効率的かつ効果的なCSIRT運営へ

管理者,利用者ともに負担軽減を目指したCSIRT運営の可能性について

島根大学CSIRTメンバー
松本多恵

2018年8月31日

講習内容

1. 差止めなく進化していくサイバー攻撃
2. CSIRTの役割
3. CSIRTの課題（人間の弱点を狙う脅威）
4. CSIRTの課題（人材不足）
5. CSIRTの課題（予算面）
6. どうすれば利用者の利便性とセキュリティを担保できるのか
7. 情報セキュリティ教育
8. まとめ

差止めなく進化していくサイバー攻撃

昨日まで安全だったものが今日は危ない！

サイバーセキュリティ上の脅威の巧妙化･高度化

愉快犯
自己顕示,見せしめ,嫌がらせなどが目的

目立つ攻撃
すぐに攻撃に気づき,対策を講じることができる

攻撃手法の巧妙化

目立たない攻撃
攻撃の発覚が遅れるため,被害の拡大長期化

2000年

2000年1月24日科学技術庁（現･文部科学省）のホームページが不正に書換,総務省統計局のホームページで公開中の国勢調査などのデータが消去

不正アクセス禁止法施行（2000年2月13日）

2005年

2004年頃から個人情報やクレジットカード情報を狙ったサイバー攻撃
2005年データに不正アクセスを行い,個人情報を盗み出す

2008年コンフィッカーと呼ばれるUSBメモリ経由で観戦するコンピュータウイルス流行

2010年以降

2013年Webサイトの改ざん総件数7,726, 2014年3,664件,2015年3,335件,2016年3,274件と徐々に減少

サイバーセキュリティ基本法（2014年10月21日）

2017年5月世界で猛威を振るった「Wanna Cryptor」と呼ばれる身代金要求ランサムウェア

2017年
- ビジネスメール詐欺
- 仮想通貨の流出
- DDoS攻撃

情報セキュリティ対策とは

何を守るのか

情報資産

何から守るのか

情報セキュリティの脅威

外部脅威
内部脅威

どのように守るのか

技術的な対策
ウイルス対策ソフト
ファイアウォール

物理的な対策
バイトメトリクス認証
入退管理
災害対策

人的な対策
従業員、構成員の情報セキュリティ教育
CSIRTメンバーの教育

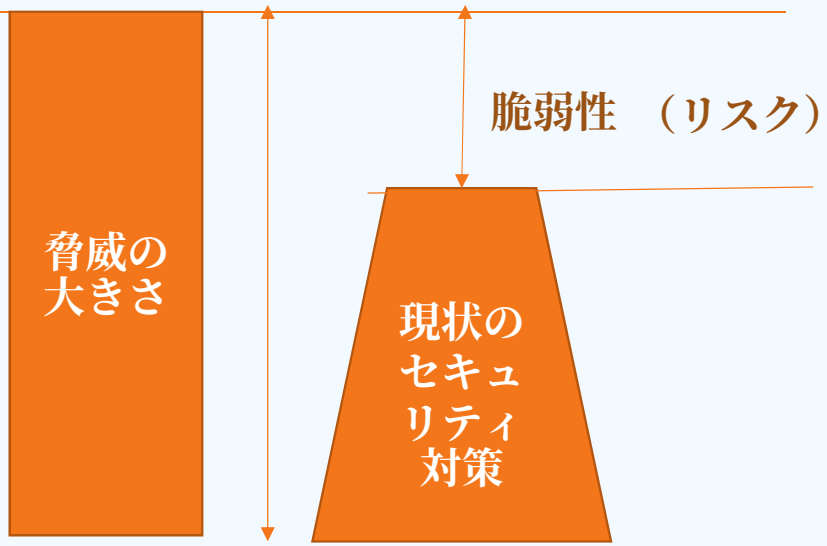
組織的な対策
情報セキュリティポリシーの策定
個人情報保護法
CSIRT等の構築

リスクの管理

脅威とは
システムまた組織に危害を与える,好ましくない偶発的事故の顕在的な原因

脅威基準値（脅威が発生すると）
（小）大きな問題にならないが,
今後の対策が重要になる可能性がある
（中）問題になる
（大）深刻な問題となる

脅威の種類	脅威の例
人（偶発的）	メール誤送信、ファイルの削除、書類の紛失,パソコンスマートフォンの破損, 意図しないウイルス感染
人（意図的）	データ改ざん、ID等の不正取得　なりすまし
環境的	地震、津波、火災等の自然災害、サーバ等の経年劣化による不備　アップデート等の不備



脆弱性の基準値
（低）現状は，脅威に対しての対策が万全
（中）現状は，対策に改善の余地あり,安全性が中位
（高）大きなセキュリティ上の欠陥が存在し,安全性
が欠如する状況で早急な対策が必須

情報セキュリティ事故（個人情報漏えいなど）が組織に与える影響

個人情報, 機密情報,知的財産, 営業秘密,社内文書, 社内システム情報,顧客情報, 個人情報など重要な情報資産が脅かされる事故が多発

- 金銭的な被害
- ブランドの失墜
- 責任者の進退問題
- サービス・業務の停止

サイバーセキュリティ対策は,経営上の課題へ

① 技術の問題 ⇒ 組織の問題へ
② IT部門の課題 ⇒ 組織全体の課題へ

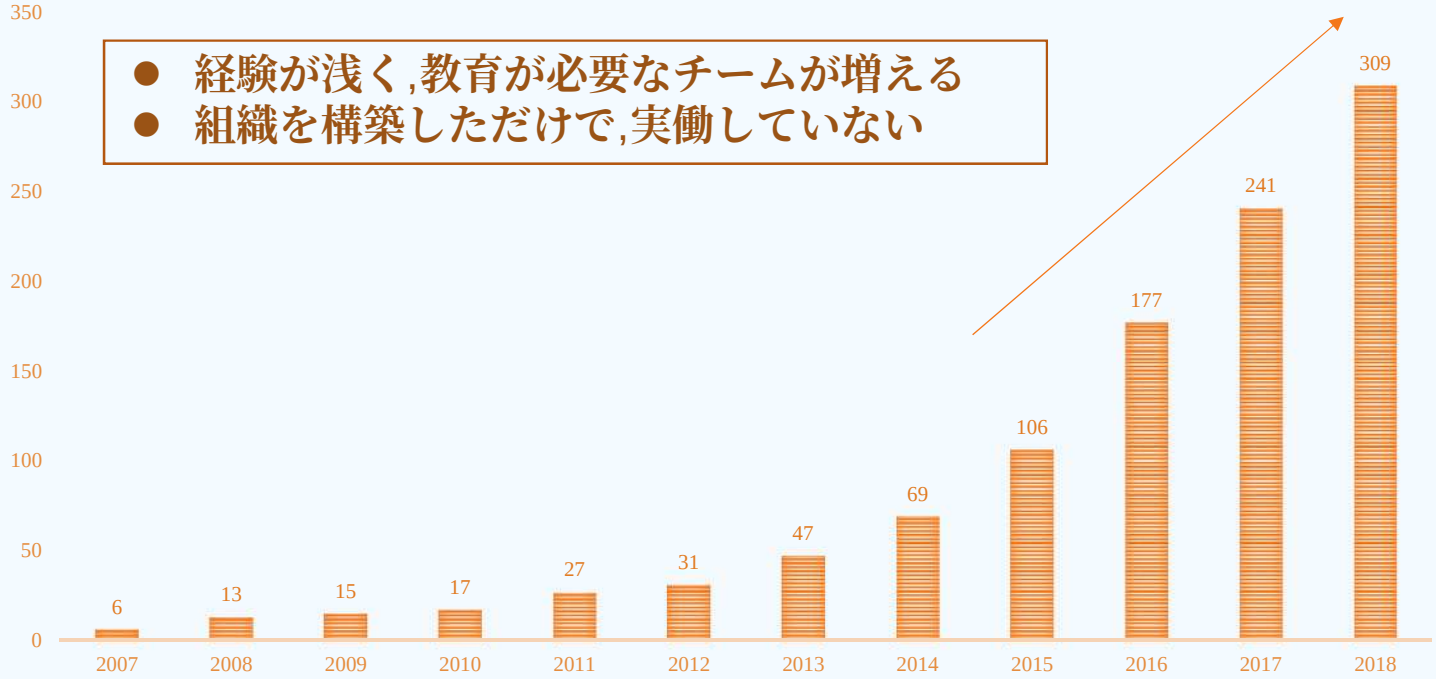
➡ CSIRTの設置

多くの組織が,サイバー攻撃,改ざん,窃取,破壊,強奪などの行為他のあらゆる干渉の被害を受けたホストやネットワークを迅速に対応し,被害を最小限に抑え,速やかに復旧させる「Computer Security Incident Response Team（CSIRT）」チームを整備

CSIRT構築ブーム

日本シーサート協議会加盟数の推移

- 経験が浅く,教育が必要なチームが増える
- 組織を構築しただけで,実働していない



出典：CSIRT構築から運用　著日本シーサート協議会をもとに作成
※241組織(2017年8月25日総会開催時点)
309組織（2018年8月6日現在　日本シーサート協議HPの会加盟数から引用）

CSIRTの役割

CSIRTの運営形態

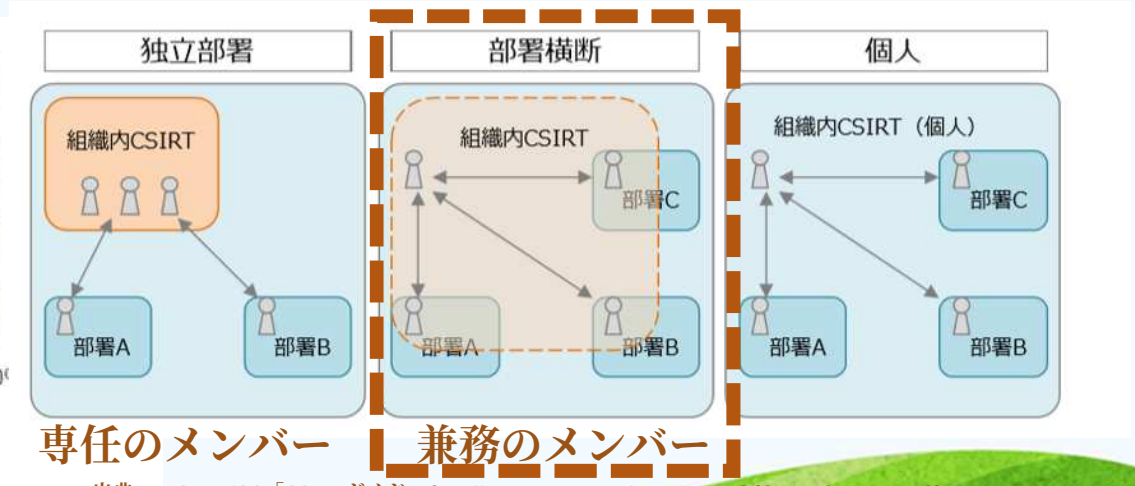
CSIRTが完全に独立した部署として運用されているケースは少ない

関連する部署にまたがった兼務のメンバーによって構成される

「仮想チーム」の形態をとるケースが多い

実装の形態

出典：日本シーサート協議会加盟組織一覧2017年版



出典：JPCERT/CC「CSIRTガイド」 http://www.jpcert.or.jp/csirt_material/files/guide_ver1.0.pdf

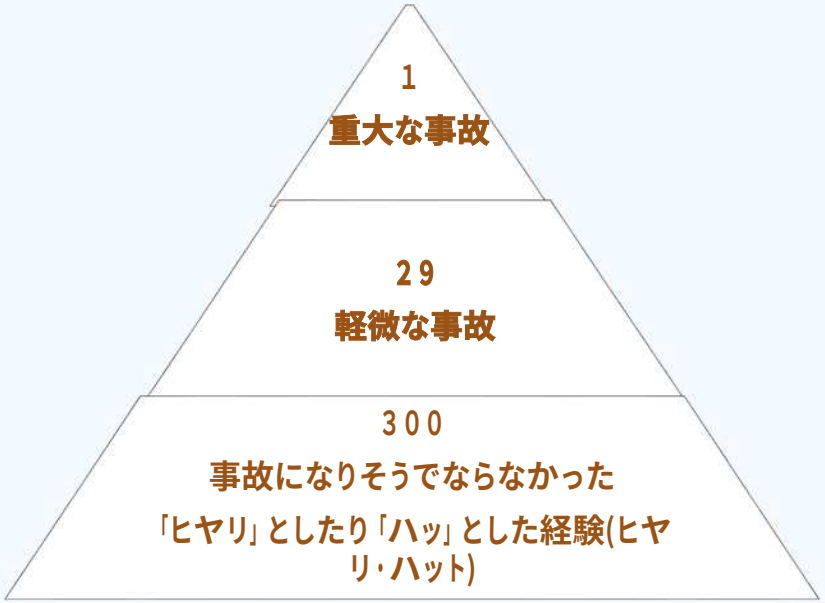
CSIRTの役割

組織内 CSIRT の基本的な役割

組織において発生したインシデントに対応する

(質問)
サンプル規定集での定義でインシデントの恐れがあるセキュリティイベントも含めて「インシデント」と定義されている一方で,上層部や構成員は「インシデント」というと重要な事態と捉えてしまい,説明に苦慮するのですが,どの様に理解を得るのがよいでしょうか

ハインリッヒの法則



効率的なインシデント対応のために

（質問）
インシデント対応に必要な情報はどのように収集しているか（すべきか）？また,日常的な活動の中で収集している（するべき）ならば,どのような方法がよいか

発生事象が「サイバー攻撃なのか、一時的な不具合なのか」などを的確に**推測・判断**する力が必要

- その時流行っている**サイバー攻撃**から推察する
- 組織内の**脆弱性**に関して事前に把握・整理する
- 攻撃者の目的を理解する
- 攻撃者に突破される可能性がある
- 対策を施す際, どのようにすれば侵入できるかの検討する（**侵入されても大きな被害を出さない**）

CSIRTの課題（人間の弱点を狙う脅威）

人的ミス事故を防止するには

ヒューマンエラーをはじめとした内部の人間に起因するセキュリティトラブル

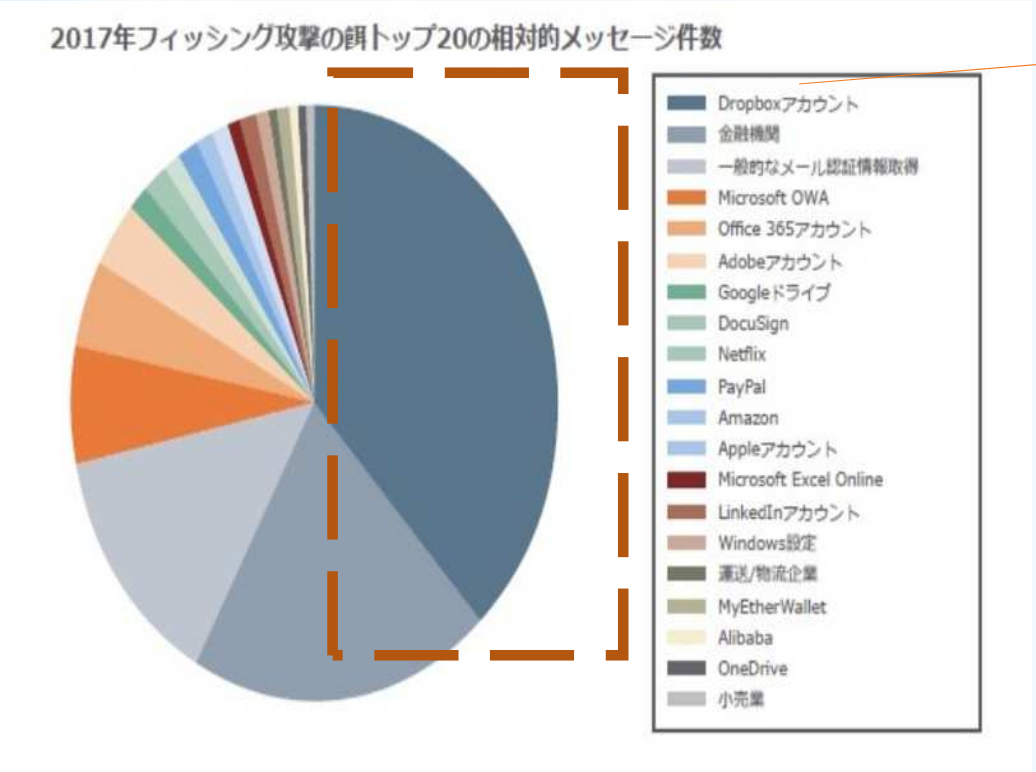
ミスが起こる５つの原因
(1) 技能の問題
(2) 性格の問題
(3) 生理的な問題
(4) 感情の起伏の問題
(5) 環境の問題

紛失・置き忘れ	盗難	メールの誤操作
誤操作によるデータ削除	内部犯罪・内部不正	規則違反

	漏えい原因比率				
	2013年	2014年	2015年	2016年	2017年
誤操作	34.90%	30.90%	25.80%	15.60%	25.10%
紛失・置忘れ	14.30%	12.60%	30.40%	13.00%	21.10%
不正アクセス	4.70%	2.40%	8.00%	14.50%	17.40%
管理ミス	32.30%	43.70%	18.80%	34.00%	13.00%
不正な情報の持ち出し	1.50%	2.80%	4.80%	6.80%	6.50%
盗難	5.50%	3.00%	5.50%	5.30%	6.50%
設定ミス	3.10%	2.10%	1.90%	4.70%	4.70%
内部犯行	1.00%	1.30%	2.10%	0.90%	2.10%
バグ・セキュリティホール	0.50%	0.30%	1.50%	1.70%	1.30%
ワーム　ウイルス	0.40%	0.30%	1.30%	1.10%	0.50%
その他	0.60%	0.40%	0.10%	1.90%	0.80%
不明	0.40%	0.20%	0.40%	ー	0.50%
目的外使用	0.70%	0.10%	0.30%	0.40%	ー

出典：特定非営利活動法人 日本ネットワークセキュリティ協会「情報セキュリティインシデントに関する調査報告書」から作成

フィッシング攻撃



出典：米Proofpoint「Human Factor 2018 Report」

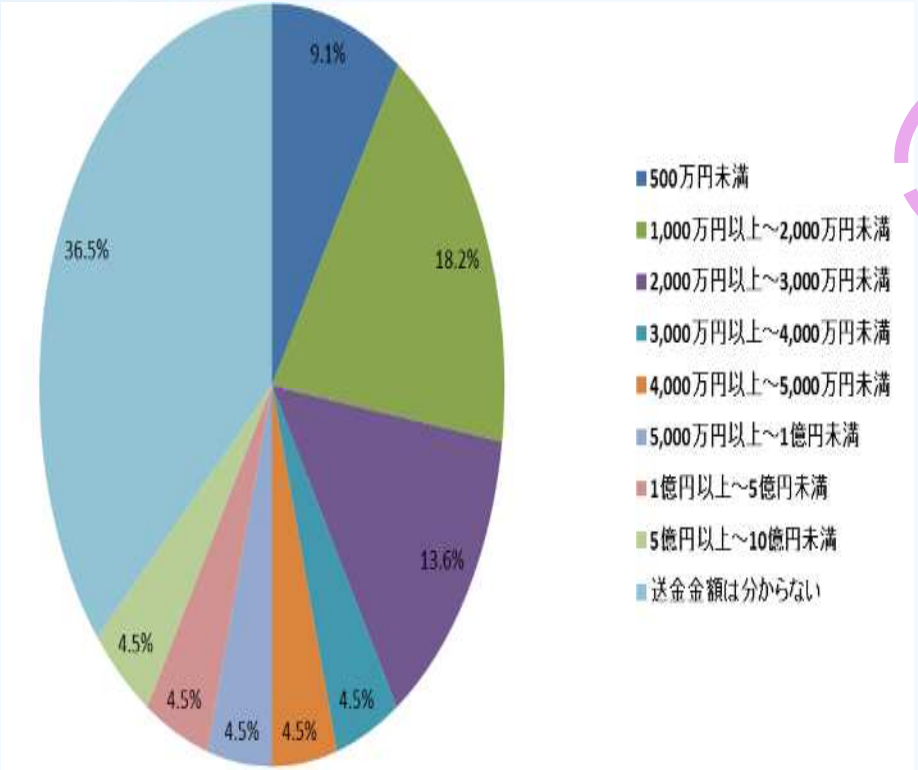
ファイル共有サービス「Dropbox」が増加

- クリック率が高いのは電子署名「DocuSing]を発信元と称するフィッシングの方がクリックされやすい
- メールが届いてかリックする時間
  1分以内11%
  5分以内4分の１

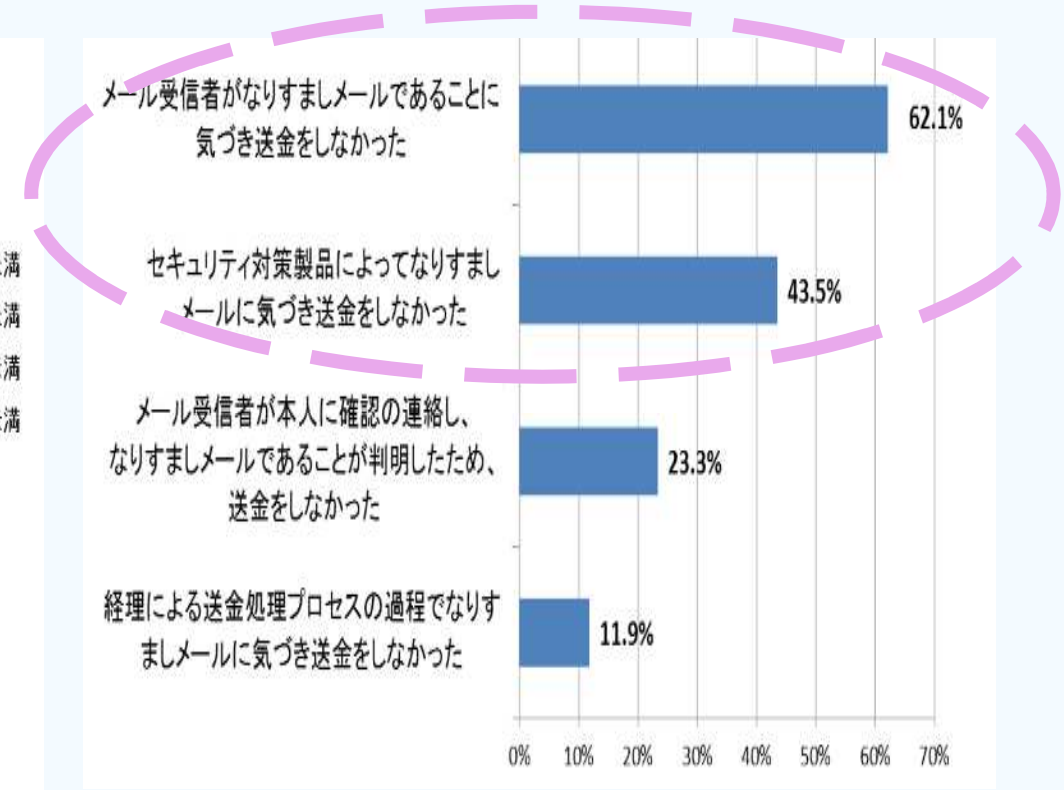
ソーシャリエンジニアリング

- 緊急性
- 信用あるブランドになりすます
- ビジネスメール詐欺（BEC）
- フェイチェーンを利用するメール詐欺
  「Re:」「Fwd:」

ビジネスメール詐欺



送金依頼メールに起因した送金金額内訳（N=22：単一回答）



送金を未然に防ぐことができた理由内訳（N=253：複数回答）

出典：トレンドマイクロビジネスメール詐欺に関する実態調査 2018

CSIRTの課題（人材不足）

業務時間の定義（長期的な人材確保のために）

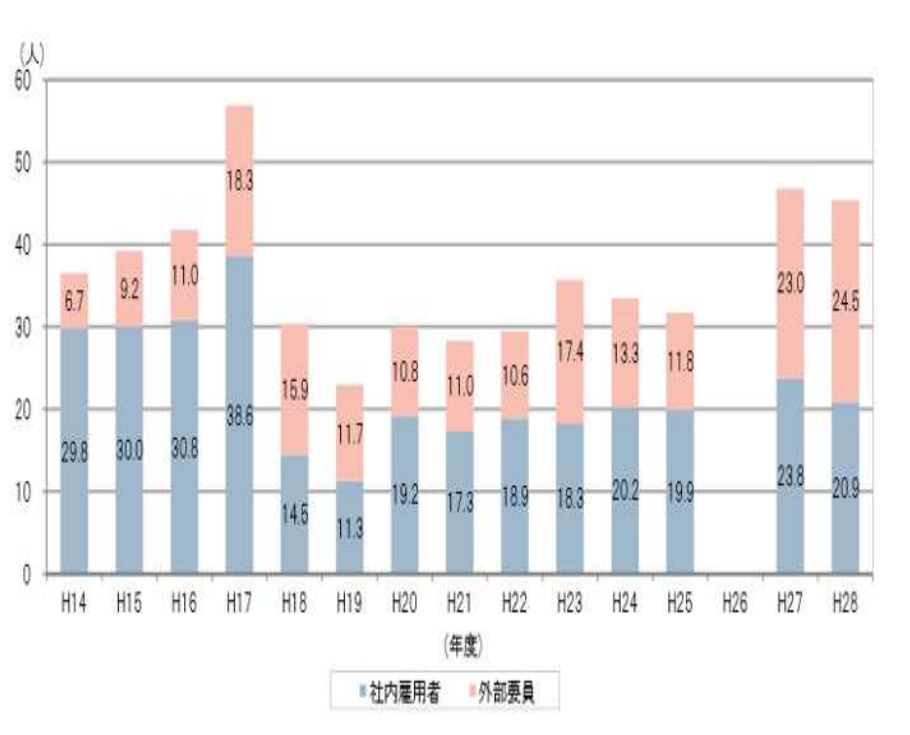
サービスの提供

- ２４時間,年中無休体制
- 交代制
- 業務時間内のみの対応
- 業務時間外の対応

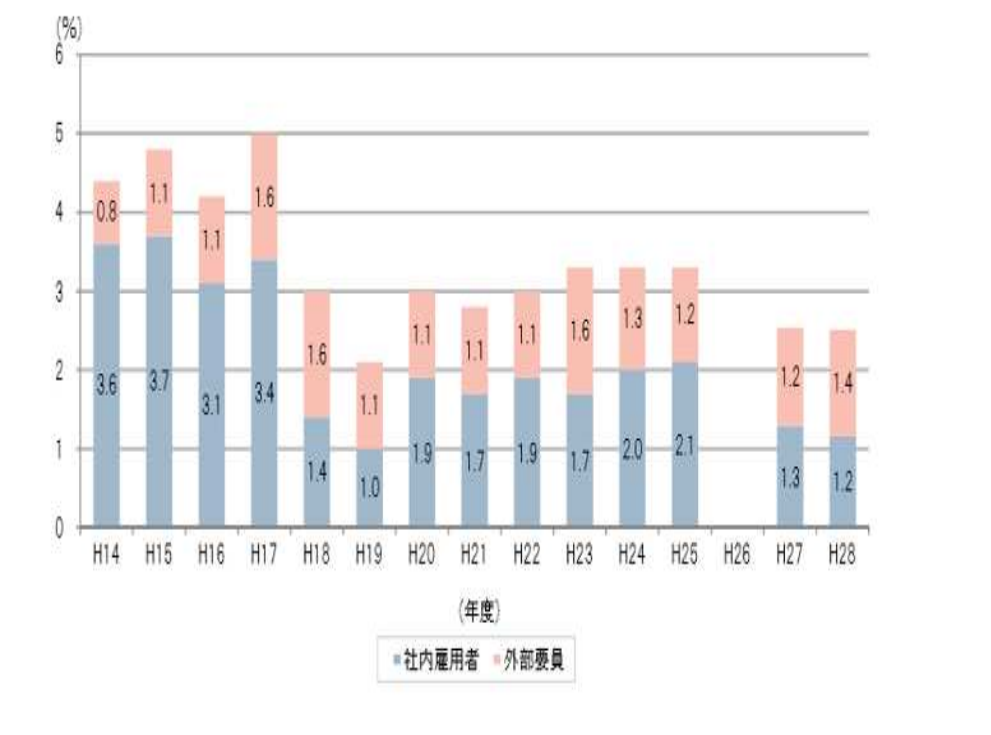
◆ 連絡体制の構築
◆ 事象により連絡体制の変化

IT人材

一社平均 IT 要員数

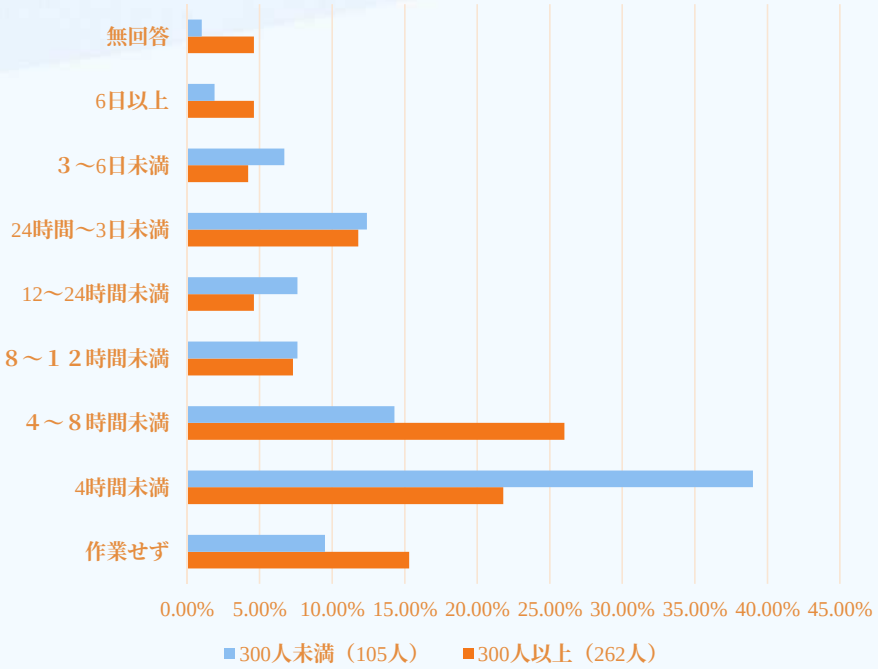


対総従業員数比

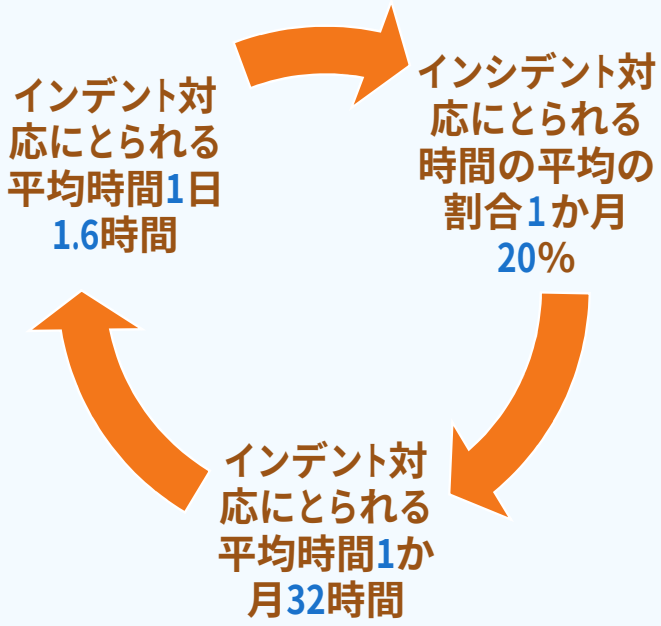


出典：経済産業省「情報処理実態調査」(2018)

ウイルス感染からの復旧作業延べ人日



出典：2014年度「情報セキュリティ事象被害状況調査　報告書」(IPA)から作成



出典：セキュリティ教育の実態調査エムオーテックス

CSIRTの課題 (予算面)

CSIRTを運営する上での課題

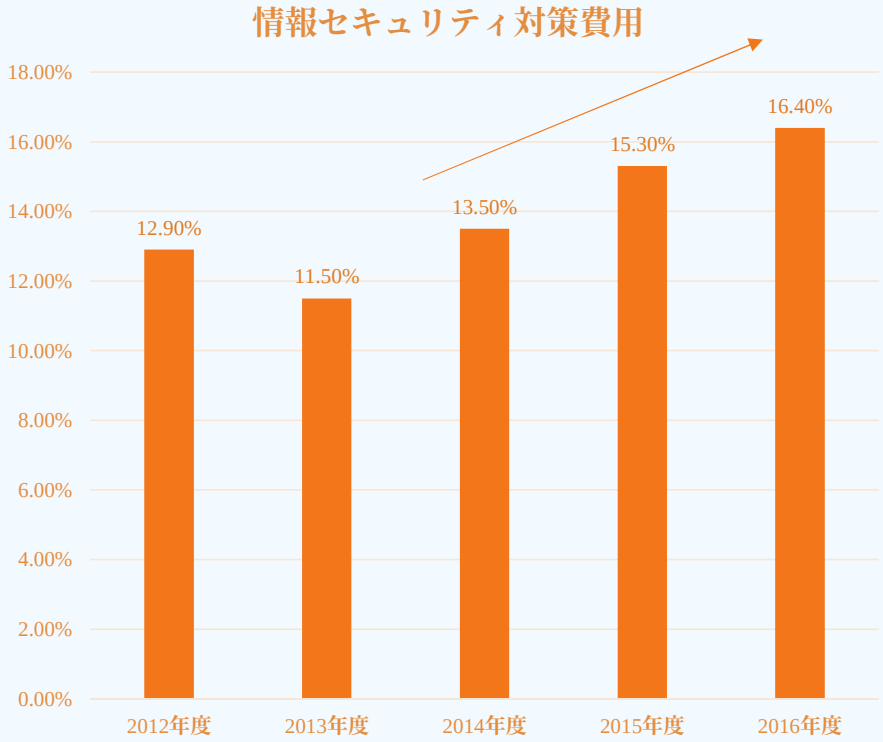
最大の課題　「予算」

ROI (Return On Investment　投資利益率)＝1,425%

マルウェア攻撃への投資

ランサムウェア攻撃を仕掛ける場合に必要な準備や運用コストと,攻撃から得られる金額から算出された値

情報セキュリティ対策費用



出典：ITR「IT投資動向調査2017」

一社平均情報セキュリティ対策費用の推移

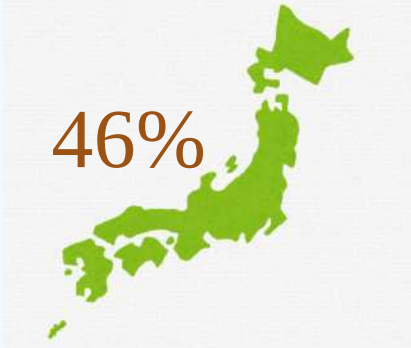
【中小企業】									(%)
	50万円未満	50～100万円	100～150万円	150～200万円	200～400万円	400～1,000万円	1,000万円以上	わからない	発生しなかった
平成22年	30.5	17.6	6.4	4.6	5.2	4.0	2.4	17.3	12.0
平成23年	30.2	16.1	6.8	4.7	5.9	3.6	1.7	18.4	12.6
平成24年	31.7	14.6	6.3	3.9	4.8	3.8	2.1	19.9	12.9
平成25年	35.2	16.9	6.0	3.1	4.9	4.0	2.0	18.0	9.8
【大企業】									(%)
	50万円未満	50～100万円	100～150万円	150～200万円	200～400万円	400～1,000万円	1,000万円以上	わからない	発生しなかった
平成22年	11.0	9.5	6.5	4.3	9.1	12.0	20.2	22.7	4.8
平成23年	10.2	10.0	5.5	5.2	10.2	11.9	18.5	23.4	5.0
平成24年	11.2	8.9	6.6	4.1	7.9	11.1	17.7	23.2	4.2
平成25年	12.7	9.1	5.3	5.1	8.5	12.1	19.5	23.5	3.8

出典　経済産業省「情報処理実態調査」

日本の企業は経済犯罪に関する事後対応費用が高額

直接的な被害額よりも事後対応費用の方が高いと答えた企業

世界全体



日本

不正が長期化

被害が全社的

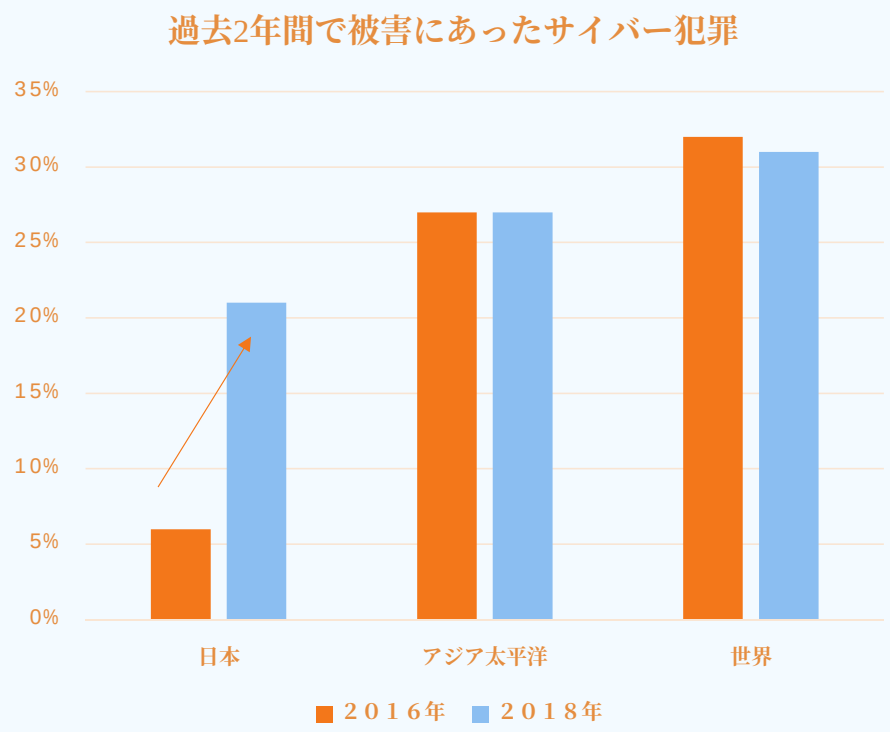
出典：経済犯罪実態調査 2018 日本分析版をもとに作成

直接損失額＝逸失利益＋復旧に要するコスト＋事故対応に要するコスト ＝（年間想定売上高÷365×業務停止日数）＋（復旧対応をおこなう人数×原価×復旧にかかる日数
＋ハードウェア・ソフトウェア費用）＋（事故対応をおこなう人数× 原価 × 事故対応にかける日数）

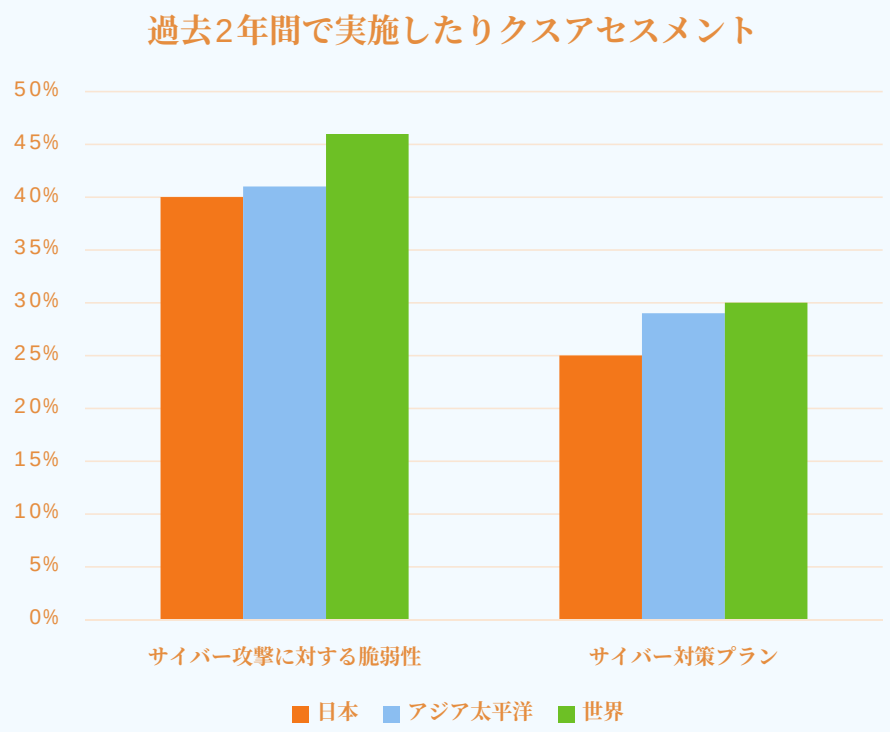
間接損失額 ＝ 補償･補填費用 ＋ 損害賠償費用 ＋謝罪広告費用

ALE（**年間損失予想額**：Annualized Loss Exposure **の頭文字**）**＝脅威の年間予想発生頻度×発生1回あたりの損失額**

なぜ日本の企業は経済犯罪に関する事後対応費用が高額になるのか



出典：経済犯罪実態調査 2018 日本分析版をもとに作成



出典：経済犯罪実態調査 2018 日本分析版をもとに作成

どうすれば利用者の利便性とセキュリティを担保できるのか

面倒な情報セキュリティ対策

情報セキュリティを万全にすればするほど,業務に支障や利用者の同意を得るのが難しい

（質問）
利用者として,手順が煩雑で不満を感じて「これで本当にセキュアになるのか？」という疑問を感じることがあると思うが,その場合に,どうやって利用者側の納得感を得るのか。工夫があれば教えて欲しい

厳しい情報セキュリティ対策
↓
実施が難しい
↓
セキュリティレベルが低い運用
↓
気がつかないままにセキュリティ・インシデントが発生

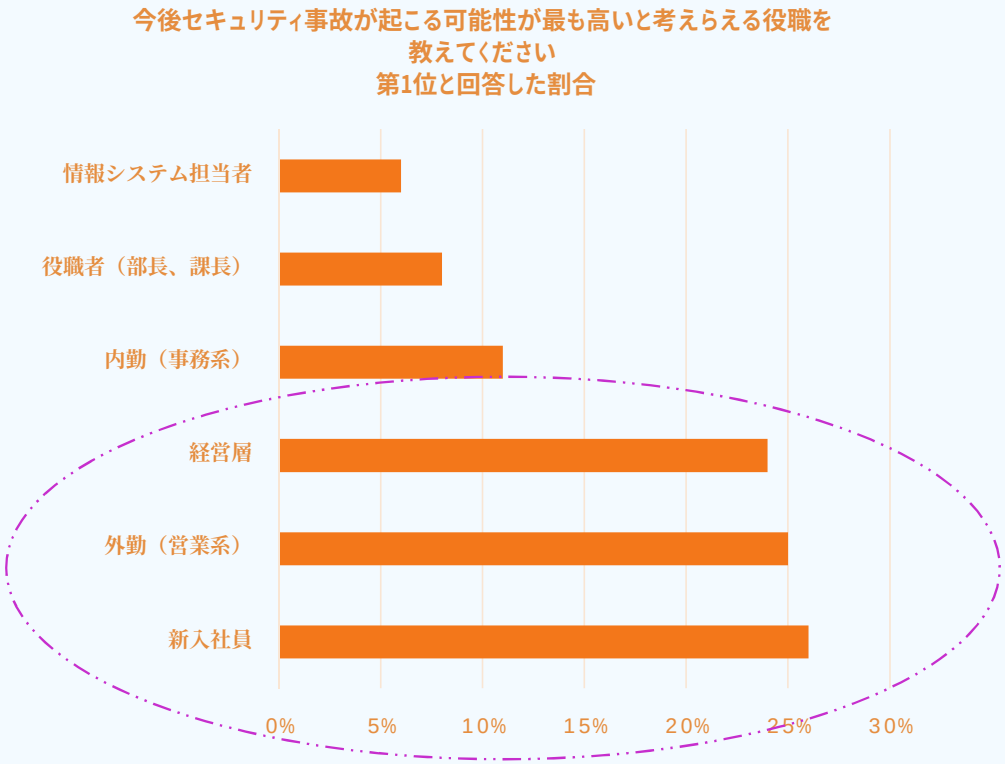
聞き取り調査(電話,対面を含む)

対象者：私立,公立,国立の教員に対して聞き取り調査期間　：2017年6月～8月
年齢　：30歳代～60歳代(男女)

質問項目
①貴大学における情報セキュリティ対策や運営に関して不満や良い点など

- 利用者の利便性とセキュリティはトレードオフだとわかるが,利用しずらい面がある
- 利用者はもちろん利便性がある方がいいが,安全面も協力したいと考えている
- 大学によって運営が異なりので,異動時は戸惑いを感じた
- セキュリティのe-learningに効果があるのか疑問である
- 注意喚起を個別に対応してほしい
- セキュリティが非常に面倒だと感じている

組織内の意識改革



出典：セキュリティ教育の実態調査エムオーテックス
から作成

①情報セキュリティの基本をルール化して守る

②潜在的な事件や事故が顕在化したときに,人的なミスや事件・事故の誘引物や条件を取り除く（悪いことができない仕組みを作る）

③情報セキュリティに対する自覚の教育や専門教育を行う

懲罰性

個人情報の不適切な取扱いに係る懲戒処分等の状況一覧（教育職員）

（単位：人）

	平成23年度	平成24年度	平成25年度	平成26年度	平成27年度	平成28年度
免職	0	0	0	0	0	0
停職	1	1	0	1	2	0
減給	10	10	9	7	10	6
戒告	28	30	22	23	24	17

出典：「公立学校教職員の人事行政状況調査について」（文部科学省）をもとに作成

ルール強化（一例）

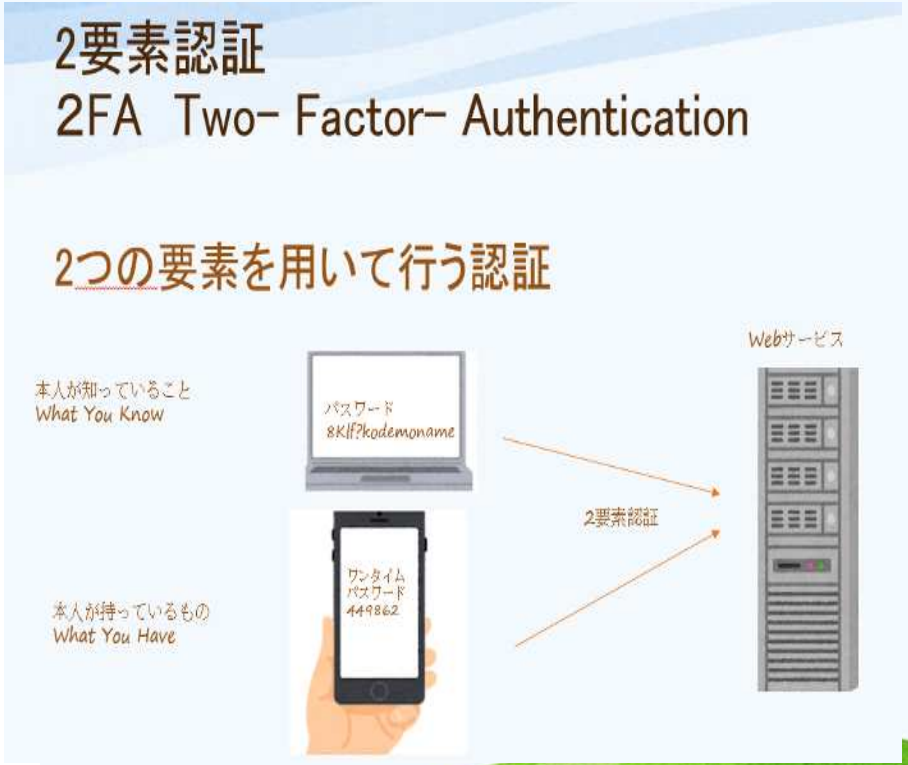
２０１３年４月２日から４月５日にかけて不正アクセスの被害にあったeBookJapan

ログイン成立分

IDあたりPW試行回数	該当ID数
1	386
2	347
3	37
4	4
5	5

ログイン失敗分

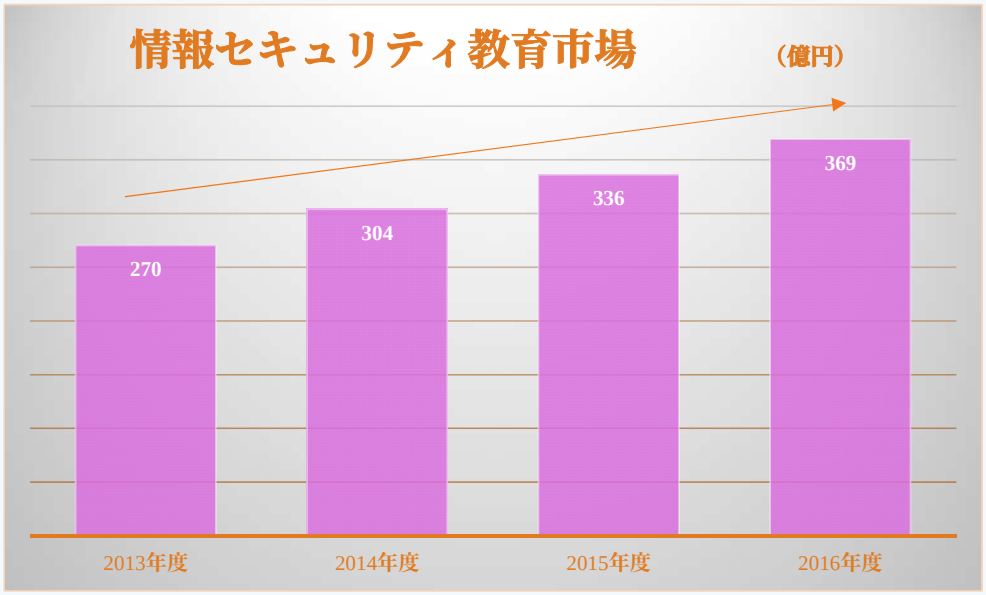
IDあたりPW試行回数	該当ID数
1	1327
2	72
3	20
4	7
5	3
6	1
9	1

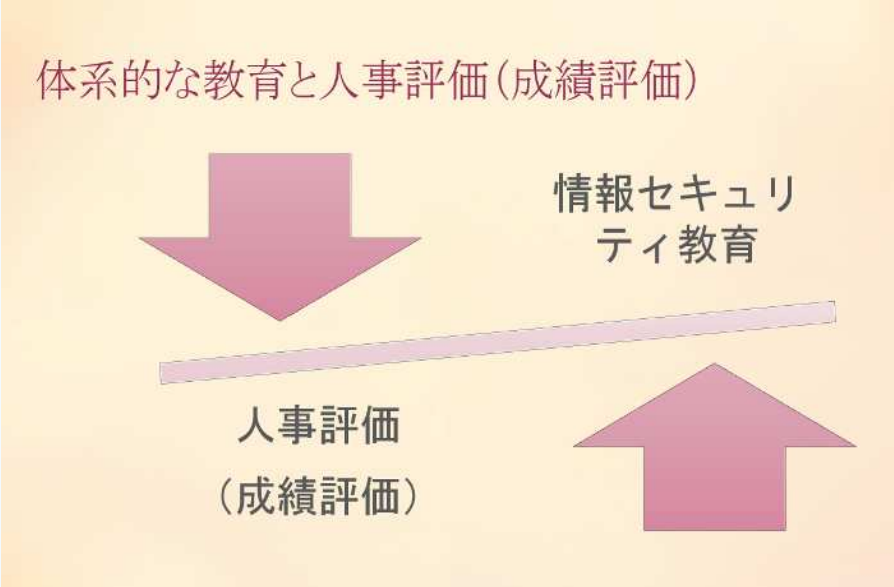


出典：eBooKJapan　不正ログインに関する最終報告より

情報セキュリティ教育

情報セキュリティ教育の導入

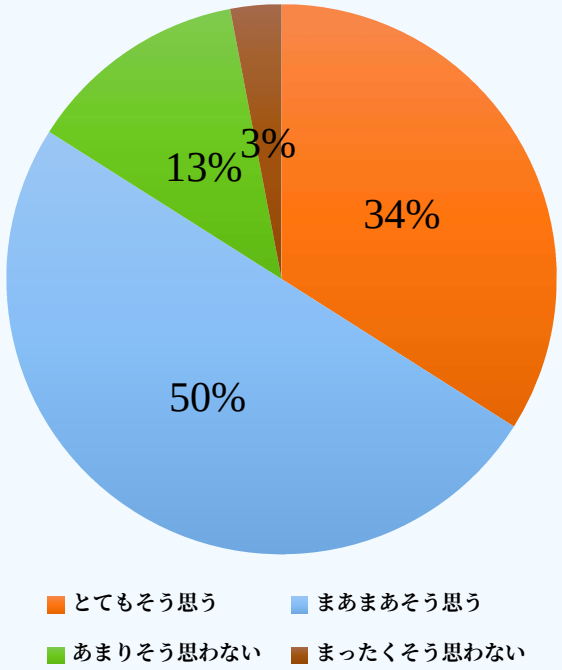




出典　2015年度 情報セキュリティ市場調査報告書

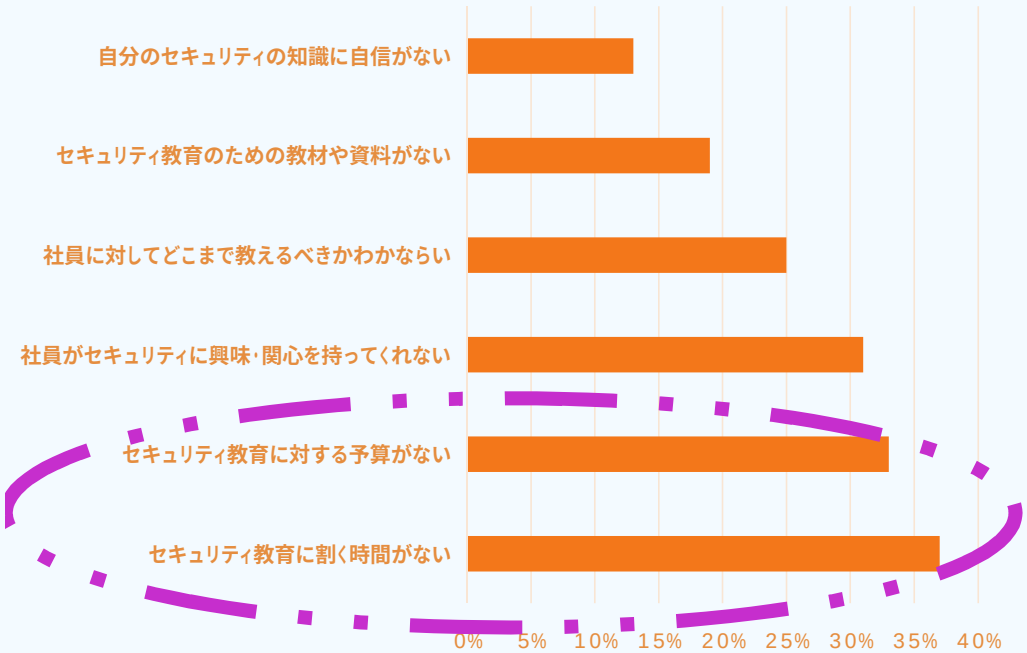
情報セキュリティ教育の問題点

社内でのセキュリティ教育に改善の必要があると感じますか



出典：セキュリティ教育の実態調査（エムオーテックス）

セキュリティに関して教育を施す際に、困っていることは



出典：セキュリティ教育の実態調査（エムオーテックス）

情報セキュリティ教育 (e-learning)

E-learningを活用した情報セキュリティ教育の問題点

- 毎年受講させないといけないのか
- 個々の情報リテラシーレベルに対応した内容のコンテンツが少ない
- テストで内容を確認する仕組みが多いが,本当に理解しているのか
- 情報セキュリティ教育の内容はあまり代り映えがしない
- 人事評価と連動する必要があるのか

作成側

- 毎年内容を見直しする必要がある

まとめ

効率的かつ効果的なCSIRT運営には

効率的なインシデント対応を実施するには

- CSIRT運用の経験値を高める
- 予算の確保 (中長期的)
- セキュリティ管理者の技術向上
- アウトソーシングの活用
- 長期的な人材確保
- 構成員のリテラシー向上 (興味深い内容のもの)