情報セキュリティ
に関する意識向上に向けて

2015年5月29日

Hello, Future!

新経済連盟

Japan Association of New Economy

インターネットセキュリティWG

１．はじめに～本提言の目的・趣旨

当連盟は、下記の目的・趣旨に基づき、「インターネット・セキュリティWG」を設置し、ワーキンググループでの会員からの意見、有識者等へのヒアリング結果等を踏まえて、今回提言をとりまとめたものである。

■インターネットがイノベーションを生み出す社会基盤として拡大定着する中、日本の国際競争力向上のために日本企業の情報セキュリティのあり方について政府に政策提言を行う

1．はじめに～本提言の背景

セキュリティー対策は、企業にとって**売上、利益と同等の重要性**がある
→短期的な売上、利益にフォーカスしていると、対策が後手後手に。

例a）
米国企業の顧客情報とソースコードが不正アクセスを受けて流出。ユーザ名とハッシュ化PWのデータがネット上で公開されてしまう。米国のIT企業は、この事件を広く伝え、PWの変更を呼びかけた。一方、日本側の対応は鈍かったと指摘する声がある。

例b）
個人情報の漏洩により、図書券などを利用者に配布する事例も。多額の費用を計上する必要がある。

2. 有識者からのヒアリング等で抽出された現状の課題①

■基本的な考え方

・今までは情報を出さない＝守ることが中心となっていたが、それでは対応策に追われてイタチごっこに陥るだけ。従来のセキュリティは、外部からの脅威を防ぐという観点で構築。
・今の時代にITを活用せずして事業成長はありえない。したがって、**ITを積極活用**してどうビジネスを伸長させていくか、**その上で情報セキュリティをどう担保していくのか**考えていくことが重要。
・日本の多くの企業は、情報セキュリティに対して認識が十分でない。そのような状況では、**一歩間違えると事業成長の阻害要因**になりえる。例えば、ある企業では情報漏えいの観点からPC持ち出しNGとなっていて移動中や外出先でネットワークにアクセスできない。これにより、ホワイトカラーの3割の時間を奪っている。セキュリティに資するコストは昔ほどかからない。それより不適切なセキュリティ対策によって生産性を阻害していることのほうが問題。**前向きな議論のほうが情報セキュリティも浸透**していく。
・**セキュリティが単なる費用という感覚をゲームチェンジし、積極的な投資であると認識する必要**がある。
・我々は、**デジタルの世界で生活する最初の世代**。子供たちに、安全なインターネットの環境を渡していくためには、**セキュリティーの問題を解決しないといけない**。
・成長戦略に位置づけられる**IoTに対応するためには、セキュリティ対策への投資が必要**。

2. 有識者からのヒアリング等で抽出された現状の課題②

■システム活用等の課題

・セキュリティ対策を導入している企業でも、**一部の機能しか使っていない**企業も多い。ツールだけでハンドリングしようとするのはかえって手間がかかる。
・ログを収集しても**活用しきれていない**ケースも多い。
・知識面が劣るため、システムセキュリティを導入しているが**使いこなせていない**のが現状。
・日本企業は、ISMSの取得比率は高いが、とりあえずとっておけばいいとの意識もあるのも事実。
・具体的かつ定量的に、どれだけの方がセキュリティリスクの認識や過失経験があるかを把握することが必ずしもできていない。

■シャドーIT(注)への対応

(注)企業の従業員が、会社の管理下にないIT機器を業務活動に利用する行為や状態。

・シャドーIT問題に対応するには、①ポリシー策定、②運用、③監視、④サービスロックの4つが必要。
・経営者は、情報セキュリティに関する**社内の現状把握がそもそもできておらず**、シャドーITに関してどのようなリスクが存在し、それぞれのリスク度合いがどのようなものかについて**経営者自身が十分認識できていない**のではないか。

2. 有識者からのヒアリング等で抽出された現状の課題③

■社内の意識改革・教育

・テクニカルな対処、ツールを活用した対処だけではなく、**企業内関係者(経営者、情報システム部職員、一般従業員等)のセキュリティに対する意識や知識の向上が重要**
・特にベンチャー企業ではセキュリティについての意識や知識が必ずしも十分でない場合が多く、教育が必要。
・セキュリティ教育は、入社時だけでなく**定常的に社員教育を行う**ことが必要。
・セキュリティリスクや管理の必要性について**分かりやすく伝える**ことで教育することが必要。
・**約1割のデータベース管理者が内部不正を行う可能性があることを示唆するアンケート調査**もある(※)。悪行を働いたときの危険度やインパクトをきちんと認識していない。
・**何をやったらクリティカルなのか**従業員が必ずしもきちんと分かっていない。
・開発部門において人員が増えると、セキュリティ教育も必要。**試験等の教育の展開が必要**。
・スキルのあるエンジニアに基礎的な教育を行わせるわけにも必ずしもいかず、**おしなべて教育を開発現場に施すことには難しさ**がある。
・アプリなどのクライアントエンジニアが増えていく中で、**サーバとの通信のセキュリティに関して必ずしも十分な知見がない**場合があることが課題

※引用元
2014年9月10日　データベース・セキュリティ・コンソーシアム「「DBA1,000人に聞きました」アンケート調査報告書」26頁
Q:将来、データベースに格納されている情報をこっそり売却するかもしれない→A　そう思う3.6%、ややそう思う7.1%
http://www.db-security.org/report/dbsc_dba_ver1.0.pdf

2. 有識者からのヒアリング等で抽出された現状の課題④

■セキュリティ人材の育成・確保

・現状セキュリティ人材が不足している。その理由は二つである。ひとつは、本業が大変でセキュリティに割く**リソースがなく**、ないがしろにされやすい。2つ目は、**経営層の理解が不足**している。
・依然として**「給料が上がらない」「採用時にアピールするとハッカーと思われる」**等のネガティブな理由が存在するため、**人材が育つ土壌がない**。
・ある企業の女性のセキュリティ担当の方がこの分野を志した理由は、セキュリティで活躍する女性ものの小説を読んで影響を受けたからという。このように**セキュリティ分野でのロールモデル**があってもいいのではないか。**若手人材の表彰**も必要。
・人材を育てていくためには、待遇面やかっこよさといったイメージの改善が必要。
・現状は、**働き先(セキュリティ人材の受け手)が不足**していることも課題。
・最近では、アウトソーシングでセキュリティ専門の会社も生まれている。**クラウドやアウトソーシングを活用**することも考えられる。
・セキュリティは敷居が高い。**セキュリティを翻訳して経営層に伝える人材が必要**。
・**セキュリティ技術者のコミュニティを拡充**させる必要がある。
・セキュリティは**最新知識が必須**。現状の情報処理技術者試験は受かればそのまま。
・**世界の企業は、急速にセキュリティ人材確保に動いている**。**グーグル**は、セキュリティやプライバシーを担当する人員の数を直近で**約500人まで拡充**（2015年3月30日　日経ビジネスオンライン「サイバー犯罪の未来は明るい？」より抜粋）

2. 有識者からのヒアリング等で抽出された現状の課題⑤

■経営層の理解

- 日本では、**CIO**(Chief Information Officer)、**CISO**(Chief Information Security Officer)と**いうポジションを設けている会社がほとんどなく**、現状では、情報システム部門にほぼ任せきりの状態。
- 今後のセキュリティの強化・発展にはCIO、CISOというポジションが必要。また、日本では、**セキュリティ担当者の地位向上も必要**。
- 諸外国では、CIOやCISOの人材を抱える専門のエージェントが各企業に人材を提供する枠組みがあり、これらの人材が各企業を転々としている。全体としてセキュリティ担当者の地位が高く評価され、浸透している。**人材確保として外部機関を利用することも必要。**

2. 有識者からのヒアリング等で抽出された現状の課題⑥

■インターネットセキュリティをめぐる技術的見地からの課題

・**アプリケーションの敷居がさがっている**。
・ネイティブアプリ全盛下にあってクライアントサーバを活用する機会が増えている。このことによって引き起こされる**脆弱な実装の上に、脆弱な通信や認証**が増えていることが課題。
・上記のトレンドは大きな流れとして食い止められない。セキュリティの仕組みやフレームワークを定着させるように**準備しておく**ことが重要。
・今後の**サイバーリスクはIoTで多く起こる。**

■利用者への啓発活動

・「ストップ・PW使い回し」等の**キャンペーンをこれまで以上に官民連携して進めていく必要。**
・一般のセキュリティーソフトだと期限切れがきたときに、更新しないので、そこが穴になる。
・プレインストールをしているソフトで、期限切れがきても、期限内と勘違いしている人も多い。

2. 有識者からのヒアリング等で抽出された現状の課題⑦

■社内セキュリティ体制の構築について

・エンジニア同士で「こういうコーディングではリスクが内在してしまうのではないか？」といった**議論ができるチームは自然と強い**。
・まずは、ISO27000の認証を取得。情報セキュリティに関する社内委員会を設置。社員に対しては、Webトレーニングを実施。
・社内講習会、テスト、擬似訓練等を実施。

【参考】ヒアリングにご協力いただいた主な方々

■fjコンサルティング株式会社　代表取締役CEO　瀬田陽介様

■エムオーテックス株式会社　代表取締役社長・河之口達也様、執行役員・中本琢也様

■グリー株式会社　執行役員常務CTO開発統括本部長・藤本真樹様　ほか

■シスコシステムズ合同会社　代表執行役員社長・平井康文様(当時)、専務執行役員・木下剛様

■ソースネクスト株式会社　取締役常務執行役員　青山文彦様　ほか

3. セキュリティ対応に関する日本と外国企業の差①

■OWASP　CISO調査2014（※）の解析結果

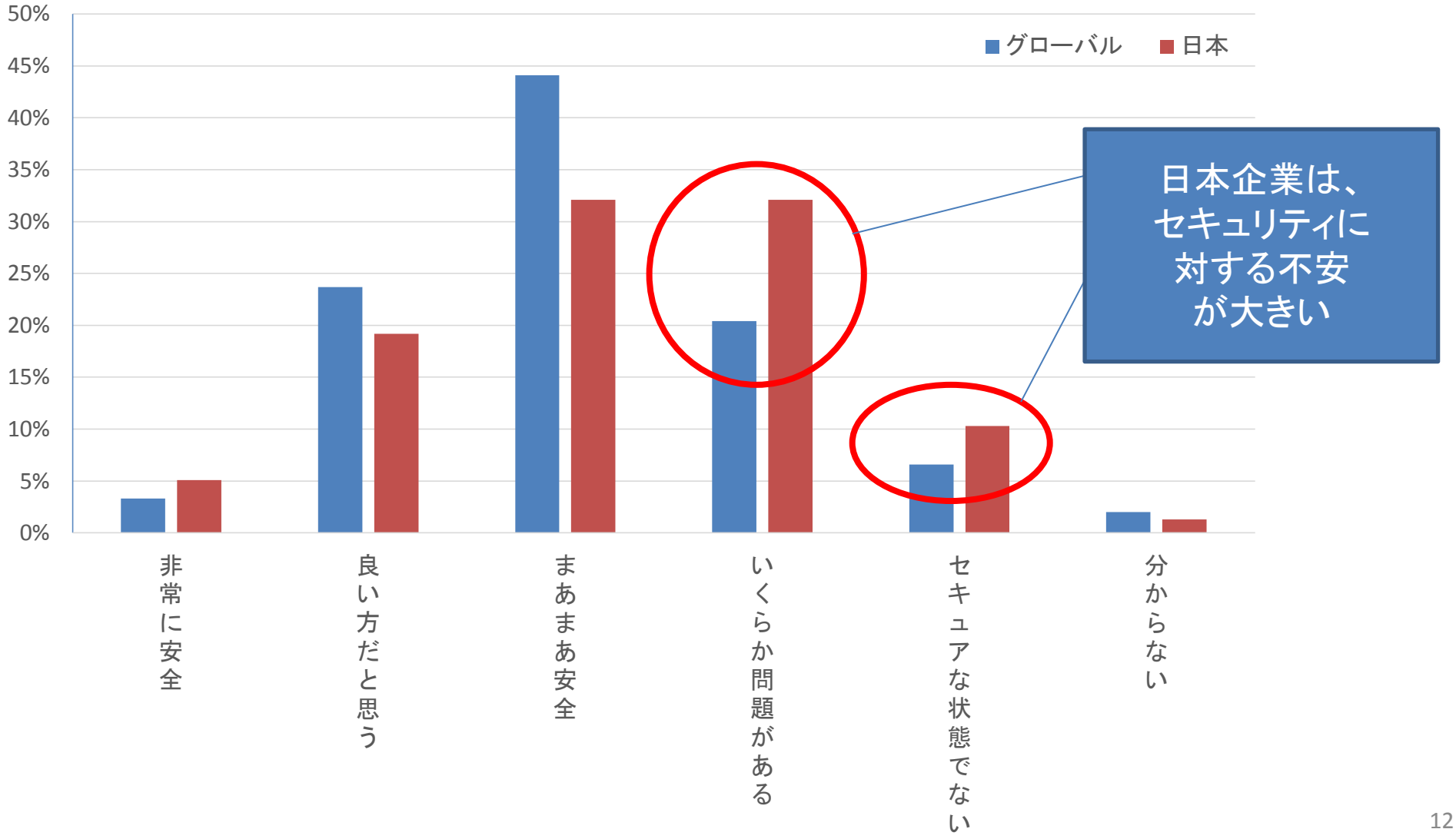
・日本企業は、**漠然とした不安**があり問題はありそうだと多くの企業が確認をもてないでいるが、**詳細にリファレンスなどを用いて調べることに踏み込めていない**。

→**日本企業は、セキュリティ対策に対する全社的な認識が十分ではないのではないか。**

※1　OWASP CISO調査2014
　OWASPが実施する、企業・団体の情報セキュリティ担当の責任者を対象としたグローバルのインターネットセキュリティの調査
※2　OWASPとは
　OWASP(The Open Web Application Security Project、読み方：オワスプ)は世界中のセキュリティプロフェッショナルが国家・組織の壁を越えて集まり、ソフトウェアのセキュリティを向上させるためのソフトウェアツール、ガイドライン等を議論・集約・成果を発展させる活動をしているコミュニティ団体。日本では、2011年よりOWASP Japanチャプターが発足し、現在までに定期的な会合やカンファレンスにのべ3,000名の技術者が集まっている。

3. セキュリティ対応に関する日本と外国企業の差②

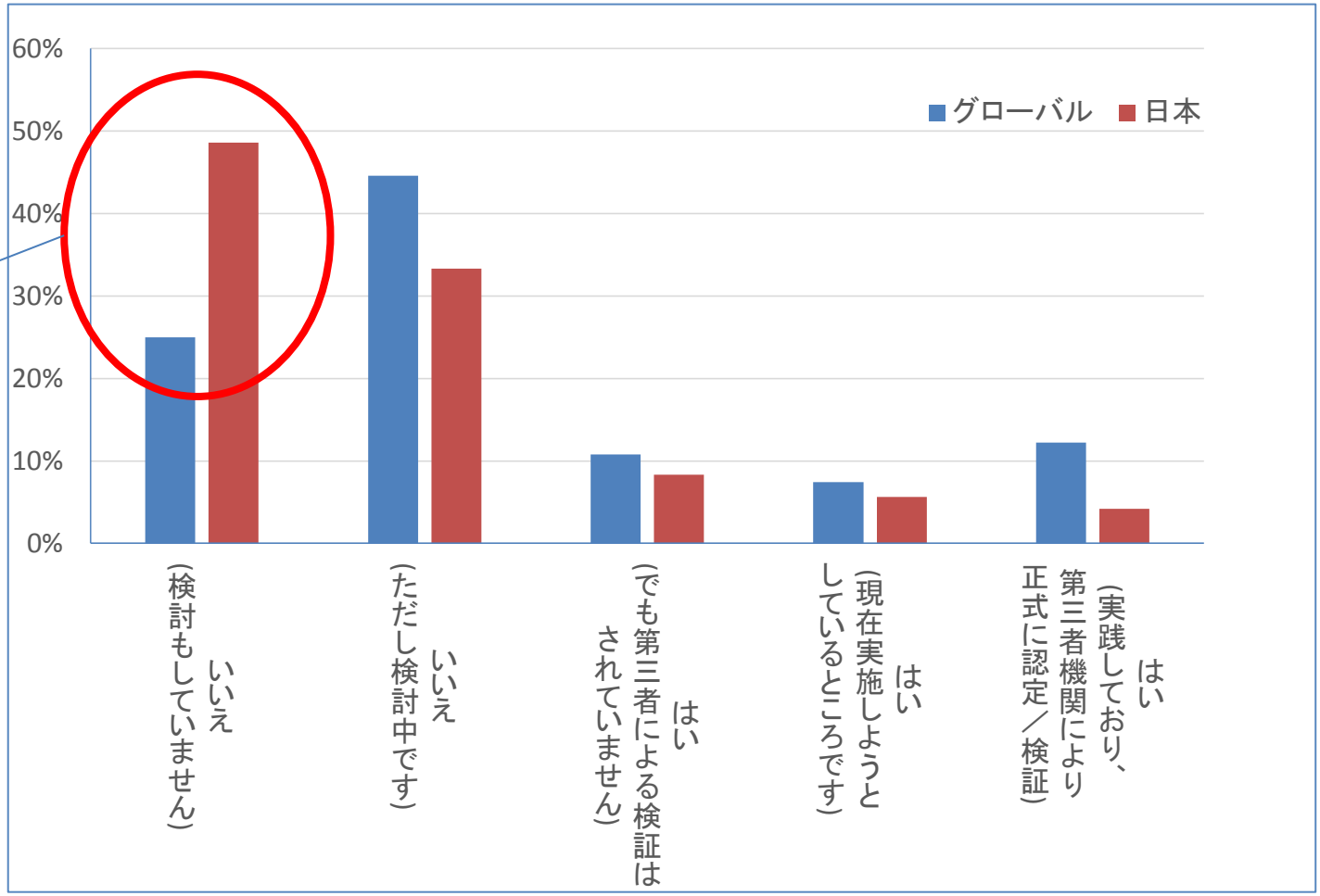
Q: サイバーセキュリティに関するリスクへの対処方針にどの程度の自信・確信がありますか？



3. セキュリティ対応に関する日本と外国企業の差③

Q: 貴社は、アプリケーション・セキュリティ・マネジメント・システム（ASMS）、または、アプリケーション・セキュリティを包括的に管理する成熟度モデルによる統合を実践してきましたか？

日本企業の方が、セキュリティ対策への意識が相対的に低い



4. 提言①　企業ボードメンバーのセキュリティの認識に関する意識改革

目標1

企業ボードメンバーによるセキュリティ対策に対する意識を向上し、当該対策に必要な経営資源を振り向けるようにする

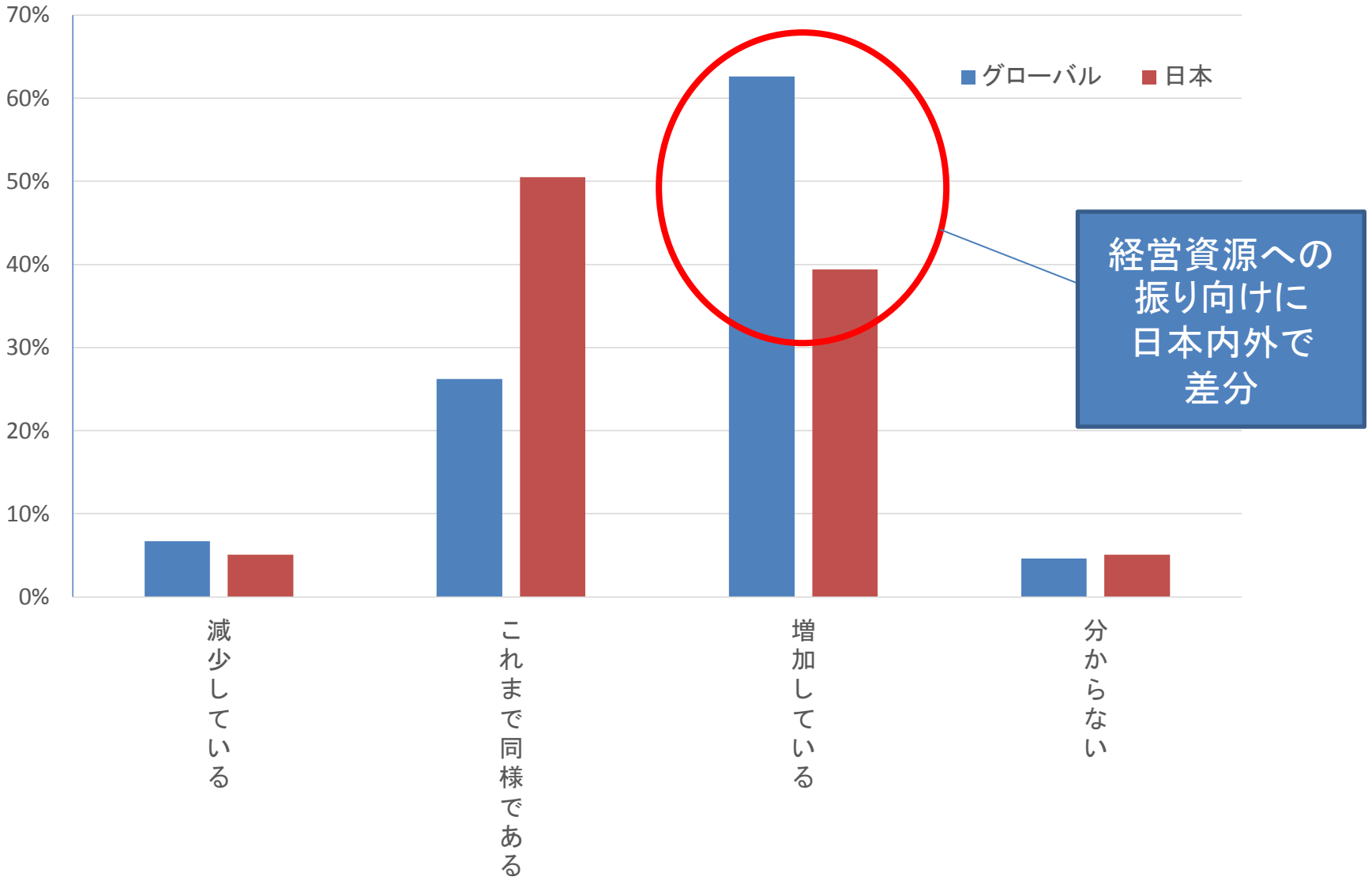
（現状）①「情報セキュリティの重要性を積極的に訴えかける役員クラスのリーダーがいる」と回答した企業は、世界全体では64%であったのに対し、日本企業の回答は41%（※）
②昨年1年間の情報セキュリティ投資額は、世界全体平均の年間4.2億円に対して、日本企業の平均は、年間2.1億円と半分

目標1を達成するための具体的施策	①官民連携による**啓発活動**の実施 ・**民間企業CEO参加によるセキュリティ会合**の開催 ・**ストーリー・テリングを活用して共通目標を設定する手法の標準化と横展開**（セキュリティ事故が自社の売上利益にどれだけ影響を与えるかなどを経営層に認識してもらうとともに、社内関係者間で対立構造を乗り越え共通の目標を設定する手法を開発する。また、その手法や成功事例を各企業へ展開していく）
	②各企業のセキュリティー施策を**IR情報**に盛り込むことを促進 ・各社の**セキュリティー施策を有価証券報告書等に記述して公開を検討**

（※出所）2014年11月5日公表の「グローバル情報セキュリティ調査2015」（プライスウォーターハウスクーパース㈱）より抜粋

【参考】 セキュリティ投資に関する動向（OWASP　CISO調査2014より）

Q: 貴社の情報セキュリティの全般的投資について最も良くあてはまる状況はどれですか？



4. 提言② セキュリティ対応人材育成その1

目標2

IT分野全般及びセキュリティに関する幅広い知見・技術と倫理観をもったセキュリティ人材の養成と地位向上

目標2を達成するための具体的施策～その1～	①**IT分野全般及びセキュリティ教育**の充実 ・高校・大学でのIT分野全般及びセキュリティに関する**高度な教育の充実** ・各企業でのセキュリティ教育実施のための**経費補助、税制支援の検討**
	②**セキュリティ人材が就職でき正当に評価されるようにする（就職・雇用改革）** ・産業界におけるセキュリティ人材の**積極採用及び採用に対する税制支援の検討** ・経済産業省の**未踏IT人材発掘育成事業出身者など**優秀なセキュリティ人材について、官民連携による**積極的な広報・育成支援強化** ・能力の客観的指標作成(**セキュリティ版TOEICの実施**)と企業内積極活用 ・**国家資格の創設**と企業による**当該資格保有者の積極採用**の支援 ・**セキュリティ人材プール**の創設と優秀な人材の官民への派遣

4. 提言② セキュリティ対応人材育成その2

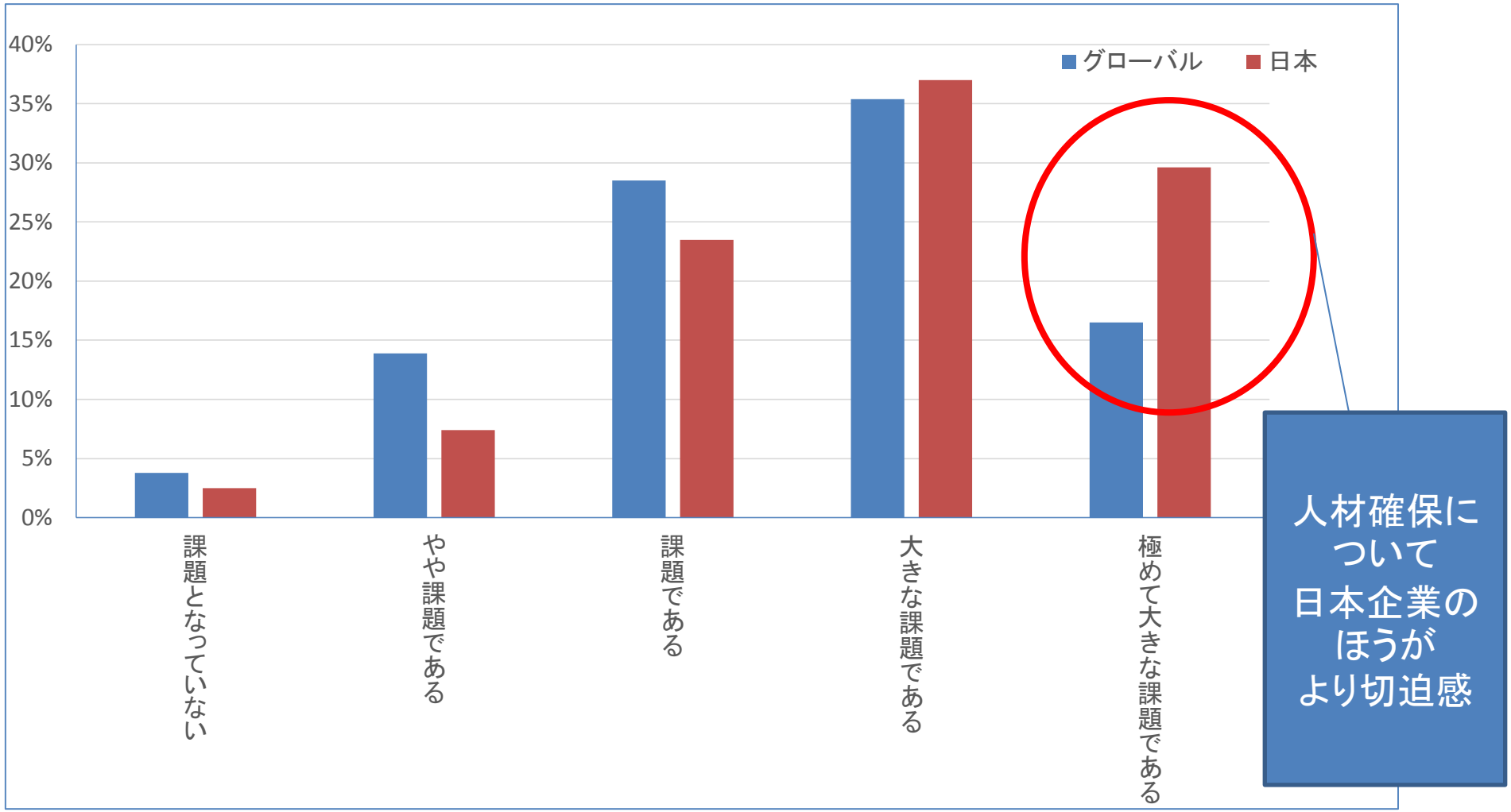
目標2

IT分野全般及びセキュリティに関する幅広い知見・技術と倫理観をもったセキュリティ人材の養成と地位向上

目標2を達成するための具体的施策～その2～	③セキュリティ人材の**発掘・表彰制度**の充実強化による**ロールモデル創設** ・**セキュリティキャンプ**等の充実強化 ・倫理観を持ったセキュリティに強いハッカー(優良プログラマ)を表彰する制度の充実強化(**総理大臣賞**)
	④各企業において**CISO、CIOを設置**することを促進 ・上記設置に向けた官民連携した**啓発キャンペーン**の展開
	⑤セキュリティ従事者に対する啓発強化 ・**倫理・モラルに関する**官民連携した**啓発活動**の充実強化

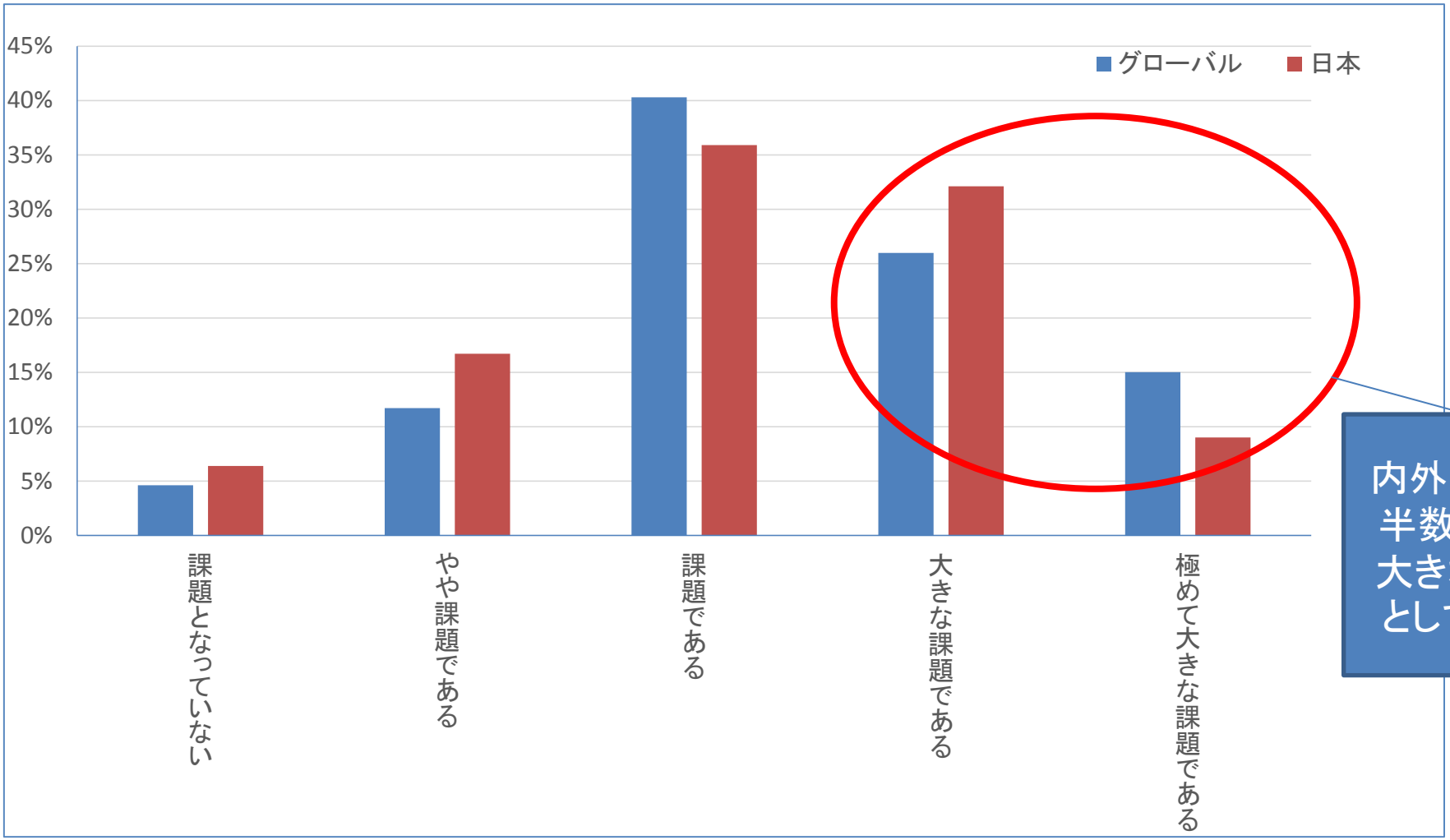
【参考】 人材確保に関する動向 (OWASP　CISO調査2014より)

Q: 貴社のアプリケーション・セキュリティを主導的に進めるにあたり、「熟練した人材の確保」はどの程度課題となっていますか？



【参考】 人材のセキュリティレベルの動向（OWASP　CISO調査2014より）

Q: 貴社のアプリケーション・セキュリティを主導的に進めるにあたり、「開発者におけるセキュリティの認識レベル」はどの程度課題となっているか



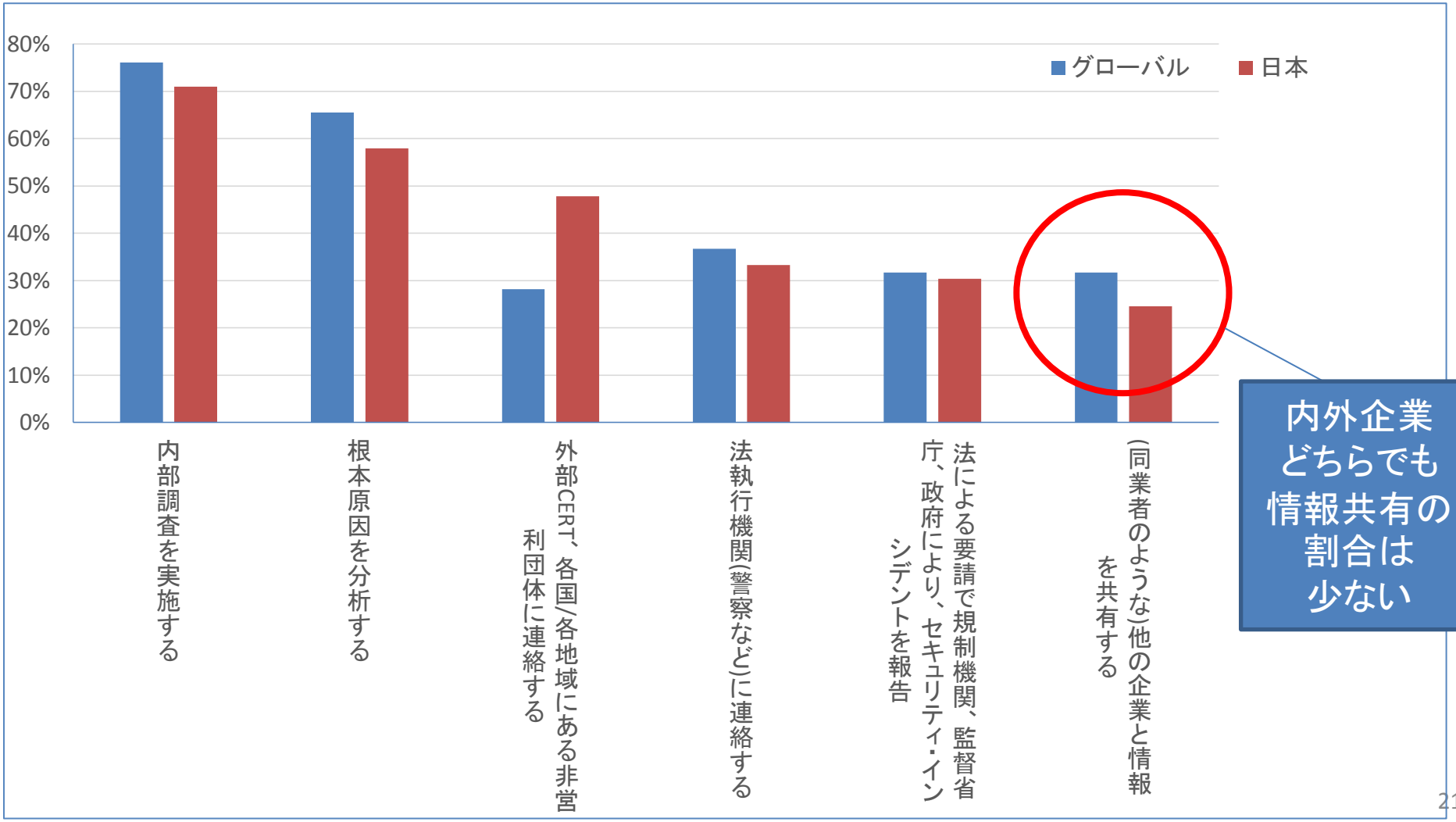
4. 提言③　セキュリティ担当者間の情報共有の充実強化

目標3
企業や業種を超えたセキュリティ担当者間の情報共有の充実強化

目標3を達成するための具体的施策	①企業や業種横断のセキュリティ人材に限った**情報共有の場の設置** ・各業界団体、経済団体等において**情報共有の仕組みをネット上での質問機能などを活用しながら構築**する。
	②情報セキュリティ担当者の**既存コミュニティとの官民連携を強化**する。

【参考】 情報共有の動向（OWASP　CISO調査2014より）

Q: インシデントや違反が発生した時にインシデント対応手順の一部として、通常実施しているものをお答え下さい（あてはまるものをすべて選択してください）



4. 提言④　一般社員・社会に対しての啓蒙活動と社会全体のセキュリティレベルの底上げ

目標4

社員へのセキュリティ教育を徹底するほか、一般社会のセキュリティ意識の向上と企業全体のセキュリティレベルの向上を図る。

目標4を達成するための具体的施策	①情報にアクセスする社員向けの、**情報セキュリティ教育の促進** ・**新入社員・中途入社員に対する基本教育**の実施 ・**毎年の定期教育**の実施（変化するIT技術、セキュリティ脅威に合わせて内容更新） ・**管理者権限（特権）所有者**（IT管理者や経営層）向け教育の実施
	②**セキュリティチェックの促進** ・チェック徹底による、各企業・社員の**セキュリティ意識の標準化** ・例えば、1年に1度、50名以上の事業所を対象 ・チェック結果に対しての、**相談先を官民連携で用意**し改善サイクルを回す
	③利用者・一般社会への**啓発活動の充実強化** ・「ストップ・PW使い回し」等のキャンペーンをこれまで以上に**官民連携**して進める。

５．本提言の検討体制、検討過程等

■インターネット・セキュリティＷＧ

〇リーダー　　兼元　謙任(新経済連盟幹事、オウケイウェイヴ代表取締役社長)

〇検討過程、活動等

(ワーキンググループ/会員向け勉強会の開催)
２０１４年６月４日
OWASP Japan・岡田良太郎様等を講師として会員向け勉強会を開催

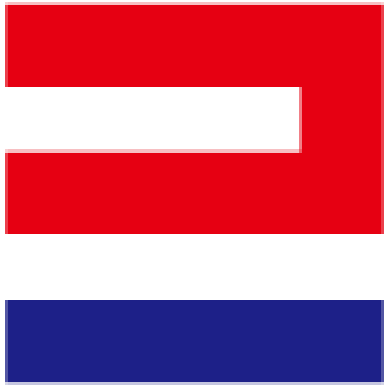
(外部アンケートへの協力)
OWASP Japan様が実施する、企業・団体の情報セキュリティ担当の責任者を対象としたインターネットセキュリティのグローバル調査「OWASP CISO調査 2014」へ協力

(外部有識者ヒアリング)
・セキュリティ関係企業、官公庁等からヒアリング

(関連セッション開催)
・２０１５年４月８日
当連盟主催の「新経済サミット」において、サイバーセキュリティのセッションを実施
(ミッコ・ヒッポネン氏(F-Secure　チーフ・リサーチ・オフィサー)の講演)

(注)本年6月より、改組して、情報セキュリティタスクフォースとして引き続き活動予定。

Hello, Future!



新経済連盟

Japan Association of New Economy