

Open Networking とセキュリティ

淵上 真一

淵上 真一

日本電気 株式会社 サイバーセキュリティ戦略統括部長
(ISC)² 認定主任講師
情報処理安全確保支援士 集合研修講師
Cisco Networking Academy Instructor Trainer
北海道大学 情報基盤センター 客員研究員

ベンチャー系システムインテグレータで
プログラマ、ネットワークエンジニアを経て、
専門学校グループを運営する学校法人に転職
組織のセキュリティコントロールを担当する傍ら、
司法、防衛関連のセキュリティトレーニングを手掛ける
2018年よりNEC NECグループのセキュリティ統括を担当



サイバーセキュリティの動向

900回/週

2021年に企業が受けた
サイバー攻撃の回数
(2020年の2倍)

11秒毎

11秒毎に
ランサムウェア攻撃
が発生

86.7%

ビジネスプロセスへ
影響が出た企業の割合

29.4%

オペレーションを完全に
停止した企業の割合

6兆\$

2021年の
サイバー攻撃による
世界の経済損失額

200億\$

(2.8兆円)

2021年の
ランサムウェア被害総額

66%

2019~22年に
ランサムウェアの攻撃
にあった組織の割合

179万\$

(2.5億円)

支払った身代金の
グローバル平均

[企業へのサイバー攻撃、1週間で平均900回も ハッカーに狙われる業種は？ | THE OWNER \(the-owner.jp\)](#)

[Top 6 Cybersecurity Predictions And Statistics For 2021 to 2025 \(cybersecurityventures.com\)](#)

[「ランサムウェア攻撃 グローバル実態調査 2022年版」を発表 | トレンドマイクロ \(trendmicro.com\)](#)

[CrowdStrike、2021年度版グローバルセキュリティ意識調査結果を発表](#)

[サイバーリスク及び保険調査2022](#)

※2019~22年に身代金を支払った
組織の割合 24%

サイバーセキュリティの動向

攻撃の巧妙化

攻撃の
ビジネス化

正規の機能
アカウントの悪用

内部犯行

拡大するリスク

大手ロジスティクのwebサイトに
不正アクセス
個人情報が流出



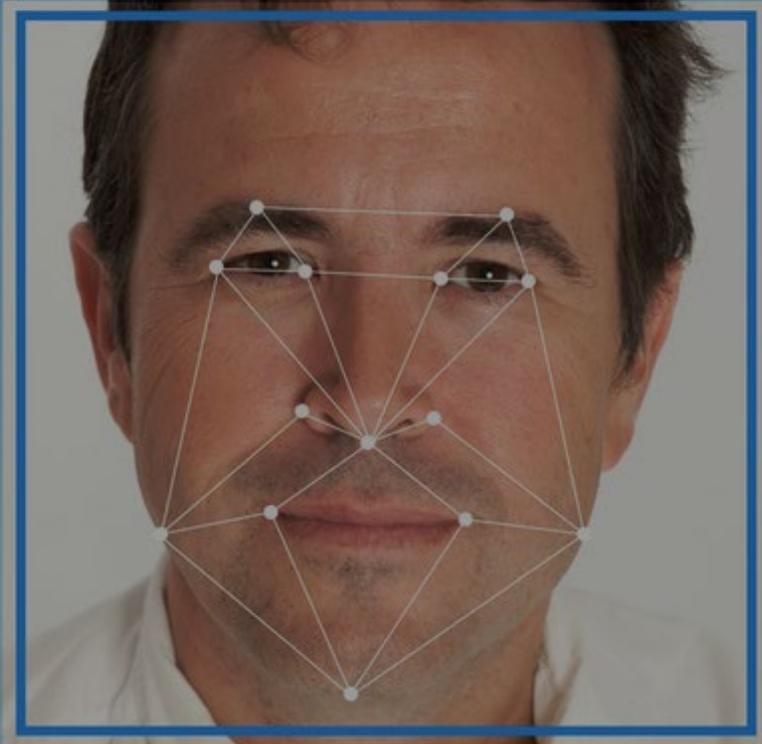
原因はパスワードリスト攻撃
(根本原因はユーザのパスワード使いまわし)



ユーザのミスも
企業の責任として問われた

拡大するリスク

00000 000 0 00000000 00100111
0000 0 0000 0 0 0 00 100010111
010011000010 01000111000110
00101110101000011110101010
1101000010 10 11111000001001



IDENTITY PROTECTION

Name:

Password:

00000 000 0 00000000 00100111
0000 0 0000 0 0 0 00 100010111

010011000010 01000111000110
00101110101000011110101010
1101000010 10 11111000

万引き防止システム
顔情報の共有



目的(機能要件/ビジネス)は果たしたが
人権侵害に当たるという指摘



レピュテーションリスク

拡大するリスク

ファストフード注文用Webサイトが
スクリーンリーダーに一部未対応



正しく注文できないのは法律違反※

※ADA法(障がいをもつアメリカ人法)に基づく訴訟

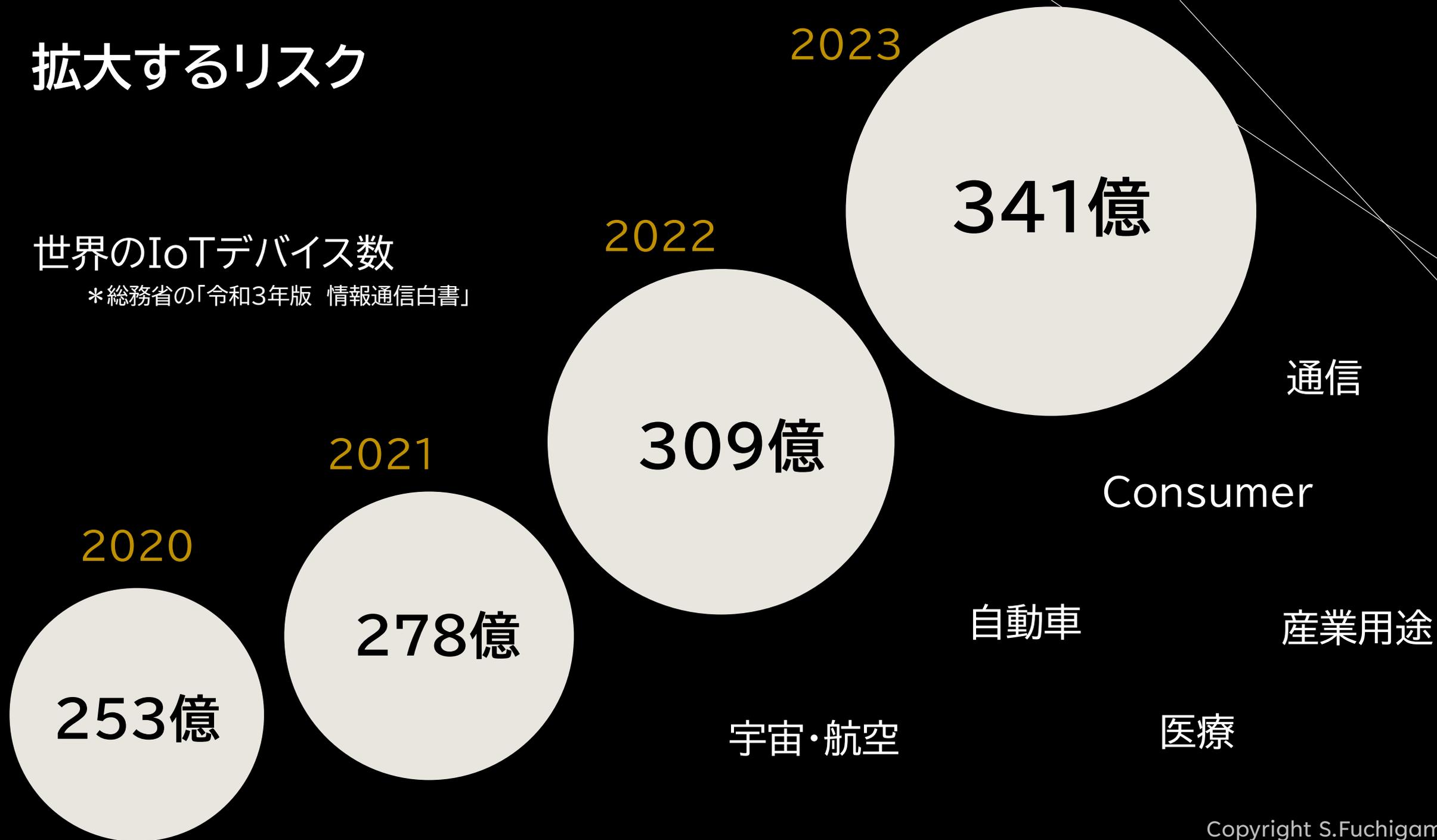


最高裁で敗訴 株価へも影響

拡大するリスク

世界のIoTデバイス数

*総務省の「令和3年版 情報通信白書」



ペリメタモデル

クローズドな世界は安全
(信頼の前提)
脅威は常に外部から



ゼロトラスト

信頼を積み上げる
脅威はあらゆる場所に

サイバーハイジーン

サイバーの手洗いうがい
基本的な対策の徹底

ゼロトラストアーキテクチャ

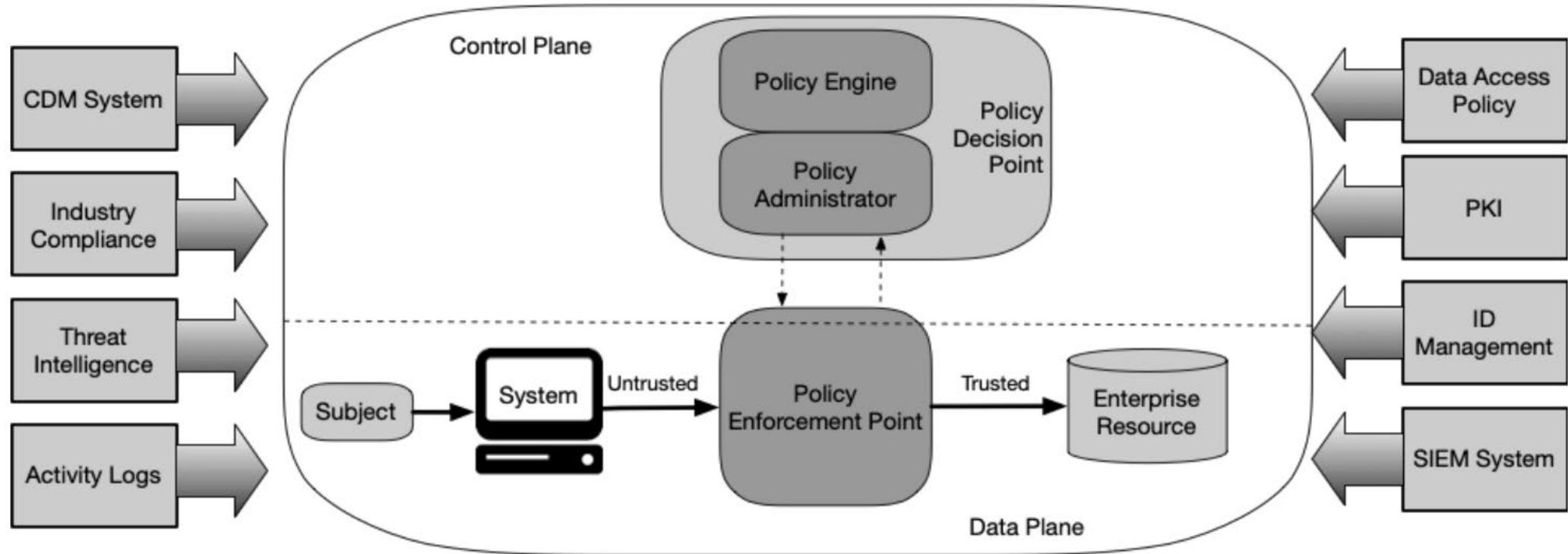


Figure 2: Core Zero Trust Logical Components

ゼロトラストアーキテクチャ

7つの原則	
 <p>全データ・計算資源を リソースとして識別</p> <p>1</p>	 <p>リソースへのアクセスは 動的ポリシーで決定</p> <p>4</p>
 <p>全ての所有機器・アプリの 安全状態を常に監視・測定</p> <p>5</p>	 <p>ネットワーク場所に関係なく 全ての通信の安全を確保</p> <p>2</p>
 <p>個々のリソースアクセスは セッション単位で許可</p> <p>3</p>	 <p>アクセスを許可する前に 動的・厳格に認証・認可</p> <p>6</p>
	 <p>機器・インフラ・通信状態の 情報収集・安全面の改善</p> <p>7</p>

ゼロトラストアーキテクチャ

データへのフォーカス

全てのデータをリソースに
全ての通信を安全に
セッション単位で

認証・認可

動的ポリシー
厳格な認証・認可

モニタリング

安全を常に監視
情報収集と改善

Security is not only authentication

ゼロトラストアーキテクチャ

データへのフォーカス

全てのデータをリソースに
全ての通信を安全に
セッション単位で

認証・認可

動的ポリシー
厳格な認証・認可

モニタリング

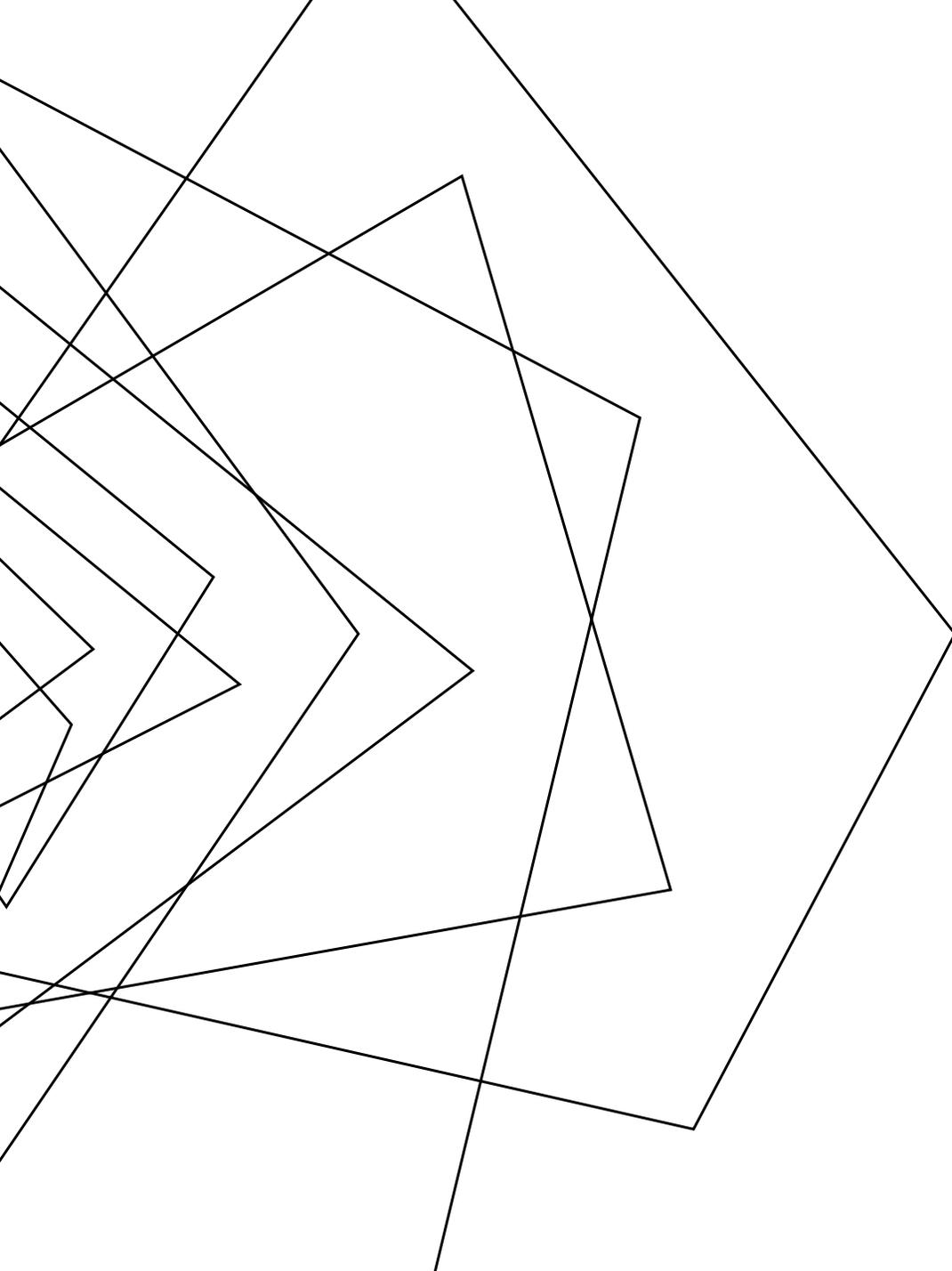
安全を常に監視
情報収集と改善

従来のNetwork



Open Networking

Elastic / Programmability / Flow Control



Build security into Open Networking
