2019年度未踏IT人材発掘・育成事業

生命情報解析向けインタプリタを搭載した秘密計算用クラウド

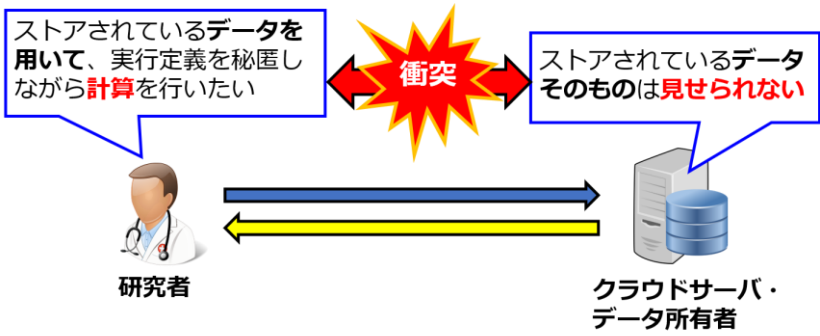
BI-SGX: Analyzing, only better.

早稲田大学大学院　櫻井 碧

■生命情報解析で用いるゲノムデータは、**様々な個人情報**を含んでおり、**漏洩**すると**非常に危険**

- **人種**
- **疾患**
- **予想される寿命**
- **体質**　　**etc…**

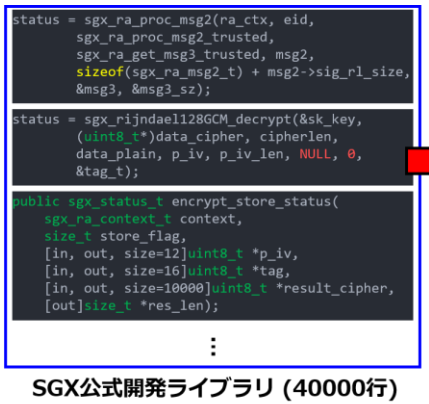
■一方で、こういった解析方法のニーズがある



■Intel SGXが生成するRAM上の**保護領域** (Enclave)上で**インタプリタ**を駆動させる事により、**簡単に**SGXの**ハイパフォーマンス**な**保護機能**の恩恵を受けた**秘密計算クラウド「BI-SGX」を実現**

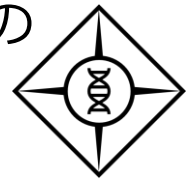
▶ストレージ機能・秘密計算機能の双方を提供

■独自言語「**Qliphoth**」により、**SGX公式SDK**を用いた場合の**10000倍**の**負担削減**が可能



```
status = sgx_ra_proc_msg2(ra_ctx, eid,
        sgx_ra_proc_msg2_trusted,
        sgx_ra_get_msg3_trusted, msg2,
        sizeof(sgx_ra_msg2_t) + msg2->sig_rl_size,
        &msg3, &msg3_sz);
status = sgx_rijndael128GCM_decrypt(&sk_key,
        (uint8_t*)data_cipher, cipherlen,
        data_plain, p_iv, p_iv_len, NULL, 0,
        &tag_t);
public sgx_status_t encrypt_store_status(
    sgx_ra_context_t context,
    size_t store_flag,
    [in, out, size=12]uint8_t *p_iv,
    [in, out, size=16]uint8_t *tag,
    [in, out, size=10000]uint8_t *result_cipher,
    [out]size_t *res_len);
⋮
```

SGX公式開発ライブラリ (40000行)




```
func main()
    a = edist("dataset0")
    println "result: ", a
end
```

Qliphoth (4行)

アウトプットプライバシを保護しつつ、劇的な負担削減を実現

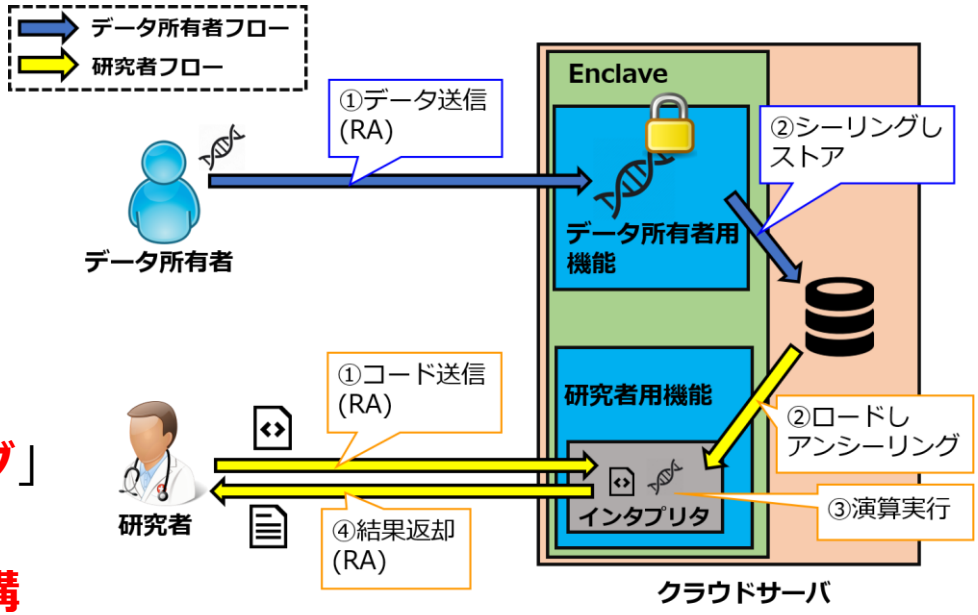
BI-SGX

■ Enclave内の**インタプリタ**と、SGXのセキュリティ機能をフル活用した**周辺機構**で**強固なセキュリティ**を実現

▶**厳重**な**遠隔認証プロトコル**「**リモート・アテステーション**」

▶よりデータの**完全性**を確実に担保できる**暗号化処理**「**シーリング**」による**データ保護**

▶大容量データ向けの**データ分割機構**



■ 生命情報解析向けではあるが、**より一般的・汎用的**な処理の実行も**可能**

```
func is_prime(n)
  return 0 ? n < 2
  return 1 ? n == 2
  return 0 ? n%2 == 0
  i = 3
  while i*i <= n
    if n%i == 0
      return 0
    end
    i = i + 2
  end
  return 1
end
```

```
func main()
  for n = 1 to 1000
    if is_prime(n)
      print n, " "
    end
  end
  println ""
end
```

素数計算プログラム

■ 一部**パブリッククラウド**上での駆動も**可能**である

クラウドサービス名	SGX対応のマシンがあるか？	SGXが有効化されているか？	BI-SGXが利用可能か？
Microsoft Azure	○	○	○
IBM Cloud	○	○	○
Alibaba Cloud	○	○	○
AWS	○	×	×
Google	○	×	×

より汎用的かつ大規模な秘密計算基盤の実現可能性がBI-SGXの今後の展望