エンタープライズ・リスク・マネジメント2009

# 減点評価から加点評価へのパラダイムシフト

## ～セキュリティリスクの見える化を通じて～

2009年 9月 4日

NRIセキュアテクノロジーズ株式会社

山倉　直

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# はじめに

NRI SECURE TECHNOLOGIES

- NRIセキュアテクノロジーズ株式会社

  ソリューション事業部　セキュリティコンサルタント　山倉　直

  - 中央官庁・大手民間企業を中心に、数多くの組織に対して、ポリシー策定やISMS構築といったセキュリティ・コンサルティング、およびセキュリティ監査やセキュリティ研修を実施
  - 自社（NRIセキュア）におけるISMS事務局を担当
  - 2002～2004年度にかけては、FISC安全対策基準の改訂委員を担当
  - JASA（日本セキュリティ監査協会）　技術部会WG1メンバー
  - ISO27001審査員、CISA公認情報システム監査人、システム監査技術者、CAIS公認情報セキュリティ監査人、会計システム専門監査人

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

1．セキュリティマネジメントにおける課題

2．課題解決の方向性

3．見える化による改善効果の事例

4．数値で見える化することによる効果

5．参考資料

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# セキュリティマネジメントにおける課題
## 対策疲れ

NRI SECURE TECHNOLOGIES

- セキュリティ管理における「対策疲れ」
  - 情報セキュリティ対策への取組みの効果が認識しづらい
  - 最低限これだけは取り組めば良いという事項が見えない
  - セキュリティへの過剰投資

また、「情報セキュリティ対策への取組みの効果が認識しづらい」ことも指摘されている。さらに、最低限これだけは取り組めば良いという事項が見えないことからセキュリティへの過剰投資が生じ、一部では「対策疲れ」の声も聞こえる。加えて、先進的企業と、規模が小さい企業の間において、意識格差が生じているのではないかとの懸念もある。

【出所】内閣官房情報セキュリティセンター「セキュア・ジャパン2008」

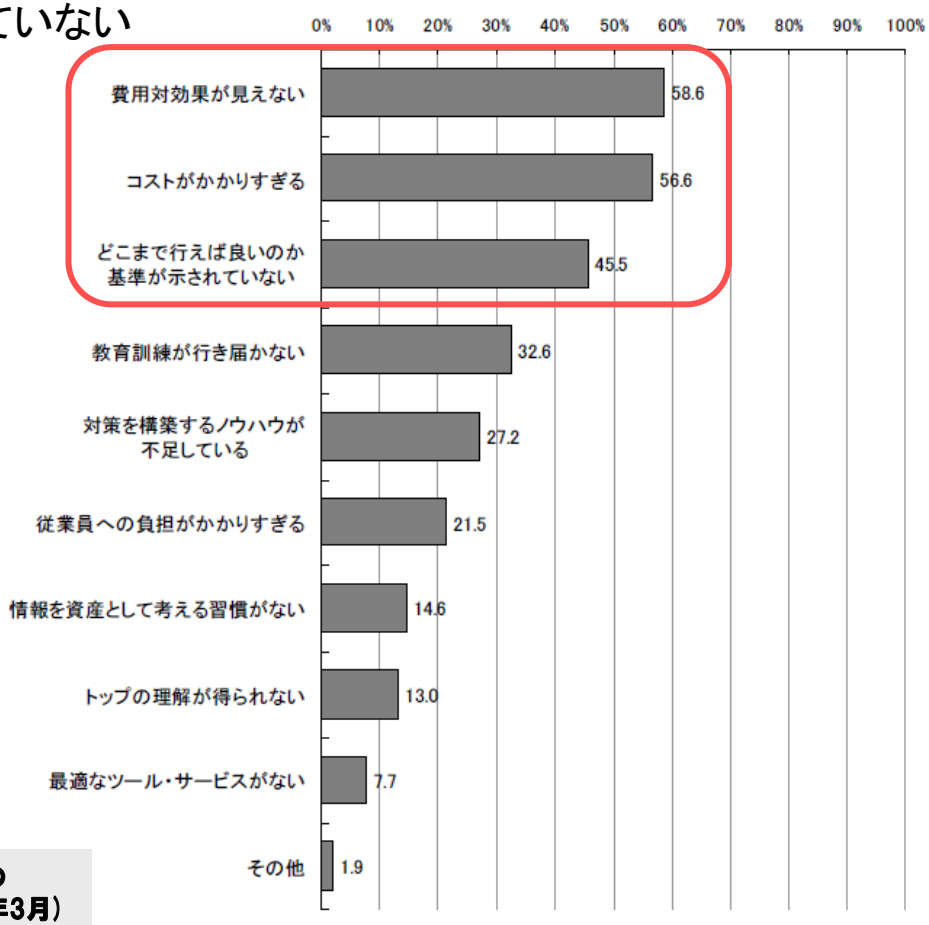
Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# セキュリティマネジメントにおける課題
## 対策疲れ（続き）

NRI SECURE TECHNOLOGIES

- セキュリティ対策実施上の問題点
  - 費用対効果が見えない
  - コストがかかりすぎる
  - どこまで行えば良いのか基準が示されていない

【全体】情報セキュリティ対策実施上の問題点 （MA、N=775）




【出所】警察庁 不正アクセス行為対策等の実態調査 調査報告書（平成21年3月）

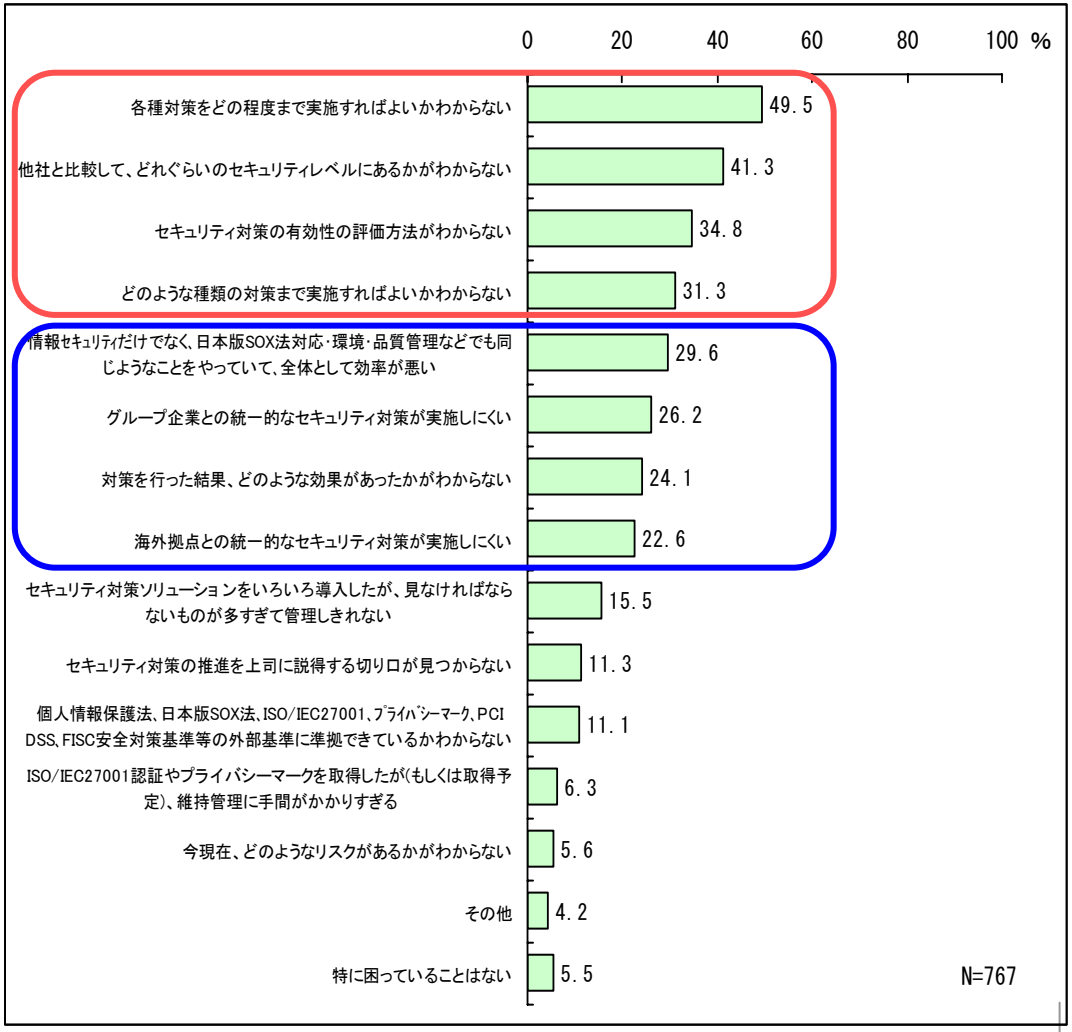
Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# セキュリティマネジメントにおける課題
## 対策疲れ（続き）

NRI SECURE TECHNOLOGIES

- **セキュリティ対策で困っていること**
  - どの程度まで実施すればよいかわからない
  - 他社と比較してどのレベルにあるかわからない
  - 対策の有効性の評価方法がわからない
  - どのような種類の対策まで実施すればよいかわからない

  - 日本版SOX法対応・環境・品質管理でも同じことをやっていて、全体として効率が悪い
  - グループ企業との統一的な対策が実施しにくい
  - 対策を行った結果の効果がわからない
  - 海外拠点との統一的な対策が実施しにくい




【出所】NRIセキュア　企業における
情報セキュリティ実態調査（平成20年11月）

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# セキュリティマネジメントにおける課題
## まとめ

NRI SECURE TECHNOLOGIES

**セキュリティ対策をやらなければならないことはもう常識になったが、ゴールや効果が見えないことが、現場のモチベーションを下げている。**

**【法制度の動向】**

- 個人情報保護法
- J-SOX

：

：

**【各企業の認識】**

- セキュリティ対策をやらなければならないのは、もう当たり前

**【事件・事故の動向】**

- 発生し続ける情報漏洩

しかし、

**【現状の課題】**

ゴールが見えない

効果が見えない

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

1．セキュリティマネジメントにおける課題

2．課題解決の方向性

3．見える化による改善効果の事例

4．数値で見える化することによる効果

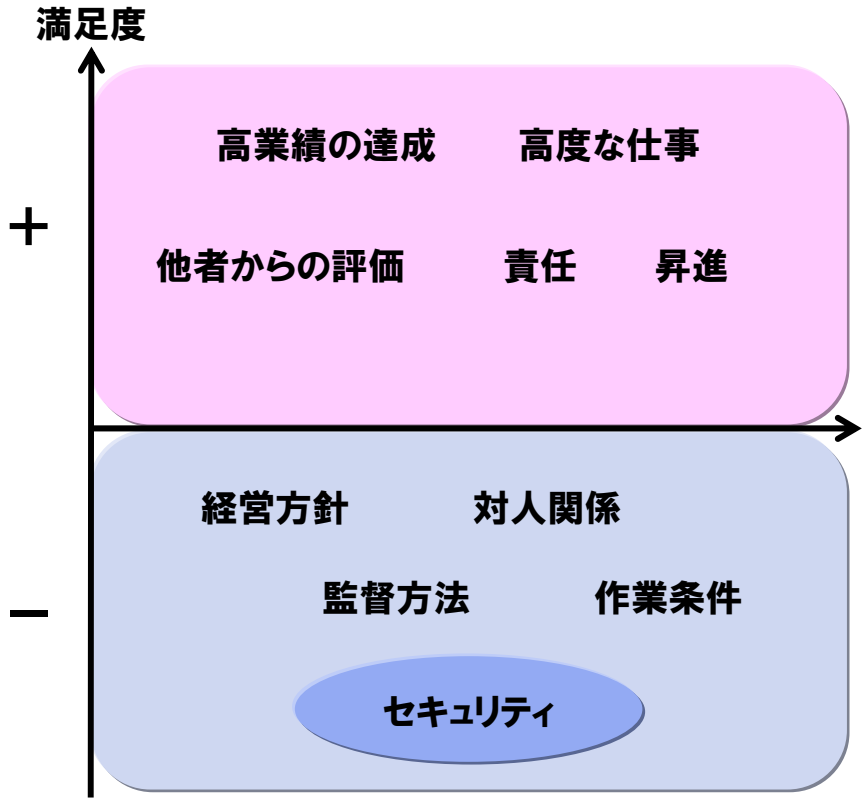
5．参考資料

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 課題解決の方向性
## 減点評価から加点評価へ

**セキュリティは不満の発生（事故の発生）を防ぐものではあるが、積極的な推進を引き出すものではない。**

- ハーツバーグの動機づけ理論




**動機づけ要因（満足要因）**

⇒成長したいという欲求を満たすもの

**衛生要因（不満足要因）**

⇒特に満足を高めるわけではないが、ないと不満を感じるもの

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 課題解決の方向性
## 減点評価から加点評価へ（続き）

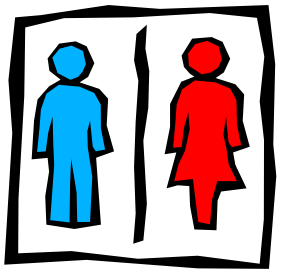
NRI SECURE TECHNOLOGIES

**ムチ（減点評価）だけではもう限界。**
**従来とは異なるアプローチが求められつつある。**

トイレを汚さないでください

どっちがやる気になるか？

いつもトイレをきれいに
使っていただいて
ありがとうございます



Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

1．セキュリティマネジメントにおける課題

2．課題解決の方向性

3．見える化による改善効果の事例

4．数値で見える化することによる効果

5．参考資料

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 見える化による改善効果の事例（1）

NRI SECURE TECHNOLOGIES

**内閣官房情報セキュリティセンター（NISC）で各省庁の対策状況を定量化し、結果を公開したところ、翌年度には各省庁の自主的努力で改善。**

## 端末及びウェブサーバに関する情報セキュリティ対策の総合評価

NISC

重点検査の項目

| 端末に関する重点検査項目 | |
|---|---|
| 不正プログラム対策 | ・OSのパッチ等の適用状況<br>・主要APのパッチ等の適用状況<br>・アンチウイルス対策ソフトの運用状況 |
| 情報保護対策 | ・モバイルPCの暗号化機能の運用状況 |
| 端末管理 | ・端末の物理的対策状況 |

| ウェブサーバに関する重点検査項目 | |
|---|---|
| 不正プログラム対策 | ・OSのパッチ等の適用状況<br>・ウェブサーバAPのパッチ等の適用状況等 |
| 不正アクセス対策 | ・不正アクセス対策状況 |
| 情報保護対策 | ・利用者に対する権限管理等の実施状況<br>・管理者に対する権限管理等の実施状況<br>・データ復旧対策状況 |

| 総合評価 | 端末 H18 | 端末 H19 | ウェブサーバ H18 | ウェブサーバ H19 |
|---|---|---|---|---|
| 内閣官房 | B | B | B | B |
| 内閣法制局 | C | B | B | B |
| 人事院 | C | A | B | B |
| 内閣府 | C | B | C | B |
| 宮内庁 | D | A | C | A |
| 公正取引委員会 | C | A | A | A |
| 警察庁 | D | A | B | A |
| 金融庁 | B | B | B | A |
| 総務省 | C | B | B | B |
| 法務省 | D | B | C | B |
| 外務省 | D | A | B | B |
| 財務省 | C | B | B | B |
| 文部科学省 | C | A | B | A |
| 厚生労働省 | D | B | B | B |
| 農林水産省 | C | A | B | A |
| 経済産業省 | C | A | B | A |
| 国土交通省 | D | B | C | B |
| 環境省 | B | B | B | A |
| 防衛省 | C | B | B | A |

・府省庁の調査に基づく結果
・平成19年3月末時点

| 評価 | 実施率 | 評価 | 実施率 | 評価 | 実施率 | 評価 | 実施率 |
|---|---|---|---|---|---|---|---|
| A | x=100% | B | 80%≦x<100% | C | 60%≦x<80% | D | x<60% |

| 上昇率 | 上昇率 | 上昇率 | 上昇率 | 上昇率 | 上昇率 |
|---|---|---|---|---|---|
| x>40% | x>30% | x>20% | x>10% | x>0% | x=0% |

【出所】
内閣官房情報セキュリティセンター（NISC）
政府機関の情報セキュリティ対策の実施状況に関する
重点検査及び評価結果について
～2007年度第1回重点検査の評価結果～
http://www.nisc.go.jp/conference/seisaku/dai13/pdf/13siryou04.pdf

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 見える化による改善効果の事例（2）

NRI SECURE TECHNOLOGIES

**某企業のグループ各社の対策状況を定量化し、**
**結果を各社にフィードバックしたところ、継続的にレベルアップ。**

- 概要
  - グループ全体のセキュリティレベル向上を目的に、グループ各社のセキュリティ調査を開始
  - 3年間にわたって調査を継続
  - チェック項目は約50項目
  - 事前に自己採点してもらったうえで各社を訪問し、インタビューとエビデンス確認を実施
  - 調査終了後に各社を再訪問し、現在のセキュリティレベルとして点数とランキング、今後の改善案をフィードバック

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 見える化による改善効果の事例（2）（続き）

NRI SECURE TECHNOLOGIES

- 実際に継続調査してみてわかったこと
  - 最低限の外圧（ムチ）は必要
  - 数値化による動機づけ（アメ）は有効
    - ✓ 達成すべき目標を明確に設定できる
    - ✓ 競争意識は、健全なモチベーション向上にも利用できる
  - どうしてもレベルが低いところだけ個別にフォロー

「他人事」から「自分事」へ
（当事者意識の喚起）

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 見える化による改善効果の事例（3）

NRI SECURE TECHNOLOGIES

## 他にも改善効果の事例あり。

- **概要**
  - 29社のIT部門長、セキュリティ担当者に対して、情報セキュリティガバナンスの実態をインタビュー調査

- **結果（インタビューの生の声）**

➢ 年１回のサイクルでPDCA

✓ 情報セキュリティも、組織のマネジメント活動の一つとして、年1回のサイクルでPDCAを回す。そのときの目標設定の仕方。あるいはアセスメントの徹底の仕方。社員、あるいは外部の人も含めた教育の徹底の仕方。いくつかの尺度を決めて、何がどこまでできているかということを、それぞれのところから出してもらって、組織間のバラツキを見ていく。自分はどのレベルにいるか。全体より下ならもうちょっとがんばってもらわないといけない。全体より上なら、さらにいいところを伸ばしてもらうという形にしないといけない。企業グループの中だけですが、そういう評価をして、少しでも見えるようにしていく努力をし始めている。

➢ 経営トップからのオーダーでモチベーションアップ

✓ グローバルでのISMSの統一認証を取るというのを、経営トップからのオーダーとして出したため、情報セキュリティに関する取り組みをやらねばならないというモチベーション、圧力がかかり、セキュリティ管理が進んでいる。

【出所】経済産業省　情報セキュリティガバナンス実態調査2008（平成21年3月）

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

1. セキュリティマネジメントにおける課題

2. 課題解決の方向性

3. 見える化による改善効果の事例

4. 数値で見える化することによる効果

5. 参考資料

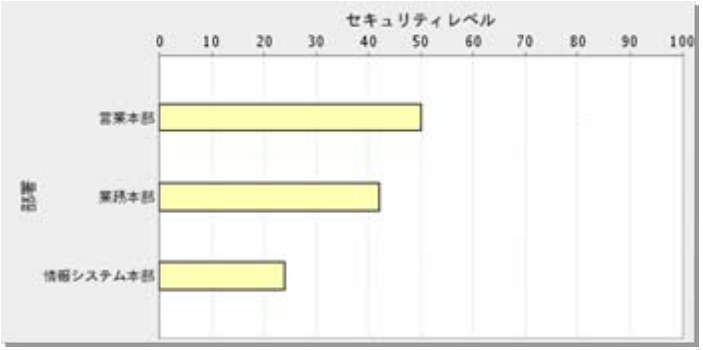
Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 数値で見える化することによる効果
## まとめ

NRI SECURE TECHNOLOGIES

**それぞれの立場でのモチベーション向上に利用できる。**

- モチベーションの向上
  - 推進役の全社セキュリティ管理部門が、経営陣に成果をアピール
  - 現場の推進役であるセキュリティ管理者は、他部署との競争意識からモチベーション向上
  - 現場の一般社員も、他部署との競争意識からモチベーション向上




**部署ごと、拠点ごと(国内外)、グループ会社ごと、外部委託先ごとに採点**

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 数値で見える化することによる効果
## まとめ（続き）

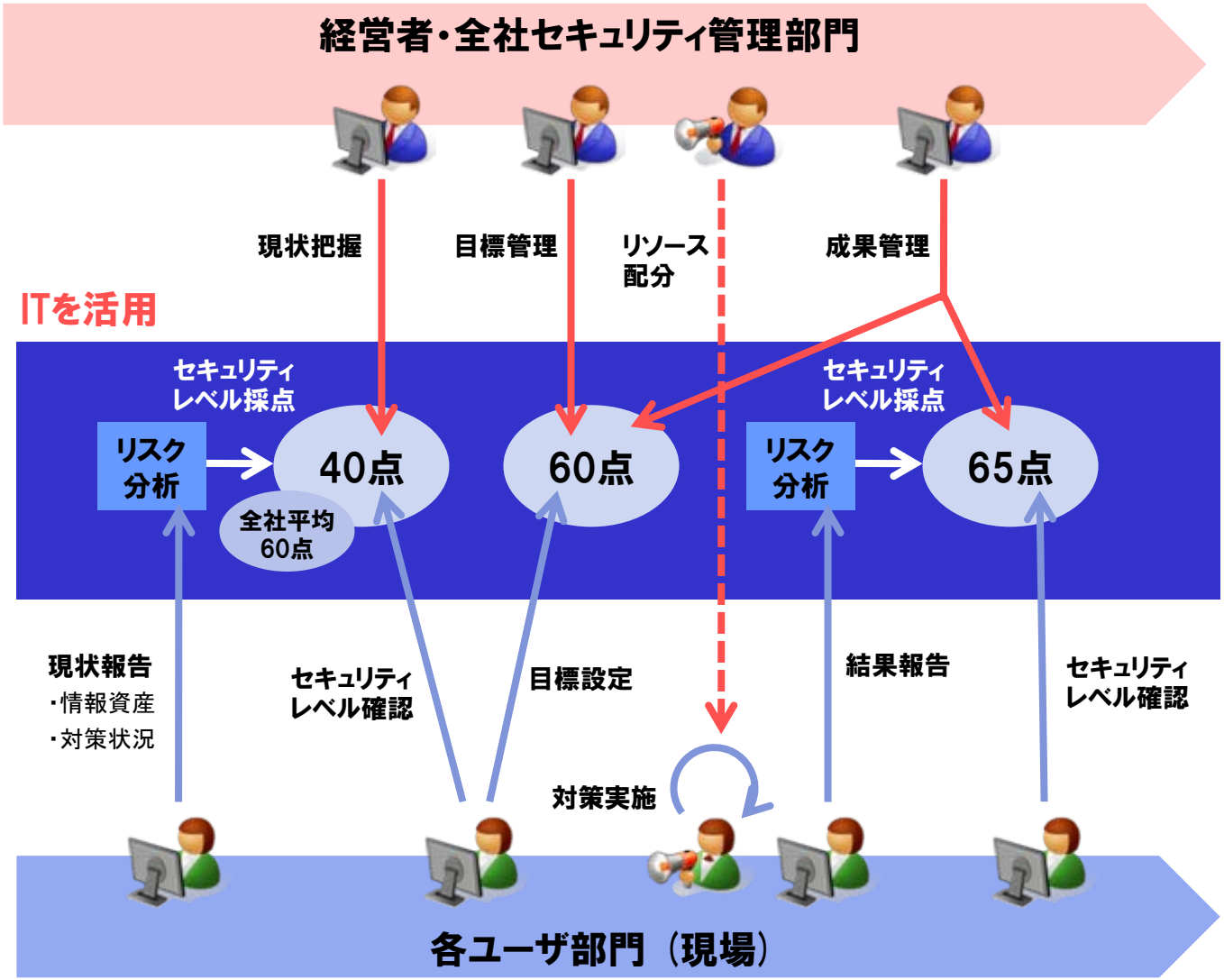
NRI SECURE TECHNOLOGIES

**「セキュリティ管理」という業務を、企業活動の1つとして評価できるようになる。**

- **経営のフレームワークの応用**
  - 経営における売上/利益に代わる指標として、現状把握だけでなく目標設定にも利用
  - PDCAサイクルの見える化による実効性向上
- **費用対効果の把握**
  - 点数の増減を効果として把握
- **他社との比較**
  - 外部の基準に対する準拠度（点数）を比較

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 数値で見える化することによる効果
## 経営のフレームワークの応用




現状把握や成果管理に注力
最適なリソース配分を検討

共通の基準でセキュリティレベルを定量化

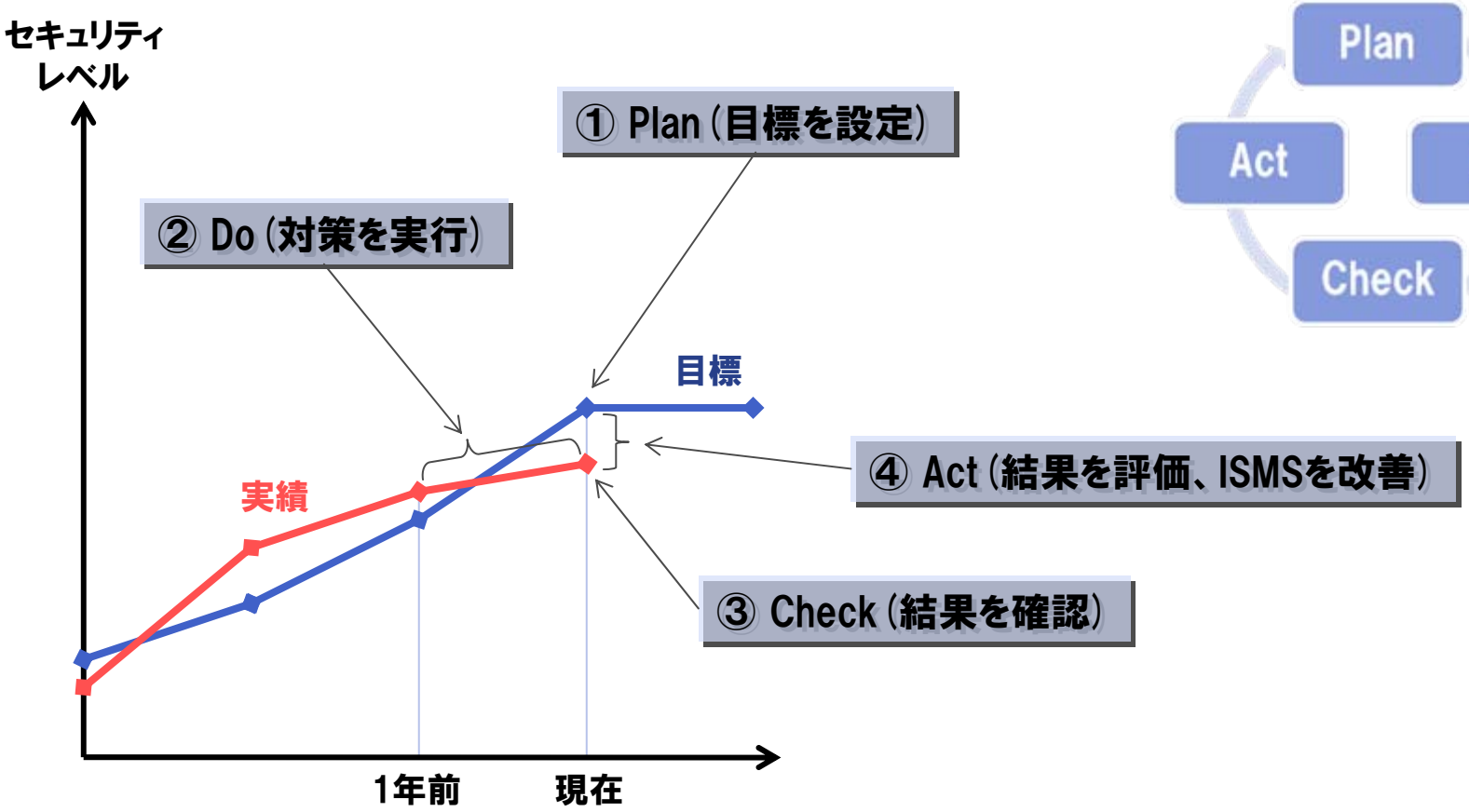
現場中心で対策を推進

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 数値で見える化することによる効果
## PDCAサイクルの見える化

NRI SECURE TECHNOLOGIES

**目標および現状をグラフ化することで、PDCAサイクルを見える化。**




Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

1．セキュリティマネジメントにおける課題

2．課題解決の方向性

3．見える化による改善効果の事例

4．数値で見える化することによる効果

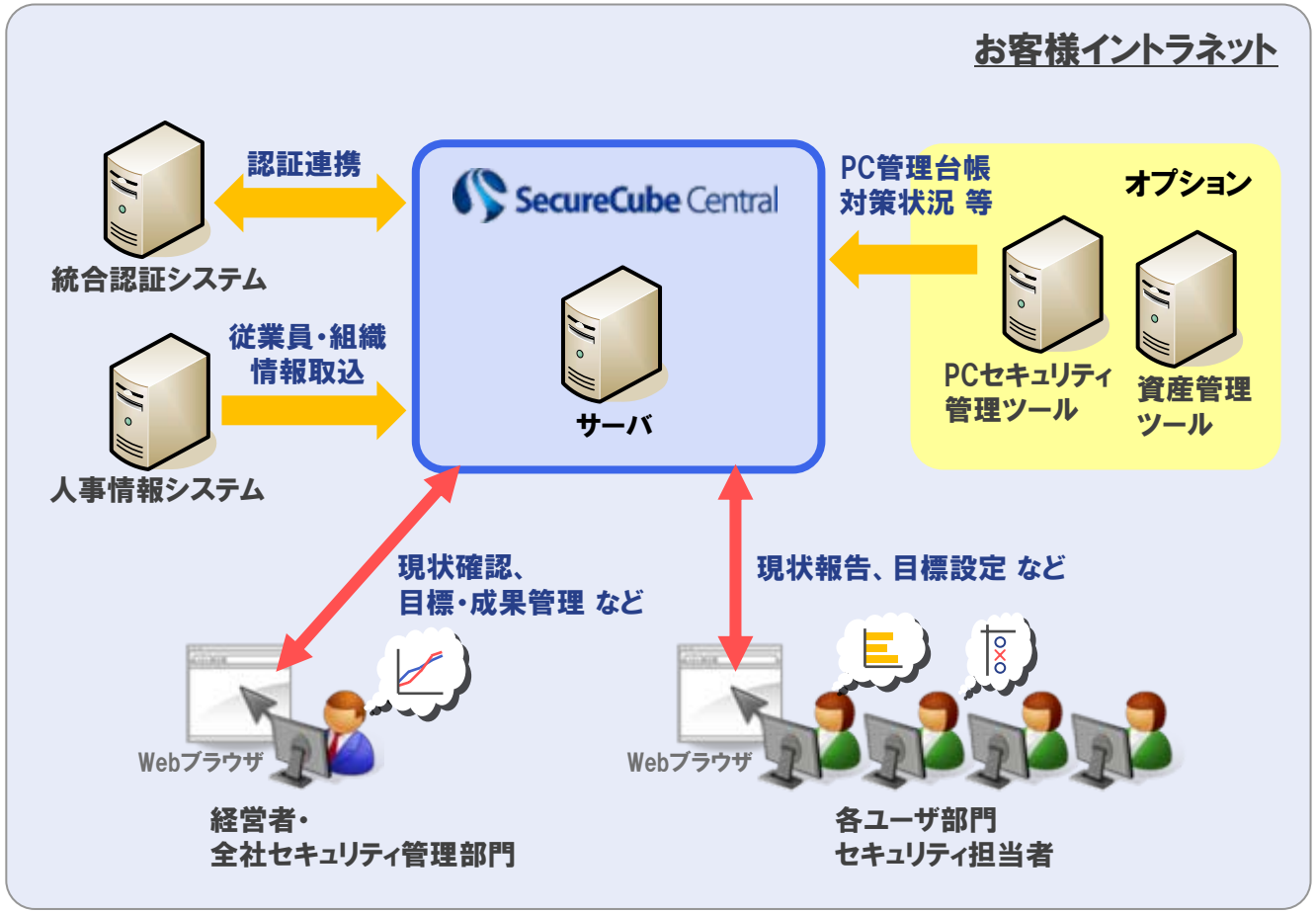
5．参考資料

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# SecureCube/Centralの概要

NRI SECURE TECHNOLOGIES

**既存システムと連携し、セキュリティマネジメントを効果的・効率的に運営するための業務アプリケーション・パッケージ。**




## ■ 特長

### ① セキュリティレベルの定量化

- 部門毎に対策状況やリスクを定量化
- 対策推進の目標・成果を数値で管理
- 担当者の成果を評価することにより、モチベーションを維持

### ② ISMSの効果的・効率的運用

- リスク分析や資産管理など、ISMSの構築維持に必要な業務をシステム化
- 現場中心でPDCAサイクルが回る仕組みを提供
- 効果的・効率的なISMSを実現する方法論を実装

### ③ システム化による大規模展開

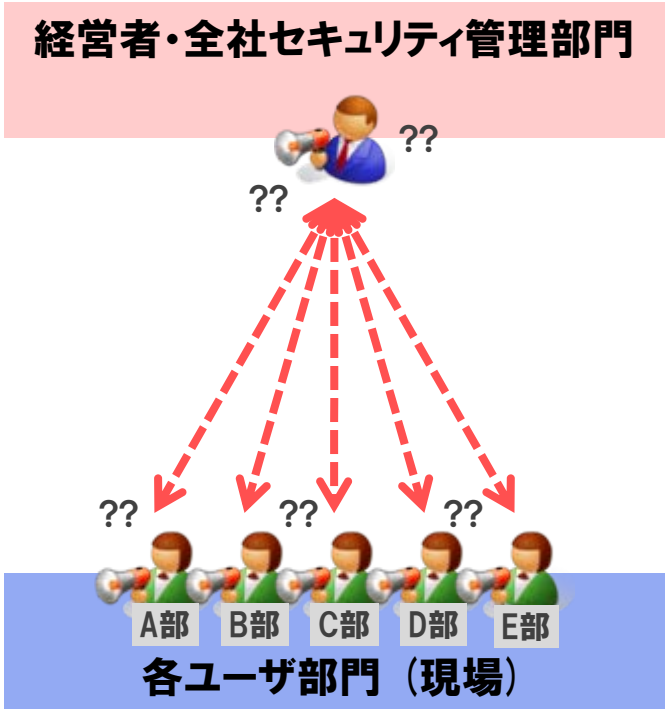
- 対策状況の収集・集計など、手間のかかる作業をシステム化
- 部門やグループ企業が多くても、業務が効率的に回る仕組みを提供

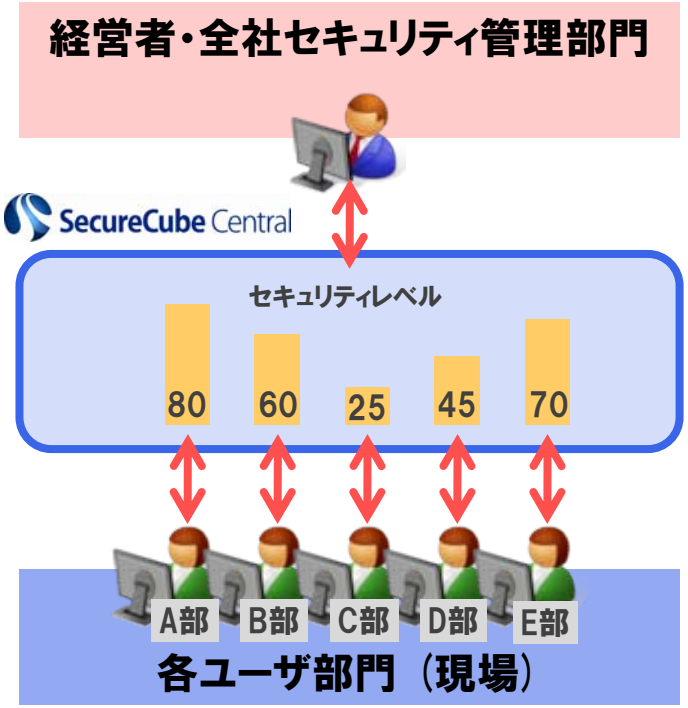
Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 導入効果

NRI SECURE TECHNOLOGIES

**各部門のセキュリティレベルを数値で「見える化」、各部門の目標・成果を管理。**
**大規模な組織でも、システム化により効率的な管理が可能。**






**課題**

- セキュリティの現状を、誰も把握できない
- 成果が評価されず、現場担当者のモチベーションが低下する
- 組織全体を管理するのに、非常に手間がかかる

**導入効果**

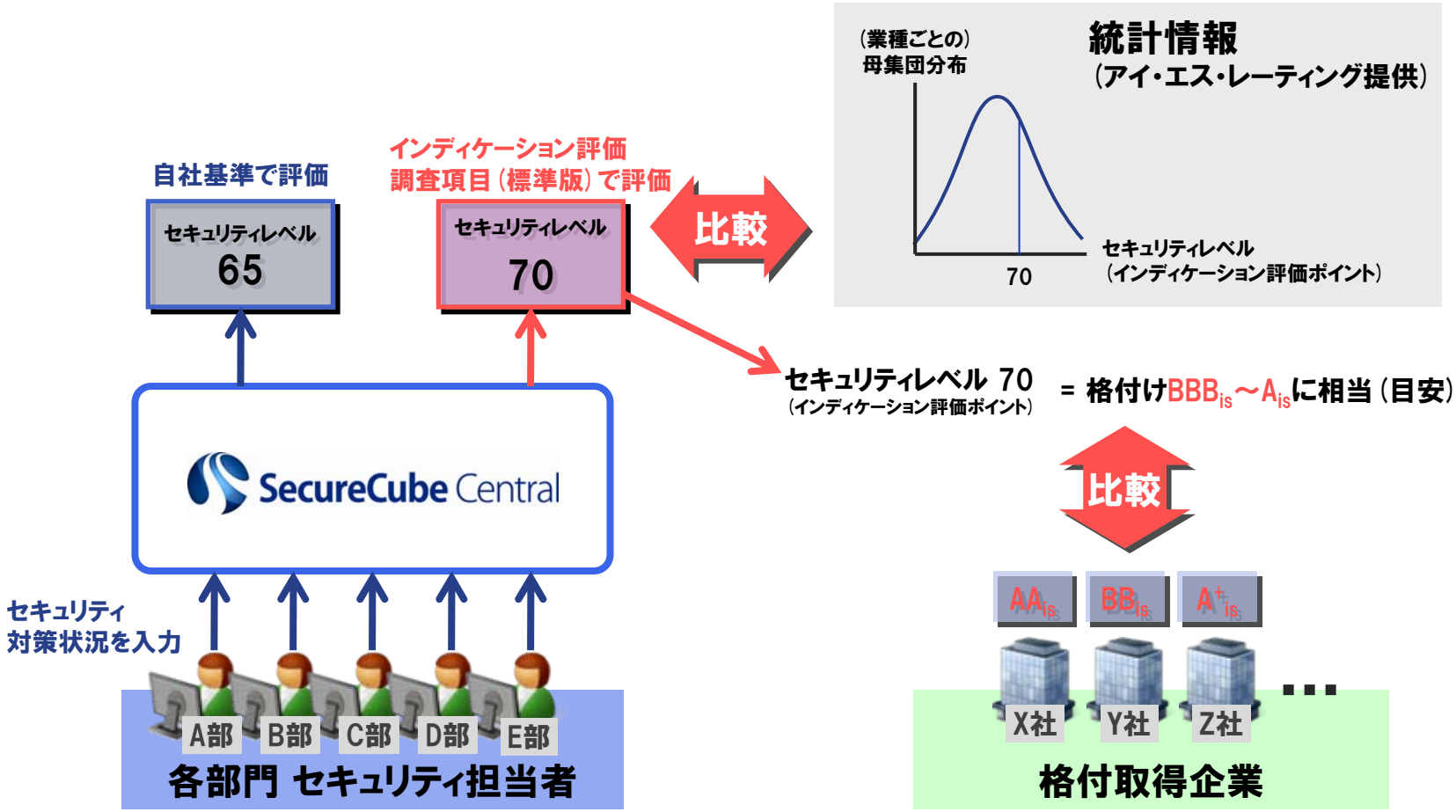
- セキュリティレベルが数値化され、誰でも一目で現状を理解できる
- 目標や成果が数値で管理され、現場のモチベーション低下を防げる
- システム化により、大規模な組織でも効率的に管理できる

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# インディケーション自己評価

NRI SECURE TECHNOLOGIES

**SecureCube/Centralにインディケーション評価調査項目（標準版）を取り込み。**
**他社とのセキュリティレベルの比較が可能に。**




Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# 謝辞

- ご清聴ありがとうございました
- ご意見・ご質問は、講演者までご一報ください

NRIセキュアテクノロジーズ株式会社
ソリューション事業部
山倉　直

yamakura@nri-secure.co.jp
03-5220-2858

Copyright©2009 NRI SecureTechnologies, Ltd. All rights reserved.

# NRIセキュアテクノロジーズ株式会社

〒100-0005　東京都千代田区丸の内1-6-5　丸の内北口ビル
TEL：03-5220-2022
E-mail：info@nri-secure.co.jp
ホームページ： http://www.nri-secure.co.jp/