

# What's CSIRT?

# ～ CSIRT<sup>※</sup>のススメ～ (※ Computer Security Incident Response Teamの略)

**Why** 毎回、同じようなトラブルに悩んでいませんか？  
(企業内の連携)

## 現状

✓先月SI部で起こった類似のトラブルが企画部でも発生してしまっ  
た。  
  
✓企画部は大変だったらしい。せ  
めてSI部と情報連携できてい  
れば・・・



## CSIRTがあれば・・・

### 事前予防

✓先月のトラブルをみんなに共有  
して、注意喚起しよう。

### 被害低減

✓万一トラブルに遭遇しても前の  
経験を活かして早期解決しよう。



**What** CSIRTは、  
企業内の「セキュリティインシデント消防署」



✓CSIRTは、**事故前提**(セキュ  
リティインシデント前提)の対  
応チームまたは機能です。

✓CSIRTは、セキュリティインシデントの  
窓口となり、情報や経験が集まってき  
ます。

✓CSIRTは、そのノウハウを活かし、セ  
キュリティインシデントに対する経験を  
積んだ消防員<sup>※</sup>として振る舞います。



※いざというときのメンバーとして振る舞えるなら、他の業務との兼務も可能です。  
その意味で、消防署ではなく、消防団に例えられることもあります。

**Why** あなたの力だけで十分ですか？(外との連携)

## 現状

✓A国で同じような事例が3か月も  
前にあったのか・・・もし知ってい  
れば手が打てたかもしれない。  
  
✓私の会社は、解析は得意だが、  
情報収集は苦手だな・・・



## CSIRTがあれば・・・

### 早期警戒

✓A-CSIRTから被害情報もらった。  
私たちが警戒しよう。

### 比較レビュー

✓他の会社ではこんなふうに情報  
収集を強化しているのか。参考に  
しよう。

### 相互補完

✓私たちの解析結果を外に共有  
して役立ててもらおう。

**What** CSIRTは、対外的な名刺になる



✓CSIRTは、対外的な交流をも解決します。あな  
たがCSIRTを自覚し、対外的に準備<sup>※1</sup>し、名乗る  
ことで、あなたの企業と他のCSIRTとの情報交換  
や協力を可能にします。

この関係は、あなたの企業のセキュリティに寄与する  
可能性があります。

✓CSIRTには、CSIRTの集うコミュニティ<sup>※2</sup>がいくつもありま  
す。

<参考(一部)>

日本シーサート協議会(国内CSIRTコミュニティ)

URL: <http://www.nca.gr.jp/>

FIRST(CSIRTの国際的コミュニティ)

URL: <http://www.first.org/>



※1※2 センシティブな情報を扱うため、コミュニティの参加には、審査が必要な場合があります。