デジタルプラクティス　Vol.9 No.3 (July 2018)

特集招待論文

高度標的型攻撃におけるインシデント対応の理論と実践

内田 法道[1]

[1]（株）ラック

本稿は，高度標的型攻撃のインシデントが発生した際に，CSIRT的組織が取るべき対応の流れについて，筆者が対応した高度標的型攻撃のインシデントでの経験に基づいた対処について解説する．

1. はじめに

（独）情報処理推進機構が毎年情報セキュリティ10大脅威を発表している．2016年から2018年の3年間，組織向けの脅威の1位を維持している脅威は，標的型攻撃による情報流出である☆1．2015年には日本年金機構が☆2，2016年には（株）ジェイティービーが☆3，標的型攻撃を受けて情報流出した旨を公表した．これらはテレビや新聞等で取り上げられ，標的型攻撃による情報流出の脅威が広く世の中に知られるきっかけとなった．

2017年は日本年金機構や（株）ジェイティービーのように，メディアに取り上げられる事案は発生していない．しかし，筆者がかかわる組織で提供している緊急対応サービスへの相談では，2017年も引き続き標的型攻撃の相談は来ており，その割合も増えている☆4．

本稿では，特定の組織を標的とした標的型攻撃の中でも，攻撃者が計画的かつ組織的に，特定の意図をもって標的組織を継続して侵害しようとする脅威を高度標的型攻撃☆5と定義する．その上で，筆者の考える高度標的型攻撃のインシデントが発生した場合のインシデント対応方法を紹介し，実際に対応した際の問題点と対処方法についても考察する．なお，本稿では，時間的余裕がなく問題が生じやすい初動フェーズを中心に紹介する．

2. 他文献での高度標的型攻撃への対応方法例

高度標的型攻撃への対応方法についてまとめた文献も公開されている．たとえば，攻撃者グループの侵害手順に着目し侵害の流れを断ち切ることで対応する方法が，Lockheed Martin Corporationから2015年に提示された[1]．これはサイバーキルチェーンと呼ばれるもので，チェーンを織り成す7段階のいずれかの段階において，予防策，検知策等の対策を実施してチェーンを断ち切れば，最終的な被害の発生を防ぐことが可能という考え方である．

また，2017年には総務省から『サイバー攻撃（標的型攻撃）対策防御モデルの解説』が公表された［2］．この文書は，インシデントレスポンスの計画と実行について，人・組織対策，事前対策・検知・事後対策の視点から技術的対策について解説している．

前者のサイバーキルチェーンの考え方は，侵害への対処という意味では有効であるが，インシデント対応のフェーズとは考え方が異なるためそのままは適用しがたいと考えられる．後者の総務省の考え方は，インシデント対応を想定した実践的な対応方法である点が本稿と近く，前者より適用しやすいと思われる．

3. 高度標的型攻撃へのインシデント対応方法

3.1 インシデント初動対応時の方針

高度標的型攻撃のインシデント対応方法の前に，インシデントが発生した際の初動対応の方針を3点述べる．これは，高度標的型攻撃に限らず，インシデントが発生した際に有用と考える．

- 原因追求の前に被害拡大を防止すべき
- 消え行く証跡を保全すべき
- 大きくとらえて，小さくおとす

3.1.1 方針1：原因追求の前に被害拡大を防止すべき

目の前で火が燃えている状況で火元を調べようとする人はいないであろう．まず消火や延焼防止に動くのが普通と思われる．ただ，サイバー攻撃の場合には，被害状況が目に見えないため，被害が継続しているのか（燃えているのか），被害が収まっているのか（鎮火しているのか）判別しにくい場合もあるが，原因追求より被害拡大防止が優先する．

特に，個人情報や取引先から受領した情報等の自組織に収まらない情報が流出している場合には，情報が流出した個人への詐欺や取引先へのサイバー攻撃等の二次被害の可能性がある．この点にも配慮し，被害拡大防止の慎重かつ十分な検討を行うべきである．

3.1.2 方針2：消え行く証跡を保全すべき

ディジタルデータは容易に変更が可能であり，その変更が見た目に判別しにくいという特徴がある．そのため，インシデントが発生したら，即座に現状を保持するために必要な措置をとる必要がある．被害が確認された機器のメモリやディスクのコピー，関連する機器のログの出力などであり，それらを保全と呼ぶ．

保全については，特定非営利活動法人デジタル・フォレンジック研究会が出している証拠保全ガイドライン[3]に詳しく記載されている．上述のガイドラインを参考に，自組織での保全方法や保全手順を検討，準備および訓練しておくことで，実際にインシデントが発生した場合でもスムーズに保全が行えるようになる．

3.1.3 方針3：大きくとらえて，小さくおとす

これは，ある警察関係者の方から聞いた話に基づく．110番に「川原にマネキンが落ちている」という通報が寄せられたときに，死体遺棄の可能性に配慮して対応するとのことである．この話を教訓とすると，インシデントの初動対応では，あらゆる可能性を想定して風呂敷を広げる．その上で，事実が確認できたら風呂敷を徐々にたたみ，最終的に広げた風呂敷が少しでも小さくなればよい，という心持ちで対応すべきと考える．

インシデント対応時に，影響や被害を小さく見積もろうとする人は少なからずいる．専門家は，その場の空気を読まずに風呂敷を大きく広げて，ヒアリングしながらたたむ姿勢が望まれる．

3.2　高度標的型攻撃へのインシデント対応方法

これまでの高度標的型攻撃のインシデント対応経験に基づき，下表の6つのステップで対応することが重要と考える．

表1　インシデント対応のフェーズ

No.	フェーズ	ステップ	概要
1	初動対応	遮断	攻撃者グループが自組織の侵害に利用している機器，ネットワーク，アカウント等を遮断し侵害状況から脱却する．
2	初動対応，本格対応	収集	攻撃者グループが自組織を侵害する際に利用していた攻撃手法や痕跡を，侵害が判明した機器等から調査，収集する．
3	本格対応	排除	収集した情報をもとに，攻撃者グループに侵害されていた機器やアカウントを特定し，当該機器の隔離やアカウントの無効化等を実施する．
4	本格対応	対策	攻撃者グループによる組織内ネットワークへの再侵入を防ぐための対策，また再侵入されても即座に検知するための対策を検討・実施する．
5	本格対応	監視	遮断を解除した上で，対策で導入した機器のログや認証ログ等を高頻度で収集，分析し，再侵入の痕跡の有無を経過観察する．
6	事後対応	復旧	監視体制を通常の頻度に戻すが，早期検知のための監視態勢は維持する．

3.2.1　初動対応フェーズ

初動対応フェーズで取るべきステップは，遮断と収集である．

遮断ステップは，前章で記載した初動対応時の方針の1つである被害拡大防止を優先するという方針に沿った対処である．攻撃者グループによる侵害状況から脱却し，以後の被害拡大防止を目的として，侵害に利用されているネットワーク，機器，アカウントを隔離，遮断，無効化等する対応である．遮断の対象は，主にネットワーク，機器，アカウントであり，遮断の範囲は，侵害範囲に限定するか全体であり，それらを組み合わせて対応する．

侵害範囲が限定的な場合は，侵害が確認された機器をネットワークから外す，指令サーバへの通信を制限する，該当アカウントを無効化するという対応となる．一方で，侵害範囲が広い場合にはインターネットと組織内LANの境界でネットワークを遮断，アカウントの無効化やパスワードの初期化といった大掛かりな対応となる．問題となるのは，侵害範囲が不明な場合で，前章で紹介した大きくとらえるという方針に従えば，確実に影響が及ばないという範囲以外は侵害の可能性を考慮して遮断対応すべきである．望ましいのは，インターネットとの境界で，安全と確認できた通信のみを許可し，それ以外の通信をすべて禁止する遮断の方法（ホワイトリストでの遮断）である．業務影響が大きいというデメリットはあるものの，適切に遮断できれば以後の被害拡大はないため，以後の対応に集中できるというメリットがある．

次の収集ステップは，攻撃者グループの攻撃手法や侵害方法を調査して情報を収集する対処である．収集した情報から攻撃者グループが利用する攻撃手法の特徴を理解することで，次の排除ステップにおいて排除する侵害範囲の特定が可能となる．

収集すべき情報としては，攻撃者グループの利用している遠隔操作型のマルウェア情報，通信する指令サーバの情報，マルウェア等を設置・感染させるフォルダ，利用する攻撃ツール，利用しているアカウント等である．攻撃者グループは組織内システムを掌握できる管理者権限の奪取を当面の目標としているため，管理者権限を保有しているアカウントの不正利用，Active Directoryサーバの侵害状況等も確認するとよい．また，攻撃方法として，遠隔操作型のマルウェアだけでなく，VPN等の社員や職員が利用する外部接続機能が利用されることもあるため，VPN等の認証ログ等の確認も重要である．

遮断した段階で，攻撃者グループにインシデント対応していることを気付かれている可能性が高い．そのため，ホワイトリストでの遮断をしていない場合は，攻撃者グループが攻撃手法を変化させる前に迅速に調査する必要がある．この段階では，新たに侵害されている機器が見つかる場合もあるため，それらに対しても攻撃手法に関する情報を収集するとともにネットワーク，機器，アカウントの遮断も実施する．

3.2.2 本格対応フェーズ

本格対応フェーズで取るべきステップは，収集，排除，対策，監視である．

排除ステップは，収集ステップで情報収集した結果をもとに侵害されている機器やアカウントを特定して，それらを隔離，無効化する対処である．本ステップの目的は，組織内ネットワークから侵害機器を排除して内部をクリーン化することである．

侵害範囲の特定は，ネットワークと機器との両面で確認する．ネットワークでの特定は，収集ステップで攻撃者の利用している指令サーバが判明していれば，まずはその指令サーバと通信している端末を特定する方法がある．加えて，外部へのWeb通信のログ，DNSのクエリログがそれぞれのサーバに保持されていれば，それらのログから遠隔操作型マルウェアと思われる不審な通信を分析することで，新たな指令サーバが見つかることもある．

機器での特定は，機器から必要な情報を収集するツール等を利用して情報を集約し，攻撃者が利用しているマルウェアや攻撃ツール等がないか確認する方法がある．また，機器に遠隔から一括で調査可能なツールが導入されている場合はそれらを利用して確認する方法もある．なお，これらの方法で新たな侵害機器が確認された場合は，収集フェーズに戻って攻撃手法等を確認し新たな痕跡がないか確認が必要である．そして，それらに基づいて排除ステップを再度行うというように，収集と排除は循環して対処することになる．

対策ステップは，遮断を解除して通常運用に戻すにあたり，可能な限りの予防策と迅速に検知可能な検知策とを実施する対処である．当該対策の実施は遮断を解除する条件となるが，原因が判明しなければ対策が実施できない訳ではない．実際には侵害時期が6カ月以上前だとログや痕跡が残っておらず原因が明確に判明しない場合も多い．そのため，人員等に余裕がある場合には初動対応フェーズと平行で対策ステップを進めることを検討すべきである．

高度標的型攻撃の対策では，マルウェア感染の防止に注目しがちである．しかし，実際にはネットワーク構成の見直し，アカウント管理の見直し，ログ取得項目や期間の見直し，VPNの認証強化，重要情報を扱うネットワークセグメントの分離，インシデント対応体制の整備といった基

本的な対策こそが有効な対策である．基本的なセキュリティ対策を確実に実施しておくことが，被害や影響を抑える重要なポイントと考える．

監視ステップは，対策ステップの実施を条件に，遮断ステップで実施した遮断を解除して通常の運用に戻す段階である．加えて，対策ステップで導入した検知策であがるアラートやイベントを継続的に監視して，侵害が継続していないか新たな侵害が発生していないか経過観察も実施する．侵害された機器を排除ステップで完全に排除できていない場合には，遮断の解除を契機として攻撃者グループが侵害を再開する可能性がある．そのため，遮断解除後少なくとも1カ月程度は監視を強化しておく必要がある．その期間に不審な事象が発生した場合には，迅速に確認・調査し再遮断も念頭に対応する．

本格対応フェーズの，排除および対策のステップが最もリソース（人，物，金）を必要とする．どの程度のリソースを投入しどこまで対応するのか，経営的な視点での判断が必要となる．

3.2.3　事後対応フェーズ

事後対応フェーズで取るべきステップは，復旧である．

復旧ステップは，監視ステップでの経過観察で不審な事象が発生しないようであれば強化された監視体制を通常の体制に戻す対処である．ただし，高度標的型攻撃の特徴は継続的かつ執拗に標的組織の侵害を試みる点にあり，引き続き警戒を怠らないようにする．

高度標的型攻撃の被害にあったある組織では，3カ月かけて通常業務へ復旧した後，同一の攻撃者グループによるものと思われる標的型メールが，その年の年末年始に届いた．また，別のケースでは，侵害された本社でのインシデント対応中に，傘下のグループ会社に同一の攻撃者グループによるものと思われる標的型メールが届いた．攻撃者グループが関心を持つ情報を保有している限り，侵害再開はあり得ると考えた方がよい．しかしながら，監視ステップで実施していた警戒態勢を維持するにはコストがかかる．そのため，特に影響の大きな管理者権限を有するアカウントの不正利用といった重要なポイントに監視を絞るなど，監視体制の工夫が必要となる．

4．実際のインシデント対応における問題と対処について

前章では高度標的型攻撃のインシデント対応方法について述べたが，実際のインシデント対応の現場では紹介した通りにことが進まない問題が発生する．本章では，そのような問題と対処について，時間的余裕がなく問題が生じやすい初動対応フェーズを中心に実際のインシデント対応経験から得た知見を述べる．

4.1　遮断ステップ：ネットワーク構成が把握できていない問題と対処

適切な遮断を実施するには，ネットワークの構成管理が実施されておりインターネット等の外部との境界が特定できている必要がある．そのためネットワークの論理構成の把握が重要となるが，ネットワーク構成図がない，ネットワーク構成図があっても最新状態ではない，ネットワーク構成図から一部の情報が削除されるというケースがある．適切な構成管理が実施されていない場合，ネットワーク管理に詳しい担当者，委託先の技術者等を集めて，その場で現状の構成を把握することから始める必要がある．

4.2　遮断ステップ：ホワイトリストでの遮断ができない問題と対処

明らかに組織内システムの広範囲が攻撃者グループに侵害されているにもかかわらず，業務影響を理由にホワイトリストでの遮断への移行を決断できない組織がある．特に社員や職員が数千人いる組織では，ホワイトリストの作成に時間がかかるため，遮断を諦める組織もある．結果として，侵害に気付いた機器を排除するという対症療法を延々と繰り返すことになる．少なくとも，流出した場合の影響が大きい情報を保持しているシステム，停止等が発生した場合に影響が大きいシステム等を洗い出した上で，それらを組織内ネットワークから物理的または論理的に分離するという対処が望まれる．本来信頼できるはずの組織内ネットワークは攻撃者グループに侵害されている前提として，真に守るべきシステムのみを確実に守るという対処である．暫定的対処ではあるが，この対処で生じる時間的かつリソース的余裕を有効に利用して，本格的な対策に繋げることが重要である．

4.3　収集ステップ：攻撃手法を確認するログが記録されていない問題と対処

Windows OSのPCで生じる事象の多くはイベントログと呼ばれるログに記録されている．イベントログは指定したサイズのログファイルとなっており，指定したサイズを超えると過去のログから上書きで消えていく仕様となっている．ログがどれくらい残っているかはPCの利用状況や環境次第であるため，数カ月残っていることもあれば数時間しか残っていないという状況もある．インシデント発生後では上書きで消えたログにアクセスできないため，事前に自組織のPCでどの程度のイベントログが保持されているのか確認し，サイズの指定を変更しておくことが重要である．

4.4　排除ステップ：侵害範囲を確認できる機器がない問題と対処

インターネットとの境界に設置されている機器がルータだけで，ファイアウォールやプロキシサーバがないというネットワーク構成のケースがある．侵害範囲が特定できないだけでなく，ホワイトリストでの遮断もできないという問題が発生する．このような場合には，緊急で次世代型ファイアウォールやプロキシサーバを構築して導入するという対処を行い，通信遮断の制御だけでなく，通信のログの取得，分析を行う対処が必要となる．対策ステップにおいて，これらの機器の導入の検討は必須であるため，初動対応フェーズにおいてこれらの機器の導入を先んじて実施しても，対策ステップで無駄になることはない．初動対応フェーズはスピードが重要であるため，機器の調達が間に合わないケースが多い．付き合いのある業者が保有している検証用の機器なども活用し，即時に導入することが重要である．

4.5　排除ステップ：機器の総入れ替えの問題と対処

社員や職員が数十名の組織では，組織内システムの機器を総入れ替えする方が，収集および排除をするよりもコスト的に有利で内部の侵害排除を確実にすることができるケースがある．一見よいことばかりに見えるこの対応の問題点は，その後の対策や監視とセットで実施しない場合，総入れ替えした翌日に社員や職員が標的型メールの添付ファイルを開いて侵害が再開する可能性がある点である．侵害が確認される度にシステムを総入れ替えするとコストもかかるため，適切な対策や監視と同時に入れ替えを実施できるようにタイミングを図ることが重要である．

5. おわりに

高度標的型攻撃の脅威では，攻撃者グループの方が自組織のシステムやネットワークに精通しているという状況もあり得る．そのため，あらゆる可能性を排除せず，過去の経験のみにとらわれず，確認できた事実に基づいて臨機応変に対処することが重要である．

参考文献

1）特定非営利活動法人デジタル・フォレンジック研究会 （2017） ：証拠保全ガイドライン 第6 版 ， https://digitalforensic.jp/wp-content/uploads/2017/05/idf-guideline-6-20170509.pdf
2）Hutchins, E. M. Cloppert, M. J. and Amin, R. M. ：Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains （ 2015 ） . https://www.lockheedmartin.com/content/dam/lockheed/data/corporate/documents/LM-White-Paper-Intel-Driven-Defense.pdf
3）総務省 （2017） ：サイバー攻撃（標的型攻撃）対策防御モデルの解説, http://www.soumu.go.jp/main_content/000495298.pdf
4）（独）情報処理推進機構 （2014） ：「高度標的型攻撃」対策に向けたシステム設計ガイド, https://www.ipa.go.jp/files/000046236.pdf
5）サイバーセキュリティ対策推進会議（2016）：高度サイバー攻撃対処のためのリスク評価等のガイドライン,https://www.nisc.go.jp/active/general/pdf/riskguide.pdf

脚注

☆1 https://www.ipa.go.jp/security/vuln/index.html
☆2 https://www.nenkin.go.jp/files/kuUK4cuR6MEN2.pdf
☆3 https://www.jtbcorp.jp/jp/160824.html
☆4 https://www.lac.co.jp/service/consulting/cyber119.html
☆5 （独）情報処理推進機構も高度標的型攻撃を定義している［4］．情報セキュリティ対策推進会議では，高度サイバー攻撃という用語を定義している［5］．

内田 法道（非会員）norimiti@lac.co.jp
1999年 （株）ラック入社．現在 サイバー救急センター長としてインシデント対応に従事．

投稿受付：2018年2月15日
採録決定：2018年3月31日
編集担当：平井 千秋（（株）日立製作所）