サイバー攻撃における状況認識

～ 2014年度データ漏洩侵害調査報告書から ～

ベライゾン

RISKチームディレクター ブライアン・サーティン

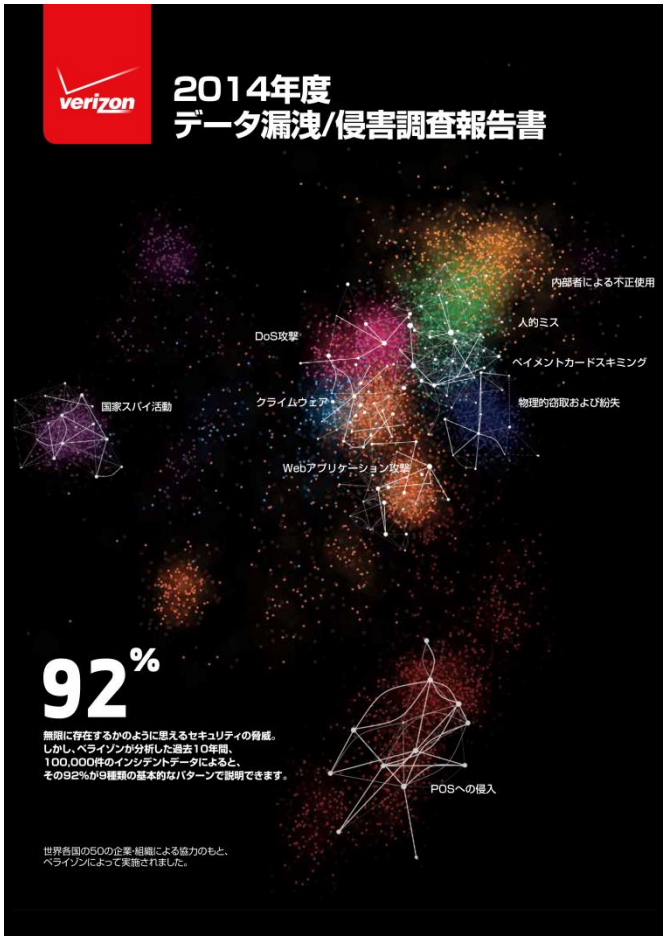
2014年度データ漏洩/侵害調査報告書

92%

無限に存在するかのように思えるセキュリティの脅威。しかし、ベライゾンが分析した過去10年間、100,000件のインシデントデータによると、その92%が9種類の基本的なパターンで説明できます。

世界各国50の企業・組織による協力のもと、ベライゾンによって実施されました。

2014年度データ漏洩/侵害調査報告書の分析データ



50
ご協力いただいた世界各国の企業・組織の数

1,367
確認済みのデータ漏洩/侵害件数

63,437
セキュリティインシデント件数

95
調査対象国の数

世界各国の50の協力企業・組織

Mishcon de Reya

KASPERSKY lab

McAfee
An Intel Company

National Cyber Security Centre
Ministry of Security and Justice

EC3 EUROPOL

Akamai

G-C PARTNERS

CENTRIPETAL NETWORKS

CIRCL
Computer Incident Response Center Luxembourg

OpenCERT Canada
semper vigilantem

Deloitte.

Homeland Security

MALICIOUS STREAMS

GDT
GRUPO DE DELITOS TELEMÁTICOS

S21sec
Comprometidos con la seguridad

REN-ISAC

AFP
AUSTRALIAN FEDERAL POLICE

POLITI

verizon

ES ISAC
Electricity Sector Information Sharing Analysis Center

CENTER FOR INTERNET SECURITY

CENTER FOR CYBERSIKKERHED

PT-ISAC

ThreatGRID
Malware Analysis & Threat Intelligence

WINSTON & STRAWN LLP

IRISS
Irish Reporting and Information Security Service

Real Estate ISAC
Information Sharing and Analysis Center

Guidance SOFTWARE

EnCase

CERT.PT

ERTA

CERT-EU

POLITIE

CERT
Software Engineering Institute
Carnegie Mellon

WhiteHat SECURITY

US-CERT
UNITED STATES COMPUTER EMERGENCY READINESS TEAM

POLICIA METROPOLITANA

CyberSecurity MALAYSIA
An agency under MOSTI

itrc
Identity Theft Resource Center

FireEye

COUNCIL ON CYBERSECURITY
LE CONSEIL DE LA CYBERSÉCURITÉ

VCDB

CERT.PL

FINANCIAL SERVICES Information Sharing and Analysis Center

ThreatSim™

2014年度データ漏洩/侵害調査報告書の協力企業・組織

CSIRTS
- CERTインサイダー脅威センター
- ポーランドCERT/NASK
- CERT-EU、欧州連合
- CERT.PT
- ウクライナコンピューター緊急事態対策チーム(CERT-UA)
- ルクセンブルグコンピューターインシデント対策センター(CIRCL)、ルクセンブルグの国家CERT
- サイバーセキュリティマレーシア、マレーシア化学・技術・イノベーション省(MOSTI)内の部門
- 産業制御システム・サイバー緊急事態対応チーム(ICS-CERT)
- アイルランドレポートおよびインフォメーションセキュリティサービス(IRISS-CERT)
- OpenCERTカナダ
- 米国コンピューター緊急事態対策チーム(US-CERT)

サイバーセンター
- サイバーセキュリティセンター、デンマーク
- サイバーセキュリティ評議会
- 防衛安全局(DSS)
- 欧州サイバー犯罪センター(EC3)
- 米国サイバーセキュリティ・通信統合センター(NCCIC)
- オランダ国家サイバーセキュリティセンター(NCSC-NL)

フォレンジックプロバイダー
- デロイト・トウシュLLP
- G-C Partners, LLC
- ガイダンスソフトウェア
- S21sec
- ベライゾンRISKチーム

情報セキュリティ製品/サービスプロバイダー
- Akamai
- Centripetal Networks, Inc.
- FireEye
- Kaspersky Lab
- Malicious Streams
- McAfee (インテルセキュリティの一部門)
- ThreatGRID, Inc.
- ThreatSim
- ベライゾンDoSディフェンス
- WhiteHat Security

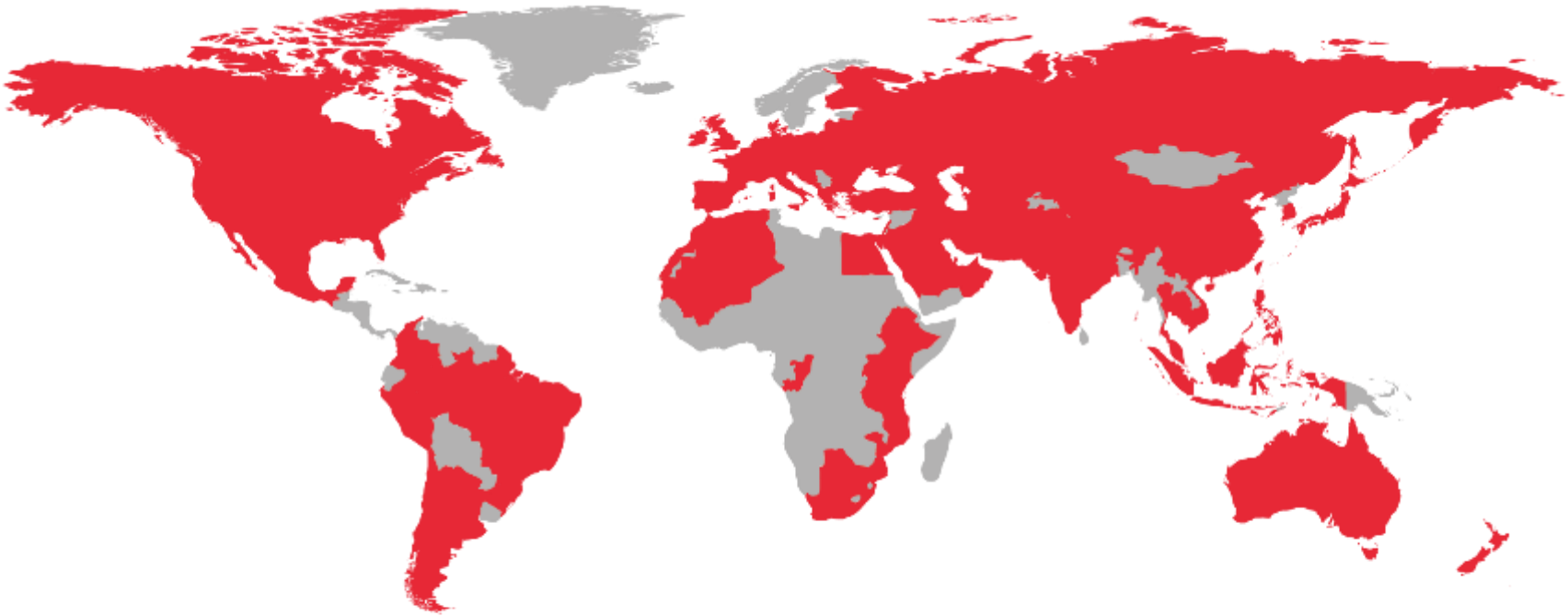
ISACS
- インターネット・セキュリティー・センター(MS-ISAC)
- 電力業界情報共有・分析センター(ES-ISAC)
- 金融サービスISAC(FS-ISAC)
- 公共輸送ISAC(PT-ISAC)
- 不動産業ISAC(RE-ISAC)
- 研究および教育ISAC(REN-ISAC)

法執行機関
- オーストラリア連邦警察(AFP)
- グアルディアシビル内サイバー犯罪中央ユニット(スペイン)
- デンマーク警察NITES(IT調査部門)
- オランダ警察:国家ハイテク犯罪ユニット(NHTCU)
- ブエノスアイレス市警察(アルゼンチン)
- コロンビア国家警察
- アメリカ合衆国シークレットサービス

その他
- 匿名の協力者の皆様
- マサチューセッツ州
- アイデンティティ窃盗リソースセンター
- Mishcon de Reya
- VERISコミュニティデータベース(VCDB)
- Winston & Strawn

調査対象国

図1.
調査対象国



調査対象国(アルファベット順):アフガニスタン、アルバニア、アルジェリア、アルゼンチン、アルメニア、オーストラリア、オーストリア、アゼルバイジャン、バーレーン、ベラルーシ、ベルギー、ボスニア・ヘルツェゴビナ、ボツワナ、ブラジル、ブルネイ・ダルサラーム国、ブルガリア、カンボジア、カナダ、チリ、中国、コロンビア、コンゴ、クロアチア、キプロス、チェコ共和国、デンマーク、エジプト、エチオピア、フィンランド、フランス、グルジア、ドイツ、ギリシャ、香港、ハンガリー、インド、インドネシア、イラン・イスラム共和国、イラク、アイルランド、イスラエル、イタリア、日本、ヨルダン、カザフスタン、ケニア、大韓民国、クウェート、キルギスタン、ラトビア、レバノン、リトアニア、ルクセンブルグ、マケドニア、旧ユーゴスラビア共和国、マレーシア、マリ、モーリタニア、メキシコ、モルドバ、モンテネグロ、モロッコ、モザンビーク、ネパール、オランダ、ニュージーランド、オマーン、パキスタン、パレスチナ占領地域、ペルー、フィリピン、ポーランド、ポルトガル、カタール、ルーマニア、ロシア連邦、サウジアラビア、シンガポール、スロバキア、スロベニア、南アフリカ、スペイン、スイス、台湾、タンザニア連合共和国、タイ、トルコ、トルクメニスタン、ウガンダ、ウクライナ、アラブ首長国連邦、イギリス、アメリカ、ウズベキスタン、ベトナム、バージン諸島。

出典:verizonenterprise.com/jp/DBIR/2014

セキュリティインシデントとデータ漏洩/侵害の比較

被害にあった企業・組織の業界別および規模別の
セキュリティインシデント数

業界	合計	小中規模の企業・組織	大規模の企業・組織	不明
ホテル業 [72]	212	115	34	63
管理サービス業 [56]	16	8	7	1
農業 [11]	4	0	3	1
建設業 [23]	4	2	0	2
教育サービス業 [61]	33	2	10	21
芸術/娯楽業 [71]	20	8	1	11
金融業 [52]	856	43	189	624
医療業 [62]	26	6	1	19
情報産業 [51]	1,132	16	27	1,089
マネジメントサービス [55]	10	1	3	6
製造業 [31, 32, 33]	251	7	33	211
鉱業 [21]	11	0	8	3
専門サービス業 [54]	360	26	10	324
公的機関 [92]	47,479	26	47,074	379
不動産業 [53]	8	4	0	4
小売業 [44, 45]	467	36	11	420
貿易/通商業 [42]	4	3	0	1
運輸業 [48, 49]	27	3	7	17
公益事業 [22]	166	2	3	161
その他 [81]	27	13	0	14
不明	12,384	5,498	4	6,822
合計	**63,437**	**5,819**	**47,425**	**10,193**

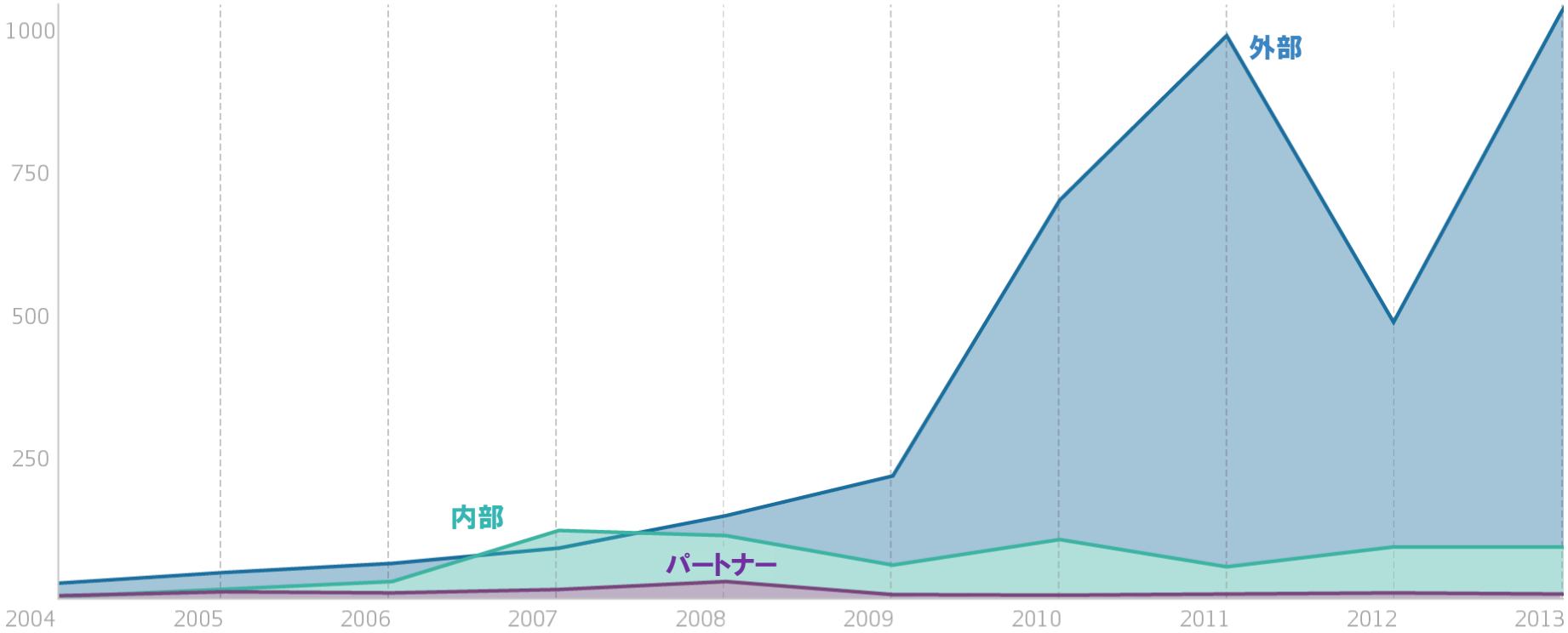
被害にあった企業・組織の業界別および規模別による
データ漏洩/侵害が確認されたセキュリティインシデント数

業界	合計	小中規模の企業・組織	大規模の企業・組織	不明
ホテル業 [72]	137	113	21	3
管理サービス業 [56]	7	3	3	1
建設業 [23]	2	1	0	1
教育サービス業 [61]	15	1	9	5
芸術/娯楽業 [71]	4	3	1	0
金融業 [52]	465	24	36	405
医療業 [62]	7	4	0	3
情報産業 [51]	31	7	6	18
マネジメントサービス [55]	1	1	0	0
製造業 [31, 32, 33]	59	6	12	41
鉱業 [21]	10	0	7	3
専門サービス業 [54]	75	13	5	57
公的機関 [92]	175	16	26	133
不動産業 [53]	4	2	0	2
小売業 [44, 45]	148	35	11	102
貿易/通商業 [42]	3	2	0	1
運輸業 [48, 49]	10	2	4	4
公益事業 [22]	80	2	0	78
その他 [81]	8	6	0	2
不明	126	2	3	121
合計	**1,367**	**243**	**144**	**980**

過去10年間の
データ漏洩/侵害調査報告書
10年間で合計4,217件の
データ漏洩/侵害事案

外部の実行者

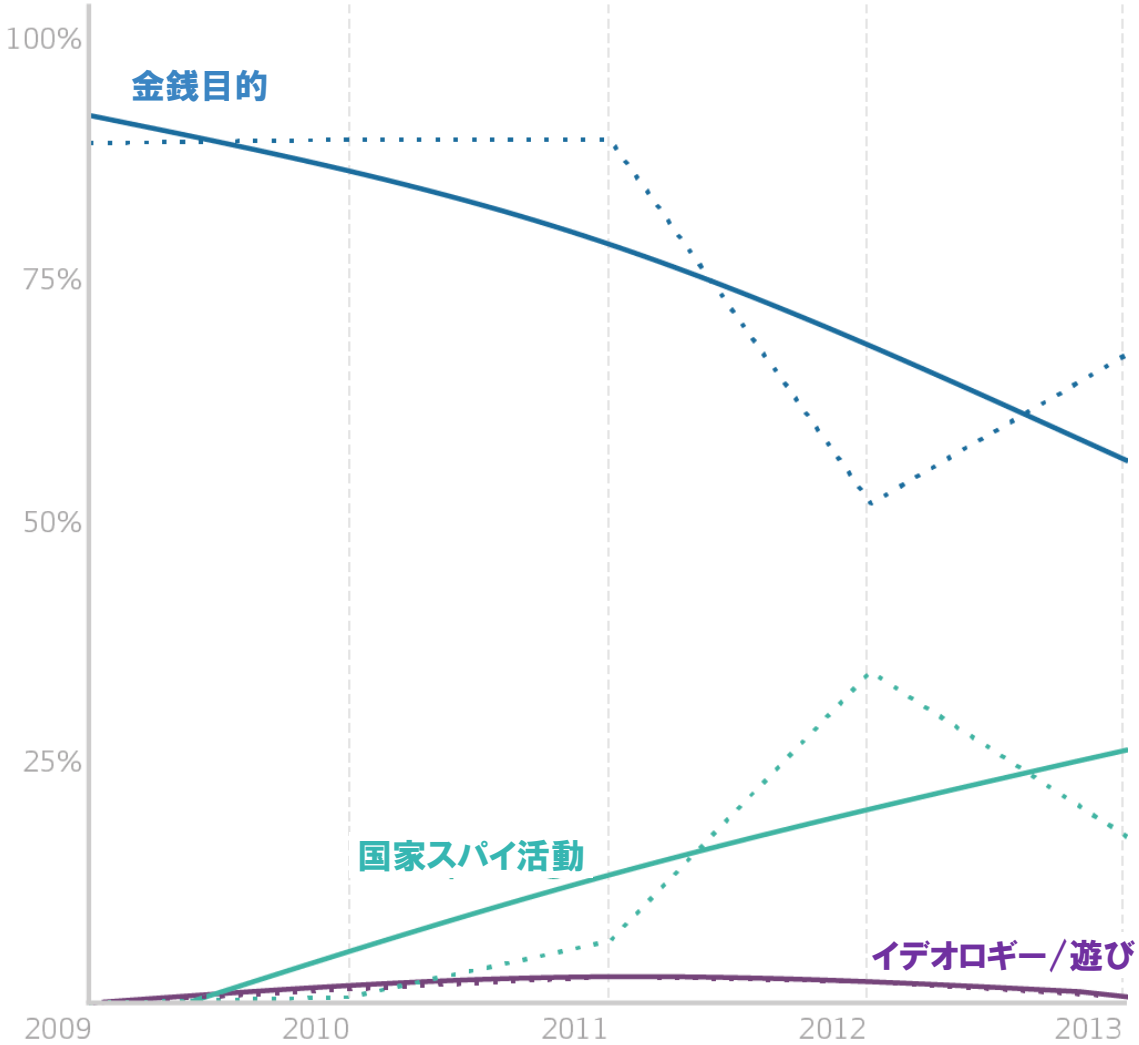
図4.
脅威実行者別のデータ漏洩/侵害事案の件数と推移



出典：verizonenterprise.com/jp/DBIR/2014

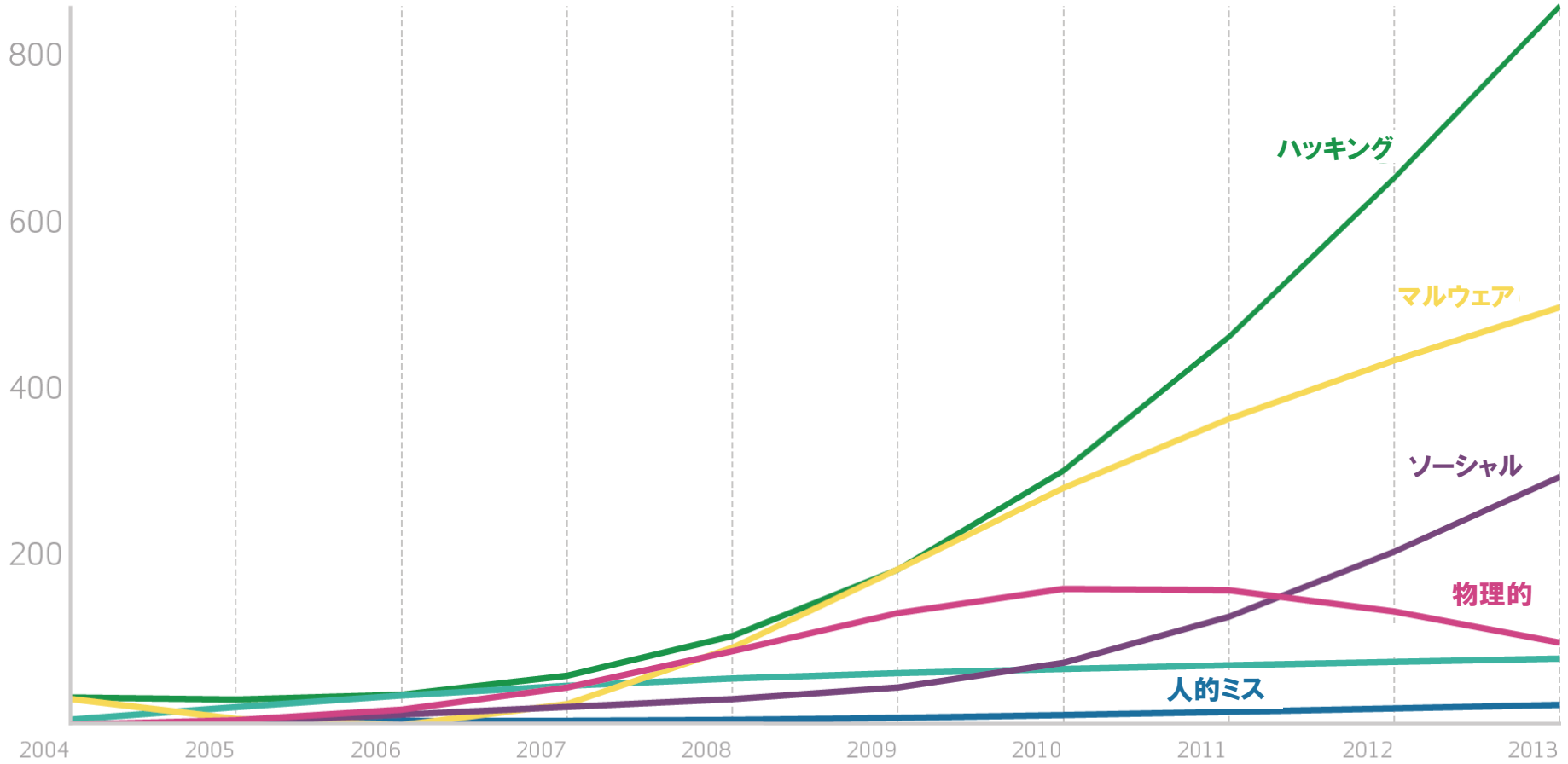
外部の実行者：動機

脅威実行者の動機別によるデータ漏洩／侵害事案の割合と推移



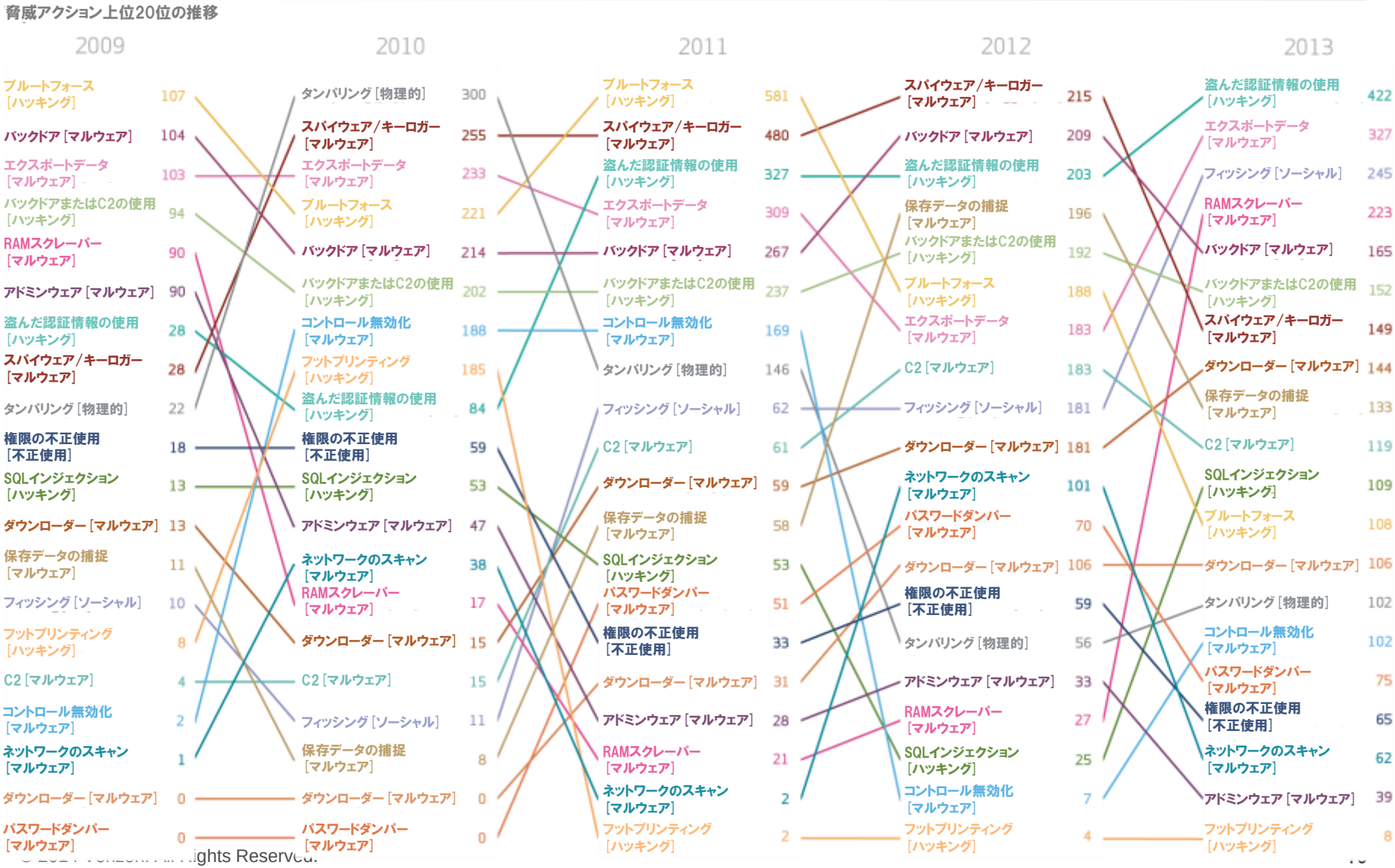
アクションの推移

図8.
脅威アクション別によるデータ漏洩/侵害事案の件数と推移



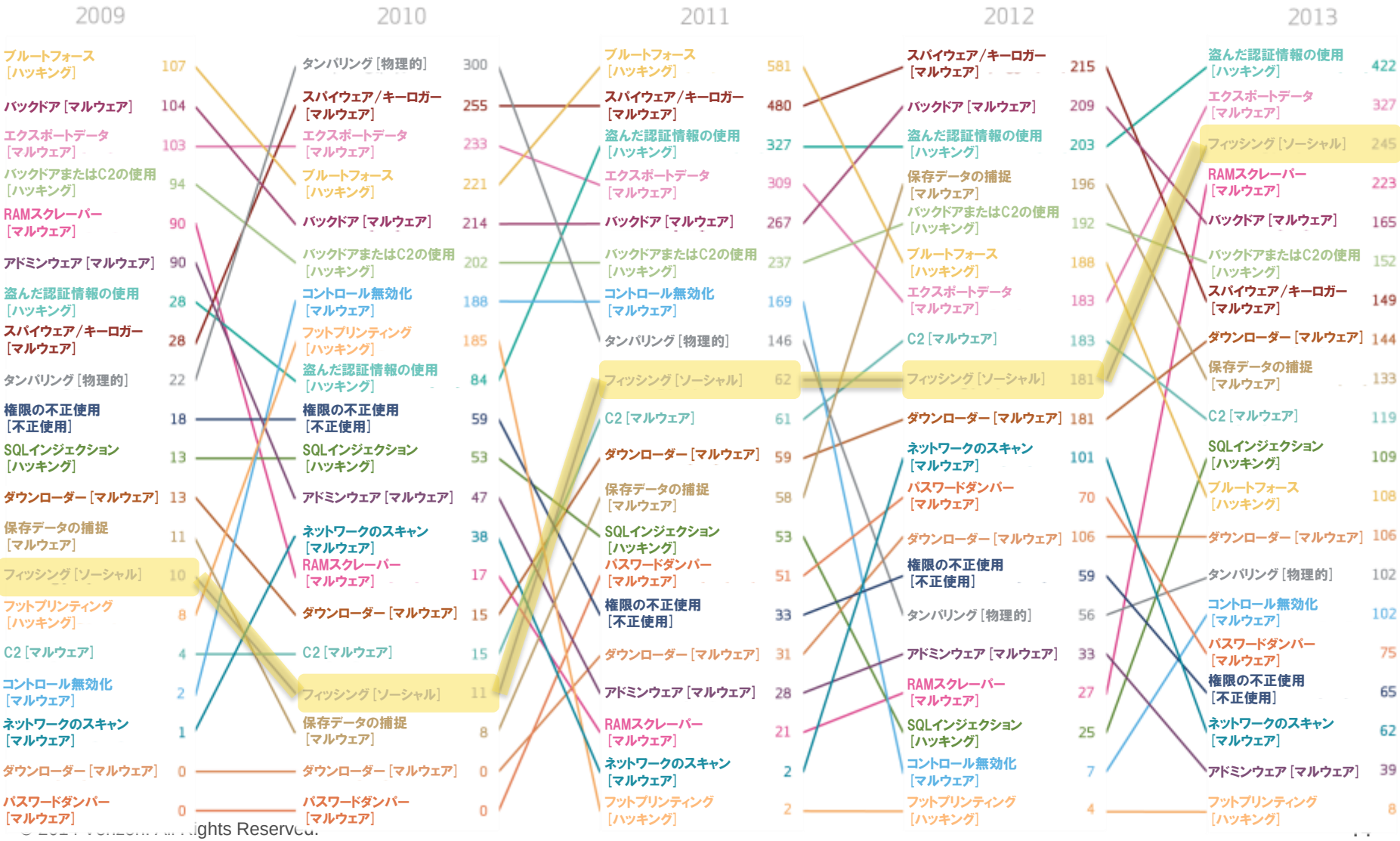
出典:verizonenterprise.com/jp/DBIR/2014

過去5年間の脅威アクションの推移：



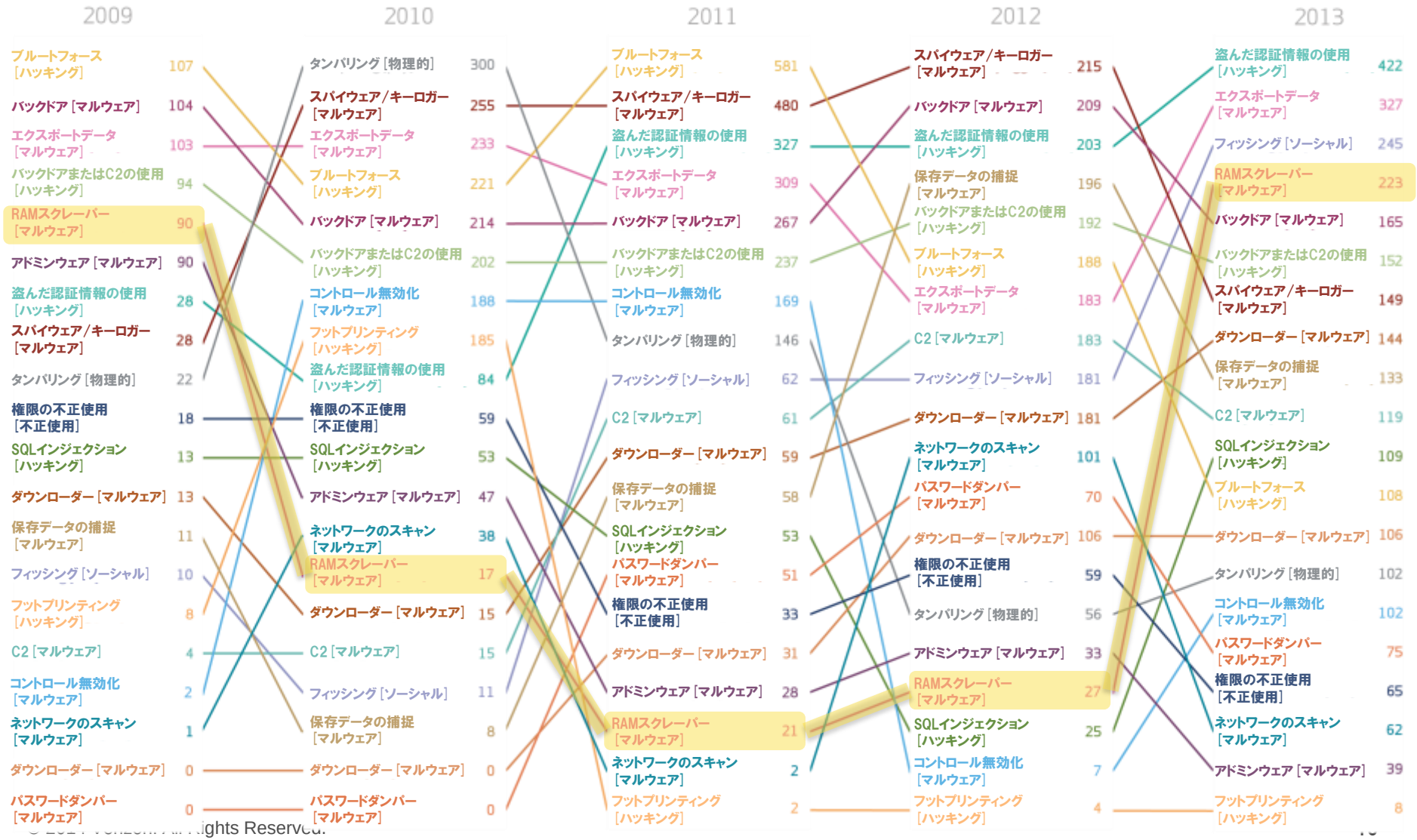
過去5年間の脅威アクションの推移：フィッシング

脅威アクション上位20位の推移

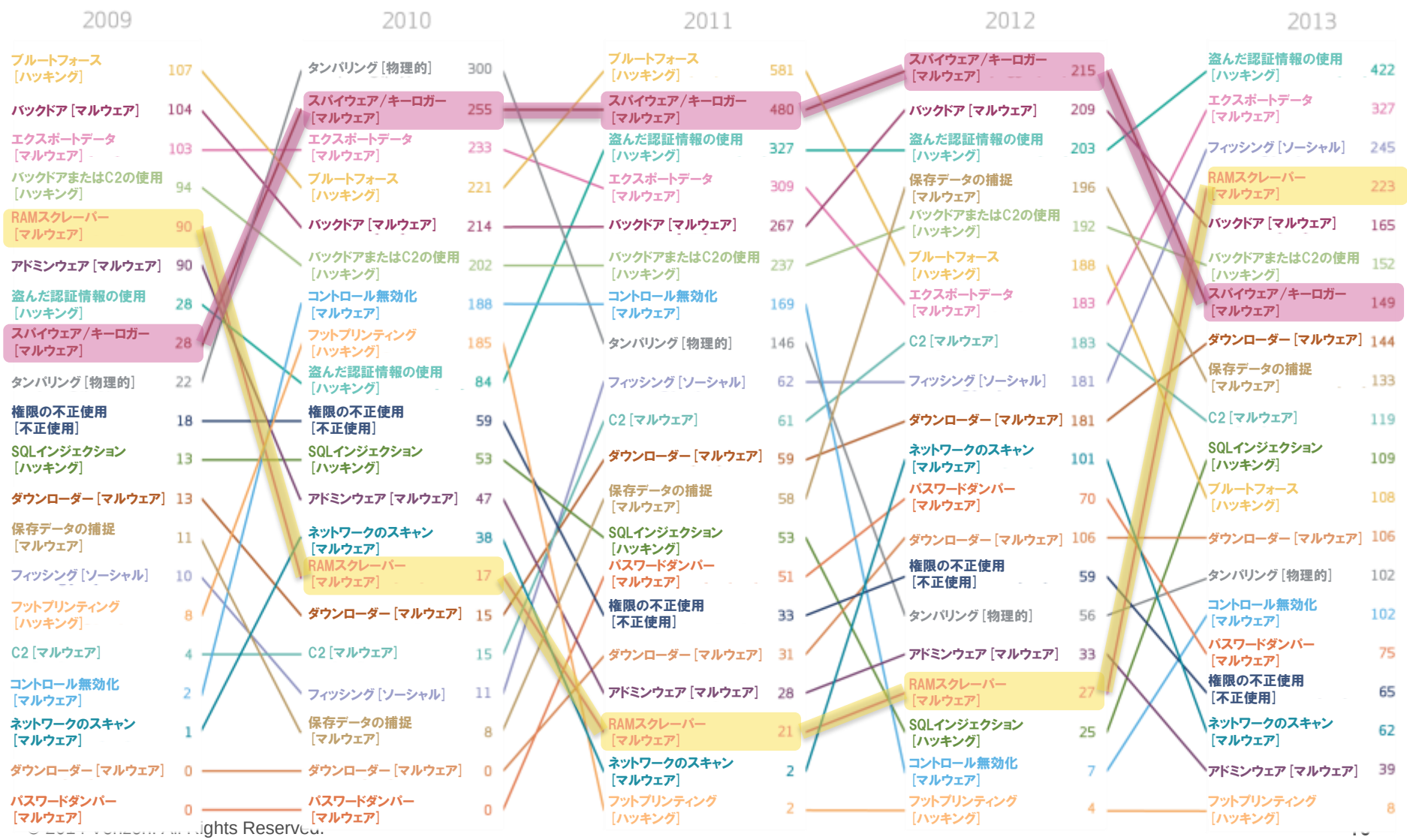


過去5年間の脅威アクションの推移：RAMスクレーパー

脅威アクション上位20位の推移

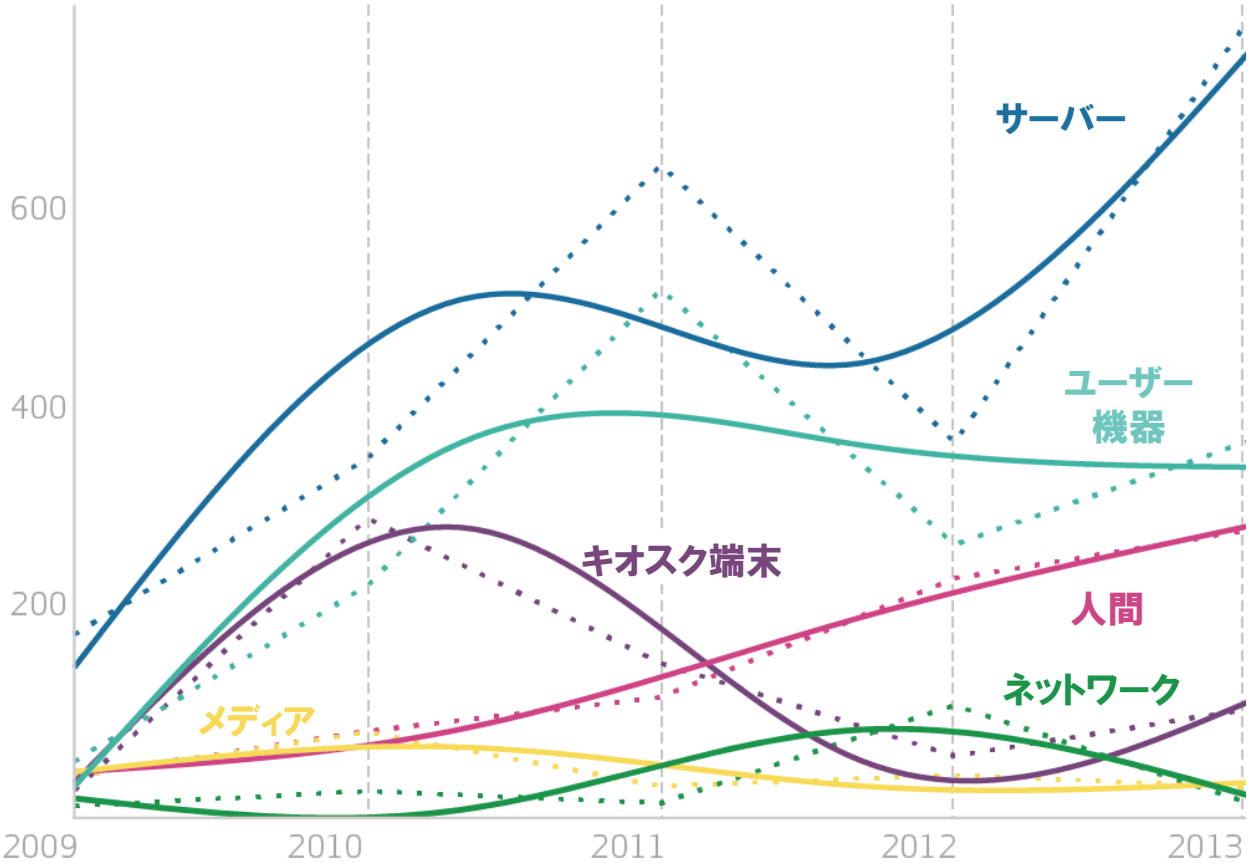


過去5年間の脅威アクションの推移：RAMスクレーパーとキーロガー



資産

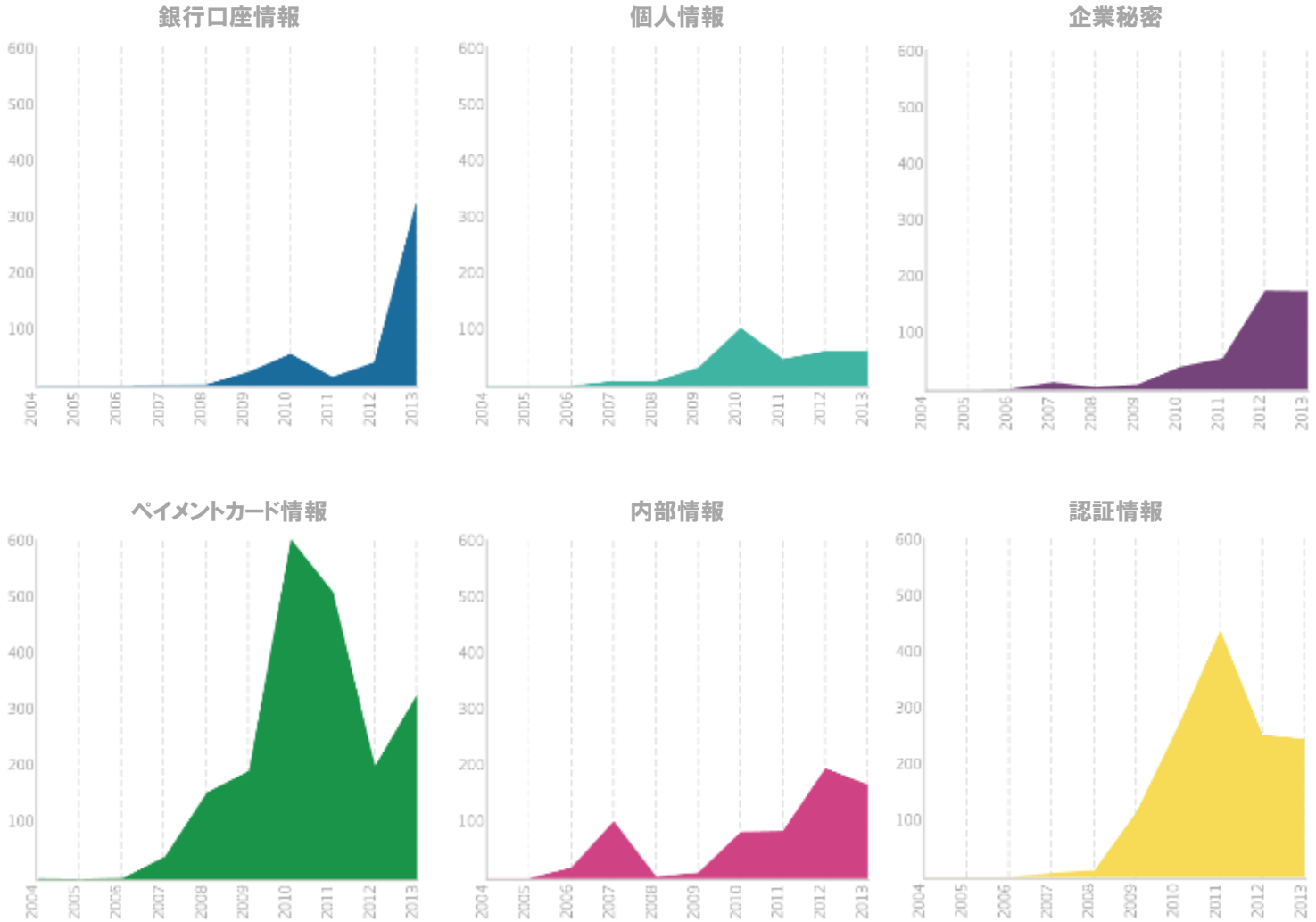
図11.
資産別のデータ漏洩/侵害事案の件数と推移



出典:verizonenterprise.com/jp/DBIR/2014

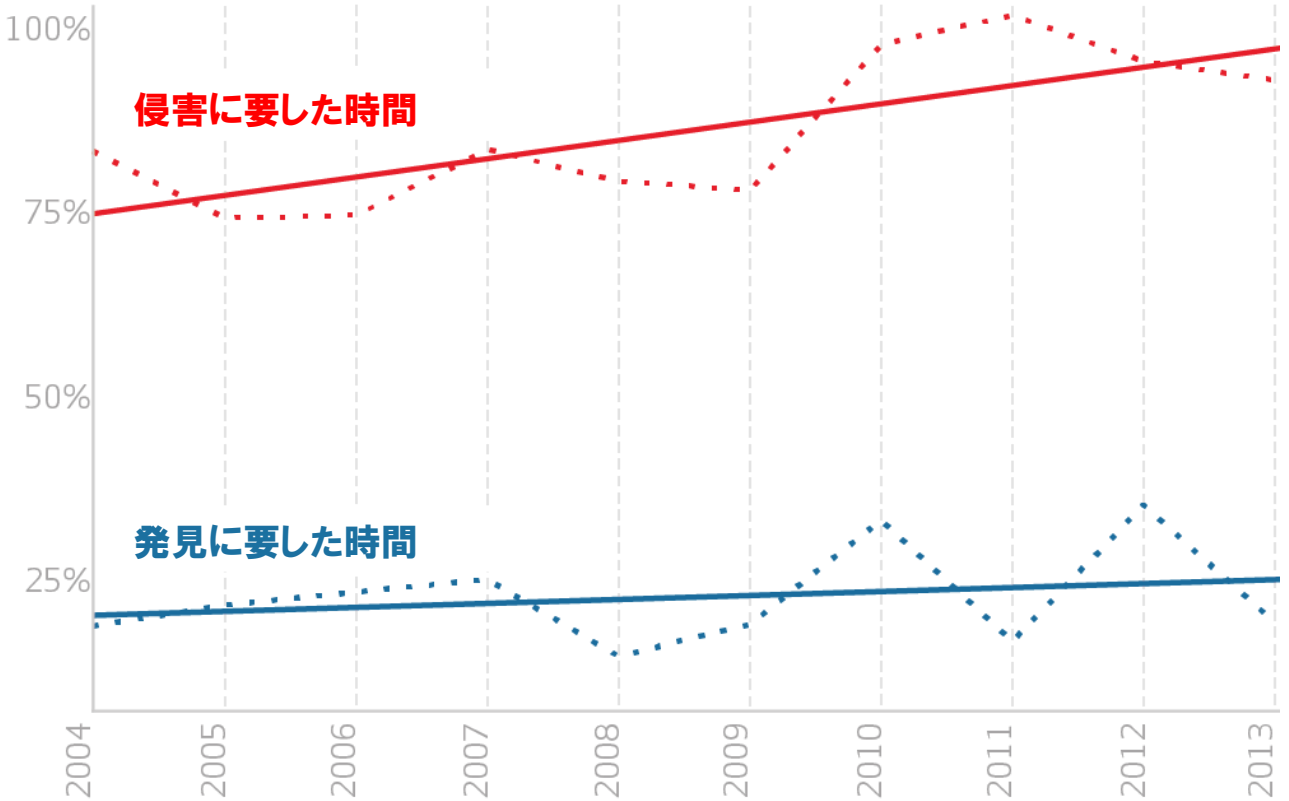
データのタイプ

漏洩情報の種類別によるデータ漏洩/侵害事案の件数と推移



侵害に要した時間と発見に要した時間の比較

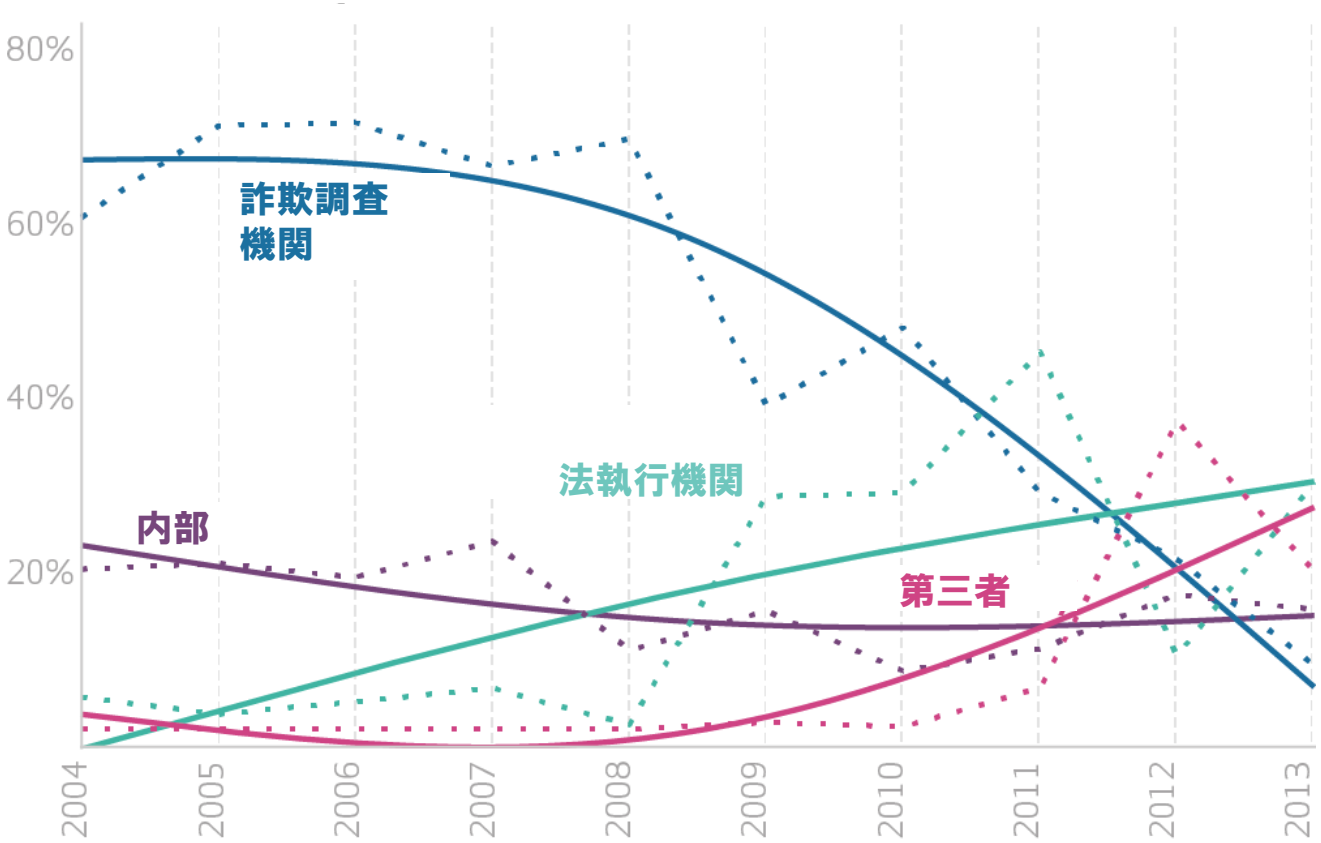
図13.
侵害に要した時間(赤)/発見に要した時間(青)が数日以内の割合



出典:verizonenterprise.com/jp/DBIR/2014

発見方法

図14.
データ漏洩/侵害の発見方法の推移



出典：verizonenterprise.com/jp/DBIR/2014

データ漏洩/侵害調査報告書の新しいアプローチ

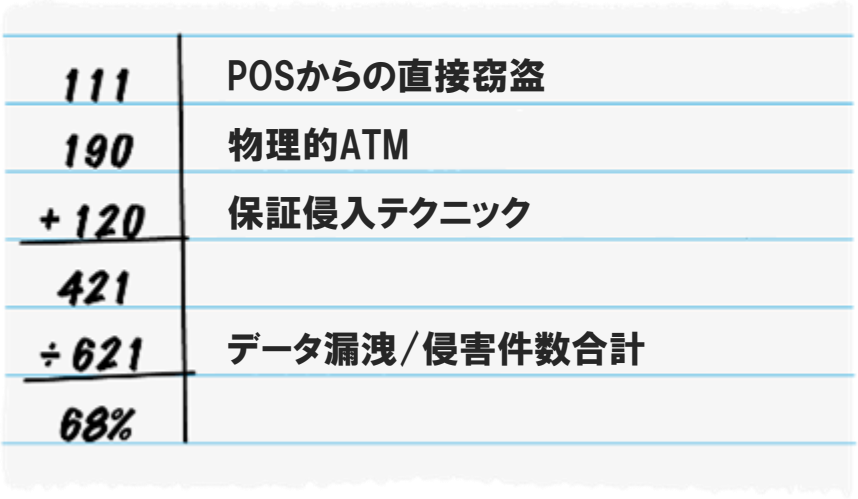
データ漏洩/侵害に関するデータの分析

過去の漏洩/侵害調査報告書に対する批判

1. データ漏洩/侵害の影響やコストに関する情報の欠如
2. 業界によっては「無関係の要因」による知見の歪み
   – 例:「POS/ATMを使っていない」、「製造業者だ」
3. 「根本原因」分析が不十分で、業界に応じた具体的な推奨事項が提示されていない
4. 反省点:「スターウォーズ」と「プリンセス・ブライド・ストーリー」への言及がない

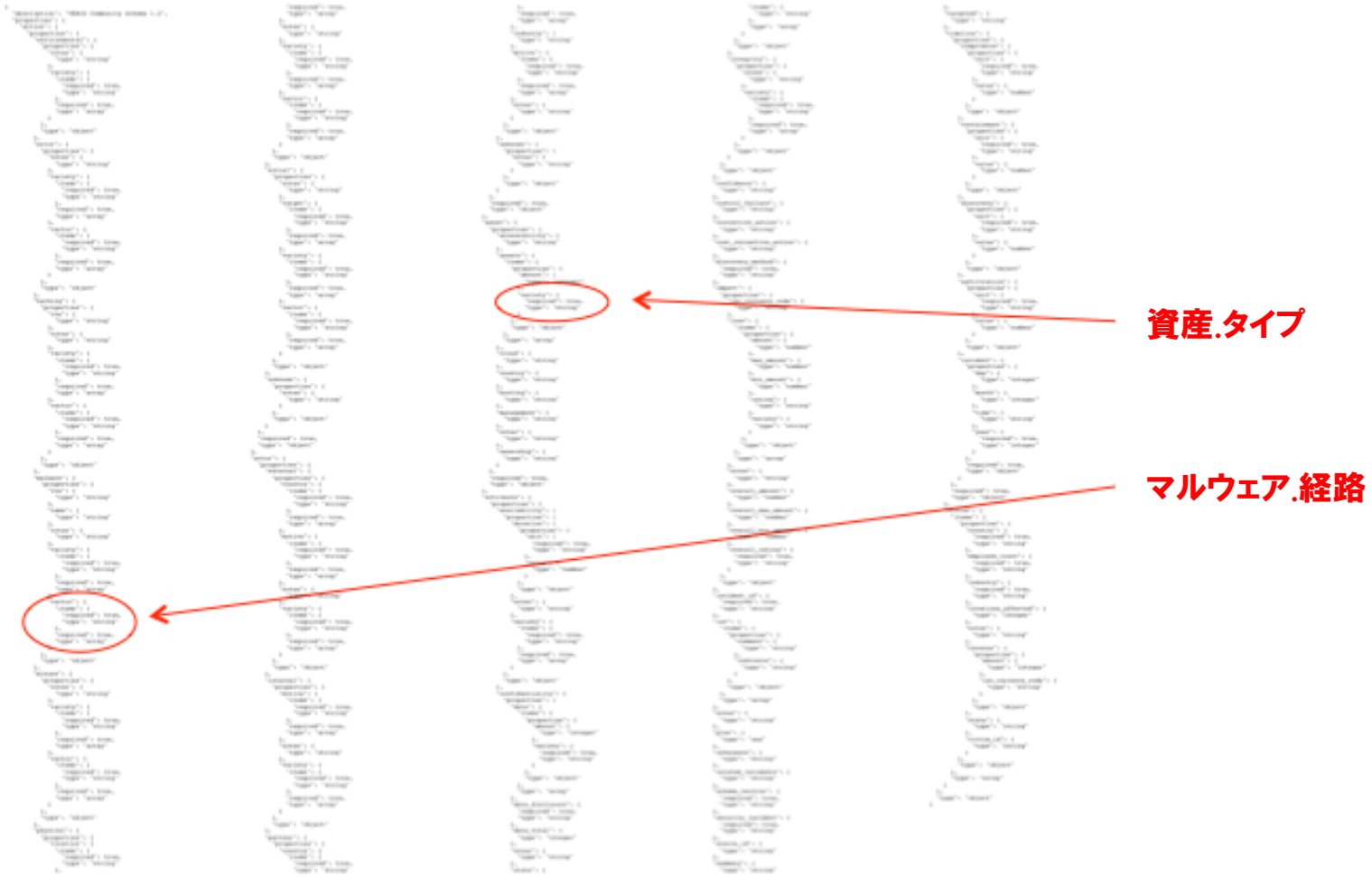
データ漏洩/侵害調査報告書:図15

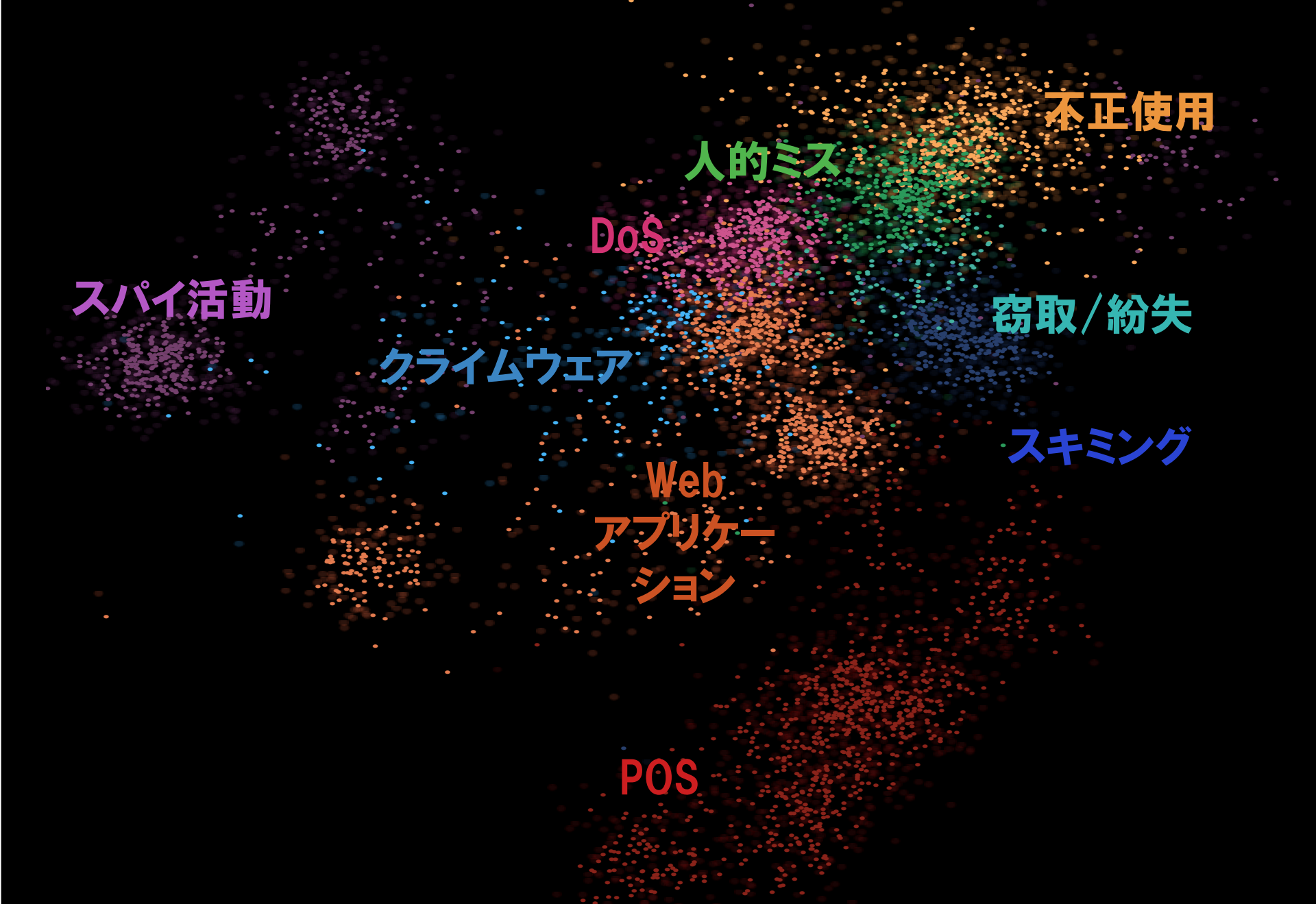
図15.
2013年度データ漏洩/侵害調査報告書で広く観測された
インシデントパターンの件数



出典:verizonenterprise.com/jp/DBIR/2014

セキュリティインシデントの「DNA」

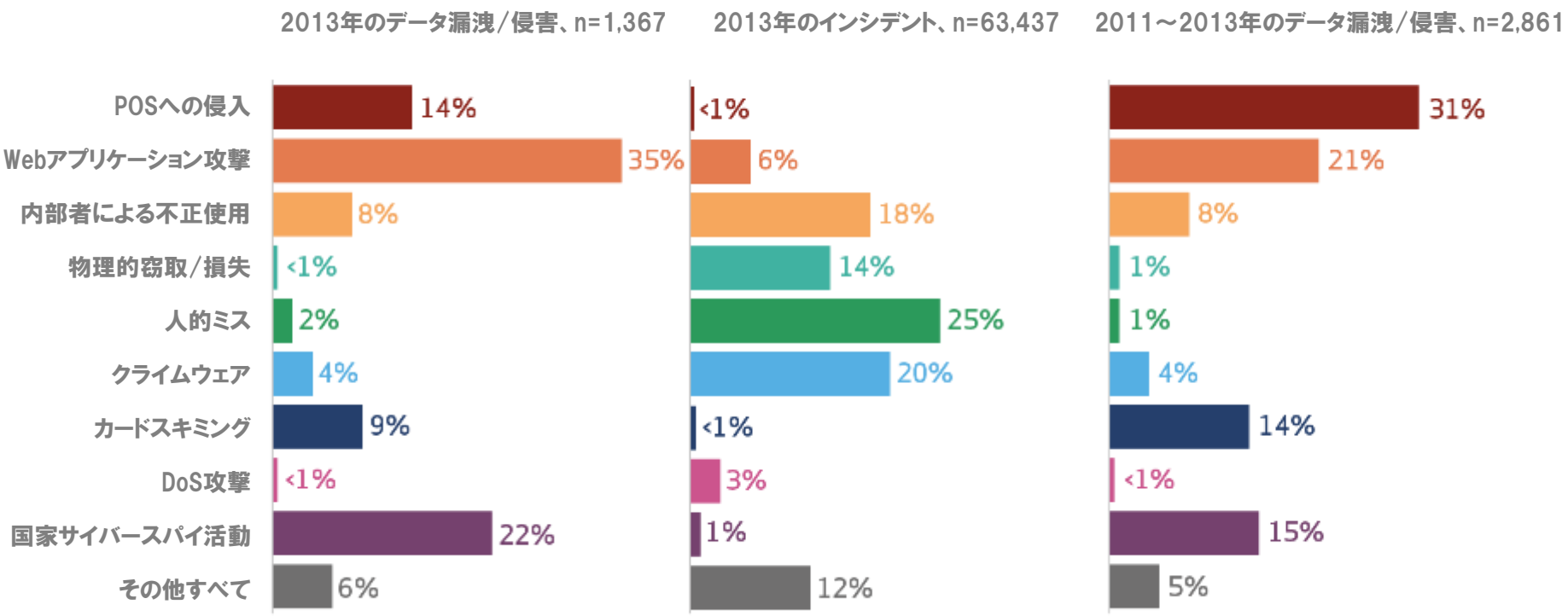




9種類のインシデント分類パターン

パターンの発生頻度

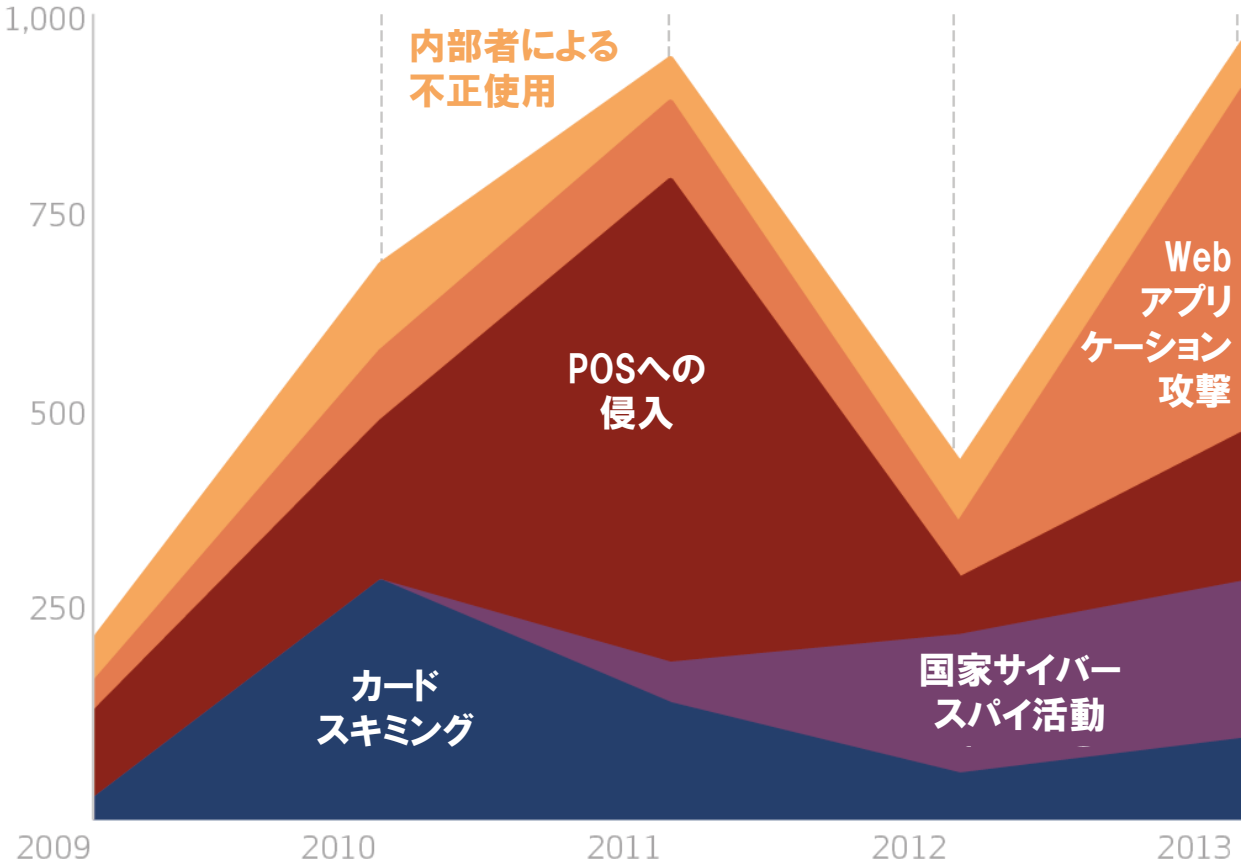
図16.
インシデント分類パターンの発生頻度



出典:verizonenterprise.com/jp/DBIR/2014

パターンの推移

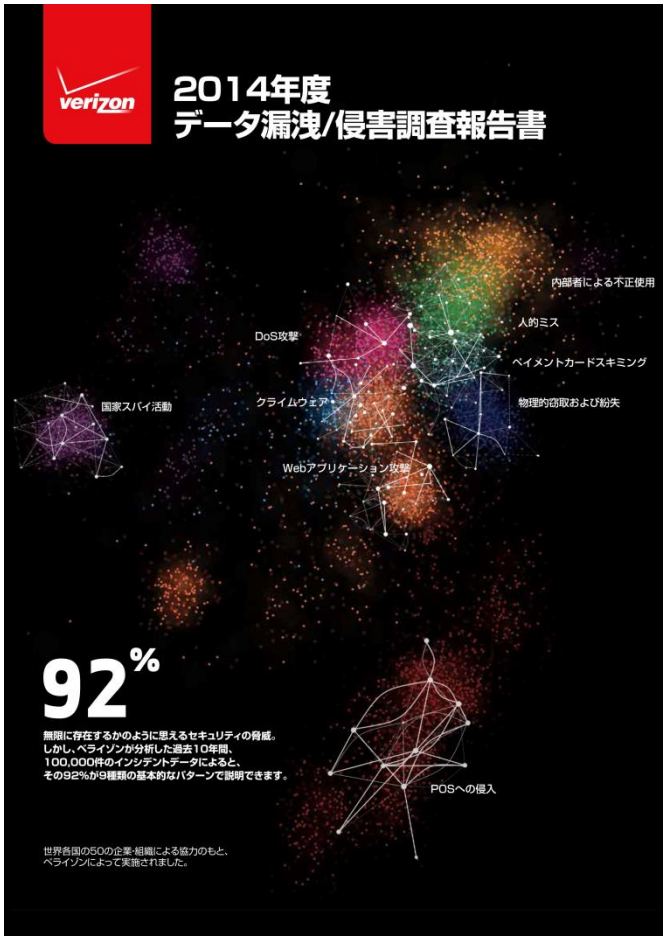
図17.
主なインシデント分類パターンの件数と推移



出典：verizonenterprise.com/jp/DBIR/2014

業界	POSへの侵入	Webアプリケーション攻撃	内部者による不正使用	窃取/紛失	人的ミス	クライムウェア	ペイメントカードスキミング	DoS攻撃	国家スパイ活動	その他すべて
ホテル業 [72]	75%	1%	8%	1%	1%	1%	<1%	10%		4%
管理サービス業 [56]		8%	27%	12%	43%	1%		1%	1%	7%
建設業 [23]	7%		13%	13%	7%	33%			13%	13%
教育サービス業 [61]	<1%	19%	8%	15%	20%	6%	<1%	6%	2%	22%
芸術/娯楽業 [71]	7%	22%	10%	7%	12%	2%	2%	32%		5%
金融業 [52]	<1%	27%	7%	3%	5%	4%	22%	26%	<1%	6%
医療業 [62]	9%	3%	15%	46%	12%	3%	<1%	2%	<1%	10%
情報産業 [51]	<1%	41%	1%	1%	1%	31%	<1%	9%	1%	16%
マネジメントサービス [55]		11%	6%	6%	6%		11%	44%	11%	6%
製造業 [31, 32, 33]		14%	8%	4%	2%	9%		24%	30%	9%
鉱業 [21]			25%	10%	5%	5%	5%	5%	40%	5%
専門サービス業 [54]	<1%	9%	6%	4%	3%	3%		37%	29%	8%
公的機関 [92]		<1%	24%	19%	34%	21%		<1%	<1%	2%
不動産業 [53]		10%	37%	13%	20%	7%			3%	10%
小売業 [44, 45]	31%	10%	4%	2%	2%	2%	6%	33%	<1%	10%
貿易/通商業 [42]	6%	30%	6%	6%	9%	9%	3%	3%		27%
運輸業 [48, 49]		15%	16%	7%	6%	15%	5%	3%	24%	8%
公益事業 [22]		38%	3%	1%	2%	31%		14%	7%	3%
その他 [81]	1%	29%	13%	13%	10%	3%		9%	6%	17%

質疑応答



Introducing Tokyoセキュリティオペレーションセンター

- ベライゾンが展開する8つ目のセキュリティオペレーションセンター（SOC)
- 日本語・英語の多言語サポート対応で24時間365日のグローバルセキュリティ監視/運用サービスを提供
- 日本のお客様のセキュリティログを国外に持ち出しすることなく、国内でセキュアに管理
- 海外及び日本を標的とした攻撃の情報収集および対応をするため、グローバルセキュリティサービスの拠点となるSOCを東京に開設