自民党本部 IT戦略特命委員会 御中

グレーゾーン解消制度又は
企業実証特例制度適用申請の背景と主旨

株式会社スプラウト

2015.4.9

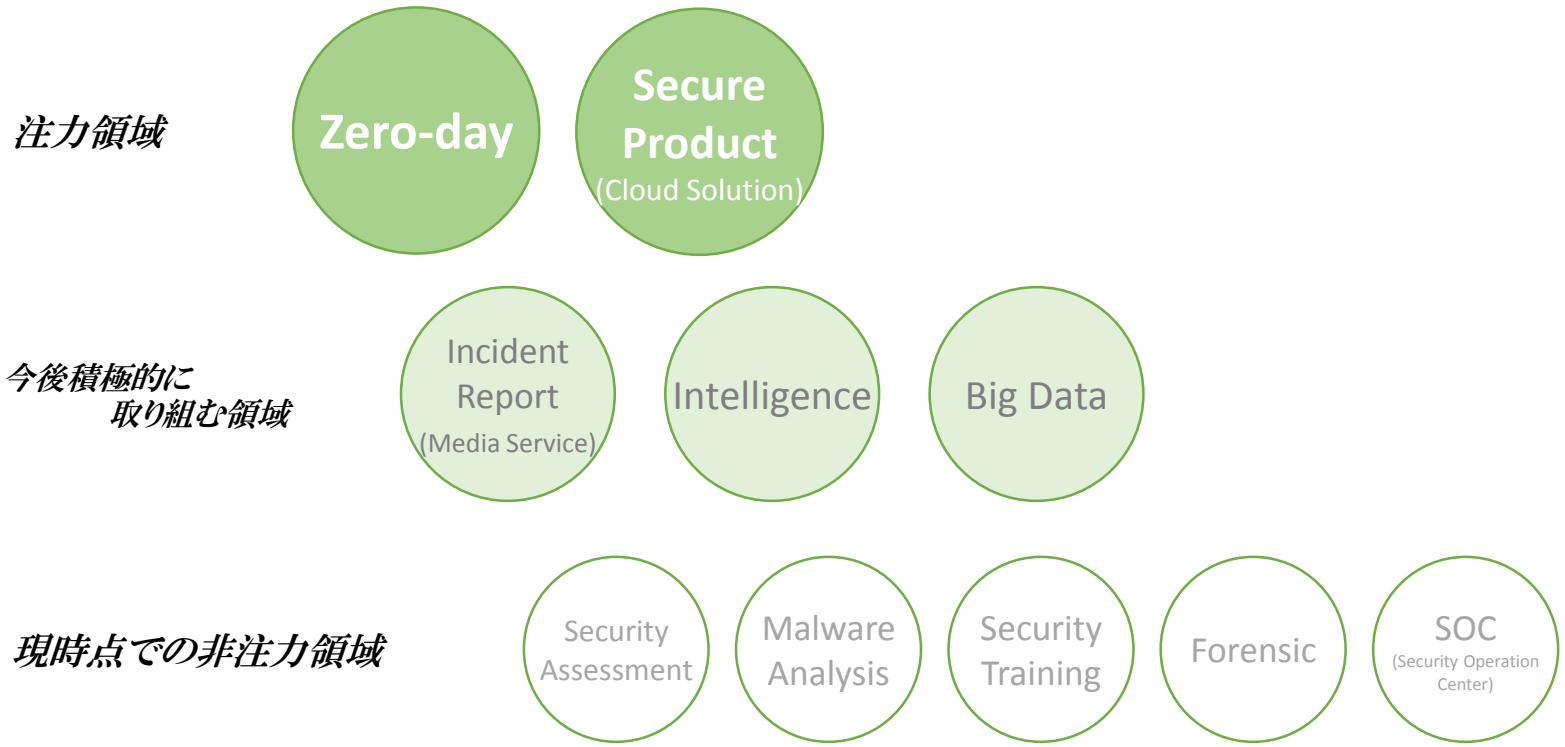
サイバーセキュリティ・ラボ sprout

株式会社スプラウト

弊社のミッション：

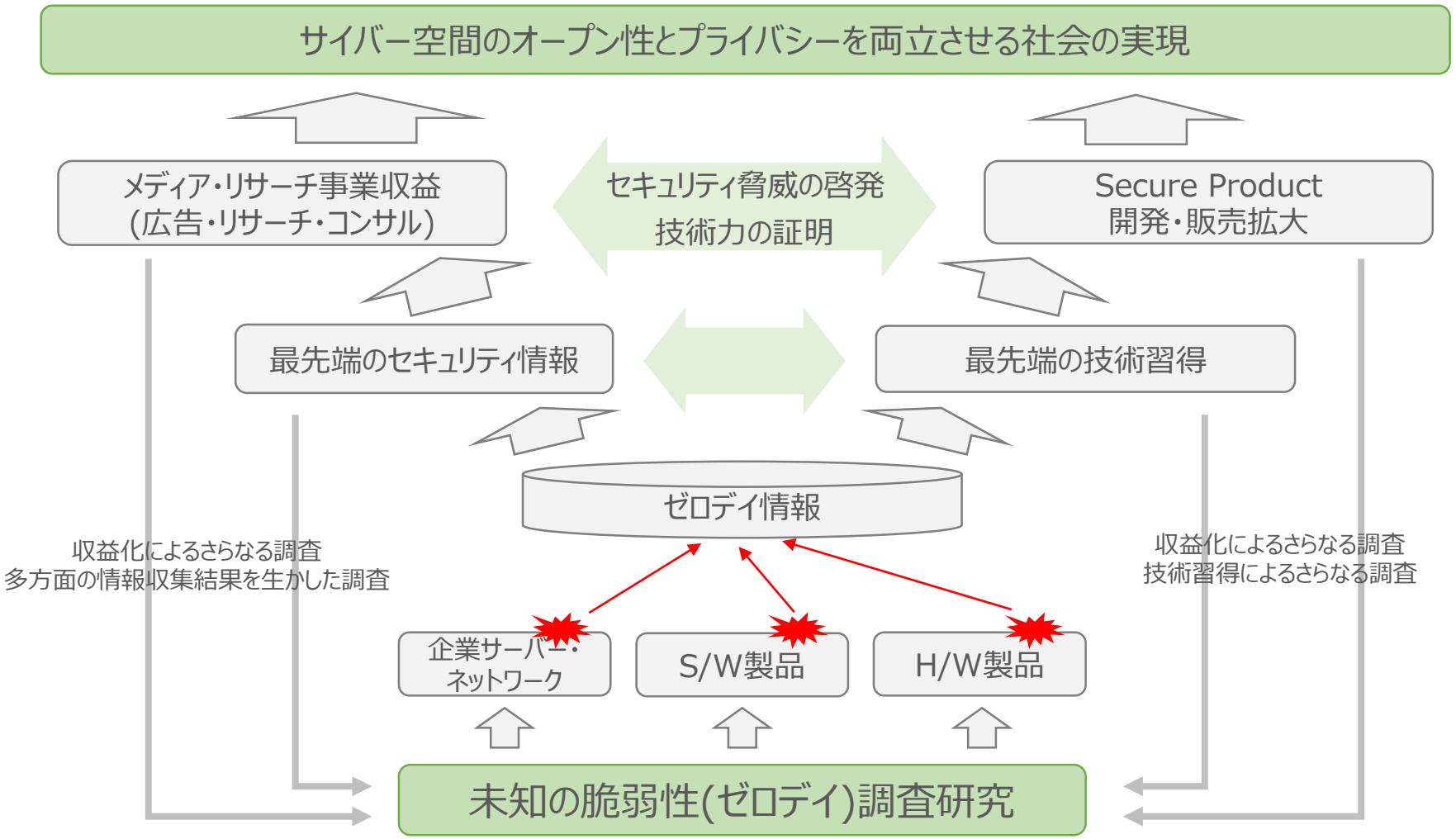
サイバー空間のオープン性とプライバシーが両立する社会を実現する

弊社はこのミッションを実現するために“圧倒的に”高い技術力を志向するセキュリティ会社です。
そのため、以下の事業領域に注力しています。



事業コンセプト

様々な脅威に対抗するためには、最先端の技術と啓発に資する情報に常にリーチしていることが重要であり、未知の脆弱性(ゼロデイ)を継続的に調査していくことが肝要と考えています。



ゼロデイ(Zeroday)＝未知の脆弱性

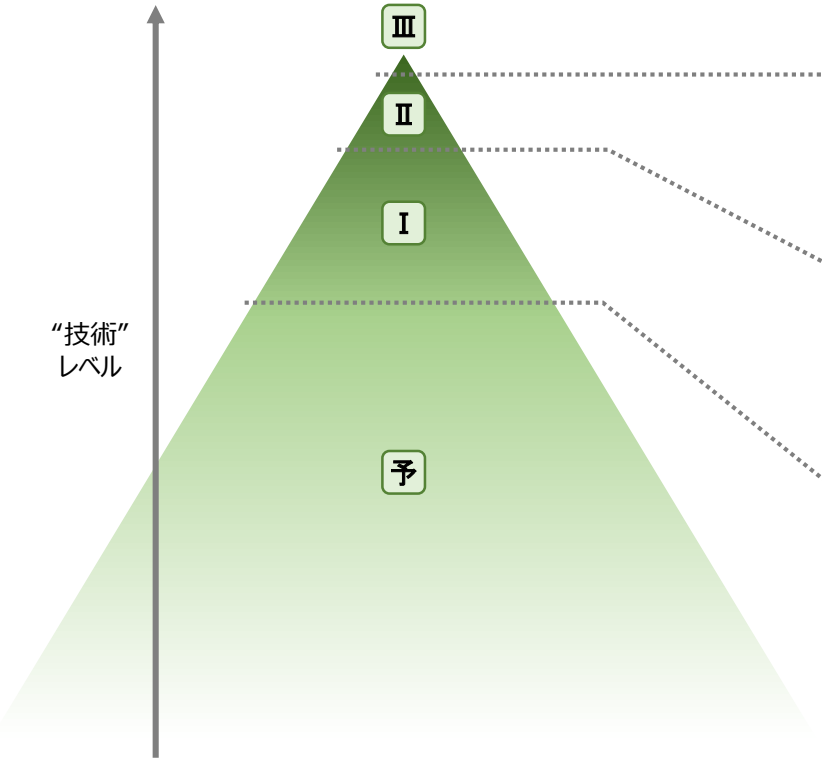
世界で5億を超えるユーザーを持つLINEに外部から通信内容、連絡先、写真等、広範囲な情報を取得できる脆弱性を発見。IPA経由で修正を依頼した。

各種報道資料（省略）

グレーゾーン解消制度又は
企業実証特例制度適用申請の背景

セキュリティエンジニア(ホワイトハッカー)とは？

“サイバーセキュリティ”に携わるエンジニア
人口イメージ



Ⅲ

IT全般に対する幅広く深い理解があり、サイバーセキュリティ領域における経験を積み重ねている。システムやアプリケーションの脆弱なポイントを見極め、新たな攻撃手法を自ら生み出すことができる

- ✓ インターネット
- ✓ ネットワーク
- ✓ ハードウェア
- ✓ ソフトウェア
- ✓ プログラミング
- ✓ 解析ツール
- ✓ セキュリティ製品
- ✓ センス、経験

高い壁が存在

Ⅱ

Webやアプリケーションのセキュリティ診断などをツールなどを用いて実施できるレベル。ITに関する知識と様々な解析ツールのノウハウ、セキュリティの一定分野に強みがある

Ⅰ

診断などを自ら実施することはできないが、サイバーセキュリティに関する用語や知識があり、問題点を指摘できる。セキュリティ製品のセールス、セキュリティコンサルティング、エバンジェリストなどの領域で活躍できる

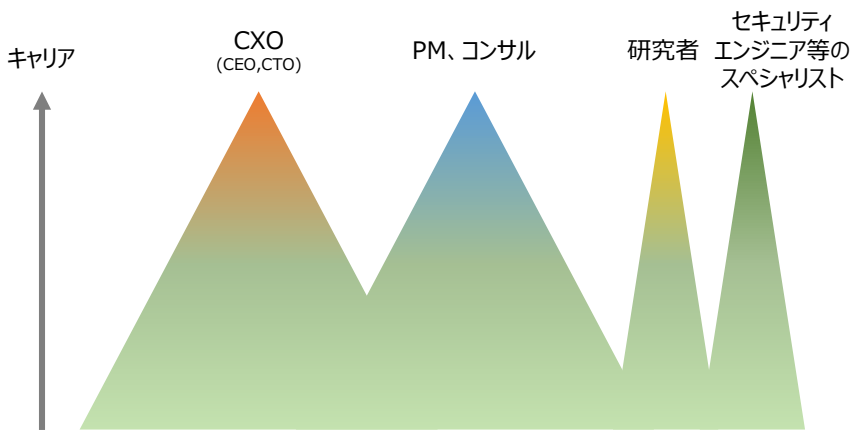
予備軍

システム開発や製品開発プロジェクトにおいてセキュリティを担当していたり、セキュリティ会社への発注・プロジェクト管理を担当しているなど、IT関係の知識や経験がありサイバーセキュリティとの接点を持っている

なぜセキュリティエンジニアが少ないのか

IT業界におけるキャリアモデルは日米で異なり、構造的にセキュリティエンジニアが育ちにくい環境となっている

日本　経営層、管理者、上流工程へと進むキャリアが一般的

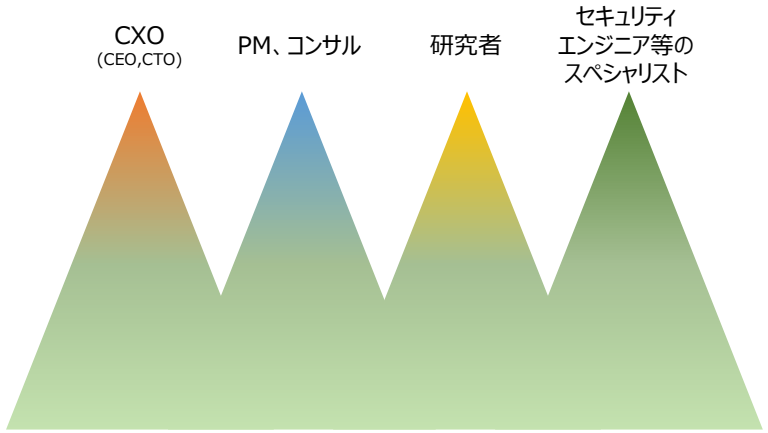


(なぜか？)

- ✓ 新卒エンジニアには文系学部出身も多くおり、何よりも“コミュニケーション能力”に重きを置かれている(技術は後からでも身に着く、という考え方)
- ✓ 管理職やコンサルなどの上流工程に重きが置かれており、報酬も高い。一方で、トップクラスの研究者でも金銭的なインセンティブが与えられていないことが散見される

⇒ セキュリティエンジニアは日本人の職人気質や品質感覚には適合しそうではあるが、このような構造上の問題で米国と比較してまだまだ少ない

研究者やスペシャリスト人材へと進むエンジニアも多くいる　米国



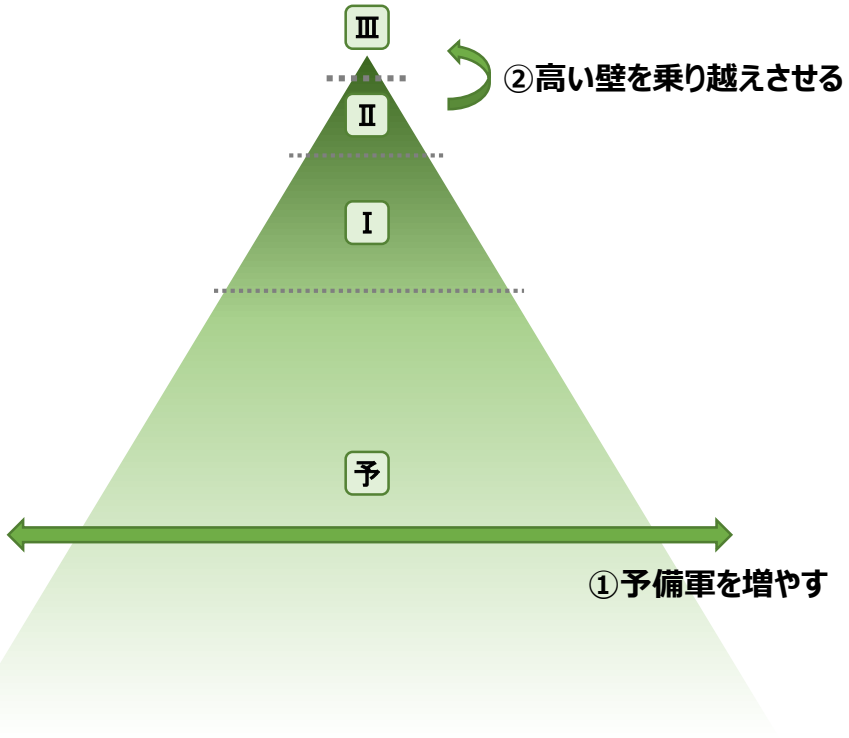
(なぜか？)

- ✓ 新卒エンジニアとはいえ工学部などの専門分野を進んだ人材が多く、研究者やスペシャリスト人材へと進むための素養が備わっている
- ✓ 管理職は役割であり、必ずしも報酬と連動していない。研究者やスペシャリスト人材に対する金銭的なインセンティブが強く働いている

⇒ さらに言えば、そもそも人口が倍であること、Geekに市民権があること、ITや技術を理解したエンジェル投資家が多いこと等が米国におけるセキュリティエンジニアの多い理由として考えられる

セキュリティエンジニアを増やすということ

現状では、いざ問題が起きた時に集まったセキュリティエンジニアが皆揃ってエバンジェリスト、という状況になりかねない。
①セキュリティエンジニアの総数を増やす、ということと並行して、②高い壁を乗り越えさせる策を打つことが重要ではないか。



※案
- 特命プロジェクト等によるインセンティブの創出
- グレーゾーン解消又は企業実証特例制度による研究目的の研究・調査推進

- セキュリティ啓発
- セキュリティ教育（セキュリティキャンプ等）
- ITセキュリティ関連の専門学部の推進　等々

グレーゾーン解消制度又は
企業実証特例制度適用申請の主旨

悪意を持った攻撃者が用いる手法例

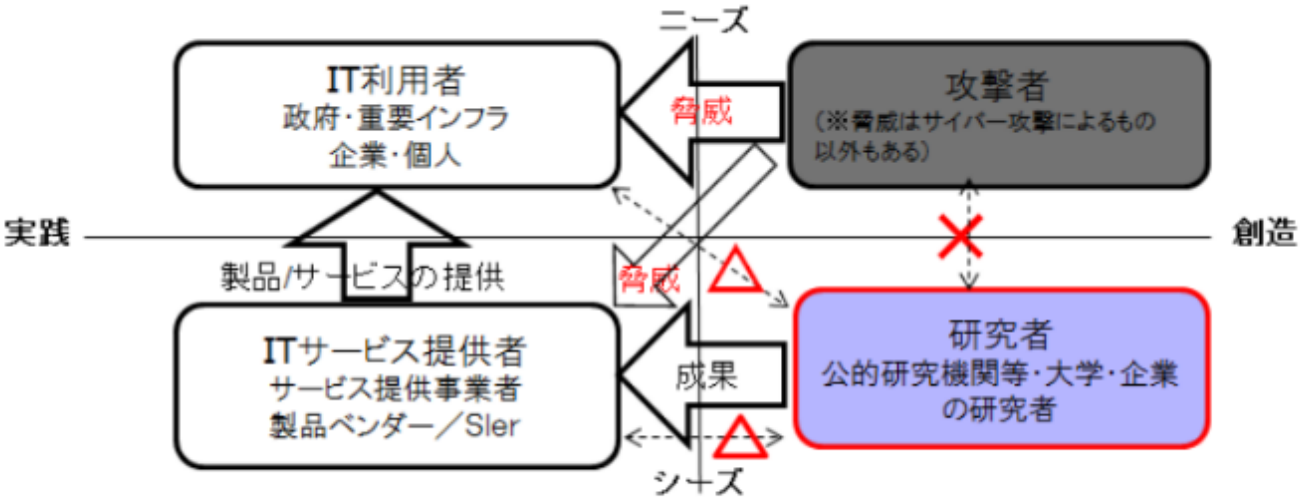
悪意を持った攻撃者が用いる手法例
パラメータ操作（テクニカル操作）
クロスサイトスクリプティング
HTTPヘッダインジェクション、ヘッダ操作
URLインジェクション
メールヘッダインジェクション
Cookie値の改ざん
SQLインジェクション
OSコマンドインジェクション
ディレクトリトラバーサル
LDAP/SSI/XPathインジェクション
パラメータ操作（ロジック操作）
識別情報の改ざん
購入情報の改ざん
固定値の改ざん
リモートファイルインクルージョン
妥当性チェックの不備
強制ブラウジング（権限昇格、認証回避）
アカウントロックアウトの欠如（ロックアウト操作）
リクエスト再送信
公開不要なファイルの表示
不正なファイルのアップロード
DoS
ポートスキャン
サービススキャン、バナー取得
ログイン処理（ブルートフォース／辞書）
サービスの脆弱性スキャン

制限付きで実施可能な手法
パラメータ操作（テクニカル操作）
クロスサイトスクリプティング
HTTPヘッダインジェクション、ヘッダ操作
URLインジェクション
メールヘッダインジェクション
Cookie値の改ざん
SQLインジェクション
OSコマンドインジェクション
ディレクトリトラバーサル
LDAP/SSI/XPathインジェクション
パラメータ操作（ロジック操作）
識別情報の改ざん
購入情報の改ざん
固定値の改ざん
リモートファイルインクルージョン
妥当性チェックの不備
強制ブラウジング（権限昇格、認証回避）
アカウントロックアウトの欠如（ロックアウト操作）
リクエスト再送信
公開不要なファイルの表示
不正なファイルのアップロード
DoS
ポートスキャン
サービススキャン、バナー取得
ログイン処理（ブルートフォース／辞書）
サービスの脆弱性スキャン

法的リスクを一切取らずに実施可能な手法
パラメータ操作（テクニカル操作）
クロスサイトスクリプティング
HTTPヘッダインジェクション、ヘッダ操作
URLインジェクション
メールヘッダインジェクション
Cookie値の改ざん
SQLインジェクション
OSコマンドインジェクション
ディレクトリトラバーサル
LDAP/SSI/XPathインジェクション
パラメータ操作（ロジック操作）
識別情報の改ざん
購入情報の改ざん
固定値の改ざん
リモートファイルインクルージョン
妥当性チェックの不備
強制ブラウジング（権限昇格、認証回避）
アカウントロックアウトの欠如（ロックアウト操作）
リクエスト再送信
公開不要なファイルの表示
不正なファイルのアップロード
DoS
ポートスキャン
~~サービススキャン~~、バナー取得
ログイン処理（ブルートフォース／辞書）
サービスの脆弱性スキャン

攻撃者視点での研究は不足

情報セキュリティ政策会議において、サイバー攻撃の検知・防御能力における課題として、攻撃者と研究者の間には「状況共有・理解がほとんど無いと思われる」ことが指摘されており、研究開発における具体的なニーズの把握が困難であるとの見解が示されている。



×：情報共有・理解がほとんどないと思われる

△：情報共有・理解が十分でないと思われる

図４： 研究者と脅威やニーズの情報流通の関係

情報セキュリティ研究開発戦略（改訂）より抜粋
http://www.nisc.go.jp/active/kihon/pdf/kenkyu2014.pdf

グレーゾーン解消制度、又は、企業実証特例制度適用の主旨

ホワイトハッカーの育成、および、研究・啓発を目的とした以下2点の活動について経産省に相談をしています。

①研究活動とリスクの早期発見を目的とした企業ネットワーク・サーバーへのペネトレーションテスト

不正アクセス禁止法の背景・目的：

・サイバー犯罪の防止・電気通信に関する秩序の維持
・他人のID・パスワードの不正流通を防止すること
・詐欺・個人情報の漏えいを早い段階で予防すること

⇒ 今後のサイバーリスクの高まりを考慮した場合、研究活動やリスクの早期発見を目的とした調査が必要ではないかと考える。現在、このような調査を行う場合、対象企業からの依頼（本人の同意）が無い場合、不正アクセス法に抵触することにより調査の範囲が限られる可能性がある状況にある。調査・研究の目的は、不正アクセス禁止法の背景・目的とも合致しており、グレーゾーン解消制度によって不正アクセス禁止法の適用はないと解釈されることを望むが、仮に適用される場合には、企業実証特例制度の適用を希望する。

②研究活動を目的としたリバースエンジニアリング

以下、情報セキュリティ研究開発戦略（改訂版）、サイバー攻撃の検知・防御能力の向上における記載。

「コンピュータウイルスやマルウェアの解析や、ITシステムやネットワーク機器の製造段階で仕掛けられた悪意のあるプログラムの解析には、リバースエンジニアリングによる解析が一つの有効な手段と考えられるが、国内企業では著作権法などに抵触しないかといった懸念が持たれており、フェアユースな情報セキュリティ目的のリバースエンジニアリングに対する適法性の解釈の明確化や周知が求められている。」

「情報セキュリティの確保という公益性に鑑み、フェアユースを前提としたリバースエンジニアリングの適法性を明確化するための措置を国として速やかに講じる。」

⇒ホワイトハッカーの育成、および、研究・啓発を目的とした調査に伴うリバースエンジニアリングについては、グレーゾーン解消制度によって著作権法及び不正競争防止法の適用がないと解釈されることを望むが、仮に適用される場合には、企業実証特例制度の適用を希望する。

End