資料7

２０１１年度補完調査

２０１２年９月27日

内閣官房 情報セキュリティセンター
（NISC）

Ⅰ.補完調査とは

補完調査は、「重要インフラの情報セキュリティ対策に係る第2次行動計画」の評価の一環としてIT障害等の事例を調査し、評価に必要となる補完的な情報を収集するため毎年実施しているもの。

Ⅱ.検証対象とした事例の概要

本年の補完調査の対象事案は、以下の2つとした。

① クラウド・サービスで同時に多数の利用者のサービスレベルが低下した事例

② 携帯電話サービスで、重要な通信設備に不正プログラムがインストールされたことを原因として大規模な通信障害が発生した事例

Ⅲ.事案

事案①クラウド・サービスにおける障害

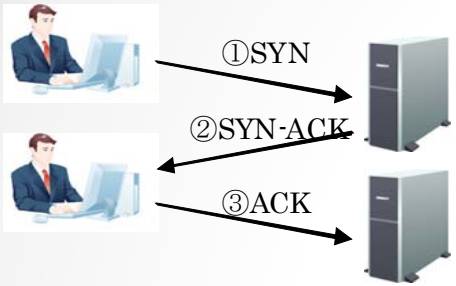
概要

地方公共団体向けの電子申請に関するSaaSサービス（利用している自治体数は217県市町村）を提供しているサーバーがSYNflood攻撃の可能性がある異常なパケットを受け、当該サービスを利用する全ての自治体の電子申請サービスにアクセスしづらい状態になった。次ページ以降の資料1で「SYNflood攻撃の類型」、資料2で「当事案の障害発生から収束までの推移」、資料3で「当事案における障害発生の概要」を説明する。

資料1：SYNflood攻撃の類型

1. 通常の接続

クライアントからの接続では以下のような手順で通信が行われます。



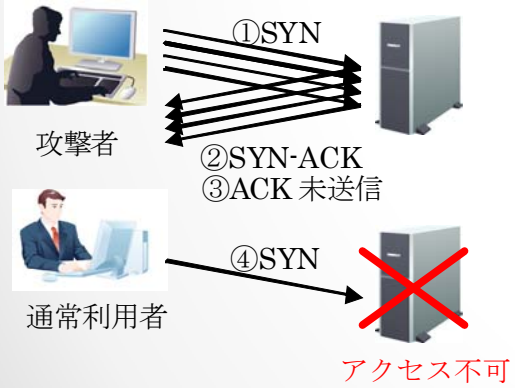
①クライアントからサーバに対してSYNパケットを送信します。

②サーバはクライアントの接続を許可するSYN-ACKパケットを送信します。

③SYN-ACKを受け取ったクライアントはACKパケットを送信し通信を開始します。

2. SYN flood攻撃時

SYN floodは、サーバ側に大量の①SYNパケットを送信した後、②SYN-ACKパケットを無視し、③ACKの操作を意図的に行わない攻撃です。通常、攻撃者の所在を隠す意味と②SYN-ACKパケットを受信しないため、①SYNパケット送信時に他人のIPアドレスを使用（偽装）します。



①悪意ある攻撃者が大量のSYNパケットを送信します。

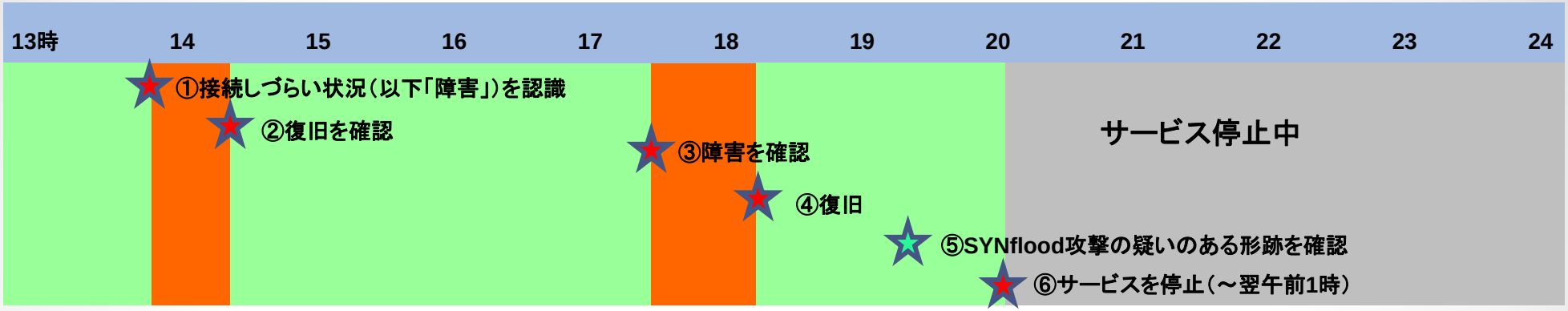
②サーバはSYN-ACKパケットを送信します。

③攻撃者はSYN-ACKパケットを無視し、放置します。

④サーバはクライアントからのACKパケットを一定時間待ち続けます。

この間、クライアントの情報を保持し続けるため大量のパケットが送信された場合、メモリを使い果たし正常なTCP要求も受け付けられなくなります。

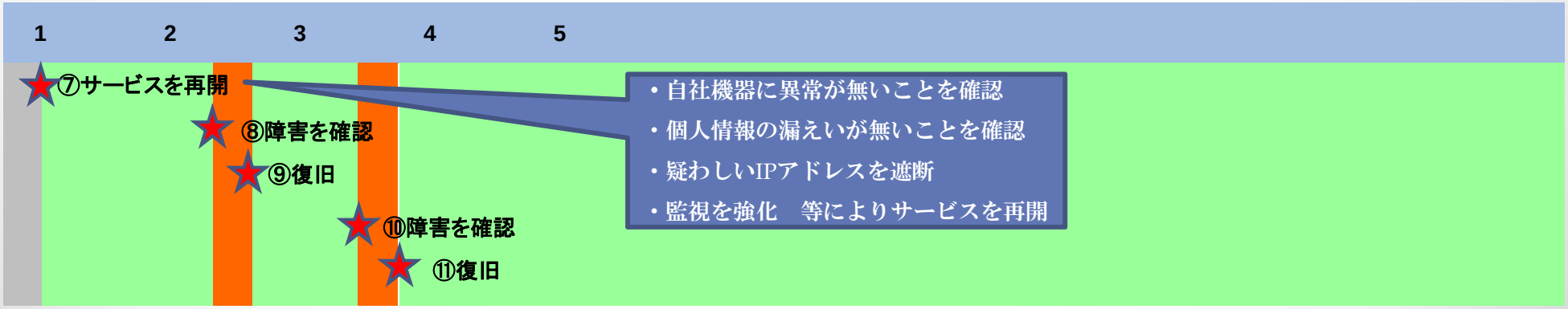
資料2：当事案の障害発生から収束までの推移



①利用者である自治体からの連絡でサービスのポータルに繋がりづらい状況にあることを認識、②の時点で自然に復旧したことを確認。

③～④にかけても障害が発生。

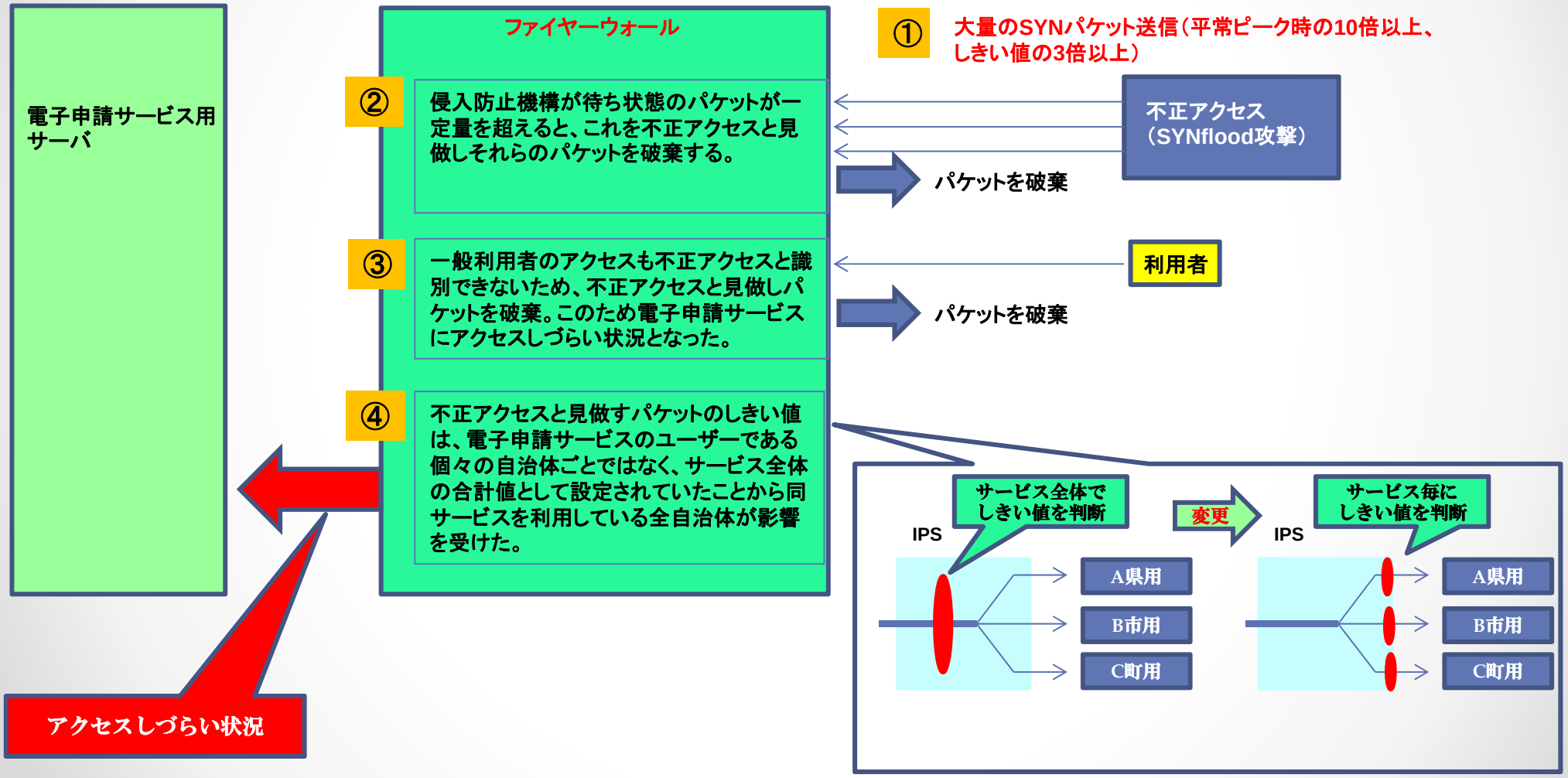
⑤の時点で原因が外部からのSYNFlood攻撃の可能性を考え、⑥でサービスを停止。



日が変わり⑦の時点でサービスを再開し、⑧～⑨、⑩～⑪にかけて2度の障害発生を確認したが、それ以降障害は確認されていない。

資料3：当事案における障害発生の概要

この案件では、侵入防止機能（IPS)がSYNパケット受信の「しきい値」を超過したことを検知し、不正アクセスと見なして利用者からのものを含めてパケットを廃棄したため電子申請サービスにアクセスしづらい状況となった。



問題点と対策

調査対象事業者は、この事案に関して以下のような問題意識を持ち改善策を実施している。

（1）侵入防止機能（IPS)における異常判断の境目となる「しきい値」の再設計

「しきい値」は、システムのキャパシティと業務特性を踏まえ個々のシステムで設定すべきものである。本事案においても過去のアクセス実績やサービスレベルにおける保証性能値等から、一定期間に アクセスが集中した場合であってもサービスを利用できるように設計していた。

しかしながら事象発生時は、定常運用時の10倍超、「しきい値」の3倍の異常な数のパケットを受信したことによりアクセスがしづらい状況が発生した。

このような状況下でサービスを受けている全ての自治体に影響が出たのは、IPSの「しきい値」の設定をサービス全体に設定していたことが原因の一つとなった。このため「しきい値」の設定をサービス全体から個々の自治体向けのサービスを担当するサーバーごとに変更した。

また、今回の事案における異常なパケット量は一般的なDDoS攻撃に比較して小規模であったと認識している。

「しきい値」は、異常を検知するための指標であり内部の機器の保護を目的にパケット破棄を開始するタイミングを定義するものである。よって、この設定のみで攻撃を回避あるいは通常サービスの継続を実現できるものではない。

このことから「しきい値」の大小問題ではなく、事象を検知した後に、どのような対策を実施するかが重要である。

これに対しては、以下の運用面での対応も合わせて行うよう運用ルールの見直しを行った。

①攻撃元のIPアドレスが特定できた場合は、その発信元を遮断

②攻撃元のIPアドレスが特定できないが、システムとして許容できるパケット量の場合、IPSの「しきい値」を変更

③上記のいずれも対策を取れないか、あるいは攻撃の規模が大きすぎて規模を想定することができない場合は、攻撃先となっているIPアドレスを遮断。この場合には攻撃先（特定の自治体）のサービスは停止することとなる。

（2）セキュリティ監査の強化

従来から定期的に行っていたセキュリティ監査に加え、別の事業者、別のアプローチによる監査を実施。

（3）障害の所在特定のための手順の改善

この案件では、当初原因として内部機器の故障や設定の誤りを疑ったことから、SYNflood攻撃の可能性を検知するまで5時間以上かかっている。このため、どのような問題が生じているかを判断するために、次のような障害対応手順を定めた。

種類	不正アクセス、サーバー踏み台、サービス妨害（DoS攻撃等）	ウィルス感染	ホームページ等の改ざん	情報漏洩、データ改ざん、サーバ不正侵入
判定基準	IPS機能のログの内容から判断	ウィルス対策ソフトのログの内容から判断	改ざん検知ソフトのログの内容から判断	サーバのログイン認証ログの内容から判断
発生箇所・影響	ログに出力されるグルーバルIP単位で発生箇所、影響範囲を判断	対象サーバ毎に改ざん箇所、影響範囲を判断	対象サーバ毎に改ざん箇所、影響範囲を判断	対象サーバ毎に問題箇所、影響範囲を判断

（4）サービス利用自治体への連絡

サービスを停止した時間がヘルプデスクの運用時間外であったことや、一時に多数のサービス利用自治体へ連絡を行う必要があったこと等からスムーズな連絡が行えなかった。このため連絡体制の整備を行った。

教訓

この案件は、障害の原因特定に時間を要したこと、その影響が各ユーザーに提供されるサービスのリソースを共有するクラウド型の性質上、多数のユーザーに同時に影響が出たことが特徴である。

クラウド型のサービスには、ユーザー毎にリソースが明確に区分される従来型のオンプレミス型のオンライン・サービスには無い要素が存在することが想定されるため、サービス提供者、利用者双方が従来から取られていた安全な運営のための対策に加え、クラウド型サービス固有の要素を把握し、適切な対処方法を定めておくことに留意することが肝要と思われる。

これらの対処について、以下に例示するように関連省庁その他の団体からガイドライン等が公表されているので参考とされたい。

経済産業省 「クラウドサービスの利用のための情報セキュリティマネジメントガイドライン」

http://www.meti.go.jp/press/2011/04/20110401001/20110401001.html

総務省 「地方公共団体におけるASP・SaaS導入活用ガイドライン」

http://www.soumu.go.jp/main_content/000061022.pdf

事案②　携帯電話会社内部の者が、不正プログラムを用いて携帯電話サービスに障害を与えた事案

概要

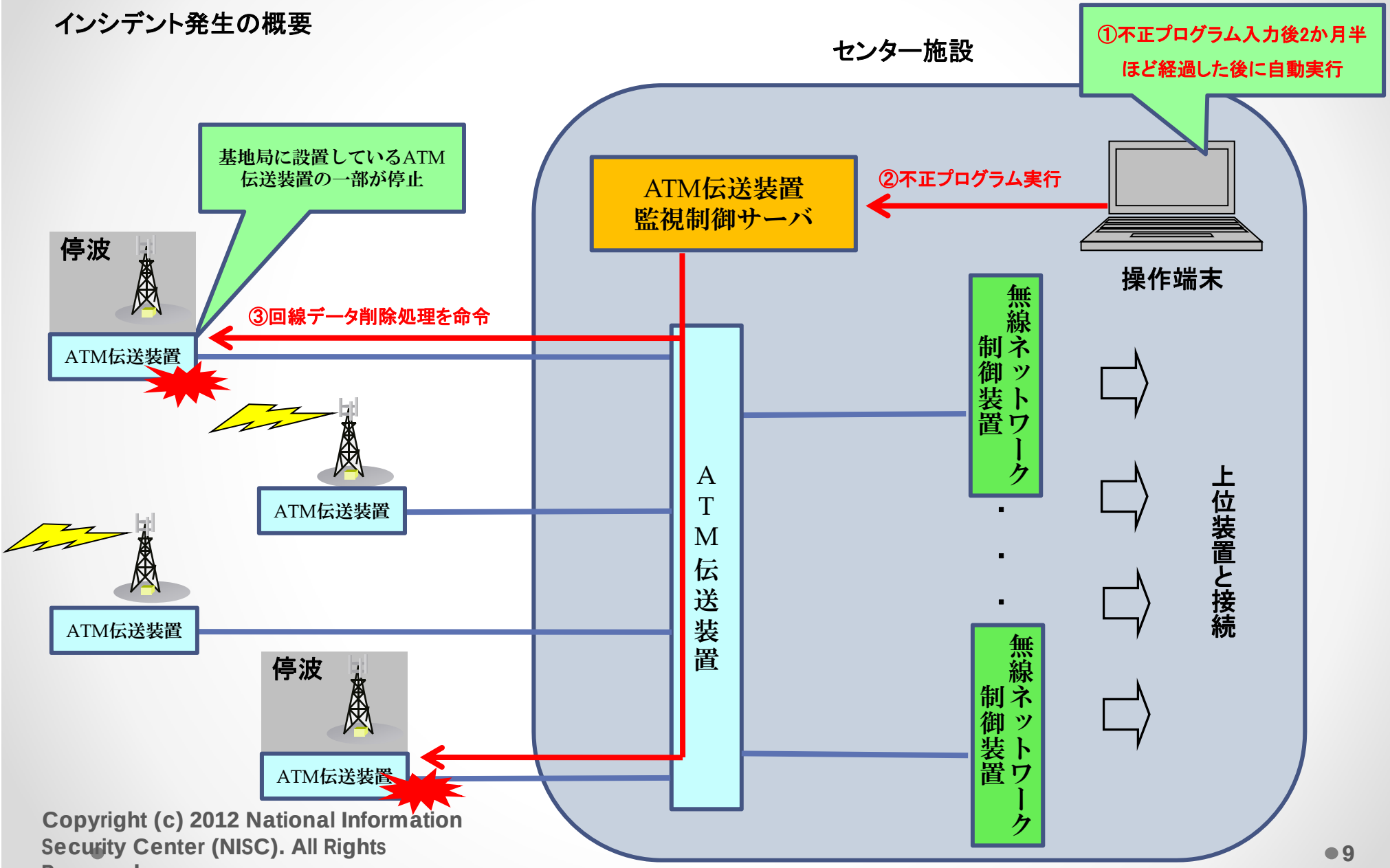
5府県の基地局に設置するATM伝送装置（注１）の内部データに破損が生じ多数の基地局が停波したことから携帯電話サービスが利用しづらい状況が生じた。

原因は 携帯電話サービス会社の通信センター施設内において、当該会社の業務委託先の社員がATM伝送装置を監視制御するサーバーの操作端末を経由して不正プログラムを入力、当該不正プログラムが入力後2か月半ほどの時間が経過してから各ATM伝送装置に対して回線データを削除処理を実行したことで、当該施設と各基地局間の通信ができなくなり、多数の基地局が停波する事態となった。（次ページの図を参照）

各基地局の復旧に時間を要したことから障害が発生したエリアにおいて携帯電話サービスが最大30時間程度利用しづらい状況となった。原因の特定は、不正プログラムを実行した端末のログ解析等により比較的早期に特定することが出来た。

（注1）非同期転送モードにより基地局とセンター施設との間の通信を行う装置

インシデント発生の概要



問題点と対策

この案件は、セキュリティ環境を承知している広義の内部の者が、重要なシステムに不正プログラムを入力 したことが原因であることから、当該企業は同様の職務に対する監視強化を主体とした以下の対策を行った。

①不正行為の発見、作業員への牽制のため、操作履歴の収集対象となる端末の範囲を拡大。

②不正プログラムが外部から持ち込まれたことにより今回の障害が起こされたことから、全ての操作端末を記憶媒体を持たないシンクライアントに置き換え。

③作業者による不正行為防止の抑止力強化を目的として、各操作端末の操作者を視認できるように監視カメラの設置台数を全国で4倍超に増加。

④作業者による不正行為防止の抑止力強化を目的として、作業者が担当業務以外のシステムへアクセスすることを防止するため、アカウント管理を個人認証に加えて担当業務を結びつけるように強化。

教訓

この案件では、不正操作に利用された操作端末のログの解析がスムーズな原因解明の端緒となった。インシデント発生後に取られた対策も監視体制の強化によって不正行為への抑止力とすることを主体としたものであり、重要インフラ・サービスの提供において適切なセキュリティ対策を維持することに加え、問題発生時の的確、迅速な対応に資する諸記録の保存と分析を行える体制を持つことが肝要と思われる。