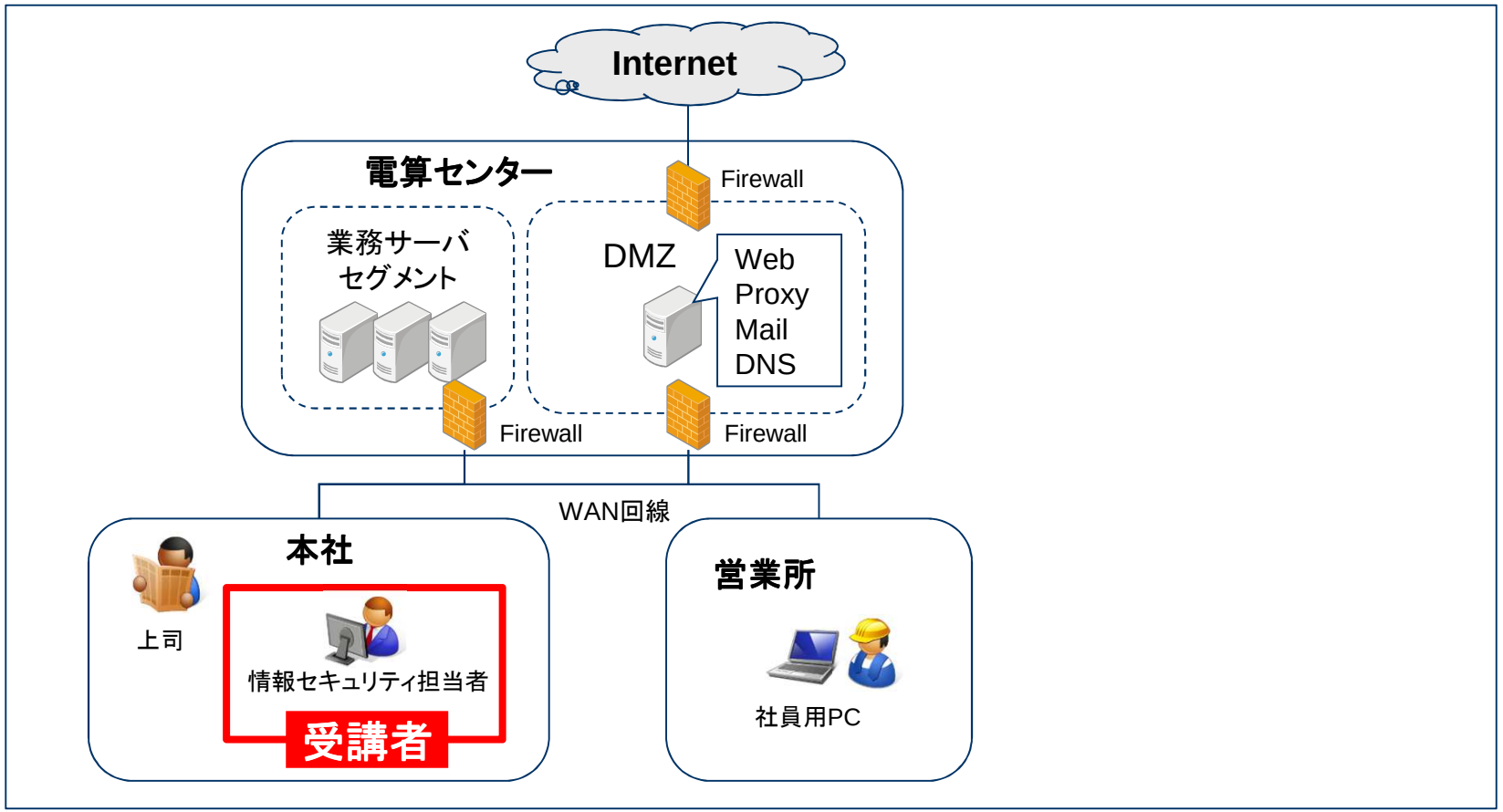
模擬訓練の概要

- 皆さんは，情報セキュリティ担当者チームです。
- 通常業務を行いながら，電子メールで通知される「ウィルス検知アラート」を監視し，必要な対応を実施してください。



模擬訓練の対応範囲

- **情報セキュリティ担当者チームは，下表の対応を実施します。**

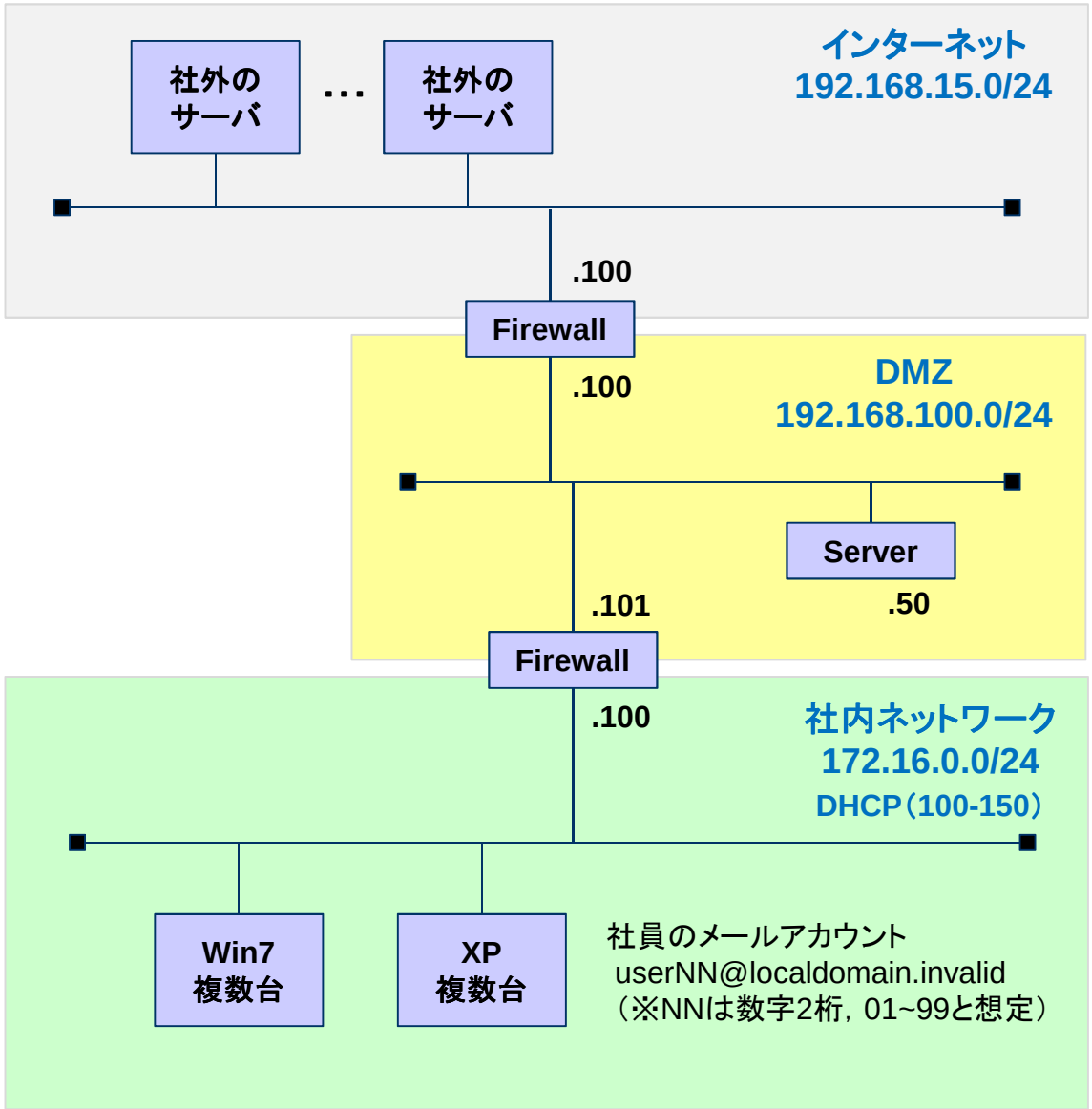
大分類	説明	説明
1.ウィルス検知アラートの監視	(1)ウィルス検知アラートの分析	• 社内PCでウィルス検知が発生すると，システム管理者に電子メールで自動通知されますので，都度，内容を確認します。
	(2)感染有無の判断	• 必要に応じて，社内PCを利用している社員への聞き取り調査を実施し，社内PCの感染有無を判断します。 • 判断した結果を上司に報告します。
2.感染事案の対応 社内PCが感染していると判断した場合の対応	(1)被害拡大防止措置	• 感染した社内PCの利用者に連絡し，ネットワークから隔離します。 • WEB経由の感染の場合は，攻撃元サイトを特定し，Proxyで遮断します。 • メール経由の感染の場合は，差出人メールアドレス，送信元MTAのIPアドレスを特定し，自社MTAで遮断します。
	(2)検体確保	• 感染した社内PCから，マルウェアの検体を確保し，ウィルス対策ソフト開発元に送付します。
	(3)影響調査	• Proxyログ，自社MTAログなどを調査し，感染が疑われる社内PCが存在しないか確認します。

模擬訓練の進行方法

- 各段階において，最初に各自で，考えの整理（または解析作業）を実施してください。
- 次に，各自の考えをチーム内で発表したうえで，チームの意見を様式1にまとめ，上司（講師）に報告・提案してください。

項目	説明
1.検知/状況整理	• 電子メールで通知されるウィルス検知アラート（講師が印刷したものを提供）を確認し，検知に至った状況の仮説を設定し，感染の有無の判断する。 ［ねらい］ウィルス検知アラートから，感染の有無を判断できるか確認する。
2.判断	• 検知報告書を作成し，上司（講師）に状況と対応方針を報告する。 ［ねらい］判断の理由を第三者に説明できるか確認する。
3.被害抑止/調査	• 「感染無し」と判断した場合は，当該検知の対応は終了とし，次のウィルス検知アラートの発生まで待機する。 • 「感染有り」と判断した場合は，感染拡大防止措置ならびに感染端末の調査を実施する。 　• ネットワーク機器の設定変更は，システム運用会社（講師）に口頭で作業を依頼する。 　• 感染端末の調査は，「検体の確保」および「感染拡大防止措置に必要な情報収集」の2つの目的で実施することとし，エビデンスは現地作業員（講師）が取得したデータをUSBメモリ等で提供する。 　• なお，感染を見逃した場合は，社外のお客さま（講師）からの連絡などにより，感染事象の発生を伝える。 ［ねらい］感染拡大防止措置の具体的な方法を指示できるか確認する。
4.訓練終了	• 感染拡大防止措置の実施ならびに検体確保が完了した時点で，講師が訓練終了を宣言する。

模擬訓練のシステム構成



社内ドメイン

localdomain.invalid
※上記以外は全て社外のドメインと想定

DMZ Server

- OS : CentOS 5
- DNS : BIND 9
- SMTP : postfix
- POP3 : dovecot
- Proxy : Squid 2

社内PC

- OS : Windows7/XP
- Mailer : Thunderbird, Outlook Express
- Adobe : 最新版
- Java : 最新版

※ウィルス対策ソフトおよび管理サーバが導入されていると想定（訓練の都合上，実際にはインストールしていません）