Internet Week 2004 ： T31

組織内 SOC (セキュリティオペレーションセンター) の構築と運用の実際

株式会社ラック
JSOC事業本部 西本 逸郎
itsuro@lac.co.jp
http://www.lac.co.jp/security/

スピーカ

西本 逸郎（にしもと いつろう）

昭和33年	福岡県生まれ
昭和59年3月	熊本大学工学部土木工学科中退
昭和59年4月	情報技術開発株式会社入社
昭和61年10月	株式会社ラック入社　一貫して通信系ソフトウェアやミドルウェアの開発に従事。

その後、ドイツのシーメンスニックスドルフ社と提携し、オープンPOS（Windows POS）を世界に先駆け開発・実践投入。堅牢なシステムを如何に作って維持していくかをテーマにセキュリティ対策という観点で邁進中。

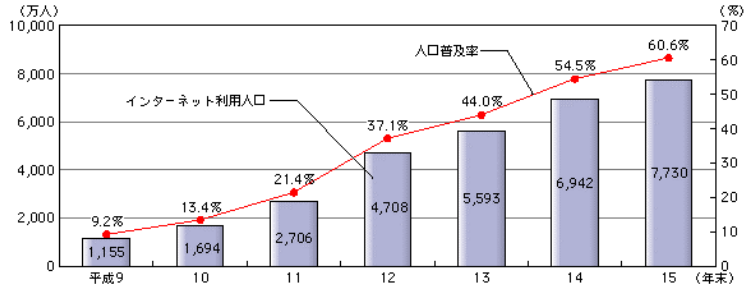
情報セキュリティ対策をテーマに展覧会などで講演会や専門雑誌への執筆を実施

株式会社ラック JSOC事業本部 取締役本部長
特定非営利活動法人 日本ネットワークセキュリティ協会 理事
熊本大学大学院自然科学研究科

目次

1．ITに関する動向

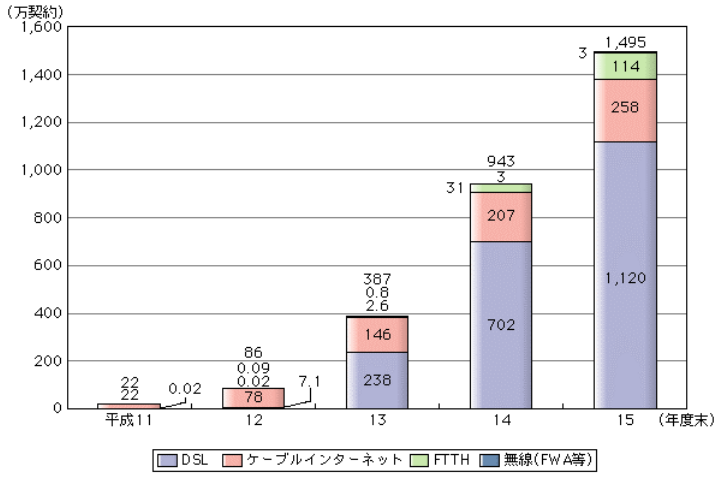
1) インターネットの国内普及状況



※1　上記のインターネット利用人口は、パソコン、携帯電話・PHS・携帯情報端末、ゲーム機・TV機器等のうち、1つ以上の機器から利用している6歳以上の者が対象
※2　平成15年末の我が国の人口普及率(60.6%)は、本調査で推計したインターネット利用人口7,730万人を、平成15年末の全人口推計値1億2,752万人（国立社会保障・人口問題研究所「我が国の将来人口推計(中位推計)」）で除したもの(全人口に対するインターネット利用人口の比率)
※3　平成9～12年末までの数値は「情報通信白書(平成12年までは通信白書)」より抜粋。平成13年末、14年末の数値は、通信利用動向調査の推計値
※4　推計においては、高齢者及び小中学生の利用増を踏まえ、対象年齢を年々拡げており、平成12年末以前の推計結果については厳密に比較できない(平成11年末までは15～69歳、平成12年末は15～79歳、平成13年末から6歳以上)

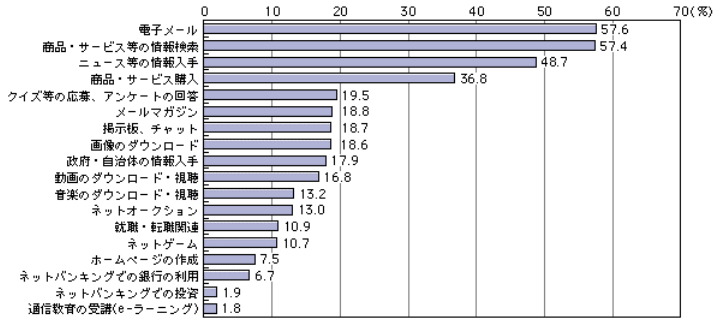
総務省発行　平成16年版 情報通信白書より
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h16/index.html

2) インターネットの国内普及状況



総務省発行　平成16年版 情報通信白書より
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h16/index.html

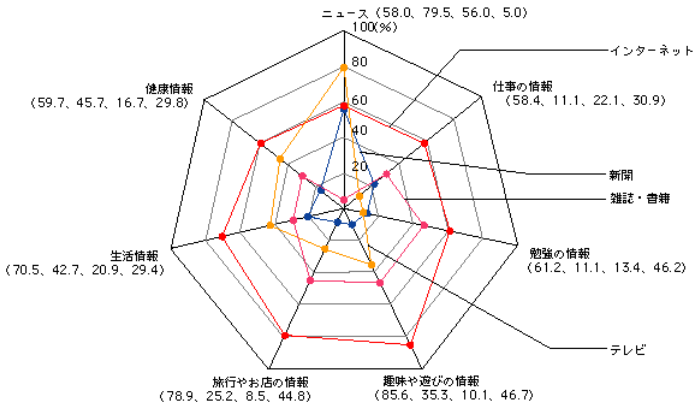
3) インターネットの国内普及状況



（出典）総務省「平成15年通信利用動向調査」

総務省発行　平成16年版 情報通信白書より
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h16/index.html

4) インターネットの国内普及状況



※　（　）内の数字は、順にインターネット、テレビ、新聞、雑誌・書籍

総務省発行　平成16年版 情報通信白書より
http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h16/index.html

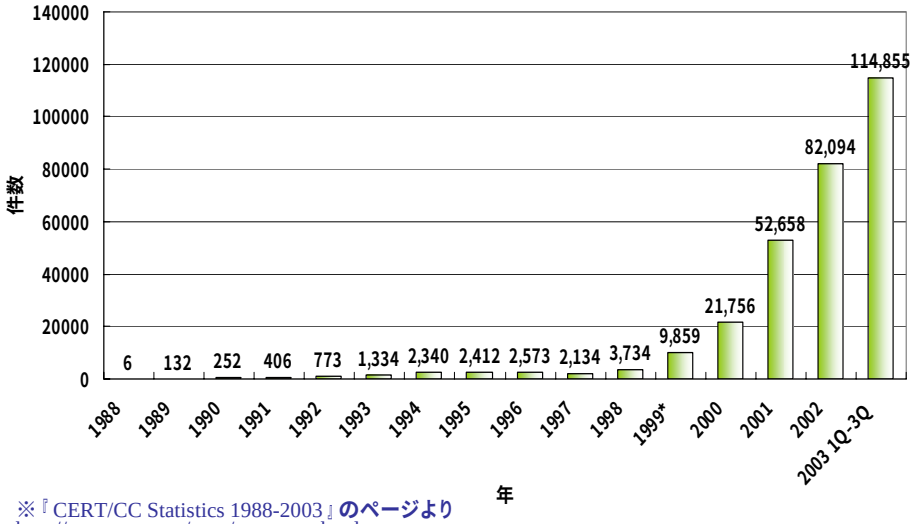
5) ITの加速度的な発展

- 情報技術(IT)の急速な発展
  - ネットワーク技術の進歩
    - 高速、大容量回線 (ADSL、CATV接続)
  - コンピュータ技術の進歩
    - 高速処理能力、大容量ハードディスク、メモリ
    - 価格の低下
  - 利用形態の変化
    - 24時間常時接続
  - 社会生活基盤のシステム化、ネットワーク化

新しいライフスタイル・コミュニケーション

急速な新社会の形成・定着化・成長

6) 情報セキュリティに関する事件の報告件数推移

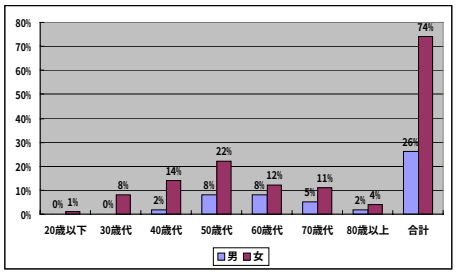


※『CERT/CC Statistics 1988-2003』のページより
http://www.cert.org/stats/cert_stats.html

7) いわゆる「おれおれ詐欺」などの内容

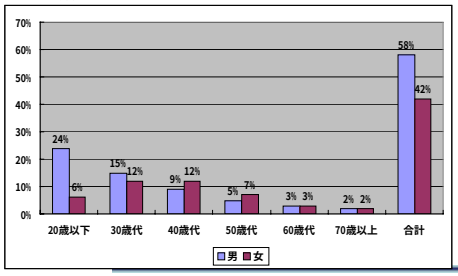
被害者の年齢 男女構成 (平成16年1月～8月)

いわゆるおれおれ詐欺

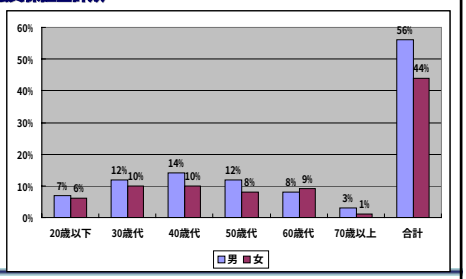


※警察庁 いわゆるオレオレ詐欺・架空請求詐欺の防犯対策を引用しグラフ化しました
http://www.npa.go.jp/sousa/souni2/oreorejoukyou16-8.pdf

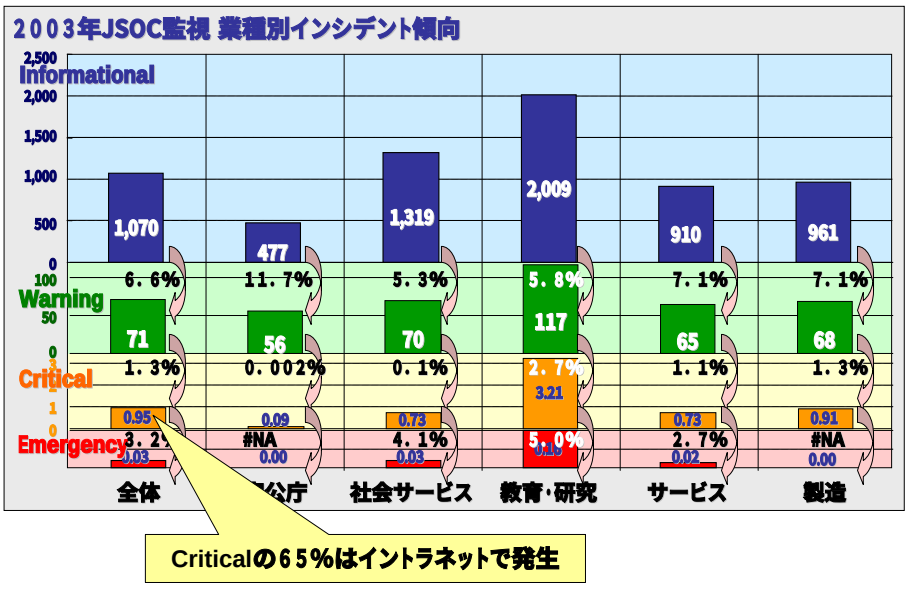
架空請求詐欺



融資保証金詐欺



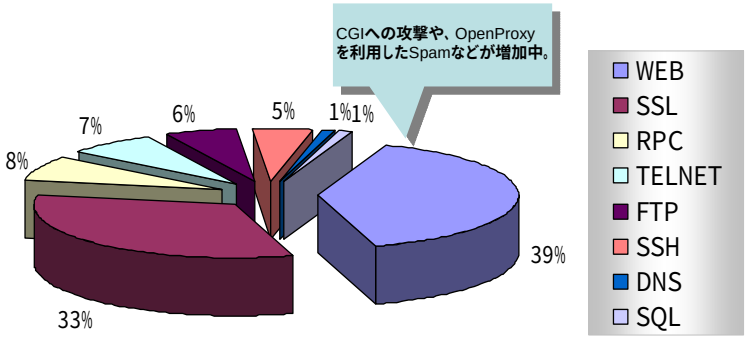
8) 昨年のインシデント統計から



Criticalの65%はイントラネットで発生

９）今年の傾向（所謂ハッカー/ポート別）

集計対象：2004 / 01 ～ 2004 / 09
（**ワームを除く**）

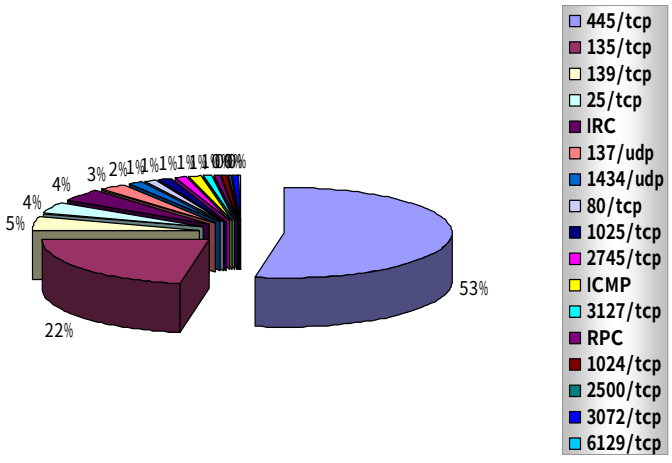


※本統計は、攻撃通信及び攻撃対象からのレスポンス通信を解析し、攻撃が成功したと判断できるインシデントの統計情報となります。

※ JSOC集計

１０）今年の傾向（ワーム系内部持ち込み/ポート別）

集計対象: 2004 / 01 ～ 2004 / 09



※ JSOC集計

１１）ポート別 推測ワーム

Port	Worm
445/tcp	Gaobot, Sasser
135/tcp	Blaster, Welchia
139/tcp	Deloder
25/tcp	Mydoom
IRC	Gaobot, Korgo
137/udp	Bugbear
1434/udp	Slammer
80/tcp	Welcha
1025/tcp	Keco
2745/tcp	Beagle
ICMP	Welchia
3127/tcp	Welchia, Mydoom
RPC	
1024/tcp	Randex
2500/tcp	
3072/tcp	
6129/tcp	Mockbot

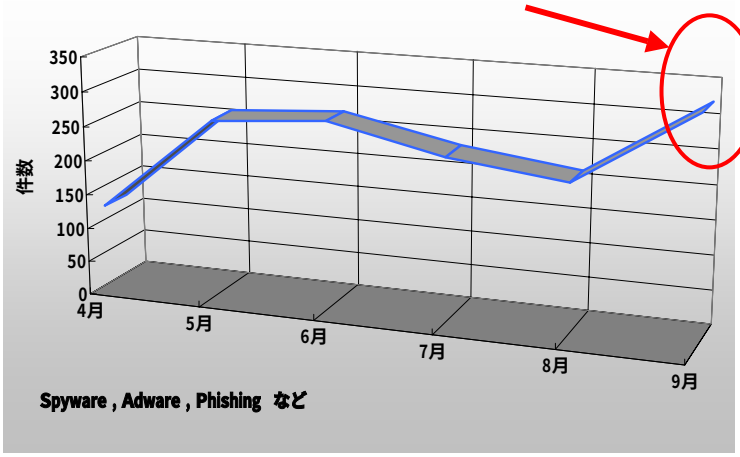
※検知デバイスはファイアウォール及びIDS

※ JSOC集計

１２）受動的攻撃の検知件数

集計対象 2004 / 04 ～ 2004 / 09

MS04-028
Microsoft GDI+ Malformed JPEG Buffer Overflow Vulnerability



※企業内から悪意のあるプログラムなどが設置されたWebサイトにアクセスした件数を集計

※ JSOC集計

13) 今年の傾向

クリティカル件数は3～4件/月・組織に増加 (昨年は1件/月・組織)

内イントラネットでの発生は90%以上（昨年は65%)

イントラネットでのインシデント件数が相対的増大した

イントラネットを監視対象とする顧客が増えてきた

2. ITリスクへのアプローチ

2. ITリスクへのアプローチ

情報システム

数多くの情報システム
自分のもの
何か文句ある？

品質？
セキュリティ？
対策はフン！

社会的責任
コンプライアンス

Eコマース ← 事業に直結

社会インフラ ← 社会的責任

対策実施は必須

2. ITリスクへのアプローチ

ITリスク

一般的なITリスクの考え方

ITを利用する上でのリスク

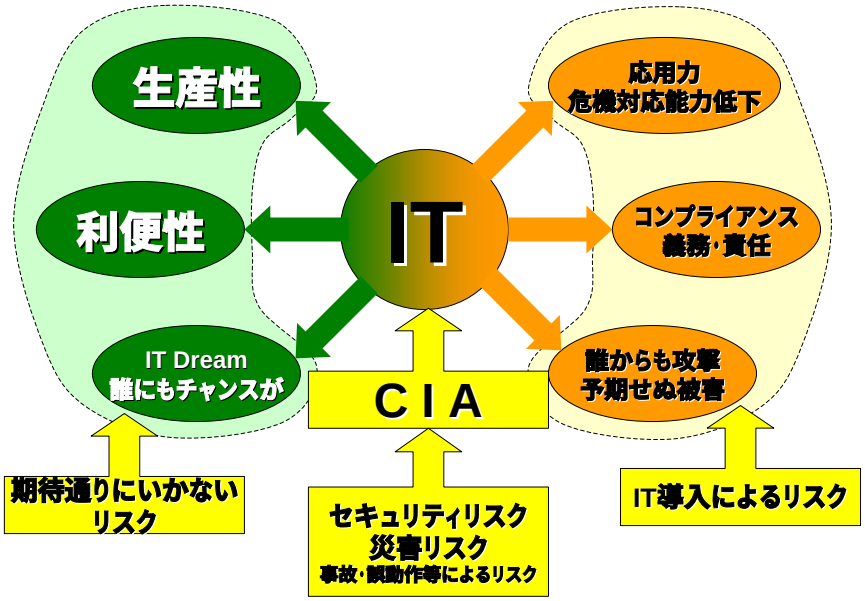
ITや情報を資産と見た場合

ITそのものが脅威となるリスク

ITや情報を負債と見た場合

今後真面目に議論すべき事項

2. ITリスクへのアプローチ

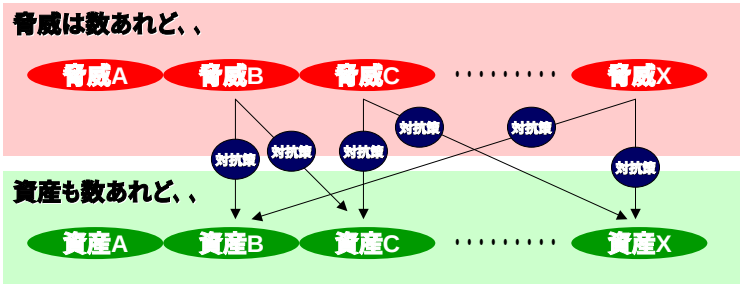


2. ITリスクへのアプローチ

■過去の動き

2. ITリスクへのアプローチ

■方針の考え方



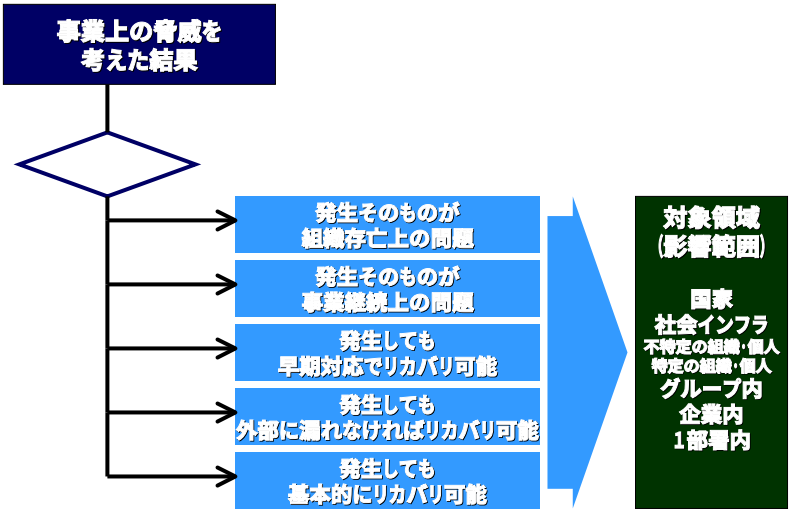
ポイントは、、

何が、どうなれば問題なのか？

対応の軸足をはっきり決めておくこと

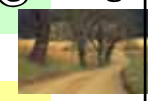
2. ITリスクへのアプローチ

■セキュリティ対策の目的



2. ITリスクへのアプローチ

自動車以上に革命的と言われるIT



整備されている基盤は、どの程度？
IT社会 VS 自動車社会

現在の状況

1. PCの高速化・高機能化	1. エンジンの高性能化
2. ブロードバンドの浸透	2. 高速道路・道路の整備
3. ネットワークとシステムの融合	3. 自動車の一般化

自動車は１００年かけて
ここまで来たが

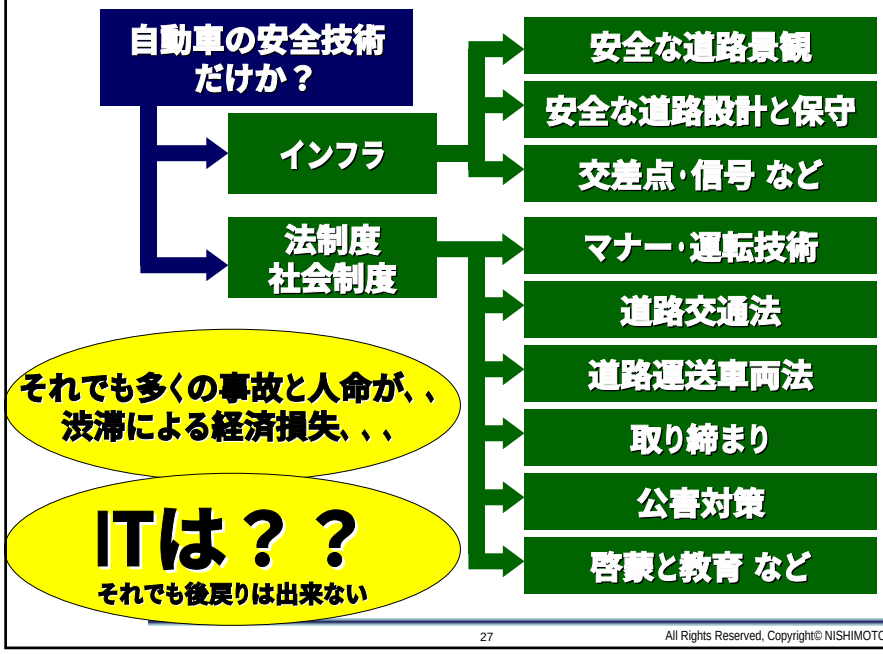
2. ITリスクへのアプローチ

いい車を
手に入れたが、、

- 運転に際して
  - ちゃんと止まりますか？
  - しっかり曲がりますか？
- いざというとき
  - 安全に
    危険回避できますか？
  - シートベルト
    エアバッグは？
  - 運転席は？
  - 脱出できますか？
  - 保険？

安全な車のためには、、
お金もかかるし、、
お客様は安いほうが、、
性能が落ちるし、、
車は自由で楽しいものだ、、

2. ITリスクへのアプローチ



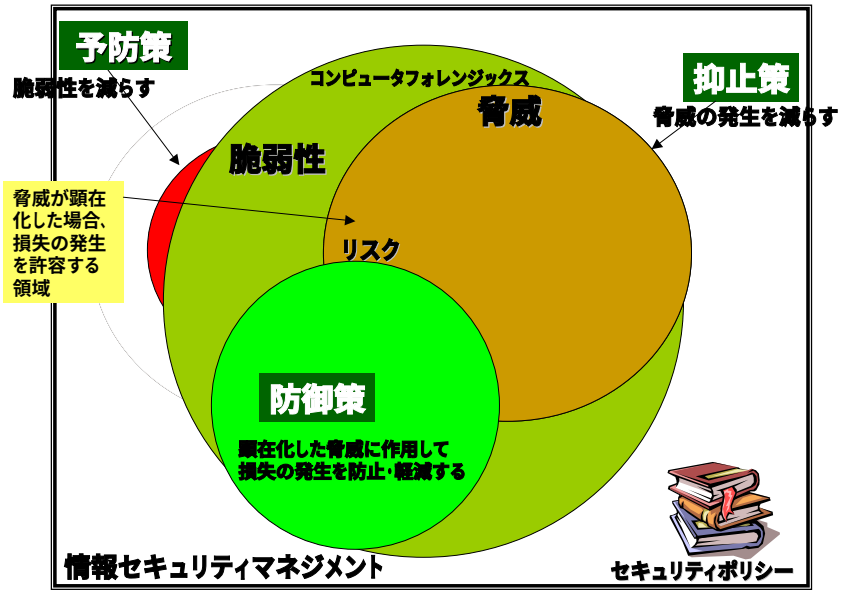
2. ITリスクへのアプローチ

もちろん、異なることも多いが、
先人の苦労は大いに参考になる。

ところで、セキュリティ対策は、、、

1. 何をどこまでやればいいの？
2. 最低、何をやればいいの？

2. ITリスクへのアプローチ



2. ITリスクへのアプローチ

一般的CIA（セキュリティ 3大基本理念）を脅かすものとして、
不正アクセスがあり、大きく分けて以下の2種類がある。

1. 無認可アクセス

通常、一般的に不正アクセスと混同され言われてことも多い
技術的な対策が概ね有効に機能する

2. 権限の乱用

一般的には社内犯罪的に言われているもので、アクセスを許可しているので技術対策が難しく、防ぐ為には抑止対策が効果的

2. ITリスクへのアプローチ

■手法のカテゴリとセキュリティ機能の関係

手法（脆弱性）		説明	抑止	予防	防御	検知	回復
無認可アクセス	実装上の弱点を利用	所属、OS、サービスアプリ ユーザアプリの セキュリティホールや設定ミス等	△	◎	○	◎	※
	運用上の弱点を利用	安易なパスワード パスワード等が漏れている ウィルス等	△	○	◎	◎	※
	技術仕様上の弱点を利用	Flood系攻撃 ICMP、UDP等成りすまし SMTP成りすまし等	×	△	○	◎	※
権限の乱用		業務上の目的以外に権限を行使 顧客情報の横流しなど	◎	×	×	◎	※

何故、完璧に守れないのか？

2. ITリスクへのアプローチ

■ コンピュータフォレンジックス

デジタルの世界に於ける証拠確保の機構と発生事象の分析であり、
目的は組織防衛にあり、基本的に以下の項目を意識して通常は考える。
事故処理時に必ず意識すべき事であり、（法的にどこまで有効かどうかを含め）事故発生前に考慮しておかなくてはならない。

① 事件発生後の調査 ⇒ 一体何が起こったのか？

② 事件発生の検知 ⇒ セキュリティ監視

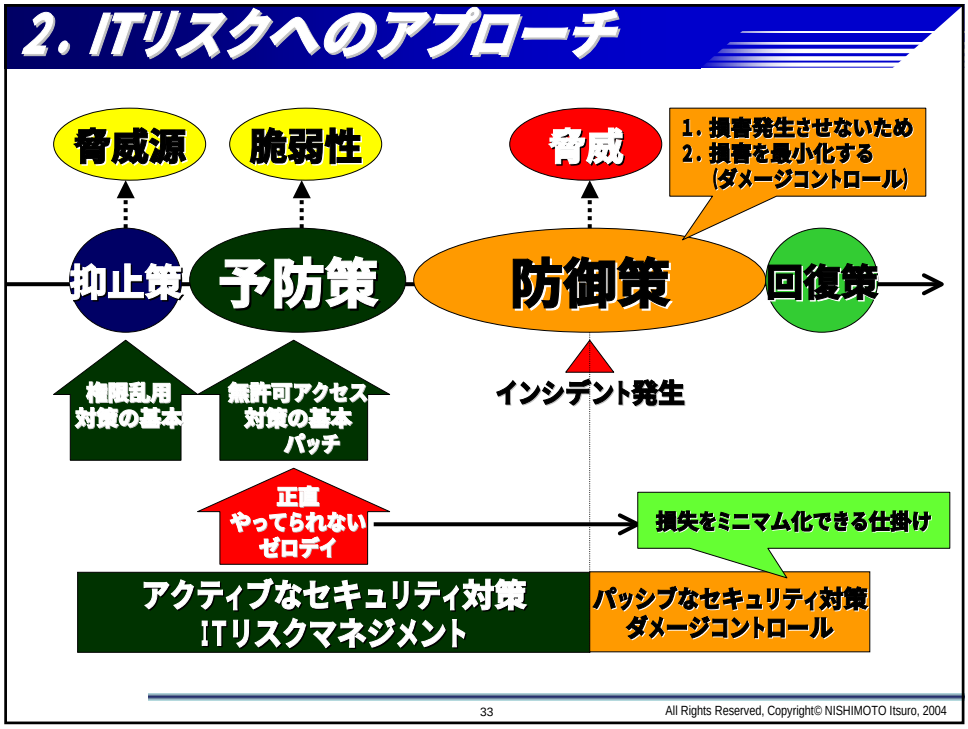
技術要素が強いツール
法的有効性

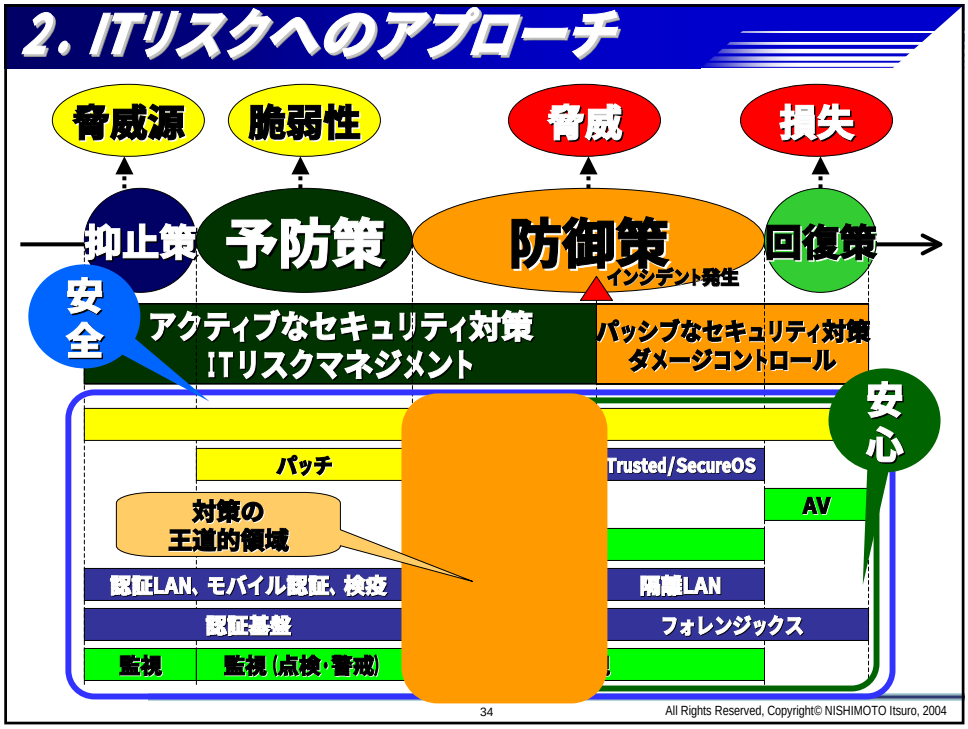
③ 事件発生時に適切管理実施を第三者へ証明
⇒ やるべきことはやっていました

経営の観点で重要課題

④ 事件未発生を第三者へ証明 ⇒そういう事件は発生しておりません。

⑤ 加害者へ証明 ⇒ あなたを訴えます


2. ITリスクへのアプローチ
脅威源
脆弱性
脅威
1. 損害発生させないため
2. 損害を最小化する
(ダメージコントロール)
抑止策
予防策
防御策
回復策
権限乱用
対策の基本
無許可アクセス
対策の基本
パッチ
インシデント発生
正直
やってられない
ゼロデイ
損失をミニマム化できる仕掛け
アクティブなセキュリティ対策
ITリスクマネジメント
パッシブなセキュリティ対策
ダメージコントロール
33
All Rights Reserved, Copyright© NISHIMOTO Itsuro, 2004


2. ITリスクへのアプローチ
脅威源
脆弱性
脅威
損失
抑止策
予防策
防御策
回復策
インシデント発生
安全
アクティブなセキュリティ対策
ITリスクマネジメント
パッシブなセキュリティ対策
ダメージコントロール
安心
パッチ
Trusted/SecureOS
AV
対策の
王道的領域
認証LAN、モバイル認証、検疫
隔離LAN
認証基盤
フォレンジックス
監視
監視（点検・警戒）
34
All Rights Reserved, Copyright© NISHIMOTO Itsuro, 2004

3．組織内SOC
(PSOC：Private Security Operation Center)

3．組織内SOC（PSOC）

1）なぜ、今、PSOCか？

① インターネットセキュリティは専門家の分野が多いが、
イントラネットでの特に情報漏えいに関わる運用は、
自分達で実施する必要があるのでは？

ポリシーありき

② セキュリティベンダーからの提案はどれもプリミティブなもので総合的なものは皆無。やっぱり自分達で計画を持って意思に則り運用すべきではないか？

リスク管理
危機管理

③ 従来のシステム運用やネットワーク運用だけではなく全体をインテリジェントに運用していく為には、セキュリティ運用も統合する必要があるのではないか？

リスク管理
危機管理

④ 自社だけではなく、グループ会社全体で、共通のポリシー制定と受け皿としての運用を用意したい。

一貫性
合理的

3．組織内SOC（PSOC）

2）目的

ケース1
社員のIT活用技術（ITリテラシ）向上させ、企業力を高めるため

ケース2
徹底した安全管理が要求されているため

ケース3
対外的にPRするため

など

3．組織内SOC（PSOC）

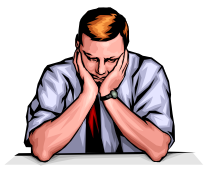
3）PSOCのパターン

① 運用方法

（1）管理と内部インタフェースは自社で他はアウトソース
（2）内部の管理・監視は自前で、専門性を要求されるところはアウトソース
（3）全て自前で

② 適用範囲

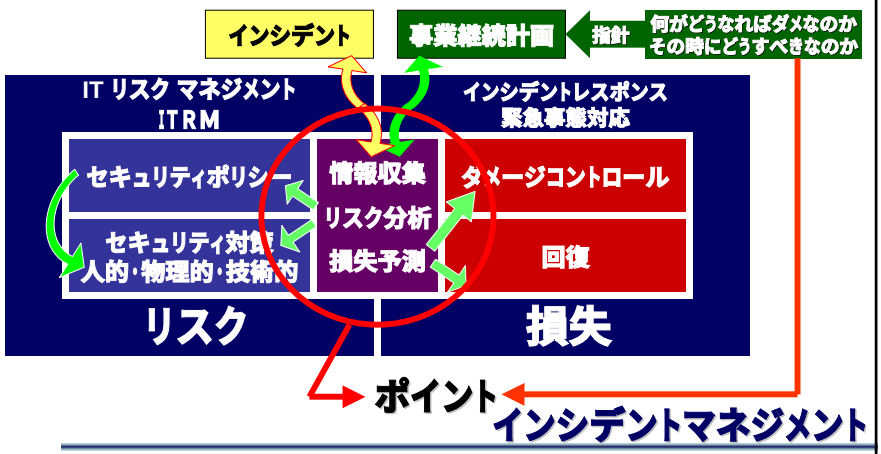
（1）会社内
（2）グループ会社で共有



3．組織内SOC（PSOC）

4）組織としてマネジメントすべき項目

① リスク　⇒ ITリスクマネジメント
② 損失　⇒ ダメージコントロール



3．組織内SOC（PSOC）

5）何をオペレーションするのか？

Private（組織内）Security Operation Center

① リスクマネジメント

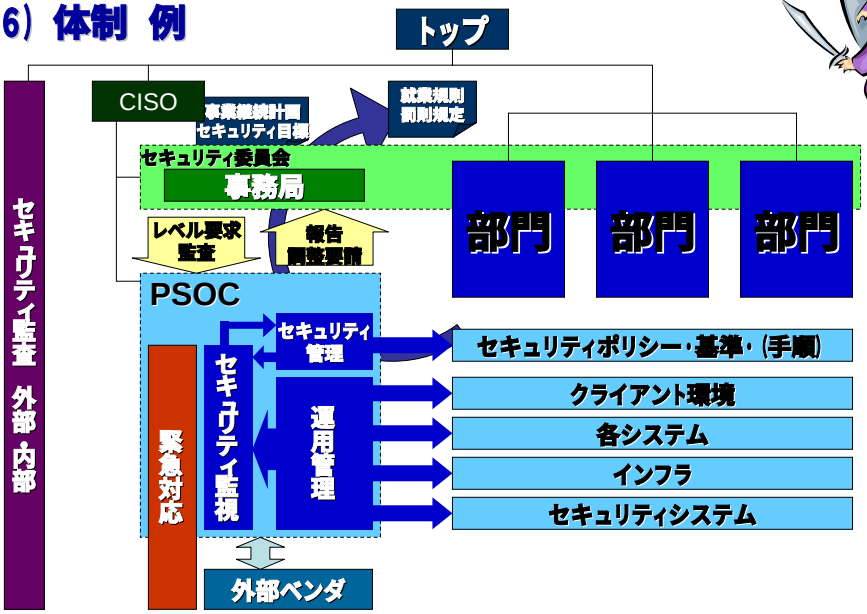
ITリスクマネジメントに関する、PDCAを運用する。

② ダメージコントロール

ITダメージが発生した場合、（それを早期に発見し）
適切に対応しダメージを最小化する。
（パッシブセキュリティの実施）

3. 組織内SOC（PSOC）

6）体制 例



4. セキュリティ管理

4. セキュリティ管理

1）PSOC取りまとめ

PSOCを代表し、セキュリティ委員会からの要求や監査を
受け入れ、また、報告等を実施する。
（場合によっては、セキュリティ委員会事務局業務も有り得る）

4. セキュリティ管理

2）インシデントマネジメント

① 事業要求、セキュリティ要求（目標）から実施施策へのブレークダウン

② 脆弱性・脅威・他での事件等の情報収集と自組織脅威分析並びに対策企画

③ セキュリティ監視からのフィードバック
無認可アクセス・セキュリティポリシー違反・不審なアクセス
脆弱性の放置など

④ 運用できない基準や手順の発見や再分析

⇒ 基準や手順の作成・改訂、ポリシー等再徹底・教育・訓練実施
必要なセキュリティ機能計画（抑止・予防・防御・検知・回復）
警戒レベル引き上げ指示
（早期発見早期対応が確実に図れるよう） など
セキュリティ委員会で実施する事も有り得る、、（機動性？ など）

4. セキュリティ管理

マネジメントすべきインシデント例

内部で発生するインシデント		外部で発生するインシデント
実際に発生している インシデントや予兆	被害や犯罪が顕在化	新たな脆弱性
	侵入され実害はまだ	新型ウイルス発生 Exploit発見
	実害の無い攻撃	攻撃トレンド
	セキュリティポリシー 違反行為	世間でのセキュリティ事件
	アノマリ行動	法律・指導・ガイドライン 社会情勢・常識 等の変化 顧客など関係機関の取り組み
	脆弱性がある	
ビジネス要求		
新システム稼動計画 新製品導入		
組織や体制変更 手順などに対する不満や意見		

※ここで言う、「インシデント」は、脅威の発生だけではなく、その予兆を含みます。

4. セキュリティ管理

3) セキュリティポリシー・基準・手順 管理

① セキュリティポリシーはセキュリティ委員会ということもある
ただしポリシーの運用管理はPSOCで実施するのが現実的

② 手順は各部門で策定するのが基本だが、運用管理（申請などのワークフロー＆記録）は一括管理が合理的

③ ポリシーの運用管理 ⇒ 後述、運用管理で実施も有り得る
- (1) ポリシー文書改訂と周知徹底と記録
- (2) ポリシー運用の合理化と記録
  通常ワークフローと連動（周知徹底や承認・申請）
- (3) 教育と訓練と記録

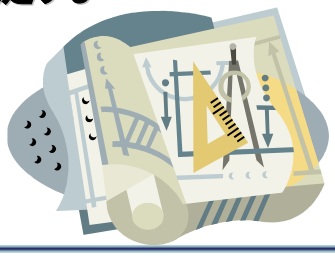
4. セキュリティ管理

4）セキュリティ機能実装管理

① 中期セキュリティ機能実装計画を策定
⇒ インシデントマネジメントを基本に、リスク予測を行い、
計画（2～3年）を策定する

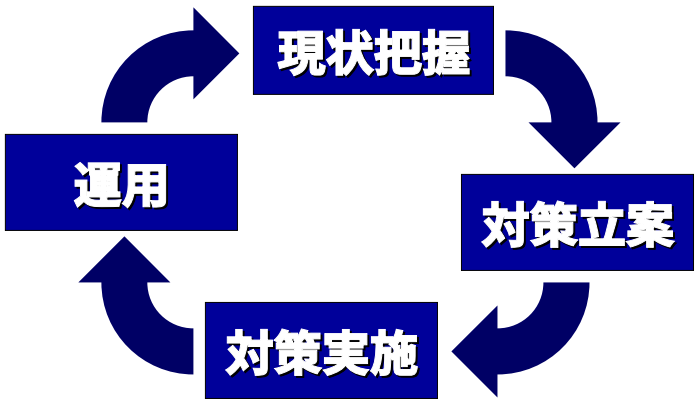
② 中期計画に従い、現状の対策技術、製品、アウトソース
サービス等の予測・調査・評価を行い、適切な実装方法を
短期実装計画（1年以内）としてを策定する

③ 短期計画の実施管理を実施
⇒ 期待効果・予算・運用コスト



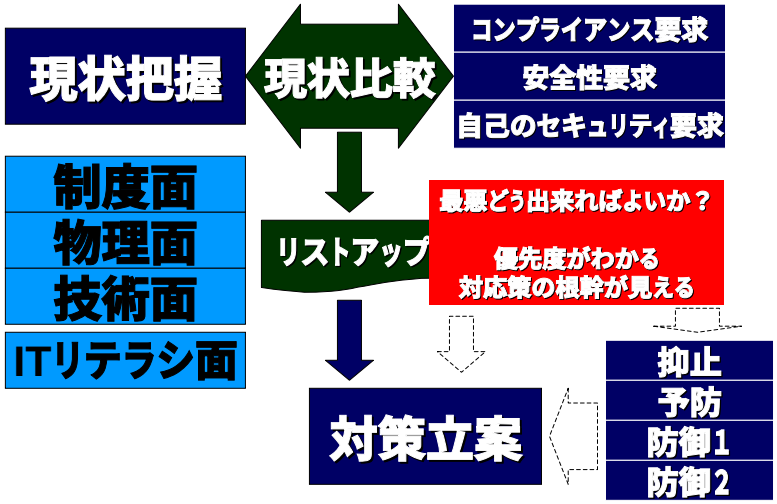
4. セキュリティ管理

4）セキュリティ機能実装管理



4. セキュリティ管理

4) セキュリティ機能実装管理

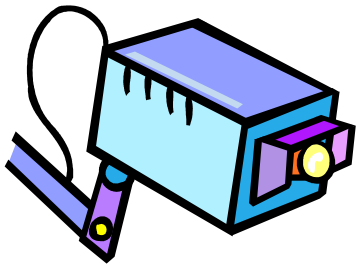


4. セキュリティ管理

4) セキュリティ機能実装管理

対策			自動	人手	制度
抑止	打てる手は 監視・ポリシー・罰則			◎	◎
予防	脆弱性管理 など 注意・警戒 など		◎	◎	◎
防御1	被害を出さない		◎	○	
防御2	防御2-1	緩和策	◎		
	防御2-2	インシデント レスポンス		◎	○

5. 運用管理（セキュリティ）

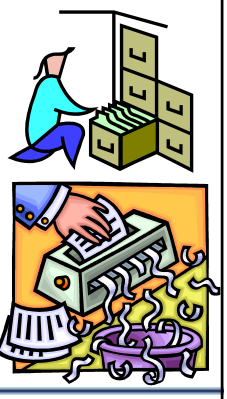


5. 運用管理（セキュリティ）

1）コンプライアンス運用管理

① ポリシー等関係ドキュメント公開と閲覧・確認
② 申請などワークフロー
③ 対策・警戒などの指示と確認

⇒ 運用記録も重要な観点

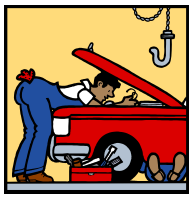


5. 運用管理（セキュリティ）

2）セキュリティデバイス運用管理

⇒ ファイアウォール、ウイルス対策、検疫LAN
　自動パッチ更新システム、監視システム など

① 稼動監視
② 定義ファイル更新や最適化
③ デバイスそのもののパッチ管理 など



5. 運用管理（セキュリティ）

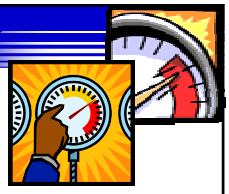
3）セキュリティヘルプデスク

① ユーザ支援
　(1) ウイルス対策支援
　(2) セキュリティ設定支援 など

② システム管理者支援
　(1) サーバ系へのパッチ適用や回避策等
　(2) 警戒方法など

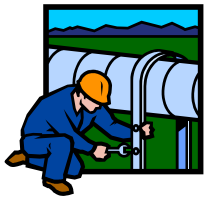
③ 緊急対応受付（恐らく兼務で対応）

5. 運用管理（セキュリティ）



4）システム健康管理

① 各システム、ネットワークの稼動状況
PING（IPレイヤ）、サービスポート（サービスAPレイヤ）
他AP、DB など



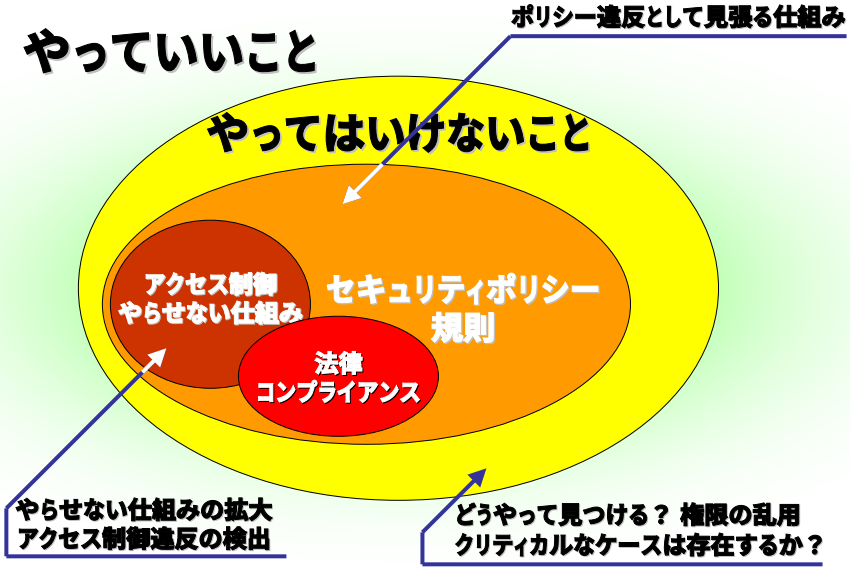
② 各システム・クライアントPCの資産管理
（設定内容、導入AP など）

⇒既存のＮＯＣやシステム運用とオーバラップ
特に可用性（Availability）の観点で、異常や変則状態を
鳥瞰できる仕組み
（1）障害・事故？
（2）セキュリティインシデント？
但し、内部セキュリティ監視と同居はよく考慮が必要

6. セキュリティ監視

6. セキュリティ監視

1) セキュリティ監視のカテゴライズ

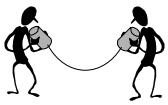


6. セキュリティ監視

2) 発生事象から見たカテゴライズ 例



① 無認可アクセス
- (1) ハッカー攻撃
- (2) ワーム (Active Attack、Remote Exploit)
- (3) コンピュータウイルス・トロイの木馬などの不正プログラム (Passive Attack、Contents Exploit)
- (4) アクセス違反




② セキュリティポリシー違反
- (1) アカウント管理違反
- (2) 権限外の行動
- (3) 危険な行動 など

③ 機器障害・災害

④ 運用事故・設定ミス

⑤ 不審アクセス
- (1) アノマリ行動
- (2) 上記①～④の分類が出来ないアクセス (調査が必要)

6. セキュリティ監視

3) 脅威から見たカテゴライズ 例

① 業務停止に関わる項目
どのシステム・セグメントで発生？

② 情報漏えいに関わる項目
どの情報？

③ モラル崩壊に関わる項目
どのレベル？（悪質度合い）

上記でアラートをくくる方法もあり

6. セキュリティ監視

4) 重要度の判定 例

発生している
時刻、システム、ネットワーク、場所 など

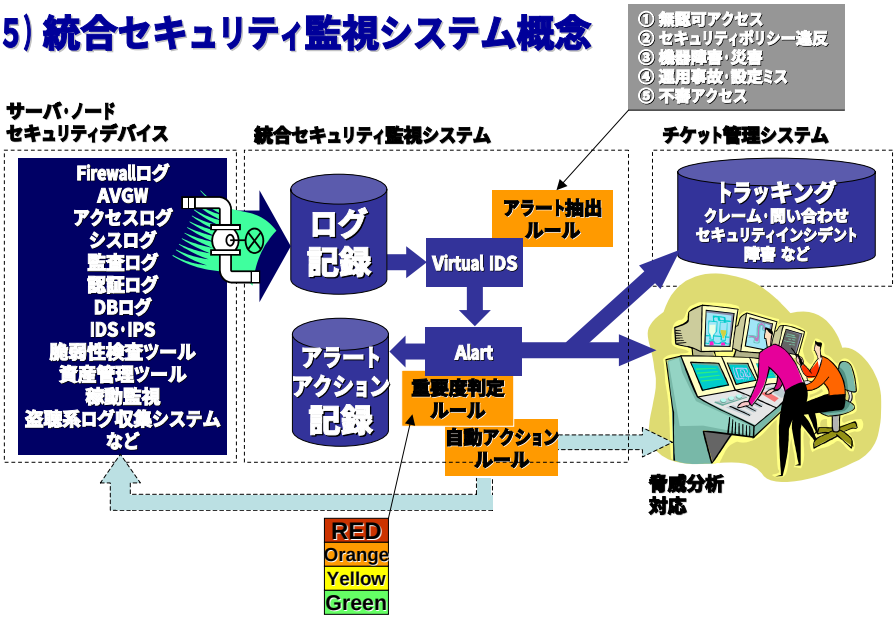
発生事象	対象脅威			重要度			
	業務停止	情報漏えい	モラル崩壊	RED	Orange	Yellow	Green
① 無認可アクセス	◎	◎	◎				
② セキュリティポリシー違反	△	◎	◎				
③ 機器障害・災害	◎	△	△				
④ 運用事故・設定ミス	◎	○	○				
⑤ 不審アクセス	上記、①～④のどれに該当するか？ 事実を現場へ確認 判断は自動化できるか？ など エスカレーションが必要						

※
RED 即時対応
Orange 要警戒・至急対応
Yellow 注意・週次/月次
Green 情報・統計

各組織での考え方

6. セキュリティ監視

5) 統合セキュリティ監視システム概念



6. セキュリティ監視

6) セキュリティポリシー監視 例

① アカウント管理
　アカウントの使いまわし
　脆弱なパスワード使用 、、、

② 使用プログラム
　禁止プログラムの使用 、、、

③ データアクセス など
　禁止されている方法でのDBアクセス 、、、

6. セキュリティ監視

7) 手法のカテゴリ

手法 (脆弱性)		説明
無認可アクセス	実装上の弱点を利用	所謂、OS、サービスアプリ ユーザアプリの セキュリティホールや設定ミス等
	運用上の弱点を利用	安易なパスワード パスワード等が漏れている ウィルス等
	技術仕様上の弱点を利用	Flood系攻撃 ICMP、UDP等成りすまし SMTP成りすまし等
権限の乱用		業務上の目的以外に権限を行使 顧客情報の横流しなど

6. セキュリティ監視

8) 手法のカテゴリと検知方法

実装上の弱点を利用		
センサー	攻撃検知	侵入検知
ネットワーク型 IDS	攻撃パターン、異常パケット サービス、脆弱性 バナースキャン等	不審なコネクション
ホスト型 IDS		ファイル改竄、権限の行使、 ログイン、バックドア等
ホストログ	不審なログ	作業手順突合せ
ファイアウォール	異常パケット	不審なDrop

6. セキュリティ監視

8) 手法のカテゴリと検知方法

運用上の弱点を利用		
センサー	攻撃検知	侵入検知
ネットワーク型 IDS	ブルートフォース	不審なコネクション
ホスト型 IDS	ログインエラー	ファイル改竄、権限の行使、ログイン、バックドア等
ホストログ	ログインエラー	作業手順突合せ
ファイアウォール	短時間での大量Accept	不審なDrop

6. セキュリティ監視

8) 手法のカテゴリと検知方法

運用上の弱点を利用		
センサー	攻撃検知	侵入検知
認証ログ		ID/パスワードの貸し借り ID/パスワードの漏洩 離席PCの無断使用 など
アクセスログ		
入退室ログ		

6. セキュリティ監視

8) 手法のカテゴリと検知方法

技術仕様上の弱点を利用		
センサー	攻撃検知	侵入検知
ネットワーク型 IDS	Flood系、Smarf系等	
ホスト型 IDS		※別途サービス稼動監視 応答監視
ホストログ	大量のエラーメール受信	
ファイアウォール	大量のDrop等	

6. セキュリティ監視

8) 手法のカテゴリと検知方法

権限を乱用		
センサー	攻撃検知	侵入検知
ネットワーク型 IDS		
ホスト型 IDS	権限の行使のアノマリ検知	
ホストログ	アクセスログから アノマリ検知	
ファイアウォール		

6. セキュリティ監視

8) 手法のカテゴリと検知方法

権限を乱用		
センサー	攻撃検知	侵入検知
DBアクセスログ	不審なアクセス 不審な時刻 不審な場所から 不審な量 不審なパターン などなど	
ファイルアクセスログ		
認証ログ		
ファイアウォール		

6. 1. セキュリティ監視の目的

1) 目的と実施範囲

【目的】
1. コンプライアンス
2. 自己資源の防衛
3. 社会的責任

【実施範囲】
1. インターネットサイド
2. DMZセグメント
3. イントラネット

6．1．セキュリティ監視の目的

2) 目的 コンプライアンスレベル

【ポイント】

1．ウィルス･ワームの外部への発信
- ⇒ ウィルスゲートウェイ監視
- ⇒ ファイアウォールでウィルス感染活動を監視

2．外部への攻撃
- ⇒ IDSで外向け攻撃を監視
- ⇒ メールサーバエラーログ監視

3．個人情報漏洩若しくは漏洩の危険性
- ⇒ IDSでP2P通信、トンネリングツールの使用監視
- ⇒ IDSでDBなどのトラップデータの監視
- ⇒ 内部でのアノマリ監視
- ⇒ 認証ログ･入退室ログ･アクセスログ相関監視

対応の優先度は 組織存続、事業継続

6．1．セキュリティ監視の目的

3) 目的 自己資源の防衛レベル

【ポイント】

1．イントラへのウィルス･ワームの侵入や内部での攻撃
- ⇒ IDSでイントラネットを監視
- ⇒ 内部のファイアウォール監視

2．公開サーバや重要サーバへの侵入行為
- ⇒ 作業手順チェック･ホスト型IDS
- ⇒ コマースサイトに対するDoS検出と緩和

3．外部への情報漏洩
- ⇒ IDSでP2P通信、トンネリングツールの使用監視
- ⇒ IDSでDBなどのトラップデータの監視
- ⇒ 内部でのアノマリ監視
- ⇒ 認証ログ･入退室ログ･アクセスログ相関監視
- ⇒ メールサーバ監査

対応の優先度は事業継続、採算性、合理性

6．1．セキュリティ監視6目的

4) 目的 社会的責任レベル

【ポイント】
1．基幹サービスへのDoS攻撃
⇒ ファイアウォールでの検知
⇒ ファイアウォールでのアクセスアノマリ検知
⇒ 基幹サービスの稼動監視（レスポンスアノマリ）など
2．セキュリティ監視へのDoS攻撃
⇒ 監視システム稼動監視（ログ量アノマリ）など
3．内部侵入の監視
⇒ トラステッドOSレベルでのアクセス制御違反監視

対応の優先度は社会責任度合い

6．2．セキュリティ監視の肝

5) セキュリティ監視といえばIDS？

セキュリティ監視といえば、ネットワーク型IDS監視を想像するが？

既存のIDSだけでどこまでのことが出来るのだろうか？

基本的にネットワーク型IDSは誤報は免れない

となると、アプローチは、、、

1．誤報の可能性のあるシグネチャーでは検知しないようにする
⇒ えっ！なに？

2．対象ネットワークの特性に合わせチューニング（ポリシー設計）を行い監視する
⇒ シグネチャー（検知パターン）の頻繁な更新、構成の変更　大丈夫？

3．IDSで検知したイベントを都度誤報かどうか確認しながら監視する
⇒ 大変そう、出来るの？

6．2．セキュリティ監視の肝

6）作戦

1．意味のあるネットワーク分断（セグメンテーション）

2．セグメントの特性に合わせたログ設定
　特にファイアウォールやサーバのログ設定

6．2．セキュリティ監視の肝

7）ファイアウォールの原点

1．ネットワークセグメント（部屋）を意味のあるものに分けること
　何故分ける必要があるのか？
　→ セグメンテーション

2．アクセス制御を行うこと
　基本的なアクセス制御は？
　→ 基本ネットワークポリシー

3．記録をつけること
　なぜ？目的は？
　→ ログ管理

6．2．セキュリティ監視の肝

8) セグメンテーション

人
情報カテゴリ
機能（サービス）
適用できる規則
物理的条件
・・・・

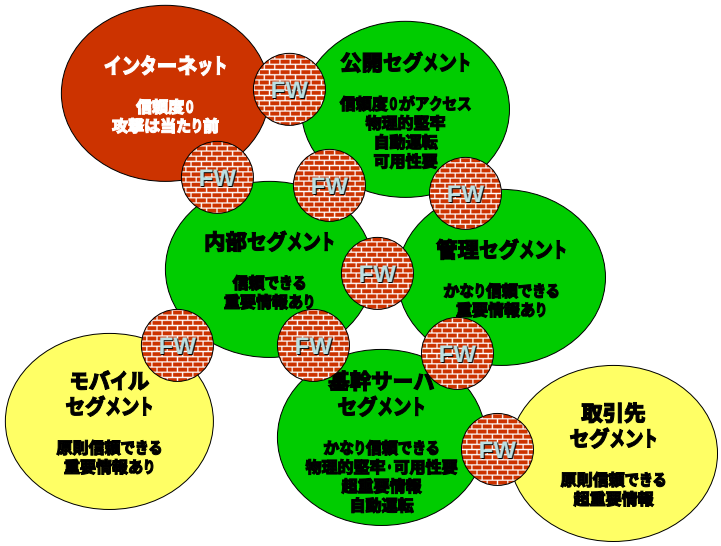
お客様、社員、経営者、管理者、攻撃者、、、
関係者以外機密情報、社外秘情報、顧客情報、、、
一般向け、特定のお客様向け、社員向け、、、
就業規則・社内ポリシーが適用、評価基準、、、
物理的セキュリティ状態

鑑みてネットワークを分断する

CIA（機密性、完全性、可用性）

6．2．セキュリティ監視の肝

9) セグメンテーション 例



6．2．セキュリティ監視の肝

10) アクセス制御 基本ネットワークポリシー

セグメント間でやり取りすることで想定される脅威（リスク分析）から、基本となるネットワークポリシー（セグメント間アクセス制御基準）を決める。

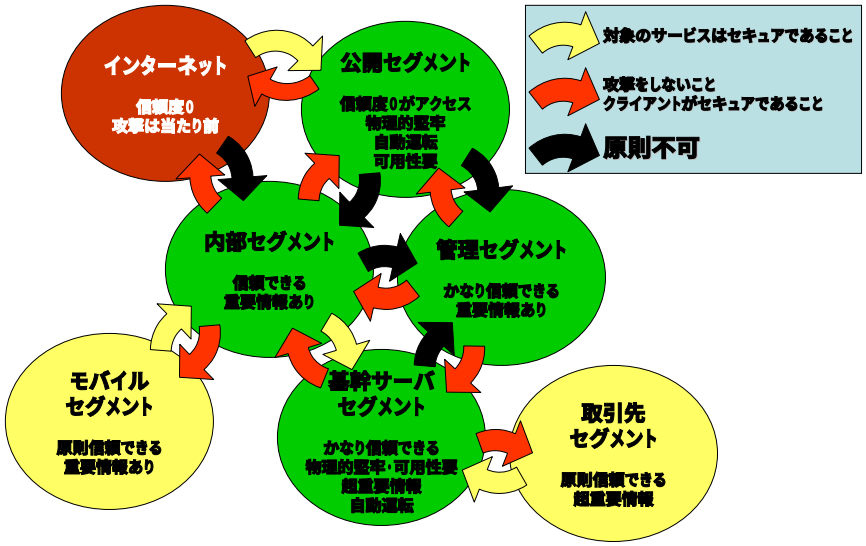
例：

1．信頼度が低いセグメントへサービスを提供する場合は、脆弱性を排除しておく必要がある
2．セグメント外のサービスを利用する場合は攻撃しないようにする
3．セグメント外のサービスを利用する場合は受動攻撃を受けないようにクライアントをセキュアにしておく

→ 重要度に応じて、登録、変更手続きを決めると良い。

6．2．セキュリティ監視の肝

11) 基本ネットワークポリシー 例



6．2．セキュリティ監視の肝

12) ログ管理

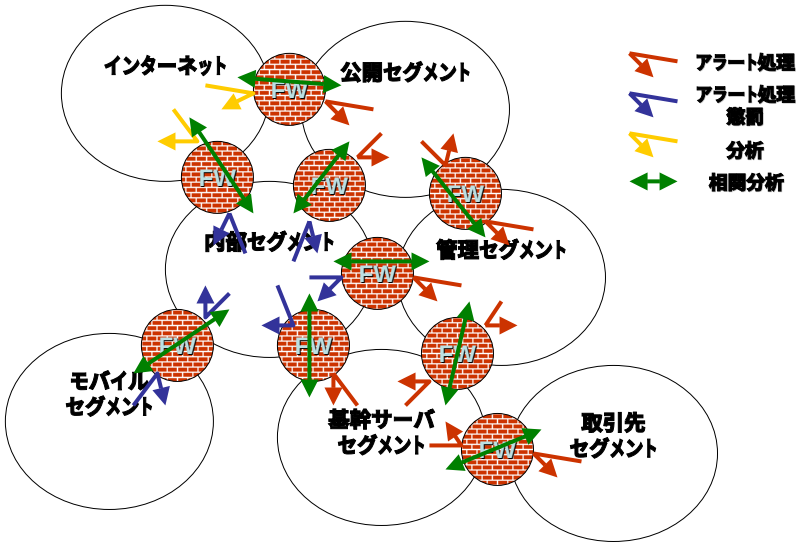
ログの種類
セグメンテーションし基本ポリシーを決めているのでログを分類できるようになる。

【例】
1．自動運転しているセグメントで何故Dropが起きるのか？
→ アラート インシデントレスポンス
2．規則を守るはずのところで何故Dropが起きるのか？
→ アラート インシデントレスポンス・懲罰
3．攻撃があるのが当たり前のところでは、Dropは当然発生
→データマイニングや相関分析が必要
4．許可ログは、基本的にはストックして置けばよい。何か有ったときの調査用。
→上記ログと併せて、分析

当然のことながら、ログは改竄されない仕組みが必要。

6．2．セキュリティ監視の肝

13) ログ管理 例



6．2．セキュリティ監視の肝

ファイアウォールの基本的な機能は

⇨ **防御**

アクセス制御を行うことで脆弱性を持ったサービスが有っても防御する

セグメンテーションを行い基本ポリシーを持ちまた運用することで

⇨ **検知**

⇨ **回復**

アラート処理が出来るようになり、検知し回復を図り、

⇨ **予防**

統合分析を行い傾向を分析することで、予防を図り、

⇨ **抑止**

規則違反を発見し、またログを管理していることで、抑止を図る。

※ 各々の対策には仕様上限界がある。
　運用場所によっては、これで十分である場合もあるが、他のセキュリティ機器を併用していくのが望ましい。

6．3．トレンドの押さえ方

1) ネットワークの性格により異なる

(1) インターネット

基本はFirewallで止まるので、公開しているサービスを重点に
攻撃がくるのは当たり前

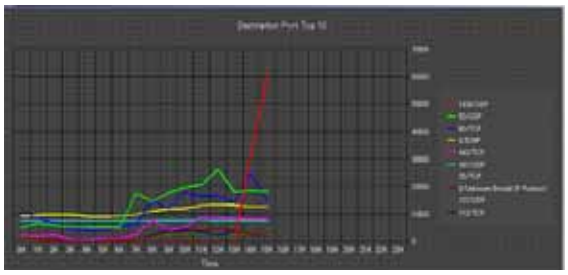
(2) イントラネット

やはり、ウイルス･ワーム対策
はやりのP2Pやゲーム系は、仕込まれバックドアなどで利用されやすい
アクティブバックドア（能動的バックドア）も要注意
権限の乱用

6．3．トレンドの押さえ方

2) インターネット

IDSでトレンドを押さえるのは、結構大変
案外ファイアウォールのInboundでのDropのトレンドは有効
※ 以下は、Destination Portでのトレンド例



※ 株式会社ラック 資料

6．3．トレンドの押さえ方

3) イントラネット

①ウイルス・ワームの感染活動

A.所謂バッファオーバランのような手法を使用
　攻撃対象生成ロジック　TCP or UDP
B.パスワードクラック
　攻撃対象生成ロジック Windows 他
C.被感染者の権限で
　ファイル共有
　　攻撃対象生成ロジック Windows P2P他
　メール送信 など
　　攻撃対象生成ロジック MTA有無

6．3．トレンドの押さえ方

3) イントラネット

TCPベースでランダムに攻撃を行う場合は、
大半のパケットはインターネットに出て行こうとする。
(Default Gateway)

(1) ファイアウォールでドロップする場合
原則、Synパケットのみ
IDS⇒ 同一ソースIPからランダムのIPに大量のSyn
ファイアウォール ⇒ 同一ソースIPからの大量のDrop

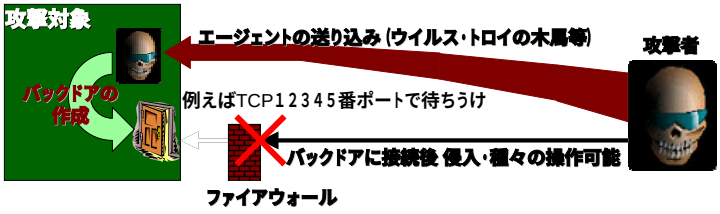
(2) ファイアウォールでドロップしない場合
IDS⇒ パターン検知 検知できないものは？
ファイアウォール ⇒ 同一ソースから大量のAccept

6．3．トレンドの押さえ方

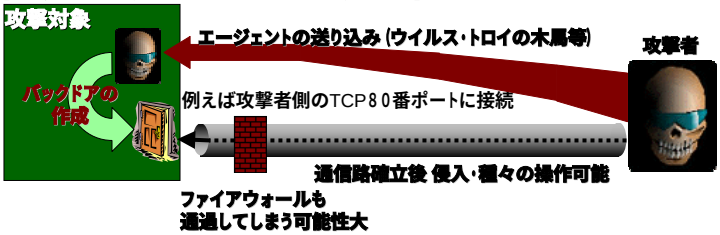
3) イントラネット

■ アクティブバックドア？リバースバックドア？

【通常のバックドア：パッシブバックドア】



【能動的なバックドア：アクティブバックドア】

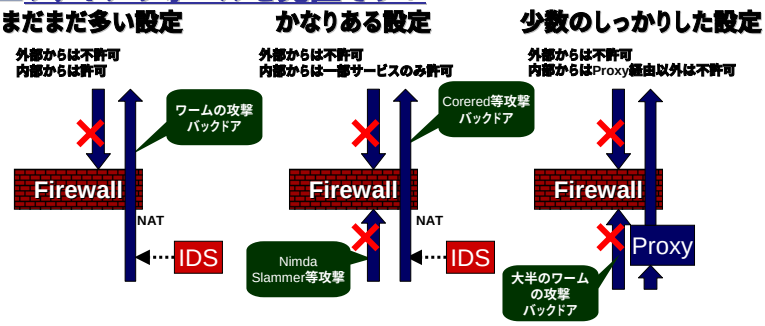


ファイアウォールも
通過してしまう可能性大

6．3．トレンドの押さえ方

3) イントラネット

■ファイアウォールを見直そう！



1．内部に侵入したワームを検知できない。外部へ感染攻撃。
2．アクティブバックドアを検知できない。防御できない。
3．P2Pツールやチャットツールを利用したウイルス、トロイの木馬の増加

6．3．トレンドの押さえ方

3) イントラネット

②バックドア
- A.パッシブ（受動的）バックドア
  - 基本はファイアウォールでDrop
- B.アクティブ（能動的）バックドア
  - ファイアウォール⇒Drop
  - IDS ⇒ 検知可能か？
- C.P2Pなど
  - ファイアウォール⇒Drop
  - IDS ⇒ 検知可能か？

⇒ 期待されるのは、IDSのアノマリ検知
アノマリって何だ？

6．3．トレンドの押さえ方

3) イントラネット

③権限の乱用

原則、防止は難しい
如何に、抑止するか？
　⇒ 個人認証とアクセス制御＋操作ログ
如何に、予兆を検知するか？
　基本はアノマリ検出と記録

6．3．トレンドの押さえ方

3) イントラネット（アノマリ検知）

①RFCアノマリ（一部のIDSでは可能）
RFC定義の違反を検知
⇒ そもそもRFCに準拠していないソフトウェア（メーラ・ブラウザ）
⇒ 大半の攻撃はRFCに準拠

②通信帯域アノマリ（一部のIDSでは可能）
急激な通信量の変化を検知
⇒ Slammer、Codered等

③通信先アノマリ（一部のIDSでは可能）
通常はどこの機器のどんなサービスにどの程度アクセス？

④情報アクセスアノマリ（これからの課題）
通常はどの機器のどんなファイルにどの程度アクセス？
通常はどのデータベースのどんな情報にどの程度アクセス？

6．4．センサー（IDS、FW）の特性と使い方

1）ファイアウォール

①NIC毎にログ制御可能？

②Acceptはとれる？

③ステートフルインスペクションレベルのログは？

④アプリケーションゲートウェイ

⑤ログ管理

6．4．センサー（IDS、FW）の特性と使い方

1）ファイアウォール

①内部のワーム･エージェントなどの活動

②内部で使用している、P2Pなどのツール

③内部での攻撃行動

④外部からのスキャンやプローブ

⑤パスワードクラックなどのブルートフォース

⑥外部で発生しているトレンドの把握

これらの検知の可能性
→ 検知には分析が必要

6．4．センサー（IDS、FW）の特性と使い方

2）IDS

①攻撃検知？

②侵入検知？

③侵入分析？

⑤アノマリ検知

6．4．センサー（IDS、FW）の特性と使い方

2）IDS

①ネットワークベース IDS

（1）基本はシグネチャ検知（パターン一致）
（2）RFC、通信帯域変化アノマリ
（3）既存環境・パフォーマンスへの影響小
（4）フォールスポジティブ・ネガティブ問題・暗号化通信

→ 基本は分析が必要
→ プロトコルが固定、通信元・先が限定或いはセキュリティポリシーが適用できるところは、精度を上げることは可能で有効

6．4．センサー（IDS、FW）の特性と使い方

2）IDS

②ホストベースIDS

(1) ネットワークベースIDSのインライン的な機能
　通信のシグネチャ検知（パターン一致）
　RFC、通信帯域変化アノマリ？？
(2) ファイルの改ざん検出
(3) ログオン･ログオフ、権限行使など 所謂監査ログでのエラー検出
(4) システムコールのトラップによる、プロテクション機能＋エラー検出
　アプリケーションのセキュア化
(3) フォールスポジティブ問題、パフォーマンス低下
(4) 対象ホストに組み入れる
　動作不安定、IDSのトラブルがシステムに影響大、運用管理

→ アプリケーションのセキュア化は期待できる？
　クリティカルなサーバへは適用考慮

6．4．センサー（IDS、FW）の特性と使い方

2）IDS

③手順違反IDS

(1) 運用手順違反を検知
　ログオン･ログオフ、権限行使など 所謂監査ログ
　基本的にエラーログではなく、正常のログが対象
　EX.
　　suの前には、XXを実施する、、等
(2) 一種のアノマリの検出？
良い道具はまだこれから

6．4．センサー（IDS、FW）の特性と使い方

2）IDS

④IPS

(1) ネットワーク型と同様の盗聴タイプとインライン、ブリッジ型を
選択できるものが多い
(2) 検知より、防御を意識している
フォールスポジティブ
最初は、盗聴タイプ、、防御機能は確認しつつ、、？
運用管理？
(3) インラインタイプがどこまで受け入れられるか？

6．4．センサー（IDS、FW）の特性と使い方

2）IDS

⑤インテリジェント化

(1) 対象機器のサービス内容・脆弱性情報と組み合わせ
脆弱性：所謂、OS、アプリの脆弱性 → パッチ
設定の脆弱性 → 再設定
パスワード、サンプル、機能など、、
どこまで、正確に把握できるか？

(2) InHouseツールの有効活用
基本データベースシステム
各種IDS、FW、サーバログ、監査ログ等統合
バーチャルIDS・エンタープライズIDS・サイトIDS的概念も有効
(多少) インテリジェントプロテクションルール
分析支援
運用管理

6．4．センサー（IDS、FW）の特性と使い方

3）IDSで検知するもの

	ベンダ提供 検出方法	ユーザ作成 検出方法
1．パターン （シグネチャ）	検出ロジック 正規表現	記述能力・閾値 バイナリ・閾値・フィルタリング他
2．異形 （アノマリ）	RFC違反 独自	項目選択・閾値
3．変則 （アノマリ）	帯域変化 通信先変化	項目選択・閾値

フォールスポジティブ
（誤検出・誤遮断）

フォールスポジティブ
1．攻撃ではない
2．影響がない
別OS、対応済み
3．確認が取れない

カスタマイズ性
（閾値・フィルタリング）

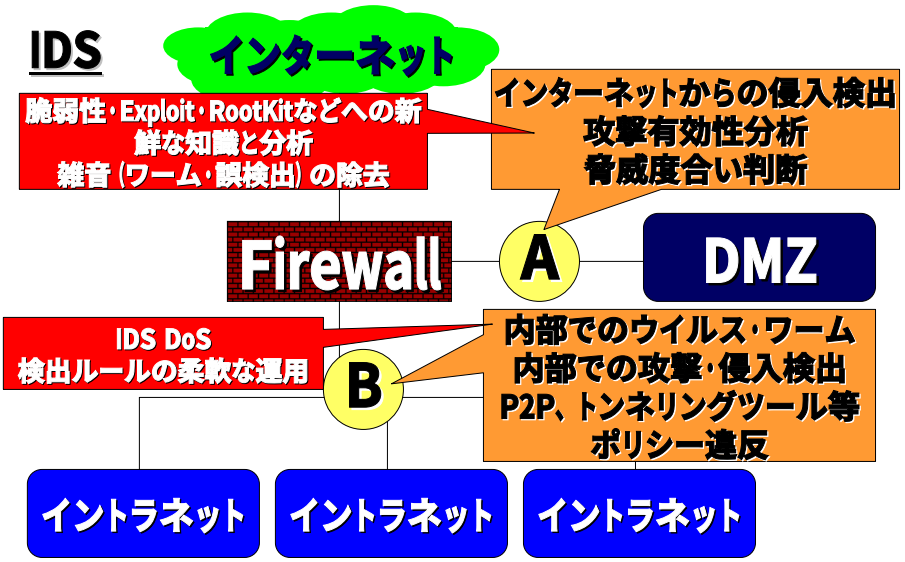
運用容易性

フォールスネガティブ
（パフォーマンス）

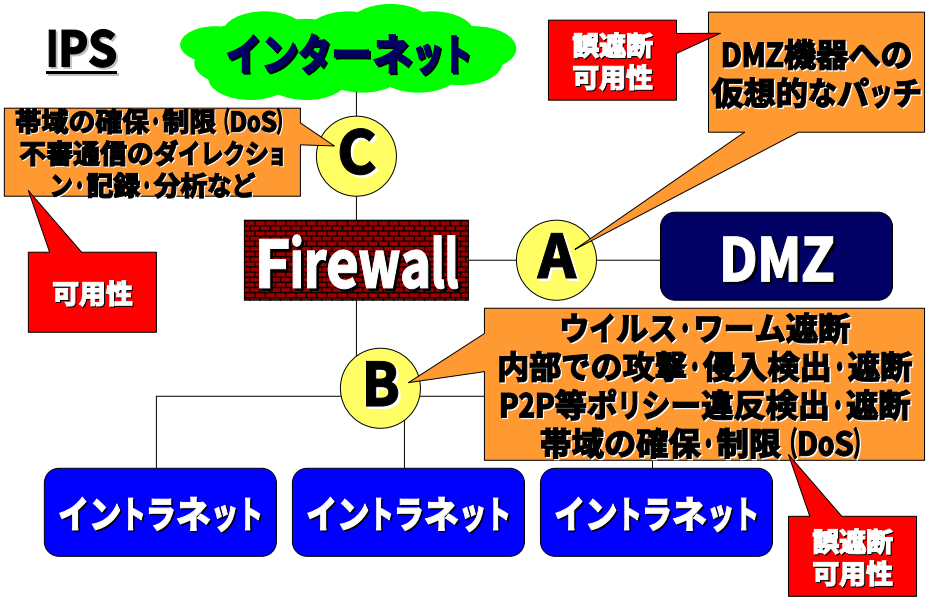
証拠能力
（セッション・ペイロード）

可用性

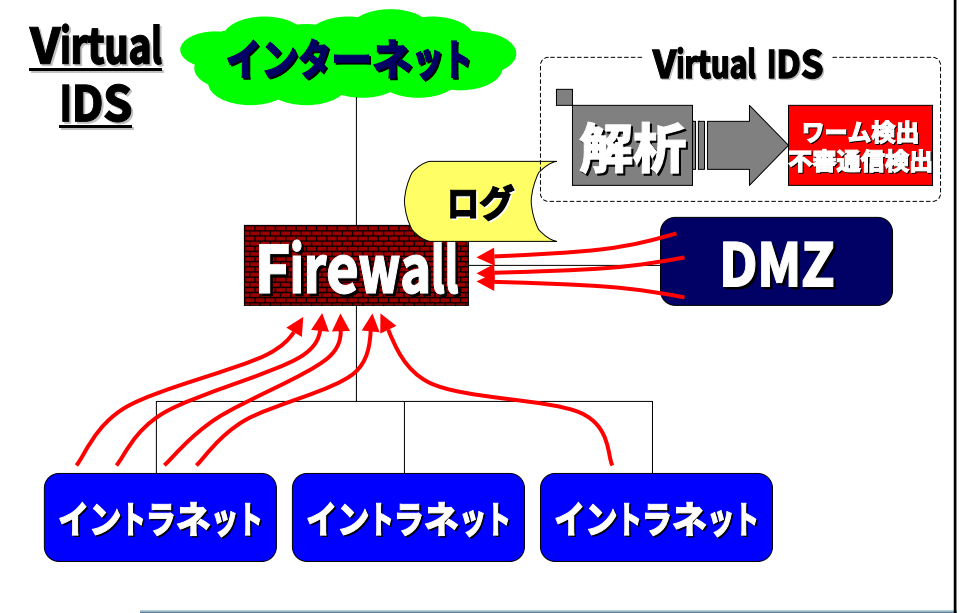
6．4．センサー（IDS、FW）の特性と使い方



6．4．センサー（IDS、FW）の特性と使い方



6．4．センサー（IDS、FW）の特性と使い方



6．4．センサー（IDS、FW）の特性と使い方

検出後の対応

IDS	1．RSTパケット	IDS DoS UDP、ICMP 間に合うか
	2．Firewallと連携	全通信遮断 どっちをとめるか
	3．人間が対応	ワームにはうざったい 間に合わない
IPS	4．遮断	RSTの取り扱い 攻撃元・先
	5．緩和	単位 BPS、PPS、TPS

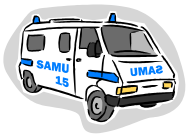
6．4．センサー（IDS、FW）の特性と使い方

DoS

悪意は
ないかもしれない

レイヤイメージ		脅威元・手法など	発生脅威
7	データベース	デッドロック 排他制御 連打ユーザ	処理不能・遅延
6	サーバアプリ	スレッド・キュー 排他制御 連打ユーザ	少数ユーザによる資源浪費 一般ユーザ処理不能
5	サービスアプリ	リクエスト数 低速回線ユーザ 連打ユーザ	新セッションのリジェクト
4	TCP	Syn Flood セッション数	プロトコルスタック Firewall等セッション管理 新セッションのリジェクト
3	IP	UDP、ICMP Flood Smarf	ノードダウン ネットワークのパンク

7. インシデントレスポンス



7. インシデントレスポンス

1) レスポンス(対応)のカテゴリ(制度面)

①内部
- (1) 脅威の把握と適用事態選択
- (2) エスカレーション・フロー
- (3) Verticalラインでの情報収集とIRTを中心とした指揮

②外部
- (1) CSIRT、ISP、キャリア など
  - ・情報交換
  - ・協力要請
- (2) マスメディア
- (3) 取引先
- (4) 株主
- (5) 警察
- (6) 監督官庁・業界団体・親会社など
- (7) 通報者

7. インシデントレスポンス

2) レスポンス (対応) のカテゴリ (技術面)

有事対応

(1) 応急処置 (分～時間：例 30分以内)
→ 被害拡大防止、被害封じ込め、証拠保全
(2) 緊急対応 (時間～日：例 2日間以内)
→手法特定、脅威の推測 (技術面) 、被害範囲の特定
目的推測 (社会面) 、攻撃元への一次対応
本格対応までの対抗策
(3) 本格対応 (日～週～月)
→ 原因などから、再度事前策を策定し、実施
→ 残存被害がないか、再度被害が出ないか、点検・監視
→ 攻撃元への根絶対応

7. インシデントレスポンス

3) 応急処置

①「被害や犯罪が顕著化しているケース」
(1) 被害が拡大しないように、他に影響しないように隔離
→ 対象機器を切り離す。(物理的、論理的)
→ 場合によってはシステム全体を切り離す
(2) 証拠保全
→ 基本的に、シャットダウン、余計な操作は厳禁
調査の為、届出の為 (被害者としての証拠)
②「侵入されているが被害はまだ」
(1) 被害が発生しないように、攻撃者から隔離 (緊急防御)
→ 対象機器を切り離す。(物理的、論理的)
→ 場合によってはシステム全体を切り離す
(2) 証拠保全
→ 基本的に、シャットダウン、余計な操作は厳禁
調査の為、届出の為 (被害者としての証拠)

拡大防止
証拠保全

⇒ 通常は、応急処置として電話などで指示する。

7. インシデントレスポンス

3) 応急処置

③ 責任者へ第一報
顕在化している被害等から判断し、先の①、②に並行し実施。
(1) 可能性のある宣言レベル
(2) 晒されている脅威の可能性
→社会面を中心に

④ 関係部署などへ連絡
責任者から実施するのか、IRTで実施するのかは、役割分担を含め、
事前取り決めだが、その取り決めに従い、実施。
連絡系はVerticalとHorizontalがある。
→ 何 (開示内容) を何処に誰がどのように (確実・信頼) 連絡するのか？

⑤ 外部からの通報であった場合
通報者へ対応状況の連絡 → 何を連絡するのか？事前検討項目
※ 場合により通報者への初期動作のまずさで、風評被害など別の脅威
へ発展可能性あり。慎重に対処。

7. インシデントレスポンス

4) 緊急対応

①手法特定
顕在化している被害や稼動サービスや構成及び痕跡などから
侵入ルート、侵入手法を特定・推測、可能なら一次攻撃元特定
→ 何が信用できるか？、複数を想定
②脅威の推測 (技術面)
起こしえる技術的脅威を推測
→ 顕在化している機器のみ？情報？稼動？
③目的推測 (社会面)
顕在化している被害や行動痕跡から、目的を推測
→ 自己顕示レベル、確信犯 (経済的、思想的、)

⇒ この時点で、責任者に一次報告が妥当
(1) 提言する宣言レベル
(2) 社会面での脅威
(3) 証拠データ、論拠
並行して、関係部署などへ連絡
→ 何 (開示内容) を何処に誰がどのように (確実・信頼) 連絡するのか？

暫定復旧
原因把握

7. インシデントレスポンス

4) 緊急対応

④被害範囲の特定
被害範囲を特定或いは推測する
→ 技術面
現実に発生している内容
→ 社会面
現実に発生している内容
今後、発展する可能性

この時点で、責任者に二次報告が妥当
(1) 提言する宣言レベル (変更)
(2) 社会面での脅威 (変更) と技術面の脅威
(3) 証拠データ、論拠

並行して、関係部署などへ連絡
→ 何 (開示内容) を何処に誰がどのように (確実・信頼) 連絡するのか？

7. インシデントレスポンス

4) 緊急対応

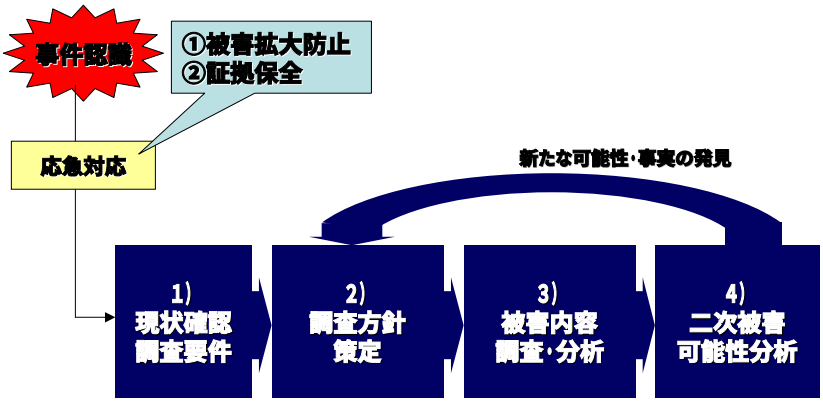
⑤本格対応までの対抗策
暫定対応は可能か？ 技術面・社会面
自組織だけで実施可能か？ (ISP、キャリア、CSIRT)

⑥攻撃元への一次対応
攻撃元への連絡など

⑦緊急対応フェーズのクローズ
基本的に、危機状態を脱したと責任者の判断でクローズ
通常は、Yellowモードで警戒態勢を引く
→ 警戒態勢の定義・範囲

7. インシデントレスポンス

5） 緊急対応時のフォレンジックス



7. インシデントレスポンス

5） 緊急対応時のフォレンジックス

（1）現状確認・調査要件

① 現状確認
(1) わかる範囲でヒアリング
発見方法・その後の対応内容・発生している事象など
ネットワーク・システム構成・関係者・体制・使用ソフト・バージョンなど

② 調査要件 ゴールの決定

(1) どこまで何を調査するのか？ 目的

① インシデントを明確に確認できればよい？
② 侵入経路・侵入方法等を徹底的に調査し、犯人を特定する？
③ 削除されたデータを復旧する必要がある？

(2) 制限時間？

7. インシデントレスポンス

5） 緊急対応時のフォレンジックス

（2）調査方針策定

1）概ね内容が推測できるか？（外部から？内部で？）

(1) 痕跡から調査
※ 攻撃＆侵入により例えばWeb改ざんなどが起こった場合によく適用される
① 詳細な調査には、コスト、時間、経験、高度なスキルが必要
② 道具
③ 課題
揮発性痕跡
(複数回にわたる改ざん行為などの) HDD に残っていない痕跡

(2) 消去法で調査
※ 内部関係者により例えば個人情報漏洩などが起こった場合によく適用される
① ルート・手法別に現状の構成と可能性、ログや痕跡から消去法にて実施

(3) いずれにせよ
調査範囲の確定と、項目別の調査方法を決定する

7. インシデントレスポンス

5） 緊急対応時のフォレンジックス

（3）被害内容調査・分析

1. ディスクイメージから調査

2. 稼動させたままで調査

メモリの状態
プロセスの状態、ポートの状態
活動内容
画面、ポート など
ファイル
テンポラリ、プログラム・スクリプト、設定、データ、ログ
オリジナル性、追加、削除
ログ システム、アクセス、アプリケーション、エラー など

3. 分析　手法、実施内容、時期 など

事前の仕掛け (記録)	道具

7. インシデントレスポンス

5） 緊急対応時のフォレンジックス

（4） 2次被害可能性分析

調査した結果、、
表に出ている以外の事実や可能性が出てきた場合
よくあるケース（最初から想定しておく）

① Webが改ざんされ調査したところ、以前からの侵入痕跡が見つかった、、
② 情報漏えいで過去のアクセスログを調査したところ、不審なアクセスが多数見つかってしまった、、
③ ウイルスの一斉調査を行ったところ、トロイの木馬も複数見つかってしまった、、

7. インシデントレスポンス

6） 本格対応

①制度的対応
（1）プロジェクト編成
（2）渉外担当
（3）セキュリティポリシー等
（4）教育・訓練

正式復旧
再発防止

②技術的対応
（1）対抗策 策定・実施（抑止、予防、防御、検知、回復）
（2）点検・監査

※ 過剰・過敏 過小・鈍感

7. インシデントレスポンス

7) カテゴリ 分類例 例

基本的に優先度を付けてBox毎に体制や手順を整備
訓練を実施

カテゴリ	概要	Red	Orange	Yellow	Green
A	基幹システムに関わる	復旧が見込めない障害	3時間以上の停止が見込まれる Redの可能性がある	3時間未満の停止 Orangeの可能性がある	
B	クライアント環境に関わる	復旧が見込めない大規模な障害	3時間以上の停止が見込まれる Redの可能性がある	3時間未満の停止 Orangeの可能性がある	
C	外部からのセキュリティ攻撃	侵入されている	侵入される可能性が高い	悪質な攻撃	
D	セキュリティ事件	情報漏えいが発覚	情報紛失が発覚	セキュリティポリシー違反行為 情報紛失につながる事故	

8. 実践レベル

8. 実践レベル

1) 判断基準

① コンプライアンス
- (1) 不正アクセス禁止法
- (2) 著作権法
- (3) 個人情報保護法・常識 など

最低限

管理してます
1. 管理項目の明確化
2. 管理実施の証明 ⇒ 記録
   実施項目の同意、実施事項
3. トレーサビリティ
4. 違反者摘出と対応 ⇒ 抑止

② 要求されている社会的責任
- (1) 重要インフラ
  ⇒ 行政、金融、情報通信、電力、ガス、航空、鉄道
- (2) 大企業など
  ⇒ 物理的被害 (人命、火災など)
  経済的損失 (サプライチェイン、など)

③ 自己被害防止
- (1) 自分の要求レベル

8. 実践レベル

2) 実施レベル概要

① コンプライアンス確保
- (1) 管理項目の明確化
  方針の告知、セキュリティポリシー
- (2) 管理実施の証明 ⇒ フォレンジックス
  伝達実施と記録、教育実施と記録
  ポリシー規定項目の実施と記録
  ⇒ グループウェアの有効活用

最低限

② パッシブセキュリティ対策
- (1) トレーサビリティ ⇒ フォレンジックス
- (2) セキュリティ監視 ⇒ フォレンジックス
- (3) 防御策中心の組み立て

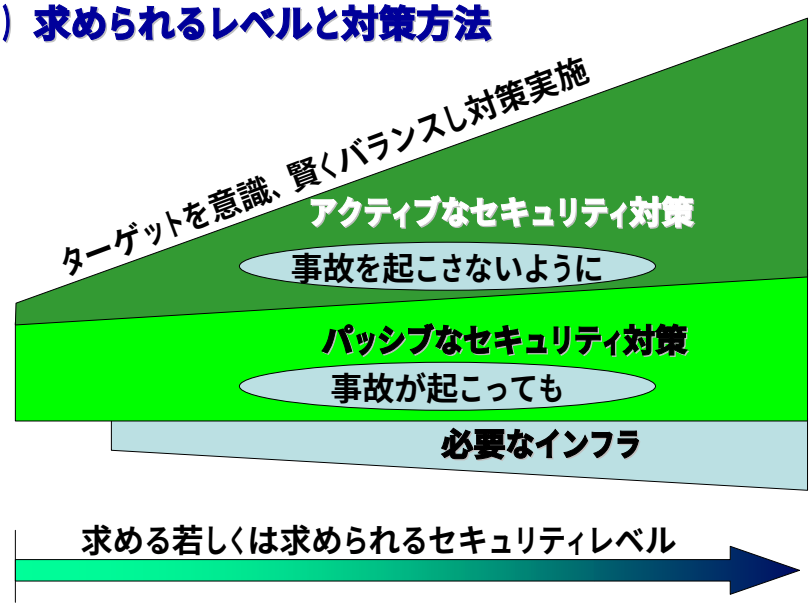
万一の時でも
最悪、こうできる

③ アクティブセキュリティ対策
- (1) 予防策
- (2) 抑止策

事件を
発生させないように

8. 実践レベル

3）求められるレベルと対策方法



8. 実践レベル

4）定義レベル 例

レベル	対　象
1 コンプライアンス（公開サイトなし）	インターネット利用のみ システムなどは基本アウトソース 個人情報保持対象企業ではない
2 コンプライアンス（公開サイトあり）	インターネット利用と公開サーバ 個人情報保持対象企業ではない
3 標準	インターネット利用と公開サーバ 個人情報保持対象企業ではない 社内で種々の情報システムが稼動している
4 高セキュリティ	個人情報保持対象企業 E-コマースサイト 重要インフラ部門 セキュリティ事故発生組織
5 超セキュリティ	大きな社会責任を負っている 大量の個人情報を取り扱っている 事業基幹となるE-コマースサイトを運用 など

ISMS　Pマーク

8. 実践レベル

5) レベル別 セキュリティ管理実装 例

レベル ＼ 対象	文書	コンプライアンス管理	ワークフロー	教育・訓練
1 コンプライアンス(公開サイトなし)	就業規則においてIT機器の適切な取り扱いを明記	現状とかわらず	現状とかわらず	現状とかわらず
2 コンプライアンス(公開サイトあり)	情報セキュリティ基本方針 公開サイトに関わる管理規定 IT利用に関わる利用規定 個人情報保護取り扱い規定	現状とかわらず	現状とかわらず	現状とかわらず
3 標準	情報セキュリティ基本方針 公開サイトに関わる管理規定 IT利用に関わる利用規定 個人情報保護取り扱い規定	文書発行、メンバー閲覧記録 教育記録	規定の実施に関わる申請・承認の記録	ITセキュリティ教育プログラムと定期的な実施
4 高セキュリティ	ISMS、Pマークでの要求	情報収集＆分析 記録 文書発行、メンバー閲覧記録 メンバーコメント記録 教育記録	規定の実施に関わる申請・承認の記録	ITセキュリティ教育プログラムと定期的な実施
5 超セキュリティ	独自な安全基準による要求	情報収集＆分析 記録 文書発行、メンバー閲覧記録 メンバーコメント記録 教育記録	規定の実施に関わる申請・承認の記録	ITセキュリティ教育プログラムと定期的な実施

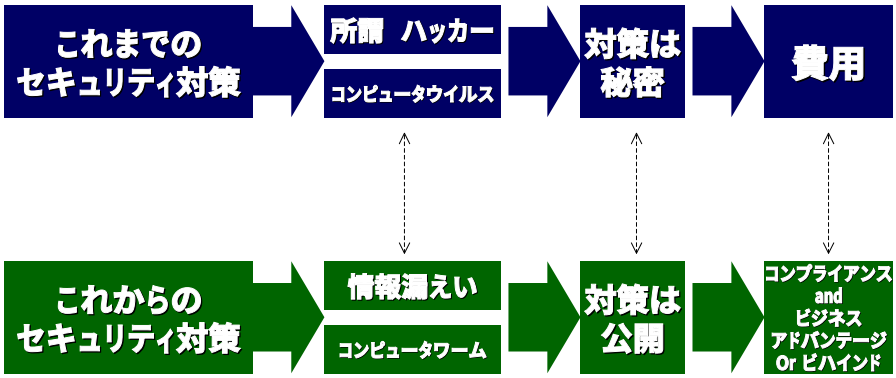
8. 実践レベル

6) レベル別 セキュリティ対策実装 例

レベル ＼ 対象	公開サイト	ネットワーク GW	サーバ	クライアント
1 コンプライアンス(公開サイトなし)		イントラワーム感染検知	なし	アンチウイルス WindowsUpdate
2 コンプライアンス(公開サイトあり)	Firewall IPS or 公開サービスパッチ・設定 定期的	イントラワーム感染検知	なし	アンチウイルス WindowsUpdate
3 標準	Firewall 公開サービスパッチ・設定 1W以内	イントラワーム感染検知 アンチウイルスGW	パッチ運用 1W以内 資産管理	アンチウイルス一括管理 WindowsUpdate ファイアウォール 暗号化
4 高セキュリティ	Firewall 公開サービスパッチ・設定 3日以内 IDS監視 SecureOS	アンチウイルスGW IPS 隔離LAN、検疫LAN、隔離LAN セキュリティポリシー違反監視 経路暗号化	パッチ運用 3日以内 資産管理 行動監視 (ファイルサーバ、DB) SecureOS	アンチウイルス一括管理 パッチ・設定管理 ファイアウォール 暗号化 資産管理・機能抑制 行動監視
5 超セキュリティ	Firewall 公開サービスパッチ・設定 即日 IDS監視 TrustedOS	アンチウイルス IPS 隔離LAN、検疫LAN、隔離LAN 物理セキュリティとの統合監視 経路暗号化	パッチ運用 即日以内 資産管理 行動監視 TrustedOS	アンチウイルス一括管理 パッチ・設定管理 ファイアウォール 暗号化 資産管理・機能抑制 行動監視 SecureOS

8. 実践レベル

7）最後に



公開できるセキュリティ対策の実施が必須となる
（自慢しよう！あなたのセキュリティ）

ご質問？

お問い合わせ ： itsuro@lac.co.jp