「2013年度データ漏洩侵害/調査報告書」から、データ漏洩の傾向と対策

ベライゾンジャパン合同会社
グローバル調査対応
プリンシパル コンサルタント
鵜沢　裕一
PID#

著作権および使用条件

本文書および添付資料は、ベライゾンの著作権に属するものであり、ベライゾンのサービス評価以外の目的で使用することは禁止されています。

本文書および添付資料は、企業の中でその内容を必要としない従業員に対して、または、ベライゾンから書面による許可を得ることなく第三者に対して開示、配布、または譲渡することはできません。

データ漏洩/侵害調査報告書（DBIR）

データ漏洩/侵害の調査で得られたフォレンジック結果をもとにいかに機密データが盗まれたか、実行者は誰か、動機は何かについて分析を行っており、また、どのようにしてデータ漏洩/侵害を防止できるかについても考察しています

「データ漏洩/侵害調査報告書」日本語完全版ダウンロード:
https://eentry11.securesites.net/verizon_security/contact01/index.html

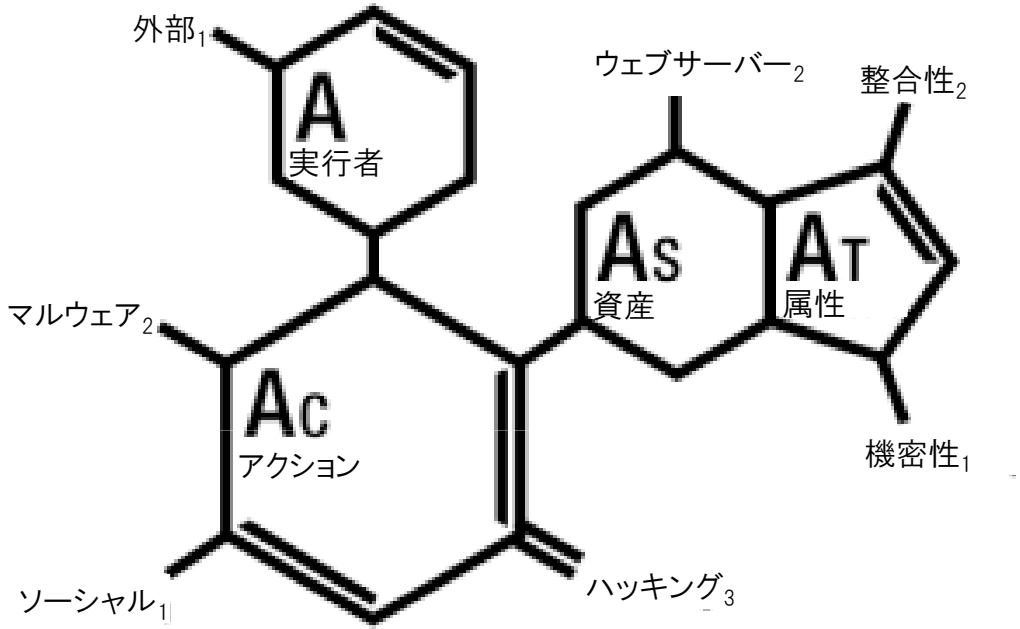
データ漏洩/侵害調査報告書（DBIR）

―『2013年度データ漏洩/侵害調査報告書』―
世界19の機関・組織が協力
4万7千件を超えるセキュリティインシデント
621件の確認されたデータ漏洩/侵害

ベライゾンRISKチームによるグローバルな研究調査 ・ 協力機関･組織一覧

VERISは、共通用語や基準を使って、セキュリティインシデント(脅威)を一定の形式で記録できるフレームワークです

(VERISは公開されており、無料で使用できます)



実行者 ー 誰がデータ漏洩/侵害を実行したか？

アクション ー どの様な方法で実行したか？

資産 ー 何が侵害されたか？

属性 ー どの様に影響を受けたか？

http://www.veriscommunity.net

脅威実行者

図10：脅威実行者別のデータ漏洩/侵害事例の割合

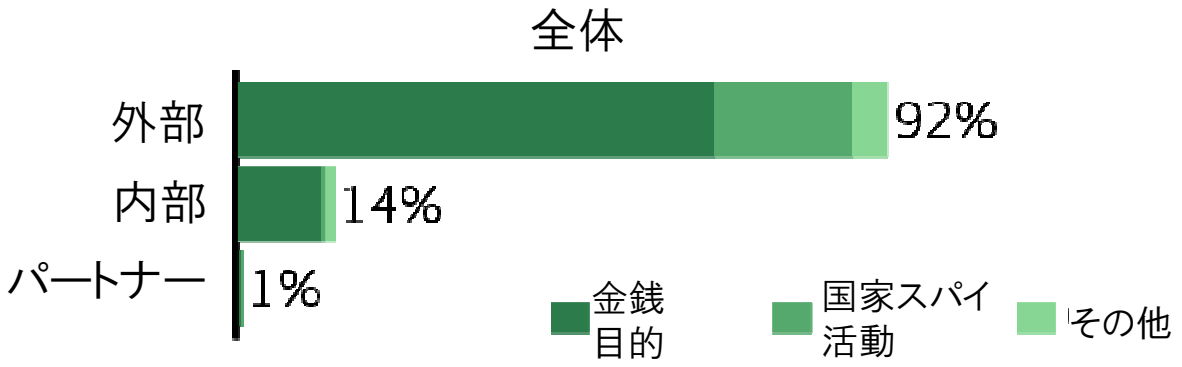
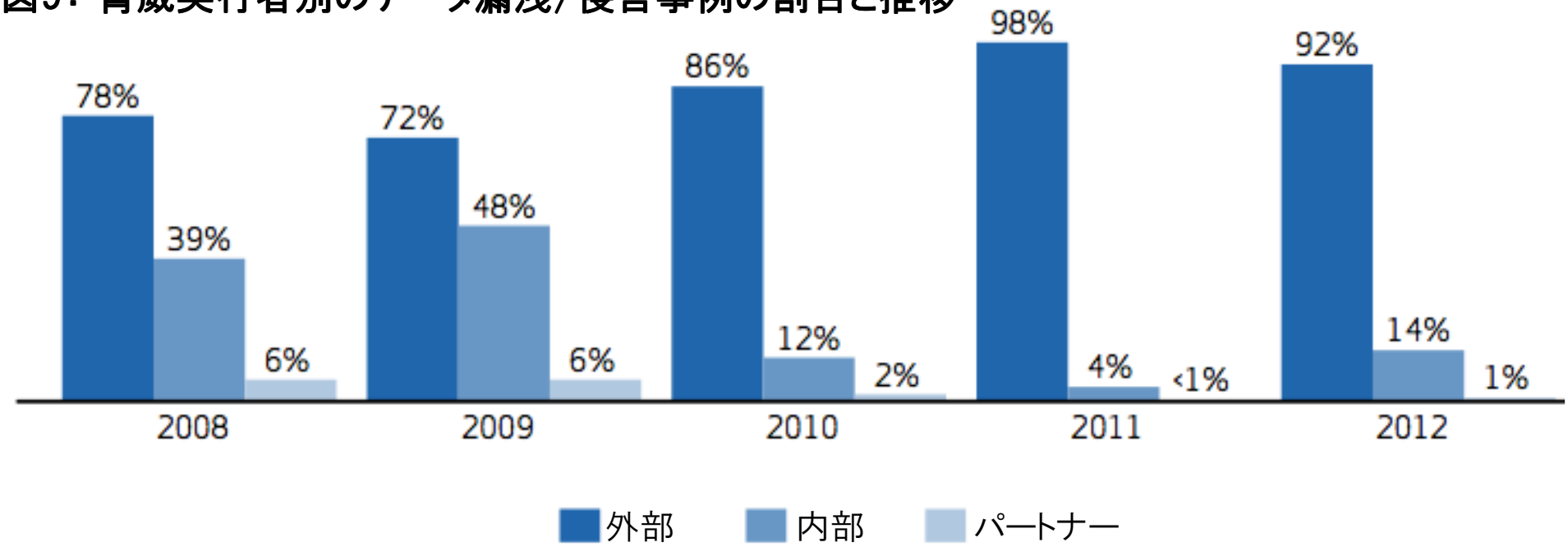


図9：脅威実行者別のデータ漏洩/侵害事例の割合と推移



脅威実行者

図12：外部実行者の種類で分類した場合のデータ漏洩/侵害の割合

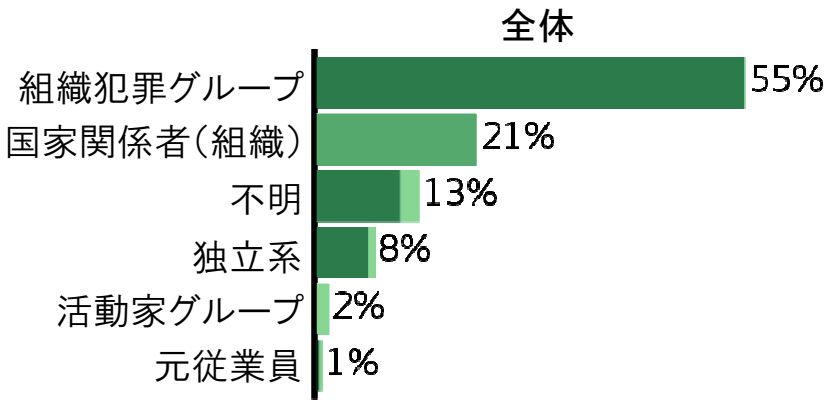


図 13：外部実行者の国（上位10位）

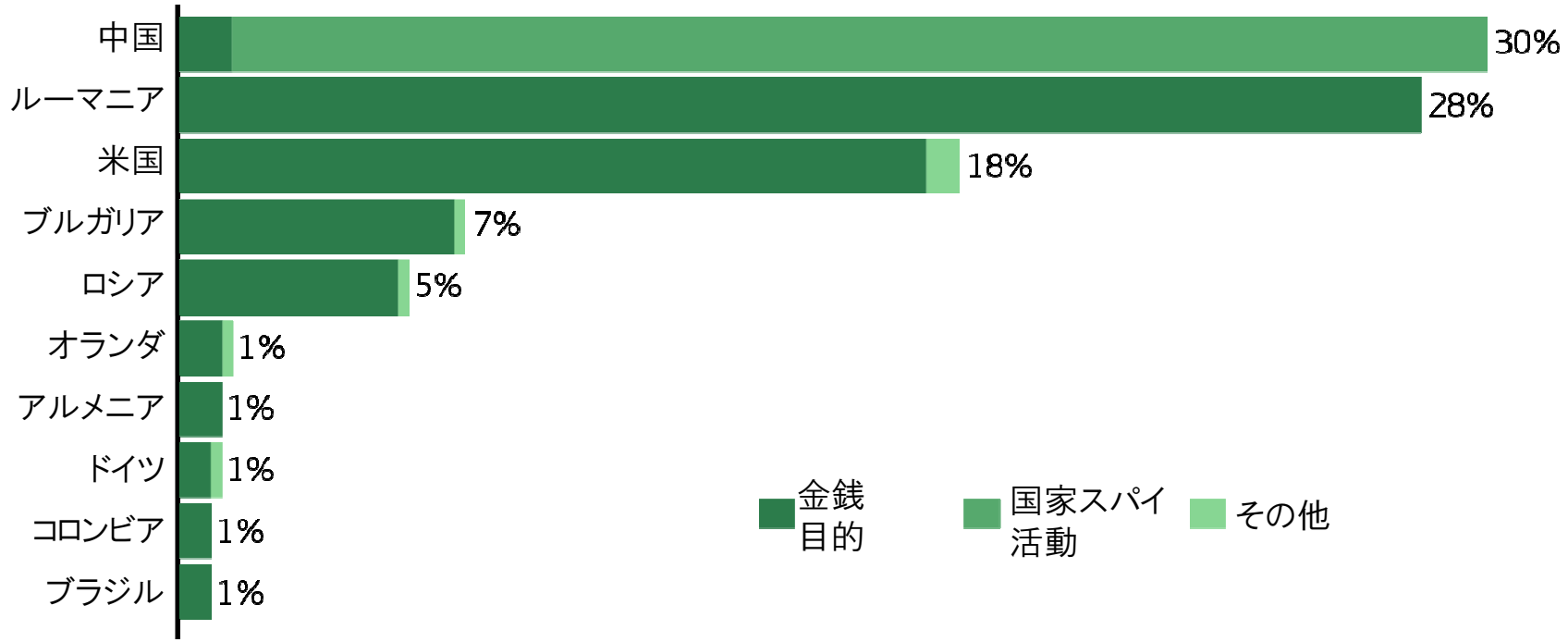
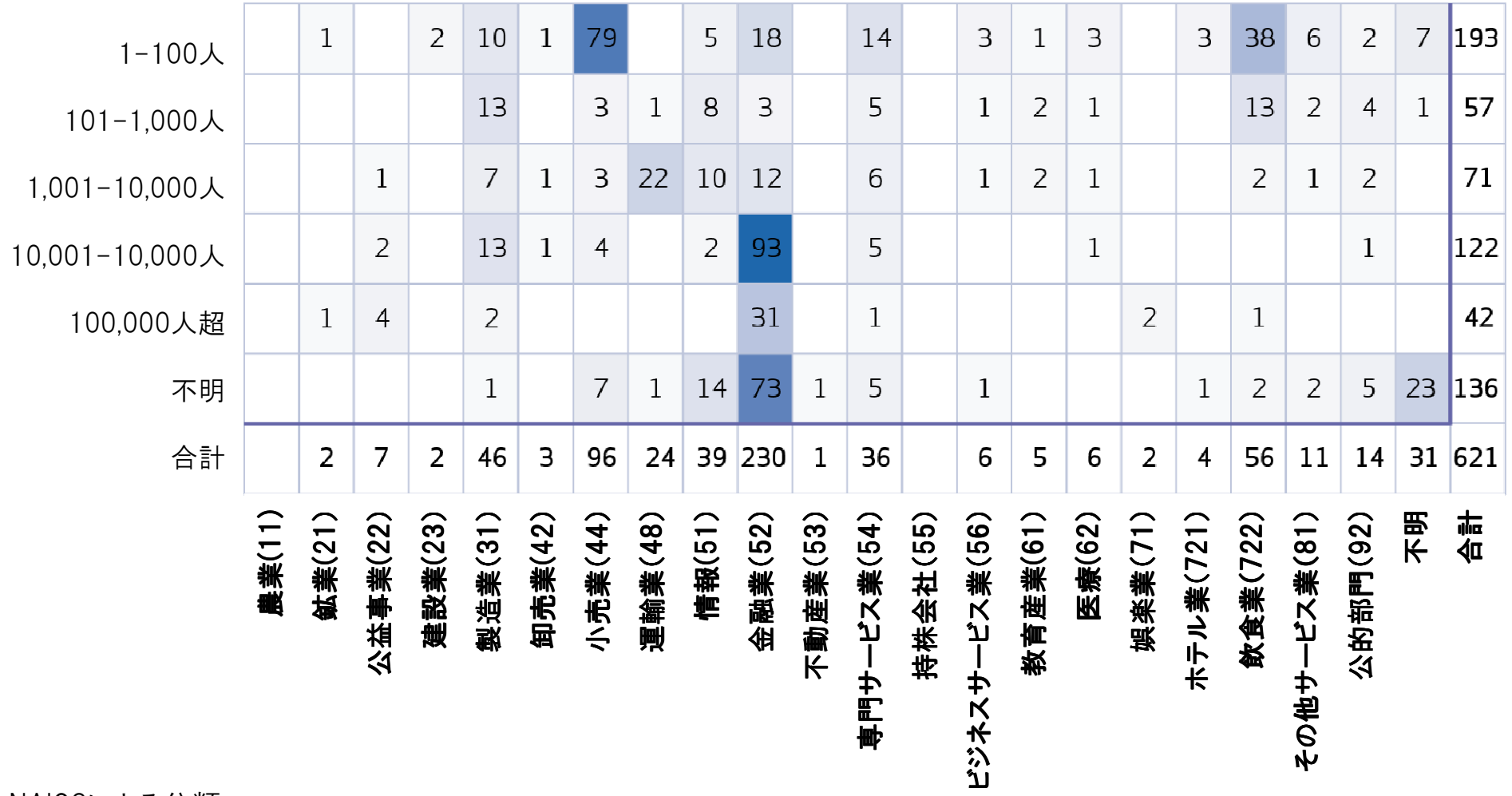


図2:データ漏洩/侵害事例を企業・組織の従業員数と業界を基準に分類*

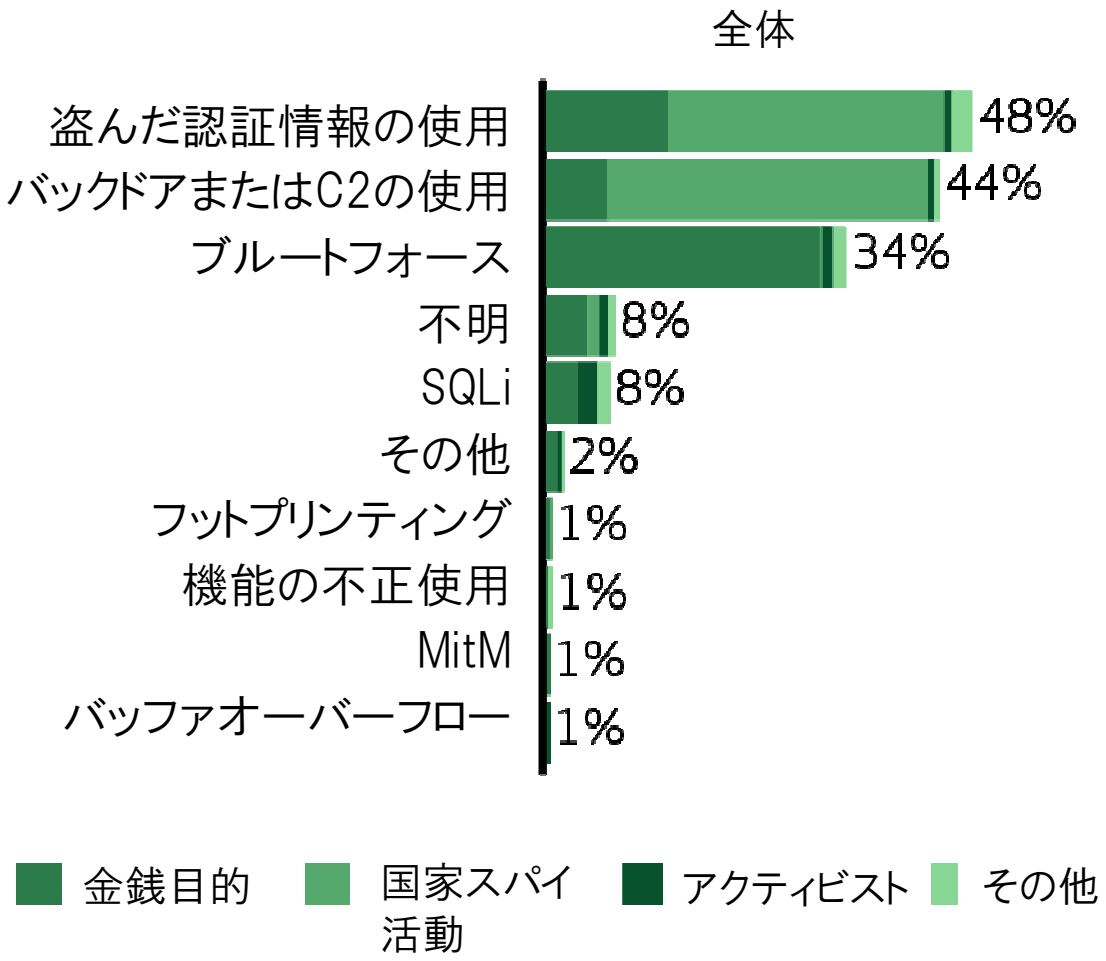


	農業(11)	鉱業(21)	公益事業(22)	建設業(23)	製造業(31)	卸売業(42)	小売業(44)	運輸業(48)	情報(51)	金融業(52)	不動産業(53)	専門サービス業(54)	持株会社(55)	ビジネスサービス業(56)	教育産業(61)	医療(62)	娯楽業(71)	ホテル業(721)	飲食業(722)	その他サービス業(81)	公的部門(92)	不明	合計
1-100人		1		2	10	1	79		5	18		14		3	1	3		3	38	6	2	7	193
101-1,000人					13		3	1	8	3		5		1	2	1			13	2	4	1	57
1,001-10,000人			1		7	1	3	22	10	12		6		1	2	1			2	1	2		71
10,001-10,000人			2		13	1	4		2	93		5				1					1		122
100,000人超		1	4		2					31		1					2		1				42
不明					1		7	1	14	73	1	5		1				1	2	2	5	23	136
合計		2	7	2	46	3	96	24	39	230	1	36		6	5	6	2	4	56	11	14	31	621

*NAICSによる分類

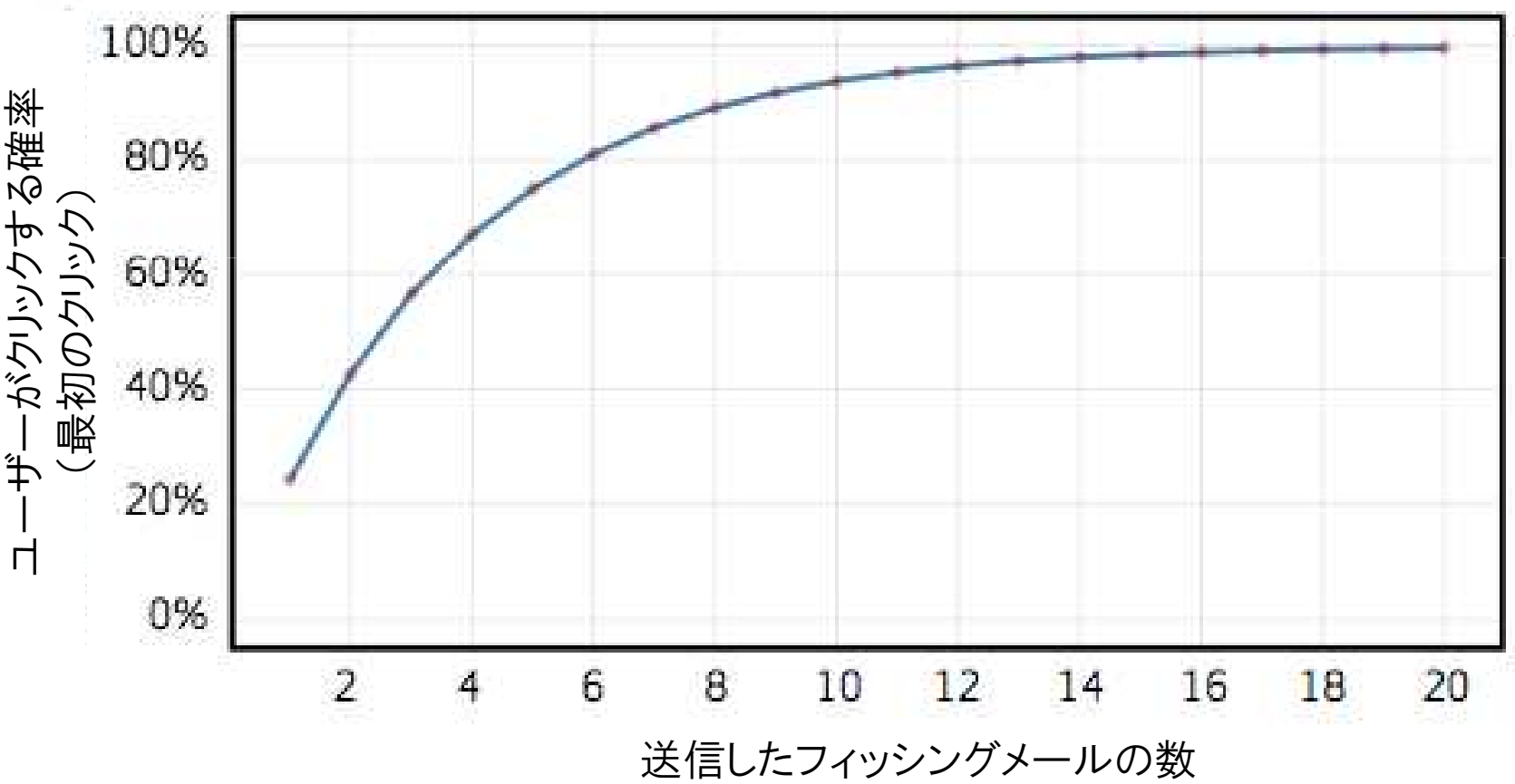
ハッキングのタイプ

図23：ハッキングのタイプ



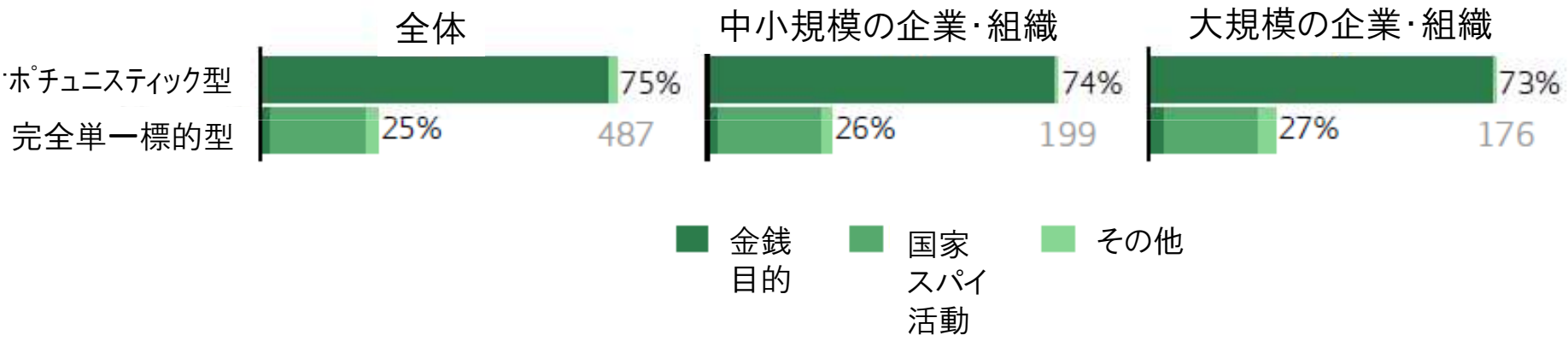
脅威アクション

図28：「クリック」は不可避？



攻撃の標的選定

図38：攻撃の標的選定



属性 ー データ窃盗と動機

図35: 侵害されたデータのタイプと脅威実行者の動機で分類したデータ漏洩/侵害の数

	ペイメントカード情報	銀行口座情報	認証情報	個人情報	医療記録	機密情報	著作権付き	システム情報	内部情報	企業秘密	その他	不明
金銭目的	376	37	100	47	1		2	7	10	6	1	13
国家スパイ活動	1	1	119	1	1	3	1	113	122	119		21
アクティビスト	2		3	8	1			2	4			
その他	1	1	14	6			1	2	10			8

攻撃の難しさ

図39：攻撃の難しさ

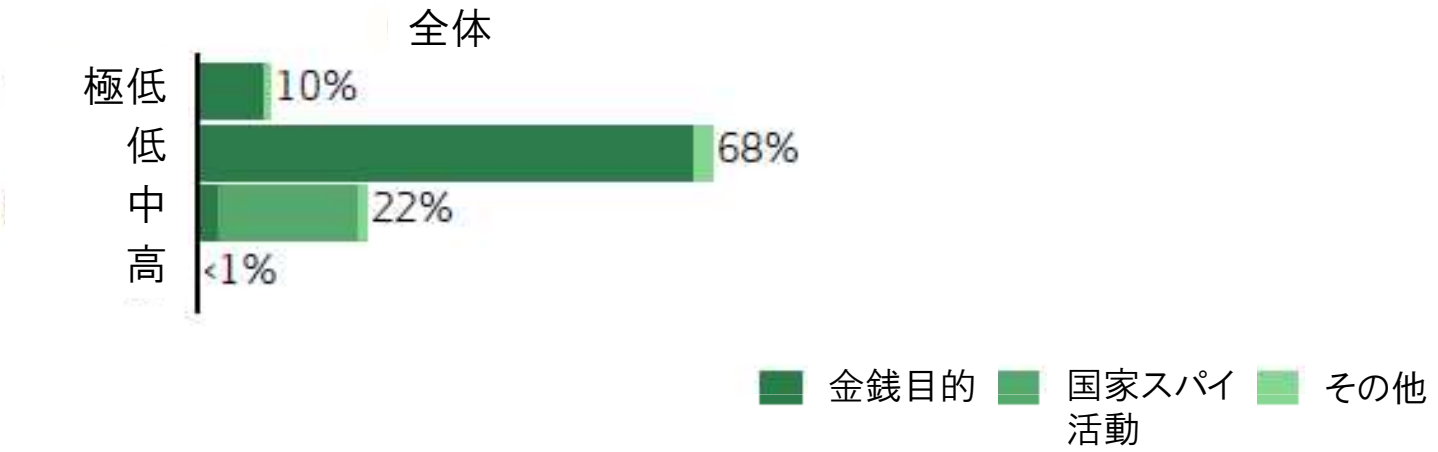
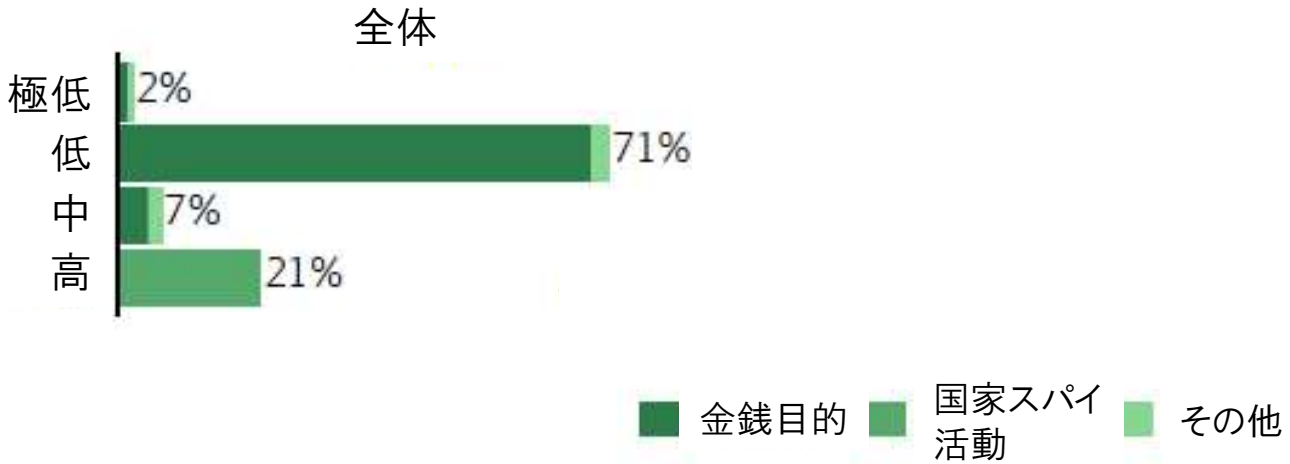


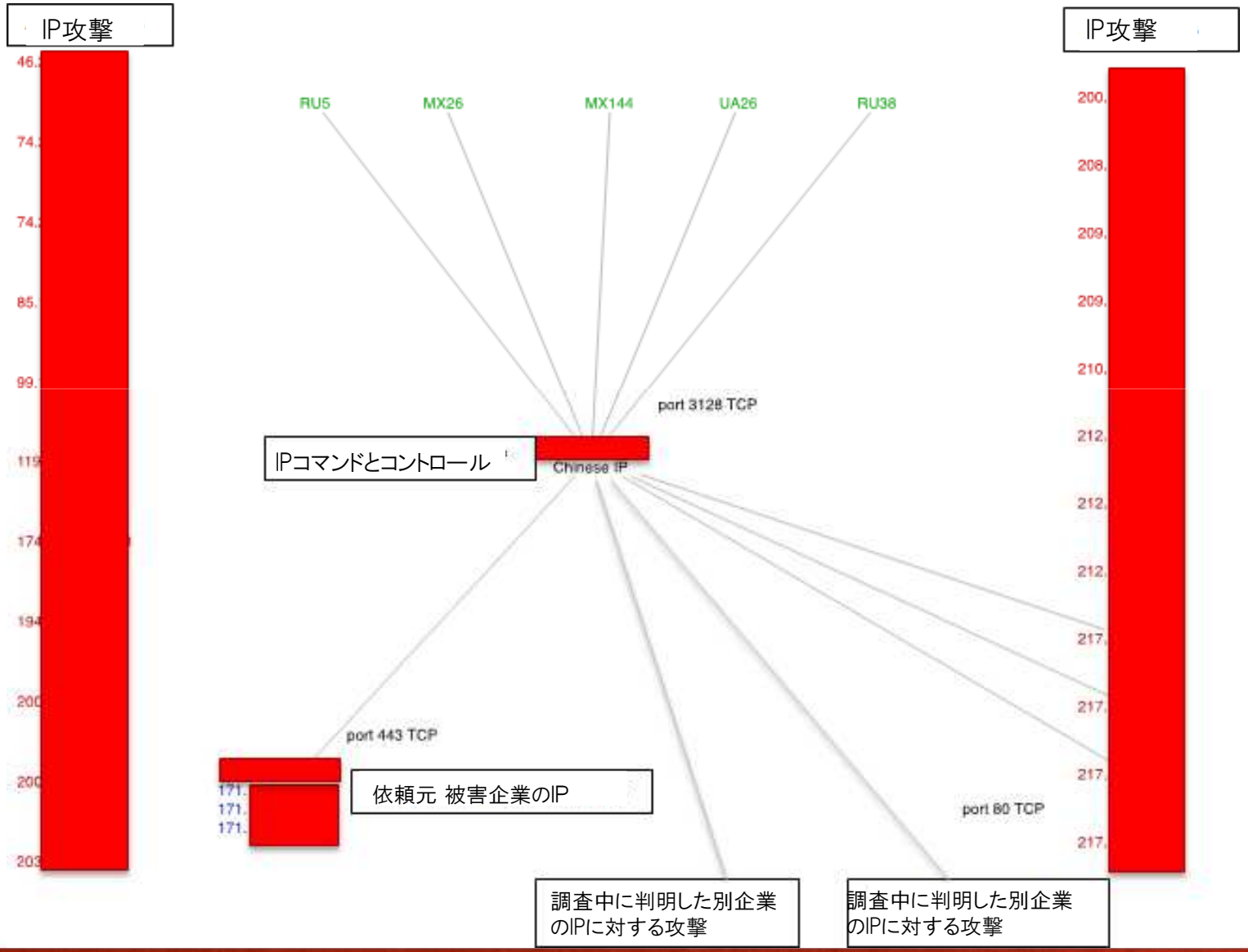
図40：後続の攻撃の難しさ



事例- DDoS / データ漏洩

米系被害企業のUDP トラフィック

事例- DDoS / データ漏洩

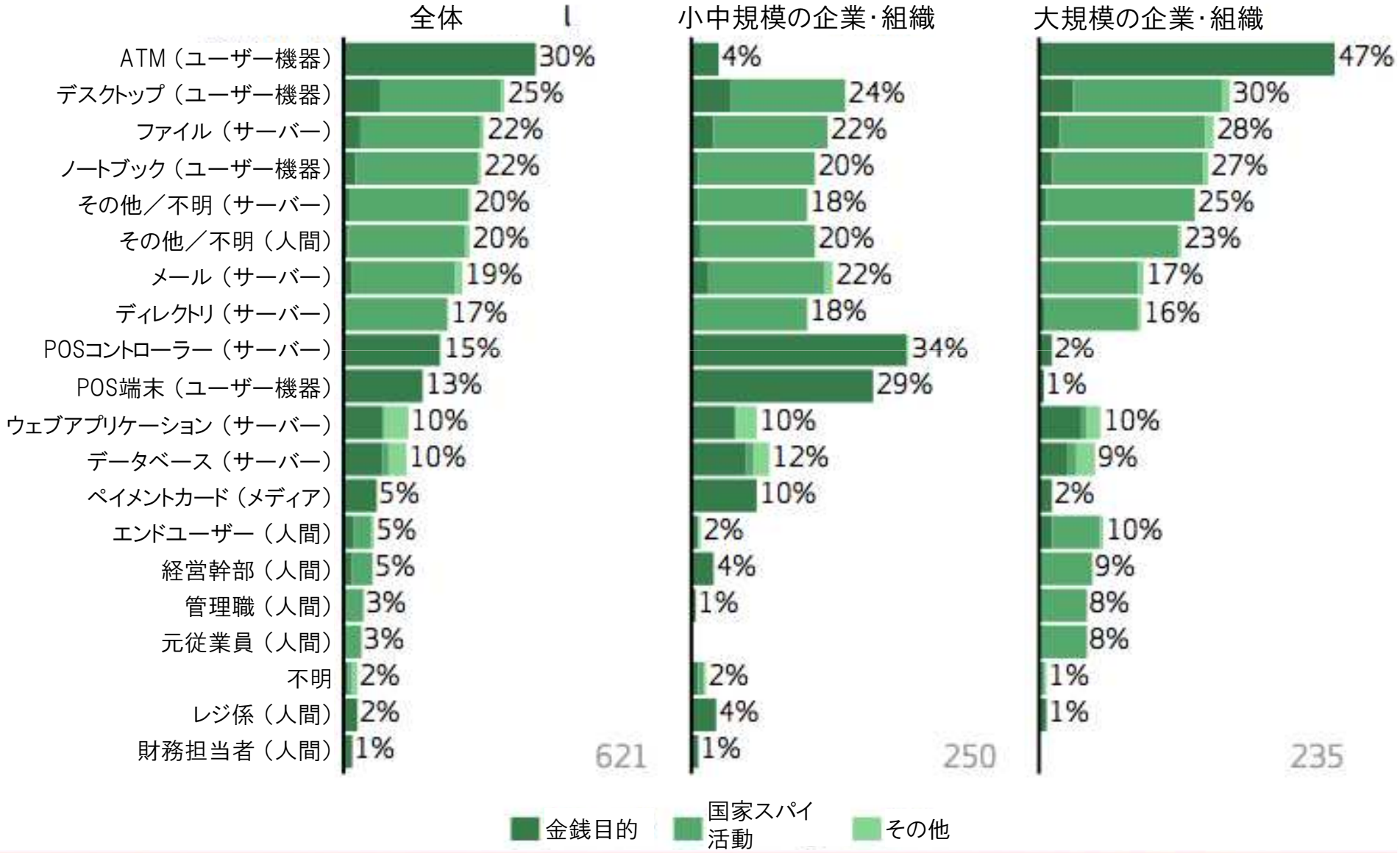


事例- DDoS / データ漏洩

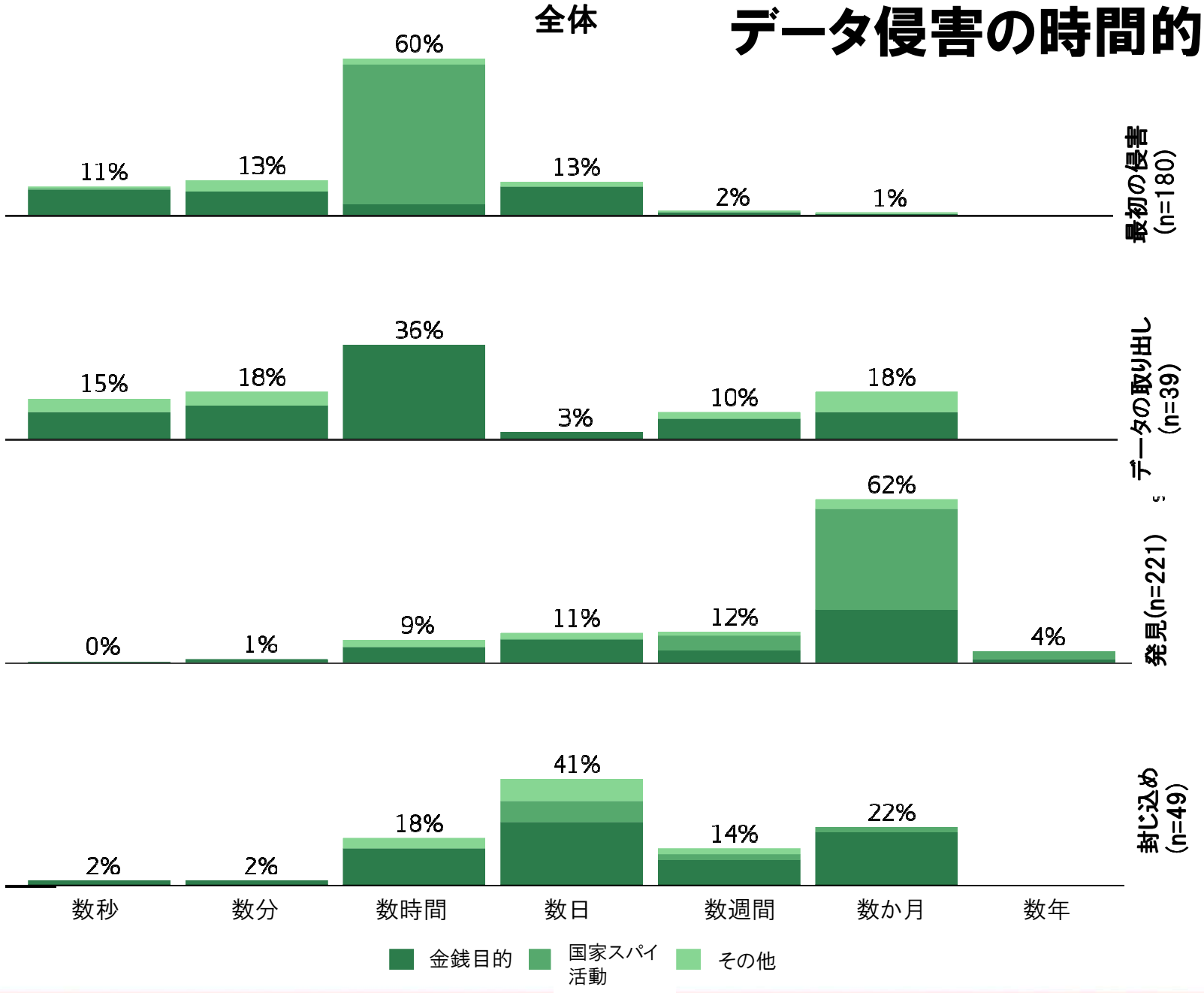
米系被害企業のUDP トラフィック

図33：侵害された情報資産のタイプ

侵害された情報資産のタイプ

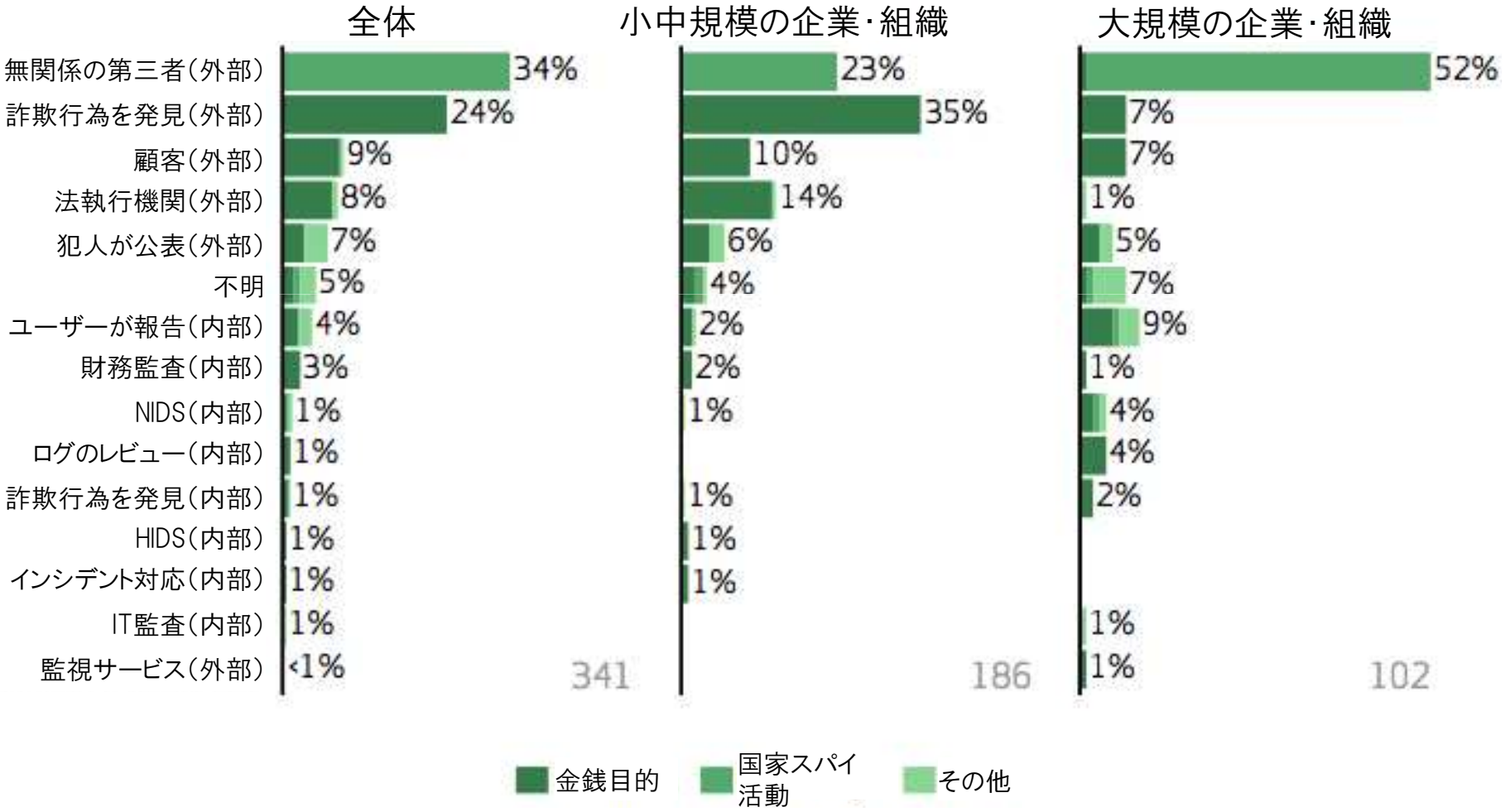


データ侵害の時間的段階



データ侵害の発見方法

図44: データ侵害の発見方法



推奨事項

- **全社的に**セキュリティに取り組む。従業員は**最大の資産**にも、時には最大の弱点にもなりうる
- 人、プロセス、テクノロジの連携を通じて、より良く、より速い**検知**手段を確立
- **攻撃者の執念**を甘く見てはならない
- 貴社独自の脅威の様態を評価し、**サイバー対策の優先付け**を行う
- **「2013年度データ侵害／漏洩調査報告書」をダウンロードして**、社内・取引先への情報共有を行い、組織全体及び関係者の知識・意識向上を図る

VERIZONENTERPRISE.COM/DBIR/2013

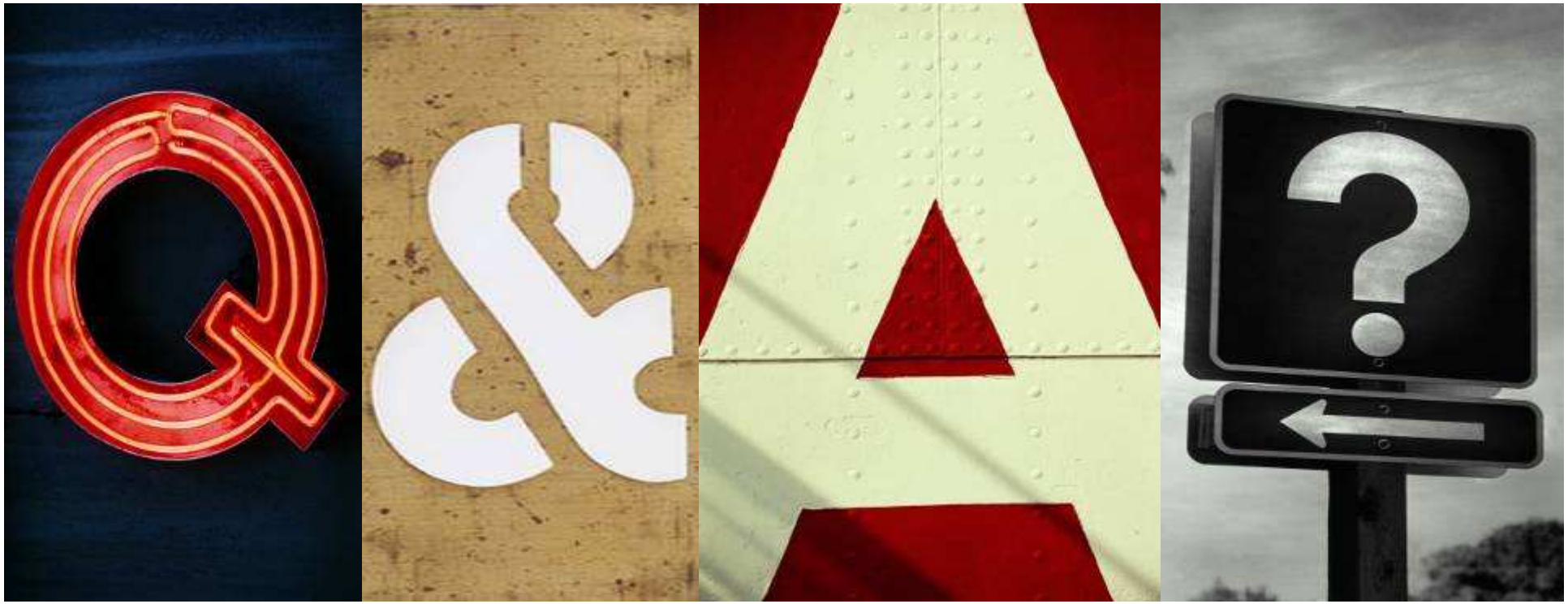
推奨事項

図46: CCAの20の重要セキュリティ対策とVERISの主要脅威アクションの対応関係

**. このバックドアには、バックドアとC2(マルウェア)、およびバックドアとC2の使用(ハッキング)の両方が含まれます。

質疑応答

「データ漏洩/侵害調査報告書」日本語完全版　ダウンロードはこちら
https://eentry11.securesites.net/verizon_security/contact01/index.html



お問い合わせ先：
ベライゾンジャパン合同会社
マーケティング部
Japan.marcom@jp.verizon.com