PCIDSS対応
～ グローバル事情から見た日本企業への示唆

ベライゾンジャパン合同会社
プロフェッショナルサービス
土屋 喜嗣（Yoshitsugu TSUCHIYA）

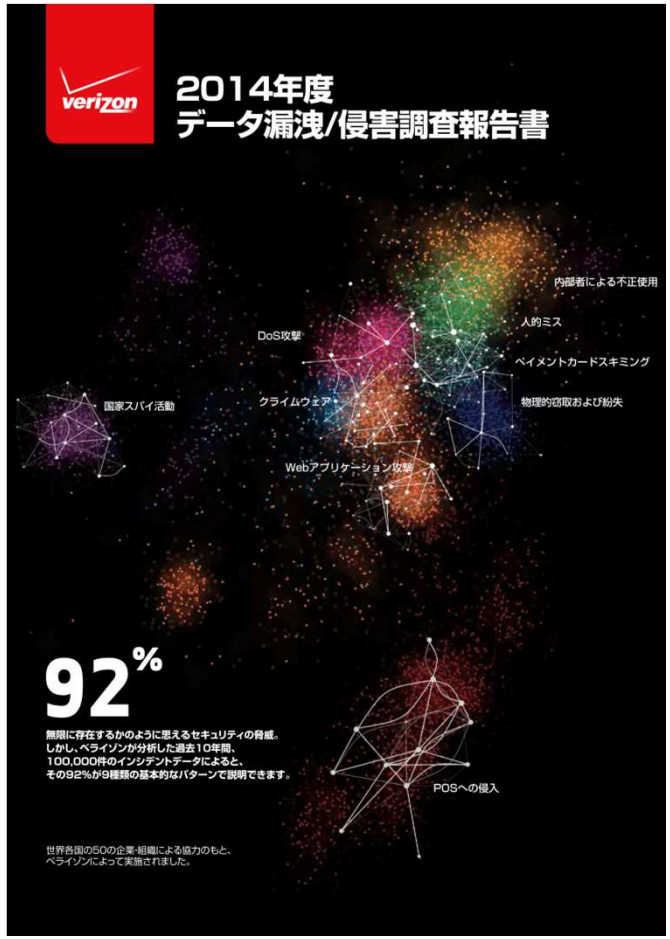
2014年7月29日

本プレゼンテーションの構成

1. グローバルでのPCIDSS対応の状況
2. PCIDSSに関連したデータ侵害・漏洩事案の動向
3. 適切なセキュリティ・リスク管理につながるPCIDSS対応
   - POS等の脆弱性対応
   - 定期的なテスト（脆弱性、システム強度）の重要性
   - モニタリング・ログ管理
4. まとめ：各企業で必要となる対策とは

ベライゾンの情報セキュリティ関連調査報告書

verizonenterprise.com/jp/pcireport/2014



verizonenterprise.com/jp/DBIR/2014

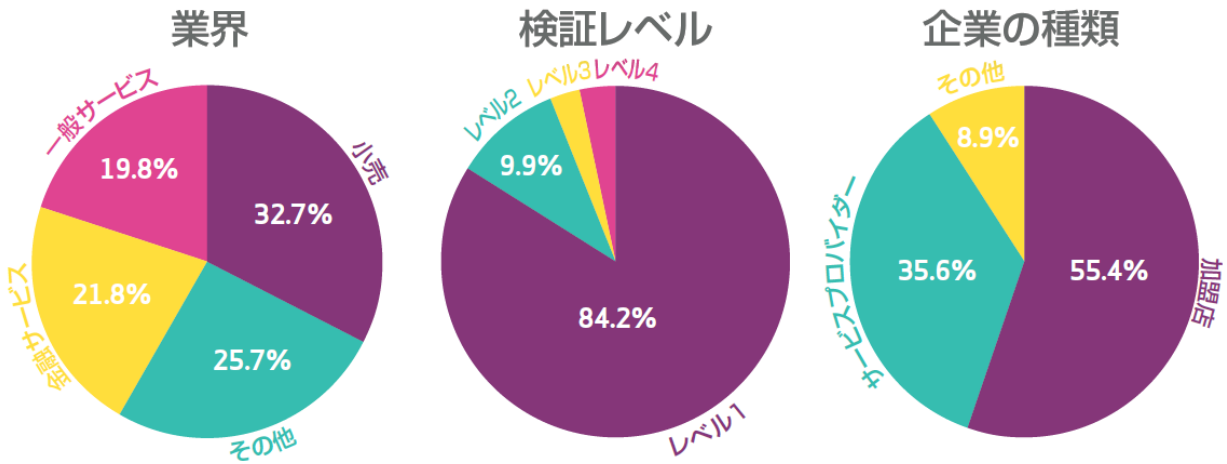
PCIDSS準拠調査：調査方法及び対象

調査方法

- QSAとしてのベライゾンがPCIDSS準拠のベースライン評価で収集したデータに基づく
- 対象年：2011年～2013年
- PCIDSS2.0 （※PCIDSS 3.0を用いた評価は2014年から）

調査対象

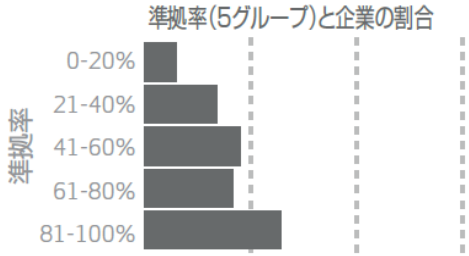
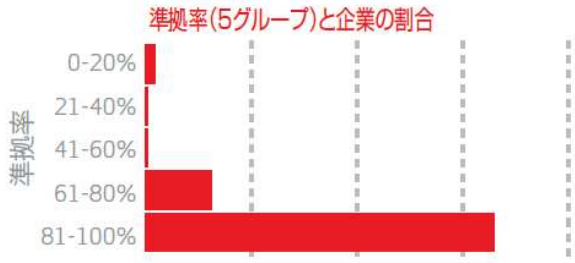
- 調査対象となっている数値データは、2009年以来ベライゾンが評価・審査を行った対象企業500以上（評価案件4,000件以上）をベースとする
- 調査対象企業のプロフィール：



※「ベライゾン2014年ペイメントカード業界コンプライアンス調査報告書」より

企業種別ごとのPCIDSS準拠率（1）

ベライゾン調査対象企業のPCIDSS準拠率（企業割合及びコントロールの割合）は上昇した：

比較項目	準拠している企業／準拠したコントロールの割合 【2012年】	【2013年】
企業が準拠していたコントロールの割合	52.9%	85.2%（+32.3pt）
完全準拠（100%）の企業の割合	7.5%	11.1%（ +3.4pt）
ほぼ準拠（81%～）の企業の割合	24.6%	71.1%（+46.5pt）
準拠率に基づく企業の分布		

※「ベライゾン2014年ペイメントカード業界コンプライアンス調査報告書」より

企業種別ごとのPCIDSS準拠率（2）

ベライゾン調査対象企業のPCIDSS準拠企業の割合（2011～2013年）：

業種別

項目	PCIDSS準拠企業の比率（80%以上準拠）
小売業	69.7%
一般サービス企業	35.0%

地域別

項目	PCIDSS準拠企業の比率（80%以上準拠）
アジア・太平洋地域	75.0%
北米地域	56.2%
欧州地域	31.3%

※「ベライゾン2014年ペイメントカード業界コンプライアンス調査報告書」より

PCIDSS各要件(1～12)毎の準拠率

PCIDSS要件（1～12）毎の平均準拠率[2012年/2013年]

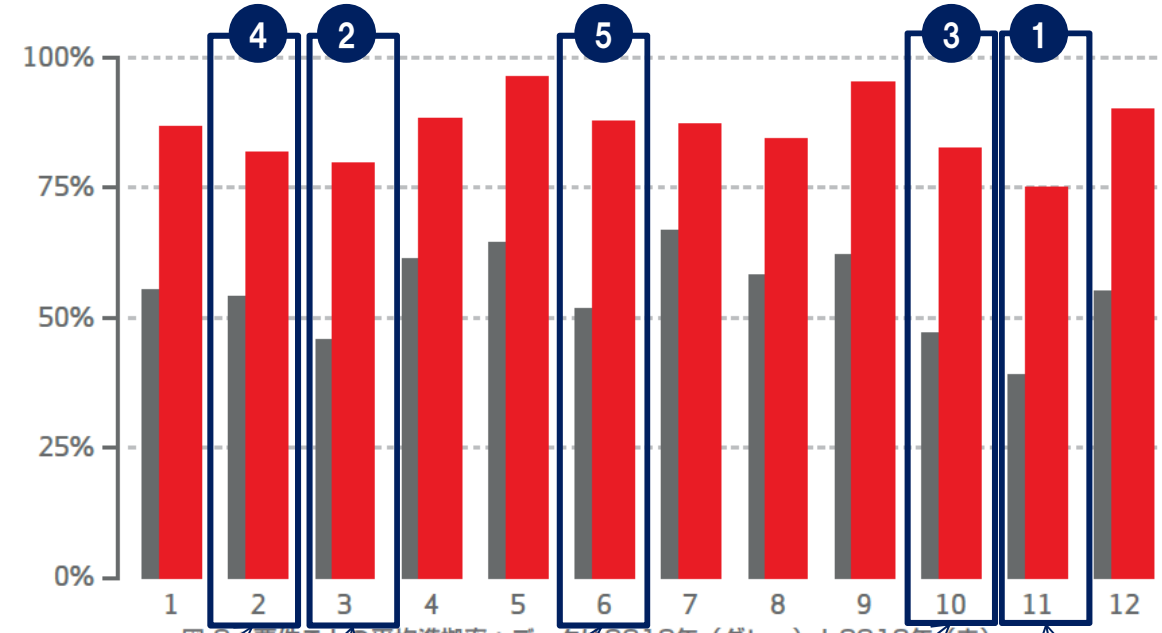


図 8 / 要件ごとの平均準拠率：データは2012年（グレー）と2013年（赤）

【準拠率下位20入り】
・2.2.2a
・2.2.2b

【準拠率下位20入り】
・---

【準拠率下位20入り】
・6.1a

【準拠率下位20入り】
・10.4.1a
・10.4.2a

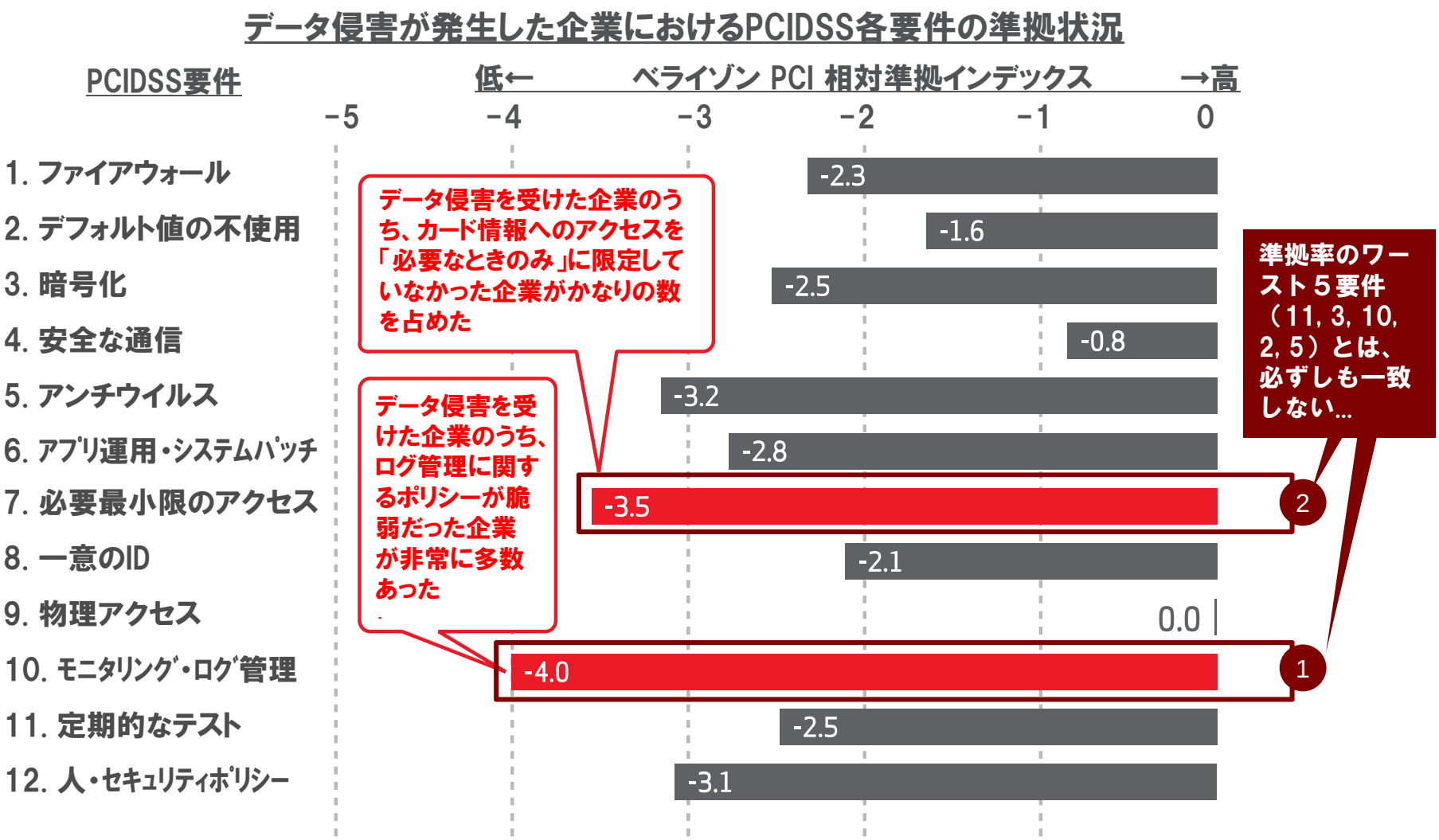
【準拠率下位20入り】
・11.3.a～b
・11.2.3.a～b
・11.2.1.a～b
・11.3.1～11.3.2
・11.2.1.c
・11.3.c

準拠率から見える状況

- 対象企業において、2013年のPCIDSS準拠率は、全要件において前年度よりも上昇
- 2013年の準拠率が依然として低い要件は下記：
  - 要件11： 定期的なテスト
  - 要件3： 暗号化
  - 要件10：モニタリング・ログ管理
  - 要件2： デフォルト値の不使用
  - 要件5： アンチウイルス
- 上記５要件中、中でも要件11においては、準拠率ワースト20位以内のサブコントロール項目を多く出している

※「ベライゾン2014年ペイメントカード業界コンプライアンス調査報告書」より
-.平均準拠率：PCIDSS各要件のサブコントロールの特定の集合に準拠した企業の割合
-.準拠率下位20： 2011年から2013年までの全データに基づく

データ漏洩/侵害を実際に経験した企業・組織とPCIDSS準拠率

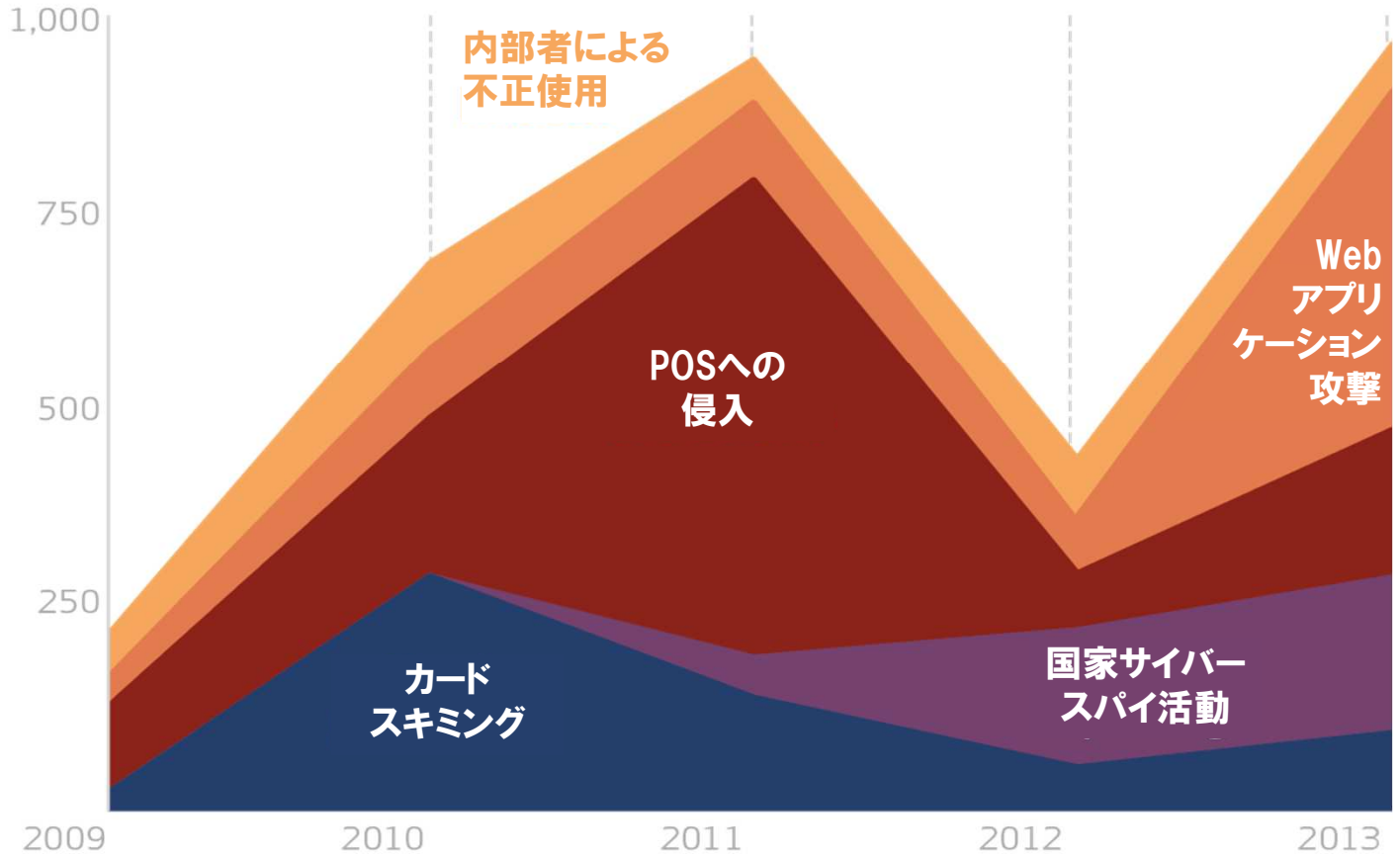


※ベライゾン「2014年度データ漏洩/侵害調査報告書」より

PCIDSSに関連したデータ侵害・漏洩事案の動向

データ侵害/漏洩におけるパターンの推移

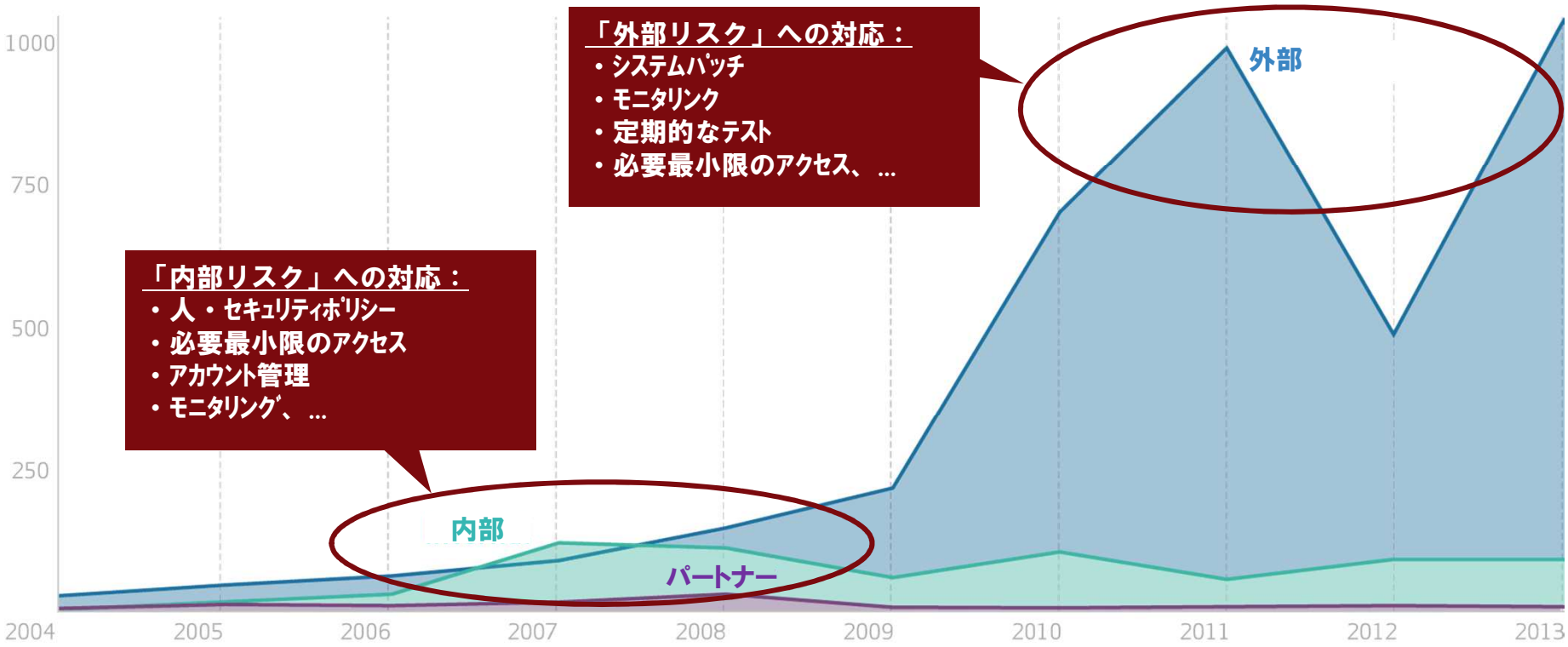
主なインシデント分類パターンの件数と推移



※ベライゾン「2014年度データ漏洩/侵害調査報告書」より

脅威の発生元の推移

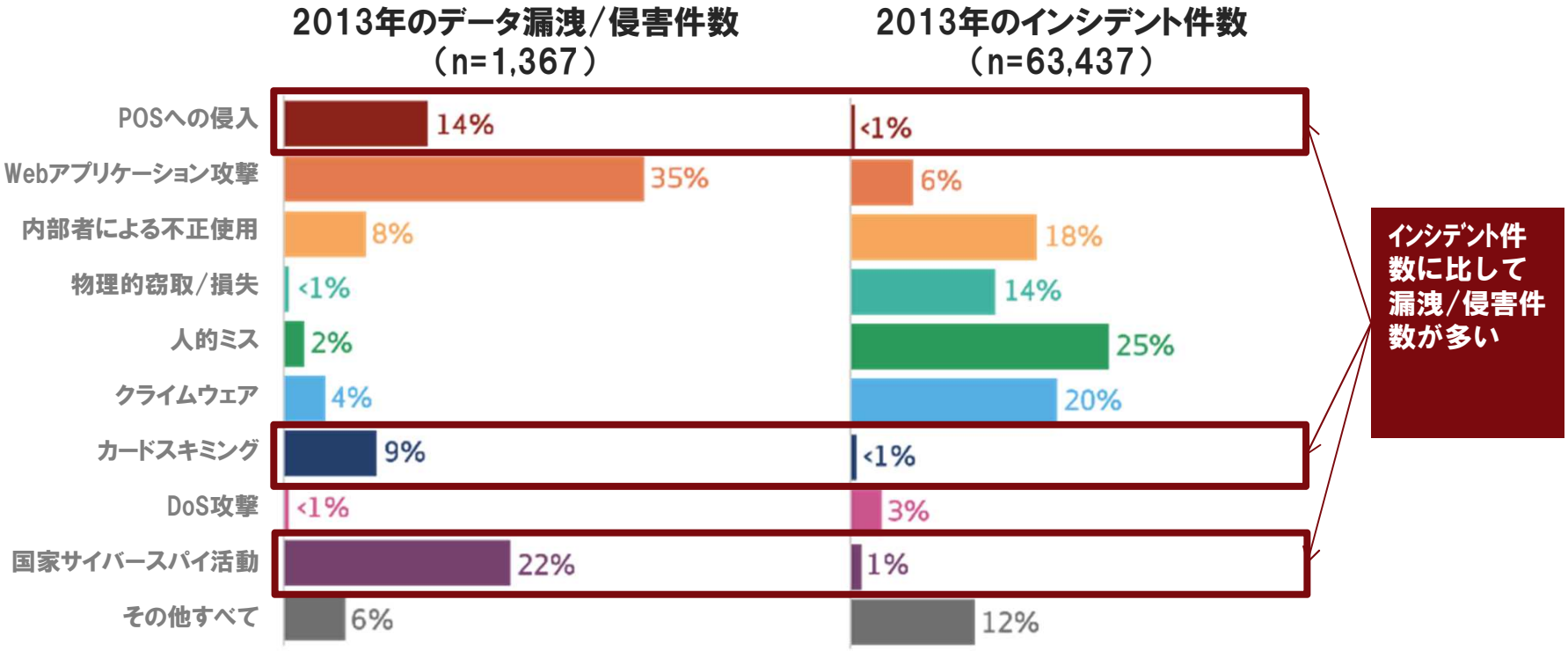
脅威実行者別のデータ漏洩/侵害事案の件数と推移



※ベライゾン「2014年度データ漏洩/侵害調査報告書」より

漏洩・侵害パターンの発生頻度

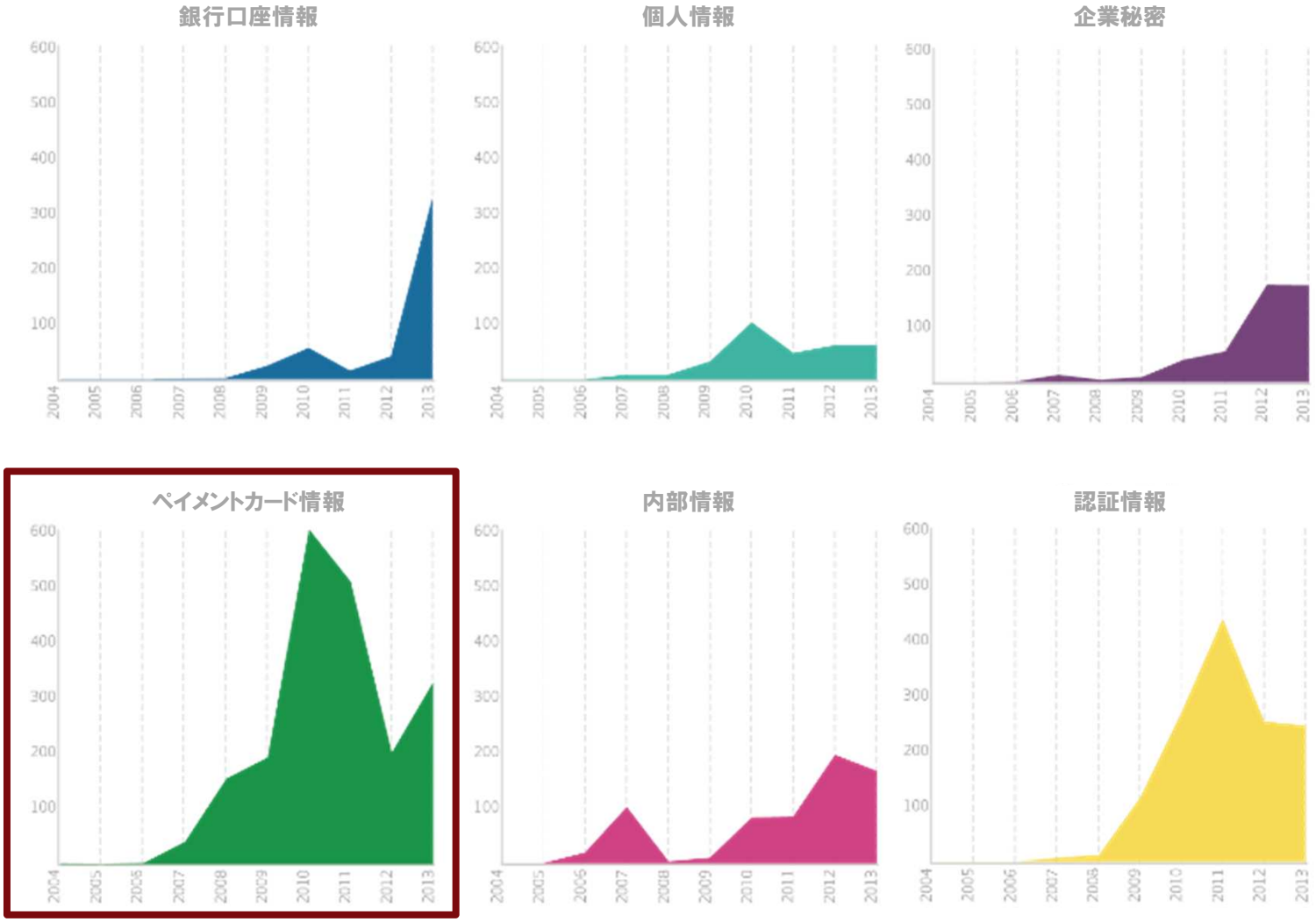
POSへの侵入、カードスキミングの各事案は、インシデント件数としては少ないが漏洩/侵害事案の件数が多い



※ベライゾン「2014年度データ漏洩/侵害調査報告書」より

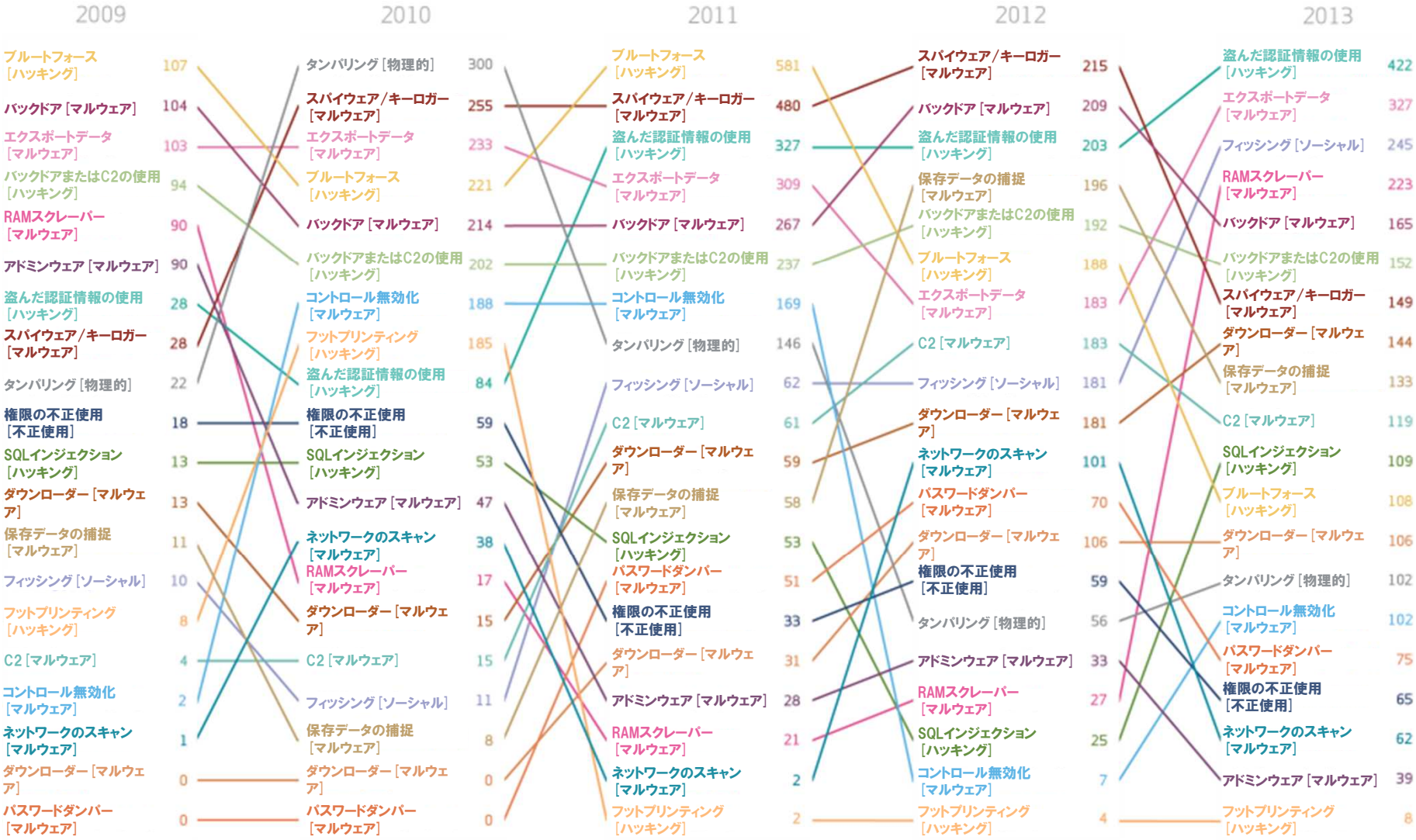
漏洩・侵害の対象となったデータタイプ

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



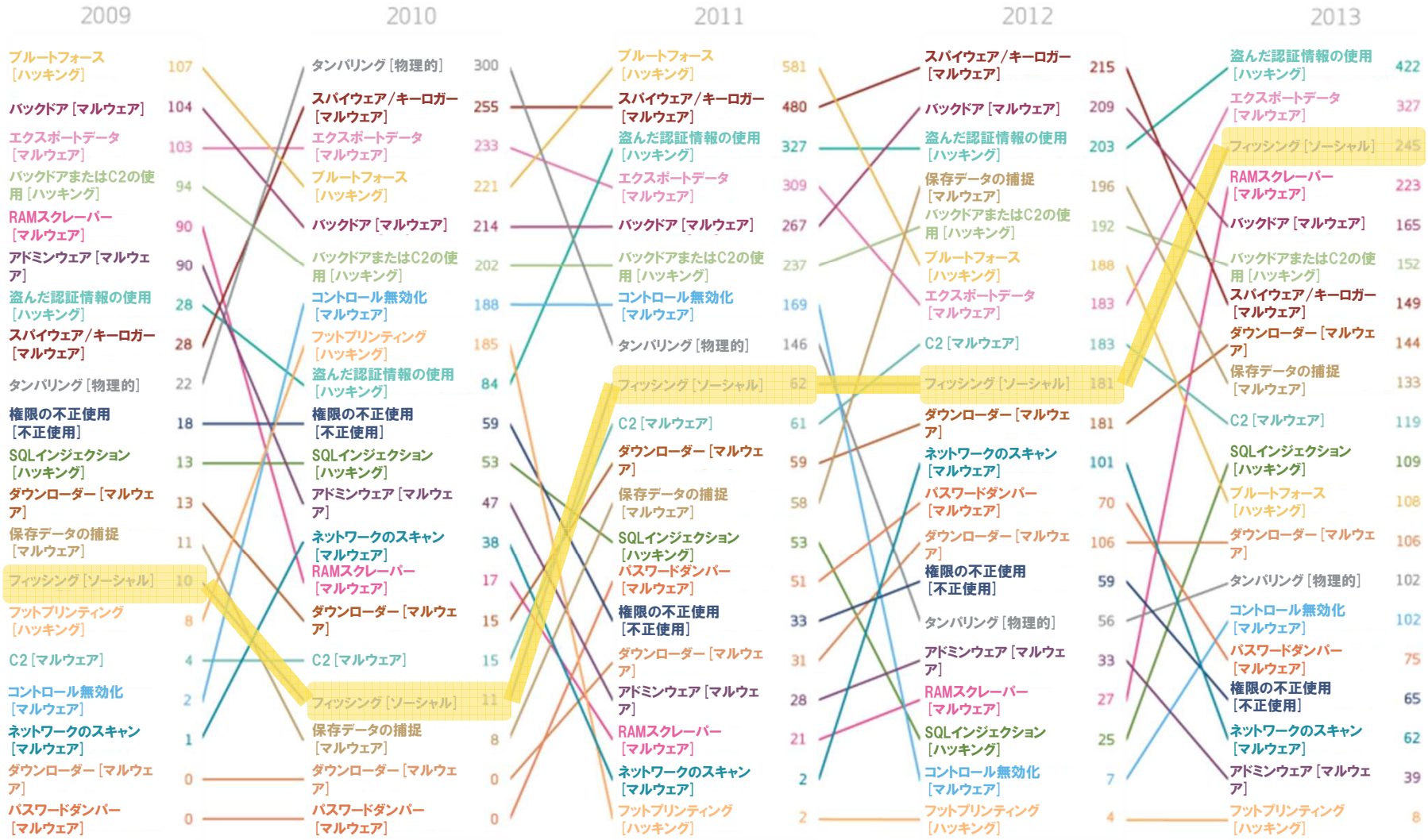
過去5年間の脅威アクションの推移：

脅威アクション上位20位の推移

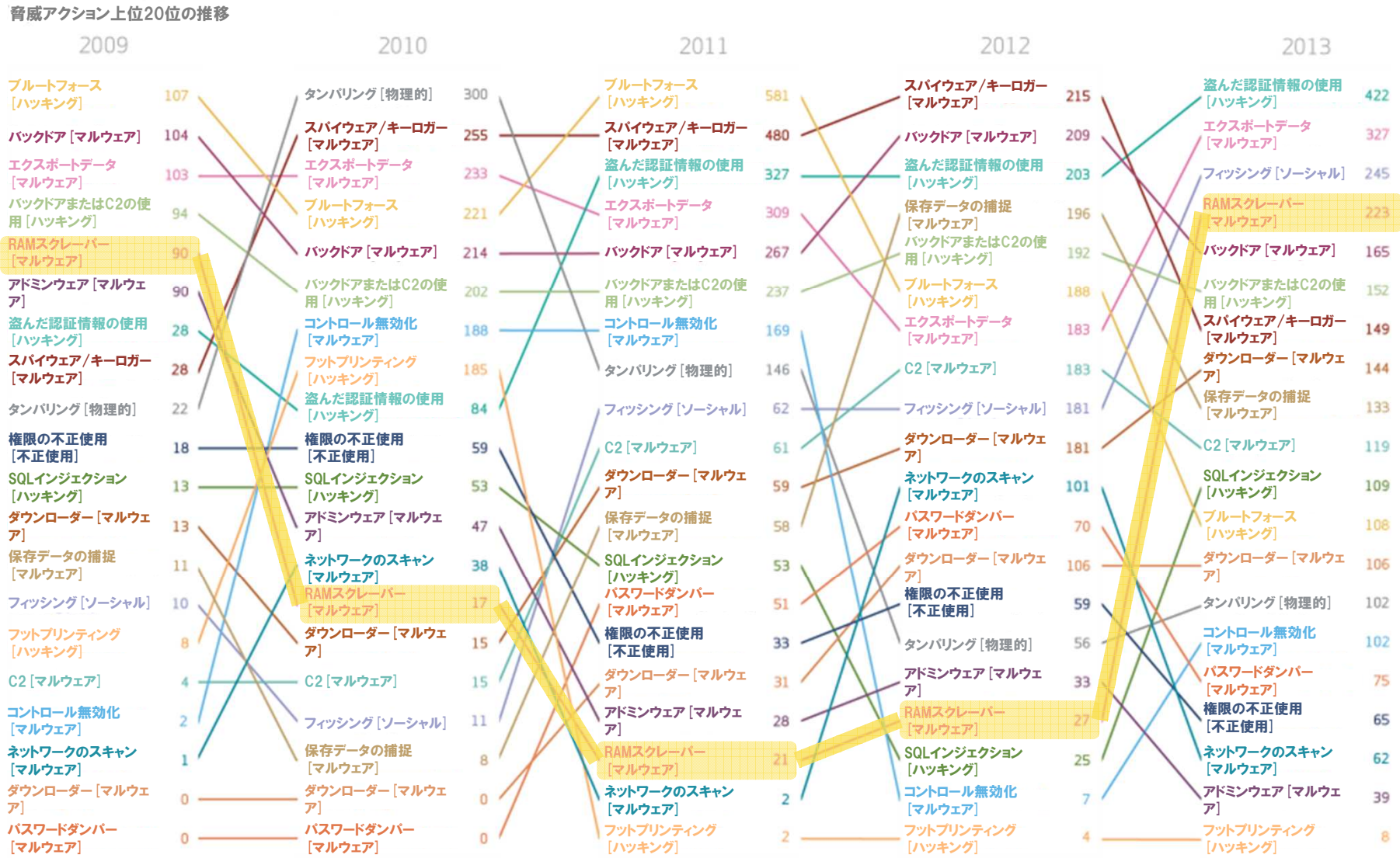


過去5年間の脅威アクションの推移：フィッシング

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



適切なセキュリティ・リスク管理につながるPCIDSS対応

POS等の機器の脆弱性への対応

RAMスクレーパー等の事案が示すPOS機器に関連する漏洩・侵害事案と教訓：

識別された主な侵害・漏洩の方法

- 典型的な手口：POSシステムの脆弱性を突き、マルウェア等を使ってシステム内で暗号化されているがメモリ上では展開されているカード会員情報を読み出す手口が多く識別された
- 識別された主な侵入経路：
  - POS端末自体（OS、通信処理等）の脆弱性
  - 通信方法（Remote Desktop Protocol等）の脆弱性
  - 通信アクセス手段（WiFi等）の脆弱性
  - POS用メンテナンス業者用PCの脆弱性を突いた侵入→その後POSに侵入
  - 管理ｻｰﾊﾞにおけるクレデンシャルの盗難、…

PCIDSS準拠に際して留意すべき対応指針例

- 組み込み機器を想定したPOSシステム（＝多くの場合、機器導入後の定期的な脆弱性への対応がされていない）について、定期的な脆弱性のチェックをプロセス化する
- システム監視の対象として上記POSシステムが対象となるよう運用プロセスを改善
- 漏洩/侵害の発生状況に鑑み、特に認証・アクセス管理についてはクレデンシャルの盗難等を想定した多要素認証等を考慮する

【参考】脆弱性と攻撃難易度

初回攻撃及び後続攻撃の「むずかしさ」

図 39：最初の攻撃の難しさ

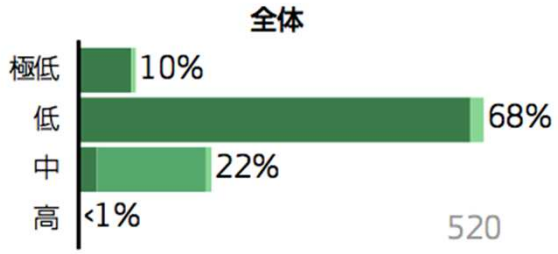
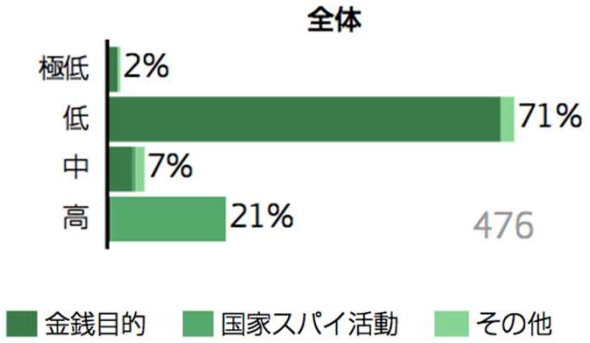


図 40：後続の攻撃の難しさ



攻撃難易度からの示唆

- 実際の漏洩事例においては、難しい手法の駆使は圧倒的に少ない。
  - 金銭目的の攻撃である場合、難易度は殆どが「極低」から「低」
  - スパイ活動では、後続攻撃にやや多くの難易度「高」攻撃が使われる

⇒ 防御にあたっては、まずは**意識せずに開けていたドア（脆弱性）を無くす**ことが肝要

攻撃の手口をつぶすための対策（例）

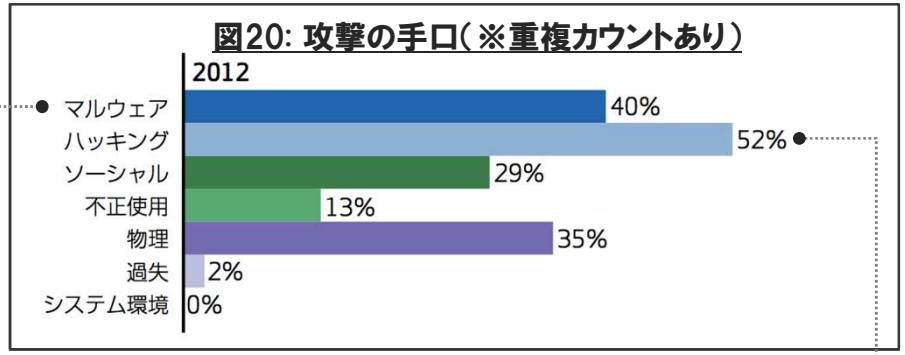
- システム基準・手順の策定
- 重要情報の所在識別と管理
- 情報に対する適切なアクセス・コントロール
- アプリ・インフラの脆弱性チェック
- パッチ適用・ウイルス対策の最新化
- 不要I/Fの閉塞／ネットワーク分離
- ⋮

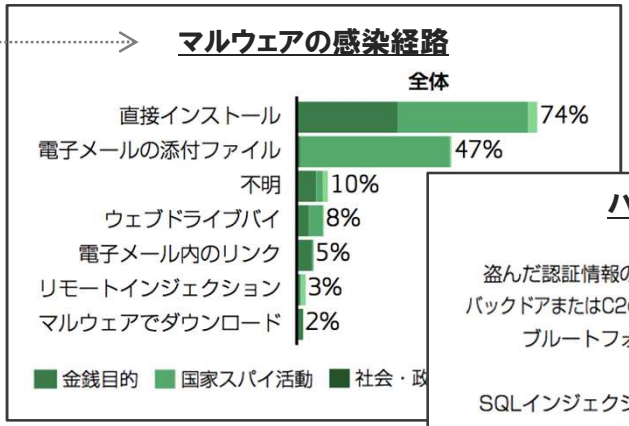
※上記で捉えきれない事象をモニタする

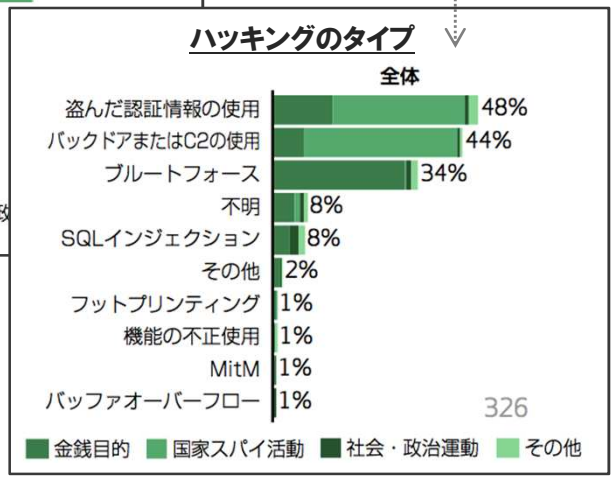
※ベライゾン「2013年度データ漏洩/侵害調査報告書」より

システム監視の側面
～ 攻撃手口・手法のタイプに見る監視方法

攻撃の手口／手法の種別







傾向と対策

- 攻撃の手口はいくつかにわかれ、大多数を占める手口は無い
- 毎年、基本はマルウェア、ハッキング、物理が主流であるが、年によってはソーシャルも1～3割を占める
- 目的別に多く見られた手口・経路の組合せとして下記が識別される：

i.共通して見られる手口

- 直接インストールによるマルウェア
- 盗んだ認証情報によるハッキング

ii.「金銭目的」で多く見られる手口

- ブルートフォースによるハッキング

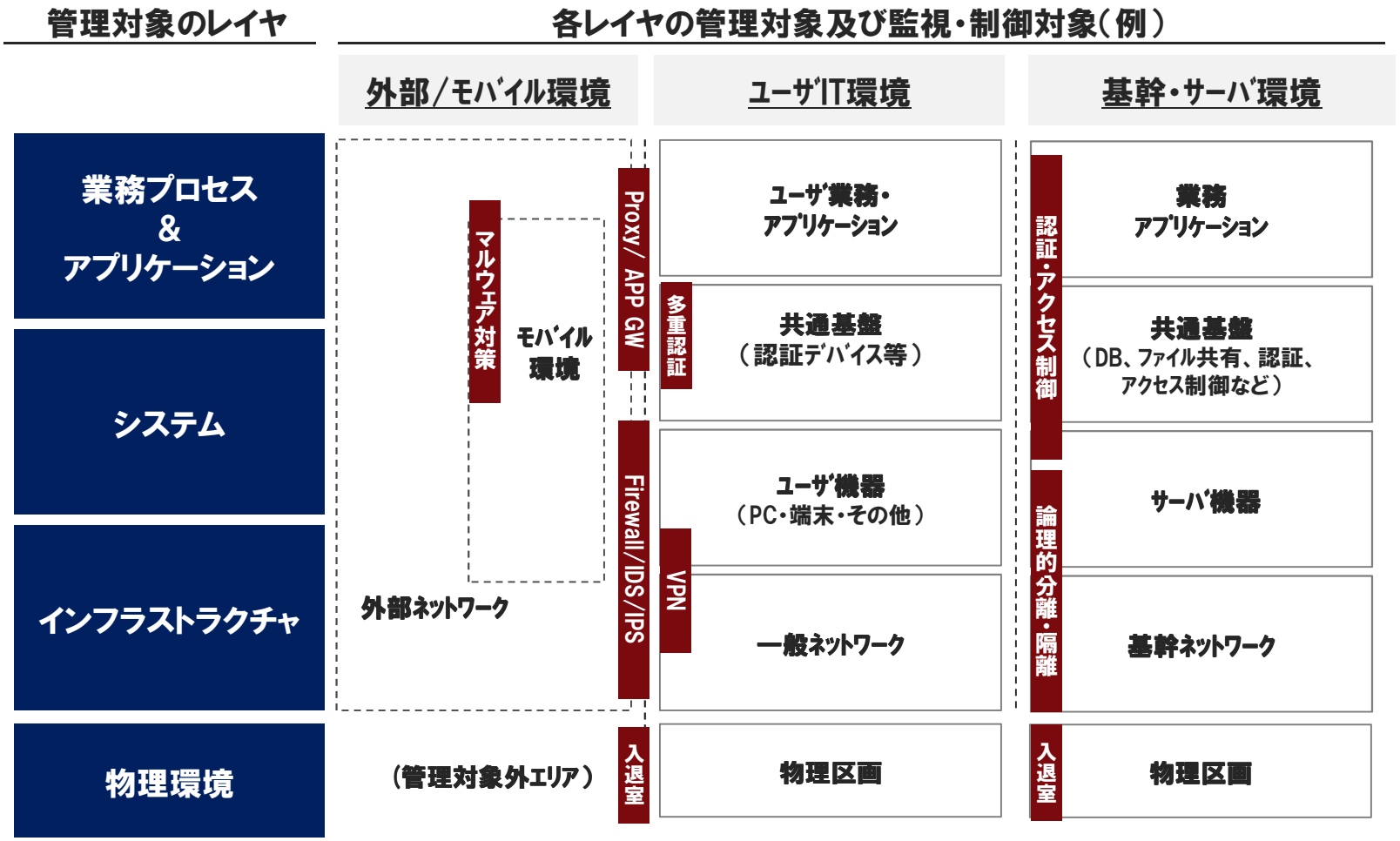
iii.「スパイ活動」で多く見られる手口

- 電子メールの添付ファイルによるマルウェア
- バックドアによるハッキング

※ベライゾン「2013年度データ漏洩/侵害調査報告書」より

セキュリティモニタリング
～ 情報システムの各領域とセキュリティ対策

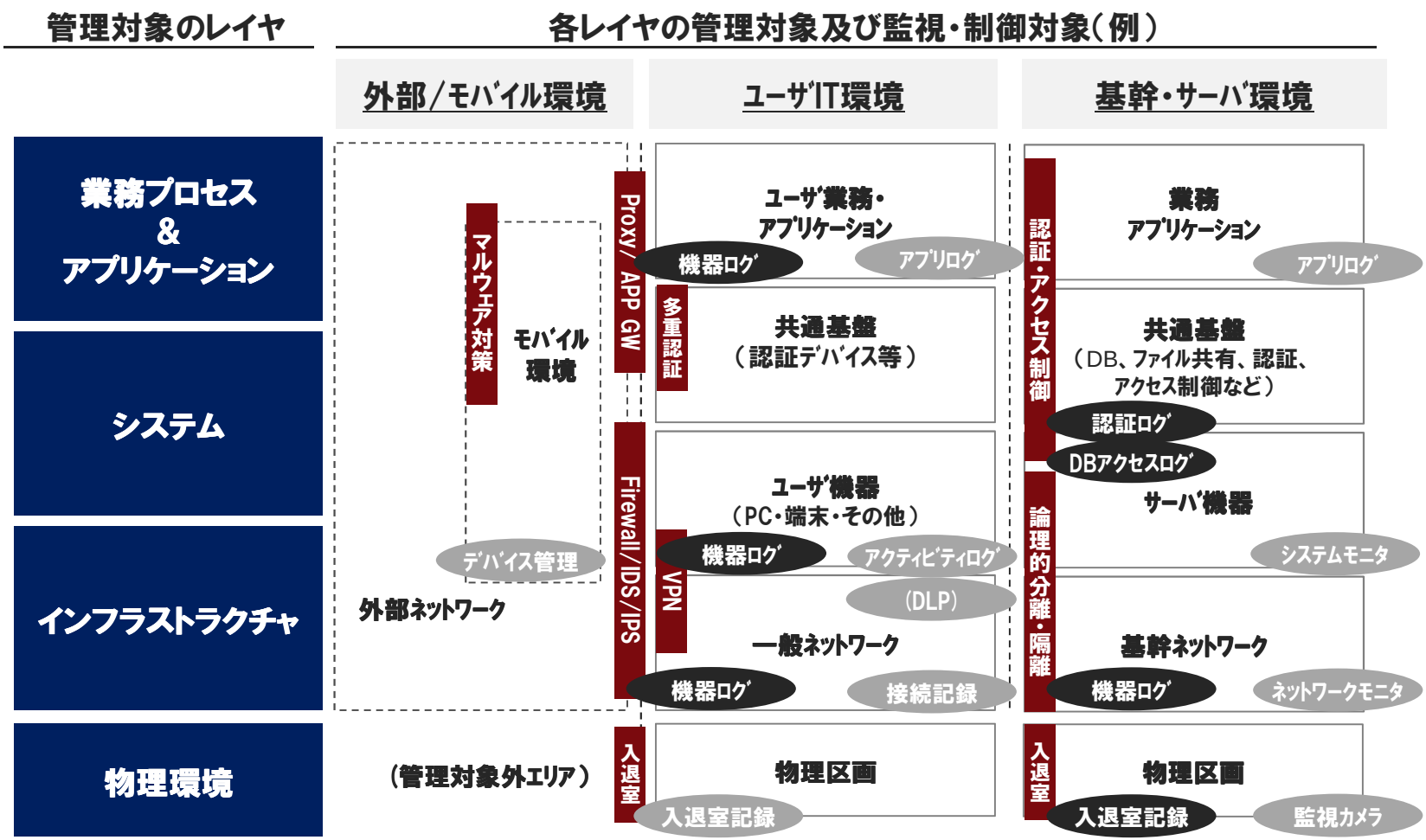
侵入を前提として早期発見・封じ込めが可能なモニタリングの検討が必要



■ ...監視・制御手段

セキュリティモニタリング
～ 現状において得られているモニタ対象情報

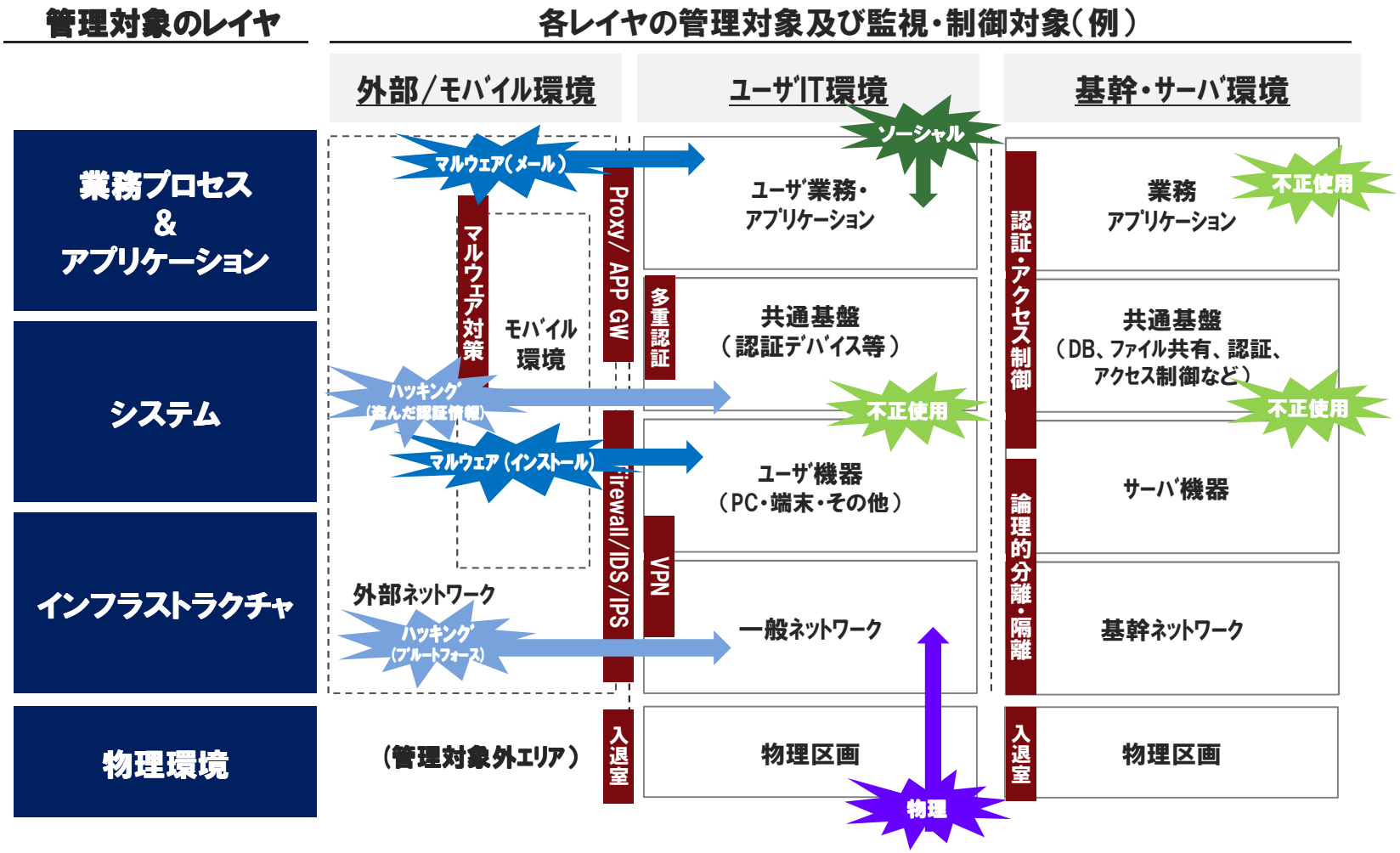
侵入を前提として早期発見・封じ込めが可能なモニタリングの検討が必要



…監視・制御手段　…証跡（多くの企業で取得可・実施済み）　…証跡（未実施が多い）

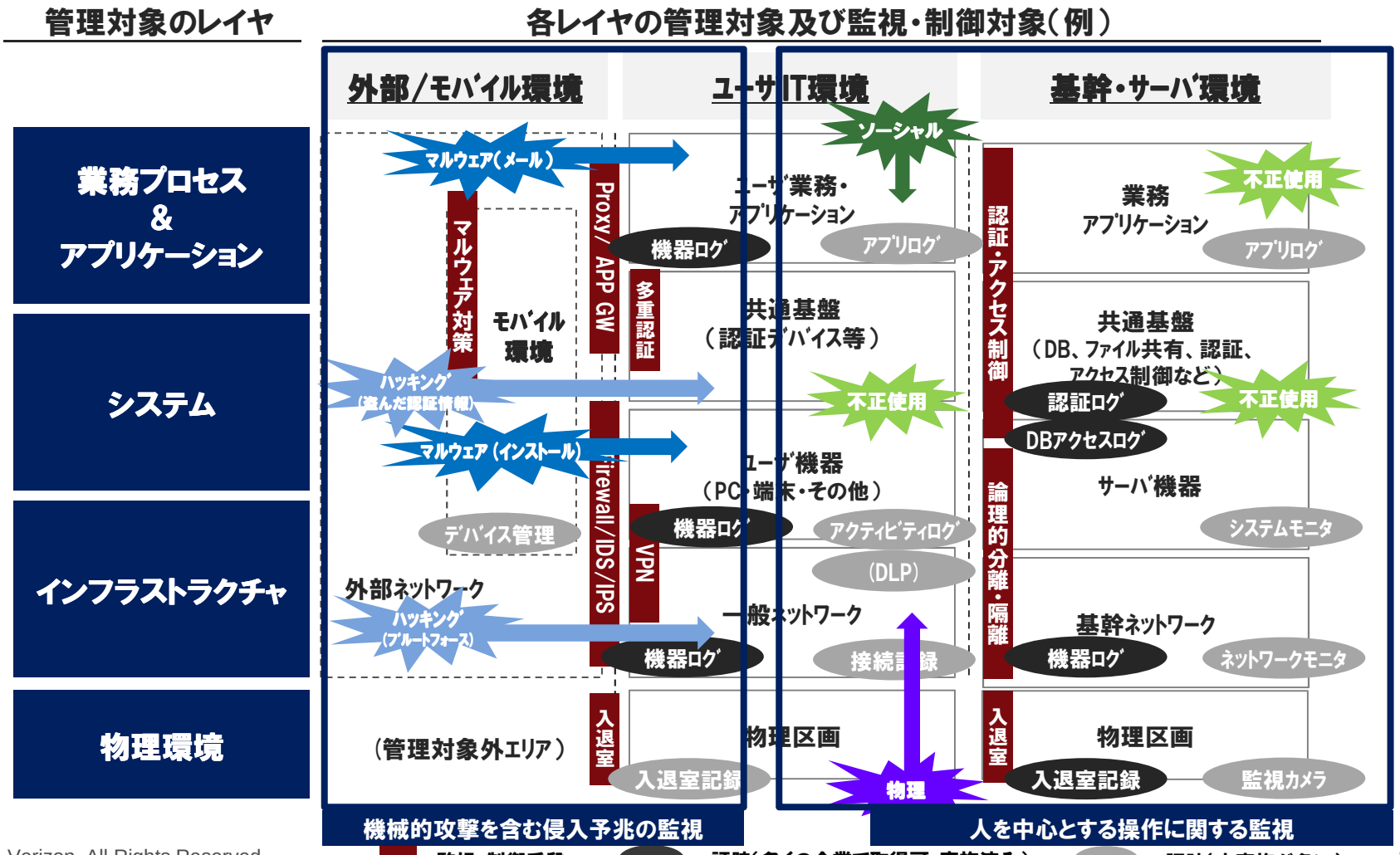
セキュリティモニタリング
～ 識別される手口と経路

現状システム構成・セキュリティ対策に対して、想定される手口・経路をマップし、必要な監視事項を識別



セキュリティモニタリング
～ 必要な対策箇所、モニタリングのポイント

対象とする侵入・漏洩事象毎に監視の対象となる行為も異なり、それぞれに監視手法・体制の検討が必要



ベライゾンとPCIDSS認証取得

ベライゾンでは、3種類のPCIセキュリティ関連サービスを提供しています。

1. PCIDSSアセスメント
   - 対象範囲の特定とギャップ分析
   - 改善策の策定
2. 改善策の実行
3. PCIDSS審査
   - ベライゾンのQSAが審査を実施

PCI DSS 準拠を達成するために必要なギャップ分析～改善策実施～審査 までの
トータル・コンサルティング・サービスをグローバルにご提供します

国内		海外	
実店舗	Web	実店舗	Web

PCIDSS取得推進体制(例)

PCIDSS取得成功だけでなく、リスク回避のための運用体制確立のための体制例:

PCIDSS対応に必要な役割		役割の概要	取組み視点		アドバイザリのレベル	
			PCIDSS範囲全体	個別システム視点	要件のレベル	対策・実行案のレベル
PCIDSS取得企業	セキュリティ／PCIDSS取りまとめ担当(プロセス・規程等)	■ 社内規程類・プロセスの整備を担う ■ プロセス・規程に関わるPCIDSS観点からの指摘に対して、社内調整を行い、必要な修正施策の実施を管理する	■		■	
	セキュリティ／PCIDSS取りまとめ担当(情報システム)	■ PCIDSS審査対象について情報システム側の対応を担う ■ PCIDSS観点からの情報システムの修正等に関わる指摘に対して、社内調整を行い、修正施策の実施を管理する	■		■	
	取得企業側ベンダー対応PM	■ 各ベンダーのPCIDSS対応のためのアクションを管理する ■ PCIDSS準拠の全体スケジュールに基づき、対象となる複数ベンダーのアクションを管理する		■	■	
ベンダー	ベンダー【例:システム毎】	■ PCIDSS指摘要件に対して、システム側の修正策の提示 ■ 合意された修正策の実行を担う ■ 各ベンダーの対応範囲は、担当するシステムの範囲内		■		■
PCIDSSコンサルタント	ITアドバイザリ	■ 立案されたPCIDSS対応策について、監査者の立場から施策の妥当性を検討し、適切なアドバイスを行う ※ 貴社の監査企業としての制約あり	■		■	
	PCIDSSコンサルタント	■ PCIDSS対象のシステム・プロセス全体視点での設計・導入支援を実施。お客様側のセキュリティ／PCIDSS取りまとめ担当の視点での支援を実施	■		■	■
	PCIDSS QSA	■ PCIDSS適合の審査者 ■ 設計・導入支援の過程においては、PCIDSSの規程への適合の視点からアドバイスを実施	■		■	

まとめ
～ 各企業で必要となる対策とは

1. PCIDSS準拠の動向
   - PCIDSS各要件への準拠率と、実際に漏洩・侵害が起こった企業における未準拠項目とのｷﾞｬｯﾌﾟ:
     - アクセス管理
     - モニタリング/ログ管理

2. 情報漏洩事案の調査による示唆
   - 近年の動向:外部からの脅威の増加、POSやカードシステムへの侵害事例の増加

3. 必要な対策は
   - 侵入/ｸﾚﾃﾞﾝｼｬﾙ盗難等を前提としたシステム作りを
   - それぞれの監視目的・監視対象により取りうる手段が異なる
     - 人を中心とする操作に関する監視
     - 機械的攻撃を含む侵入予兆の監視
   - PCIDSS取得のための体制づくり