

# クラウドセキュリティの最新動向

BSIグループジャパン株式会社（英国規格協会）

マーケティング本部

武藤 敏弘

February 7, 2014



# アジェンダ

- 1) BSI(英国規格協会)及びBSIグループジャパンの紹介
- 2) 国内のセキュリティ状況
- 3) クラウド・セキュリティの監査・認証
- 4) その他

# Who we are.

- BSIは、英国国家規格協会として、世界中のあらゆるお客様の「エクセレンス」実現をサポートします
- BSIは、150カ国で事業を展開しており、グローバルカンパニーから中小企業まで約70,000を超えるお客様がいます
- BSIは世界最古の国家規格協会であり、ISOの設立メンバーでもあります。そしてISO9001を含む世界で最も幅広く採用されている規格の策定にも携わっています



# Who we are.



- 【沿革】
- 1901年： 英国の貿易産業省の支援を受けて設立  
世界最古の国家規格協会
- 1929年： 英国王室より  
英国王室憲章授与
- 1979年： 品質マネジメントシステム規格BS5750の発行
- 1999年： BSIジャパン株式会社 設立



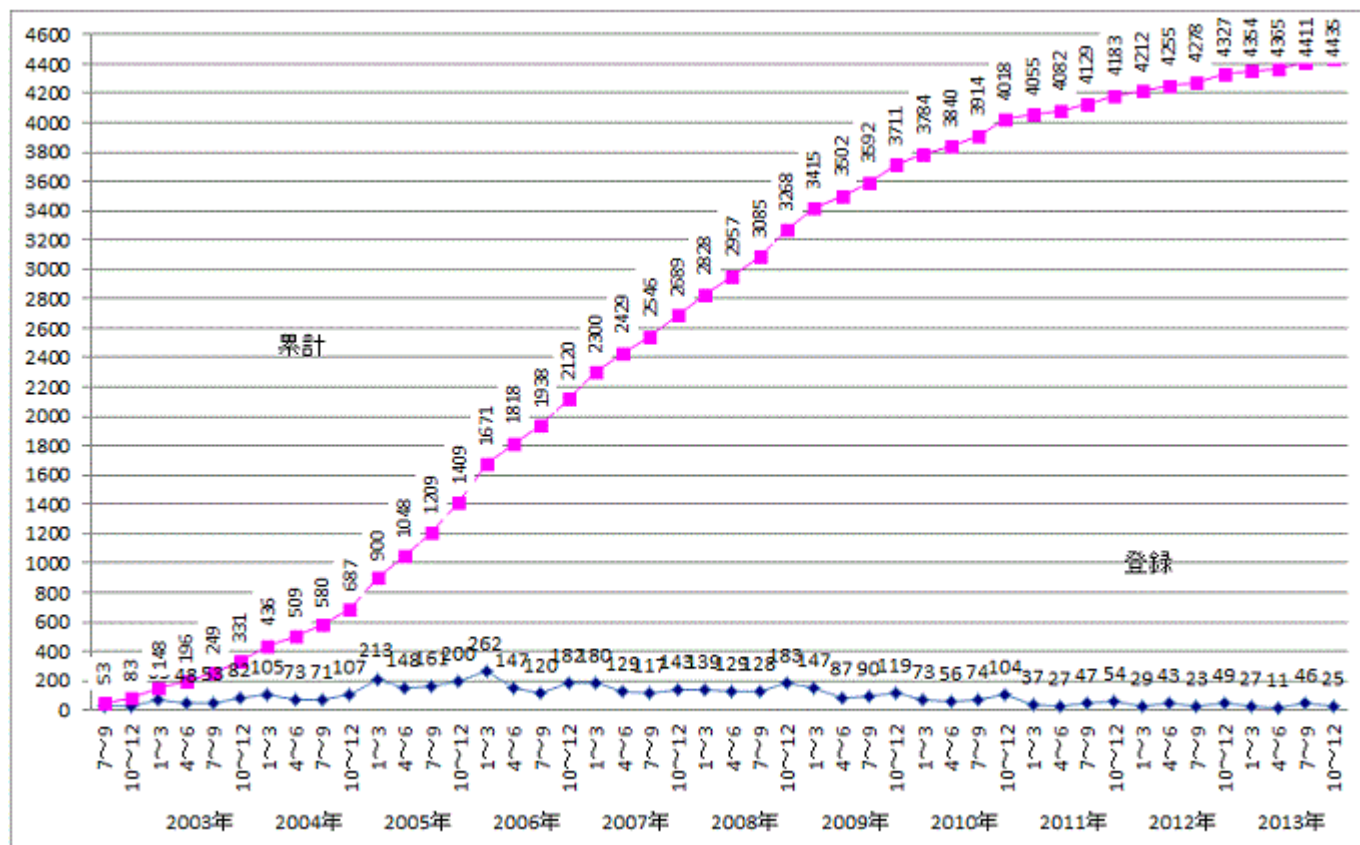
- 【BSIが開発した主な規格】
- 1979年 BS 5750 -> ISO 9001
- 1992年 BS 7750 -> ISO 14001
- 1995年 BS 7799 -> ISO/IEC 27001 ※
- 1996年 BS 8800 -> OHSAS 18001
- 1999年 BS 8600 -> ISO 10002 ※
- 2002年 BS 15000 -> ISO/IEC 20000 ※
- 2003年 PAS 56 -> BS 25999 – 1
- 2006年 BS 25999-1 ※ -> ISO 22313
- 2007年 BS 25999-2 ※ -> ISO 22301
- 2007年 BS 8901 -> ISO 20121
- 2008年 PAS 2050 -> ISO 14067  
PAS220 -> ISO/TS 22002-1
- 2009年 BS EN 16001 -> ISO 50001 ※
- 2010年 PAS2060
- 2011年 PAS223 PAS222

※日本国内認証件数  
シェアNo.1

# ■日本のセキュリティレベル ISO27001(ISMS)

ISMS認証取得組織数推移

2014年12月25日現在 登録：4 4 3 5





インターネット配信サービスのシステムが攻撃を受け、世界各国で大量の個人情報流出。クレジットカード情報の悪用が懸念される事態となった。

政府は、過去の海外での事例や対応策について企業に提供するほか、防御のた

めの国際基準などを手引書にまとめ、企業などに示す。次期計画にはこのほか、サイバー攻撃を受けた場合でも、企業がサービス提供などを行う社会的責任を初めて明記。必要な計画の策定や予算、体制の確保などを求めた。

一般社団法人 日本クレジット協会（JCA）の賀詞交換会にて

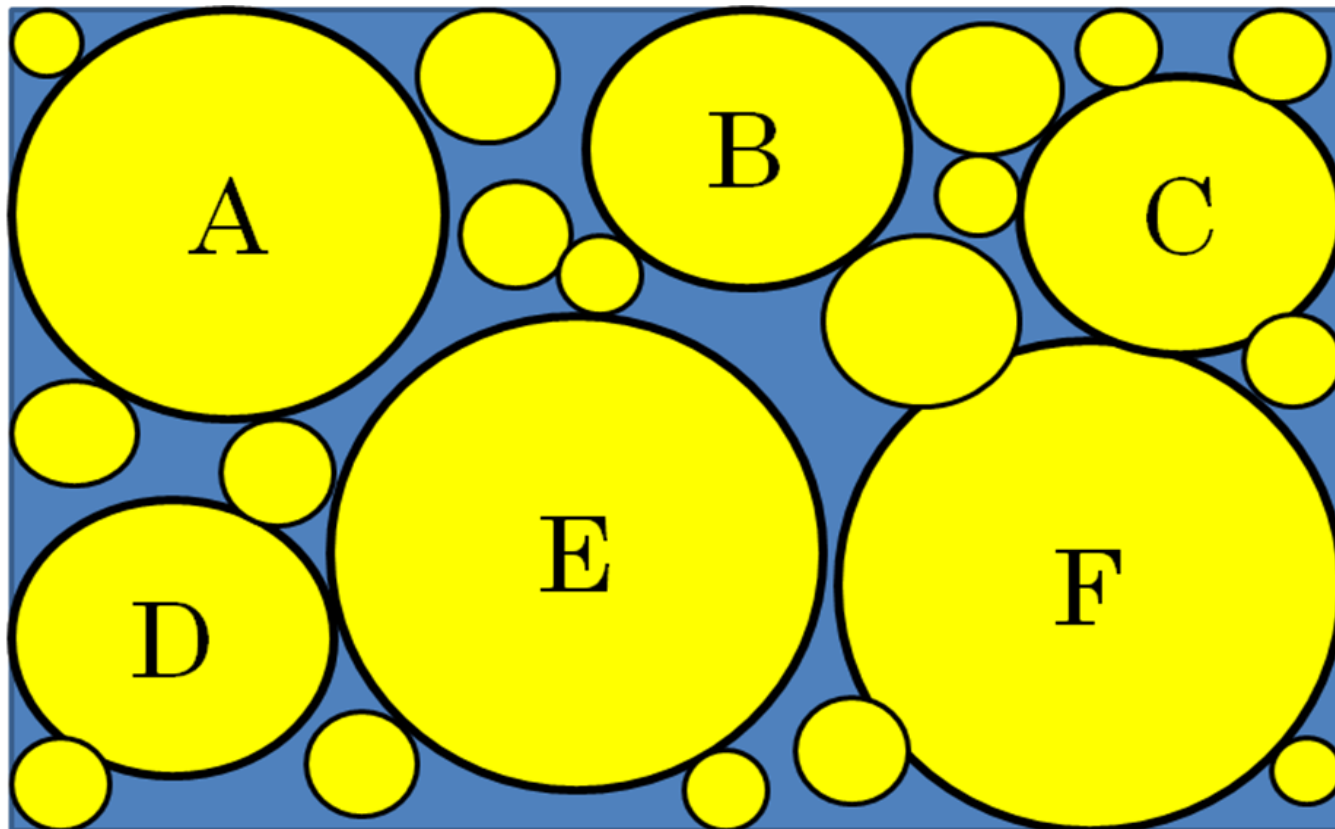
経産省の審議官が

1. ICカード化推進
  2. 加盟店のカード情報管理の強化
- を今年、来年度のテーマとしてあげていた。



# リスクの考え方

頻度の高い・影響の大きいリスクをコントロールすれば全体の80%以上を管理できる





# クラウド・セキュリティの監査・認証

# クラウドを利用するメリット・デメリット

## • メリット

- コスト削減
- 拡張性
- 専門技術者等の人的資源が不要

## • デメリット

- ガバナンス喪失
- ロックイン
- コンプライアンスリスクの可能性
- データ保護等のセキュリティ対策が不明
- プロバイダーのサービス継続性が不明



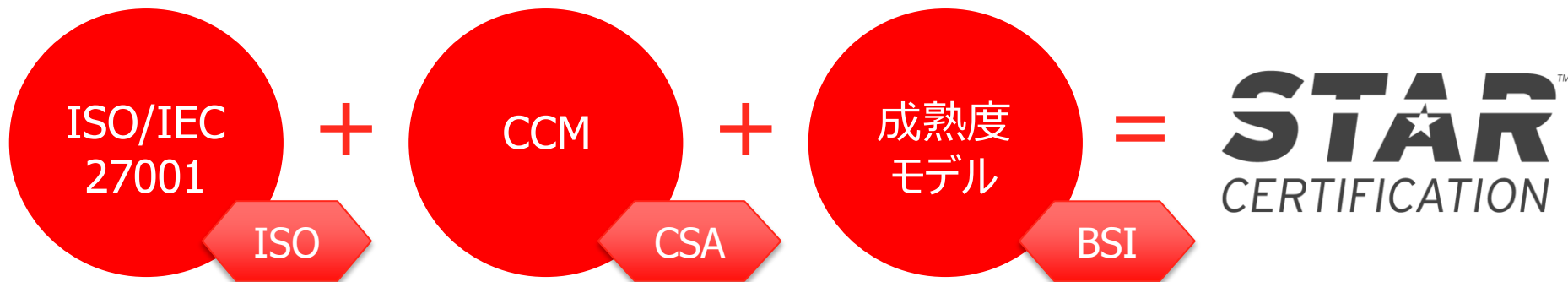
# STAR認証の背景

- ISO/IEC 27001は広く認知され、情報セキュリティマネジメントシステム規格として利用されているが、特定セクターの特定領域に関して十分に詳細に焦点を当てていないとの認識もある。
- ISO/IEC 27001は附属書以外の他の管理策が追加できるように規定されている。
- クラウドセキュリティアライアンス（CSA）が開発したクラウドコントロールマトリックス（CCM）は、クラウドセキュリティの重要な管理策に焦点が当たるような要求事項を提供する。
- BSIは、CSAとのパートナーシップにより、CCMに基づいた「**STAR認証**」を開発した。



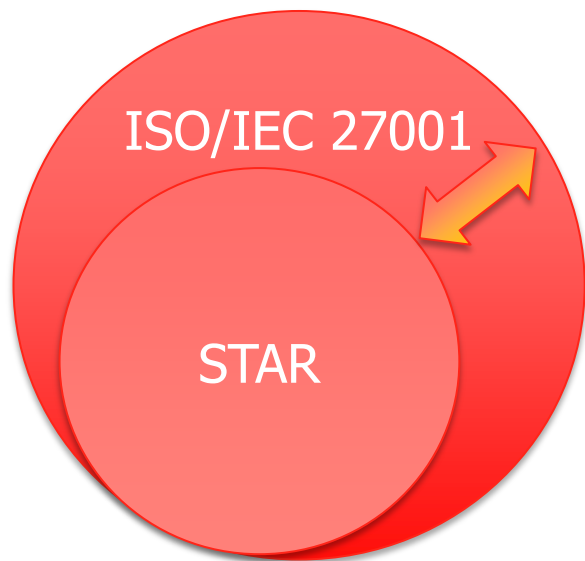
# STAR認証とは？

- ISO/IEC 27001認証審査と同時に審査を実施
- クラウドコンピューティングのセキュリティにおける成熟度を評価
  - CSAが開発したCCMを用いて、クラウドサービスの成熟度を評価
- STAR認証を受けた組織は、クラウドサービスの成熟度のレベルに応じて、「ブロンズ」「シルバー」「ゴールド」のアワードが授与される。



# STAR認証の対象組織・認証範囲

- クラウドサービスを提供している組織の全てがSTAR認証の対象となる。ただし、以下の条件を満たさなくてはならない。
- STAR認証を取得する組織は、ISO/IEC 27001認証を取得していなければならない。
- STAR認証の認証範囲はISO/IEC 27001認証範囲と同じか、又は小さくなければならない。
- ISO/IEC 27001認証と同じ認証機関からSTAR認証の審査を受けなければならない。



# STAR認証のポイント・まとめ

- 非認定の認証
- 3年間の認証有効期限（サーベイランス、再認証審査をISO/IEC 27001と同様に実施）
- ISO/IEC 27001認証取得と同時にSTAR認証を取得（初回認証審査）
- ISO/IEC 27001認証取得企業は、認証範囲の拡大でSTAR認証を取得（拡大審査）
- ISO/IEC 27001認証機関とSTAR認証機関は同一でなければならない。
- 成熟度レベルに応じたアワード（アワードなし、ブロンズ、シルバー、ゴールド）がSTARの認証書に記載される。
- 組織は、特別審査（拡大審査工数が必要）で成熟度レベルの変更を希望できる。
- STAR認証の登録に対する手数料が発生する。
- STAR認証を実施する審査員は、BSIが提供するSTAR認証の審査員研修を受けて、試験に合格しなければならない。

# Appendix



## CCMの11の管理エリア

STAR認証は、ISO/IEC 27001とCCMの基準への達成をベースとしており、CCMには、下記の11の管理エリアがあります。

1. コンプライアンス (Compliance)
2. データのガバナンス (Data Governance)
3. 設備のセキュリティ (Facility Security)
4. 人的資源のセキュリティ (Human Resources Security)
5. 情報セキュリティ (Information Security)
6. 法律 (Legal)
7. 作業管理 (Operations Management)
8. リリース管理 (Release Management)
9. 耐障害性 (Resiliency)
10. リスク管理 (Risk Management)
11. セキュリティアーキテクチャ (Security Architecture)



## マネジメントシステム成熟度レベルのスコア

- 11の管理エリアの管理策（98の管理策）に対して1～15のスコアを評価
  - 98 管理策 (CCM 1.4)
  - 145 管理策 (CCM 3.0)
- 成熟度レベルのスコアは、管理エリアで、それぞれ下表の5段階に分類される。

| SCORE | DESCRIPTOR                 |
|-------|----------------------------|
| 1-3   | No Formal Approach         |
| 4-6   | Reactive Approach          |
| 7-9   | Proactive Approach         |
| 10-12 | Improvement Based Approach |
| 13-15 | Optimising Approach        |

# CSAについて

# CSAについて

## CSA : Cloud Security Alliance クラウドセキュリティアライアンス

- 設立：2008年
- 国際的に活動を展開している非営利法人
- 使命：クラウドコンピューティングのセキュリティを実現するため、ベストプラクティスを普及させる。  
⇒ **CCM(Cloud Control Matrix)及びSTAR Certificationを開発**
- 拠点：アメリカを中心に、世界60以上の支部 (chapter)
- 40,000人以上の個人会員

## CSAジャパン

- 設立：2010年6月（世界で2番目の支部）
- 活動
  - CSA発行のガイダンス、CCMなどの日本語訳・対応解説の開発
  - 日本での普及啓発活動（イベントの開催等）
  - CSA本部の活動への参加・交流

official chapters



# CSA Corporate Members (例)



- その他、多くの企業が Corporate Memberとして参加している。
- これ以外にも次のメンバーがいる
  - Affiliate Members (NPO や産業グループ等)
  - Solution Providers

# その他

## 犯罪者はどこに目をつけているか



著者:

清水賢二

東京学芸大学大学院修了。

警察庁犯罪予防研究室室長を経て、日本女子大学教授。現在、ステップ総合研究所特別顧問。

清水奈穂

立教大学大学院修了。科学技術振興機構(JST)研究員など。現在、ステップ総合研究所代表

忍びの弥三郎(のびのやさぶろう)

猿の義ちゃん(ましろのぎちゃん)

自らを「賊」と称し、警察も含め周囲から「最後の賊」と呼ばれた。犯罪者の中でも天才的と評された。

# 対策への誤解・過信 → リスクに対する適切な対応

リスクに対する対策が適切であり充分かの検証を継続して実施する

## クレセント錠



## ディスクシリンダー

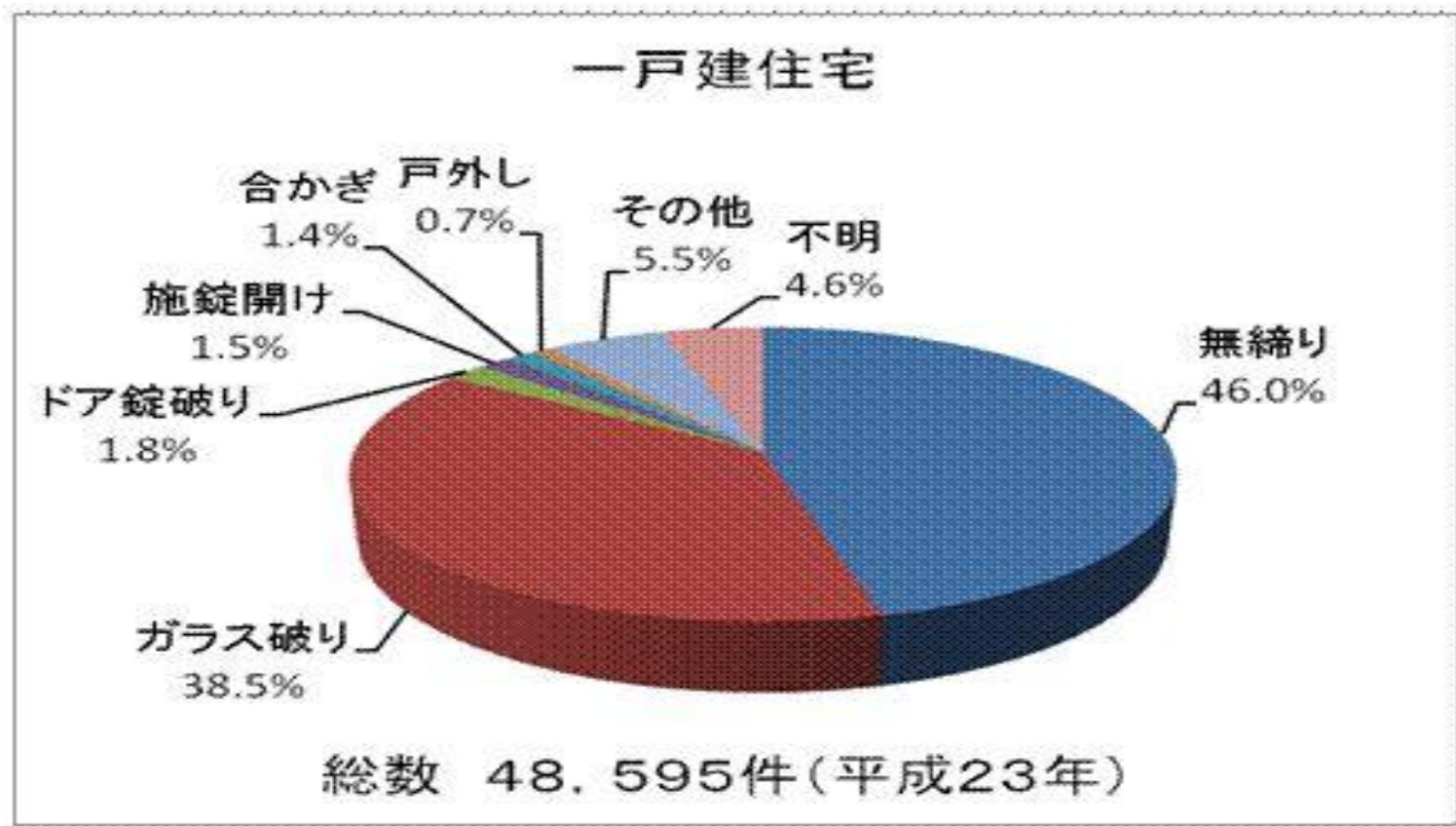


# 防犯対策ではない！



# 侵入窃盗の侵入手段

システム、重要な情報に鍵をかけていますか。





...making excellence a habit.™

BSIグループジャパン株式会社  
マーケティング本部

Tel : 03-6890-1172

Fax : 03-6890-1181

E-mail : toshihiro.muto@bsigroup.com

〒107-0061

東京都港区北青山2-12-28 青山ビル5階

[www.bsigroup.jp](http://www.bsigroup.jp)

All rights reserved 不許複製 BSIグループ ジャパン株式会社からの書面による許可なく、このプレゼンテーションのいかなる部分も、いかなる形式でも、また写真複製及びマイクロフィルムを含む一切の電子的又は幾何的な方法のいずれによっても、複製又は利用を禁ずる。