■3 群（コンピュータネットワーク）－ 7 編（コンピュータネットワークセキュリティ）

7 章 セキュリティシステムの構築と運用

（執筆者：西本逸郎・黒田征太郎・関　宏介）［2009 年 3 月 受領］

■概要■

ファイアウォール，IPS で代表される，コンピュータネットワークセキュリティ上のインシデントを検知，抑制するソフトウェアやハードウェアをまとめてセキュリティシステムと呼ぶ．セキュリティシステムを効果的に利用するためには，あらかじめネットワークセキュリティ上のリスクやセキュリティシステムの運用方法を想定し，適切な要件定義を行うことが重要となる．セキュリティシステムの設計では，リスク対策のための機能設計以外にも，セキュリティシステムに障害が発生した場合の可用性設計や，様々な環境変化に柔軟に対応できるような拡張設計を行う必要がある．構築後のセキュリティシステムの運用においては，セキュリティインシデントが発生することを想定した一連の対応方法を決めておくことが望ましい．

セキュリティシステムなどで検知したセキュリティインシデントに対する一連の対応をインシデントレスポンスと呼ぶ．インシデントレスポンスは，検出，対応，事後対応の大きく三つのフェーズに分かれ，対応フェーズにおいてはフォレンジックを意識して証拠の完全性を保持する対応が望ましい．インシデントに対応する企業や組織独自のインシデントレスポンスチームを CSIRT と呼ぶ．ネットワークセキュリティ上のインシデントは伝播が早く，広範囲に及ぶため，単一組織だけのチームでは対応が難しく，CSIRT 間の連携や情報共有が重要となる．

インシデントの電子的証拠を採取する科学捜査や手法をフォレンジックと呼ぶ．電子的証拠も証拠性を保持するため物的証拠同様に適切に取り扱う必要がある．フォレンジックは民事訴訟が頻繁に起きる米国で発達してきた技術であり，日本ではまだあまりフォレンジックの考え方が浸透していないが，近年注目が高まってきている．

【本章の構成】

本章では，セキュリティシステムの構築（7-1 節），セキュリティデバイスの設定方法（7-2 節），運用時の注意事項（7-3 節），インシデントレスポンス（7-4 節），フォレンジック（7-5 節）に関して，基本的な考え方および具体的設計例などについて述べる．

■3 群 － 7 編 － 7 章

7-1 セキュリティシステムの構築

（執筆者：西本逸郎・黒田征太郎）［2009 年 3 月 受領］

インターネットやイントラネット上でサービスを提供するとき，提供するサービスは安全に利用でき，安定して稼動し続けることを要求される．サービスを安全かつ，安定して提供するためには様々なリスクに対して対策を施す必要がある．セキュリティリスクもシステムの安定稼動を阻害する要因の一つであり，サービスの設計段階からセキュリティを考慮したシステムの設計を検討する必要がある．

サービスを提供しているサーバやアプライアンス製品を役割ごとにまとめ，役割ごとに総称してシステム名で呼ぶことがある．例えば，サービスを提供するメインシステム，システムの稼動状況をチェックする監視システム，システムに対する意図的な妨害行為などを検知・抑制するセキュリティシステム，すべてのシステムの基盤となるネットワーク環境などを提供する基盤システムなど，提供するサービスによって様々なシステムがある．本章ではセキュリティ機能をもったソフトウェアやサーバ，アプライアンス製品をセキュリティデバイスと呼び，それらのセキュリティデバイスをまとめてセキュリティシステムと定義する．セキュリティシステムは，様々なセキュリティ機能をもったセキュリティデバイスを組み合わせて，セキュリティリスクからサービスにかかわるすべてのシステムを守ることを要件として設計を行う必要がある．

守る対象のシステムと，システムを構成するサーバやソフトウェアが決まれば，それらが抱えるセキュリティリスクを回避することがセキュリティシステムの要件となる．セキュリティ要件が決まることによって，構築するセキュリティシステムの具体的な構成や設定，運用方法が決まる．セキュリティシステムの構築を行うに当たり，要件を定義する際に検討すべき内容を説明する．

7-1-1 要件定義

セキュリティシステムの導入は，提供するサービスに対して発生する脅威を未然に防ぐ目的で導入する場合と，既に提供中のサービスにセキュリティ事件や事故が発生し，事件や事故の再発防止を目的として導入する場合がある．前提となる条件によって要件の検討方法や，要件を決定するまでの過程が変わってくる．

(1) サービス要件に合わせたセキュリティ対策

提供するサービスに対して発生する脅威を未然に防ぐ目的でセキュリティシステムの導入を検討している場合は，何をサービスとしてとらえ，サービスに対してどのような脅威を想定しているか考える必要がある．インターネット上で便利なコンテンツを公開することだけがサービスではなく，組織のイントラネットが常時安定した状態で利用できることや，クライアント端末を組織のセキュリティポリシーに沿って運用させることもサービスの一つとして考えることができる．システムが提供するサービスを様々な観点で検討し，サービスにとっての「異常な状態」を定義する．異常な状態を発生させ得るセキュリティ的な要因は何かを考察した結果，それらを防ぐことがセキュリティシステムの要件と定義される．

例えば，イントラネットが常時安定した状態で利用できることをサービスの正常な状態と

考えると，ネットワークの遅延や停止，イントラネット内のサーバが停止した状態がサービスにとって異常な状態と定義することができる．異常な状態を発生させ得る要因として，イントラネット内のワームの大量発生や，ファイル共有ソフトによる通信帯域の占有，サーバへの exploit 攻撃などが考えられる．セキュリティシステムにはサービスの正常な状態を維持するために，これらの脅威が発生しないようにセキュリティ的な要因を防止することや，サービスに対して脅威が発生した際に脅威からサービスを守ることが要件として定義される．

(2) 事故・事件の再発防止策

セキュリティ事件や事故の再発防止を目的としてセキュリティシステムの導入を検討する場合は，既に発生した事件や事故の内容を基に具体的な再発防止策を検討する必要がある．

最初に事件や事故が発生した経緯を整理し，細分化する．細分化した経緯に対して誰がどのような判断で行った行為なのか，システムにどのような制限や制御が実現していれば防ぐことができたのかを検討する．検討した結果から事件の原因となった行動を防ぐ機能や，事件が発生しても被害を防ぐことができる機能がセキュリティシステムの要件として定義される．また，事件や事故を基にして要件を定義する際に気を付けなくてはならない点が，原因が非常に具体的であるために対策も局所的なものになってしまう場合がある．必ずしも同じ手口で事件が発生するとは限らないため，同じ事件を防ぐ機能だけではなく類似の事件や事故が発生した場合にも防ぐことができるように要件を定義する必要がある．

7-1-2 セキュリティシステムの構成とセキュリティデバイスの選定

セキュリティシステムの要件が定義されると，次はセキュリティデバイスの選定とセキュリティシステムの構成を決める工程に入る．要件で定義されているセキュリティシステムの実現方法として，新規にセキュリティに特化したセキュリティデバイスを導入するのか，既存のサーバやアプライアンス製品の機能を利用するのか検討する．既存サーバの機能を利用する場合は，設定を変更する箇所と，変更によるサービスへの影響がないかを確認する．

新規にセキュリティデバイスを導入する場合は，要件に定義されている機能を持つソフトウェアやアプライアンス製品を選定する．一つの製品だけでは要件の実現が難しい場合は，複数のセキュリティデバイスの機能を組み合わせてセキュリティシステムの要件を実現させる．

セキュリティシステムの構成は，保護対象のシステムに求められている可用性に合わせる必要がある．場合によってはセキュリティデバイスの多重化を検討する．また，セキュリティデバイスに障害が発生することを想定し，ほかのシステムへの影響が小さくなるようにセキュリティシステムの構成を検討する．

障害が発生してセキュリティシステムが停止した場合に，サービスの安全確保を優先してサービスの提供を停止するか，安全性を犠牲にした状態でサービスを提供し続けるか決める必要がある．安全性を犠牲にする場合は，クライアントの端末にセキュリティ対策ソフトなどを導入し，可能な限りシステム全体の安全性を低下させることがないように対策を行うことが重要である．

■3 群 － 7 編 － 7 章

7-2 セキュリティデバイスの設定方法

（執筆者：西本逸郎・黒田征太郎）［2009 年 3 月 受領］

セキュリティデバイスの設定はセキュリティシステムに定義されている要件に合わせて実施する．設定を行う際はサービスの安全性を確保する機能だけではなく，セキュリティシステム自体の安全性や可用性，パフォーマンス，将来的な拡張性を考慮する必要がある．設計，設定を行う際に考慮すべき内容について説明する．

7-2-1 機能性設計と設定

セキュリティデバイスの設計と設定を行うに当たり，まず最初に設定するセキュリティデバイスがもつ機能をすべて洗い出す．要件に定義されている機能や，要件以外にもサービスの安全性や安定性の向上・維持に有効な機能，セキュリティデバイスの運用をサポートする機能など，洗い出した機能を一つずつ検討し，最終的に使用する機能を決定する．

◎ 機能の洗い出し

- 要件を満たすための機能
- 可用性向上に必要な機能
- 運用の負荷を軽減する機能
- 定期的に実施すべきメンテナンス機能
- パフォーマンスに影響を与える機能　　など

採用された機能は，更に詳細な設定値を検討していく必要がある．設定値を決定する際は設定可能な値の範囲や種類，それに伴った動作の違いを把握し，サービスにとって最適と思われる値を決定する．

構築するセキュリティシステムによっては，IDS/IPS のシグネチャやウイルス対策ソフトのパターンファイルのように設定値に関する詳細な情報が公開されていない場合も存在し，設定値や動作の違いについて検討することが難しい状況もある．このような状況では設定を行ううえでの基本的な方針を決め，設定値について入手できる情報の範囲から基本方針に沿っているかを判断し，設定値を決定する．設定を行った後は実際にセキュリティデバイスが基本方針に沿った動作をしていることを確認するために，数週間から数か月間の観察期間を設ける必要がある．観察期間中は設定値や動作について定期的に見直しを行い，要件や基本方針に合った動作を行うように設定値の最適化を行っていく．

7-2-2 可用性設計と設定

サービスを提供している間は，サービスの安全性や安定性を確保するためにセキュリティシステムも同様に安定して稼動している必要がある．そのため，セキュリティデバイスにはサービスに求められている可用性と同等の可用性が要求される．

保護対象のシステムがアクティブ・スタンバイ構成の場合は，そのシステムが切り替わったときに，セキュリティシステムも追随するかたちで切り替わるように設計し，サービスの

提供とセキュリティの確保を常時実現する．

アクティブ・スタンバイの切り替えは，サービスやセキュリティデバイスのどの障害ポイントを基準に実施するのかをあらかじめ決定しておき，サービスとセキュリティデバイスが連動して動作するように設計・設定する．また，アクティブ・スタンバイの状態が切り替わる際に，可能な限りサービスの停止が発生しないように考慮して設計・設定を行う．セキュリティデバイスの機能だけでは要求される可用性を実現できない場合は，ほかのシステムと連携して可用性を実現する方法を検討する．

あらかじめ障害を想定してセキュリティデバイスを多重化しても，想定した範囲を超えて障害が発生し，セキュリティシステムが完全に停止してしまうことがある．セキュリティシステムが完全に停止したときに，セキュリティシステムによって保護されない状態でサービスを提供し続けるフェールオープン（Fail-Open）機能を選択するのか，もしくは，保護されない状態ではサービスの提供を停止するフェイルクローズ（Fail-Close）機能を選択するのかを検討する必要がある．この設定はサービス提供に最も影響を与える設定であるため，システム的な観点だけではなく，サービス運営の観点や，サービスを利用するユーザへの影響を十分に考慮して決定する必要がある．ほかのシステムの機能を利用してある程度の安全性を確保することができるようであれば，セキュリティシステムの停止時は別システムの機能を利用し，ある程度の安全性を確保しながらサービスの提供を行うことが可能か検討することも必要である．

7-2-3 セキュリティ設計と設定

提供するサービスだけではなく，セキュリティデバイスのプログラムにも脅威が存在することも十分に考えられる．実際にセキュリティデバイスを狙った攻撃や，セキュリティデバイスのぜい弱性が公表される事例も存在する．セキュリティデバイスの停止はサービスに大きな影響を与えるため，セキュリティデバイス自体の安全性についても十分に考慮して設計する必要がある．

実際にセキュリティデバイスの設定を行うときは，セキュリティデバイスがどの程度の自衛策を取ることが可能なのか確認する．セキュリティデバイス自身で自衛策が取れない場合や，十分な機能が備わっていない場合は，ほかのセキュリティデバイスの機能を利用して脅威から保護する方法を取る．

現在はセキュリティデバイスの自衛策は軽視されがちなため，設定後はスキャンツールなどを使用して想定どおりに脅威を防ぐことができているか確認することが重要である．

7-2-4 パフォーマンス設計と設定

セキュリティデバイスを安定して稼動させるためには，負荷が一定の値以上にならないように設計や設定を実施すべきである．セキュリティデバイスの選定を行う際に，その時点で把握しているサービスの状態や状況を考慮して，最低限その時点での状況に余裕をもって耐えられるような性能をもつセキュリティデバイスを選定している必要がある．しかし，セキュリティデバイスを構築してから時間が経過していくと，セキュリティデバイスに負荷を与える要素も変化し，当初の想定よりもセキュリティデバイスにかかる負荷が増えていく場合が多い．セキュリティデバイスに負荷をかける要素について以下にいくつか例をあげる．

◎ 変化する要素

- サービスを利用するユーザ数やアクセス数
- サービスやセキュリティデバイスが使用するネットワーク帯域
- サービスで使用する保護対象のシステム台数　　など

一般的に負荷が減ることはほとんどなく，時間経過と共に負荷が増えることを想定しておく方が良い．セキュリティデバイスを構築する場合も負荷が増えていくことを前提として設計を行う．セキュリティデバイスが構築時のシステム構成と設定のままで，どの程度の負荷まで処理することができるのか，処理可能な限界値をあらかじめ設計時に確認しておく必要がある．処理限界に達する前にセキュリティデバイスの動作が不安定になるようであれば，どの程度の負荷で動作が不安定になり始めるかを把握しておく必要がある．

日々の運用ではセキュリティデバイスのリソース監視を行い，高負荷によって動作が不安定になる前にセキュリティデバイスの増設や上位機種への移行を検討し始める必要がある．急激に負荷が増加し，システムの拡張などを検討している時間がないときは，設定変更によって一時的に負荷を低下させることも検討する．パフォーマンスに関係する設定はすぐに対処できるように設定値や，設定を変更した際の影響範囲をあらかじめ確認しておき，緊急時はすぐに対処できるような準備を行う．

7-2-5 拡張性設計と設定

日々増加する負荷が構築時に想定していた基準を超え，セキュリティデバイスの処理限界に近付いてきたら，セキュリティデバイスの拡張を検討する必要がある．セキュリティデバイスの拡張方法は，負荷を増加させる様々な要素を考慮して複数案を準備することが望ましい．

また,セキュリティデバイスの構築を実施する際は,最初からシステムの拡張を考慮して,実際にシステムの拡張が行われる際に既存の構成や設定を極力変更しなくても済むように拡張性を考慮した設定を行うことが重要である．

7-3 運用時の注意事項

（執筆者：西本逸郎・黒田征太郎）［2009 年 3 月 受領］

セキュリティシステムの運用では，セキュリティデバイスが正常に動作していることを確認するだけではなく，出力されるログの解析を行い，サービスに対して発生している脅威を監視し，発生したインシデントに対して即座に対応することが重要となる．

セキュリティシステムの運用の特徴的な作業として，日々発見される様々な脅威に対応するために，頻繁にセキュリティデバイスのアップデートを行うことがあげられる．特にアップデート作業に関してはほかのシステムとは異なった運用が求められるので注意が必要である．セキュリティシステムの運用に関して，運用時に注意すべき内容を説明する．

7-3-1 監視

セキュリティシステムに必要な監視は,サービスに対して発生したインシデントの監視と,セキュリティシステムが安定して稼動していることを確認するパフォーマンスの監視，セキュリティシステムに障害が発生していないことを確認する稼動状況の監視が必要である．セキュリティシステムの監視で注意すべきインシデント監視と性能監視について説明する．

(1) インシデント監視

セキュリティシステムの運用作業の中で，最も重要な作業がインシデント監視である．発生したインシデントを短時間で解析し，誰が，いつ，何に対して，何を行ったのかを把握する．インシデントの内容が把握できたら，発生したインシデントがサービスにとってどれほど脅威となり得るのか，セキュリティシステムやほかのシステムのログから実害が発生しているのか確認を行う．

サービスの停止や個人情報の奪取など，サービスに対して実害が発生した場合は，すぐに対応できるようにあらかじめサービスが受ける被害の種類や被害範囲，被害内容に合わせた対処方法，エスカレーションフローなどを決めておき，手順に沿って迅速に対応することが非常に重要となる．

(2) 性能監視

セキュリティデバイスの負荷が処理限界に近付いてくると，インシデントを検知することができなくなったり,サービスに対して発生する脅威を防ぐことができなくなることがある．サービスの安全性を保つためにも，セキュリティデバイスのパフォーマンスを監視し，常に正常な状態で動作していることを監視することが重要である．

7-3-2 アップデート

アンチウィルス製品のパターンファイルのように，セキュリティデバイスによっては頻繁にアップデートが行われる場合がある．一般的にシステムのアップデート作業は十分な検証やリスクの分析を行ってから実施する場合が多いが，セキュリティシステムの場合は検証作業に時間を浪費することは禁物である．検証に時間をかけている間に新しい種類の脅威が発生してしまい，サービスが実害を受けたとしても誰も気付くことができないためである．

アップデートがリリースされた際の検証項目はあらかじめ決めておき，速やかに検証から

アップデート作業までを完了する必要がある．

7-3-3 ログの運用

セキュリティシステムが検知するインシデントは，ログとして可能な限り長期間保管することが望ましい．常時，インシデントの解析を行っていても，サービスに対して発生した実害を気付くことができない場合もある．時間が経過した後に実害が発生していたことに気付いた場合は，いつから被害が発生していたのか事後調査を行い，再発防止策を検討するために犯行の手口を研究する必要がある．その際には犯行の手口を確認するために長期間のインシデントの分析が必要であるため，インシデントは長期保管・管理することを要求される．

また，長期間保管したインシデントやログの解析は，事後調査だけではなく，将来的な脅威の予測にも用いられる．サービスに対する脅威も季節変動があったり，攻撃手法に流行があったりする．これらは日々のインシデント解析だけでは気付くことができない．保管したインシデントを長期間で傾向分析を行うことによって，増加傾向にある攻撃手法を見つけることもできる．傾向分析した結果から，将来的にサービスに対して発生すると思われる脅威に対して対策を練ることが必要である．

7-3-4 情報収集

情報収集はセキュリティシステムの運用の中で軽視されることが多い．しかし，情報収集を行うことによって，最新の攻撃手法を知ることができ，サービスに対して実害が発生する前に対策を検討・実施することができる．情報収集はセキュリティデバイスをより有効活用する上で非常に重要な作業なのである．セキュリティシステムの運用で有効な情報収集について説明する．

(1) 公開情報の収集

セキュリティに関する情報は公開情報でも非常に多くの情報を得ることができる．CERT や IPA では無料で情報を公開しており，様々な情報を入手することができる．また，システムで商用製品を使用している場合は，開発元が提供している情報を常に確認しておく必要がある．

情報が公開されたときにシステムに対して対処が必要なのか判断できるように，サービスで使用しているシステムの情報は整理して管理することが重要である．公開された情報を基にセキュリティシステムによる対処方法を検討し，脅威が発生する前に対処を実施することが重要だ．

(2) ハニーポットによる情報収集

公開されている情報以外に，実用的な情報収集の方法としてハニーポットを使う方法がある．実際に悪意をもったユーザが攻撃する手口を見ることは非常に有益である．実際の手口が分かると対策も立てやすい．また，公開されていない情報を入手できる場合もある．情報収集の方法として手間はかかるが，非常に有益な情報を手に入れることができる．

■3 群 － 7 編 － 7 章

7-4 インシデントレスポンス

（執筆者：西本逸郎・関　宏介）［2009 年 3 月 受領］

7-4-1 インシデントレスポンスとは

インシデントレスポンスとは,「コンピュータシステム全般にかかわるセキュリティ事件・出来事に対する，原因特定や対策などの収束に至るまでの一連の対応」を指す．インシデントには，広義的には天災・事故といった偶発的な出来事も含まれる．

7-4-2 インシデントレスポンスの要素

以降インシデントレスポンスを大きく**図 7･1** の「検出」,「対応」,「事後対応」という三つのプロセスに分けて，各プロセスの要点を解説する．各プロセスの詳細については文献 2)を参照されたい．

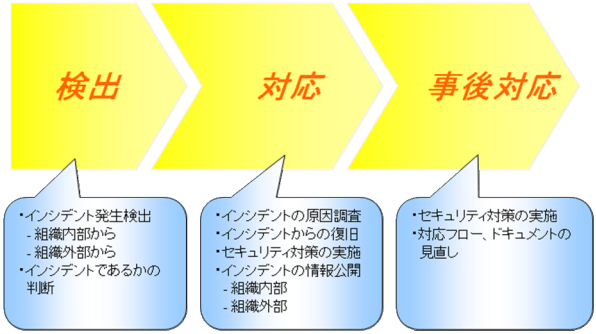

図 7・1　インシデントレスポンスのプロセス

(1)　検　出

「検出」プロセスでは，インシデントの発生（予兆を含む）を検出する役目を担う．具体的には，IDS[1]/IPS[2]やWAF[3]のアラートや，システムやネットワークの異常なログなどであるが，インシデントは組織内部で検出されるとは限らず，外部の人間（またはシステム）が検出することもある．このような場合に備え対外的に公開された連絡窓口をPOC[4]と呼ぶ．

(2)　対　応

インシデントが検出された後,「対応」プロセスに移行する．「対応」プロセスでは，インシデントレスポンス要員を召集し，影響範囲の特定・復旧・原因調査・対策を実施する役目を担う．被害範囲を最小限にするため，サービスの停止など経営層の判断が必要になることが多い．インシデントによっては，インシデントの発生ポイント以外にも影響が出ている可

[1] IDS: Intrusion Detection System（侵入検知システム）
[2] IPS: Intrusion Prevention System（侵入防止システム）
[3] WAF: Web Application Firewall（ウェブアプリケーションファイアウォール）
[4] POC: Point of Contact（連絡窓口）

能性があるため，インシデントの影響範囲を特定することが重要となる．インシデントが自組織以外にも影響する場合，適切なタイミングで情報公開を実施する．なお，被害範囲の特定や原因調査の際は，その後訴訟など法的手続きのために証拠となる情報の完全性が維持されることが重要となる．また，フォレンジック〔本章 7-5 節 参照〕の知識が要求されることがある．

(3) 事後対応

インシデントが収束したと判断したら，「事後対応」プロセスに移行する．「事後対応」プロセスでは，今後同種のインシデントの発生を防止するため，「対応」プロセスの結果をふまえて，根本的なセキュリティ対策，対応フローの見直しを実施する役目を担う．「対応」プロセスでもセキュリティ対策を実施するが，このプロセスでは根本的なセキュリティ対策を実施する．ここでのセキュリティ対策には，インシデント発生ポイントでの対策だけではなく，「検出」プロセスの見直し，コンピュータシステム全体の再構成といった点まで含める．また，実際の対応をふまえて，対応フローやインシデントレスポンス体制の見直しも実施する．

7-4-3 CSIRT (Computer Security Incident Response Team)

昨今インターネットを含むコンピュータシステムが電気・ガス・水道・交通網に代表される社会基盤の一つになり，特に企業活動には切り離せない重要なインフラとなっている．そのため，インシデントによるコンピュータシステムの停止はすなわち企業活動の停止であり，インシデントレスポンスの考え方が重要視されてきている．この背景を受けて，企業や組織独自のインシデントレスポンス専門チームである CSIRT（Computer Security Incident Response Team）を設置する機運が高まっている．

7-4-4 CSIRT 間の連係

大規模なウイルス感染やネットワーク攻撃に対抗するには，CSIRT間の連携や情報共有が重要となる．1990 年，国や組織を超えた連携のため，CSIRTの国際的な連合体FIRST[5]が形成され，2009 年 1 月 26 日現在 43 の国から 201 のCSIRTが加盟している．日本でも，2007 年 3 月にCSIRT間の密接な連携・情報交換を目的とした日本シーサート協議会[6]が設立された．

■参考文献

1) GranceTim, KentKaren, KimBrian, “コンピュータセキュリティインシデント対応ガイド,” http://www.ipa.go.jp/security/publications/nist/documents/SP800-61-J.pdf
2) Mandia Kevin, Prosise Chris, “インシデント レスポンス,” 坂井順行, 新井悠, 訳, 翔泳社, 2002.

[5] FIRST: Forum of Incident Response and Security Teams http://www.first.org/
[6] 日本シーサート協議会 http://www.nca.gr.jp/

■3 群 － 7 編 － 7 章

7-5 フォレンジック

（執筆者：西本逸郎・関　宏介）［2009 年 3 月 受領］

7-5-1 フォレンジックとは

フォレンジック（forensic）は「法医学の，科学捜査の」という意味の単語であり，情報セキュリティにおけるフォレンジックとは，すなわち「コンピュータなどの電子機器を使用した犯罪や社内規定違反を立件あるいは訴訟するために，電子的証拠を採取する科学捜査あるいはその手法」を指す．詳細については参考文献 3)を参照されたい．

7-5-2 フォレンジックの役割

コンピュータやインターネットの普及に伴い，コンピュータを対象にした，あるいはコンピュータを使用した犯罪が増えており，物的証拠だけでなく電子的証拠を重要な証拠として扱う必要が生じてきた．また，現代において企業活動とコンピュータは切り離せない存在となり，社内の規定違反を調査する際にも，書類だけなくコンピュータを調査するケースが増えてきた．

7-5-3 フォレンジックの技術要素

フォレンジックの手法は大きく分けて二つの技術要素をもつ．一つ目は，高度な科学捜査であること，もう一つは証拠性の保持である．コンピュータの調査を例に，それぞれの要素を解説する．

(1)　高度な科学調査

犯人にふき取られた血液を鑑識官がルミノール反応で浮き上がらせるように，フォレンジックにおいてもコンピュータから隠れた痕跡を様々な手法で浮き上がらせ，証拠として採取する．

コンピュータを捜査する場合，主にコンピュータのハードディスクや USB メモリなどの記憶媒体が調査対象となる．ここではハードディスクを例に，削除あるいは隠蔽した痕跡がどのようなかたちで残っているのか説明する．

ファイルをファイルシステム上に書き込む際は，セクタという細かい単位をまとめたクラスタ（アロケーションユニットとも呼ぶ）単位に書き込まれる．クラスタ単位が 4KB でフォーマットされたファイルシステムに，5KB のファイルを書き込んだ場合，2 個のクラスタ（4KB×2＝8KB 分）を使用する．クラスタサイズの関係であまった 3KB の領域をスラックスペースと呼ぶ（**図 7･2**）．

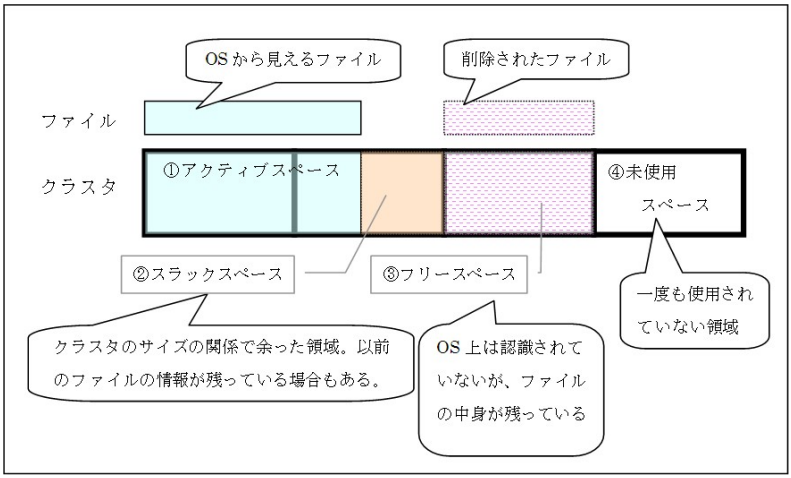

図 7・2　ファイルシステム

OS からはハードディスクに存在するファイルの情報しか確認することができないが，スラックスペースやフリースペースには，過去に存在したファイルの情報が残っている．ハードディスクを調査する際は，ログや電子メールなど，OS から見えるファイルだけではなく，OS からは見ることができないスラックスペースやフリースペースに残っている情報から痕跡を探す．多くのフォレンジック調査ツールにはこのような機能が備わっている．

(2)　証拠性の保持

犯人の指紋がついた物的証拠を法廷に提出する前に，きれいに拭いてしまったり，誰が出入りするかわからない場所に保管してあれば証拠性を失ってしまう．電子証拠も証拠性を保持するために物的証拠と同様の扱いをする必要があり，証拠が改変されておらず，なおかつどのような手順で誰が採取・保全したのか明らかにする必要がある．

証拠となるディスクに変更を加えないようハードウェア，またはソフトウェアによる書込み防止装置を使用して物理コピーを取り，更に原本と同一であることを証明するため MD5 などのハッシュを比較する方法が通常とられている．その際の調査ツールや手法は，適切な動作が証明されたものを用いることで，より調査結果に信頼性をもたせることができる．そのため，調査には商用のフォレンジック調査専用ソフトウェア・ハードウェアが一般的に使用される．

更に，調査の手順や実施時刻，作業者などの情報を詳細に取ることで，誰がいつ，どのように証拠を保全し，調査したのかを明確にし，法廷への提出に耐えうる証拠性を確保する．

7-5-4 日本におけるディジタル・フォレンジック

日本におけるディジタル・フォレンジックにはいくつか特有の問題がある．まず，マルチバイト言語圏で切っても切れない文字コードの問題がある．SJIS や EUC，更にはメールで使用されている MIME エンコードなど様々な方法で文字列が表されるため，日本語文字列を探

すときにはこれらを考慮して漏れのない検索条件を決め，更に日本語の文字コードに対応したソフトウェアを使用する必要がある．これは検索漏れが生ずる可能性があるだけでなく，数多くのパターンで検索するために英数字のみを検索する場合に比べて多くの時間がかかることを意味する．

また，フォレンジック調査の認識がまだあまり浸透していない問題もあげられる．フォレンジック調査が念頭におかれていないため，調査を始める前にウイルススキャンやリストアなどユーザの操作で意図せず証拠を消してしまう事例が見られる．米国の事情では，訴訟が念頭にあるため証拠を適切に残すようトップダウンでシステムの停止や調査が行われるようだが，日本ではシステムを止めずに調査をしてほしいとユーザが希望することが少なくない．

7-5-5 「攻め」と「守り」のフォレンジック

従来，ディジタル・フォレンジックは，企業や個人が不正アクセスなど何らかの被害を受けた場合に犯人を訴える「攻め」のフォレンジックとして使われてきた．民事訴訟が頻繁に起きる米国で発達してきた技術であり，そのため日本の一般企業ではあまり馴染みがなかったといえる．しかし近年，世界に進出する日本の企業が進出した国で訴えられるという状況を想定して，無実であることを証明するための「守り」のフォレンジックが注目されている．企業が訴えられた，あるいは不正アクセスの踏み台にされた場合に従業員を守るため，適切な証跡を残すことが重要になってきている．詳細については参考文献 1)を参照されたい．

■参考文献

1) 辻井重男監修，萩原栄幸編集責任，特定非営利活動法人デジタル・フォレンジック研究会編，“デジタルフォレンジック事典，”日科技連出版社，2006.
2) http://www.cyberpolice.go.jp/column/explanation03.html
3) http://www.cyberpolice.go.jp/column/explanation08.html