「ネットワークセキュリティ関連の用語解説」出典：日経 BP 社「PCIDSS 基準」(一部、加筆)　文責：河東岩夫　　平成 28 年 12 月 16 日

注)★赤字は前回(平成 28 年 03 月 05 日付)の追加事項

用語	英語名称	解説
【アルファベット順】		
AES	Advanced Encryption Standard	DES の後継となる共通鍵暗号方式のアルゴリズム。2001 年に米国政府(NIST)の認定を受ける。鍵長を 128/192/256 ビットに拡張、専用チップに実装し、セキュリティ機能を強化する。IPsec、SSL/TLS、WPA2 等で採用される。
ANSI	American National Standard Institute	米国の工業規格の標準化を行う非営利団体。米国規格協会という。
APT	Advanced Persistent Threat	サイバー攻撃の一つ(標的型攻撃)。特定の組織や個人を標的に、複数の攻撃手法を組み合わせ対応が難しく執拗かつ継続的に攻撃を行う手法のこと。システムへの侵入等を行う共通攻撃手法と情報窃取等の目標に応じた個別攻撃手法とがある。
CAFIS	Credit And Finance Information System	NTT データが提供している共同利用型クレジット・オンライン・システム。クレジットカードの発行会社とその加盟店とをオンライン接続し、与信限度額の確認や無効カードのチェックを行う。
CEO	Chief Executive Officer	組織において業務の執行責任を担う最高責任者のこと。
CISO	Chief Information Security Officer	機密情報や個人情報などの情報資産に対するセキュリティを総括する責任者のこと。システムにおけるセキュリティ対策も取扱う。
Cookie		Web サーバがユーザを管理・識別するための文字列、あるいはその仕組み。ユーザ属性や個人情報が多い。Web サーバにはこの情報を基にユーザを識別し、Web ブラウザはその情報を一定期間保持する。
DES	Data Encryption Standard	米国政府が認定した 40/128 ビットの共通鍵暗号方式のアルゴリズム。IPsec、SSL/TLS 等で採用される。
DH 方式	Diffie-Hellman	公開鍵交換方式の一つ。自分だけが知る秘密鍵とこの秘密鍵から数学的な演算によって計算できる公開鍵を準備し、それを相手と交換することで安全な鍵交換を行う。
DLP	Data Leak Prevention	企業内にある機密情報の漏えい対策の総称。データそのものに機密性の有無を設定することで、機密情報のみを外部に流出させない“データ中心の情報漏えい対策”である。
DMZ	De-Militarized Zone	Web、メール、DNS といったインターネットに対してサービスを公開するサーバを防御することを目的としたファイアウォールによって守られたネットワーク・セグメント。インターネットからの攻撃を防御するとともに内部ネットワークへの被害の拡散を防ぐ。
DNS サーバ	Domain Name System	TCP/IP 通信において接続したい相手先の指定を IP アドレスではなく固有のドメイン名で行えるようにするシステム。その IP アドレスとドメイン名の対応についての情報を提供するサーバ。
Do Not Track		米国連邦取引委員会(FTC)が 2010 年に勧告した、プライバシー保護に関する枠組みで、Web 上でのトラッキング(行動履歴の追跡)を拒否する機能のこと。機能を有効にしておけば、アドネットワークや Web サイトの運営者などがユーザの Web 上での行動を追跡することを阻止できる。
EDOS 攻撃	Economic Denial of Sustainability Attack	経済的な損失を狙ったサービス妨害で、サービスに対して攻撃を仕掛けることで課金対象のクラウドのリソースを大量消費して、サービス利用者のビジネスを経済的に破たんさせる目的の攻撃である。
GPnet		1995 年に日本の大手カード会社 7 社と VISA が共同出資して設立したクレジットカード取引用データの中継業務を提供する会社及びそのネットワークの名称。
GSM	Global System for Mobile communication	世界で最も普及するデジタル携帯電話で使用の無線通信方式。特徴の一つとして携帯電話機から着脱可能な特定の固有 ID 番号を設定した加入者 ID(SIM)カードを採用するものがある(SIM:Subscriber Identity Module)。
HMAC	Hashed based Message Authentication Code	改竄検出のためのメッセージ認証コード(MAC 値)を生成するアルゴリズム。IPsec、SSL/TLS、S/MIME(Secure Multipurpose Mail Extensions)等で採用される。
HSM	Hardware Security Module	暗号鍵を安全に管理する役目のある機器。鍵を一切外に出さずに本体に内蔵し、鍵の保管、鍵での暗号・電子署名演算、鍵の生成、乱数の発生を行い、諸々の攻撃から鍵を保護する機能を持つ。
IDS/IPS	Intrusion Detection System/ Intrusion Protection System	IDS:ファイアウォールでは防御不能のネットワークやサーバ上での不正パケットを検知し、ログに記録し、管理者に異常連絡するシステム。IPS:更に不正パケットを自動的に遮断するシステム。
IEEE 802.11i	Institute of Electrical and Electronic Engineers	2004 年 6 月 IEEE(米国電気電子学会)で策定された無線 LAN セキュリティの標準規格。WPA・WPA2・802.1X 等が含まれる。
IEEE 802.1X (EAP-TLS)	(Extensible Authentication Protocol-Transport Layer Security)	無線 LAN(WPA・WPA2)のユーザ・パスワード認証をアプリケーション層で EAP により行う仕組み。基本構成は端末(認証ソフト:サプリカント)、フロアスイッチ(アクセスポイント経由の端末認証要求をコントローラに中継する装置:オーセンティケータ)及びコントローラ(同スイッチの情報を一元管理し、認証サーバに伝達する装置)、認証サーバ(認証ソフト:RADIUS)である。最強の認証方式である EAP-TLS では ID/パスワードに代わり、サーバ・端末双方に電子証明書が必要となる。
IETF	Internet Engineering Task Force	インターネットに関するプロトコル等の技術仕様を検討・開発する組織。IETF の作成・公開する技術文書は RFC(Request For Comments)と呼ばれる。

用語	英語名称	解説
【アルファベット順】		
IPsec (IKE) (ESP)	Internet Protocol Security (Internet Key Exchange) (Encapsulating Security Payload)	TCP/IP にセキュリティ機能を付加するプロトコルの枠組み。ネットワーク層で通信のセキュリティを確保する。公開鍵暗号方式による強力な認証及び鍵交換、共通鍵暗号方式による通信データの秘匿を実現するが、手順が複雑なため、次に二つの独立のプロトコルがある。①IKE: 鍵の自動交換機能を持つ、②ESP:暗号化機能を持つプロトコル部の仕様。RFC2406 で規定される。データの暗号化・認証、トラフィックフローの解析を行う防御機能を持つ。
ISO	International Organization for Standardization	国際標準化機構。各国の代表的標準化機構からなる代表的標準化機構で電気及び電子技術分野を除く全産業分野(鉱工業、農業、医薬品等)に関する国際規格を作成する。
KMIP	Key Manegement Interoperability Protocol	鍵管理関連システムを相互接続させる目的の暗号化クライアントと鍵管理サーバとの通信プロトコル。鍵の生成から提出，検索，抹消に至るライフサイクルを包含し、対象暗号および非対称暗号(公開鍵暗号)用の鍵や，デジタル署名などで使う鍵の管理に使用可能である。
LDAP	Lightweight Directory Access Protocol	ITU-T 勧告 X500 シリーズで規定されたディレクトリ・サーバにアクセスするためのプロトコル。ユーザ・デバイス認証を行い、同サーバに格納されるディレクトリ情報の操作(作成、検索、変更、削除等)ができる。
MAC アドレス	Media Access Control	ネットワーク機器のハードウェアに定義される 48 ビットのアドレスで ISO/OSI モデルの物理層およびデータリンク層で機能する。このアドレスはネットワーク機器の間で重複しない。
MD5	Message Digest Algorithm 5	ハッシュ関数の一つ。128 ビットのハッシュ値を生成する。
MDM	Mobile Device Management	複数のスマートフォン／タブレット端末・アプリを統一のポリシー下で一元管理するソフトで次の 3 つの主要な機能がある。(1)紛失・盗難時の情報漏洩防止、(2)不正利用の防止、(3)端末情報の収集とポリシー一斉適用等による管理の効率化
MIC	Message Integrity Code	IEEE 802.11i で規定された通信メッセージの完全性を保護するための仕組み。通信中のデータの改竄を抑制できる。WPA/WPA2 で採用される。
MPLS	Multiprotocol Label Swiching	通信事業者が公衆回線上の閉鎖的な(通信経路の暗号化が必要でない)ネットワークでデータを転送する技術。IP パケットの宛先 IP アドレスをラベルに格納し、ラベルでユーザ毎に論理的に通信を切り分けて(仮想的な専用線を構成し)転送する。
NAT/NAPT	Network Address Translation/ Port Translation	IP パケット転送時に IP ヘッダを書き換え、内部プライベート(NAT:単数、NAPT:複数)を外部グローバル(単数)アドレスに透過的に変換し、IP ヘッダを隠匿する機能。その役割をルータが担う。
NIST	National Institute of Standard and Technology	標準及び技術を制定する米国政府機関。米国国立標準・技術院と呼ばれる。
NTP	Network Time Protocol	インターネットを使って複数のコンピュータ間で時刻の同期を取るためのプロトコル。正確な時刻を持つサーバに各コンピュータがアクセスすることで時刻を同期する。
OSI 参照モデル	Open System Interconnection	国際標準化機構(ISO)によって制定された異機種間のデータ通信を実現するためのネットワーク構造の設計方針。次の 7 階層(レイヤ)の通信機能がある。(7)アプリケーション層(IEEE 802.1X)、(6)プレゼンテーション層、(5)セッション層(SSL-VPN)、(4)トランスポート層、(3)ネットワーク層(IPsec-VPN)、(2)データリンク層、(1)物理層
P2PE (E2EE)	Point-to-Point Encryption (End-to-End application-level Encryption)	SSL による暗号化は、Web サーバまではデータを暗号化が、Web サーバは届いたデータをサーバ内でいったん平文に復号するのでサイバー犯罪者にデータを盗まれる恐れがある。P2PE ではファイアウォールの内側に設置されたサーバのアプリケーションレベルまで暗号文のまま処理する。更に E2EE であれば、アプリケーションレベルを通過し、データベースレベルまで暗号文のまま処理するのでユーザのパソコンから最終事業者のバックエンドサーバまでを暗号化した状態で情報を送受信出来る。
PAD	Packet Assembler/Disassembler	パケット化されないデータをパケットに分解したり、パケットデータから復元したりする分解組立装置又は機能のこと。PC をパケット交換機に接続するために必要となる。
PIN	Personal Identification Number	数字だけから成る個人認証用のパスワード(暗証番号)。銀行のキャッシュカードや携帯電話の認証等で使用される。
PKI	Public Key Infrastructure	公開鍵における電子署名の真正性を保証する仕組み。次の三つの機能がある。(1)認証局:公開鍵の信頼性を保証する機関、(2)証明書:公開鍵とその鍵の信頼性に対するお墨付、(3)リポジトリ:公開鍵を管理・配布するサーバシステム。
PSK	Pre-Shared Key	パーソナルモード(WPA/WPA2-PSK):一般的には無線通信を暗号化する際にアクセスポイントと端末間で事前に共通暗号鍵を手動で設定する。エンタープライズモード(WPA/WPA2 Enterprise):企業等の大規模なネットワークでは PSK による設定は手間が煩雑になるため、セキュリティ強度が高い IEEE 802.1X 対応の認証サーバを用いて端末の認証を行う。
RADIUS	Remote Authentication Dial In User Service	アクセスの許可・拒否を行うプロトコルでユーザ・デバイス認証を行う。無線 LAN、VLAN、ワンタイムパスワードの認証にも使用される。IP アドレス等の設定情報をアクセス先のサーバに伝達する。

用語	英語名称	解説
【アルファベット順】		
RC4	Rivests Clpher 4	IPsec、SSL/TLS に最もよく使用される可変長鍵を扱えるストリーム暗号アルゴリズム。その他、WEP、WPA 等の暗号アルゴリズムとして採用される。
★SIEM	Security Information and Event Management	サーバやネットワーク機器、セキュリティ関連機器、各種アプリケーションから集められたログ情報に基づいて、異常があった場合に管理者に通知したりその対策方法を知らせたりする仕組みのこと。セキュリティインシデントの予兆を発見する予防的な効果と、ログ解析による事故発生後の調査、そして内部統制の強化により注目を集めるコンプライアンス管理等が可能。
SDN	Software-Defined Networking	コンピュータネットワークを構成する通信機器を単一のソフトウェアによって集中的に制御し、ネットワークの構造や構成、設定などを柔軟に、動的に変更することを可能とする技術の総称。機器の制御機能とデータ転送機能を分離し、制御機能をソフトウェアによって一ヵ所で集中管理することにより、どの機器にどのような動作をさせるか柔軟に設定することが可能。
SHA	Secure Hash Algorithem	NIST が開発したハッシュ関数。160 ビットのハッシュ値を生成するもので強度は MD5 等を上回る。SHA-1 に脆弱性があるのでハッシュ値のビット長がより安全な SHA-2(SHA244、SHA256、SHA384、SHA512 等)への移行が推奨されている。
SMTP	Simple Mail Transfer Protocol	TCP/IP 環境で使用されるメール転送プロトコル。メーラあるいはメールサーバが別のメールサーバにメールを送る時に使用する。SMTP OVER SSL は暗号化機能を持つ(STARTTLS では通常のメール送信時(SMTP)と同じポート番号を用いるため、設定変更による影響を受けにくい特長がある)。
SNMP	Simple Network Management Protocol	ネットワーク管理のためのプロトコル。不正アクセス防止のため、エージェント側の各機器のネットワーク情報(CPU 負荷、メモリ使用量、障害等)をマネジャ側が集中監視する。
SSH	Secure Shell	セキュリティ面に関して強化されたアプリケーション群(リモートログインやファイル等)及びそれらのアプリケーションが用いるインターネットプロトコルの１つ。公開鍵暗号方式による強力な認証及び鍵交換、共通鍵暗号方式による通信データの秘匿を実現する。暗号/完全性の強度では SSH2(AES/HMAC)は SSH1(3DES/CRC)より強い。SFTP は SSH で暗号化された通信路を FTP に似たコマンド体系で任意のファイルを送受信するプロトコル。
SSID	Service Set Identifier (ESS-ID)	無線 LAN のアクセスポイント(AP)の識別子(グループ名:32 文字)。不正アクセス防止のため、AP に SSID が空白又は ANY 設定の端末からの接続拒否や SSID を送信信号(ビーコン)に含めない隠蔽機能がある。
SSL (EV SSL) (常時 SSL)	Secure Sockets Layer (Extended Validation SSL Certificate)	暗号技術を利用するインターネットプロトコルの１つ。セッション層で通信のセキュリティを確保する。Web ブラウザとサーバとの通信データの暗号化で標準となる。デジタル署名(認証局)の公開鍵暗号方式による認証及び鍵交換、共通鍵暗号方式による通信データの秘匿を実現する。 (業界統一基準に則って企業の実在性をより高い精度で認証する証明書。セキュリティを強化した Web ブラウザと組み合わせ、Web サイトの運営組織(組織名と認証局)の実在性を明確に特定する。) ログインページや決済ページなど通常暗号化が必要とされているページ以外の全てのページを SSL で暗号化する手法である。常時 SSL によって Cookie や URL パラメータで保管されることが多いユーザ識別子が常に暗号化され、検索履歴、会員情報、Web ショッピング等の安全性(信頼性)を高められる。
SSO	Single Sign-On	一度の認証処理で複数のコンピュータ上にあるリソースが、利用可能になる認証機能のことである。あるコンピュータにログインした後、グループウェアなどのアプリケーションを使う際に、再度ログイン、また他のサーバ上のアプリケーションを使用する際にログインするといった状況で、ユーザが複数の ID とパスワードを管理しなければいけなくなった時に、役に立つ機能である。
Syslog		各種の UNIX が備えるシステムログの出力機能。各種アプリケーションが Syslog 関数により出力したログデータを Syslog プロセスが処理し、ファイル等に出力する。
TKIP	Temporal Key Integrity Protocol	WPA-TKIP で使われている暗号化プロトコル。クライアントごとに異なるキーを発行し、定期的に変更する機能
TLS	Transport Layer Security	NETSCAPE 社が開発した SSL ver3 の後継規格として IETF が標準化したインターネットプロトコル。大枠の仕組みは同じであるが互換性はない。
Triple-DES		安全性を高めるために、DES の暗号化プロセスを 3 回繰り返したもの。
UTM	Unified threat Management:統合脅威管理(次世代ファイアウォールとも称す)	ファイアウォールと VPN 機能にアンチウィルス、不正侵入防御等の複数のセキュリティ機能を統合的に管理する機器。アンチウィルスには次の二つのが機能がある。(1)ネットワーク対策:ネットワーク経由で感染するウィルス(ワーム)の防御、(2)ゲートウェイ対策:ネットワーク経路上でのメールの受送信(SMT、POP3)、Web ページの閲覧(HTTP)、ファイルのダウンロード(FTP)等のプロトコル上でのウィルスの検出、駆除・削除、通信ブロック等の防御。

用語	英語名称	解説
【アルファベット順】		
(Firebox)	(ファイヤーボックス)	WatchGuard 社が開発した統合脅威管理(UTM)アプライアンス。 ファイアウォールをベースに、ウィルス対策、不正侵入阻止、迷惑メール対策、Web フィルタリング、VPN などの機能を一台のアプライアンスに集約。OSI 全 7 層を検知するアプリケーション・プロキシを採用しているほか、レポート機能をバンドルし、ネットワーク活動のグラフ化が可能である。
VDI	Virtual Desktop Infrastructure	企業等でデスクトップ環境を仮想化してサーバ上に集約したもの。利用者は端末からネットワークを通じてサーバ上の仮想マシンに接続し、端末画面から操作する。サーバで集中管理する(端末に情報を保管しない)ため、情報の追加や更新、修正等の保守が容易となり、ウィルス感染や情報漏洩の防止が容易(Windows_OS では端末とサーバとの接続に RDP(Remote Disktop Protocol)を使用)。
VLAN	Virtual Local Area Network	スイッチ等のネットワーク機器の機能を使い、仮想的に構成するネットワーク。大手の企業等ではレイヤ 3 スイッチを部門毎に設置し、ネットワークを分割してアクセスを制限するセキュリティ対策手段として使用する。
VNC	Virtual Network Computer	ネットワーク上の離れたコンピュータを遠隔操作するためのリモート操作用ソフト。VNC がインストールされるマシン同士は、OS 等のプラットフォームの種類に依存することなく通信できる。
VPN	Virtual Private Network	インターネットのような公衆回線を暗号と認証技術を用いてプライベートなネットワークのように利用する技術、もしくはそのネットワーク自身の名称。専用回線よりも安価に構築できる。IPsec-VPN:各拠点間の暗号化(IP ヘッダを含む)通信を両端の IPsec ルータ経由で行う。SSL-VPN:外部クライアントと内部ホスト間の暗号化(IP ヘッダを除外)通信を内部の SSL ゲートウェイ経由で行う。
Web Reputation		不正サイトによるウイルス感染をブロックする機能のこと。Web サイトにアクセスする際、自動的に不正サイトの危険度データが蓄積されたセンターに問い合わせ(評価)を行い、接続先のドメイン、Web サイト、Web ページが不正であった場合に迷惑メールをブロックしたり、ウィルスをばら撒く Web サイトへのアクセスを拒絶する。
Wi-Fi	Wireless Fidelity(ワイファイ)	Wi-Fi アライアンス(2.4GHz 帯の無線 LAN 規格である IEEE802.11x の相互接続性を確認・認定する業界団体)が認定した製品に与えるロゴで、異なるメーカ間でも相互接続が保証される。

用語	英語名称	解説
【五十音順】		
アクセス制御	Access Control	情報自身や情報システムに決められた人やアプリケーションだけがアクセスできるようにする仕組み。上記のアクセス制御情報を記述したリストを ACL(Access Control List)という。
暗号技術	Cryptography	通信メッセージ等のデータを本人のみが知る一定の規則に従って変換し、本人以外に対してデータを秘匿する技術。ストリーム(数ビット単位)とブロック(256 等一定量のビット単位)方式がある。
暗号鍵管理		鍵ペアー(公開鍵、秘密鍵)の作成・配布・変更・保管・無効・廃棄の管理を認証局ないし自社局において行う。
インシデント対応	Incident	インシデント(情報セキュリティリスクが発現・現実化した事象)の発生に際してそれを検知し、関係組織と連絡を取り、被害拡大の防止とともに再発防止の原因究明を行う一連の組織的活動。
インデックス・トークン		カード番号等の PAN(Primary Account Number)情報を暗号化するために通信データを類推不可能な文字列に置換えるための暗号装置。トークン化したデータは元の文字列と数学的な関係がないため、紛失時にも解読されない、又、元のデータ形式やデータ長が同じであるため、システムへの影響が小さい等の特徴がある。
エクストラネット		電子商取引(EC)や電子データ交換(EDI)の効率化を図るため、複数の企業間でインターネットや専用の通信回線を相互接続したネットワーク。IP VPN 等などの接続技術の進展により、イントラネット同士をワールドワイドで廉価かつセキュアに接続することが可能になった。
オフサイト施設		重要なデータを保管するサーバ等を会社以外に設置する施設(データセンタ)。主要都市の郊外に設置されることが多い。
オンアス取引		アクアイアラ(加盟店契約会社)とインシュア(クレジットカード発行会社)が同じ会社系列である場合のクレジットカード決済取引業務。
エンドポイントコントロール		SSL-VPN 装置で社内ネットワークに接続するパソコンの状態をシステム管理者が把握するための重要な機能。パソコンの状態を検知し、危険度の高いパソコンのアクセスを拒否する機能や、Web 上に残った URL の履歴やクッキー、パスワードのオートコンプリート等などの情報を自動的に削除する機能でリモートアクセスに使う ID、パスワードなどが第 3 者に漏れる危険性を防止出来る。
共通鍵暗号方式		暗号化と復号化に同じ暗号鍵を使う暗号方式(対象鍵暗号方式)。当方式で暗号化されたデータは、同一の暗号鍵がない限り復号化できない。DES や AES が代表的である。

用語	英語名称	解説
【五十音順】		
公開鍵暗号方式		公開鍵と秘密鍵という二種類の数学的な鍵を対にして使う暗号方式(非対象鍵暗号方式)。公開鍵は不特定多数に公開し、秘密鍵は鍵の持ち主しか知らない。SSL/TLS、SSH や IPsec が代表的である。
サーバ	Server	ネットワークで接続される他のコンピュータに対して様々なサービスを提供するコンピュータ。種類としては Web、データベース、認証、メール、プロキシ、ネットワークプロトコル(NTP)、ドメイン名(DNS)等がある。
サンドボックス	Sandbox	外部から受け取ったプログラムを保護された領域で動作させることによってシステムが不正に操作されるのを防ぐセキュリティモデル。実行されるプログラムは保護された領域に入り、他のプログラムやデータなどを操作できない状態に動作するため、プログラムの暴走やウィルスの動作によるシステムへの影響を防止する。
ゼロデイ攻撃		ソフトウェアの脆弱性(セキュリティホール)を標的とした攻撃のうち、脆弱性が発見されてから、開発者によって修正プログラムなどの対策が提供されるまでの時間差を利用して行われる攻撃で、万全に対策を講じることは難しいとされている。代表的な例として Blaster ワームが挙げられる。
ディレクトリ・サーバ	Directory Server	組織内のユーザ情報等の資源情報を纏めたツリー型のデータベースをサービスするサーバ。次の三つの機能がある。(1)目的:セキュリティ確保のための管理コストの抑制、(2)手段:各サーバ(基幹業務、グループウェア、メール、Web 等)へのアクセス制御の情報等の一元管理、(3)効果:管理責任の分割・委譲と整合性の確保。
デジタル署名		SSL:サーバの公開鍵を認証局の秘密鍵で暗号化したものや S/MIME:送信者の秘密鍵でメッセージのハッシュ値を暗号化(通常とは逆の公開鍵暗号方式)したもの。受信者は送信者の公開鍵で電子署名を復号し、本人性と完全性の確認が出来る。
★トンネリング		通信ネットワーク上の 2 点間を結ぶ閉じられた仮想的な直結回線(仮想回線：トンネル)のこと。別のプロトコルのパケットで包んで(カプセル化)送り届けることにより通信を行いパケットのカプセル化とその解除はトンネルの両端の機器が自動的に行うため、セキュリティの確保が可能。
電子認証局	Certification Authority CA	セキュリティ確保のためにネットワーク上の個人や法人が確かに“本人”であることを証明する「電子証明書」を発行するシステム、若しくはそのシステムを提供する第三者認証機関。
トークン	Token	紛失・悪用防止対策として主にハードウェアで実現される OTP(ワンタイムパスワード)生成器、PIN コードを入力する形態(二要素認証)がある。 トークン不要の OTP 認証システムはトークンや端末側に USB ポートや専用アプリケーションも不要である。ブラウザだけで OTP を実現可能なため、リモート＋モバイルと相性が良く時間、場所、端末に制約されない。又、ActiveDirectory とユーザアカウントとの同期機能、サポート業務の補助機能等、管理者の支援機能もある。
二要素認証		二要素認証では、ユーザ本人であることを確認する 2 つの「固有情報」を、二要素に分けて入力させて認証する。もし固有情報が一つ漏れても、もう一つの固有情報が漏れない限り、攻撃者が認証を突破することは難しくなる。 よく実装されている二要素認証では、一要素目の認証は従来と同じパスワードとし、二要素目は一要素目とは異なるパスワードを二要素目の認証時に入力する、二要素目の認証時に表示された質問に合わせて入力する、二要素目の認証で SMS またはメールで通知されるワンタイムパスワードを入力するが多い。
ハッシュ化		ハッシュ関数を用いて入力したデータを疑似乱数化すること。ハッシュ化されたデータから元の入力データを再現できない。
パッチ	Patch	ソフトウェアのバグやセキュリティ・ホールを修正するためのデータ、もしくは(修正)プログラム。
ファイアウォール	Fire Wall	インターネットからの攻撃や不正アクセスから内部ネットワークを守るシステム。外部から内部ネットワークへのアクセス(インバウンド)を不許可にし、内部から外部ネットワークへのアクセス(アウトバウンド)を許可する制御が基本機能。ネットワークのゲートウェイ型には次の二つの機能がある。①パケットフィルタリング(ネットワーク層)、②アプリケーションゲートウェイ(アプリケーション層)。後者は詳細な制御設定が可能で前者より強度が高い。
フォレンジック	Forensic	不正アクセスを受けた、もしくは受けた可能性がある場合の証拠保全と追跡を目的として何らかの被害を受けた後に、その被害を証明する際の証拠を集めておく技術。
ボット		広義のコンピュータウイルスの一種。ボットネットは攻撃者、C&C サーバ、感染 PC(ゾンビマシン)から成る。攻撃者はインターネット上で C&C サーバを介して感染 PC を自由に操り、感染 PC をスパムメールの送信サーバや Dos 攻撃の発信源にする等の悪さを行う。

用語	英語名称	解説
【五十音順】		
★水飲み場型攻撃		特定の組織や個人を狙う標的型攻撃の手法の一つで、標的(の組織や個人)となるWebサイトを改ざんし、アクセスした利用者にウィルスなどのマルウェアを導入するよう仕込む手法のこと。攻撃に成功すると、標的の情報システムを不正に遠隔操作して破壊したり機密情報を盗み出したりするが、標的以外の利用者がサイトにアクセスしても何も起きないため、攻撃が発覚しにくい。
ランサムウェア		マルウェア(悪意のあるソフトウェア)の一種で、ユーザのデータを人質にとり、データの回復のために身代金(ransom)を要求するソフトウェアで代表例は Cryzip 等がある。防止手段には信頼できないソフトウェアを実行しない、発見したらセキュリティベンダに連絡すること等がある。
リバース・プロキシ/プロキシサーバ		外/内部からの不正アクセスを防御するサーバ。リバース・プロキシ:外部のインターネットから内部のイントラネット等への接続する場合、ファイアウォールを超えるため、外部から内部の URL に変換を中継するサーバ(DMZ 上の SSL ゲートウェイ)。プロキシ:端末を外部 Web サーバに接続する場合、端末の接続を代行し、内部(送信元 IP アドレス等)と異なる外部情報の変換やプロトコル(HTTP、SMTP、DNS 等)上での不正なデータやコマンド等の制御を行うサーバ(アプリケーションゲートウェイ)。