RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

企業が直面する「脅威の現実」と「セキュリティ対策の現実」

SESSION ID: JPN-T07

染谷　征良

セキュリティエバンジェリスト
トレンドマイクロ株式会社

アジェンダ

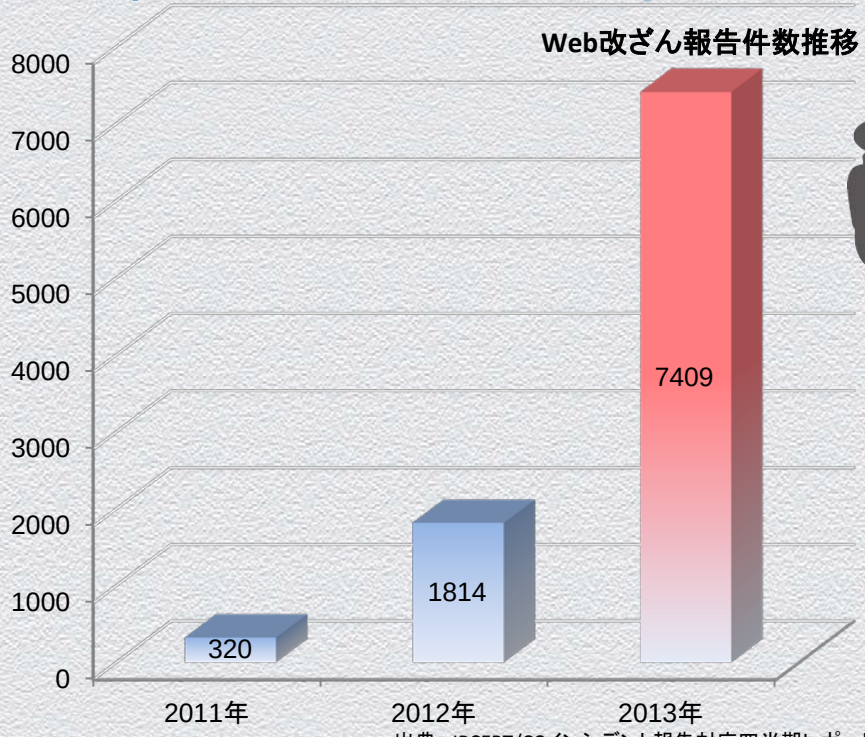
- 脅威動向から攻撃のポイントを探る
- 組織におけるセキュリティ対策、被害、課題の現状
- 「ビジネスリスクを低減するセキュリティ」とは？

アジェンダ

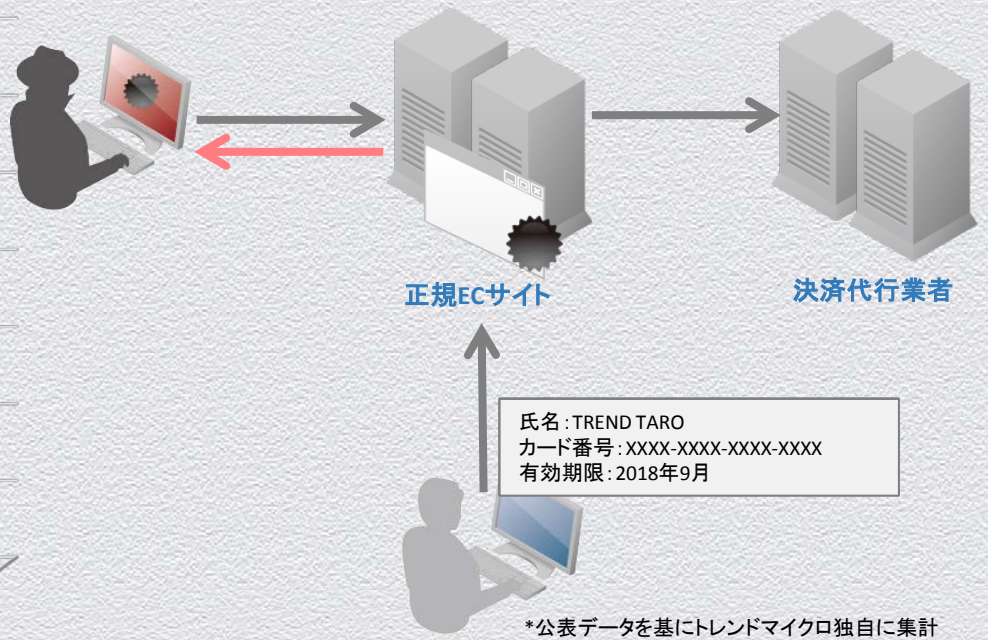
- 脅威動向から攻撃のポイントを探る
- 組織におけるセキュリティ対策、被害、課題の現状
- 「ビジネスリスクを低減するセキュリティ」とは？

止まらないWeb改ざん

- サイト訪問者への金銭詐欺を目的としたWeb改ざんが約8割*
- 情報窃取を目的としたWeb改ざんの登場
- 標的型サイバー攻撃を目的とした「水飲み場型攻撃」



出典：JPCERT/CCインシデント報告対応四半期レポート
https://www.jpcert.or.jp/ir/report.html
※JPCERT/CCインシデント報告対応四半期レポートの数字をトレンドマイクロ株式会社にて編集



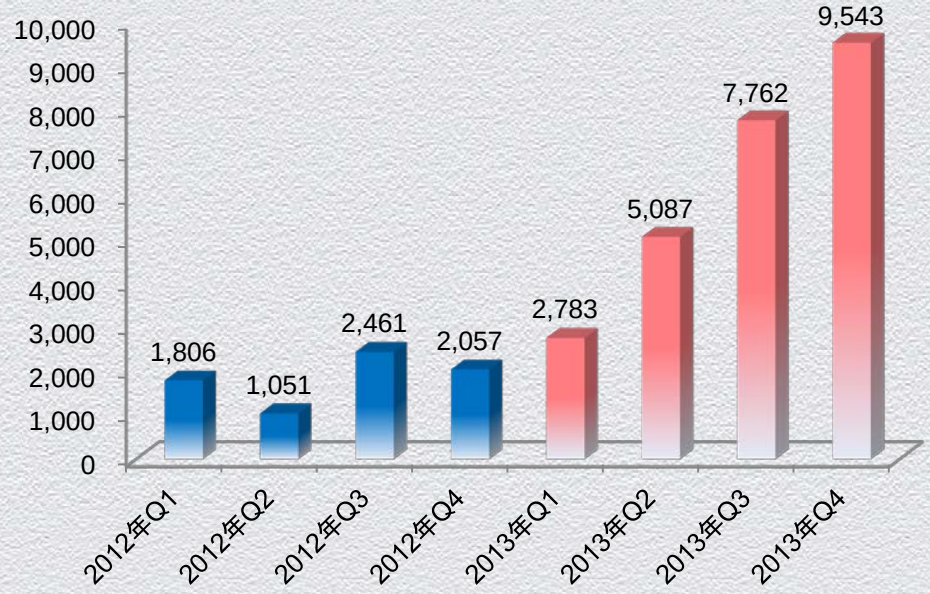
*公表データを基にトレンドマイクロ独自に集計

#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

「新しいオンライン詐欺」の到来

- ネットバンキング利用者を狙った脅威
  - 累計検出台数は、前年比約3.4倍
  - 国内検出台数の割合は、世界第2位
  - 不正送金被害は14億600万円で過去最悪、前年比約29倍（警察庁発表）

オンライン銀行詐欺ツール検出台数推移



オンライン銀行詐欺ツール国別検出台数割合

第１四半期		第２四半期		第３四半期		第４四半期	
国名	割合	国名	割合	国名	割合	国名	割合
米国	33%	米国	28%	米国	23%	米国	22%
ブラジル	10%	ブラジル	22%	ブラジル	16%	日本	19%
オーストラリア	5%	オーストラリア	5%	日本	12%	ドイツ	12%
台湾	5%	フランス	5%	インド	6%	台湾	6%
カナダ	4%	日本	4%	オーストラリア	3%	フランス	5%
日本	3%	台湾	4%	フランス	3%	ドイツ	3%
インド	3%	ベトナム	3%	ドイツ	2%	インド	3%
フランス	3%	インド	2%	ベトナム	2%	カナダ	2%
フィリピン	3%	ドイツ	2%	台湾	2%	オーストラリア	2%
ドイツ	2%	カナダ	2%	メキシコ	2%	イタリア	2%
その他	29%	その他	23%	その他	29%	その他	24%

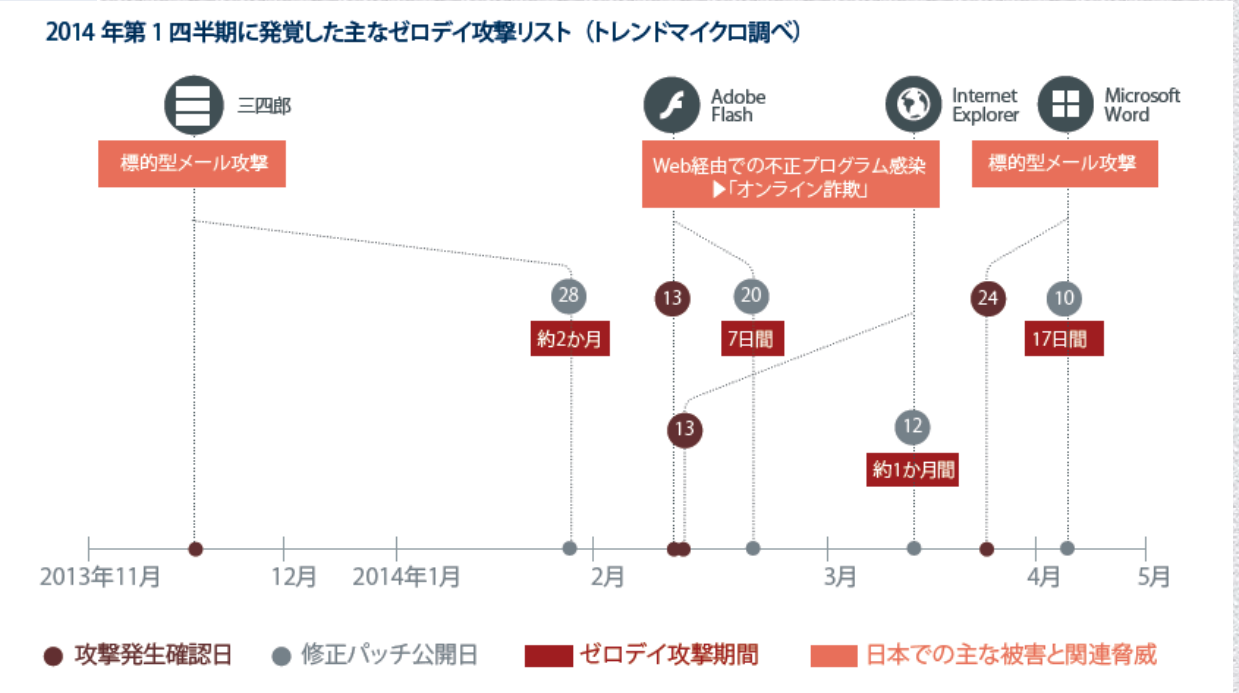
2014年トレンドマイクロ調べ

TREND MICRO

#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

頻発するゼロデイ攻撃

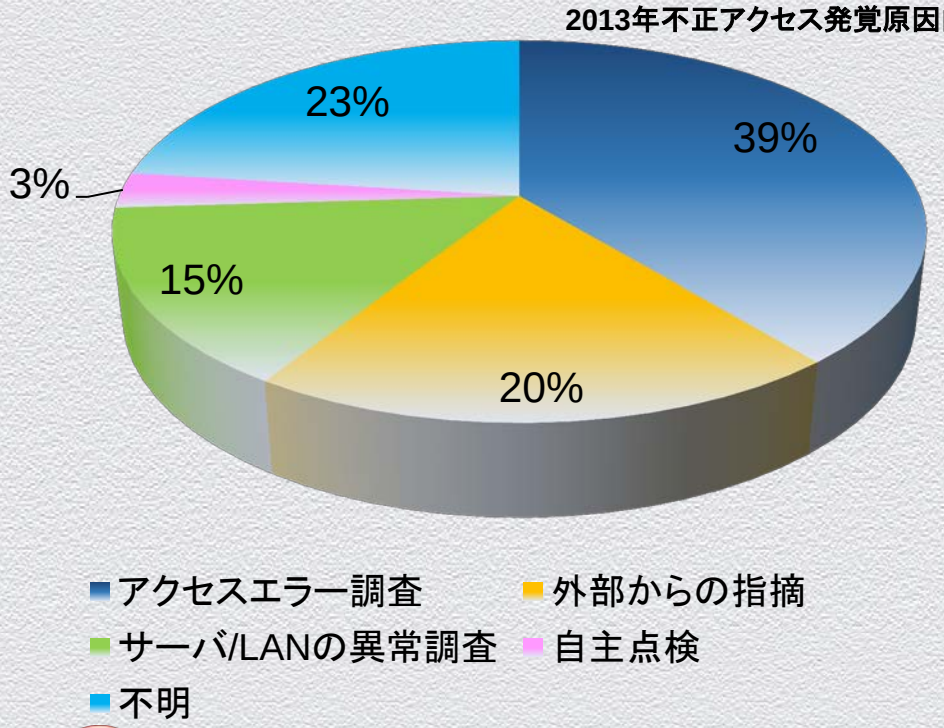
主な2013年PC向けゼロデイ攻撃事例	
1月	Java、一太郎
2月	Flash、Adobe Reader
4月	Internet Explorer
5月	一太郎
8月	Internet Explorer、Java
9月	一太郎
11月	Internet Explorer、Office、Windows XP/2003



TREND MICRO
#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

不正アクセスの脅威ーアカウントリスト攻撃

- 20%が外部からの指摘ではじめて侵害に気付く
- 54%は異常が発覚した結果の調査により侵害に気付く
- 僅か3%が定期的な監視により侵害に気付く

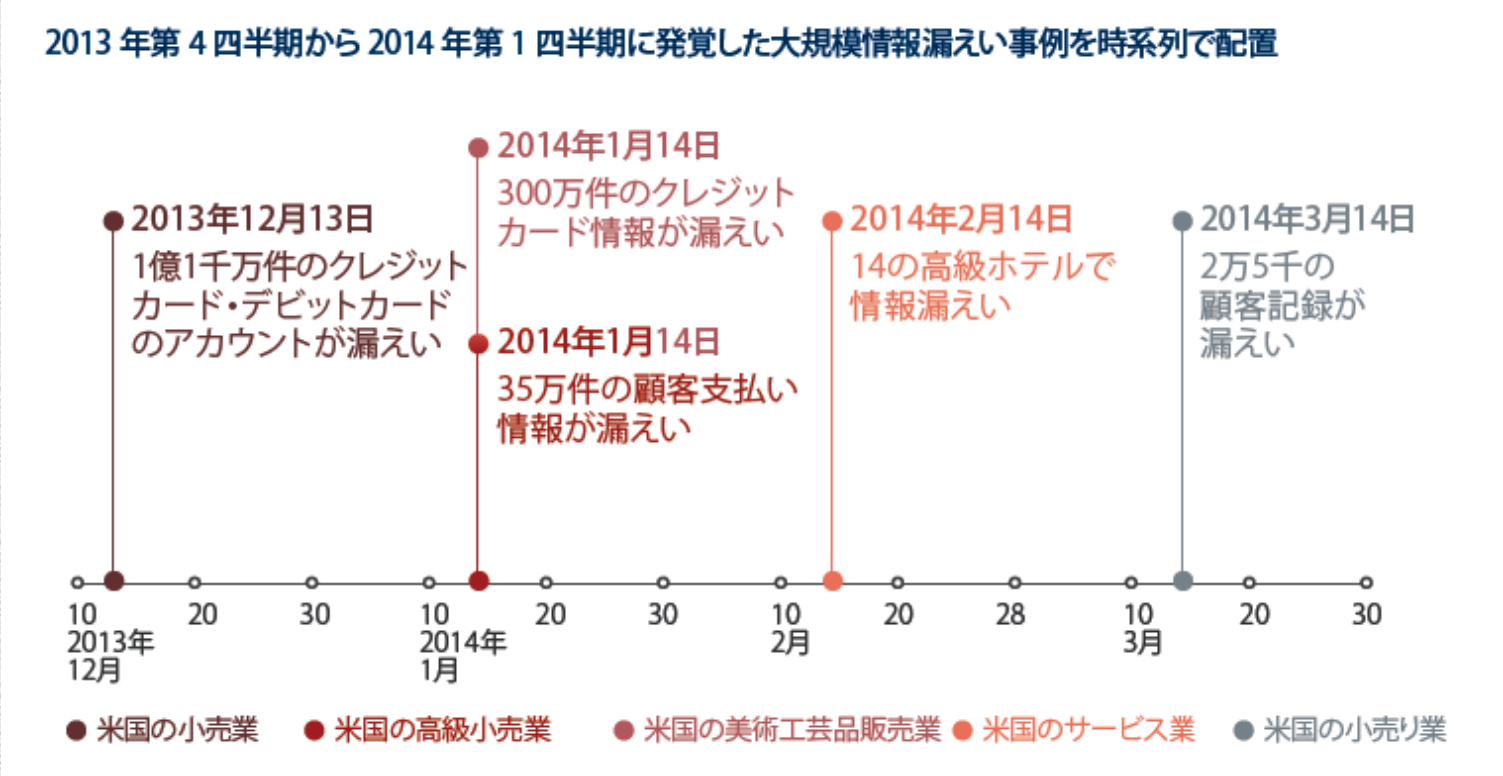


No.	不正ログイン被害 ID 数	被害企業業種
1	243,266	サービス業
2	150,165	小売業
3	83,961	情報通信業
4	39,590	情報通信業
5	35,252	情報通信業
6	28,452	サービス
7	28,000	人材総合サービス事業
8	23,926	サービス業
9	15,000	通信販売

*公表データを基にトレンドマイクロ独自に集計

#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

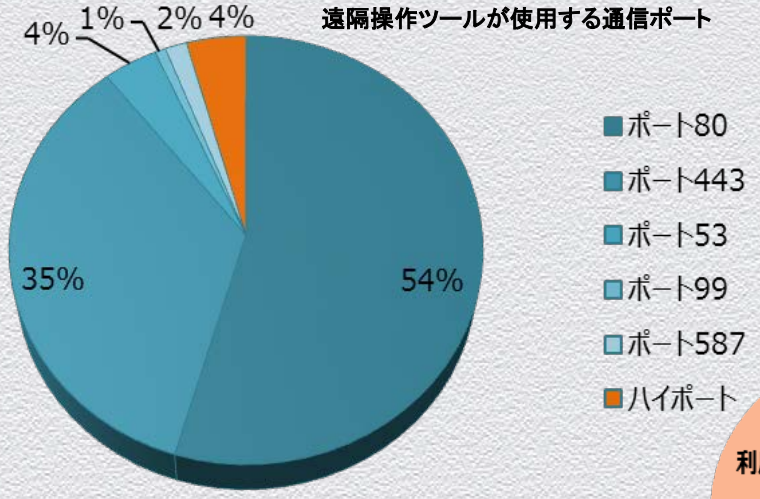
狙われるPOSシステム

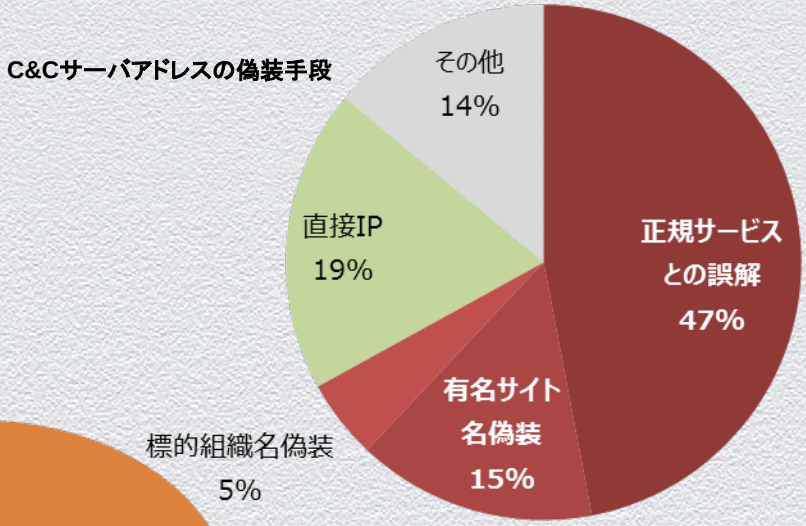


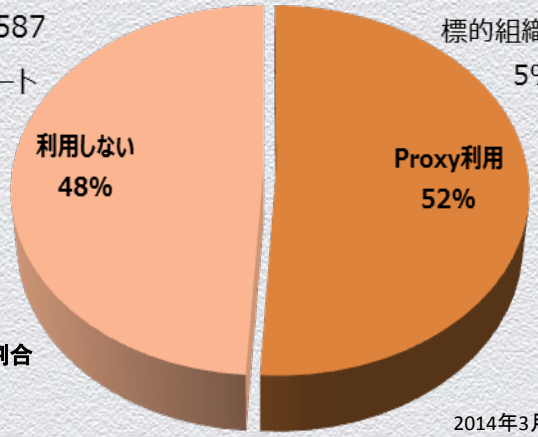
TREND MICRO
#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

標的型サイバー攻撃の傾向

- 遠隔操作ツールの96%がウェルノウンポートを通信に使用
- 通信先C&Cの67%は正規サイト・サービスを誤認させるアドレスを使用







遠隔操作ツールのプロキシ利用割合

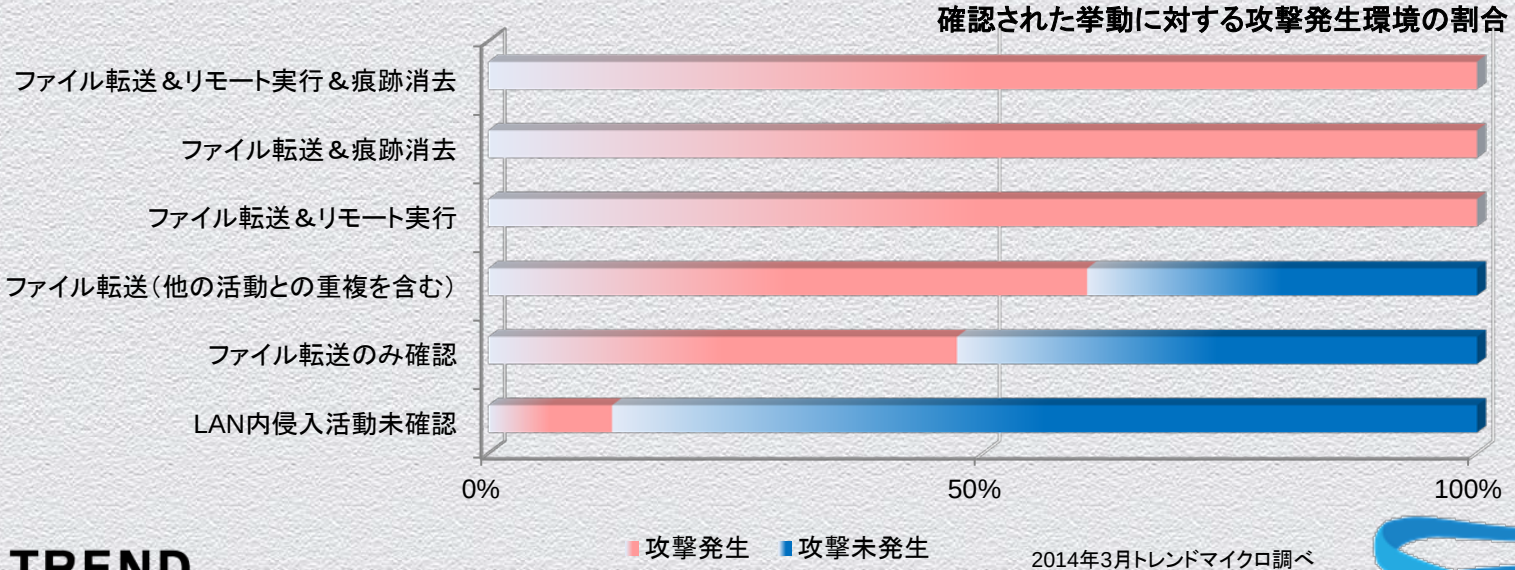
2014年3月トレンドマイクロ調べ

TREND MICRO
#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

攻撃者は必ず痕跡を消す

- ファイル転送を起点とした複数の挙動がある場合の攻撃発生率は100%

ファイル転送	Windows管理共有への実行ファイルコピー	リモート実行	PsExecの実行	痕跡消去	リモートでのタスク削除
	FTPによる実行ファイル転送		リモートでのタスク追加		リモートでのサービス削除
	リモートでのechoコマンド実行		リモートでのサービス作成		リモートでのイベントログ削除



2014年3月トレンドマイクロ調べ

TREND MICRO
#RSAC
RSACONFERENCE2014 ASIA PACIFIC & JAPAN

- 脅威動向から攻撃のポイントを探る
- 組織におけるセキュリティ対策、被害、課題の現状
- 「ビジネスリスクを低減するセキュリティ」とは？

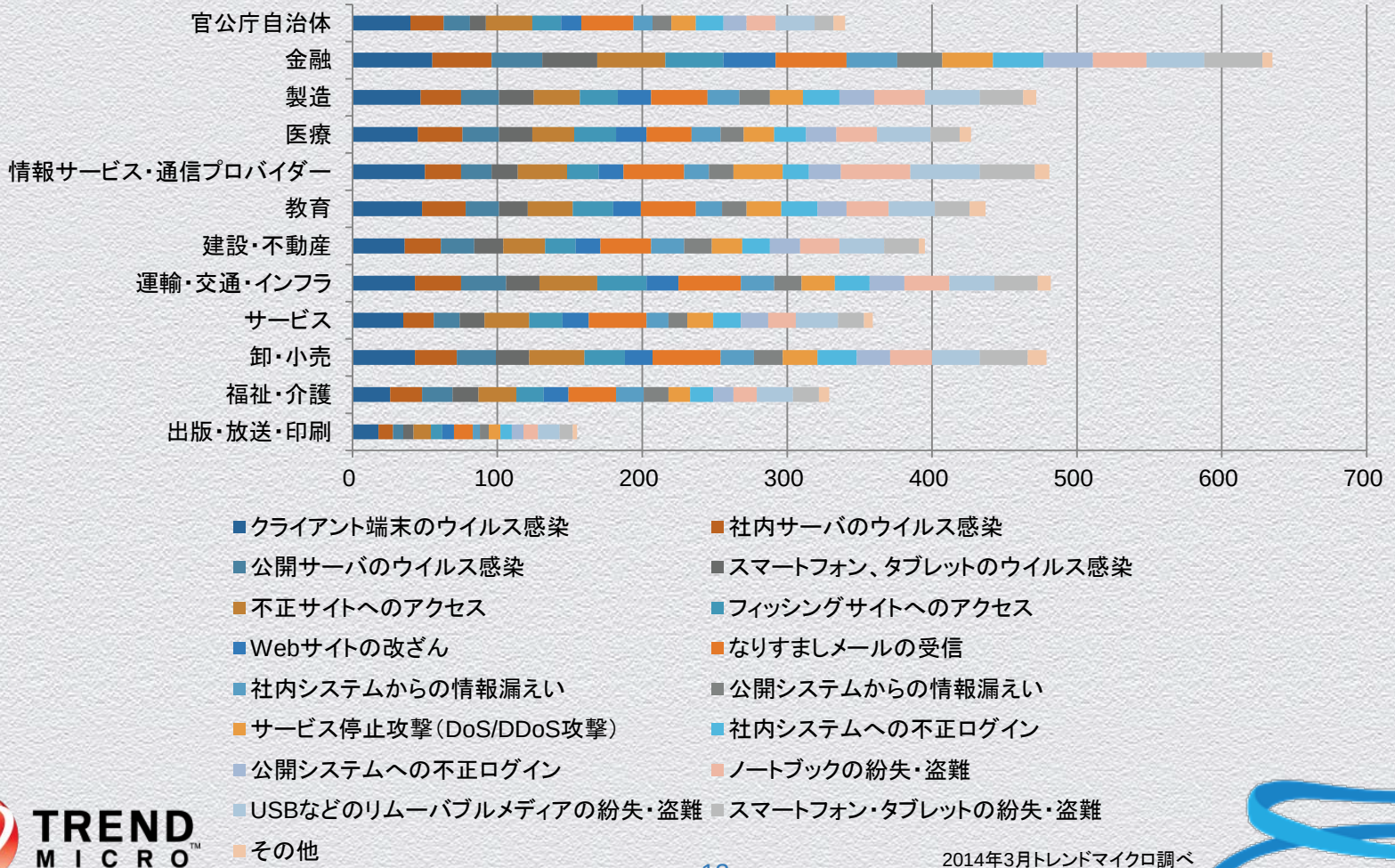
TREND MICRO
#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

- ビデオをご覧ください

TREND MICRO™
#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

セキュリティインシデント発生件数

66.2%がセキュリティ事故を経験

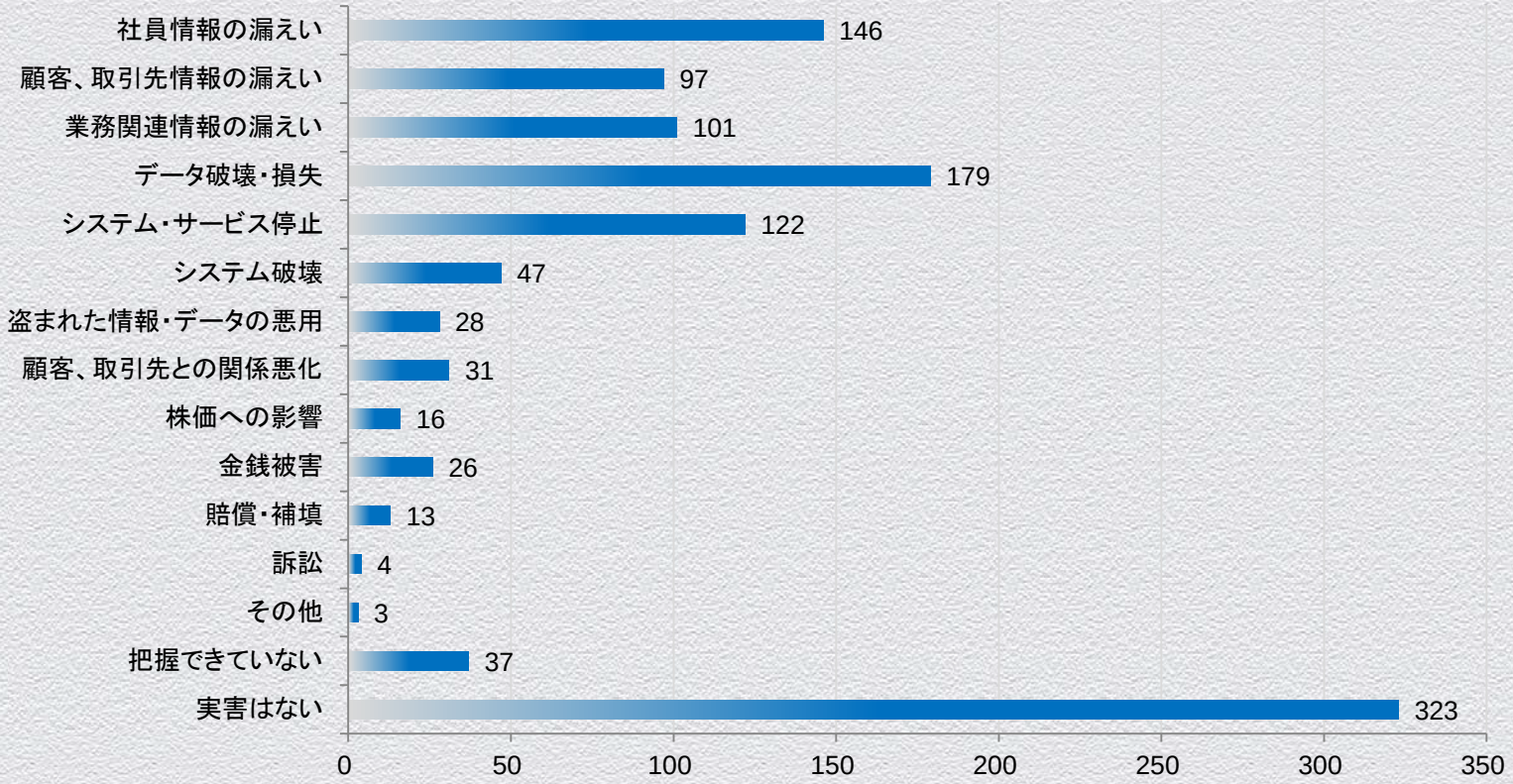


2014年3月トレンドマイクロ調べ

TREND MICRO
#RSAC
RSACONFERENCE2014 ASIA PACIFIC & JAPAN

セキュリティインシデントに実害はあるのか？

53.7%が実害に直結



2014年3月トレンドマイクロ調べ

TREND MICRO
#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

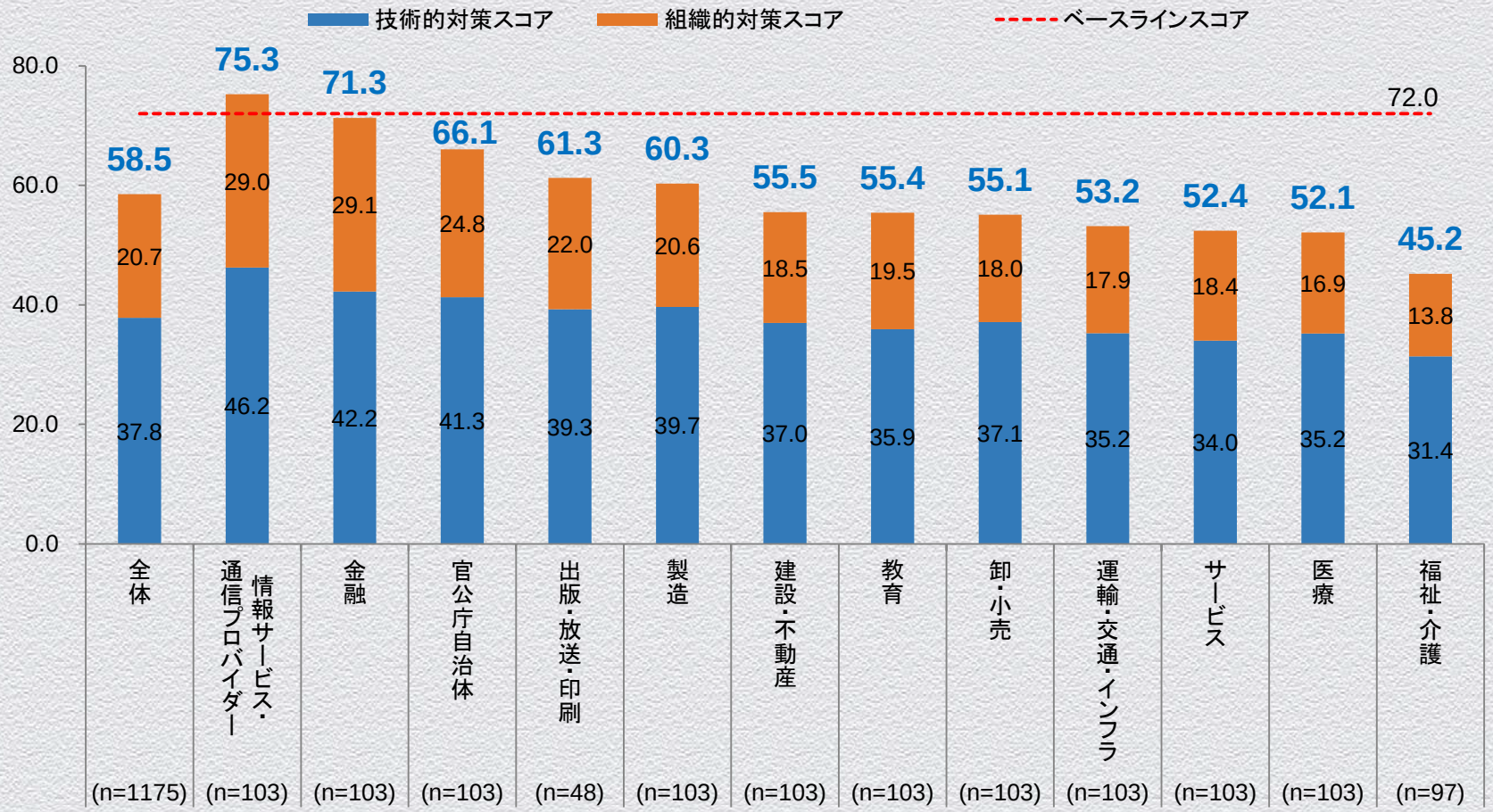
組織におけるセキュリティ対策包括度

58.5点

2014年3月トレンドマイクロ調査を基に100点満点で独自に算出

TREND MICRO™
#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

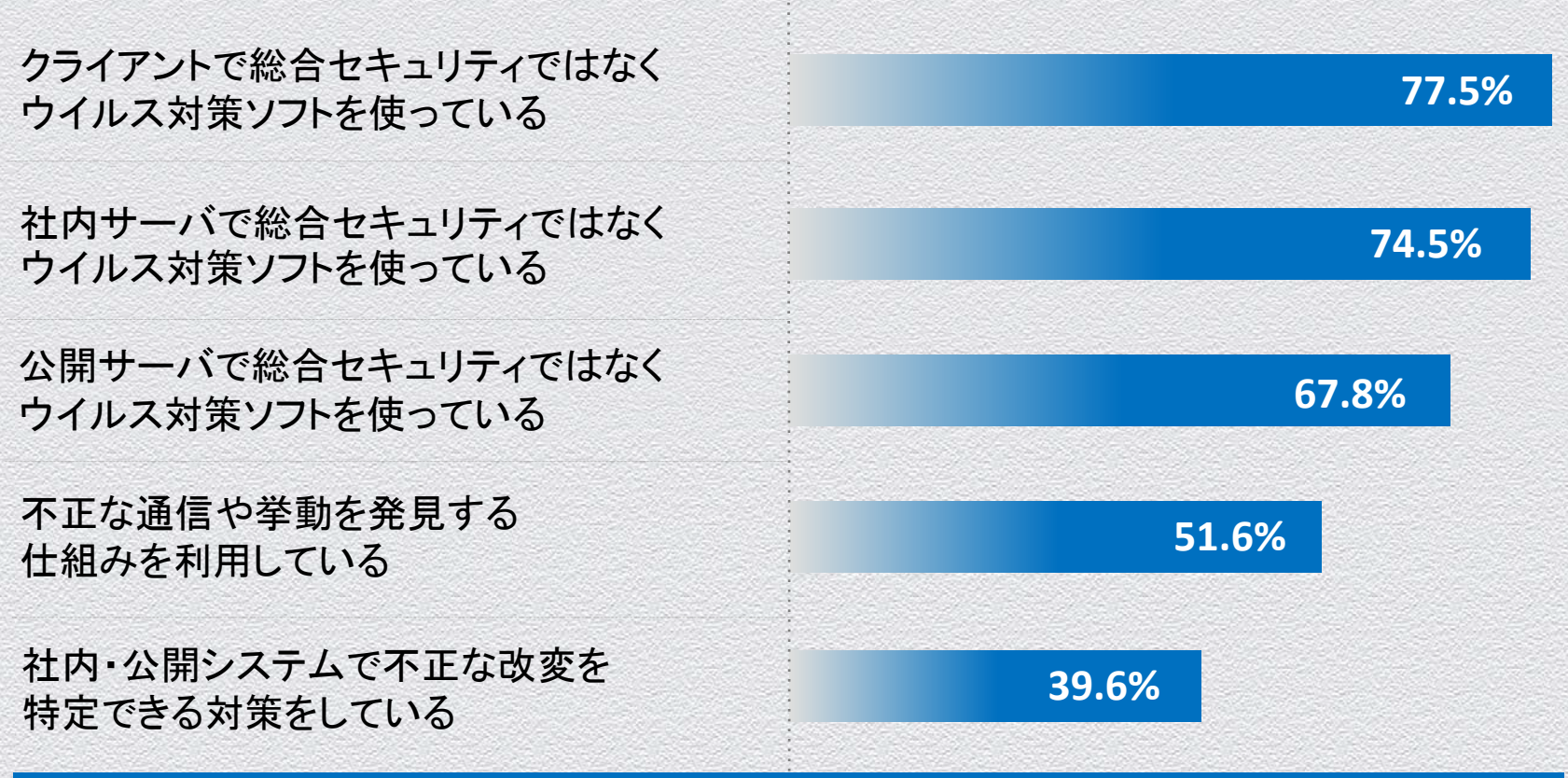
セキュリティ対策包括度ー業種別比較



2014年3月トレンドマイクロ調べ
「出版・放送・印刷」は回答者サンプルが少ないため参考値

TREND MICRO
#RSAC
RSACONFERENCE2014 ASIA PACIFIC & JAPAN

技術的な対策の実態

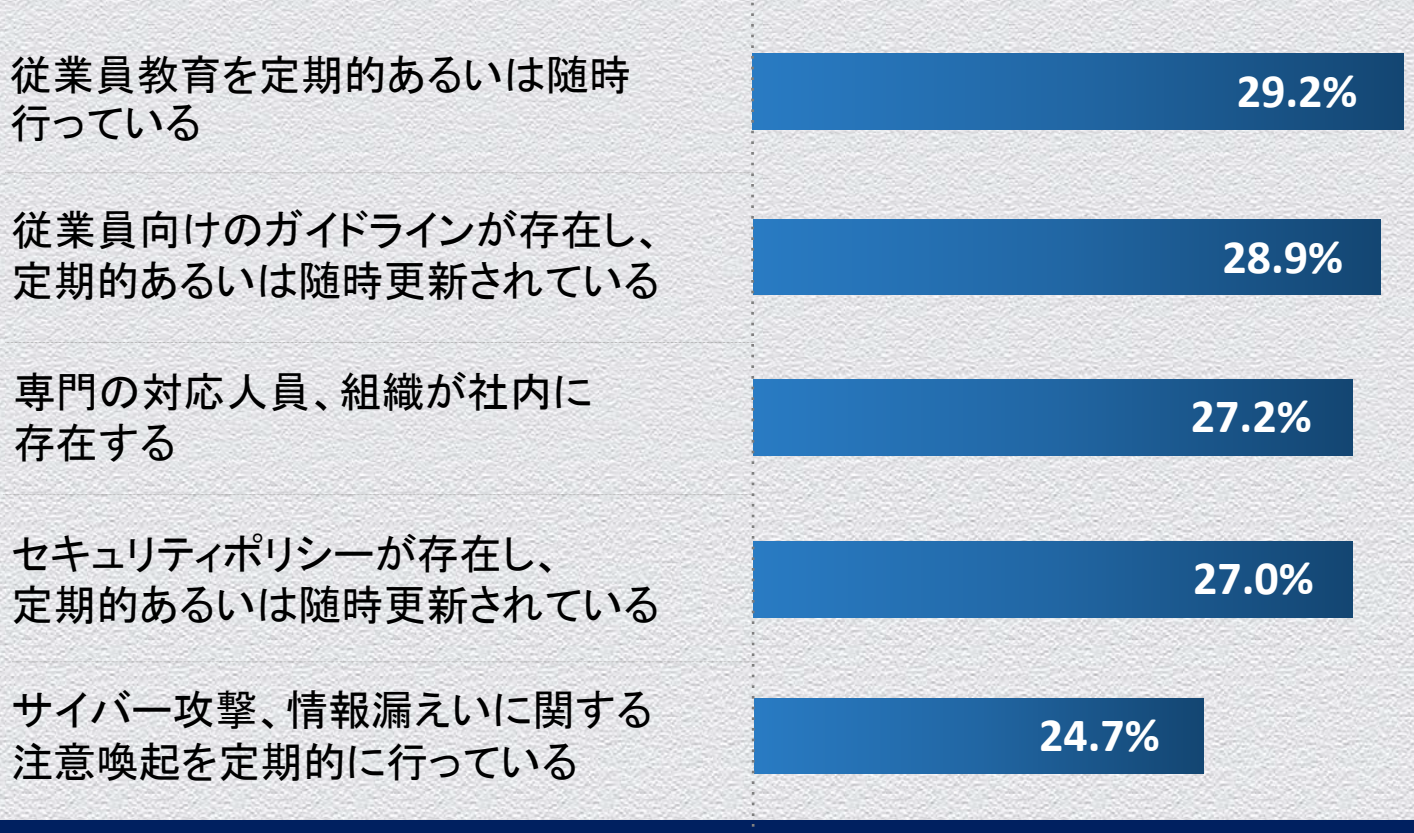


昨今の脅威に対策が追い付いていない

2014年3月トレンドマイクロ調べ

TREND MICRO
#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

組織的な対策の実態

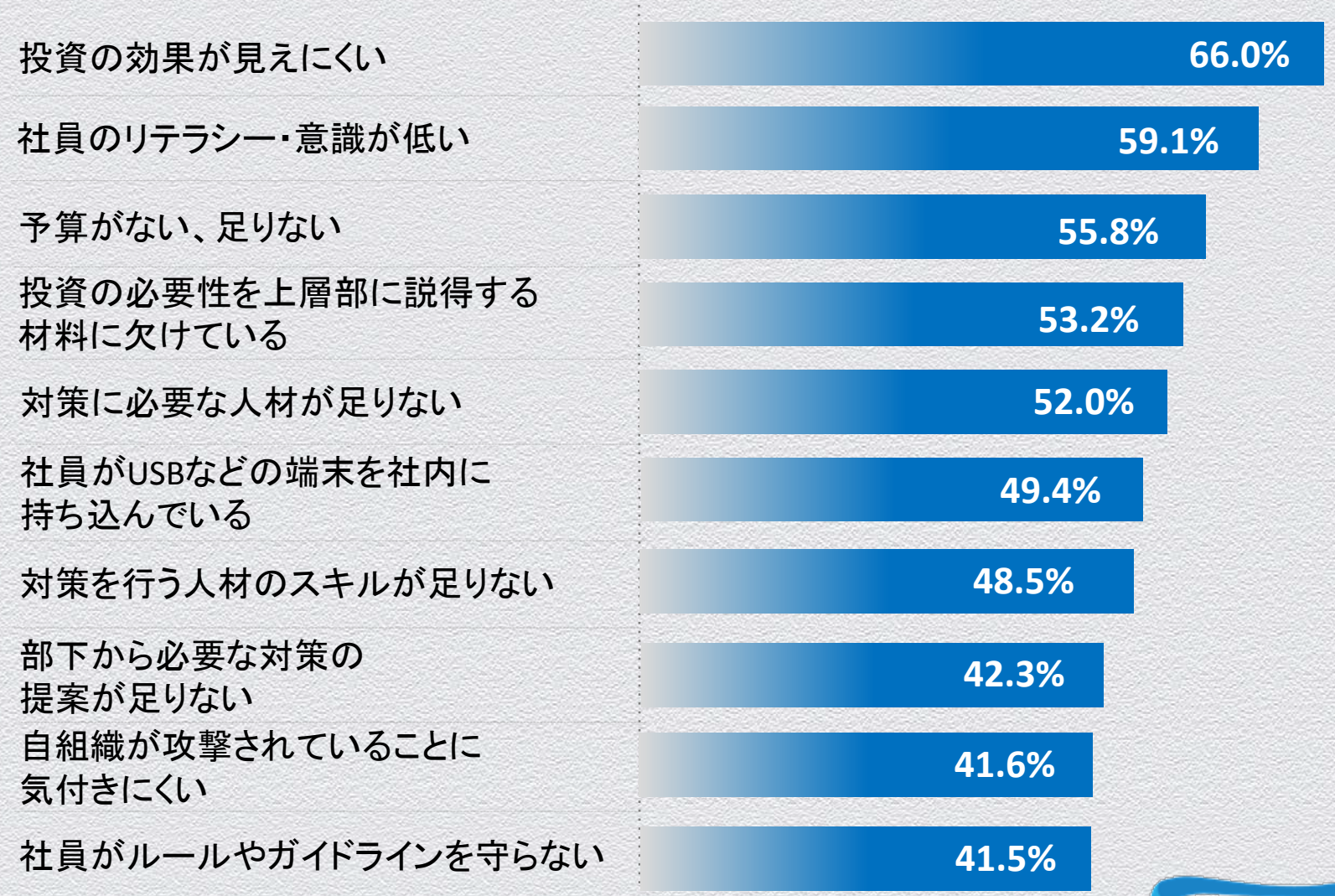


組織を守る環境・体制が整っていない

2014年3月トレンドマイクロ調べ

TREND MICRO
#RSAC
RSACONFERENCE2014 ASIA PACIFIC & JAPAN

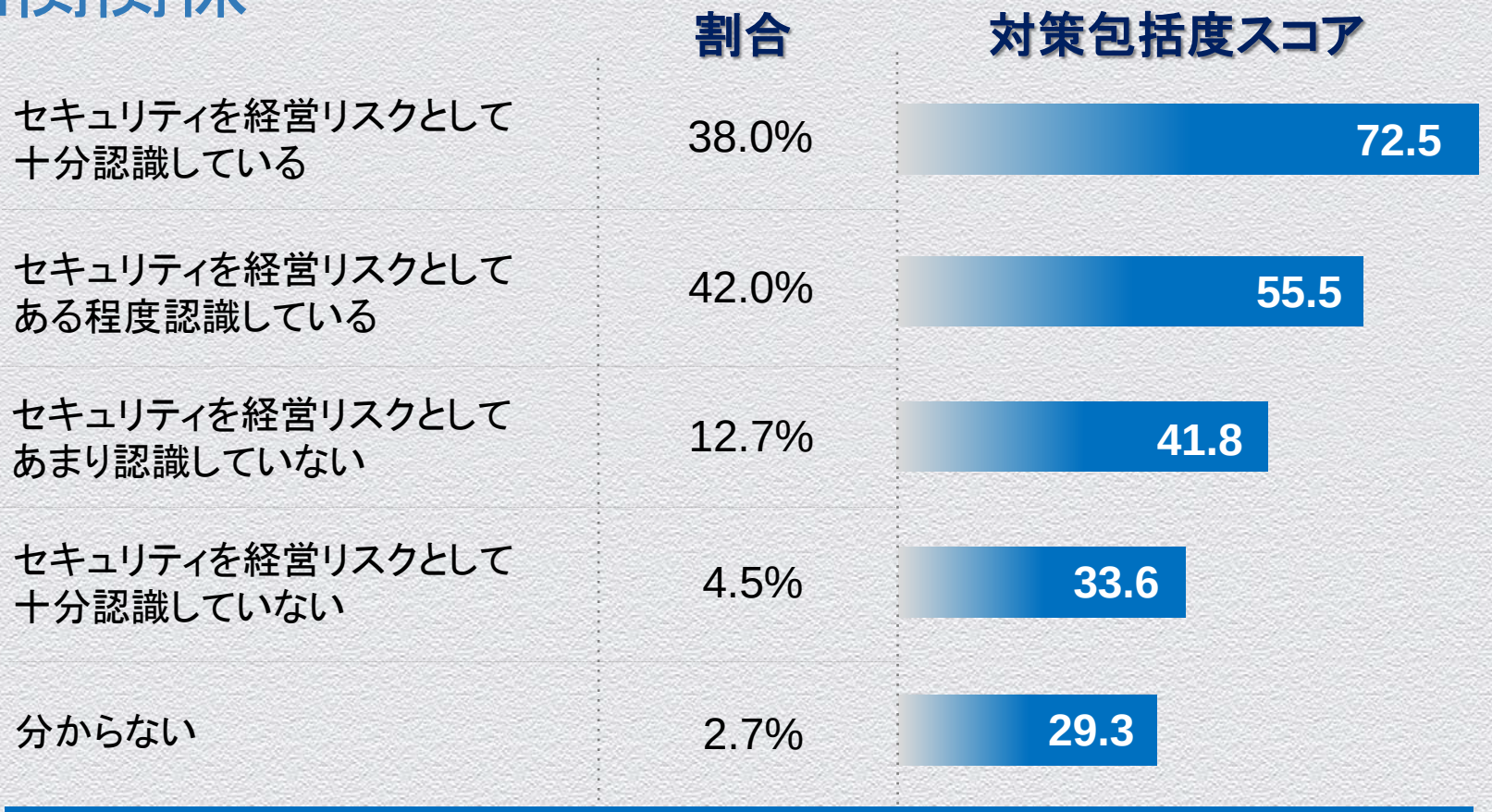
組織においてセキュリティ対策を行う上での課題



2014年3月トレンドマイクロ調べ

TREND MICRO
#RSAC
RSACONFERENCE2014 ASIA PACIFIC & JAPAN

「経営リスクとしての認識」と「対策包括度」の相関関係



「経営リスク」認識は対策レベルに直結

2014年3月トレンドマイクロ調べ

TREND MICRO
#RSAC
RSACONFERENCE2014 ASIA PACIFIC & JAPAN

- 脅威動向から攻撃のポイントを探る
- 組織におけるセキュリティ対策、被害、課題の現状
- 「ビジネスリスクを低減するセキュリティ」とは？

TREND MICRO™
#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

ビジネスリスク低減する「3ステップ」

「ビジネスリスク」としての認識

- 脅威動向の情報収集
- セキュリティ脅威に関する理解
- ビジネスリスクの分析・認識
- 対策・投資の必要性の理解

組織的な対策の強化

- 体制の見直し・強化
- 対策人材への投資
- ポリシーの策定・見直し
- 社員教育・注意喚起の実施
- ライフサイクルとしてのセキュリティの実施

技術的な対策の強化

- 端末での対策強化
- 社内・公開システムでの対策強化
- データの保護
- 内部活動の可視化
- 不正改変の早期察知

TREND MICRO™

#RSAC
RSACONFERENCE2014
ASIA PACIFIC & JAPAN

組織における優先対策項目トップ3

組織的対策

① 専任組織構築、人的投資を含めた**体制の強化**
② ポリシーやガイドラインなどの**ルールの整備と見直し**
③ 社員教育や注意喚起を通じた**全社的な底上げ**

技術的対策

① クライアント・サーバでの**旧来の対策からの脱却**
② システム侵害時の**インシデント早期発見**
③ 組織内部での**不正な通信や挙動の早期発見**

トレンドマイクロが提供する
セキュリティライフサイクルマネージメント

サーバ対策
Trend Micro
Deep Security

クライアント対策
Client / Server
Suite Premium

内部対策
Trend Micro
Deep Discovery

CSIRT/SOC
構築支援
サービス

導入・運用支援
サービス

インシデント
対応支援
サービス

プレミアム
サポートサービス

RSA CONFERENCE 2014
ASIA PACIFIC & JAPAN

ありがとうございました