

# マルウェア対策ラボの現場から ～Stuxnet,Duqu,Flame,Gaussと対峙して思うこと～

マルウェア対策研究人材育成ワークショップ(MWS2012)  
(2012年10月31日)

株式会社カスペルスキー  
情報セキュリティラボ  
チーフセキュリティエヴァンゲリスト

 前田 典彦 (まえだ のりひこ)  
maeda@kaspersky.co.jp

 @z\_norihiko

# Stuxnet



画像出典 : The New York Times

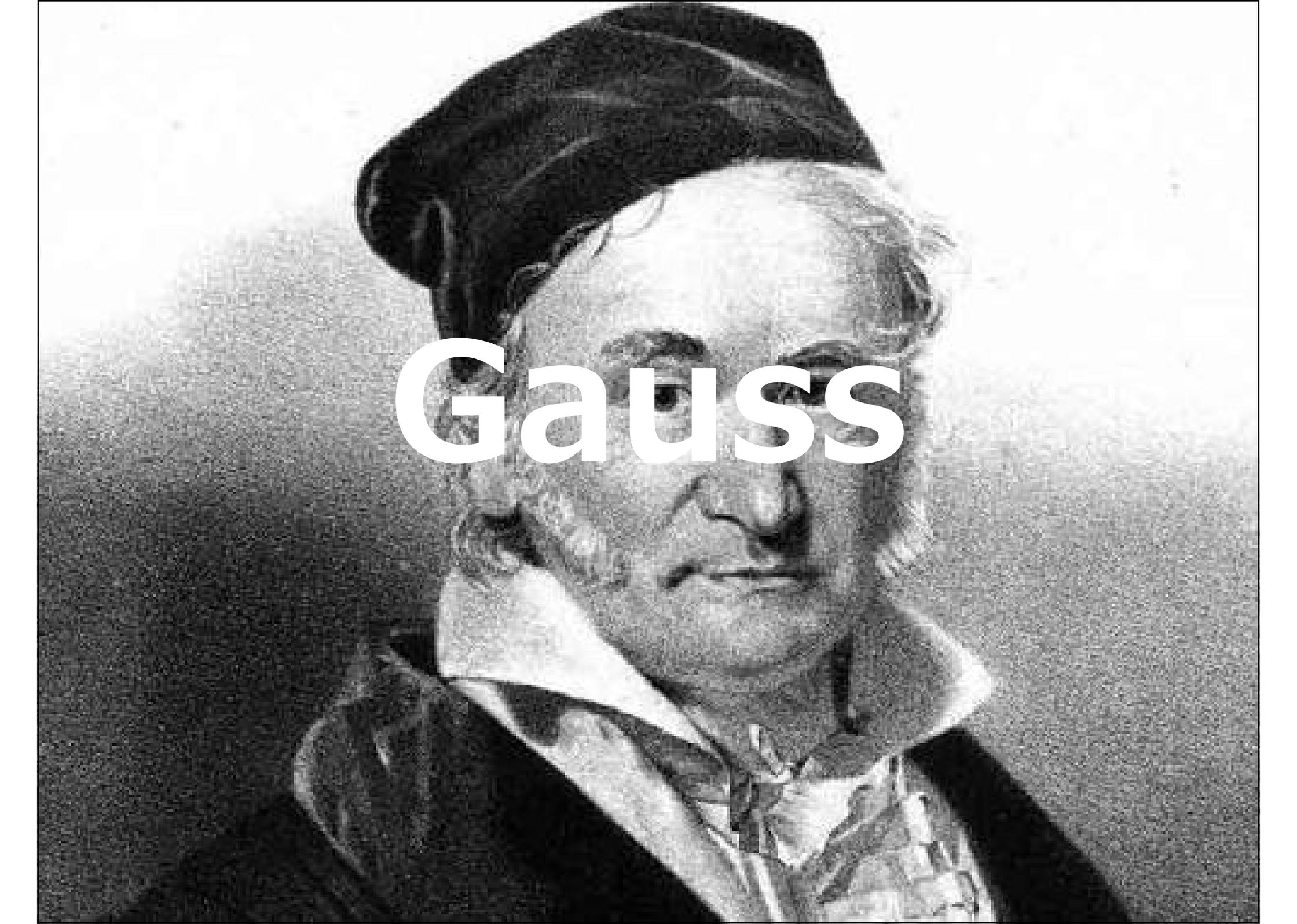
※画像はイランの核開発に関するものであり、Stuxnetと直接の関係はありません



Duqu

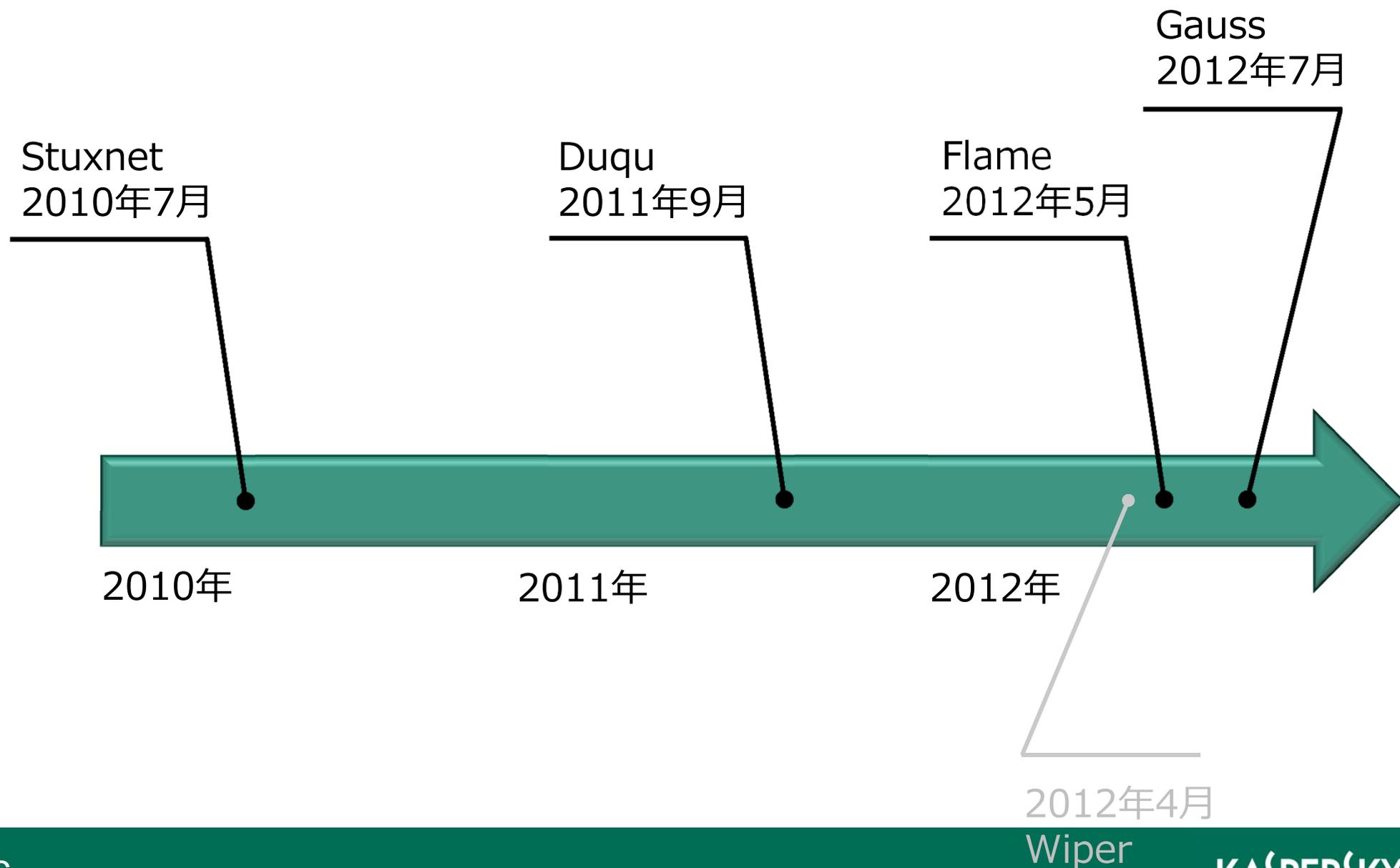
The image depicts a close-up, abstract view of a flame. The color palette is dominated by bright yellows and oranges, with some darker, almost black, areas in the background, suggesting the depth and intensity of the fire. The flame's structure is highly textured and fluid, with many thin, curved, and overlapping layers that create a sense of movement and depth. The overall effect is one of intense heat and energy. In the center of the image, the word "Flame" is written in a clean, white, sans-serif font, which stands out prominently against the fiery background.

Flame

A black and white portrait of Carl Friedrich Gauss, an elderly man with white hair, wearing a dark graduation cap and a dark suit with a white shirt and a dark tie. The name "Gauss" is written in large, white, sans-serif font across the center of his face.

Gauss

# 検出timeline



**S**tuxnet

**D**uqu

**F**lame

**G**auss

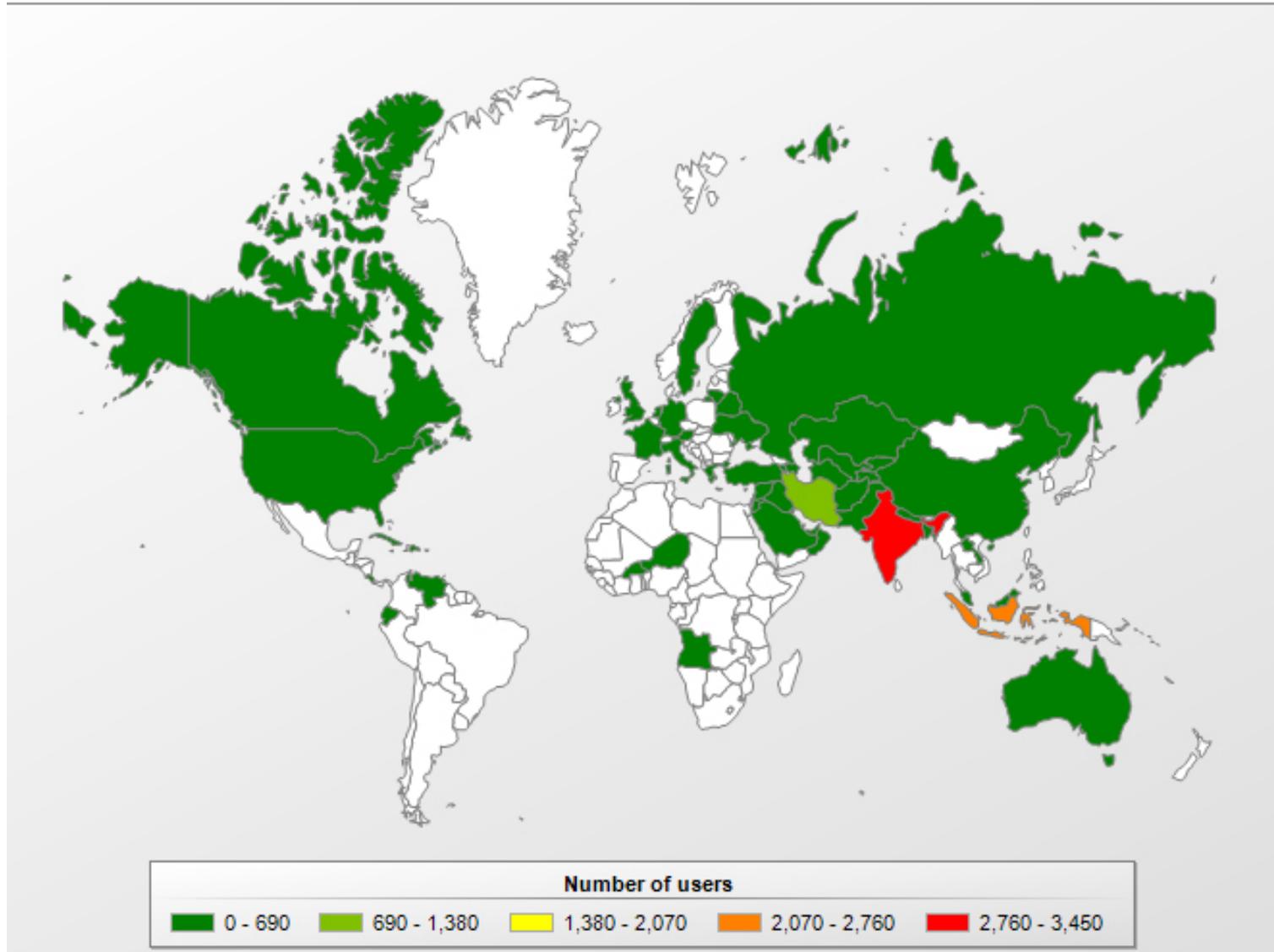
**?**



© 2012 Kaspersky Lab ZAO. All Rights Reserved

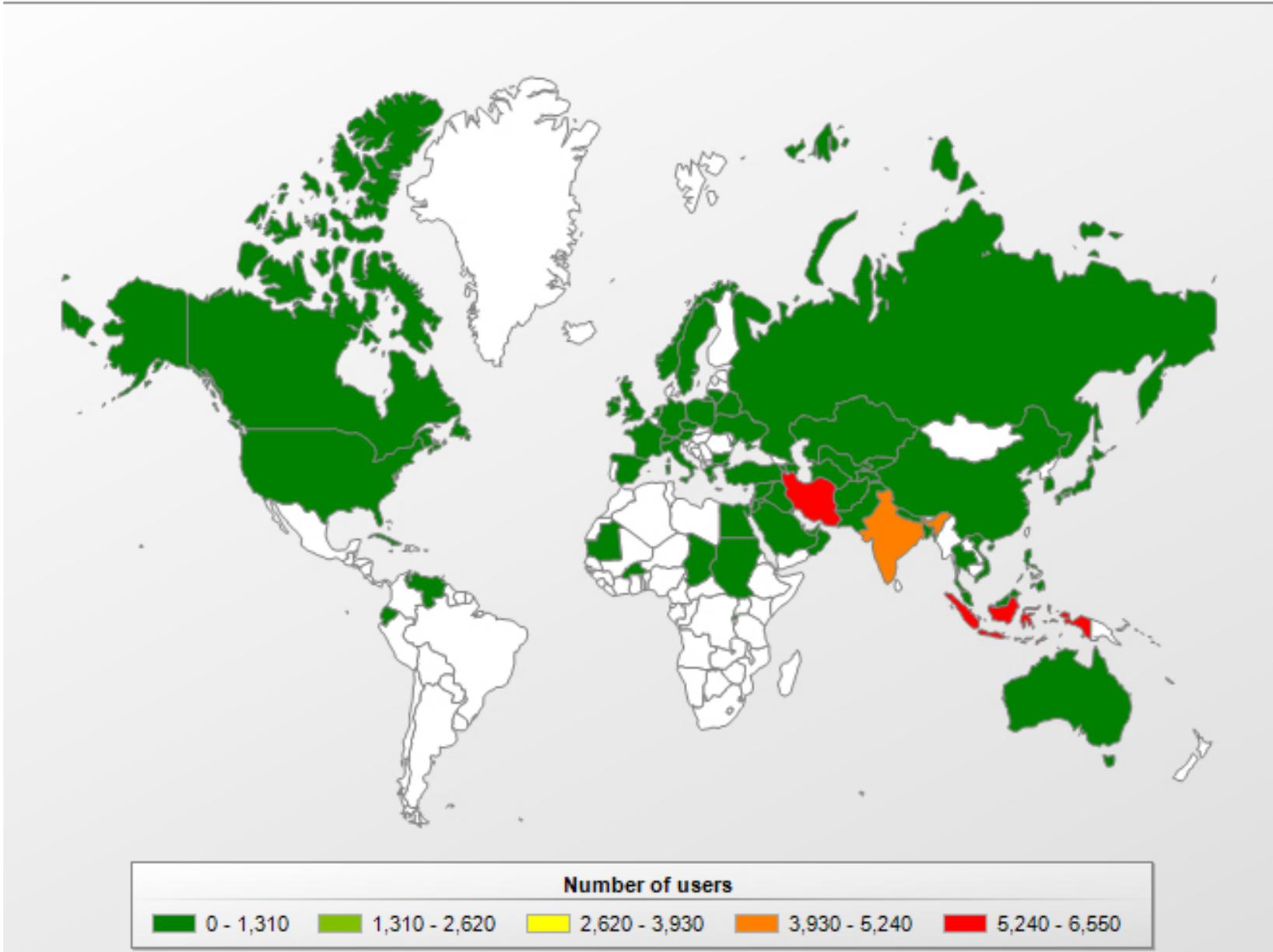
# Stuxnet検出状況（当時）

Trojan-Dropper.Win32.Stuxnet geography

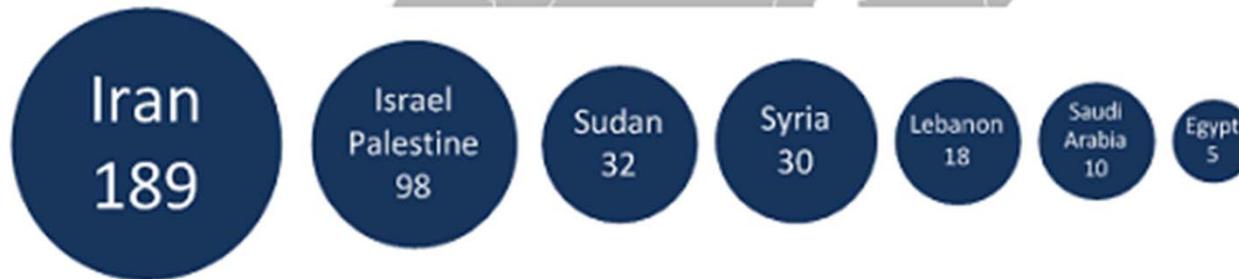


# Stuxnet検出状況（当時）

Rootkit.Win32.Stuxnet geography



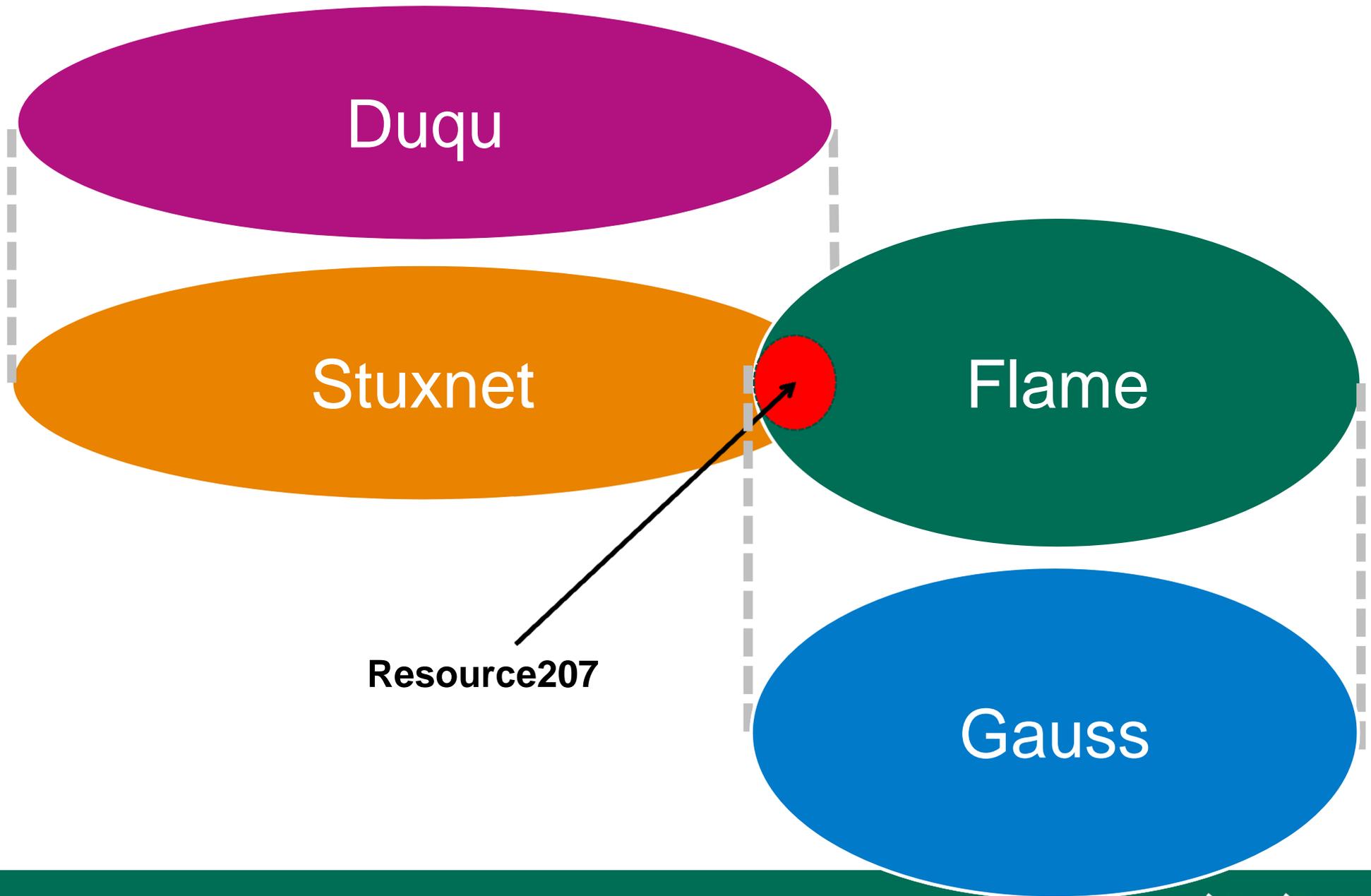
# Flame検出状況(当初)



# Gauss検出状況(当初)

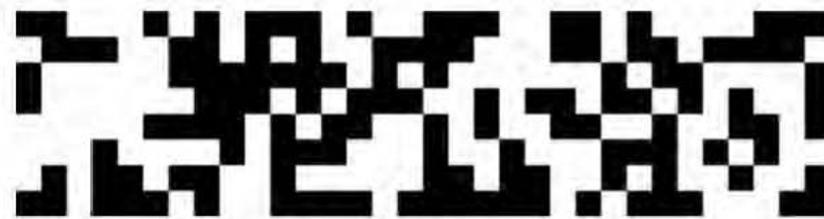
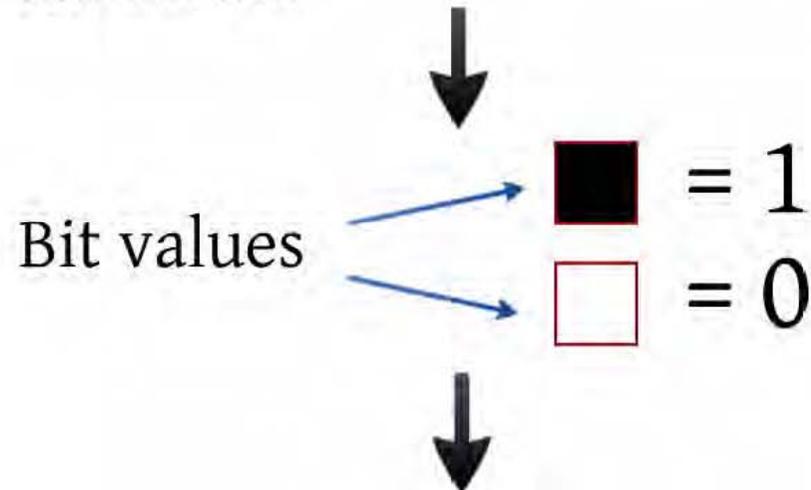


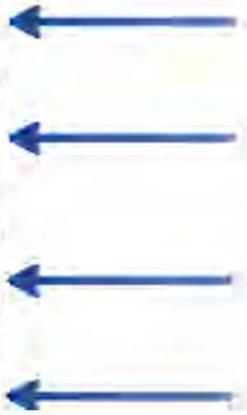
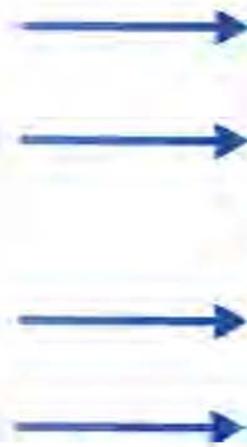
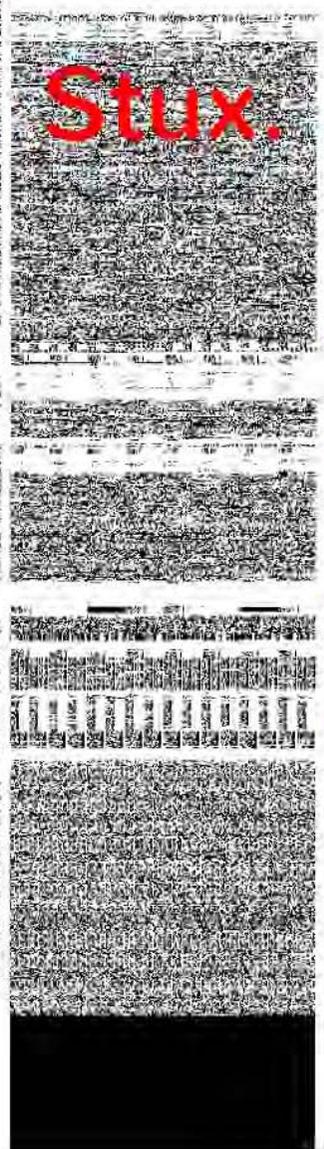
# Stuxnet, Duqu, Flame, Gauss

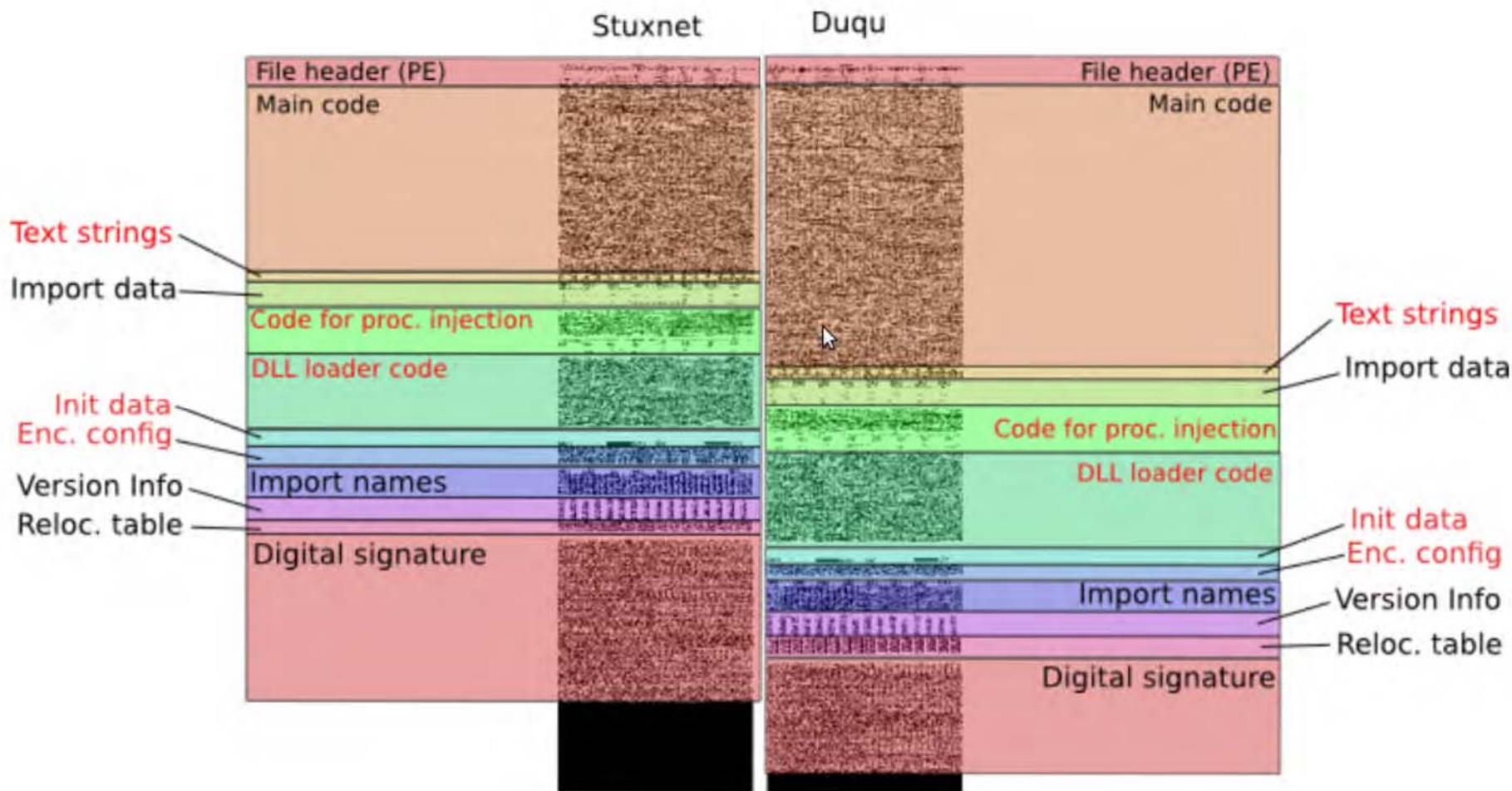


## Game of Binary Similarity

```
10100011 00101110 01100111 11100001 11001110 11001010  
01100011 01111011 11000001 01011111 10000001 10000110  
10000001 11101011 10110100 10010101 11100000 00110101  
01100101 10110010 00001000 00011101 10001001 00101011  
11011010 00000100 10011011 10010010 10111011 10111100  
01011111 11000111
```

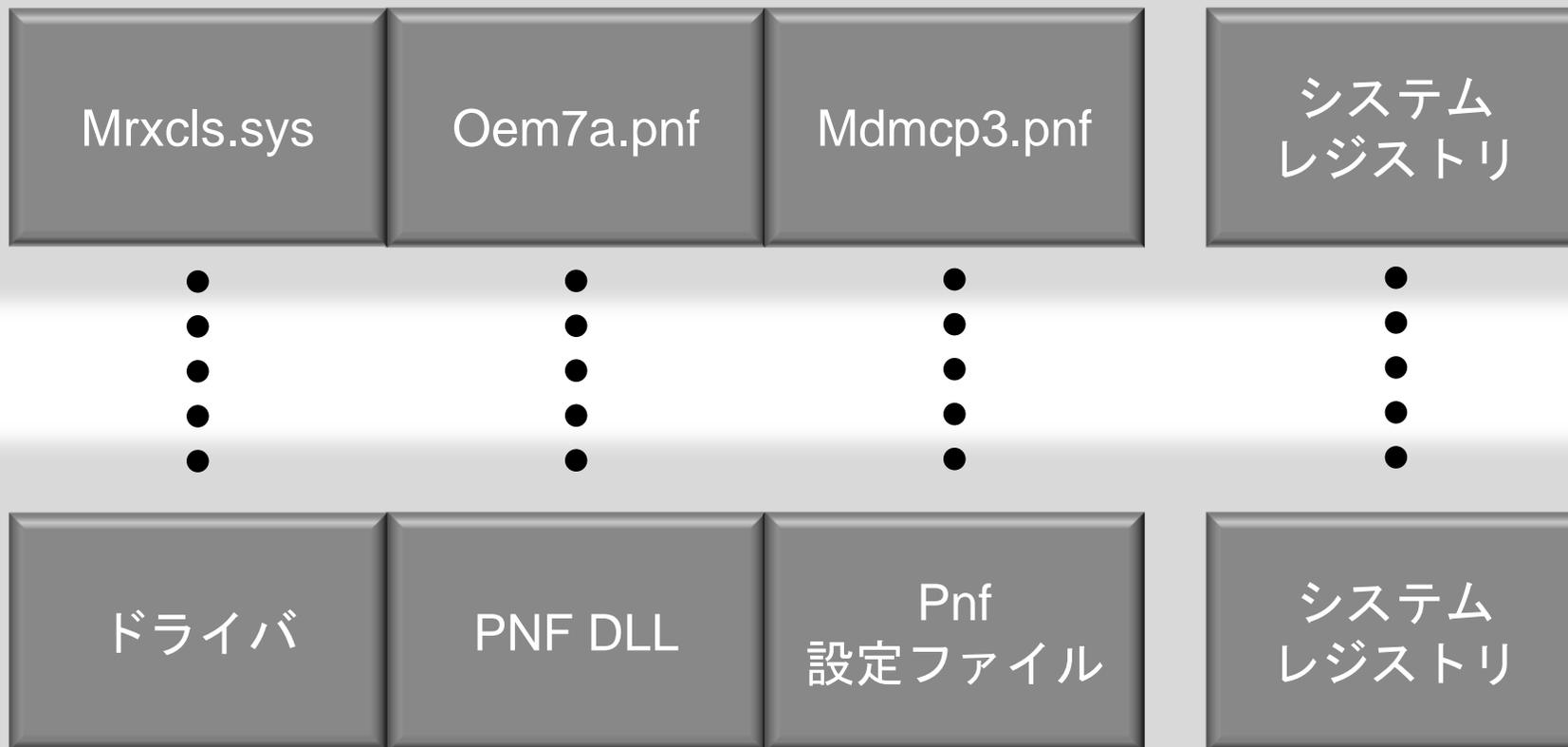






# DuquとStuxnetの構成相関

Stuxnet



Duqu

最後に

# 最後に

- 検体の収集
- 如何に迅速に解析できるか
- 如何に早期検出できるか
- 攻撃の全体像を把握するには

CnCをハッキングとか、したいと思ったりしますよね！？

# ありがとうございました

株式会社カスペルスキー

 前田 典彦

[maeda@kaspersky.co.jp](mailto:maeda@kaspersky.co.jp)

 @z\_norihiko

Kaspersky, カスペルスキーは、Kaspersky Lab, ZAOの登録商標です。  
その他の会社名・製品名等は一般的に各社の登録商標ないしは商標で  
す。本文書の無断配布・転記載・複製を禁止します。本文書の内容は  
事前の予告なく変更する場合があります。

©2012 Kaspersky Labs Japan

マルウェア対策研究人材育成ワークショップ(MWS2012)

2012年10月31日

**KASPERSKY** Lab