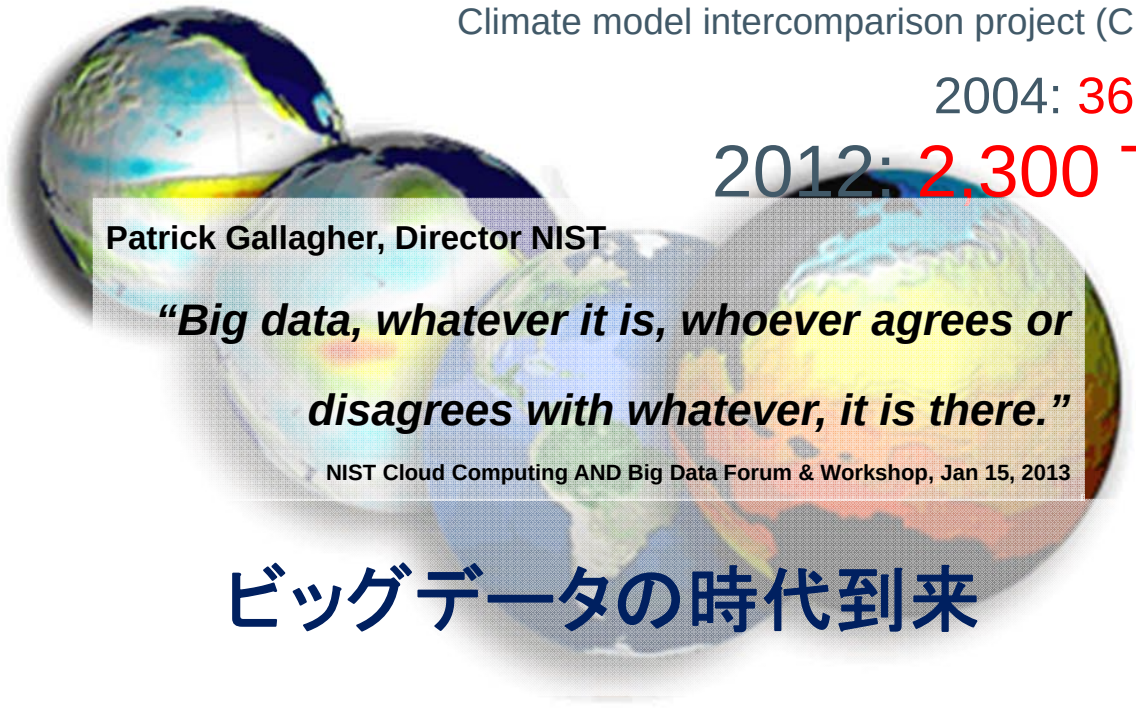
明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

セキュリティのためのBig Dataと Big Dataのためのセキュリティ

“Big Data for Security & Security for Big Data”

後藤　厚宏
情報セキュリティ大学院大学
Institute of Information Security (IISEC)

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



Climate model intercomparison project (CMIP)

2004: 36 TB

2012: 2,300 TB

Patrick Gallagher, Director NIST

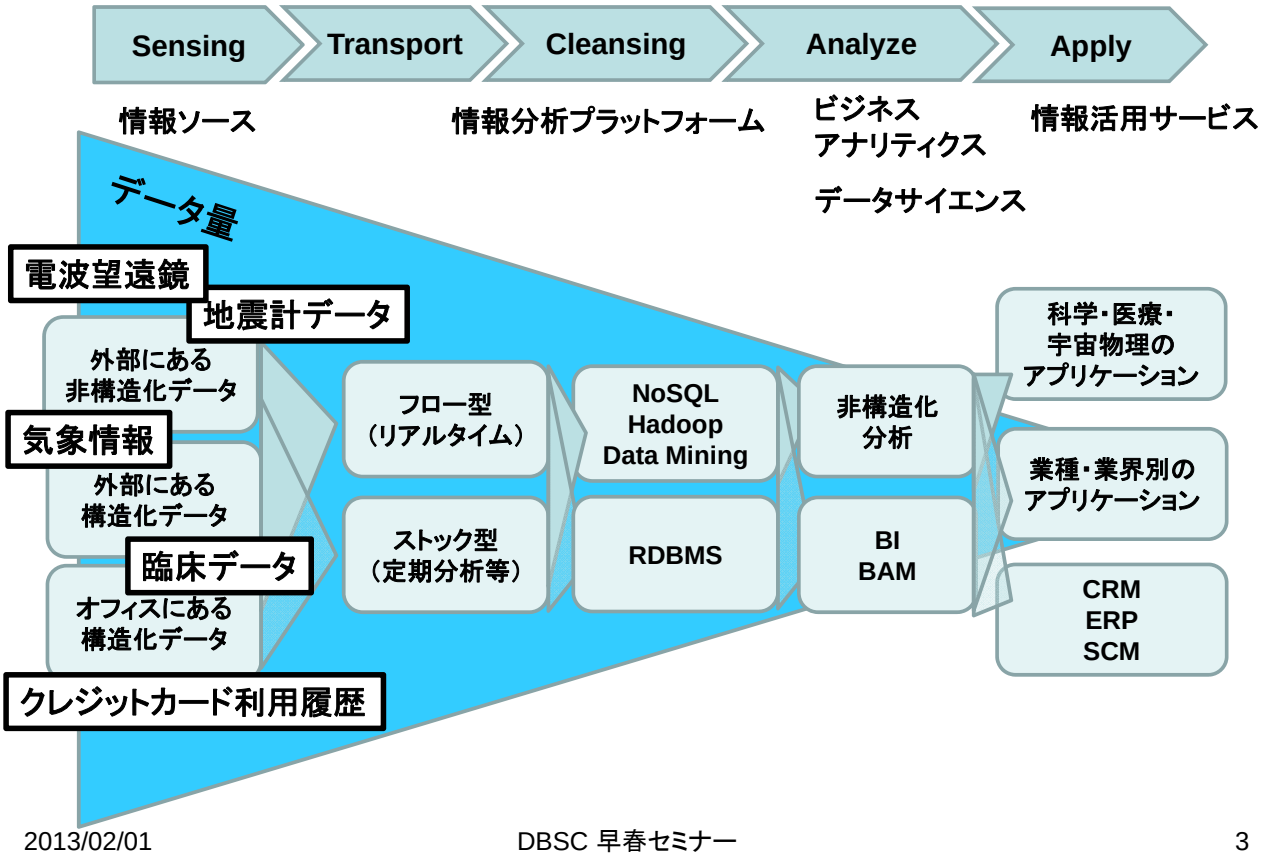
“Big data, whatever it is, whoever agrees or disagrees with whatever, it is there.”

NIST Cloud Computing AND Big Data Forum & Workshop, Jan 15, 2013

ビッグデータの時代到来

Big Data Analytics

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



社会に変革をもたらしつつある BigData

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

我々の社会生活において

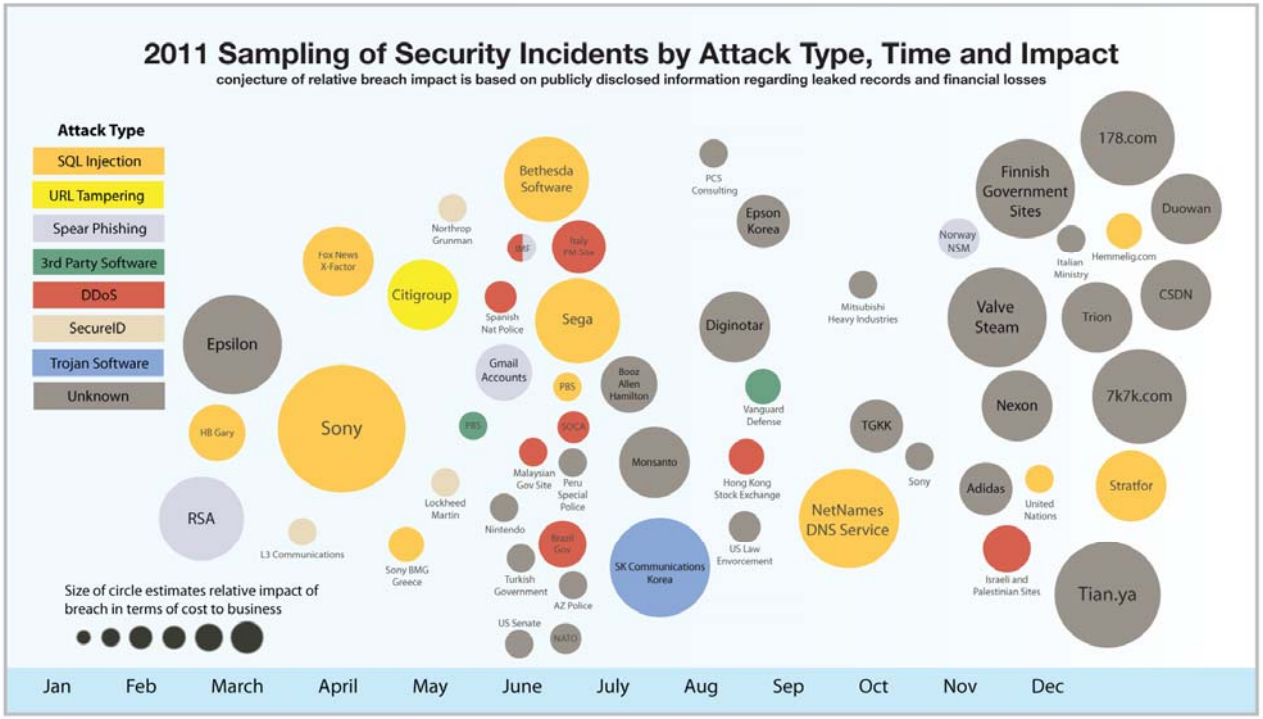
- 小売り業の変革
- 天文学の変革

- 健康医療における変革
  （医薬品開発、インフルエンザ流行予兆検知　など）
- 犯罪防止への貢献　（米国 CRUSH）
- ネットワークセキュリティへの貢献

TARGET

インシデント分析の困難さ

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



March 2012　Source: IBM X-Force® Research and Development

米国政府のITシステムの動向

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

■「**境界防御ではAPTに対処できない**」Cyber-Warを宣言する国の意識

- ●連邦政府のITシステムでは、境界が破られることを前提に、系全体に埋め込んだセンサーで早期に検知して被害が広がる前に対処

■ **情報セキュリティ・コンティニュアスモニタリング**

（ ISCM Information Security Continuous Monitoring）

- ●リアルタイムに<u>システム</u>や<u>組織</u>の状態を<u>常時(continuous)</u>モニターして分析、検証

  ⇔サンプリング的（continual）な検証では不十分

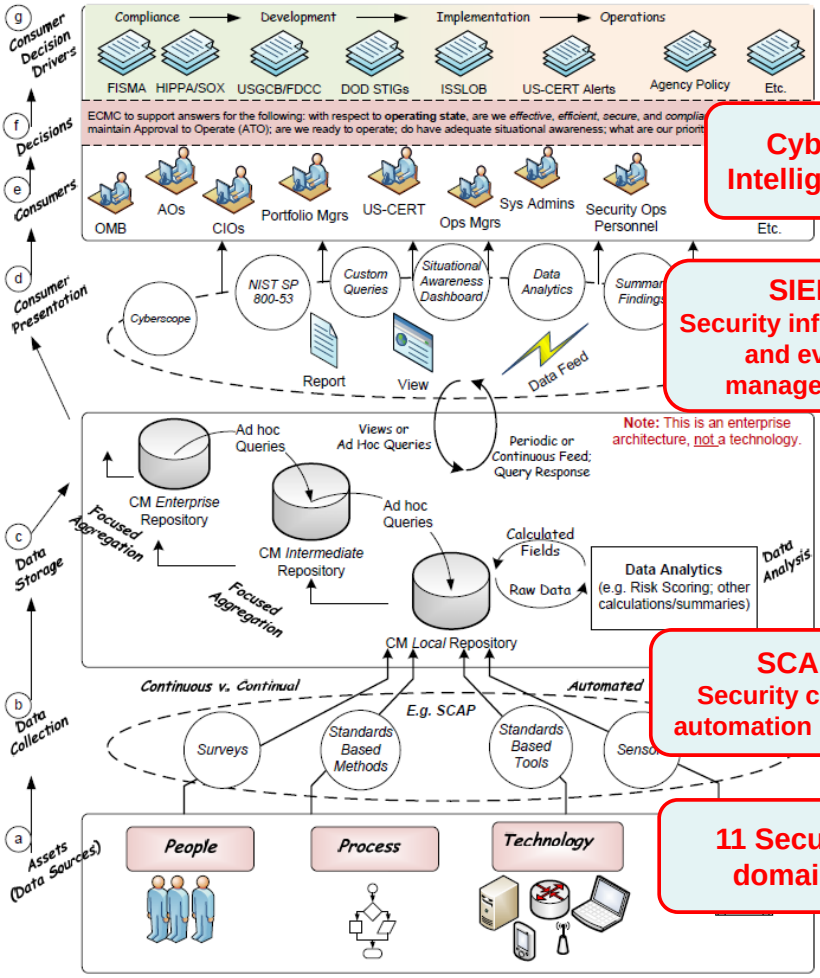
- ●統合自動化とダッシュボード機能：Security content automation protocol (SCAP)

Analysis
risk scoring

presentation
reporting

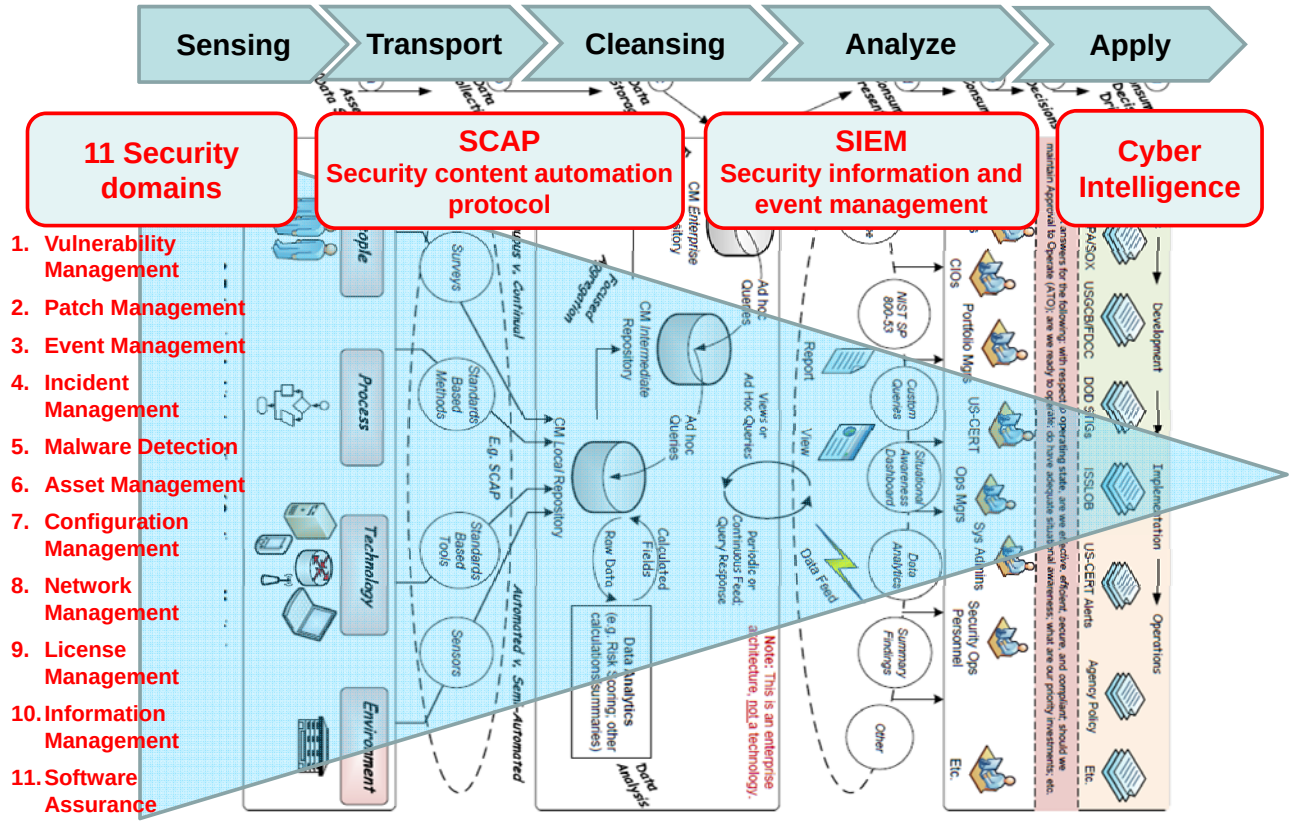
database

sensing



ISCM as Big Data Analytics

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY



Big Data for Security

明日の信頼を創ろう。
情報セキュリティ大学院大学
INSTITUTE of INFORMATION SECURITY

- 情報セキュリティは、Big Data Analyticsの重要な応用分野のひとつ
- 米国連邦政府の“Continuous Monitoring”は、そのチャレンジの代表例
- 異なる分野の多様なデータ形式の統合化技術が鍵

  SCAPからSIEMへ