サイバー犯罪捜査の苦手・疑問も一気に解決!!

新刊

クラウド・フォレンジックの基礎

一般財団法人 保安通信協会 編著
羽室 英太郎(保安通信協会：セミナー・出版分科会)
小瀬 聡幸(AOSデータ株式会社：デジタル・フォレンジック分科会)

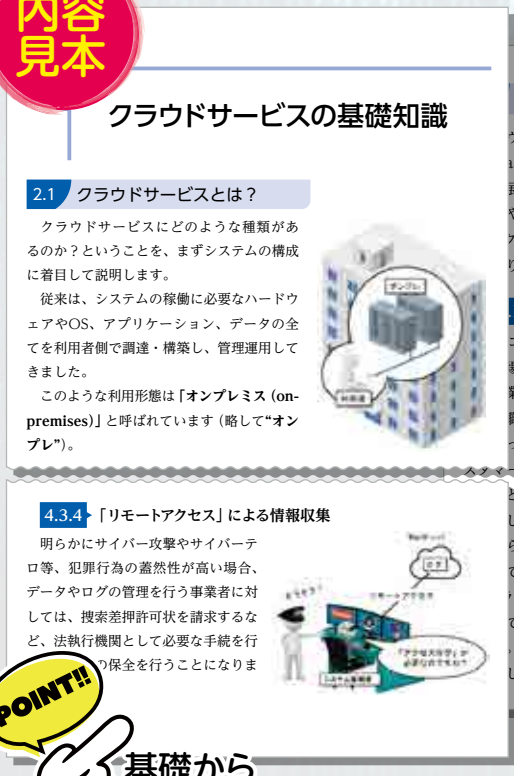
本書の特長

- クラウドとは何か?の**基礎**から丁寧に解説。知識が土台からしっかり身につく。
- クラウドの仕組み、セキュリティ・リスクや攻撃などの解説も掲載。**専門用語も細かく説明**されているから、つまずかない。
- **内容の理解を助ける、記憶に残るイラスト**や実際の**操作画面の画像**などを豊富に登載。
- 「リモートアクセス」による証拠収集や解析作業の詳細な手順、証拠データが削除されたときの対処法など、各段階で押さえておくべきポイントは必読。**実務に直結した**クラウド・フォレンジックの知識が手に入る。

A5判　208頁
定価2,750円(本体2,500円+税10%)
ISBN978-4-8090-1488-8　C3055　¥2500E
紙書籍(モノクロ版)／電子書籍(カラー版) あり

内容見本

※内容見本は電子書籍(カラー版)


クラウドサービスの基礎知識

2.1 クラウドサービスとは？

クラウドサービスにどのような種類があるのか？ということを、まずシステムの構成に着目して説明します。

従来は、システムの稼働に必要なハードウェアやOS、アプリケーション、データの全てを利用者側で調達・構築し、管理運用してきました。

このような利用形態は「**オンプレミス (on-premises)**」と呼ばれています（略して"**オンプレ**"）。

4.3.4 「リモートアクセス」による情報収集

明らかにサイバー攻撃やサイバーテロ等、犯罪行為の蓋然性が高い場合、データやログの管理を行う事業者に対しては、捜索差押許可状を請求するなど、法執行機関として必要な手続を行

の保全を行うことになりま


クラウドのセキュリティ確保と「監視」

ウドのセキュリティを確保する、といっても単一のクラウドのサービ
aS）を利用している場合から、マルチクラウドを用いて大規模なサー
展開する場合まで、様々な運用状況が考えられます。
や「フォレンジック」を行う場合には、まず被害等が発生した舞台と
クラウド」の規模や利用形態等を的確に把握することからはじめる必
ります。

1 クラウドのセキュリティと「ゼロトラスト」

コロナウイルスの感染拡大以
場に従業員が詰める、という形
業務遂行だけでなく、自宅や出
職場のデータにリモートアクセ
ったり、データセンターでのカ
施したり
取り入れ

ウド」が、その中継地点やデータの保管場
ウド」を
、正しい利用
ていれば、
正行為の発生と回避することが可能なのかもしれ

し、クラウドサービスを利用する企業等は、自組織でセキュリティ面

b クラウドサービス"X"が管理するデータを収集する場合

対象のアカウントでログインする。
ログ保管フォルダに移動する。
エクスポート先（外付けHDD等の媒体）を指定する。
目的のログファイル等をエクスポートする。
目的データが取得できていることを確認する（エクスポート時ログ等から）。
取得データのハッシュ値を算出する。

＊aと＊bの違いは、ログが保存されているディレクトリ（フォルダ）に移する、というコマンドライン等の操作が必要かどうか、ということですが、のログ保存ディレクトリ等は設定ファイルに記述されており、デフォルト定の保管場所とは異なる場合があります。また手順についても、サービスアプリにより異なっていますので、作業の際は各サービスのマニュアルにう、あるいはクラウドサービス"X"のシステム管理者等から当該保存場所に関する情報を的確に把握する必要があります。

5.2.2.1 AWS (Lambda)のデータイベントログファイルの保全手順(例)

2.1.2 でサーバレスコンピューティングサービスについては説明していますが、AWS Lambdaは発生イベントに応じてコードを実行し、利用者にわりAWSが状況に応じてサーバ等リソースを準備するもので、FaaS (Function as a Service) サービスとばれることもあります。

「サーバレス」だから"サーバは無い"のではなく、サーバ機能はクラウドサービス事業者が提供してい

POINT!! イラストや画像で理解を助ける

POINT!! 基礎から実務まで網羅

POINT!! 業務に直結する知識が満載

東京法令出版

捜査に必須の「クラウド」知識。基礎の基礎から実務のポイントまでこの一冊で。

はしがき（抜粋）

昨今は政府機関を含め様々なITインフラが「クラウド」にシフトしております。

しかしながら、クラウドサービスへの依存度が高まるにつれ、このサービスを悪用したり脆弱性を突いたサイバー攻撃等が行われてサービスが停止したならば、その社会的な影響は膨大なものとなります。

クラウド基盤はIT技術の粋を集めたサービスでもありますので、その復旧や障害対応、捜査に関する知識や技能を習得する敷居はかなり高いものとなっております。

このような状況に対応するため、今般、クラウドサービスの仕組みやセキュリティ対策、フォレンジックに関して、基礎的な知識等を整理して本書を上梓することとしました。

法執行機関のみならず、民間企業等におかれましてクラウド業務を管理されておられる方々にとって、少しでも参考になれば幸いです。

一般財団法人保安通信協会　理事長　　金井　洋

目　次

好評発売中!

デジタル鑑識の基礎シリーズ

一般財団法人保安通信協会　編著

デジタル鑑識の知識を、図表・写真・イラストを豊富に用い、コンパクトにまとめたシリーズ
上・中・下巻、どの巻からも気軽に読み進められる、使いやすい構成

デジタル鑑識の基礎（上）第2版
「証拠ファイルが削除されている!」
～残存データの可視化技術
A4判　80頁・2色刷
定価1,100円（本体1,000円＋税10%）
ISBN978-4-8090-1435-2　C3055　¥1000E

デジタル鑑識の基礎（中）
―インシデントレスポンスと初動対応―
A4判　64頁・2色刷
定価917円（本体834円＋税10%）
ISBN978-4-8090-1380-5　C3055　¥834E

デジタル鑑識の基礎（下）
―証拠保全―
A4判　64頁・2色刷
定価917円（本体834円＋税10%）
ISBN978-4-8090-1398-0　C3055　¥834E

デジタル・フォレンジック概論

～フォレンジックの基礎と活用ガイド～

羽室英太郎・國浦　淳　編著

サイバー犯罪に限らず、現代の多種多様な犯罪捜査に対応した
デジタル・フォレンジック入門の決定版

A5判　296頁　　定価2,200円（本体2,000円＋税10%）　ISBN978-4-8090-1331-7　C3055　¥2000E

申込書

クラウド・フォレンジックの基礎 定価2,750円（本体2,500円+税10%）〔コード14913〕	申込　部	送料は実費。 税込購入金額5,000円以上はサービス
「デジタル鑑識の基礎」シリーズ 各定価は、上記のとおり。〔上：コード12841〕〔中：コード13106〕〔下：コード13288〕	申込 ※いずれかを○で囲んでください。 上・中・下　部	
デジタル・フォレンジック概論 定価2,200円（本体2,000円+税10%）〔コード12401〕	申込　部	

貴社の個人情報に関する下記取扱いに同意し、上記のとおり申し込みます。　　令和　　年　　月　　日

（フリガナ）
お取扱者（自署）　　（TEL　　－　　－　　）

お届け先住所　〒

団体名　　部署名　　□公用 □私用

個人情報の取扱いについて　東京法令出版株式会社 個人情報保護管理者
★お客様の個人情報は、契約の履行及び関連製品の案内に利用します。
★本人の同意がある場合又は法令に基づく場合を除き、第三者に提供しません。
★利用目的の達成に必要な範囲内で取扱いの一部を委託することがあります。
★本人からの個人情報の利用目的の通知・開示・内容の訂正・追加又は削除・利用の停止・消去の求めに応じます。
★個人情報に関するご照会・お問い合わせ等は、弊社窓口（TEL026-224-5441、privacy@tokyo-horei.co.jp）までご連絡ください。
★お申込みには個人情報の提供が必要です。提供いただけない場合は、お申込みをお受けできないことがあります。

東京法令出版公式X（旧Twitter）アカウント
X @tokyo_horei

この申込書は、このままFAXで下記宛にお送りください。

■申込先
東京法令出版株式会社 受注センター
〒381-0022　長野市大豆島3111
FAX　0120-338-923
TEL　0120-338-272
（携帯電話からもお申込みできます。）

会社使用欄								
団体コード				□納品済 □請求済 □領収済	入力印			
得意先コード								
在庫		ラベル		〒			チェック	