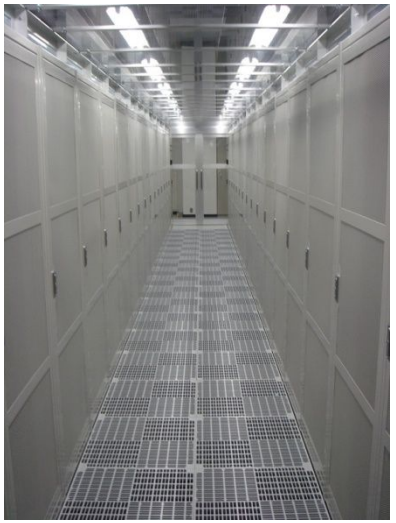
脆弱性診断（ペネストレーションテスト）

株式会社チェリーネットワーク



Ver.1.0

1.セキュリティ監査（総合）

【外部監査】

・ペネトレーション［侵入突破］

調査対象に対して、不正侵入者と同等な立場に立ち一切の予備知識・予断を廃したゼロ知識を前提に、侵入突破し内外を探査しすべてのセキュリティホールを検証し対策まで提示する調査方法
（キーボードオペレーションで、Firewall等を突破する高度な技術が前提となる）

ーウォーダイアリング（バックドア）

ダイアルアップルートの発見と侵入の可能性調査

【内部監査】

・内部の体制、ネットワークシステム、オペレーション、最新のソフト対応状況

ー内部外部のセキュリティシステムの構成、設定
ー重要サーバー検査
ーセキュリティに関する人的管理、指示系統
ー教育管理状況
ー通信インフラ、プロトコルなど
ー各種ログの分析

【物理的監査】

・オフィースの物理的セキュリティに対する監査

ー監視カメラ有無、入場者チェック、ゴミ捨て場への侵入の可否等を含む
ーソーシャルエンジニアリング

外部からの成りすまし電話や従業員、下請け、及び客に成りすまして侵入し情報収集する活動

ートラッシング（ごみ箱を漁る等の活動）

2-1.総合セキュリティ監査概要図

外部監査

Internet

公衆電話網

ユーザーのヒヤリングを行い、
社内を調査・立入検査を実施する

アタック

アタック

アタック

DNSサーバ

WWW／Mailサーバ

ルータ

DMZ

RASサーバ

ファイアウォール

外部サーバー群

内部ファイアウォール

Ｐｒｏｘｙサーバ

監査用ＰＣ

不正設置モデムも探査

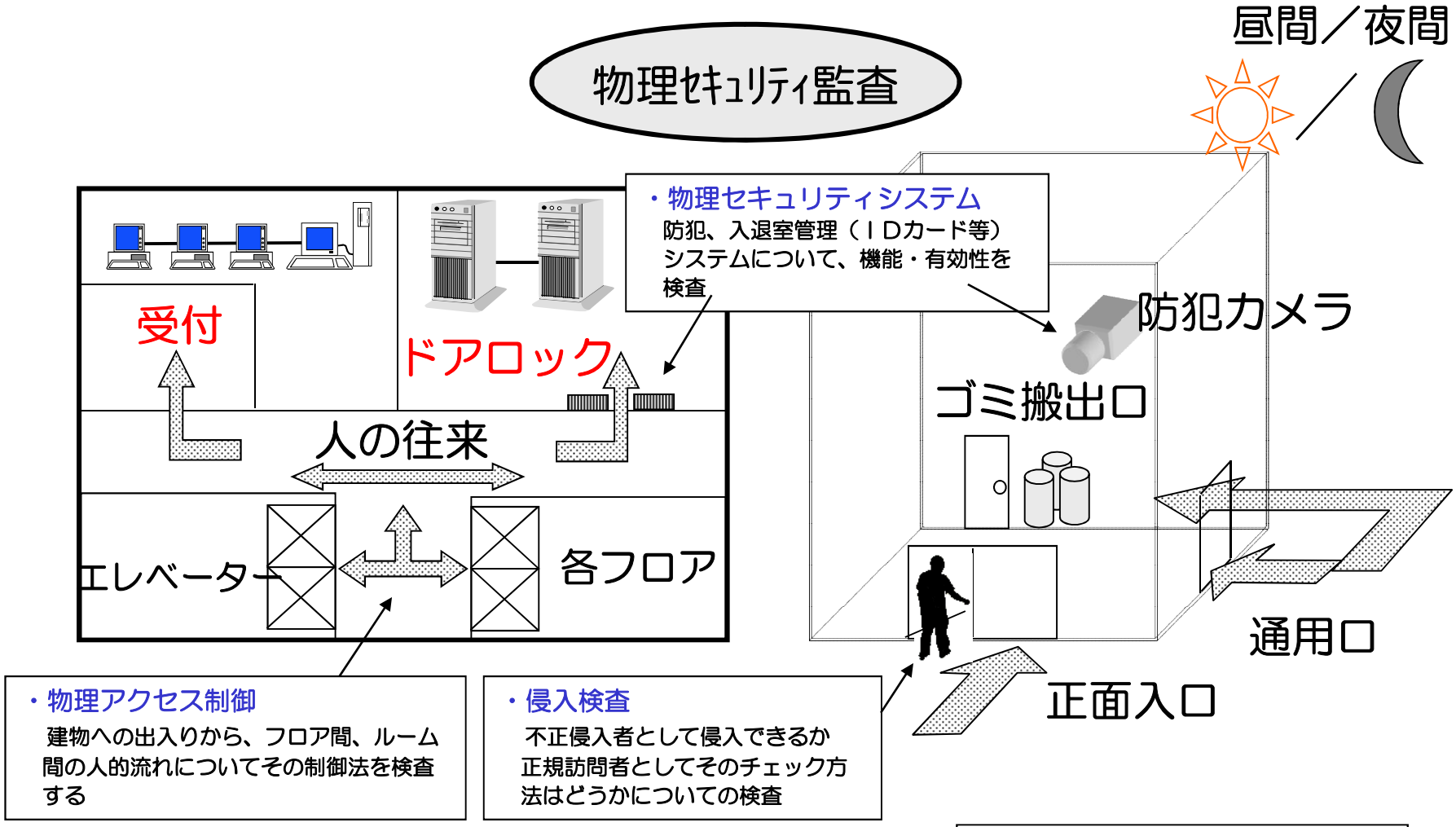
モデム

物理ｾｷｭﾘﾃｨ監査

内部監査

- ｾｷｭﾘﾃｨｼｽﾃﾑの構成・設定の監査
  - ﾈｯﾄﾜｰｸのｾｷｭﾘﾃｨｼｽﾃﾑを調査
  - ｾｷｭﾘﾃｨ機器類の設定状況等を調査
- 重要サーバの検査
  - ＯＳﾊﾞｰｼﾞｮﾝのチェック
  - ｱﾌﾟﾘｹｰｼｮﾝの種類、ﾊﾞｰｼﾞｮﾝのチェック
- 人的管理、指示系統の監査
  - 組織の構成、権限、指示系統の監査
- ｾｷｭﾘﾃｨ管理状況の監査
  - ｾｷｭﾘﾃｨ管理・運用状況・体制を監査
- ｾｷｭﾘﾃｨ教育の監査
  - ｾｷｭﾘﾃｨ教育ｼｽﾃﾑ・達成度を監査
- 基幹システムに対する監査
  - 重要な処理、重要なﾃﾞｰﾀ
- TCP/IP以外のプロトコルへの監査

2-2.物理セキュリティ監査概要図



3．診断サービスについて

（1）サービスの目的

サーバ診断サービスでは、お客様のネットワーク上に存在するサーバに対して、
攻撃者と同じ手法を用いて疑似攻撃を実施し、OSやサービス（アプリケーション）
に潜むセキュリティホールの有無、設定の不備を確認いたします。

（2）診断実施方法

⑷外部監査／リモート診断

弊社社内から、お客様の公開サーバ（サービス）に対して、診断を実施します。

⑹内部監査／オンサイト診断

弊社エンジニアが御社内にて、サーバに対して、診断を実施します。

⑹物理監査／オンサイト診断

弊社エンジニアが御社内にて、フロア・システム等に対して、診断を実施します。

4-1．診断の流れ

（1）診断実施前

お客様と弊社の間で、機密保持契約を締結させて頂きます。
お客様より『サーバ診断申込書』によりお申し込み頂き、日時を調整して弊社より
『サーバ診断確認書』を提出させて頂きます。

（2）診断実施

⑷診断開始前

診断担当者から、作業開始前に担当者様にご連絡いたします。
連絡が取れるまで、診断作業は実施いたしません。

⑹診断実施中

診断作業は、診断対象サーバのサービスが停止しないように実施いたしますが、サーバ自体の性能、または途中経路にあるネットワーク機器の性能などにより、サービスが停止してしまう可能性があります。その場合、早急に担当者様にご連絡いたします。
診断中に、緊急性の高い脆弱性が発見された場合、早急に担当者様にご連絡いたします。
診断を継続するか否かにつきましては、担当者様にご判断頂きます。

⑹診断終了後

診断担当者から、作業終了後に担当者様にご連絡いたします。

（3）報告会

お客様に訪問し、診断報告会を実施させて頂き、診断の際に判明した脆弱点、および注意点などを報告させて頂きます。

その際に下記の納品物を納品させて頂きます。

なお、実施させて頂くのは、1回とさせて頂いております。

（4）納品物

報告会の際に、以下を納品させて頂きます。

(a)診断報告書　1冊

(b)報告書PDFが保存されたCD-ROM　1枚

5. 診断内容

（1）情報収集フェーズ

攻撃の足掛かりとなるサーバが公開しているサービスやオペーレーティングシステムの種類などの情報を収集します。
公開しているサービスに応じて、使用されているであろうアプリケーション（サービス）のパッケージ名、およびバージョン情報を取得します。

（2）脆弱性確認フェーズ

情報収集フェーズで得た情報を元に、商用、およびフリーツールを用いて、脆弱性の確認を行います。弊社で作成したツール、および手動による脆弱性の確認も同時に行います。
また、脆弱性データベースなどを利用して、該当するサービスのバージョン情報などから、脆弱性の有無を確認します。

（3）総当たり攻撃フェーズ

サーバ上で公開されているサービスによっては、認証機能が備えられている場合があります。
この場合、情報収集フェーズで集められた情報、および一般的によく使用されるユーザ名、およびパスワードを使用して、総当たり（ブルートフォース）攻撃を実施いたします。

（4）その他

サーバ上で公開されているサービスによって、上記に当てはまらないような脆弱性の確認作業を実施します。

6-1．価格

（1）価格表　（お問い合わせください）

価格は、すべて税抜き価格です。

休日、および深夜に実施する場合は、料金の1.5倍となります。

IPアドレス数	リモート診断（1IPあたり）	オンサイト診断（1IPあたり）
1～3		
4～10		
11～∞		

※オンサイト診断に伴う出張費、および宿泊費は別途必要となります。

リモート、およびオンサイト診断の打ち合わせ、報告会に伴う出張費、および宿泊費は別途必要となります。

6-2. 価格

（1）お客様のネットワーク環境

下記に該当する場合、診断結果が正しく報告されない場合がありますので、あらかじめご了承ください。

⑷ロードバランサーなどにより、負荷分散を実施されている場合
⑸IDS/IDPなどを設置されている場合
⑹お客様の特定システムなどを設置されている場合

お問い合わせ先

ＩＴまたセキュリティ関連のご相談などお気軽にご連絡ください。

株式会社チェリーネットワーク
代表取締役社長

森谷　礼裕

〒226-0024
神奈川県横浜市緑区西八朔町３７－３８
TEL&FAX　045-934-9849

URL：http://www.cherrynetwork.jp
E-Mail：ymoriya@cherrynetwork.jp