サイバーセキュリティリーダー養成講座

セキュリティとリスクマネジメント

2017年11月20日
会津大学

2017年12月4日
ビッグパレットふくしま

中村章人
会津大学
nakamura@u-aizu.ac.jp

講義の目的

企業における
情報セキュリティとリスクマネジメントの強化
を顧客・消費者保護につなげるための手法等

講義の内容

1. 不正アクセス等の状況
   - 統計、事例等
2. なぜ被害がなくならないのか？
   - 防御側の不利、環境の変化、人の特性
3. セキュリティ管理の考え方と取り組み方
   - 問題のとらえ方、実施方法の具体化
   - 技術以外の対策手段
4. サイバーレジリエンスという考え方
5. まとめ

不正アクセス等の状況（統計、事例等）

- 情報漏えい
- 不正アクセス
  - システムを利用する者が、その者に与えられた権限によって許された行為以外の行為を（ネットワークを介して）意図的に行うこと
- マルウェア、ランサムウェア
  - 悪意を持って作成された、望まない結果をもたらすプログラム
  - ファイルを暗号化し、身代金を要求するマルウェア
- DoS/DDoS攻撃
  - サービス妨害（Denial-of-Service: DoS）攻撃。正当なサービスの利用を妨げる
- 現実世界への影響
- 特殊詐欺、ビジネスメール詐欺
  - 業務上のメールを利用する詐欺

情報漏えい事故（日本）

JTB（2016年6月）

- 標的型メールによる遠隔操作ウイルスで顧客情報が漏えい（最大793万件※1）
- 行政からの調査指示、海外からの渡航者が一時的に減少？

※1 後日、679万人に修正

日本年金機構（2015年5月）

- 標的型メールによる遠隔操作ウイルスで年金加入者情報が漏えい（約125万件）
- 基礎年金番号・手帳・証書の再発行、マイナンバーの利用開始を延期

ベネッセ（2014年7月）

- 委託企業の社員が顧客情報を漏えい（約3,500万件）
- おわびの手紙と金券（500円）

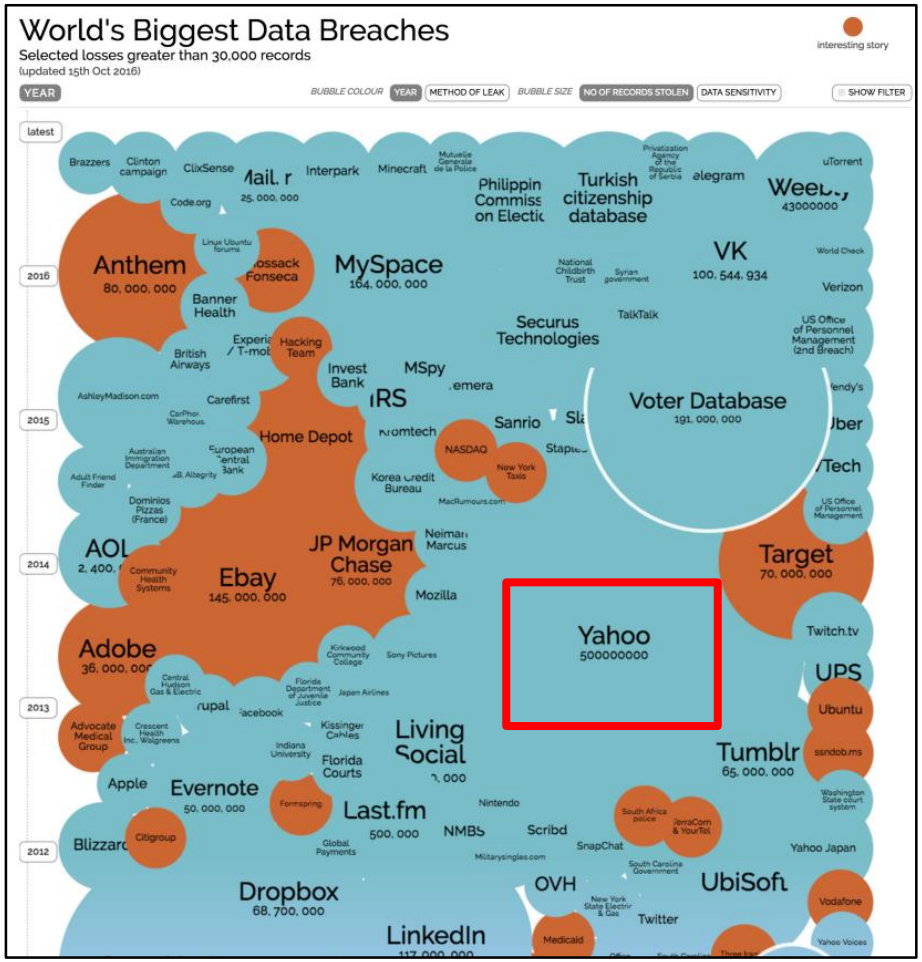
※2 現ソニー・インタラクティブエンタテインメント

ソニー・コンピュータエンタテインメント※2（2011年4月）

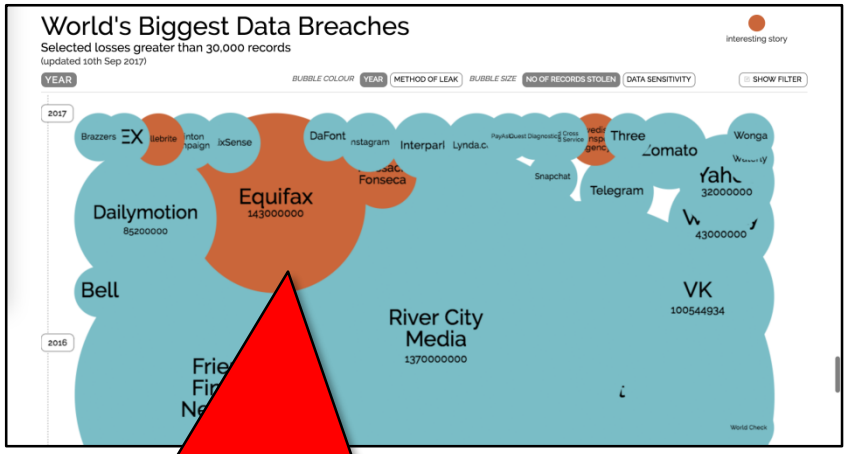
- PlayStation NetworkとQriocityの不正アクセスでユーザ情報が漏えい（最大約7,700万件）
- 行政指導（日本）、議会公聴会で幹部の証言（米国）
- 全ユーザーに対して、コンテンツやサービスの無料提供

情報漏えい事故（世界）

2016年12月時点



2017年9月時点



【Equifax】2017年9月7日発表
- 米国の個人信用情報機関
- 約1億4300万人の個人情報
  （氏名、社会保障番号、生年月日、住所、免許証番号）
- 20万9000人のクレジットカード番号

出典: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

不正アクセスの状況

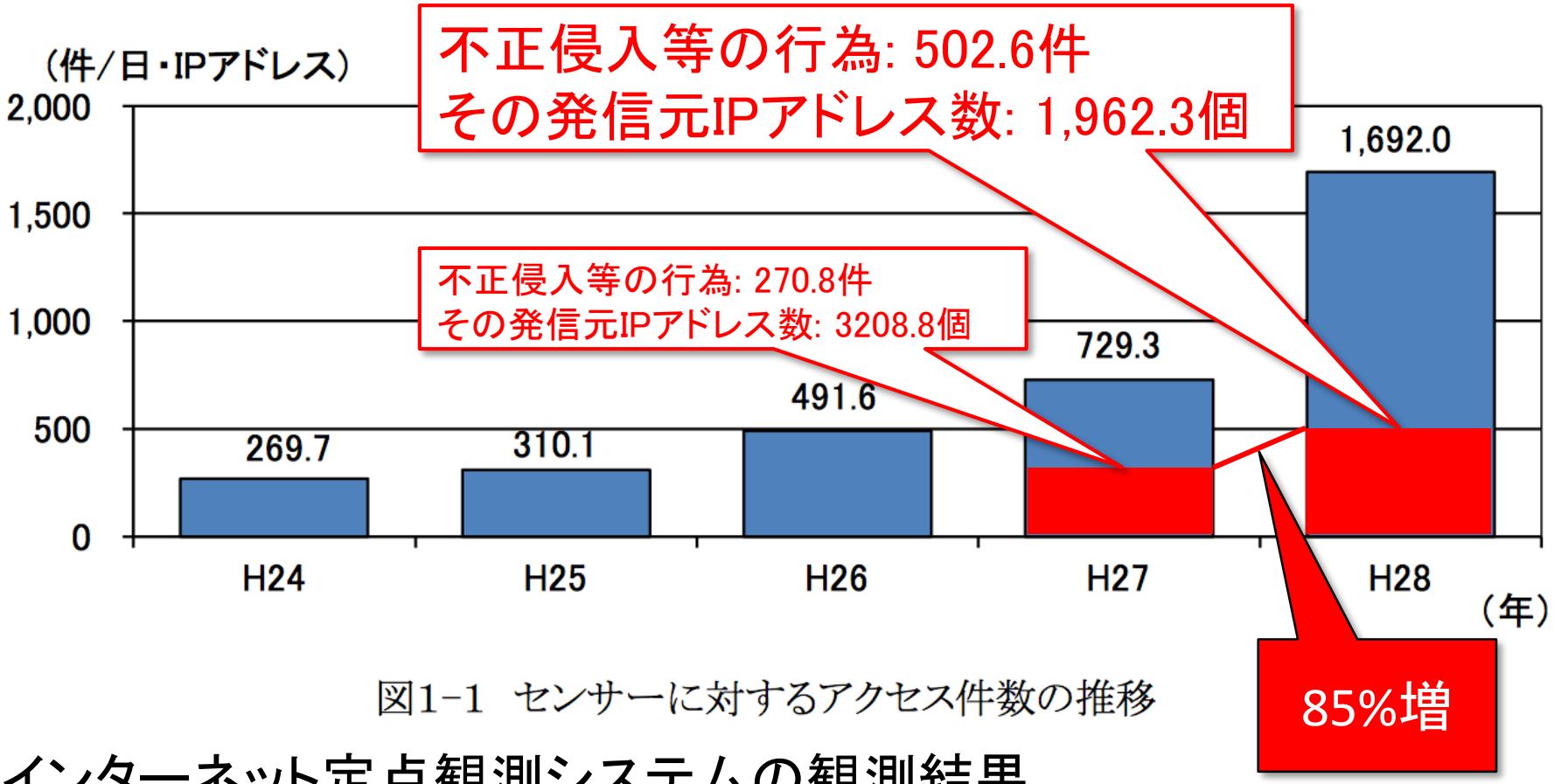
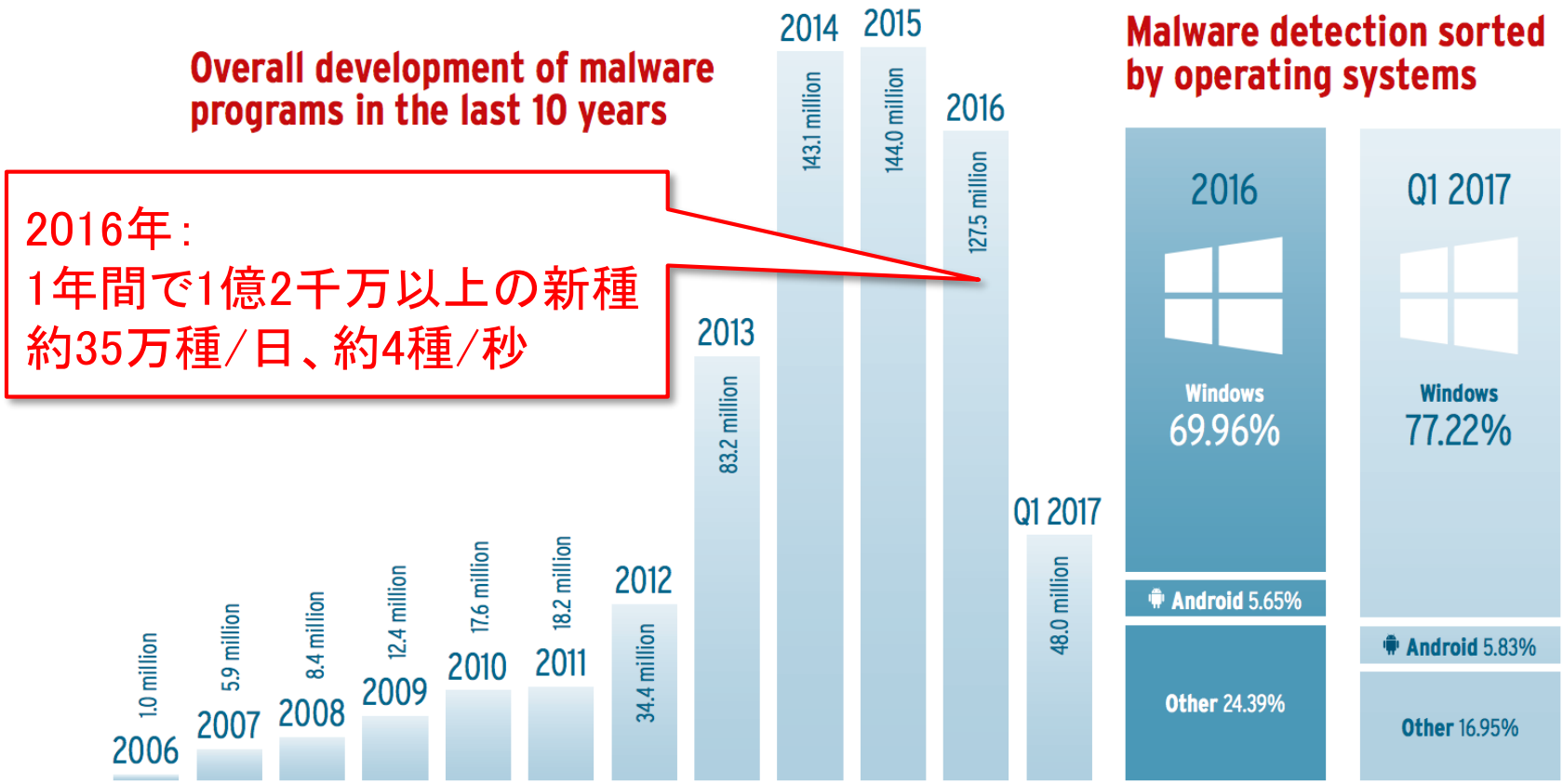


図1-1　センサーに対するアクセス件数の推移

インターネット定点観測システムの観測結果

出典: 警察庁 平成28年観測資料
https://www.npa.go.jp/cyberpolice/detect/pdf/20170323_toukei.pdf

マルウェアの状況



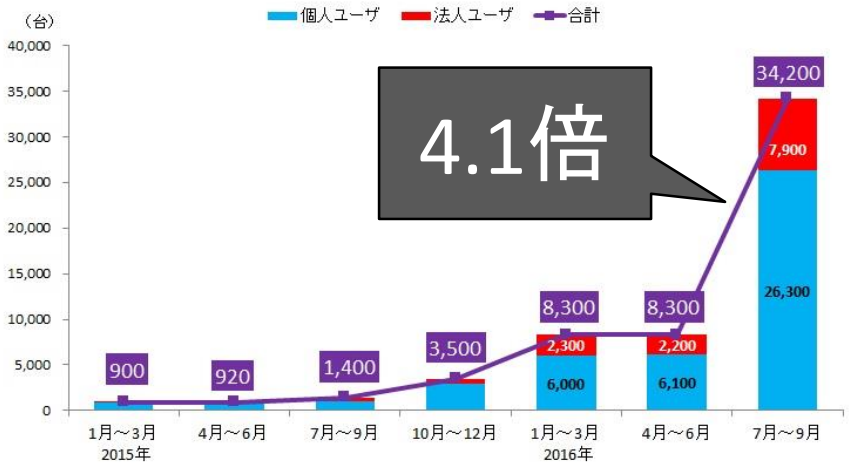
マルウェアの新種検知数

出典: Security Report 2016/17, AV-TEST GmbH

https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2016-2017.pdf

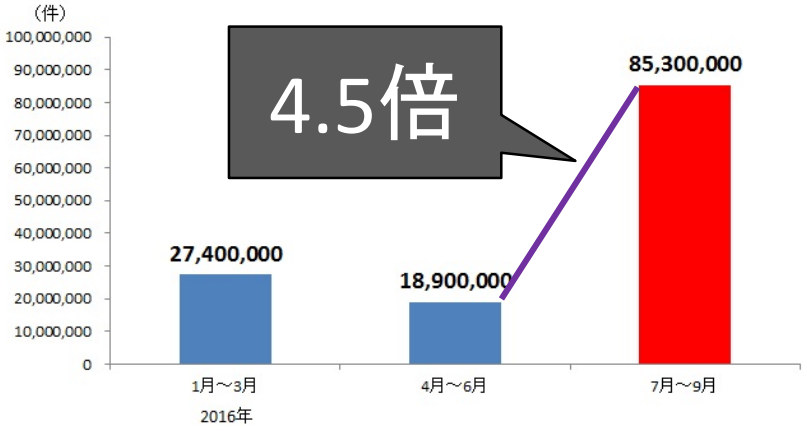
ランサムウェアの状況

ランサムウェア国内検出台数推移（日本）



2015年1月～2016年9月トレンドマイクロによる調査

ランサムウェア感染を狙った不正メールの検出数（全世界）



2016年1月～9月トレンドマイクロによる調査

※出典: http://www.trendmicro.co.jp/jp/about-us/press-releases/articles/20161115050616.html

事例: 2017年5月、WannaCryと呼ばれるランサムウェアを使った過去最大規模の一斉攻撃が発生。
--- 画像:ドイツの鉄道駅の案内板（ドイツ・ケムニッツ、5月12日）=AP

Dyn DDoS攻撃

日時
- ◆2016年10月21日
- ◆7:10 – 9:20 a.m. EDT
- ◆11:50 a.m. – 1:11 p.m. EDT
- ◆4:00 – 6:11 p.m. EDT

場所
- ◆北アメリカ
- ◆欧州

容疑者
- ◆Anonymous
- ◆New World Hackers

出典: https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

標的
- ◆Dyn社（DNSプロバイダ）

方法
- ◆DNS amp DDoS
  最大1.2 Tbps

ボットネット
- ◆マルウェアMiraiに感染した
  IoTデバイス（監視カメラや
  ビデオレコーダー）

影響を受けたサービス

DDoS攻撃の不都合な真実

サービスとしてのDDoS

- DDoS攻撃を闇市場で購入できる

脅迫の道具としてのDDoS

- DDoSの脅威を使って脅迫する

現実世界への影響

自動車

◆安全装備の無効化、自動運転ののっとり
⇒ 大規模なリコール

社会インフラ

◆発電・送電システムへの攻撃
⇒ 停電、設備の破壊による2次被害

政治

◆情報漏えいや偽情報の流布による選挙結果への影響

経済

◆フィッシングメールや偽情報を使った株価操作

事例: ロシアが米大統領選に干渉か

ワシントンポスト 2016-12-11

- 米国中央情報局（CIA）は11日までに、ロシアがサイバー攻撃を通して米大統領選に干渉したと断定
- 大統領選前に民主党全国委員会やクリントン陣営の電子メール数千通を盗み出し、告発サイト「ウィキリークス」に流した複数の人物は、ロシア政府とつながりを持っていた

ホワイトハウス 2016-12-29

- Obama大統領は、ロシアがハッキングを行い、2016年の米大統領選に干渉したと連邦捜査官が判断したことを受け、ロシアへの制裁を発表
  - https://www.whitehouse.gov/the-press-office/2016/12/29/statement-president-actions-response-russian-malicious-cyber-activity

事例: ウクライナの停電 2年連続

2015年12月23日

- 変電所への攻撃
- 数時間の停電
- 約22万人に影響
- マルウェア BlackEnergy Trojan
- ロシア政府による攻撃か？
  - http://wired.jp/2016/01/07/cyberattack-power-electricity/

2016年12月17日

- 変電所への攻撃
- 30分程度の停電
  - http://wired.jp/2017/01/14/hacking-ukraine-power/

不正アクセス vs. 特殊詐欺

約16.9億円（前年30.7）

- ◆ インターネットバンキングの不正送金被害額
- ◆ 2016年/H28
- ◆ 警察庁「平成28年中におけるサイバー空間をめぐる脅威の情勢について」
  - https://www.npa.go.jp/publications/statistics/cybersecurity/data/H28cyber_jousei.pdf
    （参照: 2017-08-25）
- ◆ 件数、被害額ともに減少※1

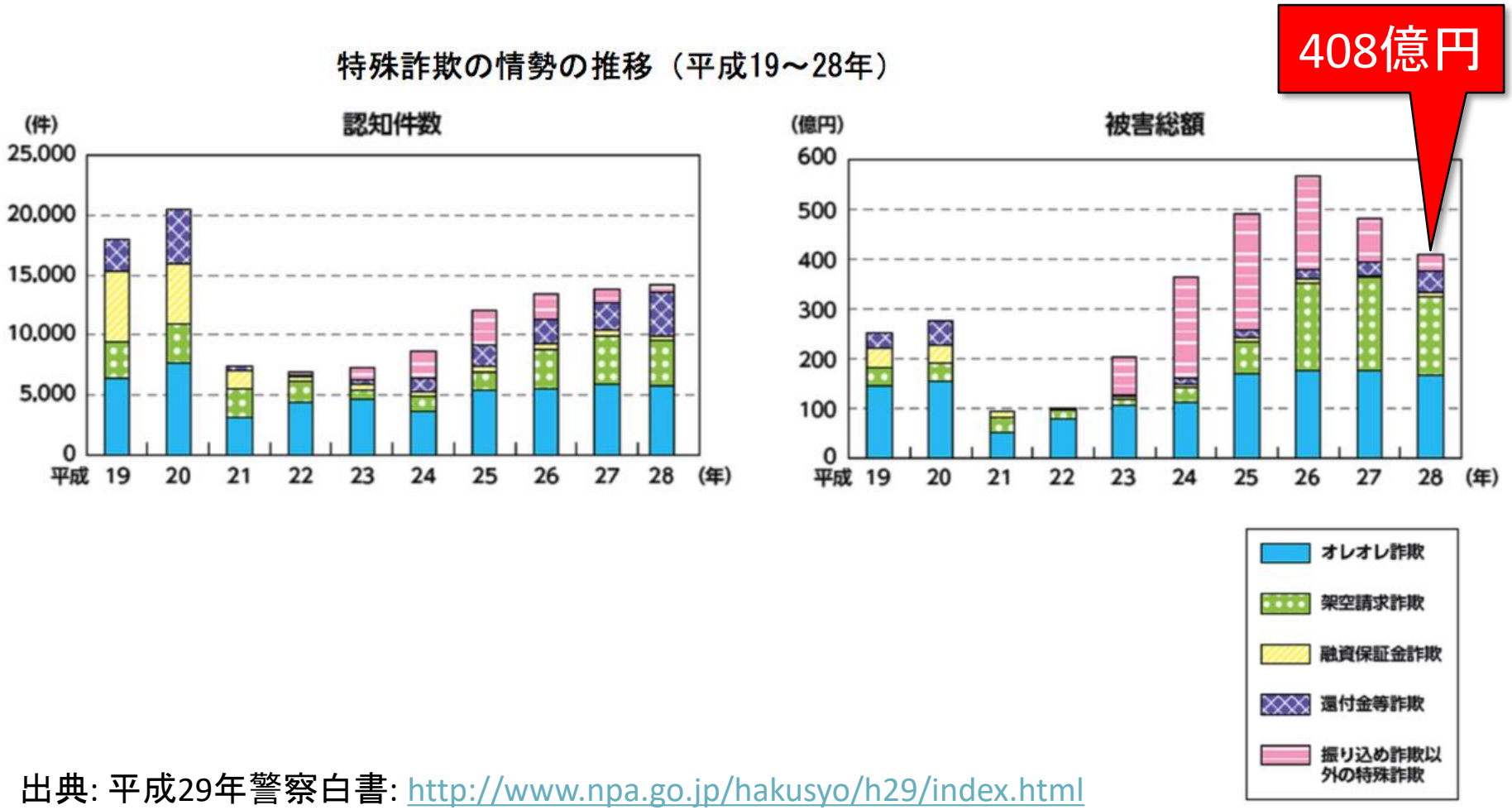
約408億円（前年482）

- ◆ 特殊詐欺※2の被害額
- ◆ 2016年/H28
- ◆ 警察庁「平成28年の特殊詐欺認知・検挙状況等について」
  - https://www.npa.go.jp/bureau/criminal/souni/tokusyusagi/hurikomesagi_toukei2016.pdf
    （参照: 2017-08-25）
- ◆ 件数微増、被害額減少

※1 被害者の多くはセキュリティ対策（ワンタイムパスワード、電子証明書など）を未実施であった。
標的: メガバンク/個人口座 → 地方銀行 → 信金 ⇒ 法人口座

※2 特殊詐欺とは、不特定の者に対して、対面することなく、電話その他の通信手段を用いて行う詐欺。なりすまし詐欺、還付金詐欺、架空請求詐欺、融資保証金詐欺を合わせて「振り込め詐欺」という。

特殊詐欺の情勢

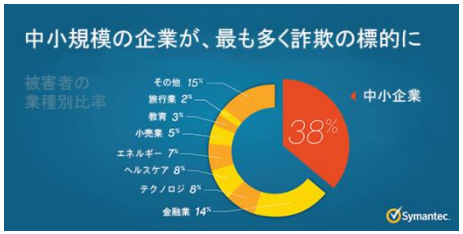


出典: 平成29年警察白書: http://www.npa.go.jp/hakusyo/h29/index.html

新手の詐欺: ビジネスメール詐欺(1/2)

Business Email Compromise (BEC) Scam

- ◆ 業務上のメールを利用する詐欺(高度な振り込め詐欺)
- ◆ FBIによる注意喚起(2016年6月)
  - 累積(過去3年)被害者数: 約2.2万、被害額: 約30億ドル



手口(例)

- ◆【事前調査】役職、業務内容、スケジュール
- ◆【メール:社長→経理】今度、業務提携の打合せに出張する。
  その場で契約するかもしれない。たぶん300万円くらい。
  .....
- ◆【メール:社長→経理】今出先だが、この前話した業務提携の件で、
  至急この口座に200万円送金してくれ。
- ◆【メール:経理→社長】承知しました、すぐに処理します。
  .....
- ◆【経理→社長】先日の契約の領収書が届かないのですが...
- ◆【社長→経理】何の契約?

参考: https://www.ic3.gov/media/2016/160614.aspx
画像: https://www.symantec.com/connect/ja/blogs/bec-0

新手の詐欺: ビジネスメール詐欺(2/2)

手口

- 不正アクセスによる、事前の綿密な調査
- 社長等の管理職、弁護士、取引先、顧客などを装う
  - 送金の指示、振込先の変更
- 出張や緊急などの状況設定で、直接確認を避ける

対策

- メールでの指示に対し、電話などで直接確認
- 不特定多数からの問合せメールを担当する機器の厳格なセキュリティ設定

※ 他に、宅配業者を装う配送連絡メール、顧客を装う商品問合せメールなどの手口がある。

なぜ被害がなくならないのか？（セキュリティ管理の難しさ）

- 防御側の不利、攻撃側の有利
- 環境の変化
- 人の特性

防御側の不利、攻撃側の有利

	防御側	攻撃側
経路	可能性のすべて	どこか1点
知識	既知の攻撃	ゼロデイ
タイミング	常に（24h/7d）	好きな時に
性質	ルールに従う	ずるい、汚い

参考: *Writing Secure Code, 2nd ed.,* by Michael Howard and David LeBlanc, Microsoft Press, ISBN-13: 978-0735617223, 2002.

対策をむずかしくする環境の変化

【ITシステム】

◆オンプレミス ⟶ Web ⟶ クラウド ⟶ IoT

【サイバー攻撃】

◆目的: 自己顕示 ⟶ 思想・信条 ⟶ 金銭

◆マルウェア: 単体 ⟶ Web・MITB ⟶ ボットネット

◆属性: 機密性・完全性 ⟶ 可用性

- 【例】DDoS、ランサムウェア

◆ターゲット: IT（サイバー空間） ⟶ 人・もの（実世界）

- 【例】不正送金、ビジネスメール詐欺、自動車の制御

根本的な対策が難しい攻撃

正規サイトの改ざん

- ◆例: Gumblar

表面上に変化を見せないマルウェア

- ◆例: 不正送金マルウェア（MITB）

標的型攻撃、フィッシング

- ◆例: 巧妙なメールと添付ファイル

可用性を侵害するDoS攻撃

- ◆例: Dyn DDoS攻撃

人の特性による被害の拡大

即応性

⇐ 若者

- すぐに応答・返事をしてしまう
  - スマフォを常に使用することが日常化している
- すぐに応答・返事をしないと、嫌われる
  - ネットでのつながりと、リアルのつながりが同等の価値をもつ

まじめ、すなお

⇐ 若者・高齢者

- 相手が間違っていると思って、連絡してしまう
- 自分が間違っていると思って、相手に従ってしまう

面倒くさがり

⇐ だれでも

- 楽な方に流れる

推測しやすいパスワード

RANK	PASSWORD
1.	123456
2.	123456789
3.	qwerty
4.	12345678
5.	111111
6.	1234567890
7.	1234567
8.	password
9.	123123
10.	987654321

約17%

6文字以下

11.	qwertyuiop
12.	mynoob
13.	123321
14.	666666
15.	18atcskd2w
16.	7777777
17.	1q2w3e4r
18.	654321
19.	555555
20.	3rjs1la7qe
21.	google
22.	1q2w3e4r5t
23.	123qwe
24.	zxcvbnm
25.	1q2w3e

- Keeper Security社調査
- 2016年度に漏えいした約1000万件のデータを調査
  - https://blog.keepersecurity.com/2017/01/13/most-common-passwords-of-2016-research-study/

面倒くさい！
覚えられない！

ソーシャルエンジニアリングとは？

攻撃の1種

- 人間の心理的な隙を突き、攻撃者の意図した行為を取るように標的（人）を誘導する行為

狭義では

- 不正アクセスのために、
  人を騙してIDやパスワードなどを獲得する行為

  ⇒ なりすまし

- または、人の行動から目的の情報を探り出す行為

なぜソーシャルエンジニアリングか？

ITの脆弱性を突くよりも人を騙す方が容易

- 騙されることに対する免疫の不足

攻撃者の候補数が多い

- 攻撃の手段・経路が多様
  - 例: 電話（高度なハッキングスキル/ツールは不要）
  - 例: キーボード入力や付箋の盗み見、ゴミ漁り
- 動機が多様
  - 例: ストーカー、復讐、金銭

成功事例

- 振り込め詐欺、ビジネスメール詐欺
- LINEのなりすましによる電子通貨の購入詐欺

セキュリティ管理の考え方と取り組み方

- サイバーセキュリティは経営問題
- 実施方法の具体化
- 技術以外の対策手段

セキュリティ管理のテーマ

テーマ	主な実施内容
経営	経営者がセキュリティを最優先する姿勢を明らかにする
人材	セキュリティ対策・リスク管理の担当者を置く
教育	セキュリティについて関係者に教育する
実践	情報資産を洗い出し、脅威・リスクを分析する インシデント発生時の被害の広がりを予想する セキュリティ対策に有効なツールを導入する
監査	セキュリティ対策について外部の目で監査をする

サイバーセキュリティは経営問題

「サイバーセキュリティ経営ガイドライン」

◆経済産業省, Ver 1.0, 2015年12月

- http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

◆想定読者: 最高経営責任者（CEO）

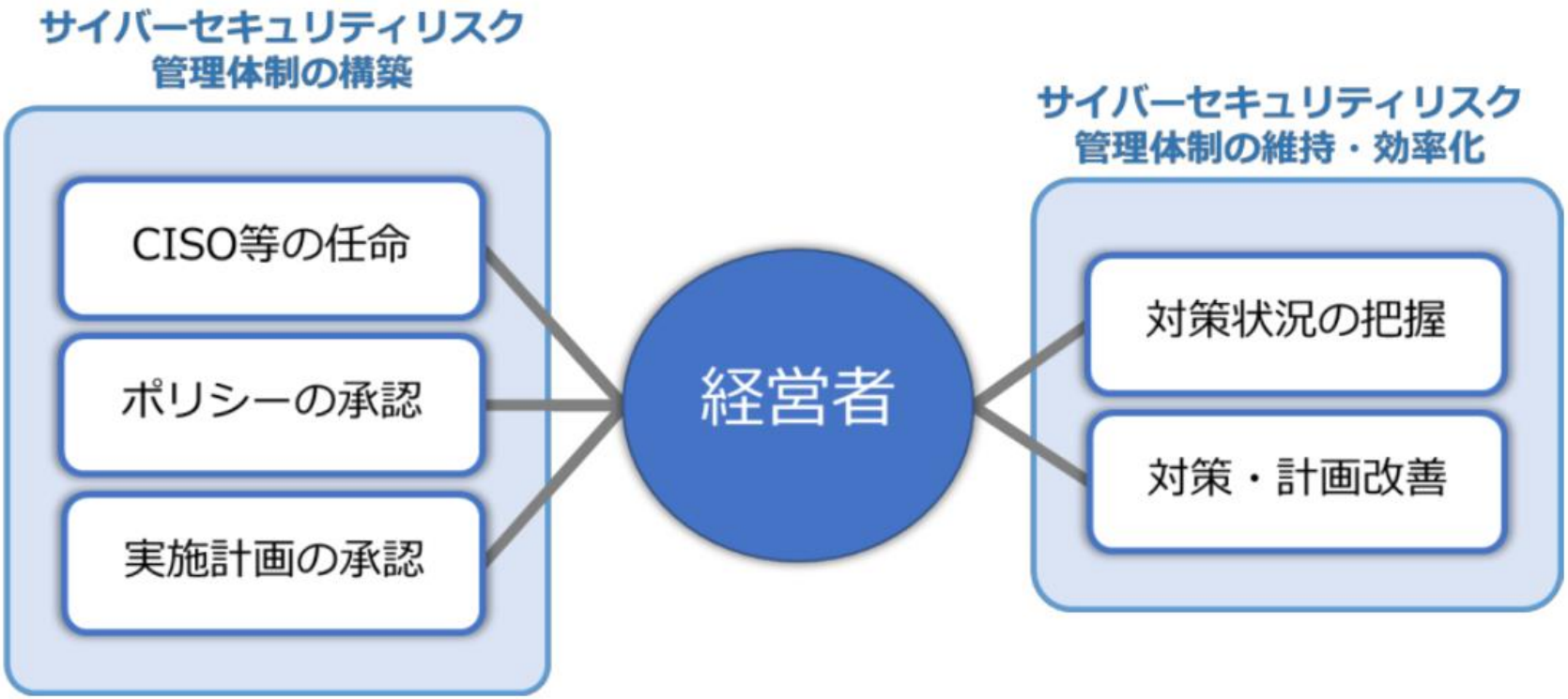
◆3原則（基本的な考え方）

① 【経営者のリーダーシップ】
経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要

② 【自社以外（ビジネスパートナー等）にも配慮】
自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を含めたセキュリティ対策が必要

③ 【平時からのコミュニケーションと情報共有】
平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

経営者が決定すべきこと



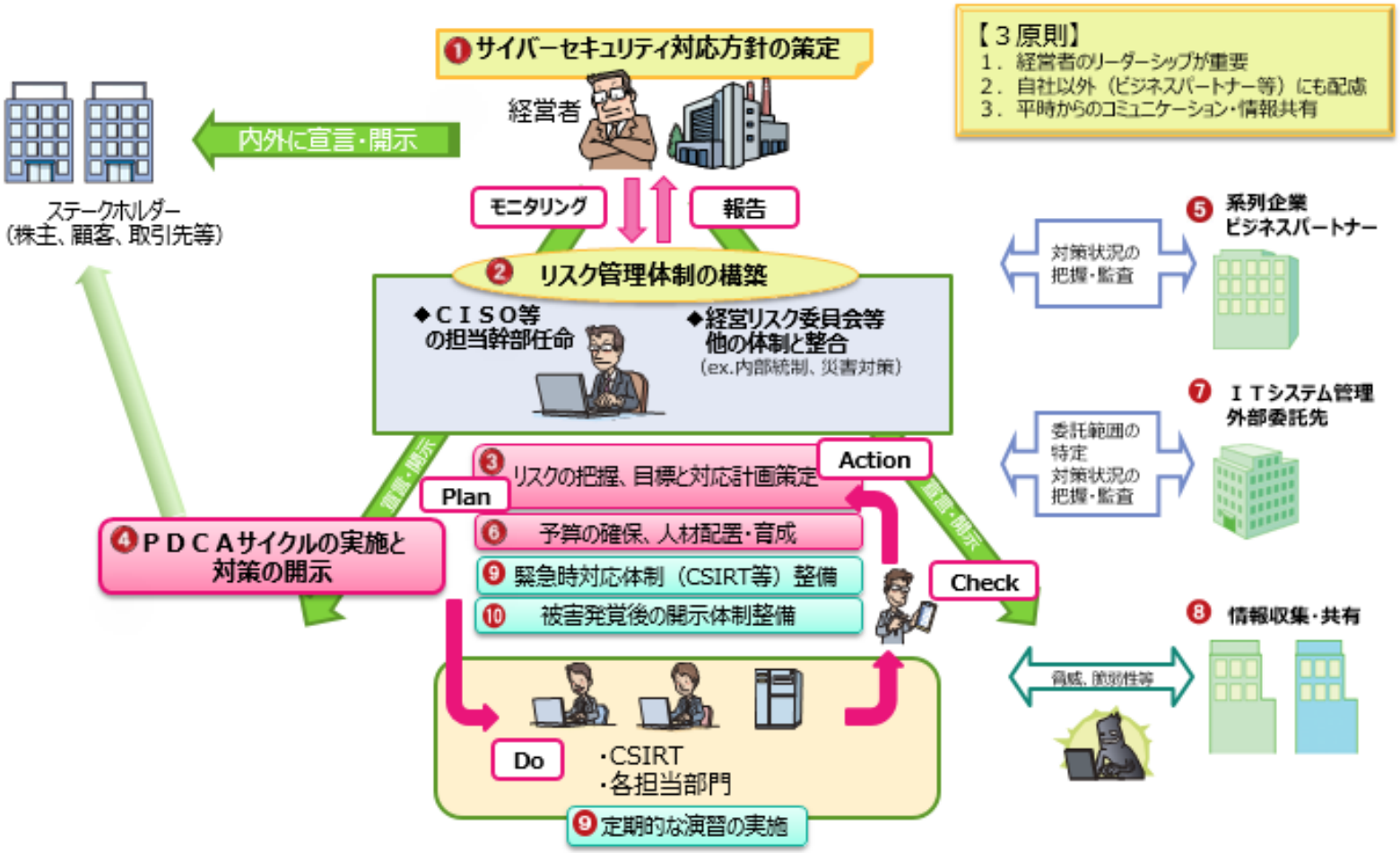
※ 画像出典: サイバーセキュリティ経営ガイドライン解説書, Ver.1, 2016年12月

経営ガイドラインの具体化方法

「サイバーセキュリティ経営ガイドライン解説書」

- ◆IPA, Ver.1, 2016年12月
  - https://www.ipa.go.jp/security/economics/csmgl-kaisetsusho.html
- ◆想定読者: 最高情報セキュリティ責任者（CISO）
- ◆ガイドラインの補足と、実施方法の具体化
  - 対策実施手順、検討のポイントなど

経営ガイドラインの具体化: 重要10項目（1/2）



※ 画像出典: サイバーセキュリティ経営ガイドライン解説書, Ver.1, 2016年12月

経営ガイドラインの具体化: 重要10項目（2/2）

1. サイバーセキュリティ対応方針の策定
2. リスク管理体制の構築
3. リスクの把握、目標と対応計画策定
4. PDCAサイクルの実施と対策の開示
5. 系列企業・ビジネスパートナーの対策実施及び状況把握
6. 予算確保・人材配置及び育成
7. ITシステム管理の外部委託
8. 情報収集と情報共有
9. 緊急時対応体制の整備と演習の実施
10. 被害発覚後の必要な情報の把握、開示体制の整備

セキュリティ管理の規格等

- 国際標準規格
  - ISO/IEC 27000シリーズ
    - ISMS適合性評価制度
  - ISO/IEC 38500（ITガバナンス）
    - 経営者対象の原理原則
- フレームワーク
  - ISMS、COBIT、他
- 補完ドキュメント
  - IPA「組織における不正行為防止ガイドライン」第3版, 2015年3月.
    - https://www.ipa.go.jp/security/fy24/reports/insider/
  - 経済産業省「情報セキュリティガバナンス確立促進事業」コンテンツ
    - http://www.meti.go.jp/policy/netsecurity/secgov.html

組織として最低限の要素を備えていることを評価・認証

オペレーションレベルにどう落とし込むか？

企業におけるセキュリティ管理の問題

セキュリティ対策は社会の要請・経営戦略

発注元の取引条件になることもしばしば

▼

ISO/IEC27001に基づくISMS第三者認証制度

担当要員の確保が必要、実務負担コストが高いという問題

中小企業には困難

▼

セキュリティ管理の省力化と具体化の方策が必要！

チェックリスト方式

セキュリティ管理を実践に移す上での
おススメのスタートポイント

- 「制御システムセキュリティ自己評価ツール(J-CLICS)」
  - JPCERT/CC, 2013年3月
    - https://www.jpcert.or.jp/ics/ics-assessment.html
  - （制御システムの）セキュリティ対策状況を把握する「チェックリスト」と、チェックリストの設問について取り組むべき具体策等がわかる解説書「設問項目ガイド」で構成
    - 「制御システム」に限らず、一般的なICTシステムにそのまま通用する

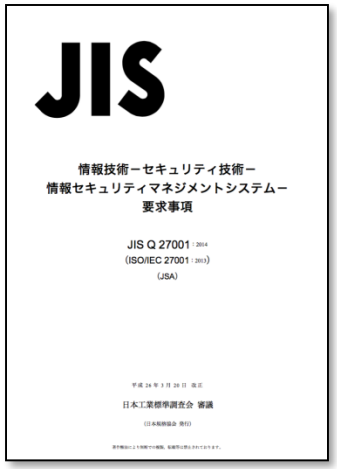
J-CLICSの構造

チェックリスト（設問）
〇×で回答

設問項目ガイド

- 背景・目的
- 想定されるリスク
- 内容解説・施策例
- 参考文献

参考文献



- JIS Q 27001

J-CLICS

チェックリスト: 2段階のレベル設定

【STEP 1（全関係者向け）】

1. 物理セキュリティ
2. 機器接続手順
3. パスワードとアカウント
4. 対応能力の確立
5. サードパーティリスクの管理
6. 継続的な評価と改善

【STEP 2（技術担当者向け）】

1. システムとビジネスリスクの理解
2. 脅威の理解
3. ネットワークアーキテクチャ
4. ファイアウォール
5. システム監視
6. ウイルス対策
7. セキュリティパッチ
8. システムの強化
9. バックアップと回復
10. 転入者と転出者用のプロセス

STEP1: 合計11問
STEP2: 合計10問

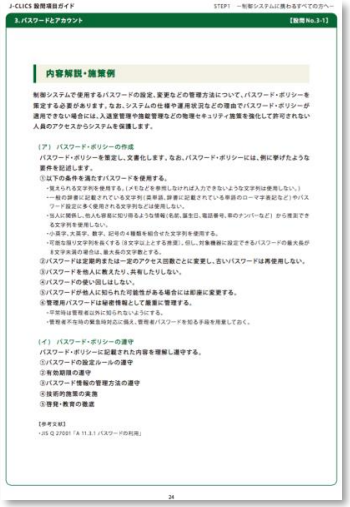
例1: パスワード

チェックリスト（設問）

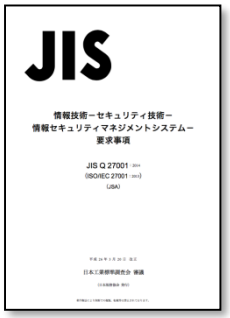
下記の設問に、「○」または「×」でお答えください。

NO		設問	○／×	設問項目ガイド対応ページ
		パスワードとアカウント		
3	1	制御システムのパスワードの強度と有効期限を含むパスワード・ポリシーがありますか？		P.23
	2	強力なパスワード※3を使用していますか？		P.25
	3	制御システムのパスワードを定期的に変更していますか？		P.27

設問項目ガイド



参考文献



- JIS Q 27001「A 11.3.1 パスワードの利用」

例1: パスワード(設問ガイド)

設問

背景・目的

想定されるリスク

内容解説・施策例

【参考文献】
- JIS Q 27001「A 11.3.1 パスワードの利用」

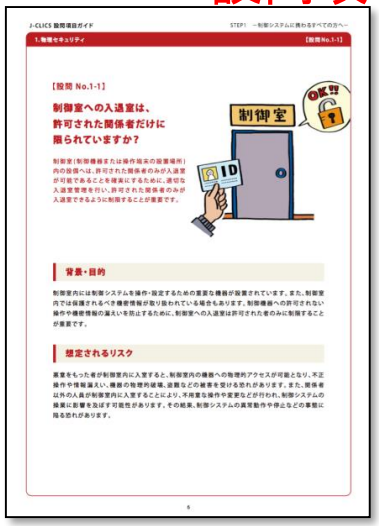
例2: 物理的セキュリティ

チェックリスト（設問）

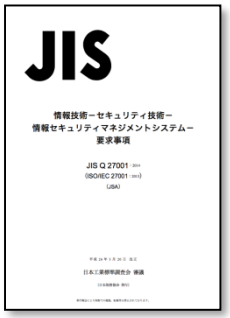
下記の設問に、「○」または「×」でお答えください。

NO		設問	○／×	設問項目ガイド対応ページ
		物理的セキュリティ		
1	1	制御室※1への入退室は、許可された関係者だけに限られていますか？		P.6
	2	制御室※1への訪問者には、常に関係者が付き添っていますか？		P.8
	3	制御室※1への入退室管理(記録と管理者による定期的な確認)を行っていますか？		P.10

設問項目ガイド



参考文献



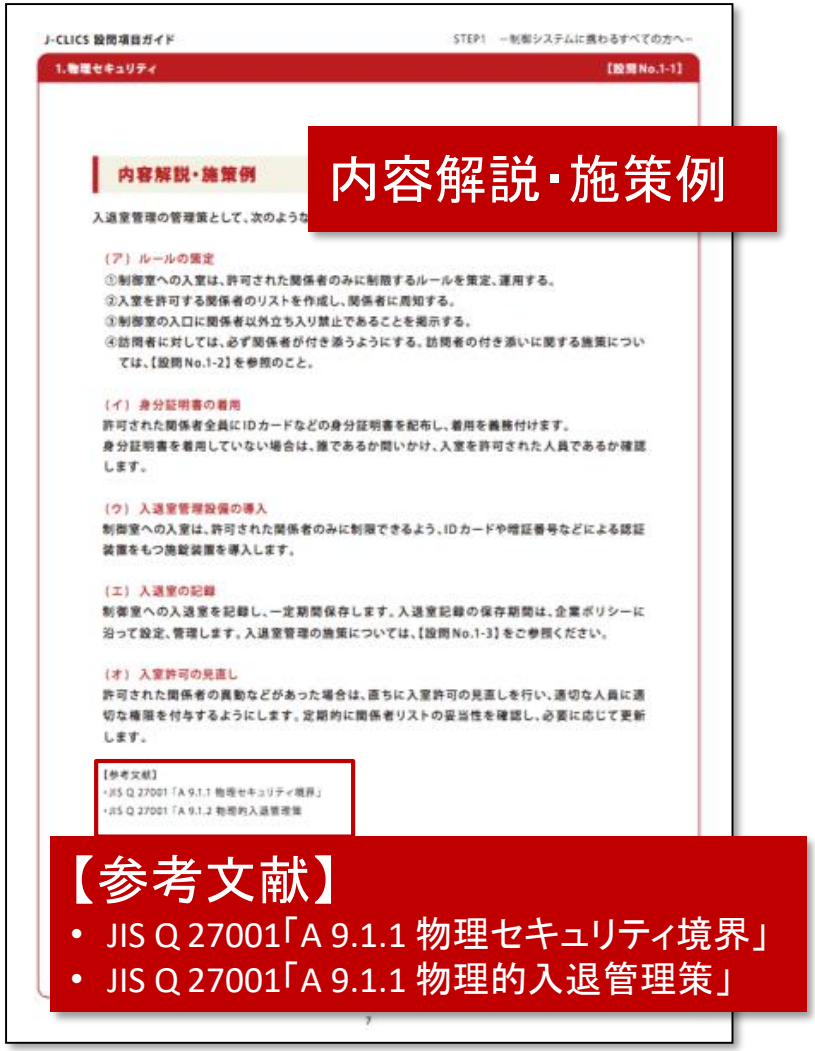
- JIS Q 27001「A 9.1.1 物理セキュリティ境界」
- JIS Q 27001「A 9.1.1 物理的入退管理策」

例2: 物理的セキュリティの設問ガイド

設問

背景・目的

想定されるリスク



内容解説・施策例

【参考文献】
- JIS Q 27001「A 9.1.1 物理セキュリティ境界」
- JIS Q 27001「A 9.1.1 物理的入退管理策」

リスク対応（1/2）

資産の価値 x 損害の程度 x 脅威の深刻さ

限られた資源
（時間、資金、能力）

↓

防御の優先付けと
コントロール（対策手段）の選択

リスク対応（2/2）

100%の解決は困難！

セキュリティ対策の限界

コントロール（対策手段）は、必ずしも
期待した効果を発揮するとは限らない

完璧なコントロールは存在しない

▼

事後対応や回復手段も必要

これまでのセキュリティ管理で注目されてこなかったポイント

ランサムウェアの被害拡大で再認識

「サイバーレジリエンス」という考え方

- ◆ レジリエンスとは？
- ◆ サイバーセキュリティからサイバーレジリエンスへ
- ◆ バックアップ再考

※ 会津大学「サイバー攻撃対策演習・情報セキュリティ講座（2016年度、2017年度）」で技術的側面について講演

レジリエンス（Resilience）とは？

心理学の用語

◆精神的な回復力、復元力、耐久力などの意

◆「脆弱性」の反対の概念

- シェリル・サンドバーグ, アダム・グラント, "OPTION B(オプションB) 逆境、レジリエンス、そして喜び", 日本経済新聞出版社, 2017年, ISBN-13:978-4532321598.

経済・経営学への転用

– 危機に直面し経営環境が変わっても、柔軟に対応して回復する力がある企業

- ピーター・D・ピーダーセン, "レジリエント・カンパニー なぜあの企業は時代を超えて勝ち残ったのか", 東洋経済新報社, 2014年, ISBN-13:978-4492557549.
  – 【例】ネスレ、P&G、ユニリーバ、GE

サイバーレジリエンス

サイバーセキュリティ から

サイバーレジリエンス へ

- レジリエンス（resilience）: 回復力、復元力の意
- 予防的対策による100%の防御は不可能
- バックアップや復旧までを含む事後対策が重要

  【例】ランサムウェアによるファイル暗号化

  ⇒ バックアップからのデータ復元

インシデントレスポンス（IR）

（コンピュータセキュリティ）インシデントとは？

- コンピュータセキュリティに関係する人為的事象で、意図的および偶発的なもの（疑いがあるものを含む）

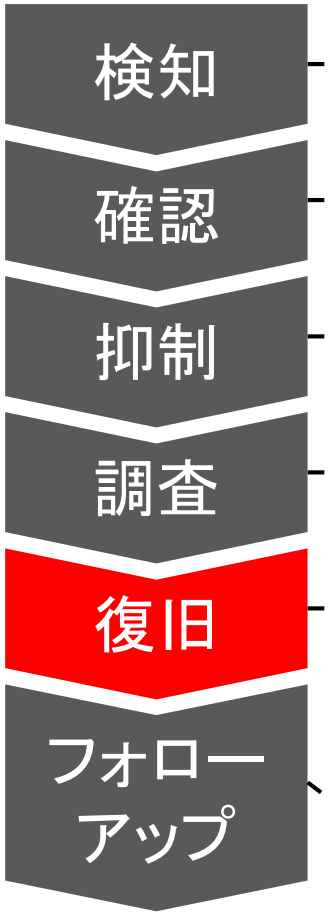
IRとは？

- インシデントに対し、脅威を排除し、損害を最小限に抑え、速やかに通常業務を回復させること

なぜIRが必要か？

- 100%の対策は不可能、またはコストに見合わない
  ⇒ 受容リスクや想定外インシデントには
  IRで対応（つまり事後対策）！

IRにおける復旧フェーズ



インシデントの可能性を検知

本当にインシデントかどうかを判定

発生している被害の抑え込み

根本原因と復旧に必要な情報とを調査

システム、データ、ビジネスの復旧
- システムの再構築
- データの復旧
- 関係者への報告

再発防止策の検討・実施、IRの見直し

サイバーレジリエンスのポイント

システムを復旧できるか？

- 再現可能な自動化されたシステム構築・設定手順
- クラウド、マイグレーション

データを復旧できるか？

- 適切なバックアップ
- ポータビリティ

ビジネスを元通り継続できるか？

- 迅速な経営判断、広報、顧客対応
- フォローアップ

バックアップ再考

【目的】

- 古くは
  - ◆故障リスクの対策
  - ◆システムの信頼性が低かった
- 今は
  - ◆セキュリティリスクの対策
  - ◆いつか起こるインシデントからの復旧手段
    - 【例】ランサムウェア

【ルール】３－２－１

- ３個（以上）のコピーを保存する
- ２種類（以上）のメディアに保存する

  【例】USBメモリとクラウド

  一つはオフラインに
- １個（以上）は他と離れた場所に置く

  【例】自宅とオフィス

まとめ

後を絶たないインシデント

- ◆インシデント（事故、犯罪）のインパクトは大きい
- ◆ITだけが攻撃の経路ではない（人間こそ弱点）

セキュリティ管理

- ◆経営問題と捉える
- ◆行動（対策実施）を具体化する（ツールの活用）
- ◆技術以外の対策方法も考慮する

レジリエンスという考え方

- ◆インシデント前提で備え、業務を元に戻せる力を養う