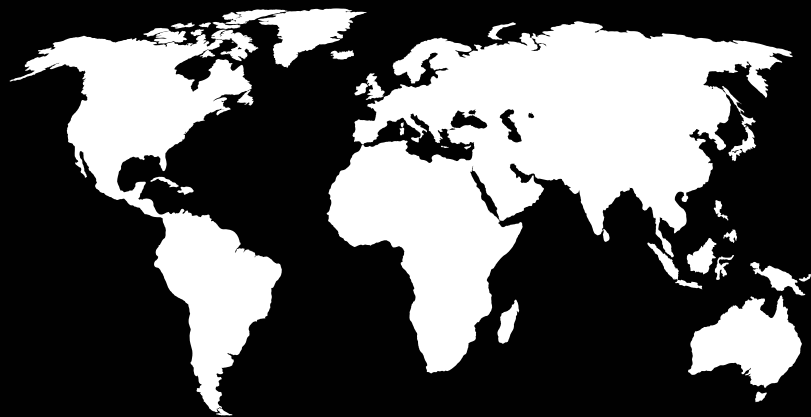


**Red Team Operations  
Attackers' Report 2021**

攻撃者が分析するRed Team Operations



## グローバルと日本のトレンド 2021



### Red Teaming 演習への SOCチームの関与が増加

ネットワークへの攻撃が長期間にわたって検出されず、特権的な情報にアクセスされてしまったというニュースが報じられました。企業にとってサイバーコントロールの有効性と防御フレームワークのレジリエンスを検証することがますます重要になっています。2021年には、Purple TeamingやコラボレーティブなRed Teaming演習などのハイブリッドなセキュリティ評価が増加し、クライアントのインフラのレジリエンスに対するストレステストを実施すると同時に、SOCチームが将来の攻撃に備え、検知するための方法についての貴重なインサイトを得ることができるようになると予想しています。

### 日本とAPAC

日本ではTLPT-FISC型テストに関心を持つ企業が増えています。しかし、アジアパシフィックの他地域と比較して、オフENSEンシブセキュリティや敵対的なシミュレーションに関する業界全体の規制要件は現在のところありません。

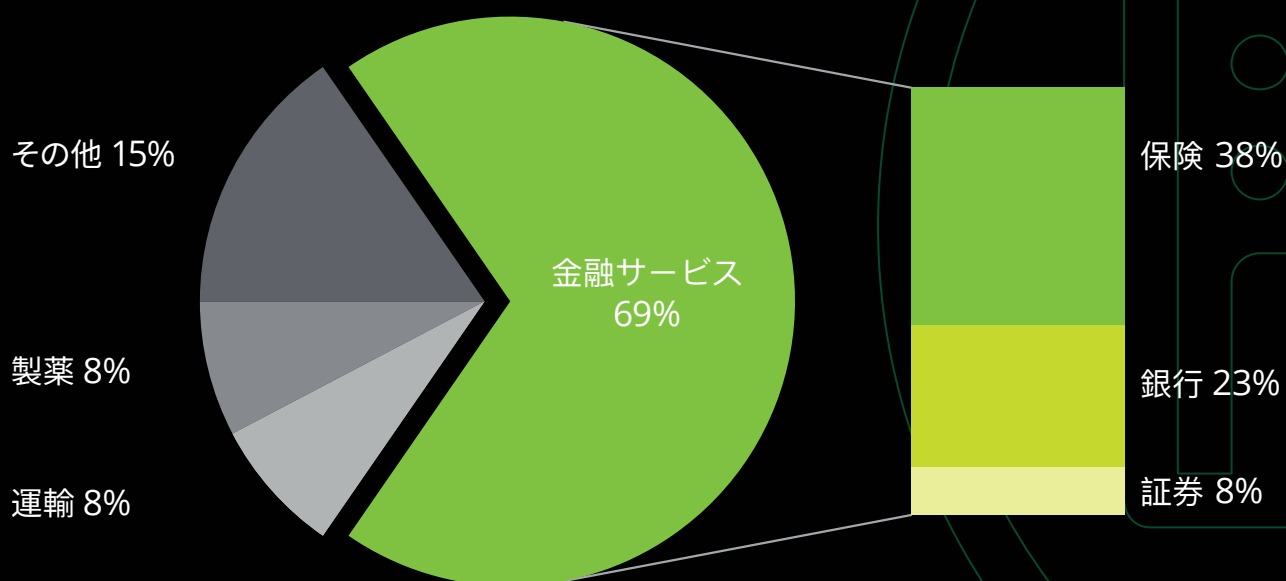


一方アジアパシフィック地域では、オーストラリアの金融規制協議会が、2020年7月にCyber Operational Resilience Intelligence-led Exercise (CORIE) 実施に向けたパイロットプログラムの広範なガイドラインを発表しました。また、シンガポールのMASをはじめとする他の規制当局も脅威主導型テストの要件を強化しており、東南アジア諸国を皮切りにルールが強化されることが予想されます。

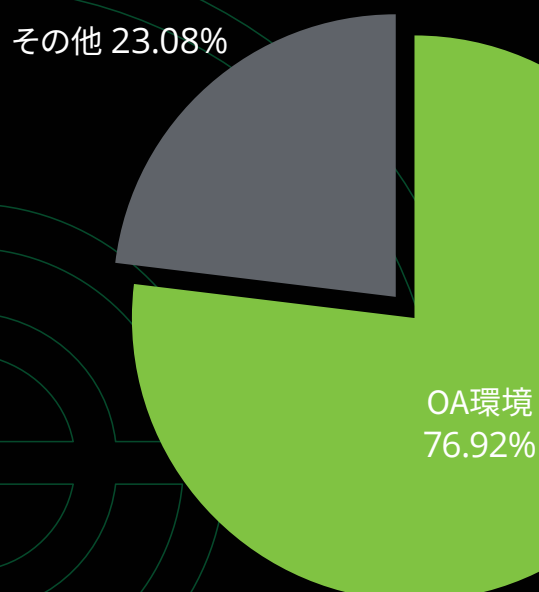
## 業界別インサイト エンゲージメントのタイプとクライアントの対応の概要

### Red Teamを実施した実績のあるクライアントの業界の割合

日本国内の実績としては金融業界の割合が最も高くなっています。2021年には保険会社のクライアント数が急増しています。



### 攻撃対象の割合



日本では、従業員の業務端末がマルウェアに感染したケースを想定し、OA環境を主な評価の対象とすることが主流になっています。通常、これらのエンゲージメントでは、クライアントの業務端末から開始し、機密情報の窃取と流出、ネットワーク間の侵入経路の特定などといった課題の識別に焦点を当てます。

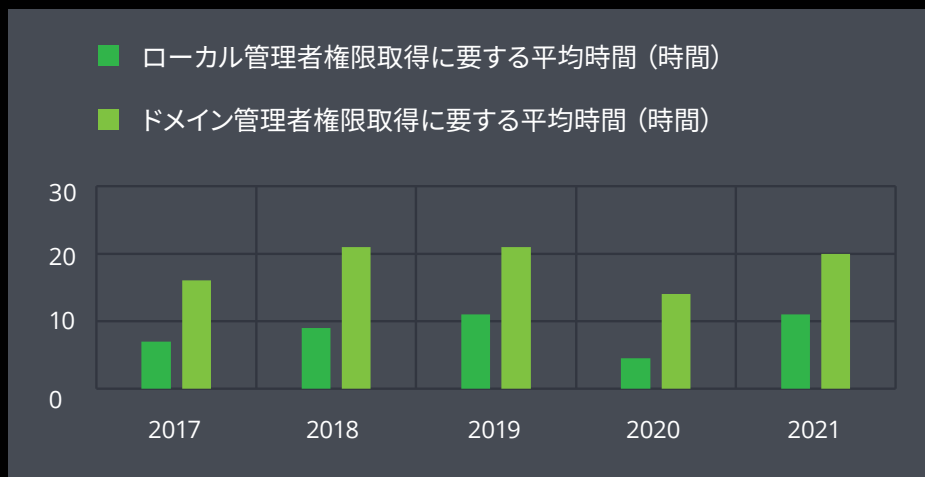
COVID-19の影響により、大半のクライアントが人的 / 物理的なセキュリティからリモートアクセスのセキュリティへと、Red Teamingの対象を変更しました。また、IoTとOTのテストに対する関心も高まっています。

# 攻撃者のパフォーマンスとクライアントのレジリエンス

## ローカル、ドメイン管理者を巡る攻防

Red Teamingのエンゲージメントでは、多くの場合、第一または第二の攻撃目標として、ローカル管理者やドメイン管理者等の特権アカウントを取得することが求められます。これまで行ってきた評価の傾向として、組織のセキュリティ成熟度と当チームがこれらの権限を取得するのににかかった時間には相関関係があり、組織のセキュリティ成熟度を測る指標となります。

ローカルおよびドメイン管理者権限の取得に要する時間には、すべてのセクターにおいて大きな差異はありません。



どのくらいの頻度ですべての目標を達成しましたか？

70%

ローカル、ドメイン管理者共に

※クラウンジュエルの達成にローカル、ドメイン管理者権限の取得が必要ないエンゲージメントを除く

ターゲットとなるネットワークに初期侵入することは依然として可能ですが、クライアントが導入する防御策や管理体制のレジリエンスが向上していることを実感しています。前年度と比較して、全業界におけるクライアントの全体的なレジリエンスが26%向上していることがわかります。

# 攻撃者のパフォーマンスとクライアントのレジリエンス

## 攻撃目標の達成率

当チームでは94%のクライアントに対して、1つ以上の攻撃目標を、定められた期間内に達成しています。

尚、攻撃目標はクライアントと当チームとの協議によって定められるため、常に異なります。

## クライアントが選択する一般的な攻撃目標例

制限されたフォルダ内  
の機密情報の取得

環境間の侵入経路  
の特定

ネットワークからの  
データの外部送出等

特定環境への  
アクセスの取得

ドメイン・コントローラ  
のフル・アクセスの取得

# 業界別およびエンゲージメントタイプ別で見るクライアントのレジリエンス

## 評価毎に識別される発見事項の平均数

当社がこれまでにさまざまな攻撃的セキュリティ評価を実施したクライアントは、提示された推奨事項に基づいて長年に渡り活動しているため、解決すべき残課題は少ないようです。当社では、クライアントのネットワークやインフラのレジリエンス向上を支援するため、詳細な推奨事項と継続的なサポートを提供しています。

平均では、私たちのチームは、エンゲージメント毎に3個から17個の発見事項をクライアントに報告しています。

## クライアントへ報告する発見事項例

特権アカウントの管理  
不備

脆弱なパスワードの  
利用

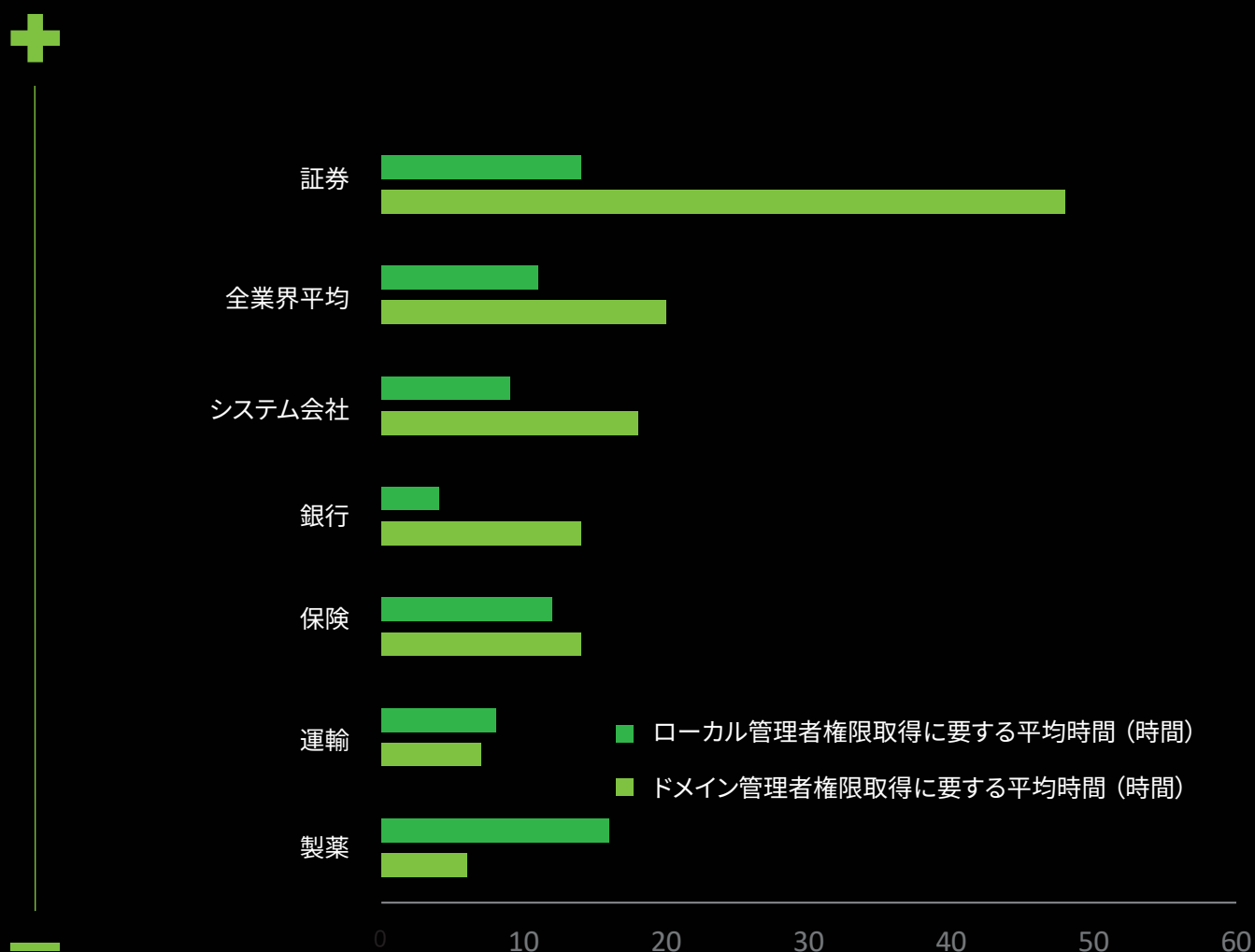
不十分な  
モニタリング

ネットワークアクセス  
制御の不備

マルウェアの実行が  
制限されていない、  
または検出されない

## 業界別およびエンゲージメントタイプ別で見るクライアントのレジリエンス

業界別に見ると、証券会社はRed Teamingエンゲージメントにおけるレジリエンスが平均して他業界よりも高いようです。一方、製薬会社や運輸のクライアントは、当社のチームが特権的なアクセスを得るために必要な時間が最短でした。



なお、クライアントのセキュリティ成熟度が高まり、ゼロトラストセキュリティがますます実装されるにつれて、ドメインへのアクセスと攻撃の成功との相関性が低下していくため、当社の評価指標もこれまでとは異なるものへと移行していくことが見込まれます。



# Deloitte.

## デロイト トーマツ

デロイト トーマツ グループは、日本におけるデロイト アジア パシフィック リミテッドおよびデロイト ネットワークのメンバーであるデロイト トーマツ 合同会社ならびにそのグループ法人（有限責任監査法人 トーマツ、デロイト トーマツ コンサルティング 合同会社、デロイト トーマツ ファイナンシャル アドバイザリー 合同会社、デロイト トーマツ 税理士 法人、DT 弁護士 法人およびデロイト トーマツ コーポレート ソリューション 合同会社を含む）の総称です。デロイト トーマツ グループは、日本で最大級のビジネス プロフェッショナル グループのひとつであり、各法人がそれぞれの適用法令に従い、監査・保証業務、リスク アドバイザリー、コンサルティング、ファイナンシャル アドバイザリー、税務、法務等を提供しています。また、国内約30都市以上に1万名を超える専門家を擁し、多国籍企業や主要な日本企業をクライアントとしています。詳細はデロイト トーマツ グループ Web サイト ([www.deloitte.com/jp](http://www.deloitte.com/jp)) をご覧ください。

Deloitte（デロイト）とは、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバル ネットワーク 組織を構成するメンバー ファームおよびそれらの関係法人（総称して“デロイト ネットワーク”）のひとつまたは複数 を指します。DTTL（または“Deloitte Global”）ならびに各メンバー ファームおよび関係法人はそれぞれ法的に独立した別個の組織体であり、第三者に関して相互に義務を課しまたは拘束させることはありません。DTTL およびDTTL の各メンバー ファームならびに関係法人は、自らの作為および不作為についてののみ責任を負い、互いに他のファームまたは関係法人の作為および不作為について責任を負うものではありません。DTTL はクライアントへのサービス提供を行いません。詳細は [www.deloitte.com/jp/about](http://www.deloitte.com/jp/about) をご覧ください。デロイト アジア パシフィック リミテッドはDTTLのメンバーファームであり、保証有限責任会社です。デロイト アジア パシフィック リミテッドのメンバーおよびそれらの関係法人は、それぞれ法的に独立した別個の組織体であり、アジア パシフィック における100を超える都市（オーストラリア、バンコク、北京、ハノイ、香港、ジャカルタ、クアラルンプール、マニラ、メルボルン、大阪、ソウル、上海、シンガポール、シドニー、台北、東京を含む）にてサービスを提供しています。

Deloitte（デロイト）は、監査・保証業務、コンサルティング、ファイナンシャル アドバイザリー、リスク アドバイザリー、税務およびこれらに関連するプロフェッショナル サービスの分野で世界最大級の規模を有し、150を超える国・地域にわたるメンバーファームや関係法人のグローバルネットワーク（総称して“デロイト ネットワーク”）を通じFortune Global 500®の8割の企業に対してサービスを提供しています。“Making an impact that matters”を自らの使命とするデロイトの約312,000名の専門家については、([www.deloitte.com](http://www.deloitte.com)) をご覧ください。

本資料は皆様への情報提供として一般的な情報を掲載するのみであり、デロイト トウシュ トーマツ リミテッド（“DTTL”）、そのグローバル ネットワーク 組織を構成するメンバー ファームおよびそれらの関係法人（総称して“デロイト ・ ネットワーク”）が本資料をもって専門的な助言やサービスを提供するものではありません。皆様の財務または事業に影響を与えるような意思決定または行動をされる前に、適切な専門家にご相談ください。本資料における情報の正確性や完全性に関して、いかなる表明、保証または確約（明示・黙示を問いません）をするものではありません。またDTTL、そのメンバーファーム、関係法人、社員・職員または代理人のいずれも、本資料に依拠した人に関係して直接また間接に発生したいかなる損失および損害に対して責任を負いません。DTTLならびに各メンバーファームおよびそれらの関係法人はそれぞれ法的に独立した別個の組織体です。

Member of  
Deloitte Touche Tohmatsu Limited

© 2021. For information, contact Deloitte Tohmatsu Cyber LLC.

Designed by CoRe Creative Services. RITM0702284