WG4－2

セキュリティ技術者の育成について

平成17年　3月　17日

株式会社ケイ･オプティコム

ケイ・オプティコムの情報通信事業コンセプト

(地域でIPサービスに特化した総合情報通信事業展開)

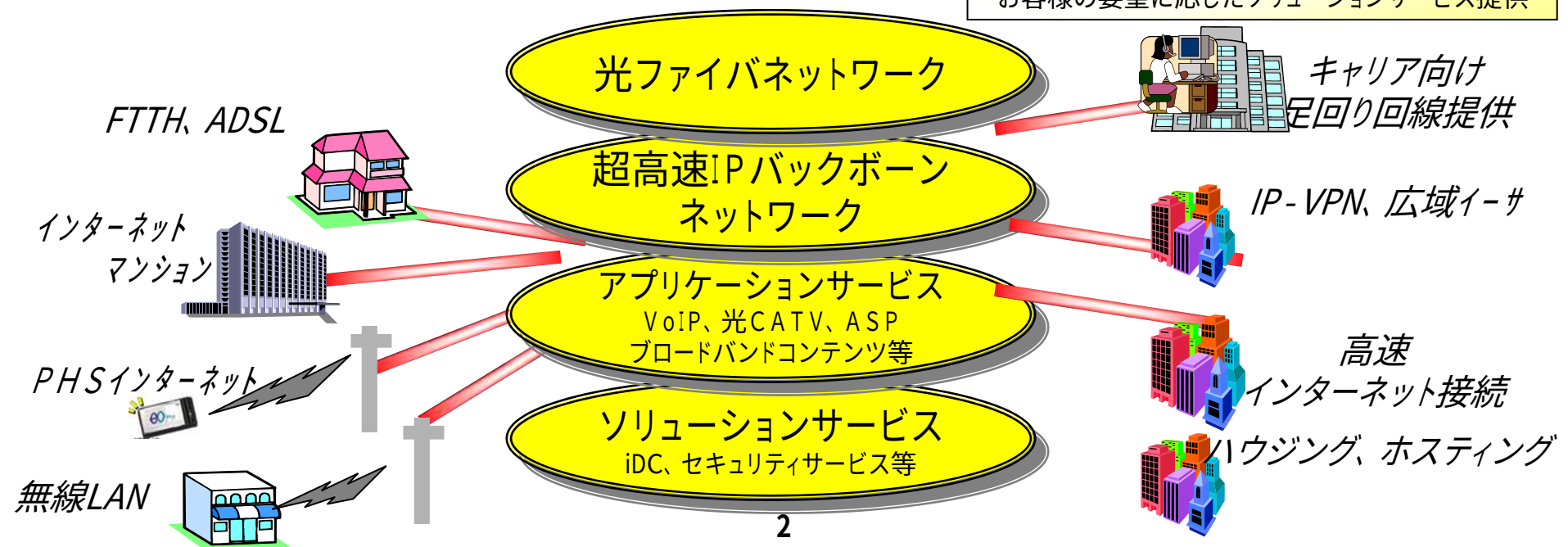
◆ 企業から一般家庭に至るまで、地域のお客さまにサービスを提供
- 超高速(100Mbps)～64kbpsまで、お客さまの利用シーンに合わせた幅広いメニュー(多様なラストアクセスメニュー)を提供
- 屋内から屋外までシームレスなサービスを提供
- アプリケーションの普及による収益力強化

個人向けサービス

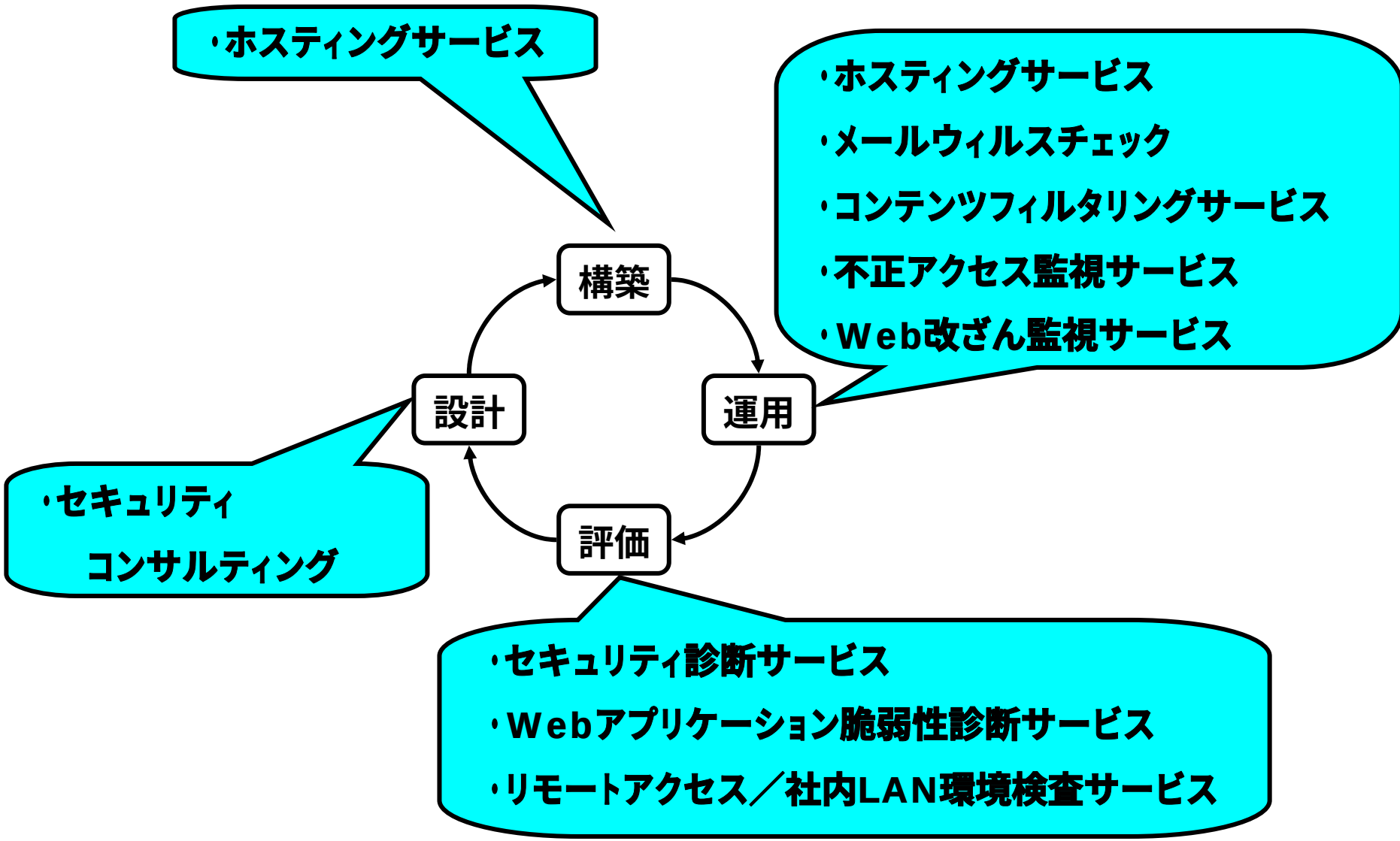
(固　定)　・FTTHを中心に、サービス展開
(ﾓﾊﾞｲﾙ)　・PHSインターネット接続ｻｰﾋﾞｽ(定額・従量制)

企業向けサービス

・インターネット接続サービスを中心に展開
・キャリア向け足回り回線の提供
　(パワードコムを主体にし、NTTｺﾑ、KDDI、JT等についても提供を行う)
・お客様の要望に応じたソリューションサービス提供



ケイ・オプティコムのセキュリティサービスの概要



ケイ・オプティコムの現状

○直営開発割合を増やすことによる基盤技術の充実

一方

○セキュリティ脅威の増大

◇物理的・人的脅威

・侵入、破壊、ソーシャルエンジニアリング、・・・

◇非物理的脅威

・ウィルス、スパム、不正アクセス、パケット盗聴、
DoS、Web改ざん・・・

・より高度なセキュリティ技術の必要性

・インシデントと対策のいたちごっこ

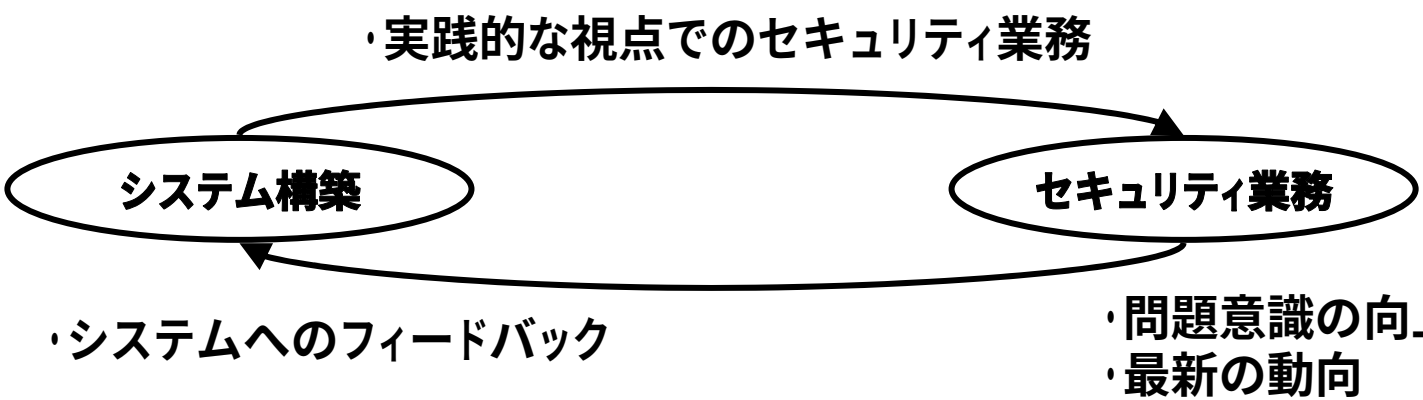
セキュリティ技術者の育成

○セキュリティ技術要員をどう育ててきたか

◆専門教育によるコアメンバーの育成

◆その後は、コアメンバーによるOJTが基本、
ホスティング提案、構築等、実践的なもの
特に系統立てた教育はしていない

◆要員配置の工夫により、技術力向上を効果的に
セキュリティ専任者でなく、システム構築、運用業務の一環として、
セキュリティ業務、セキュリティサービス提供業務を担当



セキュリティ技術者の育成

K-OPTI.COM

○それでも不足するもの

◆いくら育てても、結局は現実の後追い
　・現実とのいたちごっこ
◆セキュリティスキル（技術・技能）の評価の難しさ
◆量の確保の難しさ

○今後に向けての課題

◆生きた技術習得のために、実践に即した技術習得が必須
　（ペーパードライバーは使えない）
　←そのため、運用、開発業務に携わっていないと、
　　技術レベルの向上が難しく、技術要員の量の確保が難しい

◆入社時に、応用の利く程度の技術レベルがあれば良いのだが・・

今後に向けて（その1）

○実践技術者を速成させる提案

◆机上教育の提供だけでなく、生きた技術を習得させるための「場」の創設

・ネットワーク技術、サーバ技術及びスイッチング技術を組み合わせた「総合セキュリティ技術センター」

・その中の一つに、公的なハッカーサイトも常設し、個人の技術を各自がトライし、評価できる仕組みを作る等

今後に向けて（その2）

◆ハッキング技術を競う選手権の開催等

・技能オリンピックのようなもので個人・企業の**価値を評価**する。

◆民間の教育機関はそれなりにあるので補助金制度の対象に加える
(教育機関の一例：SANS http://sans-japan.jp/SJ/index.html)

◆セキュリティ技術者の社会的認知度の向上

・最上位資格者は会計士、弁理士、技術士並の評価を受ける制度の確立

◆セキュリティ情報のオープン化

・事例はいっぱいあるが、各社、各団体、情報をクローズ

○教育機関への期待

◆最終的には各企業のＯＪＴに委ねるとして、当該要員を業務に即組み入れることが可能な様に応用が利く程度のベーシックな知識の習得に期待。（セキュリティに関する読み書き、そろばん）速成への地ならしを期待

◆個人のモチベーションを高めるために、資格制度は有用だが、「とりっきり」の資格制度は避けるべきであるし、かつ実技の伴わないものは無駄

← セキュリティ技術は日々刻々変わるもの。
とりっきりは有り得ない

セキュリティ関連資格

K-OPTI.COM

情報セキュリティアドミニストレータ	情報システムのセキュリティに関する企画、実施、運用、分析、見直しに関する業務の知識および情報セキュリティの運用管理（マネジメント）能力が試される。 キーワード： ・基本方針・対策基準策定 ・リスクマネジメント手法 ・セキュリティシステムの設計（物理・論理セキュリティ、アクセス制御等）・実装・運用管理・事故の分析	独立行政法人 情報処理推進機構	情報セキュリティの全般的な知識に対する証明がほしい人 今後ISMS等、情報セキュリティの監督業務に携わる人	試験合格
システム監査技術者	情報システムを総合的に点検・評価し、監査結果をトップマネジメントおよび関係者に説明し、改善点を勧告する、いわゆるシステム監査業務における知識および監査によるシステムの問題点および解決策の立案能力が試される。 キーワード： ・システム監査計画策定 ・システムの現状調査・インタビュー・ドキュメントレビュー ・監査結果の記録・報告書の策定 ・改善事項の指摘	独立行政法人 情報処理推進機構	今後情報セキュリティ監査の計画を策定する人、監査を実施する人	試験合格
ISMS審査員	企業のISMSを点検・評価し、改善点を勧告する。ISMSおよびマネジメントシステムの審査能力が試される。 キーワード ・ISMS ・マネジメントシステム ・審査	日本情報処理開発協会	今後ISMSの内部監査を計画・実施する人	・情報技術分野4年経験 ・日本情報処理開発協会が認定したISMS審査員研修コースに合格していること ・3年以内に4回、20日間ISMS審査に参加した実績があること ・主任審査員2名からの推薦書
CAIS(公認情報セキュリティ監査制度)	経済産業省が施行した情報セキュリティ監査制度の監査を行う知識・経験・技術を評価する。 キーワード： ・セキュリティ監査 ・情報セキュリティ管理基準（ISMS） ・セキュリティ監査 ・成熟度モデル	日本セキュリティ監査協会	情報セキュリティ監査制度のセキュリティ監査を行う人	・協会認定研修（2日） ・協会認定トレーニング（3日） ・3年以内に4回、20日間セキュリティ審査に参加した実績があること ・面接

SANS Instituteとは
(SysAdmin、Audit、Network、Secirity)

K-OPTI.COM

○政府や企業･団体間における研究、及びそれらに所属する人々のITセキュリティ教育を目的として設立された民間組織 (本部:米国ワシントンDC)
http://sans-japan.jp/SJ/index.html

○セキュリティの専門家や情報システム監査人、システムアドミニストレータ、ネットワー ク管理者などに情報セキュリティ教育プログラムや各種セキュリティ情報･意見交換の場などを提供

○メンバーの中心は、政府機関や企業、大学の関係者などで、彼らが調査･研究した成果物である情報リソースは、ニュースダイジェストやリサーチサマリー、脆弱性情報、その他研究報告書等にまとめられ、世界各国に配信

○FBI (米国連邦捜査局) と共同で脆弱性Top20などのリストを発表

SANSにおける情報セキュリティ教育プログラム

K-OPTI.COM

○受講形態

認定インストラクターによる集合研修
e-learningによるオンライントレーニング

○主な受講者

政府機関･政府関連企業
金融機関
一般企業の情報システム部門、セキュリティ管理部門、大学

○特徴

情報セキュリティ分野に特化した教育の専門機関
最新のトピック･技術が反映
豊富な演習
業務ですぐに実践できる内容
ベンダー依存

GIAC認定について

GIAC（Global Information Assurance Certification）

○SANS Instituteが創設したセキュリティプロフェッショナルの
　技術やスキルの客観的な証明を目的とした試験

○入門レベルから高度な専門性を要求される分野まですべてカバー

○課題論文の提出によって合否を判定

○コースに応じて2年～4年で資格消滅
　　認定を維持が必要