Deloitte.

sifma
Invested in America

Quantum Dawn 2

米国金融セクターにおけるサイバー演習

～回復とクライシスマネジメント～

2013年10月21日

トーマツ.

目次

背景

2013年、多くの大手メディアは、米国内の特に重要インフラに対するサイバー攻撃の脅威が高まっていることに対して注意を呼びかけました。サイバー攻撃は、ほとんど事前警告がなく行われる場合や、ある期間にわたり行われる場合があります。そのため、米国金融サービス・セクター（以下、金融セクター）では、これらの脅威へ警戒をするとともに攻撃への対応準備を実施しておくことを推奨しています。

2013年7月18日、米国金融サービス・セクターは大規模なサイバー攻撃への対応演習を開始した。米国証券業金融市場協会（SIFMA）が主催した、Quantum Dawn 2（以下、「QD2」）と呼ばれるサイバー演習は、システミック・サイバー攻撃(*)に対して連携と対応力を強化するための継続的な取組みにより、サイバー攻撃対応の次の段階を示すものとなった。

米国デロイトはSIFMAとともに本演習の客観的なオブザーバーとして参加し、セクター全体のサイバー事案への対応能力の向上を図るためのアフターアクションレポート（本資料）の作成を支援しました。

* システミック・サイバー攻撃
本稿でのシステミック・サイバー攻撃とは、システミック・リスクを引き起こす可能性のあるサイバー攻撃のことを指す。
本稿でのシステミック・リスクとは、個別の金融機関の支払不能等や、特定の市場または決済システム等の機能不全が、他の金融機関、他の市場、または金融システム全体に波及するリスクを指す。

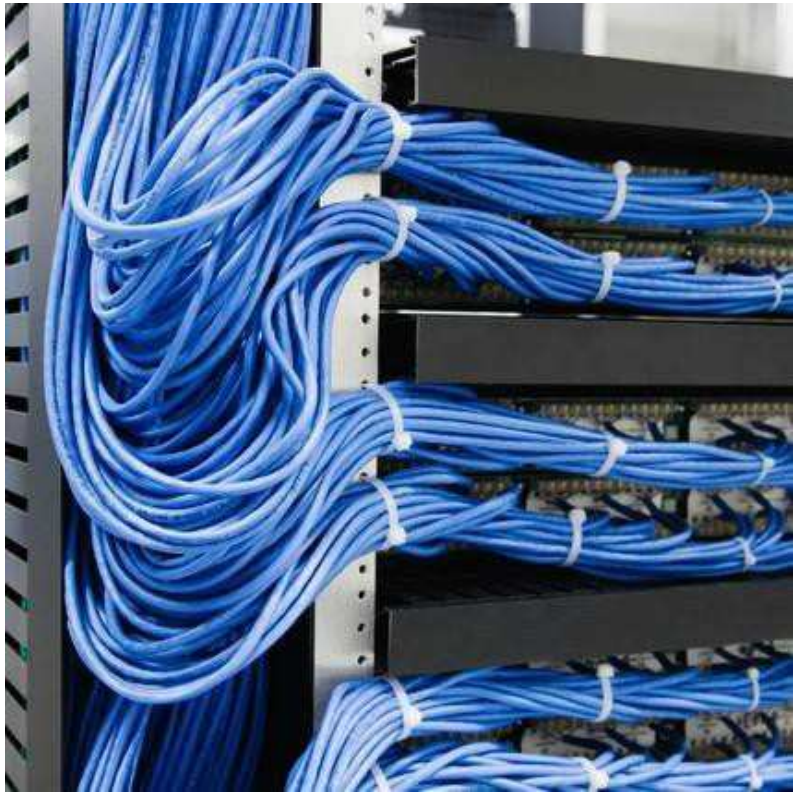
演習の目的

QD2は、取引日を想定した 6時間の演習です。SIFMAが設定した演習のゴールは、以下のとおり：

- サイバー攻撃のシナリオに応じたクライシスマネジメントプランと被害軽減策のリハーサルを行う。また、金融サービス業界における事業継続および情報セキュリティ業務に関する演習を行う。
- サイバー攻撃が起きた際の市場対応委員会の意思決定の演習を行う。市場に十分なプレッシャーをかけて、市場対応委員会がどの時点で金融市場を閉鎖する決定を行うかをテストする。
- 金融サービス業界内の重要インフラ損害時のシミュレーションを行う。
- 改訂されたセクター全体のインシデント対応フローを再検証する（QD1 AARより）。
- 攻撃後、業界の機能を復旧するための運用態勢について理解を深める。

QD2サイバー攻撃のシナリオ

演習シナリオには、外部者および悪意をもった内部関係者による双方から複数攻撃が含まれていました。その攻撃の動機は、多額の金銭の窃盗、株式市場の混乱、会社のポスト・トレード(*)処理能力低下の欲求によるものです。

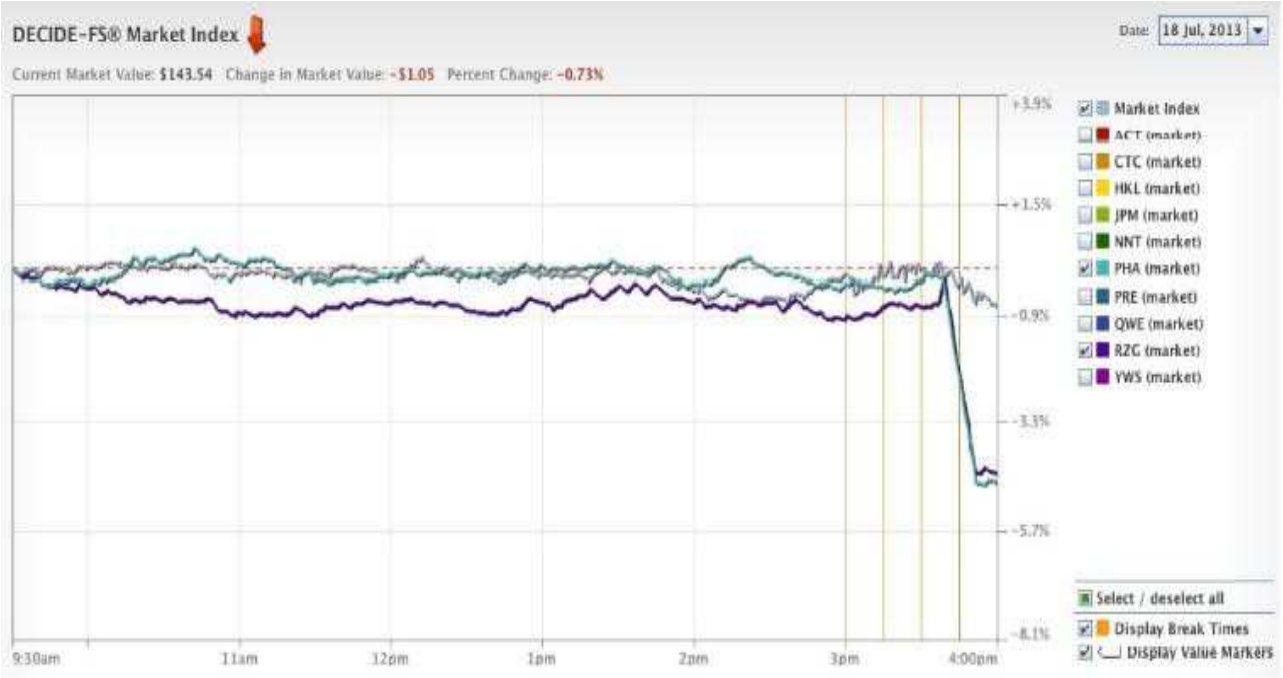


1. 不正に入手した管理者のアカウントを悪用し、標的とする株式の自動売却取引を行う
2. 関係者の注意を逸らすために偽造した悪意ある通信機器を導入し、自動売却取引の調査を遅らせる
3. 標的の株式について虚偽のプレスリリースを公表し、株価の下落を裏付ける
4. 分散型サービス拒否攻撃（DDoS攻撃）により、政府機関のウェブサイトとサービスを停止させる
5. 株式市場で広く使われている金融アプリケーションのソースコードを改竄する
6. ユーザ名とパスワードを収集するためにフィッシングメールの送信、偽の攻撃情報の送信により業界団体の信頼を低下させる
7. ポスト・トレード処理の低下を目的とした特別仕様のウイルスを放ち、技術サービスを混乱させる

*ポスト・トレード：
証券会社および資産運用会社において、市場での取引成立後、各口座への取引配分や取引内容の通知、資金や証券の決済、ステートメントの作成を行う業務を指す。

QD2サイバー攻撃のシナリオ（続き）

前ページで述べた攻撃ベクトルは、金融市場のパフォーマンスに直接的な影響を及ぼし、演習が終わるまでに金融市場を閉鎖する決定を下すように意図的に設計されました。
下のキャプチャー画面は、模擬環境下において、初日から、攻撃ベクトルが金融市場に与えた影響を示しています。マーケット指標の明らかな下落は、金融市場の反応と現実的に発生しうる次期クライシスを指し示しています。



QD2がもたらす望ましい結果

サイバー攻撃シミュレーションによって、ビジネス、オペレーション、テクノロジー、セキュリティとクライシスマネジメントの各チームの主要メンバーは結束し、攻撃シナリオの状況報告や対応を効果的に行うことができました。

金融セクターや様々な政府機関、市場と投資家の信頼の保護に重要な役割を果たす規制当局間で結ばれている官民パートナーシップは、さらにその連携を強化しました。

インシデントが展開され、米国金融サービス情報共有分析センター（米国FS-ISAC）、SIFMAおよび市場参加者は、米国FS-ISACクライシスマネジメント計画書に定められたインシデントに関する指揮体系の主要事項およびその他の関連手続を実行しました。これには、金融セクターを支援する様々な委員会やフォーラムも含まれています。

情報収集・共有のハブとしての取引所と手形交換所の役割が明確になりました。

SIFMAと米国FS-ISAC委員会間の強固な連携は歴然でした。

市場対応委員会の手続が実行され、金融市場を閉鎖する判断を下すことができました。

QD2の演習により、業界が何年もかけてインシデント対応とクライシスマネジメント実施のために取組んできた多くのプロセスと手続のテストが成功裏に終わりました。また、システミック・リスクの問題に対して協調的行動をとることについて、業界参加者の意識が高まりました。

推奨事項

この演習は、数々のポジティブな結果を生み出した一方で、インシデント対応およびクライシスマネジメントの手続を改善し、業界の参加者間の連携を強化する機会にもなりました。

セクター全体にわたるインシデントに関する指揮体系とプロセス

- 業界団体、市場参加者および政府機関の連携を強化することを目標とし、証券業界の特定のインシデントへの対応を向上させ、金融セクターにおける現行の対処計画を改善する
- サイバーインシデントにかかる分析および対処時における事業リーダーと技術リーダーの連携を向上させる
- サイバーインシデント対応とクライシスマネジメントにおける、取引所、手形交換所と委託を受けた政府提携機関の役割を拡張する。金融セクター支援のための利用可能な政府機関のリソースについての認識を高める

システミック・リスクの評価と決定プロセス

- サイバーインシデントが実際にシステミック・リスクに該当するかどうかを決定するための現行のガイドラインと意思決定フレームワークを補強する
- システミック・リスクの分析、情報共有、クライシスマネジメントを支援する次世代機能に投資する

コミュニケーションと情報共有

- サイバーインシデント対応時およびクライシス時における金融市場の開場又は閉鎖を決定する手続を体系化する
- 市場参加者間のコミュニケーションと情報共有を促進するための慣習を増進する
- 金融市場に対する信任と信頼を向上させるために、社会的認知およびコミュニケーション戦略を形成する

謝辞

- 参加された金融機関および協会
- 政府関係者 – 米国財務省、米国証券取引委員会（SEC）、米国国土安全保障省（DHS）および連邦捜査局（FBI）
- 業界団体 – 米国証券業金融市場協会（SIFMA）、米国金融サービス情報共有分析センター（米国FS-ISAC）、金融サービスセクター連携協議会（FSSCC）、金融・銀行情報インフラ委員会（FBIIC）、BITS -金融サービス円卓会議、ファーストシカゴ
- QD2はノリッジ大学応用研究所が設計したものです

連絡先

Karl Schimmeck
ヴァイスプレジデント
SIFMA
+1 212 313 1183
kschimmeck@sifma.org

Thomas Price
マネジングディレクター
SIFMA
+1 212 313 1260
tprice@sifma.org

Edward W. Powers
ナショナルマネジングプリンシパル
Deloitte & Touche LLP
+ 1 212 436 5599
epowers@deloitte.com

Walter Hoogmoed
プリンシパル
Deloitte & Touche LLP
+1 973 602 5840
whoogmoed@deloitte.com

Vikram Bhat
プリンシパル
Deloitte & Touche LLP
+1 973 602 4270
vbhat@deloitte.com

丸山 満彦
パートナー
サイバーリスクサービス
デロイト トーマツ リスクサービス株式会社
03 6213 1300
090 6492 3648
mitsuhiko.maruyama@tohmatsu.co.jp

飯塚　智
パートナー
クライシスマネジメントリーダー
有限責任監査法人トーマツ
03 6213 2450
jp_tokyo_cm_pmo@tohmatsu.co.jp

SIFMAは、数百の証券会社、銀行および資産運用会社が共有する利益を集約する団体です。これらの企業は全国のコミュニティーに参加して、事業のために資金を調達し、雇用の創出を促し、経済成長をリードします。

デロイトは、セキュリティおよびプライバシーに関する専門的な知見を活用し、企業がサイバー脅威に直面した場合に、安全かつ慎重に、危機からの回復プロセスを支援します。

http://www.sifma.org/services/bcp/cyber-exercise---quantum-dawn-2/

Member of
Deloitte Touche Tohmatsu Limited