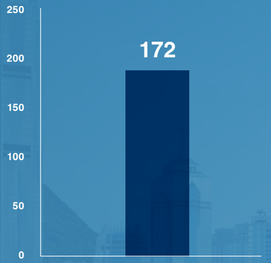
MANDIANT
A FireEye® Company

M-TRENDS® 2017

セキュリティ最前線からの視点

セキュリティ侵害の発生から検知までに要した日数（APAC）



依然としてAPACは、セキュリティ侵害の発生から検知までに要した日数が最も長くなっています。その理由としては、基本的にセキュリティ投資が少ないという点が挙げられます。

APACで特に攻撃グループに狙われやすい業種

業種	標的
建設 / エンジニアリング	• 先端材料 • 化学工学 • 産業機器 • 船舶工学 • 石油、ガス、原子力工学
金融	• 認証情報 • クレジット・カード情報 • 個人を特定可能な情報（PII） • 取引情報
官公庁	• 同盟 • 外交 • 外交政策 • 領有権問題
ハイテク / 電子	• 先進エレクトロニクス • クラウドおよびITサービス・プロバイダー • 演算装置および各種ハードウェア、半導体 • ソフトウェアおよびゲーム

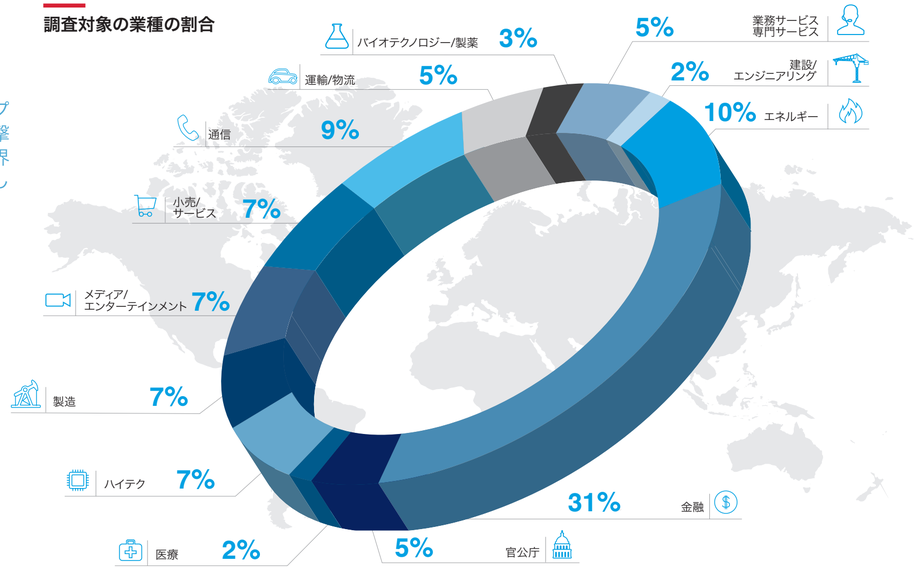
基本的なセキュリティ対策の導入

1 重要資産の把握	2 ネットワークおよびエンドポイントの可視化	3 ネットワークのセグメント化	4 アクセス管理
業務の維持に欠かせない内部システムやデータ・フローを把握する	ネットワークの境界線はあいまいになる一方であり、ネットワークやモバイル・エンドポイントに加え、ベンダーや子会社など相互接続されたすべての環境を監視する必要性が高くなっている	ネットワークのセグメント化は、見過ごされがちだが重要な対策。セグメント化が不十分な場合、ネットワークに侵入した攻撃者にたやすく水平展開を許してしまう	複数ファクタ認証を導入するとともに、職務に応じたアクセス権を設定する。「最小権限の原則」の徹底により、アカウントを侵害された場合の不正アクセスの範囲を最小化できる

消えた境界線：

金融系攻撃グループと国家レベルの攻撃グループの間に、境界線はもはや存在しない”

調査対象の業種の割合



APACの攻撃トレンド

引き続き多発する金融機関への攻撃

金融サービス業界では2016年もセキュリティ侵害の見出しがメディアを独占

ATMに対する攻撃

2016年は、各種マルウェアを駆使したATMおよびATMネットワークに対する攻撃が著しく増加

国家レベルの攻撃グループによるPIIの窃取

国家レベルのAPT攻撃グループは、2016年も民間および官公庁の脆弱な情報システムに侵入し、PIIを収集

中国周辺のサイバー・スパイ活動

複数の通信事業者が、APACにおける国家レベルのサイバー・スパイ活動の継続的な標的に

グローバルでの攻撃トレンド

金銭を目的とするサイバー攻撃は高度化する一方

Eメールが主な標的に。攻撃者は創意工夫を凝らしてEメールへのアクセスを試みている

標的に合わせて攻撃内容を調整。金銭目的の攻撃者はフィッシング・メールの内容を工夫し、標的を「サポート」するために電話をかけている

詳細については、M-Trends 2017レポートをご覧ください。

レポート全文はこちら

詳細はこちら www.fireeye.jp/current-threats/annual-threat-report/mtrends

ファイア・アイ株式会社
〒101-0054 東京都千代田区神田錦町3-22 テラススクエア8階 | TEL：03－4577－4401 | japan@fireeye.com

FireEye