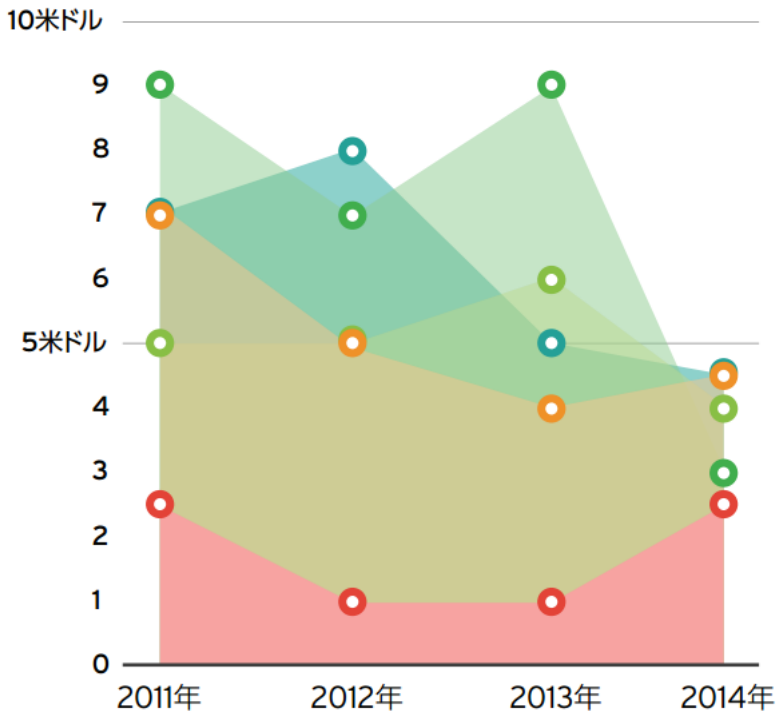
- 攻撃先の踏み台
  - より攻撃価値の高いターゲットへ
  - 重要インフラの攻撃、金銭的価値の高いターゲット

- 直接的な攻撃
  - オンラインバンキング、ランサムウェア、価値のある情報の窃取、スパイ行為

- コンピューターウィルス対策、ネットワークファイアーウォールだけでは守れない

盗んだ情報はお金になる

ロシアのサイバー犯罪アンダーグラウンドで売買されるクレジットカードの価格：年ごとの比較



	2011年	2012年	2013年	2014年
米国	2.50米ドル	1.00米ドル	1.00米ドル	2.50米ドル
オーストラリア	7.00米ドル	5.00米ドル	4.00米ドル	4.50米ドル
カナダ	5.00米ドル	5.00米ドル	6.00米ドル	4.00米ドル
ドイツ	9.00米ドル	7.00米ドル	9.00米ドル	3.00米ドル
イギリス	7.00米ドル	8.00米ドル	5.00米ドル	4.50米ドル

出典：TrendLabs 2014 年 年間セキュリティラウンドアップ

盗んだ情報・アカウントはお金になる

項目	2014 年の価格	用途
盗んだメールアドレス 1,000 件	0.5 ～ 10 ドル	スパム、フィッシング
クレジットカードの詳細	0.5 ～ 20 ドル	不正な購入
本物のパスポートのスキャン画像	1 ～ 2 ドル	個人情報の窃盗
盗んだゲームアカウント	10 ～ 15 ドル	価値の高い仮想アイテムの取得
カスタムマルウェア	12 ～ 3,500 ドル	支払いの流用、ビットコインの窃盗
ソーシャルネットワークフォロワー 1,000 人	2 ～ 12 ドル	ビューアーの関心を引く
盗んだクラウドアカウント	7 ～ 8 ドル	コマンド & コントロール（C&C）サーバーのホスティング
有効な電子メールアドレス 100 万件宛てにスパムを送信	70 ～ 150 ドル	スパム、フィッシング
登録済みで有効なロシアの携帯電話 SIM カード	100 ドル	詐欺

ブラックマーケットで販売される情報の値段

資料作成：シマンテック

インターネットバンキングの不正送金
～ 警察庁まとめ ～

平成26年中のインターネットバンキングに
不正送金事犯の発生状況等について

1　平成26年中の発生状況

（1）発生件数及び被害額　　１，８７６件　約２９億１

期間	件数	被害額（実被害額）
H26	1,876件	約29億1000万円（約24億3600万円）
H25	1,315件	約14億 600万円（約13億3000万円）
H24	64件	約 4800万円（約 4800万円）

・・犯人が送金処理を行ったすべての額

・・「被害額」から金融機関が不正送金を阻止した額を差し

多くの地方銀行や信用金庫・信用組合に
座に係る被害が拡大（別紙「１」、「２」

緊急対策により急激に減少
凍結口座などによる阻止率
H26上期 7.6%
H26下期31.4%

金融機関は“個人”の
被害は補償
法人の被害は無保証

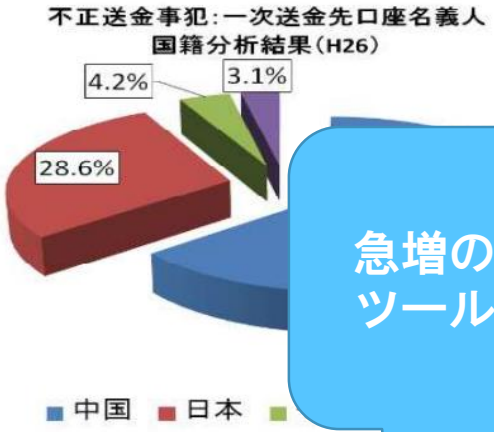
約15万 5,000件の国内の感
染端末利用者に対する注意
喚起

https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf

不正送金の逮捕者

4　一次送金先口座名義人の国籍

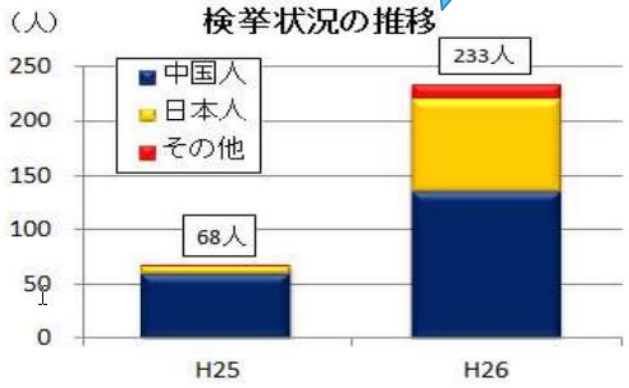
国籍	H26		H25	
	口座数	割合	口座数	割合
中国	2420	64.1%	1642	70.9%
日本	1079	28.6%	469	20.2%
その他	157	4.2%	129	5.6%
法人	118	3.1%	77	3.3%
合計	3774	100.0%	2317	100.0%



急増の理由は攻撃用ツールの流通が原因

5　関連事件の検挙状況

		H26		H25		増加数
検挙事件		115件		34件		+ 81
検挙人数		233人		68人		+ 165
内訳	中国人	134人	57.5%	59人	86.8%	+ 75
	日本人	86人	36.9%	7人	10.3%	+ 79
	その他	13人	5.6%	2人	2.9%	+ 11



https://www.npa.go.jp/cyber/pdf/H270212_banking.pdf

インターネットバンキングの不正送金対策

- まだまだ不十分
- 多くの金融機関でログインに脆弱な暗号表を未だに利用
- 金融先進国では普及しているトランザクション認証なし

【ワンタイムパスワードカード】の概要】

項目	【本件】ワンタイムパスワードカード
デザイン	
大きさ	縦7cm×横4.5cm×厚さ0.3cm
新規発行手数料	無料
再発行手数料	1,080円
対象取引	みずほダイレクト[インターネット/モバイルバンキング]
ワンタイムパスワード発行機能	あり
トランザクション認証機能	あり
お申込方法	みずほダイレクト[インターネットバンキング]/みずほ銀行店頭

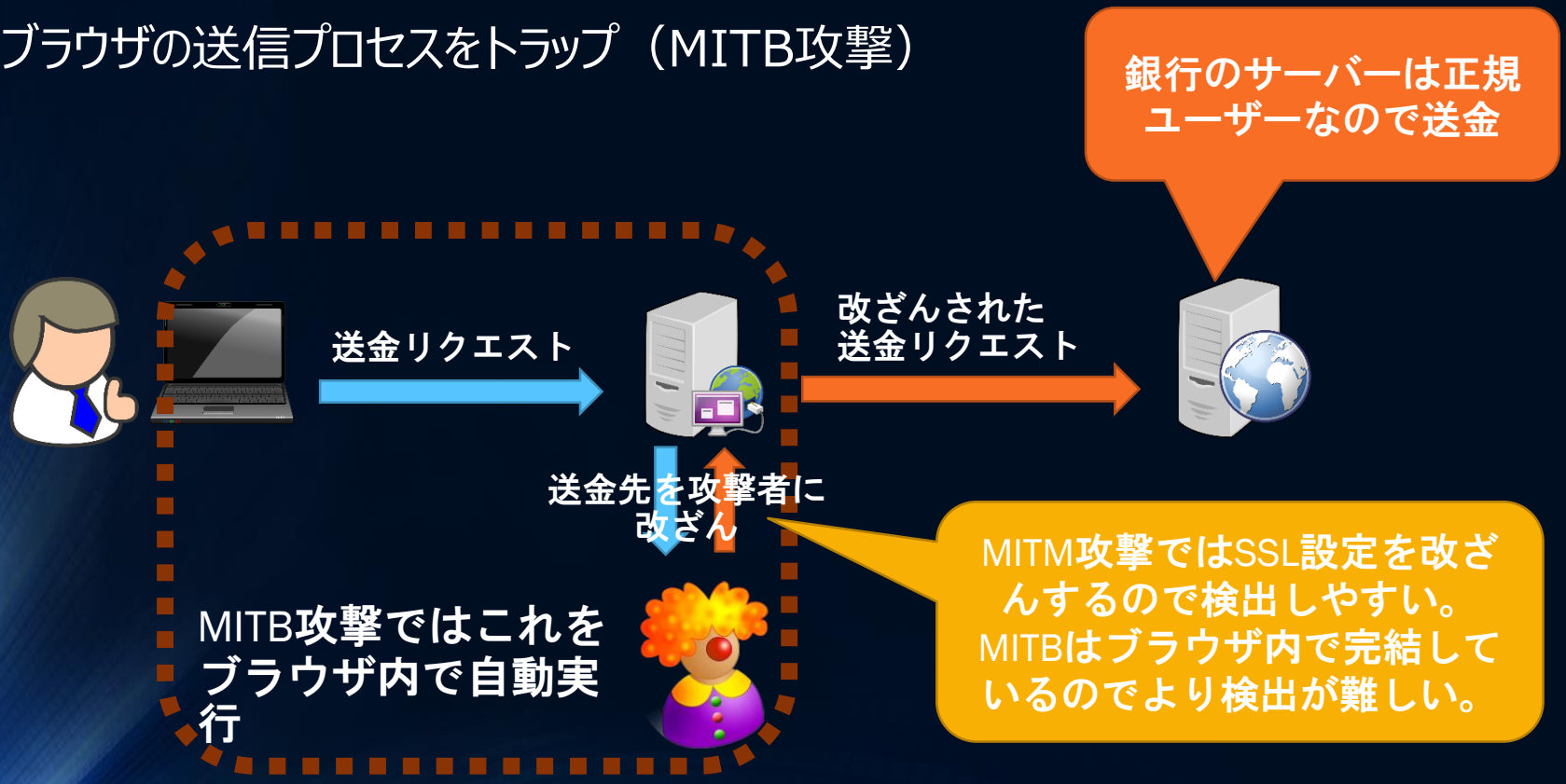
邦銀初のトランザクション認証導入はみずほ銀行
2015年3月より導入

トランザクション認証とは、送金処理のたびに変化する一時的なパスワードを利用し不正な送金を防止する仕組み

ログイン時の一時的パスワードとは異なる仕組み

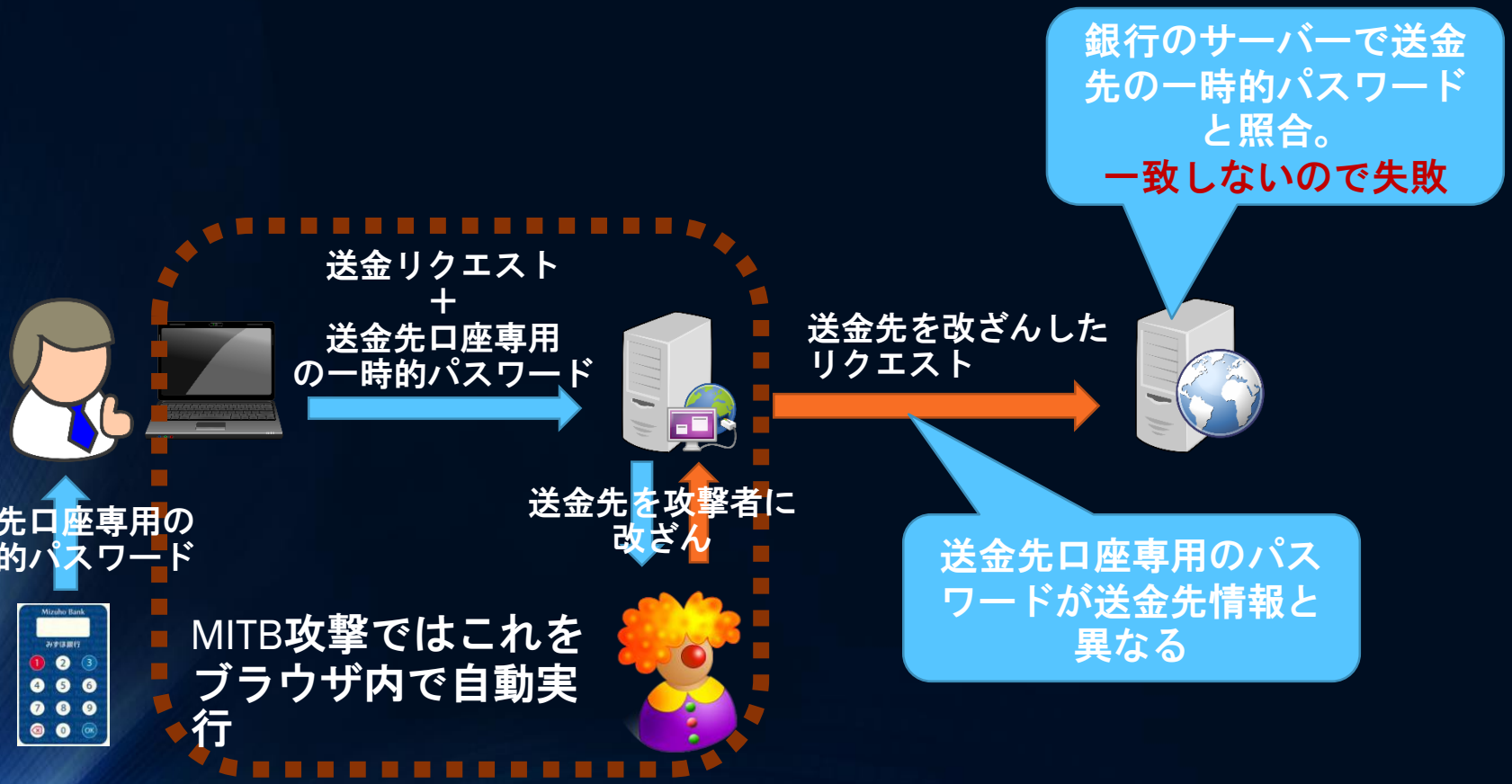
トランザクション認証が必要な理由

- ログイン時のワンタイムパスワードでは不正送金は防げない
  - 不正なSSL認証局の登録して中継（MITM攻撃）
  - ブラウザの送信プロセスをトラップ（MITB攻撃）



トランザクション認証の仕組み

- 送金情報と一緒にトランザクション（送金先、金額など）と一緒に「トランザクション用のパスワード」を設定して送信



攻撃者のROI
ランサムウェア(身代金攻撃)の場合

ランサムウェアとは被害者のファイルを暗号化し、復号の身代金を要求。
３０日間の攻撃を行った場合の試算
出典：2015 Trustwave Global Security Report

投資

項目	投資
攻撃ツール購入	$3000
脆弱性購入	$500
トラフィック購入	$1800
暗号化費用	$600
合計支出	$5900

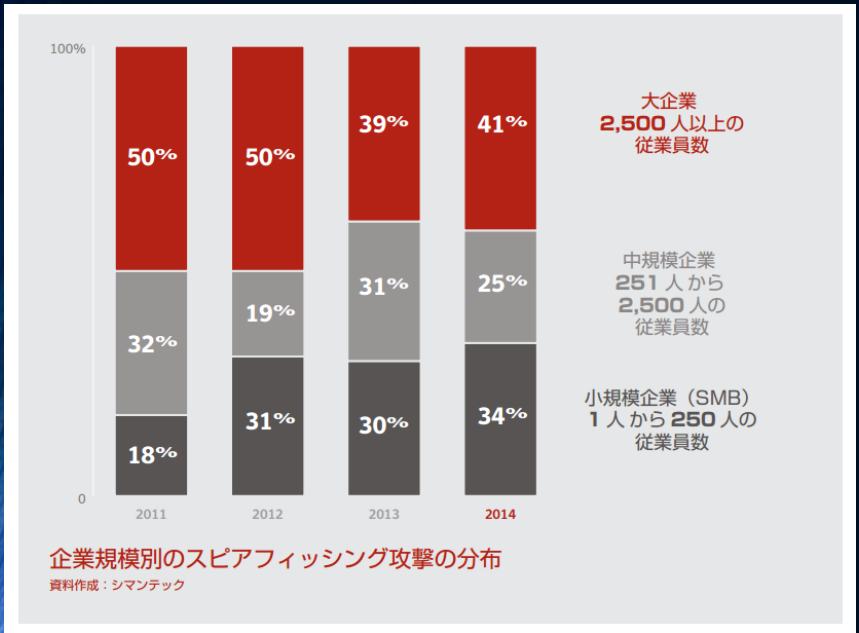
収入

項目	値
訪問者	20000
感染率	10%
身代金支払い率	0.5%
身代金	$300
合計収入	$90000

$5900の投資、一ヶ月の攻撃で$90000のリターン

ROI 1425%

規模の大小にかかわらずターゲット

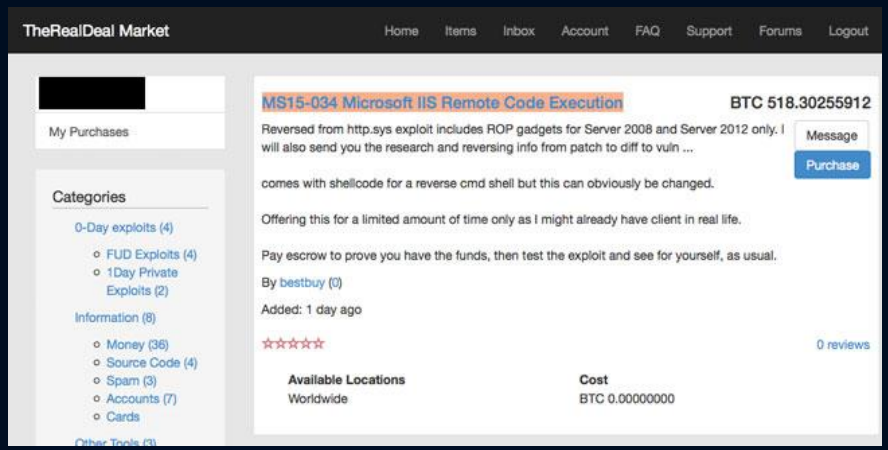


企業規模別のスピアフィッシング攻撃の分布
資料作成：シマンテック

- インターネットバンキング攻撃の増加が欧米より遅かったことと同様に、小規模会社への標的型メール攻撃が国内で増えると予想される
- 欧米より攻撃の波が遅れるのは「言葉の障壁」のおかげ
- 最近では「言葉の障壁」が小さくなってきている
- 個人も勿論ターゲット

攻撃ツールや脆弱性情報の入手ルート

- 攻撃ツール、脆弱性情報を取引するマーケットが存在
- 日本以外の国では何年も前からマーケットが確立
- 新しい攻撃ツールの価格は比較的高価だが、攻撃ツールが再販され低価格化
- 脆弱性情報は比較的安価な物も多い
  - 数十万ドルで取り引きされる場合も



無視できない愉快犯

NHK NEWSWEB

2015年（平成27年）7月4日［土曜日］

トップページ › 社会ニュース一覧 › “ハッカー”少年「身代金要求型」ウイルス作成か

ニュース詳細

“ハッカー”少年「身代金要求型」ウイルス作成か

7月1日 18時43分

発信元の特定を難しくする特殊なソフトを使って、東京の出版社のサーバーに不正にアクセスしたなどとして１７歳の少年が逮捕された事件で、少年のＵＳＢメモリーから、パソコンのデータを勝手に暗号化して金銭を要求する「身代金要求型」と呼ばれるウイルスが見つかった
は去年
いがある

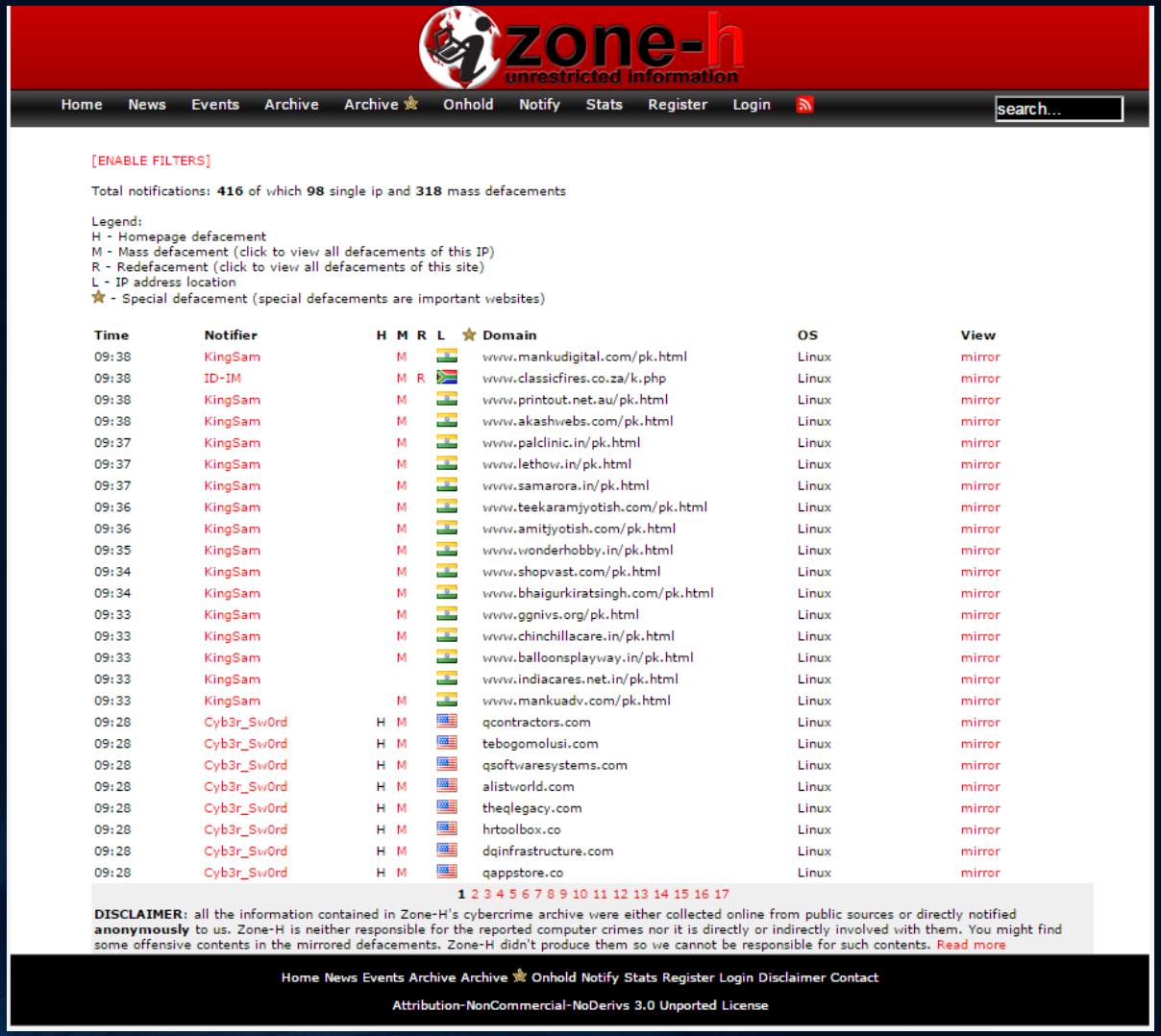
この事件
「Ｔｏｒ」を使い、自宅のパソコンから東京の出版社のサーバ
１７歳の無職の少年が不正アクセス禁止法違反などの疑いで警
ているということです。
警視庁などによりますと、少年は、インターネット上で「０Ｃｈ
し、その状況をツイッターなどでアピールするハッカーとして知られていますが、押収されたＵＳＢメモリーからパソコンのデータを勝手に暗号化して金銭を要求する「身代金要求型」と呼ばれるウイルスが見つかったことが警視庁への取材で分かりました。

この少年は技術評論社のサーバーに悪戯目的で侵入したこと、他のWebサイトを攻撃したとTwitterで発言したことが知られている。

なぜサイバー犯罪者が捕まらないのか？

- 匿名化ネットワーク（Tor）
  - 大手SNSサービスなどはTorに対応し利用できない
  - Torネットワークから匿名プロキシーサーバーを経由
- 先の少年の場合、更にクラックしたWiFiアクセスポイントから接続
- この少年はランサムウェアも作っていたようだが、単純な悪戯攻撃も多数行っていた模様
  - 悪戯攻撃は特に表面化しずらい
- 日本国内にもこの少年のような犯罪者は少なからずいる
- Webサイト改ざんには国境はない
  - 脆弱なサーバーは簡単に攻撃できる

Webサイト改ざんレポートサイトの例



zone-h
unrestricted information

Home News Events Archive Archive ★ Onhold Notify Stats Register Login search...

[ENABLE FILTERS]

Total notifications: **416** of which **98** single ip and **318** mass defacements

Legend:
H - Homepage defacement
M - Mass defacement (click to view all defacements of this IP)
R - Redefacement (click to view all defacements of this site)
L - IP address location
★ - Special defacement (special defacements are important websites)

Time	Notifier	H	M	R	L	★	Domain	OS	View
09:38	KingSam		M				www.mankudigital.com/pk.html	Linux	mirror
09:38	ID-IM		M	R			www.classicfires.co.za/k.php	Linux	mirror
09:38	KingSam		M				www.printout.net.au/pk.html	Linux	mirror
09:38	KingSam		M				www.akashwebs.com/pk.html	Linux	mirror
09:37	KingSam		M				www.palclinic.in/pk.html	Linux	mirror
09:37	KingSam		M				www.lethow.in/pk.html	Linux	mirror
09:37	KingSam		M				www.samarora.in/pk.html	Linux	mirror
09:36	KingSam		M				www.teekaramjyotish.com/pk.html	Linux	mirror
09:36	KingSam		M				www.amitjyotish.com/pk.html	Linux	mirror
09:35	KingSam		M				www.wonderhobby.in/pk.html	Linux	mirror
09:34	KingSam		M				www.shopvast.com/pk.html	Linux	mirror
09:34	KingSam		M				www.bhaigurkiratsingh.com/pk.html	Linux	mirror
09:33	KingSam		M				www.ggnivs.org/pk.html	Linux	mirror
09:33	KingSam		M				www.chinchillacare.in/pk.html	Linux	mirror
09:33	KingSam		M				www.balloonsplayway.in/pk.html	Linux	mirror
09:33	KingSam						www.indiacares.net.in/pk.html	Linux	mirror
09:33	KingSam		M				www.mankuadv.com/pk.html	Linux	mirror
09:28	Cyb3r_Sw0rd	H	M				qcontractors.com	Linux	mirror
09:28	Cyb3r_Sw0rd	H	M				tebogomolusi.com	Linux	mirror
09:28	Cyb3r_Sw0rd	H	M				qsoftwaresystems.com	Linux	mirror
09:28	Cyb3r_Sw0rd	H	M				alistworld.com	Linux	mirror
09:28	Cyb3r_Sw0rd	H	M				theqlegacy.com	Linux	mirror
09:28	Cyb3r_Sw0rd	H	M				hrtoolbox.co	Linux	mirror
09:28	Cyb3r_Sw0rd	H	M				dqinfrastructure.com	Linux	mirror
09:28	Cyb3r_Sw0rd	H	M				qappstore.co	Linux	mirror

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17

DISCLAIMER: all the information contained in Zone-H's cybercrime archive were either collected online from public sources or directly notified **anonymously** to us. Zone-H is neither responsible for the reported computer crimes nor it is directly or indirectly involved with them. You might find some offensive contents in the mirrored defacements. Zone-H didn't produce them so we cannot be responsible for such contents. Read more

Home News Events Archive Archive ★ Onhold Notify Stats Register Login Disclaimer Contact

Attribution-NonCommercial-NoDerivs 3.0 Unported License

Webサイト改ざんレポートの例

.jpドメインの検索例

7/4の検索結果
見てわかるように同じ日に多数の改ざんが登録される傾向がある

.jp以外の日本のサイト、登録されない攻撃もあるので実態はこの数倍はあると考えるべき

.jpドメインサイトの改ざん例

URLから判断するとこのサーバーは完全な乗っ取りが可能

クラッカー同士の攻撃も珍しくない
～ 脆弱性売買サイト 改ざん前 ～

web.archive.orgのコピー

Inj3cto0rと名乗るクラッカーのサイト
1337day.com

攻撃のため閉鎖？

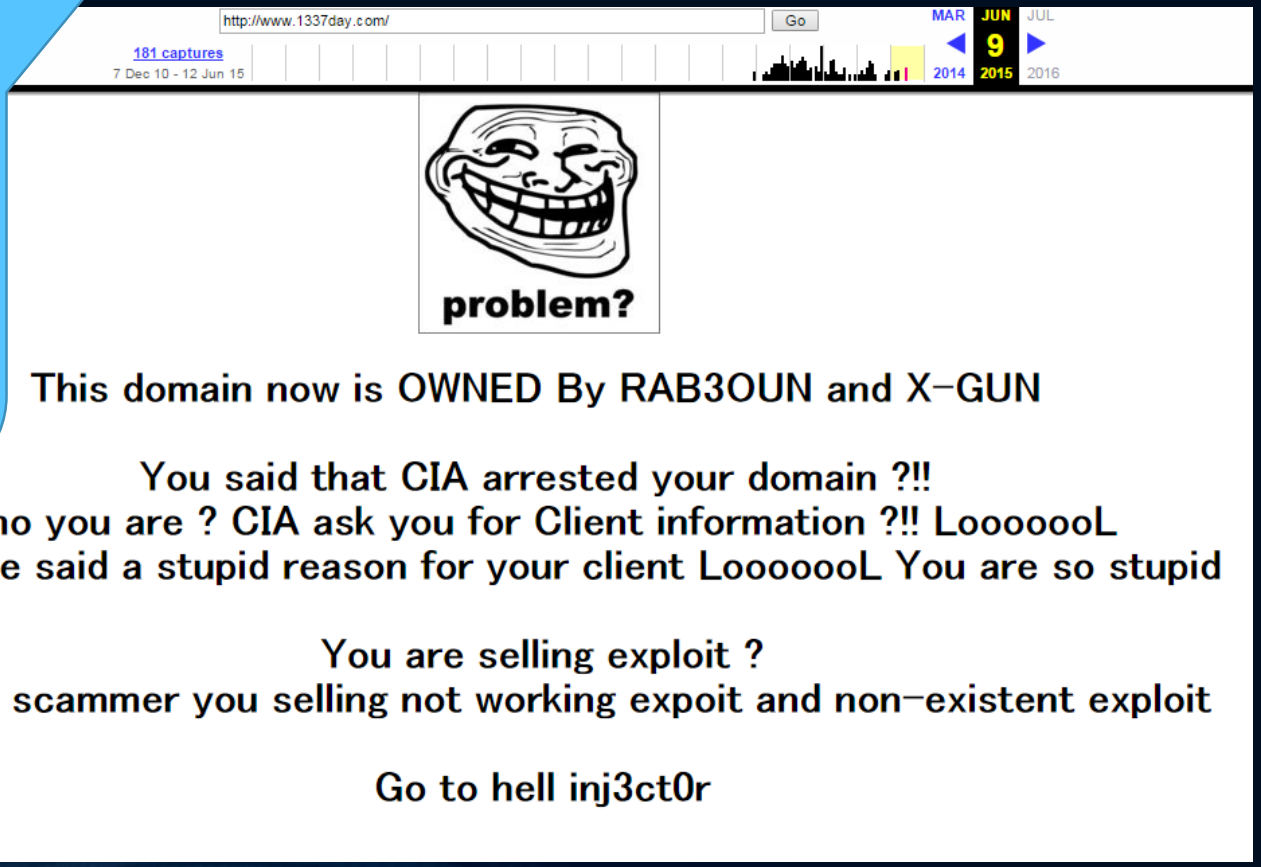
代替サイトの0day.today
も閉鎖中？

クラッカー同士の攻撃も珍しくない ～ 脆弱性売買サイト 改ざん後 ～

Zone-hには2013に過去2回サイトが改ざんされた記録がある。

サイトを閉鎖に追い込んだと思われる2015年のサイト改ざんはZone-hに登録されいない。

Date	Notifier	H	M	R	L	Domain
2013/07/09	TurkGuvenligi.Info	H	M			www.priv8.1337day.com
2013/05/15	TurkGuvenligi.Info	H	M			www.1337day.com



実は、攻撃は簡単

- 必要な情報とツールの入手が簡単
  - インターネットでいくらでも手に入る。先の少年程度の攻撃なら中学生でも可能
- 無料ツールが多数
  - ネットワークスキャナは攻撃対象の検出にも使える
  - 脆弱性検査ツールは攻撃にも使える
  - 脆弱性のPoC（実証コード）は攻撃にも使える
  - フィンガープリンティングでリモートのOS/アプリとそのバージョンまで分かる
  - 多少の知識があればこれらを使いこなせる
- 有償ツールの入手も容易
  - そもそも攻撃目的のツールが販売されている
  - 攻撃用脆弱性が販売されている
  - ボットネットも販売からレンタルシステムまである

例えばWiFiの乗っ取りは簡単

- 問題
  - WEPは脆弱すぎる
  - WPSは仕組みとして脆弱
  - WPA2でもパスワードが簡単だと攻撃される
- 対策
  - WEPは無効にする
  - WPSは無効にする
  - WPA2 AESより強い方式を利用する
  - WPA2のパスワードは強いパスワード
    - 完全にランダムで十分に長い
    - 40文字以上

https://www.youtube.com/watch?v=g-cKTPLRnEE

例えばSQLインジェクション攻撃は簡単

- http://sqlmap.org/ ツールの例：
  - 攻撃者は攻撃可能な場所を見つけるだけ
  - 攻撃可能な場所は脆弱性修正情報として公開されている
  - インターネットで脆弱なシステムを検索すれば攻撃し放題

https://www.youtube.com/watch?v=0hrRevHi1Hg

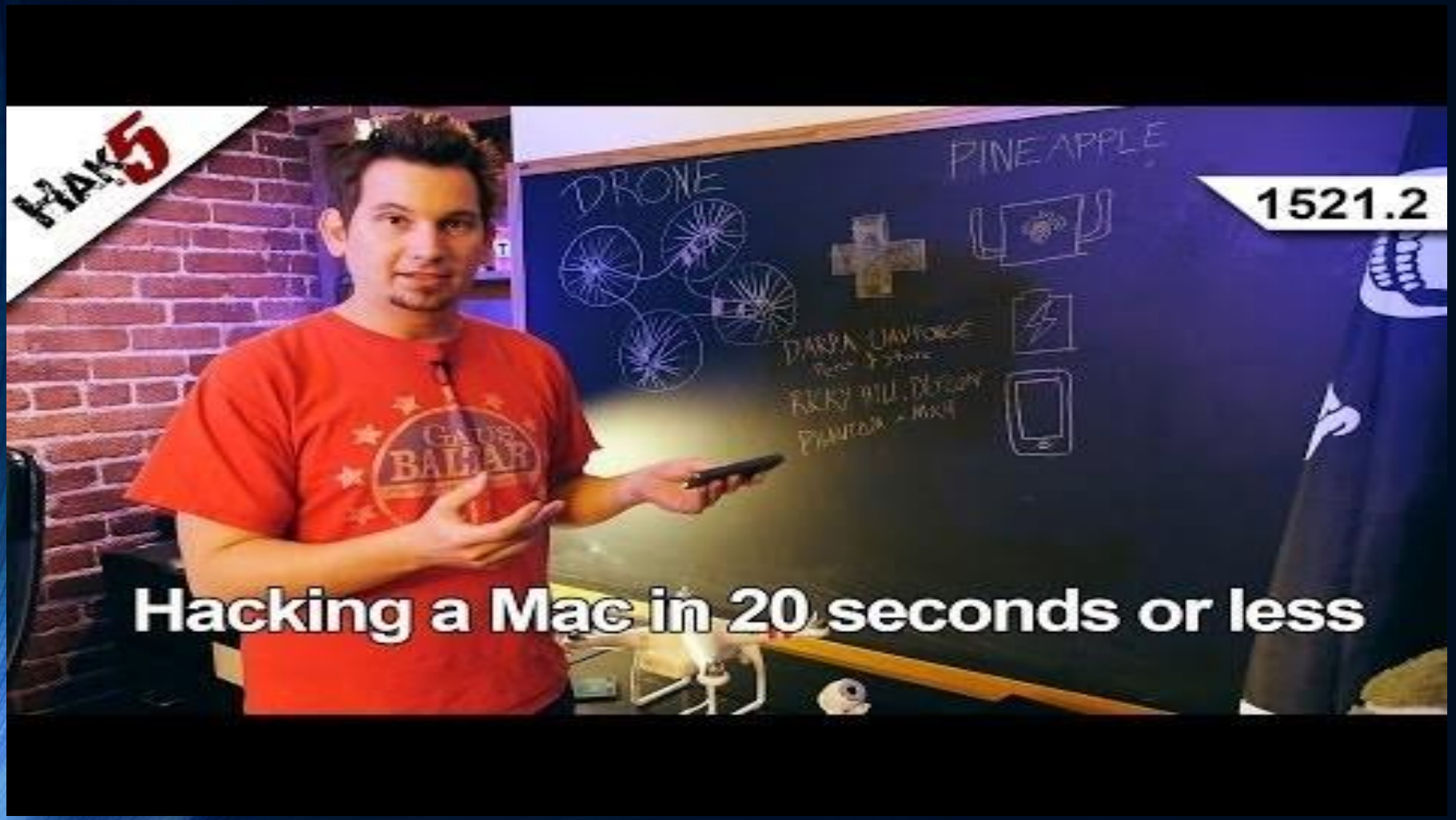
SQLインジェクション攻撃でできる事

- データベースサーバー種類の検出
- データベース構造の解析
- データベース情報の窃取・改ざん・破壊
- 他のデータベースへの攻撃（SSRF）
- 任意ファイルのダウンロード・アップロード
- 任意コマンド・コードの実行
- データベース脆弱性の攻撃（権限昇格など）

動画で気軽に学べるクラッキング
～ ネットワークのスキャン ～

https://www.youtube.com/watch?v=TyUtnOb-kS0

動画で学べるクラッキング
～ Macを20秒で乗っ取る方法 ～



https://www.youtube.com/watch?v=-ve_H-Ua6pQ

代表的な攻撃の手法・対象

- 標的型メール攻撃
- 水飲み場攻撃
- モバイルデバイスへの攻撃
- PC以外のデバイスの攻撃
- リスト型攻撃
- ドライブバイダウンロード攻撃
- WiFiネットワークへの攻撃
- Webシステム脆弱性攻撃
- サービス不能攻撃
- POSシステム
- 電話システム（VoIP・PBX）
- 脆弱なシステムのスキャン
- 盗聴
- ランサムウェア
- インターネットバンキング
- クレジットカード情報
- 個人情報
- 内部犯による犯行

標的型メールの例

標的型メールの特徴

NISC

①差　出　人：情報 太郎 [johou.taro@cas-go.jp]
　宛　　先：二鋤 次郎
②件　　名：【重要】放射線量の状況
③添付ファイル：放射線量.zip

④関係各位

いつもお世話になっております。内閣官房の〇〇〇〇です。現在の放射線量についてまとめました。添付を確認ください。
また、添付ファイルと併せて、以下のURLもご確認ください

⑤http://www3.cas.go.jp/mapserch/ ⇒ 表示は偽装できます！

クリックすると

http://10.243.23.11/詐欺/

①差出人のアドレスを確認
@より右側が省庁ドメイン（.go.jp）でない

②件名で開封を急がせる
「重要」「緊急」などを付加

③添付ファイルの確認
アイコンを文書のように偽装
・.exe等はウィルスの可能性

放射線量.doc.exe

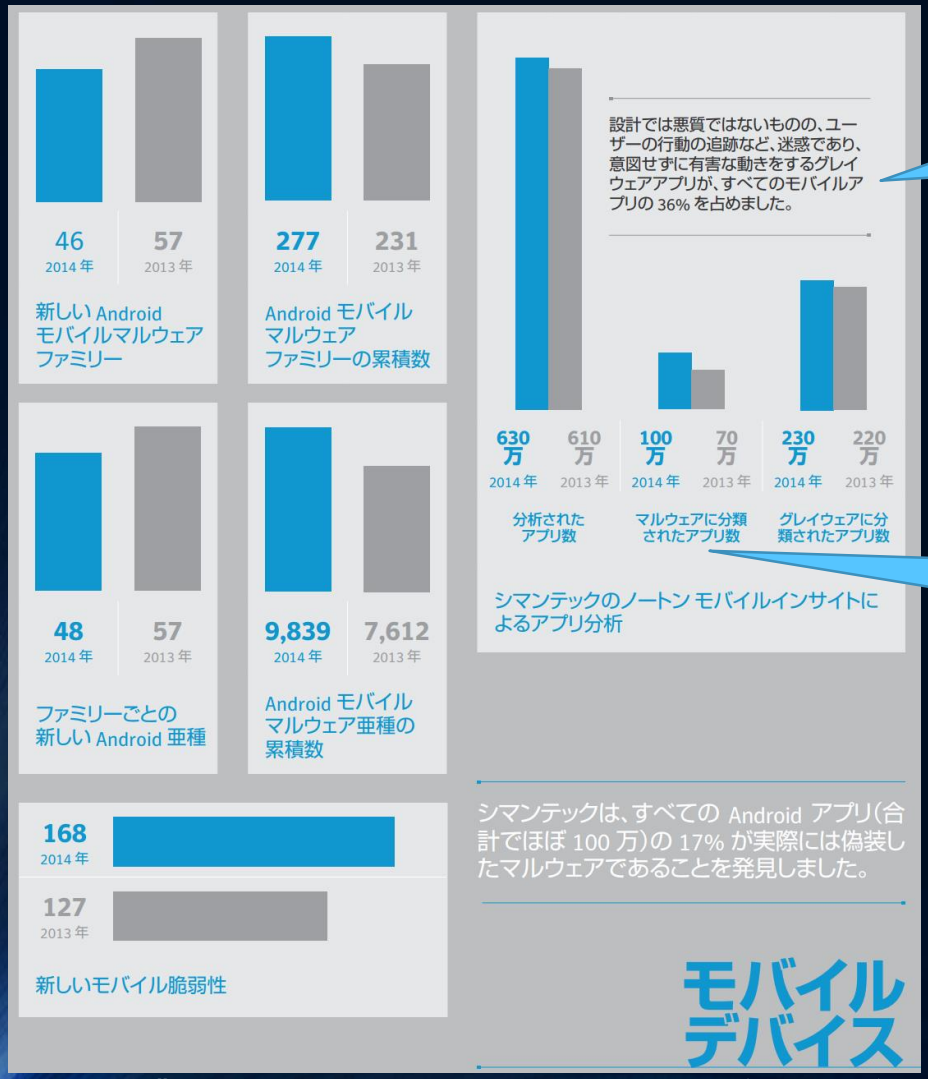
④メール本文は本物のコピー
・発信者に送信したかを確認

⑤リンク先表示
全く別のアドレスに偽装可能

9

出典：http://ogc.or.jp/wp/wp-content/uploads/2014/09/140822Y_Taniwaki.pdf

モバイルデバイスとアプリの脅威



1/3以上のモバイルアプリが不振な動作

1/6ほどのモバイルアプリがマルウェア

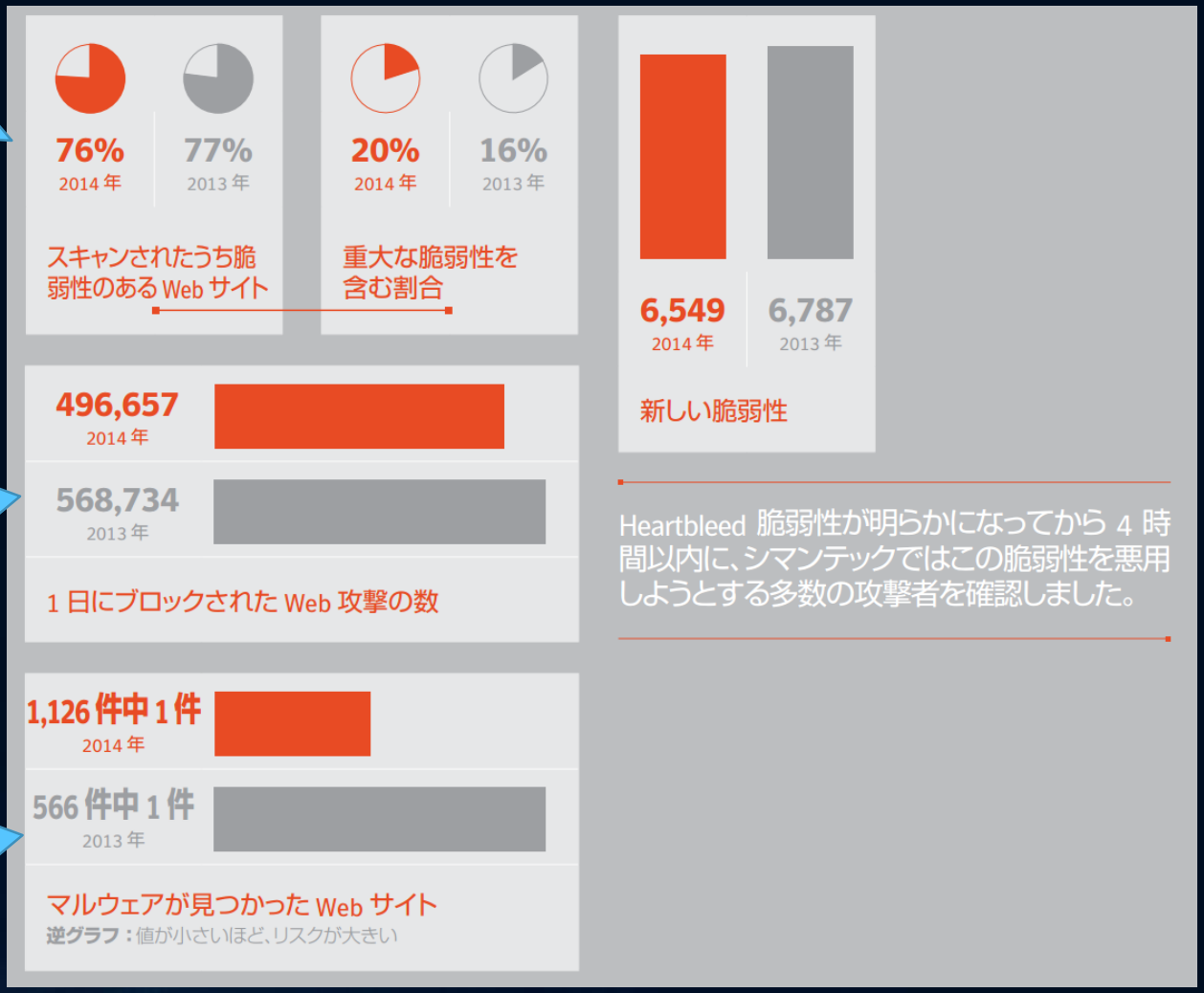
出典： INTERNET SECURITY THREAT REPORT 20（Symantec）

Webシステムの脅威

問題があるWebサイトは少なくない

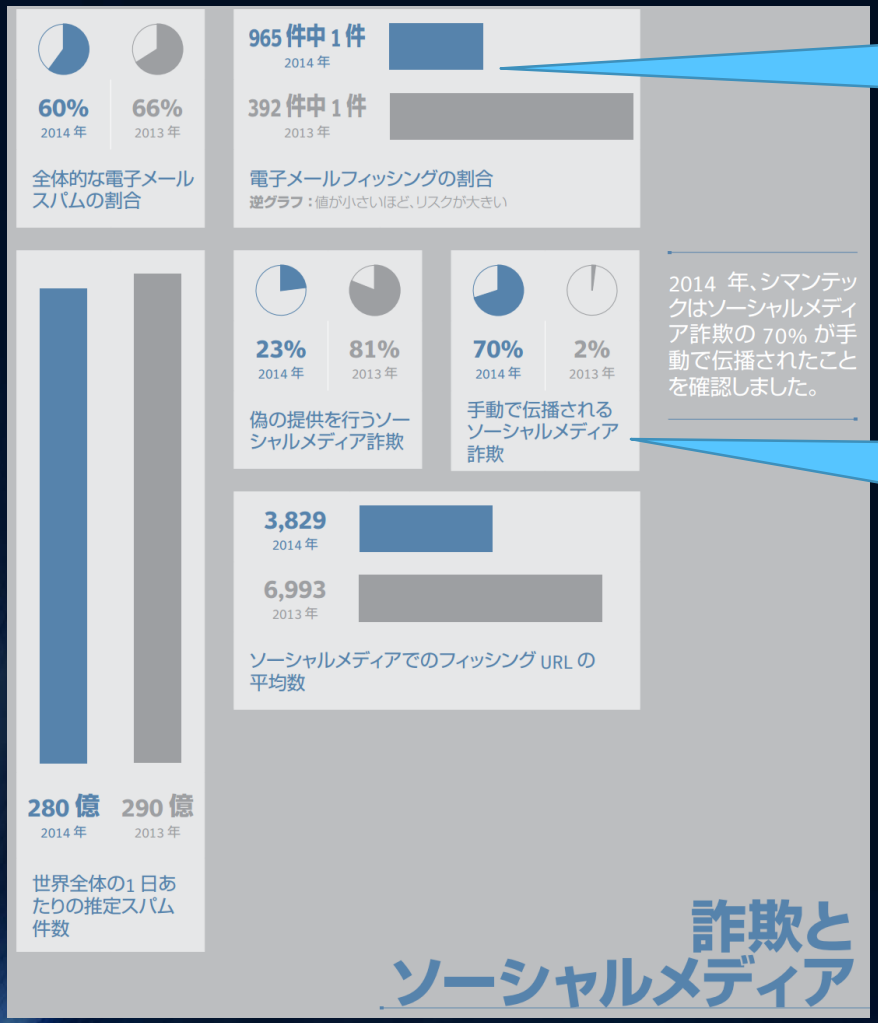
検出された一日あたりの攻撃数

不正なソフトがインストールされたサイトも少なくない



出典： INTERNET SECURITY THREAT REPORT 20（Symantec）

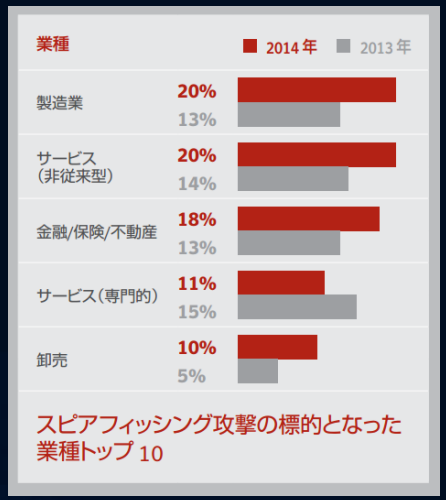
メールとSNSの脅威



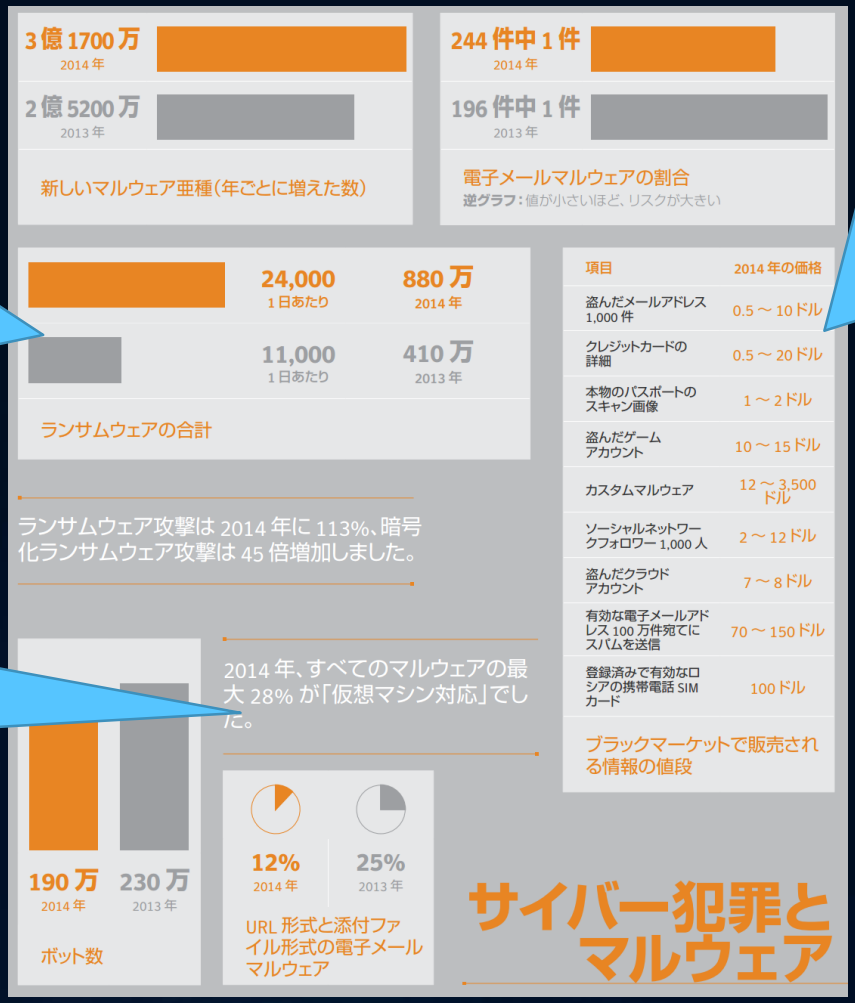
出典： INTERNET SECURITY THREAT REPORT 20（Symantec）

電子メールのフィッシングは減少傾向

SNSを利用したフィッシングが急増



サイバー犯罪とマルウェア



ランサムウェアが急増中（TrendMicroの資料では減少）

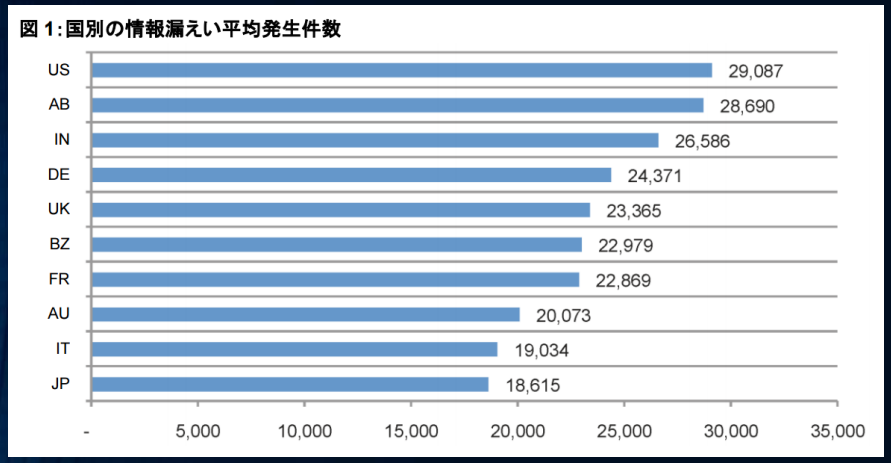
仮想環境に対応したマルウェアが28%

サイバー犯罪マーケットによる分業

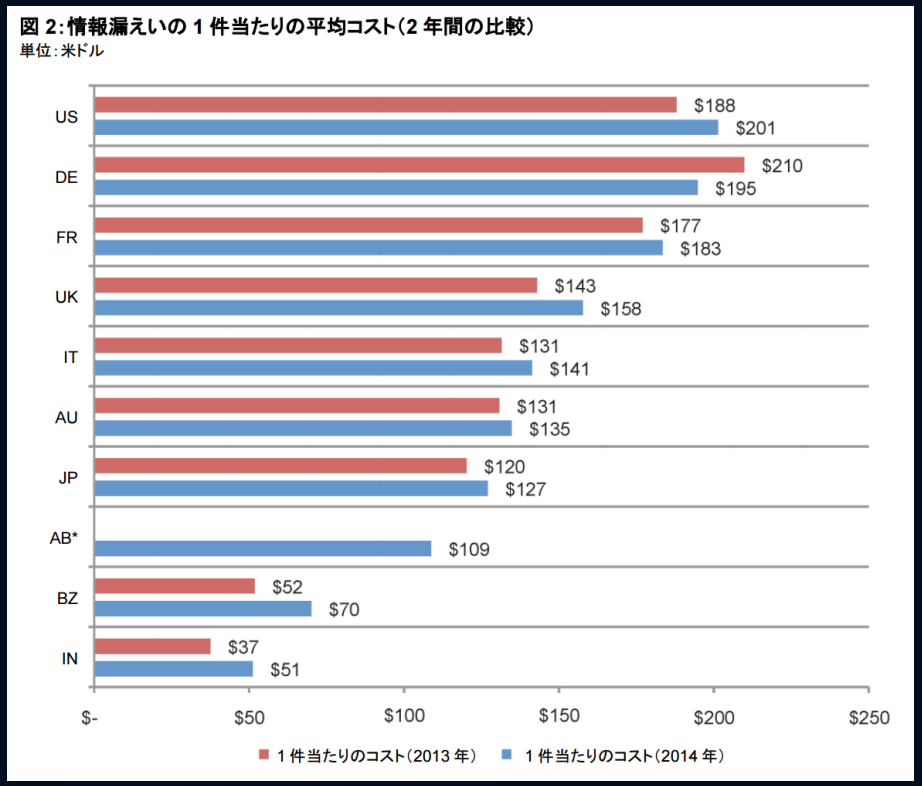
サイバー犯罪者もリスクマネージメントを行っている

出典：INTERNET SECURITY THREAT REPORT 20（Symantec）

情報漏えいの平均コスト



2014年に公表されている情報漏えい事件
国内26件の漏えい件数とコスト（IBM発表）

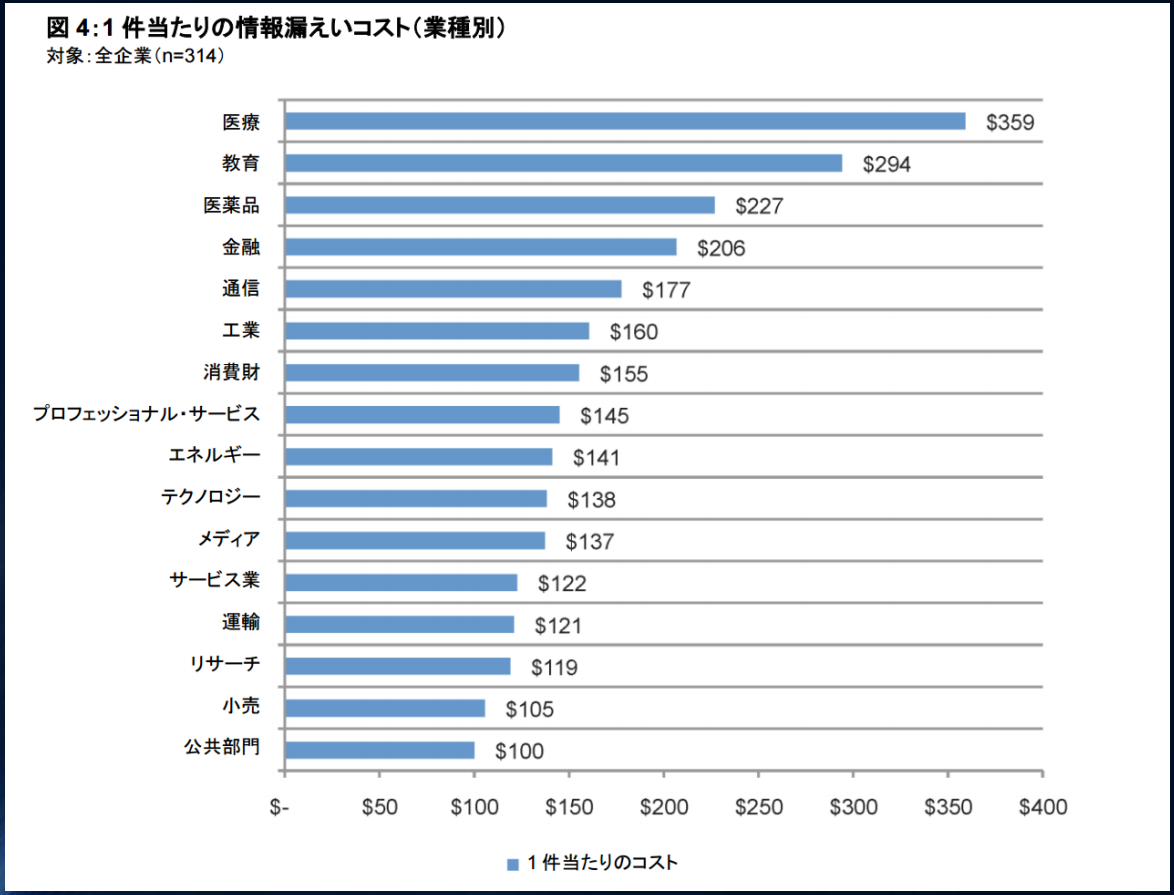


項目	数値
平均漏えい件数	18,615件
1件当たりの平均コスト	127ドル 約15000円
平均漏えいコスト	約2億7600万円

出典：2014 年情報漏えいのコストに関する調査： グローバルな分析

情報漏えいの平均コスト

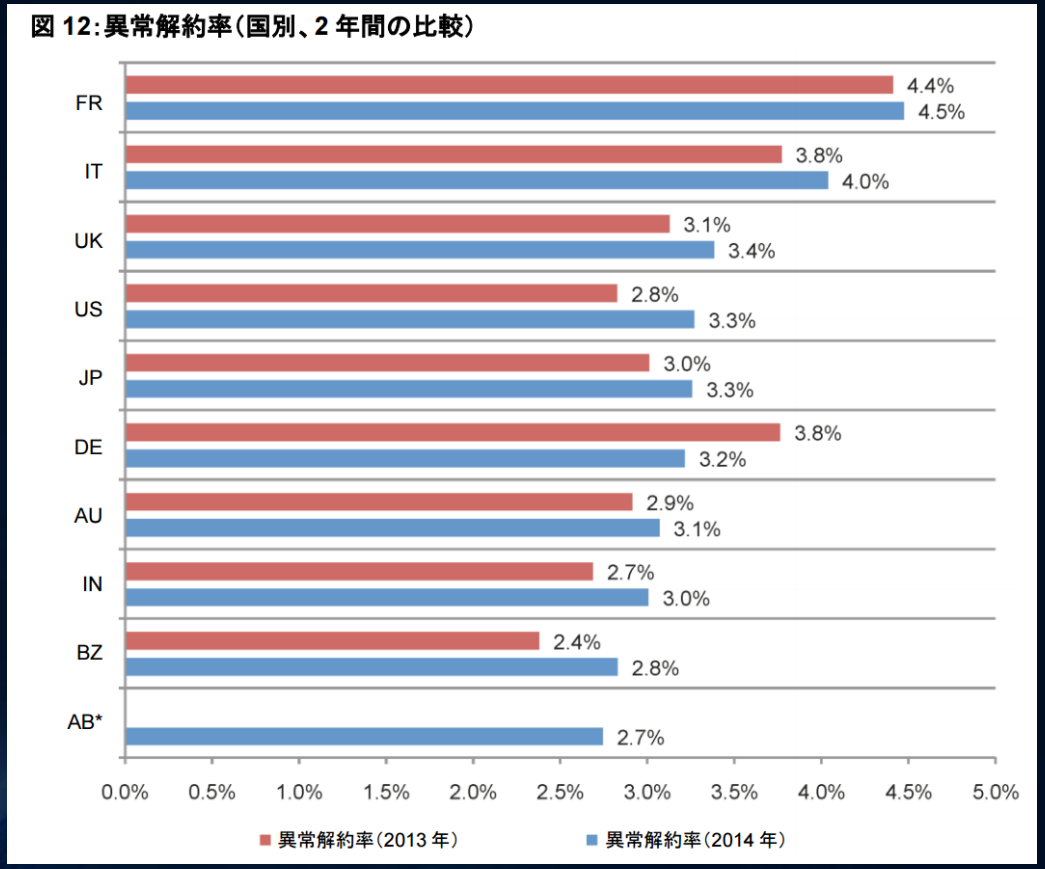
1996年の米HIPAA（Health Insurance Portability and Accountability Act of 1996;医療保険の携行性 と責任に関する法律）影響が大きい



出典：2014 年情報漏えいのコストに関する調査： グローバルな分析

情報漏えいの平均コスト

医療、金融などで影響が大きいが全産業で異常解約が見られる



出典：2014 年情報漏えいのコストに関する調査： グローバルな分析

意外な手法で盗まれる秘密情報

これらはほんの一例！

- キーボードのタイプ音でパスワードなどのキー入力を解析
- コンピュータの電磁波ノイズで秘密鍵を解析
- プログラムのレスポンス時間解析でパスワードなどを解析
- 圧縮済み暗号化データの微妙なサイズ変化で秘密情報を解析
- 指向性アンテナを用い4km先のWiFiシステムに接続
- ブラウザでWebページを表示しただけで内部ネットワークのコンピュータをスキャン
- 罠サイトにアクセスするだけで脆弱なルーターのシステムプログラムを入れ替えて乗っ取り
- 本物のURLでアクセスしても攻撃者のサイトに接続
- WiFiやホテルのネットワークに接続したら攻撃
- Webサイトの広告を表示するだけ、クリックするとマルウェアに感染

ソフィス 7 Deadly I.T. Sins ～ ITの7つの大罪 ～

1. 管理無きモバイル
2. 保護無きMac
3. 安全無きWI-FI
4. 暗号化無きEメール
5. 不完全なファイアウォール
6. 暗号化無きファイル
7. 不十分なWEBフィルタリング

出典：https://www.sophos.com/ja-jp/lp/sevendeadlysins.aspx?cmp=701j0000000ZaL5AAK

実は、よくできているWindows

- Windows＋Active Directory（AD）＋マイクロソフトのツール類を使うとかなり高度なシステム管理が容易に行える
  - ADによるポリシー/ユーザー管理（USBデバイスの無効化など、フェデレーションサービスによるアカウント統合）
  - SharePointによるRMS（Rights Management System)の自動化
  - SystemCenterによる統合管理
  - きめ細かいセキュリティ設定、システムイベントの管理

- MacはWindowsのような高度な管理を行うことが容易ではない
  - 結果としてMacは管理されていない状態で放置

APTとは？

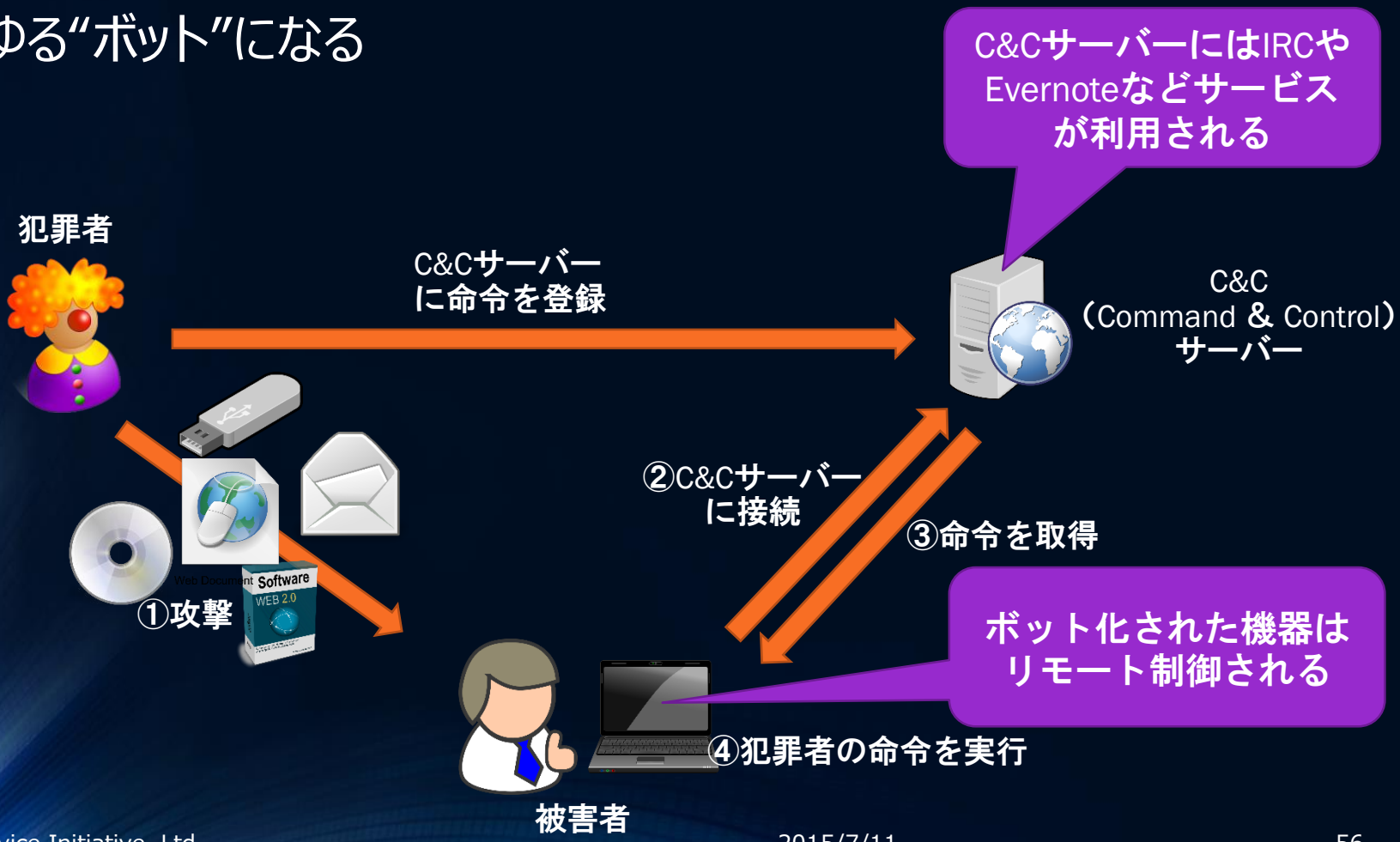
- APT – Advanced Persistent Threat
  - 持続的標的型攻撃、ターゲット型攻撃などとも呼ばれる

- 長期間に渡り持続的に情報窃取などを行う
  - APTでなくても潜伏して攻撃時期を待つ（オンラインバンキング攻撃、スパムメール送信など）

- ルーターや機器のファームウェアなどが攻撃されると長期間攻撃に気が付かないことが多い

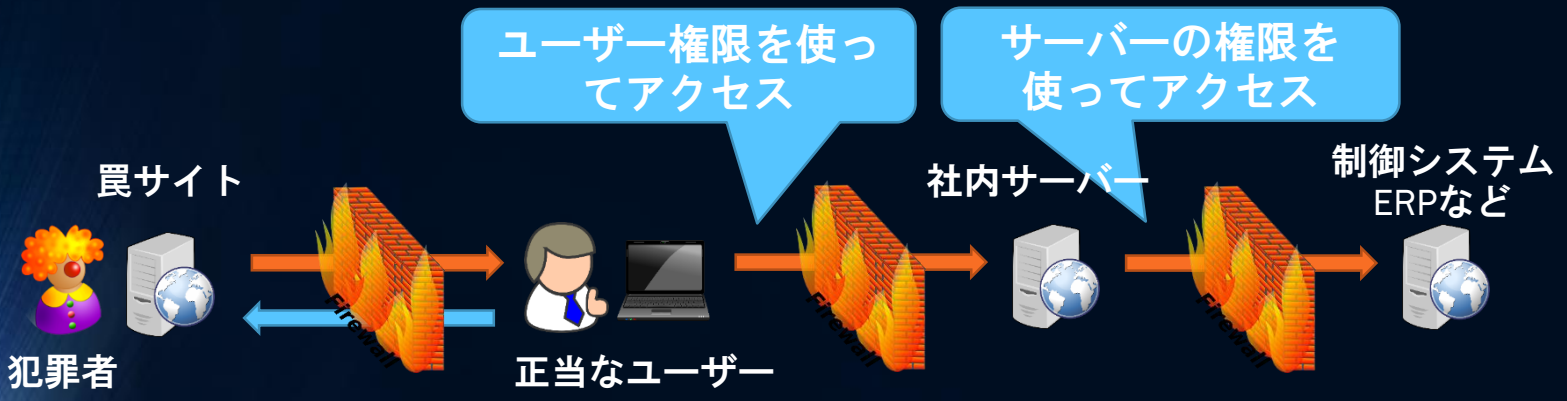
攻撃者が攻撃に成功すると

- 多くの場合、そのデバイスはリモートコントロールされる
- いわゆる“ボット”になる



実は、怖いリクエストフォージェリ

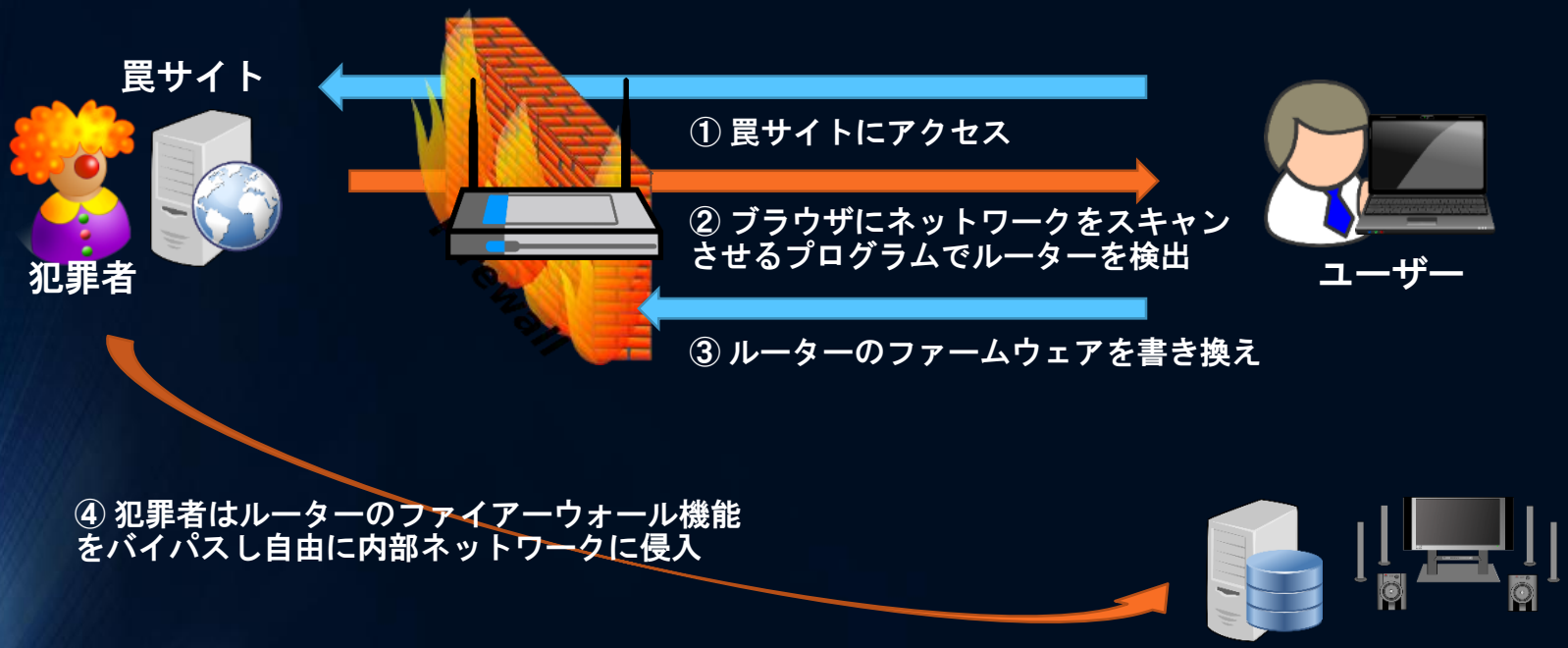
- リクエストフォージェリ攻撃 – リクエストの詐称攻撃
  - リクエストの真正性チェックの問題を攻撃する手法
  - ファイアーウォールが複数あっても攻撃、企業システムの奥深くまで攻撃



原因：社内システムからのアクセスを十分条件・正当なリクエスト/接続だと処理する仕様

Webサイトにアクセスするだけで ルーターが乗っ取られる仕組み

- 最近のブラウザの高機能化 – HTML5



対策：ルーターのファームウェアを最新に。サポート切れルーターは廃棄。パスワードは複雑かつ厳重に管理。不用意にルーターにログインしたままにしない。

最近の脅威傾向

- **物理的な脅威が増加**
  - 攻撃用USBを挿すだけで、アンチマルウェアソフトでは検出できない攻撃を実行（BadUSB攻撃:USBファームウェアにマルウェアをインストール）
  - HDDのファームウェアにマルウェア、購入したPCに元々マルウェアがインストール
  - プログラマブルUSBキーボードで高速に処理を実行
  - モバイルデバイス、IoT（脆弱なWebカメラは多数）
  - PCから漏れるノイズで暗号鍵を解析、タイプ音からキー入力を解析

- PCなどの物理的セキュリティ対策の必要性が高まってきている
  - 最低限でもディスクの暗号化、UEFIを利用したセキュアブートは必須と言える

- とは言ってもネットワーク的な保護の優先順位は高い
  - 持ち歩くPCなどを優先的に物理的なセキュリティ対策を行う

インフラ系のセキュリティ対策状況

- 攻撃を未然に防ぐ「境界防御」は当たり前
  - ネットワークファイアーウォール、プロキシサーバー、メールチェックゲートウェイ
- 「境界防御」で防げないPCなどの末端は「エンドポイント」セキュリティ対策で対応が当たり前
  - 各PCにファイアーウォール、ウイルスチェック、セキュリティチェックエージェント、PCの仮想化など
  - VLANなどを用いネットワークを分離（IEEE 802.1X認証も）
  - エンドポイントセキュリティは「縦深防御」（多層防御）
- 境界防御、縦深・多層防御で守れないケースへの対応
  - ネットワーク内部の機器だから、と信用しない！
  - システムのログを分析して「攻撃の兆候」を検出
  - ネットワーク上のデバイスのステスル化

開発者のセキュリティ知識の状況

- IT知識は不十分
  - 「セキュリティ対策」の“定義”すら浸透していない
  - “プログラミングの原則“さえ浸透していない
  - “セキュア開発プロセス”も実践されていない
  - “場当たり的な対策“が行われている
  - “基礎的・基本的なセキュリティ教育”が必要だが行われていない
    - 中には過去の手法にしがみつき、危険な思想での開発を強固に主張する開発者も

- 開発現場の多くが“皆さんのITシステム環境”と同じ程度のセキュリティレベルで開発されていると考えるべき

法規制

プライバシーマーク

- プライバシーマークとは個人情報保護を目的として認証制度
- 個人情報保護法（2005年4月）に対応
  - 5000以上の個人情報を保管する組織が対象
  - 対象組織は個人情報保護法を順守しなければならない
- ISMS同様、JIS規格化（JIS Q 15001:2006）
- 個人情報保護を目的としたシステムの管理も範囲内
- ISMSはITシステム管理全般が対象

- プライバシーマークはITシステム全体のセキュリティ対策として十分効果的とは言い難い
- ISMSより導入と認証取得が容易、一定レベルのセキュリティを実現している指標としては有用

マイナンバー

- 行政手続における特定の個人を識別するための番号の利用等に関する法律（マイナンバー法）
- マイナンバー制度で一般事業者も業務によってはマイナンバーを取り扱う必要がある
  - 税務、社会保障など
- **マイナンバーは目的外利用・収集が一切禁止**されている
  - 例：社員番号として利用、Webサイトユーザーや取引先社員のマイナンバーを不必要に請求
- 個人情報保護法の適用対象は規模で決まるが、**マイナンバー法はすべての事業者が対象**

その他

- 日本版SOX法　-　改正商法、会社法
  - 公開企業、金融機関への法規制
- 著作権法
- 特許法

- **法規制がある場合、無条件に順守**しなければならない
- **契約も法的に保護**される。契約条件も順守しなければならない
  - 情報の取り扱い、ITシステムの管理・利用方法、要員への教育など

まず脅威の概要を知る

セキュリティベンダーの情報

- **少なくとも毎年脅威の動向を把握**
  - セキュリティベンダーは毎年、半年、毎月レポートを作成
  - 取るべき対策の解説も含まれている場合が多い

- **組織として体系的・総合的に脅威に対応**
  - 攻撃者は一番弱い部分、攻撃しやすい部分を狙いやすい
  - 高度な攻撃も一般化、弱い部分の補強だけでは脆弱
  - 異常を検出する仕組みの導入が必要
  - 脅威に対応する総合的な対策が必要

参考URL

- http://know.symantec.com/LP=1624
- http://www.trendmicro.co.jp/jp/security-intelligence/sr/sr-2014annual/index.html
- https://www.sophos.com/ja-jp/lp/sevendeadlysins.aspx?cmp=701j0000000ZaL5AAK

脆弱性データベース

- ソフトウェア脆弱性は世界規模で統一された共通脆弱性識別子（CVE）で管理
  - ほぼ全ての大手ベンダーはCVEに対応している
  - セキュリティベンダーは製品ごとの脆弱性データベース、アラートサービスなどを提供

- CVEを管理する米MITRE社は共通脆弱性リスト（CWE）、共通攻撃パターンリストと分類（CAPEC）も提供
  - CWE：脆弱性の原因となるソフトウェア仕様と対策
  - CAPEC：攻撃者がソフトウェアを攻撃する手法と対策

セキュリティ標準・ガイドライン

- セキュリティ標準やガイドラインには対応すべきリスクが記載されている

- ISO/JIS規格
  - ISO 27000（JIS Q 27000）シリーズ：情報セキュリティに対する脅威と対策を体系的に規格化
    - ISMS（Information Security Management System)認証の基盤
  - ISO 31000（JIS Q 31000）シリーズ：リスク管理の手法を体系的に規格化

- CMMI（能力成熟度モデル統合）
  - 米カーネギーメロン大学で構築されたセキュアな組織・ソフトウェア開発を実現する方法論

「セキュリティ対策の目的化」に注意！

- 「セキュリティ対策」と呼ばれているモノの導入は目的ではない
- 「セキュリティ対策」の導入は手段に過ぎない

ITセキュリティ対策の目的は
許容範囲内のリスク
でITシステムを利用できるようにする事

「セキュリティ対策の目的化」に注意！

- 「セキュリティ対策」と呼ばれているモノの導入は目的ではない
- 「セキュリティ対策」の導入は手段に過ぎない

ITセキュリティ対策の目的は
許容範囲内のリスク
でITシステムを利用できるようにする事

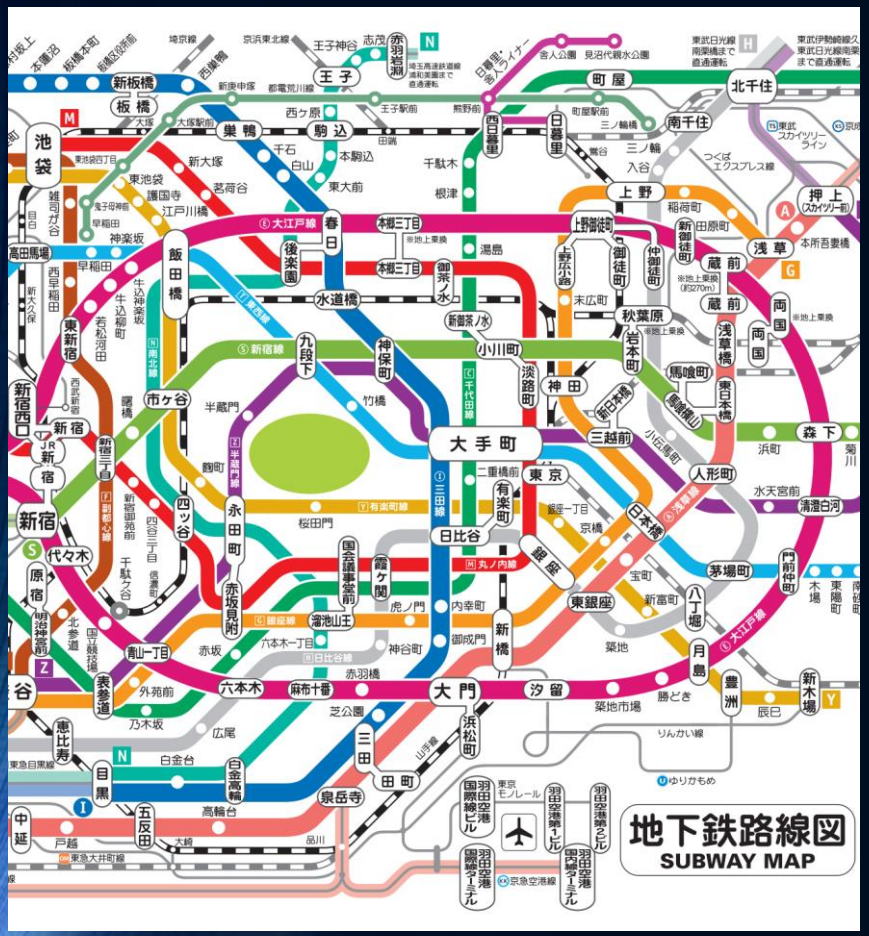
「今、しのぐために何かを足し算（による対症療法的対応）することが悪いとは限りません。しかし、現在ではITの運用の問題とセキュリティを同じ文脈でやっていかないと、難しくなってきているというのが実感です」

マイクロソフト チーフセキュリティアドバイザー 高橋氏

第二部
体系的なITセキュリティ

基本概念と国際セキュリティ標準
ITセキュリティの本質は「マネジメント」

体系的ITセキュリティ
～ 目的別の地図のような物 ～



同じ“地図”でも“目的”に合わせた地図の方が情報量が少なく
目的を達成するために効果的かつコストが少ない

体系的なセキュリティ対策の必要性

- 場当たり的・対処療法的対策の問題
  - ITシステムには多種・多様なリスクが存在する
  - リスクを識別するたびに個別に対策ではキリがない
  - リスクと対策の範囲が広く、それぞれの分野で多数の対策
  - 漏れがあると無視できないリスクが放置される
  - 全体としてのリスク評価が行えない
  - 不必要なITセキュリティ投資が行われやすい
  - リスクと対策の対象・内容が時間と共に変化する
  - 体系的にセキュリティを学ぶ機会がない
  - 概念や用語の定義が異なりコミュニケーションができない
  - 場当たり的対策には「マネジメント」がない

- 体系的セキュリティ対策が必要

体系的なITセキュリティ
～ ITシステム要件のサブセット ～

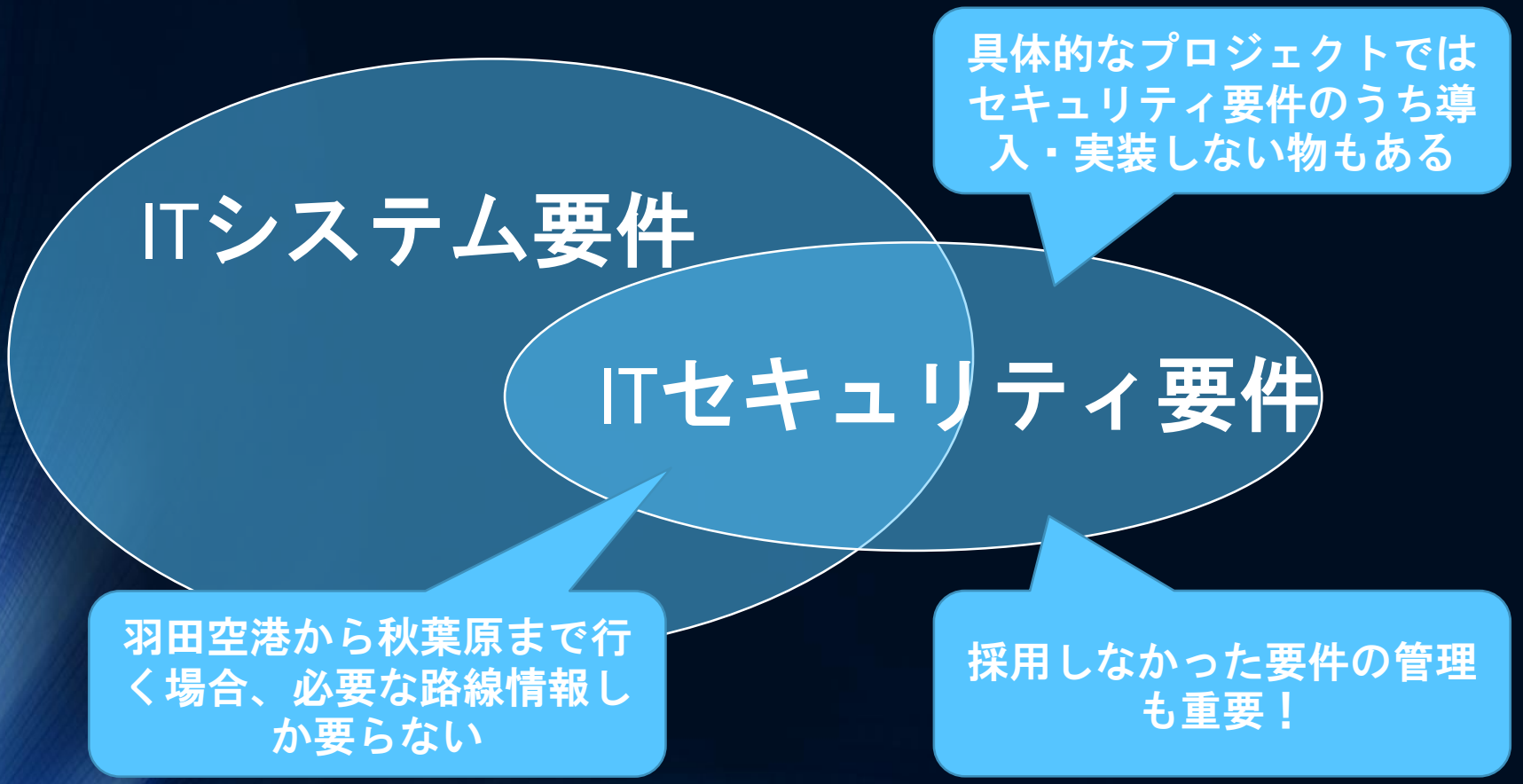
- 基本的・一般論としては“ITシステム要件 ⊃ ITセキュリティ要件”

ITシステム要件

ITセキュリティ要件

体系的なITセキュリティ
～ ITシステム要件のサブセット ～

- 個別の案件では“ITシステム要件 ⊃ ITセキュリティ要件”とならない



よくある失敗

- ISMSを導入してみたが「チェックリストを埋める」だけ
  - ISMSは能動的に行う
  - 形式的な対応では文書作成とチェックリストの消化に終わる
  - 現状の問題点、新たな脅威、新しい技術の調査と評価を行う
  - 要求事項に対して能力成熟度モデル的な評価と改善を行う

- 「ISMSの導入」がセキュリティ向上の解決策ではない
- **継続的＆能動的なKAIZENに成功のポイント**がある
- 組織の文化となるか？が鍵

ITシステム導入

基本は常に重要です。ITセキュリティの前に、
なぜITシステムを利用するのか？を再認識します。

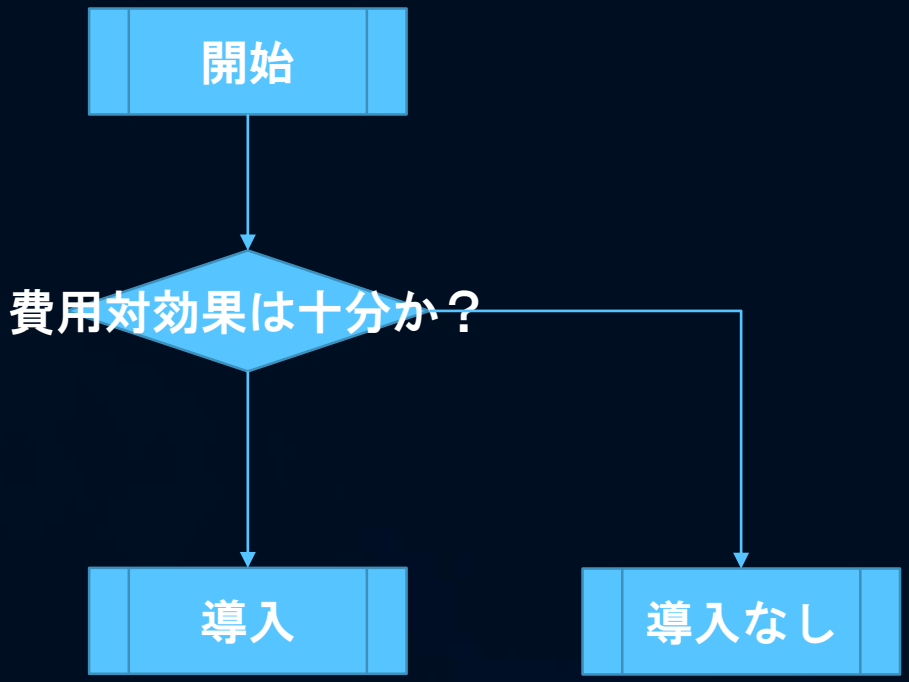
ITシステム導入の目的

- 新たな価値を生み出す
  - 効率化　－　生産性の向上
  - コスト削減　－　価値を生み出す為に必要な費用・時間削減
  - サービス提供　－　システム自体で新たな価値を生み出す

- よくある間違い
  - ITシステムの導入自体が目的化
    - 十分な価値を生み出さないITシステムに存在意義はない
    - “費用”（コスト）、“効果”（価値）を無視したITシステム導入による失敗は多い
    - 「新たな価値」とは何か？これを定義し達成するのがITシステム導入の目的
    - “費用対効果“はセキュリティ対策とも切っても切れない関係

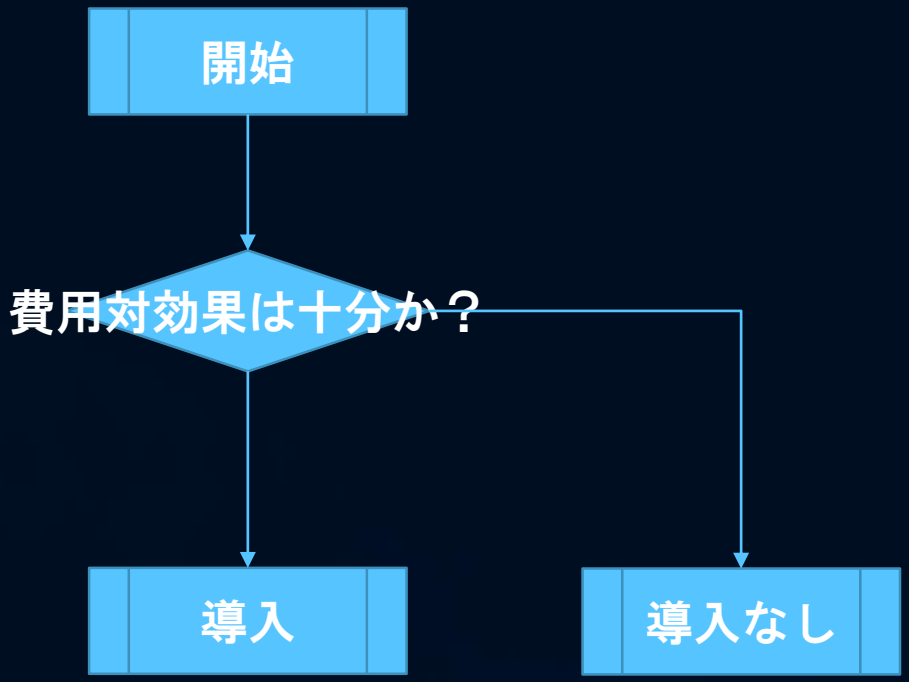
ITシステム導入の意思決定プロセス

- 意思決定プロセスは単純



ITセキュリティ対策の意思決定プロセス

- 意思決定プロセスは単純



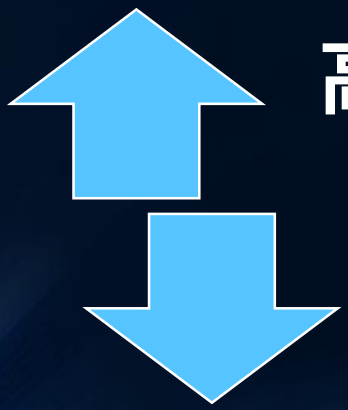
ITシステム・セキュリティ対策を導入するかしないか？

- キーワードは“費用対効果”
  - ITセキュリティ対策が導入されない原因の一つは“費用対効果”が見えないこと
- “ ITセキュリティ対策を導入しない費用”
  ＝“問題が発生するまで顕在化（発生）しない費用”
  つまり「見えないコスト」が発生
- “問題が発生した時に発生する費用”
  - 信用毀損、システム停止による事業・サービス停止による損失、情報漏えい・改ざん・破壊に対する対応、他者に与えた直接的損害の補償・賠償など
  - 法令による規制や契約に違反した場合、法的罰則も
  - 事業の継続さえ困難になる場合も

セキュリティ対策はトレードオフ

- 一般にセキュリティ対策はトレードオフ関係にある
  - セキュリティ対策の追加には何らかのコストが必要な場合がほとんど
  - 研修費用、ソフトウェア・機器の導入・設定・運用・管理、システム性能・利便性・開発費、監査・管理
  - セキュリティ対策を導入しない場合「見えないコスト」（リスク）が発生

セキュリティ対策導入のメリットとデメリット

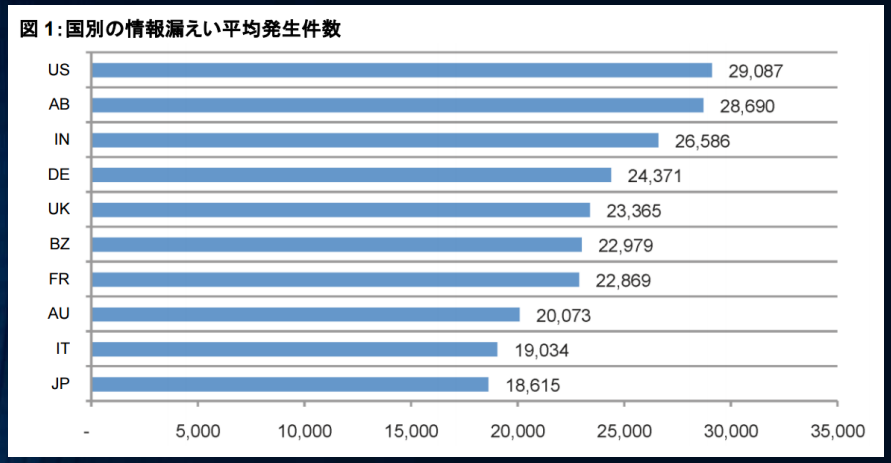


高セキュリティ

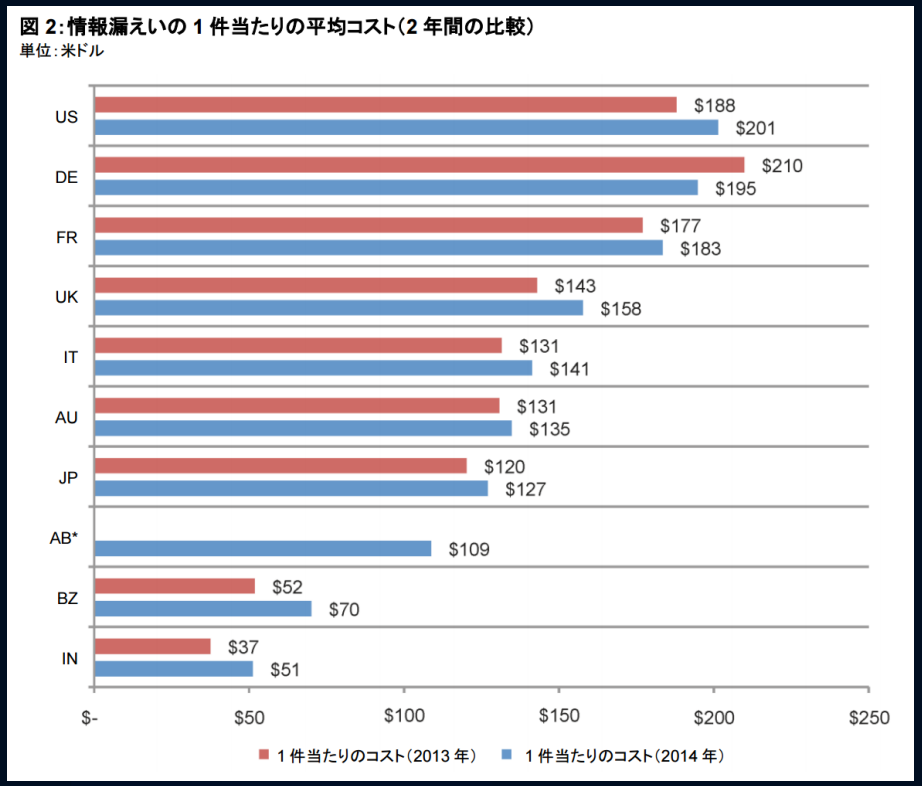
高コスト

直接的なコストが見えないコストを超えない場合は対策を導入

情報漏えいの平均コスト



2014年に公表されている情報漏えい事件
国内26件の漏えい件数とコスト（IBM発表）

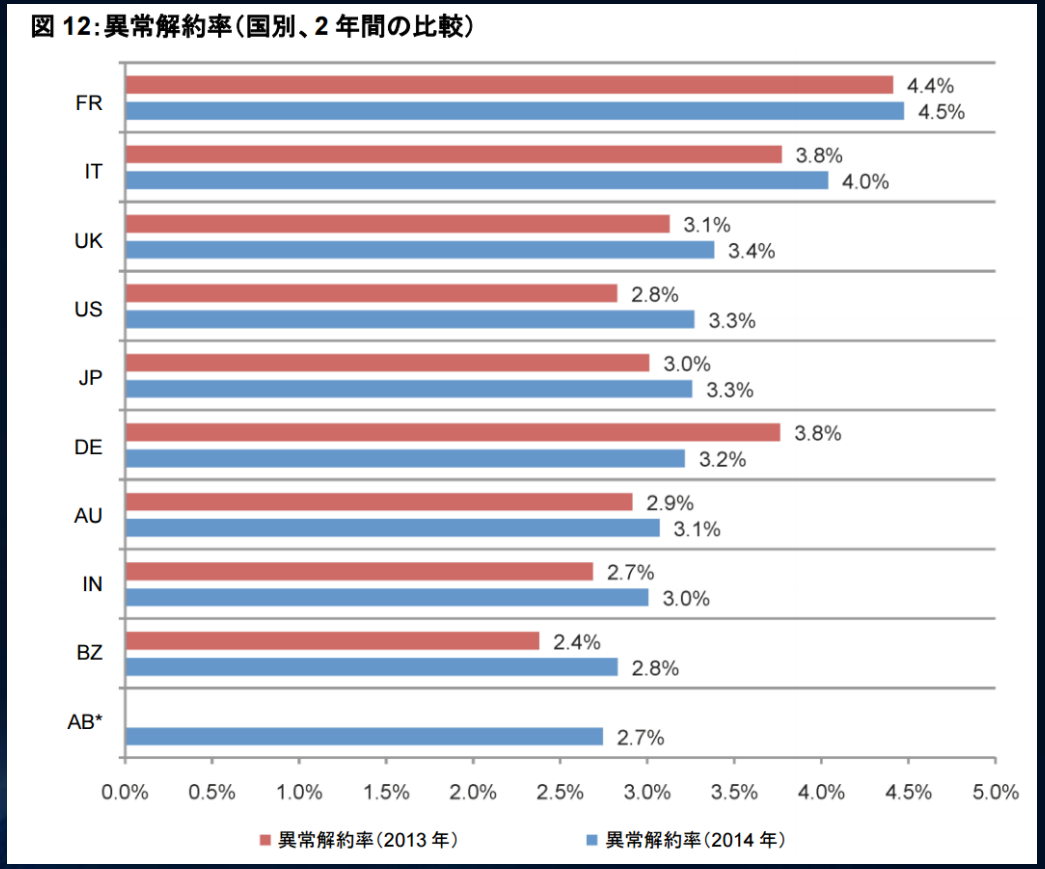


項目	数値
平均漏えい件数	18,615件
1件当たりの平均コスト	127ドル 約15000円
平均漏えいコスト	約2億7600万円

出典：2014 年情報漏えいのコストに関する調査： グローバルな分析

情報漏えいの平均コスト

医療、金融などで影響が大きいが全産業で異常解約が見られる



出典：2014 年情報漏えいのコストに関する調査： グローバルな分析

ITシステム導入時に「見えないコスト」も考慮

- ITシステムに限らず、導入時に「見えないコスト」が十分考慮されないケースは多い

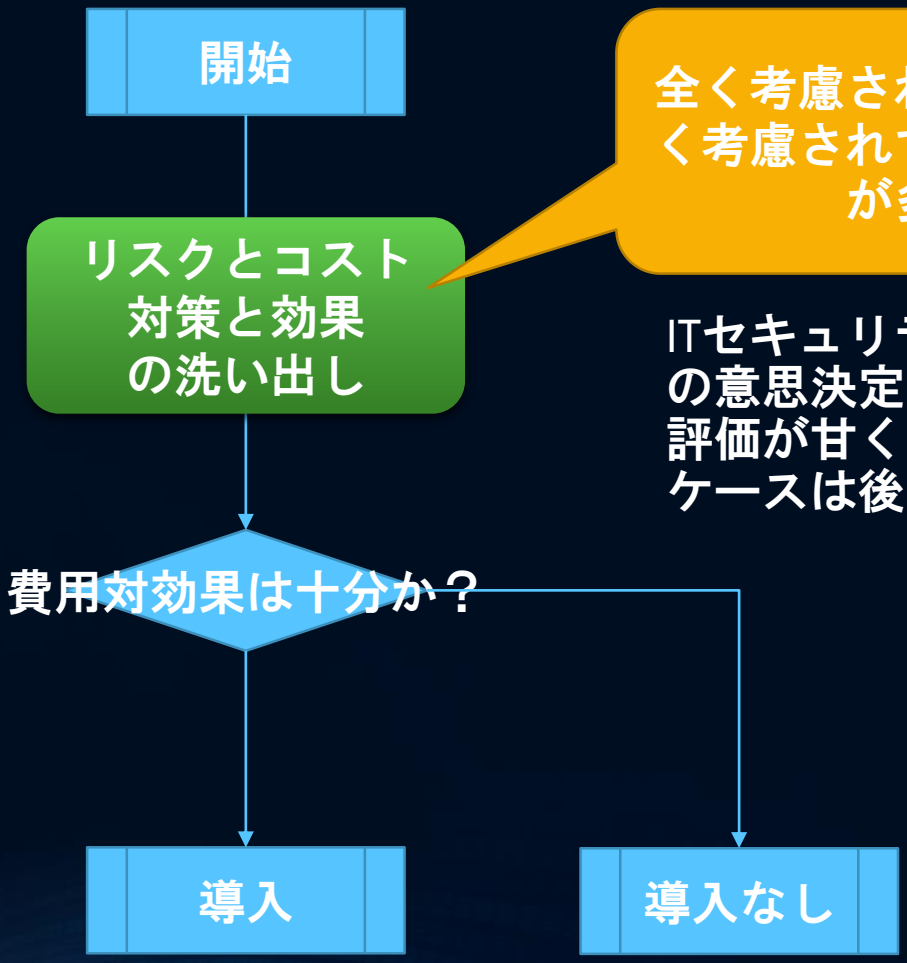
- 何かを導入・利用する場合、必ず「見えないコスト」「見えていないコスト」も考慮する
  - 自動車の運転には事故のリスク　→ 事故のリスクを保険により委譲
  - ITシステム導入には情報セキュリティのリスク → 情報セキュリティ対策を導入

リスク分析と評価

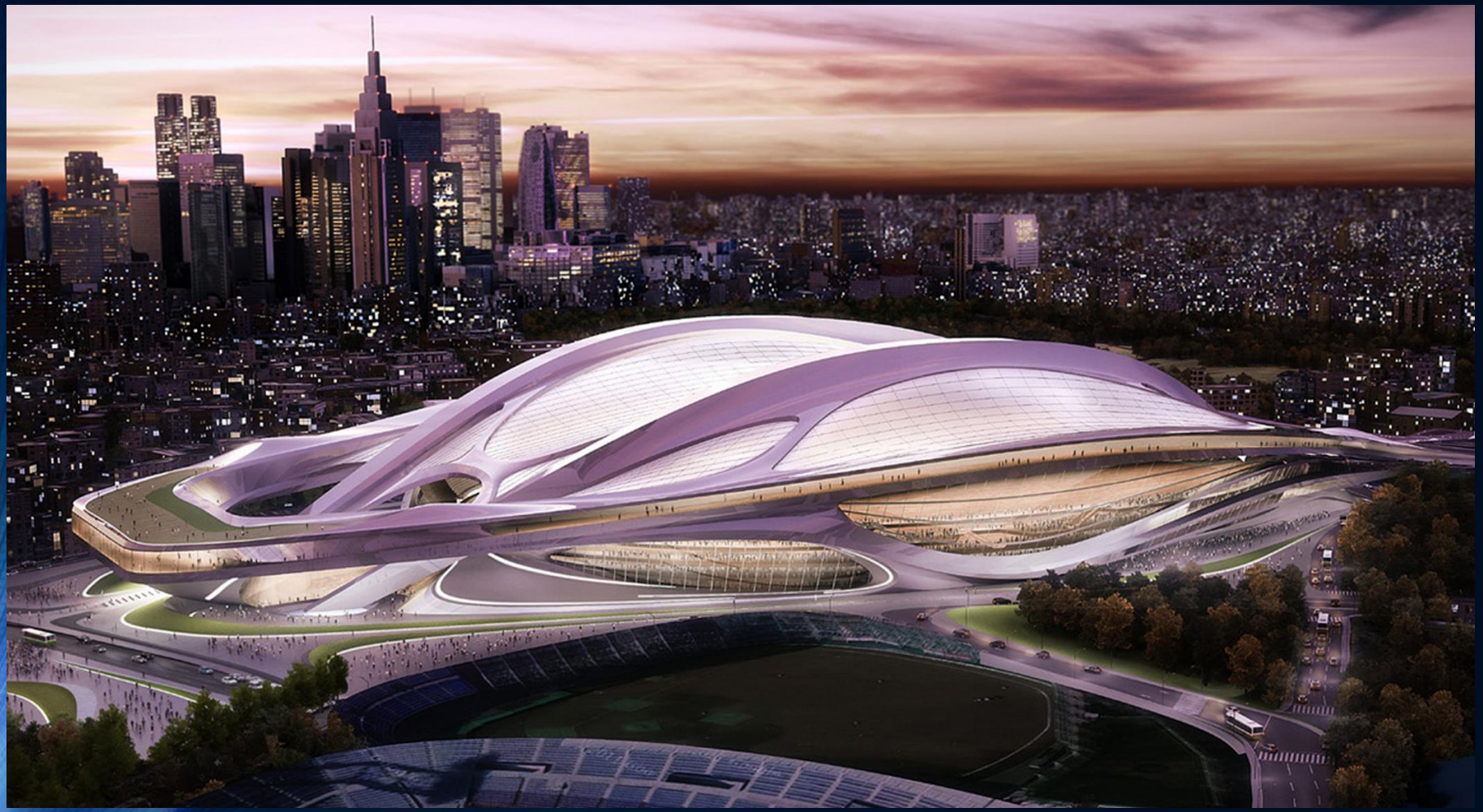
「見えないコスト」の可視化

ITセキュリティ対策の意思決定プロセス

- 意思決定プロセスは単純？



最近の代表例



http://www.jpnsport.go.jp/newstadium/Portals/0/NNSJ/winners.html

意思決定にはリスクアセスメントが必要

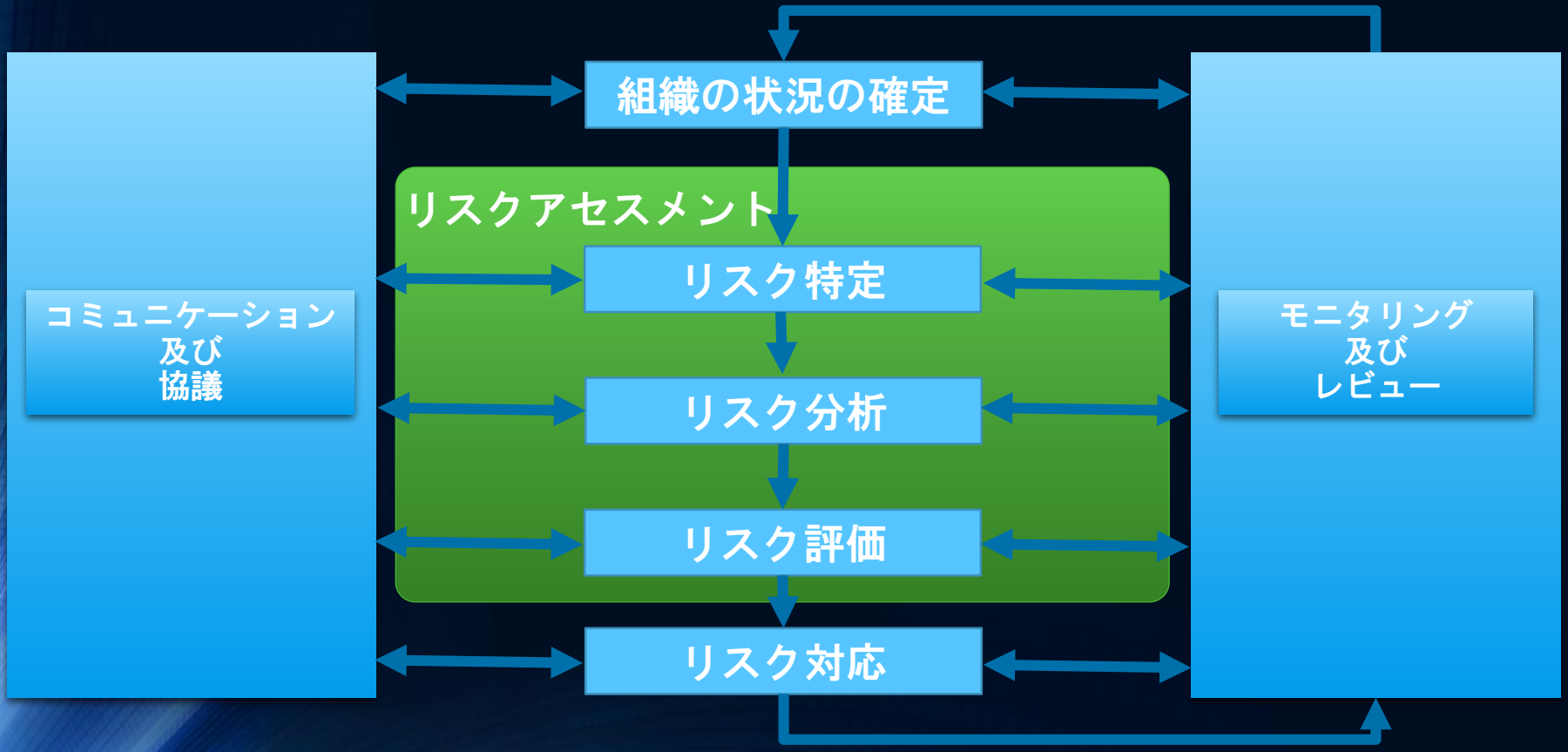
- コストはわかりやすく、ほぼ固定の場合も多い
- 効果はかなり見通せる場合も多い
- リスクは“認識”していないと見落とされることが多い
  - 認識していても低く見積もられる場合が多い

- 正しいリスク評価 → 正しい意思決定
- 誤ったリスク評価 → 誤った意思決定

- 意思決定ミスのコストは“問題が発生するまで表面化しない”

リスクの特定・分析・評価

- リスクを正しく評価・分析することは難しい
  - ISO/JISではリスクマネジメント専用の規格（31000シリーズ）も定義



ISO 31000のリスク分析手法

- JIS Q 31010:2012（IEC/ISO 31010:2009）

ブレインストーミング	構造化又は半構造化インタビュー	デルファイ法
チェックリスト	予備的ハザード分析（PHA）	HAZOPスタディーズ
ハザード分析及び必須管理点（HACCP）	環境リスクアセスメント	構造化“Whatif”技法（SWIFT）
シナリオ分析、事業影響度分析（BIA）	根本原因分析（RCA）	故障モード・影響解析（FMEA）
故障の木解析（FTA）	事象の木解析（ETA）	原因・結果分析
原因影響分析	保護層解析（LOPA）	決定木解析
人間信頼性分析（HRA）	蝶ネクタイ分析	信頼性重視保全（RCM）
スニーク回路分析（SCA）	マルコフ分析	モンテカルロシミュレーション
ベイズ統計及びベイズネット	FN曲線	多基準意思決定分析（MCDA）
リスク指標	リスクマトリックス	費用/便益分析（CBA）

附属書A（参考）リスクアセスメント技法の比較

ISO 31000のリスク分析手法

- JIS Q 31010:2012（IEC/ISO 31010:2009）

ブレインストーミング	構造化又は半構造化インタビュー	デルファイ法
チェックリスト		スタディーズ
ハザード分析及び必（HACCP）		matif” 技法
シナリオ分析、事業（BIA）		影響解析
故障の木解析（FTA）		原因－結果分析
原因影響分析	保護層解析（LOPA）	決定木解析
人間信頼性分析（HRA）	蝶ネクタイ分析	信頼性重視保全（RCM）
スニーク回路分析（SCA）	マルコフ分	ョン
ベイズ統計及びベイズネット	FN曲線	）
リスク指標	リスクマトリックス	費用/便益分析（CBA）

こんなにあるの？！無理！
ではなく
規格を利用するとまとめられ
ているので便利！

規格書には各手法の比較・解説も記載されている。最適な手法を比較的容易に選択可能

附属書A（参考）リスクアセスメント技法の比較

単純なマトリックス法も有用

組織の資産状況を調査するための調査票例

情報資産調査票	
情報資産	
用途	
管理者	
利用者（アクセス権限）	
保存（設置）場所	
保存（設置）期間	
重要性	A・B・C・D **機密性**［A・B・C・D］ **完全性**［A・B・C・D］ **可用性**［A・B・C・D］

情報セキュリティポリシーに関するガイドライン

重要性と発生頻度の分類例

重要性
A：セキュリティ侵害が、全社的に事業へ重大な影響を及ぼす。
B：セキュリティ侵害が、事業の一部に重大な影響を及ぼす。
C：セキュリティ侵害が、事業に軽微な影響を及ぼす。
D：影響をほとんど及ぼさない。

発生頻度
a：かなりの頻度で発生する。
b：時々発生する。
c：偶発的に発生する。
d：ほとんど発生しない。

重要性と発生頻度を分類し、マトリックス法で評価する簡単な方法でも、比較的十分なリスク分析となり、適格な優先順位を設定する助けとなる。

重要性と発生頻度分類のマトリックス

リスク大

重要性

発生頻度	A	B	C	D
a	ウイルスメール	ネットワーク障害		ポートスキャン
b	故障	DoS攻撃		
c	停電	操作ミス	誤送信	
d	内部犯行、地震、火災			

リスク小

これは例であり、事業内容・現状の管理策などにより
重要性・発生頻度は変化する

意思決定には
リスクと対策の効果の評価が必要

- 対策には特定の効果が期待できるが評価が難しいことも
  - 「効果」が発揮されることがまれ（問題の発生が稀。しかし被害は？）
  - 「効果」が発揮されても損害が軽微（被害が軽微。しかし発生頻度は？）
  - 「効果」が発揮される状況の予見が困難（被害額も発生頻度も予測不可）
  - 評価は客観的に行われるべきだが、主観を排除できない

- リスクと対策、効果の評価にもマネジメントが欠かせない
  - 組織現状の把握
  - リスクアセスメント（特定・分析・評価）
  - 対策の選択・実施
  - モニタリングとレビュー

リスクと対策の評価は難しい

- 瞬時電圧低下が起こす事業中断リスク
  - 2010年12月8日 午後5時20分頃、瞬間的に電圧が低下した影響で東芝四日市工場（NAND型フラッシュメモリー工場）のクリーンルーム空調が停止。その結果、数百億円の損失。
  - ある発電会社の火力発電所では年間の電圧低下件数は平均340件としている。ほとんどが落雷などの自然要因で影響は局所的としている。

- 中部電力の送電システムの品質が非常に高いのか、地域的に落雷の影響を受けなかったのか不明だが、瞬時電圧低下の影響をこれまで受けたことがなかった。
  - 東芝以外の工場も影響を受けた。同じ半導体工場であったパナソニック工場の影響は不明。

出典： http://www.sjnk-rm.co.jp/publications/pdf/101229_report.pdf

リスクと対策の評価は難しい

- 瞬時電圧低下が起こす事業中断リスク
  - 2010年12月8日 午後5時20分頃、瞬間的に電圧が低下した影響で東芝四日市工場（NAND型フラッシュメモリー工場）のクリーンルーム空調が停止。その結果、数百億円の損失。
  - ある発電[redacted]40件としている。ほとんどが[redacted]

このようなリスクとその対応を現場で評価して対策することは可能か？

- 中部電力[redacted]域的に落雷の影響を受けなかったのか不明だが、瞬時電圧低下の影響を今まで受けたことがなかった。
  - 東芝以外の工場も影響を受けた。同じ半導体工場であったパナソニック工場の影響は不明。

出典： http://www.sjnk-rm.co.jp/publications/pdf/101229_report.pdf

ITセキュリティ対策には経営的判断が必要

- リスクの見積もり・定量化は可能だが、正確な見積もり・定量化が難しい場合も多い
- コストが大きいセキュリティ対策導入は、得られるメリットとコストを天秤にかけるのは経営判断
- 決裁権をもつ経営者・マネージャーが正しい判断を行うには「ITセキュリティ対策」の基礎・専門知識が不可欠
  - CIOやCSOが必要不可欠、と言われてるのはこれが一つの理由
  - 組織として対応しなければ網羅的な対応は不可能
- 決裁権を持たない従業員にも「ITセキュリティ対策」の基礎・専門知識が不可欠
  - 十分なセキュリティはトップダウンだけでは不可能
  - ボトムアップがなければ漏れが発生、ボトムアップ型の対策が必須

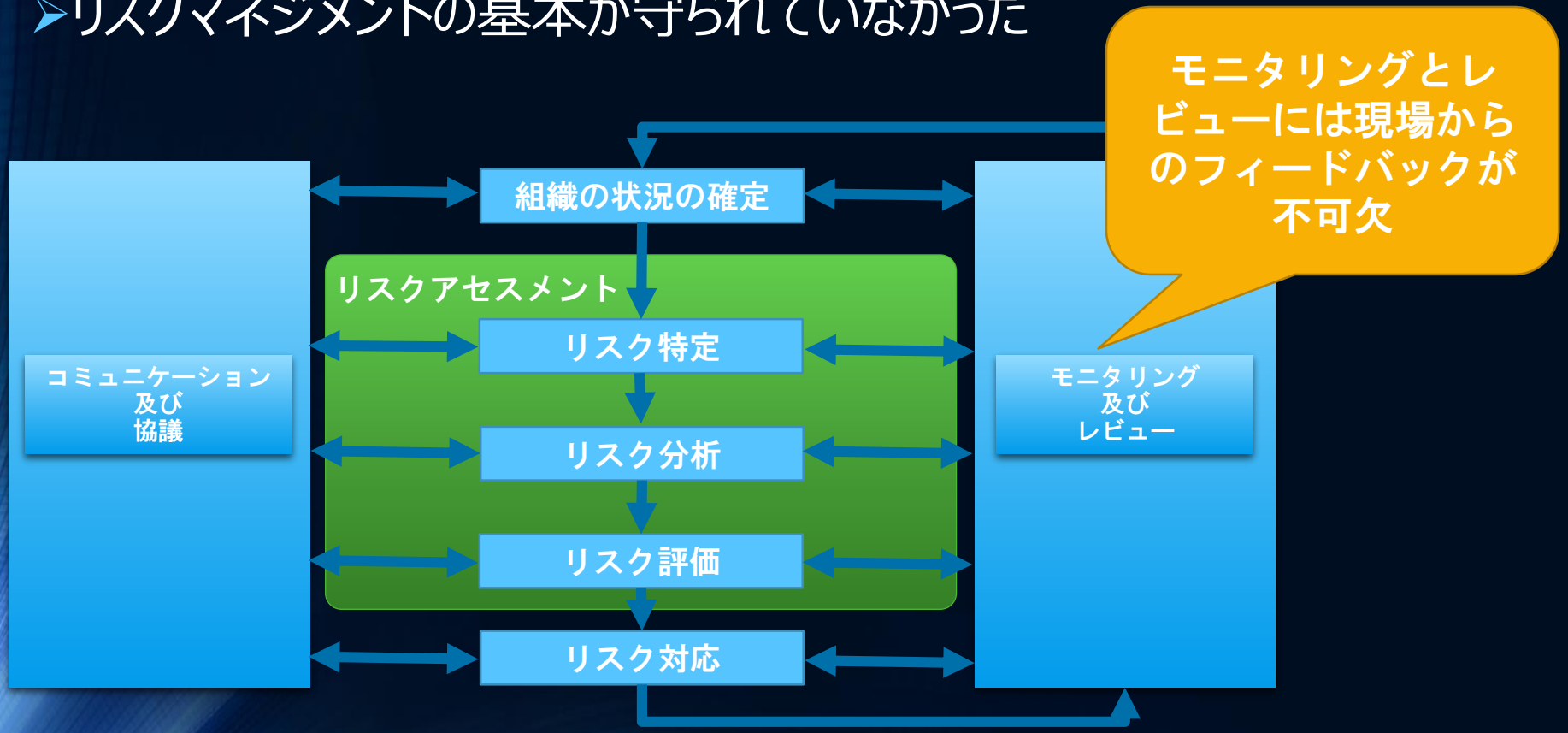
リスク評価、対策評価にマネジメントが必須

- セキュリティ対策としてまず必要なことに
  - 「セキュリティポリシー」の策定
  - 安全維持管理のための組織づくり
  - リスク評価＆対策の導入
  - PDCAサイクルマネジメント

- トップダウン型セキュリティ対策は必須
  - トップダウン型マネジメントなしでは十分なセキュリティレベルの達成は不可能
  - セキュリティ対策には予算措置・プロジェクト管理が必須
  - ボトムアップ型のサポートも忘れずに！

福島第一号原発のリスクを現場は把握していた

- 原発は典型的なトップダウンオンリーのマネジメントシステム
- リスクマネジメントの基本が守られていなかった



体系的セキュリティ対策

JIS Q 27000・ISO/IEC 27000シリーズのセキュリティ

体系的ITセキュリティ対策の指針

- 国際情報セキュリティ標準（ISO 27000 / ISMS）
- 能力成熟度モデル統合（CMMI）

- どちらも認証制度あり。
  - ISMS（Information Security Management System）認証の基盤はISO 27000
  - 国内のISMS認証取得組織は4646組織（2015年6月29日）

体系的ITセキュリティ対策の導入は大変？

- 場当たり的対策は「マネジメント」「リーダーシップ」がない状態
  - 「マネジメント・リーダーシップ不在」の会社で事業は成功するか？
  - 「マネジメント・リーダーシップ不在」のセキュリティで十分な安全性は確保できるか？

- 担当者任せ、部署任せ、ベンダー任せで十分なセキュリティの確保は困難
  - よくある現場の声「うちのマネージャーはセキュリティを解ってないから対策できない」
- セキュリティ対策を行わないことによる見えないコスト（リスク）の識別がないことは事業に対する脅威
  - 場合によっては事業の継続さえ困難に
- 十分な安全性確保のコストを最小限に留めるには「マネジメント」が必須

体系的ITセキュリティ対策の導入は大変？

- 体系的セキュリティ対策の導入は確かに大変
  - リスクの範囲が広い
  - 対策の選択肢が広い
  - 一度にすべて導入は人的・金銭的なコストにより困難
  - そもそも体系を作るコストが高い

- 既存のセキュリティ標準や方法論を使えば体系を作るコストはゼロ！

- ISO 27000以外のオプション
  - CMMI（能力成熟度モデル統合）、SAMM（ソフトウェアセキュリティ保障成熟度モデル）
  - 段階的にプロジェクトマネジメントを実施するメソドロジー
  - 開発組織以外にも成熟度モデルの考え方は有効

ISO 27000 : ITシステムを利用する全ての組織向けITセキュリティ標準

- ISO 27000は元々英国セキュリティ標準のBS7799として策定、ISO化された
  - BS7799 → ISO17799 → ISO 27001/27002
  - ISO 27000シリーズは現在も改訂・拡張中
  - ISO 27000シリーズはISMS（Information System Management System）
- JIS標準化済み JIS Q 27001:2014（ISO/IEC 27001:2013）
  - ISMS認証制度も作られている
  - 日本ではJIPDEC（一般財団法人日本情報経済社会推進協会）が認証機関を認定、認証機関が適合性検査を行う
  - 高いセキュリティが必要な組織に採用され、国内4646組織が登録（2015年6月29日）

ISO 27000シリーズの注意点！

- ISO　27000シリーズは改訂が行われている（重要！）
- 例えば、ISO/IEC　27001:2013は以前のバージョン（ISO/IEC 27001:2005）とは**管理項目などが大幅に改訂**されている
  - どのバージョンを参照しているか明確にしないと混乱の原因
- この講義では以下のJIS規格を利用している
  - JIS Q 27000:2014（ISO/IEC 27000:2014 JIS規格では対応はしているが別物として取扱い）ISMS 用語
  - JIS Q 27001:2014（ISO/IEC 27001:2013）ISMS 要求事項
  - JIS Q 27002:2014（ISO/IEC 27002:2013）情報セキュリティ管理策の実践のための規範
- ISO標準には追加標準も（以下は一例）
  - ISO/IEC 27003　Information security management system implementation guidance
  - ISO/IEC 27004　Information security management — Measurement
  - ISO/IEC 27005　Information security risk management

ITセキュリティFAQ
～ セキュリティとは何が何だか解らない ～

- 「何がセキュリティ対策で、何がセキュリティ対策でないのか解らない」
- 原因
  - セキュリティ対策の定義が曖昧・非論理的であることが原因
    - 「リスクを低減させる対策がセキュリティ対策」（低減させる物だけではない）
    - 「リスクを低減させる目的の対策がセキュリティ対策」（目的と手段の取り違え）
    - これらは間違いです
- 対策
  - 「セキュリティ対策とはリスクを変化させる対策すべて」と考える
  - 国際ITセキュリティ標準では“リスク対応”（JIS Q 27000：2014 2.79 リスク対応）、“管理策”（JIS Q 27000:2014 2.14 管理策）が一般に“セキュリティ対策”と言われている用語にあたる
- 体系的セキュリティではセキュリティ対策は“費用対効果”で判断・評価

非体系的セキュリティは
非論理的・非科学的に構築されている

- よくあるおかしな主張
  - **ホワイトリストとブラックリストは変わらない**
    - 論理的にも実証的にもホワイトリストの方が遥かに安全
    - 特にブラックリスト思考の入力サニタイズはITシステムにとって非常に有害な場合も
  - **入力妥当性検証（入力バリデーション）はセキュリティにとってどうでもよい**
    - 「セキュリティ対策ではない」と考えている人も少なくない
    - そもそも境界防御はセキュリティ対策の基本概念・原則
    - 論理的に入力バリデーションがセキュリティ（品質）保証において必須であることは明らか
  - **セキュリティ対策の定義が出鱈目**
    - セキュリティ対策を「目的」で定義（主観で決定。非科学的）
    - 論理的なセキュリティでは「効果」でセキュリティ対策を選択（客観的に決定。科学的。リスクを変化させるモノはすべてセキュリティ管理の対象）

セキュリティ標準対応の効果

- コミュニケーションギャップの解消
  - 概念・用語定義の違いによる勘違い防止
  - 組織別に異なる定義ではコミュニケーションが行えない
  - 国内4500社以上がISMS認証を取得し、取得済みITベンダーも多い
- 網羅的な対応
  - 特定の業種を想定していない
  - セキュリティ標準では用語、目標設定、組織作り、リスクの特定・評価と対応、管理項目、プロセスまで定義
  - 独自にこれらを構築するのは高コストかつ円滑なコミュニケーションの妨げ
- セキュリティ標準以外の標準との整合性
  - ISO 27000（情報セキュリティ管理）はISO 9000（品質管理）、ISO 14000（環境管理）、ISO 20000（ITサービス管理）、ISO 31000（リスク管理）など、他のISOマネジメントシステムとの整合性が考慮されている

「セキュリティ対策とは何が何だか解らない」の解消

ITセキュリティの目的

- ITシステムを**“許容可能な範囲内のリスク”で利用**する
- セキュリティ対策には“リスクの許容”、“リスクの移転”（保険など）も含まれる
- セキュリティ対策の導入の**意思決定は“費用対効果”**決まる
  - “費用対効果”で決まらない例：法令と規制、契約、社会倫理

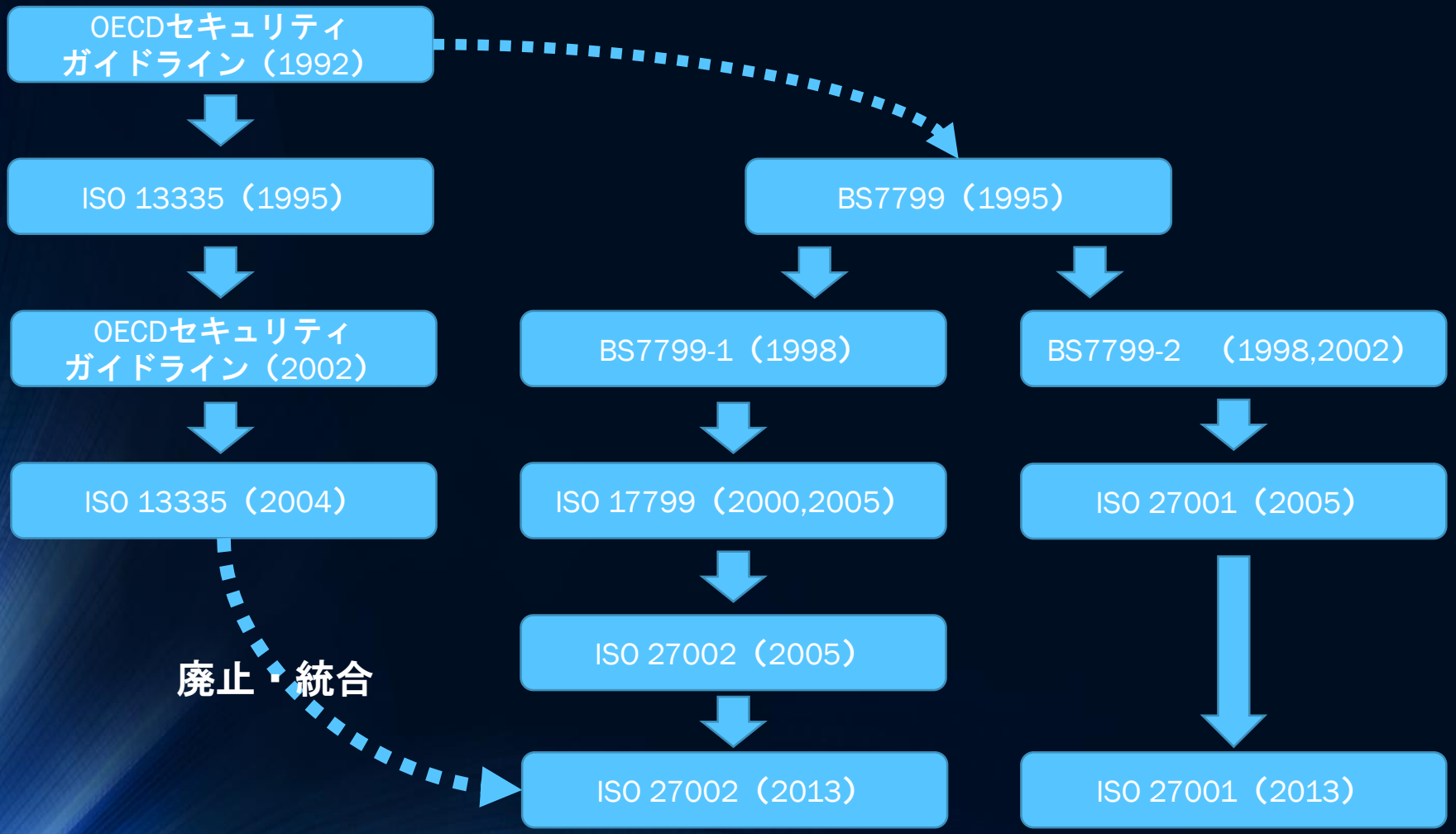
- ITセキュリティ対策の**本質はリスク管理のためのマネジメント**
- 「個々のセキュリティ対策」は目的である適切なリスク管理を達成するための手段に過ぎない

「目的 ≠ 手段」に注意

- ITセキュリティ対策の目的は「価値を生み出すITシステムの利用リスクを許容範囲内に抑える」こと
- **「手段が目的化」するとおかしなセキュリティ対策になる**
  - 「手段」を誤ると「目的」が達成できないため、「手段」が目的化しやすい
  - 生み出す価値よりセキュリティ対策コストが大きくなるなら、ITシステム導入自体を取りやめるべき
  - 「セキュリティ対策が目的化」すると「価値を生み出すITシステムの利用リスクを許容範囲内に抑える」という本来の目的を見落としがち
    - 特にITエンジニアに多い間違いが「目に見える（直接的）リスク削減・排除策のみがセキュリティ対策」
    - リスク対策済みのモノに対して、追加・多層のリスク対策を行わない（基本概念・リスク管理概念の欠如）
- ITセキュリティに限らず「手段と目的の取り違え」は致命的なミスの原因

ISO標準

ISO 27000シリーズ策定の概要



新OECDセキュリティガイドライン9原則

1 **認識の原則** Awareness	参加者は、情報システム及びネットワークのセキュリティの 必要性並びにセキュリティを強化するために自分達にできる ことについて認識すべきである。
2 **責任の原則** Responsibility	すべての参加者は、情報システム及びネットワークのセキュ リティに責任を負う。
3 **対応の原則** Response	参加者は、セキュリティの事件に対する予防、検出及び対応 のために、時宜を得たかつ協力的な方法で行動すべきである。
4 **倫理の原則** Ethics	参加者は、他者の正当な利益を尊重するべきである。
5 **民主主義の原則** Democracy	情報システム及びネットワークのセキュリティは、民主主義 社会の本質的な価値に適合すべきである。
6 **リスクアセスメントの原則** Risk assessment	参加者は、リスクアセスメントを行うべきである。
7 **セキュリティの設計及び実装の原則** Security design and implementation	参加者は、情報システム及びネットワークの本質的な要素として セキュリティを組み込むべきである。
8 **セキュリティマネジメントの原則** Security management	参加者は、セキュリティマネジメントへの包括的アプロー チを採用するべきである。
9 **再評価の原則** Reassessment	参加者は、情報システム及びネットワークのセキュリティの レビュー及び再評価を行い、セキュリティの方針、実践、手 段及び手続に適切な修正をすべきである。

http://www.ipa.go.jp/security/fy14/reports/oecd/handout.pdf

標準セキュリティはこの原則に基づいて構築されている

セキュリティ原則の実現

- 組織において原則実現の責任はマネジメントにある

マネジメント

1 **認識の原則**
Awareness

2 **責任の原則**
Responsibility

3 **対応の原則**
Response

4 **倫理の原則**
Ethics

5 **民主主義の原則**
Democracy

6 **リスクアセスメントの原則**
Risk assessment

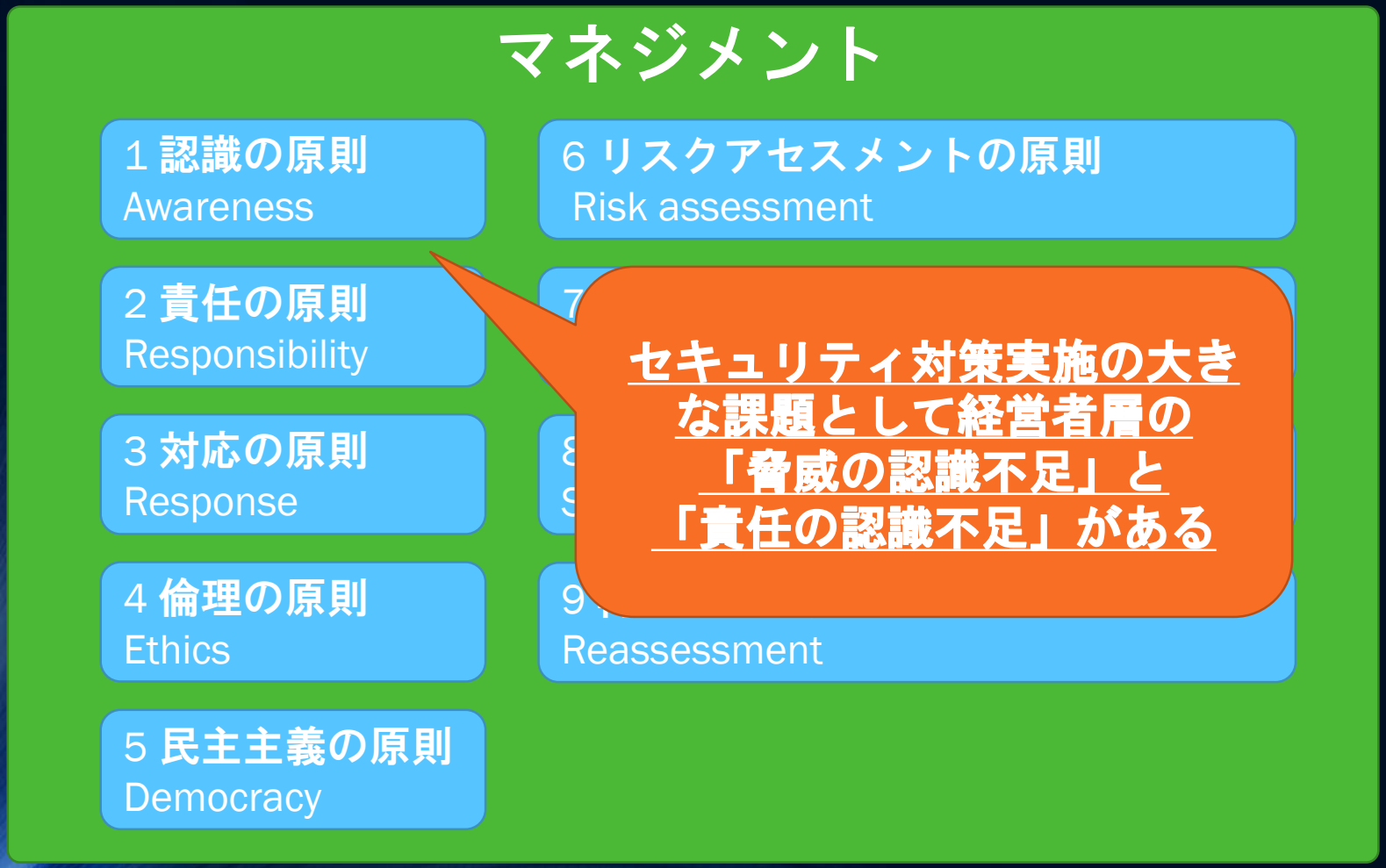
7 **セキュリティの設計及び実装の原則**
Security design and implementation

8 **セキュリティマネジメントの原則**
Security management

9 **再評価の原則**
Reassessment

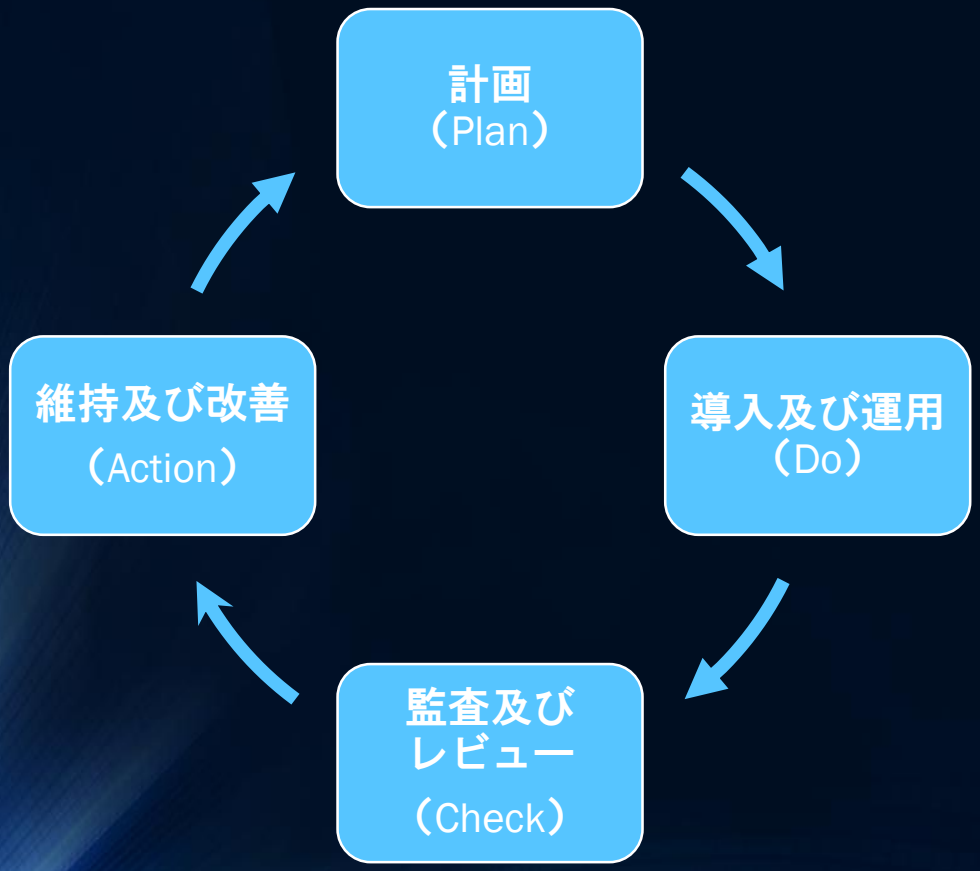
セキュリティ原則の実現

- 組織において原則実現の責任はマネジメントにある



ISOのマネジメントシステム

- ISOマネジメントシステムに共通のPDCA管理

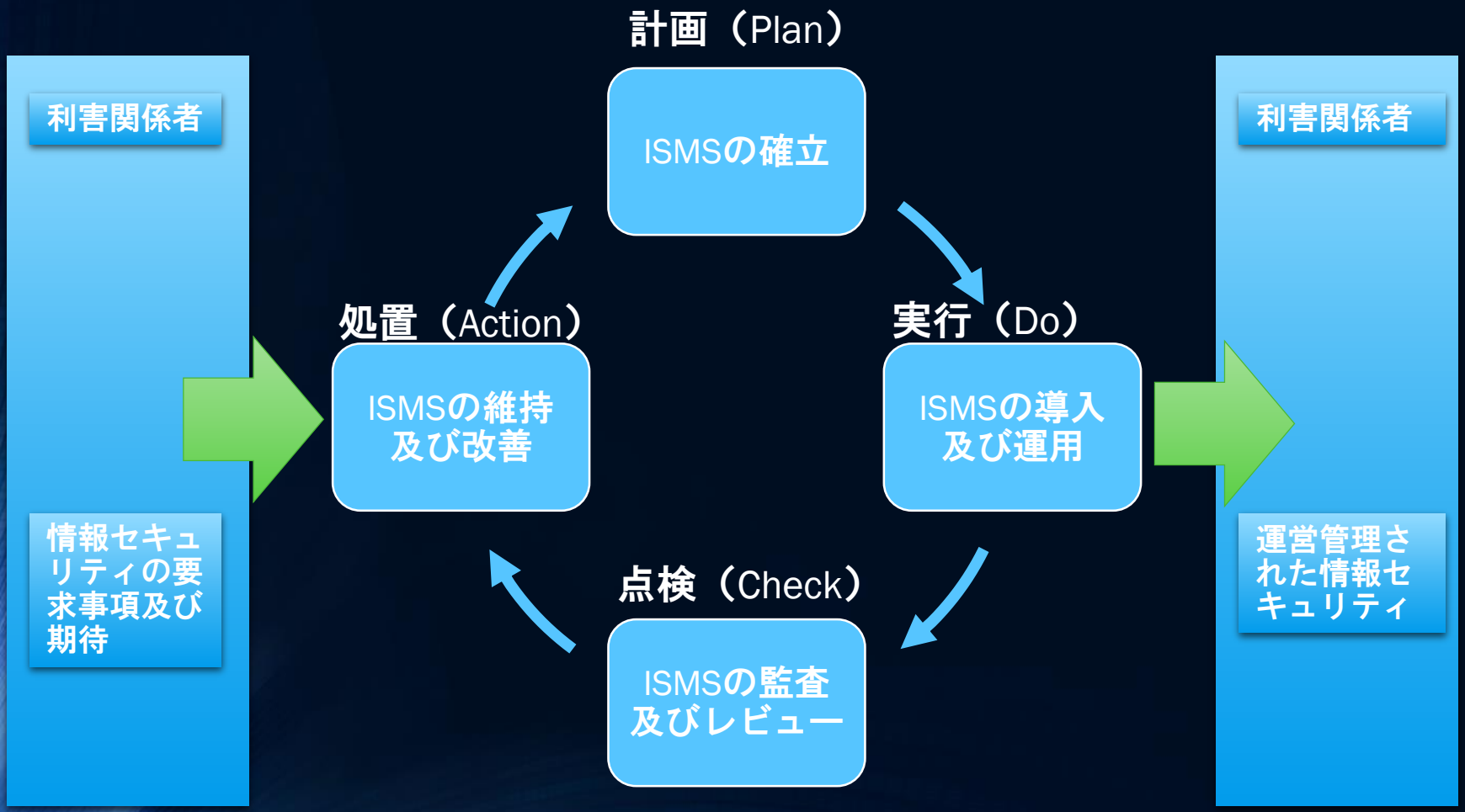


PDCAマネジメントは全ての関係者が理解すべき

ITセキュリティに限らず目的を満足させる十分な状態を維持するためにはPCDAマネジメントが必要

ISO 27000の導入

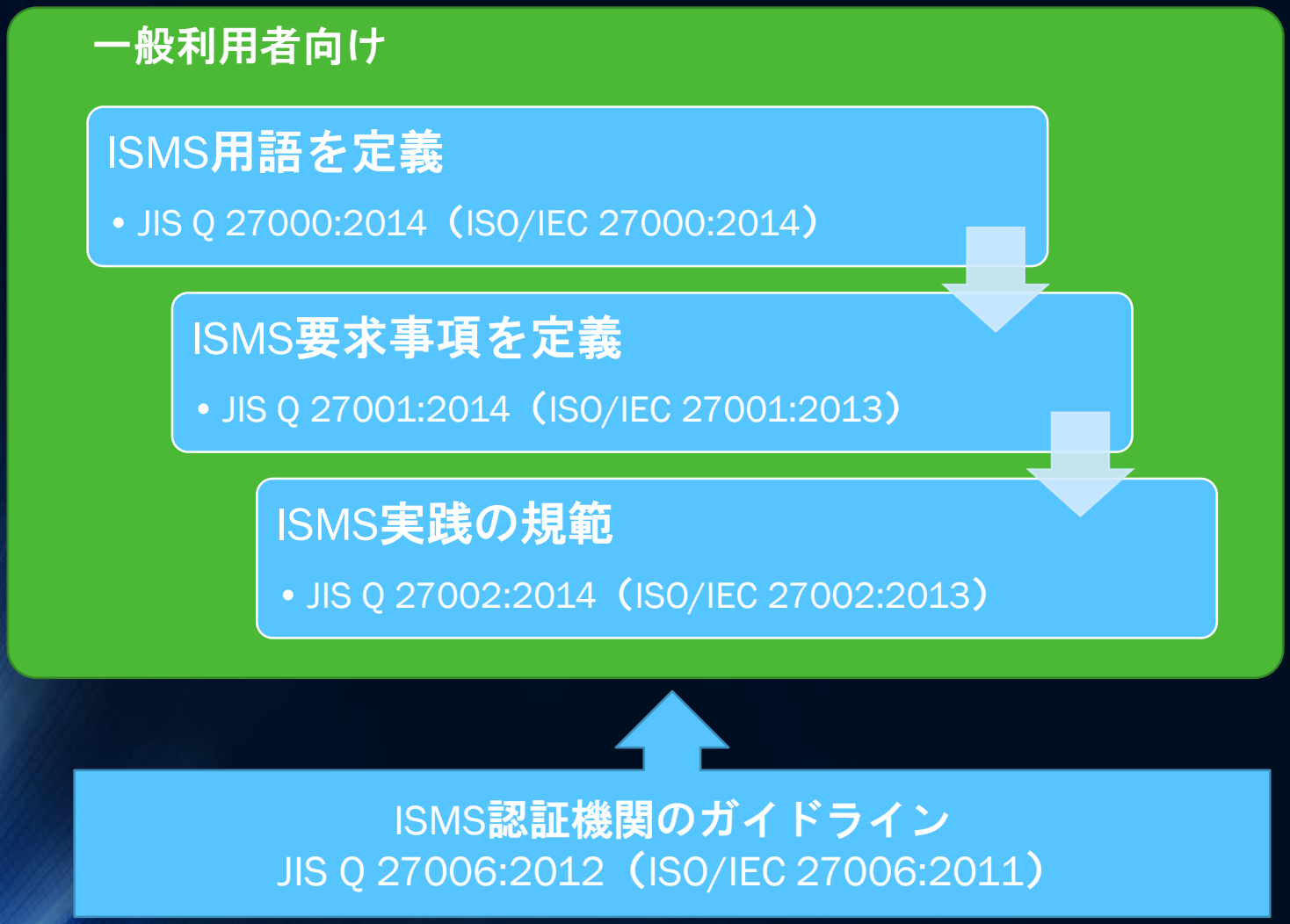
- 基本的なフレームワーク



JIS化されているISO27000シリーズ

- JIS Q 27000:2014
  - 用語を定義する。 ISO/IEC 27000に対応するJIS規格。
  - 用語定義のみで全18ページと短い
- JIS Q 27001:2014
  - ISMSの要求事項を定義する。ISO/IEC 27001:2013に対応。
  - 要求事項のみで短く附属文書含めても全24ページ
- JIS Q 27002:2014
  - JIS Q 27001:2014の要求事項を実施するプロセスにおいて、管理策を選定するための参考に用いる、又は一般に受け入れられている情報セキュリティ管理策を実施するために用いる。ISO/IEC 27002:2013に対応。
  - セキュリティ対策の実務に利用できるガイドラインとなっており、全80ページと前の二つに比べ長い
- JIS Q 27006:2012
  - ISMS認証を行う場合に認証する機関のガイドライン

JIS化されているISO27000シリーズ



JIS Q 27001:2014の内容

JIS Q 27001:2014の内容

※青字は、MSS共通要素（6頁参照）にないISMS固有の箇条

箇条	概略
4. 組織の状況	
4.1 組織及びその状況の理解 4.2 利害関係者のニーズ及び期待の理解 4.3 情報セキュリティマネジメントシステムの適用範囲の決定 4.4 情報セキュリティマネジメントシステム	組織をとりまく内外の状況や利害関係者のニーズ及び期待を理解、決定し、それらを考慮に入れたうえでISMSの適用範囲を定めることが求められている。
5. リーダーシップ	
5.1 リーダーシップ及びコミットメント 5.2 方針 5.3 組織の役割、責任及び権限	ISMSを推進し、関係者の意識向上を図るためには、トップマネジメントの強力なリーダーシップが不可欠である。ここでは、トップマネジメントの果たすべき役割について規定している。
6. 計画	
6.1 リスク及び機会に対処する活動 6.1.1 一般 6.1.2 情報セキュリティリスクアセスメント 6.1.3 情報セキュリティリスク対応 6.2 情報セキュリティ目的及びそれを達成するための計画策定	ISMSにおけるリスク及び機会を決定し、情報セキュリティリスクアセスメント、情報セキュリティリスク対応のプロセスを定めて適用することが求められている。 「規定」である「附属書A管理目的及び管理策」は、6.1.3において、附属書Aの管理策と組織が適用した管理策を比較し、除外した場合にはその理由を適用宣言書に記載することが求められている。
7. 支援	
7.1 資源 7.2 力量 7.3 認識 7.4 コミュニケーション 7.5 文書化した情報	7.5では、各箇条で要求される文書類を文書化し、管理し、維持しながら、要員の力量、並びに利害関係者との反復的かつ必要に応じたコミュニケーションを確立することを通じた、ISMSの運用の支援について規定している。
8. 運用	
8.1 運用の計画及び管理 8.2 情報セキュリティリスクアセスメント 8.3 情報セキュリティリスク対応	情報セキュリティの要求事項を実現するために必要なプロセス群の、策定、導入・実施、及び管理について規定している。また、そのために不可欠な情報セキュリティリスクアセスメント、情報セキュリティリスク対応の実施についても規定している。
9. パフォーマンス評価	
9.1 監視、測定、分析及び評価 9.2 内部監査 9.3 マネジメントレビュー	情報セキュリティパフォーマンスの評価（監視、測定、分析及び評価）、内部監査及びマネジメントレビューについて規定している。
10. 改善	
10.1 不適合及び是正処置 10.2 継続的改善	不適合発生時の処置、及びとった処置の文書化と、ISMSの適切性、妥当性及び有効性の継続的改善について規定している。

http://www.isms.jipdec.or.jp/doc/ismspanf.pdf

ISMS制度の基準・規定・ガイド等

ISO/IEC 27001（JIS Q 27001） （ISMS認証基準）	第三者である認証機関が本制度の認証を希望する組織の適合性を評価するためのISMS認証基準である。
ISMSユーザーズガイド ISMSユーザーズガイド ―リスクマネジメント編―	JIS Q 27001の要求事項について一定の範囲でその意味するところを説明しているガイドである。 リスクマネジメント編はISMSユーザーズガイドを補足し、リスクマネジメント、とりわけリスクアセスメント及びその結果に基づくリスク対応についての理解を深めるために必要な事項について、例を挙げて解説している。
医療機関向けISMSユーザーズガイド	ISMSユーザーズガイドの医療機関向け版で、医療機関におけるISMSの理解を深めるためのガイドである。
法規適合性に関する ISMSユーザーズガイド	企業がリスクマネジメントを実施する上で、企業の法的リスクを考慮することは重要であり、とりわけ個人情報保護に対応する手段としてISMSの枠組みは極めて有効である。 本書はISMSの枠組みが法的及び規制要求事項に適合させる仕組みであることを理解するためのガイドである。
クレジット産業向け “PCI DSS”／ISMSユーザーズガイド	ISMSユーザーズガイドのクレジット産業向け版で、クレジット産業におけるISMS構築を主眼として、関連する規範とISMS認証基準とのマッピングを示し、ISMSを構築することがこれらの規範を順守する上で非常に有効な手段であることを示したガイドである。
クレジット加盟店向け “情報セキュリティのためのガイド”	クレジット加盟店向けに、PCI DSS ／ ISMS準拠に関して説明しているガイドである。
地方公共団体と情報セキュリティ ～ISMSへの第1歩～	地方公共団体がISMSに取り組む際に直面するかもしれない特有な問題を洗い出し、それに対処するためのアドバイスやノウ・ハウをわかりやすく記載したハンドブックである。
外部委託における ISMS適合性評価制度の活用方法	組織又は企業において情報処理業務の一部又は全てを外部委託する場合に、情報セキュリティ責任者及び担当者が委託先の選定にISMS適合性評価制度を活用するためのガイドである。
ISMS認証機関認定基準及び指針	認証機関の認定審査及び登録を行う際の認定基準及び指針であり、ISO/IEC 27006（ISO/IEC 17021を含む）に基づいている。
IMS認証機関認定の手順 IMS認証機関認定の手引き	手順は認証機関が認定を受けるための手順と、認定を申請する機関及び認定された機関の権利と義務について規定したもの、手引きは、申請から登録までと登録維持の標準的な流れと条件を示したものである。
IMS認定シンボル使用規定	認定シンボルを使用する場合の、認定シンボルの表示及び適用条件等について規定したものである。

備考：上記の他にも、ISMS制度の普及促進のための各種文書や認定関連文書がある。

http://www.isms.jipdec.or.jp/doc/ismspanf.pdf

JIS Q 27000シリーズの参照と取得

- JIS Q 27000シリーズの参照先
  - JISC（日本工業標準調査会）のページから検索し“参照”可能
    - タイトルの検索キーワード“情報セキュリティ”
  - http://www.jisc.go.jp/app/JPS/JPSO0020.html
  - 後述する日本規格協会のJISハンドブックに含まれる解説などはなく、規格のみ参照できる

- JIS Q 27000シリーズの購入
  - JSA（日本規格協会）のサイトから購入可能
  - http://www.iso.org/iso/home.htm
  - ISO規格なども購入できる

ISO 27000シリーズ(１)

- ISO/IEC 27000:2014 Information security management systems -- Overview and vocabulary
- ISO/IEC 27001:2013 Information security management systems -- Requirements
- ISO/IEC 27002:2013 Code of practice for information security controls
- ISO/IEC 27003:2010 Information security management system implementation guidance
- ISO/IEC 27004:2009 Information security management -- Measurement
- ISO/IEC 27005:2011 Information security risk management
- ISO/IEC 27006:2011 Requirements for bodies providing audit and certification of information security management systems
- ISO/IEC 27007:2011 Guidelines for information security management systems auditing
- ISO/IEC TR 27008:2011 Guidelines for auditors on information security controls
- ISO/IEC 27010:2012 Information security management for inter-sector and inter-organizational communications
- ISO/IEC 27011:2008 Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
- ISO/IEC 27013:2012 Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- ISO/IEC 27014:2013 Governance of information security
- ISO/IEC TR 27015:2012 Information security management guidelines for financial services
- ISO/IEC TR 27016:2014 Information security management -- Organizational economics
- ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO 27000シリーズ（２）

- ISO/IEC TR 27019:2013 Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry
- ISO/IEC TR 27023:2015 Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002
- ISO/IEC 27031:2011 Guidelines for information and communication technology readiness for business continuity
- ISO/IEC 27032:2012 Guidelines for cybersecurity
- ISO/IEC 27033-1:2009 Network security -- Part 1: Overview and concepts（Part5まである）
- ISO/IEC 27034-1:2011 Application security -- Part 1: Overview and concepts
- ISO/IEC 27035:2011 Information security incident management
- ISO/IEC 27036-1:2014 Information security for supplier relationships -- Part 1: Overview and concepts（Part3まである）
- ISO/IEC 27037:2012 Guidelines for identification, collection, acquisition and preservation of digital evidence
- ISO/IEC 27038:2014 Specification for digital redaction
- ISO/IEC 27039:2015 Selection, deployment and operations of intrusion detection systems (IDPS)
- ISO/IEC 27040:2015 Storage security
- ISO/IEC 27041:2015 Guidance on assuring suitability and adequacy of incident investigative method
- ISO/IEC 27042:2015 Guidelines for the analysis and interpretation of digital evidence
- ISO/IEC 27043:2015 Incident investigation principles and processes

参考：CMMI（能力成熟度モデル統合）

- CMMIはカーネギーメロン大学のサイトからダウンロード可能（英語）
  - http://www.sei.cmu.edu/reports/10tr033.pdf
  - 全480ページ。この規格書でプロジェクトマネジメント全体をカバー

  - ISO 27000シリーズは複数の規格書で個別領域に詳細に対応している
  - ISO規格なのでリスクマネジメントのISO 31000、ITサービスマネジメント（ITIL）のISO 20000なども参考にする
    - ITILにも認証制度がある

27002の内容

- 27002はISMS実現のためのガイドライン
- 基本的に「○○することが望ましい」となっている
- 例：14.1 情報セキュリティ要求事項の分析及び仕様化

開発に適用される標準類が知られていない可能性がある場合、又は現行の最適な慣行に整合していなかった場合には、新規開発する場合及びコードを再利用する場合の両方に、セキュアプログラミング技術を用いることが望ましい。セキュリティに配慮したコーディングに関する標準類を考慮し、該当する場合は、その使用を義務付けることが望ましい。開発者は、これらの標準類の使用及び試験について訓練を受けることが望ましく、また、コードレビューによって標準類の使用を検証することが望ましい。

開発を外部委託した場合、組織は、その外部関係者がセキュリティに配慮した開発のための規則を順守していることの補償を得ることが望ましい。（14.2.7参照）

全て「望ましい」となっているのはISMSは「継続的改善」を要求しているからである。個々の管理策は直ぐに実現すべき必須事項ではない。

27002の概要(１)

➢情報セキュリティ方針

- 情報セキュリティのための経営陣の方向性と指示を、事業上の要求並びに関連する法令及び規制に従って提示

➢情報セキュリティのための組織

- 組織内で情報セキュリティの実施及び運用に着手し、これを統制するための管理上の枠組みを確立

➢人的資源のセキュリティ

- 従業員及び契約相手がその責任を理解し、その責任の遂行を確実にする

➢資産の管理

- 組織の資産を特定し、適切な保護の責任を定め、情報の適切なレベルの保護を確実にする

27002の概要(２)

- **アクセス制御**
  - 情報及び情報処理施設へのアクセスを制限し、認可された利用者のアクセスを確実にし、認可されていないアクセスを防止
- **暗号**
  - 情報の機密性、真正性及び/又は完全性を保護するために、暗号の適切かつ有効な利用を確実にする
- **物理的及び環境的セキュリティ**
  - 組織の情報及び情報処理施設に対する認可されていない物理的アクセス、損傷及び妨害を防止
- **運用のセキュリティ**
  - 情報処理設備の正確かつセキュリティを保った運用を確実にする
- **通信のセキュリティ**
  - ネットワークにおける情報の保護、及びネットワークを支える情報処理施設の保護を確実にする

27002の概要(３)

- **システムの取得、開発及び保守**
  - ライフサイクル全体にわたって、情報セキュリティが情報システムにとって欠くことのできない部分であることを確実にする
- **供給者関係**
  - 供給者がアクセスできる組織の資産の保護を確実にする
- **情報セキュリティインシデント管理**
  - セキュリティ事象及びセキュリティ弱点に関する伝達を含む、情報セキュリティインシデントの管理のための、一貫性のある効果的な取組みを確実にする
- **順守**
  - 情報セキュリティに関連する法的、規制または契約上の義務に対する違反、及びセキュリティ上のあらゆる要求事項に対する違反を避ける

27000のフレームワークと能力成熟度モデル

- ISMS認証を取得する場合、一定レベル以上のセキュリティを達成している必要がある
- **一度に全てのセキュリティ管理策導入は困難な場合が多い**
- ISMS認証の取得を目的としていない場合、能力成熟度モデル型で順次改善すると導入しやすい
- 27002のガイドラインはすべて「○○することが望ましい」となっているので、例えば以下のようにする
  - レベル０-当該「セキュリティ対策」の活動が満たされていない状態を
  - レベル１-当該「セキュリティ対策」に関する初歩的な理解とその場限りの対応
  - レベル２-当該「セキュリティ対策」の効率や効果の向上
  - レベル３-当該「セキュリティ対策」についての総合的な熟達

SAMM
～ソフトウェアセキュリティ保障成熟度モデル～

- SAMMは簡易な能力成熟度モデルであり参考にし易いモデル
  - http://www.opensamm.org/
  - Creative Commons Attribution-Share Alike 3.0 License
  - SAMMの日本語版もダウンロード可能

- 成熟度の基準やチェック方法を参考にするとよい

経営層・マネージャー
がすべきこと

すべきことはISO27001に記載されている

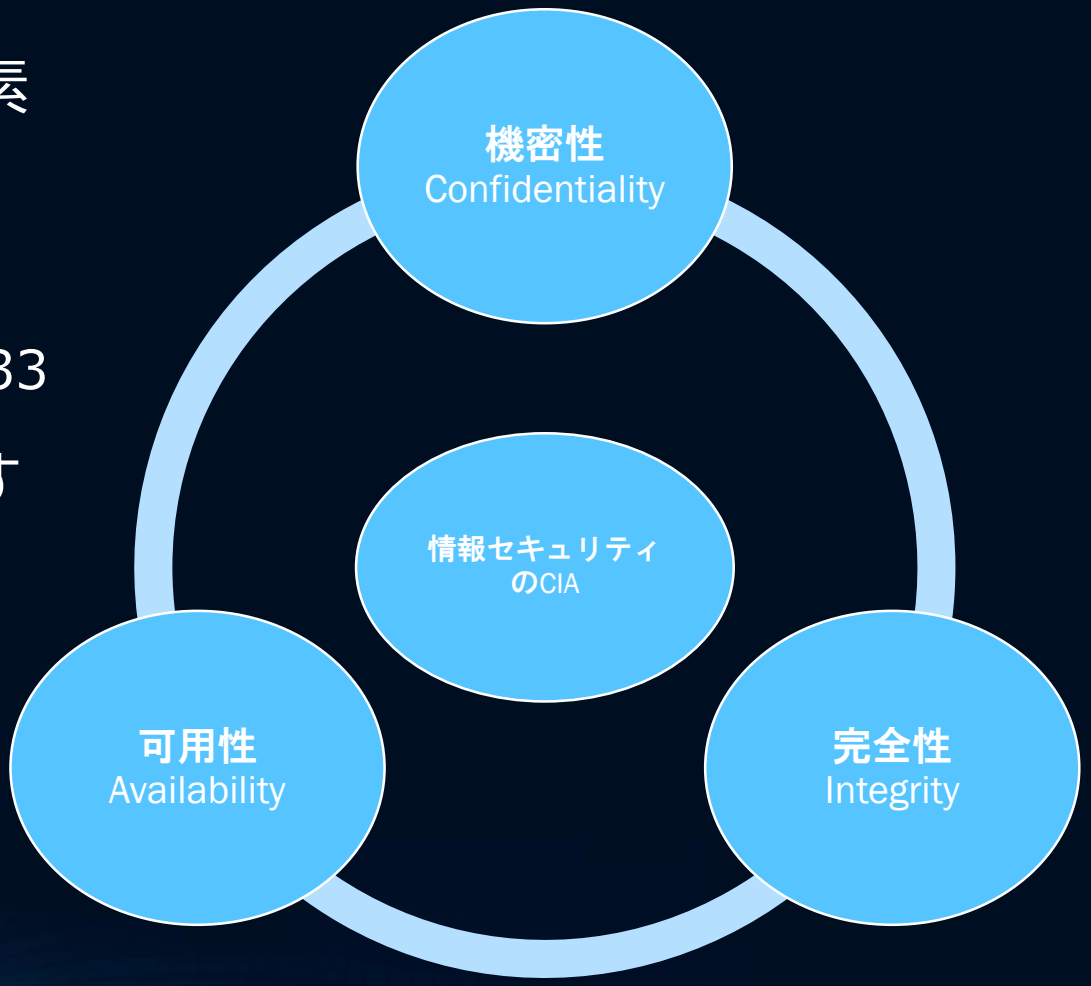
- 組織の状況把握（4）
- リーダーシップ（5）
- 計画（6）
- 支援（7）
- 運用（8）
- パフォーマンス評価（9）
- 改善（10）

基本概念

ISO/JIS標準の基本概念と
標準からは解りづらいセキュリティの基本概念を解説

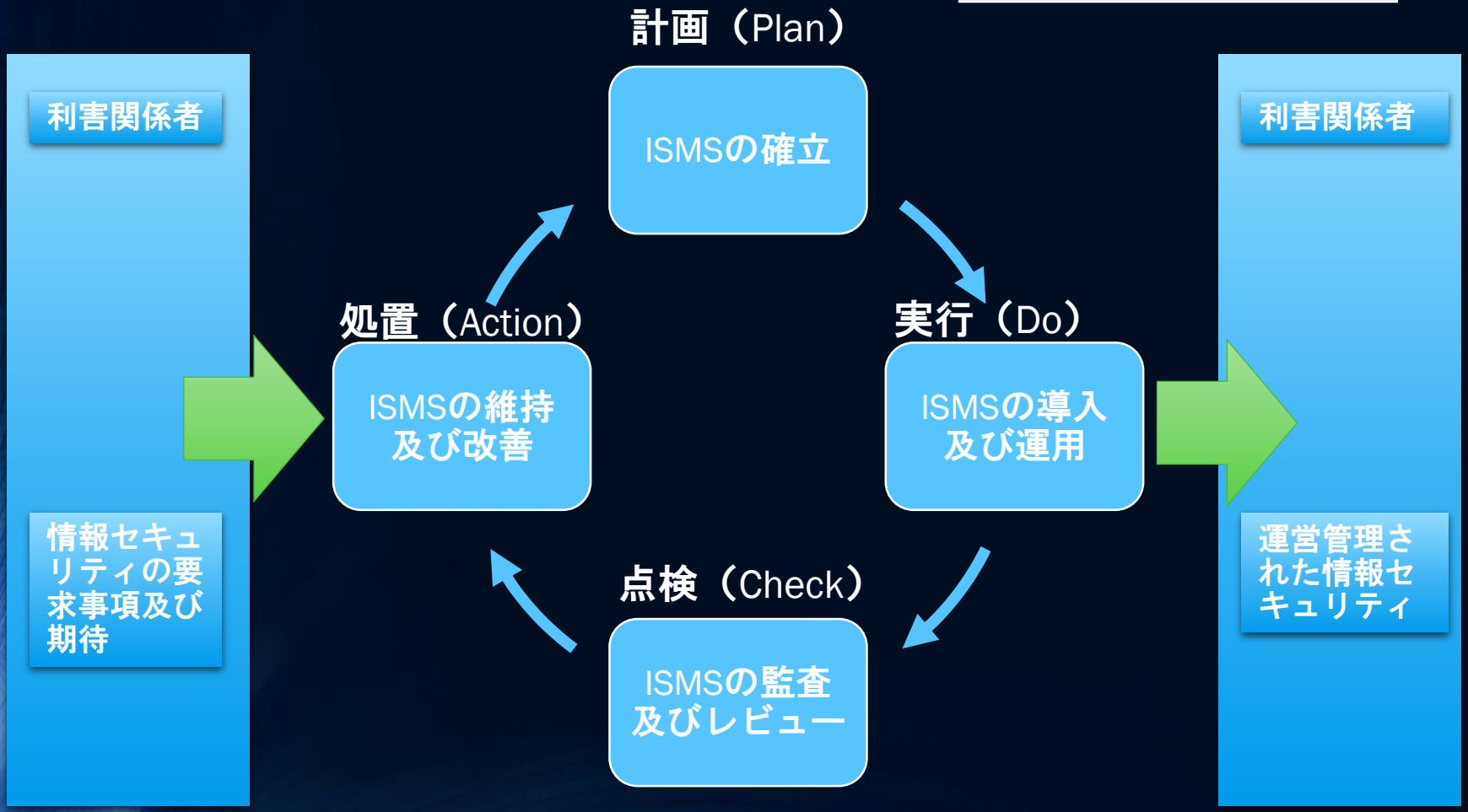
ITセキュリティの基本要素

- ITセキュリティの目的はITセキュリティの基本要素を満たすことで達成
- セキュリティのCIA
  - JIS Q 27000:2014 2.33
- 情報セキュリティに関連する全ての要素にCIAが必要



マネジメントの基本

- セキュリティのCIAをマネジメントにより実施、**リスクを許容範囲内**に



機密性 – Confidentiality

- JIS Q 27000:2014 2.12
  - **認可されていない個人、エンティティ又はプロセス（2.61）に対して、情報を使用させず、また、開示しない特性**

- 要するに
  - 他のユーザーや権限を持たないプログラムがアクセスすべきでない情報にアクセスさせない
- 対策例
  - ユーザー認証に多要素認証を用いる
  - プログラム毎に適切な権限を持たせて実行する

完全性 – Integrity

- JIS Q 27000:2014 2.40
  - **正確さ及び完全さの特性**

- 要するに
  - 送金処理後の送金元・送金先の口座残高は送金前と同じ
  - 送金処理の通信傍受などで不正に送金されない
- 対策例
  - RDBMSのトランザクション機能を利用する
  - トランザクション情報の改ざんを暗号理論的ハッシュ関数を用いて防止する

可用性 - Availability

- JIS Q 27000:2014 2.9
  - **認可されたエンティティが要求したとき、アクセス及び使用が可能である特性**

- 要するに
  - ITシステムが利用できるべき時に、ITシステムが利用できる
- 対策例
  - 停電対策としてUPS（非常用のバッテリー電源）を利用する
  - 攻撃者による大量の処理要求を無視する仕組みを導入する

追加の基本要素

- CIAと概念的に重複する部分もあるが、独立した基本要素と考える方が解りやすい
- **信頼性**（Reliability）
  - JIS Q 27000:2014 2.62
  - **意図する行動と結果が一致しているという特性**
- **真正性**（Authenticity）
  - JIS Q 27000:2014 2.8
  - **エンティティは、それが主張するとおりのものであるという特性**
- **責任追跡性、否認防止**（Non-repudiation）
  - JIS Q 27000:2014 2.54
  - **主張された事象又は処置の発生、及びそれを引き起こしたエンティティを証明する能力**

リスクアセスメントの原則

- **参加者は、リスクアセスメントを行うべきである**
  - リスクアセスメントとは、セキュ リティ上の脅威と脆弱性を識別し、リスクの許容できるレベルの決定やリスクを管理するための措置の選択を支援するものです。
  - リスクアセスメントは、技術、物理的・人的な要因、セキュリティの方針（ポリシー）、セキュリティと関わりを持つ第三者のサービスといった、内外 の要因を広く含むものであるべきです。
  - また、他人から受ける、又は、他人に対して与える、潜在的な損害についても 考慮するべきです。

出典：情報システム及びネットワークのセキュリティのためのガイドライン

セキュリティの設計及び実装の原則

- 参加者は、情報システム及びネットワークの本質的な要素として セキュリティを組み込むべきである。
  - 情報システム、ネットワーク及び セキュリティの方針（ポリシー）は、セキュリティを最適なものとするために、 適切に設計され、実装され、かつ調和が 図られる必要があります。
  - 適切な安全防護措置や解決策の設計・採用が重要で、これらは情報の価値と比例するべきです。
  - セキュリティは、すべての製品、サービス、 情報システムやネットワークの設計・構造に不可決な部分であるべきです。
  - 一方、エンドユーザの場合は、自分が 使用するシステムのために、適切な製品やサービスを選択し、構成するべきです。

出典：情報システム及びネットワークのセキュリティのためのガイドライン

セキュリティマネジメント の原則

- 参加者は、セキュリティマネジメントへの包括的アプローチを採用するべきである。
  - 情報セキュリティマネジメントは、 参加者の活動のすべてを含む包括的で、 動的なものであるべきです。
  - また情報セキュリティマネジメントには、セキュリ ティ上の事件の予防、検出、対応やシステムの復旧、保守、レビュー、監査等が含まれるべきです。
  - セキュリティの方針（ポリシー）、手段等は、首尾一貫したセキュリティシステムを構築するために調和が図られ、統合されるべきです。

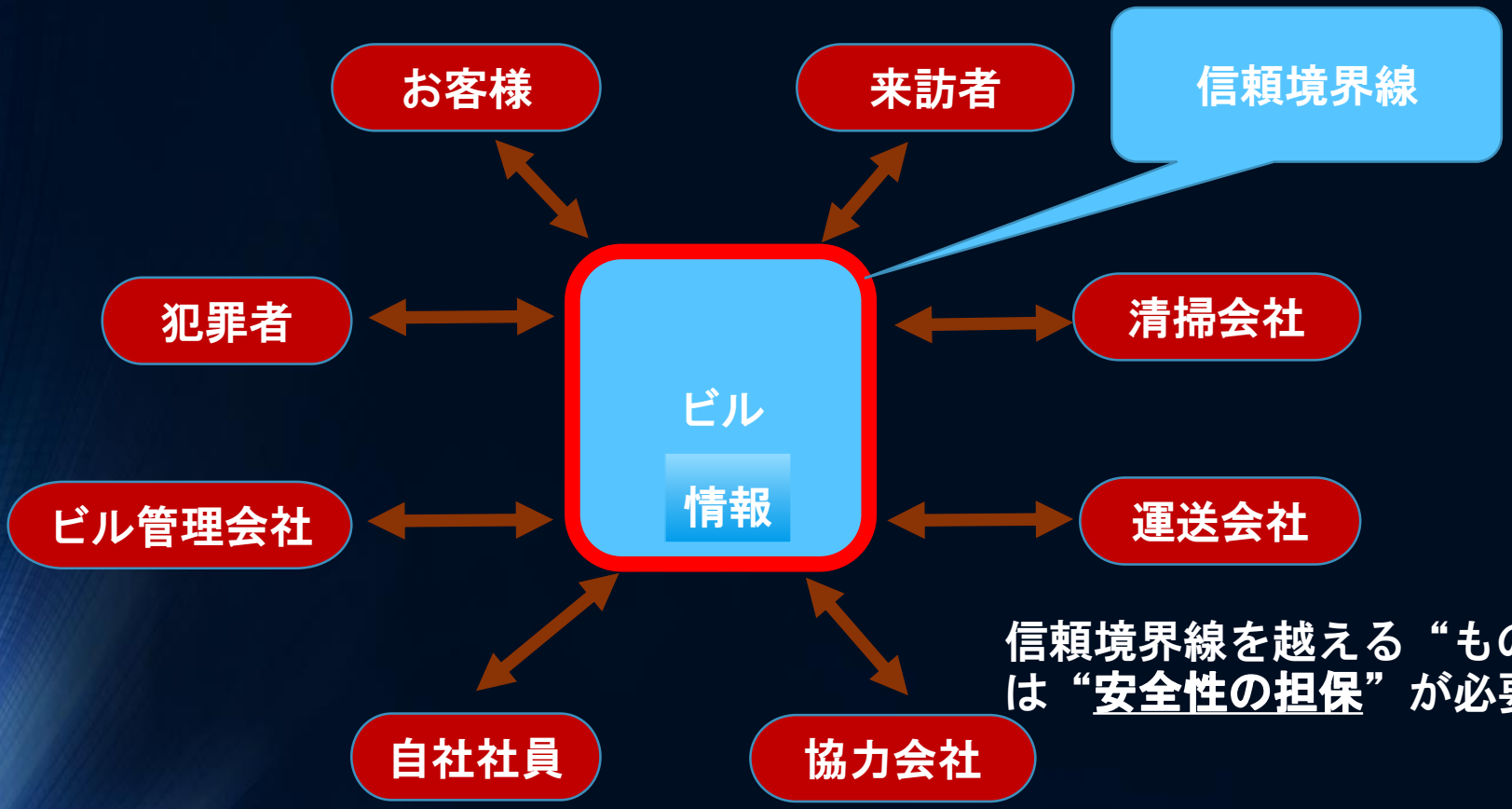
出典：情報システム及びネットワークのセキュリティのためのガイドライン

再評価の原則

- 参加者は、情報システム及びネットワークのセキュリティの レビュー及び再評価を行い、セキュリティの方針、実践、手段及び手続に適切な修正をすべきである。
  - 新たな脅威や脆弱性が絶えず発見されています。
  - 参加者は、これらのリスクに対処するために、セキュリティのすべての面のレビュー、再評価を行うとともに、セキュリティの方針（ポリシー）、手段等を適切に修正する必要があります。

出典：情報システム及びネットワークのセキュリティのためのガイドライン

信頼境界線と境界防御



信頼境界線を越える“もの”は“**安全性の担保**”が必要

社内情報・資産のセキュリティを守る場合、まず建物の境界で防御

「境界防御」と「縦深防御」（多層防御）

- **「境界防御」と「縦深防御」（多層防御）が基本原則**
  - 元々は軍事学の概念
- 境界防御
  - まず防御対象への出入りを防御
- 縦深・多層防御
  - 外側の境界防御のみでなく、内部で区分し更に境界防御や他の防御策を実施
  - フェイルセーフ、フールセーフ
  - 異常なアクセスの検出と防止、不正アクセスがあった場合の影響範囲と特定する仕組みの導入、データの暗号化など

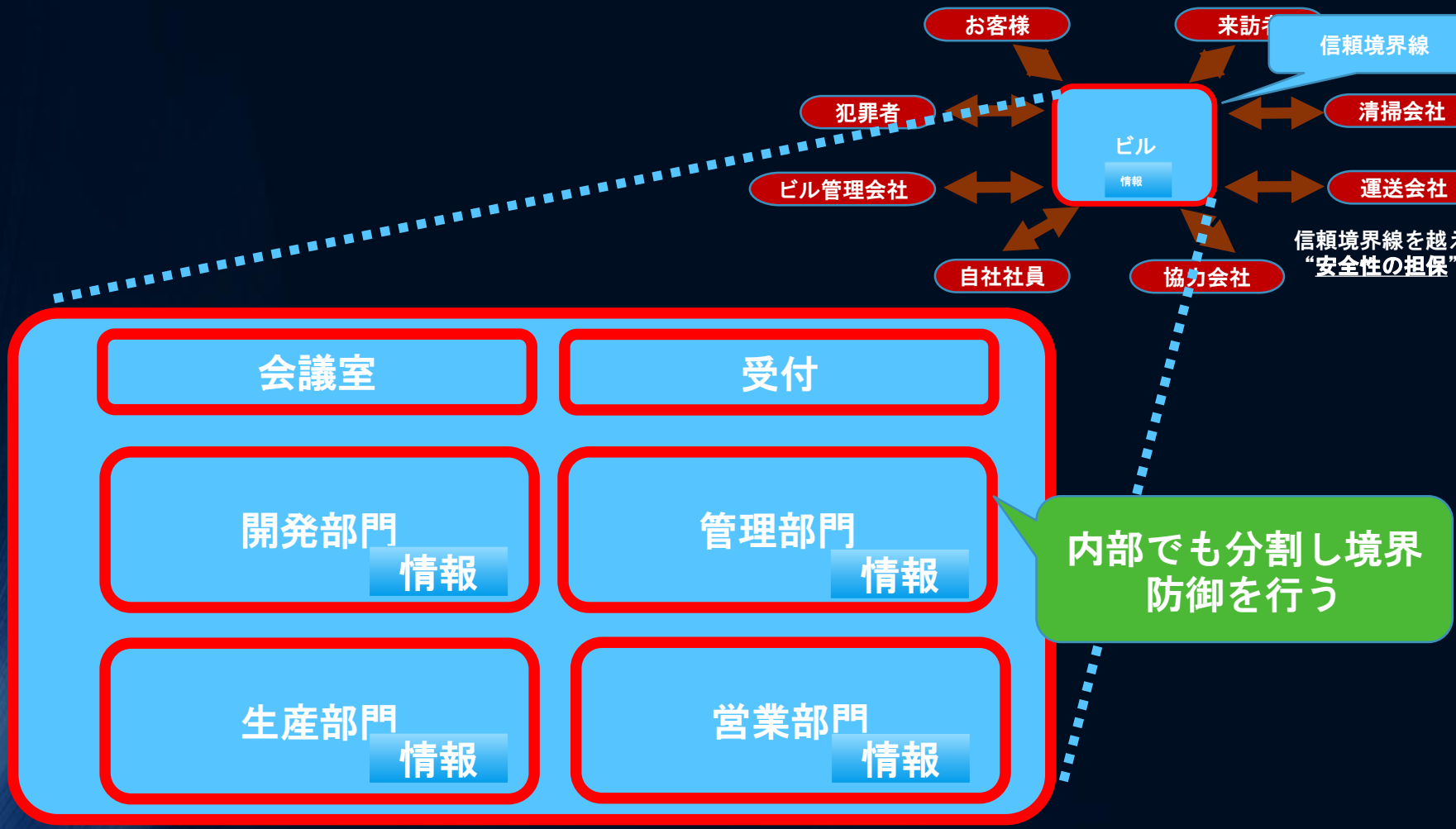
物理的、ネットワーク、ソフトウェア、人的なセキュリティ対策に利用可能

分割と統治

- **「分割と統治」は複雑な問題を解決する基本テクニック**
  - プログラミングでも頻繁に利用されるテクニック
- 分割
  - 問題の領域を適切に区分し分割して対処
- 統治
  - 分割した問題領域を適切に管理するとともに統合して管理

- 物理的、ネットワーク、ソフトウェア、人的なセキュリティ対策、プロジェクトマネジメント（ＷＢＳ-Work Breakdown Structure：作業分解構成図）などに利用可能
  - 例：会社などでオープンなエリア、訪問者も立ち入れるエリア、関係者のみのエリア、担当者のみのエリアなど、と物理的に分割して管理

境界防御と縦深･多層防御



セキュリティ対策は基本的に
「境界防御と縦深/多層防御」と「分割と統治」で成り立っている。

ホワイトリスト

- **情報セキュリティ対策の基本は「ホワイトリスト」**
  - ブラックリストは極力排除、セキュリティ対策ではホワイトリストが基本原則
- ホワイトリスト
  - 許可する項目を指定
- ブラックリスト
  - 許可しない項目を指定
- セキュアなブラックリストを作成するには「事前に全てのリスクの把握」が必要
  - 事前に全てのリスクを把握することは困難、つまり誤りやミスを犯しやすい

ホワイトリストとブラックリスト

セキュリティの基本概念

- 境界防御
- 縦深防御（多層防御/フェイルセーフ/フールセーフ）
- 分割と統治
- 最少権限の原則（ホワイトリスト）
- 認証・認可・バリデーション
- リスク識別と管理（品質/リスク管理）
- アカウンティング（責任追跡・否認拒否）
- 教育（人的リソース）

これらを組織的かつ効果的に実施するには経営層のコミットメントが欠かせない

注：これらだけではない

基本的知識が不足しているユーザー

- **「外部」から「内部」に入ってくるモノすべてに「リスク」**
  - 訪問者、取引先、委託先、従業員、データ、プログラム、ハードウェア
- **「内部」から「外部」に出ていくモノすべてに「リスク」**
  - 訪問者、取引先、委託先、従業員、データ、プログラム、ハードウェア
- **全ての「リソース」に妥当性（バリデーション）検証が必要**
  - 人、データ、プログラム、ハードウェア
- 「リソース」（資源）はいつでも使えない
  - リソース（人、データ、プログラム、ハードウェア）はいつでも使える訳ではない
  - HDD故障によるデータロス、バグによるプログラム停止・データ破壊、停電による機器の停止、災害（火災・地震）による被害

基本的知識が不足している開発者

- **「外部」から「内部」に入ってくるモノすべてに「リスク」**
  - リスク認識不足によるバグ・脆弱性が絶えない
- **「内部」から「外部」に出ていくモノすべてに「リスク」**
  - 出力時に確実な安全対策が必要だが行われていない
- **全ての「リソース・データ・プログラム」に妥当性（バリデーション）検証が必要**
  - ISO 27000/セキュア・防御的プログラミングなどで要求されているが、実施自体を否定する開発者まで存在する
- 「リソース」（資源）はいつでも使えない
  - リソースが使えない場合の対策不足は絶えない

基礎教育の必要性

- 現在社会人である人々はセキュリティの基礎・概念を学ぶ機会がなかった
  - 基礎と概念は簡単だが経験から独自に再構築するのは無駄
- セキュリティの基礎・概念はISO 27000シリーズなどを学習すれば習得可能だが、基本的には基礎・概念の解説はない
  - 基礎・概念がしっかりしていないと「根本的な誤り」「手段の目的化」が起こりやすい
- **導入当初は不可知論でのITセキュリティ導入も必要**だが、どこかの時点で**基礎教育を行った方が効率的**
  - 現場がリスク・問題点を発見・報告・対応できるようになった方が効率的
  - 「文化の構築」を意識

セキュリティ対策：サービス・事業の一環

- 脅威が増加、認識の変化が必要
  - セキュリティ対策：できれば排除する追加のコスト要素から
  - **セキュリティ対策：サービス・事業の一環である必須要素**

- 攻撃者の攻撃はどんどん進化
- 攻撃対象となる我々の意識は古いまま

あらゆるモノが攻撃対象！

1 **認識の原則**
Awareness

まずはここから！

第三部
ITシステム管理に必要な要素

セキュリティにはアーキテクチャーが必要

- アーキテクチャー（構造）なしに対策を導入しても非効果的
- アーキテクチャーの構築にはセキュリティ方針が必要
- セキュリティ方針の構築には経営者層のコミットメントが必要
  - 経営者層のコミットメントが起点
- コミットメントを行うには「**経営者層の認識**」が必要

OECDセキュリティ原則

1 認識の原則 Awareness	2 責任の原則 Responsibility	3 対応の原則 Response

セキュリティ対策を実施する領域

- 人的セキュリティ
- 物理的セキュリティ
- ネットワークセキュリティ
- ソフトウェアセキュリティ

セキュリティ対策を実施する領域

- **物理的セキュリティ**
- ネットワークセキュリティ
- ソフトウェアセキュリティ
- 人的セキュリティ

物理的セキュリティの基本

- 境界防御
  - セキュリティレベルに応じて場所・機器を分割管理
  - 場所・機器などの物理的なアクセスを適切に制限
  - 例：ネットワーク機器、サーバールーム、サーバーへのアクセスを制限
- 縦深・多層防御
  - 物理的にアクセス可能であっても防御
  - 例：USBデバイスの無効化、セキュアブートの有効化、管理コンソールからのアクセス記録の保存
- ホワイトリストの利用
  - アクセス許可はホワイトリストで定義
  - 例：サーバールームへの入退室の許可、デバイスの利用許可
- 耐障害性を実装
  - UPS利用、電源二重化、ディスク冗長化、バックアップ、ホット・コールドスタンバイなど

端末・デバイスセキュリティの基本

- 境界防御
  - 端末・デバイスは用途やセキュリティレベルに応じて分割管理
  - 未許可の端末・デバイスはネットワークに接続させない
  - ファイアーウォール・マルウェア対策ソフト・URLフィルタリングを導入
  - 無用なI/Oデバイスの無効化（USB無効化など）
  - 更新プログラムを速やかに適用
  - 検疫ネットワークの利用
- 縦深防御
  - 定期的なマルウェアスキャン
  - 使用履歴の取得と集中管理、不正/不審な動作の検出

セキュリティ対策を実施する領域

- 物理的セキュリティ
- **ネットワークセキュリティ**
- ソフトウェアセキュリティ
- 人的セキュリティ

ネットワークセキュリティの基本

- 境界防御
  - ネットワークを利用用途、セキュリティレベルの区分に応じて分割
  - ネットワーク境界にファイアーウォールを設置
  - ネットワークに接続可能なデバイスを制限
  - 不信なアクセスの検出と攻撃の防止（IDS/IPS）
- 縦深・多層防御
  - ネットワークに接続する機器自体にもファイアーウォール/フィルタリングを導入
  - PC/モバイル機器などのデバイスにはマルウェア対策
  - 管理者専用のネットワークであっても認証を有効化
  - 重要なシステムにはそのシステムのファイアーウォール機能で接続制限
  - 不信なアクセスの検出と攻撃の防止（IDS/IPS）
- ホワイトリストの利用
  - 接続制限などはホワイトリストで定義

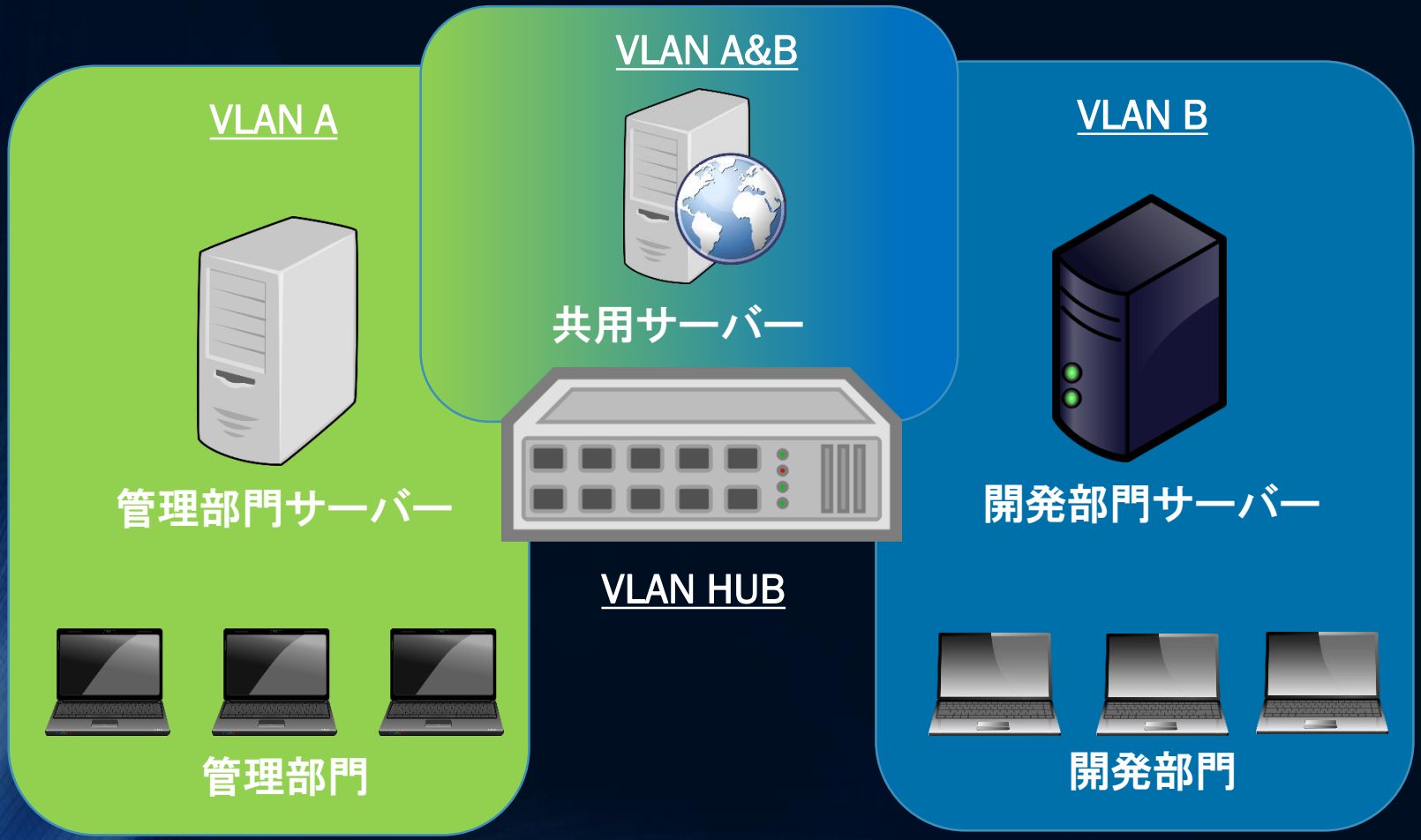
ネットワークを適切に分割＆統治

- VLANの導入は比較的容易かつ効果的
  - VLAN（仮想LAN）とは物理的に同じネットワークケーブルを利用していても、仮想的に別のネットワークとして通信する仕組み
- SOHOでも容易かつ安価
  - VLAN機能付き＋ライフタイム保障のHUBがVLANなしとほぼ同価格で販売

アンマネージプラス・スイッチ

http://www.netgear.jp/business/switch/prosafeplusswitch

VLANの仕組み


VLAN A&B
VLAN A
VLAN B
共用サーバー
管理部門サーバー
開発部門サーバー
VLAN HUB
管理部門
開発部門

セキュリティ対策を実施する領域

- 物理的セキュリティ
- ネットワークセキュリティ
- **ソフトウェアセキュリティ**
- 人的セキュリティ

ソフトウェアセキュリティの基本

- 境界防御
  - 防御的・セキュアプログラミングの原則
  - 外部からの入力はすべて厳格にバリデーションする
  - 外部への出力はすべて安全に処理されるようする
- 縦深・多層防御
  - プログラム・システムは適切に分割管理し、それぞれで境界防御を行う
  - 不正な利用、プログラムの不具合にそなえ、責任追跡性を備えた記録を保存する
  - 予期せぬ動作、機器障害などに備え、フェイルセーフを実装する
- 標準・ガイドラインの利用
  - SAMM、セキュアプログラミング標準、脆弱性対策ガイドなどを利用する

セキュリティ対策を実施する領域

- 物理的セキュリティ
- ネットワークセキュリティ
- ソフトウェアセキュリティ
- **人的セキュリティ**

人的セキュリティの基本

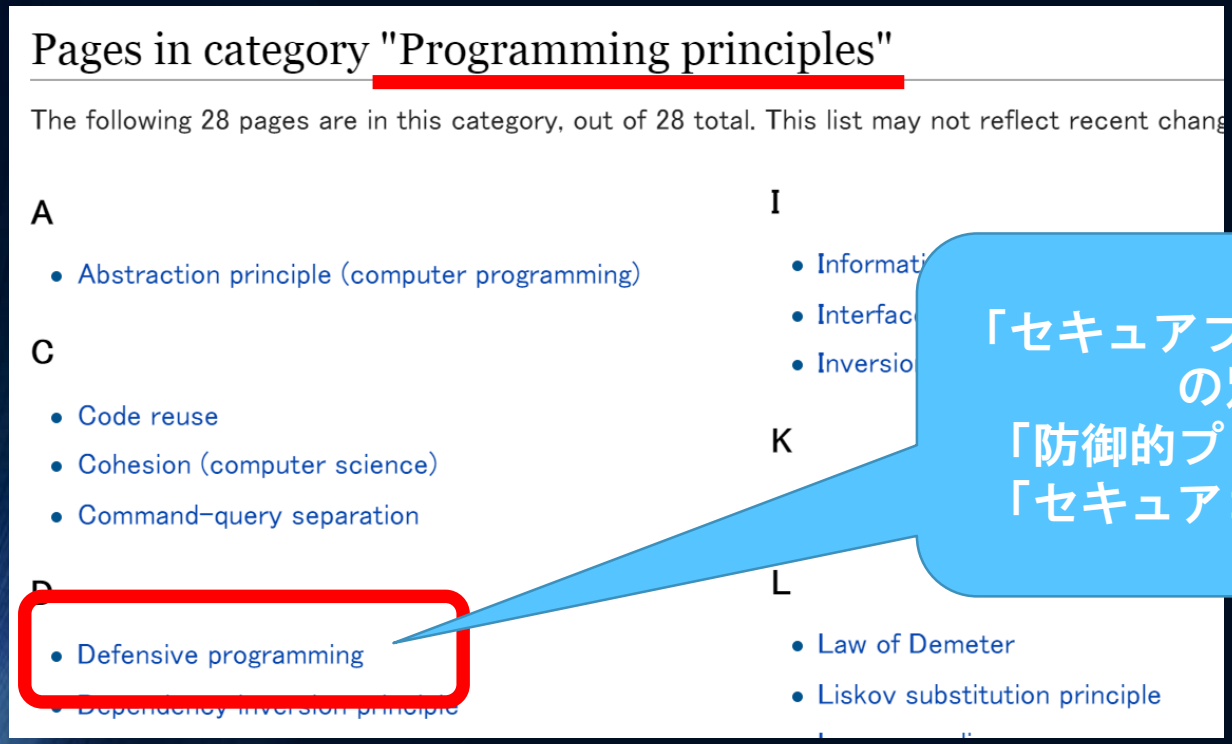
- 境界防御
  - 人的なセキュリティも物理セキュリティで対応
  - 物理的に対応できない場合、論理的（VLANによるネットワーク分割）などで対応
  - 契約の際に契約者の人的セキュリティについても条件に入れる
  - 要員の全てが職務に必要とされているセキュリティ要求を理解していることを確認する
- 縦深・多層防御
  - 監査などの手順や仕組みで不正を防止・検出
- 教育・トレーニング
  - システムのみでの対応には限界（システム的制約、リソース的制約）があり、セキュリティ教育・トレーニングが欠かせない
  - 組織として教育・トレーニングの達成目標を設定し、組織として実現に取り組む

1 認識の原則
Awareness

第四部
ITシステム開発に必要な要素

セキュアプログラミングは プログラミングの原則

- セキュアプログラミングは「プログラミング原則」と考えられている



https://en.wikipedia.org/wiki/Category:Programming_principles

セキュアプログラミング

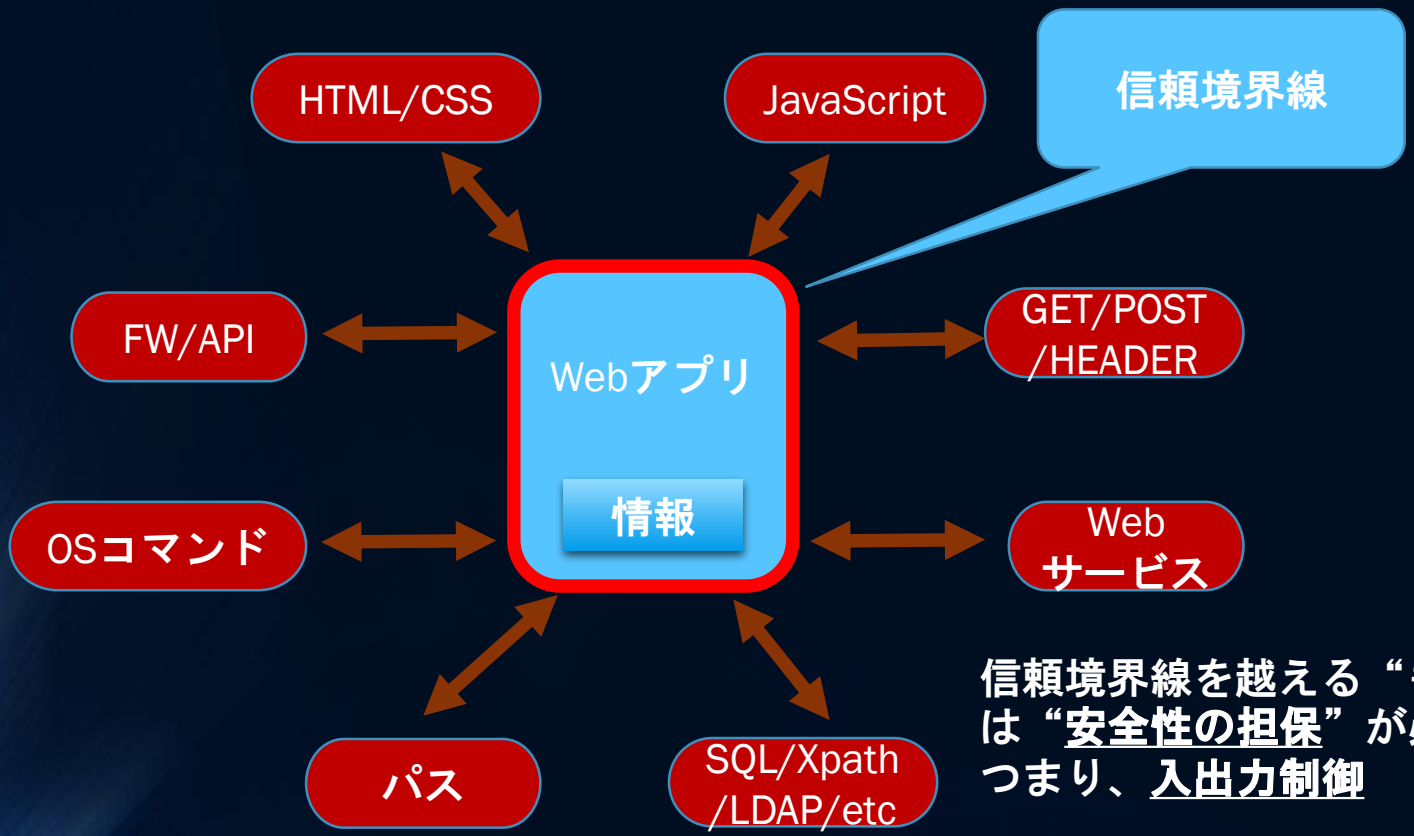
- 別名：防御的プログラミング、セキュアコーディング
- ISO 27002:2013ではソフトウェア開発に「セキュアプログラミング」が利用されていること強制することが望ましいと記載されている。

開発に適用される標準類が知られていない可能性がある場合、又は現行の最適な慣行に整合していなかった場合には、**新規開発する場合及びコードを再利用する場合の両方に、セキュアプログラミング技術を用いる**ことが望ましい。セキュリティに配慮したコーディングに関する標準類を考慮し、該当する場合は、その**使用を義務付ける**ことが望ましい。開発者は、これらの標準類の使用及び試験について訓練を受けることが望ましく、また、**コードレビューによって標準類の使用を検証**することが望ましい。

開発を外部委託した場合、組織は、その外部関係者がセキュリティに配慮した開発のための規則を順守していることの補償を得ることが望ましい。（14.2.7参照）

セキュアなソフトウェア構造

- Webアプリの例



信頼境界線を越える“もの”は“**安全性の担保**”が必要
つまり、**入出力制御**

入出力でバリデーション・エスケープは必須
ISO 27002にも記載されている

ISO27002のアプリセキュリティ対策

- セキュアなソフトウェア構造の適用を原則としている

14.2.5 セキュリティに配慮したシステム構築の原則

アプリケーションの開発手順では、入出力インターフェースをもつアプリケーションの開発に対し、セキュリティに配慮した構築技術（セキュアプログラミングなど）を適用することが望ましい。

おかしなセキュアプログラミングの現状

- 情報セキュリティとセキュリティ標準を推進すべきIPAが「おかしなセキュアプログラミング」を啓蒙
  - 先月問題を指摘し、「セキュアプログラミング講座Web編」は削除する旨の回答を得た

IPAの「セキュアプログラミング講座Web編」は
セキュアプログラミングではないので注意
このレベルでも根本的な間違いがあるのが現状

セキュアプログラミング標準

- セキュアプログラミングの本家・元祖はCERT/カーネギーメロン大学
  - https://www.securecoding.cert.org/confluence/display/seccode/SEI+CERT+Coding+Standards
- 細かいコーディング手法を定義しているが、基本は以下の通り
  - CERT TOP 10 Secure Coding Practices

1. 入力をバリデーションする
2. コンパイラの警告に用心する
3. セキュリティポリシーの為に構成／設計する
4. 簡易にする
5. デフォルトで拒否する

6. 最小権限の原則を支持する
7. 他のシステムに送信するデータを無害化する
8. 縦深防御を実践する
9. 効果的な品質保証テクニックを利用する
10. セキュアコーディング標準を採用する

開発者のセキュリティ認識は皆さんあまりと変わらない

- **プロだから当然知っているはず、は通用しない**
  - そもそもITセキュリティについて体系的に学ぶ機会がない
  - 一部では「セキュリティ業界」にいる技術者・専門家でさえ基本概念を理解していない

- 現状を認識すると**発注者が開発のセキュリティを担保**せざるを得ない

開発者のセキュリティ認識レベルを問う

- セキュリティ認識レベルを問う質問例
- 「セキュリティ対策の定義を教えてください」
  - NG：脆弱性を排除することが主目的の対策
  - NG：脆弱性を排除・緩和する対策
  - OK：リスクを変化させる対策
- 「セキュリティ対策の本質・目的を教えてください」
  - NG：脆弱性を排除・緩和する対策を導入　（←手段の目的化）
  - OK：本質はリスクマネジメント、目的はITシステムを許容範囲内のリスクで利用可能にする
- 「セキュリティ対策の原則を挙げてください」
  - NG：脆弱性に対応し排除する（←手段に過ぎない）
  - OK：OECDセキュリティガイドラインの9原則

開発者の認識への対応

- 国際標準セキュリティと一致する認識を持つ開発者は“少ない”、少なくとも多数とは言えない

- 現状では十分なセキュリティ認識を持つ開発者・開発会社を選ぶことは比較的困難
  - ISMS認証を取得していても、個々の開発者の認識は怪しいことも

- **発注者が発注時に「認識」と「対応」を要求し検証する**
  - ISMSガイドライン（ISO 27002）にも記載

ソフトウェア脆弱性の原理

ソフトウェア脆弱性問題のほとんどは インジェクション問題

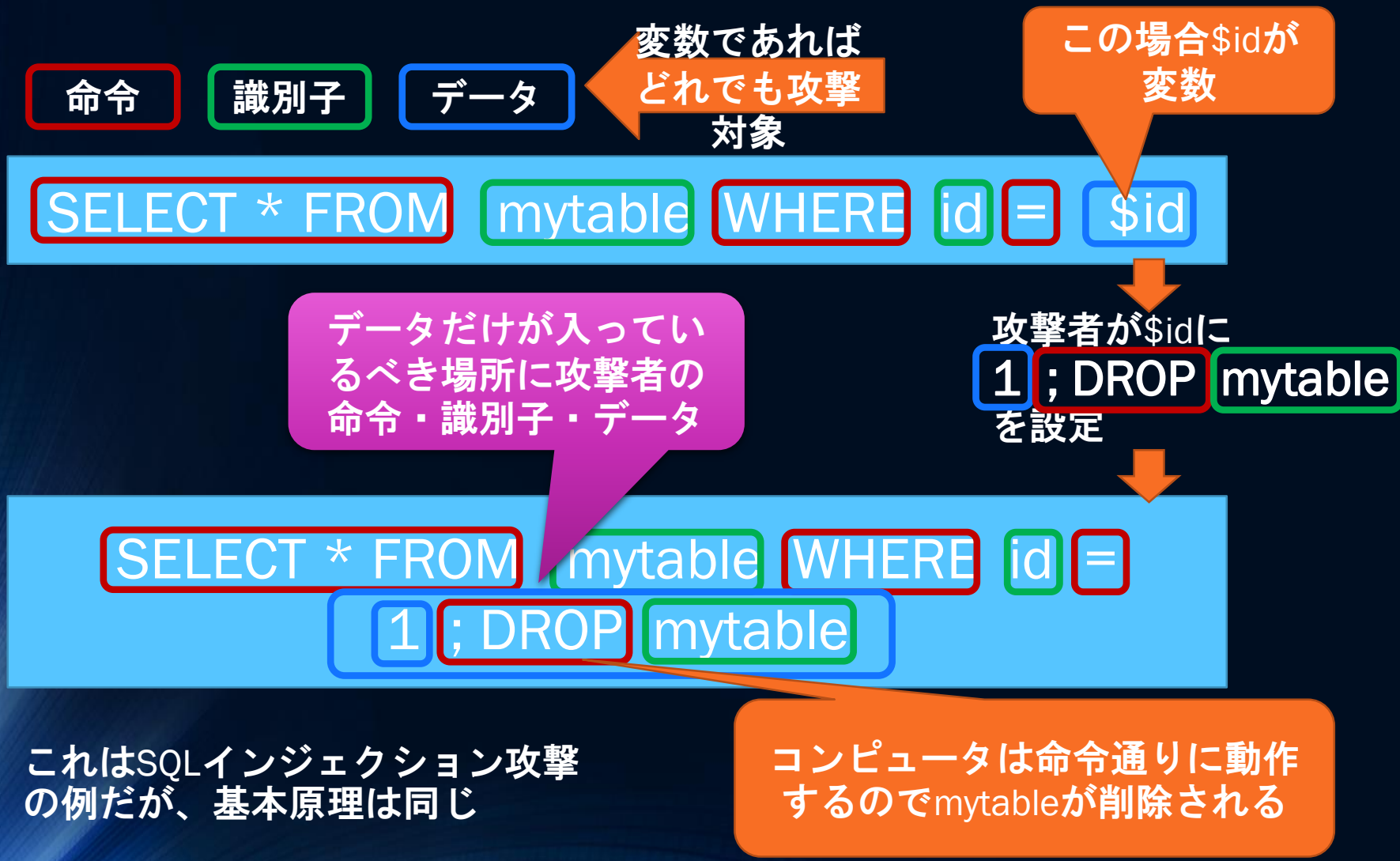
- インジェクション脆弱性の例
  - XSS（クロスサイト・スクリプティング・JavaScriptインジェクション）、SQLインジェクション、OSコマンドインジェクション、XPathインジェクション、LDAPインジェクションなど
- いろいろ名前があって良く解らない！
  - でも大丈夫、基本と原理は簡単

インジェクション脆弱性の原理

- コンピュータのプログラムは基本的に「命令」「識別子」「データ」で構成
- インジェクション攻撃とは主に「データ」に攻撃者の命令を挿入（インジェクション）する攻撃

$idには通常“1234”などのID番号が入るが、プログラムの不具合により攻撃者が命令を挿入可能になる

インジェクション脆弱性の原理



セキュアと言われるAPIが セキュアとは限らない

- プリペアードクエリの例

プリペアードクエリは データ への命令・識別子・データ埋め込みだけに対応している。従って「プリペアードクエリ“だけ”使っていればよい」は十分な対策としては誤り。

「データだけ変数」という前提条件は一般論として通用しない。こういった前提条件の間違いはセキュリティ専門家でもしがち。

インジェクション対策

- **全てのインジェクション攻撃の原理は基本的に同じ**
- CERT TOP 10 **セキュアコーディング**プラクティスの１と７で対応可能
  - **１．入力をバリデーションする**
  - **７．他のシステムに送信するデータを無害化する**

境界防御

入出力の妥当性検証・安全対策はプログラムのセキュリティ対策に限らず、全ての
セキュリティ対策に共通の対策

例：入退室管理、材料/仕入れと出荷品の管理

セキュアプログラミング（再掲）

- 別名：防御的プログラミング、セキュアコーディング
- ISO 27002:2013ではソフトウェア開発に「**セキュアプログラミング**」が利用されていること強制することが望ましいと記載されている。

開発に適用される標準類が知られていない可能性がある場合、又は現行の最適な慣行に整合していなかった場合には、**新規開発する場合及びコードを再利用する場合の両方に、セキュアプログラミング技術を用いる**ことが望ましい。セキュリティに配慮したコーディングに関する標準類を考慮し、該当する場合は、その**使用を義務付ける**ことが望ましい。開発者は、これらの標準類の使用及び試験について訓練を受けることが望ましく、また、**コードレビューによって標準類の使用を検証**することが望ましい。

開発を外部委託した場合、組織は、その外部関係者がセキュリティに配慮した開発のための規則を順守していることの補償を得ることが望ましい。（14.2.7参照）

※ IPAが公開している「セキュアプログラミング講座Web編」はISO規格のいうセキュアプログラミングとは異なるので注意

ソフトウェア開発の受発注

法的環境の変化

- SQLインジェクション脆弱性による被害で瑕疵担保責任を上回る賠償金支払いが開発会社に命ぜられる
- 基本的な脆弱性対策を怠った場合、契約書などに記載されていなくても、**開発会社は契約書に記載されている以上の損害賠償を請求**される
- 「基本的な脆弱性対策」は既に多くの脆弱性がリストアップされている
- 脆弱性対策トップ10（例：OWASP TOP 10）などに記載されているような基本対策を怠った場合、重大な瑕疵とされる可能性が高い

ITシステムを発注受発注する場合の注意点

- 「契約」がとても重要

- 発注側から見ると、契約には機能要件、費用、期間以外にもセキュリティ要件が必要
  - **黙っていても「対策してくれる」は今のところないと考える**べき
  - セキュリティ問題発生時に**瑕疵担保以上の賠償を得ても、失うモノの方が大きい**

- 受注側から見ると、契約に書かれてなくても基本的セキュリティ対策を怠ると瑕疵担保条項以上の責任が発生
  - **発注者が明示的にセキュリティ対策を指定しなくても確実に作る**べき
  - セキュリティ要件がない・不十分な場合、**受注側が明確にする責任**がある

セキュリティ要件の定義

- **簡単な方法は“標準”や“ガイドライン”の遵守をそのまま要件**とする
  - ISO 27002 14.2「開発及びサポートプロセスにおけるセキュリティ」をそのまま要件とする
  - OWASP、SANSなどのガイドラインをそのまま要件とする
- **セキュリティはトレードオフ**
  - 高セキュリティ　＝　高コスト
  - 低セキュリティ　＝　低コスト

安さだけを求めるのは実は高コスト

- 開発者のセキュリティリテラシーに関係なくセキュアな開発はコスト増
  - 専門化による要求仕様レビュー
  - 専門化によるコードレビュー
  - ツールによるコード検査・アプリ検査
  - セキュアなコードに必要なコード量増加

ソフトウェアライフサイクル全体でセキュリティ対策が必要

しかし、トレードオフでない場合も

- セキュアプログラミング（防御的プログラミング）のテクニックとして「契約プログラミング」がある

- **「契約プログラミング」を正しく適用すると、安全かつ高速かつ高品質かつ素早く構築することが可能**

- 契約プログラミングの基本
  - 開発時には関数・メソッドレベルで境界防御
  - 利用時には管理された単位で境界防御
    - アプリケーションの入出力＋縦深・多層防御

利用可能なセキュリティ標準・ガイドライン等

- ISO/JIS
- CWE/CAPEC
- PCI DSS
- NIST
- CERT Secure Coding Standard
- CWE/SANS TOP 25
- OWASP GUIDE
- CMMI
- SAMM
- NISC（内閣サイバーセキュリティセンター）
- 経産省
- 総務省
- IPA
  - 前述の通り、問題もある

ソフトウェアの運用まで考える

- **ソフトウェアは危殆化する**
  - 時間と共にセキュリティレベルが低下する
  - 新たな脆弱性・攻撃手法の発見・開発
  - 新たな機能の追加により脆弱化（例：HTML5）
  - 標準的なセキュリティ対策の進化（例：多要素認証、暗号の利用）
- **ソフトウェアは非常に複雑でありバグ（ミス）の根絶は困難**
  - 簡単に根絶できるならブラウザやそのプラグインの脆弱性はとっくに根絶
- **これらすべてを「開発者」の責任にはできない**
  - つまり運用段階でコストをかけて対応する必要がある

まとめ

ITセキュリティ対策の基本は簡単

- セキュリティの9原則
  - 認識、責任、対応、倫理、民主主義、リスクアセスメント、セキュリティの設計及び実装、セキュリティマネジメント、再評価

- セキュリティの基本概念
  - リスク認識、境界防御、縦深・多層防御、分割と統治、ホワイトリスト、レビューと改善

- **セキュリティ対策の本質はマネジメント**
  - マネジメントのコミットメント、継続的改善、PDCA
  - 目標は「セキュリティ文化の確立」

手段の目的化に注意

- 個々のITセキュリティ管理策は「手段」であり「目的」ではない

ITセキュリティ対策の目的は

ITシステムを許容範囲内のリスクで利用する！

経営者・管理者層の責任

- 組織および関係者の「認識」「責任」「対応」、その他を確実にする

経営者・管理者の責任は

組織及び関係者に原則を周知徹底させるマネジメントの実施！

ITセキュリティ管理策は現代企業の必須要素

- 人事管理、品質管理と同様にITセキュリティ管理は企業活動において「追加の管理項目」ではない

ITセキュリティ管理の不備は事業の存続にさえ関わる

ITセキュリティ管理は他人任せにできない！

知っている人に任せておく、は通用しない