CISSP Glossary List Translated

監訳：笠原久嗣 CISSP CCSP
監修：石附陽子 CISSP CCSP 佐藤雄一 CISSP 松方岩雄 CISSP 新井雅 CISSP
富杉麻衣絵 CISSP 永田真弓 CISSP 小熊慶一郎 CISSP
協力：大崎伸之 CISSP 森口裕史 CISSP 上田哲美 CISSP
福井将樹 CISSP CCSP SSCP 岩男幸子 CISSP 他用語集WGメンバ

CISSP
英日対訳集

前書き

この電子書籍を見てみようと思われた方は、既に CISSP 等の資格をお持ちの方や、これから勉強して取得しようと思われている方が多いのではないかと思います。

私が CISSP を受験したのは 2002 年ですが、その頃は日本語での受験はできませんでした。受験のための勉強も、厚い英語の書籍によるものでした。その後日本語での受験が可能になり、日本における受験者は増えました。ただ、試験問題の日本語訳の品質はあまりよくないという話も聞くようになりました。

(ISC)²が翻訳に使っているという Glossary List というものがあります。その品質に問題がありそうであるということで、まずはその改善を行いたいという思いで WG をスタートしました。最終目標としては「情報セキュリティ用語を和訳する際の手本になるようなものを作る」ということを掲げました。

そして 1 年以上かかりましたが Glossary List の日本語訳への改善提案を行いました。

その後、セキュリティ用語の電子書籍公開を目指して活動してきました。その結果がこの電子書籍です。英語の用語に対して日本語訳を皆で検討するという形で進めてきました。

英単語・熟語の日本語訳については文脈によって変わる場合も多く、一つに決めきれないこともあり、意見が分かれることもありました。その辺の議論や意見もコメントとしてつけてみました。

我々もまだまだ勉強中です。また、用語については日本語でも英語でも変わっていくことも多くあります。誤り、改善案等ございましたらお知らせくださると助かります。

2021 年 10 月

用語集 WG 主査
石附陽子

目次

A

Abstraction	抽象化

Access Control	アクセス制御

注:「アクセス制御」は「アクセス管理 (Access Management)」とは別の概念。

Account Management	アカウント管理

注:「マネジメント」は目標を達成させることを目的に定められた手段を意味し、「管理」は行動手段を意味するという説もある。ここでは「管理」を採用した。

Accountability	説明責任、アカウンタビリティ

注:「Accountability」は「説明責任」と訳されることが多いが、「Accountability」は説明に関する責任だけではないので、カタカナの方が適切かもしれない。

Accreditation	認定

注: ソフトウェアの認証と認定（C&A）で使用される言葉。

Administrative Controls	管理コントロール

注: 物理コントロール (Physical Controls)、論理コントロール(Logical Controls)の仲間

Admissibility of Evidence	証拠の認容性

注:「Evidence」はカタカナの「エビデンス」として使われることが多くなってきた。但し、フォレンジックに関する文脈では「証拠」と訳すのが適切と思われるので、「証拠」とした。

Advanced Encryption Standard	AES (Advanced Encryption Standard)

注: 次世代暗号化標準という言い方もあったが、固有名詞「AES」で現在は浸透している。

Aggregation	集約

注: データベースに対する攻撃の一種。NW 回線の集約（LAG 等）の意味では用いてなかったような…。

Air Contamination	空気汚染

注: 大気ではなく室内の空気を意味している。物理的攻撃の一種として用いられる。

Algebraic Attack	代数的攻撃

注: 代数的手法により暗号鍵を推定する攻撃らしい。

Alteration	改変

注: セキュリティの文脈で使われる場合。

Alternate Site	代替サイト

注: 類似の言葉に災害復旧サイトや災害対策サイトがある。

Annualized Loss Expectancy	年間損失予測

注: 略語 ALE で使われることも多い。

Annualized Rate of Occurrence	年間発生頻度

注: 略語 ARO で使われることも多い。

Anomaly Detection	アノマリー検知

注: 「ー」(長音)を取って「アノマリ検知」でも良いと思われる。技術系の文書では長音が無く、一般向けの文書では長音がつく傾向にあると思われる。ここでは、特に統一はしない。

Anomaly-Based	アノマリーベースの

注: 「ー」(長音)を取って「アノマリベースの」でも良いと思われる。

Anti-Malware System	マルウェア対策システム

注: 「アンチウイルス」とは異なり、Anti-malware を「アンチマルウェア」とはあまり言わない。

Anti-Passback	アンチパスバック

注: 共連れの防止対策を意味する。

Application Security Testing	アプリケーションセキュリティテスト

注: 同じ「Test」でも、内部で実施する場合は「テスト」を使い、外部ベンダに依頼する場合は「診断」にするのがしっくりくる、という意見もあった。

Approval **許可**

注: 一般用語としては「承認」として用いる事が多いように見受けられる？

ARP Attack **ARP 攻撃**

注: ARP を使った攻撃。セキュリティ製品で資産管理外の端末の接続をさせないためにこの技術を使うものもある。

Artifact **アーティファクト、成果物、生成物**

注: 直訳すると「人工物」の意味。「証拠」や「痕跡」のような意味合いで使われることが多い。文脈により「成果物」「生成物」と訳した方がわかりやすい場合もある。

Asset Management **資産管理**

Asset Value **資産価値**

Assurance **保証**

注: 「Assurance」だけの場合は「保証」と訳すことにあまり違和感は無いが、「Information Assurance」を訳すときに「情報保証」とするのは違和感を感じる(検索すると自衛隊関連の情報ばかりが見つかる)。最近はカタカナで「アシュアランス」とする場合も多く見かける。

Asymmetric Cryptography **非対称暗号**

注: 「非対称型暗号」と言う場合もある。

Atomic Operation **不可分操作**

注: 「Atomicity」の訳を「原子性」にすることに違和感は感じないが、「Atomic Operation」を「原子操作」と訳すと物理学における「原子」のことのように感じてしまう。

Atomicity **原子性**

注: データベーストランザクションにおける 4 原則(ACID)の 1 つ。

Attack surface	攻撃サーフェス

注: 「攻撃面」という意見も出たが、「面」では surface の意味を表現しきれていないのでサーフェスとした。

Attack vector	攻撃ベクター

注: Google で検索すると「攻撃ベクトル」より「攻撃ベクター」の方がはるかに多いので、「攻撃ベクター」とする。

Audit Record	監査レコード

注: 類似の言葉として監査ログ(Audit logs) もある。

Audit Trail	監査証跡

注: 監査基準を満たしていることを証明するもの。（Audit Record もその一つとなる場合が多い。）

Authentication	認証

Authenticity	真正性

Authorization	認可

Availability	可用性

Awareness	アウェアネス

注: 「Security Awareness」であれば、「セキュリティに対する認識」と訳すことができるが、「Awareness」だけの際に「認識」と訳すと違和感がある。かといって、「Awareness」だけのときに「セキュリティに対する認識」と訳語を当てるわけにはいかない。結果として、カタカナの「アウェアネス」が適切ではないかということになった。

B

Backdoor	バックドア

Background Check　　バックグラウンドチェック

注:「Background Check」は、身元調査、身元照会、信用照会、犯罪記録照会などを包括している概念と思われるので、「バックグラウントチェック」とした。「身辺調査」とすると興信所が行うことのような印象を与える。

Background Investigation　　バックグラウンド調査

Baiting Attack　　ベイティング攻撃

注: USB メモリをばらまいてユーザーに使わせるタイプの攻撃、水飲み場攻撃などのことを指すらしい。

Barrier　　防護壁

注: 物理セキュリティで使用される用語らしい。

Baseline　　ベースライン

注: セキュリティルールのベースライン(ベースラインアプローチ)として使われる場合が多いが、改ざん検知ソリューションで比較元データ的な意味で使われることもある。

Bastion Host　　要塞ホスト

Bell-LaPadula Confidentiality Model　　Bell-LaPadula 機密性モデル

注: David Elliott Bell と Leonard J. LaPadula によって開発されたセキュリティモデル。

Between-the-Lines Attack　　通信線攻撃

注: 物理的に配線にアクセスし、あるユーザーのセッションにデータを挿入するようなタイプの攻撃の意味。

Biba Integrity Model　　Biba 完全性モデル

注: Kenneth J. Biba によって開発されたセキュリティモデル。IPA の文書には「low water mark モデル」とも書かれている。

Biometric Device	バイオメトリックデバイス

注: 「装置」にすると複数のデバイスが複合した機械のように感じる。「バイオメトリックデバイス」と「バイオメトリックリーダ」の違いは無いのでは無いか?

Biometric Reader	バイオメトリックリーダ

注: 「バイオメトリックリーダー」にするとバイオメトリック市場のリーダー(Leader)のように感じる。

Biometric System	バイオメトリックシステム

Birthday Attack	誕生日攻撃

注: Google で検索すると「バースデーアタック」より「誕生日攻撃」の方がずっと多い。

Black-Box Testing	ブラックボックステスト

注: 「Testing」だけど、テスト以外に良い訳が思いつかない。

Blacklist	ブラックリスト

注: Politically incorrect な言葉。Whitelist は Allow List(許可リスト)、Blacklist は Deny List(禁止リスト)が正しいらしい。マンホールをメンテナンスホールと言うのと同じ。

Block Cipher	ブロック暗号

Blowfish	Blowfish

注: 「Blowfish」は「河豚(ふぐ)」のこと。河豚という名の対称ブロック暗号。

Bot	ボット

Bot Herder	ボットハーダー

注: Bot を羊に見立てた際の羊飼い的な役割の人物と見立てられている。

Botnet	ボットネット

Boundary Control **境界制御**

注: 「物理コントロール」「技術コントロール」などの表現と異なることがわかりやすいように「制御」としてみた。

Boundary Router **境界ルーター**

注: 「エッジルーター」は内部と外部の境界に置かれるものであり、境界ルーターはそれ以外の境界に設置されるものである。

Branch **分岐、支店、支社、支部**

注: ソフトウェアの文脈では「分岐」、組織に関する場合は「支店、支社、支部」等となる。

Breach **侵害、違反、漏洩**

注: 「違反」「漏洩」「侵害」など種々の訳語がある。CISSP CBK では原則「侵害」とした。「違反」「漏洩」の方が文脈上適するところはそちらを使っても良いと思う。なお、「漏洩」に対応する英語は、一般的には「Information Disclosure（情報漏洩）」「Data Leak/Data Leakage（データ漏洩）」となる。前者は STRIDE 脅威モデル、後者は DLP 製品についての説明で使われている。また、「Compromise」との訳語の使い分けも悩みどころ。また、情報の不正取得について「窃取」と表現することも多いが、「窃取」は「窃盗罪」で使用する法律用語であり、日本の刑法において「窃盗罪」は「財物」を「窃取」した場合にのみ成立するものであって、「情報」は「財物」に該当しないことから、「情報を窃取する」という表現は誤りである、と主張している人もいる。

Brewer-Nash **Brewer-Nash**

注: Chinese Wall モデルと同義である。

Brute Force Attack **総当たり攻撃**

注: ブルートがポパイをボコ殴りすることが由来らしい。

Buffer Overflow **バッファーオーバーフロー**

注: Google で検索すると「バッファオーバーフロー」よりも、「ー」(長音)がついている「バッファーオーバーフロー」が多い。

Burden of Proof **立証責任**

注: 法律用語らしい。

Business Continuity **事業継続**

Business Continuity Plan **事業継続計画、BCP**

注:「BCP」という言葉も一般化してきたので。

Business Impact Analysis **事業影響度分析、BIA**

注:「BIA」と略して使われることも多い。

C

Cable Plant Management **ケーブルプラント管理**

注: 構内のネットワーク配線管理に関する物理セキュリティ分野の用語。

Capability Maturity Model **能力成熟度モデル、CMM**

注:「CMM」と略して使われることも多い。

Categorization **カテゴリー化**

注: Classification (分類)との違いを明確化するため、「カテゴリー化」としている。

Certificate **証明書**

Certificate Authority **認証局、CA**

注:「CA」と略して使われることも多い

Certification **認証**

注: 日本語では Authentication(認証)と区別できない。二者間の認証は Authentication、第三者が認証する場合は Certification、という説もある。

Chain of Custody **管理の連鎖、CoC**

注: 木材用語からフォレンジック用語になったもの。CoC と表現することもある。

Chain of Trust **信頼の連鎖**

注: 連鎖する証明書により信頼を構築する意味や、サプライチェーンセキュリティの文脈でも利用される。

Change Detection Software	改ざん検知ソフトウェア

注: Change は「改ざん」ではないが、この種類のソフトウェアは一般に「改ざん検知ソフトウェア」と呼ばれている。

Change Management	変更管理

Chinese Wall Model	チャイニーズウォールモデル

注: 英語表記もある。Chinese Wall モデル

Chosen Ciphertext Attack	選択暗号文攻撃

Chosen Plaintext Attack	選択平文攻撃

Ciphertext	暗号文

Ciphertext-Only Attack	暗号文単独攻撃

Clark–Wilson Integrity Model	Clark-Wilson 完全性モデル

Classification	分類

注:「Categorization」は「カテゴリー化」。

Clipping	クリッピング

注:「clipping level」を「収集レベル」と訳している場合もある。

Closed Circuit Television	閉回路監視カメラ、CCTV

注:「CCTV」も一般的。

Cloud Computing	クラウドコンピューティング

Cognitive Passwords	コグニティブパスワード

注: コグニティブパスワードの代表例としては、いわゆる「秘密の質問」。

Common Criteria　　コモンクライテリア

注: 「CC」と略されることも多い。CC という訳をつける、というアイデアもあったが、カーボンコピーと紛らわしいので却下。

Community Cloud　　コミュニティクラウド

Compensating Controls　　補償コントロール

注： Preventative(防 止)/Deterrent(抑 止)/Detective(検 知)/Recovery(復旧)/Directive(指示)/Compensating(補償)コントロールとセットで現れ使われる。「補完コントロール」とされる場合もある。

Complete Mediation　　完全仲介

注: リファレンスモニターにおいて、すべてを仲介するという意味。

Compliance　　コンプライアンス

注: ISO/IEC27001 では「順守」と訳している。「遵守」も使われる。

Compromise　　侵害、危殆化

注:「侵害」と訳されるが、同様に breach も「侵害」と訳される。暗号鍵の場合は「危殆化」。

Computer Forensics　　コンピュータフォレンジック

注: 日本語で「フォレンジックス」はあまり使われていないので「フォレンジック」とする。但し、英語で forensic は形容詞なので「フォレンジック」はもやもやする。

Computer Incident Response Team　　コンピュータインシデントレスポンスチーム

注:「CIRT」、「CERT」、「CSIRT」など、似た略称がいろいろある。

Computer Virus　　コンピュータウイルス

注:「ウイルス」を「ウィルス」と書くこともある。英語の発音だと「ヴァイラス」。

Confidentiality　　機密性

Configuration Item	構成項目、設定項目、構成アイテム

注: 対象によって訳が変わる。

Configuration Management	構成管理

Confinement Problem	閉じ込め問題

注: 隠れチャネル(Covert channel)に関する言葉。Confinement は監禁の意味もある。

Consistency	一貫性

Containment	封じ込め

Contingency Planning	コンティンジェンシープラン

注: 以前は「緊急時対応計画」と訳されていたが、最近ではカタカナで通用するようになった。

Controls	コントロール、制御、管理策、統制

注: 文脈によっていろいろな訳がある。ISO/IEC27001 なら「管理策」、J-SOX なら「統制」。

Copyright	著作権

Corporate Memory	企業の知

注: 企業の「組織知」のようなもの。

Corrective Controls	是正コントロール

注: Preventive/Deterrent/Detective/Directive/Recovery/Compensating Controls とセットで現れる/使われる/覚える。

Coverage	カバレッジ

注:「網羅」だと抜けが無いような意味になるので、違うニュアンスになる。

Covert Channel	隠れチャネル

Credential Management	資格情報管理

Crime Prevention through Environmental Design	防犯環境設計

注: CPTED のこと。

Cross-Certification Model	相互認証モデル

Crossover Error Rate	等誤り率

注: 生体認証の文脈で使われる。

Cross-Site Scripting	クロスサイトスクリプティング

Crown Jewel	王冠の宝石、攻撃目標

注: もともとの意味は王冠の宝石だが、転じて、攻撃目標の意味で使われる。「重要資産」と訳す場合もある。盗まれると非常に困るもののことらしい。

Cryptoanalysis	暗号解読

Customer	利用者、顧客

注: セキュリティの文脈では、「顧客」より（サービス／システムの）「利用者」と訳す方が適切な場合が多い。CRM のような特殊な文脈では「顧客」が適切な場合もある。また、user は「利用者」ではなく「ユーザー」とするとよい。

Customer Relationship Management	顧客管理(CRM)

注:「顧客関係管理」と訳すこともある。CRM という言葉も一般的。

Cyber-Physical System	サイバーフィジカルシステム(CPS)

注:「サイバー・フィジカル・システム」とすることもある。

D

Data Contamination	データ汚染

Data Controller	データコントローラー

注:「データ管理者」と訳すと他の用語(Data custodian 等)と混乱するので「データコントローラー」と訳すこととする。

Data Custodian	データカストディアン

注: CISSP CBK では従来「データ管理者」としていたが、administrator と区別ができなくなる。また、CISSP 教材では Custodianship という言葉もありこちらの訳にも悩む。そこで、データコントローラー、データプロセッサー、データスチュワード、データサブジェクトなど GDPR 関連の他の用語に合わせ、Data custodian はデータカストディアン、Custodianship はカストディアンシップとした。

Data Disclosure	データ漏洩、データ開示

注: データ漏洩だけでなく、開示の意味合いで使われる場合もある。

Data Encryption Standard	データ暗号化標準(DES)
Data Flow Diagram	データフロー図
Data Hiding	データの隠蔽

注: 他に良い訳が見つからないが、「隠蔽」だと、なにか悪いことを隠すような印象がある。意味的には「データの秘匿」のような感じ。

Data at Rest	保存中のデータ
Data in Transit	転送中のデータ
Data in Use	使用中のデータ
Data Leak/Loss Prevention	データ漏洩/損失防止(DLP)
Data Management	データ管理
Data Mining	データマイニング
Data Owner	データオーナー
Data Processor	データプロセッサー
Data Quality	データ品質

Data Remanence	データ残留

Data Standard	データ標準

注: データの取り扱いに関する標準のことらしい。

Data Steward	データスチュワード

Data Subject	データサブジェクト

Database Management System	データベース管理システム (DBMS)

注: 直訳すると「データベース管理システム」だが、DBMS という略称のほうが浸透している。

Database System	データベースシステム

Decryption	復号

注: Encryption と対になる用語だが、Encryption は暗号化と「化」を付けて訳すのに対して、Decryption には「化」を付ける必要は無い。名詞と動詞の違いらしい。Encryption は Cryptography（暗号）と区別するためにも「化」を付ける。

Defense in Depth	多層防御

注: Depth だが「深層防御」とは言わない。

Demilitarized Zone	DMZ

注: 「うちの会社の非武装地帯は」と言ったりすることはないので、DMZ とする。

Denial-of-Service Attack	DoS 攻撃

注: 意味からすると、サービス妨害だが、CBK や問題集などではサービス拒否となっており、この議論が折り合わず。日経新聞などの一般紙でも DoS 攻撃が使われていることから、DoS 攻撃とした。Denial of Service は STRIDE 脅威分析モデルの”D"。

Detective Controls	**検知コントロール**

注: 検出型コントロールとしている(ISC)²の教材もあるが、情報セキュリティ分野では初期から侵入検知（Intrusion Detection）が一般的なので。（侵入検出とはあまり言わない？）

Deterrent Controls	**抑止コントロール**

注: 抑止型コントロールと訳される場合もあるが「型」は付けないことで統一する。

Dictionary Attack	**辞書攻撃**

Differential Backup	**差分バックアップ**

Differential Cryptanalysis	**差分解読法**

Digital Investigation	**デジタル調査**

Digital Signature	**デジタル署名**

Directive Controls	**指示コントロール**

注: 指示型コントロールと訳される場合もあるが「型」は付けないことで統一する。

Disaster Recovery Plan	**災害復旧計画(DRP)**

Discovery	**発見、開示、探索、検出、ディスカバリ**

注: 一般用語として「発見」と訳される文脈もあるが、情報セキュリティでは、legal discovery documents（証拠開示文書）、electronic discovery（電子情報開示／e ディスカバリ）、discovery phase of a law suit（訴訟のディスカバリ段階）、data discovery（データディスカバリ）など、文脈／イディオムに依存することが多い。その場合には「発見」でなく、「開示」「ディスカバリ」が多く採用される。

Discretionary Access Control	**任意アクセス制御**

注: 強制アクセス制御（Mandatory Access Control）の対語。

Distributed Denial-of-Service Attack	DDoS 攻撃

注: 日経新聞などの一般紙でも DDoS 攻撃という用語が使われていることから、DDoS 攻撃とした。

Distributed System	分散システム

DoS Testing	DoS テスト

Dual Control	デュアルコントロール

注: ミサイル発射装置で二人が同時にスイッチを回さないと機能しないようなイメージ。

Due Care	デューケア

注:「妥当な注意」では、「Due Care」を指している用語として明白でないため、「デューケア」と訳す方が望ましい。

Due Diligence	デューデリジェンス

注: 同上の理由から、「デューデリジェンス」とする。

Dumpster Diving	ゴミ箱あさり

注: スカベンジャリングもよく聞く。「ゴミ箱あさり」だと、浮浪者がゴミ箱をあさっているような印象がある。

Durability	永続性

注: データベーストランザクションにおける 4 原則（ACID）の 1 つ。ACID は、A: Atomicity, C: Consistency, I: Isolation, D: Durability。

Dynamic Testing	動的テスト

注: Static Testing（静的テスト）と対語。

E

Elevation of Privilege	権限昇格

注: STRIDE 脅威分析モデルの"E"。

Elliptic Curve Cryptography	楕円曲線暗号

Emanation	放射

注: 電気的、機械的、光学的、音響的なものがあったりする。英語だと"electromagnetic"が長いので略されることが多いのではないか。

Embedded System	組み込みシステム

注: 業界だと「エンベ」と呼んだりもする。

Emergency Management Team	緊急事態管理チーム
Emergency Response Team	緊急事態レスポンスチーム
Encryption	暗号化
End-User	エンドユーザー
Enterprise Security Architecture	エンタープライズセキュリティアーキテクチャー
European Union Agency for Network and Information Security	欧州ネットワーク・情報セキュリティ機関（ENISA）

注: 正式には「欧州ネットワーク・情報セキュリティ機関」だが、ENISA という略称のほうが浸透している。

Evaluation Assurance Level	評価保証レベル
Event	イベント
Executive Management	経営幹部

注: 取締役クラス（C クラス）の上級管理職のこと。

Exploit	悪用する

注:「Exploit code」の場合は「エクスプロイトコード」の方が一般的になってきた。

Exposure Factor	危険係数

注: 一般的には暴露係数と訳されているが、意味的には危険係数のほうを強く推したい。1 回の災害で失われる資産の損害額がその元の資産価値の何割かという数字なので。SLE（単一損失予測）=AV（資産価値） x EF（危険係数）。

F

Facilitated Risk Analysis Process	ファシリテイテッドリスク分析プロセス(FRAP)

注: 定性的なリスク分析のこと。

Factoring Attack	因数分解攻撃
Fail Safe	フェイルセーフ
Fail Secure	フェイルセキュア
False Acceptance Rate	他人受入率
False Rejection Rate	本人拒否率
Fault Analysis	フォールト分析
Fault Tolerance	フォールトトレランス
Federal Information Processing Standard	連邦情報処理標準(FIPS)

注: FIPS の方が分かりやすい。訳すと何のことだかわからなくなるシリーズの一つ。

Federal Information Security Management Act	連邦情報セキュリティ管理法(FISMA)

注: これも FISMA の方が分かる。訳すとわからなくなるシリーズ。

Federated Identity Management	フェデレーション ID 管理

注: "Federated"を「フェデレーション」とするには若干抵抗があるが、わかりやすさを考えるとこれがいいと思う。

Fingerprint Authentication	指紋認証
Fire Suppression System	消火システム

Firewall	ファイアウォール
Five Rules of Evidence	５つの証拠規則

注: 証拠の５つのルールのこと。①Be authentic, ②Be accurate, ③Be complete, ④Be convincing, ⑤Be admissible。

Fraggle Attack	Fraggle 攻撃
Fragmentation	フラグメンテーション
Frequency Analysis	頻度分析

注: 機械翻訳だと「周波数分析」になってしまったりする。

Functional Testing	機能テスト
Fuzz Testing	ファジングテスト

注:「ファズテスト」よりも「ファジングテスト」が呼称として一般的。

Fuzzing	ファジング

G

Greylist	グレーリスト

注: Politically incorrect な言葉かどうか不明。また、言い換えるとしたときに、どのように言い換えるかも不明。

Grid Computing	グリッドコンピューティング
Guideline	ガイドライン

H

Hacking	ハッキング

Hand Recognition	掌形認証

注: 指紋で認証するわけではなく、手の形（掌形）で認証を行う方式。米国の空港で頻繁に訪米する外国人の入国審査を簡便化するために導入された事例がある。

Hash Function	ハッシュ関数

Help/Service Desk Personnel	ヘルプ/サービスデスク担当者

Heuristic Scan	ヒューリスティックスキャン

注: アンチウイルスソフトが実行ファイルを分析する手法で、パターンマッチング法とは違い実行ファイルを解析してウイルス特有の動作をしないか検出する方法。コードを静的に解析する方法と仮想的に実行して解析する方法の二種類がある。

Hierarchical Model	階層モデル

Hoax	デマウイルス (Hoax)

注: 通常のテキストメールであるためこれ自体はウイルスではないが受信者の不安を煽って受信者に通常ではない操作をさせたり、拡散させるためのチェーンメール的な要素を併せもつ。代表的なものに「"XXXXXX.exe" というファイルがあったら、すぐに削除しないとまずいよ。このウイルス、だいぶ流行っているみたいだから」というようなメールで OS 標準の重要なファイルを消去させるようなものがある。

Honeynet	ハニーネット

Honeypot	ハニーポット

Host-Based Intrusion Detection System	ホスト型 IDS

注: HIDS と略すこともある。N-IDS と違って、HIDS の場合は H-IDS とはあまり表記されない。

Hybrid Cloud	ハイブリッドクラウド

|

ICMP Redirect Attack	ICMP リダレクト攻撃
Identification Badge	ID バッジ
Identity as a Service	IDaaS (Identity as a Service)

注: CBK では「サービスとしてのアイデンティティ」としていたが、IDaaS という表現が普及してきたので、IDaaS とする。

Illegal Software	違法ソフトウェア

注: ライセンスを受けていないソフトウェアの意味らしいが、海賊版ソフトウェアと同じ意味かどうかは不明。

Implementation Attack	実装攻撃

注: 暗号モジュールに対する攻撃のことらしい。

Inbound	インバウンド

注: 内向きトラフィックのこと。日本に来る外国人のことではない。

Incident	インシデント

注: 「事故」や「事件」と訳すこともあるが、ここでは「インシデント」で統一する。

Incident Handling	インシデントハンドリング

注: Incident response が「事故対応」とするならば、Incident handling は「事故処理」になるが、あまりこの表現は見ない。

Incident Management	インシデント管理
Incident Response	インシデントレスポンス(IR)

注: Security incident を「セキュリティ事故」とすることはあるが、Incident response を「事故対応」としている例はあまり見ない。

Incremental Backup　　増分バックアップ

注: 増分バックアップは前回のバックアップからの差分だけをバックアップすること。一方、Differential Backup(差分バックアップ)は、前回のフルバックアップからの差分をバックアップすること。

Independent Audit　　第三者監査

注: 直訳だと「独立監査」だが、第三者監査の方が一般的。

Industrial Control System　　産業制御システム(ICS)

Inference　　推論

注: 一部の情報からその他の部分を推論する Inference Attack（推論攻撃）という攻撃手法もある

Information Classification　　情報の分類

注: ちなみに、Unclassified は、未分類(まだ分類していない)という意味ではなく、機密(Classified)ではない、という意味。

Information Disclosure　　情報漏洩

注: STRIDE 脅威分析モデルの"I"

Information Flow Model　　情報フローモデル

Information Lifecycle　　情報のライフサイクル

Information Owner　　情報オーナー

Information Security Continuous Monitoring　　情報セキュリティの継続的監視

Information Security Officer　　情報セキュリティ責任者

注: 部門毎の情報セキュリティ責任者の意味で、これを束ねているのが CISO という位置づけだと思われる。Police officer のときの officer は「職員」の意味だが、こっちの officer は偉い officer。

Information Systems Audit and Control Association　ISACA（Information Systems Audit and Control Association）

注: 旧来は「情報システムコントロール協会」と訳す場合もあったが、現在は日本の組織内でも ISACA としているようだ。

Information Systems Auditor　情報システム監査人

Information Systems Professional　情報システム専門家

Information Technology Security Evaluation Criteria　IT セキュリティ評価基準

注: ITSEC と略されることがある。

Initialization Vector　初期化ベクター

注: 初期化ベクトルと訳されることもある。暗号化の結果をばらつかせるためのランダムに生成されるビット列。

Insider Attack　インサイダー攻撃

Intangible Asset　無形資産

Integrated Development Environment　統合開発環境

Integration Testing　結合テスト

注: 結合テストの後に総合テスト(システムテスト)がある。結合テストの前に単体テストがある。手法の場合は""testing""で、テスト自体を意味する場合は""test""か。どちらにするか悩ましい。

Integrity　完全性

Intellectual Property Law　知的財産法

International Data Encryption Algorithm　IDEA（International Data Encryption Algorithm）

注: 共通鍵暗号方式の一つで DES よりも安全性の高い暗号方式を目指したがさほど普及しなかったらしい。

Intrusion Detection System	侵入検知システム(IDS)
Intrusion Prevention System	侵入防御システム(IPS)
Inventory Management	インベントリー管理
Invocation Property	呼び出し属性

注: Biba や Bell-LaPadula モデルで上位や下位のオブジェクトを呼び出す際の属性らしい。

Iris Recognition	虹彩認証
Isolation	隔離、分離、独立、独立性

注: Isolate する対象によって日本語の訳を適切なものにする必要がある。データベーストランザクションにおける 4 原則(ACID)：Atomicity（原子性）、Consistency（一貫性）、Isolation（独立性）、Durability（永続性）の 1 つ。

Iterative Model	反復型モデル

注: Waterfall ではなく、CI/CD みたいなものらしい。

」

Job Rotation	ジョブローテーション

注: 「配置転換」は計画的にやる印象が無いが、ジョブローテーションは計画的に行われる感じを受ける。敢えて日本語にするなら「計画的配置転換」か?

Jurisdiction	司法管轄権、司法権、法域

注: 司法機関が国内法を適用して具体的事案を処理し、判決を行う国家の権限のことをいう。CCSP では講師の意見で「法域」とした。司法の議論ではなく、地域ごとの法的違いや考慮事項に対する認識がセキュリティプロプロフェッショナルとして必要という意味で。Cloud Security Alliance にも合わせる。IPA の文書では「司法管轄権」、「司法権」としている。

K

Key Escrow **鍵の預託**

注: キーエスクローと訳す場合もあるが、今回はキーを全て鍵と訳すことにしたため鍵の預託とした。

Key Length **鍵長**

Key Recovery **鍵回復**

注: キーリカバリと訳す場合もあるが、今回はキーを全て鍵と訳すことにしたため鍵回復とした。

Keystroke Dynamics **キーストロークダイナミクス**

注: バイオメトリックスの一種でキーボードの叩き方で本人かどうか判別する識別方法。Key は Keyboard の Key なので、「鍵」にはしない。

Knowledge Management **ナレッジ管理**

Known Plaintext Attack **既知平文攻撃**

L

Layering **階層化**

注: ソフトウェアの階層化などで使われる。Ring 0 とかの話。

Least Privilege **最小権限**

注: 最小特権と訳されることもあるが、特権に限らず使われるため最小権限とした。

Likelihood **発生可能性**

Linear Cryptanalysis **線形解読法**

注: 差分解読法（Differential Cryptanalysis）と同様にブロック暗号やストリーム暗号を解析する際に使われる手法らしい。

Link Encryption **リンク暗号化**

注: 通信する二者間の経路上で一切復号されない End to end の暗号化通信と異なり、通信経路上の中間機器で復号され、再度暗号化されながら End に伝えられる方式。

Local Annual Frequency Estimate　現地年間頻度推定値（Local Annual Frequency Estimate）

注: 地域的な発生頻度の違い。CISSP のテキスト以外ではあまり見ない言葉。天気予報の世界では、地域的年間頻度予測と言うらしい。

Locard's Exchange Principle　Locard（ロカール）の交換原理

注: エドモンド・ロカール博士の交換原理。

Log Management　ログ管理

Log Management System　ログ管理システム

Logic Bomb　論理爆弾

注: 本当の爆弾とは違う。

Logical Controls　論理コントロール

注: 物理コントロールとの対比で使われる。

M

MAC Flooding Attack　MAC フラッディング攻撃

注: ARP テーブルをあふれさせる攻撃のこと。

Magnetic Stripe Card　磁気ストライプカード

注: 俗に言う「磁気カード」。

Malware　マルウェア

注: 悪意のあるソフトウェアのこと。

Mandatory Access Control　強制アクセス制御

注: "強制アクセス制御"を略すと「MAC」。「Media Access Control address」は通称 MAC アドレス。短縮して MAC と呼ぶと違いがわからない。

Mandatory Vacation　強制休暇

注: 金融機関での実施例が多いようである。嬉しい人もそうじゃない人もいるらしい。

Mantrap **マントラップ**

注: 一人ずつしか通過できないようにするものの一種。

Matrix-Based Model **マトリクスベースモデル**

注: Google で検索してもセキュリティの用語としては出てこない。CISSP にしか出てこない言葉かも知れない。

Maximum Tolerable Downtime **最大許容停止時間**

注: MTD とも。また、Maximum Allowable Downtime (MAD)とされることもある。日本語訳は一緒。

Mean Time Between Failures **平均故障間隔**

注: MTBF とも。

Mean Time to Failure **平均故障時間**

注: MTTF とも。

Media **媒体**

注:「メディア」とカタカナにすると放送などのメディアのイメージになる。

Meet-in-the-Middle Attack **中間一致攻撃**

注: 2DES が無い理由。バースデイパラドックス的なこと。

Message Digest **メッセージダイジェスト（MD）**

注: (一方向)ハッシュ関数とも言われる。

Metadata **メタデータ**

注: 日本語では表現しづらい。構造化されたデータに関係する言葉。

Metrics **メトリクス**

注:「メトリックス」にすると「マトリックス」みたいになる。

Microwave Sensor **マイクロ波センサー**

注: 英語で「microwave」と言うと電子レンジの意味。

Middleware **ミドルウェア**

Misuse Case　　ミスユースケース

注: 悪用や誤用を想定したテストのこと。

Mitigating Factor　　低減要因

注: mitigate を緩和、軽減と訳す場合もある。CBK では reduction を軽減、mitigation を低減として使いわけることとした。また、同様に、element を要素、factor を要因として使い分けることとした。

Mobile Device Management　　モバイルデバイス管理(MDM)

Monoalphabetic Cipher　　単一換字暗号

注: シーザー暗号など。

Multicast Brute Force Attack　　マルチキャスト総当たり攻撃

Multi-Factor Authentication　　多要素認証

注: MFA という表現も見かけるようになってきた。

Multilevel Lattice Model　　マルチレベルラティスモデル

注: セキュリティモデルの一つ。

N

Need to Know　　知る必要性

注: 知らなくていい人には知らせないようにする、という意味もあるが、「知る必要性」だとそれがうまく表現しきれない。「Need to Know」のまま使うのも一案。

Network Access Control　　ネットワークアクセス制御

Network Database Management Model ネットワークデータベース管理モデル

注: データベースの仕組みの一つ。最近は聞かない。

Network-Based Intrusion Detection System　　ネットワーク型 IDS

注: いわゆる普通の IDS。N-IDS や NIDS と略すこともある。

Neural Network　　ニューラルネットワーク

注: Deep learning の基本を説明するときに使われるぐらい。

nonce　　nonce

注: ”number used once”のこと。ナンスかノンスか呼び方は意見がわかれる。リプレイ攻撃を防ぐ目的や、ブロックチェーンで使われるらしい。

Noninterference Model　　非干渉モデル

注: セキュリティモデルの一つ。

Nonrepudiation (Non-Repudiation)　否認防止

注: ”Repudiation"は STRIDE 脅威分析モデルの”R"。

Null Cipher　　NULL 暗号

注: ヌル暗号と表現されることもある。

O

Object　　オブジェクト

注: オブジェクト指向に関する意味合いで使われるときと、サブジェクト-オブジェクトの文脈で使われるときとがある。

Object-Oriented Programming　　オブジェクト指向プログラミング

注: 当たり前すぎて最近聞かなくなった。

Officer　　責任者

注: CEO 等の文脈においてこのように考えると分かりやすいかも。Security officer や Police officer として使う場合は責任者ではない。

Once In-Unlimited Access　　1 回の無制限アクセス

注: 一度アクセスに成功したら、無制限でアクセス出来る。OIUA と略されることも有り。ゼロトラストの逆。

One-Time Pad　　ワンタイムパッド

注: 暗号方式の一つ。

One-Way Hash	一方向ハッシュ

Online Analytical Processing	オンライン分析処理

注: OLAP とも。“データ分析の手法”のような概念及びシステムらしい。

Open Systems Interconnection	開放型システム間相互接続(OSI)

Open Web Application Security ProjectOWASP(Open Web Application Security Project)	

注: OWASP Top 10 が有名。

Ordinary User	一般ユーザー

注: 特権ユーザー(privileged user)と比較するような文脈で使われる。

Organizational Memory	組織の知

注: 場当たり的だったり個人技でないようにするような意味。

Outbound	アウトバウンド

注: Inbound の反対。

Overlapping Fragment Attack	オーバーラッピングフラグメント攻撃

注: タイニー フラグメント攻撃とともにちょっと古い攻撃手法かも。

P

Passive Infrared Sensor	パッシブ赤外線センサー

注: パッシブだから赤外線は出さないらしい。ルパン三世を捉えられるかもしれない。センサーは千差万別。

Passive Monitoring	パッシブモニタリング

注: Proactive Monitoring の反対語。

Password Management	パスワード管理

Patch Management	パッチ管理

Payment Card Industry Data Security Standard PCI DSS

注: クレジットカード情報を保護するために策定されたもの。「PCI データセキュリティ基準」より「PCI DSS」の方が一般的になってきた。

Penetration Test　ペネトレーションテスト

注: 脆弱性診断では網羅的に脆弱性の調査を行い実際に悪用できるかどうかまでは確認しないが、ペネトレーションテストでは見つかった脆弱性を組み合わせるなどして侵入できるかまで試すようなイメージ。「ペンテスト」とも。

Perimeter Defense　境界防御

注: 最近、境界がわかりにくくなってきたとの意見もある。

Permutation　転字

注: 字を置き換えること。古典的な暗号の話で出てくる。

Personal Identification Number　PIN

注: 俗にいう、「暗証番号」

Personal Identity Verification　個人識別情報検証(PIV)

注: ID を発行する際の本人確認のこと（FIPS 201-2 で定義されている）。米国連邦政府の発行する「PIV スマートカード」が有名。

Personally identifiable information　個人識別情報（PII）

注: それにより個人が特定できる情報のことらしい。

Phishing Attack　フィッシング攻撃

Physical Asset　物的資産

Physical Controls　物理コントロール

Physical Security Personnel　警備員

注: 英語は「Guard」の方が一般的か。「Physical Security Personnel」という表現はそれほど目にしない印象。ちなみに、「ガードマン」は和製英語らしい。

Ping of Death	Ping of Death

注: 「PoD」と略されることもある。

Ping Scanning	ping スキャン

注: ping をブロックしているところも増えてきたので、役に立たなくなってきた。

Piracy	著作権侵害

注: もともとの意味は「海賊行為」だが、ここでは「著作権侵害」の意味になる。

Pirated Software	海賊版ソフトウェア

注: サブスクリプションモデルの普及でだいぶ減ってきた印象。

Plaintext	平文

注: 読み方は「ひらぶん」。

Playfair Cipher	Playfair 暗号

注: 「Lyon Playfair」さんが普及させたのでこの名前がついたらしい。

Point-of-Sale	POS

注: 直訳だと「販売時点」で、意味としては「販売時点情報管理システム」だが、POS の方が馴染みがある。

Policy	ポリシー

Polyalphabetic Cipher	多表式換字暗号

注: 「mono」が単一、「poly」が複数。複数の表を用いてアルファベットを置換する暗号方式なので「polyalphabetic cipher」。単一換字暗号と対比される。

Port Scanning	ポートスキャン

Portability	移植容易性

注: 一般には移植が容易であるという意味で使われることが多いが、Docker などのコンテナの世界では、アプリケーションが「そのまま」どこでも動作するという意味で使われる。

Prank	いたずら(prank)

注: ジョークソフトウェアのこと

Preservation	保全

Pretexting	なりすまし

注: 「Account takeover(アカウント乗っ取り)」ではなく、言葉巧みに相手を騙して別の人間であるように思わせること。ソーシャルエンジニアリング。

Preventative Controls	防止コントロール

注: 「予防」とする場合もあり。

Private Cloud	プライベートクラウド

注: 特定の組織専用のクラウドのこと。

Private Key	秘密鍵

注: 公開鍵暗号方式における、公開鍵に対応する鍵としての秘密鍵のこと。「共通鍵暗号方式」のことを「秘密鍵暗号方式」と言ったりすることもあるのでややこしい。「プライベート鍵」とすると明確にできるが、「公開鍵」と「プライベート鍵」だと対称性に欠けるという問題がある。

Privilege Management	特権管理

注: 「特権」と言ったときに、システムの管理者権限のことを言う場合、業務上の高権限(承認権限など)を言う場合などがある。ベンダによっては、全てのアカウントの権限管理のことを「特権管理」と言っていることもある。

Proactive Monitoring	プロアクティブモニタリング

注: 監視対象に対して何からのアクションを起こして状況を確認すること。反対語は Passive monitoring。類義語に Synthetic performance monitoring がある。

Probing Attack	プロービング攻撃

注: 暗号モジュールの周辺の回路を解析するタイプの攻撃らしい。

Problem Management	問題管理

注: 日本語の「問題」には、Problem も Question も対応するので訳す時に困る。テストの問題を管理するという意味ではない。

Procedure	プロシージャー、手順

注: ポリシー、スタンダード、の流れで話す時は「プロシージャー」の方が収まりがいい。単体の名詞として使うときはプロシージャーでも違和感無いが、文中に一般名詞として登場する場合は手順や手続きの方が短いし、しっくりくる。

Process Isolation	プロセス分離

注: 分離といっても、一つの物を分離させるのではなく、隔離の意味。しかし、「プロセス隔離」の表現は一般的でない。

Profile	プロファイル

注: CC の PP で使われたりする。

Protection	保護

注: 英語だと"protection"と"safeguard"の両方が使われる場合があるが、使い分けているのか不明。

Provisioning	プロビジョニング

注: 最近、「プロビジョニング」という表現を目にするようになってきた。

Public Cloud	パブリッククラウド

注: いわゆるクラウド。

Public Key	公開鍵

注: Key を「鍵」とするか「キー」とするかはいつも悩む。ここでは「鍵」で統一している。

Public Key Infrastructure	公開鍵基盤

注: 訳としては「公開鍵基盤」だが、PKI の方が馴染みがあるかも。

Purging	パージング

注: 記憶媒体のデータを完全に消去すること。

Q

Qualitative Risk Assessment　　定性的リスクアセスメント

注:「リスクアセスメント」を「リスク評価」にする場合もあり。

Quantitative Risk Assessment　　定量的リスクアセスメント

注: 同上

Quantum Cryptography　　量子暗号

注: 量子通信とワンタイムパッドを組み合わせた物を何故か量子暗号と呼ぶらしい。

R

Rail Fence　　レールフェンス暗号

注: シーザー暗号のような初期の暗号方式の一つ。英単語に「crypto」とはついていないが、暗号方式としてしか使わないので、日本語では暗号をつけることとする。ただ、試験問題の日本語化と考えると、「暗号」と付けると余計なヒントになってしまうのでダメかもしれない。

Rainbow Table　　レインボーテーブル

注: 昔はあまり目にしなかったが、検索の高度化によって身近なものとなり、わりと目にするようになってきた。

Random Frame Stress Attack　　ランダムフレームストレス攻撃

注: VLAN に対するアタックらしい。

Real User Monitoring　　リアルユーザーモニタリング

注: Web サイトのモニタリングをする方法の一つ。実際にユーザーとしてログインするものらしい。

Reciprocal Agreements　　互恵協定

注: 災害対応の時にお互いのリソースを譲り合う話。セキュリティ以外の文脈では、二国間の協定のことを指す。

Reconnaissance Attack　　偵察攻撃

注: 複数のツールを組み合わせてシステムの様々な部分を攻撃するものらしい。偵察というのに、攻撃、というのには違和感はある。

Recovery　　復旧

注: 「リカバリ」のままの表現も良く目にする。「回復」か「復旧」かという議論もあるが、「回復」は命があるものに使い、「復旧」はそれ以外に使う、と主張している人もいる。

Recovery Controls　　復旧コントロール

注: control は「統制」「制御」「管理策」「コントロール」などが候補になる。この場合は「コントロール」が収まりが良いと思う。

Recovery Point Objective　　目標復旧時点(RPO)

注: BCP 用語。略語の方が馴染みがあるのでカッコをつけて付記した。

Recovery Strategy　　復旧戦略

注: 英語で「strategy」は割と気軽に使うが、日本語で「戦略」とすると大げさに感じる。

Recovery Time Objective　　目標復旧時間(RTO)

注: 「復旧時間目標」という表現もある模様。これも、略語を付記した。

Rectangular Substitution Table　　長方形換字表

注: 「Rectangle」は「矩形」なので正方形も長方形も含む。「長方形」としてしまうと、正方形の換字表は含まれないことになってしまう…と思って調べたところ、長方形に正方形が含まれるかどうかは議論がある模様。

Reference Check　　リファレンスチェック

注: 人を採用する際に行うバックグラウンドチェックの一種。例えば、前の職場で一緒に働いていた人に聞いたりすること。日本ではあまり行われないが、アメリカでは比較的普通に行われる。

Reference Monitor　　参照モニター

注: 「リファレンスモニター」で検索すると、色や音の調整に関する用語として出てくる。

Registration Authority	登録局(RA)

注: PKI の文脈で出てくれば「登録局」でもわかるが、いきなり出てくるとわかりづらいかも。なので略語を付記した。

Remediation	是正、修正、改善、修復

注: 「修復」だと、もともと良かったものが悪くなり、元に戻す印象がある。「是正」は、もともと良かったかどうかにかかわらず正しくするイメージ。但し、「是正」だと「correction」に近い。監査の場面では「Remediation」を「改善」とする場合があるが、「是正」よりも「改善」の方が表現がソフトだから使われているのかもしれない。

Remote Access	リモートアクセス

Remote Access Trojan	リモートアクセス型トロイの木馬

注: 長いけど短くしようが無い。「トロイ」だけだと分かりづらいので、英単語には無いが「木馬」をつける。

Replay Attack	リプレイ攻撃

注: 「replay」は「再生」かと思ったら、再生は「play」だった。replay の日本語は「再演」らしい。

Reputation Score	レピュテーションスコア

注: Web サイトのレピュテーションスコアをもとに、通信が不審かどうかを判定するような時に使う。Web サイトの怪しさ、みたいな意味。

Requirement	要件

Resilience	レジリエンス

注: 最近この言葉を耳にすることが増えてきた。訳語として「強靱」が適切だと主張する人もいる。「強靱」の本来の意味は「しなやかで強いこと」なので、Resilience の意味と近いが、「鋼鉄のように強い」という印象があり、うまく伝わらないことが多い。

Response Team	レスポンスチーム

Restoration **復元**

注: 「リストア」も日常的に使われるが、「restoration」を「リストレーション」とはできない…。

Restore **復元する**

注: 「リストアする」でもアリだと思うが、「restoration」を「復元」と訳すとなると、「restore」は「復元する」になってしまう。

Retain **保持する**

注: 文書管理規定などで、どれぐらいの期間データを保持するかについて語るときに出てくる言葉。システムの場合、ログをどの程度保存しておくかといった文脈で出ることが多い。

Retention **保持**

注: 保持期間を最低保持すべき期間として捉えるか、その期間を超えたら消すべき期間として捉えるか、という議論もある。

Retinal Scanning **網膜スキャン**

注: Apple の Retina Display のおかげで「Retina」という単語自体も普及しつつある。

Rijndael **Rijndael**

注: AES となった暗号方式。

Ring Protection **リングプロテクション**

注: CPU の権限管理についての話。

Risk Acceptance **リスク受容**

注: JIS では「リスク保有」となったが、「リスク受容」の方がわかりやすいし、広く使われている。

Risk Appetite **リスク選好度**

注: 最近よく見る単語。日本語にしても意味がわかりづらい。

Risk Assessment **リスクアセスメント**

注: 「リスク評価」でもいいと思う。

Risk Avoidance **リスク回避**

注: リスクをゼロにする方法。

Risk Management **リスクマネジメント**

注: 「リスク管理」という場合もある。「リスクマネジメント」と「リスク管理」では使われる場面が異なるという噂も。

Risk Mitigation **リスク低減**

注: 「mitigation」には「軽減」「緩和」という日本語も対応するが、リスクには「低減」が合っていると思う。

Risk Transfer **リスク移転**

注: リスク対応の一つ。意味としては、リスク共有（Risk Sharing）と同じ。

Role-Based Access Control **ロールベースアクセス制御(RBAC)**

注: RBAC という略称のほうがよく知られているため、カッコ書きで追加した。

Root Cause Analysis **根本原因分析**

注: 根本原因解析という訳し方もあるが、「分析」という訳のほうが多いので、根本原因分析とした。

Running Key Cipher **ランニングキー暗号**

注: 連続鍵暗号、進行鍵暗号という訳があるが、あまり浸透していないため、カタカナにした。

S

Safe Harbor	セーフハーバー

注: セーフハーバー協定は、2000 年に制定された米欧間の越境データ移転に関する二者間協定。2016 年に、プライバシーシールドという枠組みに切り替わっているため、セーフハーバーは古い概念だよね、という意見が出た。

Safeguard	保護策

注: ISMS ではおなじみの管理策のこと。抑止、防止、検知、回復などの管理策のうち、防止や防御に関する管理策のイメージ。

Salami Scam	サラミ法

注: Scam を直訳すると「詐欺」になるが、不正行為のやり方と解釈するとサラミ法が一般的と考えられるため、「サラミ法」とした。ちなみに、英語は「Salami Slicing」の方が一般的のよう。

Salt	ソルト

注: ハッシュ等の演算をよりセキュアにするために、追加で入力される乱数のような値だが、パスワードのハッシュ化では、ソルトに加えてペッパーも加える場合がある。

Sandbox	サンドボックス

注: お砂箱でなく、サンドボックス。

Sanitize	サニタイズ

注: 消毒ではなく、サニタイズ。データの無害化の意味で使われたり、記憶媒体のデータを完全消去することを意味したりする。

Scoping	スコーピング

Secure Hash Algorithm	SHA (Secure Hash Algorithm)

注: SHA と略されることが多い。

Security Administrator　　セキュリティ管理者

注: Managerよりも、Administratorの方がシステムを実際に使っている人のイメージがあるが、両方とも日本語訳にしたときに「管理者」になってしまうから困る。…という話は、対訳集の作業の中で、延々と続く話題だったりする（そして、Manager と Administrator が出る度、「どっちだっけ？」となっている）。

Security Architect　　セキュリティアーキテクト

Security Architecture　　セキュリティアーキテクチャー

Security Audit　　セキュリティ監査

Security Awareness　　セキュリティアウェアネス

注: 直訳すると「セキュリティ意識啓発」だったが、「アウェアネス」という単語が浸透しているため、カタカナ表記にした。

Security Control　　セキュリティコントロール

注: セキュリティ制御でも、セキュリティ管理策でも、セキュリティ統制でもなく、セキュリティコントロールがしっくりくる。

Security Council　　セキュリティ委員会

注: 直訳すると、「セキュリティ評議会」だが、「評議会」が、一般企業では利用されない単語なので、イメージしづらいとの声があった。そこで、CBK の説明に立ち戻ったところ、情報セキュリティ委員会のような組織を意味しているように読めるため、「セキュリティ委員会」とした。ただし、委員会を英語にすると committee になるため、やや意訳している感がある。Council は第三者的な意味合いがあるので、単なる委員会より、第三者委員会の方が近いかも知れない。社内の委員会とは違うイメージ。

Security Event Information Management　　セキュリティイベント情報管理

Security Event Management　　セキュリティイベント管理

注: セキュリティイベント情報管理と何が違うのかよくわからない。

Security Guard　　警備員

注:「ガードマン」は和製英語らしい。

Security Information and Event Management　　SIEM（Security Information and Event Management）

注: 前は Security Event and Incident Management(SEIM)と呼ばれていたこともあるが、Incident だけではなく、より広く Information を管理する概念として SIEM となった経緯があるらしい。

Security Manager　　セキュリティマネージャー

注: Security Administrator（セキュリティ管理者)とは別。オペレーションはしないイメージ。

Security Practitioner　　セキュリティ実務者

注: 辞書だと開業医や弁護士が出てくるが、Practitioner（手を動かして働く人)というイメージから、「セキュリティ実務者」とした。AWS の資格ではカタカナのまま「クラウドプラクティショナー」としている。

Security Principle　　セキュリティ原則

Security Professional　　セキュリティ専門家

Senior Management　　経営陣

注: 直訳すると上級管理者だが、違和感があるため、やや意訳して「経営陣」とした。日本の会社では、Senior Management や、Executive Management に該当する役職がないため、いまいちイメージしづらいという声があった。

Sensitive　　機微な

注: 「機密な」「機密の」と訳しがちだが、機密性(Confidentiality)との訳の混同を避けるため「機微な」とした。

Separation of Duties　　職務の分離

注: 職務分掌よりも職務の分離の方がコンプライアンス的要素を強く感じる。SoD と略すこともある。Segregation of Duties も同じ意味のように思える。

Service Level Agreement　　SLA (Service Level Agreement)

注: 直訳では、「サービスレベルアグリーメント」だが、SLA という略称のほうが浸透しているため、略称を正とした。

Service Organization Control Report　　SOC レポート

注: SOC レポートの SOC と言われれば内部統制の関係だよね、と理解できるので、「SOC レポート」という訳にした。SOC だけだと Security Operation Center の SOC と紛らわしい。

Session Hijacking　　セッションハイジャック

Session Management　　セッション管理

Shoulder Surfing　　ショルダーサーフィン

注: ネットサーフィンという言葉も最近聞かなくなった。ショルダーハッキングの方がわかりやすい。

Side Channel Attack　　サイドチャネル攻撃

Signature Analysis　　シグネチャー分析

注: パターンマッチングのことらしい。

Signature Dynamics　　署名ダイナミクス

注: 日本語訳としては、特段、議論はなかったが、そもそも、「署名ダイナミクス」が何を指すのか、がわからず、盛り上がった。署名ダイナミクスとは、クレジットカードの署名をするパッドで使われる技術のことで、このパッドの写真を見た際に、「ああ、これなの？！」と納得の声が。一方で、「図や写真があれば一発でわかるのに…」という意見もあった。

Signature Scanner　　シグネチャースキャナー

注: この日本語訳からはわかりづらいが、パターンマッチング方式のウイルス対策ソフトのこと。

Simple Integrity Property　　単純完全性属性

注: この用語を聞いてもピンとこないが、「Biba モデル」と言われれば皆、納得した。そして、「Biba モデル」がなにか、と言われると、皆、忘れてしまっていた(CISSP 取得時の勉強のときには覚えていたのに…)。

Simple Security Property	単純セキュリティ属性

注: この用語を聞いてもピンとこないが、「Bell-LaPadula モデル」と言われれば、皆、納得した。

Single Factor Authentication	単一要素認証

注: 直訳では「１要素認証」だが、「単一」のほうが、弱いイメージがあっていいので、「単一要素認証」とした。

Single Loss Expectancy	SLE(Single Loss Expectancy)

注: 直訳では、「単一損失予測」だが、SLE という略称のほうが浸透しているため、略称を正とした。

Single Point of Failure	単一障害点

注: SPoF と略すこともある。

Single Sign-On	シングルサインオン

注: SSO と略すこともある。

Skimming	スキミング

Smurf Attack	Smurf 攻撃

注: 体が小さいキャラクターがたくさんいるイメージなのでスマーフと名付けられたらしい。なぜシンプソンズではなかったのかは不明。

Sniffing	スニッフィング

注: スニッフィングという用語は、ネットワーク技術において登場する場合、悪い意味は含まれないが、情報セキュリティ技術の文脈では、「盗聴」の意味合いが強くなる。「盗聴」と訳す場合もあるが、ここでは、もとの意味に近づけるよう、「スニッフィング」とした。

Social Engineering	ソーシャルエンジニアリング

注: 直訳すると「社会工学」だが、それだと意味がわからない。

Software Assurance	ソフトウェアアシュアランス

注: 直訳では「ソフトウェア保証」だが、「アシュアランス」という単語が浸透しているため、カタカナ表記にした。

Software Defined Network	SDN(Software Defined Network)

注: 直訳では、「ソフトウェア定義ネットワーク」だが、SDN という略称のほうが浸透しているため、略称を正とした。

Software Development Life Cycle	ソフトウェア開発ライフサイクル

注: SDLC と略すこともある。

Something You Are	あなたが何であるか

注: 一般的な翻訳であれば、「本人認証」などが該当するが、CBK としては、「あなたが何であるか」で統一されているため、それにならった。Something You Are、Something You Have、Something You Know は認証の 3 要素。"What You Are"とすることもある。

Something You Have	あなたが持っているもの

注: 一般的な翻訳であれば、「所有物認証」などが該当するが、CBK としては、「あなたが持っているもの」で統一されているため、それにならった。"What You Have"とすることもある。

Something You Know	あなたが知っているもの

注: 一般的な翻訳であれば、「知識認証」などが該当するが、CBK としては、「あなたが知っているもの」で統一されているため、それにならった。"What You Know"とすることもある。

Source Code Analysis Tool	ソースコード分析ツール

Spam	スパム

注: Hormel 社の登録商標である「SPAM」(すべて大文字)から由来しているのは有名な話だが、それと区別するために、迷惑メールはすべて小文字の「spam」とする、という話で盛り上がった。

Spanning-Tree Attack	スパニングツリー攻撃

注: L2 プロトコルでの、可用性に対する攻撃。

Split Knowledge	知識分割

注: 割り符みたいなもの。

Spoofing	なりすまし

注: STRIDE 脅威分析モデルの"S"。

Spyware	スパイウェア

Standard	スタンダード、標準

注: 直訳すると「標準」で、ISO Standard を ISO 標準とするなど、「標準」が適切な文脈もある。ポリシー、スタンダード、プロシージャと出てくるときは、スタンダードが適切。

Standard Annual Frequency Estimate	標準年間頻度推定値（Standard Annual Frequency Estimate）

注: 日本語訳の「標準年間頻度推定値」だけでは意味がわかりづらいのだが、かといって適切な日本語訳も見つからないので、日本語訳の後ろに英文も追加。

State Attack	状態攻撃

注: ステータスに対する攻撃の意味なのだが、レースコンディションのほうが有名かも（レースコンディションは、基本情報処理技術者試験の午前問題でよく出てくる）。

State Machine Model	状態マシンモデル

Stateful Matching	ステートフルマッチング

注: ファイアウォールで出てくる技術用語のこと。

Statement on Auditing Standards	SAS(Statements on Auditing Standards)

注: 直訳では、「監査基準報告書」だが、SAS という略称のほうが浸透しているため、略称とした。

Static Binary Code Analysis	静的バイナリーコード分析

Static Source Code Analysis	静的ソースコード分析

Static Testing	静的テスト

Steganography	ステガノグラフィー

Stream-Based Cipher	ストリームベース暗号

注: 一般的には「ストリーム暗号」。「ストリームベース暗号」は CISSP 関連でしか発見できない。

Strong * Property	強化*属性

注: Biba や Bell-LaPadula 完全性モデルを発展させたもの。「*」は「スター」と読む。

Structural Testing	構造テスト

注: ソフトウェアの構造をテストすることらしい。

Structured Walk-Through Test	構造的なウォークスルーテスト

注: 「構造化ウォークスルー」とも言う。BCP の訓練で出てくる。

Subject	サブジェクト

注: 「オブジェクト」に対する「サブジェクト」。オブジェクトにアクセスする主体の意味。なお、GDPR のデータサブジェクトは個人情報の主体の意味。主体と訳す文献も多いが、ここはサブジェクト／オブジェクトで統一したい。

Substitution Cipher	換字暗号

Surviving Site	予備サイト

注: BCP における代替サイトのひとつ。

Symmetric Cryptography	対称暗号

Symmetric Key Encryption	対称鍵暗号

SYN Flood Attack	SYN フラッド攻撃

Synthetic Performance Monitoring	シンセティック性能監視

注: 「シンセティックモニタリング」または「合成監視」とも言う。実際のユーザーが Web サイトにアクセスするかのように、Web パフォーマンスに関する値を計測することらしい。

System Operator	システムオペレーター
Systems Administrator	システム管理者

注: Manager は「マネージャ」、Administrator は「管理者」とした。

T

Table-top Exercise	机上演習

注: Drill、Exercise、Training とあるが、それぞれ違うものらしい。Exercise は参加者が手を動かす、Drill は繰り返し行って体に覚え込ませる(訓練)、Training は実習・研修・育成といった感じ。

Tailgating	テールゲーティング

注: 許可を得ていない人が許可を得ている人に続いて侵入すること。似た概念に「ピギーバッキング」というものがあり、許可を得ている人が許可を得ていない人を連れて通過することや、許可を得ている人が許可はある人を正当な手続きを得ずに入れてしまう(異常イベント検知の対象になる)ことなどを意味するらしい。最初に入る人が同意しているのがピギーバッキング、同意していないのがテールゲーティングという説もある。また、テールゲーティングは、後から入る人の立場からの言葉で、ピギーバッキングは、最初に入る人の立場からの言葉、という意見も出たが、結局良く分からなかった。

Tailoring	テーラリング

注: セキュリティの評価のところで出てくる言葉。スコーピングとセットで覚える。

Tampering	改ざん

注: STRIDE 脅威分析モデルの"T"。

Tangible Asset	有形資産

注:「無形」に対する「有形」。

Targeted	標的型

注: なぜか APT は Advanced Persistent Threat なのに「標的型攻撃」と訳される。

TCP Sequence Number Attack	TCP シーケンス番号攻撃

Teardrop Attack	Teardrop 攻撃

注: Syn Flood（洪水）ほどは貯まらないから、Teadrop（涙のしずく）が貯まるらしい。

Technical Controls	技術コントロール
Test and Evaluation Strategy	テストと評価の戦略
Threat Matrix	脅威マトリクス
Threat Modeling	脅威モデリング
Threat Surface	脅威サーフェス

注:「脅威面」という意見も出たが、「面」では surface の意味を表現しきれていないのでサーフェスとした。

Time Domain Reflectometry	時間領域リフレクトメトリー

注:「時間領域反射率測定法」とも言う。物理セキュリティの用語。ケーブルを曲げられたり切断されたりした位置を検出できるものらしい。

Token	トークン
Tracking	トラッキング、追跡

注: 文脈によって２つの訳を使い分けるとよい。意訳になるが、「把握」としたほうがわかりやすい場合もあるかもしれないが、実際には「把握」に時間軸の概念が含まれるイメージ(継続的把握、のような感じ)。良い言葉があったら教えてください。

Trade Secret	営業秘密

注:「企業秘密」を保護する法律である不正競争防止法で「営業秘密」という言葉を使っている。

Trademark Law	商標法
Transient Electromagnetic Pulse Surveillance Technology	テンペスト(電磁波盗聴)

Transmission Control Protocol	TCP (Transmission Control Protocol)

Transposition Cipher	転置暗号

Trapdoor	トラップドア

注: バックドアと同義語みたいな感じ。

Triage	トリアージ

注: もとは葡萄を仕分けることを意味するワイン用語(フランス語)で、その後救急医療の世界で使われるようになり、IT セキュリティの世界にもやってきたらしい。

Trojan	トロイの木馬

注: 英語では馬が入っていないが、木馬をつける。ただ、「トロイ」だけで使うこともある。

Trusted Third-Party Model	信頼できるサードパーティーのモデル

Two factor authentication	二要素認証

注: 二段階認証とは違う言葉。

U

Uninterruptible Power Supply	無停電電源装置(UPS)

Use Case	ユースケース

User Datagram Protocol	UDP (User Datagram Protocol)

Utility	ユーティリティ

注: 水道・電気など設備の意味で使われるときと、ツールのような意味で使われるときがある。

V

Validation	**妥当性確認**

注: 「検証」としたくなるが、Verification（検証）と使い分けたいので、異なる訳語を当てることとした。

Vascular Pattern Recognition	**血管パターン認証**

注: 直訳すると血管パターン認証だが、聞いたことが無い。日本では静脈認証の方が一般的。

Ventilation	**換気**

注: 昨今のコロナ禍では重要な用語。

Verification	**検証**

注: Validation（妥当性確認）と区別する。

Virtual Private Network	**仮想プライベートネットワーク(VPN)**

Virtualization	**仮想化**

Voice Recognition	**声認証**

注: 「音声認識」は、しゃべった言葉を理解すること。「声認証」は、しゃべった声が誰のものかを認証すること。声紋認証とたぶん同じ。

Vulnerability	**脆弱性**

注: 読み方注意。

Vulnerability Assessment	**脆弱性評価**

Vulnerability Scanning	**脆弱性スキャン**

Vulnerability Testing	**脆弱性診断**

W

War Dialing **ウォーダイヤリング**

注: 死語だと思っていたが、Zoom ミーティングに対するブルートフォースを「ウォーダイアリング」と呼ぶこともあるらしい。

Waterfall **ウォーターフォール**

注: 古くからある開発手法。

White-Box Testing **ホワイトボックステスト**

注: ここでの White は見ることができる、という意味で使っているので、Politically Correct らしい。

Whitelist **ホワイトリスト**

注: Politically incorrect な言葉。Whitelist は Allow List(許可リスト)、Blacklist は Deny List(禁止リスト)が正しいらしい。マンホールをメンテナンスホールと言うのと同じ。

Wireless Network Testing **無線ネットワーク診断**

Work breakdown structure **WBS (Work breakdown structure)**

注: 作業分解構成図と言うこともあるらしい。

Work Factor **ワークファクター**

注: 仕事因子、作業因子とも言うらしいが、わかりづらい。ある目的を果たすために必要となるコストや労力のこと。たとえば、暗号解読にかかる計算コストや所要時間、建物の高い壁を乗り越えて侵入するための労力など。これを大きくすることで悪意あるセキュリティ侵害をあきらめさせることができる。

Worm **ワーム**

注: WORM だと Write Once Read Many(記録媒体)の意味になる。

Z

Zachman framework	**Zachman フレームワーク**
Zero-Day	**ゼロデイ**
Zero-Hour	**ゼロアワー**

注: ゼロデイのなかま

Zombie Program	**ゾンビプログラム**

注: ゾンビプロセス(Kill しても消えないプロセス)ではない。BOT 的なもの。

*

*** Integrity Property**	***完全性属性**
*** Security Property**	***セキュリティ属性**
*** Property**	***属性**

注: セキュリティモデル(Bell-LaPadula 機密性モデル, Biba 完全性モデル)に関する言葉。IPA の文書では「*特性」と表現されている。