入門 サイバーセキュリティ 理論と実験

～ 暗号技術・ネットワークセキュリティ・
ブロックチェーンから Python 実験まで ～

博士（情報科学） 面 和成 【著】

コロナ社

ま　え　が　き

サイバーセキュリティに関する優れた書籍は数多くあります。しかし，サイバーセキュリティの分野は非常に広範であるためか，サイバーセキュリティの理論から応用・実験までを扱う書籍は数少ないと感じます。また，「暗号技術」から「ネットワークセキュリティ」，さらには「ブロックチェーン」を一つの土俵で扱うような書籍も，決して多くはないと考えています。

本書は，暗号技術およびネットワークセキュリティに関する理論と応用のトピックスに加えて，Python 等を使用した 8 種類のセキュリティ実験を盛り込んでおり，暗号技術とネットワークセキュリティの両面からサイバーセキュリティの理解の定着を図ります。想定する読者は，理工系の大学・大学院生に加えて，ICT（Information and Communication Technology）システムの構築・運用に携わる方々です。

ブロックチェーンはデータの耐改ざん性を保証する暗号技術とデータの高可用性を保証するネットワークセキュリティに関連する新しい技術であり，近年はサイバーセキュリティの分野でも注目を集めています。ブロックチェーンを真に理解するには暗号技術とネットワークセキュリティの両面の理解が必須であり，本書はこれらの基本的な技術を学ぶことができるようになっています。

本書では，まず 1 章においてさまざまなサイバー脅威を知ることによってサイバーセキュリティの重要性を理解し，2 章でサイバーセキュリティの考え方や限界など，サイバーセキュリティの全体像を学びます。3 章では，暗号や認証，秘密分散などに用いられる数学の基礎について学びます。4 章以降では，サイバーセキュリティの具体的な話題をとりあげ，「暗号の基本技術（4 章）」，「認証の基本技術（5 章）」，「バイオメトリクス（6 章）」，「秘密分散（7 章）」，「ネットワーク侵入防御（8 章）」，「統計的不正アクセス検知（9 章）」，「VPN

(10 章)」,「暗号資産とブロックチェーン（11 章)」,「ブロックチェーンのセキュリティ（12 章)」を習得していきます。これまでのサイバーセキュリティに関する書籍が，これらのうちの一部をとりあげるだけであったのに対して，本書はこれらの話題すべてを 1 冊の本にまとめて網羅的に扱っています。さらに，上記のような幅広い話題を取り扱うだけでなく，Python 等を使用した 8 種類のセキュリティ実験についてコード例とともに掲載しています。本書のみでサイバーセキュリティとその周辺技術を体験し，十分に理解ができるように配慮されていることが最大の長所といえるでしょう。

本書の執筆にあたっては多くの方にご支援をいただきました。特に，コロナ社の皆様には大変お世話になりました。この場を借りて感謝致します。また，面研究室の大学院生・大学生とのサイバーセキュリティの研究に関するこれまでの議論も本書の執筆に役立っています。最後に，本書の出版に関係したすべての人に感謝致します。

2021 年 1 月

面　和成

本書の URL は，すべて 2021 年 1 月現在である。また，本書に登場するソースコードはコロナ社書籍ページ https://www.coronasha.co.jp/np/isbn/9784339029178/ にて公開している。

目　　次

1. サイバー脅威

1.1　サイバー空間における基礎知識 …… 1
1.2　不正アクセス …… 2
1.3　権限奪取 …… 4
1.3.1　パスワードクラック　4 ／ 1.3.2　バッファオーバーフロー　6
1.4　マルウェア …… 8
1.5　サービス停止攻撃 …… 10
1.5.1　IP スプーフィング　11 ／ 1.5.2　DoS 攻撃　11 ／ 1.5.3　DDoS 攻撃　11 ／ 1.5.4　DRDoS 攻撃　12
1.6　Web の脅威 …… 13
1.6.1　違法サイト　13 ／ 1.6.2　フィッシング詐欺　13 ／ 1.6.3　ドライブバイダウンロード攻撃　14 ／ 1.6.4　DNS キャッシュポイズニング　15 ／ 1.6.5　中間者攻撃　16
1.7　組織内ネットワークにおける脅威 …… 17
1.7.1　組織内での盗聴　17 ／ 1.7.2　標的型サイバー攻撃　18 ／ 1.7.3　ファイアウォールの限界　19
1.8　実験 A：パスワードクラック …… 19
引用・参考文献 …… 21

2. サイバーセキュリティ概論

2.1　セキュリティリスク …… 22

2.1.1 情報資産 23 / 2.1.2 脅威 23 / 2.1.3 脆弱性 24
2.2 リスクマネジメント …… 25
2.2.1 リスク評価 25 / 2.2.2 リスク対応 25
2.3 セキュリティ対策に向けて …… 26
2.3.1 セキュリティ対策の限界 27 / 2.3.2 セキュリティ対策の考え方 29 / 2.3.3 多層防御 30
2.4 セキュリティの３要素 …… 31
2.5 ケルクホフスの原理 …… 32
2.6 暗号技術の安全性と危殆化 …… 33
引用・参考文献 …… 35

3. 数学的準備

3.1 初等整数論 …… 36
3.1.1 ユークリッドの互除法 37 / 3.1.2 拡張ユークリッドの互除法 38 / 3.1.3 数の世界を広げる 39 / 3.1.4 合同と乗法逆元 40 / 3.1.5 便利な定理 43
3.2 暗号技術に利用する基本的な問題 …… 43
3.2.1 離散対数問題 44 / 3.2.2 素因数分解問題 44
3.3 中国の剰余定理 …… 44
3.4 ベイズ統計学 …… 46
3.5 情報量とエントロピー …… 47

4. 暗号の基本技術

4.1 古典暗号 …… 50
4.1.1 シーザー暗号 50 / 4.1.2 バーナム暗号 51
4.2 攻撃者のモデル …… 51

4.3　共通鍵暗号（対称鍵暗号）……52
4.3.1　ストリーム暗号　53 ／　4.3.2　ブロック暗号　54
4.4　公開鍵暗号（非対称鍵暗号）……58
4.4.1　素因数分解問題ベースの暗号　59 ／　4.4.2　離散対数問題ベースの暗号　60
4.5　鍵　共　有……61
4.5.1　基本的な鍵共有法　61 ／　4.5.2　DH 鍵共有法　61
4.6　ハイブリッド暗号……62
4.7　実験 B：RSA 暗号の common modulus attack……63
引用・参考文献……65

5.　認証の基本技術

5.1　暗号学的ハッシュ関数……66
5.1.1　バースデイパラドックス　66 ／　5.1.2　暗号学的ハッシュ関数　67 ／
5.1.3　SHA　68
5.2　暗号学的ハッシュ関数の応用……68
5.2.1　コミットメント　69 ／　5.2.2　ハッシュチェーン　69 ／　5.2.3　マークルツリー　70
5.3　メッセージ認証コード……71
5.3.1　ブロック暗号を用いた構成法　72 ／　5.3.2　ハッシュ関数を用いた構成法　72
5.4　ディジタル署名……73
5.4.1　素因数分解問題ベースの署名　74 ／　5.4.2　離散対数問題ベースの署名　74
5.5　ユ ー ザ 認 証……75
5.5.1　パスワード認証　75 ／　5.5.2　チャレンジレスポンス方式　76 ／
5.5.3　ワンタイムパスワード方式　77
5.6　公開鍵認証基盤……78
5.7　実験 C：SHA-256 の部分的衝突……82
引用・参考文献……83

6. バイオメトリクス

6.1 バイオメトリクスとは …… 84
6.2 バイオメトリクス認証 …… 85
6.2.1 認証の要素 85 / 6.2.2 1対1認証と1対N認証 86 / 6.2.3 バイオメトリクス認証の流れ 86 / 6.2.4 認証精度 87 / 6.2.5 認証システム 88
6.3 認証の強化 …… 89
6.3.1 二要素認証 89 / 6.3.2 二段階認証 90
6.4 指紋認証 …… 90
6.5 顔認証 …… 91
6.6 虹彩認証 …… 92
6.7 静脈認証 …… 93
6.8 DNA認証 …… 94
6.9 その他のバイオメトリクス認証 …… 94
6.10 バイオメトリクスのセキュリティ …… 95
6.11 実験D：バイオメトリクス認証 …… 96
引用・参考文献 …… 98

7. 秘密分散

7.1 秘密分散の利用シーン …… 99
7.2 基本的な仕組み …… 100
7.3 完全秘密分散法 …… 101
7.3.1 (k, n) 閾値秘密分散法の構成 101 / 7.3.2 有限体上でのラグランジュ補間公式 101 / 7.3.3 行列による表現 102 / 7.3.4 秘密分散法の安全性 103
7.4 完全秘密分散法の応用 …… 104
7.4.1 検証可能秘密分散 104 / 7.4.2 プロアクティブ秘密分散 105 /

7.4.3　閾値型分散復号　*106*

7.5　ランプ型秘密分散法 …… *108*

7.5.1　完全秘密分散法の欠点　*108* ／ 7.5.2　ランプ型秘密分散法の特徴　*109* ／ 7.5.3　(k, L, n) ランプ型秘密分散法の構成　*111* ／ 7.5.4　有限体上でのラグランジュ補間公式（ランプ型用）　*111*

7.6　実験 E：秘密の解読 …… *112*

引用・参考文献 …… *113*

8.　ネットワーク侵入防御

8.1　ネットワークの基礎知識 …… *114*

8.1.1　TCP/IP 階層モデルと IP パケット　*114* ／ 8.1.2　プライベート IP アドレスを用いたアクセス制御　*116*

8.2　ファイアウォール …… *116*

8.2.1　ファイアウォールの設計目標　*117* ／ 8.2.2　ファイアウォールの構成　*117* ／ 8.2.3　ファイアウォールの形態　*120* ／ 8.2.4　ファイアウォールの機能　*121* ／ 8.2.5　ファイアウォールにおけるアドレス変換　*123* ／ 8.2.6　ステートフルパケットインスペクション　*125* ／ 8.2.7　パーソナルファイアウォール　*127* ／ 8.2.8　実際のファイアウォール　*128*

8.3　その他の侵入防御対策 …… *129*

8.3.1　侵入検知システム　*129* ／ 8.3.2　侵入防止システム　*131*
8.3.3　サンドボックス　*131* ／ 8.3.4　ハニーポット　*132*

8.4　実験 F：Windows ファイアウォール …… *133*

9.　統計的不正アクセス検知

9.1　不正アクセス検知と機械学習 …… *134*

9.1.1　教師あり学習と教師なし学習　*135* ／ 9.1.2　評価指標　*136*

9.2　線形判別分析 …… *138*

9.3 ベイズ判別分析 …… 139
9.3.1 ベイズの基本公式 139 / 9.3.2 ベイズの展開公式 140 /
9.3.3 事前確率の重要性 141 / 9.3.4 ナイーブベイズ判別器 143
9.4 マルウェア検知への適用例 …… 144

10. VPN

10.1 VPN の概念 …… 147
10.2 IPsec …… 149
10.2.1 カプセル化モード 150 / 10.2.2 セキュリティアソシエーション 151 /
10.2.3 IKE 153 / 10.2.4 AH 154 / 10.2.5 ESP 155 / 10.2.6 使用されている具体的な暗号技術 157
10.3 TLS/SSL …… 157
10.3.1 セッションとコネクション 159 / 10.3.2 ハンドシェイクプロトコル 160 /
10.3.3 レコードプロトコル 161 / 10.3.4 使用されている具体的な暗号技術 161
10.4 VPN の詳細 …… 162
10.4.1 拠点間 VPN 163 / 10.4.2 リモートアクセス VPN 163 /
10.4.3 具体的なプロトコル利用例 164
引用・参考文献 …… 165

11. 暗号資産とブロックチェーン

11.1 暗号資産の特徴 …… 166
11.1.1 暗号資産による送金 166 / 11.1.2 ほかのディジタルマネーとの違い 168 / 11.1.3 アルトコイン 168 / 11.1.4 ウォレット 169 /
11.1.5 ブロックチェーンエクスプローラー 170
11.2 ブロックチェーン …… 171
11.2.1 ブロックチェーンの基本構造 171 / 11.2.2 ブロックチェーンの性質 172 / 11.2.3 ブロックチェーンの種類 173
11.3 ビットコイン …… 174

11.3.1　ビットコインの送金　*174* ／ 11.3.2　ビットコインのブロックチェーン　*176* ／ 11.3.3　探索パズルと PoW　*177* ／ 11.3.4　マイニング　*179* ／ 11.3.5　フォークとコンセンサス　*180* ／ 11.3.6　ビットコインネットワーク　*181* ／ 11.3.7　トランザクションチェーン　*182* ／ 11.3.8　ブロックチェーン生成までの流れ　*183*

11.4　イーサリアム　……*188*

11.4.1　非金融データの取り扱い　*189* ／ 11.4.2　アカウントとトランザクション　*189* ／ 11.4.3　スマートコントラクト　*192* ／ 11.4.4　イーサリアムのブロックチェーン　*196* ／ 11.4.5　イーサリアムの手数料　*196* ／ 11.4.6　PoW と PoS　*197*

11.5　実験 G：イーサリアムブロックチェーンへのアクセス　……*197*

引用・参考文献　……*198*

12.　ブロックチェーンのセキュリティ

12.1　51％　攻　撃　……*199*

12.2　Block Withholding 攻撃　……*200*

12.3　二重支払い攻撃　……*201*

12.4　Selfish マイニング攻撃　……*202*

12.5　その他のセキュリティ　……*204*

12.5.1　秘密鍵の奪取　*204* ／ 12.5.2　暗号資産の盗難とマネーロンダリング　*205* ／ 12.5.3　トランザクションの付け替え攻撃　*206* ／ 12.5.4　取引のプライバシー　*207*

12.6　なぜ暗号資産に PKI が不要なのか　……*208*

12.7　オラクル問題　……*209*

12.8　ブロックチェーンの耐改ざん性　……*209*

12.9　実験 H：暗号資産 NEM の追跡　……*210*

引用・参考文献　……*212*

索　　引　……*214*

ついての証明書を発行するので，この証明書を検証することにより，通信相手の正当性を確認できる。

図 5.6 は，公開鍵認証基盤の利用例を示している。ユーザ A が銀行 B に対して，確かに銀行 B のサイトであることを確認したいとする。まず準備として，① 銀行 B は自身の公開鍵（pk_{B}）を生成して CA に送付し，② CA は pk_{B} に対してサーバ証明書（pk_{B} に対する CA のディジタル署名になっている）を発行して銀行 B に返送する。また，①′ ユーザ A は CA の公開鍵を事前に認証チャネルでダウンロードしておく。準備が整った後，③ ユーザ A が銀行 B に TLS で接続し，④ pk_{B} を含むサーバ証明書をダウンロードする。⑤ このサーバ証明書は CA の公開鍵で検証できる。サーバ証明書が正しければ，⑥ ユーザ A は銀行 B の正しい公開鍵が pk_{B} であると判断して入手する。

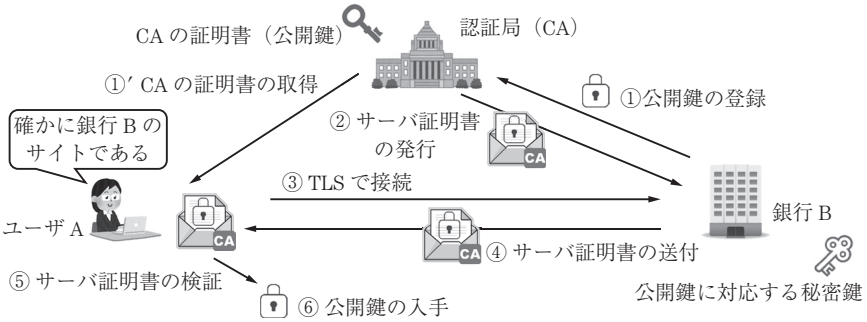


図 5.6　公開鍵認証基盤の利用例

さらに，**図 5.7** は公開鍵認証基盤と暗号通信の詳細を示している。ここで，CA の公開鍵（CA の証明書）を pk_{CA}，CA の秘密鍵を sk_{CA} とする。① まず銀行 B が公開鍵 pk_{B} を CA に登録し，② サーバ証明書である $Sig_{sk_{\mathrm{CA}}}(pk_{\mathrm{B}})$ を発行してもらう。また，①′ ユーザ A は CA の公開鍵 pk_{CA} を事前に認証チャネルでダウンロードしておく。ここで③ ユーザ A が銀行 B に TLS で接続して，まずは④ DH 鍵共有を行って秘密鍵 k を共有する。つぎに，⑤ k で暗号化された $Sig_{sk_{\mathrm{CA}}}(pk_{\mathrm{B}})$ と pk_{B} を受け取る。⑥ ユーザ A は pk_{CA} で $Sig_{sk_{\mathrm{CA}}}(pk_{\mathrm{B}})$ を検証し，検証が通れば⑦ pk_{B} を正当なものとして受理する。これ以降は平文 m の暗号化

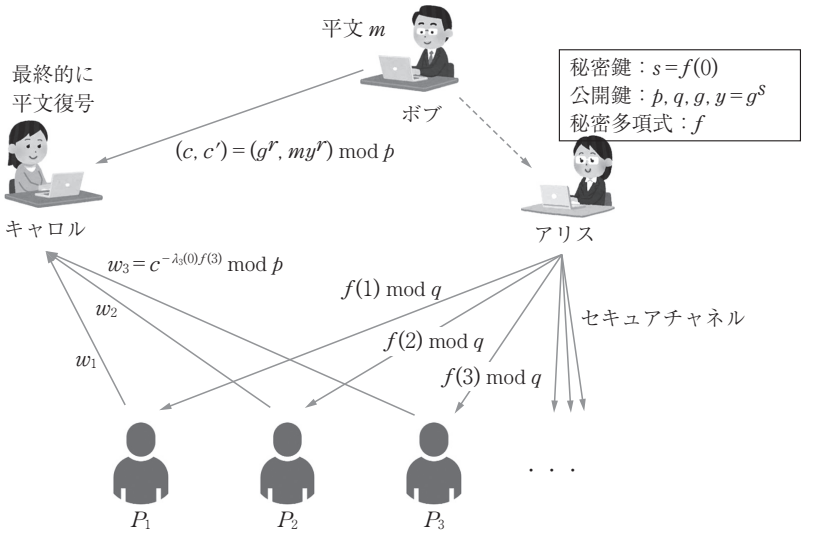


図 7.3　閾値型分散復号（エルガマル暗号ベース）の全体図

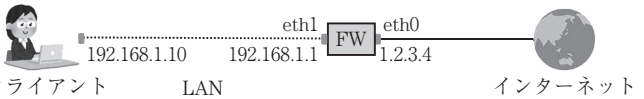
る。さらに，グループメンバは秘密鍵のシェアを含めたラグランジュ補間公式の断片を暗号文 c の指数部分に配置したままキャロルに送信しており，キャロルはシェアを知らないまま指数部分でラグランジュ補間公式を実行し，指数部分で秘密鍵が復元されている。なお，シェアや秘密鍵は離散対数問題の困難性により保護されていることに注意する。その結果，キャロルはアリスの秘密鍵を知ることなく平文 m を復号できる。

具体的な処理手順を以下に示す（図 7.3 参照）。

① **鍵生成**：　アリスは，まず大きな素数 p，および Z_p^* 上の位数 q の元 g を選ぶ。それから $x \in Z_q$ をランダムに選び，$y=g^x \bmod p$ を計算した後，公開鍵 $pk=(p, q, g, y)$ を公開し，秘密鍵 $sk=x$ を安全に保持する。ここで，位数である素数 q と秘密分散における Z_q の q を一致させている。つぎに，$(k-1)$ 次の下記多項式 $f(x)$ をランダムに選ぶ。

$$f(x)=s+a_1x+\cdots+a_{k-1}x^{k-1} \mod q \tag{7.12}$$

ただし，アリスは $f(x)$ も秘密に保持する。



フィルタテーブル（TCP）　「デフォルト＝遮断」

行為	送信元 IP アドレス	送信元 ポート	宛先 IP アドレス	宛先 ポート	フラグ	NIC
通過	192.168.1.0/24	ANY	ANY	80, 443		eth1 (in)

NAT テーブル

行為	送信元 IP	送信元 ポート	宛先 IP	宛先 ポート	変換後 送信元	変換後 宛先	NIC
NAT	192.168.1.0/24	ANY	ANY	80, 443	1.2.3.4		eth0 (out)

図 8.10　NAT 等を考慮したファイアウォールの設定例

ローバル IP アドレスに変換する NAT テーブルが追加される。ここで，送信元 IP アドレスの変換はファイアウォールの出て行くところ（eth0）でなされることに注意する。これについては後述する。

8.2.7　パーソナルファイアウォール

パーソナルファイアウォール（Personal Firewall, PFW）とは，端末内において外部ネットワークとの境界に配置され，不正アクセスを阻止するシステムである。具体的には，外部ネットワークからの通信およびコンピュータ内部からの外部ネットワークへの通信を許可／遮断する。通常のファイアウォールとの大きな違いは，アプリケーションと連携できる点である。具体的には，プロトコル（TCP/UDP/ICMP）ごとのフィルタリング，およびネットワークインタフェースごとのフィルタリングに加えて，プログラムおよびサービスごとのフィルタリングも可能となる。これにより，例えば，同じ Web ブラウザのアプリケーションでも Chrome からの Web アクセスは許可されるが, IE（Internet Explorer）からの Web アクセスは遮断されるということも実現できる。

また **Windows ファイアウォール**とは，Windows に標準搭載されているパーソナルファイアウォールのことである。Windows XP SP2 で初めて導入されたが，このときはインバウンド方向のフィルタリングのみであった。その後，

11.3.2 ビットコインのブロックチェーン

ビットコインのブロックチェーンは**図 11.5** のようになっている。各ブロックはヘッダ部とボディ部をもつ。ヘッダ部には，ハッシュ値，タイムスタンプ，マークルルート，ナンス[†1]の四つの値が格納されており，ボディ部には，トランザクション（TX）が発行者のディジタル署名付きで格納されている。マークルルート（5.2 節参照）は，ボディ部にあるトランザクション（サイズの上限は 1 MB）で構成されるマークルツリーのマークルルートが格納される。そのため，ブロックのハッシュ値はヘッダ部のハッシュ値のみで十分となる。実際各ブロックヘッダ部には，一つ前のブロックのヘッダ部のハッシュ値が格納されている。ハッシュ値は暗号学的ハッシュ関数 H によって計算され[†2]，ナンスはハッシュ値を調整するための値となる。2020 年 12 月現在では，ブロックチェーンのサイズは約 320 GB である[†3]。

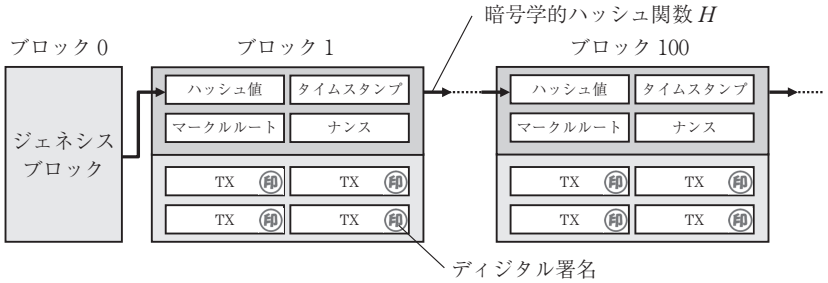


図 11.5　ビットコインのブロックチェーン

トランザクションが確定することはファイナリティと呼ばれる。51%攻撃など（12.1 節参照）の可能性がある限りファイナリティがなされることは永遠にないが，実質的なファイナリティに向けては二段階の処理を行う。一つ目は個人レベルで行うトランザクションデータの検証である。誰から誰へいくら送金するのかの内容を保証するものであり，これはトランザクション発行者のディ

†1　ナンス（nonce）とは number used once の略で，一度だけ使用される使い捨ての数を表す。
†2　ハッシュ値は SHA-256 で 2 回ハッシュされて導出される。
†3　https://www.blockchain.com/ja/charts

［**具体的な実験手順**］

1．Infura に登録してアクセスキー（Geth ノードの URL の一部）を得る。
2．下記のコード例にある Python プログラムを実行して，メインネットとテストネット（Ropsten）のそれぞれのブロック高（web3.eth.blockNumber）を取得する。
3．ブロック高の違いからメインネットかテストネットかを判断する。

［**実験結果について**］

イーサリアムのメインネットとテストネットのそれぞれのブロック高を取得して表示する。これらの値から，現在接続しているイーサリアムブロックチェーンがメインネットなのかテストネットなのかを判別できる。

［**コード例**］

```
from web3 import Web3,HTTPProvider

def main():
  # mainnet の最新ブロック番号の取得
  web3 = Web3(HTTPProvider('https://mainnet.infura.io/v3/(アク
  セスキー)'))
  blockNumber = web3.eth.blockNumber
  print(blockNumber)

  # testnet の最新ブロック番号の取得
  web3 = Web3(HTTPProvider('https://ropsten.infura.io/v3/(アク
  セスキー)'))
  blockNumber = web3.eth.blockNumber
  print(blockNumber)

if __name__=='__main__':
  main()
```

引用・参考文献

1）Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system（2008），https://bitcoin.org/bitcoin.pdf
2）Buterin, V.: Ethereum white paper: a next generation smart contract and decentralized application platform（2013）

索　　引

【あ】

アクセス構造 108
アクセス制御 116
アドレススキャン 3
アノマリ型検知方式 130
アプリケーションゲートウェイ型ファイアウォール 120
アメリカ国立標準技術研究所 68
アルトコイン 168
暗号 50
暗号学的ハッシュ関数 67
暗号危殆化 34
暗号資産 166
暗号利用モード 54
アンチウイルスソフト 8

【い】

イーサリアム 188
イーサリアムネットワーク 194
位　数 43
一次不定方程式 38
入口対策 30
インセンティブ 179
インターネット VPN 163
イントラネット 2

【う】

ウォレット 169

【え】

エクリプス攻撃 207
エルガマル暗号 60
遠隔操作ウイルス 9
演算（量）の証明 178
エントロピー 48

【お】

オイラーの定理 43
オラクル問題 209

【か】

改ざん 31
改正資金決済法 170
カウンタモード 55
顔認証 91
鍵共有 61
拡張ユークリッドの互除法 38
ガ　ス 196
ガス価格 196
カプセル化モード 150
可用性 31
完全性 31
完全秘密分散法 101

【き】

機械学習 134
技術的脅威 23
既知平文攻撃 52
機密性 31
脅　威 23
教師あり学習 135
教師なし学習 136
共通鍵暗号 52
拠点間 VPN 163
キーロガー 10

【く】

クライアント認証モデル 88
クラス分類 135
グラフィカルモデル 144
グローバル IP アドレス 1

【け】

計算量的安全性 33
軽量ノード 170
ケルクホフスの原理 32
原始元 43
検証可能秘密分散 104
原像計算困難性 67
検知漏れ 136
検知漏れ率 137

【こ】

公開鍵暗号 58
公開鍵認証基盤 78
攻撃者のモデル 51
虹彩認証 92
合　同 40
声認証 95
誤検知 136
誤検知率 137
コミットメント 69
コール 190
コールドウォレット 169
コンセンサス 180
コンソーシアムブロックチェーン 174
コントラクトアカウント 189
コンピュータウイルス 8

【さ】

採掘者 177
再現率 138
サイバー脅威 1
サーバ証明書 79, 159
サーバ認証モデル 88
サービス停止攻撃 10
サンドボックス 131

【し】

シェア 99
ジェネシスブロック 167
シェルショック脆弱性 28
耳介認証 95
閾値型分散復号 106
閾値秘密分散法 99
閾値ランプ型秘密分散法 109
シグネチャ型検知方式 130
事後確率 139
事後対策 30
シーザー暗号 50
事前確率 139
事前対策 30
指紋認証 90
シュノア署名 74
衝突計算困難性 67
乗法逆元 41
情報資産 23
情報量 47
情報理論的安全性 34
静脈認証 93
署名認証 95
人的脅威 23
侵入検知システム 129
侵入防止システム 131

【す】

ステートフルパケット
　インスペクション 125
ストリーム暗号 53
スニファ 17
スーパーノード 210
スマートコントラクト 192

【せ】

正解率 137
脆弱性 24
脆弱性検査 3
正則元 42
セキュアチャネル 88
セキュリティ
　アソシエーション 151
セキュリティ対策 26
セキュリティの３要素 31
セキュリティバイデザイン
34
セキュリティリスク 22
セーフブラウジング 135
ゼロデイ攻撃 27
線形判別分析 138
選択暗号文攻撃 52
選択平文攻撃 52

【そ】

素因数分解問題 44
ソーシャルエンジニアリング
3
素　数 36

【た】

第三者機関 171
対称鍵暗号 52
第二原像計算困難性 68
耐量子暗号技術 210
多層防御 30
他人受入率 87
多要素認証 90
単位元 41
探索パズル 178
誕生日クイズ 66

【ち】

チャレンジレスポンス方式
76
中間者攻撃 16
中国の剰余定理 44
チューリング完全 193
直接攻撃 52

【て】

ディジタル署名 73
ディジタルマネー 168
ディープパケット
　インスペクション 120
適合率 138
出口対策 31
テストネット 197
電子政府推奨暗号 32
転々流通性 168

【と】

盗　聴 31
ドライブバイダウンロード
　攻撃 14
トランザクション 167, 190
トランザクション ID 185
トランザクションチェーン
182
トランザクション手数料 179
トランザクションプール 184
トランスポートモード 150
トレーサビリティ 208
トロイの木馬 9
トンネリング 162
トンネルモード 150

【な】

ナイーブベイズ 144
ナンス 176

【に】

二重支払い攻撃 201
二段階認証 90
二要素認証 89
認　証 66
認証暗号 157
認証局 79
認証子 71

認証チャネル 78

【ね】

ネットワーク型
　侵入検知システム 129

【は】

バイオメトリクス認証 85
ハイブリッド暗号 62
パケットフィルタリング型
　ファイアウォール 120
バースデイパラドックス 66
パスワードクラック 4
パスワード認証 75
パスワードリスト攻撃 5
パーソナルファイアウォール 127
パターンファイル 9
バックドア 18
ハッシュ値 67
ハッシュチェーン 69
ハッシュレート 199
バッファオーバーフロー 6
ハードウェアウォレット 169
バーナム暗号 51
ハニーポット 132
パブリックブロックチェーン 173
パーミッション型 173
パーミッションレス型 173
ハンドシェイクプロトコル 159

【ひ】

非対称鍵暗号 58
非中央集権 174
ビットコイン 174
ビットコインネットワーク 181
否認不可 74
秘密分散 99
標的型サイバー攻撃 18
平　文 50

【ふ】

ファイアウォール 19, 116
ファイナリティ 176
ファンデルモンドの行列式 102
フィッシング詐欺 13
フィルタリング 117, 121
フェルマーの小定理 43
フォーク 180
復　号 50
不正アクセス 2
不正アクセス禁止法 30
不正アクセス検知 134
物理的脅威 23
プライバシー 3, 207
プライベート IP アドレス 1
プライベート
　ブロックチェーン 174
ブルートフォース攻撃 5
フルノード 170
プロアクティブ秘密分散 105
ブロック暗号 54
ブロック高 197
ブロックチェーン 171
ブロックチェーン
　エクスプローラー 170
プロミスキャスモード 17, 130
分散型台帳技術 167

【へ】

平均情報量 48
ベイジアンネットワーク 144
ベイズの定理 47
ベイズ判別分析 139
ベイズ理論 143
ペーパーウォレット 169
変換テーブル 123

【ほ】

報　酬 177
ホスト型侵入検知システム 130
ホットウォレット 169
ボットネット 9
ポートスキャン 3
ポート番号 2
歩容認証 95
本人拒否率 87

【ま】

マイナー 177
マイニング 179
マークルツリー 70
マークルルート 176
マネーロンダリング 206
マルウェア 8

【み】

未使用トランザクション 186
未承認トランザクション 184

【め】

メッセージ認証コード 71

【も】

網膜認証 94

【ゆ】

誘因両立性 203
尤　度 139
ユークリッドの互除法 37
ユーザ認証 75

【ら】

ラグランジュ補間公式 101
ラベル 135
ランサムウェア 10
ランプ型秘密分散法 108

【り】

離散対数問題 44
リスク評価 25

リスクファイナンス 26
リスクマネジメント 25
リバースブルートフォース攻撃 5
リプレイ攻撃 55
リモートアクセス VPN 163
量子コンピュータ 210

【る】

ルーティング 121

【れ】

レコードプロトコル 161
連立合同式 45

【わ】

ワーム 9, 134
ワンタイムパスワード 77

【数字】

1 対 1 認証 86
1 対 N 認証 86
51%攻撃 199
8333/TCP 182
8545/TCP 197

【A】

ABI 194
AEAD 157
AES 暗号 54
AH 154

【B】

bitcoin-cli コマンド 184
Block Withholding 攻撃 200
BTC 175

【C】

C&C サーバ 9
CA 79
CBC-MAC 72
CBC モード 56
CCM モード 57
common modulus attack 63
CRT 44
CRYPTREC 32
CTR モード 55
CWC モード 58

【D】

DDoS 攻撃 11
DES 暗号 54
DHE 162
DH 鍵共有法 61
DMZ 118
DNAT 123
DNA 認証 94
DNS キャッシュポイズニング 15
DNS シード 181
DoS 攻撃 11
DRDoS 攻撃 12
DSA 署名 75

【E】

ECB モード 55
ECDHE 160
ECDH 鍵共有 61
ECDSA 署名 74
EOA 189
ESP 155
ETH 188
EVM 193

【F】

FIDO 89
FIDO U2F 認証 90
FNR 136
FPR 136
F 値 138

【G】

gasPrice 196
gasUsed 196
GCM モード 57
Geth 189
Geth ノード 197

【H】

HIDS 130
HMAC 72

【I】

IDS 129
IKE 153
Infura サービス 197
ipconfig 2
IPS 131
IPsec 147
IPsec-VPN 164
iptables 128
IP アドレス 1
IP スプーフィング 11

【J】

JSON RPC API 197

【L】

L2 スイッチ 130
LAN 116

【M】

MAC 71
MAC アドレス 115
Mainnet 188
Mirai ボットネット 4

【N】

NAPT 124
NAT 123

NEM 205
netsh advfirewall firewall 128
NIDS 129
NIST 68
nonce 176

【O】

OpenSSL 57
OP_RETURN 189
OSI 参照モデル 114

【P】

P2P ネットワーク 172
PKI 78
PoS 197
PoW 178
PowerShell 128
PSS 105
Precision 136

【R】

RAT 9
Recall 136
RFC8446 158
Ropsten 198
RPC 184
RSA-OAEP 60
RSA 暗号 59
RSA 署名 74

【S】

Selfish マイニング攻撃 202
SHA 68
SHA-256 72
SNAT 123
Solidity 194
SPV 170
SSL 158
SynFlood 11

【T】

tcpdump 17
TCP/IP 階層モデル 114
TLS 157
TLS1.3 158
TLS-VPN 164

【U】

UTXO 186

【V】

VirusTotal 135
VPN 147, 162
VSS 104

【W】

web3 198
Windows ファイアウォール 127
Wireshark 17

【X】

XEM 205

―― 著 者 略 歴 ――

1997 年　大阪府立大学工学部機械システム工学科卒業
2002 年　北陸先端科学技術大学院大学情報科学研究科博士課程修了（情報システム学専攻）
　　博士（情報科学）
2002 年　株式会社富士通研究所セキュアコンピューティング研究部研究員
2011 年　北陸先端科学技術大学院大学情報科学研究科准教授
2016 年　筑波大学システム情報系准教授
　　現在に至る

入門 サイバーセキュリティ　理論と実験
～ 暗号技術・ネットワークセキュリティ・
ブロックチェーンから Python 実験まで ～

Introduction to Cybersecurity　Theory and Experiment

© Kazumasa Omote 2021

2021 年 3 月 18 日　初版第 1 刷発行　★

検印省略

著　　者　面（おもて）　和（かず）　成（まさ）
発 行 者　株式会社　コ ロ ナ 社
　　代 表 者　牛 来 真 也
印 刷 所　新 日 本 印 刷 株 式 会 社
製 本 所　有限会社　愛 千 製 本 所

112-0011　東京都文京区千石 4-46-10
発 行 所　株式会社　**コ ロ ナ 社**
CORONA PUBLISHING CO., LTD.
Tokyo Japan
振替 00140-8-14844・電話(03)3941-3131(代)
ホームページ　https://www.coronasha.co.jp

ISBN 978-4-339-02917-8　C3055　Printed in Japan　（柏原）

JCOPY ＜出版者著作権管理機構 委託出版物＞
本書の無断複製は著作権法上での例外を除き禁じられています。複製される場合は，そのつど事前に，出版者著作権管理機構（電話 03-5244-5088，FAX 03-5244-5089，e-mail: info@jcopy.or.jp）の許諾を得てください。

本書のコピー，スキャン，デジタル化等の無断複製・転載は著作権法上での例外を除き禁じられています。購入者以外の第三者による本書の電子データ化及び電子書籍化は，いかなる場合も認めていません。
落丁・乱丁はお取替えいたします。