サイバーセキュリティの基本概念と脅威

要　旨

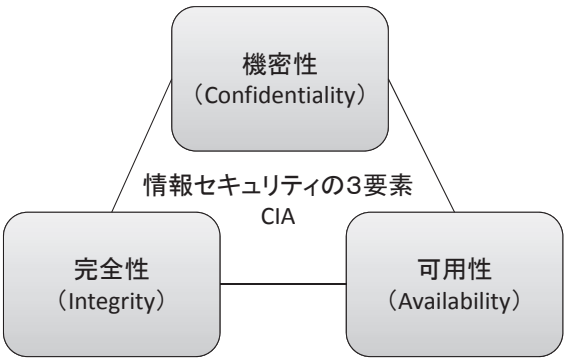
情報セキュリティとは、情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を維持することであり、それらを維持できなくなるリスクに対して、組織的、人的、技術的、物理的な情報セキュリティ対策が適切に実施される必要がある。技術的なセキュリティ対策としては、暗号技術や認証技術、アクセス制御技術などが重要である。実際のサイバー攻撃では、脆弱性を悪用し、マルウェアに感染させることで、システムやPCを乗っ取り、情報漏えいなどの機密性、完全性、可用性の3要素が維持できなくなる被害を発生させる。

I　情報セキュリティの基礎

情報セキュリティは、JIS Q 27000:2014（ISO/IEC 27000:2014）においては、情報の機密性（Confidentiality）、完全性（Integrity）、可用性（Availability）を維持することと定義されている（図1参照）。これら3つの要素の頭文字をとって情報セキュリティにおける「CIA」と略される。なお、完全性は、Completenessにも対応させられる用語であり紛らわしいため、Integrityに対応する語として、一貫性又はインテグリティが用いられることもある。

これら3つの要素はそれぞれ、①機密性：情報へのアクセス（閲覧など）が許可された場合に限定されていること、②完全性：情報への操作（書込み、書換え、消去など）が許可された場合に限定されていて改ざん等がなされないこと、③可用性：許可された者の情報へのアクセスが必要に応じて中断することなく利用・制御できることを意味しており、これらが維持できなくなる状況や可能性をセキュリティ上の脅威と見なす。例えば、機密性への脅威としては情報漏えいやなりすまし、完全性については侵入や改ざん、可用性についてはDoS/DDoS攻撃やマルウェア感染などが挙げられる。ただし「CIA」の各要素の重要度の大小は各組織が取り扱う情報や、所有する情報システムの特性により異なる。

図1　情報セキュリティの3要素



（出典）三菱総合研究所作成。

情報セキュリティ対策は、①組織的、②人的、③技術的、④物理的の4つの観点から実施さ

＊本稿におけるインターネット情報の最終アクセス日は、原則として、2015年1月13日である。

れる。セキュリティを確保するためにはそれぞれの対策が確実にかつバランスよく実施される必要がある。また、情報セキュリティ対策にはそれぞれ「抑止」「予防」「検知」「回復」等の機能がある。組織的、人的、技術的、物理的な情報セキュリティ対策と、それぞれの対策の機能を適切に使い分けたり、組み合わせたりすることで、想定する脅威に対して効果的な対策を実施することができる。例えば、不正アクセス対策であれば予防・検知、内部不正行為対策であれば抑止・検知等、システムの障害対策であれば回復の機能を高めることが特に重要となる。

II　情報セキュリティの脅威

JIS Q 27000:2014では、情報セキュリティリスクは、脅威が情報の脆弱性又は資産の脆弱性に付け込み、その結果、組織に損害を与える可能性に伴って生じるとされている。情報セキュリティ対策を実施するために、情報セキュリティのリスクアセスメントを実施する。リスクアセスメントとは、リスク特定、リスク分析及びリスク評価のプロセス全体を示す。リスク特定は、リスク源、事象、それらの原因及び起こりうる結果を特定するプロセスである。

リスクの分析及び評価は、守るべき対象である資産に発生する可能性のある脅威と、脅威の発生確率や発生した場合の影響度等を評価することである。脅威とは、表1のようにシステム又は組織に危害を与える事故の潜在的原因となるものである。

表1　ISO/IEC 27005:2008に示される脅威の種類

脅威の種類		具体的な脅威
環境的脅威		災害（地震、洪水、台風、落雷、火災など）
人為的脅威	意図的脅威	攻撃（不正侵入、ウイルス、改ざん、盗聴、なりすましなど）や盗難、破壊
	偶発的脅威	人為的ミス（紛失、操作ミス、会話からの情報漏えいなど）、障害（システム障害、ネットワーク障害など）

（出典）各種資料を基に三菱総合研究所作成。

III　脆弱性とその取扱い

一般的にサイバー攻撃には、攻撃対象が使用しているソフトウェアやハードウェア等のセキュリティ上の欠陥（セキュリティホール）や弱点である「脆弱性」が悪用されることが多い。特に、当該ソフトウェア等の開発者による修正が行われる前に脆弱性が悪用されてしまう、いわゆる「ゼロデイ攻撃」は基本的に防ぐことができないため深刻な脅威となっている。したがって「脆弱性関連情報」は、開発者による修正（修正プログラム「パッチ」の公開等）が完了するまで公にならないように慎重に取り扱われなければならない。

1　脆弱性の定義

「ソフトウェア等脆弱性関連情報取扱基準」（平成16年経済産業省告示第235号）によれば、「脆弱性」とは「ソフトウェア等において、コンピュータウイルス、コンピュータ不正アクセス等の攻撃からその機能や性能を損なう原因となりうる安全性上の問題箇所。ウェブアプリケー

ションにあっては、ウェブサイト運営者がアクセス制御機能から保護すべき情報等に誰もがアクセスできるような、安全性が欠如している状態を含む。」と定義されている。

2　脆弱性関連情報の取扱い

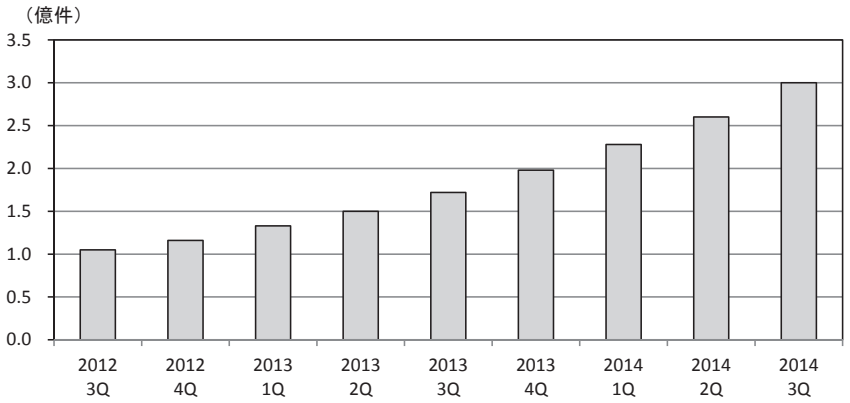
JPCERTコーディネーションセンター（JPCERT/CC）では、1996年の設立以来、米国CERT/CCや英国国家インフラ防護センター（Centre for the Protection of National Infrastructure: CPNI）及びフィンランドNCSC-FI（National Cyber Security Centre Finland）と連携し、脆弱性関連情報を安全かつ適切に取り扱ってきた。2004年7月から、「ソフトウェア等脆弱性関連情報取扱基準」に基づき制度化された「情報セキュリティ早期警戒パートナーシップ」における国内調整機関として、JPCERT/CCは、脆弱性関連情報の公表日等を当該ソフトウェア製品の開発者と調整する役割を担っている。脆弱性関連情報の報告受付機関としては、情報処理推進機構（IPA）が指定されており、JPCERT/CCがソフトウェアの開発者と調整した上で、修正完了後に、IPAとJPCERT/CCが共同で運営する脆弱性対策情報ポータルサイトJapan Vulnerability Notes（JVN）を通じて一般に公表される。

IV　ウイルス・マルウェア

マルウェア（Malware、Malicious softwareの短縮形）は、悪意のコード又は悪意のソフトウェアと呼ばれ、ユーザの同意を得ずにコンピュータ等にインストールされ（感染）、ユーザにとって有害な行為を行うプログラムの総称である。マルウェアの代表例としては、ウイルス、ワーム、トロイの木馬等があり、ほかにもバックドア、ルートキット、キーロガーや、スパイウェアとしての追跡クッキーや悪質なアドウェア（広告を表示するソフトウェアやアプリ）等もマルウェアに含まれる。

セキュリティベンダ大手のIntel Security（旧：McAfee）が公表している統計情報（図2参照）によれば、2014年第3四半期（2014年3Q）において、全世界で使われているMcAfeeのマルウェアデータベースには、約3億件のマルウェアのサンプルが登録、管理されており、前年同時期の1億7000万件から約76%増加している。これは、1分間に200件を超える脅威が新たに出現していることとなる。

図2　マルウェアデータベースへの登録サンプル数（全世界）



（＊）図中のQは、四半期を示しており、例えば1Qは、第1四半期を表す。
（出典）Intel Security「McAfee Labs脅威レポート」2014.11, p.29. <http://www.mcafee.com/jp/resources/reports/rp-quarterly-threat-q3-2014.pdf> を基に三菱総合研究所作成。

アンチウイルスソフトウェア等を販売するセキュリティベンダは独自にマルウェアの解析を行っている。セキュリティベンダは独自に配置したハニーポット（マルウェアが進入しやすいおとりサーバやネットワーク）やクローラ（ウェブサイト等を巡回してマルウェアを収集するツール）を使って、又はユーザからの提供を受けてウイルスとして疑われるファイル（検体）を収集し解析を行っている。

Ⅴ　不正アクセス・サイバー攻撃

表2に示すとおり、マルウェア感染やコンピュータ及びネットワークに対する侵入や改ざん、サービス運用妨害など、いわゆる不正アクセスやサイバー攻撃の発生件数が増えてきている。不正アクセス及びサイバー攻撃が、かつての愉快犯によるものから、金銭目的や政治的なアピールを目的としたものに変化しており、さらに昨今では国家間のサイバー戦争の様相も呈してきている。

表2　不正アクセス行為の認知件数推移（日本）

年次		2009	2010	2011	2012	2013
認知件数		2,795	1,885	889	1,251	2,951
	海外からのアクセス	40	57	110	122	289
	国内からのアクセス	2,673	1,755	678	987	2,474
	アクセス元不明	82	73	101	142	188

（出典）総務省「不正アクセス行為の発生状況」2014.3.27, p.1. <http://www.soumu.go.jp/main_content/000280516.pdf>を基に三菱総合研究所作成。

Ⅵ　標的型攻撃

特定の企業や組織を狙った標的型攻撃は、大企業や官公庁のみならず、中小企業も対象とされているが、対象が限定的であるために対策が極めて難しく、被害が国内外で続発している。その一方で、政府や民間の取組が進んでいる。

具体的な手口としては、取引先などの関係する実在の人物や組織を騙った電子メールを、受信者が関心を持つような件名や内容で送り付けることによって、受信者が添付されたファイルを開いたり、メール本文中に記載されたURLにアクセスしたりすることで、マルウェアに感染させるというものである(1)。このように、標的型攻撃においては、必ずしも技術的に高度な手法が用いられるのではなく、人間の恐怖や好奇心といった心理的な隙や行動のミスに付け込み、人間の心理を悪用する手法である「ソーシャルエンジニアリング」が用いられる場合もある。近年では手口がより巧妙となってきており、成功するまで粘り強く攻撃し続ける、いわゆる「APT（Advanced Persistent Threat）攻撃」や、何度かのやり取りを繰り返して相手を信用させた後に、マルウェアに感染させるファイルを送り付けるという「やり取り型攻撃」、攻撃対象

(1)「あなたを狙う「標的型攻撃メール」「フィッシングメール」被害防止には一人一人の情報セキュリティ対策が重要です」2014.3.3. 政府広報オンラインウェブサイト <http://www.gov-online.go.jp/useful/article/201202/3.html>

が頻繁に閲覧する正規のウェブサイトを改ざんしてマルウェアに感染させる「水飲み場型攻撃」などが発生している。

Ⅶ　重要インフラに対する攻撃

電力、水道、通信、金融、交通といった国民生活及び社会経済活動に多大な影響を及ぼすおそれのある重要インフラへのサイバー攻撃のリスクが高まっている。国内では、情報セキュリティ政策会議が、重要インフラ防護に責任を有する政府と自主的な取組を進める重要インフラ事業者等との共通の行動計画として、2014年5月に「重要インフラの情報セキュリティ対策に係る第3次行動計画」を公表している。同計画では、重要インフラ分野として情報通信、金融、航空、鉄道、電力、ガス、政府・行政サービス、医療、水道、物流、クレジット、石油、化学の13分野を指定し、「安全基準等の整備及び浸透」、「情報共有体制の強化」、「障害対応体制の強化」、「リスクマネジメント」、「防護基盤の強化」の5つの施策群を掲げている(2)。

Ⅷ　情報セキュリティの対策技術

情報セキュリティマネジメント（Information Security Management System: ISMS）を規定するISO/IEC 27001:2013の附属書Aには、A.5～A.18の14項目に31の管理目的及び114の管理策が記載されている。これらはISMSの確立プロセスにおけるリスク対応として適切な管理目的及び管理策を選択するためのものである。組織は必要に応じて追加管理目的及び管理策を選択することもできる。

情報セキュリティ対策は、①組織的、②人的、③技術的、④物理的の4つの観点から実施される。ISO/IEC 27005:2011には、情報セキュリティに対する対策が整理されており、情報資産の重要度やポリシーにしたがって、具体的な対策技術を選んでいく方法が現実的である。図3は、図中上段に示された脅威に対する対策技術の例を具体的に示したものである。

(2)　情報セキュリティ政策会議「重要インフラの情報セキュリティ対策に係る第3次行動計画」2014.5.19, pp.8-10. <http://www.nisc.go.jp/active/infra/pdf/infra_rt3.pdf>

図3　セキュリティ管理策の全体像

<table>
<tr><td colspan="2"></td><td colspan="7">脅威（＊1）</td></tr>
<tr><td colspan="2"></td><td>不正利用
なりすまし</td><td>不正アクセス
不正侵入</td><td>ウイルス
（検疫・駆除）</td><td>改ざん
書き換え</td><td>盗聴</td><td>情報漏えい</td><td>サービス妨害
（＊2）</td></tr>
<tr><td rowspan="3">人的
組織的</td><td rowspan="3">セキュリティ
全般</td><td colspan="7">情報セキュリティポリシー（リスク分析・セキュリティ基本方針・対策基準・実施手順）</td></tr>
<tr><td colspan="7">対策ベンチマーク/情報セキュリティマネジメントシステム（ISMS）の導入/情報漏えい防止強化対策</td></tr>
<tr><td colspan="7">セキュリティ診断/侵入テスト/監査（内部・外部）/教育</td></tr>
<tr><td rowspan="10">技術的</td><td rowspan="3">ネットワーク・
セキュリティ</td><td colspan="4">侵入検知システム（IDS）/ 侵入防止システム（IPS）</td><td colspan="2">通信暗号化
（IPsec/IP-VPN）</td><td rowspan="2">DoS/ DDoS対応
（フィルタリング）</td></tr>
<tr><td colspan="6">ファイアウォール（パケット・フィルタリング）</td></tr>
<tr><td>デジタル署名</td><td colspan="3">アクセス制御/デバイス認証</td><td colspan="2">WLAN（認証・暗号化）</td><td>Fake AP</td></tr>
<tr><td rowspan="4">クライアント・
セキュリティ</td><td colspan="7">セキュリティパッチ/フィッシング対応/URLフィルタリング</td></tr>
<tr><td>個人認証</td><td>パーソナルファイア
ウォール</td><td rowspan="2">ウイルス駆除</td><td rowspan="2">ファイル
暗号化</td><td>スパイウェア/アドウェア対応</td><td></td><td>spamメール
対応</td></tr>
<tr><td colspan="2">PC認証</td><td>メディア管理/プリンタ制限</td><td></td><td></td></tr>
<tr><td colspan="5">検疫ネットワーク/シンクライアント化/シンクライアントの導入</td><td></td><td></td></tr>
<tr><td rowspan="3">サーバー・
セキュリティ</td><td colspan="2">ユーザ認証</td><td colspan="3">アクセス制御/権限管理</td><td>バックアップ</td><td>負荷分散</td></tr>
<tr><td colspan="4">セキュリティ・パッチ（適用・逐次更新）・セキュアなWeb開発</td><td rowspan="2">ログ管理</td><td>メール・MSG
スキャン</td><td rowspan="2">DoS/ DDoS
対応
（パケット制限）</td></tr>
<tr><td colspan="2">Trusted OS/Secure OS</td><td>ウイルス駆除</td><td>改ざん検知・
防止</td><td>DBMS暗号化</td></tr>
<tr><td>物理的
環境的</td><td>セキュアな
環境・施設・
オフィス</td><td colspan="7">セキュア・ゾーニング、セキュア・オフィス・施設・設備・什器
（入退出管理、監視カメラ、バイオメトリクス認証/盗難・紛失防止備品）</td></tr>
</table>

（＊1）　各脅威に対する対策技術の例を具体的に示している。
（＊2）　マシンの処理量や通信量を増加させたり、ソフトウェアの脆弱性や設定の不備を悪用したりして、マシンの機能の低下や停止、あるいはネットワークを利用不可能な状態にすることを意図した攻撃。
（出典）「情報セキュリティマネジメントとPDCAサイクル」情報処理推進機構ウェブサイト <https://www.ipa.go.jp/security/manager/protect/pdca/risk.html>を基に三菱総合研究所作成。

情報セキュリティ対策の中から技術的な対策として、①暗号、②認証・アイデンティティ管理（図3では個人認証、PC認証に該当）、③アクセス制御、④監視（図3ではIDS/IPSに該当）、について以下に概略を示す。

1　暗号

暗号とは、鍵と呼ばれる情報が使用できるか否かにより、特定の操作（暗号文の復号、デジタル署名の生成など）が効率よく実行できるか否かを制御し、データの機密性や完全性などを達成する技術全般を指す。コンピュータや通信、インターネットサービスのセキュリティを担保するための基盤となる技術である。暗号のセキュリティは、鍵を使って行うべきことを鍵なしで行おうとすることがどれほど困難かで評価する。暗号解読の困難性を計算時間等の計算量で見積もる計算量ベースの暗号と、暗号解読の成功確率で見積もる情報量ベースの暗号がある。現在、社会で広く利用されている暗号方式は、計算量ベースの暗号である。暗号は、コンピュータの能力（解読能力、偽造能力）の向上や数学的な解読方法、偽造方法の進展などを考慮して、暗号アルゴリズムや暗号鍵の長さ（鍵長）を必要に応じて見直すことが望ましい。

(1)　政府による安全な暗号技術の選定

日本は、電子政府における調達に際して参照すべき暗号である電子政府推奨暗号の安全性を評価・監視し、暗号技術の適切な実装法・運用法を調査・検討するため、総務省と経済産業省が共同でCRYPTRECプロジェクトを実施している。CRYPTRECプロジェクトでは、表3に示す

ようなCRYPTREC暗号リスト（電子政府推奨暗号リスト、推奨候補暗号リスト及び運用監視暗号リストから構成される）を策定し、リストに掲載されている暗号アルゴリズムについて定期的に安全性の評価を行っている。

一方、米国国立標準技術研究所（National Institute of Standards and Technology: NIST）では、DES（Data Encryption Standard）に代わる暗号アルゴリズムを策定するプロジェクトを1997年に立ち上げ、公募により優れた方式を選定することとした。公募の結果、世界中から21方式の暗号方式が提案され、安全性とスピード（処理効率）の観点から最終的にはベルギーの研究者が提案したRijndael（「ラインドール」と読む。）と呼ばれる暗号アルゴリズムが米国標準暗号AESとして選定され、2001年にFIPS-197として標準化された。

表3　CRYPTREC暗号リスト

技術分類		名称
公開鍵暗号	署名	DSA
		ECDSA
		RSA-PSS
		RSASSA-PKCS1-v1_5
	守秘	RSA-OAEP
	鍵共有	DH
		ECDH
共通鍵暗号	64ビットブロック暗号	3-key Triple DES
	128ビットブロック暗号	AES
		Camellia
	ストリーム暗号	KCipher-2
ハッシュ関数		SHA-256、SHA-384、SHA-512
暗号利用モード	秘匿モード	CBC、CFB、CTR、OFB
	認証付き秘匿モード	CCM、GCM
メッセージ認証コード		CMAC
		HMAC

（出典）総務省・経済産業省「電子政府における調達のために参照すべき暗号のリスト（CRYPTREC暗号リスト）」2013.3.1, p.1. CRYPTRECウェブサイト <http://www.cryptrec.go.jp/images/cryptrec_ciphers_list_2013.pdf>を基に三菱総合研究所作成。

2　認証・アイデンティティ管理

電子メールや各種インターネットサービスを利用する際には、利用者個人を特定するためにユーザ認証が行われる。各種サービスが本人を特定するための重要な基盤となるため、IDの機密性、完全性、可用性を厳格に管理すること（アイデンティティ管理）が重要となる。現在はパスワード認証方式が一般的であるが、パスワード漏えいやパスワード類推などにより、不正利用が急増している。そのため、インターネットバンキングなどの重要なサービスでは、より強固な認証方式を導入する事例が増えている。

パスワード認証方式において、パスワードが第三者に知られてしまう原因には、類推が容易なパスワードを使ってしまうこと（例：暗証番号に0000や誕生日など）や一般にパスワードによく使われる文字列をリスト化（辞書化）して、それを使った総当たり攻撃（辞書攻撃）によって知られてしまうこともある。また、利用者が複数のサービスで使うIDとパスワードを同一のものに設定している場合に、別のサービスに不正アクセスがされてしまうケース（パスワード使い回し）が多い。インターネットバンキングなどの重要なサービスでは、パスワード生成器を用いて短時間に有効なパスワードを併用する「ワンタイム・パスワード方式」や、通常のア

カウント名とパスワードによる認証に加えて追加の情報（セキュリティコード等）を入力させる「2段階認証方式」、ICカードに組み込まれた電子証明書を用いて認証する「ICカード認証方式」などの、より強固な認証方式を導入する事例が増えている。

3　アクセス制御

アクセス制御は、個人情報や金融情報、企業の重要情報などの情報資産の機密性を確保するための技術である。情報資産の重要性に応じてアクセス制御を行う必要がある。様々な電子ファイルなどの情報資産に対して、物理的な鍵や暗証番号、ICカードなどを使って入退室管理を行う「物理的なアクセス制御」、LANやインターネット経由で適切な端末のみが通信ができる「ネットワークのアクセス制御」、サーバにアクセスする端末を識別する「サーバのアクセス制御」、電子ファイルの機密レベルに応じて利用者や利用者属性のアクセス権を付与し、適切な利用者のみが当該電子ファイルにアクセスできるようにする「電子ファイルのアクセス制御」などの各種アクセス制御を適切に行うことが重要である。

4　監視

ネットワークや各種ネットワークサービスの可用性を確保するためには、様々な方法で機器の稼働状況やユーザの利用状況を監視することが重要である。不正アクセス、不正侵入に対しては、専用のシステムである侵入検知システム（IDS）/ 侵入防止システム（IPS）などが使われている。

監視カメラなどの物理的な監視に加えて、サーバやネットワーク機器などに対する「ハードウェア監視」、「サービス監視」、「ネットワーク監視」などを組み合わせて行うことで、監視対象の異常を迅速に発見することが可能となる。

情報セキュリティは資産や情報のCIAを維持することであり、人的、組織的な対策が中心であるISMSが国際標準化されて10年が経過し、その対策は浸透しつつある。一方で、ソフトウェアの脆弱性を狙ったゼロデイ攻撃や標的型攻撃等によるマルウェアの感染被害も増大傾向にあることから、技術的な対策は十分ではない。さらに、インターネットに接続される機器が増えており、経済活動が活性化していることから、攻撃する側にとっても経済的リターンを求めて活動するケースが増えているため、常に対策の見直しが求められている。ただし、対策にかけるコストについては検討する必要があるだろう。

執筆：株式会社三菱総合研究所　情報通信政策研究本部　主任研究員　谷田部（やたべ）　智之（ともゆき）
監修：横浜国立大学大学院環境情報研究院　教授　松本（まつもと）　勉（つとむ）
奈良先端科学技術大学院大学　教授　山口（やまぐち）　英（すぐる）