スクエアfreeセミナー：第170回

さぁて、御社のサイバーセキュリティ対策レベルを調べて見ますか

～ アタックサーフェスからわかること ～

株式会社レオンテクノロジー

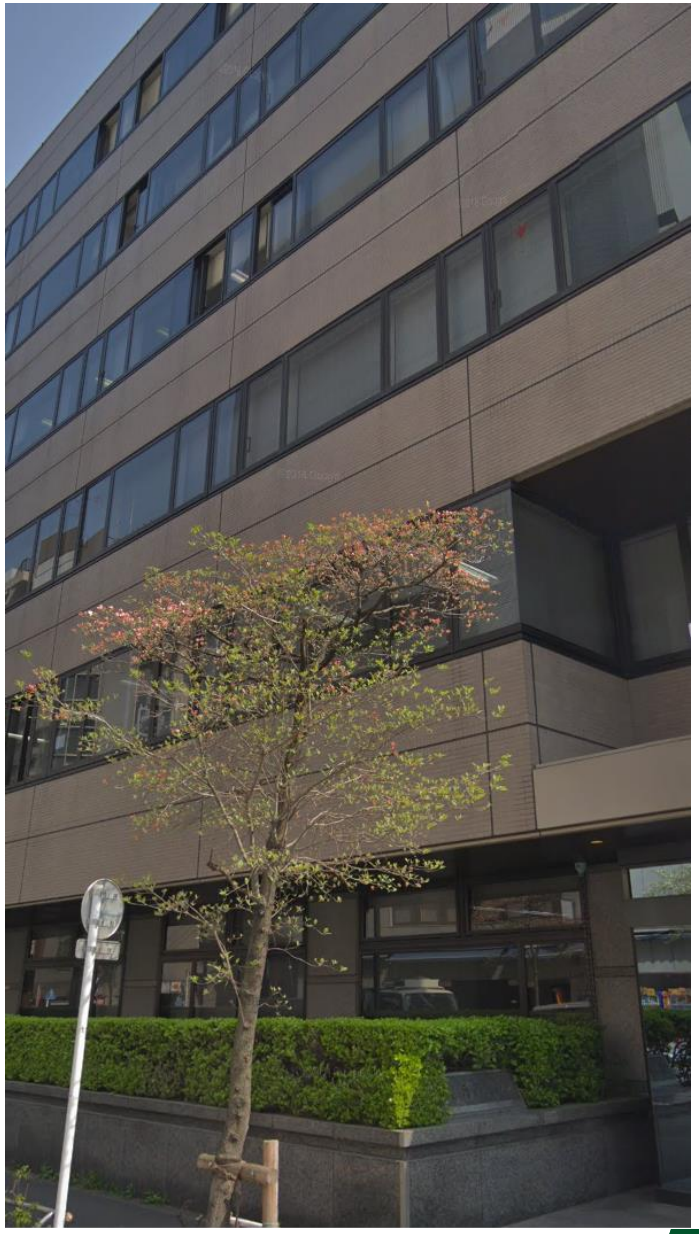
代表取締役社長

守井 浩司/Koji Morii

1981年、京都府生まれ。
株式会社レオンテクノロジーを2005年3月に設立。各種サイバーセキュリティ事業を展開。
自身も現場の最前線にて活動を続ける傍ら、ホワイトハッカー育成にも注力。
近年は金融機関および医療機関を中心に、講演や教育など、セキュリティに関する啓蒙活動を行っている。

会社概要

社名	株式会社レオンテクノロジー （英文：LEON TECHNOLOGY, Inc.）
設立	2005年3月16日
本社所在地	〒171-0014　東京都豊島区池袋2-52-8　大河内ビル3階
資本金	50,000,000円
事業内容	• セキュリティ診断サービスの提供 • セキュリティ対策サービスの提供 • フォレンジック調査（セキュリティインシデント調査・対応） • ネットワーク・インフラの構築・運用・保守 • セキュリティに関わる助言・監査・教育・コンサルティング等
認定資格	• ISMS (ISO/IEC27001:2022) • PCI DSS認証監査機関 • 情報セキュリティサービス基準適合サービス登録 (1)脆弱性診断サービス（サービス登録番号：019-0024-20） (2)デジタルフォレンジック（サービス登録番号：019-0024-30） (3)ペネトレーションテスト（サービス登録番号：019-0024-60）
加盟団体	• 日本カード情報セキュリティ協議会（JCDSC） • 日本ネットワークセキュリティ協会(JNSA) • 一般社団法人 日本スマートフォンセキュリティ協会（JSSEC） • 特定非営利活動法人 デジタル・フォレンジック研究会(IDF) • 公益財団法人 金融情報システムセンター（FISC） • PCI SSC（PCI Security Standards Council）
主な保有資格	• CEH（認定ホワイトハッカー）認定講師 • CEH • CPSA（CREST Practitioner Security Analyst） • OSDA（OffSec Defense Analyst） • OSCP（OffSec Certified Professional） • 情報処理安全確保支援士（登録セキスペ） • CISSP（Certified Information Systems Security Professional）

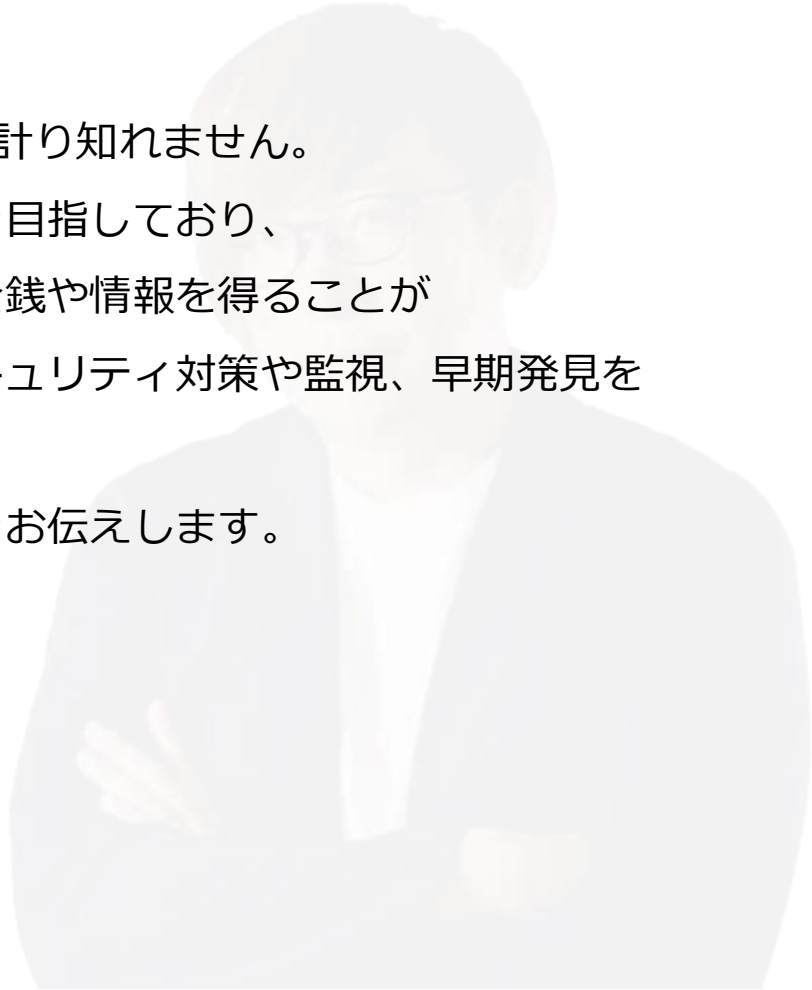


本日お伝えしたいこと

組織規模関係なく、インターネットに公開する資産があればそれはもう「標的（まと）」となります。

- 「攻撃対象領域」とは何か！？

- 「公開資産」の管理不足、放置、認知不足が組織に及ぼす影響は計り知れません。
  攻撃者が闇雲に攻撃する時代は終わり、攻撃者も攻撃の効率化を目指しており、
  攻撃成功確率や目的達成可能確率が高い資産を手間なく攻撃し金銭や情報を得ることが
  目的であるならば、攻撃者が攻撃を諦める・回避するためのセキュリティ対策や監視、早期発見を
  実現する必要があります。
  組織が保有する「公開資産をどのように管理・把握すべきか」をお伝えします。



目次

攻撃者はこのように「攻撃対象領域」を把握する。 知らんけど

・御社、HPをお持ちですよね？

例：www.example.com、*.example.com、

・メールサーバを持ちメールアカウントを保有されてますよね？

例：mail.example.com 、smtp.example.com　など

・HP以外にも自社のサービスをコーポレートドメイン以外でサイトを立ち上げ情報発信や集客を実施されてますよね？

例：example2.com 、*.example2.com　など

・御社とわかる識別子でクラウドサービスをご利用されてますよね？

例：example.Microsoft.com、saiyou.moriisan.co.jp、moriisan.zoom.us　など

普通のHPなのに、ただのメールサーバなのに、
契約してるクラウドサービスなのに、
企業規模は大きくないのに
googleにキャッシュされていないのに、
接続制限してるのに・・・

関係ないです、ネットに公開されてますので、
ただそこに存在するだけで、

「攻撃対象領域」になります！

次ページでちょい難しい言葉を使いますが細かく言うときます。

企業が保有するインターネット公開資産（攻撃対象領域）、どんなものが「攻撃対象領域」なのか！？

企業が保有する主なインターネット公開資産（攻撃対象領域）

- ドメイン・DNS関連
- Web系サービス
- メール関連システム
- リモートアクセス系
- クラウドサービス資産
- ネットワーク機器
- 公開リポジトリ・コード関連
- 証明書・暗号化関連
- 外部発信情報（間接的な資産）

企業が当たり前に保有し利用する資産が攻撃されるのやで、
ちゃんと管理しなはれや！

◆ドメイン・DNS関連

プライマリドメイン／サブドメイン

・公式サイト、サービス用ドメイン、社内向け環境を誤って公開したもの、アカンやつ。

DNSレコード

・NS、MX、SPF/TXT、DKIM、DMARC などから攻撃者に構成情報が露呈。

CDN / WAFなどに用いられるCNAME

・バックエンドのIPやクラウド資産が推測される場合がある、あんまないけどね。

◆Web系サービス

コーポレートサイト／ブランドサイト

・WordPress, Drupal など CMS 脆弱性を突かれるリスクが高い、CMSがアカンのじゃなくて
ちゃんと推奨されるセキュリティ設定なりができてないからアカンのですわ。

顧客向けWebサービス（ポータル・EC・予約・会員サイト等）

・アプリケーションの脆弱性や設定の不備、認証弱さなどが狙われる！

APIエンドポイント

・REST/GraphQL API が認証不備や過剰情報開示のリスクあることもある、ちゃんと設定しよし。

モバイルアプリのバックエンド

・iOS/Androidアプリが通信するAPIサーバが狙い目！

開発/検証環境のWebサーバ

・認証なしで公開されているケースは狙われるで。

◆メール関連システム

MXサーバ（メールサーバ）

・オープンリレー、古いSMTPサーバーの脆弱性などが狙い目！誰目線w

Webメールサービス（OWA, Zimbra, Roundcubeなど）

・ID/PW総当たりやゼロデイ攻撃の標的になりやすい、メールサーバーの認証を奪うなりで踏み台にするなりできると活用方法が多く過去のメールやり取りとか宝やん、誰目線w

◆リモートアクセス系

VPNゲートウェイ

・Pulse Secure、Fortinet、Cisco ASA など過去に大規模な被害に繋がったよね～、知らんけど。

リモートデスクトップ（RDP, VNC, Citrix等）

・ブルートフォース攻撃や脆弱性を突いて入れたら無限大な夢よ、これ

Zero Trust / SASE 系ポータル

・Misconfigや利用期限切れ証明書が狙い目かな～、ゼロトラストの実現ってほんまむずいね。

◆クラウドサービス資産

クラウドストレージ

・AWS S3、Azure Blob、GCP Storage の「公開バケット」問題あったよね～

クラウドホスティング

・不要に公開されたEC2/VMインスタンスとか管理されてなかったりで狙い目ちゃうか

SaaS連携サービス

・誤設定により外部公開されるGoogle Drive、SharePoint、Boxなどほんまごっつあんです！

◆ネットワーク機器

ファイアウォール／ルータ／ロードバランサ

・管理UIがインターネットに公開されているケース、時間かけたらいつか入れそうな気がする。

IoT/OT機器

・監視カメラ、ビル管理システム、工場制御システム（**OSINT**で検索可能！）

「OSINT」についてはまた後で説明する！多分な！

いまだに病院の監視カメラとか、
工場の制御システムの管理画面とかOSINTで出てくるから笑う

◆公開リポジトリ・コード関連

GitHub/GitLabの公開プロジェクト

・APIキー、内部サブドメイン、機密情報の漏洩リスクがあるのに管理されてないのよな～。

パッケージリポジトリ

・npm/PyPI への誤公開によるソフトウェアサプライチェーン攻撃につながる！
※ソフトウェアサプライチェーン攻撃ってのは自分で調べておくれやす。

◆証明書・暗号化関連

TLS/SSL証明書

・複数ドメインの「※ SAN情報」から内部資産を推定される！

古い暗号スイートやTLSバージョン

・中間者攻撃や既知脆弱性の利用リスク

※SAN情報とは
「Subject Alternative Name」の略、「サブジェクトの別名」。
SSLサーバ証明書に含まれる情報として、コモンネームを含むサブジェクトとは別に「SAN」という拡張領域のことな、知らんけど。
這いよれニャル子さんのSAN値とは別物、わかる人にはわかるやつ！

◆外部発信情報（間接的な資産）

robots.txt, sitemap.xml

・内部用サブディレクトリやテスト用ドメインが記載されている場合、外部リンクなどから見られたくない接続されたくない領域がわかることもある、ほんまに稀にな。

公開資料（PDF, Word, Excel）

・メタデータに内部サーバのホスト名やユーザIDが残っていることがある、ほんまに稀にな。

求人情報やヘルプページ

・使用している技術スタックやクラウド情報が特定されることもある、設定次第やな。

◆侵入口や情報漏洩につながるから危険なんやで、の何が危険につながるのか！？

- **可視化されていない資産（Shadow IT）** が放置されて狙われやすい
- 古い環境や検証用システムから **「侵入の踏み台」** とされる
- 複数の外部情報を組み合わせて攻撃者は **企業の全体像をマッピング** する
- インシデントにつながると **規制違反（FISC, IPA, 金融庁ガイドライン等）やブランド毀損** に直結

被害に遭うのが嫌ならちゃんと把握して管理せなアカン、
ただそれだけの話。

ここからは・・・

・うち、こんな公開資産持ってたんや！
・どうやってサブドメイン特定して攻撃してきよんの！

第一章のタイトル通り、攻撃者は今から説明する技法、
手法を用いたりしてサブドメインなどの公開情報を取得してくる。
言わば、守りにも把握管理するために実施した方がいい技法です。

自分らも放置資産や管理不足の公開資産がないように
管理しましょうね！という話。

サブドメイン取得の技術、手法

※これが全部ではないで！

サブドメイン取得の方法は大きくこのように取得可能！

※これが取得方法の全部じゃないで！

- DNSベースの情報収集
- 公開情報の収集
- ブルートフォース型アプローチ
- クラウドサービス・開発環境からの露出
- インフラ・サービス利用痕跡の解析
- ネットワークスキャンによる情報取得
- サードパーティ情報の利用
- トラフィック観測・データベース利用
- 誤設定による露出（人為的ミス）

物理的に企業の保有資産（サブドメイン含む）を知る人物を
拉致して吐かせるという方法もあるだろうが今までは日本では
なかったけどこれからあるかもしれない、気をつけなはれや！

◆DNSベースの情報収集

・ゾーン転送（AXFR）

DNSサーバの設定が不適切な場合、外部から「ゾーン転送（AXFR）」をリクエストすると、
ドメインに属する全サブドメイン情報が返される。
本来はプライマリDNSとセカンダリDNS間の同期用途だが、アクセス制御が誤っていると外部から利用可能になる。

・DNSクエリ／リバースルックアップ

サブドメイン名を辞書攻撃的に問い合わせ、応答が返るかで存在を確認できる。
ワードリスト（例: www、mail、dev、test、vpn）を組み合わせてDNSクエリを大量に投げ、応答があるものを列挙。
amass、sublist3r、assetfinder などOSSツールで自動化可能。
ワイルドカードDNSが設定されている場合はフィルタリングが必要。
PTRレコードや逆引きゾーンからもヒントが得られる場合がある。

◆公開情報の収集

・証明書のTransparency Log

HTTPS証明書は「Certificate Transparency (CT)」ログに登録される。

crt.sh などの公開リポジトリを検索すると、*.example.com のようなSAN欄やCN欄に記載されたサブドメインが確認できる。

・検索エンジンキャッシュ

GoogleやBingにインデックスされたURLから sub.example.com が見つかる、検索エンジンにキャッシュされてればね。

site:example.com -www のような検索式で候補を抽出できる。

・OSINTツール／DNSDB

shodan、CensysなどのOSINTを利用しサブドメインが割り当てられた資産を特定することや、

Passive DNS（Farsight DNSDB、RiskIQ、SecurityTrails など）により、過去のDNS解決結果を参照し

サブドメインを特定できることがある。

◆ブルートフォース型アプローチ

※p.24の手法と重複、手法であって手段はp.24の内容。

◆クラウドサービス・開発環境からの露出

AWS S3、Azure Blob、GitHub Pages などクラウドホスティングのFQDNからサブドメインを特定できる場合がある。

誤って公開されたソースコードや設定ファイル（例: .env、config.json）にサブドメインが含まれているケースもある。

◆インフラ・サービス利用痕跡の解析

・リソースレコードの連鎖

MX（メールサーバ）、NS（ネームサーバ）、SPF/TXT レコードに他のサブドメインが記載されているケースがある。
例：v=spf1 include:_spf.mail.example.com から _spf.mail.example.com を辿るとか。

・CNAMEチェーン

あるFQDNがCNAMEで別サブドメインを参照している場合、それを追うことで新しいサブドメインを把握できることがある。

◆ネットワークスキャンによる情報取得

・逆引きスキャン（PTRレコード）

対象ドメインの利用IPレンジを推測（WHOIS・ASN情報から）し、
そのIP帯でPTRレコードを逆引きすると、サブドメイン名が判明することがある。

・TLSハンドシェイクのSNIや証明書解析

特定のIPアドレスに対してポート443のTLSハンドシェイクを試みると、
※SNIフィールド やサーバ証明書に複数のサブドメインが含まれている場合がある。
Shodan/Censys などのOSINTはこれを利用しているっぽい、知らんけど。

※SNIとは
（Server Name Indication）とは、1つのIPアドレスで複数のドメイン名を扱うサーバーに、適切なSSL証明書を提示させるためのTLSの拡張機能

◆サードパーティ情報の利用

・WebアセットやCDNからの露出

JavaScript、CSS、APIエンドポイント内に別サブドメインがハードコードされていることがある、あざす。
CDNサービス（Akamai、Cloudflareなど）のログや構成から別のサブドメインが見えることがある。

・モバイルアプリ解析

企業公式アプリの通信先ドメイン（apk/ipaの逆コンパイルで確認）から内部APIサブドメインが発覚する。

・公開リポジトリや設定ファイル

GitHub/GitLabにコミットされた.envやconfig.yamlなどから漏れることがある、どうも～。

◆トラフィック観測・データベース利用

・パッシブDNS / セキュリティデータベース

脅威インテリジェンスサービス（例: RiskIQ、PassiveTotal、SecurityTrails）に過去解決履歴が蓄積されており、
そこからサブドメインを列挙できることがある、商用のサービスはそこそこする。

・広告/解析タグ経由の関連性発見

Webサイトに埋め込まれたGoogle Analyticsや広告タグの「アカウントID」が一致するサイト群を横断調査することで、
関連サブドメインを発見できることがある。

◆誤設定による露出（人為的ミス）

- **誤設定したrobots.txtやsitemap.xml**
  サイトマップやクローラ制御ファイルに内部サブドメインのURLが記載されている場合がある。

- **メールヘッダや公開ドキュメント**
  組織が発行するメールのReceivedヘッダやPDF/Wordのメタデータに内部サブドメインが残っていることがある。

◆セキュリティ上の危険性

・攻撃者はこうした方法で「利用されていないが公開状態のサブドメイン」を見つけ悪用する恐れがある。
・脆弱なテスト環境や古いサービスなど管理されていないサービスを足掛かりに侵入されるリスクもある。

◆防御のための推奨策

・定期的に **ASM（Attack Surface Management）**ツールやオープンソーススキャナ、
OSINTを利用し自社ドメインを調査しましょう！！！
・CTログ監視（例: crt.sh モニタリング）を導入する。
・廃止済みのリソースに紐づくサブドメインを解放しないように管理する。
・ワイルドカードDNSやゾーン転送設定の誤りをチェックする。

サブドメインはDNSの仕組み・公開証明書・検索エンジン・パッシブDNSなどの
外部情報源から収集できるため、組織は外部目線での監査を定期的に行う必要があります。

攻撃対象領域へのセキュリティ対策・監視について

第二章　攻撃対象領域へのセキュリティ対策・監視について

グランセキュノロジー渡邉氏が詳しく解説してくれる！
俺の説明よりちゃんとしてはる！

多分な！

モリシタン、隠れモリシタンの皆様へ

第三章

だいぶ軽い感じでお話はしましたが……

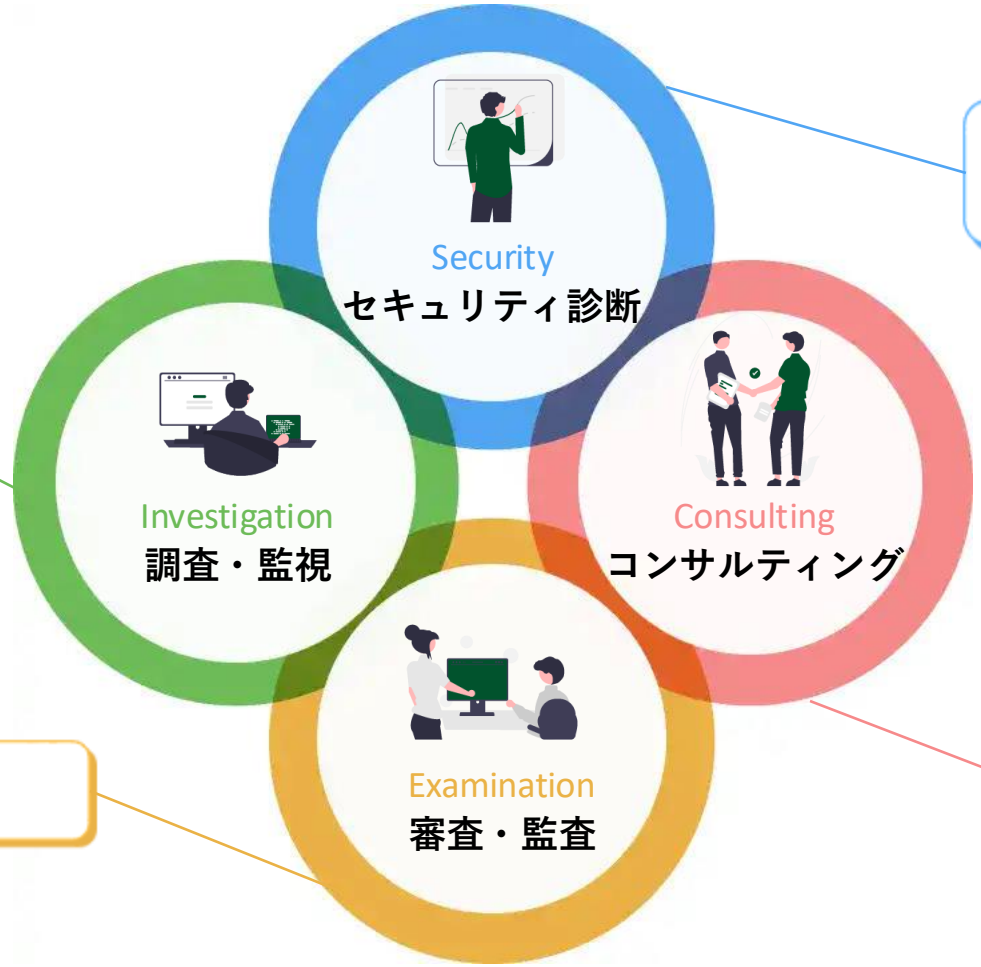
当社は大手企業や金融機関、官公庁、自治体にも頼っていただいているしっかりした会社です！

※アルファベット順

全日本空輸グループ各社 ／日本放送協会（NHK） ／花王株式会社 ／株式会社セブン銀行 ／株式会社プレコフーズ ／
株式会社長谷工コーポレーション ／富士急行株式会社 ／湘南美容クリニックグループ ／株式会社ポニーキャニオン ／
ビッグローブ株式会社／NTTデータ先端技術株式会社 ／きらぼしテック株式会社 ／グローリー株式会社 ／株式会社はてな／
株式会社セプテーニ／GMOクラウド株式会社 ／株式会社船井総合研究所／ネットイヤーグループ株式会社 ／金融機関 ／官公庁
／地方自治体 ／大学・教育機関／ etc.

第三章

だいぶ軽い感じでお話はしましたが……



セキュリティ診断

1. 脆弱性診断
2. ペネトレーションテスト
3. セキュリティレビュー

調査・監視

1. フォレンジックサービス
2. ログ保管・分析

審査・監査

1. PCI DSS審査
2. セキュリティ監査

コンサルティング

1. セキュリティ支援
2. 認証取得・準拠支援
3. 教育・研修

ログの保管方法にご不安がある場合は、セキュリティレビューやコンサルなどのサービスでサポートしています！

だいぶ軽い感じでお話はしましたが……

- モリシタンの皆様
- 隠れモリシタンの皆様
- これからセキュリティ対策を実施される皆様

どうぞ、さまざまな用途でご利用ください。

セキュリティが一定水準以上で実施できている組織はモリシタン大名

守#

モリイサン

モリイサンを起動させるためには、以下の質問に答える必要があります。

It is necessary to answer the following question to start moriisan.

セキュリティハジメマスカ？

Getting started with Security !

YES
はい

NO
いいえ

ご清聴ありがとうございました