



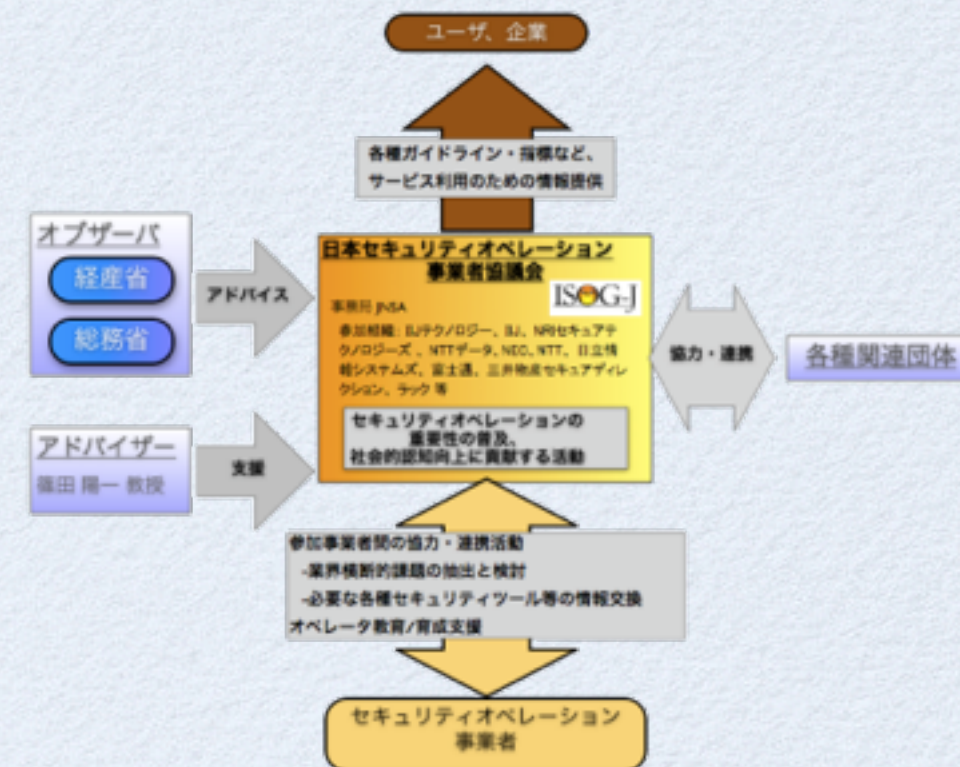
Security事業者と IPv6対応

日本セキュリティ事業者連絡協議会(ISOG-J)
(株)ブロードバンドセキュリティ
許 先明

ISOG-Jとは

- 目的

- セキュリティオペレーション事業 (MSSP/SOC)に関する普及啓発
- セキュリティオペレーションに関する業界横断的な課題の抽出と検討
- セキュリティオペレーションの重要性の普及
- セキュリティオペレータ間の交流の促進



項目	ISOG-J	経産省	総務省	警察庁	国土交通省	文部科学省	厚生労働省	農林水産省	環境省	国土形成省	デジタル庁	関係機関
ISOG-J	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授
経産省	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授
総務省	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授
警察庁	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授
国土交通省	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授
文部科学省	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授
厚生労働省	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授
農林水産省	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授
環境省	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授
国土形成省	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授
デジタル庁	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授
関係機関	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授	代表理事 篠田 陽一 教授

ISOG-Jの現在の活動

- セキュリティオペレーションガイドラインWG
 - サービスマップ、ガイドラインの作成等
- セキュリティオペレーション技術WG
 - セキュリティオペレーションにかかわる技術・情報交換等
- セキュリティオペレーション関連法調査WG
 - 事業者に関連する法規の調査、整理等
- セキュリティオペレーション認知向上・普及啓発
 - MSSPに関する認知向上・普及啓発活動（セミナーなど）

現状のMSSP

- 基本的に、MSSPの利用者は少ない
 - MSSPの知名度は低い
 - 「被害を受けなければ認識されない」ことが多い
 - MSSPが出来る範囲は限られている
 - MSSPは警察でも検察でもなく、捜査権はない
 - MSSPは本質的に運用（の一部）を委託されているに過ぎない
- Dual Stackへの移行といわれても
 - 顧客がいなければ動けない
 - サービスにできるだけの知見が足りない

Dual Stack対応

- Dual Stackになると何が変わるのだろうか？
 - IPv4だけでなくIPv6も見なければならなくなる
 - External RouterやFirewallレベルでの変更が発生する
 - 監視すべき項目が増える
 - NAT/LSN/Translatorが複雑に絡み合った場合のポリシー検討
 - 今までの単純な対応ができなくなる
 - ICMPの対応、ペイロード対応の変更等
 - アドレスが変わる
 - IPv6アドレス表記は（当たり前ですが）IPv4よりも長い
 - アプリケーション対応
 - 認証やCookieや…のIPv6環境問題

Dual Stackにすると？

- Dual Stackということは、IPv4とIPv6が混在する環境
 - 単純に考えれば、監視対象は2倍になる
 - 実際には、v6 $\longleftrightarrow$ v4の間の通信も発生する可能性がある
 - 46/64 Translatorの存在、Proxy/Reverse Proxyの存在
 - FirewallやIDS/IPS/WAFでは、アドレスによるFilterが難しくなる
 - アクセス制限をかけることが難しい
 - Windows7等では、Teredoを利用しているため、ServerがIPv6対応であるならば、途中でIPv4/IPv6の変換を行う
 - 特にIP Addressをもとに制御を行うFirewallで複雑な制御を考える必要がある（かもしれない）

ICMP問題

- IPv4ではICMPを単純にFilter outしてもほぼ問題なく動く
- IPv6ではICMPは非常に重要な役割を果たす
 - Path-MTU Discovery はICMPを利用している
 - IPv4のARPに相当する昨日はNeighbor Discoveryで実装されているが、これはICMPを利用している

IPv6では単純にICMPを落とすわけには行かない

Firewallを入れるなら、細かい設定が必要

アドレスが変わる

- IPv4とIPv6では、アドレスの表記が変わる
 - IPv4の場合、「ddd.ddd.ddd.ddd」と言えばよかった
 - IPv6になると、
「hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh:hhhh」と言わなければならない
 - このおかげで、電話で機器を特定し連絡することが難しくなった
 - ICMP neighbor whoisを使えば、ホスト名は特定出来そうだが、ICMPは止めている？
 - MSSPからすれば、お客様に正しくアドレスを伝えるだけでも一苦勞。さらに確認作業が入るとなおややこしくなる

アプリケーション対応

- Internetにて提供されているのはWebだけではない
 - 動的ページを用いたWeb ApplicationやSaaS等、様々なアプリケーションが提供されている
 - Firewall Policyの再構築が必要
 - Cookie等でv4アドレスをそのまま扱うアプリケーションが多い
- 認証の問題が発生する？
 - 認証情報をどう利用するのか？
 - 認証システムとユーザーが利用するサービスでv4/v6が混在した場合、認証情報は大丈夫なのか？
 - 認証システムがDual Stackで、Application側がIPv4だけだったら？
 - Cookieを含めた認証情報の整合性と独立性をどう担保するのか？

MSSPからみると

- MSSPは、ネットワークの中間で、トラフィックを見て判断し、通知する（必要に応じて遮断なども行う）代行業者
 - 対応しなければならない範囲が n^2 オーダーで広がる
 - ポリシーが複雑になると、作業ミスや対応されていないモノも出てくる
 - 現代はSecurity的には非常に危険な時代＝責任範囲も大きい

実際に出来ることは限られている

しかし、時代と社会の要請に対応するために、

相当のところまで要求される!!

Dual Stackへの移行

- 時代の要請
 - 利用者は今後、IPv6にも「対応しなければならない」
 - 事業者は今後、IPv6にも「対応しなければならない」
 - MSP/MSSPは、IPv6にも「対応しなければならない」
- Securityの要請
 - Securityの原則はおそらく変化しないだろう
 - しかし、運用の要請と作業量は2倍ではなく、場合によっては4倍にまで膨らむだろう

IPv6になると嬉しいこと

- MSSPとして、IPv6になってうれしいことはあるのか？
 - IPv4アドレスは新規割り当て空間が枯渇しかかっている
 - 現時点で空いている空間は10%を切ったという報道がある
 - IPv4が不足するとNAT/LSNを利用せざるを得ない
 - Source IP AddressがNATやLSN等で書き換えられてしまう
 - Attack Sourceを特定するためにISPと連携する必要が...(通秘問題)
 - 現在一部で利用されているAddress Based Black List方式の限界が...
 - IPv6になれば、少なくとも/64のレベルで相手を特定出来る
 - Open ProxyやTor等を使われれば結局ダメだが、それは今でも同じ

IPv6に移行してくれないと今の状況すら維持できない

可能性がある