公開可

SB Technology

Azure AD への不正サインインとリアルタイム遮断の考察

2023/1/26

SBテクノロジー株式会社

発表者紹介

SB Technology

氏名：安藤 翔一

所属：SBテクノロジー株式会社　サービス統括　セキュリティ＆テクノロジー本部

経歴：

ソフトバンク・テクノロジー株式会社（現：SBテクノロジー株式会社）入社後、UTM、WAF といったセキュリティ商材のインテグレーションや、 Microsoft 365 製品のセキュリティ機能の構築に従事、その後セキュリティサービス開発や運用設計に携わり、現在は Microsoft 365 を対象としたフィッシングの調査研究を行っている。

講演実績：

CODE BLUE 2022 「Microsoft 365 アカウントを攻撃するインフラの分析」

アジェンダ

SB Technology

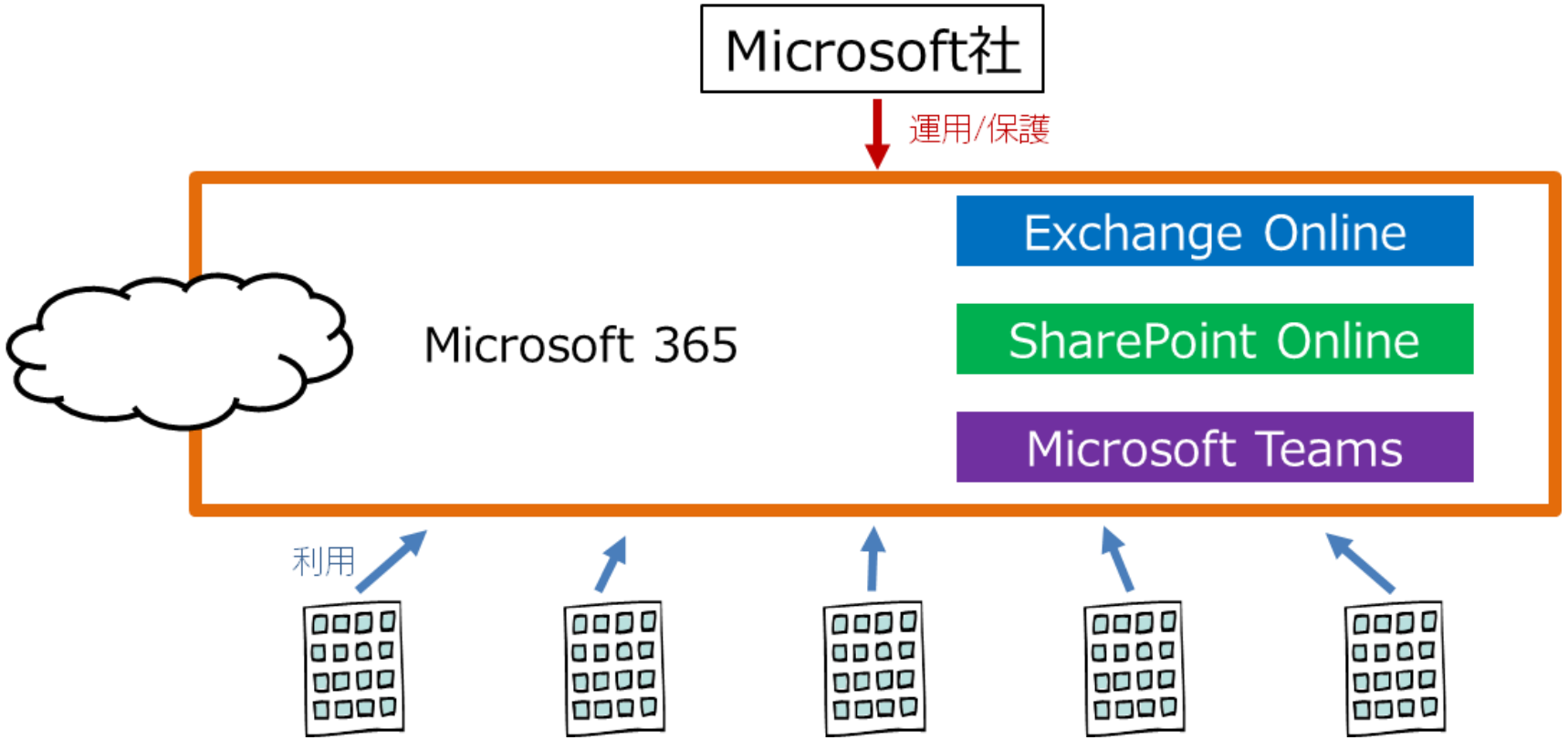
- イントロダクション
- Azure ADサインインログから見えるアカウント不正利用元IPアドレス
- 短時間のアカウント侵害による被害事例（スパムメール大量送信）
- まとめ

イントロダクション

Microsoft 365 の組織インフラとしての価値

SB Technology

Microsoft 365 を利用する多くの組織ではインフラ運用への投資費用が下がり、かつ堅牢化することができる。



Microsoft 365 に対する脅威

SB Technology

1. アカウントに対する攻撃
   - フィッシング
   - ブルートフォース
   - リスト型攻撃

2. データに対する攻撃
   - 意図せぬデータ公開
   - 不適切なアクセス権限設定

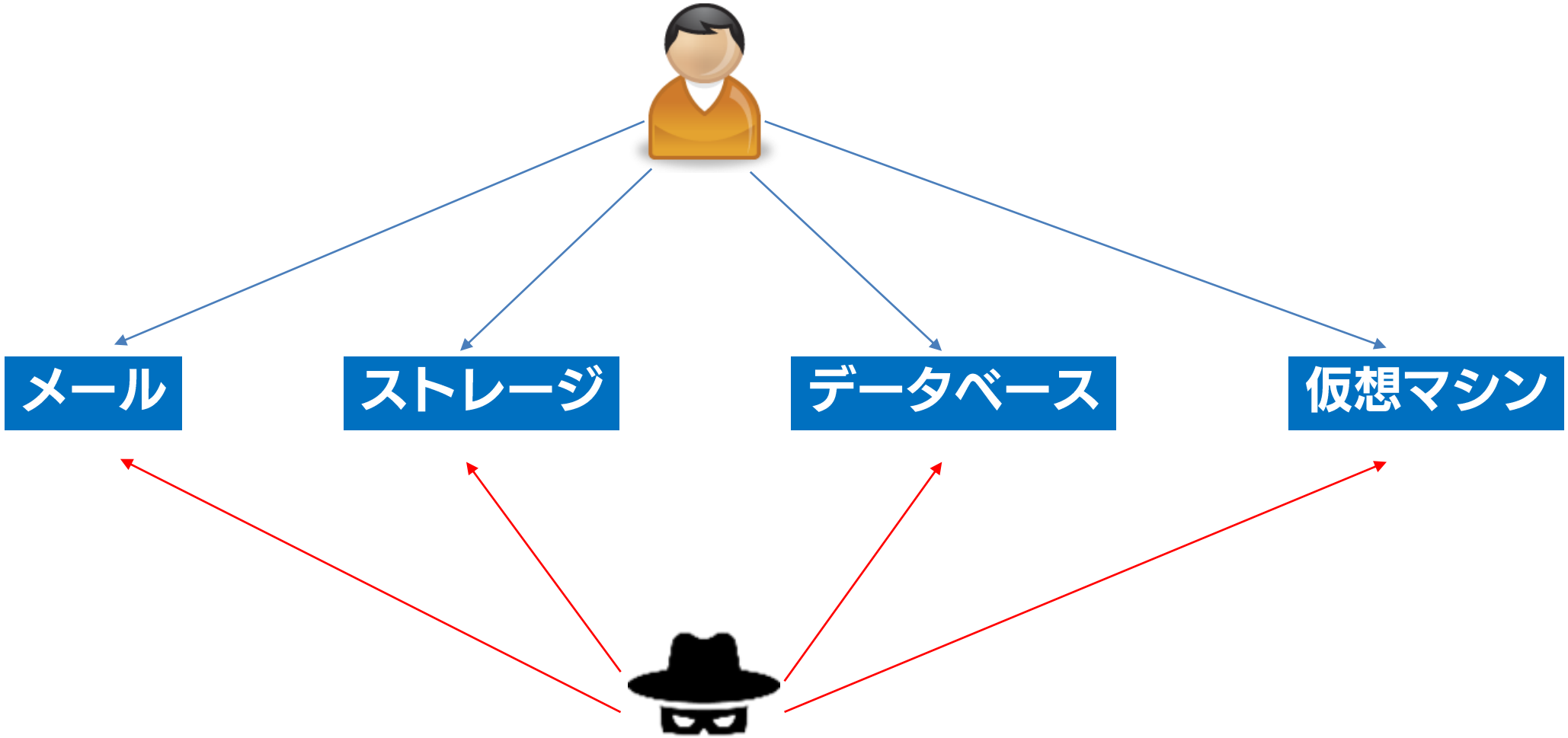
1. データセンター/物理インフラに対する攻撃

2. 通信経路に対する攻撃
   - 通信の盗聴
   - DDoS攻撃

3. アプリケーション/ミドルウェア/OSに対する攻撃
   - 脆弱性を狙ったエクスプロイト

アカウント窃取のリスク増大

SB Technology

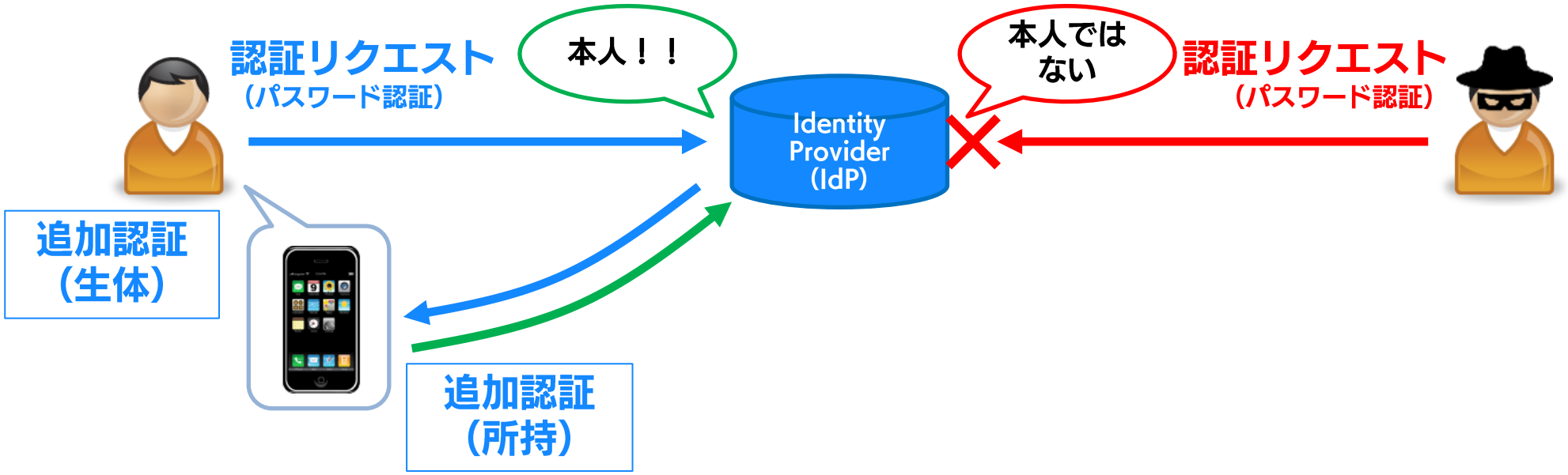


アカウントが乗っ取られてしまった場合、
数多くの情報資産が一度に乗っ取られる恐れがある

多要素認証（MFA：Multi-Factor Authentication）

SB Technology

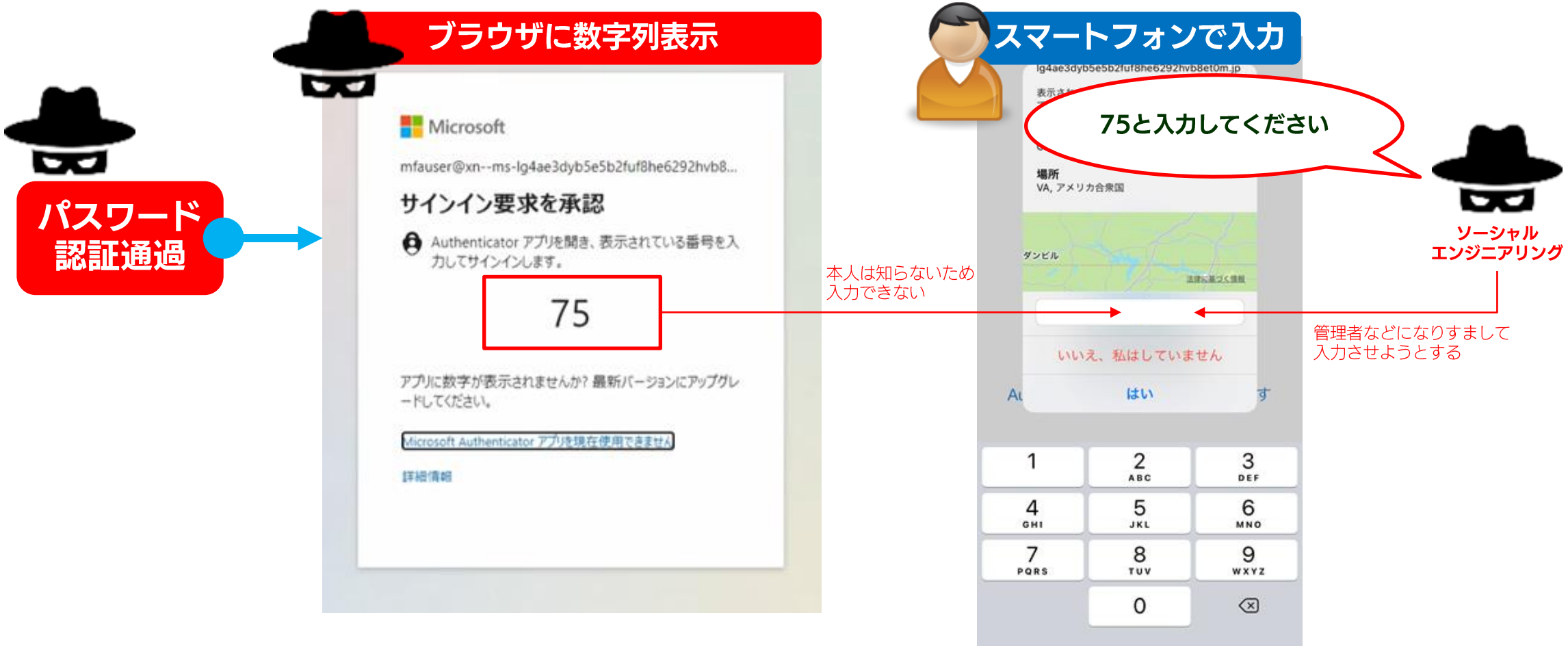
Microsoft 365 においてパスワード認証だけでは脆弱であるため、クラウドアカウントに対しては多要素認証を設定することが推奨される。



MFA疲労攻撃への対策

SB Technology

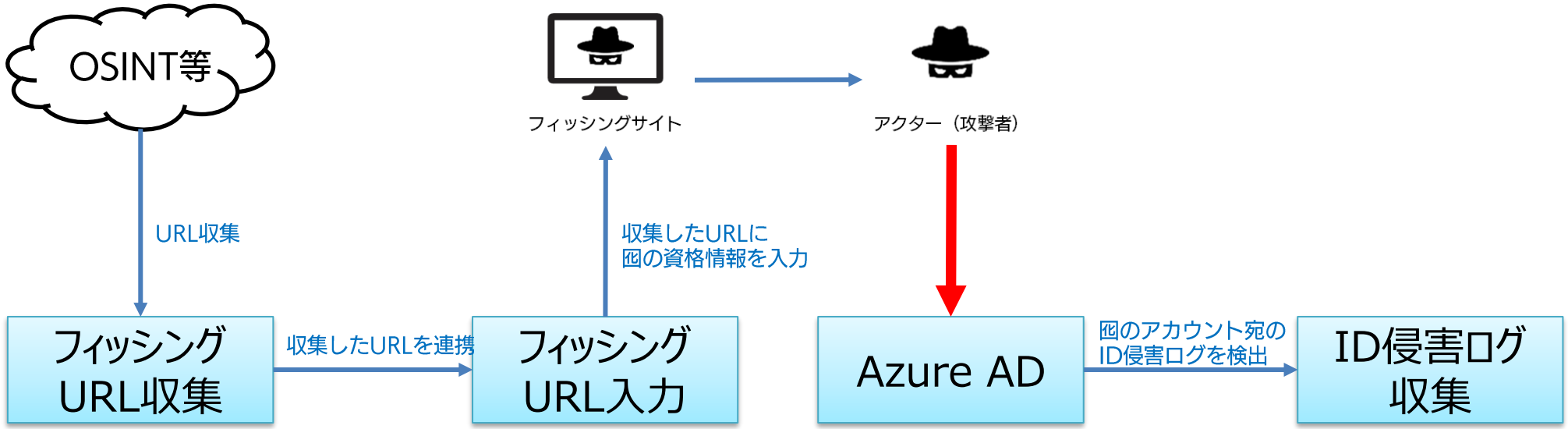
Microsoft においてはMFA疲労攻撃への対策として「ブラウザ表示された数字を入力させる」方式が推奨されているが、ユーザーが騙された場合は不正サインインを許可してしまうこともあり得る。



侵害行為ログの収集

SB Technology

アカウント乗っ取りに最も有効なのはIntuneを使用したデバイス認証だが、導入のハードルも高いためデバイス認証以外にアカウント乗っ取り対策となりうるものがないか、侵害行為に関連するログの収集基盤を構築して、アカウント乗っ取りに関連する情報の調査/分析を行った。

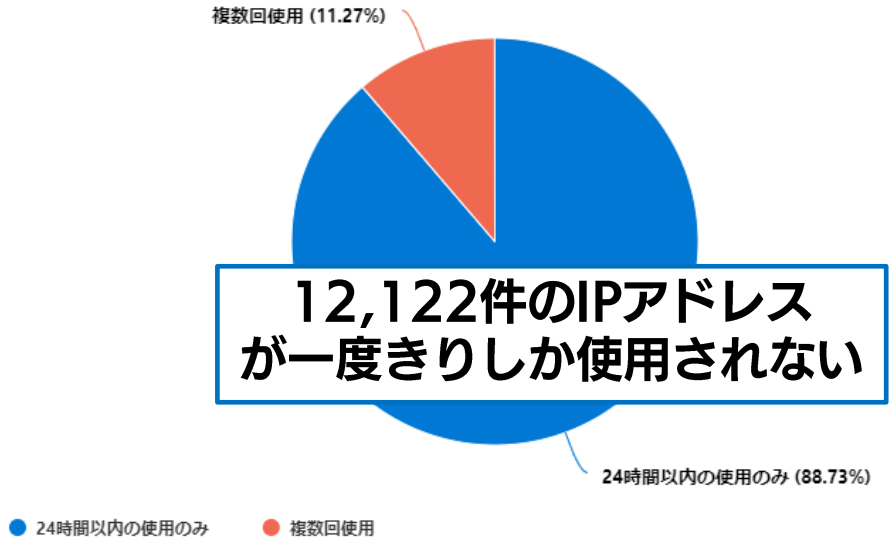


Azure ADサインインログから見える
アカウント不正利用元IPアドレス

アカウント不正利用元IPアドレス

SB Technology

2022/2/18~2023/1/5までの間に囮アカウントに対してアクセスをしたIPアドレスの総数は13,362件であったが、24時間以内の利用にとどまり一度きりの利用となったIPアドレスは88.73%（12,122件）となった。



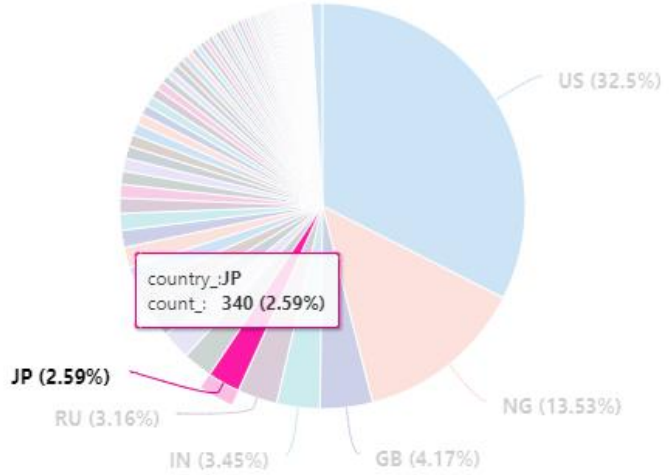
図：囮アカウントに対するサインイン元IPアドレスが
24時間経過後に再使用されたか否かの割合

約9割が一度しかIPアドレスを使わず、
ブロックリストによる大きな保護効果は見込めない

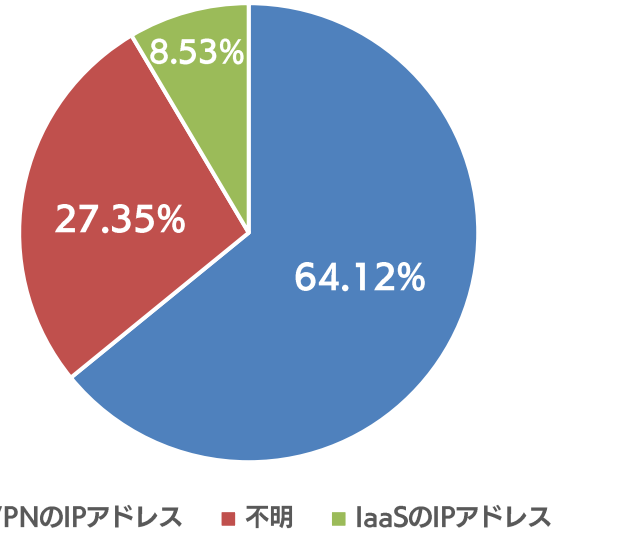
送信元IPの属性（国内）

SB Technology

2022/2/18~2023/1/5までの間に囮アカウントに対してアクセスをしたIPアドレスをSPUR（https://spur.us）を使用してレピュテーション情報を確認したところ、Geo IP情報が日本と推察されるサインイン元IPは340件であり、そのうち64.12%（218件）がVPNサービスのIPアドレスであるレピュテーション情報が確認できた。
日本国内に限っていえばVPNサービスが使用しているIPアドレスを遮断することで6割ほどの不正利用を防ぐことが出来る可能性はある。



図：囮アカウントに対するサインイン元Geo IP情報の国別割合

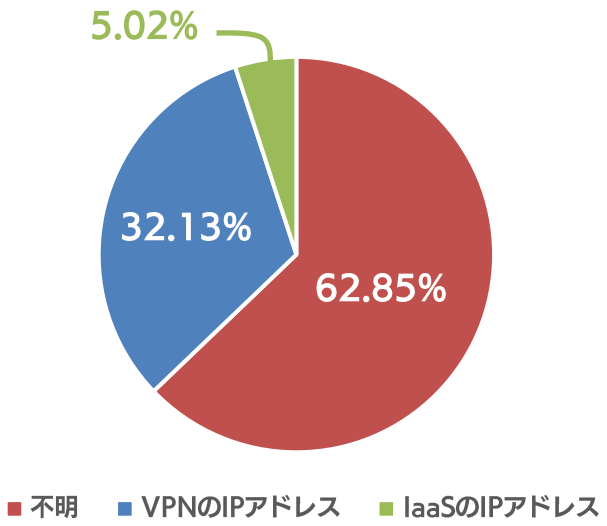


図：Geo IP情報が日本国内であるサインイン元IPアドレスがVPN又はIaaSで使用されているか否かの割合

参考：送信元IPの属性（全体）

SB Technology

2022/2/18~2023/1/5までのGeo IP情報が日本国外であるIPアドレスも含めた場合、VPNサービスのIPアドレスであるレピュテーション情報は32.13%（4,210件）あった。
また、侵害済みの囮アカウントを使用してVPNサービスに登録しようとする挙動も確認することができ、過去同様に侵害したアカウントでVPNサービスを利用しているものと思われる。



図：サインイン元IPアドレスが
VPN又はIaaSで使用されているか否かの割合

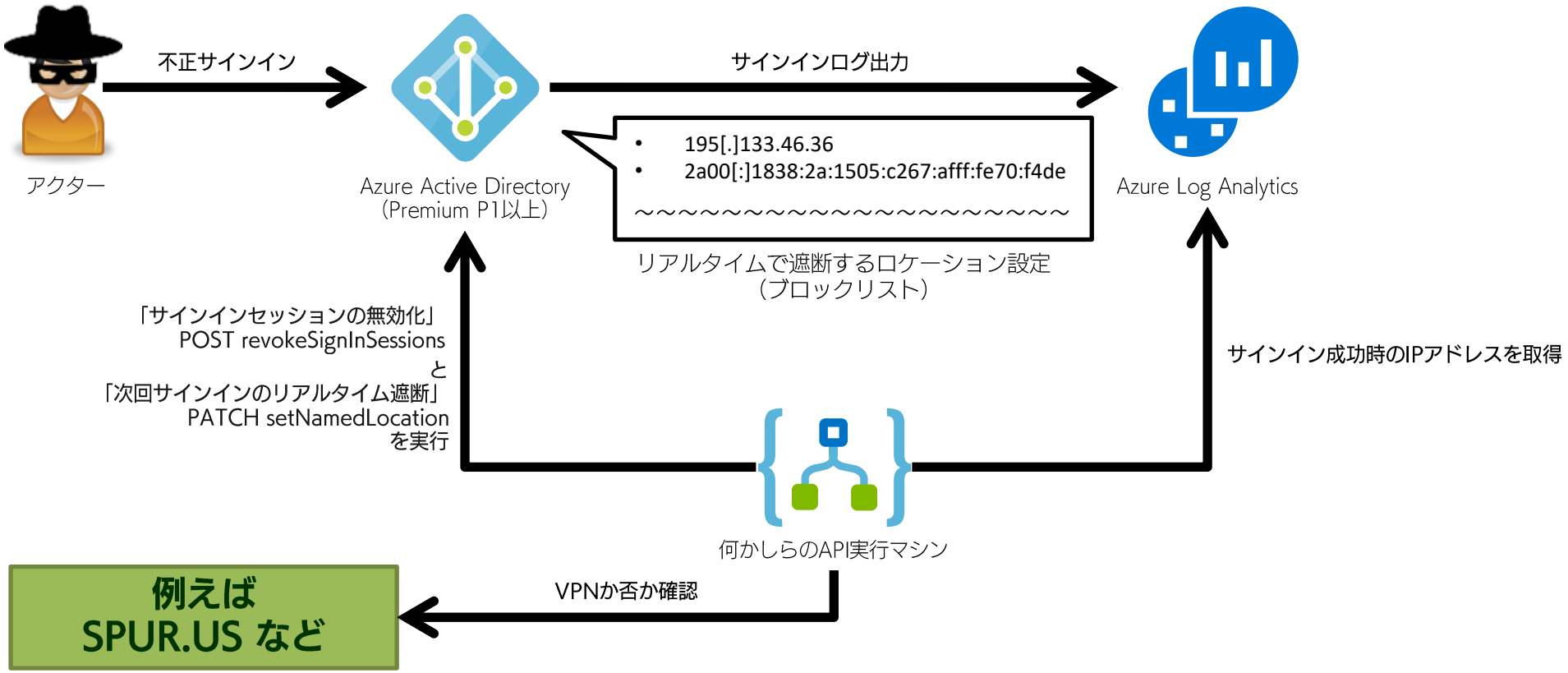
日付 (UTC +09:00)	件名	送信者
2022年6月15日 19:28	Your email has been changed	noreply@windscribe.com
2022年6月15日 19:22	Confirm your email address	noreply@windscribe.com
2022年6月15日 19:09	Confirm your email address	noreply@windscribe.com
2022年6月15日 19:03	Confirm your email address	noreply@windscribe.com

図：囮アカウントが受信したVPNサービス（Windscribe）登録メール

VPN利用のサインインを遮断する方法

SB Technology

VPNサービスを利用したサインインは Microsoft 365 単体で検出/ブロックができないため、VPNブロック機能を有したIDaaSにSAML連携等してブロックするか、APIを駆使するかのいずれかとなる。

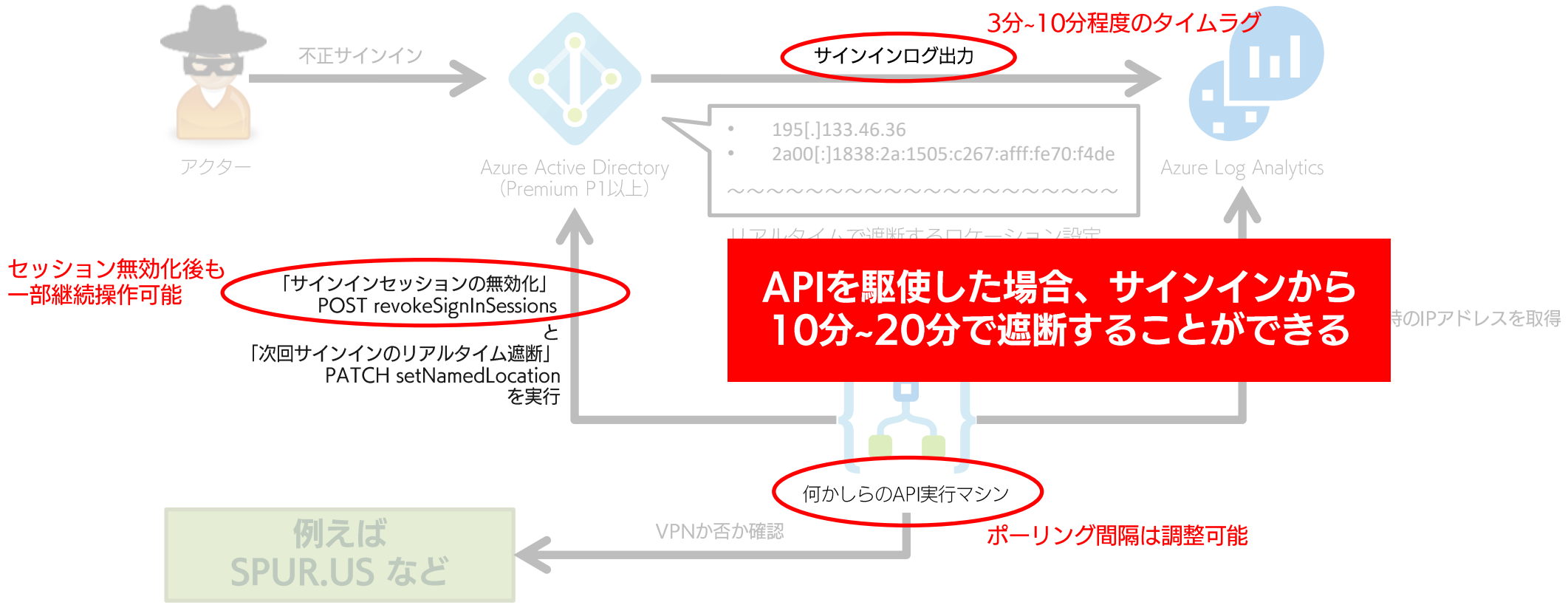


図：APIを駆使してVPNサービスを利用したサインインをブロックする方式

VPN利用のサインインを遮断する方法

SB Technology

VPNサービスを利用したサインインは Microsoft 365 単体で検出/ブロックができないため、VPNブロック機能を有したIDaaSにSAML連携等してブロックするか、APIを駆使するかのいずれかとなる。



図：APIを駆使してVPNサービスを利用したサインインをブロックする方式

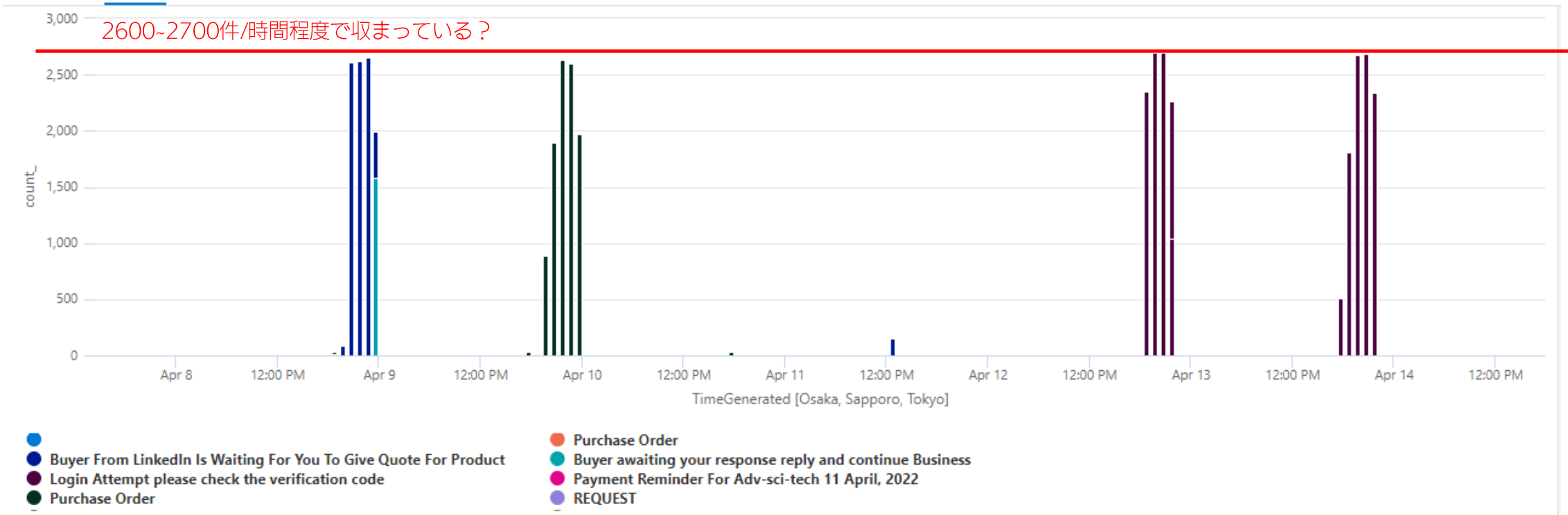
短時間のアカウント侵害による被害事例（スパムメール大量送信）

アカウント侵害後に大量にスパムメールを送信する

SB Technology

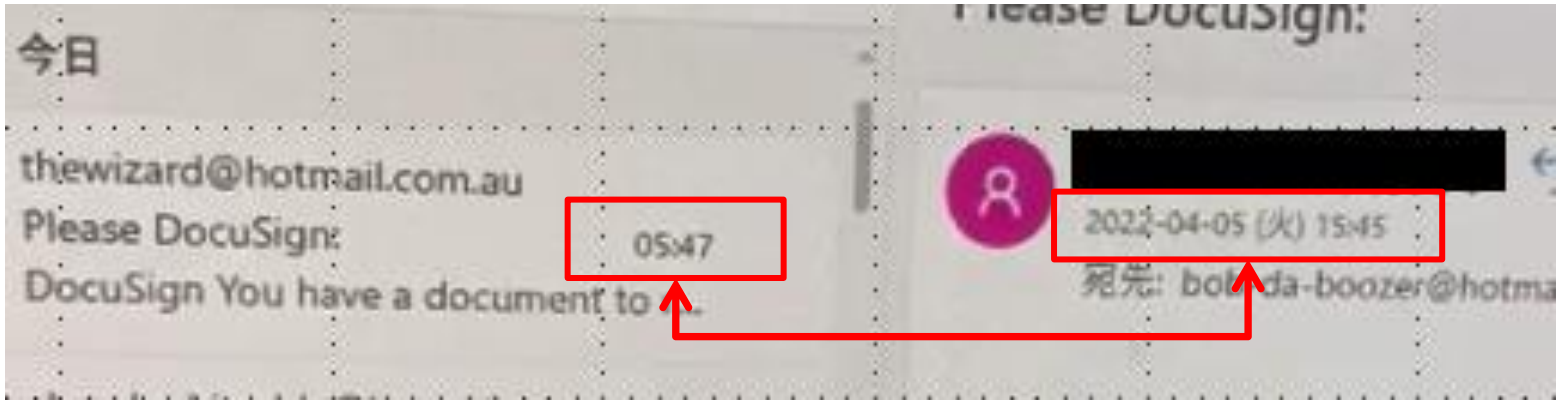
以下はアカウント侵害後に大量送信しようとしたスパムメールの件数で、1時間ごとの送信ログ件数を表すものである。

このメール送信は数分間のアカウント侵害で引き起こされたもので、尚且つアカウントの停止やサインインセッションの無効化を行っても抑制できなかった。



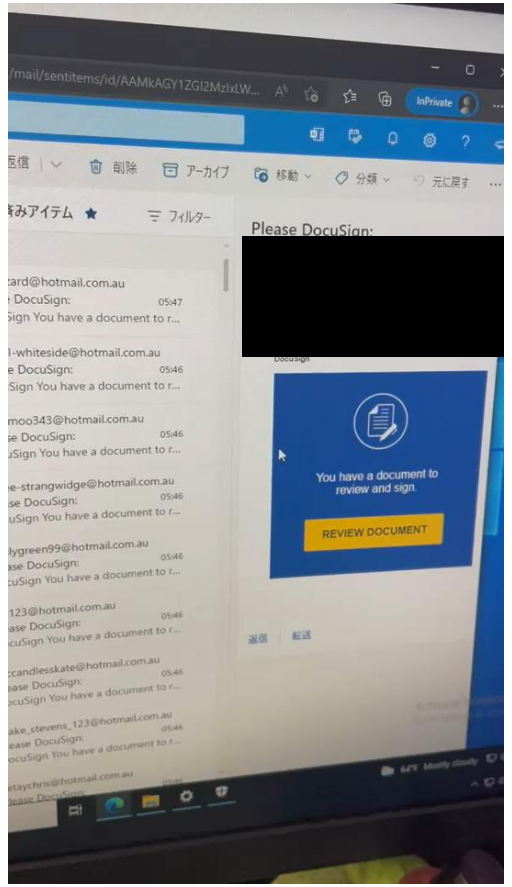
送信処理が実行され続けている

SB Technology



送信処理実行時間と送信処理完了時間に10時間ほど差がある
⇒大量送信によってメールがキューイングして遅延していると推測

【実際の送信済みメールフォルダ動画】



参考：対処方法

SB Technology

対処方法は「トランスポートルールによるメール送信の遮断」以外にない。

当該事象が発生した場合は Exchange Online 上のメッセージキューに大量のメールがキューイングされており、この場合、アカウント停止、パスワード変更、セッションリセット、メールプロトコルの制限（OWA禁止、レガシー認証プロトコル禁止など）を実施したとしてもメールの送信処理は止まらない。

トランスポートルールで止めたとしても送信キューは消えないため、
正規メールはキューがクリアされるまで送信できない

Microsoft社へ問い合わせたところ、

- メッセージ送信キューにキューイングされたメールは削除できない
- メッセージ送信キューの上限は送信制限の形であれば設定可能

との回答が得られた。

リアルタイム遮断を実施する方法

SB Technology

Azure ADによる認証時の遮断（＝リアルタイム遮断）を実施するには以下のような方法が考えられる。

- 不要な日本国外からのIPアドレスを条件付きアクセスで遮断
  他クラウドサービス連携などで国外からアクセスが発生するケースや、日本国外に拠点や従業員を有する組織の場合は運用は困難。

- Azure AD Identity Protection の有効化
  IPアドレスのレピュテーションによってリスクレベルを判定、レピュテーションに載ってこないものも多いが悪性IPは遮断可能。

- Microsoft Defender for Cloud App のセッションポリシーによってVPN利用の多いISPを遮断
  Geo IP情報がAzure ADのログ上で日本となっているIPアドレス340件のうち、VPN利用のレピュテーション情報がある218件にはISPの偏りがあった。 Microsoft Defender for Cloud App ではISP情報に基づいたリアルタイム遮断ができる。

- VPN利用のレピュテーション情報を有するIDaaSにフェデレーション
  SAML連携で他IDaaSにフェデレーションすることで認証制御に干渉してリアルタイム遮断できる。
  同様にADFSサーバにフェデレーションし、ADFSサーバへの通信制御でも実現可能。

- Azure AD へIPブロックリストの設定を行う
  収集しているIPアドレスのリストを場所として定義し、条件付きアクセスでリアルタイム遮断できる。
  同様にADFSサーバにフェデレーションし、ADFSサーバのクレームルールにIPアドレスのリストを定義して遮断できる。

まとめ

結論

SB Technology

短時間のアカウント侵害による被害事例を止めようとすると、認証時のリアルタイム遮断は必要となる。

Azure ADによって認証時に遮断するためのIPアドレスブロックリストの収集は、即時的に大きな効果は望めずとも継続すべきと考える。

公開可

情報革命で人々を幸せに

～ 技術の力で、未来をつくる ～

SB Technology