情報システムの安全を維持していただくために

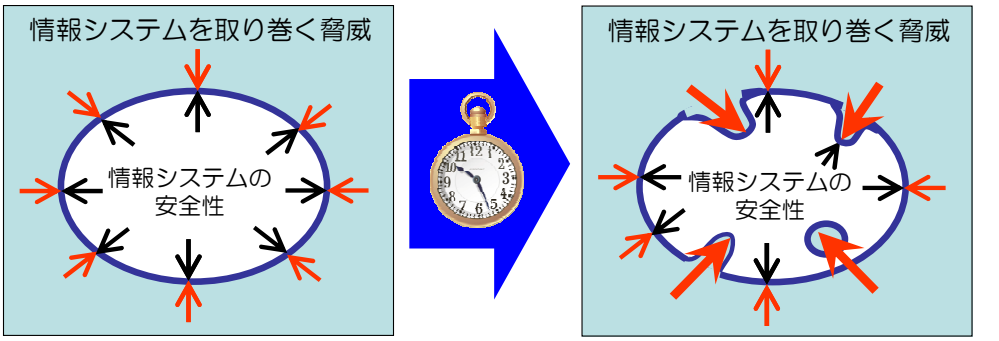
～　脆弱性（ぜいじゃくせい）対策のお願い　～

独立行政法人 情報処理推進機構
セキュリティセンター

時間が経つと情報システムの安全性は低下する

企業のビジネス活動は、様々な局面において情報システムに支えられています。コンピュータ・ソフトウェアの機能は機械のように劣化することがないため、いつまでも問題なく動くように思えます。

ところが、情報システムを取り巻く脅威は、日々変化しています。ある日突然、情報システムに対する新しい攻撃手法が開発されたり、情報セキュリティ上の「弱点」が発見されることがあります。開発時から何年間も更新されていないシステムは、そうした脅威の変化に対応できません。昨日まで安全であった情報システムが今日も安全であるとは限らないのです。



開発当初は、脅威に対して適切な対処がなされ、安全性が高い

時間が経つと脅威が変化するため、そのままでは安全性を維持できない

図　情報システムの脅威と安全性の変化

脆弱性（ぜいじゃくせい）とはなにか

攻撃者は、一般に、情報セキュリティ上の「弱点」を突いて、情報システムに侵入したり、コンピュータウイルスを感染させます。このような「弱点」は、「脆弱性（ぜいじゃくせい）」と呼ばれています。

「攻撃者など我が社とは無縁」とお考えかもしれませんが、既知の脆弱性を有するパソコンをインターネットに接続すると、わずか数十秒でコンピュータウイルスに感染すると言われており、決して他人事ではありません。

脆弱性を放置していると、大きなトラブルを招く可能性があります。ある企業では、放置していた自社サイトの脆弱性を悪用され不正侵入された結果、ユーザのメールアドレスが大量に流出した上に、サービスも停止せざるをえなくなりました。その結果、数億円規模の売上が失われ、株価も急落し、社会的信用まで失う事態に陥ったのです。

脆弱性対策が必要な理由

脆弱性は日々発見されていて、すでに数万件もの脆弱性が公表されています[1]。情報システムへの攻撃者は、まず、このような既に判明している脆弱性の悪用を試みます。したがって、情報システムを構築する際、既知の脆弱性を残してしまうことは避けなければなりません。それに、脆弱性は、ウイルス対策ソフトを使っても取り除くことができません。何度コンピュータウイルスを駆除しても、脆弱性対策を行わなければ再び感染してしまう可能性があることに留意してください。

また、情報システムを取り巻く脅威が変化すると、新たな脆弱性が発見される可能性があります。新たな脆弱性が発見されれば、攻撃者はそれを狙った攻撃ツールやコンピュータウイルスを開発します。したがって、新たな脆弱性が自社の情報システムの中にある場合には、その脆弱性を速やかに処理しなければなりません。

そのためには、自社の情報システムのソフトウェア構成（ソフトウェアの種類、バージョン、脆弱性の修正ソフトウェア（パッチ）の適用の有無等）を管理すること、脆弱性関連情報を収集すること、定期的に脆弱性検査を行うことが望まれます。もし自社での運用・保守を行うことが困難ならば、社外の情報サービス企業に委託するなどして、脆弱性対策に取り組むことをお薦めします。

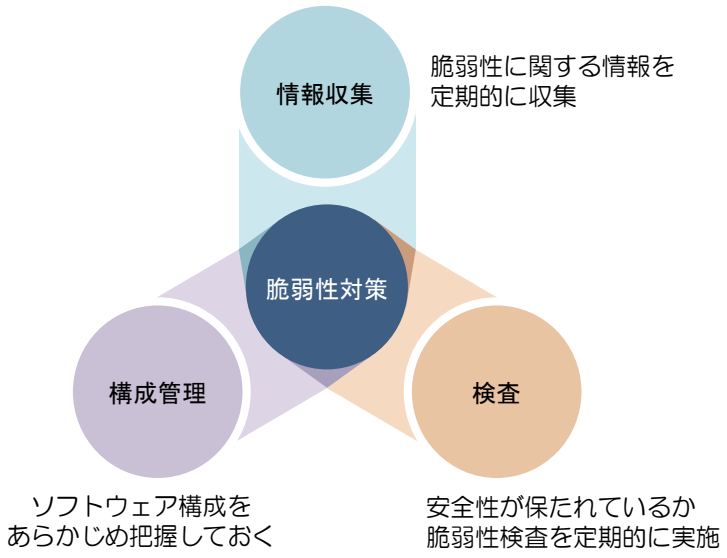


図　脆弱性対策のポイント

[1] 米NIST(National Institute of Standards and Technology)が運営するNational Vulnerability Database (http://nvd.nist.gov/)より

参考文献・URL リスト

具体的な対策については、次頁の参考文献・URL リストを参照してください。

- 「脆弱性対策情報ポータルサイト JVN（Japan Vulnerability Notes）」
  http://jvn.jp/nav/jvn.html
  日本で使用されているソフトウェアなどの脆弱性関連情報とそれに対する対策、製品開発者の対応状況を公開しているポータルサイト
- 「脆弱性対策情報データベース JVN iPedia」
  http://jvndb.jvn.jp/
  国内で利用されるソフトウェア等の製品の脆弱性対策情報を中心に収集・蓄積する脆弱性対策情報データベース
- 「知っていますか？脆弱性(ぜいじゃくせい)」
  http://www.ipa.go.jp/security/vuln/vuln_contents/
- 「安全なウェブサイトの作り方」
  http://www.ipa.go.jp/security/vuln/websecurity.html
- 「セキュア・プログラミング講座 Web アプリケーション編（新版）」
  http://www.ipa.go.jp/security/awareness/vendor/programmingv2/web.html
- 「SI 事業者における脆弱性関連情報取扱に関する体制と手順整備のためのガイダンス」
  http://www.jisa.or.jp/report/2004/vulhandling_guide.pdf

【本資料に関するお問合わせ先】

独立行政法人 情報処理推進機構
セキュリティセンター
〒113-6591
東京都文京区本駒込二丁目 28 番８号
文京グリーンコートセンターオフィス
http://www.ipa.go.jp/security/
TEL: 03-5978-7527
FAX: 03-5978-7518

名刺

２００９年 ６月８日 第１版発行
［著作・制作］情報システム等の脆弱性情報の取扱いに関する研究会
［事務局・発行］独立行政法人情報処理推進機構