

セキュリティと和解せよ！

南海の大決闘

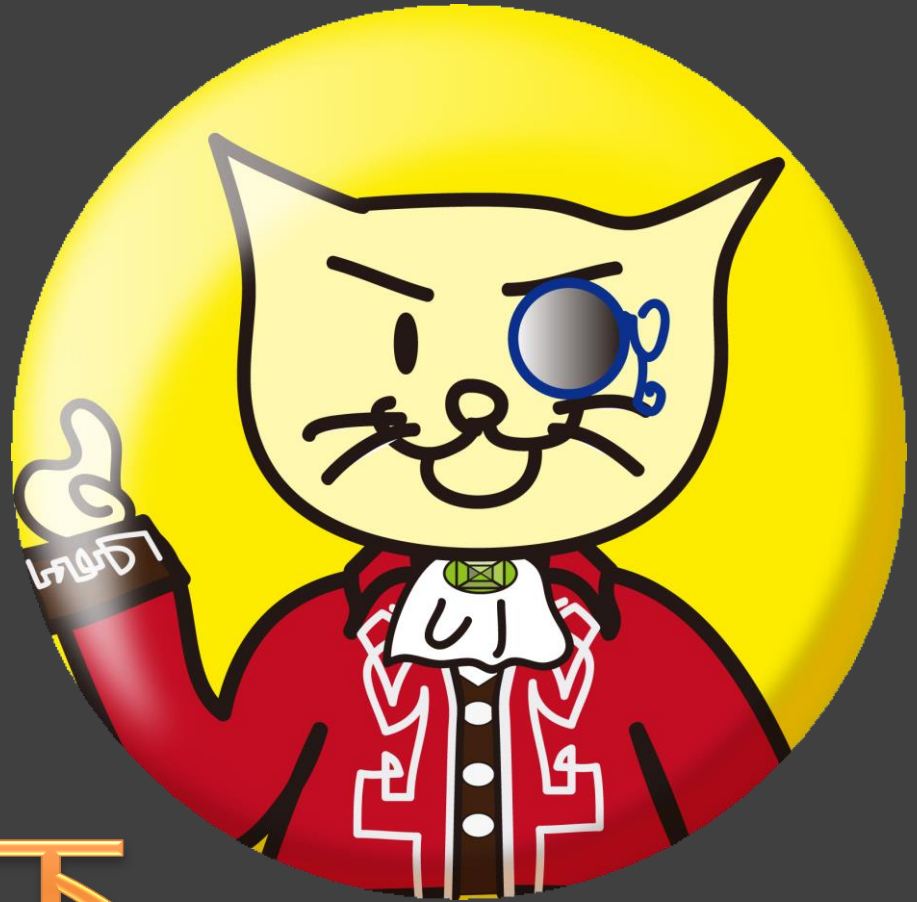
～小さいプロジェクトのセキュリティ超入門～

ニャゴロウ

(又の名を小笠原種高)



Who Am I?



にゃごろう陛下

モウフカブールの人。職業はニートと名乗りたいのだが、年齢を超えてしまったので、本とネットをさすらう風来坊ということにしている。できるだけ家から出たくない。世を忍ぶ仮の姿として、時々本を出したり、開発に関わっている。

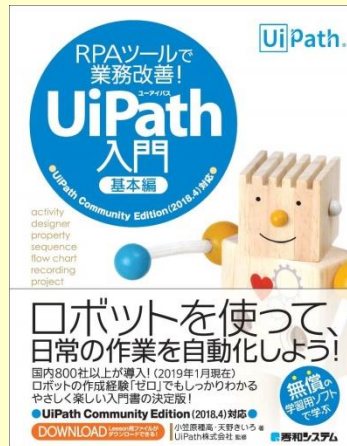


小笠原種高 最近の活動 ³



日経 Xtech Active

ドキュメント編、会議編、時間短縮術、プレゼン編など





本題

Presented by
Mofukabur





What is security

セキュリティって
何ジャロ？



MOFUKABUR



英語



日本語



security



セキュリティ

Sekyuriti

sə'kyoorədē

「security」の翻訳

名詞

安全

safety, security, keeping, preservation, sureness

保障

security, guarantee

保安

security, peace preservation

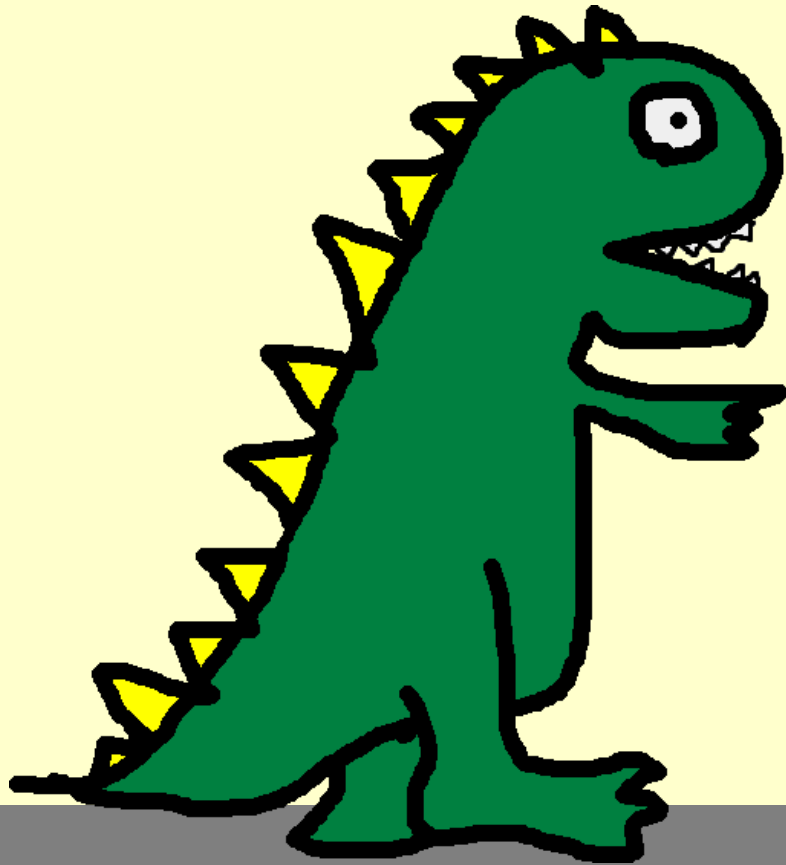


国家の安全

世界の安全

地球の安全





ゴジラから
地球を
守れない。
(伏線回収その①)

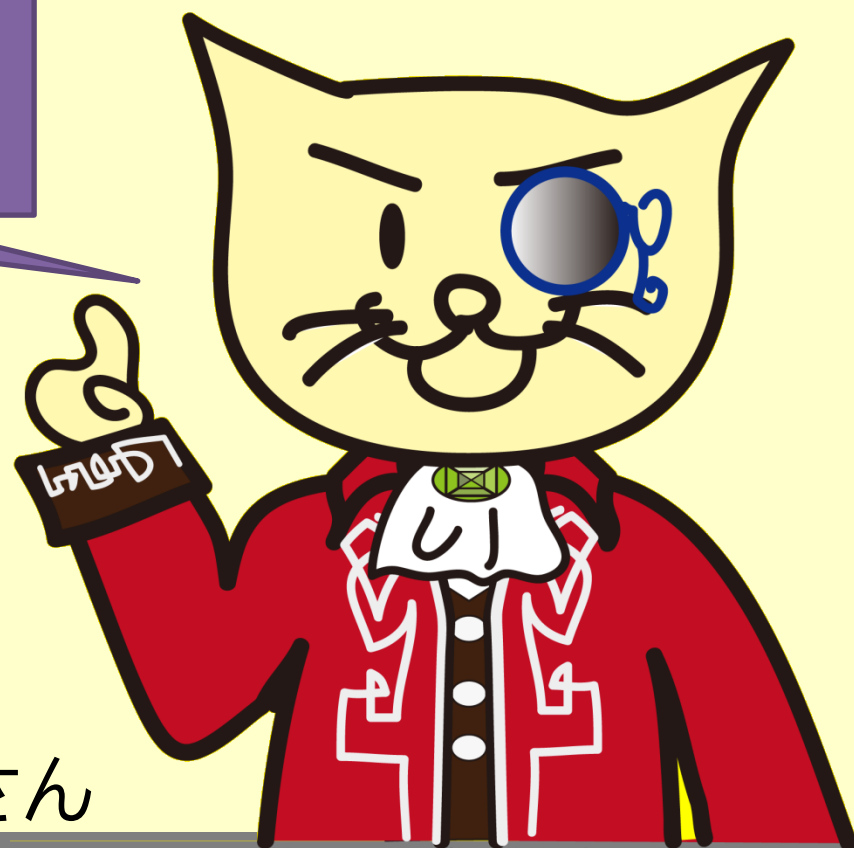
MOFUKABUR



我々が関わる安全

9

情報セキュリティ



ニャゴロウさん

Presented by Mofukabur



2. 5情報セキュリティ (information security)

情報の**機密性**、**完全性**及び**可用性**を維持すること。

さらに、真正性、責任追跡性、否認防止及び信頼性のような特性を維持することを含めることもある
(JISQ27000:2019)





機密性・可用性・完全性とは

11

データが正当であること
＝改竄されていない
壊れてない

情報の CIA

完全性
(Integrity)

機密性
(Confidentiality)

正当な権利を持った人だけがアクセスできること
＝権利の無い人は見られない

可用性
(Availability)

必要な時にアクセスできること
＝ちゃんと使える





スパイの代名詞と言えば……

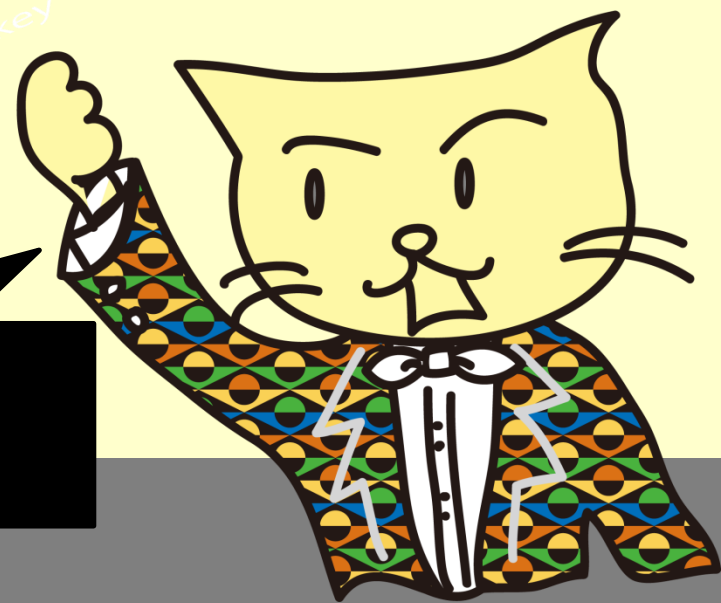
アメリカ……CIA

ソ連……KGB(今は連邦保安庁)

イギリス……MI6

イスラエル……モサド

覚えておきたまえ！



MOFUKABUR



情報セキュリティ
= CIAが保たれている

2.5情報セキュリティ (information security)

情報の機密性, 完全性及び可用性を維持すること。さらに, 真正性, 責任追跡性, 否認防止及び信頼性のような特性を維持することを含めることもある
(JISQ27000:2019)



にゃごろうさん



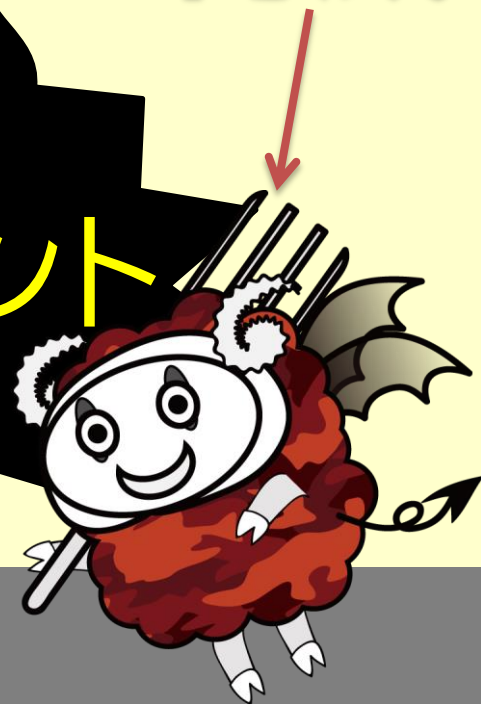
情報セキュリティが保たれてない！

個人や組織の活動や財産がピンチに陥ること
や、それを引き起こす状況



インシデント

脅威





脅威色々



15

クラッキングして
モスラ帝国の支配下に！



技術的脅威

クラッキングする
モスラさん

アッ！

物理的に踏み潰す
ゴジラさん



物理的脅威

ウツカリミスの
エビラさん(バイト中)

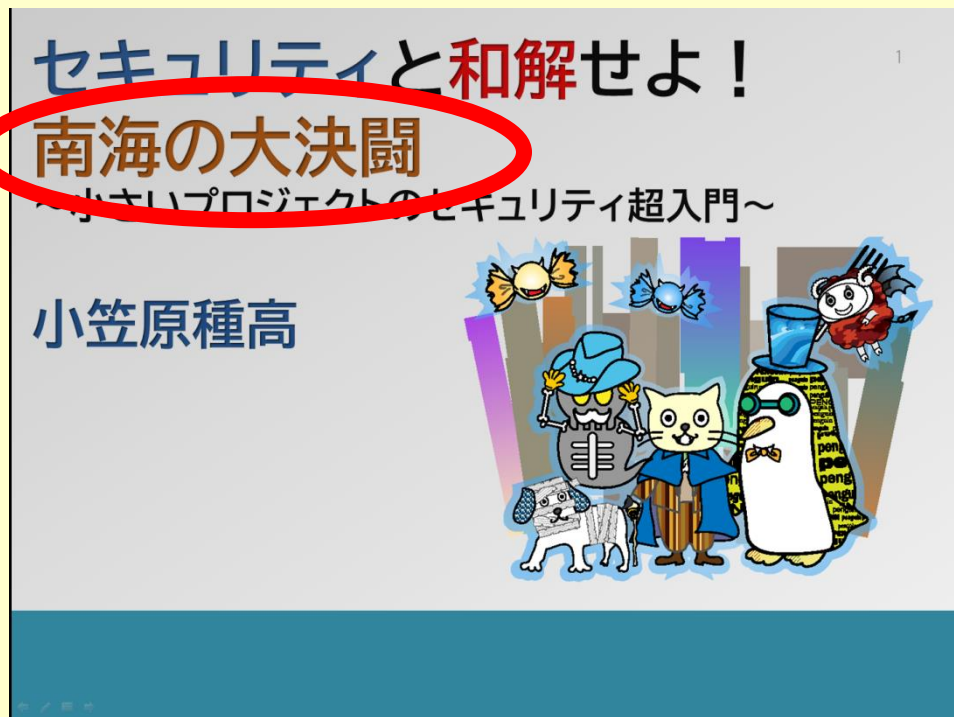
アーン！



人的脅威



伏線回収！



1966年ゴジラ映画7作目
「ゴジラ・エビラ・モスラ 南海の大決闘」
(伏線回収その②)



技術的脅威 人的脅威

物理的脅威

Presented by Mofukabur



How to defend.....?

インシデントを
防ぎたい



MOFUKABUR



脅威色々

18

CRACK !

CRACK !

技術的
脅威

アッ

人的
脅威

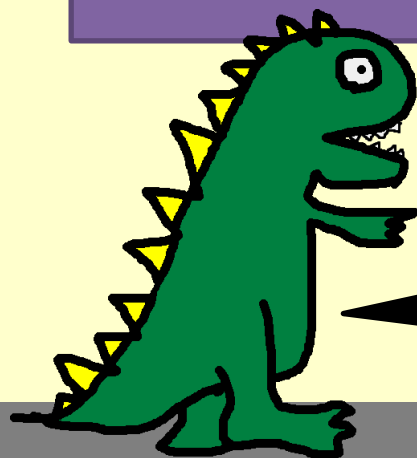
物理的
脅威

インシデント



結論から言うと

完全に防ぐのは
無理



きちゃった♥



にゃごろうさん

MOFUKABUR

- 知識がない
- 知識がある人もいない
- 顧客からお金が出ない

小さいプロジェクト(会社)
だから大丈夫

対策しなくて
良いっしょ
(暴言)





Ummmmmm.....

どうしたら
よいのだろうか？

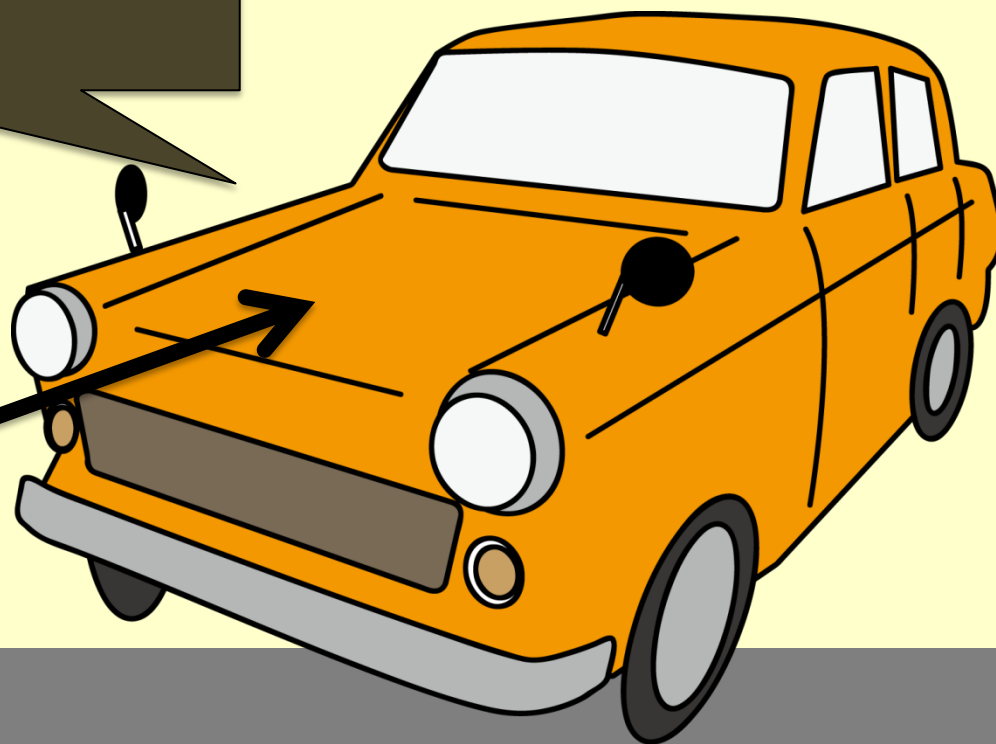


MOFUKABUR



友人の話

カギをかけない



MOFUKABUR

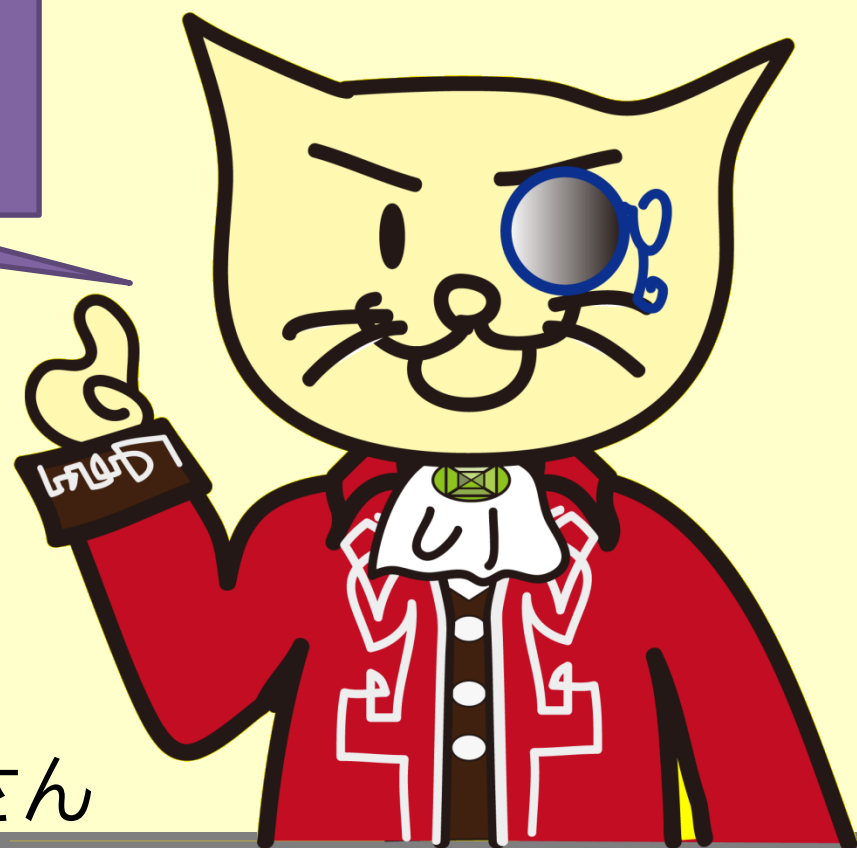
俺はどうしたら
いいんだ！

- 自分たちは、
何をしなければ
ならないか。





ぼくの考えた五原則



ニヤゴロウさん

Presented by Mofukabur



ぼくの考えた五原則

25

ぼくの考えた五原則



にゃごろうさん

何を？

- ・それは、守るべきものか？
- ・守るべきものは何か

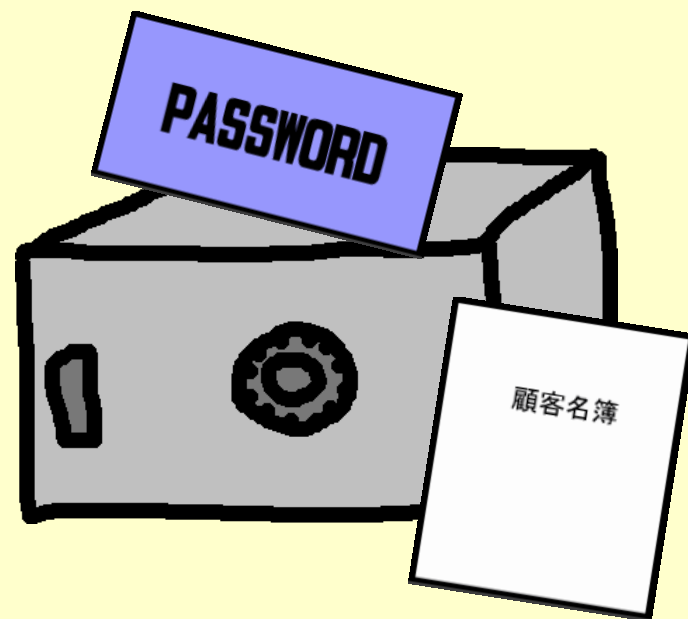


会社の住所や電話番号

モウフカブール株式会社
代表取締役社長 カブール団長
住所 東京都毛布区糸巻1-2-3
電話番号 03-XXXX-XXXX

公開しているものを
隠す必要はない

金庫の暗証番号や、
システムにアクセスするパ
スワード、
顧客の個人情報など





機密性・可用性・完全性とは

27

データが正当であること

機密性
(Confidentiality)

正当な権利を持った人だけがアクセスできること
＝関係ない人が見られるのは問題がある

完全性
(Integrity)

可用性
(Availability)

必要な時にアクセスできること

**情報の
CIA**

スパイはロマン



Presented by Pukabur



ぼくの考えた五原則

何を？

公開
情報

社内
のみ

担当者
のみ



にゃごろうさん

僕の
大事な
秘密

- ・それは、守るべきものか？
- ・守るべきものは何か？
- ・誰でも見られる情報は秘密にしないで良い
- ・何かあったら困るものは守る



ぼくの考えた五原則

29

ぼくの考えた五原則



にゃごろうさん

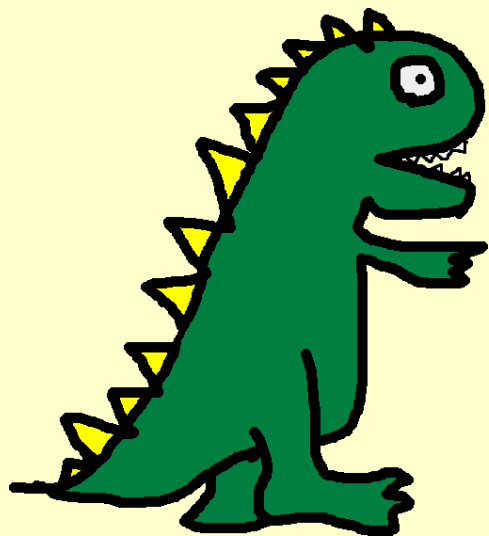
何を？

何か
から？

- どんな脅威があるのか？
- どんなインシデントが引き起こされるのか？



物理的脅威・人的脅威



物理的脅威

火事や、地震、停電、強盗
社長がLANケーブルに躓いてサーバが倒れた
など

ターン！ってやっちゃった、パスワードの漏洩、
満員電車でのお漏らし、
社長が間違えてLANケーブル抜いた
など



人的脅威



技術的脅威

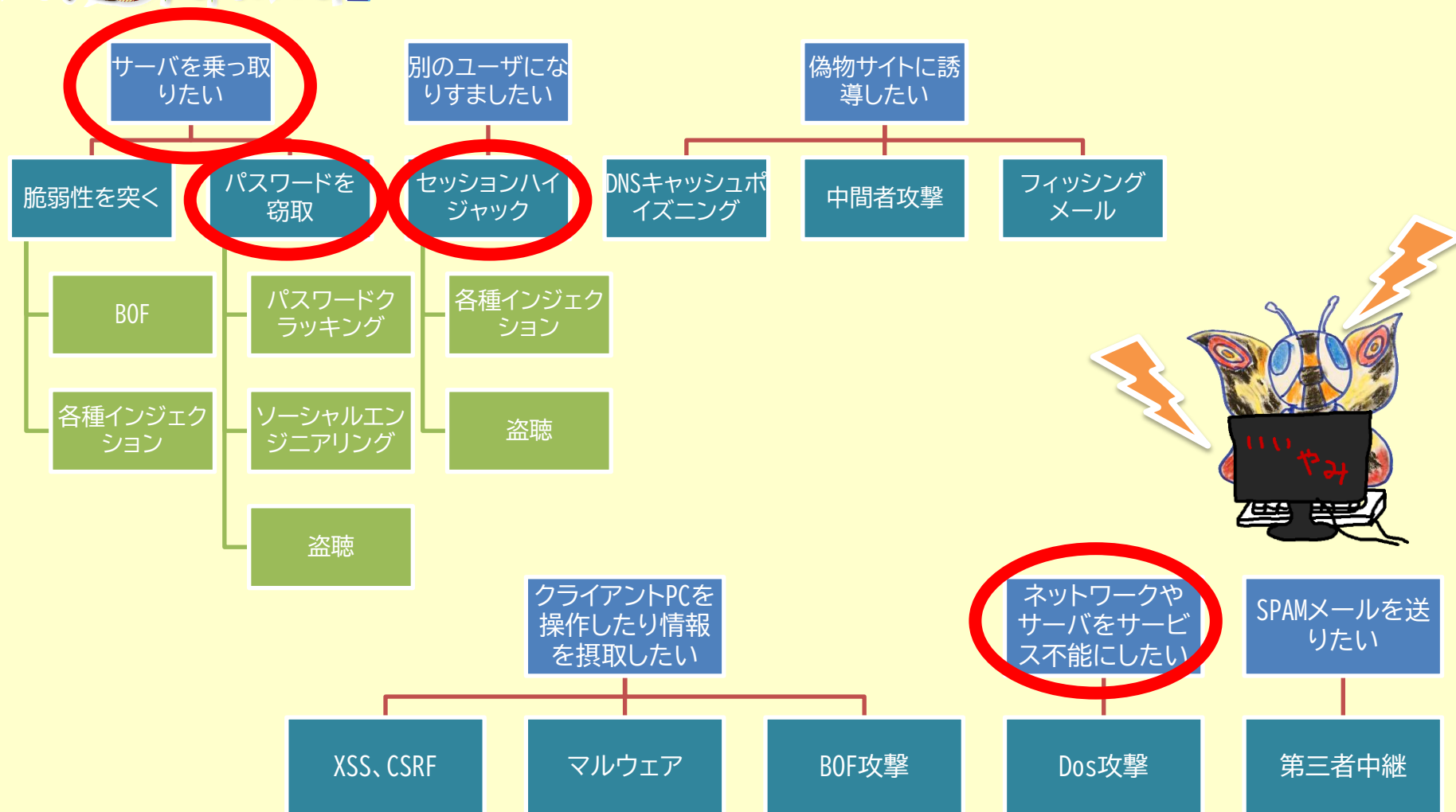
- 技術的脅威の仕組みを知る
- 「何を目的とするか」を押さえると、理解しやすい

クラッキングして
モスラ帝国の支配下に！





何を目的とした攻撃なの？





ぼくの考えた五原則

33

ぼくの考えた五原則



にゃごろうさん

何を？	何か ら？	どのよ うに？
-----	----------	------------

- 「誰が」「どのように」守るのか



誰がどのように守るの？



プログラムで対
策するよ

プログラマの大澤君
(この後15時からセッション)



顧客がお金を出さないと言う
から、何かあってもウチは責
任を取らないと契約書に明記
した

やくざなプロジェクトマネージャの僕



FWで防ぐよ

インフラ
エンジニアの
ライダーマン氏



ぼくの考えた五原則

35

ぼくの考えた五原則



にゃごろうさん

何を？

何か
ら？

どのよ
うに？

- ・「誰が」「どのように」守るのか
- ・どうやって守るのか
- ・脆弱性を塞ぐのか？
- ・サーバを隔離するのか？
- ・通信を制御するのか？

プログラムや設定上の
問題・欠点など
＝脆弱性



ぼくの考えた五原則

36

ぼくの考えた五原則



にゃごろうさん

何を？	何か ら？	どのよ うに？	続ける には？
-----	----------	------------	------------

- ・守り続けられているか
- ・守り続ける仕組みはあるか
- ・いつの間にか無くなっていないか



ぼくの考えた五原則

37

ぼくの考えた五原則



にゃごろうさん

何を？	何か ら？	どのよ うに？	続ける には？	やられた ら？
-----	----------	------------	------------	------------

- ・守れないならどうするか
- ・漏洩した時にどうするか
- ・侵入されたらどうするか
- ・壊れたらどうするか



バックアップ取れてなかった事件

バックアップが
取れてなかった

テープが入っているか、
確認はしていた
(回ってなかった)



保守を担当した
ライダーマン氏



ぼくの考えた五原則

39

ぼくの考えた五原則



にゃごろうさん

何を？	何か ら？	どのよ うに？	続ける には？	やられた ら？
-----	----------	------------	------------	------------

- ・守れないならどうするか
- ・漏洩した時にどうするか
- ・侵入されたらどうするか
- ・壊れたらどうするか



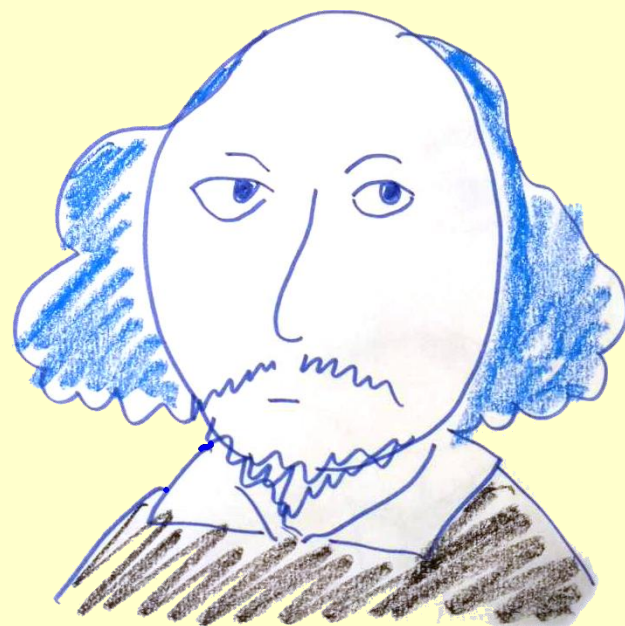
クロードィアスも言ってるよ。

「悲しみは
軍隊を連れてやってくる」
(意識)

When sorrow comes, they come
not single spies,
But in Battaliaes.

W.シェイクスピア
「ハムレット」4幕5場

インシデントは
軍隊を連れて
やってくる！





ぼくの考えた五原則

41

ぼくの考えた五原則



にゃごろうさん

何を？

何か
ら？

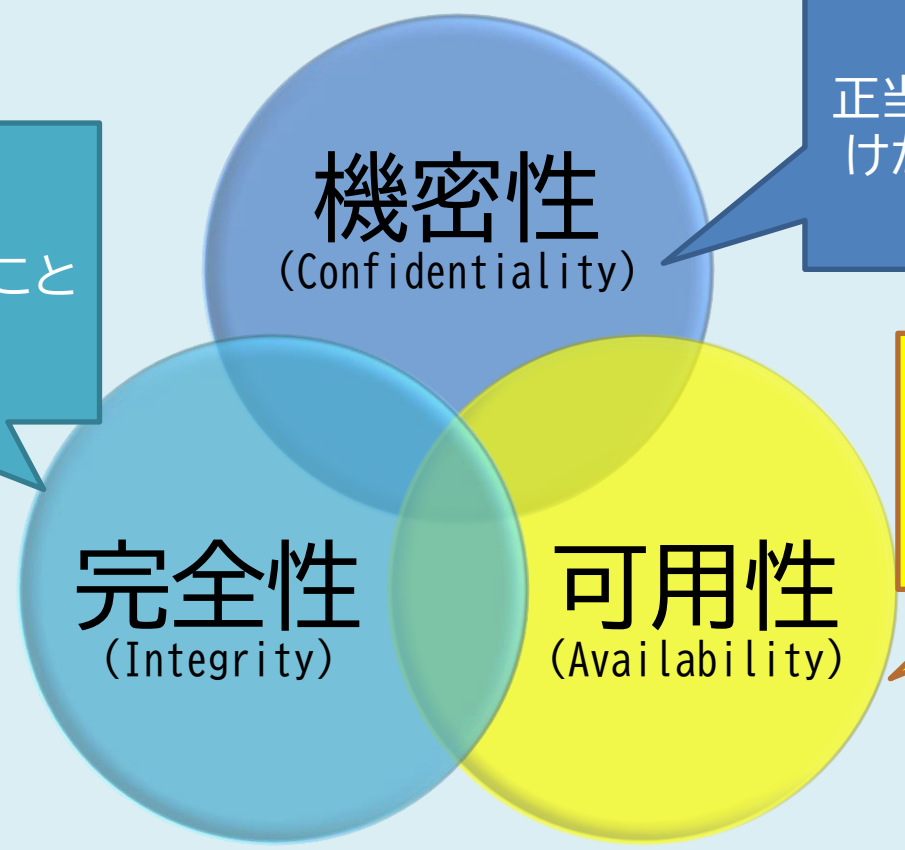
どのよ
うに？

続ける
には？

やられた
ら？

データが正当であること

情報のCIA



正当な権利を持った人だけがアクセスできること

必要な時にアクセスできること

情報セキュリティを保つ



にゃごろうさん



今日のまとめ

43

情報のCIAを保つ



Presented by Mofukabur



今日のまとめ

44

情報のCIAを保つ

完全に防ぐのは無理

Presented by Mofukabur





情報のCIAを保つ

完全に防ぐのは無理

五原則で考える





南海の大決闘は三つ巴じゃ無い

46



三つ巴じゃ
ない





宣伝 ⁴⁷

WSL2

Mac

Linux



仕組みと使い方がわかる

Docker&Kubernetes のきほんのきほん

マイナビ出版 2992円

2021年2月1日発売！！

重版というか、**6刷**です。
ありがとう！



コンテナはイメージ (image) から作る

コンテナを作成するには、**DockerEngine**で操作するのですが、そのとき、**イメージ (image)**と呼ばれるコンテナの素^{※3}になるものから生成します。

イメージにはたくさんの種類があります。中に入れるソフトウェアによって、それぞれ用意されたイメージを使います。Apacheのコンテナを作りたいなら、Apacheのイメージを使いますし、MySQLのコンテナなら、MySQLのイメージを使うのです。

コンテナは、複数作ることができます。容量が許す限り、Dockerの上にいくつも載せることができます。

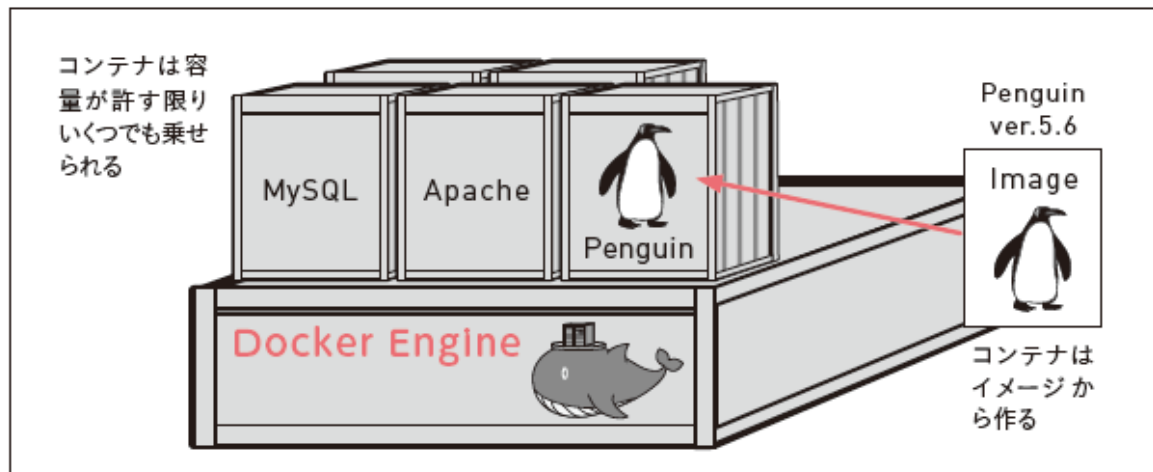


図1-1-4 コンテナはイメージから作られる

- 図が多い
- 構造から解説
たっぴり
- ハンズオンが多い
- Kubernetesもあるよ！





技書博・技術書典・コミケなどに参加 サークル名 モウフカブール

とらのあな、メロンブックス、
BOOTH、BookTechでも好評発売中！

Mofukabur
明後日から使える
Docker入門
この1冊で Docker の概要を掴む！
小笠原種高／浅居尚 著

256 Beginners

- ▶ 何から勉強していいかわからない
- ▶ Docker というものがイマイチわからない
- ▶ Docker についてすぐ知りたい
- ▶ とにかく Docker をわかりたい！

MOFUKABUR

Mofukabur
明後日から使える
AWS 入門
この1冊で AWS の概要を掴む！
小笠原種高 著

256 Beginners

- ▶ 何から勉強していいかわからない
- ▶ AWS というものがイマイチわからない
- ▶ AWS についてすぐ知りたい
- ▶ とにかく AWS をわかりたい！

MOFUKABUR

Mofukabur
明後日から使える
Kubernetes 入門
この1冊で Kubernetes の概要を掴む！
小笠原種高／浅居尚 著

256 Beginners

- ▶ 何から勉強していいかわからない
- ▶ Kubernetes というものがイマイチわからない
- ▶ Kubernetes についてすぐ知りたい
- ▶ とにかく Kubernetes をわかりたい！

MOFUKABUR

空飛ぶ
エンジン
ア用語辞典
その言葉 他人に説明できますか

256 Beginners

知ってるようで説明できないモヤモヤを解消

- ・ライブラリとフレームワークの違い
- ・機械学習は何か便利なのか
- ・SQL インジェクションとは何か
- ・OS は具体的に何をしているのか

これで知ったかぶりができる！
モウフカブール

おおよそ500円から770円くらい

ページは気持ち50頁程度

脚注が多いが、読まなくていい。何故なら、関係ない
雑談が書いてあるから。

Presented by Mofukabur





モウフカブール 参加イベント予定

新たなMBFES、ここに始まるー。

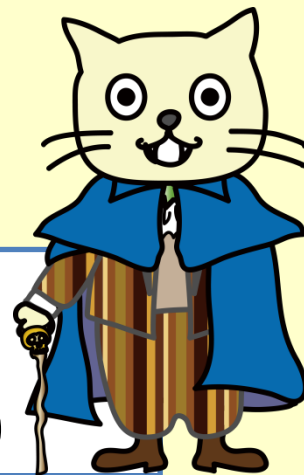


サザカル
MBFesTOKYO
2021.11.23 開催予定

2021.11.23 [TUE·HOLIDAY] 12:00~16:00 OPEN Circle OPEN 10:00~11:30
MBFES実行委員会

@プラザマーム(日本橋・人形町)
入場料 1000円

冬コミ
31日(金) 東ヒ42b



"知りたい技術"
が集まるイベント



第6回
技術書同人誌博覧会
@東京都産業貿易センター台東館

2月26日(226事件)
サークル募集中



Presented by Mofukabur



デバッグ音頭に続くCD……



恋するデータベース

- ・海とポスグレ
- ・MyLove, MySQL
- ・ぼくの大好きなMaria



メロンブックスに委託中。
ボーナストラックにDBの曲
が入ってます。

フルバージョンは、YouTubeで
視聴できます。
モウフカブールで検索！

デバッグ音頭は、
YouTubeで検索！





イラスト: 開田裕治



— 第4回 —
**映怪熱
画獣海
祭**

 ARTS COUNCIL
SHIZUOKA

2021年11月**21**(日)、**22**(月)、**23**(火・祝)

Presented by Mofukabur



・質疑応答

さっぱり
わからなかったのにゃ。

勉強していると親に言い訳しつつ
昼寝の多い生活を送っている
ニャゴローさん



FOLLOW ME !

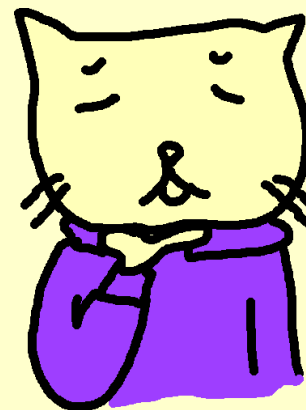
小笠原種高 @shigetaka256
モウフカブール @mofukaburTech





雑談:何を学ぶの？

セキュリティの本を読んだけど、
歯が立たない



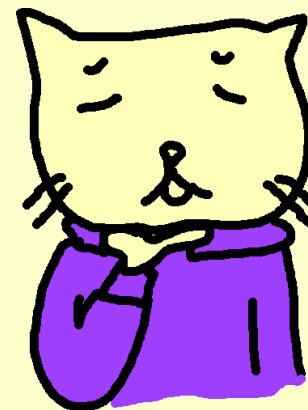
→セキュリティやdocker、AWS固有の話ではなく、
ネットワークやサーバ構築の知識が足りてないこと
が多い。





雑談:何を学ぶの？

ネットワークの本を読んだけど、
歯が立たない



- TCP/IP = ネットワークじゃない。
- HTTPもわからないと、セッション関係はわからんぞ。
- サーバを知りたいなら、サーバの本





- JPCERT/CC
- <https://www.jpcert.or.jp/>
- IPAの情報セキュリティ
- <https://www.ipa.go.jp/security/index.html>
- 脆弱性レポート
- <https://jvn.jp/>
- CODE BLUE
- <https://codeblue.jp/>



おわり



Website モウフカブール
<http://www.mofukabur.com/>