ITガバナンスと
セキュリティデバイド

過去、現在、未来の流れの中で
セキュリティ有資格者に求められる
役割とは何か

講演者略歴

- 斉藤　孝明　Ph.D. , CISA, CISM, ISMS審査員補
  (saito@nekodasuke.jp)

- ～2006年　：　大学で情報系/心理系の教鞭
- 2006年～　：　総合商社にてJ-SOX立ち上げ
- 2008年～　：　大手スーパーにてJ-SOX立ち上げ
- 2011年～　：　鉄鋼商社にてJ-SOX再構築
- 2015年～　：　有名銀行にてITガバナンス

1.0 はじめに

新聞の投書例（らしい）

- 『クラウド』という言葉がわからないので娘に聞いたら、ググれと言われた

1.1 はじめに

- ITがすっかりコモディティ化（日常品化）した現在、もはやITを特別な存在と思う人はいない（多分）。

- 一方で、情報セキュリティ技術者と、それ以外の人々の間には、セキュリティ水準のギャップが見られる。

- セキュリティデバイドの恐怖の時代が到来する。

1.2 そもそもサイバーセキュリティとは？

サイバーセキュリティ基本法での定義

「サイバーセキュリティ」とは、
電子的方式、磁気的方式その他
人の知覚によっては認識することができない方式により
記録され、又は発信され、伝送され、若しくは受信される情報の
漏えい、滅失又は毀損の防止その他の
当該情報の安全管理のために必要な措置
並びに情報システム及び情報通信ネットワークの
安全性及び信頼性の確保のために必要な措置
が講じられ、その状態が適切に維持管理されていることをいう。

1.3 セキュリティデバイドとは？

- JNSA曰く:

  「事故に学びさらにセキュリティ対策を進化させ得る人や組織と、それができない人や組織との間の格差（**セキュリティデバイド**）が広がっているとの懸念」

  （2015セキュリティ十大ニュース）

- 【デジタルデバイド】【情報格差】

  国家間、もしくは地域間における格差
  学歴、所得など待遇面で生じる機会の格差
  加齢や障害の有無など個人間の格差

1.4 セキュリティ対策？

- CSIRT（インシデント対応チーム）を行う企業
- 厳重なアカウント管理を行う企業
- 厳重なネットワーク監視を行う企業
- 脆弱性管理を行う企業
- 従業員教育を行う企業

- 政府の後押し：サイバーセキュリティ基本法
- J-SOXの洗礼

実態はどうか？

不正アクセス行為の発生状況：総務省

1.5 セキュリティ対策？

- CSIRT（インシデント対応チーム）を行う企業

日本シーサート協議会参加チーム　：　126チーム

東証1部：約2千社

言い訳はいろいろあるでしょう

1.6 セキュリティデバイドとは？

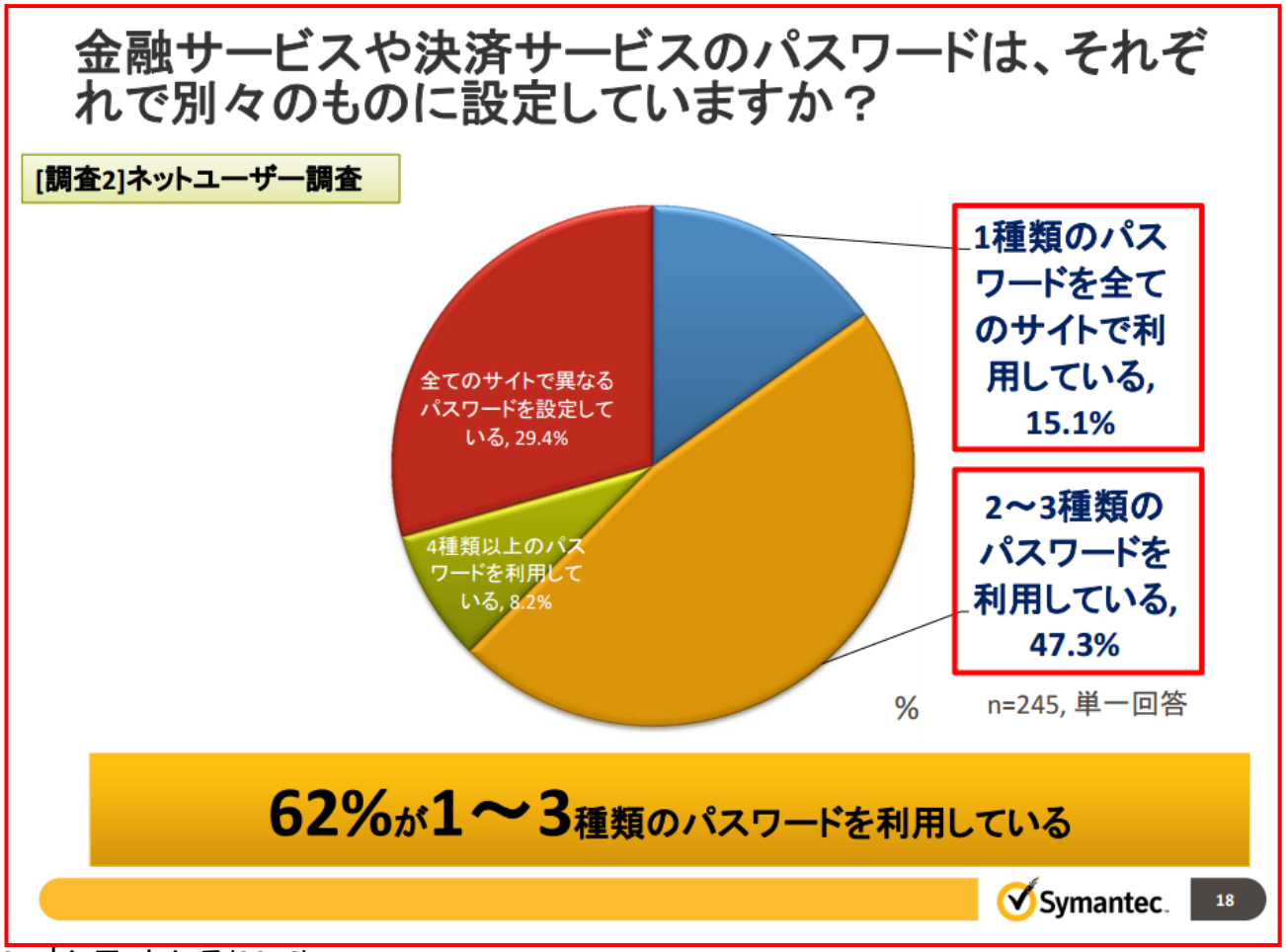
- J-SOXで、日本企業のITセキュリティは、COBIT4.1に準ずるフレームワークで、一定水準に達するはずだった。

しかし、2011年、J-SOXは一部緩和され、

ITセキュリティ的に
正しかったのか？

1.7 パスワードの流出

- 昨今、アカウント情報の流出は珍しくない。
- 約70%の人がパスワード使いまわし

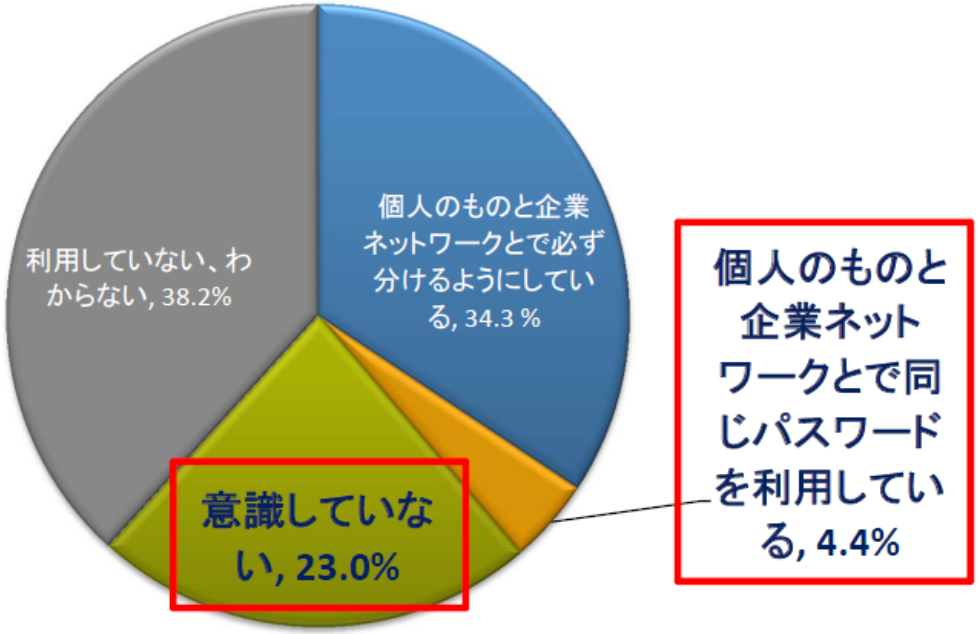


第4回東京支部CISMカンファレンス(2016)

「個人・企業のパスワード管理」に関する意識調査結果のご報告：株式会社シマンテック

1.8 会社と私用でパスワードを分けない

[調査2]ネットユーザー調査



% n=204, 単一回答

社内システムのパスワードを個人で流用している社員や意識していない社員が 27% いる

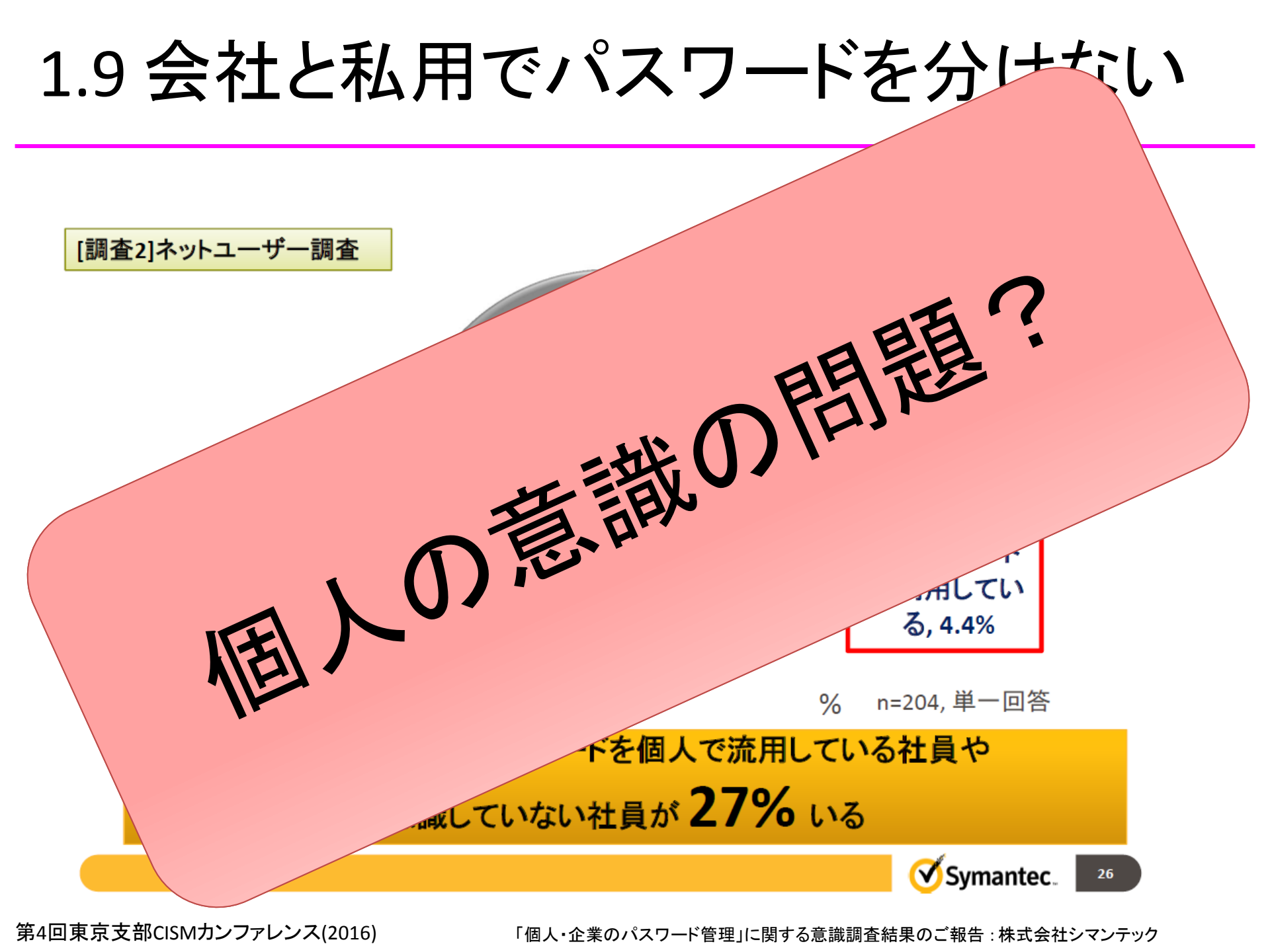
Symantec.

第4回東京支部CISMカンファレンス(2016)

「個人・企業のパスワード管理」に関する意識調査結果のご報告：株式会社シマンテック

1.9 会社と私用でパスワードを分けない

[調査2]ネットユーザー調査



「個人・企業のパスワード管理」に関する意識調査結果のご報告：株式会社シマンテック

1.10 セキュリティデバイドの古典/史実

パスワードの定期変更は有効か否か？という
ネット上の熱い議論を御存じであろうか？

パスワード定期変更に意味はあるのか？

1.11 セキュリティデバイドの古典/史実

- 十分な強度をもったパスワードを設定すれば、パスワード定期変更は不要

- 現実問題、十分な強度をもったパスワードを設定できない。
- 長く複雑なパスワードは、管理コストがかかる。

理想と現実のセキュリティデバイド？

従業員の能力が原因？

1.12　セキュリティデバイドの古典/史実

SQL インジェクション対策

古典の世界で
すよね

有名だよ？
未対策なわけ
ないよ

対策は開発規程
に明記されてる
はず

今どき
SQL インジェク
ション？

1.13　無くならないSQL インジェクション被害

SQL インジェクションの攻撃は衰えるどころか

- 2015年7月 : シャトレーゼ（食品) 21万件流出

なぜこんなことになるのか？

1.14　無くならないSQL インジェクション被害

IT現場の分業化の進行

- 昔の技術者は、サーバ構築からネットワークからプログラミングからDBチューンまで、全部を一人でこなした。

ITが高度化した今どき、
企業教育にそんな余裕は、無い

目先の技術
がやっと

1.15　ITの高度化がデバイドをもたらす

- クラウド
- GUI
- パッケージ
- 仮想化

中身を知らなくても使える

動けばいいんで
すよ（現場）

1.16　ITの高度化がデバイドをもたらす

- 自動車は、高度化と並行してコモディティ化（日用品化）した結果、一般の人は技術的に何もわからない。今や、

  『エンジンブレーキは買えますか？』

- これからもITの高度化・コモディティ化は進行する。
- 製作側・利用側ともに、分業化は進む一方。

セキュリティデバイドは進行する。

1.17 では、セキュリティデバイド対策は？

1. ユーザー/開発者への地道な啓蒙活動
2. セキュリティ専門家自身の日々是勉強
3. ガバナンス層への働きかけ

セキュリティは
金食い虫
との思い込み

2.0 未来を考える。

- 子供のころから情報機器が当たり前のように存在する世代　＝　デジタルネイティブ

未来を背負う若い彼らは・・・

2.1 デジタルネイティブの台頭1

- 生まれたときにWindow95があった世代が、大卒新入社員となる時代が到来した。

当然、CUIは知らない。

- 思春期には既にi-MODEがあった。

当然、ピーガーのモデムを知らない。

原理を学ぶ機会が乏しい

2.2 デジタルネイティブの台頭2

- １０年後、『メールは学校で習った』世代が大卒となる。

メール、という情報/手段の理解すらアヤシイ世代がやってくる（会社に）。

- メールとは何かを、会社でまた教育するのですよ。

2.3 デジタルネイティブの台頭3

- 約10年後、初めての携帯＝スマホ、通話＝LINE、という世代が大卒となる。

情報通信の基礎知識が全く必要ない世代

オンラインコミュニケーションに
慣れている！＝ITに長けている

2.4 デジタルネイティブの台頭4

- デジタルネイティブへの『セキュリティ教育』とは何か？

ITを駆使することに何の障害もない彼ら。
もし学校で教えることがあるとすれば、
・『正しい情報』の取捨選択方法

デマ、ゴミ情報が
多いから。

2.5 デジタルネイティブの台頭5

- デジタルネイティブの襲来
- IT高度化分業化の進展

同時進行している

3.1 NISCにおけるセキュリティデバイド

内閣サイバーセキュリテイセンターNISCは、
いま

http://www.nisc.go.jp/security-site/

3.2 NISCにおけるセキュリティデバイド

NISCよ、おまえもか。

- 高校生・大学生は、もはやメールを使わない。
- Webベースよりもアプリベース
- そもそも家庭で指導できない/するべきではない

家庭で親がITを子供に教えるって？

若者の傾向を理解できていない

3.3 セキュリティデバイドの背景とは

■企業内におけるセキュリティデバイド
- セキュリティ技術者、IT技術者、IT利用者

■企業間におけるセキュリティデバイド
- 資金力・社会的要請

■地域間におけるセキュリティデバイド
- 地域経済・自治体方針

■世代間におけるセキュリティデバイド
- 体力・時代背景

■情報教育におけるセキュリティデバイド
- 教師・学校

3.4 セキュリティデバイドの背景とは

格差要因

・教育/意識
⇒知っている、知っていない、の違いは大きい

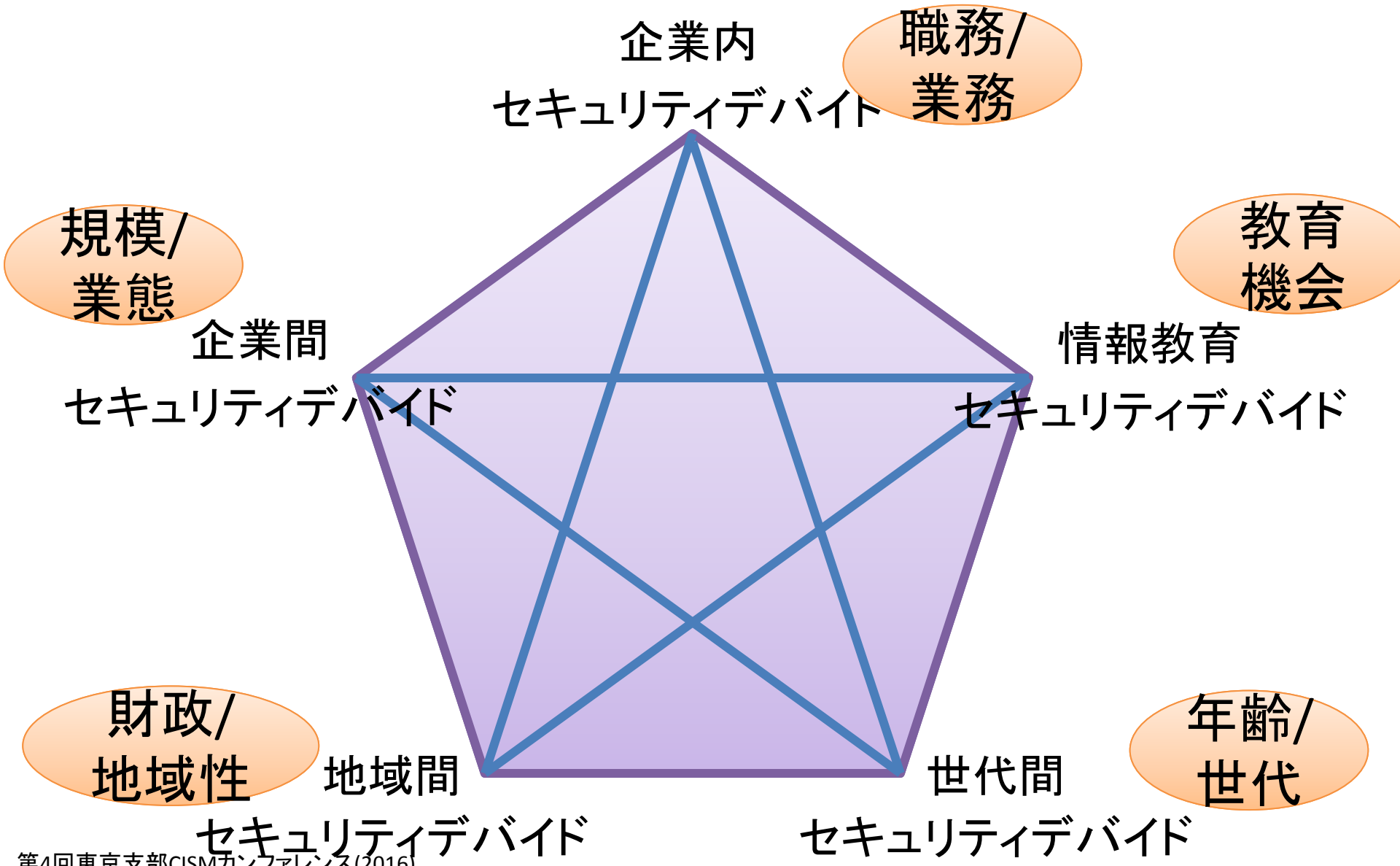
・資金
⇒安全にまわすだけのコスト負担をできるか

・社会的要請
⇒法人、大人は叩かれるが、子供は・・・。

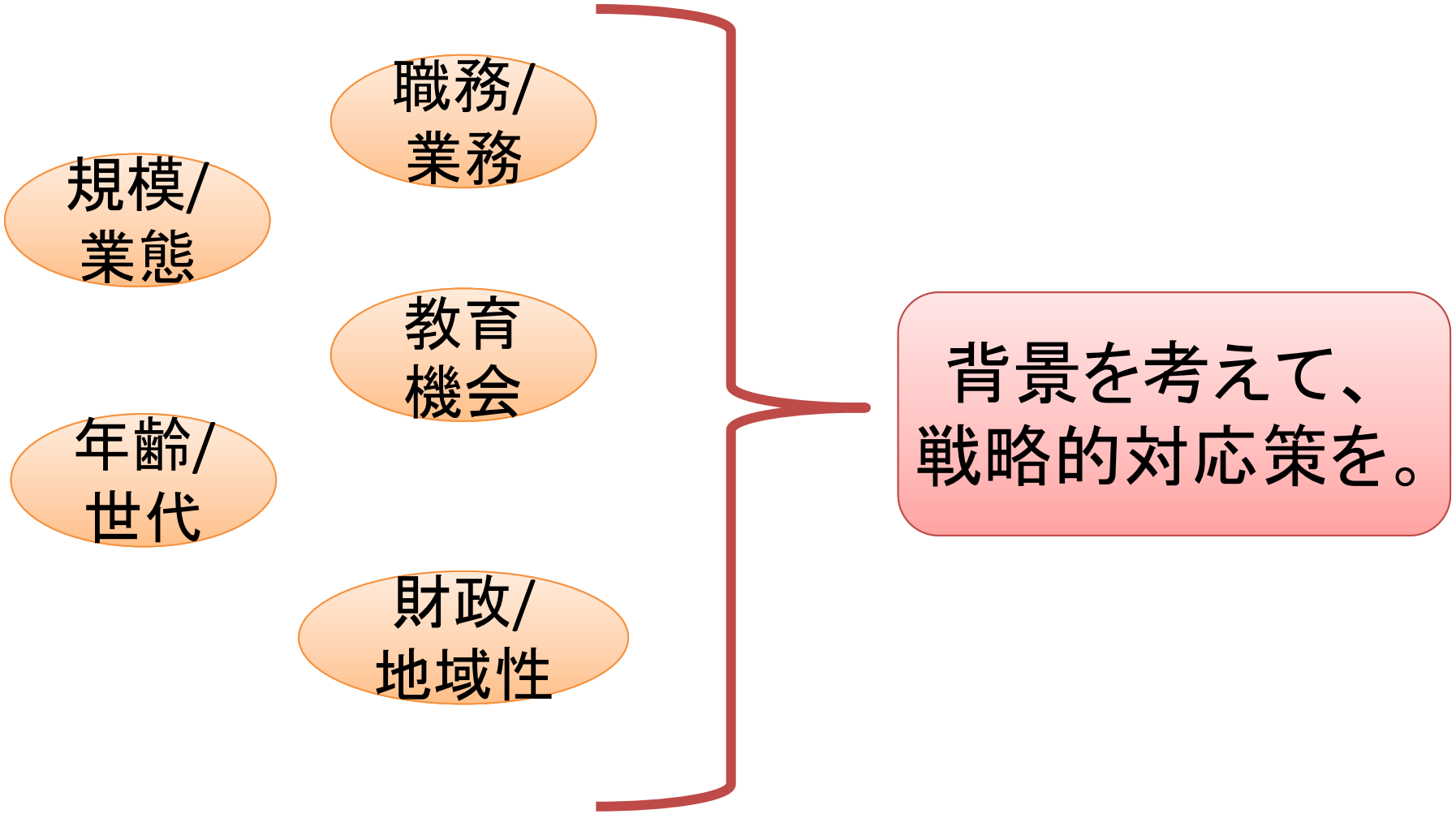
・視力 / 体力 / 脳力
⇒URLの文字の違いを識別するには、視力が必要。

・機会
⇒若いころにITに接する方がやはり有利？

3.5 セキュリティデバイドの背景とは



3.5 セキュリティデバイドの背景とは



4.1 セキュリティデバイドへの対策

- ITの利用機会は今後増えることはあっても減ることはない。
- IT自身、進化を続ける。
- 情報機器はWebベース/PCベースよりも、より背景技術が隠蔽される方向に進化する。
- IoTなど、まったく気づかれないものが増えていく。

セキュリティ人材が不足、
とよく言われるけれど

4.2 セキュリティデバイドへの対策

- 量（通常のセキュリティ）を稼ぐには、幅広いセキュリティ知識を、多数の人に。

継続学習が効果的

資格による動機づけが有効

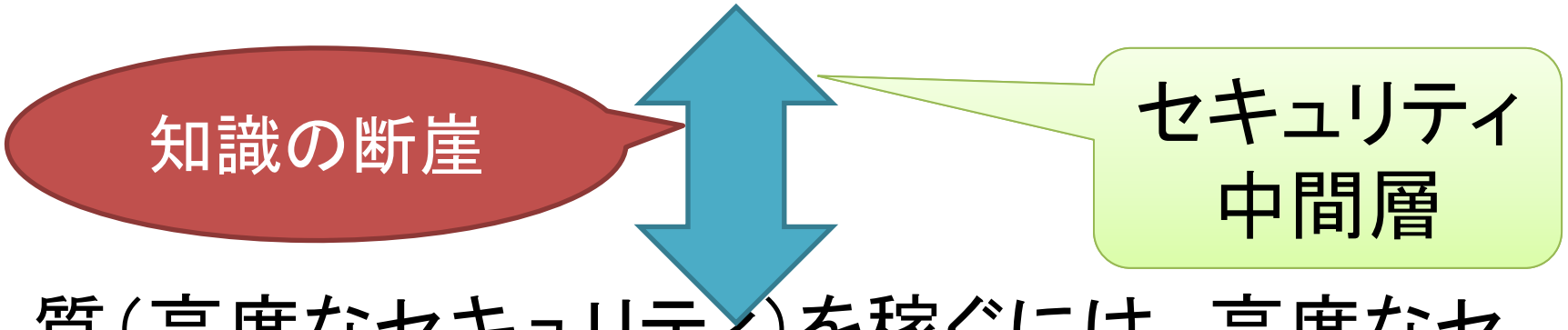
- 質（高度なセキュリティ）を稼ぐには、高度なセキュリティ知識を持ったスペシャリストに。

↑この辺は、勝手に発生する。

4.3 セキュリティデバイドへの対策

- 量（通常のセキュリティ）を稼ぐには、幅広いセキュリティ知識を、多数の人に。

継続学習が効果的



- 質（高度なセキュリティ）を稼ぐには、高度なセキュリティ知識を持ったスペシャリストに。

↑この辺は、勝手に発生する。

4.2

4.4 セキュリティデバイドへの対策

セキュリティ中間層への要求事項

- 幅広いIT専門知識 （超高度でなくて良い）
- 他者に教えられる
- セキュリティ関連技術の進歩に追従する

4.5 セキュリティデバイドへの対策

- セキュリティは進歩する。日々是勉強。

継続教育制度のある
CISMを
よろしくお願いします。

結語 1

- 『クラウド』という言葉がわからないので娘に聞いたら、ググれと言われた

『ググれる』 基礎教育（学校教育）と、

『クラウド』を扱えるだけのセキュリティ教育を。

使える、じゃないですよ

結語 2

- セキュリティデバイドは
  拡大する一方である。

セキュリティ有資格者が率先して対応を。

CISMです

参考文献

- サイバーセキュリティ経営ガイドライン: 経済産業省
  http://www.meti.go.jp/press/2015/12/20151228002/20151228002-2.pdf
- みんなでしっかりサイバーセキュリティ : 内閣サイバーセキュリティセンター
  http://www.nisc.go.jp/security-site/school/student.html
- 「個人・企業のパスワード管理」に関する意識調査結果のご報告 : 株式会社シマンテック
  https://www.jp.websecurity.symantec.com/welcome/pdf/password_management_survey.pdf
- 組織内部者の不正行為によるインシデント調査: IPA
  http://www.ipa.go.jp/files/000014169.pdf