暗号・認証勉強ノート

2023 年 10 月 12 日

目次

第 I 部
サイバーセキュリティ概論

1　セキュリティの要件

情報セキュリティとは，コンピュータおよび通信システムにおいて，データが許可なく漏洩されたり変更されたりすることを防ぐことである．情報セキュリティでは情報の機密

性，完全性，可用性を維持する必要がある．

1.0.1 Confidentiality (**機密性**)

認可されていないものが情報にアクセスできないようにすること．

1.0.2 Integrity (**完全性**)

情報とその処理方法が，改竄や消去されずに正確に完全に残っている状態を保護すること．

1.0.3 Availability (**可用性**)

認可された利用者が必要な時に情報に確実にアクセスできること．

要件	求められる特性	必要な暗号技術
機密性	データの秘匿性	暗号化・認証
完全性	データの正確性	メッセージ認証符号・署名
可用性	データへのアクセスしやすさ	秘密分散

セキュリティの拡張概念 Authenticity (真正性) ユーザー・プロセス・システムなどの情報または資源の身元が主張通りであること，偽物がまぎれていないことを保証すること Accountability (責任追跡性) システムがおかしな挙動をしたり，攻撃されたりしたときに，起きたことやその原因を追跡できること

Non-repudiation (否認防止性) ある操作や事象を後になって否定されないよう証明すること

Reliability (信頼性) システムが意図している操作と結果の間に整合性があること

セキュリティにおける操作を定義する：Authentication (認証) 相手が本人かどうか確かめること，情報が変えられていないことの確認が目的

Signature (署名) メッセージや情報の作成者が確かにそれらを作成したことを示すものなりすまし，改竄，否認を防ぐためのもの

Verify (検証) 署名が本当かどうかを確かめること

2　デジタル署名

正規の証明書の場合 1. アリスが公開鍵と秘密鍵を作成する 2. アリスが公開鍵とその所有者の情報をセットにし，CA (Certificate Authority，認証局) へ送信する．証明情報と公開鍵の二つをまとめて，署名前情報と呼び，また，署名前情報を記述するためのフォーマットを CSR と呼ぶ．- 証明書の証明情報には，シリアルナンバー，有効期限，証明者情報，被証明者情報などが組み込まれる．- CSR: 認証局に対して証明書を作ってくださいというフォーマット csr には公開鍵やその所有者の情報が書いてある．3. 認証局 (CA) も公開鍵と秘密鍵を持っている．ここで，CA は CSR に電子署名を行う．そのために，まず，CSR をハッシュ化し，メッセージダイジェストを作成する．次に，ダイジェストを CA の秘密鍵で暗号化する．これが電子署名となる．署名前情報と CA による電子署名がセットとなり，電子証明書となる．これを公開鍵証明書という．ここで，秘密鍵は承認の印鑑となっていることをイメージするとよい．4. 認証局がサーバー証明書をアリスへ送り返す．5. ボブがサーバーへ接続する 6. サーバーは証明書を渡す 7. サーバー証明書が信用できる CA で発行されていれば，接続サーバーに信用してもらい，接続することができる．まず，ボブは CA の公開鍵を使って，電子署名を復号する．そして，署名前情報をハッシュ化し，メッセージダイジェストを作成し，復号したダイジェストと比較することで，アリスの公開鍵が正しいかを検証できる．

正規の証明書の場合 1. サーバー側で公開鍵と秘密鍵を作る 2. CSR を作成し，認証局へ送信- CSR: 認証局に対して証明書を作ってくださいというフォーマット csr には公開鍵やその所有者の情報が書いてある．3. 認証局 (CA) も公開鍵と秘密鍵を持っている．CSR をもとに CA の秘密鍵を使ってサーバー証明書を作成する．ここで，秘密鍵は承認の印鑑となっていることをイメージするとよい．4. 認証局がサーバー証明書をサーバー側へ送り返す．5. ユーザー (クライアント) がサーバーへ接続する 6. サーバーは証明書を渡す 7. サーバー証明書が信用できる CA で発行されていれば，接続サーバーに信用してもらい，接続することができる．

オレオレ証明書の場合証明書を発行し，接続する流れは変わらないが，認証局にサーバー証明書の発行を希望するサーバー自身が使われていることが正規の場合と違う．サーバー自身を認証局に用いる場合，社会的信頼がないことに注意.

セキュリティ

認証

システム監査について

システム監査のフレームワークシステム監査- 監査対象からは独立した立場 (第三者の立場) かつ専門的な立場のシステム監査人が行う- 情報システムを次の観点から評価する- 信頼性- 安全性- 効率性そして，各コントロールが有効に機能していればそれを保証し，問題点を勧告したり，助言を行う一連の活動のこと

システム監査のワークフロー 1. 監査依頼監査依頼者がシステム監査へ依頼をする 2. 調査 1. システム監査は監査の目的，監査対象，そして実施すべき監査手続きの概要を明示した監査計画書を策定する 2. 行為規範であるシステム監査基準に則して監査を実施するこのとき，システム管理基準を監査上の判断の尺度とする．3. 監査報告監査実施後，システム監査人は，監査依頼者へ監査の結果を監査報告書にまとめて提出する．4. 改善支持 (監査依頼者)・助言 (システム監査) 監査結果に基づいて監査依頼者が監査対象へ改善指示を，システム監査人は指導・助言を行う．システム監査人は行動までは支持することができない.

3 基本的な定義

定義 3.1（認証） グラフ G とは**頂点集合** $V(G)$ と**辺集合** $E(G)$ からなる図形のことである．頂点集合 $V(G)$ とは**頂点 (vertex, site)** あるいは**点**と呼ばれる要素の集合である．また，辺集合 $E(G)$ とは**辺 (edge, bond)** と呼ばれる頂点の 2 元集合の集合からなるものである．辺 $e \in E(G)$ は，頂点 u, v を用いて $e = u, v$, $e = uv = vu$ で表される．ここでは，$e = u, v$ で辺を表す.

頂点集合，辺集合がともに有限集合であるグラフを**有限グラフ**という．グラフ G の頂点数 $|V(G)|$ を G の**位数 (order)**，辺数 $|E(G)|$ を G のサイズ (size) という.

グラフには，無向グラフと有効グラフの 2 種類がある.

定義 3.2（無向グラフ） 辺が，節点 2 要素からなる集合 $\{u, v\}$ で表されるとき，G は**無向グラフ (undirected graph)** であるという．無向グラフは向きのないグラフであり，単にグラフと呼ぶ.

定義 3.3（有向グラフ） 辺に向きのあるグラフ D は，**有向グラフ (directed graph)** と呼ばれ，頂点集合 $V(D)$ と**弧 (有向辺)** と呼ばれる頂点の順序対 $\{u, v\}$ の集合 $A(D)$ (**弧集合**) からなる.

定義 3.4（端点，隣接，接続） グラフ G の頂点 u と v が辺 e で結ばれているとき，頂点 u と v とは**隣接 (adjacent)** するという．辺 e は頂点 u, v と**接続する**といい，頂点 u, v

を辺 e の**端点 (edge)** という．また，頂点 v に隣接する頂点全体の集合 v の近傍といい，$N_G(v)$ で表す．辺 e_1 と e_2 が同一の頂点 u に接続しているとき 2 辺は隣接するという．

グラフ G のある接点 v に接続する辺の個数を**次数 (degree)** といい，$\deg_G(v)$ または G が明らかなときには単に $\deg(v)$ と表す．有向グラフの頂点の次数は，入次数 (いりじすう，in-degree) と出次数 (でじすう，out-degree) に分けて定義される．

定義 3.5（入次数，出次数） G が有向グラフであるとき，節点 v へ入る辺の個数を**入次数 (in-degree)** といい，$\deg^{\mathrm{in}}_G(v)$ または，$\deg^{\mathrm{in}}(v)$ と表す．一方，節点 v から出る辺の個数を**出次数 (out-degree)** といい，$\deg^{\mathrm{out}}_G(v)$ または，$\deg^{\mathrm{out}}(v)$ と表す．明らかに，$\deg(v) = \deg^{\mathrm{in}}(v) + \deg^{\mathrm{out}}(v)$ であり，辺の個数が保存していることがわかる．

3.1 木構造

定義 3.6 G が無閉路 (閉路を含まない) グラフは森，林という．また，G が無閉路かつ連結グラフであるとき，G を**木 (tree)** という．特に，有向グラフ G が木であるとき，G を**有向木 (directed tree)** という．

定義 3.7（根付き木，二分木） 有向木 $T = (V, E)$ が一つの接点 $r \in V$ について，入次数が 0 であり，その他の各 $v \in V - \{r\}$ について入次数が 1 であるとき，T を**根付き木 (rooted tree)** といい，r を**根 (root)** という．(これは入次数 0 の頂点をちょうど 1 個もち，ほかの頂点の入次数がすべて 1 であるということである．) 各節点 (ノード点) の出次数が高々 2 である根付き木のことを**二分木 (binary tree)** という．

第 II 部
暗号の基本

4 統計的機械学習理論の基礎 - データ生成モデルの再現

暗号とは平文，暗号文，鍵，暗号化，復号の 5 つの成分から成り立つ．
平文 m 暗号文 c, 鍵 k, 鍵 k による暗号化を $E_k(\cdot)$, 鍵 k による復号化を $D_k(\cdot)$

参考文献