2D-4

セキュリティ情報センターの開発[1]

榊原裕之[2]　藤井誠司[3]　中野初美[4]　牛田亘一[5]

三菱電機株式会社　情報技術総合研究所[6]　社会ｅソリューション事業所[7]

１．はじめに

近年，ソフトウェアの脆弱性を悪用したコンピュータシステムへの不正アクセスが増加している。シグネチャベースの NIDS(Network based Intrusion Detection System)は有効な対策の一つであるが，次々と発見される脆弱性を悪用する攻撃に対応するため，シグネチャの迅速な開発が課題となる。そこで，当課題を解決するためにインターネット上で公開されている脆弱性情報を効率良く収集・選定・分析し，信頼性のあるシグネチャを開発・配布するセキュリティ情報センターを組織した。本稿では、当センターの作業内容と実現する為の機能の開発について概要を発表する。

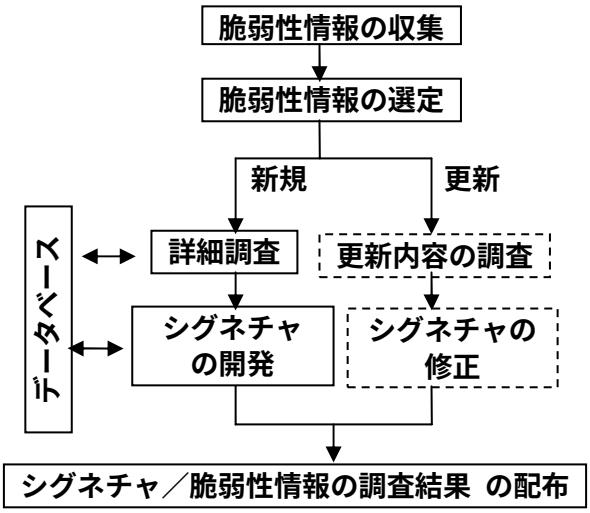

図１　セキュリティ情報センターの作業

２．セキュリティ情報センターの役割と処理

セキュリティ情報センターは NIDS 用シグネチャを開発するための組織であるが，主な作業の流れを図１に示す。まず，最新の脆弱性情報の収集を行い，防御対象のシステム向けのシグネチャを開発するために調査対象の脆弱性情報を選定する。続けて脆弱性の特徴／再現性／対策等の詳細調査を行う。さらに，調査結果を元にシグネチャを開発する。最後に利用者向けに脆弱性情報の調査結果とシグネチャを配布する。また，既に調査した脆弱性情報について更新が発生した場合は更新内容の調査とシグネチャの修正を行い再配布する。

２．１　脆弱性情報の収集

シグネチャの開発にあたり，現在発生している脆弱性の情報を収集・調査することは必須の作業である。また，調査結果によってはシグネチャが開発できないことがあり，パッチの適用／設定の変更／製品の変更等の代替手段による対処が必要となるため，代替手段の検討も踏まえ幅広く情報を収集することが重要である。

脆弱性情報のソースは Internet 上の脆弱性情報の提供 Web サイト及びメーリングリスト等を利用する[1][2]。提供情報はサイト毎に特徴があり，例えば、“脆弱性の影響を受ける製品のバージョンについて詳細である”，或いは，“広く普及している製品に関する情報の網羅性が高い”等，特徴が異なる。従って，脆弱性情報を正確に把握するために複数のサイトから収集を行う。収集した情報から，概要，詳細，攻撃の種類，脆弱性の存在する／しないバージョン，パッチ等の対処情報，攻撃コードに関する情報，参照先などの項目を抽出し，一時的に保存する。

２．２　脆弱性情報の選定

収集した脆弱性情報には，影響を受ける対象が主要 OS／Web サーバ／ブラウザなど一般的に利用者が多い重要なソフトウェアから，利用者の少ないゲーム等まで，様々な情報が含まれている。また，不正なプログラムが実行される等，危険性の高いものから，機密度の低いシステム情報が漏洩される等，危険性の低いものまで様々である。従って，多種多様な脆弱性情報から NIDS で対処すべき重要な情報を選択することが必要となる。また，シグネチャを効率よく開発するためには対処する脆弱性情報の優先度付けが必要となる。

そこで，当作業では，最初に広く普及しているソフトウェア製品に関する脆弱性情報を選択し，次に選択された脆弱性に関して，優先度付けを行うこととした。優先度付けは，危険性，攻撃の種別，攻撃コードの有無等から、システムへの影響の度合と予想される攻撃の出現時期を踏まえて総合的に判断する。

なお，情報の収集段階では複数のサイトから収集を行うが，選定段階においては，収集した情報の中で，“広く普及している製品に関して網羅性

[1] Development of a Security Information Center
[2] Hiroyuki Sakakibara, [3] Seiji Fujii,
[4] Hatsumi Nakano, [5] Kouichi Ushida
[6] Mitsubishi Electric Corporation, INFORMATION TECHNOLOGY R&D CENTER, [7] PUBLIC-USE e-SOLUTION CENTER

が高いサイトからの情報”に対して選択と優先度付けを行う。これにより，広く普及している製品に対する脆弱性情報の取りこぼしを無くす。

２．３　脆弱性情報の詳細調査

選択・優先度付けを行った脆弱性情報に対して詳細調査・分析を行う。２．１において複数サイトから収集した脆弱性情報から，関連する情報を検索し脆弱性の性質を確認するために参照する。再現性を確認するためローカルな試験環境を構築し，収集した情報に記述されている脆弱性が発現する環境を構築する（図２）。脆弱性が存在する攻撃対象 PC に対して，脆弱性再現プログラムを設定した攻撃者 PC から攻撃を実行し，指摘される脆弱性が攻撃対象 PC において再現することを確認する。例えば，データベースの情報の漏洩やソフトウェアのフリーズ等である。脆弱性再現プログラムは，公開されている攻撃コードや脆弱性情報の調査・分析から判断された攻撃手法に基づき開発する。

脆弱性の再現の確認作業を通じ、NIDS で攻撃を検知するための検知条件を検討する。脆弱性が再現した場合は攻撃対象 PC へ送信されたパケットを採取し攻撃コードとしてシグネチャ開発のための参考情報とする。また、脆弱性の再現が不可能である場合も，調査・分析に基づき検知条件を検討する。

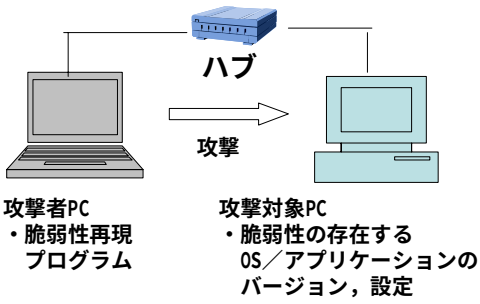

図２　脆弱性の再現環境

さらに，脆弱性への対策の有効性を検証する。パッチが提供されている場合はパッチ適用後の状態において脆弱性が再現しないことを確認する。同様に，脆弱性の存在しないバージョンの使用，設定による回避等，収集した脆弱性情報を参考に対策の有効性を検証し整理する。

２．４　シグネチャの開発

脆弱性情報の調査・分析結果に基づき，検知条件に合ったシグネチャを作成する。当社製 NIDS 用のシグネチャを開発し，動作を確認した後，脆弱性情報の調査・分析結果と共にデータベースに登録する。

２．５　シグネチャと調査結果の配布

データベースに蓄積したシグネチャと脆弱性情報の調査結果を NIDS の利用者に向けて配布するシステムを開発した（図３）。配布専用の Web サイトを構築し，利用者がブラウザでダウンロードする形式を採用した。セキュリティに関しては，HTTPS のサーバ認証によりサーバの認証と通信路の暗号化を行い，利用者の認証は ID／パスワードを HTTPS 上でセキュリティ情報センターへ提示することにより実現している。利用者はダウンロードした情報に基づき，NIDS へのシグネチャの適用や脆弱性の存在するソフトウェアのパッチ適用／設定の変更などの対策を行う。

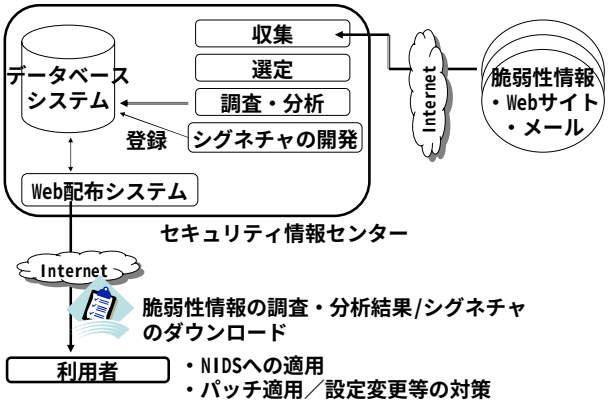

図３　シグネチャの開発と配布

２．６　脆弱性情報の更新とシグネチャの修正

既に調査した脆弱性情報が更新されることがある。例えば，新しいパターンの攻撃コードの公開や新規の影響が発現した場合である。収集された脆弱性情報が，データベースに格納されている調査済みの脆弱性情報に関する更新情報である場合は，更新内容を調査し状況によってはシグネチャを修正・追加する必要がある（図１の破線部分）。修正された情報は Web 配布システムにより再度配布する。

なお，脆弱性情報の調査・分析結果と開発したシグネチャをデータベースに登録することにより，情報の更新時の対応も含め一括管理が可能となっている。

３．おわりに

セキュリティ情報センターの役割と実現のための機能開発について概説した。現在，セキュリティ情報センターを試運転しているが，今後は脆弱性情報の関連情報の収集機能を拡張し，パッチ適用，脆弱性検査向け情報の調査も検討している。

参考文献

[1] Bugtraq, http://www.securityfocus.com
[2] Common Vulnerabilities and Exposures, http://www.cve.mitre.org